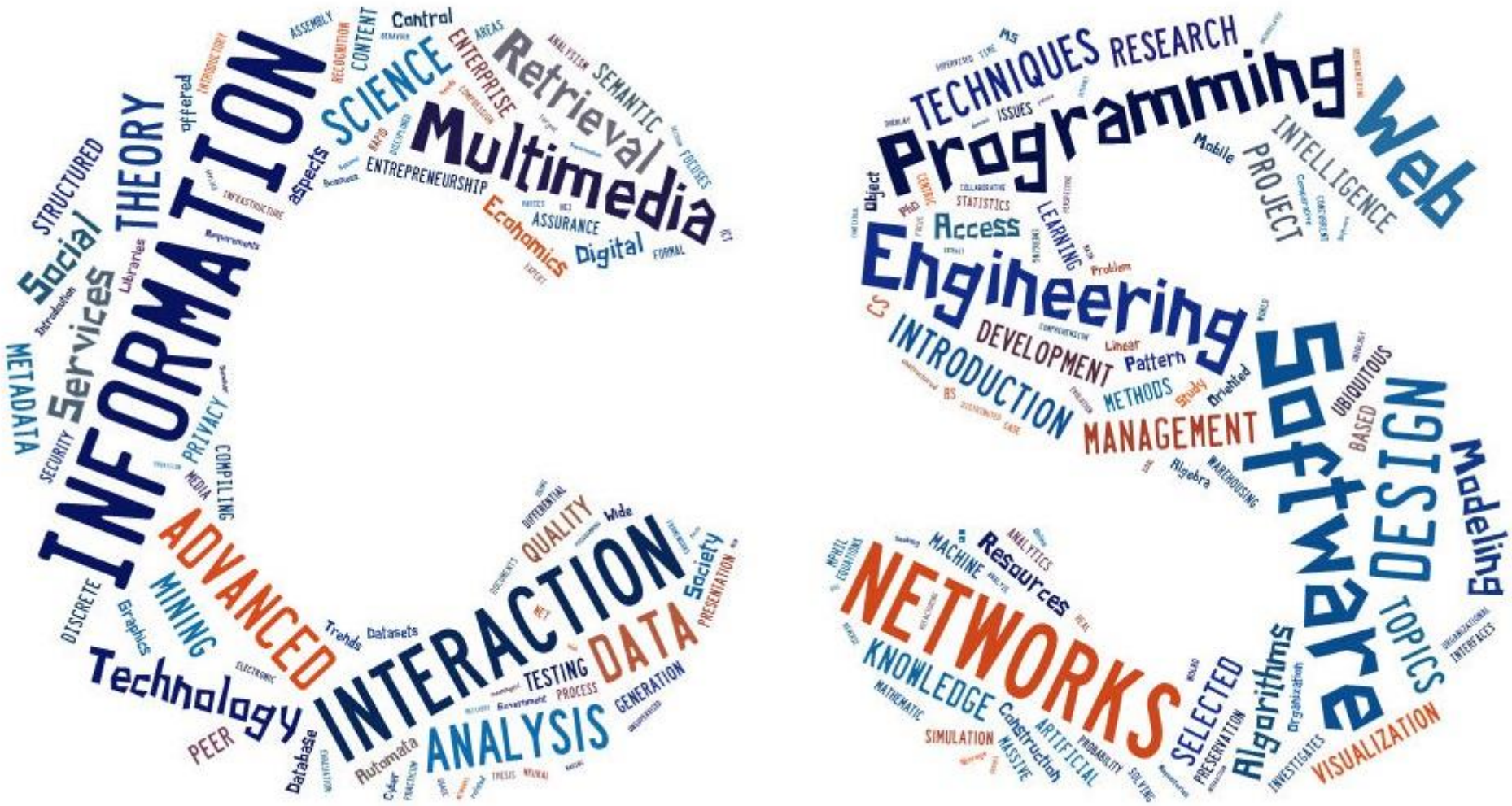

INFORMATION
SCIENCE
Retrieval
Multimedia
Programming
Web
Engineering
Software
DESIGN
Modeling
TOPICS
ADVANCED
INTERACTION
DATA
ANALYSIS
Technology
MINING
NETWORKS
Resources
KNOWLEDGE
Algorithms
SELECTED
VISUALIZATION
MANAGEMENT
INTRODUCTION
DEVELOPMENT
METHODS
TECHNIQUES
RESEARCH
PROJECT
INTELLIGENCE
Access
Digital
Economics
ENTREPRENEURSHIP
ENTERPRISE
SEMANTIC
Control
CONTENT
aSpects
THEORY
Social
Services
STRUCTURED
METADATA
PRIVACY
COMPILING
SECURITY
DISCRETE
Graphics
PEER
Database
Automata
Datasets
Trends
TESTING
PROCESS
GENERATION
QUALITY
Society
PRESENTATION
Wide
DIFFERENTIAL
MACHINE
ARTIFICIAL
SIMULATION
MASSIVE
Construction
PRESERVATION
Algebra
UBIQUITOUS
BASED
Pattern
Linear
Problem
Mobile
Object
LEARNING
STATISTICS
ISSUES
Oriented
Study
WAREHOUSING
INVESTIGATES
ORGANIZATIONAL
INTERFACES

09 정보 보안

목차

1. 정보 보안의 개요
2. 악성코드
3. 해킹
4. 정보 보안 기술
5. 컴퓨터 범죄와 정보 윤리

2011년 농협 전산망 해킹 사고

정보 보안의 개념과 목표

- 정보 보안의 개념
  - 정보를 수집하여 가공하고 저장한 후 송수신하는 과정에서 발생하는 정보의 불법 훼손 및 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법
- 정보 보안의 목표
  - 기밀성 : 허가되지 않은 사용자 또는 객체가 해당 정보의 내용을 알 수 없도록 비밀을 보장하는 것
  - 무결성 : 허가되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없게 하는 것
  - 가용성 : 허가된 사용자 또는 객체가 정보에 접근하면 언제든지 사용할 수 있게 하는것

