정보보호의 목표

구분	개념
기밀성(Confidentiality)	오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 한다는 원칙
무결성(Integrity)	정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질
가용성(Availability)	정당한 사용자가 정보시스템의 데이터 또는 자원을 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질
인증성(Authentication)	임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 성질
책임추적성(Accountability)	보안 목적에는 개체의 행동을 유일하게 추적해서 찾아낼 수 있어야 한다는 사항
부인방지(Non-repudiation)	행위나 이벤트의 발생을 증명하여 나중에 그런 행위나 이벤트를 부인할 수 없도록 하는 것

연습문제

정보보안 3요소에 대한 〈보기〉의 설명에서 (가), (나), (다)에 들어갈 말을 옳게 짝지은 것은?

보기

(가) 은 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것을 말하며 변경, 가장, 재전송 등과 같은 공격에 의해 위협받을 수 있다.
(나) 은 인가된 사용자만 정보 자산에 접근할 수 있다는 것으로 일반적인 보안의 의미와 가장 가깝다. 방화벽, 암호 패스워드 등이 대표적인 예이다.
(다) 은 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것을 말하며 DDoS와 같은 공격에 의해 위협 받을 수 있다.

	(가)	(나)	(다)
①	무결성	가용성	기밀성
②	무결성	기밀성	가용성
③	기밀성	가용성	무결성
④	기밀성	무결성	가용성

주요 암호기술

1) 대칭키 암호와 비대칭키(공개키) 암호

① 대칭키 암호(symmetric cryptography)는 암호화할 때 사용하는 키와 복호화할 때 사용하는 키가 동일한 암호 알고리즘 방식이다.

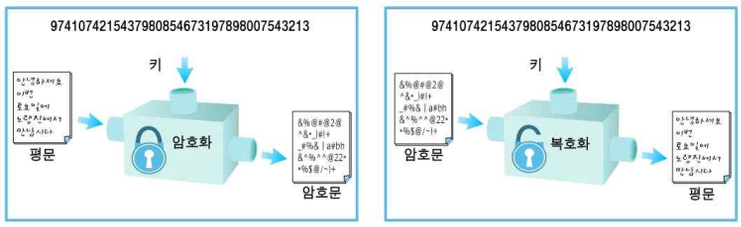
② 대칭키 암호화 방식은 공개키 암호화 방식에 비해 빠른 처리속도를 제공하고, 암호키의 길이가 공개키 암호화 방식보다 상대적으로 작아서 일반적인 정보의 기밀성을 보장하기 위한 용도로 사용되고 있다.

③ 비대칭키 암호(asymmetric cryptography)는 암호화할 때 사용하는 키와 복호화할 때 사용하는 키가 서로 다른 암호 알고리즘 방식이다.

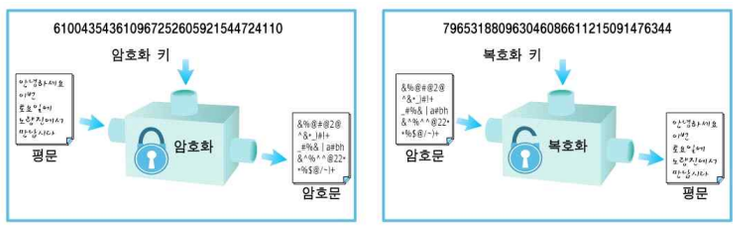
④ 비대칭키 암호 알고리즘을 사용하기 위해서는 송신자도 한 쌍의 키를 가지고 있어야 하며, 수신자도 자신만의 한 쌍의 키를 가지고 있어야 한다.

⑤ 이 한 쌍의 키를 이루는 두 개의 키를 공개키와 개인키라고 하는데, 공개키를 공개하게 되므로 이 암호 알고리즘을 공개키 암호(public-key cryptography)라고 부르기도 한다.

⑥ 공개키 암호는 1970년대에 발명되어 암호의 세계에 일대 변혁을 가져온 방법이다. 현대 컴퓨터 인터넷에서 사용하는 보안 기술은 공개키 암호에 크게 의존하고 있다.



대칭키 암호: 암호화와 복호화에 동일한 키를 사용



비대칭키 암호: 암호화와 복호화에 서로 다른 키를 사용

2) 하이브리드 암호시스템

① 대칭키 암호와 공개키 암호를 조합한 암호 방식을 하이브리드 암호 시스템(hybrid cryptosystem)이라고 한다.

② 하이브리드 암호 시스템은 대칭키 암호와 공개키 암호의 장점을 조합한 것이다.

3) 일방향 해시함수

① 해시함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해시값 또는 해시 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해시값만으로 입력 메시지를 유추할 수 없어 비밀번호와 같이 복호화 없이 입력값의 정확성 검증이 필요한 경우에 사용되고 있다.

✔ 연습문제

암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 일반적으로 대칭키 암호 알고리즘은 비대칭키 암호 알고리즘에 비하여 빠르다.

② 대칭키 암호 알고리즘에는 Diffie-Hellman 알고리즘이 있다.

③ 비대칭키 암호 알고리즘에는 타원 곡선 암호 알고리즘이 있다.

④ 인증서는 비대칭키 암호 알고리즘에서 사용하는 공개키 정보를 포함하고 있다.

모듈러(Modular) 연산

1) 정의

① Q는 몫, R은 나머지라 하고, 나눗셈을 다음과 같이 정의할 때,

$$\frac{A}{B} = Q\text{와 나머지 } R$$

② 나눗셈에서 사용된 기호를 그대로 사용하여 모듈러 연산을 나타내면 아래와 같이 나타낼 수 있다.

$$A \bmod B = R$$

③ 즉 모듈러 연산은 나눗셈에서 발생한 나머지를 구해주는 연산이라고 할 수 있다.

2) 모듈러 연산의 성질

① 모듈러 연산은 다양한 성질을 가지지만, 알고리즘 문제에서 가장 많이 활용되는 성질은 다음의 성질이다.

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$
$$(A - B) \bmod C = (A \bmod C - B \bmod C) \bmod C$$
$$(A \times B) \bmod C = (A \bmod C \times B \bmod C) \bmod C$$

3) Modular 연산의 적용 사례 : RSA 알고리즘의 키 생성

① 알고리즘

- p와 q라고 하는 두 개의 서로 다른 $(p \neq q)$ 소수를 고른다.
- 두 수를 곱하여 $N = pq$을 찾는다.
- $\phi(N) = (p-1)(q-1)$를 구한다.
- $\phi(N)$보단 작고, $\phi(N)$과 서로소인 정수 e를 찾는다.
- $d \times e$를 $\phi(N)$로 나누었을 때 나머지가 1인 정수 d를 구한다.
  $(de \equiv 1 \pmod{\phi(N)})$

✔ 연습문제

RSA 암호알고리즘을 위해 두 개의 소수가 p=3, q=11일 경우, 공개키(n)와 암호화 공개키(e=7)에 대응되는 복호용 개인키(d)로 적절한 것은?

