

1. 정보 보안의 역사

■ 1980~1990년대

■ 네트워크 해킹의 시작

- 1980년대 초 네트워크 해커라는 개념이 처음 탄생
- '414 Gang'은 대표적인 네트워크 해킹 사건
 - 414 Gang: '414 Private'이라는 BBS의 일원들이 만든 해커 그룹으로 60개 컴퓨터 시스템에 침입하여 중요 파일을 삭제함
- 1981년에는 캡틴 잭이라는 별명을 가진 이언 머피가 AT&T의 컴퓨터 시스템에 침입하여 전화 요금을 조작

■ 정보 권리 논쟁의 시작

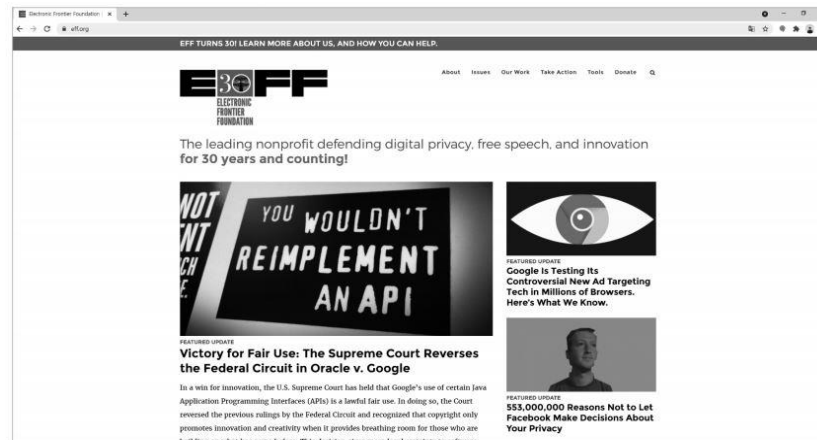
- 1981년 독일의 전설적인 해커 그룹인 카오스 컴퓨터 클럽(CCC)이 결성
- 카오스 컴퓨터 클럽의 설립 목표는 정보에 대한 자유로운 접근 권리를 공식적으로 주장
- 카오스 클럽은 소식지 창간호에서 설립 목표를 다음과 같이 규정
 - 정보 사회로 발전하려면 전 세계와 자유로운 커뮤니케이션을 가능케 하는 새로운 인권이 필요하다.
 - 인간 사회 및 개인에게 기술적 영향을 미치는 정보 교류에서 국경이 사라져야 한다.
 - 우리는 지식과 정보의 창조에 이바지할 것이다.

1. 정보 보안의 역사

■ 1980~1990년대

■ 해커의 등장

- 1980년대에 해킹이 발전하면서 역사적으로 유명한 해커들이 본격적으로 등장
 - 1986년 구소련 KGB로부터 자금을 지원받는 서독 해커들이 300여 기관에 불법적인 접근을 시도하고 군사 기밀 정보를 탈취
 - 1987년에는 **케빈 미트닉**이 컴퓨터 개발·판매 회사인 산타크루스 오퍼레이션의 시스템에 침입
 - 1988년 11월 22일 코넬대학 대학원생이었던 **로버트 모리스**는 웜 바이러스를 구동하여 미국 전역에 피해를 끼침
 - **로이드 블랭켄십**은 사이버 갱단 MoD의 멤버로 해킹과 프리킹에 관한 문서를 주고받는 장소인 Elite 보드를 운영
 - 로터스 123(스프레드시트 소프트웨어 개발 회사)을 개발한 미치 케이퍼와 존 발로는 정부의 임의적인 정보 검열에 저항해 전자프린티어 재단(EFF)을 결성
 - 전자프린티어재단은 국제 사회에서 표현의 자유, 저작물의 자유로운 이용, 개인 정보 보호, 정보 투명성을 위한 활동 수행

