민 간 사 이 버 안 전 매 뉴 얼

한국정보보호진흥원
인터넷침해사고대응지원센터

기업 정보보호 담당자용

민간사이버안전매뉴얼

한국정보보호진흥원

기업 정보보호 담당자용

민간사이버안전매뉴얼

www.kisa.or.kr, www.krcert.or.kr

한국정보보호진흥원
인터넷침해사고대응지원센터

주 의 사 항

이 매뉴얼의 사용에는 어떠한 제한도 없지만 다음과 같은 사항에 주의하여야 합니다.

- 문서 내에 언급된 상표, 제품명 등에 대한 권리는 각 상표 또는 제품을 소유한 해당 기업에 있으며, 설명을 위하여 특정 회사 제품명이나 화면이 표시된 경우 "제 1 장 1. 목적"에 정의된 매뉴얼의 고유 목적 외에 다른 어떠한 목적도 없으며 그렇게 이용되어서도 안 됩니다.

- 문서 내에 기술된 예시 등은 일반 사용자, 기업 등에 있을 수 있는 고유한 환경을 고려하지 않았으므로 실제 환경에서는 그대로 적용되지 않을 수 있습니다. 그러므로 각 절에 주어진 기술 세부사항(예를 들어 명령어 및 화면 등)을 적용할 때는 먼저 각 환경에 적합한지 시험을 통하여 문제가 없는지 확인하는 것이 필요하며, 내용의 오류로 인하여 발생하는 피해에 대하여 이 매뉴얼의 발행기관은 책임을 지지 않습니다.

※ 이 매뉴얼의 내용 중 오류가 발견되었거나 내용에 대한 의견이 있을 때에는 securitymanual@kisa.or.kr로 해당 내용을 보내주시기 바랍니다.

기업 정보보호 담당자용

민간사이버안전매뉴얼

0101001111010101000001010100011010100010101101001111010101000001010100011010100010101

www.kisa.or.kr, www.krcert.or.kr

정 보 통 신 부

한국정보보호진흥원
인터넷침해사고대응지원센터

발 간 사

초고속 인터넷 보급률 등에서 세계 1위인 우리나라는 IT 강국임을 전 세계로부터 평가받고 있으며 부러움을 사고 있습니다. 이와 같은 우리의 강점을 바탕으로 보다 강력한 IT 국가 실현을 위하여 국가에서는 야심찬 IT 839 전략을 마련하여 실천하고 있습니다. 이러한 비약적인 도약을 보장하기 위해서는 정보화 역기능을 사전에 예방하여 건전한 인터넷 문화를 조성하는 것이 무엇보다도 중요하다고 하겠습니다.

이러한 취지에서 발간한 본 매뉴얼은 기업 정보보호담당자들이 해킹 · 바이러스 등 사이버 위협으로부터 기업의 중요 정보를 보호하는데 필요한 전 분야의 전문적인 예방지식을 습득할 수 있는 기회를 제공하는데 목표를 두고 국가안전보장회의, 국가정보원 등과 긴밀한 협조 하에 작성하였습니다.

주요 내용으로는 인터넷침해사고 예 · 경보체계 및 예 · 경보 각 단계별 대응요령, 전사차원의 보안관리, 주요 서버 및 네트워크 장비의 보안관리 방법, 바이러스 백신, 침입차단 및 탐지시스템 등 보안제품의 운영방법, 무선랜의 운영방법 등 보안운영자가 꼭 알아야 할 전문적인 사항들로 전 영역에 걸쳐 구성되어 있습니다.

아무쪼록 본 매뉴얼이 기업 정보보호담당자들의 정보보호에 대한 전문성을 높여 기업 핵심 정보들을 철저히 보호함으로써 안전한 인터넷 기반에서 기업 활동을 하는 계기가 되기를 바라며, 향후 정보통신 기술의 발전과 환경의 변화에 따라 지속적으로 보완할 예정이므로 많은 활용과 조언을 바랍니다.

끝으로, 『민간사이버안전매뉴얼』 발간에 참여하여 주신 집필진을 포함하여 귀중한 시간을 내시어 조언과 감수를 맡아주신 여러분께 깊은 감사의 말씀을 드립니다.

2004년 8월

한국정보보호진흥원장 이 홍 섭

추 천 사

1996년 정보화촉진기본법 시행을 시작으로 불과 7, 8년만에 우리나라는 세계 초고속인터넷 이용률 1등 국가가 되는 등 IT 강국으로 발돋움을 하였고, 2004년 4월의 경우 IT 수출이 58억 8천만달러에 달했으며, 2012년 국민소득 2만불 시대를 달성하기 위한 IT 839 전략을 마련하여 적극 추진하는 등 원대한 성장동력을 가동하고 있습니다.

따라서, IT 839 전략 등 IT 강국으로의 지속적인 추진에 큰 차질을 가져올 수도 있는 정보화의 역기능을 해소하여 안전한 인터넷 세상을 구현하는 것은 IT 강국으로의 지속적인 발전을 위한 선택이 아닌 필수라고 하겠습니다.

필수사항인 정보화 역기능 해소를 위해서는 개인컴퓨터사용자들, 기업 종사자들, 인터넷 서비스제공자(ISP) 및 집적정보통신시설(IDC) 운영자, 학교 등 교육기관 소속자들, PC방 환경 관리를 위한 운영자들을 포함하여 모든 개개인들의 정보보호에 대한 인식이 우선되어야 할 것입니다. 즉, OECD에서 주창하고 있는 정보보호문화 운동이 필요하다고 하겠습니다.

이러한 취지에서 발간한 『민간사이버안전매뉴얼』은 인터넷 침해사고의 예방 및 대응 방법, 개인 컴퓨터의 안전한 인터넷 이용방법, ISP/IDC 및 기업내의 보안관리, PC방 등 인터넷 이용환경 제공자의 안전수칙 등을 담고 있어 정보화 역기능 해소를 통하여 우리나라의 안전한 인터넷 환경을 구축하는데 많은 도움이 될 것으로 기대합니다.

『민간사이버안전매뉴얼』의 발간을 진심으로 축하드리며, 발간을 위해 수고하신 많은 분들께 감사의 말씀을 전합니다.

2004년 8월

정보통신부장관

Contents

목 차

Contents

목 차

제 6 장 보안시스템 운영

제 1 절 바이러스 백신

제 2 절 바이러스 월(Virus Wall)

제 3 절 침입차단시스템

제 4 절 침입탐지 시스템

제 7 장 네트워크 보안관리

제 1 절 시스코 라우터의 기본 보안

Contents

목 차

Contents

목 차

제 4 절 구현

제 5 절 사후관리

부록

Contents

표목차 및 그림목차

표목차

그림목차

Contents

표목차 및 그림목차

Contents

표목차 및 그림목차

Contents

표목차 및 그림목차

Contents

표목차 및 그림목차

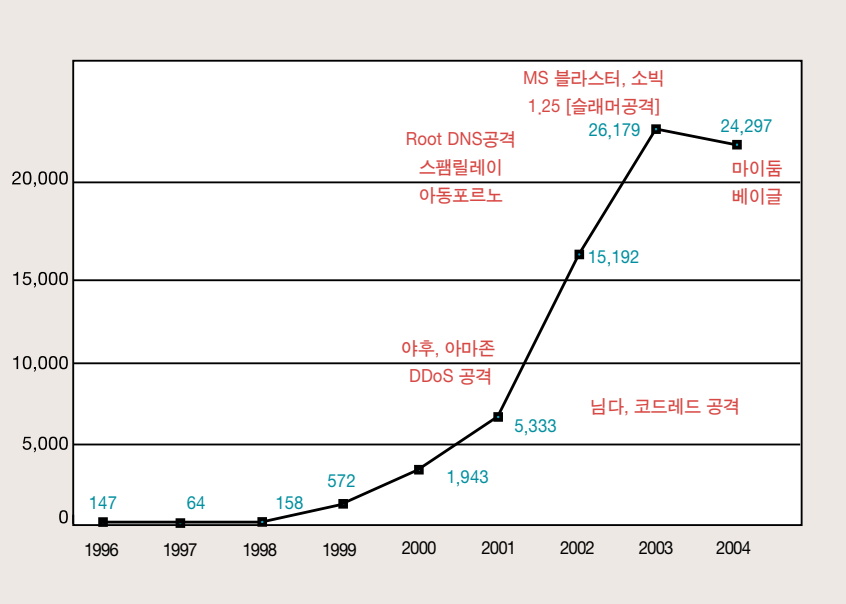
c o n t e n t s

제 1 장
개 요

1. 목적

초고속 인터넷이 사회 전반에 걸쳐 급속하게 보급되면서 과학 기술 뿐 아니라 경제, 문화 등 사회 전반에 걸쳐 인터넷 의존도가 높아지고 있다. 이와 같은 인터넷의 발전과 함께 해킹, 웜/바이러스 등 인터넷 침해사고의 공격 유형도 갈수록 지능화되고 있으며 매년 증가추세를 보이고 있다. 또한 높아진 인터넷 의존도로 인하여 인터넷 침해사고는 이제 특정 개인/기업의 문제가 아닌 범 국가적 이슈가 되고 있다.

인터넷침해사고의 증가
(그림 1-1-1)

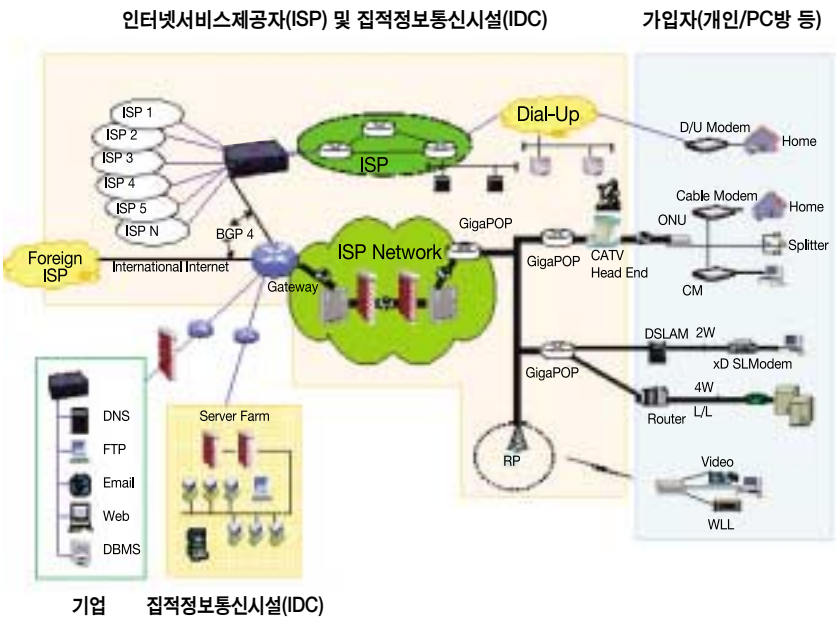


이 매뉴얼은 기업의 정보보호담당자들에게 인터넷 침해사고의 예방 및 대응요령을 제공하고자 한다.

2. 적용범위

이 매뉴얼의 적용범위는 민간부문이며 구체적인 대상은 다음과 같다.

- 기업의 정보보호담당자(또는 서버/네트워크 관리자)



국내인터넷 구성도 예시
(그림 1-1-2)

3. 용어정의

이 매뉴얼에서 사용한 용어의 정의는 다음과 같다.

[표 1-1-1] 용어정의

용 어	정 의
전자적침해행위	• 해킹, 컴퓨터바이러스, 논리 · 메일폭탄, 서비스거부 또는 고출력 전자기파 등을 사용하여 컴퓨터 시스템이나 인터넷 망을 공격하는 행위
침해사고	• 전자적 침해행위로 인하여 발생하는 사고
인터넷 침해사고	• 인터넷 망과 관계된 침해사고
민간 사이버 안전 대응 매뉴얼	• 인터넷침해사고 예방 및 대응을 위한 민간부문의 종합적이고 체계적인 예방 및 대응을 기술한 본 문서
예방 및 대응주체	• 민간부분의 인터넷 침해사고 예방 및 대응을 위하여 본 매뉴얼을 이행하는 개인 사용자, 기업 서버/네트워크 관리자, ISP, IDC를 말함
경보 단계	• 보안취약점, 웜/바이러스 등 보안위협을 전파력과 공격 위험도등 심각한 정도에 따라 수준을 정의한 것으로 정상, 관심, 주의, 경계, 심각의 5단계로 구분됨
경보 체계	• 침해사고 경보 단계를 발령하는 기관과 각 단계에 따라 예방 및 대응주체가 침해사고의 예방 및 대응을 수행하는 체계
스팸 릴레이	• 침해사고 경보 단계를 발령하는 기관과 각 단계에 따라 예방 및 대응주체가 침해사고의 예방 및 대응을 수행하는 체계
해 킹	• 다른 사람의 컴퓨터나 정보시스템에 불법 침입하거나 정보시스템의 정상적인 기능이나 데이터에 임의로 간섭하는 행위
서비스거부	• CPU, 메모리, 대역폭, 디스크 공간 등과 같은 컴퓨팅 자원을 고갈시킴으로써 특정 네트워크, 시스템, 응용 프로그램 등의 사용을 방해하거나 손상시키는 공격 유형
악성코드 공격	• 시스템을 손상시킬 목적으로 작성된 악의적인 코드에 의한 공격유형을 말하며, 일반적으로 웜, 바이러스, 트로이목마 등으로 구분 - **웜**(Worm) : 독립적으로 자기복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드 - **바이러스**(virus) : 컴퓨터 프로그램이나 메모리에 자신 또는 자신의 변형을 복사해 넣는 악의적인 명령어들로 조합하여 불특정 다수에게 피해를 주기 위한 목적으로 제작된 모든 컴퓨터 프로그램 또는 실행 가능한 코드 - **트로이 목마** : 자기복제능력은 없으나, 정상 기능의 프로그램으로 가장하여 프로그램 내에 숨어있는 코드조각으로, 의도하지 않은 기능을 수행하는 컴퓨터 프로그램 또는 실행 가능한 코드

c o n t e n t s

제 2 장
인터넷 침해사고 경보

제 1 절 경보의 정의 및 단계

1. 경보의 정의

가. 정의

● 해킹, 웜/바이러스, 기타 침해사고로 인하여 국내 민간부문 인터넷 망에 영향을 주거나 일반의 인터넷 사용에 지장을 주거나 크게 우려되는 경우 침해사고 예방 및 피해 최소화를 위하여 정보통신부 및 한국정보보호진흥원이 발령하는 대국민 안내

나. 단계

[표 2-1-1] 경보 단계

구 분	설 명
심 각 (Red)	• 국내 인터넷 전 분야에 소통장애 발생 • 주요 정보통신기반시설의 피해로 인하여 대국민 서비스 지장 발생 • 민간부분 전반에 인터넷 사용 불가능 • 국가적 차원에서 공동 대처해야 할 필요성이 있는 상황
경 계 (Orange)	• 복수 ISP망 또는 주요 정보통신 기반시설의 피해 발생 • 해킹 및 신종위협으로 주요기업 및 포털, 연구소 등 민간부문에 중대한 피해 발생 • 웜 · 바이러스, 해킹 등 침해사고로 민간부문에 대규모 피해 발생 • 상황 해결을 위해 민관 각 분야의 협조 및 공동 대응이 필요한 상황
주 의 (Yellow)	• 웜 · 바이러스, 해킹 등으로 국지적 피해발생 • 국지적인 인터넷 소통장애, 인터넷 관련 서비스에 장애가 발생 되거나 매우 우려되는 경우 • ISP/IDC, 일반 사용자, 기업 등의 긴급대응 및 보안태세 강화가 필요
관 심 (Blue)	• 위험도가 높은 웜 · 바이러스, 취약점, 해킹기법 및 공격코드 출현으로 인해 피해 가능성 증대 • 해외에서 침해사고 확산 또는 일부 국내유입 및 확산 가능성 증대 • 국내 인터넷 이상 트래픽 발생 가능성 증대

※ 위험 정도가 낮은 웜 · 바이러스, 해킹기법, 보안취약점이 발견된 경우는 경보 이전 단계인 "정상"(Green) 수준으로 간주

2. 경보 체계

가. 발령 주체

- '관심' 경보는 한국정보보호진흥원(인터넷침해사고대응지원센터)에서 발령
  ※ 정보통신부를 통하여 국가정보원 및 국방부와 사전 협의
- '주의' 경보는 한국정보보호진흥원(인터넷침해사고대응지원센터)에서 발령
  ※ 정보통신부를 통하여 국가정보원 및 국방부와 사전 협의
- '경계' 경보는 정보통신부에서 발령
  ※ 정보통신부에서 국가안전보장회의, 국가정보원, 국방부와 사전 협의
- '심각' 경보는 정보통신부에서 발령
  ※ 정보통신부에서 국가안전보장회의, 국가정보원, 국방부와 사전 협의

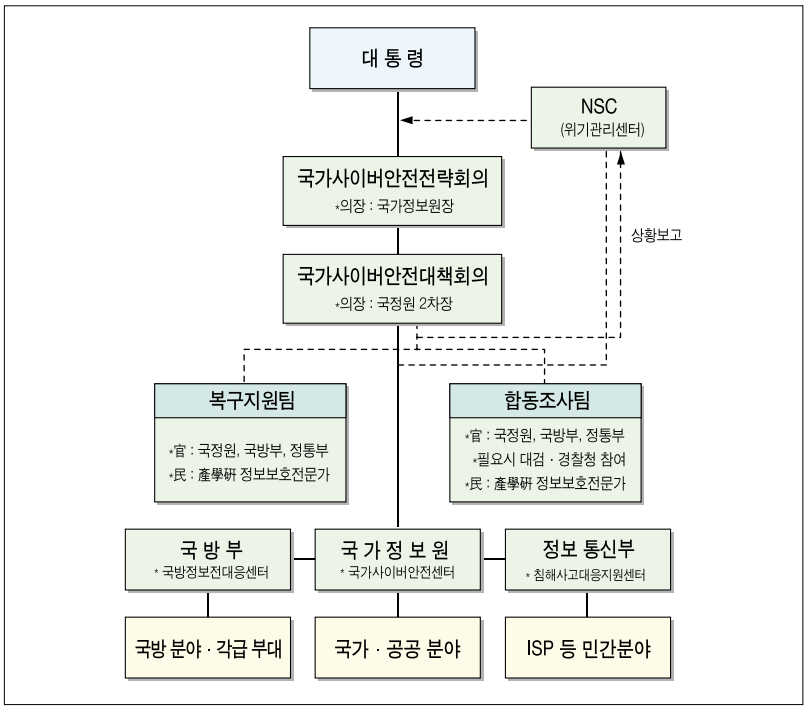
[표 2-1-2] 경보 발령 주체

단 계	단 계	발령 주체
경 보	심 각 (Red)	• 정보통신부
	경 계 (Oracnge)	• 정보통신부
	주 의 (Yellow)	• 한국정보보호진흥원
	관 심 (Blue)	• 한국정보보호진흥원
	정 상 (Green)	• 한국정보보호진흥원

※ '정상(Green)' 단계에서 웜 · 바이러스 및 보안취약점에 대한 보안권고 등은 한국정보보호진흥원 인터넷침해사고대응지원센터에서 알림

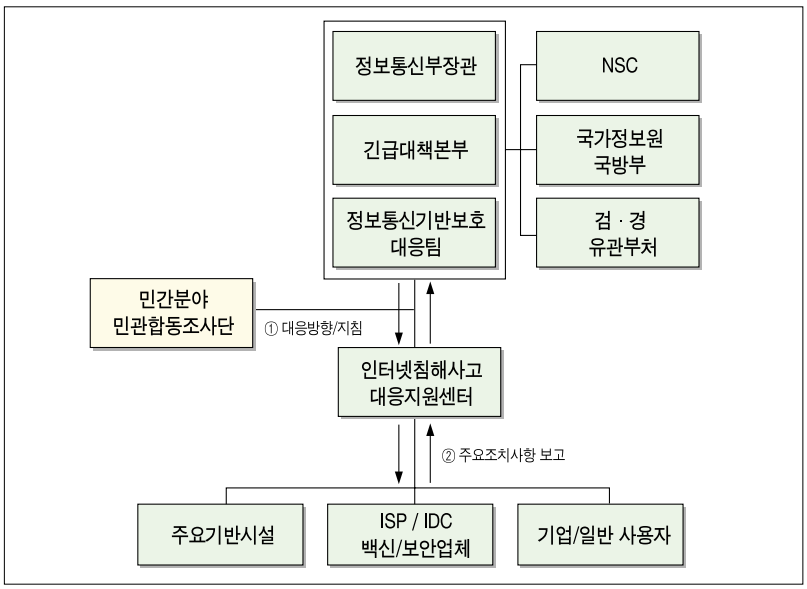
나. 발령 체계

경보 발령 체계도
(그림 2-1-1)



(2) 민간분야 위기관리 체계도

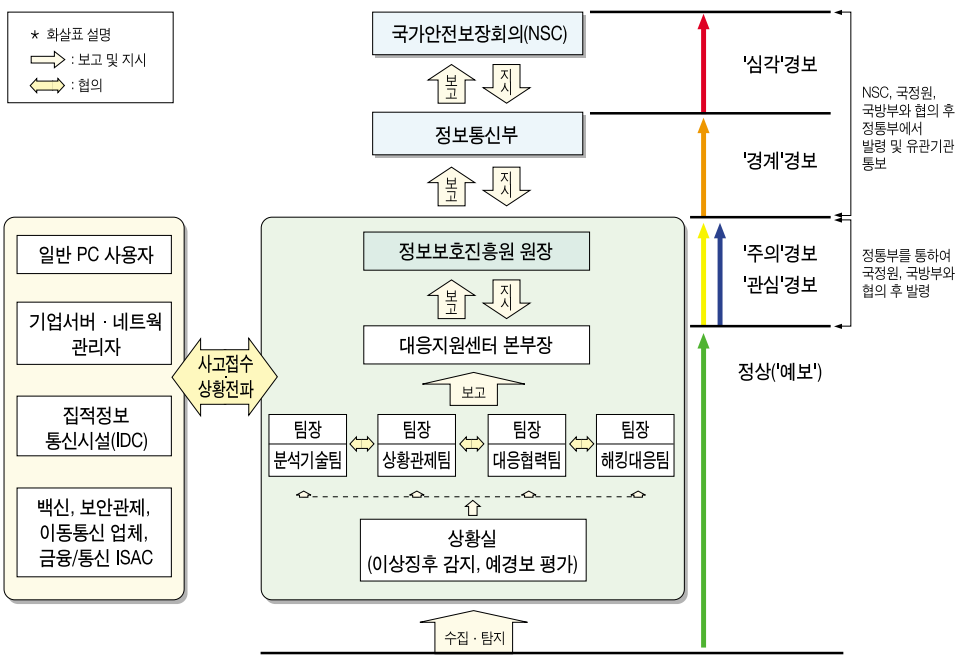
민간분야 위기관리 체계도
(그림 2-1-2)



(3) ISP 등 민간분야 비상대응 체계

비상대응 체계도
(그림 2-1-3)

(4) 민간분야 경보발령 체계

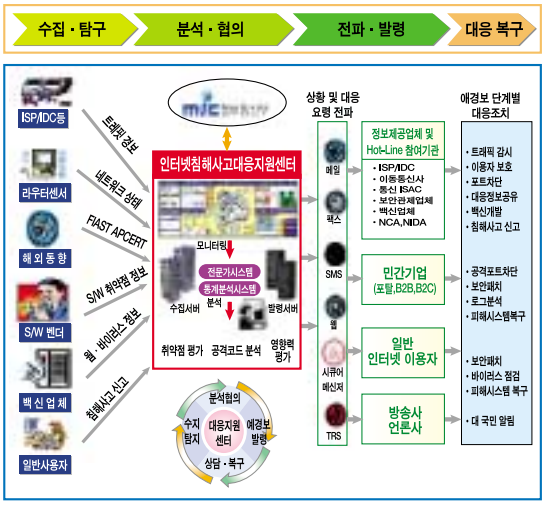


민간부문 경보 발령 체계도
(그림 2-1-4)

다. 경보 발령 과정

경보는 정보의 수집 · 탐지 ⇨ 분석 · 협의 ⇨ 전파 · 발령의 순서로 이루어진다.

경보 발령 과정
(그림 2-1-5)



(1) 수집 · 탐지 : 국내외 인터넷트래픽 및 취약점 정보, 백신업체 및 S/W 벤더 등으로부터 인터넷 트래픽 통계 및 웜 · 바이러스 정보 등 침해사고 관련 정보를 수집 · 탐지하는 과정

(2) 분석 · 협의 : 수집된 정보를 자동 및 수동 분석하고 협의하여 인터넷 경보 단계를 결정하는 과정

(3) 전파 · 발령 : 경보 상태를 다양한 전파수단을 이용하여 알림으로써 침해사고를 사전 예방하고 사고 발생 시 신속히 대응하는 과정

(4) 대응 · 복구 : 침해사고 피해 원인을 분석하고 피해 시스템을 복구하는 과정

라. 전파 수단

경보 단계별로 사용되는 전파수단 및 적용대상은 다음과 같다.

[표 2-1-3] 경보 단계별 전파수단

경보단계 \ 전파수단	웹, e-mail, 휴대폰 문자 메시지	TRS, FAX	보도기관, ISP등을 통한 경보 현황안내
'심각' 경보	○	○	○
'경계' 경보	○	○	○
'주의' 경보	○	○	○
'관심' 경보	○	○	△

※ '정상(Green)' 단계에서 웜 · 바이러스 및 보안취약점에 대한 보안권고 등은 웹(홈페이지)를 통하여 공지

○ : 모두 해당
△ : 경우에 따라 해당
× : 해당되지 않음

[표 2-1-4] 경보 전파수단 및 적용대상

전파수단 \ 적용대상	가입자 (개인/PC방 등)	기업(직원 및 정보보호담당자)	ISP 및 IDC
웹[1]	○	○	○
e-mail[2]	○	○	○
휴대폰 문자메시지[2]	○	○	○
시큐어 메신저[3]	○	○	○
보도기관, ISP 등을 통한 경보 현황 안내	○	○	○
주파수공용 통신(TRS)[4]	×	×	○
FAX[4]	×	×	○

1) http://www.krcert.or.kr, http://www.krcert.org, http://www.krcert.net 가운데 하나로 접속 가능
2) http://www.krcert.or.kr 에서 회원가입 필요
3) http://www.krcert.or.kr → "시큐어메신저" 메뉴에서 다운로드 하여 설치 필요
4) TRS 및 FAX를 이용한 상황전파문의 수신은 인터넷트래픽정보제공기관 및 Hot-Line 참여기관에 해당됨.
주파수공용통신(TRS-Trunked Radio System): 무선 통신의 한 방법으로 하나의 주파수를 여러 명의 이용자가 공동으로 사용하는 시스템

3. 인지방법

현재의 경보 단계는 다음과 같은 수단으로 파악할 수 있다.

[표 2-1-5] 경보 단계의 인지방법

구 분	인터넷 접속이 가능한 경우	인터넷 접속이 불가능한 경우
가입자 (개인/PC 방 등)	■ 인터넷 이용 ① 인터넷침해사고대응지원센터 (KrCERT) 홈페이지 접속 (http://www.krcert.or.kr)	■ 방송, 신문 등 언론 매체 이용 ■ KrCERT의 회원인 경우: 휴대폰 문자서비스 (SMS) 안내
기업 (직원 및 정보보호담당자)	② 초기화면의 경보 안내표시 확인 ➪ "정상" 의 경우  ➪ "관심" , "주의" , "경계" , "심각 " 의 경우 각각 다음 중 하나로 표시된다 관심 주의 경계 심각	■ 인터넷침해사고대응지원센터에 전화문의 (118)
ISP/IDC	■ e-mail 이용절차 ① KrCERT의 회원가입 (메일링 리스트 가입) ② KrCERT의경보 안내 메일 확인	■ 인터넷침해사고대응지원센터 종합상황실의 상황 전파내용 참고 ※ TRS, FAX, 전화 등을 통하여 통보됨

4. 경보 단계 변경 및 해제

경보 단계는 웜 · 바이러스, 해킹 등 침해사고의 진행상황에 따라 변경될 수 있다. 예를 들어, 최초 인터넷 웜이 해외에서 국내로 유입되어 '관심' 또는 '주의' 경보를 발령하였으나 국내 피해가 갈수록 확산되어 심각해지는 경우 '경계' 또는 '심각' 경보로 변경될 수 있다. 이와 반대로 국내 미치는 영향력 및 피해규모가 점차적으로 감소하여 더 이상 심각하지 않다고 판단이 될 경우 '심각', '경계' 경보에서 '주의', '관심' 경보로 변경될 수도 있다.

가. 경보 단계 변경 예시

(1) 상향 변경

경보 단계 상향 변경은 현재보다 상황이 악화되어 인터넷침해사고의 피해 또는 피해가능성이 더욱 커진 경우이며 다음과 같이 변경될 수 있다.

[표 2-1-6] 경보 단계 상향 변경 예시

변경 내용	설 명
관심 ⇨ 주의	'관심' 경보를 발령하였으나, 해킹, 웜/바이러스 등으로 '관심' 경보 발령 시보다 피해가 확산되어 더욱 많은 대응노력과 주의가 요구되는 경우
주의 ⇨ 경계	'주의' 경보를 발령하였으나 사태가 더욱 악화된 경우
경계 ⇨ 심각	'경계' 경보를 발령하였으나 범 국가적인 인터넷 위기상황이 발생하여 사태가 매우 심각한 경우
관심 ⇨ 경계	해킹, 웜/바이러스 등의 국내유입 및 피해발생으로 상황이 급속도로 악화되어 '주의' 경보 발령 없이 '경계' 경보 발령이 필요한 경우

(2) 하향 변경

경보 단계 하향 변경은 현재보다 상황이 호전되어 인터넷침해사고의 피해 또는 피해가능성이 줄어든 경우이며 다음과 같이 변경될 수 있다.

[표 2-1-7] 경보 단계 하향 변경 예시

변경 내용	설 명
주의 ⇨ 관심	'주의' 경보를 발령하였으나, 인터넷 웜/바이러스 및 해킹 등 침해사고의 영향력이 약화되어 '관심' 경보수준의 유지가 필요한 경우
경계 ⇨ 주의	'경계' 경보를 발령 후 상황이 호전되어 경보 하향조정이 필요하나 아직 '주의' 경보 수준의 대응이 요구되는 경우
심각 ⇨ 경계	범 국가적 인터넷 망에 대한 중대한 위협으로 '심각' 경보를 발령하였으나 상황이 호전되어 '경계' 경보 수준의 대응이 필요한 경우
경계 ⇨ 관심	'경계' 경보를 발령하였으나 신속한 대응조치로 침해사고로 인한 피해 또는 피해가능성이 현격히 감소하여 '관심' 경보 수준의 대응이 가능한 경우

나. 경보의 해제

- 경보의 해제란 경보 단계가 '관심', '주의', '경계', '심각'에서 '정상' 단계로 복귀하는 것을 말한다.
- 일반인의 경우 경보의 해제상태는 '경보의 인지방법'과 동일한 방법으로 파악할 수 있으며, 상황전파문을 통하여 경보 발령에 대한 트래픽 차단조치 등을 이행한 기관은 '경보 해제문'을 통하여 인지할 수 있다.

제2절 경보 단계별 대응 요령

기업의 정보보호 담당자(또는 서버/네트워크 관리자)가 경보 각 단계별로 점검 및 조치하여야 하는 침해사고 예방 및 대응요령은 [표 2-2-1]와 같다.

[표 2-2-1] 경보 단계별 대응 요령

		경보			
단계	정 상 (Green)	관 심 (Blue)	주 의 (Yellow)	경 계 (Orange)	심각 (Red)
대응요령	• 서버 네트워크, 보안장비 및 보안정책 등 점검 • 보안 패치(운영 체제, 응용 SW) • 바이러스 월 업데이트 • 침입차단시스템 및 침입 탐지 시스템 모니터링 • 서비스 포트 모니터링 • 웜 · 바이러스 취약점 동향 파악	• 기업내부 직원 및 서비스 관련 고객에게 "관심" 경보 전파 • 백신프로그램 및 바이러스 월 업데이트 • 해당 S/W 취약점 보안패치 • 기업 내부 서비스에 지장을 주지 않는 해당 포트 차단 권고 • 침해사고대응팀 비상연락망 비상 점검 ※ "정상" 단계대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "주의" 경보 전파 • 백신프로그램 · 바이러스 월 업데이트 및 점검 • 해당 S/W 보안 패치 • 기업 내부 서비스에 지장을 주지 않는 해당포트 차단 • 모든 서버 및 관리용 시스템 이상 유무 점검 ※ "관심" 단계대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "경계" 경보 전파 • 언론보도 주시 • 모든 서버 및 관리 시스템 지속적 점검 • 기업내 PC사용 최소화 권고 • 침해사고대응팀 비상연락망 비상 점검 ※ "주의" 단계 대응 요령 포함	• 기업내부 직원 및 서비스 관련 고객에게 "심각" 경보 전파 • 언론보도 주시 • 전체 네트워크 24시간 모니터링 및 해당 포트 차단 • 감염된 시스템 LAN에서 분리 • 침해사고대응팀 비상연락망 비상 점검 ※ "경계" 단계 대응 요령 포함

※ 각 기업은 본 매뉴얼을 참고하여 물리적 출입통제, 네트워크 보안정책, 서버의 접근통제 및 인증, 감사등 에 대하여 자체적인 보안정책을 수립후 내부지침을 마련하고 준수할 것을 권고한다.

1. "정상" 시 예방활동

가. 서버의 점검

서버관리자는 운영중인 서버가 해킹, 웜 · 바이러스 공격 등의 피해를 입지않도록 평소 다음과 같은 사항을 주기적으로 점검하고 이행하여야 한다.

- 불필요한 네트워크 서비스를 제거한다.
- 서버소프트웨어에 대한 보안 패치 정보를 확인[5]하고 적용한다.
- 유닉스/리눅스의 경우 root 계정은 콘솔에서만 로그인할 수 있도록 설정한다.
- 서버 운영에 불필요한 계정이 있는지 확인하고 있을 경우 삭제한다.
- 관리자가 알지 못하는 사용자 계정이 생성되어 있을 경우 어떠한 경로로 생성되었는지 원인 파악 후 불필요할 경우 삭제 조치한다.
- 운영중인 서버 플랫폼과 관련 있는 보안 취약점 정보, 해당 취약점을 이용한 공격코드의 공개여부 등을 파악하고 필요시 보안 패치 등을 실시한다.
- 신규 웜 · 바이러스 정보를 파악하고 운영중인 서버와 관련 있는지 확인하고 보안 패치 등 필요한 조치를 취한다.

※ 신규 보안취약점 및 웜 · 바이러스 정보확인 방법
인터넷침해사고대응지원센터 홈페이지(http://www.krcert.org) "웜 · 바이러스 정보" 및 "보안 권고문" 메뉴 이용

- 서버설정파일 변경, 네트워크 주소변경 등 서버 운영환경에 변화가 필요할 경우에는
  - 불필요한 서비스의 추가 여부
  - 사용자 계정에 대한 필요이상의 권한 부여 여부
  - 시스템에 대한 불법접근 가능성 여부 등에 대하여 검토하고 위와 같은 사항이 발행하지 않도록 하여야 한다.
- 주기적으로 중요한 시스템 및 데이터베이스를 백업하고 백업파일은 CD, 테이프 등 미디어 매체에 저장해 둔다.

5) 패치정보의 확인: 운영중인 서버의 제작사 홈페이지 또는 관련 웹사이트를 주기적으로 방문하거나 보안뉴스레터 등의 서비스에 가입하여 제공받을 수 있다.

※ 백업 주기 및 방법과 백업파일의 보존기한 등에 대하여는 기업 자체적으로 지침을 마련하고 준수할 것을 권고한다.

- 시스템은 보안점검을 위하여 필요한 로깅을 실시하고 로그파일은 가능하면 매일 점검하여 외부의 불법적인 접근 및 시스템의 장애여부를 파악하도록 한다.

나. 네트워크의 점검

네트워크 관리자는 인터넷침해사고의 예방을 위하여 다음과 같은 사항을 점검하고 이행하여야 한다.

- 라우터와 스위치 등 네트워크 장비에 가능한 로그기능을 설정하고 로그를 모니터링 한다.
- 라우터 ACL 등 네트워크 접근통제정책이 제대로 적용되어 있는지 확인한다.
- 라우터, 스위치 등 네트워크장비에 대한 보안 패치를 실시한다.
- 라우터, 스위치 등 네트워크장비에서 기본적으로 제공되는 서비스 가운데 사용하지 않는 서비스는 중지한다. (예를 들어 웹을 이용한 원격관리 서비스 등)
- 필요한 경우 네트워크 장비에 대한 이중화 및 백업체계를 마련한다.
- 라우터 및 네트워크 장비의 관리계정에 대한 비밀번호 관리를 철저히 하거나 RADIUS, TACAS 등 인증서버를 적용한다.
- 네트워크 취약점 스캐너 등 보안도구를 이용하여 내재된 취약점을 점검한다.

다. 보안장비의 점검

정보보호담당자는 기업의 보안 강화를 위해 설치한 보안 장비가 정확하게 설정되어 있는지 주기적으로 확인하여 침해사고를 예방하여야 한다.

- 내부/외부에서 보안 도구를 사용하여 침입차단시스템 설정을 확인한다.
- 침입탐지시스템의 탐지 규칙을 최신 규칙으로 업데이트 하여 최신 공격에 대하여 대비하여야 한다.

- 바이러스 월의 필터링 규칙을 항상 최신의 상태로 업데이트 하여 바이러스가 통과되지 못하도록 한다.
- 침입차단/탐지시스템의 로그를 주기적으로 모니터링 한다.
- 침입차단시스템 정책의 경우 가능하면 다음 내용을 기본 규칙으로 설정하도록 한다.
  - 침입차단시스템 관리 시스템에서 들어오는 트래픽은 "허용" 하고 관리시스템이 아닌 시스템에서 들어오는 다른 모든 트래픽은 "거부" 한다.
  - 내부 DNS 서버로 들어오는 모든 외부 트래픽은 "거부" 로 설정한다.
  - 외부 DNS로 가는 트래픽은 DNS (port 53 TCP/UDP) 만 "허용" 한다.
  - 각 서비스 포트는 반드시 필요한 포트만 "허용" 한다.

라. 보안정책

기업의 네트워크 혹은 서버의 보안 정책에 대해 다음과 같은 상황을 점검하여야 한다.

- 윈도우 시스템의 경우 관리자 계정을 제외한 사용자 계정 및 Guest 계정은 원격접속서비스(터미널서비스)를 통하여 로그인하는 것을 허용하지 않도록 한다.
- 중요한 로그 혹은 이벤트 메시지가 발생하면 즉시 관리자에게 통보되도록 설정한다.
- Web 서버, FTP 서버 등 모든 컨텐츠 서버에 대하여 엄격한 접근통제리스트(ACL-Access Control List)를 유지한다.
- 모든 사용자에 대하여 보안성이 있는 암호를 사용하도록 권고한다.
- 관리 계정에는 다른 계정들보다 특별히 보안성이 있는 암호를 사용하도록 한다.
- 반복적으로 로그인에 실패하는 계정은 사용하지 못하도록 한다.

마. 기타

이 외에도 Windows 서버의 경우 다음과 같은 사항을 항상 점검하여야 한다.

- 모든 서버에 대하여 바이러스 검사를 주기적으로 실시한다.

- 보안 패치 배포여부를 모니터링하고 배포되었을 때에는 즉시 적용할 수 있도록 한다.
- 바이러스/웜 사고에 관련되거나 관련이 없더라도 예측되는 영향에 따라 위험하다고 판단된 메일의 첨부문서를 삭제하도록 한다.
- 운영중인 서버가 스팸메일릴레이에 악용되고 있는지 점검 및 조치한다.

2. "관심" 경보 발령 시 대응 요령

- 기업내부 직원 및 고객들에게 "관심" 경보 발령내용 및 보안패치 방안, 내부적인 대응방안을 전파한다.
- 백신 프로그램과 바이러스 월의 업데이트 상황을 항상 파악하고 최신 버전으로 업데이트 한다.
- "관심" 경보 발령과 관련된 보안취약점에 대한 패치를 실시한다.
- 관련 네트워크 서비스 포트에 대하여 모니터링을 강화하고 기업내부 서비스에 큰 영향을 주지 않는 범위 내에서 해당 포트를 차단하거나 차단을 준비한다.
- 인터넷서비스제공관련기관(ISP/IDC) 및 서버/네트워크의 벤더 또는 유지보수 업체와 상시 연락이 가능한지 비상연락망을 점검한다.

3. "주의" 경보 발령 시 대응 요령

- 기업내부 직원 및 고객들에게 "주의" 경보 발령 내용 및 관련 포트 차단 등 내부적인 대응 방안을 전파하고 인터넷 사용을 자제하도록 한다.
- 백신프로그램과 바이러스 월을 최신 버전으로 업데이트 되었는지 확인한다.
- 경보와 관련된 보안취약점에 대한 패치가 제대로 이루어 졌으며 해당 침해사고(해킹, 웜·바이러스 등)에 대응력이 있는지 검증한다.
- 경보와 관련된 네트워크 서비스 포트에 대하여 모니터링을 강화하고 필요시 해당 포트를 차단한다.
- 기업 내부 혹은 고객의 피해가 증가하거나 증가할 가능성이 높을 경우 비상대응팀의 구성 및 운영계획을 수립하는 방안을 검토·실시한다.

※ 침해사고대응전담조직(CERT 팀)의 운용단계 상향조정 및 인력증원 등 검토

- 필요시 비상연락망을 이용하여 인터넷서비스제공관련기관(ISP/IDC) 및 서버/네트워크의 벤더 또는 유지보수 업체와 대응방안을 협의 · 실시한다.
- 기업 내 모든 서버 및 관리시스템 가운데 특히 해당 취약점 또는 침해사고에 영향력이 있는지를 점검하고 대응책을 수립한다.

4. "경계" 경보 발령 시 대응 요령

- 기업내부 직원 및 고객들에게 "경계" 경보 발령내용, 관련 포트 차단 등 내부적인 대응방안을 전파한다.
- 언론보도를 주시하고 권고하는 대응조치가 있을 경우 이를 이행한다.
- 기업 내 모든 서버 및 관리시스템 가운데 특히 해당 취약점 또는 침해사고에 영향력이 있는지 지속 점검하고 대응조치를 이행한다.
- 기업내부 직원 및 고객들에게 PC 사용을 최소화하도록 권고한다.
- 침해사고대응팀 비상연락망으로 비상소집한다.
- 경보와 관련된 보안취약점에 대한 패치가 제대로 이루어졌는지 여부와 해당 침해사고(해킹, 웜 · 바이러스 등)에 대응력이 있는지 검증한다.

5. "심각" 경보 발령 시 대응 요령

- 기업내부 직원 및 고객들에게 "심각" 경보 발령내용, 관련 포트 차단 등 내부적인 대응방안을 전파한다.
- 언론보도를 주시하고 권고하는 대응조치가 있을 경우 이를 이행한다.
- 해당 경보와 관련된 네트워크 서비스 포트에 대하여 24시간 모니터링을 강화하고 관련 포트를 차단한다.
- 웜 · 바이러스에 감염된 시스템은 네트워크에서 분리하여 사고에 영향을 최소화하도록 한다.
- 침해사고대응팀을 비상가동하고 필요시 복구활동을 신속히 지원한다.
- 가능하면 인터넷 사용을 중지하고 컴퓨터 전원을 차단한다.

제3절 사고 발생 시 대응요령

1. 침해사고 원인 분석

침해사고는 “정상” 또는 “관심” 단계에서 국지적으로 발생하여 개인, 기업 서버의 해킹 및 시스템 장애 등을 유발할 수 있으며, “주의”, “경계”, “심각” 단계에서 발생하여 국지적, 전국적 인터넷 장애를 유발할 수 있다. 침해사고에 대한 원인분석은 크게 다음과 같은 두 가지 경우로 이루어질 수 있다.

- 민관의 합동조사가 필요하지 않은 경우
  - 가입자(개인,PC방 등), 기업 서버/네트워크 관리자가 자체적으로 침해사고의 원인분석을 수행한다.

- 민관의 합동조사가 필요한 경우
  - 법률이 정하는 바에 따라 민관 합동조사단이 침해사고의 원인분석 수행한다.

[정보통신망이용촉진및정보보호등에관한법률제48조의4]

> **제48조의4(침해사고 원인분석 등)** ②정보통신부장관은 정보통신서비스제공자의 정보통신망에 중대한 침해사고가 발생한 때에는 피해확산방지 · 사고대응 · 복구 및 재발방지를 위하여 정보보호에 전문성을 갖춘 민 · 관합동조사단을 구성하여 당해 침해사고의 원인분석을 할 수 있다.

2. 피해 복구 요령

침해사고 발생시 간단한 경우 자체적으로 복구를 수행하고, 자체적인 복구가 어려울 경우 유관기관[6]의 협조를 받아 복구작업을 수행할 수 있다. 피해복구의 절차는 다음과 같다.

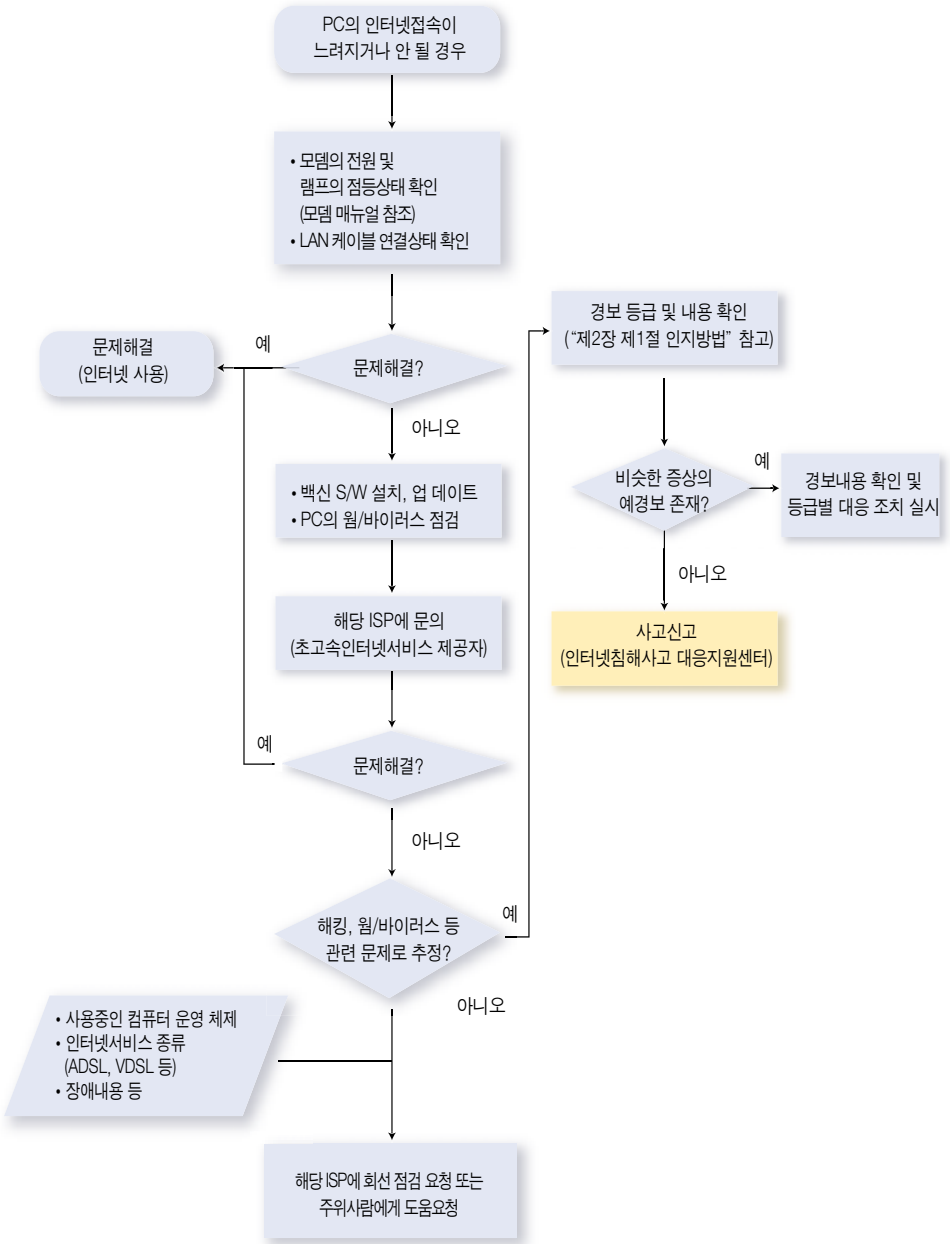
[표 2-3-1] 피해복구 절차

순서	절차	세부 내용	
1	피해복구 범위결정	단순 데이터 복구	● 시스템의 데이터에만 손상이 발생
		소프트웨어 복구	● 시스템 내 프로그램 및 운영체제에 단순 오류 발생
		시스템 재설치	● 시스템 운영체제가 복구 불가능
		하드웨어 교체	● 시스템 하드웨어의 손실 발생
2	복구 우선 순위 결정	● 피해복구 대상시스템이 2개 이상인 경우, 이들 대상에 대한 복구 우선 순위를 정함 ● 즉시 조치해야 할 복구 내용과 중장기적인 계획에 의해서 수행해야 할 복구 내용을 정함	
3	피해복구	단순 데이터 복구	● 백업 데이터로 복구
		S/W 복구	● 백신프로그램을 이용하여 치료 ● 공격에 이용된 취약점 제거 ● 응용프로그램 재 설치 ● 운영체제 CD를 이용한 운영체제 복구
		시스템 재설치	● 운영체제 및 응용프로그램 재 설치 ● 백업 자료를 이용한 데이터 복원 ● 시스템을 완료 후 정상상태 복귀 확인
		하드웨어 교체	● 파손된 하드웨어 부품 교체
4	사후관리	● 시스템 재개 후 일정기간 동안 모니터링 재개 ● 보완 보고서 작성 ● 일정기간동안 시스템 및 네트워크 주기적 재점검	

6) 정보통신부, 한국정보보호진흥원 인터넷침해사고대응지원센터 등 인터넷침해사고 대응관련기관

3. 인터넷 접속장애 대응 및 침해사고 신고 절차

인터넷 장애대응
(그림 2-3-1)



4. 침해사고 기술지원 요청 및 신고

가. 침해사고에 대한 기술지원 요청

인터넷 사용 중 발생한 해킹이나 웜 · 바이러스 등 침해사고 해결을 위하여 기술적 지원이 필요한 경우에는 한국정보보호진흥원의 인터넷침해사고대응지원센터에서 운영하는 사이버 118에서 사고 해결을 위한 지원을 받을 수 있다.

- KrCERT 홈페이지 : http://www.krcert.or.kr ⇨ 우측 상단 "침해사고 신고 및 상담" 메뉴 이용

침해사고 신고 홈페이지
(그림 2-3-2)

※ 침해사고 신고내용의 정확한 파악에 따른 신속한 기술지원을 위하여 신고내용을 기록하여 유지할 수 있도록 홈페이지나 e-mail 이용 권장

- 전화 : (국번없이) 118
- e-mail : cert@certcc.or.kr

※ e-mail 신고시 홈페이지 침해사고신고 신청양식에 있는 아래 내용이 포함되도록함

침해사고 신고 양식
(그림 2-3-3)

나. 침해사고에 대한 수사 의뢰

인터넷 사고 중 해킹, 인터넷을 이용한 사기, 주민등록번호의 도용 등 침해 행위에 대하여 침해 행위자에 대한 수사 등 법적인 처리를 고려하는 경우에는 경찰청 사이버테러대응센터에 신고하여 지원을 받을 수 있다.

- 전화 : 02-3939-112
- 인터넷 : http://www.cybercrime.go.kr/

c o n t e n t s

제3장
보안사고 유형 및 사례

제1절 해킹 · 바이러스 사고 유형 및 사례

1. 사고 유형

해킹 및 바이러스와 관련된 보안사고는 공격 유형에 따라 크게 아래처럼 분류된다.

- 악성프로그램 사고(바이러스, 인터넷 웜 등)
- 시스템 침입사고
- 서비스거부 공격(DoS, Denial of Service)으로 인한 사고
- 서비스 및 시스템의 오 · 남용 사고
- 정보수집 공격 사고

하지만 실제 해킹사고에서는 이러한 공격 유형이 복합적으로 사용된 공격형태와 피해를 보인다. 해킹 · 바이러스 사고는 다음 [표 3-1-1]에서와 같이 매년 양적인 측면에서 증가세를 보이고 있다.

[표 3-1-1] 연도별 해킹사고 피해 통계

연도	1996년	1997년	1998년	1999년	2000년	2001년	2002년	2003년
해킹사고	147	64	158	572	1,943	5,333	15,192	26,179
증가율(%)	-	-56%	147%	262%	240%	174%	185%	72%

공격기법	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
사용자도용	147	12	9	7	4	1	3	3	1	1	1	0	4	46
S/W보안오류	845	575	62	921	495	134	61	42	385	26	20	30	19	3,940
구성설정오류	4,638	733	808	2,059	1,960	2,031	585	399	203	101	218	140	392	9,899
악성프로그램	4,112	1,148	557	1,232	934	306	450	185	544	119	137	129	96	5,837
서비스거부	18	29	0	0	0	0	0	1	0	0	0	0	0	30
E-mail관련	1,943	258	346	1,018	1,617	1,905	289	353	137	63	171	370	363	6,900
취약점정보수집	3,971	703	535	1,219	930	303	440	171	175	113	129	124	95	4,937
총계	15,674	3,458	2,317	6,456	5,940	4,680	1,828	1,154	1,455	423	686	1,063	969	30,429

자료출처:
2003.12, KISA(KrCERT)
공격기법은 같은 사고에 다수의 공격기법이 사용되어 중복이 될 수 있음

[표 3-1-2] 연도별 악성 프로그램 피해 통계

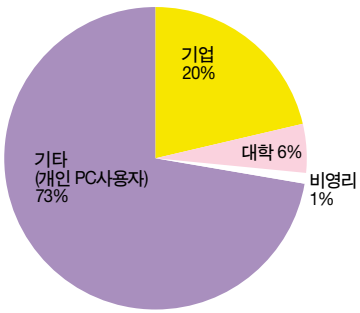
구분	2001년	2002년	2003년
신종출현건수	194	232	108
피해신고접수건수	65,033	38,677	85,023

구 분	2002년	2003년												2003년 총계
		1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	
바이러스	9,308	1,096	975	783	467	536	924	925	832	522	455	882	797	9,194
인터넷 웜	27,021	1,361	1,320	2,537	2,350	3,704	1,854	1,185	9,748	19,682	3,999	11,658	8,99	68,347
트로이목마	1,687	1,284	876	419	303	304	491	411	334	387	475	448	355	6,087
가짜(Hoax)	13	0	16	10	5	9	5	6	4	2	1	0	1	59
조크(Joke)	111	5	1	6	3	0	0	3	1	2	1	0	1	23
기타	537	11	50	42	52	59	248	20	120	86	522	49	54	1,313
합계	38,67	3,757	3,238	3,797	3,180	4,612	3,522	2,500	11,039	20,681	5,453	13,037	10,157	85,012

자료출처:
2003.12, KISA(KrCERT)

공격의 주요 피해 대상을 분류해 보면 개인 또는 기업의 PC 사용자에 대한 피해가 증가하고 있는데, 이는 최근에 Windows에 대한 공격이 증가하기 때문이다. 따라서 기업의 보안관리자 입장에서는 주요 서버에 대한 보안과 더불어 개인 사용자 PC 보안을 포함하는 전사적인 기업 보안대책을 필요로 한다.

[표 3-1-3] 피해 대상 분류



PC 사용자가 입은 피해가 가장 많았으며, 기업이 그 다음으로 많은 피해를 입었다.

PC 사용자의 피해증가는 윈도우즈 시스템의 피해증가와 밀접한 관련이 있는 것으로 추정된다.

※ 왼쪽 그래프는 2003년의 Top 4 현황임

기관	도메인	2002	2003												2003년 총계
			1	2	3	4	5	6	7	8	9	10	11	12	
기업	co	1,812	298	190	900	303	254	101	104	123	20	56	36	31	2,416
대학	ac	716	142	71	108	155	79	44	27	55	4	6	10	4	705
비영리	or	154	31	11	24	22	17	6	5	2	0	4	0	4	126
연구소	re	22	3	2	2	3	3	0	0	1	0	0	0	0	14
네트워크	ne	4	6	2	2	0	10	12	0	0	0	0	0	0	32
기타(개인)		3,736	979	635	1,235	2,042	1,587	572	410	424	100	254	395	425	9,058
총계		6,444	1,459	911	2,271	2,525	1,950	735	546	605	124	320	441	464	12,351

자료출처:
2003.12, KISA(KrCERT)

가. 악성 프로그램

악성 프로그램이란 제작자가 의도적으로 다른 정보통신 이용자에게 피해를 주고자 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미한다. 악성코드라 표현하기도 하며, 이메일/메신저/문서의 매크로 기능 등을 이용하여 유포되거나 공격에 사용한다. 주요 형태로는 컴퓨터 바이러스(Computer Virus), 인터넷 웜(Internet Worm), 트로이 목마(Troijan Horse) 등으로 나눌 수 있다. 다음은 각각의 공격형태에 대한 설명이다.

※ 악성 프로그램을 다음과 같이 여러 형태로 분류하고 있으나, 실제 사고에서는 다수의 특징을 복합적으로 사용한 경우가 많다.

(1) 컴퓨터 바이러스

컴퓨터 바이러스란 자신을 복제하기 위해 다른 숙주 파일이나 부트 영역을 변경하는 프로그램을 말한다. 대부분의 경우 숙주 개체는 악성 프로그램의 완전한 복사본을 포함하도록 변경된다. 뒤이어 감염된 숙주 파일이나 부트 영역이 실행되면 다른 개체를 감염시킨다. 이를 컴퓨터 바이러스라고 부르는 이유는 프로그래밍 로직이 생물학적 바이러스를 흉내 내고 있기 때문이다. 컴퓨터 바이러스는 돌연 변이되고 진화하면서 백신 프로그램에 대항하며, 감염범위가 커지면 시스템의 작동을 마비시킨다.

(2) 인터넷 웜(Internet Worm)

인터넷 웜은 자체 프로그램 코딩을 이용하여 전파되는 자기 복제가 가능한 복잡한 악성코드이다. 인터넷 웜은 널리 사용되는 이메일이나 채팅 채널 같은 응용 프로그램을 이용하여 전파된다. 첨부 파일의 형태로 또는 신뢰할 수 있는 시스템 사이의 파일 송수신을 이용해 전파되는 것이다. 바이러스와는 달리 웜은 정규파일이나 부트 영역에는 거의 자리 잡지 않으며, 소프트웨어나 시스템의 보안 허점을 이용한다.

(3) 트로이 목마

트로이 목마는 자신의 실체는 보여주지 않으면서 마치 다른 프로그램의 한 유형인 것처럼 가장하여 활동하는 프로그램이다. 트로이 목마는 자기 복제를 하지 않으며, 다른 파일을 감염시키거나 변경하지는 않는다. 하지만 트로이 목마가 포함된 프로그램을 실행하는 순간 시스템은 악의적 해커에게 제어 당할 수 있는 권한을 부여하게 된다.

웜과 트로이 목마의 구분

웜과 트로이 목마는 구별하기가 쉽지 않다. 트로이 목마가 자신을 다른 프로그램인 것처럼 가장하는 반면, 웜은 화면 뒤에서 보이지 않게 움직인다는 점이 다르다. 트로이 목마는 사용자가 자신을 의심하지 않고 실행하는데 중점을 두지만, 웜은 사용자의 도움 없이 시스템에서 시스템으로 전파된다. 웜은 자신의 복사본을 수없이 만들지만, 트로이 목마는 그렇지 않다.

나. 서비스 거부(DoS, Denial of Service)[7]

시스템 또는 네트워크 서비스의 정상적인 운영을 방해하는 공격으로, 시스템을 다운시키거나, 네트워크에 과부하의 트래픽을 유발시켜 사용자들이 서비스를 이용하지 못하게 하는 공격이다. 시스템 상에서 수행할 수 있는 공격과, 원격지에서 원격으로 수행할 수 있는 다양한 공격 방법이 있다. 또한 공격의 효율을 높이기 위해 다수의 시스템에서 하나의 시스템이나 네트워크를 공격하는 분산서비스거부공격(DDoS, Distributed Denial of Service Attack)[8]을 수행하기도 한다.

7) 이하모두 DoS라 칭함
8) 이하모두 DDoS라 칭함

다. 시스템 침입(비 인가된 접근)

시스템 또는 네트워크의 취약성을 이용하여 시스템에 침입하는 공격이다. 보통 특정 취약성을 공격하는 해킹프로그램을 이용하거나, 서버의 잘못된 설정 또는 운영으로 인한 문제를 이용하여 시스템에 침입한다.

(1) 시스템/어플리케이션의 취약성

보안 문제를 고려하지 않고 시스템 또는 어플리케이션을 개발함으로서 발생되는 취약성으로 주로 사용자로부터 받아들이는 입력값의 범위를 제대로 검사하지 않거나, 잘못된 접근통제 메커니즘의 구현 등으로 발생한다. 대표적인 취약성은 다음과 같다.

- 버퍼 오버플로우(Buffer overflow)
  시스템이 받아들인 입력의 길이가 예상된 것보다 더 길어서 발생하는 취약점으로 공격자는 조작된 입력 값을 보냄으로서 시스템을 정지시키거나 또는 임의의 명령을 실행시킬 수 있다.
- 접근 검증 오류(Access validation error)
  시스템의 접근통제 메커니즘 자체를 잘못 설계하여 발생하는 취약점이다.
- 예외 조건 처리 오류(Exceptional condition handling error)
  시스템이 예외 조건(Exceptional Condition)을 잘못 처리하여 발생하는 취약점이다.
- 환경변수 오류(Environmental error)
  시스템이 설치된 환경으로 인하여 발생하는 취약점으로, 종종 개발환경에서는 제대로 작동하는 시스템이 실제 운영 환경에서 보안 문제를 일으키는 경우를 예로 들 수 있다.

(2) 시스템/어플리케이션의 설정 오류

사용자가 시스템의 구성환경을 잘못 설정하여 사용함으로써 발생하는 취약성이다. 시스템 관리자가 모든 서비스에 대해서 충분한 시간을 갖고 올바른 설정 및 운영을 하기란 결코 쉽지 않은데, 이는 보안사고의 주요 원인이 된다.

라. 오남용(비 인가된 사용)

시스템 및 네트워크 자원을 허가받지 않은 방법으로 사용하거나 악용하는 공격이다. 스팸 메일을 보낼 때 다른 사이트의 시스템을 이용하는 방법, 음란물 또는 불법 소프트웨어를 유통시키기 위해 타 기업의 시스템을 FTP 서버로 사용하는 경우, 그리고 타인의 계정을 도용하여 사용하는 행위 등이 대표적인 예이다.

마. 정보수집

특정 사이트의 시스템 및 네트워크에 대한 정보를 수집하기 위한 공격으로 포트 스캔, 전화번호 스캔 등이 있다. 공격자는 정보 수집을 통해 특정 사이트에 어떠한 시스템이 존재하는지, 어떠한 서비스가 제공되는지, 어떠한 네트워크 구조를 갖고 있는지, 그리고 어떠한 취약성이 있는지를 조사하게 된다. 정보 수집은 비 인가된 접근으로 분류할 수도 있으나, 인터넷 공격의 많은 부분을 차지하기 때문에 따로 분류하여 처리하는 것이 바람직하다.

2. 사고 사례

가. MyDoom 웜

2004년 2월 전 세계적으로 100만대 이상의 컴퓨터를 감염시킨 것으로 추정되는 웜 바이러스 '마이둠' 이 미국 소프트웨어 제조업체인 SCO그룹이 운영하는 웹사이트를 공격해 마비시켰다. SCO측은 '마이둠.A' 바이러스가 25만대의 컴퓨터를 조종해 자사 웹사이트를 공격했으며 이로 인해 웹사이트가 완전히 마비됐다고 밝혔다. 또한 회사측은 마이둠 바이러스가 1일부터 12일까지 SCO 서버에 대한 '서비스 거부 공격(DoS)' 을 수행하도록 프로그래밍 되어 있어 배포자에 대한 정보 제공자에게 25만 달러의 현상금을 주겠다고 공표한 바가 있다.

SCO는 지난해부터 IBM을 포함해 리눅스를 사용하는 회사에 대해 지적재산권 침해로 고발하겠다고 밝혔으며 개인사용자에 대해서도 경고성 편지를 보낸 이후 해커들의 표적이 돼왔다.

나. SARS 웜

(1) Windows 바이러스

2003년 4월에는 중국에서 처음으로 발생되어 전 세계로 전파된 생물학적 바이러스인 SARS(중증급성호흡기증후군)와 관련된 내용이 포함된 사스 바이러스(일명 Coronex)가 발견되어 눈길을 끌었다. 이 웜은 SARS와 관련된 정보를 제공하는 것처럼 위장, 메일을 통해 전파되었으며, 메일의 제목이나 본문에 '사스 바이러스' (SARS Virus) 나 '데쓰 바이러스' (death virus)라는 문구가 포함돼있었다. 감염이 일어나면 웜이 인터넷 익스플로러의 기본 시작 페이지를 사스 관련 사이트(www.who.int/csr/don/2003_04_19/en)로 변경시켰다. 그러나 시스템에 치명적인 피해는 일으키지 않아 그 피해가 크지는 않았다.

(2) Linux SARS 웜

2003년 4월 30일 국내 중소기업 S사의 시스템 관리자로부터 자사의 시스템에 과부하가 발생하는 원인을 확인해 달라는 요청 메일이 KrCERT로 접수되었다. 피해시스템은 웹/이메일/FTP 서비스를 운영하고 있는 RedHat Linux 7.3 버전의 운영체제 시스템이었다. 공격 프로그램은 피해시스템에 공격자가 만들어 놓은 다음과 같은 index.html 파일이 설치되어 홈페이지가 변조 되도록 하는 인터넷 웜이었다.

변조된 홈페이지 초기화면
(그림 3-1-1)

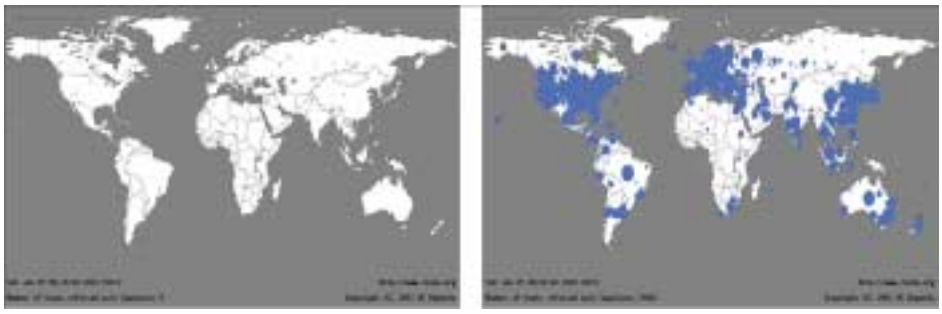
KrCERT 홈페이지:
http://www.krcert.or.kr

다. 슬래머 웜(SQL Slammer Worm)

2003년 1월 25일에 국내로 유입된 슬래머 웜으로 인하여 MS-SQL 2000 서버와 관련된 UDP 1434 포트에 대한 트래픽이 증가하였고 국내 주요 ISP의 통신망에 장애가 발생하는 인터넷 대란이 발생하였다. 슬래머웜은 컴퓨터의 소프트웨어를 파괴하지 않으면서도 인터넷을 무력화하였으며 패킷의 크기는 376바이트(패킷 헤더를 포함하면 전체 404바이트)에 불과했다. 최초 발생시점부터 8.5초마다 감염시스템의 수가 두 배로 증가했으며, 10분 이내에 인터넷상의 취약한 시스템의 90% 이상을 감염시켰다.

이 웜은 마이크로소프트 SQL 서버, MSDE 2000의 취약성을 공격한 것인데, 이는 이미 2002년 7월에 그 취약성이 발표되었고 패치도 제공되고 있었다. 이 공격으로 인하여 항공 일정 변경, ATM 오류, 그리고 국내의 경우 인터넷 마비와 같은 큰 피해가 발생하였다.

(그림 3-1-2)은 슬래머 웜의 전파 모습을 보여준다.



슬래머 웜 전파
(2003.1.25, 05:29:00 ~ 06:00:00 (UTC))
(그림 3-1-2)

자료출처:
http://www.caida.org

라. 주요 전자 상거래 사이트에 대한 DDoS 사고

2000년 2월 미국의 주요 전자상거래 사이트인 Yahoo, E-bay, Amazone, CNN 등의 사이트가 DDoS를 받아, 수 시간동안 서비스를 제공하지 못하는 사고가 발생하였다. 이 공격으로 인하여 20억 달러 이상의 피해를 본 것으로 추정된다. 본 공격은 인터넷상의 수 천, 수만의 해킹당한 시스템을 이용하여 몇몇 주요 전자 상거래 사이트를 공격한 최초의 DDoS 사례이다.

(1) 야후 사이트 DDoS 공격 및 대응

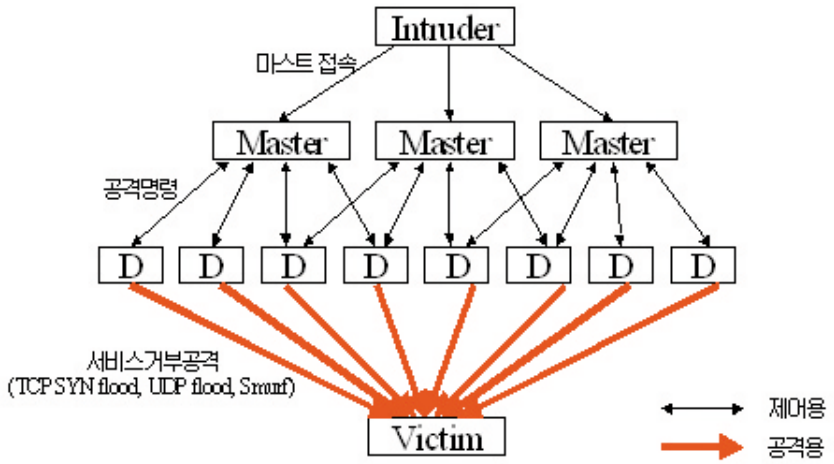
2000년 2월 야후 사이트는 4번의 공격을 받았으며, 처음 받은 공격에 대한 자료는 없었으나, 모든 공격에서 분산 "smurf" 공격요소를 포함하고 있었던 것으로 추측된다. 다른 공격받은 사이트들도 공격형태가 비슷하였으며, 간혹 몇 몇 소스주소로부터의 SYN 공격을 받은 사이트도 있다고 보고되었다.

가장 큰 영향을 준 공격은 월요일 아침 10:30am PST경에 받은 공격이다. 처음의 flooding 공격으로 초당 1G bit 이상의 패킷을 받았으며, 라우터 중 하나가 다운되었다. 라우터가 복귀된 후에도 상당시간동안 상위 ISP로의 모든 라우팅이 되지 않았던 것으로 밝혀졌다. 그리고, 서버로 향하는 모든 트래픽을 막고 나서야 정상적인 라우팅이 되었다. 얼마 후 결국 네트워크가 안정화되었는데, 분석 결과 DOS 공격으로 판명되었다.

(2) 분산서비스거부공격(DDoS) 이란 ?

비교적 단순한 전통적인 DoS 공격에 비해 DDoS 공격은 지능화, 자동화, 대규모화, 분산화된 공격기법이다. DDoS 공격 개요도는 다음과 같다.

분산서비스거부 공격 개요도
(그림 3-1-3)



DDoS 공격 시스템은 마스터(master)와 데몬(daemon)이 시스템들로 구성되어 있다. 마스터란 공격자로부터 접속을 허용하여 명령어를 입력받아 데몬에 그 명령을 전달하는 시스템이고, 데몬이란 마스터 시스템으로부터 공격 명령을 받아 공격대상 호스트에 다량의 데이터 패킷을 전송하는데 이용당하는 시스템이다. 공격자는 몇 개의 마스터 프로그램이 설치된 호스트를 제어하며, 이 마스터 프로그램은 또한 데몬 프로그램이 설치되어 있는 다수의 호스트를 제어한다. 이 데몬 프로그램들이 실제 목표 시스템에 DoS 공격 패킷을 보내게 된다.

공격 패킷은 SYN flooding, UDP flooding, ICMP echo requesting, ICMP broadcasting 등 다양하다. DDoS 공격은 이처럼 다수의 마스터와 그보다 훨씬 많은 수의 데몬들로 이루어져 있어 피해자 입장에서는 수십개 혹은 수백개의 호스트에서 동시에 엄청난 패킷을 받게 되는 것이다. 그러므로 DDoS 공격의 목표 시스템이나 네트워크는 물론이고 공격에 이용되는 마스터와 데몬이 설치된 호스트들도 서비스가 지연되거나 마비된다.

DDoS 공격에는 주로 Trinoo, TFN, Stacheldraft, TFN2K, Shaft 등의 공격도구가 이용되는데 최근에 윈도우즈용 DDoS 공격 도구도 등장하여 DDoS 공격에 윈도우즈 시스템까지도 이용되고 있음을 보여준다. 이러한 다양한 공격 도구들은 파괴력이 한층 증가되었고, 또한 자동 업그레이드 기능을 가지고 있다. 공격자들이 이미 공격한 타 시스템을 DDoS 공격에 이용하여 자신의 공격 출처를 숨김과 동시에 자원을 이용한다. 이처럼 DDoS 공격은 전통적인 DoS 공격에 비해 훨씬 지능적이고 복잡해지고 있기 때문에 이에 대한 대응 또한 쉽지 않다.

바. 이메일 오·남용 사례

다음은 이메일 오·남용과 관련된 사고로 메일폭탄 공격을 받은 사이트가 어떻게 사고에 대응했는지를 보여준다. 다수의 메일 릴레이 서버 사용, 적대적 성격의 공격, 구체적인 피해사실을 갖고 있는 전형적인 이메일 관련사고 사례이다.

(1) 사고 개요

1999년 1월 어느 날 새벽 1시 30분 정도부터 4시 30분 정도까지 한 웹 호스팅 업체가 메일 폭탄 공격을 받았다. 이로 인하여 메일 서버가 다운되고, 디스크 용량이 전부 소모되었다.

(2) 사고 확인

동일 오전 근무 시간에 메일서버가 다운된 것을 확인하고, spool 디렉토리를 확인한 결과, 엄청난 양의 쓰레기 메일이 쌓여 있는 것을 확인하였고, 해당 메일을 수신하기 시작한 시간과 종료된 시간을 확인할 수 있었다.

(3) 사고분석

1차적인 분석은 메일폭탄 공격이었으므로 대량으로 수신된 메일의 헤더를 분석하는 것이었다. 많은 메일 중에 내용이 다른 메일들을 샘플로 뽑아 분석하였다.

```
From help@xxx.xxx  Wed Jan  6 01:51:51 1999
Return-Path: 〈help@xxx.xxx〉
Received: from mail.relay.host1 (mail.relay.host1[mail.relay.host1.ip])
                    by xxx.xxx (8.9.1/8.9.1) with SMTP id BAA24672
                    for 〈help@xxx.xxx〉; Wed, 6 Jan 1999 01:51:51 +0900
Received: from [attack.host.ip.addr] ([attack.host.ip.addr])
                    by mail.relay.host1 (8.6.12h2/8.6.9) with SMTP id BAA05012
                  for help@xxx.xxx; Wed, 6 Jan 1999 01:38:48 +0900
Date: Wed, 6 Jan 1999 01:38:48 +0900
From: help@xxx.xxx
Message-Id: 〈199901051638.BAA05012@mail.relay.host1〉
  X-Authentication-Warning: mail.relay.host1: Host [attack.host.ip.addr] didn' t use HELO protocol
subject: Mail Delivery Problems
Apparently-To: help@xxx.xxx

Mail Delivery Problems
```

먼저, "From:" 하고 "Received:" 라인의 "for"가 서로 같고, "To:" 라인도 없는 것으로 보아 정상적인 메일헤더는 아니다. 그리고 실제로 본 메일을 수신한 계정은 "help@xxx.xxx" 이다. 다른 것은 볼 것 없이 바로 "Received:" 라인을 분석하였다. 각각의 시스템 이름과 IP 주소가 서로 일치하는 것으로 보아 메일 전달 경로는 위조되지 않은 것으로 판단된다. 따라서 공격자의 IP 주소는 마지막 "Received:" 라인의 "attack.host.ip.addr" 이다.

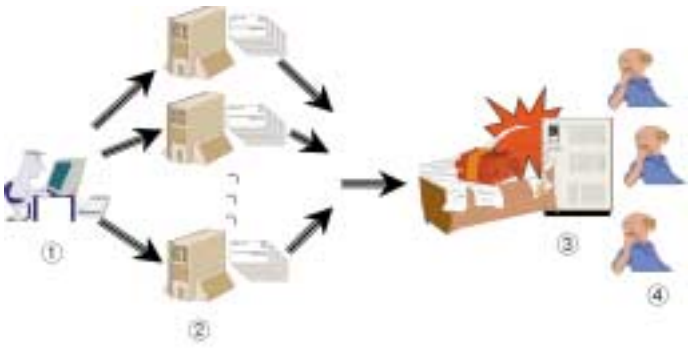
"Return-Path:"는 메일 수신자 계정과 똑같이 설정되어 있다. 이는 만약 송신한 메일이 여러 이유로 수신자 계정으로 가지 못했을 때, 메일이 되돌아오는 주소이다. 따라서 만약 피해시스템에 이상이 생겨서 메일을 더 이상 수신하지 못하게 되더라도, 해당 메일이 또 다시 피해시스템으로 전송되는 현상을 발생시킨다. 공격의 효과를 높이기 위한 방법이다.

그리고 "X-Authentication-Warning" 헤더에서 공격자 시스템이 정상적으로 메일 서비스를 이용하지 않았다는 경고가 나오는데(Host [attack.host.ip.addr] didn't use HELO protocol), 이는 mail.relay.host1 시스템이 메일 릴레이 시스템으로 사용되었음을 보여준다. 이러한 방식으로 다른 메일에 대해서도 분석한 결과, 대부분의 메일이 비슷한 패턴을 갖고 있었으며, 메일의 전달 경로가 전부 4곳의 시스템을 경유해서 전달되었다. 그리고 공격의 타겟이 된 계정은 "help@xxx.xxx, sysop@xxx.xxx, chief@xxx.xxx" 세계의 계정이었다.

Received: from **mail.relay.host2** (mail.relay.host2 [mail.relay.host2.ip]) by xxx.xxx (8.9.1/8.9.1) ...
Received: from [attack.host.ip.addr] ([attack.host.ip.addr]) by mail.relay.host2 (8.8.8H1/8.8.7) ...
Received: from **mail.relay.host3** (IDENT:root@[mail.relay.host3.ip]) by xxx.xxx (8.9.1/8.9.1) ...
Received: from [attack.host.ip.addr] ([attack.host.ip.addr]) by mail.relay.host3 (8.9.1a/8.8.5) ...
Received: from **mail.relay.host4** (IDENT:root@[mail.relay.host4.ip]) by xxx.xxx (8.9.1/8.9.1) ...
Received: from [attack.host.ip.addr] ([attack.host.ip.addr]) by mail.relay.host4 (8.9.1a/8.8.5) ...

수신된 메일을 확인한 결과 다음과 같은 공격의 전체적인 모습을 그릴 수 있었다.

메일 폭탄 공격
(그림 3-1-4)



① 공격자 : attack.host.ip.addr

② mail Relay : 4개의 Relay 서버경유(mail.relay.host1, mail.relay.host2, mail.relay.host3, mail.relay.host4)

③ 피해 호스트 : 웹호스팅 업체

④ 피해 사용자 메일 주소 : 3개(help@xxx.xxx, sysop@xxx.xxx, chief@xxx.xxx)

여기서 몇 가지 명백한 사실을 추측할 수 있다. 먼저 공격이 호스팅 업체 같은 특정 대상을 정하고 새벽에 이루어 졌다는 것은, 공격자가 악의적 목적을 갖고 공격을 했다는 것이다. 그리고 메일 폭탄의 목적지도 현재 사용하고 있는 3개의 계정인데 이는 무작위로 메일을 보낸 것이 아니라, 공격자가 대상 사이트에 대해서 먼저 정보를 수집하고 나서 그 정보를 바탕으로 공격을 했다는 것이다.

피해사이트의 시스템 로그 어딘가에 또 다른 공격자의 흔적이 있을 수 있다는 추측을 할 수 있다. 제일 먼저 의심이 되는 로그는 웹서버 로그이다. 웹 페이지를 조사해 본 결과 "ask.html" 페이지에서 위 3개 피해 계정이 사이트 연락처로 사용되고 있는 것을 알 수 있었다. 그리고 웹서버 로그에서 다음과 같이 같은 날 새벽 12시 35분경에 공격자가 웹 페이지에 접근했던 사실을 발견하였다. 즉, 공격자는 메일 폭탄 공격을 위해서 피해사이트 홈페이지에 접속하여 공격 대상 메일 계정을 알아낸 뒤 바로 공격을 한 것이다.

```
# grep attack.host.ip.addr /var/log/httpd/*
---------------------------------------
access_log:attack.host.ip.addr - - [06/Jan/1999:00:35:50 +0900] "GET / HTTP/1.1" 200 3028
access_log:attack.host.ip.addr - - [06/Jan/1999:00:35:52 +0900] "GET /image/bgr.gif HTTP/1.1" 200 401
...
access_log:attack.host.ip.addr - - [06/Jan/1999:00:37:08 +0900] "GET /ask.htm HTTP/1.1" 200 3650
access_log:attack.host.ip.addr - - [06/Jan/1999:00:37:10 +0900] "GET /image/ic1_1.gif HTTP/1.1" 200 639
access_log:attack.host.ip.addr - - [06/Jan/1999:00:37:10 +0900] "GET /image/ic4_2.gif HTTP/1.1" 200 713
 ------------------------------------------------
```

자료 출처:
사례로 배우는 해킹사고 분석 & 대응, 영진 출판사 (http://www.securitymap.net)

(4) 사고 대응

이 사건은 공격자가 분명한 의도를 가지고 공격을 한 것이며, 상당한 피해를 입었기 때문에 적극적인 조치가 필요하다. 만약 조치를 하지 않는다면 또 다른 공격을 당할 수 있음이 명백하였다. 대응조치는 공격자 추적, mail relay 사이트 추적 및 통보, 시스템 보완의 크게 세 부분으로 나뉠 수 있다.

제2절 개인정보보호 사고 유형 및 사례

1. 사고 유형

개인정보 사고는 주로 해당 정보를 다루는 회사나 담당 관리자의 부주의 또는 내부 직원에 의한 불법 도용으로 인하여 발생하는 경우와, 기업의 일반 사용자 PC가 악성 프로그램에 감염되거나, 또는 해킹에 의해서 유출될 수 있다.

[표 3-2-1]은 개인정보 침해와 관련된 사고의 유형과 그에 따른 사고접수 건수를 보여준다.

[표 3-2-1] '03년 유형별 개인정보 피해구제 신청현황

침 해 유 형	건 수	비율(%)
이용자의 동의 없이 개인정보 수집	19	2.3
개인정보 수집시 고지 또는 명시의무 불이행	2	0.2
고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공	39	4.6
개인정보 취급자에 의한 훼손 · 침해 또는 누설	28	3.4
개인정보 처리 위탁시 고지의무 불이행	2	0.2
개인정보관리책임자 미지정	1	0.1
기술적 · 관리적 조치 미비로 인한 개인정보 누출 등	12	1.4
수집 또는 제공받은 목적 달성 후 개인정보 미파기	81	9.6
동의철회 · 열람 또는 정정요구 불응	52	6.2
동의철회, 열람 · 정정을 수집보다 쉽게 해야 할 조치 미이행	1	0.1
법정대리인의 동의 없이 아동의 개인 정보 수집	561	66.4
타인 정보의 훼손 · 침해 · 도용	39	4.6
기타	8	0.9
합 계	845	100

자료 출처:
2004. 1., 2003
개인정보분쟁조정사례집

가. 부적절한 접근과 수집

부적절한 접근과 수집에는 보안관리자의 허가를 받지 않고 공공기관이나 기업 등의 컴퓨터에 침입하여 개인정보를 수집하거나 변경하는 행위, 또는 인터넷에 연결된 PC에 은밀하게 침입하여 개인정보를 수집하는 행위가 이에 속한다. 예를 들어, 은행이나 백화점의 데이터베이스에 침입하여 개인의 신용정보를 빼내거나, PC에 침입하여 사용자의 이메일 주소, 사용하는 소프트웨어 유형, 웹 접근 기록, 개인적인 데이터베이스를 수집하는 등의 침해행위가 있다.

정보주체의 동의가 없는 개인정보 수집, 개인정보 수집시 고지 또는 명시 의무를 이행하지 않는 행위, 과도한 개인정보 수집 등이 모두 여기에 속한다. 나아가 정보주체의 동의나 철회 · 열람 또는 정정 요구에 불응하거나 동의 철회 · 열람 또는 정정을 수집보다 쉽게 해야 할 조치를 이행하지 않는 행위도 여기에 포함시킬 수 있을 것이다.

나. 부적절한 모니터링

인터넷 마케팅업체들은 쿠키(cookie)를 사용해서 소비자들이 어느 웹 사이트를 접속해 얼마나 머무르고 어떤 거래를 하는지를 알아낸다. 본인들에게 알리지 않고 소비자들의 인터넷 활동을 모니터링하는 것이다. 호텔의 침실에 몰래카메라를 설치하여 투숙객들의 행동을 촬영하여 판매하거나 공장이나 백화점과 같은 일터에 CC 카메라 등을 설치하여 근로자들의 행동을 감시하는 행위도 여기에 속한다.

다. 부적절한 분석

소비자들이나 직원들에게 알려주지 않고 그들의 사적인 정보를 분석하는 행위를 말한다. 부적절하게 접근되고 수집된 정보와 부적절하게 모니터링된 정보가 분석되면 그것은 당연히 부적절한 분석이 된다. 그러나, 정당하게 수집된 정보일지라도 원래 소비자가 동의한 목적이외의 용도로 부적절하게 분석될 수 있다. 부적절한 분석을 통해 소비자의 구매나 소비패턴을 파악할 수 있으며, 분석결과를 지불능력에 따른 차별적인 서비스 제공 혹은 직원에 대한 통제강화에 이용할 수 있다.

라. 부적절한 이전

고객에게 알리지 않고 고객의 개인정보를 다른 기업들에게 넘겨주는 행위가 이에 속한다. 인터넷 업체들이 고객의 동의 없이 이름, 주소, 이메일주소, 전화번호 등 고객의 개인정보가 담긴 데이터베이스를 사고파는 경우가 적지 않다. 고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공도 이에 해당된다. 개인정보 취급자에 의한 누설, 기술적 · 관리적 조치미비로 인한 개인정보 누출도 이 범주에 포함시킬 수 있을 것이다.

마. 원하지 않은 영업행위

주로 인터넷 사용자의 동의나 허가 없이 상품 광고메일, 즉 스팸(spam) 메일을 보내는 행위를 말

한다. 이 유형의 프라이버시 침해에는 정크메일(Junk mail), 대량DM(Direct Mail), 정크 인터넷 푸시채널(Junk Internet Push Channel) 등 영리 목적의 광고성 정보전송이 포함된다.

바. 부적절한 저장

개인정보를 안전하지 못한 방식으로 보관하여 저장된 정보의 신뢰성을 떨어뜨리고 정보접근에 대한 인증을 수행하지 못하는 행위를 말한다. 예컨대, 데이터베이스 시스템 관리를 잘못하여 개인 사용자가 다른 사용자의정보를 훔쳐볼 수 있다. 개인정보 취급자에 의한 훼손이나 침해 및 수집, 그리고 제공한 개인정보를 활용 후 파기하지 않은 행위도 여기에 속한다.

2. 사고 사례

다음은 개인정보와 관련된 침해행위에 대하여 "개인정보침해신고센터"에 신고 접수된 사례 또는 언론에 발표된 사례로 각 기업이 개인의 정보를 올바르게 다루지 못하거나 또는 침해할 경우 입을 수 있는 손실을 보여준다.

가. 개인정보를 유출한 구직 사이트에 피해 보상을 요구

신청인 A씨(만27세)는 지난 2002년 11월 구직업체인 B사(피신청인)에 이직에 대한 상담을 받은 적이 있었는데 B사가 본인 동의 없이 무단으로 자신의 사례를 모 신문사에 제공하였다. 문제는 당시 A씨가 근무하던 회사 사장이 신문기사를 읽게 되어, A씨는 승진과 연봉 계약에 불이익을 받게 된 것. 이에 A씨는 B사를 상대로 경제적 · 정신적 손해에 대한 보상을 요구하였다.

한편, B사는 A씨의 동의 없이 상담 내용을 신문사에 제공한 것은 과실임을 인정하나 신문기사에는 A씨의 성명이 기재되어 있지 않아 당사자가 누구인지 식별할 수 없다고 주장하였다.

이에 대해 위원회는 비록 신청인의 성명이 포함되어 있지 않더라도 직업, 직책, 직종, 근무 연수, 전공 등이 구체적으로 기재되어 있어 당해 기사만으로도 충분히 신청인임을 식별할 수 있다고 판단하였다. 위원회는 B사가 A씨의 개인정보를 무단 유출한 사실을 인정, A씨가 입은 정신적 피해에 대한 보상으로 100만원을 지급하라고 결정하였다.

나. 탈퇴한 회원정보를 누출한 온라인게임업체에게 피해 보상 요구

A씨(신청인, 만29세)는 B사(피신청인)의 서비스를 이용하다가 2002년 8월 탈퇴하였음에도 불구하고, 지난 12월 제3자인 X씨의 포토앨범에 자신의 사진이 게재되어 있었을 뿐만 아니라 자신을 상대로 성적 수치심을 자극하는 글들이 게재되어 있는 사실을 발견, B사에 이에 대한 시정과 함께 정신적 피해에 대한 보상을 요구하였다.

조사결과 A씨의 회원탈퇴 당시 B사의 서버에 오류가 발생해 A씨의 사진과 개인정보가 파기되지 않은 것으로 밝혀졌다. 문제는 정상적인 절차를 거쳐 신청인이 이전에 사용했던 아이디를 부여받은 X씨의 포토앨범에 B씨의 사진이 누출되었고, 사진을 본 회원들이 X씨의 방명록에 성적 모욕감을 주는 글들을 게재하였다.

위원회는 피신청인이 자사 개인정보보호정책에 명시한 보유기간(탈퇴 후 3주 이내에 개인정보 삭제)을 넘어 신청인의 사진 등 개인정보를 보유한 위법 사항이 인정될 뿐만 아니라 피신청인의 경우 고객들의 개인정보를 수집 · 이용 · 관리함에 있어 개인정보가 누출되지 않도록 기술적 · 관리적 조치를 취할 의무가 있음에도 불구하고 이러한 의무를 소홀히 하여 신청인에게 돌이킬 수 없는 고통을 주었다면서 정신적 피해에 대한 보상으로 150만원을 지급하라고 결정하였다.

다. 고객DB를 소홀히 관리하여 고객의 개인정보를 누출

박철수(가명, 신청인, 만 29세)는 2003년 1월 B사(피신청인)가 운영하는 음식정보사이트에 회원으로 가입하여 이용하던 중, 지난 3월말 C 포탈사이트의 검색엔진을 통해 회원가입시 제공한 자신의 개인정보(성명, 주민등록번호, 주소, 전화번호, 아이디 및 PW 등)가 누출되는 것을 발견하였다. 이에 박철수는 B사가 고객DB의 관리를 소홀히 하여 자신의 개인정보가 인터넷 검색엔진을 통해 누출되었다며, 이로 인한 정신적 피해 및 향후 있을 수 있는 경제적 손해에 대한 보상으로 금 500만원을 요구하였다.

이에 대해 사업자측에서는 고객DB의 관리를 소홀히 한 적이 없다며 박철수의 개인정보가 인터넷 검색엔진을 통해 누출된 것은 당해 검색엔진이 자사의 고객DB를 해킹하였기 때문이라고 주장하였다.

위원회는 C 포탈사이트의 검색엔진의 경우 보안기능이 설정되어 있지 아니한 정보만이 검색되고 있는 점에 미루어 볼 때, 이를 해킹으로 볼 수 없다고 판단하였다. 또한 사업자는 정보통신망이용촉진및정보보호등에관한법률 제28조의 규정에 의하여 회원의 개인정보를 수집 · 처리함에 있어 고객의 정보가 누출되지 않도록 안전하게 관리할 책임이 있는 바, B사는 고객DB에 대한 기술적 · 관리적 조치를 미비하였을 뿐만 아니라, 신청인의 신속한 개선조치 요구에 대하여 아무런 조치를 취하지 아니한 위법이 있다고 판단하고 이로 인한 정신적 피해에 대한 보상으로 신청인에게 금 50만원을 지급하라고 결정하였다. 특히, 위원회는 누출된 개인정보의 도용으로 신청인에게 추가적인 손해가 발생한다면, 신청인은 추후 별도의 피해구제를 요구할 수 있다고 밝혔다.

라. 모회사 회원 30만 명 정보 유출

국내 최대의 xx 업체인 x사의 인터넷 사이트가 해킹 당해 회원 30만 명의 개인 정보가 유출된 사실이 뒤늦게 밝혀졌다. x사는 2001년 최초로 정보통신부 장관 데이터베이스 대상을 수상까지 했으나, 이번 해킹 사건으로 보안 관리 체계에 허점을 드러냈다.

서울경찰청 사이버수사대는 14일 x 사와 인터넷 부동산사이트 등의 인터넷 시스템에 침입해 개인 회원정보 30만 건 등 40만 건을 해킹한 김모(21 · 광진구 군자동)씨를 정보통신망이용촉진및정보보호등에관한법률 위반 혐의로 구속했다. 경찰은 또 김씨가 유출한 개인정보를 이용해 모 게임업체에서 사이버머니로 교환하려 했던 노모(38)씨 등 2명을 불구속 입건했다. 경찰에 따르면 김씨는 7일 오후 11시께 S대 보안동아리 회원인 친구의 계정을 이용, x사 인터넷 홈페이지의 회원정보 데이터베이스(DB)를 해킹 하는 등 이 달 초부터 총 3차례에 걸쳐 각종 인터넷 사이트에서 약 40만 건의 개인정보를 해킹한 혐의다. 조사결과 김씨 등은 상당수 네티즌이 각종 인터넷 사이트에서 똑같은 아이디와 비밀번호를 사용한다는 점에 착안, 이들의 신상정보로 모 게임 사이트에 접속해 회원들의 사이버머니를 몰래 빼돌리려 했던 것으로 밝혀졌다. 중졸 학력의 김씨는 약 3개월 동안 인터넷 보안업체에서 근무하기도 했으며, 아이러브스쿨, SBS등의 홈페이지를 해킹 하는 등 전문 해커 활동을 해 온 것으로 전해졌다.

x사측은 데이터베이스가 해킹 당한 사실을 전혀 눈치 채지 못하다가 사건발생 이틀 뒤인 9일 경찰의 통보를 받고 처음 알게 된 것으로 밝혀졌다. 특히 20대 후반~30대 중반의 전문직 종사자들이 가입한 x사의 회원 정보에는 주민번호, 주소 등 일반적인 회원 정보는 물론 가족관계, 종교, 연봉, 성장기 등이 상세히 게재돼 있다. 회사측은 아직 회원들에게 개인정보 유출 사실을 통보하지 않은 상태다. 경찰 관계자는 "x사의 개인정보 관리 프로그램은 상당히 취약해 보완 조치가 필요했으나 회사측이 이를 무시해왔다"면서 "x사를 담당하는 보안업체는 국내 최고 수준인데도 불구하고 해킹 직후 회사측에 경고조치도 취하지 않았다"고 밝혔다.

마. 개인정보 유출시 기업책임 강화해야

정보통신부가 3월 제시한 개인정보보호관리 가이드라인에 따르면 개인정보가 훼손된 경우 해당 개인정보를 신속히 복구할 수 있도록 정기적으로 저장하고 안전한 용기 또는 장소에 보관, 유지토록 하고 있다. 또 개인정보 취급 시스템에 대해 정기적으로 취약성 진단을 실시하며 취약점 보완을 위한 절차 및 지침을 운영하게 하고 있다. 개인정보 침해사고 발생 시 적절히 대처할 수 있도록 상황 진단 · 보고, 응급 조치 및 침해사고 복구 · 대응팀 및 연락체계 구축 등에 관한 지침을 운영토록 했다. 정통부의 가이드라인을 보면 개인정보 유출 방지에 초점이 맞춰져 있다. 유출이 되지 않도록 기업들이 만반의 준비를 하라는 것. 그러나 인터넷 시대에 있어 해킹으로 인한 개인정보 유출은 피할 수 없다는게 보안 전문가들의 지적이다. 방지대책만으로는 개인정보 유출 문제를 근본적으로 해결하기 어려운 것이다. 이 때문에 국내에서도 방지 대책은 물론, 유출사고 발생 이후 기업이 책임정신을 발휘하도록 해야 한다는 주장이 설득력을 얻고 있다. 캘리포니아 주정부와 정보통신부 정책간 가장 큰 차이점도 바로 여기에 있다.

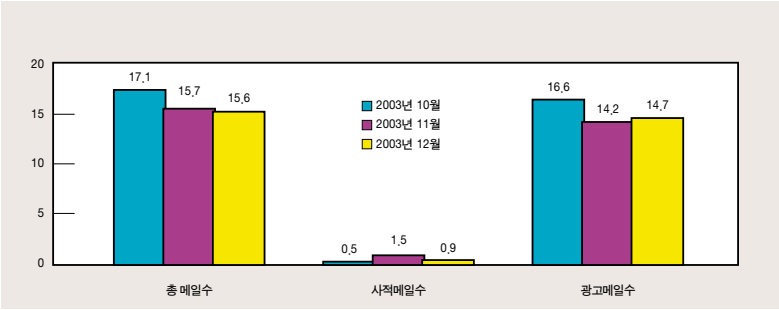
자료 출처 :
2003. 06. 05, news24

제3절 스팸메일 사고 유형 및 사례

1. 사고 유형

스팸메일이란 본인이 원하지 않고 요청하지 않았음에도 전송되는 이메일이다. 일반적으로 발신자가 자신과 아무런 관계가 없는 수신자에게 발송하는 전자 메시지를 스팸(spam)이라 하며, 쓰레기와 다름없다고 하여 정크메일(junk mail)이라고도 한다. 스팸메일에는 요청하지 않은 벌크메일(Unsolicited Bulk Email), 요청하지 않은 상업메일(Unsolicited Commercial Email)로 구분하기도 한다. 스팸메일은 컴퓨터 통신망에서 무차별적으로 배포되어 원치 않는 사람이 이러한 메일을 읽거나, 처리하게 하는 많은 시간과 비용을 낭비하게 한다.

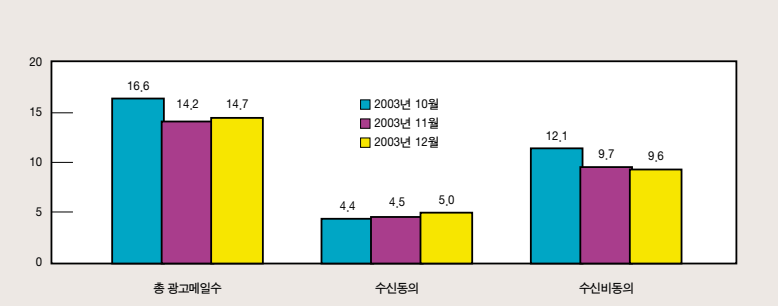
최근의 조사에 따르면 메일 계정 1개당 하루평균 총 수신 수는 15건 이상, 그리고 그중 광고메일 및 불법메일에 해당하는 건수가 90% 이상으로 조사되었다. 즉, 대부분의 수신되는 메일이 광고메일로 채워지고 있음을 알 수 있다.



광고메일 수신 비중
(그림 3-3-1)

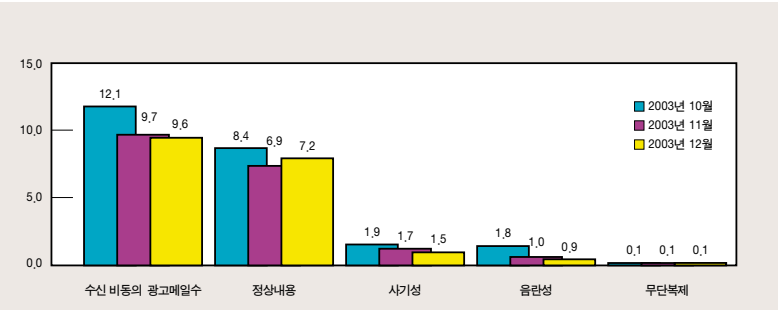
또한 이러한 광고메일 중 수신동의를 얻지 않은 불법 스팸메일에 해당하는 메일의 비중을 조사한 결과 60-70%의 비중을 차지하고 있다.

광고메일 중 불법 스팸메일 비중
(그림 3-3-2)



불법 스팸메일의 유형은 크게 수신동의를 하지 않은 정상적인 광고메일이 대부분을 차지하며, 기타 불법적 내용인 사기, 음란, 무단복제와 관련된 메일로 구분된다.

스팸메일 종류
(그림 3-3-3)



이러한 스팸메일로 인한 가장 큰 피해는 메일을 읽고 삭제하는데 따른 시간낭비가 가장 크며, 다른 필요한 정보를 수신하는데 방해가 되거나, 시스템의 손상까지도 가져오는 경우가 발생한다. 기업 측면에서 스팸메일로 인한 피해 유형을 살펴보면 다음과 같다.

- 시간 낭비
  기업 내의 모든 직원이 스팸메일을 읽거나 삭제하는데 소요되는 시간과 더불어 이러한 작업에 드는 정신적 스트레스를 포함할 수 있다. 스팸메일의 가장 큰 피해 형태이다.
- 정상적인 메일 수신 방해
  과도한 스팸으로 인하여 정상적인 메일을 수신하지 못하거나, 수신이 지연되는 경우가 발생

한다. 각 개인은 과도한 스팸으로 인하여, 정상적인 메일을 스팸으로 오인하여 무시하거나 삭제하는 경우도 발생한다.

- 자원 낭비

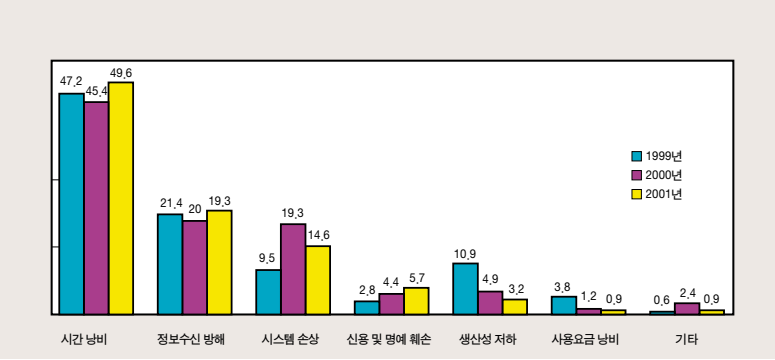
  스팸메일을 수신하고 처리하는데 소요되는 저장 공간, 프로세스, 네트워크 회선 사용 점유 등이 해당된다.

- 시스템 손상

  과도한 스팸메일은 메일서버의 정상적인 작동에 영향을 주며, 경우에 따라서 시스템 손상 또는 정상적인 메일을 수신하지 못할 수 있는 상황이 될 수도 있다.

- 이미지 훼손

  기업의 메일서버가 스팸메일의 경유지로 사용되거나, 또는 해당 기업의 이름으로 스팸이 발송된 경우, 기업 이미지에 심각한 문제를 야기할 수 있다. 이러한 사고 및 분쟁은 흔히 발생할 수 있는데 특히 스팸메일 경유지로 사용된 경우, 다른 사이트에서 해당 기업의 메일을 차단하는 경우가 많다.



연도별 스팸메일로 인한 피해유형
(그림 3-3-4)

최근의 조사에 따르면 스팸메일로 인한 피해 산출액이 국내의 경우 1조 3천억원, 전 세계적으로는 24 조원에 이르는 것으로 조사되고 있다.

[표 3-3-1] 스팸메일로 인한 피해규모 추정

피해부분	피해규모(원)	비중(%)
스토리지 비용	394,036,565,884	28.5
회선비용	49,496,524,442	3.6
처리비용	918,569,002,395	66.5
운영비용	19,362,000,000	1.4
합계(회선비용 포함)	**1,381,464,092,721**	**100.0**

2. 사고 사례

가. 불법 스팸메일 발송 68개 업체에 과태료

정보통신부는 지난해 11~12월 불법스팸대응센터에 신고된 업체들을 대상으로 사실조사와 의견진술 절차를 거쳐 68개 업체에 과태료를 물리고 127개 업체에 시정명령을 내리는 등 모두 195개 업체에 제재조치를 취했다고 19일 밝혔다.

정통부는 '성인광고' 표기의무 등을 위반하면서 음란성 스팸메일을 발송한 N사에 대해서는 법정 상한액인 1000만원의 과태료를 부과했고 이외에 광고 등 단순 영리목적의 광고성 정보를 전송한 67개 업체에는 250만~500만원의 과태료를 부과했다.

정통부 관계자는 '이번 제재와는 별도로 음란 스팸메일 발송자에 대해서도 성인광고 표기기준 위반여부를 조사중' 이라며 '위반 행위에 대해서는 올해 초 개정된 법률에 따라 최고 3000만원의 과태료를 부과할 방침' 이라고 말했다.

나. 마이크로소프트, 야후 스팸메일 첫 소송

마이크로소프트와 야후, AOL, 어스링크 등 4대 인터넷서비스공급업체(ISP) 는 10일(현지시간) 수신자가 원하지 않는 수백만 통의 스팸메일을 제작 발송한 수백 명을 상대로 6건의 소송을 제기했다고 발표했다.

지난해 4월 스팸메일에 대항하기 위한 반스팸메일 연합을 결성한 바 있는 이들 4개 업체는 이날 소송을 제기하면서 "미국 내에서 가장 악명 높은 스팸 발송자들이 포함돼 있다" 고 덧붙였다. 이들 업체는 스팸메일을 보낸 사람들의 신원을 파악하기 위해 관련 정보를 공유해 왔으나 수십 명의 혐의자는 구체적인 신원을 밝히지 못해 소장에서 불특정인을 의미하는 '존 도(John Doe)' 로 지칭했다.