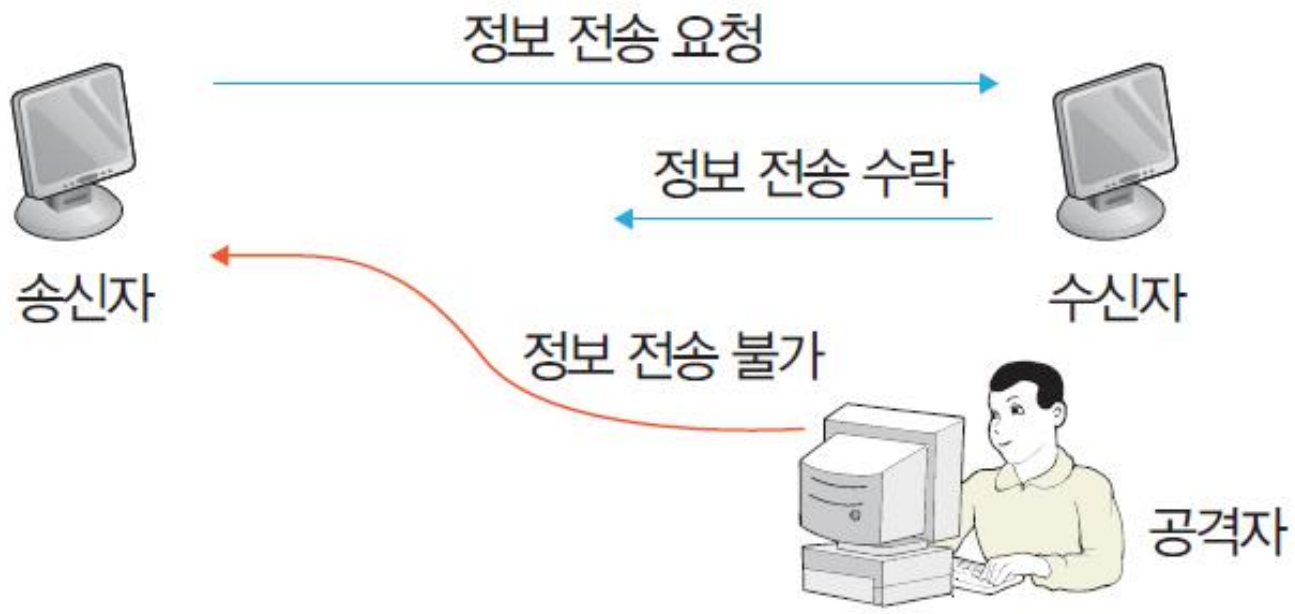
정보 보안을 위협하는 공격 형태

- 정상적인 정보의 통신 과정

- 정보 보안을 위협하는 공격 형태
  - 정보 가로막기
  - 정보 가로채기
  - 정보 수정
  - 정보 위조

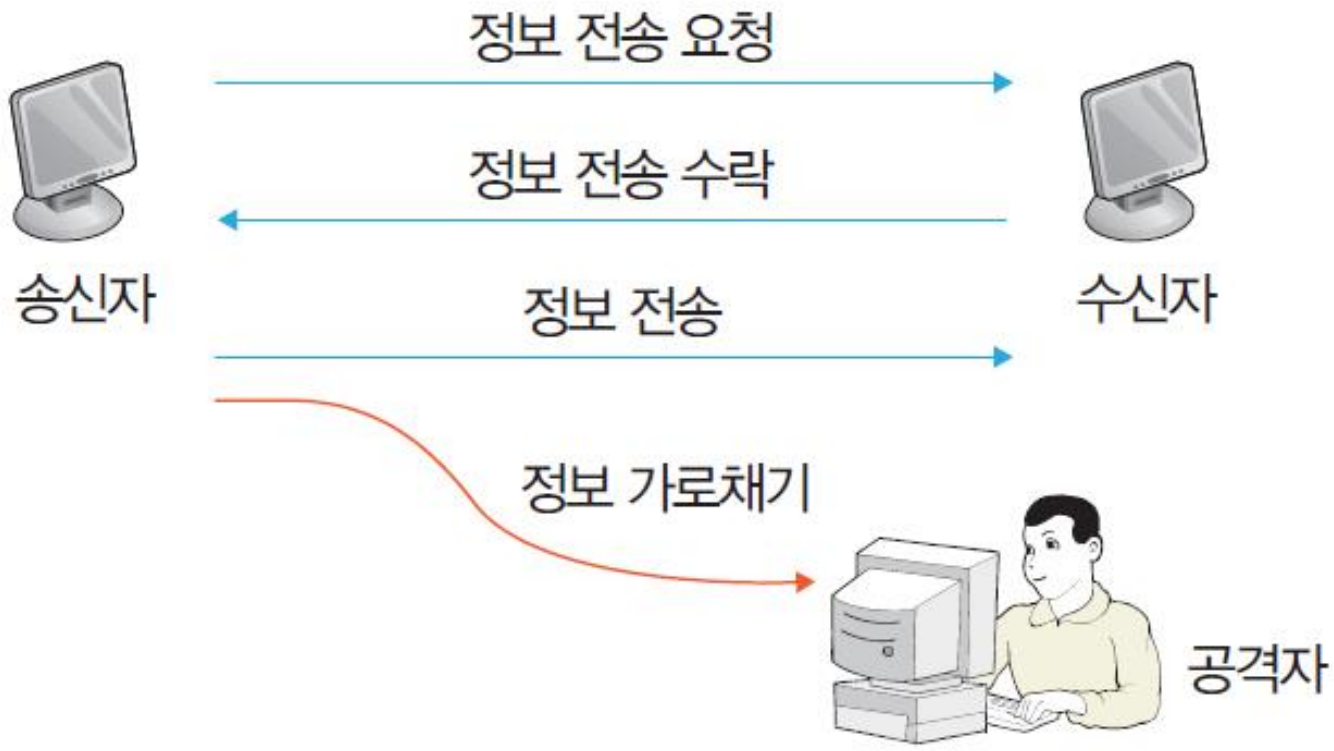
정보 보안을 위협하는 공격 형태

- 정보 가로막기



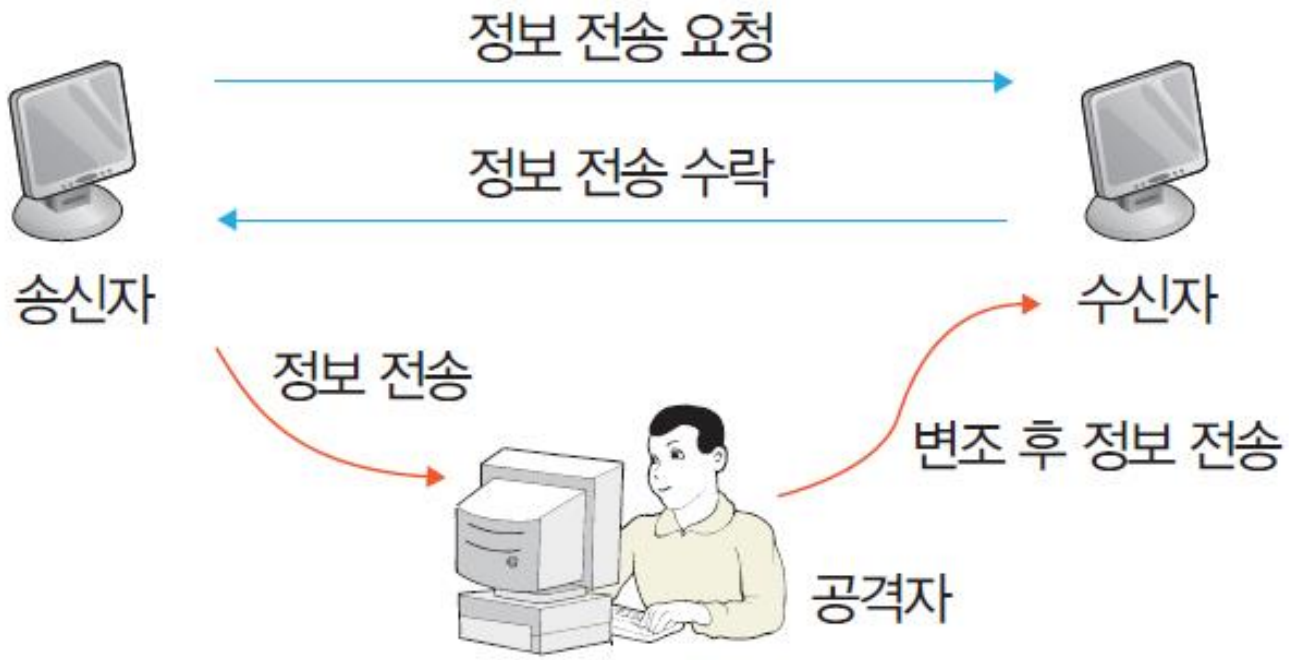
정보 보안을 위협하는 공격 형태

- 정보 가로채기



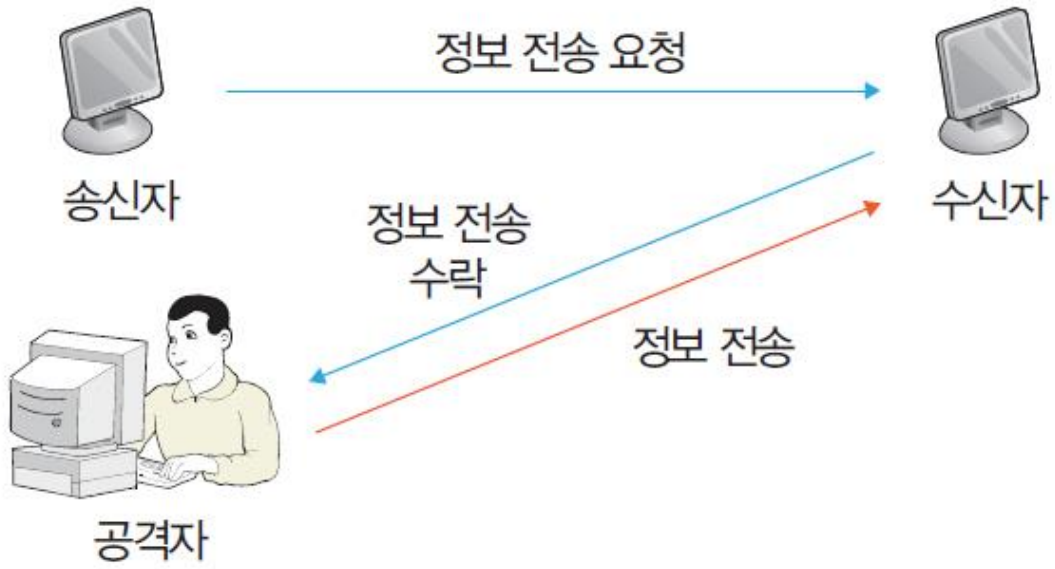
정보 보안을 위협하는 공격 형태

- 정보 수정

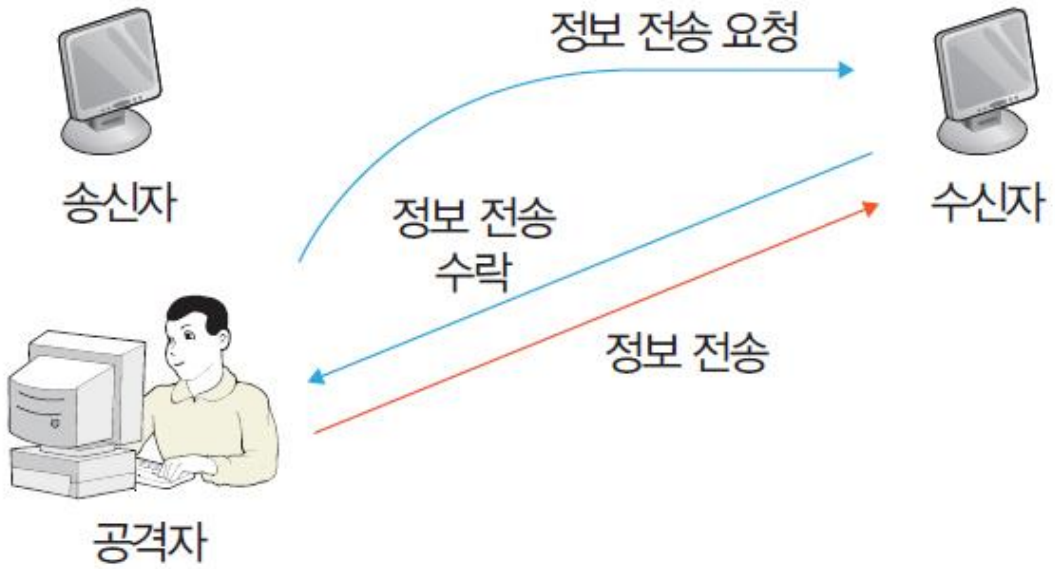


정보 보안을 위협하는 공격 형태

- 정보 위조



(a) 송신자가 정보 전송 요청을 하는 경우



(b) 공격자가 정보 전송 요청을 하는 경우

정보 보안을 위한 서비스

- 인증
  - 정보시스템에서 송신자 및 수신자의 신분을 확인하는 서비스
- 접근 제어
  - 허가되지 않은 사용자가 정보에 접근할 수 없도록 막는 서비스
- 부인 방지
  - 송신자 또는 수신자가 정보를 송신 또는 수신한 후 그 사실에 대해 부인하지 못하도록 하는 서비스