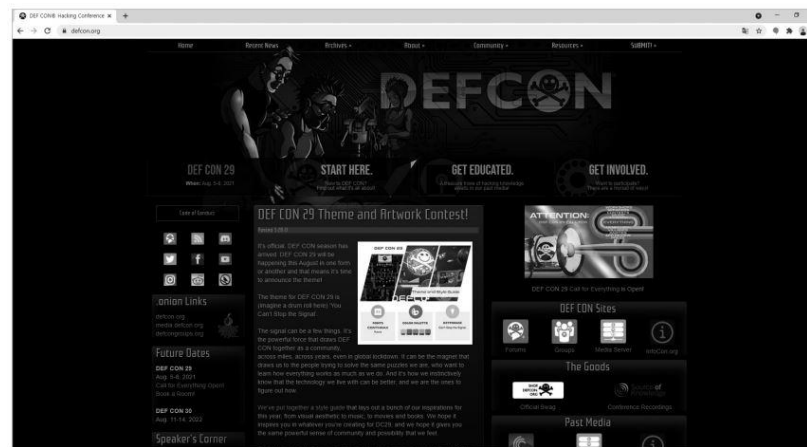


1. 정보 보안의 역사

■ 1980~1990년대

■ 데프콘 해킹 대회

- 최초의 해킹 대회인 '**데프콘**'이 1990년 라스베이거스에서 개최
- 데프콘 해킹 대회는 지금도 매년 열리는데, 팀 단위로 예선을 거쳐 여덟 팀이 라스베이거스에서 본선 진행
- 자신의 팀을 보호하면서 상대 팀을 공격하여 상대 시스템을 많이 해킹한 팀이 승리



데프콘 사이트(<http://www.defcon.org>)

■ 해킹 도구의 개발

- 1994년 인터넷 브라우저인 넷스케이프가 개발되어 웹 정보에 대한 접근이 가능해짐
- 해커들은 자신의 노하우와 프로그램을 BBS에서 웹 사이트로 옮기고 해킹 정보와 해킹 툴을 웹에서 공개
- 일부 사용자들은 해킹 툴을 사용하여 개인 정보를 캐기도 하고 은행 컴퓨터의 계좌 정보를 변조
 - 언론은 이들을 해커라 부르기 시작
- 이때부터 해커라는 용어가 순수한 목적으로 시스템 내부를 연구하는 컴퓨터광을 지칭하지 않게 됨

1. 정보 보안의 역사

■ 1980~1990년대

- 아메리카온라인 해킹
 - 1997년에 아메리카온라인(AOL) 침입만을 목적으로 고안된 무료 해킹 툴인 AOHell이 공개
 - 아메리카온라인(AOL): 미국의 인터넷 미디어 회사이자 PC통신 서비스 기업
 - AOHell은 초보 해커와 스크립트 키드가 사용하도록 개발된 것
 - 스크립트 키드: 정확히는 [해킹](#)에 대한 전문적인 지식이 없는데도 스스로 보안 전문가라고 주장하는 자
 - 이후 며칠 동안 초보 해커들이 악용하여 미국 내 수백만 명의 온라인 사용자가 대용량 메일 폭탄 공격을 받음
- 트로이 목마, 백 오리피스
 - 1998년에는 'CDC'라는 해킹 그룹이 데프콘 해킹 대회에서 트로이 목마 프로그램인 '백 오리피스'를 발표
 - The Analyzer라는 이스라엘의 10대 해커가 미국 펜타곤의 시스템에 침투해서 소프트웨어를 훔쳐낸 사건이 발생

1. 정보 보안의 역사

■ 2000년대 이후

■ 분산 서비스 거부 공격 (DDoS)

- 2000년 2월 인터넷에서 소통량이 많은 몇 개 사이트에 분산 서비스 거부(DDoS) 공격이 가해짐
- 이로 인해 야후, CNN, 아마존 등의 사이트가 ICMP 패킷을 이용한 스머프 공격으로 몇 시간 동안 마비
- 네트워크를 스캔한 후 취약한 서버에 trojans(트로이목마)라는 클라이언트 프로그램을 설치하여 정해진 시간에 목표 사이트에 수많은 패킷을 전송함으로써 사이트가 다운되도록 하는 공격

