Chapter 7

정보시스템 보안

학습목표

- 왜 정보시스템은 고장, 오류, 오남용 등에 취약한가?
- 보안과 통제의 비즈니스 가치는 무엇인가?
- 보안과 통제를 위한 조직 프레임워크의 구성요소는 무엇인가?
- 정보 자원 보호를 위한 주요 도구와 기술은 무엇인가?

보스턴 셀틱스 스파이웨어를 상대로 대승

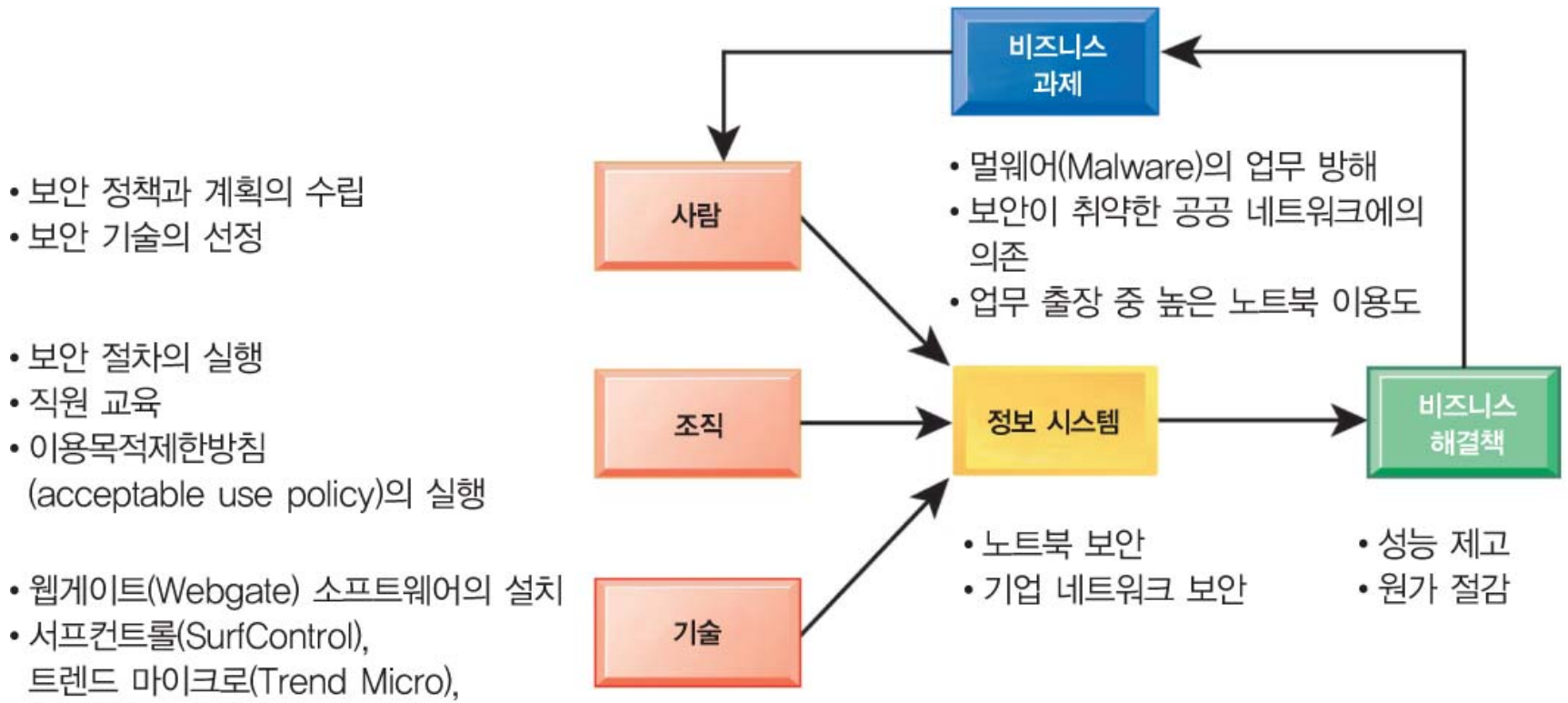
- Problem: 빈번한 무선 사용으로 인한 셀틱스의 시스템의 스파이웨어에 노출

- Solutions: 위협 요인을 식별하고 해킹의 시도의 위험을 줄이는 발전된 보안 시스템 설치

보스턴 셀틱스 스파이웨어를 상대로 대승

- Mi5 Networks’ Webgate security appliance의 설치 : 셀틱스의 방화벽과 네트워크 사이에 설치되어 스파이웨어의 침투를 방지하고, 감염된 장치의 연결을 사전에 방지토록 함
- 컴퓨터 보안에 노력하며, 유지하기 위한 정보기술의 역할을 상징
- 웹 상에서의 보안을 달성하기 위한 디지털 기술의 역할을 나타냄.

