2007 CERT 구축 및 운영 가이드

CONsortium of CERT
CONCERT

KISA 한국정보보호진흥원

본 가이드는 국내 기관 · 기업의 침해사고 대응을 위한 CERT 구축 및 운영작업을 지원하기 위해 (사)한국침해사고대응팀협의회, 한국정보보호진흥원, 그리고 국내 기업 정보보호 관리자 및 전문가들과 공동으로 작성하였습니다.

2007년 9월

〈 편집위원 〉

강 승 봉 팬 택 앤 큐 리 텔
구 형 준 삼 성 네 트 웍 스
박 의 원 인 터 파 크 지 마 켓
박 종 섭 한 영 회 계 법 인
안 미 현 한국정보보호진흥원
유 우 영 현 대 정 보 기 술
이 상 용 삼 성 전 자
이 준 원 컨 설 팅 하 우 스
정 철 기 통신정보공유분석협회
정 현 철 한국정보보호진흥원

(※ 이름 가나다 순)

2007

CERT 구축 및 운영 가이드

목차

Ⅰ 개 요

Ⅱ CERT 구축 시 고려사항

Ⅲ CERT 활동 계획 수립

Ⅳ CERT 활동

Ⅰ 개 요

1. CERT의 정의 및 목적

2. 보안사고의 정의

3. 국내외 침해사고대응체계 구축 및 운영 현황

1 CERT의 정의 및 목적

정보 시스템 및 정보유통 체계의 발달로 수많은 정보가 인터넷을 통하여 유통되고, 또 노출되어 있다. 이 과정에서 정보 시스템과 정보를 겨냥한 보안사고가 등장하고 있으며, 특히 최근에는 금전적 이익을 취득하기 위한 목적으로 다양한 공격 기법들이 등장해 기승을 부리고 있다.

CERT(Computer Emergency Response Team, 침해사고대응팀)는 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직을 말한다.

국내에서는 1996년 한국정보보호진흥원 중심으로 CERT 활동이 시작된 이후, 사이버 침해사고에 대하여 조직적인 대응체계를 구축함으로써 기술적인 사이버 침해사고 대응이 다루어져왔는데, 현재는 다양한 보안 위협에 대응하기 위하여 기존의 기술적인 측면뿐만 아니라 관리적인 측면과 물리적인 측면에 대한 관심도 점차 높아지고 있다. 때문에 CERT를 구성하고 운영하는 조직에서는 보안을 기술적인 부분에 한정하여 다루어서는 안 되며, 해당 조직 전체를 보호할 수 있도록 조직체계와 역할을 정의하여야 한다.

2 보안사고의 정의

보안사고는 조직이나 업무 등에 파급효과가 없는 개인에 국한된 단순한 사고와 달리, 조직의 업무에 영향을 미치는 승인되지 않은 정보자산에 대한 접근, 변경, 유출 등의 사건을 말한다. 보안사고는 사건의 파급 영향의 정도에 따라 일반 보안사고와 파급효과가 큰 중대보안사고로 차등 구분해 관리하여야 하며, 중대 보안사고와 일반 보안사고의 구분은 아래 예시를 참고하여 조직의 특성에 맞게 선택하면 된다.

일반 보안사고의 정의

- 악성 소프트웨어(웜, 바이러스, 백도어, 트로이 목마 등)에 의한 침해
- 네트워크 및 시스템에 대한 비인가된 침해 및 시도
- 일반 자산의 도난, 분실, 파손 및 파괴
- 보안취약점으로 정보 시스템의 정상적인 운영에 지장을 초래한 사건
- 정보의 비인가자 사용, 승인되지 않은 개인에게 정보 접근 허용
- 비인가자의 보안 구역 접근 시도
- 조직이나 업무 등에 파급효과가 없는 단순히 개인에 국한된 사고는 보안사고의 범주에서 제외하여 단순사고로 처리 가능

중대 보안사고의 정의

- 정보시스템이 비인가 접근에 의해 변조, 파괴되어 정성적인 서비스를 제공하지 못하는 경우
- 중요도 등급이 1등급(예 : 중요도 1/2/3 등급)인 정보자산 또는 비밀문서가 외부로 누출된 경우
- 정보자산의 오용으로 인하여 조직의 대외 이미지에 중대한 손상을 끼친 경우
- 관련 법규 및 규정 저촉으로 인하여 사회적 물의를 일으키는 경우
- 기타 고의 또는 과실에 의해 조직의 정상적 업무에 심각한 지장을 초래하는 경우
- 보안 장치의 변경이나 파괴 : 출입보안, 침입탐지시스템, 잠금장치, 보안 카메라 등

3 국내외 침해사고대응체계 구축 및 운영 현황

3.1. 국내 침해사고 대응체계

▮ 국가 사이버안전관리체계

우리나라는 사이버안전에 관한 국가적 조직체계의 확립을 목적으로 '국가사이버안전관리 규정'(대통령훈령 제141호, 2005.1.31)을 제정하였다. 이 규정을 기반으로 국가 사이버안전 체계의 수립 및 개선, 기관 간 역할 조정 등 국가 사이버안전에 관한 중

〈그림 1-3-1-1〉 국가 사이버 안전관리체계

요 사항을 심의하기 위한 '국가사이버안전전략회의'와 전략회의의 효율적 운영을 위한 '국가사이버안전대책회의'가 설치됨으로써 사이버안전 관리체계가 확립되었다.

국가정보원은 국가 사이버안전과 관련된 정책 및 관리에 대하여 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하고 있으며, 원 산하에 설립된 국가사이버안전센터를 통해 국가차원의 종합적이고 체계적인 대응을 수행하고 있다.

국가사이버안전센터(National Cyber Security Center : NCSC)는 지난 2004년 2월 20일 공식 출범, 정보통신망에 대한 24시간 사이버 위협 정보를 수집·분석·전파하는 국가상황실을 운영하는 것은 물론, 각종 사이버 공격에 대한 예방·대응활동과 피해확산을 방지함으로써 국가 주요 전산망에 대한 안전성을 확보하고 있다. 이들의 업무는 다음과 같다.

- '국가사이버안전매뉴얼' 및 '국가사이버안전관리규정' 제정 등 국가 사이버안전 정책 총괄
- 사이버안전 예방활동으로 각급기관의 정보통신망 신·증설 등 정보화사업 추진 시 보안성 검토, 정보보안관리수준 평가, 각급기관 내·외부 정보통신망에 대한 보안측정, 민·관·군 통합 사이버전 모의훈련, 국가 및 공공기관의 정보통신망에서 사용하고자 하는 정보보호 제품의 안전성 검증을 위해 보안적합성 검증제도 운영

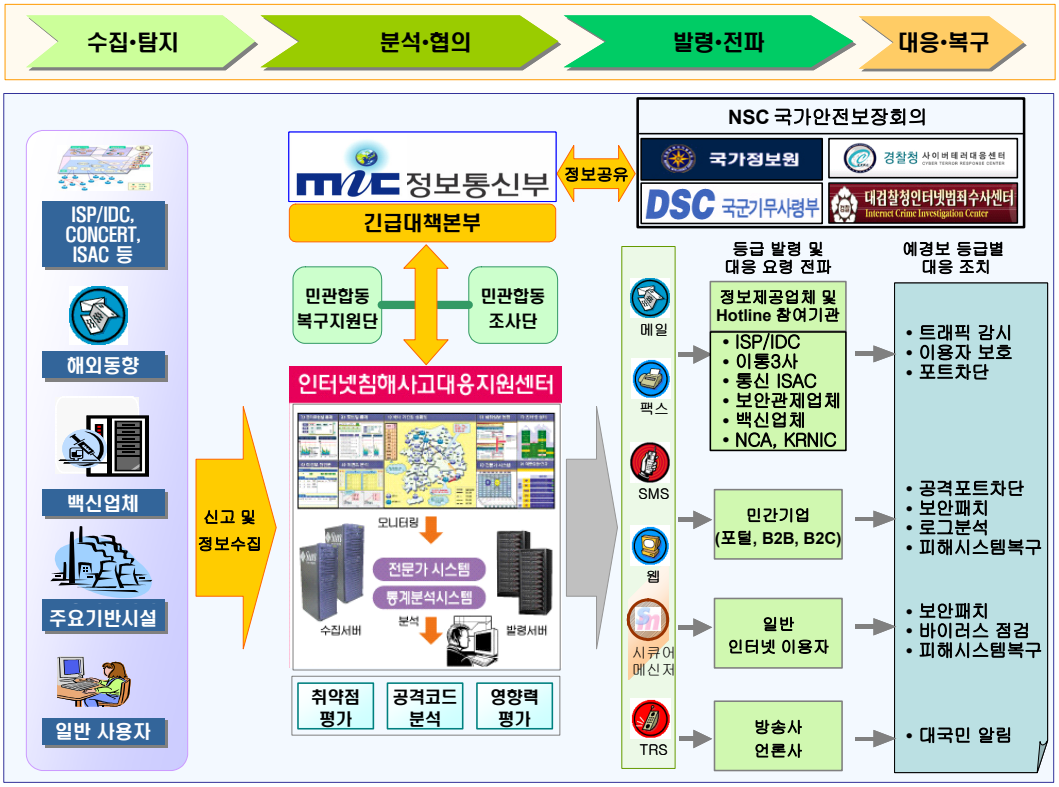
- 국가 주요 전산망에 대한 사이버 위협정보 수집·분석·전파 및 국가 사이버 위협 경보체계 마련·시행
- 침해사고 긴급대응 조사 및 복구지원, 피해 심각시 범정부 합동조사 및 복구지원팀을 구성·운영
- 국내·외 사이버안전 전담기구와 정보협력 및 공유체계 운영

한편, 국방부는 산하 국방정보전대응센터를 통해 국방 분야의 사이버안전 업무를 수행하며, 정보통신부는 산하 한국정보보호진흥원에 설치된 인터넷침해사고대응지원센터를 통해 민간분야의 사이버안전 업무를 수행하고 있다.

▌민간분야 침해사고 대응 체계

한국정보보호진흥원이 2003년부터 운영하고 있는 인터넷침해사고대응지원센터(www.krcert.or.kr)에서는 인터넷망의 트래픽 이상 유무를 24시간 관찰하고 신종 웜·바이러스 및 해킹 동향을 수집·분석하고, 예·경보 발령을 통해 침해사고에 신속히 대응하고 있으며, 다음과 같은 임무를 수행하고 있다.

- 24시간 주요 정보통신망에 대한 모니터링 및 조기 예·경보 실시
- 침해사고 발생 시 신속한 침해사고 원인 분석 및 적절한 대국민 대응조치 전파·지원
- 백신업체, S/W개발자 등과 시스템적으로 연계해 인터넷 침해사고 정보, 보안패치 정보 등을 종합적으로 수집·전파
- 금융·항공 등 개별망은 소관부처에서 보호하되 동 센터와 개별망 간에 Hot-Line을 구축하여 침해사고 정보공유 등 지원
- 국내·외 침해사고대응팀(CERT) 및 정보공유·분석센터(ISAC) 등과 비상연락체계를 정비하고, 세미나 등을 개최하여 정보공유의 장을 마련



〈그림 1-3-1-2〉 인터넷침해사고대응지원센터 업무 흐름도

한국침해사고대응팀협의회(CONCERT)

국가사이버안전센터나 인터넷침해사고대응지원센터처럼 국가기관이 주도하는 침해사고대응조직과 함께 국내에는 민간 기업 및 기관 내 소속된 침해사고대응팀이 자발적으로 참여하는 (사)한국침해사고대응팀협의회(CONCERT, CONsortium of CERT, www.concert.or.kr)가 있다.

(사)한국침해사고대응팀협의회는 기업, 대학 등의 소속 CERT들 간의 정보공유, 기술교류, 공동 침해 사고 대응을 위해 1996년 설립되었으며, 2005년 6월 사단법인으로 재출범하였다. 2007년 8월을 기준으로 정회원 102개사, 준회원 169개사, 협력회원 88개사 등 총 359개 민간 기업 및 기관 CERT, 그리고 정보보호 관련 서비스·솔루션 제조업체들이 CONCERT 회원사로 가입되어 있으며, 정보보호 사용자 그룹이라는 위상을 쌓아나가고 있다.

특히, '내 정보는 내가 지킨다'는 모토 아래, 각 기업 및 기관의 정보보호 수준제고를 위해 다양한 컨퍼런스·세미나·교육 프로그램을 기획·개최하고 있으며 이를 통해 정보보호에 대한 최신 동향과 기술흐름을 소개하는 한편, 기업 정보보호 실태조사 등 회원사들이 필요로 하는 다양한 보고서를 제작하고 있다. CONCERT의 주요업무는 다음과 같다.

- 신속한 정보교환을 위한 연락체계 구축
- 정보통신망 침해사고 관련 정보 및 기술 상호교환
- 국제적인 정보통신망 침해사고 대응을 위한 제반 활동
- 정보통신망 운영기관들의 CERT 구성 지원
- 침해사고 대응기술력 향상을 위한 교육 및 세미나 개최

이외에도 민간분야의 침해사고 관련 조직으로는 '전자금융거래 안전성 강화 종합대책'에 따라 금융부문의 정보보호 업무를 지원하기 위해 설립된 '금융보안연구원', '정보통신기반보호법' 제16조를 근거로 금융분야 주요 기반시설에 대한 침해사고 정보제공 등 공동 대응체계를 구축하기 위해 설립된 '금융 ISAC(Information Sharing and Analysis Center)'이 있으며, 국내 11개 기간통신사업자가 소속되어 있는 통신 ISAC은 2006년 독립 법인단체로 공식 출범하면서 "통신정보공유분석협회"로 개명하여 통신분야의 침해사고 대응과 정보보안 체계강화에 일조하고 있다.

▮ 사이버 범죄 관련 사법기관

해킹·바이러스 유포와 같은 사이버 범죄와 전자상거래를 이용한 사기, 개인정보 침해 등에 대한 수사기법 개발 및 관련 컴퓨터 범죄에 대한 총괄수사와 단속업무 수행을 위해 검찰과 경찰에도 사이버 범죄와 관련된 조직을 구성하여 운영하고 있다.

- 경찰청 사이버테러 대응센터 : http://www.netan.go.kr
- 대검찰청 인터넷범죄수사센터 : http://icic.sppo.go.kr

검·경찰의 사이버 범죄관련 조직의 임무는 다음과 같다.

- 사이버 범죄신고
- 프로그램 저작권을 복제하거나 배포, 전송 방지
- 불법 사이트 운영에 대한 처벌

3.2. 해외 침해사고 대응체계

대표적인 국제 침해사고 대응 조직으로는 FIRST(Forum of Incident Response and Security Teams, http://www.first.org)와 APCERT(Asia Pacific Computer Emergency Response Team, http://www.apcert.org)를 꼽을 수 있다.

FIRST(국제침해사고대응팀협의회)

FIRST는 전세계 침해사고 공동대응과 침해사고 예방, 정보공유 등의 협력강화를 목적으로 1990년 공식 출범하였으며, 2007년 8월 현재 전세계(아시아, 유럽, 미주 등)적으로 다양한 분야(대학, 정부, ISP 등)의 186개 침해사고대응팀이 회원기관으로 가입되어 되어 있다. 국내에서는 국가정보원, KISA, 안철수연구소, 인포섹 등 4개 기관이 회원기관으로 활동하고 있다.

- FIRST 회원 기관 리스트 및 연락처 : http://www.first.org/members/teams

FIRST는 다음과 같은 역할을 수행하고 있다.

- 기술정보, 도구, 방법론, 절차 및 모범사례 개발·공유
- 고품질의 보안제품, 정책, 서비스 개발 장려 및 홍보
- 컴퓨터 보안 관련 모범사례 개발 확산
- 침해사고대응팀 설립/확산 및 전세계 기관의 회원가입 장려

- 전세계 IT환경을 좀더 안전하게 만들기 위하여 자신의 지식, 기술, 경험을 통합하여 활용

APCERT(아 · 태침해사고대응팀협의회)

APCERT는 2003년 2월에 아·태지역내 국제 공동 침해사고대응 및 정보공유 등의 협력강화를 목적으로 공식 출범되었다. 2007년 8월 현재 14개의 정회원과 6개의 준회원으로 구성되어 있으며, 국내에서는 KrCERT/CC가 정회원 자격으로 APCERT에 가입되어 있다.

- APCERT 회원 기관 리스트 및 연락처 :
  http://www.apcert.org/about/structure/members.html

APCERT의 임무는 아래와 같다.

- 정보보호를 위한 아·태지역 및 국제적인 협력 확대
- 대규모의 네트워크 침해사고에 대응하기 위한 대책 개발
- 회원국 간 컴퓨터 바이러스, 악성코드 등에 대한 정보 공유 및 기술 교류
- 신속하고 효과적으로 회원들 간의 정보공유를 도모할 수 있도록 회원들의 관심주제에 대하여 연구개발 촉진
- 침해사고에 효과적으로 대응할 수 있도록 각 지역의 침해사고대응팀 지원
- 지역적 경계를 넘어선 침해사고에 효과적으로 대응하기 위한 법률적인 검토 및 조언

Ⅱ CERT 구축 시 고려사항

1. CERT 조직 구성

2. 구성원의 역할과 책임

3. 부서별 협력체계

1 CERT 조직 구성

CERT 혹은 정보보호 관련 조직체계는 기업의 규모와 산업분야에 따라 차이를 보이며, 인력 및 조직의 규모도 큰 차이를 보이고 있다. 과거에는 IT 조직 내 하나의 부서로 정보보호 관련 조직이 편성되어 있었지만 침해사고와 정보보호에 대한 중요성이 강조됨에 따라 정보보호 관련 부서가 IT 조직에서 벗어나 독립적으로 위치하는 경우가 늘어나고 있다. 또 정보보호와 관련된 조직 역시 기능과 역할에 따라 사내 전 부서를 아우를 수 있도록 다음과 같은 위원회 및 조직이 구성되고 있으며, 직무체계도 보다 세분화되고 있다.

▮ 정보보호위원회

정보보호위원회는 IT 센터의 장, 고문, 각 팀장, 운영파트장, 기업 정보보호 전담조직의 장으로 구성되며 정보보호 관련 최고 의사 결정 기구 역할을 한다.

▮ 정보보호 전담조직

정보보호 전담조직은 IT 센터장 직속기구이며, 회사 전체 내 정보보호 활동 및 보안 취약성 점검 기능을 수행한다.

▮ 정보보호 실무협의체

정보보호 실무협의체는 기업의 각 부서 혹은 팀 내 정보보호담당자로 구성되며, 정보보호 활동에 있어서 정보보호 전담조직과의 대응창구로서 각 부서 및 팀 내 정보보호 활동을 주관한다.

〈표 2-1-1-1〉 정보보호 관련 부서 직무체계 예시

구 분	정보보호 주요 역할
정보보호위원장 (기업최고책임자)	회사 정보보호 총괄 및 책임
	회사 정보보호에 관한 주요사항을 최고경영자 및 임원회의에 보고
정보보호위원회 (Security Forum)	회사 정보보호 활동 계획 및 예산 편성 검토
	정보보호 정책/지침/절차 등 규정의 검토 및 승인
	회사 주요 정보보호 이슈에 대한 대책 결정
	중대 정보보호 사고에 대한 검토 및 협의
	정보보호관리체계에 대한 개선기회의 평가 및 변경에 대한 필요성 평가 실시 등을 통한 경영검토 실시
정보보호 전담조직의 장 (Security Officer)	회사의 정보보호 실무 총괄 및 회사 정보보호 전담조직 관리
	정보보호위원회 회의 소집, 안건 상정 및 활동기록 유지
	회사 사업방향에 기초한 정보보호 계획수립 및 수행
	정보보호 관련 회사 소요 예산 편성/집행
	유관기관의 정보보호 관련 법, 규정 검토 준수 총괄
	정보보호 인식제고를 위한 교육 계획의 수립 및 실시총괄
	보안 취약성 점검 계획 수립 및 주관
정보보호전담조직 (Information Security Team)	정보보호 지침, 절차의 제정/개정/폐기 주관
	정보보호 사고 예방 및 대응 지원
	시스템 도입 또는 개발시 보안성 승인 시행
	임직원에 대한 정보보호 교육 및 인식제고 프로그램 주관
	보안솔루션 운영
	보안관제 시스템 운영 (보안관제 시스템 안정화 이후에는 운영팀으로 운영이관)
	주기적인 보안 취약성 점검
	회사자산에 대한 위험평가 수행
팀별 정보보호담당자 (Security Coordinator)	회사 정보보호전담조직과 협업 체계를 통해 팀내 정보보호 활동 수행 및 홍보
	팀내 자산 목록 관리
	팀내 보안사고 발생 시 회사 정보보호 전담조직과 협력하여 이를 처리
	정보보호에 대한 팀내 의견 수렴 및 전달
	새로운 시스템 또는 서비스에 대한 정보보호 기능 구현 시 팀내 적정성 평가 및 지원

팀별 품질관리자	정보보호 지침, 절차의 개정/폐기 관리
	사업계획서 관리 (정보보호 관련 사항)
각 팀장/파트장	팀내 정보보호 활동의 감독 및 책임
	정보보호 규정에 대한 팀내 준수여부 확인
시스템운영자	정보보호 정책/지침/절차 등의 규정에 준하여 시스템, 네트워크의 관리 및 운영
	고객사 및 사용자들에게 원활한 시스템 및 네트워크 서비스의 제공
	하드웨어, 소프트웨어 설치 및 관리
일반사용자	회사 정보보호 정책/지침/절차 등의 규정 준수
	자신에게 부여된 자산의 보호
	정보보호 취약점, 사고 및 각종 위반 발생시 지체 없이 관련자에게 보고
	회사 자산을 업무 외의 목적으로 사용하지 않음
	허용되지 않은 정보에 접근을 시도하거나 업무와 무관한 활동을 위해 정보보호 기능을 우회하는 시도를 하지 않음
	업무상 취득한 회사 또는 제3자 소유의 정보를 승인 없이 누설하지 않음

2 구성원의 역할과 책임

침해사고 예방 및 대응 업무 처리과정은 CERT를 구성하고 있는 구성원의 개인 능력과 신뢰성에 의존하게 된다. 특히, 최근에는 CERT 업무가 침해사고 발생 시 필요한 기술적 대응뿐만 아니라, 예방활동을 위한 보안정책 수립, 감사, 타 부서와의 업무 협의 등 다양한 업무를 수행해야 한다는 점에서 CERT 구성원의 개인능력은 더욱 중요해지고 있다. CERT 구성원이 갖춰야 하는 능력을 열거해 보면 다음과 같다.

- 개인 Skills : Communication, Problem Solving, Team Interactions, Time Management
- 기술 Skills : Security Principles, Risks Analysis, Vulnerability, Network Protocol, Security/Virus Issue, Application,

- 사고대응 Skills : Team Policy/Procedure, Communication, Incident Analysis, Recording, Tracking Information
- 전문 Skills : Presentation, Leadership, Expert Technology, Programming Skill

또한, CERT 구성원은 침해사고의 처리를 위해 아래와 같은 IT 분야의 기본 기술들을 이해하고 있어야 한다.

- 전반적인 데이터 네트워크(전화, ISDN, X.25, PBX, ATM, 프레임 릴레이 등)
- 네트워크 프로토콜(IP, ICMP, TCP, UDP 등)
- 네트워크 기반 요소(라우터, DNS, 메일서버 등)
- 네트워크 응용 프로그램, 프로토콜(SMTP, HTTP, FTP, TELNET 등)
- 기본 보안 원칙
- 컴퓨터와 네트워크 위험 및 위협
- 보안 취약성과 관련된 공격(IP 스니핑, 스니퍼와 컴퓨터 바이러스 등)
- 네트워크 보안 이슈(침입차단시스템, 가상사설망 등)
- 암호 기술, 전자서명, 해쉬 알고리즘 등
- 사용자와 시스템 관리자 측면의 호스트 시스템 보안(백업, 패치 등)

3 부서별 협력체계

앞서 언급했던 침해사고 대응과 예방을 위해 조직되는 정보보호위원회, 정보보호 전담조직, 정보보호실무협의체 등은 조직 내 침해사고 예방을 위한 보안정책 승인, 부서별 협력체계 구축, 보안정책 이행점검 등을 수행하게 되는데, 정보보호 전담조직이 계획한 정보보호 관련 정책 및 규정을 정보보호위원회가 승인하고 정보보호실무협의체가 이를 각 팀별 부서별로 적용시키는 것이 일반적이다.

정보보호위원회는 각 기업의 정보보호 전담조직의 장이 사전에 위원회 구성원을 통해 소집하며, 정기회의는 분기당 1회 실시하고 비정기 회의는 중대 보안사고 발생 시 소집되는 것이 일반적이다. 또한 정보보호실무협의체에서는 각 부서별 담당자들로 구성된 만큼 현업과 보안규정을 조율하게 된다. 부서별 보안체계에 대한 점검은 정보보호 전담조직이 수행하는 것이 일반적이며, 최근에는 부서별 참여도를 높이기 위해 정보보호 점검 체크리스트를 배포한 후 이에 대해 평가하는 방법이 등장하고 있다. 평가된 내용은 부서 혹은 팀별 성취도를 정량적으로 환산해 해당 부서나 팀에 대한 상벌규정으로 적용하기도 한다.

Ⅲ CERT 활동 계획 수립

1. 보안활동 계획 수립

2. 보안정책 및 지침 수립

3. 보안성 검토

4. 보안활동 성과관리 방법

1 보안활동계획 수립

CERT의 성공적인 활동을 위해서는 우선 해당 조직에 대한 정보보호 정책이 구축되어야 하며, 수립된 정보보호 정책을 통해 CERT의 역할 및 범위와 정보보호 활동 계획 등이 정의되어 유기적인 연관관계를 가져야 한다. 또, 필요에 따라 별도의 지침을 통해 세부활동 사항을 명시하여 수행해야 있다.

정보보호 정책은 기업이나 기관에서 보호해야 할 대상을 정의하고, 보호대상에 대한 해를 입힐 수 있는 위협대상을 분석 및 설정하여 유·무형의 자산보호 대책을 구현하고 이를 지속적으로 검토 보완해 나갈 수 있는 방안을 담고 있어야 한다.

1.1. 연간, 월간 계획

보안활동의 계획 수립 시 우선적으로 고려해야 할 사항은 기업이나 기관의 사업수행을 위한 요구사항을 만족하여야 한다는 점이다. 즉, 보안활동 자체를 위한 계획이 아닌 조직의 계속적인 사업수행을 보호하기 위한 활동이어야 한다. 이를 위해서는 정보보호 정책 또는 CERT 수행지침서를 통해 조직의 사업을 정의하고 사업 수행의 위협대상을 예방하고 제거하며 완화시키기 위한 목표로부터 보안활동을 계획하여야 한다.

보안활동 계획은 조직의 성격에 따라 연간 또는 월간 계획을 수립하여 진행하는 것이 체계적인 보안활동 수행에 효과적이다. 보안활동 계획수립 시 조직의 정보를 보호하기 위한 전략방향을 먼저 선정하고 그 전략에 따른 세부 실행과제를 설정한다. 이때 각 실행과제에 우선순위와 현황 및 목표를 명시하는 것이 중요하다. 마지막으로 실행과제의 수행시기를 표시하는 것으로 보안활동 계획을 수립한다.

〈표 3-1-1-1〉 보안활동 계획 수립(안)

보안활동 계획 수립

전략방향	전략과제	실행과제	우선순위	07년 목표	계획	2007年 1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	확인	비고
보안전략 및 계획	회사 경영방침에 준한 분야별 보안계획 수립	관리적, 기술적, 물리적 보안계획	H	2회/년	1월, 7월														
		해외법인 보안대책 강구	L	7월	1월~7월														
보안관리체계 확립	보안관리체계 일원화	보안관련 결치 및 양식 통일	M	즉시	1월~3월														
보안결차·지침 개선	표준 제/개정 활동	방문객 보안관리 지침 수립	P	제정	3월														
		세부 문서보안 관리지침 문서화	M	제정	3월														
		각 팀단별 테러 대비 방지책 수립	P	제정	5월														
위험분석 및 관리	Communication 활성화	보안장비 유지보수 및 개선 활동 . 출입통제, 검색장비, CCTV, 도감청	P	1회/분기	3월,6월,9월,12월														
		팀별 보안담당자 QBA 운영 및 워크샵 실시(	L	수시	5월														
	저장매체 사용 Log 분석	개인PC 보안 시스템 운영 및 결과보고	M	1회/분기	3월,6월,9월,12월														
	저장매체 사용 승인	각종 사용매체 타당성 분석 및 승인	M	수시	년간														
교육·홍보 활동	정기 보안교육	계층별 보안교육 실시	M	1회/년	4월														
	수시 입사자 보안교육	수시 입사자 보안교육 실시	M	1회/년	발생시														
	특별 보안교육(외부감사 초빙 교육)	임원 및 팀장급 대상 실시	L	1회/년	3월														
	보안담당자 전문화 활동	각 팀별 보안오림 교육	P	2회/년	2월, 10월														
		임직원 보안의식 설문조사 실시	L	1회/년	4월, 11월														
	보안 홍보·캠페인 활동	보안표어 신규 제작 및 배포	L	교체	1월														

1.2. 보안관리 성과지표

보안활동 계획 수립 후 실행과제의 목표달성을 위해 구체적인 달성방안을 수립하여 지속적으로 노력하여야 한다. 각 실행과제에 대한 목표 달성방안 및 성과지표를 수립하고 해당 목표수준을 가능한 수치/계량화하여 설정한다. 또한, 실행과제의 실적을 월별 또는 분기별마다 주기적으로 확인한다. 이러한 성과관리지표(KPI) 등을 통해 각 실행과제의 실적을 점검하고 향후 계획수립에 반영하여 보안활동의 개선 및 수준향상이 진행되어야 한다. 보다 자세한 성과관리지표 내용은 별도로 파트로 구분돼 4절에서 다룰 예정이다.

〈표 3-1-1-2〉 보안활동 성과관리지표(KPI)

KPI 관리양식

구분	지표명	가중치	'06년 목표	당분기		누적		차이분석(당분기)
				분기 계획	분기 실적	누적 계획	누적 실적	
보안부문	보안의식 강화활동	10	계열보안 의식도 90% 이상 달성	90%	91.3%	90%	91.3%	계획대비 101% 달성 (보안의식도=접수율+실사트점수)/2-보안감점)
	이동형 저장장치 관리방안 수립 및 시행	10	저장장치 보안 준수율 95% 이상 달성	95%	86%	95%	86%	계획대비 90% 달성 (팀별 저장장치 준수평가리스트 평균율)

2 보안 정책 및 지침 수립

기업이나 기관의 정보보호 활동은 해당 조직에 대한 위험을 분석하여, 규정을 수립하고, 해당 사항에 대한 표준을 제정하여 교육 및 홍보를 통해 기준을 적용한 후 보안점검 및 실사를 통해 개선활동을 하는 일련의 순환적인 관리체계로 구성되어 있다.

조직의 정보관리 체계를 성공적으로 수립하고 존속시키기 위한 초석으로는 최고경영진의 참여와 지원이 반드시 이루어져야 하며, 최고 경영진의 지도방향이 보안정책 및 지침을 통해 구성원들에게 선언되어야 한다. 또한 개별 자산들을 보호하고 특정한 보안 프로세스를 수행하기 위한 조직이 필요하며, 조직의 모든 구성원들에게 보안정책 및 절차에 대한 보안의 중요성에 대한 훈련 및 교육을 해야 한다. 마지막으로 보안통제의 효과를 평가하기 위해 규정준수 확인과 보안사고 발생 시 사고처리 및 대응도 성공적인 보안관리를 위한 핵심요소이다.

이러한 보안관리 핵심요소들의 역할과 관계는 보안정책을 통해 보안활동을 위한 상위수준의 문서로서 조직의 경영철학 및 고위경영진과 업무 프로세스 책임자들의 전략적인 사고를 나타내야 한다.

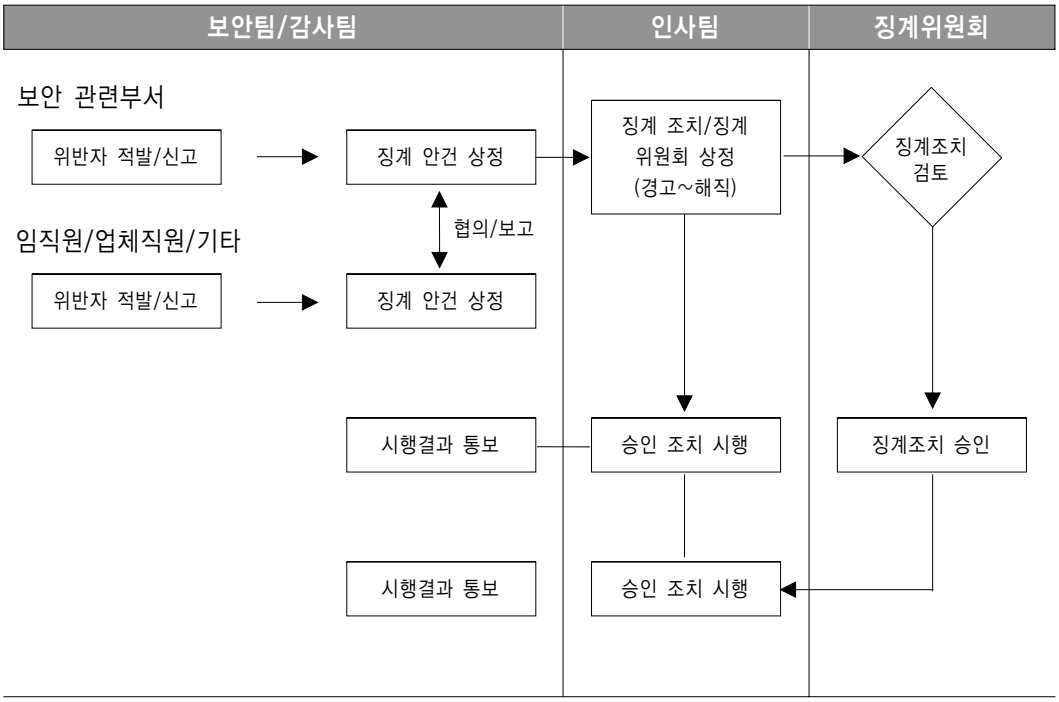
2.1. 보안정책의 일반적인 구성

- 보안조직 구성 및 운영
- 정보자산 관리
- 출입자 및 반출입 관리
- 인원 보안(입/퇴사자 관리)
- PC 보안
- 저장장치 보안
- 전산시스템 보안
- 통신망 보안

- 보안사고 예방 및 관리
- 상벌 기준

2.2. 보안정책 위반 시 대응 및 처벌방법

사내에서 발생하는 보안정책 위반사항에 대해서도 분명한 징계가 필요하다. 보안정책 위반사항 적발 시 징계위원회는 보안기준 위반자(고의, 실수, 공모, 교사, 방조자 등)와 해당 부서 관리책임자에 대해 징계 조치할 수 있다. 기업마다 징계처리 절차 및 수준은 다르겠지만, 일반적으로 보안기준 위반자를 대상으로 1차 보안경고장을 발부하고, 위반사항의 경중에 따라 보안책임자(CSO), 최고경영자(CEO) 명의의 경고장 발송하여 연간 벌점이 12점 이상 및 경고 1회 이상 대상자는 인사고과에 반영하도록 한다.