■ 웜과 바이러스

- 2000년에는 러브 버그바이러스가 등장하여 87억 5,000만 달러의 경제적 손실을 입힘
 - 바이러스 메일에는 "ILOVEYOU"라는 제목에 "발송드린 첨부 LOVELETTER를 확인 부탁드립니다"라는 내용의 본문 메시지와 'LOVELETTER.TXT.VBS'라는 파일이 첨부
 - 첨부 파일에 접근하면 다른 이메일 계정으로 메일이 복제 및 전송
 - 러브 버그는 감염된 컴퓨터의 파일을 삭제하거나 손상시키는 등의 악성 행동 수행. 특히, 특정 파일 형식(.jpg, .vbs 등)을 삭제
- 2003년 1월 마이크로소프트의 MS-SQL 2000 서버를 공격하는 슬래머 웜이 전국 네트워크를 마비시킨 사건 발생
 - UDP 포트 취약성: 공격의 주 대상이 된 DB용인 UDP 1434 포트는 외부에서 내부로 접속하기 위한 대문과 같은 역할을 하는 포트
- 2004년에는 베이글 웜, 마이둠 웜, 넷스카이 웜이라는 웜 삼총사가 등장

■ 개인 정보 유출과 도용

- 2005년~2006년 사이에 우리나라에서 주민 등록 번호 수십만 개가 유출되어 개인 정보가 무단 도용 사건 발생
- 사이버테러대응센터에서 접속 IP를 분석해보니 중국에서 직접 접속한 경우, 국내 사설망 등을 통해 접속한 경우, 해킹으로 중간 경유지를 이용한 경우 등이 원인으로 밝혀짐
- 2005년 11월에는 금융 정보를 이용하여 은행 계좌에서 잔고를 인출한 사건 발생

1. 정보 보안의 역사

■ 2000년대 이후

■ 전자 상거래 교란

- 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건이 발생
 - 범인들은 해킹으로 타인의 신용카드 번호를 입수한 후, 인터넷에서 이루어지는 신용카드 결제 방식의 제도적·기술적 취약점을 이용하여 물품을 대신 결제하고 현금을 돌려받아 수익 원을 인출(환불 또는 되팔기)
 - 대부분의 신용카드 사용자들이 일반 사이트, 쇼핑몰, 카드사 사이트의 접속 아이디와 비밀번호가 동일한 점에 착안한 범죄
 - 비록 잘못 입력하더라도 몇 번이고 다시 입력할 수 있는 점을 이용
- 2006년 3월에는 국내 대형 포털 사이트의 정보 검색 순위를 조작한 인터넷 광고 대행 업체의 대표가 입건
 - 국내 4개 대형 포털 사이트의 검색 순위에 업체의 홈페이지 주소를 상위에 노출시켜 주는 조건으로 광고주를 모집
 - 자체 개발한 프로그램을 이용하여 750개 회사의 홈페이지 주소를 자동으로 클릭하게 만들어 정보 검색 순위를 조작

■ APT 공격의 등장

- APT 공격(Advanced Persistent Threat): 고도화된 지속적 위협을 의미. 이는 특정 목표를 가진 공격자가 조직이나 개인에 대해 장기간에 걸쳐 은밀하게 공격하는 것 - 장시간에 걸쳐 사이트의 취약점을 분석하고 다양한 해킹기법을 사용
- 2008년 해커 8명으로 구성된 캐시어가 영국 RBS 은행의 월드페이 시스템에 침입하여 복제 카드를 제작
- 신용카드의 한도를 올리고 12시간 동안 세계 49개 도시의 2,100개 ATM 기기에서 약 950만 달러를 인출
- 이 해킹 사건을 최초의 APT(지능적 지속 위협) 공격으로 흔히 언급

1. 정보 보안의 역사

■ 2000년대 이후

■ 농협 사이버 테러

- 2011년 4월 대규모 데이터 삭제로 농협의 전산 시스템이 멈추는 사건이 발생
- 정부는 이를 북한의 사이버 테러라고 발표
- 이 사건은 국내 기업의 보안 인식 자체를 바꿔 놓는 계기가 됨

■ 스마트폰 해킹

- 대표적인 스마트폰 운영체제인 애플의 iOS와 구글의 안드로이드는 모두 유닉스(리눅스)와 유사
- 리눅스에 기반을 둔 안드로이드에는 리눅스 해킹툴을 비교적 쉽게 설치할 수 있음
- 스마트폰은 긴 시간 동안 전원 공급이 가능하고 와이파이, 3G 망, LTE 망도 이용 가능한 최고의 해킹 도구
 - 스마트폰에 무선 랜 해킹 도구를 설치하고 택배 상자에 넣어 공격 대상 회사로 보내 무선 네트워크를 해킹하는 방식