보스턴 셀틱스 스파이웨어를 상대로 대승



시스템의 취약성과 오남용

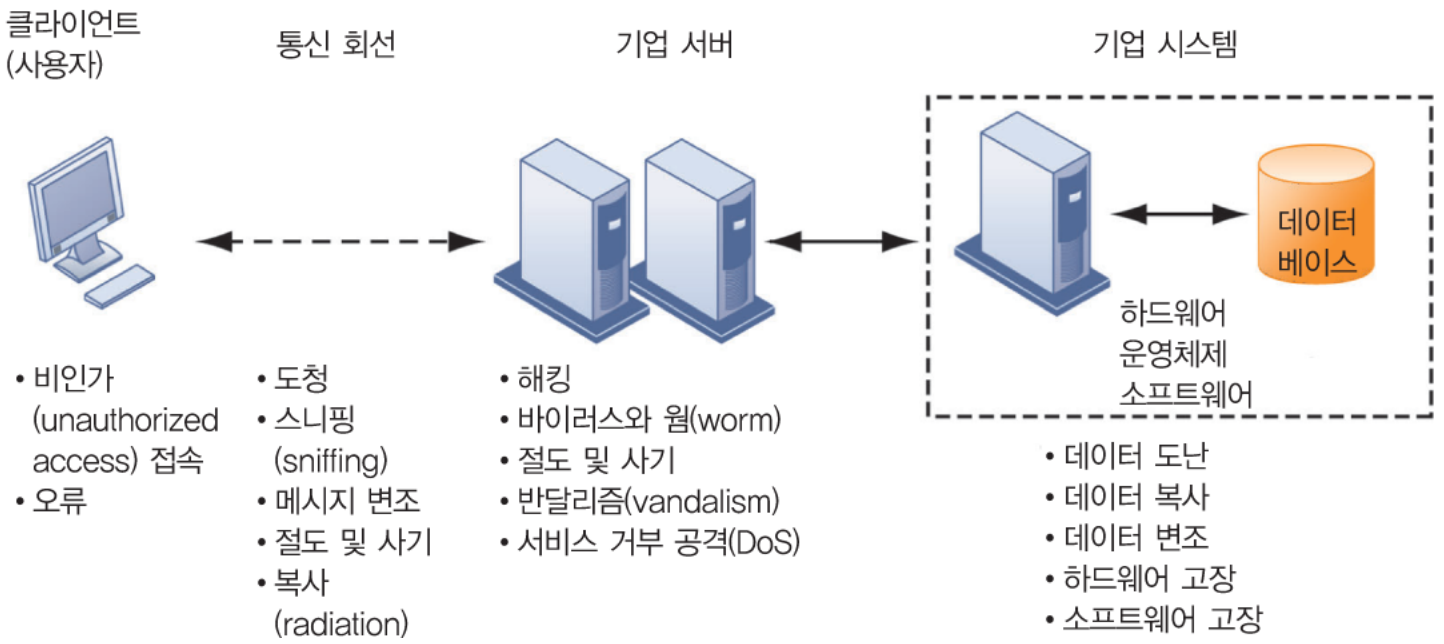
- **인터넷에 연결된 보호되지 않은 컴퓨터는 몇 초안에 불능 상태가 될 수 있다.**
- **보안:**
  - 정보시스템에 대한 인증되지 않은 접속, 변조, 절도, 및 물리적 침해를 방지하기 위한 정책, 절차 및 기술적 기준
- **통제:**
  - 조직 자산의 안정성, 회계 기록의 정확성과 신빙성, 경영 표준에 대한 운영상의 엄수성을 확보하기 위한 방법, 정책 및 조직 절차

왜 시스템은 취약한가?

- **하드웨어 문제**
  - 고장, 설정 오류(configuration errors), 부적절한 사용 또는 범죄로 인한 손상
- **소프트웨어 문제**
  - 프로그래밍 에러, 설치 오류, 허가되지 않은 변경
- **재해**
  - 전력 공급 차단, 홍수, 화재 등
- **기업의 통제 영역 이외의 네트워크와 컴퓨터의 사용**
  - 예) 국내외 아웃소싱 벤더

현대의 보안 문제와 취약성

그림 7-1 현대의 보안 문제와 취약점
웹기반 응용 시스템의 구조는 보통 웹클라이언트, 서버, 데이터베이스에 연결한 기업 정보 시스템 등을 포함한다. 이들 각각의 구성 요소는 보안 문제와 취약점을 가지고 있다. 홍수, 화재, 전력 고장 및 기타 전기적 문제들 역시 네트워크의 어느 지점에서든지 장애를 일으킬 수 있다.

