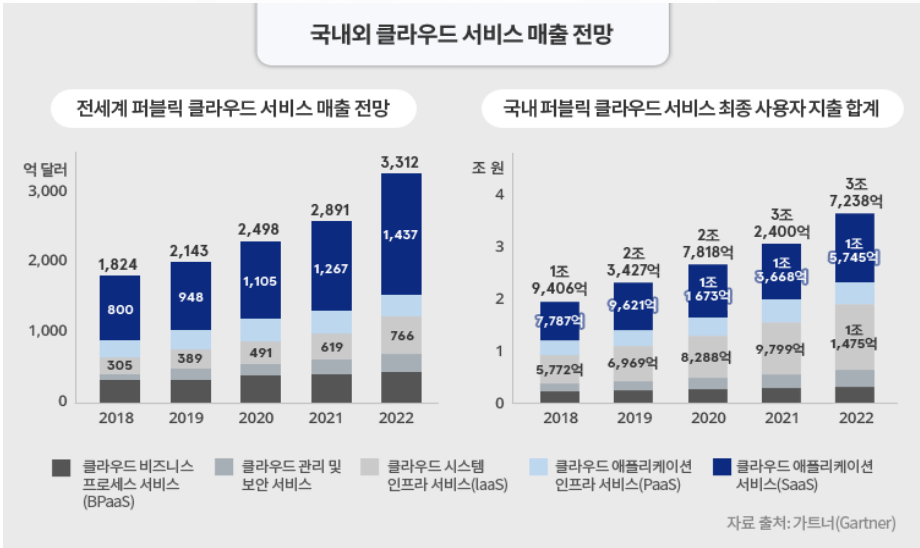
의료분야 개인정보 유출사고 대응방안

KISA 개인정보조사단 이 준

디지털 전환 가속화


D.N.A 생태계, 데이터 댐
5G
5G, IoT, 센서, 로봇 등을 활용한 데이터 수집
데이터 활용 및 AI 혁신 서비스 창출
DATA
AI
데이터 축적 및 가공/결합
자율주행차
미세먼지 저감
스마트 공장
AI기반질환예측
지능형 CCTV
지능형 범죄분석
에너지 절감
디지털 정부

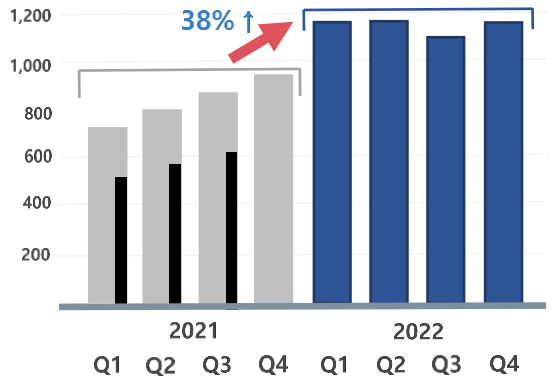

국내외 클라우드 서비스 매출 전망
전세계 퍼블릭 클라우드 서비스 매출 전망
억 달러
3,000
2,000
1,000
0
1,824
800
305
2,143
948
389
2,498
1,105
491
2,891
1,267
619
3,312
1,437
766
2018
2019
2020
2021
2022
국내 퍼블릭 클라우드 서비스 최종 사용자 지출 합계
조 원
4
3
2
1
0
1조 9,406억
7,787억
5,772억
2조 3,427억
9,621억
6,969억
2조 7,818억
1조 1,673억
8,288억
3조 2,400억
1조 3,668억
9,799억
3조 7,238억
1조 5,745억
1조 1,475억
2018
2019
2020
2021
2022
클라우드 비즈니스 프로세스 서비스 (BPaaS)
클라우드 관리 및 보안 서비스
클라우드 시스템 인프라 서비스(IaaS)
클라우드 애플리케이션 인프라 서비스(PaaS)
클라우드 애플리케이션 서비스(SaaS)
자료 출처: 가트너(Gartner)