① n=33, d=3

② n=21, d=5

③ n=21, d=3

④ n=33, d=5

접근통제

1) 접근통제 3단계

단계	설명
식별	◦ 본인이 누구라는 것을 시스템에 밝히는 것 ◦ 인증 서비스에 스스로를 확인시키기 위하여 정보를 공급하는 주체의 활동 ◦ 식별자는 각 개인의 신원을 나타내기 때문에 사용자의 책임추적성 분석에 중요한 자료가 됨
인증	◦ 주체의 신원을 검증하기 위한 사용 증명(verify, prove) 활동 ◦ 본인임을 주장하는 사용자가 그 본인이 맞다고 시스템이 인정해 주는 것
인가	◦ 인증된 주체에게 접근을 허용하고 특정 업무를 수행할 권리를 부여하는 과정 ◦ 알 필요성(Need-to-know): 주체에게 어떤 정보가 유용할지 여부와 관계가 있는 공인된 형식상의 접근수준

2) 사용자 인증의 유형

유형	설명	예
Type1 (지식)	주체는 그가 알고 있는 것을 보여줌(Something you know)	패스워드, 핀(PIN)
Type2 (소유)	주체는 그가 가지고 있는 것을 보여줌(Something you have)	토큰, 스마트 카드
Type3 (존재)	주체는 그를 나타내는 것을 보여줌(Something you are)	지문
(행위)	주체는 그가 하는 것을 보여줌(Something you do)	서명, 움직임
Two Factor	위 타입 중에서 두 가지 인증 메커니즘을 결합하여 구현	토큰+PIN
Multi Factor	가장 강한 인증으로 세 가지 이상의 인증 메커니즘 사용	토큰+PIN+지문인식

연습문제

사용자 인증 방법 중에서 신분증, 주민등록증 등을 이용하여 인증하는 방법으로 가장 적절한 것은?

① 지식 기반 인증(What you know)

② 소유 기반 인증(What you have)

③ 커버로스 인증(Kerberos)

④ 생체 기반 인증(What you are)

접근통제 모델

항목	MAC	DAC	RBAC
정의	주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근통제	접근하고자 하는 주체의 신분에 따라 접근권한을 부여하는 접근통제	주체와 객체 사이에 역할을 부여하여 임의적, 강제적 접근통제의 약점을 보완한 방식
권한부여	System	Data Owner	Central Authority
접근결정	Security Label	신분	역할(Role)
정책	경직	유연	유연
장점	중앙집중, 안정적	유연함, 구현 용이	관리용이
단점	구현 및 운영의 어려움 성능, 비용이 고가	트로이목마에 취약, ID도용 시 통제방법이 없음	-
적용 사례	방화벽	ACL	HIPAA

연습문제

임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?

① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙에 기반을 둔다.

② 주체 또는 주체가 소속되어 있는 그룹의 식별자(ID)를 근거로 객체에 대한 접근을 승인하거나 제한한다.

③ 소유권을 가진 주체가 객체에 대한 권한의 일부 또는 전부를 자신의 의지에 따라 다른 주체에게 부여한다.

④ 전통적인 UNIX 파일 접근제어에 적용되었다.

악성 소프트웨어의 분류

구분		설명	종류
독립형과 기생형	독립형	자체적으로 구동될 수 있는 프로그램으로 운영체제에 의해 스케줄되어 구동	웜, 좀비
	기생형	프로그램 단편으로 다른 실제 응용프로그램이나 유틸리티나 시스템 프로그램 없이 독립적으로 존재할 수 없음.	바이러스, 논리폭탄, 백도어
자기 복제 여부	바이러스성	자기 복제 함	웜, 바이러스
	비-바이러스성	자기 복제 안 함	트로이목마, 백도어

연습문제

다음은 트로이목마의 특징에 대한 설명이다. 성격이 가장 다른 하나는?