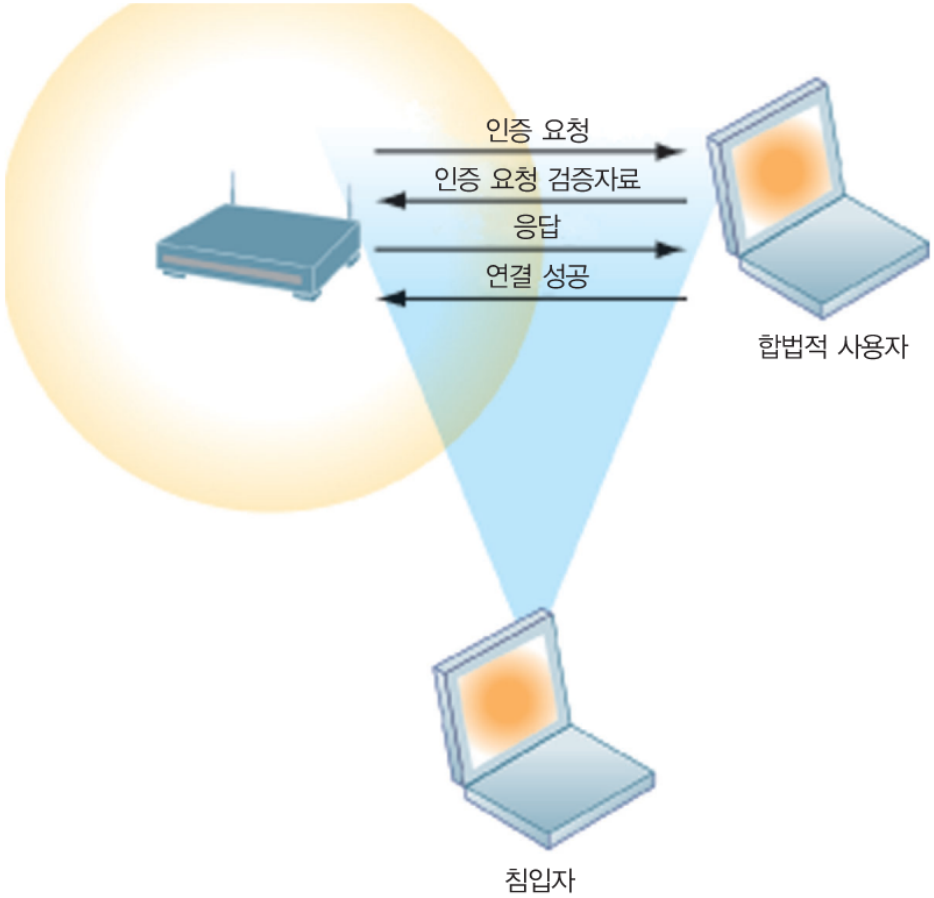


- 인터넷 취약성
  - 누구나 에게 개방된 네트워크
  - 인터넷 기반의 엄청난 오남용 규모가 광범위한 양향을 가짐.
  - 인터넷에 고정 또는 영구적 연결된 고정 인터넷 주소의 사용은 해커들에 의해 식별 되기가 용이하다.
  - 이메일 첨부
  - 거래의 비밀을 전송하는데 사용되는 이메일
  - 인스턴트 메시징 시스템은 보안에 취약하고 쉽게 노출될 수 있다.

- 무선 보안 과제
  - 무선 주파수 대역은 쉽게 스캔이 가능
  - SSIDs (service set identifiers)
    - 접속지점을 식별
    - 반복적 송출
  - War driving
    - 도청자가 건물 주변이나 외부 공원 등을 자동차로 배회하면서 무선 네트워크 통신을 가로채는 것
    - 해커가 SSID로의 접근권을 얻으면, 네트워크의 자원에 대한 접근권을 얻을 수 있음.
  - WEP (Wired Equivalent Privacy)
    - 보안 표준 (802.11)
    - 기본 명세상에서 사용자와 접속포인트 사이에 패스워드를 공유하고 있음.
    - 사용자가 보안 기능을 제대로 사용을 하지 못하는 경우

시스템의 취약성과 오남용

그림 7-2 와이파이 보안 문제
많은 와이파이 네트워크는 인가 없이 네트워크 자원에 접근하기 위한 주소를 수집하는 스니퍼 프로그램을 사용하여 침입자가 쉽게 침투할 수 있다.



악성 소프트웨어 : 바이러스, 웜, 트로이목마, 스파이웨어

- 악성 소프트웨어 (Malware)
  - 바이러스 (Viruses)
    - 사용자의 인지나 허락없이 실행되도록 하기 위해 다른 소프트웨어나 데이터 파일에 첨부시키는 악성 소프트웨어 프로그램
  - 웜(Worms)
    - 한 컴퓨터에서 네트워크 상의 다른 컴퓨터로 자기 자신을 복사할 수 있는 독립적인 컴퓨터 프로그램
  - 트로이 목마(Trojan horses)
    - 처음에는 호의적인 듯 하나 다른 무언가를 수행하는 소프트웨어 프로그램. 스스로의 복제는 하지 않지만 다른 바이러스나 악성코드를 이식하는 경로로 활용.

악성 소프트웨어 : 바이러스, 웜, 트로이목마, 스파이웨어

- 스파이웨어(Spyware)
  - 웹 활동을 감시하고 광고를 위해 은밀하게 설치된 작은 소프트웨어
- Key loggers
  - 시리얼 번호나 패스워드를 훔쳐 인터넷 공격을 감행하기 위해 컴퓨터 상의 모든 타이핑을 기록

해커와 컴퓨터 범죄

- 해커 (Hackers) vs 크래커(crackers)
- 활동:
  - 시스템 침입
  - 시스템 손실
  - 사이버 파괴행위(Cybervandalism)
    - 고의적 방해, 명예훼손, 웹사이트 또는 기업 정보시스템 파괴

해커와 컴퓨터 범죄

- 스프핑(Spoofing)
  - 가짜 이메일 주소를 사용하거나 다른 누군가호 위장함으로써 실체를 숨기려하는 행위
  - 본래 사용자가 방문하고자 하는 것 처럼 위장한 사이트를 이용하여 원래 의도와 다른 주소로 웹연결을 재설정하려는 행위
- 스니퍼(Sniffer)
  - 네트워크를 통해 전달되는 정보를 감시하는 도청 프로그램의 유형
  - 해커들이 이메일, 기업 파일 등과 같은 소유된 정보를 훔치도록 하게함.