마이크로소프트는 이날 매사추세츠주에 거주하는 볼프강 호크 씨와 뉴햄프셔주의 브레이든 부미벌 씨 등에 대해 체중 감량 보조제와 발모제, 포르노사이트 등을 소개하는 수백만 통의 스팸메일을 무차별적으로 보낸 혐의로 소송을 제기했다고 밝혔다.

야후도 지난 1월부터 야후 가입자들에게 9400만통 이상의 스팸메일을 보낸 캐 나다 온타리오주에 위치한 업체 대표인 에릭과 매튜, 바디 등 3명을 새너제이 연방법원에 고소했다. 야후는 이들 3명이 '무단 포르노 사진 추방 및 마케팅 규제법' 과 '컴퓨터 사기 및 악용에 관한 법' 을 위반했다며 이들의 이메일 발송 금지를 요구했다. 이번 소송은 지난 1월 반스팸메일법(Can Spam Act)이 발효된 이래 처음이다.

반스팸메일법은 남을 기만하는 이메일 제목을 사용하거나 추적을 피하기 위해 제3자 컴퓨터를 이용해 이메일을 보내는 것을 금지하고 있다.

제4절 불건전정보유통 사고 유형 및 사례

1. 사고 유형

불건전 정보는 사회적, 윤리적 가치관이 확립되지 못하고 정서적으로 민감한 청소년에게 매우 유해하며, 사회의 안정성에도 큰 영향을 미치기 때문에 이의 유통에 대하여 법으로 제재를 가하고 있다. 기업의 경우, 특히 해킹에 의해 자사의 서버가 음란물 등의 불건전 정보를 유통시키는데 이용되는 경우가 발생할 수 있다.

불건전 정보는 다음과 같이 분류 할 수 있다.

불건전 정보

- 음란물
  - 성행위 등을 표현하는 내용
  - 청소년 성매매 · 매춘 등을 권유 · 유도 · 조장하는 내용
  - 성관계를 목적으로 하는 만남 등을 유도하는 내용
  - 어린이 또는 청소년을 성 유희의 대상으로 묘사한 내용

● 명예훼손

- 개인의 사생활 침해 · 초상권을 침범한 내용
- 개인이나 단체에 대한 비방이나 허위사실에 관한 내용

● 폭력/잔혹/혐오

- 욕설 · 폭력행사 또는 조직폭력을 하게 하거나, 또는 이를 미화 · 조장하게 하는 등의 내용
- 살인을 촉탁하거나, 또는 이를 권유 · 유도 · 매개하는 등의 내용
- 사이버스토킹에 관한 내용

● 사행심조장

- 금전(사이버머니)거래를 통한 도박행위를 하게 하거나, 조장하는 등의 내용
- 불법적인 피라미드식 영업행위를 권유 · 조장하는 등의 내용
- 불법적인 경품/복권을 강매 또는 판매하는 등의 내용
- 아이템을 거래하거나 이를 판매하는 하는 등의 내용

● 사회질서관련

- 자살을 미화 · 권유 · 조장하거나, 자살방법을 적시하거나, 또는 동반자살을 유도하는 등의 내용
- 범죄 관련한 내용을 미화 · 권유 · 조장하는 등의 내용
- 불법적인 해킹이나 바이러스를 유포하는 행위
- 특정계층이나 종교를 비하하는 등의 내용

이러한 불건전 정보를 유통하는 대표적인 수단은 역시 인터넷인데, 2002년 1월부터 2003년 2월 중순까지의 경찰청 사이버테러대응센터의 유해사이트 관리현황에 따르면 전체 유해 사이트는 모두 3,649개였지만, 이 중 폐쇄된 사이트 1,517개를 제외한 나머지 2,132개가 여전히 가동되고 있는 것으로 조사됐다. 분야별로는 음란성 사이트가 1,239개로 가장 많고, 대포통장(타인명의 통장)등 기타 사이트 637개, 도박 등 사행성 91개, 총기 폭발물 제조 및 거래 80개, 청부살인 해결사 46개, 마약 의약품 거래 39개 등으로 집계됐다.

[표 3-4-1] 위법 · 유해사이트 집중단속 결과 (2003. 3. 3 - 4. 6)

구 분	음 란 사이트	음란스팸 메일발송	불법물 거 래	자살 · 해결사	기타위법 사이트	사이트 폐 쇄	총 계
계(건)	633	12	111	4	306	1,214	2,280
형사입건 (구속)	717 (40)	14 (2)	166 (52)	8 -	613 (168)	-	1,518 (262)

자료출처: 2003. 4 경찰청 보도자료

2. 사고 사례

가. 자살사이트 운영자 20대 3명 불구속

부산 동부경찰서는 인터넷에 자살사이트를 개설해 자살 방법을 알려준 혐의(자살방조)로 24일 정모씨(29 · 여) 등 3명을 불구속 입건했다. 경찰에 따르면 정씨 등은 모 인터넷 포털사이트에 '자살천사' , '죽음의 미소' 라는 이름의 동호회를 운영하면서 동반 자살한 이모씨(24) 등 회원 3명에게 게시판 등을 통해 간접적으로 자살 방법을 알려준 혐의를 받고 있다. 이에 앞서 경찰은 숨진 이씨 등에게 e메일과 전화로 자살 방법과 극약을 구입하는 방법을 자세하게 알려준 엄모씨(25) 등 2명을 20일 구속했다. 이씨와 또 다른 이모씨(23 · 부산D대 2년), 손모씨(31 · 여)는 9일 부산 동구 초량동 S여관에서 극약을 먹고 숨진 채 발견됐다.

나. 아동 포르노 유포

선생님 인적사항을 도용하여 '애플 로리타' 라는 아동포르노 인터넷 사이트를 운영한 중학생 유모군을 비롯, 도합 2,400여개 아동포르노 사진 또는 링크된 아동포르노 사이트 주소를 유포한 운영자 등 5명 검거

피의자1)은 중학생으로 피의자2)와 공모하여 2001.11.30경 피의자2)가 개설한 '애플로티타' 아동포르노 사이트를 운영하기 위해 학교 선생님 인적사항을 도용하고, 동사이트 회원인 피의자3), 피의자4)와 더불어 국내.해외 아동포르노 사진 등이 링크되어 있는 인터넷 주소 2,187개를 직접 게시하거나 회원들의 행위를 방조하고, 피의자5)는 2001.12.16경 타인 명의를 도용하여 '초딩동굴 탐험교실' 이라는 아동포르노 사이트를 개설한 뒤, 아동포르노 동영상 12개를 게시하고, 7차례에 걸쳐 1,000여명 상당의 동사이트 회원들에게 전체메일을 발송하여 아동포르노 주소 59개를 유포하고, 아동 포르노물을 게시하는 회원들의 행위를 방조하였다.

※ 정보통신망이용촉진등에관한법률 제65조 제 1항 제 2호....1년 이하, 1천만원이하 벌금

자료 출처 : 2002. 1. 17, 서울지방경찰청 사이버범죄 수사대 보도자료

다. 해외서버 등 유해사이트 262명 구속

경찰청 사이버테러 대응센터는 지난달 3일부터 한달 여간 각종 위법 · 유해사이트에 대한 집중단속을 벌여 모두 2천 280건을 적발, 262명을 구속하고 1천214개 사이트를 폐쇄조치 했다고 9일 밝혔다. 적발된 사이트는 유형별로 음란사이트가 633개로 가장 많았고 '대포폰'과 '대포통장' 등 불법물 거래 사이트 111개, 음란 스팸메일 발송이 12건, 자살 및 해결사사이트가 4개, 기타 위법사이트가 306개였다. 경찰은 음란사이트들이 국내 법망을 피해 음란물에 대한 법적 제재가 없는 외국에서 운영되는 경우가 늘고 있으며, 캐나다에서 현지인을 고용해 인터넷 포르노 방송국을 운영하다 검거된 박 모(32)씨처럼 인터넷 생방송 형태의 음란사이트도 증가하고 있다고 밝혔다. 경찰 단속을 피하기 위해 외국사이트를 가장한 음란사이트도 적발됐다.

경찰은 이런 유해사이트 단속의 문제점으로

▲ '표현의 자유' 문제로 일률적 통제가 어렵고

▲ 서버가 외국에 있는 경우 문화적 차이로 외국과 공조수사가 어려우며

▲ 대포통장 등 불법물 거래 사이트는 운영사실만으로는 형사처벌이 불가능한 점 등을 지적했다.

이에 따라 경찰은 운영자가 입건된 사이트 외에 현행법상 운영 자체만으로는 처벌이 어려운 사이트와 카페 등은 인터넷 서비스 업체 자체 약관에 의해 폐쇄를 의뢰하고 있다. 경찰은 "표현의 자유는 보호하되 반사회성이 명백한 사이트는 철저히 단속하며 신종범죄에 대한 처벌법규가 미비한 경우 관련 법령을 정비하고 시민 · 사회단체들과 협조해 인터넷 정화운동을 지속적으로 벌일 방침"이라고 밝혔다.

자료 출처:
2003. 04. 09, 연합뉴스

c o n t e n t s

제 4 장
서버운영관리

제1절 Windows 2000 Server

근래 들어 Windows의 취약성에 대한 공격이 증가하고 있는 추세이다. 따라서, 보안운영자 입장에서는 불필요한 서비스를 제거하고 사용 중인 서비스에 관련된 사항을 정확히 설정하여 공격으로부터 정보시스템을 최대한 보호 하도록 한다. 또한 취약성 관련 사항 확인 및 패치를 지속적으로 하는 것 또한 빼놓을 수 없는 중요한 보안대책 중 하나이다.

1. 패치 및 서비스 팩 설치

보안에 대한 문제가 발생하는 부분의 대부분은 사용자의 과실이다. 이러한 과실을 최소한으로 줄이기 위한 여러 가지 방법 중, 윈도우즈 시스템에 대한 패치와 보안 설정에 대해 자동으로 점검할 수 있는 부분에 대해서 설명 하고자 한다.

가. MBSA (Microsoft Baseline Security Analyzer)를 통한 보안 점검

MBSA는 Windows NT 계열의 시스템을 점검할 수 있으며, 해결 방법도 제시하고 있다. 단, Windows 2000 이상의 시스템에서 구동가능하다.

MBSA는 HFNetChk 도구를 사용하여 보안 업데이트가 시스템에 적용되었는지를 확인하는 도구이다.

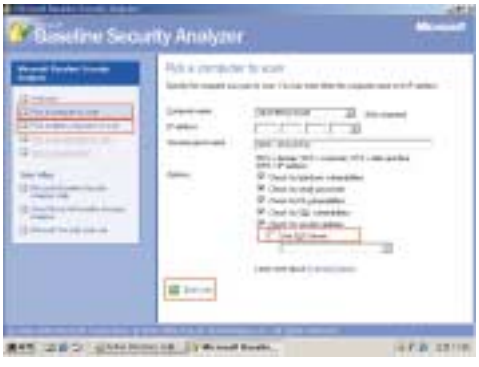
HFNetChk는 Microsoft가 지속적으로 업데이트하는 XML 보안 핫픽스 데이터베이스를 조회하여 다음의 작업을 수행한다.

- 강력한 암호와 같은 일반 보안 최적의 활용을 위해 Windows 데스크톱과 서버를 검사하는 작업
- 잘못된 일반 보안 구성을 확인하기 위해 IIS와 SQL Server를 운영하는 서버 스캔 작업
- Microsoft Office와 Outlook, Internet Explorer에 잘못 구성된 보안 영역 설정, Exchange Server 에 대한 검사 작업

가장 단순한 작동 모드에서 MBSA는 하나의 컴퓨터만 스캔 할 수 있다. 이 모드에 대한 전형적인 시나리오는 self-scan인데, [Pick a computer to scan] 작업을 선택하면, 스캔 할 컴퓨터의 이름이나 IP 주소를 입력하는 옵션이 있다. 기본적으로 이 옵션을 선택할 때 표시되는 컴퓨터 이름은 도구가 실행되고 있는 로컬 컴퓨터의 이름이 된다. 다중 컴퓨터의 경우 [Pick Multiple Computers to Scan]을 선택하면 하나 이상의 컴퓨터를 스캔 할 수 있다. 도메인 이름을 입력하여 전체 도메인을 스캔 하도록 할 수도 있고 IP 주소의 범위를 지정하여 그 범위 내의 모든 Windows 기반 시스템을 스캔 할 수도 있다.

① [시작] ⇨ [프로그램] ⇨ [Microsoft Baseline Security Analyzer 1.2] 실행

② [단일/다중컴퓨터]를 선택 후 "컴퓨터/그룹 이름"이나 "IP를 입력"하고 [option] 항목에서 원하는 항목을 선택한 뒤 [start scan]을 선택 한다. 단, 다중 컴퓨터를 스캔 할 경우 계정에 대한 문제가 해결이 되어야한다.



MBSA Self-scan 실행화면
(그림 4-1-1)

③ SUS (Software Update Services)와 연동도 가능하다. 이 서비스는 마이크로소프트 보안 데이터베이스에 접근하여 필요한 목록을 다운받아 로컬로 배포가능하다. 한글로 작성된 문서는 MBSA와 연동하는 부분에 대해서는 간략하게 나와 있으므로 상세한 설명은 영문 자료를 참고한다.

※ SUS 관련 문서 (한글)
http://www.microsoft.com/korea/windows2000/windowsupdate/sus/susoverview.asp?SD= GN&L=KO&gssnb=1

④ scan이 완료된 후 각각의 항목에 빨간색 X 표시의 경우는 처리되지 않은 부분이 서버 보안설정에 맞지 않은 상태이다. 나타나는 항목은 선택한 항목에 따라 다르지만 Windows 보안 업데이트, Windows 서버 자체에 대한 기본적인 보안설정, IIS 보안설정, SQL 보안 업데이트 및 설정, Exchange 관련된 사항도 점검이 가능하다.

MBSA 스캔 실행화면
(그림 4-1-2)

MBSA 결과 화면
(그림 4-1-3)

※ MBSA 다운로드 사이트

http://search.microsoft.com/search/results.aspx?st=b&na=88&View=en-us&qu=mbsa

나. 오프라인으로 서비스 팩 및 중요 핫픽스 설치

서비스 팩이란 제품이 출시되고 난 뒤 윈도우와 관련된 응용프로그램, 서비스, 실행파일 등 여러 수정 파일들을 모아 놓은 프로그램이다. 서비스 팩은 필요에 따라 일년에 몇 번씩 발표된다.

반면 핫픽스(hotfix)는 말 그대로 즉시 교정되어야만 하는 주요한 취약점으로 주로 보안과 관련된 사항들을 패치하기 위해서 배포되는 프로그램이다. 핫픽스는 각각의 서비스 팩이 발표된 후 중요 정정사항에 대해 발표된다. 한 가지 주의할 것은 간혹 서로 다른 핫픽스가 동일한 파일을 변경하는 경우가 있으므로 핫픽스 설치 시 먼저 배포된 것을 먼저 설치하는 것이 안전하다.

여기서는 "Service Pack 4" 와 "kb824146" 핫픽스(hotfix)를 예로 들어 설명한다. 이 패치는 블래스터 웜(Blaster Worm)이라는 Windows 바이러스에 대한 패치이다.

※ 서비스 팩 4 및 kb824146 다운로드 경로

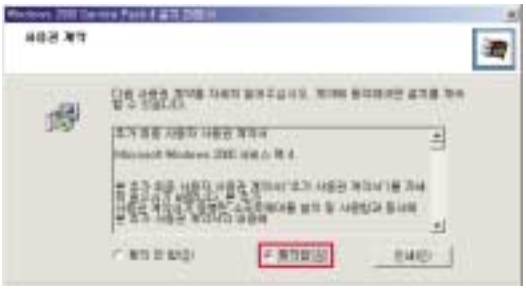
http://www.microsoft.com/korea/Windows2000/downloads/servicepacks/sp4/download.asp

http://www.microsoft.com/downloads/details.aspx?displaylang=ko&FamilyID=F4F66D56-E7CE-44C3-8B94-817EA8485DD1

① 서비스 팩을 실행하면 압축이 풀리고, 마법사가 실행된다.

서비스 팩과 hotfix 다운로드
(그림 4-1-4)

② 다음 버튼을 클릭하면 사용권계약에 대해 나오는데 동의를 하지 않으면 설치가 중단되니 동의를 하고 다음으로 넘어간다.



사용자 동의 화면
(그림 4-1-5)

③ 다음은 파일 보관 여부를 선택해야하는데, 서비스 팩 설치로 인해 문제가 발생될 수 있으므로 보관 할 것을 권장한다. 보관을 하지 않은 상태일 경우 서비스 팩 제거시 문제가 발생할 수도 있다.

파일 보관 선택 메뉴
(그림 4-1-6)

④ ③번 과정이 끝나면 설치로 들어간다. ③번 과정에서 파일보관을 선택 시에는 이전 파일들을 백업 후 설치를 시행한다.

시스템 업데이트 중
(그림 4-1-7)

⑤ 설치완료 창에서 **[다시 시작 안함]**에 체크를 하지 않으면 재부팅을 하게 되는데, 설치 할 업데이트가 남아있기 때문에 체크를 선택하고 마치도록 한다.

설치 마법사 완료
(그림 4-1-8)

⑥ 위에서 이야기한 추가적인 패치(kb824146)적용을 바로 수행한다. 실행 이후의 작업은 ① ~ ④ 번 까지는 동일하며, ⑤번 작업 시에는 **[다시 시작 안함]** 에 체크를 하지 않고 마친다.

설치 마법사 완료
(그림 4-1-9)

다. Windows Update를 통한 설치

① 인터넷 연결이 되어있는 상태에서 작업표시줄에서 **[시작]** ⇨ [Windows Update]를 클릭하면 업데이트가 실행되며, 인증 창이 나타나면 **[예]**를 클릭한다.

Windows Update
(그림 4-1-10)

업데이트 사이트 접속
(그림 4-1-11)

② Windows Update 페이지로 연결되면 "Windows Update 소프트웨어 확인중" 이라는 메시지가 나타난다.

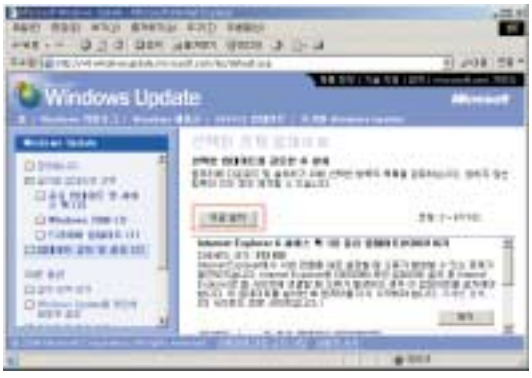
업데이트 확인중
(그림 4-1-12)

③ "Windows Update를 시작합니다." 라는 메시지 화면에서 **[업데이트 검색]**을 클릭 한다. 사용자의 시스템에 설치되어 있는 윈도우즈 정보와 업데이트 정보를 분석하는 화면이 나온 후 업데이트 할 항목의 개수를 보여준다. **[업데이트 검토 및 설치]** 버튼을 클릭한다.

업데이트 검토 및 설치
(그림 4-1-13)

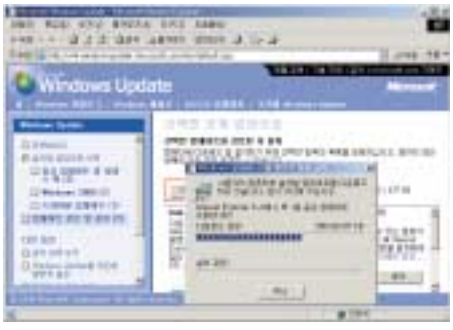
※ 인터넷 속도와 업데이트 목록에 따라서 수분 ~ 수십 분이 걸릴 수도 있으며, 웹 브라우저를 업데이트 할 경우는 일반 다운로드 사이트에서 Internet Explorer 6.0 버전을 다운받아서 설치하면 조금이나마 시간을 절약할 수 있다.

④ **[업데이트 검토 및 설치]** 버튼을 클릭하면 업데이트 할 세부항목에 대한 설명이 나오며, 다운로드에 필요한 파일의 크기와 시간이 나온다. **[지금설치]**를 누르면 필요한 파일을 다운로드하고, 설치하는 과정이 나오면서 업데이트가 시작된다.



설치하기 클릭
(그림 4-1-14)

⑤ 설치가 완료되면 메시지에 따라 시스템을 재부팅 한다. 일부 설치된 패치들은 Windows를 재부팅 한 후에 시스템에 적용된다. 설치 완료 후 ① ~ ② 과정을 반복하면 왼쪽의 창에서 **[설치 내역 보기]**를 확인할 수 있는데, 이 메뉴를 클릭하면 다운로드 하여 설치한 날짜나 성공여부 및 내용 등을 확인할 수 있다.



설치과정
(그림 4-1-15)

설치 내역 보기
(그림 4-1-16)

2. 계정 및 패스워드 관리

가. 워크그룹 관리

① **[내 컴퓨터]**에서 오른쪽 마우스를 눌러, **[관리]**를 클릭하여 **[컴퓨터 관리]**를 실행한다.

컴퓨터 관리 선택
(그림 4-1-17)

② **[컴퓨터관리]** ➪ **[시스템 도구]** ➪ **[로컬 사용자 및 그룹]** ➪ **[사용자]**를 클릭한다.

컴퓨터 관리에서 사용자 선택
(그림 4-1-18)

③ **[사용자]**의 오른쪽 창에 나타나는 것이 계정이며, 생성은 오른쪽 창에서 오른쪽 마우스를 클릭하여 **[새 사용자]**를 클릭한다.

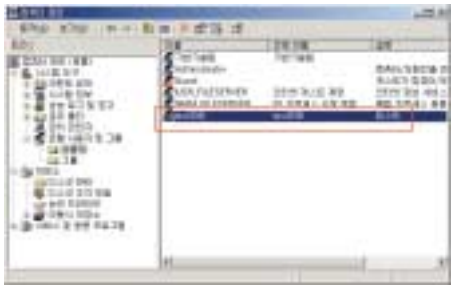
④ **[사용자 이름]**에 "로그인 ID"를 입력하고, **[암호]** 및 **[암호확인]**에 , "암호"를 입력하고 **[만들기]** 버튼을 클릭하여 계정을 생성한다.

※ [다음 로그온 할 때 반드시 암호 변경]은 최초 로그온 시 암호를 변경하도록 설정하는 기능을 가지고 있다. 일반적으로 체크를 제거한 후 바로 아래에 있는 두 개의 체크박스에 체크를 하고 생성한다.

새 사용자 설정
(그림 4-1-19)

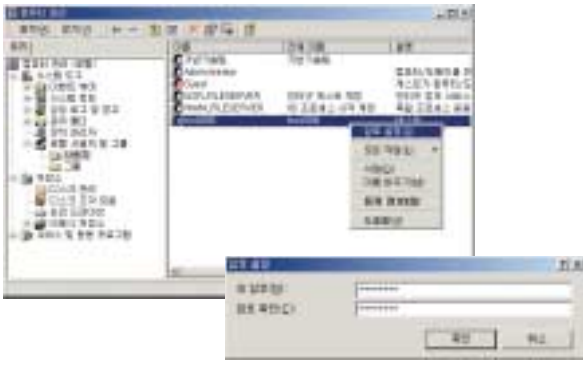
새 사용자 암호 설정
(그림 4-1-20)

⑤ 계정 리스트에서 방금 생성한 계정을 확인할 수 있다.



계정 확인
(그림 4-1-21)

⑥ 기존 계정의 암호 변경을 원할 경우 원하는 계정에서 마우스 오른쪽 버튼을 눌러 **[암호설정]**을 클릭하여 변경할 암호를 입력 후 **[확인]**을 눌러 저장한다.

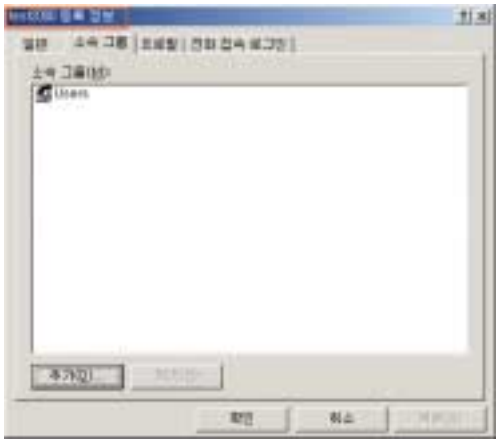


암호 설정 선택
(그림 4-1-22)

암호 변경하기
(그림 4-1-23)

⑦ 계정 등록정보 변경을 원할 경우는 계정을 더블클릭하거나 마우스 오른쪽 버튼을 클릭 하여 **[등록정보]**를 열어서 편집하면 된다.

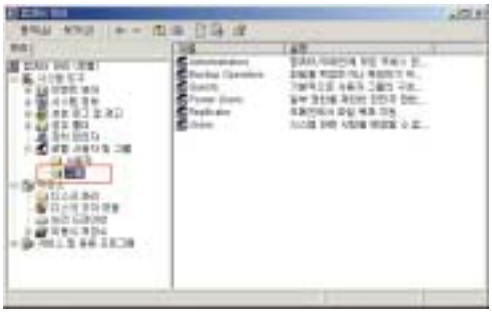
계정 등록 정보 변경
(그림 4-1-24)



⑧ **[소속그룹]** 눌러 자신이 속해있는 그룹을 변경할 수도 있다. 최초 계정 생성 시에는 "Users" 그룹의 구성원으로 속해있으며, 이는 공유나 컴퓨터 사용 시에 권한을 제한하는데 사용된다. 컴퓨터에 직접 로그인을 하여야 되는 경우는 **[Administrators 그룹]**을 클릭하여 소속그룹에 추가 후 작업을 하여야 제한이 없다.

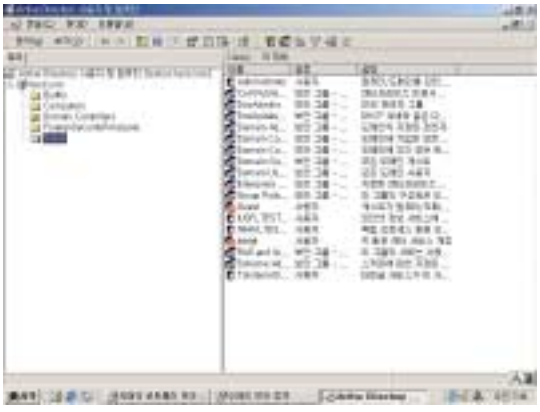
※ 그룹은 [로컬 사용자 및 그룹] ⇨ [그룹] 을 선택하여 확인할 수 있다. 여러 가지의 그룹이 존재하는데, 각 그룹의 설명을 보면 어떠한 작업을 할 수 있는지 확인이 가능하다. Administrators 그룹의 경우는 윈도우의 모든 부분에 대해서 제한을 받지 않는 그룹이다.

그룹 선택
(그림 4-1-25)

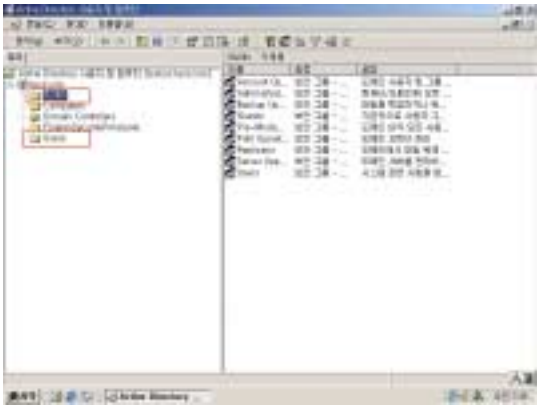


나. 도메인 구조

① 계정관리 도구 **[컴퓨터 관리]**가 아닌, **[Active Directory 사용자 및 컴퓨터]**에서 설정하여야 한다. 콘솔창이 열리면 [User] 라는 컨테이너가 보이는데 이 부분에 사용자 계정 및 새로 생성된 그룹이 존재하며, [Builtin] 에는 워크그룹 상태의 그룹이 존재한다.



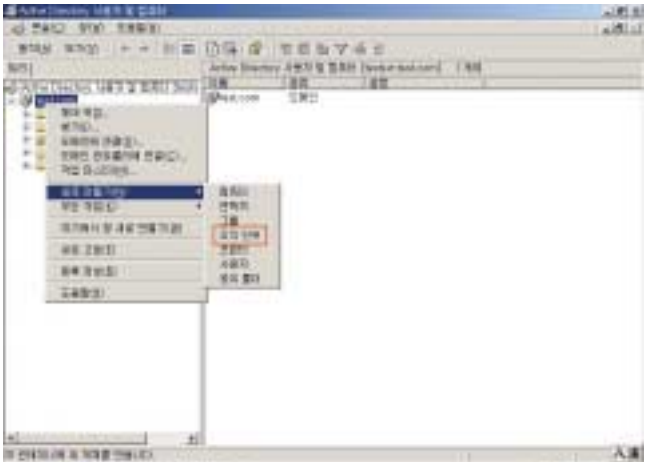
Active Directory 사용자 및 컴퓨터(User)
(그림 4-1-26)



Active Directory 사용자 및 컴퓨터(Builtin)
(그림 4-1-27)

② 계정 생성 시 가능하다면 OU(Organization Unit)를 사용하도록 한다. 이 방법이 차후 계정 관리나 정책 적용 시 용이하다. 생성 방법은 원하는 위치에 마우스 오른쪽버튼을 눌러 **[새로 만들기]** ⇨ **[조직단위]**를 선택 후 원하는 이름을 입력하여 만든다.

OU 추가 작업
(그림 4-1-28)



③ 그룹정책은 기본적으로 상위 도메인의 정책을 상속받게 되지만, 상속을 받지 않고 새로운 그룹정책을 생성하여 적용할 수 있다. 위에서 생성된 OU 를 마우스 오른쪽 버튼으로 선택 후 **[등록정보]**를 선택하여, **[새로 만들기]** 나 **[추가]**를 할 수 있다. 상위의 정책을 거부 시에는 **[정책을 상속받지 못하게 함]** 체크 박스를 클릭하면 된다.

OU 정책 생성 및 추가
(그림 4-1-29)

※ 계정은 눈에 보이는 것으로 관리되지만, 실제 Windows에서 관리되는 아이디는 S-x-x-xx-.... 형태로 남게 된다. 이를 SID(Security ID)라고 한다. 기본적인 SID 정보는 다음과 같다.

o Administrator : 마지막이 500으로 끝난다.
o Guest : 마지막이 501로 끝난다.
o 윈도우 설치 후 생성된 사용자 계정 : 마지막이 1000 이후부터 시작한다.

이러한 정보를 이용하여 해킹을 시도하는 경우도 적지 않으니, 반드시 Administrator 의 계정 이름 변경을 하도록 한다. Windows 2003 의 경우는 500의 SID를 가진 사용자를 사용하지 않을 수 있지만, Windows 2000 의 경우는 아직 불가능하기 때문이다.

3. 공유폴더 관리

가. 관리적 공유

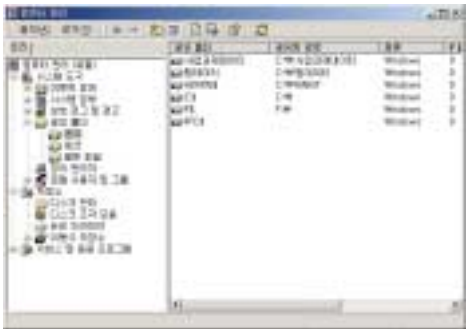
관리 폴더란, 드라이브문자$(a$, c$, d$ 등)인 ADMIN$, IPC$, PRINT$ 등의 공유를 말하며, 드라이브 문자$의 경우 Administrators 또는 Backup Operators 그룹의 구성원이 접근 가능하다. 이러한 공유는 편리하지만, 보안적인 측면에서는 상당히 취약하다. 이러한 공유를 제거하는 방법에 대해 설명한다.

① **[시작]** ⇨ **[제어판]** ⇨ **[관리도구]** ⇨ **[컴퓨터관리]**를 실행한다.

컴퓨터 관리 선택
(그림 4-1-30)

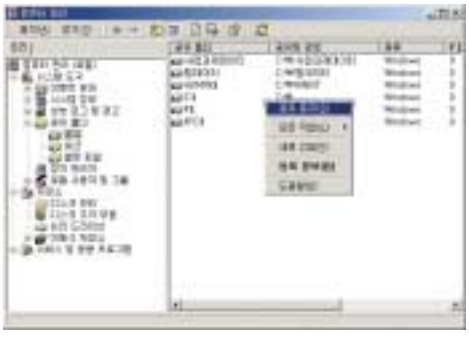
② **[시스템 도구]** ⇨ **[공유 폴더]** ⇨ **[공유]**를 클릭하면 위에서 언급한 공유 리스트가 보인다.

공유 리스트 확인
(그림 4-1-31)



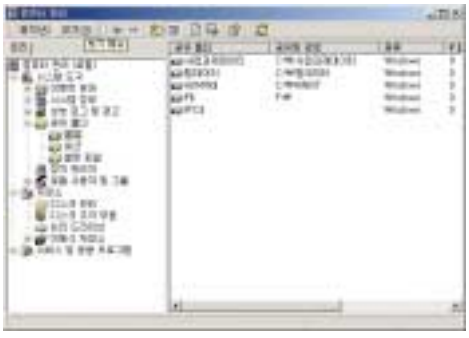
③ 제거를 원하는 공유폴더를 클릭 후 마우스 오른쪽 버튼을 눌러 **[공유 중지]**를 선택하여 제거한다.

공유중지 선택
(그림 4-1-32)



공유중지 확인
(그림 4-1-33)

공유 중지 후 화면
(그림 4-1-34)



④ ③번에서 공유를 제거 했다고 해서 제거가 되는 것은 아니다. 위의 그림처럼 재부팅을 하게 되면 다시 공유를 생성하게 되기 때문이다. 이 부분까지 해결하기위해서는 레지스트리 키를 수정해 주어야 한다.

[시작] ➪ **[실행]** ➪ "regedt32" 를 입력 후 엔터를 치면 레지스트리 편집기가 실행된다.

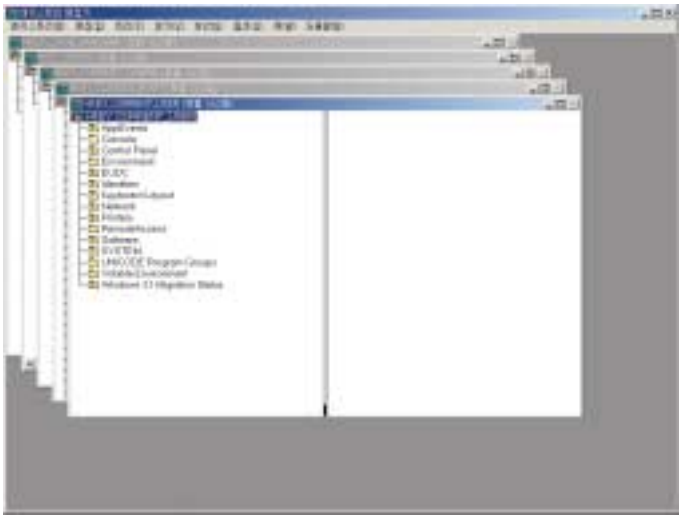
※ 레지스트리(registry)란 Windows 운영체제에서 사용되는 환경설정 및 시스템에 관련된 정보가 저장된 장소를 의미한다. 재부팅 후 관리폴더의 디폴트 공유를 제거하기 KEY_LOCAL_MACHINE을 선택하여 "\" 내부에 있는 항목 순으로 확장을 하여 아래 값을 생성하면 된다.

KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

Value Name : AutoShareSvr

Type : REG_DWORD

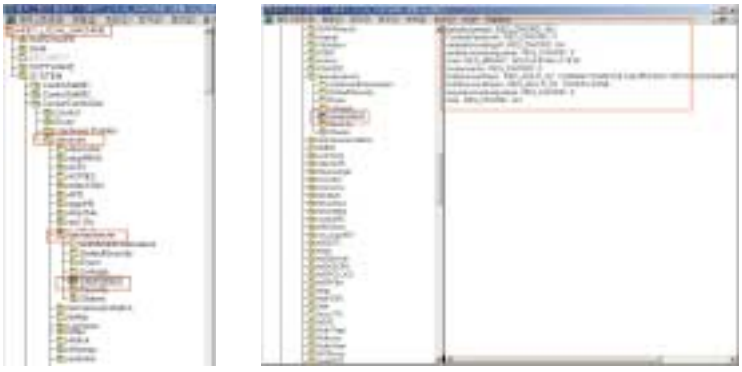
Value : 0



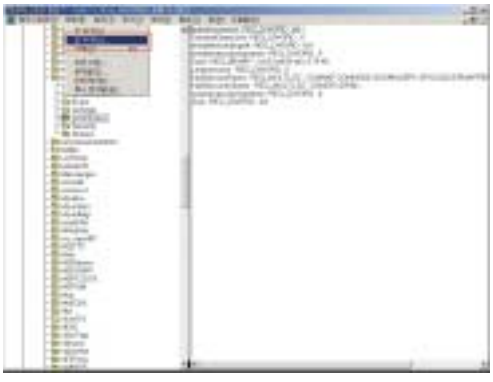
regedt32 실행화면
(그림 4-1-35)

레지스트리 항목
(그림 4-1-36)

레지스트리 상세항목
(그림 4-1-37)



레지스트리 추가방법
(그림 4-1-38)



레지스트리 값 추가
(그림 4-1-39)

⑤ IPC$ 의 경우는 제거가 되지 않으므로 널 세션 (Null Session)을 제거하는 방법으로 작업을 하도록 한다.

※ 널 세션(Null Session) 접속은 윈도우 NT계열 시스템으로부터 사용자 인증을 받지 않은 접속이다. 윈도우 NT계열 시스템으로의 널 세션 접근을 획득한다는 것은 해커가 윈도우 NT계열 컴퓨터에 대한 정보를 제공받아 해킹 할 수 있다는 의미이다. 따라서 아래처럼 레지스트리 키 값을 변경하여 넬 세션 접속을 막도록 설정한다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Value: 1

기본 값은 0 으로 되어 있으며, 1로 변경

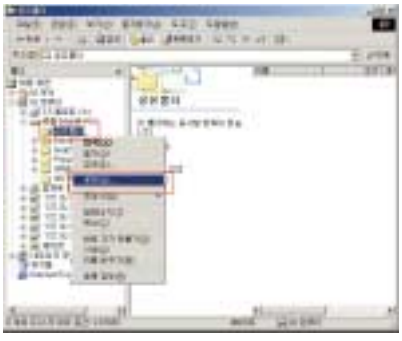
이 값은 이미 존재하기 때문에 값(value)을 수정하도록 한다.

레지스트리 값 변경
(그림 4-1-40)

나. 사용자 공유

사용자 공유란, 사용자의 필요에 의해 임의로 생성한 공유를 말하며, 관리자가 지정한 사용자는 모두 접근이 가능하다. 왜냐하면, 공유 생성 시 기본적으로 EveryOne 그룹에 읽기 권한이 주어진다.

① 공유를 원하는 폴더를 마우스 오른쪽 버튼으로 선택하여 **[공유]**를 클릭하면 **[공유폴더 등록정보]** 화면이 나오는데, **[이 폴더를 공유함]**을 클릭하여 공유를 하며 **[공유이름]**에서 원하는 이름으로 변경을 하도록 한다.



공유 설정
(그림 4-1-41)

공유폴더등록정보
(그림 4-1-42)

② [사용 권한]을 클릭하여 공유폴더의 사용권한에서 [변경] 체크박스를 [거부]로 선택한다.

공유폴더의 사용권한
(그림 4-1-43)

※ Windows 2000 이상의 경우 권한설정에서 허용과 거부가 동시에 적용이 될 때는 거부권한이 우선권을 가지게 된다. 예를 들면, 위의 그림에서 EveryOne 권한의 허용에 읽기권한이 체크되고 거부에 모든 권한이 체크되면, 아무도 접근을 할 수 없게 된다.

4. 파일시스템 권한 설정

일반적으로 관리자라면 시스템 파티션과 데이터 파티션은 분리하여 사용할 것이다. 또한, NTFS 파일시스템을 사용해야 보안상 안전하다고 알고 있다. NTFS 파티션을 사용하면 FAT이나 FAT32, FAT32x 파일 시스템에서는 불가능한 액세스 제어와 파일 보호가 가능하다. 만약 NTFS가 아니라면 convert 유틸리티를 사용하면 데이터의 손상 없이 FAT 파티션을 NTFS로 변환할 수 있다.

최초 설치시 디스크는 드라이브 루트상에 [EveryOne] 그룹에 [Full Control] 권한이 부여된 상태인데, Windows 98과 같은 상태라고 보면 된다.

※ convert 유틸리티를 사용하면 ACL은 변환된 드라이브를 모든 사용자가 모든 권한(Full Control)을 가지도록 설정된다. Windows 2000 Server Resource Kit에 포함된 fixacls.exe 유틸리티를 사용하여 ACL을 적절하게 재설정한다.

가. 권한 설정 및 변경

① 각 드라이브의 등록정보를 클릭하여 **[보안]**을 선택하여 [EveryOne]을 제거한다.

기본적인 사용권한
(그림 4-1-44)

② **[추가]** 버튼을 클릭하여 [administrators]와 [SYSTEM] 및 각 서비스에 필요한 계정만 접근할 수 있도록 권한을 부여한다. [administrators]와 [SYSTEM]에는 **[모든 권한]**에 체크를 한다.

계정 선택
(그림 4-1-45)

사용권한 설정
(그림 4-1-46)

나. 권한 변경 시 주의사항

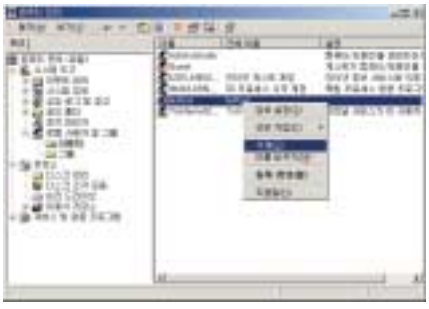
폴더에 권한 부여 시 사용자 별로 권한을 부여하는 것이 좋지만, 차후 계정이 삭제되어도 "S-x-x-xx-...." 형태로 권한은 부여된 상태로 남아있게 되기 때문에 계정을 삭제할 경우 디스크에 부여된 권한도 같이 제거를 해주도록 한다.

예를 들어 "test" 라는 폴더를 생성하고 "testsvr" 라는 계정을 추가해보자.

testsvr 계정 설정
(그림 4-1-47)

"testsvr" 라는 사용자가 퇴사를 하여 계정이 불필요하게 되어서 삭제를 하고 폴더에는 별다른 작업을 하지 않았다면 그 계정의 SID 는 그대로 남아있게 된다. S-1-5-21-xxx... 이 "testsvr" 계정의 실제 아이디 인 셈이다.

계정 삭제 시 등록정보에 보이는 화면
.(그림 4-1-48)



시스템 파티션의 경우는 Windows를 설치할 때 권한이 이미 부여되는데, 그중 Winnt 폴더의 경우 권한을 재설정시에는 신중을 기해 설정하도록 한다. 만약, 이미 설정된 권한을 제거한 후 [administrators] 와 [SYSTEM]에게만 권한을 부여할 경우 서비스에 장애가 나타날 수 도 있다.

C : 루트 상에서 권한을 수정한다고 해서 하부의 권한이 제거되지는 않는데, 이는 상속은 되지만, 각각의 폴더에서 다시 권한이 추가된 상태이기 때문이다. 특히, 데이터 폴더의 경우는 최소한의 권한만 주어야 한다.

상속된 권한의 경우는 수정이 불가능 하도록 바탕이 회색으로 나타나며, 권한이 새롭게 설정된 경우는 바탕이 흰색으로 나타난다.

※ 공유폴더의 사용자 권한과 NTFS 권한이 충돌이 일어날 경우 최소한의 권한으로 적용된다.

5. 각 서비스별 보안 관리

가. 윈도우즈 어플리케이션 서비스

[표 4-1-1]은 Windows 2000 SVR를 처음 설치시에 나타나는 서비스 목록이다. 각 서비스가 어떠한 작업을 하는지에 대해서 추가적으로 확인을 원할시 아래의 주소에서 확인을 할 수 있다.

※ 서비스 목록

http://www.microsoft.com/korea/technet/prodtechnol/windows2000serv/deploy/prodsp ecs/win2ksvc.asp

[표 4-1-1] 서버 형태별 서비스 시작유형

이 름	기 본	IIS	File 및 Print	Domain Controller
Alerter	자동			
Application Management	수동			
Automatic Updates	자동			
Background Intelligent Transfer Service	수동			
ClipBook	수동			
COM+ Event System	수동	자동		
Computer Browser	자동	수동	자동	자동
DHCP Client	자동	수동	수동	수동
Distributed File System	자동	수동	자동	자동
Distributed Link Tracking Client	자동	수동	자동	자동
Distributed Link Tracking Server	수동			
Distributed Transaction Coordinator	자동			
DNS Client	자동	수동		
Event Log	자동			
Fax Service	수동			
File Replication	수동			자동
FTP Publishing Service	자동		제거	제거
IIS Admin Service	자동		제거	제거
Indexing Service	자동			
Internet Connection Sharing	수동			
Intersite Messaging	사용 안함			
IPSEC Policy Agent	자동			
Kerberos Key Distribution Center	사용 안함			자동
License Logging Service	자동			
Logical Disk Manager	자동			
Logical Disk Manager Administrative Service	수동			
Messenger	자동	수동	수동	수동
Net Logon	수동			자동
NetMeeting Remote Desktop Sharing	수동			
Network Connections	수동			
Network DDE	수동			
Network DDE DSDM	수동			

이 름	기 본	IIS	File 및 Print	Domain Controller
NT LM Security Support Provider	수동	자동		
Performance Logs and Alerts	수동			
Plug and Play	자동			
Print Spooler	자동	수동	자동	수동
Protected Storage	자동			
QoS RSVP	수동			
Remote Access Auto Connection Manager	수동			
Remote Access Connection Manager	수동			
Remote Procedure Call (RPC)	자동			
Remote Procedure Call (RPC) Locator	수동	자동		
Remote Registry Service	자동	수동	수동	수동
Removable Storage	자동			
Routing and Remote Access	사용 안함			
RunAs Service	자동	수동	수동	수동
Security Accounts Manager	자동			
Server	자동			
Smart Card	수동			
Smart Card Helper	수동			
SMTP(Simple Mail Transport Protocol)	자동		제거	제거
System Event Notification	자동			
Task Scheduler	자동			
TCP/IP NetBIOS Helper Service	자동	수동		
Telephony	수동			
Telnet	수동			
Terminal Services	사용 안함			
Uninterruptible Power Supply	수동			
Utility Manager	수동			
Windows Manager	수동			
Windows Management Instrumentation	수동			
Windows Management Instrumentation Driver Extensions	수동			
Windows Time	수동			
Wireless Configuration	수동			
Workstation	자동			
World Wide Web Publishing Service	자동		제거	제거

위의 내용은 일반적인 상황에서의 서비스 시작 유형 일 뿐이다. 복합적으로 사용 할 경우는 대부분의 서비스를 테스트 해보면서 변경을 하여야 한다. 설정 후 서버를 재시작하여 이벤트 로그에 문제가 없는지 확인하면서 사용 안함으로 변경하는 것이 좋다.

SNMP 서비스를 구동하여 MRTG를 활용하면 유용한 네트워크 관리 프로그램이면서 보안 도구도 될 수가 있다. MRTG를 이용해서 서버의 트래픽을 점검 하면 불법적인 네트워크 사용을 어느 정도 파악해 낼 수 있을 것이다. 이렇게 MRTG를 이용하려고 한다면 SNMP 서비스를 사용해야 하는데 Windows2000에서는 SNMP가 설치 되면 community string이 기본값으로 public으로 설정이 된다. 이렇게 기본값인 public으로 설치가 된다면 시스템 정보가 유출 될 수가 있다. 아래는 그 결과값이다.

snmp 의 community string을 이용한 정보 스캔
(그림 4-1-49)

(그림 4-1-49)에서 확인 할 수 있는 것은 파란색 물음표 표시가 된 것은 네트워크가 안 된다거나 침입차단시스템이나 해당 SNMP에 서비스에 대해서 조치가 취해진 상태이다.

서비스를 클릭하게 되면 현재 이 서버에서 어떤 서비스가 실행이 되고 있는지 그리고 account를 클릭하게 되면 현재 이 서버에 설정된 계정이 모두 보이게 된다. 이것은 포트 스캔보다 한 단계 위의 개념으로 보아도 될 것이다. 또한 개별적인 것이 아니라 subnet으로 구분을 할 수 있기 때문에 광범위한 스캔도 가능하다. 따라서 SNMP를 서비스한다면 IP 대역을 엄격하게 제한하고, community 문자열을 추측하기 어려운 것으로 수정하여야 한다.

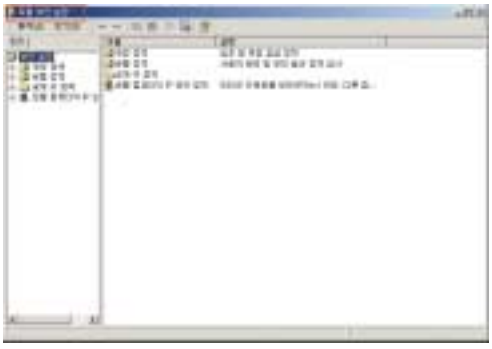
6. 그룹정책을 통한 보안 설정

가. 워크그룹 서버

[로컬 보안 정책]은 **[시작]** ⇨ **[프로그램]** ⇨ **[관리도구]**에서 확인할 수 있으며, 크게 4가지의 메뉴로 구성되어 있다.

- 계정정책 : 계정에 대해 암호의 길이나 복잡성, 로그온 실패 숫자 제한 등으로 계정을 잠기게 하여 더 이상의 비정상적인 접근을 차단할 수 있다.
- 로컬정책 : 서버에 접근을 하거나 접근하여 작업한 내용에 대해 감사로그를 남길 수 있으며, 접근권한이나 서버에 접근권한에 대해 여러 가지 방법으로 제한을 할 수 있다.
- 공개키 정책 : 데이터를 암호화 하고자 할 때 사용한다. 이 부분에서 사용하길 원할 경우는 인증서 서비스가 설치가 되어야 한다.
- 로컬 컴퓨터의 IP 보안정책 : 여기에서 IPSec을 설정할 수 있으며, 보안이 중요시 될 경우는 보안 서버 항목을 선택하여 서버의 모든 트래픽에 대해 보안을 설정할 수 있다. 단, 이렇게 설정하였을 때 보안이 되지 않은 패킷은 서버에서 거부를 하게 되므로 각별히 주의하도록 한다.

로컬 보안 설정
(그림 4-1-50)

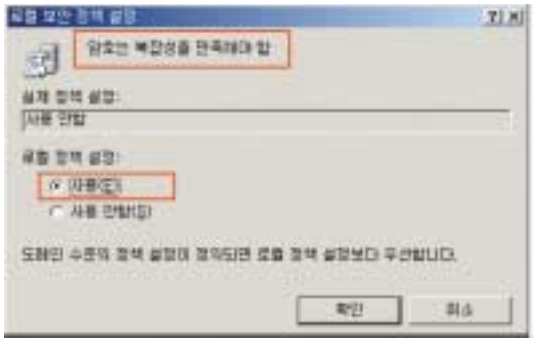


① 암호정책

복잡한 암호 설정과 암호 최소길이에 대해 설정하고자 한다.

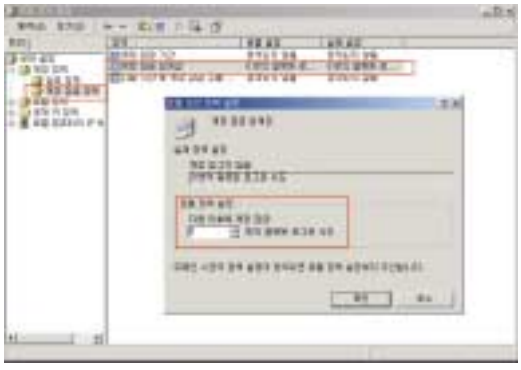
[암호는 복잡성을 만족해야 함]을 더블클릭 하여 **[사용함]**을 선택 후 저장하고, **[최소 암호 길이]**의 경우는 숫자형태로 길이를 지정하는 것이다.

암호 보안 정책
(그림 4-1-51)



② 계정 잠금 정책

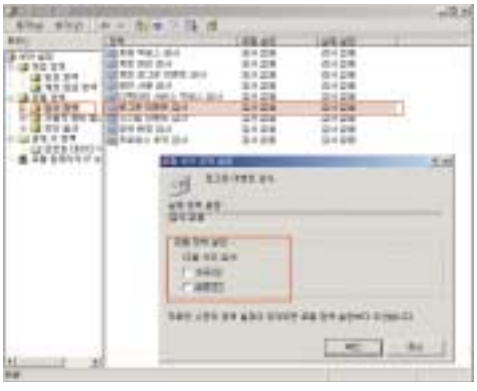
로그온 시도 실패 횟수를 지정하여 그 횟수를 초과하면 계정을 잠그도록 설정한다. **[계정 잠금 임계값]**을 열어 잘못된 로그온 시도 횟수를 지정한다.



계정 잠금 설정
(그림 4-1-52)

③ 감사 정책

계정이 액세스 하는 부분에 대해 감사를 할 수 있는 부분이며, 여기서는 **[로그온 이벤트 감사]** 중 실패했을 때만 체크를 하도록 한다. 설정이 저장되면 이벤트 로그의 **[보안]** 부분에 로그온 실패 로그가 남게 된다.

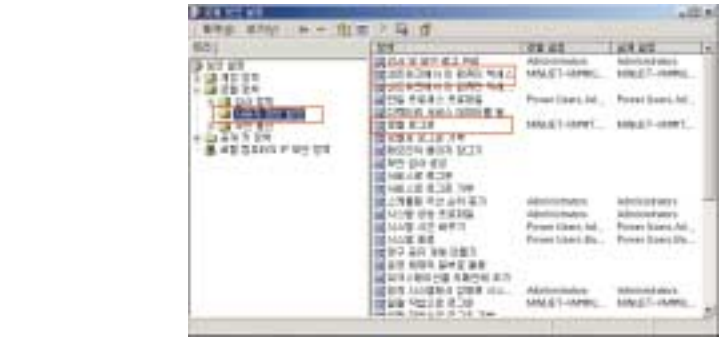


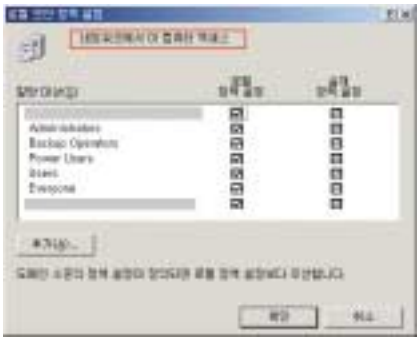
로그온 이벤트 감사
(그림 4-1-53)

④ 사용자 권한 할당

서버접근에 대해서 권한을 할당할 수 있다. 네트워크 및 서버컴퓨터에서 서버에 접근할 수 있는 사용자나 그룹에 대해 확인하고, 불필요한 계정은 삭제한다.

사용자 권한 할당
(그림 4-1-54)





⑤ 보안옵션

서버의 보안에 대한 추가적인 설정이 가능하다. 여기에서는 Administrator와 Guest의 계정이름 변경에 대해서 살펴보자. **[Administrator 계정 이름 바꾸기]**를 선택하여, 서버의 이름이나 기타 사내 정보와 관련이 없는 이름으로 변경한다.

Administrator 계정 이름 변경화면
(그림 4-1-55)

나. 도메인 컨트롤러

도메인 구조로 바뀌게 되면 최상위에 Domain Controller가 존재하고, 하부에 멤버 서버 및 사용자 컴퓨터 형태로 존재를 하게 된다. 만약 Domain Controller가 문제가 생길 경우는 모든 계정에 대한 인증처리가 되지 않아 사내 대부분의 시스템이 마비될 가능성이 높기 때문에 각별히 신경을 쓰도록 한다. 도메인 구조에서의 보안설정은 **[시작]** ⇨ **[프로그램]** ⇨ **[관리도구]**에서 **[도메인 보안 정책]** 과 **[도메인 컨트롤러 보안정책]**을 설정하여 변경한다.

도메인 컨트롤러 설정
(그림 4-1-56)

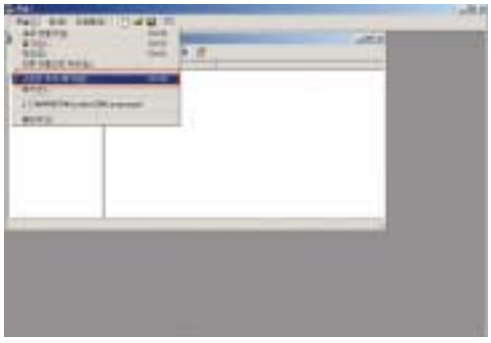
멤버 서버나 사용자 컴퓨터의 보안정책 설정시에는 **[도메인 보안 정책]**에서 설정하면 된다. 기본적인 정책은 비슷하게 진행을 하지만, 보안상 더 강력한 설정이 가능하다.

다. 보안템플릿

보안템플릿이란 마이크로소프트사에서 미리 서버의 보안정책을 구성해 놓은 자료이다. 수정도 가능하고 바로 적용도 가능하다.

템플릿을 확인하는 방법은 **[시작]** ⇨ **[실행]** ⇨ [mmc] ⇨ **콘솔창**에서 **[스냅인 추가/제거]** ⇨ **[추가]** ⇨**[보안템플릿]**을 선택하여 추가 ⇨ 각각의 템플릿을 확인 후 적합한 것을 선택하여 적용한다.

보안템플릿
(그림 4-1-57)



7. TCP/IP를 통한 보안설정

가. RRAS(Routing and Remote Access) 사용

RRAS의 경우 서버 설치시에는 기본적으로 사용안함으로 설정이 되어 있다. 그런 이유 때문인지 이 서비스에 대해서 많은 자료가 존재하지 않는데, 만약 설정을 잘 한다면, 비싼 침입차단시스템을 쓰지 않고도 비슷한 효과를 낼 수 있다. 그렇다고 침입차단시스템보다 좋다는 것은 아니다. 침입차단시스템이 있다면 당연히 사용을 하도록 하는 것이 좋을 것이다. 또한, VPN, NAT, 사내 라우터로도 사용이 가능하다.

아래는 RRAS의 설정 방법이다.

① **[시작]** ➪ **[프로그램]** ➪ **[관리도구]** ➪ **[라우팅 및 원격 액세스]** 순으로 선택한다.

RRAS 선택
(그림 4-1-58)

② 콘솔 창이 나타나면 서비스가 구성되지 않은 상태로 나타나는데, 서버 아이콘에 마우스 오른쪽 버튼을 클릭하여 **[라우팅 및 원격 액세스 설치 및 구성]**을 선택한다.

라우팅 및 원격 액세스 설치 및 구성
(그림 4-1-59)

③ **[네트워크 라우터]**를 선택한다.

네트워크 라우터 선택
(그림 4-1-60)

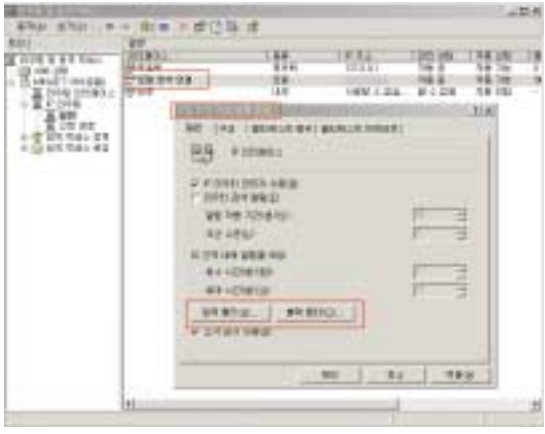
④ 프로토콜 선택창이 나타나는데, 일반적으로 TCP/IP를 사용하므로, 그대로 진행하도록 한다.

TCP/IP 사용
(그림 4-1-61)

⑤ 구성이 완료되면 **[IP 라우팅]** ⇨ **[일반]** 선택하면 메인창에 NIC(Network Interface Card) 리스트가 나타나며, 필터라는 부분이 **[사용안함]**으로 되어있는데, 이 부분에서 필터링이 설정가능하다.

RRAS 필터
(그림 4-1-62)

⑥ 설정을 원하는 NIC를 선택한 후, 입력필터와 출력필터를 설정한다.



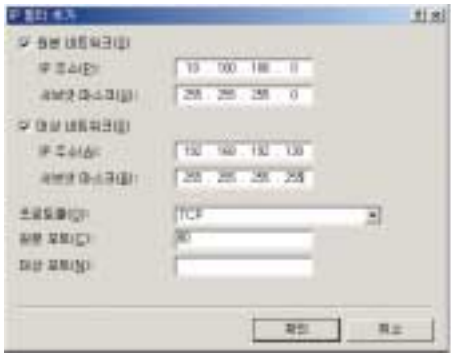
입력필터와 출력필터
(그림 4-1-63)

⑦ 입력필터를 설정하도록 하자. 위의 그림에서 입력필터를 클릭하면 추가버튼만이 나타날 것이다. (그림 4-1-64)는 먼저 설정을 한 것이다. 아래와 같이 설정을 하면 모두 닫겠다는 설정이 된다. 조건에 대한 부분은 보안 정책을 어떻게 가져갈 것인가에 따라 다르다. 두 번째의 조건은 강력하긴 하지만 설정이 복잡하고 일일이 확인을 해줘야 한다.

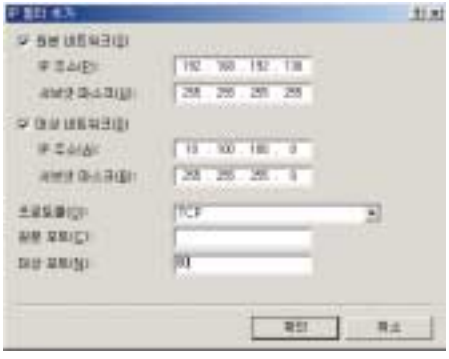
입력 필터
(그림 4-1-64)

⑧ 필터링 구성은 라우터의 필터링 구성과 유사하다. 아래 (그림 4-1-65)는 조건에 맞지 않는 모든 패킷 버리기를 설정하고, 로컬(192.168.192.130)에서 외부(10.100.100.0/24)에서의 80번 Port 접속하여 데이터를 가져오기를 원할 경우의 예이다.

인바운드 필터 설정
(그림 4-1-65)



아웃바운드 필터 설정
(그림 4-1-66)



※ 위 설정을 잘못 실행할 경우 서비스가 제대로 이뤄지지 않을 수 있으므로 각별히 신경을 써서 설정하기 바란다. 또한, 이 구성내용은 필터링 리스트를 제외한 나머지 정보는 다른 시스템에 이전이 되지 않는다. 따라서 대규모 보안 설정을 원할 경우는 IPSec을 사용하길 바란다.

나. TCP/IP 필터링 옵션을 이용

먼저 필터링을 구성하기 위해서는 컴퓨터 바탕화면에서 **[네트워크 환경]** 선택 ⇨ 마우스 오른쪽 버튼 클릭하여 **[등록정보]** 선택 ⇨ **[로컬영역연결]** 선택 ⇨ 마우스 오른쪽 버튼 클릭해 **[인터넷프로토콜(TCP/IP)]** 선택 ⇨ **[등록정보]** 클릭 ⇨ **[고급]** 클릭⇨ **[옵션]** 선택 ⇨ **[TCP/IP필터링]** 선택 ⇨ **[등록정보]** 클릭하여 TCP/IP 필터링 설정화면으로 넘어간다.

TCP/IP 필터링 설정 사용화면
(그림 4-1-67)

기본 설정은 TCP/IP 필터링 사용(모든 어댑터) 확인란에 체크가 되어 있지 않아 필터링 정책이 설정되어 있지 않다. 이 설정은 외부에서 사용자 컴퓨터로의 접근을 할 수 있도록 구성하는 부분이다.

※ 세 번째 항목인 IP프로토콜은 모두 허용으로 설정해두고 변경하지 않는다. TCP/UDP 의 포트 번호는 1 ~ 65535 번까지 존재하며, 1 ~ 1024 국제적 표준으로(well-known port) 정해져 있다.

일반사용자가 유해 트래픽을 차단하려고 한다면

- TCP/IP 필터링 사용 (모든 어댑터)] 부분을 체크하고
- [TCP 포트 부분에서 다음만 허용]을 선택한 후 포트를 추가하지 않고
- [UDP 포트에서 모두허용]을 선택하면 된다.

※ 설정이 끝난 후 시스템을 재부팅 하여야 필터링 설정이 적용된다. 참고로 Windows에서 주로 사용하는 서비스 포트 정보는 winnt\system32\drivers\etc\services 파일에 등록되어 있다.

단순히 차단하는 게 좋다고 해서 허용을 하지 않을 경우, 기존에 사용하는 기능들에 문제가 발생할 수 있으므로 서비스별 포트정보를 확인한 후 작업하도록 한다.

지금까지의 설명은 TCP 포트만 설명하였지만, UDP 포트나 IP 프로토콜 부분도 사용 중인 서비스를 제외한 후 포트를 차단하는 방식이다.

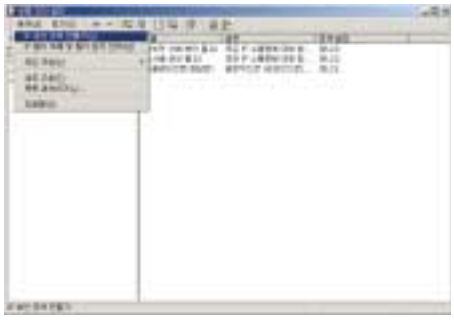
TCP/IP 필터링
(그림 4-1-68)

다. IPSEC(Internet Protocol Security Protocol) 기능을 이용한 필터링

Windows 2000에는 IPSEC 기능을 자체적으로 내장하고 있다. IPSEC은 보안 통신을 위해서 여러 가지 기능을 제공하지만 여기에서는 간단하게 인 바운드, 아웃바운드에 대한 필터링 부분만 설명하기로 한다.

IPSEC을 설정하려면 **[시작]** ⇨ **[제어판]** ⇨ **[관리도구]** ⇨ **[로컬보안정책] 더블클릭** ⇨ **[로컬 컴퓨터의 IP 보안정책]** 선택한다. 아래 그림은 Windows 2000에서 공유와 관련된 포트인 TCP/139, TCP/445 관련 포트를 막는 예를 보여준다.

① **[동작]** 메뉴에서 **[IP 보안정책 만들기]**를 선택한다.



IP 보안 설정 만들기
(그림 4-1-69)

보안정책 마법사
(그림 4-1-70)

② 필터링 규칙 이름을 임의로 정한다. 기본응답 규칙 활성화 체크를 제거한다.

IP보안정책 이름
(그림 4-1-71)

IP보안정책 마법사
(그림 4-1-72)

③ 등록정보 편집이 체크되어 있는 상태에서 **[마침]**을 누르면 필터링 세부 규칙을 설정할 수 있는 **[공유접근막기 등록정보]** 창이 뜬다.

공유접근 막기 등록정보
(그림 4-1-73)

④ PC에서 기본적으로 필터링 규칙만 사용할 것이므로 **[추가마법사 사용]**체크를 지운 후 **[추가]** 버튼을 클릭 한다. 첫 번째 **[IP 필터 목록]**에서 **[추가]**를 클릭 한다.

공유접근막기 등록정보
(그림 4-1-74)

IP규칙등록정보
(그림 4-1-75)

⑤ 이름 칸에 "**139/445 포트막기**" 등 임의의 이름을 넣고 **[추가]**를 클릭 하여 필터 마법사를 시작한다.

IP필터 마법사
(그림 4-1-76)

⑥ 여기서부터 제일 중요한 부분으로 외부로부터 내부로 들어오는 모든 TCP 139/445번을 막고자 하므로 원본 주소란에는 **[모든 IP 주소]**를 선택하고 그리고 대상 주소는 **[내 IP 주소]**를 선택한다.

필터 마법사 실행 화면
(그림 4-1-77)

⑦ IP 프로토콜은 TCP를 선택한 후 **[다음]** 버튼을 누른 후 외부 쪽의 소스포트는 임의적 바뀌므로 **[모든 포트에서]**를 선택하고 내 시스템으로는 139번 포트로 접속하므로 139번을 적어놓고 **[다음]** 버튼을 누른다.

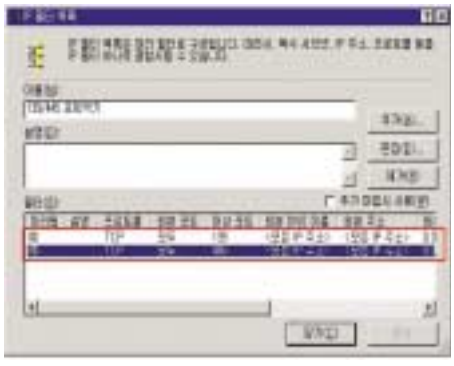
필터 마법사
(그림 4-1-78)

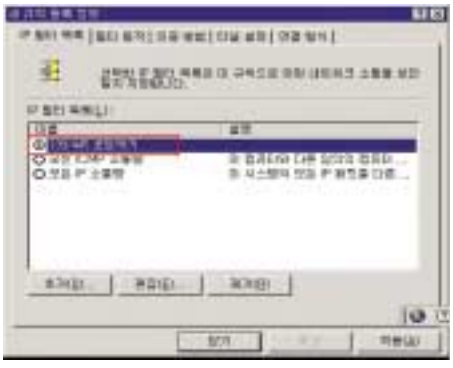
⑧ 화면에서 **[속성편집]**을 체크되지 않도록 한 후 **[마침]**버튼을 누르면, 이로써 하나의 필터링 규칙이 정해졌고 목록에 하나가 정의 되어 있는 것을 볼 수 있다.

IP 필터 목록 확인
(그림 4-1-79)

⑨ ⑤번에서 ⑧번까지 반복하면 필터링을 원하는 모든 프로토콜과 포트를 정의할 수 있다. TCP 445번을 필터링 하는 항목도 만든 후 닫기를 클릭하면 새로운 목록이 만들어진다.

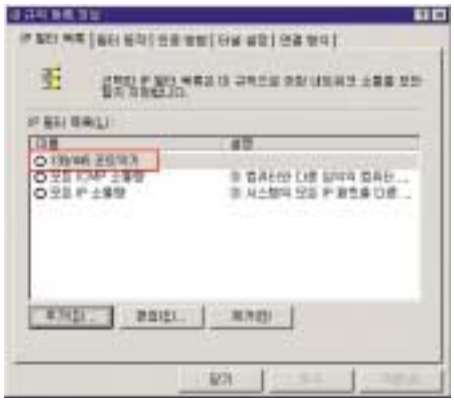
TCP/445 필터 추가 등록 정보
(그림 4-1-80)



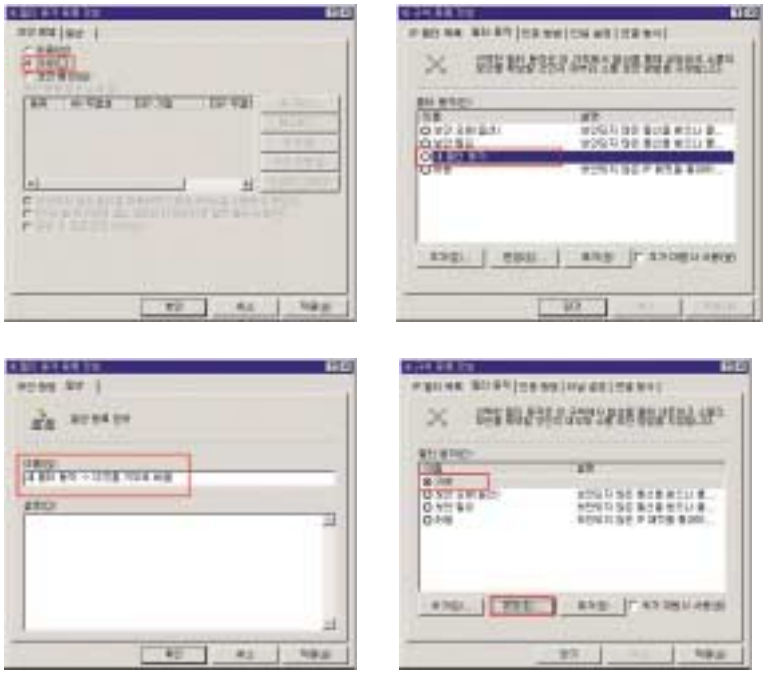


⑩ 이제는 정의된 필터 목록의 동작을 정의해 주어야 하므로 새롭게 만든 필터 목록을 선택한 후 두 번째 탭인 **[필터동작]**부분을 선택하고 **[추가]**를 클릭 한다.

필터 목록의 동작 정의
(그림 4-1-81)



⑪ 139/445번 포트로 접근하는 것을 막기 위해서는 "**새 필터 동작**"을 생성해야한다. **[추가 마법사 사용]**은 체크하지 않게 한 후 생성은 **[추가]** 버튼을 클릭 하여 거부를 선택하고 확인을 누른다. 이제 새로운 필터 동작이 생성되었다. 등록해 놓은 필터 동작은 다음에도 계속 사용할 수 있으므로 필터 동작을 알기 쉽게 정의해 놓자. **[새 필터 동작]**을 선택한 후 **[편집]**을 눌러 일반 탭에 있는 이름부분의 **[새 필터 동작]**을 **[거부]**로 변경한다.



필터 동작 편집
(그림 4-1-82)

⑫ **[적용]**을 누르면 **[닫기]** 버튼이 **[확인]**으로 바뀐다. **[확인]**을 누르고 **[닫기]** 버튼을 누르면 **[공유접근 막기]**라는 새로운 정책이 만들어졌다. 지금까지 해오면서 기타 옵션 및 세부설정이 많이 있으나 개인이 사용하기에는 위의 과정만 따라한다면 간단하게 필터링 부분은 쉽게 설정할 수 있다. 위의 설명 이외에 부가적인 기능 및 정보를 얻고 싶다면 아래의 링크에서 IPSEC에 관한 정보를 찾아볼 수 있다 .

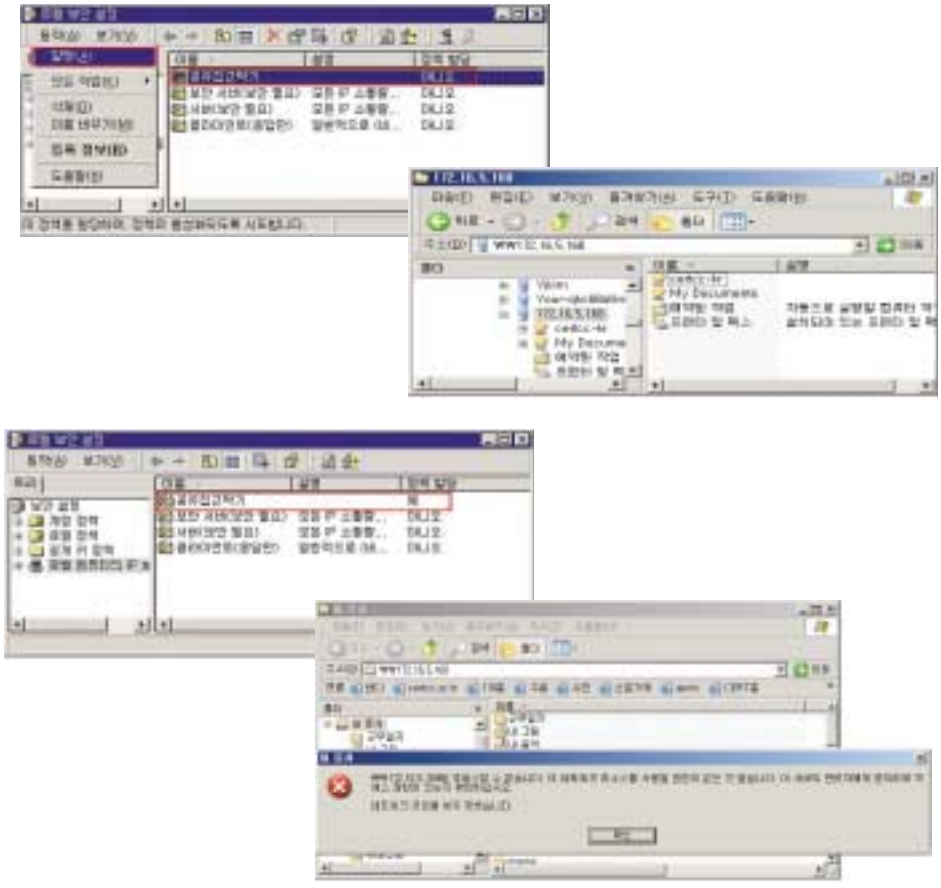
http://support.microsoft.com/search/default.asp

공유접근 차단 정책
(그림 4-1-83)

⑬ **[로컬보안정책]** ⇨ **[동작]** 메뉴에서 **[할당]**을 선택하면 정책이 활성화되고 다시 설정을 해지하려면 할당된 정책을 선택한 후 **[해제]**를 선택하면 된다.

마지막으로 만들어진 정책을 할당하고 테스트 해 보면 된다. 위쪽에서 정책을 할당하기 전에는 공유 폴더로 접근이 가능했지만 아래쪽에는 정책을 할당한 후 공유 폴더 접근이 불가능함을 확인할 수 있다.

공유 접근 불가 예
(그림 4-1-84)



제2절 유닉스/리눅스 서버

1. 운영체제 보안

시스템 설치 후 본격적인 서비스를 제공하기 전에 기본적으로 취해야 하는 필수 보안 설정법에 대해 알아보자.

가. 사용하지 않는 서비스 중지

시스템 설치 후 가장 먼저 하여야 할 일은 사용하지 않는 서비스에 대한 중지이다. 일반적으로 필요한 패키지만 설치하지만 설치자에 따라서는 모든 패키지를 설치하는 경우도 적지 않고, 설사 꼭 필요한 패키지만 선택하여 설치했다 하더라도 기본적으로 불필요한 서비스가 제공되는 경우가 많으므로 불필요한 서비스를 찾아 중지하도록 한다.

(1) 보안상 취약한 서비스

원격에서 데몬의 취약성을 악용하여 루트(root) 권한을 획득할 수 있는 imapd, sadmind, rpc.cmsd, rpc.ttdbserverd와 같은 서비스나 rsh, rlogin, rexec 등과 같은 'r' 기반의 명령어들이 굳이 필요하지 않다면 반드시 제거하도록 한다.

(2) inetd, xinetd에서 서비스 관리

슈퍼 서버 데몬이라 불리는 Inetd나 Xinetd의 경우 설정파일에서 서비스 여부를 관리할 수 있는데, 레드햇 리눅스 6.x까지 사용되었던 Inetd의 설정 파일인 /etc/inetd.conf 파일에는 기본적으로 여러 다양한 서비스들이 설정되어 있으나 대부분 telnet 이나 pop3 정도만을 사용할 것이다. 기타 imapd, rsh와 같은 사용하지 않는 서비스들은 주석(#) 처리하여 서비스를 제거하면 된다.

① 일반 사용자는 설정 파일을 쓰거나 읽을 필요가 없으므로 오직 root만이 읽기/쓰기가 가능하도

록 퍼미션(permission)을 변경한다.

```
# chmod 600 /etc/inetd.conf
```

② /etc/inetd.conf 파일을 아래와 같이 주석 처리 및 편집한다. 만약, ftp를 inetd로 작동하지 않고, 독립실행형(standalone) 모드로 서비스할 때는 inetd.conf에서 주석 처리하도록 한다.

```
# vi /etc/inetd.conf

ftp    stream  tcp   nowait  root  /usr/sbin/tcpd  in.ftpd  -l -L -i -o
telnet  stream  tcp    nowait    root  /usr/sbin/tcpd   in.telnetd
#gopher  stream  tcp   nowait    root   /usr/sbin/tcpd   gn
#smtp  stream   tcp   nowait    root   /usr/bin/smtpd   smtpd
#nntp   stream   tcp   nowait   root   /usr/sbin/tcpd   in.nntpd
```

③ inetd 데몬을 다시 띄워준다.

```
#killall -HUP inetd 또는 /etc/rc.d/init.d/inetd restart
```

④ ext2 나 ext3 파일 시스템을 사용할 경우에는 설정 파일에 읽기 전용(read only) 속성을 주어 설사 root라 하더라도 바로 변경이나 삭제를 할 수 없도록 설정할 경우 자동화된 프로그램에 의한 공격이나 변경 시도 등을 차단할 수 있는데, 이는 “change attribute”의 의미인 chattr 명령어에 적당한 옵션을 지정하여 이용하면 된다. /etc/inetd.conf 파일에 +i 속성변경 설정을 하는 것으로 만약 해제를 하려면 +i 대신 -i를 실행하면 된다. 참고로 파일의 속성은 lsattr 을 실행하면 된다.

```
#chattr +i /etc/inetd.conf
```

⑤ xinetd 는 inetd 에 대한 eXtended 즉, 확장된 기능을 제공하는 것으로 주 설정 파일인 /etc/xinetd.conf 및 설정 파일 디렉토리인 /etc/xinetd.d에 있는 각 서비스별 파일에서 제어할 수 있다. 각각의 서비스에 대해 /etc/xinetd.conf 에서 직접 설정하거나 제어하고자 하는 서비스명 파일을 열어 주석처리 및 편집하면 된다.

```
# cd xinetd.d
# ls
chargen      echo      imaps  pop3s   rsync    talk      vsftpd
chargen-udp  echo-udp  ipop2  rexec   servers  telnet
daytime      finger    ipop3  rlogin  services time
daytime-udp  imap      ntalk  rsh     sgi_fam  time-udp
```

서비스명으로 된 파일을 삭제하거나 각 서비스에서 disable = yes 로 설정하면 해당 서비스가 실행되지 않는다.

```
# vi telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

⑥ xinetd데몬을 재시작한다.

```
# /etc/rc.d/init.d/xinetd restart 또는 killall -HUP xinetd
```

다. 불필요한 데몬 관리

inetd나 xinetd 등 슈퍼서버 데몬 이외 독립실행형(standalone) 형태로 작동 하는 서비스에 대한 제어는 다음과 같이 설정할 수 있다.

(1) ntsysv 실행

터미널 상에서 직접 ntsysv를 실행하거나 setup을 실행 후 "System services"를 선택하면 된다. 여기에서 부팅시 자동으로 시작되기를 원하는 서비스를 선택한 후 OK를 클릭하면 된다. [*] 로 표시되면 부팅시 자동으로 실행되는 서비스이고 비어 있으면 부팅시 실행되지 않는다.

ntsysv 실행 화면
(그림 4-2-1)

(2) 불필요한 서비스 제거

/etc/rc.d/rc3.d 디렉토리로 이동하여 ls -la S* 명령을 실행하여 S 로 시작되는 서비스명을 직접 확인해도 된다. 따라서 S로 되어 있는 서비스를 해제하려면 K로, K로 되어 있는 서비스를 가동하려고 하면 S로 mv를 이용하여 변경해 주면 된다. 참고로 여기에서 rc3.d의 3은 Full multiuser mode로서 일반적으로 서버로 이용시 사용되는 런레벨(runlevel)이며, S는 start로서 부팅시 작동할 서비스, K는 kill 의 의미로 작동하지 않을 서비스를 뜻한다.

대표적으로 보안상 제거하도록 권고되는 서비스는 다음과 같다.

[표 4-1-2] 살펴보아야 할 서비스

서 비 스	서비스 내용
S45pcmcia	노트북에서만 필요하므로 삭제한다.
S50snmpd	원격의 이용자가 트래픽 등 시스템에 대한 정보를 필요로 할 때 필요한데, 사용한다면 snmp community string을 엄격하게 설정하고 사용하지 않는다면 삭제한다.
S55named	DNS 서비스를 제공하지 않는다면 삭제 한다
S55routed	라우터가 아닌 이상 일반 서버에서는 삭제한다.
S60lpd	프린트 서버가 아닌 이상 반드시 삭제한다.
S60mars-nwe	Netware 에서 쓰는 file이나 printer server 이므로 삭제한다.
S60nfs	NFS server 에서 필요하므로 nfs를 서비스하지 않는다면 삭제한다.
S72amd	AutoMount daemon으로 원격지의 File system 을 mount 할 때 필요하다. amd 는 전통적으로 치명적인 보안 취약성이 있으므로 삭제한다.
S75gated	routed 처럼 라우터가 아닌 이상 삭제한다.
S80sendmail	메일 서비스를 이용한다면 필요하지만 메일 서비스가 필요없다면 삭제한다.
S85httpd	Apache 웹 서버이다. 웹 서비스를 제공한다면 삭제하지 않는다.
S05apmd	laptop에서 전원관리를 위해 필요하므로 서버에서는 필요없다.
S10xntpd	Network time protocol이다. 사용할 경우가 없으므로 필요없다.
S11portmap	NIS 나 NFS 서비스 이용시 R 서비스에 대한 port를 mapping 시켜주는 서비스이므로 보안상 문제가 많다. 일반적으로 NFS를 사용하지 않는다면 필요 없으니 삭제한다.
S15sound	서버에서 Sound 를 서비스 하지 않으므로 필요없다.
S15netfs	nfs client 가 nfs server를 마운트 할 때 필요하므로 NFS를 사용하지 않는다면 삭제한다.
S20rstatd, S20rusersd S20rwhod, S20rwalld	R 로 시작하는 서비스는 Remote 에서 실행하는 것이므로 반드시 서비스를 하지 않도록 하여야 한다.
S20bootparamd	하드나 플로피등 부팅 수단이 없을 때 이용하는 것으로 반드시 서비스하지 않아야 한다.
S25squid	squid 프록시 서버를 가동하는 설정이므로 squid를 사용하지 않는다면 삭제한다.
S34yppasswdd	NIS server 에서 필요하므로 사용하지 않는다면 삭제한다.
S35ypserv	NIS 에서 필요한 설정이므로 사용하지 않는다면 삭제한다.
S35dhcpd	dhcp(IP 동적할당 서비스)에서 필요하므로 일반 서버에서는 필요없다.
S40atd	cron 과 같은 서비스인데, 일반적으로 cron 서비스를 이용하므로 보안상 취약한 atd 는 삭제한다.
S87ypbind	NIS 를 쓸 때 필요한데, 사용하지 않는다면 삭제한다.
S90xfs	X font server 로 서버에서는 X-Windows 서비스를 하지 않으므로 삭제한다.
S95innd	News server 로 News 서비스를 하지 않으므로 삭제한다.
S99linuxconf	원격지에서 브라우저를 통해 Linux 시스템의 설정을 변경할 수 있는 것으로 보안상 취약성을 가지고 있으므로 반드시 삭제하여야 한다.

2. SUID/SGID 파일 관리

전통적으로 suid/sgid가 설정된 파일에서 보안 취약성이 많이 발견되었다. 따라서 수시로 현 시스템내 suid/sgid가 설정된 파일을 모니터링 하여 suid 나 sgid가 불필요한 파일이라면 파일 자체를 삭제 하거나 s비트를 해제하는 것이 좋다.

가. SUID/SGID 파일의 개념 및 중요성

suid나 sgid는 일반적인 퍼미션의 예외사항이라고 생각하면 된다. 즉, suid나 sgid가 설정된 파일을 실행할 경우에는 실행 사용자의 권한으로 작동하는 것이 아니라 s비트가 설정된 파일의 소유자 권한으로 작동하는 것이다.
대표적인 예가 암호 변경시 사용되는 passwd인데, 일반 사용자가 이 파일을 실행할 경우 임시로 root 권한을 할당받아 root 소유로 암호를 변경하게 되는 것이다. 일반 사용자가 suid/sgid가 설정된 파일을 실행시에는 해당 사용자 또는 그룹 권한으로 작동하게 되므로 suid/sgid는 보안적인 관점에서 매우 중요한 역할을 한다.

나. SUID/SGID 파일의 검색 및 해제

전통적으로 root 권한의 suid/sgid가 설정된 파일에서 보안 취약성이 많이 발견된 것이 사실이다. 따라서 수시로 현 시스템에서 suid/sgid가 설정된 파일을 모니터링 하여 suid나 sgid가 불필요한 파일이라면 파일 자체를 삭제 하거나 s비트를 해제하는 것이 좋다.

```
# find / -type f \( -perm -04000 -o -perm -02000 \)
```

먼저 위의 명령어를 실행하여 전체 시스템 내(/)에서 suid(4000)나 sgid(2000)가 설정된 파일을 검색하도록 한다. 배포판이나 버전에 따라 결과는 조금씩 다를 수는 있지만 일반적으로 다음과 같은 결과가 보일 것이다.

아래의 파일들은 가능하다면 s비트를 해제할 것을 권장한다.

```
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/wall
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/write
/usr/bin/at
/usr/sbin/usernetctl
/usr/sbin/userhelper
/bin/mount
/bin/umount
/usr/sbin/lockdev
/bin/ping
/usr/sbin/traceroute
```

suid가 설정된 파일에서 s비트를 해제하는 명령어는 아래와 같다.

```
# chmod u-s /usr/sbin/suid_file
```

위는 user에 설정된 s비트를 해제(-)하는 명령어이고, 만약 s비트를 설정하려면 -s 대신 “chmod u+s” 를 실행하면 된다.

같은 방법으로 sgid가 설정된 파일에서 s비트를 해제하는 명령어는 아래와 같다.

```
# chmod g-s /usr/sbin/sgid_file
```

또는 chmod 0700, 0755 와 같이 해 주어도 된다.

3. 커널 파라미터 조작으로 시스템 보안 강화

리눅스에서 제공하는 커널(kernel) 파라미터를 조작함으로써 기본적인 DoS 공격을 차단하거나 커널 수준에서의 보안을 강화할 수 있는데, 시스템 운영시 권장할만한 보안 설정법을 알아보도록 하자.

가. 커널 튜닝의 필요성 및 편의성

리눅스에서 제공하는 /proc 파일시스템은 마치 Windows의 레지스트리(registry)처럼 시스템을 재부팅하지 않고도 OS 커널의 상세한 부분을 수정, 변경할 수 있도록 제공하고 있다.
설정값은 /proc/sys/디렉토리 이하의 디렉토리 및 파일에 대해 cat 과 echo를 이용하여 조회, 설정할 수 있는데, 사용방법은 다음과 같다.

- 현재 변수값 조회

  cat /proc/sys/변수값

- 현재 변수값 수정

  echo xx 〉 /proc/sys/변수값

최근에는 전용 유틸리티인 sysctl을 이용하여 조회 또는 설정할 수 있는데, sysctl 설정 파일은 /etc/sysctl.conf이다. sysctl에서는 /proc/sys 디렉토리 이하에 있는 변수를 변경할 수 있는데, 디렉토리(/)는 sysctl에서 마침표(.) 로 변경된다.
현재의 모든 변수 설정은 sysctl -a 로 확인 가능하며 특정한 변수를 질의하려면 sysctl -n을 쓰면 되고, 변수를 특정한 값으로 설정하려면 sysctl -w 을 사용하면 된다. 아래의 예를 살펴보자.

```
# cat  /proc/sys/net/ipv4/tcp_syncookies
0
```

위에서 tcp_synncokies 변수가 0 이므로 off 즉, 사용되지 않는다는 의미인데, 아래와 같이 echo 로 설정 후 확인해 보면 1 로 변경된 것을 알 수 있다.

```
# echo 1 〉 /proc/sys/net/ipv4/tcp_syncookies
# cat  /proc/sys/net/ipv4/tcp_syncookies
1
```

이를 sysctl로 사용할 경우 아래와 같이 사용하면 동일한 결과이다.

```
# sysctl -n net.ipv4.tcp_syncookies
0
# sysctl -w net.ipv4.tcp_syncookies=1
# sysctl -n net.ipv4.tcp_syncookies
1
```

나. 각종 권장 커널 튜닝 파라미터

이외 보안과 관련된 몇 가지 다른 커널 파라미터를 알아보도록 하자. 아래의 사항은 권장 사항이므로 어떠한 시스템이든 설정할 것을 권장한다.

```
echo “0” 〉 /proc/sys/net/ipv4/tcp_timestamps
# timestamps 기능은 불필요하므로 사용하지 않는다.

echo “1” 〉 /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
# smurf 공격에 악용될 수 있으므로 broadcast 주소를 통한 icmp echo 에 대해 응답하지 않는다.

echo “0” 〉 /proc/sys/net/ipv4/conf/all/accept_source_route
# 스푸핑을 막기 위해 source route 패킷을 허용하지 않는다.
# 소스 라우팅을 허용할 경우 악의적인 공격자가 IP 소스 라우팅을 사용해서 목적지의 경로를 지정할 수도 있고,
원래 위치로 돌아오는 경로도 지정할 수 있다. 이러한 소스 라우팅이 가능한 것을 이용해  공격자가 마치 신뢰받
는 호스트나 클라이언트인 것처럼 위장할 수 있는 것이다.

echo “0” 〉/proc/sys/net/ipv4/ip_forward
# 해당 시스템을 통해 다른 시스템으로 패킷이 포워딩 되지 않도록 한다. 만약 시스템이 라우터 등 게이트웨이
용도로 사용할 것이 아니라면 끄는 것이 좋다.
```

```
echo "0" 〉 /proc/sys/net/ipv4/conf/all/accept_redirects
# icmp redirects 를 허용하지 않는다.
# 만약 ICMP Redirect 를 허용할 경우에는 공격자가 임의의 라우팅 테이블을 변경할 수 있게 되어 자신이 의도하지 않는 경로, 즉 공격자가 의도한 경로로 트래픽이 전달될 수 있는 위험이 있다.

echo "1" 〉 /proc/sys/net/ipv4/conf/all/log_martians
# 스푸핑된 패킷이나 소스라우팅,  Redirect 패킷에 대해 로그파일에 정보를 남긴다.
echo "1" 〉 /proc/sys/net/ipv4/tcp_syncookies
# syn flooding 공격에 대응하기 위해 syncookies 기능을 켠다. syn flooding 공격에 매우 효과적이다.

echo "1024" 〉 /proc/sys/net
/ipv4/tcp_max_syn_backlog
# 역시 syn flooding 공격과 관련된 설정인데, backlog queue의 사이즈를 늘려 공격에 대응하도록 한다.

위의 모든 설정은 재부팅 후에 원래의 값으로 다시 초기화되므로 /etc/rc.d/rc.local 에 두어 부팅시마다 실행하도록 하여야 한다.
```

4. 사용자 계정 및 암호 관리

처음 시스템을 설치하면 설치된 패키지가 많으면 많을수록 불필요한 계정들이 많이 설치되어 있다. 또한 암호가 계정명과 동일하거나 쉬운 암호로 설정되어 있는 경우도 있는데, 불필요한 계정은 삭제하고, 쉬운 암호를 사용 중인 계정은 확인 후 추측이 어려운 암호로 변경하도록 하는 것이 좋다.

가. 불필요한 계정 정리

시스템에서 사용하지 않는 사용자 계정은 삭제하거나 사용하지 못하도록 설정하는 것이 좋은데, 초기 설치 이후 추가로 패키지를 설치하였을 경우 자신도 모르게 새로운 계정이 추가되는 경우가 있으므로 수시로 점검하여야 한다. 특정 계정을 사용할 수 없도록 하려면 /etc/passwd 나 /etc/group 파일에서 주석 처리를 하거나 아예 삭제하는 방법도 있다.

불필요한 계정(user)을 삭제하려면 userdel 로 삭제한다.

```
# userdel adm; userdel lp; userdel shutdown; userdel halt; userdel news;  userdel operator; userdel
games; userdel gopher; userdel ftp
```

여기에서 특히 ftp를 삭제시 anonymous ftp를 차단하는 효과도 있다.
불필요한 계정 외 불필요한 group도 삭제하는 것이 좋은데, 이는 groupdel 명령어로 삭제한다.

```
# groupdel adm;  groupdel lp; groupdel news; groupdel games;
```

나. John the Ripper를 활용한 쉬운 암호 검색

이외 또 하나 문제가 될 수 있는 것은 암호가 없는 계정은 물론이고, 쉬운 암호를 사용하는 계정이다. 아이디와 동일한 암호를 사용하거나 1111 등 추측하기 쉬운 암호는 정기적으로 관리하여야 한다. 이를 위해서 "John the Ripper" 프로그램을 이용하여 쉬운 암호를 사용하는 아이디를 검색해 보도록 하자.

아래의 John the ripper 홈페이지에 접속하여 소스파일을 다운로드 하여 컴파일하여 설치하면 된다.

http://www.openwall.com/john/

```
[root@www root]# tar zxvfp john-1.6.tar.gz        // 압축해제
[root@www root]# cd john-1.6/src      // john-1.6/src 디렉토리로 이동
[root@www src]# make linux-x86-any-elf         // 컴파일
[root@www src]# cd ../run/                  // run 디렉토리로 이동
[root@www run]# ./unshadow /etc/passwd /etc/shadow 〉 passwd.1
              // 암호화된 암호가 저장된 passwd.1 파일 생성
[root@www run]# ./john passwd.1            // 암호해독 시작
olympia       (olympia)
```

```
allmall         (allmall)
lee             (lee)
v3              (v3)
1234            (gaucho)
111             (weblog)
```

여기에서 오른쪽의 괄호 안에 있는 것이 계정 이름이고 왼쪽이 해당하는 계정의 암호인데, 보는 바와 같이 아이디와 암호를 동일하게 사용하거나 추측하기 쉬운 암호를 사용하는 계정이 적지 않다는 것을 알 수 있다. 위의 결과는 john.pot 파일에 암호화되어 저장되는데, 새롭게 확인하려면 이 파일을 삭제 후 다시 실행하면 된다.

c o n t e n t s

제 5 장
응용 서버 관리

제1절 Apache 웹서버

유닉스/리눅스 계열에서 가장 많이 사용되고 있는 Apache 웹서버의 보안 설정 방법에 대해 알아보자.

SANS(http://www.sans.org/) 에서 발표된 취약성 TOP20 (http://www.sans.org/ top20/)에 의하면 Apache 웹서버는 전통적으로 수위를 차지하고 있는데, 웹서버 자체의 취약성 뿐만 아니라 특히 최근에는 웹서버 설정상의 취약성을 이용하거나 침입차단시스템에서 웹 서비스가 열려 있는 것을 이용하여 해킹을 하는 사례가 증가하고 있어 웹서버에서의 보안이 더욱 중요해 지고 있다.

1. 웹서버 프로세스를 위한 계정

Apache와 관련된 사용자 계정은 크게 두 가지가 있다.

- Apache 서버가 설치 및 구동을 위한 계정 - 운영체제에 로그인하여 Apache를 설치하고, 웹서버를 시작/종료 시키는 계정
  ※ 웹 서비스를 위한 포트로 1024번 미만 포트번호(80번 포함)를 사용하기 위해서는 이 계정이 root이어야 한다.

- 웹서버 프로세스를 위한 계정 - 웹서버 데몬이 시작된 후 일반사용자의 웹 접속을 처리하기 하기 위하여 생성되는 프로세스가 사용하는 계정

"웹서버 프로세스 계정"의 경우 반드시 로그인할 수 없는 계정 즉, 쉘(shell)이 없는 계정으로 설정하여야 한다. 일반적으로는 사용자 ID와 그룹으로 쉘이 없는 "nobody" 계정을 사용한다. 아래 그림처럼 /etc/passwd파일과 /etc/shadow파일의 nobody 계정에 대하여 맨 마지막에 /bin/sh, /bin/csh등 shell을 명시하는 부분이 제외되어 있음을 확인 할 수 있다.

```
〈/etc/passwd〉
nobody:x:99:99:Nobody:/:

〈/etc/shadow〉
nobody:*:11900:0:99999:7:::
```

또한, 이러한 계정(쉘이 없는 계정, 아래 예에서는 "nobody")이 실제 웹 서비스에 적용되려면 Apache 설정파일(httpd.conf)에서 "User", "Group" 지시자(directive)가 아래와 같이 설정되어야 한다.

```
User nobody
Group nobody
```

2. 웹서버 DocumentRoot의 설정

웹서버 DocumentRoot는 모든 웹 컨텐트가 저장될 디렉토리 구조이며 이 디렉토리에 위치된 컨텐츠는 웹을 통하여 공개된다. 따라서 가능하면 이 디렉토리는 시스템의 루트 파일시스템 등과는 별도의 파일시스템을 사용해야 한다.

Apache 기본 설치시에는 htdocs 디렉토리를 DocumentRoot로 사용하고 있는데 이를 바꾸도록 한다. htdocs 디렉토리에는 공개될 필요가 없거나 공격에 악용될 수 있는 시스템 관련 정보가 담긴 파일이 기본적으로 설치 될 수 있다.

"/usr/local/www"를 DocumentRoot로 지정하고자 할 경우 httpd.conf 파일에서 다음과 같이 할 수 있다.

```
#DocumentRoot "/usr/local/apache/htdocs"
DocumentRoot "/usr/local/www"
```

웹서버 데몬은 chroot를 통해 설치하는 것을 권고한다. 만약 웹서버 데몬이 공격당했다고 하더라도 공격자는 chroot 디렉토리로 정해놓은 디렉토리 이외로는 접근할 수 없어 피해를 최소화할 수 있다.

3. 불필요한 CGI 스크립트 제거

Apache 배포판에는 불필요한 CGI 스크립트들이 포함되어 있어 공격에 이용될 수 있다. Apache 설치시 기본적으로 cgi-bin 디렉토리에 설치되는 모든 CGI 스크립트들은 제거하는 것이 안전하다.

4. Apache 환경파일(httpd.conf)의 설정

- 디렉토리 리스팅 방지
  - 웹 브라우저에서 사용자가 URL을 입력했을 경우, 웹 컨텐츠가 없을 경우 기본적으로 디렉토리 리스트를 보여주는 것을 방지해야 한다.
  - DocumentRoot 디렉토리 내의 모든 파일들이 리스팅되는 것을 방지하기 위해서는 환경설정화일(httpd.conf) "Options" 지시자에서 "Indexes" 옵션을 제거한다.

- 심블릭 링크의 사용 방지
  - 웹서버에서 심블릭 링크를 이용해서 기존의 웹 문서 이외의 파일시스템에 접근하는 것이 가능하나 심각한 보안 문제를 야기시킬 수 있다. 가령 시스템 자체의 root 디렉토리(/)를 링크 걸게 되면 웹서버 구동 사용자 권한(nobody)으로 모든 파일시스템의 파일에 접근할 수 있게 된다.(예를 들면 /etc/passwd을 공개하게 될 수도 있다.)
  - 이를 방지하기 위해서는 "Options" 지시자에서 심블릭 링크를 가능하게 하는 옵션인 "FollowSymLinks"를 제거함으로써 이를 막을 수 있다.

- SSI(Server Side Includes) 사용 제한
  - SSI는 HTML 페이지 안에 위치하고 있으며, 동적인 웹 페이지를 제공할 수 있도록 한다.

하지만 SSI가 포함된 파일은 "exec cmd"를 사용해서 어떤 CGI 스크립트나 프로그램들을 Apache가 구동하는 사용자와 그룹 권한으로 실행시킬 수 있다.

- 이 SSI 페이지가 스크립트나 프로그램을 실행시킬 수 없도록 하기 위해서는 "Options" 지시자에 "IncludesNoExec" 옵션을 추가함으로써 차단할 수 있다.

● CGI 실행디렉토리 제한

- 사용자들이 CGI 스크립트들을 어느 디렉토리에서나 실행할 수 있도록 할 경우 악의적인 사용자가 CGI 프로그램을 업로드한 후 이를 실행하여 임의의 명령을 실행시킬 수 있다.
- 따라서, CGI 프로그램의 실행은 관리자가 지정한 특정 디렉토리에서만 가능하도록 제한할 필요가 있다. CGI 실행은 "ScriptsAlias" 지시자에 의해서 실행가능한 디렉토리를 제한할 수 있다. "ScriptsAlias" 지시자 문법은 다음과 같다.

```
정의방법: ScriptAlias URL-path file-path | directory-path
```

예를들어 cgi-bin이라는 디렉토리에서만 CGI프로그램을 실행가능하도록 할 경우 다음과 같이 지정할 수 있다.

```
ScriptAlias /cgi-bin/ "/usr/local/apache/cgi-bin/"
```

앞서 언급한 디렉토리 리스팅, 심블릭 링크, SSI 등에 대한 제어는 "Options" 지시자에 의해 제어가 가능하다.

```
정의방법: Options [+|-]option [[+|-]option] ...
```

"Options" 지시자에서 사용할 수 있는 옵션값은 다음 표와 같다.

[표 5-1-1] Options 지시자(directive) 및 설정 값

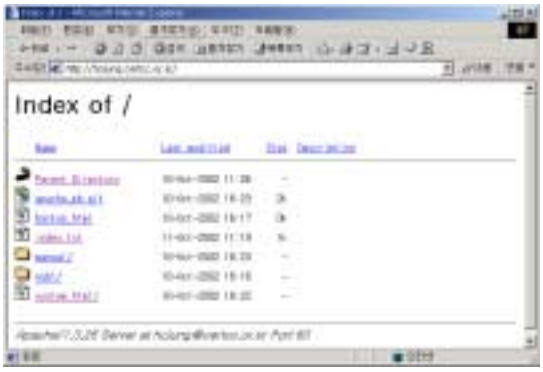
옵 션 값	설 명
All	MultiViews를 제외한 모든 옵션을 줌(default 설정값임)
None	옵션을 주지 않음
ExecCGI	CGI 프로그램 실행을 가능하게 함
FollowSymLinks	심볼릭 링크로의 이동을 가능하게 함
Includes	Server Side Includes를 가능하게 함
IncludesNOEXEC	Server-side includes는 가능하지만 CGI 스크립트나 프로그램들은 실행할 수 없도록 함.
Indexes	해당 디렉토리 안에 DirectoryIndex에 명기된 파일(index.html 등)이 없을 경우 디렉토리와 파일 목록을 보여줌
MultiViews	유사한 파일이름을 찾아 주는 기능을 실행함(예를들어 index라고만 입력하더라도 index.*를 찾아 보여줌)
SymLinksIfOwnerMatch	The server will only follow symbolic links for which the target file or directory is owned by the same user id as the link.

● httpd.conf 설정 예시

- DocumentRoot 디렉토리가 다음과 같이 설정되어 있다고 하자.

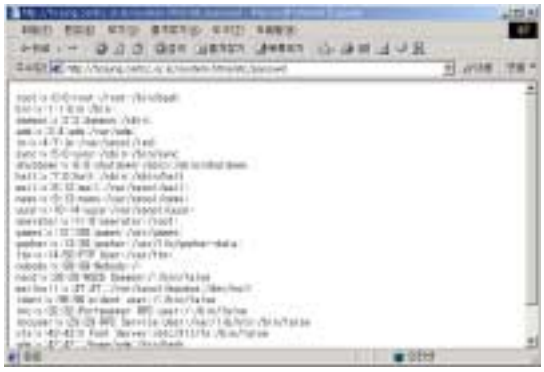
```
〈Directory "/usr/local/www" 〉
    Options Indexes FollowSymLinks
〈/Directory〉
```

- 이 경우 다음 그림과 같이 DirectoryIndex에 정의된 초기 파일(index.html)이 존재하지 않을 경우 디렉토리 내의 파일목록을 리스트업 해 준다.



DirectoryIndex에 정의된 초기 파일이 존재하지 않을 경우 (그림 5-1-1)

- 또한, FollowSymLinks로 인해 루트 디렉토리(/)에 심볼릭 링크된 system.html 파일(ln -s / system.html)을 열었을 경우 DocumentRoot 디렉토리 상위의 passwd 파일까지 열람이 가능함을 알 수 있다.



루트 디렉토리에 심볼릭 링크된 system.html 파일을 열었을 경우 (그림 5-1-2)

- 이러한 문제점을 제거하기 위해서는 Indexes 옵션과 FollowSymLinks 옵션을 제거하고, IncludesNoExec 옵션을 사용하도록 한다.