① 원격조정

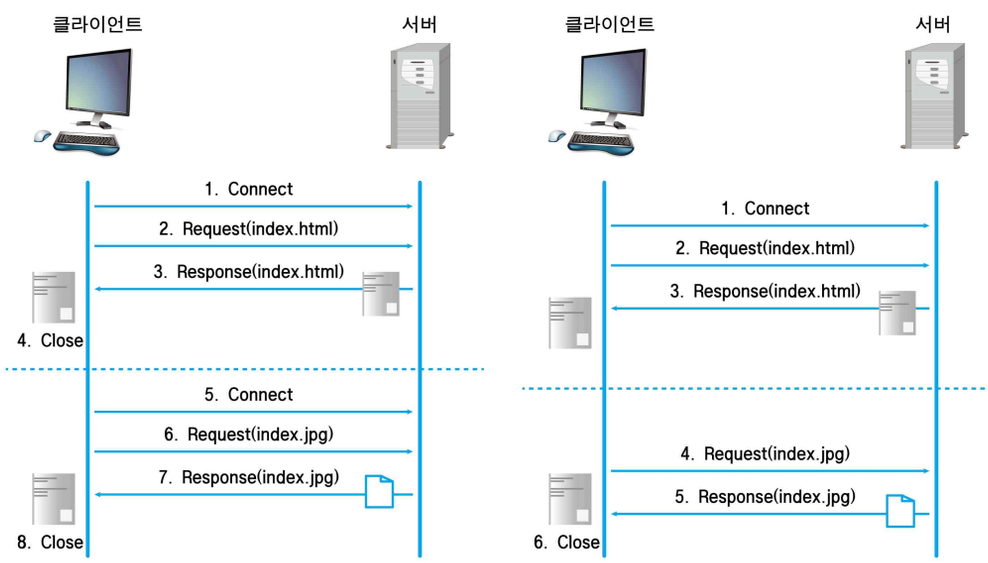
② 시스템 파일 파괴

③ 자기복제

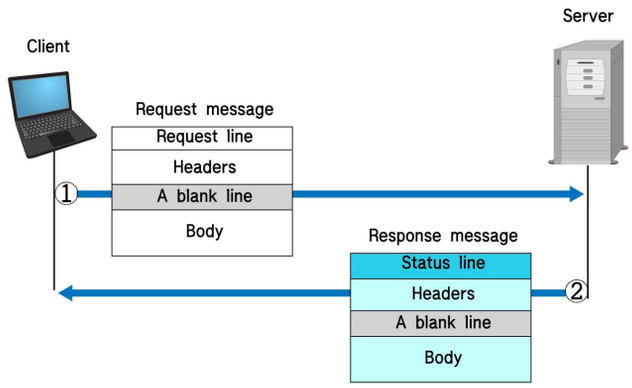
④ 데이터 유출

HTTP

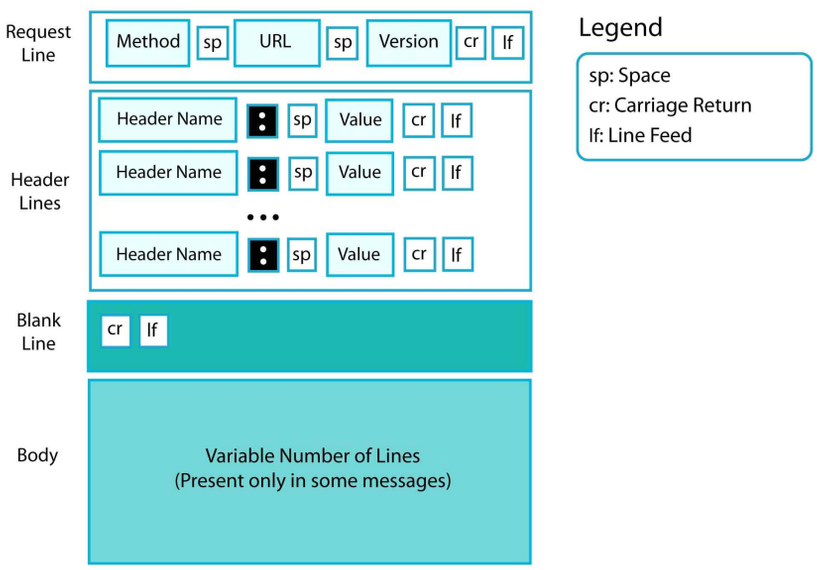
1) 비영속적 연결과 영속적 연결



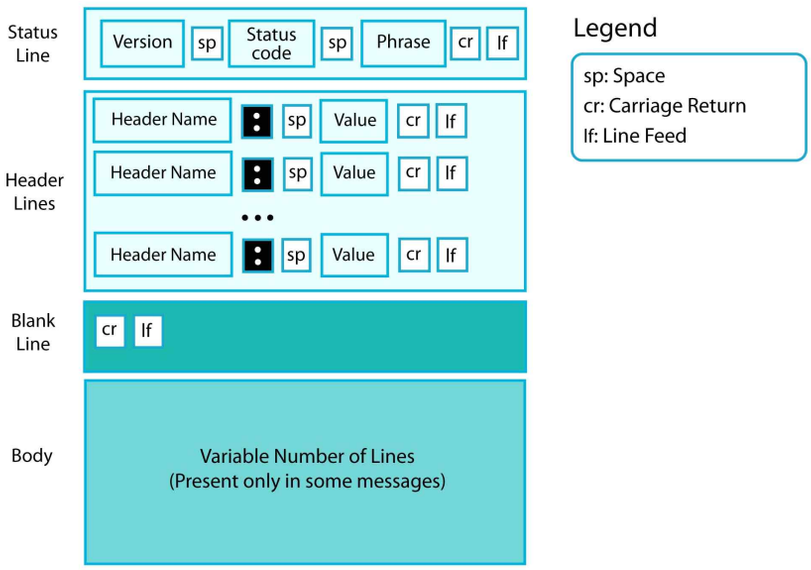
2) HTTP 트랜잭션



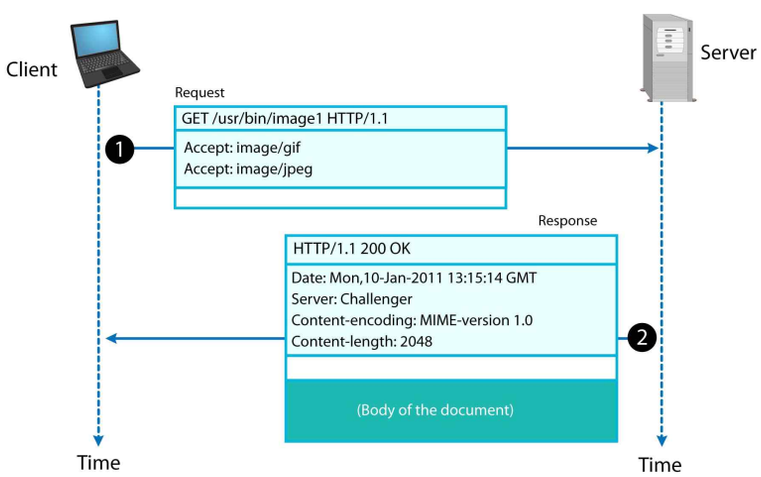
3) 요청 메시지 형식



4) 응답 메시지 형식



5) 요청 메시지와 응답메시지 예제



연습문제

HTTP 버전 1.1에 대한 설명으로 옳지 않은 것은?

① TCP를 전송 프로토콜로 사용한다.

② 요청 메시지의 첫 줄인 요청 라인에는 메소드, URL, HTTP 버전 필드가 포함된다.

③ 요청과 그에 대한 응답이 같은 연결로 보내지는 지속 연결(persistent connection)을 기본으로 하며, 분리된 별도의 연결을 이용하는 비지속 연결(non-persistent connection)도 지원한다.

④ HTTP 서버가 클라이언트에 대한 정보를 유지하는 상태(stateful) 프로토콜이다.

