발 간 등 록 번 호
11-1721000-000621-01

「초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술개발 및 공유·협력 플랫폼 구축」

공동기획연구 최종보고서

2021. 12. 23.

한국과학기술정보연구원

KOREA INSTITUTE OF SCIENCE AND TECHNOLOGY INFORMATION

제 출 문

과학기술정보통신부장관 귀하

본 보고서를 「초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술개발 및 공유·협력 플랫폼 구축」에 관한 공동기획연구 보고서로 제출합니다.

2021. 12. 23.

기획연구기관명 : 한국과학기술정보연구원

기획연구책임자 : 송중석
참 여 연 구 원 : 이 준
참 여 연 구 원 : 권태웅
참 여 연 구 원 : 최상수
참 여 연 구 원 : 김규일
참 여 연 구 원 : 최윤수
참 여 연 구 원 : 이윤수
참 여 연 구 원 : 문형우
참 여 연 구 원 : 김태용
참 여 연 구 원 : 박건량
참 여 연 구 원 : 차충일
참 여 연 구 원 : 고영민
참 여 연 구 원 : 연현화
참 여 연 구 원 : 한국전자통신연구원 문대성
참 여 연 구 원 : 한국과학기술원 조호묵

요 약 본

❑ 사업 목표

대국민 공공 서비스·인프라*에 대한 **암호화된 사이버위협을 선제적으로 탐지·대응**하기 위한 **차세대 보안관제 기술 개발 및 공유·협력 체계 구축**

* 지능형 ICT(과기정통부), 지능형 교통(C-ITS, 국토교통부), 스마트 선박 · 항만(LTE-M, 해양수산부), 스마트 City(세종특별자치시) 등

○ **【원천기술 개발 및 實데이터 확보】** 암호화 트래픽에 대한 실시간 수집·처리, 공격·정상 행위 분석·탐지·대응 원천기술 개발 및 實환경 기반 대규모 학습데이터 확보

○ **【공유·협력 플랫폼 개발】** 암호화된 사이버위협 정보 및 탐지·분석 모델·규칙을 공유하고 효율적인 대응체계 구축·운영을 위한 통합 플랫폼 개발

❑ 사업 범위

○ 【**대상 인프라·서비스**】 정부에서 추진하는 ICT 기반 대국민 공공 서비스·인프라 중 **다양한 암호화 통신환경을 포함**(유·무선망, IoT망, 기간망, 복합망 등)하고 **국민생활과 밀접하게 연결**(생활, 도시, 교통, 선박)되어 있는 핵심 4종 서비스·인프라(※ 아래 그림 참조)

- **암호화된 공격·정상** 데이터(평문쌍 포함) 수집 및 개발 기술의 실증 수행

○ 【**원천기술 개발**】 암호화된 트래픽에서 실제 사이버위협과 정상행위를 **자동으로 탐지·분류** 할 수 있는 **행위기반 보안관제** 기술 개발

- 암호 트래픽의 복호화에 따른 **시스템·네트워크 성능 저하, 국민 사생활 침해 등 현실적인 한계를 극복**하기 위해 별도의 복호화를 요구하지 않는 **(비복호화 기반)** 기술 개발

○ 【**기술표준화·실증 및 플랫폼 구축**】 모든 부처에서 추진하는 대국민 공공 서비스·인프라에 활용 가능하도록 **범용성과 실용성이 보장**된 기술 개발 및 **공유·협력 플랫폼** 개발

- 각 부처의 통신환경별 **최적화 및 표준화** 연구 필수 수행, 사업성과에 대한 **활용성 제고**

❑ 사업 내용

○ 【정보 수집】 대국민 공공 서비스·인프라 기반 암호화통신·디바이스 전주기 정보 수집

- 정상 및 악성 행위 암호화·평문 네트워크 트래픽 정보 수집(프로토콜 헤더, 메타데이터 등 포함)
- 통신 디바이스 행위 정보 수집(어플리케이션, 게이트웨이, 활성화 정보 등)
- 공공·민간 위협 인텔리전스 기반 데이터 수집(MITRE ATT&CK, NCTI 등)
- 오픈 데이터 소스를 활용한 최신 공개 데이터 수집(APCERT/CTA 등)

○ 【분석·탐지】 암호화기반 공격·악성 행위 분석·탐지 원천 기술 개발

- 네트워크 메타정보*를 활용한 공격·악성 행위 분석·탐지 모델 개발

* 암호화 트래픽에도 통신 절차 수립을 위한 일부 메타(평문)정보 포함

- 디바이스·네트워크 행위 기반의 공격·악성 행위 탐지 모델 개발

※ 악성·정상·이상 행위별 모델링 및 화이트·블랙리스트 데이터베이스 구축

- 암호화기반 악성코드(멀웨어) 공격·악성 행위 분석·탐지 모델 개발

※ 랜섬웨어, 백도어, 스파이웨어, 웜 등 주요 악성코드 분석 · 탐지 기술 확보

○ 【최적화·실증】 부처별 서비스·인프라 대상 자동탐지 시스템 설계·최적화 및 실증·성능평가

- 지능형 ICT 환경에서의 탐지시스템 설계·개발·최적화 및 實환경 기반 테스트베드 구축·실증·성능평가(초고속 통신망 등)
- C-ITS 환경에서의 탐지시스템 설계·개발·최적화 및 實환경 기반 테스트베드 구축·실증·성능평가(자율주행차량, 통신 기지국 등)
- LTE-M 및 e-Nav 환경에서의 탐지시스템 설계·개발·최적화 및 實환경 기반 테스트베드 구축·실증·성능평가(선박, 센서 등)
- 스마트 City 환경에서의 탐지시스템 설계·개발·최적화 및 實환경 기반 테스트베드 구축·실증·성능평가(도시 제어, 교통, 생활 센서 등)

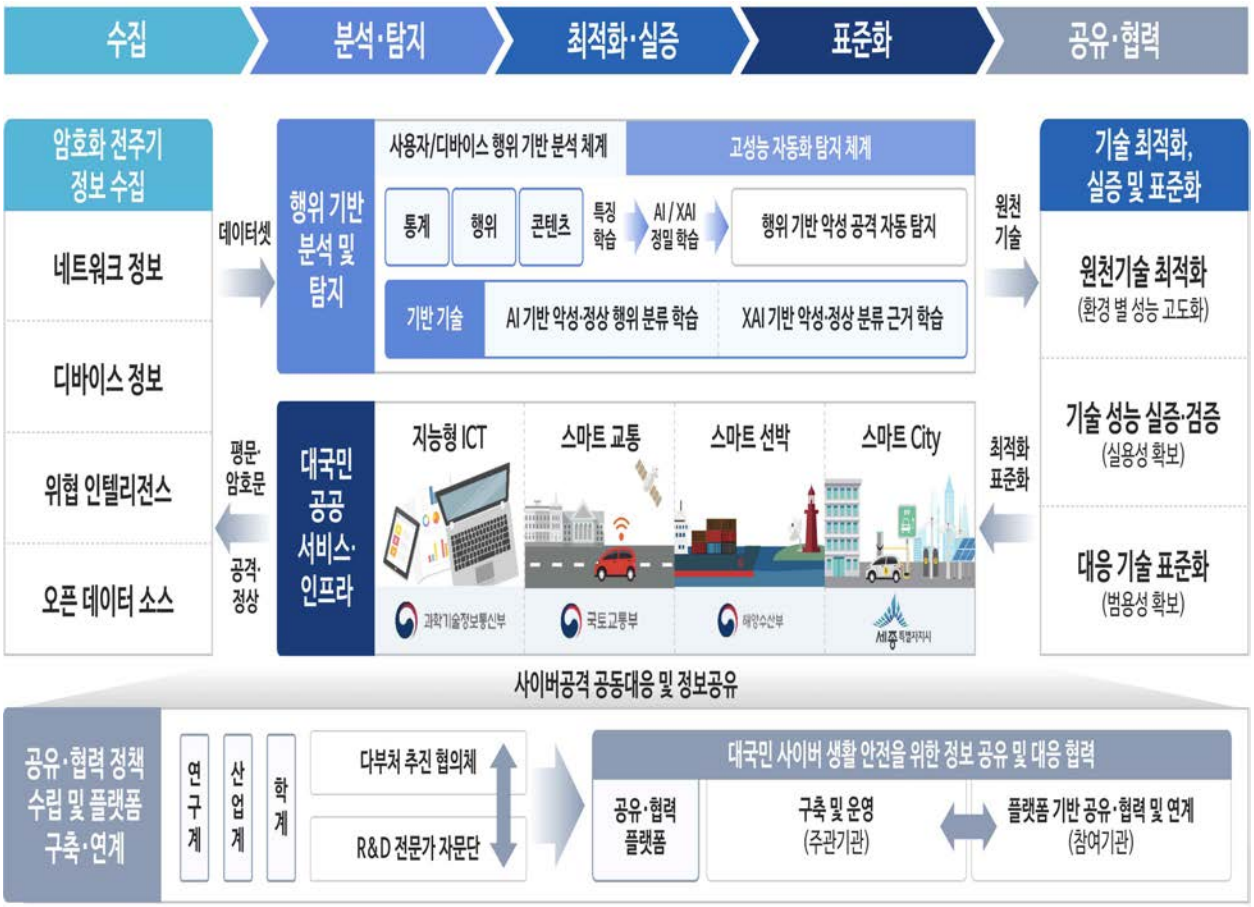
○ 【표준화】 다양한 암호화 공격·악성행위 통합 대응 및 협력을 위한 행위 표준화 기술 개발

- 암호화 통신 기반 네트워크 트래픽 특징·행위 정보 모델링 및 표준포맷 정의
- 네트워크 보안장비와의 연동을 위한 행위 기반 표준 모델의 탐지 패턴화

※ 암호화트래픽 분석 보안장비의 상용화를 고려한 탐지 패턴 개발 · 구축

○ 【공유·협력】 국가·공공 분야 암호화 공격 대응을 위한 공유·협력 체계 구축

- 암호화통신 기반 공격·악성 행위 공유 및 대응, 협력 플랫폼 개발 및 구축
- 공유·협력 플랫폼 기반 정보공유 활성화 및 위협 공동 대응 추진
- 국가·공공 분야를 비롯한 민간 분야를 포함한 공유, 협력 체계 확산 추진



❑ 사업 추진체계

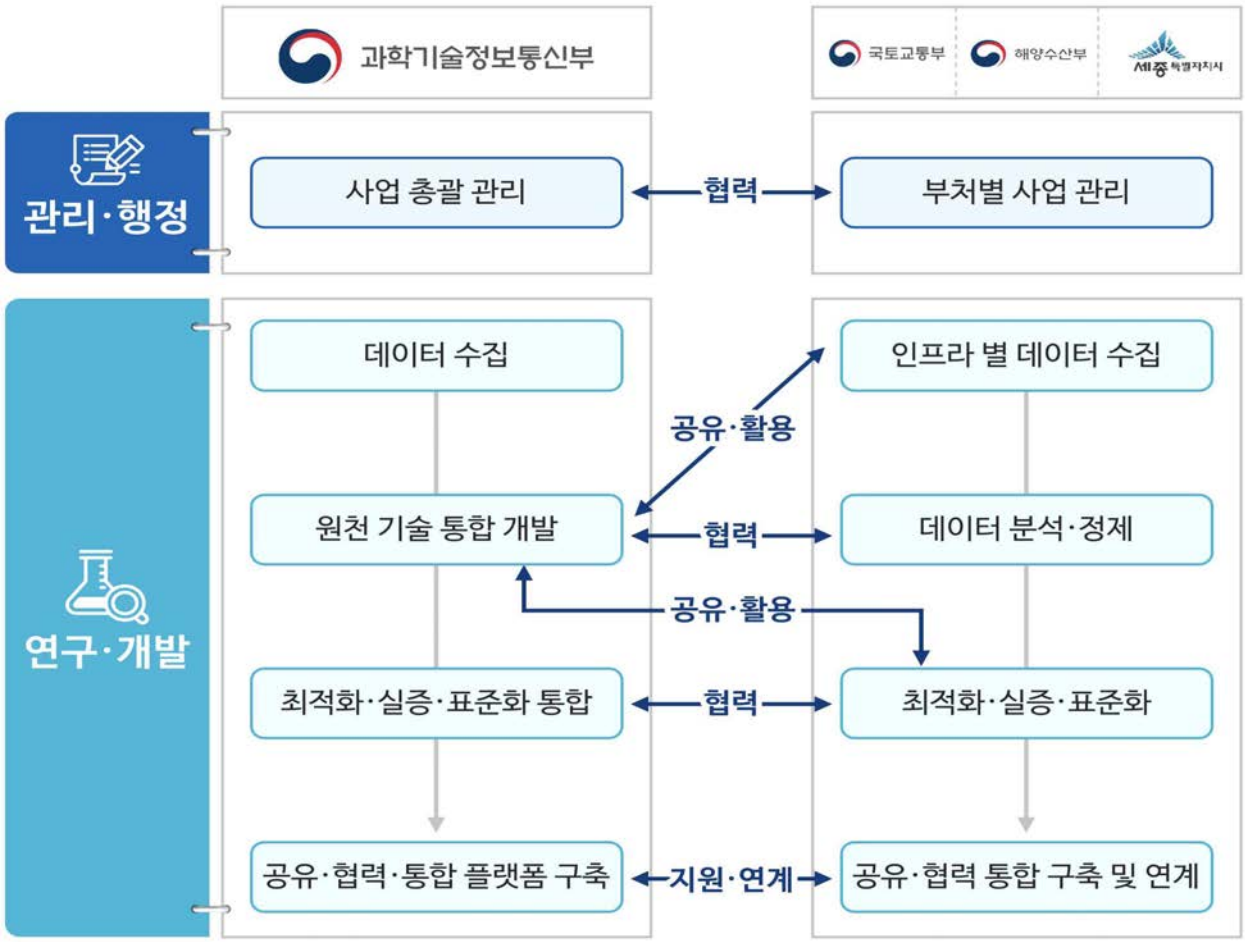
○ 【역할정립·협력체계 구축】 부처, 개발·수요 기관, 연구수행·지원 기관별 역할 정립 및 긴밀한 협조·추진체계 구축

- **(주관·참여 부처)** 부처 內 개발·수요 기관들의 요구사항을 수렴하고 다부처 사업 수행을 지원함으로써 연구개발 성과창출 추진
- **(개발·수요 기관)** 부처 및 연구 수행·지원 기관들과 상호협력을 통한 원활하고 주도적인 사업 추진 및 성과 확산 방안 수립
- **(연구 수행·지원 기관)** 산·학·연을 포함한 전문성·관련성 있는 기관간의 공유·협력을 통해 원천기술연구, 일자리 창출지원 및 인력양성 등 사회문제해결에 기여

※ 효율적인 부처협업사업 추진을 위하여 '통합관리형'으로 관리체계 수립

○ 【협의체 구성·운영】 사업 추진 범위 및 연구방향 정립을 위한 다부처 추진 협의체 및 R&D 전문가 협의체 구성

- **(다부처 추진 협의체)** 사업간 지속적인 공동연구 계획·방법·추진 체계 수립을 위해 부처 담당자, 사업 주관 부서, 실무기관 관계자 등으로 구성
- **(R&D 전문가 협의체)** 암호기술, 네트워크, AI 등 사업 관련 각 분야의 전문가들로 구성된 R&D 전문가 협의체 구성을 통해 구체적인 연구방향 수립·검토 및 원천기술 개발 자문 수행



○ **【역할 세분화】** 성공적인 다부처 사업 추진이 가능하도록 기술개발 체계를 고려하여 주관부처와 참여부처간 역할을 세분화

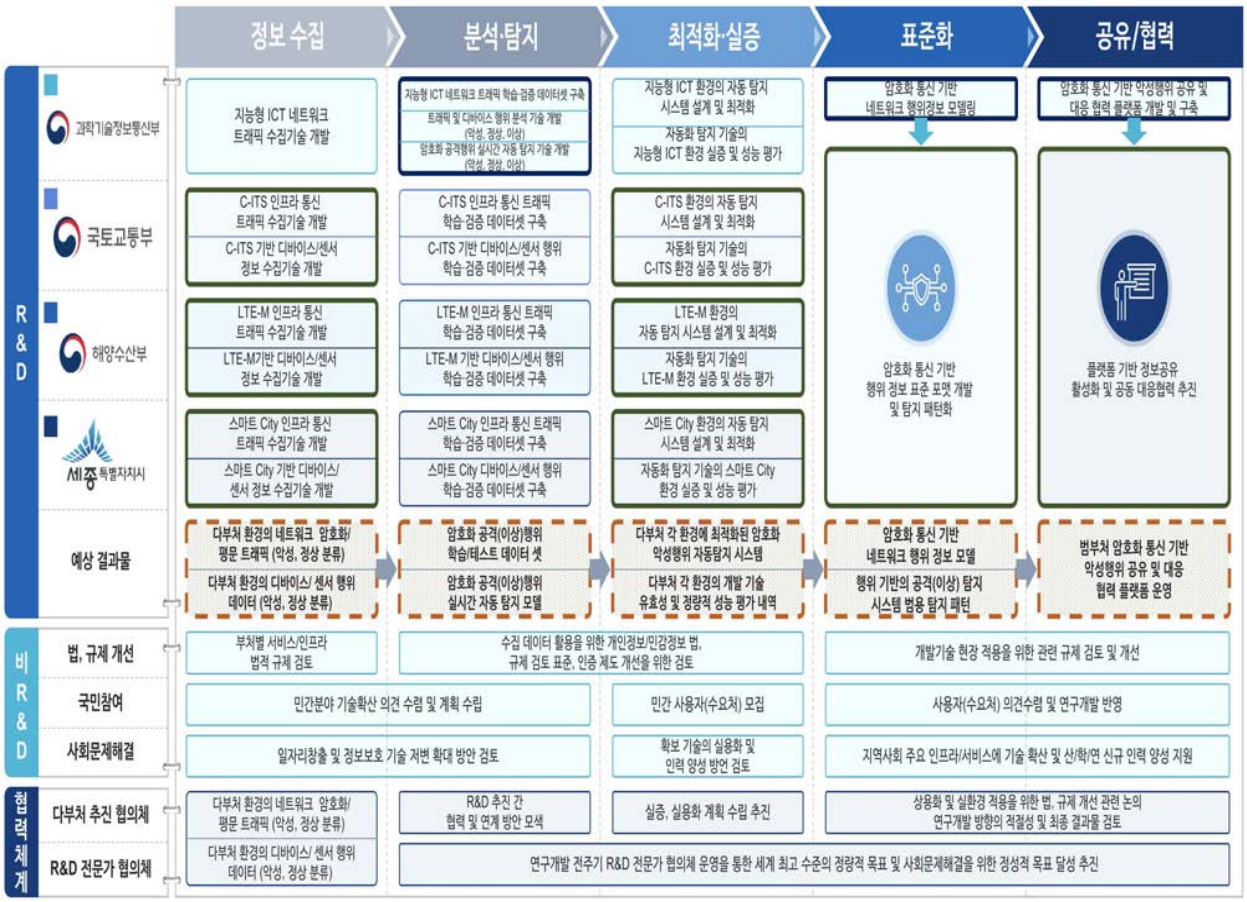
- **(주관부처 : 과학기술정보통신부)** ICT환경 기반 데이터 수집, 최적화 기술 개발 및 실증, 행위기반 자동화 분석·탐지 원천기술 및 공유·협력 플랫폼 개발 주도
- **(참여부처 : 국토교통부, 해양수산부, 세종특별자치시)** 환경 및 데이터 특수성을 고려하여 데이터 수집, 최적화 기술개발 및 실증을 부처별 상황에 따라 각각 수행

- **(전체부처)** 위협정보 표준포맷 개발 및 표준화 작업 공동 수행

○ **【특수성 고려】** 다양한 환경에 대한 고려가 필수적인 암호화 기반 사이버 공격 대응의 특수성을 반영하여 서로 다른 유형의 대국민 공공서비스·인프라를 운용 중인 각 부처가 기술 수요처이자 공급처로서 참여하고, 긴밀한 연계 협력 추진

○ **【성과 도출방안】** 주관·참여부처, 수요기관, 협의체 등의 긴밀한 협조를 통해 각 연차별 결과와 최종 암호화통신 기반 악성·공격행위 탐지·대응 기술의 실증 및 실용화 추진

- 수집, 분석·탐지, 최적화·실증, 표준화 및 공유·협력 5단계로 구분된 연구개발 과정을 5년에 걸쳐 수행
- 각 차년도별로 명확한 연구 예상결과물 목표 설정 및 추진 계획 수립
- 법, 규제 및 사회문제해결 방안을 고려한 정량·정성적 성과목표 수립



❑ 기대효과

○ 【기술적 측면】

- (**패러다임 전환 원천기술 확보**) 폭발적으로 증가하는 암호화된 사이버 공격을 선제적으로 분석·탐지·대응할 수 있는 **차세대 사이버보안 원천기술** 확보 및 국내 기업의 **글로벌 기술경쟁력** 확보
- (**기술 완성도 제고**) 부처 간 **긴밀한 협력을 기반으로 대규모 실제 인프라·데이터**를 활용한 R&D를 수행함으로써 개발된 기술의 **완성도 제고**
- (**국가 사이버안보 자주권 확보**) 사이버안보 패러다임 전환을 위한 **핵심기술을 국산화 및 조기 확보**함으로써 해외 기업의 기술종속에 따른 **제2의 화웨이 사태를 미연에 방지**하고 국산 장비를 활용한 **자주적 사이버안보 체계 구축·운영** 가능

  ※ 특히, 보안장비는 **모든 기관에 설치 · 운영**되고 송 · 수신되는 **모든 데이터를 모니터링**하기 때문에 해외 기업에 기술종속이 될 경우 **국가 안보에 심각한 타격**을 받음

○ 【사회적 측면】

- (**디지털 안심국가 실현**) 모든 사물이 네트워크로 연결되는 4차산업혁명 시대의 **대국민 공공 인프라·서비스에 대한 보안성 및 안전성**을 확보함으로써 **디지털 안심국가를 실현**
- (**국민의 생명과 안전 보장**) **대규모 재난·재해급**의 사회적 혼란을 초래할 수 있는 암호화된 사이버공격을 조기에 탐지 및 대응함으로써 **국민의 생명과 안전을 보장**하고 **삶의 질 제고에 기여**
- (**코로나 시대 사이버안전 확보**) 암호화 통신 기반의 온라인 서비스가 폭증하는 코로나 시대에 재택근무, 화상회의, 원격접속 등 **대국민 업무·생활 서비스의 안전한 이용**환경 제공에 기여

○ 【경제적 측면】

- (**예산 절감**) 다부처사업 추진을 통한 유사 R&D 사업 **중복투자를 원천 차단**하여 **국가 R&D 예산을 절감**하고 **연구수행 효율화 향상**

- **(경제적 피해 최소화)** 재난화·대형화되는 사이버위협을 사전에 차단 또는 조기에 탐지·대응함으로써 발생 가능한 **경제적 피해 규모를 최소화**하고 **복구비용을 절감**
- **(사이버안보 산업 발전)** 약 7조원 규모의 국내 **사이버안보 산업의 발전**에 기여하고 국내 기업의 **해외시장 진출을 통한 수출증대** 및 **글로벌 기업으로의 성장**을 위한 기반 마련

○ **【실용·사업화 측면】**

- **(범국가적 대응체계 구축)** 대국민 공공 서비스·인프라에 대한 암호화된 사이버 공격을 선제적으로 분석·탐지·대응하기 위한 **범국가적 차원의 일원화된 공동대응 체계 구축** 및 **사이버안보 역량 강화**에 기여
- **(기술·서비스 경쟁력 강화 및 일자리 창출)** 핵심 원천기술을 국내 보안장비 제조사, 보안솔루션 공급사, 보안관제 전문기업 등에 기술이전을 실시함으로써 **제품·서비스의 기술 경쟁력 강화** 및 새로운 **일자리 창출 기회** 마련

목 차

그 림 목 차

표 목 차

제1장 다부처공동R&D 추진 필요성

제1절 사회문제 개요

❑ 사이버위협의 급증

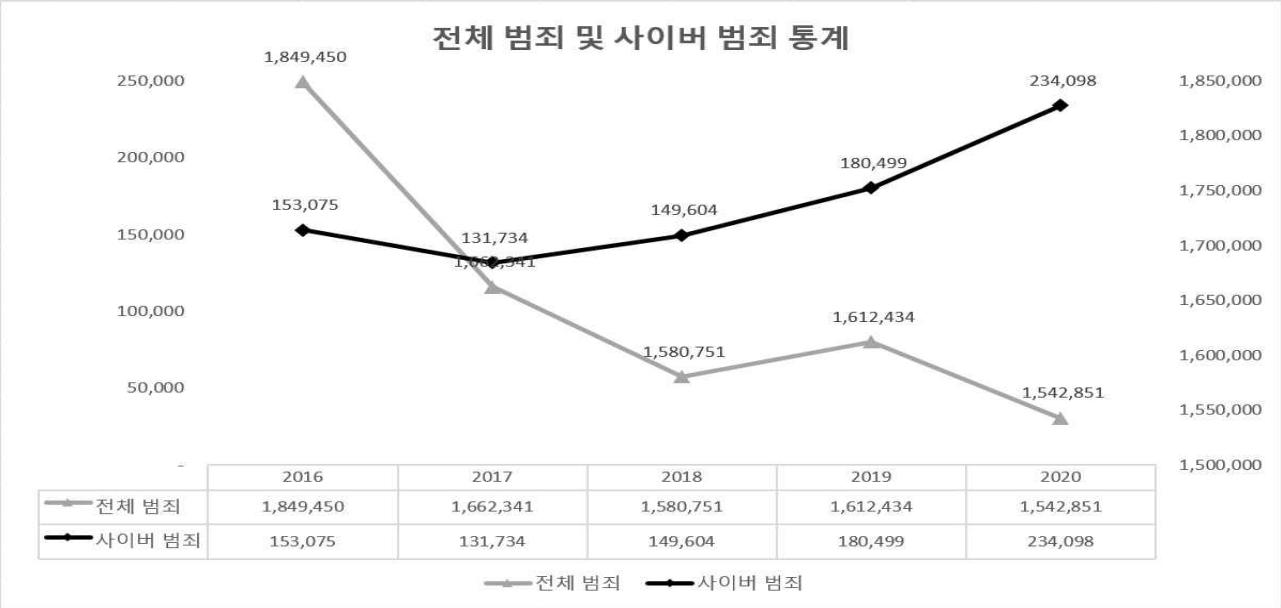
ㅇ 사이버위협의 전 세계적인 증가

- 공공기관 및 민간·기업들을 대상으로 수행되는 사이버 범죄·위협의 피해 사례 및 피해 규모가 해마다 증가하고 있음

- 최근 5년동안 국내 전체 범죄의 수는 16.6% 줄어든 반면 **사이버 범죄의 수는 매년 증가**하였으며, **'20년은 '16년 대비 52.9% 증가함**

- 사이버 공격 트렌드: 2021 중간보고서(Cyber Attack Trends: 2021 Mid-Year Report, Check Point Software Technologies)에 따르면 전 세계 조직들에 대한 **사이버위협은 29% 증가**함

- 또한, 포브스(Forbes)에 따르면 국내뿐만 아니라 해외에서 역시 '20년에는 '19년에 비해 **멀웨어가 358%, 랜섬웨어가 435% 증가**한 것으로 확인됨



<그림 1> 최근 5년 전체 범죄 및 사이버 범죄 통계, 국가수사본부

ㅇ 사이버위협 유형의 다양화

- KISA의 2021년 랜섬웨어 최신 동향 분석 및 시사점 보고서에 따르면, 정부 및 기업 등 특정 대상을 표적으로 한 공격이 증가하고 있는 추세

- 기존 전통적인 사이버 공격의 피해는 단순 서비스 마비, 정보 유출 정도에 한정되었으나, 사이버 물리 시스템(CPS)들이 네트워크에 연결되기 시작한 초연결 디지털 사회에서는 복합적인 피해로 이어질 수 있음

- 공격자들의 사이버 공격 전술에 대한 문서화를 수행하는 국제 프로젝트인 MITRE ATT&CK 프레임워크는 공격자의 공격 기법·목표들을 세분화하여 정리함

