

# 오리엔테이션

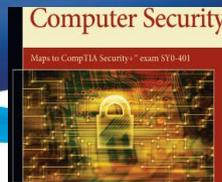
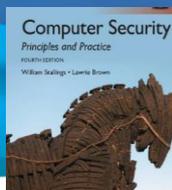
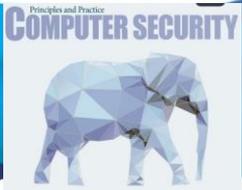
(교과목 개요 및 수업 방향)

2024. 9

박종혁 (Jong Hyuk Park) 교수

서울과학기술대학교 컴퓨터공학과

[jhpark1@seoultech.ac.kr](mailto:jhpark1@seoultech.ac.kr)



1. 교과목 개요
2. 평가방법
3. 컴퓨터보안의 필요성
4. 컴퓨터보안의 정의 및 종류
5. 강의내용
6. 컴퓨터보안 전망

# 1. 교과목 개요

# 1.1 담당교수 소개



## 박종혁교수 (Jong Hyuk Park)

- 최종학위: 박사1(정보보호), 박사2(Human Science)
- 주 연구분야: 컴퓨터보안, 블록체인, IoT 및 클라우드 보안, 양자정보기술, AI보안
- 연구실: 미래관 325호
- 홈페이지: <http://www.parkjonghyuk.net>
- 연구실: UCS Lab, <https://ucs.seoultech.ac.kr/index.do>  
연구실소개 자료 **CLICK** 
- 대표 약력
- GQAS 연구소 부소장, <https://gqas.seoultech.ac.kr>

연도(부터 ~ 까지)	기관명	업무	직위
2009.9 ~ 현재	서울과학기술대학교 컴퓨터공학과	교육 및 연구	교수
2002.12 ~ 2007.7	한화에스앤씨(주) 기술연구소	선임연구원	연구
2011.1 ~ 현재	국제 HCIS 논문지 (SCIE, 세계 상위 15%)	총괄편집위원장	편집위원장
2009.9 ~ 현재	한국정보처리학회	국제 및 저널 총괄	부회장

## 1.2 교과목 소개

---

교과목 명	컴퓨터보안 (Computer Security)
교과 구분	전공 선택 (3학점)
강의 시간	월 2,3,4 교시
강의 구성	이론 (3)
강의 방법	대면

---

## 1.3 교과목 개요

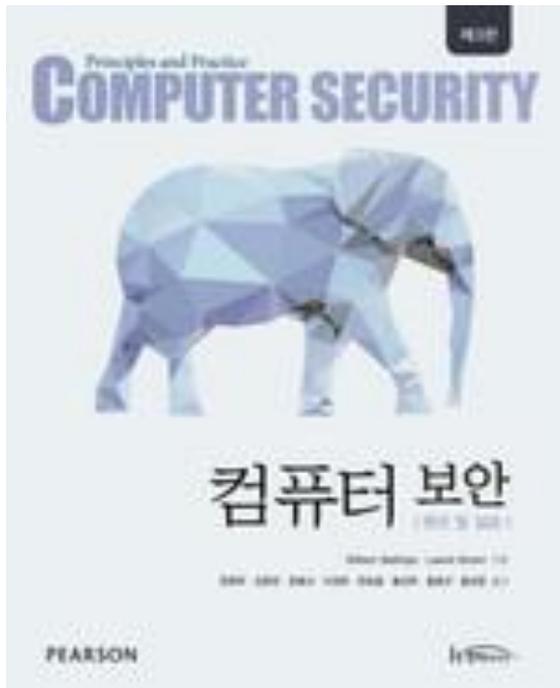
- 컴퓨터보안 개념 (정보보안 기초, 네트워크 보안, 보안 정책 등)의 이론, 응용, 실무에 대해서 학습함
- 인증, 접근제어 등 기본 필수 보안요소 및 악성 소프트웨어, 보안공격, 모바일 및 IoT 보안 등 응용보안에 대해 학습 함
- 컴퓨터보안 사이버 범죄 수사관련 응용 분야인 디지털 포렌식에 대해 학습함

