



# 사이버 보안 (Cyber Security)

[1강] 사이버 공격과 사이버 보안의 개념과 역사



이 자료는 Elixir의 사전 서면 승인 없이 외부에 배포하기 위해  
그 일부를 배포, 인용 또는 복제 할 수 없습니다.

© Copyright Elixir

## 학습 목표

---



### 학습 목표

사이버 공격과 사이버 보안의 개념에 대해 알아봅니다.

사이버 공격과 사이버 보안의 역사를 알아봅니다.

# 사이버 공격 vs 사이버 보안



# 사이버(Cyber)

사이버는 ‘컴퓨터의~’, ‘인터넷의~’, ‘가상현실의~’ 등 가상공간(Cyberspace)과 관련된 것을 의미하는 접두어로서, 인터넷의 발달로 사이버 대학교, 사이버 경찰청 등 다양한 종류의 학교나 기관이 가상공간에 존재하게 되었다.



인사혁신처  
사이버국가고시센터

시험안내 원서접수 시험문제/정답 서류전형/면접시험 채용후보자 시험통계/자료실

최근소식 및 공지

공채5급(외교관)	공채7급	공채9급	경력채용	+
◀ 2023년도 국가공무원 공개경쟁채용시험 등 계획 공고 2023.01.02				
◀ 2023년도 국가공무원 공채·경채 및 외교관후보자 선발시험 장애인 등 응시자 편의제공 안내 2023.01.02				
◀ 2023년도 국가공무원 5급 민간경력자 일괄채용시험 시행계획 공고 2023.04.21				
◀ 2023년도 국가공무원 7급 민간경력자 일괄채용시험 시행계획 공고 2023.04.21				
▣ 2023년도 중증장애인 국가공무원 경력경쟁채용 면접시험 편의제공 대상자 명단 안내 2023.06.02				
▣ 2023년도 국가공무원 5급 공채 및 외교관후보자 선발 제2차시험 코로나19 방역 주요사항 및 면… 2023.06.02				
▣ 2023년도 중증장애인 국가공무원 경력경쟁채용 면접시험 추가 응시자 결정 및 명단 공고 2023.06.01				

홈 | 로그인 | 회원가입 | 시험종합안내 | 온라인 민원

Elixirr

## 스토리와 함께 배우는 데이터 분석과 인공지능

단순히 데이터 분석 코딩 수업이 아닌, 프로젝트를 처음부터 끝까지 수행해봄으로써 실제 생활이나 업무에서 활용할 수 있는 능력을 기를 수 있습니다

### 강의찾기

전체보기 >

- 공무원인사제도
- 합격증명서교부
- 책임있는 인공지능
- 노코드 클라우드 마신러닝
- 파이썬으로 배우는 아르테미스 담당사
- 엑셀로 만든 파워앱

2023년 국가공무원 민간경력자 일괄 채용시험 가이드북

공직 비전 인재상, 공직문화, ... & 사회인 등을 확인하세요.

4 Elixirr

# 사이버 공격이란? (Cyber Attack)

사이버 공격은 컴퓨터 또는 전산화된 정보 시스템의 요소를 표적으로 삼아 데이터를 변경, 파괴 또는 유출하고 네트워크를 악용하거나 손상하고자 의도한 행동을 말한다.



©Matejmo/Getty Images

## 사이버 공격의 유형

- 대상 컴퓨터를 비활성화하거나 오프라인으로 만드는 공격
- 대상 컴퓨터의 데이터에 접근해 관리자의 권한을 얻는 것이 목표인 공격

# 사이버 보안 (Cyber Security)

사이버 보안은 컴퓨터, 네트워크, 소프트웨어 애플리케이션, 중요 시스템 및 데이터를 잠재적 디지털 위협으로부터 보호하는 행위이다. 조직은 데이터에 보안을 적용하여 고객의 신뢰를 유지하고 규제를 준수할 책임이 있다.



[사진: 셔터스톡]

## 사이버 보안이 중요한 이유

- 침해로 인한 비용 방지 또는 절감 - 고객 신뢰 유지 및 사업 운영 중단 최소화
- 규제 요구사항 준수 - 유럽 데이터 보호 규제(GDPR) 준수
- 진화하는 사이버 위협 완화 - 진화하는 사이버 공격 기술과 도구를 따라잡기 위한 사이버 보안 조치를 채택 및 업그레이드해야 한다.