※ MITRE ATT&CK은 신규 공격 기법 및 공격 현황을 반영하여 지속적으로 현행화하고 있으며, 특히 사이버 킬 체인의 확장 및 재구성을 통해 공격 목표 달성까지의 과정을 13단계로 정의함

- MITRE ATT&CK의 공격자가 최종적으로 공격 목적을 달성하는 단계인 Exfiltration(정보 유출 등의 기밀성 훼손)과 Impact단계(서비스 마비 등의 무결성·가용성 훼손)를 정리하면 아래 표와 같음

[표 1] 목적 달성 단계에서의 공격 기법 (MITRE ATT&CK Framework)

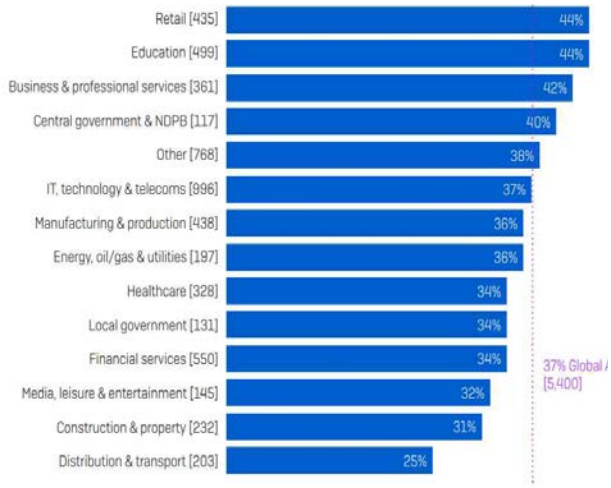
공격 목적	공격 기법	내용
Exfiltration	Automated Exfiltration	탈취 데이터를 자동화 프로세스를 통해 유출
	Data Transfer Size Limits	탈취 데이터를 고정 크기로 세분화하여 임계치 기반 패킷 탐지기법 우회
	Exfiltration Over Alternative Protocol	기존 명령 및 제어 통신 채널과 다른 프로토콜을 통해 탈취 데이터 유출
	Exfiltration Over C2 Channel	명령 및 제어 통신 채널을 통해 탈취 데이터 유출
	Exfiltration Over Other Network Medium	명령 및 제어 통신 채널과 다른 통신 채널을 통해 탈취 데이터 유출

Impact	Exfiltration Over Physical Medium	물리적 저장 매체를 통해 탈취 데이터 유출
	Account Access Removal	공격 대상 시스템의 사용자 계정 삭제/잠금/조작
	Data Destruction	공격 대상 시스템 내 파일, 디렉토리 단위의 개별 데이터 파괴
	Data Encrypted for Impact	공격 대상 시스템 내 데이터 암호화
	Data Manipulation	공격 대상 시스템 내 데이터 조작 및 변조
	Defacement	공격 대상 시스템 내 시각적 미디어 데이터 조작 및 변조
	Disk Wipe	공격 대상 시스템 내 디스크 단위의 전체 데이터 손상/삭제
	Endpoint Denial of Service	공격 대상의 종단 시스템에 DoS 공격 시도
	Firmware Corruption	공격 대상의 플래시 메모리 내 데이터인 BIOS나 펌웨어의 변조를 통한 악성행위 수행
	Inhibit System Recovery	시스템 복구 서비스 제거를 통한 시스템 복구 방해
	Network Denial of Service	공격 대상 네트워크에 DoS 공격 시도
	Resource Hijacking	공격 대상 시스템 자원 탈취를 통한 암호화폐 채굴 등 악성행위 수행
	Service Stop	공격 대상 시스템 서비스 중지/비활성화
	System Shutdown/Reboot	공격 대상 시스템 강제종료/리부팅

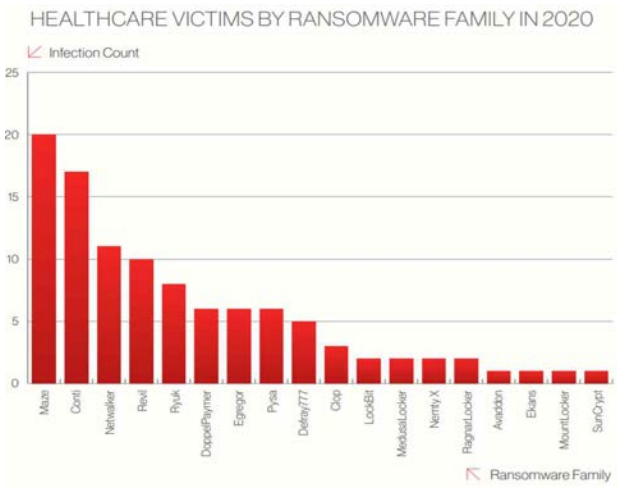
- 무결성·가용성 훼손 기법에서도 확인할 수 있듯 사이버 공격의 피해는 **단순 정보 유출**에서 **물리 시스템 작동 불능의 물리적 피해와 같은 비가역적 피해까지 발전**할 수 있어 이에 대한 대처 중요성이 크게 증가

- 보안전문기업(Sophos)의 2021년도 설문조사에 따르면 전체 산업군 중 평균 약 37%정도의 기업들이 전년도에 랜섬웨어 피해를 경험함

※ 일례로 보안전문기업(CrowdStrike)에 따르면, 2020년에 Maze, Conti 등 18개 랜섬웨어 패밀리에 의해 **미국**에 위치한 **104개 의료기관이 감염됨**



<그림 2> 산업 분야별 랜섬웨어 피해 발생 유무 현황 (Sophos, State of Ransomware, 2021)



<그림 3> 2020년 랜섬웨어 패밀리에 의해 감염된 의료부문 피해 수(Crowdstrike Global Threat Report, 2021)

o 사이버위협 대상의 확대

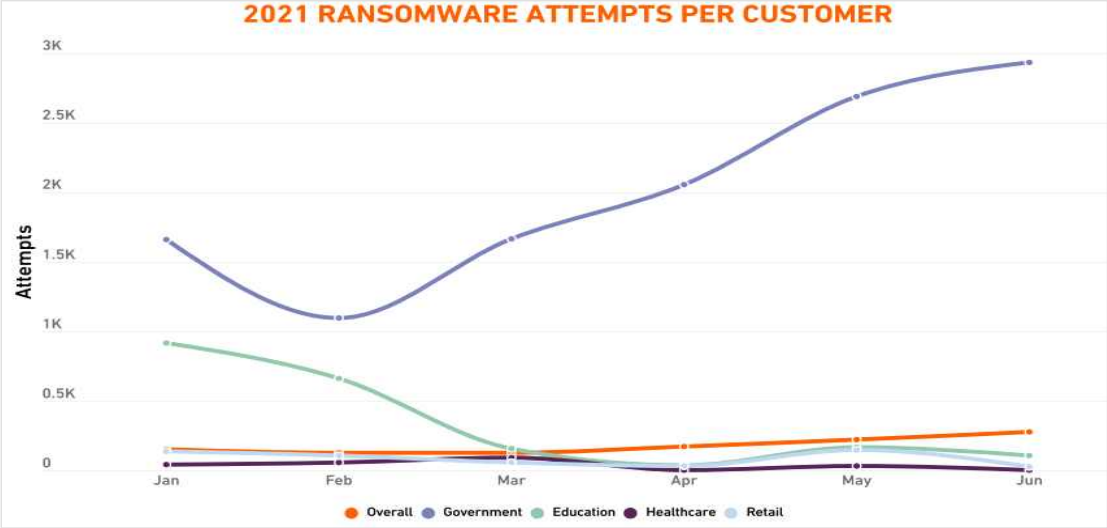
- (IoT 디바이스) 4G/5G+ 등의 통신 환경의 발달로 인해 사회 다방면에서의 IoT(Internet of Things, 사물인터넷)기반 서비스가 점차 확대

  ※ 가전제품부터 의료기기, 웨어러블 기기, 스마트 기기를 포함한 스마트 City를 구성하는 모든 서비스·인프라가 인터넷에 연결되어 상호작용

- 인터넷에 연결된 모든 기기들은 멀웨어와 해킹의 대상이 될 수 있으며, 실제 IoT를 대상으로 하는 공격들은 해마다 증가하고 있음

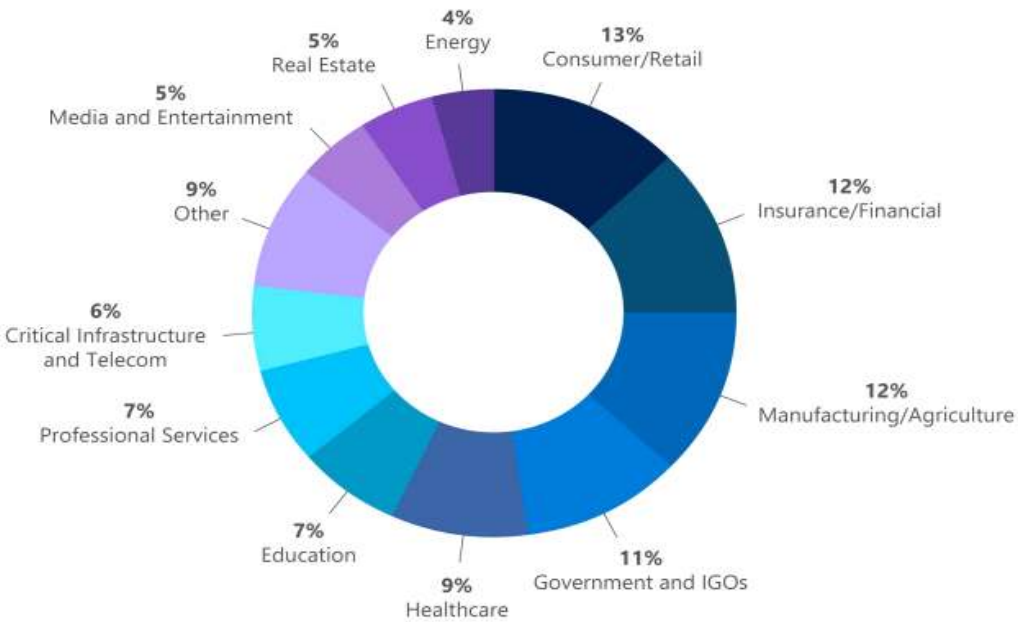
- FBI는 러시아 해킹조직으로 알려진 WIZARD SPIDER의 공격이 의료기관 랜섬웨어 감염 및 **의료서비스 중단**으로 이어지고 있다고 경고함

- 이처럼 의료, 유통, 교육, 금융 관련 기업을 필두로 **산업 분야 전반으로 공격이 발생**하고 있는 실정이며, 특히 정부기관의 경우 **공격 발생 비율이 전년 대비 약 3배 증가**



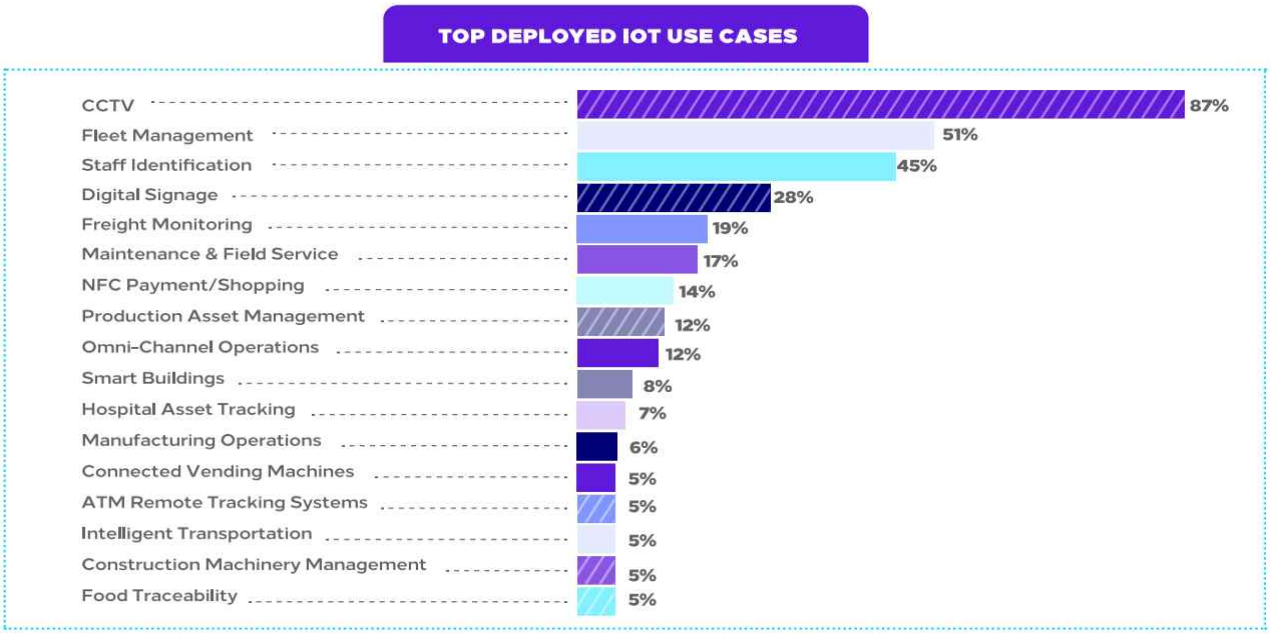
<그림 4> 정부기관에 대한 공격 급증 현황 (SonicWall threat report, 2021)

- 또한, Microsoft사의 침해대응팀 Detection and Response Team(DART)의 연간 침해대응 데이터에 따르면 **2021년도 기준 국가 기반시설을 포함해 산업 분야 전반에 대해 공격이 발생**하고 있음



<그림 5> 산업 분야별 공격 비율 통계 (Microsoft DART Digital Defense Report, 2021)

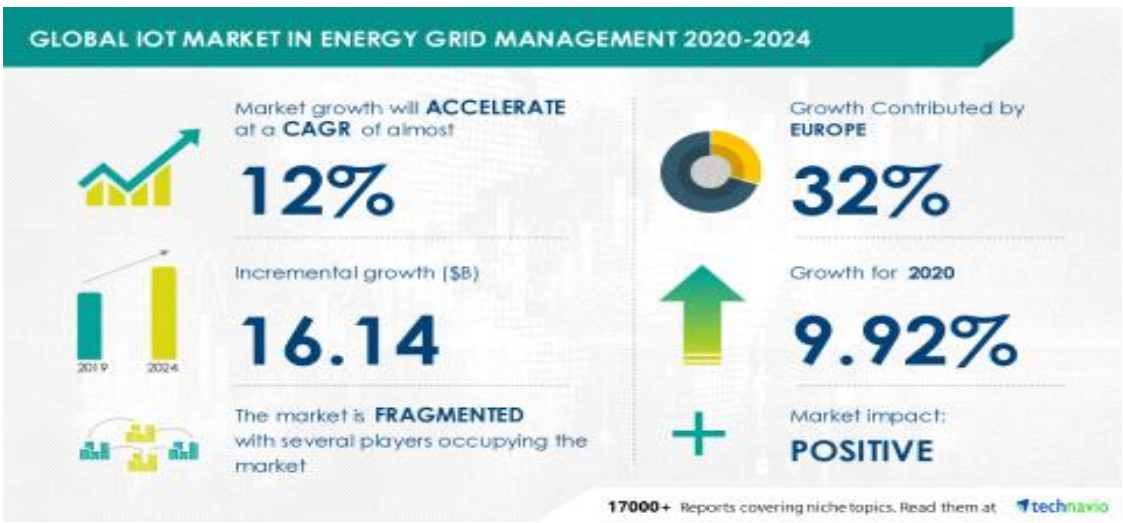
- 국외의 경우(사우디아라비아) 국가 기간시설 내 다양한 분야에서 IoT기기들을 도입 및 사용 중에 있으며, 이후에도 기간시설 내 IoT기기의 추가적인 도입을 추진할 예정임을 밝힘



<그림 6> 사우디아라비아 기간시설 내 IoT기기 도입 현황 (CITC, 2021)

- 글로벌 시장 조사 기업 Technavio에 따르면 에너지 그리드 관리 분야의 IoT 시장은 예측기간(2020년~2024년) 동안 **연평균 12%(CAGR) 성장**할 것으로 예상

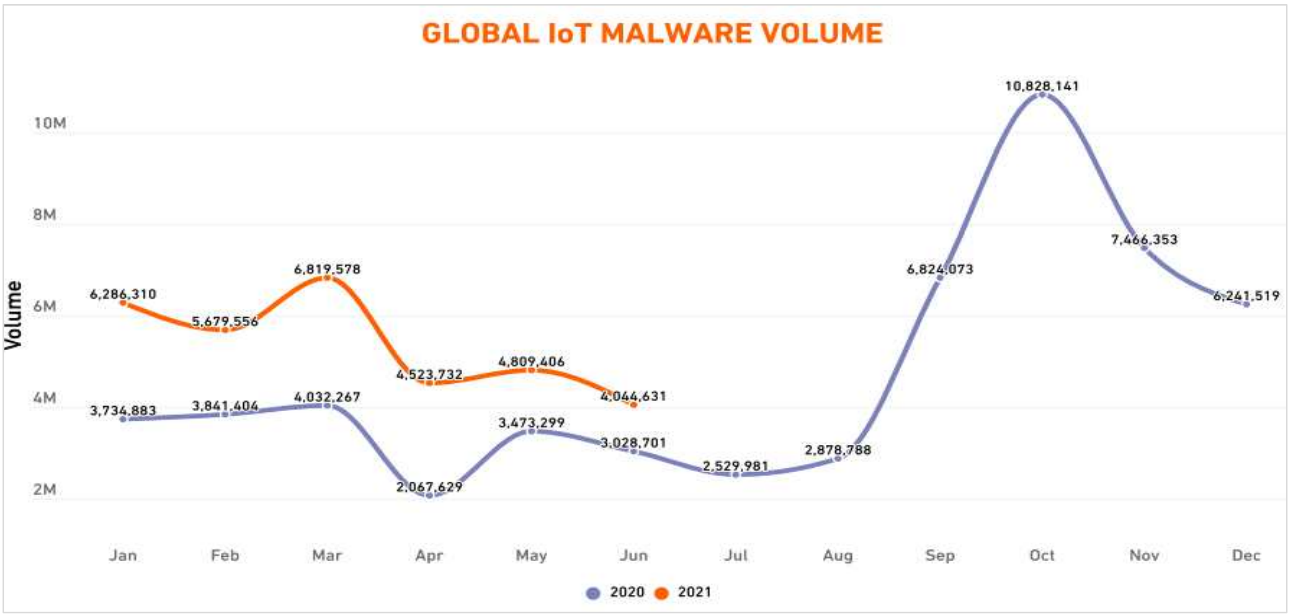
- 이에 따라 국가 기간시설 인프라에 해당하는 발전, 수도 등 다양한 분야에서의 IoT기기 도입 또한 보편화되어 사이버보안 위협에 영향을 줄 것으로 예상됨



<그림 7> 글로벌 에너지 관리 분야 IoT 시장 전망 (Technavio, 2020)

- IBM X-Force와 SonicWall CYBER THREAT REPORT에 따르면 '19년 10월부터 '20년 6월까지 발생한 IoT 공격이 지난 2년 동안의 IoT 공격을 합친 것에 비해 **400% 증가**했다고 보고함

- IoT기기들은 저전력, 소형화, 경량화를 위해 본래 기능을 제외한 보안 등의 부가적 기능은 포함하지 않아 보안에 취약함



<그림 8> 전 세계 IoT 기기에 대한 공격 59% 증가 (SonicWall CYBER THREAT REPORT, 2021)

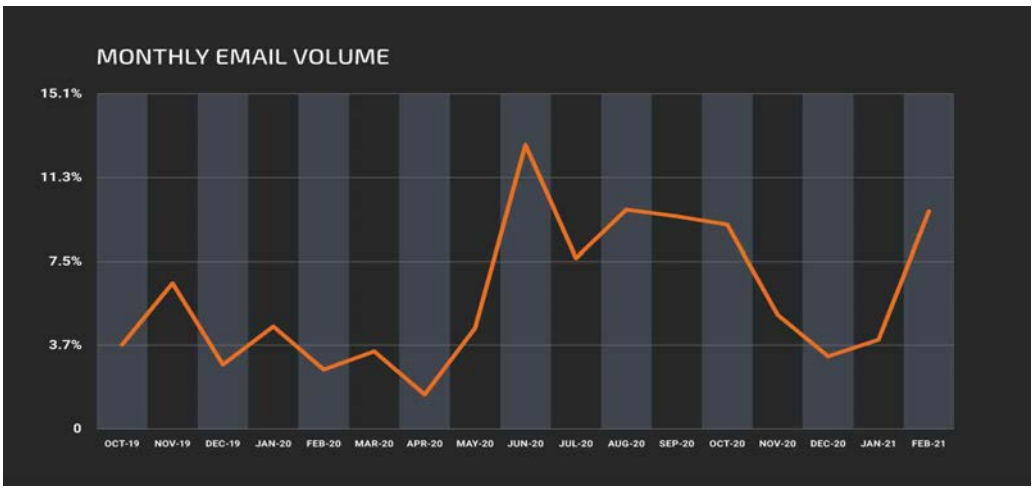
○ 암호화통신을 악용한 사이버공격의 확산

- 통신환경의 변화에 따라 해커는 사이버공격 행위를 은닉하고, 탐지기법을 우회하기 위한 수단으로 암호화통신 기반 서비스·인프라를 악용하고 있는 실정

- 보안전문기업(CiscoTalos) 분석에 따르면 COVID-19 바이러스가 전 세계적으로 확산됨에 따라 근무 환경이 원격으로 전환되면서 공격자는 Slack, Discord 등 협업 플랫폼을 악용해 악성코드를 은닉 및 배포하는 공격 수행

- 공격자의 입장에선 이러한 협업 플랫폼은 암호화 통신 기반 서비스이므로 악성코드가 암호화(HTTPS)된 통신채널을 통해 유포되어 보안장비를 우회할 수 있는 이점이 있음

- 특히, 해당 보안전문기업에서 악성메일 유포 현황을 조사한 결과, 2020년에 악성코드를 협업 플랫폼에 호스팅 한 뒤 이를 악용하여 유포하는 사례가 증가한 것이 관찰



<그림 9> 협업 플랫폼을 악용한 악성메일 유포 현황

※ Sowing Discord: Reaping the benefits of collaboration app abuse (CISCO TALOS, 21.4)

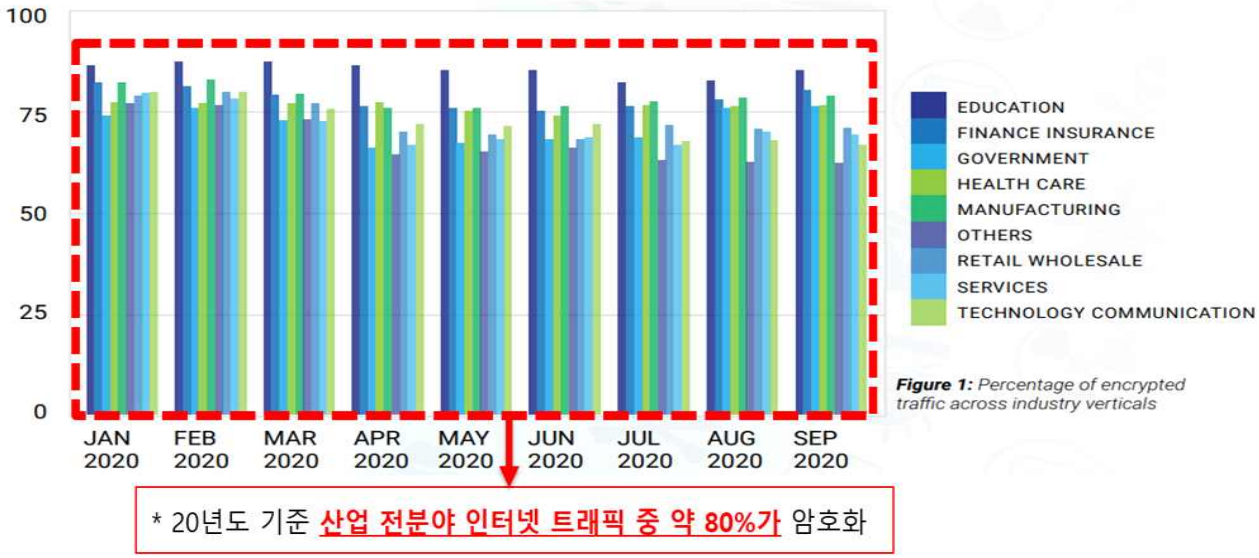
- 보안전문기업(Zscaler)의 보고서에 따르면 2021년 1월 ~ 9월간 탐지된 암호화 통신 공격은 약 207억건에 달하고, 이는 전년도 대비 314% 대비 증가한 양이며 전체 공격 대비 약 80%의 비율을 차지

※ The state of Encrypted Attacks (Zscaler ThreatLabZ, 21.11)

- 글로벌 네트워크 전문업체 CISCO '18년 사이버보안 분석 보고서와 Zscaler의 '20년 분석 보고서에 따르면 '20년도 기준 **산업 전 분야 인터넷 트래픽 중 약 80%가 암호화 통신**이며, **암호화 통신을 악용한 공격이 2019년 대비 260% 증가**하였음

- 또한, 현재 **IoT 디바이스에서는 약 41%가 암호화통신**을 사용하고 있으며 정부의 암호화통신 확대 정책으로 인해 **인터넷망과 유사한 수준으로 증가**할 것으로 예측되는 상황

- 포네몬연구소가 발간한 '21 글로벌 암호화 동향 보고서에 따르면, '15년 이후 암호화를 적용하는 기업이 꾸준히 증가하고 있으며, 조사 응답자의 절반(50%)이 전사적으로 일관되게 적용하는 암호화 계획 또는 전략이 있다고 답함