## 1.4 학습 목표

- I. 컴퓨터보안의 실무분야를 위한 기본 이론, 응용, 실무 적용 등에 대한 필수 지식 습득
- II. 컴퓨터 보안 개념이 적용된 최근 관련 응용 연구 분야 조사, 분석 및 신규 아이디어 제안을 통한 컴퓨터보안 지식의 창의성 및 활용성 능력을 배양함

## 1.5 학습 교재

- **주교재**  
컴퓨터 보안, William Stallings 저, 한영옥외 8인 역,  
한티미디어, 2016



# 1.5 학습 교재

- **보조교재**

- 정보보안 개론 (개정4판), 양대일 저, 한빛 출판네트워크, 2021
- 네트워크 해킹과 보안(4판), 양대일 , 홍성혁 저, 한빛 아카데미, 2023
- 인터넷 해킹과 보안(4판), 김경곤 저, 한빛 아카데미, 2022



# 1.6 주차별 강의 운용 계획

주별	날짜	강의내용	수업방식	비고	보강 날짜
1	9/9	OT 및 교과목 개요	대면		
2	9/16	보안 위협요소와 백신	휴강	추석연휴	온라인 영상 수업
3	9/23	사용자 인증	대면		
4	9/30	접근제어	대면		
5	10/9	데이터베이스와 클라우드	대면	한글날	
6	10/14	악성 소프트웨어	대면		
7	10/21	네트워크 보안 (1)	대면		
8	10/28	중간고사	대면	과제 1차 제출	
9	11/4	네트워크 보안 (2)	대면		
10	11/11	디지털 포렌식 (1)	대면		
11	11/18	디지털 증거	휴강	논술고사일	온라인 영상 수업
12	11/25	디지털포렌식(2-1)	대면		
13	12/2	디지털 포렌식 (2-2), 보안관리	대면		
14	12/9	최신 ICT 보안 기술 및 과제 발표	대면	과제 2차 제출	
15	12/16	기말고사	대면		

## 2. 평가 방법

### 2.1 학습평가 방법

### 2.2 과제 설명

## 2.1 학습평가 방법

- 출석 (10%), 과제물 (20%), 중간고사 (30%), 기말고사 (30%), 기타(10%)
- 기타
  - 과제 발표 (14주차)
  - 비정기 과제

## 2.2 과제 설명

### 과제 #1

- 컴퓨터 보안 관련 최근 연구 동향 보고서를 작성하여 기한 내 eClass에 업로드 한다.

(8주차, 중간고사 당일 23시 까지)

### 과제 #2 :

- 개인과제 #1을 기반으로 "컴퓨터 보안 응용 기술 또는 서비스에 대한 신규 아이디어 제안"을 작성하여 기한 내 eClass에 업로드 한다.

(14주차 수업 전일 23시 까지)

\*\* 과제 양식을 꼭 사용하여 작성할것 (다른 양식 사용시 감점) \*\*

\*\* Copy Killer 검사 결과 꼭 제출할것 \*\*

### 기타 발표 (14주차)

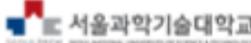
\* 희망자 선착순 10명

- 개인과제# 2 발표 (10분) ← 기타 점수 추가점 부여!!
- 희망자는 조교선생님한테 9/22 18:00까지 메일을 보내세요  
(조교: 김민지 대학원생, mjdorothy679@seoultech.ac.kr)

# 과제 제출관련 중요사항

## 도서관 표절 검사기 (Copykiller) 활용

- 각 과제 보고서를 도서관의 표절검사기로 유사율을 검사하여 함께 제출 해야 함 (유사율이 높을 경우, 표절로 판정함)

