제 4 장 정보보호론

1. 암호학

1.1 암호 알고리즘

1.1.1 암호 관련 용어

o 핵심가이드

- 암호시스템의 관련 용어와 정보보호 서비스의 개념 이해

(1) 암호시스템의 관련 용어

(가) 평문

송신자와 수신자 사이 주고받고자 하는 내용을 적은 일반적인 문장으로 모든 사람들이 이해할 수 있는 일반 형태의 문장을 말한다. 평문은 암호화의 대상이 되는 문장으로 한글이나 영어 등의 일반 언어로 작성된 문장이다.

(나) 암호문

송신자와 수신자 사이에 주고받고자 하는 내용을 제 3자가 이해할 수 없는 형태로 변형된 문장을 암호문이라 한다.

(다) 암호화

평문을 제 3자가 알 수 없도록 암호문으로 변형하는 과정을 말하며 일반적으로 암호화 과정은 송신자가 수행한다.

(라) 복호화

암호문을 다시 일반인들이 이해할 수 있는 평문으로 변환하는 과정을 말하며, 일반적으로 복호화 과정은 암호문을 수신한 수신자가 수행한다.

(마) 키

평문의 암호화 과정이나 암호문의 복호화 과정에 필요로 하는 파라미터로 암호화키와 복호화 키로 나누어진다.

(바) 암호 알고리즘

암호 알고리즘은 암호화와 복호화에 사용되는 수학적인 함수이며, 암호 알고리즘은 암호화에 사용되는 암호화 알고리즘, 복호화에 사용되는 복호화 알고리즘이 있다.

(사) 암호해독

암호의 목적은 제3자의 도청으로부터 평문을 보호하는 데 있다. 암호해독은 암호방식의 정당한 사용자가 아닌 제3자가 불법적으로 암호문으로부터 평문을 원복하는 시도를 말하며, 암호해독은 암호화에 사용된 암호키를 찾거나 부대 정보를 이용하여 암호문으로부터 평문을 찾는 과정을 말하며 암호 공격이라고도 한다.

(아) 송신자와 수신자

통신망 상에서 비밀리에 평문을 주고받는 사람들을 말하며, 평문을 암호문으로 변경하여 수신자에게 전달하는 사람이 송신자이며 암호문으로부터 평문을 복호화하는 사람이 수신자이다.

(자) 공격자

암호방식의 정당한 참여자가 아닌 자로 암호문으로부터 평문을 해독하려는 제3자를 공격자라 한다. 특히, 송/수신자 사이의 암호통신에 직접 관여하지 않고 네트워크상의 정보를 관찰함으로써 공격을 수행하는 공격자를 도청자라 한다.

(차) 암호체계 (암호시스템)

암/복호화 열쇠, 평문, 암호문을 포함한 암/복호 알고리즘을 말한다.

(2) 정보보호 서비스 개념

(가) 무결성

메시지전송 중 인가되지 않은 자, 혹은 인가되지 않은 방법으로 정보가 변조되지 않아야 하는 성질

(나) 기밀성

인가된 자만이 접근하여 취득하여야 하는 성질

(다) 부인봉쇄

송수신자가 송수신 사실에 대한 부인을 할 수 없도록 하는 성질

(라) 인증

인가된 자만이 정보 혹은 정보시스템에 접근하여야 하는 성질

(마) 가용성

컴퓨터 시스템이 인가 당사자가 필요할 때 이용할 수 있게 하는 것

(바) 접근제어

특정 권한을 가진 자만 접근할 수 있도록 하는 것

(사) 전자서명

정보의 송/수신 과정에서 정보의 송신자와 수신자의 인증과 전송되는 정보의 무결성을 보장하는 성질

1.1.2 암호 공격 방식

o 핵심가이드

- 각종 공격방식에 대한 방법의 분류와 이해
- 안전성의 개념 이해

(1) 보안공격

전송되는 메시지에 대한 불법적인 공격자의 위협

(가) 수동적 공격

1) 전송되는 파일을 도청

불법적인 공격자가 전송되는 메시지를 도중에 가로채어 그 내용을 외부로 노출시키는 공격 (메시지의 내용 공격)

2) 트래픽 분석

전송 메시지의 암호화로 도청을 통한 메시지 내용 파악이 불가능하더라도 메시지의 송신측과 수신측 신원의 파악 가능 (메시지 존재에 대한 공격 - 익명성 제공으로 방어)

(나) 능동적 공격

1) 메시지 변조

전송되는 메시지들의 순서를 바꾸거나 또는 메시지의 일부분을 다른 메시지로 대체하여 불법적인 효과를 발생시키는 공격

2) 삽입공격

불법적인 공격자가 정당한 송신자로 가장하여 특정 수신자에게 메시지를 보내어 역시 불법적인 효과를 발생시키는 공격

3) 삭제공격

정상적인 통신시설의 사용, 관리를 방해하는 서비스 거부 공격, 특정 수신자에게 전송되는 메시지의 전부 또는 일부가 공격자에 의해 삭제되는 것.

4) 재생공격

공격자가 이전에 특정 송신자와 수신자간에 행해졌던 통화내용을 도청하여 보관하고 있다가 나중에 재생하여 전송하는 공격

(2) 암호공격 방식

암호 해독자가 도청한 암호문으로부터 그에 해당하는 평문이나 비밀키를 도출하는 수동적 공격법

(가) 암호문 단독 공격 (Ciphertext only attack)

암호 해독자는 단지 암호문 C만을 갖고 이로부터 평문 P이나 키 K를 찾아내는 방법으로 평문 P의 통계적 성질, 문장의 특성 등을 추정하여 해독하는 방법

(나) 기지 평문 공격 (Known plaintext attack)

암호 해독자는 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법으로 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해하는 방법

(다) 선택 평문 공격 (Chosen plaintext attack)

암호 해독자가 사용된 암호기에 접근할 수 있어 평문 P를 선택하여 그 평문 P에 해당하는 암호문 C를 얻어 키 K나 평문 P를 추정하여 암호를 해독하는 방법

(라) 선택 암호문 공격 (Chosen ciphertext attack)

암호 해독자가 암호 복호기에 접근할 수 있어 암호문 C에 대한 평문 P를 얻어내 암호를 해독하는 방법

(3) 안전성 개념

주어진 암호 시스템의 안전성을 말할 때는 두 가지 관점이 있다. 첫 번째는 암호 시스템을 공격하기 위해 필요한 계산량이 매우 커 현실적으로 공격할 수 없는 경우를 **계산적으로 안전하다**고 말한다. 둘째는 무한한 계산능력이 있어도 공격할 수 없는 경우를 **무조건적으로 안전하다**고 말한다. 암호 알고리즘 사용자가 해야 할 일은 다음 두 기준 중의 하나 또는 전부를 만족하는 알고리즘을 개발하는 것이다.

- o 암호 해독 비용이 암호화된 정보의 가치 초과
- o 암호 해독 시간이 정보의 유효 기간 초과

1.1.3 정보이론 [1급]

o 핵심가이드

- 엔트로피의 개념 이해
- 키 결정(판정)거리의 개념 이해

(1) 엔트로피

엔트로피는 1948년 Shannon에 의해 도입된 정보량 또는 정보의 불확실도를 측정하는 수학적 개념이다. 즉, 유한개의 사건을 가지는 확률변수 X에 대해 확률 분포 p(X)를 알 때 발생하지 않는 사건의 불확실도를 엔트로피라 하며 H(X)로 나타낸다.

(가) 엔트로피의 정의

X를 유한 집합 위에서 정의된 확률 변수라 하고 확률 분포를 p(X)라 하자. 이

확률 분포에 대한 엔트로피 H(X)는 다음과 같이 정의된다.

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

여기서 $p_i = p(X = x_i)$이다.

만약 모든 사건이 발생할 확률이 $\frac{1}{n}$이면 H(X) = $\log_2 n$이다. 또한 $H(X) \geq 0$이고 H(X)=0이 필요충분조건은 적당한 i에서 p_i=1이고 그 외에서는 p_j=0인 경우이다.

(2) 키 결정(판정)거리

암호계 (P, C, K, E, D)에서 |C|=|P|이고 열쇠가 같은 확률로 주어졌다고 할 때 충분히 큰 n에 대하여 주어진 길이 n인 암호문 문자열에 대하여 기대되는 의사열쇠의 개수 $\overline{S_n}$는 $\frac{}{S_n} \geq \frac{|K|}{|P|^{nR_L}} - 1$ 이다. 실제로 n이 증가하면 $\frac{|K|}{|P|^{nR_L}} - 1$은 0에 접근한다.

한편 $\overline{S_n}$이 0이 되는 n을 암호계의 키 거리라 하고 n_0으로 나타낸다. 즉, n_0은 충분한 계산시간이 주어진 경우에 유일한 열쇠를 찾을 수 있는 암호문의 평균량이다.

1.1.4 스트림 암호

o 핵심가이드

- 스트림암호의 정의
- 동기식/비동기식 스트림 암호의 특징 및 비교
- 스트림암호의 암호화 방법 [1급]
- LFSR의 특징과 비선형 결합논리에 대한 이해 [1급]
- 안전성 개념(선형복잡도, 주기, 상관관계 공격, 랜덤 특성, 대수적 공격) [1급]

(1) 스트림 암호의 개념

평문과 같은 길이의 키 스트림을 생성하여 평문과 키를 비트단위로 XOR하여 암호문을 얻는 방법이다.

(2) 스트림 암호 종류

(가) 동기식 스트림 암호

1) 암호화와 복호화에서 상호 동기화가 필수

2) 전송도중 변조되어도 후속 암호문에 오류의 영향이 파급되지 않음

3) 의도적인 변조가 복호화 단계에서 검출 불가

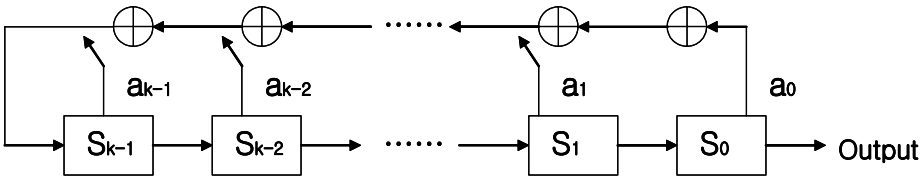
(나) 자기 동기식 스트림 암호

1) 암호문이 전송도중 변경되어도 자기 동기화가 가능

2) 변조된 암호문이 후속 암호문 복호화에 사용되지 않아 오류파급이 제한적

(3) 선형 귀환 시프트 레지스터(LFSR)

LFSR을 이용하면 유한상태머신으로 달성할 수 있는 최대 주기의 수열을 얻을 수 있으며, 수학적인 분석이 용이하다. 특히 선형 복잡도라는 측도를 사용하면 다음에 출력될 값을 예측하기 위해 필요한 수열의 양을 계산할 수 있는 장점이 있다. LFSR의 길이가 작으면 쉽게 해독될 수 있다. 따라서 주어진 수열을 표시할 수 있는 LFSR들의 길이 중 최소의 길이를 선형 복잡도라고 정의한다.



(그림 4-1) LFSR의 동작도

o $s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_r s_{i-r} \bmod 2,\ i \geq r$

LFSR의 초기상태가 $[s_{r-1}, s_{r-2}, \cdots, s_1, s_0]$이면 LFSR는 다음과 같은 선형 점화식을 만족하는 수열 s_0, s_1, s_2 ….을 생성한다.

o 쉬프트 레지스터의 연속적인 상태는 주기 p를 가진다. ($p \leq 2^r$)

o r개의 플립플롭으로 구성된 LFSR이 생성하는 수열의 최대 주기는 $p = 2^r - 1$ 이다.

(가) 비선형 결합논리

LFSR을 단독으로 사용하는 것은 쉽게 해독되기 때문에 출력 수열을 비선형 결합하여 스트림 암호를 구성한다. LFSR을 이용한 스트림 암호는 크게 두 가지 형태로 볼 수 있는데 하나는 출력 수열만을 비선형 결합하는 것이고 다른 하나는 LFSR의 동작을 제어함으로써 선형 복잡도가 큰 수열을 얻는 방법이다.

1) 비선형 여과 생성기(Nonlinear Filter Generator)

비선형 여과 생성기는 하나의 LFSR과 비선형 함수로 구성된다. 비선형 함수

는 LFSR의 각 단에 있는 내용을 변수로 하여 출력을 생성한다.

2) 비선형 결합 생성기(Nonlinear Combination Generator)

비선형 결합 생성기는 여러 개의 LFSR과 비선형함수로 구성된다. 동작방식은 LFSR들을 동시에 동작시킨 후 각각의 출력을 비선형 함수의 입력 변수로 하여 최종 출력수열을 얻는다.

(나) 시각 제어 논리

하나의 LFSR의 출력에 의해 다른 LFSR의 동작을 제어하는 논리를 통칭하여 시작제어 논리라 한다.

1) Cascade Generator

n개의 LFSR로 구성되며 i번째 LFSR의 출력과 그 전단의 출력의 XOR로 i+1번째 LFSR동작을 제어하는 방식

2) Stop and Go Generator

두개의 LFSR로 구성되는데 하나의 LFSR출력이 '0'인 경우에는 다른 LFSR을 동작시키지 않고 '1'인 경우에만 LFSR을 동작시키는 방식

3) Alternating Step Generator

세 개의 LFSR을 이용하여 출력이 랜덤하지 않은 문제점을 효과적으로 극복하였다. LFSR1의 출력수열이 '0'이면 LFSR2를 동작시키고, '1'이면 LFSR3를 동작시켜 LFSR2의 출력과 LFSR3의 출력을 XOR하여 최종출력을 결정한다.

4) Shrinking Generator

기존의 시각 제어 논리는 LFSR의 작동을 제어하였지만 Shrinking Generator는 출력을 제어한다. LFSR1의 출력이 '0'이면 LFSR2의 출력을 내보내지 않고, '1'인 경우에만 LFSR2의 출력을 최종 수열로 한다.

(다) 상관관계 공격과 Summation Generator

상관관계 공격과 선형복잡도 문제를 동시에 해결할 수 있는 수단으로 Summation Generator가 제안되었다. Summation Generator는 두개의 LFSR 출력을 정수로 고려하여 더하고 Carry는 피드백 시키는 형태이다.

(4) 키 수열의 안전성

(가) 키 수열 주기의 길이

주기를 가지기 때문에 수열의 일부가 노출되면 위험하다. 안전한 키 수열의 주기는 스트림 암호가 적용되는 응용분야에 전적으로 의존한다.

(나) 유사-난수열의 조건

키 수열은 무작위로 선정된 진정한 난수열이어야 예측이 불가능하다.

o Golomb의 공리계

$$C(t)=\sum_{i=0}^{p-1}\frac{(2S_i-1)(2S_{i+t}-1)}{p}=1 \qquad if\ t=0,\ \text{K}\ if\ 1\le t\le p-1$$

(그림 4-2) Golomb의 공리계

- 매 주기마다 발생되는 '1'의 개수와 '0'의 개수의 차이는 기껏해야 1이다.
- 매 주기마다 길이가 짧은 연속적인 값들이, 길이가 긴 연속적인 값들보다 더 자주 나타난다.
- P의 주기에서 두 가지 값을 가지는 자기상환함수 C(t)가 존재한다.

(다) 상관공격

비선형함수에 의하여 출력되는 열쇠이진수열의 주기와 복잡도는 LFSR의 크기와 비선형함수에 의존된다. 그러나 열쇠이진수열이 어떤 LFSR에 의한 출력수열과 상관관계가 있으면 이 성질을 이용하여 열쇠를 쉽게 찾을 수 있는 해독법이 있다. 이와 같은 해독법을 상관공격이라 한다.

(라) 랜덤 특성

스트림 암호 체계에서 보안을 유지하기 위해서는 적어도 다음 세 조건이 만족되어야 한다.

1) 키를 선택할 수 있는 방법의 가짓수를 충분히 크게 함으로써 암호해독으로 하여금 키 전부를 시험해 볼 수 없도록 하여야 한다.
2) 보안이 유지되기 위해서는, 생성되는 무한 이진수열들의 주기를 알 수 있어야 한다. 이 값을 아는 경우에는 이보다 짧은 길이의 평문만을 해독하면 되기 때문이다.
3) 암호문은 반드시 '랜덤' 하여야 한다.

어떤 무한 이진수열이 랜덤하다라는 말은, 이 수열의 유한개의 연이은 항들만으로는 그 다음 항을 예측할 수 없음을 뜻한다. 물론, finite state machine에 의하여 생성되는 수열은 진정한 의미에서 랜덤하지 않다. 실제로, 이러한 수열의 항들은 주기적으로 반복되고, 따라서 이 수열의 순환마디로부터 모든 항을 알 수 있다.

그러나, 수열의 주기가 충분히 큰 경우에는 이 수열의 난수성(randomness)을 정의할 수 있다. Golomb은 주기를 갖는 무한 이진수열의 난수성에 관한 공리계를 설정하였는데, 위의 세 공리 1), 2), 3)를 만족시키는 수열을 흔히 G-random수열 이라고 한다.

앞에서 말한 좋은 난수성을 가진 무한 이진수열을 생성하는 방법에는 여러 가지가 있으나, 거의 모든 방법이 Shift register를 이용하고 있다.
이와 같이 Shift register를 이용하는 주된 이유는, 비교적 싸고 손쉽게 구입할 수 있고 Shift register에 의하여 생성되는 수열의 성질을 수학적으로 연구할 수 있기 때문이다.

(5) FCSR

Summation Generator의 정수덧셈을 확장시켜 LFSR의 동작에서 XOR대신에 정수덧셈을 하는 쉬프트 레지스터가 FCSR이다. FCSR을 스트림 암호의 기본요소로 사용하면 선형 복잡도 측면 주기의 반 정도가 되는 장점이 있다.

(6) 대수적 공격 <최근 동향> [1급]

대수적 공격은 알려진 입출력 쌍을 가지고 내부 알고리즘의 기본 대수 방정식을 이용하는 방법으로, 과포화된 다변수 연립 방정식을 통하여 변수의 값을 얻고 이를 이용하여 키를 복구해내는 방법이다. 대수적 공격은 초기에 공개키 알고리즘인 HFE에 적용되었고, 이후 SERPENT, AES와 같은 대수적 성질을 가지는 블록 암호의 분석에 적용되었다. 이 공격법은 이후 블록암호 보다 적용이 용이한 LILI-128, E0 등의 여러 스트림 암호의 분석에 사용되었다.

(가) 대수적 공격의 특성

1) 주어진 알고리즘에 대한 대수적 방정식들이 과포화(overdefined, 방정식의 개수가 변수의 개수가 많은 경우)라면 대수적 공격은 확률 1로 내부 변수(초기 상태 혹은 마스터 키)의 값을 찾을 수 있다.
2) 대수적 공격의 복잡도는 오직 내부 변수의 개수에만 의존하고 변수 값을 구하기 위한 복잡도는 변수 개수의 증가에 따라 지수적으로는 증가하지는 않는다.

(나) 대수적 공격을 효과적으로 적용하기 위한 문제

1) 낮은 차수의 대수적 방정식을 찾는 문제
2) 연립 방정식을 효율적으로 계산하여 해를 찾는 문제

(다) 대수적 공격의 대응책

대수적 공격에 안전하기 위해서는 변수 대 방정식의 비가 높아야 하고, 이를 달성하기 위해서는 내부 변수는 높은 비선형 함수를 이용하여 적절히 갱신되어야 한다. 또한 내부 변수의 갱신 비율이 높으면 높을수록 라운드 수가 증가함에 따라 변수 대 방정식의 수가 감소하지 않는다.

(라) 대수적 공격에 안전한 소프트웨어 구현에 적합한 스트림 암호의 설계 시 고려해야할 사항

1) 키 스트림의 출력 길이

변수 대 방정식의 비가 출력의 길이가 길면 길수록 감소한다. 라운드 당 출력 길이가 작을수록 대수적 공격에 보다 안전할 수 있으므로, 라운드 당 출력 길이의 사이즈를 신중히 고려해야 한다. 출력의 길이가 많아지면 많아질수록 방정식 대 변수의 비율이 점점 줄어들어 과포화 상태 혹은 비율 1의 값에 수렴할 수 있어 대수적 공격에 대한 내성이 작아질 수 있다.

2) 비선형 방정식의 형태

음함수(Implicit Function)형태의 방정식은 높은 차수의 변수를 직접적으로 사용하지 않기 위해서는 추가적인 변수가 필요한 반면, 양함수(Explicit Function)의 경우에는 이러한 추가적 변수가 필요하지 않다. 따라서 대수적 차수가 같더라도 음함수 형태의 방정식이 사용되었다면 양함수에 비해 보다 많은 내부 변수를 갖게 되어 대수적 공격에 내성을 가지게 되므로, 비선형 함수도 신중히 고려하여 설계되어야 한다.

3) 내부 변수의 위치 및 갱신 과정

내부 변수들이 갱신되어 변하는 위치 등도 대수적 공격의 안전성에 영향을 준다. 구체적으로 설명하자면, 내부 변수를 이용하여 출력 스트림을 생성할 때, 내부 변수의 값을 그대로 출력 할 경우 내부 변수의 값이 그대로 노출되어 대수적 공격에 대한 내성이 작아질 수 있다. 또한 내부 변수를 통해 출력 스트림 생성시 내부 변수의 위치가 주기적인 간격만을 이용하여 생성하거나 전체 내부 변수 값을 이용하지 않고 특정 부분의 변수만을 이용할 경우, 내부 변수의 주기적 성질을 이용한 공격 등에 취약할 수 있다. 따라서 알고리즘의 설계시 내부 변수의 위치 및 갱신 과정을 신중히 선택해야 한다.

1.1.5 블록 암호

o 핵심가이드

- 블록암호의 개요 및 구조
- 블록암호 운영모드의 이해
- 블록암호 알고리즘들의 구조와 특성, 안전성, 암/복호화 과정, 키의 크기, 사용된 연산, 개발된 국가와 개발년도

(1) 블록암호의 개요

암호문을 만들기 위해 평문을 일정한 단위로 나누어서 각 단위마다 암호화 과정을 수행하여 블록단위로 암호문을 얻는 대칭 암호화 방식이다.

[표 4-1] 대칭키 암호방식

	대칭키 암호방식
암호키 관계	암호화키 = 복호화키
암호화 키	비밀
복호화 키	비밀
암호 알고리즘	비밀/공개
비밀키 수	${}_{n}C_{2}$
안전한 인증	곤란
암호화 속도	고속

(2) 블록암호 알고리즘 구조

블록암호 알고리즘은 비밀키를 이용하여 고정된 크기의 입력블록을 고정된 크기의 출력블록으로 변형하는 암호 알고리즘에 의해 암/복호화 과정을 수행하며, 이때 출력블록의 각 비트는 입력블록과 키의 모든 비트에 영향을 받는다.

블록 암호는 주로 단순한 함수를 반복적으로 적용함으로써 암호학적으로 강한 함수를 만드는 과정으로 개발된다. 이때 반복되는 함수를 라운드 함수라 하고 라운드 함수에 작용하는 키를 라운드 키라고 한다.

일반적인 경우 키를 입력하여 라운드 키를 발생하여 사용하는데 이러한 과정을 키 스케줄 이라 부른다. 키 스케줄은 입력된 키의 모든 비트를 균등하게 사용하여 라운드 키를 독립인 것처럼 발생시켜야 한다.

(가) Feistel 구조

Feistel구조는 3라운드 이상이며, 짝수 라운드로 구성된다. 이러한 Feistel 구조는 라운드 함수와 관계없이 역변환이 가능하며(즉, 암/복호화 과정이 같음), 두 번의 수행으로 블록간의 완전한 확산(diffusion)이 이루어지며, 알고리즘의 수행속도가 빠르고, 하드웨어 및 소프트웨어구현이 용이하고, 아직 구조상에 문제점이 발견되고 있지 않다는 장점을 지니고 있다.

Feistel 구조는 입력을 좌우 블록으로 분할하여 한 블록을 라운드 함수에 적용시킨 후의 출력 값을 다른 블록에 적용하는 과정을 좌우블록에 대해 반복적으로 시행하는 방식으로, 라운드 키가 역순으로 작용한다는 점을 제외하면 암/복호화

과정이 동일하고 라운드 함수에 대한 제약 조건이 없어 DES를 비롯한 대부분의 블록암호에 채택되어 사용되고 있다.

Feistel 구조는 입력 n비트를 두개의 블록 (L_0, R_0)으로 나누어 라운드 함수를 F, 라운드 키를 K_i라 할 때, i번째 라운드 과정이 다음과 같다.

- o $L_i = R_i$
- o $R_i = L_{i-1} \oplus F_i(R_{i-1}, K_i)$

(나) SPN 구조

SPN 구조는 라운드 함수가 역변환이 되어야 한다는 등의 제약이 있지만 더 많은 병렬성(parallelism)을 제공하기 때문에 암/복호화 알고리즘의 고속화가 요구되고 최근의 컴퓨터 프로세스(CPU)가 더 많은 병렬성을 지원하는 등의 현 추세에 부응하는 방식이라 할 수 있다.

SPN은 입력을 여러 개의 소블록으로 나누고 각 소블록을 S-box로 입력하여 대치시키고 S-box의 출력을 P-box로 전치하는 과정을 반복한다.

(다) Feistel구조와 SPN구조를 사용하는 알고리즘

[표 4-2] Feistel구조와 SPN구조를 사용하는 알고리즘

Feistel 구조를 사용하는 알고리즘	SPN 구조를 사용하는 알고리즘
DES	SAFER
LOKI	IDEA
CAST	SHARK
Blowfish	Square
MISTY	SRYPTON
RC5, RC6,	Rijndael
CAST256	SAFER+
E2	Serpent
Twofish	*
Mars	*

(3) 블록암호 요소의 특징

블록암호 알고리즘을 특징하는 요소로는 다음과 같은 것이 있으며, 이러한 요소에 의해 전체 블록암호의 안전성이 결정된다.

(가) 블록 크기

입출력 블록의 비트수로, 일반적으로 더 클수록 안전하다고 보지만, 암/복호화 과정에서 시간이 더 걸린다. 주로 64비트가 널리 쓰였지만, 최근에는 128바이트를 채택하고 있다.

(나) 키 크기

비밀키의 비트수로, 일반적으로 더 클수록 이 역시 라운드키를 생성할 때 시간이 더 걸린다. DES는 56비트를 사용하였는데 작은 키의 크기로 인하여 안전성에 큰 문제가 되었고, 최근에는 128비트나 그 이상을 주로 사용한다.

(다) 라운드 키 생성

비밀키로부터 각 라운드에 사용할 키를 생성하는 과정으로, 유사시에 라운드 키가 누출되더라도 비밀키는 안전해야 한다.

(라) 라운드 함수

암/복호화를 수행하는 핵심함수로 다양한 암호분석을 거쳐 안전하게 만들어 져야 한다.

(마) 라운드 수

한 번의 암/복호화를 위해 반복하는 라운드 함수의 횟수로, 많을수록 더 안전하다고 보지만 암/복호화 과정에서 시간이 더 걸린다. 근본적으로 한 번의 라운드 함수로 충분한 안전성을 확보할 수는 없기에 라운드 함수에 대한 다양한 암호분석을 통해 충분한 안전성을 얻을 수 있도록 라운드 횟수를 결정한다.

(4) 블록암호의 사용방식

(가) 전자코드북 모드 (Electronic Code Bool Mode)

ECB모드는 가장 단순한 방식으로 각 블록을 독립적으로 암호화 한다. 이 방식은 동일한 평문블록은 동일한 암호문을 생성하는데 이는 안전성에 있어서 이런 점은 바람직하지 않다. 이러한 이유로 ECB모드는 잘 사용하지 않는다.

1) 암호화 : $C_i = E_k(P_i)$

2) 복호화 : $P_i = D_k(C_i)$

(나) 암호블럭연결 모드 (Cipher Block Chaining Mode)

CBC모드는 초기치를 암호화한 값과 평문 블럭을 XOR하여 암호문 블럭을 생성하고 그 암호문을 초기치로 하여 다시 암호화한 값과 평문 블록을 XOR하여 암호문블록을 반복하여 생성하는 방식이다. 암호화에서는 특정 입력이후로 영향을 미치지만, 복호화에서는 특정 암호문의 오류가 계속적으로 이후에 영향을 미치지는 않는다는 특징이 있다.

1) 암호화 : $C_i = E_k(C_{i-1} \oplus P_i)$

2) 복호화 : $P_i = D_k(C_i) \oplus C_{i-1}$

(다) 암호피드백 모드 (Cipher FeedBack Mode)

CFB모드는 초기치를 암호화한 값과 평문 블록을 XOR하여 암호문 블럭을 생성

하고 그 암호문을 초기치로 하여 다시 암호화한 값과 평문 블록을 XOR하여 암호문블록을 반복하여 생성하는 방식이다. 암호화에서는 특정 입력이 이후로 영향을 미치지만, 복호화에서는 특정 암호문의 오류가 계속적으로 이후에 영향을 미치지는 않는다는 특징이 있다.

1) 암호화 : $C_i = P_i \oplus E_k(I_i) \langle i.....r \rangle, I_{i+1} = (I_i \langle\langle r) \oplus (0..0 \| C_i)$

2) 복호화 : $P_i = C_i \oplus E_k(I_i) \langle i.....r \rangle, I_{i+1} = (I_i \langle\langle r) \oplus (0..0 \| C_i)$

(라) 출력피드백 모드(Output FeedBack Mode)

OFB모드는 초기치 Ⅳ를 암호화 하고 그 값을 다시 암호화하는 과정을 반복함으로써 생성된 수열과 평문 수열을 XOR하여 암호문을 생성하는 방식으로, 주로 블록암호 시스템을 스트림암호 시스템처럼 사용하고자 할 때 이용된다. 이 방식에서 암호문의 오류는 복호화 과정에서 대응되는 한 블록에만 영향을 비치므로, 영상이나 음성 같은 디지털 신호화한 아날로그 신호에 많이 사용된다.

1) 암호화 : $I_i = E_k(I_{i-1}), C_i = P_i \oplus I_i$

2) 복호화 : $C_i = P_i \oplus E_k(I_i), P_i = C_i \oplus I_i$

(마) 카운터 모드(Counter Mode)

Counter모드는 초기치 Ⅳ와 Ⅳ+1, Ⅳ+2,....을 암호화하여 생성된 평문수열을 XOR하여 암호문 블록을 생성하고 그 암호문을 기초로 하여 다시 암호화한 값과 평문블록을 XOR하여 암호문블록을 반복하여 생성하는 방식이다. 암호화에서는 특정 입력이 이후로 영향을 미치지만, 복호화 할 때 Ⅳ가 주어지면 미리 계산할 수 있어 평문이 주어지면 바로 암호문을 만들 수 있다는 장점이 있지만, 동일한 비밀키와 Ⅳ를 반복하여 사용할 경우 안전성에 문제가 생긴다는 약점이 있다.

1) 암호화 : $C_i = P_i \oplus E_k(I_i), P_i = I_{i+1} + 1$

2) 복호화 : $P_i = C_i \oplus E_k(I_i), P_i = I_{i+1} + 1$

(5) 블록암호 알고리즘 종류

[표 4-3] 블록알고리즘 종류와 특징

	개발 국가	개발 년도	특징	블록 크기	키의 길이	라운드수
DES	미국	1972년	NIST에서 표준으로 공표(1977년)	64	56	16
IDEA	유럽	1990년	PGP채택	64	128	8
Rijndael	벨기에		2000년 AES알고리즘으로 선정	128	128,192,256	10,12,14
SEED	한국	1999년	한국표준 블록암호 알고리즘	128	128	16
CRYPTON	한국	1998년		128	0-256	12
RC5	미국	1994년	알고리즘이 간단하여 속도가 빠름	64	0-256	16
FEAL	일본	1987년	S/W구현에 적합	64	64	4
MISTY	일본	1996년	차분/선형공격에 안전성증명구조	64	128	8
SKIPJACK	미국	1990년	Fortezza카드에 사용	64	80	32

(가) DES의 암/복호화 과정

현재까지 DES는 가장 널리 사용되어 왔지만 열쇠의 길이가 짧고, 컴퓨터 속도의 개선과 암호해독기술의 발전으로 오늘날 더 이상 DES를 안전하다고만 생각하지 않게 되었다. 최근 DES를 보완하는 끊임없는 연구로 많은 블록 암호들이 개발되어 공개되어왔으며 또한 DES가 공모 되었던 것과 같이 새로운 암호 AES를 선정하였다.