■ 가상 화폐 해킹

- 현재 가상 화폐는 큰 돈이 되고 있기 때문에 관련 해킹 사건도 증가

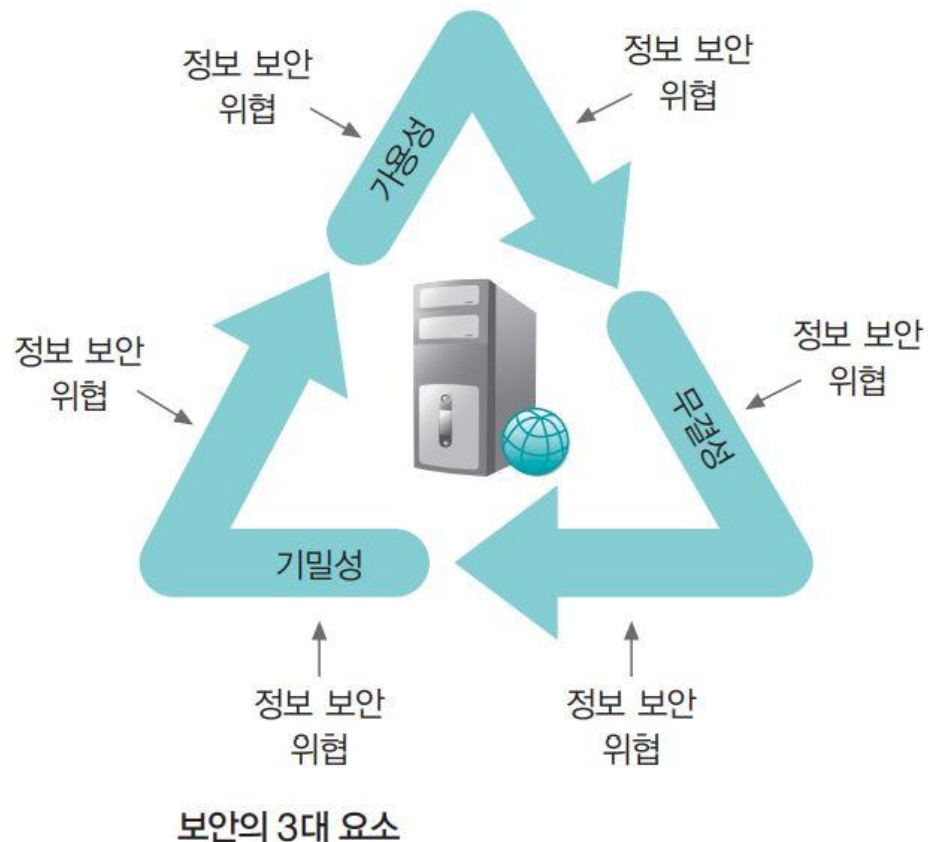
가상 화폐 해킹 사례

발생 시기	거래소 명	피해 원인	피해 규모
2019년 11월	업비트	핫월렛 해킹	580억 원
2018년 6월	빗썸	이메일 악성 코드 추정	350억 원
2018년 6월	코인레이	이메일 악성 코드 추정	400억 원
2017년 12월	유빗(구 아피존)	핫월렛해킹	172억 원

2. 정보 보안의 이해

■ 보안의 3대 요소

- 보안은 기밀성, 무결성, 가용성이라는 세 가지 속성으로 집약



2. 정보 보안의 이해

■ 보안의 3대 요소

■ 기밀성(Confidentiality)

- 인가된 사용자만 **정보 자산에 접근**할 수 있다는 것으로, 일반적인 보안의 의미와 가장 가까움
- 허가되지 않은 사람 (비인가자)이 정보에 접근하는 것을 막는 자물쇠
- 보안과 관련 된 많은 시스템과 소프트웨어는 기밀성과 밀접한 관련이 있음
- 방화벽, 암호, 패스워드 등은 기밀성의 대표적인 예

■ 무결성(Integrity)