〈그림 3-2-2-1〉 보안 규정 위반자 징계 절차 예시

〈표 3-2-2-1〉 보안기준 위반내용 및 벌점/징계 건의 기준 예시

항 목	위반내용	대상자	벌점/징계건의 기준		
			A	B	C
보안의식 및 책임감	• 보안관리 점검 · 교육 미실시	책임자, 관리자	3점	2점	1점
	• 보안점검 결과 최하위 평가 시	책임자, 관리자	3점	2점	1점
	• 보안점검 수검 불량자	책임자, 관리자	3점	2점	1점
정보자산 관리	• 고의 또는 무단으로 비밀정보 유출 반출, 변조, 절취, 복제, 복사, 분실 후 은닉 등 위반 행위	위반자, 관리자	징계해직	견책	경고
	• 비밀정보 유출 및 공모하는 행위	위반자, 관리자	징계해직	감봉	경고
	• 비밀 및 대외비 자산 분실, 방치	위반자, 관리자	감급	견책	경고
출입자 및 반출입 관리	• 불법출입, 무단반출(임직원)	위반자, 관리자	징계해직	견책	경고
	• 불법출입, 무단반출(임직원외)	위반자, 해당	계약해직	출입취	퇴출
	• 사원증 미패용, 대여, 절취, 도용	위반자	징계해직	견책	경고
	• 출입시스템 Positive 미적용, 출입자 및 반출입 현황 미보관	운영담당자, 운영관리책임자	3점	2점	1점
	• 출입통제, 반출입 관리 부실	책임자, 담당자	감급	견책	경고
입.퇴사자 관리	• 퇴사자에 의한 비밀, 대외비성 정보 자산 유출	해당팀 관리자, 책임자	감급	견책	경고
	• 입.퇴사자 관리 기준 부실 – 전산장비 및 사원증 미회수 – ID 미삭제 등	해당부서 관리 책임자. 담당자	감급	견책	경고
	• 영업비밀보호 및 퇴직 보안서약서 미징구 등 관리 소홀	관리책임자/ 담당자/해당자	감급	견책	경고
PC 관리	• 백신, PC보안 S/W 등 미적용	책임자, 사용자	3점	2점	1점
	• 회사 전산장비 분실 및 관리 소홀	사용자, 관리자	감급	견책	경고
	• 개인용 PC 관리 기준 미준수 – 부팅, 화면보호기, 공유폴더 관리소홀	위반자, 관리자	3점	2점	1점
	• 미승인 전산장비/장치 반입 및 사용	위반자, 관리자	감급	견책	경고
	• 전산장비/장치 사외 무단 반출	위반자, 관리자	징계해직	감봉	경고
	• 전산장비/장치 업무 외적인 사용	위반자, 관리자	감급	견책	경고
	• 불법 H/W, S/W 사용	위반자, 관리자	감급	견책	경고
	• 임의 PC 본체 해체 및 파괴	위반자, 관리자	감급	견책	경고
	• 해킹의 경로 제공, 영업비밀 유출	위반자, 관리자	감급	견책	경고

3 보안성 검토

보안성 검토는 크게 보안기준 준수여부와 물리적인 자산의 반출여부, 전산시스템 등의 사용권한 요청을 검토 및 승인하는 것으로 다음과 같은 업무에서 적용에는 반드시 적용해야 한다.

- 네트워크 서비스 사용 절차
- 보안지침 절차 변경검토 절차
- 보안사고 신고 절차
- 비밀문서 반출/반입 절차
- 사원증 임시출입증 발급 절차
- 신규 정보시스템 도입절차
- 전산장비 반입/반출 절차

다음은 앞선 보안성 검토절차 일부를 차트형식으로 정리한 사례이다. 이를 바탕으로 각 업무 특성을 보안적 요소 구현에 정리할 수 있을 것이다.

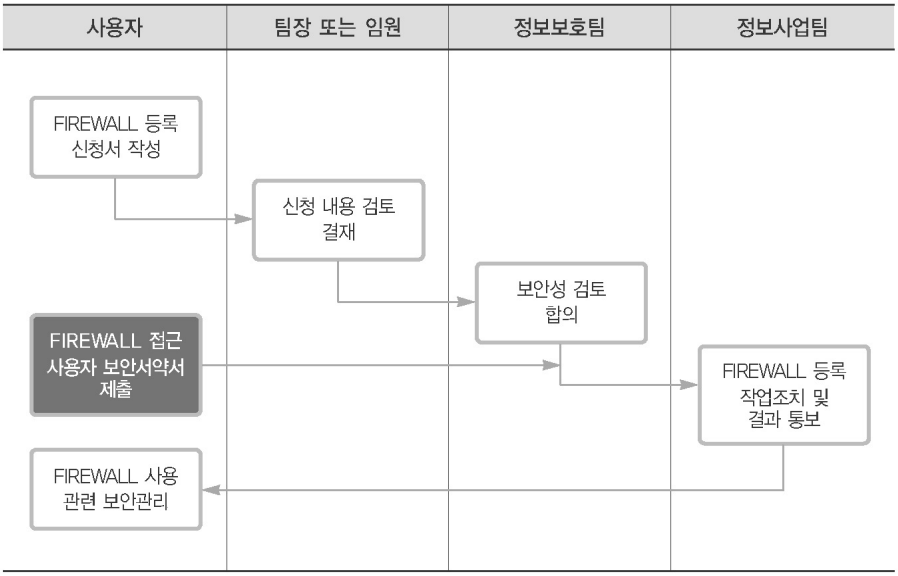
■ 절차 NO : 001

절차명	네트워크(FIREWALL) 서비스 사용 절차
생성일자	2005. 9. 1
소유자	정보보호팀
사용자	모든 임직원

■ 절차 개요

구 분	내 용
목적	- 네트워크(FIREWALL) 서비스 사용 허가에 대한 승인 통제
적용대상	- 모든 임직원(업무상 외부업체 및 거래성과의 정보교류시)
책임과 역할	- 신청자 : 신청서에 의거 신청(서약서 제출) - 팀장 또는 임원 : 검토 후 결재 - 지식보안팀 : 보안성 검토후 승인/반려 - 정보사업팀 : 지식보안팀 승인시 신청 사항 처리, 결과 통보
적용시점	- 매주 월요일, 수요일, 금요일 신청 시 적용

■ 절차 흐름도



〈그림 3-3-1-1〉 네트워크 서비스 사용 허가 보안성 검토절차 예시

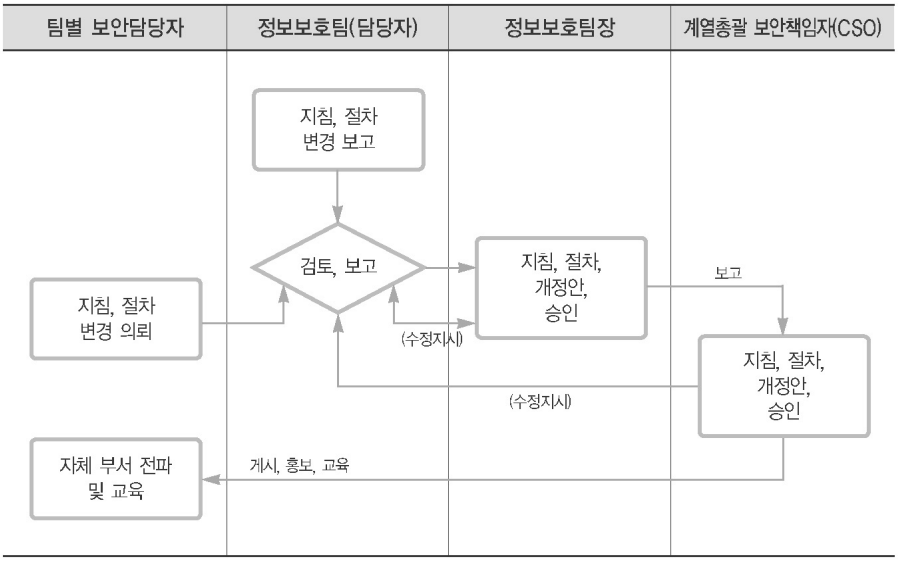
■ 절차 NO : 003

절차명	보안 지침/절차 관련 변경 검토 절차
생성일자	2005. 9. 1
소유자	정보보호팀
사용자	계열별 보안 관련 조직(총무팀, 연구소, 정보사업팀) 및 지식보안팀

■ 절차 개요

구 분	내 용
목적	– 보안 지침/절차 관련 변경 요청 및 의뢰가 있는 경우 적절한 검증 및 승인 절차에 따라 변경하는데 있음
책임과 역할	– 보안 지침/절차의 변경 의뢰 : 팀별 보안담당자 – 보안 지침/절차의 변경 검토, 보고 : 정보보호팀(담당자) – 보안 지침/절차의 변경 1차 승인 : 정보보호팀장 – 보안 지침/절차의 변경 2차 승인 : 계열총괄 보안책임자(CSO) – 변경된 관련 문서의 게시, 홍보, 교육 : 정보보호팀(담당자)
적용시점	– 최종 승인시 게시일자 기준으로 적용

■ 절차 흐름도



〈그림 3-3-1-2〉 보안지침/절차 변경 검토절차 예시

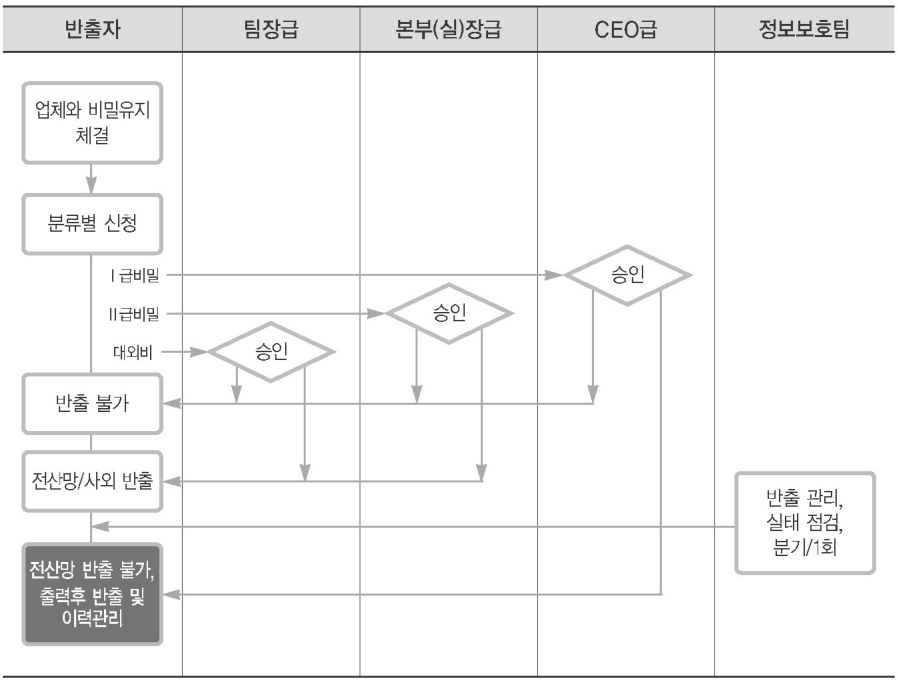
■ 절차 NO : 005

절차명	비밀문서 반출/반입 신청 절차
생성일자	2005. 9. 1
소유자	정보보호팀
사용자	모든 임직원

■ 절차 개요

구 분	내 용
목적	– 비밀문서 반출시 절차 명시
적용대상	– 모든 임직원
책임과 역할	– 비밀문서 반출 승인시 보안등급별로 적절한 관리 및 책임 의무
적용시점	– 비밀문서 반출시

■ 절차 흐름도(전산망/사외 반출)



〈그림 3-3-1-3〉 비밀문서 반철, 반입신청절차 예시

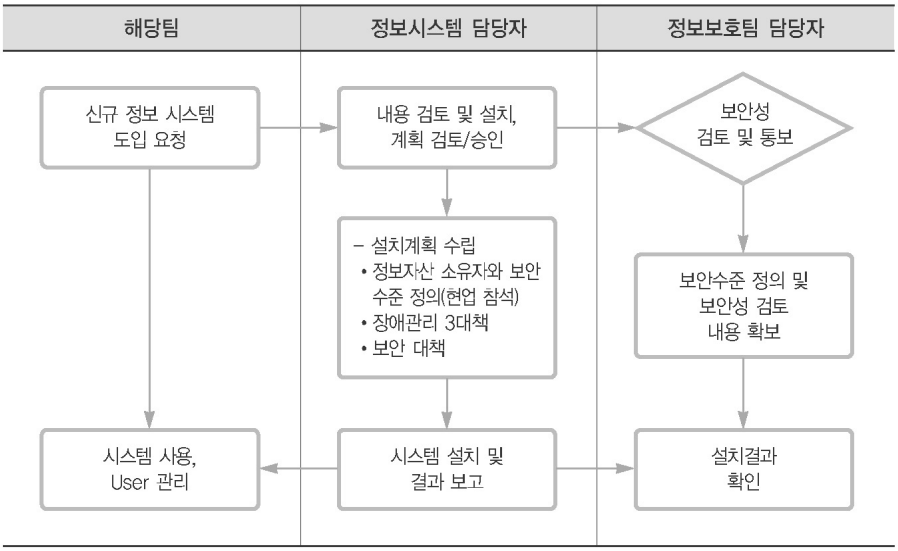
■ 절차 NO : 009

절차명	신규 정보시스템 도입 절차
생성일자	정보보호팀
소유자	정보보호팀
사용자	모든 임직원

■ 절차 개요

구 분	내 용
목적	- 신규 정보시스템(시스템, H/W, APP, OS, DB) 도입 표준에 대한 절차 정의 및 관리
적용대상	- 신규 정보시스템(시스템, H/W, APP, OS, DB) 도입하는 모든 부서
책임과 역할	- 해당 실(팀) : 신규 정보시스템 도입 및 설치 요청 - 정보사업팀 : 신규 정보시스템 설치계획 검토/승인, 보안적용 항목 정의 및 보안대책 적용 - 정보보호팀 담당자 : 신규 정보시스템에 대한 보안적용 항목 및 대책 적용 여부 감사
적용시점	- 항시

■ 절차 흐름도



〈그림 3-3-1-4〉 신규정보시스템 도입절차 예시

4 보안활동 성과관리 방법

기업 내에서 CERT 혹은 정보보호 활동을 펼치는 조직들은 타 부서와 달리, 이들의 성과를 증명하는 것이 쉽지 않다고 말한다. 해외 전문가들에 따르면, 이런 현상은 정보보호 관련 분야의 역사가 비교적 짧기 때문이라고 설명하고 있는데, 그럼에도 불구하고 최근에는 정보보호 관련 활동에 대한 성과를 입증하고 이를 관리하려는 노력이 지속되고 있다.

보안활동에 대한 성과관리를 도출할 때 가장 중요한 부분은 조직의 핵심 업무와 이해 관계자들의 요구사항에 얼마만큼 근접하고 있는가 하는 것이다. 보안업무에 대한 성과관리가 업무 요구사항과 일치하지 않고, 관리 지표가 명확하지 않다면 보안관리에 대한 지속적인 개선은 기대하기 어렵다.

보안활동에 대한 관리는 기본적인 것부터 조직의 핵심 업무와 연계된 복잡한 사안까지 다양하게 적용될 수 있겠지만, 여기에서는 일반적으로 적용 가능한 지표를 중심으로 소개해 보고자 한다. 향후 이 같은 지표를 바탕으로 정량적 보안수준평가 방법과 보안 성과관리가 조직성과에 어떠한 영향을 미치는 지에 대한 부분은 기업별 특성에 맞게 심도 있게 다루어야 할 필요가 있다.

성과관리를 위해서는 다음과 같은 절차가 필요하다.

4.1. 성과관리 계획 수립 및 기초 자료 수집

성과관리를 시행하기 전에 보안관리를 통하여 이루고자 하는 목표, 관리 분야. 보안업무 영향도 등을 분석해야 한다. 본격적인 활동에 앞서 각 기업 환경에 적합하고 현실적인 결과를 도출하기 위하여 예비지표를 정한다.

일부 기업의 경우, 보안 활동에 대하여 지표 관리를 실시하고 있었으나, 대부분 보안시스템 가용성, 즉 네트워크 보안장비의 가용성 값을 측정해, '99.99%에 이른다'는 식으로 표현하고 있는데, 이런 수치는 기술·운영 측면에서는 의미가 있지만 그 이상의 효과는 기대할 수 없는 경우이다.

4.2. 조직업무와 연관된 보안 관리

보안 업무 성과관리는 기술·운영 측면 이외에 조직 업무목표와 부합되도록 명확하게 정의하고 측정해야 한다. 보안업무 역시 조직의 목표와 전략적인 연관 관계가 명확하지 않다면, 이상적이고 관념적인 방향으로 치우칠 수 있으며, 실질적인 효과를 증명하기 어렵다.

4.3. 핵심 보안 관리 지표 선정

도출된 예비 지표를 기초로 목표에 대한 관리 수준을 설정하여야 한다. 성과관리의 목표는 현재의 보안수준을 파악하고 지속적으로 발전하기 위한 것이므로, 현재의 보안수준을 정확하게 인지하는 것이 무엇보다 중요하다. 조직 보안수준을 진단하기 위해서는 자체 기준을 설정할 수도 있고, 외부의 표준을 적용할 수 있는데, 이때 ISO27001, ISMS, SSE-CMM, NIST SP800-26, 800-53 등의 사례를 참조하는 것이 좋다.

보안관리의 지표는 아래 KPI 참조 표와 같이 Main 지표와 Sub 지표로 구분하여 관리하는 것이 향후 확대적용에 용이하다.

4.4. 자료 수집 및 분석

적절한 성과관리 지표가 선정되었다면 사전에 정의된 측정 주기별로 성과를 측정하고 평가하여야 하는데, 이때 가장 중요한 것은 결과에 대한 피드백이다. 즉, 시행 초기에 선정된 지표들이 실제 측정은 용이한지, 결과 값이 보안업무를 평가하는데 효과가 있는지 등을 지속적이고 주기적으로 분석하여야 한다. 특히 가용성 위주의 효율적인 보안시스템 운영에 대한 업무평가는 보안 관리업무의 효과성을 증명하는 단계로의 전환되어야 한다.

〈표 3-4-4-1〉 보안 성과관리 단계

구 분		내 용
1단계	계획수립 및 예비 KPI 선정	• 조직 업무와 연관된 보안 관리 지표 선정 • 가급적 정량적인 효과를 나타낼 수 있도록 선정
2단계	기초 정보 수집	• 주요 지표를 핵심적으로 관리하기 위하여 조직 보안수준 평가 필요 • 기존에 누적하여 축적된 데이트가 있다면 충분히 활용
3단계	핵심 보안 관리 지표 선정	• 예비 지표와 업무 영향을 고려하여 핵심 보안관리 지표 선정
4단계	관련 데이터 수집 및 분석	• 수집된 성과지표는 모든 이해 관계자들이 모여 검토 • 초기에는 월 1회 정도의 검토 회의가 적절
5단계	결과 재검토	• 일정기간 축적되고 관리된 성과지표는 일정 주기로 효과를 재검토하여 개선하여야 함

아래 표는 대부분의 조직에서 적용 가능한 보안 관리업무 범위를 사례로 보여주는 것인데, 어떤 보안 관리지표를 적용하는 것이 각 기업에 효과적인가에 대한 판단은 전적으로 보안 관리자의 몫이 된다. 선정된 성과지표는 성과지표가 가지는 목적, 측정 방법, 조직 내 보안 정책과의 연관, 측정 주기 등을 자세하게 기록하여야 한다.

〈표 3-4-4-2〉 보안 관리 주요 KPI(Key Performance Indicator) 예시

구 분	관리 지표	비 고
정보보호 활동 달성도	1. 정보보호 활동 계획 달성율	
보안 성숙도 관리	2. 보안 정책 준수율 - 개인보안 - 계정 및 패스워드 - 출입보안 - 영상보안 - 문서보안 - 외부인 출입 관리 등	
보안사고 예방 관리	3. 보안성 승인율	
	4. 보안 패치 적용률	
	5. 취약점 점검 개선율	
	6. 보안 정책 검토	
보안사고 관리	7. 중대한 보안 사고 처리 8. 보안사고 처리율	
가용성 관리	9. 보안 서비스 가용성	

〈표 3-4-4-3〉 성과지표 정의서 예시

정보보호 활동 계획 달성율	지표구분	정보보호 활동 달성도
	지표번호	xx-001
	개정번호	1.00
사용목적	조직의 정보보호 활동이 조직의 사업 요구사항을 합리적으로 지원하고, 정보보호관리체계 및 정보보호 활동에 대하여 평가하고 지속적으로 개선하기 위함	
위험	정보보호 계획에 대하여 달성도 검토가 누락되거나, 계획된 정보보호 활동 계획이 실행되지 않을 경우 조직의 정보보호 정책의 실효성 및 개선을 위한 활동이 상실되어 심각한 보안 취약점이 실현된 위험이 있음.	
관련지침	보안 정책 및 지침서	
핵심 성공 요소	고위 관리자에 의한 정보보호 활동 계획 승인 및 결과 검토	
측정공식	A /B * 100	
측정변수 정의	A	시행된 보안 활동 건수
	B	고위 관리자에게서 승인된 보안 활동 계획 건수
측정주기	분기	
측정책임자	보안 책임자	
측정대상 Source Data	A	보안 활동 결과 보고
	B	년간 보안 활동 계획서 및 관련 회의록
측정 시 주의사항	해당사항 없음	
목표치	70 %	
비고	해당사항 없음	

〈그림 3-4-4-1〉 월간 성과지표 측정결과 샘플

보안관리 업무는 조직의 특성에 따라 조금씩 다르기 때문에, 보안 성과관리 또한 자신의 환경에 맞는 표준이 있어야 한다. 이를 위해서는 6개월~1년 간 축적된 데이터와 시행착오를 바탕으로 현 조직체계에 적합한 보안 관리 표준을 선정하여야 하고, 이러한 지표들이 비즈니스 목표에 부합함을 지속적으로 평가하고 증명하여야 한다. 또한 성과관리 업무 또한 시행 초기부터 모든 부분을 충족시키겠다는 목표보다는 쉽게 접근할 수 있는 부분부터 실시하며, 타사 또는 선진 사례를 충분히 확보하여야 한다.

여기에서 가장 중요한 사항으로는 보안업무 역시 기업 내 타 부서와 마찬가지로 비즈니스 목표를 지원해야 한다는 것이다. 때문에 성과관리에서는 단지 자신의 업무를 측정하는 것에 그치지 않고, 조직의 업무목표와 연계되어 있음을 나타내어야 한다.

Ⅳ CERT 활동

1. 보안사고 예방활동

2. 보안교육 방법론

3. 보안감사

4. 법률준수(IT Compliance)

5. 보안 솔루션 도입

6. 보안사고 대응

7. 사이버 침해사고·범죄 신고 및 조사절차

8. 대외협력

1 보안사고 예방활동

1.1. 위험관리

▌위험관리와 정보자산의 분류

정보자산은 기존의 물리적 설비, 빌딩, 노트북, PC, 책상, 프린터 등과 같은 물리적인 형태로만 존재하는 것뿐만 아니라 데이터베이스 내 저장된 정보, PC 내 저장된 정보, 네트워크로 유통되는 정보 등 정보(Information)를 포함하고 있는 모든 것을 일컫는다. 때문에 기업의 정보자산을 해킹·바이러스 등의 침해사고로부터 보호해야 하는 CERT 혹은 정보보호 관련 부서는 기업 정보자산에는 무엇(정보자산 및 영향도)이 있고, 내재된 위험(취약성)은 무엇이며, 이를 위협하는 요소(위협요소)에는 무엇이 있는지, 또 이를 보호하기 위해서는 어떠한 보안대책(리스크 관리)을 수립해야 하는지 점검해 볼 필요가 있다.

이를 위해 가장 우선시 되어야 하는 단계는 정보자산을 분류하는 것이다. 일반적인 정보자산 분류 범주는 'Information, Paper, Software, Physical, People, Image, Service'로 구분되며 구체적인 항목을 각 분류로 묶을 수 있다. 이때 비즈니스에 미치는 중요도에 따라 식별된 자산에 대해 가치를 상(3점)·중(2점)·하(1점) 등의 방법으로 평가하고 위협 및 취약성 평가를 통해 위험을 산출해야 한다. 산출된 위험은 CERT 활동목표에 반영돼 해킹·바이러스 등의 침해사고 예방활동에 적용된다.

▌위협 발생 시나리오

위협과 취약성, 정보자산의 영향도 그리고 이들의 상관관계를 계산해 도출되는 리스크에 대해 하나의 시나리오를 가정해 보자.

1) PC에 중요 정보가 저장되어 있다.
2) 하지만 해당 PC는 백신 업데이트 및 패치가 적용되지 않았다.

3) 해당 PC에 저장된 정보는 암호화되지 않아 바이러스나 해킹 등으로 중요 정보의 기밀성, 무결성, 가용성이 손상될 수 있으며, 이 경우에는 사내 업무에 심각한 영향을 미칠 수 있다.

기업의 정보자산을 위협하는 리스크는 '리스크 = 위협 + 취약성 + 정보의 영향도'로 산출되는데 이렇게 산출된 리스크는 외부의 위협이 내부에 존재하는 취약성을 악용해 정보자산에 피해를 줄 수 있는 잠재성을 나타내며, 정보의 영향도와 위협의 빈도, 취약성의 정도를 각각 평가하여 그 합을 구함으로써 정량화할 수 있다.

앞선 시나리오를 바탕으로 리스크의 수치를 환산해 보면, 시나리오 상의 취약성이 발견되므로, 위협(2점)이 존재하며, 백신 업데이트, 정보 암호화, 패치 등이 적용되지 않았으므로, 여러 취약성(3점)을 갖고 있으며, 피해사고 발생 시 심각한 영향(3점)을 미칠 수 있으므로, 앞선 시니라오 상의 리스크 값은 8점으로 정량화할 수 있다.

여기에서 위협요소는 해당 정보가 존재하는 물리적, 논리적 공간의 특성에 따라 다르게 평가될 수 있으며, 컴퓨터 바이러스 이외에도 다양한 위협들을 대입시켜 볼 수 있다. 또 위협요소가 이미 발생한 경우, 누적된 히스토리 정보를 바탕으로 통계적 분석을 통해 빈도를 측정하고, 아직 발생하지 않은 위협은 기존에 발행한 위협과 비교하여 빈도를 추정해 위협요소와 함께 DB화해 각 정보자산에 대입시키는 것이 필요하다. 물론 구축된 위협 DB는 사고 및 침해 발생 시 주기적으로 갱신함으로써 현실과의 부합성을 유지하도록 지속적으로 관리해야 한다.

또한 취약성도 위협과 마찬가지로 단순한 기술적인 문제에서부터 사회공학적인 문제에 이르기까지 다양한 위협에 관계되어 여러 가지 형태로 존재한다. 특히, 네트워크나 시스템 공간에서 나타나는 취약성의 경우, 정보유통 및 이전 속도의 증가에 따른 위협과 관계가 있다. 그러나 대부분의 취약성은 기술적인 요인보다는 접근권한의 불확실성, 권한관리자의 이해부족, 오동작, 실수, 관리 절차의 미비, 규정, 절차 미준수 등 사람에 의한 것이 80% 이상을 차지하고 있다.

〈표 4-1-1-1〉 위협과 취약성 DB 예시

No	위협(Threat)	No	취약성(Vulnerability)	No	Concern (위협 + 취약성)
1	정보의 삭제	1	접근 통제 절차의 부재 혹은 부적절함	1+1	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 삭제
	정보의 삭제	2	사용자의 부주의	1+2	사용자의 부주의로 인한 정보의 삭제
	정보의 삭제	3	사용자 등록에 대한 관리 부족 혹은 결여	1+3	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 삭제
	정보의 삭제	4	정보 분류의 부정확성	1+4	정보 분류의 부정확성으로 인한 정보의 삭제
2	정보의 변조	1	접근 통제 절차의 부재 혹은 부적절함	2+1	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 변조
	정보의 변조	2	외부에서 장비 사용 시 보안 결여	2+2	외부에서 장비 사용 시 보안 결여로 인한 정보의 변조
	정보의 변조	3	암호화 통제 정책의 부재 혹은 부적절함	2+3	암호화 통제 정책의 부재 혹은 부적절함으로 인한 정보의 변조
	정보의 변조	4	사용자 등록에 대한 관리 부족 혹은 결여	2+4	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 변조
	정보의 변조	5	입출력 데이터 검증의 부재	2+5	입출력 데이터 검증의 부재로 인한 정보의 변조
	정보의 변조	6	키 관리의 부적절함	2+6	키 관리의 부적절함으로 인한 정보의 변조로 인한 정보의 변조
3	정보의 유출	1	접근 통제 절차의 부재 혹은 부적절함	3+1	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 유출
	정보의 유출	2	사용자의 부주의	3+2	사용자의 부주의로 인한 정보의 유출
	정보의 유출	3	암호화 통제 정책의 부재 혹은 부적절함	3+3	암호화 통제 정책의 부재 혹은 부적절함으로 인한 정보의 유출
	정보의 유출	4	사용자 등록에 대한 관리 부족 혹은 결여	3+4	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 유출
	정보의 유출	5	키 관리의 부적절함	3+5	키 관리의 부적절함으로 인한 정보의 유출
	정보의 유출	6	정보 분류의 부정확성	3+6	정보 분류의 부정확성으로 인한 정보의 유출
4	입출력 데이터의 오류	1	사용자의 부주의	4+1	사용자의 부주의로 인한 입출력 데이터의 오류
	입출력 데이터의 오류	2	입출력 데이터 검증의 부재	4+2	입출력 데이터 검증의 부재로 인한 입출력 데이터의 오류

▮ 리스크(Risk) 평가와 보장수준 정의

산출된 리스크는 위협 및 취약성 DB에서 해당 정보자산과 관계된 항목을 선택해 출현빈도 및 정도를 평가하고 정보의 영향도 값을 고려하여 평가된다.

〈표 4-1-1-2〉 위험도 산출 Sheet 예시

자산	자산 가치			위협/취약성(Concern)	Concern Value	Risk Value		
	C	I	A			C	I	A
메일	2	2	2	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 삭제	2	6	6	6
메일	2	2	2	사용자의 부주의로 인한 정보의 삭제	2	6	6	6
메일	2	2	2	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 삭제	2	6	6	6
메일	2	2	2	정보 분류의 부정확성으로 인한 정보의 삭제	2	6	6	6
메일	2	2	2	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 변조	2	6	6	6
메일	2	2	2	외부에서 장비 사용 시 보안 결여로 인한 정보의 변조	2	6	6	6
메일	2	2	2	암호화 통제 정책의 부재 혹은 부적절함으로 인한 정보의 변조	2	6	6	6
메일	2	2	2	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 변조	2	6	6	6
메일	2	2	2	입출력 데이터 검증의 부재로 인한 정보의 변조	2	6	6	6
메일	2	2	2	키 관리의 부적절함으로 인한 정보의 변조로 인한 정보의 변조	2	6	6	6
관리직 고과	3	3	1	접근 통제 절차의 부재 혹은 부적절함으로 인한 정보의 유출	2	7	7	5
관리직 고과	3	3	1	사용자의 부주의로 인한 정보의 유출	2	7	7	5
관리직 고과	3	3	1	암호화 통제 정책의 부재 혹은 부적절함으로 인한 정보의 유출	2	7	7	5
관리직 고과	3	3	1	사용자 등록에 대한 관리 부족 혹은 결여로 인한 정보의 유출	2	7	7	5
관리직 고과	3	3	1	키 관리의 부적절함으로 인한 정보의 유출	2	7	7	5

평가가 완료되면 위험도가 가장 높은 것부터 어느 수준까지 대책을 마련하여 조치를 취할 것인지를 자산 소유자간 협의를 통해 결정하게 된다. 조치방안이 필요한 대상이 아닌 감내할 만한 위험(Acceptable Risk)이라고 판단되면 그 수준을 보장수준(DoA : Degree of Assurance)으로 정의하게 된다. 가령, 감내할 위험의 수준을 6이라고 가정했을 경우, 앞선 위험도 산출표에서 리스크 가치가 7 이상이라고 평가된 관리적 고과의 경우, 사용자의 부주의로 인한 정보 유출이 발생할 경우 기밀성과 무결성 측면의 정보 훼손이 기업에 치명적인 영향을 가져오게 될 것이므로 적절한 보안대책이 필요하다는 것을 의미한다.

지금까지 정보자산의 종류 및 이에 대한 위협/취약성 도출, 위험평가와 보장수준(DoA)의 정의에 대해 살펴보았다. 그런데 이런 정보자산에 대해 위험평가 실시나 보장 수준결정은 왜 필요한 것일까. 기업에는 무수히 많은 정보가 존재한다. 하지만 모든 정보가 보호해야 할 대상이 되는 것인지는 생각해 볼 필요가 있다. 또 모든 정보에 대해 완벽한 보안환경을 구축하는 것이 최선인 것인지, 또 그로 인해 발생되는 구축비용, 시간 등의 투자 및 보안환경 구축 등이 업무 효율의 저하나 예산 및 시간을 낭비하는 것은 아닌지 점검해 보아야 한다. 이처럼 보안활동의 효율성을 고려한다면 정보자산의 중요도 및 위협이나 취약성을 명확하게 평가하고 분석할 수 있으며 특히, 중요한 자산들을 보호하는데 기업의 한정된 예산을 집중해 집행할 수 있게 된다.

1.2. 보안설정 가이드라인

지금까지 대부분의 기업들이 정보보호를 위해 각종 보안 솔루션을 도입함으로써 외부에서의 접근을 원천적으로 통제해 왔다. 하지만 최근에는 단순히 텍스트와 이미지만을 사용하는 홍보 웹 페이지에서 CGI를 이용한 게시판, 인터넷 카페, 실시간 예약, 인터넷 뱅킹까지 다양한 서비스가 이용되면서 그 구조는 점점 더 복잡해지고 있다. 특히, 웹 서버에 설치된 운영체제의 취약점, 웹서버 자체 취약점, 웹 애플리케이션 취약점 등 다양한 위협에 노출돼 있다. 또 DMZ를 구성해 운영한다고 하더라도 서버 존이 공격 받으면 내부망에 피해를 줄 수 있어, 네트워크 장비 보안, DB 보안, PC 보안 등은 총체적인 입장에서 보안을 고려해야 한다. 최근 등장하는 공격형태를 보면, 그들이 원하는 것은 단순히 자신의 실력과시를 넘어 주요 기밀정보나 금전적인 목적을 위

해 해킹을 시도하기 때문에 이들 시스템과 네트워크에 대한 보안점검은 필수적이다.

침해사고가 일어난 후 공격자의 의도를 파악하고 시스템이 어떤 식으로 악용되었는지를 찾는 행위는 사고가 일어나기 전 간단한 보안 설정을 하는 것보다 훨씬 어렵고 시간과 비용 소모적인 일이다. 때문에 이번 보안설정 가이드라인에서는 보안활동 중 예방활동의 측면에서 국내에서 가장 많이 사용되고 있는 플랫폼을 중심으로 장비의 보안 설정을 어떻게 해야 하는지 예제를 통해 체크해 보고자 한다. 이러한 체크리스트는 최초 설치 시 한 번의 점검에 그치는 것이 아니라, 주기적으로 체크하고 결과를 보관하는 과정이 필요하다. 보안은 심층방어(Defense in Depth) 속에서 지속적으로 행해야 하는 일련의 과정이라는 점을 기억해야 한다.

한편, 여기에서는 관리자들이 명령어 지식이나 설정을 할 수 있다는 전제하에 작성한 체크리스트이므로 어떻게 설정(How to)해야 하는지 보다는 웹서버(IIS, Apache), 운영체제(Windows NT, UNIX, Linux), 네트워크 장비(Router), PC, DB 등 5개 부분으로 나누어 보기 쉽게 표로 작성하였다. 다만, 아래에 제시되는 체크리스트에서는 다음과 같은 점을 염두에 두고 활용해야 한다.

1) 체크리스트에 제시된 조치예제는 시스템, 운영체제나 버전에 따라 조금씩 달라질 수 있다.
2) 보안패치, 로깅, 불필요한 요소 제거, 안전한 설정, 운영 등 5~6개 항목에 따라 분류했다.
3) 굵은 글씨로 표기한 것은 필수적으로 만족해야 할 항목을 의미한다.
4) 상세설명에서 〈참고〉란을 통해 보충설명을 포함한다.