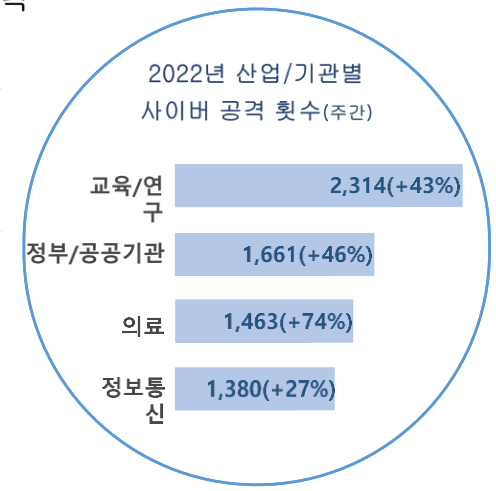
최근 인터넷 정보보호 동향

- 2022년 세계 사이버 공격 38% 증가, 교육·정부·의료 분야 공격 증가

- 악성 이메일과 피싱은 여전한 감염의 주요 요인
  - **2022년(7~10월) 피싱 공격 비율 1.3배 증가, 모든 공격의 76% 차지**

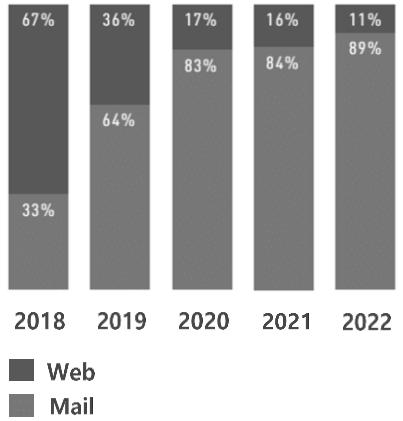
[2021~2022 글로벌 주간 평균 사이버 공격 횟수]





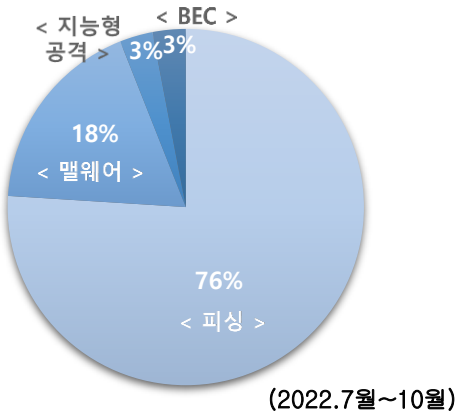
* Source: Check Point, 2023.2

[이메일 악성파일 전송 비율]



* Source: Check Point, 2022.8

[사이버 공격 유형]

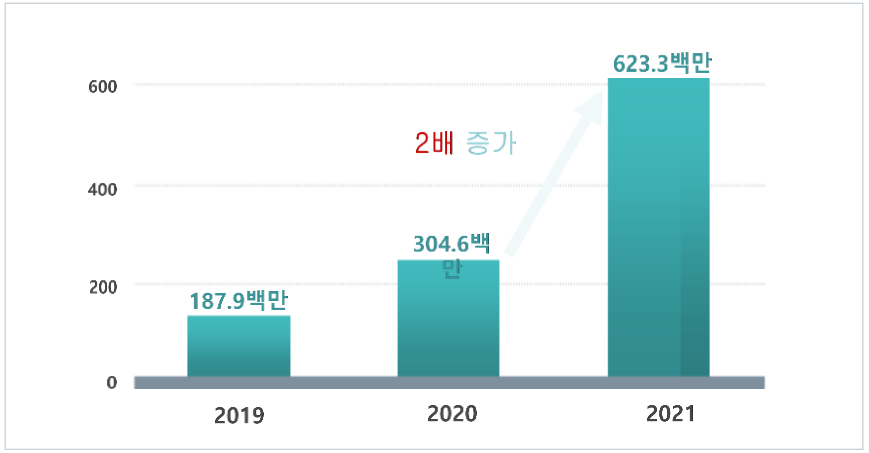


* Source: Acronis, 2023.1

최근 인터넷 정보보호 동향

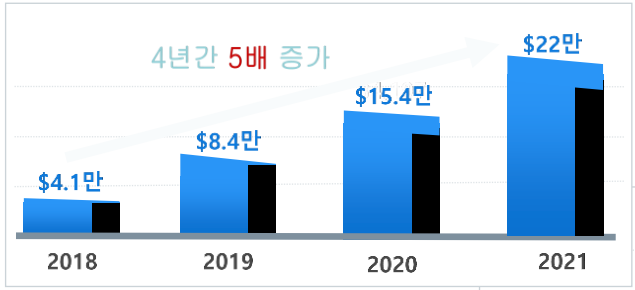
- 전 세계 랜섬웨어 공격 2배 증가
  - 병원, 의료센터 및 공공기관 등을 주요 공격 대상으로 집중 공격
  - 의료기관의 경우 랜섬웨어 공격 2배, 개인정보 유출 11배 증가(2016년→2021년)
- 랜섬웨어 평균 협상 금액 건당 약 3억원에 육박