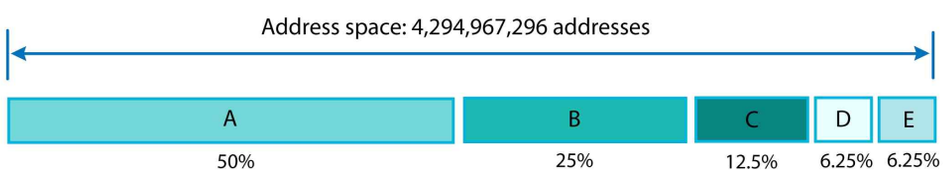
OSI 7 Layer의 구조

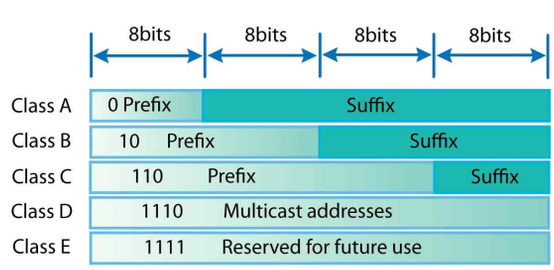
계층		특징	데이터 종류	예
7	응용 (Application)	◦ 각종 응용서비스 제공 ◦ 네트워크 관리	메시지 (Message)	FTP, TFTP, SNMP, SMTP, Telnet, HTTP, DNS, DHCP
6	표현 (Presentation)	◦ 네트워크 보안(암/복호화) ◦ 압축/압축해제, 포맷 변환 수행		ASCII, Mpeg, jpg, MIME
5	세션 (Session)	◦ 소켓 프로그램 ◦ 동기화 ◦ 세션 연결/관리/종료		전송모드 결정(반이중, 전이중 등), SQL, RPC
4	전송 (Transport)	◦ 데이터 전송보장 ◦ 흐름 제어 ◦ Quality Of Service(QOS)	세그먼트 (Segment)	TCP, UDP, SCTP
3	네트워크 (Network)	◦ 통신경로 설정, 중계기능 담당 ◦ 라우팅 ◦ IPv4 & IPv6	패킷 (Packet)	IP, ICMP, IGMP, ARP, RARP, NAT, RIP, BGP
2	데이터 링크 (Data Link)	◦ 오류제어, Frame화 ◦ 매체제어(MAC) ◦ 에러검출, 에러정정, 흐름제어	프레임 (Frame)	이더넷, 토큰링, PPP, SLIP, 802.11(WLAN)
1	물리 (Physical)	◦ 물리적 연결설정, 해제 ◦ 전송방식, 전송매체	비트 스트림 (Bit Stream)	기계적, 전기적, 절차적 규격

패킷의 전송방법

전송 방식	설명
유니캐스트(Unicast)	하나의 송신자가 하나의 수신자에게 패킷을 보내는 방식이다.(특정인에게 전송)
멀티캐스트(Multicast)	하나의 송신자가 다수의 수신자에게 패킷을 보내는 경우로 일대다의 패킷 전송방식이다. 멀티캐스트 전송을 수행하기 위해서는 네트워크 장치가 멀티캐스트를 지원해야 하며, 멀티캐스트 그룹에 가입되어 있어야 한다.(특정 다수인에게 전송)
브로드캐스트(Broadcast)	같은 네트워크에 있는 모든 호스트에게 패킷을 보내는 방식으로 브로드캐스트 주소에서는 호스트 주소를 모두 1로 설정한다.(불특정 다수인에게 전송)

클래스별 IP 주소 분류



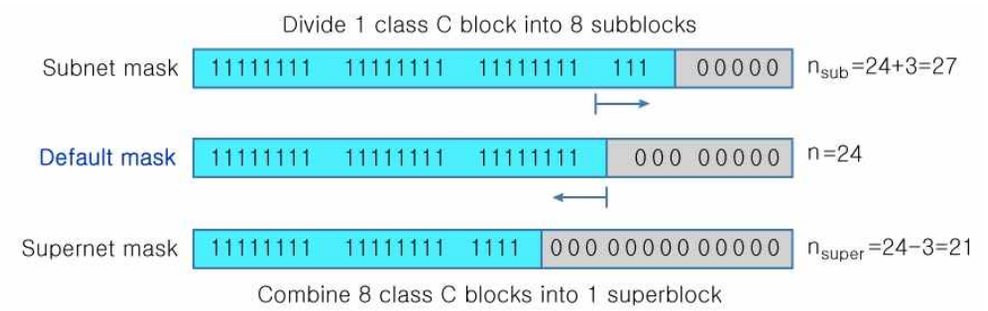


Class Prefixes		First byte
A	n = 8bits	0 to 127
B	n = 16bits	128 to 191
C	n = 24bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

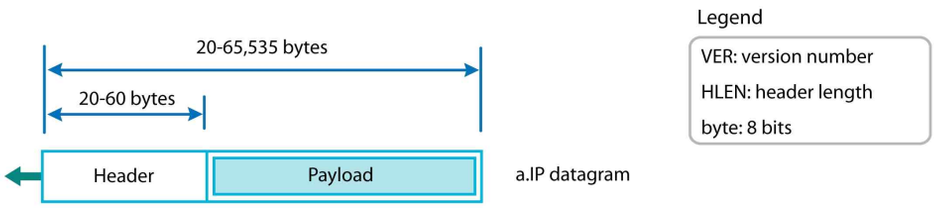
클래스별 IP 주소 내용

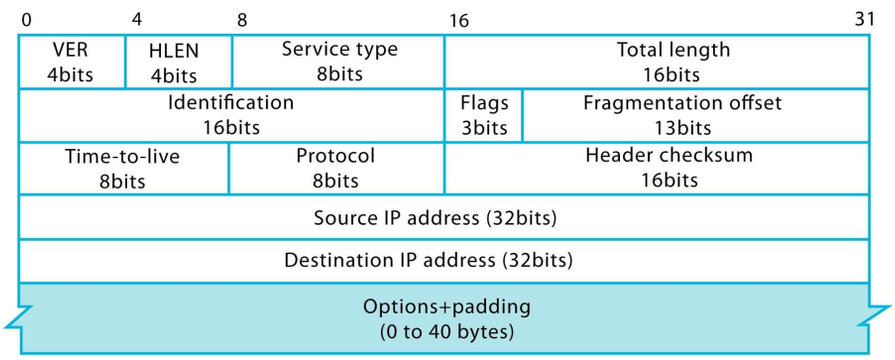
클래스	설명
클래스 A	첫 번째 비트가 「0」인 IP 주소를 클래스 A주소라고 한다. 첫 바이트의 나머지 7비트가 네트워크 주소이고, 하위 세 바이트는 호스트 주소이다. 클래스 A주소는 약 2^{24}–2 = 16,777,214개의 호스트를 수용할 수 있기 때문에 큰 규모의 호스트를 갖는 기관에서 사용한다.
클래스 B	처음 두 비트의 값이 「10」인 주소를 클래스 B주소라고 한다. 첫 바이트의 나머지 6비트와 두 번째 바이트가 네트워크 주소이고, 마지막 두 바이트는 호스트 주소로 사용된다. 클래스 B주소는 약 2^{16}–2개의 호스트를 수용할 수 있다.
클래스 C	처음 세 비트의 값이 「110」인 주소를 클래스 C주소라고 한다. 세 번째 바이트까지가 네트워크 주소이고 마지막 한 바이트는 호스트 주소이다. 클래스 C주소는 네트워크마다 254개까지 호스트를 수용할 수 있기 때문에 작은 규모의 네트워크에서 사용된다.
클래스 D	처음 네 비트의 값이 「1110」인 주소를 클래스 D주소라고 한다. 클래스 D주소는 네트워크 주소와 호스트 주소의 구분이 없고 전체 주소가 멀티캐스트용으로 사용된다. 정보, 멀티미디어 데이터 그리고 리얼타임 비디오 등을 보내는 데 사용된다.
클래스 E	처음 네 비트의 값이 「1111」인 주소를 클래스 E주소라고 하며 추후 사용을 위해 예약된 주소이다.