IIS Web Server 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 웹서버가 운영되고 있는 운영체제는 최신 보안 업데이트를 하였는가?** **2. 현재 사용하는 웹서버 버전에 대한 최신 보안 업데이트를 하였는가?** (흔히 최신 보안 업데이트는 사용 중인 Application과의 호환을 이유로 미루는 경향이 있는데, 보안패치를 하지 않아 Critical한 문제가 발생하는 경우가 종종 있으므로 개발장비에서 반드시 미리 테스트 후 적용하도록 함) **3. ASP.NET Framework을 사용시 최신 버전으로 업데이트하였는가?**	

주요 Tool	1. IISLockDown (MS 제공 IIS 운영시 보안향상용 툴) 2. URLScan (MS 제공 IIS 운영시 HTTP 요청 제한 툴) 3. WebKnight (KISA 제공 IIS용 무료 웹방화벽)	
로깅	**1. 웹서버 로깅을 하고 있는가?** **2. 로그파일에 적절한 ACL을 설정하였는가? (관리자만 Read-Only)** 3. 로그파일은 주기적으로 백업하고 있는가?	
불필요 요소 제거	**1. 샘플 디렉토리와 기본 컨텐츠를 제거하였는가?** - %systemdirectory%₩inetsrv₩iisadmin - systemdirectory%₩inetsrv₩iisadmpwd - inetpub₩wwwroot (or ₩ftproot or ₩smtproot) - inetpub₩scripts - inetpub₩iissamples - inetpub₩adminscripts - %systemroot%₩help₩iishelp₩iis - %systemroot%₩web₩printers - %systemdrive%₩program files₩common files₩system₩msadc 2. 불필요한 COM 구성요소를 제거하였는가? - regsvr32 scrrun.dll /u 3. 불필요한 스크립트 매핑(Script Mapping)은 제거하였는가? - 홈 디렉토리 탭 → 응용 프로그램 구성 → 응용 프로그램 매핑 .asa, .asp, .bat, .cdx, .cer, .htr, .htw, .ida, .idc, .idq, .printer, .shtm, .shtml, .stm **4. 불필요한 ISAPI 필터는 제거하였는가?** [Frontpage ISAPI 제거] c:₩program files₩common files₩microsoft shared₩web server extensions₩40₩bin₩fpsrvadm -o uninstall -p all [Digest 인증], [HTTP 압축] 5. 사용하지 않는 모든 스크립트와 실행 파일은 제거하였는가? 6. 불필요한 SubSystem은 제거하였는가? - HKKM/System/CurrentControlSet/Control/Session Manager/SubSystems 삭제 - %systemroot%/system32 폴더에서 os2*, posix*, psx* 파일 삭제	
안전한 설정	**1. 디렉토리 인덱싱이 가능한 디렉토리가 있는가?** **2. 실행권한이 필요한 경우 특정 디렉토리로 한정하였는가?** (사용자가 임의로 업로드하는 디렉토리의 경우 실행권한 제거) **3. 불필요한 HTTP Method를 제거하였는가?** 4. 사용자 지정 에러 페이지를 사용하고 있는가? (웹서버의 에러코드는 RFC2616의 상태코드 정의부분에 명시되어 있음) **5. 상위 디렉토리로 갈 수 없도록 설정하였는가?** - 홈 디렉토리 탭 → 구성 버튼 → 옵션 → 상위 디렉토리 Disabled	

	6. SYN Attack을 방어하기 위한 설정을 하였는가? – HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩Services₩Tcpip₩Parameters – SynAttackProtect : 2 [REG_DWORD] 3 way-Handshaking이 완료될 때까지 자원의 할당을 지연 – TcpMaxHalfOpen : 100 (Server), 500 (Advanced Server) [REG_DWORD] SYN-ATTACK 공격이 동작하기 전 SYN-RCVD 상태 연결 개수 제한 – TcpMaxHalfOpenRetried : 80 (Server), 400 (Advanced Server) [REG_DWORD] SYN-RCVD 상태에서 연결되는 개수 제어	
운영	**1. 웹서버는 제한적인 계정으로 최소한의 권한을 가지고 운영되는가?** **2. 웹서버 설정파일과 주요데이터는 정기적으로 백업하고 있는가?** **3. 백업된 데이터는 정상적으로 복구하여 검증하는 절차가 있는가?** 4. cmd.exe, runas.exe에 대한 권한은 admin을 제외하고 모두 삭제하였는가? 5. 터미널 서비스를 사용하고 있다면, 적절한 ACL을 설정하였는가? 6. 주요 디렉터리(백업, 문서, 임시파일 등)는 webroot 외부에 생성하는가? 7. 가상 디렉터리에 적절한 ACL을 설정하였는가?	
주요정보 암호화	**1. 민감한 정보는 인증서를 이용하여 SSL/TLS로 암호화하고 있는가?** 2. IIS 서버에 RootCA 인증서를 업데이트하였는가?	
참고 사이트	IIS 공식패치사이트 www.microsoft.com/technet/security/current.aspx 웹서버 에러코드 정의 www.w3.org/Protocols/rfc2616/rfc2616-sec10.html SSL 설정 kldp.org/HOWTO/html/SSL-RedHat-HOWTO/ssl-redhat-howto-4.html IIS 보안설정 참고사이트 windows.stanford.edu/docs/IISseccheckIist.htm www.windowsecurity.com/articles/Installing_Securing_IIS_Servers_Part[1-3].html IISLockDown Tool www.microsoft.com/technet/security/tools/locktool.mspx URLScan Tool www.microsoft.com/technet/security/tools/urlscan.mspx	

아파치(Apache) Web Server 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 웹서버가 운영되고 있는 운영체제의 최신 보안 업데이트 하였는가?** **2. 현재 사용하는 웹서버 버전에 대한 최신 보안 업데이트하였는가?** (흔히 최신 보안 업데이트는 사용 중인 Application과의 호환을 이유로 미루는 경향이 있는데, 보안패치를 하지 않아 Critical한 문제가 발생하는 경우가 종종 있으므로 개발장비에서 미리 테스트 후 반드시 적용하도록 함)	

운영	**1. 웹서버 데몬이 최소권한(nobody 등)으로 운영되고 있는가?** **2. 웹서버 Root 외부 디렉토리 접근권한통제를 하고 있는가?** **3. 웹서버 설정파일과 주요데이터는 정기적으로 백업하고 있는가?** 4. 백업된 데이터는 정상적으로 복구하여 검증하는 절차가 있는가? 5. Rewrite 룰을 이용한 침입탐지를 하고 있는가? 6. 보안강화를 위한 보안 모듈(mod_Security 등)을 사용하고 있는가?	
로깅	1. 웹서버 로깅(access_log, error_log)을 하고 있는가? **2. 로그파일에 적절한 ACL을 설정하였는가?** 3. 로그파일은 주기적으로 백업하고 있는가?	
불필요한 요소제거	1. 설치 기본 디렉토리를 제거하였는가? (htdoc) 2. 불필요한 CGI 스크립트를 제거하였는가? **3. 불필요한 HTTP Method를 제거하였는가?** (일반적으로 GET,POST,HEAD만 허용)	
안전한 설정 (httpd.conf)	**1. 디렉토리 인덱싱이 불가능하도록 설정되었는가?** - Options → “ “Indexes” ” 제거 **2. 심볼릭 링크 기능을 해제하였는가?** - Options → “ “FollowSymLinks” ” 제거 **3. SSI를 이용한 실행권한을 제거하였는가?** - Options → “ “IncludeNoExec” ” 추가 **4. 실행권한이 필요한 경우 특정 디렉토리로 한정하였는가?** (사용자가 임의로 업로드하는 디렉토리의 경우 실행권한 제거) - ScriptAlias /cgi-bin/ “ “/usr/local/apache/cgi-bin/” ” 5. 응답헤더에서 웹서버의 버전정보(배너)를 숨기는 설정을 하고 있는가? - ServerTokens ProductOnly 6. 사용자 지정 에러 페이지를 사용하고 있는가? (웹서버의 에러코드는 RFC2616의상태코드 정의부분에 명시되어 있음) (예) ErrorDocument 404 /errorpagedefined/usr404page.htm 7. 시스템 설정을 보호하고 있는가? <Directory /> AllowOverride None </Directory>	
주요정보 암호화	**1. 민감한 정보는 인증서를 이용하여 SSL/TLS로 암호화하고 있는가?** 2. Apache 서버에 RootCA 인증서를 업데이트하였는가?	
참고 사이트	Apache 공식패치 사이트 www.apache.org/dist/httpd/patches 웹서버 에러코드 정의 www.w3.org/Protocols/rfc2616/rfc2616-sec10.html SSL 설정 kldp.org/HOWTO/html/SSL-RedHat-HOWTO/ssl-redhat-howto-4.html	

	Apache 보안 설정 팁 httpd.apache.org/docs/1.3/misc/security_tips.html (Version 1.3) httpd.apache.org/docs/2.0/misc/security_tips.html (Version 2.0) httpd.apache.org/docs/2.2/misc/security_tips.html (Version 2.2) Apache 보안 모듈 사용 mod_security : www.modsecurity.org (참고서적) Apache Security O' relly Book www.apachesecurity.net/download/apachesecurity-ch02.pdf www.thinkingstone.com/talks/Apache_Web_Platform_Security.pdf	

라우터 장비 보안 설정(Cisco 장비 기준)

항목	상세설명	체크
보안 패치	**1. 라우터 IOS는 최신 버전이거나 또는 최신 보안 업데이트하였는가?** (주요 네트워크 장비의 경우 가용성 때문에 오히려 최신버전의 IOS가 장애를 일으킬 수도 있어 운영자들이 업데이트를 꺼려하는 경향이 있으나, Critical한 보안 문제를 내포하는 버전의 경우 반드시 긴급패치를 해야 함)	

운영	1. 적절한 배너를 사용하고 있는가? (Banner)
	`Router(config)# banner exec ^C`
	2. 로그인 시간을 제어하고 있는가?
	`Router(config)# line con 0`
	`Router(config-line)# exec-timeout 15 0`
	`Router(config)# line vty 0 4`
	`Router(config-line)# exec-timeout 10 0`
	3. NTP를 통한 시간 동기화를 하고 있는가?
	`Router(config)# ntp update-calendar`
	`Router(config)# ntp server xxx.xxx.xxx.xxx`
	4. 설정 파일은 주기적으로 백업하고 있는가?
	5. 원격접근시 SSH를 사용하고 있는가?
	`Router(config)# line vty 0 4`
	`Router(config-line)# transport input ssh`
	6. 적절한 DNS 서버가 명시되어 있는가?
	`Router(config)# ip domain-lookup`
	`Router(config)# ip name-server xxx.xxx.xxx.xxx`
	또는
	`Router(config)# no ip domain-lookup`
	7. 일반 사용자 모드와 특권 모드의 패스워드가 다르게 지정되어 있는가?	

8. 라우팅 프로토콜 사용시 AS간 또는 피어 라우터에 MD5 인증을 적절히 구현하였는가?

(프로토콜별 예제)

BGP	router bgp 100 neighbor external-peers peer-group neighbor xxx.xxx.xxx.xxx remote-as 200 neighbor xxx.xxx.xxx.xxx peer-group external-peers neighbor yyy.yyy.yyy.yyy remote-as 300 neighbor yyy.yyy.yyy.yyy peer-group external-peers neighbor xxx.xxx.xxx.xxx password xxxxxxxxxx neighbor xxx.xxx.xxx.xxx password xxxxxxxxxx
OSPF	interface Ethernet0 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ip ospf message-digest-key 10 md5 xxxxxxxxxx router ospf 10 network xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy area 0 area 0 authentication message-digest
EIGRP	interface Ethernet0 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 mypassword . key chain xxxxxxxxxx key 12345 key-string abcdefg accept-lifetime infinite . router eigrp 1 network zzz.zzz.zzz.zzz no auto-summary

9. 주요 지점 네트워크 장비에서는 비공인 IP(RFC1918)를 필터링하여 IP Spoofing에 대응하고 있는가?

로깅

1. 라우터 장비 접속 로깅을 하고 있는가?

① 인증서버가 있다면, aaa logging을 적용하고 로그를 남기고 있는가?

② 로그에 timestamp를 남기고 있는가?

③ ACL 위반 패킷들을 로깅하고 있는가?

```
Router(config)# access-list 3 deny any log
Router(config)# access-list 101 deny any log
```

〈참고 : Logging 방식〉

○ Buffered Logging : 로그를 라우터 장비에 버퍼크기만큼 남김

```
Router(config)# logging on
Router(config)# logging buffered [size] debugging
Router(config)# service timestamp log date msec local show-timezone
```

ㅇ Syslog Logging : 로그를 원격 호스트에 514/udp를 통해 전달

```
Router(config)# logging on
Router(config)# logging host xxx.xxx.xxx.xxx
Router(config)# logging console critical
Router(config)# logging trap informational
Router(config)# logging facility local7
```

〈참고 : Logging Level〉

로깅레벨	보안수준	설명
Emergencies	0	
Alerts	1	즉각적인 조치 필요
Critical	2	치명적인 수준
Errors	3	에러 수준
Warnings	4	경고 수준
Notifications	5	보통이지만 알림 수준
Informational	6	정보 수준
Debugging	7	디버깅 메시지

2. 로그파일은 주기적으로 백업하고 있는가?

불필요 서비스 제거

1. 불필요한 AUX 라인이 제거되었는가?

```
Router(config)# line aux 0
Router(config-line)# transport input none
Router(config-line)# no exec
Router(config-line)# no password
```

2. 불필요한 서비스는 중단하였는가?

```
Router(config)# no service udp-small-servers          (echo, discard,
Router(config)# no service tcp-small-servers          daytime 등 중지)
Router(config)# no service finger                     (fingerd 중지)
Router(config)# no service tftp                       (tftp 서비스 중지)
Router(config)# no service pad                        (X.25 중지)
Router(config)# no ip bootp server                    (booting server 중지)
Router(config)# no service config                     (네트워크를 통해
Router(config)# no boot network                       config 파일을
Router(config)# no boot system                        읽어오는 설정중지)
Router(config)# no boot host
Router(config)# no ip source-route                    (IP Spoofing 대응)
Router(config)# no ip http server                     (웹서비스 중지)
Router(config-if)# no ip redirects                    (라우팅테이블변경악용)
Router(config-if)# no ip unreachables                 (스캐닝공격대응)
Router(config-if)# no ip directed-broadcast           (Smurf Attack 대응)
Router(config-if)# no ip proxy-arp                    (ARP 서비스 중지)
Router(config-if)# no ip mask-relay                   (netmask요청응답중지)
```

3. FTP, RCP, RSH 등과 관련된 다음 라인들이 존재하지 않는가?

```
ftp-server enable
ip rcmd rcp-enable
ip rcmd rsh-enable
transport input rlogin telnet
```

안전한 설정 (show running-config)

1. 라우터 안전한 패스워드를 사용하고 있는가?

[Console 접속시(물리적인 접근 필요)]

```
Router(config)# line con 0
Router(config-line)# password xxxxxx
Router(config-line)# service password-encryption
```

[Virtual Terminal 접속 시 (Telnet 등을 통한 원격접근 시)]

```
Router(config)# enable secret xxxxxx
```

➔ enable secret0이 가장 우선이지만 같은 패스워드를 쓰지 않도록 주의

```
Router(config)# line vty 0 4
Router(config-line)# transport input none
Router(config-line)# no exec
Router(config-line)# exec-timeout 0 1
```

➔ 원격접속 자체가 필요없는 소규모 사업장인 경우 telnet listener 다운

〈참고 : Password 저장방식〉
ㅇType0 : Config 파일에 누구나 읽을 수 있는 평문으로 저장
service password-encryption 명령어로 Type7 암호화 가능
ㅇType5 : MD5의 해시함수를 사용하여 복호화가 불가능, 가장 안전함
ㅇType7 : Vigenere Algorithm을 사용하여 암호화하나 역함수 존재

2. 접근통제(ACL)를 하고 있는가?

ㅇ 유의사항 및 예제
- access-list 룰을 원격접속에 적용시 access-class 사용
  ➔ access-class [ACL#] {in|out}
- access-list 룰을 특정 인터페이스에 적용시 access-group 사용
  ➔ access-group [ACL#] {in|out}
- access-list는 중복설정 불가
- 해당 룰의 마지막에는 항상 “deny any any” 가 추가됨
- access-list의 룰의 여러 개일 때 특정라인만 삭제/변경 불가

```
Router(config)# access-list 10 permit host xxx.xxx.xxx.xxx
Router(config)# access-list 10 permit host yyy.yyy.yyy.yyy
Router(config)# access-list 10 deny any log
Router(config)# access-list 100 deny tcp any any eq 135
Router(config)# access-list 100 deny ip host x.x.x.x host y.y.y.y
Router(config)# access-list 100 permit tcp any any
Router(config)# line vty 0 4
Router(config-line)# access-class 10 in
Router(config-line)# exit
Router(config)# int s0
Router(config-if)# ip access-group 100 in
Router(config)# access-list 100 deny ip zz.zz.zz.zz yy.yy.yy.yy any log
```

〈참고 : Access-List 유형과 사용법〉
ㅇstandard access-list : 패킷의 소스IP로만 허용/차단 (1~99)
➔ access-list [ACL#] {permit|deny} {src IP wildcard|any}
ㅇextended access-list : 소스IP, 목적지IP, Port, Protocol 등으로 확장하여 허용/차단 (100~199)
➔ access-list [ACL#] {permit|deny} [ip|tcp|udp|icmp] {src IP wildcard|any|host} {dst IP wildcard|any|host}

3. SNMP(Simple Network Management Protocol) 접근제한을 하고 있는가?

① Community String은 쉽게 추측할 수 없는 문자열로 설정했는가?
② SNMP RO(Read Only)와 RW(Read Write) 문자열을 다르게 설정했는가?
③ 암호화가 지원되는 상위 SNMP(v3)를 사용하고 있는가?

➔ snmp-server community [string] {ro|rw} [ACL#]

```
Router(config)# access-list 10 permit host 7.7.7.5
Router(config)# snmp-sever community xxxxxx RO 10
```

4. 사용자 계정을 통해 인증을 하고 있는가?

```
Router(config)# username xxxxxxx password 7 xxxxxxxxxxx
```

5. 인증서버가 있다면 적절히 구성되었는가? (AAA 서버)

① 인증서버를 이용하여 원격접근시 구성을 적절히 하고 있는가?

```
Router(config)# aaa new-model
Router(config)# aaa authentication login [list-name] tacacs+ local
.
Router(config)# tacacs-server host x.x.x.x
Router(config)# tacacs-server key xxxxxxx
Router(config)# line vty 0 4
Router(config)# login authentication [list-name]
```

② 인증서버를 이용하여 SSH,SCH 구성을 적절히 하고 있는가?

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization exec default group tacacs+
.
Router(config)# ip ssh time-out 120
Router(config)# ip ssh authentication-retries 3
Router(config)# ip scp server enable
```

참고 사이트	Cisco Router 공식 IOS 사이트 www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html www.cisco.com/warp/public/732/updatesw.shtml 참고사이트 www.windowsecurity.com/whitepapers/Cisco_Router_Security_Overview.html

PC 보안 체크리스트(Windows XP 기준)

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 최신보안패치를 하였는가?** Internet Explorer → **도구** → Windows Update 사이트 **2. 서비스팩이 설치되어 있는가?** **3. 자동 업데이트를 사용하고 있는가?** 시작 → 설정 → 제어판 → 보안센터 → 자동업데이트를 사용함으로 설정	
주요 Tool	**1. 바이러스 백신을 설치하고 최신 버전의 엔진으로 업데이트하였는가?** **2. 윈도우에서 기본적으로 제공하고 있는 개인 방화벽을 사용하고 있는가?** 시작 → 설정 → 제어판 → 네트워크 연결 → 로컬영역 연결 속성 → 고급 탭 → 윈도우 방화벽 사용 → 예외 탭에서 예외 프로그램 / 포트 추가 **3. 스파이웨어/애드웨어 제거 프로그램을 설치하고 최신 업데이트하였는가?** 4. 기타 무상/상용 침입차단시스템 또는 개인 방화벽이 있는가? 5. 사용하고 있는 소프트웨어(오피스 등)는 주기적으로 업데이트하고 있는가? 6. 사내 전용 PC보안 프로그램으로 통제하고 있는가? (존재시)	
불필요 요소 제거	**1. 불필요한 공유를 중지하였는가?** ① 시작 → 설정 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 공유폴더 → 공유 → 불필요한 공유 폴더 중지 ② 시작 → 실행 → cmd.exe C:₩ net share [공유폴더명] /delete ③ 시작 → 실행 → regedit.exe (레지스트리 편집) KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver ₩parameters (키 생성하기) Value Name : AutoShareWks Type : REG_DWORD Value : 0 **2. 널세션을 제거하였는가? (IPC$)** 시작 → 실행 → secpol.msc → 로컬보안정책 → 보안옵션 → 네트워크 액세스 : SAM계정과 공유의 익명열거 허용안함을 사용함 설정 3. 드라이브 전체를 공유하거나 공유폴더 설정이 잘못되어 있지는 않은가? 4. 불필요한 서비스를 제거하였는가? SMTP, FTP , World Wide Web Publishing, NNTP, IIS ADMIN MSSQLServer / MySQL 등 DB서버, Telnet, Terminal Services, Messenger Service, SNMP Service, SNMP Trap Service 등	
안전한 설정	**1. 웹브라우저의 보안 설정을 하였는가?** ① Internet Explorer → 도구 → 인터넷 옵션 → 보안 → 보통이상 설정 ② Internet Explorer → 도구 → 인터넷 옵션 → 내용 → 자동완성 비활성화 **2. 불필요한 ActiveX가 존재하는가?** C:₩windows₩Downloaded Program Files	

	3. ActiveX 컨트롤에 대해 서명되지 않은 플러그인은 통제하고 있는가? Internet Explorer → 도구 → 인터넷 옵션 → 보안 → 사용자 지정 수준 → ActiveX 컨트롤 및 플러그인 관련설정 서명 안 된 ActiveX 컨트롤 다운로드 : 사용안함 안전하지 않는 것으로 표시된 ActiveX 컨트롤 초기화 및 스크립트 : 사용안함 ActiveX 컨트롤에 대해 자동으로 확인 : 사용안함 4. 메신저를 사용하는 경우 자동로그인이나 자동저장기능을 해제하였는가? 5. 주요메시지나 파일은 암호화하여 전송하는가? 6. 웹메일을 사용하는 경우 보안접속 기능을 사용하여 로그인하는가? **7. P2P 프로그램으로 출처를 알 수 없는 파일을 받았거나, 웹에서 다운로드받은 프로그램을 실행하기 전 백신프로그램으로 해당 파일을 검사하고 있는가?** **8. 메일 클라이언트에서 '사용할 IE' 보안영역을 제한된 사이트로 한정했는가?** **9. 공유 폴더 설정시 Everyone 그룹을 제거하고 특정 사용자에게 읽기/쓰기 권한을 명확히 주고 있는가?** 10. 원격지원이 불가능하도록 설정되어 있는가? 내컴퓨터 → 속성 → 원격 → 원격지원 요청/사용자 원격연결 체크박스 해제 11. 관리자 계정 administrator를 다른 이름으로 바꾸었는가?	
관리	**1. CMOS 또는 로그온시 패스워드를 설정하였는가?** **2. 8자 이상의 길이로 영문자, 숫자, 특수문자 등이 혼용된 비밀번호를 쓰고 있으며 주기적으로 변경하는가?** **3. 불필요한 사용자 계정을 삭제했는가?** 시작 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 로컬 사용자 및 그룹 → 사용자 → Guest 등 불필요한 계정 사용 안 함 4. 화면 보호기의 암호를 설정하였는가? 바탕화면 오른쪽 마우스 버튼 → 등록정보 → 디스플레이 등록정보 → 화면보호기 → 암호사용 → 변경 5. NTFS 파일 시스템을 사용하고 사용자별로 접근통제를 하는가? C:₩ convert drive_letter: /fs:ntfs **6. 출처가 불분명한 이메일이나 수상한 첨부파일이 있는 경우 확인하지 않고 바로 삭제하고 있는가?** **7. 웹사이트 방문시 보안경고 창이 뜰 경우 신뢰할 수 있는 기관에 대해서만 프로그램 설치에 동의하는가?** **8. 주요 데이터는 주기적으로 별도의 저장장치에 백업하고 있는가?** **9. 금융 거래용 공인인증서는 USB와 같은 별도 저장장치에 보관하고 있는가?** 10. 사용하지 않을 때 PC를 인터넷에 연결하여 켜놓지는 않는가? 11. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	[FAT->NTFS 변경] technet.microsoft.com/en-us/library/bb456984.aspx www.microsoft.com/protect/yourself/home/office.mspx	

유닉스(UNIX) 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 최신 Patch를 적용하였는가?** **2. 보안 업데이트 주기를 설정하고, 정기적으로 수행하고 있는가?** **3. 사용하고 있는 소프트웨어는 최신 버전으로 유지하고 있는가?** **4. 특히 SUID, SEUID가 설정된 파일 중에서 버퍼 오버 플로우 등 공개된 취약점을 내포하고 있는 파일들은 최신 Patch를 적용하였는가?** 〈참고 : Overflow 취약성이 많이 공개된 서비스들〉 RPC, SNMP, NFS, X Window, BIND, OpenSSH, OpenSSL 의 낮은 버전	
주요 Tool	**1. TCP Wrapper를 사용하여 접속제한을 하고 있는가?** ① /etc/hosts.deny 파일 내용을 "ALL:ALL"로 구성하여 불필요한 호스트로부터의 서비스 접근통제를 하고 있는가? ② /etc/hosts.allow 파일에서 인가된 관리자에게만 권한이 허용되어 있는가? ③ 각 설정 파일은 일반 사용자가 읽을 수 없도록 600 권한을 주었는가? ④ /etc/inetd.conf 내의 모든 TCP 서비스를 wrapping 하고 있는가? 2. Iptables와 같은 방화벽(방화벽을 따로 사용하지 않을 경우)에서 Inbound Traffic에 대한 접근통제(INPUT, OUTPUT, FORWARD)를 하고 있는가? **3. Tripwire 등 무결성 검사 소프트웨어를 정기적으로 수행하여 시스템상 변경 여부를 정기적으로 확인하고 있는가?** 4. John the Ripper 등의 도구를 이용하여 패스워드 점검을 정기적으로 수행하는가? (암호가 없는 계정, 추측 가능한 암호 사용 등) 5. nmap 등의 포트 스캐닝 도구를 이용하여 로컬시스템에서 불필요한 포트에 대한 점검을 정기적으로 수행하는가? **6. 평문으로 전송하는 Telnet, ftp 대신 OpenSSH와 같은 공개툴을 이용하여 암호화된 통신을 하고 있는가?** **7. Cron 등 정기적으로 수행할 수 있는 도구을 이용하여 주요 보안 리포트를 정기적으로 관리자에게 리포팅하는가?** 8. chkrookit 등과 같은 백도어 설치 탐지 툴을 이용하여 주기적으로 시스템 내 백도어 존재 유무를 점검하고 있는가?	
불필요 요소 제거	**1. 반드시 필요한 소프트웨어만 설치되었는가?** **2. 불필요한 계정은 삭제되었는가?** 3. /etc/hosts 파일에 불필요한 시스템이 포함되어 있지는 않은가? **4. 보안상 취약한 setuid, seteuid, setgid가 제거되었는가?** # find / -type f ₩(-perm -04000 -o -perm -02000 ₩) -exec ls -lg {} ₩; 5. 소유자가 없거나 그룹 아이디가 없는 파일이 존재하지 않는가? # find / -type f -nouser -o -nogroup -print 6. 누구나 변경할 수 있는 민감한 파일(World-Writable)은 존재하지 않는가? # find / -type f -perm -2 -print **7. NFS를 사용하여 불필요하거나 민감한 디렉토리가 마운트되지 않았는가?** # showmount -e	

8. Cron 데몬에 불필요하게 자원을 낭비하는 사용자/프로세스는 제거되었는가?
9. DoS 공격에 취약한 네트워크 서비스와 불필요한 서비스가 제거되었는가?

tcpmux	1/tcp	unrpc	111/tcp
echo	7/tcp	etbios-ns	137/tcp
echo	7/udp	etbios-ns	137/udp
discard	9/tcp	etbios-dgm	138/tcp
discard	9/udp	etbios-dgm	138/udp
systat	11/tcp	etbios-ssn	139/tcp
daytime	13/tcp	etbios-ssn	139/udp
daytime	13/udp	map	143/tcp
netstat	15/tcp	nmp	161/udp
chargen	19/tcp	nmp-trap	162/udp
chargen	19/udp	dmcp	177/udp
ftp	21/tcp	xec	512/tcp
ssh	22/tcp	iff	512/udp
telnet	23/tcp	login	513/tcp
smtp	25/tcp	who	513/udp
domain (DNS)	53/tcp	shell	514/tcp
domain (DNS)	53/udp	syslog	514/udp
bootps	67/tcp	printer	515/tcp
bootps	67/udp	talk	517/udp
bootpc	68/tcp	ntalk	518/udp
bootpc	68/udp	route	520/udp
tftp	69/udp	klogind	543/tcp
finger	79/tcp	socks	1080/tcp
http	80/tcp	nfs	2049/tcp
pop2	109/tcp	nfs	2049/udp
pop3	110/tcp	X11	6000+n/tcp

안전한 설정

1. /etc/passwd 파일은 적절히 구성되었는가?

① 사용자 패스워드는 암호화되어 /etc/shadow에 존재하는가?
② UID가 0인(루트 권한) 사용자가 존재하는가?
③ GID가 0인(루트 권한) 사용자가 존재하는가?
④ 추측하기 쉬운 패스워드를 사용하는 사용자가 존재하는가?
⑤ 벤더 기본 계정(daemon, bin, adm, lp, uucp 등)에 shell이 부여되어 있는가?
⑥ 패스워드 에이징(Aging,일정기간 이상이면 변경 또는 잠금) 정책이 있는가?

- /etc/default/passwd
  ➔ MAXWEEKS, MINWEEKS, PASSLENGTH 설정

〈참고〉
/etc/shadow 파일 필드 내용
[(1)아이디 : (2)암호화된 패스워드:최근 패스워드 변경일 : (3)패스워드를 변경해야 하는 최소일수 : (4)변경한 패스워드를 사용할 수 있는 최대일수 : (5)패스워드를 변경하도록 강제하는 경고일수 : (6)패스워드가 만기된 후 실제 사용중지까지 일수 : (7)사용중지날짜]

2. 원격 접속시 루트로 로그인할 수 없도록 통제되어 있는가?

① /etc/securetty (HP-UX) : CONSOLE
/etc/default/login (Solaris) : CONSOLE=/dev/console

② 파일 권한은 600으로 설정하였는가?

3. /etc/inetd.conf 은 적절히 구성되었는가?

① 소유자는 root이고 파일 권한은 600으로 설정하였는가?

② r 시리즈 명령어 (rlogin, rsh, rexec)는 사용하지 않고 있는가?
만일 사용하고 있다면, 접근통제를 철저하게 하고 있는가?

③ ttdb, cmsd, tftp 등 보안에 취약한 데몬은 제거되었는가?

4. /etc/hosts.equiv, $HOME/.rhosts 파일이 존재한다면, 적절히 구성되었는가?

① "+","+ +" 설정(임의의 사용자과 권한 획득가능 상태)이 금지되었는가?

② 사용하지 않는다면, /dev/null로 링크되어 있는가?

③ 일반 사용자들이 자신의 홈디렉토리에서 생성할 수 없도록 통제하는가?

④ 소유자는 root이며, 파일 권한은 600으로 설정하였는가?

5. 일정시간이 지난 후 자동 로그아웃하는 session timeout이 설정되었는가?
(예제) /etc/system ➔ set swip:tcpidletimeout=100
/etc/default/login ➔ TIMEOUT=300

6. 서버 접근시(telnet, ssh, ftp 등) IP별 접근 제한을 설정하였는가?

7. 비로그인 데몬은 root가 아닌 nobody 권한으로 동작하고 있는가?

8. 시스템 환경변수 PATH에 현재 디렉토리를 의미하는 . 이 제거되었는가?

9. 파일/디렉토리 권한은 다음과 같이 설정되어 있는가?

파일/디렉토리	권한 (소유자)
사용자 홈디렉토리, 히스토리 파일, /boot 로그인시 환경설정 파일 등	700 (사용자)
cron.allow, cron.deny, at.allow, at.deny initd.d 디렉토리, rc.d 디렉토리	755 이하
/var/log 내 각종 로그파일 (wtmp, dmesg, xferlog, messages,lastlog 등) /etc/services, /etc/motd, /etc/syslog.conf	644 (Root)
/etc, /bin, /sbin,, /usr/bin, /usr/sbin. 등	741 (Root)
/tmp, /var/tmp	1777 (Root)

10. /etc/profile의 umask가 027로 설정되어 있는가?
〈참고〉

권한	umask	권한 통제
744	022	Group, Others 쓰기 권한
741	026	Group 쓰기 권한, Others 읽기/쓰기 권한
740	027	Group 쓰기 권한, Others 읽기/쓰기/실행 권한
700	077	Group, Others 읽기/쓰기/실행 권한

11. 일반 사용자가 로컬 시스템에서 리소스 사용을 제한하고 있는가?
(생성 가능한 최대 프로세스 개수, 최대 메모리 크기 등)

12. 네트워크 서비스의 경우 배너 설정을 하여 버전 정보를 숨기고 있는가?
/etc/default/telnetd, /etc/default/ftpd ➔ BANNER=" banner_information"

13. 보안에 관련된 적절한 커널 튜닝을 하였는가?

① Smurf 공격 대응
ndd -set /dev/ip ip_forward_directed_broadcasts 0

	② SYN Flooding 공격 대응 # ndd -set /dev/tcp tcp_conn_req_max_q0 512 ③ IP Forwarding 공격 대응 # ndd -set /dev/ip ip_forwarding 0 ④ Source Routing 공격 대응 # ndd -set /dev/ip ip_ip_forward_src_routed 0 14. /dev 에 디바이스 이외의 파일이 존재하는가? # find /dev -type f -exec ls -l {} ₩; 15. 일반 사용자가 스택 상에서 프로그램 실행 방지를 위한 설정이 존재하는가? /etc/system ➔ set noexec_user_stack=1, set noexec_user_stack_log=1 16. 일반 사용자가 주요 시스템 명령어(su, last, ifconfig, gcc 등)을 사용하지 못하도록 접근 권한을 설정하였는가?	
관리	**1. 적절한 패스워드 정책이 존재하는가?** ① 주요 패스워드 변경은 ○○일, 그 외는 ○○일마다 변경하는가? ② 최소 ○자 이상 길이로 영문자, 숫자, 특수문자를 혼용하여 사용하는가? ③ 안전한 패스워드를 사용하기 위해 패스워드 조합 툴을 실행하는가? ④ ○회 로그인 실패시 로그인 계정을 잠그도록 하는가? ⑤ 사용자의 패스워드를 저장시켜 놓지 않고 있는가? ⑥ 기본 계정이 기본 패스워드를 갖지 않도록 하는가? **2. BIOS와 부트 매니저(존재시)에 패스워드를 사용하고 있는가?** 3. 주요 파일들은 백업하고 복구하는 절차를 따르고 있는가? (일별, 주별, 월별) (예제) # ufsdump 0uf /dev/rmt/0 /home # ufsrestore xvf /dev/rmt/0 /home 4. 비정상적인 로그인 접속을 로깅하고 있는가? (예제) /etc/default/login ➔ RETRIES=5 5. 주기적으로 로그를 분석하고 있는가? 6. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	1. UNIX 관련 공식 패치 및 보안 홈페이지 [Sun Solaris] ftp://sunsolve1.sun.com/pub/patches/ http://sunsolve.sun.com/show.do?target=patchpage [HP-UX] http://www4.itrc.hp.com/service/patch/mainPage.do [IRIX] http://www.sgi.com/support/security/ http://www.sgi.com/support/security/advisories.html [BSD/OS] http://www.bsdi.com/services/support/patches/ http://www.bsdi.com/services/support/ [FreeBSD] ftp://ftp.freebsd.org/pub/FreeBSD/releases/ http://www.freebsd.org/security/	

	[NetBSD] http://www.netbsd.org/support/security/ [OpenBSD] ftp://ftp.openbsd.org/pub/OpenBSD/patches/ http://openbsd.org/errata.html 2. CERT.org UNIX 체크리스트 http://www.cert.org/tech_tips/usc20_full.html 3. Useful Tools : http://sectools.org/ [Portsentry] http://sourceforge.net/projects/sentrytools/ [tcpdump] http://www.tcpdump.org/ [tcp wrapper] ftp://ftp.porcupine.org/pub/security/ [Tripwire] http://www.tripwire.com/ [lsof] http://freshmeat.net/projects/lsof/ [openssh] http://www.openssh.com/ [nessus] http://www.nessus.org/ [nmap] http://insecure.org/ [iptables] http://security.maruhn.com/ [SAINT] http://www.saintcorporation.com [SARA] http://www-arc.com/sara/ [john the ripper] http://www.openwall.com/john/ [Ethreal] http://www.ethereal.com/ [antisniff] http://www.securitysoftwaretech.com/antisniff/ [snort] http://www.snort.org/	

▌리눅스(Linux) 보안 체크리스트(배포판에 종속되지 않는 일반적인 리눅스 환경)

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 리눅스 배포판의 커널 패치를 적용하였는가?** **2. 사용하고 있는 공개 소프트웨어는 최신 버전으로 유지하고 있는가?** **3. SUID, SEUID가 설정된 파일 중에서 특히 버퍼 오버 플로우 등 공개된 취약점을 내포하고 있는 파일들은 최신 패치를 적용하였는가?** 〈참고 : Overflow 취약성이 많이 공개된 서비스들〉 RPC, SNMP, NFS, X Window, BIND, OpenSSH, OpenSSL 의 낮은 버전	
주요 Tool	**1. TCP Wrapper를 사용하여 접속제한을 하고 있는가?** ① /etc/hosts.deny 파일 내용을 "ALL:ALL"로 구성하여 불필요한 호스트로부터의 서비스 접근통제를 하고 있는가? ② /etc/hosts.allow 파일에서 인가된 관리자에게만 권한이 허용되어 있는가? ③ 각 설정 파일은 일반 사용자가 읽을 수 없도록 600 권한을 주었는가?	