악성코드의 개념과 종류

- 개념
  - 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어
  - 웹 페이지를 검색하거나 P2P 서비스를 이용하거나 셰어웨어를 사용하거나 불법 복제 프로그램을 사용하거나 전자메일에 첨부된 파일을 열 때 침투
  - 주요 증상으로는 네트워크 트래픽 발생, 시스템 성능 저하, 파일 삭제, 전자메일 자동 발송, 개인 정보 유출 등이 있음
- 종류
  - 컴퓨터 바이러스
  - 웜
  - 트로이 목마

컴퓨터 바이러스

- 개념
  - 사용자 컴퓨터 내부에 있는 프로그램이나 실행 가능한 데이터에 자신 또는 변형된 자신을 복사하는 명령어들의 조합
- 감염 경로
  - 불법 복제한 CD를 사용하거나 여러 사람이 공동으로 사용하는 컴퓨터에서 작업한 USB를 통해 감염
  - 인터넷으로 자료를 주고받을 때 감염되기도 함
- 주요 증상
  - 컴퓨터가 구동되지 않거나 구동되더라도 평소보다 시간이 오래 걸림
  - 자동으로 하드디스크가 포맷됨
  - 특정 프로그램이 실행되지 않거나 실행되더라도 평소보다 오래 걸림
  - 메모리나 하드디스크 용량이 줄어듬
  - 파일이 열리지 않거나 파일 이름이나 크기가 변경됨
  - 컴퓨터 화면에 이상한 글자가 나타나거나 프로그램의 크기가 달라짐

컴퓨터 바이러스

분류	특징	종류
제1세대 원시형 바이러스 (primitive virus)	· 도스나 윈도우 초기 버전에서 출현한 대부분의 바이러스를 칭한다. · 구조가 단순해 분석하기 쉽다.	미켈란젤로 바이러스, 브레인 바이러스, 돌 바이러스(stoned virus), LBC 바이러스, 예루살렘 바이러스(Jerusalem virus), CIH 바이러스
제2세대 암호화 바이러스 (encryption virus)	· 백신이 등장하면서부터 출현했다. · 백신이 바이러스를 진단할 수 없도록 바이러스가 암호화되어 저장되어 있다.	폭포 바이러스(cascade virus), 느림보 바이러스(slow virus)
제3세대 은폐형 바이러스 (stealth virus)	· 컴퓨터를 감염시킨 후에도 메모리 손실이나 파일 크기의 변화가 없는 것처럼 은폐한다. · 기억 장소에 기생하면서 감염된 파일의 길이가 늘어나지 않은 것처럼 보이게 한다. · 백신 프로그램이 치료하려고 해도 감염되기 전의 내용을 보여줌으로써 바이러스가 없는 것처럼 속인다.	브레인 바이러스(brain virus), 조시 바이러스(Joshi virus), 방랑자.1347 바이러스(Wanderer.1347 virus), 프로도 바이러스(Frodo virus)
제4세대 갑옷형 바이러스 (armor virus)	· 암호를 푸는 부분을 감염시켜 실행할 때마다 자기 변형을 시도하기 때문에 사용자나 백신 프로그램이 감염 사실을 알지 못하게 한다.	고래 바이러스(whale virus), 다형성 바이러스(polymorphic virus)
제5세대 매크로 바이러스 (macro virus)	· 아래아한글이나 MS 오피스 같은 응용 프로그램의 매크로 내부에서 기생하여 동작한다.	엑셀 매크로 바이러스(ExcelMacro virus)
제6세대 차세대 바이러스 (next generation virus)	· 개인 정보의 유출 및 도용이나 시스템의 파괴 및 장악 등 사이버 범죄에 사용되어 심각한 피해를 줄 수 있는 바이러스를 모두 말한다.	–

웜

- 개념
  - 독립적으로 자기 복제를 실행해 번식하는 컴퓨터 프로그램 또는 실행 가능한 코드
- 감염 경로
  - 네트워크를 통해 스스로 감염됨
  - 보통 전자메일에 첨부되어 상대방 컴퓨터에 전송됨
- 증상
  - 컴퓨터 시스템에 무리를 줌
  - 특정 파일을 0바이트로 만듦
  - 하드디스크 포맷
  - 인터넷 속도가 느려짐
  - 사용자의 정보를 빼냄

트로이목마

- 개념
  - 정상적인 프로그램으로 가장하여 숨어 있다가 프로그램이 실행될 때 활성화되어 자료 삭제, 정보 탈취 등 의도하지 않은 기능을 수행하는 프로그램 또는 실행 가능한 코드

영화 'Troy' 에 등장하는 트로이 목마

트로이목마

- 감염 경로
  - 전자메일이나 소프트웨어에 숨어 있다가 인터넷을 통해 특정 컴퓨터가 감염되면, 해커가 감염된 컴퓨터의 정보를 탈취
- 증상
  - 해커가 악의적인 목적으로 컴퓨터의 자료를 빼내갈 수 있음
  - 예를 들어 사용자가 누른 자판 정보를 외부에 알려주기 때문에 신용카드 번호나 비밀번호 등이 유출될 수 있음

기타 유해 프로그램

- 개념
  - 컴퓨터 바이러스처럼 악의적인 목적으로 사용자에게 피해를 주는 것은 아니지만, 컴퓨터 이용에 불편을 주거나 다른 악성코드에 의해 악용될 수 있는 프로그램
- 스파이웨어(spyware)
  - 사용자의 동의 없이 설치되어 광고나 마케팅용 정보를 수집하거나 개인 정보를 몰래 훔쳐가는 프로그램
- 키로거(key logger)
  - 키보드로부터 정보를 수집하여 저장하고, 필요한 경우 특정 전자메일로 저장된 정보를 전송하는 프로그램
- 조크(joke)
  - 악의적인 목적 없이 사용자의 심적 동요나 불안을 조장하는 가짜 컴퓨터 바이러스

해킹

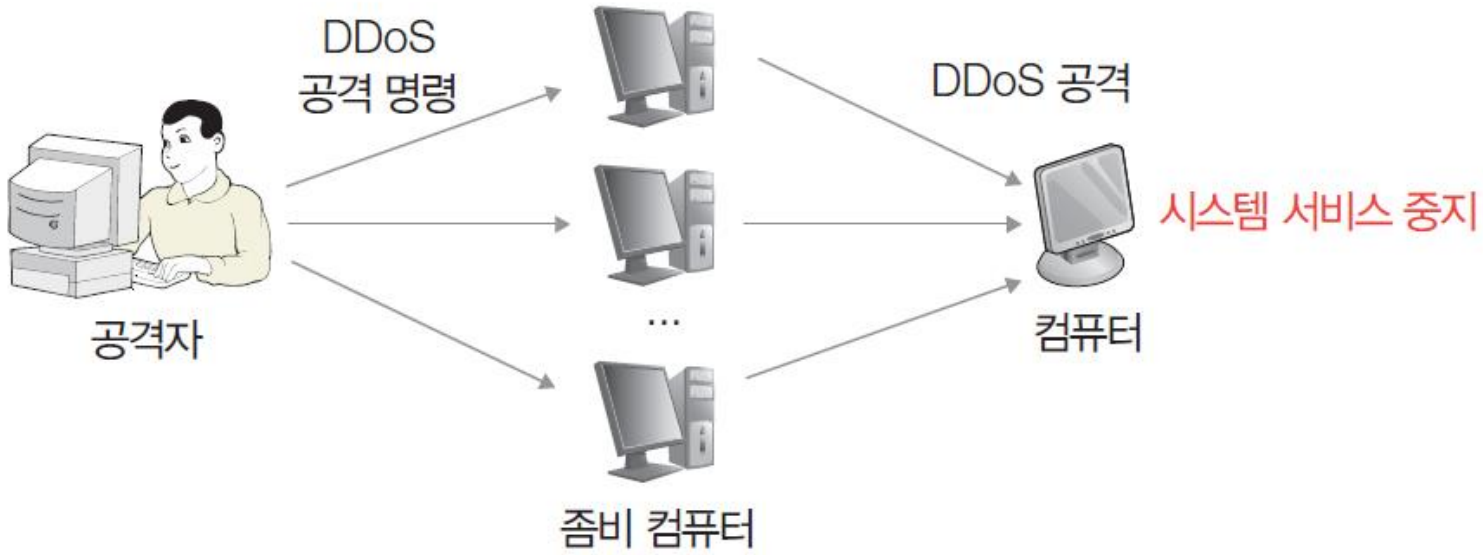
- 개념
  - 다른 사람의 컴퓨터 또는 정보시스템에 침입하여 정보를 빼내는 행위
- 종류
  - 도스
  - 디도스
  - 스푸핑
  - 스니핑
  - XSS
  - 피싱

도스

- 도스
  - Denial of Service의 약자로 '서비스 거부 공격'이라고도 함
  - 공격자가 좀비 컴퓨터를 이용하여 공격 대상 컴퓨터나 네트워크에 과도한 데이터를 보내 시스템의 성능을 급격히 저하시킴

