1주차: 정보 보안의 세계

ChulSoo Park

School of Computer Engineering & Information Technology

Korea National University of Transportation

E-Mail : pcs8321@naver.com

박 철 수 대한민국산업현장 교수(정보통신 분야) / 공학박사

❖ 경력

2019~현재 한국정보통신기술사협회 사업단장
2017~현재 대한민국산업현장교수(정보통신, 고용노동부)
2022~현재 중소벤처기업부 정보화 지원단
2019~현재 한국창의재단(과학기술정보통신부) 컨설턴트
2020~현재 고경력 과학기술인(과학기술정보통신부)
2019~현재 스마트팩토리,스마트팜, 스마트서비스 컨설턴트
2018~현재 국가기술자격 정책 심의 위원(과학기술정보통신부)
2018~2018 대학생 ICT분야 멘토(과학기술정보통신부)
1987~2020 농협/ 정보관리(보안)최고책임자(CIO/CISO), 임원

❖ 학력

2011~2016 서울과학기술대학교 공학박사

❖ 저서

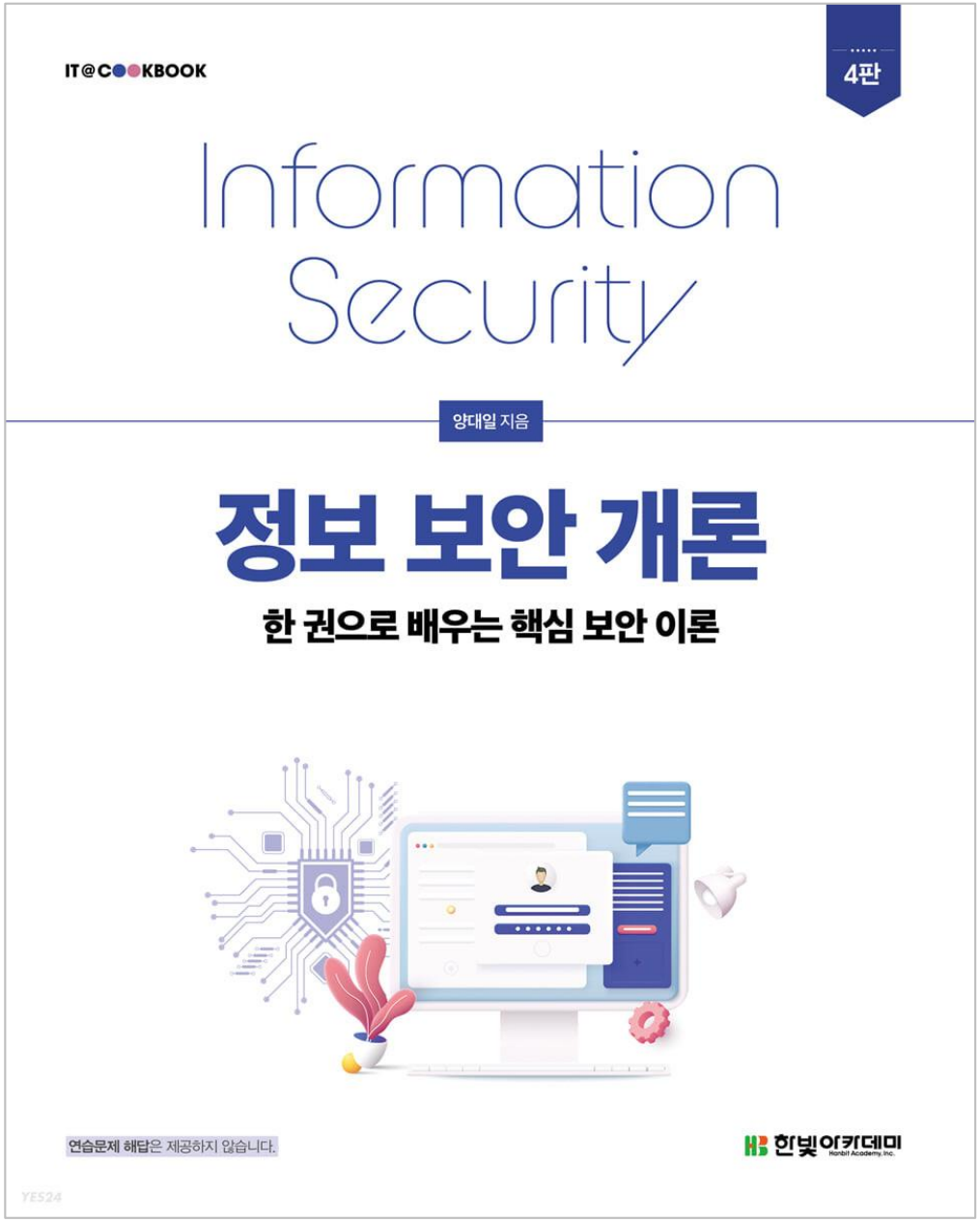
2019년 NCS학습모듈(빅데이터,인공지능 4권 집필 책임)
2020년 NCS학습모듈(지능형영상정보처리,생체인식 2권 집필 책임)
2021년 NCS학습모듈(인공지능,커넥티드카 등 5권 집필 책임)

주교재 소개

저　자 : 양대일

출판사 : 한빛아카데미

발행일 : 2021.06

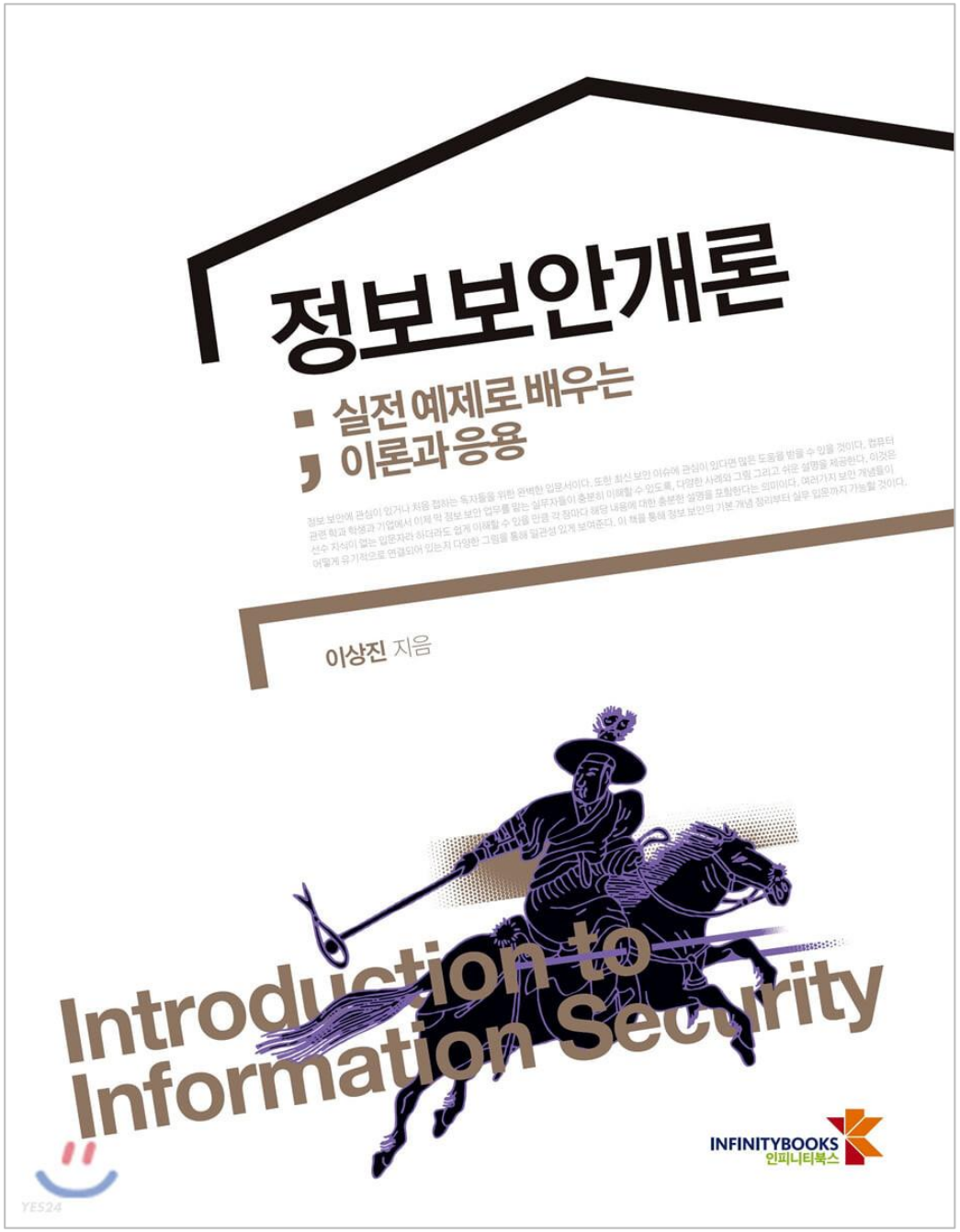


부교재 소개

저　자 : 이상진

출판사 : 인피니티북스

발행일 2021.8



학습목표 (교과목)

정보보안에 대한 전반적인 개념의 이해 및 시스템 보안, 네트워크 보안, 악성코드, 웹 보안, 소프트웨어 보안, 정보보호 정책 및 법 제도, 보안 관리 등의 주요 용어, 개념 등 기본 기술을 중심으로 학습함으로써, ICT 분야의 정보를 보호하기 위한 **소프트웨어 개발자 측면에서 정보보안 기본 지식을 습득**한다.