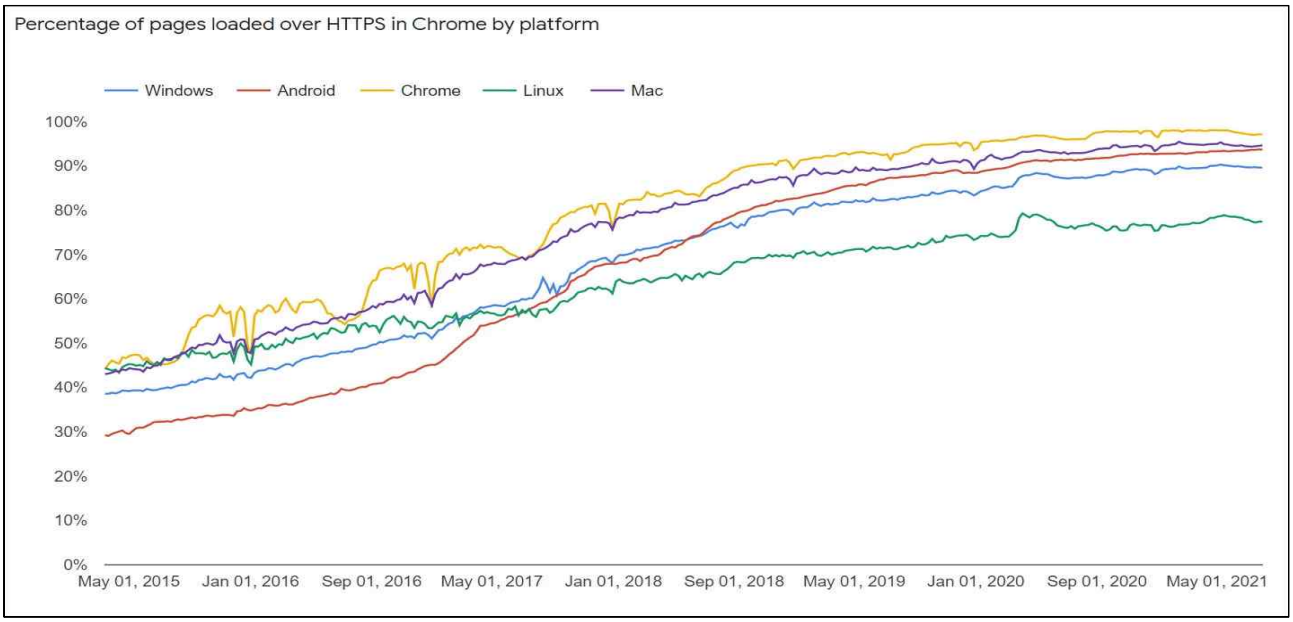


<그림 10> 20년도 기준 산업 전 분야 인터넷 트래픽

- '21년 7월 기준 인터넷 웹브라우저(Windows, Chrome)를 사용하는 사용자의 95% 이상이 HTTPS 암호화 통신을 사용

※ 2015년 기준 약 40%에 불과했던 암호화 통신의 비중이 해마다 증가하고 있음

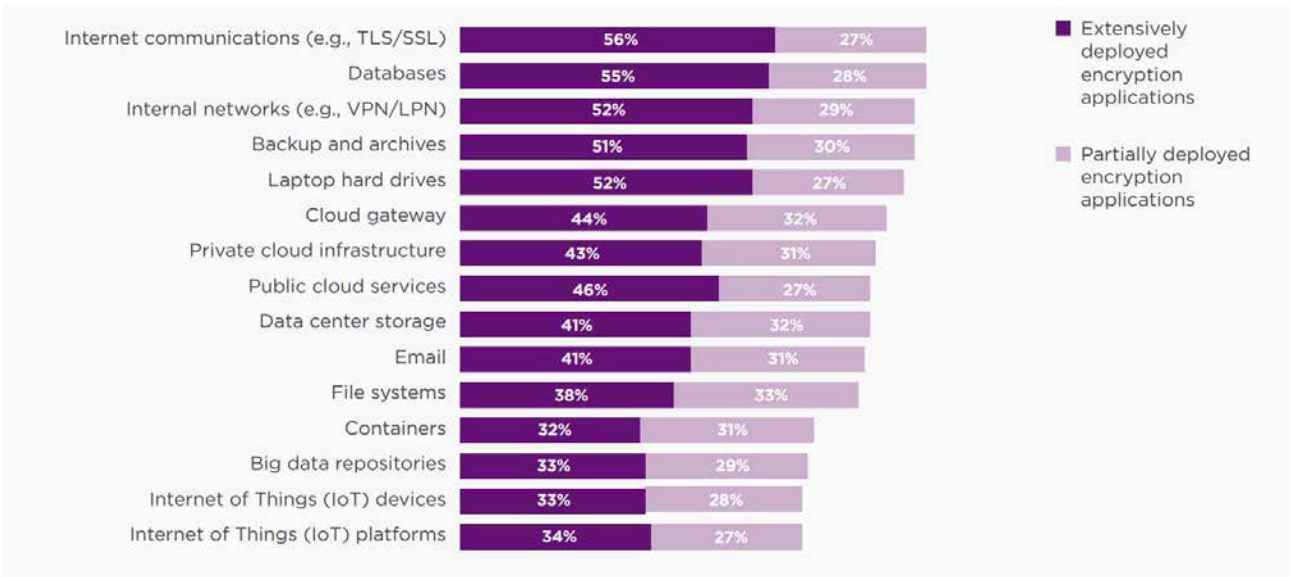
※ google은 정보 가로채기 방지 및 수·발신 정보의 무결성을 보장하기 위해 모든 웹 트래픽에 대해 완전한 암호화를 실현하기 위해 노력 중



<그림 11> 21년도 웹브라우저(Chrome) HTTPS 암호화 통신 사용 현황

- 웹 통신 뿐만 아니라 클라우드, 이메일, VPN, 데이터 센터 등 대부분의 대국민 서비스들이 개인정보보호 및 지적재산권 보호를 위해 암호화통신 기반의 서비스를 제공 중

- 특히, IoT 디바이스·플랫폼을 이용한 스마트 서비스·인프라 또한 정부 시책으로 인해 암호화통신을 의무화하고 있어 암호화통신의 비중은 지속적으로 증가 예정



<그림 12> Consolidated view on the use of 15 encryption technologies

❑ 암호화통신 악용한 사이버공격의 재난화·대형화

ㅇ 암호화 사이버공격의 국민생활 및 주요시설로의 확산

- 국가 및 사회 기반 시스템에 대한 암호화 기반 사이버공격이 증가함에 따라 국민생활과 밀접한 영역으로 피해가 확산되어 대규모의 사회적 혼란 및 경제적 손실이 유발되는 등 재난화·대형화되고 있음

※ 미국 신용기관 에퀴팩스에 대한 해킹으로 약 1억 4천 8백만건의 미국 성인의 개인정보 유출 (2017.7)

※ 깃허브에 대한 1.35Tbps 수준의 DDoS 공격 발생으로 서비스 일부 장애 발생 (2018.2)

※ 비대면 화상회의 솔루션인 Zoom 서비스에 줌폭탄(Zoom bombing), 제로데이 취약점 등의 문제 발생 (2020)

※ 미국 날씨 전문 방송미디어 웨더채널에 대한 랜섬웨어 공격으로 약 90분동안 방송 마비 발생 (2019.4)

※ 미국의 가상화 소프트웨어 기업 시트릭스(Citrix)에 비밀번호 살포(password spraying) 공격을 이용한 해킹이 발생하여 데이터 유출 발생 (2019.3)

※ 웹 호스팅 업체 마루인터넷 랜섬웨어 감염 (2020.3)

※ 미국의 장난감 회사인 클라우드펫츠에 대한 해킹으로 해커가 해당 회사의 인터넷 연결형 스마트 장난감 관련 사용자 계정정보 및 전송된 음성 메시지 데이터에 접근한 사실이 확인됨 (2017.2)

※ 대만정부가 국영으로 운영하는 대만중유(CPC)에 대한 랜섬웨어 공격 (2020.5)

※ 대만 반도체 기업인 파워테크 테크놀로지(PTI)에 대한 공격 발생으로 반도체 생산 시스템 가동 중단 (2020.5)

※ 일본의 혼다(Honda)를 노린 해킹사고로 전세계에 걸쳐있는 혼다 자동차 생산 시스템의 가동이 중단 (2020.6)

※ 국내 원전시설, 발전, 가스 공급 등의 국가 핵심 기반시설에 대한 사이버 공격 시도가 2천 건이 넘는 것으로 확인 (2021 사이버 위협 전망, KISA)

[표 2] 사회기반시설 및 중요 인프라를 겨냥한 사이버공격 사례 (KISA, 보안뉴스, BBC)

구분	내용	발생년도
국내	"솔라윈즈 SUNBURST 보안시스템 취약점 해킹을 통한 공급망 공격" – 솔라윈즈 시스템을 사용하던 대학병원 및 공공기관 등의 제로데이 스캔 공격 탐지	2020
	"의료 관계자들이 사용하는 대한의학회 홈페이지 내 숨겨둔 악성코드 문서 발견" – 의료 관계자를 통해 국내 의료기관 및 제약사에 대한 공격을 위한 시도	
	"국내 원전 시설, 발전, 가스 공급망 등의 국가 핵심기반 시설 공격 시도" – "2021 KISA 사이버 위협 보고서" 공격 시도가 2,000건 이상 확인	2021
	"국내 백화점, 아울렛 등을 운영하는 이랜드 그룹사의 대규모 랜섬웨어 공격" – 그룹사 주요 매장이 클롭(Clop) 랜섬웨어 감염으로 인해 영업 중단되는 사태	
	"원자력 연구원과 한국항공우주산업(KAI)에 대한 사이버 공격을 통한 침투 확인" – 북한 해커의 가상 사설망인 VPN의 취약점을 이용해 전산망 침투	
	"서울대학병원을 비롯한 국가기관 및 병원에 대한 대규모 침해 시도 확인" – 북한 해커 조직인 "김수키" 가 병원망 해킹을 통해 환자의 의료정보 유출가능성 확인	
	"국내 부품 제조기업의 서버 및 직원의 PC를 해킹하여 기업을 협박" – PC 데이터 암호화(1차 공격), 임직원 개인정보, 해외사업 데이터 다크웹 유출(2차 공격), DDoS 공격으로 홈페이지 마비(3차 공격)	
해외	"대만 정부가 국영으로 운영하는 대만중유(CPC)에 대한 랜섬웨어 공격" – 주요 컴퓨터 시스템이 해킹 공격 받아, 컴퓨터 약 7천여대 피해	2020
	"대만 반도체 기업 파워테크 테크놀로지(PTI)에 대한 공격 발생" – 랜섬웨어 감염을 통해 반도체 생산 시스템 가동 중단	
	"일본의 글로벌 자동차 생산 기업인 혼다를 노린 해킹 사고 발생" – 미국, 터키 및 인도 등 전세계의 혼다 자동차 생산 시스템 가동 중단	
	"CCTV 보안 카메라 제공 업체인 "SmartPSS" 웹 사이트 공격" – 다크사이드 연계 조직인 UNC2465는 웹사이트를 해킹해 트로이 목마 설치	2021
	세계 6위의 미국 보험사 CNA가 "Phoenix Locker" 랜섬웨어 공격 – CNA 네트워크에 연결된 15,000개 이상의 기기가 암호화 됨	
	"미국 플로리다 소도시의 국가 기반 시설 제어 망인 하수 처리 시설 공격 시도" – 원격 제어 소프트의 취약점을 통해 제어 시설에 접근하여 해킹 시도	

- 특히 랜섬웨어는 '20년 이후 암호화 기반 사이버 공격의 가장 큰 비중을 차지하고 있으며, 국내 다수의 기업 역시 랜섬웨어로 인한 경제적 손실 발생

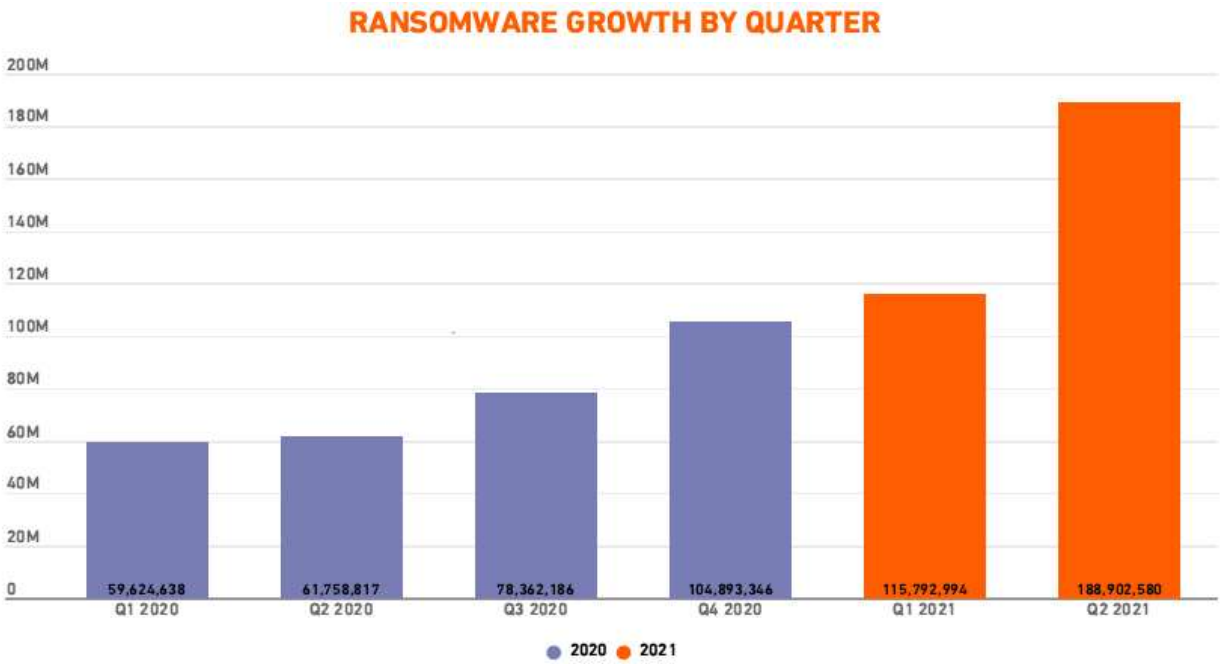
※ 국내 기업의 59.8%가 랜섬웨어 피해 경험 (20년 정보보호실태조사)

※ 공격 전 금전을 요구하고 지불하지 않으면 추가 공격을 예고하는 형태의 랜섬 디도스 공격이 국제 사이버 범죄집단 팬시 베어에서 국내 은행을 상대로 발생 (2021년 사이버 위협 전망, KISA)

- 랜섬웨어 범죄조직은 더욱 분업화, 전문화 되어가는 추세

※ 데이터 복구에 필요한 금전을 요구하는데 그치지 않고 데이터를 유출하는 등의 협박과 이를 전담하는 조직의 등장과 같이 분업화 형태로 변화

※ 랜섬웨어로 부당이익을 얻고자 하는 수요가 증가함에 따라, 랜섬웨어를 제작·판매하는 '서비스형 랜섬웨어(RasS)'로 진화



<그림 13> 매 분기마다 증가하는 랜섬웨어 - 21' SonicWall CYBER THREAT REPORT

- IoT를 대상으로 하는 사이버 공격은 2021년 상반기 기준 전년도 대비 59% 이상 증가

※ 북미 IoT를 대상으로 한 사이버 공격은 전년도 대비 21% 증가하였으며, 유럽은 113% 증가하였고, 아시아의 경우 190%로 가장 큰 증가율을 보임.

※ 최근 미국, 일본의 대학에서 음성 명령을 암호화한 레이저를 이용한 AI 스피커 해킹 성공 사례를 통해 일상에 많이 사용되고 있는 IoT 결합 서비스를 대상으로 하는 사이버 위협의 증가 가능성을 시사 (2020년 7대 사이버 공격 전망, KISA)

- 2027년까지 사용되는 IoT 장비의 개수가 약 410억 개로 증가할 것으로 전망되며, 이를 악용한 사이버 범죄 역시 함께 증가할 것으로 예측

❑ 암호화 트래픽 기반 사이버보안 위협·사고 사례

ㅇ (국내) 대북 매체 홈페이지를 통한 악성코드 유포

- 국내 북한 관련 언론사 홈페이지 워터링홀(APT) 공격지로 악용

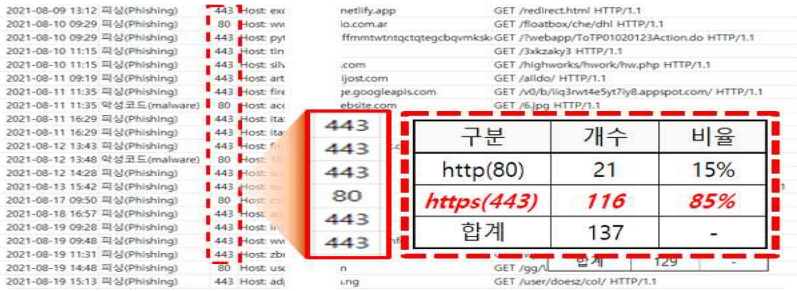
- 언론사 홈페이지 및 악성코드 유포지 암호화 통신(HTTPS)을 악용해 악성코드 감염 행위 은닉 및 공격 피해자 데이터 절취

<그림 14> 워터링홀 공격 방법

※ North Korean APT InkySquid Infects Victims Using Browser Exploits (Volexity, 21.8)

ㅇ (국내) 과학기술사이버안전센터 악성메일 위협 분석결과, 최근(7~8月) 악성경유지 중 85% 암호화 통신(HTTPS) 악용

- 분석을 통해 확인된 악성경유지는 암호화 통신을 수행할 경우 평문기반 패턴매칭 탐지기법을 활용한 보안장비에서 탐지 불가



<그림 15> 사이버보안 위협 정보 분석결과(암호화 통신 기반 위협 급증)

ㅇ (국내) VPN 취약점을 악용해 국내 연구기관·방산업체 공격

- 암호화 통신을 수행하는 보안장비(VPN) 취약점을 악용해 내부 시스템 공격 시도

※ 방산업체 해킹 어떻게 이뤄졌나…VPN 등 민간 '취약점' 집중 공격 (뉴스1, 21.7)

ㅇ (국내) 아파트 홈 네트워크 기기 해킹

- 아파트 월패드 해킹으로 거주자 사생활 영상 다크웹 등에 불법 유통

<그림 16> 다크웹에 게시된 국내 월패드 유출 영상

※ 아파트 '월패드' 해킹 공포 확산...대응 방법은? (YTN, 21.11)

ㅇ (국내) 서울 소재 아파트, 설비 자동제어 시스템 해킹 경유지로 악용

- 냉난방기, 배수펌프, 난방수 온도조절 등을 자동으로 제어하는 아파트 설비 자동제어 시스템 해킹 경유지로 악용

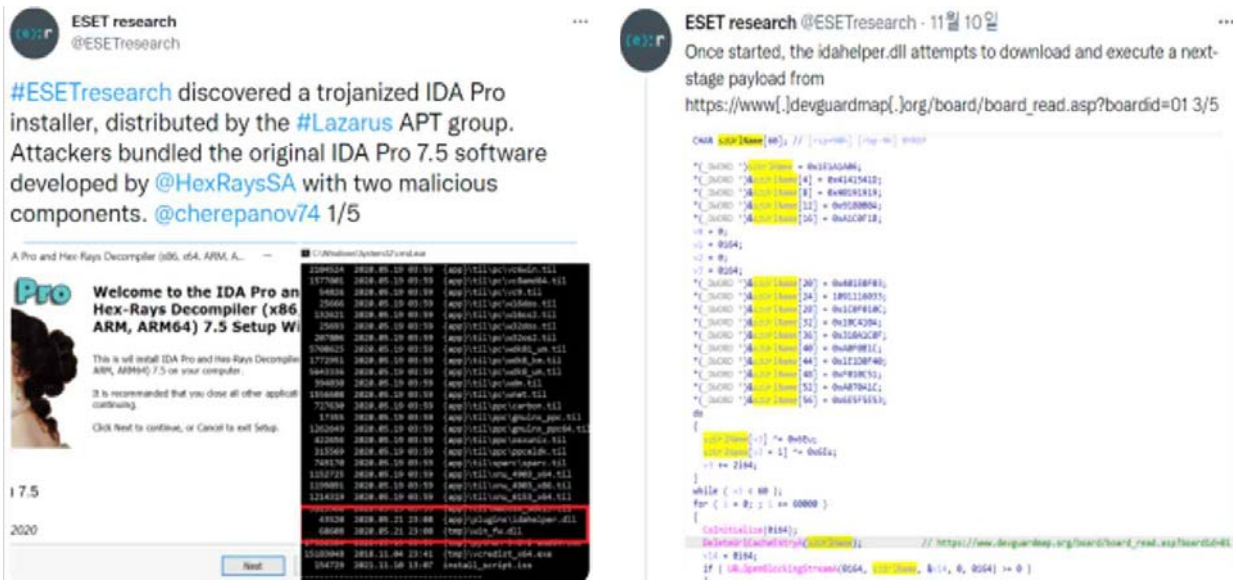
- 해당 경유지는 해외 40개 국가에 소재해 있는 인터넷 서버를 공격하는 경유지로 악용

※ 아파트 월패드 이어 설비제어시스템도 뚫려…(이데일리, 21.12)

ㅇ (국내) 북한 추정 해커조직 불특정 다수 사이버보안 전문가 공격 시도

- 사이버보안 전문가가 사용하는 분석 도구에 악성코드를 포함시켜 사이버보안 전문가를 노린 공격 수행

- 해당 분석 도구 설치 프로그램 실행 시 암호화 통신을 수행하는 C&C에서 추가 악성코드를 다운로드 하는 등 악성코드 감염행위 은닉



<그림 17> ESET research 악성코드 분석

ㅇ (미국) 국가기반시설에 대한 지속적인 랜섬웨어 공격

- 국토안보부의 보고서에 따르면, BlackMatter로 명명된 랜섬웨어가 2021년

7월부터 미국 전역의 국가기반시설에 대한 공격을 수행하였으며, 감염된 PC의 데이터를 암호화통신을 통해 탈취하는 것으로 확인

※ BlackMatter Ransomware(CISA, 21.10)

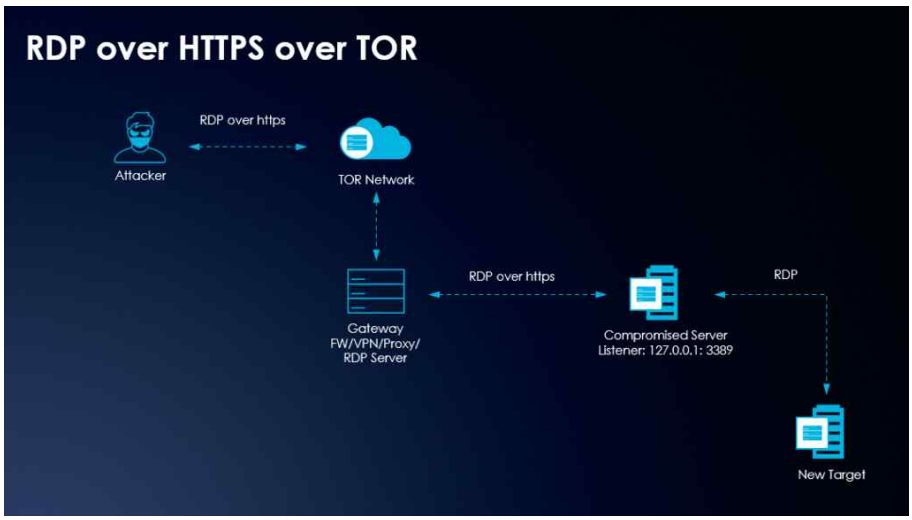
ㅇ (미국) 미국 플로리다 주 상수도 시스템(IoT기반) 해킹

- 미상의 해커가 플로리다 주 상수도 시스템 해킹을 통해 오염 시도
- 상수도 제어시스템 내 설치되어 있는 원격 접속 프로그램(팀뷰어)을 악용, 수산화나트륨 투입 비율 100배 상승 조절

※ Compromise of U.S. Water Treatment Facility (CISA,21.2)

ㅇ (미국) 미국 동부 최대의 송유회사 Colonial Pipeline, 랜섬웨어 감염

- 미국 동부 해안 연료 공급의 절반을 담당하는 Colonial Pipeline이 DarkSide 랜섬웨어에 감염되어 송유관 기능 6일간 마비
- 공격자는 초기공격부터 랜섬웨어 공격 수행까지 암호화 통신을 악용해 공격 징후 발견 및 초기 대응 지연



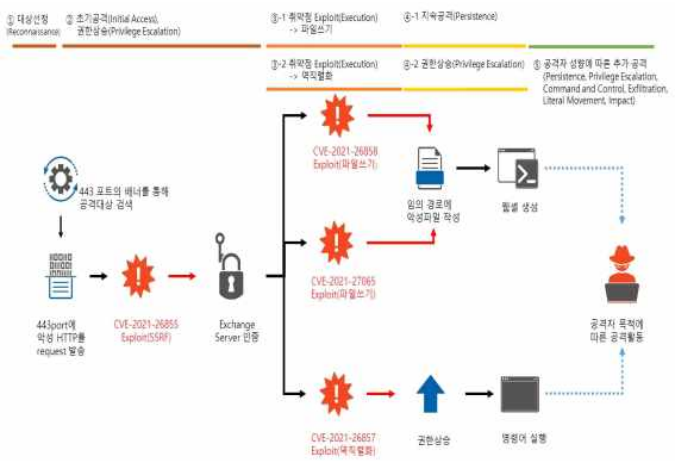
<그림 18> Darkside Ransomware Analysis(Varonis, 2021)

※ Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign (Varonis, 21.7)

ㅇ (국내) MS Exchange 서버 취약점을 악용한 침해사고

- 443 포트(HTTPS)를 통하여 취약한 버전의 Exchange 서버를 선정

- 공격코드를 실행하여 서버 내부에 접근할 수 있는 권한 획득



<그림 19> MS Exchange Server 취약점을 악용한 공격 절차 개요도(KISA, 2021)

※ 국내 기업들도 당했다! MS 익스체인지 서버 취약점 사고사례 살펴보니 (보안뉴스, 21.5)

ㅇ (미국) PulseSecureVPN 취약점 악용 뉴욕 철도교통관리시스템 공격

- 보안전문기업 Fireeye의 보고서에 따르면 Pulse Secure VPN의 취약점인 CVE-2021-22893를 악용한 그룹의 공격 정황을 확인

- 해당 공격의 일환으로 뉴욕 **철도교통관리시스템** 내부에 해당 취약점을 악용하여 침투에 성공한 것으로 확인됨

※ Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day(Fireeye, 21.6)

ㅇ (이란) 국가 배후 해킹조직의 기반시설(철도·유류) 사이버공격

- 해킹그룹 Indra의 와이퍼 악성코드 Meteor를 통한 공격으로 인한 **열차 행정시스템 마비 및 웹·키오스크 화면의 디페이싱** 공격 수행

<그림 20> 철도시스템 해킹 후 전광판 화면변조

- 동일 해킹그룹으로 추정되는 조직의 유류 시스템(연료보조 수급 카드시스템) 공격으로 **시스템 마비**

- 해당 공격들의 영향으로 당일 대다수 열차 운행 지연·중단 및 **12일간의 유류 유통 장애 발생**

※ MeteorExpress, Mysterious Wiper Paralyzes Iranian Trains with Epic Troll (SentinelLABS, 21.7)

ㅇ (이란) 에빈 교도소 사이버공격으로 CCTV 영상 유출

- 이란의 핵티비스트 단체가 에빈 교도소 보안 카메라 영상 탈취 후 유포

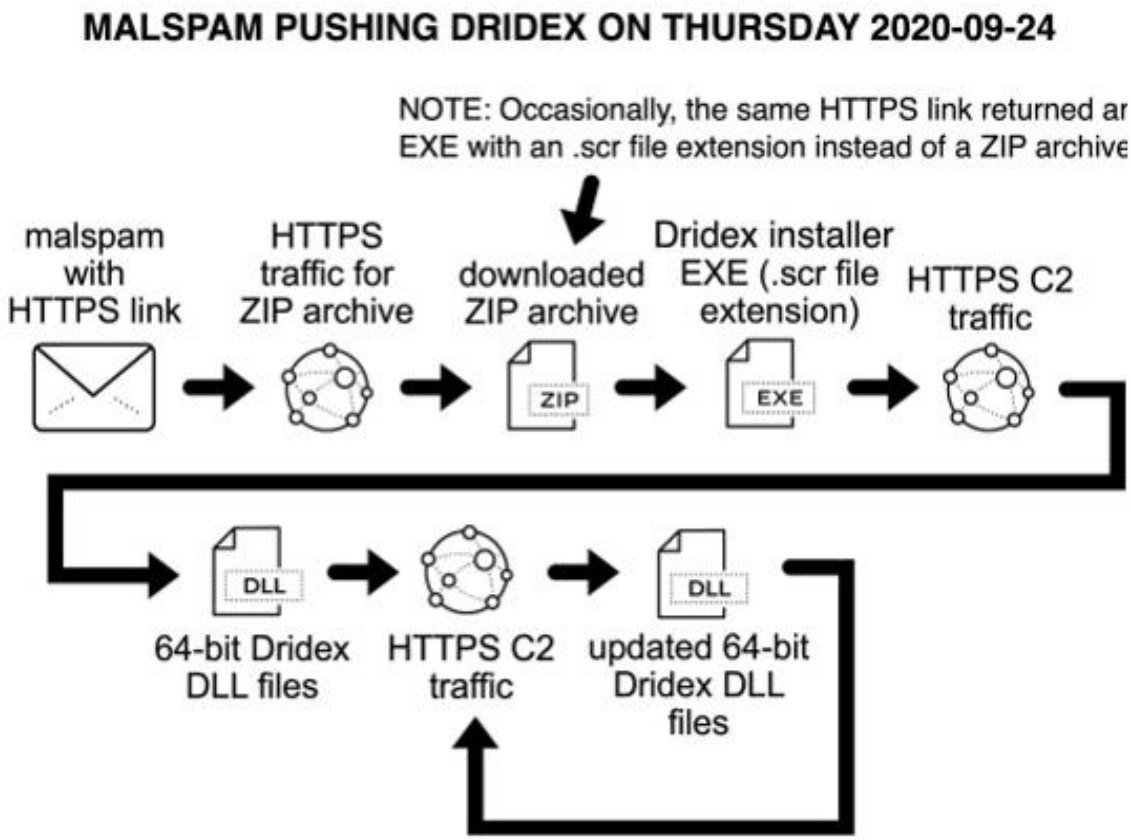
<그림 21> 보안카메라 해킹 후 화면 변조

※ Hackers Release Security Footage From Iran’s Evin Prison(IRAN International, 21.8)