DES는 64비트의 평문을 46비트의 암호문으로 만드는 블록 암호 시스템으로 64비트의 키를 사용한다. 64비트의 키(외부 키) 중 56비트는 실제의 키(내부 키)가 되고 나머지 8비트는 검사용 비트로 사용한다. 또한 DES의 안전성을 증가시키기 위하여 키의 길이를 두 배 즉, 128비트, 십진수 16개를 키로 선택한 변형된 알고리즘을 일반적으로 사용한다. DES는 16라운드(Round)의 반복적인 암호화 과정을 갖고 있으며, 각 라운드마다 전치(Transposition) 및 대치(Substitution)의 과정을 거친 평문과 56비트의 내부키에서 나온 48비트의 키가 섞여 암호문을 만든다. 복호화는 암호화 과정과 동일하나 사용되는 키만 역순으로 작용하는 것이다. DES는 컴퓨터 성능의 발달로 인해 보안성이 약화되어 3DES를 사용하고 있다.

1) 암호화 과정

- o 64비트의 평문 P에 64비트 대칭키 K가 적용되어 세 단계를 거침
- o 64비트 평문은 초기치환을 거쳐 재배열된다.
- o 대체와 치환의 16회 반복
- o 16회 반복으로 생성된 LE_{16}과 RE_{16}의 위치 교환 후 역초기치환이 적용되어 64비트 암호문이 생성됨

2) 복호화 과정

o 부분키를 역으로 적용 시키는 것을 제외하면 암호화 과정과 동일

o $R_{i-1} = L_i$

o $L_{i-1} = R_i \oplus f(R_{i-1}, k_i) = R_i \oplus f(L_i, K_i)$

(나) 3DES

DES의 56비트라는 짧은 키 길이로 인한 안전성 문제를 해결하기 위한 대안으로 3개의 키로 DES를 3회 반복하여 사용하는 Triple DES를 사용한다. 3DES는 속도가 DES보다 3배 정도 느리다는 단점에도 불구하고, 기존의 DES를 이용하여 쉽게 구현되며 DES의 안전성 문제를 해결하는 장점으로 인하여 여러 표준에서 사용되었다. 서로 다른 키로 DES 암호 방식을 반복적용하면 외형상으로는 2배의 키 길이지만 메모리 용량이 충분하면 57비트 효과밖에 얻지 못한다. 그러나 두개의 암호키를 사용하여 첫 번째 키 K_1으로 암호화하고 다시 두 번째 키 K_2로 복호화한 다음 또다시 첫 번째 K_1로 암호화하면 강한 암호를 얻을 수 있다.

(다) IDEA

스위스에서 1990년 Xuejia Lai, James Messey에 의해 만들어진 PES(Proposed Encryption Standard)는 이후 1992년 IDEA(International Data Encryption Algorithm)로 이름을 고쳐 제안하였고, 블럭 초당 177Mbit의 처리가 가능한 빠른 암호화 방법이다. IDEA은 128비트 키, 8라운드, 64비트 블록암호이며 주된 세 가지 연산은 XOR, add mod 216, multiply mod 216+1이다. RSA와 더불어 PGP에 사용되는 방식이기도 하다.

IDEA는 블록 암호 알고리즘으로써 64비트의 평문에 대하여 동작하며, 키의 길이는 128비트이고, 8라운드의 암호 방식을 적용한다. 또한 암호화와 복호화에 동일한 알고리즘이 사용된다. IDEA 알고리즘은 상이한 대수 그룹으로부터의 세 가지 연산을 혼합하는 것으로 이들은 모두 하드웨어나 소프트웨어로 쉽게 구현될 수 있다. IDEA는 16비트 단위 연산을 사용하여 16비트 프로세스에 구현이 용이하도록 설계되었다.

1) 암호화 과정 [1급]

다른 암호화 방식과 마찬가지로 암호화 함수는 암호화될 평문과 키의 두 가지 입력을 갖는다. 이 경우 평문은 64비트이고, 키는 128비트이다. IDEA알고리즘은 마지막 변환함수에까지 8개의 라운드 혹은 반복들로 구성된다. 이 알고리즘은 입력을 4개의 16비트 서브블록으로 분해한다. 각각의 반복과정은 4개의 16비트 서브블록들을 입력받고, 4개의 16비트로 된 결과블록을 생성한다. 최종 변환은 또한 4개의 16비트 블록들을 생성하는데, 이것들은 다시 64비트암호문

을 형성하기 위해 연결된다. 각 반복들은 전체 52개의 서브키에 대하여 6개의 16비트 서브키를 이용하는 반면 최종변환은 4개의 서브키를 사용한다.

2)복호화 과정 [1급]

복호화 과정은 암호화 과정과 본질적으로 같은 작업이다. 복호화는 같은 IDEA구조로서 암호문을 입력으로 사용함으로써 얻어진다. 그러나 서브키의 선택에 있어서 다르다. 복호화 서브키 U_1, ..., U_{52}는 암호화 서브키로부터 유도된다.

(라) SEED

SEED는 한국 정보보호센터가 1998년 10월에 초안을 개발하여 공개검증과정을 거쳐 안전성과 성능이 개선된 최종수정안을 1998년 12월에 발표하였다. 1999년 2월 최종결과를 발표하고 128비트 블록암호표준(안)으로 한국통신기술협회에 제안하였다. SEED알고리즘의 전체 구조는 변형된 Feistel구조로 이루어져 있으며, 128비트 열쇠로부터 생성된 16개의 64비트 회전열쇠를 사용하여 총 16회전을 거쳐 128비트의 평문 블록을 128비트 암호문 블럭으로 암호화하여 출력한다. 이 알고리즘의 전체 구조는 블록의 길이만 다를 뿐 DES의 구조와 같으며, 평문 블럭 128비트를 64비트 블록을 L_0과 R_0로 나누어 DES와 같은 단계를 거쳐 16회전을 하여 최종출력비트를 얻는다.

1) 암호화 과정 [1급]

- o SEED의 평문 128비트는 좌측 64비트 $L_0(64)$와 우측 64비트 $R_0(64)$로 나뉘어 입력된다.
- o 우측 64비트 $R_0(64)$는 암호화 보조키 64비트 $K_1(64)$와 함께 f함수에 입력된다.
- o f함수의 출력 64비트 $f(R_0(64), K_1)$은 좌측 64비트 $L_0(64)$와 비트별로 XOR를 거쳐 $R_1(64)$가 된다.
- o 다시 좌측 64비트 $L_1(64)$와 암호화 보조키 K_2가 f함수에 입력된다.
- o f 함수의 출력 64비트 $f(R_1(64), K_2)$는 좌측 64비트 $L_1(64)$와 XOR를 거쳐 $R_2(64)$가 된다.

(마) AES (Rijndael)

1997년 미국의 NIST는 기존의 DES를 대신할 수 있는 새로운 암호 알고리즘(AES, Advanced Encryption Standard)을 공모하였다. 기존의 3중 DES보다 안전하면서 128비트 이하의 키를 사용해야 한다는 조건에도 불구하고, 약 15개의 알고리즘이 응모하였다. 2000년 안전성분석과 구현 효율성을 검증받은 5개의 후보 가운데 J. Daemen과 V. Rijmen이 제출한 Rijndael이 차세대 AES로 선정되었다.

AES의 암호화 과정의 각 라운드는 비 선형성을 갖는 S-Box를 적용하여 바이트 단위로 치환을 수행하는 SubBytes( ) 연산, 행단위로 순환 시프트를 수행하는 ShiftRows( ) 연산, Diffusion을 제공하기 위해 열 단위로 혼합하는 MixColumns( ) 연산과 마지막으로 라운드 키와 State를 XOR하는 AddRoundKey( ) 연산으로 구성된다.

[표 4-4] AES의 라운드 수(Nr)

	키 길이 (Nk Words)	블록 길이 (Nb words)	라운드 수 (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

사용하는 암호화 키의 길이에 따라, 암/복호화 과정에 필요한 라운드 수는 아래의 표와 같다.

1) 암호화 과정

o AES의 암호화 과정은 DES와 달리, 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 XOR연산을 수행하므로, 암호화 과정에 필요한 전체 라운드 키의 개수는 Nr+1개가 된다. 그리고 암호화의 마지막 라운드에서는 MixColumns( )연산을 수행하지 않는다는 특징이 있다.

2) 복호화 과정

o AES의 복호화 과정은 암호화 과정을 역변환으로 InvSubBytes( ) 연산, InvShiftRows( ) 연산, InvMixColumns( ) 연산, AddRoundKey( ) 연산으로 구성된다. 암호화 과정에서 마지막 라운드는 이전의 라운드들과 달리 MixColumns( ) 연산을 포함하지 않으므로, 복호화 과정의 첫 번째 라운드가 이후의 라운드들과 달리 InvMixColumns( ) 연산을 포함하지 않는다. 복호화 과정의 첫 번째 라운드를 제외한 각 라운드는 AddRoundKey( ) 연산, InvMixColumns( ) 연산, InvShiftRows( ) 연산, InvSubBytes( ) 순서로 연산을 수행하며 라운드 키는 암호화의 역순으로 Nr번째 라운드 키부터 사용한다.

1.1.6 블록 암호 공격 [1급]

o 핵심가이드

- 각 공격법에 대한 기본개념 이해

(1) 차분공격에 대한 기본개념(Differental Crptanalysis)

1990년 Biham과 Shamir에 의하여 개발된 선택된 평문공격법으로, 두개의 평문 블록들의 비트의 차이에 대하여 대응되는 암호문 블록들의 비트의 차이를 이용하여 사용된 암호열쇠를 찾아내는 방법이다.

(2) 선형공격에 대한 기본개념(Linear Cryptanalysis)

1993년 Matsui에 의해 개발되어 알려진 평문 공격법으로, 알고리즘 내부의 비선형 구조를 적당히 선형화시켜 열쇠를 찾는 방법이다.

(3) 전수공격법(Exhaustive key search)

1977년 Diffie와 Hellman이 제안한 방법으로 암호화할 때 일어날 수 있는 모든 가능한 경우에 대하여 조사하는 방법으로 경우의 수가 적을 때는 가장 정확한 방법이지만, 일반적으로 경우의 수가 많은 경우에는 실현 불가능한 방법이다.

(4) 통계적 분석(Statistical analysis)

암호문에 대한 평문의 각 단어의 빈도에 관한 자료를 포함하는 지금까지 알려진 모든 통계적인 자료를 이용하여 해독하는 방법이다.

(5) 수학적 분석(Mathematical analysis)

통계적인 방법을 포함하며 수학적 이론을 이용하여 해독하는 방법이다.

1.1.7 인수분해 기반 공개키 암호

o 핵심가이드

- 공개키 암호시스템의 장단점
- 공개키 알고리즘들의 암호학적 안전성, 알고리즘 안전성, 변수선정 방법, 암/복호화 알고리즘의 키 생성 및 구성
- 이차잉여류 문제 [1급]

(1) 공개키 알고리즘의 특징

데이터의 암호화에서는 공개키가 사용되고, 복호화에서는 비밀키가 사용되는 암호시스템으로 이 시스템은 암호화 조작이 용이하고 복호화에는 방대한 조작이 필요하지만 어떤 복호화 키가 주어지면 용이하게 역변환이 가능하게 되는 일방향성 함수의 개념이 사용되고 있다. 공개키 암호시스템은 다수의 정보교환자 간의 통신에

적합하고 전자서명을 용이하게 실현할 수 있는 특징이 있다.

[표 4-5] 공개키 암호 암호방식

	공개키 암호방식
암호키 관계	암호화키 ≠ 복호화키
암호화 키	공개
복호화 키	비밀
암호 알고리즘	공개
비밀키 수	2n
안전한 인증	용이
암호화 속도	저속

(2) 소인수 분해를 이용한 공개키 암호

(가) 소인수분해 문제

소인수 분해란 하나의 정수를 소인수로 분해하는 것을 말한다. 충분히 큰 두개의 소수를 곱하는 것은 쉽지만, 이들 결과를 소인수 분해한다는 것은 계산적으로 매우 어렵다. RSA 등과 같은 공개키 암호 알고리즘들은 이렇게 소인수 분해의 어려움에 기반을 두고 설계되었다.

(나) RSA 암호

RSA는 1978년 Rivest, Shamir 그리고 Adleman에 의해 설계된 암호로써 Diffie와 Hellman이 제안한 공개키 암호시스템에 대한 개념을 가장 충실히 반영한 것으로 소인수 분해의 어려움에 그 기반을 둔 공개키 암호이다. RSA의 암호 방식의 안전성은 소수 p와 q에 달려 있다. RSA의 암호방식의 안전성을 보장받기 위한 소수 p와 q의 선택조건과 공개 암호화키와 비밀 복호화키의 조건들이 부가적으로 필요하다.

1) 암/복호화 과정

o 준비과정

- 수신자 B가 공개되지 않은 홀수인 두 소수 p_B, q_B의 곱 $n_B = p_B . q_B$를 구한다.
- 수신자 B는 $\phi(n_B) = (p_B - 1)(q_B - 1)$을 구한다.
- 수신자 B는 n_B와 서로서인 e_B를 선택하고 $d_B e_B \equiv 1 \bmod \phi(n_B)$를 만족하는 d_B를 구한다.
- 수신자 B는 위에서 구한 (n_B, e_B)를 공개한다.

o 암호화 과정

- 송신자 A는 평문 P와 공개키를 이용하여 $C \equiv P^{d_b} \bmod n_B$를 계산하여 암호문 C를 얻어 수신자 B에게 송신한다.

o 복호화 과정

- 수신자 B는 암호문 d_B를 이용하여 $C^{d_b} \equiv P \bmod n_B$를 계산하여 평문 P를 얻는다.

o 정리

- 이러한 과정에서 B가 공개한 수 e_B와 n_B를 이 암호방식의 공개키라 한다. 한편, 두 소수 $p_B, q_B, \Phi(n_b)$ 및 d_B는 B만이 가지고 보안을 유지하고 있어야 한다. 특히, (n_B, d_B)는 암호문을 복호화 하는데 필요한 개인키라 한다.

2) 암호학적 안전성

RSA 암호의 비도가 크게 되려면 n의 소인수 분해가 계산적으로 불가능해야 하므로 소인수 분해 알고리즘 등에 의하여 인수분해 되지 않는 꼴이어야 한다. 따라서 p와 q는 다음과 같은 조건을 만족해야 한다.

o p와 q는 같지 않고 거의 같은 크기의 자릿수이어야 한다.

o p-1과 q-1은 커다란 소인수를 각각 가져야 한다.

o p-1과 q-1의 최대 공약수는 작은 수이어야 한다.

위와 같은 조건은 n = p * q의 소인수 분해를 어렵게 만들므로 이를 이용한 RSA암호 방식의 공격을 어렵게 만든다. RSA알고리즘의 공격으로는 다음과 같은 가능한 접근 방법이 있다.

o 전사적 공격 : 모든 가능한 개인키로서 시도한다.

o 수학적인 공격 : 두 소수의 곱을 인수분해하는 몇 가지 접근이 있다.

o 시간적인 공격 : 이것은 복호알고리즘의 실행시간에 의존한다.

(다) Rabin 암호

Rabin암호 역시 소인수분해 어려움에 안전성의 근거를 두고 있다. 결국 Rabin 암호를 해독하는 어려움과 소인수 분해를 하는 어려움은 같은 것이다.

Rabin암호는 RSA와 같은 원리를 이용하지만 암호화 과정이 RSA암호방식보다 빠른 것이 특징이다.

1) 암/복호화 과정

o 준비과정

- 수신자 B가 공개되지 않은 $p_B \equiv 3 \bmod 4$이고 $q_B \equiv 3 \bmod 4$인 두 소수를 선

택하고 p_B, q_B의 곱 $n_B = p_B \cdot q_B$를 구한다.

- 수신자 B는 b를 선택하고 (n_B, b)를 공개한다.

o 암호화 과정

- 송신자 A는 평문 P와 공개키 (n_B, b)를 이용하여 암호문 $C \equiv P(P+b) \bmod n_B$를 구하여 A에게 전송한다.

o 복호화 과정

- 수신자 B는 암호문 C를 복호하기 위하여 $n_B = p_B \cdot q_B$임을 이용하여 $p \equiv \sqrt{\frac{1}{4} + C - \frac{b}{2}} \bmod n_B$을 계산하여 평문 P를 얻는다.

o 정리

- 암호화 함수 Ek는 m을 법으로 한 2차 합동식이므로 암호화하는 속도가 RSA 암호와 비교하여 상당히 빠르다. 그러나 중국인의 정리에 의하여 이차 합동식을 만족하는 해가 4가지이므로 주어진 암호문에 대하여 4가지로 복호되므로 이들 중에서 평문을 찾아야 한다. 따라서 평문을 쉽게 찾을 수 있도록 사전에 평문에 관한 정보를 약속하므로 평문을 얻는다. 이를테면, 평문으로 이용되는 수를 적당하게 제약하므로 실제로 1개의 해가 평문이 되도록 한다.

(라) 이차 잉여류 문제 [1급]

[표 4-6] 이차 잉여와 그 예

	이차 잉여	이차 비잉여
이차 잉여 정의	- gcd(a, m) = 1 - $x^2 \equiv a \bmod m$	- $x^2 \not\equiv a \bmod m$
이차 잉여 예 (Z_{13})	- {1, 3, 4, 9, 10, 12}	- {2, 5, 6, 7, 8, 11}

(3) 효과적인 암호구현 알고리즘 [1급]

(가) 연산의 시행회수를 줄이는 알고리즘

1) Karatsuba 방법

2) Barrett 방법

3) Takagi 방법

4) Montgomery 방법

(나) 연산의 횟수를 감소시키는 알고리즘

1) 지수의 이진표현을 이용하는 이진방법
2) 지수의 소인수분해를 이용하는 소인수 분해 방법
3) 지수의 m진 표현을 이용한 m진 이용방법
4) 지수의 가산고리를 이용하는 가산고리방법

1.1.8 확률적 공개키 암호 [1급]

o 핵심가이드

- 확률적 공개키 암호의 안전성 개념 이해
- RSA-OAEP의 이해
- BBS, Goldwasser-Micali에 대한 내용 이해

(1) 확률적 공개키 암호의 안전성 개념

(가) 의미론적 안전성(Semantically Security)

의미론적 안전성은 Goldwasser와 Micali에 의해 소개된 개념으로서 공개키 암호 방식의 증명 가능한 안전성을 제공하기 위한 효시가 된 정의라고 볼 수 있다. 의미론적 안전성은 암호문으로부터 효율적으로 계산 가능한 것은 모두 단지 평문의 길이만 주어졌을 때에도 효율적으로 계산 가능한 것이라는 사실을 의미한다. 즉, 평문의 길이 이외에 다른 정보가 없다면 암호문은 평문을 유추해 내는 데에 아무런 역할도 하지 못한다는 개념이 의미론적으로 안전하다는 뜻이다. 의미론적으로 안전한 암호 방식을 사용하는 통신로 상에서 암호문을 도청하는 공격자는 평문에 대해서 아무런 정보도 얻지 못한다.

(나) NM-안전성(Non-Malleability)

NM-안전성 개념은 Dolev, Dwork, Naor에 의해서 처음 소개된 것으로 이들의 머리글자를 인용하여 DDN-안전성이라 부르기도 한다. NM-안전성을 정의할 때는 공격자의 공격 목표가 낮아진다는 것이 큰 특징이다. 이전의 안전성 개념에서의 공격자의 목표는 주어진 도전 암호문 C로부터 평문 P를 찾아내는 것이었다. 그러나 NM-안전성 개념 정의에 나타나는 공격자의 목표는 도전 암호문 C의 평문 P을 찾는 것이 아니고 단지 그것의 평문이 P와 알려진 방법으로 관계 지워진 어떤 암호문을 얻어내는 것이다. 즉 다른 안전성 개념에서 보다 공격 성공의 목표치가 약하기 때문에 NM-안전성에 고려되는 공격자는 그만큼 공격을 쉽게 성공시킬 수 있는 것이다. NM-안전성에 고역 관점의 안전성을 결합한 개념을 NM-CPA, NM-CCA, NM-ACC 등으로 표현한다.

(2) RSA-OAEP

공개키 암호화의 경우(서명과 비밀키 전송에 널리 사용되고 있다) 단지 약간의 알고리즘만이 널리 사용되고 있는데 가장 널리 사용되고 있는 알고리듬 중의 하나는 RSA이다. RSA의 알고리듬은 단지 미국에서만 특허화되어 있으며 2000년 9월에 만료되어 자유롭게 사용될 수 있다. 공격자가 직접적으로 제공한 원값(raw value) 을 RSA를 사용해 절대로 복호화하거나 서명하지 말아야 한다. RSA는 비밀키를 드러낼 수 있기 때문에 결과를 들어낸다. (대부분의 프로토콜은 원값이 아닌 사용자가 계산한 해쉬에 서명하는 것을 포함하거나 결과를 드러내지 않기 때문에 이는 실제 문제가 되지는 않는다) 절대로 정확히 동일한 원값을 여러 번 복호화하거나 서명하지 말아야 한다.(원래 값이 노출될 수 있다) 이러한 두 문제 모두 임의의 패딩(padding, 아무런 의미가 없는, 고정 길이를 갖는 레코드 또는 블록에 무의미한 문자로 채우는 기법)을 늘 추가함으로써 해결될 수 있다. 보통의 접근 방법은 Optimal Asymmetric Encryption Padding (OAEP) 라고 불린다.

- o RSAES-OAEP는 Bellare-Rogaway의 방식에 기초한 인코딩 방법이다. Random oracle model을 바탕으로 plaintext-awareness을 주는 알고리즘이며 Make Generation Funcion(MGF)이 필요하다.
- o MGF

  주어진 string을 Seed로 하여 주어진 길이만큼의 난수열을 생성하는 의사 난수 함수이며 RSA 서명 알고리즘 중에 PKCS#1-PSS와 P1363a의 EMSR3 의 안전성은 MGF의 랜덤성에 의존한다. PKCS#1에서는 MGF로 MGF1을 사용 권고하고 있으며 MGF1에서의 해쉬함수는 SHA1을 사용한다.

(가) BBS (Blum Blum Shub)

암호적인 강도에 있어서 가장 강력한 것으로 공개적으로 증명되었다.

1) Generation 절차

- o 4로 나누었을 때 나머지가 모두 3인 두 개의 큰 소수 p와 q를 선택한다. 즉,

$$p \equiv q \equiv 3 (\mathrm{mod} 4)$$

$$n = p \times q$$

- o s가 상대적으로 n에 대해 소수인 난수 s를 선택한다.
- o 아래의 알고리즘에 따라 B_i 비트들의 수열을 생성한다.

$$X_0 = s^2 \mathrm{mod} n$$

for i = 1 to ∞

$$X_i = (X_{i-1})^2 \bmod n$$

$$B_i = X_i \bmod 2$$

2) BBS는 암호학적으로 안전한 pseudorandom bit 발생기(CSPRBG)라고 한다.

o CSPRBG는 정의된 순서에 따라 다음 비트 시험을 통과함으로써 정의된다. => "출력 수열의 첫 번째 k개의 비트들이 입력에서 1/2 보다 월등히 큰 확률로$(k+1)$번째를 예측할 수 있는 다항-시간 알고리즘이 없다면 한 pseudorandom bit 발생기가 다음 비트 시험을 통과했다"고 말한다.

(나) Goldwasser-Micali

암호문으로부터 평문의 어떤 부분 정보도 노출되지 않는 암호 방식. 인수분해 문제와 제곱 잉여의 원리를 이용한 확률 암호를 정의.

1) 준비 과정

o 수신자 B는 공개되지 않은 홀수인 두 소수 p_B, q_B의 곱 $n_B = p_B q_B$를 구하고 n_B를 법으로 한 제곱비잉여로 $\left(\frac{b}{n_B}\right)=1$를 만족하는 b를 생성하고 ($n_B$, b)를 공개한다.

2) 암호화 과정

o 송신자 A는 평문 P∈{0, 1}를 암호화하기 위하여 Z_n^*의 원소 r을 선택한다.

o 송신자 A는 (b, r, n_B)를 이용하여 $C \equiv b^P r^2 \bmod n_B$ 를 계산하여 암호문 C를 B에게 송신한다.

3) 복호 과정

o 수신자 B는 $n_B=p_Bq_B$를 이용하여 C가 n_B를 법으로 한 이차잉여인가 또는 이차 비잉여 인가를 판정한다.

o 수신자 B는 평문을 C가 이차잉여이면 0으로, 이차 비잉여이면 1로 복호한다.

이 암호에는 Z_n^*의 원소인 암호문이 n_B를 법으로 이차잉여와 이차 비잉여일 확률은 각각 $\frac{1}{2}$인 원리를 추가하였다. 따라서 암호문으로부터 평문의 어떤 정보도 노출되지 않으며 암호문의 일부에 대응되는 평문이 노출되어도 이외 평문에 대한 정보가 노출되지 않는 장점이 있다. 그러나 암호화 단위가 1비트이므로 효율적이 아니다.

1.1.9 이산대수 기반 공개키 암호

o 핵심가이드

- 유한체의 이산 대수 문제 이해
- ElGamal 암호체계의 변수 선정법, 암/복호화 순서 및 방법, 사용된 연산, 안전성
- Diffie-Hellman 키 교환체계의 변수 선정법, 암/복호화 순서 및 방법, 사용된 연산, 안전성
- 타원곡선 이산대수 문제(ECDLP)의 이해 [1급]
- 타원곡선 공개키 암호시스템의 변수 선정법, 암/복호화 순서 및 방법, 사용된 연산, 안전성 [1급]

(1) 유한체의 이산대수

(가) 유한체의 이산대수문제

이산대수 문제는 군(group)을 이용한다. 일반적으로 차수가 t인 집합 G의 원소 g와 집합 G의 다른 원소 $y = g^x$ 가 주어졌을 때 x를 구하는 것은 어려우며 이를 이산대수 문제(DLP: Discrete Logarithm Problem)라 한다. 여기서 $0 \leq x \leq t-1$이다. y는 g를 x번 곱한 결과이다. 원소 g는 전형적으로 G의 모든 원소들을 생성하거나 또는 적어도 0에서 t-1사이의 모든 정수들을 가지고 누승함으로서(즉, 반복적으로 그룹 연산을 함으로서)큰 부분집합을 생성할 수 있다. 원소 g가 군 내의 모든 원소들을 생성할 수 있다면 원소 g를 생성자(generator)라고 한다.

유한체의 이산대수문제는 유한체의 곱셈군에 대한 이산대수문제이다. 소인수분해 문제와 마찬가지로 이산대수 문제는 일방향 함수의 어려운 문제라 여겨지고 있다. 이러한 이유로 이산대수 문제는 ElGamal 시스템과 DSS를 포함한 여러 공개키 암호 시스템들의 기초를 이루어 왔다. 이들 시스템들의 안전성은 이산대수를 계산하기가 어렵다는 가정에 의존하고 있다.

이산대수 문제는 유한체(finite fields)상에서 보다 임의의 군(group)상에서 훨씬 더 어려운 듯하다. 즉, 이것은 타원 곡선(elliptic curve)군에 기초한 암호 시스템의 동기 부여이다. 일반적으로 임의의 군 내에서 이산대수를 계산하기 위한 동작시간(running time)은 $o(\sqrt{p})$이다. 여기서 p는 군의 위수(order)이다.

(나) ElGamal

EIGamal은 1985년 이산 대수 문제에 바탕을 둔 공개키 암호시스템이다.

1) 준비과정

o 소수 q와 체 F_a에서 위수가 큰 임의의 원소 g를 공개한다.

o 사용자 A는 자신이 암호문을 전달받기 위하여 임의의 정수 A를 0 < a < q-1 이 되도록 하고 $g^a \bmod q$를 계산하고 a는 공개하지 않고 $g^a \bmod q$를

공개한다.

2) 암호문 전달과정

o 사용자 B는 임의의 k를 선택하여 $P\,g^{ak} \bmod q$를 계산하고 평문 P의 암호문으로 $(g^k, P\,g^{ak})$을 A에게 보낸다.

o 사용자 A는 개인키 a를 이용하여 $(g^k)^a \equiv g^{ak} \bmod q$를 계산하고 $P\,g^{ak}$을 g^{ak}로 나누어 평문 P를 구한다.

(다) Diffie-Hellman

1) 준비과정

o 사용자 A와 사용자 B가 사용할 소수 p와 원시원소 g를 상의하여 결정

2) 개인키 생성

o 사용자 A는 a를 선택하고 $g^a \bmod p$ 를 계산하여 공개하고 사용자 B는 b를 선택하고 $g^b \bmod p$를 계산하여 공개한다.

o 사용자 A는 사용자 B의 공개키 $g^b \bmod p$와 자신의 개인키 a를 이용하여 $(g^b)^a \bmod p$를 계산하고, 사용자 B는 사용자 A의 공개키 $g^a \bmod p$와 자신의 개인키 b를 이용하여 $(g^a)^b \bmod p$를 계산하여 공동 비밀키로 사용한다.

o 실제로 $K \equiv (g^a)^b \equiv (g^b)^a \bmod p$ 이므로 A와 B는 같은 비밀키를 공유할 수 있다. 또, 이산대수를 구하는 어려움 때문에 $g^a \bmod p$와 $g^b \bmod p$로부터 a,b를 얻을 수 없으므로 $g^{ab} \bmod p$를 구할 수 없기 때문에 안전하다.
즉, 만나는 번거로움 없이 K를 비밀키로 결정하여 안전하게 공유하고 이용할 수 있다.

(2) 타원곡선 암호 (Elliptic Curve Cryptosystem) [1급]

타원곡선상의 이산대수 문제를 통해 제안된 암호 시스템으로 RSA 알고리즘보다 작은 비트수를 가지고 동일한 암호의 강도를 지닐 수 있다. 스마트카드나 휴대폰 등 키의 길이가 제한적인 무선 환경이나 작은 메모리를 가지고 있는 시스템에 적합하다.

(가) 타원곡선 이산대수 문제

실수체 위에서 정의된 타원곡선과는 달리 유한체 F_q에서 정의된 타원곡선은 유한개의 원소들로 이루어지며, 연산에 있어서 실수체 위에서 정의된 타원곡선에서와 달리 계산오류가 없이 정확한 값을 얻는 장점이 있다.

타원곡선 위에 한 점 P의 위수를 n이라면 집합 H={P, 2P,…,nP=O}는 군 $E(F_q)$의 순환부분군이다. 즉, 군 H의 임의의 원소 Q에 대하여 적당한 자연수 k가 존재

하여 Q=kP이다. 한편, k와 P를 알면 Q를 구하는 것은 어렵지 않지만, n이 충분히 클 경우에 점 P와 점 Q가 주어질 때, k를 구하는 것은 쉽지 않다. 이를 타원곡선 이산대수 문제(ECDLP: Elliptic Curve Discrete Logarithm Problem)라 한다.

(나) 타원곡선 Diffie-Helloman 비밀키 교환 시스템

사용자 A와 B는 우선 자기 자신의 개인키와 공개키를 만들기 위해 유한체 F_q와 그 위에서 정의되는 타원곡선 E를 정하여 공개하고 반드시 생성원일 필요는 없지만 위수가 충분히 큰 E 위의 원소 Q를 선택하여 공개한다.

1) 준비 과정

o 두 사용자 A와 B가 사용할 타원곡선 E와 위수가 충분히 큰 E 위의 원소 Q를 결정한다.

2) 비밀키 생성 과정

o 사용자 A와 B는 각각 임의의 정수 a, b를 선택하여 자신의 개인키로 보관하고, aQ와 bQ를 계산하여 공개한다.

o 사용자 A와 B가 비밀키를 공유하기 위하여, 사용자 A는 B의 공개키 bQ에 자신의 개인키 a를 곱하여 P=abQ를 구하고 사용자 B도 같은 방법으로 P=abQ를 구하여 비밀키를 생성한다.

(다) 타원곡선 Massey-Omura 암호방식

1) 준비 과정

o 유한체 F_q에서의 타원곡선 E의 점의 개수 N을 구한다.