```
service telnet
{
        flags         = REUSE NAMEINARGS
        protocol      = tcp
        socket_type = stream
        wait          = no
        user          = telnetd
        server        = /usr/sbin/tcpd
        server_args = /usr/sbin/in.telnetd
}
```

2. Iptables와 같은 방화벽(방화벽을 따로 사용하지 않을 경우)에서 Inbound Traffic에 대한 접근통제(INPUT, OUTPUT, FORWARD)를 하고 있는가?
3. **Tripwire 등 무결성 검사 소프트웨어를 정기적으로 수행하여 시스템상 변경 여부를 정기적으로 확인하고 있는가?**
4. John the Ripper 등의 도구를 이용하여 패스워드 점검을 정기적으로 수행하는가? (암호가 없는 계정, 추측 가능한 암호 사용 등)
5. Nessus, nmap 등의 공개 스캐닝 도구를 이용하여 로컬시스템의 취약점과 불필요한 포트에 대한 점검을 정기적으로 수행하는가?
6. **평문으로 전송하는 Telnet, ftp 대신 OpenSSH, OpenVPN과 같은 공개툴을 이용하여 암호화된 통신을 하고 있는가?**
7. **Cron, At 등 정기적으로 수행할 수 있는 도구을 이용하여 주요 보안 리포트를 정기적으로 관리자에게 리포팅하는가?**
8. PORTSENTRY와 같은 공개 침입탐지 및 방어 툴을 사용하고 있는가?
9. chkrookit 등과 같은 백도어 설치 탐지 툴을 이용하여 주기적으로 시스템 내 백도어 존재 유무를 점검하고 있는가?
10. **PAM, ulimit 등을 활용하여 일반 사용자에게 리소스 제한을 하고 있는가?**
    ① 사용 가능한 메모리를 제한하고 있는가?
    ② 생성할 수 있는 프로세스를 제한하고 있는가?
    ③ 로그인 동시접속을 제한하고 있는가?
    ④ Core 파일을 생성하지 않고 있는가?
    /etc/pam.d/login ➔ session required /lib/security/pam_limits.so
    /etc/security/limits.conf ➔ core, rss, nproc, maxlogins 설정

불필요 요소 제거

1. **/etc/rc.d/init.d 내 불필요한 서비스가 중지되었는가?**
   (예제) # chkconfig –list | grep 3:on
   # ls -l /etc/rc.d/rc3.d/S*

   〈참고 – 꼭 필요한지 확인해야 할 서비스〉
   apmd, xntpd, portmap, sound, netfs, rstatd, rusersd, rwhod, rwalld, named, bootparamd, squid, yppasswdd, ypservd, dhcpd, atd, pcmcia, snmpd, ,routed, lpd, mars-new, nfs, amd, gated, sendmail, httpd, ypbind, xfs, innd, linuxconf

2. **불필요한 계정은 삭제되었는가?**
3. /etc/hosts 파일에 불필요한 시스템이 포함되어 있지는 않은가?
4. **보안상 취약한 suid, sgid가 제거되었는가?**

find / -type f ₩(-perm -04000 -o -perm -02000 ₩) -exec ls -lg {} ₩;
(예제) # chmod u-s /usr/bin/chage

5. 소유자가 없거나 그룹 아이디가 없는 파일이 존재하지 않는가?
find / -type f -nouser -o -nogroup -print

6. 누구나 변경할 수 있는 민감한 파일(World-Writable)은 존재하지 않는가?
find / -type f -perm -2 -print

7. NFS를 사용하여 불필요하거나 민감한 디렉토리가 마운트되지 않았는가?
showmount -e

8. Cron 데몬에 불필요하게 자원을 낭비하는 사용자/프로세스는 제거되었는가?

9. 불필요한 포트가 오픈되어 리스닝하고 있는가? # netstat -a

안전한 설정

1. /etc/passwd 파일은 적절히 구성되었는가?

① 사용자 패스워드는 암호화되어 /etc/shadow에 존재하는가?
② UID 또는 GID가 0인(루트 권한) 사용자가 존재하는가?
③ 추측하기 쉬운 패스워드를 사용하는 사용자가 존재하는가?
④ 벤더 기본 계정(daemon, bin, adm, lp, uucp 등)에 shell이 부여되어 있는가?
⑤ 패스워드 에이징(Aging,일정기간 이상이면 변경 또는 잠금) 정책이 있는가?
- /etc/login.defs
➔ PASS_MIN_DAYS, PASS_MAX_DAYS, PASS_MIN_LEN, PASS_WARN_AGE

〈참고〉
/etc/shadow 파일 필드 내용
[(1)아이디 : (2)암호화된 패스워드 (3)최근 패스워드 변경일 : (4)패스워드를 변경해야 하는 최소일수 : (5)변경한 패스워드를 사용할 수 있는 최대일수 : (6)패스워드를 변경하도록 강제하는 경고일수 : (7)패스워드가 만기된 후 실제 사용중지까지 일수 : (8)사용중지날짜]

2. 원격 접속시 루트로 로그인할 수 없도록 통제되어 있는가?

① /etc/securetty : console
② 파일 권한은 600으로 설정하였는가?

3. /etc/xinetd.conf 은 적절히 구성되었는가?

① 파일 권한은 600으로 설정하였는가?
② r 시리즈 명령어 (rlogin, rsh, rexec)는 사용하지 않고 있는가?
③ /etc/xinetd.d 내 보안에 취약한 데몬은 제거되었는가?

4. 파일/디렉토리 권한은 다음과 같이 설정되어 있고 정기적으로 점검하는가?

파일/디렉토리	권한 (소유자)
사용자 홈디렉토리, 히스토리 파일 로그인시 환경설정 파일 등	700 (사용자)
Cron 데몬의 cron.allow, cron.deny, at.allow, at.deny Initd.d 디렉토리, Rc.d 디렉토리	755 이하
/var/log 내 각종 로그파일 (wtmp, dmesg, xferlog, messages,lastlog 등) /etc/services, /etc/aliases, /etc/motd, /var/log/wtmp, /var/run/utmp, /etc/syslog.conf, /etc/fstab, /etc/passwd, /etc/group	644 (Root)
/etc, /bin, /sbin,, /usr/bin, /usr/sbin. 등	741 (Root)
/tmp, /var/tmp	1777 (Root)

5. /etc/profile의 umask가 027로 설정되어 있는가?
〈참고〉

권한	umask	권한 통제
744	022	Group, Others 쓰기 권한
741	026	Group 쓰기 권한, Others 읽기/쓰기 권한
740	027	Group 쓰기 권한, Others 읽기/쓰기/실행 권한
700	077	Group, Others 읽기/쓰기/실행 권한

6. /etc/hosts.equiv, $HOME/.rhosts 파일이 존재한다면, 적절히 구성되었는가?
① "+","+ +" 설정(임의의 사용자과 권한 획득가능 상태)이 금지되었는가?
② 사용하지 않는다면, /dev/null로 링크되어 있는가?
(예제) # ln -s /dev/null /etc/hosts.equiv
ln -s /dev/null /.rhosts
③ 일반 사용자들이 자신의 홈디렉토리에서 생성할 수 없도록 통제하는가?

7. 서버 접근시(telnet, ssh, ftp 등) IP별 접근 제한을 설정하였는가?

8. 비로그인 데몬은 root가 아닌 nobody 권한으로 동작하고 있는가?

9. 시스템 환경변수 PATH에 현재 디렉토리를 의미하는 . 이 제거되었는가?
 # echo $PATH

10. 일정시간이 지난 후 자동 로그아웃하는 session timeout이 설정되었는가?
(예제) /etc/default/login ➔ TIMEOUT=300

11. 일반 사용자가 로컬 시스템에서 리소스 사용을 제한하고 있는가?
(생성 가능한 최대 프로세스 개수, 최대 메모리 크기 등)

12. 네트워크 서비스의 경우 배너 설정을 하여 버전 정보를 숨기고 있는가?

13. 보안에 관련된 적절한 커널 튜닝을 하였는가?
① Smurf 공격 대응
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
② SYN Flooding 공격 대응
sysctl -w net.ipv4.tcp_max_syn_backlog=1280 (백로그 큐 증가)
sysctl -w net.ipv4.tcp_syncookies=1 (공격시 로깅 메시지 출력)
③ ICMP Redirect 비허용 (임의의 라우팅 테이블 변경 방지)
sysctl -w net.ipv4.conf.eth0.accept_redirects=0
sysctl -w net.ipv4.conf.lo.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
sysctl -w net.ipv4.conf.all.accept_redirects=0
④ Source Route 패킷 비허용
sysctl -w net.ipv4.conf.eth0.accept_source_route=0
sysctl -w net.ipv4.conf.lo.accept_source_route=0
sysctl -w net.ipv4.conf.default.accept_source_route=0
sysctl -w net.ipv4.conf.all.accept_source_route=0
⑤ Proxy ARP 미설정
sysctl -w net.ipv4.conf.eth0.proxy_arp=0
sysctl -w net.ipv4.conf.lo.proxy_arp=0
sysctl -w net.ipv4.conf.default.proxy_arp=0
sysctl -w net.ipv4.conf.all.proxy_arp=0

	14. /dev 에 디바이스 이외의 파일이 존재하는가? (예제) # find /dev -type f -exec ls -l {} ₩; 15. 일반 사용자가 스택 상에서 프로그램 실행 방지를 위한 설정이 존재하는가? (예제) /etc/system ➔ set noexec_user_stack=1 16. 일반 사용자는 제한적인 쉘을 사용하고 있는가? **17. 일반 사용자가 주요 시스템 명령어(su, last, ifconfig, gcc 등)을 사용하지 못하도록 접근 권한을 설정하였는가?**	
관리	**1. 적절한 패스워드 정책이 존재하는가?** ① 주요 패스워드 변경은 OO일, 그 외는 OO일마다 변경하는가? ② 최소 O자 이상 길이로 영문자, 숫자, 특수문자를 혼용하여 사용하는가? ③ 안전한 패스워드를 사용하기 위해 패스워드 조합 툴을 실행하는가? ④ O회 로그인 실패시 로그인 계정을 잠그도록 하는가? ⑤ 사용자의 패스워드를 저장시켜 놓지 않고 있는가? ⑥ 기본 계정이 기본 패스워드를 갖지 않도록 하는가? **2. BIOS와 부트 매니저(존재시)에 패스워드를 사용하고 있는가?** **3. SUDO를 사용하여 루트 권한을 제한하고 있는가?** **4. Root만이 Cron에 접근하도록 설정되었는가?** **5. 로컬/원격 시스템 접근시 적절한 배너가 설정되었는가?** /etc/motd, /etc/issue, /etc/issue.net 4. 주요 파일들은 백업하고 복구하는 절차를 따르고 있는가? (일별, 주별, 월별) 5. 비정상적인 로그인 접속을 로깅하고 있는가? (예제) /etc/default/login ➔ RETRIES=5 5. 주기적으로 로그(messages, secure, maillog 등)를 분석하고 있는가? 6. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	1. 리눅스 배포판 공식 보안 홈페이지 Calera http://www.calderasystems.com/support/security/ Debian http://www.debian.org/security/ Mandrake http://www.linux-mandrake.com/en/security/ Redhat http://www.redhat.com/security/ Slackware http://www.sastk.org/ SuSe http://www.suse.com/us/support/security/index.html Turbo http://www.turbolinux.com/cgi-bin/security/index.cgi?mode=all Gentoo http://www.gentoo.org/security/en/index.xml Selinux http://www.nsa.gov/selinuX/ 2. 국내 리눅스 포털 http://www.superuser.co.kr 3. Useful Tools : http://sectools.org/ [Portsentry] http://sourceforge.net/projects/sentrytools/ [tcpdump] http://www.tcpdump.org/ [tcp wrapper] ftp://ftp.porcupine.org/pub/security/ [Tripwire] http://www.tripwire.com/ [lsof] http://freshmeat.net/projects/lsof/ [openssh] http://www.openssh.com/	

	[nessus] http://www.nessus.org/ [nmap] http://insecure.org/ [iptables] http://security.maruhn.com/ [SAINT] http://www.saintcorporation.com [SARA] http://www-arc.com/sara/ [john the ripper] http://www.openwall.com/john/ [Ethreal] http://www.ethereal.com/ [antisniff] http://www.securitysoftwaretech.com/antisniff/ [snort] http://www.snort.org/ [lids] http://www.lids.org/ 4. X window 보안 http://www.stanford.edu/services/securecomputing/x-window/	

Windows 2000 Server 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 주기적으로 업데이트하고 있는가?** Internet Explorer → 도구 → Windows Update 사이트 **2. 서비스팩이 설치되어 있는가?** **3. 자동 업데이트를 사용하고 있는가?**	
주요 Tool	1. 바이러스 백신을 설치하였는가? 2. 윈도우에서 기본적으로 제공하고 있는 개인 방화벽을 사용하고 있는가? 시작 → 설정 → 제어판 → 네트워크 연결 → 로컬영역 연결 속성 → 고급 탭 → 윈도우 방화벽 사용 → 예외 탭에서 예외 프로그램 / 포트 추가 3. 스파이웨어 제거 프로그램을 주기적으로 실행하는가? 4. 기타 무상/상용 침입차단시스템 또는 개인 방화벽이 있는가?	
불필요 요소 제거	**1. 불필요한 [숨김] 공유를 중지하였는가?** ① 시작 → 설정 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 공유폴더 → 공유 → 불필요한 공유 폴더 중지 ② 시작 → 실행 → cmd.exe C:₩ net share [공유폴더명] /delete ③ 시작 → 실행 → regedit.exe (레지스트리 편집) HKLM₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver₩ Value Name : AutoShareWks Type : REG_DWORD Value : 0 **2. 널세션을 제거하였는가? (IPC$, 레지스트리 편집)** HKLM₩SYSTEM₩CurrentControlSet₩Control₩LSA Value Name: RestrictAnonymous	

	Data Type: REG_DWORD Value: 1 3. 익명(Anonymous)의 네트워크 공유는 제한되었는가? 3. 불필요한 자동 시작 서비스는 제거되었는가? 시작 → 실행 → services.msc 4. 프린터 공유 권한이 있다면, 일반 사용자에게 불필요한 권한이 제거되었는가? 5. 넷미팅을 통한 원격 데스크탑 공유가 해제되었는가? 6. 불필요한 컴포넌트가 설치되어 있지 않은가?	
안전한 설정	**1. 관리자로 자동 로그인되는 기능을 해제하였는가?** HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: AutoAdminLogon Data Type: REG_SZ Value Data: 0 2. 로그온 캐시 사용을 해제하였는가? HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: CachedLogonsCount Data Type: REG_SZ Value Data: 2 이하 3. 레지스트리에 익명 접근을 통제하고 있는가? HKLM₩System₩CurrentControlSet₩Control₩SecurePipeServers₩Winreg Administrators : all 4. 로컬로 로그온시 경고 메시지가 출력되는가? 5. 스크린 세이버가 패스워드로 보호되어 있는가? 6. CMOS 패스워드는 설정되어 있는가? **7. 공유 폴더 설정시 특정 사용자에게 읽기/쓰기 권한을 명확히 주고 있는가?**	
관리	**1. 시스템 접근시 경고문을 사용하고 있는가?** HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: LegalNoticeCaption Data Type: REG_SZ Value Data: "경고문" **2. 불필요한 사용자 계정을 삭제했는가?** 시작 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 로컬 사용자 및 그룹 → 사용자 → Guest 등 불필요한 계정 사용 안 함 **3. 패스워드 정책설정이 적절하게 구성되었는가?** ① 사용자 패스워드는 최소 0 이상을 강제하는가? ② 패스워드는 0일 이후 만기되고 있는가? ③ 0회 잘못된 시도에 로그아웃되고 ○분 후 초기화되는가? ④ 복잡도를 만족하는 패스워드를 사용하도록 강제하는가? 4. NTFS 파일 시스템을 사용하고 있는가?	

5. 사용자 권한이 적절히 할당되어 있는가?

사용자 권한	도메인 컨트롤러	멤버 서버
네트워크에서 액세스 가능	Administrators Authenticated Users Enterprise Domain Controllers	Administrators Users
백업파일과 디렉토리	Administrators Backup Operators	Administrators Backup Operators
바이패스 순환 체킹	Authenticated Users	Users
시스템 시간 변경	Administrators	Administrators
페이지 파일 생성	Administrators	Administrators
토큰 객체 생성	(None)	(None)
글로벌 객체 생성	SERVICE, Administrators	SERVICE, Administrators
공유 객체 생성	(None)	(None)
프로그램 디버깅	Administrators	Administrators
네트워크에서 액세스 제한	Guests	Guests
로컬에서 로그온 제한	Guests	Guests
컴퓨터와 사용자 계정에 트러스트 위임 가능	Administrators	(None)
원격 시스템에서 강제종료	Administrators	Administrators
쿼터 증가	Administrators	Administrators
스케줄링 우선순위 변경	Administrators	Administrators
장치 드라이버 로딩	Administrators	Administrators
로컬에서 로그온 가능	Administrators Backup Operators	Administrators Backup Operators
감사 및 보안 로그 관리	Auditor's Group (Exchange Enterprise Servers Group)	Auditor's Group (Exchange Enterprise Servers Group on Exchange server)
펌웨어 환경변수 수정	Administrators	Administrators
파일 및 디렉토리 복구	Administrators Backup Operators	Administrators Backup Operators
시스템 종료	Administrators	Administrators
디렉토리 서비스 데이터 동기화	Not checked (Checked in AD STIG Checklist)	N/A

6. 도메인 컨트롤러 사용시 적절한 커버러스 정책이 반영되었는가?
   ① 사용자 로그온 제한이 설정되어 있는가?
   ② 서비스 티켓 최대 시간(Service Ticket Lifetime)이 설정되어 있는가?
   ③ 사용자 티켓 최대 시간(User Ticket Lifetime)이 설정되어 있는가?
   ④ 사용자 티켓 갱신시간 (User Ticket Renewal Lifetime)이 설정되어 있는가?
   ⑤ 시간 동기화 (Clock Synchronization)이 설정되어 있는가?

7. 이벤트 로깅을 적절히 설정하고 주기적으로 분석하고 있는가?

%SystemRoot%₩System32₩CONFIG₩AppEvent.evt

%SystemRoot%₩System32₩CONFIG₩SecEvent.evt

	%SystemRoot%₩System32₩CONFIG₩SysEvent.evt ① 시스템/보안/응용프로그램의 최대 로그사이즈가 설정되었는가? ② 네트워크를 통한 이벤트 로그 접근이 제한되었는가? ③ 보안 이벤트를 ○개월 이상 보존하고 있는가? **8. 이벤트 감사권한를 적절히 설정하고 주기적으로 검사하고 있는가?** 9. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	[Security Templates] http://support.microsoft.com/kb/321679 [Win2K Server] www.microsoft.com/technet/archive/security/chklist/w2ksvrcl.mspx	

DB 보안 체크리스트

<table>
<tr><th>항목</th><th>상세설명</th><th>체크</th></tr>
<tr><td>보안 패치</td><td>1. 사용하고 있는 DB는 최신 버전의 보안 업데이트를 적용하였는가?
2. 보안 업데이트 주기를 설정하고, 정기적으로 수행하고 있는가?</td><td></td></tr>
<tr><td>불필요 요소 제거</td><td>1. 데이터베이스 디폴트 계정(아이디, 패스워드)을 변경 또는 제거하였는가?
〈참고〉
<table>
<tr><th>오라클 기본 계정</th><th>MS SQL 기본 계정</th></tr>
<tr><td>scott/tiger
system/manager
dbsnmp/dbsnmp
tracesvr/trace
sys/change_on_install
sapr3/sap
demo/demo
outln/outln
mtssys/mtssys
ordsys/ordsys
ordplugins/ordplugins
mdsys/ddsys
ctxsys/ctxsys
adams/wood
blake/paper
jones/steel
clark/cloth
auroraorbunauthenticated/invalid
wksys/wksys
olapsys/manager
olapdba/olapdx
LBACSYS/LBACSYS
olapsvr/instance</td><td>sa / null
probe / null
MySQL 기본 계정
root / null
null / null
mysql / null
Sybase 기본계정
sa / sa</td></tr>
</table>
2. 데이터베이스 초기 설치시 꼭 필요한 Product만 설치하였는가?
3. 시스템 권한 및 오브젝트 권한은 Public으로부터 제거되었는가?</td><td></td></tr>
</table>

4. 시스템 임의의 디렉토리나 파일에 대한 읽기/쓰기 권한이 제한되어 있는가?
5. **OS에서 불필요한 서비스는 모두 제거되었는가? (telnet, ftp, tftp 등)**

안전한 설정

1. **기밀성이 요구되는 주요정보를 저장하는 필드는 암호화되어 만약의 유출에 대비하고 있는가?**
2. **IP별로 DB에 접근을 통제하고 있는가?**

```
(예제)
protocol.ora (oracle net configuration)
   tcp.validnode_checking = YES
   tcp.excluded_nodes = {list of IP addresses}
   tcp.invited_nodes = {list of IP addresses}
```

3. **DB에 접근할 수 있는 클라이언트는 특정 장비로만 통제하고 있는가?**

```
(예제)
$ORACLE_HOME/network/admin/protocol.ora
tcp.validnode_checking = yes
tcp.invited_nodes=( xxx.xxx.xxx.xxx )
```

4. **데이터 사전 권한은 보호되어 있는가?**
   init〈sid〉.ora ➔ DICTIONARY_ACCESSIBILITY = FALSE
5. 원격접근시 클라이언트에 대한 표준 인증 절차를 하고 있는가?
   REMOTE_OS_AUTHENT = FALSE
6. (오라클 사용시) 리스너를 적절하게 보호하고 있는가?
   LISTENER.ORA ➔ ADMIN_RESTRICTIONS_LISTENER=ON

```
(예제 - SSL 사용)
LISTENER=
   (DESCRIPTION=
      (ADDRESS_LIST=
         (ADDRESS=
            (PROTOCOL=tcps)
            (HOST = xxx.com)
            (PORT = 8281)))
(예제 - 원격에서 관리자 접근시)
User_admin =
   (DESCRIPTION =
      (ADDRESS =
         (PROTOCOL = tcps)
         (HOST = xxx.com)
         (PORT = 8281)))
```

7. 오라클 10g R10이전의 버전인 경우 TNS 리스너 패스워드를 설정하였는가?

