

비상경제 중앙대책본부

21-42-5

(의결, 공개)

---

# 랜섬웨어 대응 강화방안

---

2021. 8. 5.

관계부처 합동

# 랜섬웨어 대응 강화방안(요약)

## I 추진 배경 및 현황

□ 최근 국내·외에서 해킹으로 피해자의 데이터를 암호화하고, 이를 풀어주는 대가로 돈을 요구하는 랜섬웨어(Ransomware) 피해 증가

○ 미국에서 랜섬웨어 공격은 송유관·육가공업체 등 기반시설과 국민 생활에 밀접한 분야가 목표가 되어 국가적 혼란 야기

\* 송유관회사(5.7) → 최대 육가공업체(5.30) → 뉴욕시 법무전산시스템(6.7) 등

○ 우리나라도 피해가 증가 중이며, 보안 투자여력이 부족한 중소기업을 중심('21.7월까지 81%)으로 다양한 분야\*에서 피해 발생

\* 자동차 부품 제조기업(5.2) → 배달대행 기업(5.15) → 의료기관(5.22) 등

▶ 우리나라 랜섬웨어 신고는 39건('19) → 127건('20) → 97건('21.7월)이지만, 민간 보안업체의 통계와 차이 → 신고를 기피하는 경향이 큰 것으로 파악

▶ 국내 기업이 경험한 침해사고 중 59.8%가 랜섬웨어('20년 정보보호실태조사)

□ 랜섬웨어 공격은 '서비스형 랜섬웨어\*' 활성화로 범죄형태가 분업화·조직화되고 있으며, 지속적인 취약점 탐색(APT) 등 갈수록 지능화

\* 별도의 프로그래밍 지식 없이도 비용을 지급하면 서비스 형태로 제공되는 랜섬웨어

□ 그간 우리나라는 디지털 전환에 대비하여, '디지털 뉴딜', 'K-사이버 방역' 등 추진으로 사이버보안 경쟁력을 개선\*하였지만,

\* 국제전기통신연합(ITU) 정보보호지수 순위 상승 ('19년 15위 → '21년 4위)

○ 랜섬웨어 공격의 영향·범위 확대 등에 대비, 대응을 지속 강화하여 개인·기업의 디지털 전환과 국가적 안전을 뒷받침할 필요

✓ 랜섬웨어는 복구가 어렵기 때문에 백업 등 **선제적 예방이 중요**

✓ 랜섬웨어는 **다양한 경로**를 통해 발생하기 때문에, 국가 기반시설 부터 중소기업·개인까지 **맞춤형 대응 지원체계** 구축 필요

✓ **진화하는 랜섬웨어**에 대응하여 지속적인 기술·기반 구축 등 **핵심 대응역량 제고** 필요

## II 목표 및 전략

목표

“랜섬웨어에 안심할 수 있는 디지털 환경 구축”

추진전략

■ [전략1: 예방] 국가중요시설-기업-국민 수요자별 선제적 예방



■ [전략3: 기반] 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고



■ [전략2: 대응] 정보공유-피해지원-수사 등 사고대응 쏠주기 지원



## III 주요 추진 내용

### [전략1] 국가중요시설 - 기업 - 국민 수요자별 선제적 예방

#### 1] 튼튼한 국가중요시설 관리 체계 구축

- (기반 시설) 정보통신기반시설의 범위를 확대하고, 예방체계 강화
  - 정유사(공정제어시스템)·자율주행 관제시스템 등 새로운 중요시설에 대한 기반시설 확대 지정을 검토('21~'22년)
  - 기반시설의 보호대책에 ①백업시스템 구축, ②위기발생시 복구방안, ③업무지속계획(BCP) 포함\* ('22년) \* 참고지침 마련·배포 → 보호대책 반영
  - 망 분리가 어려워 인터넷과 연결·사용 중인 공공분야 정보시스템의 외부 접점에 설치·운영 중인 보안장비·DMZ\* 구간 현장 점검 등 강화
    - \* Demilitarized Zone : 외부에 서비스 제공 시, 내부 자원을 보호하기 위해 내부망과 외부망 사이에서 접근 제한을 수행하는 영역
  - 기반시설 긴급점검\*과 모의훈련\*\* 추진('21년 민간분야 9개)
    - \* 민간 147개, 공공 277개('21.7월 현재) \*\* 화이트해커 활용 모의 침투 등
  - 랜섬웨어 등 최신 보안위협 관련 현장 점검·조치 근거\* 마련('21~'22년)
    - \* 정보통신기반보호법 개정 추진

- (軍, 연구기관 등) 정밀 점검 실시 및 긴급 대응반 운영
  - 국방정보체계, 軍 기반시설 제어시스템에 대한 취약점 점검을 실시하고, 사이버 특별훈련, 장병 보안교육 등 강화
  - 출연연(원자력연 등 26개), 과기원(4개)에 연구용서버 자가진단시스템\*을 구축하고, 모의훈련·취약점개선 등 강화된 보안대책 수립·적용('21년~)
  - \* 출연연구원, 4대 과기원 연구·개발용 서버에 대한 상시 원격 점검·분석 수행
- (공급망 및 공공 이메일 보안 강화) 기반시설에 구축된 SW·시스템의 공급망(SW업체 등)에 대한 보안 점검 체계 구축('22년~)
  - SW 개발 단계부터 보안강화를 위해 'SW 개발보안 허브' 구축(판교, '21.7월), SW·솔루션 설계-구현-유통 단계별 보안강화 지원('21년~)
  - 주 감염 경로인 이메일의 보안 강화 기술을 공공분야 적용 확대 검토('21년~)

## ② 중소기업 보안역량 지원 강화

- (중소기업 지원) 중소기업들의 업무중단, 데이터 유실 예방 강화를 위해 데이터 금고\* 구축을 통한 백업 지원('22년~)
  - \* 중소기업의 데이터 이중화 지원을 위해 클라우드(또는 하드웨어) 기반 백업 지원



- 민·관 합동으로 메일보안SW, 백신, 탐지·차단SW '랜섬웨어 대응 3종 패키지\*' 지원('21년 3천여개) 등 중소기업 지원 강화
  - \* ①보안제품, ②클라우드 기반 보안, ③원격 서버점검 등의 형태로 지원하며, 정부 지원과 별도로 민간 보안업체(11개)에서도 영세기업 대상 무료 보안솔루션 지원 동참
- 실시간 보안관제 등을 통한 '기술유출 방지'도 지원('21년~)
- '코로나백신' 접종 의료기관에 안티-랜섬웨어 SW 지원('21년~)

- (예방활동 강화) ISMS 기업의 심사시 예방활동 평가를 강화하고, 정보보호공시제(약 1천개, '21.12월 시행) 공시내용에 업무지속계획 포함