2) 암호문 전달 과정

o 사용자 A와 사용자 B는 각각 e_A와 e_B를 선택하고 각각 $d_A=e_A^{-1} \bmod N$과 $d_B=e_B^{-1} \bmod N$을 계산하여 각각 (e_A, d_A)와 (e_B, d_B)를 개인키로 한다.

o 사용자 A는 평문 P와 자신의 키 e_A를 이용하여 $e_A(P)$를 계산하여 사용자 B에게 보낸다.

o 사용자 B는 $e_A(P)$를 수신하고 자신의 키 e_B를 이용하여 $e_B(e_A(P))$를 계산하여 사용자 A에게 보낸다.

o 사용자 A는 $e_B(e_A(P))$를 수신하고 자신의 키 d_A를 이용하여 $d_A(e_Be_A(P))=e_B(P)$ 를 계산하여 사용자 B에게 보낸다.

o 사용자 B는 $e_B(P)$를 수신하고 자신의 키 d_B를 이용하여 $d_B(e_B(P))=P$를 계산하여 평문 P를 얻는다.

(라) 타원곡선 ElGmal 암호방식

1) 준비 과정

o 두 사용자 A와 B가 사용할 타원곡선 E와 위수가 충분히 큰 E의 원소 Q를

결정한다.

2) 암호문 전달 과정

o 사용자 A는 자신이 암호문을 전달받기 위하여 임의의 정수 e_A를 선택하고 개인키로 보관하고 $e_A(Q)$를 계산하여 공개한다.

o 사용자 B는 임의로 정수 k를 선택하여 kQ를 계산하고, 평문 P의 암호문으로 순서쌍(kQ, $P+k(e_A(Q))$)를 사용자 A에게 보낸다.

o 사용자 A는 kQ에 자신의 개인키 e_A를 곱하여 $e_A(kQ)$를 구하고 이를 이용하여 $P+k(e_A(Q))-e_A(kQ)$를 구하여 평문 P를 얻는다.

1.2 해쉬함수와 전자서명

1.2.1 해쉬함수 일반

o 핵심가이드

- 해쉬함수의 성질
- 해쉬함수의 특성과 그 핵심 논리
- 생일역설과 안전성개념

(1) 해쉬함수의 성질

해쉬함수 h가 가져야 할 기본 성질들로는 다음과 같은 것들이 있다.

(가) 역상 저항성

주어진 임의의 출력값 y에 대해, y=h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능하다.

(나) 두 번째 역상 저항성

주어진 입력값 x에 대해 h(x)=h(x′), $x \neq x'$을 만족하는 다른 입력값 x′을 찾는 것이 계산적으로 불가능하다.

(다) 충돌 저항성

h(x)=h(x′)을 만족하는 임의의 두 입력값 x, x′을 찾는 것이 계산적으로 불가능하다.

(2) 전자서명에 이용되는 해쉬 함수의 특성

(가) 해쉬함수의 계산 효율이 양호해야 한다.

(나) 약 일방향성 (Weak onewayness)

해쉬값 H로부터 h(M) = H되는 서명문 M을 찾는 것은 계산상 불가능해야 한

다.

(다) 강 일방향성 (Strong onewayness)

어떤 서명문 M과 그의 해쉬값 H=h(M)가 주어졌을 때 h(M′)=H되는 서명문 M′≠M을 찾는 것이 계산상 불가능해야 한다.

(라) 충돌 회피성(collision freeness)

h(M)=h(M′)되는 서명문 쌍(M, M′) (M≠M′)을 찾는 것이 계산상 불가능해야 한다.

여기서 첫 번째 특성은 해쉬함수의 성능조건이고 두 번째, 세 번째, 네 번째 특성은 해쉬 함수의 안전성에 관한 제약이다. 두 번째, 세 번째 특성은 해쉬 함수의 역함수를 계산하는 것을 방지하는 기능을 말하며 네 번째 특성은 서명자가 서명문 M을 서명하여 전송하고 나중에 M′를 서명하여 전송하였다고 주장하는 이른바 내부 부정을 방지하기 위한 기능이다.

(3) 생일역설과 해쉬함수의 안전성 개념

해쉬 함수의 특성 중 충돌 회피성은 서로 다른 서명문 M, M′의 해쉬값 H가 동일한 값을 갖지 않는다는 조건이나 실제의 경우 서명문 M의 길이가 해쉬값 H보다 훨씬 길기 때문에 충돌은 반드시 발생하기 마련이다. 이러한 충돌 회피성조건을 만족하기 위해서는 동일한 해쉬값 H를 갖는 서로 다른 서명문 M과 M′를 찾는 것이 어려워야 된다.

동일한 해쉬값 H를 갖는 서명문 M과 M′를 구하는 문제는 흔히 생일 공격으로 설명된다. 생일이 같은 날일 확률이 $\frac{1}{2}$이려면 몇 명의 사람이 있어야 하나 그 결과는 23명이다.

일반적으로 해쉬값 H가 같아질 확률이 1/2이 되려면 서명문 M의 수가 몇 개나 있어야 하는 문제는 $K = 1.17\sqrt{M}$이다. 따라서 생일 공격을 차단하기 위해서는 적어도 128비트, 즉 2^{64}비트 서명문을 비교해야 하는 경우 이상이어야 한다. 예로 DSS에서는 160비트로 제한하고 있다.

1.2.2 블록암호 이용 방식

o 핵심가이드

- 각종 해쉬함수 종류

n비트의 블록 암호를 이용하여 만들어진 해쉬함수들은 (n비트)단일 길이의 해쉬

값을 생성하는 것과 (2n비트) 이중 길이의 해쉬값을 생성하는 해쉬함수로 나누어진다.

[표 4-7] n비트 블록 암호에 기초한 해쉬함수의 요약

해쉬함수	(n, k, m)	해쉬 비율
Matyas-Meyer-Oseas	(n, k, m)	1
Davies-Meyer	(n, k, m)	k/n
MDC-2(DES)	(64, 56, 128)	1/2
MDC-4(DES)	(64, 56, 128)	1/4

1.2.3 전용 해쉬 함수

o 핵심가이드

- 전용 해쉬함수들의 핵심 내용과 비교
- 해쉬함수 공격의 이해

전용 해쉬함수란 블록 암호 혹은 모듈 연산과 같은 기존의 시스템 성분들을 다시 이용하지 않고 해쉬만을 목적으로 최적화된 수행을 하도록 디자인된 해쉬함수이다.

(1) MD4

MD5의 초기 버전으로서, 입력 데이터(길이에 상관없는 하나의 메시지)로부터 128비트 메시지 축약을 만듦으로써 데이터 무결성을 검증하는데 사용되는 알고리즘이다.

(가) MD4의 설계 원칙

1) 수학적인 가정 없이 안전한 해쉬함수를 설계한다.
2) 해쉬함수의 수행속도는 가능한 빨라야 한다. 특히, 소프트웨어로 구현 했을 때의 속도를 고려한다.
3) 알고리즘은 단순하며 구현이 용이해야한다.
4) little-endian 구조(word의 최하위 바이트가 low-address 바이트 위치에 있는 구조)를 고려한 알고리즘을 설계한다.

(2) MD5

o 128비트 출력

o 512비트 블록단위로 처리

o 4라운드 64단계로 구성

(가) MD4와 MD5의 차이

1) MD4는 16단계의 3라운드를 사용하나 MD5는 16단계의 4라운드를 사용한다.

2) MD4는 각 라운드에서 한번씩 3개의 기약함수를 사용한다. 그러나 MD5는 각 라운드에서 한번씩 4개의 기약 논리 함수를 사용한다.

3) MD4는 마지막 단계의 부가를 포함하지 않지만, MD5의 각 단계는 이전 단계의 결과에 부가된다.

(3) SHA-1

o 160비트 출력

o 512비트 블록단위로 처리

o 4라운드 80단계로 구성

(4) RIPEMD-160

o 21워드 입력값을 5개의 워드 출력값으로 변환시킨다. 각 입력블록은 동시에 각기 다른 압축 함수에 의해 실행된다.

o 임의의 길이의 메시지를 512비트-블록단위 처리

o 160비트 출력

[표 4-8] MD5, SHA-1, RIPEMD-160 비교

	MD5	SHA-1	RIPEMD-160
다이제스트 길이	128비트	160비트	160비트
처리의 기본단위	512비트	512비트	512비트
단계 수	64(16번의 4라운드)	80(20번의 4라운드)	160(16번의 5병행 라운드)
최대 메시지 크기	unlimited	$2^{64}-1$ 비트	$2^{64}-1$ 비트
기약 논리 함수	4	4	5
덧셈 상수	64	4	9
Endianness	Little-endian	Big-endian	Little-endian

(5) 해쉬함수 공격의 종류 및 그 특성 [1급]

(가) 일치블록 연쇄공격

새로운 메시지 M′를 사전에 다양하게 만들어 놓았다가 공격하고자 하는 메시지 M의 해쉬함수값 h(M)과 같은 해쉬함수 값을 갖는 것을 골라 사용하는 공격

(나) 중간자 연쇄공격

전체 해쉬값이 아니라 해쉬 중간의 결과에 대한 충돌쌍을 찾는다. 특정 포인트를 공격대상으로 한다.

(다) 고정점 연쇄공격

압축함수에서 고정점이란 $f(H_{i-1,}x_i)=H_{i-1}$을 만족하는 쌍 $(H_{i-1,}x_i)$를 말한다. 그러한 메시지 블록과 연쇄변수 쌍을 얻게 되면 연쇄변수가 발생하는 특정한 점에서 임의의 수의 동등한 블록들 x_i를 메시지의 중간에 삽입해도 전체 해쉬값이 변하지 않는다.

(라) 차분 연쇄공격

1) 다중 라운드 블록암호의 공격

다중 라운드 블록암호를 사용하는 해쉬 함수에서, 입력값과 그에 대응하는 출력값의 차이의 통계적 특성을 조사하는 기법을 사용

2) 해쉬함수의 공격

압축함수의 입출력 차이를 조사하여, 0의 충돌쌍을 주로 찾아내는 방법을 사용.

(마) 최근 동향

최근 Wang의 공격으로 표준 해쉬함수 SHA의 안전성에 문제가 발견되어 미국 NIST는 2005년 10월 해쉬함수 워크샵을 개최하여 해쉬함수의 안전성을 강화하는 방안을 논의하는 자리를 마련하였다. 이 워크샵에서 해쉬함수의 정의, 설계 요구조건, 압축함수의 설계기법 등에 대하여 심도있는 재검토가 필요하다는 공감대가 형성되었으며 장기적으로 용도에 따라 다양한 해쉬함수를 개발해야 한다는 쪽으로 논의가 진행되었다.

1.2.4 해쉬 함수 설계 원리 [1급]

o 핵심가이드

- 압축함수의 정의
- 패딩기법
- MDC 해쉬함수의 안전성
- 일방향 함수의 정의
- MAC 설계방법

(1) 압축함수와 패딩기법

(가) 압축함수란

크기가 고정된 해쉬함수로 압축성, 계산의 용이성에 일방향 성질을 추가시킨 함수이다. 하지만 정의역이 제한되어 있어 고정된 크기의 입력값을 갖는다. 즉, m 비트 크기의 입력을 n비트 크기의 출력값으로 압축시킨다. (m > n)

(나) 패딩기법

블록 단위로 해쉬하는 방법에서 일반적으로 블록 길이를 맞추기 위해 해쉬하기 전에 메시지에 대한 비트열이 패딩된다. 패딩된 비트는 보내는 사람과 받는 사람이 동의한다면 전송 또는 저장될 필요가 없다.

1) 패딩방법 1

- o 입력 : 비트길이가 n인 데이터 x.
- o 출력 : 비트 길이가 n의 배수인 패딩된 데이터 x′.
- o 패딩 : 비트 길이가 n의 배수가 되도록 필요한 만큼 x에 ′0′비트들을 패딩한다.

2) 패딩방법 2

- o 입력 : 비트 길이가 n인 데이터 x.
- o 출력 : 비트 길이가 n의 배수인 패딩된 데이터 x′.
- o 패딩 : x에 ‘1’비트를 패딩한다. 비트 길이가 n의 배수가 되도록 필요한 만큼 데이터 x에 ‘0’비트들을 패딩한다.

위의 패딩방법 1은 데이터의 뒤에 붙은 ‘0’비트가 패딩 ‘0’비트와 구별되지 않으므로 모호하다. 이런 방법은 다른 수단에 의해 수신자에게 데이터의 길이를 알려줄 수 있다면 좋은 방법이 될 수 있다. 패딩방법2는 패딩되지 않은 데이터 x와 패딩된 데이터 x′사이에 일대일 관계가 있으므로 모호하지 않다.

(2) MD-method

(가) MDC 해쉬 함수의 안전성

안전하고 효율적인 MDC 해쉬함수 h( )는 다음 조건을 만족하는 함수이다.

1) 함수 h( )는 공개된 함수이고 어떠한 비밀키도 함수계산에 사용되지 않는다.
2) 변수 m의 길이에는 제한이 없고 h(m)의 길이는 l비트로 고정된다.
(l > 64)
3) h( )와 m이 주어졌을 때 h(m)의 계산은 용이하여야 한다.
4) m가 h(m)이 주어졌을 때 h(m′)=h(m)을 만족하는 m′(≠m)을 찾는 것은 계

산적으로 불가능해야 한다.

[표 4-9] MDC

구분	입력	출력	해쉬율
MDC-2	n	2n	1/2
MDC-4	n	2n	1/4

(3) Universal One-Way Hash Function

(가) 일방향성

임의의 해쉬값 h(M)이 주어졌을 때 그것에 대해서 입력 메시지 M를 도출해 내는 것이 불가능한 조건

(4) 해쉬 함수를 이용하여 MAC을 설계하는 방법

(가) MAC의 안전성

안전하고 효율적인 MAC 해쉬함수 h( )는 다음 조건을 만족하는 함수이다.

1) 함수 h( )는 공개된 함수이고 비밀키 k가 함수 계산에 사용된다.
2) 변수 m의 길이에는 제한이 없고 h(k, m)의 길이는 l비트로 고정된다. ($l \geq 64$)
3) h( ), m 그리고 k가 주어졌을 때 h(k, m)의 계산은 용이하여야 한다.
4) 여러 쌍의 {mi, h(k, m_i)}가 관측되었다고 할지라도 이를 이용하여 비밀키 k를 도출한다거나 또는 임의의 m′($\neq m_i$)에 대해서 h(k, m′)을 계산해 내는 것 역시 계산적으로 불가능해야 한다.

[표 4-10] 해쉬유형 표

해쉬 유형	**설계 목적**	**이상적인 길이**	**공격자의 목적**
OWHF	역상 저항; 두 번째 역상 저항	2n 2n	역상 생성; 같은 상을 갖는 다른 역상 생성
CRHF	충돌 저항	$2^{n/2}$	충돌 생성
MAC	키 회복불능; 계산 저항	2t $P_f=\max(2^{-t}, 2^{-n})$	MAC키 찾기; 새로운(메시지, MAC) 생성

1.2.5 전자서명 일반

o 핵심가이드

- 전자서명의 조건들
- 수기 서명과 전자서명의 차이점 분석
- 공개키 기반 구조(PKI)의 개념 및 구성객체 종류
- PKI 인증서 관리구조
- 서명위조와 안전성에 대한 개념
- 메시지 복원형과 메시지 부가형의 차이

(1) 전자서명의 조건

(가) 위조 불가 조건

합법적인 서명자만이 전자 문서에 대한 전자 서명을 생성할 수 있어야 한다.

(나) 서명자 인증 조건

전자 서명의 서명자를 누구든지 검증할 수 있어야 한다.

(다) 부인 불가 조건

서명자는 서명 후에 자신의 서명 사실을 부인할 수 없어야 한다.

(라) 변경 불가 조건

서명한 문서의 내용은 변경될 수 없어야 한다.

(마) 재사용 불가 조건

전자 문서의 서명은 다른 전자 문서의 서명으로 사용될 수 없어야 한다.

(2) 수기 서명과 전자서명의 차이점

(가) 서류에 서명하는 문제

수기서명에서는 서명이 서류의 일부분인 반면에 전자서명은 서명되는 서류의 일부분이 아니며 서류의 전체이다.

(나) 서명을 확인하는 인증문제

수기 서명에서는 실제의 서명과 비교함으로써 증명되는 반면, 전자서명은 공개된 알려진 인증 알고리즘에 의하여 증명될 수 있다. 즉, 수기 서명은 보는 사람에 따라 주관적이므로 위조여부의 식별에 차이가 있지만 전자서명은 모든 사람에게 객관적이므로 위조여부의 식별에 차이가 없다.

(다) 복사의 문제

수기 서명에서는 실제의 서명을 복사하기 힘들지만 전자서명에서는 똑같이 복사될 수 있다.

(3) X.509 인증서

(가) X.509인증서의 역사

전자서명을 위한 인증서는 디지털 형태로 표준화가 필요하다. 인증서는 온라인 상에서 배포되고 검증할 수 있어야 하기 때문에 현재 가장 널리 쓰이는 디지털 인증서 형태는 X.509인증서이다. 1988년 ITU(International Telecommunications Union)에 의해 표준으로 개발된 X.509인증서는 1993년 두 번째 버전이 출시되면서 2개의 인식자가 첨가되었고, 1997년 세 번째 버전에 다시 확장영역이 추가되면서 표준으로 자리 잡게 되었다. 1988년 처음 등장한 X.509인증서는 강력하고 유연한 메커니즘으로 다양한 정보를 포함할 수 있으며, ASN.1구조를 채택하여 꾸준히 발전하고 있다. 특히 IETF(Internet Engineering Task Force)가 인터넷상에서 X.509인증서 사용을 결정함에 따라 X.509인증서의 확장영역에 인터넷 사용에 필요한 요건을 정하게 되면서 획기적인 발전을 이루었다.

(나) X.509 인증서의 ASN.1 구조

X.509 인증서의 ASN.1 구조는 크게 OID(Object Identifiers), AI(Algorithm Identifiers), DS(Directory String), DN(Distinguished Names), GN(General Names)의 5부분으로 나누어진다.

1) OID(Object Identifiers)

OID X.509인증서에서 OID(Object Identifiers)는 다양한 정보를 나타내기 위해 사용된다. 예를 들면 CA가 사용하는 RSA 또는 DSA와 같은 암호 알고리즘, 인증정책 등을 X.509인증서에 기록하기 위해 사용되는 것이다.

2) AI(Algorithm Identifiers)

AI(Algorithm Identifiers)는 X.509인증서에서 암호 알고리즘과 키에 대한 정보를 나타낸다. 예를 들면 X.509인증서가 사용하는 전자서명 알고리즘을 알 수 있고, 공개키와 관련된 알고리즘을 알 수 있는 것이다.

3) DS(Directory String)

DS(Directory String)는 X.509인증서에 텍스트(text) 정보를 나타내기 위한 것이다. DS는 다양한 언어와 문자를 사용할 수 있도록 PrintableString, TeletexString, BMPString, UTF8String, UniversalString 등 여러 형태로 정의된다. PrintableString은 ASCⅡ를 지원하고, TeletexString은 북유럽 언어를 지원하며, BMPString은 16비트로 암호화된 다양한 언어를 지원하고, UTF8String과 UniversalString은 디지털로 암호화된 다양한 언어를 지원한다.

4) DN(Distinguished Names)

DN(Distinguished Names)은 X.509인증서에 계층적으로 이름을 부여하기 위한 것이다. 이는 국제적 디렉토리(directory)에서 X.509인증서를 식별해야 하기

때문이다.

5) GN(General Names)

GN(General Names)은 X.509인증서의 이름을 암호화하기 위한 것이다. 이를 위해 GN은 7개의 표준이름 형태를 사용한다.

(다) X.509인증서의 내용

X.509인증서의 내용은 크게 개인정보와 공개키로 구성된다. 이름과 소속 그리고 연락처(주로 전자우편 주소) 등의 개인정보가 기록되어 있고, 인증서의 발급일과 만료일 그리고 인증서의 고유성을 확보하기 위한 일련번호와 인증서를 발급한 인증기관의 명칭이 나타나 있다. 또한 인증서에는 인증기관의 전자서명이 첨부되어 있다. 인증기관의 전자서명은 인증서가 진본임을 증명해 준다.

(라) X.509인증서 3부분

X.509인증서의 내용 X.509인증서는 크게 3부분으로 나누어진다. 개봉봉투(Tamper-Evident Envelope)는 인증서의 모든 내용을 담고 있고, 인증서 내용(Basic Certificate Content)은 모든 인증서가 기본적으로 갖추어야 하는 정보를 담고 있으며, 확장영역(Certificate Extension)은 인증서에 따라 다양한 선택적 정보를 담고 있다. 따라서 인증서 내용은 확장영역을 포함하며 개봉봉투는 인증서 내용을 포함한다.

(4) 공개키 기반 구조(PKI)의 개념

(가) 정의

공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안시스템 환경이다. 즉, 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템이다.

(나) 공개키 기반구조(PKI)의 객체 구성

1) 공개키 인증서를 발급, 폐지하는 인증기관(CA)
2) 공개키와 인증서 소유자 사이의 관계를 확인하는 등록기관(RA)
3) 인증서를 발급받고, 전자문서에 서명하고 암호화를 할 수 있는 공개키 인증서의 소유자
4) 인증기관의 공개키를 사용하여 인증경로 및 전자서명을 검증하는 사용자
5) 공개키 인증서와 CRL을 저장하는 저장소

(다) 공개키 기반구조(PKI)의 요구사항

1) 비용 및 성능을 고려한 사용자의 편의성 제공
2) 전자상거래에 대한 법적 효력유지

3) 사용자의 보안 정책 및 관리 체계 반영

5) 인증서의 생성, 획득, 취소 및 검증가능

6) PKI 기반의 전자상거래 실체 인증

7) 메시지의 무결성 보장 및 변조 검출

8) 메시지 및 전자상거래 관련자의 기밀성 보장

9) 기타의 정보보호 서비스 제공

(라) PKI 인증서 관리구조

[표 4-11] 인증서 관리구조

인증 구조	장점	단점
계층구조	●축차적 정부 조직에 유리 ● 계층적 디렉토리 명칭 사용 ●인증 경로 탐색 용이 ●모든 사용자는 루트로 향하는 후진 경로 이용 가능	●전세계 단일 루트 **CA** ●상업용 신뢰 경로는 계층적이 아님 ●루트 개인키의 손상 결과는 심각한 피해
네트워크 구조	●상업적 상호 신뢰 관계를 반영 ●원격 **CA** 간에 직접적 상호 인증 ●**CA** 개인키 손상에 대한 복구 용이 ●융통성 있는 정책과 인증경로 처리부하 경감	●인증경로 탐색 매우 복잡 ●다양한 인증 경로의 관리 문제
복합형 구조	●계층적 구조 및 네크워크 구조의 특성을 조합 ●인증경로의 검증을 효과적으로 처리	●인증경로 검증이 다양하고 복잡 ●다양한 형태의 상호 인증서 필요

1) COI구조

o 자주 거래하는 관심 주제에 따라 그룹을 형성한 인증기관구조

o 인증경로가 거래 사용자간에 특별히 설정되어 저장할 인증서의 수효감소

2) 조직에 따른 구조

o 어떤 기관의 현재 계층적, 또는 부서별 조직 관계를 반영한 구조

o 조직의 계층적 상하 관계가 분명한 기관에서 유리하며 구현용이

3) 보증 단계 따른 구조

o 어떤 등급의 보증 수준을 나타내는 대상자별로 그룹을 형성한 구조

o 신뢰성 보증수준에 따른 효과적 보안정책수립

4) 복합형 인증서 관리 구조

o COI구조, 조직에 따른 구조, 그리고 보증 단계에 따른 구조 3가지의 형태를 각각 하나의 세그먼트로써 허용하는 복합적인 구조

o 한 국가의 종합적인 환경은 정부기관, 일반 상거래 관계의 기업, 또는 특수한 분야의 서비스 조직 등 다양한 형태별 구성가능

(마) PKI 응용모델

1) SDSI(Simple Distributed Security Infrastructure)

o 1996년 X.509의 복잡성에 대응하여 보다 단순화된 방식 제안

o X.509의 기능들 중에서 인증서 정책, 제약조건, 키 생명주기 관리 등의 기능 생략

o 단순한 응용환경에서 운용할 수 있는 X.509 기능의 일부를 정의

o X.509에서 사용된 ASN.1보다 단순한 방식의 구문표현기법 사용

o 특별한 자료구조를 사용하여 단순하게 기능을 제공하는 것이 장점

o 공식적인 정책들이 요구되는 대형 조직에서는 구현하기 어려움

2) SPKI(Simple Public-Key Infrastructure)

o X.509 PKI 신뢰모델의 인증서와는 다르게 실체-기반 인증서가 아니라 신용-기반 인증서를 정의

o 대응되는 개인키의 소유자에게 필요한 실체명을 요구하지 않고 SPKI인증서가 공개키에 명시된 인가 또는 특권을 인정하는 새로운 기법

o SPLI 인증서의 주요목적이 어떤 동작의 인가를 부여하고 자격을 인정

o 폐쇄된 환경에서 자원들의 접근을 보호하기 위하여 특별히 사용할 수 있는 새로운 가능성 제시

(바) SET(Secure Electronic Transaction)

1) 인터넷 기반 전자쇼핑 또는 서비스 규정의 일부로써 은행카드 지불을 지원하기 위하여 비자와 마스터 카드사가 개발한 프로토콜 하부구조

2) 공개키 기반구조는 하향식 계층구조 사용

(사) PGP(Preety Good Privacy)

1) 신뢰성의 확인은 각 사람 자신들의 믿음을 통하여 전달

2) PGP의 공개키 링의 각 키 인증서는 믿음의 유효성과 신뢰성 등급표현

3) PGP의 인증체계 기반기술은 PKI표준과 일치하지 않으며, 개별적인 획득 사용이 쉽지만 대규모의 전자상거래를 지원하기에는 부적합

(아) S/MIME(Secure/Multipurpose Internet Mail Extension)

1) RSA데이터 보안기술 기반하여 MIME 인터넷 전자우편 형식의 표준을 확장 구현

2) PGP가 많은 사용자들에 대하여 개인적 전자우편 보안을 다룬다면, S/MIME은 상업적인 조직의 산업적 표준을 수행

3) X.509의 버전 3에 일치하는 공개키 인증서를 사용

4) 사용된 키 관리구조는 엄격한 X.509 인증서 계층과 PGP의 신뢰모델에 대한 복합적인 방식을 채택

5) S/MIME 관리자 및 사용자들은 PGP처럼 신뢰하는 키의 목록과 CRL을 갖고 각 클라이언트를 구성

(5) 서명 위조와 안전성 개념

(가) 위조에 대한 관점

1) 일반적 위조 불가

o 서명의 위조가 불가능한 문서가 존재

2) 선택적 위조 불가

o 어떤 정해진 문서이외에 대해서는 서명의 위조가 불가능

3) 존재적 위조불가

o 어떠한 문서에 대해서도 서명의 위조가 불가능

(나) 공격에 대한 관점

1) 수동공격

o 공개키만을 사용하여 위조

2) 일반 선택문서 공격

o 선택한 문서에 대한 서명문을 얻은 후 그 정보를 통하여 제 3의 문서의 서명을 위조하는 공격

3) 적응적 선택문서 공격

o 매회 적응적으로 임의로 선택한 문서의 서명문을 얻은 후 그 정보를 통하여 제 3의 문서의 서명을 위조하는 공격

(6) 메시지 복원형과 메시지 부가형

(가) 메시지 복원형 전자서명(Digital Signature Scheme Giving Message Recovery)

이 방식은 RSA와 같이 공개키로 암호화하고 비밀키로 복호화할 때 본래의 메시지가 환원되고, 비밀키로 암호화하고 공개키로 복호화 하여도 본래의 메시지가 환원되는 방식이다. 즉, 서명자가 자신의 비밀키를 이용하여 메시지를 암호화하여 전송하면 검증자가 서명자의 공개키를 이용하여 서명된 암호문을 복호화하여 그 결과가 일정한 규칙을 만족하는 메시지가 되는지를 확인함으로써 서명을 검증하는 방식이다. 이처럼 서명 검증 과정에서 원래의 메시지가 복원되는 방식을 메시

지 복원형 전자서명이라고 한다. 메시지 복원형 전자서명은 기존의 암호 시스템을 이용하기 때문에 별도의 전자서명 프로토콜이 필요하지 않은 장점이 있지만, 메시지를 일정한 크기의 블록으로 나누어 각각의 블록에 대하여 서명을 하여야 하기 때문에 서명의 생성이나 검증과정에서 많은 시간이 소요되는 단점이 있다.

(나) 부가형 전자서명(Digital Signature With Appendix)

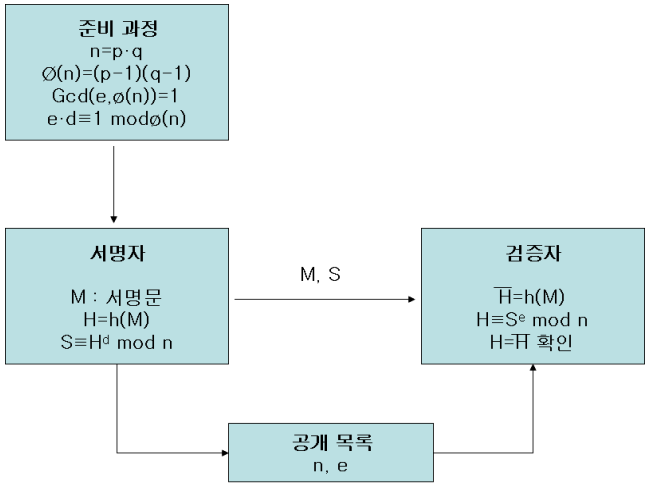
이 방식은 임의의 길이로 주어진 메시지를 해쉬 알고리즘을 이용하여 일정한 크기로 압축하고, 그 해쉬 알고리즘의 결과와 서명자의 비밀키를 이용하여 전자서명을 생성해서 메시지를 덧붙여 보낸다. 이렇게 생성된 서명의 검증은 수신된 메시지를 해쉬한 결과와 전자서명 및 공개키를 이용하여 계산된 값을 비교함으로써 이루어진다. 부가형 전자서명은 메시지 이외에 서명을 별도로 전송해야 하기 때문에 전송량이 조금 늘어나는 반면에 메시지가 아무리 길더라도 단 한 번의 서명 생성만을 필요로 하기 때문에 효율적이라 할 수 있다. 임의의 길이의 메시지를 일정한 길이로 압축해 주는 해쉬 알고리즘은 입력메시지가 조금만 변하더라도 그 해쉬 결과가 전혀 다른 값으로 변하기 때문에 서명의 위조나 메시지의 변조를 막을 수 있다. 따라서 안전한 해쉬 알고리즘을 개발하는 것이 필수적이다. 상기의 두 가지 전자서명 방식 중에서 부가형 전자서명의 장점이 비교적 크기 때문에 현재 세계적인 추세도 부가형 전자서명을 선호하고 있다.

1.2.6 전자서명 예

o 핵심가이드

- RSA 및 ElGamal, Schnorr 전자서명의 이해
- 전자서명 표준(DSS), 국내 표준 전자서명(KCDSA)의 이해
- 타원곡선 전자서명 표준(ECDSA)의 이해 [1급]

(1) RSA 전자 서명



(그림 4-3) RSA 암호 방식을 이용한 전자 서명

(2) ElGamal 전자 서명

ElGamal 전자 서명은 이산대수 문제를 기반으로 정보보호 기능 없이 서명만을 위하여 고안된 방식이다. 서명자는 큰 소수 p를 선택하고 Z_p 상에서 원시원소 g를 선정한다. 서명자는 비밀 서명키로 X를 선택하고 이산대수 문제 $y \equiv g^X \bmod p$를 계산하여 p, q, y를 공개 목록에 공개한다. 이 때 X가 비밀 서명키가 되고 y가 공개 검증키가 된다.

(3) Schnorr 전자 서명

Schnorr의 이산대수를 이용하는 전자서명의 효율성을 높이기 위하여 $q|(p-1)$인 소수의 p, q의 사용을 처음 제안하였다. ElGamal서명의 길이는 RSA서명 길이의 2배이며 지수승의 계산량은 거의 4배에 이른다. 이러한 문제를 해결하기 위하여 Schnorr는 위수 p-1을 갖는 원시 원소를 사용하는 대신, p-1의 소인수 q를 위수로 갖는 생성원을 사용하였다. Schnorr서명을 위한 시스템 변수들은 다음과 같다.

(가) Schnorr서명을 위한 시스템 변수

1) q는 140비트 (또는 160비트) 소수이고 p는 p|q - 1 인 소수이다.

2) g는 위수 q를 갖는 ZE^*_A원소이다($g^q = g^x \bmod p$).

3) 각 사용자는 비밀키 0 < x < q 와 공개키 $y = g^k \bmod p$를 생성한다.