- 적절한 권한을 가진 사용자가 인가한 방법으로만 **정보를 변경**할 수 있도록 하는 것
- 무결성은 일상생활에서 중요하게 작용
 - 예시) 지폐의 경우
 - 오직 정부(적절한 권한을 가진 사용자)만이 한국은행을 통해 (인가된 방법으로만) 지폐를 만들거나 바꿀 수 있음
 - 이런 조건이 갖추어지지 않은 상태로 만든 지폐라면(무결성이 훼손된 경우) 위조지폐로 취급되어 엄중한 법의 처벌을 받음
- 흔히 보안의 첫 번째 요소로 기밀성을 말하지만, 경우에 따라서는 무결성을 우선으로 둘 수 도 있음

■ 가용성(Availability)

- **필요한 시점**에 정보 자산에 대한 접근이 가능하도록 하는 것을 의미
- 일상생활에서 가용성을 상품화한 대표적인 예로는 24시간 편의점
- 현대 사회에서 정보의 가용성이 훼손되는 것은 필수 불가결한 요소의 가용성이 훼손되는 것과 마찬가지로

2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

■ 사이버 범죄의 유형

- 사이버 테러형 범죄는 해커 수준의 범죄를, 일반 사이버 범죄는 인터넷을 이용한 일반인 수준의 범죄
- 정보 통신망 침해 범죄는 27%, 정보 통신망 이용 범죄는 73%, 불법 콘텐츠 범죄는 67%의 검거율
- 해킹이 점점 교묘해져서 추적하기가 어렵기 때문에 검거율이 점점 낮아지는 추세

사이버 범죄의 유형

구분	설명
사이버 테러형 범죄	정보 통신망 자체를 공격 대상으로 한다. 해킹, 바이러스 유포, 메일 폭탄, 서비스 거부(DoS) 공격 등 전자기적 침해 장비를 이용하여 컴퓨터 시스템과 정보 통신망을 공격하는 불법 행위다.
일반 사이버 범죄	사이버 공간을 이용한 일반적인 불법 행위로 사이버 도박, 사이버 스토킹, 사이버 성폭력, 사이버 명예 훼손, 사이버 협박, 전자 상거래 사기, 개인 정보 유출 등의 행위를 가리킨다.

■ 윤리 의식

- 윤리 강령
 - 보안이나 해킹과 관련된 기술을 배워 좋은 곳에 활용하는 전문가가 되기를 바라는 목적

정보통신 윤리 강령

- 우리는 타인의 자유와 권리를 존중한다.
- 우리는 바른 언어를 사용하고 예절을 지킨다.
- 우리는 건전하고 유익한 정보를 제공하고 올바르게 이용한다.
- 우리는 청소년 성장과 발전에 도움이 되도록 노력한다.
- 우리 모두는 따뜻한 디지털 세상을 만들기 위하여 서로 협력한다.

2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

■ 윤리 의식

• 정보통신망 이용촉진 및 정보보호 등에 관한 법률

- 정보통신과 관련된 가장 광범위한 법률로 안전한 정보통신망 환경을 조성하는 것이 목적
- 정보통신 서비스 사업자와 관련된 내용 포함
- 개인정보 보호와 관련된 내용 포함

조항	내용
제70조 제1항	사이버 명예 훼손(사실 유포) 시 3년 이하 징역 또는 3천만 원 이하 벌금
제70조 제2항	사이버 명예 훼손(허위 사실 유포) 시 7년 이하 징역, 10년 이하 자격 정지 또는 5천만 원 이하 벌금
제71조 제1항	다음 각 호의 하나에 해당하는 자는 5년 이하 징역 또는 5천만 원 이하 벌금 • 제1호: 이용자의 동의 없이 개인 정보를 수집한 자 • 제3호: 개인 정보를 목적 외에 이용한 자 및 제3자에게 제공하거나 제공받은 자 • 제5호: 이용자의 개인 정보를 훼손·침해·누설한 자 • 제9호: 정보통신망에 침입한 자 • 제10호: 정보통신망에 장애가 발생하게 한 자 • 제11호: 타인의 정보를 훼손한 자 및 타인의 비밀을 침해·도용·누설한 자
제72조 제1항	다음 각 호의 하나에 해당하는 자는 3년 이하 징역 또는 3천만 원 이하 벌금 • 제2호: 속이는 행위에 의해 개인 정보를 수집한 자 • 제5호: 직무상 비밀을 누설한 자 및 목적 외에 사용한 자
제73조	다음 각 호의 하나에 해당하는 자는 2년 이하 징역 또는 2천만 원 이하 벌금 • 제1호: 기술적·관리적 조치 미이행으로 개인 정보를 분실·도난·유출·위조·변조·훼손한 정보통신 서비스 제공자 • 제2호: 청소년 유해 매체물임을 표시하지 않고 영리 목적으로 제공한 자 • 제3호: 청소년 유해 매체물 광고를 청소년에게 전송·공개한 자
제74조 제1항	다음 각 호의 하나에 해당하는 자는 1년 이하 징역 또는 1천만 원 이하 벌금 • 제1호: 표준화 및 인증을 위반한 제품을 표시·판매·진열한 자 • 제2호: 음란한 부호·문언·음향·영상 등을 배포·판매·임대·전시한 자 • 제3호: 공포와 불안을 유발하는 부호·문언·음향·화상·영상을 반복한 자 • 제4호: 사전 동의를 받지 않고 영리 목적의 광고성 정보를 전송한 자 • 제6호: 불법 행위를 위한 광고성 정보를 전송한 자

