



# 네트워크 보안 및 개인정보 유출



사례를 통한 사이버 공격과 보안





# 목차



**01** 네트워크 보안의 정의

**02** 정보 보안 핵심 원칙

**03** 대표적인 보안 위협

**04** 대표적인 보안 방안

**05** 주요 사례 분석

**06** 네트워크 보안 방안



# ■ 네트워크 보안의 정의

## 포괄적 의미

- 컴퓨터 네트워크 및 리소스 보호
- 무단 액세스, 오용, 수정, 거부 방지
- 데이터와 시스템의 안전성 확보
- 사이버 위협으로부터 조직 보호
- 지속적인 모니터링 및 대응 체계

## 주요 구성 요소

- 보안 제어: 기술적 방어 수단
- 정책: 조직의 보안 지침
- 프로세스: 체계적인 보안 절차
- 관행: 일상적인 보안 습관
- 인적 요소: 직원 교육 및 인식

# ■ 정보 보안 핵심 원칙 (1)

## 기밀성(Confidentiality)

권한 없는 접근을 차단하고  
허가된 사용자에게만 정보의 접근을 허가하는 것

- 권한 없는 접근 차단
- 민감 정보 보호
- 데이터 유출 방지
- 프라이버시 보장
- 정보의 비밀성 유지

## 구현 방법

- 강력한 암호화 기술 적용
- 접근 제어 시스템 구축
- 다중 인증 방식 도입

## ■ 정보 보안 핵심 원칙 (2)

### 무결성(Integrity)

정보가 허가되지 않은 방식으로  
변경되거나 손상되지 않는것

- 데이터 정확성 유지
- 변조 방지 및 탐지
- 신뢰할 수 있는 정보 보장
- 시스템 일관성 유지
- 무단 수정 차단

### 구현 방법

- 해시 함수 활용
- 디지털 서명 기술 적용
- 체크섬 검증
- 버전 관리 시스템 도입
- 정기적인 데이터 감사

## ■ 정보 보안 핵심 원칙 (3)

### 가용성(Availability)

정보가 필요할 때 언제든지 접근할수 있도록 하는 것

- 권한 있는 사용자의 데이터 및 리소스 접근 보장
- 필요한 때에 시스템과 데이터 사용 가능
- 서비스 중단 최소화 및 신속한 복구 목표
- 자연재해, 기술적 장애, 사이버 공격에도 대응

### 구현 방법

- 백업 시스템 구축 : 데이터와 시스템의 정기적 백업
- 장애 복구 시스템(DRS) 운영: 신속한 서비스 복구
- 부하 분산 : 트래픽 분산으로 시스템 안정성 향상
- 중복성 확보 : 주요 시스템 및 네트워크 구성요소 이중화
- 보안 업데이트 : 최신 보안 패치 적용으로 취약점 해소