ㅇ (스위스) 지중해 해운 회사(MSC) 사이버 공격

- 지중해 해운 회사에 C2 서버와 암호화 통신을 수행하는 멀웨어 Dridex를 이용한 공격 발생 및 **내부 직원들의 메일계정 다수 탈취**

- 이후 탈취한 메일계정들을 이용해 **'해사 공급망' 유관 기관들**에 스피어 피싱 메일 유포, 이로 인한 **추가 피해 발생**



<그림 22> Examining Dridex Infection Traffic(Paloalto, 2020.8)

제2절 사회문제 원인 분석

❑ 암호화통신 중심의 네트워크 패러다임 전환

ㅇ **개인정보 및 네트워크 데이터 보호 등을 위한 암호화통신 활용 활성화**

- 정보보호 중요성 증가에 따른 데이터 암호화 비율 증가

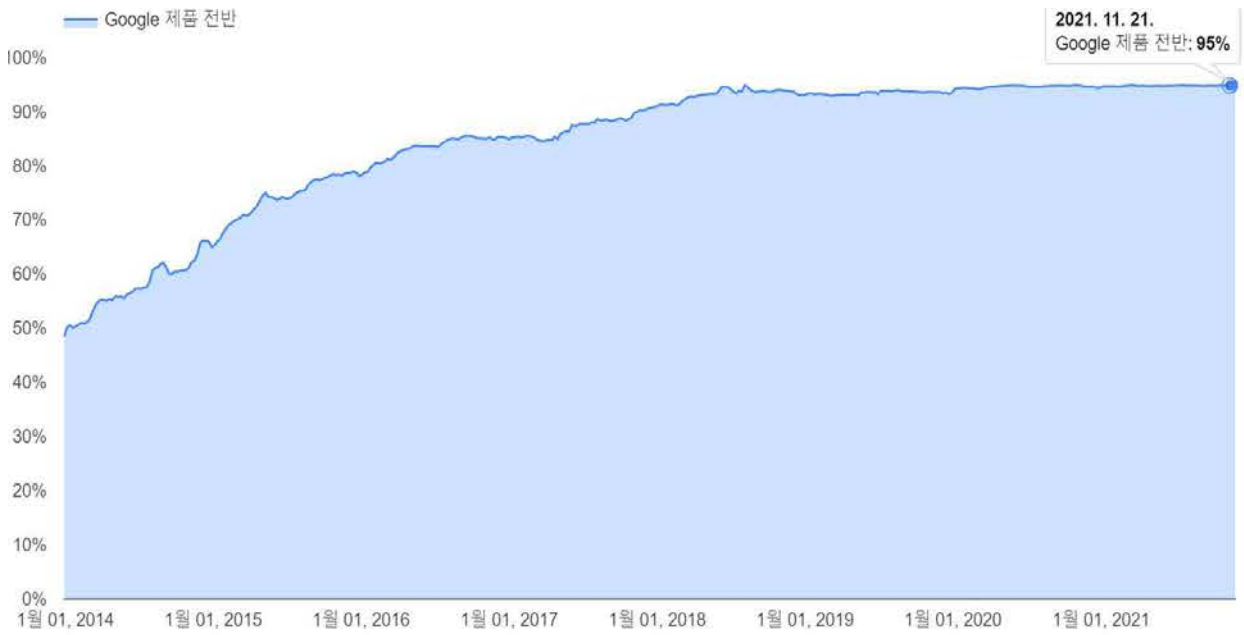
- 전통적인 유·무선 통신을 포함하여 IoT, 5G 및 기간 통신망 등 초연결 기반 서비스·인프라의 통신환경이 **'평문' → '암호문'**으로 급변

- 국내외 암호화통신 의무화 시행으로 인한 암호화통신 증가

※ EU GDPR, 국내 개인정보보호법 개정 등에 의해 개인정보 보호 조치 필수

※ 행정안전부의 HTTPS-ONLY 정책 검토 (2020.12), 구글의 HTTPS 정책 (2015 ~ 현재), 보안 프로토콜 준수 및 안전한 파라미터 설정 (IoT 공통보안원칙, KISA) 등에 의해 네트워크 암호화 프로토콜 사용이 필수적

※ 구글에서 제공하는 서비스의 95% 이상이 암호화 통신을 사용



<그림 23> Google 제품 내 암호화된 트래픽 비율

- 전 세계적으로 암호화 통신 바탕의 IoT기반 인프라·서비스가 급속히 구축·확산되고 있으며, 이를 활용한 대국민 서비스의 안전성·보안성 확보를 위해 암호화 트래픽 기반 악성행위의 대응 필요성이 시급히 대두됨

- 다양한 통신 디바이스가 연결되는 초연결 시대의 진입에 따라 이를 대상으로 한 악성행위도 급격하게 증가하고 있으며, 특히 암호화 통신을 악용하여 탐지를 더욱 어렵게 하는 사례가 폭발적으로 증가하고 있음

ㅇ 디바이스 및 통신서비스의 암호화 통신 확대

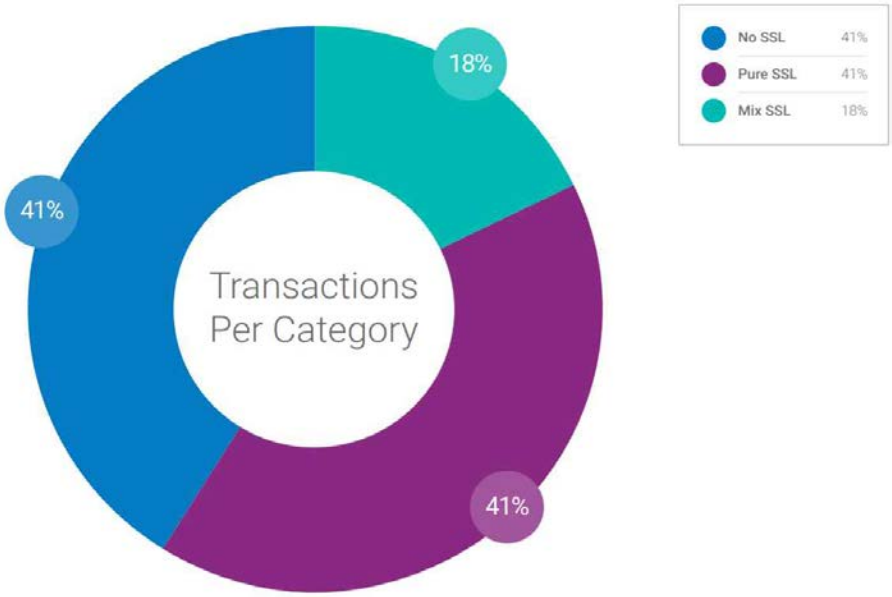
- 클라우드 및 빅데이터 등의 서비스가 증가하면서 데이터의 저장 및 송·수신 시 데이터 유출을 방지하기 위해 네트워크 트래픽에 대한 암호화 필요

- 최근 클라우드 사용의 증가로 인해 이를 보호하기 위한 클라우드 보안 서비스 시장의 성장이 두드러짐

- 클라우드 보안은 데이터의 안전한 저장·활용뿐만 아니라 사용자의 인증 및 안전한 통신환경이 필수적으로 요구되기 때문에 암호화 통신이 필수적으로 요구됨

- 클라우드 시장이 확대됨에 따라 ICT보안 시장에서의 클라우드 보안 및 암호화통신의 사용은 점차 확대될 것으로 예측됨

- 또한, 글로벌 보안업체(Zscaler) 조사에 따르면, **모든 통신을 암호화 하는 IoT 디바이스는 41%**로 조사되었으며, 非암호화 통신 41%, 일부 통신만 암호화 18%로 확인됨



<그림 24> The percentage of IoT transactions per category, Zscaler ThreatLab Report 2020

- IoT 디바이스는 현재 41%가 암호통신을 사용하지만, 향후 IoT 보안정책 강화로 인해 인터넷망과 유사한 수준으로 증가할 것으로 예측됨

- 특히 낮은 CPU 성능 및 작은 메모리 용량을 가지는 IoT 디바이스들에 특화된 경량 메시징 프로토콜을 지원할 수 있는 LEA 등의 경량 암호화 알고리즘들이 새로이 **ISO/IEC 경량 블록 암호 표준으로 지정**되고 있음

※ LEA를 포함하여 ECC, SIMON, Speck, HIGHT 등 IoT기기의 암호화 통신을 위한 다양한 경량 암호 연구가 현재 진행 중

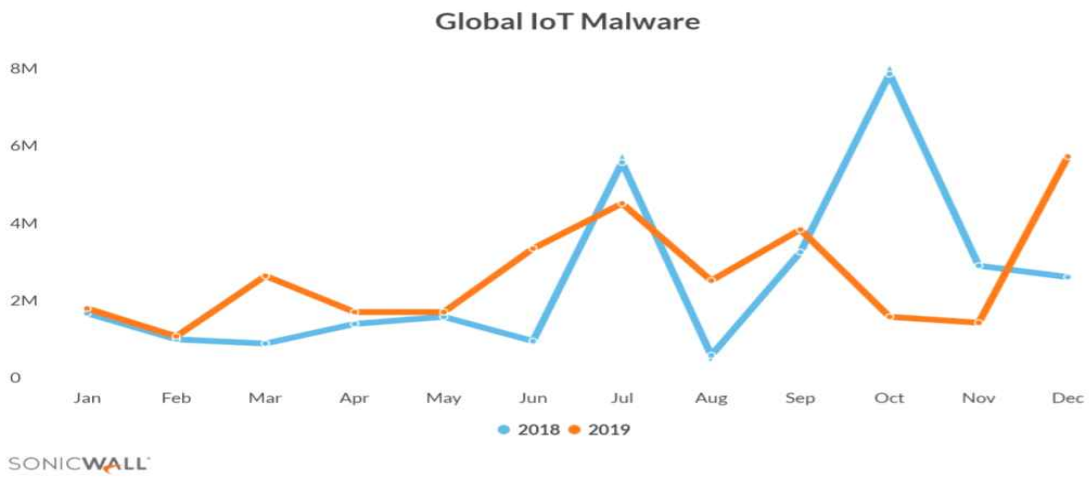
- 스마트 홈, 스마트 City, 스마트 팩토리 등 초연결 스마트 환경이 구축됨에 따라 저전력 및 저사양 **IoT 기기 환경에 대한 보안 수준을 점차 강화**하기 위해 **암호화 통신 및 암호화 통신 IoT 보안솔루션이 대중화**

※ AutoCrypt사의 'AutoCrypt V2X'는 보안 통신을 위한 암호화 및 전자서명을 제공, PentaSecurity사의 'HomeCrypt'는 통신데이터 암호화를 위한 SSL-VPN for IoT를 적용

※ 스마트 경량 IoT 기기용 PANA 보안 프로토콜 기술, TLS 기술, DTLS 보안프로토콜 기술, 링크 계층 암호키 분배 기술 등의 연구 및 개발을 통해 보안 프로토콜 적용 확장 가능

※ AMI 전문업체 및 보안업체 등에 기술이전을 통해 IoT 기기의 암호화 통신과 같은 보안기술 적용이 증가할 것으로 보임

- 글로벌 보안업체(SonicWall) 조사에 따르면, 18년 대비 19년에 TLS 및 SSL 암호화 표준 기반의 HTTPS를 거친 **IoT 멀웨어 공격이 5% 증가**했으며, **총 공격량은 3,430만 건으로 집계**됨



<그림 25> Global IoT Malware, 2020 SonicWall CYBER THREAT REAPORT

- 포춘 비즈니스 인사이츠(Fortune Business Insights)는 글로벌 암호화 소프트웨어 시장 가치가 2019년부터 2027년까지 연평균 성장률은 14.1%를 기록할 것이라 전망

※ 코로나 시대에 암호화 소프트웨어 시장 성장으로 인해 암호화 통신이 증가할 것으로 예상되며, 2019년 88억 2,000억 달러에서 2027년 249억 4,000억 달러 수준으로 성장할 것이라는 전망

❑ 암호화 통신 환경 전환을 위한 정부 정책

○ **(국내)** 개인정보보호법 시행 및 개인정보보호위원회가 설치·운영됨에 따라 개인정보를 취급하는 모든 웹사이트들은 보안 서버를 의무적으로 구축해야함

- 개인정보보호법 제30조 1항에는 개인정보처리자가 수행해야 할 안정성 확보 필요 조치 등이 명시되어 있으며, 제3호 '개인정보를 안전하게 저장, 전송할 수 있는 암호화 기술의 적용 또는 이에 상응'에 따라 SSL 보안 서버 구축 필요

- 이를 위반할 경우 개인정보보호법 제75조 제2항 제6호에 따라 3천만 원 이하의 과태료가 부과

○ **(국내)** 디지털사회 시대의 사이버위협 및 정보보호 패러다임 변화에 대응하기 위해『디지털 안심국가 실현』중점 추진

- 정부는 다양한 정책을 발표하고, 성공적인 정책추진을 위한 네트워크(인터넷, IoT 등) 보안 요구사항을 정립

- 사물인터넷(IoT) 정보보호 로드맵 3개년 계획(舊미래창조과학부, '15.6)

※ 홈 · 가전, 의료, 교통(ITS), 환경 · 재난, 제조, 건설, 에너지 등 7대 IoT 분야의 보안성 확보를 위한 「암호화 통신 기반 공통 보안원칙 도출」

- 세계 최고 디지털 안심국가 실현을 위한 K-사이버방역 추진전략(과학기술정보통신부, '20.2)

※ 5G, 인공지능 등 4차 산업혁명, 비대면 경제 활성화에 따라 증가하는 사이버 보안 위협으로부터 국민이 안전하고 신뢰할 수 있는 세계 최고의 디지털안심국가를 실현하기 위한 정보보호 종합 계획

- 디지털 경제로의 대전환을 위한 21년 디지털 뉴딜 실행계획(관계부처 합동, '21.1)

※ 일반국도의 지능형교통시스템(ITS) 구축, 108개 도시에 스마트 City 통합플랫폼을 조기 보급하여 스마트 City 안전망 혜택 제공

- **(국토교통부, 세종시)** 한국판 디지털 뉴딜 계획 중 사회간접자본(SOC)

디지털화의 일환으로 스마트 City, 스마트교통 등 IoT 기반의 도시·교통체계 첨단화 사업을 추진 중

- **(해양수산부)** 해상 정보통신 분야의 신산업 육성을 위한 초고속 해상무선통신망(LTE-M) 구축 사업을 추진

- **(경찰청)** 국민 생활 안전을 강화하기 위해 영상데이터 모니터링 및 위치정보 모니터링 등을 위한 안전한 스마트치안 센터 구축 사업 추진

ㅇ **(미국)** 미국 정부는 사이버위협을 방지하고 IoT 기기 보안을 강화하기 위한 조치로 '사물인터넷(IoT) 사이버보안 개선법'을 제정('20.12)하였으며, 기기 제조업체는 새로운 보안 표준을 충족해야 함

- 특히, 미국 캘리포니아에서는 '사물인터넷 보안법(SB327)'이 2020년 1월부터 발효돼 향후 인터넷 연결이 가능한 모든 기기는 보안 기능을 필수로 탑재해야 하며, 해당 법은 커넥티드 디바이스 생산 기업이 해당 기기에 합당한 '보안' 기능을 반드시 탑재하도록 규제

ㅇ **(일본)** 일본 총무성은 2017년 1월 사이버보안 TF를 구성하고 봇넷 대응 등 IoT보안 정책을 체계적으로 추진하기 위해 'IoT 종합보안대책'(2017.10)을 수립, 5G 상용화에 따른 신규 위협 발생, AI활용 등 급변하는 ICT환경에 대응하기 위해 'IoT·5G 보안 종합 대책'(19.08)을 발표 및 추진

- 총무성, 경제산업성 등 다부처 협력을 통해 '사이버 물리 보안 대책 프레임워크'(19.04)를 발표함으로써 IoT시스템, 서비스, 네트워크, 단말에 이르기까지 사이버보안 대책 수립을 추진

- 특히, CCDS, EDSA 보안 인증도입을 통해 데이터 통신 간에 암호화 수행 및 검증을 의무화하고 있음

○ **(중국)** 국가인터넷정보판공실에서 사이버 공간상의 국가주권 수호를 반영한 '국가 사이버 보안 전략'(16.11) 발표

- 특히, 사이버공간에서 통신비밀, 언론자유, 상업성 비밀, 명예권, 재산권 등에 대한 합법적 권익보호 강화

○ **(유럽)** 유럽연합은 2019년 6월 27일부터 새로운 정보통신기술규정인 사이버보안법(Cybersecurity Act)을 시행하여 전체 유럽연합에 적용되는 사이버보안 제품 및 서비스에 대한 인증을 강화함

- 최근 '암호화를 통한, 그리고 암호화 상황에서도 안전한 보안'(Security through and despite encryption, 20.07)이라는 결의서를 발표함으로서 부작용을 최소화할 수 있는 End-to-End 암호화의 중요성을 강조

❑ 코로나(언택트) 시대의 암호화 사이버 위협 증가

○ 언택트 환경의 보안 사각지대를 노린 암호화 공격 급증

- 사회적 거리두기가 장기화됨에 따른 비대면 근무환경의 활성화로 인해 VPN, RDP 등을 이용한 원격 근무가 증가하였으며, 개인정보 및 업무자료 유·노출 예방을 위해 암호화통신의 사용량 또한 함께 증가함

- 재택근무와 비대면 회의뿐만 아니라 언택트 환경을 기반으로 한 온라인 게임/쇼핑, 원격 교육 등의 서비스들이 활성화됨

- 원격근무에 사용되는 이메일, VPN, 원격접속(RDP) 등을 대상으로 하는 사이버 공격 및 온라인 쇼핑, 택배 등과 관련된 이메일이나 문자메세지를 위장한 암호화 공격 급증(악성코드, 랜섬웨어 등)

※ 시스코에서는 COVID-19로 인해 암호화 통신 기반의 원격 업무 환경이 필수적으로

요구되고 있으며, 이를 악용하는 공격행위 은닉 사례가 증가하고 있음을 알림

※ 공격자는 원격근무에 이용되는 직원의 VPN 계정 정보를 획득하고 보안 취약점을 이용해 기업 내부망에 침투, 기업의 S/W 변조를 시도 (Avast)

※ 업무관련, 교육관련 키워드를 악용한 피싱 사이트를 통해 사용자에게 블루크랩(BlueCrab) 랜섬웨어를 유포하는 공격 발생 (2020. AhnLab)

※ VPN은 암호화 기반의 통신을 수행하기 때문에 악성행위에 대한 분석이 어려움

<그림 26> Security impacts and prospects from the COVID-19 (ISACA, 2020)

ㅇ 지능형 지속 위협(APT : Advanced Persistent Threat)의 증가

- APT공격의 경우 공격자 추적을 피하기 위해 VPN과 같은 암호화 통신을 이용하기 때문에 기존 평문기반 네트워크 트래픽 분석으로 탐지가 어려움

- COVID-19와 같이 사회적 이목이 집중되는 키워드 등을 활용하여 개인PC 및 경유 서버를 탈취하여 경유지로 활용, 이때 공격자는 암호화 통신 활용하여 접근하기 때문에 이에 대한 탐지 및 대응이 불가함

- 전문화된 해킹조직을 통한 주요기반시설과 인프라에 대한 APT 공격이 지속적으로 증가되는 추세

ㅇ 안전한 언택트 환경 활용을 위한 사용자 중심 안전대책 수립

- 한국인터넷진흥원(KISA)에서는 이러한 사이버 공격들로부터 안전한 VPN, RDP 활용을 위하여 재택·원격 근무 정보보호 6대 실천 수칙 발표

[표 3] 재택·원격근무 정보보호 6대 실천 수칙 (KISA, 2020)

	사용자 실천 수칙	보안관리자 실천 수칙
1	개인 PC 최신 보안 업데이트 – 재택근무 시 개인 PC를 업무에 사용하는 경우 운영체제 및 응용프로그램을 최신 상태로 유지	원격근무시스템(VPN) 사용 권장 – 사내 보안정책에 따른 VPN 사용 권장 – 미보유 기업의 경우 사내망 접속PC 백신 최신화 및 수시 점검 정책 시행
2	백신 프로그램 업데이트 및 검사 – 백신 보안패치 최신 업데이트 및 주기적 바이러스 검사 (원격근무 접속 전 및 일일 1회 이상) 수행 – 백신 자동 업데이트 설정 및 실시간 검사기능 해제 금지	재택근무자 대상 보안지침 마련 및 보안 인식 제고 – PC 운영체제, 소프트웨어, 백신 최신화, 공유기 패스워드 설정, 웹사이트 이용 자제 등 보안지침 마련 및 교육 실시
3	가정용 공유기 보안설정(비밀번호) 및 사설 와이파이·공용PC 사용 자제 – 가정의 인터넷 공유기를 최신 SW로 업데이트하고 공유기 비밀번호 설정 ※ 비밀번호는 유추가 어렵도록 특수문자 등 포함 – 개인영업장(카페, 식당 등)에 설치된 사설 와이파이, 공용PC를 이용한 재택근무 자제	재택근무자의 사용자 계정 및 접근 권한 관리 – 재택근무자의 비밀번호 설정 강화 및 재택근무 시 접근권한 최소화 방안 마련 – 원격근무시스템 접근 시 비밀번호 이외 OTP 등 2차 인증수단 적용 필요
4	회사 메일 권장, 개인 메일 사용주의 – 회사에서 제공하는 메일서비스 사용 권장 – 상용 메일서비스 사용 시 목적 외 메일 열람 자제 및 링크·파일 실행 주의 ※ 공용PC에서 메일열람 후 반드시 접속 종료	일정 시간 부재 시 네트워크 차단 – 재택근무자가 사내 네트워크 접속 후 부재 시 네트워크 접속 차단 설정 ※ 10분~30분 동안 부재 시 차단 권장
5	불필요한 웹사이트 이용 자제 – 업무를 위한 웹사이트 이용 이외에 개인 목적의 웹사이트 접속을 자제	원격 접속 모니터링 강화 – 재택근무자의 사내 네트워크 접속 현황 관리 및 우회 접속 집중 모니터링 실시
6	파일 다운로드 주의(랜섬웨어 감염 주의) – 메일 또는 웹브라우저를 통해 파일 다운로드 시 랜섬웨어 감염 가능성이 있으므로 출처가 의심스러운 파일 다운로드 금지 – 업무 파일은 별도의 저장장치에 주기적 백업 실시	개인정보, 기업정보 등 데이터 보안 (랜섬웨어 감염 주의) – 기업의 중요 문서의 경우 DRM 설정 등 데이터 유출 방지 대책 마련 ※ 데이터 외부 유출 시 관리자의 승인 절차 등 – 재택근무자의 작업 파일 내부 반입 시 랜섬웨어 감염 여부 등 파일 검사 필요 – 중요 기업 데이터 백업 권장

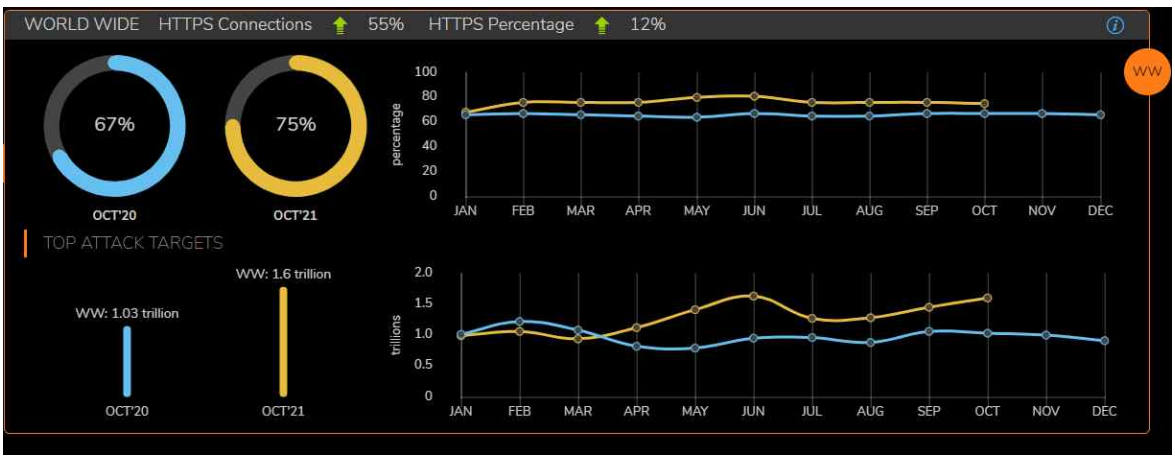
❑ 암호화 사이버공격에 대한 대응체계 미흡

ㅇ 암호화 사이버공격의 증가와 공격대상의 다양화

- 암호화 기능이 추가된 프로토콜의 사용 증가

※ 네트워크 트래픽을 중간에 탈취하여 악용하는 스니핑(sniffing) 공격을 방지하기 위해 프로토콜의 암호화 필요

※ 원격 접속을 위해 사용되는 SSH(Secure Shell), 파일전송을 위해 사용되는 SFTP(Secure File Transfer protocol), 메일서비스에 사용되는 SMTPS(Simple Mail Transfer Protocol Secure), POP3S(Post Office Protocol over SSL/TLS) 등은 모두 기존 프로토콜에서 암호화 통신 기능이 추가된 형태



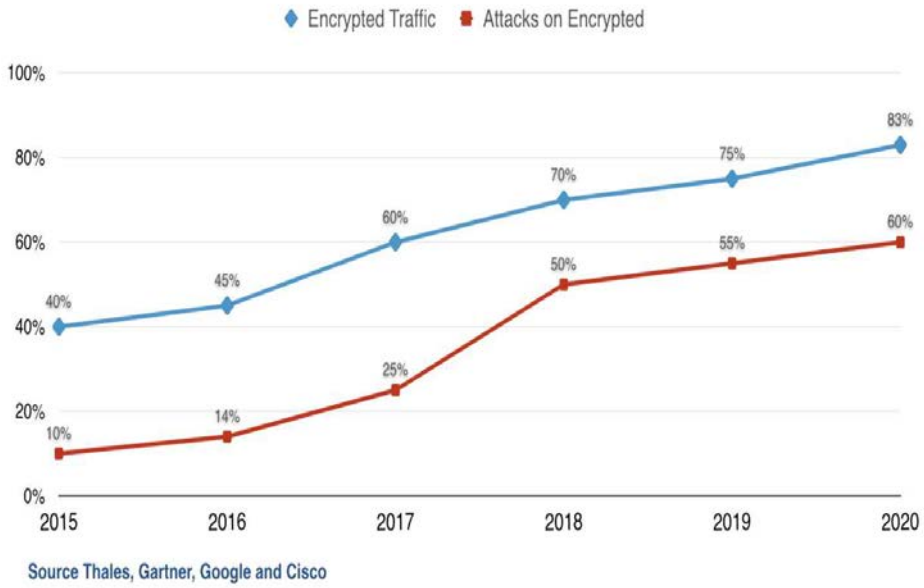
<그림 27> 암호화된 사이버 공격의 증가 - SonicWall Lab.