```
LSNRCTL〉 CHANGE_PASSWORD
Old password: *************
New password: *************
Reenter new password: *************
LSNRCTL〉 SET PASSWORD
Password:
LSNRCTL〉 SAVE_CONFIG
```

	4. 저장 프로시져 및 툴을 사용하여 설정된 접근권한을 체크하고 수정하는가? 5. 테이블에 Seclect, Insert, Update, Delete 등 행위별 권한과 각 필드 접근 권한 등의 객체 권한을 통제하고 있는가?	
관리	**1. DB를 보호하기 위한 방화벽이 있는가?** **2. 파견자, 휴직자, 이직 및 퇴직자의 DB 접근 권한이 제거되었는가?** (예제) sqlplus〉 connect mydba sqlplus〉 alter user acme account lock; sqlplus〉 alter user acme identified by p83d7d3f; sqlplus〉 alter user acme account unlock; **3. 파견자, 휴직자, 이직 및 퇴직자 발생시 기존 패스워드 변경을 하고 있는가?** **4. DB 사용자 계정을 발급하고 폐기하는 일련의 프로세스가 존재하는가?** **5. 적절한 패스워드 정책이 존재하는가?** ① DB 사용자의 패스워드 변경은 ○일마다 변경하는가? ② 최소 ○자 이상 길이로 영문자, 숫자, 특수문자를 혼용하여 사용하는가? ③ 사용자의 패스워드를 평문으로 저장시켜 놓지 않고 있는가? ④ 아이디와 패스워드가 같거나 추측하기 쉬운 패스워드를 사용하는 계정을 사용하고 있지 않은가? **6. 제한된 수의 로그인 실패시 로그인 계정을 잠그도록 하는가?** **7. 일정한 시간이 지나면 자동으로 로그아웃되고 있는가?** **8. 누가 로그인 중인지 모니터링하고 있는가?** **9. DB 백업과 복구하는 절차를 가지고 있는가? (일별, 주별, 월별)** **10. 적절한 로깅과 감사를 하고 있는가?** ① 비정상적인 로그인 접속과 접속에 실패한 접근시도를 로깅하고 있는가? ② 사용자의 로그인, 로그아웃 시간을 로깅하고 있는가? ③ DB 내의 데드락(deadlock)을 로깅하고 있는가? ④ 시스템 테이블로의 접근을 로깅하고 있는가? ⑤ 새로운 객체 생성을 로깅하고 있는가? ⑥ 일반 사용자의 데이터 조작을 로깅하고 있는가? ⑦ 로깅 파일은 보안 관리자에게 읽기 권한만을 부여하고 있는가? ⑧ 일정기간 동안 로깅 파일을 보관하고 있는가? ⑨ 주기적으로 로그를 분석하고 있는가? 11. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	1. Oracle 보안 패치 공식 홈페이지 www.oracle.com/technology/deploy/security/alerts.htm 2. DB 보안 관련 페이지 [MS-SQL] www.sqlsecurity.com [MySQL] http://dev.mysql.com/doc/refman/5.1/en/security-guidelines.html	

1.3. 보안관제

매년 증가하고 있는 인터넷 침해사고, 해킹 등으로 기업은 정보보호에 대한 관심이 고조되어가고 있지만, Firewall, IDS, IPS, 네트워크 장비 등의 개별 단위장비로는 더욱 복잡해진 네트워크 및 시스템을 안전하게 관리하고 침해유형에 맞게 적절히 통제하는데는 한계를 보이고 있다.

보안장비 도입 초기에는 단일 보안장비들 자체가 모든 보안 침해사고에 대한 해결책이 되지 못했다. 예를 들면 방화벽의 도입만으로 모든 보안은 해결될 것으로 생각하여 제품을 구매하고 운영에 필요한 보안 전담인력을 만들고 인터넷과 연결된 내부 또는 외부망에 적용을 하였으나, 정상 서비스를 이용한 해킹사례가 속출하는 문제를 비롯해 관리자의 정책설정의 오류, 우회공격 등 많은 문제점들이 나타나고 있다. IDS 또한 자체장비에서의 미탐지/오탐지의 증가로 기업 내 보안관리자의 혼동을 야기했다. 이와함께 단위 보안장비들의 많은 로그들(이벤트로그, 시스템로그, 침입로그 등)을 어떻게 처리할 것인지에 대한 고민도 더불어 증가했다.

이러한 보안 시스템간 의 비효율적인 부분을 해결하기 위한 방안으로 보안관제 기술이 도입되었다. 보안관제 서비스는 서버와 네트워크 장비, 보안 시스템 등을 원격지에서 안전하게 관리하며 인가받지 않은 외부 침입자를 실시간으로 탐지하여 원격 관제실에 경보를 보냄으로써 외부 침입에 즉각적인 대응 및 역추적을 할 수 있을 뿐만 아니라, 이기종간에 보안 관리까지 할 수 있는 통합보안 개념으로 발전해 나가고 있다.

▮ 정의 및 역할

보안관제의 효과적인 업무처리를 수행하기 위해서는 기술적·관리적인 측면을 고려하여 신속한 예방 및 대응조치에 필요한 최적의 환경을 구축하여야 한다. 보안관제의 정의에 근거해 관제의 주요 역할을 살펴보면 다음과 같다.

〈표 4-1-3-1〉 보안관제의 주요 역할

항 목	역 할
보안시스템 통합관리	• 이기종에 대한 Agent를 통한 모니터링 및 관리 ex) 침입탐지시스템, 침입차단시스템, 네트워크, 자원관리 등
일관성있는 정책구현	• 중앙에서 일관된 정책적용을 통합관리로 보안장비에 대한 위험요소를 최소화
신속한 대응처리	• 침해사고에 대한 사전 예방활동강화 (모니터링, 사전대응, 효과적인 정책 적용 등) • 24X365일 실시간 감시, 장애처리, 업무중단에 대한 위협요소 감소
최적의 보안체계 운영	• 정보자산에 대한 효과적인 방안을 마련할 수 있는 환경 구성

다음으로 보안관제에 대한 세부적인 역할을 알아보면 다음과 같다

〈표 4-1-3-2〉 보안관제 세부 업무

역 할	주요 내용
통합관리 및 모니터링	• 각종 로그 통합관리 • 24시간 관제 모니터링 • 침해사고에 대한 사전 감시활동 • 침해사고 대응 및 조치
각종 보고서 종합	• 주기적인 보안권고 • 보안패치 관리 • 다양한 레포팅
관리적 보안	• 다양한 환경의 정책관리 • 업무처리에 대한 관리 • 관제운영에 대한 관리 • 기타 관리적인 사항
기술적 보안	• 네트워크 보안 • 시스템 보안 • 에플리케이션 보안 • 켄텐츠 보안 • 서비스 보안
시스템 운영 및 관리	• 시스템 용량 관리, 성능관리 • 구성관리, 환경설정 관리 • 변경관리, H/W장애 관리

▮ 보안관제 구성 및 운영

보안관제의 구성요소를 살펴보면 크게 3가지로 구분할 수 있다. 첫째로 네트워크나 시스템에 설치된 에이전트를 꼽을 수 있다. 이것은 각종 보안장비 및 서버, 네트워크에 설치하여 해당 시스템에 맞게 설정된 로그정보를 실시간 전송하여 중앙관제센터에서 각종 로그를 싶게 모니터링하고 분석할 수 있도록 정보를 제공해 주는 것이다.

둘째로는 정보수집 서버가 있다. 정보수집 서버는 각 에이전트에서 보내진 각종 정보를 주집하고 분석하여 처리하여 DB에 저장하는 역할을 한다. 여기서 에이전트에 대한 Health Check를 통한 모니터링과 분석에 가능한 리포팅 소스를 제공한다.

마지막으로 통합관제용 시스템이다. 여기서 주 역할은 각종 이벤트 로그에 대한 분석을 주로 수행한다. 다양하게 수집되고 분석된 정보를 종합하고 상황을 분석하여 관제요원들이 신속하게 정보를 파악할 수 있도록 최적의 정보를 제공·반영하며, 로그분석에 대한 결과를 주기적으로 저장한다.

보안관제 처리 절차는 크게 예방, 탐지, 대응 부문으로 구분되며, 각각 상세의 활동은 다음과 같다.

〈표 4-2-3-3〉 보안관제 상세활동

업무구분	활 동	내 용
예방부문	보안패치	서버, 네트워크, 응용프로그램 등에 발생된 보안취약점에 패치를 통해 제거하는 활동
	취약점 점검	시스템 및 네트워크에 주기적인 취약점 점검 및 조치활동
	정책관리	IDS, IPS, F/W, N/W 장비 등 보안정책 적용 활동
	모니터링	침입로그, 시스템 로그 등 각종 이벤트에 대한 확인하는 활동
탐지부문	NMS, Alert	네트워크 및 시스템에서 제공하는 예·경보 탐지활동
	시스템 장애 이벤트	각종 시스템 장애에서 발생되는 경보에 대한 탐지 활동
	관리적 이벤트	기타 관리에 필요한 각종 이벤트에 대한 탐지 활동
대응부문	웜·바이러스	웜, 바이러스, 백도어, 악성 봇 등 악의적인 프로그램 감염에 대한 대응
	스캐닝	악의적인 의도로 시설에 관련된 정보 수집하는 활동
	침해사고	주요 시스템에 불법적인 접근을 시도 권한을 획득하는 활동
	기타 사고대응	정상적인 활동에 대한 대응활동(사이버 시위 등)

수많은 이 기종 보안 솔루션을 통합하고 관리했다는 점에서 보안관제는 효과가 있을 수 있지만 실질적 침해사고가 발생하면 신속한 조치 및 기업 보안정책을 수립하는 데에 대한 경험 미숙 등으로 적절한 대처가 이뤄지지 않을 수도 있다. 때문에 수많은 장비를 한곳에서 모니터링한다는 것은 분명 장점이지만, 보안 담당자의 적극적인 대처 능력이나 정책수립, 그리고 수많은 보안장비에 대한 장비 간 분석능력이 수반되어야 한다.

또한 자동적이고 지능적인 자동명령 실행 등을 통해 신속한 대처능력과 문제점을 정책수립에 설정시킬 수 있어야 보안관제 능력을 향상시킬 수 있다.

2 보안교육 방법론

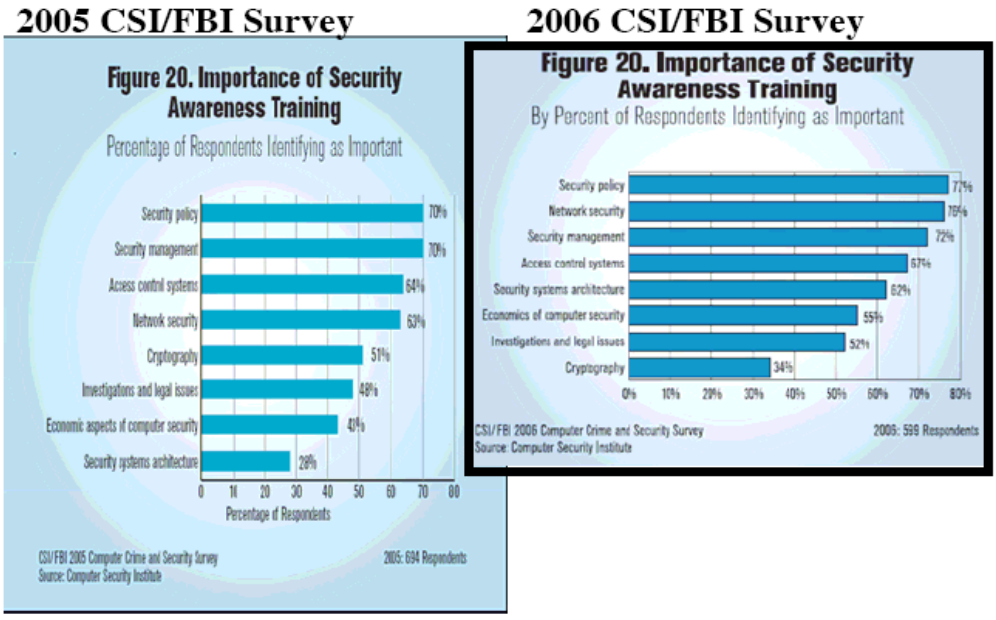
2.1. 정보보호 인식제고 개요

정보보호 인식제고는 기업 정보보호의 가장 중요한 요소의 하나로 특성상 단시간에 보안사고 예방효과에 대한 분석이 이루어지기 힘들어 많은 기업들이 정보보호 인식제고에 투자하지 않고 있다. 특히 정보보호 인식제고의 가장 중요한 요소인 정보보호 교육은 많은 기업들이 도입을 하거나 시행을 하고 있지만 실질적인 효과를 거두지 못하고 있다.

아래 그림에서 볼 수 있듯 2005년, 2006년 CSI/FBI가 내놓은 Computer Security Survey에 따르면, 기업의 보안책임자/CIO 등이 가장 아쉽고 시급히 여기는 과제 중의 하나로 보안교육(Security Awareness)을 언급하고 있다.

일반적으로 기업의 정보보호 교육체계는 크게 다음과 같이 2가지로 구분해 볼 있다.

① 임직원에게 보안정책을 인식시키고 보안규정들을 지키고 실천하도록 하는 교육
② 보안담당자의 업무능력을 향상시켜 보안업무에 있어서 최대한의 효과를 거둘 수 있도록 보안 전문가를 양성하는 교육



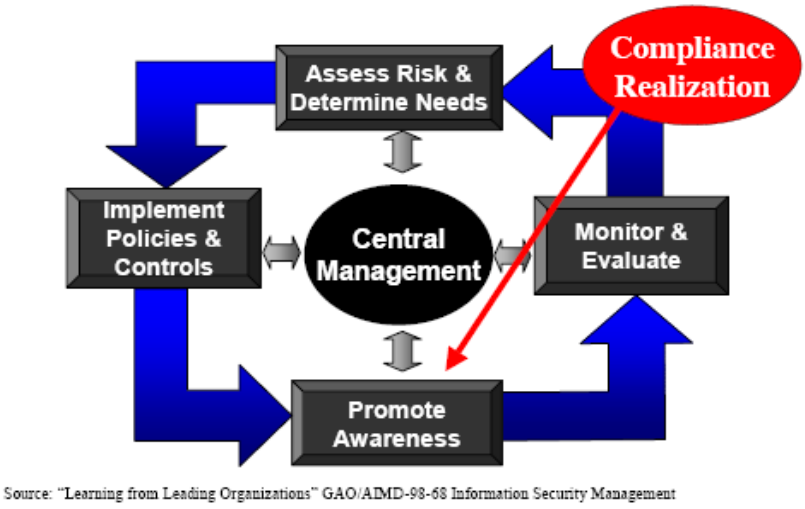
〈그림 4-2-1-1〉 2005, 2006 CSI/FBI Computer Crime And Security Survey

2.2. 보안교육정책 제도

▌보안교육정책 제도화

기업은 우선적으로 기업 내에 규정되어 있는 정보보호 규정을 통해 보안교육과 관련된 정책을 명문화하고, 전 임직원이 공통적으로 다음과 같은 사항을 준수하도록 하여야 한다.

① 모든 임직원은 입사 시 입문교육 보안과정을 이수해야 한다.
② 승격자는 승격교육에 포함된 보안교육과정을 이수해야 한다.
③ 모든 임직원은 연간 1회 보안교육과정을 이수해야 한다.
④ 보안전담조직 및 유관조직의 담당자는 정기적으로 보안관련 과정을 이수하도록 해야 한다.



〈그림 4-2-2-2〉 정보보안 교육의 표준 모델

▌보안교육 실시 및 홍보활동

정보보호 부서에서는 보안교육 및 홍보활동을 통해 사내보안 준수사항에 대한 내용을 임직원에게 전달하고 교육하여야 한다.

① 정보보안 규정을 통해 정보보호교육의 기준을 제시
② 대상자별, 계층별로 차별화된 교육 자료제작 및 교육실시
③ 기획물, 보안전시회를 통한 홍보 실시

▌교육 대상별 차별화된 보안교육 운영

정보보호 교육은 대상에 따라 직급, 채용형태, 테마별로 차별화되어 운영되어야 하며, 각 부문별로도 차별화하여 진행해야 한다.

▶ 보안교육제도의 예

- 계층별에 따른 분류 : 임원, 관리자(간부), 사원대상 정기/비정기 교육

임원의 경우는 외부 초빙강사를 초빙해 간담회 등을 통한 교육을 실시하고 최근 보

안 동향 및 이슈사항을 공감하는 형태로 비정기적으로 진행하는 것이 가장 효과적이다. 특히 사고사례를 통해 정보보호가 회사에 미치는 영향 등을 교육시키도록 하여야 한다.

간부의 경우에는 부서 내 보안 관리자의 역할을 교육하고 정기·비정기적으로 부하직원에게 어떠한 보안교육을 하여야 하는지를 추가적으로 교육하여야 한다.

일반사원의 경우 사내보안 준수사항 및 정책공지(연간 1회 이상)를 통하여 보안의 중요성에 대해 강조하고 위반 시 이에 따른 본인에게 어떠한 불이익이 따르는지에 대한 내용도 명확히 전달되어야 한다.

- 채용형태에 따른 분류 : 경력사원, 신입사원 등 채용 시 이루어지는 보안교육

경력사원의 경우 타 회사에서의 경험이 있으므로 사내보안 규정의 특징 및 사내 보안 중요성 등을 주지시켜 해당 기업의 보안정책 이해에 중점을 두어야 한다. 반면 신입사원의 경우에는 기본적인 보안 마인드 및 사내 보안 중요성 등 보안정책 이해에 중점을 두고 교육을 실시해야 한다.

- 테마별 대상자에 따른 분류 : 보안 위규자, 특별 프로젝트 대상자, 업무직군(마케팅 등)에 따라 이루어지는 비정기 테마 교육

2.3. 보안교육의 내용

보안교육은 필요에 따라 각각 다른 형태로 운영해야 하나 대체적으로 다음과 같은 내용으로 구성되어야 한다.

▮ 일반적인 보안교육 내용(채용 시, 재직 임직원 대상)

- 정보보호의 중요성에 대한 소개
- 기업의 경영 환경변화에 따른 정보보호의 필요성
- 정보보호 정책 및 시스템 소개

- 임직원 정보보호 준수사항 소개
- 정보유출 시 사내 징계기준 및 국내 영업비밀보호법 처벌기준 소개
- 국내 외 각종 정보보안 사건사고 사례 소개

임원, 간부대상 교육

- 기업 내 보안관련 준수사항 및 부서장, 간부로서의 보안관리 역할
- 사내 보안사고 사례 위주의 동향 및 중요성 공감

보안홍보

임직원의 정보보호에 대한 인식과 참여, 실천을 유도할 수 있도록 전시회, 홍보 캠페인, 사내 공지 등 매체를 적절히 사용하여 보안홍보를 통하여 보안 인식제고를 향상시켜야 한다.

예) 보안뉴스레터, 외부초청강연, 보안캐릭터/포스터제작
사내게시판 사용공지, 보안관련 웹사이트 운영,
보안이벤트(퀴즈, 전시회 등)를 실시

〈그림 4-2-3-1〉 보안홍보 포스터

2.4. 보안업무 담당자를 위한 교육 및 성공 요소

▌보안업무 담당자 전문가과정 운영

보안업무를 담당하는 정보보호 부서원들은 최근 변화하는 기업환경과 기술변화에 대응하는 보안 기술을 습득하고 적용해야 한다. 따라서 이러한 보안담당자를 위한 보안 전문가 과정을 개발하고 정기적으로 운영해야 한다.

보안업무의 특성상 외부의 보안이론(개론)만으로는 사내 보안시스템 운영 등의 현실적인 사내 보안수준의 향상은 어려우므로, 실제적으로 업무현장에 적용이 가능한 내용을 선별하여 교육을 실시하여야 한다.

▌보안 담당자교육 내용

- 회사의 경영환경, 사업 및 조직의 이해
- 정보보호 개론 및 이론 습득
- 사내 물리적·시스템적 보안 인프라에 대한 실무교육 및 실습실시

앞에서도 언급 했지만 많은 기업들이 최근 임직원 보안의식 향상을 위한 보안교육을 이미 실시하고 있으나, 보안교육 효과는 단기간에 이루어지지 않으므로 보안사고 예방효과에 대해서는 정확한 분석이 이루어지기 어렵다. 따라서 보안교육 효과 때문에 보안교육의 미루거나 실시하지 않는 기업은 Top-Down방식의 경영진의 관심이 우선이 된다면, 노력에 비해 단기간에 많은 효과를 얻을 수 있다.

3 보안감사

보안 감사는 회사에서 이뤄지는 보안활동이 적절히 이뤄지고 있는지 확인하는 활동으로 각 회사의 업무와 정해진 정책 그리고 수행되고 있는 보안 활동에 따라 감사활동은 다르게 수행되어야 한다.

3.1. 보안감사의 분류

보안감사는 감사 주체에 따라 내부감사와 외부감사로 나눌 수 있으며, 감사시기에 따라 정기 보안감사와 수시 보안점검으로 나눌 수 있다.

〈표 4-3-1-1〉 보안감사 분류

보안감사 주체	내부 보안감사	• 보안팀 또는 감사팀에 의해 수행
	외부 보안감사	• 감리회사, 회계법인, 보안 컨설팅 전문회사 • 정보보호안전진단 등 • 금융감독원 등 정부기관
보안감사 시기	정기 보안감사	• 연간 감사계획에 따라 보안영역 전반에 대하여 정기적으로 실시하는 보안감사 • 매월 또는 분기, 반기 등 일정한 기간마다 시행되는 보안 감사
	수시 보안감사	• 보안사고 발생직후 또는 보안사고 징후가 있다고 판단될 경우 실시되는 특별한 보안 감사 • 감사 대상의 평시 보안 상태를 점검하기 위해 공지하지 않은 상태에서 실시하는 보안 감사

내부감사는 기업 조직 및 각 팀의 업무 정의에 따라 보안팀 또는 감사팀에서 수행되며, 외부감사는 회사의 업종 및 해당 법규 등 규제에 따라 달라지며, 감사 주체도 다르다.

감사시기에 따른 분류로는 정기 보안감사와 수시 보안감사로 나눌 수 있으며, 정기 보안감사는 연간 계획에 의해 진행되며 보안 영역 전반을 대상으로 하는 감사와 매월, 분기 또는 반기 등 회사의 정책에 따라 수행되는 정기 보안감사로 나눌 수 있다.

매월, 분기 또는 반기 등 시행되는 정기 보안감사는 전체 보안영역이 아닌 일부 보안영역 가령, VPN 사용현황, 데이터베이스 접근 현황 감사 등에 국한되어 진행되어진다.

반면, 수시 보안감사는 보안사고 발생 직후 또는 보안사고 징후가 있을 경우 전체 또는 일부분에 대해 시행되는 보안 감사로, 예를 들어 한 대의 웹 서버의 쓰기 권한 허용으로 인해 홈페이지 변조사고가 발생하였을 경우, 신속한 조치 후 전체 웹 서버의 쓰기 권한을 점검하는 활동이나, 일부 서버가 꼭 적용해야 할 패치를 적용하지 않았음

을 발견한 직후 모든 서버에 대해 패치 적용여부를 점검하는 활동 등이 있다. 또한 감사대상에 대한 일상적인 보안활동을 점검하기 위해 수시로 시행되는 보안 점검을 수행할 수 있는데 이 역시 수시 보안 감사의 한 예다. 예를 들어 임직원이 PC 보안 상태를 확인하기 위해 퇴근한 직후 끄지 않은 컴퓨터를 점검하는 활동이나, 임직원 PC의 패스워드 정책 및 바이러스 백신 정책적용 등을 점검하는 활동 역시, 수시 보안감사라고 하겠다.

3.2. 보안 감사 정책 수립

정보보호 관련 부서는 회사의 비즈니스에 대한 보안 위협 및 위험(Risk)을 감소시키기 위해 감사 정책을 수립하여 관련 부서에 공지하고 이를 추진하여야 한다. 불필요한 보안감사는 업무 프로세스에 부담을 줄 수 있으며, 인원 및 시간 등 업무 자원의 낭비를 초래하고 임직원 간의 불필요한 오해를 야기할 수 있으므로 보안감사 기준에 대한 정책수립이 우선되어야 한다.

〈그림 4-3-2-1〉 보안감사 절차

보안감사 정책을 수립하기 위해서는 비즈니스에 대한 위험과 위협을 분석하여 이에 맞는 보안감사 정책을 수립하여야 하며 보안감사 정책수립 시 결정하여야 하는 사항은 아래와 같다.

- 감사대상 보안 영역
- 감사목적 (감소시키고자 하는 보안 위험)
- 감사범위 및 중점감사항목
- 감사일정 및 기간
- 감사대상 부서

- 참여 감사자
- 감사기법 및 감사기준
- 기타 필요사항 등

3.3. 보안감사 영역

보안감사의 영역은 보안감사 정책 설정 시 결정되며, 일반적으로 아래와 같은 영역으로 구분할 수 있다.

〈표 4-3-3-1〉 보안감사 영역

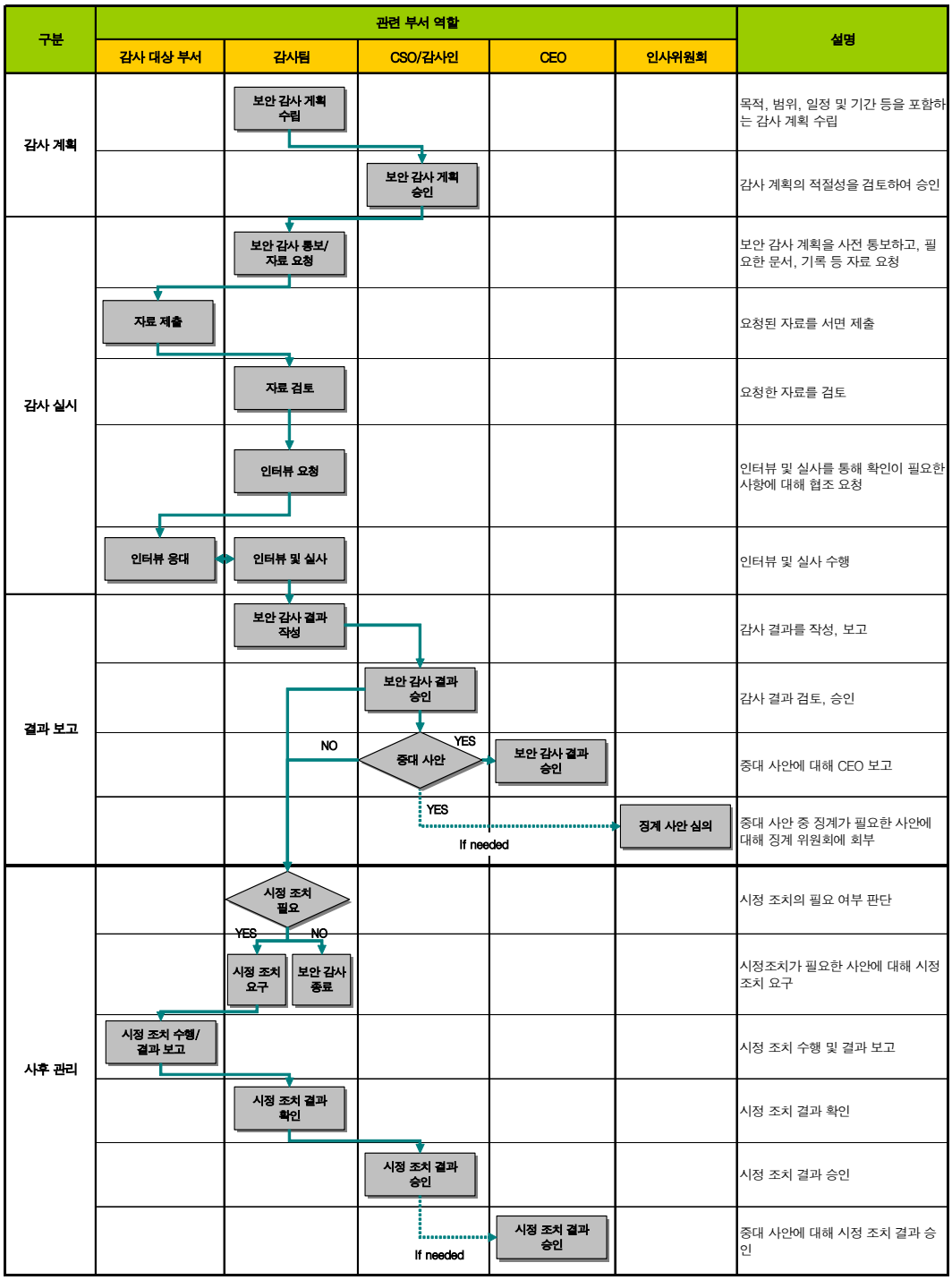
인적 보안감사		• 입사자, 퇴사자에 대한 보안 활동에 대한 감사 • 계약직, 임시직에 대한 보안 활동에 대한 감사 • 외부 인원에 대한 보안 활동에 대한 감사 • 보안 교육에 대한 감사
물리적 보안감사		• 전산실 출입 통제 및 로깅에 대한 감사 • 전산실 전원 설비 및 공조에 대한 감사 • 전산실 환경 및 비상 사태 대비에 대한 감사
업무용 프로그램 감사		• 업무용으로 사용하는 프로그램의 계정 생성 및 폐기에 대한 감사 • 업무용 프로그램의 중요 권한에 대한 권한 부여자 감사
정보 시스템 보안감사	시스템	• 사용자 관리 및 접근통제 감사 • 로깅 및 감사에 대한 감사 • 백업 및 복구
	네트워크/ 보안장비	• 사용자 관리 및 접근통제 감사 • 로깅 및 감사에 대한 감사 • 백업 및 복구
	DB	• 사용자 관리 및 접근통제 감사 • 로깅 및 감사에 대한 감사 • 백업 및 복구 • 데이터 추가/삭제/변경에 대한 활동 감사
PC 보안감사		• PC 보안 설정 감사 • 바이러스 백신 등 보안 프로그램 설치 여부 및 설정 감사 • 패스워드 관리 감사
내부 접속 프로그램 감사 (VPN 등)		• 사용자 관리 및 접근통제 감사 • VPN을 통한 내부 시스템 접속 내역 및 수행 업무 내역 감사

앞선 표에서 표시된 보안감사 영역은 각 기업이 필수적으로 따라야 하는 영역은 아니며, 각 영역 중 각 회사의 업무상 필요에 따라 대상영역을 설정하면 된다. 다만 보안감사를 기술적인 취약점 위주보다는 보안 프로세스를 점검하는 방향으로 하는 것이 바람직하다.

3.4. 정기 보안 감사

정기 보안감사는 보안감사 전 영역에 걸쳐 1년에 1회 또는 2회 실시하는 하는 감사와 매월, 분기별 또는 반기별로 일정 영역에 따라 진행하는 보안감사가 있다.

예를 들어, 장애 발생 시 신속한 조치를 위해 VPN을 통해 시스템, 네트워크 장비 또는 데이터베이스에 직접 접속할 수 있다면 VPN에 대한 보안감사는 매월 수행되어야 하며, 그 결과는 최고 보안 책임자에게 보고되어야 한다. 보안감사 전 영역에 걸쳐 수행되는 정기 보안감사는 매년 작성되는 '연간 보안 활동계획'에 포함되어야 한다. 정기 보안감사를 수행하는 프로세스는 일반적으로 다음의 그림과 같다.



〈그림 4-3-4-1〉 보안감사 프로세스

다음은 감사 시 사용되는 체크리스트 예시로 보안 감사 영역별로 체크리스트를 작성하여 배포하여야 한다.

〈표 4-3-4-1〉 보안감사 체크리스트 예시

정보보호 시스템관리	유지관리	IT보안실무자	정보보호 시스템 변경 시 변경계획서를 작성하고 있는가?
		IT보안실무자	정보보호 시스템에 대한 원격관리가 필요한 경우에는 세부절차를 수립하여 이행하고 있는가?
		IT보안실무자	정보보호 시스템에 대한 업그레이드(패치 등)를 주기적으로 실시하고 있는가?
	계정관리	IT보안실무자	정보보호 시스템에는 IT 보안실무자 및 관리자 이외의 계정은 생성하지 않고 있는가?
	변경관리	IT보안실무자	침입차단시스템 룰(보안정책) 등록, 변경 및 삭제 요청 시 침입차단시스템 룰 변경신청서를 작성하도록 하고 있으며, IT보안실무자는 적정성을 평가 후 작업을 실시하고 있는가?
		IT보안실무자	침입차단시스템 룰 변경신청서 상의 기한이 경과하여 별다른 통보가 없는 경우에는 해당 룰을 삭제하고 있는가?
		IT보안실무자	침입차단시스템 룰 변경 결과는 관리대장에 기록하고 있는가?
		IT보안실무자	침입탐지시스템의 침입패턴은 항상 최신의 것으로 유지하고 있는가?
	접근통제	IT보안실무자	정보보호 시스템에 대한 접근은 규정된 콘솔 또는 경로를 통해서만 가능하도록 하며 불필요한 포트는 모두 차단하고 있는가?
	서비스정책	IT보안실무자	네트워크 서비스 기본 정책은 Deny all로 정의하고, 업무상 필요한 서비스에 대해서만 접근을 허용하고 있는가?
		IT보안실무자	불법적인 침입 또는 이상징후 발생 시에는 침입탐지시스템에서 관련 서비스를 중지시키고, 침입차단시스템과 연동하여 관련 Source IP를 차단하고 있는가?
	로그 및 백업관리	IT보안실무자	정보보호 시스템 로그를 분석하고, 이상 징후 발생 시 적절한 조치를 취하고 있는가?
		IT보안실무자	정보보호 시스템 로그, 소프트웨어, 환경 설정 데이터 등을 매월 1회 백업하고 있는가?
		IT보안실무자	백업된 로그는 6개월이상 보관하고, 안전하게 관리하고 있는가?

3.5. 수시 보안감사

임직원의 평상시 보안상태를 점검하기 위해 공지하지 않은 상태에서 실시하는 불시 보안감사로는 PC에 대한 불시 보안감사와 사무실 불시 보안점검이 있다. PC 불시 보

안 점검은 비밀번호 설정 여부, PC보안 설정 현황, 바이러스 백신 등 보안 프로그램 설치 여부 및 설정 등을 감사하는 것으로 그 결과를 각 부서별로 비교하여 공지하기도 한다.

PC 불시 보안감사와 사무실 불시 보안점검에 대한 체크리스트 예시는 아래와 같다.

〈표 4-3-5-1〉 PC 불시 보안감사 체크리스트

구분	세부항목	진단내용
접근통제	부팅패스워크 설정	부팅시 CMOS 패스워드 설정여부 점검
	부재시 전원관리	장기간 자리를 비우거나 퇴근시의 전원관리 상태 점검
데이터 보관	비밀정보 보호관리	비밀정보에 대한 별도 보호조치 여부 점검
	백업 관리	정기적인 데이터 백업 실시 여부 점검
	데이터 이동관리	데이터 전송 시 바이러스 검사 여부 점검
PC관리	PC사용 인가자 관리	취급자 및 관리책임자 지정 여부 점검(스티커 부착여부)
패스워드 관리	패스워드 길이	패스워드 길이의 절적성 여부 점검
	패스워드 관리	패스워드에 영문자, 숫자, 특수문자 혼용여부 점검
공유폴더	공유폴더 암호 사용	공유폴더 사용시 암호 사용 여부 점검
네트워크 서비스	불필요한 서비스 제거	기본적으로 제공되는 불필요한 서비스 여부 확인 (예:DHCP Client, DNS Client 등)
계정관리	계정과 같은 패스워드 사용	계정명과 같은 패스워드 사용 여부 점검
	패스워드가 없는 계정	패스워드가 없는 계정의 사용 여부 점검
	기본 관리자 계정의 존재	기본 관리자 계정(Administrator) 사용 여부 확인
시스템보안설정	Null Session 설정	Null Session의 설정 여부 확인(Net Bios)
	자동 로그인	자동로그인 기능 사용 여부 확인
	레지스트리 보호진단	레지스트리의 원격 접근 보호
	로그접근 권한 점검	Guest 권한으로 로그 접근 가능 점검
보안패치	최신 Hot Fix 적용	최신 Hot Fix 적용 여부 확인
공유폴더	공유폴더 점검	패스워드가 없이 공유된 폴더 확인
	기본 공유 점검	C$ D$ 등 기본 공유 사용여부 점검
바이러스 통제	백신 설치	바이러스 백신 설치 여부확인
	최근 바이러스 점검	가장 최근에 바이러스 점검을 수행확인
	실시간 감시	실시간 감시 수행여부확인
	백신 업데이트	최신 바이러스 백신 엔진 업데이트 확인
접근통제	화면보호기 사용	화면보호기 대기 시간 확인(기준 10분)
		화면보호기 암호 사용 여부 확인

〈표 4-3-5-2〉 사무실 불시 보안점검 체크리스트

구분	점검 내용	대상 수	점검 결과	
			양호 수	양호 %
시건 상태	캐비닛 시건 상태			
	개인 책상 서랍 시건 상태			
문서 보관상태	개인 책상 위 주요 업무문서 방치 여부			
	사무실 바닥 주요 업무문서 방치 여부	N/A	N/A	
노트북 관리 상태	퇴근 시, 개인 책상 위 Notebook 방치 여부 (물리적 잠금 미흡)			
	점심시간 중, 개인 책상 위 Notebook 방치 여부(물리적 잠금 미흡)			
	점심시간 중, 개인 책상 위 Notebook 비밀번호 미 설정 여부			

4 법률준수(IT Compliance)

1990년대 중반 이후 국가사회의 정보화 및 폭발적인 인터넷 이용인구 증가와 더불어 촉진된 정보기술의 고도화는 정보를 통한 부가가치 창출과 사회 각 분야의 업무 효율화 등 순기능과 함께 사이버범죄, 개인정보 및 프라이버시 침해 등 정보화의 많은 역기능까지도 만들어냈다.

정보보호와 관련된 법 제도는 정보화의 역기능 방지의 관점에서 정보보호의 대두와 그동안 진화해온 민주주의의 결실로 신장된 개인의 자유와 권리를 보장하기 위한 다양한 법제도들은 시민사회의 성숙과 더불어 보다 다양하고 구체적인 형태로 정비되고 발전해 가고 있다. 이와 함께 오늘날 기업 정보보호는 기업의 정보자원에 대한 불법적인 접근으로부터의 방어라는 전통적인 정보보호의 기능만이 아닌, 기업활동의 각 부문에서 요구되는 법제도적인 요건의 만족이라는 규제준수(Compliance)의 영역으로 그 외연을 확장해 나가고 있다. 때문에 CERT나 정보보호 관련 조직 내에서도 이와 같은 정보보호와 관련된 법률과 위반 시 처벌규정에 대한 이해가 요구되고 있다.

4.1 정보보호 관련 법·제도의 분류

국내 정보보호 관련 법·제도들은 제정목적 및 기능에 따라 ▲정보보호 추진체계 관련 법률, ▲국가 기밀보호 관련 법률, ▲중요정보의 국외유출 방지 관련 법률, ▲전자서명 및 인증 관련 법률, ▲정보통신망과 정보시스템의 보호추진 관련 법률, ▲침해행위의 처벌에 관한 법률 및 ▲개인정보보호 관련 법률로 구분해 볼 수 있다. 이와 함께 정보화 역기능의 측면에서 크게 개인정보와 프라이버시 보호, 정보이용의 신뢰와 안전성 확보 및 정보통신 윤리 확립을 위한 법제도로도 구분해 볼 수 있다.

이러한 분류방식을 결합하여 이 장에서는 기업의 정보보호 조직 및 CERT 담당자들의 법규준수활동과 가장 밀접한 관련이 있는 영역이라 할 수 있는 중요정보의 국외유출방지, 정보이용의 신뢰와 안전성 확보, 개인정보 및 프라이버시 보호와 정보통신 윤리확립 관련 법률에 대하여 각 영역별로 준수해야 할 조항들을 소개해 보도록 하겠다.

4.2. 정보보호 영역별 주요 법률 및 위반 시 처벌규정

▌중요정보의 국외유출방지와 관련된 법률

〈표 4-4-2-1〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

조항	제51조 (중요정보의 국외유출제한 등)
대상	정보통신서비스제공자 또는 이용자
내용	①정보통신부장관은 국내의 산업·경제 및 과학기술 등에 관한 중요정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스제공자 또는 이용자에 대하여 필요한 조치를 강구하게 할 수 있다. ②제1항의 규정에 따른 중요정보의 범위는 다음 각 호와 같다. 1. 국가안전보장과 관련된 보안정보 및 주요정책에 관한 정보 2. 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보 ③정보통신부장관은 제2항 각 호의 규정에 따른 정보를 취급하는 정보통신서비스제공자에게 다음 각 호의 조치를 강구하게 할 수 있다. 1. 정보통신망의 부당한 이용을 방지할 수 있는 제도적·기술적 장치의 설정 2. 정보의 불법파괴 또는 조작을 방지할 수 있는 제도적·기술적 조치 3. 정보통신서비스제공자가 취급 중 알게 된 중요정보의 누출을 방지할 수 있는 조치
벌칙	해당사항 없음

〈표 4-4-2-2〉 산업기술의 유출방지 및 보호에 관한 법률

조항	제10조 (국가핵심기술의 보호조치)