서브네팅과 슈퍼네팅



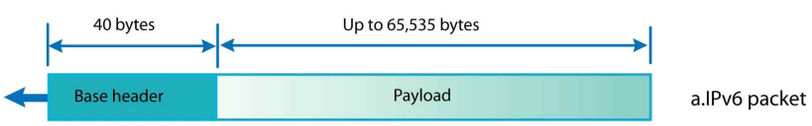
IPv4 데이터그램

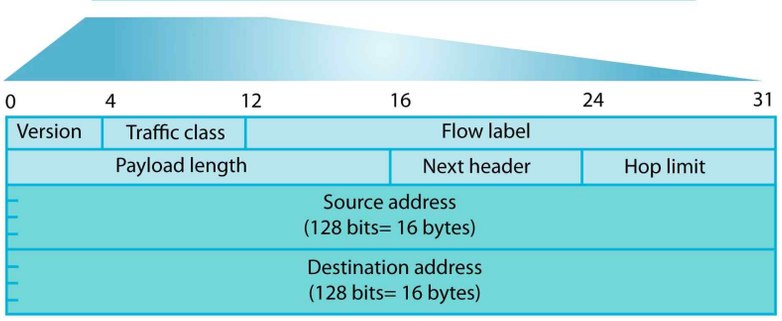




b.Header format

IPv6 데이터그램

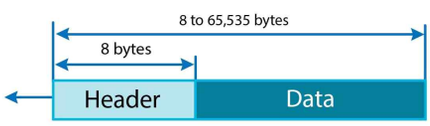




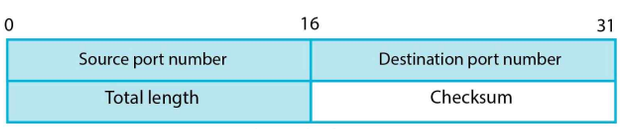
IPv4와 IPv6 특징 비교

구분	IPv4	IPv6
주소 길이	32비트	128비트
표시 방법	8비트씩 4부분 10진수 표시 예) 203.252.53.55	16비트 8부분 16진수로 표시 예) 2002:0221:ABCD:DCBA:0000:0000:FFFF:4002
주소 개수	약 43억개	2^{128}개(약 43억×43억×43억×43억)
주소할당 방식	A,B,C,D 등의 클래스 단위 비순차 할당	네트워크 규모, 단말기수에 따라 순차할당
브로드캐스트 주소	있음	없음(대신, 로컬범위 내에서의 모든 노드에 대한 멀티캐스트 주소 사용)
헤더 크기	가변	고정
QoS 제공	미흡	제공
보안	IPSec 프로토콜 별도 설치	IPSec 자체 지원
서비스 품질	제한적 품질 보장(Type of Service에 의한 서비스 품질 일부 지원)	확장된 품질 보장(트래픽 클래스, 플로우 레이블에 의한 서비스 품질 지원)

사용자 데이터그램(UDP) 형식



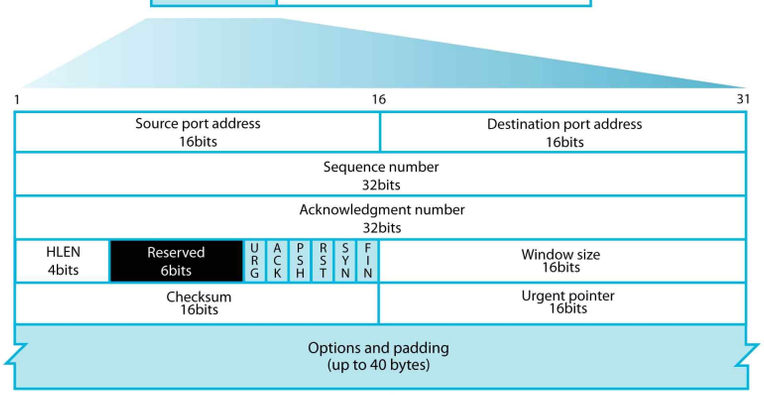
a. UDP user datagram



b.Header format

TCP 세그먼트 형식

a. Segment



b. Header

TCP와 UDP의 주요 차이점

서비스	TCP	UDP
신뢰성	패킷이 그들의 목적지에 도달했는지 확인하며, 패킷이 도달될 때마다 ACK를 수신하기 때문에 신뢰성 있는 프로토콜이다.	ACK를 보내지 않으며 패킷이 그들의 목적지에 도달되는 것을 보장하지 않기 때문에 신뢰성이 없는 프로토콜이다.
연결	연결지향적이므로, 핸드쉐이킹 과정을 수행하고 목적지 컴퓨터와 함께 가상연결을 형성한다.	비연결지향적이므로 핸드쉐이킹 과정을 수행하지 않으며, 가상연결도 형성하지 않는다.
패킷 순서	패킷 내에 순서번호를 사용하여 각 패킷들이 순차적으로 수신되도록 한다.	순서번호를 사용하지 않는다.
혼잡 제어	목적지 컴퓨터는 송신지 컴퓨터의 너무 많은 데이터 전송으로 인해 처리가 어렵거나 전송속도가 느려질 경우 이를 통보한다.	목적지 컴퓨터는 흐름제어에 대한 통보를 송신지 컴퓨터에 하지 않는다.
사용	신뢰성 있는 전송이 필요할 때 사용된다.	스트리밍 비디오와 브로드캐스트 등 신뢰성 있는 전송이 불필요할 때 사용된다.
속도와 오버헤드	상당한 양의 자원을 사용하며 UDP보다 느리다.	더 적은 자원을 사용하고 TCP보다 빠르다.

연습문제

OSI 7계층은 다양한 네트워크 간의 호환을 위해 만든 표준 네트워크 모델이다. 다음 중 OSI 7계층에서 네트워크 계층에 대한 설명으로 가장 옳은 것은?

① 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공한다.
② 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해준다.
③ 두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층으로 16진수 12개로 구성된 MAC 주소를 사용한다.
④ 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층으로 라우터를 통한 패킷 포워딩을 담당한다.