- 암호화를 악용하여 보안장비의 탐지를 우회하는 사이버공격의 증가

※ 네트워크 트래픽의 내용을 확인할 수 없는 암호화 통신을 악용하여 보안장비 및 기존 평문기반 관제체계 우회

※ 네트워크 트래픽의 암호화와 함께 암호화된 사이버공격 또한 지속적으로 증가

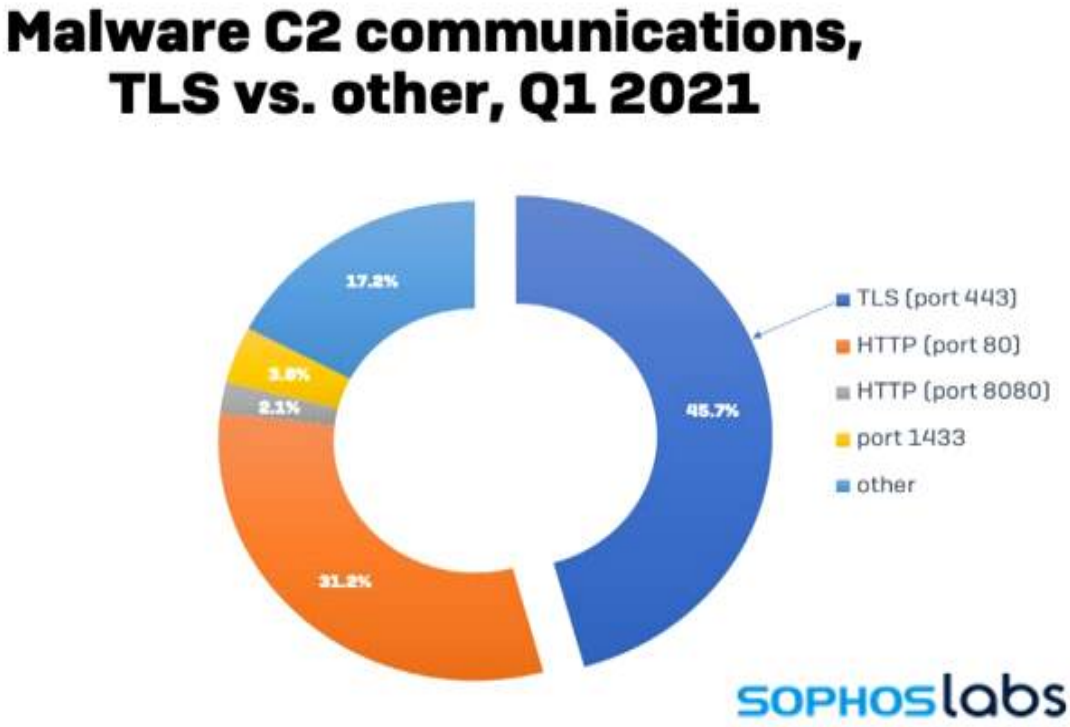
※ 2020년을 기준으로, 암호화 트래픽 내의 악성행위는 60%를 넘어서고 있으며 HTTPS를 통한 악성코드 배포, 명령 및 제어 등이 주로 발생



<그림 28> 암호화 트래픽에서의 공격행위 증가

※ 보안전문기업 SonicWall의 21년도 위협분석보고서에 따르면 아시아 지역에서의 암호화 통신을 악용한 사이버 공격이 전년대비 151% 증가함

※ 보안전문기업 SOPHOS의 21년도 1분기 위협분석보고서에 따르면 전체 알려진 멀웨어들 중 약 절반(45.7%)이 암호화 통신(HTTPS 등)을 사용



<그림 29> 암호화 통신 악용 사이버 공격 현황 (SHPHOS, 2021)

ㅇ 기존 관제장비의 기술적 한계

- 보안관제센터에 사용되는 보안장비의 기술적 한계

※ 네트워크 통신의 송/수신 단위인 TCP/IP 패킷(Packet)은 크게 헤더(Header)와 페이로드(Payload)로 구분되며, 헤더는 네트워크 연결 정보(송신자 정보, 수신자 정보, 페이로드 크기 등)를 포함하며 암호화의 주된 대상이 아님

※ TCP/IP 페이로드는 실제 송/수신 되는 중요한 데이터이며 SSL/TLS 기술은 주로 페이로드를 암호화하는데 암호화된 페이로드를 그대로 분석하는 것은 불가

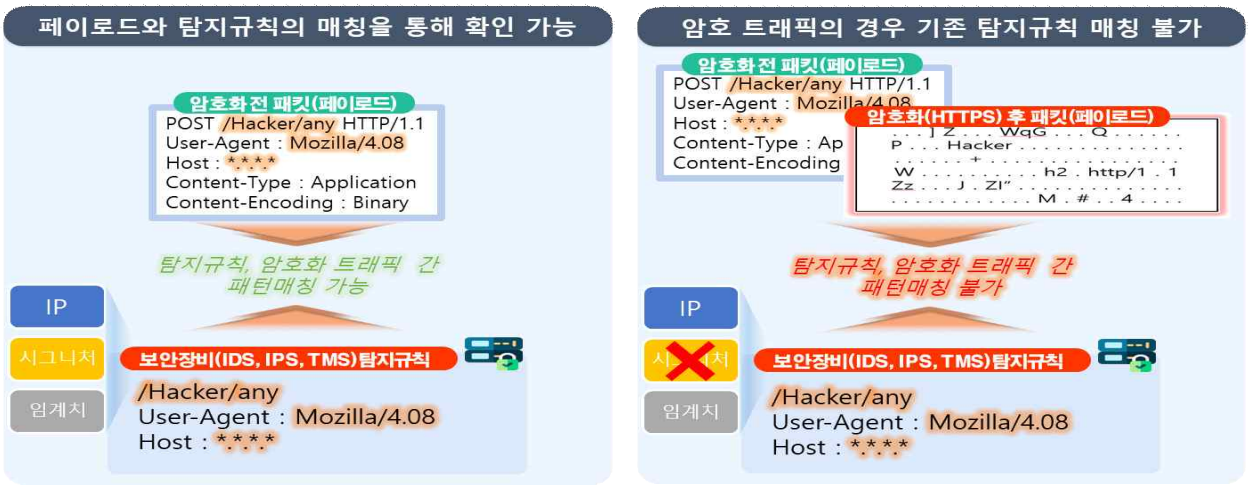
※ Cisco에 따르면 기업의 60%가 HTTPS를 통해 암호화된 트래픽에 대한 탐지가 복호화의 어려움으로 불가능할 것을 예상

- 국내 공공 보안관제센터에서 활용되는 보안장비의 기능 미흡

※ 공공 보안관제센터에서는 국내 기업의 보안장비(TMS, IDS, IPS)를 활용하여 네트워크 관제 업무를 수행 중이며, 주로 IP, 임계치, 페이로드(payload) 내용 매칭의 3가지 방법을 통해 사이버공격을 탐지

※ 이 중 IP와 임계치는 가변적인 데이터이므로 매칭되어도 위협에 대한 신뢰도가 낮을 수 있으며, 암호화 트래픽의 경우 페이로드(payload)에 대한 매칭은 불가

※ 암호화 트래픽 분석 기능이 미흡한 장비를 활용할 경우 관제 사각지대 발생 가능성이 높음



<그림 30> 보안장비의 평문 트래픽에 대한 탐지 가능(좌), 보안장비의 암호화 트래픽 패턴 매칭 불가(우)

ㅇ 암호화 통신 분석을 위한 기술개발 추진 유형

- **(국내)** 국내외 보안업계를 중심으로 암호화 트래픽 및 암호화된 악성행위 대응 기술을 개발 중이나 네트워크 트래픽 병목현상 및 네트워크 성능 저하가 유발되어 초연결 통신 기반 서비스의 원활한 제공이 불가능

※ 암호화된 트래픽을 복호화하는 과정에서 개인정보 침해 유발 가능성 존재

- **(국외)** 복호화 없이 암호화된 트래픽에 내재된 보안 위협 탐지를 시도하는 연구(ETA)가 진행 중

※ 암호화 트래픽 복호화로 인해 발생하는 네트워크 성능 저하 및 프라이버시(privacy) 문제 회피 가능하지만 현재 초기연구단계 수준이며, 다양한 트래픽이 혼재된 실환경에 대한 적용은 어려움

- 사이버공격 대응을 위한 암호화 수준·범위 강화 진행 중

※ 평문 · 암호문을 비롯한 네트워크 트래픽 · 디바이스에 대한 공격 수준이 향상됨에 따라 보편적인 암호화 기술인 SSL(Secure Socket Layer), TLS(Transport Layer Security)의 기존 버전(TLS 1.2이하)은 중간자 공격(Man In The Middle)과 같은 취약점 발견

※ 따라서 암호화 네트워크 통신 전반에 걸쳐 평문의 노출을 최대한 억제하는 TLS 1.3버전 등으로의 암호화 수준 · 범위 강화 및 사용 권장이 진행 중

※ 특히 IoT 장비의 경우 저전력/소형화를 이유로 보안 기능을 축소하여 취약점 증가 가능성이 높으므로, 통신 과정 전반에 걸쳐 암호화가 요구됨과 동시에 최신 버전의 암호화 기술(cipher suite)이 사용되도록 권장 중

제3절 국내외 대응 정책·기술·산업 동향

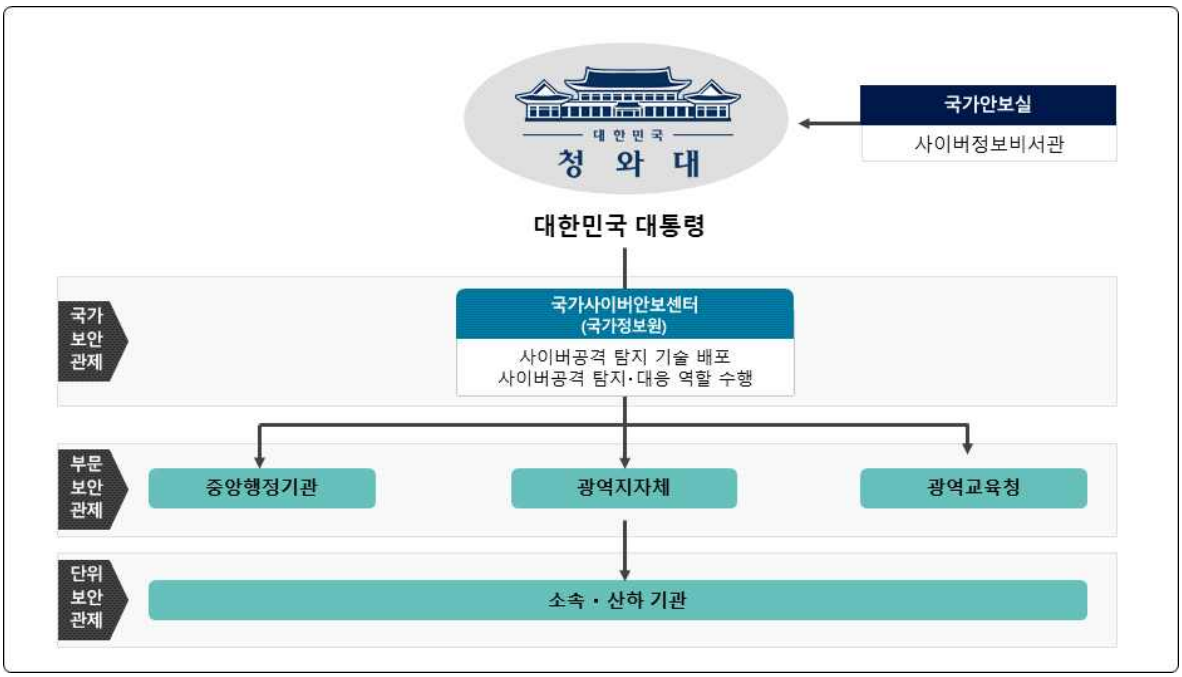
❑ 현재 보안관제 체계 (평문기반 네트워크보안 체계)

○ **(국내)** 국내 보안관제는 「국가사이버안전관리규정」, 「국가 정보보안 기본지침」에 의거하여 보안관제를 수행

- 국가·공공기관의 보안관제는 「국가사이버안전관리규정」에 의거하여 중앙행정기관, 지방자치단체 및 공공기관의 장은 보안관제센터를 설치·운영해야 한다고 명시

- 국가·공공기관의 보안관제는 단위보안관제(각급기관) → 부문보안관제(중앙행정기관) → 국가보안관제(국가사이버안보센터)로 구성된 3단계 사이버공격 탐지·차단 체계로 구성

- 보안관제센터의 설치·운영에 관한 법적 근거는 대통령훈령 제316호 「국가사이버안전관리규정」제10조의 2로, 각 부문보안관제센터는 사이버안전센터 운영규정 또는 운영지침을 제정하여 보안관제센터를 운영 중



<그림 31> 국가 보안관제 체계

- 민간에서의 보안관제는 과학기술정보통신부 산하 한국인터넷진흥원(KISA)의 인터넷침해대응센터(KrCERT)를 통해 수행

- 국내 보안관제는 위협관리시스템(TMS), 침입탐지시스템(IDS), 침입방지시스템(IPS:Intrusion Prevention System) 등의 핵심 보안관제시스템 활용 중심의 네트워크 기반 보안관제 체계

○ **(미국)** 2001년 9·11 테러를 기점으로 사이버관련 법제도를 마련하기 시작해 「국토안보법」, 「국가사이버안보보호법」, 「연방 사이버안보 강화법안」 등 50개가 넘는 법에 사이버안보 조항을 넣거나 법을 공표하고 국방부(DOD), 국가안보국(NSA), 국토안보부(DHS) 등의 기관에서 사이버안보를 담당

- 미국의 국토안보부(DHS)내 사이버보안 및 기반보호를 위한 전문기관(CISA) 산하 미국 사이버침해사고 대응팀(US-CERT)에서 유해트래픽 감시시스템(Einstein)을 사용하여 보안관제를 수행

※ 유해트래픽 감시시스템(Einstein)은 네트워크 기반의 침입탐지 시스템으로 알려진 시그니처를 기반으로 탐지하며 현재 Einstein 3 Accelerated를 사용

○ **(영국)** 1998년에 제정된 「정보보호법」에 의거하여 정보보호 관련 사항을 규제해왔으며, 공공 및 민간 부문에서 사이버공격이 증가함에 따라 2011년 新「사이버 보안전략」을 수립 발표

- 영국은 정부통신본부(GCHQ) 산하 사이버안보운영센터(CSOC)를 두고 외부 사이버 공격, 사이버 범죄 및 테러로부터 각 부처와 민간기업을 보호하기 위한 보안관제를 수행

○ **(일본)** 2014년 「사이버보안기본법」을 제정하고 사이버안보 정책을 담당하는 컨트롤 타워로 사이버보안 전략본부가 내각관방에 설치

- 사이버보안 전략본부 산하 내각사이버보안센터(NISC)는 기존 내각관방 정보보안센터를 개편하여 해킹・웜 바이러스 등 사이버위협징후에 대한 보안관제를 수행

○ **(중국)** 2015년 「국가보안법」을 제정하고 「사이버보안법」, 「중국비밀보호법」, 「암호법」을 제정하여 사이버보안 규정

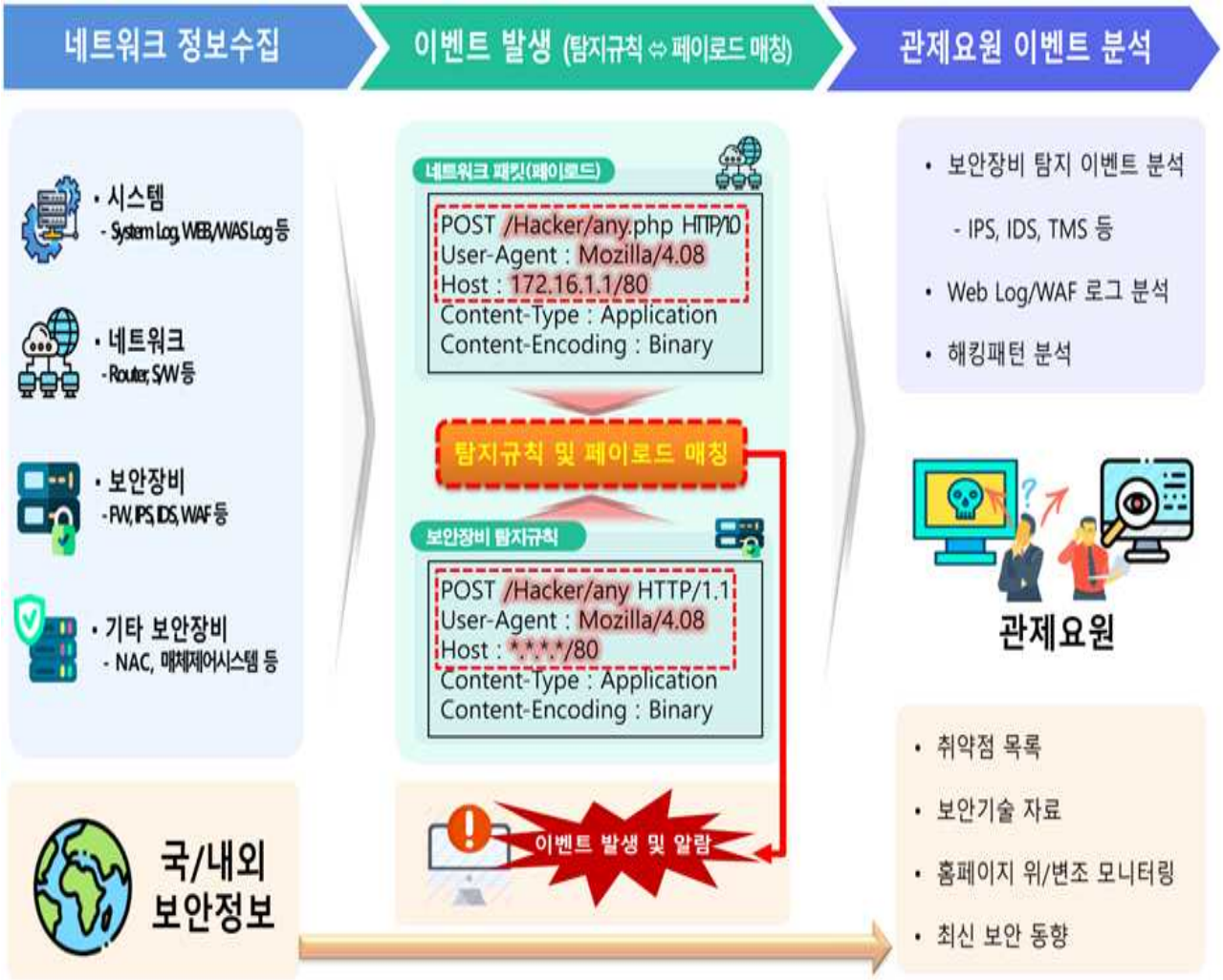
- 「사이버보안법」과 「중국비밀보호법」 제정하여 네트워크 위험도에 따라 보안등급을 구분하고, 3등급 이상의 특수의무의 경우 네트워크 운영관리를 위한 상시적 안전관리와 모니터링 의무가 추가 부여

- 「암호법」은 상용암호 관련 표준화 추진, 인증제도 설립 및 산업계 보급, 네트워크 핵심설비 및 안전 전용제품에 대한 상용암호 강제 인증, 특정범위 상용암호에 대한 수출입 관리를 규정

- 핵심 정보 기반시설 운영자는 상용암호를 사용하여 인프라를 보호하고 상용암호 응용 안전성 평가를 실시

○ **(평문기반 보안관제)** 국내외 보안관제 체계는 네트워크 기반의 보안관제 체계로 수행되고 있으며, 네트워크상의 문자열을 식별할 수 있는 시그니쳐 기반의 탐지시스템을 활용한 방법이 주를 이룸

- TMS, IDS, IPS 등 탐지 시스템은 시그니쳐(패턴) 기반의 탐지 장치로 現 네트워크 기반의 보안관제 체계에서 네트워크 상 평문이 아니면 탐지가 어려우며, 국가적으로 암호화 트래픽 대응 정책이 미비한 실정



<그림 32> 평문기반 보안관제 체계

❑ 암호화 트래픽 활용에 관한 국내외 법, 제도, 표준화 등

○ **(국내)** 정부는 「사물인터넷(IoT) 정보보호 로드맵 3개년 계획」, 세계 최고 디지털 안심국가 실현을 위한 「K-사이버방역 추진전략」, 디지털 경제로의 대전환을 위한 「21년 디지털 뉴딜 실행계획」 등 다양한 정책을 발표하고, 성공적인 정책추진을 위한 네트워크(인터넷, IoT 등) 보안 요구사항을 정립

- 국내에서는 각종 표준화 및 지침, 가이드를 통해 네트워크 통신 간의 암호화 및 보안조치를 명시

- 2020년 12월 행정안전부는 「HTTPS-ONLY」정책 도입을 검토하였으며, 각 정부부처, 지자체 등 모든 사이트에 대해 HTTPS로 전환 계획을 갖고 있음

[표 4] 국내 표준화 및 지침, 가이드 현황

구분	명칭
표준화	스마트그리드 표준화 보안 가이드라인(TTA, 2014)
	산업제어시스템 보안 요구사항(TTA, 2017)
	대규모 사물인터넷 환경에서 기기 종류에 따른 접근제어 절차(TTA, 2017)
	LTE-R 기반 스마트 철도 플랫폼(기술보고서)(TTA, 2019)
	해상무선통신망 LTE-M, 송수신기 상호운용성 시험 규격(TTA, 2020)
	차량 · 사물(V2X) 통신 보안 지침(TTA, 2020)
지침 및 가이드	IoT 공통보안 가이드(KISA, 2016)
	사물인터넷(IoT) 환경에서의 암호 · 인증기술 이용 안내서(미래창조과학부, 2017)
	정부사물인터넷 도입 가이드라인(행정안전부, 2019)
	스마트교통 사이버보안 가이드(KISA, 2019)
	산업제어시스템 보안(국가기술표준원, 2020)
	자동차 사이버보안 가이드라인(국토교통부, 2020)

- 홈·가전, 의료, 교통, 환경·재난, 제조, 건설, 에너지 등 7대 IoT 분야의 보안성 확보를 위한 「암호화 통신 기반 공통 보안원칙 도출」

- 5G, 인공지능 등 4차 산업혁명, 비대면 경제 활성화에 따라 증가하는 사이버보안 위협으로부터 국민이 안전하고 신뢰할 수 있는 세계 최고의 '디지털안심국가'를 실현하기 위한 정보보호 종합 계획 수립

[표 5] 네트워크 보안 요구사항

구분	명칭
인터넷망	홈페이지 등 안전성 확보를 위해 HTTPS, VPN(암호화) 적용 (과학기술정보통신부 지시사항, ‘18.7.)
IoT망	원격제어 기능이 탑재된 스마트 홈 · 가전 등의 디바이스는 외부 비인가접근을 방지하기 위한 사용자 인증 및 암호화 통신 기능 적용 ※ 적용분야 : 스마트 City, 스마트교통, 스마트선박 등 암호화 통신 필수

○ **(미국)** 미국 정부는 IoT 기기 수가 기하급수적으로 증가하면서 늘어나는 사이버위협을 방지하고 IoT 기기 보안을 강화하기 위한 조치로 「사물인터넷(IoT) 사이버보안 개선법」을 제정하였으며, 기기 제조업체는 새로운 보안 표준을 충족해야 함

- 특히, 미국 캘리포니아에서는 「사물인터넷 보안법(SB327)」은 2020년 1월부터 발효돼 향후 인터넷 연결이 가능한 모든 기기는 보안 기능을 필수로 탑재해야 하며, 해당 법은 커넥티드 디바이스 생산 기업이 해당 기기에 합당한 보안 기능을 반드시 탑재하도록 규제

- 미국 하원에서 초당적 법안인 2019 IoT 사이버보안 개선법을 발의하였으며, IoT 기기의 사이버보안에 대한 미국 국립표준기술연구소(NIST)의 조치 강화 노력을 반영해, IoT 사이버보안 기능 구현을 위한 최저 요건을 중요하게 다룸

○ **(일본)** 일본 총무성은 2017년 1월 사이버보안 TF를 구성하고 봇넷 대응 등 IoT보안 정책을 체계적으로 추진하기 위해 「IoT 종합보안대책」을 수립하였고, 5G 상용화에 따른 신규 위협 발생, AI 활용 등 급변하는 ICT 환경에 대응하기 위해 「IoT·5G 보안 종합대책」을 발표 및 추진

- 최근 총무성, 경제산업성 등 다부처 협력을 통해 「사이버 물리 보안 대책 프레임워크」를 발표함으로써 IoT시스템, 서비스, 네트워크, 단말에 이르기까지 사이버보안 대책 수립을 추진하고 있으며, 특히, CCDS, EDSA 보안인증 도입을 통해 데이터 통신 간에 암호화 수행 및 검증을 의무화하고 있음

○ **(영국)** 2018년 3월 영국 국가사이버보안센터(NCSC)는 사물인터넷(IoT), IP 카메라 등 인터넷이 연결된 제품을 대상으로 한 가이드라인을 발표했으며, 제품 출시할 시 기본 암호를 고유하게 설정하도록 하는 등 보안조치 강화의 내용이 담김

○ **(유럽)** EU의 개인정보보호법(GDPR)은 2016년 5월 개정됐으며, 개정 내용 중 개인정보보호의 책임주체는 해당 기업으로, 해당 기업은 해킹 및 악성코드 삽입 등에 대한 사이버 범죄 방어 및 암호화 방안 수립 등 자체 정보보호 시스템을 구축하고 개인정보보호책임자를 두도록 명시

○ **(인도)** 2017년 전기정보기술부(MeiTY)가 IT Act 2000의 선지급 결제방식에 대한 규정안을 발표하였으며, 전자 선지급 결제방식(e-PPI)의 내용 중 종단간 암호화에 대한 요건과 규정을 제시함

○ **(중국)** 중국 산업 정보 통신부(MIIT)는 2021년 공용 네트워크 보안 위험 방지를 위해 「IoT 기본 보안 표준 시스템 구축을 위한 지침」을 발표하였으며, 접근 인증 테스트 및 데이터 보안 테스트를 포함하여 IoT와 관련된 각 보안 조치 테스트 및 평가하는 방법의 내용이 담김

❑ 네트워크 보안관제 기술연구 동향

○ **(국내)** 인공지능을 활용한 악성 네트워크 트래픽 탐지기술연구

- IP 주소, 포트 번호, 사용 프로토콜 등 기본적인 네트워크 정보를 학습을 위한 특징정보로 사용하여 악성 트래픽 탐지 인공지능 모델 생성

- 페이로드 길이, HTTP 상태코드 등 추가적인 정보를 학습하여 탐지 모델 성능 향상

※ 기계학습 기반 IDS 보안이벤트 분류 모델의 정확도 및 신속도 향상을 위한 실용적 feature 추출 연구(KISTI, '18.4)

- 군집화, 차원 축소 등 비지도학습 기법을 통해 정상 트래픽의 특징을 학습하여 네트워크 이상징후 탐지

※ 오픈소스 기반 Deep Learning 기술을 활용한 보안관제시스템의 Anomaly Detect Model 연구 (강용석, 신용태, '17.9)

○ **(국내)** 보안관제 데이터에 자연어처리 기술적용을 통한 침입탐지 이벤트 유효성 검증기법 연구

- 페이로드에 포함된 단어·문장에 자연어처리 기술을 적용

- 자연어처리 기술을 통해 추출된 단어·문장별 가중치를 활용하여 이벤트 로그 내 정상·악성 키워드의 비율을 계산함으로써 침입탐지 이벤트 유효성 검증

※ TF-IDF를 이용한 침입탐지 이벤트 유효성 검증 기법 (전남대학교, '18.12)

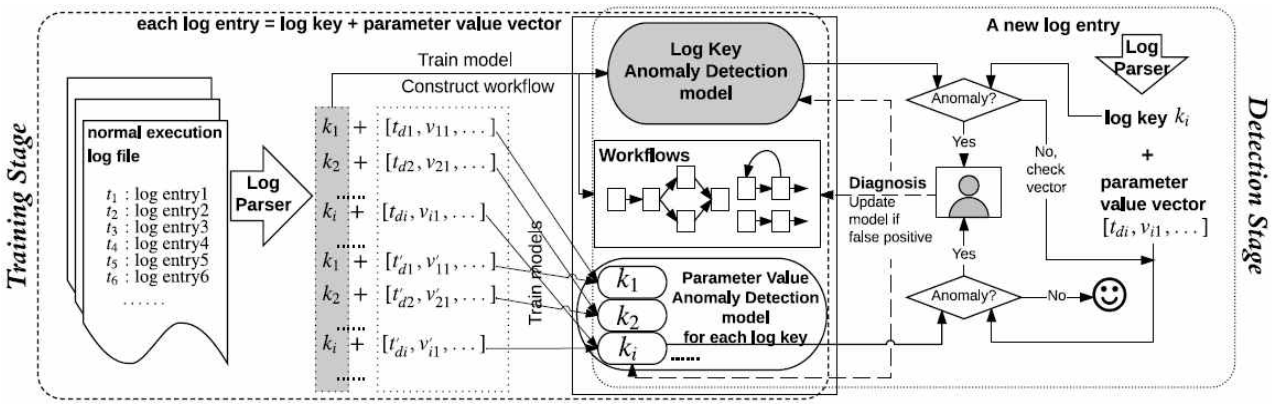
○ **(국외)** 순환신경망(RNN:Recurrent Neural Networks)을 활용한 이벤트 로그 이상징후 탐지기술연구