해커와 컴퓨터 범죄

- Denial-of-service attacks (DoS)
  - 네트워크를 붕괴할 목적으로 수천 건의 잘못된 통신이나 서비스요청을 네트워크 서버나 웹서버에 쏟아 붓는 것.
- Distributed denial-of-service attacks (DDoS)
  - DoS를 실행하기 위한 수 많은 컴퓨터의 사용
  - Botnets
    - Bot malware에 감염된 네트워크 상의 "zombie" PCs

해커와 컴퓨터 범죄

- 컴퓨터 범죄
  - 범죄의 대상으로서 컴퓨터:
    - 보호된 컴퓨터 데이터에 대한 기밀성 침해
    - 허가되지 않은 시스템 접속
  - 범죄의 수단으로서 컴퓨터:
    - 거래 기밀의 절도
    - 위협 및 희롱을 위한 이메일의 사용

해커와 컴퓨터 범죄

- 신분위장 절도(Identity theft)
  - 다른 사람을 가장하여 개인정보 (주민번호, 운전면허 번호, 신용카드 번호 등)을 절도하는 행위
- 피싱(Phishing)
  - 사용자의 정보를 요청하도록 만들어진 가짜 웹 사이트의 설치 및 이메일 전송
- Evil twins
  - 인터넷의 와이파이 연결을 제공하는 척하는 무선 네트워크

해커와 컴퓨터 범죄

- 파밍(Pharming)
  - 정확한 웹 페이지 주소를 입력했음에도 불구하고 다른 가짜 웹사이트로 방문하도록 하는 것.
- 클릭 사기(Click fraud)
  - 정보 수집 및 구매 목적 없이 온라인 광고에 허위로 클릭하는 행위

사례 연구(조직의 관점) : ICICI 은행의 보안

- 다음의 사례 연구를 읽고 다음 물음에 답하시오.
  - 본 사례에서 나타난 은행의 보안대책은 무엇인지 나열하시오.
  - 각 보안 대책 별 어떤 위협에 효과적인지 설명하시오.
  - 이러한 보안 대책이 적합하다고 생각하는가? 미래의 이 은행이 시스템을 보호하기 위해 무엇을 해야 하는가?

내부 위협 : 직원

- 보안의 위협은 때로는 조직 내부에서 발생한다.
  - 내부 지식
  - 허술한 보안 절차
    - 사용자의 지식 부족
  - 사회공학(Social engineering):
    - 시스템에 접근하고자 하는 악의적 침입자는 가끔 정보가 필요한 기업의 정규직원으로 가장하여 직원이 암호를 노출시키게 속임수를 사용한다.

소프트웨어의 취약성

- 보안의 취약성을 만들어 내는 상업용 소프트웨어의 오류
  - Hidden bugs (프로그램 코드 오류)
    - 완벽한 테스트는 없기 때문에 무결점의 프로그램은 존재하기 힘들다.
  - 프로그램 오류는 침입자에게 네트워크를 공개하게 한다.
- 패치(Patches)
  - 프로그램 공급자들이 배포하는 오류를 수정하기 위해 배포하는 프로그램 조각
  - 사용 중인 수많은 소프트웨어는 패치가 보급되어 시행되기 이전에 이미 사용된다.

보안과 통제의 비즈니스 가치

- 컴퓨터 시스템의 오류는 비즈니스 기능의 커다란 손실을 야기할 수 있다.
- 기업들은 과거보다 더욱 취약하다.
  (정보기술 에 대한 높은 의존도)
- 보안으로 인한 문제는 기업의 시장 가치에 즉각적으로 반영된다.
- 부적절한 보안과 통제는 신뢰 및 책임의 문제를 야기함.

전자기록 관리에 대한 법적 규제적 요건

- 기업들은 개인 프라이버시 보호 뿐 아니라 전자기록의 유지와 저장에 대한 새로운 법적 의무에 직면하고 있음.
  - HIPAA: 의료 보안과 개인보호정책의 규제와 절차
  - Gramm-Leach-Bliley Act: 재무관련 기관들의 고객 데이터에 대한 보안과 기밀성 요구
  - Sarbanes-Oxley Act: 내부에서 사용되어 외부로 배포되는 재무 정보의 정확성과 일치 여부를 감시하는 기업과 경영자에 대한 책임을 부여

전자증거와 컴퓨터 과학수사(Computer Forensics)