(나) 서명생성과정

1) 난수 0 < x < q을 생성하여 $r = g^k \bmod p$를 계산한다.

2) 서명자는 메시지 M, r의 해쉬값 e=h(M, r)을 계산한다.

3) $s = xe + k \bmod q$ 을 계산한다.

4) (s, e)을 메시지 M의 서명으로 수신자에게 보낸다.

(다) 서명검증과정

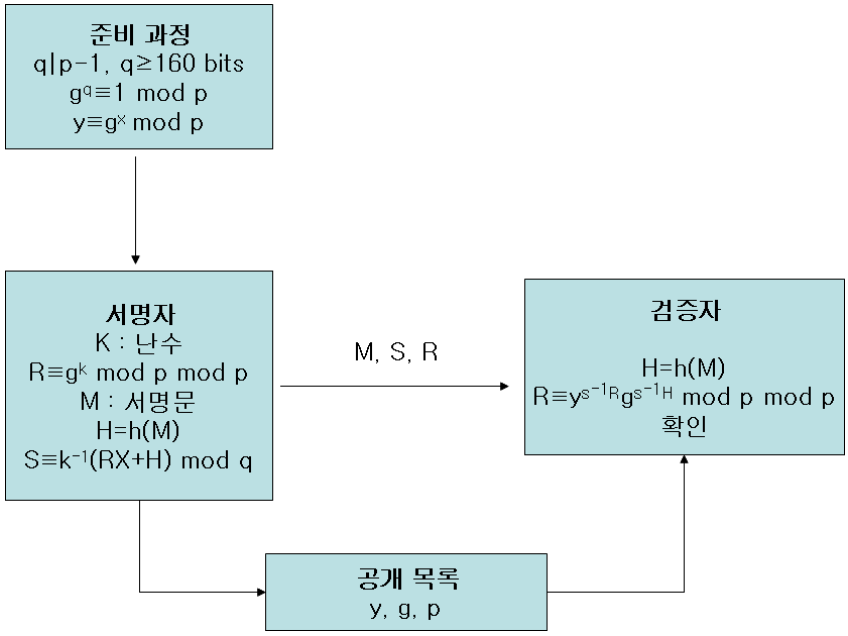
1) $v = g^s \bullet y^{-e} \bmod p$를 계산한다.

2) $e? = h(M,v)$를 확인하여 만족하면 서명으로 받아들인다.

Schnorr 서명에서는 서명 s, e의 사이즈가 소수 q의 비트 사이즈와 같거나 작으며 지수 k의 크기도 q의 크기와 같기 때문에 서명 계산량이 적으므로 ElGamal방식에 비하여 효율적이다. Schnorr 서명이 제안된 이후의 ElGamal형태의 서명 방식들은 p - 1의 소인수 q를 위수로 갖는 생성원을 사용한다.

(4) 전자 서명 표준(DSS = DSA)

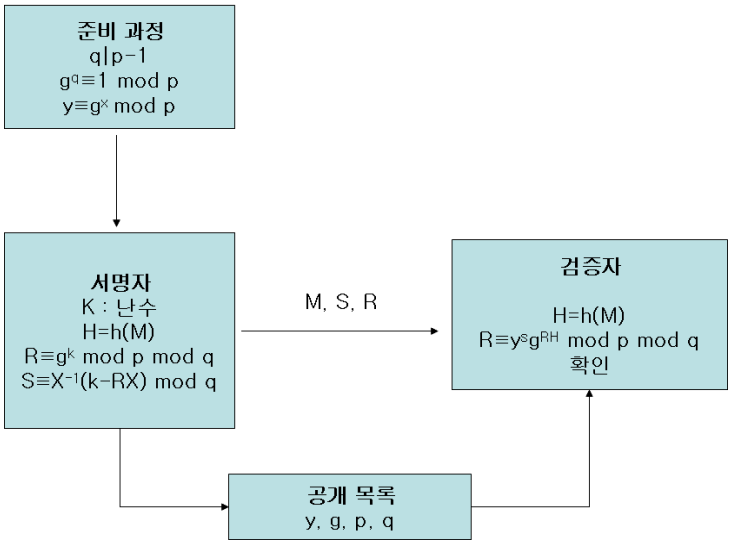
전자 서명 표준은 미국의 전자 서명 표준으로 ElGamal 전자 서명을 개량한 방식이다. 전자 서명 표준은 ElGamal 전자 서명 방식과 유사하지만 서명과 검증에 소요되는 계산량을 획기적으로 줄인 방식이다.



(그림 4-4) 전자 서명 표준(DSS = DSA)

(가) KCDSA 전자 서명

국내 표준 전자 서명 방식



(그림 4-5) KCDSA 전자 서명

(나) 타원곡선 전자서명 표준(ECDSA) [1급]

ECDSA(Elliptic Curve DSA)는 타원곡선(elliptic curve)상에서 군을 정의하고 이에 대한 이산대수 계산의 어려움에 근거를 두고 있다. 타원 곡선 상에서의 이산대수문제는 일반적인 군에서 정의되는 이산대수 문제보다 훨씬 어려우며, 이에 따라, 작은 키로도 RSA보다 높은 비도를 유지할 수 있다. ECDSA는 2000년 2월 8일에 발표된 FIPS 186-2 DSS에 새롭게 포함된 내용으로 타원곡선 전자서명 알고리즘이다. ECDSA(Elliptic Curve DSA)는 DSA를 타원곡선 알고리즘으로 옮긴 것으로 X9.62로 표준화되었다. 따라서 본질적인 알고리즘은 유한체 위에서의 DSA와 동일하다. ECDSA는 DSA 전자서명을 타원곡선을 이용한 전자서명 알고리즘으로 변형한 것으로, 다른 공개키 시스템의 키 길이에 비해서 훨씬 짧은 키를 사용하여도 동일한 안전도를 제공하므로 스마트카드, 무선 통신 등과 같이 메모리와 처리능력이 제한된 분야에서 매우 효과적일 수 있다.

ECDSA을 구현하기 위해서는 타원곡선과 모듈러 연산이 필요하며 키와 서명생성 시 난수 알고리즘이 필요하다. 또한 서명생성 및 검증과정에서는 타원곡선의 상수곱 연산이 필요하다.

1) ECDSA 키 생성

o 간단하게 하기 위하여, 소수체 F_p상에서 정의된 타원곡선 E를 사용한다. P를 $E(F_p)$에 있는 소수위수 q를 갖는 점이라 하자. q가 p보다 훨씬 작아야 하는 DSA에서와는 달리 ECDSA에서는 q는 p와 거의 같은 크기이다. 각 사용자 A는 $1 < x < q-1$인 무작위 정수 x를 선택하여 $xP = Q$를 계산한다.

2) ECDSA 서명 생성

메시지 M을 서명하기 위해 A는 다음을 한다.

o (1단계) $1 < k < q-1$인 무작위 정수 K를 선택한다.

o $kP=(x_1, y_1)$를 계산하고 $r= x_1 \bmod q$를 놓는다. (즉, $x_1 \in \{0, 1, \cdots, p-1\}$, r는 q를 법으로 하는 최소 음이 아닌 잉여류로 택한다.) 만약 r=0 이면 A는 1)단계로 되돌아간다.

o A는 $k^{-1} \bmod q$ 를 계산한다.

o H(M)이 메시지의 해쉬값일 때 A는 $s = k^{-1}(H(M)+x \cdot r)$를 계산한다.
만약 s=0이면 (1)단계로 되돌아간다. (k를 무작위로 선택할 경우 r=0 또는 s=0일 확률은 지극히 작다)

o M에 대한 서명은 (r, s)이다.

3) ECDSA 서명 인증

메시지 M에 대한 A의 서명 (r, s)를 인증하기 위해 다음을 해야만 한다.

o A의 공개키 Q의 확실한 복사본을 얻는다.

o r과 s가 [1, q-1]에 있는지 조사한다.

o $w=s^{-1} \bmod q$와 H(M)을 계산한다.

o $u_1 = H(M)w \bmod q$와 $u_2 = rw \bmod q$를 계산한다.

o $u_1P + u_1Q= (x_0, y_0)=(u_1+u_2)P = s^{-1}(H(M)+xr)P = kP = (x_0, y_0)$와 $u=x_0 \bmod q$를 계산한다.

o 서명을 접수한다. $\Leftrightarrow r = v$.

1.2.7 특수서명 [1급]

o 핵심가이드

- 부인방지 전자서명의 이해
- 은닉서명의 이해
- 위임서명의 이해

(1) 부인 방지 전자 서명

부인 방지 서명은 자체 인증 방식을 배제시켜 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 전자 서명 방식이다. 부인 방지 서명 방식은 서명자가 자신의 서명문을 검증자에게 확인시켜 주는 확인 과정과 추후에 서명자가 자신의 서명임을 부인하지 못하게 하는 부인과정으로 구성되어 있다. 부인방지 서명은 이산 대수 문제를 기반으로 구성된다.

(2) 은닉 서명

은닉 서명 방식은 D.Chaum에 의해서 제안된 서명 방식이다. 서명 용지 위에 묵지를 놓아 봉투에 넣어 서명자가 서명문 내용을 알지 못하는 상태에서 서명토록 한 방식을 수식으로 표현한 것이 은닉 서명이다. 즉, 서명문의 내용을 숨기는 서명 방식으로 제공자(provider: 서명을 받는 사람)의 신원과 서명문을 연결시킬 수 없는 익명성을 유지할 수 있다.

(3) 위임 서명

위임 서명 방식은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 구성한 서명 방식을 말한다. 따라서 위임 서명 방식은 다음 두 가지 조건을 만족해야 한다.

(가) 위임 서명을 생성할 수 있는 사람은 서명자로부터 위임 서명자로 지정된 사람만 가능해야 하며, 제3자는 위임 서명을 생성할 수 없어야 한다.

(나) 위임 서명을 확인하는 검증자는 위임 서명을 위임한 서명자의 동의가 있었음을 확인할 수 있어야 한다.

위임 서명은 위임 방법에 따라 다음과 같이 세 가지로 나눌 수 있다.

자신의 비밀 서명 정보를 직접 위임 서명자에게 알려주는 완전위임 방식, 위임 서명자의 비밀 서명 정보를 서명자가 자신의 비밀 서명 정보로부터 별도로 만들어 주는 부분 위임방식, 그리고 서명자가 위임 서명자로 지정한 사실 증명을 만들어 위임 서명자에게 제공하는 보증 위임방식이 있다. 세 가지 위임 서명 중 실용성과 응용성이 뛰어난 방식이 두 번째 방식인 부분 위임 방식이다. 이 방식은 서명자가 위임 서명자를 통제할 수 있을 뿐 아니라 안전성이 우수하다.

1.3 인증 및 키분배

1.3.1 사용자 인증

o 핵심가이드

- 패스워드를 이용한 개인식별의 문제점과 관리방법
- 시도-응답 개인 식별 프로토콜의 이해 (영지식 프로토콜의 Fiar-shamir와 Schnorr에 대한 이해) [1급]

중요한 정보나 자원을 보호하기 위해서 컴퓨터 통신망에 불법 접속을 시도하는 것을 차단하는 방법이 필요, 이러한 정당한 사용자를 확인하는 과정을 사용자 인증

이라고 한다.

(1) 패스워드를 이용한 개인 식별

특정 사용자가 자신만이 알고 있는 비밀 정보인 패스워드를 사용자 이름과 함께 서버에 제공함으로써 서버의 서비스를 제공받을 수 있는 가장 전통적인 개인 식별 방법이다.

(가) 문제점

- o 통신망을 통하여 원격 접속을 시도할 때 주로 공격자에게 노출되는 패스워드에 대한 불법적인 도청이다.
- o 일반적으로 패스워드는 사용자가 암기하기 쉬운 문자의 열로 이루어지기 때문에 공격자가 추측하기 쉽다.
- o 모든 사용자의 패스워드를 보관하는 시스템 서버의 효율적인 파일 관리의 어려움이다.

1) 패스워드의 추측

패스워드의 추측을 어렵게 만들기 위하여 사용자 자신이 예측하기 어려운 문자열을 사용하는 경우에도 사용자 자신의 편의성을 고려하면 문자열의 길이에 한계가 있다. 이와 같은 상태에서 만들어진 패스워드는 생일 공격 등에 의하여 어렵지 않게 공격된다. 이와 같은 공격으로부터 안전하게 하려면, 현재까지 패스워드에서 대부분 숫자만을 사용하고 있는 것을 영문자 또는 한글이 사용되도록 함으로써 생일 공격에 대응하도록 하는 방법이다.

2) 패스워드 파일

모든 사용자의 패스워드를 보관하고 있는 시스템 파일을 효과적으로 관리하여야 한다. 이를 위하여 패스워드 자체를 그대로 보관하지 않고 해쉬함수를 이용하여 암호화한 값을 보관하고 다음과 같은 시스템을 통하여 접근하도록 한다.

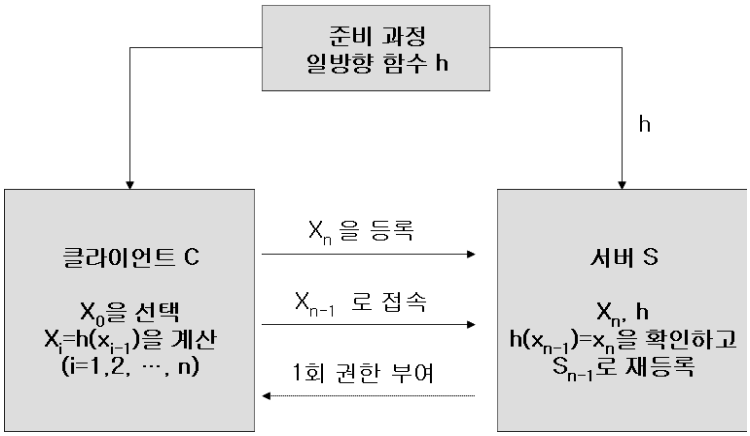
3) 패스워드 관리 방법

사용자 개인이 패스워드를 선택할 때, 시스템 관리자가 일반 사용자에게 패스워드의 중요성과 패스워드를 선택하는 기준을 교육시키므로 일반 사용자가 추측하기 어려운 패스워드를 선정할 수 있도록 도와주는 방법과 안전한 패스워드를 선택하도록 유도하는 방법이 있다. 또한 이들과 병행하여 패스워드의 유효기간을 설정하므로 패스워드를 관리할 수 있다.

4) 일회용 패스워드

유효 기간이 없이 매 세션마다 서로 상이한 패스워드를 사용하면 특별 세션의 개인 식별 과정에서 해당 패스워드가 노출되어도 다음 세션에 사용될 패스

워드를 예측할 수 없는 장점이 있다.



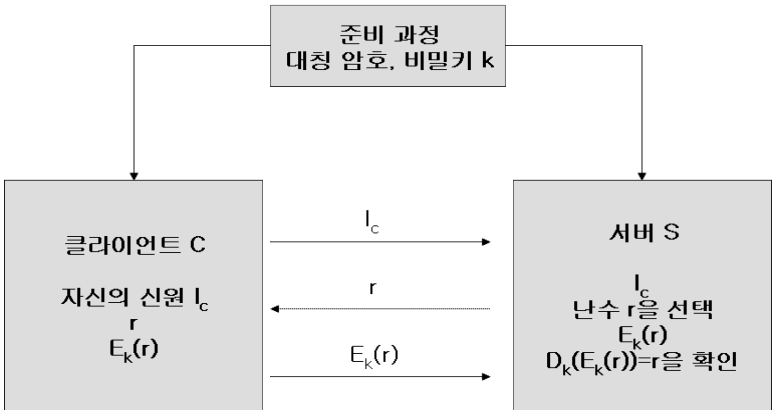
(그림 4-6) Lamport 개인 식별 과정

(2) 시도-응답 개인 식별 프로토콜

대칭형 암호와 공개키 암호에 기반을 둔 시도-응답 프로토콜을 설명한다. 이 프로토콜은 어떤 실체가 자신의 신분을 다른 실체에게 증명하기 위하여 자기 자신만이 소유하고 있는 어떤 비밀 정보를 자신이 알고 있다는 사실을 간접적으로 보여주는 프로토콜이다. 즉, 신분 증명을 요청하는 서버가 신분을 밝히라는 시도를 클라이언트에게 보내면 클라이언트는 그 비밀 정보를 이용하여 적당하게 응답함으로써 서버에게 자신을 증명하는 프로토콜이다. 시도-응답 방식의 개인 식별 프로토콜에서 사용되는 시도는 그 값이 가변적인 난수, 순번, 시각표 등을 사용해야 한다.

(가) 일방향 개인 식별 프로토콜

시스템 서버 또는 클라이언트 중에 어느 한 대상이 다른 대상을 식별하는 프로토콜을 일방향 개인 식별 프로토콜이라 한다.



(그림 4-7) 시도-응답 개인 식별 프로토콜

(나) 상호 개인 식별 프로토콜

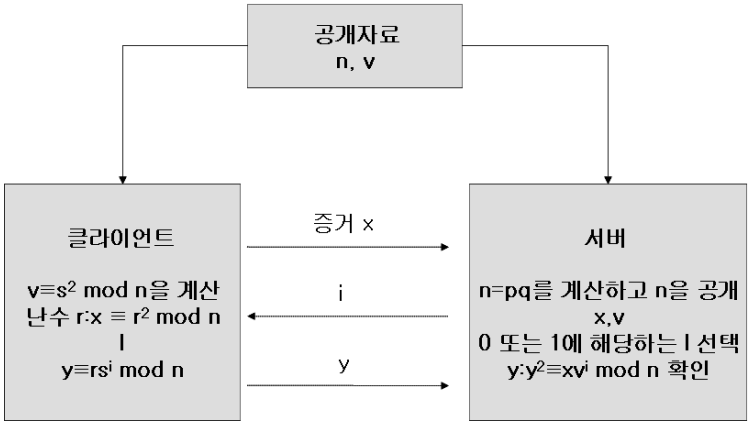
일방향 개인 식별 프로토콜처럼 서버가 클라이언트의 신원을 확인할 수 있는 것과 달리 클라이언트 또한 서버를 확인하기를 원하는 경우가 자주 일어난다. 즉, 서버의 입장과 마찬가지로 클라이언트의 입장에서도 신원 확인을 원하는 상호 개인 식별 프로토콜이 요구된다.

(다) 영지식 기반 개인 식별 프로토콜

자신의 비밀 정보를 서버에게 제공하지 않고 자신의 신분을 증명하는 방식을 영지식 개인 식별 프로토콜이라 한다. 영지식 개인 식별 프로토콜에서 클라이언트는 자신의 신분을 증명해야 하므로 증명자(prover)라 하고 서버는 클라이언트를 확인해야 하므로 검증자(verifier)라고 한다.

1) Fiat-Shamir 개인 식별 프로토콜

Fiat와 Shamir에 의하여 제시된 영지식 개인 식별 프로토콜은 매우 큰 두 소수의 곱을 법으로 하는 어떤 수에 대한 제곱근 계산의 어려움에 기반을 두고 있다.



(그림 4-8) Fiat-Shamir 개인 식별 과정

2) Schnorr 개인 식별 프로토콜

Schnorr에 의하여 제시된 영지식 개인 식별 프로토콜은 매우 큰 소수를 법으로 하는 이산대수 문제의 어려움에 기반을 두고 있다.

(3) 생체인식 <최근 동향> [1급]

생체인식이란 개인의 독특한 생체 정보를 추출하여 정보화시키는 인증방식을 말한다. 지문, 목소리, 눈동자 등 사람마다 다른 특징을 인식시켜 비밀번호로 활용하는 것이다. 즉, 인간의 신체적, 행동적 특징을 자동화된 장치로 측정하여 개인식별

의 수단으로 활용하는 모든 것을 가리킨다. 지문, 얼굴, 홍채, 정맥 등 신체 특징과 목소리, 서명 등 행동특징을 활용하는 분야로 나뉜다.

얼굴모양이나 음성·지문·홍채 등과 같은 개인특성은 열쇠나 비밀번호처럼 타인에게 도용이나 복제될 수 없으며, 변경되거나 분실할 위험성이 없어 보안 분야에 활용된다. 특히 이용자에 대한 사후 추적이 가능하여 관리 면에서도 안전한 시스템을 구축할 수 있다는 장점이 있다.

현재까지 개발된 생체인식 시스템은 신체 일부의 데이터를 획득하는 방법에 따라 분류된다. 현재까지 가장 많이 사용되는 방법은 신체 일부의 영상를 획득하여 특징을 추출 비교하는 것으로 지문인식, 얼굴인식, 망막인식, 홍채인식, 정맥인식, 장문인식 등이 이에 속하며, 음성(화자)인식은 사람의 음성을 이용하는 방법을 사용한다. 생체인식 시스템은 이미지 또는 음성을 획득하는 입력부와 입력된 데이터에서 특징을 추출하고 이를 데이터베이스에 저장되어 있는 특징들과 비교하여 신원을 확인하는 처리부로 구성되어 있다.

1.3.2 메시지 인증

o 핵심가이드

- 관용 암호 방식을 이용한 메시지 인증의 이해
- 공개키 암호 방식을 이용한 메시지 인증의 이해
- 해쉬함수 방식의 이해
- MAC의 이해

정보보안 분야에서 중요한 문제 중에 하나인 메시지 인증은 전달되는 메시지의 이상 유무를 확인할 수 있는 기능으로 전송 중 발생할 수 있는 메시지 내용 변경, 메시지 순서 변경, 메시지 삭제 여부를 확인하는 기능이다. 메시지 인증 방식으로 메시지 암호화 방식, MAC(Message Authentication Code)방식, 해쉬함수를 이용하는 방식 등이 있다.

(1) 메시지 암호화 방식

(가) 관용 암호 방식을 이용한 메시지 인증

A가 메시지 M을 인증하여 검증자 B에게 전달하는 경우에 A, B는 관용 암호 방식을 사용하고 있으므로 사전에 동일한 키를 분배해 갖고 있어야 한다. 이 경우 메시지 인증과 비밀성 서비스가 동시에 제공된다.

사용자 A가 메시지 M을 암호화하여 암호문 $C=E_k(M)$을 전송하면 검증자 B만이 암호문 C에서 메시지 M을 복원할 수 있다. 이 때 복원된 메시지 M이 의미 있는

문장이면 전송 중 메시지 내용 변경, 메시지 순서 변경, 메시지 삭제 등의 공격이 없었음을 확인할 수 있다.

(나) 공개키 암호 방식을 이용한 메시지 인증

공개 암호화키와 비밀 복호화키의 기능을 반대로 이용하면 용이하게 메시지 인증 기능을 실현할 수 있다. 사용자 A는 자신의 비밀 복호화 키 K_{dA}로 암호화하여 암호문 $C=E_{KdB}(M)$를 검증자 B에게 전달한다. 검증자 B는 사용자 A의 공개 암호화 키 K_{eA}로 인증자의 메시지 $M = D_{keA}(C)$를 복호하여 인증을 확인한다.

(다) 해쉬함수 방식

일방향 함수로 메시지 압축 기능을 갖고 있는 해쉬 함수 계산값 H=h(M)를 메시지 M에 부가시켜 M||H를 전송하면 이를 수신한 수신자는 메시지 M으로부터 해쉬값 H를 계산하여 수신한 해쉬값 H를 비교하여 메시지 인증을 할 수 있다.
메시지 인증 기능에 필요한 해쉬함수는 다음 성질을 갖고 있어야 한다.

1) 해쉬함수 h는 임의의 길이의 메시지 M을 입력할 수 있어야 하며 이를 일정 길이의 해쉬값 H로 출력할 수 있어야 한다.
2) 해쉬함수 h는 어떠한 메시지 입력에도 해쉬값 H의 계산이 간단해야하며 하드웨어 혹은 소프트웨어 구성이 용이해야 한다.
3) 어떠한 해쉬값 H에 대해서도 h(M) = H가 되는 메시지 M을 찾는 것이 계산상 불가능해야 한다.
4) 어떠한 메시지 M과 그의 해쉬값 H=h(M)이 주어졌을 때 h(M′)=H이 되는 메시지 M≠M′를 찾는 것이 계산상 불가능해야 한다.
5) h(M) = h(M′)가 되는 메시지 M≠M′를 찾는 것이 계산상 불가능해야 한다.

성질 1), 2)는 해쉬함수의 일반적인 성질로 간단하고 효율적인 메시지 인증 구성방법을 제공한다. 성질 3), 4), 5)는 메시지 인증 기능을 의미한다.

(라) MAC

관용 암호 방식을 이용하여 메시지 M으로부터 작은 길이의 암호학적 checksum이나 MAC(Message Authentication Code)을 만들어 메시지에 부가시키는 방법. 관용 암호 방식을 사용하기 때문에 메시지 인증을 하는 사용자와 검증자는 사전에 관용 암호 방식용 암호키 K를 나누어 갖고 있어야 한다.
사용자 A는 인증할 메시지 M과 암호화 알고리즘에 암호키 K를 적용시켜 메시지 M의 MAC = $E_k(M)$을 계산하여 메시지 M과 함께 검증자 B에게 전송한다. 메시

지 M과 MAC를 수신한 검증자 B는 메시지 M과 자신이 비밀리에 보관하고 있는 암호키 K을 이용하여 사용자 A가 계산한 방법으로 MAC을 계산하여 수신한 MAC을 비교한다.

1.3.3 키 분배 프로토콜 [1급]

o 핵심가이드

- 열쇠 사전 분배방법 (Diffie와 Hellman의 열쇠 사전분배 방법)의 이해
- 온라인 열쇠 분배방법 (Kerberos, Diffie-Hellman)의 이해
- 키 로밍

암호 방식에서 키 관리는 키의 생성에서부터 키 분배, 키 설치, 키 갱신, 키 취소, 키 폐기, 키 저장, 키 복구 등을 포함하는 포괄적인 개념이다. 이들 개념 중에 암호 방식을 구현하기 위하여 먼저 요구되는 것이 한 사용자 또는 기관이 비밀키를 설정하여 다른 사용자에게 전달하는 기술이다. 이 기술을 키 분배라 한다. 한편, 둘 또는 더 많은 사용자가 공개된 통신로를 통하여 공동으로 비밀키를 설정하는 기술을 키 공유라 한다. 열쇠분배 또는 열쇠공유 프로토콜의 목적은 관련된 사용자들이 같은 열쇠를 소유하고 열쇠가 신뢰되는 열쇠관리기관(TA, trusted authority)을 제외하고는 알려지지 않도록 하여 비밀정보를 보호하는 것이다. 이와 같은 프로토콜을 설계하는 것은 쉬운 일이 아니며, 프로토콜을 설계할 때에 생각할 수 있는 방안으로 TA에 의한 열쇠 사전분배(key predistribution)와 온라인 열쇠분배(on-line key distribution)가 있다.

(1) 열쇠 사전분배

열쇠 사전분배란 TA가 사전에 임의의 두 사용자(A, B)에게 비밀 경로를 통하여 임의 열쇠 $K_{A,B}=K_{B,A}$를 선택하여 전달하는 방법이다. 이 방법은 일반적으로 TA와 네트워크상의 모든 사용자 사이에 안전한 통로가 필요하며, 소수의 사용자들에게는 무조건적으로 안전할 수 있지만 사용자가 많은 경우에 TA는 물론 사용자들도 많은 열쇠를 관리해야 하는 문제점을 가지고 있다. 즉, n명의 사용자가 있다면 각 사용자는 n-1개의 열쇠를 관리하여야 하고 TA는 n(n-1)/2개의 열쇠를 관리하여야 하므로 매우 복잡하며 관리비용이 많이 지불되어야 한다.

(가) Diffie와 Hellman의 열쇠 사전분배 방법

유한체 Z_p의 원시근 α와 p를 모든 네트워크 사용자에게 공개하고 각 사용자 A는 자신의 비밀지수 a_A를 정하고 $b_A \equiv \alpha^{aA} \bmod p$ 를 계산하여 공개한다. Diffie-Hellman 암호 알고리즘에서와 같이 α^{aA}과 α^{aB}을 알고 α^{aAaB}을 구하기 어려

운 점을 이용한 열쇠교환방법이다.

[표 4-12] Diffie-Hellman 열쇠 사전분배 방법

1단계 : 소수 p와 원시근 $\alpha \in Z_p^*$ 를 공개한다. 2단계 : B는 A의 인증서로부터 공개된 값 b_A와 자신의 비밀열쇠 a_B를 함께 사용하여 $K_{A,B}$ 값을 계산한다. $K_{A,B} \equiv \alpha^{aAaB} \bmod p \equiv b_A^{aB} \bmod p$ 3단계 : A는 B의 인증서로부터 공개된 값 bB와 자신의 비밀열쇠 aA를 함께 사용하여 KA, B값을 계산한다. $K_{A,B} \equiv \alpha^{aAaB} \bmod p \equiv b_B^{aA} \bmod p$

(2) 온라인 열쇠분배

TA가 네트워크상의 모든 사용자와 필요할 때마다 열쇠를 공유하는 방법이다. 즉, 사용자 A와 B가 비밀통신을 원할 때 TA에게 작업시간을 포함하는 세션열쇠를 요구하게 되고 TA는 열쇠를 생성하여 A와 B가 복호할 수 있도록 암호화된 상태로 열쇠 K를 전달하는 방법이다.

(가) Kerberos

온라인 분배방법 중 비밀열쇠 암호작성법에 기초를 둔 자주 이용되는 온라인 열쇠 분배방법이 Kerberos이다.

[표 4-13] Kerberos를 이용한 세션키의 전송

1단계 : A는 TA에게 B와 통신할 수 있는 세션키를 의뢰한다.
2단계 : TA는 세션키 K와 요청된 시간인 타임스탬프 T와 제작시간인 라이프타임 L을 임의로 선택한다.
3단계 : TA는 m_1과 m_2를 아래와 같이 계산하여 A에게 보낸다. $m_1=e_{KA}(K, ID(B), T, L)$, $m_2=e_{KB}(K, ID(A), T, L)$
4단계 : A는 TA로부터 얻은 m_1을 복호함수 d_{KA}를 이용하여 계산하여 K, T, L과 ID(B)를 얻고 $m_3=e_k(ID(A), T)$를 계산하여 TA로부터 얻은 m_2와 함께 B에게 보낸다.
5단계 : B는 TA로부터 얻은 m_2를 복호함수 d_{KB}을 이용하여 계산하여 K, T, L와 ID(A)를 얻고 m_3로부터 d_K를 이용하여 계산하여 T, ID(A)를 얻어서 두 개의 T와 ID(A)값들을 비교한다. 이 때, 그 값들이 각각 모두 같다면 $m_4=e_K(T+1)$를 계산하여 A에게 보낸다.
6단계 : A는 d_K를 사용하여 m_4를 복호한 후, 그 결과가 T+1인지를 확인한다.

(나) Diffie-Hellman 열쇠교환

공개키 암호 부분 참조

(다) 키 로밍

키 로밍 기술은 사용자가 별도의 저장매체 없이도 인터넷이 연결되는 모든 단말기에서 키 로밍 서버로부터 자신의 개인키를 다운받아 암호서비스를 이용할 수 있는 기술로 저장매체의 손·망실 문제를 해결하고 사용자에게 이동성을 제공한다.

1.3.4 영지식 증명 [1급]

o 핵심가이드

- 영지식 증명의 개념과 과정
- 영지식 증명 프로토콜의 예
- 영지식 비대화형 증명의 이해

(1) 영지식 증명의 개념

영지식 증명체계(zero-knowledge proof system)란 한사람이 다른 사람에게 사실의 증명에 관한 어떤 정보도 보이지 않고, 사실의 증명을 알고 있음을 확신하도록 만드는 방법 즉, 정보를 전혀 주지 않고 상대방에게 정보를 알고 있음을 증명하는

방법.

(가) 준비과정

1) 적당한 집합이 정해진다.

(나) 증명과정

1) 증명자는 정해진 집합 내에서 임의로 선정된 난수에 대한 증거를 계산하여 검증자에게 제시한다. 여기에서 증거는 정당한 증명자만이 알고 있는 비밀 정보를 알고 있다는 사실을 검증자에게 입증시키는 방법이다.
2) 검증자는 증거를 이용하여 여러 개의 질문을 증명자에게 제시한다.
3) 증명자는 검증자가 제시하는 모든 질문에 대답함으로써 정당한 클라이언트임을 확인시킨다. 이때 대답의 내용은 증명자의 비밀 정보를 유추할 수 있는 어떤 정보도 포함되지 않아야 한다.