```
〈Directory "/usr/local/www" 〉
    Options IncludesNoExec
〈/Directory〉
```

이 경우 다음과 같이 초기 파일(index.html)이 존재하지 않을 경우 디렉토리 리스트를 보여주는 것이 아니라 오류 창을 띄워주는 것을 확인할 수 있다.

초기 파일이 존재하지 않을 경우
(그림 5-1-3)

● 웹서버 응답 메시지 헤더 정보 숨기기

- 웹서버 헤더 정보란 다음과 같이 클라이언트가 Apache 웹서버에 접속했을 때 웹서버에서는 응답 메시지의 헤더를 말한다.

```
[root@hcjung conf]# telnet xxx.xxx.xxx.xxx 80
Trying xxx.xxx.xxx.xxx...
Connected to xxx.xxx.xxx.xxx.
Escape character is '^]'.
GET / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Tue, 15 Oct 2002 11:25:10 GMT
Server: Apache/1.3.19 (Unix) PHP/4.0.4pl1
```

- 이 정보는 공격자에 의해 Apache 웹서버 버전별 또는 구동되고 있는 응용프로그램에 잘 알려진 취약점을 공격하는데 유용하게 악용될 수 있으며, 인터넷 웜과 같은 자동화된 공격에서도 이러한 배너(banner) 정보가 사용되어지기도 한다. 따라서 공격자에게 웹서버의 버전과 같은 banner 정보를 숨기는 것이 안전하다.

- Apache 웹서버에서는 "ServerTokens" 지시자를 수정함으로써 헤더에 의해 전송되는 정보를 바꿀 수 있다.

정의방법: ServerTokens Minimal|ProductOnly|OS|Full

- ServerTokens 지시자를 이용하여 설정할 수 있는 각 키워드와 표시되는 헤더 정보는 다음과 같다.

[표 5-1-2] ServerTokens 지시자(directive) 및 설정 값

키워드	제공하는 정보	예
Prod[uctOnly]	웹서버 종류	Server: Apache
Min[imal]	Prod 키워드 제공 정보 + 웹서버 버전	Server: Apache/1.3.0
OS	Min 키워드 제공 정보 + 운영체제	Server: Apache/1.3.0 (Unix)
Full	OS 키워드 제공 정보 + 설치된 모듈(응용프로그램) 정보	Server: Apache/1.3.0 (Unix) PHP/3.0 MyMod/1.2

- 공격자를 속이기 위해서 서버의 헤더 정보를 앞에서 명기한 내용과는 전혀 다른 내용으로 조작하여 클라이언트에 보낼 수도 있는데 이를 위해서는 Apache 소스코드를 수정한후 재컴파일하여야 한다.

5. 사용자 인증

가. 사용자 인증의 종류

(1) 기본 사용자 인증(Basic Authentication)

- 기본 사용자 인증은 Apache에서 제공되는 htpasswd를 이용하여 사용자 계정을 생성하고 인증하는 방법이다.
- 패스워드가 암호화되어서 저장되지만 클라이언트에서 서버로 전송되는 도중에는 암호화되지 않아 전송 중 노출될 수 있다.

(2) 다이제스트 사용자 인증(Digest Authentication)

- 기본 사용자 인증과 마찬가지로 Apache에서 제공되는 htpasswd를 이용하여 사용자 계정을 생성하고 인증하는 방법이다.
- 기본 사용자 인증과의 차이점은 패스워드를 MD5 암호화 해쉬하여 전송하므로 전송중에도 비교적 안전하지만 인증에 사용되는 패스워드만 암호화되고 데이터는 평문으로 전송됨을 주지할 필요가 있다.

(3) 어플리케이션에서의 인증(데이터베이스 등 로그인 정보유지)

- 어플리케이션에서의 인증은 Apache에서 제공되는 htpasswd 명령을 이용하지 않고 사용자 이름과 패스워드를 데이터베이스에 저장하고 이를 이용하여 인증하는 방법이다.
- 데이터베이스에 저장된 사용자 계정에 대한 정보는 기업의 보안정책에 따라 다르지만 일반적으로, 암호화나 단방향 함수(해쉬)등을 적용하여 저장하는 것이 안전하다(내부자에 의한 정보유출 방지).

나. 기본 사용자 인증

- 기본 사용자 인증은 크게 다음과 같은 두가지 절차로 설정할 수 있다.

① 패스워드 파일 생성

- Apache 설치시 제공되는 htpasswd 명령을 이용하여 패스워드 파일을 생성한다. htpasswd 파일의 사용법은 다음과 같다.

```
사용법: htpasswd [-cmdps] passwordfile username
```

- 패스워드 파일을 최초로 생성할 경우에는 -c 옵션을 사용하여 새로운 패스워드 파일을 만든다.

```
[root@hcjung bin]# ./htpasswd -c /usr/local/apache/passwords hcjung
New password:
Re-type new password:
Adding password for user hcjung
```

- 이후, 새로운 사용자를 추가하고자 할 경우에는 -c 옵션을 빼고 사용하면 된다. 실수로 -c 옵션을 줄 경우 기존에 등록된 사용자들이 지워지므로 주의하여야 한다.

```
[root@hcjung bin]# ./htpasswd /usr/local/apache/passwords webmaster
```

- 생성된 패스워드 파일은 가능한 안전한 장소에 보관하고 웹서버 자체가 읽을 수 있는 최소한의 권한만을 주어야만 한다. 만일 웹서버가 nobody 사용자와 nobody 그룹으로 구동된다면 다음과 같이 소유권과 접근권한을 줄 수 있다.

```
[root@hcjung bin]# chown root.nobody /usr/local/apache/passwords
[root@hcjung bin]# chmod 640 /usr/local/apache/passwords
```

② 패스워드 파일을 사용가능하도록 환경설정

- 패스워드 파일의 생성이 끝났으면 Apache 웹서버에게 이 파일을 사용할 수 있도록 설정하여 주어야 한다.
- 먼저 각 디렉토리별로 사용자 인증을 하기 위해서 httpd.conf 파일 내의 AllowOverride 지시자의 옵션을 None에서 AuthConfig 또는 All로 바꾼다.(사용자 인증만을 위해서는 AuthConfig 사용을 권고)

```
〈Directory "/usr/local/www" 〉
   AllowOverride AuthConfig
〈/Directory〉
```

그리고, 사용자 인증이 필요한 디렉토리에 다음의 지시자들이 포함된 .htaccess 파일을 생성한다.

[표 5-1-3] htaccess파일에 사용되는 지시자(directive)

지 시 자	설 명
AuthType	인증 형태(Basic 또는 Digest)
AuthName	인증 영역(웹 브라우저의 인증창에 표시됨)
AuthUserFile	사용자 패스워드 파일의 위치
AuthGroupFile	그룹 파일의 위치(옵션)
Require	접근을 허용할 사용자 또는 그룹 정의 ex) Require user userid [userid] ... Require group group-name [group-name] ... Require valid-user

앞서 패스워드 파일에 등록된 hcjung와 webmaste만이 웹서버에 접속할 수 있도록 하기 위해서는 다음과 같이 설정할 수 있다.

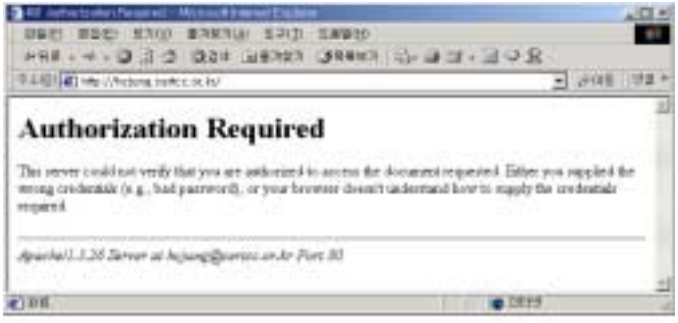
```
[root@hcjung /root]# cd /usr/local/www
[root@hcjung www]# vi .htaccess
AuthType Basic
AuthName "Welcome HyunCheol' s Home"
AuthUserFile /usr/local/apache/passwords
Require user hcjung webmaste
```

- 위에서 접근을 허용할 사용자를 hcjung와 webmaste로 한정을 했는데 패스워드 파일에 등록된 모든 사용자들이 접근할 수 있도록 하기 위해서는 사용자를 지정하는 대신 "Require valid-user"라고 하면 된다.

모든 사용자들이 접근하도록 지정
(그림 5-1-4)

- 정상적으로 사용자 인증 설정이 완료되었을 경우 웹 브라우저에서 웹서버 접속시 다음과 같은 사용자 이름과 암호를 묻는 인증창이 뜨게 된다.

- 사용자 이름과 암호가 정확하게 입력된 경우는 웹 페이지 접속이 가능하지만 정확하지 않을 경우 다음과 같은 경고창이 뜨고 접속을 허가하지 않는다.



사용자 이름과 암호가 정확하지 않을 경우
(그림 5-1-5)

6. SSL 인증서 또는 웹 암호화 솔루션의 적용

- 웹을 통하여 회원신상, 금융거래, 카드번호 등 데이터의 기밀성이 요구되는 데이터가 전송된다면 SSL을 적용하거나 기타 웹 암호화 제품의 적용을 고려하여야 한다.
- Apache에서는 mod-ssl을 이용하여 SSL 암호화를 적용할 수 있다.
- SSL의 적용은 기본적으로 OpenSSL을 이용한 Apache용 SSL모듈(apache/mod-ssl)을 이용하여 생성한 자체 SSL 인증서를 이용할 수도 있고, 유료로 제공되는 SSL인증서를 이용할 수도 있다.

● 자체 SSL인증서와 유료 인증서 방식의 차이점은 접속하는 사용자 관점에서 해당 사이트가 정말로 그 사용자가 믿고(알고)있는 웹 사이트인지 여부에 대하여 제3자(인증기관)이 보증해 주느냐 안해주느냐의 차이다. 데이터에 이용되는 암호화 수준은 알고리즘과 키길이와 관련되므로 별개의 문제이다.

7. 보안 패치

● Apache설치후 버전별로 발견된 취약점은 ApacheWeek (http://www. pacheweek.com /security/) 에서 확인할 수 있다.

● 가능한 주기적으로 보안 패치정보를 확인후 조치하여야 한다. Apache 웹서버 관련 취약점에 대한 패치는 아래 링크에서 다운받을 수 있다.
http://www.apache. org/dist/httpd/patches/

8. 설정파일 및 데이터 백업

● 초기 서버 설정파일들과 이후의 기본적인 설정파일들은 일반에 공개되거나 다른 변화가 일어나기 전에 백업해서 보관되어져야 한다. 또한 시스템 설정이 변경될 때마다 이력관리가 필요하고 다수의 수정이 있을 경우에는 반드시 백업을 하도록 한다.

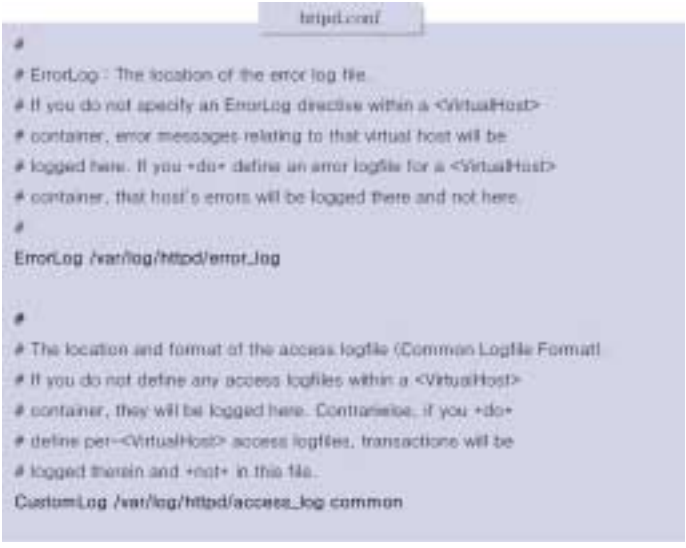
● 백업해야 하는 주요 데이터는 다음과 같은 것이 있다.
- Apache 각종 환경설정 파일
- Apache 설치과정에 사용된 Install 파일(경우에 따라 Rebuild 에 많은 시간을 단축할 수 있음)
- 사용자 프로그램 소스(PHP, JSP, CGI등)
- 웹 서비스와 관계된 데이터베이스 등

9. 로그 설정 및 분석

● Apache는 두 개의 로그 파일을 사용하는데, 에러 로그(error log)와 액세스 로그(access log)이다. 에러 로그는 Apache 서버의 에러 정보를 기록하고, 액세스 로그는 Apache 서버

가 처리하는 모든 요청에 대한 정보를 기록한다.

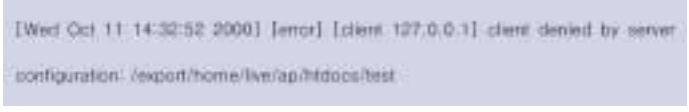
- 로그 파일의 위치는 httpd.conf 파일에서 지정한다.



httpd.conf 파일에서 지정
(그림 5-1-6)

가. 에러 로그

- 에러 로그 파일의 포맷은 비교적 자유로운 형식인데, 대부분의 경우 다음과 같은 정보가 포함된다.



에러로그 1
(그림 5-1-7)

① 메시지의 날짜와 시간
② 에러의 위험도
③ 에러를 발생시킨 클라이언트의 IP주소
④ 에러 메시지의 내용 (클라이언트가 요청한 문서를 파일 시스템 경로로 표현)

● 에러 로그 파일에 기록될 에러의 위험도 수준은 다음과 같이 httpd.conf파일에서 LogLevel 지시자를 이용하여 지정할 수 있다.

에러로그 3
(그림 5-1-8)

```
httpd.conf
#
# LogLevel : Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel  error
```

나. 액세스 로그

● 액세스 로그는 서버가 처리하는 모든 요청에 대한 정보를 기록한다. 액세스 로그의 위치와 로그 포맷은 CustomLog 지시자를 통해 지정된다. LogFormat 지시자를 이용해서 다양한 로그 포맷을 만들어 놓고, 간단하게 선택하여 사용할 수 있다.
● 액세스 로그로 사용되는 공통적인 로그 포맷은 Common Log Format(CLF)과 Combined Log Format(CLF)이다.

(1) Common Log Format(CLF): 많은 다른 웹서버에서도 동일하게 생성되는 포맷이고, 많은 로그 분석 프로그램이 읽을 수 있는 포맷이다. httpd.conf 파일에서 다음과 같이 설정할 수 있다.

액세스 로그 1
(그림 5-1-9)

```
httpd.conf
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log common
```

● LogFormat 지시자는 하나의 포맷 스트링을 정의하고 common이라는 닉네임을 붙인다. CustomLog 지시자는 로그가 저장될 파일의 위치와 이름, 그리고 저장될 로그의 포맷을 정의한다.
● 이 포맷에 의해 생성된 로그는 다음과 같다.

액세스 로그 2
(그림 5-1-10)

```
172.16.5.100 - jun [08/Apr/2003:16:03:45 +0900] "GET /php HTTP/1.1" 301
```

① 클라이언트의 IP 주소(%h) : 다(이 설정으로 서버가 크게 느려질 수 있기 때문에 가능하면 사용하지 않도록 한다).

② 클라이언트의 identity(%l) : 클라이언트 컴퓨터의 identd에 의해 결정된 클라이언트 identity. IdentityCheck가 On으로 설정되어 있지 않으면 이 정보를 찾지 않는다(이 설정으로 서버가 느려질 수 있고, identity 정보도 신뢰하기 어렵기 때문에 가능하면 사용하지 않도록 한다).

③ HTTP 인증을 받은 사용자의 ID(%u) : 인증을 받지 못한 경우에(상태 코드가 401인 경우) 이 값은 부정확하다. 또한 요청받은 문서가 인증을 요구하지 않는 경우에는 -로 표시된다.

④ 서버가 요청 처리를 끝낸 시간(%t) : [일/월/년:시:분:초 지역]

⑤ 클라이언트의 요청 내용(\ %r\ ) : 사용한 메소드, 요청한 자원, 사용한 프로토콜이 표시된다.

⑥ 상태코드(%>s) : 서버가 클라이언트에게 보낸 상태 코드에는 2XX(성공), 3XX(redirection), 4XX(클라이언트에 의한 에러), 5XX(서버에 의한 에러)가 있다.

⑦ 클라이언트에게 전송된 컨텐츠의 크기 response header 부분은 포함되지 않는다. 클라이언트에게 전송된 컨텐츠가 없으면 이 값은 '-' 로 표시된다.

(2) 다음은 Combined Log Format :

- httpd.conf 파일에서 다음과 같이 설정할 수 있다.

httpd.conf

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-
agent}i\"" combined
CustomLog log/acces_log combined
```

Combined Log Format 1
(그림 5-1-11)

- 이 포맷은 두 개의 필드를 제외하면 Common Log Format과 동일하다. 추가된 필드는 퍼센트 지시자 %{header}를 사용하고 있는데, header는 HTTP request header 중 일부가 될 수 있다. 이 포맷에 의해 생성된 로그는 다음과 같다.

```
172.18.5.100 - jun [08/Apr/2003:18:03:43 +0900] "GET /php HTTP/1.1" 301
313 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
```

Combined Log Format 2
(그림 5-1-12)

① 클라이언트가 요청한 자원이 include되었거나 링크된 페이지(\ %{Referer}I\) 위 예제에서는 그러한 페이지가 없음
② 클라이언트 브라우저에 대한 정보(\ %{User-agent}I\)

다. 로그 설정시 유의사항

- Apache는 대부분의 경우 root권한으로 로깅을 수행하는데, 시스템사용자는 Apache의 로그 파일을 다른 중요 시스템 파일에 대한 링크로 대체하여, root 권한으로 다른 중요 시스템 파일의 내용을 변경할 수 있다.
- 따라서, 일반사용자는 로그가 저장되는 디렉토리에 대해 쓰기 권한이 없도록 설정해야 한다.
- 또한 로그 파일에 클라이언트가 제공하는 데이터가 들어갈 경우 악의적인 클라이언트가 제어문자 등을 로그 파일에 삽입하여 웹서버를 침해할 수 있다. 특히 클라이언트가 웹 서비스를 통해서 Apache의 로그 파일을 볼 수 없도록 해야 한다.

제2절 Microsoft IIS (Internet Information Server)

1. 부팅파티션과 웹 서비스 파티션의 분리

부트파티션과 데이터파티션을 분리하도록 한다. 서로 다른 디스크를 사용하거나 최소한 파티션을 나누어서 설치하도록 한다. 이렇게 하면 웹 서비스의 피해가 서버 전체의 피해로 확산되는 것을 최소화 할 수 있다.

2. NTFS 파일 시스템의 사용

Windows 서버 운영체제에서는 두가지 파일 시스템을 제공한다. FAT(File Allocation Table)과 NTFS(NT File System)인데, 이 중에서 NTFS가 보안, 성능, 로깅(logging) 측면에서 우수하다.

특히 보안 측면에서 NTFS는 파일단위의 암호화 및 권한 설정이 가능하고, 디스크 할당량을 설정할 수 있다. 따라서 반드시 NTFS를 사용해서 웹서버 보안을 강화하도록 한다. 웹서버를 운영하는 시스템에서는 최소한 부트 파티션과 웹 서비스를 제공하는 파티션은 NTFS를 사용하도록 한다.

다음은 NTFS 파일 시스템을 사용하는 3가지 방법이다.

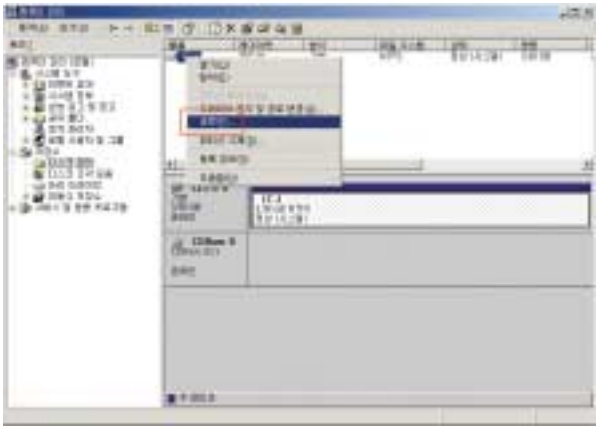
① OS를 설치하지 않은 경우 OS 설치과정에서 파일 시스템을 NTFS로 포맷한다.

② OS가 이미 설치된 경우에는 Convert 유틸리티를 사용해서 FAT 파티션을 NTFS로 변환한다. Convert 유틸리티 사용 예제는 다음과 같다.

```
C:₩convert D: /FS:NTFS
```

Convert 유틸리티 사용 예제
(그림 5-2-1)

③ 데이터가 없는 파티션의 파일 시스템을 변환하는 경우 디스크 관리자를 이용해서 파티션을 NTFS로 재포맷한다. **[시작]** ➪ **[프로그램]** ➪ **[관리도구]** ➪ **[컴퓨터 관리]**에서 **[디스크 관리]**를 선택한 후, 해당 드라이브에 대해 마우스 오른쪽 버튼을 클릭한 후 **[포맷]**을 선택하면 된다.



데이터가 없는 파티션의 파일 시스템을 변환하는 경우
(그림 5-2-2)

3. 필요한 구성요소만을 설치

● 불필요한 구성요소의 설치는 보안과 시스템 성능 측면에서 도움이 되지 않는다. 웹 서비스에 꼭 필요한 요소만을 설치하여 보안관리를 용이하게 하고 예측하기 어려운 위험에 대한 노출을 최소화 하도록 한다.

● 인터넷 정보 서비스의 구성요소들은 다음과 같다.
- 공용파일
- 설명서
- 인터넷 서비스 관리자(HTML)
- 인터넷 정보 서비스 스냅인
- FTP 서버
- FrontPage 2000 Server Extension
- NNTP Service
- SMTP Service
- Visual InterDev RAD Remote Deployment Support
- World Wide Web 서버

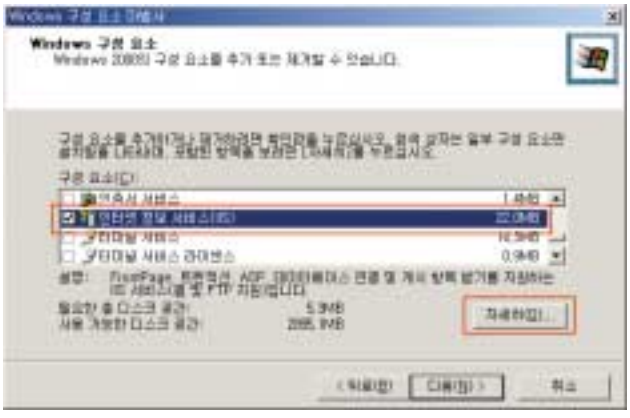
● 이 가운데 다음 3가지 요소는 웹서버 운영에 필수적인 요소로서, 이 3가지만으로도 웹서버 운영이 가능하다. 그 외의 구성요소는 필요에 따라 추가하면 된다.
- 공용파일
- 인터넷 정보 서비스 스냅인
- World Wide Web 서버

● Windows 2000 Serve 설치시 인터넷 정보 서비스의 구성요소를 결정할 수 있고, Windows 2000 Server 설치 후에는 다음과 같은 방법으로 구성요소를 추가하거나 제거 할 수 있다.

① **[제어판]** ⇨ **[프로그램 추가/제거]** 아이콘을 실행한다.

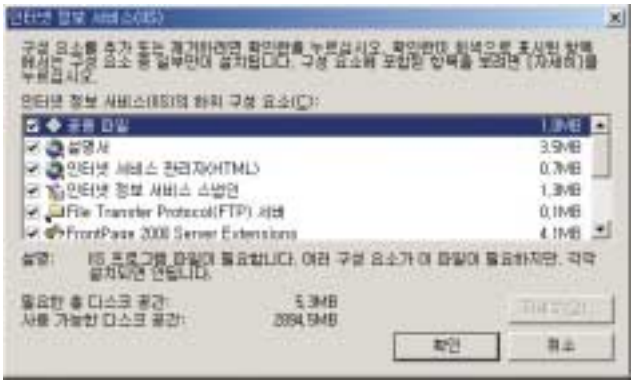
② **[프로그램 추가/제거]** 창에서 좌측 **[Windows 구성 요소 추가/제거]** 메뉴를 클릭한다.

③ **[Windows 구성 요소 마법사]** 창에서 **[인터넷 정보 서비스(IIS)]**를 선택한 후 **[자세히]** 버튼을 클릭한다.



Windows 구성 요소 추가/제거 1
(그림 5-2-3)

④ 이제 추가할 구성요소는 체크를 하여 선택한 후 **[확인]** 버튼을 클릭한다.



Windows 구성 요소 추가/제거 1
(그림 5-2-4)

4. 웹전용 서버로 구성(불필요한 서비스 제거)

● 웹서버 운영에 필요한 서비스들만 구동시키고 불필요한 서비스들을 중지시켜서 보안 문제의 발생 가능성을 최소화 시킨다.

아래 표는 IIS가 동작하기 위해 필요한 서비스들이다.

[표 5-2-1] IIS 동작에 필요한 서비스

서비스명
Event Log
License Logging Service
Windows NT Lanman(NTLM)
Security Support Provider
Remote Procedure Call(RPC) Service
Windows NT Server or Windows NT Workstation
IIS Admin Service
Microsoft Distributed Transaction Coordinator(MSDTC) Protected Storage
Microsoft Distributed Transaction Coordinator(MSDTC) Protected Storage

● 현재 운영하려는 웹서버에 반드시 필요한 서비스가 어떤 것이고 어떤 서비스가 불필요한지를 결정하기 위해 Microsoft에서 제공하는 다음 문서를 참고하도록 한다.

http://www.microsoft.com/korea/technet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp
(혹은 Technet 사이트내 검색 ⇨ Windows 2000 서비스 입력 ⇨ 검색결과에서 **[기술 자료]** 카테고리내의 **[Windows 2000 서비스]**를 클릭)

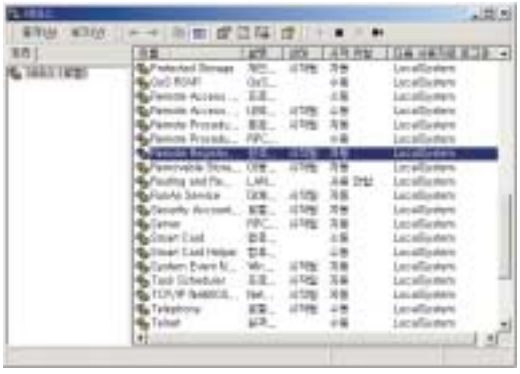
● 다음 서비스들은 사용하지 않도록 권장된다.

[표 5-2-2] 사용중지를 권장하는 서비스

서비스명
Application Management
Clipboard Service
DHCP Client
Fax
Messenger
Print Spooler
Remote Registry Service
Smart Card / Smart Card Helper
Telnet

● 불필요한 서비스를 중지시키는 방법은 다음과 같다.

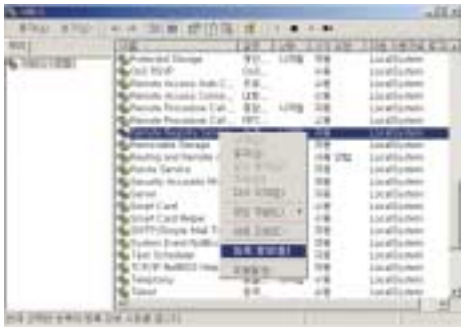
① **[시작]** ⇨ **[프로그램]** ⇨ **[관리도구]** ⇨ **[서비스]** 프로그램을 실행한다.

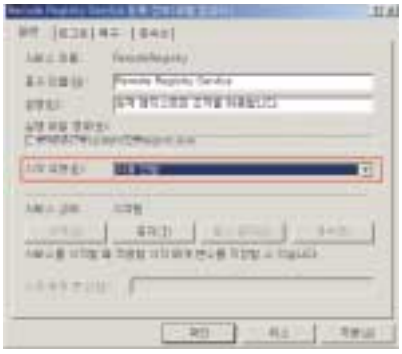


불필요한 서비스를 중지시키는 방법 1
(그림 5-2-5)

② 중지하려는 서비스에 대해 마우스 오른쪽 버튼을 클릭하고 **[등록 정보]**를 선택한 후, 시작 유형에서 **[사용 안함]**을 선택한다.

불필요한 서비스를 중지시키는 방법 2
(그림 5-2-6)





③ 서비스간의 의존성에 따라 서비스 사용중지가 불가능한 경우가 있는데, 이런 경우에는 각 서비스에 대한 서비스 종속성 옵션을 살펴볼 수 있다. 각 서비스의 **[등록정보]**의 **[종속성]** 탭을 선택하면 다음과 같이 그 서비스가 종속된 서비스 목록과 그 서비스에 종속된 서비스 목록을 볼 수 있다.

불필요한 서비스를 중지시키는 방법 3
(그림 5-2-7)

5. 계정의 수와 권한을 최소화

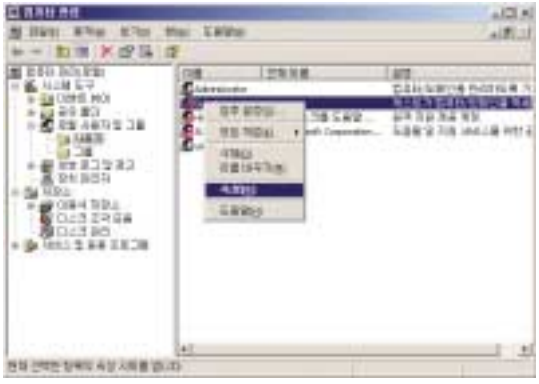
- 웹서버에는 꼭 필요한 계정만을 만들고, 각 계정에 대해서는 필요한 최소한의 권한만 주도록 한다. 일반적으로 웹서버에는 관리자 계정과 웹서버 구동을 위한 계정만 남기고 일반 사용자 계정은 삭제하도록 하는 것이 좋다.

- IIS를 설치하면 두 개의 익명 계정이 생성되는데, IUSR_컴퓨터이름과 IWAM_컴퓨터이름이다. IUSR_컴퓨터이름은 웹자원에 대한 익명 접근을 허용하는데 사용되는 계정이다. IWAM_컴퓨터이름은 MTS(Microsoft Transaction Server)와 다양한 IIS 개체가 사용하는 계정이다. 이 두 계정에 대해서는 최소한의 권한만 유지하도록 한다.

- 디폴트 계정 중에 불필요한 계정은 사용안함으로 설정하고 디폴트 이름을 가지고 있는 주요 계정은 이름을 변경하도록 한다. 예를 들어 Guest계정은 사용안함으로 설정하고 Administrator 계정은 해커가 추측하기 어려운 계정명으로 바꾸도록 한다.

Guest 계정을 사용하지 않기 위해서는 다음과 같이 설정한다.

① **[시작]** ⇨ **[프로그램]** ⇨ **[관리도구]** ⇨ **[컴퓨터 관리]**에서 **[로컬 사용자 및 그룹]**을 선택한 후 **[사용자]**를 선택한다.



Guest 계정을 사용하지 않기위한 설정1
(그림 5-2-8)

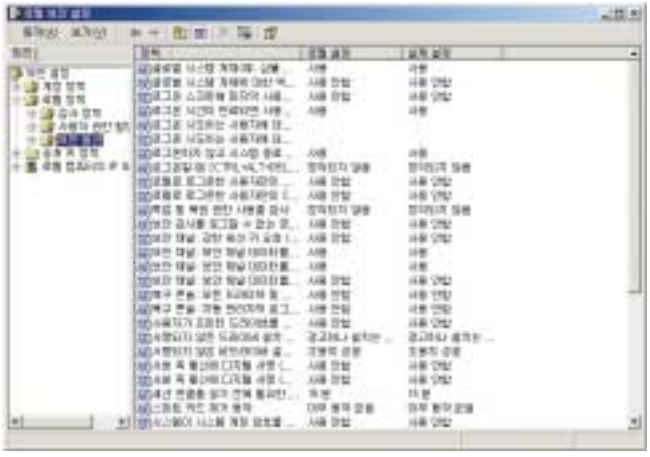
② 오른쪽에서 Guest 계정에 대해 마우스 오른쪽 버튼을 클릭한 후 **[등록 정보]**를 선택한다. 여기에서 **[계정 사용 안함]**을 선택한다.

Guest 계정을 사용하지 않기위한 설정2
(그림 5-2-9)

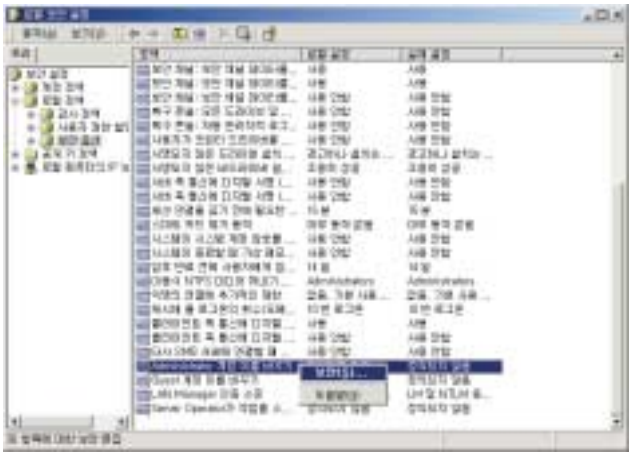
Administrator계정을 다른 이름으로 바꾸는 방법은 다음과 같다.

① **[프로그램]** ⇨ **[관리도구]** ⇨ **[로컬 보안 정책]** ⇨ **[로컬 정책]**을 선택하고 **[보안 옵션]**을 선택한다.

Administrator계정을 다른 이름으로 바꾸는 방법1
(그림 5-2-10)

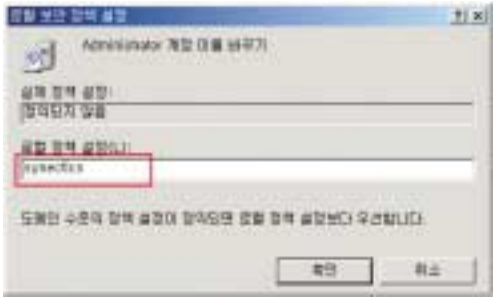


② Administrator 계정 이름 바꾸기에 대해 마우스 오른쪽 버튼을 클릭하고 **[보안]**을 선택한다.



administrator계정을 다른 이름으로 바꾸는 방법2
(그림 5-2-11)

③ 로컬 보안 정책 설정 화면에서 새로운 관리자 계정 이름을 입력한다.



administrator계정을 다른 이름으로 바꾸는 방법3
(그림 5-2-12)

시스템을 재시작하면 Administrator 계정이 바뀌어 있음을 확인할 수 있다.

6. 공유 사용 안함

- 많은 바이러스가 윈도우즈의 네트워크 공유를 통해 감염되기 때문에 웹서버에서는 공유를 절대 사용하지 않도록 한다. 일반 공유뿐만 아니라 관리 공유의 경우도 반드시 필요한 것만 사용하고 나머지는 제거하도록 한다.

- 관리 공유는 관리자와 운영 체제 서비스가 네트워크에서 컴퓨터 환경을 관리하는 데 사용하도록 만들어 진 것이다. 관리 공유는 설정을 해제할 수 있지만 컴퓨터를 다시 시작하면 공유가 다시 설정되어 있다.
- 관리 공유에는 다음과 같은 것들이 있다.
  - 루트 파티션 또는 볼륨
  - 시스템 루트 폴더
  - FAX$ 공유
  - IPC$ 공유
  - NETLOGON 공유
  - PRINT$ 공유
- 루트 파티션과 볼륨은 $ 기호가 추가된 드라이브 문자 이름으로 공유된다. 예를 들어, C와 D 드라이브는 C$와 D$로 공유된다.
- 시스템 루트 폴더 (%SYSTEMROOT%)는 ADMIN$로 공유된다. 이 관리 공유를 사용하면 관리자는 네트워크를 통해 시스템 루트 폴더 계층에 쉽게 액세스할 수 있다.
- FAX$ 공유는 팩스를 보내는 과정에서 팩스 클라이언트가 사용한다. 이 공유 폴더는 파일을 캐싱하고 파일 서버에 저장된 표지 페이지에 액세스한다.
- IPC$ 공유는 네트워크 프로그램 간 통신에 명명된 파이프를 통해 클라이언트와 서버 사이를 임시로 연결하는 데 사용된다. 이것은 네트워크 서버의 원격 관리에 주로 사용된다.
- NETLOGON 공유는 Netlogon 서비스가 로그온 요청을 처리하는 데 사용된다. PRINT$ 공유는 프린터의 원격 관리에 사용된다.

이 중 **[드라이브 문자]**$, PRINT$, FAX$는 웹서버에서 반드시 제거하도록 하고 나머지 공유도 사용하지 않는다면 제거하도록 한다. IPC$는 시스템을 시작할 때마다 제거해주어야 한다.

관리 공유 설정을 해제하는 방법은 다음과 같다.

① 레지스트리 편집기를 실행한다.

② HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanServer\parameters에서 다음 두 값들을 생성하도록 한다.

AutoShareServer : 0
AutoShareWks : 0

관리 공유 설정을 해제하는 방법1
(그림 5-2-13)

생성방법은 다음과 같다. 우선 **[편집]** 메뉴에서 **[값 추가]**를 선택한다.

관리 공유 설정을 해제하는 방법2
(그림 5-2-14)

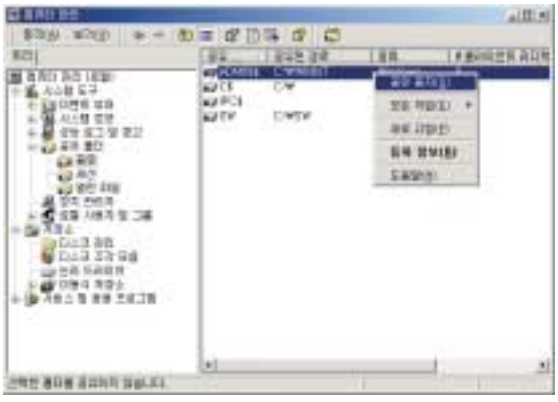
[값이름]으로 AutoShareServer를 입력하고, **[데이터 형식]**으로 REG_DWORD를 선택한 후 **[확인]**을 누른다.

관리 공유 설정을 해제하는 방법3
(그림 5-2-15)

위와 동일한 방법으로 AutoShareWks도 생성한다.

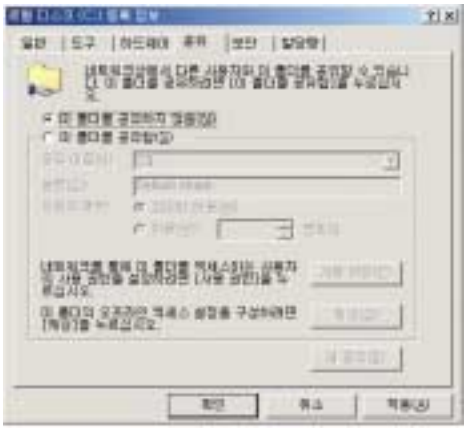
③ **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[컴퓨터 관리]**에서 **[공유 폴더]**와 **[공유]**를 차례로 선택하면 오른쪽에 관리 공유 목록이 보인다. 제거하려는 공유에 대해서 마우스 오른쪽 버튼을 클릭하고 **[공유 중지]**를 선택한다.

AutoShareWks 생성1
(그림 5-2-16)



PRINT$의 경우 Print Spooler 서비스를 사용중지 해줘야 완전한 삭제가 가능하다. 관리 공유를 삭제하면 재부팅을 해도 다음 그림과 같이 관리 공유 설정이 다시 살아나지 않는다.

AutoShareWks 생성2
(그림 5-2-17)

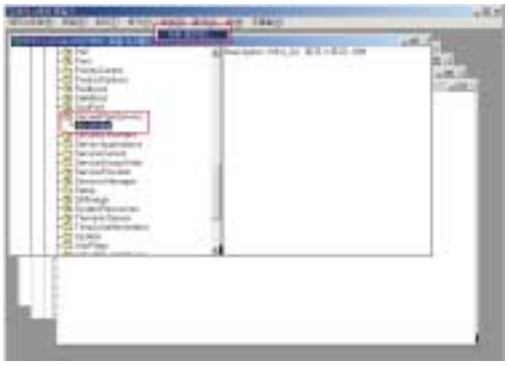


7. 레지스트리 원격 접근 제한

● Windows 2000 레지스트리 편집 도구에서 기본적으로 원격 액세스를 지원하므로, 레지스트리 원격 액세스 권한은 관리자에게만 부여해야 한다. 레지스트리에 대한 네트워크 액세스를 제한하는 방법은 다음과 같다.

① 레지스트리 편집기(regedt32)를 실행한다.

② HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secure Pipe Servers에서 winreg를 선택하고 **[보안]** 메뉴를 선택한 다음, **[사용 권한]**을 선택한다.



네트워크 액세스를 제한하는 방법1
(그림 5-2-18)

③ Administrators 사용 권한을 모든 권한(Full Control)으로 설정하고, 다른 사용자나 그룹이 표시되지 않는 지 확인한 다음 **[확인]**을 클릭한다.

네트워크 액세스를 제한하는 방법2
(그림 5-2-19)

이 키에 설정된 보안 권한은 원격 레지스트리 액세스를 위하여 시스템에 연결할 수 있는 사용자나 그룹을 정의한다.

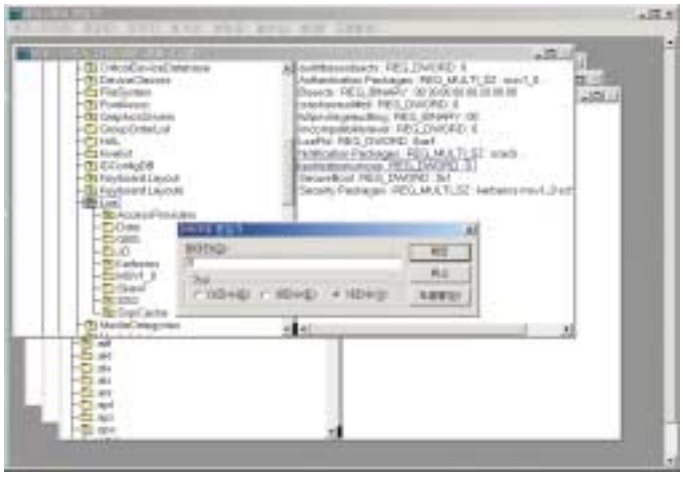
AllowedPaths 하위 키에는 winreg 키의 보안 권한과 별도로 Everyone 그룹의 구성원이 액세스할 수 있는 키 목록이 있다. winreg 레지스트리 키에서의 액세스 제한에 관계없이 프린터 상태 확인과 같은 특정 시스템 기능을 사용할 수 있다. AllowedPaths 레지스트리 키의 기본 보안 설정은 Administrators만이 경로를 관리할 수 있도록 되어 있다.

8. 공개 로컬 보안 인증(LSA)의 정보에 대한 접근 제한

- 익명 사용자가 Windows NT Security Subsystem의 LSA 구성 요소에 대해 얻을 수 있는 공개 정보를 최소화해야 한다. LSA는 로컬 컴퓨터의 액세스와 사용 권한을 포함한 보안 관리 항목을 처리한다. 이 제한을 설정하는 방법은 다음과 같다.

① 레지스트리 편집기(regedt32)를 실행한다.
② HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa에서 restrictanonymous를 더블클릭한 후 데이터 값으로 1을 입력하고 **[확인]** 버튼을 누른다.

LSA 설정
(그림 5-2-20)



9. 시스템 실행 파일에 대한 제한

- 사용되지 않는 실행 파일들을 모두 제거하거나 관리자만 실행 가능하도록 설정하여 잠재적인 위험 요소를 제거한다.

다음 실행 파일들에 대해 관리자만 실행이 가능하도록 설정한다.

[표 5-2-3] 사용중지를 권장하는 서비스

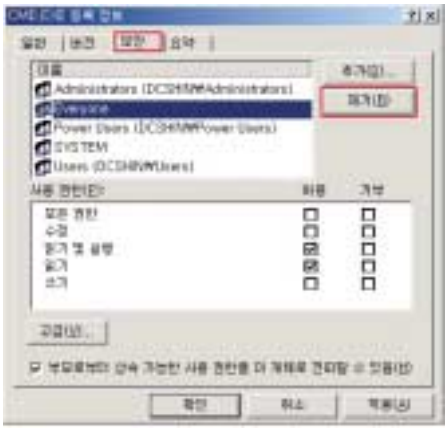
arp.exe	at.exe	cmd.exe	edit.com
edlin.exe	finger.exe	ftp.exe	ipconfig.exe
net.exe	netstat.exe	nslookup.exe	ping.exe
qbasic.exe	rcp.exe	regedit.exe	regedt32.exe
rexec.exe	route.exe	runas.exe	rsh.exe
syskey.exe	telnet.exe	tracert.exe	tftp.exe
xcopy.exe			

① 실행 파일에 대해 마우스 오른쪽 버튼을 클릭한 후 **[등록정보]**를 선택한다.

시스템 실행 파일에 대한 제한1
(그림 5-2-21)

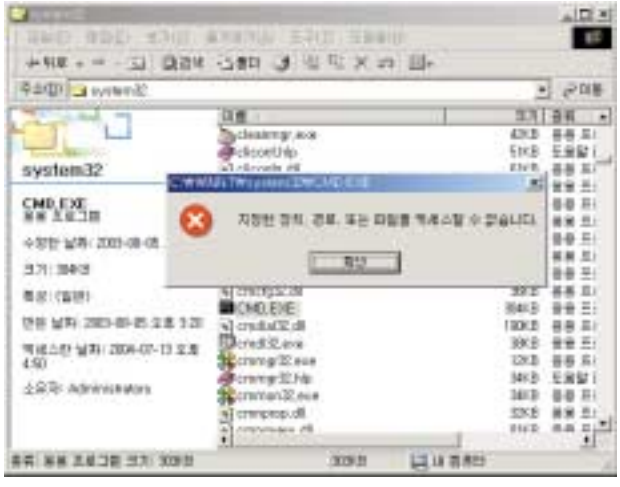
② 등록정보에서 **[보안]**탭을 선택하고 Administrator와 SYSTEM을 제외한 모든 사용자를 제거한다.

시스템 실행 파일에 대한 제한2
(그림 5-2-22)



이렇게 설정하면 해당 실행 파일을 일반 사용자권한으로 실행시키려고 할 때 다음과 같은 에러가 발생한다.

시스템 실행 파일에 대한 제한3
(그림 5-2-23)



※ 가장 많이 악용되는 IIS 취약점들은 URL을 통해 cmd.exe를 실행하도록 하는 것이다. 공격자는 cmd.exe의 파라미터로 명령어를 주어서, IIS서버에서 임의의 명령어를 실행시킨다. 이러한 공격을 막기 위한 좋은 방법은 cmd.exe를 삭제하거나, 이 파일이 필요하다면 이 파일의 위치를 다른 곳으로 옮기는 것이다. 그런데 Windows 2000에서는 WFP(Windows File Protection) 메커니즘이 cmd.exe 파일이 이동되거나 이름변경 혹은 삭제되는 경우 재배치를 수행한다. 따라서 Windows 2000에서 cmd.exe를 보호하는 가장 좋은 방법은 이 파일에 대한 접근권한을 관리자에게만 허용하는 것이다.

10. Windows 이벤트 로그 점검

- IIS는 Windows와 통합된 서비스이기 때문에, 관리자들은 웹서버 보안을 위해 IIS의 로그뿐만 아니라 Windows의 로그도 분석할 필요가 있다.
- Microsoft사에서는 IIS 5.0 보안과 관련해서 다음 정책 목록에 대해 감사를 수행하도록 권고하고 있다(Microsoft 기술자료 300549-Windows 보안 감사 설정 및 적용 참조).

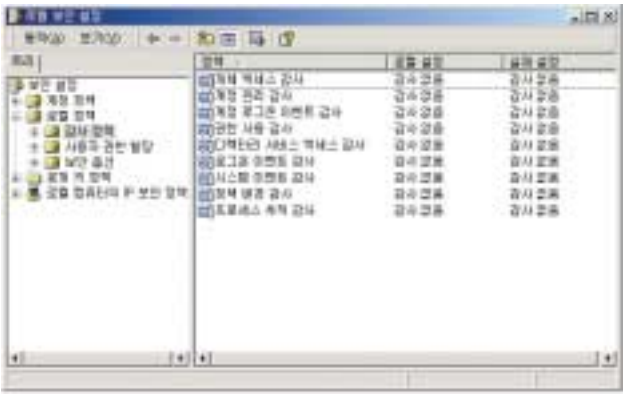
[표 5-2-4] IIS 관련 감사를 수행해야 할 정책 목록

감사를 수행할 정책목록	시 도	
	성 공	실 패
계정 로그온	사용함	사용함
계정 관리	사용 안 함	사용함
디렉터리 서비스 액세스	사용 안 함	사용함
로그온	사용함	
개체 액세스	사용 안 함	사용 안함
정책 변경	사용함	사용함
사용 권한 사용	사용 안 함	사용함
프로세스 추적	사용 안 함	사용 안 함
시스템	사용 안 함	사용 안 함

위 [표 5-2-4] 정책 목록들에 대해 감사를 설정하는 방법은 다음과 같다.

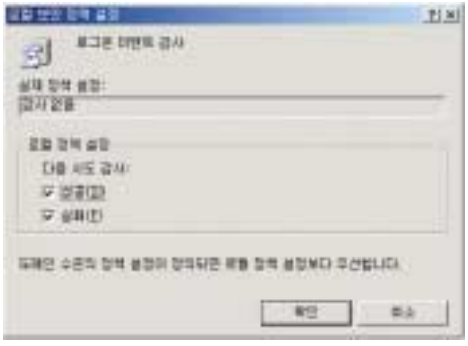
① **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[로컬 보안 정책]**을 실행시키고, **[보안 설정]** ⇨ **[로컬 정책]** ⇨ **[감사 정책]**을 선택한다.

정책 목록들에 대해 감사를 설정하는 방법1
(그림 5-2-24)

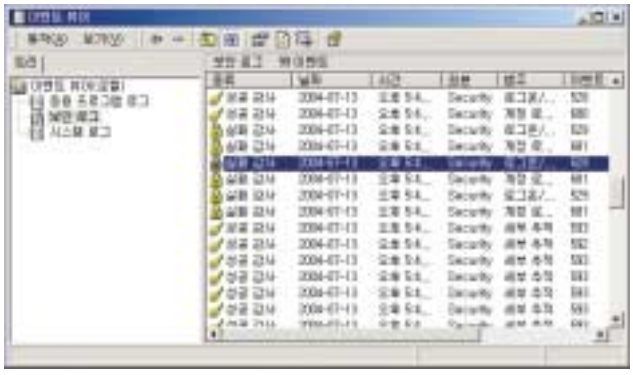


② 오른쪽 창에서 설정하거나 해제하려는 정책을 선택하여 더블클릭한다. 예를 들어 계정 로그온 이벤트 감사를 더블클릭하면 다음과 같은 설정 창이 뜬다. 여기에서 감사를 수행할 시도를 선택한다.

정책 목록들에 대해 감사를 설정하는 방법2
(그림 5-2-25)



위와 같은 방법을 통해서 제안된 모든 정책 목록에 대해 감사를 설정한 후에 잘못된 아이디와 패스워드로 로그온을 시도하면 다음과 같은 로그를 이벤트 뷰어에서 볼 수 있다. Windows의 이벤트 로그는 **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[이벤트 뷰어]**에서 볼 수 있다.



Windows의 이벤트 로그
(그림 5-2-26)

한번의 로그온 시도에 대해 두 개의 이벤트가 발생했는데, 각 이벤트를 두 번 클릭하면 다음과 같은 **[이벤트 등록 정보]**를 볼 수 있다. 첫번째로 발생한 이벤트는 컴퓨터명이 NSYNECTICS인 컴퓨터에서 utest라는 계정으로 로그온을 시도했는데 실패했다는 기록이고, 두번째로 발생한 이벤트는 로그온 실패의 원인이 알 수 없는 사용자 이름 또는 잘못된 암호라는 기록이다.

컴퓨터명이 NSYNECTICS인 컴퓨터에서 utest라는 계정으로 로그온을 시도했는데 실패한 기록
(그림 5-2-27)

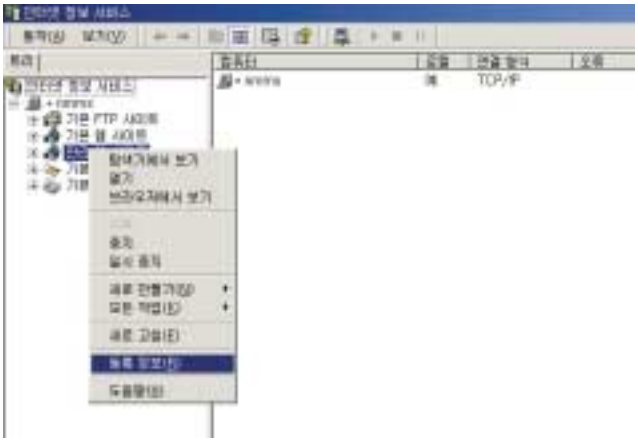
로그온 실패의 원인이 알 수 없는 사용자 이름 또는 잘못된 암호라는 기록
(그림 5-2-28)

11. HTMLA에 대한 접근 제어

- 인터넷 서비스 관리자(HTMLA)는 웹 기반의 웹서버 관리도구로서 원격에서 웹서버를 관리하는데 사용되므로 접근제어가 필요하다.

① **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[인터넷 서비스 관리자]**를 실행하고, **[관리 웹사이트]**를 마우스 오른쪽 버튼으로 클릭한 후 **[등록정보]**를 선택한다. **[등록정보]**에서 **[디렉토리 보안]** 탭을 선택하면 **[IP주소 및 도메인 이름 제한]**과 **[익명 액세스 및 인증 제어]** 기능을 설정할 수 있다.

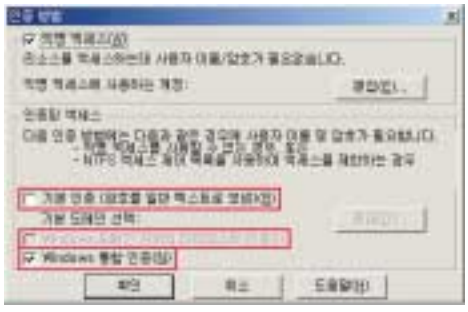
HTMLA에 대한 접근 제어2
(그림 5-2-29)



HTMLA에 대한 접근 제어3
(그림 5-2-30)

② 우선 **[IP주소 및 도메인 이름 제한]**에서 **[편집]**을 클릭하여 특정 컴퓨터(관리자PC)에서만 접근이 가능하도록 설정한다. 아래 (그림 5-2-31)처럼 기본적으로 모든 컴퓨터에 대해 **[액세스 거부]**를 설정하고, 접근을 허용할 IP주소(관리자 PC의 IP주소)를 추가한다.

③ 다음으로 관리자만 접근이 가능하도록 사용자 인증을 설정하도록 한다. **[익명 액세스 및 인증 제어]**에서 **[편집]**을 클릭하면 다음 그림과 같이 3가지 인증방법을 선택할 수 있다. (기본 인증, 다이제스트 인증, 통합인증)



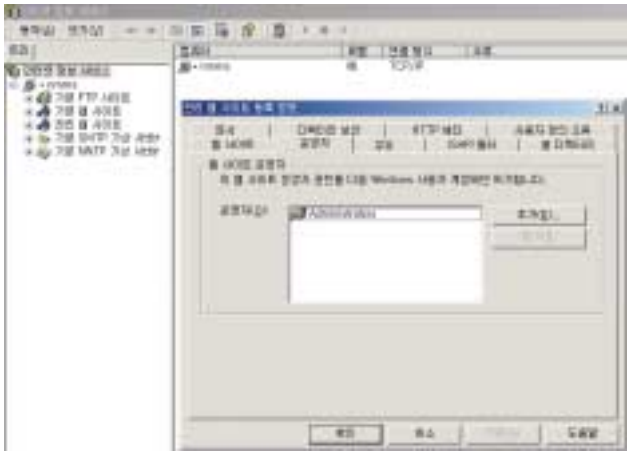
HTMLA에 대한 접근 제어4
(그림 5-2-31)

- 기본 인증방법은 암호를 평문으로 전달하기 때문에 보안상 위험하다. 다이제스트 인증은 암호를 해시값으로 전달하기 때문에 기본 인증 방법에 비해 비교적 안전하다.

- 통합인증은 브라우저로 반드시 익스플로러만을 사용해야 한다는 단점이 있다.은 네트워크를 통해 암호를 전달하지 않고 자신이 암호를 알고 있음을 증명하는 방식이기 때문에 보안상 안전하다.
- 따라서 가급적 인증방법을 다이제스트 인증이나 통합인증을 선택하도록 한다.

④ 웹사이트 운영자 권한은 가능하면 기본설정인 Administrators만 허용하도록 한다.

HTMLA에 대한 접근 제어5
(그림 5-2-32)



12. 기본 문서 설정

- 기본 문서는 브라우저 요청에서 디렉토리만 지정하고 문서 이름을 지정하지 않았을 때 기본적으로 보여지는 문서를 말한다. 예를 들어 기본 문서로 default.htm이 지정되어 있는 경우 http://your.server.com/info/를 요구하면 IIS는 http://your.server.com/info/default.htm을 리턴해 준다.
- 기본 문서를 설정하기 위해서는 **[시작]** ➪ **[프로그램]** ➪ **[관리 도구]** ➪ **[인터넷 정보 서비스]**를 실행시키고, **[기본 웹 사이트]**에 대해 마우스 오른쪽 버튼을 클릭한 후 **[등록정보]**를 선택한다. 아래 (그림 5-2-33)과 같이 **[등록정보]**에서 **[문서]**탭을 선택하면, 기본 문서를 추가 혹은 제거할 수 있다.

기본 문서 설정
(그림 5-2-33)

- 기본 문서가 여러 개 지정된 경우 리스트에서 상위에 있는 문서가 우선 순위가 높다. 위 그림의 경우 Default.htm이 존재하면 그 파일을 리턴해주고, Default.htm이 존재하지 않으면 Default.asp 파일을 리턴해 준다. Default.asp 파일도 없으면 iisstart.asp 파일을 찾아서 리턴해준다.
- 그런데 여기서 리스트의 순서에 주의해야 한다. 위와 같이 설정한 상태에서 디렉토리에 Default.asp 파일만 존재하고 Default.htm 파일이 존재하지 않는 경우, 만약 공격자가 Default.htm 파일을 업로드 한다면 관리자가 의도했던 Default.asp 대신 공격자가 업로드 한 Default.htm 파일이 처리된다.

따라서 기본 문서의 목록이 적절하게 배열되어 있는지 점검하도록 한다.

13. 모든 예제 응용 프로그램을 제거

IIS를 설치하면 기본적으로 예제와 설명서 등이 같이 설치된다. 이 폴더들은 해킹에 이용되거나 백도어가 심어질 위험이 있으므로 제거해 주어야 한다. [표 5-2-5]는 IIS 예제들이 저장되는 기본 위치이다.

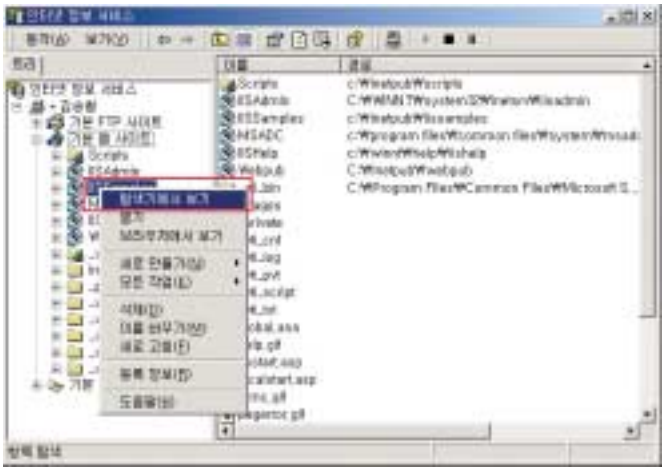
[표 5-2-5] IIS 예제 응용프로그램의 위치

예 제	가상 디렉토리	위 치
IIS 예제	\IISSamples	c:\inetpub\iissamples
IIS 설명서	\IISHelp	c:\winnt\help\iishelp
데이터 액세스	\MSADC	c:\program files\common files\system\msadc

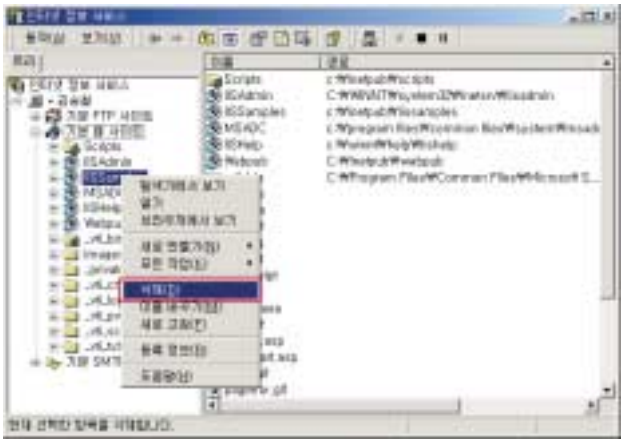
이러한 가상 디렉토리와 실제폴더를 삭제하는 방법은 다음과 같다.

① **[인터넷 서비스 관리자]**에서 삭제하려는 가상 디렉토리 (여기에서는 IISSamples)를 선택하고, 마우스 오른쪽 버튼을 클릭한 후 **[탐색기에서 보기]**를 선택하면 해당 디렉토리를 보여주는 탐색기 창이 뜨게 된다.

가상 디렉토리와 실제폴더를 삭제하는 방법1
(그림 5-2-34)



② 우선 **[인터넷 서비스 관리자]**에서 다음과 같이 가상 디렉토리를 삭제한다.



가상 디렉토리와 실제 폴더를 삭제하는 방법2
(그림 5-2-35)

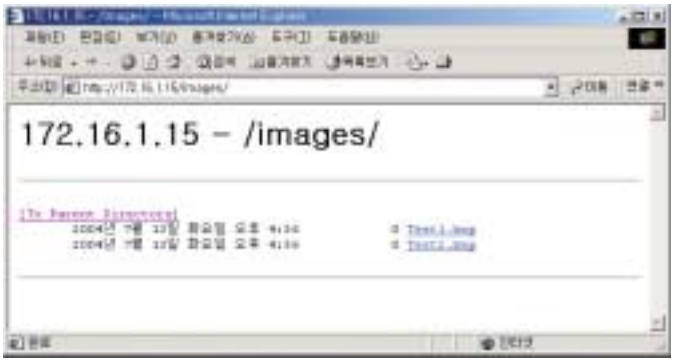
③ 그리고 나서 탐색기로 열어두었던 실제 디렉토리도 제거한다.

가상 디렉토리와 실제 폴더를 삭제하는 방법3
(그림 5-2-36)

14. 디렉토리 목록 검색방지

- 디렉토리 검색은 검색페이지로 디렉토리명이 지정되었을 때 해당 디렉토리에 기본 문서가 존재하지 않을 경우 디렉토리 내에 존재하는 파일 목록을 보여주는 것을 말한다.

디렉토리 검색
(그림 5-2-37)

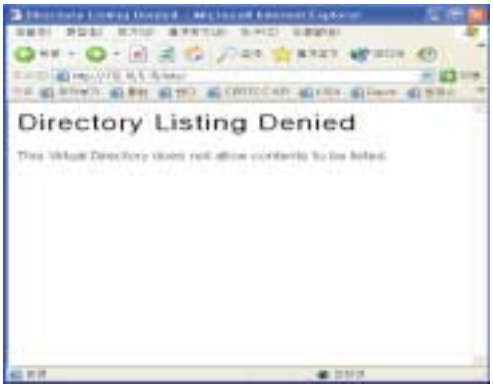


디렉토리 검색이 허용되면 외부에서 디렉토리 내의 모든 파일에 대한 접근이 가능하여 백업 파일이나 소스 파일 등 공개되어서는 안되는 중요한 파일들이 노출될 수 있다. 따라서 다음과 같은 방법으로 디렉토리 검색이 불가능하도록 설정한다.

[시작] ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[인터넷 정보 서비스]**를 실행시킨 후 **[기본 웹 사이트]**에 대해 마우스 오른쪽 버튼을 클릭한 후 **[등록정보]**를 선택한다. **[디렉토리]**탭에서 **[디렉토리 검색]**을 다음 그림과 같이 체크되지 않은 상태를 유지하도록 한다.

디렉토리 목록 검색 방지 설정
(그림 5-2-38)

이렇게 하면 해당 디렉토리 접근시 접근불가 메시지가 나타난다.



디렉토리 접근시 접근불가 메시지
(그림 5-2-39)

15. 익명 사용자 계정 권한 제한

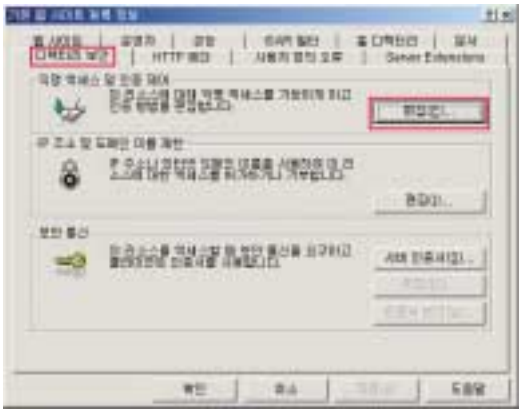
- 익명 사용자 계정은 익명 액세스를 허용하는 경우에 방문자가 사용하게 되는 Windows 2000 사용자 계정이다. 기본적으로 IIS를 설치하면 IUSR_서버이름 계정이 생성된다. IUSR_서버이름 계정은 가장 제한적인 권한만을 갖고 있어야 한다.

익명 사용자 계정은 다음 위치에서 설정할 수 있다.

① **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[인터넷 정보 서비스]**를 실행하고, 기본 웹 사이트에 대해 마우스 오른쪽 버튼을 클릭한 후 **[등록정보]**를 선택한다.

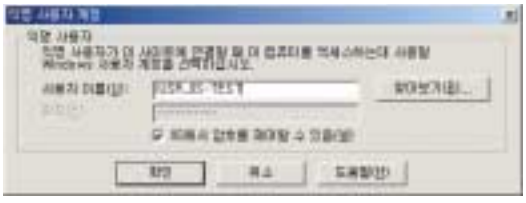
② **[기본 웹 사이트 등록 정보]** ⇨ **[디렉토리 보안]** ⇨ **[익명 액세스 및 인증 제어]** ⇨ **[편집]** 버튼을 클릭한다.

익명 사용자 계정 설정1
(그림 5-2-40)



③ 명 사용자 이름이 디폴트로 IUSR_서버이름으로 설정되어 있는 것을 볼 수 있다. 익명 사용자 이름으로 권한 있는 계정을 설정하지 않도록 유의한다.

익명 사용자 계정 설정2
(그림 5-2-41)



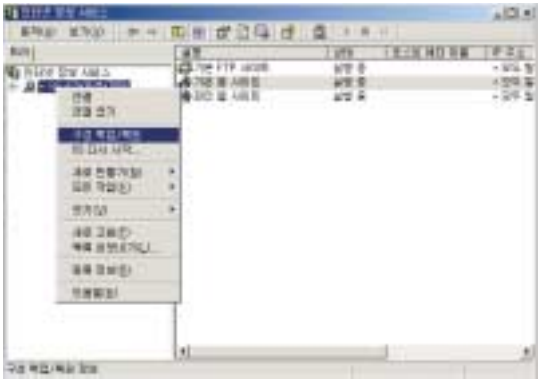
여기에서 **[IIS에서 암호를 제어할 수 있음]**을 선택하면 사용자 관리자에서 IUSR_서버이름 계정의 암호를 변경할 경우 자동으로 수정된 암호가 웹사이트에 반영된다. 이 옵션을 선택하지 않으면 사용자 관리자에서 익명 사용자 계정의 암호를 변경할 때 이곳에서도 암호를 변경해 주어야 한다.

IIS 익명 액세스에 사용되는 계정의 이름을 IUSR_서버이름에서 다른 이름으로 변경하여 외부에서 추측할 수 없도록 하는 것이 좋다. 그리고 이 계정에 대한 원격 로그인이 불가능하도록 설정하는 것이 좋다.

16. 웹서버의 설정값 백업

IIS는 설정정보를 IIS 메타베이스에 저장한다. 메타베이스는 Windows 레지스트리와 비슷하지만 IIS에 한정된다. IIS가 재설치 되거나 재설정되어야 하는 경우, 백업받은 메타베이스를 이용해서 빠르게 IIS를 원상 복구할 수 있다. 메타베이스의 백업 및 복원 방법은 다음과 같다.

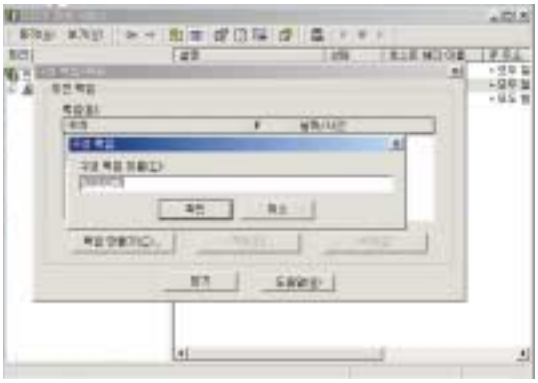
① **[시작]** ⇨ **[프로그램]** ⇨ **[관리 도구]** ⇨ **[인터넷 정보 서비스]**를 실행하고, 서버를 마우스 오른쪽 버튼으로 클릭한 후 **[구성 백업/복원]** 메뉴를 선택한다.



메타베이스의 백업 및 복원 방법1
(그림 5-2-42)

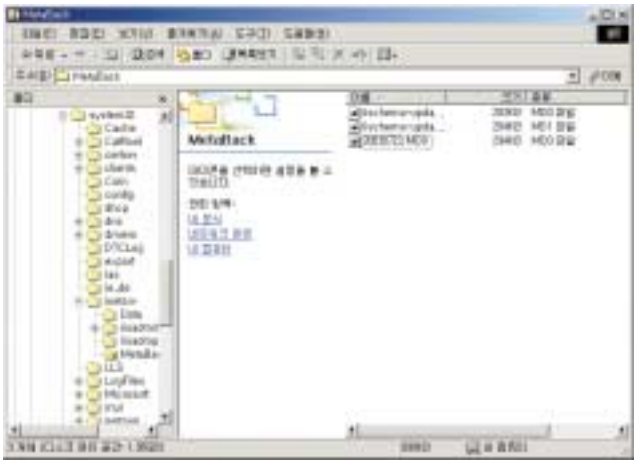
② **[구성 백업/복원]** 대화상자에서 **[백업 만들기]**버튼을 클릭하면 (그림 5-2-43)과 같은 구성 백업 대화상자가 나타난다. 현재 웹 서비스의 설정을 저장할 파일의 이름을 입력한다. 여기에서는 백업날짜를 입력하였다. **[확인]**버튼을 누르고 백업 목록에 백업 파일이 만들어진 것을 확인한 후 **[닫기]**버튼을 클릭하여 상자를 닫는다.

메타베이스의 백업 및 복원 방법2
(그림 5-2-43)



메타베이스 백업 파일은 C:\WINNT\system32\inetsrv\MetaBack에 저장된다.

메타베이스의 백업 및 복원 방법3
(그림 5-2-44)



복원은 백업절차와 동일하다. **[구성 백업/복원]** 대화상자에서 **[백업 만들기]** 버튼 대신 **[복원]** 버튼을 누르면 된다.

IIS 설정의 백업은 허가받은 관리자만 접근할 수 있는 안전한 영역에 저장되어야 한다.

제3절 메일서버 보안관리

1. MS Exchange 서버

Microsoft Exchange 서버는 윈도우즈 서버 사용자가 가장 손쉽게 MS IIS와 함께 메일서버를 구축할 수 있는 방법이다. 기본적으로 Exchange 2000을 설치하기 위해서는 Windows 2000이상의 운영체제, 서비스팩 1 이상 설치 및 AD(Active Diretory), IIS(SMTP포함), NNTP가 설치되어 있는 시스템이 필요하다.

가. Exchange 서버 설치

- 컴퓨터에 Exchange CD-ROM을 넣고 자동실행 화면이 나타나면 "Exchang Server Setup"을 선택한다.

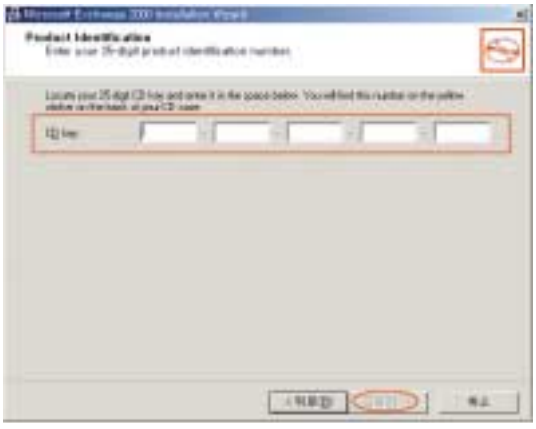
MS Exchange서버 자동실행화면
(그림 5-3-1)

● (그림 5-3-2)와 같이 라이센스 동의 관련 화면이 나오면 "I agree"를 체크하고 다음을 클릭한다.

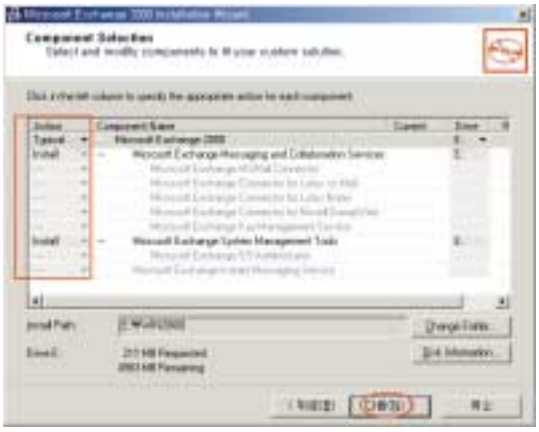
라이센스 동의화면
(그림 5-3-2)

● (그림 5-3-3)에 CD Key 값을 입력한다.

일련번호(시리얼 번호) 입력
(그림 5-3-3)



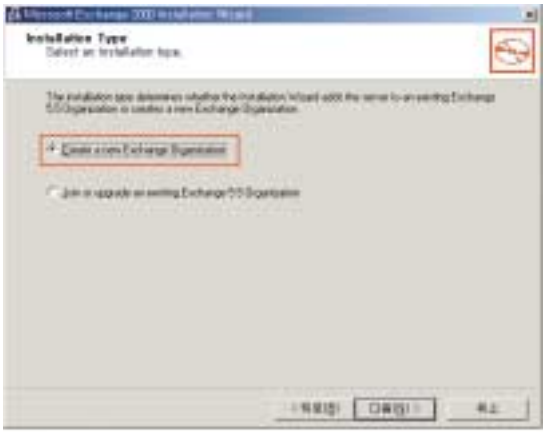
● 설치구성요소를 선택하기 위한 (그림 5-3-4)의 설치방법 선택 화면이 나타나면 설치방법을 선택하며, 일반적으로 Typical 설치를 권장한다.



설치구성요소 선택화면
(그림 5-3-4)

- Typical : 일반적인 설치방법
- Minimum : 최소설치
- Custom : 설치자가 선택해서 설치
- (그림 5-3-4)와 같이 설치타입을 선택하는 화면이 나타나는데, 새로 설치할 것인지 기존의 Exchange 5.5를 2000으로 업그레이드하거나 동시에 사용할지를 선택한다. 본 문서에서는 "새로 설치"를 선택하여 진행하도록 한다.

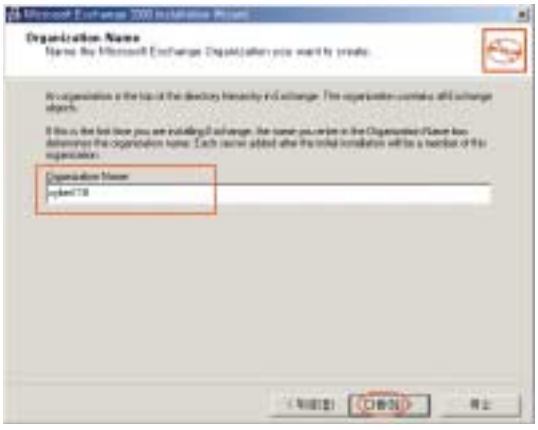
※ Typical 설치 후 추가하고자 하는 구성요소가 있는 경우에도, 신규옵션을 사용하여 추가 설치가 가능하다.



설치타입 지정화면
(그림 5-3-5)

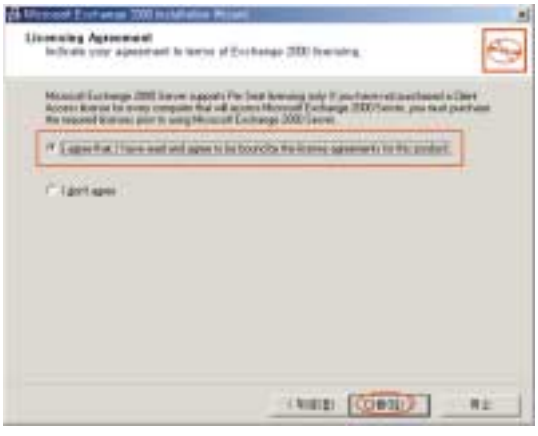
● Organization Name(조직 이름) 입력

조직 이름 입력화면
(그림 5-3-6)

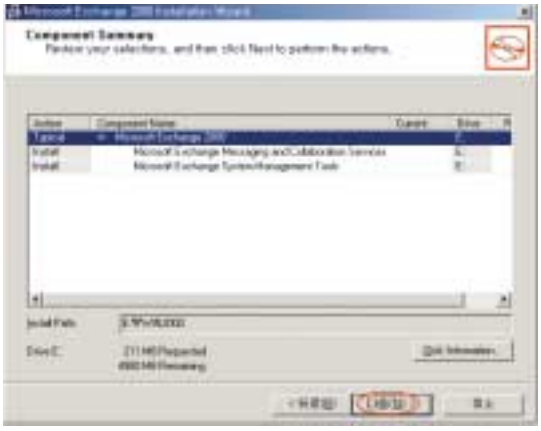


● (그림 5-3-7)과 같은 라이센스 동의 화면이 나타나면, Exchange 2000은 클라이언트 라이센스에 사용자 단위 라이센스만을 허용하며 Exchange 2000을 사용하기 위해서는 클라이언트 수만큼의 라이센스를 구입하여야 한다는 내용에 동의한다.

클라이언트 라이센스 동의 화면
(그림 5-3-7)



● 설치과정에서 선택한 모든 설치 구성요소가 적절히 표시되었는지 (그림 5-3-8)에서 최종 확인

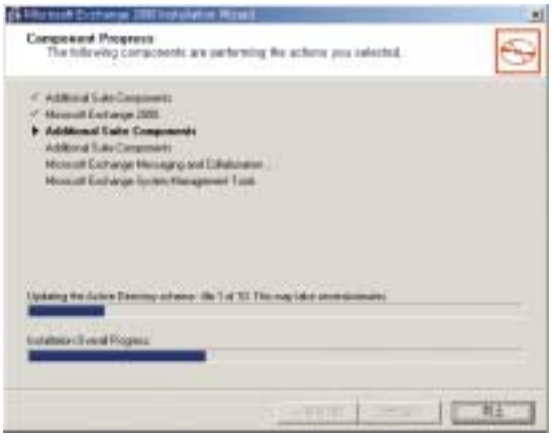


최종 설치구성요소 확인
(그림 5-3-8)

● (그림5-3-9)에서 **[확인]**을 눌러 설치 마법사를 실행한다.

설치마법사 실행화면
(그림 5-3-9)

● Exchange 2000에 필요한 파일 복사 등 설치과정



설치화면
(그림 5-3-10)

● 설치완료

MS Exchange 설치완료
(그림 5-3-11)

나. Spam Mail Relay 방지

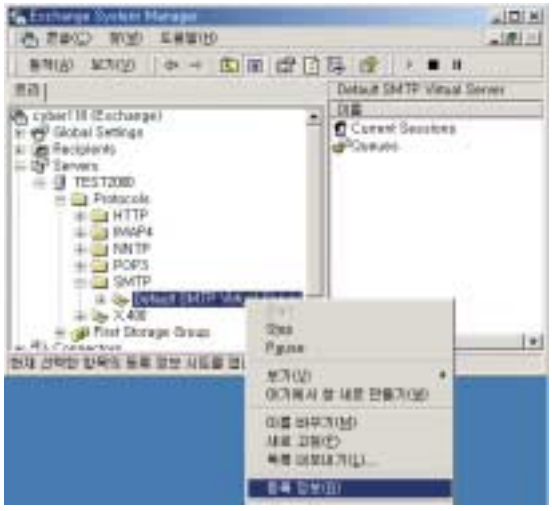
스팸릴레이 방지 설정을 하지 않아 운영하는 메일서버가 스팸 메일 발송서버로 악용되는 사례가 많다. 이는 단순히 스팸메일 발송 사실뿐만 아니라 다량의 메일을 처리하여 메일서버 자체에 부하를 증가시킴으로써 정상적인 메일서버 동작을 방해한다.

● (그림 5-3-12)과 같이 시스템 관리자를 실행한다.

[시작] ➪ [프로그램] ➪ [Microsoft Exchange] ➪ [System Manager]

시스템 관리자 실행화면
(그림 5-3-12)

● (그림 5-3-13)에 나타난 바와 같이 “Servers” 하위에 있는 서버명을 더블 클릭하고 “Potocols” 하위에 있는 항목 중 “SMTP” 더블 클릭한다. 그리고 “Default SMTP Virtual Server” 등록 정보를 연다.



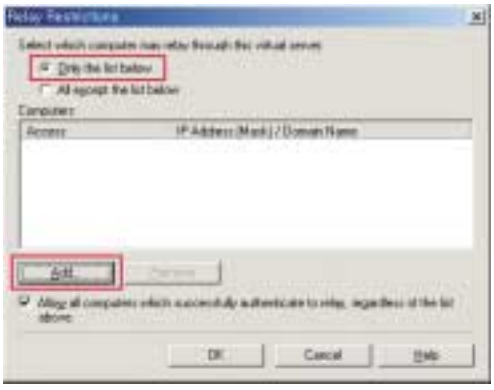
서버의 등록정보 메뉴
(그림 5-3-13)

● (그림 5-3-14)에 나타난 바와 같이 [Access] 선택 후 아래 부분에 있는 [Relay] 버튼 클릭

릴레이 설정 메뉴
(그림 5-3-14)

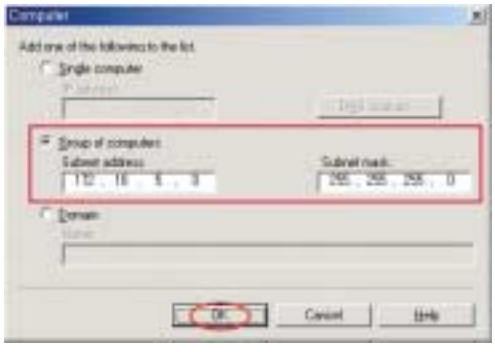
● 관리자가 지정하는 IP주소 또는 IP영역의 사용자만이 릴레이 기능을 이용할 수 있도록 (그림 5-3-15)의 [Only the list below]를 체크 한 후 아래 부분에 있는 [Add] 버튼 클릭

릴레이 허용 대상 추가 화면
(그림 5-3-15)



● 중간에 있는 [Group of computers] 체크 후 릴레이를 허용할 [Subnet address] 와 [Subnet mask] 값 입력 후 [OK] 버튼 클릭

릴레이 허용 대상 지정
(그림 5-3-16)



(※ 허용지정대상 이외의 시스템은 모두 릴레이 기능이 방지됨)

2. Sendmail 서버

Sendmail은 Linux나 Solaris 등 유닉스 시스템에서 메일을 교환하기 위하여 사용하는 프로그램이다. 여기에서는 Linux에서 소프트웨어 설치 관리시스템인 rpm을 사용하여 서버를 구축하는 방법과, Sun사의 솔라리스에서 소스파일을 사용하여 sendmail 서버를 안전하게 구축하는 방법을 설명한다.

가. Linux에서 rpm으로 Sendmail설치

(1) 설치

- Sendmail 설치 확인
  Linux 운영체제를 설치하면 대부분 Sendmail은 기본으로 설치된다. Sendmail이 설치되어 있는지는 다음과 같이 rpm명령어를 사용하여 확인할 수 있다.

```
# rpm -qalgrep sendmail
sendmail-doc-8.11.6-3
sendmail-cf-8.11.6-3
sendmail-8.11.6-3
```

- Sendmail 프로그램의 다운로드
  Sendmail 프로그램은 해당하는 Linux 배포판 사이트에서 rpm으로 다운받을 수 있다. Redhat Linux의 경우 아래의 사이트에서 최신 버전의 프로그램을 다운받을 수 있다. 이 문서에서는 sendmail-8.12.8을 기준으로 설명한다.

- rpm으로 sendmail 패키지 설치
  rpm으로 다운받은 Sendmail은 -Uvh옵션을 써서 설치한다.

```
# rpm -Uvh sendmail*
Preparing...                ########################################### [100%]
   1:sendmail               ########################################### [ 33%]
   2:sendmail-cf            ########################################### [ 66%]
   3:sendmail-doc           ########################################### [100%]
```

● 설치된 정보 확인

```
# rpm -qi sendmail
Name        : sendmail                     Relocations: (not relocatable)
Version     : 8.12.8                       Vendor: Red Hat, Inc.
Release     : 4     Build Date: 2003년 02월 25일 (화) 오전 09시 16분 00초
Install date: 2003년 06월 27일 (금) 오후 11시 56분 04초
Build Host: stripples.devel.redhat.com
Group:시스템 환경/ 데몬들
Source RPM: sendmail-8.12.8-4.src.rpm
Size        : 4389045                                 License: BSD
Signature   : DSSA/SHA1, 2003년 02월 25일 (화) 오루 01시 30분 42초, Key ID    219180cddb42a60e
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : 널리 사용되는 메일 전송 에이전트 (MTA).
Description :
The Sendmail program is a very widely used Mail Transport Agent (MTA).
MTAs send mail from one machine to another. Sendmail is not a client program,   which you use to read
your email. Sendmail is a behind-the-scenes program which    actually moves your email over networks or
the Internet to where you want it to go.

If you ever need to reconfigure Sendmail, you will also need to have the  sendmail.cf package installed. If
you need documentation on Sendmail, you can    install the sendmail-doc package.
```

설치후 /etc/services 파일을 열고 25번 포트(smtp) 주석처리가 되어 있는지 확인한다.

```
# more /etc/services|grep smtp
smtp          25/tcp          mail
smtp          25/udp          mail
smtps         465/tcp         # SMTP over SSL (TLS)
```

● Sendmail 데몬 시작

```
# /etc/rc.d/init.d/sendmail start
Starting sendmail: [  OK  ]
```

Sendmail 서버가 정상적으로 설치되었는지 확인하기 위해 telnet을 사용해 25번 포트(smpt)로 접속해 본다. 아래와 같은 메시지가 출력되면 Sendmail이 정상적으로 설치된 것이다.

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.12.8/8.12.8; Wed, 17 Mar 2004 10:56:33 +0900
quit
221 2.0.0 localhost.localdomain closing connection
Connection closed by foreign host.
```

(2) Sendmail 환경 설정

● sendmail.cf 생성

Sendmail의 설치가 끝나면 서버의 구성파일인 sendmail.cf 파일을 다음의 명령을 사용하여 구성한다.

```
# m4 /etc/mail/sendmail.mc> /etc/sendmail.cf
```

구성이 모두 끝났으면 sendmail을 재 시작한다.

```
# /etc/rc.d/init.d/sendmail restart
```

● /etc/sendmail.cf 파일 내용 확인

/etc/sendmail.cf는 Sendmail의 가장 중요한 설정파일로 sendmail이 메일을 보내고 받을 때마다 /etc/sendmail.cf 파일을 참조한다. 다음의 구성 예는 메일서버를 관리하기 위하여 중요한 설정들이다.

- Fw/etc/mail/local-host-names

  메일을 수신할 호스트 이름을 명시한 파일의 위치를 지정한다.

- FR-o /etc/mail/relay-domains

  relay-domains파일에는 Relay를 허용할 호스트의 이름을 설정하는데 주석으로 처리하면 모든 IP에 대해서 Relay가 허용되므로 주의하여야 한다.

- DnMAILER-DAEMON

  Sendmail 서버가 에러메시지를 보내야 할 경우 보낸 사람의 이름을 결정한다. 잘못된 메일이 되돌아 온 경우 "FROM : Mail Delivery Subsystem &ltMAILER-DAEMON〉"과 같은 메시지를 보여준다.

- Kaccess hash -o /etc/mail/access.db

  Relay를 허용하거나 거부할 특정 IP와 도메인을 설정하는 파일이며 relay-domains보다 사용이 편리하므로 많이 사용된다.

- O ForwardPath=$z/.forward.$w:$z/.forward

  특정 메일계정으로 들어온 메일을 다른 계정으로 전달하기 위한 포워딩 파일을 지정한다. 이 예제는 사용자의 홈 디렉토리에 .forward라는 파일을 만들고 내용에 포워딩시킬 메일 주소를 입력하면 된다.

- O MaxMessageSize=1000000

  메일의 최대 크기를 지정하며 지정한 크기(Byte단위)보다 큰 메일은 전송할 수 없게 된다. 이 예는 1000000 바이트, 즉 1메가바이트 이상의 메일을 보낼 수 없도록 설정한 예이다.

- O QueueDirectory=/var/spool/mqueue

  메일 큐 디렉토리를 지정한다.

- O Timeout.initial=5d

  이것은 Sendmail이 메일을 보내려고 시도하는 기간을 설정하는 옵션이다. 메일 수신측 호스트에 문제가 생기면 메일은 큐 디렉토리에 저장된다. Sendmail 서버는 쌓인 메일을 보내기 위해 상대방 호스트에 주기적으로 접속을 시도하며, 정해진 기간이 지나면 (이 예제에서는 5일) 메일을 다시 발송한 사람에게 되돌려 보낸다.

- O Timeout.queuewarn=4h

  큐에 쌓인 메일이 지정한 시간 안에 전송되지 못할 경우 메일을 보낸 사람에게 경고 메일을 발송한다. 기본값은 4h로 4시간 내에 전송되지 못하면 보낸 사람에게 경고 메일이 발송된다.

나. SunOS 5.7, Solaris 7 에서 소스파일로 Sendmail 설치

(1) 설치

● 프로그램 다운로드

Sendmail의 소스 패키지는 www.sendmail.org에서 소스파일을 다운받을 수 있다. 이 예제에서는 sendmail.8.12.9를 설치하도록 한다.

www.sendmail.org 사이트
(그림 5-3-17)

다운로드 한 sendmail.8.12.9.tar.gz 파일을 설치하고자 하는 Sendmail 서버로 전송한다 (설치 디렉토리는 상관없음).

● gzip과 tar명령어를 사용하여 압축을 해제한다.

```
# gunzip sendmail.8.12.9.tar.gz
# tax xvfp sendmail.8.12.9.tar
```

● Sendmail에서는 Build라는 컴파일용 쉘 스크립트를 제공하므로 설치 디렉토리에서 "sh Build" 명령의 실행을 통하여 Sendmail 설치환경을 구성한다.

```
# sh Build
```

● Sendmail의 configuration file 설치

- 설치디렉토리의 하위 디렉토리인 cf/cf디렉토리는 Sendmail의 구성파일을 생성하기 파일들이 존재한다. .mc 파일은 sendmail.cf 파일을 생성하는데 사용되며 OS 별로 적합한 .mc파일이 각각 존재하므로 설치하고자 하는 시스템과 부합하는 .mc파일을 선택하여 sendmail.mc로 복사한다(SunOS 5.7인 경우).
- SUN Solaris 2.X버전은 generic-solaris2.mc 파일을 사용한다.

sendmail-8.12.9/cf/cf 디렉토리에서

```
# ls
./              cs-solaris2.mc   generic-hpux9.mc        generic-sunos4.1.cf
../             cs-sunos4.1.mc   generic-linux.cf        generic-sunos4.1.mc
Build*          s2k-osf1.mc      python.cs.mc            cs-ultrix4.mc
generic-linux.mc  generic-ultrix4.cf  s2k-ultrix4.mc     Makefile
cyrusproto.mc   generic-ultrix4.mc  tcpproto.mc          cs-hpux9.mc
chez.cs.mc      generic-bsd4.4.cf   huginn.cs.mc         ucbarpa.mc
clientproto.mc  generic-bsd4.4.mc   generic-osf1.cf      knecht.mc
cs-hpux10.mc    generic-hpux10.cf   generic-osf1.mc      mail.cs.mc
```

```
generic-hpux10.mc       generic-solaris2.cf     mail.eecs.mc        vangogh.cs.mc
cs-osf1.mc              generic-hpux9.cf        ucbvax.mc           mailspool.cs.mc
generic-nextstep3.3.mc generic-nextstep3.3.cf generic-solaris2.mc uucpproto.mc


# cp generic-solaris2.mc sendmail.mc
```

● 생성된 sendmail.mc파일을 사용하여 sendmail.cf파일을 생성한다.

```
# sh Build sendmail.cf
Using M4=/usr/ccs/bin/m4
rm -f config.cf
/usr/ccs/bin/m4 ../m4/cf.m4 config.mc 〉 config.cf ll ( rm -f config.cf && exit 1 )
chmod 444 config.cf
```

● 구버전의 /etc/mail/sendmail.cf 파일을 백업한다.
- 일부 시스템은 /etc/sendmail.cf 파일을 사용하므로 주의하여야 함
- cp, mv, tar 등의 명령어를 사용

```
[penguin:root]:/etc/mail/cp sendmail.cf /백업디렉토리/sendmail.cf
[penguin:root]:/etc/mail/mv sendmail.cf /백업디렉토리/sendmail.cf
```

● 설치된 sendmail/ 디렉토리에서 “sh Build install”명령 실행한 후에 새로 만들어진 sendmail.cf 파일과 submit.cf 파일을 각각 /etc/mail sendmail.cf 와 /etc/mail/submit.cf로 설치한다. 이때 cp 명령을 사용하거나 “sh Build install-cf” 명령을 사용할 수 있다.

```
# sh Build install
Making all in:
/user1/ksch/sendmail-8.11.6/libsmutil
Configuration: pfx=, os=SunOS, rel=5.7, rbase=5, rroot=5.7, arch=sun4, sfx=, variant=optimized
.....
```

```
# cp ./cf/cf/config.cf /etc/mail/sendmail.cf
 또는

# sh Build install-cf
Using M4=/usr/sbin/m4
../../devtools/bin/install.sh -c -o root -g bin -m 0444 sendmail.cf /etc/mail/sendmail.cf
../../devtools/bin/install.sh -c -o root -g bin -m 0444 submit.cf /etc/mail/submit.cf
```

- Sendmail과 관련된 도구들(makemap, mailstats 등)을 설치
  각 도구들이 위치한 디렉토리에서 README 파일을 참고하여 "sh Build install"을 실행하여 관련 파일들을 설치한다.

```
[penguin:root]:/user1/ksch/sendmail-8.11.6/makemap〉 ls
./    ../   Build*     Makefile   Makefile.m4
makemap.0     makemap.8     makemap.c
[penguin:root]:/user1/ksch/sendmail-8.11.6/makemap〉sh Build install
```

- 새로운 버전의 makemap도구를 사용하여 Database Maps을 생성한다.
- /etc/mail/local-host-names파일을 생성하여 메일서버의 호스트명을 입력한다.

```
[penguin:root]:/etc/mail〉 cat local-host-names
penguin                 〈== 메일서버의 호스트 이름
penguin.certcc.or.kr        〈== 메일서버의 도메인 이름
```

- Sendmail의 컴파일 및 설치에 대한 상세한 자료는 다음 페이지를 참조한다.
  - http://www.sendmail.org/compiling.html
  - http://www.plus.or.kr/document/etc/sendmail.html
  - http://www.superuser.co.kr/

3. 메일 릴레이 제한하기

가. /etc/mail/relay-domains를 이용하여 relay 제한하기

Sendmail 8.9.x 이상의 버전은 허가받지 않은 메일의 중계(relaying)는 기본적으로 거부하게 되어 있다. /etc/mail/relay-domains의 목적은 중계를 허용할 도메인 목록을 지정한다. 이 파일은 sendmail을 설치하였을 때 기본적으로 생성되지 않으므로 touch나 vi 등으로 만들어야한다.
자신의 도메인과 중계를 허용할 도메인은 이 파일에 지정해 두어야 하며 IP 주소를 사용할 수도 있다. 또한, Sendmail이 relay를 허용하고 있는 도메인리스트의 확인은 다음과 같이 할 수 있다.

```
# echo '$=R' | sendmail -bt
```

나. /etc/mail/access를 이용하여 Spam 메일 방지하기

/etc/mail/access 파일은 특정 IP 또는 Domain 또는 Email Address 및 네트워크에 대하여 Sendmail에 접근하지 못하도록 제한을 설정할 수 있는 파일이며, 다음과 같은 방법으로 제한을 설정할 수 있다.

- 특정 IP Address로부터 오는 메일
- 특정 Email Address로부터 오는 메일
- 특정 Domain으로부터 오는 메일

즉, 스팸메일 발송자의 Email 주소나 스팸메일 발송에 사용되는 서버의 IP Address를 등록하여 스팸메일을 발송하는 것을 방지할 수 있다.

- /etc/mail/access파일 등록형식 및 방법

메일 릴레이를 특별히 설정하지 않은 구성파일은 다음과 같다. 여기서 왼쪽부분은 특정 호스트

네임, 도메인, IP 주소, 네트워크 IP주소 등을 입력하고, 오른쪽 부분은 왼쪽에 적은 호스트나 IP 주소에 대한 접근을 제어하는 옵션 명령어를 기재한다.

```
# cat access
# Check the /usr/share/doc/sendmail-8.11.6/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail-8.11.6/README.cf is part of the sendmail-doc
# package.
#
# by default we allow relaying from localhost...
localhost.localdomain          RELAY
localhost                      RELAY
127.0.0.1                      RELAY

spam@hacker.com REJECT
spammail.com REJECT
useful.org OK
211.252.150 RELAY
211.252.151 RELAY
```

위의 구성 예는 다음과 같은 의미를 가진다.

- spam@hacker.com의 메일사용자 및 spammail.com 도메인으로 부터 오는 모든 메일은 거절
- useful.org 도메인으로부터 오는 모든 메일은 받아들인다는 설정
- 마지막의 것은 C-Class의 네트워크가 211.252.150, 211.252.151의 IP를 사용하는 모든 IP 주소에서 발송한 메일의 릴레이를 허용한다.

위와 같은 형식의 access DB는 텍스트 파일로 Sendmail이 참조할 수 없으므로 다음과 같이 makemap 프로그램을 사용하여 Sendmail이 인식할 수 있는 DB 형태로 만들어 주어야 한다.