### ③ 대국민 랜섬웨어 면역력 향상

- (국민 보안성 향상) PC·IoT 기기의 랜섬웨어 취약 여부를 원격으로 진단·개선하는 '내 PC 돌보미 서비스' 지원('21년~)
- (인식제고) '예방 플레이북' 보급 등 전방위 예방 캠페인 전개('21년~)

## [전략2] 정보공유 - 피해지원 - 수사 등 사고대응 쏠주기 지원

### ① 정보 공유·협력 채널 강화

- (민·관 협력) 민간(C-TAS), 공공(NCTI) 사이버위협 정보공유 시스템을 상호 유기적으로 연동할 수 있는 체계 구축('22년~)
  - ※ 의료, 금융 등 분야별 정보공유분석센터(민간 분야)와 C-TAS 간에도 체계 연동 추진
  - C-TAS에 가상자산거래소, 유통·제조 분야 기업 등의 참여 확대
  - 웹사이트(2만여개) 탐지 결과, 국외 해킹정보 등 민간과 신속 공유('21년~)
- (국제 협력) 주요국 인터넷 보안기관(CERT), 사이버보안 협의체 ('한미 사이버 워킹그룹' 등)를 통해 랜섬웨어 정보를 신속 입수·분석

### ② 확산 방지 및 신속한 피해지원

- (확산 방지) 네트워크 트래픽, 행위·패턴 분석 등 AI 기술을 활용해 실시간 악성도메인 탐지·차단 실시('21년 말)
  - 백신 개발사와 협력하여 랜섬웨어 백신을 신속 배포
  - '랜섬웨어 대응사례 수집'과 피해기업에 대응방법 공유 강화('21년~)
- (전국단위 피해지원) 지역정보보호 지원체계\*와 연계, 피해 시 인력·장비를 현장 파견하여 피해극복을 지원하고, 적극 수사 의뢰('21년~)
  - \* 지역정보보호센터(전국 10개) 및 지역보안전문업체 보안전문가 활용

### ③ 2차 피해 방지를 위한 사이버공격 수사 강화

- (모니터링 강화) 다크웹 모니터링으로 해킹조직 감시를 강화하고, 노출된 개인정보 등은 관계부처와 공유 → 피해자의 2차 피해 방지 지원
- (수사 강화) 랜섬웨어 전담 수사체계 구축, 엄정 대응 강화('21년~)
  - 민간(☎118), 공공(☎111) 부문별 신고·대응을 지원, 수사기관과 정보공유
  - 인터폴 회원국들과 해킹조직 분석, 범죄자 공동검거를 강화하고, 수사공조 확대를 위해 유로폴과도 실무약정 체결 추진('21년~)

## [전략3] 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고

### ① 랜섬웨어 등 사이버공격 대응 핵심기술력 확보

- (탐지·차단·복구) 랜섬웨어 탐지·차단 기술을 개발('21년~)하고, 랜섬웨어 복구기술을 개발하여 산업계 배포('22년~)
- (근원지 추적) 해킹조직의 공격 근원지 추적 기술('22년~), 가상자산 흐름 추적 기술('21년~) 등 개발 추진
- (데이터·네트워크 보안) 동형암호\* 등 암호기술, 공급망 보안 기술, 5G 네트워크 보안 기술 개발 등 추진('21년~)

\* 랜섬웨어 공격으로 데이터가 탈취되어도 개인정보 등 민감한 데이터의 노출 방지

### ② 사이버보안 생태계 강화 기반 마련

- (기본법 제정) 공공·민간 분야별로 규정된 사이버보안 법제도를 체계화 하고 산업분야간 협력을 강화하기 위한 기본법 제정 추진('21~'22년)

△ 사이버보안 기본계획 수립    △ 침해사고 대응 대책본부 구성, 사고조사, 대응훈련 등  
△ 정보공유 등 민·관 협력체계 강화    △ 주요정보통신기반시설 관리 강화

- (민·관 랜섬웨어 대응협의체 확대) 다양한 랜섬웨어 대응 역량 결집을 위해, 연구기관·지자체·지역중소기업 등의 참여 확대('21년~)

# 순 서

I. 추진 배경 .....	1
II. 랜섬웨어 현황 및 시사점 .....	2
III. 목표 및 전략 .....	7
IV. 주요 추진 과제 .....	8
1. 수요자별 선제적 '예방' .....	8
2. '사고대응' 쏠주기 지원 .....	15
3. 핵심 대응 역량 제고 .....	18
V. 추진 일정 .....	20

## I. 추진 배경

□ 최근 국내·외에서 해킹으로 피해자의 데이터를 암호화하고, 이를 풀어주는 대가로 돈을 요구하는 랜섬웨어(Ransomware) 피해 증가

○ 미국에서 랜섬웨어 공격은 송유관·육가공업체 등 기반시설과 국민 생활에 밀접한 분야가 목표가 되어 국가적 혼란 야기

- ▶ 미국 송유관 회사는 6일간 美 동부지역 송유 중단, 휘발유 가격 7년 내 최고(5.7)
- ▶ 최대 육가공업체 'JBS SA'의 미국 자회사는 생산시설 일부가 3일간 운영 중단(5.30)

○ 우리나라도 피해가 증가('20년 대비 64% 이상) 중이며, 최근 제조기업, 배달대행 플랫폼, 병원 등 다양한 분야\*에서 피해 발생

\* 자동차 부품 제조기업(5.2) → 배달대행 기업(5.15) → 의료기관(5.22) 등

□ 랜섬웨어 공격은 조직화·지능화되고 있으며 지속 증가할 우려

○ 프로그래머가 랜섬웨어를 제작하여 범죄조직에 공급하고 수익을 공유하는 등 범죄형태가 분업화·조직화(서비스형 랜섬웨어)

○ 신뢰가 있는 인물의 이메일 등을 활용한 사회공학적 기법, 지속적인 취약점 탐색(APT) 등 해킹 공격은 갈수록 지능화

□ 그간 우리나라는 디지털 전환에 대비하여, '디지털 뉴딜', 'K-사이버 방역' 등 추진으로 사이버보안 경쟁력을 개선\*하였지만,

\* 국제전기통신연합(ITU) 정보보호지수 순위 상승 ('19년 15위 → '21년 4위)

○ 랜섬웨어 대응 역량을 강화하지 않는 경우 개인·기업의 디지털 전환 저해와 국가적 안전 약화 우려

➡ 랜섬웨어 공격의 영향·범위 확대 등에 대응해 체계적 예방·대응·기반강화 등 랜섬웨어 대응 강화 대책을 신속히 수립·추진할 필요

## II. 랜섬웨어 현황 및 시사점

### 1 랜섬웨어 현황

랜섬웨어를 상품화하여 판매, 랜섬웨어 악용이 용이

- 서비스형 랜섬웨어\*를 제작하여 범죄조직에 공급하고 수익을 공유하는 형태로 범죄 분업화

\* Ransomware as a Service(RaaS)