**Copy Killer**  

<https://seoultech.copykiller.com>

- 최근 전세계적으로 문서(레포트, 논문 등)에 관한 유사도를 확인하고있으며, 연구 윤리 측면에서 심각한 문제로 대두됨
- 우리 수업에서도 표절을 이용 감산제를 적용함
- 유사도 검사 결과 표절율이 **30% 이상**인 학생에게 패널티를 부여함
  - 과제점수 \* 표절율 감점 적용
- 예) 과제점수 7점, 표절율 40%
  - 패널티 점수 = 3점
  - 과제점수 (7) \* 표절율 (40%) = 2.8 (3점 적용)
  - 최종 과제 점수 = 기본점수 (7) - 패널티 점수 (3점) = 4점
- 표절률이 60% 이상인 보고서는 완전 표절로 판단 “0점”을 부여함

# 3. 컴퓨터보안의 필요성

- **보안사고 영상**

"피해 더 커지기 전에..." 대국민 권고 나선 국정원 / SBS 8뉴스  
[https://www.youtube.com/watch?v=b0g5\\_D7LHbl](https://www.youtube.com/watch?v=b0g5_D7LHbl)

이런 내용이 어쩌다 그대로...취약계층 '정보 보안 사고' [9시 뉴스] / KBS  
<https://www.youtube.com/watch?v=MsY6vBD6Jdw>

대법원·국방부·국토부 홈페이지 맘만 먹으면 해킹..."직접 뚫어 봤습니다!" / YTN  
[https://youtu.be/oHRFGv\\_ljyo](https://youtu.be/oHRFGv_ljyo)

'트위터 계정 해킹'...역사상 최악의 보안사고 / C채널방송  
<https://www.youtube.com/watch?v=TPxOtILDs2U>

- **사이버 보안기술 영상**

스스로 형태 바뀌 방어" 신개념 사이버 보안기술 등장 / YTN  
<https://www.youtube.com/watch?v=j67RZmqZvO8>

사이버 공격을 인공지능으로 대처하다 / YTN 사이언스  
<https://www.youtube.com/watch?v=bzk0UVJujPQ>

# 컴퓨터보안의 필요성

- 정보 자산에 대한 중요성 증가에 따른 사이버 위협의 증가
- 비대면 사회 활동 증가에 따른 사이버 활동의 신뢰성 이슈
- 개인의 프라이버시 이슈 증가
- IT기술 발달로 인한 컴퓨터의 사회적 영향력 증가
  - 해킹, 인터넷 사기 등 사이버 공격 및 범죄 이슈 증가

→ 이러한 이슈들을 해결하기 위한  
컴퓨터 보안 (정보보호)의 필요성 대두

## 4. 컴퓨터보안의 정의

### ◆ 좁은 의미

컴퓨팅(Computing) 의미? 계산하다  
Computer Security

계산능력을 갖는 정보 시스템 내의 자원(하드웨어, 소프트웨어, 데이터, 통신 등)들의 무결성, 가용성, 기밀성을 보존하기 위해 제공되는 보안(보호)



### ◆ 넓은 의미

컴퓨터보안 = 정보보호 (정보보안) = 사이버 보안

정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적, 정책적 수단, 또는 그러한 수단으로 이루어지는 행위

# 컴퓨터보안의 종류

- 악성 소프트웨어
  - 시스템 보안
  - 네트워크 보안
  - 웹 보안 / 모바일 보안
  - 운영체제 보안
  - 데이터베이스 보안
  - 보안 관리/보안정책
- 
- ICT 융합 보안 (IoT, 클라우드, AI 등)
  - 블록체인 (NFT)
  - 디지털 포렌식
  - 양자 암호 (보안)