```
#/etc/mail/makemap hash /etc/mail/access < /etc/mail/access
```

※ 참고자료

- Sendmail 메일서버의 스팸릴레이 방지 설정 방법

  http://www.certcc.or.kr/paper/tr2002/tr2002_04/sendmail_spam.htm

- 메일서버의 스팸릴레이 방지 설정 방법

  http://www.certcc.or.kr/paper/tr2002/tr2002_04/spam.htm

- 메일서버의 스팸릴레이 시험방법 및 대응방법

  http://www.certcc.or.kr/paper/tr2001/tr2001-06/spam_relay_test.pdf

  http://www.superuser.co.kr/

제4절 DNS서버

도메인이란 숫자로 표현되는 IP 주소를 알아보기 쉬운 형태를 가진 알파벳 이름으로 표현해 주는 것을 말한다[9]. 보통 우리는 인터넷에 연결된 컴퓨터를 지정할 때 www.test.co.kr과 같이 표현되는 FQDN (Fully Qualified Domain Name) 형태의 주소를 사용한다. 그러나 이와 같은 형태의 주소는 대상 컴퓨터에 접속하는데 그대로 사용할 수 없고 반드시 숫자로 표현되는 IP 주소로 변환되어야 한다.
이와 같이 알파벳 형태로 표현된 컴퓨터 이름을 IP 주소로 변환하기 위하여 DNS 서버를 사용한다. DNS 서버는 윈도우즈에서 지원되는 기능을 사용하거나 유닉스 운영체제의 BIND를 사용하여 구축한다.

1. Windows DNS 서버

가. Windows DNS 설치

Windows 2000이나 WinNT 설치시에 DNS 서비스는 기본적으로 설치되는 것이 아니기 때문에 직접 설치해 주어야 하는데, 다음과 같은 순서로 진행하면 간단히 DNS를 설치할 수 있다. DNS 설치파일들이 Windows 설치 CD에 포함되어 있기 때문에 Administrator 또는 관리자 권한이 있는 계정으로 로그인한 뒤 다음과 같이 진행하면 된다.

9) 윈도우즈 운영체제의 도메인은 인터넷 도메인과 다른 의미로 사용된다. 윈도우즈 운영체제의 도메인이란 관리의 편의를 위하여 설정되는 컴퓨터들의 집합을 의미한다.

▶ Windows NT에서 설치

- [시작] ⇨ [설정] ⇨ [제어판] 클릭
- [네트워크] ⇨ [서비스] ⇨ [추가] 클릭
- [Microsoft DNS서버] ⇨ [확인] 클릭 후 리부팅

▶ Windows 2000에서 설치

- [시작] ⇨ [설정] ⇨ [제어판] 클릭
- [프로그램 추가/제거] ⇨ [Windows 구성 요소 추가/제거] 클릭
- 'Windows 구성 요소 마법사' 가 시작되면, [네트워킹서비스] ⇨ [자세히] 클릭

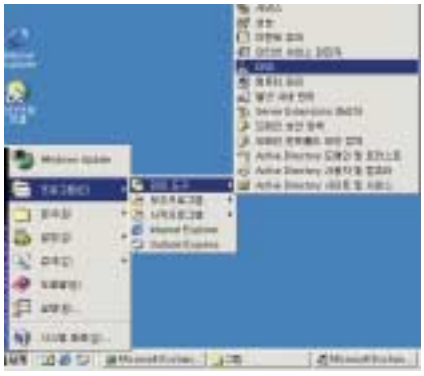
네트워크 구성요소 설정
(그림 5-4-1)

- (그림 5-4-2)와 같이 [DNS(도메인 이름 시스템)]를 체크하고 [확인] 클릭

도메인네임서버 서비스 설정
(그림 5-4-2)

● **[다음]**을 누르고 **[마침]**을 클릭하면 설치 완료

● **[시작]** ⇨ **[프로그램]** ⇨ **[관리도구]** ⇨ **[DNS]** 가 생성되었는지 확인



DNS설정 확인화면
(그림 5-4-3)

※ Windows2000 서버에서는 부트 파티션의 %Systemroot%\System32\DNS 폴더가 생성되고 DNS 데이터베이스 파일들이 생성된다.

나. Windows DNS 설정하기

DNS 설정은 '영역(zone)등록' 과 '레코드(record)등록' 의 두 가지 설정을 필요로 한다.

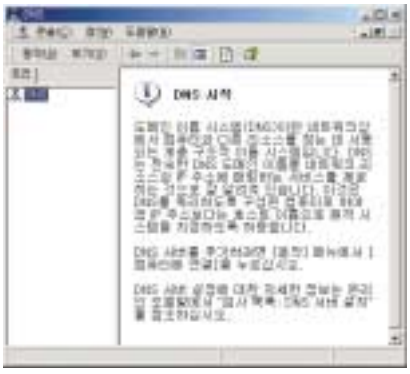
● 영역등록 : 해당 도메인에 대한 DNS 서버를 등록. test.co.kr이라는 도메인에 대하여 질의가 오면 등록한 DNS서버가 응답을 하도록 설정한다.
● 레코드등록 : 앞서 등록한 DNS서버에 서비스할 정보를 입력. 예를 들어 www.test.co.kr, mail.test.co.kr처럼 test.co.kr에 붙는 모든 호스트에 대하여 해당 시스템의 DNS가 관리하도록 그 호스트들을 이 '영역등록' 이라는 절차를 통해 등록하는 것이다.

(1) 영역 생성하기

● (그림 5-4-4)와 같이 DNS 설정 마법사를 실행한다.

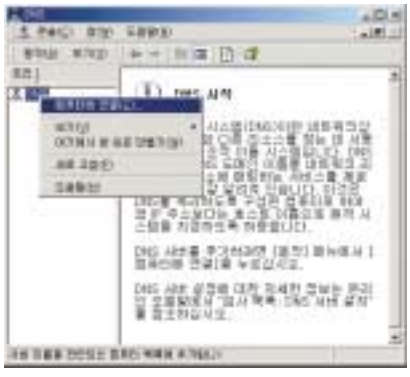
[시작] ⇨ [프로그램] ⇨ [관리도구] ⇨ [DNS] 선택

DNS설정마법사 실행화면
(그림 5-4-4)



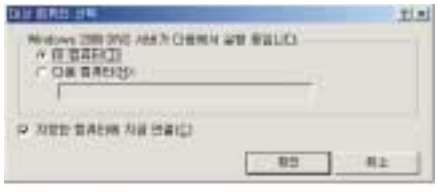
● DNS를 설치할 시스템으로 연결한다. (그림 5-4-5)와 같이 **[DNS]**를 선택한 후 오른쪽 버튼을 클릭하여 **[컴퓨터에 연결]**을 선택한다.

DNS시스템 연결 화면
(그림 5-4-5)

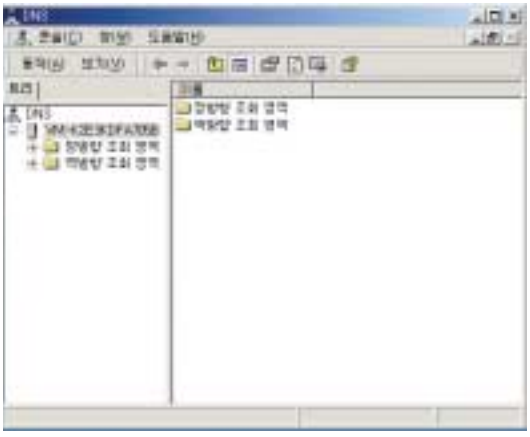


● 대상 컴퓨터를 선택한다. (그림 5-4-6)과 같이 DNS서버가 설치된 시스템과 동일하므로 **[이 컴퓨터]**를 선택하고 옵션을 지정하여 **[지정한 컴퓨터에 지금연결(C)]**을 선택 후 확인을 클릭한다.

대상시스템 선택 화면
(그림 5-4-6)



● DNS서버 추가가 완료되면 (그림 5-4-7)과 같이 **[정방향 조회 영역]**과 **[역방향 조회 영역]** 이라는 트리가 생성된다.



영역트리 생성 확인 화면
(그림 5-4-7)

가) 주영역 설정하기

① 정방향 조회영역 설정

● **[정방향 조회 영역]** 트리메뉴를 선택 후, 마우스 오른쪽 버튼을 클릭한 후 **[새 영역]**을 클릭하면 (그림 5-4-8)과 같이 **[새 영역 마법사]**가 실행된다.

[새 영역 마법사] 실행화면
(그림 5-4-8)

● (그림 5-4-9)와 같이 **[정방향 조회영역 생성]**을 선택한 후 **[표준 주 영역]** 생성을 설정한다.

표준 주 영역 설정화면
(그림 5-4-9)

● 영역이름 입력 란에 (그림 5-4-10)과 같이 NIC에 등록한 도메인 이름 또는 가상의 이름을 입력

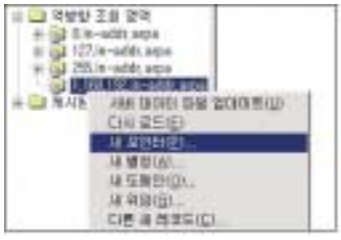
도메인 명 입력 화면
(그림 5-4-10)

● 영역 파일명 입력 란에는 자동으로 도메인명에 ".dns"가 붙은 파일명이 생성된다. 영역파일명 입력이 완료되면 정방향 영역이 생성 완료된다.

영역 파일명 입력 화면
(그림 5-4-11)

② 역방향 조회영역 설정

- **[정방향 조회영역]**과 동일한 형태로 역방향 조회영역을 선택하고 새 영역 마법사를 실행한다.
- 화면이 나타나면 **[네트워크 ID]** 항목에 IP 입력 후, **[다음]**을 진행하면 정방향 조회영역에서와 마찬가지로 영역파일이 생성되고 영역이 추가된다.
- 역방향 영역이 추가되면 SOA(권한의 시작), NS(이름서버) 레코드가 추가된다.
- 새 포인터(PTR) 레코드를 추가하려면 (그림5-4-12)와 같이 역방향 영역을 마우스 오른쪽 버튼을 클릭하고 **[새 포인터]** 를 선택한다.



새 포인터 설정 화면
(그림 5-4-12)

- (그림 5-4-13)과 같은 **[새 리소스 레코드]** 창에서 **[호스트 IP 번호]**란에 추가할 IP 주소 입력 ⇨ **[호스트 이름]**란에 해당 호스트의 이름입력 ⇨ **[확인]** 클릭한다.

새 레코드 추가 화면
(그림 5-4-13)

- 동일한 방법으로 필요한 레코드들을 추가한다.

나) 보조영역 설정

보조 영역(Secondary Zone)이란 주 영역(Primary Zone)으로부터 전송된 영역을 말한다. 보조 영역은 주 영역으로부터 일정한 시간마다 복사본을 전송 받는다.
등록기관에 도메인 신청시 입력한 2개의 네임서버 중 하나의 서버에 주 영역을 추가하고, 다른 네임서버에 보조 영역을 추가한다. 보통 주 영역 서버를 사내 DNS 서버로 이용하고 보조 영역 서버를 ISP 업체의 DNS 서버로 이용하는 것이 일반적이다.

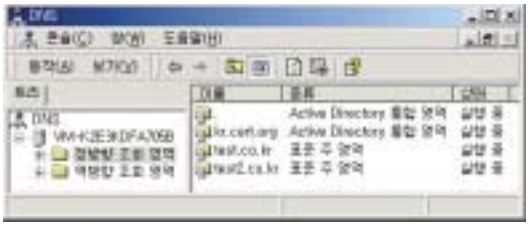
- 표준 보조 영역의 설정은 기본적으로 주영역 설정과 동일하게 진행한다. (그림 5-4-14)은 같은 화면이 나타나면 보조영역, 표준 보조 영역을 선택한다.

표준보조영역 설정
(그림 5-4-14)

- 주 영역과 동일한 방법으로 영역의 이름을 입력한다.
- (그림 5-4-15) 화면에 사용할 공인 IP나 가상 IP를 입력한다.

마스터 DNS서버 지정
(그림 5-4-15)

● 추가된 영역이 (그림 5-4-16)에서와 같이 트리메뉴에 정상적으로 생성되었는지 확인



추가영역 생성확인 화면
(그림 5-4-16)

※ 만일 주 영역 서버로부터 정보를 가져오지 못하면 보조영역 오른쪽 클릭 ⇨ "마스터에서 전송"을 클릭한다. 그래도 전송이 안되는 경우 "관리도구" ⇨ "서비스"에서 "DNS Server" 서비스를 멈추었다가 재구동 시킴

(2) 네임서버 레코드 등록

네임서버(NS) 레코드는 도메인의 네임서버 정보를 나타낸다. 한국인터넷정보센터(KRNIC)이나 도메인등록 대행기관에 도메인을 신청할 때 보통 2개의 네임서버 정보를 입력한다. 그리고 DNS 서버에는 신청시 입력한 네임서버를 나타내는 NS 레코드를 추가해야 한다.

아래 설명에서는 test.co.kr 이란 도메인을 예를 들어 설명한다. 신청한 네임서버는 ns.test.co.kr 과 ns.nuri.net 이라 가정한다.

● 기본적으로 추가된 NS 레코드를 선택 후, 마우스 오른쪽 버튼을 클릭하고 "등록 정보"를 선택 또는 왼쪽화면에서 도메인을 오른쪽 클릭하고 "등록 정보"를 클릭

등록정보
(그림 5-4-17)

● **[이름 서버]** ⇨ **[서버 이름]**란에 네임서버 이름을 입력 ⇨ IP 주소 값을 입력하고 **[추가]** ⇨ **[확인]** 클릭

네임서버 이름을 입력
(그림 5-4-18)

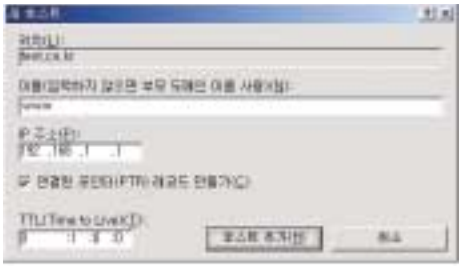
● 동일한 방법으로 여러 개의 네임서버를 추가 할 수 있다.

여러 개의 네임서버를 추가
(그림 5-4-19)

가) 호스트(A) 레코드 추가하기

새 영역을 만들었으면 영역에 필요한 레코드들을 추가해야 한다. 호스트(A) 레코드는 특정 호스트의 이름(예:www, ftp, mail, ...)을 IP 주소로 매핑하는 역할을 한다. 다음 예에서 www.test.co.kr 이라는 호스트 이름이 지정되면 DNS는 이 호스트에 지정된 IP 주소 (192.168.1.1)을 되돌려 준다.

● 해당 도메인을 선택 한 후, 마우스 오른쪽 버튼을 클릭하고 **[새 호스트]**를 선택



[새 호스트]를 선택
(그림 5-4-20)

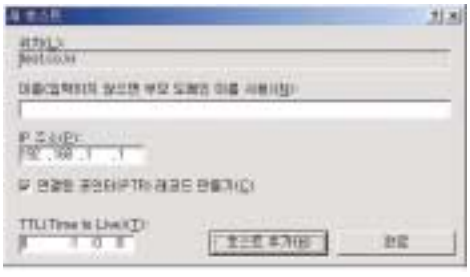
● **[이름...]**란에 추가할 호스트 이름을 입력 ⇨ **[IP주소]**란에 IP 주소를 입력하고 **[호스트 추가]** 클릭

- **[연결된 포인터(PTR) 레코드 만들기]** 옵션은 역방향 영역을 추가한 경우에만 체크
- [TTL(Time to Live)] 값은 이 호스트 정보를 참조한 DNS 서버의 캐시에 남겨둘 시간을 설정

● 레코드를 성공적으로 만들었으면 확인 클릭

레코드 생성
(그림 5-4-21)

● **[이름...]**란을 비워둔 채 IP 주소만 입력하고 **[호스트 추가]** ⇨ **[예]** 클릭



호스트 추가
(그림 5-4-22)

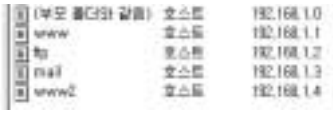
※ 홈페이지 접속을 www.test.co.kr 뿐만 아니라 test.co.kr로도 가능하게 하려면 해당 도메인에 대한 호스트 레코드가 필요하기 때문이다.

● [예]를 클릭 해 주면 설정 완료

추가 완료
(그림 5-4-23)

● 추가된 호스트 레코드 정보화면 예

추가된 호스트 레코드 정보화면 예
(그림 5-4-24)



● 추가된 호스트 레코드들에 대한 역방향 영역 정보(PTR 레코드)

추가된 호스트 레코드들에 대한 역방향 영역 정보
(그림 5-4-25)

(3) DNS 동작 확인

● 루트 디렉토리 확인

처음 DNS를 구성하는 동안 DNS 서버를 찾지 못하면 새 DNS 서버가 루트서버로 지정된다. (루트서버란 전 세계의 DNS서버 중 가장 상위에 있는 DNS 서버이지만 아직 설정이 완료되지 않아 자신이 루트 DNS로 인식하고 있는 것임) 즉, 다른 DNS를 참조하지 못하게 된다. 그러므로 다음과 같이 "." 으로 된 조회 영역이 있다면 삭제한다.

루트 디렉토리 확인
(그림 5-4-26)

● DNS Client 설정

DNS Client 설정
(그림 5-4-27)

설치된 DNS서버로 질의를 보내기 위해선 nslookup을 실행하는 시스템의 DNS 설정에서 "기본 설정 DNS서버" 의 주소를 새로 설치된 DNS 서버의 주소로 바꾸어 주어야 한다.

2. Unix DNS (BIND) 서버

Unix 계열 시스템들은 DNS 운영을 위해서 주로 BIND(Berkeley Internet Name Domain) 프로그램을 이용한다. 최신버전의 BIND는 아래 사이트에서 구할 수 있다. BIND는 Unix 계열의 시스템을 위한 소스코드 형태와 Windows NT, Windows2000을 위한 Binary Kit 버전으로 제공되고 있다.

● BIND 다운로드하기

http://www.isc.org/products/BIND/

http://www.isc.org/ISC/MIRRORS.html (ISC FTP mirror sites 목록)

http://www.sunfreeware.com/ (SunOs, Solaris 계열)

가. 설치

대부분의 Unix 시스템에는 BIND가 이미 설치되어 있거나 파일이 존재하는 경우가 많으므로 설치 전에 먼저 확인해 보아야 한다.

●설치여부 및 버전 확인

```
[root@localhost kong]# dig @localhost
```

(1) RPM 으로 설치

DNS 관련 RPM파일들은 배포 CD나 웹사이트를 통해서 RPM을 구할 수 있다.

●BIND RPM 다운로드 하기

http://www.redhat.com/apps/download/results.html?search:change_source_cb=rpm

Red Hat Linux CD-ROM 에서는 RedHat/RPMS 디렉토리 안에 bind*.rpm 파일이 존재하며, 다음과 같은 명령으로 실행할 수 있다.

●CD-ROM 마운트 및 파일 확인

```
[root@pub /root]# mount /dev/cdrom /mnt/cdrom
[root@pub /root]# cd /mnt/cdrom/RedHat/RPMS
[root@pub /root]# ls -al | grep bind*
```

● RPM 설치

```
[root@pub RPMS]# ls -al bind*
[root@pub RPMS]# rpm -Uvh bind-*
```

(2) 소스파일로 설치

http://www.isc.org/products/BIND/에서 소스파일을 다운로드해 설치한다. 본 문서에서 bind-9.2.3.tar.gz 소스파일로 설치하는 예를 보인다.

● 파일 압축해제

```
[root@localhost kong]# tar -xvzf bind-9.2.3.tar.gz  또는
[root@localhost kong] gzip -d bind-9.2.3.tar.gz
[root@localhost kong] tar -xvf bind-9.2.3.tar
```

● Linux 시스템에서 설치

설치될 디렉토리를 지정해서 컴파일하고 인스톨하는데, 일반적으로 설치 위치는 /usr/local/dns 이다.

```
[root@localhostbind-9.2.3]#./configure --prefix=/usr/local/dns
[root@localhost bind-9.2.3]# make
[root@localhost bind-9.2.3]# make install
```

● Unix (Sun) 시스템에서 설치

설치될 디렉토리를 지정해서 컴파일 및 인스톨하는데, /usr/local/bind 또는 /var/cache/bind를 기본 위치로 주로 사용한다.

```
[penguin:root]:/user1/kong/bind-9.2.3〉 ./configure --prefix=/usr/local/dns
[penguin:root]:/user1/kong/bind-9.2.3〉 make
[penguin:root]:/user1/kong/bind-9.2.3〉 make install
```

나. DNS 서버 설정하기

(1) BCT(BIND Configuration Tool)를 이용한 설정

Redhat Linux 7.2 이상의 버전에서는 BIND나 DNS의 설정을 간편하게 제공하기 위해서 X window 환경에서 실행되는 BCT라는 도구를 제공하며, 순차적으로 설치를 진행하면 구성파일을 별도로 수정할 필요가 없다. 그러나 설정 파일들이 BCT 도구의 고유한 포맷으로 생성되기 때문에 다른 편집 도구로 설정파일들을 수정하게 되면, 그 후로는 BCT를 사용하지 못할 수도 있다는 단점이 있다. BIND의 설정파일은 /etc/named.conf이며, DNS 파일들은 /var/named 디렉토리에 생성된다.

- RedHat Linux의 공식 사용자 가이드 - DNS 설정참고
  http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-bind.html

가) Bind Configuration Tool 실행방법

- GUI 환경에서 실행
  - GNOME [Main Menu] ➪ [Program] ➪ [System] ➪ [Configure DNS] 클릭
  - KDE [Main Menu] ➪ [RedHat] ➪ [System] ➪ [Configure DNS] 클릭
- Text 상에서 실행
  /usr/bin/bindconf 입력

나) Bind Configuration Tool 초기화면

BCT의 초기화면에는 로컬호스트의 기본 값인 localhost와 0.0.127.in-addr.arpa가 이미 생성되어 있고, 여기에 도메인 정보를 가지게 될 zone 파일들을 추가 설정하여 DNS 설정을 완료하게 된다.

Bind Configuration Tool 초기화면
(그림 5-4-28)

다) Domain Name 설정하기

① Zone 파일 타입

- Forward Master Zone : 도메인 ⇨ IP로 변환하기 위한 zone 파일 생성
- Reverse Master Zone : IP ⇨도메인으로 변환하기 위한 zone 파일 생성
- Slave Zone : DNS 서버가 두 개 이상인 경우 2차 DNS 연결을 위한 zone 파일 생성

Ⓐ Forward Master Zone 만들기

- **[New]** 버튼을 누른 다음 **[Forward Master Zone]**을 선택 ⇨ Domain name을 입력 ⇨ **[확인]** 클릭

Forward Master Zone 만들기
(그림 5-4-29)

위의 예제는 /etc/named.conf와 /var/named/forward.example.com.zone 파일에 다음과 같은 구성을 가진 항목을 생성한다.

```
/etc/named.conf :
zone  "forward.example.com" {
      type master;
      file  "forward.example.com.zone" ;
};
```

/var/named/forward.example.com.zone :

```
$TTL 86400
@      IN     SOA     ns.example.com.  root.localhost (
                      2 ; serial
                      28800 ; refresh
                      7200 ; retry
                      604800 ; expire
                      86400 ; ttl
                      )

          IN     NS      192.168.1.1.
```

- Maste Zone Name, FileName, Contact, SOA 입력

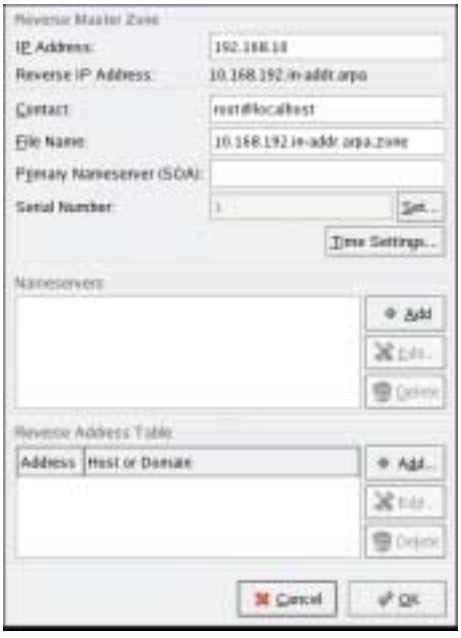
  (그림 5-4-29)의 [Name]은 /etc/named.conf 파일에 삽입되고, [File Name]은 /var/named/test.co.kr.zone 파일에 삽입된다. [Contact]는 도메인 관리자의 메일 주소를 의미한다. [serial number]는 대부분 DNS 정보를 수정한 날짜를 입력한다. Time Settings은 일반적으로 기본값을 사용한다.

- 서버 호스트 추가하기

Master Zone 설정화면 record에서 [Add] 클릭 ⇨ **[호스트명 입력]** ⇨ 호스트의 IP 입력 ⇨ **[확인]**

Ⓑ Reverse Master Zone 만들기

- 초기화면의 [New] 클릭 ⇨ [Reverse Master Zone] 선택 ⇨ IP 3옥텟입력



Reverse Master Zone 만들기
(그림 5-4-30)

- Name Servers에서 [Add] 클릭 ⇨ Name Server에 서버 주소 입력 ⇨ [OK] 클릭
- Reverse Address Table에서 [Add] 클릭 ⇨ IP의 마지막 옥텟 입력 ⇨ 호스트 이름 또는 IP 입력 (이 예제에서는 도메인을 입력) ⇨ [OK] 클릭

위 그림과 같은 예제를 실행할 경우 /etc/named.conf 파일과 /var/named /10.168.192.in-addr.arpa.zone 파일에 다음과 같은 항목들이 생성된다.

/etc/named.conf:

```
zone "10.168.192.in-addr.arpa" {
        type master;
        file "10.168.192.in-addr.arpa.zone";
};
```

/var/named/10.168.192.in-addr.arpa.zone:

```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )

@       IN      NS      ns2.example.com.

1       IN      PTR     one.example.com.
2       IN      PTR     two.example.com.
```

(2) DNS 구성파일 수동 설정

소스파일로 다운로드를 받았을 경우에는 Bind를 설치한 후 설정파일과 zone 파일을 직접 구성해야 하며, 주요 파일들은 다음과 같다.

① 주요 구성파일

- named.conf : 네임서버의 기본 설정하는 파일로, 로컬 호스트와 도메인에 대한 zone 파일 내용을 포함한다.
- /etc/resolv.conf : 네임서버의 위치를 지정하는 파일로, DNS를 사용하는 모든 시스템이 가지고 있어야 한다. 도메인 네임과 네임 서비스를 받기 위한 서버를 지정하는 파일이다.

```
[penguin:root]:/usr/local/dns〉 cat /etc/resolv.conf
search test.co.kr          → 자동으로 찾을 도메인 주소
nameserver 172.16.14.90    → 네임서버로 사용할 호스트의 IP
```

- zone 파일
  - 도메인 zone 파일 : 도메인 네임(test.co.kr) 정보를 기록하는 파일
  - reverse zone 파일 : IP와 도메인 네임을 맵핑시켜주는 역할을 하는 파일

※ DNS 구성에 필요한 기본 zone 파일들

localhost.zone	0.0.127.in-addr.arpa.zone
test.co.kr.zone	5.16.172.in-addr.arpa.zone
named.ca	named.local

- rndc.conf 파일 : Rndc(Remote Name Daemon Control)도구 설정파일로 DNS 서버간에 서로의 정보를 공유할 때 인증을 하여 보안강화를 위해 사용한다.
- named.ca 파일 : 1차 Name server에 대한 정보를 가지는 캐쉬파일로 네임서버의 캐싱기능이 동작할 수 있도록 Root name server와 그것의 IP Address만을 가지고 있다.
- named.local 파일 : 루프백 IP 주소(127.0.0.1)에 대한 reverse 맵핑 파일

② /etc/named.conf 설정하기

● named.conf 파일 구성

[표 5-4-1] named.conf 파일 구성

구 분	설 명	
controls	다른 DNS 와 서로 DNS정보를 주고받을 때 Rndc 키 값을 사용하여 신뢰관계를 맺도록 하여 보안성 향상을 위한 Rndc 설정파일	
Options	zone 파일의 위치를 지정	
zone	localhost , 도메인등에 대한 정보 설정	
type	hint	루트도메인들이 있는 IP 주소가 들어있는 파일로, 이문서에는 named.ca로 되어 있음 (ftp://rs.internic.net에서 구할수 있음)
	master	1차 네임 서버를 정의
	slave	2차 네임 서버를 정의

● 설정 예

```
[root@test root]# vi /etc/named.conf
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
 include "/etc/rndc.key";
options {
        directory "/var/named/";
};
zone  "." {
        type hint;
        file  "named.ca";
};
zone  "0.0.127.in-addr.arpa"  {
        type master;
        file  "0.0.127.in-addr.arpa.zone";
};
```

```
zone  "5.16.172.in-addr.arpa" {
        type master;
        file  "5.16.172.in-addr.arpa.zone";
};
zone  "localhost" {
    type master;
    file  "localhost.zone";
};
zone  "test.co.kr" {
    type master;
    file  "test.co.kr.zone";
};
```

③ zone 파일 구성

다음과 같이 localhost에 대한 zone파일과 도메인 test.co.kr에 대한 zone 파일을 생성한다. RPM이나 BCT를 이용해 설치하는 경우에는 localhost.zone 이나 0.0.127.in-addr.arpa.zone 파일과 같은 로컬호스트에 대한 zone 파일은 자동으로 생성되므로, 도메인에 대한 zone 파일만 구성하면 된다.

● 설정 예 (test.co.kr.zone파일)

```
[root@test named]# cat test.co.kr.zone
$TTL 86400
@       IN      SOA     @  root.localhost (
                        20020609 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )
@       IN      NS      test.co.kr
@       IN      A       172.16.5.47
www     IN      A       172.16.5.75
```

● 설정 예 (5.16.172.in-addr.arpa.zone파일)

```
[root@test named]# cat 5.16.172.in-addr.arpa.zone
$TTL 86400
@       IN      SOA     @       root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

@       IN      NS      test.co.kr.
47      IN      PTR     test.co.kr.
```

● zone 파일 구성

[표 5-4-2] zone 파일 구성

구 분	설 명	
	SOA(Start of Authority)	소유권을 가지고 있는 도메인 네임
zone파일의 리소스레코드	NS (Name Server)	네임 서버의 리소스 레코드
	A	도메인에 IP 어드레스를 연결해주는 레코드
@	Origin 도메인을 의미함. @대신 도메인 네임 입력 가능	
	networking IP 어드레스 클래스를 의미함	
IN(InterNet)	zone 파일의 시작을 알리고, 전역에 영향을 "all" 은 파라미터를 정의함. SOA 다음에는 1차 네임서버의 관리자 e-mail주소가 오는데, Origine을 의미하는 @은 사용하지 않고 대신 "." 을 사용한다.	
	serial : 네임서버의 데이터 버전 (보통 날짜와 시간을 씀)	
SOA	refresh :Secondary네임서버가 Primary네임서버로 새로운 정보가 업데이트 여부를 요청하는 시간 간격	
	retry : Secondary 네임서버가 Primary 네임서버로 넘어가기 위한 재시도 시간	
정보갱신 관련	expire : 정보의 파기	
	TTL : DNS 정보를 캐시에 저장해 두는 기간. 기본은 하루	

● 새로운 호스트 추가

새로운 호스트를 추가해야 하는 경우가 생기면 도메인 zone 파일과 reverse zone 파일에 새로운 호스트의 정보를 추가하고 SOA의 Serial 값을 갱신한 다음, in.named 데몬을 재구동 시켜주면 된다.

예) first.test.co.kr(172.16.5.48)을 추가한다면

- /usr/local/dns/ 또는 /var/named/ 디렉토리의 test.co.kr.zone 파일에 다음을 추가하고 Serial 값을 update 한다.

```
first        IN    A      172.16.5.48
```

- host reverse data 파일인 /usr/local/dns/5.16.172.rev 또는 5.16.172.in-addr.arpa.zone 에 다음을 추가하고 Serial 값을 update 한다.

```
48           IN    PTR    first.test.co.kr
```

(3) 실행 및 설정 점검

① 실행 및 재 구동

●Linux에서 네임서버 재구동

```
[root@test named]# cd /etc/rc.d/init.d
[root@test named]# ./named start
[root@test named]# ./named restart
```

●Unix(Solaris)에서 네임서버 재구동

```
[penguin:root]:/etc〉 ps -ef | grep in.named
[penguin:root]:/etc〉 kill -9 PID ← in.named 프로세스 ID
[penguin:root]:/etc〉 /usr/sbin/in.named
```

② 설정점검

● nslookup

도메인 네임 서버를 아직까지는 가장 많이 사용되는 도구이며, RedHat 7.3에서는 dig나 host 프로그램을 이용하라는 경고 메시지가 뜨는데, -sil 옵션을 주면 메시지가 나타나지 않는다.

```
[root@test named]# nslookup
Note:  nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead.  Run nslookup with the `-sil[ent]' option to prevent
this message from appearing.
> test.co.kr
Server:         172.16.5.47
Address:        172.16.5.47#53

Name:   test.co.kr
Address: 172.16.5.47
```

● DIG (domain information groper)

도메인 네임서버에 질의하여 결과를 보여주는 검색도구이다.

사용 예)

```
[root@test init.d]# dig 172.16.5.47

; <<>> DiG 9.1.3 <<>> 172.16.5.47
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22322
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;172.16.5.47.                IN     A

;; AUTHORITY SECTION:
.    10800   IN    SOA  A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM. 2002061101 1800  900
604800 86400

;; Query time: 428 msec
;; SERVER: 172.16.5.47#53(172.16.5.47)
;; WHEN: Tue Jun 11 16:51:21 2002
;; MSG SIZE  rcvd: 104
```

● Linux에서는 named.conf 파일과 zone 파일 설정 체크명령을 지원한다.

```
[root@localhost etc]# named-checkconf /etc/named.conf
[root@ns conf]# named-checkzone /var/named/zone-test.co.kr
```

③ DNS 동작확인

다음은 test.co.kr의 DNS를 nslookup으로 점검한 결과와 기본 DNS를 172.16.14.90으로 설정하고 www.test.co.kr(172.16.14.75)로 접속한 실행 예이다.

```
[penguin:root]:/etc〉 nslookup www.test.co.kr
Server: 172.16.14.90
Address: 172.16.14.90
Non-authoritative answer:
Name:    www.test.co.kr
Address:  172.16.5.75
```

실행 예
(그림 5-4-31)

제5절 DataBase 보안

1. Mysql 보안

mysql은 유닉스/리눅스 운영체제에서 가장 많이 사용되는 데이터베이스이고 그 사용량도 꾸준히 늘고 있다. 특히 mysql은 아래와 같은 장점을 가지고 있는데, 데이터베이스로서 mysql 사용 시 일반적으로 취해야 하는 가이드라인에 대해 알아보자.

- 동시 사용자의 수가 무제한적인 처리 능력
- 50,000,000+ record를 처리할 수 있는 용량
- 매우 빠른 명령 수행 능력
- 쉽고 능률적인 사용자 특권 시스템
- 무료로 사용이 가능

가. DB 구동 계정

비단 여기에서 설명하는 mysql 뿐만 아니라 oracle 이나 msql, MS-SQL 등 대부분의 DB는 시스템 관리자인 루트와는 별개의 계정으로 작동하여야 한다. 만약 DB를 루트 권한으로 구동할 경우

다음과 같은 위험이 있다.

- buffer overflow 등 DB 자체의 취약성이 발생할 경우 DB를 구동하는 사용자 즉, 시스템의 루트 권한을 빼앗길 수 있다.
- FILE 권한을 가진 사용자의 경우 root 권한으로 /root/.bashrc 와 같은 파일을 생성할 수 있다.

따라서 일부 DB의 경우 root 계정으로 구동하면 아예 실행되지 않도록 디자인된 경우도 있다. mysql의 경우 통상적으로 mysql이라는 별도의 계정으로 구동하며 부팅시 mysql 계정으로 작동하도록 하려면 su mysql -c "/usr/local/mysql/bin/mysql.server start" 부분을 rc.local 파일에 정의해 주면 된다. 또는 /etc/my.cnf에 다음과 같이 추가하면 루트가 아닌 다른 사용자(아래의 경우 mysql)로 작동하게 된다.

```
[mysqld]
user=mysql
```

나. 어려운 암호 설정

다른 응용 프로그램과 마찬가지로 쉬운 암호를 사용하지 않는 것은 보안의 가장 기본이라 할 수 있다. 특히 mysql의 경우 "mysql -u root"로 실행하면 암호만 안다면 누구나 mysql의 root 권한으로 접근 가능하므로 반드시 root 암호는 추측하기 어려운 암호로 설정하여야 한다. brute force (무작위 입력) 방식으로 mysql의 root 암호를 해독할 수 있는 방법이 있으므로 각별히 신경 써야 한다. 특히 사전에 나오는 단어를 사용하지 말고 영문 자판으로 한글을 입력하는 방식의 암호를 사용하는 것도 좋은 방법이다.

아울러 root 암호를 재설정하여야 하는데, 아래와 같이 새로운 root 암호를 설정하도록 한다.

```
$ mysql -u root mysql
mysql> UPDATE user SET Password=PASSWORD( 'new_password' )
       WHERE user=' root' ;
mysql> FLUSH PRIVILEGES;
```

다. 침입차단시스템 이용

mysql은 기본적으로 3306/tcp를 사용하는데, 외부에서 이 포트로의 직접 접근을 차단하여야 한다. 이를 위해 mysql DB 앞단에 침입차단시스템을 설치하는 것이 좋은데, 외부에서 mysql DB에 직접 접근 가능한지는 다음과 같이 확인해 보도록 한다.

(1) 외부에서 nmap 으로 스캔(scan)해 본다.
(2) 외부에서 telnet hostname 3306 으로 접속해 본다.
(3) 외부에서 mysql -h hostname 으로 접속해 본다.

또한, local에서만 mysql을 구동한다면 3306/tcp에서 구동하지 않고 유닉스 도메인 소켓을 통해 서비스하도록 하는 것이 좋다. 이러한 경우 3306/tcp를 통하지 않으므로 굳이 침입차단시스템을 설치하지 않아도 될 것이다. 이를 위해서는 두 가지 방법이 있는데, 첫번째로 /etc/my.cnf 파일에서 아래와 같이 설정 후 mysql을 재구동하는 방법이 있다.

```
[mysqld]
skip-networking
```

두 번째는 mysql 구동시 "--skip-networking"을 추가하면 된다. 참고로 이는 3.23.27 이하 버전에서는 작동하지 않는다.

라. 평문 데이터 전송 제한

원격지의 웹-DB 연동시 DB에 접속하기 위해서는 아이디/패스워드로 인증을 하게 되는데, 이러한 경우 평문(plain text)으로 전송된다면 아이디/패스워드 가 그대로 유출되는 문제가 발생할 수 있으므로 인터넷을 통해 전송시에는 SSL 또는 SSH를 통해 암호화 하도록 한다. 특히 SSH port forwarding을 이용할 경우 암호화 뿐만 아니라 패킷의 터널링(tunneling)을 통해 패킷 압축 효과도 기대할 수 있다. 그리고 mysql 4.0 이상에서는 자체적으로 OpenSSL을 지원하므로 mysql을

업그레이드하는 것도 고려할 수 있다.

실제, 스니핑을 통해 아이디/패스워드 등이 노출되는지는 다음과 같이 확인해 볼 수 있다.

```
# tcpdump  -l -i eth0 -w - src or dst port 3306 | strings
```

마. 접근 권한 제한

(1) mysql 관리자가 아닌 일반 사용자에게 process 권한을 주지 않도록 한다. 만약 이 권한이 주어질 경우 "show processlist;"를 실행하면 현재 실행되는 query를 모니터링 할 수 있으며 이 중에는 "UPDATE user SET password=PASSWORD('xxxxx')"와 같은 query 도 직접 볼 수 있으며 결국 암호도 알 수 있게 될 수 있다.
(2) mysql 관리자가 아닌 일반 사용자에게 SUPER 권한을 부여하지 않도록 한다. 만약 이 권한이 주어질 경우 client 의 connection을 종료하거나 서버의 시스템 변수를 변경할 수 있게 된다.
(3) mysql 관리자가 아닌 일반 사용자에게 FILE 권한을 부여하지 않도록 한 다. 만약 이 권한이 주어질 경우 mysqld 가 실행되는 권한으로 파일을 생성할 수 있게 될 것이다.
(4) 각 사용자당 허용되는 동시 접속자수를 제한하려면 mysqld 가동시 "max_user_connections" 옵션을 사용하도록 한다.
(5) 만약 mysqld를 mysql 로 실행할 경우 mysql 디렉토리 이하에 대한 읽 고 쓰기 권한은 mysql 로 제한한다.

2. MSSQL 보안

가. 가장 최신의 서비스 팩 설치

MS SQL Server 보안을 위한 가장 효과적인 조치는 가장 최신의 서비스 팩을 설치하는 것이고 Microsoft 코리아 SQL Server 홈페이지를 방문하여 확인할 수 있다.

※ SQL Server 홈페이지: http://www.microsoft.com/korea/sql/

나. Windows 인증 모드 사용

가능하면 SQL Server 연결에 Windows 인증을 하도록 한다. 이렇게 하면 SQL Server에 대한 연결을 Microsoft Windows 사용자 및 도메인 사용자 계정을 제한하여 외부 인터넷 기반 공격으로부터 보호가 가능하다.

SQL Server의 Enterprise Manager로 Windows 인증 모드 보안을 설정하려면
① 서버 그룹을 확장한다.
② 서버를 마우스 오른쪽 버튼을 클린한 후, **[속성]**을 클릭한다.
③ **[보안]** 탭의 인증에서 Windows만을 클릭한다.

다. 정기적인 서버 백업

가능한 데이터베이스는 회사 인트라넷의 안전 구역에 설치되어야 하며 인터넷에 직접 연결하지 않도록 하며, 모든 데이터를 정기적으로 백업하고 복사본을 안전한 오프 사이트 장소에 보관한다.

> ※ 자세한 백업 절차는 SQL Server 2000 운영 가이드를 참조

라. 시스템 관리자 계정(sa) 암호를 어렵게 설정

sa 암호를 지정하려면,
① 서버 그룹을 확장하고 서버를 확장한다.
② 보안을 확장하고 **[로그인]**을 클릭한다.
③ 상세 내용 창에서 **[SA]**를 마우스 오른쪽 버튼을 클린한 후, **[속성]**을 클릭한다.
④ **[암호]** 입력란에 새 암호를 입력한다.

> ※ Windows 인증을 사용하는 경우에도 sa 암호는 반드시 입력한다.

마. SQL 서버 서비스 실행 권한 수준 제한

SQL Server 2000 및 SQL Server Agent는 Windows 서비스로 실행된다. 각 서비스는 Windows 계정에 연결되어 있으며 sa같은 SQL Server는 운영체제에 접근할 수도 있다.

따라서, 서버(구체적으로는 SQL Server와 관련 있는 서비스)가 공격당하면 해당 서비스가 접근 권한이 있는 운영 체제내의 다른 자원으로 공격이 확대될 수 있으므로, SQL Server 서비스에는 필요한 권한만을 부여해야 한다.

다음과 같은 서비스의 권한 설정에 유의한다.

(1) MSSQLServer : 일반적인 사용자 권한이 있는 Windows 도메인 사용자 계정으로 실행하도록 하고 로컬 시스템, 로컬 관리자 또는 도메인 관리자 계정으로 실행하지 않도록 한다.

(2) SQLServerAgent : 이 서비스는 가능하면 사용하지 않도록 하고 필요할 경우 일반 Windows 도메인 사용자 계정으로 실행하고 로컬 시스템, 로컬 관리자 또는 도메인 관리자 계정으로 실행하지 않는다.

바. 침입차단시스템에서 SQL Server 포트 차단

SQL Server를 기본 설정으로 설치했다면 TCP 포트 1433 및 UDP 포트 1434를 사용 합니다. 가능하면 이 포트로 들오어는 외부 패킷을 차단하도록 하고 관련 데이터베이스 서비스가 추가로 사용하는 포트들도 침입차단시스템에서 차단한다.

사. SQL Server 설정 파일

다음과 같은 SQL Server 설정 파일은 공격자에게 유용한 시스템 정보가 포함되어 있으므로 사용하지 않는 것은 삭제하거나 별도로 저장하는 등 안전하게 보관한다.

(1) 기본 설치의 경우 〈시스템드라이브〉:\Program Files\Microsoft SQL Server\MSSQL\

Install 폴더, 인스턴스 이름이 있는 경우 경우 〈시스템드라이브〉:\Program Files\Microsoft SQL Server\ MSSQL$〈인스턴스이름〉\Install 폴더에 있는 sqlstp.log, sqlsp.log 및 setup.iss 파일을 확인한다.

(2) 현재 시스템이 SQL Server 버전 7.0에서 업그레이드된 경우에는 다음 파일들도 확인해야 한다: %Windir% 폴더의 setup.iss, Windows Temp 폴더의 sqlsp.log 파일을 확인한다.

3. 오라클

가. 필요한 서비스만 설치

오라클 데이터베이스를 처음 설치할 때, 꼭 필요한 요소만 설치하여야 한다. 무엇이 꼭 필요한 요소인지 확실치 않다면, 일반적인 구성으로 설치(즉, Typical installation을 선택하여 설치)하도록 한다.

나. 디폴트 사용자 아이디

오라클 데이터베이스를 설치하면 다수의 디폴트 사용자 아이디가 생긴다. 이때 오라클의 사용자 관리도구(DBCA : Database Client Administration Tool)가 이러한 디폴트 사용자 아이디를 자동으로 잠그고 기간만료 시키는데 (언제나 그렇듯이)예외가 되는 사용자 아이디들이 있다.

그 예외들은 아래와 같다.
SYS, SYSTEM, SCOTT, DBSNMP, OUTLN, 그리고 3개의 JSERV사용자 아이디들

만약 수동으로(즉, DBCA를 사용하지않고) 오라클을 설치하는 경우라면, 디폴트 사용자 아이디는 모두 열린(즉, lock되지 않는다.) 상태가 되므로 보다 세심한 주의가 필요하다. 따라서 수동으로 설치한 데이터베이스는 SQL문을 통하여 디폴트 사용자 아이디를 잠그고 기간만료 시켜야 한다(물론 상기의 SYS, SYSTEM, SCOTT, DBSNMP, OUTLN, 그리고 3개의 JSERV사용자 아이디들을 제외하고 말이다).

다음과 같은 SQL을 통해서 사용자 아이디목록과 그 상태를 알 수 있다.

```
SQL> SELECT username, account_status FROM dba_users;

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
SYS                            OPEN
SYSTEM                         OPEN
OUTLN                          OPEN
DBSNMP                         OPEN
TRACESVR                       OPEN
AURORA$JIS$UTILITY$                    OPEN
OSE$HTTP$ADMIN                         OPEN
AURORA$ORB$UNAUTHENTICATED     OPEN
ORDSYS                         OPEN
ORDPLUGINS                     OPEN
MDSYS                          OPEN

USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------------
USER1                          OPEN
USER2                          OPEN
```

특정 사용자 아이디를 사용하지 못하도록 하며, 계정사용기간을 만료시키는 SQL 문장은 다음과 같다.

```
SQL> ALTER USER test ACCOUNT LOCK PASSWORD EXPIRE;
```

※ 단, External 인증의 사용하는 경우는 expire 할 수 없다.

또한 불필요한 사용자 아이디를 삭제하는 것도 좋은 방법이 될 것이다. 예를 들어 USER1을 삭제하고자 한다면 아래의 SQL 문장을 이용할 수 있다.

```
SQL> DROP USER user1;
```

다. 디폴트 사용자 아이디 암호 변경

'나' 의 단계에서 잠그고 기간만료하지 않은 디폴트 사용자 아이디(SYS, SYSTEM, SCOTT, DBSNMP, OUTLN, 그리고 3개의 JSERV 사용자 아이디의 암호를 변경시켜야 한다.

오라클 데이터베이스를 공격하는 가장 손쉬운 (또한 가장 어처구니없는)방법은 설치당시의 디폴트 비밀번호를 사용하는 사용자 아이디를 찾아내는 것이다. 이러한 암호의 변경은 설치직후 지체없이 이루어져야 한다.

아래 예는 디폴트 비밀번호를 이용하여 로그인을 시도한 예이다.

```
줄번호 명령

(01)  $ sqlplus
(02)
(03)  SQL*Plus: Release 8.1.7.0.0 - Production on Mon Sep 2 13:59:11 2002
(04)
(05)  (c) Copyright 2000 Oracle Corporation.  All rights reserved.
(06)
(07)  Enter user-name: system
(08)  Enter password: manager
(09)
(10)  Connected to:
(11)  Oracle8i Enterprise Edition Release 8.1.7.0.0 - Production
(12)  With the Partitioning option
(13)  JServer Release 8.1.7.0.0 - Production
(14)
(15)  SQL> exit
```

디폴트 사용자 아이디의 암호는 아래 표와 같다.

[표 5-5-1] 디폴트 사용자 아이디의 암호

	사용자 아이디종류사용자 아이디	패스워드
관리자사용자 아이디	SYS	CHANGE_ON_INSTALL
	SYSTEM	MANAGER
일반사용자 아이디	SCOTT	TIGER
jserv 사용자 아이디	AURORAJISUTILITY$	임의로 생성된 패스워드
	OSE$HTTP$ADMIN	임의로 생성된 패스워드
	AURORAORBUNAUTHENTICATED	임의로 생성된 패스워드

※ 그 외의 디폴트 사용자 아이디는 사용자 아이디와 비밀번호가 동일함 ex) MDSYS / MDSYS

아래의 예제는 user2 라는 사용자 아이디의 비밀번호를 'new_passwd' 로 변경하는 SQL 문장이다. 다른 디폴트 사용자 아이디도 동일한 방법으로 변경할 수 있다.

```
SQL〉 ALTER USER user2 IDENTIFIED BY new_passwd;
```

또한, 오라클 엔터프라이즈 에디션을 사용한다면 kerberos, 토큰 카드(token card), 스마트 카드, X.509 인증서 등과 같은 강화된 인증기능을 이용할 수 있다.

라. 데이터 사전(Data Dictionary)의 보호

데이터 사전(Data Dictionary)을 보호하기 위해서는 "파라미터 파일(Parameter File)" 인 init〈sid〉.ora의 내용을 OS가 제공하는 에디터를 이용하여 아래와 같이 수정하면 된다.

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

이렇게 하면 오직 적절한 권한을 가진 사용자(즉, DBA 권한으로 접속을 생성한 사용자)만이 "데이터 사전" 상의 'ANY' 시스템권한('ANY' system privilege)을 사용할 수 있다.
만일 이러한 설정을 위처럼 하지 않는다면, 'DROP ANY TABLE' 시스템 권한을 가진 사용자는 누구라도 "데이터 사전" 의 내용을 악의적으로 DROP할 수 있을 것이다.

"데이터 사전"를 조회해야만 하는 사용자에게는 'SELECT ANY DICTIONARY' 시스템 권한을 주어 "데이터 사전" 뷰(view)로의 접근만을 허용하도록 할 수 있다.
오라클9i에서는 디폴트로 O7_DICTIONARY_ACCESSIBILITY = FALSE 값을 갖는다. 그러나 오라클8i에서는 해당 값이 디폴트로 TRUE로 설정되어 있으므로 반드시 수정하여야 한다.

마. 권한(privilege)의 부여(GRANT)

꼭 필요한 만큼만 권한을 주어야 한다.

- 사용자들에게 꼭 필요한 최소권한(least privilege)만을 부여(GRANT)하여야 한다.
- PUBLIC 사용자 그룹에서 불필요한 권한을 회수(REVOKE)하여야 한다.

PUBLIC은 오라클 데이터베이스의 모든 사용자에게 디폴트 롤(role)로 적용된다. 따라서 모든 사용자는 PUBLIC에 권한 부여(GRANT)된 것은 어떤 일이든 할 수 있다. 이런 경우 사용자가 교묘하게 선택된 PL/SQL 패키지를 실행시켜 본래 자신에게 권한 부여된 권한 범위를 넘어서는 작업을 할 수도 있을 것이다.

- 또한 PL/SQL 보다 더 강력한, 아래와 같은 패키지들도 오용될 소지가 있으므로 주의하여야 한다.

[표 5-5-2] 다른 패키지들

패키지명	패키지의 역할	발생할 수 있는 문제점
UTL_SMTP	임의의 메일 메시지를 임의의 사용자간에 전송할 수 있도록 하는 패키지	이 패키지를 PUBLIC 그룹에서 사용할 수 있도록 권한부여(GRANT)하면 허가받지 않은 메일 전송이 발생할 수 있음
UTL_TCP	외부의 네트워크 서비스로 TCP 컨넥션을 열 수 있도록 하는 패키지	임의의 데이터가 데이터베이스 서버와 외부의 네트워크 서비스 사이에서 오갈 수 있음
UTL_HTTP	HTTP를 통한 데이터 검색 등을 가능케하는 패키지	HTML 형식의 임의의 데이터가 전송될 수 있음
UTL_FILE	파일처리와 관련된 패키지	설정이 잘못되는 경우, 정보시스템상의 모든 파일에 TXT LEVEL의 접근이 가능할 수 있음
DBMS_RANDOM	저장된 데이터를 암호화하는데 사용되는 패키지	일반적으로 대부분의 사용자들은 데이터를 암호화하는 권한을 가져서는 안됨

이와 같은 패키지들은 특정한 응용프로그램에 아주 유용하게 이용될 수 있다. 바꾸어 말하면, 모든 경우에 이러한 패키지들을 꼭 필요로 하는 것이 아니라는 뜻이다. 꼭 필요하지 않은 패키지들의 사용권한을 PUBLIC에서 제거하자.

- 'run-time facilities' 에 제한된 퍼미션을 주어야 한다(Restrict permission on run-time facilities).

  '오라클 자바 버추얼 머신(OJVM : Oracle Java Virtual Machine)' 이 데이터베이스 서버의 run-time facility의 예가 될 수 있다. 어떠한 경우라도 이러한 run-time facility에 ' all permission' 을 주어서는 안된다.
  또한 데이터베이스 서버 외부에서 파일이나 패키지를 실행할 수 있는 facility에 어떤 퍼미션을 줄 때는 반드시 정확한 경로를 명시하여야 한다. 아래의 예를 자세히 살펴보면 좀 더 이해가 쉬울 것이다.

```
- 취약한 run-time call의 예제
  call dbms_java.grant_permission( 'SCOTT' ,' SYS:java.io.FilePermission' , '〈〈ALL FILES〉〉' ,' read' );
- 안전한 run-time call의 예제
  call dbms_java.grant_permission( 'SCOTT' ,' SYS:java.io.FilePermission' , '〈〈actual directory path 〉〉' ,'
```

바. 강력한 인증정책

강력한 인증정책을 수립하고 운영해야 한다.

- 클라이언트에 대한 철저한 인증이 필요하다.
  오라클 9i는 원격인증 기능을 제공한다. 만일 해당기능이 활성화되면(TRUE), 원격의 클라이언트들이 오라클 데이터베이스에 접속할 수 있도록 한다. 즉, 데이터베이스는 적절하게 인증된(즉, 클라이언트 자체의 OS가 인증한) 모든 클라이언트들을 신뢰한다. 일반적으로

PC의 경우에는 적절한 인증여부를 보장할 수 없기 때문에, 원격 인증 기능을 사용하면 보안이 대단히 취약해진다.

원격 인증 기능을 비활성화(FALSE)하도록 설정한다면 오라클 데이터베이스에 접속하려는 클라이언트들은 server-based 인증(즉, 데이터베이스 서버의 인증)을 해야하므로 보안이 강화된다.

원격인증을 제한하여 클라이언트의 인증을 데이터베이스 서버가 행하도록 하려면 오라클 "파라미터 파일(Parameter File)"인 init〈sid〉.ora의 내용을 OS가 제공하는 에디터를 이용하여 아래와 같이 수정하면 된다.
REMOTE_OS_AUTHENTICATION = FALSE

● 데이터베이스 서버가 있는 시스템의 사용자 수를 제한하여야 한다.
오라클 데이터베이스가 운영되고 있는 시스템의 사용자수를 OS 차원에서 제한하여야 한다. 제한이란 꼭 필요한 사용자 아이디만 만들라는 의미로서 관리자권한을 가진 사용자에 특히 주의해야 함은 두말할 것도 없다.

※ 오라클사(Oracle Corporation)는 백서(White Paper)인 'A Security Checklist for Oracle 9i' 에서 시스템 관리자, 해당 데이터베이스의 소유자 혹은 그 누구라도 오라클 데이터베이스의 홈디렉토리 아래의 디폴트화일이나 디렉토리 퍼미션을 오라클사의 지도없이 변경하지 말 것을 권고하고 있다.

사. 네트워크를 통한 접근 제한

● 방화벽을 구축/운영하라.
다른 중요한 서비스와 마찬가지로 데이터베이스 서버는 방화벽 뒤에 설치하여야 한다. 오라클 네트워킹 인프라스트러처인 Oracle Net Service (Net8 and SQL*Net으로 많이 알려져 있다)는 다양한 종류의 방화벽을 지원한다.

● 어렵게 방화벽을 구축하였다면 허점을 만들지 말라.

오라클 데이터베이스를 외부 네트워크에서 접근할 수 있도록 방화벽의 1521 port를 open 하며 스스로 치명적인 허점을 만드는 경우가 있을지도 모른다.

더 나아가, 암호설정 없이 오라클 리스너를 운영한다면 데이터베이스에 대한 중요한 정보(trace & loggin 정보, banner information, db descriptor, service name)들이 노출될 수 있다. 이러한 노출정보가 많으면 많을수록 데이터베이스가 공격당할 가능성이 높아질 것이다.

● 원격에서 오라클 리스너의 설정을 함부로 변경할 수 없도록 하여야 한다.

아래와 같은 형식으로 listener.ora(오라클 리스너 설정화일 : Oracel listener control file) 내의 파라미터를 설정하면, 원격에서 오라클 리스너 설정을 함부로 바꿀 수 없게 된다.

ADMIN_RESTRICTIONS_listener_name=ON

● 접속을 허용할 네트워크 IP 주소 대역을 지정하는 것이 좋다.

데이터베이스 서버가 특정한 IP 주소대역으로부터의 클라이언트 접속을 제어하려면 "Oracle Net valid node checking" 기능을 이용하면 된다. 이 기능을 사용하려면 protocol.ora (Oracle Net configuration file)내의 파라미터를 아래와 같이 설정하여야 한다.

```
tcp.validnode_checking = YES
tcp.excluded_nodes = { list of IP addresses }
tcp.invited_nodes = { list of IP addresses }
```

직관적으로 알 수 있듯이 첫 번째 파라미터가 나머지 두 개 파라미터 기능의 활성화를 결정하며, invited_nodes에 포함된 IP 주소 대역의 접속 요구만이 받아들여진다.

※ 이 기능은 DoS 공격의 잠재적인 위협도 경감시켜 준다.

● 네트워크 트래픽을 암호화하라.

가능하다면 'Oracle Advanced Security' 를 사용하여, 네트워크 트래픽을 암호화하라(문제는 Oracle Advanced Security가 오라클 데이터베이스 엔터프라이즈 에디션에서만 제공

된다는 점이다).

- 데이터베이스 서버가 있는 시스템의 OS를 강화하라.
  불필요한 서비스를 제거하면, 데이터베이스 서버 시스템이 보다 안전해진다. Unix와 Windows를 막론하고 불필요한(그리고 보안취약점이 있는) 많은 서비스들을 디폴트로 제공한다(ftp, tftp, telnet 등등).
  또한 제거된 서비스가 사용하는 UDP/TCP port를 막아라. 이때, UDP/TCP port 둘중 하나만 막는 실수를 저지르기 쉽다.

아. 보안 패치 적용

오라클 데이터베이스가 운영되고 있는 OS와 데이터베이스 자신에 대한 모든 중요한 패치를 정기적으로 실시하여야 한다. 조직이나 기업 차원에서 패치와 관련된 업무 프로세스를 만드는 것도 좋다. 그리고, 아래의 사이트에서 보안과 관련된 정보를 얻을 수 있을 것이다.

- http://otn.oracle.com
- http://technet.oracle.com

c o n t e n t s

제 6 장
보안시스템 운영

제1절 바이러스 백신

바이러스 백신은 항상 켜 둔 상태로 하루에 한번 혹은 일주일에 한번 사용자 임의의 점검 시간을 설정하여 바이러스 검사를 주기적으로 하는 것이 좋다. 하지만, 사용자들이 관심을 갖고 주의를 기울이더라도 바이러스 유포 및 바이러스 감염은 자신도 모르는 사이 뜻하지 않게 발생할 수 있으며 다른 사용자에게 피해를 줄 수 있다.

특히, 컴퓨터 사용 중 바이러스에 걸린 듯한 느낌이 들기 시작했을 때는 이미 바이러스가 활동을 시작하여 어느 정도의 피해를 준 시점일 수 있기 때문에 이때의 바이러스 백신 실행은 무의미할 수 있다.

이렇듯 현재에 있어 바이러스 백신의 중요성에도 불구하고 시스템의 속도를 조금이나마 빠르게 하기 위해 실행중인 백신의 실시간 감지 기능이나 침입차단시스템 등의 보안프로그램들을 꺼버리는 사용자가 간혹 있으므로 주기적으로 보안프로그램들의 정상 작동 여부를 확인해야 한다.

1. 개요

컴퓨터 바이러스는 최근 들어 계속해서 새롭게 만들어지고, 변화하고, 유포되고 있다. 이에 대응하여 백신회사는 새로운 바이러스에 대해서 백신을 업데이트하고 있다. 또한 신속하게 확산되고 있는 바이러스가 권고 되면, 긴급 업데이트를 실행한다. 따라서 백신 프로그램은 컴퓨터를 사용하는 모든 이들에게 절대적으로 필요하다.

바이러스 백신 설치운영이 컴퓨터와 인터넷 사용에 있어 중요한 위치를 자리잡고 있지만, 실제 사용자들은 구입에 있어서는 망설이게 된다는 것이다. 또는 주의 사람들이 소유하고 있는 복사본을 얻어 사용하거나 혹은 불법으로 유통되는 소프트웨어를 구입 · 설치하여 사용하는 것이 당연하리라 생각하는 사용자들을 볼 수 있다.

하지만, 이렇게 설치된 바이러스 백신은 "사용권 계약"에 문제가 될 뿐만 아니라 최근의 바이러스

정보가 자동 업데이트 되지 않아 새롭게 생성된 바이러스 유포에 따른 위험과 위협에 항상 처해있기 때문에 향후 백신 구입에 드는 비용보다 피해 후 컴퓨터 원상복구에 드는 비용이 더 큰 피해를 발생할 수 있다. 그것뿐만이 아니다. 컴퓨터에 들어있던 기밀 정보나 시급히 요구되는 자료를 사용할 수 없을 경우엔 비용과 시간을 떠나 책임을 져야 하는 더욱 큰 문제로 확대될 수 있다.

바이러스 백신 구입, 설치, 운영이 모든 상황으로부터 안전하게 사용할 수 있도록 보장하지는 않지만, 최근 컴퓨터 및 네트워크 전송 처리 속도의 신속성, 근원지가 불분명한 무차별적인 메일전송, 사용자들의 대용량의 파일전송, 신종 바이러스의 지능화 등으로 자신의 PC를 지키기 위해서는 바이러스 백신의 운영은 기본적인 보안운영사항으로 바람직하다고 본다.

바이러스의 최근 동향을 보면 웜과 함께 동작하는 형태로 진화되어 사용자의 네트워크를 마비시키거나 일부 서버의 운영을 다운시키는 등 학교 혹은 회사의 전산망 전체에 위협적인 행동을 하도록 만들어지고 있다. 이를 방어하기 위해 많은 백신 개발 기업들은 막대한 연구비와 우수한 인력을 투입하여 바이러스 백신 개발을 연구하였고, 지금도 진행중이다. 여기 설명하는 백신 제품들은 백신 개발 기업에서 데모용으로 사용자에게 정품 구입전 제품에 대한 평가를 받고 구입을 제안하는 제품이다.

데모용의 주요기능은 실시간 업데이트, 디렉토리 및 파일 관리, 애드웨어차단, 바이러스 차단, 실시간 바이러스 검사, 인터넷 바이러스 검사, 메일 바이러스 검사(일부 제품), 예약 검사 등 기본적으로 필요한 기능만 제공한다. 추가적인 기술지원이나 제품 회사에서 제공하는 전체기능을 제공받으려면 정식 버전을 구입하여야 한다. 또한 임시로 혹은 정식 버전을 구입한 고객에게 웹에서 직접 사용자 컴퓨터를 진단 해주는 서비스도 있다.

[표 6-1-1] 인터넷을 통한 사용자 컴퓨터 진단 해주는 사이트

백신 업체	사이트	비고
안철수 연구소	http://clinic.ahnlan.com/clinic/myv3.jsp	고객 지원
하우리	http://www.livecall.co.kr/levecall/remedy/scan.html	일반인 가능
시만텍	http://security.symantec.com/default.asp?productid=symhome&langid&venid=sym	일반인 가능

요즘 인터넷을 서핑하다 보면 특정사이트(금융권/관공서/일부대학) 접속시 자동으로 사용자 컴퓨터의 바이러스 감염여부를 검사해주거나 웹에서 콘텐츠를 다운받아가지 못하도록 하는 기능이 있다. 이 기능은 사용자들에 의하여 웹 서비스를 하는 서버에 악영향을 미치는 것을 막고 또한 관련 콘텐츠를 도용하는 행위와 사용자 정보를 유출 하는 행위를 막아주고 있다.

2. V3

가. 설치 및 삭제 방법

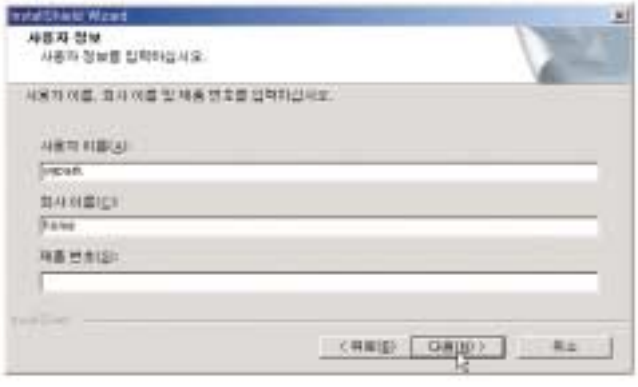
(1) 다운로드 사이트

인터넷 검색창을 이용하여 개별적으로 받을 수도 있고, 안철수 연구소에 접속하여 30일 데모 버전을 다운로드하여 설치 할 수 도 있다.

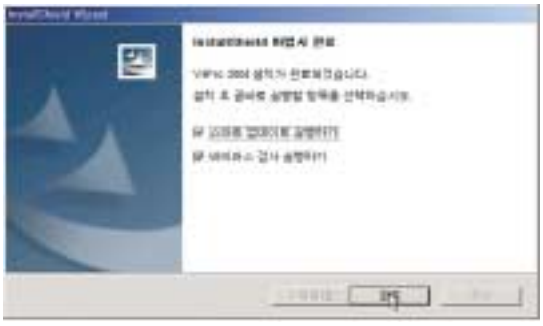
(2) 설치 방법

개인용으로 다운로드하여 받은 백신프로그램을 실행하면 아래와 같은 절차가 진행되어 설치가 완료된다.

V3제품 라이센스 넣기 까지의 과정
(그림 6-1-1)



[제품 번호]란을 공란으로 놓고 다음을 누르면 30일 평가판으로 사용한다는 의미로 인식한다.



설치 완료
(그림 6-1-2)

설치가 완료후 자동 업데이트를 위한 스마트 업테이트와 바이러스 검사를 하도록 선택하는 것이 바람직하다.

스마트 업데이트 설치와 바이러스 검사 화면
(그림 6-1-3)

(3) 삭제 방법

[제어판] ⇨ **[프로그램 추가/제거]**에서 백신 프로그램을 선택하여 삭제 작업을 진행한다. V3의 경우 기본적인 바이러스 운영 프로그램과 스마트 업데이트가 설치되어 있다. 따라서 프로그램 추가/제거에서 각각 선택하여 삭제를 해야 한다. 삭제 작업 후 사용자 컴퓨터를 재시작하여야 한다.

V3 백신 삭제 절차
(그림 6-1-4)

나. 다양한 기능의 환경설정

(1) 실시간 감시 기능 설정

[V3] ⇨ **[시스템 감시]** 체크박스에서 **[On]**에 체크표시를 하면 실시간 감시 기능이 활성화되며, **[시스템 감시 On/Off], [more]**를 클릭 해 환경설정 화면에서 [검사 파일 형식]을 [모든 파일]로 설정한다.

실시간 검사기능 On/Off 설정
(그림 6-1-5)

(2) 자동 업데이트 설정

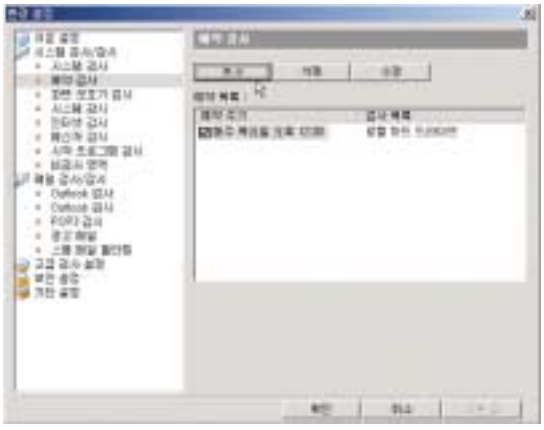
[엔진예약 업데이트] ⇨ **[more]**부분을 클릭해 **[스마트 업데이트 유틸리티]**가 나타나면 추가 버튼을 누른 후 업데이트 주기를 설정 한다.

자동 업데이트 설정
(그림 6-1-6)

(3) 예약 감시 설정

컴퓨터 화면 하단 시스템 트레이 아이콘 [ ]에서 마우스 오른쪽 버튼을 누르면 메뉴가 나오는데 그중 **[환경설정]**을 선택한다. **[환경설정]** ⇨ **[예약검사]**를 선택하여 원하는 디렉토리 혹은 파일을 선택한다. 그리고 예약 기능 수행자를 기록할 필요가 있는 경우는 기록한다.

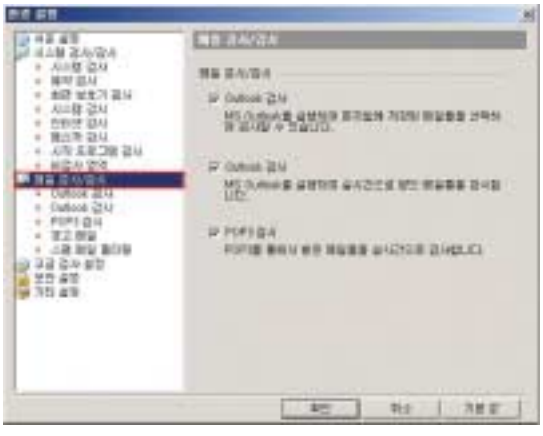
예약 검사 기능 설정 화면
(그림 6-1-7)



다. 기타 기능

(1) 이메일 감시기 활성화

[POP3 감시] 체크박스에서 [On]에 체크표시를 하면 메일감시 기능이 활성화되며, [POP3 감시 On Off] ⇨ [more] ⇨ [메일검사/감시]에서 설정한다.

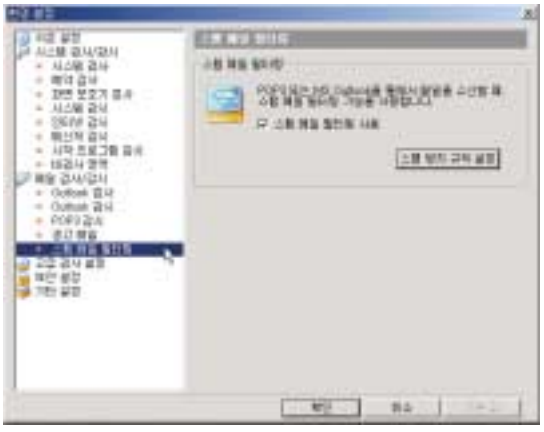


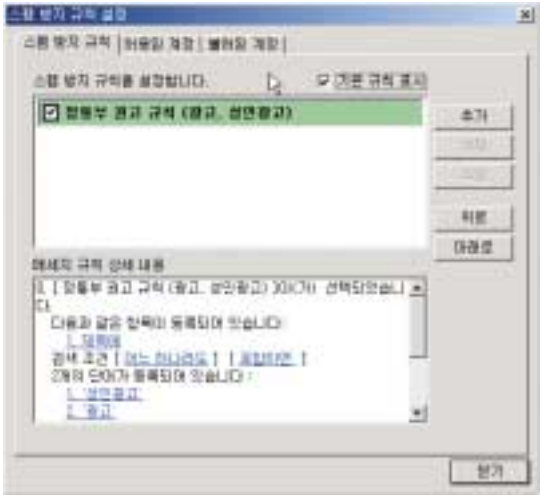
이메일 감시 활성화 설정 화면
(그림 6-1-8)

(2) 스팸 감시 설정 기능

스팸 감시 설정은 받는 메일중에 해당 스팸 패턴이 있는 경우에 스팸으로 처리하도록 하는 기능이다. **[환경설정]** ⇨ **[스팸메일설정]**을 선택하여 "스팸의 규칙"과 "허용 계정" 혹은 "불필요한 계정"을 기록한다.

스팸 차단 설정 기능 (1)
(그림 6-1-9)





스팸 차단 설정 기능 (2)
(그림 6-1-10)

3. 바이로봇

가. 설치 및 삭제 방법

(1) 다운로드 사이트

인터넷 검색창을 이용하여 개별적으로 받을 수도 있고, (주)하우리(http://www.hauri.co.kr/download/)에 접속하여 30일 체험판을 다운 받아 설치 할 수 도 있다.

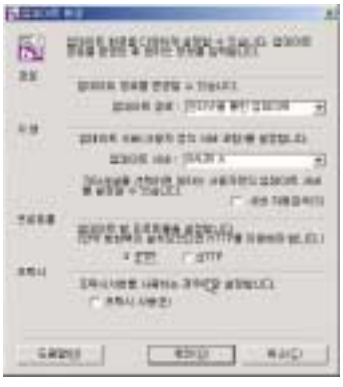
(2) 설치 방법

바이로봇의 경우 30일 체험판은 별도의 라이센스를 넣는 부분이 없이 설치가 진행된다. 설치 작업시에 바이로봇을 시스템에 설치전 내부 바이러스 감염 검사부분을 실행한다. 아래의 그림은 설치에 관한 그림이다.

설치전 실행 프로세스 및 시스템 검사 (1)
(그림 6-1-11)

설치전 실행 프로세스 및 시스템 검사 (2)
(그림 6-1-12)

설치 완료후 최신 패치 버전을 받기 위한 업데이트 작업
(그림 6-1-13)



(3) 삭제 방법

바이로봇의 삭제작업의 경우 시스템을 다시 시작하는 경우는 없으며 시스템 트레이에서 우선적으로 바이로봇 프로세스를 종료 한 후 **[제어판]** ➪ **[프로그램 추가/제거]**에서 바이로봇을 삭제하도록 한다.

바이로봇 삭제 작업
(그림 6-1-14)

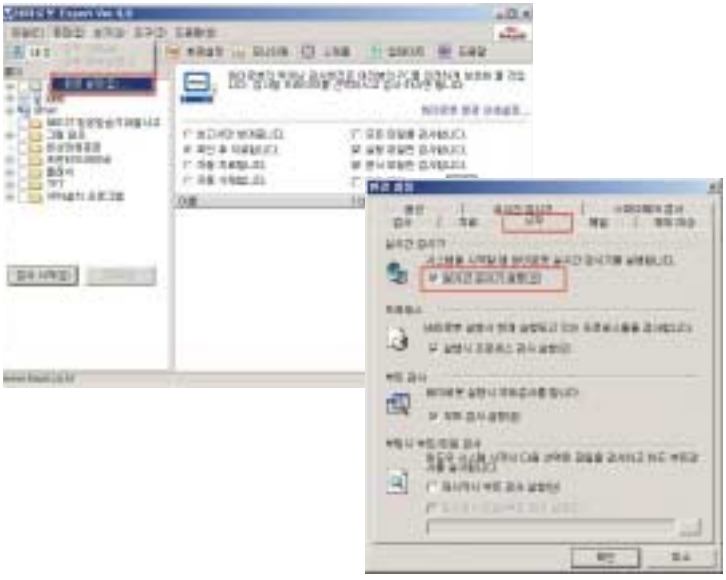
나. 다양한 기능의 환경설정

(1) 실시간 감시 기능 설정

[편집] ➪ **[환경설정]** ➪ **[시작]** ➪ **[실시간 감시기 실행]**에 체크표시를 하면 실시간 감시 기능이 활

성화된다. **[검사]** ⇨ **[검색 대상]** ⇨ **[모든 파일]**로 정한다.

실시간 감시기능 설정
(그림 6-1-15)



(2) 자동 업데이트 설정

[메뉴] ⇨ **[스케줄]** ⇨ **[바이로봇 스케줄 마법사]** ⇨ **[다음]** ⇨ **[업데이트예약]**을 선택하여 업데이트 주기를 설정할 수 있다.

자동 업데이트 설정
(그림 6-1-16)

(3) 예약 감시 설정

[검사옵션 설정] 혹은 **[메뉴바]**에서 **[스케줄]** ⇨ **[바이로봇 스케줄 마법사]** ⇨ **[다음]** ⇨ **[바이러스 검사 예약]**를 선택하여, 예약일자와 검사 대상을 설정할 수 있다.

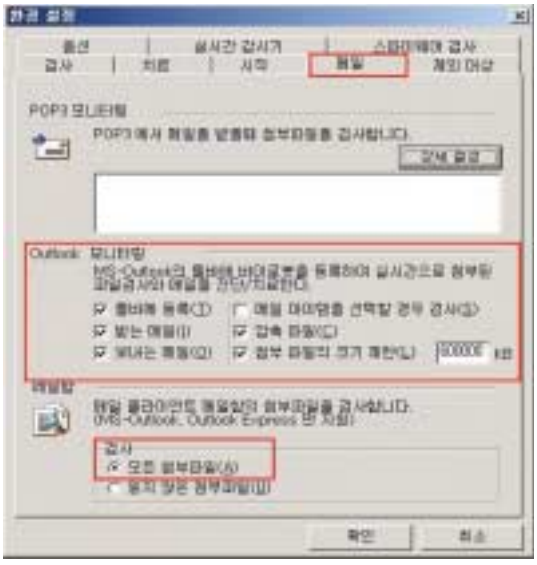
예약 감시 설정
(그림 6-1-17)

다. 기타 기능

(1) 이메일 감시기 활성화

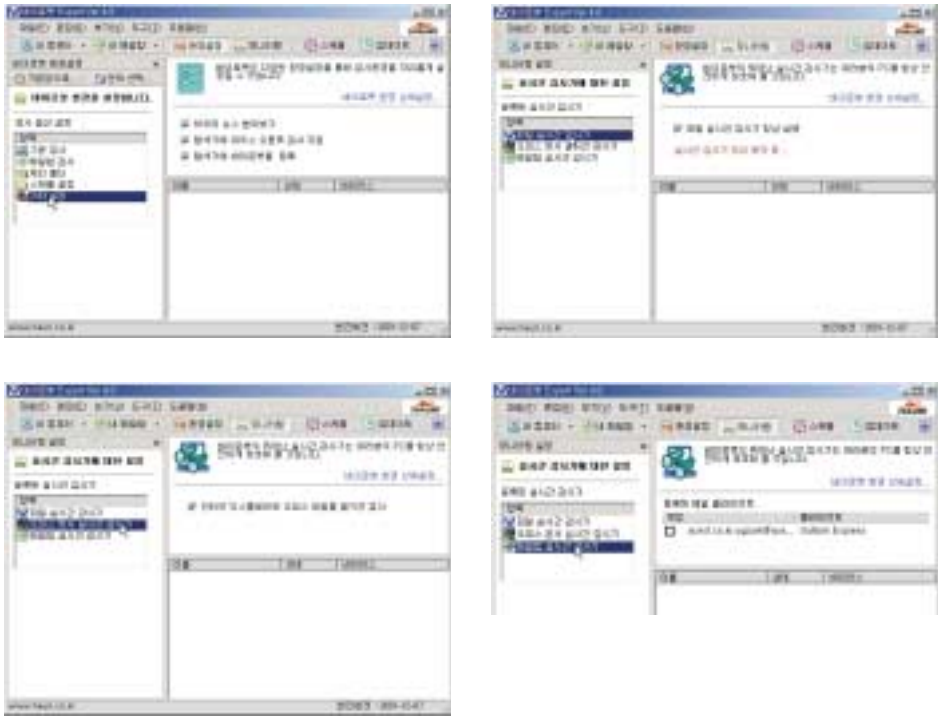
[환경설정] ⇨ **[메일]** ⇨ **[Outlook 모니터링]** ⇨ **[받는 메일]**에 체크표시가 되어 있어야 하며, **[메일함]** ⇨ **[모든 첨부파일]**에 체크표시를 한다.

이메일 감시기 활성화
(그림 6-1-18)



(2) 기타 설정

기타 설정 부분은 바이러스에 대한 정보 받기와 바이로봇의 실시간 파일 검사/오피스 문서 실시간 검사/메일함 실시간 검사 부분으로 되어 있다.



기타 설정
(그림 6-1-19)

제2절 바이러스 월(Virus Wall)

1. 개요

바이러스 월의 경우 네트워크 보안 시스템 운영에 있어서 최근 필수적인 보안시스템으로 자리잡고 있다. 이유는 다양한 바이러스가 나오고 있기 때문이다. 최근에는 P2P을 이용한 웜 · 바이러스의 유포로 더욱 심각한 상황이라고 할 수 있다.

바이러스 월은 주로 HTTP(80), FTP(21), TELNET(23), SMTP(25), POP3(110)의 프로토콜 상에서 주요 웜 · 바이러스에 대한 차단 기능을 담당한다.

기업에서 바이러스 월 도입시 기업의 네트워크 트래픽을 분석하는 분석단계 및 회선 품질을 시험하는 회선 품질검사 단계을 거치는 것이 좋다. 위의 단계를 거쳐 기업 환경에 적합한 바이러스 월 제품을 선택하도록 한다. 왜냐하면, 바이러스 월은 응용서버와 같이 네트워크 서비스에 올라가는 것이 아니라 네트워크 장비로 설치되므로 전체 네트워크 혹은 바이러스 월이 설치된 서브 네트워크에 장애가 생길 수 있기 때문이다.

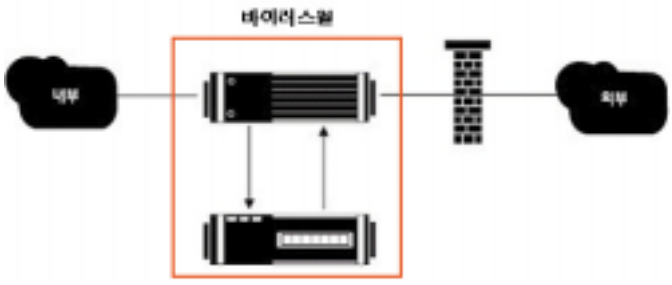
아래 소개되는 제품은 국산 바이러스 월의 주요 기능을 위주로 설명한 것이다.

2. 바이러스 월의 특징

가. 기본 구성도

바이러스 월은 하나의 장비에서 모두 처리하는 형태로 운영되거나, 프로토콜을 분리하여 각 프로토콜별로 바이러스를 차단하는 형태로 운영된다. 예를 들어, 특정 프로토콜 양이 많은 경우 해당 프로토콜에 대한 바이러스 월 시스템이 개별적으로 운영될 수 있다. (그림 6-2-1)은 두 개의 바이러스 월이 작동하는 모습이다. 물론 트래픽이 적은 사이트에서는 프로토콜별로 분리하여 운영할 필요는 없다.

그러나, 두 가지 경우 모두 현재 알려진 프로토콜을 이용하지 않는 웜/바이러스가 유입되는 경우 내부망으로 그대로 유입되므로 주의해야 한다.



기본 구성도
(그림 6-2-1)

나. 주요 기능 및 특징

- HTTP, SMTP, POP3, FTP, TELNET 프로토콜 지원
- Content Scanning
- 제목라인, 메시지 내용, 첨부파일 이름, 첨부문서 필터링
- Blocking 기능
- Spam Mail 차단 기능
- Alerting 기능
- 최신 바이러스 정보 유지
- 원격 관리 및 리포팅 기능 (보고서, 로그, 통계 등)
- 키워드, 파일명, 파일의 확장자, URL 메소드, 메일 발송자에 따른 스팸 메일 필터링 기능

다. 운영 정보

● 프로그램

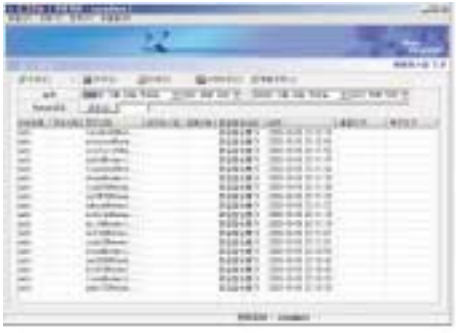
프로그램 메뉴는 사용자 인터페이스를 고려하여 로그정보, 통계정보, Xshield, LIVE 업데이트, 환경설정, 로그아웃, 프로그램 종료로 이루어져 있다.

기본 메뉴
(그림 6-2-2)

● 로그정보

바이러스 월은 로그에 대해 프로토콜, 보낸 사람, 받는 사람, 바이러스 명, 원본 내용, 메일 발송 상태, 날짜, 출발지 IP, 목적지 IP, 메시지 크기, 데이터 방향 등 다양한 조건의 검색이 가능하다. 또한 다양한 조건의 검색으로 원활한 관리와 리포팅 작업이 가능하다.

전체 운영 화면
(그림 6-2-3)



● 통계정보

바이러스 월은 로그를 바탕으로 각 조건별, 통계메뉴별 통계데이터를 작성할 수 있으며 여러 가지 형태의 그래프로 표현이 가능하다. 통계정보를 이용하여 각종 보고서의 레포팅 기능을 제공한다.

통계 및 조회 화면
(그림 6-2-4)

- LIVE 업데이트
  안티바이러스 제품은 꾸준한 바이러스 패턴의 업데이트가 중요하다. 바이러스 월은 최신 바이러스 엔진을 업데이트하여 계속 진보하는 바이러스에 대해 실시간으로 완벽한 검색 및 치료를 할 수 있다. 바이러스 패턴 업데이트를 실행하려면 프로그램에서 LIVE 업데이트를 선택하여야 한다.

제3절 침입차단시스템

1. 개요

침입차단시스템이란 내부 네트워크와 외부 네트워크를 구분 하여 외부에서 내부에 접근하는 트래픽에 대한 규제를 하기 위한 장치로 브릿지 모드(L2 스위치 형태)와 라우팅 모드를 대부분 지원을 한다. 여기서 말하는 브릿지 모드는 기존 네트워크 상황에 아무런 변화를 주지 않고 설치하는 형태를 의미하며, 라우팅 모드란 라우터와 같이 기존 네트워크 환경에 영향을 주어 변경을 하여야 하는 형태를 말한다. 물론 소프트웨어로 구현된 침입차단시스템의 경우는 브릿지 모드(L2 스위치형태)를 지원하지 못한다.

2. 구축 시 고려사항

인터넷 등의 외부 전산망에 연결된 내부 네트워크를 보호하기 위해서 침입차단시스템을 구축하고자 할 경우 고려해야 할 사항은 다음과 같다.

- 어떤 자원을 보호할 것인가?
  보호하고자 하는 하드웨어, 소프트웨어, 각종 중요한 정보, 시스템 사용자, 시스템 관리에 대한 다큐먼트 등을 정의하고 시스템 구축시 이를 고려해야 한다.

- 어떤 위협이 존재하는가?
  보호하고자 하는 자원 및 정보들에 대한 위협이 어떤 것들이 있는가를 분석한다.

- 자원이 얼마나 중요한가?
  보호하고자 하는 자원의 중요성이 어느 정도인가를 분석한다.

- 어떤 사용자를 인가할 것인가?
  사용자 계정을 가진 사용자만이 네트워크를 사용하도록 할 것인지 비인가자라도 제한된 자원에만 사용하도록 할 것인지를 결정한다.

- 요구되는 응용 및 서비스는 무엇인가 ?
  보호하고자 하는 네트워크에서 사용 가능한 응용 및 서비스들이 어떤 것들이 존재하는지를 분석한다.

- 비용 대 효과 측면에서 보호하기 위해 실현될 수 있는 기법은 무엇인가 ?
  파일이나 디렉터리 등은 액세스 제어에 의해 보호하고, 네트워크 장비 및 호스트의 보호는 방화벽 시스템 사용 등의 보호 기법을 고려한다.

- 해커 등의 불법 침입 감지 시 취해야 할 행동은 무엇인가?
  해커 등과 같은 불법 침입자가 시스템 내부에 침입했을 때 취해야 할 대응책을 마련해야 한다.

- 정기적으로 시스템을 점검한다.
  보호하고자 하는 네트워크 및 자원들에 변화가 일어났는지 정기적으로 점검하고 기록한다. 이러한 행위는 시스템 관리자 및 네트워크 관리 시스템에 의해 자동적으로 실행한다.

3. 침입차단시스템의 종류

침입차단시스템은 OSI 참조 모델과 관련하여 침입차단시스템이 동작하는 프로토콜 계층에 따라 분류 될 수 있다.

계층 3인 네트워크 계층과 계층 4인 트랜스포트 계층에서 패킷필터링 기능을 수행하는 스크리닝 라우터와 응용 계층에서 패킷필터링 기능과 인증 기능 등을 수행하는 응용 계층의 게이트웨이로 분류할 수 있다.

일반적으로 스크리닝 라우터를 설계할 경우 "명확하게 내부 네트워크로의 진입이 방지되지 않은 트래픽은 네트워크로의 진입을 허용" 하는 정책을 적용하고, 게이트웨이 혹은 proxy 서버의 경우 "내부 네트워크로의 진입을 명확하게 허용하지 않은 트래픽은 내부 네트워크로의 진입을 방지"하는 정책에 입각하여 설계한다.

가. 스크리닝 라우터(Screening Router)

스크리닝 라우터는 OSI 참조 모델의 계층 3과 계층 4에서 동작되기 때문에 계층 3과 4에서 동작하는 프로토콜인 IP, TCP 혹은 UDP의 헤더에 포함된 내용을 분석해서 동작한다.

스크리닝 라우터란 네트워크에서 사용하는 통신 프로토콜의 형태, 근원지 주소와 목적지 주소, 통신 프로토콜의 제어 필드 그리고 통신 시 사용하는 포트 번호를 분석해서 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽을 허가 및 거절하거나 혹은 외부 네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입 허가 및 거절을 행하는 라우터를 말한다.

이러한 진입 허가 혹은 거절 결정은 패킷필터 규칙에 따른 라우팅 테이블에 의해 결정된다. 일반 패킷과 특수한 프로토콜에 입각한 포트로 전송되는 패킷을 구별하는 능력 때문에 패킷 필터 라우터라고도 한다.

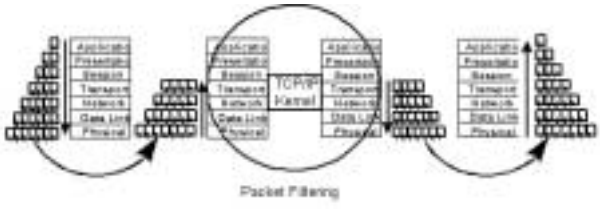
(그림 6-3-1)은 스크리닝 라우터(패킷 필터 라우터)의 위치 및 기능을 보여 준다.

스크리닝 라우터
(그림 6-3-1)

(1) 패킷 필터의 동작

스크리닝 라우터로 연결에 대한 요청이 입력되면, IP, TCP 혹은 UDP의 패킷 헤더를 분석하여 근원지/목적지의 주소와 포트 번호, 제어 필드의 내용을 분석하고, 이들을 패킷 필터 규칙에 적용하여 계속 진입시킬 것인지 아니면 거절할 것인지를 판별한다. 연결 요청 패킷의 진입이 허가되면 이 후의 모든 패킷은 연결 단절이 발생할 때까지 모두 허용된다.

gateway 상에서의
packet filtering
(그림 6-3-2)



(2) 패킷 필터 규칙

패킷 필터 규칙은 [표 6-3-1]과 같이 근원지 주소, 근원지의 포트 번호, 목적지 주소, 목적지의 포트 주소, 프로토콜 플래그, 행위(허가/거절) 등으로 구성된다. 이러한 패킷 필터 규칙이 정해지면 인터넷 주소에 적용하는 허가 /거절하는 조건의 순차적인 액세스 집합인 액세스 리스트를 정의한다.

스크리닝 라우터는 이러한 액세스 리스트를 가지고 프로그램 되며, 패킷을 허가 혹은 거절할 것인지를 액세스 리스트에 있는 행위에 대해서 순차적으로 결정하며, 패킷에 해당하는 액세스 리스트가 나타날 때까지 혹은 마지막 액세스 리스트에 도달할 때까지 순차적으로 점검한다.

침입차단시스템을 실현할 경우 액세스 리스트의 점검 순서는 매우 중요하기 때문에 액세스 리스트의 점검 순서를 신중히 검토하여 사용한다.

[표 6-3-1] 패킷 필터 규칙(예)

규칙번호	Source Address	Source Port	Destination Address	Destination Port	Protocol	Action
1	130.1.20.1	1024	203.239.46.1	80	TCP	PASS
2	130.1.20.5	50	203.239.46.1	80	TCP	REJECT

● 장점
- 필터링 속도가 빠르고, 비용이 적게 든다.
- 네트워크 계층에서 동작하기 때문에 클라이언트와 서버에 변화가 없어도 된다.
- 사용자에 대해 투명성을 유지한다.

하나의 스크리닝 라우터로 보호하고자 하는 네트워크 전체를 동일하게 보호할 수 있다.

● 단점
- 네트워크 계층과 트랜스포트 계층에 입각한 트래픽만을 방어할 수 있다.
- 패킷 필터링 규칙을 구성하여 검증하기 어렵다.
- 패킷내의 데이터에 대한 공격을 차단하지 못한다.
- 스크리닝 라우터를 통과 혹은 거절당한 패킷에 대한 기록(log)을 관리 하기 힘들다.

나. Bastion 호스트

Bastion 호스트는 인터넷 등의 외부 네트워크와 내부 네트워크를 연결해 주는 침입차단시스템 시스템 역할을 한다. 인터넷 사용자가 내부 네트워크로의 액세스를 원할 경우 우선 Bastion 호스트를 통과하여야만 내부 네트워크를 액세스하여 자원 및 정보를 사용할 수 있다.

해커 및 불법 침입자가 Bastion 호스트에 있는 중요한 정보를 악용하여 내부 네트워크로 접근하는 것을 방지하기 위해서는 Bastion 호스트 내에 존재하는 모든 사용자 계정을 지워야 하며, 중요하지 않은 화일이나 명령 및 유틸리티, IP forwarding 화일 그리고 라우팅 정보 등을 삭제하여야 한다. Bastion 호스트로의 입력시 강력한 인증 기법을 구현하여야 하며, Bastion 호스트는 내부 네트워크로의 접근에 대한 기록(log), 감사 추적을 위한 기록 및 모니터링 기능을 가지고 있어야 한다.

bastion 호스트
(그림 6-3-3)

(그림 6-3-3)은 침입차단시스템으로 동작하는 Bastion 호스트를 이용하여 외부 네트워크의 불법 사용자들로부터 내부 네트워크로의 접근을 방지하는 구성도를 나타낸 것이다.

- 장점
  - 응용 서비스 종류에 보다 종속적이기 때문에 스크리닝 라우터보다 안전 하다.
  - 정보 지향적인 공격을 방어할 수 있다.
  - 각종 기록(logging) 정보를 생성 및 관리하기 쉽다.

- 단점
  - Bastion 호스트가 손상되면 내부 네트워크를 보호할 수 없다.
  - 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.

다. Dual-Homed 게이트웨이

Dual-Homed Gateway
(그림 6-3-4)

Dual-Homed 게이트웨이는 (그림 6-3-4)와 같이 두개의 네트워크 인터페이스 를 가진 Bastion 호스트를 말하며, 하나의 네트워크 인터페이스는 인터넷 등 외부 네트워크에 연결되며, 다른 하나의 네트워크 인터페이스는 보호하고자 하는 내부 네트워크에 연결되며, 양 네트워크간의 라우팅은 존재하지 않는다. 따라서 양 네트워크간의 직접적인 접근은 허용되지 않는다.

만약 라우팅이 가능하면 외부 네트워크로부터 내부 네트워크로의 액세스가 가능 하다. 라우팅이 없는 Dual-Homed 게이트웨이를 이용하여 인터넷 혹은 내부 네트워크의 정당한 사용자들이 응용 서비스를 제공받는 방법은 두 가지로 구분되는데,
첫째 방법은 Dual-Homed 게이트웨이 상에서 실행되며 서비스를 제공하는 proxy 서버를 사용하는 것이고,
두번째 방법은 응용 서비스를 제공해주는 Dual-Homed 게이트웨이에 직접 로그인한 다음 다시 내부 네트워크로 접근하는 것인데, 이 경우 강력한 인증 방법이 게이트웨이에 구현되어야 한다.
따라서 해커나 불법 침입자가 악용할 소지가 있는 명령어(suid, sgid 등), 유틸리티 및 불필요한 서비스, 프로그래밍 도구(컴파일러 등)를 이들이 사용할 수 없도록 Dual-Homed 게이트웨이에서 삭제하여야 하며, 라우팅이 되지 않도록 하여야 한다. 또한 로그인에 대한 기록 정보 및 감시 추적에 필요한 기록을 정확히 유지 관리하여야 한다. 외부 네트워크로부터 내부 네트워크로 진입하기 위해서는 Dual-Homed 게이트웨이를 통과하여야 한다.

- 장점
  - 응용 서비스 종류에 좀더 종속적이기 때문에 스크리닝 라우터보다 안전 하다.
  - 정보 지향적인 공격을 방어할 수 있다.
  - 각종 기록 정보를 생성 및 관리하기 쉽다.

- 설치 및 유지보수가 쉽다.

● 단점
- 제공되는 서비스가 증가할수록 proxy 소프트웨어 가격이 상승한다.
- 게이트웨이가 손상되면 내부 네트워크를 보호할 수 없다.
- 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.

라. 스크린드(Screened) 호스트 게이트웨이

Screened Host Gateway
(그림 6-3-5)

스크린드 호스트 게이트웨이는 Dual-Homed 게이트웨이와 스크리닝 라우터를 혼합하여 사용한 침입차단시스템이다.

침입차단시스템의 구성 방법은 (그림 6-3-5)와 같이 인터넷과 Bastion 호스트 사이에 스크리닝 라우터를 접속하고, 스크리닝 라우터와 내부 네트워크 사이에서 내부 네트워크 상에 Bastion 호스트를 접속한다.

인터넷과 같은 외부 네트워크로부터 내부 네트워크로 들어오는 패킷 트래픽을 스크리닝 라우터에서 패킷 필터 규칙에 의해 1차로 방어하고, 스크리닝 라우터를 통과한 트래픽은 모두 proxy 서버를 구동하는 Bastion 호스트에서 입력되는 트래픽을 점검하며, 스크리닝 라우터 혹은 Bastion 호스트를 통과하지 못한 모든 패킷 트래픽은 거절된다.

내부 네트워크로부터 인터넷 등으로 나가는 트래픽은 1차로 proxy 서버를 구동하는 Bastion 호스트에서 점검한 후, 통과된 트래픽을 스크리닝 라우터로 보내고 스크리닝 라우터는 Bastion 호

스트로부터 받은 트래픽을 인터넷 등의 외부 네트워크로 송신할 것인지 결정한다.

Bastion 호스트와 스크리닝 라우터를 통과한 트래픽만이 외부 네트워크로 전달된다. Bastion 호스트는 외부 네트워크로 또는 외부 네트워크로부터의 서비스 요청을 허용할 것인지 아니면 거절할 것인지를 결정하기 위해서 응용 계층의 proxy 서버를 구동한다.

스크리닝 라우터의 라우팅 테이블은 외부 트래픽이 Bastion 호스트로 입력되도록 구성되어야만 하며, 침입자로부터 안전하게 보호되어야 하고 비인가된 변환을 허용해서는 안된다. 만약 라우팅 테이블이 변환되어 외부 트래픽이 Bastion 호스트로 입력이 되지 않고 곧바로 내부 네트워크로 진입할 수 있다면 해커 및 불법 침입자는 내부 네트워크의 자원 및 정보를 변환, 파괴 등을 할 수 있다.

이와 같은 침입차단시스템의 스크리닝 라우터에서는 정적 라우팅 테이블을 사용하는 것이 안전하다.

- 장점
  - 2 단계로 방어하기 때문에 매우 안전하다.
  - 네트워크 계층과 응용 계층에서 방어하기 때문에 공격이 어렵다.
  - 가장 많이 이용되는 침입차단시스템이며, 융통성이 좋다.
  - Dual-Homed 게이트웨이의 장점을 그대로 가진다.

- 단점
  - 해커에 의해 스크리닝 라우터의 라우팅 테이블이 변경되면 이들을 방어 할 수 없다.
  - 침입차단시스템 구축 비용이 많다.

마. 스크린드 서브넷 게이트웨이

인터넷과 내부 네트워크를 스크린드 게이트웨이를 통해서 연결하며, 일반적으로 스크린드 서브

넷에는 침입차단시스템이 설치되어 있으며, 인터넷과 스크린드 서브넷 사이 그리고 서브넷와 내부 네트워크 사이에는 스크리닝 라우터를 사용한다. 이와 같은 침입차단시스템 시스템의 구성도는 (그림 6-3-6)과 같다.

Screened Subnet Gateway
(그림 6-3-6)

스크리닝 라우터는 인터넷과 스크린드 서브넷 그리고 내부 네트워크와 스크린드 서브넷 사이에 각각 놓이며, 입출력되는 패킷 트래픽을 패킷 필터 규칙을 이용하여 필터링하게 되며, 스크린드 서브넷에 설치된 Bastion 호스트는 proxy 서버(응용 게이트웨이)를 이용하여 명확히 진입이 허용되지 않은 모든 트래픽을 거절하는 기능을 수행한다. 이러한 구성에서 스크린드 서브넷에 대한 액세스는 Bastion 호스트를 통해서만 가능하기 때문에 침입자가 스크린드 서브넷를 통과하는 것은 어렵다.

만약 인터넷을 통해 내부 네트워크로 침입하려고 한다면 침입자는 자기가 자유롭게 내부 네트워크를 액세스할 수 있도록 인터넷, 스크린드 서브넷 그리고 내부 네트워크의 라우팅 테이블을 재구성해야만 가능하다. 그러나 스크리닝 라우터가 존재하기 때문에 이는 힘들다.
비록 Bastion 호스트가 침해되었더라도 침입자는 내부 네트워크상에 존재하는 호스트로 침입해야 하고, 그리고 스크린드 서브넷를 액세스하기 위해서 스크리닝 라우터를 통과해야 한다.

- 장점
  - 스크린 된 호스트 게이트웨이 침입차단시스템의 장점을 그대로 가진다.
  - 융통성이 뛰어나다.
  - 해커들이 내부 네트워크를 공격하기 위해서는 방어벽을 통과할 것이 많아 침입이 어렵다.
  - 매우 안전하다.

● 단점
- 다른 침입차단시스템들 보다 설치하기 어렵고, 관리하기 어렵다.
- 침입차단시스템 구축 비용이 많다.
- 서비스 속도가 느리다.

바. Proxy 서버/응용 게이트웨이

응용 게이트웨이 혹은 proxy 서버는 침입차단시스템(일반적으로 Bastion 호스트)에서 구동되는 응용 소프트웨어를 말하는데 store-and-forward 트래픽 뿐만 아니라 대화형의 트래픽을 처리할 수 있으며, 사용자 응용 계층에서 트래픽을 분석할 수 있도록 프로그램 된다. 따라서 이것은 사용자 단계와 응용 프로토콜 단계에서 액세스 제어를 제공 할 수 있고, 응용 프로그램의 사용에 대한 기록을 유지하고 감시 추적을 위해서도 사용될 수 있다. 응용 게이트웨이는 사용자 단계에서 들어오고 나가는 모든 트래픽에 대한 기록을 관리하고 제어할 수 있으며, 해커 및 불법 침입자를 방어하기 위해서 강력한 인증 기법이 필요하다.

응용 게이트웨이는 사용되는 응용 서비스에 따라 각각 다른 소프트웨어를 구현하여 사용하기 때문에 고수준의 보안을 제공할 수 있다.

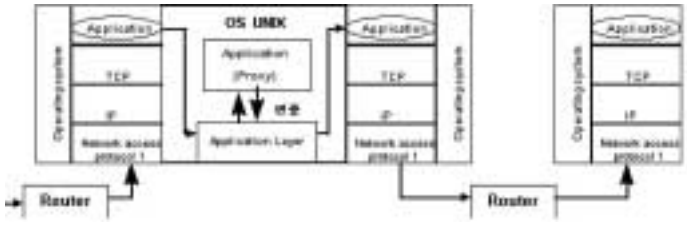
네트워크에 첨가되고 보호가 필요한 새로운 응용이 생기면 이를 위해 새로운 특수 목적용 코드를 생성해야 한다.

응용 레벨 게이트웨이를 사용하기 위해서 사용자는 응용 게이트웨이 장치에 로그인하거나 서비스를 이용할 수 있는 특수한 클라이언트 응용 서비스를 실현해야 한다. 각각 응용에 따라 다르게 사용하는 특수한 게이트웨이는 제각기 내부에 관리 도구와 명령 언어를 가지고 있다.

응용 게이트웨이는 실제 서버의 관점에서 볼 때 클라이언트처럼 동작하며, 클라이언트 관점에서 볼 때는 실제 서버처럼 동작한다. 응용 게이트웨이의 실현 예는 TELNET 게이트웨이, FTP 게이

트웨이, Sendmail, NNTP News Forwarder 등이 있다.

Application(Proxy) Gateway
(그림 6-3-7)



- 장점
  - 응용 서비스마다 각각 다른 응용 게이트웨이를 구현하므로 보다 안전 하게 보호할 수 있다.
  - 응용 사용에 따른 기록 및 감시 추적을 유지 관리 가능하다.
  - 융통성이 좋다.
  - 정보보호 서비스를 응용 게이트웨이에 구현 가능하다.

- 단점
  - 응용 서비스마다 제각기 다른 응용 게이트웨이가 필요하다.
  - 사용되는 응용 서비스가 증가할수록 구축 비용이 증가한다.

제4절 침입탐지시스템

1. 개요

침입탐지시스템의 일반적인 구조는 다음과 같다.

데이터 수집 ⇨ 데이터 축약(reduction) ⇨ 탐지 ⇨ 응답(resopnse)

즉 침입탐지시스템은 보호하고자 하는 시스템으로부터 침입을 판단하기 위한 데이터를 수집하고

중복된 데이터나 쓸모 없는 데이터를 필터링하고 탐지 기법을 사용해 침입을 탐지하고 그에 해당하는 응답을 하는 시스템이다.

2. 구축 시 고려사항

- 다양한 침입탐지가 가능한가?
  가장 다양하고 많은 침입유형을 탐지할 수 있는 제품을 선택하는 것이 안정적이다. 이를 결정하는 요인으로 침입탐지 룰(rule)의 종류와 그 갯수이다. 또한 도입 목적에 맞는 침입유형을 탐지할 수 있는지도 검증해 봐야 한다.

- 오탐률이 낮은가?
  침입탐지시스템 운영의 대부분은 침입탐지 결과가 사실인지 확인하는 것이다. 만약 침입탐지를 발견한 결과, 그중 약 5%만이 침입이고 나머지는 잘못 탐지한 것(오탐)이라면 그 제품은 제대로 역할을 못하는 것이다. 각종 응용프로토콜이나 서비스에 맞는 정밀한 해석기능과 침입탐지시스템 회피(evasion) 공격에 대응할 수 있는 기능을 갖추고 있는지 체크해야 한다.

- 침입탐지 룰(rule)의 업데이트가 신속한가?
  새로운 침입유형을 탐지하기 위해서는 반드시 '침입탐지 룰' 이나 기능의 업데이트가 필요하다. 지난해 여름에 발생한 '코드레드 웜' 의 경우 취약점이 발견된 시기와 공격이 활발했던 시기가 몇 개월간 차이가 있어 미리 취약점을 대비한 곳은 큰 피해를 입지 않았다. 또한 오래된 취약점은 이미 대부분 패치가 이뤄져 실제 공격이 성공할 가능성이 적으며 이를 탐지하는 것도 큰 의미가 없다.

- 환경에 맞는 유연한 설정이 가능한가?
  제품의 성능이 뛰어나도 모든 운영환경에 최적화되지는 않는다. 환경적인 요인으로 인해 오용탐지가 발생할 가능성도 있다. 따라서 사용자 권한에 따라 침입과 업무 수행을 별도로 분류할 수 있어야 하며 많은 침입탐지 룰에 대한 적절한 설정과 정책을 수립하기 위해 룰설

명서와 같은 충분한 자료가 제공돼야 한다.

- 다양한 침입대응 기능을 제공하는가?
  침입탐지시스템이 침입을 탐지 했다해도 그 사실을 관리자가 즉시 인지할 수 없거나 침입을 방관하고 있다면 무용지물이 된다. 관리자에게 침입탐지 정보를 즉시 통보하기 위해 핸드폰 알림 등을 지원하는지, 침입 세션 차단기능과 같은 능동적 대응이 가능한지를 검증해야 한다.

- 침입 재현 기능이 제공되는가?
  침입 재현 기능은 관리자가 실질적인 대응을 위해 필수적인 기능이다. 침입을 탐지하고 그 사실을 확인했다고 해도 정확한 침입경로나 피해상황을 파악할 수 있어야 향후 대처방안을 결정할 수 있기 때문이다.

- 타 시스템과 유기적인 연동이 가능한가?
  침입탐지시스템의 침입탐지 결과를 방화벽이나 기타 다른 정보보호시스템과 유기적으로 연동 대응해 보안성을 향상시킬 수 있어야 한다. 또한 전사적인 보안관리가 가능하다면 대규모 정보보호시스템들을 효과적으로 운영할 수 있다.

- 자기보호 기능을 가지고 있는가?
  침입탐지시스템이 항상 정상적으로 동작하기 위해서는 자체 보호가 필요하다. 실제로 일부 침입탐지시스템들은 네트워크 상의 해킹 시도는 탐지하지만 정작 침입탐지시스템 자체에 대한 침입시도에 취약하다. 따라서 침입탐지시스템의 중요 파일들에 대한 무결성 검사 기능이나 접근제어 기능, 침입탐지시스템이 외부에 노출되지 않도록 하는 stealth mode 등의 자기보호 기능을 제공하는 제품을 선택하는 것이 좋다.

3. 침입탐지시스템의 종류

침입탐지시스템의 분류는 보호하고자 하는 타켓 시스템 즉 참입을 판단하기 위한 데이터를 제공

하는 소스(source)에 따라 분류가 이루어지는데 크게 네트워크 기반(network-based) 침입탐지시스템과 호스트 기반(host-based) 침입탐지시스템으로 분류된다. 네트워크 기반 침입탐지시스템이 좀 더 일반적이며 네트워크를 통해 전송되는 트래픽을 검사하여 침입을 탐지 하게 된다. 반면 호스트 기반 침입탐지시스템은 로컬 호스트에서 사용자의 행위나 프로세스들(processes)을 검사하여 침입을 탐지하게 된다.

가. 호스트 기반 침입탐지시스템

호스트 기반 침입탐지시스템은 단일 호스트에서 침입을 탐지 하는 것으로 그 호스트의 감사(audit) 기록이나 들어오는 패킷 등을 검사하여 침입을 탐지하게 된다. 예를 들어 호스트에 login 프로세스를 감시하고 root 사용자의 행동을 감시하며, 파일 시스템 감시 등을 통해 침입을 발견하는 것이다.

호스트 기반 침입탐지시스템은 가능한 공격에 대해 꽤 강력한 도구로 사용될 수 있다. 예를 들어, 시스템 로깅을 통해 공격자가 어떤 행위를 했는지 어떤 파일을 열었고, 어떤 시스템 콜(system call)이 실행되었는지 등을 알 수 있다. 또 네트워크 기반 침입탐지시스템 보다 잘못된 탐지, 즉 침입이 아님에도 불구하고 침입이라 판단 하는 경우가 좀 더 적다.

호스트 기반 침입탐지시스템의 단점으로는 우선 침입탐지시스템을 타겟 호스트에 설치해야 하므로 해당 호스트의 성능이 저하되고 데이터를 얻기 위해 로깅 등에 대한 설정이 번거로우며 타겟 호스트가 있는 네트워크 내의 다른 호스트들이 공격을 당해도 알 수가 없다.

나. 네트워크 기반 침입탐지시스템

네트워크 기반 침입탐지시스템은 패킷 스니퍼(packet sniffer)와 패킷 모니터(packet monitor) 도구의 발전으로 볼 수 있다. 네트워크의 모든 트래픽에 대해 패킷을 수신하고 분석하여 침입을 발견하는 일이 엄청나게 복잡함은 당연하다. 이를 자동으로 처리하는 것이 바로 네트워크 기반 침입탐지시스템라고 볼 수 있다.

네트워크 기반 침입탐지시스템은 특히 권한 없이 접근한다거나 권한을 초과하는 접근에 대한 탐지에 뛰어난 편이다. 또한 네트워크내의 호스트나 서버에서의 별도의 설정 없이 사용이 가능하며, 오류 발생시 라우터나 방화벽과는 달리 큰 피해를 주진 않는 편이다.

반면 네트워크 기반 침입탐지시스템은 성능에 대한 요구사항 때문에 서명 분석(signature analysis)를 하는 경우가 많은데 이는 일반적인 알려진 공격을 탐지하는데는 뛰어나나 복잡한 정보를 가진 위협요소에 대한 공격은 탐지하기가 어렵다. 또한 분석을 위해 엄청난 양의 데이터 교환을 필요로 할 수 있다. 이를 위해 분석을 위한 데이터를 축약 과정을 통해 필터링하게 된다. 물론 모든 패킷에 대한 분석이 좀 더 많은 침입을 좀 더 정확히 탐지할 수 있음은 당연하다. 네트워크 기반 침입탐지시스템은 암호화 세션(encrypted session)에 대한 침입 탐지는 뛰어 나지 않다. 상용 침입탐지시스템 중 60% 이상이 네트워크 기반 침입탐지시스템이며 오픈 소스로도 개발이 진행되고 있다.

4. 침입탐지 기법

가. 비정상 행위 탐지(anomaly detection)

비정상 행위 탐지는 정상적인 시스템 사용에 대한 프로파일 상태를 유지하며 이에 어긋나는 행위를 탐지하는 방식이다. 즉 시스템 가동 전에 정상적인 행동에 대한 프로파일을 작성해 두고 가동 후에 현재 행위들을 정상적인 프로파일과 비교하여 공격을 탐지하게 된다. 비교 과정에서 기존의 프로파일을 수정하거나 새로운 프로파일을 추가하기도 한다.

비정상 행위 탐지를 위한 접근 방식은 다음과 같다.

- 통계적 접근(Statistical approaches)
  이 방식은 과거의 통계 자료를 바탕으로 현재 프로세스의 행위를 관찰하여 프로파일을 작성하고 작성된 프로파일을 통해 비정상 정도(anomality)를 측정하여 침입을 탐지한다. 비교적 정확한 탐지가 가능하다고 알려져 있다.

- 예측 가능 패턴 생성(Predictive pattern generation)
  이 방식은 해당 순간까지 발생한 이벤트들을 바탕으로 다음 이벤트를 예측하여 침입을 탐지하게 된다. 즉 룰에 따라 어떤 이벤트들이 순차적으로 발생했다고 가정하면 그 후에 발생할 수 있는 이벤트와 그것의 발생확률까지 예측이 가능하게 된다.

- 신경망(Neural networks)
  이 방식은 현재까지의 사용자의 행동이나 명령이 주어졌을 때 사용자의 다음 행동이나 명령을 신경망이 예측하도록 훈련시킨 후 실제 사용자들의 프로파일을 작성케 하여 이를 이용하여 침입을 탐지한다.

비정상 행위 탐지는 알려지지 않은 새로운 공격 기법도 탐지가 가능하다는 장점이 있지만 그에 앞서 정상적인 행위에 대한 프로파일을 구축해둬야 하기 때문에 많은 데이터의 분석이 필요하게 된다. 때문에 상대적으로 구현 비용이 큰 편이고 그만큼 어렵기 때문에 상용 제품에서는 오용 탐지를 주로 사용하고 비정상 행위 탐지는 보조하는 측면에서 사용되고 있다.

나. 오용 탐지(misuse detection)

오용 탐지는 알려진 취약성을 통한 공격에 대한 정보를 가지고 실제적인 공격이 시도될 때 이를 탐지하는 방식이다. 비정상 행위 탐지가 침입으로 여겨지는 행위를 탐지한다면 오용 탐지는 명백한 침입을 탐지하게 된다.

오용 탐지를 위한 접근 방식은 다음과 같다.

- 전문가 시스템(Expert system)
  이 방식은 매칭 부분과 액션 부분을 구분한 if-then 룰을 이용해 현재 행위와 일치하는 공격 패턴을 찾는 방식으로 정해진 액션을 통해 대응하게 된다. SRI에 의해 개발된 NIDES(Next Generation Intrusion Detection Expert System)가 이 방식을 사용하고 있다.

- 키 모니터링(Keystroke monitoring)
  이 방식은 매우 간단한 것으로 공격 패턴을 keystroke를 모니터링하여 발견하게 된다.

- 상태 전이 분석(State transition analysis)
  이 방식은 시스템의 상태에 따라 전이하면서 공격을 감지하게 된다. USTAT(State Transition Analysis Tool for UNIX) 에서 찾아 볼수 있다.

- 패턴 매칭(Pattern matching)
  이 방식은 알려진 공격 유형들을 패턴으로 가지고 있으면서 현재 행위와 일치하는 패턴을 찾아내 침입을 탐지한다.

오용 탐지는 비정상 행위 탐지와 비교하여 비교적 구현 비용은 저렴하나, 탐지를 위한 데이터가 시스템의 로그 정보를 주로 이용하며 또 최신 공격 기법이 발견되면 룰을 추가해줘야 하는 번거로움이 있다.

c o n t e n t s

제 7 장
네트워크 보안관리

제1절 시스코 라우터의 기본 보안

시스코 라우터는 현재 대부분의 기업인터넷 환경에서 많이 이용하는 인터넷 관문 장비 중 한가지이다. 인터넷 관문 장비의 가장 중요한 역할은 빠른 인터넷 접속을 위한 고속의 데이터 처리라고 할 수 있다. 하지만 최근 들어 네트워크 보안에 대한 관심이 집중되면서, 라우터나 스위치 장비의 올바른 보안설정이 필요하게 되었다. 실제 라우터에 보안 기능을 설정하게 됨으로써, 침입차단시스템이나 침입탐지시스템에서의 보안기능 구현 이전에 또 다른 보안 장비로의 활용이 가능하다.

이것은 침입차단시스템이나 침입탐지 장비의 효율적인 자원 활용에도 도움이 될 뿐만 아니라, 보안의 영역을 한층 더 넓힐 수 있다는 데 그 의미가 크다.

이 절에서는 시스코 라우터 장비 관리의 보안 설정과 기타 보안 설정 구현을 통한 유해 트래픽의 제어 기법을 알아보기로 한다.

1. IOS 버전 보안

현재 시스코 라우터의 운영 체계는 IOS (Internet Operation System)로 구동이 된다. 유닉스나 윈도우즈 운영체계에서의 보안 설정강화를 위해 패치를 받거나 운영체제를 업그레이드 하는 것처럼 , 라우터의 운영체계도 지속적인 업그레이드와 보안 패치가 중요하다.

시스코에서는 IOS에서 제공되고 있는 기능 또는 장비 가운데 보안 취약점이 있는 버전에 대한 패치와 향상된 IOS 및 작업환경에서의 취약점 방지 구성 방법 등을 공개하고 있다. 따라서 시스코 라우터를 사용하고 있는 기업 관리자들은 이러한 정보를 시스코 사의 웹이나 정보보호진흥원의 보안 권고안을 적극 활용할 필요가 있다.

> ※ 다음의 사이트에서 시스코 라우터에 대한 보안권고안과 패치 등을 다운로드 받을 수 있다.
> http://www.cisco.com/en/US/partner/products/products_security_advisory09186a00801d2d9d.shtml

먼저 시스코 IOS 버전은 아래와 같은 방법으로 확인이 가능하다.

IOS 버전 확인
(그림 7-1-1)

2. 기본 접근 통제

가. 로컬 사용자 접근 통제

시스코 라우터의 접근 통제는 보안의 가장 기본이라 할 수 있다.

시스코 라우터의 접근 방법은 크게 콘솔을 통한 장비에 직접 접속할 수 있는 방법과 모뎀(AUX)이나 텔넷 등을 통한 접속이 있다. 이러한 접근에 대한 적절한 권한 부여와 접속 제한은 장비 보안의 기본이다.

접속 제한의 방법으로는 패스워드 설정을 통한 방법이 있다. 그러나 패스워드는 기본적으로 일반적인 문자열(Clear Text)로 전송하게 됨으로 네트워크 상에서 노출될 가능성이 있으므로 되도록이면 암호화하여 전송하도록 구성하는 것을 권고한다.

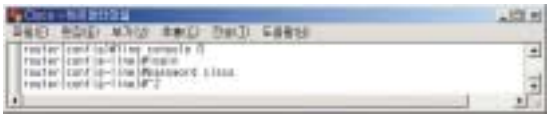
(1) 콘솔 포트 패스워드 보안

콘솔 패스워드를 설정하기 위해서는 아래와 같은 명령어를 적용 한다.