- 가상자산과 익명성이 보장된 다크 웹(Dark Web)으로 금전확보 용이



- '20년 랜섬웨어 공격 중 64%가 서비스형 랜섬웨어이며, 랜섬웨어 개발자의 수요 증가로 몸값이 2배 이상 증가\*

\* 랜섬웨어 2020-2021 보고서(Group-IB), 2021.3월

랜섬웨어 피해는 전 세계적으로 급증

- (국내) 서비스형 랜섬웨어의 영향으로 전년 대비 '20년은 3배 이상, '21년 현재(7월)는 이미 64% 이상 공격 수치 증가

※ 랜섬웨어 신고는 39건('19) → 127건('20) → 97건('21.7월)이지만, 민간 보안업체의 통계(월간 수만건 감염)와 차이 → 신고를 기피하는 경향이 큰 것으로 파악

※ 국내 기업이 경험한 침해사고 중 59.8%가 랜섬웨어('20년 정보보호실태조사)

- 특히, 보안 투자 여력이 부족한 중소기업(약 81%) 중심으로 피해 발생

\* '21.7월까지 랜섬웨어 신고 97건 중 79건이 중소기업

- (세계) '21년 매주 약 950개(1~3월)의 기업이 랜섬웨어 피해, '20년 같은 기간(1~3월)의 약 470개에 비해 102% 증가

※ (출처) The New Ransomware Threat : Triple Extortion(check point, '21.5월)

## 참고1 최근 국내·외 랜섬웨어 피해사례 분석

- 미국 콜로니얼 파이프라인 사건 ('21.5월)
  - 미국 최대 송유관 업체인 콜로니얼 파이프라인社가 공격으로 시스템이 마비되어 송유관 가동을 6일간 전면 중단
  - 공격조직은 해킹단체인 다크사이드로 추정, 해킹조직에 440만 달러 상당의 비트코인 지불(FBI 추적을 통해 일부 회수)
- 미국 육가공업체(JBS SA) 사건 ('21.5월)
  - 글로벌 육가공업체인 JBS SA의 미국지사 에 대한 공격으로 미국, 호주, 캐나다 등에서 공장 가동 중단
  - 미 FBI는 해킹조직인 레빌 소행으로 파악하고 있으며, 해킹조직에 1,100만달러 상당 비트코인 지불
  - ※ 메사추세츠 증기선 관리국(6.2), 뉴욕시 법무전산시스템(6.7) 등도 발생
- 국내 부품기업 사건 ('21.5월)
  - 부품 제조기업의 서버 및 직원 PC의 데이터를 암호화(1차 공격), 임직원 개인정보와 해외사업 관련 데이터 다크웹 유출(2차 공격), 협상기간 동안 DDoS 공격으로 홈페이지 마비(3차 공격)
  - 해커와 협상하지 않고 1차 공격에 대한 암호화 복구 작업 완료
- 국내 배달대행 플랫폼기업 공격 ('21.5월)
  - 해커가 배달대행 플랫폼 기업의 서버를 암호화, 전국 3만5천 점포가 서비스 접근이 차단되어 1만5천명 라이더 피해발생
- 국내 성형외과 사건 ('21.5월)
  - 해커가 성형외과 서버에 침입하여 자료를 암호화하고, 유출한 환자들의 개인정보를 이용하여 협박 문자 발송
- 국내 운송업체 사건 ('21.6월)
  - 회사 일부 서버 및 PC가 랜섬웨어에 감염되어 업무 시스템 장애가 발생했으나 내부 백업 시스템을 이용하여 복구

## 참고2 미국 정부, 랜섬웨어 대응조치 현황

- 미국 바이든 대통령이 연방정부 기관들의 사이버보안 강화에 초점을 둔 행정명령\*을 발표('21.5.12)

\* Executive Order on Improving the Nation's Cybersecurity

- 사이버보안 정책을 국가 안보 및 경제 안보의 필수 요소이자 최우선 역점 영역으로 인식
- 주요 관계부처에 대해 명령 사항별 이행 시한을 구체적으로 설정하고 민간과 정보 공유 확대, 소프트웨어 공급망 보안 강화 등을 요구

행정명령 주요 내용: △ 민간과의 정보 공유 확대, △ 연방정부 사이버보안 현대화, △ 소프트웨어 공급망 보안 강화, △ 사이버안전 검토 위원회 설립, △ 보안 취약점 및 사고 대응을 위한 연방정부 플레이북 표준화, △ 연방정부 네트워크의 사이버보안 취약점 및 사고 탐지 강화, △ 연방정부의 사이버보안 조사 및 개선 역량 강화, △ 국가안보시스템 보안 강화

- 미국 CISA\*는 기업 리더들에게 랜섬웨어 대응 강화를 촉구하는 '랜섬웨어 위협으로부터 보호하기 위한 조치사항\*\*' 전달('21.6.3)

\* 사이버보안 및 인프라보안국 (Cybersecurity and Infrastructure Security Agency)

- △ 사이버보안을 강화하기 위한 모범사례 제시
- △ 데이터, 시스템, 설정을 백업 및 정기테스트하고 오프라인으로 유지
- △ 운영체제, 응용프로그램의 업데이트 및 패치를 즉각 적용
- △ 특정 시스템 피해시 비즈니스 운영 등 사고 대응계획 수립 및 테스트
- △ 3자 평가를 통해 조직 보안팀 및 보안시스템 허점 확인
- △ 핵심 비즈니스 운영 네트워크와 인터넷 네트워크 분리 검토

- 韓·美 정상회담, 랜섬웨어 공동대응을 위한 「사이버워킹그룹」 설립을 포함하는 등 국제 공조 강조

- 송유관 시설의 사고신고 의무화(교통안전청 지침, 5.28) 등 제도개선 추진

- 미국 FBI, 콜로니얼 파이프라인에서 해킹조직에 지불한 비트코인 중 일부(230만 달러 상당) 환수

## 2

## 랜섬웨어 특징

- (감염 원인) 악성코드가 삽입된 홈페이지 방문 또는 이메일 열람, 서버-네트워크 등 시스템 취약점 해킹 등 다양한 방식으로 감염

< 랜섬웨어 감염경로 >

구분	홈페이지 방문	이메일·SNS 유포	타깃형(APT) 공격
감염 경로	랜섬웨어가 유포 중인 홈페이지 방문	첨부파일 다운로드·링크 실행시 설치	해커가 서버 침투 및 악성코드 설치
원인	운영체제 등 SW 취약점 존재	이용자 부주의 등 보안인식 부족	기업의 보안관리 수준 취약