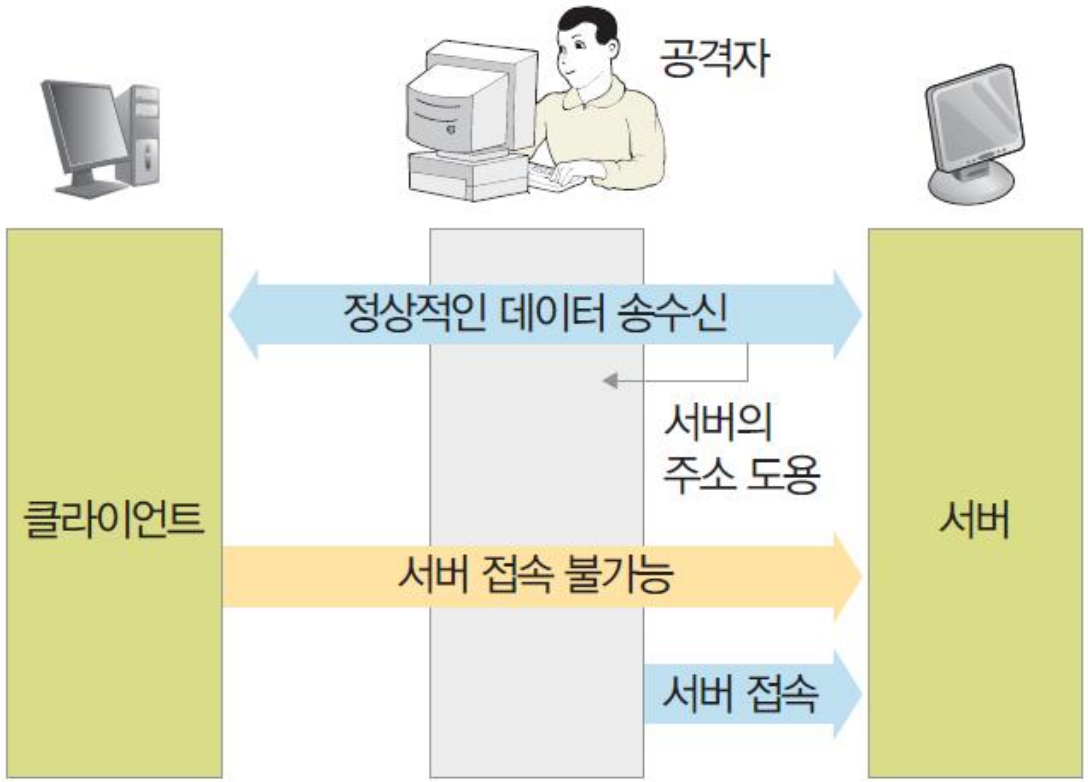
디도스

- Distributed Denial of Service의 약자로 '분산 서비스 거부' 또는 '분산 서비스 거부 공격'이라고 함
- 공격자는 여러 대의 좀비 컴퓨터를 분산 배치하여 동시에 공격 대상 컴퓨터나 네트워크를 공격



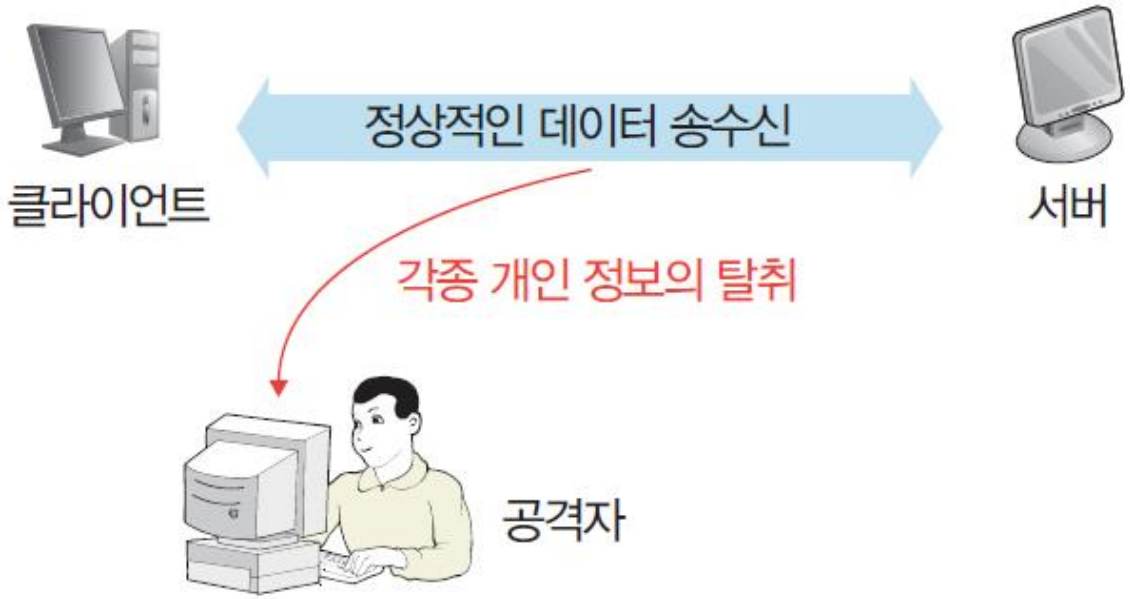
스푸핑

- 공격자가 MAC 주소, IP 주소, 전자메일 주소 등 자신의 정보를 위장하여 정상적인 사용자나 시스템이 위장된 가짜 사이트를 방문하도록 유도한 뒤 정보를 빼가는 수법



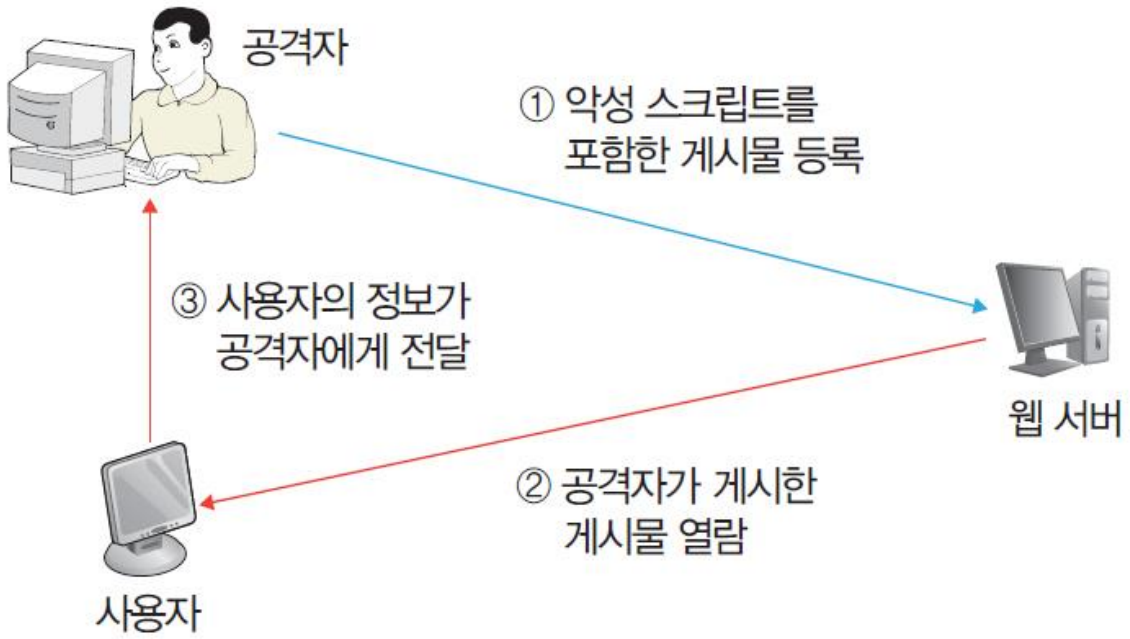
스니핑

- 네트워크에서 주고받는 데이터를 도청하여 사용자의 ID, 비밀번호, 전자메일 내용, 쿠키(cookie) 등을 가로채는 수법



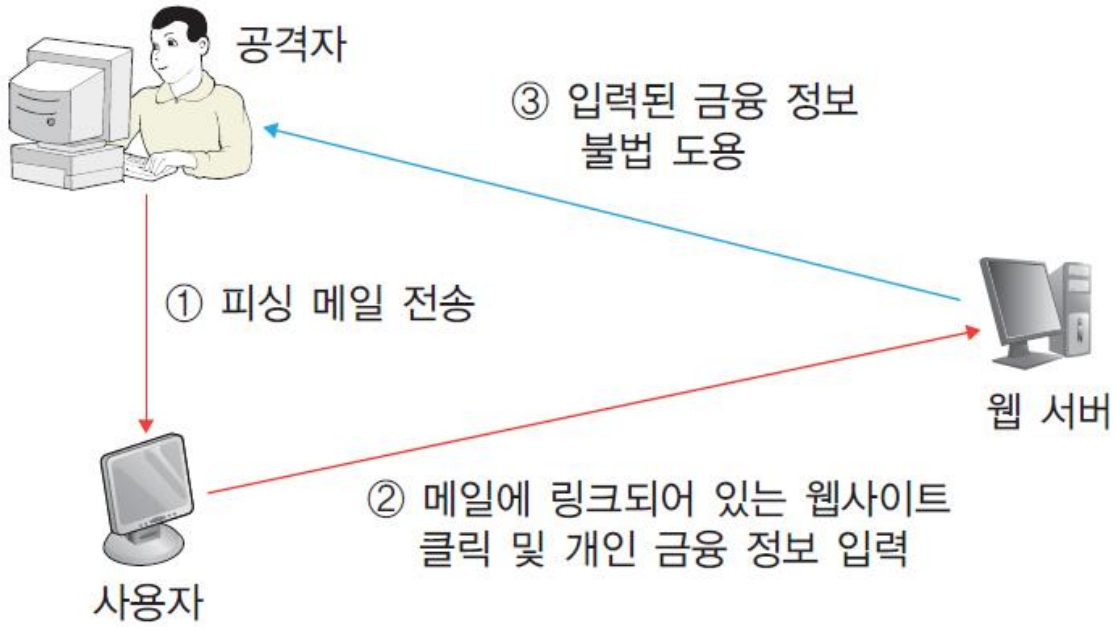
XSS

- 공격자가 게시판에 악성 스크립트가 포함된 글을 등록하면 사용자가 게시물을 열람하고, 그 순간 악성 스크립트가 실행되어 사용자의 정보가 공격자에게 전달됨