강의 계획표

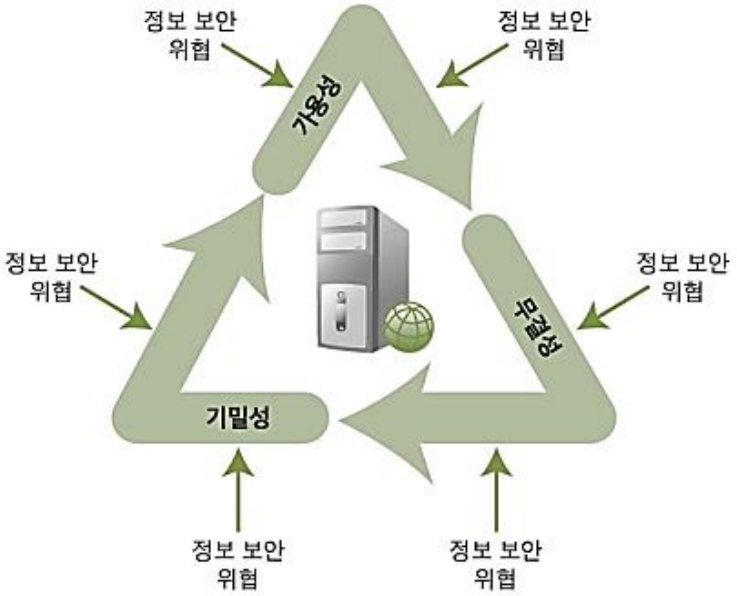
주차	교재	주제
1	1장	정보 보안의 세계
2	2장	시스템 보안
3	3장	네트워크 보안
4	4장	웹 보안
5	5장	코드 보안
6	6장	악성 코드
7	7장	암호의 이해
8		중간고사(30%)
9	8장	전자 상거래 보안
10	9장	보안 시스템
11	10장	IoT보안과 AI보안
12	11장	침해 대응과 디지털 포렌식
13	12장	사회 공학
14	13장	보안 관리
15		보강 주간
16		기말고사(40%)

학습목표 (1주차)

- 시대별 정보 보안의 역사 파악
- 보안의 3대 요소를 이해
- 보안 전문가가 갖춰야 할 자격 요건을 파악
- 보안 관련 법률 학습
- 4차 산업혁명 시대에 개발자로 정보보안의 중요성 인식

01 CHAPTER

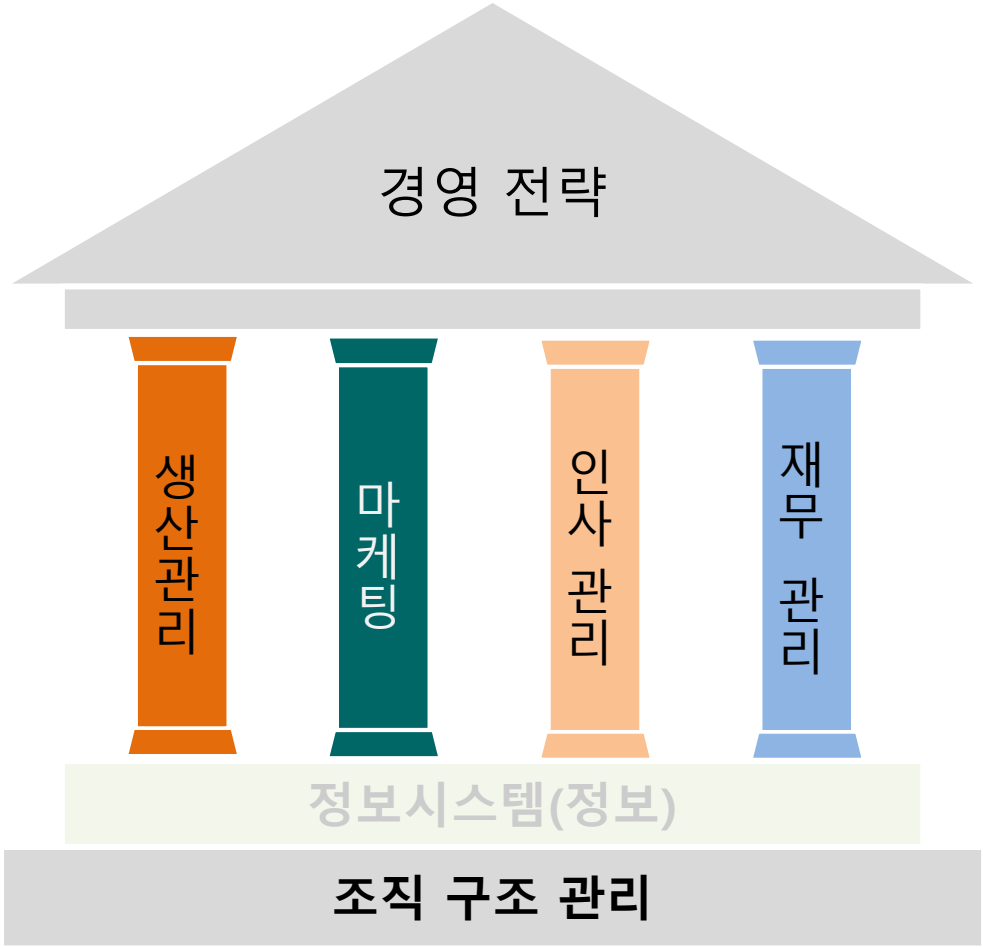
정보 보안의 세계



CONTENTS

Orientation

기업 경영의 2가지 기반과 4가지 기둥



사람(Man),
돈(Money),
물자(Material),
정보와 전략

출처 : 한영석 교수, 전략 경영

[유통가 해킹 전쟁]① “500억 내놔” 이랜드 협박사건...샤넬·풀무원도 뚫렸다.

출처 : https://biz.chosun.com/distribution/channel/2021/08/27/KCWPF4II5BFILNF6WKP6XNQLWU/

[유통가 해킹 전쟁]① “500억 내놔” 이랜드 협 풀무원도 뚫렸다

국제 해커조직, 개인정보 인질 삼아 몸값 요구
유통기업 겨냥한 사이버 공격 지속
결제단말기 등 통신장비 보안 취약…카드 정보 줄줄 샌다
“해킹 피해 숨기지 말고, 보안 시스템 투자 늘려야”

윤희훈 기자

입력 2021.08.27 06:00

[편집자주] 유통가를 향한 해커들의 공격이 계속 되고 있다. 이달 초 샤넬코리아 데이터베이스가 공격을 받아 주요 고객들의 정보가 유출됐다. 이랜드는 지난해 해커 그룹의 공격을 받은 뒤, 이들로부터 거액의 몸값을 요구 받았다. 정보가 자원인 지금, 방대한 양의 고객 정보를 보유한 유통기업은 해커 집단의 주요 타깃이 되고 있다. 해커가 흔드는 유통가의 현실과 대책을 3편에 거쳐 알아본다.

디도스, 랜섬웨어 등 사이버 테러는 이제 기업의 생존을 위협하는 최대 위협으로 부상했다.