<https://www.digitaltoday.co.kr/news/articleView.html?idxno=424285>

# 사이버 공격과 사이버 보안의 역사

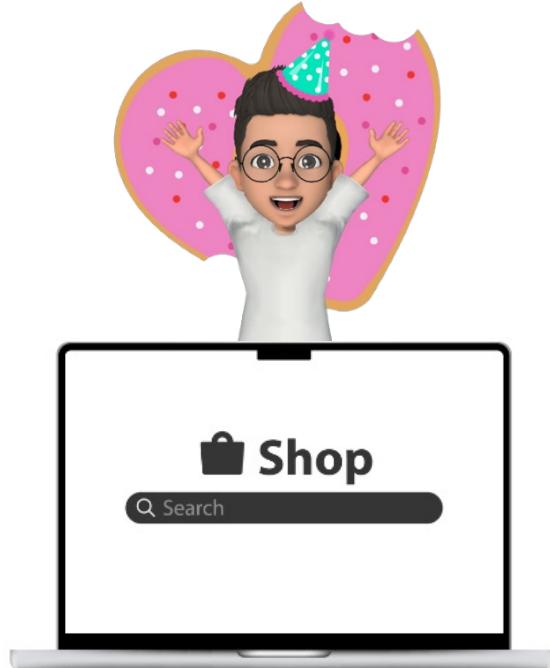


# 사이버 공격과 보안의 역사 - (1)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.

## 1960년대 : 사이버의 탄생

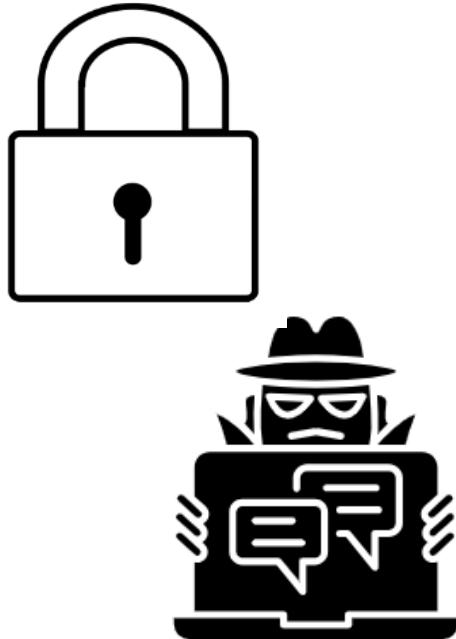
- 사이버 보안이 중요한 개념이 되기 시작한 시점은 컴퓨터가 연결되어 네트워크를 구성하게 되면서부터이다.
- 첫번째 컴퓨터 네트워크와 모뎀은 1950년대에 개발되었지만 오늘날 우리가 말하는 인터넷이 구축되기 시작한 때는 1960년대이다.
- 인터넷의 초기 형태가 탄생하기 전에는 컴퓨터를 해킹하는 유일한 방법은 컴퓨터에 물리적으로 액세스하는 것이다. 사실상 무단 침입 행위에 가까웠다.
- 1960년대 후반에 미국은 컴퓨터가 장거리에서도 서로 통신할 수 있는 시스템을 개발했고 그 이전에는 대부분의 컴퓨터는 동일한 장소에 있을 때만 네트워크를 구성할 수 있었다.



<https://nordvpn.com/ko/blog/the-history-of-cybersecurity/>

# 사이버 공격과 보안의 역사 - (2)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.



## 1970년대 : 새로운 라이벌 등장

- 멀웨어와 사이버 보안 소프트웨어라는 두 개의 라이벌이 탄생한 시대라고 말할 수 있다.
- 스스로 작동하고 자가 복제하며 다른 장치로 확산되는 특징을 가지는 멀웨어의 탄생은 사이버 범죄가 탄생하게 된 계기였다.(크리퍼의 탄생)
- 바이러스를 추적하고 제거하는 ‘리퍼’라는 프로그램이 탄생하였고 이것은 사이버 보안의 시작이었다.
- 1979년 미국 고등학생 케빈 미트닉이 미국 중요 기관의 해킹 사건 - 높은 수위의 처벌 케빈 미트닉이 사용한 소셜 엔지니어링 기법과 휴먼 에러는 현재도 사이버 범죄에 악용
- 암호화의 표준화 - 데이터 암호화 표준(DES) 개발에 따라 사이버 보안이 한단계 발전

<https://nordvpn.com/ko/blog/the-history-of-cybersecurity/>

# 사이버 공격과 보안의 역사 - (3)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.



## 1980년대 : 사이버 보안이 주류에 편입

- 정부와 금융 기관 등이 인터넷이 연결된 컴퓨터를 사용 - 해커의 정보 탈취 가능성, 바이러스 및 멀웨어로 인한 시스템 중단이 발생할 가능성이 높아졌다.
- AT&T, 내셔널 CSS, 기타 주요 기관에 대한 사이버 공격 - 언론의 집중 보도
- '사이버'라는 개념이 대중에게 확실히 각인 - 많은 사람들이 인터넷의 장점과 위험성에 대해 인식
- 비엔나 바이러스 출현 및 이를 제거하는 백신 소프트웨어 개발 - 바이러스 백신 소프트웨어
- 다양한 신규 보안 소프트웨어 개발 및 판매 - 사이버 보안의 시작

<https://nordvpn.com/ko/blog/the-history-of-cybersecurity/>

## 영화 '위험한 게임'

1980년대에는 미국 주요 기관에 대한 사이버 공격이 언론의 관심을 받은 가운데 1983년에는 핵 무기 시스템에 액세스하는 해커를 다룬 영화 '위험한 게임'이 개봉함에 따라 해커라는 개념이 주류로 등장하였다.