# ■ 대표적인 보안 위협

## 스니핑(Sniffing)

네트워크를 통해 전송되는 패킷을 가로채서 엿보는 행위

- 보안이 약한 공공 와이파이 등에서 자주 발생
- 통신 빈도, 데이터 내용등의 정보가 유출

### 대응 방안

- 네트워크 세그멘테이션
- 암호화된 통신(VPN) 사용
- 데이터 암호화

## 스푸핑(Spoofing)

다른이의 IP등을 이용해서 신원을 위장하는 행위

- 탈취한 IP로 정보를 빼내거나 다른 서비스에 접속
- DDoS 공격으로 이어지는 경우도 있음

### 대응 방안

- 패킷 필터링
- 데이터 암호화
- 인증 절차 강화

# ■ 대표적인 보안 위협

## DDos(Distributed Denial-of-service)

분산된 여러 좀비PC등을 이용해 타겟 시스템에 과부하를 거는 행위

- 간단하지만 막기 어려운 사이버 공격의 형태
- 완벽히 방어하는 것이 아니라 완화시키는 것이 목표

### 대응 방안

- 트래픽 모니터링
- 네트워크 필터링
- 애플리케이션 계층 보안 솔루션 사용

## 세션 하이재킹

사용자가 로그인한 상태의 세션을 빼앗아서 로그인하지 않고도 정보에 접근하는 행위

- 세션ID가 저장된 쿠키를 탈취하는 방식
- 미리 악성 스크립트를 설치해 두는 방식

### 대응 방안

- 웹 트래픽 암호화
- 세션 만료 설정
- 인증 절차 강화



# ■ 주요 보안 기술

## SSL/TLS

- 데이터 암호화
- 통신 보안 강화

## VPN

- 가상 사설망
- 암호화된 터널 생성
- 원격 접속 보안
- 공용 네트워크 보호

## HTTPS

- 웹 통신 암호화
- 데이터 무결성
- SSL/TLS 기반

## 2FA

- 2단계 인증
- 추가 보안 계층
- 비밀번호 +  $\alpha$