2020년 11월 국제 해커 조직이 이랜드를 공격해 탈취한 정보를 공개하겠다고 협박하며 4000만달러(한화 약 500억원)를 요구하는 사건이 발생했다. 해커 조직이 기업의

자율주행차 서비스에서의 보안위협과 보안

KISA 발표 '자율주행차 서비스 보안모델' 꼼꼼히 살펴보니 자율주행차 서비스 구간별 보안위협과 대응 가능한 보안기술 제시

.....이에 따라 무인 셔틀, 주차, 배송 등 자율주행차를 활용한 서비스 모델이 활발하게 개발되고 있는데, 이러한 서비스들은 자동차, 인프라, 통신, 전자, ICT 등이 융합되어 시너지를 발휘하고 있다. 하지만 **이런 융합으로 인해 기존 ICT 환경에서 발생했던 사이버 공격들이 자동차 환경으로 전이되고 있다.**

상암DMC 누비는 자율주행택시, 2022년 2월10일부터 누구나 탈 수 있다.(2,000원)

https://www.boannews.com/media/view.asp?idx=95018

중앙연구소 ECM(문서중앙화)시스템 장애 발생 및 업무 지원 보고

구 분	내 용
보고내용	1. 시간대별 현황 : 2019.05.28

시간	내용	비고
11:50	서버파일 이상징후 발견 및 관리자 알림 랜섬웨어 감염 추정	연구지원팀 신동화과장
12:00	유지보수 업체 연락 전체 PC 랜선 분리	비오엠네트웍스 자체조치
13:00	중앙연구소 신고 접수	박성현차장
14:00	유지보수 업체 원격 지원 -> 현황 파악 및 복구 방법 검토	비오엠네트웍스 최백길팀장
15:00	중앙연구소 도착 및 전체 PC 점검 증별 스위치 파워 OFF	현장 도착
16:00~17:30	유지보수 업체 중앙연구소 이동	비오엠네트웍스 최백길팀장
17:30~	복구 작업 진행	

2. 중앙연구소 PC 작업

가. 조합 PC 유지보수 업체(유엔터스)통한 전체 PC 포맷

전체대수 : 41 대

나. 랜선 접속

다. 문서중앙화 접속

3. 문서 파일 복구작업

가. 백업 데이터 복구 : 2019.05.25 가능

나. 랜섬웨어 복구 업체 통한 복호화 키 요청

다. 복호화 키 통한 복구 작업

1) ECM(문서중앙화)암호화 -> 복호화 작업

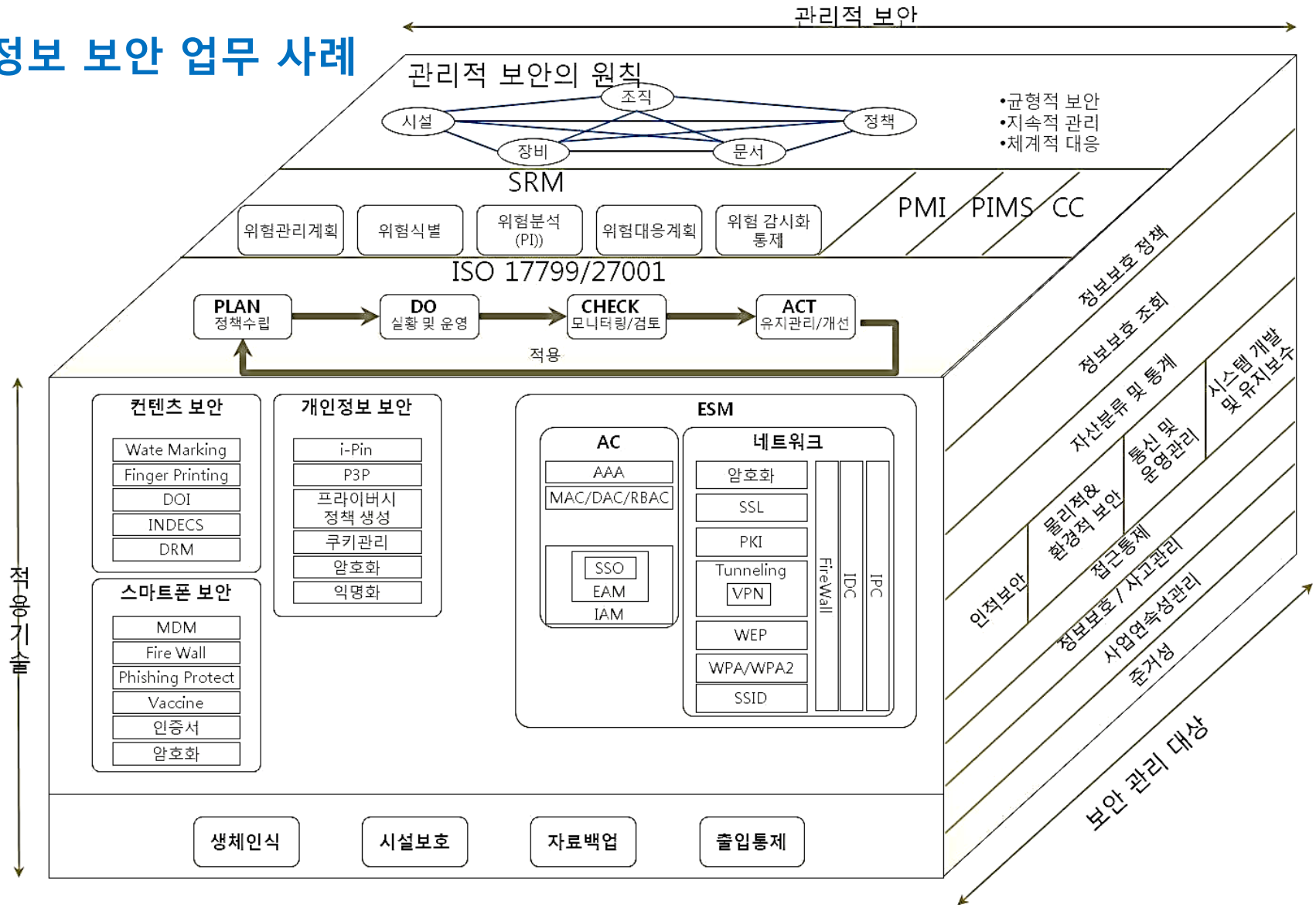
2) 랜섬웨어 복호화 작업

원 인	중앙연구소 PC 랜섬웨어 감염 -> ECM(문서중앙화)시스템내 문서 파일 감염
조치사항	1. PC 랜선제거 2. 각 증별 스위치 OFF 3. 파일 복구 작업 진행
조치일시	1. 사전조치 : 5.28(화) 23:30 2. PC 포맷 : 5.29(수) 3. 문서 복구 예정 : 5.30(목) 약 48 시간
비 용	
향후계획	1. 감염 경로 파악 2. 백업 복구 프로세스 점검 3. 랜섬웨어 솔루션 검토

정보 보안 업무 사례

Orientation

정보 보안 업무 사례



Orientation

구성요소	설명	대표사례
관리적 보안	- 인적 자산에 대한 보안 - 관리적 보안대책은 각종관리 절차 및 규정을 의미 - 조직 내부의 정보 보호 체계를 정립하고, 인원을 관리하고, 정보 시스템의 이용 및 관리에 대한 절차를 수립하고, 비상 사태 발생을 대비하여 계획을 수립하는 등의 대책을 포함	**보안정책** / 절차관리, 보안조직구성 및 운영, 인력 **보안 관리,** 보안 감사, 보안 사고 조사
물리적 보안	- 설비 / 시설 자산에 대한 보안 - 물리적 보안대책은 각종 물리적 위협으로부터 보호하는 것을 의미 - 일반적으로 정보 시스템을 구성하는 정보 자산에 가해질 수 있는 피해를 최소화하기 위한 물리적 대책으로 구성 - 비인가자 접근 통제, 주요 시설물 설계 등 정보 시스템에 관련된 전반적인 대책을 포함	사업장 출입 관리, 주요시설(서버실)관리, **자료 백업,** 자산 반출입 관리
기술적 보안	- 정보자산에 대한 보안 - 기술적 보안대책은 실제 정보 시스템에 적용된 기술에 특화하여 기술적으로 마련할 수 있는 정보 보호 대책을 의미 - 물리적 보안을 수행 할 수 있도록 하는 모든 기반 기술(ex : 지문인식 시스템, 카드출입 시스템, 데이터 **암호화** 기술 등) 및 정보화 역기능(해킹, 스팸메일, Phishing, Pharming 등)에 대한 탐지 기술, 예방 기술, 조치 기술 등의 보안 기술	**네트워크 보안,** **시스템 보안,** **어플리케이션 보안,** **데이터베이스 보안,** **PC 보안**