```
login  #라우터에 접근하기 위해서 로그인 과정을 반드시 통과해야 한다는 의미#
password "사용을 원하는 콘솔 패스워드"
```

아래 화면은 콘솔 패스워드를 cisco로 설정한 예를 보여주고 있다.

콘솔 패스워드를 cisco로 설정한 예
(그림 7-1-2)



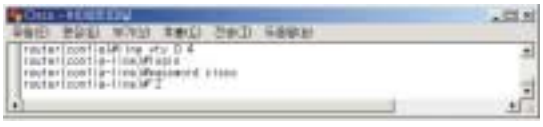
(2) AUX, VTY 포트 패스워드 보안

아래 화면은 AUX 포트의 패스워드를 "cisco"로 설정하는 예를 보여주고 있다

AUX 포트의 패스워드 설정 예
(그림 7-1-3)

아래 화면은 VTY 라인 0~4의 패스워드를 "cisco"로 설정하는 예이다.

VTY 라인 0~4의 패스워드 설정 예
(그림 7-1-4)



(3) 안전한 enable 패스워드 설정방법

시스코 라우터는 레벨 1에서 레벨 15까지 15 단계의 권한 수준이 있다. Enable 명령어를 사용하여 privileged EXEC 모드로 레벨을 변경하면 조회뿐만 아니라 설정 변경 등의 작업을 할 수 있다. privileged EXEC 모드로 변경할 때 사용하는 enable 패스워드를 설정하기 위해서는 enable password와 enable secret의 두 가지 명령어를 사용할 수 있다.

① enable password

enable password 명령어는 기본적으로 패스워드를 암호화하지 않는다. enable password 명령을 실행한 다음 service password-encryption 명령을 사용하면 패스워드를 암호화할 수 있지만 암호화 방법이 비교적 취약하여 보안 유지가 어렵다. enable password 명령어를 사용하여 패스워드를 설정하기 위해서는 아래와 같은 명령을 사용한다.

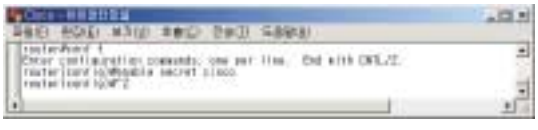
아래 화면은 enable password 명령을 사용하여 패스워드를 "cisco"로 설정하고 이를 암호화한 예를 보여주고 있다.

enable password를 이용한 패스워드 설정 및 암호화 예
(그림 7-1-5)

② enable secret

enable secret는 MD5 알고리즘을 이용하여 암호화된 패스워드를 설정 한다.

아래 화면은 enable secret 명령을 사용하여 패스워드를 "cisco"로 설정한 예를 보여주고 있다



enable secret를 이용한 패스워드 설정 예
(그림 7-1-6)

(4) 사용자 계정 관리

위에서 살펴본 시스코 라우터 인증 방법은 사용자를 별도로 설정하지 않으므로 여러 명의 관리자가 라우터를 관리하는 경우에는 적합하지 않다. 여러 관리자에 의하여 라우터가 관리되는 경우에는 여러 명의 사용자를 생성하고 사용자별로 패스워드를 설정해야 한다. 그 설정 방법은 아래와 같다.

```
transport input none
no exec
exec-timeout 0 1
username "사용자이름" password "사용자별 패스워드"
login local
```

아래 화면은 새로운 사용자 "admin1"을 생성하고 패스워드를 "cisco1"로 설정한 뒤에 이를 VTY 라인에 적용하는 예를 보여준다.

VTY 라인에 적용하는 예
(그림 7-1-7)

(5) 콘솔, AUX, VTY 포트로의 접속 차단

No password 명령을 사용하여 어떤 사용자도 해당하는 라인에 접속할 수 없도록 설정할 수 있다. No password 명령은 패스워드를 입력하지 않고 사용자가 라우터에 접속할 수 있도록 하는 명령어가 아니라 설정되어 있는 패스워드를 제거하고 어떤 사용자도 접속할 수 없도록 하는 명령어이다. no login 명령을 사용하면 로그인 과정 없이 모든 사용자가 접속할 수 있게 한다.

아래 화면은 AUX 포트를 차단한 예를 보여준다.

VTY 라인에 적용하는 예
(그림 7-1-8)

나. 원격으로부터 접근 통제

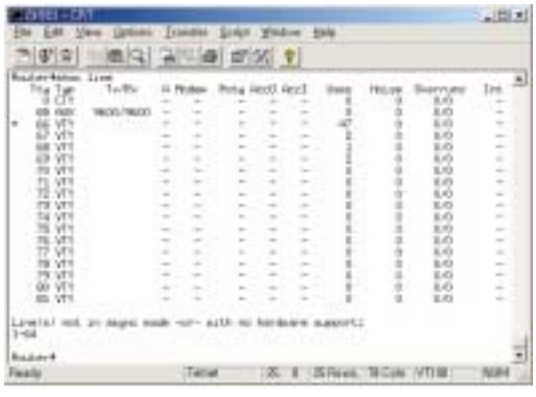
원격에서 라우터를 관리할 수 있는 방법으로는 AUX 포트에 모뎀을 이용하여 접속하는 방법과 VTY 포트를 사용한 텔넷, HTTP 접속 등이 있다.

(1) AUX 포트를 이용한 안전한 접속

AUX 포트의 기본적인 목적은 원격의 관리자로 하여금 모뎀을 통하여 라우터에 접속할 수 있도록 하는 것이다. AUX 포트 패스워드를 반드시 설정하여야 한다.

(2) Reverse 텔넷을 이용한 안전한 접속

Reverse 텔넷은 물리적으로 연결된 포트를 네트워크 연결을 이용하여 접속하는 것을 의미한다. 현재 라우터에 설정되어 있는 라인 목록을 보기 위해서는 show line 명령을 사용할 수 있으며 아래 화면은 show line 명령을 실행한 예이다.



show line 명령을 실행한 예
(그림 7-1-9)

transport input none 명령을 사용하여 해당되는 라인의 네트워크 접속을 차단시킨다.

(3) 텔넷을 이용한 안전한 접속

텔넷을 사용하여 라우터에 접속하게 되면 네트워크를 통과하는 모든 데이터가 암호화되지 않은 형태이므로 보안 취약점을 지니게 된다. 따라서 라우터에 접속된 후 전송되는 데이터까지도 암호화할 것을 권고한다.

현재 시스코 라우터에서는 이러한 텔넷 접속 후 전송되는 데이터의 암호화를 위해 SSH(Secure Shell Host)를 통한 접속을 지원하고 있다. 또한 특정 사용자, 관리자 등 정의된 사용자들만 라우터 장비에 접속할 수 있도록 접근 제어 목록을 설정할 수 있다.

① SSH를 사용한 텔넷 접속

SSH를 설정하는 방법은 다음과 같다.

```
Router(config)# hostname "router name"
Router-name(config)# ip domain-name "domain name"
Router-name(config)# crypto key generate rsa
Router-name(config)# ip ssh time-out "time out value"
Router-name(config)# ip ssh authentication-retries "retries value"
Router-name(config)# line vty 0 4
Router-name(config-line)# transport input ssh
```

② IP 주소 필터링을 통한 텔넷 연결

기본적으로 VTY 포트는 외부로부터의 연결 시도를 모두 받아들인다. 라우터로 들어오는 패킷의 IP 주소를 필터링하여 허가된 IP를 가진 사용자에게만 연결 시도를 허용한다.

아래의 화면은 172.16.5.105, 172.16.5.106 IP 주소를 가진 사용자만이 VTY 포트로 접속을 할 수 있게 하는 "10번" ACL을 생성하고 이것을 적용하는 방법을 보여주고 있다

10번 ACL을 생성 및 적용 방법
(그림 7-1-10)

③ 안전한 텔넷 연결을 위한 추가 설정

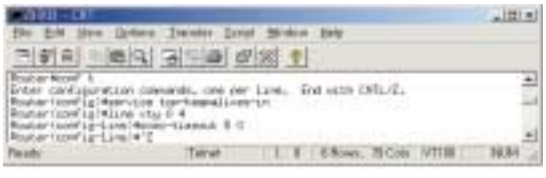
추가적으로 VTY 접속을 보다 안전하게 하기 위해서 아래의 명령어가 사용될 수 있다.

```
exec-timeout [분] [초]
```

Service tcp-keepalives-in 명령어를 사용하면 라우터의 모든 연결을 계속 모니터링하면서 비정상적으로 종료된 세션을 발견하면 이를 종료시킨다. 명령어의 사용법은 아래와 같다.

```
service tcp-keepalives-in
```

아래 화면은 VTY라인에 service tcp-keepalives-in 명령을 적용하고 exec-timeout을 5분 0초로 적용하는 예를 보여준다.



service tcp-keepalives-in 명령 사용 예
(그림 7-1-11)

3. 안전한 사용자 관리 및 권한 부여

가. 텍스트 형태의 패스워드의 암호화

콘솔, AUX, VTY 등의 라인에 적용한 패스워드 및 기타 설정 사항을 살펴보기 위해서는 show run 명령을 사용한다. show run 명령을 실행한 결과에서 패스워드 설정 부분은 아래의 화면과 같다.

Show run 명령 사용 예
(그림 7-1-12)

텍스트 형태로 노출된 패스워드는 공격 대상이 될 수 있기 때문에 암호화가 요구된다. 이와 같이 암호화되지 않은 상태로 저장되어 사용되는 대표적인 패스워드들은 아래와 같다.

- enable password 명령을 사용하여 설정한 패스워드
- username 명령을 사용하여 설정한 사용자별 패스워드

위에서 설명한 패스워드들은 Vigenere 암호화를 사용하는 service password-encryption 명령을 사용하여 암호화를 할 수 있다. 아래 화면은 service password-encryption 명령을 적용한 예를 보여준다.

service password-encryption 명령 사용 예
(그림 7-1-13)

위의 명령을 사용하여 암호화를 하고 나서 다시 show run 명령을 실행하면 아래와 같이 사용자별 패스워드, 콘솔, AUX, VTY 등의 라인에 적용된 패스워드가 암호화되었음을 알 수 있다.

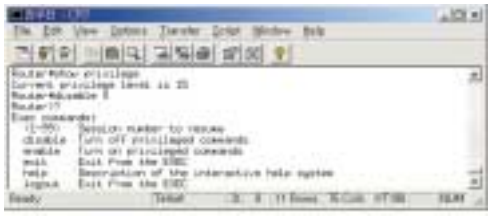
사용자별 패스워드 암호화 예
(그림 7-1-14)

나. 권한 수준

시스코 IOS에서는 0에서 15에 이르는 16개의 서로 다른 권한 수준을 규정하고 있다. show privilege 명령을 사용하여 현재의 권한 수준을 조회할 수 있다. 아래의 화면은 설정하기 전의 사용자 EXEC 모드에서는 레벨 1이며, enable을 하고 난 뒤의 privileged EXEC 모드에서는 레벨 15임을 보여준다.

enable 전 · 후 권한 변화 예
(그림 7-1-15)

각 권한 수준간의 이동은 enable, disable 명령을 사용하여 할 수 있다. enable, disable 명령 뒤에 아무것도 입력하지 않으면 기본적으로 라우터에 지정된 레벨인 레벨 1과 레벨 15 사이를 자동으로 전환하며 뒤에 이동하고자 하는 레벨 번호를 붙이면 해당하는 레벨로 이동한다. 아래 화면은 레벨 15에서 레벨 0으로 이동하여 레벨 0에서 실행 가능한 명령어 리스트를 조회하는 방법을 보여준다.



레벨 0에서 실행 가능한 명령어 리스트를 조회
(그림 7-1-16)

다. 사용자별 권한 수준 지정

특정한 사용자의 라우터 사용 및 설정 권한을 제어하기 위하여 사용자별로 권한 수준을 적용할 수 있다. 사용자별로 권한 수준 지정하는 방법은 아래와 같다.

```
username "사용자이름" privilege "권한" password "사용자별 패스워드"
```

다음은 사용자 "kiyoung"에게는 level 10의 권한을 사용자 "young"에게는 level 5의 권한을 부여한 예이다.

사용자별 권한 부여 예
(그림 7-1-17)

라. 명령어별 권한 수준 지정

특정 명령에 대해서도 권한 수준을 적용할 수 있는데 그 사용법은 아래와 같다.

```
privilege exec level "권한" "권한을 적용할 서비스명"
```

아래의 화면은 텔넷은 레벨 10 이상의 사용자만이 debug는 레벨 5 이상의 사용자만이 실행 가능하도록 설정한 예이다.

서비스별 권한 부여 예
(그림 7-1-18)

4. 불필요한 프로토콜과 서비스 제거

시스코 라우터는 대부분의 프로토콜과 서비스들을 인식하고 라우팅되도록 제공하고 있다. 이는 다양한 사용자가 특별한 설정 없이 라우터를 이용하기 용이하도록 제공하기 위함이다. 따라서 기업 사용자의 환경에 따라서 불필요한 프로토콜과 서비스는 제거할 것을 권고한다.

가. ICMP

(1) ICMP MTU Discovery

MTU[10] discovery는 데이터 링크 계층에서 출발지와 도착지 사이를 지나는 패킷 크기를 조절해 주는 역할을 한다. ICMP 패킷을 차단하더라도 MTU discovery를 제공하는 패킷은 허용해야 네트워크가 제대로 동작할 수 있다.

아래와 같은 ACL을 적용하게 되면 MTU discovery를 담당하는 패킷인 ICMP type 3, 4번 패킷만을 허용하고 다른 ICMP 패킷은 모두 차단하게 된다.

ACL을 적용 예
(그림 7-1-19)

(2) ICMP Redirects

공격자들은 ICMP Redirect를 전송하여 네트워크를 지나는 패킷의 방향을 바꿀 수 있다. 따라서 이 서비스는 차단하는 것이 권장된다.

10) MTU(Maximum Transmission Unit)

① ICMP Redirects - sending

라우터의 인터페이스로 들어오는 ICMP Redirects 패킷을 막기 위해서는 no ip redirects 명령을 각 인터페이스 별로 적용한다. 설정 방법은 아래의 화면과 같다.

설정 방법
(그림 7-1-20)

② ICMP Redirects - receiving

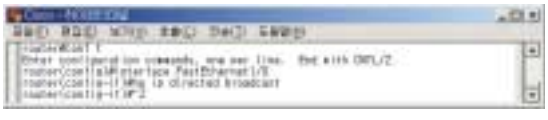
ICMP Redirects 패킷이 라우터로부터 나가는 것을 막기 위해서는 각 인터페이스의 입력 트래픽에 ACL을 적용하여야 한다.

각 인터페이스의 입력 트래픽에 ACL을 적용 예
(그림 7-1-21)

(3) ICMP - Directed Broadcasts

ICMP directed broadcast 가 설정되어 있을 경우, 스머프 공격과 같은 ICMP 공격에 노출될 가능성이 있으므로, 특수한 환경이 아닌 기업에서는 서비스를 제거하는 것을 권고한다.
directed broadcast를 막기 위해서는 no ip directed-broadcast 명령을 라우터의 인터페이스에 적용해야 한다. 그 방법은 아래의 화면과 같다.

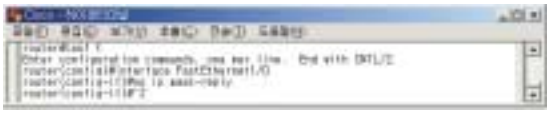
no ip directed-broadcast 명령을 라우터의 인터페이스에 적용
(그림 7-1-22)



(4) ICMP Mask Reply

ICMP mask reply는 라우터로 하여금 해당되는 네트워크의 서브넷 마스크를 전송하도록 한다. 공격자는 이 기능을 이용하여 네트워크의 구성을 알아낼 수 있으므로 이 기능은 차단할 것을 권장한다.

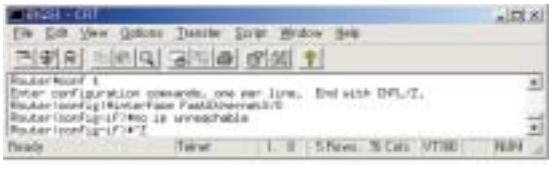
이 기능을 차단하기 위해서는 no ip mask-reply 명령을 사용할 수 있으며 그 사용법은 아래와 같다.



no ip mask-reply 명령을 사용
(그림 7-1-23)

(5) ICMP Unreachable

ICMP Unreachable은 공격자에 의해 스캐닝에 이용될 수 있다.
ICMP Unreachable을 차단하기 위해서는 아래와 같이 인터페이스 별로 no ip unreachable 명령을 사용한다.



인터페이스 별로 no ip unreachable 명령을 사용
(그림 7-1-24)

(6) ICMP Timestamp and Information Requests

ICMP Timestamp and Information Requests는 공격자가 네트워크 현황을 알 수 있는 정보를 제공하므로 차단할 것을 권고한다.

아래의 화면은 ACL을 적용하여 두 개의 서비스를 차단하는 방법을 보여준다.

ACL을 적용하여 두 개의 서비스를 차단하는 방법
(그림 7-1-25)

나. Source Routing

Source Routing은 패킷이 네트워크의 어떤 경로를 거쳐서 전달되는가를 보여주는 취약점이 존재한다. 또한 Source Routing은 IP 라우팅 경로를 변조할 수 있으므로 기본 취지와 어긋난 악의적인 목적으로도 사용될 수 있다.

아래의 화면은 no ip source-route 명령을 사용하여 이를 차단하는 방법을 보여준다.

no ip source-route 명령을 사용하여 이를 차단하는 방법
(그림 7-1-26)

다. Small Services

시스코 라우터에 사용되고 있는 IOS 버전에 따라서 TCP, UDP Small Services가 자동으로 설정되어 실행된다. 이러한 서비스는 네트워킹에 특별히 중요한 역할을 담당하지는 않기에 모두 차단할 것을 권장한다. 아래의 화면은 no service tcp-small-servers와 no service udp-small-servers 명령을 사용하여 각각 TCP, UDP 서비스들을 차단하는 방법이다.

TCP, UDP 서비스들을 차단하는 방법
(그림 7-1-27)

라. Finger

Finger 서비스는 원격의 사용자로 하여금 어떤 사용자가 라우터에 접속해 있는지를 알려주는 역할을 한다. no service finger 명령을 사용하여 finger 서비스를 차단시킬 수 있지만, 원천적으로 finger 요청 자체를 받아들이지 않도록 동작하지는 않는다. 이를 해결하기 위해서는 라우터의 인터페이스로 들어오는 TCP 포트 79번 패킷을 ACL을 이용하여 차단한다.

ACL을 이용하여 차단
(그림 7-1-28)

마. HTTP

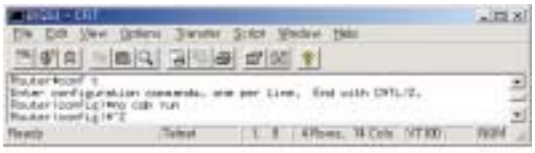
시스코 라우터는 http 프로토콜을 사용하여 원격에서 여러 가지 기능 설정이 가능하다. 웹 기반에서의 라우터 관리를 하지 않는 기업 환경에서는 불필요하게 웹 서비스를 동작시킬 필요는 없다. 따라서 no ip http server 명령을 사용하여 차단할 것을 권고한다.

no ip http server 명령을 사용하여 차단
(그림 7-1-29)

바. CDP(Cisco Discovery Protocol)

CDP는 시스코 장비와 직접 연결된 시스코사의 장비 정보를 열람하는 기능을 제공하고 있다. 사용목적에 따라 CDP는 공격자에게 유용한 정보를 제공하므로 사용에 주의하여야 한다. CDP를 라우터 전체에서 사용 불가능하게 하기 위해서는 no cdp run 명령어를 사용하며, 특정 인터페이스에서 사용하지 못하게 하려면 no cdp enable 명령어를 사용한다.

no cdp run 명령어를 사용 (그림 7-1-30)



no cdp enable 명령어를 사용 (그림 7-1-31)

사. Proxy ARP(Address Resolution Protocol)

Proxy ARP는 디폴트 라우터나 게이트웨이를 가지고 있지 않은 네트워크의 호스트들에게 ARP 서비스를 제공하는 역할을 한다. 공격자들은 패킷의 주소를 위조하여 Proxy ARP를 요청할 수 있으며 라우터가 이에 응답하는 것을 이용하여 라우터와 네트워크에 관련된 정보를 획득할 수 있다.

Proxy ARP를 차단하기 위해서는 no ip proxy-arp 명령을 사용할 수 있으며 그 사용 예는 아래와 같다.

no ip proxy-arp 명령을 사용 (그림 7-1-32)

5. 안전한 라우팅과 주소 위조 방지

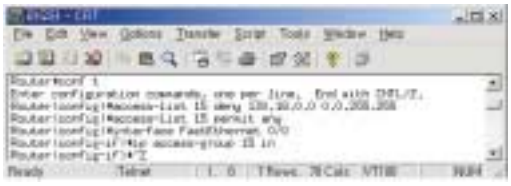
가. 주소 위조 방지

라우터를 경유하여 전체 네트워크를 공격할 수 있는 주소가 위조 되었을 경우, 라우터에서 필터링을 통해 주소의 무결성을 유지 할 수 있다.

(1) 입/출력 필터링

① 입력 필터링

입력 필터는 먼저 외부로부터 유입되는 패킷의 주소가 내부의 네트워크 범위에 포함되는 주소가 아닌가를 판별한다. 아래의 화면은 출발지 주소가 130.18.X.X인 패킷이 라우터로 유입되는 것을 금지하는 ACL을 생성하고 이를 적용시킨 예이다.



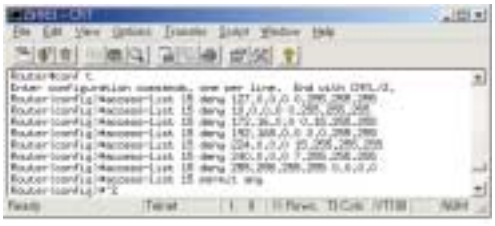
입력 필터링
(그림 7-1-34)

주소 위조 방지 필터는 또한 예약된 IP 주소를 가진 패킷이나 사설 IP 주소를 가진 패킷도 차단해야 안전하다. 이와 같이 일반적으로 외부로부터 유입되는 것을 차단해야할 네트워크 주소 목록은 아래와 같다.

- o 127.0.0.0/8
- o 10.0.0.8/8
- o 172.16.0.0/12
- o 192.168.0.0/16
- o 224.0.0.0/4
- o 240.0.0.0/5
- o 255.255.255.255/32

위에서 나열한 네트워크 주소를 가진 패킷이 라우터로 유입되는 것을 막기 위해서는 아래와 같은 ACL을 생성하여 적용하면 된다.

ACL을 생성하여 적용
(그림 7-1-35)



② 출력 필터링

출력 필터링은 내부 네트워크로부터 주소가 위조된 IP 주소를 가진 패킷이 유출되는 것을 방지한다. ACL을 이용하여 내부 네트워크 IP 주소를 가진 패킷만 라우터로부터 전송되는 것을 허용하고 나머지 패킷들은 모두 차단한다.

내부 네트워크 주소가 130.218.0.0/16 인 경우의 ACL 적용한 예는 아래와 같다.

출력 필터링
(그림 7-1-36)

(2) uRPF(Unicast Reverse Packet Forwarding)

uRPF 기능은 관리자로 하여금 위조된 IP 주소를 가진 패킷을 차단하도록 할 때 사용한다. uRPF를 사용하기 위해서는 아래와 같이 설정하여야 한다.

```
ip cef
ip verity unicast reverse-path
```

아래는 uRPF를 FastEthernet0/0 인터페이스에 설정한 예이다.

```
Router(config)#ip cef
Router(config)#interface FastEthernet0/0
Router(config-if)#ip verify unicast reverse-path
```

나. 라우팅 프로토콜 보안

(1) Static 라우팅

공격자가 임의로 라우팅 정보를 조작할 수 없기 때문에 가장 안전한 라우팅 방법이다.

(2) Dynamic 라우팅 - 인증

Dynamic 라우팅을 가장 안전하게 사용하는 방법은 라우팅 프로토콜에 인증 기능을 적용하는 것이다.

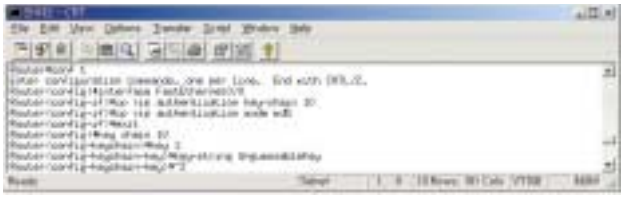
① RIP v2

RIP v1는 인증 기능을 제공하지 않는 단점이 있다. RIP v2 프로토콜은 이를 개선하여 텍스트 형태의 패스워드를 지원한다. RIP v2 프로토콜에 인증 기능을 적용하기 위한 방법은 아래와 같다.

- 인터페이스 설정 모드에서 key-chain을 설정
  ip rip authentication key-chain [key-chain 번호]
- 인터페이스 설정 모드에서 MD5를 이용하여 암호화된 패스워드 사용
  ip rip authentication mode md5
- Global 설정 모드에서 key-chain 설정
  key chain [key-chain 번호]
- Keychain 설정 모드에서 key 번호 설정
  key [key 번호]
- Keychain-key 설정 모드에서 key 스트링 설정
  key-string [key 스트링]

위의 방법을 적용한 예는 아래와 같다.

RIP v2 적용 예
(그림 7-1-37)



② EIGRP

EIGRP 프로토콜에 인증 기능을 적용하는 방법은 RIP v2와 유사하다.

- 인터페이스 설정 모드에서 EIGRP 인증을 설정

  ip authentication mode eigrp [AS 번호] md5
- 인터페이스 설정 모드에서 key-chain 설정

  ip authentication key-chain eigrp [AS 번호] [key-chain 이름]
- Global 설정 모드에서 key-chain 설정

  key chain [key-chain 이름]
- Keychain 설정 모드에서 key 번호 설정

  key [key 번호]
- Keychain-key 설정 모드에서 key 스트링 설정

  key-string [key 스트링]

위의 방법을 적용한 예는 아래와 같다.

```
RouterOne(config)#interface FastEthernet0/0
RouterOne(config-if)#ip authentication mode eigrp 10 md5
RouterOne(config-if)#ip authentication key-chain eigrp 10 Chain1
RouterOne(config-if)#exit
RouterOne(config)#key chain Chain1
RouterOne(config-keychain)#key 1
RouterOne(config-keychain-key)#key-string UnguessabeKey
```

③ OSPF

OSPF에 라우팅 정보 교환을 위한 인증을 설정하는 것은 다른 프로토콜의 경우와 비교하여 간단하다.

- 각각의 인터페이스에 ip ospf message-digest-key 명령을 사용하여 key 정의
- area [area 번호] authentication message-digest 명령을 사용하여 OSPF 프로토콜 사용시에 인증을 하도록 설정

```
RouterOne(config)#interface FastEthernet0/0
RouterOne(config-if)#ip ospf message-digest-key 1 md5
                                    UnguessabeKey
RouterOne(config-if)#exit
RouterOne(config)#router ospf 10
RouterOne(config-router)#area 0 authentication message-digest
```

④ BGP

BGP는 기본적으로 텍스트 형태의 패스워드를 지원하지 않고 MD5 인증을 제공하기에 이를 설정하는 과정이 필요 없다. BGP를 설정할 때 neighbor 명령을 사용하여 password 키워드를 명령에 추가함으로써 단순하게 설정이 가능하다.

아래는 AS 번호가 109인 RouterOne, RouterTwo에 BGP 인증을 설정하는 방법이다.

```
RouterOne(config)#router bgp 109
RouterOne(config-router)#neighbor 130.18.6.7 password MyBGPpassword
RouterOne(config)#router bgp 109
RouterOne(config-router)#neighbor 19.6.7.8 password MyBGPpassword
```

6. 로깅(Logging)

시스코 라우터에서는 로깅 기능을 통해서, 장비에서 발생한 이벤트들을 저장하거나 저장된 이벤트를 열람할 수 있는 기능을 제공한다. 이는 보안 사고가 발생하거나 장비가 이상 동작할 경우 분석에 매우 유용한 역할을 수행한다.

가. 라우터 로깅

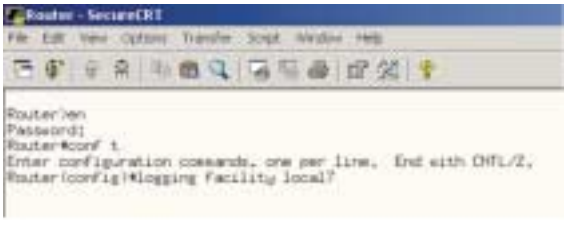
- 콘솔 로깅
  콘솔 로그 메시지는 콘솔 포트에서만 보인다. 따라서 이 로그를 보기 위해서는 반드시 콘솔 포트에 연결하여야 한다.
- Buffered 로깅
  Buffered 로깅은 로그를 라우터의 RAM에 저장한다. 로깅 버퍼가 라우터에 설정되어 있어야 하며 이 버퍼가 가득 차게 되면 오래된 로그는 자동으로 새로운 로그에 의해 대체되게 된다.
- Terminal 로깅
  Terminal monitor 명령을 사용하여 로깅을 설정하면 라우터에서 발생하는 로그 메시지를 VTY terminal에 보내게 된다.
- Syslog
  시스코 라우터는 라우터의 로그 메시지가 외부의 syslog 서버에 저장되도록 설정할 수 있다.
- SNMP traps
  SNMP trap이 설정되면 SNMP는 특별한 상황을 외부의 SNMP 서버에 전송하도록 설정될 수 있다.

(1) 콘솔 로깅

콘솔 메시지를 보기 위해서는 먼저 콘솔 포트에 물리적으로 연결하여야 한다. 콘솔은 기본적으로 레벨 5(Notifications)로 설정되어 있다.

① 콘솔 로깅 레벨의 변경

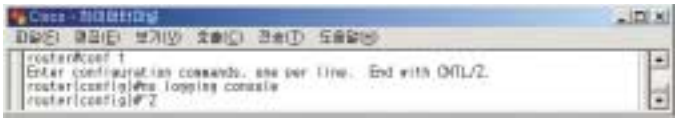
모든 로그 메시지를 보기 원한다면 레벨 7(Debugging)로 설정하면 된다. 아래 화면은 콘솔 로깅 레벨을 레벨 7(Debugging)로 변경한 예를 보여 준다 .



콘솔 로깅 레벨을 레벨 7(Debugging)으로 변경한 예
(그림 7-1-38)

② 콘솔 로깅 차단

적은 양의 로그 메시지일지라도 이를 화면에 보여주는 것은 라우터의 성능에 영향을 미치게 되므로 로깅이 필요하지 않은 경우에는 콘솔 로깅을 차단한다. 아래 화면은 라우터의 콘솔 로깅을 차단하는 예이다.



라우터의 콘솔 로깅을 차단하는 예
(그림 7-1-39)

(2) Buffered 로깅

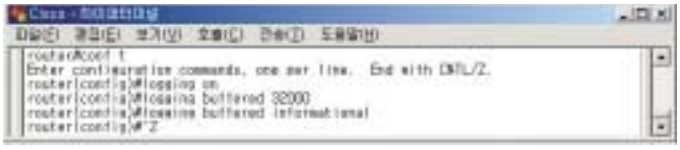
라우터의 버퍼 크기는 RAM 크기를 고려하여 설정 한다. 일반적으로 16Kbyte에서 32Kbyte의 크기가 적당하다.

Buffered 로깅을 설정하기 위해서는 아래와 같은 방법을 사용한다.

- o logging on 명령어를 사용하여 로그를 메모리에 백업하도록 설정
- o logging buffered 명령어를 사용하여 버퍼의 크기를 설정
- o logging buffered 명령어를 사용하여 로깅 버퍼의 severity 레벨을 설정

아래의 화면은 위와 같은 방법을 사용하여 32Kbyte의 크기로 레벨 6 (Informational)의 Buffered 로깅을 설정한 예이다.

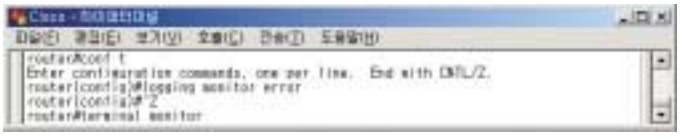
32Kbyte로 레벨 6(Informational)의 Buffered 로깅 설정 예
(그림 7-1-40)



(3) Terminal Monitor

VTY를 통해서 로그 메시지를 받기 위해서는 terminal monitor 명령을 사용한다.
아래 화면은 레벨 3(Errors)으로 severity 레벨을 설정하고 VTY 로깅을 설정하는 과정을 보여준다.

레벨 3(Errors)로 severity 레벨을 설정하고 VTY 로깅 설정 과정
(그림 7-1-41)



로깅을 중단시키려면 terminal no monitor 명령을 사용한다.

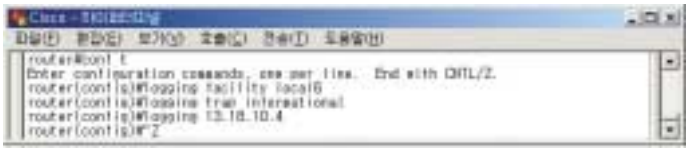
(4) Syslog

① syslog 로깅 설정 방법

syslog 로깅을 설정하기 위해서는 아래와 같은 방법을 사용한다.

- logging facility 명령어를 사용하여 syslog facility를 설정
- logging trap 명령어를 사용하여 syslog severity 레벨을 설정
- logging 명령어를 사용하여 로그 메시지를 저장할 syslog 서버를 지정

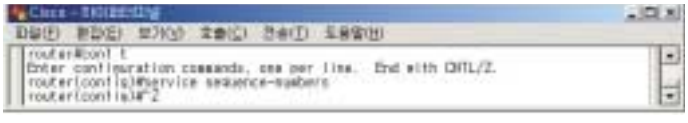
아래 화면은 라우터가 13.18.10.4의 IP 주소를 가진 syslog 서버에 로그 메시지를 저장하도록 하고 facility를 local6로 severity 레벨을 informational로 설정하는 것을 보여주고 있다.



syslog 로깅 설정
(그림 7-1-42)

② Syslog sequence numbers

service sequence-numbers 명령을 사용하여 로그 메시지의 조작여부를 판단 할 수 있게 설정할 수 있다. 아래의 화면은 syslog sequence numbers를 설정하는 방법을 보여주고 있다.



syslog sequence numbers를 설정하는 방법
(그림 7-1-43)

③ syslog 메시지 제한

logging rate-limit "메시지 수" 명령어를 사용하여 라우터에서 로깅 서버로 보내는 메시지 수를 제한할 수 있다.

아래는 이러한 과정을 실행한 예로써 1초에 10개의 메시지만 syslog 서버로 전달되도록 설정하는 것을 보여주고 있다.

1초에 10개의 메시지만 syslog 서버로 전달되도록 설정하는 것
(그림 7-1-44)

나. ACL Violation 로깅

ACL violation 로깅은 ACL을 생성할 때 log 혹은 log-input 키워드를 ACL 끝에 추가하여 설정한다. ACL 로깅은 라우터로 불필요하게 유입되는 트래픽을 막기 위해 설정한 정책에 위반하는

트래픽에 대한 분석을 위해 설정을 하게 된다.

ACL 로깅 기능은 라우터의 CPU 자원을 많이 사용할 수 있기 때문에 ACL 로깅을 설정할 때는 라우터의 CPU 사용율을 점검한 후에 설정하는 것이 좋다.

(1) 주소 위조 방지 로깅

아래는 내부 네트워크가 130.18.0.0/16인 경우 주소 위조 방지를 위하여 입력 트래픽에 130.18.x.x의 IP 주소를 가진 패킷이 유입되지 못하도록 하는 ACL을 적용한 예이다.

주소 위조 방지 로깅
(그림 7-1-45)

(2) VTY 접속 로깅

아래는 172.16.5.105의 IP 주소를 가진 사람만이 VTY 접속을 하도록 설정하고, 접속 실패에 대해서는 로깅을 하도록 하는 예이다.

접속 실패에 대해서는 로깅을 하도록 하는 예
(그림 7-1-46)

제2절 주니퍼 라우터

주니퍼 라우터는 시스코 라우터와 함께 인터넷 관문 장비로써 기업 환경에서 많이 사용되어 지고 있는 라우터 이다.

주니퍼 라우터 역시 제공되고 있는 기능과 장비에 따라 보안 취약점에 대한 해결책으로 새로운 패치 또는 JUNOS가 발표되므로 이에 따라 적절한 조치를 취할 필요가 있다.

1. JUNOS 버전 보안

JUNOS의 버전을 확인하여, 취약한 버전에 대해서는 패치를 적용하거나 최신의 버전을 사용하여야 한다.

가. JUNOS 버전 확인

show system software 명령을 사용하여 버전을 확인한다.

```
lab@kisa# show system software

Information for jbase:
Comment:
JUNOS Base OS Software Suite [5.0R3.3]

Information for jcrypto:
Comment:
JUNOS Crypto Software Suite [5.0R3.3]
Information for jdocs:
Comment:
JUNOS Online Documentation [5.0R3.3]
```

```
Information for jkernel:
Comment:
JUNOS Kernel Software Suite [5.0R3.3]

Information for jpfe:
Comment:
JUNOS Packet Forwarding Engine Support [5.0R3.3]

Information for jroute:
Comment:
JUNOS Routing Software Suite [5.0R3.3]

Information for junos:
Comment:
JUNOS Base OS boot [5.0R3.3]
```

2. 기본 접근 통제

가. 로컬에서의 사용자 접근 통제

(1) 콘솔 포트 패스워드 보안

초기 설정이 되어있지 않은 경우 "root" ID를 사용하여 콘솔 포트에 접속이 가능하다. 다음과 같이 CLI[11] 모드로 변경하여, 사용자 설정, 인터페이스 설정과 같은 라우터 초기 설정을 한다.

```
[edit system]
lab@kisa# set root-authentication plain-text-pasword
New passwd: 〈password〉
Retype new password: 〈retype password〉
```

11) CLI(Command Line Interface)

라우터의 기본적인 설정이 완료된 후에는 아래의 화면과 같이 set insecure 명령을 사용하여 "root" ID를 사용한 콘솔 포트로의 접속을 제한한다.

```
[edit system ports console]
lab@kisa# set insecure
```

(2) 관리용 포트의 사용

주니퍼 라우터는 별도의 관리용 포트를 제공하고 있다. 관리용 포트를 사용하기 위해서는 먼저 콘솔 포트로 접속하여 관리용 포트에 IP 주소를 할당해야 한다.

```
[edit interfaces fxp0]
lab@kisa# set interfaces fxp0 unit 0 family inet address [IP 주소]
```

나. 원격으로부터 접근 통제

(1) Firewall Filter를 사용한 접근 통제

Firewall Filter를 설정하기 위해서는 아래의 항목들을 순서대로 설정해야 한다.

- Firewall Filter 이름 설정
- Term 이름 설정
- Match 선언문 작성
- Action 선언문 작성
- 인터페이스에 Firewall Filter를 적용

① Firewall Filter 이름 설정

Firewall Filter의 이름을 설정하기 위해서는 set filter 명령어를 사용한다.

```
lab@kisa# set filter RE-SECURE
```

② Term 이름 설정

아래의 화면은 위에서 설정한 RE-SECURE라는 Firewall Filter에 BLOCK-MARTIANS라는 이름의 term을 설정하는 방법을 보여준다.

```
lab@kisa# set filter RE-SECURE term BLOCK-MARTIANS
```

③ Match 선언문 작성

Match 선언문이 패킷 필터링을 위하여 사용할 수 있는 요소들은 IP 주소, 포트 번호, 패킷 길이, 프로토콜 등 매우 다양하며 from "match 조건" 키워드를 사용하여 필터링 조건을 설정할 수 있다. 하나의 term에 여러 개의 match 선언문을 적용하여 다양한 조건으로 필터링할 수도 있다.

아래의 화면은 from source-address 명령어를 사용하여 패킷 필터링을 하기 위한 조건으로 출발지 주소를 선택한 예이다.

```
lab@kisa# set filter RE-SECURE term BLOCK-MARTIANS from source-address
```

④ Action 선언문 작성

패킷을 필터링할 match 조건문을 설정한 뒤에는 action 선언문을 사용하여, 이 조건을 만족하는 패킷을 어떻게 처리할 것인가를 설정해야 한다. 아래는 match 선언문에서 설정한 조건을 만족하는 패킷의 경우는 라우터에서 이를 받아들이도록 설정한 예이다.

```
lab@kisa# set then accept
```

⑤ 인터페이스에 Firewall Filter를 적용

Firewall Filter를 적용하기 위해서는 set unit "unit number" family inet filter

"input | output" "Firewall Filter name" 명령어를 해당 인터페이스에 적용하여야 한다. 다음 화면은 루프백 인터페이스에 RE-SECURE라는 이름의 Firewall Filter를 인터페이스의 입력 방향으로 적용한 예이다.

```
lab@kisa# set unit 0 family inet filter input RE-SECURE
```

(2) IP 주소 필터링을 통한 텔넷 연결 제한

라우터로 들어오는 패킷의 IP 주소를 필터링하여 허가된 IP를 가진 사용자에게만 연결 시도를 허용한다.

아래는 100.1.1.0/28, 200.0.0.0/28, 10.1.1.1/32의 네트워크 대역에 있는 사용자만이 라우터에 텔넷을 이용하여 접속할 수 있도록 설정한 예이다.

```
firewall {
    filter protect-RE {
        term telnet-permit {
            from {
                source-address {
                100.1.1.0/28;
                200.0.0.0/28;
                10.1.1.1/32;
            }
                protocol tcp;
                destination-port telnet;
            }
            then {
            count telnet-permitted;
accept;
        }
}
```

```
term telnet-deny {
            from {
protocol tcp;
                destination-port telnet;
            }
            then {
            count telnet-denied;
            log;
            discard;
           }
}
term default {
            then {
            count default-accept;
           }
}
    }
}
```

아래는 위에서 생성한 protect-RE Firewall filter를 루프백 인터페이스의 입력 트래픽에 설정한 예이다.

```
interfaces {
    lo0 {
        unit 0 {
            family inet {
                filter {
                input protect-RE;
            }
            address 10.1.1.1/32
           }
      }
     }
  }
```

(3) SSH를 사용한 안전한 접속

SSH를 설정하기 위해서는 set ssh connection-limit "SSH 세션 수" 명령을 사용하여 설정할 수 있으며 동시에 생성될 수 있는 최대 SSH 세션 수를 지정할 수 있다.

아래의 화면은 동시에 10개의 SSH 세션이 형성될 수 있도록 SSH를 설정한 예이다.

```
lab@kisa# set ssh connection-list 10
```

3. 안전한 사용자 관리 및 권한 부여

login Class를 생성하고 이 login class에 속하는 사용자 계정을 추가해야 한다.

- Login class 정의
- idle-timeout 설정
- 실행 권한 설정
- allow-commands/deny-commands 명령 적용
- 사용자 계정 생성
- 위에서 생성한 login class 선택하고 사용자 계정 생성
- 사용자 식별자 설정
- Local 인증 설정

가. 사용자 그룹 정의

주니퍼 라우터의 모든 사용자 계정은 login class에 소속되어 있어야 하며 하나의 login class는 여러 사용자 계정을 포함할 수 있다. 사용자가 새로운 login class를 생성하고자 할 때에는 set class "login class 이름" 명령어를 사용하여 login class를 생성할 수 있다.

아래는 bigdogs라는 이름의 login class를 생성한 예이다.

```
[edit system login]
lab@kisa# set class bigdogs
```

(1) idle-timeout 설정

Login class가 생성된 후에는 키보드로부터 입력이 없는 상황이 얼마나 지속되었을 때 접속을 자동으로 종료시킬 것인가를 의미하는 idle-timeout을 설정할 수 있다. idle-timeout을 설정하기 위해서는 set idle-timeout "설정하고자하는 idle time" 명령어를 사용할 수 있다.
아래의 그림은 bigdogs라는 이름의 login class에 idle-timeout을 30초로 설정한 예이다.

```
lab@kisa# edit class bigdogs
[edit system login class bigdogs]
lab@kisa# set idle-timeout 30
```

(2) 실행 권한 설정

Login class에 실행 권한을 설정하기 위해서는 set permissions "실행 권한" 명령어를 사용할 수 있다.
아래 그림은 bigdogs라는 이름의 login class의 실행 권한을 "all"로 설정한 예이다.

```
[edit system login class bigdogs]
lab@kisa# set permissions all
```

(3) allow-commands/deny-commands 명령 적용

set allow-commands 명령어와 set deny-commands 명령어를 사용하여 특정 명령어의 실행을 허용하거나 금지 설정할 수 있다.

아래의 화면은 bigdogs라는 이름의 login class에 clear, network, reset, trace, view의 실행 권한을 부여하고 halt, reboot 명령을 실행할 수 있도록 allow-commands 명령을 적용한 예를 보여주고 있다.

```
[edit system login class bigdogs]
lab@kisa# set permissions [clear network reset trace view]
[edit system login class bigdogs]
lab@kisa# set allow-commands "request system halt | request system reboot"
```

아래의 화면은 bigdogs2라는 이름의 login class에 all의 실행 권한을 부여하고 set, clear, delete로 시작되는 명령을 실행할 수 없도록 deny-commands 명령을 적용한 예를 보여주고 있다

```
[edit system login class bigdogs2]
lab@kisa# set permissions all
[edit system login class bigdogs2]
lab@kisa# set deny-commands "·set | ·delete | ·clear"
```

나. 사용자 계정 생성

Login class의 설정이 완료된 뒤에는 주니퍼 라우터에 접속하기 위한 사용자 계정을 생성하는 과정이 필요하다.

(1) Login class를 선택하고 사용자 계정 생성

사용자 계정을 생성하기 위한 첫 번째 과정은 사용자 계정이 소속될 login class를 선택하는 것이다. 아래의 화면은 set user "사용자 계정 이름" class "login class 이름" 명령을 사용하여 bigdogs라는 이름의 login class에 gsondere라는 사용자 계정을 추가한 예이다.

```
[edit system login]
lab@kisa# set user gsondere class bigdogs
```

(2) 사용자 식별자 설정

사용자 식별자(User Identifier)는 JUNOS의 몇몇 프로세스들을 이용하여 사용자 활동을 관리하기 위하여 사용자 계정에 부여한 숫자이다. 사용자 식별자는 set uid "사용자 식별자" 명령을 사용하여 1000에서 64000까지의 숫자 가운데서 지정될 수 있으며 아래의 화면은 "gsonder"라는 사용자 계정에 사용자 식별자를 설정한 예이다.

```
[edit system login]
lab@kisa# edit user gsondere
[edit system login user gsondere]
lab@kisa# set uid 1001
lab@kisa# show
uid 1001
class bigdogs
```

(3) 사용자 인증 설정

사용자 인증이 설정되어 있지 않으면 사용자는 패스워드를 입력하라는 프롬프트 없이 바로 라우터에 접속하게 된다. 사용자 인증을 설정하는 방법에는 radius, tacplus, local 패스워드 3가지가 있으며 관리자가 지정하는 순서에 따라서 3가지 방법을 차례대로 사용하여 인증을 시도하도록 설정할 수 있다.

- Radius - RADIUS 인증서비스를 통해서 이용자 인증
- Tacplus - TACACS+ 인증 서비스를 통해서 이용자 인증
- Local 패스워드

만약 관리자가 인증순서를 특별히 지정하지 않으면, 기본적으로 모든 사용자는 local 패스워드를 사용하여 인증을 하게 된다.

패스워드는 아래와 같이 set authentication plain-text-password 명령을 사용하여 설정할 수 있다.

```
[edit system login user gsondere]
lab@kisa# set authentication plain-text-password
New passwd: 〈password〉
Retype new password: 〈retype password〉
```

4. 안전한 라우팅과 주소 위조 방지

가. 안전한 라우팅

(1) RIP

RIP v1은 라우팅 프로토콜을 이용하여 정보를 주고받을 때 인증 기능을 제공하지 않지만 RIP v2는 인증 기능을 제공한다. RIP v2의 인증 기능 설정 과정은 아래와 같다.

- 인증 방법의 설정

  set authentication-type [simple|md5]

- 인증 패스워드의 설정

  set authentication-key [인증을 위한 패스워드]

아래의 화면은 RIP v2 라우팅 프로토콜의 인증 기능을 설정한 예로써 텍스트 형태의 패스워드를 "juniper01"로 설정한 예를 보여준다.

```
[edit protocols rip]
lab@kisa# set authentication-type simple
lab@kisa# set authentication-key juniper01
```

(2) OSPF

OSPF에 인증 기능을 설정하는 방법은 RIP v2의 것과 비슷하지만 인증 패스워드를 설정할 때 인

터페이스 단위로 이루어진다는 차이점이 있다.

- 인증 방법의 설정

  set authentication-type [simple|md5]

- 인증 패스워드의 설정
  - 인증 패스워드를 설정할 인터페이스를 선택
  - set authentication-key "인증을 위한 패스워드" key-id "키 ID" 명령어 사용
  - OSPF를 인증 기능을 설정하기 위해서는 먼저 인증 방법을 설정해야 함
  - 텍스트 형태의 패스워드를 사용하고자할 때에는 "simple"을 선택하고 MD5 알고리즘을 사용하고자할 때에는 패스워드를 설정할 때에는 "md5"를 선택
  - 인증 방법을 설정한 뒤에는 라우터의 각 인터페이스에 패스워드와 키 ID를 설정

아래의 화면은 OSPF 라우팅 프로토콜의 인증을 MD5 알고리즘을 사용하도록 설정하고 인터페이스 at-0/1/1.10에 패스워드가 "juniper02"이고 키 ID가 1인 인증 키를 설정한 예이다.

```
[edit protocols ospf area 0.0.0.0]
lab@kisa# set authentication-type md5
lab@kisa# edit interface at-0/1/1.10
[edit protocols ospf area 0.0.0.0 interface at-0/1/1.10]
lab@kisa# set authentication-key juniper02 key-id 1
```

(3) IS-IS

IS-IS를 사용하여 라우팅 정보를 전달하는 라우터에 인증 기능을 설정하는 데에는 Global 패킷을 이용하여 라우팅 정보를 전달하는 방법과 hello 패킷을 사용하여 라우팅 정보를 전달하는 방법이 있다. Global IS-IS 인증은 IS-IS 라우팅 프로토콜을 사용하는 인접한 라우터 모두에게 인증 기능을 설정하고자 할 때 사용되며, hello IS-IS 인증은 라우터 두 대 사이에서 인터페이스 레벨의 인증 기능을 설정할 때 사용된다.

Global IS-IS 인증을 설정하는 방법은 아래와 같다.

- 인증 방법의 설정

  set authentication-type [simple|md5] 명령어 사용

- 인증 패스워드의 설정

  set authentication-key [인증을 위한 패스워드] 명령어 사용

아래의 화면은 MD5 알고리즘을 사용하여 패스워드를 "juniper03"으로 설정하는 level 2 인증의 예를 보여주고 있다.

```
[edit protocols isis]
lab@kisa# set level 2 authentication-type md5
lab@kisa# set level 2 authentication-key juniper03
```

Hello IS-IS 인증을 설정하는 방법은 일반적으로 level 1 인증이라고 불리며 라우터 두 대 사이의 인증 기능을 설정한다. 아래의 화면은 MD5 알고리즘을 사용하여 패스워드를 "juniper04"으로 설정하는 level 1 인증의 예를 보여주고 있다.

```
[edit protocols isis]
lab@kisa# edit interface fe-0/0/0
[edit protocols isis interface fe-0/0/0]
lab@kisa# set hello-authentication-type md5
lab@kisa# set hello-authentication-key juniper04
```

(4) BGP

BGP 프로토콜은 별도의 인증 방법 설정이 필요 없이 set authentication-key "key" 명령을 사용하여 패스워드만 지정해주면 된다.

아래의 화면은 패스워드를 "juniper05"로 설정한 예를 보여주고 있다.

```
[edit protocols bgp]
lab@kisa# set authentication-key juniper05
```

나. 주소 위조 방지나. 주소 위조 방지

uRPF(Unicast Reverse Packet Forwarding)는 위조된 패킷을 라우터 단에서 방어하여 내부 네트워크로 유입되지 못하도록 한다. 주니퍼 라우터의 uRPF 설정은 active-paths와 feasible-paths라는 두 가지 방법을 제공한다. active-paths는 패킷의 소스 주소가 라우팅 테이블에 등록되어 있는 입력 인터페이스로 반드시 들어와야만 패킷을 받아들인다. Feasible-paths는 패킷이 최적의 경로로 통하여 라우터로 입력되지 않았더라도 패킷내부 네트워크로 유입되도록 설정한다.

(1) Active-paths로 들어오는 패킷 처리

아래의 그림은 active-paths를 사용한 uRPF로써 라우팅 테이블에 등록된 정보와 다른 인터페이스로 패킷이 들어 왔을 경우에 이 패킷을 차단함을 보여주고 있다.

```
routing-options {
    forwarding-table {
        unicast-reverse-path active-paths;
    }
}
interfaces {
    fe-0/1/0 {
        unit 0 {
            family inet {
                rpf-check fail-filter rpf-check;
                address 10.2.2.2/24;
            }
```

```
            family iso;
        }
    }
}
firewall {
    filter rpf-check {
        term 20 {
            then {
                count rpf-other;
                syslog;
                discard;
            }
        }
    }
}
```

- unicast-reverse-path active-paths

  uRPF를 사용함에 있어서 active-path를 설정하여 라우터의 라우팅 테이블에 등록된 최적의 경로로 라우터에 유입되는 패킷을 받아들이도록 설정 한다.

- rpf-check fail-filter rpf-check

  인터페이스에 uRPF 기능을 설정한다. fail-filter는 Filterwall Filter를 가리키며 uRPF에 의해서 차단되는 패킷을 어떻게 처리할 것인가를 Filterwall Filter를 이용하여 지정해준다.

- filterrpf-check

  rpf-check라는 이름의 필터를 설정하였으며 uRPF에 의해서 차단되는 패킷을 카운트하고 syslog 서버에 그 로그를 전송한다.

(2) Feasible-path로 들어오는 패킷 처리

같은 목적지 네트워크로 패킷을 전송할 때 최적의 경로를 사용할 수도 있지만 그렇지 않은 경우도 발생한다. feasible-paths로 설정이 되어 있다면 이러한 경우를 방지 할 수 있다.

5. 로깅

가. 라우터 로깅

아래는 라우터에서 발생하는 로그 관련 메시지를 저장하기 위한 설정이다.

```
system {
syslog {
file security-msg {
        firewall any;
        change-log any;
        interactive-commands any;
    }
  }
}
```

(1) 로그파일 포맷

위의 설정에 따라 저장되는 로그 파일의 포맷 형식은 아래와 같다.

```
[Format]
timestamp [router-name] software-process[process-ID]: message-code: message-text
```

```
[각 field가 의미하는 내용]

[예]
Jan  9 10:54:23 Central-GHM132 mgd[11894]:
UI_CMD라인_READ_LINE: User  'xxx' , command  'show'
```

- *timestamp : Jan 9 10:54:23*
- *[router-name] : Central-GHM132*
- *software-process[process-ID] : mgd[11894]:*
- *message-code : UI_CMDLINE_READ_LINE:*
- *message-text : User 'xxx' , command 'show'*

(2) system 로그 메시지의 분류

주니퍼 라우터가 만들어 내는 로그 메시지는 아래의 표와 같은 분류체계를 갖고 있다.

[표 7-2-1] 주니퍼 라우터가 만들어 내는 로그 메시지

로그메시지	내 용
Facility	에러나 이벤트의 유형
any	모든 상황에 대해서 로그 발생
Authorization	인증 및 인가와 관련된 시도가 있을때
change-log	JUNOS의 특성에 변화가 있을 때 발생
conflict-log	라우터와 하드웨어가 충돌이 발생하는 설정을 했을 경우 발생
cron	cron 데몬에 의해 정기적으로 발생
daemon	여러 가지 시스템 데몬에 의해 발생
firewall	Firewall filter에 의해 패킷필터링이 발생하는 경우 발생
interactive-commands	CLI위 연산모드에서 명령어를 실행할 경우 발생
kernel	JUNOS 커널에서 에러나 특정 작업이 수행될 경우 발생
Pfe	패킷 포워딩 엔진에서 에러나 특정 작업이 수행될 경우 발생
user	사용자 프로세스에서 에러나 특정 작업이 수행될 경우 발생

System 로그의 기본 설정은 다음과 같다. 아래의 설정은 files 옵션은 파일의 수를 5개까지 표시하고 syslog 데이터를 사용하고 있으며, sizes 옵션은 각각의 syslog 파일을 5MB의 최대 사이즈를 허용하는 예이다

```
[edit system syslog]
lab@kisa# set archive files 5 sizes 5m world-readable
[edit system syslog]
lab@kisa# show
archive sizes 5m files 5 world-readable;
```

Syslog파일의 최대 가능한 수는 1000개이다. 최소한의 사이즈는 64K이다. 각각의 syslog파일에 허용 가능한 최대사이즈는 1GB이며 syslog파일은 /var/log/디렉토리에 저장된다. CLI 명령을 사용하여 syslog 정보를 다른 파일에 저장하거나 콘솔 포트나 특정 호스트로 syslog 데이터를 리다이렉트 시킬 수 있다.

```
lab@kisa# show
archive size 5m files 5 world-readable;
host 124.35.35.14 {
    any emergency;
}
console {
    any critical;
}
```

Class 레벨과 severity 레벨을 변경하기 위해서는 키워드를 사용해야 한다. 사용 가능한 키워드는 아래의 리스트 목록과 같으며 이 목록은 메시지의 class의 선택사항을 보여준다.

```
[edit system syslog]
lab@kisa# set console ?
Possible completions:
  any                  Matches any facility
  authorization        The authorization system
  change-log           Configuration change log
```

cron	The cron daemon
daemon	Various system daemons
ftp	The file transfer protocol daemon
interactive-commans	Commands executed by the UI
kernel	Messages generated by the kernel
pfe	Messages generated by the packet forwarding engine
user	Messages from random user processes

로그 메시지는 라우터의 동작에 미치는 영향에 따라 emergency, alert, critical, error, warning, notice, info, debug의 분류체계를 갖는다. 이 분류는 라우터에 미치는 영향정도에 따라 분류되는 것이다.

그 분류체계와 특징은 아래와 같다.

```
[edit system syslog]
lab@kisa# set console ?
Possible completions:
```

any	Matches any facility
authorization	The authorization system
change-log	Configuration change log
cron	The cron daemon
daemon	Various system daemons
ftp	The file transfer protocol daemon
interactive-commans	Commands executed by the UI
kernel	Messages generated by the kernel
pfe	Messages generated by the packet forwarding engine
user	Messages from random user processes

```
[edit system syslog]
lab@kisa# set console any ?
Possible completions:
  alert                Conditions that should be corrected immediately
  any                  Matches any level
  critical             Critical conditions
  error                Error conditions
  info                 Information messages
  notice               Conditions that should be handled specially
  warning              Warning messages
```

(3) 거부된 트래픽의 로깅

다음은 활동 중인 모든 사용자에게 비상 정보를 전달하고 2대의 서로 다른 syslog 서버로 서로 다른 유형의 syslog 정보를 전송하기 위한 구성 사례이다.

```
syslog {
    user * {
        anyy emergency;
    }
    host 10.1.3.1 {
        authorization any;
        daemon info;
        kernel notice;
        interactive-commandsany;
    }
    host 10.1.3.2 {
        authorization any;
        daemon info;
        kernel notice;
        user notice;
        interactive-commandsany;
    }
}
```

(4) 인증 및 명령 이벤트의 로깅

모든 사용자 명령과 인증 및 권한의 부여, 거부를 기록하는 파일은 라우터상의 모든 관리 작업을 추적하기 위해 효과적인 방법이다.

(5) 라우팅 프로토콜 이벤트 및 오류

라우팅 프로토콜 이벤트와 오류는 라우팅 프로토콜에 대한 공격을 나타내는 훌륭한 지시요인이 될 수 있다.

(6) 카운트

Firewall filter에 설정한 조건을 만족하지 않는 패킷의 숫자를 파악할 때 사용할 수 있는 기능이다.

아래는 Firewall filter에 적용한 count 설정 예이다.

```
firewall {
    filter filter-name {
        term 10 {
            from {
                        condition  1;
}
            then {
                    count count-1;
                    log;
                    accept;
            }
        }
        term 20 {
            from {
                        condition 2;
```

```
        }
        then {
                count count-2;
              log;
                accept;
        }
    }
    term 30 {
        from {
                    condition  3;
        }
        then {
                count count-3;
                    log;
                accept;
        }
    }
}
```

```
root@host〉 show firewall
Filter: filter-name
Counters:
Name                Bytes           Packets
Count-1              4837758            87394
Count-2              3261909112          41994056
Count-3              5380384           111640
```

나. 샘플링 로그

샘플링은 네트워크를 통과하는 패킷을 일정 간격으로 캡처하여 전체 네트워크의 데이터 유형을 파악하는데 사용하는 유용한 방법이다. 아래의 설정은 1000개마다 3개의 패킷을 샘플링하는 설정을 하는 예이다.

```
lab@kisa> file show /var/tmp/test-sample
# Feb 17 10:08:04
#  Time  Dest  Src   Dest   Src  Proto  TOS   Pkt  Intf    IP   TCP
#  addr   addr  port  port    len   num  frag flags
# Feb 17 10:08:04   218.145.171.127   218.145.171.88   137137    17   0x0    78    69   0x0   0x0
# Feb 17 10:08:04   218.145.171.127   218.145.171.43   137   137    17   0x0    96    69   0x0   0x0
# Feb 17 10:08:04   218.145.171.33    192.168.2.1     1920  1900    17   0x0   314    69   0x0   0x0
# Feb 17 10:08:05   218.145.171.127   218.145.171.43   137   137    17   0x0    96    69   0x0   0x0
# Feb 17 10:08:06   218.145.171.127   218.145.171.43   137   137    17   0x0    96    69   0x0   0x0
# Feb 17 10:08:08   218.145.171.43    192.168.2.1     1067  1900    17   0x0   314    69   0x0   0x0
# Feb 17 10:08:08   218.145.171.127   218.145.171.43   137   137    17   0x0    96    69   0x0   0x0
```

위와 같이 설정하면 샘플링된 데이터는 test-sample라는 이름으로 저장된다.

다음은 샘플링한 데이터의 내용을 보여주는 예이다.

```
forwarding-options {
    sampling {
        input {
            family inet {
                rate 1000;
                run-length 2;
                max-packets-per-second3000;
            }
        }
        output {
            cflowd 10.1.1.1 {
                aggregation {
                    autonomous-system;
                    destination-prifix;
                    protocol-port;
                    source-destination-prefix {
                        caida-compliant;
```

```
    }
    source-prefix;
                }
                port 2056;
                version 5;
            }
            file {
    filename test-sample;
    files 5;
    size 256k;
    world-readable;
    stamp;
            }
        }
    }
}
```

샘플링에 의하여 수집된 Flow data는 네트워크의 이상징후를 발견하기 위하여 분석할 때 참조되는 가장 유용한 정보 중 하나로 지속적인 정보 수집과 이전 데이터의 저장이 매우 중요하다.

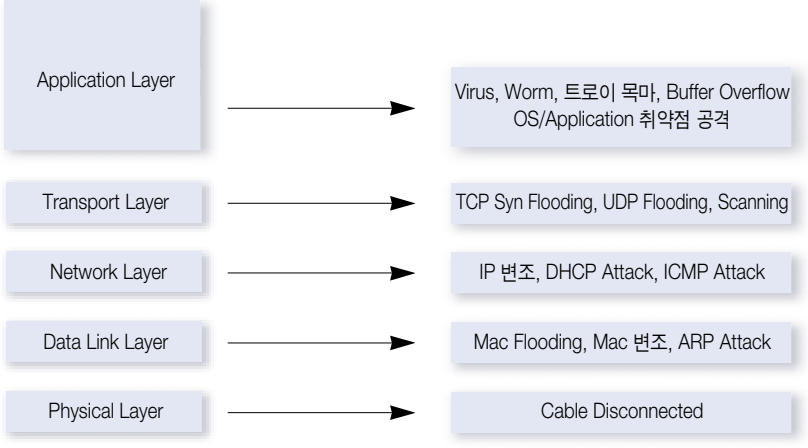
주니퍼 라우터의 경우 적절한 sample rate을 지정하면 서비스에 영향을 주지 않으면서도 지속적인 샘플링이 가능하고 결과를 분석하기 위한 출력 옵션이 다양하므로 flow data 수집에 유용하다. 특히 모니터링 PIC 을 이용하면 ASIC에 기반한 샘플링을 수행하므로, CPU에 전혀 부하를 주지 않으면서도 더욱 효과적인 샘플링이 가능하다.

제3절 스위치 보안 관리

스위치 기반의 보안은 라우터의 보안과는 달리 직접 사용자가 접속된다는 구성상에 커다란 차이점이 있다.

이러한 구성상의 차이는 OSI 7 계층의 모든 공격이 통과하거나 목표가 되기도 하다. 따라서 스위치에서 제공되는 기본적인 보안 기능을 설정하여 내부 사용자의 공격이나 피해를 최소화하는 것이 중요하다.

1. Layer 별로 본 스위치 기반의 공격 유형



Layer 별 Attack 유형
(그림 7-3-1)

가. 물리적(Physical) 계층 공격 유형

먼저 Physical 계층에서의 공격은 대표적인 것이 악의적 의도로 Cable을 강제로 단절시키는 경우를 생각해 볼 수 있다. 사전에 대처하기 위한 방법들이 여러가지가 있겠지만, 이런 예기치 못한 경우를 대비해서 대응 시나리오를 준비해 두는 것이 가장 좋은 방법이라 할 수 있다.

나. 데이터 링크(Data Link) 계층 공격 유형

Data Link 계층에서는 MAC 주소의 변조나 MAC Flooding 공격 등이 있다. 스위치 장비에서의 MAC 주소에 대한 처리 부담을 주게 되어 스위치 장비의 CPU를 고갈 시키거나, ARP 공격을 통한 Traffic 흐름 변화, MAC 변조를 통한 지능화된 공격 등이 그 대표적 예이다.

다. 네트워크(Network) 계층 공격 유형

네트워크 계층에서는 대표적인 공격이 IP 주소 변조와 DHCP 공격 등이 있다.

데이터 링크 계층에서의 MAC 변조가 주민등록번호 변조라고 가정한다면, Network 계층에서의 IP 변조는 주소지 변조라고 생각해 볼 수 있다. 대부분의 네트워크 공격이 IP 변조가 그 출발점이 된다는 데서 많은 관심을 가질 필요가 있다.

라. 전송(Transport) 계층 공격 유형

전송 계층에서는 대표적인 공격이 TCP, UDP Flooding 공격이다.

특정 공격 목표를 향해 UDP 트래픽 폭탄 공격을 한다거나, 출발지 IP 주소를 변조한 상태에서 TCP 3-handshaking 을 반복적으로 수행시키는 방법이다.

마이둠이나 슬래머 웜 같은 공격 형태들이 이러한 대표적인 예이며, 네트워크 장비와 서버 등에는 치명적인 부하를 주는 무서운 공격들이다.

마. 응용(Application) 계층 공격 유형

Application Layer에서는 OS나 Application 취약점을 이용한 공격이나, 수많은 웜과 바이러스들을 생각 해 볼 수 있다.

2. 스위치 기반의 물리적 계층(Physical Layer) 공격과 대처 방법

Cabling 단선이나 접속 불량 등의 물리적인 문제에 있어서 가장 효과적으로 진단하는 방법 중 하나는 길이의 측정이다.

네트워크 장비에는 장비에 접속된 UTP Cable을 통해 펄스 신호를 보내도록 설계되어 있다. 따라서 네트워크 장비에서 특정 명령어로 펄스 신호를 보내게 되면, 단선이나 접촉 불량을 만나게 되면 그 펄스 신호는 되돌아오게 된다.

이 때 최초로 펄스를 보낸 시간과 되돌아온 시간차를 계산해서 문제가 발생한 거리를 측정 Print 해주게 된다.

```
Console〉(enable) test cable-diagnostics tdr 3/7 〈 펄스 신호 발생 〉
TDR test started on port 3/7. Use show port tdr 〈m/p〉 to see the results
Console〉(enable) show port tdr 3/7 〈 TDR 결과물 Print 〉
TDR test last run on Mon, June 3 2003 at 4:21:00 pm
Port  Speed  Local pair  Pair length        Remote pair  Pair status
----- ------ ---------- ------------------ ------------ ------------
3/7   1000  Pair A     12 +/- 3 meters     Pair A       Terminated
            Pair B     12 +/- 3 meters     Pair B       Terminated
            Pair C     12 +/- 3 meters     Pair C       Terminated
```

좀 더 세부적으로 설명하면 이러한 값들은 Cable 제조사 별로 조금씩 차이가 있게 마련이고, 약간의 오차범위를 가진다.

이러한 네트워크 장비에서의 TDR 기능은 예측하지 못한 Cable 단절 상황에 관리자들에 신속한 대응력을 가지게 해 준다.

3. 스위치 기반의 데이터 링크(Data Link) 계층 공격과 대처 방법

가. MAC Address 변조

모든 물리적인 장비에는 이른바 일련 번호가 내장이 되어 있으며, 이러한 일련번호를 통해서 장비 제조사와 Interface Address를 구분할 수가 있다.

Windows 2000/XP 등은 이러한 고유의 MAC address를 손쉽게 변경할 수 있도록 되어 있다.

MAC Address 변조의 예
(그림 7-3-2)

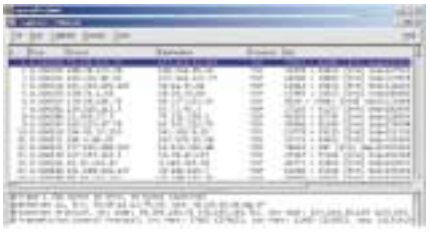
변조를 방지하기 위한 방법 중 하나는 호스트와 직접 연결이 되는 스위치 장비에서 미리 MAC Address를 Switch의 물리적인 Port 와 매핑 시켜 놓은 방법을 생각해 볼 수 있다.

나. MAC Address 폭탄 공격

MAC Flooding은 MAC Address 자동 생성 Tool을 통해서 MAC Address를 스위치에 쏟아 붓는 방식으로, 공격 목표가 되는 스위치는 처리할 수 있는 최대한의 용량을 초과하게 되면서 Down

되거나 오동작을 일으키게 된다.

실제 Packet Decoding Tool을 통해서 보면 마치 TCP Syn Flooding 공격처럼 보이기도 한다.



MAC Flooding 발생 후 Packet Decoding 분석
(그림 7-3-3)

이러한 MAC Flooding은 근래 사고가 급증하고 있으며, 방어 방법으로는 해당 Access Switch에서 최대 수용할 수 있는 MAC Address 숫자를 제한시켜 놓는 것이 효과적인 방법이다.

```
Switch(config)# interface fastethernet 5
Switch(config-if)# switchport port-security maximum 5
    ➪ 최대 허용 MAC address 숫자를 5개로 제한 시켜 놓는다.
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
    ➪ FasteEthernet 5번 Port에 접속될 MAC address 를 미리 정의해 놓는다.
Switch(config-if)# switchport  port-security violation [protect/restrict/shutdown]
    ➪ 해당 포트의 규칙에 위배될 경우에 제한 규칙 설정.
Switch(config)# mac-address-table static 0050.3e8d.4444 vlan(해당vlan) drop
    ➪ 유해 트래픽을 발생시키는 MAC address Filtering
```

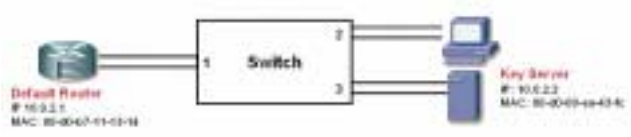
다. ARP 공격

ARP 관련 공격기술은 동일한 Subnet/ VLAN에 속한 공격자가 , 정상적인 사용자가 원하는 목적지의 MAC 주소를 요청하는 ARP Request Packet을 중간에 가로채서 Traffic의 흐름을 강제로 바꾸어 놓는 다든지, 정상적인 사용자의 MAC Address로 변조하여 일련의 부정행위를 하는 것 등이 있다.

특히 일부 ARP 변조 공격 도구들은 패스워드 사전과 연동되어 패스워드까지 Crack 시키는 기능까지 수행하기도 하므로, 이에 대한 대책들을 수립하는 것이 좋다.

스위치 장비에서 이러한 ARP 공격을 방어하는 대표적인 예가 ARP 인스펙션(Inspection) 기능이다.

ARP Inspection
(그림 7-3-4)



SW〉 (enable) set security acl ip A1 permit arp-inspection host 10.0.2.1 00-d0-b7-11-13-14

SW〉 (enable) set security acl ip A1 permit arp-inspection host 10.0.2.2 00-d0-00-ea-43-fc

⇨ ARP Table을 사전에 등록을 해 둔다.

SW〉 (enable) set security acl ip A1 permit arp-inspection any any

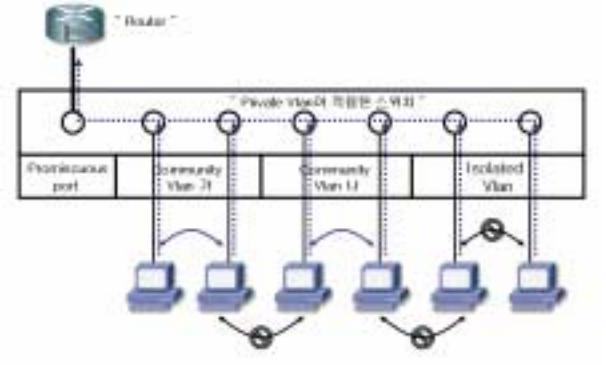
SW〉 (enable) set security acl ip A1 permit ip any any

SW〉 (enable) commit security acl A1

ARP 인스펙션 기능은 주요 Server와 Host들의 IP와 MAC Table 을 Mapping 시켜 놓음으로써 Traffic의 흐름이 강제로 변경되거나, Server의 MAC Address로 변조되는 것을 방지하도록 구성하는 방법이다.

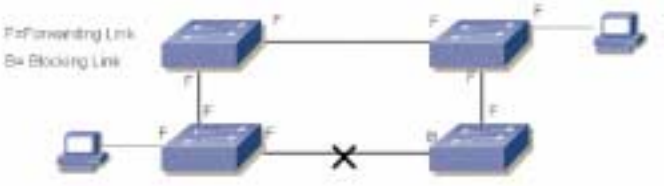
라. 스위치 기반의 사설 Vlan 기능

Private Vlan 개요
(그림 7-3-5)



데이터 링크 계층의 데이터를 안전하게 보호하는 방법 중 또 다른 하나는, Private VLAN을 사용하는 방법이 있다. 마치 사설 IP address를 사용하듯이, 공인 Vlan 내부에 사설 Vlan을 할당하여 동일한 공인 Vlan 내부에서도 정보의 보안을 꾀하는 방식이다. 동일 Community Vlan 내에서의 Host는 서로의 정보를 공유할 수 있지만, 서로 다른 Community Vlan 에 속한 Host는 Promiscuous Port를 통해서만 통신이 가능하다. 또한 Isolated Vlan에 속한 Host는 동일한 Vlan 이라 할지라도 상호 보안을 유지 할 수 있도록 구성할 수도 있다.

마. 스패닝 트리(Spanning Tree) 공격



스위치 간 Spanning Tree
(그림 7-3-6)

(그림 7-3-6)에서 보는 것처럼 오른쪽의 호스트가 왼쪽의 호스트로 데이터를 보내기 위해서는 다양한 경로가 생성될 수 있다. 스위치 4대가 다중 링크를 확보함에 따라 루핑 구조 형태를 갖게 된다. 이러한 Looping을 방지하기 위해 스위치는 일련의 순서에 따라 RootSwitch를 설정하고, 해당 RootSwitch 방향으로는 Forwarding Link를 설정하고 다른 한쪽의 링크로는 Blocking Link를 설정하여 루프를 방지하도록 구성한다. 이러한 일련의 절차를 진행하기 위해 스위치는 상호 BPDU(Bridge Port Data Unit)을 주고 받게 된다.

문제는 공격자 PC가 이러한 BPDU 메시지를 스위치에 보내게 될 경우, RootSwitch가 변경이 되면서 스위치 구성에 오동작이 발생할 수 있다. 따라서 Switch Uplink를 제외하고는 BPDU Message를 주고 받지 않도록 설정하거나, RootSwitch에서 Designate port를 설정하는 것이 중요하다.

```
IOS(config)# spanning-tree portfast bpduguard
 →BPDU Guard 기능 설정을 통한 STP Attack 방어
Switch(config)# spanning-tree guard root (or rootguard)
 →Root Switch 에서 Root Guard 설정을 통한 STP Attack 방어
```

바. 스위치 기반의 Vlan 호핑(Hopping) 공격

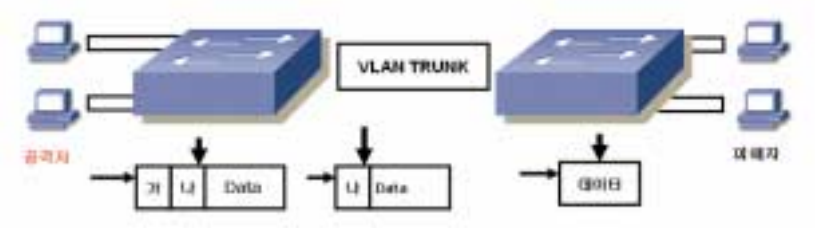
Vlan Hopping Attack은 VLAN 구성의 취약점을 이용한 공격이라 할 수 있다.

일반적인 Vlan 트렁크(Trunk) 구성
(그림 7-3-7)

(그림 7-3-7)에서 일반적인 Vlan 트렁크(Trunk) 구성 에서 "가" vlan 그룹과 "나" vlan 그룹에 속한 호스트들은 양쪽 어느 스위치에서나 동작할 수 있도록 구성이 되어 있으며, 이러한 이동성과 편리성을 겸비한 구성을 위해 양단의 스위치 간에는 Vlan 트렁크를 통해서 "가", "나" Vlan의 정보를 공유 할 수가 있다.

Vlan 트렁크 공격은 이러한 Vlan 트렁크의 구성의 취약점을 이용한 공격이다.

Vlan 호핑 공격
(그림 7-3-8)



(그림7-3-8)에서처럼 레드 Vlan 에 속한 공격자는 공격 목표에 Data를 전송할 때 Vlan 태그(Tag)를 두개를 붙여서 보내게 되고, 공격자가 속한 스위치를 통과하면서 "가" Vlan에서 "나" Vlan으로 변경하게 된다. 따라서 "가" Vlan에 속한 피해 시스템은 마치 "가" vlan에서 패킷이 온 것으로 판단하고 공격자에게 노출된다.

이러한 공격은 스위치 구성시 기본적으로 스위치 포트의 모드가 자동으로 할당되어 있는 구성상 취약점을 노린 공격이다. 따라서 트렁크를 사용하지 않는 물리적인 포트들은 모두 트렁크를 강제로 오프 시켜 놓는 것이 좋다.

```
IOS(config-if)# switchport mode access
  ⇦ 스위치 포트의 트렁크(Trunk) 모드를 오프 시켜 둔다.
```

사. 그 밖의 스위치 기반의 데이터 링크 공격 예방을 위한 구성

① Switch 자체 보안을 위해 관리방법을 SSH 기반으로 사용한다.
② Vlan 1 설정을 되도록이면 사용하지 않는다.
③ SNMP version 3 사용을 통해 SNMP의 보안을 향상 한다.
④ 사용하지 않는 Port들에 불필요하게 Vlan 설정을 하지 않는다.

4. 스위치 기반의 네트워크 계층(Network Layer) 공격과 대처 방법

가. IP 변조 방지

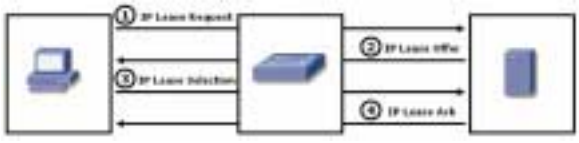
IP 주소 변조는 모든 네트워크 공격의 가장 기본이 되는 공격의 출발점 중 하나이다. 그 변조 방법도 다양해서 TCP 순차 번호 추측 공격, 소스 라우팅 변조를 통한 IP 주소 변조 등 다양한 방법이 있다.

IP 주소 변조를 스위치 기반에서 방어하는 방법은 ACL(Access-Control List)을 통한 구성과 uRPF(Unicast Reverse Path Forwarding) 방법 등이 있다.

```
Switch6500(config)#inter vlan 1
  ⇦ 적용하고자 하는 해당 Vlan
Switch6500(config-if)#ip verify unicast reverse-path
  ⇦ 해당 Interface의 IP 변조방지 기능 적용
```

나. DHCP 공격 방어

DHCP 동작방식
(그림 7-3-9)



DHCP 동작 방식은 (그림-7-3-9)와 같이 크게 4가지의 주요한 흐름을 가지고 있다.

먼저 DHCP 요청 클라이언트는 DHCP Discover 메시지를 브로드캐스트 형식으로 전송한다.

DHCP Discover 메시지를 받은 DHCP 서버는 Disover Offer 메시지를 답하게 된다. 이때 Discover Offer 메시지 안에는 클라이언트 MAC 주소, 할당될 IP 주소, 서브넷, 대여기간, 서버 식별자 IP 등을 포함하고 있다. DHCP Server로부터 메시지를 받은 Client는 IP lease selection 메시지를 서버에게 Broadcast로 전송한다. 이 때 Client들이 브로드캐스트 방식으로 메시지를 전송하는 이유는 DHCP가 다중으로 구성되어 있을 수도 있기 때문이다. 마지막으로 IP Lease selection 메시지를 받은 서버는 DHCP ACK 메시지를 전송함으로써 DHCP 의 IP 부여 과정을 마치게 된다.

이 때 주목할 점은 이러한 동작 방식들이 동일한 Subnet에 존재하는 공격자가 얼마든지 이러한 메시지를 가로채서 오동작을 발생시킬 수 있다는 데 있다.

DHCP 환경에서의 IP, MAC 변조를 스위치 장비에서 방어할 수가 있다. 스위치 장비에서 DHCP Snooping 기능을 적용하게 되면, 네트워크 장비를 통과하는 DHCP 에 대한 정보를 저장하고 있다가 이미 할당된 MAC Address와 IP를 불법적으로 도용하여 네트워크 장비를 통과하는 패킷을 폐기시키도록 할 수 있다.

```
Switch(config)# ip dhcp snooping    DHCP Snooping enable
Switch(config)# ip dhcp snooping vlan 10   DHCP Snooping 적용 Vlan 정의
```

```
## DHCP Trust 기능
Switch(config-if)# ip dhcp snooping trust  DHCP Server 인가 포트 지정

## DHCP Rate Limit 기능
Switch(config-if)# ip dhcp snooping limit rate 100 DHCP Request 허용 수치 제한

## DAI(Dynamic ARP Inspection 기능
Switch(config)# ip arp inspection vlan 1
Switch(config-if)# ip arp inspection trust

## IP source guard 기능
Switch(config-if)# ip verify source vlan dhcp-snooping port-security
Switch(config)# ip source binding ip-addr  vlan number interface interface
```

5. 스위치 기반의 전송 계층(Transport Layer) 공격과 대처 방법

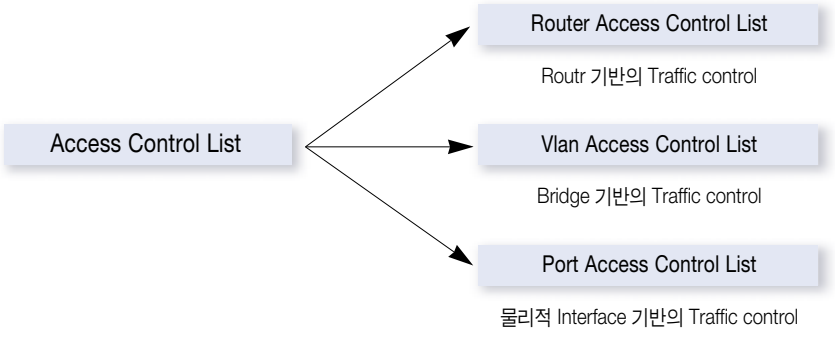
전송 계층에서의 공격 형태 중 가장 대표적인 공격 유형이 특정 포트를 통한 웜이 유입 되거나, TCP syn flooding, UDP Flooding 공격등을 꼽을 수가 있다.
이러한 전송 계층에서의 네트워크 장비에서 방어 요령을 크게 두가지 방법으로 축약 될 수 있다. 먼저 대표적인 네트워크 장비의 Packet Filtering 방식인 Access-list가 있고, QoS를 통한 제어 방법이 있다.

보안장비에 많은 비용을 투자를 해도 웜과의 전쟁에서 효과적으로 방어하지 못하는 이유 중 하나는 보안장비들이 대부분 인터넷 라우터와 백본 스위치에 집중 되기 때문이다.

일단 웜이 보안장비를 통과해서 들어오게 되면 내부의 고속 인프라를 타고 급속도로 전이되고 이에 대한 효과적인 방어력을 설정할 수 없다는 것은 관리자로써는 커다란 고민이 아닐 수 없다.

가. ACL (Access-Control List) 구성
스위치 장비에서는 이러한 취약점 포트나, 웜이 전이되는 포트를 효과적으로 방어하기 위해서 다양한 Access-list 기법을 제공하고 있다.

ACL 종류
(그림 7-3-10)



먼저 관리자들이 사용하는 대부분의 ACL은 라우터 기반의 트래픽 제어이다. 이것은 동일 Subnet 이나 Vlan에서의 웜 전이나Traffic 제어를 할 수 없다. 하지만 Vlan기반 접근제어리스트를 적용하게 되면 동일한 브로드캐스트 영역에서의 Traffic을 제어할 수 있으므로, 웜이 전이되는 취약점 포트에 대한 제어를 통해, 그 전이 속도를 현저히 떨어뜨릴 수 있는 강력한 ACL 기능이다.

물론 물리적인 포트 기반의 접근제어리스트를 활용한 트래픽 제어를 할 수 있지만, 보통 Access-switch가 24 Port 이상으로 구성되어 있는 상황에서 ACL을 물리적 포트별로 제어한다는 것은 관리상 무리가 따를 수 있다.

```
Nachi 웜 내부망 전파를 제어하기 위한 Vlan ACL 구성 예제
## Access-list 규칙 작성
Switch(config)#ip access-list extended worm_block
Switch(config)# deny tcp any any 135
Switch(config)# deny tcp any any 139
Switch(config)# deny tcp any any 445
Switch(config)# deny tcp any any 4444
Switch(config)# deny tcp any any 707
Switch(config)# deny udp any any 69
Switch(config)# deny icmp any any echo
Switch(config)# deny icmp any any echo-reply
Switch(config)# permit ip any any
## Vlan ACL 규칙 작성
Switch(config) #vlan access-map worm_vacl 10
```

```
Switch(config)#match ip address worm_block
Switch(config)#action forward
## 해당 VLAN 에 적용
Switch(config)#vlan filter worm_vacl vlan-list 100 -150
```

나. QoS를 통한 유해 트래픽 제어

QoS를 통한 물리적, 논리적 인터페이스에 Policing QoS를 미리 설정해 두는 방식은 유해 트래픽이나 분산 서비스 거부 공격에 효과적으로 대응할 수 있는 방법 중 하나이다.

이 경우 TCP, UDP Flooding 뿐만 아니라, P2P 등 Traffic에 위협을 주는 요소에 시간대별 QoS 제어 등 유연한 보안 구성이 가능하므로 기업, 대학 등에서 많이 적용되고 있는 사례이다.

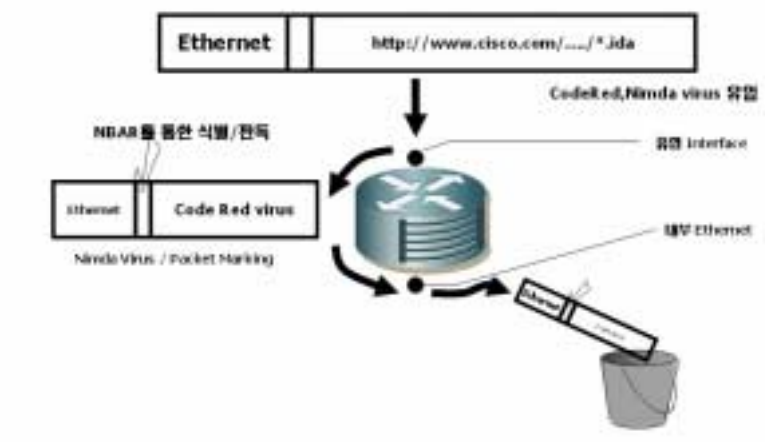
```
## TCP Syn Flooding Packet 관련 Access-list 작성
Switch(config)# access-list 100 permit TCP any any syn

## Class-Map 작성
Switch(config)# class-map tcp-syn-class
Switch(config-cmap)# match access-group 100

##Policy-Map 작성
Switch(config)# policy-map tcp-syn-policing
Switch(config-pmap)# class tcp-syn-class
Switch(config-pmap-c)# police 80000 conform transmit exceed drop

##Interface 기반의 Policing
Switch(config)#interface gigaethernet 1/1
Switch(config-if)# service-policy output tcp-syn-policing

##Control Plane 기반의 Policing
Router(config)# control-plane
Router(config-cp)# service-policy output tcp-syn-policing
```

6. 스위치 기반의 응용 계층(Application Layer) 공격과 대처 방법

NBAR(Network Based Application Recognition)는 스위치 장비에서의 응용계층에 대한 탐지 기능을 보유하고 있는 기술 중 하나이다.

네트워크 장비의 핵심기능은 Packet을 얼마만큼 고속으로 전송하는가에 있다. 따라서 NBAR와 같은 Layer 7 까지 탐지해서, 유해 트래픽을 탐지하고 패킷을 폐기시키는 기능은 결국 네트워크 자원 자체에 어느 정도의 부하를 끼칠 가능성이 있다. 따라서 관리자는 NBAR를 적용하기에 앞서 해당 장비의 CPU 점유상태를 점검하고 적용하는 것을 권고 한다.

NBAR를 이용한 Virus 탐지 및 폐기
(그림 7-3-11)



NBAR의 동작 방식은 먼저 패킷이 유입되는 해당 인터페이스에서 프로토콜별 패턴과 문자열을 검색을 먼저 수행한다. 이 때 미리 정의해둔 패턴이나 문자열과 동일한 Packet이 발견되면 Packet의 DSCP 값에 Marking을 해두고, DSCP에 Marking 된 Packet은 목적지로 나가게 되는 Interface에서 미리 정의된 규칙에 따라 폐기되거나 통과하는 방식이다. 즉 NBAR는 순수하게 감지만 하고, Marking과 패킷 폐기는 QoS와 ACL이 그 기능을 담당하게 된다.

```
##Class-map 정의
class-map match-any http-hacks
  match protocol http url "*default.ida*"
  match protocol http url "*x.ida*"
  match protocol http url "*.ida*"
  match protocol http url "*cmd.exe*"
  match protocol http url "*root.exe*"
  match protocol http url "*readme.eml*"

##Policy map 정의 및 DSCP 값 Setting
policy-map mark-inbound-http-hacks
  class http-hacks
    set ip dscp 1

## Interface 에 해당 Packet이 통과하면 DSCP Marking
Interface serial 1/0
 service-policy input mark-inbound-http-hacks
```

➪ 위에서 Class map에서 정의된 내용이 들어오면 dscp값을 1로 정의 해 둔다.