연습문제

인터넷 프로토콜(IP)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 클래스 기반 주소 지정에서 처음 세 비트의 값이 '110' 으로 시작하는 주소를 클래스 C주소라고 한다.
② IPv4의 데이터그램(Datagram)에서 첫 번째 필드는 선택사항(Option)을 포함한 헤더(header)의 길이 값이다.
③ IPv6에서는 헤더(header)가 40바이트로 고정되어 있어 헤더의 길이 필드가 불필요하다.
④ IPv6에서는 IPv4에서 사용하던 체크섬(Checksum) 필드가 삭제되었다.

연습문제

IPv6(Internet Protocol version 6)에 관한 설명으로 가장 적절하지 않은 것은?

① 16bit씩 8부분, 총 128bit로 구성된다.
② 각 부분은 세미콜론(;)으로 구분되며 16진수로 표현한다.
③ IPv4에 있던 헤더 체크섬(checksum) 필드가 라우터의 처리 시간 감소를 위해서 제거되었다.
④ 기본 헤더 길이가 40byte로 고정되고, 확장 헤더는 추가적인 전송 기능이 필요할 때 사용된다.

✔ 연습문제

공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기

② 패킷을 송신하고 수신하는 프로세스의 포트 번호

③ 수신자측에서 앞으로 받고자 하는 바이트의 순서 번호

④ 송신 시스템의 TCP 패킷의 생성 시간

✔ 연습문제

TCP 헤더의 제어용 플래그(control flags, 1: on, 0: off) 6 bits에 할당된 값 010001이 의미하는 것은?

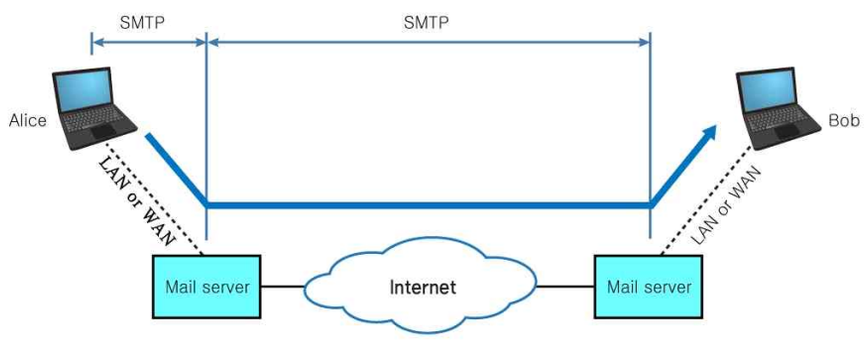
① SYN(synchronization)과 RST(reset) 값이 1이다.

② ACK(acknowledgment)와 FIN(finish) 값이 1이다.

③ URG(urgent)와 PSH(push) 값이 1이다.

④ SYN(synchronization)과 PSH(push) 값이 1이다.

SMTP의 적용 범위



✔ 연습문제

SMTP에 대한 설명으로 옳지 않은 것은?

① SMTP는 실행 파일이나 2진 데이터를 텍스트 형태로 변환하여 전송한다.

② 송·수신 측이 직접 상대방을 상호 인증하는 방식을 통해 메시지를 전송한다.

③ SMTP 서버는 특정 크기 이상의 메일 메시지를 처리하지 못하고 거부한다.

④ 주로 TCP 포트 25번을 사용한다.

PEM, PGP, S/MIME 비교

항목	PEM	PGP	S/MIME
개발자	IETF	Phil Zimmermann	RSA Data Security Inc
특징	◦ 중앙집중화된 키 인증 ◦ 인터넷 표준(안) ◦ 구현의 어려움 ◦ 높은 보안성(군사용, 금융계 등) ◦ 이론 중심 ◦ 많이 사용되지 않음	◦ 분산화된 키 인증 ◦ 응용 프로그램 ◦ 구현의 용이성 ◦ 일반 용도의 보안성 ◦ 실세계 사용 중심 ◦ 현재 많이 사용	◦ MIME 기반 ◦ 다양한 상용 툴킷 ◦ X.509 인증서 지원

연습문제

전자우편 서비스의 보안 기술로 옳지 않은 것은?

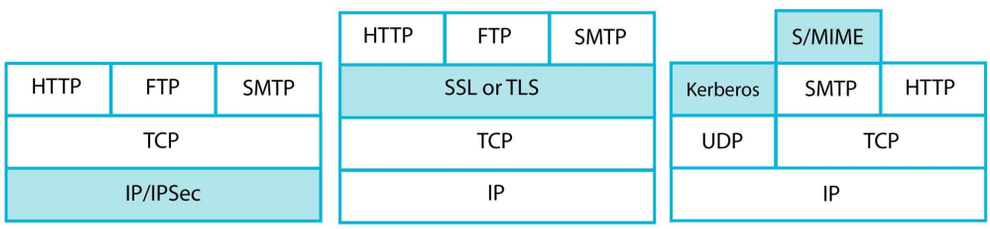
① PGP(Pretty Good Privacy)

② S/MIME(Secure/Multipurpose Internet Mail Extension)

③ SET(Secure Electronic Transaction)

④ PEM(Privacy Enhanced Mail)

Layer별 웹 보안 적용 현황



(a) 네트워크 레벨 (b) 전송 레벨 (c) 응용 레벨

연습문제

다음의 OSI 7계층과 이에 대응하는 계층에서 동작하는 보안 프로토콜을 바르게 연결한 것은?