- 화이트 칼라 범죄의 증거가 디지털 형태로 남는다.
  - 컴퓨터 장치, 이메일, 메신저, 전자상거래에 대하여 저장된 데이터
- 데이터에 대한 적절한 통제는 법적 조사 요청에 시간과 비용을 절감하게 한다.
- 컴퓨터 과학수사(Computer forensics):
  - 법적 증거물로 사용될 수 있는 컴퓨터 저장 장치의 데이터에 대한 분석, 과학적 수집, 조사, 인증, 보존을 의미
  - 숨겨진 데이터에 대한 복원 포함

- 정보시스템 통제
  - 일반 통제
    - 조직의 정보기술 인프라구조 전역에 걸친 일반적인 설계, 보안, 프로그램의 사용, 데이터 파일에 대한 보안을 관장
    - 모든 컴퓨터화된 응용 시스템에 적용
    - 포괄적인 통제 환경을 만들기 위한 하드웨어, 소프트웨어, 물리적, 수동적 절차의 결합
  - 유형 : 소프트웨어 통제, 하드웨어 통제, 컴퓨터 운영통제, 데이터 보안 통제, 구현 통제, 관리 통제

- 응용통제 (Application controls)
  - 급여처리, 주문처리와 같은 특정 응용시스템에 대한 통제
  - 자동/수동의 절차를 모두 포함
  - 단지 권한을 부여 받은 데이터만 응용시스템을 통해서 처리되어진다는 것을 확인
  - 포함내용:
    - 입력 통제 (Input controls)
    - 처리 통제 (Processing controls)
    - 출력 통제 (Output controls)

- 위험도 평가
  - 특정 활동이나 처리가 제대로 통제되지 않을 때 기업에 미치는 위험도에 대한 수준을 결정
    - 위협의 유형
    - 연중 발생 확률
    - 잠재적 손실, 위협의 가치 환산
    - 예측되는 연간 손실

EXPOSURE	PROBABILITY	LOSS RANGE	EXPECTED ANNUAL LOSS
Power failure	30%	$5K - $200K	$30,750
Embezzlement	5%	$1K - $50K	$1,275
User error	98%	$200 - $40K	$19,698

보안과 통제를 위한 프레임워크의 수립

- 보안 정책 (Security policy)
  - 정보위험도의 순위 결정, 수용 가능한 목안목표 설정, 목적 달성을 위한 매커니즘 구현
  - 그 밖의 보안 관련 정책
    - 이용목적 제한 방침(Acceptable use policy : AUP)
      - 기업의 정보자원과 컴퓨터 장비의 사용에 대한 정의
    - 인가정책 (Authorization policies)
      - 정보자산에 대한 사용자의 접근 권한을 결정
- 인가관리 시스템(Authorization management systems)
  - 사용자에 따라 웹사이트의 어느 부분 또는 어떤 데이터베이스에 접근이 허락되어지는가에 대한 결정 (접근 규칙과 프로파일에 따라 허용)

Security Profiles for a Personnel System

보안 프로파일 1

사용자: 인사부서 사무원 위치: 제 1 사업부 해당 프로파일에 대한 종업원 식별 코드	00753, 27834, 37665, 44116
데이터 필드 제한	**접근 유형**
제 1 사업부 종업원 데이터에 한함	조회 및 수정
• 의료 기록 데이터	해당 없음
• 급여	해당 없음
• 연금 소득	해당 없음

보안 프로파일 2

사용자: 사업부 인사부서 관리자 위치: 제 1 사업부 해당 프로파일에 대한 종업원 식별 코드	27321
데이터 필드 제한	**접근 유형**
제 1 사업부 종업원 데이터에 한함	읽기 전용

그림 7-3 인사관리 시스템을 위한 보안 프로파일
이 두 예제는 인사관리 시스템에서 흔히 발견할 수 있는 두 개의 보안 프로파일이나 데이터 보안 유형을 보여주고 있다. 보안 프로파일에 따라 사용자는 조직 내의 다양한 시스템, 구역, 데이터에 대한 접근에 있어 특정 제한을 받게 된다.

재난복구 계획과 비즈니스 연속성 계획

- 재난 복구 계획 : 파괴된 서비스의 복원을 위한 계획을 고안
- 비즈니스 연속성 계획 : 재난 이후의 비즈니스 운영을 재개하는 것에 대한 계획에 초점
  - 두 가지 계획 모두 기업의 가장 중요한 시스템에 대한 인식이 우선적으로 필요
  - 정전으로 인한 충격을 결정하기 위한 비즈니스 영향 분석
  - 경영진은 어느 시스템이 우선적으로 복구되어야 하는지 결정해야 한다.

감사(Auditing)의 역할

- 경영정보시스템 감사(MIS audit)
  - 개별 정보시스템을 관장하는 통제 뿐만 아니라 기업의 전반적인 보안 환경을 조사
  - 기술, 절차, 문서화, 훈련, 인적자원에 대한 조사
  - 기술, 정보시스템 관련 직원, 그 밖의 직원들의 위기 대처 능력을 테스트하기 위한 가상 훈련
  - 모든 통제 취약점을 열거하고 운선 순위를 정하며, 발생 가능성을 추정
  - 각각의 위협에 대한 재무적, 조직적 측면에서의 충격 정도를 평가

Sample Auditor's List of Control Weaknesses

그림 7-4 감사자의 통제 취약점 목록 예시
이 도표는 감사자가 지역 시중 은행의 대출 시스템에서 발견할 수도 있는 통제 취약점 목록의 예시 페이지이다. 이러한 양식은 감사자가 통제 취약점을 기록하고 평가하는 것을 도와주며 경영진이 대응한 어떤 정정 지시는 물론 경영진과 취약점에 대해 논의한 결과도 보여준다.