- (피해 형태) 범죄조직이 이메일·SNS 등을 통해 악성코드를 대량으로 살포하는 등 무차별적으로 공격

- 서비스형 랜섬웨어\*를 통해 해킹에 대한 전문지식 없이도 랜섬웨어 공격이 가능하게 됨에 따라 범죄의 문턱도 낮아짐

\* 별도의 프로그래밍 지식 없이도 비용을 지급하면 서비스 형태로 제공되는 랜섬웨어

- 통신 등 기반시설뿐만 아니라 디지털 전환으로 유통·제조·의료 등 다양한 분야가 공격 대상

- (피해 복구) 사전에 백업된 파일을 활용하거나 공개된 일부 복구 도구\*를 사용하는 것을 제외하고 암호화된 파일의 복구가 어려움

\* 국제 랜섬웨어 대응 프로젝트 그룹(No More Ransome) 150종 보유

- 피해자가 금전을 지불해도 파일이 복구되지 않거나, 개인정보가 공개되는 등 등 2차 피해 가능성 상존

- (범죄 대응) 범죄조직이 다국적 기업화되고, 가상자산과 다크웹(Dark Web)\*을 사용하여 범죄 추적에 기술적, 절차적 어려움 발생

\* 일반적인 방법으로 접속자·서버를 확인할 수 없어 사이버범죄에 많이 활용되는 웹

3

시사점

- ◇ 랜섬웨어의 형태와 특징을 고려하여 대응방향 마련 필요
- ◇ 예방, 대응, 핵심 역량 제고 등 각 단계별 정책 마련

랜섬웨어 특징		대응 방향	비고
감염 원인	SW 취약점	사전적 점검 및 취약점 조치	예방
	보안관리 취약	기업 정보보호 강화 유도 및 지원	
	보안인식 부족	국민·기업의 보안인식 제고	
피해 형태	빠른 확산 속도	악성코드 탐지·차단 체계 구축 및 신속한 피해극복 지원	대응
	무차별 공격	민관 간, 산업분야 간 정보공유	
	다양한 분야 피해		
피해 복구	기술적으로 복구 어려움	데이터 백업 인식제고 및 지원	예방
	2차 피해 우려	복구기술 개발·지원	기반
		범죄 모니터링, 수사 강화	대응
범죄 대응	다국적 기업화	국가 간 공조 강화	대응
	추적 어려움	범죄 추적기술 개발	기반



- √ 랜섬웨어는 복구가 어렵기 때문에 백업 등 **선제적 예방이 중요**
- √ 랜섬웨어는 **다양한 경로**를 통해 발생하기 때문에, 국가 기반시설 부터 중소기업·개인까지 **맞춤형 대응 지원체계** 구축 필요
- √ **진화하는 랜섬웨어**에 대응하여 지속적인 기술·기반 구축 등 **핵심 대응역량 제고** 필요

### III. 목표 및 전략

#### 목 표

## 랜섬웨어에 안심할 수 있는 디지털 환경 구축

- 국민들이 신뢰할 수 있는 랜섬웨어 예방·대응·기반강화 체계 구현 -

#### [전략1 : 예방] 국가중요시설 - 기업 - 국민 수요자별 선제적 예방

중요 시설	<ul style="list-style-type: none"> <li>· 주요정보통신기반시설 추가 지정 검토 및 예방 체계 강화</li> <li>· 軍, 연구기관 등 대상 보안점검 및 공급망 보안 강화</li> </ul>
기업	<ul style="list-style-type: none"> <li>· 중소기업 패키지형 보안역량 강화 지원 (데이터금고 등)</li> <li>· 기업 예방활동 강화(ISMS, 정보보호공시제, CISO 등 연계)</li> </ul>
국민	<ul style="list-style-type: none"> <li>· 국민 PC·IoT 기기 보호 '내 PC 돌보미 서비스' 확대</li> <li>· '랜섬웨어 예방 플레이북' 보급 등 예방 캠페인</li> </ul>

#### [전략2 : 대응] 정보공유 - 피해지원 - 수사 등 사고대응 쏠주기 지원

정보 공유	<ul style="list-style-type: none"> <li>· 사이버위협정보공유시스템(C-TAS) 참여 확대</li> <li>· 민·관, 국제 협력을 통한 정보 공유 강화</li> </ul>
피해 지원·수사	<ul style="list-style-type: none"> <li>· 지역정보보호센터 등 활용 전국단위 피해지원</li> <li>· 2차 피해 방지를 위한 사이버공격 수사 강화</li> </ul>

#### [전략3 : 기반] 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고

기술 개발	<ul style="list-style-type: none"> <li>· 랜섬웨어 등 사이버공격 대응 기술 개발 강화(범죄 근원지, 가상자산 추적 등)</li> <li>· 신형 랜섬웨어 복구기술 개발, 산업계 보급</li> </ul>
기반 강화	<ul style="list-style-type: none"> <li>· 기본법 제정을 통한 사이버보안 법제도 체계화</li> <li>· '민·관 랜섬웨어 대응 협의체' 확대</li> </ul>

## IV. 주요 추진 과제

### [전략1] 국가중요시설 - 기업 - 국민 수요자별 선제적 예방

1

#### 튼튼한 국가중요시설 관리 체계 구축

美 송유관·육가공업체 랜섬웨어 피해 사례처럼, 대형 인프라는 사고 시 사회 전반에 막대한 피해 전파, 지속적인 안전 제고 필요

#### ① 주요정보통신기반시설 예방 체계 강화

- (기반시설 확대) 정유사(공정제어시스템), 자율주행 관제시스템 등 새로운 중요시설의 기반시설 확대 지정 검토('21~'22년)
- (보호대책 개선) 기반시설관리기관이 마련하는 보호대책에 ①백업 시스템 구축, ②위기발생시 복구방안, ③업무지속계획(BCP\*) 포함('22년)
  - ※ 참고 지침 마련·배포 → 보호대책에 반영 추진
  - \* Business Continuity Plan : 재난 발생시 업무 연속성을 유지하기 위한 계획으로, 랜섬웨어 등 사이버공격 예방 대책, 사고시 확산단계별 대응계획 등 반영
- (공공분야 보안) 공공분야 시설 중 망 분리가 어려운 정보시스템\*의 외부접점에 운영 중인 보안장비·DMZ\*\* 구간 현장 점검 등 강화
  - \* 공공병원, 연구기관, 일부 지자체 등
  - \*\* Demilitarized Zone : 외부에 서비스 제공 시, 내부 자원을 보호하기 위해 내부망과 외부망 사이에서 접근 제한을 수행하는 영역
- (긴급점검 확대) 공공·민간 기반시설\* 긴급점검을 통해 보호대책의 준수 및 백업 여부, 사고시 신고·복구 준비 상황 등 점검(상시)
  - ※ 주요정보통신기반시설 : 민간 147개, 공공 277개 ('21.7월 현재)
- (모의훈련 확대) 통신사, IDC, 금융사 등 핵심 기반시설의 랜섬웨어 대응 강화를 위해 모의 훈련\* 추진('21년 민간분야 9개)
  - \* 화이트해커 활용 기반시설의 홈페이지·이메일·서버 모의 침투 등