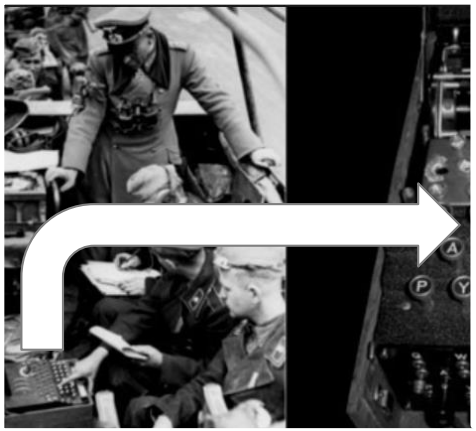
1. 정보 보안의 역사

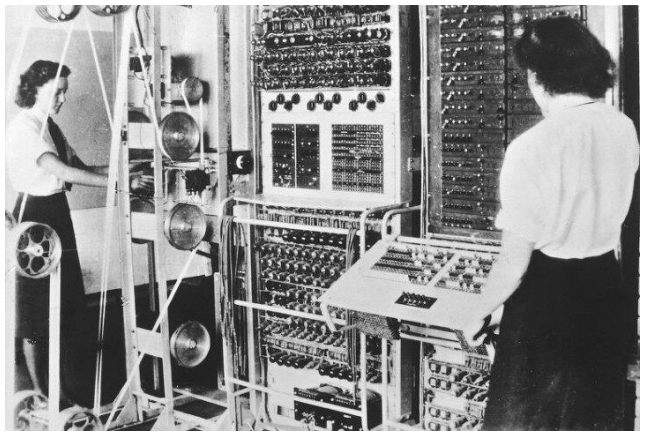
1 1950년 이전

1. 정보 보안의 역사

▪ 에니그마와 콜로서스

- ✓ **1918년 폴란드의 암호 보안 전문가**들이 개발한 평문 메시지를 암호화된 메시지로 변환하는 장치, 은행의 통신 보안 강화를 위해 개발(**에니그마(Enigma)**)
- ✓ 제2차 세계대전(1939.9.1~1945.9.2)에서 독일군의 군사 통신 보안용으로 사용
- ✓ 문자판의 키 하나를 누르면 나란히 원판 3개가 회전하면서 복잡한 암호가 만들어짐
- ✓ 에니그마를 해독한 것은 영국의 앨런 튜링이 만든 최초의 컴퓨터인 **콜로서스(1943년)**
- ✓ 해석된 메시지를 1초에 약 5,000자 정도로 종이테이프에 천공할 수 있었으며, 천공된 암호문이 에니그마의 암호와 일치 할 때까지 비교하는 방식으로 해독



1. 정보 보안의 역사

해킹의 태동기(1970년대까지)

- **최초의 컴퓨터 연동망 ARPA(The Advanced research Project Agency)**
  - ✓ **1967년** 미국 국방부는 관련 기관 사이의 정보 공유를 지원하는 ARPA 프로젝트를 통해 컴퓨터 연결망을 개발
  - ✓ IMPS(Interface Message Processors) **네트워크**라고 불린 이 연동망은 오늘날 인터넷의 뿌리
- **유닉스 운영체제와 C 언어 개발**
  - ✓ **1969년** 켄 톰프슨과 데니스 는 운영체제인 유닉스(UNIX)와 C언어를 개발
  - ✓ 개발자 툴 및 컴파일러에 **접근**하기가 쉽고 여러 사용자가 동시에 사용할 수 있다는 특성 **(해커 친화적)**
- **최초의 이메일 전송**
  - ✓ 1971년 레이먼드 톰린슨은 최초의 이메일 프로그램을 개발
  - ✓ 64노드의 아르파넷에서 @을 사용한 최초의 이메일을 발송

1. 정보 보안의 역사

▪ 마이크로소프트 설립

- ✓ 1974년 MITS사가 세계 최초로 조립식 개인용 컴퓨터 앨테어 8800를 만들어 판매
- ✓ **1975년 빌 게이츠(하버드 법학) 마이크로소프트를 설립**
- ✓ 1981년 컴퓨터 전시회에서 빌 게이츠는 당시 막 발매된 IBM PC의 메모리가 640KB로 제한된 것을 옹호하는 의미에서 "640KB면 누구에게나 충분하다".

▪ 애플 컴퓨터의 탄생

- ✓ **1979년 애플 컴퓨터가 스티브 워즈니악과 스티브 잡스의 손에 탄생**
- ✓ 오늘날의 PC와 비슷한 모습의 애플 컴퓨터는 그 당시에 666달러 66센트라는 가격에 판매, 데스크톱 PC가 보급과 함께 원격으로 시스템을 해킹
- ✓ 1985년 CEO 존 스킬러에 의해 회사에서 퇴출(상식 이상의 괴짜스런 행동)

1. 정보 보안의 역사

스티브잡스의 창조신화의 비밀

Harvard Business Review

Article at a Glance

애플은 아이맥(iMac), 아이팟(iPod), 아이팟 나노(iPod nano), 아이튠즈 스토어(iTunes Store), 애플 스토어(Apple Stores), 맥북(MacBook), 아이폰(iPhone), 아이패드(iPad) 등 기존의 기업과는 다른 혁신적인 제품을 선보였다. 이런 성공을 가능케 했던 핵심 요인은 스티브 잡스의 리더십에서 비롯된다. 하지만 그의 리더십은 기존의 경영대학원에서 가르쳤던 CEO의 성공요인과는 다르다.

①집중하라 ②단순화하라 ③처음부터 끝까지 책임져라 ④뒤처졌을 땐 뛰어넘어라
⑤이윤보다 제품을 중시하라 ⑥포커스 그룹의 노예가 되지 말라
⑦현실을 왜곡하라 ⑧강인한 인상을 남겨라 ⑨완벽을 위해 끊임없이 노력하라
⑩오직 최고의 인재만 용인하라 ⑪직접 대면하라 ⑫큰 그림과 세부 사항을 두루 섭렵하라
⑬과학에 인문학을 더하라 ⑭항상 갈망하고 우직하게 살아라

https://dbr.donga.com/article/view/1401/article_no/5378/ac/magazine

1. 정보 보안의 역사

▪ 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 컴퓨터에 침입하여 중요 파일을 삭제함**
- ✓ **1981년에는** 캡틴 잽 이라는 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 권리 주장**
- ✓ 카오스 클럽은 소식지 창간호에서 설립 목표를 다음과 같이 규정
  - 정보 사회로 가려면 전 세계와 자유로운 커뮤니케이션 위한 새로운 인권이 필요.
  - 인간 사회 및 개인에게 기술적 영향을 미치는 정보 교류에서 국경이 사라져야 함.
  - 우리는 지식과 정보의 창조에 이바지할 것이다.

1. 정보 보안의 역사

- **데프콘 해킹 대회**
  - ✓ 최초의 해킹 대회인 '데프콘'이 1990년 라스베이거스에서 개최, 지금도 열리 대회
  - ✓ 자신의 팀을 보호하면서 상대 팀을 공격하여 상대 시스템을 많이 해킹한 팀이 승리

- **아메리카 온라인 해킹**
  - ✓ 1997년에 아메리카온라인(AOL)침입만을 목적으
    이 공개
  - ✓ AOHell은 초보 해커와 스크립트 키드가 사용하
    보 해커들이 악용하여 미국 내 수백만 명의 온라
    격을 받음


KAIST·POSTECH, 이공계 최고는 어디?…학생대제전 개최

이성현 기자 | 승인 2021.09.24 09:27 | 댓글 0

24일 KAIST에서 개막, 1박 2일간 5개 종목에서 승부 겨뤄

제2회 사이버 이공계 학생교류전 로고

카포전 혹은 포카전으로 불리는 한국과학기술원(KAIST)·포항공대(POSTECH) 학생대제전이 막을 올린다.

KAIST는 24일 POSTECH과 제2회 사이버 이공계 학생교류전을 이틀간 개최한다고 밝혔다.

두 학교는 지난 2002년부터 매년 대전과 포항을 벌갈아 오가는 종합 교류전을 개최해왔다. 지난해부턴 코로나19 상황으로 고려해 비대면 온라인 교류전으로 대체해 진행하고 있다.

올해는 해킹, 인공지능 경연대회, 과학퀴즈 등 과학경기 3종목이 진행되며 야구·축구·농구 등 대면 교류전에서 진행해오던 구기 종목을 대신해 리그 오브 레전드, 카트라이더 등 e-스포츠 경기 2종목을 추가해 총 5종목에서 실력을 겨룬다.