- N개의 연속된 데이터가 입력되었을 때, (N+1)번째 데이터에 대한 예측이 가능하도록 순환신경망 모델 학습하여 높은 확률을 배정받은 상위 예측 값들이

실제 값을 포함하면 정상으로 간주하며, 그렇지 않으면 이상징후로 판단

- 이벤트 로그를 키(Key) 부분과 인자(Parameter) 부분으로 분리하여 각각에 대한 이상징후 발생여부를 확인함으로써 탐지 효율 높임

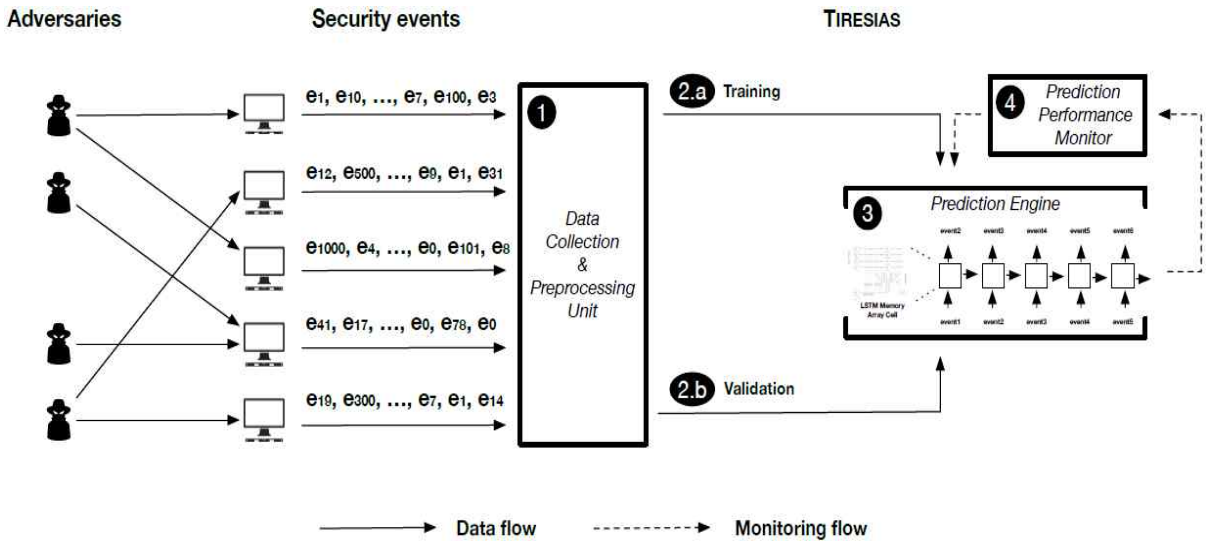
※ DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning (M. Du 외 3명, ACM CCS'17)



<그림 33> DeepLog 기술의 전체 구성도

- 침입방지시스템에서 발생한 이벤트 로그 시퀀스를 학습하여 일정 개수의 이벤트 로그 시퀀스가 주어졌을 때, 다음에 발생할 이벤트에 대한 예측을 수행하며 약 4,000종의 이벤트에 대해 90% 이상의 분류 성능을 보임

※ Tiresias: Predicting Security Events Through Deep Learning (Y. Shen 외 3명, ACM CCS'18)



<그림 34> Tiresias 기술의 전체 구성도

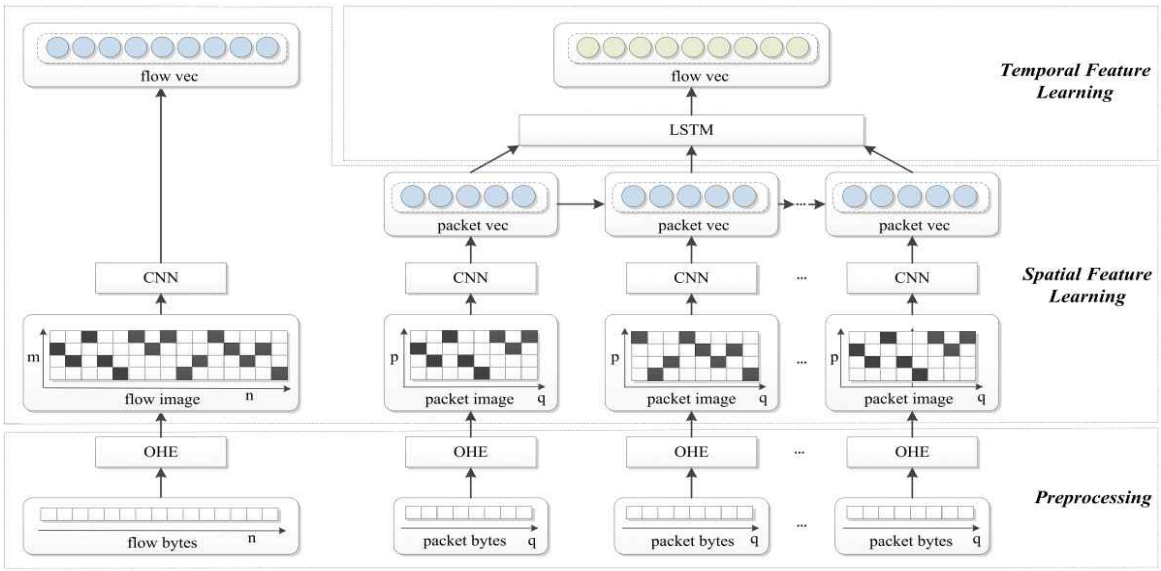
○ **(국외)** 보안관제 데이터에 자연어처리 기술적용을 통한 악성 트래픽 탐지 기술연구

- 네트워크 트래픽과 자연어 간 구조적 유사성을 활용하여 악성 네트워크 플로우 탐지 인공지능 모델 생성

※ 네트워크 트래픽과 자연어의 유사성 – 바이트:패킷:플로우 = 문자:문장:문단

- 합성곱신경망(CNN:Convolutional Neural Networks)과 순환신경망을 통해 각각 네트워크 트래픽의 공간적, 시간적 특징을 학습하여 입력된 네트워크 플로우의 악성여부 판단 및 공격 유형 분류

※ HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection (W. Wang 외 6명, IEEE Access'17)



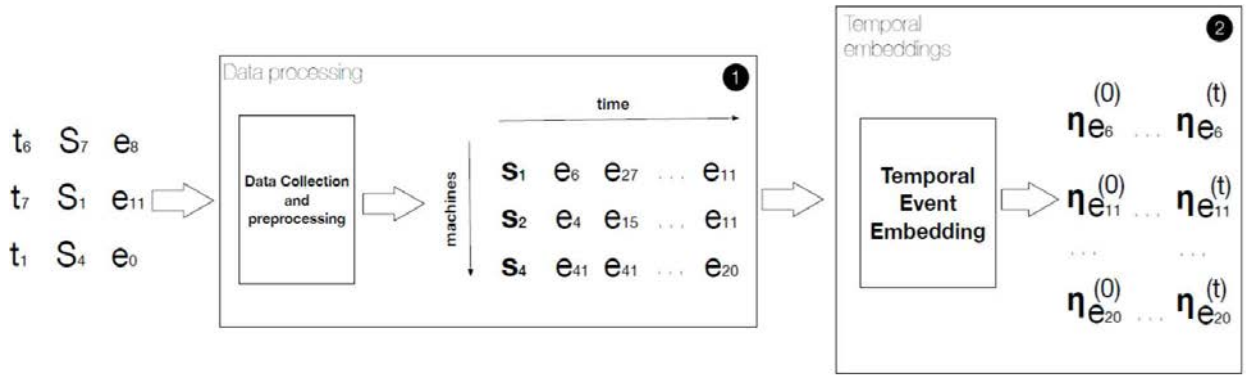
<그림 35> HAST-IDS 기술의 전체 구성도

- 사이버공격에서 다양한 공격기술이 동시에 사용되는 경우가 많으며, 여러 대의 보안장비에서 동시에 동일한 공격 시도가 목격되는 점을 착안하여 자연어처리 분야의 임베딩 기법을 보안관제에 적용

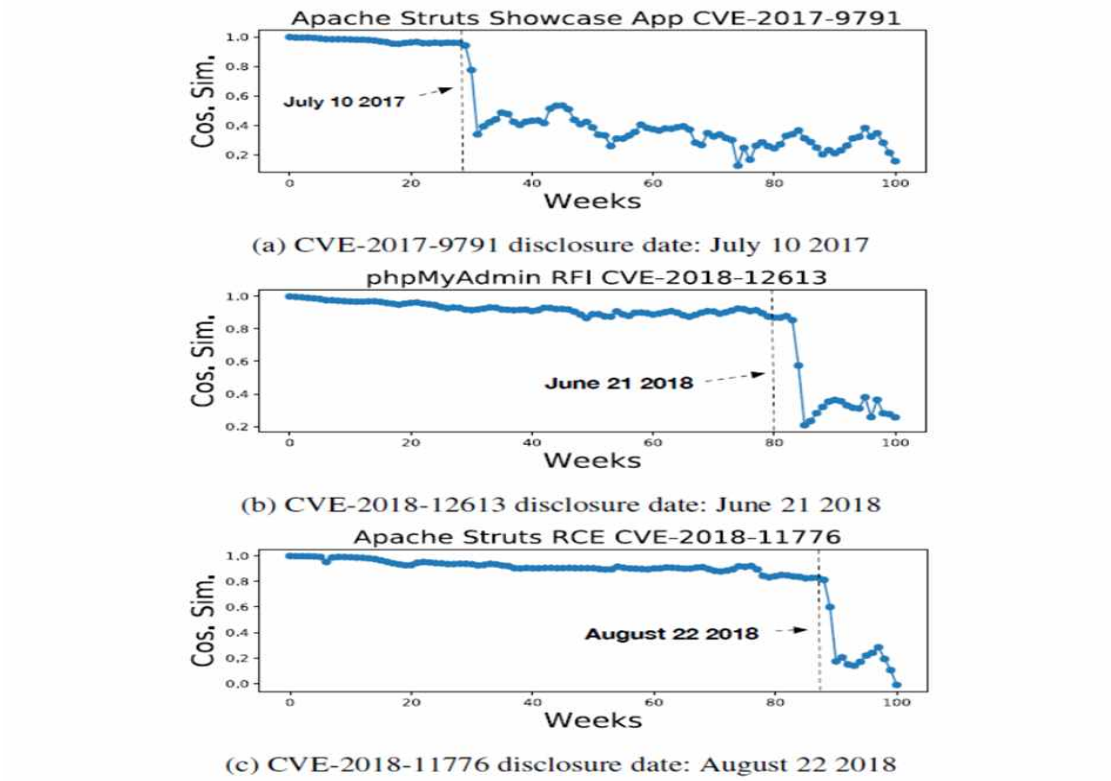
- 침입방지시스템에서 발생하는 이벤트를 하나의 단어로 보고 단어 주변의 컨텍스트 정보를 학습

- 생성된 임베딩 벡터를 통해 벡터 간 유사도 측정이 가능해지며 주기적으로 침입탐지 이벤트를 임베딩하여 이벤트의 변화를 탐지하거나 트렌드 파악하는 것이 가능해짐

※ ATTACK2VEC: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks (Y. Shen, G. Stringhini, USENIX Security'19)



<그림 36> ATTACK2VEC 기술의 전체 구성도



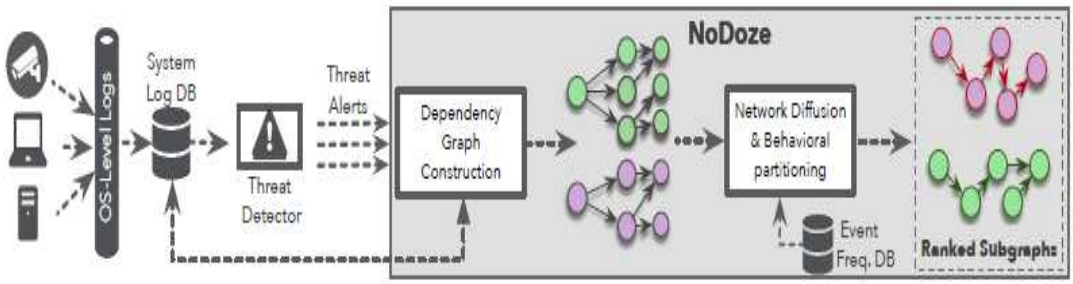
<그림 37> 임베딩 벡터 간 코사인 유사도를 측정하여 이벤트 변화 탐지 예시

ㅇ **(국외)** 그래프 이론을 활용한 보안관제 이상징후 탐지기술연구

- 그래프 이론과 이상징후 스코어링 기술을 사용하여 서버로부터 수집된 로그를 분석하고 높은 이상징후 점수를 갖는 로그 위주로 보안관제 업무를 수행하게 하는 방법이 제안됨

- 인공지능 기반 기술과 달리 그래프 이론을 적용함으로써 원인과 결과에 대한 추론이 가능하다는 장점을 보임

※ NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage (W. Hassan 외 6명, NDSS'19)



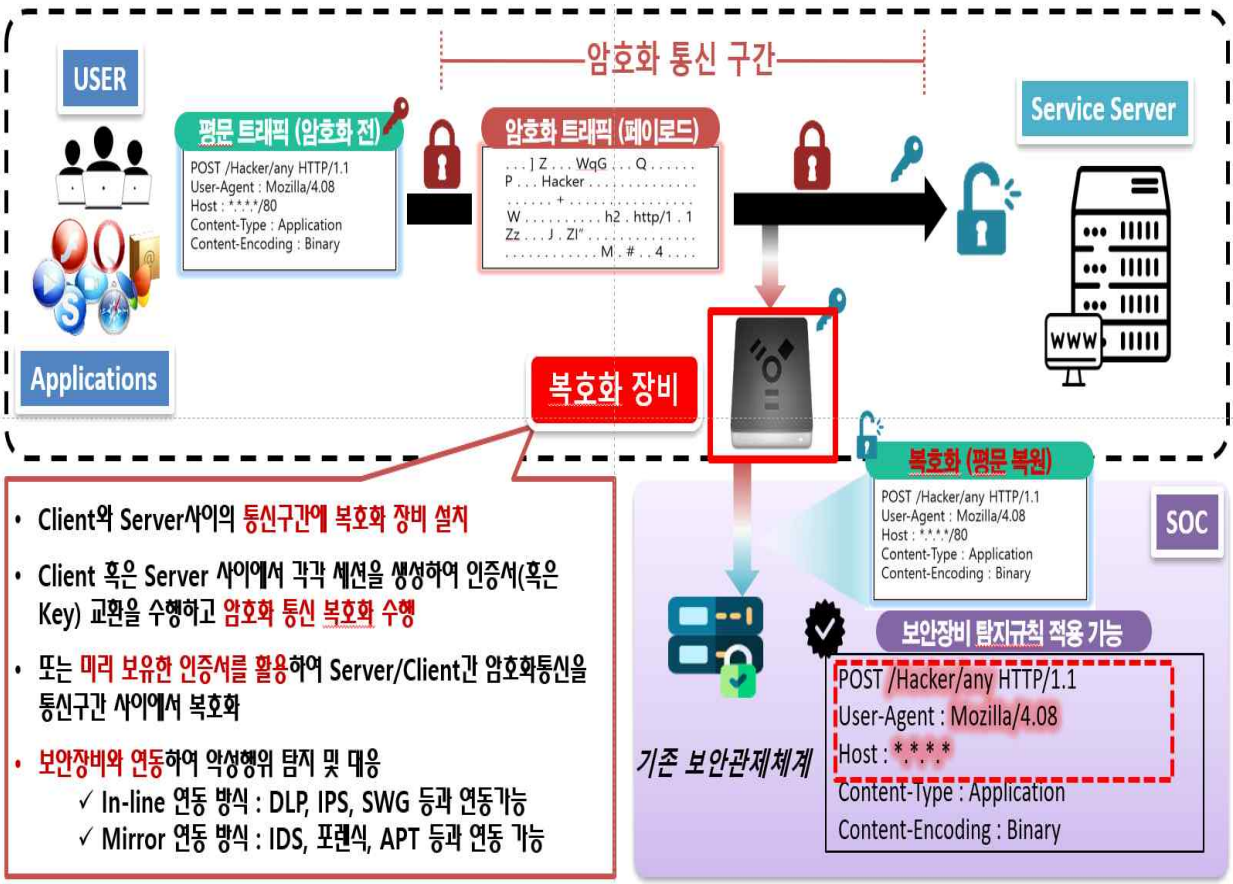
<그림 38> NoDoze 기술의 전체 구성도

❑ 암호화 트래픽 분석 기술연구 동향

○ 기존 네트워크 보안관제 기술연구는 대부분 <u>규칙 기반의 침입탐지 시스템에서 발생한 이벤트 로그를 활용하거나 평문의 페이로드 정보를 활용</u>하여 이상징후를 탐지하는 방법으로 진행되어왔음

- 모든 디바이스가 네트워크로 연결된 초연결 사회·디지털 시대로 진입함에 따라 데이터 보호 및 보안성 강화를 위해 **암호화 통신기반 네트워크 환경으로의 통신 패러다임 전환**됨으로써 **기존에 진행되어온 연구에 사용된 정보를 활용하기 어려워짐**

○ 암호화 트래픽 분석에 기존 보안관제체계 및 네트워크 보안관제 기술연구를 활용하기 위해 암호화 통신 구간에 복호화 장비를 설치하여 암호화 트래픽을 복호화하여 관제 수행



<그림 39> 복호화 기반 암호화 트래픽 분석 단계

- 초고속·대용량 네트워크 환경에서의 통신속도 및 용량 대비 부족한 암·복호화 처리량으로 인해 복호화 시 **네트워크 병목현상 및 통신지연이 발생**하며, **현실적으로 모든 네트워크 환경에 복호화 장비 설치가 불가능**한 한계점이 발생

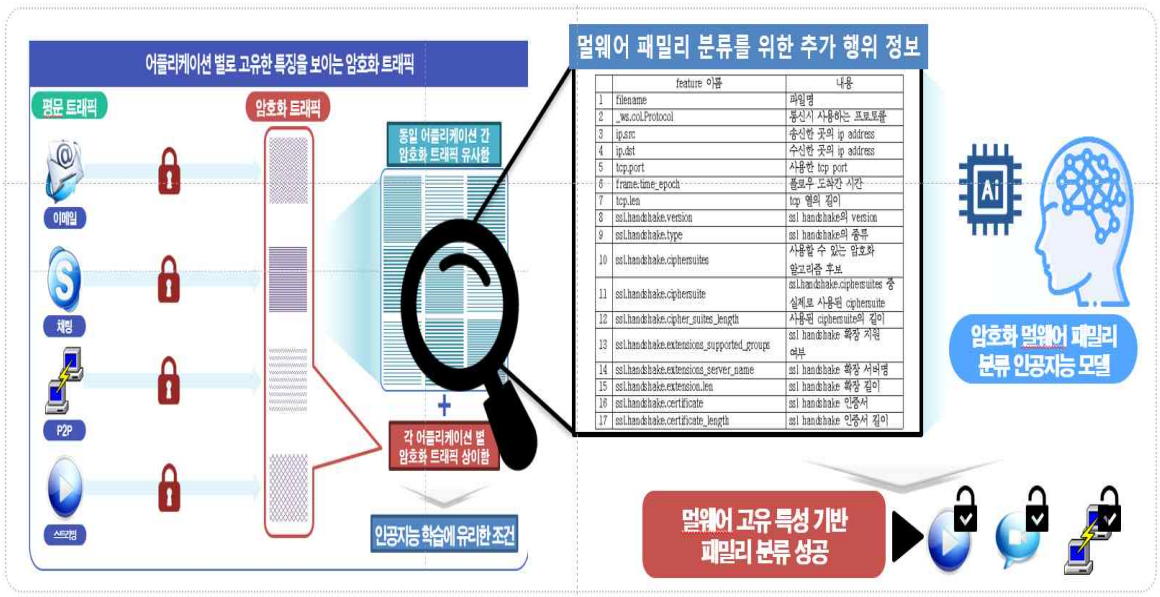
- 다양한 트래픽 암호화 방법으로 인해 모든 애플리케이션 환경의 **암·복호화에 대응이 불가능**하며 **주로 SSL/TLS 기반 트래픽에 대해서만 복호화 및 분석 가능한** 한계점이 발생

- 암호화 트래픽 복호화 구간에서 **개인·민감정보가 유출 또는 노출**이 가능해지며 복호화 트래픽 분석 단계에서 **개인정보 침해에 관한 문제가 발생**할 수 있음

○ 암호화 트래픽 복호화로 인해 발생하는 네트워크 성능 저하 및 프라이버시(privacy) 문제를 회피하기 위해 **복호화 없이 암호화된 트래픽에 내재된 보안 위협 탐지를 시도하는 연구(ETA)**가 진행 중

- **ETA(Encrypted Traffic Analytics)** : 암호화 트래픽을 복호화하지 않고 패킷 길이, 전달 시간, 순서, 최초 데이터 패킷 등의 메타정보를 분석하여 이상징후 탐지

※ 암호통신 기반 사이버공격 탐지를 위한 AI/X-AI 기술연구 동향(KISTI, '19.6)



<그림 40> 멀웨어 고유 특성 기반 패밀리 분류

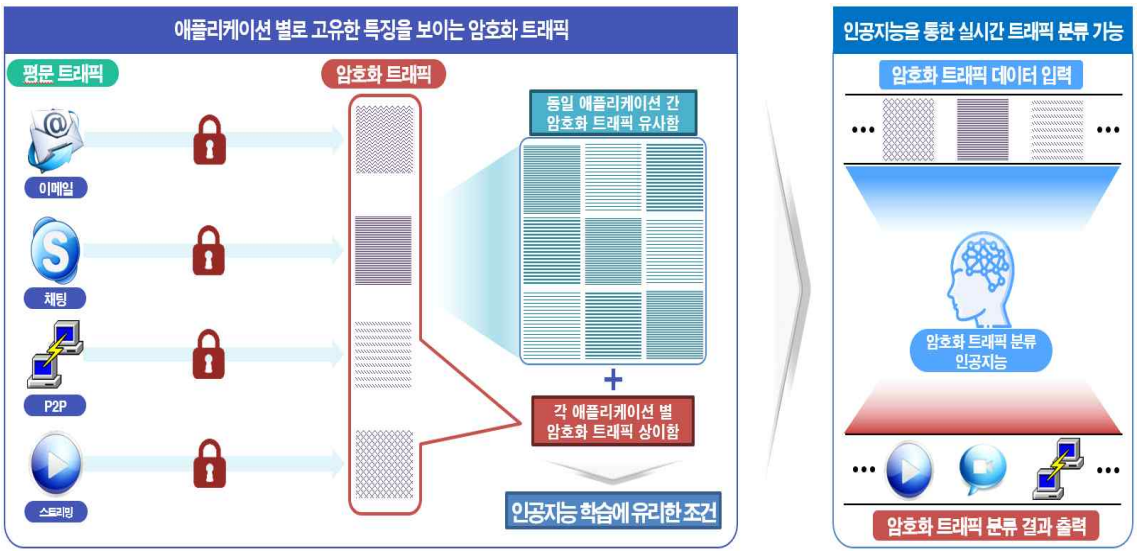
○ **(국내)** 인공지능 기술을 활용한 암호화 트래픽 멀웨어 패밀리 분류 기술연구

- 각 멀웨어 패밀리마다 암호화 트래픽 상에서 고유한 특징을 보이는 점을 활용하여 패밀리별로 암호화 네트워크 통신 간 발생하는 연관 플로우를 수집·분석·가공한 정보를 학습하여 멀웨어 패밀리 분류 인공지능 모델 생성

※ 마르코프 체인 모델 기반 암호화된 악성 트래픽의 패밀리별 분류(고려대학교, `20.8)

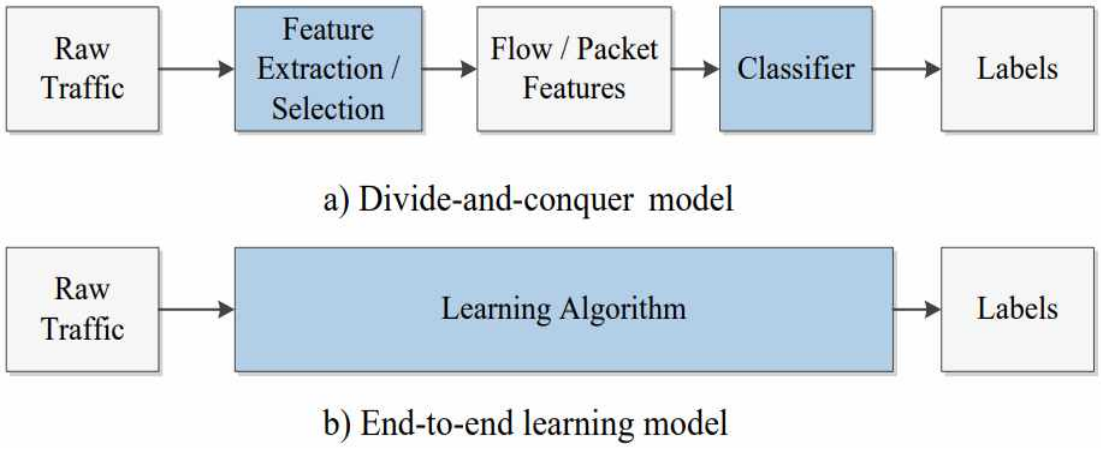
○ **(국외)** 인공지능 기술을 활용한 암호화 트래픽 특징 자동학습 기술연구

- 암호화된 네트워크 트래픽 양상이 애플리케이션 유형별로 고유한 특징을 보이며 동일 애플리케이션 유형에서 발생하는 암호화 트래픽 간 양상의 유사한 부분을 활용하여 원본 트래픽을 합성곱신경망, 순환신경망 등의 인공지능 모델에 입력으로 사용함으로써 애플리케이션별 암호화 트래픽 특징이 자동으로 학습되도록 유도



<그림 41> 애플리케이션별로 고유한 특징을 보이는 암호화 트래픽

- 원본 데이터를 별도의 특징정보 분석을 통한 추출·가공과정 없이 인공지능 모델의 입력으로 사용하는 종단간 학습(End-to-End Learning) 방법을 사용함으로써 모델 생성에 소요되는 인적·시간적 자원에 대한 절약이 가능해지며 모든 애플리케이션 유형에 대응 가능해짐



<그림 42> 기존 인공지능 모델 생성 과정(a), 종단간 학습 모델 생성 과정(b)

※ End-to-end encrypted traffic classification with one-dimensional convolution neural networks" (W. Wang 외 4명, IEEE ISI'17)

※ Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework (Y. Zeng 외 3명, IEEE Access'19)

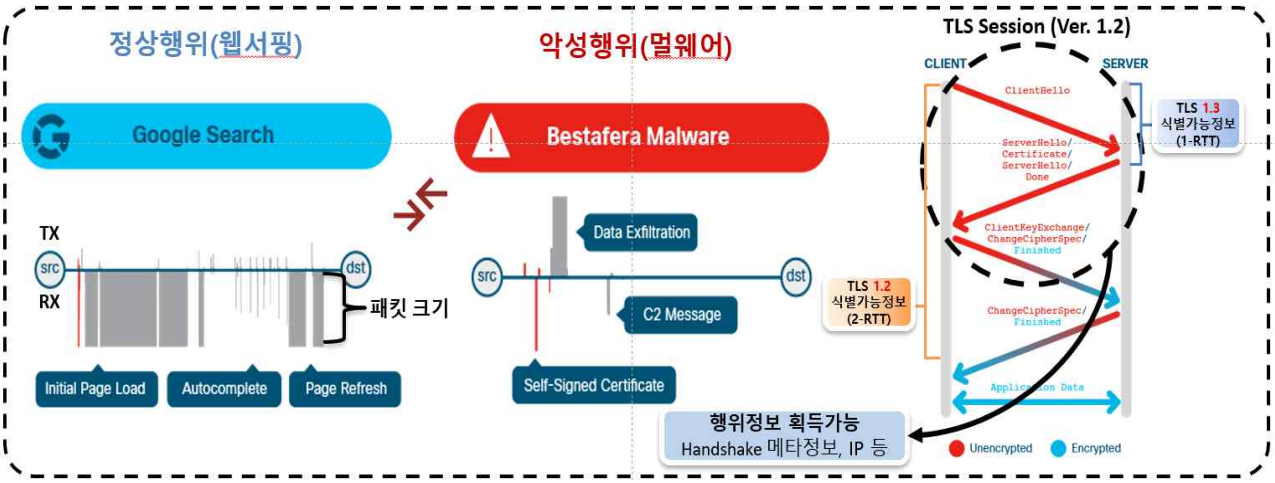
※ Malware Traffic Classification Using Convolutional Neural Network for Representation Learning (W. Wang 외 3명, ICOIN'17)