업무: 대출 위치: Peoria, IL	작성자: J. Ericson 작성일: 2010.6.16		수신자: T. Benson 검토일: 2010.6.28	
취약점과 파급 효과	오류/오남용의 기회		경영진 알림 사항	
	예/아니요	사유	보고일	경영진의 대응 사항
잊어버린 패스워드를 가진 사용자 계정	예	인가받지 않은 외부인 또는 공격자에게 시스템이 개방된 채로 방치됨	5/10/10	패스워드 없는 계정 삭제
시스템 파일의 공유를 허용하게 설정된 네트워크	예	핵심 시스템 파일을 네트워크에 연결된 적대적 집단에게 노출시킬 가능성이 있음	5/10/10	필요한 디렉터리만 공유되도록 하고 이를 강력한 패스워드로 보호해야 함
소프트웨어 패치는 표준 및 통제(Standards and Controls) 그룹의 최종 승인 없이 업무 프로그램을 업데이트 할 수 있음	아니요	모든 업무 프로그램은 관리자의 허가가 요구함. 표준 및 통제(Standards and Controls) 그룹이 이 사례를 한시적 업무 진행 상태로 분류함		

접근 통제

- 조직 내/외부의 비 권한자의 시스템에 대한 접속을 방지하는 정책과 절차
  - 인가
  - 인증
    - Password systems
    - Tokens
    - Smart cards
    - 생체인증 (Biometric authentication)

방화벽, 침입탐지 시스템, 안티바이러스 소프트웨어

- 방화벽:
  - 비 권한자의 사설 네트워크로의 접근을 차단하는 하드웨어와 소프트웨어의 결합
  - 관련 기술:
    - 정적 패킷 필터링 (Static packet filtering)
    - Network address translation (NAT)
    - Application proxy filtering