# 5. 강의 내용

## 주차 별 강의 내용 간략 소개

- 컴퓨터보안 개요
- 보안위협
- 최근 ICT 서비스 보안 위협

## 2장 사용자 인증

- 사용자 인증 개요
- 비밀번호 기반 인증
- 토큰 기반 인증
- 생체 인식 인증
- 원격 사용자 인증
- 인증 보안 이슈
- CAPTCHA

# 3장 접근제어

- 접근제어 원리
- 주체, 객체, 접근권한
- 임의 접근제어
- 역할 기반 접근제어
- 속성 기반 접근제어
- 자격 기반 접근제어
- 신원, 신용장, 접근 관리
- 실무 접근제어 솔루션 및 사례

# 4장 데이터베이스와 클라우드 보안

- 데이터베이스 보안의 필요성
- 데이터베이스 관리 시스템(DBMS)
- SQL 주입 공격
- 데이터베이스 접근 제어
- 추론
- 데이터베이스 암호화
- 클라우드 컴퓨팅
- 클라우드 보안 위험과 대응
- 클라우드 데이터 보호
- 서비스로서 클라우드 보안
- 기타 클라우드 보안 이슈

- 악성 소프트웨어의 유형
- 지능형 지속 위협 (APT)
- 전파: 손상된 내용, 바이러스
- 전파: 사회 공학, 스팸 전자메일, 트로이 목마
- 페이로드: 시스템 파괴
- 페이로드: 공격 에이전트, 좀비, 봇
- 페이로드: 정보 도용, 키로거, 피싱, 스파이웨어
- 페이로드: 은신, 백도어, 루트킷
- 대비책

- 네트워크의 이해
- 네트워크 공격과 보안
- 무선 네트워크 공격과 보안
- 방화벽
- 침입 탐지 시스템
- 침입 방지 시스템

# 7장 디지털 포렌식 (1) - 개관

## -디지털 포렌식 개요

- 등장 배경
- 디지털 포렌식 흐름
- 디지털 포렌식 연구분야

## -디지털 포렌식 조사의 일반 원칙

## -디지털 포렌식 수행 과정

## -디지털 증거

- 디지털 증거의 종류
- 디지털 저장 매체
- 디지털 증거의 특징

-디지털 증거의 개념 및 특성

-디지털 증거의 법적 허용성

-위법수집증거배제의 원칙

- 전문법칙 (傳聞法則, Hearsay Rule)

-디지털 증거의 법적 허용성 요건

- 디지털 증거의 증거 능력을 보장하기 위한 특성
- 디지털 증거의 법적 허용성 보장을 위한 장치
- 디지털 데이터의 증거 능력 관련 판례

-디지털 포렌식 조사 모델 정의

-디지털 포렌식 조사 모델 비교

-디지털 포렌식 조사 모델

- 조사 준비
- 현장 도착 시 대응
- 증거 확보 및 수집
- 운반 및 확인
- 조사 및 분석
- 보고 및 증언

# 10장 디지털 포렌식 (2) - 증거 수집 기술 및 분석 기술

- 디지털 증거 수집 장비 및 SW
- 활성 시스템 조사
- 디스크 이미징
- 임베디드 시스템 증거 확보
- 디스크 브라우징 기술
- 검색 기술
- 타임라인 분석
- 로그 분석
- 시각화 기술
- 안티포렌식 대응 기술
- 파일시스템의 이해

- 정보 보안 거버넌스
- 보안 프레임워크
- 보안조직
- 보안 정책과 절차
- 보안 인증
- 개인 정보 보호
- ISMS-P 소개

-양자 정보기술 (보안)