2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

■ 윤리 의식

• 정보통신기반 보호법

- ISP (인터넷 서비스 사업자)나 통신사와 같은 주요 정보 통신 기반 시설에 대한 보호법
- 주요 정보 통신 기반 시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억 원 이하의 벌금에 처하는 것으로 규정

• 클라우드컴퓨팅법

- 일반화되고 있는 클라우드 환경과 관련한 서비스를 안전하게 이용할 수 있는 환경을 조성하기 위한 법률
- 이용자의 동의 없이 이용자 정보를 이용하거나 제삼자에게 제공한 자 및 이용자의 동의 없음을 알면서도 영리 또는 부정한 목적으로 이용자 정보를 제공받은 자는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처함

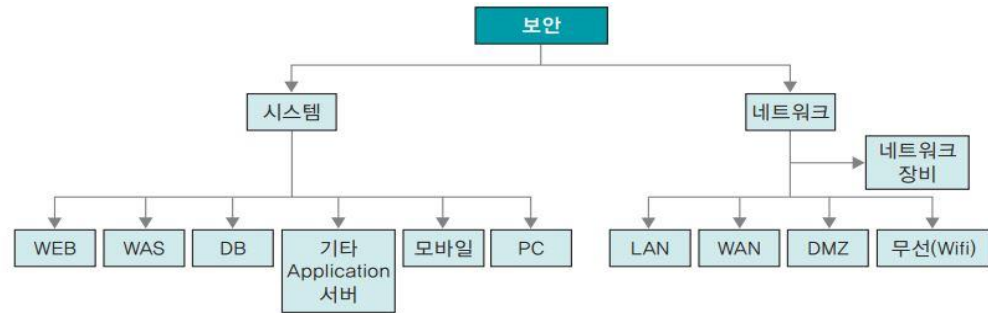
• 전자정부법

- 많은 공공 데이터를 생성·관리하는 전자정부를 보호하기 위한 법
- 행정 정보를 위조·변경·훼손하거나 말소하는 행위를 한 사람은 10년 이하의 징역에 처함
- 행정 정보 공동 이용을 위한 정보 시스템을 정당한 이유 없이 위조·변경·훼손하거나 이용한 자, 행정 정보를 변경하거나 말소하는 방법 및 프로그램을 공개·유포하는 행위를 한 자는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처함