보안을 위한 기술과 도구

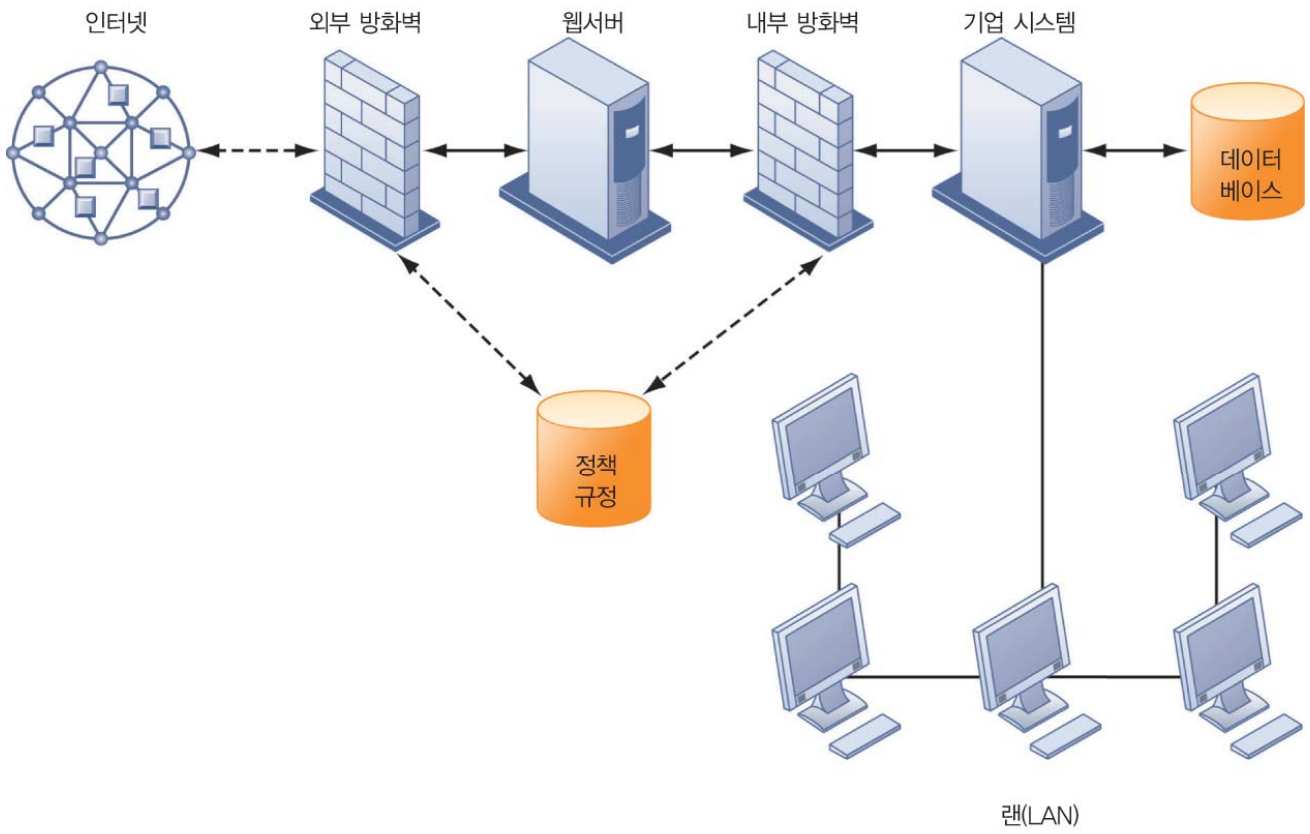


그림 7-5 기업 방화벽
방화벽은 인가받지 않은 통신 트래픽으로부터 기업의 사설 네트워크를 보호하기 위하여 기업의 사설 네트워크와 공공 인터넷이나 다른 신뢰할 수 없는 네트워크 사이에 위치한다.

방화벽, 침입탐지 시스템, 안티바이러스 소프트웨어

- **침입탐지 시스템:**
  - 침입자를 발견하고 저지하기 위한 중요지점(hot spots)을 감시
  - 진행중인 공격을 발견하기 위해 발생하는 모든 이벤트를 조사
- **안티바이러스와 안티스파이웨어 소프트웨어:**
  - 악성 프로그램의 존재여부를 확인하고 제거
  - 지속적인 업데이트 요구

무선 네트워크 보안

- 유선 동등 프라이버시(wired equivalent privacy : WEP) 보안의 기능 개선
  - WEP 실행
  - 네트워크의 SSID에 고유한 이름 할당
  - 사설통신망과 함께 사용
- Wi-Fi Alliance의 WAP2 specification 승인(강력한 표준), WEP의 대체
  - 지속적으로 keys의 변경
  - 중앙 서버의 암호화 인증 시스템

암호와(Encryption)와 공개키(Public Key) 인프라

- 암호화 (Encryption):
  - 의도되지 않은 수신자들이 읽지 못하도록 텍스트와 데이터를 암호 형태의 텍스트로 전환
  - 네트워크 상에서의 암호화를 위한 두 가지 방법
    - Secure Sockets Layer (SSL)와 successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)

암호와(Encryption)와 공개키(Public Key) 인프라

- 암호화의 두 가지 방법
  - 대칭키 암호화 (Symmetric key encryption)
    - 송신자와 수신자가 단일의 공유된 키를 사용
  - 공개키 암호화 (Public key encryption)
    - 수학적으로 관계된 두 가지 키를 사용 : public key와 private key
    - 송신자가 수신자의 공개키를 가지고 메시지를 암호화
    - 수신자는 개인키를 가지고 해독

Public Key Encryption

그림 7-6 공개키 기반 암호화

공개키 암호화 시스템은 데이터를 전송할 때는 잠그고 수신할 때는 여는 공개키와 비밀키의 시리즈로 볼 수 있다. 송신자는 수신자의 공개키를 디렉터리에서 찾고 메시지를 암호화할 때 이를 사용한다. 메시지는 인터넷이나 사설 네트워크를 통해 암호화된 형식으로 전송된다. 암호화된 메시지가 도착하면 수신자는 데이터를 해독하고 메시지를 읽기 위해 자신의 비밀키를 사용한다.

암호와(Encryption)와 공개키(Public Key) 인프라

- 전자인증서 (Digital certificate):
  - 온라인 거래의 보호를 위해 사용자와 전자적 자산을 고유성을 확립하기 위해 사용되는 데이터 파일
  - 믿을 수 있는 제 3자의 기관을 이용하여 사용자의 고유성을 확립
  - 제 3자 기관은 사용자의 고유성을 확인하고, 서버상에 정보를 저장하여 소유자의 ID 정보와 공개키의 사본을 담고 있는 전자 인증서를 발급
- 공개키(Public key infrastructure :PKI)
  - 인증 권한을 가지 공개키 암호화를 사용
  - 전자상거래에서 널리 사용