[랜섬웨어 공격 건수]



* Source: Statista, 2022.8

[랜섬웨어 평균 협상 금액(건당)]



* Source: coveware 2021

[랜섬웨어 피해금액(전망)]

* Source: Cyber Crime magazine, 2022.6

2023년도 사이버 보안 위협 전망

1

국가·산업 보안을 **위협**하는
글로벌 해킹 조직의 공격 증가

2

재난, 장애 등 민감한 **사회적 이슈를**
악용한 사이버 공격 지속

2023년도 사이버 보안 위협 전망

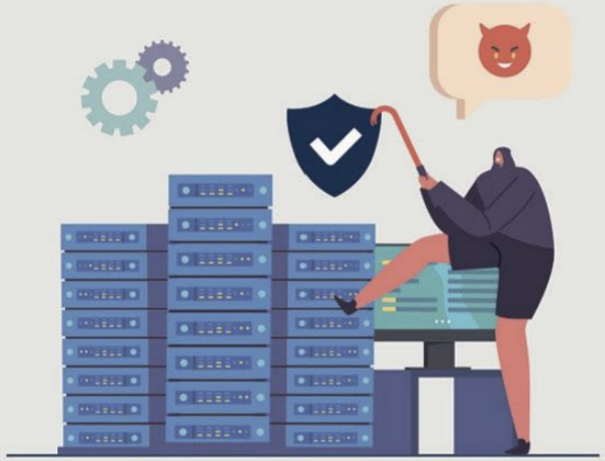
3

지능형 지속 공격과 **다중협박**으로
무장한 **랜섬웨어의 진화**

4

디지털 시대
클라우드 전환에 따른 **위협 증가**

5



갈수록 복잡해지는 **기업의**
SW 공급망과 **위협 증가**

주요 위반 사례

- 아주대학교의료원 : 고유식별정보 처리 제한
- 성형외과의원 : 영상정보처리장치(CCTV), 마케팅 관련 동의, 파기
- 순천제일병원 : 정보주체의 개인정보자기결정권 침해
- 서울대학교의료원 : 고유식별정보 처리 제한, 안전성 확보조치, 유출 통지
- 비대면진료 플랫폼 : 안전성 확보조치, 포괄동의, 처리방침 공개 미흡 등

개인정보 보호법 개정에 따른 업무의 변화

⑤ 형벌 중심을 경제제재 중심으로 전환

☑ (이 유) 개인정보 침해에 대한 책임이 개인에 대한 형벌 중심으로 이루어지고
실질적 책임이 있는 기업에 대한 경제제재는 낮은 수준에 머물러,
개인정보 보호에 대한 기업의 투자를 촉진하지 못하는 한계

- 경제적 제재 수단인 과징금은 '위반 행위 관련 매출액'의 3% 이하로 정보통신서비스 제공자에게만 부과되고 있어 실효성 논란이 제기

  ※ (EU) GDPR, 2천만 유로 또는 전 세계 총 매출액의 4% 중 높은 금액을 기준으로 부과

  → 브리티시 항공 50만명 유출(2,700억원 과징금, 영국), 구글 동의 방식 미 준수(650억원 과징금, 프랑스)

☑ (개 정) 형벌 중심을 경제 제재 중심으로 전환하여 실효성 제고 ['23. 9월 시행]

- 형벌 폐지 동의 없이 개인정보 수집, 개인정보 미파기, 개인정보 유출 시, 형사 처벌 폐지

- 과징금 확대 정보통신서비스 제공자등에 적용되는 과징금을 개인정보처리자로 확대하고, 과징금의 부과 기준은 전체 매출액의 3% 이하로 상향

개인정보 보호법 개정에 따른 업무의 변화

⑥ 민감정보 공개 가능성 고지 의무 신설

☑ (이 유) SNS·온라인 지도 등 온라인 공유 서비스 이용 시, 민감정보를 포함한 대량의 개인정보가 일상적으로 처리되고 있으나, 이에 따른 위험성 등에 대한 고지가 이루어지지 않음