```
## Access-list 정의 및 filtering
Access-list 105 deny ip any any dscp 1
Access-list 105 permit ip any any
Interface ethernet 2/0
```

➪ ip access-group 105 out 인터넷 구간을 통해 들어온 패킷 중 dscp값이 1로 정의 된 것 filtering

제4절 기업 환경의 무선랜 구축 운영

1. 무선랜 보안 위협

기업 네트워크의 생산성 향상을 위해 IT 인프라의 이동성과 편리성을 고려한 설계가 요구되어지고, 이러한 요구에 대한 적절한 인프라로 무선랜이 기업 네트워크에 고려되고 있다.

저렴한 비용 투자를 통한 장비 구매, 편리한 설치와 운영 등의 장점들은 기업들에게 생산 하지만 이러한 무선랜의 데이터 전송 방식이 실제 데이터를 허공에 전송한다는 점과, 사용자의 편의를 위해 모든 보안 기능을 사용하지 않도록 설정되기 때문에 보안의 취약 요소들의 가지고 있다.

무선랜에 부가적으로 설치가 가능한 안테나를 사용하는 경우, 무선랜은 기업이 의도한 범위를 벗어난 먼 곳 까지 도달이 가능하다. 이런 상황에서 권한 없는 공격자에 의해 기업의 데이터를 언제든지 훔쳐 볼 수 있다는 시나리오를 고려해야만 한다. 또 하나의 불행한 시나리오는 마치 유선 네트워크의 DoS 공격에서처럼, AP[12]에 대한 접근 요청을 과다하게 수행하게 되면, AP가 사용할 수 있는 최대한의 주파수 대역이 고갈 되어 네트워크를 다운 시키게 되는 시나리오가 발생 할 수도 있다.

2. 기업을 위한 무선랜 보안 기술

IEEE 802.11/11i에서 표준이 진행되고 있는 WLAN[13]은 취약한 암호화, 안전한 로밍 기술의 부재, 무선 네트워크 인식 문제, Rogue 액세스 포인트 등의 취약점이 존재한다. 이에 대해서, 사용자 인증, AP인증, Fast Hand-off의 요구사항이 도출되고, 802.11i 키 관리, 유무선 통합 인증 프레임워크, AES-CCM 암호화 기술 등이 정보보호 요소기술로 개발되었다.

12) AP(Access Point)
13) WLAN(Wireless LAN)

[표 7-4-1] WLAN 취약성, 보안 요구사항, 보안 요소기술

취약성 및 역기능	보안 요구사항	보안 요소기술
무선 네트워크 인식 문제	디바이스 인증	DIAMETER 802.11i Key Management 유무선 통합 인증 프레임워크 802.1h(DFS, TPC) 불법 AP 관리(감시, 차단, 보고) SNMPv3 Mobile IP over IPv6 AES-CCM 암호화 기술
취약한 인증 시스템	사용자 인증	
취약한 암호화	강력한 암호화 알고리즘	
안전한 로밍기술의 부재	빠른 재인증 기술 (Pre-authentication, Local Authentication, Fast Hand-off)	
하드웨어 장비의 분실	디바이스 인증	
Rogue 액세스포인트	AP 인증	
DoS 공격	802.1h	

가. 기업 환경의 무선랜 취약성과 역기능

(1) SSID 방식의 취약성

SSID (Service Set Identifier)는 설치된 각 무선랜의 네트워크 이름으로 사용자가 무선 네트워크의 존재 유무를 확인하고, 접속하기 위해 사용한다. 이때 사용자의 무선접속 편의를 위해 액세스 포인트에서 이 SSID를 대기 중에 브로드캐스팅하게 되는데, 이때 허가받지 않은 사용자에게까지 SSID를 통해 액세스 포인트의 위치가 알려지게 된다. 액세스 포인트가 설치되어 있다는 것이 일단 알려지고 나면 손쉬운 공격목표가 될 수 있으므로 이러한 SSID 브로드캐스팅은 금지하도록 설정하는 것을 권장 한다

무선랜 AP 에서의 SSID 브로드캐스팅 금지 설정
(그림 7-4-1)

(2) 기업 환경의 취약한 인증 시스템

① 무인증 시스템

무선랜의 접속을 위해서 IEEE 802.11 표준에서는 2가지의 인증방식을 제안하고 있다. OPEN과 SHARED 방식으로 구분되는 이 2가지 인증 메커니즘은 실제로 어떠한 인증을 수행한다기보다는 접속절차의 하나로써의 의미로, 보안을 위해 인증과는 관계가 없다.

OPEN 인증의 경우, 클라이언트의 인증요청 시, 요청의 내용에 관계없이 인증 성공 메시지와 함께 접속절차를 시작한다. SHARED 인증에서는 WEP 키를 사용해서 장치 인증을 시도한다. 그 방법은 AP에서 클라이언트에게 암호화되지 않은 텍스트를 보낸 후, 클라이언트에서 암호화키를 가지고 암호화하여 데이터를 되돌리는 방식이다. 그런데, 이 방식의 경우, man-in-middle attack등 수많은 공격이 발생할 수 있다.

② WEP (Wired Equivalent Privacy)

IEEE 802.11b 표준은 WEP라 불리는 부가적인 암호적 기능을 규정하고 있다. WEP은 무선랜의 데이터 스트림을 보호하는 메커니즘을 제공한다. 그리고 대칭 암호화 알고리즘을 사용하기 때문에 자료의 암호화와 복호화를 처리할 때 동일한 키와 알고리즘을 사용한다. WEP의 주요 목적은 접근제어(Access Control)와 프라이버시(Privacy)기능을 제공하는 것이다.

WEP에서의 접근 제어는 올바른 WEP 키를 보유하고 있지 않는 사용자들이 네트워크에 접근하지 못하게 사용되며, 프라이버시는 올바른 WEP 키를 가지고 있는 사용자들에 의해서만 무선랜 구간에서 사용하는 자료들을 암호화 하거나 복호화 시킬 수 있도록 하는 것이다.

IEEE 802.11 표준은 무선랜에 사용되는 WEP 키를 정의함에 있어서 두 가지 방식을 사용한다. 첫 번째는 4개의 디폴트 키를 정의하여 모든 장비들 (AP, Clients)과 공유하는 체계이다. 즉 클라이언트가 디폴트 키를 획득하였을 때는 서브 시스템에 있는 모든 다른 시스템들과 안전하게 자료들을 통신할 수 있다. 이러한 디폴트 키의 사용에 대한 문제점은 많은 시스템들이 넓게 분포되어 있을 때 디폴트 키들을 악의적으로 사용하고자 하는 시스템과 타협될 수 있다는 것

이다.

두 번째 방식은 각각의 클라이언트들이 다른 시스템들과 상호관계의 키 맵핑(Key Mapping) 체계를 갖는 것이다. 이러한 방식은 일부 시스템들이 키들을 가지기 때문에 더 안전하게 운영될 수 있다. 그러나 이러한 단방향 키들의 분배는 시스템들의 수가 증가할수록 관리 및 운영이 어려워진다는 단점이 있다.

③ 취약한 장치 인증 기술(MAC 인증)

무선랜 카드별로 사용자 접속을 통제하고자 나온 기술이 MAC 인증 기술이다. 이것은 클라이언트 랜카드마다 고유하게 가지고 있는 하드웨어 주소값인 48bit의 MAC 주소를 가지고 액세스 포인트에서 접속 허용여부를 결정하도록 필터링하는 기술이다.

이 방식은 2가지 취약성이 존재한다.
첫째는, 무선랜 액세스 포인트에서의 MAC 인증은 표준화되어 있는 방법이 아니라는 것이다. 장비마다 지원범위나 구현방식이 상이하므로 상호운영상의 문제가 있을 수 있다.
둘째로, 무엇보다 오늘날에는 이러한 MAC주소의 위조가 간단히 이루어지기 때문에 적절한 보안강화 방법이라 할 수 없다. 사용자의 네트워크 소프트웨어는 하드웨어 주소인 MAC을 일단 메모리 영역에 읽어 들인 후, 통신에 사용하므로, 이 메모리 내용을 변경하는 소프트웨어를 가지고 MAC위조가 손쉽게 이루어진다. 때문에 MAC 인증방식은 무선랜의 보안기술의 하나로 사용되기에는 충분치 않다.

④ 취약한 암호화

무선랜 표준인 IEEE 802.11에 포함된 암호화 기술은 WEP(Wired Equivalent Privacy) 이라고 불린다. WEP은 RC4 대칭키 암호화 기술에 바탕을 두고 있으며, 24자리의 초기값을 베이스 키에 추가한 값을 초기 암호화 키로(Initial vector) 사용한다.

WEP 암호화는 간단한 처리로 무선 데이터 전송시의 암호화 처리가 가능하였으나, 시간이 지나면서 여러 가지 취약점이 발견되었다. 사용자가 암호화키를 안전하게 입력하는 방법이 없는

탓에, 현재는 관리자가 LAN카드 배포시 직접 하드웨어에 입력하는 방식을 사용하고 있다. 이러한 방식의 문제점은 모든 무선 단말과 AP가 항상 동일한 암호키를 사용 해야 하므로 랜카드나 AP의 분실 및 도난시에 키를 공유하고 있던 모든 구간에서 암호화가 무력화 된다. 또한 WEP 암호화는 수학적 허점으로 인해서 해커가 암호화된 데이터를 일정량 이상 수집할 경우, 키를 쉽게 분석 해낼 수 있는 취약점이 존재한다.

⑤ 안전한 로밍 기술의 부재

무선랜 세션은 AP와 클라이언트 사이의 1:1 연결로 이루어진다. AP 는 자신에게 접속된 클라이언트를 관리하며, 트래픽을 주고받는다. 무선 환경의 특성상 사용자가 다른 공간으로 이동할 경우, 접속되어 있는 AP의 셀 범위를 벗어나 다른 AP의 셀 범위로 들어가는 경우가 발생한다. 이때, 원래 접속되어 있던 AP에서 새로이 접속한 AP에게 클라이언트의 정보를 전달하고, 암호화키와 같은 보안정보를 함께 전달하여야 한다. 현재는 이러한 안전한 로밍 기술이 표준화되어 있지 않으며 몇 가지 상용화된 경우가 있으나 제품간의 호환성은 제공되지 않는다.

⑥ 하드웨어 장비의 분실

하나의 클라이언트 호스트를 분실한다면, 허가된 사용자들은 더 이상 MAC 주소나 WEP 키를 사용하여 접근 권한을 얻지 못할 것이며, 이러한 무선랜 사용을 알고 있는 비인증된 사용자들은 무선랜에 접근할 수 있을 것이다. 이러한 이유로 관리자들은 보안위험을 탐지하는 것이 불가능해질 것이다. 그렇기 때문에 클라이언트 사용자들은 이러한 장비의 분실에 대한 내용을 반드시 관리자에게 알려주어야 하며 관리자는 무선랜 접근에 대한 WEP 키와 MAC 주소를 더 이상 사용하지 못하도록 하여야 하며, 보안정책을 수정해 주어야 한다. 클라이언트의 수가 많으면 많을수록 WEP키나 MAC 주소의 관리업무는 많아질 것이다.

⑦ Rogue AP

IEEE 802.11b의 공유키(Shared-key) 인증체계는 상호인증방식이 아닌 단방향의 인증방식을 사용한다. 즉 AP는 한 사용자를 인증하지만, 사용자는 AP를 인증할 수 없다는 것이다. 올바르게 설정되어 운영되지 못하는 AP가 무선랜 구간에 위치되어 질 경우에는 합법적인 사용자의 하이재킹(Hijacking)에 의하여 서비스 거부공격의 시발점이 될 수 있는 문제점이 있다.

나. 기업의 무선랜 보안 요구사항

무선랜 사용자가 안심하고 네트워크를 사용할 수 있도록, 안전한 암호화 기법을 채택해야하며, 대규모 조직의 경우, 사용자 인증을 통해 허가받은 사람만이 AP를 통해 네트워크에 접근 할 수 있도록 해야 한다. 또한 장치 인증 기술을 통해 허가받은 AP만을 네트워크에 연결할 수 있도록 하는 것 또한 중요하다. 이것은 보안설정이 되어 있지 않은 AP를 통해 허가받지 않은 외부의 사용자가 네트워크에 무단으로 접속해 들어오는 것을 방지하며, 동시에 해커가 설치한 AP를 통해 사용자의 인증정보를 수집하는 것을 방지하기 위해 필수적이다.

(1) 기업의 무선랜 정책적 요구사항

- 무선랜 보안 위협을 인식하고, 무선랜 도입 전에 안전하고 충분한 보안정책을 결정한다
- 무선랜 보안설정은 설치과정의 일부임을 인식한다.
- 무선랜을 기존 네트워크와 분리하고 침입차단시스템 및 DMZ를 두고 운영하는 것은 네트워크의 2중 투자를 유발하므로, 기존 네트워크의 액세스 영역 확장의 입장에서 접근하여야 한다.
- 다양한 클라이언트 OS환경을 지원할 수 있어야 한다.
- 다양한 클라이언트 애플리케이션(무선랜 내장 PDA, 산업용 임베디드 기기, 프린터, POS 시스템, 계측기등)에 대응할 수 있어야 한다.
- 채택하는 인증기술(인증서, 패스워드)에 따라 관리의 부담이 달라진다.
- 중앙식, 분산식 등 인증서버의 설치 운영 정책이 필요하다.
- 802.11i 등 진화하는 표준안에 대응할 수 있는 시스템 운영방안을 마련한다.

(2) 기업 무선랜 기술적 요구사항

- 브리지와 같이 무선 클라이언트의 개입이 없는 유선 네트워크간의 무선 연결시에도 인증 및 동적 암호화키와 같이 일반 AP-클라이언트와 동일하거나 그 이상의 보안 강화가 필요하다
- 사용자 사이에서, 또는 장치 사이에서 이루어지는 Ad-hoc 기반의 통신에 대해서도 적절한

보안 강화체계가 필요하다.

- 사용자인증은 조직내부의 인사 시스템과 연계할 수 있도록 적용되어야 한다.
- 데이터 암호화 이전에 발생하는 인증과정은 외부의 도청에 대해 강건 해야 한다.
- 사용자 패스워드나 인증서등은 제한된 기간 내에서만 사용되며, 사용자에 의해 갱신할 수 있어야 한다.
- QoS, 멀티캐스트, 멀티프로토콜과 같은 유선랜 환경을 최대한 계승할 수 있도록 해야 한다.
- 다양한 사용자 프로파일을 수용할 수 있는 복수, 다계층 보안설정을 지원해야 한다.

다. 무선랜 보안 요소기술 분석

WLAN의 보안 요소기술을 인증, 암호화, 안전한 무선랜 로밍, 서비스 거부 방어 공격에 대하여 분류하고, 각각에 적용되는 세부기술에 대하여 [표 7-4-2]에 제시하였다.

[표 7-4-2]에 제시된 보안요소 기술에 대한 세부적인 사항을 설명한다.

[표 7-4-2] WLAN 보안 요소기술 분석

보안요소기술	분 류	세부 기술
인증기술	사용자인증	EAP-MD5, EAP-TLS, EAP-Cisco(LEAP), EAP-TTLS, PEAP(MS-CHAPv2), PEAP(EAP-GTC), EAP-SIM
	AP 인증	불법 AP 탐지 및 검색 기술 스위치 상의 802.1x 기술 불법AP의 차단 및 분리 기술
암호화 기술	WEP을 대체하는 새로운 암호화 기술 도입	WPA 표준에 준한 TKIP-MIC 802.11i 표준에 의한 AES-CCM 암호화 기술
안전한 무선랜 로밍	빠른 재인증 기술 (동일 서브넷에서 AP간 로밍시)	Pre-authentication Local Authentication Fast Hand-off 무선랜 셀간 이동을 위한 고속 로밍체 기술
	빠른 재인증 기술 (서브넷간 AP 로밍시)	Mobile IP over IPv4 Mobile IP over IPv6
서비스 거부 공격 방어	802.1h 적용	DFS / TPC 기술
	관리기능 향상	불법노드의 물리적인 탐지 및 제거

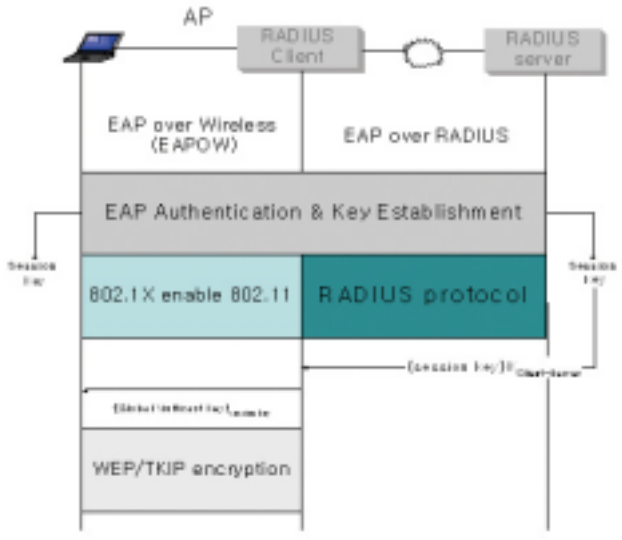
(1) 인증기술

① 사용자 인증

사용자 인증시 암호화키를 교환할 수 있도록 하되, 암호화 키는 인증과정을 통해 생성된 세션키의 형태로 전달된다. 양방향 인증으로 사용자의 정보 및 세션키, 인증 타입등의 정보가 포함되어 있는 인증 데이터가 해커에게 노출되지 않도록 조치해야 한다. 이를 위해서, IEEE 802.1x 인증 프레임워크가 세계적으로 폭넓게 사용되고 있으며, 802.1x 프레임워크를 사용한 다양한 인증 프로토콜이 개발되고 있다.

802.1x에서 사용되는 인증프로토콜은 EAP (Extensible Authentication Framework)가 대표적이며, 인증에 사용되는 정보와 메커니즘에 따라 다양한 EAP 프로토콜이 등장하고 있다.

WLAN의 안전한 인증 과정을 위한 802.1x
(그림 7-4-2)



802.1x에서 사용하는 보안 요소기술인 EAP의 종류에 대하여 나열하고 각각에 대해서 분석한다.

- EAP-MD5

  인증서버의 인증과정이 없는 단방향 인증인 탓에, 인증정보의 유출가능성이 있으며, 해시 형태의 패스워드와 외부에 노출된 사용자 이름(ID)을 가지고 인증을 하므로, 이 정보를 해커가 대기를 통해 수집한 후 오프라인 딕셔너리 공격을 통해 패스워드를 복구할 수 있는 허점이 있다.

  또한 세션키 교환 과정이 없으므로 무선랜의 암호화 키를 교환하지 않는다. 이것은 사용자 인증과 암호화라는 2가지 보안요소를 적용할 수 없다는 단점으로 나타나므로 향후의 보안 인증 기술로써는 부족하다고 할 수 있다.

- EAP-TLS

  공개키 기반의 인증서의 교환을 통해 사용자 인증 및 암호화 키 생성이 가능하다. 표준화

된 EAP 기술중 가장 안전하지만, 인증과정의 부담이 큰 편이고, 복잡한 인증서 관리가 필요하다. 또한 한번 사용자 클라이언트에 인증서를 다운받은 후에는, 아무런 추가 인증과정 없이 무인증으로 네트워크에 접근할 수 있으므로, 별도의 추가 네트워크 보안 체계를 필요로 한다.

- EAP-Cisco(LEAP)

  양방향 인증이므로 해커의 인증정보 수집을 막고, 무선데이타 암호화를 위한 세션키의 생성도 제공한다. 서브넷내의 AP간 이동시에 암호화 키 및 인증정보를 AP 끼리 주고 받아 빠르고 안전한 로밍이 가능하다.
  해시된 패스워드를 인증정보로 사용하므로 해커가 이를 수집하여 오프라인기반의 사전대입 공격에 사용할 수 있다. 시스코의 무선AP에서만 지원하는 방식.

- EAP-TTLS

  양방향 인증, 세션키 교환, 터널링을 통한 인증 정보 암호화 등 진보된 인증기술을 제공하고 있으나, 클라이언트 OS에 기본 제공되지 않는, 상용 제품화된 기술이다. 또한 인증과정에 참여하지 않고도 접속이 가능한 Man-in-the-Middle 공격 가능성에 노출되어 있다. 아직 표준화가 완료되지 않았다.

- PEAP(MS-CHAPv2)

  양방향 인증, 세션키 교환, 터널링을 통한 인증정보 암호화등 진보된 인증기술을 제공하면서, 클라이언트 OS 에서도 기본 포함된 기술이다. 마이크로소프트와 시스코등 대형 회사가 지지하고 있는 기술이다. EAP-TTLS 와는 달리 Man-in-the-Middle 공격의 보완방안을 제시하고 있다. 표준화는 아직 진행 중이다.

- PEAP(EAP-GTC)

  기본적인 PEAP 인증방식의 특징을 유지하면서, 클라이언트 인증방식에 토큰카드 방식을 적용한 방식으로 OS에 기본 내장되어 있지 않고 별도 클라이언트 설치가 필요하다. RDBMS, LDAP, NDS 등 폭넓은 사용자DB를 인증용도로 사용가능 하다.

● EAP-SIM

GSM 의 SIM 모듈을 사용해서 EAP 인증에 사용하기 위한 표준기술로, 노키아와 시스코가 표준화 추진 중에 있다.

② AP 인증

AP 인증은 관리자의 허락 없이 무단으로 설치되는 AP 들로 인해 조직 내의 보안 체계가 무너지고 사용자 인증 정보가 외부로 유출되는 것을 막기 위해 필수적으로 적용해야 하는 정책이다. AP 인증을 위해서 우선 올바른 AP 와 불법AP를 유/무선 상에서 구분할 수 있는 체계가 필요하며, 2차적으로 탐지된 불법 AP를 네트워크 상에서 분리 할 수 있는 시스템이 요구된다.

(2) 암호화 기술

● 취약한 WEP을 대신하는 새로운 암호화 기술의 도입
- WPA 표준에 준한 TKIP-MIC 암호화 기술
  • 48bit 초기화 벡터(IV) 사용
  • Per Packet Key Mix
  • 유니캐스트용 PMK 와 멀티캐스트용 GMK 관리
  • SOHO 환경을 위한 PSK
- 802.11i(WPA2) 표준에 준한 AES-CCM 암호화 기술

(3) 안전한 무선랜 로밍

● 동일 서브넷내의 AP간 로밍시, 빠른 재인증 기술
- Pre-authentication
- Local Authentication
- Fast Hand-off
- 고속의 메트로 무선랜 셀간 이동을 위한 고속 이동체 로밍 기술

● 서브넷간 AP 로밍시, 빠른 재인증 기술
- Mobile IP over IPv4
- Mobile IP over IPv6

(4) 퍼블릭 무선랜 보안 기술

● 가상 AP (Virtual AP) : 복수개의 ISP 가 하나의 AP 인프라 스트럭처를 공유 하는 기술.

(5) 서비스 거부 공격 방어

Denial-of-Service, 즉 AP 에 접속요청을 반복하거나, 노이즈 형태의 무선신호를 무선구간에 전파, 네트워크를 사용불능으로 만들게 하는 공격형태로부터의 방어

● 802.11h 적용
802.11h 는 DFS(Dynamic Frequency Selection) 및 TPC (Transmit Power Control) 기술이다. 이중 DFS 기술은 DoS 형태의 공격시, AP가 네트워크의 중단없이 사용하는 주파수를 자동변경토록 하는 기능이다.

● 관리기능 향상
제한 출력이상의 클라이언트가 무선구간에 존재할 경우, 중앙의 NMS 에 이를 보고하고, 관리자로 하여금 불법노드의 물리적인 탐지 및 제거를 할 수 있도록 한다.

c o n t e n t s

제8장
개인정보보호

제1절 개인정보관리책임자의 개인정보보호

1. 개인정보관리책임자의 현황 및 문제점

산업전반에서의 개인정보 활용 업무 빈도가 높아짐에 따라 사내 개인정보관리 및 보호 체계를 감독하는 개인정보관리책임자의 역할이 더욱 중요시되고 있다. 그러나 2003년 7월, 학원, 게임 사이트, 통신사업자, 호텔 등 448개 사업자의 웹 사이트 모니터링 결과 수집 및 이용 목적 등 정보통신망이용촉진및정보보호등에관한법률(이하 '정보통신망법' 이라 한다)의 한국정보보호진흥원에서 규정하고 있는 의무고지 사항 5가지를 모두 고지하고 있는 사업자는 45%에 불과하였다. 모니터링 결과 개인정보관리책임자가 지정되지 않거나, 형식적으로 지정된 경우가 많은 것으로 나타났다. 개인정보관리책임자가 지정된 경우는 57%에 불과하고, 개인정보관리책임자가 지정된 경우에도 24%가 법률 위반사항이 있는 것으로 조사됨으로써 개인정보관리체계가 매우 허술함이 심각한 것으로 나타나고 있다.

[표 8-1-1] 2003년 개인정보보호 준수 모니터링 결과

업종	조사 사업자수	평균 준수율	업종	조사 사업자수	평균 준수율
금융회사	60	75.1%	호텔	30	19%
결혼정보	50	38%	여행사	30	33.3%
학원	50	39%	구인 · 구직	20	69.1%
유선방송	48	10.3%	검색포털	10	90%
게임	30	79.5%	기타 기업	90	67.3%
인터넷 ISP	30	47.6%			

2. 개인정보관리책임자의 의무

국민의 프라이버시를 효과적으로 보호하고 법제정 취지에 부합하기 위해서는 개인정보관리책임자에게는 정보보안과 관련된 사항 뿐 아니라, 개인정보의 인권적인 측면, 법 · 제도적인 측면 등 다양한 분야의 전문적인 지식습득 등의 자질이 요구된다.

정보통신망이용촉진및정보보호등에관한법률에서는 정보통신서비스제공자등에게 이용자의 개인정보를 취급하는 자를 최소한으로 제한하도록 규정하고(제24조제3항), 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정할 것을 의무화하고 있다(제27조제1항). 또한 이용자의 개인정보를 취급함에 있어 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적 · 관리적 조치를 강구시행토록 하며(제28조), 개인정보의 수집 목적 또는 제공받은 목적을 달성한 때에는 당해 개인정보를 지체 없이 파기하도록 규정하고 있다(제29조). 그리고 이용자의 개인정보를 취급하거나 취급하였던 자가 직무상 알게 된 개인정보를 훼손 · 침해 또는 누설하는 행위를 금지하고(제24조제4항), 이를 위반하는 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있다.

한편, 개인정보보호지침은 개인정보관리책임자의 임무를 보다 구체적으로 규정하고 있다. 동 지침 제15조는

▶개인정보관리책임자에게 이용자 개인정보의 수집 · 이용 · 제공 및 관리에 관한 업무의 총괄

▶서비스제공자등의 소속 직원 또는 제3자에 의한 위법 · 부당한 개인정보침해행위에 대한 점검

▶이용자로부터 제기되는 개인정보에 관한 불만이나 의견의 처리 및 감독, 기타 이용자의 개인정보보호에 필요한 사항에 대한 감독 의무를 부과하는 규정을 두고 있다.

개인정보보호의 중요성 그리고 법령 규정의 취지에 따라서 개인정보관리책임자는 개인정보보호와 관련한 전문지식 습득을 위하여 노력하여야 하고, 적어도 법이 규정한 개인정보보호 사항을 이해할 수 있도록 개인정보보호 의식 및 자율규제 역량을 강화할 필요가 있다.

기업의 건강한 정보윤리 의식과 고객 정보보호의 사명감을 고취하는 행동강령 및 실천의지를 확립하는 차원에서 2003년 3월 26일 소공동 롯데호텔에서 이동통신사, 쇼핑몰 및 포탈업체, 코스닥 기업 등 일부 금융권과 정보통신산업계 36개 업체 대표임원과 개인정보관리책임자 120여명이 참여한 가운데 '정보윤리 및 개인정보보호 선언문'을 채택, 대외에 공표했다.

국민에 대한 기업의 정보윤리 및 개인정보보호를 위한 책임의식과 경영의지를 담은 이 행동강령은 1 · 25 인터넷 대란과 일부 기업의 개인정보 불법 유출 등으로 인한 인터넷 및 전자상거래 시장

에 대한 사회적 불신과 실추된 신뢰감을 회복하기 위한 관련 업계의 자성과 함께 자발적으로 시장질서를 쇄신해야 한다는 취지에서 마련된 것으로, 정직하고 올바른 기업윤리와 고객의 개인정보를 보다 철저히 보호하고 관리토록 하는 내용을 담고 있다.

정보윤리 및 개인정보보호 공동선언문

우리는 정보화 시대의 선도 기업으로서 정직하고 올바른 기업윤리를 바탕으로 소비자의 개인정보를 내 자신의 정보와 같이 철저하게 보호하고, 모든 고객으로부터 깨지지 않는 신뢰와 깊은 사랑을 받을 수 있도록 건전한 기업으로 거듭남으로써, 지식 정보화 사회 정착에 이바지하고자 다음과 같이 우리의 행동강령을 정하여 이를 실천해 나가고자 한다.

하나. 우리는 대한민국의 기업으로서 사회 공익에 대한 책임과 의무를 다하며, 소비자의 건전한 정보문화 생활과 권익보호에 앞장선다.

하나. 우리는 정보화 시대의 선도 기업으로서 기업 상호간의 공정한 경쟁을 추구하며, 정보윤리 및 개인정보 보호에 최선을 다한다.

하나. 우리는 고객정보를 수집하는 경우 소비자의 동의에 따라, 공정한 절차와 수단을 통하여 기본적 인권을 침해할 우려가 있는 내용을 배제하고 최소한의 정보만을 수집하고 활용한다.

하나. 우리는 수집된 고객정보를 제공받은 목적 이외의 다른 용도나 부적절한 이익을 위하여 이용하거나 타인에게 제공하지 않는다.

하나. 우리는 고객정보의 수집목적 또는 제공받은 목적을 달성한 때에는 해당 고객정보를 지체없이 파기하거나 정당한 조치를 취한다.

하나. 우리는 고객정보를 소중하게 보호함과 동시에 최신의 상태로 유지 관리함으로써, 소비자의 권익증진과 사생활 보호에 최선을 다한다.

하나. 우리는 고객정보의 안전과 정확성 및 최신성을 위하여 고객정보 접근은 최소한의 직원으로 한정하며, 내부직원의 철저한 교육과 책임 부여로 소비자보호에 최선을 다한다.

하나. 우리는 건강한 기업정신과 책임감을 바탕으로 고객정보의 건전한 활용과 창의적인 정보문화 생활 정착에 기여한다.

제2절 개인정보보호의 주요 현황

1. 개인정보침해 현황

기업이 보유하고 있는 고객의 개인정보는 그 자체가 중요한 자산으로서 해킹 등에 의한 유출 등 대내외 침해 가능성이 상존하고 있다. 이에 따라 개인정보침해신고센터가 설립된 2000년 4월 이후 개인정보침해 관련 상담 및 신고 접수 건수도 해마다 증가하고 있다. 다음의 [표 8-2-1]에서 보는 바와 같이 2003년 개인정보침해 상담 · 신고 접수는 21,585건으로 2002년 17,956건에 비해 1.2배 증가했다. 이 수치는 2000년의 2천여 건에 비하면 10배 이상 증가한 수치이다.

[표 8-2-1] 연도별 신고 · 상담 접수현황

구 분	2000년	2001년	2002년	2003년	계
신 고	329	388	1,237	8,991	10,945
상 담	1,706	10,776	16,719	12,594	41,795
합 계	2,035	11,164	17,956	21,585	52,740

(단위 : 건)

[표 8-2-2] 개인정보 침해 유형별 신고 · 상담 접수현황

순위	침 해 유 형	2003
1	주민번호, ID 도용 등 타인 정보의 침해	8,058
2	개인정보 수집시 고지 또는 명시 의무 불이행	2,491
3	개인정보관리책임자 미지정	1,279
4	법정대리인의 동의없는 아동의 개인정보 수집	1,195
5	동의철회 · 열람 또는 정정 요구 불응	825
6	고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공	337
7	이용자의 동의없는 개인정보 수집	260
8	동의철회, 열람 · 정정을 수집보다 쉽게 해야할 조치 미이행	229
9	기술적 · 관리적 조치 미비로 인한 개인정보 누출 등	181
10	개인정보 취급자에 의한 훼손 · 침해 또는 누설	172

11	수집 또는 제공받은 목적 달성 후 개인정보 미파기	129
12	과도한 개인정보 수집	38
13	영업의 양수 등의 통지의무 불이행	9
14	개인정보 처리 위탁시 고지의무 불이행	8
15	기타	6,374
	합 계	**21,585**

(단위 : 건)

※ 침해 유형 중 기타(15) 유형은 해킹 · 바이러스, 불법 스팸, 인터넷 사기결제, 도청, 몰래 카메라, 불법채권 추심, 텔레마케팅, 기타 법령 질의 등을 분류하여 구성한 것이다.

위 표에서 볼 수 있듯이 사업자가 개인정보 수집시 이용자에게 고지하여야 할 사항을 고지하지 않는 경우와 이용자의 고충을 해결하기 위한 개인정보관리책임자 지정 의무를 지키지 않는 경우가 각각 2,500여건, 1,300여건으로 이를 합하면 전체 민원의 20%에 근접하여 아직도 사업자의 개인정보 보호의 중요성에 대한 인식이 저조한 것으로 나타났다. 개인정보보호 인식이 상대적으로 낮은 신생 웹사이트 운영업자의 증가도 개인정보 침해의 한 원인으로 분석된다.

2. 개인정보 피해구제 신청 현황

2003년 한 해 동안 개인정보분쟁조정위원회에 접수된 개인정보 피해구제 신청은 총 845건이 접수되었다. 이 중 개인정보를 수집하여 그 수집목적을 달성한 후에 해당 개인정보를 파기하여야 함에도 불구하고, 파기하지 않은 사업자에 대한 피해구제 신청 건수가 81건으로 2003년 4/4분기부터 큰 폭의 증가를 보이고 있다. 또한 이용자의 개인정보 사용에 대한 동의의 철회, 개인정보의 열람 · 정정 청구에 대하여 즉시 필요한 조치를 취하지 않은 사업자에 대한 피해구제 신청 건이 52건, 그리고 사업자가 서비스이용약관이나 개인정보보호정책에 고지 · 명시한 범위를 넘어서 이용자의 개인정보를 이용하거나 제3자에게 무단으로 제공하는 경우에 대한 피해구제 신청 건은 39건에 이르고 있다. 이는 역시 사업자가 이용자의 개인정보 중요성에 대한 인식이 저조함을 보여주는 것이다.

3. 개인정보침해관련 주요 사례

개인정보관리책임자가 개인정보를 저장 또는 관리하는 유형을 살펴보면, 일반적으로 정보를 DB화하여 정보시스템의 서버 및 컴퓨터 하드디스크에 저장 하거나 또는 회원가입신청서 등 개인정보가 담긴 문서를 캐비넷, 금고, 창고 등 특정 장소에 보관한다. 그리고 이에 대한 관리는 정보보호 시스템(침입차단시스템, 암호화 S/W의 활용 등)을 이용하여 보호를 위한 기술적 조치를 취하고, 개인정보 취급 및 관리에 대한 내부 지침을 마련하고 취급자에 대한 교육 등을 통해 관리적 조치를 취한다.

그러나 이러한 개인정보의 안전성 확보를 위한 관리적 · 기술적 조치를 취하지 않아 이를 원인으로 하는 개인정보 침해가 발생하는 경우가 많다. 예컨대,

▶ 조직 내부의 개인정보 취급자에 의해 유출 · 훼손 · 변경 되는 경우
▶ 외부인의 불법적인 접근에 의해 개인정보가 유출 및 훼손되는 경우
▶ 사업자의 인식부족, 과실 등으로 인해 개인정보가 누출되는 경우
가 그것이다.

〈사례 1〉 이동 통신사 직원의 친구는 동거하던 여자를 찾던 중 평소 친하게 지내던 동거녀의 친구 주소를 얻기 위해 이동통신사 고객정보 제공을 부탁하여, 그의 친구가 고객의 주소를 알려줌으로써 살인사건 발생

〈사례 2〉 공공도서관에서 근무하는 직원이 회원 2만명에 대한 개인정보를 빼내어 타인에게 매매하여 경제적 이익을 취득

〈사례 3〉 이동통신사의 고객관리요원이 회사의 고객 DB를 통하여 개인정보를 수집한 후에 당해 정보의 주체를 지속적으로 스토킹

〈사례 4〉 화재보험회사의 대리점 직원이 고등학교 후배의 부탁으로 동 후배로부터 제공받은 차량번호를 이용하여 차량조회컴퓨터 시스템을 이용하여 20여명의 개인정보를 제공한 사례

〈사례 5〉 해킹 등의 수단을 통해 고객정보를 빼내거나 정보를 훼손시키는 경우

〈사례 6〉 인터넷 쇼핑몰을 운영하여 속옷을 판매하는 사업자가 개인정보보호의 인식 부족으로 방송국에서의 취재 과정에서 속옷에 인쇄될 연인 사진이 방송에 나가는 것을 방치하여 심각한 인격 침해 발생

〈사례 7〉 인터넷 쇼핑몰 운영자가 상품을 구매한 소비자가 게시판을 통하여 상품의 품질에 대해 이의를 제기하자 이의를 제기한 소비자의 신상정보 및 거래 정보 등을 그대로 게시판에 공개한 사례

〈사례 8〉 온라인 구인구직업체가 고객과의 이직알선 컨설팅 내용을 업체 홍보를 위해 신문 기자에게 제공하였으나, 컨설팅 내용이 신문기사화 됨으로서 당해 고객이 현재 근무하고 있는 직장 내에서 피해를 입는 등 정신적 · 물질적 피해를 입은 사례

〈사례 9〉 이동통신사의 위치확인 서비스를 이용하던 한 여성이 통신사의 기술적 오류로 인하여 자신의 위치정보가 모든 사람에게 공개된 사례(위치확인 서비스는 당초 특정 대상자와의 약속을 통해 당해 대상자만이 자신의 위치를 확인하도록 되어 있는 서비스이나, 당시 자신과 사전에 설정되어 있지 않던 남자친구가 자신의 위치를 파악하게 됨으로써 알리고 싶지 않은 정보가 유출되었다)

〈사례 10〉 통신사업자의 기술적 조치 오류로 인하여 내부에서만 접속 및 이용할 수 있는 프로그램이 유출되어 당해 프로그램을 통하여 고객의 신상정보의 열람이 가능하였던 사례 및 고객에게 제공하는 개인 미니홈페이지에서 가입자의 동의 없이 이동전화번호가 공개된 사례 발생

〈사례 11〉 사업자의 업무실수(요금내역 발송 이메일 리스트를 한명씩 밀려 입력함으로써 다른 사람에게 요금내역서가 송부됨)로 고객 3천명의 신용카드번호 및 신상정보 등이 유출된 사건

〈사례 12〉 구인 구직 웹사이트 운영자가 취직 희망자의 이력서 관리를 소홀히 하여 웹사이트에 이력서가 공개된 사례 및 여행사가 운영하는 웹사이트의 회원정보가 누출되어 특정인이 피해자의 ID와 비밀번호를 이용하여 피해자의 계정 자체를 변경하는 등 정보를 훼손시킨 사례 발생

〈사례 13〉 보험사가 기술적 오류로 인하여 보험가입 정보 등 중요 정보를 암호화 등 보안조치 없이 전송한 사례 발생

제3절 개인정보보호 관련 법 및 제도

1. 주요 정책 및 법제도 현황

헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다."고 규정해 사생활의 비밀과 자유(프라이버시)의 불가침을 명문으로 선언하고 있으며, 국민에게 프라이버시를 침해당하지 않을 소극적 권리뿐만 아니라 자신에 관한 정보를 적극적으로 통제할 수 있는 권리도 보장하고 있다.

사생활이란 "개인의 가장 깊은 곳에 자리한 자아의 외부로부터의 불가침을 전제로 한 것으로, 인격의 자유로운 발현과 인간으로서의 존엄성을 유지하게 하는 핵심영역"이다. 대법원은 헌법상 사생활 비밀의 자유를 보장하는 것은 "개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것"이라고 설명했다. 사생활의 자유와 비밀 보장은 언론의 자유와 마찬가지로 헌법에 보장된 권리이지만 언론의 자유와는 성격이 약간 다르다. 사생활의 자유는 자유권인 동시에 청구권의 성격을 갖고 있다. 즉 정부의 규제로부터 자유로운 권리인 동시에 정부의 힘을 빌어 보호를 받아야 하는 권리이기도 하다. 사생활의 자유가 보장되기 위해서는 개인의 사적 영역에 대한 정부의 통제와 간섭을 최소화해야할 뿐만 아니라, 기업이나 제3자로부터 개인의 사생활이 침해받지 않도록 정부가 적극 방지해야 하기 때문이다.

우리나라의 개인정보보호법제는 헌법과 개별 법률로 이루어지다가 공공부문의 행정전산망사업이 상당부분 성과를 보여 공공정보의 전산화가 이루어짐에 따라, 컴퓨터로 처리하는 개인정보를 보호하기 위한 '공공기관의개인정보보호에관한법률'이 제정되었다. 1994년에 제정된 이 법률은 정보사회의 개인정보 즉, 정보주체의 자기정보통제권이나 정보적 자기결정권 등으로 일컬을 만한 인식이 생긴 이후의 의미 있는 일반입법이라 할 수 있다. 이는 공공부문에서 컴퓨터로 처리되는 개인정보를 보호하기 위한 일반법으로 제정되었으며, 민간부문의 경우 1995년 '신용정보의이용및보호에관한법률'(이하 '신용정보법')의 제정을 비롯해 여러 개별 법률에 개인정보의 보호조항이 삽입되기에 이르렀다. 그러나 신용정보법의 경우 신용정보를 보호하려는 목적 보다는 신용정보를 제한적으로 이용해 관련 산업을 진흥시키고자 하는 목적이 더 강한 것이라 할 수 있으며, 다른 개별법에 삽입된 개인정보보호 관련 조항도 일반적·선언적 규정에 불과했다. 이후 초고속망 등 정보통신망이 확충되고 이를 통한 개인정보의 수집 및 유통이 일반화되어 민간부문의 개인정보보호 체계에 대한 반성이 일어남에 따라 1999년 기존의 '전산망보급확장및이용촉진에관한법률'의 제명을 '정보통신망이용촉진등에관한법률'로 바꾸고 미흡하나마 정보통신망을 통해 수집 및 유통, 활용되는 개인정보를 보호하기 위한 법제의 기틀을 마련하게 되었다. 그러나 공공부문의 개인정보보호법제가 단일 법제를 마련하고 있는 것에 비하면 이 역시 초보적 단계에 불과했다. 이후 2001년 이 법률의 제명을 다시 '정보통신망이용촉진및정보보호등에관한법률'로

바꾸면서 개인정보 관련 조항을 대폭적으로 개선함으로써 공공부문과 비슷한 보호 수준에 이르렀다.

이렇게 보면 우리나라 개인정보보호법제는 헌법을 최상위 근거법으로 하고 이에 대한 기본권을 보장하는 구체적 법률로서 공공분야에는 '공공기관의개인정보보호에관한법률' 이, 민간분야에는 '정보통신망이용촉진및정보보호등에관한법률' 이 각각 일반법으로 적용된다고 할 수 있다. 이외에 개별 법률은 양대 일반법에 대한 특별법으로서 개별 상황에 우선 적용된다고 볼 수 있다.

외국의 입법례를 보면, 우리나라와 같이 공 · 사 부문을 구별하면서 별개의 법률로 규율하고 있는 나라(미국), 공 · 사 부문을 구별하지 않고 단일 법률로 규율하고 있는 나라(스웨덴, 영국), 공 · 사 부문을 구분하되 단일 법률로 규율하고 있는 나라(독일, 프랑스) 등으로 대별할 수 있다.

[표 8-3-1] 우리나라 개인정보보호 관련 법률의 체계

헌 법

공공부문	구분	민간부문
공공기관의개인정보보호에관한법률	일반법(컴퓨터정보)	정보통신망이용촉진및정보보호등에관한법률
전자정부구현을위한행정업무등의 전자화촉진에관한법률		신용정보의이용및보호에관한법률
주민등록법, 호적법, 도로교통법, 자동차관리법령, 국세기본법, 예금자보호법	특별법 (일반선언규정 포함, 개별분야 적용)	보험업법령, 의료법, 전자거래기본법, 전자상거래등에서의소비자보호에관한법률, 응급의료에관한법률

국가인권위원회법, 전자서명법, 정보화촉진기본법, 정보통신기반보호법, 보건의료기본법, 사회보장기본법, 약사법, 정신보건법, 통신비밀보호법, 금융실명거래및비밀보장에관한법률 등

2. 민간부문의 개인정보보호 정책 및 법제도 현황

가. 민간부문의 개인정보보호 정책

정보화의 급속한 진전으로 인터넷 이용이 일상생활 속으로 확대되고, 공 · 사적 부분에서 정보기술 활용이 크게 증가하고 있다. 흔히들 21세기는 정보화 사회라고 한다. 정보화 사회란 컴퓨터의 신속한 정보처리와 다양한 통신 미디어의 광범위한 정보 전달로 대량의 정보가 생산 · 축적 · 전달되는 사회이다. 이와 같은 정보화 사회에서의 정보통신 발달과 범세계적 정보통신서비스의 기반 확대에 따라 사회 · 경제적 이익이 증가하고 있고, 또 한편으로는 개인정보가 컴퓨터에 의해 처리 · 활용되면서 개인의 명예훼손이나 지적재산권의 문제, 정크(Junk Mail)의 홍수 등 디지털화 된 개인정보의 오 · 남용 피해가 증가하고 있어 빅브라더스(Big Brothers)의 출현이 현실로 다가오게 되었다. 이처럼 프라이버시 침해가 증가함에 따라 정보통신 서비스 이용자들의 개인정보보호(Personal Information Protection) 문제에 대한 능동적인 규제의 요구가 증가하게 되었다. 이에 정보통신부는 공공부문을 제외한 민간부문의 개인정보보호를 위해 1999년에 종전의 '전산망보급확장및이용촉진에관한법률' 을 '정보통신망이용촉진등에관한법률' 로 개정하고 민간부문의 개인정보보호를 위한 법제를 최초로 마련한 것을 계기로 하여, 2000년 2월에 정보통신부 정보화기획실 내에 직제를 신설하고 정보이용보호과를 주축으로 개인정보보호를 위해 적극적으로 정책을 수립 · 시행하게 되었다.

2000년 이후에는 일차적으로 개인정보보호제도의 정착을 위해 '정보통신망이용촉진등에관한법률' 을 개정, 법 명칭을 변경해 '정보통신망이용촉진및정보보호등에관한법률' 을 시행(2001년 7월)함으로써 민간부분의 종합적인 개인정보보호 법제를 마련하게 되었다. 이에 따라 종래 정보통신서비스사업자에게만 적용되었던 개인정보보호 의무를 여행사, 호텔, 항공사, 학원 · 교습소에도 부여하고, 기업의 양도 · 양수, 합병시 이용자에게 개인정보 이전 사실을 통보하도록 의무화하는 한편, 14세 미만 아동의 개인정보 수집시 부모 등 법정대리인의 동의를 필수화했다. 또한 개인정보침해 분쟁을 신속 · 간편하게 해결하기 위해 개인정보분쟁조정위원회를 설치 · 운영하는 근거를 마련했다.

개인정보보호법제에 대한 사업자 및 이용자의 이해를 돕고 정보통신망법령의 부족한 부분을 보완하고자 2002년 1월 '개인정보보호지침'을 개정해 최초로 고시하고 2002년 4월에는 이에 대한 해설서를 마련·배포했으며, 2002년 9월에는 '인터넷 쇼핑몰 개인정보보호 가이드라인'을, 2002년 10월에는 만14세 미만 아동의 개인정보 수집 시 부모 등 법정대리인의 동의를 얻는 요령을, 2002년 12월에는 '개인정보보호를 위한 기술적·관리적 대책 수립을 위한 가이드라인'을 마련·배포했다. 또한 2003년 12월에는 '해지고객개인정보관리 지침'을 마련·보급해 이동통신사업자 등 정보통신서비스제공자가 보유하는 해지고객 정보에 대한 관리방안에 대한 기준을 정했고, 2003년 12월 '게임사이트 개인정보보호 지침'을 마련해 인터넷 게임사업자에게 개인정보보호 강화 방안을 제시했다.

2000년 4월에는 개인정보 침해사건에 대한 신고 접수 및 상담 기능을 수행하도록 개인정보침해신고센터를 한국정보보호진흥원(당시 한국정보보호센터)에 설치해 개인정보침해 민원을 해결하는 한편, 1999년 11월 이후로 인터넷사이트에 대한 모니터링을 매년 실시(2003년말 까지 총 8회, 3,400여개 사이트)해 법 위반 정도가 심한 사업자에 대해서는 과태료 처분 등 강력한 행정조치(2003년 11월말 현재, 시정명령 686건, 과태료부과92건, 수사의뢰 5건 등 784건 조치)를 취해 왔다. 2001년 12월에는 박준수 위원장 외 14명의 위원으로 개인정보분쟁조정위원회를 구성해 개인정보침해에 따른 각종 분쟁을 처리(2003년 12월말 현재, 24회, 1,151건)하고 있으며, 사무국 기능은 한국정보보호진흥원에서 수행하고 있다.

또한, 2001년 10월부터 11월까지 이동통신사(SKT, KTF, LGT, 신세기통신)의 본사, 대리점, 고객센터 및 판매점에 대한 개인정보보호 실태를 조사해 이동전화 가입자의 개인정보보호 강화를 위한 조치계획을 수립(2001년 12월), 각 이동통신사별 문제점 개선을 내용으로 하는 자체 추진계획을 2002년 1월까지 수립·시행토록 조치했다. 2002년에는 인터넷쇼핑몰(150개)에 대한 실태조사를 실시해 법 위반 업체를 처벌(9개 업체 과태료, 84개 업체 시정명령)하고 개선방안을 마련(2002년 6월)했으며, 7월부터 11월까지는 호텔·항공사·여행사(90개 업체) 등 Off-line 업체에 대한 실태조사를 실시해 호텔·항공사·여행사 총 6개 업체에 시정조치 명령을 내렸다. 2003년 8월에는 2001년에 이행토록 한 이동통신사 개인정보 조치계획에 대한 이행점검을 실시, 미진한 부분에 대해 시정조치 등 행정처분 조치를 했고, 2003년 7월부터 8월까지는 구인구직, 포털, 게임,

금융회사 등 448개 사이트에 대한 모니터링 및 실태조사를 실시해 법 위반 정도가 심한 사업자에 대해 시정조치 등 행정처분을 내렸다.

한편, 개인정보보호에 대한 민간자율규제를 활성화하는 차원에서 한국정보통신산업협회에서는 2002년 2월부터 '개인정보보호마크제도'를 도입·시행하고, 미국·일본 등 주요국과 마크 상호 인정을 추진하고 있으며(2003년 11월까지 KTF 등 102개 업체에 마크를 부여), 개인정보보호 및 스팸메일 방지를 위한 개인정보관리책임자협의회를 2002년 7월 구성했다. 또한 정보통신서비스 제공업체 개인정보관리책임자와 이용자에 대한 개인정보보호 교육·홍보를 위해 정보보호교양 교육을 실시하고 있으며, 2001년에는 130개 공공기간을 중심으로 2만 3천여 명에 대한 교육을 실시했고, 2002년에는 2001년 중 교육이 실시되지 않은 기관을 대상으로 상반기 중 20개 기관 3,000여명을 대상으로 교육을 실시했다. 아울러 한국정보보호진흥원에 사업자 개인정보관리책임자를 대상으로 하는 교육과정을 설치해 68개 업체 112명을 대상으로 교육을 실시했고, 2003년에는13개 기관 3,500여명의 이용자 교육을 실시했다.

나. 개인정보보호 법제도 현황

(1) 개인정보보호 제도의 연혁

민간부문의 개인정보를 보호하기 위해 포괄적으로 적용되는 법률로는 '정보통신망이용촉진및정보보호등에관한법률'(이하 '정보통신망법')이 있다. 이는 1999년 제정된 '정보통신망이용촉진등에관한법률'이 2001년 1월 16일 법률 제6330호로 전면 개정되고 명칭도 변경된 것으로서, 이 법률은 OECD에서 제시한 개인정보보호 8원칙을 수용하고, 유럽연합의 개인정보보호지침을 고려해 국민의 프라이버시 보호를 위한 개인정보의 수집·이용·제공에 따른 제반 사항과 스팸메일 등 악성 광고성 정보 전송행위 방지를 위한 제반 사항을 규정하고 있다.

(2) 정보통신망법의 주요 내용

(가) 개인정보의 정의

'개인정보'란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의해 당해 개인을 알아

볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합해 알아볼 수 있는 것을 포함한다)를 말한다. 흔히 개인정보를 개인이 보유한 정보로 잘못 인식하는 경우가 있는데, 신용정보, 거래정보, 내면의 비밀, 심신의 상태, 사회경력, 경제관계, 생활 · 가정 · 신분관계로 분류되는 각종 정보가 개인정보의 대상이 된다. 특히, 개인정보의 주체는 자연인이며, 법인 또는 이미 사망했거나 실종선고 등 관계 법령에 의해 사망한 것으로 다루어지는 자는 개인정보의 주체가 될 수 없으며, '정보' 를 "부호 · 문자 · 음성 · 음향 및 영상 등의 정보"라고 부연함으로서 다양한 개인 인식 수단이 포함된다는 것을 명확히 밝히고 있다.

(나) 적용 대상

'정보통신망이용촉진및정보보호등에관한법률' 에서의 개인정보보호 규정은 정보통신서비스제공자와 그로부터 개인정보를 제공받은 자(이하 '정보통신서비스제공자등'), 정보통신서비스제공자로부터 개인정보의 수집 · 관리를 위탁받은 자를 비롯해 '관광진흥법' 제3조제1항의 규정에 의한 여행업 또는 호텔업을 행하는 자, '항공법' 제2조제23호의 규정에 의한 항공운송사업을 행하는 자, '학원의설립 · 운영및과외교습에관한법률' 제2조제1호의 규정에 의한 학원 또는 동조 제2호의 규정에 의한 교습소를 설립 · 운영하는 자, 그 밖에 재화 또는 용역을 제공하면서 회원제 또는 그와 유사한 형태로 개인정보를 수집하는 사업자로 관계 행정기관의 장과 협의해 정보통신부령으로 정하는 자를 적용대상으로 하며, 스팸방지 규정은 영리목적의 광고성 정보를 전송하는 모든 국민을 적용대상으로 한다.

'정보통신서비스제공자' 는 전기통신사업법상 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용해 정보를 제공하거나 정보의 제공을 매개하는 자로서 PC통신 및 인터넷서비스제공사업자(ISP)를 비롯해 텔레마케팅업자, 인터넷 쇼핑몰, 인터넷 포털사이트 개설자 등이 모두 이에 포함되며, 보통 영업행위를 하는 주체가 홈페이지를 개설하는 경우에는 모두 적용대상이 되는 것으로 해석하고 있다. 특히 '영리 목적' 은 자기 또는 제3자의 재산적 이익을 얻기 위한 목적을 말하는 것으로 폭넓게 해석하고 있으며, 여기서의 이익은 계속적, 반복적일 필요는 없는 것으로 해석하고 있다.

'정보통신서비스제공자외의자' 는 정보통신서비스제공자에 해당되지 않는 호텔, 여행사, 항공사, 학원 · 교습소 등 off-line 사업자로서 이 법의 개인정보보호에 관한 규정이 준용되도록 하고 개인정보보호 의무를 위반한 자의 경우 정보통신서비스제공자와 동일한 벌칙에 처하고 있어 이 법은 사실상 민간부문의 개인정보보호에 관한 일반법으로서의 역할을 하고 있다.

이 법에서 보호하는 개인정보는 종이, 디스켓, 컴퓨터, 인터넷 등 개인정보가 저장되거나 유통되는 방법과는 무관하게 적용하고 있다.

(다) 다른 법률과의 관계

정보통신망법 제5조에서는 "정보통신망이용촉진및정보보호등에관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 의한다"고 규정하고 있으므로, '공공기관의 개인정보보호에관한법률' 은 적용대상이 공공기관이기 때문에 정보통신망법의 적용 대상인 영리목적의 정보통신서비스제공자와는 구분되나, 일부 중복되는 부분에 있어서는 '공공기관의개인정보보호에관한법률' 의 해당 조항이 우선 적용되고 있다.

또한 전자거래기본법, 전자서명법 등과 같이 민간부문에 적용되는 기타 법률의 경우에는 해당 법률이 특수 분야 즉, 전자거래, 전자서명, 신용거래, 증권거래 등 적용범위를 한정하고 있기 때문에 정보통신망법에 우선해 적용되며, 해당 법률에 규정이 미비한 경우에는 정보통신망법이 보충적으로 적용되어 정보통신망법이 민간분야 개인정보보호에 있어 일반법적 성격을 지니고 있다.

(라) 개인정보의 수집

① 필요 최소한의 수집 원칙

정보통신서비스제공자(법 제58조에 의해 이 법이 준용되는 재화용역제공자를 포함한다)는 이용자의 개인정보를 수집하는 경우 ① 정보통신서비스 이용계약의 이행을 위해 필요한 경우, ② 정보통신서비스 제공에 따른 요금정산을 위해 필요한 경우, ③ 이 법 또는 다른 법률에 특별한 규정에 있는 경우를 제외하고는 당해 이용자의 동의를 얻어야 한다. 한편, 정보통신서비스제공자는

이용자의 동의를 얻고자 하는 경우에는 개인정보의 수집 목적 및 이용 목적, 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공 목적 및 제공할 정보의 내용 등을 미리 이용자에게 고지하거나 정보통신서비스이용약관에 명시하도록 하고 있다

또한, 정보통신서비스제공자는 이용자의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우를 제외하고는 사상, 신념, 과거의 권리, 이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집해서는 안 되며, 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위해 필요한 최소한의 정보를 수집해야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 않는다는 이유로 당해 서비스의 제공을 거부해서는 안 된다.

② 동의의 원칙 및 그 예외

정보통신서비스제공자가 개인정보를 수집하는 경우에는 당해 이용자의 사전동의를 받도록 의무화(제22조제1항)하고 수집에 대한 동의를 받고자 하는 경우에는 미리 고지하거나 약관에 명시토록 의무화(제22조제2항)하고 있어, OECD 개인정보보호지침의 목적명확화의 원칙(Purpose Specification Principle) 및 공개의 원칙(Openness Principle)과 같은 취지로 규정하고 있다. 이러한 동의 원칙은 정보통신서비스 이용계약의 이행을 위해 필요한 경우, 요금정산을 위해 필요한 경우, 이 법 또는 다른 법률에 특별한 규정이 있는 경우에는 예외를 인정하고 있다.

③ 고지사항 또는 정보통신서비스이용약관 명시사항

정보통신서비스제공자는 개인정보 수집시 이용자에게 동의를 받기 전에 개인정보 관리책임자의 소속 · 성명 · 직위 및 전화번호 기타 연락처, 개인정보의 수집 목적 및 이용 목적, 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공 목적 및 제공할 정보의 내용, 이용자의 권리 및 그 행사 방법, 기타 대통령령이 정하는 사항(개인정보의 수집 항목, 수집하는 개인정보의 보유 기간 및 이용 기간)을 먼저 고지하거나 정보통신서비스 이용약관에 명시토록 함으로써 본인이 제반 상황을 정확히 인식한 상태에서 자신의 개인정보를 사업자에게 제공할 수 있도록 규정하고 있다.

(마) 개인정보의 이용 및 제공

정보통신서비스제공자가 이용자의 개인정보를 이용하거나 제3자에게 제공함에 있어 수집시 고

지된 범위를 초과하거나 정보통신서비스 이용약관에 명시한 범위를 넘어서는 경우 본인의 사전 동의를 얻도록 의무화하고 있다. 다만, 요금정산을 위해 필요한 경우, 통계작성, 학술연구 또는 시장조사 등의 목적을 위한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공해 제공하는 경우, 다른 법률에 특별한 규정이 있는 경우에는 본인의 동의를 얻지 않아도 제공이 가능하도록 규정하고 있다.

(바) 개인정보처리의 위탁

정보통신서비스제공자등으로부터 개인정보의 처리를 위탁받은 자가 당해 업무와 관련해 초래한 손해의 배상책임에 한해 그를 정보통신서비스제공자등의 소속 직원으로 보아 민법 제756조의 사용자책임 규정이 적용될 수 있도록 규정하고 있다. 따라서 위탁자인 정보통신서비스제공자가 선임 · 감독상의 과실이 없음을 입증하면 면책되나 아직 면책을 인정한 판례가 없으므로 사실상 무과실책임을 지도록 하고 있다.

(사) 영업의 양수 등의 통지

정보통신서비스제공자가 영업양도 · 양수 및 합병시 개인정보의 이전에 관해 이용자의 사전 동의를 얻도록 하는 것은 현실적으로 사업자에게 과도한 부담이 될 수 있다. 이러한 부담를 완화하기 위해 정보통신서비스제공자등이 영업을 양도하거나 합병 · 상속 등으로 그 권리 · 의무를 이전하는 경우와 정보통신서비스제공자 등으로부터 영업을 양수하거나 합병 · 상속 등으로 그 권리 · 의무를 승계한 자는 관련 사항을 이용자에게 통지하도록 의무화함으로써 전자상거래업체의 인수 · 합병이나 영업의 양도 · 양수의 경우에 사업자들의 편의를 위해 개인정보의 제3자 이전 시 동의의 예외를 인정하고 있다.

정보통신서비스제공자등이 영업의 전부 또는 일부를 양도하거나 합병 · 상속 등으로 그 권리 · 의무를 이전하는 경우(제26조제1항)에는 영업의 전부 또는 일부의 양도, 합병 또는 상속 등의 사실, 정보통신서비스제공자등의 권리 · 의무를 승계한 자의 성명(법인인 경우 법인의 명칭), 주소, 전화번호 기타 연락처를 이용자에게 통지하도록 규정하고 있다. 또한 정보통신서비스제공자등으로부터 영업의 전부 또는 일부를 양수받거나 합병 · 상속 등으로 정보통신서비스제공자등의 권리 · 의무를 승계한 자(제26조제2항)는 정보통신서비스제공자등의 권리 · 의무를 승계한 사실 및 해당

정보통신서비스제공자등의 성명(법인인 경우 법인의 명칭), 개인정보관리책임자의 성명 · 소속 부서 · 지위 및 전화번호 기타 연락처, 개인정보의 이용 목적, 동의의 철회 및 개인정보의 열람 · 정정 요구에 관한 이용자의 권리 및 그 행사 방법, 기타 개인정보보호를 위해 필요한 사항으로서 대통령령으로 정하는 사항을 이용자에게 통지하도록 규정하고 있다.

(아) 개인정보관리책임자의 개인정보의 보호조치 의무

정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 않도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 조취를 취하여야 한다(법 제28조). 즉 개인정보관리책임자는 이용자 개인정보의 훼손 및 누출 등을 방지하기 위한 저장 및 관리에 있어서, 정보보호 시스템(침입차단시스템, 암호화)에 의한 기술적 조치와 개인정보 취급자의 교육, 내부 지침 등 개인정보 체계 구축을 위한 관리적 조치를 취하여야 한다. 부연하면, 개인정보를 적절한 보안장치를 통해 분실 또는 불법적인 사용 · 변경 · 공개 등의 위험으로부터 보호되어야 하고, 이러한 법적 및 자율적 의무가 개인정보관리책임자에게 있음을 잊어서는 안된다.

(자) 아동의 개인정보보호

정보통신서비스제공자가 만14세 미만의 아동으로부터 개인정보를 수집하는 경우에는 사전에 부모 등 법정대리인의 동의를 얻도록 의무화(제31조)하고 법정대리인에 대한 동의는 전화, 이메일, 법정대리인에 의한 동의양식에의 기재, 우편 등을 이용하도록 하는 한편, 2003년 12월에는 14세 미만의 아동의 개인정보를 수집하면서 관행처럼 주민번호를 수집하는 것에 대해 생년월일만 수집하도록 하는 가이드라인을 제시, 이행토록 했다.

(차) 이용자의 권리

이용자는 정보통신서비스제공자등에 대해 언제든지 개인정보의 수집 · 이용 및 제3자에 대한 제공, 목적 외 용도에 대한 동의를 철회할 수 있으며(제30조제1항), 자신의 개인정보에 대한 열람을 요구할 수 있고, 오류가 있는 경우에는 그 정정을 요구할 수 있다(제30조제2항).

2003년 12월에는 개인정보를 이용하거나 제3자에게 제공한 내용을 요구할 수 있도록 이용자 권

리사항을 확대하는 내용을 개정했다(제30조제2항). 또한 정보통신서비스제공자는 이용자가 동의철회, 열람 · 내역 또는 정정 요구를 하는 경우에는 지체 없이 필요한 조치를 취해야 하고(제30조제3항, 제4항), 정보통신서비스제공자는 이용자로부터 오류의 정정 요구를 받은 경우 그 오류를 정정할 때까지 당해 개인정보를 제공 또는 이용해서는 안되며(제30조제5항), 만14세 미만의 아동으로부터 개인정보를 수집, 이용하는 경우에는 법정대리인의 동의를 얻도록 규정(제31조)하고 있다.

더불어 개인정보보호 규정 위반으로 손해가 초래되는 경우 정보통신서비스제공자등은 고의 또는 과실이 없음을 입증하지 않으면 책임을 면할 수 없게 입증책임을 전환하도록 규정하고 있다.

(카) 개인정보의 파기 · 삭제 의무

이용자가 개인정보의 이용 · 제공 등에 대해 한 동의를 철회한 경우, 정보통신서비스제공자는 개인정보를 삭제하지 않을 정당한 사유가 없는 한 이용자의 개인정보를 지체 없이 삭제하도록 했다. 다만, 이용자의 개인정보 삭제요청에도 불구하고 정보통신서비스제공자가 삭제하지 않을 수 있는 정당한 사유로는 다른 법에서 개인정보의 보유를 의무로 하고 있거나, 이용자가 서비스 이용요금을 연체하는 등 권리 · 의무 관계가 정산되지 않은 경우를 상정하고 있다.

(타) 개인정보의 침해에 대한구제

개인정보가 침해되는 전형적인 유형은 개인정보 주체(본인)의 승낙이나 동의 없이 개인정보를 수집 · 저장하는 경우, 동의한 범위를 넘어 제3자에게 개인정보를 제공하거나 양도한 경우, 고의 또는 우발적으로 발생한 개인정보의 오류를 유통함으로써 본인 및 제3자에게 침해를 가져오는 경우, 개인정보를 처리할 정당한 권한이 없는 자가 임의로 개인정보를 수집 · 이용하거나 제3자에게 양도하는 경우 등으로 분류할 수 있다. 정보통신망법에서는 개인정보침해신고센터를 통한 고충처리와 개인정보분쟁조정위원회를 통한 피해보상, 시정명령 · 과태료 부과 및 형사처벌에 의한 구제방법을 규정하고 있다.

개인정보보호법제 체계도
(그림 8-3-1)

① 개인정보침해신고센터를 통한 고충처리

개인정보침해와 관련한 고충처리와 상담을 전담하기 위해 한국정보보호진흥원(KISA)에 개인정보침해신고센터를 설치 · 운영(정보통신망법시행령 제26조)하고 있다. 개인정보침해신고센터는 정보통신서비스제공자등이 정보통신망법상의 개인정보보호 규정을 이행하는지 여부를 감시하고, 신고 접수된 사항에 대해서는 법 위반 여부에 대한 사실확인 조사를 거쳐 위반 정도에 따라 정보통신부에 과태료 등 행정처분 부과를 요청하거나 경찰에 수사 의뢰를 한다.

② 개인정보분쟁조정위원회에 의한 피해보상

개인정보에 관한 분쟁을 이용자의 비용부담 없이 신속 · 간편하게 조정하기 위해 2001년 12월부터 개인정보분쟁조정위원회를 설치 · 운영(제4장 제4절)하고 있다. 2003년 12월에는 분쟁업무를 효율적으로 수행하기 위해 분쟁조정위원회에 5인 이하의 위원으로 구성되는 조정부를 두도록 하고, 일부 분쟁에 대해 조정부에 일임해 신속한 분쟁처리를 도모하도록 정보통신망법을 개정했다.

③ 벌칙을 통한 규제

이용자의 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공한 자, 타인의 정보를 훼손하거나 타인의 비밀을 침해 · 도용 또는 누설한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에

처하도록 하고, 개인정보 최소수집의 의무, 고지의무, 동의 의무를 위반한 자, 수집 또는 제공받은 목적을 달성한 개인정보를 파기하지 않은 자, 개인정보관리책임자를 지정하지 않은 자, 개인정보의 오류를 정정하지 않고 이를 이용한 자 등은 1천만원 이하의 과태료에 처하도록 규정하고 있다.

제4절 부문별 개인정보보호

1. 금융부문 현황

가. 금융부문의 개인정보보호의 필요성

금융부문은 다른 업종에 비해 신용거래가 많기 때문에 거래 상대방에 대한 신용도를 판단하는 일이 매우 중요하다. 보다 정확한 신용도 판단을 위해서는 다양한 개인정보의 활용이 요구되며, 현실적으로도 다른 업종에 비해서 개인정보의 수집과 이용이 훨씬 더 광범위하게 이루어지고 있다는 점에서 금융부문에서의 개인정보보호의 필요성은 그 어느 분야보다 크다. 또한 오늘날 경제활동에서는 금융거래가 필수적이기 때문에 금융기관에 집적된 개인정보의 양과 질은 실로 방대하며, 개인정보가 부가가치를 창출하는 중요한 재화(Goods) 또는 재산적 가치가 있는 것으로 인식되고 있기 때문에 금융부문에서의 개인정보보호의 필요성은 재론할 여지가 없다.

나. 개인정보의 활용 체계

금융부문의 개인정보 중 '예금 등 금융자산을 대상으로 하는 거래에 관한 정보'(이하 '금융거래정보')는 '금융실명거래및비밀보장에관한법률'(이하 '금융실명제법')에 따라 특정한 경우[14]를 제외하고는 원칙적으로 제공·활용이 금지되어 있는 반면, 대출거래나 신용카드 발급 등과 관련한 신용정보는 '신용정보의이용및보호에관한법률'(이하 '신용정보법')에 따라 신용정보주체의 동의를 전제로 신용정보집중기관 및 신용조회업자에 의해 집중·관리되며, 금융기관 등 신용정

14) 법원의 제출명령, 조세범죄 관련 조사, 국정감(조)사, 금융감독목적 등

보제공 · 이용자가 동 정보를 이용할 수 있도록 허용하고 있다.

금융부문의 개인신용정보 활용체계는 신용정보집중기관 및 신용조회업자를 통해서 제공 · 활용되는 경우와 신용정보제공 · 이용자간 자체 협약[15] 또는 다른 법률에 따라 직접 공유되는 경우로 대별할 수 있다.

다. 금융부문에서의 개인정보보호 법제도

금융부문의 개인정보보호의 근거는 크게 금융실명제법과 신용정보법으로 대별할 수 있다. 금융실명제법은 금융거래정보의 보호에 한정되는 반면, 신용정보법은 금융거래정보를 포함한 식별정보, 대출정보, 연체정보 등 거래처의 신용도 판단 여부와 관련되는 정보의 보호에 관한 내용을 규율하고 있다.

(1) 금융실명제법상 보호 체계

금융기관에 종사하는 자는 명의인의 동의나 요구 없이 금융거래의 내용에 대한 정보를 타인에게 제공하거나 누설하여서는 안되며, 누구든지 금융기관에 종사하는 자에게 금융거래의 내용에 대한 정보를 요구해서도 안된다고 규정하고 있다(동법 제4조). 다만, 법원의 제출명령이나 조세탈루 혐의 조사목적, 국정감(조)사, 금융감독 목적 등에 따라 제공을 요구하는 경우는 예외이다. 뿐만 아니라 금융기관에 종사하는 자에게는 위법 또는 부당한 정보 제공 요구가 있는 경우 이를 거부하도록 의무화하고 있으며, 동법을 위반해 제공 · 누설된 정보를 취득한 자도 그 정보를 타인에게 제공 또는 누설할 수 없도록 규정하고 있다.

(2) 신용정보법상 보호 체계

신용정보법상 개인신용정보보호를 위한 장치는 첫째, 신용정보 제공 · 이용의 요건 제한, 둘째, 개인신용정보보호를 위한 보안장치 및 대책, 내부관리규정 수립 의무화, 셋째, 신용정보의 업무목적 외 누설 또는 제공의 금지 등으로 나누어 볼 수 있다.

15) 신용정보법 제27조제2항제1호에서는 "신용정보제공 · 이용자가 다른 신용정보제공 · 이용자의 업무에 활용하도록 하기 위하여 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공" 할 수 있도록 규정하고 있으며, 이 경우 제공된 신용정보제공 · 이용자 간에는 신용정보의 보안관리대책을 포함한 계약을 체결해야 한다.

(가) 신용정보 제공 · 이용의 요건 제한

신용정보의 제공 · 이용에 있어 일정한 요건을 제시하고 있는 바, 우선 절차에 있어서는 반드시 사전 동의를 받아야 제공 · 활용이 가능함을 명시하고 있다. 즉, 금융회사 등 신용정보 제공 · 이용자는 당해 신용정보주체로부터 제공 · 활용할 신용정보의 종류, 제공 대상기관 등을 구체적으로 명시한 '개인신용정보 제공 · 활용 동의서' 를 받도록 하고 있다(제23조).

또한 그 이용 목적에 있어서도 당해 신용정보주체와의 금융거래 등 상거래 관계의 설정 및 유지여부 등의 판단 목적으로만 제공 · 이용할 수 있도록 정하고 있으며, 상품안내 목적과 같이 동 목적 외의 제공 · 활용에 대해서는 반드시 별도의 동의를 받도록 하고 있다(제24조).

(나) 개인신용정보보호를 위한 보안장치 및 보안대책, 내부관리규정 수립 의무화

- 신용정보업 허가요건으로서 정보보안장치 강구 규정
  신용정보법 및 동법시행령, 신용정보업감독규정에서는 신용정보업 허가의 세부요건으로서 적절한 정보보안장치를 갖추도록 규정하고 있다. 이러한 정보보안장치의 구체적 내용은 침입차단시스템(Fire-wall)이나 정보이용자 확인체계 · 데이터 암호화처리체계 등을 갖추거나 외부침입 방지 · 출입자관리 통제 및 데이터 반 · 출입 통제에 대한 대책과 백업 및 소산관리 대책을 강구하도록 하고 있다.

- 전산보호대책 수립 의무화
  신용정보업자 외에 신용정보집중기관, 신용정보제공 · 이용자(이하 '신용정보업자등')도 신용정보시스템(공동전산망을 포함)에 대한 제3자의 불법접근 또는 입력된 정보의 변경 · 훼손 · 파괴, 기타 위험에 대한 기술적 · 물리적 보안대책을 수립하도록 하고 있으며, 이를 위반할 시 300만원 이하의 과태료에 처하도록 규정하고 있다.

- 신용정보업무 수행에 관한 내부관리규정 마련
  신용정보업자 등은 신용정보의 수집 · 처리 및 이용에 대해 금융감독위원회가 정하는 바에 의한 내부관리규정을 마련해야 한다. 이러한 내부관리규정의 구체적 내용은 신용정보의 수

집 · 처리 및 이용에 관한 세부절차, 신용정보 전산시스템의 기술적 · 물리적 보안대책, 신용정보의 열람 및 정정 청구업무 처리절차, 신용정보의 정확하고 신속한 등록 및 등록된 정보의 정확성을 상시 점검할 수 있는 시스템 등을 규정해 놓고 있다. 아울러 신용정보업자 등은 신용정보업무처리의 기록(의뢰인, 의뢰내용, 의뢰목적, 제공내용 등)을 일정 기간(3년) 보존토록 의무화하고 있어 개인신용정보 제공 · 이용에 대한 철저한 사후관리를 명시하고 있다.

● 업무목적 외 누설 또는 제공의 금지

신용정보업자 등과 신용정보의 처리를 위탁받은 자의 임직원이거나 임직원이었던 자는 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀을 업무목적 외로 누설 또는 이용할 수 없으며, 신용정보업 관련자로부터 신용정보를 제공받은 자는 타인에게 그 신용정보를 제공할 수 없도록 함으로써 신용정보를 제공받는 법인에 대한 책임뿐만 아니라 신용정보를 실질적으로 취급하는 개인에 대해서도 엄중한 관리책임을 묻고 있다.

[표 8-4-1] 신용정보법상 개인정보보호 관련 규정

구분	내용	위반시 벌칙 규정
신용정보의 제공 · 이용	제공 · 이용시 사전 동의 요함(§24)	3년 이하의 징역 또는 3천만원 이하의 벌금
	제공 · 이용 목적 제한(§24) (상거래관계의 설정 및 유지여부 판단 목적)	〃
정보보호 장치 및 규정 수립 의무화	정보보안장치 마련을 허가요건으로 규정 (§4조의2, 시행령 제4조의2 제1항 제1호 나목)	허가시 고려
	전산보호 대책 수립 의무화(§19)	과태료 300만원
	신용정보 내부관리규정 마련 의무화(§20 1항)	〃
업무목적외 누설 또는 제공금지	업무목적 외 누설 또는 이용 금지(§27 1항)	3년 이하의 징역 또는 3천만원 이하의 벌금
	신용정보관련자로부터 신용정보를 제공받은 자의 타인에 대한 신용정보 제공 금지(§27 3항)	〃

마. 최근의 이슈와 향후 추진과제

(1) 개인정보보호와 관련한 새로운 이슈

현재 우리나라의 금융환경은 급격한 변화일로에 있다. 외환위기 이후 부실기업의 부도와 금융시장에서 부실금융기관이 퇴출됨에 따라 부실채권의 발생을 사전에 예방하는 것이 금융기관의 건전성을 유지하고 금융기관의 존폐를 결정하는 요인으로 인식되어 각 금융기관은 여신 심사기법의 선진화에 주력하고 있다. 아울러, 부실기업 퇴출에 따른 기업자금수요 축소와 직접금융시장의 발달로 금융기관의 자금운용 대상이 기업중심에서 개인으로까지 확대되었다. 이에 따라 기업에 국한되었던 신용평가기법 활용과 데이터 집적의 필요성이 개인으로까지 확대되어 개인신용평가업(Credit Bureau : CB사업)의 중요성이 부각되고 있다. 또한, 금융기관들이 보험회사의 보험상품을 판매하는 방카슈랑스의 등장으로 금융기관 보험대리점과 보험회사간의 개인정보 공유체계가 현재보다 넓어질 전망이다.

- 개인신용평가업(CB사업)의 활성화

  미국 등 선진국에서 보편화되어 있는 개인신용에 대한 평가사업이 우리나라에서도 2002년 말 정식 출범했다. CB사업은 주로 개인의 신용도를 판단함에 있어 필요로 하는 각종 정보들을 집중, 가공 및 평가(Scoring)해 생성된 신용보고서를 신용공여기관에 제공하는 사업을 말한다. 주로 연체정보 등의 불량정보 위주의 데이터를 원형 그대로 집중·제공하는 기존의 신용조회업과는 달리 CB사업은 우량정보(Positive Information) 등을 추가로 집중해 신용평가를 위한 변수(Variables)를 현저하게 확대시키면서, 원형의 정보를 적절한 형태로 세분화하고 가공해 보다 객관적이고 정확한 신용도 판단이 가능하도록 지원해 준다.

  이러한 CB사업의 원활한 운영을 위해서는 집중대상 정보의 확대가 불가피하다. 즉, 현재 금융기관 등 신용정보제공·이용자에게 제공되고 있는 주요 개인신용정보는 대출정보(대출 및 보증현황, 신용카드 개설정보), 신용불량정보, 단기 연체정보 등에만 국한되어 있어 보다 정확하고 객관적인 신용평가가 불가능하다. 따라서 채무상환 이력정보, 소득정보, 직업정보, 납세실적, 각종 공공요금(Utility) 납부정보 등 우량정보 및 각종 공공기록정보의 제공이 필수적으로 요구될 뿐만 아니라 불량정보에 있어서도 현재의 단편적인 정보(연체

및 불량정보 등록 유무)가 아닌 연체기일, 연체금액, 상환방법 등 보다 입체적인 정보의 제공이 요구된다.

이러한 점을 고려할 때 CB사업의 활성화는 신용정보 인프라 확대를 통한 건전한 신용질서 확립에 크게 기여한다고 판단할 수 있지만, 개인정보보호 문제에 있어서는 보다 엄격한 장치 및 제도가 선결되어야 할 것이다.

● 방카슈랑스 개시

은행, 증권회사, 상호저축은행 등 판매망을 갖춘 금융기관에서 보험회사의 보험상품을 판매하는 방카슈랑스 제도가 2003년 9월 3일 시행됐다. 보험대리점인 금융기관은 일선 창구에서 자사 고객에게 보험상품을 판매하고 고객정보를 관리하는 한편, 보험회사는 보험대리점으로부터 당해 고객정보를 제공받아 관리하게 된다. 이로 인해 보험회사나 금융기관 모두 다양한 고객정보를 수집 및 접근할 수 있게 되어 이를 대출업무 등 다른 영업목적상 활용할 수 있는 범위가 넓어졌다. 그러나 이 과정에서 금융기관이 우월적 지위를 이용해 개인정보의 제공을 요구[16]하거나 무단으로 이용할 가능성이 더 커진 측면도 간과할 수 없으며, 보험상품 판매대리점인 금융기관과 보험회사간에는 고객정보의 소유권[17]이나 이용 · 접근 범위에 있어 대립이 발생할 소지도 있다. 그러나 어느 경우이든 신용정보법 제24조에 따라 보험계약의 체결 및 유지 이외의 목적에 의한 정보 활용은 별도의 동의를 받도록 되어 있으므로 다른 영업목적 외의 제공 · 활용에 있어서는 보험대리점 금융기관이나 보험회사 공히 사전동의 의무 준수가 철저히 요구된다.

(2) 향후 추진 과제

(가) 신용정보주체 보호 강화

개인신용정보의 보다 자유로운 유통과 접근을 통해 개인신용정보의 부당유출에 대한 통제 및 신용정보주체의 정보통제 권리를 현재보다 강화할 필요가 있다. 이를 위해서는 신용정보주체로 하여금 자신의 신용정보가 제공 · 활용되는 현황을 정확하게 알 수 있게 함은 물론, 제공 · 활용에 대해 적절하게 대응할 수 있는 권리를 부여해야 한다.

16) 이와 관련해 보험업감독규정 제4-39조 제2항 나목의 (2)에서는 금융기관 보험대리점 등의 금지행위로서 "적법한 절차 없이 보험계약자 등 제3자의 개인정보를 요구하는 행위"를 명시적으로 규정하고 있다.
17) 금융감독원 보험감독국에서는 이와 관련한 보도자료(2003. 8. 27.)를 통해 "보험청약서상의 정보는 보험사의 계약심사에 필요한 기초정보로서 그 소유권은 보험사에 있음"을 밝힌 바 있다.
18) 만일 신용도 판단 목적에 따른 제공 · 활용 동의에 대해 철회를 할 수 있도록 한다면 신용정보 인프라 구축에 역행할 뿐만 아니라, 미국 등

구체적인 방안으로는 첫째, 개인신용정보 제공 · 활용 동의서상 다소 모호하게 규정되어 있는 문구를 명확하게 적시할 필요가 있으며, 신용정보주체가 사후적으로 개인신용정보의 제공 · 활용 현황을 요청할 수 있도록 함으로써 자신의 정보에 대한 효과적인 통제가 가능하도록 해야 한다. 둘째, 신용정보의 열람방법 · 열람절차 · 열람요청대상 기관 등에 관한 내용을 안내함으로써 개인으로 하여금 자신에 대한 신용정보를 보다 쉽게 확인하고 개인정보에 대한 일상적인 관리가 이루어질 수 있게 해야 한다. 마지막으로 위법 또는 부당한 신용정보 제공 · 활용에 대해 제한적인 범위 내에서 정보제공 · 활용 동의 철회권을 부여하는 것도 고려해야 할 것이다. 즉, 신용정보주체가 상품안내 목적[18] 등에 대한 제공 · 활용에 동의를 했다 하더라도 위법 또는 부당한 제공 · 활용 사실이 있을 경우 해당 신용정보제공 · 이용자에 대해 동의 철회권을 행사할 수 있도록 함으로써 보다 실효성 있는 권리구제가 이루어질 수 있도록 해야 한다.[19]

(나) 신용정보관리제도의 개선 및 정보보호체계의 향상 도모

현재의 신용정보관리제도의 근간인 신용정보법을 CB사업의 출범 · 방카슈랑스 개시 등 새로운 금융 환경 변화에 맞게 보완해야 하며, 인터넷 대출이나 전화ARS대출시 개인신용정보제공 · 활용동의서를 받는 문제 등과 같이 금융기관의 다양한 영업 전략에 맞는 적절한 정보보호 장치나 기준을 마련해야 할 것이다.[20] 아울러, 신용정보와 관련한 대국민 홍보 및 교육을 강화해 신용정보주체가 신용사회의 한 일원으로 보다 능동적으로 자신의 신용상태를 관리 · 확인할 수 있도록 해야 한다.

2. 전자거래 등 부문에서의 개인정보보호 법제도

가. 전자거래기본법상의 개인정보보호

전자거래사업자는 전자거래이용자의 개인정보를 수집 · 이용 · 제공 및 관리함에 있어서 정보통신망이용촉진및정보보호등에관한법률 등 관련 규정을 준수하여야 하며, 전자거래사업자(정보처리시스템의 운영을 위탁받은 자를 포함한다)는 전자거래이용자의 영업비밀을 보호하기 위한 조치를 강구하여야 한다. 또한 전자거래이용자의 동의를 얻지 아니하고는 당해 이용자의 영업비밀을 타인에게 제공하거나 누설하지 못하도록 규정하고 있다(전자거래기본법 제12조제2항, 동법

선진국에서처럼 신용도 판단자료의 전무는 곧 금융거래불가라는 부작용을 낳을 수 있으므로 동의철회권 부여문제는 상품안내 목적 등을 위한 제공 · 활용에 한정하는 것이 바람직하다.

19) 미국에서는 공정신용보고법(FCRA : Fair Credit Reporting Act) §604(e)에 따라 소비자는 금융회사 등이 일정한 소비자를 대상으로 각종 상품정보를 제공하는 것(Target Marketing)에 대해 제공받는 소비자리스트에서 제외시켜줄 것을 요청할 수 있으며(Opt-out권), 요청시 2년 동안 리스트에서 제외된다.

제13조제2항, 제3항).

나. 전자상거래 등에서의 소비자보호에 관한법률

전자상거래를 행함에 있어서 소비자의 권익을 보호하고 전자거래 등의 신뢰도를 향상시키기 위하여 전자상거래소비자보호법은 사업자가 전자상거래 또는 통신판매를 위하여 소비자에 관한 정보를 수집 또는 이용(제3자에게 제공하는 경우를 포함한다. 이하 같다)하고자 하는 경우에는 정보통신망이용촉진및정보보호등에관한법률 등 관련 규정에 따라 소비자의 개인정보를 공정하게 수집 또는 이용하여야 한다고 규정하고 있다. 또한 사업자는 재화 등을 거래함에 있어서 소비자에 관한 정보가 도용되어 당해 소비자가 재산상의 손해가 발생하였거나 발생할 우려가 있는 특별한 사유가 있는 경우에는 본인 확인이나 피해의 회복 등 필요한 조치를 취할 의무를 부과하고 있다(전자상거래소비자보호법 제11조제1항, 제2항).

3. 의료부문에서의 개인정보보호 법제도

개인의 건강 상태에 관한 정보인 개인의료정보는 지극히 사적인 정보로서, 본인 이외의 사람에게 알려질 경우 해당 개인에게 매우 불리한 상황이 발생할 수 있다. 이에 따라 의료법 제19조(비밀누설의 금지)에 "의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료 · 조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다"고 규정되어 있는 바, 개인에 관한 의료정보는 환자 본인 이외의 사람들에게 알리지 않는 것이 원칙이다. 즉 개인의료정보는 특별한 사유가 없는 한 대규모로 수집 · 이용하는 것이 법적으로 금지되어 있다.

그러나 예외적으로 개인의료정보를 대량으로 보유 · 제공하는 경우가 있는데, 우선 개별 의료기관에서 진료 목적으로 진료를 받은 환자들의 정보를 보유하는 경우, 의료기관간 환자의 이송 등에 따라 타 의료기관에 정보를 제공하는 경우, 국민건강보험법에 의한 건강보험 청구를 위해 국민건강보험공단에 정보를 제공하고 공단에서 이를 보유하는 경우 등이 있다. 이 외에도 민 · 형사상의 사유로 법원이나 검 · 경찰에 정보를 제공하거나, 의학 연구 등을 위해 정보를 이용하는 경우 등이 있다.

20) 현재 신용정보법 제23조에서는 서면동의를 명시하고 있으므로 인터넷대출이나 전화ARS 대출시 개인신용정보제공 · 활용동의서를 받는 문제가 발생한다. 이와 관련해 금융감독원에서는 "인터넷대출의 경우 공인전자서명(공인전자인증서)을 제시하고 관련 법규에서 정한 동의서식에 따라 동의의사를 표시한 경우에 한하여 신용정보법에 따른 서면동의를 받은 볼 수 있으며, 전화ARS대출의 경우는 구두 동의의사를 확인하였다고 하더라도 별도의 서면동의를 받아야 한다"는 입장을 표명한 바 있다.

c o n t e n t s

제9장
스팸대응

제1절 스팸메일 규제 법 · 제도

법에서 규정하고 있는 아래의 의무사항을 위반하였다고 판단할 경우, 한국정보보호진흥원 불법스팸대응센터 (www.spamcop.or.kr, 02-405-4774) 에 신고하거나 상담을 의뢰할 수 있다

1. 스팸메일 규제 법 · 제도

가. 광고 전송시 명시할 사항(법률 제50조 제2항, 제3항)

(1) 이메일로 영리목적의 광고를 전송할 경우,

- 제목 앞에 "(광고)" 또는 "(성인광고)" 문구 및 제목 끝에 "@"를 표시해야 하며, 본문 란의 주요 내용을 제목으로 명시해야 한다.
- 또한 본문 안에는 전송자의 명칭/연락처 및 한글과 영문의 수신거부방법, 이메일 수집출처 등을 명시해야 한다.

☞ 위반시 3천만원 이하의 과태료 부과

※ (광@고) (광 고) (광.고) ('성인 광고') 같이 제목을 변칙 표기한 경우와 유니코드를 사용하여 문자를 조합한 경우 모두 과태료 대상임.

※ 광고수신에 동의를 받은 전송자의 경우, 위의 표시를 하지 않거나 "(동의)" 문구를 표시할 수 있으며, 이 때 본문란에 동의를 얻은 시기 및 내용을 구체적으로 명시해야 함.

(2) 사람이 직접 전화로 영리목적의 광고를 전송할 경우,

- 정보를 제공하기 전에 광고라는 사실을 먼저 밝혀야 한다.(전자상거래등에서의소비자보호에 관한법률 제13조제1항의 규정에 의한 광고 및 방문판매등에관한법률 제6조제3항의 규정에 의한 전화권유의 경우 예외)

☞ 위반시 3천만원 이하의 과태료 부과

(3) 휴대폰의 문자메시지로 영리목적의 광고를 전송할 경우,

- 광고할 내용 앞에 "(광고)" 또는 "(성인광고)" 문구를 표시해야 하며, 광고전송자의 명칭을 밝혀야 한다.
- 또한, 수신자가 비용을 들이지 않고 용이하게 수신거부를 할 수 있는 방법을 명시해야 한다. 다만, 수신자의 수신동의를 얻었을 경우에는 해당되지 않는다.

※ 수신거부방법으로 080을 이용한 무료전화를 제공할 경우, 광고 대상 지역을 모두 무료 전화 범위에 포함해야 함.
예시 : 광고 대상 지역이 서울로 한정되었을 경우, 080의 수신 지역을 서울로 한정 가능. 그러나 전국을 대상으로 할 경우 080의 수신 지역이 전국이 되어야 함.

(4) FAX로 영리목적의 광고를 전송할 경우,

- 광고할 내용 앞에 "(광고)" 또는 "(성인광고)" 문구를 표시해야 하며, 광고전송자의 명칭 및 주소를 밝혀야 한다.
- 또한, 수신자가 비용을 들이지 않고 용이하게 수신거부를 할 수 있는 방법을 명시해야 한다. 다만, 수신자의 수신동의를 얻었을 경우에는 해당되지 않는다.
  ☞ 위반시 3천만원 이하의 과태료 부과

※ 수신거부방법으로 080을 이용한 무료전화를 제공할 경우, 광고 대상 지역을 모두 무료 전화 범위에 포함해야 함.
예시 : 광고 대상 지역이 서울로 한정되었을 경우, 080의 수신 지역을 서울로 한정 가능. 그러나 전국을 대상으로 할 경우 080의 수신 지역이 전국이 되어야 함.

(5) 메신저(Messenger) 등 전자적 전송매체로 영리목적의 광고를 전송할 경우,

- 제목 앞에 "(광고)" 또는 "(성인광고)" 문구 및 제목 끝에 "@"를 표시해야 하며, 본문 란의 주요 내용을 제목으로 명시해야 한다.

※ 제목과 본문 구분이 어려운 경우, 광고내용을 시작하기 전에 "(광고)" 또는 "(성인광고)"를 표시하고 이어서 "@"를 표시할 수 있음.

- 또한 본문 안에는 전송자의 명칭/연락처 및 한글과 영문의 수신거부방법 등을 명시해야 한다.

나. "수신거부"와 관련한 의무사항(법률 제50조 제1항, 제4항, 제5항)

(1) 영리목적의 광고성 이메일, 전화, 팩스 등을 받고 싶지 않다는 의사를 밝힌 수신자에게 반복하여 광고를 전송해서는 안되며,

☞ 위반시 3천만원 이하의 과태료 부과

(2) 수신자가 수신거부의사를 밝히는 것을 방해하거나 회피하기 위해 기술적인 조치를 해서는 안된다.

☞ 위반시 1천만원 이하의 벌금(형사처벌) 부과

※ 기술적 조치의 예 : 이메일 발송시 메일내용안에 수신거부방법을 기재하지 않고 발송자 정보 및 전송경로 정보와 같은 헤더(header)정보를 위 · 변조하여 수신거부를 불가능하게 해놓는 경우

다. 청소년에게 청소년유해매체물 광고 금지(법률 제42조의2)

● 만 19세 미만의 청소년에게 이메일, 전화, 팩스, 휴대폰 SMS, 메신저 등을 이용하여 청소년유해매체물(청소년보호법에 따라 청소년보호위원회가 고시한 전기통신을 통한 음성정보 · 영상정보 및 문자정보) 광고를 전송해서는 안된다.

☞ 위반시 2년 이하의 징역 또는 1천만원 이하의 벌금 부과

청소년유해매체물 여부 확인 방법

● 청소년보호위원회가 제공하는 「유해매체물 검색」서비스 (http://www.youth.go.kr/environment/default_retrieval.htm)를 통하여 청소년유해매체물 여부 확인

● 확인방법 : 회원가입 ▶ 유해매체물 검색 DB 열람 ▶ 고시내용 확인

라. 수신자의 연락처 생성 및 수집 프로그램 사용 제한
(법률 제50조 제6항 및 제50조의2 제1항, 제2항)

(1) 불특정 다수의 전화번호 · 이메일주소, IP주소 등 수신자의 연락처를 자동으로 생성하는 프로그램을 사용하여 영리목적의 광고를 전송해서는 안된다.
☞ 위반시 1천만원 이하의 벌금(형사처벌) 부과

(2) 이메일주소 수집거부 의사를 밝힌 인터넷 홈페이지에서 이메일주소추출기와 같은 이메일주소 자동수집 프로그램을 이용하여 이메일주소를 수집하거나, 이렇게 수집된 이메일주소를 판매 · 유통해서는 안되며,
☞ 위반시 1천만원 이하의 벌금(형사처벌) 부과

(3) 이렇게 수집 · 판매 · 유통이 금지된 이메일주소임을 알고 이를 정보전송에 이용하는 행위도 금지된다.
☞ 위반시 1천만원 이하의 벌금(형사처벌) 부과

마. 광고성 프로그램 설치 제한(법률 제50조의5)

- 영리목적의 광고성 정보를 이용자의 컴퓨터에 자동으로 보이도록 하거나 개인정보를 수집하는 프로그램을 설치하고자 하는 사업자는 사전에 이에 대해 이용자의 동의를 얻어야 하며, 이용자에게 해당 프로그램의 용도와 삭제방법을 알려주어야 한다.
☞ 위반시 3천만원 이하의 과태료 부과

바. 광고 전송 대행시 유의사항(법률 제50조의3 제1항, 제2항)

- 영리목적의 광고성 이메일, 전화, 팩스의 전송을 외부 업체 등 제3자에게 위탁하여 대행할 경우 광고를 의뢰한 업체는 대행업체가 위법행위를 하지 않도록 관리 · 감독해야 하며, 대행업체가 법을 위반하여 이용자에게 손해가 발생한 경우 이에 대해 손해배상 책임을 져야 한다.

사. 정보통신서비스제공자의 스팸메일 차단권리(법률 제50조의4 제1항)

● 스팸메일로 인해 서비스 제공에 장애가 발생하거나 발생할 우려가 있는 경우 또는 이용자가 스팸메일 수신을 원하지 않을 경우, 정보통신서비스제공자는 스팸메일을 차단하는 조치를 취할 수 있다.

제2절 광고성 정보 송 · 수신시 유의사항

1. 광고성 정보 전송시

● 메일 제목란의 처음에 빈칸 없이 '(광고)' 또는 '(성인광고)' 라는 문구를 기재하여야 한다.

☞ **잘 표시한 예** : (광고) 창업!창업!부업!부업!
(성인광고) 성인동영상, 공짜로 다운로드 받으세요.
☞ **잘못 표시한 예** : 초기 사업자 모집! [광 고]
(廣告) 돈이 보이는 화끈한 쇼핑몰
(광-고) 월7만원에 쇼핑몰 창업!
(정보) 무료 프랜차이즈 신청
대출 안내서(홍보)

● 메일 제목은 메일을 열어보지 않아도 메일의 내용을 쉽게 알 수 있도록 기재하여야 한다.

☞ **잘 표시한 예** : (광고) 핸드폰 최저가 판매!
(광고) 트렌드 인기 화장품세트 공동구매
(광고) 100% 국비 무료 IT 교육
(성인광고) 성인동영상, 무료로 감상하실 수 있습니다

☞ **잘못 표시한 예** : (광고) 세상에는 이런 일도 있습니다
[부자까페] 성공할 준비 되셨습니까?
오빠, 나야 나
Re : 문의사항입니다
요청하신 자료입니다
민아... 아이디 보구 답장 줘...!
일생일대의 기회!

- 메일 내용 중에 수신자가 광고메일을 쉽게 수신거부할 수 있는 방법을 알리고 전송자의 명칭 및 연락처(전화번호 및 이메일 주소)를 명시하여야 한다.
- 메일의 발신자 및 전송경로를 숨기기 위한 어떠한 행위도 해서는 안된다.
- 광고메일 수신자들이 수신거부의사를 전달할 메일박스 용량 및 시스템을 정기적으로 점검하여 광고메일 수신자들의 수신거부의사 전달에 불편함이 없도록 한다.
- 1일 1회 이상 수신거부의사가 도착한 메일박스를 확인하여 수신거부의사를 밝힌 사람에게는 더 이상 광고메일이 전송되지 않도록 조치를 취해야 한다.
- 자사 광고메일 수신을 신청한 회원에게만 메일을 발송하고, 회원이 광고메일의 수신을 거부할 경우에는 즉시 메일링리스트(mailing list)에서 삭제해야 한다.
- 업무제휴 등을 이유로 제3자에게 자사 회원의 이메일 주소를 제공하고자 하는 경우에는 그 사실을 회원에게 정확히 고지하고 동의를 구해야 한다.
- 자사 웹사이트에서 이메일 주소가 추출되지 않도록 이메일 추출방지프로그램을 설치하거나 보안 게시판을 사용하는 등 필요한 기술적 조치를 강구해야 한다.

2. 광고성 정보 수신시

- 스팸메일 발송자의 특정 이메일 주소 및 아이피(IP), 도메인(Domain) 등을 수신거부하거나, 스팸메일 발송 릴레이 서버로 이용되지 않도록 메일서버환경을 설정한다. 불가피하게 릴레이를 허용한다면 IP를 한정지어서 설정하도록 한다.

※ 메일서버 릴레이 차단방법에 대해서는 "스팸릴레이 점검"에서 설명하고 있음

- 스팸을 자주 전송하는 메일서버 IP, 도메인네임, 이메일주소 등을 수신거부하도록 메일서버환경을 설정한다.
- 서버용 스팸메일 차단 프로그램을 사용하는 것도 좋다.
- 자체적인 스팸방지정책을 마련하여 자사 메일서버를 스팸전송에 이용할 경우 IP 차단 등 불이익을 줄 수 있음을 약관을 통해 고지한다.
- 스팸메일 관련 국내 · 외 민원 접수시 스팸메일 여부를 조사한 후 자사 정책에 따라 스팸메일 발송자에게 적극적으로 대처해야 한다.

제3절 스팸차단

1. 스팸릴레이 점검

여기서는 Sendmail 및 MS Exchange의 스팸릴레이 점검방법을 소개하고, 기타 메일서버에 대해서는 한국정보보호진흥원 내 인터넷침해사고대응지원센터에서 제공하는 "메일서버의 스팸릴레이 방지 설정 방법" (http://www.krcert.or.kr/paper/tr2002/tr2002_04/spam.htm) 참조

가. Sendmail

- Sendmail8.9.0부터는 디폴트로 메일 릴레이 기능을 제한하도록 되어 있으며 이러한 기능들을 제어하기 위한 많은 환경변수들을 제공한다.
- 환경변수들은 sendmail.cf파일에 저장되어 지는데, 많은 관리자들이 Sendmail 프로그램을 설치하는데 있어 가장 애로를 겪는 부분이다.
- Sendmail이 anti-spam 기능이 있다고 해도, 이 파일을 적절히 만들어 적용하지 못하면 무용지물이 되기 때문에 관리자들은 이 파일의 적용방법을 반드시 숙지하여 운영하여야 한다.
- Sendmail 8.9로 버전이 높아지면서 새롭게 추가된 기능이 바로 이 Anti-Spam과 관련된 기능이며 Access DB라는 새로운 데이터베이스를 도입해서 이것의 설정에 따라 특정 메일들을 받지 않도록 할 수가 있다.

● Access DB는 아래와 같다.

```
spam@hacker.com REJECT
spammail.com REJECT
useful.org OK
211.252.150 RELAY
211.252.151 RELAY
```

- 첫번째 필드는 이메일 주소, 도메인 네임, 인터넷 네트워크 주소등이 오게 되며, 두 번째 필드는 해당 주소로부터 오는 메일을 어떻게 처리할 것인가를 결정하는데 사용한다.
- 위의 예를 보면 spam@hacker.com 및 spammail.com 도메인으로부터 오는 모든메일은 거절하게 되고, useful.org 도메인으로부터 오는 모든 메일은 받아들이게 되며, 211.252.150, 211.252.151의 C-Class의 네트워크가 사용하는 모든 IP주소에 대하여 릴레이를 허용하게 된다.

● 위와 같은 형식의 access DB는 /etc/mail/access란 이름으로 파일 시스템에 저장되는데 Access 파일구조는 텍스트 파일이어서 Sendmail이 참조(Lookup)할 수가 없으므로, makemap이란 프로그램을 사용하여 Sendmail이 인식할 수 있는 DB 형태로 만들어 주어야 한다.

- 디렉토리를 /etc/mail로 옮긴 다음 "etc/mail/makemap dbm /etc/mail/access 〈 /etc/mail/access" 명령어를 실행하면, access.dir과 access.pag라는 이름으로 DB가 생성된다.
- /etc/mail/access 파일을 수정할 때마다 makemap을 사용해 새롭게 DB를 만들어주어야 한다.

● 버클리 DB를 이용한다면 약간 형식이 틀려지는데, 그럴 때는 다음과 같이 hash옵션을 사용하여야한다.

```
# /etc/mail/makemap hash /etc/mail/access 〈 /etc/mail/access
```

● 다음의 표는 이러한 access파일을 통하여 Sendmail이 참조할 수 있는 Access DB 파일을 생성하는 방법 및 과정을 보여준다.