## IDS/IPS

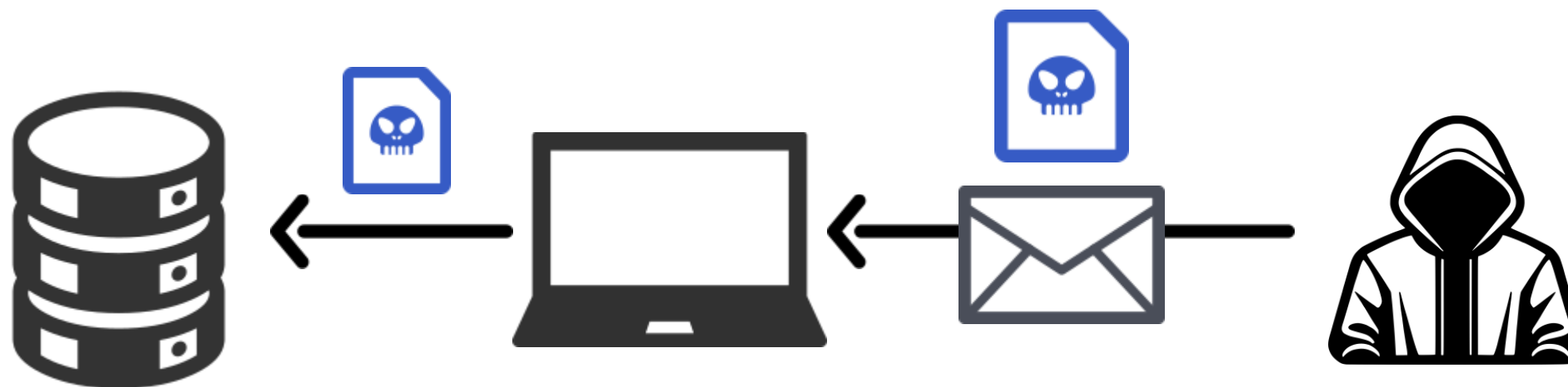
- 침입 탐지/방지
- 실시간 모니터링
- 자동 대응 가능

## 사례 분석



### 2016년 인터파크 개인정보 유출

- 공격 기술 : 이메일을 통한 악성코드 공격으로  
공유된 회사 전산망을 통해 DB서버에 액세스



- 대처 방안 : 이메일 악성코드 검사 강화, 직원 교육, 네트워크 세그멘테이션

# 사례 분석



## 2016년 인터파크 개인정보 유출

---

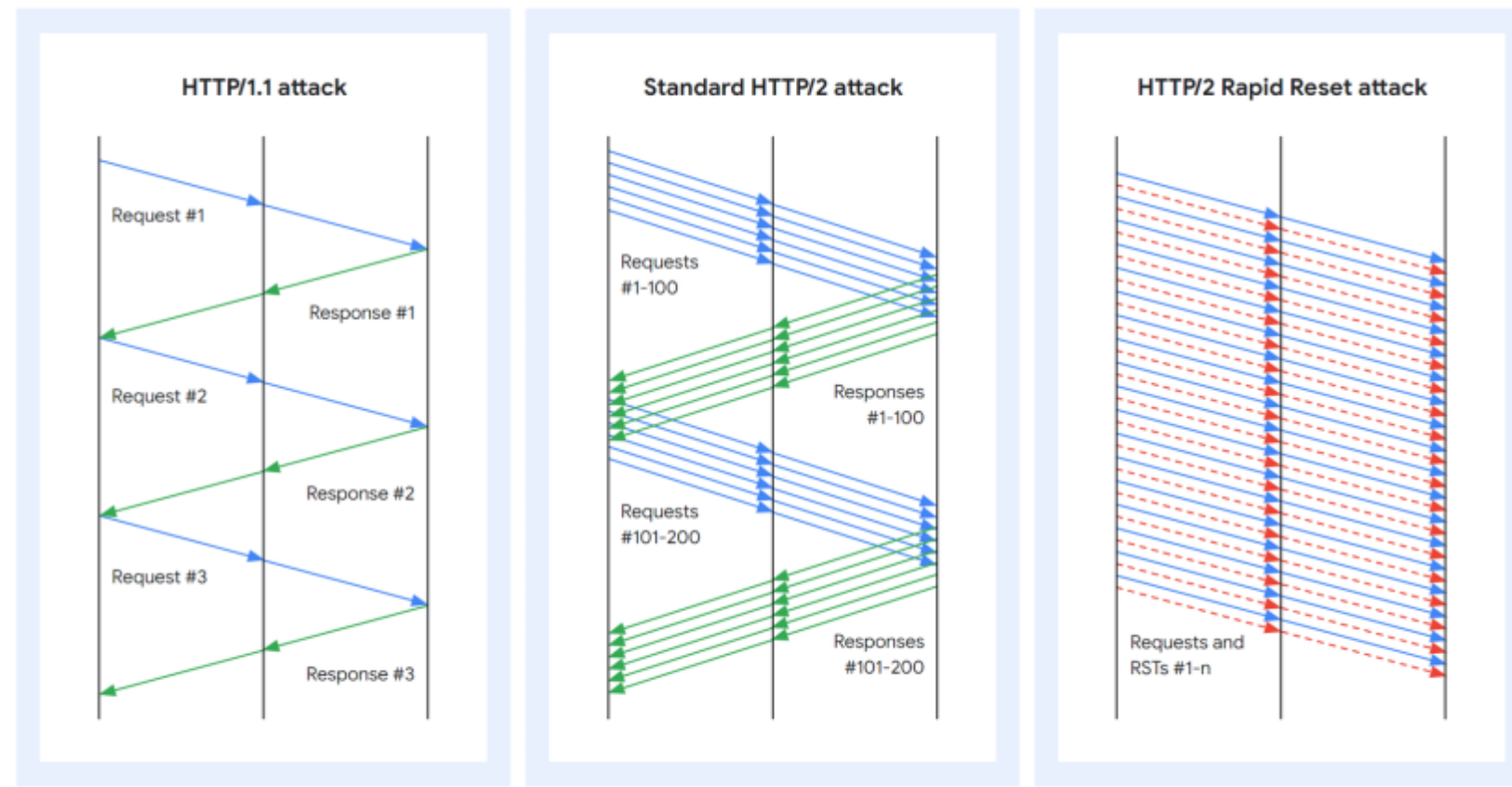
- 피해 규모: 1030만 명의 개인정보 2540만 건 유출
  - 유출 정보: 아이디, 비밀번호, 이름, 성별, 생년월일, 전화번호, 이메일
  - 결과: 총 45억원의 과징금 처분 (당시 개인정보 유출 사고로 부과된 역대 최고액)
- 
- 사건의 의의: 대규모 개인정보 유출 사고의 대표적 사례
  - 교훈: 이메일을 통한 악성코드 유포의 위험성 부각
  - 대응 방안: 이메일 보안 강화, 직원 교육 필요성 증대
  - 영향: 개인정보 보호법 강화 계기

# 사례 분석



## 2023년 10월 Google DDoS 공격

- 공격 기술: HTTP/2 프로토콜 결함 악용
- 공격 규모: 398 million RPS 이상
- 특징: Rapid Reset 기술 사용



# 사례 분석



## 2023년 10월 Google DDoS 공격

---

- 피해 여부: Google Cloud의 성공적인 방어
- 대응 방법: 글로벌 로드 밸런싱 인프라로 트래픽 완화
- 의의: 역대 최대 규모 DDoS 공격 방어 성공 사례
- 교훈: 지속적인 보안 시스템 업데이트의 중요성