보기

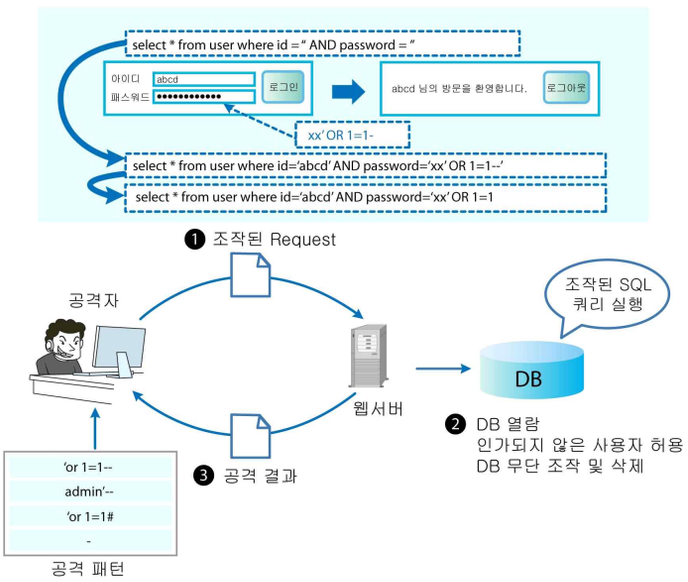
ㄱ. 2계층 ㄴ. 3계층 ㄷ. 4계층

보기

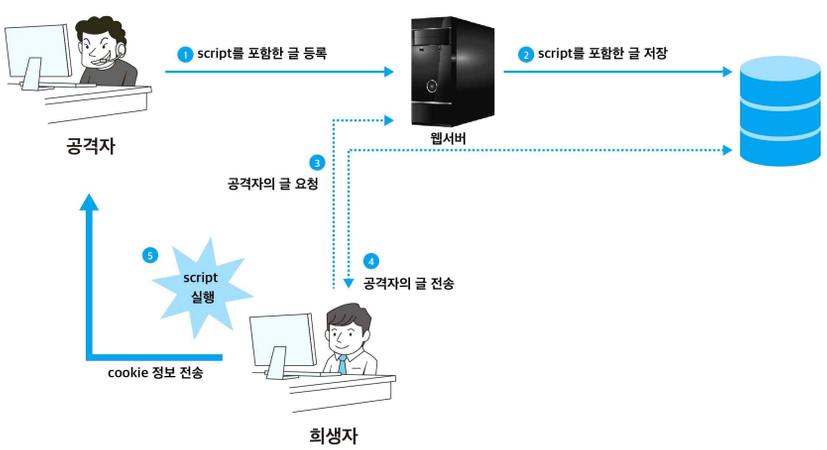
A. SSL/TLS B. L2TP C. IPSec

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	C	A
④	B	A	C

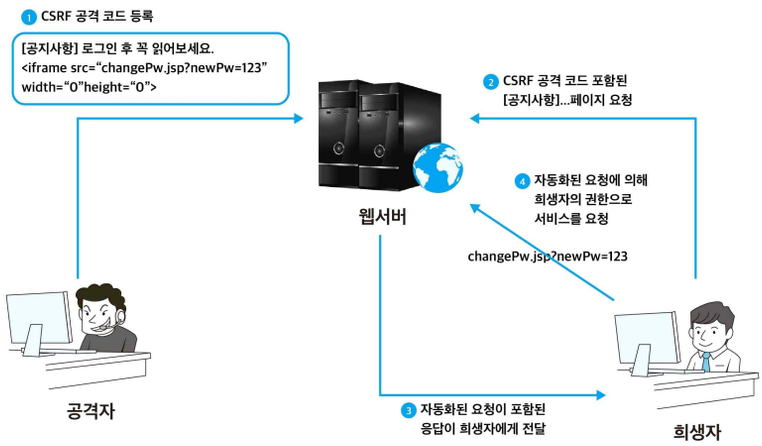
SQL Injection 공격



저장형 XSS 공격 과정



CSRF 공격 과정



연습문제

XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 게시판 등의 웹페이지에 악의적인 코드 삽입이 가능하다는 취약점이 있다.

② 공격 코드를 삽입하는 부분에 따라 저장 XSS 방식과 반사 XSS 방식이 있다.

③ 악성코드가 실행되면서 서버의 정보를 유출하게 된다.

④ Javascript, VBScript, HTML 등이 사용될 수 있다.

위험에 대한 대책

구분	설명
위험 수용(Risk Acceptance)	현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것
위험 감소(Risk reduction, mitigation)	위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것
위험 회피(Risk avoidance)	위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것
위험 전가(Risk Transition, Transfer)	보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당하는 것

정량적, 정성적 분석의 장단점

구분	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 사용할 시 신뢰도가 벤더에 의존된다.	◦ 위험평가 과정과 측정기준이 지극히 주관적이어서 사람에 따라 달라질 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.

✔ 연습문제

정보보호 대책 수립을 위한 대응 전략으로 가장 적절하지 않은 것은?

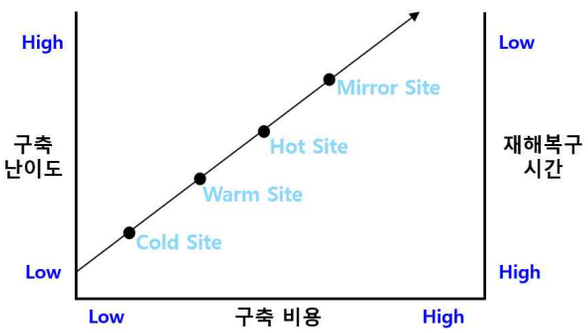
① 위험전가는 위험이 발생하는 원인을 제3자를 통해 제거한다.

② 위험감소는 위험을 줄일 수 있는 대책을 채택하여 구현한다.

③ 위험회피는 위험이 존재하는 프로세스나 사업을 수행하지 않는다.

④ 위험수용은 식별된 위험을 받아들이고 비용을 감수한다.

2차 사이트 종류



재해복구 시스템 복구 수준별 유형 비교

유형	설명	RTO	장점	단점
미러 사이트	◦ 주 센터와 동일한 수준의 정보기술 자원을 원격지에 구축하고, '운영-운영(Active-Active)'상태로 실시간 동시 서비스를 제공	즉시	◦ 데이터 최신성 ◦ 높은 안정성 ◦ 신속한 업무재개	◦ 높은 초기투자비용 ◦ 높은 유지보수비용 ◦ 데이터 업데이트가 많은 경우 과부하 초래하여 부적합
핫 사이트	◦ 주 센터와 동일한 수준의 정보기술 자원을 원격지에 구축하여 대기(Stand-by)상태로 유지하며 '운영-대기'(Active-Standby)상태로 서비스 제공. ◦ 주센터 재해 시 원격지시스템을 운영(Active) 상태로 전환하며 서비스 제공 데이터는 동기적 또는 비동기적 방식의 실시간 미러링을 통하여 최신상태 유지	수시간 이내	◦ 데이터 최신성 ◦ 높은 안정성 ◦ 신속한 업무재개 ◦ 데이터의 업데이트가 많은 경우에 적합	◦ 높은 초기투자비용 ◦ 높은 유지보수비용(최신 데이터와 패치 유지) ◦ 보안적인 문제
웜 사이트	◦ 중요성이 높은 정보기술 자원만 부분적으로 재해복구센터에 보유 ◦ 데이터는 주기적(수시간~1일)으로 백업	수일 ~ 수주	◦ 구축 및 유지비용이 핫 사이트에 비해 저렴	◦ 데이터에 다소의 손실 발생 ◦ 초기 복구수준이 부분적임 ◦ 복구소요시간이 비교적 길다.
콜드 사이트	◦ 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보 ◦ 재해 시 데이터를 근간으로 필요한 정보자원을 조달하여 정보시스템의 복구 개시 ◦ 주 센터의 데이터는 주기적(수일~수주)으로 원격지에 백업	수주 ~ 수개월	◦ 구축 및 유지비용이 가장 저렴	◦ 데이터의 손실 발생 ◦ 복구에 매우 긴 시간이 소요됨 ◦ 복구 신뢰성이 낮음 ◦ 테스트가 곤란

연습문제

다음에서 설명하는 재해복구시스템의 복구 방식은?