대상	산업자원부 장관으로부터 지정받은 국가핵심기술을 보유 · 관리하고 있는 대상기관의 장
내용	①국가핵심기술을 보유 · 관리하고 있는 대상기관의 장은 보호구역의 설정 · 출입허가 또는 출입시 휴대품 검사 등 국가핵심기술의 유출을 방지하기 위한 기반구축에 필요한 조치를 하여야 한다. ②제1항의 규정에 따른 조치에 관하여 필요한 사항은 대통령령으로 정한다.
벌칙	해당사항 없음

조항	제15조 (산업기술 침해신고 등)
대상	산업자원부 장관으로부터 지정받은 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장
내용	①국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장은 제14조 (산업기술의 유출 및 침해행위의 금지) 각 호의 어느 하나에 해당하는 행위가 발생할 우려가 있거나 발생한 때에는 즉시 산업자원부장관 및 정보수사기관의 장에게 그 사실을 신고하여야 하고, 필요한 조치를 요청할 수 있다.
벌칙	1천만원 이하의 과태료

▮ 정보이용의 신뢰와 안전성 확보와 관련된 법률

〈표 4-4-2-3〉 정보통신기반보호법

조항	제5조 (주요정보통신기반시설보호대책의 수립 등)
대상	주요정보통신기반시설을 관리하는 기관의 장
내용	①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석 · 평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적 · 기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립 · 시행하여야 한다. ②관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다. ③지방자치단체의 장이 관리 · 감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정자치부장관에게 제출하여야 한다. ④관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다. ⑤정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.
벌칙	해당사항 없음

조항	제9조 (취약점의 분석 · 평가)
대상	주요정보통신기반시설을 관리하는 기관의 장
내용	①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석 · 평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적 · 기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립 · 시행하여야 한다. ②관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다. ③지방자치단체의 장이 관리 · 감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정자치부장관에게 제출하여야 한다. ④관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다. ⑤정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.
벌칙	해당사항 없음

조항	제13조 (침해사고의 통지)
대상	주요정보통신기반시설을 관리하는 기관의 장
내용	①관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란 · 마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.
벌칙	해당사항 없음

조항	제14조 (복구조치)
대상	주요정보통신기반시설을 관리하는 기관의 장
내용	①관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다. ②관리기관의 장은 제1항의 규정에 의한 복구 및 보호조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 보호진흥원의 장에게 지원을 요청할 수 있다. 다만, 제7조제2항의 규정에 해당하는 경우에는 그러하지 아니하다.
벌칙	해당사항 없음

〈표 4-4-2-4〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

조항	제45조 (정보통신망의 안정성 확보 등)
대상	정보통신서비스제공자
내용	①정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다.
벌칙	해당사항 없음

조항	제46조 (집적된 정보통신시설의 보호)
대상	타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 사업자
내용	①타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 사업자(이하 "집적정보통신시설사업자"라 한다)는 정보통신시설의 안정적 운영을 위하여 정보통신부령이 정하는 바에 의한 보호조치를 취하여야 한다. ②집적정보통신시설사업자는 집적된 정보통신시설의 멸실, 훼손 그 밖의 운영장애로 인하여 발생한 피해의 보상을 위하여 정보통신부령이 정하는 바에 따라 보험에 가입하여야 한다.
벌칙	1천만원 이하의 과태료 (②항 위반자)

조항	제46조의2 (집적정보통신시설사업자의 긴급대응)
대상	타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 사업자
내용	①집적정보통신시설사업자는 다음 각호의 1에 해당하는 경우에는 이용약관이 정하는 바에 따라 당해 서비스의 전부 또는 일부의 제공을 중단할 수 있다. 1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에 발생한 이상현상으로 인하여 다른 시설이용자 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우 2. 외부에서 발생한 침해사고로 인하여 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우 3. 중대한 침해사고가 발생함에 따라 정보통신부장관 또는 보호진흥원이 요청하는 경우 ②집적정보통신시설사업자는 제1항의 규정에 의하여 당해 서비스의 제공을 중단하는 때에는 중단사유 · 발생일시 · 기간 · 내용 등을 명시하여 시설이용자에게 즉시 통보하여야 한다. ③집적정보통신시설사업자는 중단사유가 해소된 때에는 즉시 당해 서비스의 제공을 재개하여야 한다.
벌칙	해당사항 없음

조항	제47조의3 (이용자의 정보보호)
대상	주요정보통신서비스제공자
내용	②주요정보통신서비스제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있는 경우에는 이용약관이 정하는 바에 따라 당해 이용자에게 보호조치를 취하도

	록 요청하고, 이를 이행하지 아니하는 경우에는 당해 정보통신망으로의 접속을 일시적으로 제한할 수 있다. ③소프트웨어산업진흥법 제2조의 규정에 의한 소프트웨어사업자는 보안에 관한 취약점 보완프로그램을 제작한 때에는 이를 보호진흥원에 통지하고, 당해 소프트웨어 사용자에게는 제작한 날부터 1월 이내에 2회 이상 이를 알려야 한다. ④제2항의 규정에 의한 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 정보통신부령으로 정한다.
벌칙	해당사항 없음

조항	제48조의2 (침해사고의 대응 등)
대상	내용 참조
내용	②다음 각호의 1에 해당하는 자는 정보통신부령이 정하는 바에 의하여 침해사고의 유형별 통계, 당해 정보통신망의 소통량통계 및 접속경로별 이용통계 등 침해사고 관련정보를 정보통신부장관 또는 보호진흥원에 제공하여야 한다. 1. 주요정보통신서비스제공자 2. 집적정보통신시설사업자 3. 그 밖에 정보통신망을 운영하는 자로서 대통령령이 정하는 자
벌칙	해당사항 없음

조항	제48조의3 (침해사고의 신고 등)
대상	내용 참조
내용	①다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생한 때에는 즉시 그 사실을 정보통신부장관 또는 보호진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항의 규정에 따른 통지가 있는 때에는 전단의 규정에 의한 신고로 본다. 1. 정보통신서비스제공자 2. 집적정보통신시설사업자
벌칙	해당사항 없음

조항	제48조의4 (침해사고의 원인분석 등)
대상	정보통신서비스제공자 등 정보통신망을 운영하는 자
내용	①정보통신서비스제공자 등 정보통신망을 운영하는 자는 침해사고가 발생한 때에는 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다. ③정보통신부장관은 제2항의 규정에 의한 침해사고의 원인분석을 위하여 필요하다고 인정하는 때에는 정보통신서비스제공자 및 집적정보통신시설사업자에게 정보통신망의 접속기록 등 관련자료의 보전을 명할 수 있다. ④정보통신부장관은 침해사고의 원인분석을 위하여 필요한 때에는 정보통신서비스제공자 및 집적정보통신시설사업자에게 침해사고관련 자료의 제출을 요구할 수 있으며, 제2항의 규정에 의한 민·관합동조사단으로 하여금 관계인의 사업장에 출입하여 침해사고 원인을 조사하게 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호의 규정에 의한 통신사실확인자료에 해당하는 자료의 제출은 동법이 정하는 바에 따른다.
벌칙	2년 이하의 징역 또는 1천만원 이하의 벌금 (③항 위반자)

〈표 4-4-2-5〉 전자거래기본법

조항	제17조 (전자거래사업자의 일반적 준수사항)
대상	전자거래를 업으로 하는 자
내용	전자거래사업자는 전자거래와 관련되는 소비자를 보호하고 전자거래의 안전성 및 신뢰성을 확보하기 위하여 다음 각호의 사항을 준수하여야 한다. 1. 상호(법인의 경우에는 대표자의 성명을 포함한다) 그 밖에 자신에 관한 정보와 재화 · 용역 · 계약 조건 등에 관한 정확한 정보의 제공 2. 소비자가 쉽게 접근 · 인지할 수 있도록 약관의 제공 및 보존 3. 소비자가 자신의 주문을 취소 또는 변경할 수 있는 절차의 마련 4. 청약의 철회, 교환 및 반품을 쉽게 할 수 있는 절차의 마련 5. 소비자의 불만과 요구사항을 신속하고 공정하게 처리하기 위한 절차의 마련 6. 거래의 증명 등에 필요한 거래기록의 일정기간 보존
벌칙	해당사항 없음

▮ 개인정보 및 프라이버시 보호와 관련된 법률

〈표 4-4-2-6〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

조항	제22조 (개인정보의 수집 · 이용 동의 등)
대상	정보통신서비스제공자
내용	①정보통신서비스제공자는 이용자의 개인정보를 이용하려고 수집하는 때에는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 때에도 또한 같다. 1. 개인정보의 수집 · 이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 ②정보통신서비스제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항의 규정에 따른 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있다. 1. 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제23조 (개인정보의 수집의 제한 등)
대상	정보통신서비스제공자
내용	①정보통신서비스제공자는 사상 · 신념 · 과거의 병력 등 개인의 권리 · 이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 제22조제1항

	의 규정에 따른 이용자의 동의를 얻거나 다른 법률에 따라 특별히 수집대상 개인정보로 허용된 경우에는 그러하지 아니하다 ②정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니된다.
벌칙	1천만원 이하의 과태료 (①항 또는 ②항 위반자)

조항	제24조 (개인정보의 이용 제한)
대상	정보통신서비스제공자
내용	정보통신서비스제공자는 제22조 및 제23조제1항 단서의 규정에 따라 수집한 개인정보를 이용자로부터 동의받은 목적 또는 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.
벌칙	5년 이하의 징역 또는 5천만원 이하의 벌금

조항	제24조의2 (개인정보의 제공 동의 등)
대상	정보통신서비스제공자
내용	①정보통신서비스제공자는 이용자의 개인정보를 제3자에게 제공하려는 경우 제22조제2항제2호 및 제3호의 규정에 해당하는 경우를 제외하고는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ②제1항의 규정에 따라 정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.
벌칙	5년 이하의 징역 또는 5천만원 이하의 벌금

조항	제25조 (개인정보의 취급위탁)
대상	정보통신서비스제공자와 그로부터 제24조의2제1항의 규정에 따라 이용자의 개인정보를 제공받은 자
내용	①정보통신서비스제공자와 그로부터 제24조의2제1항의 규정에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 1. 개인정보취급위탁을 받는 자(이하 "수탁자"라 한다) 2. 개인정보취급위탁을 하는 업무의 내용

	②정보통신서비스제공자등은 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항의 규정에 따라 공개하거나 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지한 경우에는 개인정보취급위탁에 따른 제1항의 고지 및 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. ③정보통신서비스제공자등은 개인정보취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다. ④정보통신서비스제공자등은 수탁자에 대하여 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다. ⑤수탁자가 개인정보취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시킨 경우에는 그 수탁자를 손해배상책임에 있어서 정보통신서비스제공자등의 소속직원으로 본다.
벌칙	3천만원 이하의 과태료 (①항 또는 ②항 위반자)

조항	제26조 (영업의 양수 등에 따른 개인정보의 이전
대상	정보통신서비스제공자등, 영업양수자등
내용	①정보통신서비스제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지하여야 한다. 1. 개인정보를 이전하려는 사실 2. 개인정보의 이전을 받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다)·주소·전화번호 그 밖의 연락처 3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법 및 절차 ②영업양수자등은 개인정보의 이전을 받은 경우에는 지체 없이 그 사실을 인터넷 홈페이지 게시, 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지하여야 한다. 다만, 정보통신서비스제공자등이 제1항의 규정에 따라 그 이전사실을 이미 통지한 경우에는 그러하지 아니하다. ③영업양수자등은 정보통신서비스제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공할 수 있다. 다만, 이용자의 별도의 동의를 얻은 경우에는 그러하지 아니하다.
벌칙	3천만원 이하의 과태료 (①항 또는 ②항 위반자) 5년 이하의 징역 또는 5천만원 이하의 벌금 (③항 위반자)

조항	제27조 (개인정보관리책임자의 지정)
대상	정보통신서비스제공자등
내용	①정보통신서비스제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정하여야 한다. 다만, 종업원 수·

	이용자 수 등이 정보통신부령이 정하는 기준에 해당하는 정보통신서비스제공자등의 경우에는 지정하지 아니할 수 있다. ②제1항 단서의 규정에 따른 정보통신서비스제공자등이 개인정보관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보관리책임자가 된다. ③개인정보관리책임자의 자격요건 그 밖의 지정에 관하여 필요한 사항은 정보통신부령으로 정한다.
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제27조의2 (개인정보취급방침의 공개)
대상	정보통신서비스제공자등
내용	①정보통신서비스제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보취급방침을 정하여 이를 이용자가 언제든지 쉽게 확인할 수 있도록 정보통신부령이 정하는 방법에 따라 공개하여야 한다. ②제1항의 규정에 따른 개인정보취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다. 1. 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목 및 수집방법 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인의 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적 및 제공하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 방법(제29조 단서의 규정에 따라 개인정보를 보존하려는 경우에는 그 보존근거 및 보존하는 개인정보 항목을 포함한다) 4. 개인정보취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에 한한다) 5. 이용자 및 법정대리인의 권리와 그 행사방법 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항 7. 개인정보관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처 ③정보통신서비스제공자등은 제1항의 규정에 따른 개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 정보통신부령이 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제28조 (개인정보의 보호조치)
대상	정보통신서비스제공자등
내용	①정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 조치를 하여야 한다. ②정보통신서비스제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제28조의2 (개인정보의 누설 금지)
대상	일반
내용	이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손 · 침해 또는 누설하여서는 아니 된다.
벌칙	5년 이하의 징역 또는 5천만원 이하의 벌금

조항	제29조 (개인정보의 파기)
대상	정보통신서비스제공자등
내용	정보통신서비스제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다. 1. 제22조제1항 · 제23조제1항 단서 또는 제24조의2제1항 및 제2항의 규정에 따라 동의를 얻은 개인정보의 수집 · 이용 목적 또는 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우 2. 제22조제1항 · 제23조제1항 단서 또는 제24조의2제1항 및 제2항의 규정에 따라 동의를 얻은 개인정보의 보유 및 이용 기간이 종료한 경우 3. 제22조제2항의 규정에 따라 이용자의 동의를 얻지 않고 수집 · 이용한 때에는 제27조의2제2항제3호의 규정에 따른 개인정보의 보유 및 이용 기간이 종료한 경우 4. 사업을 폐지하는 경우
벌칙	1천만원 이하의 과태료

조항	제30조 (이용자의 권리 등)
대상	정보통신서비스제공자등, 영업양수자등
내용	①이용자는 정보통신서비스제공자등에 대하여 언제든지 개인정보수집 · 이용 · 제공 등의 동의를 철회할 수 있다. ②이용자는 정보통신서비스제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람 또는 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다. 1. 정보통신서비스제공자등이 보유하고 있는 이용자의 개인정보 2. 정보통신서비스제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 내역 3. 정보통신서비스제공자등에게 개인정보수집 · 이용 · 제공 등의 동의를 한 내역 ③정보통신서비스제공자등은 이용자가 제1항의 규정에 의하여 동의를 철회한 경우에는 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하여야 한다. ④정보통신서비스제공자등은 제2항의 규정에 따라 열람 또는 제공을 요구받은 경우에는 지체없이 필요한 조치를 취하여야 한다. ⑤정보통신서비스제공자등은 제2항의 규정에 따라 오류의 정정을 요구받은 경우에는 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 통지하는 등 필요한 조치를 취하여야 하고, 필요한 조치를 취할 때까지는 당해 개인정보를 제공 또는 이용하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그

	러하지 아니하다. ⑥정보통신서비스제공자등은 제1항의 규정에 따른 동의의 철회 또는 제2항의 규정에 따른 개인정보의 열람 · 제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집 방법보다 쉽게 하여야 한다. ⑦제1항 내지 제6항의 규정은 영업양수자등에 이를 준용한다. 이 경우 "정보통신 서비스 제공자등"은 "영업양수자등"으로 본다.
벌칙	1천만원 이하의 과태료 (③항 또는 ④항 또는 ⑤항 또는 ⑥항 위반자)

조항	제31조 (법정대리인의 권리)
대상	정보통신서비스제공자등
내용	①정보통신서비스제공자등이 만 14세 미만의 아동으로부터 개인정보수집 · 이용 · 제공 등의 동의를 얻고자 하는 경우에는 그 법정대리인의 동의를 얻어야 한다. 이 경우 정보통신서비스제공자는 그 아동에게 법정대리인의 동의를 얻기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다. ②법정대리인은 당해 아동의 개인정보에 대하여 제30조제1항 및 제2항의 규정에 따른 이용자의 권리를 행사할 수 있다. ③제30조제3항 내지 제5항의 규정은 제2항의 규정에 의하여 법정대리인이 동의를 철회하거나 열람 또는 오류정정의 요구에 관하여 이를 준용한다.
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제44조 (정보통신망에서의 권리보호)
대상	정보통신서비스제공자
내용	①이용자는 사생활의 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 아니 된다. ②정보통신서비스제공자는 자신이 운영 · 관리하는 정보통신망에 제1항의 규정에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
벌칙	해당사항 없음

조항	제44조의2 (정보의 삭제요청 등)
대상	정보통신서비스제공자
내용	①정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 인하여 사생활의 침해 또는 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스제공자에게 침해사실을 소명하여 당해 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다. ②정보통신서비스제공자는 제1항의 규정에 따른 당해 정보의 삭제등의 요청을 받은 때에는 지체 없이 삭제, 임시조치 등의 필요한 조치를 취하고 이를 즉시 신청인 및 정보게재자에게 통지하여야 한다. 이 경우 정보통신서비스제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다. ③정보통신서비스제공자는 자신이 운영 · 관리하는 정보통신망에 제42조의 규정에 따른 표시방법을 준수하지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2의 규정

	에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 이를 삭제하여야 한다. ④정보통신서비스제공자는 제1항의 규정에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다. ⑤정보통신서비스제공자는 필요한 조치에 관하여 그 내용 · 절차 등을 포함하여 미리 약관에 명시하여야 한다. ⑥정보통신서비스제공자는 자신이 운영 · 관리하는 정보통신망에 유통되는 정보에 대하여 제2항의 규정에 따른 필요한 조치를 한 경우에는 이로 인한 배상책임을 줄이거나 면제받을 수 있다.
벌칙	해당사항 없음

조항	제44조의3 (임의의 임시조치)
대상	정보통신서비스제공자
내용	①정보통신서비스제공자는 자신이 운영 · 관리하는 정보통신망에 유통되는 정보가 사생활의 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되는 경우에는 임의로 임시조치를 할 수 있다.
벌칙	해당사항 없음

조항	제44조의5 (게시판이용자의 본인확인)
대상	내용참조
내용	①다음 각 호의 어느 하나에 해당하는 자가 게시판을 설치 · 운영하려는 경우에는 그 게시판이용자의 본인 확인을 위한 방법 및 절차의 마련 등 대통령령이 정하는 필요한 조치(이하 "본인확인조치"라 한다)를 하여야 한다. 1. 국가기관, 지방자치단체, 「정부투자기관 관리기본법」 제2조의 규정에 따른 정부투자기관, 「정부산하기관 관리기본법」의 적용을 받는 정부산하기관, 「지방공기업법」에 따른 지방공사 및 지방공단(이하 '공공기관등'이라 한다) 2. 정보통신서비스제공자로서 제공하는 정보통신서비스의 유형별 일일평균 이용자수 10만명 이상으로서 대통령령이 정하는 기준에 해당되는 자
벌칙	해당사항 없음

조항	제49조의2 (속이는 행위에 의한 개인정보의 수집금지 등)
대상	일반
내용	①누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나, 제공하도록 유인하여서는 아니 된다. ②정보통신서비스제공자는 제1항의 규정을 위반한 사실을 발견한 때에는 즉시 정보통신부장관 또는 보호진흥원에 신고하여야 한다.
벌칙	2년 이하의 징역 또는 1천만원 이하의 벌금 (①항 위반자)

조항	제50조의5 (영리목적의 광고성 프로그램 등의 설치)
대상	정보통신서비스제공자
내용	정보통신서비스제공자는 영리목적의 광고성 정보가 보이도록 하거나 개인정보를 수집하는 프로그램을 이용자의 컴퓨터 그 밖에 대통령령이 정하는 정보처리장치에 설치하고자 할 때에 이용자의 동의를 얻어야 한다. 이 경우 해당 프로그램의 용도와 삭제할 수 있는 방법을 고지하여야 한다.
벌칙	3천만원 이하의 과태료

조항	제54조 (국외이전 개인정보의 보호)
대상	정보통신서비스제공자등
내용	①정보통신서비스제공자등은 이용자의 개인정보에 관하여 이 법의 규정을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니된다. ②정보통신서비스제공자등은 이용자의 개인정보를 국외로 이전하고자 하는 때에는 이용자의 동의를 얻어야 한다. ③정보통신서비스제공자등은 제2항의 규정에 따른 동의를 얻고자 하는 경우에는 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다. 1. 이전되는 개인정보 항목 2. 개인정보가 이전되는 국가 · 이전일시 및 이전방법 3. 개인정보를 이전받는 자의 성명(법인의 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다.) 4. 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유 · 이용 기간 ④정보통신서비스제공자등은 제2항의 규정에 의한 동의를 얻어 개인정보를 국외로 이전하는 경우 정보통신부령이 정하는 바에 따라 보호조치를 취하여야 한다.
벌칙	해당사항 없음

〈표 4-4-2-7〉 전자거래기본법

조항	제12조 (개인정보보호)
대상	전자거래를 업으로 하는 자
내용	②전자거래사업자는 전자거래이용자의 개인정보를 수집 · 이용 · 제공 및 관리함에 있어서 정보통신망이용촉진및정보보호등에관한법률 등 관련 규정을 준수하여야 한다.
벌칙	정보통신망이용촉진및정보보호등에관한법률에 의거

조항	제13조 (영업비밀보호)
대상	전자거래를 업으로 하는 자
내용	②전자거래사업자(정보처리시스템의 운영을 위탁받은 자를 포함한다. 이하 이조에서 같다)는 전자거래이용자의 영업비밀을 보호하기 위한 조치를 강구하여야 한다. ③전자거래사업자는 전자거래이용자의 동의를 얻지 아니하고는 당해 이용자의 영업비밀을 타인에게 제공하거나 누설하여서는 아니된다.
벌칙	해당사항 없음

▮ 정보통신 윤리확립과 관련된 법률

〈표 4-4-2-8〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

조항	제42조 (청소년유해매체물의 표시)
대상	전기통신사업자의 전기통신역무를 이용하여 일반에게 공개를 목적으로 정보를 제공하는 자
내용	전기통신사업자의 전기통신역무를 이용하여 일반에게 공개를 목적으로 정보를 제공하는 자(이하 "정보제공자"라 한다)중 청소년보호법 제7조제4호의 규정에 의한 매체물로서 동법 제2조제3호의 규정에 의한 청소년유해매체물을 제공하고자 하는 자는 대통령령이 정하는 표시방법에 따라 당해 정보가 청소년유해매체물임을 표시하여야 한다.
벌칙	2년 이하의 징역 또는 1천만원 이하의 벌금

조항	제42조의2 (청소년유해매체물의 광고금지)
대상	일반
내용	누구든지 청소년보호법 제7조제4호의 규정에 의한 매체물로서 동법 제2조제3호의 규정에 의한 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호 · 문자 · 음성 · 음향 · 화상 또는 영상 등의 형태로 동법 제2조제1호의 규정에 의한 청소년에게 전송하거나 청소년 접근을 제한하는 조치없이 공개적으로 전시하여서는 아니된다.