(2) 영지식 증명 프로토콜의 예

(가) 대화형 증명 시스템

{0 ,1}* 상의 언어 L에 대하여, 대화형 프로토콜인 프로토콜 (P, V)가 다음의 두 조건을 만족할 때, 대화형 증명 시스템이라 한다.

1) completeness(완전성)

(P, V)에 주어지는 임의의 입력 x∈L에 대하여 임의의 c > 0인 적어도 1-｜x｜$^{-c}$의 확률로 중지하고 수리한다.

$$Prob((P, V) \text{ accepts } x) = 1 - |x|^{-c}$$

2) soundness(건전성)

임의의 대화형 튜링 기계인 P*, (P*, V)에 주어지는 임의의 입력 x∉L에 대하여, 임의의 c>0인 기껏해야 ｜x｜$^{-c}$ 의 확률로 중지하고 수리(accept)한다.

$$Prob((P^*, V) \text{ accepts } x) = |x|^{-c}$$

쉽게 설명하면, 완전성은 증명이 올바르다면, 검증자 V는 1 또는 1에 아주 가까운 압도적인 확률로 수리하며, 건전성은 증명이 옳지 않으면, 증명자가 어떠한 능력을 가졌다할지라도 검증자 V는 압도적인 확률로 거부(reject)한다는 것을 의미한다. 대화형 증명 시스템에서는 완전성면에서 반드시 1이 되는 것은 불가능하지만, 상호 대화를 계속하여 반복하면 확률 1에 가까워지게 된다. 물론 가까워지는 속도는 지수 함수적이며 고속으로 근접하게 된다.

(나) Quadratic Residue 문제의 영지식 대화 증명 프로토콜

mod n에 대한 x의 quadratic residue 문제에 대한 영지식 증명 시스템 (P, V)는 다음과 같이 구성한다.

1) 증명자 P는 랜덤 수 r을 선택한 후, r^2 mod n을 검증자 V에게 전송한다.

2) 검증자 V는 랜덤 비트 b를 선택한 후, P에게 전송한다.

3) P는 랜덤 비트 b의 값에 따라 아래의 y를 V에게 전송한다.

o b=0이면, y= r mod n

o b=1이면, y= $r \cdot x^{1/2}$ mod n

4) V는 다음을 확인한다.

o b=0이면, y= r^2 mod n^2

o b=1이면, y^2= $r^2 \cdot x$ mod n

(3) 영지식 비대화형 증명 (ZHNIP)

영지식 대화 증명의 비효율성을 개선하기 위한 방법이다. 영지식 비대화 증명은 M.Blum, P.Feldman, S.Micali에 의하여 제안되었으며, DeSantis, Micali, Persiano, Bellare와 Goldwasser 그리고 Naor와 Yung에 의하여 더욱 발전되었다. Blum 등의 제안은 영지식 비대화 증명의 개념을 소개하고 세 개의 소수곱으로부터 2개의 소수곱을 구별하는 것이 어렵다는 가정 하에 computationally ZKNIP가 존재함을 보였다. 또한, 적응 선택 암호문 공격에 대하여 안전성 증명 가능한 공개키 암호 시스템을 만드는데 ZKNIP가 적용될 수 있음도 보였다.

영지식 비대화 증명의 개략적인 정의로, 언어 L 상의 NIP(Non-Interactive Proof) (P, V)는 증명자 P만이 x∈L이라는 증거만을 검증자 V에게 보내며, 검증자 V는 P에게 아무것도 요청할 수 없으며 증명 과정 전에 동일하나 랜덤 테이프를 사전 공유하고 있다고 가정한다. 그리고 언어 L상의 ZKINP(P, V)는 NIP의 정의에 추가하여, 검증자 V가 x∈L이라는 정보 이외에는 어떠한 추가적인 정보도 얻지 못하는 영지식성 프로토콜이다.

1.4 최근동향 [1급]

1.4.1. 워터마킹

전체 파일 크기를 변화시키지 않고 저작권자가 불법복제여부를 파악할 수 있는 정보를 삽입하는 기술을 말한다.

워터마킹은 텍스트, 이미지, 비디오, 오디오 등의 데이터에 원 소유주만이 아는 마크(Mark)를 사람의 육안이나 귀로는 구별할 수 없게 삽입하고 이를 네트워크에서 제공한다. 만약 사용자들이 멀티미디어 디지털 정보를 불법 복제하여 정당한 대가나 허락 없이 상업용 혹은 기타 용도로 사용되었을 때에는 자신의 '마크'를 추출함으로써 자신의 소유임을 밝힐 수 있고, 이는 재산권 행사에 결정적인 증거가 된다.

워터마크를 나타내는 실제 비트들은 그것들이 식별되거나 조작되지 않도록 파일 전체에 걸쳐 퍼져 있어야만 한다. 그리고 마지막으로, 디지털 워터마크는 그 파일에 대한 일반적인 변경, 예를 들어 로씨 압축알고리즘에 의한 축소 등에 견딜 수 있도록 충분히 견고해야만 한다.

워터마킹은 저작권 보호를 위한 영역에서 소유권의 증명정보, 불법복제추적, 복제방지(기기제어), 방송모니터링, 위변조 적발 및 방지, 데이터 은닉등의 용도로 사용할 수 있다.

1.4.2. 스테가노그래피(Steganography)

스테가노그래피(steganography)는 전달하려는 기밀 정보를 그래픽, 사진, 영화, 소리(MP3)파일 등에 암호화해 숨기는 심층암호 기술로써, 정보를 교환하고 있다는 것을 숨기면서 통신을 하는 기술이다.

스테가노그래피는 암호화 기법과는 달리, 정보를 전송하는데 있어서 많은 양의 오버헤드를 요구한다, 즉 간단한 정보를 전송하기 위해서 보내고자 하는 정보와는 관계가 없는 많은 양의 데이터를 함께 전송해야 한다는 단점이 있는 것이다.
현재 멀티미디어 데이터 중에서 비교적 쉽게 다룰 수 있는 정지 영상 데이터를 이용한 스테가노그래피 기법이 많이 개발되어 있고 그중에 대표적인 방법 중 하나가 디지털 정지 영상 데이터에 정보를 숨기는 대표적인 방법 중 하나가 LSB(Least Significant) insertion 방법이다. 이 밖에도 변환공간영역(transformed domain)에서 스테가노그래피를 하는 기법도 많이 사용되고 있는데, 대표적인 것이 JPEG 압축 알고리즘에 사용된 DCT(Discrete Cosine Transform) 영역에서 메시지를 숨기는 방법이 있다.

스테가노그래피는 암호화를 대신하는 것이 목적이 아니라, 암호화와 함께 스테가노그래피 기법을 사용해서 보안 수준을 더욱 높이는 것이 목적이다.

2. 정보보호 관리

2.1 정보보호 관리 개념

2.1.1 정보보호의 목적 및 특성

o 핵심가이드

- 정보보호의 필요성 이해
- 정보보호의 정의
- 정보보호의 목적

(1) 정보보호의 필요성

산업사회에서 정보화 사회로 바뀌면서 오프라인에서 수행되던 일이 대부분 온라인으로 수행 가능해 지고 있다. 하지만 정보화의 순기능과 함께 개인정보가 노출, 악용되는 등의 사례가 증가함에 따라 사생활이 침해되거나, 조직 내 중요 정보가 오용과 악의적인 의도에 의해 유출되는 등의 치명적인 정보화의 역기능이 발생하게 되었다. 정보화 역기능의 사례는 지속적으로 증가하고 있으며 사용되고 있는 기술도 정보기술과 함께 발달하고 있으므로, 정보보호의 필요성이 더욱 중요시되고 있다.

(2) 정보보호의 정의

정보보호(Information Security)란 의도되었건 의도되지 않았건 간에, 인가받지 않은 노출, 전송, 수정 그리고 파괴로부터 정보를 보호하는 것을 말하는 것으로, 정보화촉진기본법 제2조에서는 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 강구하는 것을 말하고 있다.

(3) 정보보호의 목적

(가) 기밀성 서비스

(나) 무결성 서비스

(다) 인증서비스

(라) 접근제어 서비스

(마) 부인방지 서비스

(바) 감사추적 서비스

2.1.2 정보보호와 비즈니스

o 핵심가이드

- 비즈니스에서의 정보보호의 필요성
- 정보보호 모델

(1) 정보보호의 필요성

(가) 전자상거래, 전자정부 등 사이버 공간에서의 활동 증가에 따른 안전성, 신뢰성 해결

(나) 글로벌화에 따른 국내 정보 유출 우려

(다) 공공기관에서 소유하고 있는 개인의 정보

(라) 회사의 제품개발 및 축적기술

(마) 회사간의 각종 사업계획에 관한 정보교환 및 사업행위

(바) 각종 지적소유권 보호

(2) 정보보호 모델

(가) ISMS (정보보호관리체계)

1) 정보보호관리체계는 정보보호의 목적인 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립•문서화 하고 지속적으로 관리•운영하는 시스템이다.

2) 조직에 적합한 정보보호를 위해 정책 및 조직수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 정리하고 이를 통해 구현된 여러 정보보호 대책들이 유기적으로 통합된 체계(정보보호관리체계)를 갖추었는지 제 3자의 인증기관(한국정보보호진흥원)을 통해 객관적이고 독립적으로 평가하여 인증기준에 대한 적합 여부를 보증해 주는 제도

2.1.3 정보보호 관리의 개념

o 핵심가이드

- 정보보호관리의 개념 이해

조직이 가지고 있는 취약점을 찾아내 이를 보완할 수 있는 다양한 통제 방안을 도입함으로서, 조직의 정보에 대한 다양한 위협들로부터 정보를 보호하기 위한 체

계로서 효율적인 정보보호 관리 체계를 구축하기 위해서는 체계적인 절차가 필요하다. 각 조직은 자신의 정보보호 요구사항에 따라 필요한 통제들을 적절히 선정하여 효율적인 정보보호 관리 체계(ISMS : Information Security Management System)를 구축한다.

정보보호관리를 이행하기 위해서 조직은 정보보호정책 및 조직수립, 범위설정 및 정보자산 식별, 위험관리, 구현, 사후관리활동으로 구성된 6단계의 논리적이고 체계적인 정보보호관리 프레임워크를 수립하고, 기획, 관리하여야 한다.

2.1.4 정보보호 관리와 타 관리 기능간의 관계 [1급]

(1) 구성관리

(2) 성능관리

(3) 계정관리

(4) 문제관리

(5) 서비스수준관리 등 관리기능과 정보보호관리기능과의 관계

(6) 통합정보보호관리의 의미와 접근방법

정보보호관리는 조직의 자산에 대한 안전성 및 신뢰성을 향상시키기 위해 관리, 운영하여 정보보호의 목표인 비밀성, 무결성, 가용성을 실현한다.

2.2 정보보호 정책 및 조직

2.2.1 정보보호 정책의 의미 및 유형

o 핵심가이드

- 정보보호정책의 상세내용 및 구성
- 정보보호정책의 절차 및 대책수립

정보보호정책은 조직의 정보보호에 대한 방향과 전략 그리고 정보보호 프로그램의 근거를 제시하는 매우 중요한 문서이다. 따라서 정책의 의미, 유형, 수립과정, 포함될 내용을 이해하여야 한다. 또한 정보보호 프로그램이 조직 내에서 효과적으로 수행되기 위해서는 정보보호에 대한 책임과 역할이 명확히 구명되어야 하고 이것이 조직 체계로서 구현되어야 한다. 따라서 정보보호를 위한 조직의 유형과 역할, 구성 등에 대한 이해가 필요하다.

정보보호 정책은 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술이다. 또한 정보보호 임무를 관리하기 위한 수단이다.

2.2.2 정보보호정책 수립과정 및 내용 [1급]

o 핵심가이드

- 정보보호정책의 목표
- 정보보호목표를 선정할 때의 고려 사항
- 정보보호정책의 특징 이해

(1) 정보보호정책의 정의

정보보호정책은 어떤 조직의 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술이다.

(2) 정보보호정책의 목표

조직의 정보보호정책 목표는 조직이 달상하고자하는 목표와 달성방법(전략), 그리고 목표달성을 위한 정책을 조직의 각 단계 및 사업 단위 또는 부서별로 정의하여야 하며, 효율적인 정보보호 정책을 위해서 각각의 조직 수준과 사업 단위별로 다양한 목표, 전략, 정책을 수립하여야 한다.

(3) 정보보호정책의 필요성

정보보호와 관련된 결정은 대부분 정보보호 관리자가 네트워크의 안전여부, 제공기능, 사용하기 쉬운 방법에 대해 결정했을 때에 만들어진다. 정보보호정책의 목표를 결정하지 않고서는 보안에 관하여 적절한 결정을 할 수 없다. 정보보호목표를 결정할 때까지는 무엇을 점검하고 무엇을 제한할 것인지를 전혀 알지 못하기 때문에 어떤 보안도구도 효과적으로 사용할 수 없다.

(4) 정보보호목표를 선정할 때의 고려 사항

(가) 서비스 제공

사용자에게 제공하는 서비스의 이점이 위험의 비중보다 크다면 정보보호관리자는 사용자들의 위험으로부터 서비스를 안전하게 사용할 수 있도록 보호대책을 수립하여야 한다.

(나) 용이성

누구나 쉽게 시스템에 접근하여 사용할 수 있다면 사용하기에 편리할지 모르지만, 각종 위험으로부터 완전히 노출되어 있다고 해도 과언이 아니다. 따라서 정보보호관리자는 시스템 사용의 용이성이 다소 떨어지더라도 시스템의 안전을 최우

선 과제로 선정해야 한다.

(다) 정보보호 비용과 손실위험

정보보호를 하기 위해서는 비용이 많이 소용되므로 사생활에 대한 손실 서비스에 대한 손실 등으로부터의 각 비용의 형태는 손실의 형태에 따라서 신중하게 결정해야 한다. 정보보호정책의 영역이 정보기술, 저장된 정보, 기술에 의해 조직된 정보의 모든 형태를 포함한다.

정보보호정책의 내용에는 다음과 같은 최소한의 표준을 포함하여야 한다.

1) 필요한 보호의 수준에 따른 자산의 분류
2) 비인가 된 접근으로부터의 정보 보호 원칙
3) 정보의 기밀성 보장, 무결성 유지
4) 정보 및 정보시스템의 가용성에 관한 사업 요구사항
5) 물리적, 논리적, 환경적 보안 및 통신보안
6) 준수하여야 할 법, 규정 및 계약 요구사항
7) 시스템 개발 및 유지 방법론
8) 비상대책 계획의 수립, 유지, 점검
9) 모든 직원에 대한 정보보호 교육훈련
10) 정보시스템 정책 위반에 대한 징계 또는 처벌
11) 정보시스템 보안사고 보고 및 조사
12) 준수해야 할 표준, 관례 및 절차와 바이러스 방지, 패스워드, 암호화를 포함하는 정보보호정책 지원 수단의 구현

(5) 정보보호정책의 특징

수용 가능한 지침 또는 다른 적절한 방법을 수립하고 시스템 관리절차를 통해 구현이 가능해야 하며, 예방이 기술적으로 불가능한 곳에서 인가에 의해 적절한 경우에 보안도구가 실행 가능해야 한다. 또 사용자, 관리자, 기술요원에 대한 책임 영역이 명확하게 정의되어야 한다.

2.2.3 조직 체계와 역할/책임

o 핵심가이드

- 조직 체계의 역할과 구성원들의 책임
- 조직의 정보보호 정책요소

정보보호조직은 적합한 정보보호정책을 계획, 구현, 승인, 감독할 수 있는 조직

체계를 수립하여야 하며, 모든 조직은 독자적인 체계를 가지고 이에 적합한 방식으로 정보보호와 관련된 직무를 할당하여야 한다.

(1) 역할

(가) 사고 대응팀/정보보호 위원회의 역할

1) 전략적 보안 계획과 관련하여 IT운영위원회에 조언
2) IT전략적 지원에 관련하여 조직 IT 정보보호정책을 수립하고 IT 운영위원회로부터 승인 획득.
3) 조직 IT정보보호정책을 IT보안 프로그램으로 전환
4) IT보안 프로그램 실행을 모니터링
5) 조직 IT보안 정책의 유효성 검토
6) IT 보안 문제 인식 촉진
7) 계획 프로세스를 지원 및 IT 보안 프로그램 실행을 지원하는데 필요한 자원(인력, 예산 등)에 입각하여 조언.

(나) 정보시스템 관리 책임자의 주요 임무

1) IT 보안 프로그램 실행을 감독
2) 정보보호 관리팀 및 조직 정보보호 임원에 대한 연락 및 보고
3) 조직 IT 보안 정책과 지침을 유지
4) 사고 조사 조정
5) 조직의 전반적인 보안 인식 프로그램 관리
6) IT 프로젝트 및 시스템 보안 담당의 권한 결정

(다) 프로젝트 보안 담당과 시스템 보안 담당의 주요 임무

1) 정보보호 관리팀 및 조직 IT보안 담당에 대한 연락 및 보고
2) IT 프로젝트 또는 시스템 보안 정책을 수립, 유지
3) 정보보호 계획을 개발, 구현
4) IT 대책의 구현 및 사용을 모니터링
5) 사고 조사의 착수, 지원

(2) 책임

구성원의 역할과 책임 및 권한을 명확히 규정하여 모든 직원이 이를 이해하도록 한다.

(가) 최고 경영자

정보보호를 위한 총괄책임이 있다.

(나) 정보시스템 정보보호 관리자

조직의 정보보호 정책, 표준, 대책, 실무 절차를 설계, 구현, 관리, 조사할 책임이 있다.

(다) 데이터 관리자

정보시스템에 저장된 데이터의 정확성과 무결성을 유지하고 데이터의 중요성 및 분류를 결정할 책임이 있다.

(라) 프로세스 관리자

해당 정보시스템에 대한 조직의 정보보호 정책에 따라 적절한 보안을 보증할 책임이 있다.

(마) 기술지원 인력

보안대책의 구현에 대하여 조언할 책임이 있다.

(바) 사용자

조직의 정보보호 정책에 따라 수립된 절차를 준수할 책임이 있다.

(사) 정보시스템 감사자

보안 목적이 적절하고 정보보호 정책, 표준, 대책, 실무 및 절차가 조직의 보안 목적에 따라 적절하게 이루어지고 있음을 독립적인 입장에서 관리자에게 보증할 책임이 있다.

(3) 조직의 정보보호 정책요소

(가) 자산 소유자의 관점에서 본, 기밀성, 무결성, 가용성, 책임 추적성, 신뢰성에 관한 IT 보안 요건

(나) 조직의 기반 구조 및 책임 할당

(다) 시스템 개발, 조달과 보안의 통합

(라) 지침과 절차

(마) 정보 분류 등급 규정

(바) 위험 관리 전략

(사) 비상 계획

(아) 문제(유지보수 인력 및 시스템 관리와 같이 신뢰를 필요로 하는 지위의 인력에 특별한 주의를 기울여야 한다.)

(자) 인식, 훈련

(차) 법과 규제의 준수

(카) 외주 관리

(타) 사고 처리

2.2.4 예산 수립 및 정당화 방법 [1급]

o 핵심가이드

- 예산 수립시 고려해야할 사항
- 정보보호 예산/투자에 대한 정당화기법
- ROSI, TCO

(1) 정보자산의 식별

조직의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다. 자산 식별을 통하여 조직의 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, 정보자산과 업무처리와의 관계도 알아낼 수 있다. 자산평가는 위험분석 결과의 정확도를 결정하는 매우 중요한 과정이다.

자산평가 과정은 자산조사와 자산가치산정의 2가지로 나눌 수 있으며, 자산조사 과정에서는 조사할 자산의 범위를 설정하고, 자산목록을 작성한다. 자산가치산정 과정에서는 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의한다.

(그림 4-9) 자산식별 과정

(2) 자산가치 산정

자산가치 산정은 자산의 중요도를 파악하고 위협이 발생할 경우 있을 수 있는 피해를 측정하기 위한 정보를 얻기 위해 위험분석 대상 자산의 가치를 정량 또는 정

성적인 방법으로 평가하는 과정이다.

정량적 기준은 자산 도입 비용, 자산 복구비용, 자산 교체 비용이 기준이며, 정성적인 기준은 업무처리에 대한 자산의 기여도, 자산이 영향을 미치는 조직과 작업의 수, 시간(복구시간), 기타(조직의 특성에 맞는 기타요소)가 기준이 된다.

2.3 위험관리

2.3.1 위험관리 전략 및 계획수립

o 핵심가이드

- 위험관리 전략 및 방법의 이해
- 위험분석의 정의
- 위험분석의 절차와 요소
- 위험관리 용어

(1) 위험의 정의

위험이란 비정상적인 일이 발생할 수 있는 가능성을 말하며, 위험분석은 위험을 분석하고 해석하는 과정으로 조직 자산의 취약성을 식별하고, 위협분석을 통해 발생 가능한 위험의 내용과 정도를 결정하는 과정이다.

(2) 위험관리의 정의 및 목적

위험관리란 위험을 평가하고, 피해자가 수용할 수 있는 수준까지 위험 부담을 줄이기 위한 조치를 강구하며 그러한 위험을 용인할 수 있는 수준으로 유지하는 것을 말한다. 위험의 측정과 관리를 통하여 다양한 위협요소로 인해 피해를 최소화하거나 막기 위함이다.

(3) 위험관리의 구분

(가) 정보보호정책을 바탕으로 각 조직에 적합한 전반적인 위험관리 전략의 결정

(나) 위험분석 활동의 결과 혹은 기본 통제에 따른 개별 IT 시스템에 대한 대책의 선택

(다) 보안 권고에 의거한 IT 시스템 보안 정책의 정형화, 조직의 정보보호 정책

(라) 승인된 IT시스템 보안 정책을 토대로 하여 대책을 구현하기 위한 IT 보안 계획의 수립

(4) 위험관리 계획

위험관리는 크게 위험분석, 위험평가, 대책설정 3가지의 과정으로 구분된다.

(가) 위험분석

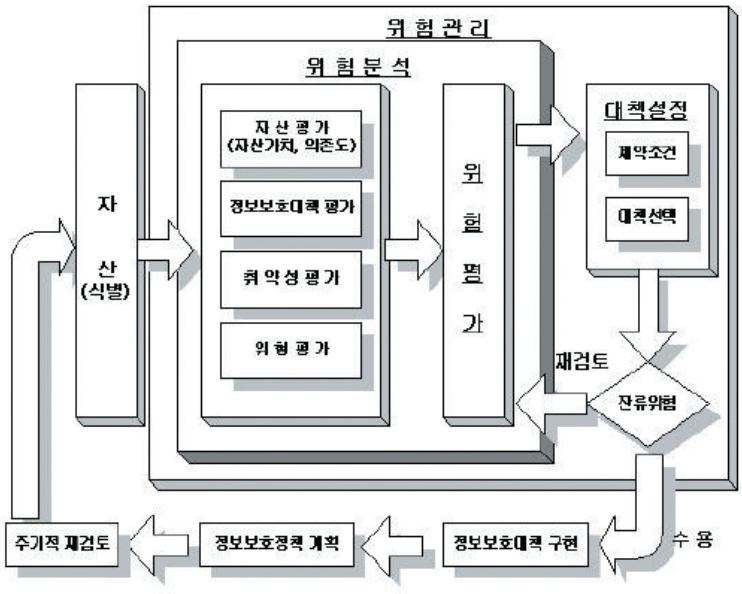
통제되거나 받아들여질 필요가 있는 위험을 확인하는 것이다. 위험분석은 자산 가치평가, 위협, 취약성을 포함하며, 모든 시스템에 대한 간단한 초기분석을 통해 불필요한 시간과 자원의 투자 없이 실행할 수 있다.

(나) 위험평가

위험평가의 목적은 적절하고 정당한 보안 대책을 선정하고 식별하기 위하여 시스템 및 그 자산이 노출된 위험을 평가하고 식별하기 위한 것이다. 위험은 위험에 처한 자산, 잠재적인 불리한 업무충격을 유발하기 위해 발생하는 위협 가능성, 식별된 위협으로 인한 취약성의 용이한 사용 및 위험을 감소시키는 기존의 혹은 계획된 어떤 대책에 따른 새로운 위협 가능성 등을 포함한다.

(다) 대책설정

허용가능 수준으로 평가된 위험을 줄이기 위해 적절하고 정당한 대책을 식별 및 선정한다. 대책은 위협을 방지하고, 취약성을 감소시키고, 원치 않는 사고의 충격을 제한하고, 원치 않은 사고를 감지하고, 복구를 촉진하는 실행, 절차, 메커니즘이다. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층을 제공하는 다양한 대책의 조합이 요구된다.



(그림 4-10) 위험관리 절차

2.3.2 위험분석

o 핵심가이드

- 위험분석의 정의
- 위험분석의 절차 및 세부사항
- 위험분석의 방법론에 대한 세부항목의 이해

위험관리 부분에서 가장 중요한 역할을 하는 부분으로서 정보시스템과 그 자산의 기밀성, 무결성 그리고 가용성에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템의 취약성을 인식하고 이로 인해서 인식할 수 있는 예상손실을 분석한다.

위험을 경감시키는 대책은 아래 네 가지 사항 중 하나로 선택될 수 있다.

(1) 기본적인 접근 방법

(가) 조직의 보안정책을 참조하여 세부통제사항을 작성한다.

(나) 공공기관의 경우 정부부처 및 공공기관에서 요구하는 보안요구사항을 참조하여 반영한다.

(다) ISO, KICS 등 국내/외 표준을 참조하여 반영한다.

(라) 외국의 보안 컨설팅 기관에서 작성한 기본통제를 참조한다.

(마) 정보감리 등을 통하여 얻은 결과를 반영한다.

1) 장점

위험분석을 위한 자원이 필요하지 않고, 보호대책 선택에 들어가는 시간과 노력이 줄어든다. 일반적으로 기본적인 보호대책을 확인하기 위해 어떠한 중요한 자원도 필요하지 않다.

큰 노력 없이 많은 시스템에 같은 또는 비슷한 안전요소가 적용될 수 있다. 만약 같은 환경에서 운영되는 조직의 시스템이 많고, 사업 필요성이 비교가능하다면 기본적인 안전요소는 비용 효과적인 선택이다.

2) 단점

만약 기본적인 보호대책이 너무 높게 설정되었다면 어떤 시스템에 대해서는 비용이 너무 많이 들고, 너무 제한적이며, 만약 너무 낮게 설정되었다면, 어떤 시스템에 대해서는 보안결핍을 가져올 수 있다.

(2) 위험분석의 방법론

(가) 정량적 위험분석

1) ALE(연간예상손실)

o 자산가치 * 노출계수 = 단일예상손실 (SLE)

o 단일예상손실 * 연간발생률 = 연간예상손실 (ALE)

2) 과거자료 분석법

과거의 자료를 통해 위험발생 가능성을 예측하는 방법. 이 방법은 위협에 대한 과거 자료가 많을수록 분석의 정확도가 높아진다. 그러나 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며, 과거의 사건 중 발생 빈도가 낮은 자료에 대해서는 적용이 어렵다는 단점이 있다.

3) 수학공식 접근법

수학공식 접근법은 위협의 발생빈도를 계산하는 식을 이용하여 위험을 계량하는 방법으로 이 방법은 과거자료의 획득이 어려울 경우 위험 발생 빈도를 추정하여 분석하는데 유용하다. 또한 위험을 정량화 하여 매우 간결하게 나타낼 수 있다는 점이다. 그러나 기대손실을 추정하는 자료의 양이 낮다는 단점이 있다.

4) 확률 분포법

미지의 사건을 추정하는데 사용되는 방법이다. 이 방법은 미지의 사건을 확률적(통계적)편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다. 그러나 확률적으로 추정하는 방법이기 때문에 정확성이 낮다.

(나) 정성적 위험분석

1) 델파이법

시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다. 이 방법은 위험 분석을 짧은 기간에 도출할 수 있어 시간과 비용을 절약할 수 있기 때문에 추정의 정확도가 낮다.

2) 시나리오법

어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다. 이 방법은 적은 정보를 가지고 전반적인 가능성을 추론할 수 있고, 위험분석팀과 관리층 간의 원활한 의사소통을 가능케 한다. 그러나 발생 가능한 사건의 이론적인 추측에 불과하고 정확도, 완성도, 이용기술의 수준 등이 낮다.

3) 순위결정법

비교우위 순위결정표에 위험 항목들의 서술적 순위를 결정하는 방법이다. 각각의 위협을 상호 비교하여 최종 위협요인의 우선순위를 도출하는 방법이다. 이 방법은 위험 분석에 소요되는 시간과 분석하여야 하는 자원의 양이 적다는 장점이 있으나, 위험 추정의 정확도가 낮은 단점이 있다.

(다) 정량적, 정성적 분석의 장단점

[표 4-14] 정량적, 정성적 분석의 장단점]

	정량적 분석	정성적 분석
장점	- 객관적인 평가기준이 적용된다. - 정보의 가치가 논리적으로 평가되고 화폐로 표현되어 납득이 더 잘된다. - 위험관리 성능평가가 용이하다. - 위험 평가 결과가 금전적 가치, 백분율, 확률 등으로 표현되어 이해하기 쉽다.	- 계산에 대한 노력이 적게 든다. - 정보자산에 대한 가치를 평가할 필요가 없다. - 비용/이익을 평가할 필요가 없다.
단점	- 계산이 복잡하여 분석하는데 시간, 노력, 비용이 많이 든다. - 수작업의 어려움으로 자동화 도구를 사용할시 신뢰도가 벤더에 의존된다.	- 위험평가 과정과 측정기준이 지극히 주관적이어서 사람에 따라 달라 질 수 있다. - 측정결과를 화폐가치로 표현하기가 어렵다. - 위험완화 대책의 비용/이익 분석에 대한 근거가 제공되지 않고, 문제에 대한 주관적인 지적만 있다. - 위험관리 성능을 추적할 수 없다.

(3) 비공식적인 접근

비공식적 접근은 구조적인 방법에 의존하지 않고, 개인적인 지식과 경험을 이용한다. 만약, 내부 보안 전문가가 가용하지 않다면 외부 계약자가 이 분석을 시행할 수 있다.

(가) 장점

비공식적 분석을 하기 위한 추가적인 기술의 습득이 필요하지 않고 세부적인 위험분석보다 신속하게 수행된다. 이 접근방식은 비용 효과적이며, 소규모 조직에 적합할 수 있다.

(나) 단점

구조화되지 못해서, 어떤 위험이 있는 관심지역을 잃어버릴 가능성이 증가한다. 이 방법은 비공식적인 특성 때문에 재검토자의 주관적 관점과 편견에 영향을 받을 수 있다.

1) 보호대책 선택에 정당성이 부족하다. 따라서 보호대책에 들어가는 비용이 정

당화되기 어렵다.

2) 반복적인 재검토 없이는 시간에 따른 보안관련 변화의 관리가 어려울 수 있다. 비공식 위험분석을 했던 사람이 조직을 떠나면 문제가 발생할 수 있다.

(4) 세부적인 위험분석

세부적인 위험분석은 정당성과 자산의 가치, 이 자산들에 대한 위협의 수준평가, 그리고 자산들의 취약성을 포함한다. 위험분석은 자산에 대해 확인된 위험에 대한 만족하는 안전요소의 정당성, 선택 그리고 채택을 지원하고, 관리에 의해 정의된 받아들일 수 있는 수준의 위험의 감소를 지원한다. 세부적인 위험분석은 많은 자원이 소모되는 프로세스이고, 경계의 설정에 주의해야 하고, 지속적인 관리에 주의를 요한다.

(가) 장점

1) 각 시스템에 필요한 적절한 보안의 수준이 확인된다.

2) 세부적인 위험분석으로부터 얻은 추가적인 정보로 보안관련 변화의 관리는 이익을 얻는다.

(나) 단점

1) 가시적인 결과를 얻기 위해, 많은 시간, 노력 그리고 전문성이 필요하다.

2) 중요한 시스템의 보안 필요성이 너무 늦게 다루어질 가능성이 있다. 모든 시스템이 같은 세부사항으로 간주될 수 있고, 이 분석을 완성하는데 많은 시간이 소요되기 때문이다. 따라서 모든 시스템에 세부적인 위험분석을 사용하는 것은 바람직하지 못하다.

(5) 복합적인 접근

기준선 접근과, 세부위험분석에 설명된 기능들 중 최상의 핵심기능들의 조합이다. 결론적으로 이것은 보안요소 식별에 소요되는 최소한 시간과 노력의 좋은 균형을 제공한다. 대부분의 시스템에서 이 선택이 가장 비용 효율적인 접근을 제공하고, 대개의 조직에서 가장 권장되는 위험분석방법이다.