피싱

- 공격자가 금융 기관 등으로 위장하여 개인 정보를 알아낸 뒤 이를 이용하는 사기 수법



모바일 디바이스 해킹

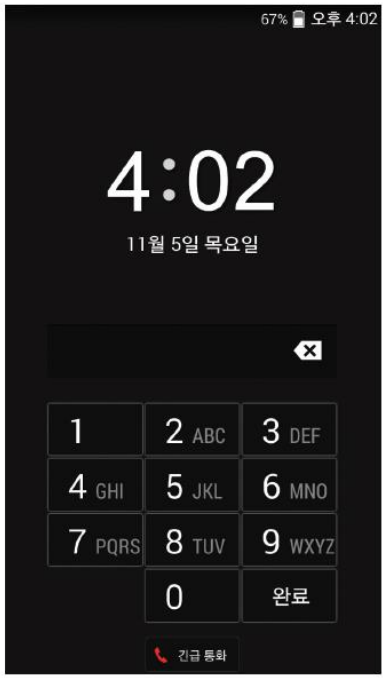
- 방식
  - 특정 앱의 업데이트를 사칭해 악성 앱 링크를 문자 메시지로 보냄. 사용자가 앱 링크를 클릭하면 자신도 모르는 사이에 악성 앱이 설치됨
  - 지하철, 커피숍 등에서 쓰이는 공용 와이파이를 이용해 타인의 스마트폰을 훔쳐봄
  - QR코드로 악성코드를 유포
- 피해
  - 스마트폰에 저장된 주소록, 문자 메시지, 금융 정보 등의 개인 정보를 빼내 악용
  - 스마트폰 카메라나 마이크를 의도적으로 작동시켜 사생활 염탐
  - 스마트폰의 GPS 위치 정보를 활용해 사용자의 위치 추적
  - 스마트폰을 좀비 스마트폰으로 만들어 해당 지역 통신사 기지국을 공격하는 해킹 도구로 사용

모바일 디바이스 해킹

- 예방
  - 스마트폰 비밀번호를 항상 설정해두기
  - 블루투스 같은 무선 네트워크는 사용할 때만 켜기
  - 중요한 정보는 스마트폰에 저장하지 않기
  - 문자 메시지나 SNS로 수신된 의심스러운 URL은 클릭하지 말고, 알 수 없는 파일은 설치하지 않기
  - 모바일 백신을 최신 버전으로 업데이트하고 실시간 감시 기능을 켜 놓기

모바일 디바이스 해킹

- 예방



(a) 비밀번호 설정

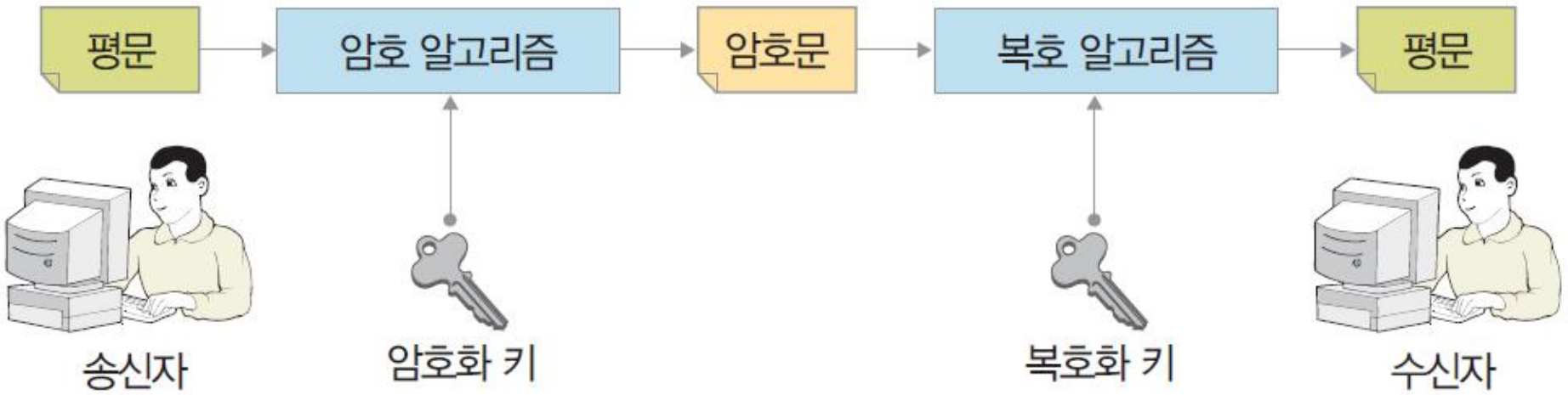
(b) 모바일 백신 설치

정보 보안 기술의 개념

- 개념
  - 컴퓨터 범죄를 억제하고 정보 자산을 보호하기 위한 기술 및 시스템
  - 크게 암호화 기술, 인증 기술, 네트워크 보안 기술로 나뉨

암호화 기술

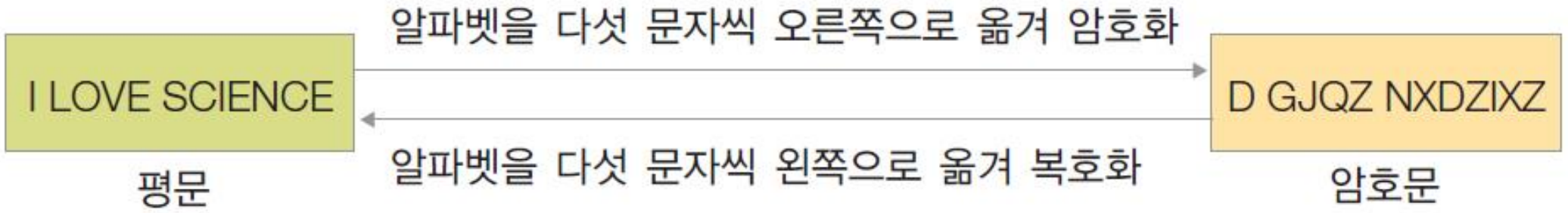
- 암호화(encryption)
  - 암호를 사용해 평문(plain text)을 암호문(cipher text)으로 변환하는 것
- 복호화(decryption)
  - 암호문을 원래의 평문으로 복원하는 것



암호화 기술

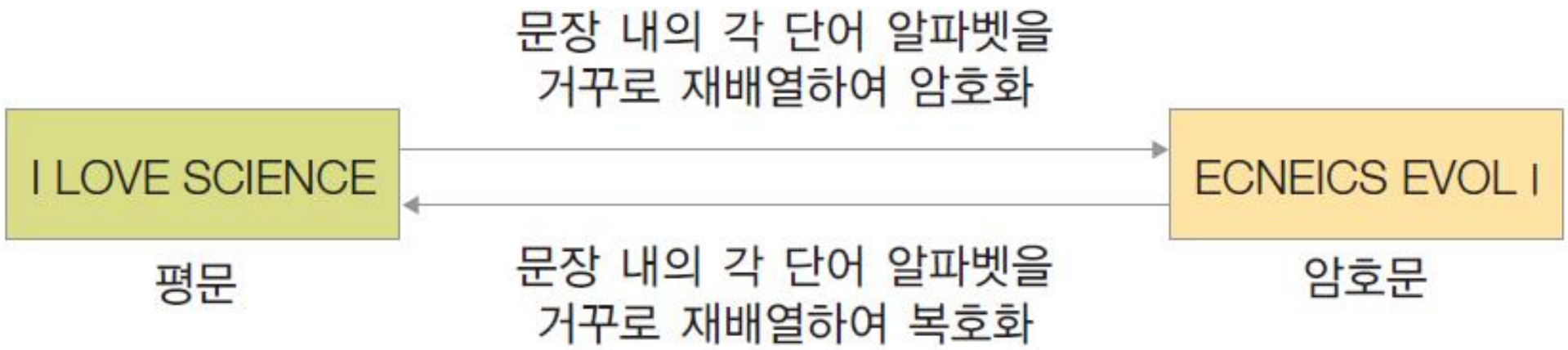
- 대체 암호

평문 문자	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	V	Z
암호문 문자	V	W	X	V	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U



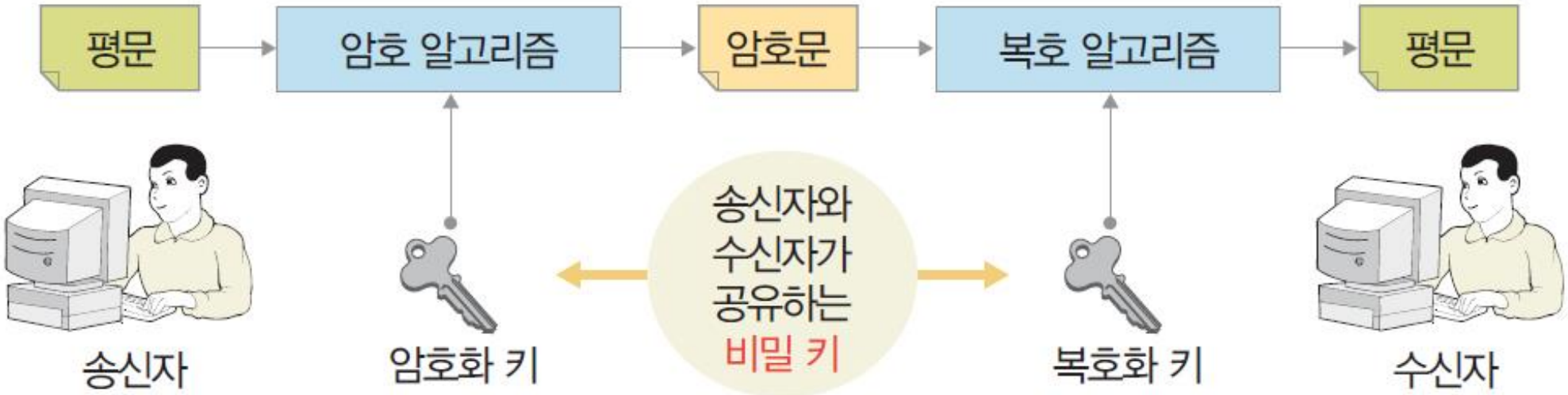
암호화 기술

- 전치 암호


문장 내의 각 단어 알파벳을
거꾸로 재배열하여 암호화
I LOVE SCIENCE
ECNEICS EVOL I
평문
암호문
문장 내의 각 단어 알파벳을
거꾸로 재배열하여 복호화