벌칙	2년 이하의 징역 또는 1천만원 이하의 벌금

조항	제42조의3 (청소년보호책임자의 지정 등)
대상	정보통신서비스제공자중 일일평균이용자의 수, 매출액 등이 대통령령이 정하는 기준에 해당하는 자
내용	①정보통신서비스제공자중 일일평균이용자의 수, 매출액 등이 대통령령이 정하는 기준에 해당하는 자는 정보통신망상의 청소년유해정보로부터 청소년을 보호하기 위하여 청소년보호책임자를 지정하여야 한다. ②청소년보호책임자는 당해 사업자의 임원 또는 청소년보호와 관련된 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자중에서 지정한다. ③청소년보호책임자는 정보통신망상의 청소년유해정보의 차단 및 관리, 청소년유해정보로부터의 청소년보호계획 수립 등 청소년보호업무를 수행하여야 한다. ④제1항의 규정에 의한 청소년보호책임자의 지정에 관하여 필요한 사항은 대통령령으로 정한다.
벌칙	1천만원 이하의 과태료 (①항 위반자)

조항	제43조 (영상 또는 음향정보제공사업자의 보관의무)
대상	청소년보호법 제7조제4호의 규정에 의한 매체물로서 동법 제2조제3호의 규정에 의한 청소년유해매체물을 이용자의 컴퓨터에 저장 또는 기록되지 아니하는 방식으로 제공하는 것을 영업으로 하는 정보제공자중 대통령령이 정하는 자

내용	①청소년보호법 제7조제4호의 규정에 의한 매체물로서 동법 제2조제3호의 규정에 의한 청소년유해매체물을 이용자의 컴퓨터에 저장 또는 기록되지 아니하는 방식으로 제공하는 것을 영업으로 하는 정보제공자중 대통령령이 정하는 자는 당해 정보를 보관하여야 한다. ②제1항의 규정에 의한 정보제공자가 당해 정보를 보관하여야 할 기간은 대통령령으로 정한다.
벌칙	1천만원 이하의 과태료

4.3. 정보보호 관련 법제도와 CERT의 역할

지금까지 기업의 정보보호 담당자들이 숙지하고 지켜나가야 할 법적 책임과 의무에 대하여 표로 정리해 보았다. 앞서 기술된 법률들은 정보보호 관련 법률을 모두 아우를 수 있는 리스트는 아니며, 실무적인 적용을 위해서 관련 시행령과 시행규칙 등에 대한 구체적인 이해가 수반되어야 한다. 서두에서 언급한 바와 같이 법제도 등 규제준수가 기업 정보보호의 주요한 목표 중 하나로 떠오른 최근의 상황을 감안하면, 변화하는 사회상황에 발맞춰 제·개정되는 정보보호 관련 법률을 인지하여 전파하고, 또 대응방안을 마련하고 준수여부를 감시하는 것도 기업 정보보호 담당자들과 CERT의 중요한 역할과 임무라 할 수 있을 것이다.

제·개정 법률에 대한 최신 정보는 법제처(www.moleg.go.kr)를 통해 관련 내용을 확인할 수 있으며, 한국정보보호진흥원 또는 정보통신부 홈페이지에서도 관련 법률에 대한 정보를 접할 수 있다. 기업 정보보호 담당자들은 자신이 속해있는 기업의 규모와 성격에 따라 적용되는 법규의 내용을 정확히 인지하고 관련사항의 변동내역을 꾸준히 습득하여 현재 각 기업활동에 있어 준수되어야 할 세부 법규가 무엇인지, 위반 시 어떠한 불이익이 있는지 인식하여야 한다.

5 보안 솔루션 도입

일반적으로 "보안"이라고 하면 조직 내에서는 해킹과 같은 보안사고를 떠올린다. 실제로 매년 적지 않은 보안사고가 발생하고 있고, 그 중요성을 인지하고 있는 실정이다. 하지만 정작 대응책(Countermeasure)이 무엇인가에 대한 질문에는 보안 솔루션에 투자만 하면 된다는 식의 비교적 단순한 생각만으로 일관하고 있다. 또한 솔루션을 도입하였다고 할 지라도 보안사고가 터진 후 시간이 흐르면 금방 뇌리에서 사라지고 안일한 방식으로 운영되고 있는 실정이다. 문제는 많은 정책 결정자들이 보안 솔루션의 도입 자체가 보안 문제를 해결했다라고 보는 시각이다.

최근 솔루션 공급업체들이 내놓고 있는 통합보안장비들은 기존에 비해 성능과 기능 그리고 관리적인 측면에서 많이 향상되었지만 새로운 창 앞에서 방패는 또다시 무력화되기 마련이다.

보안 장비는 주로 기존의 패턴을 인식하여 탐지(Detection)하고 차단(Blocking)하는 방식이므로 패치가 되지 않은 새로운 익스플로잇(Zero-Day Attack)이 나오면 신속한 대응이 불가능한 경우도 발생한다. 그런 점에서 조직의 실질적인 보안은 솔루션 도입 자체가 아닌 장기적인 정책(Master Plan)에 기반한 실질적인 보안 프로세스 정착과 조직 구성원들의 보안 인식강화에 있다.

보안 솔루션은 필요하지만 그 자체가 보안의 필요충분조건이 되지는 못하며, 조직의 보안을 위한 도구에 지나지 않아, 운영관리와 구성원들의 보안 마인드가 맞물려 움직여야 한다. 여기에서는 다양한 보안 솔루션을 조직에 보다 효율적으로 운영하기 위해 전반적인 보안 솔루션 맵을 작성해 보고, 실제 솔루션 도입을 위한 고려사항과 BMT 진행방법을 실제 예제를 통해 알아보기로 한다.

5.1. 보안 솔루션 맵

여러 기능을 통합한 보안 솔루션이 등장하면서 조직에서 필요로 하는 적절한 보안 솔루션을 찾는 것은 점점 어려워지고 있다. 과거에는 네트워크 방화벽과 바이러스 백

신과 같은 단편적인 솔루션이 대부분이었으나, 정보기술이 발전하고 복잡해지면서 인증, 컨텐츠, 접근관리 등 타깃형 보안 솔루션, 통합적인 보안을 위한 UTM, TMS, RMS, ESM 등 다양한 관리형 솔루션이 출시되고 있다.

여기에서는 다양한 솔루션을 네트워크, 시스템, 어플리케이션, 통합보안 관리, 인증 등 8개 카테고리로 나누어 각 단계별 보안 솔루션 맵을 그려보기로 한다. 1~4단계까지 총 네 단계로 분류하였으며, 높은 단계에 있는 솔루션을 구현할수록 상위 수준의 보안을 다루고 있음을 의미한다. 각 단계의 보안 솔루션은 해당 조직의 특성과 요구수준에 따라 선별하여 도입 시 참고하기 바란다.

〈표 4-5-1-1〉 기업 규모별 보안 솔루션 맵

분 류	Step 1	Step 2	Step 3	Step 4
네트워크 보안	방화벽(Firewall)	침입탐지시스템(IDS) 프로토콜 분석도구	침입방지시스템(IPS)	네트워크 접근통제(NAC)
시스템 보안	바이러스 백신 시스템 방화벽	스팸차단 소프트웨어 패치관리시스템(PMS)	보안운영체제 시스템취약점 분석툴	
애플리케이션 보안		웹방화벽(WAF) 스팸메일차단솔루션	문서저작권관리(DRM) DB 보안 솔루션 웹스캐너(취약점분석)	소스코드 분석도구 취약점스캔 Appliance
통합 보안관리	로그관리 및 분석도구	보안구성관리(SCM)	통합보안시스템(UTM) 전사적보안관리(ESM)	위협관리시스템(TMS) 위험관리시스템(RMS) 포괄적위협관리(CTM)
인증 및 접근통제	싱글사인온(SSO)	스마트 카드 통합접근관리(EAM)	하드웨어 토큰 일회용 비밀번호(OTP) 통합계정관리(EIM)	바이오인식시스템(지문,정맥,얼굴,홍채,다중인식 등)
PC 보안	바이러스 백신 안티 스파이웨어	개인용 PC 방화벽	개인용 안티스팸	통합 PC 보안
기타보안	가상사설망(VPN)	공개키기반구조(PKI) 무선랜 보안(Wireless)	모바일 보안(Mobile) RFID 보안	기업정보 유출방지
보안 서비스	인증(공인/사설)	솔루션 유지보수	보안관제 보안교육훈련	보안 컨설팅

단계	적용범위	설명
Step 1	소규모 조직 (15명 이하), 비영리 기관	조직을 안전하게 운영하기 위한 최소한의 보안 솔루션
Step 2	중소기업	중소 규모의 조직에서 효과적인 보안 체계를 갖추기 위한 보안 솔루션
Step 3	대기업	대규모 조직에서 관리 및 통제를 효율적으로 하기 위한 보안 솔루션
Step 4	기밀정보를 다루는 주요 조직	군사, 주요 정부기관, 핵심 사업부 등 고도의 보안 수준을 요구하는 조직을 위한 보안 솔루션

5.2. 보안 솔루션 도입 시 고려사항

보안 솔루션을 도입하기 위해 어떤 점을 고려해야 하는가? 앞서 단계별로 보안 솔루션을 분류해 보았듯이 독립적인 제품 하나로 다양한 보안위협에 효율적으로 대응하기란 무척 어렵다. 전반적인 보안정책을 중심으로 승인 통제 메커니즘, 평가 및 확인, 호환성 및 상호 운용성을 모두 고려할 수 있는 포괄적이고 통합된 보안 솔루션을 요구하고 있다.

이상적인 솔루션 선정을 위해서는 다음과 같은 계획을 검토해야 한다.

1. 장기적인 보안 정책 로드맵 작성
2. 보안목표 수립
3. 핵심 자산 정의
4. 주요 자산을 위협하는 위험 정의
5. 수용 가능한 위험수준(Acceptable Risk Level) 선정
6. 구현하고자 하는 보안목표와 현 수준 차이 분석
7. 정량적/정성적 분석을 통한 ROI(Return On Investment) 산정(비용 및 시간 단축 측면)
8. 경쟁제품 성능비교 테스트(BMT)

9. 도입 후 솔루션 전담 관리
10. 도입한 보안 솔루션 유지보수 및 향후계획

정보보호 제품의 경우 솔루션 도입 전후의 투자 대 비용효과(ROI)를 정량적으로 산정하기가 어려운 면이 있다. 이럴 때에는 주로 비용 및 시간단축 측면에서 Man/Month로 계산한다면, 보다 현실적인 기대효과 분석을 할 수 있을 것이다. 일반적으로 신속한 의사결정이 요구되거나 도입을 위한 오버헤드를 적정수준으로 유지하기 위해 도입 시 모든 프로세스를 따라가지 못하는 경우가 많이 있는데, 그럴 경우라도 간단하게 다음과 같은 점은 꼭 인지하고 활용할 수 있도록 한다.

1. 피해가 예상되는 시스템은 무엇인가?
2. 보안 솔루션 부재로 인한 손실은 어느 정도인가?
3. 어떤 보안 솔루션을 얼마만큼 도입할 경우 효과를 극대화할 수 있는가?(플랫폼 비용, 네트워크 규모, 아키텍쳐, 위치, 기존 장비와 호환성)
4. 보안 솔루션을 지속적으로 운영하고 관리할 수 있는가?

5.3. 보안 솔루션 BMT

▌BMT 정의와 목적

흔히 BMT라고 부르는 벤치마킹(Benchmarking)이란 서로 다른 칩셋이나 아키텍쳐로 구성된 시스템으로 실제 작업수행을 통해 하드웨어나 소프트웨어의 성능을 측정하고 비교하는 평가방법을 말한다. 하드웨어 장비나 소프트웨어 제품을 구매하기 전 객관성을 확보하고 조직에 최적화된 솔루션을 찾으려는 데 그 목적을 두고 있다.

▌국내 BMT 한계점

많은 비용이 소요되는 테스트 장비와 전문인력 보유, 소프트웨어와 하드웨어 등이 종합적으로 고려되어야 하는 BMT는 그 수행이 쉽지 않으며, 국내에는 객관성과 공정

성을 갖춘 BMT 수행만을 위한 제3의 전문 공인기관이 없는 실정이다. 따라서 공급업체나 발주자가 자체적으로 실시하는 BMT의 경우 다음과 같은 한계점을 가질 수 있다.

첫째, 공급업체에게 의뢰하는 경우 대부분 공급업체가 제시하는 BMT 스펙에서 최상의 성능을 내기에 유리한 환경에서 테스트가 이루어질 수도 있으며 이는 실제 환경과 차이가 있을 수 있음을 인지해야 한다.

둘째, 대다수 BMT는 발생하는 비용을 공급업체에서 일방적으로 부담하고 있으므로 발주자의 적극적인 협조가 없이는 실제 환경에서 신뢰할 수 있는 결과를 얻을 수 없다.

셋째, 발주자는 BMT 결과에 대해 공급업체간의 마찰과 이의제기 문제로 인해 결과를 비공개하고 있어 자칫 잘못하면 공식적인 절차를 위한 형식적인 BMT에 그칠 수 있다.

위와 같은 문제점을 해결하기 위해서 최선의 방법은 투명한 BMT를 진행하기 위한 공인기관을 만들어 추진하고 그 결과를 공개하는 절차를 마련하여 공급업체의 솔루션을 보완하고 불필요한 BMT를 줄일 수 있도록 해야 할 것이다.

▮ 보안 솔루션 선정과 BMT 진행방법

일단, 조직에서 BMT의 한계점을 인지하고 필요한 보안 솔루션 항목을 선정했다면, 다양한 경쟁제품들 중 한 제품을 선택하기 위한 가장 간편한 방법은 국가기관(국가정보원, KISA 등)이나 국제기관(ISO CC 등)으로부터 인증을 받은 제품을 우선적으로 고려하는 것이다. 여기에 벤치마킹을 전문적으로 대행하는 해외기관에 검증을 의뢰하거나 테스트가 완료된 외부기관 결과를 활용할 수도 있으며, 국제적으로 진행되고 있는 보안이슈 프로젝트를 참고해 진행할 수도 있다. 예를 들어 최근 이슈가 되고 있는 웹 애플리케이션에 대한 보안은 오픈소스 진영에서 진행하고 있는 OWASP 프로젝트(Open Web Application Security Project)나 웹 방화벽 평가기준을 제공하는 Webappsec(Web Application Security Consortium)과 같은 사이트를 참조하여 BMT를 진행하는 것도 좋은 방안이 될 것이다. 또 대표적인 제3의 전문 검증기관으로 톨리그룹(The Tolly Group)이 있다. 보안 솔루션마다 다양한 형태의 BMT 시나리오를 수립하여 진행할 수 있으나, 여기에서는 솔루션 업체에서 진행함을 전제로 간략하게 일반적인 절차와 고려해야 할 사항을 짚어보기로 하겠다.

I. 개요
i. 목적 ii. 선정배경 iii. 범위 및 한계 iv. 해당 보안 솔루션 동작 구조파악
II. BMT 대상 및 벤더선정
i . BMT 벤더 선정 : 국내 솔루션, 해외 솔루션, 해외 솔루션 국내총판 등 ii. 보안 솔루션에 관한 정보제공을 위한 상호 미팅 iii. 공급업체의 BMT 준비를 위한 진행정보 제공 및 진행 협의 • 테스트 개요, BMT 환경, 각 항목별 가중치 등 • 일정, 장소, 참여인원, 예상소요시간 등 협의
III. 테스트 항목 선정 및 구체적인 시나리오 작성
※ 보안정책에 따라 조직이 요구하는 중요도 순으로 가중치를 적용할 것 i. 기능면 • 각 보안 솔루션에 따른 충족해야 할 기능을 세부평가항목으로 선정할 것 • 필요시 대분류, 중분류, 소분류로 나누어 구체적인 시나리오를 작성할 것. ii. 관리면 • 보안솔루션 운영시 GUI에 대한 편의성/유연성/확장성을 고려하여 평가항목을 작성할 것 • 로그관리, 백업 및 복구 관리, 통보 및 리포팅 iii. 성능 및 안정성 • 네트워크 규모에 따른 성능과 운영 안정성 • 물리적/논리적 위치 검토 iv. 기술지원 및 유지보수 v. 시나리오 작성 참고 기술 자료 기록 vi. BMT 환경 정의 및 구축, 테스팅
IV. BMT 진행
i. BMT 진행 가이드: 개요설명, BMT 환경에 따른 제품구성 ii. 진행시 유의사항 • 벤더별 BMT는 완전히 동일한 환경에서 진행할 것 • 특정 기능에 대하여 정확하고 공정한 룰을 적용하여 애매모호함이 없도록 할 것 • 보안 솔루션이 제공하는 기능에 조직이 요구하는 우선순위를 적용하되 공정을 기할 것 • 진행을 하면서 공급업체와 발주자 간 솔루션의 정상동작 여부를 상호 확인/인정할 것

▮ 보안 솔루션 BMT 시나리오 예제

다음은 BMT의 실제 사례로, 웹방화벽 BMT를 위한 테스트 항목을 선정하고 작성한 구체적인 시나리오다. 보안 솔루션마다 특징적인 요소가 있으므로, 이를 고려해 벤

치마킹을 진행해야 한다. 여기에서는 웹방화벽 구매 시 적용할 수 있는 BMT 시나리오를 제시해 보기로 하겠다.

A. 개 요

1. 일 정 : OOOO년 OO월 O일 O시
2. 장 소 : OOOO센터
3. 참가인원 (총 O명) : [A사] OOO 과장 외 O 명, [B사] OOO 대리 외 O명
4. 환 경 : Windows 2000 Server / IIS 5.0 / MS SQL Server 2000 / ASP
5. **시나리오 상세정보**

5.1 기능면 :항목별 가중치 부여
- Injection Flaw (SQL Injection 등)
- XSS (Cross Site Scripting)
- 데이터 절취
- 서비스 거부공격 (DoS)
- 불필요한 파일 노출
- 시스템 정보노출차단 (에러페이지 노출차단)
- 웹서버 구성 취약점 방어
- 인증 취약점 (Session 변조)
- 파일 다운로드
- 파일 업로드

5.2 관리면
- 편의성, 유연성, 확장성
- 통보 및 리포팅
- 운영관리
- 로그관리, 백업 및 복구관리

5.3 성능 및 안정성
- Response Time
- 장애 발생시 서비스 영향도

5.4 기술지원 및 유지보수

6. **진행정보**

6.1 기능 : 취약한 웹사이트에서 취약성 확인 후 방어할 수 있는지 확인
로그를 확인하고, 어떤 형식으로 동작하는지 확인
6.2 관리 : 실제 웹사이트에 도입하여 운영시 고려해야 할 사항 검토
6.3 성능 : 웹방화벽(WAF) 설치 전후의 Throughtput 비교
6.4 BMT 진행 당일 기능 평가를 위한 구성 가이드에 따라 적절한 설정 후 테스팅
6.5 각 평가항목별 가중치 부여, 최종점수 산출 후 적합한 제품 선정

B. 기능면 테스트 항목 정의 (시나리오)

번호	OWASP TOP 10	평가항목 (공통)		가중치	제품평가 점수		제품평가 의견		비고
		대분류	중분류		A사	B사	A사	B사	
1	N/A	웹서버 취약점 방어	디렉토리 리스팅 차단	0 %					
2	N/A		웹서버 옵션 차단						
3	N/A		기본 디렉토리 접근						
4	A4	불필요한 파일 노출	주요정보차단1	0 %					
5	A4		주요정보차단2						
6	A1	XSS	URL상 차단	0 %					
7	A1		Pattern1						
8	A1		Pattern2						
9	A2	Injection Flaw	String SQL Injection	0 %					
10	A2		SQL Injection without '						
11	A2		일반 SQL Injection						
12	A2		히든필드 변조						
13	A2		SQL Injection						
14	A3	파일업로드	실행가능파일 업로드	0 %					
16	A7	인증취약점	쿠키변조 공격 차단	0 %					
17	A7		Session 변조						
18	A8	파일 다운로드	상대경로 조작차단	0 %					
합 계				100%					

- 오탐일 경우 감점요인
- XSS 테스팅시 인코딩된 공격코드를 막지 못하면 실패한 것으로 처리
- 쿠키와 세션 변조 차단방식에 대한 설명 필요
- 각 기능 테스트 후 웹서버 로그와 장비에서 적절하게 방어하였는지 확인
- 각 평가항목은 OWASP Top10 기능에 대응

C. 운영관리

보안 솔루션을 도입 후 운영 시 필요한 모든 항목을 고려하여 작성하는 것이 좋다.

분류	가중치	평가항목	A사	B사	비고
로그 관리	0 %	Log File Format의 사용자 정의 수준을 지원하는가?			
		콘솔에서 알려진 파일 포맷으로 저장하여 쉽게 가공할 수 있는가?			
		Log 데이터는 주기적으로 서버와 동기화하는가?			
백업 복구 관리	0 %	백업내용을 찾을 경우 빠른 검색기능을 제공하는가?			
		기존의 룰을 실수로 삭제하였을 경우 빠른 복구가 가능한가?			
		지원하는 DB는?			
통보 리포팅	0 %	이벤트 필터링 기능을 제공하는가?			
		Signature / Pattern DB 업데이트 주기는?			
		리포트 포맷은 어떤 것을 지원하는가?			
		리포팅시 적절한 그래프를 수반하는가?			
		DoS 공격시 자체적으로 공격자 주소를 차단할 수 있는가?			
		공격이나 위험도에 따라 단계별로 공격차단이 가능한가?			
		침입탐지시 설정된 보안정책과 연관성을 제시하는가?			
		자동으로 주기적 리포팅 가능한가?			
편의성 유연성 확장성	0 %	특정 룰을 일괄적으로 등록할 수 있는가?			
		초기 전체 디렉토리와 파일을 수집할 수 있는가?			
		정책 등록시 정규식을 지원하는가?			
		디렉토리별 세부정책 설정이 가능한가?			
		웹기반의 관리콘솔을 제공하는가?			
		다수 콘솔을 중앙집중 제어할 수 있는가?			
운영 관리	0 %	URL 업데이트 또는 정책 수정 변경이 실시간 가능한가?			
		사용자 콘솔 접근에 대한 기록을 제공하는가?			
		정책 설정 변경시 바로 적용되는가?			
		미사용 URL에 대한 자동삭제 기능을 지원하는가?			
		보안정책의 만료기간을 설정할 수 있는가?			
		특정 확장자를 일괄적용/차단할 수 있는가?			
		특정 정책을 특정 디렉토리 또는 파일에만 적용할 수 있는가?			
		외국어를 지원하는가?			
		특정 IP로부터의 공격을 Bypass할 수 있는가?			
		특정 공격 패턴을 예외처리할 수 있는가?			
		정책변경시 기존 세션이 끊어지는 경우가 있는가?			
		에러페이지를 작성하여 운영할 수 있는가?			
		ESM 등 통합보안 솔루션을 위한 외부 로그전송을 지원하는가?			
합 계					

D. 성능 및 안정성

- 실트래픽 생성기(Real Traffic Generator)를 사용해 유해 트래픽과 정상 트래픽을 동시에 발생시켜 웹방화벽의 기능이 정상적으로 동작하는지 테스트
- 동시 세션수 OO으로 트래픽을 발생시켜 웹방화벽 설치 전후 응답속도 측정
- 측정시 가중치는 가용성을 우선으로 함
- 실제 트래픽은 웹방화벽을 적용시킬 네트워크 전단 평균 트래픽을 사용한 안전성 검증

E. 기술지원 및 유지보수

- 웹방화벽 문제 발생시 응급조치 지원
- 향후 웹방화벽 내 악성코드 패턴 업데이트 유지보수 지원사항

F. 참고 기술 자료

〈2007 Released OWASP TOP 10〉

A1 – Cross Site Scripting (XSS)
A2 – Injection Flaws
A3 – Malicious File Execution
A4 – Insecure Direct Object Reference
A5 – Cross Site Request Forgery (CSRF)
A6 – Information Leakage and Improper Error Handling.
A7 – Broken Authentication and Session Management
A8 – Insecure Cryptographic Storage
A9 – Insecure Communications
A10 – Failure to Restrict URL Access

〈Detection Techniques〉

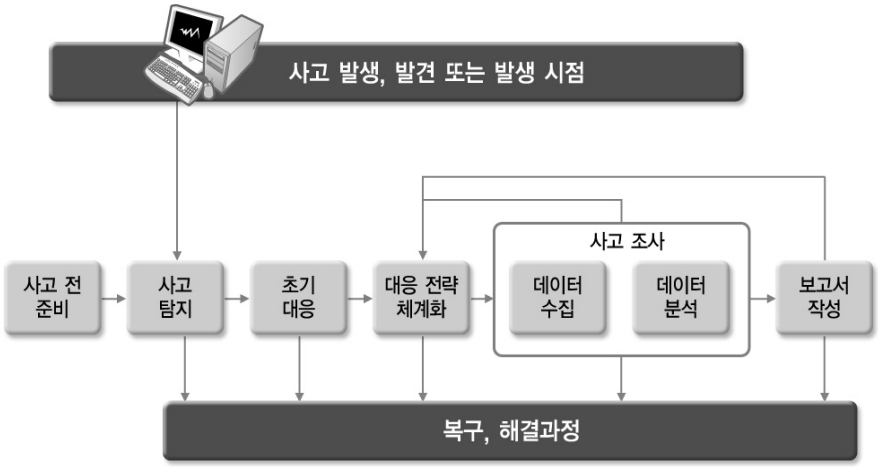
- URL-Decoding
- Null Byte string Termination
- Self-Referencing paths (./ or encoded)
- Path-back Refereces (../ or encoded)
- Mixed Case
- Excessive use of white space
- Comment removal
- Conversion of backslash characters into forward slash characters
- Converstion of IIS-specific Unicode encoding
- Decode HTML entries (c, $#xAA;)
- Escaped Characters (₩t, ₩001, ₩xAA, uAABB)

6 보안사고 대응

침해사고에는 바이러스, 트로이잔, 웜, 백도어, 악성코드 등의 공격을 비롯해 비인가된 시스템 접근 및 파일 접근, 네트워크 정보 수집을 포함한 비인가된 네트워크 정보접근, 네트워크 서비스의 취약점을 이용하여 서비스를 무단 이용하는 비인가된 서비스 이용, 네트워크 및 시스템의 정상적인 서비스를 마비 또는 파괴시키는 서비스 방해 등 다양한 종류들이 존재하고 있다. 최근 침해사고는 지능화·자동화된 공격기법이 늘어나고 있으며 다음과 같은 특징을 가지고 있다.

- 대규모(동시에 다수의 서버를 공격)
- 분산화(다수의 서버에서 목표 시스템을 공격)
- 대중화(해킹 관련 정보의 손쉬운 획득)
- 범죄적 성향(금전적 이익, 산업정보 침탈, 정치적 목적)

이러한 공격들은 복잡하고, 다양한 기술을 이용하여 시도되고 있어, 우수한 보안 기술을 채택하여 침해사고 발생을 억제할 필요가 있으며, 침해사고가 발생한 경우에도 이를 철저히 조사하여 향후 동일한 사고가 발생되지 않도록 조치를 취해야 한다. 아래 그림은



〈그림 4-6-1-1〉 사고 대응 7단계

단계별 침해 사고 대응 절차를 나타내고 있다. 여기서 제시된 절차는 7가지 대응 요소로 나뉜다.

- 사고 전 준비 과정 : 사고가 발생하기 전 침해사고대응팀과 조직적인 대응을 준비
- 사고 탐지 : 정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해 사고의 식별
- 초기 대응 : 초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응팀 신고 및 소집, 침해사고 관련 부서에 통지
- 대응 전략 체계화 : 최적의 전략을 결정하고 관리자 승인을 획득. 초기 조사결과를 참고해 소송이 필요한 사항인지를 결정하여 사고 조사과정 시 수사기관 공조 여부를 판단
- 사고 조사 : 데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정
- 보고서 작성 : 의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서를 작성
- 해결 : 차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획수립 등을 결정

6.1. 사고 전 준비과정

사고 전 준비 과정에서는 침해사고대응팀이 사고 현장에 도착해서 빠르고 정확하게 사고 대응을 실시할 수 있도록, 관리자와 긴밀한 협조관계를 유지하고 각 직책별 행동 방안을 구축해야 한다. 이와 더불어 사고 대응을 위한 기술 개발, 도구의 준비, 네트워크와 시스템의 사전 조치 등을 취하여야 한다.

- 사고 대응 체제의 준비(범 조직적인 전략과 대처방안)
  - 호스트 및 네트워크 기반 보안 측정 수행
  - 최종 사용자 교육 훈련

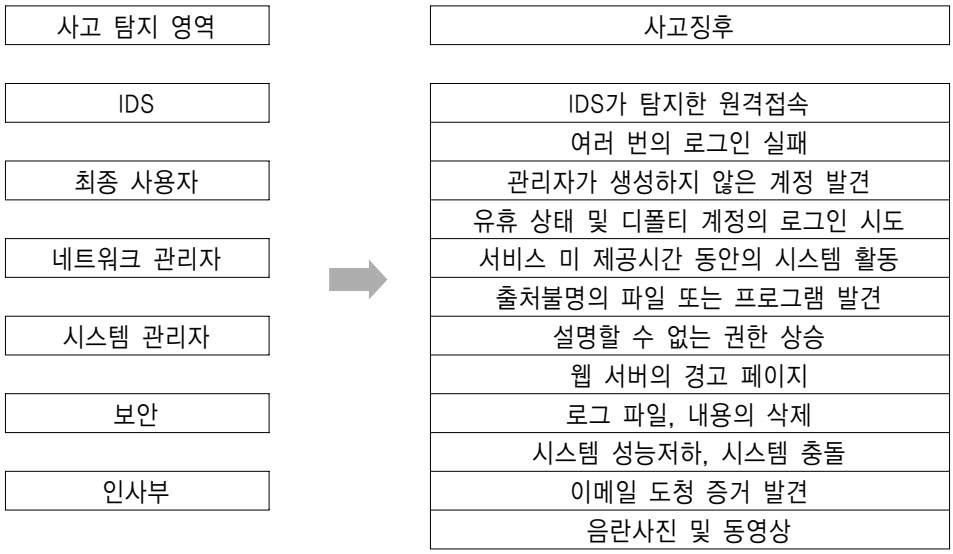
- 침입탐지 시스템 설치
- 강력한 접근 통제 실시
- 적절한 취약점 평가 실시
- 규칙적인 백업 수행
- 침해사고 대응팀과의 비상 연락망 구축

• 침해사고대응팀의 준비

- 사고 조사를 위한 도구(H/W, S/W) 구비
- 사고 조사를 위한 문서양식 정형화
- 대응 전략 수행을 위한 적절한 정책과 운용 과정 수립
- 간부, 직원들에 대한 교육 훈련 실시

6.2. 사고탐지

만약 효과적으로 사고를 탐지할 수 없다면 사고 대응을 성공적으로 수행할 수 없다. 사고 탐지와 관련된 영역과 징후는 아래 그림과 같다.



〈그림 4-6-1-2〉 사고탐지 영역과 징후

대부분의 조직에서는 다음 세 가지 방법 중에 하나를 이용하여 탐지된 사고를 보고하게 된다.

- 직속상관에게 보고
- 전산 지원실에 신고
- 정보보호 부서에 의해 관리되는 사고 핫라인으로 신고

어떤 식으로 사고가 보고될지라도, 중요한 것은 최초 탐지하게 된 경위와 인지된 상황을 빠짐없이 보고하는 것이다. 이때 적절한 요소들을 기록하고, 대응 절차를 단계별로 수행하기 위해 초기 대응 점검표를 이용하는 것이 좋다. 초기 대응 점검표는 사고가 탐지된 이후에 확인해야 할 세부항목들을 기술하고 있다. 초기 대응 점검표 구성에 중요한 요소는 다음과 같다.

- 현재 시간과 날짜
- 사고보고 내용과 출처
- 사건 특성
- 사건이 일어난 일시
- 관련된 하드웨어, 소프트웨어의 목록
- 사고 탐지 및 사고 발생 관련자의 네트워크 연결 지점

초기 대응 점검표가 완전히 작성된 이후 침해사고대응팀이 활동을 시작하여야 정확하고 신속한 대응이 가능하다. 따라서 침해사고대응팀은 사고 관련자들과 면담을 하면서 초기 대응 점검표를 정확히 작성할 수 있어야 한다.

6.3. 초기 대응

초기 대응의 첫 단계는 전산 관리팀의 전문가가 조치를 수행하고, 침해사고대응팀이 도착한 이후에는 초기 조치 사항들을 인수인계하고, 이후의 조치는 침해사고대응팀에

맡기거나 함께 공조를 하게 된다. 원활한 인수인계 및 조치사항 검토를 위해 각 단계에서 수행되는 모든 행동들은 문서화를 통해 그 기록을 유지하는 것이 중요하다.

초기 대응 이후에는 관련 데이터를 수집하게 되는데, 이 과정에서는 다음과 같은 작업들이 포함된다.

- 사건의 기술적인 내용을 통찰할 수 있는 시스템 관리자와 면담
- 사건 분석을 위한 정황을 제공해 줄 수 있는 인원들과의 면담
- 침입 탐지 로그와 데이터 식별을 위한 네트워크 기반 로그의 분석
- 공격 경로와 수단을 알아내기 위한 네트워크 구조와 접근 통제 리스트의 분석

초기 대응 단계가 마무리되면 실제로 사고가 일어났는지(혹은 오탐인지), 침해된 시스템에 대한 적당한 대응책이 있는지, 사건의 유형은 무엇인지, 그리고 사고로 인한 잠재적인 업무 영향은 무엇인지 등을 알 수 있을 것이다. 이렇게 적절한 정보가 준비되면 이를 판단근거로 하여, 현재 사고를 어떻게 처리할 것인지를 결정(대응 전략 수립)할 수 있을 것이다.

6.4. 대응전략 수립

대응전략 수립 단계의 목표는 주어진 사건의 환경에서 가장 적절한 대응전략을 결정하는데 있다. 전략 수립 시에는 정책, 기술, 법, 업무 등 사고와 관련된 요인들을 전체적으로 고려해야 한다.

- 침해당한 컴퓨터가 얼마나 중요하고 위험한가?
- 침해당하거나 도난당한 정보가 얼마나 민감한 것인가?
- 사건이 외부에 알려졌는가?
- 직/간접적인 공격자는 누구인가?
- 공격자에 의해 침해된 비인가 접근의 수준은 어느 정도인가?
- 공격자의 수준은 어느 정도인가?

- 시스템과 사용자의 업무중단 시간은 어느 정도인가?
- 어느 정도의 경제적 피해가 있었는가?

공격 환경과 대응 능력을 고려하여, 다양한 대응 전략을 수립하여야 한다. 다음 표는 일반적인 상황을 가정하여 작성된 대응 전략과 가능한 결과이다.

〈표 4-6-4-1〉 사고 유형에 따른 대응 전략 수립의 예

사고	예	대응 전략	예상 결과
DoS 공격	TFN DDoS 공격	Flooding의 효과를 최소화 하기 위해 라우터 재설정	라우터 재설정으로 공격의 효과를 완화
비인가 사용	업무용 컴퓨터 오용	증거물의 포렌식 이미지 확보와 조사 용의자와 면담	범인 식별, 징계를 위한 증거 확보. 해당 직원의 직위나 과거 조직 정책의 위반 등을 고려하여 징계
파괴 행위	웹 사이트 손상	웹 사이트 모니터 온라인 상태로 조사 웹 사이트 복구	웹사이트의 복구 범인 식별을 위해 수사기관이 참여할 수 있음
정보의 도난	신용카드 도난 및 고객정보 유출	관련된 시스템의 이미지 확보. 도난 신고 법적 대응 준비	상세한 조사 시작. 수사 기관 참여 예상된 피해복구를 위한 민사 소송 얼마간 시스템의 오프라인 유지
컴퓨터 침입	Buffer Overflow 또는 IIS 공격을 통한 원격 접속	공격자의 활동 감시 비인가 접속 봉쇄 시스템의 보안 재설정 및 복구	침입에 사용된 취약점을 식별하고 수정 및 패치 시행 범인의 식별 유무를 결정