-Zero Trust

-AI 보안 등

# 6. 컴퓨터보안 전망

## ◆ 전망: 현정부 - 대통령 공약

- 디지털경제 패권국가' 도약을 위한 실천과제: **사이버보안 10만 인재 양성**
  - 신규 인력공급
  - 재직자 역량 강화

정규 과정 (1.0만명)	<b>[고급] 대학원(0.1만명)</b> <ul style="list-style-type: none"> <li>• (확대) 융합보안대학원 확대 (8개교 → 12개교, 석사 → 석·박사)</li> </ul>	사이버 훈련장 (2.5만명)	<b>'디지털 실전형 사이버훈련장' 구축(2.5만명)</b> <ul style="list-style-type: none"> <li>• [고급] 실전형 사이버 공격·방어 훈련 실시</li> <li>• [중급] 침해사고 대응 등 해킹방어 기본기술 습득</li> <li>• [초급] 동영상 강의, 실습 등 기초역량 교육</li> </ul>	
	<b>[중급] 대학(0.4만명)</b> <ul style="list-style-type: none"> <li>• (확대) 정보보호특성화대 확대(3개교→10개교)</li> </ul>		지역 교육 (2.6만명)	<b>'지역 정보보호교육센터' 설립(2.6만명)</b> <ul style="list-style-type: none"> <li>• [중·고급] 악성코드 분석·탐지 등 실무형 교육</li> <li>• [초급] 사이버보안 소양, 보안제품 실습 등 기초 직무 교육</li> </ul>
	<b>[초급] 특성화고·전문대학(0.4만명)</b> <ul style="list-style-type: none"> <li>• (신규) 사이버부서관 특화 정보보호 전문대학</li> </ul>			
특화 교육 (3.9만명)	<b>[고급] 최정예 우수 인력 확보(0.1만명)</b> <ul style="list-style-type: none"> <li>• (신규) 최정예 보안제품 개발과정 'S-개발자'(50명)</li> <li>• 정예 화이트해커(Best of Best, BoB) 양성(200명)</li> </ul>			
	<b>[중급] 실무형 인재 양성(3.6만명)</b> <ul style="list-style-type: none"> <li>• (확대) 구직자 대상 K-Shield Jr.(300명→1000명)</li> <li>• (신규) 중급 화이트해커(화이트햇 스쿨) 양성(300명)</li> <li>• (신규) 시큐리티 아카데미 도입(200명)</li> </ul>			
	<b>[초급] 보안관리 인력 공급 확대(0.2만명)</b> <ul style="list-style-type: none"> <li>• (확대) ICT 융합 보안교육 확대(400명→600명)</li> </ul>			

◆ **전망: 현정부 - 보안투자 확대**

○ 2023년 우리나라 정부의 정보 보호 정책 사업 예산(출처: 과학기술정보통신부)

구분	세부 사업	예산(전년 대비 증가율)
사이버보안 인재 양성	보안 핵심 인재 육성	67억 6000만 원(17.4%)
	정보 보호 전문 인력 육성	162억 8000만 원(68.2%)
	지역 정보 보호 교육 지원	23억 8000만 원 (36.6%)
	실전형 사이버 훈련장 구축	20억 원(신규)
정보 보호 산업 육성	정보 보호 산업 경쟁력 강화	74억 2000만 원(3.4%)
	정보 보호 시스템 평가 및 인증 기반 강화	21억 8000만 원(9.9%)
	전자 서명 인증	45억 원(116.4%)
사이버 보안 기술 개발	암호화 사이버 위협 대응 기술	30억 원(신규)
	국방 드론 사이버 보안 기술 개발	17억 7000만 원(신규)
	데이터 프라이버시 기술 R&D	56억 원(30.2%)
	무인 서비스 물리 보안 플랫폼 개발	40억 원(33.3%)
	사이버 보안 챌린지	33억 원(41.9%)
사이버 침해 사고 대응	해킹, 바이러스 대응 체계 고도화	641억 4000만 원(1.2%)

## ◆ 정보보호산업의 글로벌 경쟁력 확보 전략

○ 2027년까지 정보보호산업 시장규모 30조원 달성, 보안유니콘 육성 등을 목표로 4대 전략과 13개 과제를 추진 (출처: 과학기술정보통신부)