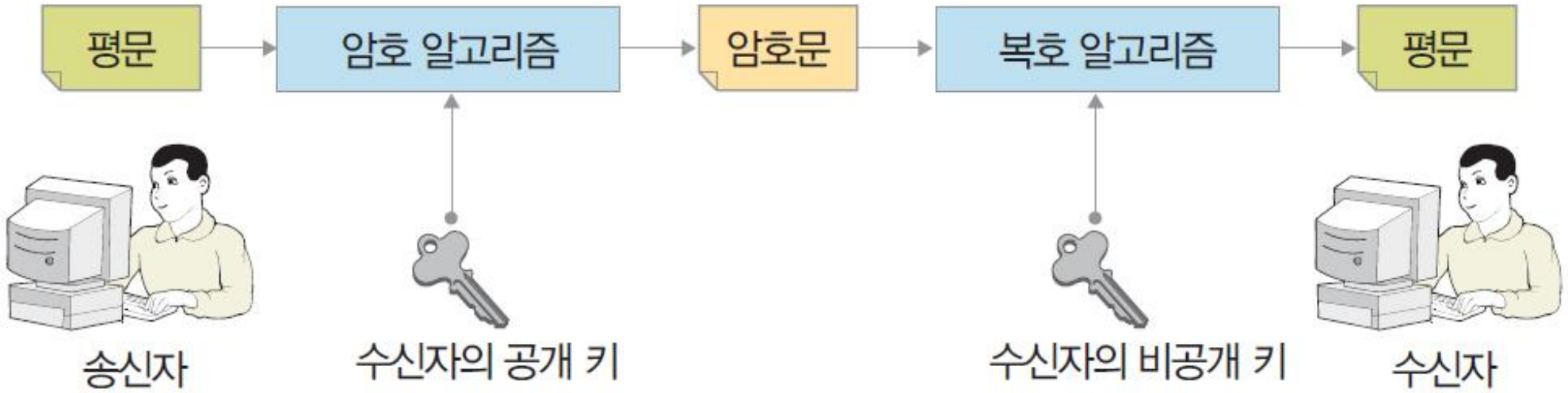
암호화 기술

- 비밀 키 암호화



암호화 기술

- 공개 키 암호화

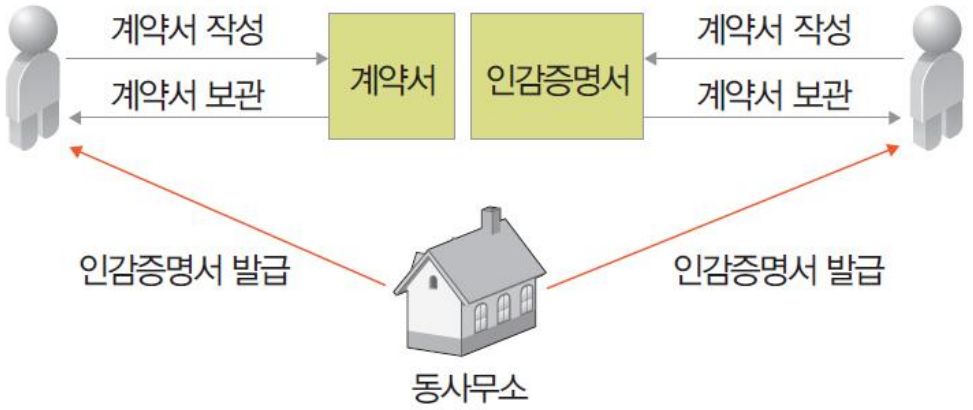


인증 기술

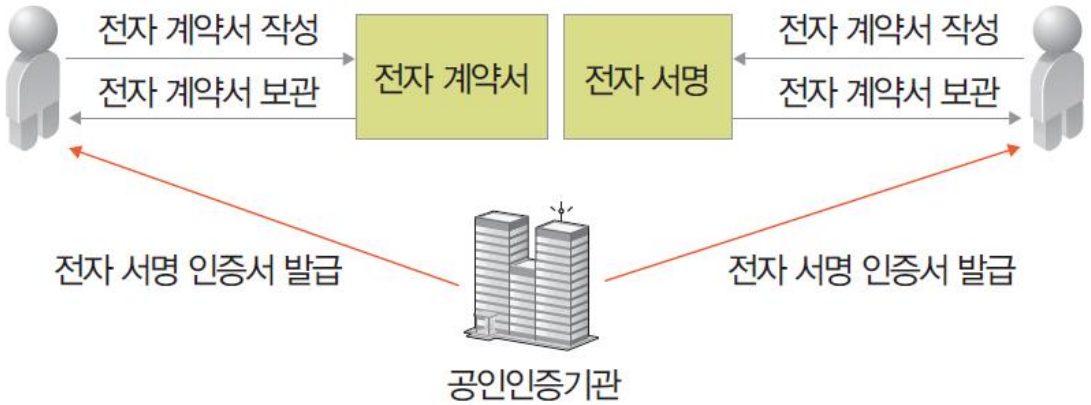
- 개념
  - 컴퓨터로 주고받는 문서에 대한 작성자의 신원을 보증하고 문서 내용을 인증하는 데 사용되는 기술