<화이트해커 활용 모의침투 훈련>



- (기타 제도 개선) 랜섬웨어 등 최신 보안 위협에 대한 예방 강화를 위해 현장 점검과 점검결과에 대한 개선 조치 근거\* 마련('21~'22년)

\* 정보통신기반보호법 개정 추진

② 軍, 연구기관 등 긴급 대응반 운영을 통한 보안강화

- (국방 보안) 국방정보체계, 軍 기반시설 제어시스템에 대한 취약점 점검을 실시하고, 사이버 특별훈련, 장병 보안교육 등 강화

※ 백업 관련하여 주요 체크리스트 마련을 통해 준수여부 점검 실시('21년~)

- (연구기관 보안) 원자력연구 등 출연연구(26개)과 4대 과기원 대상으로, 강화된 사이버 보안대책\*을 수립·적용 추진('21년~)

\* 모의 침투훈련, 취약점 점검, 연구용서버 자가진단시스템 구축 등

① 공급망 및 공공 이메일 보안 강화

- (기반시설 공급망) 기반시설에 구축된 SW·시스템의 공급망에 대한 보안 점검 체계 구축('22년~, 민간분야 기반시설관리기관 대상)

- (SW 개발 보안 지원) SW 개발 단계부터 보안강화를 위해 'SW 개발보안 허브'를 구축(판교, '21.7월)하고,

- SW·솔루션 설계-구현-유통 단계별 보안 강화 지원('21년~)

- (공공 이메일 보안) 랜섬웨어 감염의 주 경로인 이메일의 보안 강화를 위한 '이메일 보안 기술'을 공공분야 적용 확대 검토('21년~)

### 참고3

## 주요정보통신기반시설 보호체계

#### □ 개 요

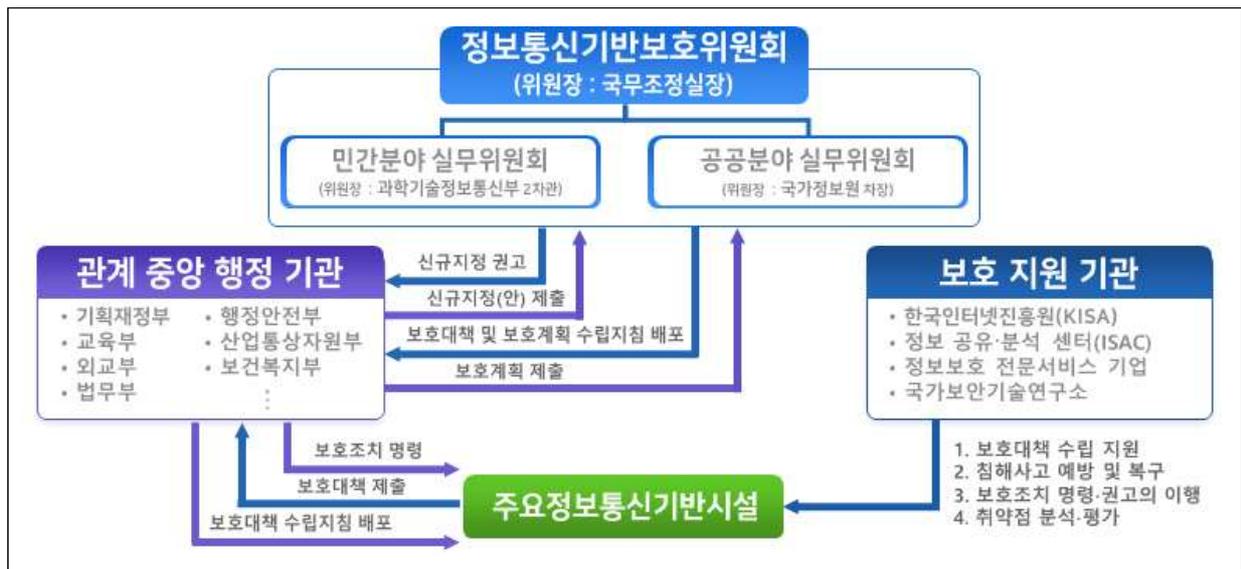
- 국가안전보장, 행정, 통신, 금융, 의료 등 국가·사회적으로 중요한 시설을 주요정보통신기반시설로 지정·관리(정보통신기반보호법 제8조)
- (현황) 총 228개 관리기관, 424개 시설(민간: 147개, 공공: 277개, '21.7월)

구분	합계	과기정통부	행안부	금융위	산업부	복지부	국토부	방통위	기타
민간	147	61	10	54	2	9	2	9	-
공공	277	16	93	7	54	6	16	-	85

- (지정절차) 기반시설 지정권고(과기정통부·국정원) → 기반시설 선정요구(관계중앙행정기관) → 지정여부 평가(지정대상 관리기관) → 지정여부 심사·결정(관계중앙행정기관) → 기반시설 지정심의·의결(정보통신기반보호위원회)

#### □ 기반보호 체계 및 절차

- (보호체계) 종합적인 범정부 대응체계를 구축하기 위하여 정보통신기반 보호위원회(위원장 : 국무조정실장) 및 민간·공공 실무위원회 설치



- (보호절차) 보호계획/대책 수립지침 배포(과기정통부·국정원/부처, ~5월) → 취약점 분석·평가(관리기관) → 보호대책 수립(관리기관, ~8월) → 보호계획 수립(부처, ~10월) → 보호대책 이행점검(과기정통부·국정원) 등

## 2

## 중소기업 보안역량 지원 강화

우리나라에서 특히 랜섬웨어에 취약한 중소기업을 대상으로 데이터 금고를 통한 백업, 랜섬웨어 대응 3종 패키지 등 지원 강화

### ① 중소기업 보안역량 강화 패키지 지원

○ (데이터금고 구축) 중소기업들의 업무중단, 데이터 유실 예방 강화를 위해 데이터금고\* 구축을 통한 백업 지원('22년~)