```
[penguin:root]:/etc/mail〉 ls -al access*
-rw-r--r-- 1 root other 71 5월 3일 17:25 access
[penguin:root]:/etc/mail〉 cat access
spam@hacker.com REJECT
spammail.com REJECT
useful.org OK
172.16 RELAY

[penguin:root]:/etc/mail〉 makemap dbm /etc/mail/access 〈 /etc/mail/access
[penguin:root]:/etc/mail〉 ls -al access*
-rw-r--r-- 1 root other 71 5월 3일 17:25 access
-rw-r--r-- 1 root other 0 5월 3일 17:27 access.dir
-rw-r--r-- 1 root other 1024 5월 3일 17:27 access.pag

[penguin:root]:/etc/mail〉 cat access.pag
衆詳鳩픈RELAY172.16OKuseful.orgREJECTspammail.comREJECTspam @hacker.com
```

● 이러한 환경파라미터들의 상세한 내용에 대한 설정을 올바르게 사용하기 위해서는 cf/README 파일의 Anti-Spam 환경제어 부분을 참조한다.

- http://www.sendmail.org/tips/relaying.html
- http://www.sendmail.org/m4/anti-spam.html

● 대부분의 이러한 Anti-Spam Relay 솔루션들은 메일관리자가 허용되는 Relay 도메인들의 리스트들을 설정하는 것을 필요로 한다. 이 리스트에는 모든 허가 인증된 도메인들을 포함하고 있는지 반드시 확인하여야 하며 주의하여야 할 점은 반드시 MX (Mail Exchanger)뿐만 아니라 도메인에서 사용하고 있는 가상의 도메인들이 포함되도록 설정하여야 한다. 그렇지 않으면 여러분이 보낸 메일이 거절될 수도 있을 것이다.

- 메일 서버가 FEATURE(relay_entire_domain)을 사용해서 8.9.x버전 이상의 Sendmail을 구성하였다면, 이는 도메인 내에 있는 모든 호스트의 릴레이를 허용한다는 것을 의미한다. 만약 "relay_entire_domain"에 호스트명("host." : host.domain.com)을 사용한다면 디폴트로 Sendmail은 시스템에 있는 모든 IP주소를 체크해서 "reverse lookups"를 수행하여 메일서버의 시스템 부하를 가중시키게 될 것이다.

- Spam Relay의 가장 좋은 해결방법은 .cf파일을 포함하여 relay_ entire_domain을 사용하는 대신에 IP주소를 사용하여 Relay호스트를 설정하는 것이 설정상의 오류를 해결할 수 있는 좋은 방법이 될 수 있다.

나. 마이크로소프트 Exchange

(1) Exchange Server 메일 설정시 스팸릴레이 방지

스팸릴레이방지1
(그림 9-3-1)

① Exchange Server를 설치 후 맨 먼저 Microsoft Exchange Administor를 실행시켜 [File] ⇨ [New Other] ⇨ [Internet Mail service]를 선택한다.

스팸릴레이방지2
(그림 9-3-2)

② 인터넷 메일 서비스를 설치하기 전에 DNS(Domain Name Service)에 반드시 메일서버 관련 사항을 설정하라고 명시하고 있다.

스팸릴레이방지3
(그림 9-3-3)

③ IMS(Internet Mail Sevice)가 메일 메시지를 전송할 때 DNS를 이용해서 수신서버와 직접 연결할 것인지, 또는 메일을 relay 서버로만 보내고 최종 수신서버와 relay서버가 통신하도록 할 것인지를 지정하는 화면이다.

- 보통 Use Domain name system (DNS)...를 선택한다.
- Relay 서버를 이용하는 경우는 Route all mail through...를 선택한다.

스팸릴레이방지4
(그림 9-3-4)

④ 다음 설정은 송신주소를 제한하는 설정으로 첫 번째 기본 옵션을 선택한다. 다음은 SMTP 메일 어드레스의 뒷부분을 지정하는 화면이다. 기본적으로는 @site-name .serve-name으로 지정된다. SMTP(Simple Mail Transfer Protocol)메일은 @ 뒷부분의 DNS 명을 참조하여 서버와 연결을 시도하므로, @ 뒷부분은 DNS의 서버 이름이어야만 SMTP가 이 서버와 접속 할 수 있다. 대부분은 서버자신의 DNS 명이 될 것이다. (예 @mail.certcc.or.kr)

⑤ 다음은 인터넷 메일의 관리자용 메일박스에 대한 설정 및 이 서비스를 기동시킬 서비스 계정을 지정하는 화면이다.

스팸릴레이방지5
(그림 9-3-5)

(2) Exchange Server 메일 동작 확인방법

서비스 정상 동작여부 확인
(그림 9-3-6)

설치가 완료된 후 일단 서비스가 정상적으로 실행되었는지 **[시작]** ➪ **[제어판]** ➪ **[서비스]** 를 선택하여 'Microsoft Exchange Internet Mail Service' 가 시작되었는지 확인한다.

(3) 레지스트리 편집을 통한 스팸릴레이 방지

Exchange Server 5.5 SP1 이후 버전으로 업그레이드할 수 없는 경우에는 레지스트리 키를 추가하여 릴레이(Relay) 제한을 구성할 수 있다.

[시작] ➪ **[실행]**에서 "regedit"를 입력하여 아래의 키를 생성한다.

☞ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\MSExchangeIMC\Parameters

☞ RelayFlags, RelayDenyList, RelayAllowList, RelayLocalIPList 추가

① RelayFlags, REG_DWORD (이름, 데이터 유형)

릴레이 설정을 위한 레지스트리값 추가
(그림 9-3-7)

어떤 릴레이(Relay) 제어 규칙을 사용하는지 정의한다.

RelayFlags 비트 설정별 릴레이 정책

- RelayFlags가 비트 1로 세트(십진수 1)되고 클라이언트의 IP주소가 RelayDenyList의 주소와 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 없다.
- RelayFlags가 비트 2로 세트(십진수 2)되고 클라이언트의 IP주소가 RelayAllowList의 주소와 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있다.
- RelayFlags가 비트 3으로 세트(십진수 4)되고 클라이언트의 IP주소가 RelayLocalList 의 주소와 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있다.
- RelayFlags가 비트 4로 세트(십진수 8)되고 클라이언트가 인증을 얻는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있다.

② RelayDenyList, REG_MULTI_SZ

서버를 통해 메시지를 릴레이(Relay)할 수 없는 호스트의 IP주소를 설정한다

- RelayDenyList, RelayAllowList 및 RelayLocalIPList의 각 행(Line)은 두 부분, 즉 세미콜론(;)으로 분리된 네트워크 주소 및 마스크로 이루어진다. 예를 들면, 192.168.0.0;255.255.0.0인 경우 주소는 192.168.0.0, 마스크는 255.255.0.0이다. 마스크가 생략되면 기본값 255.255.255.255가 사용된다.

※ 데이터 유형중 하나인 REG_MULTI_SZ는 일반 regedit를 사용치 않고 regedt32를 이용하여 값을 추가하여야 한다. 그리고 Regedt32에서 제공하는 복수 문자열 편집기를 이용하여 작업을 하여야 한다.

③ RelayAllowList, REG_MULTI_SZ

메일서버를 통해 메시지를 릴레이(Relay)할 수 있는 호스트 IP주소를 설정한다.

④ RelayLocalIPList, REG_MULTI_SZ

SMTP 서비스를 사용할 IP주소와 메일을 릴레이(Relay)할 수 있는 서버의 로컬 IP주소를 지정한다. 이것은 내부 및 외부 인터페이스가 있는 다중 홈 서버(Multi-homed Server)에 유용하다. IP 전달을 설정하면 이 기능을 사용할 수 없다.

자세한 사항은 아래의 문서를 참조한다.

☞ http://support.microsoft.com/default.aspx?scid=%2Fisapi%2Fgomscom%2Easp%3Ftarget%3D%2Fkorea%2Fsupport%2Fxmlkb%2Fkr193922%2Easp&LN=KO

(4) Exchange Server 보안패치 방법

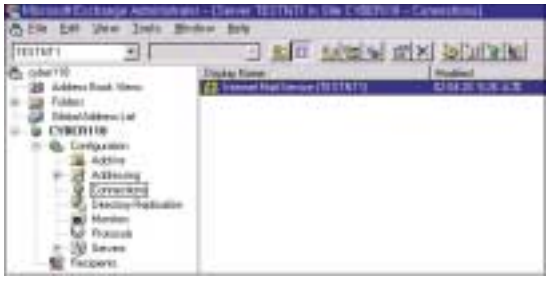
① Exchange Server 5.5의 SP1이나 이후 버전의 서비스 팩을 설치한다. 아래의 사이트로 이동하여 최신 SP1을 다운받는다.

서비스팩 다운로드 사이트
(그림 9-3-8)

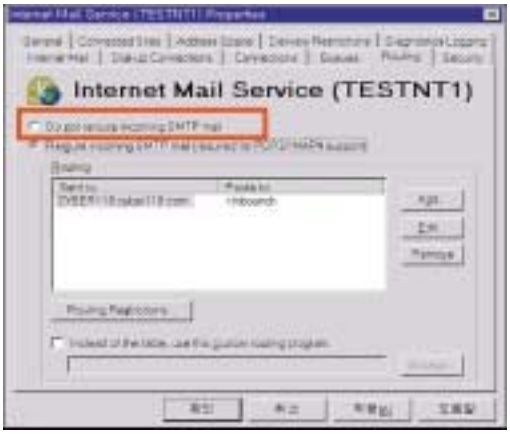
※ 다운로드 사이트 : http://www.microsoft.com/exchange/downloads/

② Exchange Server Administrator 프로그램에서 Connections에서Internet Mail Servece를 더블 클릭한다.

Exchange Administrator Menu
(그림 9-3-9)



③ Internet Mail Servece Properties에서 Routing탭을 선택한다.



Internet Mail Servece Properties 메뉴
(그림 9-3-10)

스팸릴레이를 허용하지 않으려면 "Do not reroute incoming SMTP mail"를 체크한다.
특정 클라이언트에서만 릴레이를 허용하기 위해서는 "Reroute incoming SMTP mail" 을 선택한 다음 "Routing Restrictions"을 선택하여야 한다.

Routing Restrictions
(그림 9-3-11)

④ "Host and clients that successfully Authenticate" 옵션은 메일 서버의 인증을 받은 호스트 또는 클라이언트의 릴레이를 허용하는 설정부분이다.

⑤ "Hosts and clients with these IP address" 옵션은 릴레이를 허용할 호스트와 클라이언트의 IP를 지정하는 부분으로 IP 입력 후 Add를 누른다.

⑥ "Hosts and clients with these internal address" 옵션은 릴레이를 서로 허용할 메일서버의 내부 IP를 지정하는 부분으로 IP 입력 후 Add를 누른다.

※ 이 옵션은 다수의 메일서버를 사용할 때에 한해 적용 가능한 옵션이다.

⑦ "Specify the hosts and Clients that can NEVER route mail" 옵션은 메일이 전달되지 않을 IP대역을 입력하는 부분으로 IP입력 후Add를 누른다.

⑧ 설정을 수정한 후 서비스를 중지 후 재시작하여야 변경내용이 적용된다.

2. 스팸발송 악성 프로그램 제거 및 예방

일반 사용자의 PC에 악성프로그램 설치를 유도하고, 이 악성 프로그램이 설치된 사용자의 PC에서 직접 스팸성 광고 메일을 발송하는 새로운 형태의 스팸메일이 유포되고 있다. 아래의 방법을 통해 스팸발송 악성 프로그램이 설치되어 있는지를 확인, 제거, 예방할 수 있다.

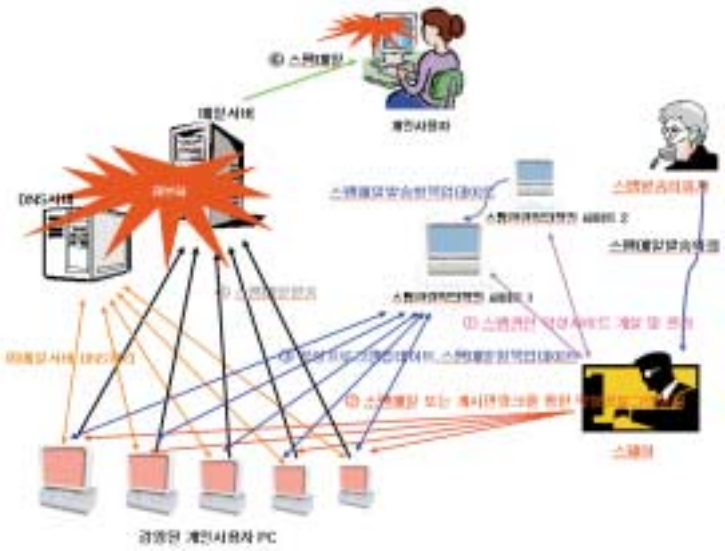
가. 확인방법

이 악성프로그램은 스팸메일을 발송하는 횟수가 많지 않아 시스템에 부하를 주지 않고 백도어가 설치되지 않아 사용자가 감염사실을 알기 어렵지만 시스템 부팅 후 메일 관련 프로그램(아웃룩 익스프레스, 기타 메일발송프로그램)을 구동하지 않은 상태에서 25번 포트의 접속여부로 감염유무를 파악할 수 있다. 시스템 시작 후 (그림 6-1)과 같이 netstat -na 명령을 사용하여 네트워크 연결상태를 확인해 보면 감염된 시스템은 외부IP주소(Foreign Address)쪽에 스팸메일을 보내고자

하는 메일서버의 25번 포트로 접속하고 있는 것을 확인할 수 있다.

악성프로그램의 확인방법
(그림 9-3-12)

나. 스팸 발생경로



스팸 발생 경로
(그림 9-3-13)

① 스패머에 의한 스팸숙주로 사용하기 위한 사이트를 개설한다.

② 스팸메일 또는 게시판링크를 통해 일반사용자가 악성프로그램을 다운로드를 받게된다.

악성프로그램이 링크된 메일이나 게시판의 글을 열람시 아래와 같은 컨트롤러를 다운받는 창이 뜨고 사용자가 (무의식적으로) 예(Y)를 클릭하면 악성프로그램이 설치될 수 있다.

악성프로그램의 다운로드
(그림 9-3-14)

악성프로그램 설치시 설치되는 요소들

- ActiveX 컨트롤러
- 실행파일 및 설정파일
- 리부팅 후 자동 재시작을 위하여 실행파일 레지스트리에 등록

③ 악성프로그램 관련프로그램 다운로드

실행 후 숙주서버로부터 악성프로그램 설정 파일 다운로드 및 업데이트되며, 숙주서버에서 발송할 스팸항목을 받아온다.

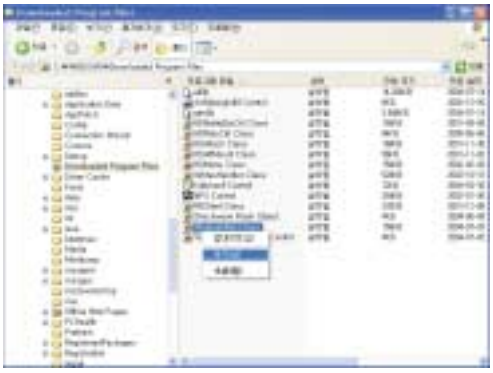
④ 받는 사람 메일주소의 메일서버 DNS 쿼리 및 메일서버에 접속

메일서버의 거부에도 불구하고 계속적으로 DNS쿼리 및 스팸발송을 계속적으로 시도로 DNS서버 및 메일서버 과부하 원인이 된다.

⑤ 스팸메일 발송

다. 제거방법

● ActiveX 컨트롤러



ActiveX 컨트롤러의 제거방법
(그림 9-3-15)

- 탐색기를 실행하여 C:\winnt(또는 windows)\Downloaded Program Files 경로로 이동한다. 이 폴더는 일반적으로 인증관련 콘트롤러가 저장되는 디렉토리로 주로 은행이나 신용기관 등의 인증과정을 거쳐서 로그인이 되는 사이트의 Control 프로그램이나 프로그램 업로드 및 다운로드에 대한 승인 및 인증 프로그램을 필요로 하는 업체(웹하드, 게임사이트, 인터넷공유 사이트)의 Control 프로그램들이 다운로드 되어 있다.

- 여기서 설치된 control을 더블클릭하면 상세 정보를 얻을 수 있기 때문에 최근에 설치되었거나 알 수 없는 ActiveX Component를 찾아 제거한다. 이 폴더에 있는 프로그램들은 해당 프로그램을 운영하는 사이트에 접속할 때 검사하여 관련된 파일이 없으면 자동으로 다운로드하여 사용하므로 백업 할 필요는 없다. 그러므로 의심이 가는 파일은 삭제하는 것이 안전하다.

● 실행파일 및 설정파일

[표 9-3-1] 실행파일 및 설정파일

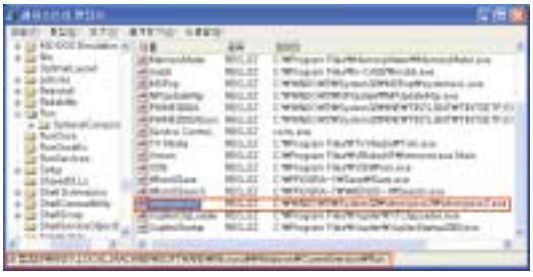
파일명	설치경로	역 할
winmgrsvc2.cab, (sysdbmsmgr.cab, IMG.cab,IMG2.cab)	숙주서버에 있는 악성파일의 원본(변종)	개인PC에서 다운로드되어 압축이 풀리면서 설치됨
InstallGhostMail Control	C:\WINDOWS\Downloaded Program Files\	악성프로그램 설치구성정보, 업데이트 정보, 스팸발송 항목을 원격에서 가져오는 역할
winmgrsvc2.exe (sysdbmsmgr.exe)	C://windows/system32/winmgrsvc2/ (C://windows/system32)	smtp엔진 (백도어 포트 없음)
config.cfg	상동	악성프로그램정보, 메일전송 데이터, 메일발송주기설정파일
sended_count.cfg	상동	스팸 발송횟수 카운트파일
update.cfg	상동	악성프로그램의 업데이트정보
Test.html	숙주서버에서 수집	실행시 악성프로그램을 다운받게 하는 파일

- 해당 경로로 이동한 후 DEL키를 눌러 삭제하면 된다. 악성프로그램을 삭제시 지울 수 없다는 경고 창이 뜰 경우 현재 해당 악성프로그램이 실행되고 있으므로 현재 실행중인 해당 프로세스를 찾아서 프로세스(실행중인 프로그램)를 끝낸 후 삭제하여야 한다.
  - 윈도우즈 98인 경우에는 Ctrl+Alt+Del키를 동시에 한번 누른 후 실행중인 프로그램 창에서 현재 실행되고 있는 프로그램 중 악성프로 그램과 관련된 프로세스를 먼저 종료시킨 후 제거한다.
  - 윈도우 2000/XP인 경우 Ctrl+Alt+Del키를 동시에 한번 눌러 작업관리자를 실행시킨 후 프로세스 탭에서 실행중인 프로세스 중에서 해당 악성프로그램을 선택한 후 아래의 "프로세스 끝내기"를 클릭 하여 프로세스를 종료시킨 후 삭제한다.

● 재시작 후 프로그램 자동 재시작을 위한 레지스트리 등록

☞HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 에 키 값을 등록("winmgrsvc2 C://windows/system32/winmgrsvc2/winmgrsvc2.exe")

※ 이 키는 악성프로그램이나 바이러스가 주로 변경시키는 레지스트리 키이므로 백업해 두거나 항상 확인하여 변경 유무를 확인하여 악성프로그램에 대비하여야 한다.



자동시작을 위한 레지스트리 등록
(그림 9-3-16)

- 제거방법 : 해당 레지스트리 이름을 클릭후 Delete키를 눌러 삭제한다.

※ 레지스트리를 잘못 삭제 후에는 문제가 발생할 수 있으므로 편집할 레지스트리 키를 우선 백업 한 후 해당 레지스트리를 편집

※ 참고: KRCERT홈페이지(http://www.krcert.or.kr)의 [보안문서] - [사고노트] - [2002년] "악성스크립트를 이용한 특정사이트 접속유도"

라. 예방 방법

- 인터넷 보안수준 설정은 **[인터넷 익스플로러 메뉴]** ⇨ **[도구]** ⇨ **[인터넷 옵션]** ⇨ **[보안]**에서 기본수준 이상으로 설정한다.
- 광고성 스팸메일이나 게시판의 글을 클릭 하여 알 수 없는 사이트의 프로그램을 다운받는 창이 뜰 때에는 절대 확인이나 "예"를 누르지 말고 "아니오"를 선택하여 악성프로그램이 설치되지 않게 한다.
- 윈도우즈 취약점을 이용한 악성프로그램이 배포될 것에 대비하여 항상 윈도우즈를 최신버전으로 업데이트 한다.
- 현재 일부 스팸메일 발송 악성 프로그램은 백신으로 탐지가 가능하므로 주기적으로 최신으로 업데이트 하여 시스템을 점검한다.

c o n t e n t s

제10장
불건전정보유통 예방

제 1 절 개요

국내 정보통신서비스산업은 1990년대 후반부터 정보통신 이용환경이 PC통신에서 인터넷으로 변화하기 시작하면서 포털(Portal), 채팅, ISP(Internet Service Provider) 및 성인정보제공 사업자 등 다양한 정보통신서비스제공 사업자가 성장하기 시작하였다. 이와 함께 정보통신서비스제공 이용자는 급격히 증가하기 시작하였고, 정보화 순기능과 더불어 역기능이 점차 사회적으로 문제시됨에 따라 공적 규제와 함께 민간영역에서의 자율규제활동의 필요성이 대두되기 시작하였다. 이는 인터넷환경의 개방성 · 가변성 · 커뮤니케이션의 쌍방향성 등의 특성에 기인한 것으로, 기존의 공중파 방송매체처럼 공적 규제만으로는 정보건전화를 위한 규제의 실효성을 달성하기 어렵기 때문이다. 사업자 자율규제활동은 유럽, 미국 등의 예에서 볼 수 있듯이, 사업자 또는 사업자 단체가 핫라인(Hotline)을 구축하여 신고 · 처리시스템을 운영하거나, 행동강령 또는 약관 제정, 자체모니터링 및 신고센터 운영, 캠페인 등 사업자 스스로 정보건전화를 위한 다양한 활동을 추진하는 것이라 할 수 있다.

따라서, 사업자는 불건전정보(불법 · 청소년유해정보)의 개념 및 유통의 폐해를 정확히 이해하고, 불건전정보 유통에 따른 청소년보호방안 등을 강구하여야 할 것이다.

1. 불건전정보(불법 · 청소년유해정보)의 정의

불건전정보라 함은 건전하지 않은 정보를 의미하며, 누군가 실명 또는 익명으로 음란, 명예훼손, 자살, 살인청부, 폭탄제조, 불법다단계판매, 도박, 지적재산권 침해 등 각종 법률상 금지행위 위반 정보 등이 이에 해당한다. 이러한 불건전정보가 웹사이트 게시판에 공개된 경우 그 내용은 빠른 시간내 불특정 다수인에게 전파되어 사실에 대한 진위여부와 관계없이 정치적, 사회적, 도덕적으로 큰 타격을 입게 된다.

'불건전' 의 의미

'불건전' 이라는 단어의 사전적 의미는 신체나 정신이 튼튼하지 않고 온전하지 않거나 조직 따위의 활동이나 상태가 건실하지 않고 비정상적인 것이라는 사실을 인용할 때, 불건전정보는 사람의 신체나 정신을 온전하게 유지시키지 못하게 하는 정도의 비정상적인 정보라고 할 수 있음.

불건전정보는 흔히 불법정보, 유해정보 혹은 불건전정보, 불법 · 청소년유해정보라는 단어를 혼용하여 제각각 사용하고 있기도 함.

가. 불법정보

불법정보라 함은 현행법에 저촉되는 정보로서, 그 유통이 금지되어 있는 정보를 말한다. 형법 등 각종 금지규범은 해서는 안되는 여러 가지 범죄유형을 규정하여 이를 규제하고 있는데 특히 인터넷상의 정보가 이러한 형법 등 금지규범에 저촉되는 경우에 이를 불법정보라고 할 것이다.
예를 들어, 국가의 안전 자체를 위협하는 정보, 타인을 비방할 목적으로 사실 또는 허위의 적시하여 명예를 훼손하는 정보, 음란한 정보 등 법과 질서의 존엄성을 해하는 정보들이 그것이다.

[표 10-1-1] 전기통신사업법 제53조상 불법정보의 개념

제53조 제1항	내 용	조문표현
제1호	음란한 전기통신	음란한 부호 · 문언 · 음향 · 화상 또는 영상을 배포 · 판매 · 임대하거나 공연히 전시하는 내용의 전기통신
제2호	명예훼손	사람을 비방할 목적으로 공연히 사실 또는 허위의 사실을 적시하여 타인의 명예를 훼손하는 내용의 전기통신
제3호	사이버스토킹	공포심이나 불안감을 유발하는 부호 · 문언 · 음향 · 화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 내용의 전기통신
제4호	해킹, 바이러스 유포	정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손 · 멸실 · 변경 · 위조 하거나 그 운용을 방해하는 내용의 전기통신
제5호	청소년유해매체물 표시의무위반	청소년보호법에 의한 청소년유해매체물로서 상대방의 연령확인, 표시의무 등 법령에 의한 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 전기통신
제6호	도박 등 사행행위	법령에 의하여 금지되는 사행행위에 해당하는 내용의 전기통신
제7호	국가기밀누설	법령에 의하여 분류된 비밀 등 국가기밀을 누설하는 내용의 전기통신
제8호	국가보안법 위반	국가보안법에서 금지하는 행위를 수행하는 내용의 전기통신
제9호	범죄관련정보	범죄를 목적으로 하거나 교사 또는 방조하는 내용의 전기통신

나. 청소년유해정보

청소년유해정보는 넓은 의미에서는 정보통신망을 통해 유통되는 정보 중 청소년에게 유해에 정보를 말하며, 좁은 의미에서는 정보통신윤리위원회와 청소년보호위원회가 청소년유해매체물로 결정 · 고시한 음란성, 폭력성, 사행성, 반사회성을 띄는 영리 · 비영리 정보를 말한다. 이러한 청소년유해정보에는 청소년에게 성적욕구나 폭악성을 불러일으키는 정보, 반사회적, 비윤리적인 것으로 청소년의 정신적 · 신체적 건강에 해를 끼칠 수 있는 정보를 포함하며(청소년보호법 제10조), 청소년유해성의 판단은 전문적 심의기구인 정보통신윤리위원회가 정보통신망을 통해 유통되는 음성 · 영상 · 문자정보에 대한 사후심의를 통해 결정하고 있다(청소년보호법 제7조, 제8조).

※ '음성' : 신음소리, 괴성 등의 소리(음란게시글, 음란소설 등), '영상' : 그림화면, 사진과 같은 정지화상 및 동영상 (사진, 그림, 만화, 애플릿 등), '문자' : 글자나 문장

[표 10-1-2] 청소년보호법상의 기본개념

개 념	내 용
청소년	◈ 만19세 미만의 자를 말함. 다만, 만19세에 도달하는 해의 1월 1일을 맞이한 자는 제외함(청소년보호법 제2조제1호). 예를 들어, 2003년도의 경우 1985년 1월 1일생부터 보호대상 청소년에 해당함(태어난 해를 기준으로 하는 '연 나이 제도' 임)
청소년유해매체물	◈ 청소년보호법 제8조 및 제12조의 규정에 의하여 청소년보호위원회 또는 정보통신윤리위원회 등 각 심의기관이이 청소년에게 유해한 것으로 의결 또는 결정하거나, 제12조의 규정에 의하여 청소년에게 유해하다고 확인하여 청소년보호위원회가 고시한 매체물 ◈ 청소년보호법 제12조제6항에 따라 매체물의 제작 · 발행자, 유통행위자 또는 매체물과 관련된 단체가 자율적으로 청소년유해표시 또는 포장을 한 매체물 중 청소년보호위원회 또는 정보통신윤리위원회 등 각 심의기관의 청소년유해매체물 최종결정이 있기 전까지의 매체물
청소년유해정보 적용범위	◈ 전기통신사업법 및 전기통신기본법의 규정에 의한 전기통신을 통한 음성정보 · 영상정보 및 문자정보(청소년보호법 제7조제4호)

다. 정보통신윤리심의규정상의 불건전정보

불건전정보의 개념을 종합적으로 정리할 수 있는 정보통신윤리심의규정상의 불법 · 청소년유해정보의 개념을 살펴보고자 한다.

(1) 헌법에 위배되거나 국가의 존립을 해하는 등의 정보

"헌법에 위배되거나 국가의 존립을 해하는 등의 정보"라 함은 자유민주적 기본질서, 기본적 인권의 존중, 권력분립, 의회제도, 복수정당제도, 선거제도, 사유재산과 시장경제를 골간으로 한 경제질서 및 사법권의 독립 등을 규정하는 등 국가의 통치구조 및 운영, 국민의 기본적 권리와 의무를 규율하는 최고근본법규인 헌법에 위배되거나 국가의 존립 · 안전에 실질적 해악을 줄 명백한 위험성이 있는 경우를 말한다.

구체적 위반 형태
i) 국가의 존립을 위협 · 침해하거나 국가기관을 전복 · 파괴 · 마비시킬 우려가 현저한 정보
ii) 헌법 및 자유 민주적 기본질서를 현저히 부정하거나 비방하는 정보
iii) 헌법에 반하여 역사적 사실을 현저히 왜곡하는 정보
iv) 국제간의 우의를 훼손할 우려가 현저한 정보

(2) '범죄 기타 사회질서 위반' 정보

일반적인 범죄를 목적으로 하거나 교사 또는 방조하는 등 범죄 기타 사회질서 위반행위에 관련된 내용의 정보는 유통이 적합하지 아니한 정보로서 간주되고 있다.

구체적 위반 형태
i) 범죄를 목적으로 하거나, 그 수단이나 방법 또는 결과를 구체적으로 묘사하는 정보
ii) 범죄를 미화하거나 정당한 수단 또는 방법으로 보이게 하는 정보
iii) 범죄를 예비하거나 교사 · 방조하거나 선전 · 선동할 우려가 현저한 정보
iv) 기타 반사회적 행위를 묘사하여 건전한 사회질서를 현저히 해하는 정보

(3) '선량한 풍속 저해' 정보

'선량한 풍속 저해' 정보로는 ①성적인 욕구를 자극하거나 정상적인 성적 수치심을 해하여 일반인의 공분(公憤)을 일으킬 우려가 있는 정보, ②폭력성 · 잔혹성 · 혐오성 등이 심각한 정보, ③사회통합을 저해하는 정보, ④타인의 권리를 침해하는 정보, ⑤기타 패륜적 · 반인륜적 행위를 묘사하여 사회의 선량한 풍속을 현저히 저해하는 정보 등이 있다.

● 성적인 욕구를 자극하거나 정상적인 성적 수치심을 해하여 일반인의 공분(公憤)을 일으킬 우려가 있는 정보

구체적 위반 형태
i) 남녀의 성기, 국부, 음모 또는 항문(이하 "남녀의 성기 등" 이라 한다)이 구체적으로 묘사되는 내용
ii) 성행위를 현저하게 노골적으로 묘사한 내용
iii) 항문성교, 구강성교, 성기애무 등을 구체적 · 사실적으로 묘사한 내용
iv) 남녀의 성기 등에 대한 자위행위를 직접적이고 구체적으로 묘사하는 내용
v) 성행위와 관련된 기성 등 신음소리를 극히 자극적으로 묘사된 내용
vi) 수간, 시간(屍姦), 혼음, 근친상간, 가학성 · 피학성 음란증, 관음증 등 변태적 성행위를 구체적으로 묘사한 내용
vii) 매춘 등 성매매를 권유, 유도, 조장, 방조하는 내용
viii) 아동 또는 청소년을 성적 유희의 대상으로 직접적이고 구체적으로 묘사한 내용
ix) 성적 표현을 통하여 성적 유희의 대상을 찾거나 이를 매개하는 내용 등의 정보

● 폭력성 · 잔혹성 · 혐오성 등이 심각한 정보

구체적 위반 형태
i) 강간, 윤간, 성고문 등 성폭력행위를 묘사하여 성적굴욕감 또는 혐오감을 불러일으키는 내용
ii) 존속, 노인, 스승에 대한 살상, 폭행, 협박, 학대 행위 등을 구체적으로 묘사하는 내용
iii) 본인, 아동, 부녀, 장애인 등에 대한 살상, 폭행, 협박, 학대 행위 등을 구체적으로 묘사하는 내용
iv) 구토 · 방뇨 · 배설시의 오물, 정액 · 여성생리분비물 등을 구체적 · 사실적으로 묘사하여 혐오감을 불러일으키는 내용
v) 낙태, 절개 · 절단, 수술장면 등 의료행위를 지나치게 상세히 표현하여 혐오감을 불러일으키는 내용
vi) 출산상황을 지나치게 흥미위주로 묘사하여 혐오감을 불러일으키는 내용
vii) 욕설, 성기명칭 등 노골적인 성적 표현으로 굴욕감 내지 불쾌감을 불러일으키는 내용
viii) 기타 육체적 · 정신적 고통, 살상, 사체 등을 사실적 · 구체적으로 표현하여 잔혹 또는 혐오감을 주는 내용 등의 정보

● 사회통합을 저해하는 정보

구체적 위반 형태
i) 도박 등 사행심을 조장하는 내용 ii) 학교교육 등 교육을 왜곡하여 현저히 교육기풍을 해하는 내용 iii) 합리적 이유없이 성별, 종교, 장애, 연령, 사회적 신분, 인종, 지역, 직업 등을 차별하거나 이에 대한 편견을 조장하는 내용 등의 정보

● 타인의 권리를 침해하는 정보

구체적 위반 형태
i) 사생활의 비밀과 자유를 침해할 우려가 현저한 내용, 초상권 등 인격권을 현저히 침해하는 내용 ii) 정당한 권한없이 저작권 등 지적재산권을 침해하거나 이를 매개하는 내용 등의 정보

● 기타 패륜적 · 반인륜적 행위를 묘사하여 사회의 선량한 풍속을 현저히 저해하는 정보

(4) 불법 · 청소년유해정보를 배포 · 판매 · 임대 등을 하거나 공연히 전시 또는 전송을 할 목적으로 매개 · 광고 · 선전 등을 하는 내용의 정보(광고성정보)

인터넷상의 선정적 · 사행적 배너광고 및 무차별적인 광고성 메일발송 등은 이미 모든 정보이용자 및 학부모들로부터 극도의 불만이 표출된 상태이며, 정보이용자 및 학부모에게 정신적 충격이나 이를 제거하기 위한 사회 · 경제적 비용을 야기시켰다. 따라서 이러한 불법 · 청소년유해정보를 배포 · 판매 · 임대 등을 하거나 공연히 전시 또는 전송을 할 목적으로 매개 · 광고 · 선전 등을 하는 내용의 정보에 대하여 강한 규제가 필요할 것이다.

2. 불건전정보의 유통

가. 불건전정보 유통의 특성

사이버공간의 불건전정보는 정보통신기술을 기반으로 유통되기 때문에 기본적으로 정보통신기술을 통한 정보유통의 특성을 그대로 반영하고 있다. 이러한 특성이 사이버상의 불건전정보 유통의 가능성을 높이고 그 폐해를 보다 심각하게 하고 있다. 즉, 인터넷의 기술의 보급과 확산은 순기능적인 측면에서 기여한 바가 크지만, 음란 · 폭력콘텐츠 등 불건전정보의 유통, 사이버공간을 통한 인권침해, 사이버 중독으로 인한 현실공간에서의 혼란 등 사회적 문제를 크게 증가시켰으며, 인터넷의 익명성, 개방성 등을 악용하는 사례가 빈번하게 발생하고 있고, 인터넷에서 급격한 불건전정보의 상업화 추세와 연계되면서 건전한 정보이용 활성화를 저해하고 있다.

현대사회를 '정보사회' 라고 할 정도로 오늘날은 정보의 대량 · 신속한 유통과 정보의 공개원칙을 매개로 개방적이고 참여지향적인 지배체제를 형성할 수 있는 토대가 마련되어 있으며, 인터넷은 정보사회의 기반구조를 이루는 핵심요소인 것이다. 특히, 전기통신을 이용하는 인터넷 등 뉴미디어상의 정보의 경우 인터넷상의 정보유통의 특성으로 인하여, 정보이용자인 개인의 정보통제권이 강화됨으로써 공동체의 운영에 개인이 손쉽게 참여할 수 있는 등 순기능적인 측면이 있으나, 인터넷상의 표현의 자유를 절대적 · 무제한적으로 인정하는 경우, 그 역기능적인 측면에 있어 타인에 대한 명예훼손 또는 사생활침해, 청소년의 음란정보에의 노출 등의 문제점이 날로 심각해지고 있다.

인터넷상의 정보유통 특성

① 시 · 공간적 무제한성 : 시간적 · 장소적 제한을 받지 않는다.
② 익명성 : 정보이용 및 유통자의 신원을 확인하기 어렵다.
③ 쌍방향성 : 누구나 간편히 정보를 인지 또는 제공할 수 있다.
④ 신속 전파성 : 정보유통 및 복제가 신속 · 용이하다.
⑤ 비국경성 : 정보유통에 있어서 특정국가영역이라는 지역적 제한을 받지 않는다.

즉, 음란, 명예훼손, 프라이버시침해, 저작권침해, 인종차별 · 성차별 등 불법 · 청소년유해정보가 인터넷을 통해 국경을 넘어 유통 · 범람함으로써 오늘날 인터넷상의 이러한 표현과 관련된 법적 분쟁과 사건이 표면화되고 있으며, 그 폐해는 극도로 심각하다. 특히, 정신적 · 신체적 형성단계에 있는 청소년에게 미치는 악영향이 지대할 뿐만 아니라, 청소년이 온라인 · 오프라인상의 범죄행위주체로까지 이어지고 있어 그 심각성이 증폭되고 있다.

나. 불건전정보 유통 실태 및 경향

(1) 음란정보의 유통

불건전정보의 대표적인 예로는 음란한 정보가 있을 수 있다. 음란한 정보는 성을 흥미중심으로 선정적으로 왜곡해서 전달하는 성에 관한 잘못된 정보이다. 즉, 음란한 정보라 함은 일반인의 정상적인 성적 수치심과 선량한 성적 도의관념에 반하는 정보를 가리킨다. 이러한 음란한 정보는 성에 대해 잘못된 견해를 가지게 만들며, 나아가 개인 각자가 자신의 성에 대해 가져야만 하는 사회적 책임에 무관심하게 만들어서 성범죄를 저지르게 하거나 아니면 그 자신이 성범죄의 피해자가 되게 하며, 전반적으로 사회의 성도덕을 타락시킨다.

이러한 음란정보를 불법 제작하여 인터넷 웹사이트를 개설하거나 이메일, 모바일, 커뮤니티 사이트 등 정보통신을 활용하여 불법적으로 배포 · 판매하거나 음란한 화상 또는 영상물을 이용자에게 전송하는 행위는 금지되어 있음에도 불구하고, 이제 인터넷을 이용한 음란정보의 유통으로 인한 폐해는 더 이상 간과하여서는 아니 될 정도로 사회 전반적으로 큰 문제가 되었다.

문자, 영상, 음란동영상, 음란게임, 음란채팅, 음란사이트 배너광고, 음란물 판매광고 등이 전자게시판, 이메일, 웹사이트, 모바일, 위성통신 등을 통하여 급속히 전파되고 있다. 이러한 음란정보는 성인뿐만 아니라 10세 안팎의 어린이나 청소년에게도 무분별하게 유통되고 있고, 심지어 음란 홈페이지를 초등학생이나 중학생 등의 미성년자가 직접 유료로 운영하는 사례도 있다. 과거 현실세계에서 은밀하게 유통되던 음란영화나 사진들이 인터넷상에서 공개적이라 할 수 있을 만큼 널리 퍼져 있다.

성에 대하여 흥미가 생기는 시기인 초 · 중 · 고등학생 시기에 음란정보를 통해 처음부터 성에 대해 잘못된 지식을 얻게 되는 경우, 이에 대한 후유증은 이후 성인이 된 이후까지도 지속되는 경우가 많다. 이렇게 되면 성인이 된 이후에도 성에 대한 잘못된 정보와 편견 때문에 행복한 가정생활을 만들어 가지 못할 뿐만 아니라 사회의 성도덕을 타락시켜서 심각한 사회문제를 낳기도 한다. 따라서 성에 관련된 잘못된 정보를 제공하는 음란정보는 개인과 사회 모두에 상당히 심각한 피해를 입히게 된다.

이처럼 개인의 생활과 사회에 심각한 영향을 끼치는 음란정보가 최근 들어 눈부시게 발전하고 있는 정보통신 기술로 더욱 심각하게 증가하고 있다.

(2) 폭력정보의 유통

음란정보와 마찬가지로 폭력적인 정보에 의해서도 인간 및 사회적으로 심각한 피해를 가져온다. 실제로 폭력정보는 독립적으로 나타나기 보다는 음란정보와 결부되어 유통되고 있는데, 이러한 폭력정보의 유통은 실제적인 폭력이 행사되고, 그것이 사회구성원 누구에게나 피해를 줄 수 있다는 점에서 매우 심각한 문제가 되고 있다. 반사회적 가치를 갖고 있는 최근의 엽기사이트에서는 시체나 손가락, 목절단, 급소찾아 때리기 등의 신체상해에서 근친상간에 이르기까지 사회가치의 근간을 뒤흔들만한 내용들이 상당수 있다. 이렇게 사람을 쉽게 죽이는 장면의 게임을 계속하여 반복적으로 할 경우 인간은 자신도 모르는 사이에 공격적이 되어 남에게 쉽게 폭력을 쓰게 될 수도 있기 때문에 폭력적인 정보는 나와 남을 모두 폭력의 희생자로 만드는 결과를 낳고 만다.

(3) 허위정보의 유통

정보통신망상에서 자신의 신분이 나타나지 않는다는 사실을 이용하여 허위정보를 유통하는 것은 바람직한 사회 건설에 커다란 지장을 초래한다. 허위정보를 퍼뜨리는 경우는 허위정보를 사실로 믿고 퍼뜨리는 경우도 있으며, 고의로 남을 골탕 먹이거나 장난으로 퍼뜨리는 경우도 있다. 두 경우 모두 허위정보를 유통시킴으로 해서 상호간에 믿지 못하는 분위기를 만들게 됨으로써 신뢰할 수 없는 사회를 만든다는 것에서는 차이가 없다.

남을 골탕 먹이는 재미로 허위정보를 유통시키는 경우는 나중에 자신이 올바른 정보를 유통시키려 해도 남이 믿어주지 않음으로 해서 결과적으로는 자신이 피해를 보게 된다. 허위정보는 피해를 받은 사람에게 자신이 속았다고 하는 데서 오는 심리적인 고통을 줄 뿐만 아니라 허위정보를 유통시킨 사람은 피해자가 허위정보에 의한 경제적인 피해를 받게 될 경우 명예훼손 및 사기죄라고 하는 범죄에 의한 처벌을 받도록 되어있어 허위정보의 유통은 자신은 물론 타인에게도 여러 가지의 피해를 주게 된다.

우리는 이러한 사실을 인식하여 허위정보의 유통을 스스로 자제해야 할 것이며, 허위정보의 유통은 신뢰할 수 있는 사회를 만들기 위해 반드시 근절되어야 할 것이다.

(4) 바이러스 유포 및 해킹 정보의 유통

인터넷의 개방성 및 익명성 등을 악용한 정보시스템의 불법침입 · 파괴 등의 빈번한 발생은 정보사회를 위협하는 주요 요인이 되고 있다. 더욱이 전 세계가 인터넷을 통하여 네트워크화되어 해커 등에 의한 불법침입 및 바이러스 유포 등으로 정보시스템에 대한 침해 및 그 피해는 매우 심각한 수준에 이르렀으며, 이에 대한 법적 제재가 불가피하게 되었다.

컴퓨터바이러스(computer virus)는 정보시스템의 정상적인 작동을 방해할 목적으로 고의로 제작 · 유포된 악성프로그램을 말한다. 이러한 컴퓨터바이러스는 컴퓨터 프로그램이나 실행 가능한 부분을 변형하여 여기에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합을 일컫는 것으로서 컴퓨터 내에 침투하여 자료를 파괴하거나 컴퓨터 손상시킬 뿐만 아니라 다른 프로그램을 파괴하여 작동할 수 없도록 하는 컴퓨터 프로그램의 한 종류이다. 한편, 해킹(hacking)의 의미는 매우 광범위하지만 일반적으로 타인의 정보시스템에 권한 없이 또는 권한을 넘어 불법적으로 접근하여 데이터를 빼내거나 파괴하는 행위를 말하는데, 뛰어난 컴퓨터 사용능력을 이용하여 타인의 컴퓨터에 침입, 그 속에 축적되어 있는 각종 정보를 빼내거나 없애는 행위이다. 해킹은 남의 집에 몰래 들어가 그 집의 살림살이를 이것저것 뒤져보거나, 물건을 부수고 귀중품과 현금을 훔쳐 도망가는 행위와 같다. 따라서 해킹은 도둑질이며, 기물 파괴, 그리고 무단 침입과 같은 범죄와 같은 성질의 행위이다. 그럼에도 불구하고 해킹을 하는 사람들은 자기

가 하는 행위의 범죄적 성격을 이해하지 못하고, 해킹이 마치 자신의 컴퓨터 작동기술을 과시하는 것으로 잘못생각하고 범죄를 저지르는 경향이 있다.

컴퓨터가 바이러스에 감염되면, 동작이 일시 중지되는 가벼운 증상부터 모든 기능이 작동되지 않는 치명적인 증상에 이르기까지 그 증상이 다양하다. 어쨌든 일단 컴퓨터가 바이러스에 감염되면, 컴퓨터의 정상적인 작동은 어렵게 된다. 컴퓨터 바이러스 프로그램이 침투한지 모르고 그 컴퓨터를 사용하거나, 그러한 컴퓨터와 정보를 교환하거나 컴퓨터 바이러스에 감염된 컴퓨터에서 작성한 파일 등을 자신의 컴퓨터에 다시 사용하였을 경우 자신의 컴퓨터에도 바이러스가 감염된다. 따라서 컴퓨터 바이러스 프로그램의 유포는 상상할 수 없을 정도의 많은 사람에게 막대한 양의 피해를 미칠 수 있다.

또한, 컴퓨터가 바이러스에 한 번 감염되어 고장이 날 경우 원 상태로 돌아가기 위한 복구 작업에 따르는 경제적인 손실은 대단히 크다. 자신의 컴퓨터가 고장이 났을 때의 드는 복구 작업비용은 적을 수 있다. 그러나 그러한 복구 작업비용도 여러 사람의 것을 합치면 거대한 비용이 될 수 있으며, 특히 막대한 돈을 들여 설계한 컴퓨터 시스템이 컴퓨터 바이러스에 의해 고장날 경우 시스템 복구를 위해 들여야 하는 경비는 막대하다. 따라서 컴퓨터 바이러스 프로그램의 유포는 개인과 국가에 경제적으로 막대한 손실을 끼칠 수 있는 잘못된 행동이며 범죄행위이다.

(5) 사생활 침해 관련 정보의 유통

정보사회에서는 정보통신 기술의 발달로 인해 개인에 관련된 여러 가지의 정보(성별, 주소, 나이, 재산정도, 학력정도, 취미 등)들이 전자기록으로 컴퓨터 속에 저장되어 보관되기 때문에 관리하기 쉬운 장점이 있는 반면에 컴퓨터에 접근할 수 있는 사람들이나 해커들에 의해서 개인 정보가 쉽게 노출될 수 있는 위험성이 있다. 그러나 개인의 정보가 쉽게 노출될 수 있다고 하는 것이 반드시 개인의 정보를 쉽게 악용할 수 있다는 것을 의미하는 것은 아니다. 하지만 자신과 관련된 정보를 남이 모두 알고 있다거나 다른 사람이 자신과 관련된 정보를 빼내어 자신의 이익을 위해 사용한다는 사실은 매우 기분이 언짢은 일이다. 뿐만 아니라 개인의 사적인 정보를 악용하는 행위는 단순히 피해자의 기분을 언짢게 하는 것을 넘어서 때로는 그 개인에게 엄청난 피해를 입히기도

한다. 따라서 개인의 사적 정보를 악용하는 것은 엄연한 범죄행위가 된다.

타인에 관한 정보를 쉽게 얻을 수 있다고 하여 타인의 정보를 마음대로 사용할 수 있는 것은 아니다. 오히려 우리는 우리가 획득한 다른 사람의 개인 정보를 가능한 한 보호해 주기 위해서 노력해야 한다. 내가 타인의 사생활과 개인 정보를 보호해 주지 않는다면, 다른 사람들도 마찬가지로 나의 사생활과 개인 정보를 보호해 주지 않을 것이다. 내가 타인의 정보를 악용할 수 있는 것처럼 타인도 나의 정보를 악용할 수 있다. 따라서 우리는 우리 자신의 정보는 물론 타인의 정보도 우리 자신의 정보와 마찬가지로 중요하다는 것을 깨닫고 타인의 정보를 보호하기 위해서 노력해야 한다. 특히 개인의 사적인 생활과 연결되는 정보의 이용은 그것이 악용되지 않는다고 하더라도, 혹은 그것이 자신의 것이든 타인의 것이든 개인의 사적인 생활을 침해하는 중대한 범죄가 되기 때문에 개인의 사적 정보는 보호되어야 하며, 함부로 다른 사람의 사적 정보를 이용해서는 아니된다. 아울러 우리는 우리 자신의 개인 정보가 함부로 유출되지 않도록 주의를 기울여야 한다.

(6) 재산권 침해 관련 정보의 유통

컴퓨터에 사용되는 여러 가지 프로그램에는 이를 만든 사람들이 자신의 프로그램에 갖는 재산상의 권리가 있다. 우리가 어떤 물건을 하나 만들어 팔 때 그 물건을 판 값은 물건을 만든 사람의 노력에 대한 일종의 대가로서 지불된 것이다. 마찬가지로 컴퓨터 프로그램은 그 프로그램을 만든 사람에게 만든 노력에 대한 대가가 지불되어야만 한다. 그러나 종종 컴퓨터 프로그램도 하나의 재산으로서 보호되어야 한다는 생각을 하지 못하고, 컴퓨터 프로그램을 만든 사람에게 허락을 받지 않고 다른 사람이 그대로 원본의 프로그램을 복사하여 판매하는 경우가 있다. 이러한 행위는 그 프로그램을 만든 사람의 노력을 훔치는 것으로서 명백한 범죄 행위이다. 이러한 경우는 우리가 읽는 책에도 해당된다. 어떤 사람이 자신의 이야기를 소설로 써서 판매한 경우 그 소설책을 팔아 많은 수익을 얻었다고 하자. 이 경우 책을 팔아 얻은 수익은 마땅히 그 소설을 쓴 원작자의 노력에 대한 대가이다. 그러나 원작자가 아닌 다른 사람이 원작자의 소설을 그대로 베껴 또 다른 책을 다른 제목으로 출판하였을 때 이러한 행동은 원작자의 내용을 훔친 것이 된다. 따라서 남의 물건을 훔친 것과 같은 원리가 되는 것이다. 이처럼 어떤 사람이 스스로 노력하여 만들어낸 물건이나 내용에는 그것을 가장 먼저 만들고 생각해낸 사람에게 물건과 내용에 대한 재산상의 권리가 주어진다.

컴퓨터 프로그램의 경우에도 프로그램을 최초로 만든 이에게만 그 프로그램에 대한 소유가 인정되고 그 프로그램을 팔아 얻어지는 모든 수익에 대한 권리를 인정한다. 이것을 바로 '지적재산권'이라고 한다. '지적재산권' 이란 현금이나 주택을 소유한 사람에게만 현금과 주택의 소유가 인정되는 것과 마찬가지의 고유한 재산권에 해당된다. 따라서 다른 사람이 만든 컴퓨터 프로그램을 사용하고자 할 경우에는 지적재산권을 소유한 사람의 승인이 있어야만 사용할 수 있게 된다.
정품의 소프트웨어란 지적 소유권을 가진 사람이 자신의 프로그램을 사용하도록 공식적으로 승인한 소프트웨어이다. 그러나 정품의 소프트웨어를 구입하지 않고 남이 사용하는 소프트웨어를 몰래 복사하여 사용할 경우 지적 소유권을 가진 사람의 물건을 몰래 훔쳐 사용하는 범죄를 저지르는 것이 된다. 특히 정품 소프트웨어를 불법으로 복제하여 판매하는 사람의 경우는 남의 물건을 훔쳐 파는 것과 똑 같은 범죄를 저지르는 것으로 도둑질에 해당된다고 할 수 있다. 뿐만 아니라 대다수의 사람들이 정품 소프트웨어를 사용하지 않고 불법 복제 소프트웨어를 사용한다면, 아무도 소프트웨어를 개발하려고 하지 않을 것이고, 그렇게 되면 우리나라의 소프트웨어 산업은 발전할 수 없을 것이며, 그 만큼 정보사회의 발전도 지체될 것이다.

제2절 불건전정보의 차단

1. 개요

불건전정보의 차단과 관련하여 정보통신망을 통한 불법 · 청소년유해정보의 유통방지를 위해 다양한 기술개발이 되고 있다.

현재, 불법 · 청소년유해정보(불건전정보)를 차단 또는 규제하는 방식으로는 여과방식(filtering)과 구획방식(zoning)으로 크게 구분할 수 있는데, 여과방식은 콘텐츠에 등급을 매겨 그 등급에 따라 콘텐츠를 여과하는 방식으로서 현재 민간자율적으로 시행되고 있는 인터넷내용등급제도 및 음란 · 도박 등 해외불법사이트의 유입차단조치 등이 그 예이고, 구획방식은 정보이용자의 특성에 따라 규제하는 방식으로서 성인인증 등을 통한 진입장벽을 설치하는 식으로 성인구역과 청소년구역으로 구분하는 방법이다. 현행 정보통신망이용촉진및정보보호등에관한법률에 의한 청소

넌유해매체물표시제도가 그 대표적인 예이다.

2. 불건전정보 차단 기술

가. 인터넷내용등급제의 (SafeNet) 선별기술

인터넷의 정보를 선별 · 차단하는 방법은 인터넷 보급의 초기단계부터 제안되어 왔다. 그 중 초기에 이용되었던 블랙리스트(Black List)의 방법은 내용에 등장하는 단어, 문구, 또는 사이트 이름 등을 기준으로 접근을 금지시키는 방법이다. 하지만 이러한 방법은 불건전정보를 효율적으로 차단하는데 한계성이 있다. 이에 따라 인터넷내용에 등급을 부여하여 이용자가 원하는 내용을 선별적으로 차단할 수 있도록 하는 방법이 가장 타당성이 있는 것으로 연구되었다.

인터넷과 PC통신상의 불법 및 불건전 정보를 차단하는 방법에는 불건전 정보 사이트 차단목록 기반의 선별기술(Black List Filtering)과 허용목록 기반의 선별기술(White List Filtering)이 있다. 또한 웹사이트의 전자소스를 인식하여 특정 정보를 선별할 수 있는 인터넷내용선별(Platform for Internet Content Selection : PICS) 기술이 있다.

(1) 차단목록 기반의 선별기술(Black List Filtering)

차단목록 기반의 선별기술은 불건전정보만 선별하여 차단하는 방식이다. 즉, 음란 및 폭력물 등 불건전한내용을 담고 있는 사이트를 차단하는 방식으로 유해정보 사이트의 주소목록(Black List)을 기억하고 있다가 사용자가 인터넷의 특정 사이트에 접속할 때, 이 사이트의 주소가 블랙리스트(Black List)에 있을 경우 접속을 허용하지 않는 방식이다.

(2) 허용목록 기반의 선별기술(White List Filtering)

허용목록 기반의 선별기술 내용은 리스트에 등록된 사이트만 접근을 허용하고 이외의 사이트는 모두 차단하는 방식이다. 이와 같은 차단목록 기반의 선별기술(Black List Filtering)과 허용목록

기반의 선별기술(White List Filtering) 리스트 이외의 항목은 차단할 수 없다는 측면에서 실효성이 미약하다. 이에 따라 인터넷내용등급 기반의 선별기술(PICS)이 대두되었다.

(3) PICS 인터넷내용선별 기술

인터넷내용선별(Platform for Internet Content Selection : PICS)기술은 인터넷 내용물을 선택적으로 접근하게 하는 국제적 기술표준을 말한다. 내용선별 소프트웨어(Filtering S/W)와 등급서비스들 간에 잘 동작할 수 있게 도와주는 기술규격이며, 확장 가능한 구조로 되어 있어 정보를 빠르게 검색하거나 지적소유권 등에 활용이 가능하다. PICS의 선별방법은 모든 사이트 내용물을 차단하는 것이 아니라 정의된 등급에 의해 선별 · 차단한다.

PICS는 정보이용자의 컴퓨터에서등급코드를 처리하여 정보이용자가 내용을 선별할 수 있도록 개발된 문법이다. PICS는 매우 유연하고 중립적인 기술로써, PICS기반의 등급부여는 정보제공자의 선택에 따라 홈페이지, 홈페이지내의 디렉토리 또는 페이지 단위 등 다양한 형태의 등급부여가 가능하며, 하나의 웹 페이지에 여러 기관에서 제공하는 등급을 표기할 수도 있다. 이러한 PICS의 유연성은 등급부여가 특정한 목적의 검열 수단으로 전락하지 않도록 고안되었다.

(4) ICEC의 인터넷내용 선별기준

정보통신윤리위원회(Information Communication Ethics Committee : ICEC)의 등급기준은 객관성, 국제 호환성, 이용자 편의성, 한국적 문화가치 등을 고려하였고, 해외 등급서비스 운영기관인 인터넷내용등급협회(ICRA)의 RSACi 1994년 워싱턴에서 출범하였던 RSACi(오락소프트웨어자문협의회)는 1999년에 ICRA에 통합되었다. 등급기준과 New ICRA 45개 기술어 등급 기준, 그리고 제3자등급 서비스를 제공하고 있는 일본 인터넷기업협회(IAjapan, 구 ENC)의 Safety Online 등급기준을 벤치마킹하여 마련하였다.

SafeNet 등급기준의 범주와 등급 수준은 노출, 성행위, 폭력, 언어, 기타 등 5개 범주와 각 범주별 5단계(0~4등급)로 정하였는데, 단, 기타 범주는 등급수준(0~4등급)을 정하지 않고 정보제공

여부(있음/없음)로 구분하였다.

[표 10-2-1] 정보통신윤리위원회 SafeNet 등급기준

범주 / 수준	노출	성행위	폭력	언어	기타
4 등급	성기노출	성범죄 또는 노골적인 성행위	잔인한 살해	노골적이고 외설적인 비속어	1. -마약사용조장 -무기사용조장 -도박 2. -음주조장 -흡연조장
3 등급	전신노출	노골적이지 않은 성행위	살해	심한 비속어	
2 등급	부분노출	착의상태의 성적접촉	상해	거친 비속어	
1 등급	노출복장	격렬한 키스	격투	일상비속어	
0 등급	노출없음	성행위없음	폭력없음	비속어 없음	

나. 게임등급 등 게임정보 제공 소프트웨어(게임정보알림이)

게임을 즐기는 연령층이 대부분 청소년이지만, 이들의 게임이용을 지도해야 할 부모들은 게임사용이나 교육 등에 대한 별다른 정보가 없어 무조건 게임을 못하게 하거나 방치해두고 있는 실정이다. 이에 정보통신윤리위원회는 부모들이나 청소년들이 게임정보를 쉽게 접할 수 있도록 게임정보를 알리어 청소년들의 게임이용을 건전하게 유도할 수 있도록 안내하는 일명 '게임정보알림이' 소프트웨어를 개발하여 보급하고 있다. 게임정보알림이 소프트웨어는 게임정보 알림기능, 신고기능, 시간관리기능 등 다양한 기능을 가지고 있는데, 게임정보 알림기능을 위해서는 게임에 대한 제작사, 게임스토리, 청소년유해매체물 결정여부, 유료 결재 여부, 수상 경력 등 다양한 정보를 DB화하고 청소년들이 게임정보에 접근할 경우 DB화된 정보를 알려준다. 게임정보에 따라서는 청소년들이 이용할 수 있거나 부모의 동의가 필요한 게임으로 분류되고 내용에 따라 원천적으로 청소년의 접근을 차단할 수 있도록 되어 있다. 한편, 게임정보알림이는 최근 게임으로 인한 각종 피해가 속출하고 있어 문제가 되는 내용을 신고접수하여 처리할 수 있도록 하는데 목적을 두고 있는 신고기능을 두고 있다.

다. 음란스팸차단 소프트웨어(음란스팸잡이)

이메일(이메일)은 편리성, 경제성, 신속성 등으로 인하여 정보통신사회의 중요한 의사소통수단으로서 기능한지 오래다. 그러나 시간과 장소를 구분하지 않고 무분별하게 전송되는 불법스팸메일로 인하여 순기능이 상실되고 신뢰성 저하, 막대한 경제적 손실 등 사회적으로 큰 문제가 야기되었고, 음란스팸메일 등으로 인하여 청소년의 건전한 인격형성에 저해가 되는 요소가 될 뿐만 아니라 성인들에게도 혐오감 및 수치심을 유발하거나 정신적 · 시간적 · 경제적으로 손해를 끼치고 있다. 이에 따라 정보통신윤리위원회가 2003년 11월 음란스팸메일을 효과적으로 차단할 수 있는 음란스팸차단 소프트웨어를 개발 · 보급하고 있는 것은 국민적으로 큰 호응을 얻고 있다. 음란스팸잡이는 음란스팸메일의 제목과 본문내용에 포함되어 있는 음란키워드 및 음란이미지를 인식하여 필터링하고 정보통신윤리위원회가 보유하고 있는 해외 한글음란 등급DB와 연동되어 음란스팸메일을 차단하고 있는 소프트웨어이다.

즉, 메일을 통해 전송되는 음란사이트를 정보통신윤리위원회가 구축한 해외 음란사이트 DB와 비교 · 분석하여 차단하고 정보통신윤리위원회에서 음란사이트 DB를 지속적으로 갱신함으로써 차단의 효과를 극대화하고 있으며, 메일의 제목과 본문내용에 포함된 문자정보 및 메일로 전송되는 이미지패턴의 음란성 여부를 인식하여 차단하는 기능을 가지고 있다. 또한 POP3형식의 일반메일(outlook 등)뿐만 아니라 청소년이 많이 이용하고 있는 웹메일(hanmail, hotmail, dreamwiz 등)에 접근하여 음란스팸을 차단하는 기능을 가지고 있으며, 사용자 임의로 키워드나 송신자 ID를 선별하여 허용(White List)목록과 차단(Black List)목록을 설정하여 차단하는 방식을 취하고 있다. 그러나 하루에도 수많은 음란스팸메일이 신규로 생성 · 삭제되고 있어 100% 차단할 수는 없지만, 음란스팸메일을 최대한 차단할 수 있도록 관련기능을 지속적으로 업그레이드하고 있으며, 관련기술 개발을 지속히 수행하고 있다.

라. 해외 불법정보 기술적 차단

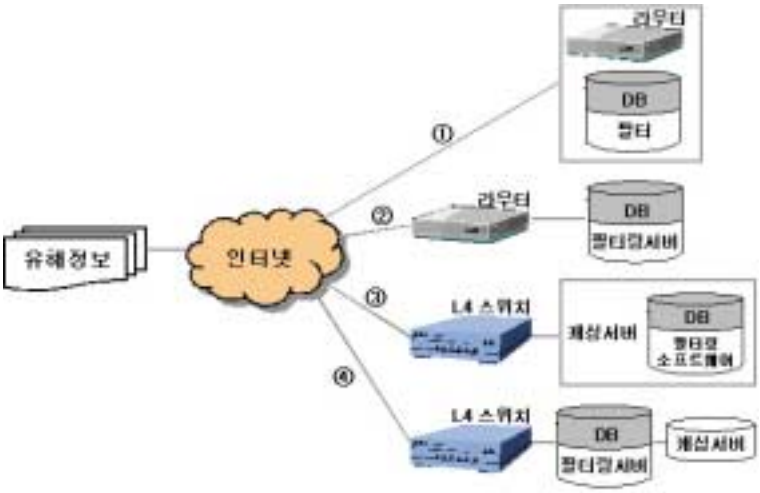
국내로 유입되는 해외불법정보 중 음란 · 도박정보 등은 내국인 정보이용자의 접근용이성으로 말미암아 다양한 사회적 문제가 야기 시키고 있다. 특히, 개인의 프라이버시를 침해하는 몰래카메

라, 미성년자를 성적 유희의 대상으로 이용한 로리타, SM(변태성욕) 등 각종 불법 포르노 정지·동영상정보, 사행심을 조장하는 도박정보, 정상적인 수입 절차 없이 유통되고 있는 불법식품 및 의약품정보가 유통됨으로 인해 해당 사이트 가입비, 도박비용, 구매비용 등 외화의 해외유출 및 국민보건 등에 있어 심각한 문제를 낳고 있다.

이러한 해외불법정보는 국내법을 적용하는데 한계가 있어 현재로서는 국내유입을 원천적으로 차단하는 조치를 취할 수밖에 없는 실정이다. 인터넷을 통한 정보제공은 서버와 라인을 그 기반으로 하므로, 해외불법정보의 국내유입을 차단하고자 하는 때에는 통상 해외 송수신라인을 가진 각 ISP업체의 협조를 통하여 국내라인과 해외라인을 연결하는 라우터에 부가적 장비(Proxy server, 보안서버 등)를 설치, 활용하여 불법정보제공 IP 및 Domain을 차단하게 된다. 라우터 차단 방식은 정보를 요청하는 Client Computer와 국외 불법정보제공 Server와의 정보 송수신 과정에서 문제의 목적IP와 Domain의 Data Base를 검색, 차단하는 방법이므로, 통상적인 정보송수신 과정(특별한 여과절차가 없는 정보 송수신)과는 달리 정보 송수신과정에 중간검색작업이 개입되므로 시간지연, 정보트래픽 등이 발생하여 정보이용자의 통신이용에 장애 등 불편이 나타날 수 있고, 정보이용자가 다수가 되면 될수록 정보이용에 따른 불편의 정도는 비례적으로 가중될 수 있다는 문제가 있을 수 있다.

현재 ISP업체에서 취하고 있는 라우터차단 방식은 (그림 9-2-1)과 같이 크게 4가지로 구분되는데 ①과 같이 제한적으로 라우터 내부에 필터링기능이 있는 경우, ②와 같이 라우터와 별도로 필터링서버를 두는 경우, ③·④와 같이 ISP업체가 사용하고 있는 L4스위치와 연동되어 ③과 같이 캐싱서버 내에 필터링기능을 구현하는 경우, ④와 같이 L4스위치와 캐시 서버간에 필터링서버를 두는 경우 등이 있다.

4가지 해외불법정보 차단방식
(그림 10-2-1)



① · ③의 경우에는 라우터나 캐시 서버 내부에 필터나 필터링S/W를 구현할 수 있으며, ② · ④의 경우에는 기존장치의 외부에 필터링서버를 구현할 수 있다.

한편, 차단과 관련하여 프록시서버를 이용하거나 네트워크 캐시 이용하는 방법을 사용하고 있는데, 프록시서버 이용방법은 이용자의 IP를 기반으로 하여 인터넷접속을 제한하는 것이지만 ISP나 대형사설망에는 적합하지 않고, 서버 자체가 S/W로 구현되어 있어 속도가 느리며 이를 보상하기 위해 서버의 하드용량을 확장하는 경우에도 제한을 받는다는 단점이 있다. 네트워크 캐시의 이용방법(대표적으로 Cisco사의 웹 캐시 엔진이 있음)은 프록시서버의 단점을 보완하기 위한 대안적 형태로서, 캐싱에 적합하도록 S/W를 최적화함으로써 프록시서버보다 나은 성능을 제공할 수 있으나, 범용 운영체제 상에서 수행되는 경우 오버헤드가 크고, 대용량의 트랜잭션 처리에 부적합할 수 있다는 단점이 있다.

정보통신윤리위원회의 요청에 따라 2000년 4월부터 시작된 해외불법정보의 차단은 URL단위와 IP주소 단위로 이루어지고 있는데, 해외불법정보제공자 및 사이트 운영자는 국내에서 음란 · 도

박정보의 유통이 불법이라는 사실을 이미 인지하고 있으면서 수개의 IP를 연결 · 활용하거나 IP를 손쉽게 변경하여 국내에서의 라우터 차단 등을 회피하기도 하며, URL단위나 ISP주소단위 중 1개의 단위만으로 차단하거나 이를 병행하여 차단하는 등 ISP업체마다 다른 차단방식을 이용하고 있어 차단기술의 일관성을 유지하는데 한계가 있다. 현재, ISP업체의 라우터 시스템 및 서비스 이용제한을 최소화할 수 있는 방식의 기술을 개발 중에 있다.

한편, 목적IP를 추적함에 있어서는 비쥬얼라우터, 네오트레이서 등의 IP추적 유틸리티를 일반적으로 이용하고 있지만, 보안서버를 두고 정보를 제공하는 경우에는 정확한 추적이 불가능할 뿐만 아니라 프록시서버를 유 · 무료로 제공하는 업체의 서비스를 이용하거나 프록시프로그램을 사용하여 차단된 해외불법사이트를 우회하여 접속하는 것이 용이할 수 있어 이에 대한 대안 기술도 강구되어야 한다.

제3절 정보통신서비스제공 사업자의 정보통신윤리 실천방안

1. 정보통신서비스제공 사업자의 자율규제활동

디지털 기술의 발전은 초고속 정보통신망 구축을 기반으로 새롭고 다양한 정보통신서비스 매체의 등장 및 각종 데이터의 생성 · 가공 · 전송 · 보안 관련 등의 기술 발전을 가져왔으며, 이러한 변화로 인해 정보통신서비스 콘텐츠, 즉 정보통신을 통해 제공되는 '정보' 에 대한 개념 및 이용 등에도 많은 변화를 초래하였다.

기존의 '정보' 에 대한 수동적 접근에서 벗어나 최근에는 보다 능동적이고 효율적으로 '정보' 에 접근하여 이를 이용하거나 더 나아가 가공 · 활용하게 되었으며, 정보의 선점및 적절한 이용이 개인의 발전, 소득, 만족 등 개인생활에도 큰 영향을 미치게 되었다. 나아가 국가간 경쟁에 있어서도 이러한 디지털 환경 및 정보가 중요한 국가 경쟁력으로 여겨지게 되어, 디지털 환경의 변화는 '정보' 를 생산 · 가공 · 판매하여 부가가치를 극대화시키려는 정보통신서비스제공자들의 증가를 가져오게 되었다.

초기 정보통신서비스제공자가 제공하는 '정보'는 크게 유선망(700전화)을 통하여 의료 · 교육 · 교양 · 날씨 · 운세 · 오락 등의 콘텐츠를 음성형태로 제공하는 서비스, PC통신을 통해 유선정보와 같은 종류의 콘텐츠를 텍스트 형태로 제공하는 서비스 등 크게 두가지로 나누어지며, 당시의 정보통신서비스 환경에 따라 콘텐츠 내용 및 서비스는 극히 단순하고 초보적인 형태를 띠고 있었다.

그러나 초고속정보통신망 구축 및 각종 기술개발은 음성과 텍스트로 각각 분리되어 제공되던 서비스 형태를 그림, 정지영상, 동영상, 화상, P2P(Peer-to-Peer), 실시간 영상 · 음성 동시서비스 등 다양하고 복합적인 형태로의 제공을 가능하게 하였으며, 또한 일방향 정보제공에서 벗어나 정보제공자와 이용자, 혹은 이용자 개인간에 실시간으로 정보를 주고받을 수 있는 양방향성을 추구하는 형태로 변화되었다.

한편 이러한 정보통신서비스의 환경 변화와 함께 정보의 양적 증가를 가져왔으나, 반대로 불건전정보의 유통의 증가 등 다양한 역기능이 나타났다. 초기 음성이나 텍스트 환경에서의 음란 · 폭력물과 달리 지금은 다양한 매체 및 양방향 정보교류를 통해 성매매(원조교제), 음란물 판매, 자살, 폭탄, 청부살인, 가출조장 등 반사회적인 불법 · 불건전정보의 유통 등이 심각한 사회문제로 부각되고 있으며, 이에 정부, 시민단체, 전기통신서비스 관련단체 등 여러 기관에서 다양한 형태의 대책 및 방안이 마련되고 있으나, 가장 중요한 역할을 해야 할 주체는 역시 정보통신서비스제공업을 하는 사업자일 것이다.

현재 인터넷 불건전정보 방지를 위한 과제 중의 하나인 사업자의 자율규제는 정착초기단계에 있다. 그러나 자율정화에 참여하는 사업자단체가 증가하고 사회적으로도 이를 권장 촉진하려는 분위기가 조성되고 있어, 사업자 자율정화가 부문적으로는 빠르게 자리를 잡아가게 될 것이다.

2. 정보통신서비스제공 사업자에게 필요한 자세

사업자는 정보를 공급하는데 있어서 그 정보가 가져다 줄 파급영향을 고려하여 신중을 기해야 한다. 직업윤리의식이 있어야 하고, 정보통신이 미치는 광범위한 영향력에 대한 책임성을 자각하여

야 하는 것이다.

사업자는 대부분이 정보제공의 목적을 수입에 두고 있고, 사업경쟁도 치열하다. 따라서 인간의 말초적인 심리를 건드려 관심을 끌기 위하여 음란 · 폭력성을 경쟁적으로 제공한다. 그러나 영리만을 위하여 불량정보를 양산하는 정보제공 자세는 반드시 고쳐져야 한다.

그리고 사업자는 불건전정보의 제공이 윤리문제를 벗어나서도 자유롭지 못한 행위라는 점을 인식해야 한다.

원칙적으로 제공한 정보에 관한 법적 책임을 지는 것은 사업자임을 충분히 인식할 필요가 있다. 인터넷을 이용할 때라 해서 법적 · 도덕적으로 기존의 기본적인 규칙을 어겨서는 안 된다는 의식을 가져야 한다.

우리나라는 관습이나 도덕에 있어 나름의 전통이 있다. 외국과 정서도 다르고, 문화도 차이가 있다. 인터넷으로 해외 음란물이 범람한다 해서 우리에게도 일순간 그와 같은 현상이 허락된다는 의미는 아니며, 그렇게 될 수도 없다. 이러한 기본 정서에도 불구하고 국내 정보통신서비스에는 인터넷과 내용이 동일한 음란정보가 다량 유통되고 있다.

이것은 비양심적이고, 우리 사회의 정서를 외면한 정보제공자의 범법행위이다. 인터넷은 열려있지 않느냐라는 의문하고는 별개의 것이다. 이는 다른 사람이 물건을 훔치니까 나도 도둑질을 한다는 논리와 같아 합리화될 성질의 것이 아니다.

불건전정보 유통이 인터넷이나 PC통신과 같은 새로운 매체에 의하여 이루어진다 해서 예외로 생각해서는 안된다. 공개되지 않은 것은 적발하기가 어려운 점이 있고, 현실의 흐름이 감안되어 제재되지 않는다 하여, 그것이 제도적으로 허용된 것이라 여겨서는 안 된다는 것이다.

아무리 제도가 잘 발달되어 있다 하여도 사업자 개개인이 건전해지지 않으면 복제에 복제가 거듭되어 기하급수적으로 퍼지는 음란정보의 근절은 현실적으로 어렵게 된다.

사회가 변화하면 법과 윤리도 변하기 마련이다. 제도나 규범을 바꾸는 데는 어떤 논의와 시간이 필요하다. 그러나 아무리 진보적인 변화가 이루어진다 하여도 인륜의 도를 지나치는 것은 허락될 수 없는 한계가 있는 것이다.

3. 사업자가 실천해야 할 윤리

사업자가 윤리적으로 실행할 내용들이 무엇인가를 생각하는 데는, 1997년에 만들어진 정보통신사업자윤리실천강령이 도움이 될 것 같다. 강령의 내용에는 사업자가 지녀야 할 기본 정신이 들어 있다.

정보통신사업자 윤리실천 강령

우리는 미래의 정보사회를 이끌어 갈 정보통신사업자로서 건전한 정보통신 문화 창달의 책임과 의무를 성실히 수행할 것을 다짐하며, 그 구체적인 실천 강령을 다음과 같이 선포한다.

- 우리는 정보통신사업자로서 보람과 긍지를 가지고 올바른 정보를 제공하여 국가 사회 발전에 이바지한다.
- 우리는 사회적 도덕성에 입각하여 건전한 정보가 유통될 수 있는 환경을 구축한다.
- 우리는 양질의 정보를 제공함으로써 삶의 질을 높이는 데 최선을 다한다.
- 우리는 불건전 정보가 유통되지 않도록 스스로 자제하여 사회 공익에 우선될 수 있는 풍토를 조성한다.
- 우리는 인권과 사생활을 존중하고 저작권을 보호함으로써 정보사회 질서를 확립한다.
- 우리는 비판적 시각을 중시하고 상호 협력을 통하여 자율적인 정보통신 문화 정착에 앞장선다.
- 우리는 정보통신 윤리강령에 따라관련 법령과 규정을 준수하여 정보통신인으로서 책임과 의무를 다한다.

1997. 4. 29

정보통신사업자일동

4. 정보통신서비스제공 사업자의 형사적 책임

가. 개요

정보통신서비스제공 사업자가 이용자에게 정보통신망의 가입을 개방하는 것은 법적으로 허용된 행위이고 그 자체로 처벌할 수 있는 내용의 유포행위에 해당하지 아니하지만, 제3자에 의하여 정보가 입력된 경우에 비로소 정보통신서비스제공자는 법적인 책임이 따른다.

정보통신서비스제공 사업자는 원칙적으로 정보통신서비스이용자들의 통신과정에는 개입하지 못한다. 그가 직접 제공한 토론포럼과 고유의 편집내용을 제외하고 그는 인터넷에 정보를 제공하지도 못함은 물론 개개의 정보나 뉴스그룹에 대한 고객의 접근을 조정, 통제하지 못하는 경우도 있다.

통상 정보통신서비스제공 사업자를 비난하려면, 사업자가 정보의 이동을 충분히 감시하지 않았고, 불법통신의 저지 가능성을 충분히 기대할 수 있음에도 이를 저지하지 아니한 경우에만 가능하다. 이 점에 비추어 보아 정보통신서비스제공 사업자에 대한 비난 가능한 행동의 핵심은 그의 '부작위' 에 있다고 할 수 있다.

나. '보증인적 지위' 의 문제

정보통신서비스제공 사업자는 결과가 발생하지 아니하도록 하는 보증인적 지위에 서 있어야 처벌이 가능하다. 보증인적 지위가 누구에게, 언제, 어떻게 발생하느냐에 대하여는 아직까지 명확하지는 않지만, 특별한 법 · 규정으로부터, 사실상 법익에 대한 책임의 인수로부터, 특별한 신뢰관계로부터 각각 발생할 수 있다.

다. 정보통신서비스제공 사업자의 '고객에 대한 법익 보호의무'

정보통신서비스제공 사업자는 고객들이 정보통신망에 가입하여 인터넷상에서 통신이 가능하도록 할 계약상 의무를 부담할 뿐 고객들에 대한 법익을 보호할 직접적인 의무는 없기 때문에 인터넷상 처벌 가능한 내용으로부터 고객을 보호할 법적 의무는 거의 없다.

라. '정보통신' 이라는 위험원 제공자나 관리자로서의 보호의무

정보통신서비스제공 사업자는 고객에게 정보통신망 가입의 허용을 통하여 법적으로 허용된 영업적 활동을 추구한다. 정보통신서비스제공 사업자의 활동 그 자체가 형사법적으로 보호된 법익에 대한 특별한 위험원을 창출하지는 아니한다. 이러한 위험원은 통상적으로 불가결하게 일반적인 정보통신의 범주에서는 제3자의 행위를 통하여 비로소 발생한다.

정보통신서비스제공 사업자의 보증인적 지위를 인정할 수 없는 것은 아니다. 정보통신서비스제공 사업자는 정보통신망의 관리자로서 그의 고객을 위하여 위험원에 대한 접근과 가입에 대하여 어느 정도 지배하고 통제할 수 있기 때문이다. 따라서, 정보통신서비스제공 사업자는 이러한 위험원의 영향범위에서 발생하는 고객들의 모든 법익을 보호하기 위하여 그에 상응하게 안전조치를 취할 증대된 책임을 지게 된다.

c o n t e n t s

제 11 장
사고대응

제 1 절 해킹 · 바이러스

1. 침해사고 대응팀 구축

신규 보안취약점의 증가, 공격기법의 고도화, 각 기업의 정보시스템의 중요도 증가 등으로 인해 기업의 정보자산에 대한 보호는 필수적으로 요구되고 있다. 이러한 요구에 의해 각 기업에서는 기업의 정보자산을 보호하고 전자적 침해사고 발생시 신속한 대응으로 피해를 최소화하기 위한 침해사고 대응팀(CERT, Computer Emergency Response Team)의 구축과 운영이 요구되고 있다.

본 절에서는 침해사고 대응팀을 구축하기 위해 필수적으로 요구되는 침해사고대응 정책과 지침, 침해사고대응조직의 구성 및 인력과 침해사고 대응팀의 업무에 대해서 알아보도록 한다.

가. 침해사고대응 정책 및 지침

침해사고대응 정책은 조직의 사명과 특성에 부합되도록 침해사고 발생시 어떻게 행동해야 하는지를 기술한 전반적인 규칙의 집합이라고 할 수 있다. 이 정책은 기업 내의 모든 임직원에게 적용되며 어떤 상황에서 어떻게 대처를 하고, 어떤 상호작용을 해야 하는지에 대해서 기본적인 지침을 제공한다. 또한, 침해사고 대응팀 대내외적으로 어떤 상호작용을 해야 하는지도 기술한다.

다음은 침해사고대응 정책 작성 예이다.

Ⅰ. 침해사고대응팀 임무 및 구성
1. 침해사고대응팀 임무
2. 침해사고의 범위
 2.1 침해사고의 정의
 2.2 침해사고의 종류
3. 인력 구성 및 역할
 3.1 침해사고대응지원팀장
 3.2 침해사고 접수 담당
 3.3 침해사고 처리 담당

Ⅱ. 침해사고 접수 및 처리
1. 침해사고 접수
 1.1 침해사고 접수 수단
 1.2 국내 침해사고 접수
 1.3 국외 침해사고 접수
 1.4 침해사고 접수 처리
 1.5 바이러스 사고 접수
2. 침해사고 분석 및 처리
 2.1 지원 범위
 2.2 현장 지원 업무
 2.3 관련기관 연락업무
 2.4 침해사고 분석
 2.5 침해사고 처리
3. 사후 조치
 3.1 피해기관 보안 조치
 3.2 사후 침해사고 분석

Ⅲ. 침해사고 정보 관리
1. 인적 관리
2. 안전한 전자메일 사용
3. 기록 및 보관
4. 정보의 중요성에 따른 처리
5. 정보 공개

Ⅳ. 해킹기법 시험 · 분석, 대책
1. 보안권고문 및 기술문서
2. 해킹기법 시험 · 분석
3. 해킹방지기술 연구

Ⅴ. 대외 업무
1. 조직내 각 IT 담당자
2. 관련 대외기관 담당자
3. CONCERT / 수사기관

Ⅵ. 내부 보안
1. 출입통제
2. 시스템 및 네트워크 보안
3. 재해 대책

나. 침해사고대응조직 구성 및 인력

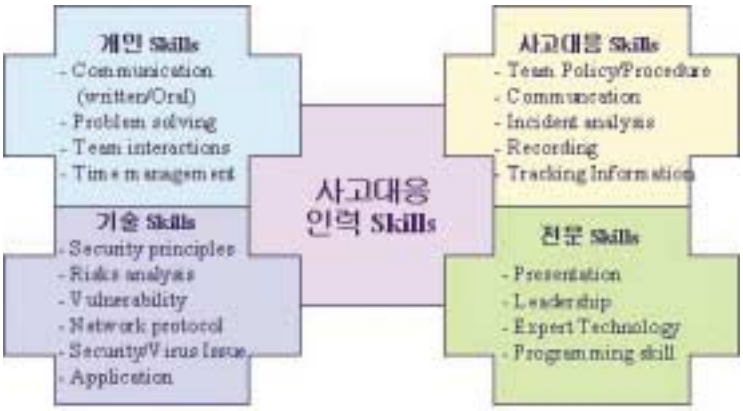
침해사고대응 업무 처리시 조직의 정책 및 절차를 효과적으로 수행하는 것은 전적으로 침해사고대응팀원의 능력과 자질에 의존하게 된다. 그러므로 침해사고대응팀원은 서비스 운영과 임무를 효과적으로 수행하는데 중추적인 역할을 한다.

침해사고대응팀원의 자질에 대해 대부분의 사람들은 침해사고대응팀원의 기술적인 경험을 가장

중요하게 생각할 수 있다. 기술적인 경험이 중요한 요소지만 보다 중요한 요소는 개인의 의지와 고객 및 다른 팀원과 업무 협조시 절차 준수 능력이다.

일반적으로 사고대응을 위한 전문 인력은 (그림 11-1-1)과 같이 다양한 기술과 능력이 요구된다.

사고대응 인력의 자질
(그림 11-1-1)



사고대응 인력은 전문적인 기술력 뿐 아니라 다음과 같이 유연한 대인관계 능력도 요구된다.

- 명확한 규정이 없거나, 스트레스를 받고 있거나 힘든 경우에도 효율적이고 타당한 판단을 할 수 있는 상식
- 다른 팀이나 의뢰자와 효율적인 구어, 문어 대화 능력
- 언론이나 협력기관 등 다른 기관과의 절충 능력
- 정책과 절차를 따르는 능력
- 지속적인 교육 의지
- 스트레스와 업무 부하를 견딜 능력
- 팀 업무협조
- 팀 명성과 품위를 지킬수 있는 품위
- 실수를 인정하는 태도
- 새로운 상황에서 효율적인 사고처리를 위한 문제해결 능력
- 일의 우선순위를 관리할 수 있는 시간 관리 능력

기술적인 측면에서 각 사고 처리자는 기본적인 기술의 이해와 개인은 그들의 전문성에 기초를 두어야 하는데, 아래는 사고 처리자가 갖추어야할 기술적인 요소들이다.

- 일반적인 데이터 네트워크(인터넷, X.25, ATM, 프레임 릴레이 등)
- 네트워크 프로토콜(IP, ICMP, TCP, UDP 등)
- 네트워크 기반 요소(라우터, DNS, 메일서버 등)
- 네트워크 응용프로그램 또는 서비스와 관련된 프로토콜 (SMTP, HTTP, FTP, TELNET 등)
- 기본 보안 원칙
- 컴퓨터와 네트워크 위험 및 위협
- 보안 취약성과 관련된 공격 기법(인터넷 웜, 컴퓨터 바이러스 등)
- 네트워크 보안 이슈(침입차단시스템 혹은 가상사설망)
- 암호 기술, 전자서명, 해쉬 알고리즘
- 사용자와 시스템 관리자 측면의 호스트 시스템 보안(백업, 패치)

침해사고대응팀원이 갖추어야하는 기술적 요소들을 열거하였으나, 실제 이러한 모든 기술을 갖춘 인력을 드물 것이다. 사고대응팀의 각 구성원들은 위 기술요소 중 각자의 전문 분야를 육성할 필요가 있다.

팀원 교육은 새로운 팀원이 그들의 직무를 수행하기 위해 필요한 기술을 습득하거나 팀원 개인 발전을 위한 역량 강화와 새로운 기술과 공격자의 경향을 파악하는 전반적인 기술향상을 위해 필요하다. 팀의 전체적인 교육을 검토할 때 팀 전체의 일반적인 기술뿐만 아니라 각 팀원의 특성화된 기술을 구분하는 것이 중요하다.

다. 침해사고 대응팀의 업무

▶ 침해사고 접수

침해사고 대응팀은 기업 내 · 외부로부터의 침해사고 관련 연락의 단일 창구 역할을 수행하여야 하며, 침해사고대응 서비스를 위해 들어오는 정보를 접수(accepting), 수집(collecting), 정렬, 전달하는 기능을 제공한다.

침해사고는 email, fax, 전화, 우편 등 접수 수단에 상관없이 단일한 창구를 통해 관리가 되어야 한다. 대내외적으로 침해사고와 관련된 정보를 주고받을 수 있는 공식적인 채널이 마련되어 있어야 한다. RFC2142에서는 보안과 관련한 메일 주소를 다음과 같이 사용하기를 권고하고 있다.

security@domain.name	보안관련 사고 담당자 메일 주소
cert@domain.name	보안관련 사고 담당자 메일 주소
abuse@domain.name	네트워크 오용 담당자 메일 주소

침해사고 신고를 위한 표준화된 보고 양식을 제공하여 침해사고 처리에 필요한 모든 정보가 신고될 수 있도록 한다. 침해사고 보고 양식에는 다음과 같은 정보를 기본적으로 입력하도록 한다.

- 보고하는 사이트와 이 사고와 관련되어 통신하는 다른 집단들의 연락 정보
- 사고와 관련된 호스트의 이름과 네트워크 주소
- 사고에 대한 설명
- 사고와 관련된 세부 로그(time-zone 정보 포함)
- 이미 할당되었다면 그 할당번호

접수된 각 사고에 대해서는 고유한 할당번호를 부여하여 각각의 사고를 식별할 수 있도록 한다. 할당번호는 email의 제목이나 Fax의 표지 또는 정해진 음성 메시지에 쉽게 사용될 수 있으며, 개별 사건을 추적하고 관리하는데 사용되어질 수 있다.

▶ 침해사고 분석 및 대응

접수된 침해사고 신고 중 컴퓨터 보안 사고라고 의심되거나 확실한 사건에 대해서는 침해사고 분석 · 복구 등에 필요한 지원을 하고, 가이드를 제공한다.

침해사고 사고분석은 다음의 두 가지로 분류할 수 있다.

첫째, 특정한 사고 내에서의 분석으로써 로그파일 분석, 공격자의 행위에 의해 남겨진 자료(artifact) 분석, 사고가 발생된 소프트웨어 환경 분석, 사고 내의 상호연관관계 분석 등을 수행한다.

둘째, 사고간의 분석으로써 사고간의 관계를 고려한 구조적인 구조 분석이라고 할 수 있다. 이 분석은 일치하거나 관련이 있는 공격자 출처를 가진 별개의 사건들 사이의 연관성을 찾거나 유사한 공격 기법의 발견 등을 위해서 수행한다.

침해사고 분석 및 대응시 피해 기업 자체적인 해결이 어려운 경우 관련 ISP, 수사기관(경찰청 사이버테러대응센터, 대검찰청 인터넷범죄수사센터), 침해사고대응전문기관(한국정보보호진흥원 인터넷침해사고대응지원센터), 민간 정보보호 전문업체 등의 도움을 받도록 한다.

▶ 침해사고 예방을 위한 정보제공

침해사고 대응팀은 침해사고 발생 후 사후 대응뿐만 아니라 침해사고를 예방하기 위한 활동도 수행하여야 한다. 침해사고 예방활동은 현재의 위협들과 이러한 위협을 방어하기 위한 절차와 최신 공격 동향에 대한 정보 등을 작성 · 배포한다.

하지만 각 기업세서 자체적으로 신규 보안취약점 및 공격기법에 대해 분석하고 정보를 생성하기에는 시간과 기술 인력의 한계에 부딪치는 경우가 많다. 이런 경우에는 다음과 같은 기관들로부터 정보를 수집하여 재배포하거나 기업의 특성에 맞게 수정하여 배포할 수도 있다.

[표 11-1-1] 해킹 · 바이러스 정보제공 사이트

기관명	홈페이지	비고
국가사이버안전센터	http://www.ncsc.go.kr	국가정보원
인터넷침해사고 대응지원센터	http://www.krcert.or.kr	한국 침해사고대응팀
CERT/CC	http://www.cert.org	미국 침해사고대응팀
SecurityFocus	http://www.securityfocus.org	민간 취약점 정보제공 기관

2. 침해사고대응 관련 기관

해킹 · 바이러스 사고대응을 위한 관련기관으로는 국가정보원의 국가 사이버안전센터, 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 한국정보보호진흥원 인터넷침해사고대응지원센터 등 서비스 대상기관과 업무내용에 따라 다수의 기관이 존재하고, 이들간에는 상호협력 관

계를 유지하고 있다.

[표 11-1-2] 해킹 · 바이러스 사고 신고기관

기관명	홈페이지	전화번호	E-mail	비 고
국가정보원 국가사이버안전센터	http://www.ncsc.go.kr	국번없이 111	info@ncsc.go.kr	국가 · 공공기관 보안사고처리 · 접수
대검찰청 인터넷범죄수사센터	http://icic.sppo.go.kr	02)3480-3600	icic@icic.sppo.go.kr	컴퓨터보안사고 수사
경찰청 사이버테러대응센터	http://www.ctrc.go.kr	02)3939-112	홈페이지에서 신고	컴퓨터보안사고 수사
한국정보보호진흥원 인터넷침해사고 대응지원센터	http://www.krcert.or.kr	02)118	cert@certcc.or.kr	민간 보안사고접수 · 처리

기업에서 해킹 · 바이러스 사고 발생시 지원을 받을 수 있는 대표적인 기관으로는 해킹 · 바이러스 관련 기술적인 정보제공 및 예방 · 대응관련 기술적인 상담을 해주는 한국정보보호진흥원의 인터넷침해사고대응지원센터와 해킹으로 인한 금전적 피해 등 사이버범죄에 대한 신고를 할 수 있는 경찰청의 사이버테러대응센터가 있다.

이외에도 대학, 기업 등 국내 침해사고 대응팀들간의 컨소시엄인 한국침해사고대응팀협의회(CONCERT : CONsortium of CERTs), 금융감독원, 한국증권전산(주), 금융결제원에서 운영하는 금융 정보공유분석센터(ISAC : Information Sharing & Analysis Center) 등이 침해사고대응과 관련한 업무를 수행하고 있다.

가. 한국침해사고대응팀협의회

한국침해사고대응팀협의회(http://www.concert.or.kr)는 국내 정보통신망 침해사고 대응팀들간의 정보교류, 기술공유, 업무협조 등의 협력체계를 통하여 국내 정보통신망에 대한 침해사고를 예방하고 침해사고 발생시 피해의 확산을 방지함으로써 정보통신망의 안전한 운영에 기여하기

위해 설립되었다.

한국침해사고대응팀협의회 초기 화면
(그림 11-1-2)

한국침해사고대응팀협의회에서는 다음과 같은 업무들을 수행하고 있다.

- 정보통신망 운영기관들의 CERT 구성지원
- 침해사고 대응기술력 향상을 위한 교육 및 세미나 개최
- 신속한 정보교환을 위한 연락체계 구축
- 정보통신망 침해사고 관련 정보 및 기술 상호교환
- 국제적인 정보통신망 침해사고 대응을 위한 제반 활동

일반 기업들도 한국침해사고대응팀협의회에 가입함으로써 CERT팀 구축 · 운영을 위한 지원, 보안장비 운영경험 공유 등의 혜택을 누릴 수 있다.

나. 인터넷침해사고대응지원센터

인터넷침해사고대응지원센터(KrCERT, http://www.krcert.or.kr)는 해킹 · 바이러스 등 인터넷 침해사고의 조기탐지, 분석, 예 · 경보, 그리고 침해사고 대응활동 등을 통해 인터넷 침해사고로

인한 피해 확산 방지를 위해 한국정보보호진흥원에서 운영하고 있다.

인터넷침해사고대응지원센터 초기 화면
(그림 11-1-3)

다음은 인터넷침해사고대응지원센터의 주요 업무 내용이다.

- 365일 네트워크 모니터링을 통한 해킹 · 바이러스 예 · 경보 발령
- 해킹 · 바이러스 기법 분석 및 대처방안 배포
- 민간분야 해킹 · 바이러스 상담접수 및 기술지원
- 국내 · 외 인터넷 침해사고 관련 조직과의 공동대응 협력체계 구축

인터넷침해사고대응지원센터에서는 휴대폰 문자메시지, 메일링리스트(sec-info@certcc.or.kr) 등을 통해 해킹 · 바이러스 관련 다양한 정보를 제공하고, 예 · 경보를 발령하고 있으므로, 개인사용자들도 인터넷침해사고대응지원센터에 회원으로 가입(무료)함으로써 이러한 정보를 제공받을 수 있다.

기업들은 인터넷침해사고대응지원센터를 통해 24시간/365일 언제나 해킹 · 바이러스에 대한 일반적인 문의나 피해에 대한 조치방법에 대해 상담과 기술지원을 받을 수 있다.

다. 경찰청 사이버테러대응센터

사이버테러대응센터(http://www.ctrc.go.kr)는 사이버테러형 범죄(해킹 · 바이러스 등)의 수사,

범죄예방, 수사기법개발 등을 위해 경찰청에서 운영하고 있다. 경찰은 경찰청 내의 사이버테러대응센터 뿐만 아니라 각 지방 경찰청에도 사이버수사대를 두고 있어 전국적인 사이버 수사 조직을 가지고 있다.

사이버테러대응센터 초기 화면
(그림 11-1-4)

사이버테러대응센터의 주요 업무로는 사이버테러의 탐지 · 추적 및 경보 등 조치, 사이버범죄의 수사 및 지도, 사이버테러관련 수사기법의 연구 · 개발, 국제경찰기구 등과의 대(對)사이버테러 협력 등이 있다.

기업에서는 기업 중요자료의 유출, 정상적인 서비스를 방해하는 서비스거부공격 등의 사건이 발생되었을 경우 공격자 추적과 법적인 조치를 위해 사이버테러대응센터의 도움을 받을 수 있다. 사이버범죄에 대한 신고는 사이버테러대응센터 홈페이지(http://www.ctrc.go.kr)를 통해 인터넷으로 신고하거나 가까운 경찰관서에 신고할 수 있다.

3. 침해사고대응 및 복구 절차

인터넷 웜이나 서비스거부공격과 같은 대규모 인터넷 침해사고에 대한 신속한 대응은 피해를 최소화한다. 이러한 신속한 대응은 사전에 준비된 침해사고대응체계와 절차서에 따라 구성원들이 훈련되어 있어야만 가능하다. 따라서, 각 기업에서는 다양한 경우에 대비한 사고대응절차를 사전에 마련하고, 각 기업 담당자들은 이러한 대응절차를 숙지하고 있어야만 한다.

일반적으로 사고 처리자는 소방관에 비유되기도 하는데, 화재시 소방관의 사소한 실수나 조급함이 더 큰 피해를 초래할 수도 있다. 마찬가지로 사고처리자도 신중하게 사고처리에 임해야 하며, 주어진 절차에 의해 수행하여야 한다. 사고 처리자가 일반적으로 범하기 쉬우면서도 반드시 지켜야 하는 행동수칙은 다음과 같다.

- 서두르지 말라.
- 모든 것을 기록하라.
- 도움을 줄 수 있는 사람들의 연락처를 유지하라.
- 사건에 대해 반드시 알아야 할 사람에게만 알려라.
- 해킹당한 컴퓨터로 통신하지 말라.
- 해킹당한 컴퓨터를 네트워크에서 분리하라.
- 가능한 빨리 백업 받으라.
- 공격당한 문제점(취약점)을 제거하라.
- 백업본으로 재설치하고, 이상여부를 살핀다.
- 사고경험을 익혀, 유사 사고에 대비한다.

발생된 침해사고의 종류와 기업의 보안정책 및 침해사고대응지침서에 따라 대응절차도 다를 수 있지만 일반적인 침해사고 대응절차를 소개하기로 한다. 일반적으로 기업에서 침해사고 발생시 단계별 사고대응절차는 [표 11-1-5]과 같다.

[표 11-1-3] 단계별 사고대응절차

사전준비
↓
사고인지
↓
침해사고 확산방지
↓
시스템 분석과 원인제거
↓
시스템 복구 및 서비스 재개
↓
보고서 작성

가. 사전준비

사전준비 단계에서는 침해사고가 실제 발생하기 이전에 취하는 행동으로 신속한 사고처리를 위한 준비단계라고 할 수 있다. 사전준비 단계에서 취해야 하는 행동은 주로 예방을 위한 활동인데 다음과 같은 사항들이 있을 수 있다.

- 침해사고 대응팀 구성 및 훈련
- 침해사고 대응을 위한 재난복구 계획 마련
- 비상연락체계 구축
- 네트워크 모니터링 센터 운영(24시간/365일)
- 침해사고 접수 창구 마련(이메일, 웹, 전화 등)
- 신규 취약점이나 바이러스 정보수집

나. 사고인지

실제 인터넷 침해사고가 발생되었을 때 기업 담당자는 다음과 같은 채널을 통해 사고사실을 인지할 수 있다.

- 내부 직원으로부터의 신고(전화, 홈페이지, 이메일 등)
- 네트워크 장비(라우터, 스위치)의 과부하 확인(CPU, BPS, PPS 등)
- 네트워크 장비 및 고객 장비의 장애 유무 확인(ICMP등)
- 침입탐지시스템(IDS) 등 보안장비를 통한 침입 확인
- 수사기관, KISA 등 국내 유관기관으로부터의 신고
- 국외 ISP 등 국외 피해기관으로부터의 신고

침해사고를 접수시 신고자로부터 장애 상황에 대해 충분히 설명을 받고 침해사고의 종류, 침해범위 및 규모를 판단하도록 한다.

사고의 범위나 피해가 큰 경우에는 해당사고에 대한 대응을 위해 전담반을 구성하여 운영한다. 이 경우 해당 사고의 유형에 따라 관련 분야 전문가들로 구성하고 필요에 따라서는 외부 전문가도

활용할 수 있다. 또한, 필요에 따라 내부의 관리자나 한국정보보호진흥원, 경찰청 등 국내 침해사고대응 기관에 연락을 취하여 도움을 받을 수도 있다.

다. 침해사고 확산 방지

최근의 인터넷 웜은 수 십분 내에 전 세계의 취약한 서버를 감염시킬 정도로 전파속도가 빠르므로 침해사고의 확산을 방지하기 위한 신속한 조치가 필요하다. 필요에 따라서는 감염된 서버를 기업 네트워크로부터 분리시키거나 네트워크 접근통제를 실시한다.

그리고 해킹피해시스템에는 Sniffer와 같은 악성코드가 깔려 내부 네트워크의 트래픽을 모니터링하여 사용자 아이디와 패스워드를 가로채는 경우가 많다. 이 경우 피해가 확인된 시스템 뿐만 아니라 동일 네트워크의 다른 시스템들도 공격을 당했을 가능성이 많으므로 주변의 시스템들도 로그분석을 통해 피해 유무를 확인하여야 한다.

라. 시스템 분석과 원인제거

해킹으로 인한 피해확산에 대한 조치를 완료한 후에는 본격적으로 해킹 피해의 원인과 피해정도에 대한 상세한 분석에 들어간다. 해킹 피해 분석은 피해 시스템에서 직접 수행할 수도 있지만 가급적이면 이미지 백업을 받은 후 백업본에서 분석하는 것이 바람직하다. 백업본은 향후 법적인 문제 발생시 법적인 증거자료로도 제출될 수 있도록 내용의 변경이 없도록 주의하여야 한다.

해킹 피해 분석 기법에 대해서는 "5. 침해사고 피해시스템 분석 기법" 에서 자세히 다루기로 한다. 시스템 분석을 통해 공격을 받은 원인이 밝혀지면 해당 취약점에 대한 보호대책을 마련하여 향후 피해가 다시 발생되지 않도록 조치하여야 한다. 해킹 피해 발생시에는 단편적으로 피해 시스템에 대한 분석과 조치로 끝내지 않고 기업전체의 정보시스템 운영환경 파악, 보안 위협요인 식별 및 평가, 보안취약점 점검 등을 통해 기업의 보안 위험수준을 평가하고 이에 대해 관리적, 기술적, 물리적인 보안대책을 마련하는 것이 바람직하다.

마. 시스템 복구 및 서비스 재개

해킹 피해분석과 보안대책을 수립한 후에는 피해시스템을 복구하고 서비스를 중단했을 경우 서비스를 재개한다.

피해시스템을 복구할 경우 해킹 당하기 이전의 백업본을 사용하는 것이 바람직하고, 복구된 시스템에 공격자가 남겨 놓은 백도어 프로그램이 존재하지 않는지 주의 깊게 살펴보아야 한다. 일반적으로 공격자는 시스템 침입 후 재침입을 용이하게 하기 위하여 백도어 프로그램을 시스템 곳곳에 숨겨놓는 경우가 많다. 완전한 백도어 프로그램의 탐색이 불가능할 경우에는 시스템을 재설치하여야 하는 경우가 발생될 수도 있다.

시스템 복구 후에는 일정기간 동안 해당 시스템에 대한 모니터링을 통해 해당 시스템에 대한 재침입시도 또는 비정상적인 작동에 대해 감시하고 대응할 수 있도록 하여야 한다.

바. 보고서 작성

침해사고에 대한 전 대응과정을 거친 후에는 사고대응의 전과정을 상세히 기록하여 보고서로 작성할 필요가 있다. 이 보고서는 법적인 증거자료로도 사용될 수 있을 뿐만 아니라 침해사고대응팀원 간의 사고대응경험을 공유하는데도 유용하게 사용될 수 있다.

사고대응 보고서에는 해당 침해사고에 대한 원인과 대응뿐 아니라 보다 안전한 기업의 정보시스템 환경을 구축하기 위한 중장기적인 정보보호 대책에 대한 건의도 추가하여 상급 관리자 또는 경영진에 보고하도록 한다.

4. 침해사고 피해시스템 분석 기법

피해 시스템을 분석한다는 것은 결국 공격의 흔적 즉, 증거를 찾아내는 과정으로 여기에서는 공격자들이 주로 사용하는 루트킷, 백도어, 트로이에 대한 지식을 바탕으로 피해시스템 분석 방법

을 설명한다.

가. 시스템 상태 자료 수집

아래와 같은 명령을 사용하여 피해 시스템의 현재 프로세스, 열린 파일, 로그인 사용자 정보, 네트워크 상태 등에 대해 따로 기록하여 보관한다. 프로세스 상태, 네트워크 접속 상태, 현재 로그인 정보, /tmp 파일의 내용 등은 시스템 리부팅 후에는 사라지는 휘발성 정보이므로 피해시스템 분석에 앞서 반드시 수집하여야 한다.

- ps -elf 또는 ps -aux : 현재 시스템에서 수행중인 프로세스 정보
- netstat -an : 현재 네트워크 활동에 대한 정보
- lsof : ps와 netstat를 대체할 수 있는 것으로 현 시스템의 모든 프로세스와 프로세스가 사용하는 포트 및 열린 파일 정보
- last : 사용자, 터미널에 대한 로그인, 로그아웃 정보
- who : 현재 시스템에 있는 사용자 정보
- find / -ctime -ndays -ls : ndays 이전 시점부터 현재까지 ctime이 변경된 모든 파일에 대한 정보
  ※ 주의 : 이 명령어는 파일의 접근시간(atime)을 변경시키므로, 침입자가 어떠한 파일에 접근했는지 알고 싶은 경우에는 사용하지 않도록 한다.

- nmap : 네트워크 점검 도구인 nmap을 이용하여 원격에서 피해 시스템의 열린 포트 점검
  # nmap -sT -p 1-65535 xxx.xxx.xxx.xxx(피해시스템 IP 주소)
  # nmap -sU -p 1-65535 xxx.xxx.xxx.xxx(피해시스템 IP 주소)

나. 시스템 상태 자료 분석

(1) 수집한 정보 분석

- ps : sniffer 또는 취약점 스캔 프로그램 등 공격 프로그램이 실행되고 있는지 확인
- netstat : 서비스하지 않는 포트가 열려 있는지 또는 이상한 사이트로 접속이 있는지 확인
- lsof : 공격 프로그램이 실행되고 있는지 또는 서비스하지 않는 포트가 열려 있는지 확인 (ps와 netstat 기능 대체)

- last : 사용하지 않는 계정 또는 이상한 사이트에서 로그인한 정보가 있는지 확인
- who : 현재 누가 접속해 있었는지 확인
- nmap 스캔결과 : 네트워크 백도어를 가장 빨리 찾을 수 있는 방법으로, 피해 시스템에 이상한 포트가 열려있는지를 확인

(2) 공격 시간대를 중심으로 분석

① 대략적인 공격시간대를 알 경우

대부분의 공격 시간대는 사고 접수 시간이나 사고 내용에 남은 로그를 중심으로 알 수 있다.

예) 로그에 남은 공격 시간이 3월 1일이고 시스템 분석을 3월 6일에 한다면 아래와 같은 명령을 사용하여 현재로부터 6일 이전까지 변경된 파일을 점검할 때

```
# find / -mtime -6 -ls
```

② 공격시간대를 알 수 없는 경우

공격자는 흔히 시스템 파일의 변화를 숨기기 위해 시간을 수정하므로 이러한 경우에는 파일의 inode 변경시간(ctime)을 점검한다.

예) 지난 n 날짜동안 수정된 inode를 갖는 모든 파일을 점검할 때

```
# find / -ctime -ndays -ls
```

(3) 온라인 분석시 주요 정보 관리

온라인으로 피해 시스템을 직접 분석할 경우에는 다음과 같은 주요 정보를 다른 안전한 시스템에 복사해 둔다.

- 시스템의 모든 로그 파일
- inetd.conf 파일, 패스워드 파일, 기타 주요 설정 파일
- 주요 디렉토리에 대한 "ls -alt" 결과값 (예: /dev/, /, /etc 등)
- "find / -ctime -ndays -ls" 결과값
- 침입자가 사용한 디렉토리 파일
- 기타 시스템을 분석하면서 나온 정보들

다. 잘 알려진 공격기법에 대한 분석

공격자가 주로 사용하는 해킹툴 및 백도어, 루트킷 등에 대한 사전 지식을 바탕으로 분석하는 방법으로 공격흔적 및 공격방법을 쉽게 발견할 수 있다.

(1) /etc/passwd 파일 점검

관리자가 생성하지 않은 새로운 계정이나, uid=0인 계정, 패스워드가 없는 계정이 있는지 확인한다.

```
# ls -al /etc/passwd
```

(2) history 파일 점검

공격자가 history 파일을 삭제하지 않았다면, 이 파일에서 상당히 유용한 정보를 얻을 수 있다. 따라서 루트나 의심이 가는 사용자의 홈 디렉토리에서 history 파일을 점검한다.

```
Linux : # more bash_history
Solaris : # more .history
```

(3) 숨겨진 디렉토리 점검

공격자들은 주로 "." 이나 ".." 으로 시작하는 디렉토리를 만들어 사용하는데 이는 관리자가 아무런 옵션 없이 "ls" 명령을 사용했을때는 보이지 않게 된다. 따라서 다음과 같은 명령을 사용하여 숨겨진 디렉토리를 찾는다.

```
# find / -name "..*" -print    또는
# find / -name ".*" -print
```

(4) 공격자가 자주 사용하는 디렉토리 점검

공격자들은 주로 /dev, /var, 각종 /tmp 디렉토리 등 일반적으로 파일이 아주 많은 디렉토리나

누구든 쓰기 가능한 디렉토리에 작업 디렉토리를 만드는 경우가 많다.
특히 /dev 디렉토리는 루트킷이나 백도어 설정파일의 디폴트 디렉토리로 많이 사용되므로 아래의 명령어를 사용하여 점검할 수 있다.

```
# find /dev -type f -print
```

※ /dev 디렉토리는 보통 일반파일이 존재하지 않으므로 일반파일이 있는지를 검사한다.

(5) 백도어 파일 점검

사용자 홈 디렉토리의 ".rhosts" 파일이나 ".forward" 파일, etc/inetd.conf 파일, /etc/services 파일, /etc/rc.d/ 디렉토리내의 파일들에 이상한 포트나 서비스가 열려 있는지 점검한다.

(6) 시스템날짜 변경 확인

/bin 디렉토리나 /sbin 디렉토리 등 시스템 파일들의 날짜가 변경되었는지를 점검한다.