비전 	글로벌 정보보호산업 강국 도약		
목표 	'27년까지 정보보호산업 세계 5위권 진입 	'27년까지 정보보호산업 시장규모 30조원 달성 	'27년까지 보안 유니콘 육성 
추진 전략 	<ol style="list-style-type: none"> <li>① 보안패러다임 전환 주도권 확보 및 新시장 창출</li> <li>② 협업기반 조성을 통한 신흥시장 진출 강화</li> <li>③ 글로벌 공략을 위한 단단한 산업 생태계 확충</li> <li>④ 차세대 정보보호 기술 경쟁력 확보</li> </ol>		

# 7. 2023 상반기 보안 동향

## 1. 통계기반 보안 동향 결산 - 안랩

### 악성코드 종류별 통계

1위 다운로드(Downloader)(36.1%)

추가 악성코드를 감염PC에 내려받는 악성코드

2위 백도어(Backdoor)(34.9%)

차후 공격을 수행할 목적으로 시스템에 설치하는 악성코드

3위 인포스틸러(Infostealer)(26.6%)

계정정보, 가상화폐 지갑주소, 문서파일 등 다양한 사용자 정보를 탈취하는 악성코드

### 피싱 메일 키워드 통계

1위 주문·배송 (29.2%)

'Shipping(수송)', 'Order(주문)', 'Delivery(배달)' 등

2위 결제·구매 (14.9%)

'Payment(지불)', 'Receipt(영수증)', 'Invoice(청구서)' 등

3위 공지·알림 (9.8%)

'Urgent(긴급)', 'Alert(경고)', 'Notice(공지)' 등

### 업종별 공격탐지 통계

1위 게임개발 (17.7%)

모바일/PC 게임 개발 기업, 퍼블리셔(유통사) 등

2위 방송 (15.1%)

방송사, 스트리밍 서비스, CP사 등

3위 교육 (8.9%)

학교, 온라인 강의, 교육 콘텐츠 플랫폼 등

## 2. 보안 동향 결산 - 데일리 뉴스

- 이메일 피싱 공격 전년비 464% 급증
- 챗GPT 등 생성형 AI 활용한 사이버 공격 증가
- 랜섬웨어가 중소기업 주요 위협 요소
- 공급망 공격 - 60,000명 이상의 고객이 영향 받음

# 3. 보안 위협 및 대응기술 전망 - 이글루쿠퍼레이션

## ○ 보안위협 전망

### 1. 사이버 공격의 서비스화, 랜섬웨어 생태계 확장

#RaaS, #Multi Extortion, #DDoS, #CaaS, #블랙마켓,  
#공격도구양극화

### 2. 오픈소스 생태계 확장으로 인한 보안위협 진화

#Log4Shell, #Spring4Shell, #Text4Shell, #Open Source  
Project Repository, #DevSecOps

### 3. 위협의 체인화, 공급망 공격 증가 추세

#Supply Chain, #Exploit Chaining, #ICS/OT, #3rd Party,  
#Compromise, #SBOM

### 4. 가상화폐의 불확실성 증가, 가상화폐 타겟팅 사이버 공격 확산

#가상화폐거래소, #DeFi, #CeFi, #디지털자산

### 5. 국제정세 불안, 국가 사이버 안보 위협 증가

#Cybercrime, #Hacktivists, #State-sponsored hacker,  
#CyberWar, #DeepLocker

## ○ 보안 대응기술 전망

### 1. 사이버 공격의 서비스화, 랜섬웨어 생태계 확장

#AI, #Automation, #SOAR, #Threat Intelligence, #보안관제, #SOC

### 2. Security를 넘어 Safety로, 융합보안 필요성 강화

#ISO/IEC 62443, #CMMI, #HW, #Firmware, #Software

### 3. 클라우드 전환의 시작, 클라우드 보안 고려사항

#SASE, #CWPP, #CASB, #CSPM, #SECaaS, #ZTNA,  
#Never Trust, Always Verify

### 4. 데이터 경제의 시대, 데이터 활용과 보안

#데이터 거래, #마이플랫폼, #데이터 거버넌스, #암호화

### 5. 사이버 공격의 저지선, 공격표면관리

#External Attack Surface Management, #Cybersecurity  
Mesh, #Unknown Threat, #Known Threat