인증 기술

- 전자 서명
  - 전자 문서에 기존의 서명 또는 인감과 동일한 역할을 하는 서명을 하는 것



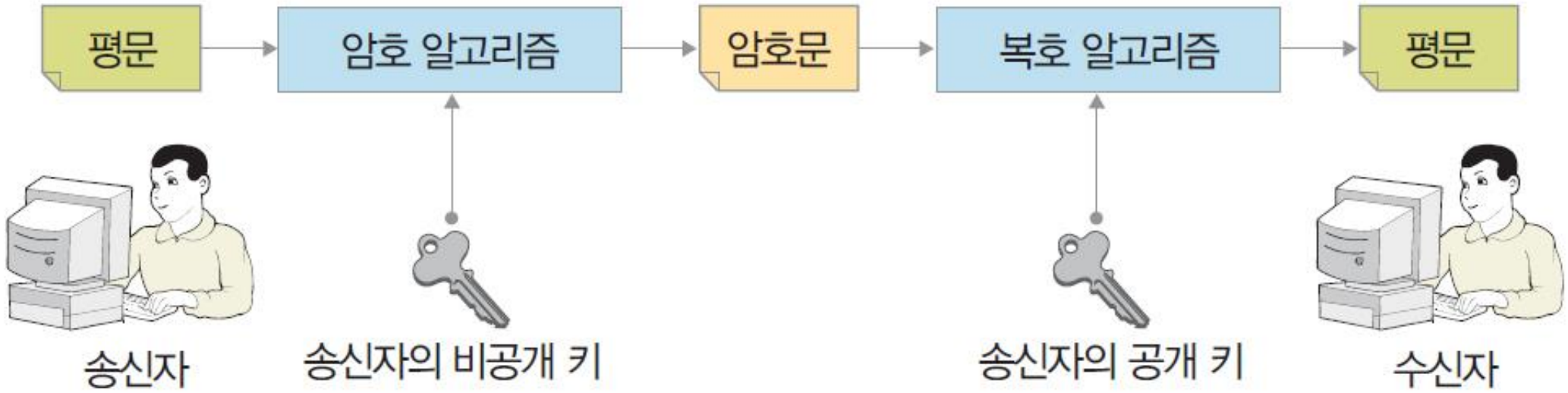
(a) 인감



(b) 전자 서명

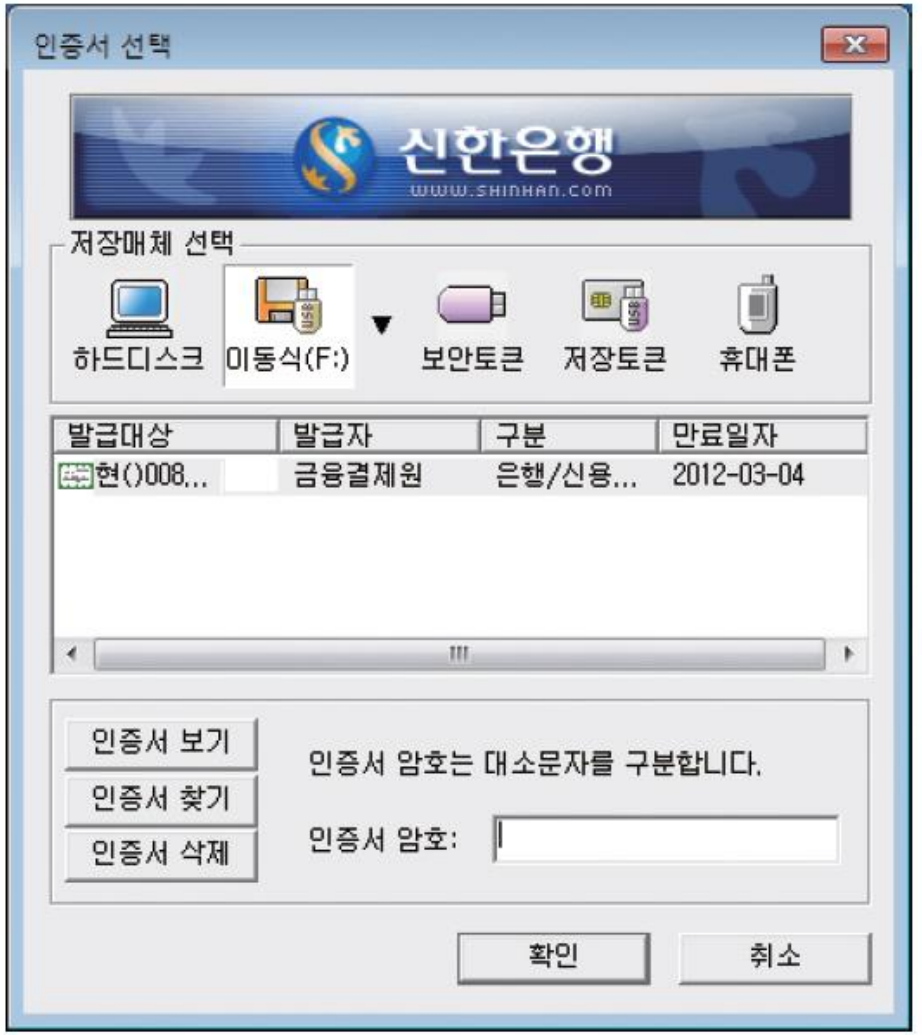
인증 기술

- 디지털 서명
  - 메시지 인증과 사용자 인증을 포함하는 개념



인증 기술

- 공인인증서
  - 공인인증 기관(CA, Certification Authority)이 발행하는 전자 정보 형태의 사이버 거래용 인감증명서



인증 기술

- 공인인증서
  - 우리나라의 최상위 인증기관 : 한국인터넷진흥원(KISA)

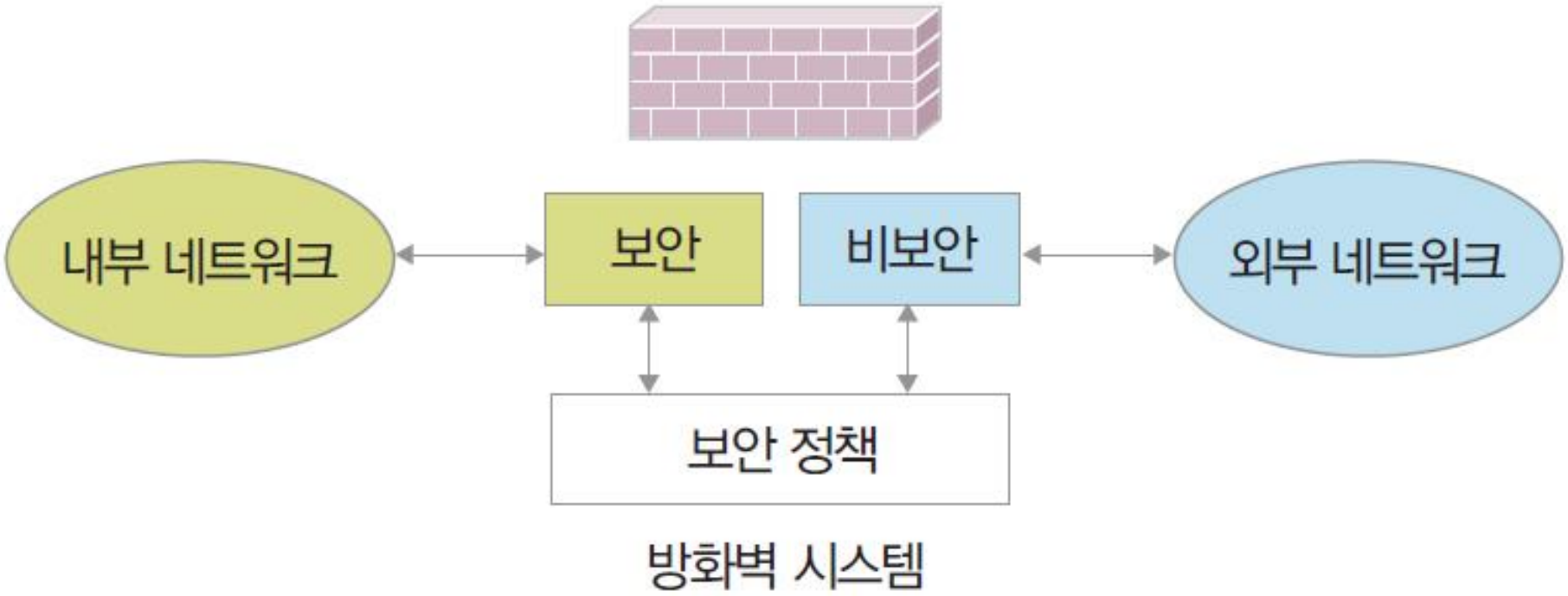
공인인증기관	홈페이지 주소
한국정보인증㈜	http://www.signgate.com/
㈜코스콤	http://www.signkorea.com/
한국전자인증㈜	http://www.crosscert.com/
한국무역정보통신	http://www.tradesign.net/
금융결제원	http://www.yessign.or.kr