(가) 장점

1) 중요한 자원이 투입되기 전에 필요한 정보를 얻기 위한 간단한 고수준접근을 사용하는 것은, 위험관리 프로그램에 더 적합하다.

2) 이것은 조직적인 보안 프로그램의 신속한 전략 구상이 가능하고, 또 좋은 계획보조도구로 사용될 수 있다.

3) 자원과 비용은 가장 큰 이익이 있는 곳에 사용될 수 있고, 높은 위험은 미리

다루어질 수 있다.

(나) 단점

1) 만약 고수준분석이 부정확한 결과를 가지고 온다면, 세부적인 분석이 필요한 어떤 시스템은 적절히 다루지 못할지도 모른다.
2) 만약 고수준 위험분석이 적절하게 점검된다면 어떤 사건에 대해서는 그 시스템은 여전히 기준선 안전요소에 의해 보호된다.

2.3.3 정보보호 대책 선정 및 계획서 작성

o 핵심가이드

- 대책선정의 이해 (대책이 사용될 수 있는 영역)

대책은 위협을 방지하고, 취약성을 감소시키고, 원치 않은 사고의 충격을 제한하고, 원치 않는 사고를 감지하고, 복구를 촉진하는 실행, 절차, 메커니즘이다. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층을 제공하는 다양한 대책의 조합이 요구된다. 대책은 감지, 억제, 방어, 제한, 교정, 복구, 모니터링, 인식 중 하나 이상의 기능을 수행하는 것으로 대책의 적절한 선택은 보안 프로그램의 올바른 구현에 필수적이다. 대부분의 대책들이 복합적인 기능을 수행함으로 복수의 기능을 만족시키는 대책을 선택하는 것이 비용 효율적이다.

(1) 문서요건

정보보호관리체계 활동에 관련된 다음 사항을 해당 조직의 규모, 기능 등을 고려하여 문서화 하여야 한다. 또한 관련 문서들은 정보보호 관리체계의 정책에 따라 필요한 모든 임직원이 쉽게 이용할 수 있어야 한다.

(가) 정보보호관리체계의 내역서
(나) 문서화된 보안정책과 목적
(다) 정보보호 조직 및 책임정의서
(라) 위험 분석·평가 보고서
(마) 정보보호 계획서
(바) 통제사항 적용명세서
(사) 정보보호과정의 효과적인 계획, 운영, 통제를 보증하기 위해 요구되는 기타문서
(아) 이 기준에 요구되는 문서

(2) 대책선정

대책은 위협을 방지하고, 취약성을 감소시키고, 원치 않는 사고의 충격을 제한하고, 원치 않는 사고를 감지하고, 복구를 촉진하는 실행, 절차, 메커니즘이다. 일반적으로 효과적인 보안에는 자산에 대한 보안 계층을 제공하는 다양한 대책의 조합이 요구된다.

대책은 감지, 억제, 방어, 제한, 교정, 복구, 모니터링, 인식 중 하나 이상의 기능을 수행하는 것으로 대책의 적절한 선택은 보안 프로그램의 올바른 구현에 필수적이다. 대부분의 대책들이 복합적인 기능을 수행함으로 복수의 기능을 만족시키는 대책을 선택하는 것이 비용 효율적이다.

대책이 사용될 수 있는 영역의 예는 다음과 같다.

- o 물리적 환경
- o 기술적 환경(하드웨어, 소프트웨어, 통신)
- o 인력
- o 행정

보안 인식은 인적 영역에 관련된 대책이다. 조직이 운영하는 환경과 문화는 대책의 선택, 조직의 보안 인식 등과 관련이 있으며, 어떤 대책은 조직의 보안 태도에 대해 강력하고 명확한 메시지를 전송한다. 이러한 관점에서, 조직이 운영되는 문화 및 사회에 공격적이지 않은 대책을 선택하는 것이 중요하다.

(3) 제약의 식별 및 검토

대책 선정에 영향을 주는 많은 제한이 있다. 권고안 작성 시 그리고 실행 시 반드시 시간적, 재정적, 기술적, 사회적, 환경적, 법적 제약을 고려해야 한다.

2.4 대책구현 및 운영

2.4.1 정보보호 대책구현, 정보보호 대책유형, 대책 구현 시 고려사항

o 핵심가이드

- 예방, 탐지 교정대책의 이해
- 잔류위험의 이해
- 대책식별의 이해 (대책이 적용되는 영역, 위험을 경감시킬 요소, 실행 대책 선정 시 요소, 권고안 작성 시 그리고 실행 시 전형적인 제약)
- 위험수용의 이해

정보보호대책은 안전대책, 혹은 통제, 혹은 대응책이라고 한다. 정보보호대책은 위험을 감소시키기 위한 정보보호조치를 의미하며, 여기에는 장치, 절차, 기법, 행위 등을 포함한다.

(1) 예방 통제

오류나 부정이 발생하는 것을 예방할 목적으로 행사하는 통제이다. 발생 가능한 잠재적인 문제들을 식별하여 사전에 대처하는 능동적인 개념의 통제이며, 물리적 접근통제, 논리적 접근통제 등으로 나눌 수 있다. 물리적 접근통제란 관계자 이외의 사람이 특정 시설이나 설비에 접근할 수 없게 하는 각종의 통제를 뜻하며, 논리적 접근 통제란 승인을 받지 못한 사람이 정보통신망을 통하여 자산에 대한 접근을 막기 위한 통제 방법이다.

(2) 탐지 통제

발생 가능한 모든 유형의 오류나 악의적 행위를 예측하고 이에 대한 예방책을 마련한다 하더라도 예방 통제로만 완전히 막을 수는 없다. 예방 통제를 우회하여 발생한 문제점들을 찾아내기 위한 통제가 필요하다.

(3) 교정 통제

탐지 통제를 통해 발견된 문제들을 해결하기 위해서는 별도의 조치가 필요하다. 문제의 발생 원인과 영향을 분석하고 이를 교정하기 위한 조치가 취해져야 하며, 문제의 향후 발생을 최소화하기 위하여 시스템을 변경하는 등의 일련의 활동을 교정 통제라 한다. 예기치 못하였던 시스템 중단이 발생할 경우 어떻게 재실행해야 하는지를 규정한 절차, 백업과 복구를 위한 절차 그리고 비상사태에 대한 대처 계획 등이 포함된다. 특히 불법적인 접근 시도를 발견해내기 위한 접근 위반 로그는 탐지 통제에 속하지만, 데이터 파일이 복구를 위해 사용되는 트랜잭션 로그는 교정 통제에 속한다.

(4) 잔류 위험

보통 대책에 의해서도 위험은 부분적으로 경감될 뿐이다. 부분적 경감이 일반적으로 달성할 수 있는 전부이고 그 이상의 경감에는 비용이 증가한다. 이는 일반적으로 잔류 위험이 존재함을 시사하는 것이다. 보안이 조직의 필요에 적절한지 여부를 판단하는 일의 일부는 잔류 위험의 허용이다. 이 프로세스를 위험허용(risk acceptance)이라 한다.

관리를 통해 사건의 발생 가능성과 충격의 관점에서 모든 잔류 위험을 인식할 수 있어야 한다. 원치 않는 사고의 발생에 의한 충격의 결과를 허용할 수 있는 위치에 있는 사람들 및 잔류 위험의 수준을 허용할 수 없을 때 추가적인 대책의 구현하는 권한을 가진 사람이 잔류 위험의 허용 여부에 대한 결정을 내려야 한다.

(5) 대책 식별

평가된 위험에 대응하여 효율적으로 보호하는 대책을 선정하기 위해, 위험분석 결과를 고려해야 한다. 관련 위협에 대한 취약성은 추가적인 보호가 필요한 곳 및 어떤 방식을 취해야 하는가를 지적한다.

고려된 대책 비용에 따라 결정되는 대안이 있다. 대책이 적용되는 영역은 다음을 포함한다.

- o 물리적 환경
- o 인력
- o 경영
- o 하드웨어/소프트웨어
- o 통신

대책이 충분히 효율적이지 않는 경우 기존의 또는 계획된 대책은 개선 또는 제거의 관점에서 유지 보수를 포함하는 비용 대조를 조건으로 하여 재검토되어야 한다. 때로는 대책을 적소에 두는 것보다 부적절한 대책을 제거하는 것이 더 비용이 많이 들 수 있다. 더욱이 현재의 검토 영역 외의 자산을 위해 대책의 보호를 제공하는 것이 가능하다.

대책 식별로 인해 취약성이 보호되어야 하는 취약성 및 이러한 취약성을 이용할 수 있는 관련 위협을 갖는 것은 유용하다. 일반적으로 위험을 경감시킬 많은 가능성들이 있다.

- o 위험 회피
- o 위험 전환(예, 보험)
- o 위협 감소
- o 취약성 감소
- o 가능한 충격 감소
- o 원치 않은 사고 감지 대응, 복구 등

대책 선정에 있어 중요한 또 다른 측면은 비용 요소이다. 대책이 보호해야 하는 자산의 가치보다도 유지 및 실행에 있어 훨씬 더 비싼 대책은 부적절하다. 그러나 실행될 대책의 품질이나 수를 감소시키는 예산의 경우에는 많은 주의를 기울여야

한다. 왜냐하면 계획된 것보다 큰 불분명한 위험 수락으로 이어질 수 있기 때문이다. 대책을 위해 수립된 예산은 상당한 주의를 가지고 제한적 요소로서 사용되어야 한다.

IT 시스템 보호를 위해 기준선 접근이 선정되는 경우에는 대책 선정은 비교적 간단하다. 대책 카탈로그는 가장 일반적인 위협에 대해 IT 시스템을 보호하기 위한 일련의 대책을 제안한다. 이러한 추천된 대책들은 기존의 그리고 계획된 대책들과 이미 적소에 없거나 기준선보호를 취득하기 위해 실행되는 대책목록 형식으로 계획되지 않은 것들과 비교된다.

대책 선정은 작동 및 기술적 대책들의 균형을 항상 포함한다. 작동중인 대책은 물리적 인력 및 관리적 보안을 제공하는 것들을 포함한다.

물리적 보안 대책은 내부 건물 벽, 키 코드 문 잠금장치, 화재 억제 시스템, 방어 장치 및 위험 방지기의 강화를 포함한다. 인력 보안은 인력 채용 점검, 직원 모니터링, 보안 인식 프로그램을 포함한다.

절차상의 보안은 안전한 작동 절차문서, 응용 개발, 수용 절차뿐만 아니라 사고 처리 절차를 포함한다. 이러한 범주에 관련하여 일관된 계획/재난 복구를 포함하여 적절한 업무 지속성,

전략 및 계획(들)은 각각의 시스템을 위해서 개발된다는 것은 매우 중요하다. 계획은 재난이나 서비스 중단이 발생되었을 때 복구를 위한 핵심 기능과 우선권, 프로세스 필요성 및 수행할 조직의 절차의 세부사항을 포함한다. 그러한 계획은 사업을 계속하게 하는 한편 중요한 정보가 대책에 프로세스 되도록 요하는 단계를 포함해야 한다.

기술적 보안은 통신 대책뿐만 아니라 하드웨어와 소프트웨어를 포함한다. 이러한 대책들은 위험이 보안 기능 및 보증을 제공하는 정도에 따라 선정된다. 예를 들어 기능은 식별, 인증, 논리적 접근 통제 요건, 감사 추적/보안 기록 필요성, 다이얼-백(dial-back)보안, 메시지 인증, 암호화 등을 포함한다. 보증 요건은 보안 기능 및 그에 따른 점검 수량 및 유형 등에 필요한 신뢰 수준을 문서로 증명한다. 작동 및 기술적 대책의 알맞은 융합에 대한 결정에 있어서 기술적 보안 요건을 실행하기 위한 상이한 옵션이 있을 것이다. 기술 보안이 요하는바와 같이 기술 보안 구조는 보안이 제공할 수 있는 것을 식별하도록 각각의 옵션에 대하여 정의되어야 한다. 또한 보안이 가용한 기술로 사용 가능하도록 정의되어야 한다.

조직은 최종 시스템 해결의 일부로 평가된 제품 및 시스템을 사용하도록 결정한다. 평가된 제품은 제 3자에 의해 검사된 것들이다. 제 3자는 동일한 조직의 또 다른 부분이거나 또는 제품 및 시스템 평가에 있어서 전문성이 있는 독립조직이다.

특히 평가는 구축 중인 시스템을 위해 만들어진 일련의 전 기준에 대응하여 수행될 수 있고, 여러 상황에서 사용될 수 있는 일련의 일반화된 기준이다. 평가 기준은 기능적 요건 혹은 보증 요건을 규정한다. 많은 평가 계획이 실재하며 그들 중 대다수는 정부 및 국제 표준 단체가 지원한다. 조직이 구현된 일련의 기능이 필요한 것이라는 확신을 요구할 때 그리고 그러한 기능의 실행 중 정확성과 완전성에 관하여 신뢰할 필요가 있을 때 평가된 제품 및 시스템을 사용할 수 있다. 대안적으로 강조하는 실용적인 보안 시험은 보안 제공에 있어서 확실한 보증을 제공한다.

실행 대책 선정 시 많은 요소들은 다음을 포함하여 고려된다.

- o 대책 사용의 용이성
- o 사용자를 위한 명백성
- o 그들을 수행하는 사용자를 위해 제공하는 도움
- o 대책의 상대적 강화
- o 수행 기능의 유형-예방 조치, 제지, 감지, 복구, 교정, 모니터링, 인식

일반적으로 대책은 이러한 기능들 중의 하나 이상을 충족시킨다. 더 많이 충족하면 할수록 좋다. 전반적인 보안이나 사용될 일련의 대책을 검사할 때, 적어도 가능하다면 기능 유형간의 균형을 유지한다. 이는 전체적인 보안들이 더더욱 효율적이고 능률적이게 한다. 비용/혜택 분석을 요구할 뿐만 아니라 거래분석(특수한 상황에 관하여 상대적인 중요성에 무게를 두는 일련의 기준을 사용하는 경쟁 대안을 분석하는 방법)도 마찬가지로 요구될 수 있다.

(6) 제약의 식별 및 검토대책 선정에 영향을 주는 많은 제한이 있다. 권고안 작성 시 그리고 실행 시 반드시 이러한 제한을 고려해야 한다.

전형적인 제약으로 다음과 같은 사항들이 있다.

(가) 시간적 제약

많은 형태의 시간제한이 존재한다. 예를 들어 관리를 위해서 수용하는 시간적 기간 내에 대책을 구현해야 한다. 또 다른 형태의 시간제한은 대책이 기간 내에 구현되는지 여부이며 세 번째의 시간제한은 관리가 결정하는 시간적 기간이 시스템을 특수한 위험에 노출되도록 남겨 두는 허용 가능 기간이다.

(나) 재정적 제약

대책은 보호하기 위하여 설계된 자산가치보다 실행을 위한 것이 보다 비싸지 않다. 모든 노력은 배정된 예산을 초과하지 말아야 한다. 그러나 몇몇 경우에 원하는 보안 및 그러한 예산 제한 내에서 위험 수용 수준을 달성하는 것은 불가능하다. 따라서 이것은 이러한 상황의 해결에 대한 관리 결정이다.

(다) 기술적 제약

프로그램이나 하드웨어의 호환성과 같은 기술적 문제는 대책 선정 시 그들에 대한 평가가 이루어진다면 쉽게 회피될 수 있다. 또한 기존의 시스템에 대한 회상적 대책 구현은 기술적 제한으로 인해 흔히 저지된다. 이러한 난관들은 대책의 균형이 절차상 그리고 물리적 보안 측면을 지향하도록 한다.

(라) 사회적 제약

대책 선정에 대한 사회학적 제한은 국가, 영역, 조직 심지어 조직 내의 부서에게까지 구체적이다. 많은 기술적 대책들이 직원의 능동적인 지원에 의존하기 때문에 이러한 사회학적 제한은 무시될 수 없다. 만약 직원이 대책에 대한 필요성을 이해하지 못하고 문화적으로 수용할 만하다는 것을 알지 못한다면 대책은 시간이 지날수록 비효율적인 것이 될 것이다.

(마) 환경적 제약

환경적 요소들은 자연적, 도시적 등의 지리학 주위에서 공간 가용성이나 극한의 기후 조건들과 같은 대책 선정에 영향을 끼칠 것이다.

(바) 법적 제약

정보 프로세스에 대한 개인 자료 보호나 형사상의 코드 조항들과 같은 법적 요소들은 대책의 선정에 영향을 미칠 수 있다. 화재 부서 규정, 노동법과 같은 비IT의 특수 법과 규정은 대책 선정에 영향을 미칠 수 있다.

(7) 위험 수용

대책을 선정하고 이러한 대책들이 달성하려고 하는 위험 감소를 식별한 후에도 항상 잔류위험은 존재한다. 어떠한 시스템도 절대적으로 안전할 수 없다. 이러한 잔류 위험은 조직을 위해 '허용 가능'또는 '허용 불가능'으로 구분한다. 이러한 범주는 위험과 연관된 잠재적인 불리한 업무 충격을 검토하여 수행될 수 있다. 분명히 허용 가능 위험은 추가의 고찰 사항 없이 허용되어서는 안 된다. 이러한 위험들이 다른 제한으로 인해 수용될 것인가 또는 어쩌면 추가의 비용이 드는 대책이 허용 불가능한 위험을 감소시키기 위해서 선정되는가는 관리결정 사항이다.

2.4.2 정보보호교육 및 훈련교육/훈련 프로그램 작성방법 인식제고 방법

o 핵심가이드

- 교육 및 훈련의 중요성
- 교육 내용 및 범위

최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호 대책의 필요성을 이해하도록 하며 구현된 대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.

(1) 정보보호 인식 프로그램

정보보호 인식 프로그램의 목적은 조직 내의 인식 수준을 모든 사람이 쉽게 수행할 수 있는 수준까지 증대시키는 것이다. 훈련에는 구성원들이 무엇을 해야 하며, 어떻게 할 수 있는지에 대한 교육을 포함해야 한다. 훈련의 내용에는 가장 기본적인 보안 단계의 실행에서부터 좀 더 진보적이고 전문화된 기술에 이르기까지 다양한 단계로 나누어 구성될 수 있다.

(2) 교육 대상의 분류

교육의 대상자는 다음과 같은 기준으로 분류할 수 있다.

(가) 최고 경영자를 포함한 임원
(나) 조직의 신입직원
(다) 조직의 IT 이용자 그룹
(라) 조직의 IT 시스템 운영자와 개발자 그룹
(마) 조직을 물리적/전자 정보적으로 출입하는 제3자 그룹
(바) 조직이 제공하는 정보를 이용하는 일반 외부 이용자 그룹

(3) 교육 내용 및 점검 사항

인식 교육 프로그램에는 다음 사항이 포함되어야 한다.

(가) 물리적 보안
(나) 정보처리 정책
(다) 정보의 방치 및 억제 정책
(라) 인터넷 접근 정책
(마) 개방 접근 구역
(바) 휴대용 컴퓨터
(사) 재택근무
(아) 무선 통신

(4) 교육 훈련의 내용

처음에는 정보보안의 중요성, 주어진 보안장치의 사용방법, 오용의 보고 절차 등

을 언급하여야 하고 모든 직원에게 IT 보안 필요성을 인식시키기 위해 많은 노력을 해야 한다. 운영/관리 직원은 독립적으로 관리 직무를 수행할 수 있는 범위와 단순 고장에 대한 검출과 조치, 직접 자료를 저장하는 방법, 외부 운영자에 취해지는 안전대책의 이해 사항 등을 미리 훈련받아야 한다.

2.4.3 운영, 컴퓨터 운영, 네트워크운영, 매체관리

o 핵심가이드

- 컴퓨터 운영(로그관리) 전반에 대한 이해
- 네트워크 운영 전반에 대한 이해
- 매체관리 전반에 대한 이해

(1) 컴퓨터 운영

(가) 컴퓨터 운영관리 기준

컴퓨터 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토한다. 적절한 운영관리를 위해 다음과 같은 사항을 유지한다.

1) 시스템 시작 및 종료 시간

2) 시스템 오류 및 수정내용

3) 데이터 파일 및 컴퓨터 출력물의 정확한 취급에 대한 확인

4) 기록을 이행한 직원의 신원 정보

(나) 컴퓨터 운영기록 관리

운영기록의 관리는 컴퓨터 운영 및 응용 프로세스의 활동과 사용자 활동에 대한기록을 유지하는 것으로, 적당한 도구와 절차를 함께 사용하여 보안 위반사항이나 성능문제 등을 찾는데 도움을 준다. 운영기록의 관리는 개인의 책임성, 사건의 재구성, 침입탐지 등을 포함한 몇 가지 보안과 관련된 목적을 달성하는데 도움을 준다.

1) 개인의 책임성

운영기록 관리는 사용자에게 운영기록에 기록된 내용을 이용하여 개인에게 책임을 추구할 수 있다는 것을 조언할 수 있어, 사용자가 올바르게 행동하도록 고무시킬 수 있다.

2) 사고조사

운영기록을 관리함으로써 문제가 일어난 후에 사건을 재구성하는데 사용될 수 있다. 시스템 활동에 대한 운영기록을 조사함으로써 어떻게, 언제, 왜 일상적인 동작이 정지되었는지 정확하게 지적하여 피해 평가를 쉽게 할 수 있다.

3) 침입탐지

운영기록이 적절한 정보를 기록하도록 설계되고 구현되었다면 침입을 탐지하는 데에도 도움을 줄 수 있다.

(다) 운영기록관리 기준관련 사항 및 조치방법

운영기록관리는 어떤 사건이 발생하였고, 누가 또는 무엇이 그 사건을 발생시켰는지 확정할 수 있는 충분한 정보를 포함하여야 한다. 일반적으로 사건기록은 언제 사건이 발생하였고 그 사건에 연관된 사용자 ID, 그 사건을 일으키는데 사용된 프로그램이나 명령, 그리고 결과를 명기하여야 한다. 날짜와 시간은 실제사용자에 의한 것인지, 사용자로 가장한 사람에 의한 것인지를 결정하는데 도움이 된다.

또한, 운영기록 데이터는 외부인이나 비인가자가 접근할 수 없도록 보호되어야 하는데, 이를 위한 방법으로 전자서명을 이용하는 방법이 있다. 다른 방법으로는 한번만 쓸 수 있는 저장장치를 이용하는 것이다. 예를 들어 침입자는 운영기록레코드를 수정하여 자신의 증거를 덮어버리려 할 수 있으므로 운영기록 파일들의 보호가 필요하다.

1) 적절한 운영기록 데이터는 기본적으로 다음의 내용을 포함해야 한다.

- o 시스템 시작 및 종료 시간
- o 시스템 오류 및 수정내용
- o 데이터 파일 및 컴퓨터 출력물의 정확한 취급에 대한 확인
- o 기록을 수행한 직원의 이름

(2) 네트워크 보안 정책

네트워크에 접근하는 비인가 된 접근을 막기 위해 사용자 터미널과 컴퓨터 서비스 간에 물리적·논리적 경로를 통제해야하며, 접근이 허가된 네트워크나 네트워크서비스, 누가 네트워크나 네트워크서비스를 접근할 수 있는가를 결정하는 인가 절차, 네트워크 연결과 네트워크 서비스에 대한 접근을 보호하기 위한 관리 통제와 절차와 같은 사항을 접근 정책에 포함해야 한다.

(3) 네트워크 운영

네트워크의 효율적인 관리를 위해 정보통신망 접속에 따른 접속 기준 및 절차를 규정하고 접근 가능한 통신 경로 및 컴퓨터를 최소화하여 정보통신망 접속에 따른 장애발생을 최소화하고 장애 발생 시의 책임한계를 명확히 한다.

중요한 전송로 및 네트워크에 대해서는 각각의 전송로 및 네트워크의 특성에 따

른 감지, 제어, 및 통보기능을 설치해야 한다.

(가) 서비스를 제공하는 전산망은 다른 업무용 전산망과 분리된다.

(나) 개발업무에 사용되는 네트워크는 다른 업무의 네트워크와 분리한다.

(다) 네트워크 서비스에 관련되는 기기에 대한 관리는 해당 기기를 소장하고 있는 구역뿐만 아니라 시스템 요소들을 연결하는 통신구역 전력서비스, 냉/난방 플랜트, 전화와 데이터라인, 백업 매체와 소스 문서, 그리고 시스템의 운영에 필요한 모든 다른 요소 및 그 위치를 포함한다. 이를 관리하기 위한 방안은 다음을 포함한다.

1) 물리적 보호 조치를 취함으로써 보호구역에 대한 위협을 감소

2) 출입구에서의 출입통제 강화

3) 폐쇄회로 텔레비전 카메라나 침입탐지기와 같은 기기의 이용

4) 단말 등에 대한 자동 상태확인 기능

(라) 중요한 네트워크 및 네트워크 설비에 대해서는 각각의 특성에 따른 감지, 제어 및 통보기능을 설치해야 한다.

1) 이용회선 구분

전용회선, 공중회선 등에 따른 작동상황 및 통신수용능력을 감지 제어할 수 있는 기능을 설치한다.

2) 접속기기

음성전송, 화상전송, 데이터 전송 기기 등에 따른 데이터 전송능력을 파악하고 작동 상황을 감지 제어할 수 있어야 한다.

3) 데이터 송수신 포맷

데이터 송수신 포맷의 특성에 따른 적절한 감지, 제어 기능을 설치한다.

(4) 매체관리

(가) 데이터의 보관

1) 관리기준에 명시되어야 할 사항

o 데이터 식별번호

o 보관 목적

o 보관 일시

o 보관 기간

o 보관 책임자

2) 데이터 관리 기록부

데이터를 관리하기 위해 데이터 관리기록부를 비치해야 한다.

3) 데이터의 폐기

데이터의 폐기는 절차를 규정하여 실시하여야 하며, 규정에 포함될 내용은 다음과 같다.

o 데이터 보존연한

o 데이터 매체에 따른 폐기방식

o 폐기 확인 방법

o 폐기 이유

o 폐기 일시

o 폐기 내용

(나) 데이터의 출납

데이터의 출납은 출납 요청서에 의해 데이터 담당자가 처리해야하며 보안책임자는 보안책임자 의무사항에 따라 데이터의 보안에 만전을 기해야 한다.

(다) 보안책임자 의무사항

데이터 파일의 통제 및 보호책 강구

2.4.4 사후관리, 모니터링, 변경관리, 내부감사

o 핵심가이드

- 사후관리의 이해
- 사고대응절차의 이해
- 변경관리의 이해
- 내부감사의 이해

(1) 사후관리

(가) 정보보호관리체계의 재검토

조직의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.

적절한 단계에서, 다음 목적을 위하여 정책의 계획 및 구현에 대한 체계적인 검토를 수행한다. 그러한 검토에 참여하는 인원에는, 검토가 진행되고 있는 대상의 계획 및 구현 단계에 관련된 인원이 포함되어야 하며, 검토 및 검토로 야기된 조치의 결과를 기록하여야 한다.

1) 정보보호관리체계의 재검토에는 다음과 같은 사항을 고려하여야 한다.

o 검증 및 유효성 확인의 목적에 부합

o 정보보호정책의 영향분석이나 잠재적인 위험성 평가

o 정보보호정책에 대한 전 과정(Life Cycle) 재검토

(나) 정보보호관리체계의 모니터링 및 개선

정보보호관리체계가 정보보호정책과 목적을 충족시키는지 여부에 대해 모니터링 하여, 개선사항을 식별하고, 적절한 수정이나 예방 조치를 통해 효과적으로 개선사항을 구현하여야 한다.

조직은 필요에 따라 모니터링, 측정, 분석 등을 통하여 정보보호관리체계의 지속적 개선 프로세스를 계획하고 실행하여야 한다.

1) 정보보호정책의 성과 측정 시 요구사항

o 정보보호정책의 적합성 실증

o 정보보호관리체계의 적합성 보증

o 정보보호관리체계의 효과성에 대한 지속적 개선의 달성

이는 통계적 기법을 포함한 적용 가능한 방법의 필요성, 범위 및 사용에 대한결정을 포함하여야 한다.

2) 감시 및 측정방법은 다음사항을 고려할 수 있다.

o 정책 만족도 측정

o 내부감사

o 재정평가

o 자체평가 등

3) 모니터링 및 측정

o 조직은 정보보호관리체계의 성과 측정방법으로 정보보호정책이 조직의 요구사항을 충족시키는 지 여부에 대해 모니터링 하여야 하며, 이 정보의 획득 및 활용에 대한 방법을 결정하여야 한다.

(2) 내부감사

조직은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피 감사분야의 관리자는 발견된 부적합 사항 및 그들의 원인을 제거하기 위한 조치가 취해졌으며, 취해진 조치가 검증되고 검증결과가 보고됨을 보장하여야 한다.

다음 사항을 결정하기 위하여 조직은 계획된 주기로 내부감사를 수행하여야 한다.

(가) 정보보호정책이 계획된 결정사항 및 조직이 설정한 요구사항을 충족시키는지

그리고 이 규격의 요구사항을 충족시키는지 여부

(나) 효과적으로 실행되고 유지되는지 여부

조직은 감사 대상 및 영역의 상태와 중요성뿐만 아니라 이전 감사의 결과를 고려하여 감사 프로그램을 계획하여야 한다. 또한 조직은 감사 목적 범위 주기 및 방법을 정하여야 하며, 감사자 선정 및 감사 수행에는 감사 프로세스의 목적성 및 공정성이 보장되어야 한다. 감사자는 자신의 업무에 대하여 감사를 수행하여서는 안 된다. 문서화된 절차에는 감사의 계획, 수행, 감사의 독립성 보장, 결과의 기록 및 보고에 대한 책임과 요구사항을 정하여야 한다.

감사대상 업무에 책임을 지는 경영자는 발견된 부적합 및 원인을 제거하기 위한 조치가 적시에 취해질 수 있도록 보장하여야 한다. 후속조치는 취해진 조치의 검증 및 검증 결과의 보고를 포함하여야 한다.

(3) 변경관리

정보시스템에 관련된 변경을 지속적으로 관리한다. 장비, 소프트웨어, 절차 등에 대한 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립한다. 변경절차 수립 시에는 다음과 같은 사항들을 반영한다.

(가) 변경대상 및 주요변경사항에 대한 정의 및 기록

(나) 변경사항이 자원의 성능, 보안기능. 구조에 미치는 영향

(다) 변경방법 및 변경시간이 업무에 미치는 영향

(라) 제안된 변경사항에 대한 공식적인 승인절차

(마) 변경사항에 대한 관련인력들의 관계 및 책임

(바) 변경사항에 대한 공지 및 교육

(사) 변경작업이 실패하였을 경우 복구나 폐기에 대한 책임 정의 및 절차

(아) 비상계획

(4) 침해사고 대응절차

(가) 1단계

사고처리 지침 및 절차, 필수적인 문서, 업무연속성 계획 등 준비

(나) 2단계

사건을 보고하기 위한 수단 및 책임

(다) 3단계

사고조사 및 심각성 조사를 위한 절차 및 책임

(라) 4단계

사고처리, 피해제한, 사고근절, 상부보고에 대한 절차 및 책임

(마) 5단계

정상 서비스 등 재구축을 위한 절차 및 책임

(바) 6단계

법적 연투 관계에 대한 조사 및 분석을 포함한 후기사고 조치에 대한 절치 및 책임

2.5 업무연속성관리

2.5.1 업무연속성관리 체계, 업무연속성관리 과정, 프레임워크 [1급]

o 핵심가이드

- 업무연속성관리의 정의 및 목적

(1) 업무연속성관리(BCM)의 정의

업무 연속성 계획의 계획, 수립, 시험 및 보수 등을 포함하는 관리행위를 의미한다. 주요 통제 목표는 목표복구시간과 목표복구대상이며 전사적인 차원에서 이루어지는 관리활동이다.

(2) 업무연속성관리 단계

(가) 시작 단계

업무지속성관리에 관한 정책을 수립하는 단계로서 수립된 업무지속성계획이 조직의 업무나 기술관련 정책과 적절히 통합되는 것을 보장하고 업무지속성관리에 관한 제반 사항을 준비하는 프로세스이다.

(나) 전략수립 단계

재해가 업무에 미치는 잠재적인 영향 및 위험을 평가하고 위험감소 및 업무 프로세스 복구를 위한 여러 옵션들을 파악하고 평가하여 업무지속성관리를 위한 비용 효과적인 전략을 수립하는 프로세스이다.