## 4. 24兆 '양자암호', 이통사 주도권 쟁탈전 심화

- 양자암호 기술이 미래의 '게임체인저' - 이동통신 3사의 주도권 경쟁 심화될 전망
- SKT, VPN에 '핵심 기술' 양자난수생성 기술 적용
- KT, QKD에 중점... 양자암호통신네트워크 국제표준 승인
- LGU+, 세계 첫 PQC 전용회선 출시

### ❖ 양자암호 기술

- 양자역학 원리를 적용, 빛의 가장 작은 단위인 광자에 정보를 담아 암호화해 전송하는 차세대 보안 통신 기술
- 양자특성을 통해 제3자가 암호기 탈취시도시, 이를 즉시 감지하고 정보는 변형됨



# (홍보) UCS 연구실 - 연구원 모집

- 본 연구실은 양자정보기술, 메타버스, 유비쿼터스 컴퓨팅, 클라우드 컴퓨팅, 스마트홈 보안, 딥 러닝 기반 지능형 보안 서비스, 블록체인 보안, 디지털 포렌식, 보안 프로토콜 등 최신 IT 트렌드와 관련된 컴퓨터 보안 이론 및 실무에 대한 다양한 분야의 연구를 진행해 오고 있습니다.

SeoulTech UCS Lab  
Ubiquitous Computing & Security Laboratory

## 2. 모집 분야 및 자격

- 모집인원: 서울과학기술대학교 일반대학원 컴퓨터공학과, 석사과정 0명, 석박사통합과정 0명, 박사과정 0명 (

Full time

모집요강 상세

[http://parkjonghyuk.net/file/UCS\\_kor.pdf](http://parkjonghyuk.net/file/UCS_kor.pdf)

- 모집과정 1 (한국인)

박사과정: 국방 IT 계약학과-취업보장형 0명

석사과정: 컴퓨터공학과 0명/국방 IT 계약학과-취업보장형 0명

학부연구원: 0명 (3-4학년)

학석과정: 0명 (3학년만 지원가능)

- 자세한 사항은 다음 연락처로 연락 주시기 바랍니다.

- **연락처: 조병현 (석사과정)**

이메일: [jbh1020@seoultech.ac.kr](mailto:jbh1020@seoultech.ac.kr), 휴대폰: 010-3089-2723

1. 尹 정부, 사이버보안 인재 10만명 키운다, 2022, <https://zdnet.co.kr/view/?no=20220713103021>
2. 2023년 정부 정보보호 정책 사업에 약 3000억원이 투입된다. 올해보다 4.5% 늘어난다., 2022, 전자신문, <https://www.etnews.com/20220905000100>
3. 보보호 산업규모 2027년 30조원 목표... 예산 1조 1천억 투입, 보안뉴스, 2023, <https://www.boannews.com/media/view.asp?idx=121642>
4. 주요 통계로 보는 '2023년 상반기 보안위협 동향'은?, 보안뉴스, 2023, [https://m.boannews.com/html/detail.html?mtype=3&tab\\_type=H&idx=120206](https://m.boannews.com/html/detail.html?mtype=3&tab_type=H&idx=120206)
5. 아크로니스 "챗GPT 등 생성형 AI 활용한 사이버 공격 증가", 데일리뉴스, 2023, <http://www.itdaily.kr/news/articleView.html?idxno=215933>
6. 2023년 사이버 보안위협 및 대응기술 전망, 이글루쿠퍼레이션, <https://www.igloo.co.kr/security-information/2023년-사이버-보안위협-및-대응기술-전망>
7. 24兆 미래먹거리 '양자암호', 이통사 주도권 쟁탈전 심화, 데일리뉴스, 2023 <https://biz.newdaily.co.kr/site/data/html/2023/07/03/2023070300206.html>