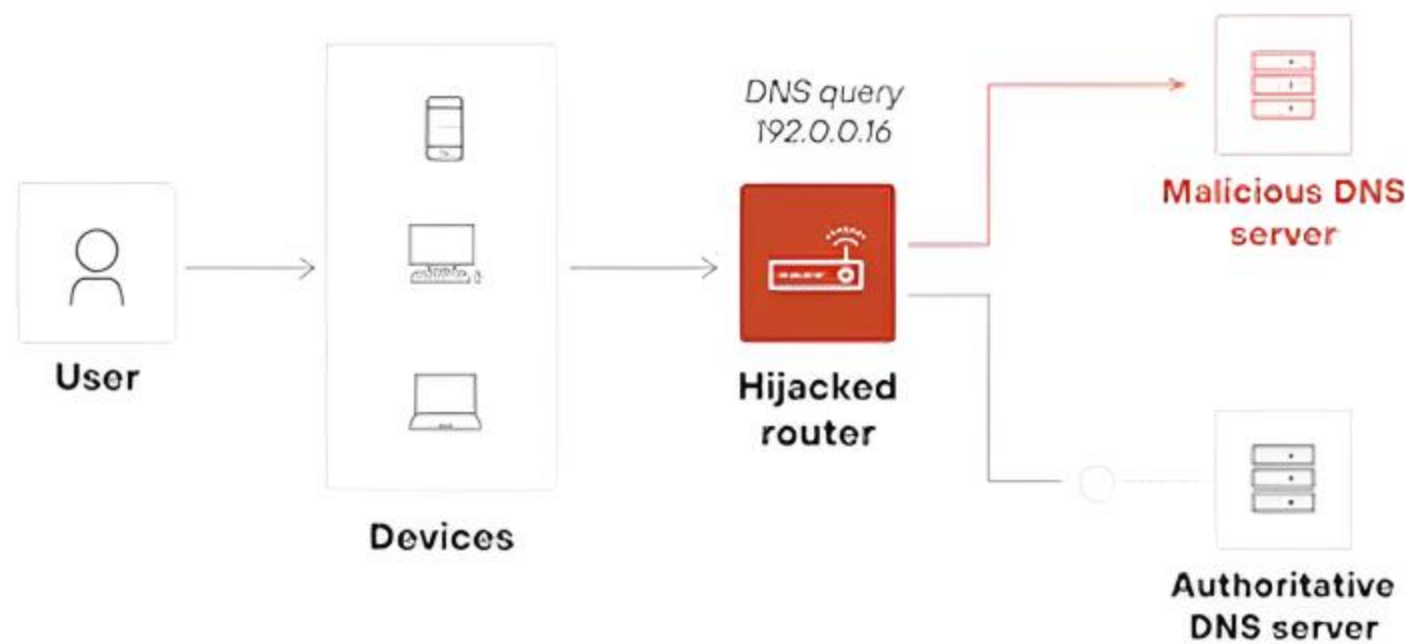
# 사례 분석



## 2024년 미국 통신 해킹

- 라우터 취약점(버퍼 오버플로) 악용
- 제로데이 취약점 공격으로 악성 파일 변조

### Router DNS hijack





# 사례 분석



## 2024년 미국 통신 해킹

---

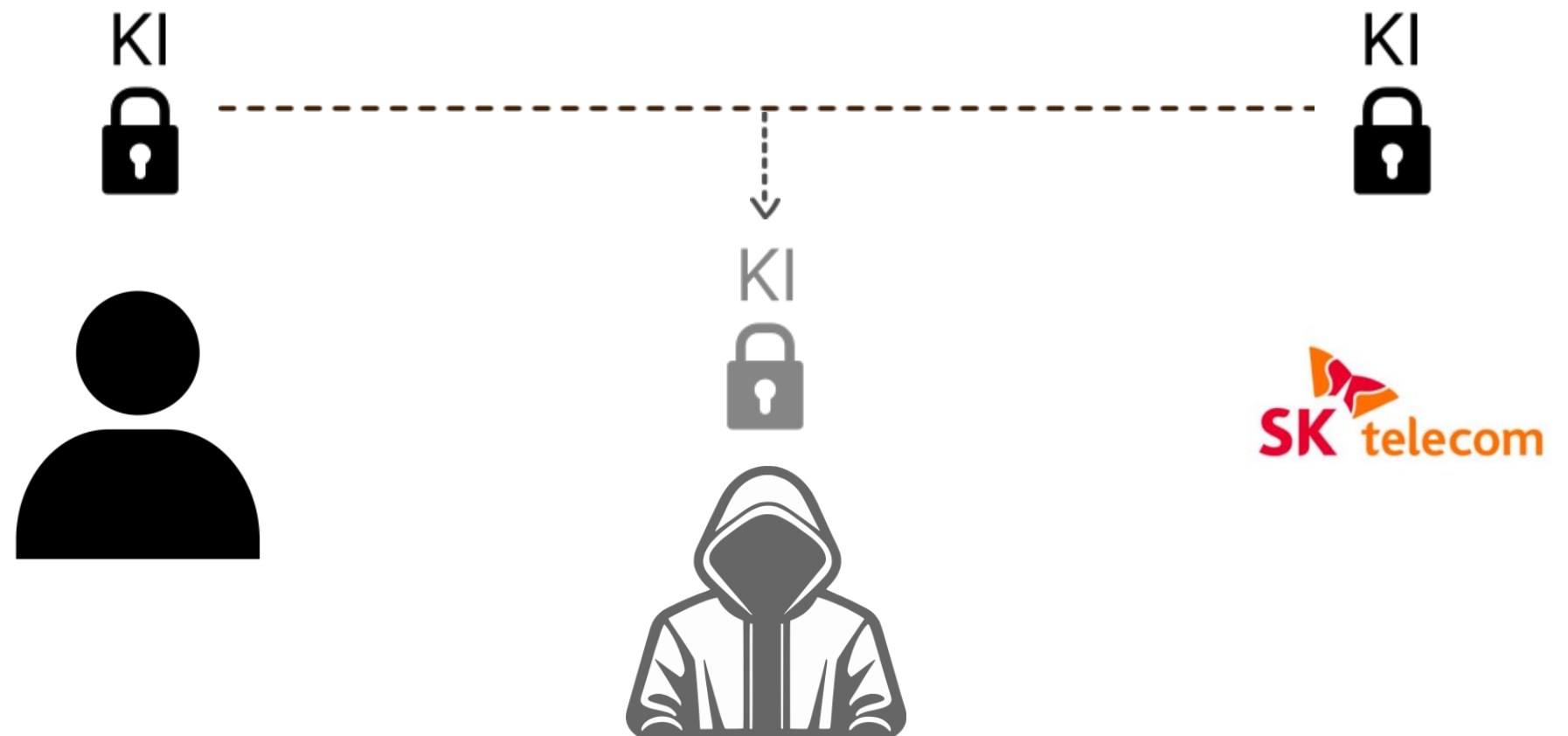
- 워싱턴 D.C. 메트로 지역 100만 명 이상 영향
- 통화 기록, 시간 정보, IP 주소, 전화번호 유출
- 개인정보 및 통신 비밀 침해 심각
- 국가 안보 위협 가능성 제기

# 사례 분석



## SKT 유심정보 해킹

- BPFDoor 악성코드 사용
- 리눅스 환경 패킷 필터 악용
- Symmetric key 인증 방식 취약점



# 사례 분석



## SKT 유심정보 해킹

---

- 2500만 유심정보 유출
- 개인정보 및 통신 보안 위협
- 군사 보안 문제로 확대
- 추가 조사 진행 중

# ■ 보안의 중요성

## 기술 발전과 보안 위협

- 기술 진보에 따른 새로운 보안 위협 등장
  - 사이버 공격의 복잡화 및 지능화
- IoT, 클라우드 등 신기술 보안 취약점 증가
- 제로데이 취약점 등 예측 불가능한 위협 증가

## 공동 책임의 필요성

- 기업: 강력한 보안 시스템 구축 및 유지
  - 정부: 관련 법규 제정 및 규제 강화
- 개인: 보안 의식 제고 및 기본 수칙 준수
- 전문가: 최신 보안 기술 연구 및 개발