네트워크 보안 기술

- 개념
  - 외부의 공격으로부터 내부 시스템을 보호하는 기술로, 소프트웨어와 하드웨어를 총망라함

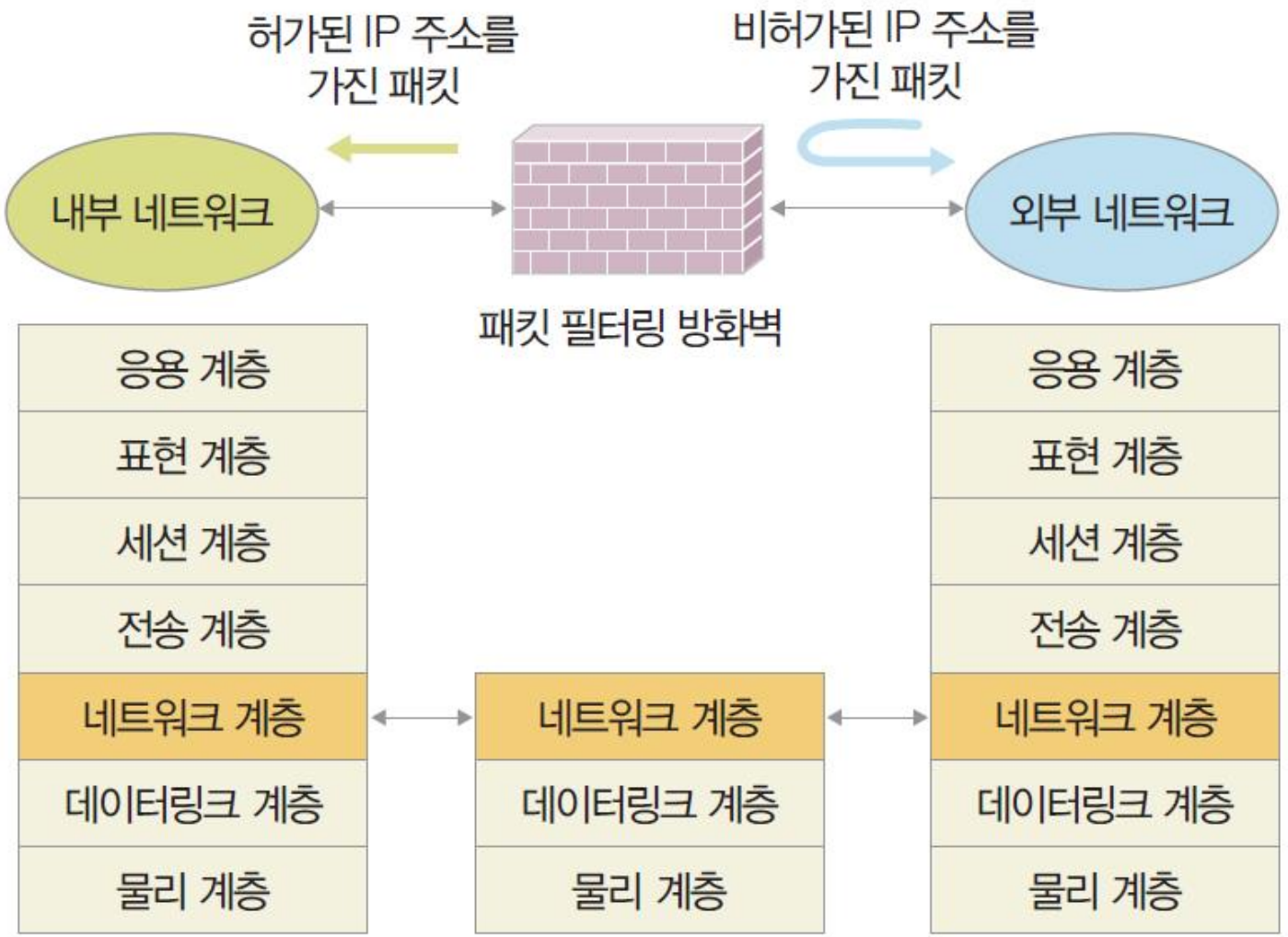
네트워크 보안 기술

- 방화벽
  - 외부의 공격으로부터 시스템을 보호하고 내부의 중요한 정보가 유출되지 않도록 차단하는 하드웨어 및 소프트웨어



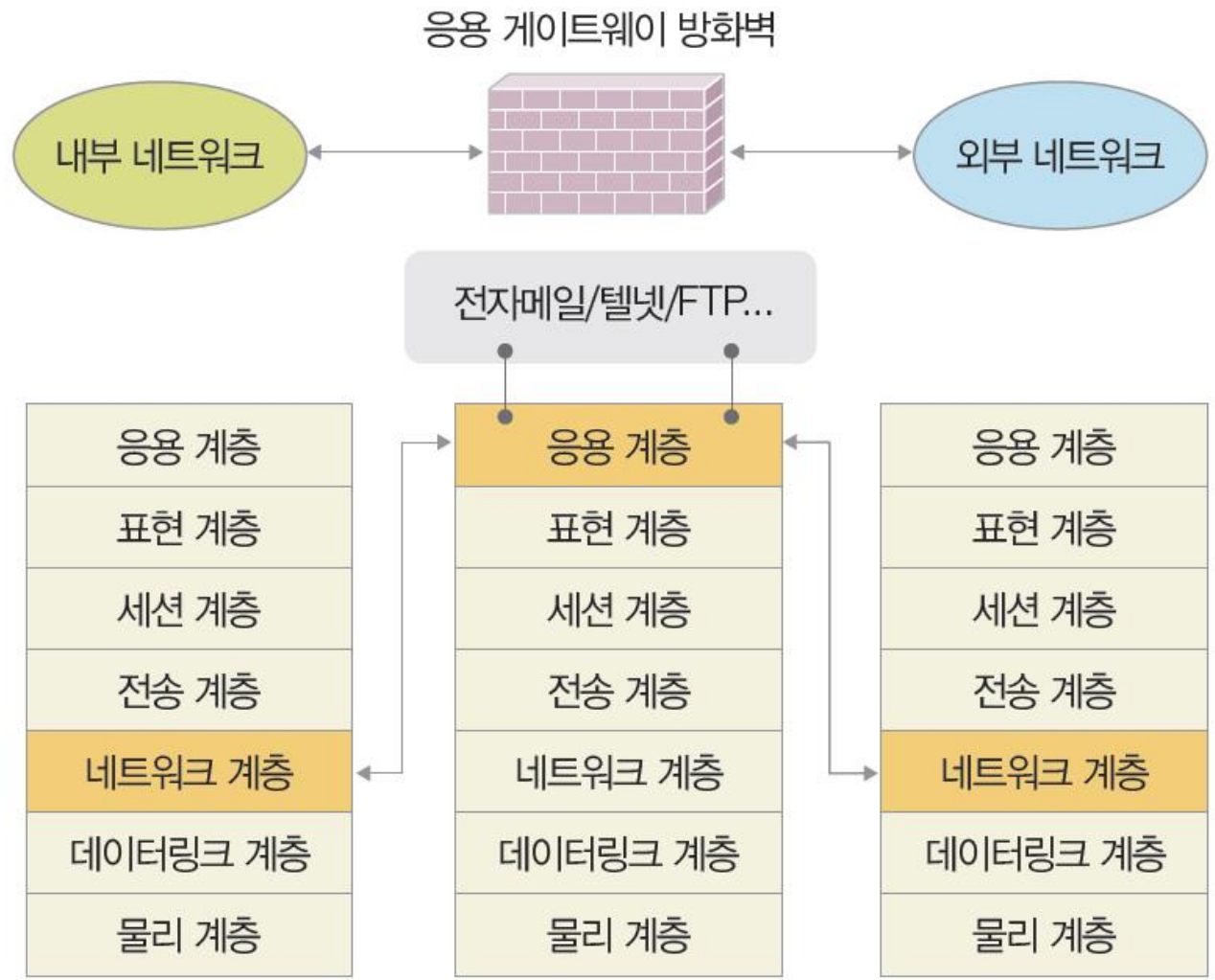
네트워크 보안 기술

- 방화벽
  - 패킷 필터링 방식



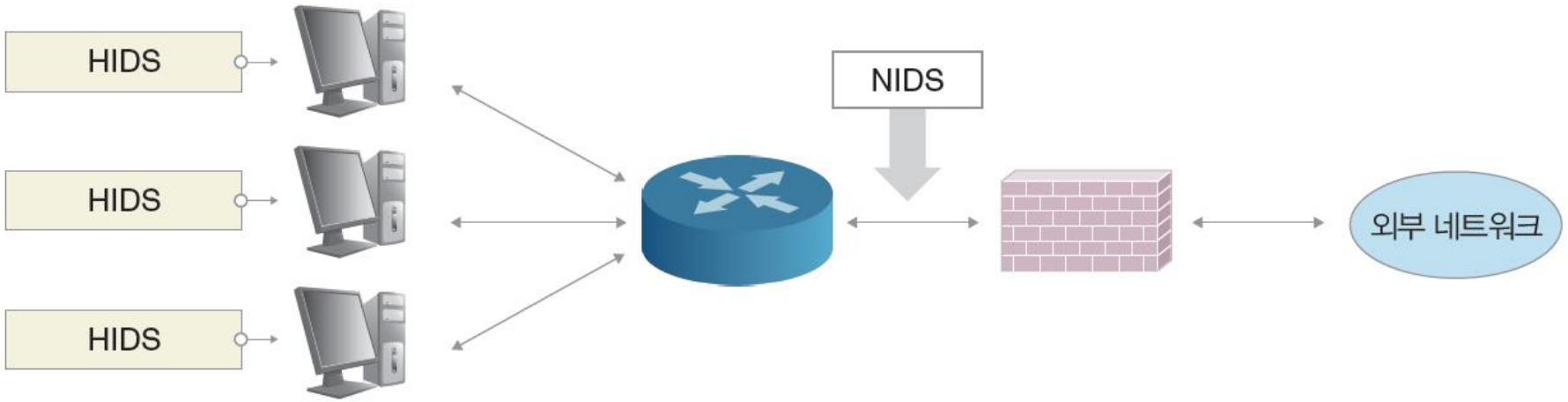
네트워크 보안 기술

- 방화벽
  - 응용 게이트웨이 방식



네트워크 보안 기술

- 침입 탐지 시스템
  - 악의를 가진 숙련된 해커에 의한 공격을 탐지하는 시스템
  - 건물에 비유하면 방화벽은 건물에 들어가기 전 입구에 설치된 경비 시스템이 고, IDS는 건물 곳곳에 설치된 감시카메라에 해당



네트워크 보안 기술

- 허니팟
  - 실제로 공격을 당하는 것처럼 보이게 하여 해커를 추적하고 정보를 수집
  - 해커를 유인하는 함정을 꿀단지(honey pot)에 비유한 것

컴퓨터 범죄 사례

- 디도스 공격 사례
  - 7.7 디도스 사건
  - 2009년 7월 7일에 발생
  - 정부 기관, 언론사, 금융 기관, 교육 기관 등 사회의 중추적인 역할을 담당하는 기관을 대상으로 공격 감행
  - 악성코드에 감염된 좀비 컴퓨터가 계획된 시각에 지정된 사이트를 공격
- 3.4 디도스 사건
  - 2011년 3월 4일에 발생
  - 네이버, 다음, 옥션 등 포털 사이트와 청와대, 국가정보원, 국방부 등 정부 기관, 그리고 금융 기관 등 총 40여 개의 기관을 대상으로 공격 감행
  - 7.7 디도스 공격보다 한층 더 진화된 공격 방식을 사용

컴퓨터 범죄 사례

- 소셜 네트워크와 모바일 기기를 이용한 범죄 사례
  - 가짜 초대 : 가짜 초청장을 발송해 스팸 웹 사이트로 유도
  - 사진 댓글 : 사진 댓글 알림창을 만들어 스팸 웹 사이트로 유도
  - 가짜 설문 : 설문 조사를 위장한 메시지를 전송해 스팸 웹 사이트로 유도
  - 애플리케이션 정보 : 인기 게임 등의 애플리케이션을 알려준다고 위장
  - 악성코드 유포 : 다운로드 안내 메시지 등으로 악성코드를 퍼뜨리는 스팸 메시지 발송
  - 사생활 보호 및 보안 업데이트 위장 : 개인 정보 관리 실태 파악 중이라고 속여 개인 정보 요구

정보 윤리

- 정보 윤리 실태 조사 (한국정보화진흥원 2010년 자료)
  - 정보 예절 : 부정적 언어 사용에 대한 문제점을 인식하고 있음
  - 정보 규범 : 인터넷 이용자들의 일탈 행동을 말하는 것, 일탈자 10명 중 4명은 '의도적 일탈자'
  - 온라인 신뢰 : 이용자 절반 이상이 정부, 지자체 등 공공 기관 사이트와 포털 사이트를 신뢰, 민간 사이트 및 정보 콘텐츠에 대한 신뢰는 낮음

정보 윤리

- 인터넷 불법 유해 정보 실태 조사 (방송통신심의위원회 2014년 자료)

유형	비율
성매매 및 음란 정보	26.9%
도박 등 사행성 정보	22.8%
권리 침해 정보	13.5%
불법 식의약품 정보	10.4%
기타 법령 위반 정보	10.1%

접속 경로	비율
스팸 메일	44.9%
포털 사이트 카페/블로그	38.4%
인터넷 팝업/배너 광고	34.1%
모바일 메신저 서비스	33.5%

- 정보 윤리 강화 방안
  - 정부, 교육 기관, 민간 단체가 범국민적인 정보 윤리 교육 실시
  - 인터넷 콘텐츠 사업자의 책임감 강화