☑ (개 정) 서비스 제공 과정에서 정보주체에 의하여 민감정보가 공개될 위험이 있는 경우 공개 가능성 및 비공개 선택 방법에 대한 통지 의무 신설 ['23. 9월 시행]

⑦ 이동형 영상정보처리기기 운영 기준

☑ (이 유) 현행법은 고정형 영상기기(CCTV)만을 규율하고 있어, 드론, 자율주행차 등 이동형 영상정보처리기기의 특성에 맞는 기준제시에 한계

- 현재 이동형 영상기기를 통한 개인정보 수집·이용 시 일반 규정이 적용되어 정보주체의 개별적 동의를 요하는 등 산업적 측면에서 유연한 대처에 한계

☑ (개 정) 공개된 장소 등에서 업무 목적으로 이동형 영상정보처리기기를 이용하여 개인영상정보를 촬영하는 행위를 원칙적으로 제한하되, ['23. 9월 시행]

- 정보주체의 동의가 있거나, 촬영사실을 표시하였음에도 거부의사를 밝히지 않은 경우 등 예외적 허용

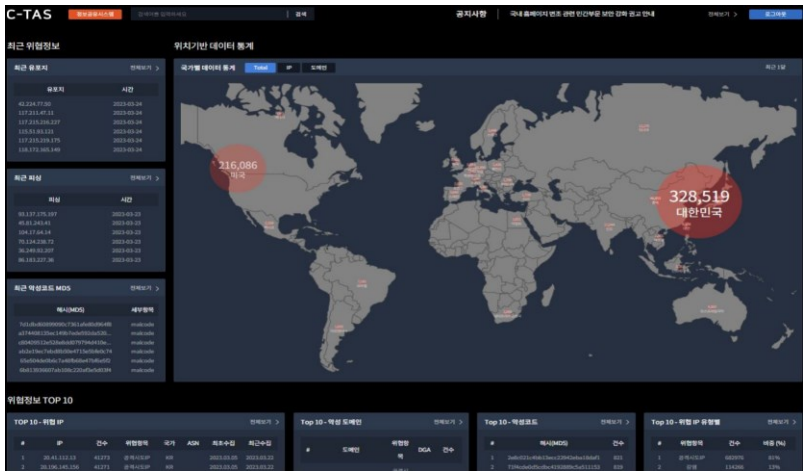
KISA

[참고] C-TAS 소개

기업의 신속한 침해사고 탐지와 대응을 지원하기 위한
사이버 위협정보 분석 · 공유 시스템(C-TAS) 운영('14년 8월~)

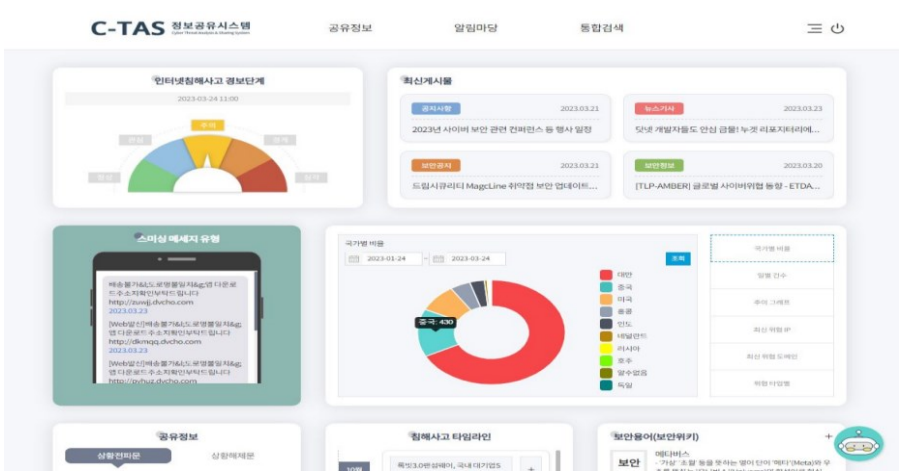
- API로만 정보를 공유하던 공유형 C-TAS 방식에서 원하는 산·학·연 모두가 사이버 위협정보를 제공받을 수 있도록 개방형 홈페이지 개설 ·오픈(22년 1월~)

공유형 C-TAS



공격시도 IP, 경유지, 유포지, 악성코드 등 40종 정보 공유

개방형 C-TAS



긴급 상황전파 서비스, 최신뉴스, 위협정보(악성코드/스미싱 등)

KISA 한국인터넷진흥원

감사합니다 !