> 보기
>
> 재해복구센터에 주 센터와 동일한 수준의 시스템을 대기상태로 두어, 동기적 또는 비동기적 방식으로 실시간 복제를 통하여 최신의 데이터 상태를 유지하고 있다가, 재해 시 재해복구센터의 시스템을 활성화 상태로 전환하여 복구하는 방식이다.

① 핫 사이트(Hot Site)
② 미러 사이트(Mirror Site)
③ 웜 사이트(Warm Site)
④ 콜드 사이트(Cold Site)

TESEC, ITSEC, CC의 비교

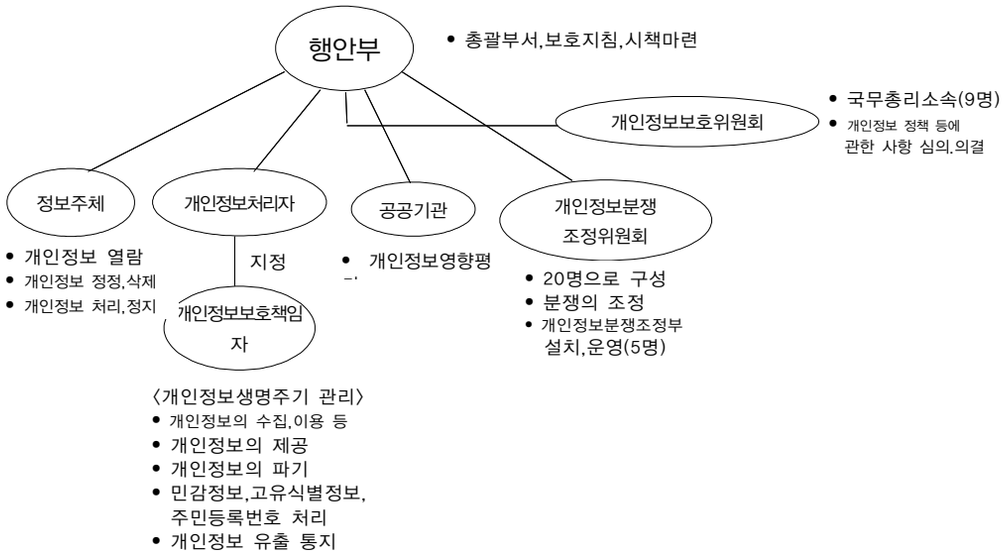
구분	TCSEC	ITSEC	CC
명칭	Trusted Computer System Evaluation Criteria	Information Technology Security Evaluation	Common Criteria
표준화	미국표준제정기관(NCSC)	영국, 독일, 프랑스, 네덜란드	국제표준기관(ISO/IEC15408)
적용범위	미국 내 보안표준	유럽	세계공통의 보안표준
등급	A1,B1,B2,B3,C1,C2 (6등급), D(부적합)	E6-E1(6등급) E0(부적합)	EAL7-EAL1(7등급) EAL0(부적합)

연습문제

유럽의 국가들에 의해 제안된 것으로 자국의 정보보호 시스템을 평가하기 위하여 제정된 기준은?

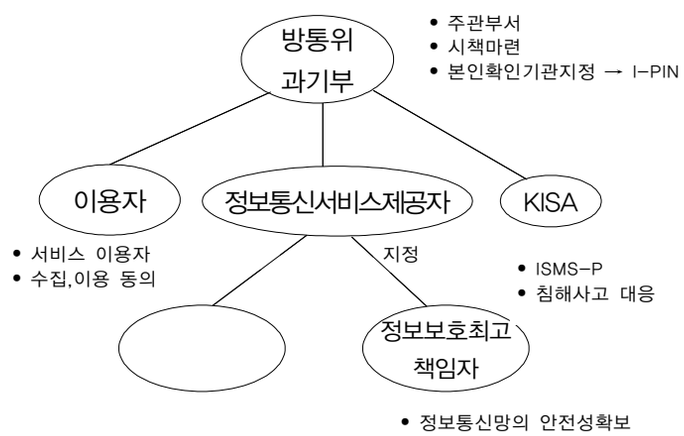
① TCSEC
② ITSEC
③ PIMS
④ ISMS-P

개인정보보호법

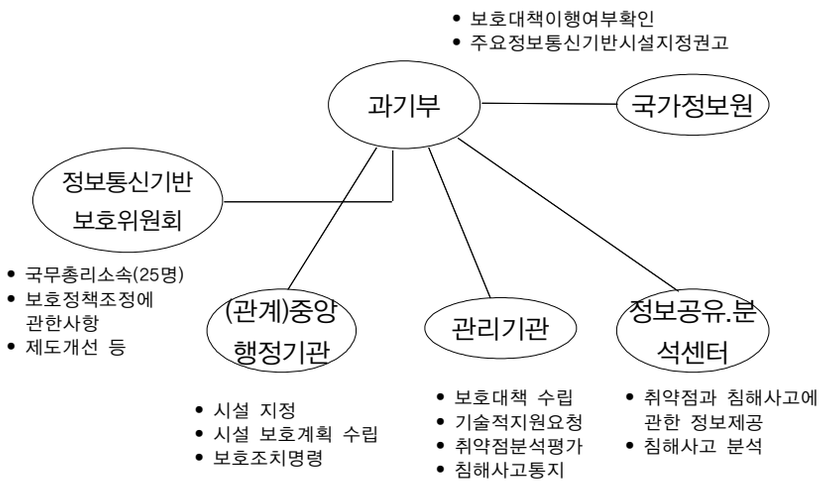


〈개인정보생명주기 관리〉
- 개인정보의 수집,이용 등
- 개인정보의 제공
- 개인정보의 파기
- 민감정보,고유식별정보, 주민등록번호 처리
- 개인정보 유출 통지

정보통신망법



정보통신기반보호법



연습문제

정보통신기반 보호에 대한 설명으로 옳지 않은 것은?

① 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 업무의 국가사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 국가안전보장과 경제사회에 미치는 피해규모 및 범위 등을 고려하여 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

② 주요정보통신기반시설 보호계획에는 주요정보통신기반시설의 취약점 분석·평가, 침해사고에 대한 예방·백업·복구대책, 보호에 관하여 필요한 사항을 포함해야 한다.

③ 정보통신기반보호위원회는 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당 분야 관리기관의 장에게 이를 지키도록 권고할 수 있다.

④ "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다.