## 예방 중심 보안문화

- 사전 위험 평가 및 취약점 분석 정례화
- 임직원 대상 정기적인 보안 교육 실시
  - 보안 정책 수립 및 지속적인 개선
- 모의 해킹 등을 통한 실전 대비 훈련

## 지속적인 대응 체계

- 24/7 보안 모니터링 시스템 운영
- 인공지능 기반 위협 탐지 기술 도입
- 신속한 보안 패치 및 업데이트 체계 구축
- 사이버 보안 전문 인력 양성 및 확보

# ■ 기술적 대응 방안

## 패치

- 정기적 보안 업데이트
- 제로데이 취약점 대응
- 자동 패치 시스템 구축
- 패치 관리 정책 수립
- 레거시 시스템 관리

## 다중 인증

- 생체 인증 기술 도입
- 싱글 사인온(SSO) 구현
- 권한 관리 체계 강화
- 인증 정책 주기적 검토

## 모니터링

- 실시간 로그 분석
- 이상 트래픽 탐지
- AI 기반 위협 인텔리전스

## 암호화

- 데이터 전송 시 암호화
- 저장 데이터 암호화
- 키 관리 시스템 운영



# ■ 제도적 대응 방안

## 개인정보보호법

- 개인정보 수집, 이용, 제공 규제
- 정보주체의 권리 보장 강화

## 정보통신망법

- 정보통신서비스 제공자의 책임 강화
- 개인정보 유출 시 과징금 부과
- 이용자의 권리 보호 확대
- 정보보호 관리체계 인증 의무화

**KISA**

- 사이버 보안 정책 수립
- 보안 기술 연구 개발
- 침해사고 대응 지원
- 정보보호 인력 양성
- 국민 대상 보안 교육

## 사이버수사대

- 사이버 범죄 수사 전담
- 디지털 포렌식 기술 활용
- 해킹 사건 추적 및 검거

## 국제협력

- 국제 사이버보안 협약 참여
- 정보 공유 네트워크 구축
- 글로벌 보안 기업과 협력



# 사용자 측 대응 방안



비밀번호 관리 철저

---



공용 와이파이 사용 주의

---



의심스러운 앱 설치 금지

---



피싱 문자 클릭 주의

---

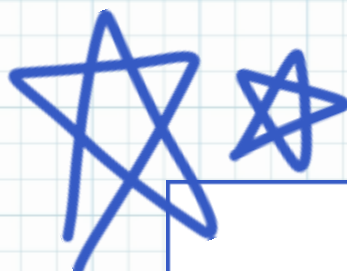





정기적인 보안 업데이트



# 결론 및 향후 과제

---

- 
- 
- 
- 네트워크 보안의 중요성 지속 증가
  - 기술, 제도, 사용자 측면의 종합적 대응 필요
  - 새로운 위협에 대한 지속적 모니터링 및 대비 강화
  - 국제 협력을 통한 글로벌 사이버 보안 체계 구축
- 

## 참고문헌



네트워크 보안 개념 :

<https://www.ibm.com/kr-ko/topics/network-security>

---



인터파크 개인정보 유출 :

<https://www.catchsecu.com/archives/22388>

---



구글 DDos 방어 :

<https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack?hl=en>

---



미국 통신 해킹 :

[https://en.wikipedia.org/wiki/2024\\_United\\_States\\_telecommunications\\_hack](https://en.wikipedia.org/wiki/2024_United_States_telecommunications_hack)

---



SKT 유심정보 해킹 :

<https://www.youtube.com/watch?v=4Xze-DEGN7c>

## 참고문헌



<https://velog.io/@doolchong/CIA-%ED%8A%B8%EB%9D%BC%EC%9D%B4%EC%96%B4%EB%93%9C>

---



<https://www.fortinet.com/kr/resources/cyberglossary/advanced-persistent-threat>

---



<https://n.news.naver.com/mnews/article/032/0002716609?sid=101>

---



<https://blog.naver.com/techref/223235223764>

---



<https://velog.io/@shkim0730/ddos-protection>