- **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

보안에 대한 중요성 인지 시기

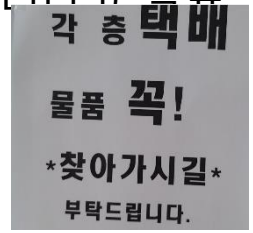
- **분산 서비스 거부 공격(DDoS, Distributed Denial of Service) : CNN,아마존**
- **웜과 바이러스 : ILOVEYOU(2000년대)**
- **개인정보 유출과 도용**
- **전자 상거래 교란**
  - ✓ 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건이 발생
  - ✓ 범인들은 해킹으로 타인의 **신용카드 번호를 입수한 후 신용카드 결제**
  - ✓ 국내 4개 대형 포털 사이트의 검색 순위에 업체의 홈페이지 주소를 상위에 노출시켜 주는 **정보 검색 순위를 조작**
- **APT(Advanced Persistent Threat) 공격의 등장**
  - ✓ 2008년 다국적 해커 8명으로 구성된 캐시어(Cashier)가 영국 RBS 은행의 월드페이 시스템에 침입하여 복제 카드를 제작, 세계 49개 도시의 2,100개 ATM 기기에서 약 950만 달러를 인출,이 해킹 사건을 최초의 APT(지능적 지속 위협) 공격으로 흔히 언급
  - ✓ **APT 공격: 오랜 시간을 들여 사이트를 분석하고 취약점을 찾아내어 해킹하는 경우를 APT 공격이라고 함**

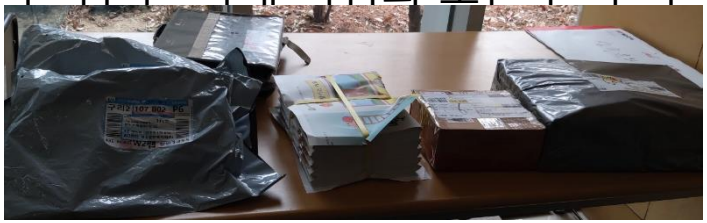
1. 정보 보안의 역사

▪ 농협 사이버 테러

✓ 2011년 4월 대규모 데이터 삭제로 **농협의 전산 시스템이 멈추는 사건**이 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

표 1-1 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	코인레일	이메일 악성 코드 추정	400억 원
2017년 12월	유빗(구 야피존)	핫월렛해킹	172억 원

1. 정보 보안의 역사

4 2000년대 이후

원전 인터넷망 해킹 10년간 1,463건 발생

김병욱 기자 |

양정숙 의원,

[투데이에너지

하다는 지적이

국회 과학기술

난 2012년부터

다.

같은 기간 동안

장 많았으며 이

서비스 거부 공

'해킹이 국가 재난 될 수 있다' 인도 핵발전소 해킹 사건의 전말

J.M. Porup | CSO

민간 기반시설 공

는 민간 핵발전소

하는 동안 파괴 공

다음은 인도의 쿠

했으며 어떻게 쉽

KNPP 해킹 사건

소식이 알려진 것

Express)에 따르

터 수립에 중요한

'랜섬웨어 먹잇감 스마트팩토리' 구출 위해 IT-OT업계 손잡고 보안 강화

고명훈 기자 | 승인 2021.06.23 16:49 | 댓글 0

-LG CNS, 이글루시큐리티와 MOU...양사 축적한 고급 보안 솔루션 결합 기대
-'글로벌 CDA 선정' 포스코ICT, 업무협력 통해 자사 솔루션 '포쉴드' 현장 적용 계획
-3대 중점업무에 'OT 보안서비스 구축' 포함한 삼성SDS, 추후 행보에 주목

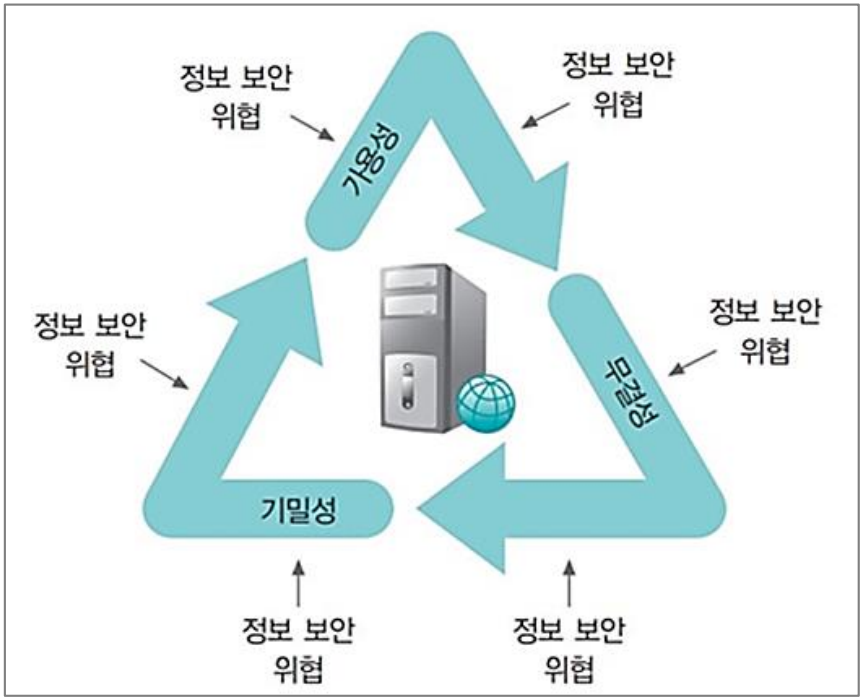
많

1
2
3
4
5
6
7
8
9
10

2. 정보 보안의 이해

- 보안을 이루는 속성
- 보안 전문가의 자격 요건
- 보안과 관련된 법

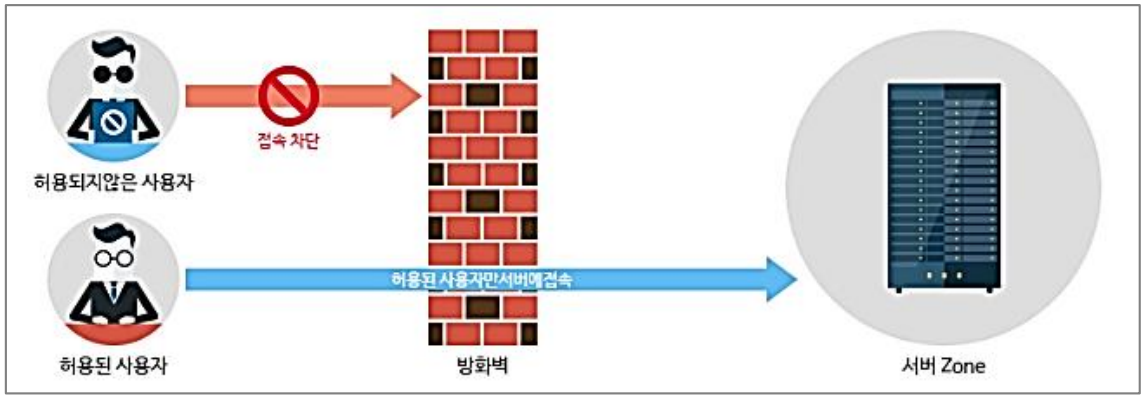
보안의 3대 요소 : 기밀성(confidentiality), 무결성(integrity), 가용성(availability)



2. 정보 보안의 이해

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 변경할 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) 위조 지폐로 취급되어 엄중한 법의 처벌을 받음
  - ✓ **자신의 메신저 대화를 누군가 임의로 바꾼다면**
- 흔히 보안의 첫 번째 요소로 기밀성을 말하지만,
  경우에 따라서는 무결성을 우선으로 둘 수 도 있음