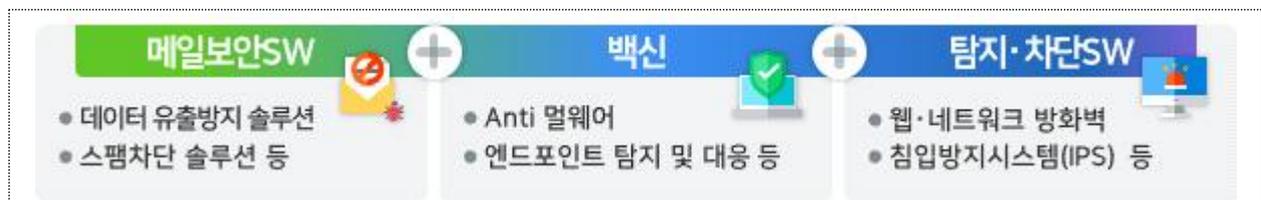
- \* 중소기업의 데이터 이중화 지원을 위해 클라우드(또는 하드웨어) 기반 백업 지원
- 실시간 '데이터 백업'뿐만 아니라 '데이터 암호화', 랜섬웨어 사고시 '데이터 복구'까지 종합 지원

<데이터금고의 개념>



○ (랜섬웨어 대응 3종 패키지 지원) 메일보안SW, 백신, 탐지·차단SW 등 '랜섬웨어 대응 3종 패키지' 중소기업 지원 강화('21년 3천여개)

<랜섬웨어 대응 3종 패키지>



- (클라우드 기반 보안) 보안전문기업이 클라우드를 기반으로 원격에서 중소기업에 필요한 보안 기능 전반을 제공\* ('21년 670개)

\* SECURITY as a Service(SECaaS)

- (원격 서버점검) 서버 보안 관리에 예산·기술적 어려움을 겪는 중소기업 대상 원격 서버점검 서비스 제공('22년~)
- (맞춤형 컨설팅) 중소기업의 서버·네트워크 등 ICT 인프라 규모, 보안 정책 및 조직 유무 등을 진단하여 맞춤형 보안 개선방안 제공

<맞춤형 정보보호 컨설팅 진행절차>



- (민관 합동 보안제품 도입 지원) 컨설팅 결과 등을 바탕으로, 중소기업에 필요한 보안제품(SW·솔루션 등) 도입 지원\*('21년~)

\* 정부지원 '21년 600개 + 민간주도형(보안기업 11개 참여) 지원 연간 2천여개

- o (기술유출 방지 지원) 기술집약적 중소기업을 대상으로 24시간 실시간 보안관제 등을 바탕으로 '기술유출 방지' 지원('21년~)
- o (의료기관 지원) '코로나 백신' 접종 민간위탁 의료기관 대상(1기관 당 최대 5개 PC) 안티 랜섬웨어 SW 보급('21년~)

## ② 기업의 랜섬웨어 예방활동 강화

- o (ISMS 연계) ISMS 인증 기업의 사후·갱신 심사시 랜섬웨어 예방 활동(예방·사고대응 교육, 백업 등 시스템 보안조치 등) 평가 강화('22년~)
- o (정보보호공시 연계) 정보보호공시제(대상기업 약 1천여개)에 업무 지속계획(BCP)을 공시내용에 포함 추진(공시 의무화 '21.12월 시행)
- o (CISO 연계) 정보보호최고책임자(CISO, 약 2.4만명) 대상 정기·수시 세미나를 통한 최신 랜섬웨어 동향 및 예방 교육 강화(상시)

## 참고4 데이터금고 지원 방안

### □ 데이터 금고 구축 필요성

- 랜섬웨어로 인한 업무중단 및 금전적 피해를 예방하기 위해서는 주기적인 백업을 통해 데이터 복원력을 확보하는 것이 중요
- 중소기업의 경우 백업 시스템 구축에 대한 비용·인력 부담 존재

※ 18만 여개 기업이 PC·네트워크 시설을 보유(20 정보화통계집, NIA)하고 있지만 백업을 실시하는 기업은 47.3%에 불과

### □ 주요 지원내용

- (클라우드) 클라우드 기업체\*와 협력하여 자체 백업 공간을 확보하기 어려운 영세·중소기업을 대상으로 클라우드 백업 서비스 제공

\* IDC센터를 보유하고, 클라우드 기반의 데이터 백업·복구 서비스를 제공하는 기업  
- 보안관제 등 클라우드 사업자의 보안시스템을 통한 안정적 서비스 지원이 가능해 자체 백업 절차를 수행하기 어려운 영세기업에 적합

- (하드웨어) 고용량 백업이 필요한 기업에게 NAS\* 등 하드웨어 백업 시스템 도입 지원

\* Network-Attached Storage(네트워크 연결 저장소)  
- 일정 규모 이상의 PC를 보유하여, 대용량(20TB 이상) 백업 시스템 구축이 필요한 중소기업에 적합

< 클라우드·하드웨어 데이터 백업 >



비대면 환경 활성화로 일반국민들에 대한 랜섬웨어 위협도 증가, 국민들의 ICT 기기 보안성 향상 및 랜섬웨어 예방 인식 제고 필요

### ① 국민들의 정보통신 기기 보안성 향상 지원

○ (원격점검 지원) PC·IoT 기기의 랜섬웨어 취약 여부를 원격으로 진단·개선하는 ‘내 PC 돌보미 서비스’ 지원(‘21년~)

\* 필수 보안항목 점검, 랜섬웨어 예방 패치 설치, 안전한 이용수칙 안내 등

< 내 PC 돌보미 서비스 >



○ (알림 서비스) 언제 어디서든 기기의 취약점 정보를 실시간 알려주는 모바일 전자고지 기반 ‘찾아가는 알림 서비스’ 추진(‘22년~)

※ 단순 알림에 그치지 않고, ‘내 PC 돌보미’와 연계하여 사후조치도 지원

### ② 랜섬웨어 예방 인식제고 및 예방수칙 보급

○ (플레이북 보급) 국민들의 랜섬웨어 예방을 위한 ‘랜섬웨어 예방 플레이북(예방 수칙)\*’을 지속 업데이트·보급하고(‘21년~),

\* (주요 내용) △최신 보안 패치 적용, △출처 불명확한 이메일·URL 링크 주의, △P2P 파일 다운로드 주의, △중요한 자료 정기적 백업 등

- 최신 랜섬웨어 동향을 반영한 정보통신 기기 자가보안 진단도구도 배포하여 보유 기기의 보안수준 유지 지원(상시)

○ (예방 캠페인) “랜섬웨어는 감염되면 복구가 어렵기 때문에 예방이 최선”이라는 메시지를 온·오프라인\*으로 전방위 홍보(‘21년~)