(다) 구현 단계

업무가 지속적으로 운영되기 위한 프로그램을 수립하는 단계로서 업무지속성전략에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 업무복구를 위한 계획 및 절차를 작성하고 초기 시험을 수행하는 프로세스로 구성된다.

(라) 운영 관리 단계

수립된 업무지속성전략, 계획 및 절차를 계속적으로 테스트, 검토 및 유지보수하며 이에 대한 적절한 교육 및 훈련 프로그램을 운영하는 프로세스로 구성되어 있다.

2.5.2 업무연속성 계획수립, 응급조치, 백업계획, 정상복구 [1급]

o 핵심가이드

- 업무연속성 계획의 목적
- 업무연속성 접근 단계
- 재난복구 계획과 그 종류의 이해 (각 유형의 장단점)
- 업무영향평가의 이해

(1) 업무연속성계획(BCP)의 정의

각종 재해 시 재난의 발생을 대비하기 위하여 핵심 시스템의 가용성과 신뢰성을 회복하고 사업의 연속성을 유지하기 위한 일련의 사업지속성계획과 절차를 말한다. 업무연속성계획은 단순한 데이터의 복구나 신뢰도를 유지하며 나아가 기업의 전체적인 신뢰성 유지와 가치를 최대화하는 방법과 절차이다.

(2) 업무연속성계획(BCP)의 접근 5단계 방법론

(가) 프로젝트의 범위 및 설정 및 기획

조직의 독특한 사업경영과 정보시스템의 지원서비스들을 조사해서 다음 활동단계로 나아가기 위한 프로젝트 계획을 수립하는 단계.

이 단계에서는 명확한 범위, 조직, 시간, 인원 등을 정의하여야 한다. 또한 프로젝트의 근본 취지나 요구사항들이 조직전체 및 BCP의 개발에 가장 중요한 역할을 수행할 부서나 직원들에게 명료하게 전달하여야 한다.

(나) 사업영향평가(BIA)

컴퓨터나 통신서비스의 심각한 중단사태에 따라 각 사업단위가 받게 될 재정적 손실의 영향도를 파악한다.

(다) 복구전략 개발

BIA단계에서 수집된 정보를 활용하여 time-critical한 사업기능을 지원하는데 필요한 복구자원을 추정한다. 또한 여러 가지 가능한 복구방안들에 대한 평가와 이에 따른 예상비용에 대한 자료를 경영자 층에 제시하는 것도 이 단계에서 해야 할 일이다.

(라) 복구계획 수립

사업을 지속하기 위한 실제 복구 계획을 수립하는 단계이다. 효과적인 복구과정을 수행하기 위해 명시적인 문서화가 반드시 요구되며 여기에는 경영 재산 목록 정보와 상세한 복구팀 행동계획이 포함된다.

(마) 프로젝트의 수행 테스트 및 유지보수

마지막 단계로 테스트와 유지보수 활동 현황을 포함하여 향후에 수행할 엄격한 테스트 및 유지보수 관리 절차를 수립한다.

(3) 업무연속성계획(BCP)의 접근 6단계 방법론

(가) 사업상 중대업무 규정

조직의 중요한 사업단위를 식별하고 우선순위를 수립한다.

(나) 사업상 중대업무를 지원하는 자원의 중요도 결정

사업단위의 중요도가 1단계에서 정해졌다면, 그 사업단위를 지원하는 자원을 식별하는 것이 중요한데, 자원을 식별, 분석할 때는 그 자원의 기능을 잘 아는 사람이 하는 것이 바람직하며, 자원도 사업단위처럼 중요도에 따라 자원의 기능을 잘 아는 사람이 하는 것이 바람직하며 자원도 사업단위처럼 중요도에 따라 우선순위를 정하는 것이 좋다. 자원은 사람, 처리장비, 컴퓨터 관련서비스, 자동화 어플리케이션과 데이터, 물리적인 인프라, 문서 등 6가지로 분류한다.

(다) 발생 가능한 재난에 대한 예상

(라) 재난대책 수립

필요한 자원을 복구하는 방법을 계획한다. 또한 발생된 재난과 위험을 최소화하거나 아니면 방지하는데 그 목적이 있다. 이 때 고려해야할 점은 비용인데, 위험을 방지하는데 드는 비용이 실제 사업을 지속하는 비용보다 더 많이 소요되는 경우 그 방지책은 쓸모가 없는 것이므로 비용대비 효과를 고려하여 대책을 수립하여야 한다.

1) 재난대책계획수립

- o 비상응답체제 : 재산상 손상을 최소화하고 생명을 보호하기 위해서 취해지는 초기 활동
- o 복구 : 중요한 사업기능들을 계속적으로 지원하기 위해서 취해지는 일련의 활동
- o 재개 : 모든 사업기능들을 정상적인 운영환경으로 복귀하는 일련의 활동

(마) 재난대책수행

수립된 재난대책계획에 따라 적절한 준비와 수행, 문서화 그리고 직원들에 대한 훈련과정

(바) 테스트 및 수정

비상대책계획은 계획의 결점발견과 수행의 원활함을 도모하기 위하여 정기적으로 테스트 수정하는 과정을 말함

(4) 재난복구계획(DRP)

정보시스템의 재해나 재난 발생에 대비하여, 실제상황이 발생했을 때 취해야 할 행동절차를 미리 준비하는 것을 말한다.

(가) 목적

1) 정보의 비밀성, 무결성, 가용성, 인증성 등 확보
2) 핵심적인 기업업무의 연속성 유지
3) 테스트와 시뮬레이션을 통하여 DRP의 신뢰성을 유지
4) 재난 발생 시에 의사결정 시간을 최소화하여 복구시간을 단축
5) 시스템 운영중단 요인을 식별
6) 생존에 대한 계획을 마련
7) 재난 복구 방법 구축

(5) 재난복구서비스의 종류

(가) 중복 시스템 운영

전산센터와 동일한 시스템을 하나 더 설치하여 운영하는 것.

(나) 핫 사이트

재난 발생으로 영향을 받는 업무 기능을 즉시 복구할 수 있도록 전산 센터와 동일한 모든 설비와 자원을 보유하고 있는 거의 안전한 시설로서 수 시간 안에 가동이 이루어 질 수 있다.

(다) 웜 사이트

부분적으로 설비를 가지고 있는 백업 사이트로서 대개 디스크 드라이브, 테이프 드라이브와 같이 가격이 저렴한 선택적인 주변기기를 가지고 있으나 주 컴퓨터는 가지고 있지 않다.

(라) 콜드 사이트

재난 발생 시 새로운 컴퓨터를 설치할 수 있는 컴퓨터실을 미리 준비해 둔 것으로 별 다른 장비는 가지고 있지 않다.

(마) 백업 서비스

일부 응용 서비스는 통신 라인을 통하여 그 응용 서비스를 제공하는 기관에서 업무처리를 대행 받을 수 있다.

(바) 상호 백업 협정

서로 비슷한 시스템을 가지고 있는 회사들끼리 재난 발생 시 서로를 백업해주기로 협정

(사) 수작업

시스템 복구 설비를 갖추지 못한 경우에는 새로운 컴퓨터가 설치될 때까지 사람이 업무를 대행.

(6) 업무영향평가

(가) 업무영향분석

조직을 계속 운영하기 위해서는 잠재적인 재해를 인지하고, 주요 기능의 중지를 최소화시킬 수 있는 계획을 개발하고, 성공적으로 운영을 복구시킬 수 있어야 한다. 업무복구계획의 주요 목적은 운영의 전부 혹은 일부 그리고 컴퓨터서비스가 작동하지 않을 때, 조직을 보호하는 것이다. 그러므로 조직의 모든 기능적 분야에 대해서 다양한 재해위협과 관련된 잠재적인 위험과 영향이 분석되어야 한다.

(나) 업무영향분석의 목적

1) 핵심 업무를 파악하는 것
2) 핵심 업무의 정지로 인해 조직에 발생되는 잠재적인 손해 혹은 손실 파악

(다) 업무영향분석 시 고려사항

1) 수입상실, 추가적 비용부담, 신용상실 등과 같은 형태의 손실
2) 사건 발생 이후 시간이 경과함에 따라 손해 혹은 손실이 검증되는 정도
3) 업무가 최소한의 수준으로 계속 운영되는데 필요한 최소한의 직원, 시설, 서비스
4) 최소한의 운영에 필요한 직원, 시설, 서비스를 복구하는데 소요되는 시간
5) 전체 업무를 운영하는데 필요한 직원, 시설, 서비스를 충분히 복구하는데 소요되는 시간

(라) 업무영향분석의 구성요소

1) 업무 프로세서의 식별
2) 영향시나리오의 정의
3) 잠재적 업무영향에 대한 측정
4) 업무복구 목표의 정의
5) 최소한의 요구사항에 대한 평가

(마) 업무 프로세스의 식별

업무 프로세스(business process)란 공통 목표를 추구하는 특정 조직에서의 업무활동의 집합이다. 업무 프로세스는 단일 업무기능 혹은 여러 업무기능에 의해서 처리된다. 업무 프로세스는 정보기술, 인력자원, 사무서비스 등과 같은 여러 업무지원기능에 의존되어 있다. 업무프로세서는 간혹 독립적으로 운영되기도 하지만, 기술이 발전함에 따라 통합되어가고 있다. 업무지속성관리는 중요한 업무 프로세스의 지속성을 유지하는데 초점을 두고 있기 때문에, 업무영향분석의 목적을 위해서 업무프로세서들을 파악하는 것이 중요한 첫 단계의 작업이다. 각 업무 프로세스별로 업무영향분석이 수행될 것이다. 업무 프로세스를 파악 하는데 다음과 같은 자료가 필요하다.

o 전략적 혹은 업무계획 문서

o 업무 프로세스 재설계(Business process re-engineering)에 의한 산출물

o 조직적 정보모형(organizational information models)

업무 프로세스가 식별된 후에는 어떠한 프로세스 혹은 프로세스의 집단이 업무영향분석의 대상이 되는지를 결정해야 하는데 이를 위해서는 다음과 같은 사항을 고려해야 한다.

o 업무 영향분석의 범위

o 경영층의 중요 업무 프로세스에 대한 초기 인식

o 업무 프로세스간의 통합 및 상호의존성 정도

업무영향분석의 목적은 업무 중단으로 인한 영향을 평가하는 것이다. 업무 프로세스는 서로 밀접하게 통합되었거나 서로 의존되어 있을 경우에는, 업무 프로세스들은 업무영향분석의 목적을 위해서 함께 고려되어야 한다.

(바) 영향 시나리오의 정의

잠재적 업무영향은 각 프로세스의 영향 시나리오에 대해서 측정된다. 영향분석은 중요한 업무 프로세스들에 관한 시나리오에 의한 위험비용을 결정하는 방법으로서, 업무 혹은 서비스중단(disruption)의 영향을 파악하는 것이다. 영향 시나리오는 잠재적인 영향이 시간이 경과함에 따라 어떻게 변화하는 가를 파악하기 위해 여러 시간 간격을 고려하여 분석되어야 한다. 즉 주문처리 서비스가 하루, 이틀, 일주일, 또는 한 달 동안 중단되었을 경우의 영향을 파악해야 한다.

각 업무 프로세스에 대한 영향 시나리오와 시간 간격은 분석 대상에 포함되어 있는 위험에 따라 달라질 것이다.

잠재적 업무영향을 다음과 같은 시간 간격에 따라서 측정하면, 업무영향이 시r 간에 따라서 어떻게 변화하는지 나타나게 된다.

15분 이하, 1시간, 3시간, 12시간, 1일, 2일, 1주, 2주, 1달, 2달 이상 영향 시나

리오와 시간간격을 가능한 각 프로세스별로 파악된 후에, 경영층과 잠재적 업무영향을 측정하기 위한 토론 및 인터뷰가 실행되어야 한다.

(사) 잠재적 업무영향에 대한 측정

업무영향 시나리오를 파악한 후에, 업무 프로세스를 책임지는 관리자들과의 인터뷰에 의해서 업무영향을 측정하게 된다. 각 업무 프로세스에 대한 잠재적 업무영향은 각 영향 시나리오와 시간 간격 별로 측정된다. 업무영향의 영역에는 재무적(financial or hard)영역과 비재무적(non-financial or soft)혹은 운영적 영역이 있다. 재무적 영향은 화폐가치로 측정할 수 있으나, 비재무적 영향은 화폐가치로 측정할 수가 없다.

- o 재무적 영향 : 매출감소 혹은 장기적 시장 지분 감소, 이자증가, 계약위약금 혹은 법의 침해, 영업권 혹은 신용(goodwill or credibility)손실, 기타 추가비용
- o 운영적 영향 : 공공의 부정적 이미지, 주주들의 신뢰감 추락, 종업원들의 사기 저하, 개인의 안전에 대한 위험, 약속했던 서비스 수준 달성 실패, 법규 위반 또한, 재무적 영향을 평가하는 데는 다음과 같은 경우도 고려해야 한다. 영향 시나리오와 관련된 재무적 영향은 한계(marginal) 재무적 영향이다. 추가 작업 비용등과 같은 형태의 재무적 영향이라면, 이것은 개별적으로 기록한 후에 전체 재무적 영향을 평가하는데 결합시켜야한다. 운영적 혹은 비재무적 영향도 측정되어야 하지만, 주관적으로 측정되는 경우가 대부분이다. 보안 관리에서 사용되는 일반적인 위험평가방법은 재무적 및 운영적 영향을 기록하고 비교하는데 유용한 지침과 척도를 제공하고 있다.

2.5.3 업무연속성계획 유지보수 시험, 변경관리 [1급]

o 핵심가이드

- 업무연속성계획의 시험에 대한 이해 (시험방법과 유형)
- 업무연속성계획의 유지관리에 대한 이해 (교육/훈련, 변경관리)

(1) 업무연속성계획의 시험

초기시험은 전반적인 업무지속성관리 프로세스의 중요한 부분이며 선택한 전략, 재해복구대책, 업무복구계획 그리고 절차가 실제상황에서 유용하다는 것을 보장하는 유일한 방법이다.

초기 시험은 전략이 효과적으로 구현되었다는 것을 체크하기 위해서 그리고 계획이 공식적으로 발표되기 전에 필요한 수정을 허용하기 위한 구현 단계의 마지막 활

동이다. 초기 시험에 이어서 시험 유형(검토회, 기술부문 시험, 업무부문 시험, 전체 시험)의 적절한 혼합을 통한 지속적인 시험 프로그램을 구축해야 한다. 전체 시험은 업무중단과 그와 관련된 위험으로 인하여 거의 선택되지 않을 것이다. 그러므로 일반적인 시험 프로그램은 기술부문과 업무부문의 모든 시험으로 구성될 가능성이 높다. 구조적 검토회는 시험뿐만 아니라 팀 구성원의 재해복구에 대한 인식을 높이는 이중적인 효과를 가진다. 시험 빈도는 얼마나 빠르게 조직, 채택된 복구 전략과 목표가 변화하는가에 달려있다. 가장 중요한 업무 프로세스를 위한 재해복구대책은 적어도 일 년에 한번은 시험할 필요성이 있다. 시험 자체가 업무에 중요 방해 요인이 되지 않는다는 것을 보장하기 위해 신중하게 시험 계획을 작성할 필요가 있다. 또한 시험의 진행 프로세스는 변경 요구사항을 파악하고 실행되는지 여부를 보장하기 위해 면밀히 감시 및 검토되어야 한다.

초기 시험프로세스는 다음의 활동으로 구성된다.

- o 시험 목표의 개발
- o 시험 유형 결정
- o 시험 시나리오 구축
- o 시험 계획 개발
- o 시험 실행
- o 시험 결과의 문서화 발간

(가) 시험목표개발

초기 시험의 전형적인 목표는 다음과 같다.

1) 업무복구전략들에 대한 실질적인 평가
2) 업무복구계획에서 세부적으로 기술된 작업과 절차가 복구 목표를 달성하기 위해 필요한 실제 작업과 절차와 일치하는지에 대한 보장
3) 전략, 계획, 절차에 변경을 위해 필요한 요구사항 파악
4) 재해복구대책과 계획이 실제로 가동되었을 경우 제대로 작동할 것이라는 것을 보장

(나) 시험 유형의 결정

업무복구 시험은 일반적으로 4가지 형태로 분류된다.

1) 구조적 검토회 (Walk throughs)

팀이나 혹은 팀들이 여러 시나리오를 가정하면서 논리적인 토론을 거쳐 재해복구계획의 타당성이나 실증성을 검증하는 방법으로 종이를 이용하여 하는 방식

2) 기술적 구성요소 시험

전략과 계획에서 명시된 기술적 구성요소를 시험하는 것으로 예를 들면 다음과 같다.

o 외부에서 이루어진 재해 복구 계약의 실행 여부 시험

o 예비 공간에 비상접근 가능 여부 시험

o 예비 공간에 전화 서비스 설치 가능 여부 시험

3) 업무 구성요소 시험

업무 프로세스나 기능이 복구되는지 여부를 시험하는 것으로 이는 반드시 관련 있는 업무종사자가 포함되어야만 한다.

4) 모든 구성요소를 포함한 시험

(다) 시험 시나리오 구축

모든 시험은 충분한 현실성을 가지고 구축된 시험 시나리오를 이용하여야만 한다. 시험 시나리오의 예는 다음과 같다.

1) 빌딩의 3층에서 7층까지의 불로 인하여 무기한 빌딩으로의 접근이 불가능하다. 사고는 밤에 발생하였고 피해 직원은 없다.

2) 평일에 빌딩 밖에서 화학약품 유출사고가 발생 하였다. 반경 1마일 이내는 24시간 동안 대피하여야만 하고 직원 몇 명이 병원으로 후송되었다.

3) 중요 서비스 제공자가 부도를 냈다.

4) 가까운 전화국에서 폭탄이 터져 모든 서비스가 열흘 동안 중단되었다.

(라) 시험 계획 개발

부적절하게 계획된 시험은 오히려 조직에 중요 방해요인이 되는 위험요인이 될 수 있다. 주의 깊게 시험의 성격과 시기를 결정해야만 한다. 시험계획 준비를 위해 고려할 사항은 다음과 같다.

1) 시험팀의 파악 : 초기 시험 기간 동안 시험팀은 복구계획은 준비한 팀이어야 한다.

2) 시험을 위해 재정될 수 있는 시간

3) 시험을 위해 이용될 수 있는 자원(직원, 공간, 사무기구, 컴퓨터 시스템과 네트워크 그리고 통신설비)의 정도

5) 재정적인 한계

6) 시험으로 인해 허용될 수 있는 업무중단의 정도

(마) 시험의 실행

시험계획과 목표와 일치되게 시험이 진행되는가를 평가하기 위해서는 시험 프로세스를 감시할 필요가 있다. 감시는 일반적으로 시험을 담당하는 구성원이 작성하는 시험일지와 시험 감독관이 작성하는 기록을 통해서 이루어진다.

시험일지를 통해 다음의 사항들을 감독한다.

1) 사건의 신고 접수 기간
2) 업무 복구 목표가 성취되는 시간
3) 계획의 실행 가능성에 의문을 제기하는 사건
4) 제 3자와의 접촉 내용과 시간
5) 시험에 영향을 미치는 실제 사건의 세부적인 사항
6) 시험이 종결되는 시간

(바) 시험결과의 문서화와 발표

여러 시험 수행 후, 그 결과는 문서화되고 발간하여 재해복구전략과 재해복구대책, 위험감소 대책, 업무복구계획과 절차에 필요한 수정을 할 수 있도록 준비한다.

(2) 업무연속성계획의 유지관리

업무연속성을 위한 효과적인 유지관리는 매우 중요하다. 업무연속성 관리 생명주기에서 유지관리단계에 도달하면 대부분의 조직은 이미 전 단계를 거치면서 많은 시간과 재정적 자원을 투자하였다. 즉, 전략구축과 구현을 통해 업무연속성관리에 대한 이해와 경각심이 제고되었고 복구대책 구현을 위한 많은 투자가 진행되었다. 그러나 모든 조직이 지속적으로 변화하므로 이에 대한 적절한 관리구조나 프로세스 등을 통한 대응이 미흡할 경우, 재해복구 전략과 계획은 곧 쓸모없는 것이 될 것이다. 유지관리 단계에서는 다음과 같은 단계가 포함된다.

o 시험
o 교육과 경각심 제고
o 훈련
o 변경관리
o 보증

(가) 시험

세부내용은 앞의 “업무연속성계획의 시험“의 내용에 따른다.

(나) 교육과 경각심 제고

업무연속성 정책, 전략과 계획에 대한 교육과 경각심 제고는 조직 내 업무연속성관리 노력을 위해서는 필수 성공요인이다. 교육과 경각심 제고의 목적은 업무연속성관리가 관리활동의 일상적인 한 부분이 됨으로써 모든 주요 업무활동에 업무연속성이 고려되는 상황에 도달하도록 하는 것이다. 이는 업무연속성관리를 위한 효과적인 정책과 관리구조를 구축함으로써 이루어질 수 있다.

시험과 더불어 교육과 경각심 제고 프로그램은 다음과 같은 목표를 가진다.

1) 재해나 다른 중요한 사건에 대응하는 방식을 직원들에게 이해시킨다.
2) 업무연속성전략이나 계획에 영향을 줄 수 있는 변경인 이슈를 파악하고 실행한다.
3) 팀원이나 대리인이 그들의 책임과 취해야 할 행동에 대해 인식할 수 있다.

교육방법의 예는 다음과 같다.

4) 경계 필요성과 비상 절차를 모든 직원에게 브리핑
5) 핵심 직원에게 복구설비가 구비되어 있음을 전시
6) 업무연속성관리의 개괄적인 내용을 전달하기 위해 조직의 사보 사용
7) 정규 진행보고서를 이사회나 기타 위원회에 보고

(다) 훈련

교육 및 경각심 제고와 더불어 직원들에게 복구전략의 특정 요소에 대한 훈련이 필요하다.

다음은 훈련이 필요한 부분이다.

1) 비상시 사용되는 대체 프로세스나 시스템
2) 비상시 컴퓨터 시스템이나 네트워크의 재구성 방법
3) 자동 시스템이 복구될 때까지 사용되는 수작업 방식

(라) 검토와 변경통제

재해복구대책, 위험감소대책, 그리고 업무복구계획은 구현 당시의 업무의 요구사항을 반영하고 있다. 따라서 요구사항이 시간이 경과함에 따라 변경될 수 있으므로 재해복구 전략과 계획이 현실을 반영하여 효과적이기 위해서는 검토와 변경통제를 포함하는 변경관리 프로세스가 필요하다.

변경의 유형은 다음의 두 범주로서 구분될 수 있다.

1) 유지보수를 통한 변경

이러한 변경은 업무연속성계획의 현실성을 유지하는데 필요한 것이고 근본적으로 복구 목표나 업무 지속성 전략에 영향을 주는 것은 아니다. 예를 들면, 직원의 퇴사나 타부서 배치, 시스템 구성의 소규모 변화 등

2) 검토를 통한 변경

이러한 변경은 근본적으로 복구목표나 전략에 영향을 줄 수 있다. 예를 들면, 새로운 업무 프로세서의 도입, 시스템의 대폭적인 변화, 자산의 처분이나 구매 등으로 인한 변화

(마) 변경관리 프로세스

변경관리의 접근방법은 변경의 유형에 따라 다르나 변경관리 프로세스는 다음

과 같은 활동으로 구성된다.

o 변경 전략 결정

o 변경 요구사항 파악

o 변경 실행

o 계획과 절차 갱신

1) 변경 전략 결정

효과적인 변경관리를 위해서는 재해복구전력과 계획에 대한 명확한 소유권을 규정하는 것이 가장 기본적인 요구사항이다. 일반적인 소유권의 분류는 다음과 같다.

o 업무연속성전략과 마스터플랜은 복구 관리자에게 소유권이 있고 또는 복구 관리자를 대행하는 업무지속성 관리자에게 소유권이 있다.

o 모든 다른 계획은 관련된 팀 리더에게 소유권이 있다.

유지보수를 통한 변경인 경우에는 해당 계획 소유자에 의해 그 계획이 변경되면 변경된 내용 계획을 소지하고 있는 자에게 배포한다. 만약 해당 계획의 변경이 다른 계획에도 영향을 준다면 해당 계획 소유자는 관련 계획 소유자에게 사실을 알린다.

검토를 통한 변경인 경우에는 해당 계획 소유자나 중앙통제 팀원 또는 업무복구 팀원에 의해 변경 필요성이 제기되면 이를 업무지속성 관리자에게 통보한다. 업무지속성 관리자는 변경 내용을 검토하고 변경이 복구 목표, 재해복구대책, 위험감소대책, 그리고 업무복구계획에 미치는 영향을 평가한 후 필요한 변경을 실현하는 활동을 조화/통제한다.

2) 변경 요구사항 파악

변경 전략은 계획 소유자나 다른 구성원에 의해 인식되는 변경 필요성에 의해 결정된다. 변경을 위한 요구사항이 인식되는 것을 보장하기 위해 각각의 업무영역 내에서 변경 절차를 구비한다.

다음과 같은 이유로 해서 계획에 대한 변경이 이루어질 수 있다.

o 업무 변경 혹은 운영상의 변경

o 사무공간의 변경

o 컴퓨터 시스템과 네트워크의 변경

o 통신(전화, 팩스 등)변경

o 서비스 제공자 변경

3) 변경 실행

변경의 실행은 유지보수를 통한 변경인 경우에는 계획 소유자에 의해 실시되

고 검토를 통한 변경인 경우에는 업무연속성 관리자에 의해 실시된다.

검토를 통한 변경인 경우, 업무연속성 관리자는 다음과 같은 활동을 조사/통제해야 한다.

- o 변경을 통한 업무의 잠재적인 영향(업무방해)을 받게 된다면 변경에 따른 영향 분석을 수행하고 직원, 시스템, 통신을 위한 최소한의 요구사항 확인
- o 변경의 결과로 인하여 복구 목표의 수정이 필요한지 여부를 검토
- o 변경이 업무에 대한 잠재적인 위협 및 취약성을 변경시킬지 여부를 결정
- o 복구목표를 변함없이 달성하기 위해 기존의 복구전략과 재해복구대책이 수정될 필요가 있는지를 결정
- o 현재의 위험감소대책이 변경으로 인한 위험수준의 변화에 충분히 대처할 수 있는지 결정
- o 제안된 변경을 검토하고 중앙통제 팀으로부터 합의를 도출하고 필요하면, 최고 경영층/이사회로부터 승인을 획득

일단 재해복구 대책과 위험감소 대책이 구현되었고 업무연속성계획이 갱신되었다면 다음의 사항을 보장할 수 있어야 한다.

- o 변경된 계획에 대해 구조적 검토와 시험의 실행
- o 시험 프로그램을 필요에 따라 수정
- o 경각심 재고, 교육과 보증 프로그램을 필요에 따라 수정

유지보수를 통한 변경인 경우는 개별 계획소유자에 의해 실시된다. 변경을 실시하기 위해서는 다음과 같은 행동 중에 전부 혹은 일부를 포함할 수 있다.

- o 작업 리스트에서 필요한 변경 실시
- o 작업 리스트가 변경됨으로써 참고자료나 지원절차가 변경될 필요성이 있는지 결정
- o 변경이 다른 업무복구계획에 반영될 필요가 있는지 결정
- o 변경의 세부사항을 복사하여 업무연속성 관리자에게 전달

4) 계획과 절차의 배포

계획과 절차가 갱신된 후에 모든 팀원에게 배포해야 한다. 변경의 정도에 따라 이전 계획과 절차의 일부분을 교체하거나 아니면 완전한 새로운 버전이 될 수도 있다. 모든 갱신은 구 버전을 파기하는 절차와 신 버전 계획의 보관에 관한 지침을 포함하는 엄격한 버전 통제 하에 수행되어야 한다.

(바) 보증

업무연속성 관리 생명주기의 마지막 단계는 업무연속성 관리 결과물에 대한 품

질에 대해 상위 경영층이 만족하는지에 대한 보증과 운영관리 프로세스에서도 만족스럽게 작용하고 있는지 여부에 대한 보증의 획득을 포함한다. 업무연속성관리 결과물은 경영층의 검토를 통해 승인을 얻어야 한다. 만약 승인을 받았다면 차기 재검토 일자를 내포하고 있는 인증서를 발급하여 결과물 작성자에게 전달할 수 있다.

2.6 관련 표준/지침

2.6.1 국제/국가 표준 국제 협약 및 지침, OECD보안지침, 사이버공간 국가전략, 관리과정관련 표준/지침, GMITS, ISO17799등 정보보호제품 관련 표준 CC [1급]

o 핵심가이드

- OECD 정보보호 가이드라인의 9개 원칙
- 미국의 보안 평가 기준들에 대한 이해
- 정보보호 관리 표준/지침(BS7799)에 대한 이해
- 정보보호제품 관련 표준/지침(CC)에 대한 이해

(1) OECD 정보보호 가이드라인

(가) 인 식

참여자들은 정보시스템과 네트워크 보호의 필요성과 그 안전성을 향상시키기 이하여 취할 수 있는 사항을 알고 있어야 한다.

(나) 책 임

모든 참여자들은 정보시스템과 네트워크의 보호에 책임이 있다.

(다) 대 응

참여자들은 정보보호 사고를 예방, 탐지, 대응하기 위해서 적기에 협력해서 행동해야 한다.

(라) 윤 리

참여자들은 타인의 적법한 이익을 존중해야 한다.

(마) 민주성

정보시스템과 네트워크의 보호는 민주주의사회의 근본적인 가치들에 부합하여야 한다.

(바) 위험평가

참여자들은 위험 평가를 시행해야 한다.

(사) 정보보호의 설계와 이행

참여자들은 정보보호를 정보시스템과 네트워크의 핵심 요소로 수용하여야 한다.

(아) 정보보호 관리

참여자들은 정보보호관리에 대해 포괄적인 접근 방식을 채택해야 한다.

(자) 재평가

참여자들은 정보시스템과 네트워크의 보호를 검토하고 재평가하여 정보보호 정책, 관행, 조치, 절차를 적절히 수정해야 한다.

(2) 미국의 평가 기준

(가) TCSEC

1983년에 오렌지북으로 불리는 컴퓨터시스템 평가기준 초안 제정,

보안등급은 A, B, C, D 로 구분하며 기본 요구사항으로는 보안정책, 책임성, 보증, 문서화이다.

[표 4-15] TCSEC의 보안 등급

보안 등급	세부 보안등급	내 용	비 고
A	A1	검증된 설계 (Verified Design)	높은 등급
B	B3	보호 영역 (Security Domain)	
	B2	구조화된 보호 (Structured Protection)	
	B1	레이블을 이용한 보안 보호 (Labeled Security Protection)	낮은 등급
C	C2	통제적 접근 보호 (Controlled Access Protection)	
	C1	재량에 의한 보안 보호 (Discretionary Protection)	
D	D	최소한의 보호 (Minimal Protection)	

(나) TNI

NCSC에서 네트워크용 정보보호시스템의 평가를 위해 개발.

(다) TDI

NCSC에서 TCSEC을 기준으로 데이터베이스관리 시스템의 평가를 위해 개발, 보안 요구 사항으로는 보안 정책, 기록성, 보증, 문서화이다.

[표 4-16] TDI의 보안 등급

보안 등급	세부 보안등급	내 용	비 고
A	A1	검증된 설계 (Verified Design)	높은 등급
B	B3	보호 영역 (Security Domain)	
	B2	구조화된 보호 (Structured Protection)	
	B1	레이블을 이용한 보안 보호 (Labeled Security Protection)	낮은 등급
C	C2	통제적 접근 보호 (Controlled Access Protection)	
	C1	재량에 의한 보안 보호 (Discretionary Protection)	
D	D	최소한의 보호 (Minimal Protection)	

(라) CSSI

TCSEC의 평가기준을 모두 만족하지 못하고 일부 시스템만이 만족시키는 보안 제품에 대한 평가 기준

(2) ITSEC

유럽의 국가들이 자국의 정보보호시스템을 평가하기 위해 각각의 기준을 제정하여 시행하였다. TCSEC을 참고하여 만들어져 중복되는 내용이 많았으나, TCSEC과는 다르게 낮은 등급에서 높은 등급에 따라 적용되는 요구사항을 다르게 하였고, 단일 기준으로 모든 정보보호 제품을 평가하고자 하였다.