○ **(국외)** 네트워크 행위기반 암호화 트래픽 분석 기술연구

- 정상·악성 애플리케이션 간 네트워크 행위 차이를 활용하여 악성 암호화 트래픽 분석·분류 시도

- 네트워크 트래픽이 암호화되기 전 TLS Handshake 단계에서 얻을 수 있는 Handshake 메타정보, IP 정보 등과 패킷 길이, 패킷 순서, 전송 주기, 헤더 구성 등 암호화되지 않은 정보와 바이트 분포 등을 활용하여 암호화 트래픽 분류 인공지능 모델 생성

※ Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity (Cisco, KDD'17)



<그림 43> 정상 · 악성 트래픽 간 네트워크 행위 차이

ㅇ 암호화 트래픽 악성행위 분석·대응 상용화 개발 동향

- 국내외 보안 업계(장비벤더, 제조사 등)를 중심으로 암호화 트래픽 및 암호화된 악성행위 분석의 중요성을 인식하고 이에 대한 대응기술과 전용장비 개발에 착수

[표 6] 암호화 트래픽 악성행위 분석 · 대응 제품 동향

국가	기업명	암호화 트래픽 악성행위 분석·대응 제품 동향
대한민국	수산INT	암호화 트래픽 복호화 장비(ePrism SSL) 개발 및 보급 추진
미국	Symantec	암호화 트래픽 가시화 장비(Visibility appliance) 개발
미국	CISCO	전용장비(Catalyst 9000 series) 개발을 통한 암호화 트래픽 대응기술 개발
미국	Juniper	전용장비(SRX series) 개발을 통한 메타데이터 분석기술 개발

- (복호화 기반) 하지만, 암호화 트래픽은 통신내용 확인 및 분석이 원천적 불가능하기에 평문으로 변환 후 악성행위 분석을 수행해야 하며, 이를 위해 복호화 장비 개발이 필수적으로 요구됨

※ 암호화 통신 구간 상에 복호화 장비를 설치하여 모든 암호화 통신을 복호화하고, 이를 기존 보안장비와 연계·분석함으로써 악성 암호화 트래픽 탐지 및 차단

※ 그러나, 이러한 방법은 복호화 트래픽 검사 등에 소요되는 시간으로 인해 트래픽 병목현상 및 네트워크 전반의 성능 저하가 유발됨으로써 초연결 통신 기반 서비스의 원활한 제공이 불가능

※ 또한, 암호화된 트래픽을 복호화하여 분석 시 개인정보 침해에 관한 문제를 유발할 수 있음

- (ETA 기반) 암호화 트래픽 복호화로 인해 발생하는 네트워크 성능 저하 및 프라이버시(privacy) 문제를 회피하기 위해 복호화 없이 암호화된 트래픽에 내재된 보안 위협 탐지를 시도하는 연구가 진행 중

- 암호화 트래픽 분석 기술에 대한 관심 및 중요성이 대두됨에 따라 국내 學·硏계에서도 연구 필요성을 인식하여 최근 ETA관련 연구를 다음 [표 7]와 같이 추진하기 시작함

[표 7] 국내외 ETA 기술 연구 현황

국가	기관명	ETA관련 연구
대한민국	한국과학기술정보연구원	암호통신 기반 사이버공격 탐지를 위한 AI/X-AI 기술연구 동향('19.6)
대한민국	고려대학교	마르코프 체인 모델 기반 암호화된 악성 트래픽의 패밀리별 분류('20.8)

- 현재까지 수행된 ETA 기술은 초기 연구 단계이기 때문에 다양한 유형의 디바이스 및 네트워크가 혼재된 實환경에 적용하기에는 어려운 수준이며, 지속적인 연구개발이 요구되고 있음

❑ 네트워크 보안관제 기술 및 체계 시장 동향

○ 지능화되는 사이버침해위협에 대응하기 위해 국내외 정보보안 기업들은 다음 [표 8]과 같은 제품체계로 보안관제 시장에 접근하고 있음

- 네트워크 트래픽 평문형태의 패턴매칭을 통한 사이버공격 탐지

[표 8] 국내외 잘 알려진 네트워크 정보보안 기업 및 보안제품

국가	기업명	제품유형	제품명
대한민국	시큐레이어	IPS	eyeCloudIPS
		SIEM	eyeCloudSIM
	안랩	IPS	AhnLab AIPS
		TMS	AhnLab TMS
	윈스	IPS	Sniper ONE-i
		TMS	Sniper TMS-plus
	네오리진	IDS	TAS Series
		TMS	TESS TMS
	어울림정보기술	IPS	SECUREWORKS IPSWall
	시큐아이	IPS	SECUI MF1
	이글루시큐리티	SIEM	SPiDER TM
	엑스게이트	TMS	TMS

미국	FORTINET	IPS	FortiGate IPS
	TREND MICRO	IPS	NGIPS
	CISCO	IPS	Secure IPS
	McAfee	IPS	NSP
		SIEM	SIEM
	Exabeam	SIEM	Fusion SIEM
	IBM	SIEM	IBM Security QRadar SIEM
	LogRhythm	SIEM	LogRhythm NG-SIEM
	microsoft	SIEM	Azure Sentinel
	Splunk	SIEM	Enterprise Security
	FireEye	SIEM	FireEye Helix
	Juniper	SIEM	Juniper Secure Analytics

ㅇ 국외 기업(CISCO, Juniper)에서는 네트워크 패킷 메타데이터를 모니터링하여 암호화 트래픽의 악성행위를 감지하는 소프트웨어 플랫폼 개발

- 암호화 통신 네트워크 패킷의 메타데이터를 분석하여 사이버공격 탐지

[표 9] 국외 보안장비 · 솔루션(ETA) 제품 현황

국가	기업명	제품유형	제품명
미국	CISCO	Switch (ETA 기능 포함)	Catalyst 9000 series (9200, 9300, 9400, 9500, 9600, 9800)
	Juniper	F/W, IDS, IPS (ETA 기능 포함)	SRX series

ㅇ 글로벌 정보보안 시장현황

- '20년 전 세계 사이버보안 시장규모 1,522억 1천만 달러(한화 약 171조 1,601억)로 추정

※ 전년도 1,494억 6천만 달러(한화 약 168조 678억 원)에서 1.8% 증가한 수준으로, 코로나19로 인한 전반적인 경기침체로 기업의 사이버보안 소프트웨어 예산이 감소하면서 즉각적으로 시장 성장률에 영향을 미침

- 전 세계 사이버보안 시장에서 PC 부문이 절반(50%)을 차지, 뒤이어 IoT(27.4%), 모바일 네트워크(16.1%) 순으로 확인됨

※ PC 부문의 사이버보안 시장규모는 730억 달러(한화 약 82조 885억 원)로, 전년 대비 5.8% 증가

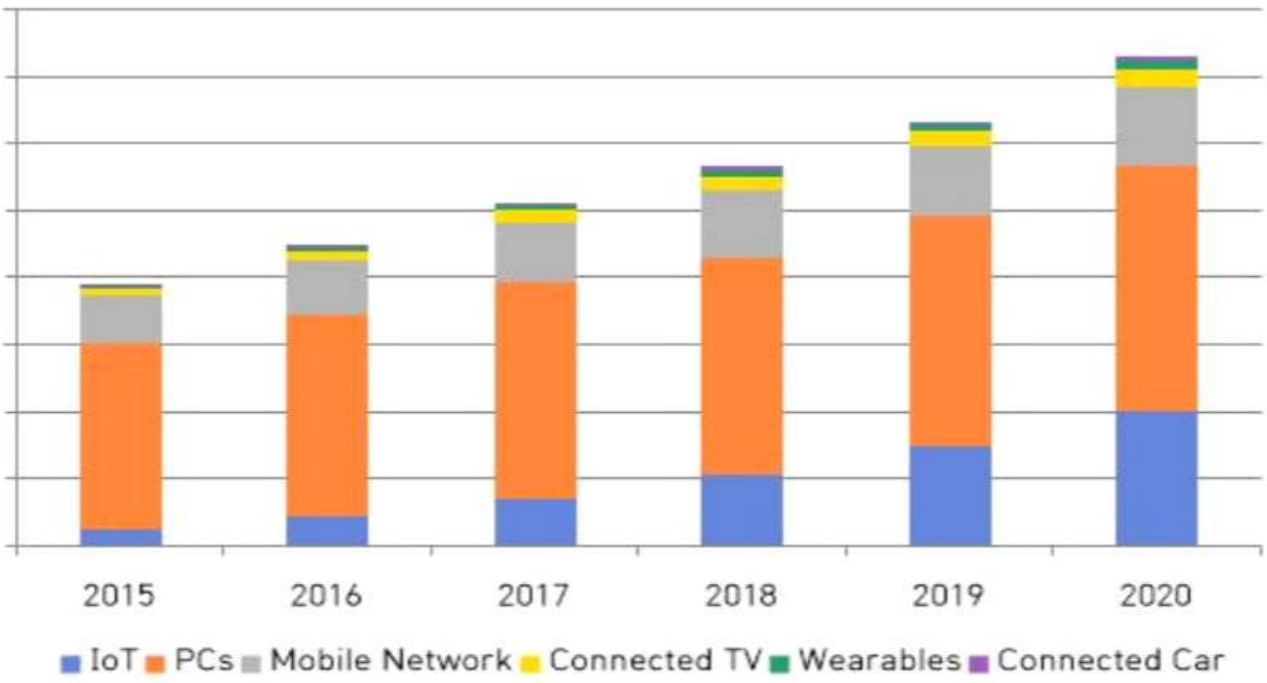
※ IoT 부문의 사이버보안 시장규모는 400억 달러(한화 약 44조 9,800억)로 전년 대비 35.6%, '15년 이후 연평균 54.8%의 높은 성장률을 보임

※ 모바일 네트워크 부문의 시장규모는 전년대비 14.6% 증가한 235억 달러(한화 약 26조 4,258억 원)로 최근 6년간 연평균 10.9% 성장률 기록

[표 10] 세계 부문별 사이버보안 시장규모(추정치) 및 추이 (2015-2020)

(단위 : 십억 달러)

부문	2015	2016	2017	2018	2019	2020	비중	증감률	
								전년비	연평균
IoT	4.5	8.5	14.0	21.0	29.5	40.0	27.4	35.6	54.8
PCs	56.0	60.0	64.5	65.0	69.0	73.0	50.0	5.8	5.4
Mobile Network	14.0	16.5	18.0	20.2	20.5	23.5	16.1	14.6	10.9
Connected TV	2.0	2.5	3.5	4.0	4.5	5.5	3.8	22.2	22.4
Wearable	1.0	1.5	1.5	2.0	2.0	2.5	1.7	25.0	20.1
Connected Car	0.25	0.5	0.5	1.0	1.0	1.5	1.0	50.0	43.1



<그림 44> 세계 부문별 사이버보안 시장규모(추정치) 및 추이(2015-2020)

※ 출처 : 2020년 글로벌 정보보호 산업시장 동향보고서 (KISA)

ㅇ 권역별 사이버보안 시장현황 및 전망

[표 11] 권역별 사이버보안 시장 규모 및 성장률

구분	북미	아시아	유럽	중동	중남미	아프리카
20년도	72조	34조	18조	18조	13조	2조
25년도	130조	78조	50조	32조	23조	4조
성장률 (연)	+8%	+18.3%	+22.6%	+12.2%	+12.3%	+11.1%

- 글로벌 사이버보안 시장은 점차 회복세 통해 '23년까지 연평균 11.0% 성장하고 시장규모 한화 약 234조 2,019억에 이를 것으로 예상

- **북미권역 시장전망** : '25년까지 북미 시장규모는 한화 약 131조 6천억원을 상회할 것으로 전망, '18년 한화 약 72조 5천억 원에서 81.5% 증가한 수준으로, 연평균 성장률은 8%에 달할 것으로 기대

※ North America Cybersecurity Market Revenue to Surpass USD 118 Billion by 2025, The Daily Chronicle(2020.10.01.)

- **유럽권역 시장전망** : 유럽 사이버보안 역시 '25년까지 연평균 22.6%의 높은 성장률 기록할 것을 예상하며 한화 약 50조, 8천억 원에 달할 것으로 예상, '19년 프랑스 사이버보안 관련 지출액은 한화 약 23억 원으로 주요 6개국 중 가장 많은 예산 확보 및 비용 지출

※ EUROPE CYBER SECURITY MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021-2026), Mordor Intelligence(2020)

- **아시아권역 시장전망** : 아시아태평양 지역 사이버보안 시장규모는 '19년 한화 약 33조 9천억 원에서 '25년까지 연평균 18.3% 성장할 것으로 전망

※ Asia-Pacific Cybersecurity Market New Opportunities for Sustained Growth and Expansion 2021-2025, Market Watch(2020.12.18.)

- **중동권역 시장전망** : 중동의 사이버보안 시장규모는 '20년 한화 약 17조 9천억 원에서 연평균 12.2% 성장률로 2025년 한화 약 32조 3백억 원에 달할 전망

※ MIDDLE EAST & AFRICA CYBERSECURITY MARKET – GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026), Mordor Intelligence(2020)

- **중남미권역 시장전망** : 남미지역의 사이버보안 시장규모는 '23년까지 연평균 12.3%로 성장해 한화 약 23조 460억 원에 달할 것으로 예상

※ Latin America Cybersecurity Market 2020 Analysis, Overview, Growth, Demand and Forecast Research Report to 2023, Market Watch(2020.11.24.)

- **아프리카권역 시장전망** : '20년 아프리카의 사이버보안 시장규모는 한화 약 2조 5천억 원으로 '15년 이후 연평균 20.41%의 성장률을 보일 것으로 예측된 바 있으며, 권역 특성상 사이버보안 인프라가 취약해 타지역 대비 보안 솔루션의 공급이 느린 편이지만, 남아프리카의 사이버보안 시장이 '26년까지 연평균 11.1%의 성장률을 기록할 것으로 기대

※ Africa Cyber Security Market by Solution, Markets and Markets(2020)

ㅇ 국가별 사이버보안 시장현황 및 전망

- **(미국)** '19년 사이버보안 시장규모 한화 약 23조 5천억 원으로 전체 GDP의 0.1을 차지, 미국 사이버보안 시장은 전 세계의 최대 시장을 차지(40%), '23년까지 시장규모 연평균 8.2% 성장, 한화 약 31조 9천억 원에 달할 전망, 또한 사이버보안 인프라 강화를 위해 지속적인 투자를 계획하였으며, 2021년 연방정부가 국방부에 요청한 사이버보안 예산은 한화 약 6조 2백억 원으로 전체 사이버 예산의 55.1%를 차지

- **(영국)** '19년 정보보안산업 규모는 한화 약 12조 5천억 원으로 추정되며 전년 대비 46% 증가, 정보보안 서비스 산업 규모 한화 약 4조 2천억 원으로

33.7%를 차지, 정보보안 제품 산업 약 2조 2,600억으로 18.1%를 차지하였음

- **(일본)** ’20년 정보보안 시장규모가 전년 대비 1.3% 감소한 한화 약 7조 450억 원으로 추정되며, 이는 코로나19로 인한 투자환경 변화 및 경제 활동 위축으로 시장규모가 소폭 축소된 것으로 예상, ICT 시장 확대로 사이버위협이 증가 및 고도화됨에 따라 정보보안 시장이 성장될 것으로 전망

- **(중국)** ‘19년 사이버보안 시장규모는 전년 대비 23% 증가한 한화 약 11조 원으로 전 세계 2위 규모로 집계, ’17년부터 ‘22년까지 정보기술보안 분야 지출액은 연평균 25.6%의 성장세로 ’22년 한화 약 15조 4,100억 원 규모로 성장 전망되며 정보기술보안 SW 시장규모는 ‘23년 한화 약 2조 6,000억 원으로 확대될 것으로 전망

❑ 기술 수요 대상 현황

ㅇ 공공기관 및 공공 보안관제센터

- 4차 산업혁명이 진행되면서 ICT를 전 산업 분야에 융합하고 코로나로 인한 경제위기를 극복하기 위해 D(Data). N(Network). A(A.I) 기반의 '디지털 뉴딜' 사업이 추진 중

※ ICT를 전 산업분야에 융합하는 국가 디지털 대전환 프로젝트

※ 자율주행차량(산업통상자원부), 스마트공장(중소벤처기업부), K-에듀 통합플랫폼 구축(교육부), 스마트병원(보건복지부), 국민안전 스마트 인프라(국토부, 해수부, 환경부) 등의 31대 대표과제를 추진

※ 국토교통부는 '스마트 교통' 사업 추진을 위해 차세대지능형교통시스템(C-ITS, Cooperative-Intelligent Transport Systems)의 도입하여 15개의 교통안전 서비스 구현과 통신 인프라를 개발 및 구축

※ 해양수산부는 'e-Nav', '스마트 항만' 등의 사업 추진을 위해 초고속 해상 무선 통신망 LTE-M을 구축하여 LTE-M 기지국 263개소, 운영센터 8개소에 실해역 시험·검증 등을 통한 시범운영 중이며 우리나라 전 연안에 해안으로부터 100km 내외 통신 품질 보장 서비스를 제공

※ 세종특별자치시는 '스마트 City' 사업 추진을 위해 도시 내 모든 사물에 사물인터넷(IoT) 기술을 이용한 교통제어, 무인운송수단 등의 다양한 서비스와 통신 인프라를 개발 및 적용 중

※ 5G·AI·빅데이터를 활용한 디지털 뉴딜 사업에서 네트워크 암호화는 필수적 (C-ITS는 DSRC, WAVE, ITS-G5 등의 암호화 프로토콜 사용 중이며, LTE-M과 IoT 장비는 정부사물인터넷 도입 가이드라인과 같은 정책에 의해 암호화 통신 프로토콜 사용이 필수)

- 정부의 ICT 융합 정책 추진에 따라 증가될 암호화 통신에서 발생하는 사이버공격의 위협 해소 및 대응을 위해 과학기술정보통신부는 관련 기술에 대한 연구 필요

※ 현재 과학기술정보통신부는 산하 및 소속기관에 대한 네트워크 보안관제 서비스를

제공 중이며, 국내 과학기술정책·국가연구개발사업을 총괄하는 컨트롤타워의 역할을 수행 중

※ 데이터 댐 프로젝트, XR 플래그십 프로젝트, 양자암호통신 인프라 구축, ICT 중소기업 보안강화 및 시스템(SW) 안전진단 등 다양한 디지털 뉴딜 사업을 추진 중이며 관련된 사이버보안 기술의 확보 필요

- 국가의 중요행정기관 및 광역지자체와 같은 중요한 시설을 목표로 발생하는 사이버 공격에 대응하기 위해 공공 보안관제센터를 운영 중

※ 공공 보안관제센터는 국가정보원(NCSC)을 중심으로 부문 보안관제센터와 단위 보안관제센터로 운영 중이며, 부문 보안관제센터는 중앙행정기관, 광역지자체 등 주요 부처에 대해 보안관제를 수행

※ 사이버공격에 의한 사고 발생 시 개인은 물론 사회적으로 피해가 발생할 수 있으므로 암호화된 트래픽 분석 기술의 개발 및 적용이 시급

- 2021년 기준 44개의 부문 보안관제센터가 운영 중

[표 12] 국내 부문 보안관제센터 목록

관제체계	세부관제체계	관련부처	관제센터
부문보안관제	중앙행정기관	국무조정실	국조실 사이버안전센터
		공정거래위원회	공정위 사이버안전센터
		고용노동부	고용노동 사이버안전센터
		과학기술정보통신부	과학기술정보통신사이버안전센터
			과학기술사이버안전센터
			KISA(한국인터넷진흥원) 인터넷정보센터
			우정사업본부

관제체계	세부관제체계	관련부처	관제센터
		교육부	교육부 사이버안전센터
		국방부	사이버작전사령부
		국토부	국토교통 사이버안전센터
		기획재정부	재정경제 사이버안전센터
		농림축산식품부	농림축산식품 사이버안전센터
		문화체육관광부	문화체육관광 사이버안전센터 / 문화재청 사이버안전센터
		법무부	법무 사이버안전센터
		보건복지부	보건복지사이버안전센터
		산업통상자원부	산업통상자원 사이버안전센터
		외교부	외교사이버안전센터
			한국제협력단(KOICA) 사이버보안관제센터
		중소벤처기업부	중소벤처기업부 사이버안전센터
		통일부	통일 사이버안전센터
		해양수산부	해양수산 사이버안전센터
		행정안전부	국가정보자원관리원(대전) / 행정안전부 사이버보안관제센터
		환경부	환경부 사이버안전센터
		식품의약품안전처	식약처 사이버안전센터
		행정안전부	국가정보자원관리원(광주) / 감사원 관제센터

관제체계	세부관제체계	관련부처	관제센터
			한국지역정보개발원
		산업통상자원부	한국전력거래소
		경찰청	경찰사이버보안관제센터 (경찰정보보호관제센터)
		관세청	관세청 관제센터
		국세청	국세청 사이버안전센터
		기상청	기상 사이버안전센터
		대검찰청	대검 사이버안전센터
		방위사업청	방위사업청 보안관제센터
		병무청	병무청 사이버안전센터
		산림청	산림청 사이버안전센터
		조달청	조달청 사이버안전센터
		통계청	통계청 사이버보안관제센터
		특허청	특허청 관제센터
		해양경찰청	해양경찰청 사이버보안관제센터
		금융위원회	금융보안원
		소방청	소방청 사이버안전센터
		농촌진흥청	농진청 사이버안전센터
		부처합동	부처합동 사이버안전센터
		공무원연금공단	공무원연금공단 사이버보안관제센터

ㅇ (기타 수혜 대상) 주요기반시설

- 정부는 「정보통신기반보호법」에 따라 국가안보 및 경제사회에 미치는 영향 등을 고려하여 각 부처 소관의 중요시스템을 주요정보통신기반시설로 지정함

※ 국가적 · 사회적으로 중대한 역할을 수행중이기에 해킹, 랜섬웨어 유포 등의 사이버 공격으로 인한 침해가 발생할 경우 국가 안보, 국민의 기본 생활 및 경제에 중대한 영향을 미칠 수 있음

[표 13] 행정안전부 소관 주요정보통신기반시설 지정 현황

(단위: 개)

제어시스템						정보시스템			합계
철도운영	교통신호	상수도	지역난방	U-City	물재생	긴급구조	시 · 도 행정	행안부	102
12	12	16	2	5	3	19	17	16	

[표 14] 연도별 주요정보통신기반시설 지정 현황

(단위 : 개)

부문	2013	2014	2015	2016	2017	2018	2019
공공	135	193	227	243	252	262	265
민간	74	99	127	142	141	149	149
합계	**209**	**292**	**354**	**385**	**393**	**411**	**414**

- 또한 주요정보통신기반시설은 해마다 증가하고 있으며 2019년 기준, 주요정보통신기반시설로 지정된 기관은 국내 총 414개로 2013년에 비해 약 2배 이상 증가

- 게다가 기존 폐쇄적인 환경에서 운용 중이던 국가기반시설의 경우 현재 개방적인 환경으로 변화하고 있으며, 사이버공간으로까지 범위가 확장되고 있어 사이버 위협의 새로운 대상이 될 가능성이 높음

[표 15] 국가기반시설 보호기관 현황(주관기관 9개, 관리기관 103개)

(단위 : 개)

구분	주관기관	관 리 기 관				
		중앙행정기관	특별행정기관	지자체	공공기관	민간사업자
합 계 (112)	9	10	12	16	44	18
에너지 (16)	1				9	6
	산업통상자원부				한국수력원자력(주) 한국남동 · 한국중부 · 한국서부 · 한국남부 · 한국동서발전(주) 한국석유 · 한국가스공사 한국전력거래소	SK에너지 SK인천석유화학 GS칼텍스 현대오일뱅크 S-Oil(주) ㈜대한송유관공사
정보통신 (11)	1	1	1		4	4
	과학기술정보통신부					KT(주) LG U+ SK텔레콤 SK브로드밴드
	–	국가정보자원관리원	우정사업정보센터(우정사업본부)		한국고용정보원(고용노동부) 국민건강보험공단(복지부) 국민연금공단(복지부) 근로복지공단(고용부)	
교통수송 (30)	2	1	11		10	6
	국토교통부	항공교통본부			한국철도공사 한국도로공사	의왕 ICD(주) 신분당선(주),

구분	주관기관	관 리 기 관				
		중앙행정기관	특별행정기관	지자체	공공기관	민간사업자
		(국토교통부)			인천국제공항 한국공항공사 서울 · 부산 · 인천 교통공사 대구 · 광주 · 대전 도시철도공사	서울메트로 9호선(주), 공항철도(주), 서울메트로 9호선운영(주), 경기철도(주)
	해양수산부		부산 · 인천 · 여수 · 마산 · 울산 · 동해 · 군산 · 목포 · 포항 · 평택 · 대산지방해양수산청			
금융 (10)	2				6	2
	기획재정부				한국은행, 한국수출입은행	
	금융위원회				한국산업은행, 금융결제원, 중소기업은행, 한국예탁결제원	코스콤, 한국거래소
보건의료 (14)	1				13	
	보건복지부				국립중앙의료원, 서울의료원 대한적십자사, 서울 · 부산 · 경북 · 충남 · 충북 · 전남 · 전북 · 분당	

구분	주관기관	관 리 기 관				
		중앙행정기관	특별행정기관	지자체	공공기관	민간사업자
					서울대 · 양산부산대 · 경상대학교병원	
원자력(2)	1				1(2)	
	원자력안전위원회				한국수력원자력(주) 한국원자력환경공단	
식용수(20)	0(2)			19	1	
	국토교통부				한국수자원공사	
	환경부			서울 · 부산 · 대구 · 인천 · 광주 · 대전 · 울산 · 안양 · 안산 · 군포 · 김포 · 성남 · 부천 · 춘천 · 여수 · 목포 · 김해 · 창원 · 진주시		
정부중요시설(9)	1	8				
	정부청사관리본부	정부과천 · 대전 · 서울청사 관리소				
	–	국방부,대검찰청, 경찰청, 기상청, 농촌				

구분	주관기관	관 리 기 관				
		중앙행정기관	특별행정기관	지자체	공공기관	민간사업자
		진흥청				

[표 16] 국가기반시설 지정현황 (8개 분야, 113개 기관, 267개 시설)

분 야 별		계	지 정 시 설
에너지 (43) (산업부)	전 력	21	화력(13) : 삼천포 · 영흥 · 보령 · 인천 · 하동 · 신인천 · 부산복합 · 당진 · 울산화력본부, 태안 · 평택 · 서인천발전본부, 삼척그린파워 원자력(4) : 고리 · 한빛 · 월성 · 한울 원자력발전소 수 력(2) : 양양 양수발전소, 팔당 수력발전소 전 기(2) : 한국전력거래소(중앙전력관제센터, 중부지사)
	가 스	4	생산기지(인수, 저장, 기화, 송출)(4) : 평택, 인천, 통영, 삼척
	석 유	18	생산시설(5) : SK에너지 울산, SK인천석유화학 인천, GS칼텍스 여수, S-Oil 온산, 현대오일뱅크 대산 공장 비축시설(9) : 한국석유공사 울산 · 거제 · 여수 · 서산 · 평택 · 구리 · 용인 · 곡성 · 동해지사 수송시설(4) : 대한송유관공사 서울 · 경인 · 대전 · 충청지사
정보통신 (19) (과기부)	통신망	11	통신교환국사(7) : KT 광화문 · 혜화지사, 용인교환국, LGU+ 종합연구소, SKT 분당사옥(NW관리센터), 보라매 · 둔산사옥(교환/전송실) 망관리센터(3) : KT 전국망센터, 상암교환국, SK브로드밴드 동작종합정보센터 해저케이블육양국(1) : KT 송정해저케이블육양국
	전산망	8	전산망(4) : 우정사업정보센터, 국가정보자원관리원, 국가정보통신망, 국가정보자원관리원 광주센터 정보센터(4) : 고용보험전산망, 국민건강보험공단, 국민연금 · 산재보험 정보시스템