2. 정보 보안의 이해

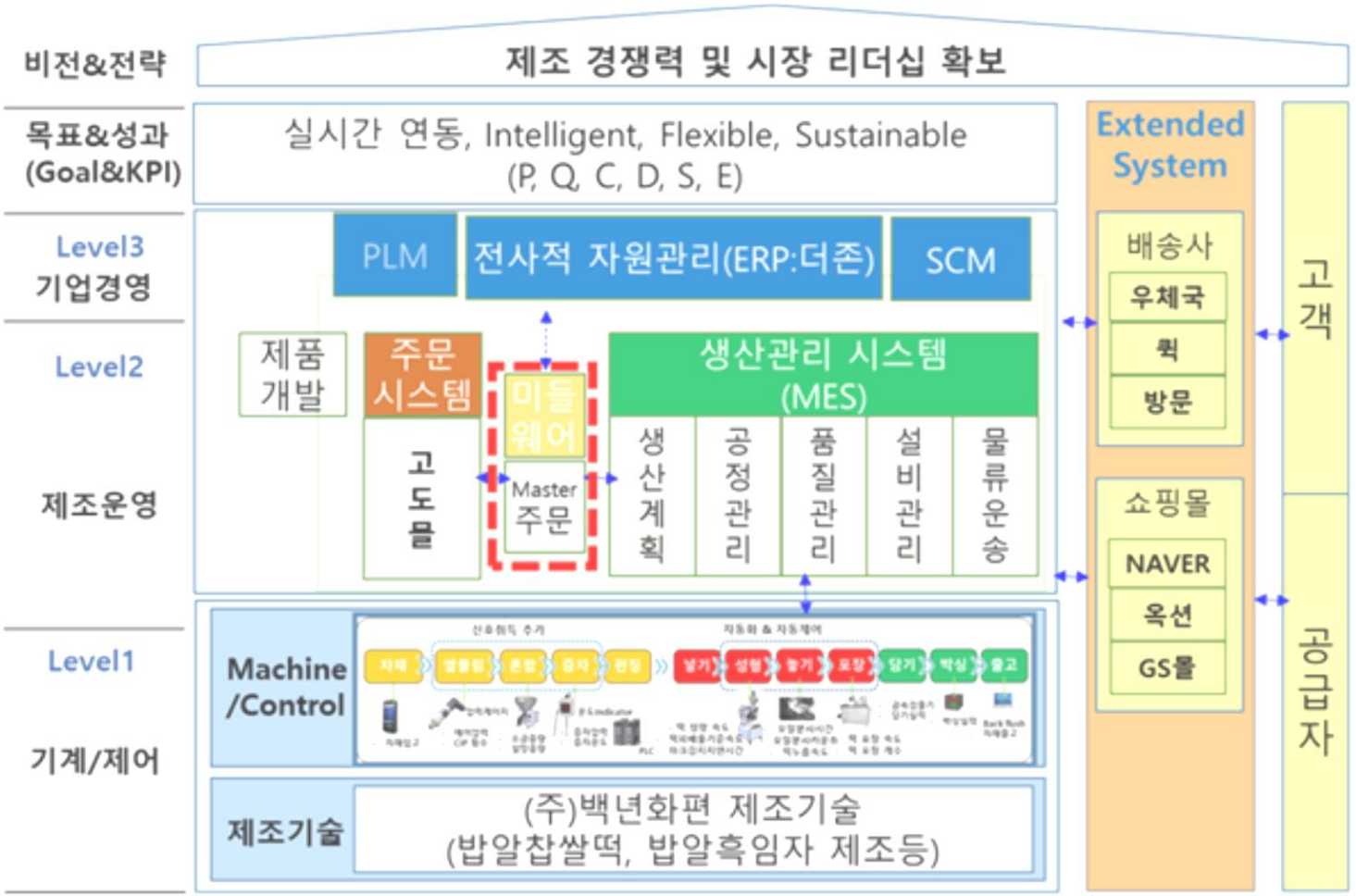
무결성(integrity)

- 현재 발생하는 많은 프로젝트에서 데이터의 **일관성과 정확성**을 위한 규칙의 파악이 대개 데이터 전문가의 역할이 아니라 **프로그램 담당자의 역할인 경우가 많음.**

- 문제는 데이터는 통합 관리되어야 하는데 **프로그램 관점에서 데이터를 접근하는 사람들은 데이터 전문가 보다는 상대적으로 통합의 개념이 약함**. 프로그램 전문가들은 본인이 담당하는 프로그램이 문제 없이 잘 수행되는 것에 당연히 더 관심이 많은 것이다. 즉, *애플리케이션의 위주의 절차 중심의 분석, 설계는 데이터 통합이라는 너무도 중요한 사상을 놓칠 수 있는 가능성이 높음.*

2. 정보 보안의 이해

무결성(integrity) 관련 사례



2. 정보 보안의 이해

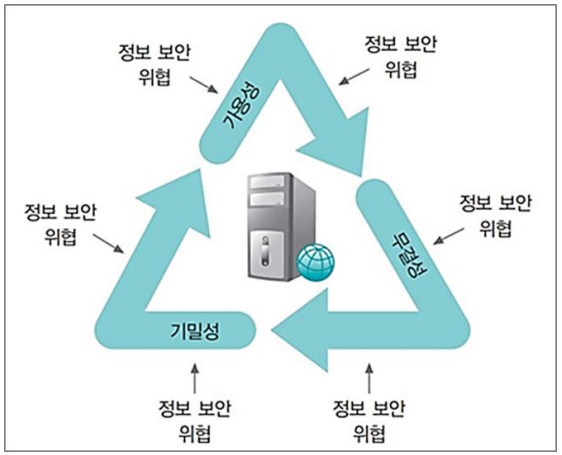
가용성(availability)

- **가용성은 인가를 받은 사용자가 정보나 서비스를 요구할 경우, 정보시스템에 대한 사용 가능 여부에 대한 요구 사항**
- 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것을 의미
- 원하는 시간, 환경, 서비스시에 특정 정보를 사용할 수 있어야 하며, 만약 사용이 불가하다면 해당 정보에 대해서는 가용성이 깨졌다고 한다.
- 일상생활에서 가용성을 상품화한 **대표적인 예로는 24시간 편의점,카드 사용**
- 현대 사회에서 정보의 가용성이 훼손되는 것은 필수 불가결한 요소의 가용성이 훼손되는 것과 마찬가지

2. 정보 보안의 이해

[반복되는 통신장애] 초연결시대 '위험사회' 극복 위한 해법 없나

"공급망은 모든 기관과 기업들의 글로벌 운영에 있어서 매우 중요한 요소다. 사이버공격 10건 중 4건은 조직이 아니라 공급망 링크 중 하나에서 발생한다" 라며 "기업의 공급업체가 조직의 데이터를 손상시킬 수 있도록 허용하면 정보의 **기밀성, 가용성 및 무결성**이 위협받게 된다"고 설명했다. 출처 : 투데이 신문(http://www.ntoday.co.kr)



2. 정보 보안의 이해

사이버 범죄 유형

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

사이버 범죄의 유형

구분	설명
사이버 테러형 범죄	정보통신망 자체를 공격 대상으로 한다. 해킹, 바이러스 유포, 메일 폭탄, 서비스 거부(DoS) 공격 등 **전자기적 침해 장비를 이용하여 컴퓨터 시스템과 정보통신망을 공격하는 불법 행위**
일반 사이버 범죄	**사이버 공간을 이용한** 일반적인 불법 행위로 사이버 도박, 사이버 스토킹, 사이버 성폭력, 사이버 명예훼손, 사이버 협박, 전자상거래 사기, 개인정보 유출 등의 행위를 말함

2. 정보 보안의 이해

윤리 의식

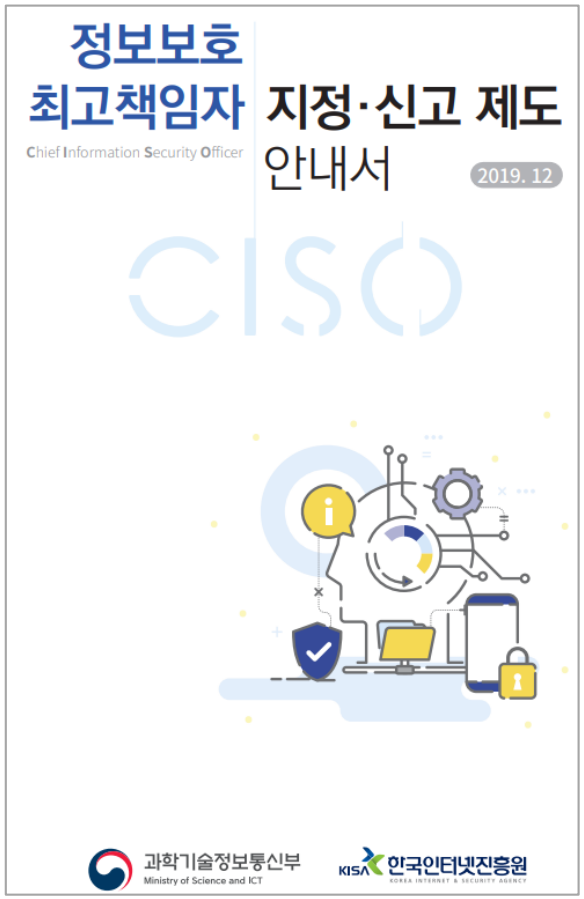
윤리 강령 : 보안이나 해킹과 관련된 기술을 배워 좋은 곳에 활용하는 전문가가 되기를 바라는 목적

정보통신 윤리 강령

- 우리는 **타인의 자유와 권리를 존중**한다.
- 우리는 **바른 언어를 사용**하고 예절을 지킨다.
- 우리는 **건전하고 유익한 정보를 제공**하고 올바르게 이용한다.
- 우리는 **청소년 성장과 발전에 도움이 되도록** 노력한다.
- 우리 모두는 **따뜻한 디지털 세상**을 만들기 위하여 서로 협력한다.