```
# ls -alct /bin    또는
# ls -alct /sbin
```

제2절 스팸메일

1. 관련기관 소개

가. 스팸 수신

불법스팸대응센터(http://www.spamcop.or.kr)는 국민의 스팸관련 상담 및 불법스팸신고를 원활히 처리하기 위하여 2003년 1월 24일 한국정보보호진흥원내 개설하였다.

당 센터는 일반 국민에게 스팸차단 방법 등을 안내하고,「정보통신망이용촉진및정보보호등에관

한법률」에서 정하고 있는 불법스팸의 신고를 연중 접수하여 처리하고 있다.

이외에도 스팸피해를 사전에 예방하기 위한 각종 인식제고 활동들을 벌이고 있으며, 스팸방지 프로그램을 개발 배포하는 등의 기술적인 대책 마련에도 주력하고 있다. 또한 스팸규제 강화를 위한 법 제도 개선방안을 연구하고, 스팸방지대책을 수립 시행하는 한편, 한국발 스팸문제를 해소하기 위해 외국의 스팸대응기구와의 국제협력도 추진하고 있다.

나. 스팸 릴레이

해킹 · 바이러스 예방/대응 업무를 주로 수행하는 한국정보보호진흥원 내 인터넷침해사고대응지원센터(http://www.krcert.or.kr)에서 스팸 릴레이에 대한 민원도 함께 접수받아 원격점검 및 차단 정보를 제공하고 있다.

2. 사고신고 및 대응요령

가. 스팸 수신

> 원치 않는 스팸을 수신하였을 때에는 자신이 가입한 이메일서비스업체나 이동통신사에 1차 신고할 수 있으며, 그 중 현행 스팸규제법인 정보통신망법을 위반한 스팸에 대해서는 관련 자료를 첨부하여 불법스팸대응센터에 신고할 수 있다.

(1) 이메일서비스업체 및 이동통신사 신고 방법

① 이메일 스팸 : **[편지읽기]**에서 해당 스팸을 선택한 후 상단 메뉴 바에서 **[스팸신고]**를 선택
② 휴대폰 스팸 : 이용자의 휴대폰 단말기에서 국번없이 "114"를 누르면, 해당 이동통신사 고객센터로 연결됨

(2) 불법스팸대응센터 신고 방법

① 민원접수 방법 전화

전 화	02-405-4774
인 터 넷	http://www.spamcop.or.kr, 불법스팸대응센터.kr
우 편	서울시 송파구 가락동 78번지 IT 벤처타워 서관 한국정보보호 진흥원 불법스팸대응센터 (우편번호 : 138-803)
팩 스	02-405-4789
방 문	위치 : 지하철 8호선 가락시장역 2번 출구 경찰병원 방향 400m

[전화상담 가능 시간]

▣ 월 ~ 금 : 09:00 ~ 18:00(11월 - 2월은 17:00까지)

▣ 토 요 일 : 09:00 ~ 12:00

▣ 휴 무 일 : 일요일 · 법정공휴일 및 두 번째 · 네번째 토요일

※ 온라인 상담/신고접수는 24시간 가능

② 민원접수시 증거자료 첨부요령

● 이메일

- 정보통신망법에서 금지하고 있는 행위를 한 영리목적의 광고메일을 수신하였을 경우, 해당 메일을 원본을 손상하지 않도록 "*.eml" 파일로 저장한 후 불법스팸대응센터 홈페이지 (http://www.spamcop.or.kr)로 신고 접수한다.

예) 수신거부의사를 전달한 이후에도 지속적으로 광고메일이 수신될 경우,

① 처음 수신한 광고메일

② 그에 대해 수신거부의사를 밝힌 메일이나 증거화면 캡쳐(수신거부한 날짜 포함)

③ 수신거부 이후 재수신된 스팸메일(날짜 포함) 등을 첨부하여야 한다.

● 휴대폰 문자메시지

- 정보통신망법에서 금지하고 있는 행위를 한 영리목적의 광고메시지를 수신하였을 경우, 해당 문자메시지를 스캔하여 그림파일로 저장한 후 불법스팸대응센터 홈페이지(http://www.spamcop.or.kr)로 신고 접수한다.

● 광고성 프로그램

- 광고성 프로그램 설치시 해당 프로그램의 용도 및 삭제방법을 명확히 고지하지 않거나 사전 동의를 받지 않고 설치한 경우 등 정보통신망법 위반행위에 대해 관련 증거화면을 캡쳐하여 불법스팸대응센터 홈페이지(http://www.spamcop.or.kr)로 신고접수한다.

● IP 팝업 광고

- 정보통신망법에서 규정하고 있는 광고성 정보 명시 의무를 위반하였을 경우, 해당 광고를 화면 캡쳐하여 불법스팸대응센터 홈페이지(http://www.spamcop.or.kr)로 신고접수한다.

나. 스팸 릴레이

● 한국정보보호진흥원내 인터넷침해사고대응지원센터
(http://www.krcert.or.kr/secureyourserver)에서 스팸 릴레이 여부 점검 서비스를 받는다.

- 서비스 페이지에 메일서버 담당자 이름, 이메일 주소, 전화 연락처, 점검하고자 하는 메일서버의 IP주소를 입력한 후에 '점검시작' 버튼을 클릭하면, 자동으로 스팸릴레이 여부를 점검해준다.

● 스팸릴레이 점검 후 릴레이가 되고 있을 경우, 한국정보보호진흥원 내 인터넷침해사고대응지원센터에서 제공하는 "메일서버의 스팸릴레이 방지 설정 방법"(http://www.krcert.or.kr/paper/tr2002/tr2002_04/spam.htm) 등을 참조하여 릴레이를 차단할 수 있다.

메일서버의 스팸릴레이 점검서비스 페이지
(그림 11-3-1)

제3절 불건전정보 유통

1. 불법 · 청소년유해정보신고센터 "인터넷119" 소개

불법 · 청소년유해정보신고센터 "인터넷119"(http://www.internet119.or.kr)는 정보통신 이용자(네티즌)들이 불법, 청소년 유해정보를 신고할 수 있는 사이트이다.

"인터넷119"에 신고된 내용은 정보통신윤리위원회의 심의를 통하여 불법 또는 청소년에게 유해한 정보로 결정할 경우 인터넷서비스제공자(ISP), PC통신사 등을 통하여 시정되도록 조치하고 있다.

아울러 신고물이 정보통신윤리위원회 심의대상이 아닌 경우 그 성격에 따라서 검찰청 · 경찰청 · 개인정보분쟁조정위원회 등 관련기구에 전달된다. 정보통신윤리위원회는 정보통신망의 각종 불건전정보의 효과적인 유통방지를 위하여 청소년보호위원회, 검찰, 경찰 등 관련 기관과의 긴밀한 협력체제를 유지하고 있다. 또한 특히 인터넷의 해외 불법 · 청소년유해정보 대응을 위하여 해외 관련기구 및 단체와 국제협력체제를 구축하여 운영하고 있다.

인터넷119 초기화면
(그림 11-4-1)

"인터넷119"의 주요 업무는 다음과 같다.

- 불법 · 청소년유해정보 신고 접수 및 조치
- 손쉬운 신고 프로그램(인터넷파랑새) 제공
- 사이버패트롤(불법 · 유해정보 신고 자원봉사자) 커뮤니티 활동 지원
- 건전한 정보를 이용하기 위한 각종 정보 제공
- 인터넷 피해, 사이버 범죄 등 분야별 신고 사이트로 접속 지원
- 해외기관과의 불법 · 청소년유해정보에 대한 대응 공조

2. 신고 요령

인터넷119에는 음란, 명예회손, 폭력/잔혹/혐오, 사행심조장, 사회질서 등에 관련된 내용을 신고할 수 있다.

불건전정보에 대한 신고시에는 사실을 입증할 내용을 반드시 첨부하여야 한다. 정확한 증거자료를 주지 않거나 허위 신고된 경우 처리가 불가능하니 다음의 사항들을 첨부하여 신고하도록 한다.

- o 해당화면 갈무리(화면 캡쳐)
- o 정보제공자(개인 및 회사명 또는 아이디)
- o 이메일
- o 유해정보제공 주소(사이트 또는 PC통신상의 위치)

인터넷119 신고화면
(그림 11-4-2)

신고하고자 하는 사실을 입증하기 위해서는 증거자료를 반드시 첨부하여야 하는데 증거자료를 갈무리하는 방법은 다음과 같다.

텍스트 화면 및 그림 화면 저장하기

1. 신고하고자 하는 정보의 화면을 띄우고〈Alt〉 + 〈Print Screen〉
2. 시작메뉴 ⇨ 프로그램 ⇨ 보조 프로그램 ⇨ 그림판
3. 그림판 메뉴의 〈편집〉 ⇨ 〈붙여넣기〉
4. 새 파일명으로 저장

대화방에서 대화 내용 저장하기

1. 대화방 화면에서 〈갈무리 시작〉 또는 〈대화저장〉클릭
2. 대화 내용을 저장할 창에 저장경로 지정과 파일 이름 입력 후 〈저장〉
3. 그림판 메뉴의 〈편집〉 ⇨ 〈붙여넣기〉
4. 윈도우 탐색기를 열어 저장된 파일 이름 확인(저장된 파일에 상대방 아이디, 대화내용, 대화시간 등 기록)

신고할 내용

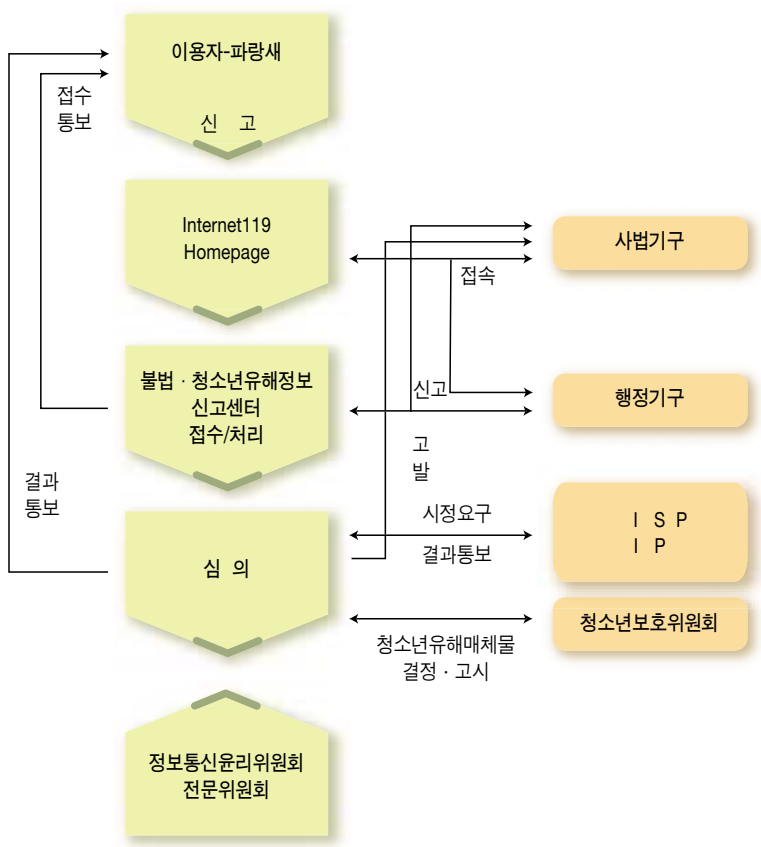
1. 언 제 : 발생시간
2. 어디서 : 유해정보 제공 주소(인터넷 사이트 또는 PC통신상의 위치)
3. 누 가 : 정보제공자(개인 및 회사명 또는 아이디)
4. 무엇을/어떻게 : 불건전정보 내용(구체적)

인터넷119에서는 인터넷 이용자에게 불법, 청소년유해정보 신고의 편의성을 제공하고 신고활성화 및 신고확인, 통보 자동화를 통한 신고처리 체계 효율화를 높이기 위해서 신고전용 S/W인 "인터넷파랑새"를 배포하고 있다

인터넷 파랑새
(그림 11-4-3)

인터넷파랑새는 다음 사이트에서 다운로드 받아 설치할 수 있다.
http://www.internet119.or.kr/iblue/iblue_download.html

신고된 불건전정보에 대한 처리는 다음의 절차를 통해 이루어지며 그 결과를 신고자에게 통보하게 된다.



불건전정보 사고처리 절차
(그림 11-4-4)

c o n t e n t s

제12장
정보보호 관리

인터넷의 급속한 발달로 인하여 해킹과 정보보호의 역기능으로 인한 기업의 정보유출 및 금전적인 손실이 점차로 커지고 있다. 조직의 정보자산에 대한 각종 정보위협에 효과적으로 대응하기 위해서는 조직차원에서의 체계적 · 지속적인 관리활동이 필요하다. 안전한 전자상거래 활성화 도모 및 정보통신환경의 안전 · 신뢰성 확보에 대한 중요성 대두되고 있다.

이러한 정보보호의 역기능으로부터 주요 정보를 보호하고 정보보호에 대한 체계적인 관리의 필요성이 대두되면서 국외는 물론 국내에서도 정보보호관리에 대한 관심이 고조되고 있으며, 정보보호관리를 위한 체계적인 노력이 확산되고 있다.

정보보호관리체계[21](관리 프레임워크)는 조직 내에서 정보보호 임무를 관리하기 위한 수단이다. 또한 정보보호관리체계는 보안 프로그램을 생성하고 그 목표를 설정하며, 책임을 부여하는 등과 같은 최고 경영자의 지시나 특정한 시스템을 위한 정보보호정책 등을 포함한다. 이러한 정보보호관리체계는 최고 경영자가 예산을 기획하거나, 경쟁목표를 선정하고, 기술 자원이나 정보를 보호하는데 관련된 조직적 전략 수립과 같은 선택적 상황에서 의사결정을 내리는데 도움을 준다.

국내의 기업들이 지금까지 기술적인 방법으로만 전자적인 침해에 대응해 왔으나 한계를 느끼고 있다. 기업의 경영진이 정보보호관리에 대한 관심이 높아지고 궁극적으로 전사적인 정보보호관리의 필요성을 느끼고 있다. 최근들어, 영국표준인 BS7799[22]와 한국정보보호진흥원에서 수행하고 있는 정보보호관리체계인증제도[23](정보통신망이용촉진및정보보호등에관한법률 제47조)에 관심을 갖고 조직의 정보보호관리체계 수립을 진행중이며, 정보보호관리체계를 수립함으로써 기업의 전자적/물리적 침해사고를 미연에 방지할 수 있고, 취약성 분석, 위험분석 등의 정보보호를 위한 정보기술의 향상 및 정보보호 역량 강화 및 이를 통하여 고객으로부터 신뢰성을 확보하고 있다. 이러한 체계수립을 통하여 위험수준의 가시적 표현으로 관리자와 사용자의 보안 의식을 고취시키고 있다.

본 장은 정보보호관리체계를 수립하기 위하여 필요한 정보보호정책 수립, 정보보호관리체계범위 설정, 위험관리, 구현 및 사후관리의 정보보호관리체계의 생명주기에 대한 내용을 다룬다. 정보보호관리에 필요한 통제항목인 정보보호정책, 정보보호조직, 외부자보안, 정보자산분류, 정보보

21) 조직이 보유하고 있는 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립하여 지속적으로 관리 · 운영하는 시스템

22) BSI (British Standards Institute)에서 개발한 정보보호관리 지침서인 BS7799 Part 1, 2에 의해 제3자 인증제도 시행

23) 정보통신서비스제공자 및 정보통신서비스를 제공하기 위한 물리적 시설을 제공하는자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 수립 · 운영하고 있는 기술적 · 물리적 보호조치를 포함한 종합적 관리체계가 당해서비스에 적합한지에 관하여 인증을 받을 수 있음

호교육 및 훈련, 인적보안, 물리적보안, 시스템개발보안, 암호통제, 접근통제, 운영관리, 전자거래보안, 보안사고관리, 검토 · 모니터링 감사 및 업무연속성관리의 내용은 한국정보보호진흥원 홈페이지(http://www.kisa.or.kr/isms)을 참조하여 활용하기를 바란다.

제1절 정보보호정책 수립

1. 정보보호정책 수립

조직의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과, 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.

가. 정보보호정책의 정의

정보보호정책은 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술이다. 또한 정보보호 임무를 관리하기 위한 수단이다.

나. 정보보호정책의 필요성

정보보호와 관련된 결정은 대부분 정보보호 관리자가 네트워크의 안전여부, 제공기능, 사용하기 쉬운 방법에 대해 결정했을 때에 만들어진다. 정보보호정책의 목표를 결정하지 않고서는 보안에 관하여 적절한 결정을 할 수 없다. 정보보호 목표를 결정할 때까지는 무엇을 점검하고 무엇을 제한할 것인지를 전혀 알지 못하기 때문에 어떤 보안도구도 효과적으로 사용할 수 없다.

다. 정보보호정책의 목표

(1) 정보보호정책의 목표

조직의 정보보호정책 목표는 조직이 달성하고자하는 목표와 달성 방법(전략), 그리고 목표달성

을 위한 정책을 조직의 각 단계 및 사업 단위 또는 부서별로 정의하여야 하며, 효율적인 정보보호 정책을 위해서 각각의 조직 수준과 사업 단위별로 다양한 목표, 전략, 정책을 수립하여야 한다.

(2) 목표의 선정 기준

조직의 특성을 고려하여야 한다. 정부 기관, 공공 기관, 기업, 기업, 기업내의 부서, 개인 등 조직의 규모와 정보시스템의 활용 특성 등 비용 효과적인 보안 목적을 달성할 수 있도록 정책 적용의 대상이 되는 조직을 충분히 파악하여야 한다. 둘째, 새롭게 제정 또는 개정되는 보안 정책은 기존의 상위 정책이나 규칙, 법령 등과 부합되어야 한다. 조직이 계층 구조로 이루어져 있고 단위 조직별로 정책을 가질 경우, 상부 조직의 정책을 준수하면서 자신의 환경에 맞게 세분화 하여야 한다. 정부기관이나 공공조직 및 법에 적용되는 일반기업도 자체적인 정책을 제정하기 전에 국가의 법령이나 정책을 기반으로 하여야 한다.

정보보호 목표를 선정할 때 다음과 같은 내용을 고려해야 한다.

- 서비스제공 : 사용자에게 제공하는 서비스의 이점이 위험의 비중보다 크다면 정보보호관리자는 사용자들이 위험으로부터 서비스를 안전하게 사용할 수 있도록 보호대책을 수립하여야 한다.
- 용이성 : 누구나 쉽게 시스템에 접근하여 사용할 수 있다면 사용하기에 편리할지 모르지만, 각종 위험으로부터 완전히 노출되어 있다고 해도 과언이 아니다. 따라서, 정보보호관리자는 시스템 사용의 용이성이 다소 떨어지더라도 시스템의 안전을 최우선 과제로 선정해야 한다.
- 정보보호 비용과 손실위험
  - 정보보호를 하기 위해서는 비용이 많이 소용된다. 즉, 재정상(하드웨어 보안 장치의 비용, 침입차단시스템이나 패스워드 생성기 같은 소프트웨어 구입비용), 실행상(암 · 복호화에 걸리는 시간), 그리고 용이성 등에 대한 비용이 있다.
  - 많은 손실위험들이 존재하고 있다. 사생활에 대한 손실(권한이 없는 사용자가 정보를 읽는 것), 정보의 손실(정보의 변조 또는 삭제), 그리고 서비스에 대한 손실 (즉, 데이터의 저장 장소가 가득 찼거나 컴퓨터 사용자원 감소, 그리고 네트워크 접근의 부인) 등이 있다.
  - 각 비용의 형태는 손실의 형태에 따라 신중히 결정해야 한다. 정보보호의 목표는 "정보보호정책"라 불리는 정보보호 규칙을 통해 모든 사용자와 운영 직원, 그리고 관리자들간에 정보를 전달하는 것이다. 정보보호정책의 영역이 정보 기술, 저장된 정보, 기술에 의해 조작되는 정보의 모든 형태를 포함한다.

라. 정보보호정책의 내용

(1) 조직의 정책은 최소한의 표준을 포함하여야 한다.

- 필요한 보호의 수준에 따른 자산의 분류
- 비인가된 접근으로부터의 정보 보호 원칙
- 정보의 기밀성 보장
- 정보의 무결성 유지
- 정보 및 정보시스템의 가용성에 관한 사업 요구사항
- 물리적, 논리적, 환경적 보안 및 통신보안
- 준수하여야 할 법, 규정 및 계약 요구사항
- 시스템 개발 및 유지 방법론
- 비상대책 계획의 수립, 유지, 점검
- 모든 직원에 대한 정보보호 교육훈련
- 정보시스템 정책 위반에 대한 징계 또는 처벌
- 정보시스템 보안사고 보고 및 조사
- 준수해야 할 표준, 관례 및 절차와 바이러스 방지, 패스워드, 암호화를 포함하는 정보보호 정책 지원 수단의 구현

(2) 정보보호정책의 특징은 다음과 같다.

- 수용 가능한 지침 또는 다른 적절한 방법을 수립하고 시스템 관리절차를 통해 구현이 가능해야 한다.
- 예방이 기술적으로 불가능한곳에서 인가에 의해 적절한 경우에 보안도구가 실행 가능해야 한다.
- 사용자, 관리자, 기술요원에 대한 책임 영역이 명확하게 정의되어야 한다.

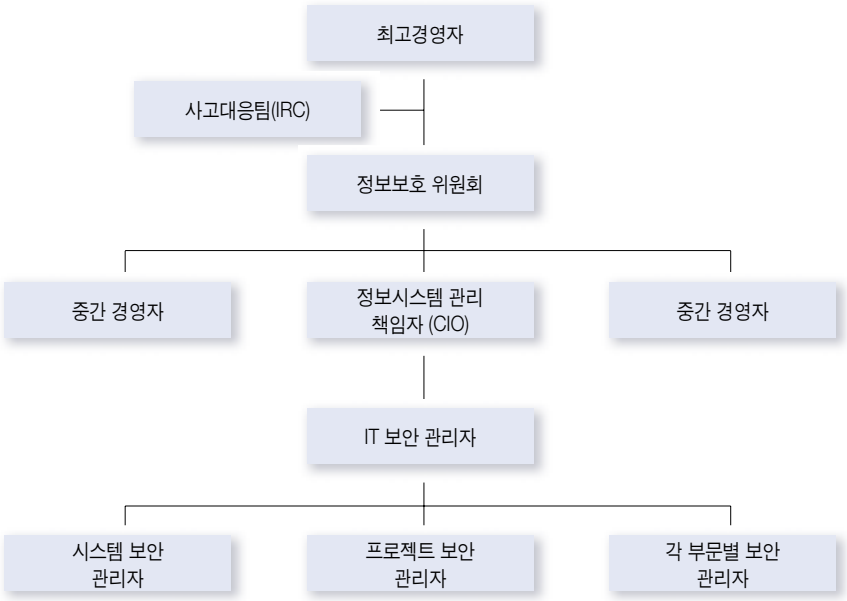
2. 조직 및 책임의 역할

가. 정보보호조직

정보보호조직은 적합한 정보보호정책을 계획, 구현, 승인, 감독할 수 있는 조직 체계를 수립하여야 한다.

모든 조직은 독자적인 체계를 가지고 있으며, 이에 적합한 방식으로 정보보호와 관련된 직무를 할당하여야 한다. 아래의 정보보호조직의 구성의 예는 일반적인 예시를 들은 것으로 모든 조직에 적용되지 않고 조직의 특성과 환경에 맞게 재구성된다.

정보보호조직의 구성 예
(그림 12-1-1)



(1) 사고대응팀 / 정보보호 위원회의 역할

- 전략적 보안 계획과 관련하여 IT운영위원회에 조언
- IT 전략적 지원에 관련하여 조직 IT 정보보호정책을 수립하고 IT 운영위원회로부터 승인획득
- 조직 IT 정보보호정책을 ITP보안 프로그램으로 전환
- ITP보안 프로그램 실행을 모니터링
- 조직 ITP보안 정책의 유효성 검토
- IT 보안 문제 인식 촉진
- 계획 프로세스를 지원 및 IT 보안 프로그램 실행을 지원하는데 필요한 자원(인력, 예산, 지식 등)에 입각하여 조언

(2) 정보시스템 관리 책임자의 주요 임무

- IT 보안 프로그램 실행을 감독
- 정보보호 관리팀 및 조직 정보보호 임원에 대한 연락 및 보고
- 조직 IT 보안 정책과 지침을 유지
- 사고 조사 조정
- 조직의 전반적인 보안 인식 프로그램 관리
- IT 프로젝트 및 시스템 보안 담당의 권한 결정

(3) 프로젝트 보안 담당과 시스템 보안 담당의 주요 임무

- 정보보호 관리팀 및 조직 ITP보안 담당에 대한 연락 및 보고
- IT 프로젝트 또는 시스템 보안 정책을 수립, 유지
- 정보보호 계획을 개발, 구현
- IT 대책의 구현 및 사용을 모니터링
- 사고조사의 착수, 지원

나. 책임의 설정

구성원의 역할과 책임 및 권한을 명확히 규정하여 모든 직원이 이를 이해하도록 한다. 각각의 직책에 대한 책임은 다음과 같다.

[표 12-1-1] 직책별 책임

직 책	책 임
최고경영자	정보보호를 위한 총괄책임이 있다.
정보시스템 정보보호 관리자	조직의 정보보호 정책, 표준, 대책, 실무 절차를 설계, 구현, 관리, 조사할 책임이 있다.
데이터 관리자	정보시스템에 저장된 데이터의 정확성과 무결성을 유지하고 데이터의 중요성 및 분류를 결정할 책임이 있다.
프로세스 관리자	해당 정보시스템에 대한 조직의 정보보호 정책에 따라 적절한 보안을 보증할 책임이 있다.
기술지원 인력	보안대책의 구현에 대하여 조언할 책임이 있다.
사용자	조직의 정보보호 정책에 따라 수립된 절차를 준수할 책임이 있다.
정보시스템 감사자	보안 목적이 적절하고 정보보호 정책, 표준, 대책, 실무 및 절차가 조직의 보안 목적에 따라 적절하게 이루어지고 있음을 독립적인 입장에서 관리자에게 보증할 책임이 있다.

다. 정보보호정책 수립팀 구성

적절하고 효과적인 정보보호정책을 위해서는 조직내 임직원의 동의와 지지가 필요하다. 특히 공동 관리에 임직원들이 영향을 줄 수 있는 정보보호정책 과정을 완전히 지지하는 것은 매우 중요하다. 아래의 그림은 생성과 관련된 개별 목록으로 정보보호정책 문서의 생성과 검토 과정에 참여해야할 구성원을 나타낸 것이다.

정보보호정책 개발관리 팀 구성도
(그림 12-1-2)

라. 조직의 정보보호정책 요소

(1) 조직의 정보보호정책은 다음의 요소들을 포함해야 한다.

- 특히 자산 소유자의 관점에서 본, 기밀성, 무결성, 가용성, 책임추적성, 신뢰성에 관한 IT 보안 요건
- 조직의 기반구조 및 책임 할당
- 시스템 개발, 조달과 보안의 통합
- 지침과 절차
- 정보 분류 등급 규정
- 위험 관리 전략
- 비상 계획
- 문제 (유지보수 인력 및 시스템 관리와 같이 신뢰를 필요로 하는 지위의 인력에 특별한 주의를 기울여야 한다)
- 인식, 훈련
- 법과 규제의 준수
- 외주 관리
- 사고 처리

제 2 절 정보보호 관리체계 범위설정

1. 정보보호관리체계 범위설정

가. 정보보호관리체계 범위설정

조직의 특성, 위치, 기술, 자산 등 내 · 외적 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호관리체계의 범위를 설정하여야 한다.

정보보호관리체계의 범위설정은 조직의 정보보호목표 달성에 매우 중요하다. 범위의 설정은 해당 조직에서 중요하다고 판단되는 요소를 포함해야 하며, 일반적인 범위 설정 방법은 다음과 같이 구분할 수 있다.

- Host(호스트) 중심
- 서버중심
- 서비스 중심
- 업무기능 중심
- 업무조직 중심
- 인터넷(네트워크) 중심

특히 서비스 중심의 경우 인터넷 뱅킹 서비스, 전자메일 서비스, 전자상거래 서비스, 정보검색 서비스 등이 있다.

2. 정보자산의 식별

조직의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.

자산식별을 통하여 조직의 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, 정보자산과 업무처리와의 관계도 알아낼 수 있다. 자산평가는 위험분석 결과의 정확도를 결정하는 매우 중요한 과정이다.

자산평가 과정은 크게 자산 조사와 자산가치산정의 2가지로 나눌 수 있으며, 자산조사과정에서는 조사할 자산의 범위를 설정하고, 자산목록을 작성한다. 자산가치산정 과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의한다.

자산식별 과정
(그림 12-2-1)

가. 자산조사

자산조사는 조직의 운영/경영에 중요한 영향을 미치는 다양한 IT자산을 식별하고, 분류하는 작업으로서, IT 자산에 관한 적절한 관리는 조직의 자산을 적절하게 보호하는데 있어서 필수적인 과정이다. 정확한 자산조사 만으로도 기본적인 위험관리가 가능할 만큼 자산조사는 매우 중요하다. 자산조사 수행에는 많은 시간, 노력, 인력, 정보가 필요하고, 따라서 조직에서 요구하는 보안수준과 업무처리에 맞는 조사가 필요하다.

자산조사 방법에는 자산범위설정과 자산목록작성으로 나뉜다.

(1) 자산범위설정

자산범위 설정시에는 다음과 같은 업무적인 측면을 고려해야한다.

- 조직의 운영/경영 측면의 검토 : 조직의 목표와 업무의 중요도 등을 고려하여 도출한다.
- 핵심 업무처리 도출 : IT보안측면에서 타당한지 검토한다.
- 자산조사 범위 선정 기준 도출 : 자산조사 범위를 조직의 IT환경과 업무목적에 맞게 설정함으로서 위험분석의 정확도를 높이고 불필요한 작업을 사전에 예방한다.

최종적인 범위 선정 기준은 정보보호정책에 기술된 보안 요구 수준과 조직의 경영측면에서 핵심 업무처리를 고려하여 보안이 필요한 자산 범위 파악 및 경영진의 요구사항과 보안 예산 범위 등을 고려하여 조직의 환경에 맞는 선정 기준을 도출하도록 한다.

(2) 자산목록작성

자산목록작성은 자산 범위 설정을 통하여 파악된 조직의 규모와 운영목적 및 환경을 바탕으로 위험분석 대상 자산의 실질적인 파악작업이다. 자산범위 선정기준을 통하여 파악된 핵심 업무처리와 기타 선정기준의 범위 내에서 작성한다. 경영진의 요구나 보안예산의 제약으로 인하여 분석에서 제외된 자산(인적, 물적 자산포함)은 위험분석 과정을 통하여 중요성이 인식될 경우 분석 결과에 따라 재고될 수 있다.

자산목록 작성시 고려사항은 다음과 같다.

- 자산항목별 분류 및 자산범위에 따른 선별
- 업무처리를 고려한 자산조사
- 조직을 고려한 자산조사
- 업무처리와 자산가의 관계정립

● 자산항목별 분류 및 조사 : 자산목록은 크게 자산항목별 분류 및 조사와 업무 처리 분류 및 조사의 2가지 관점에서 작성이 가능하다.

- 자산항목별 분류 및 조사 : 자산항목별로 분류 및 조사는 자산의 유형과 성질을 바탕으로 다음과 같이 7개의 대분류와 이를 세분화해서 분류한 뒤 목록으로 작성할 수 있다.

• 하드웨어 : 전산 시스템에서 기계적, 전자적, 전기회로적인 물리적 특성을 갖는 자산을 말한다.

• 운영체제 : 운영체제는 컴퓨터 하드웨어를 효율적으로 운영하기 위한 일종의 소프트웨어로서 자원의 균형 있는 사용 및 처리능력의 자동화를 통해 운영의 능률과 신뢰성을 높이는 역할을 한다.

• 응용소프트웨어 : 응용 소프트웨어는 컴퓨터 시스템을 문서편집, 급여계산, 정보처리, 계산 등 사용자가 필요한 특정 분야에 사용하기 위하여 작성된 소프트웨어를 말한다.

• 네트워크 : 네트워크는 데이터를 서로 다른 시스템 간에 공유할 수 있는 기능을 제공할 수 있는 하드웨어 및 소프트웨어를 말한다.

• 데이터 : 데이터는 전산 시스템에 저장, 처리, 연산될 수 있는 전자 정보를 말한다.

• 사용자 : 사용자는 정보시스템을 사용하는 운영자, 개발자, 분석가, 이용자 등의 모든 인력을 말한다.

• 환경 : 환경은 정보 시스템과 간접적 관계를 가지고 있는 유형, 무형 자산을 통칭한다.

일반적으로 IT위험분석 수행시 자산을 중심을 분석해 왔으나, 이는 대상조직에 잠재하고 있는 위험의 실체를 파악하는데 부족하다 위험의 피해는 IT자산 각각에 가해지기도 하지만 궁극적으로는 IT 자산이 조합되어 수행되어지는 업무처리에 대해 가해지는 것이다. 업무처리와 자산간의 관계를 정립함으로서 각 자산의 가치와 중요도를 더욱 정확하게 파악할 수 있다.

(3) 자산가치 산정

자산가치 산정은 자산의 중요도를 파악하고 위협이 발생할 경우 있을 수 있는 피해를 측정하기 위한 정보를 얻기 위해 위험분석 대상 자산의 가치를 정량 또는 정성적인 방법으로 평가하는 과정이다.

자산가치를 산정하는 방법에는 크게 정량적 방법과 정성적 방법 두 가지가 있다. 자산의 특성에 따라 정량적인 수치로 산정이 가능한 것도 있으나, 그렇지 못한 경우도 많으므로 정확한 정량/정

성 분석이 가치 기준을 적용할 수 있다. 자산 가치 산정시 정량적, 정성적 방법을 적용할 때 기준은 다음과 같다.

[표 12-2-1] 자산 가치 산정의 기준

정량적 기준	정성적 기준
• 자산 도입 비용 • 자산 복구 비용기준 • 자산 교체 비용기준	• 업무처리에 대한 자산의 기여도 • 자산이 영향을 미치는 조직과 작업의 수 • 시간(복구시간) • 기타(조직의 특성에 맞는 기타 요소들)

제3절 위험관리

1. 위험관리전략 및 계획 수립

조직의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 위헌관리 전략 및 계획을 수립하고, 조직에 적합한 위험관리 방법을 선택하고 문서화하여야 한다. 이 위험분석 방법은 조직과 정보보호 환경 변화에 대응할 수 있도록 지속적으로 검토하여야 한다.

조직은 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위험에 대하여 취약성을 인식하고, 이로 인해서 예상되는 손실, 즉 위험을 평가하기 위한 기준을 확립하여야 한다.

가. 위험관리

(1) 위험의 정의

위험이란 비정상적인 일이 발생할 수 있는 가능성을 말하며, 위험분석은 위험을 분석하고 해석하는 과정으로 조직 자산의 취약성을 식별하고, 위협분석을 통해 발생 가능한 위험의 내용과 정도를 결정하는 과정이다.

(2) 위험관리의 정의 및 목적

위험관리란 위험을 평가하고, 피해자가 수용할 수 있는 수준까지 위험 부담을 줄이기 위한 조치를 강구하며 그러한 위험을 용인할 수 있는 수준으로 유지하는 것을 말한다. 위험의 측정과 관리를 통하여 다양한 위협요소로 인한 피해를 최소화하거나 막기 위함이다.

(3) 위험관리의 구분

위험 관리는 4가지 활동으로 구분된다.

- 정보보호정책을 바탕으로 각 조직에 적합한 전반적인 위험 관리 전략의 결정
- 위험 분석 활동의 결과 혹은 기본 통제에 따른 개별 IT 시스템에 대한 대책의 선택
- 보안 권고에 의거한 IT 시스템 보안 정책의 정형화, 조직의 정보보호 정책(적절한 부서별 IT 보안 정책)의 갱신
- 승인된 IT 시스템 보안 정책을 토대로 하여 대책을 구현하기 위한 IT 보안 계획의 수립

나. 위험관리계획 수립

위험관리계획이란 정보와 자산의 보호를 위해 조직, 역할, 책임, 프로세스를 포함하는 활동을 수립하는 것으로, 보안 강화를 원하는 조직은 환경에 맞는 위험 관리계획을 세워야 한다. 그리고 효율적인 방법으로 위험을 다루는 방법이 포함되어야 한다. 계획에는 어디에 보안 노력을 집중시킬 것인지 어떤 접근이 비용, 시간이 효율적인지가 필요하다.

(1) 위험관리계획 수립시 고려사항

위험관리 수행을 위한 전담반을 구성하는 것이 바람직하다. IT 보안 위험관리는 그 조직의 전반적인 요소들이 요구되므로, 필요한 인원들로 구성하는 것이 바람직하다. IT 실무 부서 인원 및 기타 관리부서의 인원들로 충당하는데, 보통 IT 실무자중에서는 시스템 설계 책임자, 시스템 프로그래머, 시스템 운영자 등으로 이루어지고, 관리부서로서는 IT 관리 책임자, 각 일반 업무 부서의

책임자나 경영자들이다.

물론, 여기에는 IT 보안 위험관리 업무를 전문적으로 잘 이해하며 위험관리 과정과 전담반을 잘 이끌 수 있는 구성원을 책임자로 선임해야 하며, 외부의 전문가를 초빙하여 자문을 받거나 또는 영입할 수도 있다. 그리고 IT 조직의 규모나 위험관리에서 도출될 수 있는 요구사항과 범위를 예측하여 전담반의 구성인 수, 포함되는 인원을 조정할 수 있으며, 최소 3, 4명에서 8, 9명으로 구성할 수 있다. 이 전담반은 위험관리를 위한 한시적인 조직이지만, 위험관리 이후의 활동에 대해서도 지원 및 적극 참여할 수 있어야 한다.

IT 보안 위험관리는 각각의 계획 수준에서 그 수준에 맞춰 실행될 수 있으나, 가장 유익한 수준은 전략계획, 즉 실행계획 수준이다.

전략계획 수준에서의 위험관리는 5-10년을 단위로 수행되게 되므로 너무 개략적일 수 있고, 반면에 프로젝트 단위의 위험관리는 너무 세밀하여 비용 효과적이지 못할 수 있다. 따라서 위험관리는 실행계획 수준의, 즉 1-2년에 한번씩 하는 것이 바람직하지만, 현대 IT환경과 정보보호 환경이 급속하게 변하여 조직의 환경의 변화가 발생된다면, 위험분석 및 취약성 분석 등을 수행해야 된다.

IT 조직에 알맞은 위험관리 방법론과 소프트웨어의 선택이 요구된다. IT 보안요구사항과 범위가 결정되면 본격적인 위험분석 과정과 위험평가과정이 시작되고 여기에는 100여 개가 넘는 여러 가지 방법론과 약 1,000여 개가 넘는 위험관리 소프트웨어 중에서 적절한 것을 선정할 필요성이 대두된다. 간단하게 위험관리를 수행하고자 할 경우에는 간단한 방법론, 즉 기본적인 접근과 같은 방법을 사용하여 위험분석과 평가를 수행할 수 있다.

그러나 IT 조직의 규모가 크고, 위험손실이 크게 예측되거나 보다 정확하고 상세한 위험관리를 수행하고자 할 경우에는 위험분석 및 위험평가 방법론을 비교하여 적절한 소프트웨어의 사용이 필요하다. 흔히 위험관리는 매우 복잡하고, 또한 전문적 지식이 요구되므로 전문가의 자문을 받아 수행하는 것이 바람직하다.

위험관리 계획 수립시 고려해야 할 주요한 사항은 관련 법/제도이다. 최근 국제적으로 조직의 위험 수준을 측정하여, 적정한 경우 그 조직을 인정해 주는 인증제도가 도입되고 있다. 국내적으로도 보안 관련 법/제도, 정보보호관리체계 인증제도 등이 제정되고 있어 위험관리 계획 수립시 이를 고려해야 한다.

(2) 위험관리 계획

위험 관리는 크게 위험분석, 위험평가, 대책설정 3가지의 과정으로 구분된다.

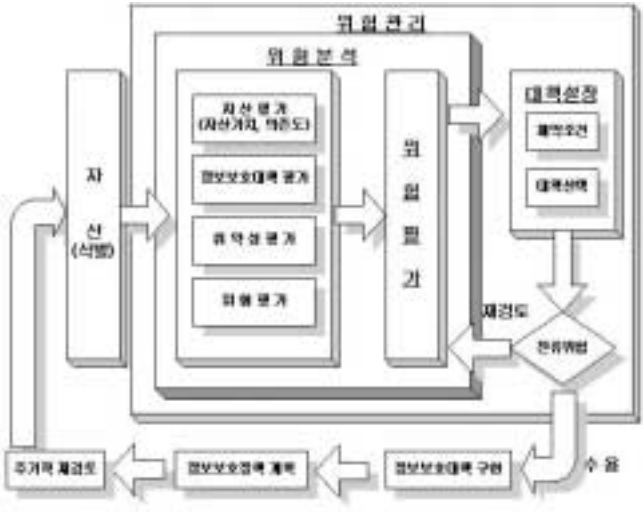
- 위험분석 : 통제되거나 받아들여질 필요가 있는 위험을 확인하는 것이다. 위험분석은 자산가치평가, 위협, 취약성을 포함하며, 모든 시스템에 대한 간단한 초기분석을 통해 불필요한 시간과 자원의 투자 없이 실행할 수 있다.

- 위험평가 : 위험평가의 목적은 적절하고 정당한 보안 대책을 선정하고 식별하기 위하여 시스템 및 그 자산이 노출된 위험을 평가하고 식별하기 위한 것이다. 위험은 위험에 처한 자산, 잠재적인 불리한 업무충격을 유발하기 위해 발생하는 위협가능성, 식별된 위협으로 인한 취약성의 용이한 사용 및 위험을 감소시키는 기존의 혹은 계획된 어떤 대책에 따른 새로운 위협가능성 등을 포함한다.

- 대책설정 : 허용가능 수준으로 평가된 위험을 줄이기 위해 적절하고 정당한 대책을 식별 및 선정한다. 대책은 위협을 방지하고, 취약성을 감소시키고, 원치 않는 사고의 충격을 제한하고, 원치 않는 사고를 감지하고, 복구를 촉진하는 실행, 절차, 메커니즘이다. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층을 제공하는 다양한 대책의 조합이 요구된다. 예를 들면, 컴퓨터에 적용되는 접근 통제 메커니즘은 감사 통제, 인사 절차, 교육훈련, 물리적 보안으로 지원되어야 한다. 어떤 대책은 환경의 일부 또는 자산의 고유한 측면에서 이미 존재할 수도 있고 시스템이나 조직에 이미 마련되어 있을 수도 있다.

(3) 위험관리 절차

위험관리 절차
(그림 12-3-1)



2. 위험분석

조직은 식별된 정보자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 식별하고 분류하여야 한다. 또한 조직은 위협, 취약성 및 위험에 대한 계속된 변화를 인식하여야 한다.

정보보호관리체계 범위 내에 있는 정보자산의 가치와 위험을 고려하여, 위험분석 방법을 결정하고 이 정보자산에 대한 위협, 취약성 및 기밀성, 무결성, 가용성 등의 잠재적 손실에 대한 영향을 식별 · 분석하여야 한다.

가. 위험분석 전략의 선택

모든 시스템에 대해 세부적인 검토를 수행하는 것은 시간이나 자원 측면에서 효율적이지 않다. 그렇다고 중대한 위험을 다루지 않는 것도 효율적이라 할 수 없다. 이러한 극단적인 사항간의 균

형을 고려한 접근은 필요성에 따른 고수준의 검토를 포함한다. 이는 심도 있는 분석으로 시스템의 IT 보안 필요성을 결정하기 위한 것이다. 어떤 조직의 보안 필요성은 조직 규모, 조직이 영위하는 사업 유형 그리고 환경과 문화에 따라 다르다. 기업 위험 분석 전략의 선택은 이러한 사실에 직접 관련된다.

어떤 상황에서 조직은 아무 조치도 취하지 않거나 대책 구현의 연기를 결정할 수 있다. 이러한 관리 결정은 조직이 상세한 검토를 완료한 후에 이루어져야 한다. 그러나 만약 이러한 결정이 내려진다면 경영진은 책임져야 하는 위험, 영향 및 원치 않는 사고의 발생 가능성을 완전히 인지해야 한다. 이러한 지식이 없다면 조직은 의도하지 않아도 법이나 규정을 위반하게 될 수 있고 사업은 잠재적 손실에 노출될 수 있다. 아무 조치도 취하지 않거나 대책 구현의 연기 결정 및 판단은 이러한 사항과 다른 가능한 역효과를 신중히 고려한 후 내려져야 한다.

상세 검토 결과를 토대로 위험을 경감시키는 대책은 아래의 네 가지 사항 중 하나로 선택될 수 있다.

(1) 기본적인 접근

첫 번째 선택은 모든 시스템에 기본적인 보호의 수준을 달성하기 위한 보호대책을 선택하는 것이다. 표준보호대책의 다양함은 기본적인 문서와 관행코드에서 지원된다. 기본 필요의 실행 후에 이 보호대책들은 국제/국가적 표준조직, 산업부분 표준 또는 권고안, 사업목표, 크기 등에 적절한 유사성이 있는 다른 회사에 받아들여질 수 있다.

기본적인 접근 방법

- 조직의 보안정책을 참조하여 세부통제사항을 작성한다.
- 공공기관의 경우 정부부처 및 공공기관에서 요구하는 보안요구사항을 참조하여 반영한다.
- ISO, KICS 등 국내/외 표준을 참조하여 반영한다.
- 외국의 보안 컨설팅 기관에서 작성한 기본통제를 참조한다.
- 정보감리 등을 통하여 얻은 결과를 반영한다.

[표 12-3-1] 기본적인 접근방법의 예

분류		기 본 접 근 방 법	중요도		보안목적		
대분류	소분류		상	하	기밀성	무결성	가용성
논리적 통제	소프트웨어통제	1. 중요 프로그램의 접근 통제가 이루어지고 있는가? 2. 모든 사용자들이 사용 아이디를 가지고 있는가?	○ ○		○	○	
물리적 통제	시설물 접근통제	1. 카드를 이용한 접근통제가 이루어지고 있는가? 2. 전산실에 대한 접근 통제가 이루어지고 있는가?	○	○	○	○	

장점	위험분석을 위한 자원이 필요하지 않고, 보호대책 선택에 들어가는 시간과 노력이 줄어든다. 일반적으로 기본적인 보호대책을 확인하기 위해 어떠한 중요한 자원도 필요하지 않다. 큰 노력 없이 많은 시스템에 같은 또는 비슷한 안전요소가 적용될 수 있다. 만약 같은 환경에서 운영되는 조직의 시스템이 많고, 사업 필요성이 비교가능 하다면 기본적인 안전요소는 비용 효과적인 선택이다
단점	만약 기본적인 보호대책이 너무 높게 설정되었다면 어떤 시스템에 대해서는 비용이 너무 많이 들고, 너무 제한적이며, 만약 너무 낮게 설정되었다면, 어떤 시스템에 대해서는 보안결핍을 가져올 수 있다.

(2) 비공식적인 접근

두 번째 선택은 모든 시스템에 대한 위험분석을 비공식적이고 실용적으로 수행하는 것이다. 비공식적 접근은 구조적인 방법에 의존하지 않고, 개인적인 지식과 경험을 이용한다. 만약, 내부 보안 전문가가 가용하지 않다면 외부 계약자가 이 분석을 시행할 수 있다.

- 장점
  비공식적 분석을 하기 위한 추가적인 기술의 습득이 필요하지 않고 세부적인 위험분석에 비해 신속하게 수행된다. 이 접근방식은 비용 효과적이며, 소규모 조직에 적합할 수 있다.
- 단점
  - 구조화되지 못해서, 어떤 위험이 있는 관심지역을 잃어버릴 가능성이 증가한다. 이 방법의 비공식적인 특성 때문에 재검토자의 주관적 관점과 편견에 영향받을 수 있다.
  - 보호대책 선택에 정당성이 부족하다. 따라서 보호대책에 들어가는 비용이 정당화되기 어렵다.
  - 반복적인 재검토 없이는 시간에 따른 보안관련 변화의 관리가 어려울 수 있다. 비공식 위험분석을 했던 사람이 조직을 떠나면 문제가 발생할 수 있다.

(3) 세부적인 위험분석

모든 시스템에 대한 세부적인 위험분석을 수행하는 것이다. 세부적인 위험분석은 정당성과 자산의 가치, 이 자산들에 대한 위협의 수준평가, 그리고 자산들의 취약성을 포함한다. 위험분석은 자산에 대해 확인된 위험에 대한 만족하는 안전요소의 정당성, 선택 그리고 채택을 지원하고, 관리에 의해 정의된 받아들일 수 있는 수준의 위험의 감소를 지원한다. 세부적인 위험분석은 많은 자원이 소모되는 프로세스이고, 경계의 설정에 주의해야 하고, 지속적인 관리에 주의를 요한다.

- 장점 :
  - 각 시스템에 필요한 적절한 보안의 수준이 확인된다.
  - 부적인 위험분석으로부터 얻은 추가적인 정보로부터 보안관련 변화의 관리는 이익을 얻는다.
- 단점 :
  - 가시적인 결과를 얻기 위해, 많은 시간, 노력 그리고 전문성이 필요하다.
  - 중요한 시스템의 보안 필요성이 너무 늦게 다루어질 가능성이 있다. 모든 시스템이 같은 세부사항으로 간주될 수 있고, 이 분석을 완성하는데 많은 시간이 소요되기 때문이다. 따라서, 모든 시스템에 세부적인 위험분석을 사용하는 것은 바람직하지 못하다.

(4) 복합적인 접근

높은 수준의 위험분석 접근을 이용해 높은 위험이나, 조직운영에 중요한 시스템을 우선적으로 확인하는 것이다. 이 결과를 기반으로, 적절한 보안을 획득하기 위한 세부위험분석이 필요한 것하고, 기준선 보호로 충분한 시스템으로 분류된다.

이 선택은 기준선 접근과, 세부위험분석에 설명된 기능들 중 최상의 핵심기능들의 조합이다. 결론적으로 이것은 보안요소 식별에 소요되는 최소한의 시간과 노력(모든 시스템이 여전히 적절하게 보호되고 있는 동안)의 좋은 균형을 제공한다

- 장점 :
  - 중요한 자원이 투입되기 전에 필요한 정보를 얻기 위한 간단한 고수준접근을 사용하는 것은, 위험관리 프로그램에 더 적합하다.
  - 이것은, 조직적인 보안 프로그램의 신속한 전략 구상이 가능하고, 또 좋은 계획보조도구로 사용될 수 있다.
  - 자원과 비용은 가장 큰 이익이 있는 곳에 사용될 수 있고, 높은 위험은 미리 다루어질 수 있다.

● 단점
- 만약 고수준 분석이 부정확한 결과를 가지고 온다면, 세부적인 분석이 필요한 어떤 시스템은 적절히 다루지 못할 지도 모른다.
- 만약 고수준 위험분석이 적절하게 점검된다면 어떤 사건에 대해서는 그 시스템은 여전히 기준선 안전요소에 의해 보호된다.

대부분의 시스템에서 이 선택이 가장 비용 효율적인 접근을 제공하고, 대개의 조직에서 가장 권장되는 위험분석방법이다.

나. 위험분석 방법론 선택

위험분석 방법론은 위험분석 결과의 성격에 따라 크게 정량적 분석과 정성적 분석으로 구분된다. 정량적 방법은 손실 및 위험의 크기를 금액으로 나타내는 정밀한 분석이 요구되는 방법이며, 정성적 방법은 손실이나 위험을 개략적인 크기로 비교하는 방식이다. 이들 특징 비교는 [표 12-3-2]과 같다. 또한 정량적 방법과 정성적 방법을 모두 이용하는 혼합 접근방법도 존재한다. 혼합 접근방법은 일차적으로 정성적 방법을 이용하되 특정한 관심사에는 면밀한 정량적 결정을 내리는 방식이다.

[표 12-3-2] 위험분석 방법론의 분류

	정량적 접근 방법	정성적 접근 방법
개념	위험 발생 확률 × 손실 크기 = 기대 위험 가치 분석	손실 크기를 화폐가치로 표현하기 어려움 위험 크기는 기술 변수로 표현
유형	• 수학공식 접근법 • 확률분표 추정법 • 확률지배 • 몬테카를로 시뮬레이션 • 과거자료 분석법	• 델파이법 • 시나리오법 • 순위결정법 • 퍼지행렬법 • 질문서법
주사용 지역	미국	유럽
척도	연간 기대 손실	점수(5점, 10점 척도)
장점	비용/가치 분석, 예산 계획, 자료분석이 쉬움	금액화하기 어려운 정보의 평가가 가능 분석 시간이 짧고 쉽다.
단점	분석의 시간, 노력, 비용이 큼	평가 결과가 주관적이어서 사용자에 따라 달라질 수 있음

3. 위험평가

자산에 대한 잠재적 및 알려진 위협과 취약성으로 나타날 수 있는 조직의 피해와 현재 구현된 통제대책의 실패 가능성 및 영향을 평가하고 수용 가능한 위험수준을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 대책 선정 및 우선 순위의 확보를 지원하여야 한다.
위험은 기밀성, 무결성, 가용성, 책임 추적성, 신뢰성의 훼손에 의한 잠재적 충격의 관점에서 평가된다. 위험 분석 검토의 결과는 자산에 충격을 줄 수 있는 위험을 나타낸다.

가. 위협

자산은 다양한 종류의 위협에 처해 있다. 위협은 시스템, 조직, 조직의 자산에 피해를 주는 원치 않는 사고를 일으킬 잠재성을 갖는다. 이러한 피해는 비인가된 파괴, 공개, 변경, 훼손, 불가용성, 손실 등 IT 시스템에 의해 처리되는 정보 또는 서비스에 대한 직 · 간접의 공격으로부터 발생할 수 있다. 자산에 피해를 입히기 위하여 위협은 자산의 취약점을 파고든다. 위협은 자연적이거나 사람의 의도에 의한 것일 수 있으며 우연히 또는 계획적으로 발생한다. 두 경우 모두 위협을 식별하고 그 수준과 가능성을 평가해야 한다.

위협에 의한 피해 규모는 경우별로 광범위하다. 예는 다음과 같다.

- 소프트웨어 바이러스는 활동 양상에 따라 피해 규모가 달라진다.
- 특정 지역의 지진은 발생할 때마다 강도가 다르다.
- 이러한 위협에는 심각성의 측정이 따른다. 예를 들면,
- 바이러스는 파괴적, 비 파괴적으로 기술된다.
- 지진의 세기는 리히터 강도로 기술된다.

어떤 위협은 하나 이상의 자산에 영향을 줄 수 있다. 그러한 경우, 어떤 자산이 영향을 받느냐에 따라 충격이 다를 수 있다. 예를 들면, 한 대의 PC에 침입한 소프트웨어 바이러스의 충격은 제한적, 국소적이다. 그러나 동일한 바이러스가 파일서버를 기반으로 하는 네트워크에 퍼진다면 그

충격은 광범위하다. 다른 위협 또는 다른 장소에서의 동일한 위협은 그로 인한 피해의 규모에 일관성을 갖기도 한다. 위협이 야기하는 피해가 일관적이라면 총체적인 접근 방식을 취할 수 있다. 그러나 광범위한 피해의 경우에는 각각의 위협에 대한 좀더 구체적인 접근이 적절하다.

위협은 위협 자체에 대한 유용한 정보를 제공하는 특성이 있다. 이러한 정보의 예는 다음과 같다.

- 출처 즉, 내부 또는 외부
- 동기 즉, 재정 이익 또는 경쟁 우위
- 발생빈도
- 위협의 심각한 정도

조직이 처한 환경과 문화는 조직에 대한 위협의 취급과 지대한 관계, 영향을 갖는다. 극단적인 경우, 어떤 위협은 문화에 따라 유해한 것으로 인식되지 않기도 한다. 위협을 다룰 때는 환경, 문화의 측면을 반드시 고려해야 한다.

나. 취약성

자산과 관련된 취약성은 물리적 배치, 조직, 절차, 인력, 관리, 행정, 하드웨어, 소프트웨어 또는 정보상의 약점을 포함한다. 취약성은 IT 시스템이나 사업 목표에 유해한 위협이 침투하는 경로가 된다. 취약성 자체는 피해를 일으키지 않는다. 취약성은 단지 하나의 조건 즉, 위협에 의해 자산이 피해를 입게 되는 일련의 조건이다. 다양한 근원의 취약성을 고려해야 하는데 예를 들면 자산 고유의 취약성 등이다. 취약성이 더 이상 적용되지 않게 자산 자체가 변화하지 않는 한 취약성은 잔류한다.

취약성에는 악용의 소지가 있고 바람직하지 않은 결과를 초래할 수 있는 시스템상의 약점이 포함된다. 취약성은 위협이 피해를 일으키는 기회가 된다. 예를 들면, 접근 통제 매카니즘의 부재는 침투 위협을 야기하여 자산의 손실을 가져오는 취약성이다. 특정 시스템이나 조직내의 모든 취약

성이 위협으로 직결되는 것은 아니다. 취약성에 대응하는 위협이 존재하는 경우가 관심의 대상이다. 그러나 환경이 역동적으로 변화하면서, 신구 위협에 노출되는 취약성을 식별하기 위해서는 모든 취약성을 모니터링 해야 한다.

(1) 취약성 분석

취약성 분석은 식별된 위협이 침투할 수 있는 약점을 점검하는 것이다. 취약성 분석에서는 환경과 기존의 대책을 고려해야 한다. 위협에 대한 특정 시스템이나 자산의 취약성은 시스템 또는 자산이 피해를 입을 수 있는 지름길이다.

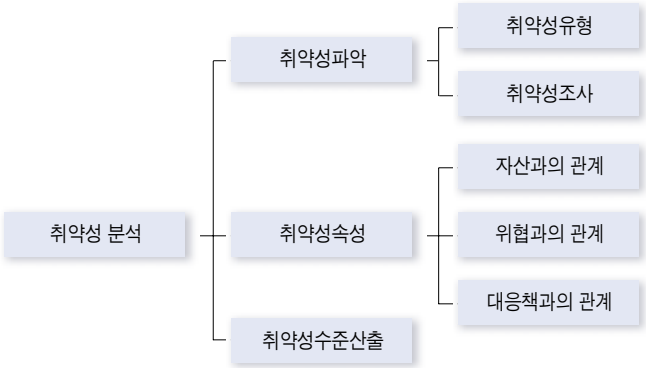
위협분석 과정
(그림 12-3-2)

(2) 취약성 속성

취약성과 자산, 위협, 대응책의 관계를 파악하기 위해서 일반적으로 알려진 취약성과 각 요소들과의 관계를 바탕으로 속성을 정의하면 다음과 같다.

- 취약성은 모든 자산이 잠재적으로 지니고 있다.
- 취약성은 그 자체만으로 어떠한 위험도 초래하지 않는다.
- 취약성은 위협에 의해 이용되어 위협이 위험을 초래할 환경을 제공한다.
- 취약성은 대응책이 늘어날수록 감소한다.
- 취약성은 대응책 자체도 잠재적으로 지니고 있으므로, 취약성은 결코 0이 될 수 없다.

취약성분석 과정
(그림 12-3-3)



(3) 취약성 등급기준

취약성 등급기준은 위험평가 과정에서 산출되는 취약성 수준을 평가하기 위한 기준이다. 모든 취약성 수준은 절대적 가치로 수치가 계산되지만 평가는 조직에 따라 상대적일 수 있다. 따라서 조직의 수준과 보안 정책 등을 고려하여 취약성 수준을 평가해야 한다.

(4) 충격(영향력)

충격은 계획적으로 또는 우연히 일어난 사고의 결과로 자산에 영향을 줄 수 있다. 결과는 어떤 자산의 파괴, IT 시스템에 대한 손상, 기밀성, 무결성, 가용성, 책임추적성 또는 신뢰성의 손실이 될 수 있다. 간접적인 결과로는 재무적 손실, 시장 점유율 하락 또는 조직 이미지 실추 등을 들 수 있다. 충격의 측정을 통해 원치 않은 사고의 결과와 그에 따른 대책 비용의 균형을 유지할 수 있다.

원치 않는 사고의 발생빈도를 고려할 필요가 있다. 이것은 특히 각각의 사고는 경미하지만 그 누적된 영향이 위해한 경우에 중요하다. 충격에 대한 평가는 위험 평가와 대책 선택에 있어 중요한 요소이다.

충격에 대한 정량적, 정성적 측정은 다양한 방법으로 이루어질 수 있다. 예를 들면 다음과 같다.

- 재정비용의 수립
- 경험적인 심각한 정도의 계량화. 예를 들면 1~10 등급.
- 사전 정의한 형용사의 사용. 예를 들면 상 · 중 · 하

4. 정보보호대책 수립

조직의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험 전가 등의 전략을 설정하고, 통제사항을 선택한다. 통제사항의 선택은 비용 · 효과 분석에 의해 정당화 될 필요가 있다.

대책은 위협을 방지하고, 취약성을 감소시키고, 원치 않는 사고의 충격(영향)을 제한하고, 원치 않는 사고를 감지하고, 복구를 촉진하는 실행, 절차, 메커니즘이다. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층을 제공하는 다양한 대책의 조합이 요구된다. 예를 들면, 컴퓨터에 적용되는 접근 통제 메커니즘은 감사 통제, 인사 절차, 교육훈련, 물리적 보안으로 지원되어야 한다. 어떤 대책은 환경의 일부 또는 자산의 고유한 측면에서 이미 존재할 수도 있고 시스템이나 조직에 이미 마련되어 있을 수도 있다.

대책은 감지, 억제, 방어, 제한, 교정, 복구, 모니터링, 인식 중 하나 이상의 기능을 수행하는 것으로 대책의 적절한 선택은 보안 프로그램의 올바른 구현에 필수적이다. 대부분의 대책들이 복합적인 기능을 수행함으로 복수의 기능을 만족시키는 대책을 선택하는 것이 비용 효율적이다. 대책이 사용될 수 있는 영역의 예는 다음과 같다.

- 물리적 환경
- 기술적 환경(하드웨어, 소프트웨어, 통신)
- 인력
- 행정

보안 인식은 인적 영역에 관련된 대책이다. 조직이 운영하는 환경과 문화는 대책의 선택, 조직의 보안 인식 등과 관련이 있으며, 어떤 대책은 조직의 보안 태도에 대해 강력하고 명확한 메시지를 전송한다. 이러한 관점에서, 조직이 운영되는 문화 및 사회에 공격적이지 않은 대책을 선택하는 것이 중요하다.

가. 잔류 위험

보통 대책에 의해서도 위험은 부분적으로 경감될 뿐이다. 부분적 경감이 일반적으로 달성할 수 있는 전부이고 그 이상의 경감에는 비용이 증가한다. 이는 일반적으로 잔류 위험이 존재함을 시사하는 것이다. 보안이 조직의 필요에 적절한지 여부를 판단하는 일의 일부는 잔류 위험의 허용이다. 이 프로세스를 위험 허용(risk acceptance)이라 한다.

관리를 통해 사건의 발생 가능성과 충격의 관점에서 모든 잔류 위험을 인식할 수 있어야 한다. 원치 않는 사고의 발생에 의한 충격의 결과를 허용할 수 있는 위치에 있는 사람들 및 잔류 위험의 수준을 허용할 수 없을 때 추가적인 대책의 구현하는 권한을 가진 사람이 잔류 위험의 허용 여부에 대한 결정을 내려야 한다.

적절하고 정당한 대책은 허용 가능 수준으로 평가된 위험을 줄이기 위해 식별 및 선정한다. 기존의 그리고 계획된 대책, IT 보안 구조, 여러 가지 유형의 제한 사항은 적절한 선정을 위해 허용하기 위해서 고려되어야 한다.

나. 대책 식별

평가된 위험에 대응하여 효율적으로 보호하는 대책을 선정하기 위해, 위험 분석 결과를 고려해야 한다. 관련 위협에 대한 취약성은 추가적인 보호가 필요한 곳 및 어떤 방식을 취해야 하는가를 지적한다.

고려된 대책 비용에 따라 결정되는 대안이 있다. 대책이 적용되는 영역은 다음을 포함한다.

- 물리적 환경
- 인력
- 경영
- 하드웨어/소프트웨어
- 통신(네트워크)

대책이 충분히 효율적이지 않는 경우 기존의 또는 계획된 대책은 개선 또는 제거의 관점에서 유지보수를 포함하는 비용 대조를 조건으로 하여 재검토되어야 한다. 때로는 대책을 적소에 두는 것보다 부적절한 대책을 제거하는 것이 더 비용이 많이 들수 있다. 더욱이 현재의 검토 영역 외의 자산을 위해 대책의 보호를 제공하는 것이 가능하다.

대책 식별로 인해 취약성이 보호되어야 하는 취약성 및 이러한 취약성을 이용할 수 있는 관련 위협을 갖는 것은 유용하다. 일반적으로 위험을 경감시킬 많은 가능성들이 있다.

- 위험 회피
- 위험 전환(예, 보험)
- 위협 감소
- 취약성 감소
- 가능한 충격 감소
- 원치 않은 사고 감지 대응, 복구 등

이러한 가능성들(이 요소들의 결합)중 어떤 것이 환경에 따라 가장 적절한 것이다. 대책 카탈로그도 유용하다. 그러나 카탈로그에서 대책을 선정하는데 있어서 조직의 특수한 필요성에 그들을 맞추는 것이 중요하다.

대책 선정에 있어 중요한 또 다른 측면은 비용 요소이다. 대책이 보호해야 하는 자산의 가치보다도 유지 및 실행에 있어 훨씬 더 비싼 대책은 부적절하다. 그러나 실행될 대책의 품질이나 수를 감소시키는 예산의 경우에는 많은 주의를 기울여야 한다. 왜냐하면 계획된 것보다 큰 불분명한 위험 수락으로 이어질 수 있기 때문이다. 대책을 위해 수립된 예산은 상당한 주의를 가지고 제한적 요소로서 사용되어야 한다.

IT 시스템 보호를 위해 기본적인 접근이 선정되는 경우에는 대책 선정은 비교적 간단하다. 대책 카탈로그는 가장 일반적인 위협에 대해 IT 시스템을 보호하기 위한 일련의 대책을 제안한다. 이러한 추천된 대책들은 기존의 그리고 계획된 대책들과 이미 적소에 없거나 기준선 보호를 취득하기 위해 실행되는 대책 목록 형식으로 계획되지 않은 것들과 비교된다.

대책 선정은 작동 및 기술적 대책들의 균형을 항상 포함한다. 작동중인 대책은 물리적 인력 및 관리적 보안을 제공하는 것들을 포함한다.

물리적 보안 대책은 내부 건물 벽, 키 코드 문 잠금 장치, 화재 억제 시스템, 방어 장치 및 위험 방지기의 강화를 포함한다. 인력 보안은 인력 채용 점검(특히 '신뢰의 견해' 로 사람들), 직원 모니터링, 보안 인식 프로그램을 포함한다.

절차상의 보안은 안전한 작동 절차문서, 응용 개발, 수용 절차뿐만 아니라 사고 처리 절차를 포함한다. 이러한 범주에 관련하여 일관된 계획/재난 복구를 포함하여 적절한 업무 지속성, 전략 및 계획(들)은 각각의 시스템을 위해서 개발된다는 것은 매우 중요하다. 계획은 재난이나 서비스 중단이 발생되었을 때 복구를 위한 핵심 기능과 우선권, 프로세스 필요성 및 수행할 조직의 절차의 세부사항을 포함한다. 그러한 계획은 사업을 계속하게 하는 한편 중요한 정보가 대책에 프로세스 되도록 요하는 단계를 포함해야 한다.

기술적 보안은 통신 대책뿐만 아니라 하드웨어와 소프트웨어를 포함한다. 이러한 대책들은 위험이 보안 기능 및 보증을 제공하는 정도에 따라 선정된다. 예를 들어 기능은 식별, 인증, 논리적 접근 통제 요건, 감사 추적/보안 기록 필요성, 다이얼-백(dial-back)보안, 메시지 인증, 암호화 등을 포함한다. 보증 요건은 보안 기능 및 그에 따른 점검 수량 및 유형 등에 필요한 신뢰 수준을 문서로 증명한다. 작동 및 기술적 대책의 알맞은 융합에 대한 결정에 있어서 기술적 보안 요건을 실행하기 위한 상이한 옵션이 있을 것이다. 기술 보안이 요하는 바와 같이 기술 보안 구조는 보안이 제공할 수 있는 것을 식별하도록 각각의 옵션에 대하여 정의되어야 한다. 또한 보안이 가용한 기술로 사용 가능하도록 정의되어야 한다.

조직은 시스템의 결정을 위해 위험을 감소시킬 수 있는 보호대책의 일부로 평가된 제품 및 시스템을 사용하도록 결정한다. 평가된 제품은 제 3자(예, K4인증 등)에 의해 검사된 것들이다. 제 3자는 동일한 조직의 또 다른 부분이거나 또는 제품 및 시스템 평가에 있어서 전문성이 있는 독립조직이다. 특히 평가는 구축 중인 시스템을 위해 만들어진 일련의 전 기준에 대응하여 수행될 수 있고, 여러 상황에서 사용될 수 있는 일련의 일반화된 기준이다. 평가 기준은 기능적 요건 혹은 보증 요건을 규정한다. 많은 평가 계획이 실재하며 그들 중 대다수는 정부 및 국제 표준 단체가 지원한다. 조직이 구현된 일련의 기능이 필요한 것이라는 확신을 요구할 때 그리고 그러한 기능의 실행 중 정확성과 완전성에 관하여 신뢰할 필요가 있을 때 평가된 제품 및 시스템을 사용할 수 있다. 대안적으로 강조하는 실용적인 정보보호 시험은 보안 제공에 있어서 확실한 보증을 제공한다.

실행 대책 선정시 많은 요소들은 다음을 포함하여 고려된다.

- 보호대책 사용의 용이성
- 사용자를 위한 명백성
- 그들을 수행하는 사용자를 위해 제공하는 도움
- 보호대책의 상대적 강화
- 수행 기능의 유형 - 예방 조치, 제지, 감지, 복구, 교정, 모니터링, 인식

일반적으로 보호대책은 이러한 기능들 중의 하나 이상을 충족시킨다. 더 많이 충족하면 할수록 좋다. 전반적인 보안이나 사용될 일련의 보호대책을 검사할 때, 적어도 가능하다면 기능 유형간의 균형을 유지한다. 이는 전체적인 보안들이 더욱 효율적이고 능률적이게 한다. 비용/이익 분석을 요구할 뿐만 아니라 거래 분석(특수한 상황에 관하여 상대적인 중요성에 무게를 두는 일련의 기준을 사용하는 경쟁 대안을 분석하는 방법)도 마찬가지로 요구될 수 있다.

다. 제약의 식별 및 검토

대책 선정에 영향을 주는 많은 제한이 있다. 권고안 작성 시 그리고 실행 시 반드시 이러한 제한을 고려해야 한다. 전형적인 제약으로 다음과 같은 사항들이 있다.

(1) 시간적 제약

많은 형태의 시간적 제한이 존재한다. 예를 들어 관리를 위해서 수용하는 시간적 기간 내에 대책을 구현해야 한다. 또 다른 형태의 시간적 제한은 대책이 기간 내에 구현되는지 여부이며 세 번째의 시간적 제한은 관리가 결정하는 시간적 기간이 시스템을 특수한 위험에 노출되도록 남겨 두는 허용 가능 기간이다.

(2) 재정적 제약

대책은 보호하기 위하여 설계된 자산가치 보다 실행을 위한 것이 보다 비싸지 않다. 모든 노력은 배정된 예산을 초과하지 말아야 한다. 그러나 몇몇 경우에 원하는 보안 및 그러한 예산 제한 내에서 위험 수용 수준을 달성하는 것은 불가능하다. 따라서 이것은 이러한 상황의 해결에 대한 관리 결정이다.

(3) 기술적 제약

프로그램이나 하드웨어의 호환성과 같은 기술적 문제는 대책 선정 시 그들에 대한 평가가 이루어

진다면 쉽게 회피될 수 있다. 또한 기존의 시스템에 대한 회상적 보호대책 구현은 기술적 제한으로 인해 흔히 저지된다. 이러한 난관들은 대책의 균형이 절차상 그리고 물리적 보안 측면을 지향하도록 한다.

(4) 사회적 제약

보호대책 선정에 대한 사회학적 제한은 국가, 영역, 조직 심지어 조직내의 부서에게까지 구체적이다. 많은 기술적 대책들이 직원의 능동적인 지원에 의존하기 때문에 이러한 사회학적 제한은 무시될 수 없다. 만약 직원이 대책에 대한 필요성을 이해하지 못하고 문화적으로 수용할 만하다는 것을 알지 못한다면 대책은 시간이 지날수록 비효율적인 것이 될 것이다.

(5) 환경적 제약

환경적 요소들은 자연적, 도시적 등의 지리학 주위에서 공간 가용성이나 극한의 기후 조건들과 같은 대책 선정에 영향을 끼칠 것이다.

(6) 법적 제약

정보 프로세스에 대한 개인 자료 보호나 관련 법률 조항들과 같은 법적 요소들은 대책의 선정에 영향을 미칠 수 있다. 소방법, 노동법과 같은 비 IT의 특수 법과 규정은 대책 선정에 영향을 미칠 수 있다.

라. 위험 수용

대책을 선정하고 이러한 대책들이 달성하려고 하는 위험 감소를 식별한 후에도 항상 잔류 위험은 존재한다. 어떠한 시스템도 절대적으로 안전할 수 없다. 이러한 잔류 위험은 조직을 위해 '수용 가능' 또는 '수용 불가능' 으로 구분한다. 이러한 범주는 위험과 연관된 잠재적인 불리한 업무 충격을 검토하여 수행될 수 있다. 분명히 수용 가능 위험은 추가의 고찰사항 없이 허용되어서는 안

된다. 이러한 위험들이 다른 제한(빌딩으로의 비행기 추락, 지진과 같은 경우와 같이 비용이나 단순한 보호 불능 같은 그러나 그러한 사고에 대한 복구계획은 여전히 만들어질 수 있음)으로 인해 수용될 것인가 또는 어쩌면 추가의 비용이 드는 대책이 수용 불가능한 위험을 감소시키기 위해서 선정되는가는 관리 결정 사항이다.

5. 정보보호계획 수립

보호대책의 선정이후 구현할 보호대책 및 구현의 우선 순위, 일정계획, 예산, 책임, 운영계획 등을 포함하는 정보보호계획을 수립하고, 대책이 필요한 각 위험에 대한 통제사항 및 선택에 대한 의사결정 결과를 정보보호대책 명세서로 문서화하여야 한다.

정보보호 계획서 내에 정보보호대책 구현을 위해 최소한 다음과 같은 사항을 포함해야 한다.

- 구현할 정보보호대책 정의
- 정보보호대책 구현 우선순위
- 각 대책별 책임부서, 구현일정, 예산, 운영계획 등

정보보호계획에 대한 효율적, 효과적 실행을 위해서는 최고경영자, 정보보호위원회, 정보보호관리자 등 상위 경영층의 승인을 반드시 득해야 한다.

선정된 정보보호대책에 대해서 자세하게 기술하고 예산, 기간, 기타 다른 문제로 정보보호대책을 선정하지 못한 경우에는 향후, 정보보호 계획에 반드시 명문화하고 정보보호 계획을 수행할 수 있도록 상위 경영층에 보고해야 한다.

제4절 구현

1. 정보보호대책의 효과적 구현

정보보호에 대한 위험으로부터 정보자산을 보호하기 위해 선택된 통제사항은 적절한 관리 조치와 우선 순위에 따라 구현되어야 한다.

가. 구현과정에서의 포함사항

- 정의된 보안 목적을 달성하기 위해 역할 할당, 책임 할당, 예산 등을 포함한 세부적인 관리 프로그램의 구현
- 선택된 통제사항의 구현
- 운영관리
- 자원관리
- 시행절차와 보안 사고를 신속히 탐지하고 대응할 수 있는 통제의 구현

보안 대책의 정확한 실행은 잘 구성되고 문서로 증명된 보안 계획에 따라 의존한다. 각각의 시스템 관련 보안 인식 및 훈련은 병행하여 실시한다. 보안 계획 구현이 완성될 때, 대책에 대한 승인은 시스템 또는 서비스가 사용되기 전에 이루어져야 한다.

각각의 시스템에 필요한 대책의 구현은 보안 계획을 따라야 한다. 일반적인 보안 인식의 개선은 대책의 유효성을 위해 중요한 측면이다.

나. 선택한 통제 사항들의 효과적 구현

지속성과 일관성의 보장은 대책에 대한 문서는 보안 자료 중 중요한 부분이다.

이러한 프로세스는 상이한 여러 가지 방법으로 이루어질 수 있으며 여러 가지 보안 문서의 일부이다. 즉 보안 계획, 업무 지속성 계획, 위험 분석 자료, 보안 정책 및 절차와 같은 일련의 보안 문

서들이다.

이는 형상 및 변화 관리에 관련된 사람들, 관리자, 사용자, 시스템 관리자, 유지 인력의 필요성을 충족시키기 위해 설계되었다. 완벽한 상세 내용으로 보안 착오 또는 과실을 없애고 보안 작동이 정확하고 능률적으로 수행될 것이라고 보증하는 정보를 유포하고 제공할 필요가 있다.

특히 위협, 취약성, 위험에 대한 많은 문서는 매우 중요하고 비인가된 노출에 대비하여 항상 이들을 보호해야 한다. 결과적으로 대부분의 조직들은 이러한 문서를 매우 조심스럽게 처리할 필요가 있고 '안전한' 배치 절차를 사용하도록 한다. 그러한 절차가 사용될 경우 대책 정보의 중요한 부분들을 어떻게 저장하고 접근하여 사용할 것인지에 대해 설명하는 방법의 문서 자료로 증명되어야 한다. 더욱이 절차는 그 대책 정보가 저장되는 방법 결정에 대해 누가 책임을 지고 있으며 누가 그러한 절차를 사용 및 평가할 수 있을 것인지 식별해야 한다. 배치 절차 설계 시 대책 정보 접근성은 중요한 시기에 재난 혹은 다른 예상하지 못한 사건이 발생 시 비상 계획 및 재난 복구 계획을 포함하여 업무 지속성, 전략 계획을 찾아내고 사용하는 필요성과 같은 구체적인 요소를 고려해야 한다. 마지막으로 비의도적으로 또는 모르고 대책의 유효성을 감소시키는 것이 비인가된 변화를 초래할 수 없다는 사실을 보장하기 위하여 대책 문서 자료의 엄격한 형상 통제 역시 필요하다.

IT 보안 계획이 일단 완료되고 책임 있는 최고경영자의 승인(서명)으로 마무리되면 대책 실행 및 시험하고 보안 준수를 점검한다. 보안 준수 점검 검토는 보안 대책이 정확히 실행되었는지 그리고 효율적으로 사용 중이며 적절히 시험되고 있는지를 확인하기 위해 실시된다. 보안 시험은 본 검토의 일부로써 실시될 수 있다. 시험은 실행이 정확하게 수행되어 완성되었음을 보증하는 중요한 기법이다. 보안 시험은 시험 접근, 계획 및 환경을 설명하는 보안 시험 계획에 의해 지도되어야 한다. 모의 침투시험은 평가된 위험에 의해 정당화되면 사용될 수 있다. 세부적인 보안 시험 절차를 반드시 기록하고 표준 시험 보고서를 사용해야 한다. 목적은 규정한 대로 IT 보안 계획 요건을 충족시키고 감소되었음을 보증하는 방법으로 실행 및 시험을 수행하는 것이다.

2. 정보보호 교육 및 훈련

조직의 정보보호 관련직원들 및 최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호 대책의 필요성을 이해하도록 하며 구현될 대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.

가. 정보보호 인식 프로그램

정보보호 인식 프로그램의 목적은 조직 내의 인식 수준을 모든 사람이 쉽게 수행할 수 있는 수준까지 증대시키는 것이다. 프로그램은 IT 직원 및 최종 사용자들이 IT 시스템에 대한 충분한 지식을 가지고 있고 대책이 필요한 이유와 그것을 정확하게 이용하고 이해하는 방법을 그들이 이해하고 있다는 사실을 보장해야 한다. IT 직원이 대책을 수용하면 최종 사용자들이 효율적으로 작업할 수 있다.

정보보호 인식 프로그램에 대한 정보는 조직의 모든 단계로부터 나온다. 이는 조직IT 보안 정책을 포함해야 하며 조직의 IT 보안 계획의 모든 목적을 포함한다. 인식 팀을 위하여 모든 부서로부터의 관리 지원이 필요하다. 보안 인식 프로그램에 기술된 일정, 강연 및 다른 모든 활동에 의해 다음 주제들을 상세하게 다루어져야 한다.

- 조직과 개인 모두에게 보안의 중요성 설명
- 기밀성, 무결성, 가용성, 책임추적성, 신뢰성을 조건으로 IT 시스템을 위한 보안 필요성 및 목적
- 조직과 개인 간 보안 사고의 밀접한 관계
- 하드웨어와 소프트웨어를 포함하여 IT 시스템의 정확한 사용
- 위험과 대책에 대한 이해를 유도하여 배후의 목적과 조직 IT 보안 정책, 모든 보안 지침, 지시사항, 위험 관리 전략의 설명
- IT 시스템 위험과 IT 시스템 보호
- IT 영역(인가된 인력, 문 잠금 장치, 배지, 입회 기록)과 정보(논리 접근 통제, 판독/갱신 권리)에 대한 제한된 접근 그리고 이러한 제한이 필요한 이유

- 정보보호 및 기획 위반을 보고 해야 할 필요성
- 절차, 책임, 작업 설명
- 정보보호 요소이기 때문에 IT 직원 및 최종 사용자들이 금해야 할 모든 것
- 만약 직원이 보안 위반에 책임을 지는 경우의 결과
- 대책을 실행 및 점검하는 IT 시스템 보안 계획
- 이러한 대책이 필요한 이유와 정확하게 사용하는 방법
- 정보보호 준수 검사 관련 절차
- 변화 및 형상 관리

정보보호 인식 프로그램 개발은 보안 전략, 대상, 정책 검토로 시작한다. 이러한 프로세스는 조직의 중요한 기능을 식별할 정도의 지위에 있을 뿐 아니라 상위 관리자의 지원을 받는 개인들로 구성된 팀이 수행해야 한다.

검토 팀은 기업 IT 보안 정책에 따라 요건의 파기를 반드시 결정한다. 이는 전반적인 정보보호 시작과 결합시킨다(즉, 단지 IT만이 아닌). 인식 포스터, 간행물, 회사 소개서, 내부 우편과 같은 여러 가지 형식으로 간행되어야 한다.

그리고 팀은 보안 문제들에 대한 구체적인 브리핑을 실시한다. 요건의 완전한 검토는 브리핑을 위해 필수 정보 기반을 구축하기 위하여 수행해야 한다. 모든 직원들이 최신의 정보 기술에서 고유의 위험에 익숙하다는 것을 보증하기 위하여 각각의 브리핑은 주기적인 간격으로 실시해야 한다.

인식 프로그램의 목적 및 내용을 결정에 관한 책임은 상위 관리 수준으로 정보보호관리팀에 배정되어야 한다. 기업 IT 임원 및 정보보호 인식 개발 팀에게 개발 및 실행을 위한 책임을 할당해야 한다. 이는 다른 기업 훈련 및 교육 활동과 연계하여 실행해야 한다. 그러나 조직의 작업 환경의 보안 정책 및 절차를 검토하고 그들에게 익숙해지는 것은 개개인 모두의 책임이다. 따라서 보안 인식 프로그램은 비로소 조직의 모든 계층에게 이행된다.

나. 필요성 분석

목표 그룹(실행자, 관리, 피고용인)내에 이미 존재하는 인식 수준과 새로운 정보를 전달하는 가장 수용할 만한 방법을 결정하기 위해서 보안 지식 필요성 분석을 수행할 필요가 있다. 필요성 분석은 현재의 실제 수행과 관련하여 정책, 절차, 태도, 보안 지식 그리고 원하는 수행을 검사한다.

다. 프로그램 배급

전체적인 정보보호 인식 프로그램은 상호작용 및 촉진 기법을 포함한다. 인식 프로그램 본 영역의 초점은 필요성 분석을 통해 식별된 결핍에 있다. 고용인은 IT 자산이 가치 있고 자산에 대한 위험이 사실이라고 인정하고 이해를 얻을 필요가 있다.

그러한 조직의 정보보호 인식 프로그램에서 도출되는 하나의 혜택은 보안 프로그램에 참가할 기회를 고용인들에게 제공한다는 사실이다. 상호 작용 기법은(직원회의, 훈련 과정)은 참가자와 보안 인력들이 필요성 분석에서 기인하는 개념 및 요건들을 확인하도록 두 가지 통신 방법을 제공한다. 촉진 기법은(비디오, 이메일보안, 배너, 포스터, 출판물)은 단일 방향의 통신 도구이며 이들은 관리 집단이 저렴한 방법으로 개념, 정보, 태도를 방송하도록 허용한다.

라. 정보보호 인식 프로그램의 모니터링

정보보호 인식 프로그램의 효과적인 모니터링을 구성하는 두 가지의 특징적 요소가 있다.

(1) 주기적 수행 평가

정보보호 관련 작동 모니터링으로 인해 인식 프로그램의 유효성을 결정하고 프로그램 배급에 영향을 주는 변화를 요구하는 곳을 식별하는 것이다.

(2) 인식 변화 관리

전체 정보보호 프로그램에 변화가 있을 때마다 그러한 변화들을 반영하여 기존의 지식 및 기술 수준을 향상시키는 정보보호 인식 프로그램을 개조할 필요성이 있다.

(3) 보안 훈련

조직내의 모든 사람에게 적용하는 일반적인 정보보호 인식 프로그램 외에 구체적인 보안 훈련이 IT 시스템에 관련된 업무 및 책임을 가진 인력에게 요구된다. 보안 훈련의 심도는 IT 보안이 조직에 대해 가지는 전체적 중요성에 달려 있고, 수행된 직무의 보안 요건에 따라 다르다. 필요한 경우 대학 강의 과정에 참여와 같은 보다 광범위한 교육이 제공되어야 한다. IT 보안 훈련 프로그램은 조직에 관련된 모든 보안 필요성을 다루기 위해 개발되어야 한다. 구체적인 보안 훈련이 필요한 인력을 결정할 때 다음을 고려해야 한다.

- IT 시스템 설계 및 개발에 대해 중요한 책임을 가진 인력
- IT 시스템 작동에 대해 중요한 책임을 가진 인력
- 조직의 IT 프로젝트, IT 보안 임원
- 접근 통제 혹은 디렉토리 관리와 같은 관리적 책임을 가진 인력

더욱이 진행중이거나 계획된 업무 또는 프로젝트 등에 대하여 특수 보안 훈련을 요구하는 경우를 알기 위하여 점검이 이루어져야 한다. 구체적인 정보보호 요건을 가진 업무 혹은 프로젝트에 착수시 상응하는 프로젝트 착수 전에 정보보호 훈련 프로그램이 개발되고 그러한 활동이 제때에 수행되어야 함을 보증해야 한다. 정보보호 훈련 과정이 다루는 주제는 참가 인력의 직무 및 업무능력에 달려 있다

- 보안
  - 기밀성, 무결성, 가용성 위반의 예방 조치이다.
  - 조직 또는 개인에 대한 잠재적 불리한 사업 충격

- 정보 중요도 분류 계획
- 전체적인 보안 프로세스
  - 전체적인 프로세스 설명
  - 위험 분석 요소
- 대책과 이를 수행하기 위하여 필요한 훈련
- 직무 및 책임
- IT 시스템 보안 정책

보호대책의 정확한 구현 및 사용은 정보보호 훈련 프로그램이 다루어야 할 가장 중요한 사안 중의 하나이다. 각각의 조직은 필요에 따라 그 자체의 정보보호 훈련 프로그램 및 기존의 혹은 계획된 대책을 개발해야 한다. 다음은 기술적 및 비 기술적 대책 간 균형을 위한 필요성을 강조하고 다루어야 할 대책 관련 주제의 예이다.

- 보안 하부 조직
  - 직무 및 책임
  - 보안 정책
  - 주기적인 보안 준수 점검
  - 보안사고 처리
- 물리적 보안
  - 빌딩
  - 사무 지역, 장비실
  - 장비
- 인력 보안
- 매체 보안 (디스크, CD, 테이프 등)
- 하드웨어/소프트웨어 보안
  - 식별 및 인증
  - 논리 접근 통제
  - 회계 및 보안 감사
- 통신 보안

- 네트워크 하부 조직
- 통행로, 출구, 방화벽
- 인터넷과 다른 외부 연결

● 비상 계획/재난 복구를 포함하는 업무 지속성, 전략 및 계획
● 침해사고 예방 및 대응 계획

제 5 절 사후관리

1. 정보보호관리체계의 재검토

조직의 목표, 기술 등 내 · 외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.

적절한 단계에서, 다음 목적을 위하여 정책의 계획 및 구현에 대한 체계적인 검토를 수행하여야 한다. 그러한 검토에 참여하는 인원에는, 검토가 진행되고 있는 대상의 계획 및 구현 단계에 관련된 인원이 포함되어야 하며, 검토 및 검토로 야기 된 조치의 결과를 기록하여야 한다. 정보보호관리체계의 재검토에는 다음과 같은 사항을 고려하여야 한다.

가. 변화관리 체계 구축

조직의 업무, 정보시스템, 법/제도 등의 대내외적 환경 변화와 내부 감사 및 보안사고 결과 및 보안사고 결과 등을 반영한 변화관리 체계가 구축되어야 한다.

나. 정보보호정책의 영향분석이나 잠재적인 위험성 평가

정보보호관련 대내외 환경변화가 조직에 미치는 영향을 분석하며, 또한 내부감사 지적사항과 보안사고의 영향을 반영할 수 있는 정보보호관리체계의 재검토 절차가 필요하다.

다. 정보보호정책에 대한 전과정(Life Cycle) 재검토

정보보호관리체계의 재검토시에는 정보보호관리체계의 효율성, 범위의 적정성, 잔류위험의 수준, 기타 절차 등을 포함해야 한다.

2. 정보보호관리체계의 모니터링 및 개선

정보보호관리체계가 정보보호정책과 목적을 충족시키는지 여부에 대해 모니터링하여, 개선사항을 식별하고, 적절한 수정이나 예방 조치를 통해 효과적으로 개선사항을 구현하여야 한다. 이에 관련된 조치와 결과는 조직의 임직원에게 전달되어야 하고, 관련자들에게 자문을 구하여야 한다.

가. 정보보호관리체계 일치성 확인

정보보호관리체계는 지속적으로 모니터링되어 정보보호정책과 조직의 목적과의 일치성을 만족시켜야 한다.

조직은 필요에 따라 모니터링, 측정, 분석 등을 통하여 정보보호관리체계의 지속적 개선 프로세스를 계획하고 실행하여야 한다.

- 정보보호정책의 성과 측정시 요구사항
  - 정보보호정책의 적합성 실증
  - 정보보호관리체계의 적합성 보증
  - 정보보호관리체계의 효과성에 대한 지속적 개선의 달성

이는 통계적 기법을 포함한 적용 가능한 방법의 필요성, 범위 및 사용에 대한 결정을 포함하여야 한다.

- 감사 및 측정방법은 다음사항을 고려
  - 정책만족도 측정
  - 내부감사
  - 재정평가
  - 자체평가 등
- 모니터링 및 측정

조직은 정보보호관리체계의 성과 측정방법으로 정보보호정책이 조직의 요구사항을 충족시키는지 여부에 대해 모니터링 하여야 하며, 이 정보의 획득 및 활용에 대한 방법을 결정하여야 한다. 개선사항에 대한 조치 및 결과가 피드백되어야 지속적인 개선활동 사이클이 재강화되어 보다 개선된 관리체계로 발전할 수 있다.

3. 내부감사

조직은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 부적합 사항 및 그들의 원인을 제거하기 위한 조치가 취해졌으며, 취해진 조치가 검증되고 검증결과가 보고됨을 보장하여야 한다.

다음 사항을 결정하기 위하여 조직은 계획된 주기로 내부감사를 수행하여야 한다.

- 정보보호정책이 계획된 결정사항 및 조직이 설정한 요구사항을 충족시키는지 그리고 이 규격의 요구사항을 충족시키는지 여부
- 효과적으로 실행되고 유지되는지 여부

조직은 감사 대상 및 영역의 상태와 중요성뿐만 아니라 이전 감사의 결과를 고려하여 감사 프로그램을 계획하여야 한다. 또한 조직은 감사 목적 범위 주기 및 방법을 정하여야 하며, 감사자 선정 및 감사 수행에는 감사 프로세스의 목적성 및 공정성이 보장되어야 한다. 감사자는 자신의 업무에 대하여 감사를 수행하여서는 안된다.

문서화된 절차에는 감사의 계획, 수행, 감사의 독립성 보장, 결과의 기록 및 보고에 대한 책임과 요구사항을 정하여야 한다.

감사대상 업무에 책임을 지는 경영자는 발견된 부적합 및 원인을 제거하기 위한 조치가 적시에 취해질 수 있도록 보장하여야 한다. 후속조치는 취해진 조치의 검증 및 검증 결과의 보고를 포함하여야 한다.

c o n t e n t s

부 록

해킹 · 바이러스 방지 체크리스트

분 류	체크리스트 항목	비 고
윈도우즈 시스템	마이크로소프트의 보안공지 메일서비스에 가입하였는가 ?	
	최신의 서비스팩 및 핫픽스를 모두 설치하였는가 ?	
	관리 공유폴더를 제거하였는가 ?	
	적절한 로컬 보안 정책을 설정하였는가 ? - 암호, 계정 잠금, 감사, 사용자 권한, 보안옵션 등	
	적절한 사용자 계정 관리 및 정책을 설정 - Administrator 계정 이름을 변경하였는가 ? - 패스워드 길이를 최소 7자리로 설정하였는가 ? - Guest 계정을 사용중지 했는가 ?	
	불필요한 서비스를 제거 하였는가 ?	
	하드 디스크를 NTFS 로 포맷하였는가 ?	
	NTFS에 대하여 적당한 ACLs를 설정하였는가?	
리눅스 시스템	사용하지 않는 서비스를 제거하였는가 ?	
	최신버전의 S/W 및 패치를 설치하였는가 ?	
	불필요한 SUID/SGID 파일의 권한을 변경하였는가 ?	
	사용자 계정 및 암호관리 - 불필요한 계정을 제거 하였는가 ? - 안전하지 않은 패스워드의 사용을 관리하고 있는가 ?	
	시스템 보안을 위한 커널 파라미터 설정을 했는가 ?	
웹서버 (아파치)	일반계정(nobody 또는 apache) 권한으로 웹서버가 실행되도록 설정하였는가 ?	
	디렉토리 리스팅 방지를 위한 설정을 하였는가 ?	
	심볼릭 링크 사용 방지를 위한 설정을 하였는가 ?	
	SSI(Server Side Include) 사용을 제한하였는가 ?	
	mod_security 모듈 설치 및 활용하고 있는가 ?	
웹서버 (IIS)	IIS 서버 운영을 위한 최소한의 서비스만 설치하였는가 ?	
	IIS 샘플디렉토리를 삭제 하였는가 ?	
	필요한 응용프로그램 맵핑만을 설정 하였는가 ?	
	IIS Log Files에 대한 ACL은 적절하게 설정 되어 있는가?	
	SSL을 사용하기 위한 IIS 설정을 하였는가 ?	

해킹 · 바이러스 방지 체크리스트

분 류	체크리스트 항목	비 고
메일 서버	메일의 첨부파일 사이즈를 제한하고 있는가?	
	한번에 발송 가능한 참조 발송자를 제한하고 있는가?	
	메일 중계(relay) 기능 제한 설정을 하였는가?	
	버전정보 공개를 제한하였는가?	
DNS 서버	recursion 기능을 제한하였는가?	
	zone-transfer를 제한하고 있는가?	
	버전정보 공개를 제한하였는가?	
보안시스템 운영	바이러스 백신 설치 및 운영 - 모든 직원 사용자 PC에 설치하였는가? - 실시간 감시/자동 업데이트/이메일 감시 기능을 설정하여 사용하고 있는가? 또는 바이러스월(서버용 백신)을 운영하고 있는가?	
	침입차단시스템을 설치 운영하고 있는가?	
라우터	네트워크 장비의 OS를 최신버전으로 설치하였는가?	
	네트워크 장비로의 접근 통제 - 콘솔/AUX/VTY 포트 패스워드를 설정하였는가? - enable 패스워드를 설정하였는가? - 접속 가능한 사용자/시스템에 대한 ACL을 설정하였는가?	
	불필요한 프로토콜/서비스를 제거하였는가? - ICMP관련 서비스, Source Routing, Small Services	
	IP 주소 위조 방지 수단을 사용하였는가? - 사설 IP 주소 차단 - uRPF 사용	
	라우팅 프로토콜 인증 설정을 하였는가? - RIPv2, EIGRP, OSPF, BGP 등	
	ACL로 차단된 트래픽을 로깅하고 관리하고 있는가?	
스위치	가상 LAN(VLAN)을 구성하여 운영하는가?	
	Port Security 기능을 설정하였는가?	
	ARP Inspection 기능을 설정하였는가?	

스팸대응 체크리스트

분 류	체크리스트 항목	비 고
스팸 대응	자사 메일서버에 스팸릴레이 차단 기능을 설정하였는가?	
	자사 메일서버에서 이용자들이 원하지 않는 스팸을 필터링 할 수 있도록 조치하였는가?	
	악성 프로그램 설치를 통한 이용자 PC의 스팸발송을 예방 하기 위해 정기점검을 실시하고 있는가?	
	이용자들이 자사 메일서버를 이용하여 스팸을 발송하지 않는지 상시적으로 모니터링을 수행하고 있는가?	
	이용자들이 스팸을 발송하거나 스팸을 수신하지 않도록 관련 정보를 주기적으로 제공하고 있는가?	
	메일서버 보안을 위한 상용화된 제품을 사용할 경우, 스팸방지 기능이 있는 것을 사용하는가?	
	자사 메일서버 이용자의 이메일주소 DB가 유출되지 않도록 기술적?관리적 보안조치를 취하고 있는가?	

■ 주요서비스포트

다음의 포트들은 P2P, 웹폴더, 메신저 및 트로이 목마에 사용되는 포트목록으로 포트스캔을 통해 해당 서비스가 발견된 경우 특별한 주의를 기울여야 할 필요가 있다.

1. 메신저 사용 포트

서비스명	서 버	포 트	설 명
MSN	64.xxx.xxx.xxx/24	TCP 1863,80	1863접속 시도후 차단 되면 80 접속 시도
	207.xxx.xxx.xxx/24		
	207.xxx.xxx.xxx/24	TCP 6891-6900	파일전송
	207.xxx.xxx.xxx/24	TCP 6901	음성채팅
	207.xxx.xxx.xxx/24	UDP 1863, 5190	Microsoft Network Messenger
	207.xxx.xxx.xxx/24		
Yahoo	216.xxx.xxx.xxx/32	TCP 5050,5101	5050 접속 시도 후 차단 되어 있으면 Port를
	216.xxx.xxx.xxx/32		계속적으로 변경
	216.xxx.xxx.xxx/32		
	216.xxx.xxx.xxx/32	TCP 5000-5001	음성채팅
	66.xxx.xxx.xxx/32		
	216.xxx.xxx.xxx/32		
	216.xxx.xxx.xxx/32	TCP 5100	화상채팅
	66.xxx.xxx.xxx/32		
	216.xxx.xxx.xxx/32		
Nate On	203.xxx.xxx.xxx/32	TCP 5004-5010	기본포트
	203.xxx.xxx.xxx/32		5004-5010 접속 시도후 차단되어 있으면 Port를
	203.xxx.xxx.xxx/32		
		TCP 80,83,7003	웹 컨텐츠 및 문자 보내기
Daum	211.xxx.xxx.xxx/32	TCP 8062	
SayClub	211.xxx.xxx.xxx/32		
AOL		TCP 5190	AOL Instant Messenger Also used by: ICQ
		UDP 4000	ICQ_locator
Dreamwize	211.xxx.xxx.xxx/32	TCP 10000	
	211.xxx.xxx.xxx/32		
버디버디		TCP 810	
		TCP 940	
		TCP 950	
케이친구		TCP 7979	
천리안		TCP 1420	
		TCP 4949,8989	파일송수신
ICQ		TCP 5190	
UIN		TCP 8080	
Genile		TCP 10000	

2. 웹폴더 사용 포트

서비스명	프로토콜	포트	설명
PDBOX(UP/Down Load)	TCP	10000	나우콤에서 운영하는 웹스토리지 서비스
		10100	
		19000	
		29230	
		29231	
		28290	
PDBOX(Web Connection)	TCP	8000 - 80013	
iDisk	TCP	9553	한국통신 메가패스
DiskPOP	TCP	4255	디스크 팝
		3306	
		5770	
엑스폴더	TCP	80, 8080	Default 하나로 포스에서 서비스
		20100, 20200	변경
웹폴더	TCP	80, 8080	Default 네이버 서비스
		20100, 20200	변경
팝폴더	TCP	80, 8080	구루구루 만든 GRETECH에서 운영하는 폴더
		20100, 20200	
웹하드	TCP	139	데이콤 운영
	UDP	137	
		138	

3. 주요 어플리케이션 사용 포트

서비스명	프로토콜	포트	설명
Oracle	TCP	1521	
Informix-IBM	TCP	1546	
		1100	
DB2-IBM	TCP	523	
		5001	
Lotus Notes	TCP	1352	
MSSQL	TCP	1433	
MSSQL Moniteor	UDP	1434	
Microsoft Terminal	TCP	3839	
Pcmlinux	TCP	1267	
Netshow	TCP	1755	
VNC	TCP	5900	
		5800	
PcanyWhere	TCP	5631	
	UDP	5632	
Netmeeting	TCP	389	
		1720	
Netflow	UDP	2055	
Snmp	UDP	161	
echo	TCP	7	
	UDP	7	
IKE(IPSEC Protocol)	UDP	500	
OpenWindows	TCP	2000	
RealPlayer	TCP	7070	
		554	
Syslog	UDP	514	
TFTP	UDP	69	

4. P2P 프로그램 사용 포트

서비스명	프로토콜	포트	설명
당나귀	TCP	4661	서버 접근 포트(변경가능)
		4662	자료 전송 포트(변경 가능)
		4242	
	UDP	4672	
		4665	
iMash	TCP	5000	
Bit Torrent	TCP	6881	
		6889	
	UDP	22321	hello message, bye message 사용 포트
소리바다 v.2		7674	mp3를 검색
		7675	mp3파일을 보내는 사람
소리바다 v.1	TCP	9001 - 9004	
WINMX	TCP	6699	
	UDP	6257	
Direct-Connect	TCP	411 - 412	
	UDP	411 - 412	
KaZaA	TCP	1214	
Guntella-Morpheus	TCP	6346 - 6347	
	UDP	6346-6347	
GuRuGuRu	TCP	9292	
		8282	
		31200	
파일 구리	TCP	9493	
Madster-Aimster	TCP	23172	
		9922	
HotLine	TCP	5497	
		5498	
		5500 - 5503	
	UDP	5499	
V-Share	TCP	8404	
Maniac	TCP	2000	
	UDP	2010	
	TCP	2222	
MiRC	TCP	6667	Default
		6665 - 6670	변경
		7000	
Shareshare	TCP	6399	
	UDP	6777	
Bluster	UDP	41170	
GoToMyPc	TCP	8200	
Napster	TCP	6600 - 6699	
		4444	
		5555	
		6666	
		7777	
		8888	
		8875	

5. 트로이 목마 사용 포트

서비스명	프로토콜	포트	설명
Backdoor/SubSenen	TCP	1243, 1999, 2773, 54283, 7215, 6776, 27374	
Netbus	TCP	12345, 20034, 12346	
	UDP	12345, 20034, 12346	
Back Orifice 2000	TCP	31337, 54321, 54320	
	UDP	31337, 54321, 54320	
GirFrend	TCP	21554	
WinCrash	TCP	2583, 3024, 4092, 5742	
DeepThroat	TCP	2140, 3150, 41, 60000, 6670, 6771	
	UDP		
Hack 'A' Tack	TCP	31785, 31787, 31788, 31790, 31792	
	UDP	31789, 31791	
Master Paradise	TCP	3129, 40421, 40422, 40423, 40425, 40426	
	UDP		
Bla	TCP	1042, 666(doom)	
	UDP		
Donald Dick	TCP	23476, 23477	
Portal of Doom	TCP	10067, 10167, 3700, 9872, 9873, 9874, 9875	
	UDP		
NetSphere	TCP	30100, 30101, 30102	
NetMonitor	TCP	7300, 7301, 7306, 7307, 7308	
TransScout	TCP	1999, 2000, 2001, 2002, 2003, 2004, 2005	
Doly	TCP	1010, 1011, 1012, 1015	
FC Infector	TCP	146	
	UDP	146	
Dmsetup	TCP	58	
FireHotcker	TCP	5321	
RASmin	TCP	1045, 531(conference)	
Stealth Spy	TCP	555	
FTP 공격	TCP	666(doom)	
Dark Shadow	TCP	911	
Silencer	TCP	1001	
Netspy	TCP	1024	
Exterme	TCP	1090	
Ultor' s	TCP	1234	
Whack-a-Mole	TCP	12361, 12362, 12363	
WhackJob	TCP	12631	
FTP99CMP	TCP	1492	
Shiva Burka	TCP	1600	
Spy Sender	TCP	1807	
ShockRave	TCP	1981	
Remote Explorer	TCP	2000	
Trojan Cow	TCP	2001	
Ripper	TCP	2023	
Bugs	TCP	2115	
Striker	TCP	2565	
Phinneas Phucker	TCP	2801	
RAT	TCP	1097, 1098	Remote Administration Tool
Rat	UDP	2989	
Filenail	TCP	4567	

서비스명	프로토콜	포트	설명
Sokets de Trois v1.	TCP	5000, 5001	
Blade Runner	TCP	5400, 5401, 5402	
SERV-Me	TCP	5555	
BO-Facil	TCP	5556, 5557	
Robo-Hack	TCP	5569	
'The Thing'	TCP	6400	
Indoctrination	TCP	6939	
GateCrasher	TCP	6969, 6970	
Priority	TCP	6969	
Remote Grab	TCP	7000	
iCkiller	TCP	1027, 7789	
iNi Killer	TCP	9989	
Acid Shivers	TCP	10520	
COMA	TCP	10607	
Senna Spy	TCP	11000, 13000	
Progenic	TCP	11223	
GJammer	TCP	12076	
Keylogger	TCP	12223	
Proziack	TCP	22222	
EvilFTP, UglyFTP	TCP	23456	
Delta Source	TCP	26274	
	UDP		
Trinoo	TCP	1524	
Trinoo DDoS	UDP	34555	
SubSeven 2.1/2.2	TCP	27374, 2774, 16959, 4267	
QaZ	TCP	7597	
Back_Door_setup	TCP	5000	Also used by: BioNet Lite, Blaxer5, Bubbel Trojans
Backage	TCP	411	
BackDoor-G	TCP	1243	
Connect-Back_backdoor	TCP	4000	Also used by: SkyDance trojan
DaCryptic	TCP	1074	
DerSphere	TCP	1000	
DerSphere II	TCP	2000	
Freak2k	TCP	7001	
InCommand	TCP	1029	
Jade	TCP	1024	
Kaos	TCP	1212	
Kuang2	TCP	17300	
Idpw0rm	TCP	515	
Mneah	TCP	4666	
NoBack0	UDP	1201	
Port_6667	UDP	6667	
Remote_storm	TCP	1025	
RexxRave	UDP	1104	
Shady shell	TCP	1337	
Sockesdestoie	TCP	1	
Terrortrojan	TCP	3456	
TheFlu	TCP	5534	
WinHole	TCP	1081	
Xanadu	TCP	1031	

이 매뉴얼은 국가안전보장회의(NSC)의 “국가사이버안전표준매뉴얼”을 기준으로 하고 국가정보원의 “국가사이버안전매뉴얼” 체계를 참고하여 작성되었습니다.

이 매뉴얼의 작성을 위하여 다음과 같은 분들께서 수고 하셨습니다.

2004년 8월

	한국정보보호진흥원		
총괄 책임자	**인터넷침해사고대응지원센터**	**본 부 장**	**김 우 한**
사업 책임자	기반보호기술팀	팀 장	이 강 신
참여연구원		연 구 원	민 복 기
		연 구 원	이 진 태
		연 구 원	조 영 덕
		연 구 원	김 동 현
집 필 자	인포섹(주)		신 수 정
	한국정보보호진흥원		정 현 철
	정보통신윤리위원회		한 명 호
	(주)오늘과내일		홍 석 범
	시스코 시스템즈 코리아		최 우 형
			이 현 우
			이 상 규
			박 영 길
감 수	정보통신부	부이사관	장 광 수
		서 기 관	장 석 영
		서 기 관	안 효 범
		사 무 관	손 지 윤
		사 무 관	배 성 준
		사 무 관	최 선 경
	연세대학교		송 주 석
	함께하는 시민행동		박 준 우
	중소기업정보화경영원		주 석 정
	(사)한국인터넷PC문화협회		조 영 철
	해커스랩		정 문 수

민간사이버안전매뉴얼

2004년 8월 초판 인쇄
2004년 8월 초판 발행
2005년 12월 개정 발행

발행인: 이 홍 섭
발행처: **한국정보보호진흥원**
서울특별시 송파구 가락동 78번지
IT벤처타워(서관)
Tel: (02) 4055-114
인쇄처: 호정씨앤피
Tel: (02) 2277-4718