\* 공익광고, 대중교통 캠페인(지하철, KTX 등), 전광판, 정부 간행물 등

## [전략2] 정보공유 - 피해지원 - 수사 등 사고대응 쏠주기 지원

1

### 정보공유·협력 채널 강화

민·관간(산업분야간), 국가간 랜섬웨어 위협·탐지 정보 공유를 활성화하여 국가전체의 랜섬웨어 대응 집단 체력 강화

#### 1 민·관간 정보공유·협력 채널 활성화

○ (시스템 유기적 연동) 민간(C-TAS), 공공(NCTI) 사이버위협 정보공유 시스템\*을 상호 유기적으로 연동할 수 있는 체계 구축('22년~)

\* △Cyber-Threat Analysis and Sharing △National Cyber Threat Intelligence

- 의료, 금융 등의 민간분야 정보공유분석센터(ISAC\*)와 C-TAS 간에도 실시간 정보공유가 가능하도록 체계 연동 추진

\* Information Sharing & Analysis Center

< 사이버위협 정보공유 시스템의 유기적 연계 >



○ (C-TAS 참여 확대) 가상자산거래소, 유통·제조 분야 기업 등의 C-TAS 참여를 확대하여, 기업들에 대한 랜섬웨어 정보\* 공유 및 대응 지원

\* 랜섬웨어 해킹 URL·메일, 복구비용 지불용 가상자산 주소 등

- C-TAS에서 수집된 정보는 대국민 공지, ISMS 인증기업, CISO 협의회, 주요정보통신기반시설 등에도 신속히 공유 추진

○ (웹사이트 심층탐지\*) 국민들의 이용이 많은 웹사이트(2만여개)의 랜섬웨어 위협을 탐지하고, 정보를 C-TAS 등에 신속 공유('21년~)

\* 주요 웹사이트의 메인페이지뿐만 아니라 전체페이지를 탐지

## ② 국가간 정보공유 강화

- (정보공유) 해외 정보기관, 주요국가 인터넷 보안기관(CERT\*)간 정보공유를 통해 신종 랜섬웨어 및 다크웹 등 정보 신속 입수·분석
  - \* Computer Emergency Response Team : 인터넷 보안 지원과 관련된 기관
  - 분석결과는 공공·민간에 신속 공유하고, 백신 개발·배포 지원 추진
- (제도 협력) '한미 사이버 워킹그룹\*' 등 사이버보안 협의체를 통해 랜섬웨어 정보, 위협 대응 사례 공유, 수사공조 등 협력 강화 추진('21년~)
  - \* 한미정상회담(5.21)에서 랜섬웨어 대응 등을 위한 양국의 법집행·국토안보 기관 간 협력 강화에 중점을 둔 '사이버 워킹그룹' 추진에 합의

## 2

### 확산방지 및 신속한 피해지원

랜섬웨어 공격의 확산 방지를 위해 AI기술 활용 악성도메인 차단, 다중이용시설 취약점 개선, 전국단위 피해지원 체계 구축 등 추진

#### 1 랜섬웨어 공격의 확산 방지

- (AI 기반 악성도메인 차단) 네트워크 트래픽, 행위·패턴 분석 등 AI 기술을 활용해 실시간 악성도메인 탐지·차단\* 실시('21년 말)
  - \* DNS 트래픽 수집 → 악성 도메인 특성 기반 모델링 → 악성 도메인·IP 탐지 → 접속 차단
- (다중이용시설 취약점 점검) 가상자산거래소, 비대면 서비스 개발 업체 등 이용자가 많은 서비스 대상 취약점 점검\* 지원('21년 300개)
  - \* 랜섬웨어 사고 원인과 밀접한 시스템 및 업무·운영 환경 등 점검
  - 보안취약점 발견 시 기업이 단계적으로 취약점 보완 조치를 강화하도록 법·제도적 장치 마련('21년~)
  - ※ 현재는 기업이 보안 취약점을 방치하더라도 개선을 강제할 법적근거 미비



- (백신 배포) 수집한 랜섬웨어 정보는 백신 개발사와 협력하여 랜섬웨어 백신을 신속 개발, C-TAS 등을 통해 배포하여 확산 방지('21년~)
- (피해시 대응 상담) '랜섬웨어 대응사례'를 수집하고, 상담을 통해 피해기업에 대응방법 공유 강화('21년~)
- (제도 개선) 일반적인 사고라도 확산 가능성이 큰 랜섬웨어 사고는 기관에 원인분석·대책마련 권고할 수 있도록 제도 개선 추진('22년~)

## ② 신속한 사고·피해극복 지원

- (전국단위 피해지원) 지역정보보호 지원체계\*와 연계, 피해 시 인력·장비를 현장 파견하여 피해극복을 지원하고, 적극 수사 의뢰('21년~)

\* 지역정보보호센터(전국 10개) 및 지역보안전문업체 보안전문가 등 활용

## 3

### 2차 피해 방지를 위한 사이버공격 수사 강화

#### 다크웹 모니터링을 통한 해킹조직의 활동 감시 강화

- 다크웹 상에 노출된 피해자의 개인정보 등은 관계부처에 신속 공유하고, 피해자의 2차 피해 방지 지원

## ② 랜섬웨어 해킹조직 수사 역량 강화

- (전담 수사체계 구축) 경찰청·시도경찰청의 사이버테러수사대(팀) 내 랜섬웨어 전담 대응체계 구축, 랜섬웨어 공격에 엄정 대응 강화('21년~)

※ 경찰청 본청에 '랜섬웨어 및 가상자산 추적수사 TF'도 구축, 일선 수사 지원

- 민간(과기정통부, ☎118), 공공(국정원, ☎111) 부문별 사고 신고·대응을 지원하고, 수사기관과 실시간 정보공유('21년~)

※ 신고 활성화를 위해 신고한 피해기업에 대해 취약점점검·보안컨설팅·솔루션 등 정부지원을 우선 제공할 수 있도록 제도적 개선 검토('21년~)

- (국제 공조) 인터폴 회원국들과 해킹조직 분석, 범죄자 공동 검거를 강화하고, 공조 확대를 위해 유로폴과도 실무약정 체결 추진('21년~)

## [전략3] 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고

1

### 랜섬웨어 등 사이버공격 대응 핵심기술력 확보

신형 랜섬웨어의 신속한 탐지·복구를 지원하는 기술을 확보하고, 공격근원지 및 가상자산의 흐름을 추적하는 기술개발 강화

#### ① 신형 랜섬웨어 탐지·복구 기술 확보

- (탐지·차단) ‘펌웨어·하드웨어 기반 탐지·차단\*’ 등 랜섬웨어 공격 탐지·차단’ 기술 개발(‘21년~)
  - \* SW형 탐지기술보다 탐지·차단 속도가 빨라 데이터의 손실을 최소화하는 기술로서, 기반시설·기업 등에 적용하기 적합
- (복구 기술) 랜섬웨어 암호학적 특징에 의거한 DB를 지속 축적하고, 랜섬웨어 복구기술을 개발, 산업계 신속 배포(‘22년~)