2. 정보 보안의 이해

정보보호 최고책임자 관련 직책



참고 2 정보보호 최고책임자 관련 직책 비교

직책	근거	대상	역할	직위	비고
정보보호 최고책임자 (CISO)	정보통신망법 제45조의3	정보통신서비스 제공자	정보통신시스템 등에 대한 보안 및 정보의 안전한 관리	임원급	신고
개인정보 보호책임자 (CPO)	정보통신망법 제27조	정보통신서비스 제공자등	이용자의 개인정보 보호 및 개인정보 관련 이용자 고충 처리	임원, 개인정보 관련 이용자 고충처리 부서의 장	공개
	개인정보 보호법 제31조	개인정보처리자	개인정보의 처리에 관한 업무 총괄 책임	고위공무원, 사업주 또는 대표자, 임원, 개인정보 처리 부서의 장	공개
정보보호 책임자 (CISO)	정보통신기반 보호법 제5조	주요정보통신기반 시설 관리기관	시설 보호에 관한 업무 총괄	4·5급 공무원, 영관급 장교, 임원급 관리·운영자	통지
정보보호 최고책임자 (CISO)	전자금융 거래법 제21조의2	금융회사, 전자금융업자	전자금융업무 및 기반 정보기술부문 보안 총괄	임원 (상법 제401조의2 제1항제3호에 따른 자 포함)	-
신용정보 관리·보호인	신용정보법 제20조	신용정보회사, 신용정보집중기관, 신용정보제공·이용자	신용정보의 관리 및 보호에 관한 업무	임원	공시
고객정보 관리인	금융지주 회사법 제48조의2	금융지주회사등	고객정보의 엄격한 관리	임원	-
정보화 책임관(CIO)	국가정보화 기본법 제11조	국가기관, 지방자치단체	국가정보화 시책 수립·시행과 국가정보화 사업 조정 등의 업무 총괄	-	통보

2. 정보 보안의 이해

정보보호 최고책임자의 겸직 제한

대규모 기업 등의 경우에는 정보보호 최고책임자가 정보보호 업무 이외의 다른 업무를 겸직할 수 없도록 하여 기업의 정보보호 대응능력 강화

1. 일반 자격요건(정보통신망법 시행령 제36조의6제2항)

- 정보보호 최고책임자는 임원급으로서 다음 중 어느 하나의 자격요건을 갖추어야 함

  - 정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람

    - 정보보호 또는 정보기술 분야 학위란 전자 관련 학과, 정보통신 관련 학과, 정보보호 또는 정보처리기술 관련 학과의 과정을 이수·졸업한 학력(이하 같음)

  - 정보보호 또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년 이상 수행한 경력이 있는 사람

    - 정보보호 관련 업무는 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호 업무 등을, 정보기술 관련 업무는 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 업무 등을 말함(이하 같음)
    - 학위 취득 시기와 경력의 선·후는 자격요건 부합여부를 판단하는데 관계가 없음(이하 같음)

2. 정보 보안의 이해

정보보호 조직

본문바로가기 >

충북대학교 CHUNGBUK NATIONAL UNIVERSITY

Home | Login | Sitemap

- 정보화본부 소개
- 정보 서비스
- 온라인 서비스
- 강의실 운영
- 정보보안
- 소프트웨어 안내
- 정보화본부 소식

충북대학교 바로가기

정보화본부 충북대학교 정보화본부입니다.

업무및직원정보 Home > 정보화본부 소개 > 업무및직원정보

전산운영지원팀 한국교통대학교

성명	직책	전화번호	주요업무
최종환	팀장	043-841-5084	· 전산운영지원팀 업무 총괄 · 시스템 도입 및 운영 업무 총괄 · 정보통신보안 및 개인정보보호 업무 · 전산장비 및 PC 유지보수 관리 · 전자서명 인증관련 업무 · 정보공시 담당 · 정보보안 및 개인정보보호 수준진단
최용희	주무관	043-841-5085	· Network(전산망) 관리(증평 캠퍼스 포함) · System 서버 등 각 종 H/W 관리 · 보안시스템 관리(방화벽, 침해방지(차단)시스템 등) · VPN(가상사설망) 시스템 관리 · 사이버 보안 관제 · Client 유지보수 관리 (증평 캠퍼스 포함) · 원내 물품 관리 · IP Address 운영 관리

- 정보보안 기획 및 운영
- 사이버 보안관제 업무

교육연구지원팀

- 전산 실습실 관리
- 교육용 및 연구용 소프트웨어 관리
- 전산관련 특강 계획 수립 및 추진

2. 정보 보안의 이해

정보보호 관련 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률

조항	내용
제70조1항	다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금
제70조2항	악성프로그램을 전달 또는 유포하는 자는 7년 이하의 징역 또는 7천만원 이하의 벌금
제71조1항	다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금 제1호~제8호 삭제(2020.02.04) 제9호 : 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망정보통신망에 침입한 자 제10호 : 정보통신망에 장애가 발생하게 한 자 제11호 : 타인의 정보를 훼손하거나 타인의 비밀을 침해・도용 또는 누설한 자
제72조1항	다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금 제2호 : 속이는 행위로 다른 사람의 정보를 수집한 자 제5호 :직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자
제73조	다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금 제1호 기술적,관리적 조치 미이행으로 개인 정보를 분실,도난,유출,위조,변조,훼손한 정보통신서비스 제공자.....
제74조1항	다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금 제2호 음란한 부호,문언, 음향, 영상 등을 배포,판매,임대,전시한 자 제3호 공포와 불안을 유발하는 부호, 문언, 음향, 화상, 영상을 반복한 자 .....

정보보호 관련 법률

개인정보 보호법

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. <개정 2014. 3. 24.>

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014. 3. 24., 2020. 2. 4.>

1. "개인정보"란 **살아 있는 개인에 관한 정보**로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. **성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보**

제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 **책임질 개인정보 보호책임자를 지정**하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

정보보호 관련 법률

제10장 벌칙 <개정 2020. 2. 4.>

제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 **10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.** <개정 2015. 7. 24.>

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 **자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.** <개정 2016. 3. 29., 2020. 2. 4.>

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항(제39조의14에 따라 준용되는 경우를 포함한다), 제19조, 제26조제5항, 제27조제3항 또는 제28조의2를 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제23조제1항을 위반하여 민감정보를 처리한 자

정보보호 관련 법률

- **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 조성 하기 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