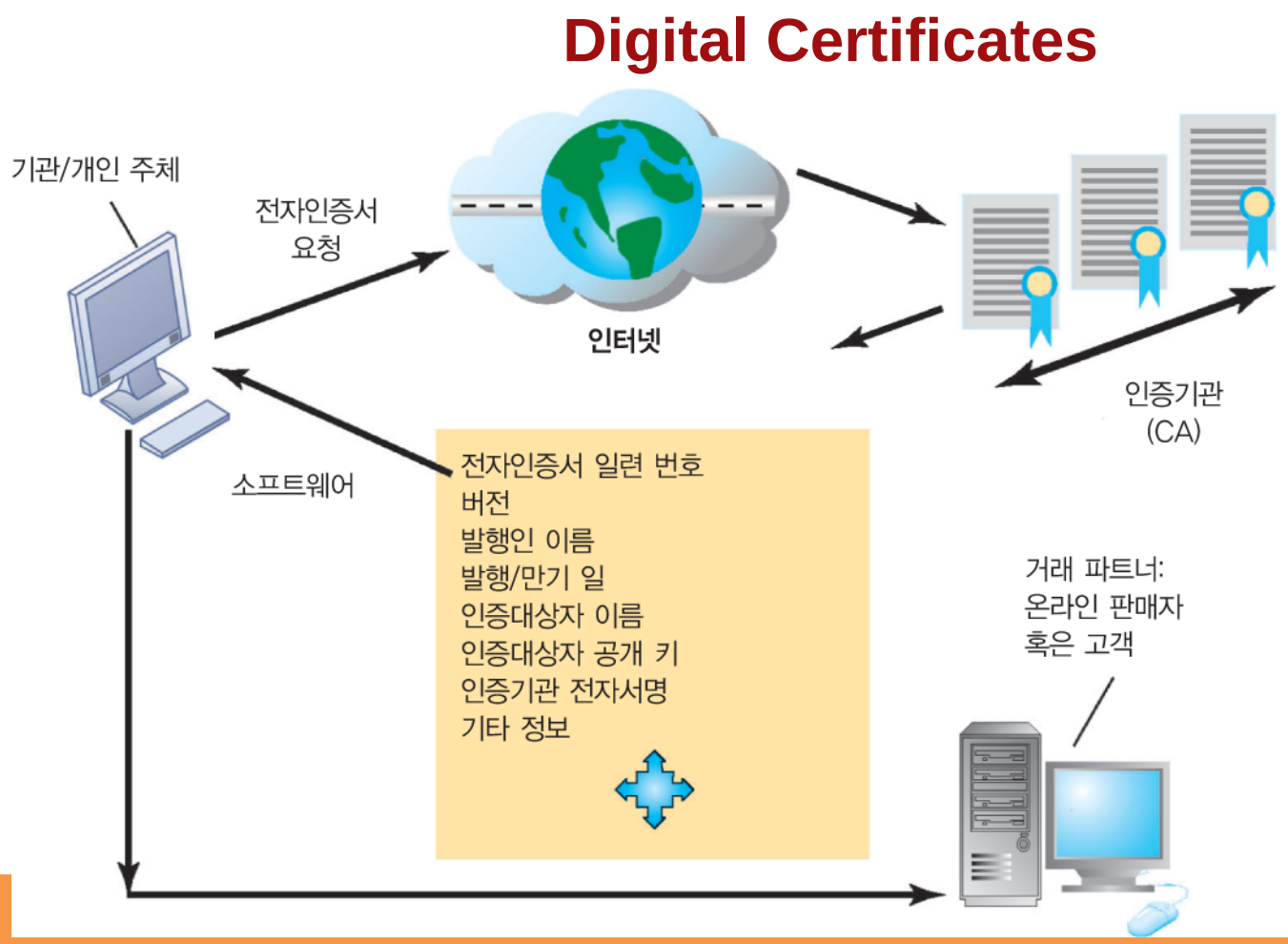


그림 7-7 전자 인증서
전자인증서는 사람 또는 전자적 자산의 고유성을 확립하도록 돕는다. 전자인증서는 안전하고 암호화된 온라인 통신 방법을 제공하여 온라인 거래를 보호하고 있다.

시스템 가용성의 확보

- 온라인 거래 처리는 100%의 가용성을 요구한다.
- 내결함성 컴퓨터 시스템 (fault-tolerant)
  - 지속적 가용성 (주식시장)
  - 지속적이고 중단 없는 서비스 제공을 위한 환경을 조성할 수 있는 여분의 하드웨어, 소프트웨어, 전원 공급 요소를 포함
- 고 가용성 컴퓨팅
  - 충격으로부터 빠른 복구를 지원
  - 다운타임의 최소화

시스템 가용성의 확보

- **복구지향 컴퓨팅 (Recovery-oriented computing)**
  - 다요소의 시스템에서 운영자가 결함을 정확히 찾아내어 빠르게 해결할 수 있도록 시스템을 설계
- **네트워크 트래픽의 통제 (Controlling network traffic)**
  - Deep packet inspection (DPI)
    (video나 music 차단 : 속도저하의 원인)
- **보안 아웃소싱 (Security outsourcing)**
  - Managed security service providers (MSSPs)

소프트웨어의 품질 확보

- Software Metrics: 계량적 척도의 형식으로 시스템에 대한 객관적인 평가
  - 거래 숫자
  - 온라인 응답시간
  - 시간 당 출력되는 출력
  - 백줄의 코딩에서 발생하는 버그의 수
- 초기와 정규 검사
- Walkthrough: 소규모의 전문가 집단의 명세서 및 설계 문서의 검토
- Debugging: 오류가 제거되어지는 절차

사례연구 (기술의 관점) : 클라우드 컴퓨팅은 얼마나 안전한가?

- 사례 연구를 읽고 다음의 물음에 답하시오.:
  - 이 사례에서 기술된 보안과 통제의 문제는 무엇인가? 이러한 문제에 인간, 조직, 기술의 어떠한 요소가 영향을 끼쳤는가?
  - 클라우드 컴퓨팅은 얼마나 안전한가?
  - 만약 당신이 회사의 정보시스템 담당부서에 근무한다면, 클라우드 관련 업체와 어떠한 문제를 명확히 하고 싶은가?
  - 기업 시스템을 클라우드 컴퓨팅 업체에 맡길 의향이 있는가?