[표 4-17] ITSEC의 보안 요구사항

보안 기능	내 용
식별 및 승인 (Identification and Authentication)	• 신분 확인을 요청한 사용자에 대하여 이를 식별하여 검증하는 기능 • 식별 및 인증을 위해 사용자가 제공한 신분확인 관련 정보를 유지하고, 식별 및 인증 데이터의 추가, 삭제, 변경 등이 가능해야 함
접근 제어 (Access Control)	• 정보나 자원에 대한 접근 허가가 없는 사용자 또는 프로세스가 접근 허가를 얻는 것을 막기 위한 요구사항 • 허가받지 않은 자원의 생성,갱신, 삭제 등을 막아야 함 • 정보흐름에 대한 통제를 수행해야 함
책임성 (Accountability)	• 사용자 및 프로세스의 행동을 기록하여 문제가 발생하는 경우 책임 소재를 가릴 수 있는 연결고리를 유지하는 것
감사 (Audit)	• 감사정보에 대한 수집, 보호 및 분석 기능을 포함 • 분석을 통하여 보안위반 사건이 실제로 일어나기 전에 잠재성을 탐지하여 사전에 알려줄 수 있도록 함 •일상사건 및 예외사건에 대한 정보를 기록하여 보안 위반 사건이 실제로 발생하였는지 판단하고 이로 인해 정보나 다른 자원의 손해 정도를 알아내기 위한 기초자료로 활용
객체의 재사용 (Object Reuse)	• 보호대상인 주기억장치나 디스크 저장장소와 같은 자원들이 재사용 할 수 있도록 보장하는 내용 기록하는 요구사항 • 객체 재사용 기능에서는 데이터 재사용을 위한 제어기능까지 포함
책임성 (Accountability)	• 데이터가 허가받지 않은 방법에 의해 수정될 수 없도록 하여야 하며 연관된 데이터 사이의 관계를 정확하게 설정 및 유지할 수 있는 기능이 제공되어야 함
서비스의 신뢰성 (Reliability of Service)	• 시간이 중요한 요소로 작용하는 작업에 대해서는 정확한 시기에 수행 되도록 보장하여야 함 • 오류 검출 및 오류 복구 기능까지 제공하여 서비스에 대한 중단이나 손실을 최소화하도록 하며 외부 사건과 이에 대한 결과를 시간 내에 응답할 수 있도록 스케쥴링을 할 수 있어야 함
데이터 교환 (Data Exchange)	• 통신채널을 통하여 데이터가 전송되는 동안 데이터에 대한 보안기능을 제공하는 것 • 인증, 접근통제, 데이터 기밀성, 데이터 무결성, 부인방지 등의 보안서비스가 뒷받침되어야 함

(3) BS7799

정보보호관리체계에 대한 표준으로 최상의 정보보호관리를 위한 포괄적인 일련의 관리 방법에 대하여 요건 별로 해석해 놓은 규격으로 기업이 고객 정보의 기밀성, 무결성, 가용성을 보장한다는 것을 공개적으로 확인하는 것이 목적이다.

[표 4-18] BS7799 관리 항목

세션	내 용
보안 방침	정보보호에 대한 경영 방침과 지원 사항을 제공
보안 조직	조직 내 효과적인 정보보호 관리를 위해서 보안에 대한 책임을 배정
자산 분류 및 관리	조직의 자산에 대한 적절한 보호책 유지
인사 보안	사람들의 실수, 절도, 부정 행위나 설비의 잘못된 사용으로 인한 위험 감소
물리적 보안	비 인가된 접근에 의한 손상 및 사업장, 정보의 위험 방지
운영 관리	설비의 정확하고 안전한 운영보장
접근 통제	정보에 대한 접근 통제
시스템 개발 및 유지	정보 시스템 내에 보안이 수립되었음을 보장
업무 지속성 관리	업무 활동에 방해 요소를 완화시키며 주요 실패 및 재해 영향으로부터 주요 업무 활동을 보호
부합성	범죄 및 인사상의 법률, 법규, 규정 또는 보안 요구 사항의 불일치 회피

(가) BS7799 구축 및 인증단계

1) 보안정책 수립

정보보호정책을 규명하는 단계. 최고경영자를 비롯해 경영층의 정보보호에 대한 의지를 담고 있어 회사 사원들의 정보보호에 대한 인식, 태도에 큰 영향을 미친다.

2) 정보보호 관리체계 범위 수립

조직 전체 또는 일부자산, 시스템, 응용시스템, 서비스, 네트워크 그리고 정보처리, 저장 및 통신에 사용된 기술 등을 ISMS 범위로 정의하는 것을 말함.

3) 위험평가

자산에 대한 위협요인, 취약점 및 조직에 대한 영향을 식별하고 위험수준을 결정하는 과정을 말함.

4) 위험관리

위험평가를 토대로 적정한 수준의 위험요인 통제수단을 도출해야 하고 통제수단 선택 시 비용, 통제수단 구현기간 등의 변수와 조직이 얻을 수 있는 이익과의 관계를 고려해야함

5) 통제 및 통제목표설정

조직의 모든 위험 통제목표 및 방안은 규격서를 근거로 선택하고, 그 선택을 정당화 하는 과정

6) 통제사항 적용명세서 작성

선택한 통제목표 및 방안과 그 선택을 정당화 할 수 있는 사유를 적용성 보

고서로 문서화 하는 과정

(4) CC

한나라에서 평가 받은 제품을 다른 나라에서 사용하기 위해서는 다시 재평가 받아야 하는 문제가 있다. 이러한 재평가에 소요되는 비용을 줄이기 위하여 국제 공통기준(CC)이 탄생하게 되었으며 현재 ISO 국제 표준으로 제정되었다. CC는 크게 3가지 부분으로 구성되어 있는데 1부는 일반적인 소개와 일반모델을 제시, 2부는 보안기능 요구사항, 3부는 보증요구사항을 제시하고 있다.

(5) ISO/IEC TR 13335(GMITS)

GMITS는 문서의 성격상 특정 기술의 규격을 정한 표준의 성격을 갖는 것보다는 여러 소스로부터 자료를 수집하여 작성하였다. 원래 5개의 Part로 구성되어 있다. Part 1에서는 IT 보안관리를 설명하기 위해 사용되는 기본적인 개념 및 모델을 보여준다.

- o Part 2는 Part 1과 상당 부분 중복되어 1부와 개정 작업 중이며 삭제.
- o Part 3는 보안 관리 과정을 계획, 설계, 구현, 시험, 습득 또는 운영과 같은 생명주기 동안 동에 사용할 수 있는 보안기법을 기술.
- o Part 4는 정보보안 대책의 선택 지침을 제공하고 있다.
- o Part 5는 외부 네트워크에서 IT 시스템이 연결된 조직의 경우에 사용할 수 있는 네트워크 보안지침을 제공.

2.6.2 인증체계, 정보보호 관리체계 인증, 정보보호제품 인증 [1급]

o 핵심가이드

- 정보보호 관리체계 인증
- ISMS의 정의
- KISA와 KAB의 인증체계

(1) 정보보호 관리 체계 구축 및 인증 단계

(가) 정보보호 정책 정의

(나) ISMS 범위 정의

(다) 위험평가 수행

(라) 위험 관리

(마) 통제 목적과 구현되는 통제 방안 선택

(바) 적용 보고서 작성

(2) 목 적

(가) 정보자산의 안전, 신뢰성 향상

(나) 정보보호관리에 대한 인식 제고

(다) 조직의 정보보호역량 강화를 통한 국가 주요정보통신기반시설이 보호 및 국제적 신뢰도 향상

(라) 정보보호서비스 산업의 활성화

(3) ISMS의 정의

정보보호 관리시스템을 의미한다. 조직 정보보호의 근간으로서 정보보호 대상이 되는 자산의 식별, 위험평가 및 위험관리 방법과 그 구현을 위한 정보보호관리 활동 전체 체계를 의미한다.

(4) ISMS 인증심사 기준

(가) 정보보호 정책

(나) 정보보호 조직

(다) 외부자 보안

(라) 정보자산 분류

(마) 정보보호 교육 및 훈련

(바) 인적 보안

(사) 물리적 보안

(아) 시스템개발 보안

(자) 암호통제

(차) 접근통제

(카) 운영관리

(타) 운영관리

(파) 전자거래 보안

(하) 보안사고 관리

(거) 검토, 모니터링 및 감사

(너) 업무연속성 관리

(5) BS7799

(가) Part1

먼저 part1은 기업 내 정보보호관리에 있어 실질적으로 도움을 줄 수 있는 지침으로 총 10개의 section으로 구성되어 있으며, 정보보호 관리 최적의 실행 지침을 집대성한 것이다. 하지만 part1은 정보보호 업무를 수행하는 기업의 환경에 따라 선택할 수 있는 내용이 달라질 수 있으므로 BS7799 심사 및 인증을 위한 목적으로는 사용하지 못하도록 규정되어 있어 BS7799 심사원들의 참조문서로 사용되어 진다.

BS7799 part1이 다루는 정보보호의 분야는 다음과 같다.

- o Information Security Policy
- o Security Organization
- o Asset Classification and Control
- o Personnel Security
- o Physical and Environmental Security
- o Communications and Operations Management
- o Access Control
- o Systems Development and Maintenance
- o Business Continuity Management
- o Compliance

(나) Part2

part2는 정보 보호 관리시스템(ISMS)에 대한 규격서이다. 규격서라 함은 실제 BS7799 인증 심사 시 심사원들이 전적으로 의존하는 문서를 말하며 인증 심사는 이 part2규격서를 토대로 수행되어진다. Part2는 10개의 Clause, 36개의 Objective, 127 Control들로 이루어져 있으며 정보보호 관리시스템 문서화 및 실행에 대한 필요사항과 개별 조직의 필요성에 따라 선택적으로 실행될 수 있는 정보보호 관리요건을 규정하고 있다.

Part2규격서에는 조직은 문서화된 ISMS(Information Security Management System)를 구축하고, 유지 관리하여야 한다고 명시하고 있다. 보통 ISMS문서화 관련 요구사항은 해당 조직의 정보보호 통제 하에 포함되는 자산의 범위, 조직의 위험 평가 및 관리방안, 그리고 정보보호 통제목표 및 통제방안, 그리고 요구되는 보장수준 등을 문서화하여 언급하고 있으면 충족시킨다고 볼 수 있다.

(다) BS7799인증절차

조직 내 정보보호 관리체계가 수립되었다고 생각한다면 인증심사를 신청하면 된다. 우선 어느 인증기관에서 BS779인증을 받을 것이지 선택해야 하며 우리나라

에서는 BSI Korea를 비롯한 몇몇의 기관에서 인증 업무를 수행하고 있다. 인증기관을 선택한 후에는 인증기관과 심사비용, 기간 등 견적사항에 대해 합의를 한다. 그 후 인증기관에 인증 신청서를 제출하면 실질적인 심사가 시작되게 된다.

1) 1단계 심사

보통 Desktop Review라 불리는 과정으로 인증 심사를 위한 조직의 준비상태를 점검하는 과정이다. 심사원들은 이 단계에서 조직의 정보보호 정책, 정책을 지원하는 다양한 정보보호 관련 절차서, 위험평가 및 관리방법, 적용성 보고서 등을 살펴본다. 심사원들의 조직 ISMS의 이해를 위한 과정이고, 실질적인 감사를 위한 준비과정이라고 보면 된다.

2) 2단계 심사

BS7799 심사원들이 실제 현장을 방문하여 조직이 구축한 ISMS가 BS 7799의 요건에 부합하는지 확인하고, 입증 증거를 수집하는 단계이다. Desktop Review에서 검토된 사항들의 실제 적용여부도 감사하게 되며, 모든 BS7799 문서화 요구사항도 점검한다. 결론적으로 조직의 ISMS가 조직의 사업 목표, 환경에 적합하게 구축되어 효율적으로 작동하고 있는지 여부를 확인하는 과정이라고 보면 된다.

(그림 4-11) BS7799인증절차

(6) 국내 ISMS 인증체계

(가) 한국인정원(KAB)의 인증

1) BS 7799-2(심사규격, Requirement)

2) ISO/IEC 17799(수행평가지침)

(나) 한국정보보호진흥원(KISA)의 인증

1) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조 규정에 근거 인증기준
2) BS7799를 기반으로 국내 환경에 적합하게 작성
3) 5개 정보보호관리 과정
4) 15개 분야의 120개 세부통제항목
5) 인증업무지침

3. 관련법규

3.1 정보화촉진 기본법[1)]

3.1.1 정보보호의 정의 [1급]

o 핵심가이드

- 정보보호의 법률적 정의가 무엇인지를 정확히 알고, 일반적인 정의 또는 학술적인 정의와의 차이를 이해한다.

(1) 관련조항

제2조 제4호

3.1.2 정보화시책의 기본원칙 [1급]

o 핵심 가이드

- 개인의 사생활 보호(프라이버시)와 정보자료의 안전성 유지 같은 정보보호는 정부가 정보화촉진 등을 위한 시책을 강구함에 있어서 따라야 할 중요한 기본원칙이다.

(1) 제3조 (정보화시책의 기본원칙)

3.1.3 정보화촉진기본계획 [1급]

o 핵심 가이드

- 행정, 산업, 재정·금융, 교육·연구·과학기술·환경, 지역·문화·생활 기타 분야별 정보보호와 개인정보보호호에 관한 기본 사항을 이해한다.

(1) 5조 정부는 정보화 촉진등을 위하여 5년의 기간을 단위로 하는 정보화촉진기본법(이하 “기본계획”이라 한다)을 수립하여야 한다.

(2) 기본계획에 포함되어야할 사항

제3조 ③항의 1~15.

---

1) 이 가이드라인의 정보화촉진기본법에 관한 법률은 2004.12.30 법률 7265호를 참고하였으며 2005. 12. 30 개정 법률 제7814호는 SIS 제 10회(1급), 12(2급)부터 적용된다.

3.1.4 정보보호시책 강구 [1급]

o 핵심가이드

- 정보보호에 필요한 시책을 강구할 정부의 책무와 정보통신서비스 안전조치를 강구할 정부의 책무에 대하여 이해한다.

(1) 정부의 책무

제14조 (정보보호 등) ① 정부는 정보의 안전한 유통을 위하여 정보보호에 필요한 시책을 강구하여야 한다.

(2) 암호기술 개발 및 이용 및 정보통신 서비스 안전조치를 강구할 책무

3.1.5 정보보호시스템 평가, 인증 [1급]

o 핵심가이드

- 정보보호 시스템의 기준고시, 권고, 감리에 대한 내용과 절차에 대하여 이해한다.

(1) 정보보호시스템 성능 및 신뢰도 기준 고시, 권고

제15조 (정보보호시스템에 관한 기준고시등) ①항, ②항, ③항.

(2) 정보보호 시스템 평가 및 인증

제15조의 2 (정보시스템에 대한 감리) ①항, ②항.

3.2 정보통신망 이용촉진 및 정보보호 등에 관한 법률[2)]

3.2.1 용어의 정의

o 핵심가이드

- 정보보호와 관련된 용어의 정의(특히 “개인정보”)를 정확히 이해한다.

(1) 정보화촉진기본법의 용어정의 준용

제 2조.

3.2.2 정보통신망이용촉진 및 정보보호 등 시책강구

2) 이 가이드라인의 정보화촉진기본법에 관한 법률은 2004.12.30 법률 7262호를 참고하였으며 2005. 12. 30 개정 법률 제7812호 는 SIS 제 10회(1급), 12(2급)부터 적용된다.

o 핵심가이드

- 정보통신망의 정보사회의 기반을 조성하기 위한 시책 마련에 대한 정보통신부장관의 책무, 시책 내용, 서비스이용자의 책무, 정보화촉진 기본계획과의 연계에 대한 내용을 이해한다.

(1) 정보통신부장관의 책무

제 4조 ①항.

제 3조 ③항.

(2) 시책의 내용

제 4조 2항

(2) 정보화촉진 기본계획과의 연계

제4조 (정보통신망이용촉진및정보보호등에 관한 시책의 강구) ③항.

3.2.3 타 법률과의 관계

o 핵심가이드

- 정보보호와 관련하여 타 법률과의 관계는 어떠한지 이해한다.

(1) 정보보호에 관하여 특별한 규정이 있는 다른 법률이 우선

정보보호와 관련하여 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 다른 법률과의 관계에서 일반법의 지위를 가짐.

제5조 (다른 법률과의 관계)

3.2.4 개인정보보호

o 핵심가이드

- 개인정보의 수집과 관련한 정보통신서비스 제공자의 의무와 제한, 고지의무, 영업양수 등의 통지, 개인정보 책임관리자, 개인정보보호조치, 개인정보파기, 개인정보이용자의 권리, 개인정보 분쟁 조정위원회, 개인정보관련 국제계약의 제한에 대한 법적 내용에 대하여 알아보고 이해한다.

(1) 개인정보의 수집과 관련한 정보통신서비스 제공자의 의무와 수집제한

제22조 (개인정보의 수집) ①항, ②항.

(2) 개인정보의 이용 및 제공과 관련한 정보통신서비스제공자의 의무

제23조 (개인정보의 수집의 제한 등) ①항, ②항, ③항, ④항.

제25조 (개인정보수집 등의 위탁) ①항, ②항, ③항.

제26조 (영업의 양수 등의 통지) ①항, ②항.

제27조 (개인정보관리책임자의 지정) ①항, ②항.

제28조 (개인정보의 보호조치)

제29조 (개인정보의 파기)

(3) 개인정보와 관련한 이용자의 권리

제30조 (이용자의 권리 등) ①항, ②항, ③항, ④항, ⑤항, ⑥항, ⑦항.

제31조 (법정대리인의 권리) ①항, ②항, ③항.

제32조 (손해배상)

(4) 개인정보 분쟁 조정위원회

제33조 (개인정보분쟁조정위원회의 설치 및 구성) ①항, ②항, ③항, ④항, ⑤항, ⑥항.

제34조 (위원의 신분보장)

제35조 (위원의 제척・기피・회피) ①항, ②항, ③항

제36조 (분쟁의 조정) ①항, ②항, ③항.

제37조 (자료요청 등) ①항, ②항.

제38조 (조정의 효력) ①항, ②항, ③항, ④항.

제39조 (조정의 거부 및 중지) ①항, ②항.

제40조 (조정절차 등)

(5) 개인정보관련 국제계약의 제한

제54조 (국외이전 개인정보의 보호) ①항, ②항, ③항, ④항.

(6) 정보통신서비스 제공자외의 자에 대한 준용

제58조 (정보통신서비스제공자외의 자에 대한 준용) ①항, ②항.

3.2.5 정보통신망의 안정성 확보

o 핵심가이드

- 정보통신망의 안정성을 확보하기 위한 정보통신서비스제공자의 정보보호조치와 집적정보통신시설운영·관리자의 정보보호조치 의무에 대하여 알고 정보보호관리체

계의 인증에 대한 내용을 이해한다.

(1) 정보통신서비스제공자의 정보보호조치(제3조1항, 제45조)
제3조 (정보통신서비스제공자 및 이용자의 책무) ①항.
제45조 (정보통신망의 안정성 확보 등) ①항, ②항, ③항, ④항.
(2) 집적정보 통신시설 운영관리자의 정보보호조치 의무 (제46조)
제46조 (집적된 정보통신시설의 보호) ①항, ②항.

(3) 정보보호 관리체계 인증 (제 47조)
제47조 (정보보호관리체계의 인증) ①항, ②항, ③항, ④항.

3.2.6 정보통신망 침해행위 등의 금지
o 핵심가이드
- 해킹, 컴퓨터 바이러스 유포, 서비스거부공격 등으로 인한 침해행위 금지와 타인 정보에 대한 훼손과 침해, 광고성 정보전송의 제한과 중요정보 국외유출에 대한 법적 조항을 이해한다.

(1) 해킹, 컴퓨터 바이러스 유포, 서비스거부공격의 금지
제48조 (정보통신망 침해행위 등의 금지) ①항, ②항, ③항.

(2) 타인정보의 훼손・침해
제49조 (비밀 등의 보호)

(3) 광고성 정보전송의 제한
제50조 (영리목적의 광고성 정보전송의 제한) ①항, ②항, ③항, ④항, ⑤항, ⑥항, ⑦항.

(4) 중요정보의 국외유출 제한
제51조 (중요정보의 국외유출제한 등) ①항, ②항.

3.2.7 한국정보보호진흥원
o 핵심가이드
- 한국정보보호진흥원의 설립이유와 운영 및 사업내용, 비밀유지의 의무에 대한 내

용을 이해한다.

(1) 운영 및 사업내용

제52조 (한국정보보호진흥원) ①항, ②항, ③항, ④항, ⑤항, ⑥항, ⑦항.

(2) 비밀유지의무

제57조 (비밀유지 등)

3.2.8 벌칙

o 핵심가이드

- 타인의 명예훼손에 대한 벌칙과 각 규정을 위반했을 시 과태료에 대한 내용을 이해한다.

(1) 제61조 내지 제 67조

제61조 (벌칙) ①항, ②항, ③항.

제67조 (과태료) ①항, ②항, ③항, ④항, ⑤항, ⑥항.

3.3 정보통신기반 보호법[3)]

3.3.1 용어의 정의

o 핵심가이드

- 정보통신기반 보호법과 관련된 용어의 정의를 정확히 알고, 각 용어의 차이점과 의미를 이해한다.

(1) 정보통신 기반시설

제1조의 1.

(2) 전자적 침해행위

제1조의 2.

(3) 침해사고

3) 이 가이드라인의 정보통신기반 보호법에 관한 법률은 2005.3.31 법률 7428호를 참고하였다.

제1조의 3.

3.3.2 주요정보통신 기반시설 보호체계

o 핵심가이드

- 주요정보통신 기반시설 보호체계의 용어를 이해하고, 각 시설들의 역할과 보호체계를 이해한다.

(1) 정보통신기반보호위원회

제3조 (정보통신기반보호위원회) ①항, ②항, ③항, ④항, ⑤항.

제4조 (위원회의 기능)

(2) 관계중앙행정기관

제6조 (주요정보통신기반시설 보호계획의 수립 등) ①항, ②항, ③항, ④항, ⑤항, ⑥항.

(3) 주요 정보통신기반시설 보호 지원 기관의 장

제 7조 (주요정보통신기반시설의 보호지원) ①항, ②항, ③항.

3.3.3 주요정보통신기반시설의 지정과 취약점 분석

o 핵심가이드

- 정보통신기반시설의 지정 요건과 절차, 취약점 분석·평가의 방법 및 절차를 이해한다.

(1) 지정요건과 절차

제8조 (주요정보통신기반시설의 지정 등) ①항, ②항, ③항, ④항, ⑤항, ⑥항, ⑦항.

(2) 취약점 분석·평가의 방법 및 절차

제9조 (취약점의 분석・평가) ①항, ②항, ③항, ④항, ⑤항.

3.3.4 주요정보통신기반시설의 보호 및 침해사고 대응

o 핵심가이드

- 주요정보통신기반시설의 보호 지침 및 조치와 대응방법을 이해한다.

(1) 보호지침의 재정, 권고

제10조 (보호지침) ①항, ②항.

(2) 보호조치명령

제11조 (보호조치 명령 등) ①항, ②항.

(3) 침해행위 등의 금지

제12조 (주요정보통신기반시설 침해행위 등의 금지)

(4) 침해사고의 통지

제13조 (침해사고의 통지) ①항, ②항.

(5) 복구조치

제14조 (복구조치) ①항, ②항, ③항.

(6) 대책본부

제15조 (대책본부의 구성 등) ①항, ②항, ③항, ④항, ⑤항, ⑥항.

(7) 정보공유분석센터

제16조 (정보공유・분석센터) ①항, ②항, ③항, ④항, ⑤항.

3.3.5 정보보호컨설팅 전문업체

o 핵심가이드

- 정보보호컨설팅전문업체의 지정기준 및 절차, 결격사유, 양도·합병, 휴지·폐지·재개 등의 경우 절차, 지정취소, 기록・자료의 보존에 대한 규정을 이해한다.

(1) 지정기준 및 절차

제17조 (정보보호컨설팅전문업체의 지정) ①항, ②항, ③항, ④항.

(2) 결격사유

제18조 (결격사유)

(3) 양도·합병, 휴지·폐지·재개 등

제19조 (정보보호컨설팅전문업체의 양도・합병 등) ①항, ②항, ③항.

제20조 (업무의 휴지・폐지・재개)

(4) 지정취소, 기록·자료의 보존 등

제21조 (정보보호컨설팅전문업체의 지정취소 등)

제23조 (기록・자료의 보존 등) ①항, ②항, ③항.

3.3.6 비밀유지의무

o 핵심가이드

- 직무상 알게 된 비밀의 유지와 예외 규정을 이해한다.

(1) 제27조 (비밀유지의무)

3.3.7 벌칙

o 핵심가이드

- 각 규정을 위반 하였을 시 행해지는 처벌과 과태료에 대한 내용을 이해한다.

(1) 28조 내지 30조

제28조 (벌칙) ①항, ②항.

제29조 (벌칙)

제30조 (과태료) ①항, ②항, ③항, ④항, ⑤항.

3.4 전자서명법[4)]

3.4.1 용어의 정의

o 핵심가이드

- 전자서명, 공인전자서명, 인증서, 공인인증서, 공인인증기관, 가입자, 서명자 등의 전자서명법상 용어의 법률적 정의에 대한 기본적인 이해를 요한다.

(2) 전자서명법 용어정리

제 2조 1~ 13.

4) 이 가이드라인의 정보통신기반 보호법에 관한 법률은 2005.3.31 법률 7428호를 참고하였으며 2005. 12. 30 개정 법률 제7813호 는 SIS 제 10회(1급), 12(2급)부터 적용된다.

3.4.2 전자서명의 효력

o 핵심가이드

- 전자서명이 가지는 효력과 효력이 발생되는 조건을 이해한다.

(1) 제3조 (전자서명의 효력 등) ①항, ②항, ③항.

3.4.3 공인인증기관

o 핵심가이드

- 공인인증기관의 지정기준 및 절차, 결격 사유를 정확히 이해하고 업무수행의 제반에 대한 내용을 이해해야 한다.

(1) 지정정차

제4조 (공인인증기관의 지정) ①항, ②항, ③항, ④항, ⑤항.

(2) 결격사유

제5조 (결격사유)

(3) 공인인증업무준칙 등

제 6조의 ①항, ②항, ③항, ④항.

(4) 공인인증업무 수행

제8조 (공인인증기관의 업무수행)

(5) 인증업무의 휴지·폐지 등

제 10조 ①항, ②항, ③항, ④항, ⑤항.

(6) 시정명령, 업무정지, 지정취소 등

제 11조 1~12.

3.4.4 공인인증서

o 핵심가이드

- 공인인증서의 발급, 효력소멸, 효력정지, 폐지 등 공인인증서에 관한 규정내용 특히 공인인증서의 내용 및 법률효과에 대하여 유의한다.

- 공인인증서를 이용한 본인확인에 대해서 이해한다.

(1) 공인인증서의 발급

제15조 (공인인증서의 발급) ①항, ②항, ③항, ④항, ⑤항, ⑥항.

(2) 공인인증서의 효력의 소멸

제16조 (공인인증서의 효력의 소멸 등<개정 2001.12.31>) ①항, ②항, ③항.

(3) 공인인증서의 효력정지

제17조 (공인인증서의 효력정지 등) ①항, ②항.

(4) 공인인증서의 폐지

제18조 (공인인증서의 폐지) ①항, ②항.

(5) 공인인증서를 이용한 본인확인

제18조의2 (공인인증서를 이용한 본인확인)

3.4.5 인증업무의 안전성 및 신뢰성 확보

o 핵심가이드

- 인증업무의 안전성 및 신뢰성 확보를 위한 보호조치, 인증업무에 관한 시설 및 장비의 안전 운영, 전자문서의 시점 확인, 전자서명생성정보 및 개인정보 보호에 관한 규정 내용을 이해한다.

(1) 안전성 확보

공인인증기관은 인증업무에 관한 시설의 안전성 확보를 위하여 정보통신부령이 정하는 보호조치를 취하여야 한다.

(2) 인증업무설비 운영

제19조 (인증업무에 관한 설비의 운영) ①항, ②항, ③항

(3) 전자문서 시점확인

제20조 (전자문서의 시점확인)

(4) 정보·기록등 관리

(가) 전자서명생성정보의 관리

제 21조

(나) 인증업무에 관한 기록의 관리

제 22조

(다) 공인인증서의 관리

제 22조의 2

(5) 전자서명생성정보 및 개인정보 보호

제23조 (전자서명생성정보의 보호 등) ①항, ②항, ③항, ④항, ⑤항.

제24조 (개인정보의 보호) ①항, ②항.

3.4.6 이용자의 준수사항, 특정 공인인증서 요구금지, 배상책임

o 핵심가이드

- 이용자의 준수사항, 특정 공인인증서 요구금지와 공인인증기관의 인증업무 수행과 관련한 손해배상에 대하여 이해한다.

(1) 이용자의 준수사항

제25조의2 (이용자의 준수사항)

(2) 특정 공인인증서 요구금지

제25조의3 (특정 공인인증서 요구 금지)

(3) 배상책임

제26조 (배상책임) ①항, ②항.

3.4.7 전자서명인증정책 추진 등

o 핵심가이드

- 전자서명의 안전성과 신뢰성을 확보하고 그 이용을 활성화하는 등 전자서명 및 인증업무의 발전을 위한 정부의 시책 수립·시행, 상호연동, 기술개발 및 인력양성, 시범사업 및 지원에 관한 규정 내용을 이해한다.

(1) 시책의 수립

제26조의2 (전자서명인증제도의 발전을 위한 시책의 수립 등)

(2) 상호연동

제26조의3 (전자서명의 상호연동) ①항, ②항.

3.4.8 벌칙

o 핵심가이드

- 각 호에 해당하는 위반 행동에 따른 벌칙과 과태료에 대한 내용을 이해한다.

(1) 벌칙

제31조 (벌칙)

(2) 과태료

제34조 (과태료) ①항, ②항, ③항, ④항, ⑤항.

3.5 전자거래 기본법[5)]

3.5.1 전자서명 [1급]

o 핵심가이드

- 전자서명의 법적 효력에 대하여 이해한다.

(1) 전자서명에 관하여 전자서명법을 준용

제11조 (전자서명에 관한 사항)

3.5.2 정보보호 [1급]

o 핵심가이드

- 개인정보보호의 전자거래당사자의 의무와 안전대책마련에 대한 내용을 이해하여야 한다.
- 영업비밀보호의 정의와 영업비밀 침해행위, 손해배상책임과 신용회복을 위한 조치와, 선의자에 관한 특례에 대한 법률적 내용에 대한 이해가 필요하다.

(1) 개인정보보호

5) 이 가이드라인의 정보통신기반 보호법에 관한 법률은 2005.3.31 법률 7440호를 참고하였다.

제12조 (개인정보보호) ①항, ②항.

(2) 영업비밀보호

제13조 (영업비밀보호) ①항, ②항, ③항, ④항.

3.5.3 암호제품의 사용 [1급]

o 핵심가이드

- 암호제품 사용에 대한 정부의 허가 및 규제에 대한 내용을 이해한다.

(1) 암호제품의 사용

제14조 (암호제품의 사용) ①항, ②항.

참 고 문 헌

[1] 정철헌, PKI전자서명과 인증제도, 다산출판사, 2003.

[2] 이만영 외 5명, 현대암호학 및 응용, 생능출판사, 2002.

[3] 서광석 외 1명, 초보자를 위한 암호와 타원곡선, 경문사, 2000.

[4] 강주성 외 6명, 현대암호학, 경문사, 2000.

[5] 원동호, 현대암호학, 도서출판 그린, 2003.

[6] 이민섭, 현대암호학, 교우사, 2001.

[7] 김세헌, 정보보호관리 및 정책, 생능출판사, 2002.

[8] William Stalling, 컴퓨터통신보안, 도서출판 그린, 2002.

[9] 이홍섭 외 1명, 정보보호관리, 생능출판사, 2003.

[10] 이동훈 외 4명, Summation Generator에 대한 대수적공격, 국가보안기술연구소, 2004.

[11] 한국전자통신연구원, “Ctypropia 제 6권 3호”, 국가보안기술연구소, 2002

[12] 국가공인 정보보호 전문가 자격증 모임, http//cafe.naver.com/nsis.cafe

[13] 한국정보보호진흥원, http://www.kisa.or.kr

[14] 법제처, http://www.moleg.go.kr