#### ② 근원지 추적기술 개발 강화

- (공격 근원지 추적) 해킹조직의 프로파일링 시스템\*을 구축하고, 해킹조직의 서버·이메일 역추적 기술 등 개발(‘22년~)
  - \* 코드·공격수법·서버IP·이메일 등 공격정보를 DB화하고 유사도 분석
- (가상자산 흐름 추적) AI 기반으로 부정합 가상자산 거래 기록을 추적·학습, 흐름을 추적하는 기술 개발(‘21년~)
  - ※ FBI는 콜로니얼 파이프라인이 지불한 몸값 중 일부(230만불 상당) 환수

#### <랜섬웨어 근원지 추적기술>



## ① 데이터·네트워크 및 AI 기반 보안기술 개발 강화

- (데이터) 동형암호\* 등 랜섬웨어로 데이터가 탈취되어도 개인·금융 정보 등 민감정보의 노출을 방지하는 암호기술 확보('21년~)

\* 암호화된 상태에서 데이터에 대한 연산·분석 등이 가능한 암호

- (네트워크) 공급망 네트워크 취약점 분석·탐지 기술을 확보하고, 5G 네트워크 쉐어링(코어망, 엣지망, 디바이스) 보안 기술 개발('21년~)

- (AI 기반 보안) AI 기반 통합 보안 관제, 랜섬웨어 자동 탐지·차단·분류 등 AI기반의 첨단 보안 기술 심층\* 육성('21년~)

\* (기존) 시제품 개발 지원 → (개선) 상용제품 제작, 사업화·해외진출까지 지원 확대

## 2

### 사이버보안 생태계 강화 기반 마련

사이버보안 생태계 강화를 위해 기본법 제정을 추진하고, 민·관 협의체 확대를 통해 랜섬웨어 대응 역량 결집

#### 1] 사이버보안 기본 법제(가칭 '사이버보안기본법') 마련

- 공공·민간 분야별로 규정된 사이버보안 법제도를 체계화하고 산업분야간 협력을 강화하기 위한 기본법 제정 추진('21~'22년)

△ 국가 사이버보안 기본계획(5년) 및 시행계획(1년) 수립

△ 정보공유 등 민·관 사이버보안 협력체계 강화

△ 주요정보통신기반시설 관리 강화

△ 침해사고 대응을 위한 대책본부 구성, 침해사고 조사 및 대응훈련 등

#### 2 「민·관 랜섬웨어 대응 협의체」 확대 운영

- 다양한 랜섬웨어 대응 역량 결집을 위해, 연구기관·지자체·지역 중소기업 등의 참여 확대('21년~)

## V. 추진 일정

추진 과제	추진일정	소관부처
<b>전략1. 국가중요시설-기업-국민 수요자별 선제적 예방</b>		
<b>① 튼튼한 국가중요시설 관리체계 구축</b>		
① 주요정보통신기반시설 예방 체계 강화	'21~'23	과기정통부, 국정원, 산업부 등 관계부처
② 軍, 연구기관 보안 강화	'21~	국방부, 과기정통부
③ 공급망 및 공공 이메일 보안 강화	'21~'24	과기정통부, 국정원
<b>② 중소기업 패키지형 보안역량 강화 지원 및 책임성 증진</b>		
① 중소기업 보안역량 강화 패키지 지원	'21~'23	과기정통부, 복지부, 중기부
② 기업의 랜섬웨어 예방활동 강화	'21~'22	과기정통부
<b>③ 대국민 랜섬웨어 면역력 향상</b>		
① 국민들의 정보통신 기기 보안성 향상 지원	'21~'23	과기정통부
② 랜섬웨어 예방 인식제고 및 예방수칙 보급	'21~	과기정통부, 관계부처
<b>전략2. 정보공유-피해지원-수사 등 사고대응 쉼주기 지원</b>		
<b>① 정보공유·협력 채널 강화</b>		
① 민·관간 정보공유·협력 채널 활성화	'21~	과기정통부, 국정원, 복지부, 금융위 등
② 국가간 정보공유 강화	'21~	과기정통부, 국정원, 외교부 등
<b>② 확산방지 및 신속한 피해지원</b>		
① 랜섬웨어 공격의 확산 방지	'21~'23	과기정통부, 관계부처
② 신속한 사고·피해극복 지원	'21~	과기정통부, 관계부처
<b>③ 2차 피해 방지를 위한 사이버공격 수사 강화</b>		
① 다크웹 모니터링을 통한 해킹조직 감시 강화	'21~	국정원
② 랜섬웨어 해킹조직 수사 역량 강화	'21~	경찰청, 과기정통부
<b>전략3. 진화하는 랜섬웨어에 대한 핵심 대응 역량 제고</b>		
<b>① 랜섬웨어 등 사이버공격 대응 핵심기술력 확보</b>		
① 신형 랜섬웨어 탐지·복구 기술 확보	'21~'23	과기정통부
② 근원지 추적기술 개발 강화	'21~'23	과기정통부, 경찰청
③ 데이터·네트워크 및 AI 기반 보안기술 개발	'21~'23	과기정통부
<b>② 사이버보안 생태계 강화 기반 마련</b>		
① 사이버보안 기본 법제 마련	'21~'22	과기정통부, 국정원 등
② 「민·관 랜섬웨어 대응 협의체」 확대 운영	'21~	과기정통부

# 랜섬웨어에 안심할 수 있는 디지털 환경을 구축하겠습니다!

01  
예방

국가중요시설 - 기업 - 국민 수요자별로 선제적 지원하겠습니다

튼튼한 국가중요시설  
관리 체계 구축



중소기업 보안역량  
지원 강화



대국민 랜섬웨어  
면역력 향상



02  
대응

정보공유-피해지원-수사 등 사고대응 전주기 지원하겠습니다

정보공유·협력 채널  
강화



확산방지 및  
신속한 피해지원



2차 피해 방지를 위한  
사이버공격 수사 강화



03  
기반

진화하는 랜섬웨어에 대한 핵심 대응 역량을 제고하겠습니다

랜섬웨어 등 사이버공격 대응  
핵심기술력 확보



사이버보안 생태계 강화  
기반 마련



국민들이 신뢰할 수 있는

●●● 랜섬웨어 예방·대응·기반강화 체계를 구현하겠습니다! ●●●