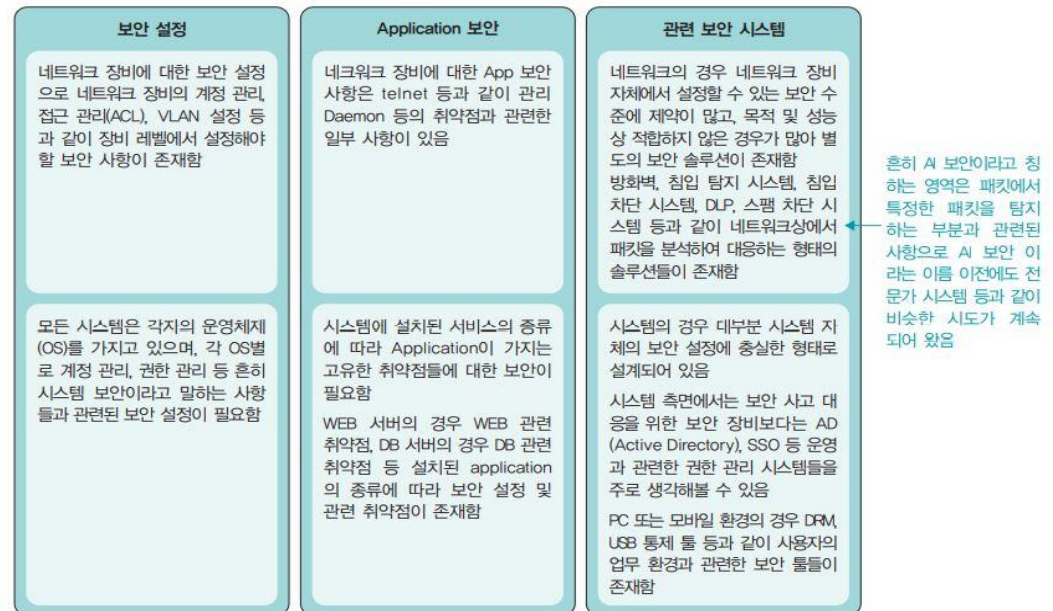
2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

- 다양한 분야의 지식
 - 보안 전문가가 알아야 할 지식



(a) 보안의 대상(객체)



(b) 보안 사항

2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

■ 다양한 분야의 지식

- 운영체제
 - 운영체제 운영체제에는 윈도우, 유닉스, 리눅스, 맥 OS 등이 있음
 - 실무적으로 가장 중요한 운영체제는 가장 많이 사용되고 있는 윈도우
 - 리눅스는 유닉스와 비슷한 환경을 제공하면서도 쉽게 구할 수 있고, 소스가 공개되어 있어 자유롭게 배우기 좋은 운영체제
- 네트워크
 - 네트워크는 하나의 시스템에서 데이터를 처리한 뒤 다른 시스템으로 전달하는 일종의 '길' 과 같은 역할 수행
 - 1973년에 만들어진 TCP/IP는 지금도 네트워크의 기본이 되는 프로토콜로서 매우 중요
- 프로그래밍
 - 기본적인 C 프로그래밍과 객체 지향 프로그래밍에 대한 이해, HTML에 대한 이해가 필요
 - 자신만의 해킹 툴이나 보안 툴을 만들고자 한다면 C 언어를 충분히 알아야 함
 - 최근에는 파이썬을 기반으로 해킹 툴이나 보안 툴이 대세임
- 서버
 - 보안전문가는 기업이 안전하고 신뢰할 수 있는 서비스를 제공하도록 서버를 운용하기 위해 서버에 대한 이해가 필요
 - 데이터베이스의 경우 기본적인 SQL 지식이 필요

2. 정보 보안의 이해

■ 보안 전문가의 자격 요건

■ 다양한 분야의 지식

• 보안 솔루션

- 보안 솔루션의 경우 시스템 별 기본 보안 통제와 적용 원리, 네트워크 상의 구성과 목적 등을 이해
- XDR (Extended Detection and Response): 여러 보안 제품에서 수집된 데이터를 통합하여 위협을 탐지하고 대응하는 솔루션. 안랩의 XDR은 조직 내 보안 위협 리스크를 관리
- SIEM (Security Information and Event Management): 보안 이벤트를 실시간으로 모니터링하고 분석하여 위협을 탐지하는 시스템. 로그 수집 및 분석 기능을 통해 보안 사고를 예방
- EDR (Endpoint Detection and Response): 엔드포인트에서 발생하는 보안 위협을 탐지하고 대응하는 솔루션으로, 악성코드 및 비정상적인 활동을 실시간으로 감지

• 모니터링 시스템

- 네트워크 관리 시스템 (NMS), 네트워크 트래픽 모니터링 시스템 (MRTG)과 같은 모니터링 시스템의 기본 개념을 인지
- 암호와 해시의 차이, 대칭 키 알고리즘 및 비대칭 키 알고리즘의 종류와 강도, 공개 키 기반 구조를 파악

• 정책과 절차

- 보안 정책과 해당 기업의 핵심적인 업무 프로세스를 잘 이해하고 있어야 함
- 보안 거버넌스: '조직의 보안을 달성하기 위한 구성원 간의 지배 구조' / 보안 정책에서 가장 핵심적인 요소