다음에 등장하는 기준들은 사고 대응에서 수사기관에 신고하여 법적인 대응을 할 것인지 아닌지를 결정할 때, 고려되어야 할 사항들이다.

- 사고의 비용이나 피해정도가 범죄 전문가를 초빙할만한가?
- 사법이나 형사 조치가 조직이 원한 만큼 결과를 이끌어 낼 것인가?(상대로부터 피해를 복구하거나 손해배상을 받을 수 있나?)
- 사고 원인 분석은 타당한가?

- 효과적인 수사에 도움이 되는 적절한 문서와 정리된 보고서를 가지고 있는가?
- 수사관이 효과적으로 행동할 수 있도록 준비될 수 있는가?
- 수사관들과 공조한 경험이 있거나 그 방법을 잘 알고 있는가?
- 사고 내용의 공개를 감수할 수 있는가?
- 데이터 수집 절차는 합법적인 행동이었는가?
- 법률 분쟁이 사업 수행에 어떻게 영향을 줄 것인가?

사건의 내용이 법적인 제제가 필요한 사항이 아니라 내부에서 처리해야 할 사항이라면, 직원 관리 차원에서 사원을 징계하고 해고하는 것이 일반적이다. 다음은 사원 인사 조치의 예이다.

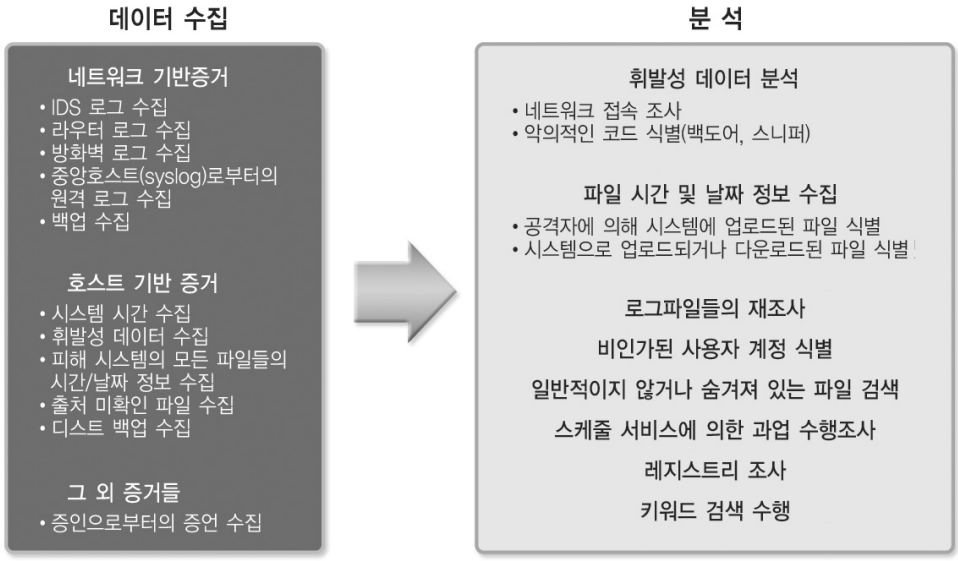
- 공식적인 징계 문서
- 해고
- 일정 기간 동안의 근신
- 업무 재분배
- 임시 봉급 삭감
- 행동들에 대한 공개적, 개인적인 사과
- 네트워크 및 웹 접근과 같은 권한의 박탈

6.5. 사고 조사

사고 조사는 '누가, 무엇을, 언제, 어디서, 어떻게 그리고 왜'와 같은 사항들을 결정하는 것이 필요하다. 이를 위해 사건 조사는 호스트 기반과 네트워크 기반 증거로 나누어 조사해야 한다. 사고 조사가 어떻게 진행하든 조사의 초점은 공격자에 의해서 일어난 사고를 수습하고 공격자를 색출하는 것에 맞추어질 것이다. 즉, 조사의 핵심은 누가 어떤 것에 손상을 입혔는가를 확인하는 것이다. 따라서 누가, 무엇을, 언제, 어

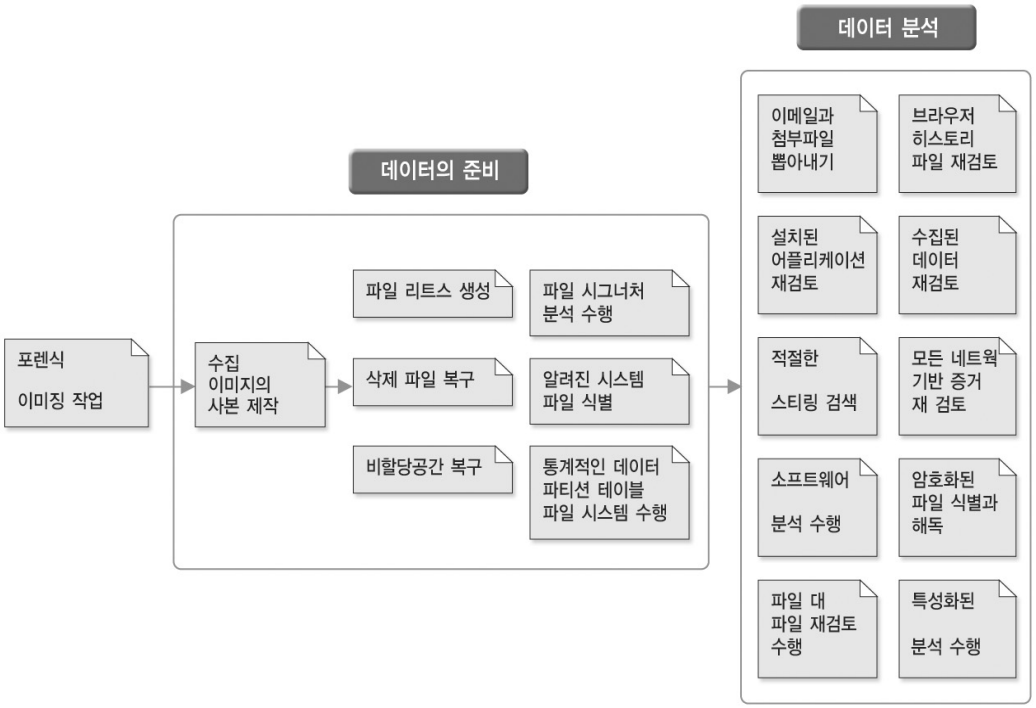
디서 그리고 어떤 정보가 사고와 관련된 것인지를 확인하기 위해 사고 조사과정은 데이터 수집과 자료 분석 단계로 나뉜다.

데이터 수집은 사건분석을 하는 동안 깊이 살펴보아야 할 범행들과 단서들의 수집 과정이다. 특히, 법적 소송을 염두해 둔다면, 증거가 무결성과 적법성을 유지하도록 디지털 데이터를 수집해야 하며, 엄청난 양의 데이터를 수집하고 보관해야 할 경우가 있다. 이런 요구사항들은 만족시키면서 기술적인 데이터를 획득하고 사고 분석을 하려면 컴퓨터 포렌식 기술이 필요하다.



〈그림 4-6-5-1〉 수집된 데이터의 분석 예

데이터 분석은 모든 수집된 정보의 전체적인 조사를 의미하며, 로그 파일, 시스템 설정 파일, 웹 브라우저 히스토리 파일, 이메일 메시지와 첨부파일, 설치된 어플리케이션 그리고, 그림 파일 등을 포함한다. 소프트웨어 분석, 시간/날짜 스탬프 분석, 키워드 검색, 그 외의 필요한 조사과정을 수행한다. 포렌식 조사는 또한 Low 레벨에서의 조사도 수행한다. 이 과정에 수행되는 각 요소들은 다음 그림에 나타나 있다.



〈그림 4-6-5-2〉 데이터의 분석 절차

6.6. 보고서 작성

보고서 작성은 가장 어렵고도 중요한 단계이다. 보고서를 읽게 되는 상급자 또는 소송 관련자들은 컴퓨터에 대한 기본지식이 부족한 경우가 많기 때문에, 누구나 알기 쉬운 형태로 작성되어야 한다. 데이터 획득, 보관, 분석 등의 과정을 육하원칙에 따라 명백하고 객관적으로 서술해야 한다. 또한 사건의 세부 사항을 정확하게 기술하고, 의사 결정자가 이해하기 쉽게 설명되어야 하며, 재판 과정에서 발생하게 될 논쟁에 대응할 수 있도록 치밀하게 작성되어야 한다.

6.7. 복구 및 해결과정

컴퓨터 보안사고 대응의 마지막 단계는 현재 발생한 사고로 인해 제2, 제3의 피해를 막고 재발을 방지하기 위한 조치들이 이루어져야 한다. 이를 위해 다음과 같은 조치들을 취해야 한다.

- 조직의 위험 우선순위 식별
- 사건의 본질을 기술 : 보안 사고의 원인과 호스트, 네트워크 복원시 필요한 조치
- 사건의 조치에 필요한 근원적이고 조직적인 원인 파악
- 침해 컴퓨터의 복구
- 네트워크, 호스트에 대해 밝혀진 취약점에 대한 조치(IDS, Access Control, Firewall)
- 시스템을 개선할 책임자 지명
- 시스템 개선이 이루어지고 있는지 추적
- 모든 복구 과정이나 대책의 유용성 검증
- 보안 정책 개선

7 사이버 침해사고·범죄 신고 및 조사절차

7.1 공공분야 사이버 침해사고 신고 및 조사절차

국내에서 발생하는 사이버 침해사고는 2005년 10월 국가정보원이 제정한 '국가사이버안전매뉴얼'에 근거, 民·官·軍 분야별로 초동대응 및 사고조사와 피해복구가 이루어진다. 특히, 공공기관의 경우 지난 2005년 1월 31일 제정된 '국가사이버안전관리규정'에 근거하여 각종 사이버 침해사고 발생 시 국가정보원 국가사이버안전센터로 지체

없이 신고하도록 되어 있다. 국가정보원은 관계 중앙행정기관에 사고복구 및 피해 확산방지를 위한 조치를 요청할 수 있으며, 필요시 범정부적 합동조사 및 복구지원팀을 구성하여 사고대응 업무를 수행한다.

▮ 침해사고 신고절차

침해사고가 발생한 기관의 장은 지체없이 사고의 일시·장소·사고내용 및 현재 취하고 있는 조치를 국가정보원장에게 통보하여야 한다. 다만, 국방분야의 경우에는 관련 내용을 국방부장관에게 통보하고 국방부장관은 국가안보에 필요하다고 판단되는 경우에는 관련내용을 국가정보원장에게 통보하여야 한다. 이와 함께 정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통신기반시설 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 국가정보원, 수사기관 또는 한국정보보호진흥원에 통지하여야 한다.

※ 국가사이버안전관리규정 12조 및 국가사이버안전매뉴얼 3장 참조

- 신고방법

  1) 공공분야의 경우, 국가사이버안전센터 홈페이지(www.ncsc.go.kr)를 방문하여 사이버 침해사고 신고를 하거나

  2) 전화 또는 전자우편, 팩스로 신고할 수 있으며 관련 신고양식은 국가사이버안전매뉴얼 부록6을 참조한다.
     - 전화 : 02-3432-0462(국번없이 111), 02-557-0716
     - 전자우편 : cert@ncsc.go.kr
     - 팩스 : 02-3432-0463

〈그림 4-7-1-1〉 공공분야 사이버침해사고 신고서식

3) 국방분야의 경우, 국군기무사령부 홈페이지(www.dsc.mil.kr)를 방문하거나 전화로 사이버 침해사고를 신고할 수 있다.

- 전화 : 02-731-3631(국번없이 1337)

〈그림 4-7-1-2〉 국방분야 사이버침해사고 신고서식

침해사고 조사절차

※ 국가사이버안전관리규정 13조 및 국가사이버안전매뉴얼 3장 참조

국가정보원장은 국가·공공기관의 사이버 침해사고 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고일 경우는 해당기관의 장이 자체적으로 조사할 수 있으며, 자체조사완료 결과를 사고대응조치 서식에 의거, 국가정보원장에게 통보하여야 한다.

또한, '심각' 수준의 사이버위협 경보가 발령된 경우나 범국가 차원의 대응이 필요하여 국가사이버안전전략회의 또는 대책회의 의장이 지시한 경우 범정부적 합동조사 및 복구지원팀을 구성·운영한다.

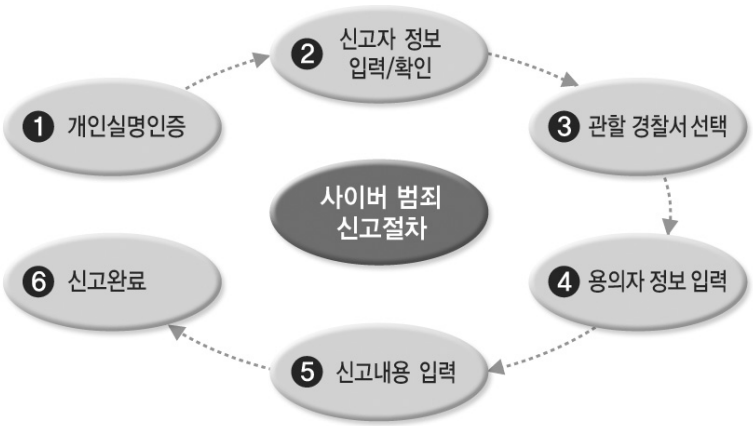
<table>
<tr><td colspan="4">기 본 정 보</td></tr>
<tr><td>기 관 명</td><td></td><td>부 서</td><td></td></tr>
<tr><td>성 명</td><td></td><td>직 위</td><td></td></tr>
<tr><td>전자우편</td><td colspan="3"></td></tr>
<tr><td>연 락 처</td><td colspan="3">전화 : H.P : Fax :</td></tr>
<tr><td colspan="4">사 고 내 용</td></tr>
<tr><td rowspan="2">사고 일시</td><td rowspan="2">년 월 일
시 분</td><td>피해
IP주소</td><td></td></tr>
<tr><td rowspan="2">운영체제</td><td>□윈도우 □유닉스 □네트워크장비</td></tr>
<tr><td>피해시스템
용 도</td><td>*사고신고시와 동일하게 작성</td><td>상세버전정보:</td></tr>
<tr><td>사고 유형</td><td>*사고신고시와 동일하게 작성</td><td>피해범위</td><td>OO 대
*피해시스템이 여러대인 경우 피해숫자 기입</td></tr>
<tr><td>사고 내용</td><td colspan="3"></td></tr>
<tr><td colspan="4">조 치 내 용 요 약</td></tr>
<tr><td>사고 원인</td><td colspan="3">*자체긴급대응반, 합동조사팀의 사고조사에 대한 내용요약작성</td></tr>
<tr><td>피해 현황</td><td colspan="3">*사고대응 조치전의 피해현황을 요약작성</td></tr>
<tr><td>사고 대응
조치사항</td><td colspan="3">*자체 긴급응반, 복구지원팀의 피해복구 조치에 대한 내용을 요약작성</td></tr>
<tr><td>피해복구결과</td><td colspan="3">*사고대응 조치 현황을 요약작성</td></tr>
<tr><td colspan="4">기 타</td></tr>
<tr><td colspan="4">*자세한 사항은 사고원인 · 피해현황 · 조치내역 · 향후개선대책 등을 망라하여 '사고처리결과보고서' 작성</td></tr>
</table>

〈그림 4-7-2-3〉 사이버침해사고 대응조치서식

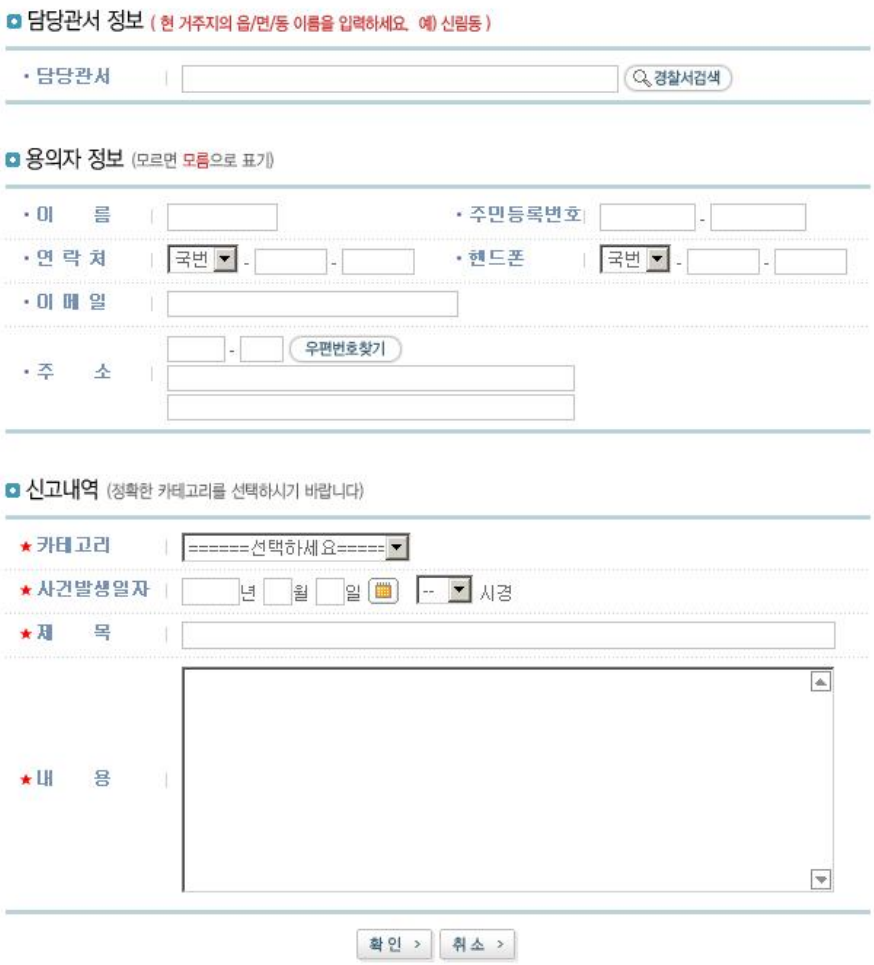
7.2 사이버 범죄 수사절차

경찰이 일반 범죄를 수사하듯 사이버 범죄에 대해서도 별도의 수사조직과 절차가 마련돼 있다. 해킹·바이러스 유포와 같은 사이버 테러형 범죄와 전자상거래를 이용한 사기, 개인정보 침해 등 일반 사이버 범죄에 대한 수사를 의뢰할 수 있으며, 전국 1,000여명(경찰청 사이버테러대응센터 16개, 지방경찰청 사이버수사대 235개 경찰서 수사팀)의 사이버캅 네탄(NATAN)이 이에 대한 업무를 수행하고 있다. 사이버 범죄와 관련된 수사 착수가 이뤄지게 되면, '피해자 상대 조사 → 피해자 시스템 증거 수집(시스템 관리자의 피해 시스템의 증거 훼손 금지) → 용의자 파악을 위한 추적수사 → 용의자 사용 네트워크 및 서버 등 위치 파악 → 법원의 영장에 의한 증거 수집' 등의 절차를 통해 수사가 진행된다.

- 사이버 범죄 신고 대상기관 : 국가기관, 공공기관, 교육기관, 금융기관, IT 관련 업체, 개인 등 모든 사이버 범죄 발생 기관



〈그림 4-7-2-1〉 사이버 범죄 신고절차



〈그림 4-7-2-2〉 사이버 범죄 신고양식

사이버 범죄가 착수되면 각 수사 담당자는 다음과 같은 원칙을 바탕으로 수사를 진행하게 된다.

적법절차의 준수

1) 수사 등에 필요한 한도 내에서 최소한의 증거 수집을 원칙으로 한다.

2) 형사소송법, 경찰관직무집행법 등의 법규 및 지침에 규정된 일반적인 원칙과 절차를 준수한다.

원본의 안전한 보존

1) 증거수집 시에는 반드시 쓰기방지장치를 이용하여 증거 원본에 대한 무결성을 유지한다.

2) 증거 원본은 이송 및 보관에 주의하여 손상을 방지한다.

증거의 무결성 확보

1) 증거 수집 시점에 수집된 디스크 또는 각각의 파일에 대해서 단방향 암호화 알고리즘으로 계산값(이하 해쉬값)을 확보한다.

2) 생성된 해쉬값을 출력 후 입회인의 서명 날인을 받는다.

3) 증거 원본에 대한 사본을 생성하고 이에 대한 해쉬값을 생성 후 이미 생성된 원본 해쉬값과 비교하여 무결성을 검증한다.

4) 증거분석은 원본 해쉬값과 동일한 해쉬값을 가진 사본을 이용하여 수행한다.

이와 함께, 수사 과정에서 가장 중요한 단계 중 하나인 디지털 증거수집 과정은 다음과 같은 절차에 따라 진행된다.

디지털 증거수집 절차

1) 사진촬영 및 현장 스케치를 수행한다.
   ① 컴퓨터등 대상물의 앞·뒷면 사진, 주변장치를 포함한 사진, 전원이 켜져 있는 경우는 모니터 화면 촬영
   ② 현장에 있는 수집 대상물의 위치를 상세히 스케치

2) 네트워크 정보 등 휘발성 증거를 수집한다.

3) 수집 대상물의 전원을 확인한다.
   ① 컴퓨터 등 대상물의 전원이 꺼져 있는 경우 그대로 수집
   ② 전원이 켜져 있는 경우, 정상적인 시스템 종료 절차를 수행하면 임시 데이터가 삭제되므로 이를 방지하기 위해서 컴퓨터의 경우 종료 절차 없이 전원플러그를 강제 분리(단, 서버는 정상 종료 절차 수행)

4) 본체 수집을 원칙으로 하되, 부득이한 경우 하드디스크만 분리하여 수집한다.
   ① BIOS의 메인 메뉴에서 시스템 시간과 날짜정보 확인
   ② BIOS 시간과 표준 시간 간의 오차를 확인 후 기록
   ③ 컴퓨터 본체에서 하드디스크를 안전하게 분리

5) 외장형 디스크, USB 메모리 등 기타 디지털 저장매체와 각종 소프트웨어, 주변장치, 케이블 등을 수집한다.

6) 증거물을 포장하고 상세정보를 기재하여 증거물에 부착한다.
   ① 하드디스크는 보호박스를 사용하여 개별 포장함이 원칙
   ② 컴퓨터 및 주변 장치 등에 대한 상세 정보를 기재하여 증거물에 부착
   ③ 상세정보의 내용은 사건번호, 수집자, 입회인, 수집일시, 장소, 물품, 제조번호 등이고, 하드디스크만 분리하여 수집하는 경우에는 추가로 BIOS 시간 오차를 기재

7) 압수증명서를 작성하여 입회인에게 교부하고, 입회인으로부터 압수확인서 및 압수증거물 목록에 서명 날인을 받는다.

8) 사용자 질의서를 작성한다.
   ※ 컴퓨터 사용자를 상대로 컴퓨터의 용도, 설치된 운영체계, 주로 사용하는 응용 프로그램명, 패스워드가 설정된 프로그램 명, 패스워드 정보 등을 질의 후 기재

한편, 사이버 범죄 신고는 사이버테러대응센터 홈페이지(http://www.netan.go.kr, 02-3939-112)을 통해 신청양식을 기입하면 접수가 진행되며, 각 민원 및 신고에 대한 수사 진행사항을 홈페이지를 통해 확인할 수 있다.

8 대외협력

앞서 1장의 국내 침해사고대응체계에서도 살펴본 바와 같이 국내에는 침해사고 예방 및 대응을 위해 다양한 기관들이 존재하고 있다. 국가정보원의 국가사이버안전센터,

대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 한국정보보호진흥원 인터넷침해사고대응지원센터 등 서비스 대상기관과 업무내용에 따라 다수의 기관이 존재하고 있으므로, 각 기업의 성격에 따라 이들 기관과 상호협력관계를 유지하고, 비상연락처를 확보할 필요가 있다.

〈표 4-8-1-1〉 국내 침해사고 관련기관 연락처

기관명	홈페이지	전화번호	이메일	비 고
국가정보원 사이버안전센터	http://www.ncsc.go.kr	국번없이 111	-	정부 및 공공기관 보안사고 접수·처리
대검찰청 인터넷범죄수사센터	http://icic.sppo.go.kr	02)3480-3600	icic@icic.sppo.go.kr	컴퓨터보안사고 수사
경찰청 사이버테러대응센터	http://www.netango.kr	02)3939-112	-	컴퓨터보안사고 수사
한국정보보호진흥원 인터넷침해사고 대응지원센터	http://www.krcert.or.kr	국번없이 118	cert@krcert.or.kr	민간 보안사고 접수·처리

민간 기업에서 침해사고 발생 시 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.

민간 기업을 비롯해 대학 등 국내 침해사고대응팀들간의 협의체인 CONCERT(한국침해사고대응팀협의회)는 "내 정보는 내가 지킨다"는 모토를 가지고 회원 간에 정보 및 기술 교류, 침해사고 공동 대응을 하고 있다.

또한, 금융, 통신과 같이 특정 분야에 속한 기업의 경우, 금융보안연구원, 금융ISAC, 통신정보공유분석협회 등 해당 분야에 특화된 보안 조직의 도움을 받는 것도 바람직 하다. 이외에도 기업에서 운영하고 있는 시스템, 네트워크의 장비업체 또는 유지보수업체 등과의 협력관계를 유지하여 해당 장비에 대한 장애 발생 시 신속하게 대응할 수 있도록 한다.

〈참 고 서 적〉

- 국가정보보호백서 / 국가정보원/정보통신부, 2007
- 리눅스 서버 기본 보안정책 Step by Step / Security proof, 2005
- 리눅스 서버 보안관리 실무 / 홍석범, 2005
- 리눅스 체크리스트 / SANS, www.sans.org/score/checklists/linuxchecklist.doc
- 민간사이버안전매뉴얼 / KISA, 2004
- 보안정책수립 체크리스트 / 정보보호21c
- 시스코 보안 솔루션 선택 가이드 / Cisco Homepage
- Apache 웹서버 보안 관리 / 정현철, 2002
- 침해사고대응팀 구축 운영 지침서, 한국정보보호진흥원/한국침해사고대응팀협의회, 2004
- 침해사고 분석 절차 가이드, 한국정보보호진흥원, 2006.
- Guide to Securing Microsoft Windows XP / NSA (2007.5)
- Hacking Exposed 4th Ed. / McGraw Hill (2003.8)
- Linux Security Administrator's Guide / Dave Wreski (1998.8)
- NIST Security Configuration Checklists Repository, 2007
- Oracle Database Hardening / Oracle (2007.1)
  www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- OWASP 2007 Top 10 (Open Web Application Security Project), www.owasp.org
- Web Application Security Consortium, www.webappsec.org

부 록

기업 정보보호수준

자가측정 서비스 따라해 보기

[부 록]

우리 회사, 사이버 위협으로부터 얼마나 안전한가?

"기업 정보보호수준 자가측정 서비스" 를 활용한 자기측정 방법

1 정보보호 첫걸음은 손쉬운 자가진단으로

- 김대리의 PC에는 올해 가을 런칭 예정인 신규 서비스의 기획문서가 저장되어있습니다.
- 우리 회사 온라인 게임서비스는 고객에게 24시간, 일주일 내내 제공되고 있습니다.
- 홈페이지에 가입한 회원의 주민등록번호는 사내 DB서버/혹은 PC에 저장되어 있습니다.

위와 같은 사례는 여러분의 기업에서도 흔히 찾아 볼 수 있는 모습일 겁니다.

요즘 많은 기업이 PC, 서버, 네트워크 등을 통한 IT 업무환경을 갖추고 있으며, 문서작성과 인터넷 검색 등의 개인업무에서부터 고객관리와 회계처리 등의 기업 주요업무에 이르기까지 기업의 IT 활용범위는 점차 늘어나고 있습니다. 하지만 이렇게 발전된 IT 업무환경을 구축한 많은 기업들이 정보시스템 침해사고의 위험에 노출되어 있다는 점은 기업에서 결코 간과해서는 안 될 부분입니다.

정보시스템 침해사고는, 바이러스 감염에 의한 PC 속도 저하, 스파이웨어 감염 등과 같이 상대적으로 많이 알려지고 흔히 발생하는 보안사고에서부터, 퇴사한 직원에 의한 기밀정보 유출, 홈페이지를 통한 주민등록번호 노출처럼 기업 비즈니스에 심각한 영향을 미칠 것으로 예상되는 심각한 사고들까지 다양한 형태로 나타납니다. 특히 이러한 정보보호 침해사고는, 피해를 당한 기업이 어떻게 느끼는가를 떠나 기업 존폐를 결정하는 상상 이상의 결과를 초래할 수 있습니다.

여러분의 회사는 이러한 위험으로부터 얼마나 안전하십니까? 우리 신체가 작게는 감기, 크게는 암 등의 질병으로부터의 예방을 위해 '주기적인 건강검진'이 필요한 것처

럼, 우리 회사에도 웜·바이러스, 해킹 등의 보안사고로부터의 예방을 위해 '주기적인 보안검진'이 필요합니다. 한국정보보호진흥원(KISA)에서는 기업의 보안수준을 손쉽고 간단하게 자가진단할 수 있는 '기업 정보보호수준 자가측정 서비스'(이하 자가측정 서비스)를 온라인으로 제공하고 있습니다. 이 서비스는 KISA 홈페이지(www.kisa.or.kr)에 로그인을 한 후 정보보호 체크리스트로 구성된 객관식 문답을 체크하는 방식으로, 크게 '정보화 규모판단 → 의존도 판단 → 정보보호 수준측정' 3단계로 이루어져 있습니다.

정보보호수준 자가측정 절차

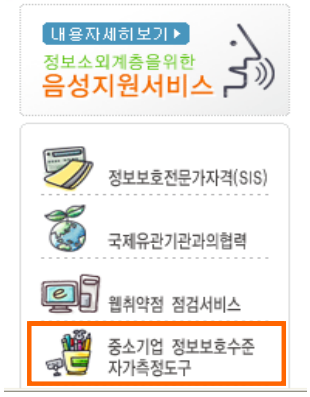
자가측정 서비스는 정보시스템에 대해 잘 알고 있는 CEO나 정보시스템 담당자가 측정하기를 권고하며, 처음 사용자의 경우 약 30분 정도의 시간이 소요됩니다. 이제부터, 자가측정 서비스를 활용한 보안수준 측정방법을 단계별로 알아보겠습니다.

※ 아래의 내용은 KISA에서 가상의 기업을 설정하여 자가측정서비스를 실시한 것으로 각 기업의 응답결과에 따라 상이한 결과가 나올 수 있습니다.

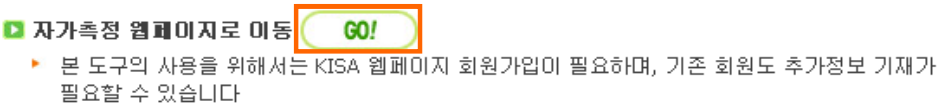
2 자가측정 서비스 찾아가기

자가측정 서비스는 KISA 홈페이지를 통하여 무료로 제공되며, 아래의 경로로 찾을 수 있습니다.

① KISA 홈페이지에 접속하여 왼쪽의 링크 메뉴 중 '중소기업 정보보호수준 자가측정 도구'를 클릭합니다. 클릭으로 이동하는 페이지는 자가측정 서비스의 개요 및 절차에 대하여 설명이 제공됩니다.

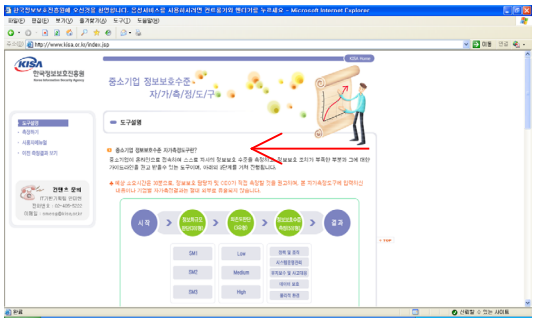


② 이동한 페이지의 하단에 있는 '자가측정 웹페이지로 이동 GO!'를 클릭합니다.



③ KISA 홈페이지 회원 로그인을 할 사용자는 '중소기업 정보보호수준 자가측정도구' 웹페이지로, 회원로그인을 하지 않은 사용자는 "회원로그인" 페이지로 이동하게 됩니다.

기존 회원은 아이디와 비밀번호를 입력한 후 로그인(LOGIN)을, 미회원은 '회원가입'을 클릭하여 가입화면으로 이동합니다.



[회원 로그인 한 사용자가 보는 화면]

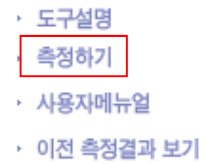
[회원 로그인을 하지 않은 사용자가 보는 화면]

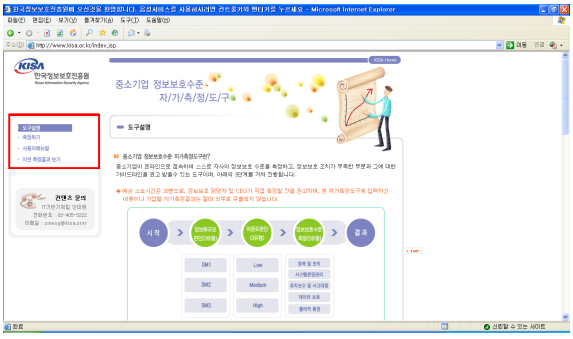
다만 자가측정 서비스는 기업 사용자를 위하여 제공되는 무료서비스이기 때문에 회원가입 시 아래의 체크박스에 클릭한 후, 사용자 소속단체의 정보를 기입하여야 합니다.

☑ **정보보호산업지원센터(LAB실, 회의실, 교육실), 중소기업 정보보호수준 자가측정도구를 이용하실분은**
왼쪽을 체크하여 주시고 아래 소속단체 정보를 반드시 입력하여 주시기 바랍니다.

3 자가측정 서비스 시작하기

④ "중소기업 정보보호수준 자가측정 웹페이지"의 왼쪽 메뉴에서 〔측정하기〕를 클릭하여 자가측정을 시작합니다.





[중소기업 정보보호수준 자가측정 웹페이지 화면]

구성도 측정

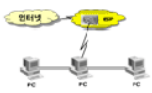
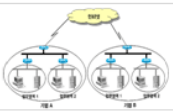
⑤ 측정하기의 첫 단계는 [구성도 측정]입니다. 본 단계에서는 10개의 설문항목을 통하여 기업의 정보화 유형을 3개로 분류합니다.

[구성도 측정 화면]

※ 정보화 유형이란?

정보화 유형은 기업의 IT환경에 에 따라 3가지(SM1, SM2, SM3)로 분류되며, 일반적으로 정보화 유형이 SM(Small & Medium)1에서 SM3로 이동하게 되면 지켜야 할 정보자산의 규모가 커지게 되고, 그에 따라 요구되는 정보보호 수준도 높아지게 됩니다.

› 유형별 정의

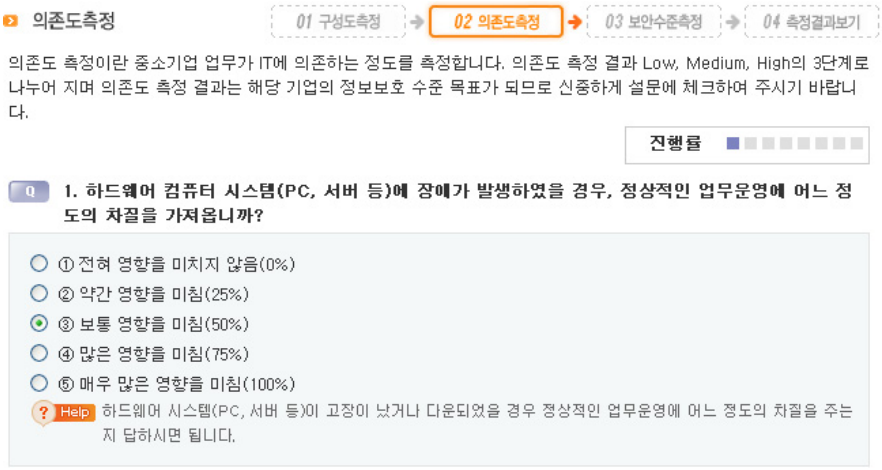
정보화유형	유형별정의	정보화규모
SM1	고객관리, 사내업무 등을 단순 PC를 중심으로 처리하는 기업	
SM2	인사, 재무, 공정관리 등 업무를 내부 네트워크 기반으로 처리하는 기업	
SM3	B2B, B2C 등 외부 네트워크와 연결하여 전자거래 하는 기업	

⑥ 구성도 측정을 마치면, 기업의 정보화 유형결과를 화면에서 확인할 수 있습니다. 아래의 경우, 측정 기업은 인사, 재무, 공장관리 등의 단위 업무가 내부 내부워크 기반으로 처리되는 SM2 유형의 기업임을 확인할 수 있습니다. "다음 단계로"를 클릭하여 [의존도 측정] 단계로 이동합니다.

[구성도 측정 결과화면]

의존도 측정

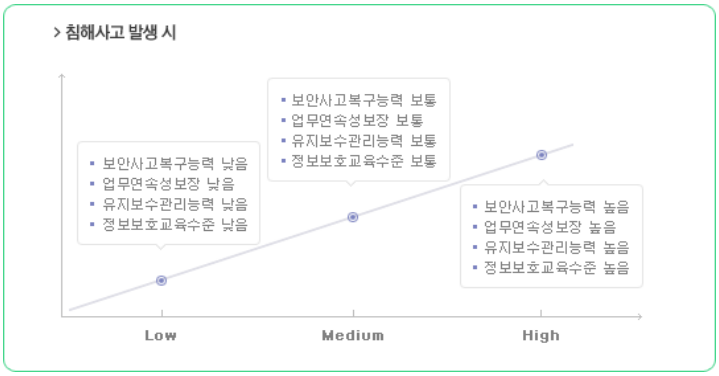
⑦ 두번째 분류는 [의존도 측정]입니다. 본 단계에서는 컴퓨터 시스템에 대한 의존도 분야 6개, 보안사고에 따른 의존도 분야 6개, 기업 구성요소에 대한 의존도 분야 5개(총 17개) 설문문항을 토대로 기업의 정보화 의존도를 3단계(Low, Medium, High)로 분류합니다.



[의존도 측정 화면]

※ 정보화 의존도란?

정보화 자산의 민감성, 정보보호 재난 발생 시 기업에 미치는 영향 등에 따라 기업의 정보화 의존도를 3가지(Low,Medium, High)로 분류합니다. 아래의 표는 침해사고 발생 시 요구되는 보안수준을 의미하며, 낮음·보통·높음은 상대적인 지표를 의미합니다.



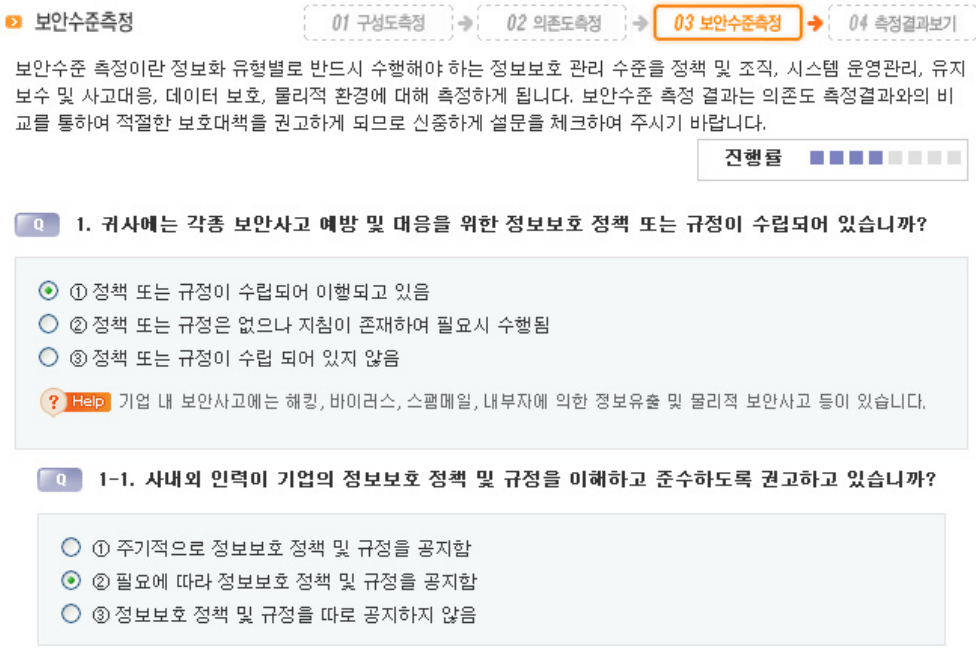
⑧ 의존도 측정을 마치면, 기업의 정보화 의존도 결과를 화면에서 확인할 수 있습니다. 아래의 경우, 측정 기업은 보안사고 발생시, 기업 비즈니스에 보통 수준의 영향을 미칠 수 있는, Medium에 속하는 기업임을 확인할 수 있습니다. 다음 단계인 [보안수준 측정]으로 넘어가기 위하여 '다음 단계로'를 클릭합니다.

※ 동일한 SM2의 정보화 유형에 속하는 기업일지라도, 정보화 의존도가 높은 기업일수록 보다 높은 정보보호 수준이 요구됩니다.

[의존도 측정 결과화면]

보안수준 측정-정책 및 조직

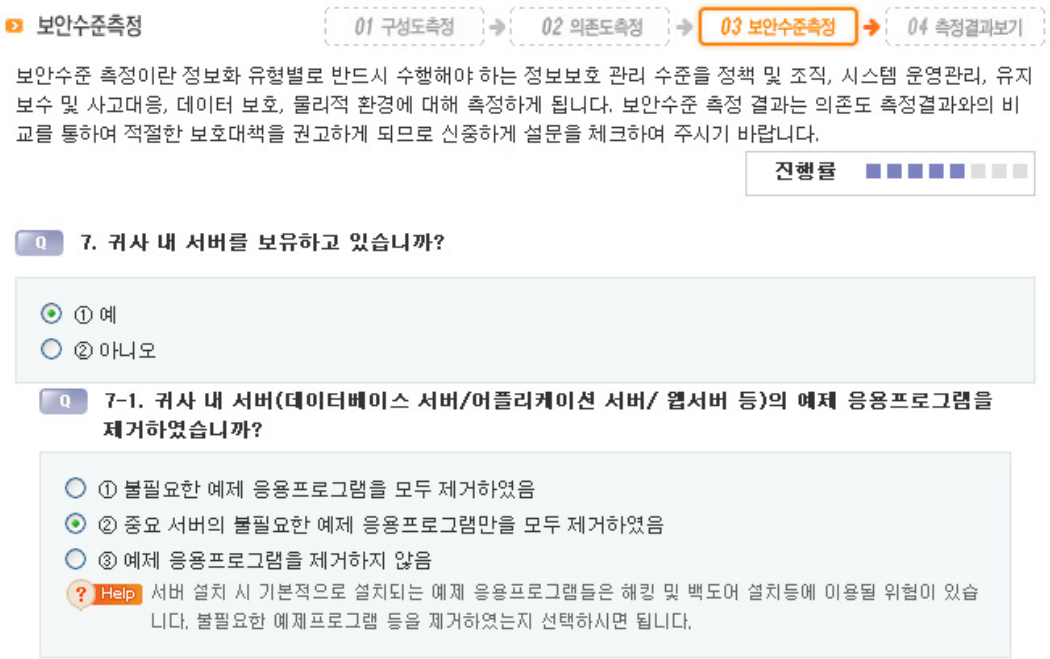
⑨ 자가측정 서비스의 세번째는 [보안수준 측정]입니다. [보안수준 측정]은 정책 및 조직, 시스템 운영관리, 유지보수 및 사고대응, 데이터 보호, 물리적 환경 등 총 5개 분야에 대하여 최대 28개 문항으로 이루어져 있으며, 정보화 유형에 따라 응답하는 문항은 변동됩니다. 첫번째 분야는 정책 및 조직 분야로 정보보호 정책 및 규정의 수립, 정보보호 조직, 자산분류, 아웃소싱 관리, 교육 및 훈련 등에 관한 보안수준을 측정합니다.



[정책 및 조직분야 측정 화면]

보안수준 측정-시스템 운영관리

⑩ 두번째 측정분야는 시스템 운영관리 분야로 PC 및 서버의 운영체제 업데이트, 사용자 권한설정, 공유폴더 관리, 계정 및 암호관리, 웹 브라우저 보안설정 등에 관한 보안수준을 측정합니다.



[시스템 운영관리 분야 측정 화면]

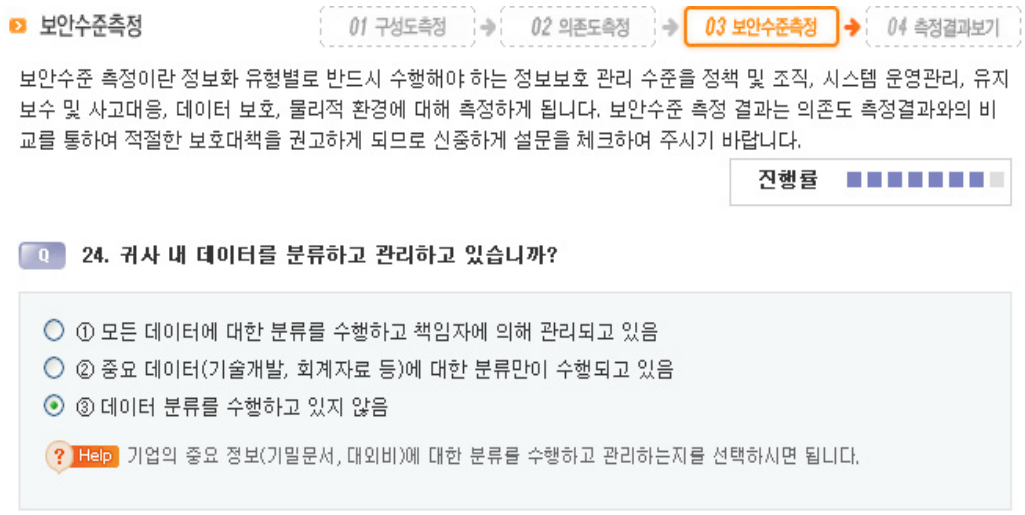
보안수준 측정-유지보수 및 사고대응

⑪ 세번째 측정 분야는 유지보수 및 사고대응 분야로 유지보수 대책 및 관리, 사고대응 대책 및 업무연속성 지원 등에 관한 보안수준을 측정합니다.

[유지보수 및 사고대응 분야 측정 화면]

보안수준 측정-데이터 보호

⑫ 보안수준 측정의 네번째 분야는 데이터 보호 분야로 데이터 관리대책, 데이터 백업 및 시스템 이중화 등에 관한 보안수준을 측정합니다.



[데이터 보호 분야 측정 화면]

▌보안수준 측정-5.물리적 환경

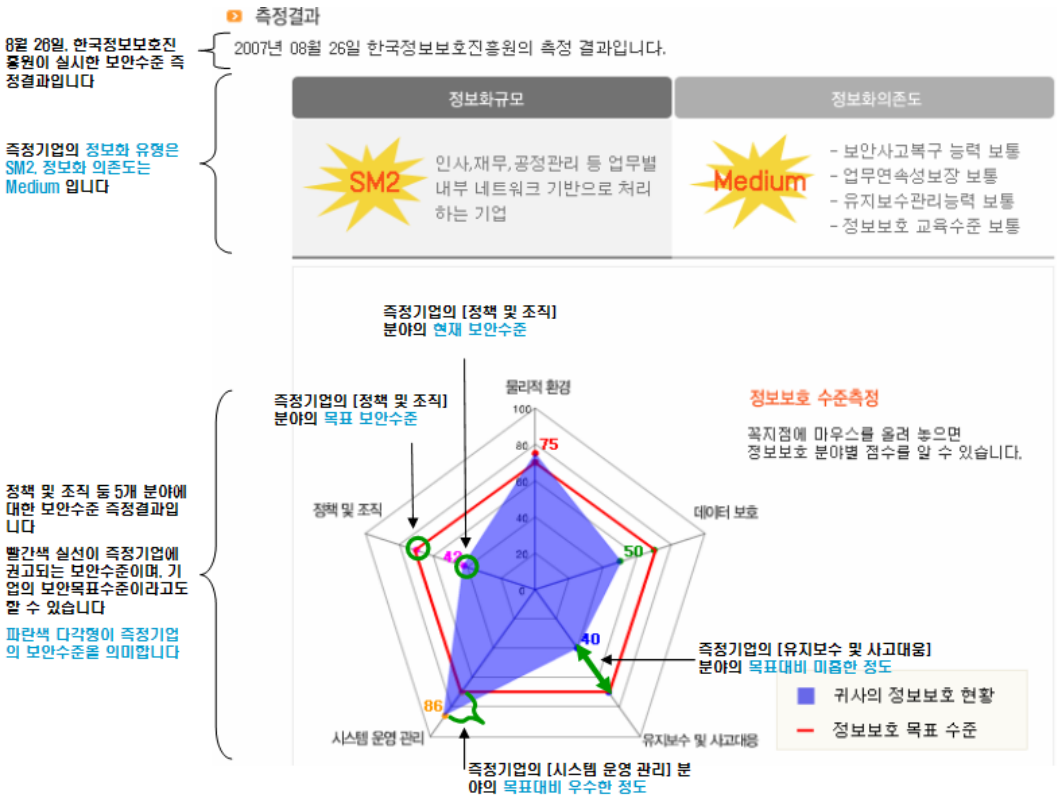
⑬ 보안수준 측정의 다섯번째 분야는 물리적 환경분야로 사무실 및 물리적 시설 보호를 위한 출입통제, 매체관리 및 소방설비 등에 관한 보안 수준을 측정합니다.

[물리적 환경 분야 측정 화면]

4 자가측정 결과보기

▌자가측정 결과보기-측정결과

⑭ 모든 측정이 끝나면 곧바로 화면에서 [측정결과]를 확인할 수 있습니다. 결과보고서는 [측정결과]와 [총평 및 대책] 등 두 부분으로 나누어져 있습니다. [측정결과] 부분은 아래와 같이 나타나며, 해석의 예시는 아래와 같습니다.



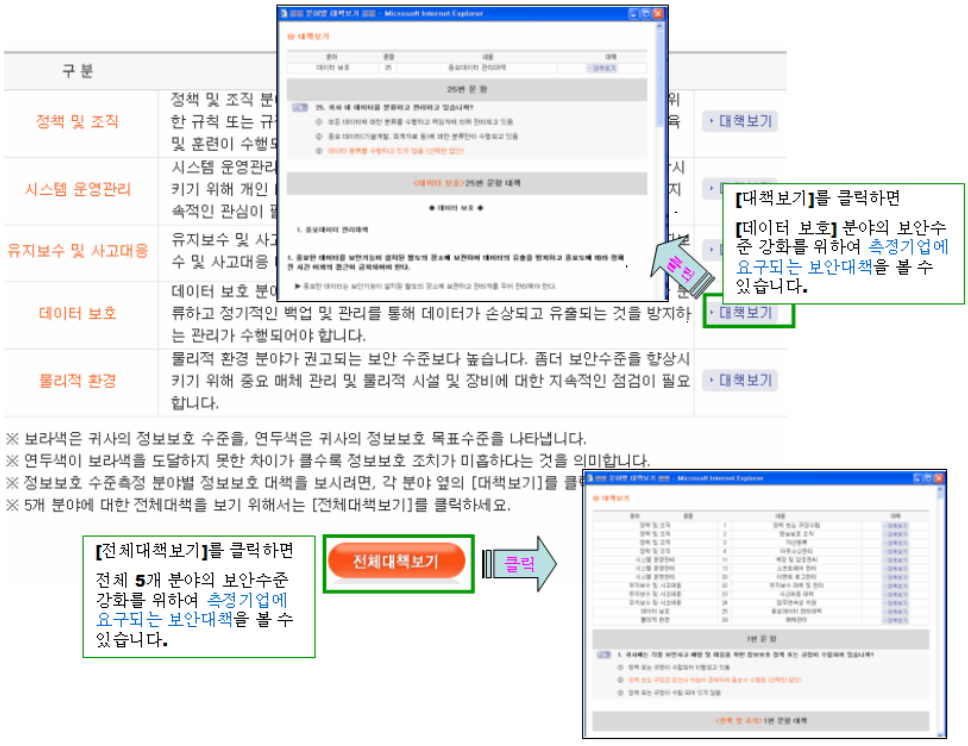
[측정결과화면-측정결과(방사선그래프)]

자가측정 결과보기-총평 및 대책

⑭ [총평 및 대책] 부분에서는 각 분야별 보안현황에 대한 총평과 상세 보안대책을 제공하고 있습니다. 해석의 예시는 아래와 같습니다.

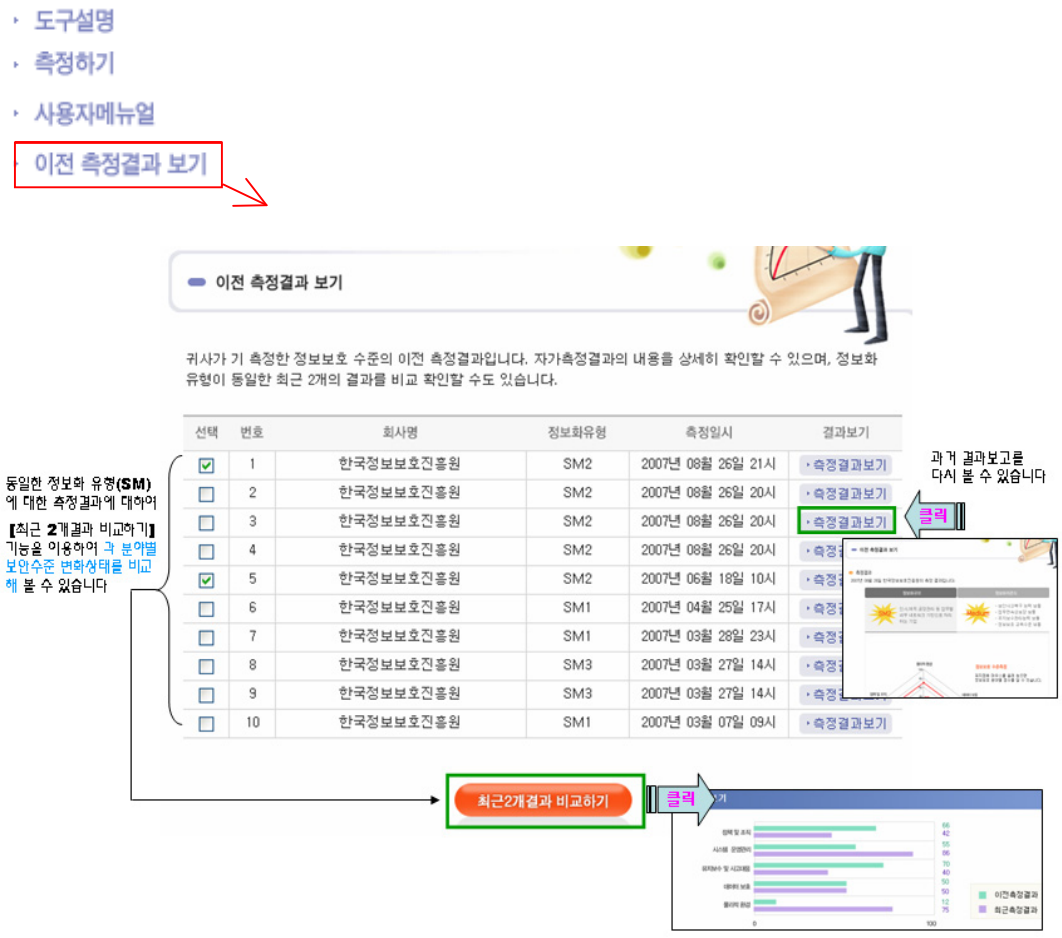
[측정결과화면-보안총평(막대그래프)]

⑮ [대책보기] 혹은 [전체대책보기]를 클릭하면, 각 분야별 대책을 제공받을 수 있습니다. 보안대책은 '중소기업 정보보호 가이드라인' 등을 활용하여 제공됩니다.



[측정결과화면-보안대책보기]

⑯ 이로써, 자가측정 및 결과보기는 모두 종료된 것이며, 사용자는 [이전측정결과 보기]를 클릭하여 과거 본인이 시행한 기업보안수준 측정결과를 다시 볼 수 있으며, 동일한 정보화 유형의 결과에 대해서는 분야별 보안수준을 비교할 수도 있습니다.



[이전 측정결과 보기]

5 맺음말

자가측정 서비스는 정체된 것이 아닌, 향후 기업 보안동향 및 사용자 의견을 수렴하여 지속적으로 개선될 프로그램입니다. 본 자가측정 서비스가 기업보안의 중요성을 인식하고 적절한 보안대책을 찾아가는 시발점이 될 수 있기를 바랍니다.

※ 문의 : IT기반기획팀 중소기업 정보보호 담당, smesg@kisa.or.kr, 02-405-5123

CERT 구축 및 운영 가이드

2007년 9월 인쇄
2007년 9월 발행

발행처 : (사)한국침해사고대응팀협의회·한국정보보호진흥원

서울시 서초구 서초동 1327-29 KT 파라곤 404호
(사)한국침해사고대응팀협의회
Tel : 02-3474-2490~1
http://www.concert.or.kr, info@concert.or.kr

서울시 송파구 가락동 가락동 78번지 IT벤처타워(서관)
한국정보보호진흥원
Tel : 02-4055-114
http://www.kisa.or.kr, http://www.krcert.or.kr

인쇄처 : 호정씨앤피(Tel 02-2277-4718)