<https://www.youtube.com/watch?v=DiMGhHbZloY>

0:44 – 6:15

# 사이버 공격과 보안의 역사 - (4)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.



## 1990년대 : 인터넷의 시작

- 뉴노멀 - 마이크로소프트의 윈도우 운영체제를 대중에게 보급, 인터넷 익스플로러 출시  
인터넷의 접근성이 높아져 모든 사람이 이메일을 보내고 자료 조사와 온라인 게임을 수행
- 이메일의 위험성 - 이메일을 통한 사이버 공격인 멀리사 바이러스 출현
- 멀리사 바이러스 - '중요 메시지'라는 제목으로 이메일 전송, 첨부 파일에 멀리사 바이러스 포함, 파일을 열면 멀웨어가 장치에 설치되고 다양한 문제 발생
- 새로운 인터넷 통신 네트워크로 인해 멀웨어가 빠르게 전파
- 보안 프로토콜도 소셜 엔지니어링 기법 앞에서 무력

<https://nordvpn.com/ko/blog/the-history-of-cybersecurity/>

# 사이버 공격과 보안의 역사 - (5)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.



## 2000년대 : 새로운 수준의 연결성

- 사이버 범죄의 진화 - 이메일의 위험성 인식, 이메일 서비스에서 첨부 파일을 스캔
- 해커는 이메일 서비스의 보안 조치를 피하기 위해 자신이 만든 웹 페이지를 방문하도록 유도 - 이메일이 은행이나 정부 기관에서 보낸 것처럼 위장 - 사용자가 해당 링크를 클릭하도록 유도 - 장치에 멀웨어 설치 또는 개인 정보 데이터 유출
- 소셜 엔지니어링 - 보안 소프트웨어가 인지하지 못하는 방식으로 해킹
- 미국 국토안보부 - 국가 사이버 보안 부서 창설
- 사이버 보안의 진화 - 무료 보안 소프트웨어 배포, 다양한 보안 도구 사용
- VPN 출시 - 사용자가 온라인에서 전송하고 수신하는 데이터를 암호화하는 애플리케이션

<https://nordvpn.com/ko/blog/the-history-of-cybersecurity/>

# 사이버 공격과 보안의 역사 - (6)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.



## 2010년대 : 사이버 공간에서의 갈등

- 사이버 전쟁

2010년 이란의 핵 프로그램 관련 컴퓨터가 멀웨어에 감염되어 네트워크 전반에서 중단 미국과 이스라엘의 보안 부대가 만들어 낸 것이라고 추정 - 정부가 사이버 공격을 무기화해 경쟁국에 사이버 공격을 수행 - 사이버 보안은 국가 보안과 관련된 문제로 대두

- 러시아와 미국이 서로 사이버 보안 감시 - 미국 국토안보부는 국가 사이버 보안 부서 창설
- 개인 정보 유출 피해 - 페이스북, 구글 등이 사용자의 방대한 양의 개인 정보 수집하여 타겟 광고 송출 및 제3자 광고업체에 판매 -> 프라이버시 제품이라는 새로운 보안 시장
- 기업의 데이터 유출 사건 - 2019년 페이스북 데이터 유출, 2019년 퍼스트 아메리칸 데이터 유출, 2013년 야후 데이터 유출
- 위의 사례에서 알 수 있듯이 개인 정보를 보호하고 데이터 수집을 제한하는 것은 기본 원칙일 뿐만 아니라 보안 문제이다.

# 사이버 공격과 보안의 역사 - (7)

인터넷의 탄생부터 글로벌 사이버 분쟁까지 사이버 보안의 역사를 10년 단위로 살펴본다.

## 2020년대 이후

- 다시 시작되는 뉴 노멀 - 2020년 초의 코로나 팬데믹 - 컴퓨터와 인터넷이 확산되는 계기
- 원격 근무로 전환  
수백만 명의 사람이 집에서 회사 네트워크와 데이터베이스에 접속, 업무에 개인 장치를 사용 - 해커에게 엄청난 기회 - 보완 소프트웨어가 설치된 업무용 장치보다 개인 장치가 사이버 공격에 취약 - 2020년에만 비즈니스의 절반이 랜섬웨어 공격 피해 -피싱 사기 급증
- 인프라 공격 - 2021년 미국 가스 회사 콜로니얼 파이프라인 랜섬웨어 공격  
시스템이 재가동되자 자동차에 연료를 채우려는 사람들이 몰려들어 가스 가격이 급상승하고 미국 동부 해안에서 혼란 발생
- 사이버 전쟁 - 2022년 우크라이나 vs 러시아 전쟁  
전쟁 발발 전에 우크라이나는 사이버 공간에서 공격을 받고 있는 상태  
러시아의 사이버 공격에 대비하기 위해 리투아니아를 중심으로 유럽 국가들이 사이버 신속 대응팀 창설