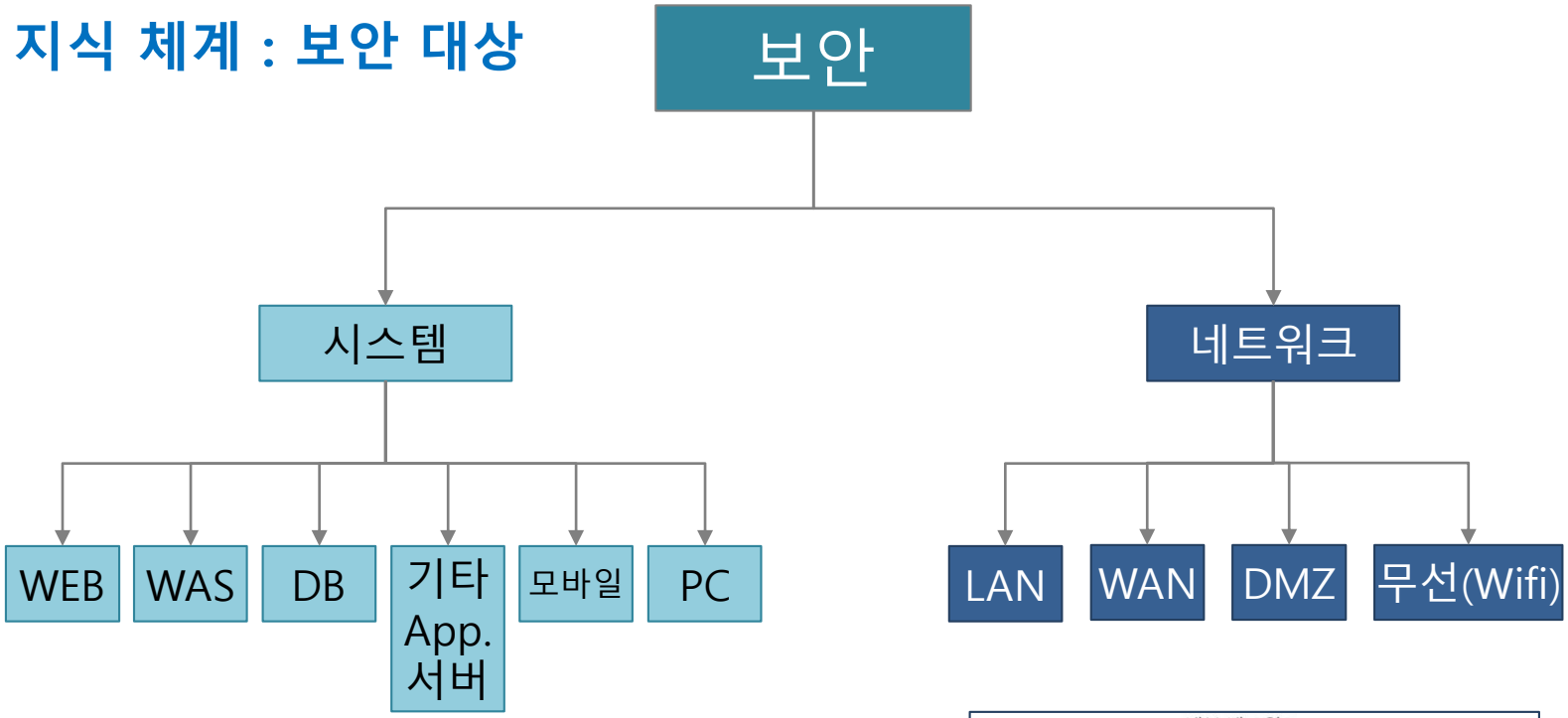
2. 정보 보안의 이해

보안 전문 분야

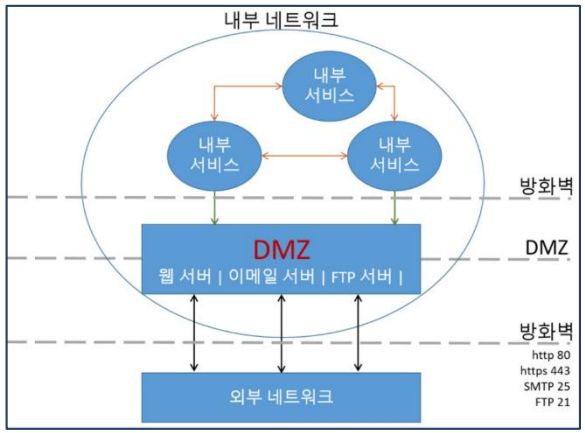
1.	시스템	운영체제 및 애플리케이션 설정과 관련된 분야
2.	네트워크	네트워크 장비 설정과 네트워크 보안 장비와 관련된 분야
3.	웹	웹 서비스 및 웹 소스코드의 취약점과 관련된 분야
4.	리버스 엔지니어링	애플리케이션 소스 코드와 관련된 취약점 관련 분야
5.	관리 보안	보안 정책(Policy), 거버넌스 등과 관련된 사항

2. 정보 보안의 이해

보안 지식 체계 : 보안 대상



컴퓨터 보안에서의 비무장지대(Demilitarized zone, DMZ)는 **조직의 내부 네트워크와 (일반적으로 인터넷인) 외부 네트워크 사이에 위치한 서브넷이다**. ... DMZ는 일반적으로 **메일서버, 웹서버, DNS, 주문시스템** 서버와 같이 외부에서 접근되어야 할 필요가 있는 서버들을 위해 사용된다.



2. 정보 보안의 이해

보안 지식 체계 : 보안 사항

보안 설정	Application 설정	관련 보안 시스템
네트워크 장비에 대한 보안 설정으로 네트워크장비의 계정관리, 접근관리(ACL), VLAN 설정 등과 같이 장비 레벨에서 설정 해야할 보안 사항이 존재	네트워크 장비에 대한 App 보안 사항은 **telnet 등과 같이 관리 Demon 등의 취약점과** 관련한 일부 사항이 있음	네트워크의 경우 네트워크 장비 자체에서 설정할 수 있는 보안 수준에 제약이 많고, 목적 및 성능상 적합하지 않은 경우가 많아 별도의 보안 솔루션이 존재함 **방화벽, 침입탐지 시스템, 침입차단시스템, DLP, 스팸 차단 시스템**과 같이 네트워크상에서 패킷을 분석하여 대응하는 형태의 솔루션들이 존재함
모든 시스템은 각자의 운영체제(OS)를 가지고 있으며, 각 OS별로 **계정 관리, 권한 관리 등 흔히 시스템 보안**이라고 말하는 사항들과 관련된 보안 설정이 필요함	시스템에 설치된 서비스의 종류에 따라 Application이 가지는 고유한 취약점들에 대한 보안이 필요함 **WEB서버의 경우 WEB관련 취약점. DB서버의 경우 DB관련 취약점** 등 설치된 Application 종류에 따라 보안 설정 및 관련 취약점이 존재함	시스템의 경우 대부분 시스템 자체의 보안 설정에 충실한 형태로 설정되어 있음 시스템 측면에서는 보안사고 대응을 위한 보안 장비보다는 AD, SOO 등 운영과 관련한 권한 관리 시스템을 주로 생각. PC 또는 모바일 환경의 경우 DRM, USB 통제 툴과 같이 사용자의 업무환경과 관련한 보안 툴들이 존재함.

2. 정보 보안의 이해

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/IP**는 지금도 네트워크의 기본이 되는 프로토콜로서 매우 중요

다양한 분야의 지식

- **프로그래밍**
  - ✓ 기본적인 **C** 프로그래밍과 객체 지향 프로그래밍에 대한 이해, JavaScript, HTML에 대한 이해가 필요
  - ✓ 자신만의 해킹 툴이나 보안 툴을 만들고자 한다면 **C 언어**를 충분히 알아야 함, 파이썬(Python)

- **서버**
  - ✓ 보안전문가는 기업이 안전하고 신뢰할 수 있는 서비스를 제공하도록 서버를 운용하기 위해 서버에 대한 이해가 필요
  - ✓ 데이터베이스의 경우 기본적인 SQL 지식이 필요
  - ✓ 웹, DBMS, WAS, FTP, 네트워크 프로토콜(SSH(Secure Shell Protocol) 등), Telnet

2. 정보 보안의 이해

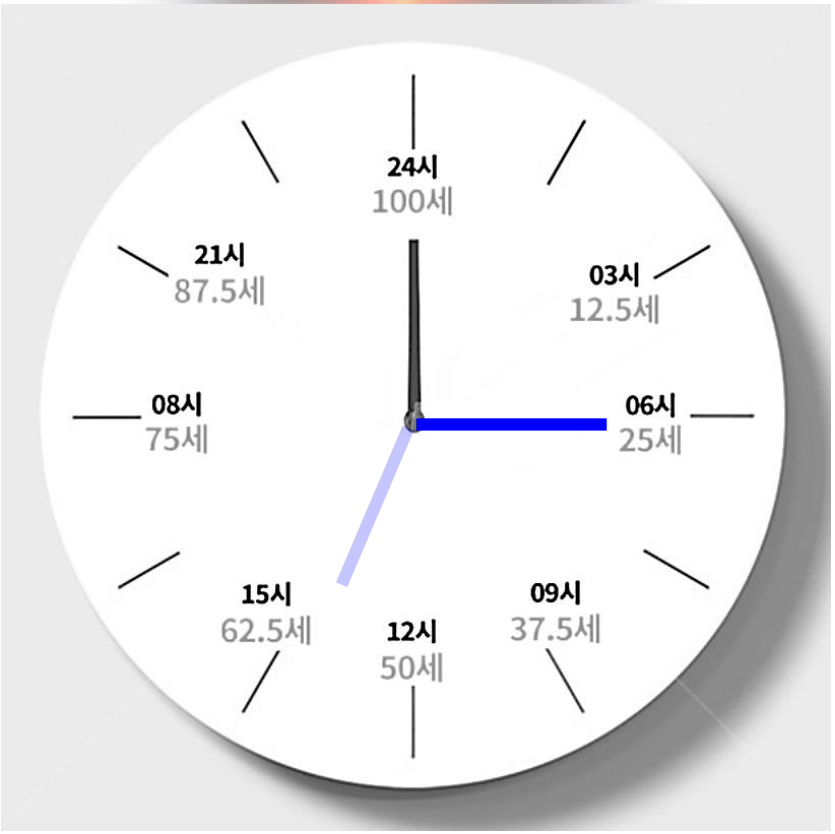
다양한 분야의 지식

- **보안 솔루션**
  - ✓ 보안 솔루션의 경우 시스템별 기본 보안 통제와 적용 원리, 네트워크 상의 구성과 목적 등을 이해

- **모니터링 시스템**
  - ✓ **네트워크 관리 시스템 (NMS), 네트워크 트래픽 모니터링 시스템 (MRTG**, Multi Router Traffic Grapher)과 같은 모니터링 시스 템의 기본 개념을 인지
  - ✓ 암호 암호와 해시의 차이, 대칭 키 알고리즘 및 비대칭 키 알고리즘의 종류와 강도, 공개 키 기반 구조를 파악

- **정책과 절차(법(法))**
  - ✓ 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

인생(人生)


24시
100세
03시
12.5세
06시
25세
09시
37.5세
12시
50세
15시
62.5세
08시
75세
21시
87.5세

Thank you


INFORMATION SECURITY
INTERNET
KT-VPN
VPN 접속 라우터
L4 Content 스위치
SAN 스위치
TAPE백업장치