분 야 별		계	지 정 시 설
교통수송 (34) (국토부, 해수부)	철 도	1	철도(1) : 한국철도공사(전국 철도시설)
	항 공	9	항공교통센터(1) : 인천 중구 공항(8) : 인천국제, 김포, 김해, 제주, 울산, 양양, 여수, 무안공항
	화 물	1	내륙컨테이너기지(1) : 의왕ICD
	도 로	1	고속국도(1) : 한국도로공사(전국 고속국도 시설)
	지하철	11	지하철(11) : 서울·부산·인천교통공사, 대전·대구·광주도시철도공사, 서울메트로9호선(주), 신분당선, 공항철도, 서울메트로9호선운영(주), 경기철도(주)
	항 만	11	무역항(11) : 부산·인천·광양·마산·울산·동해묵호·군산·목포·포항·평택당진·대산항
금융(8) (기재부, 금융위)	금융	8	한국·한국수출입·산업·중소기업은행 금융결제원, 한국거래소, 코스콤, 한국예탁결제원
보건의료 (31) (복지부)	의료 서비스	12	병원(12) : 국립중앙의료원, 서울의료원, 서울·부산·경북·충남·충북·전남·전북·경상·분당서울대·양산부산대학교병원
	혈 액	19	혈액원(16) : 대한적십자사 혈액관리본부, 서울남부·서울동부·서울서부·부산·대구경북인천·울산·경기·강원·충북·대전세종충남·전북·광주전남·경남·제주 혈액원

분 야 별		계	지 정 시 설
			혈액검사센터(3) : 중앙 · 중부 · 남부 혈액검사센터
원자력 (36) (원안위)	원자력	36 (5)	원자력발전소(4) : 고리 · 한빛 · 월성 · 한울 원자력본부 ※ 4개소 35개 시설(주제어실, 방사능방재시설 등) 방사성폐기물처분시설(1) : 중 · 저준위 방사성폐기물처분시설
식용수 (84) (국토부, 환경부)	댐	34	다목적댐(20) : 소양강 · 충주 · 횡성 · 안동 · 임하 · 합천 · 남강 · 밀양 · 대청 · 용담 · 섬진강 · 주암 · 부안 · 보령 · 장흥 · 군위 · 보현산 · 김천부항 · 성덕 · 영주댐 생공용수댐(14) : 대곡 · 사연 · 대암 · 선암 · 영천 · 안계 · 구천 · 연초 · 광동 · 달방 · 수어 · 운문 · 평림 · 감포
	정수장	50	광역정수장(20) : 반월 · 시흥 · 성남 · 수지 · 와부 · 덕소 · 일산 · 송전 · 청주 · 충주 · 석성 · 보령 · 천안 · 고산 · 화순 · 구미 · 사천 · 고양 · 덕정 · 반송 지방정수장(30) : 서울 암사 · 강북, 부산 화명 · 덕산, 대구 매곡 · 고산, 인천 부평 · 수산, 광주 용연 · 덕남, 대전 송촌 · 월평, 울산 회야 · 천상, 성남 복정, 부천 까치울, 안양 비산 · 포일 · 청계, 안산 안산 · 연성, 군포, 김포 고촌, 춘천 소양, 여수 둔덕, 목포 몽탄, 김해 삼계 · 명동, 창원 칠서, 진주
정부중요 시설(12) (정부청사 관리본부)	정부중 요시설	12	중앙행정기관(12) : 정부서울청사, 정부과천청사, 정부대전청사, 정부세종청사, 국방부, 대검찰청, 경찰청, 농촌진흥청, 기상청, 국가기상위성센터, 국가기상슈퍼컴퓨터센터, 국가태풍센터

ㅇ (기타 수혜 대상) 국내 정보보호 관련 기업

- 국내 보안관제업체의 경우 평문 기반의 네트워크 트래픽 분석 및 사이버 공격에 대한 탐지·대응을 수행하므로 암호화된 트래픽에 대한 적절한 대응책을 마련할 필요가 있음

※ 보안관제 전문기업은 18개 업체가 선정 (한국인터넷진흥원, 2021.6)

[표 17] 보안관제 전문기업 18곳

번호	업체명
1	㈜이글루시큐리티
2	한국통신인터넷기술㈜
3	㈜안랩
4	한전KDN㈜
5	㈜싸이버원
6	㈜에이디티캡스
7	㈜윈스
8	롯데정보통신㈜
9	㈜에이쓰리시큐리티
10	㈜시큐어원
11	㈜ktds
12	삼성에스디에스㈜
13	㈜파이오링크
14	㈜가비아
15	㈜LGCNS
16	㈜시큐아이
17	씨엠티정보통신㈜
18	㈜피디정보통신

- 네트워크보안업체는 비복호화 기반의 암호화 트래픽 분석·대응 기술 개발을 통해 국내 보안관제 체계의 기술력 강화 및 신뢰성 확보가 가능하며, 국내시장 및 해외시장에서의 기술 경쟁력 확보 가능

※ 네트워크 기반 침입탐지(NIDS) 및 침입방지(NIPS) 시스템을 개발·판매 중인 국내업체들은 윈스, 코닉, 안랩 등이 있음

제4절 다부처공동R&D 추진 타당성

❑ 다부처 추진 필요성

○ 각 부처에서 추진하는 ICT 기반 대국민 공공 서비스·인프라에 대한 **암호화된 사이버위협이 급증**하고 **재난화·대형화 형태로 진화**함에 따라 **범국가적 차원에서 대응책 마련이 시급**함

- 정부는 국민에게 양질의 대국민 공공 서비스를 제공하기 위하여 첨단 ICT 기술을 적극적으로 도입·적용(표18 참고)하고 있으며, 특히 보안성 강화를 위해 **암호화 통신을 필수적으로 요구**하고 있음

- 하지만, ICT 기반 대국민 서비스·인프라를 대상으로 발생하는 **암호화된 사이버위협**은 **기존의 정보보호 기술·솔루션으로는 대응이 불가능**한 상황임

- 따라서, 암호화된 사이버위협을 신속·정확하게 분석·탐지·대응할 수 있는 **차세대 보안기술 개발이 매우 시급한 상황**으로 다부처 간 협력을 통해 **개발기간 및 예산투입을 최소화**할 필요가 있음

※ 각 부처의 독자개발에 따른 **국가 R&D 예산 중복투자를 방지**하고 개발기술의 **호환성·확장성 문제를 사전에 회피**할 필요가 있음

- 특히, 암호화된 사이버위협은 상용망, IoT망, 기간망, 복합망 등 **다양한 통신환경**과 도시, 교통, 해양 등 **다양한 국민 생활** 분야에서 동시다발적으로 발생하기 때문에 **범국가 차원의 대응체계 마련**이 매우 중요

[표 18] ICT기술 기반 디지털 뉴딜정책 대표과제의 예

주관부처	디지털뉴딜 대표과제	대분류
과학기술정보통신부	데이터 댐 프로젝트	D.N.A 생태계 강화
	양자암호통신 인프라 구축	
	ICT 중소기업 보안강화 및 SW안전진단	
	닥터앤서2.0	비대면 산업 육성

주관부처	디지털뉴딜 대표과제	대분류
국토교통부	자율주행차량	D.N.A 생태계 강화
	스마트건설	
	국민안전 스마트 인프라	SOC 디지털화
	스마트 City	
	스마트 육상물류	
해양수산부	자율운항선박	D.N.A 생태계 강화
	국민안전 스마트 인프라	SOC 디지털화
	스마트 해운물류	
행정안전부	공공데이터 개방	D.N.A 생태계 강화
	모바일 신분증	
	국민 비서	
	스마트 재해위험 알리미	SOC 디지털화
중소벤처기업부	제조데이터 플랫폼 구축	D.N.A 생태계 강화
	스마트공장 보급 · 확산	
	비대면 디지털기업 육성	
	중소기업 비대면 전환	비대면 산업 육성
	중소기업 공동활용 화상회의실	
	스마트기술 적용 소상공인 상점 · 공방	

○ 다양한 통신환경에 적용·활용 가능한 **범용성과 실용성이 보장된 원천기술을 확보**하기 위해서는 **다부처 간 긴밀한 협력이 반드시 요구**됨

- 암호화된 사이버공격은 특정 서비스·인프라를 대상으로 발생하는 것이 아니라, 경계가 없는 사이버공간에서 발생하므로 **서로 상이한 환경에서 호환될 수 있는 범용성** 확보 필요

- 각 부처에서 추진하는 대국민 공공 서비스·인프라에 대한 통신환경, 암호 프로토콜, 공격·정상 행위 정의·범위, 시스템·네트워크 구성 등에 대한 **종합적인 고려**를 통해 **포괄적인 분석·탐지·대응 매커니즘** 개발 필요

○ 각 부처가 추진하는 대국민 공공 서비스·인프라를 활용하여 **대규모의 실제 학습데이터를 확보·공유**하고 **협력체계를 구축**함으로써 **개발기술 성능 극대화** 및 **R&D 예산의 효율성 제고 필요**

- 다부처의 다양한 서비스·인프라에서 수집한 데이터를 활용할 경우,

대규모의 학습데이터를 구축할 수 있을 뿐만 아니라, **공격·정상 행위에 대한 다양성도 증가**하기 때문에 개발기술의 **확장성·견고성도 확보** 가능

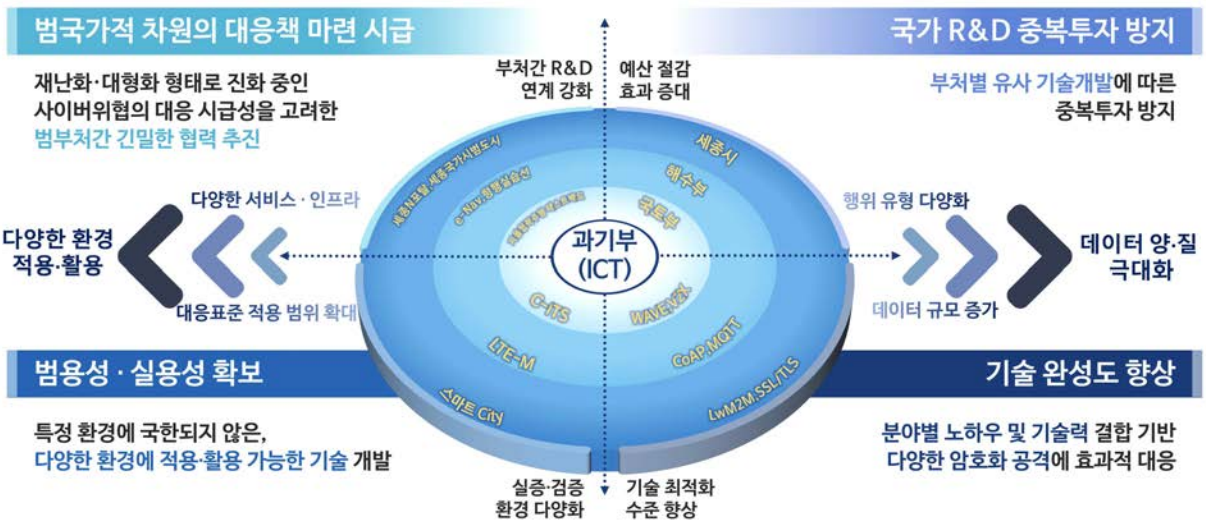
- 특정 환경에서 수집한 데이터를 활용하여 기술을 개발할 경우, 해당 환경에서만 성능이 보장되는 이른바 **'과적합', '국소해' 문제가 발생**할 수 있음

  ※ 개발 기술의 **범용성·확장성을 확보**하기 위해서는 **추가적인 R&D 사업을 추진**해야할 뿐만 아니라 **기술개발 기간이 길어**지고 **현장의 활용 시기가 늦어짐**에 따라 **유·무형의 막대한 피해 발생** 가능

- 각 부처가 보유한 서비스·인프라 **구축·운영 노하우 및 보안 기술의 성과를 결합**하여 개발 기술의 완성도 제고

○ 지속적으로 진화하고 증가하는 사이버위협에 효율적으로 대응하기 위해서는 탐지모델 및 탐지체계 협력, 위협정보 공유, 공동대응 등 **다부처가 참여하는 범국가적 일원화된 대응체계 구축**이 필요

- 효율적인 사이버 재난 예방·대응을 위해서는 **정부 중앙부처를 중심으로 하는 民·官·産·學·硏 협력 체계 구축**이 반드시 필요하고 이를 위해서는 국가적 사이버위협 상황에 신속·정확한 대응을 위한 **통합 공유·협력 플랫폼 구축** 필요



<그림 45> 암호화통신 악용 사이버공격의 다부처 협력 대응 필요성

❑ 정부 지원 필요성

ㅇ 정책적 측면

- 정부는 全산업 디지털 혁신을 위한 데이터 연결·융합(D·N·A) 중심의 정책을 중점적으로 추진하고 있으며, 특히 디지털 안심국가 실현을 위해 디지털 뉴딜 실행계획 및 K-사이버방역 추진전략을 대표적으로 발표·실행 중

- 디지털 안심국가 실현을 위해 ICT 기반 대국민 공공 서비스·인프라 등에 대한 서비스 품질 향상과 함께 보안성 및 안전성 확보를 위해 암호화 통신을 필수적으로 요구함

- 하지만, 이는 사이버위협도 동시에 암호화된다는 것을 의미하며, 기존의 평문통신에 대한 사이버위협을 분석·탐지·대응하는 기술 및 솔루션은 활용이 불가능하게 됨

- 따라서, 정부의 디지털 뉴딜 및 K-사이버방역의 성공을 뒷받침하고 암호화 통신 기반의 대국민 공공 서비스·인프라를 사이버위협으로부터 안전하게 보호하기 위해서는 차세대 보안기술 개발 및 범정부 차원의 대응체계 구축이 반드시 필요

ㅇ 사회·경제적 측면

- 대형 재난급의 사회적 혼란을 초래할 수 있는 암호화된 사이버공격을 조기에 탐지·대응할 수 있는 기술·체계를 정부 주도로 확보·적용함으로써 대국민 공공 서비스·인프라에 대한 국민 신뢰도를 향상시키고 新기술·서비스 이용에 따른 사회적 불안감 해소

- 정부에서 추진하는 대국민 공공 서비스·인프라에 대한 사이버 공격으로 발생 가능한 피해를 사전에 방지함으로써 국가재정 손실 최소화 및 복구 비용 절감

- 암호화된 사이버위협 탐지·대응 연구개발은 국내외적으로 **아직 초기 개발 단계**로서, **정부 R&D사업**을 통해 **선도적으로 원천 기술 및 응용 기술을 개발**함으로써 국내 기업의 **해외시장 선점이 기대**됨

  ※ 해외의 일부 글로벌 보안기업(美 Cisco, Juniper 등)이 원천기술 개발에 착수하였으며, 국내의 경우 정부 및 민간 주도의 연구개발이 전무하여 향후 **국내 보안시장 독점 및 기술 종속 우려** 존재

- 암호화 공격에 대한 분석·탐지·대응이 가능한 **전문 인력 교육** 및 **인력 양성**을 통해 **새로운 일자리 창출 기대**

  ※ 개발한 기술 · 시스템이 산업계로 확산할 경우 초연결 기반 암호화공격 대응을 위한 ICT 시스템 관리자, 공격 수집 · 분석 전문가, AI 전문가, 보안관제 인력 등대규모 일자리 창출 가능

ㅇ 기술적 측면

- **사이버보안 패러다임**이 기존 평문 중심 대응에서 암호화 통신 대응 중심으로 **급격하게 전환**되고 있어, **국가 주도의 핵심 원천기술 개발** 및 **범국가 차원의 사이버안보 역량 강화** 필요

- 해외 글로벌 기업 대비 **국내 보안기업의 규모가 매우 작은 상황**을 고려할 때, **민간 부문에서 대규모 R&D 예산을 투입하는 것은 현실적으로 불가능**

- 암호화된 사이버위협 분석·탐지·대응 기술 개발을 위해서는 **데이터 수집 인프라 확보**, **대규모 실제 데이터 수집**, **원천기술 개발을 위한 상당수의 석·박사급 전문가**가 필요하기 때문에 **국가 주도의 연구개발**이 반드시 필요

- 정부의 디지털 안심국가 실현을 위해서는 **국가 R&D 예산을 투입**하여 **원천기술을 확보**하고 **민간 부문에 보급·전파**함으로써 사이버보안 산업 발전 및 글로벌 기술 경쟁력 확보 기여

❑ 기존 정부 R&D 사업과의 연계성

○ 기존 사업과의 연계 및 차별화 전략

- **(기존 연구)** 암호화 트래픽 기반 공격·이상탐지 분야에서는 복호화 중심의 연구사업 추진·수행을 통해 기존 보안체계와의 연계에 초점을 맞춤

[표 19] 정부주도 관련 연구사업 및 세부내역 목록 (최근 5년)

주관부처 (사업명)	연구과제명	기간	세부 내역
과기정통부 (투자연계형기업성장 R&D지원사업)	암호화 트래픽 가시성 제공을 통한 잠재적 위협대응기술의 개발	2017.09 ~ 2018.09	·주관: ㈜피즐리소프트 ·FPGA 보드를 활용한 암호화 트래픽 가시성 확보 ·총 연구비: 400백만원
중소기업기술 정보진흥원 (창업성장기술개발사업)	무선환경에서의 산업제어시스템 보호시스템 개발	2020.12 ~ 2021.12	·주관: 빅오주식회사 ·복호화기반의 ICS 프로토콜 취약점 분석 ·총 연구비: 360백만원
정보통신기획평가원 (정보보호 핵심원천기술개발)	딥웹 및 토르기반 악성코드 분석 기술개발	2018.04 ~ 2019.12	·주관: ㈜유엠로직스 ·복호화를 통한 딥웹/토르 등 암호화 트래픽 분석 ·총 연구비: 775.1백만원
산업통상자원부 (민군기술협력사업)	암호화된 트래픽 처리를 위한 보안성을 갖춘 침입 탐지 및 차단 기술 연구	2018.06 ~ 2021.12	·주관: ㈜아토리서치 ·복호화 기반의 침입탐지, 차단 기술 개발 ·총 연구비: 381.6백만원

※ 시만텍, 수산INT社 등 보안장비제조사를 중심으로 암호화 트래픽 복호화(가시화) 장비 개발 · 보급 중

- **(차별화 방안)** 旣 사업들은 개인정보 유·노출, 한정된 복호화 대상, 대용량·초고속 네트워크 환경에서의 네트워크 병목현상 유발 등의 현실적인 문제점으로 인해 보안관제에 적용하는 것이 불가능하므로, **본 사업에서는 비복호화 기반 원천기술 연구에 초점을 맞춤**

※ 복호화의 경우 현재 1~10Gbps 수준의 환경을 지원하고 있으며, 물리적·비용적으로 100Gbps 이상의 통신을 수행 중인 대국민 서비스·인프라 전체 환경에 복호화 장비 설치 불가

- **(연계 방안)** 기존사업과의 연계 및 암호화 기반 공격·악성 트래픽 원천 행위 분석을 위해 복호화 수행을 통한 {암호문, 평문} 형태의 공격행위 연구 데이터 셋 구축 추진

※ 참여부처별 다양한 환경의 서비스 · 인프라 테스트베드 상에 복호화(가시화) 장비 설치 및 연구 데이터 수집 예정

<그림 46> 기존사업과의 차별화 및 연계 방안

❑ 다부처공동사업 참여부처 협업 방안 및 기대 효과

○ 대국민 공공 서비스·인프라를 운영, 보유한 참여부처는 본 사업의 공급처이자 수요처로써, 부처별 운용 환경을 고려한 최적화된 원천기술 개발 및 즉각적인 협력체계 구축이 가능

- **(과학기술정보통신부)** 악성 암호화 트래픽 분석·탐지·대응 핵심 원천기술 개발과 데이터 공유 체계 구축을 위한 통합 플랫폼 구축 선도

- **(국토교통부)** 지능형교통체계(C-ITS 등) 환경에서의 암호화 트래픽 및 악성코드 수집·공유 및 개발된 원천기술 적용·최적화 수행

- **(해양수산부)** LTE-M 기반 스마트 선박·항만 환경에서의 암호화 트래픽·악성코드 수집·공유 및 개발된 원천기술 적용·최적화 수행

- **(세종특별자치시)** 스마트 City 환경에서 발생하는 암호트래픽·악성코드 수집·공유, 실환경 테스트베드 제공 및 기술 검증·최적화 수행

○ 다부처 추진 협의체 구성을 통한 정기적인 회의를 바탕으로 기술적 이슈에 대한 마일스톤 방식의 개발관리 협의 및 조정

- 요구사항, 기능, 설계 검토 및 기본·상세 설계, 시험방안, 운영방안 검토 등을 수행

- 부처별 운영요구사항 부합성 평가 등을 실시하여 수요처 니즈 충족 및 사업 완성도 향상 추진

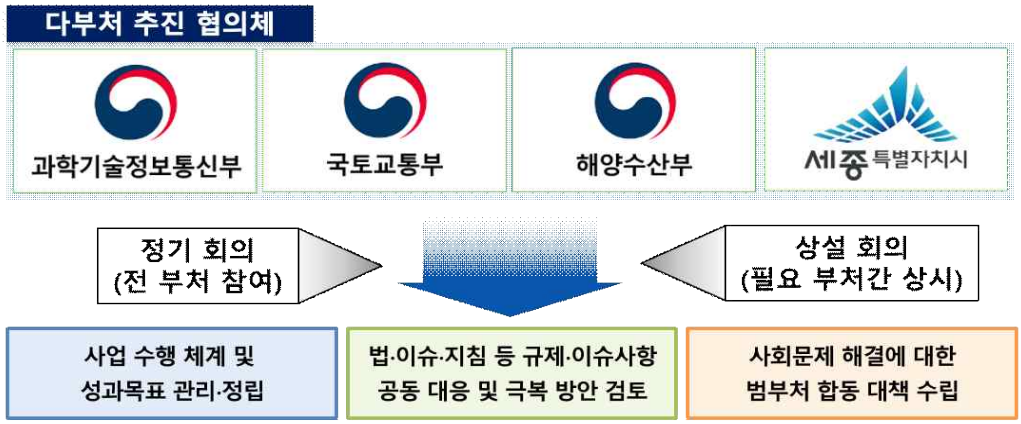
<그림 47> 주관 · 참여부처의 다부처 추진 협의체 구성 및 운영

○ **다부처 추진 협의체 구성 기대 효과**

- 사업의 목적, 요구사항 및 수행방법 등을 긴밀히 논의·협력하여 성공적인 사업 수행 및 성과목표 달성 추진

- 사업추진 관련 부처간 상이한 법, 지침 등 규제·이슈 사항에 대한 공동 대응 및 극복 방안 검토 추진

- 일자리창출 등 사회문제 해결에 대한 범부처 합동 대책 수립 추진을 통해 정책 실효성 확보



<그림 48> 다부처 추진 협의체 구성의 기대효과

제2장 사업목표 및 내용

제1절 사업목표

❑ 사업 최종 목표

○ 대국민 공공 서비스·인프라*에 대한 **암호화된 사이버위협을 선제적으로 탐지·대응**하기 위한 **차세대 보안관제 기술 개발 및 공유·협력 체계 구축**

- 암호화 트래픽에 대한 실시간 수집·처리, 공격·정상 행위 분석·탐지·대응 원천기술 개발 및 실환경 기반 대규모 학습데이터 확보

- 암호화된 사이버위협 정보 및 탐지·분석 모델·규칙을 공유하고 효율적인 대응체계 구축·운영을 위한 통합 플랫폼 개발

* 지능형 ICT(과기정통부), 지능형 교통(C-ITS, 국토교통부), 스마트 선박·항만(LTE-M, 해양수산부), 스마트 City(세종특별자치시) 등

<그림 49> 연구개발 목표

○ **(원천기술)** 국민의 사생활 보호를 위해 별도의 복호화 없이 암호화 통신에 숨겨진 악성코드 및 고위험 사이버공격을 탐지·차단하는 원천기술 개발

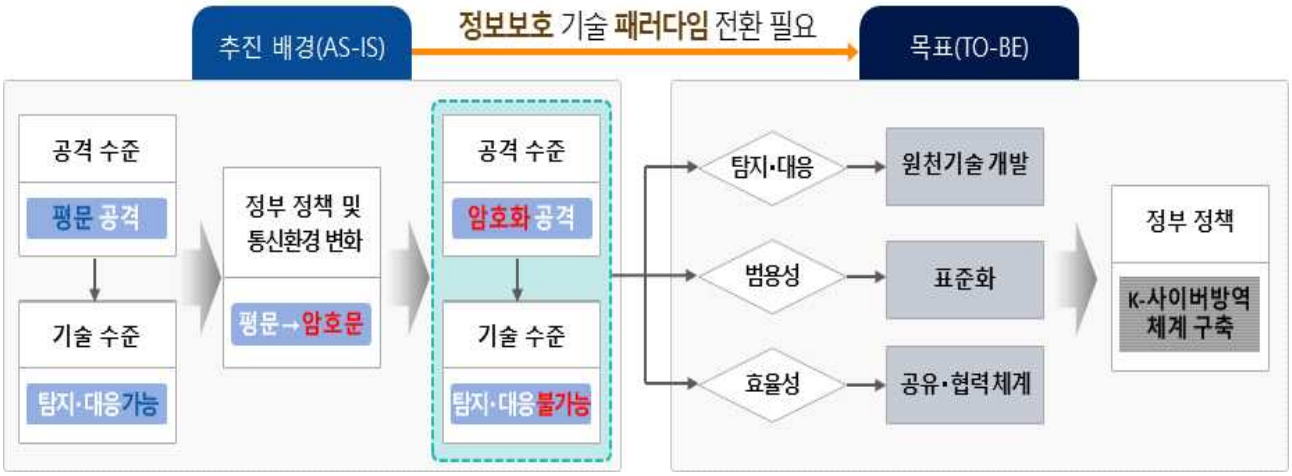
- **(정보 수집)** 환경별 암호화 정상·공격 트래픽, 디바이스·센서 정보 수집 기술 설계 및 데이터셋 구축

- **(분석·탐지)** 트래픽 및 디바이스 행위 분석 기술 개발 및 악성·정상·이상 행위 모델링

- **(실증 및 최적화)** 환경별 자동화 탐지기술 실증 및 성능평가, 실환경 적용 및 모델 성능 최적화

○ **(표준화)** 서로 다른 공공 서비스·인프라에서 발생하는 다양한 유형의 암호화 공격 공동대응 및 협력을 위한 공격행위 표준화 기술 개발

○ **(협력체계)** 전통적인 정보보호체계의 한계점을 극복하기 위하여 암호화된 악성공격 대응 및 정보 공유·협력 체계 구축



<그림 50> 연구개발 및 사업 범위

❑ 사업 범위

○ (**대상 인프라·서비스**) 정부에서 추진하는 ICT 기반 대국민 공공 서비스·인프라 중 **다양한 암호화 통신환경을 포함**(유·무선망, IoT망, 기간망, 복합망 등)하고 **국민생활과 밀접하게 연결**(생활, 도시, 교통, 선박)되어 있는 핵심 4종 서비스·인프라(아래 그림51 참조)

- **암호화된 공격·정상** 데이터(평문쌍 포함) 수집 및 개발 기술의 실증 수행

○ (**원천기술 개발**) 암호화된 트래픽에서 실제 사이버위협과 정상행위를 **자동으로 탐지·분류** 할 수 있는 **행위기반 보안관제** 기술 개발

- 암호 트래픽의 복호화에 따른 **시스템 및 네트워크 성능 저하, 국민 사생활 침해 등 현실적인 한계를 극복**하기 위해 별도의 복호화를 요구하지 않는 **(비복호화 기반)** 기술 개발

○ (**기술 표준화·실증 및 플랫폼 구축**) 모든 부처에서 추진하는 대국민 공공 서비스·인프라에 활용 가능하도록 **범용성과 실용성이 보장**된 기술 개발 및 **공유·협력 플랫폼** 개발

- 각 부처의 통신환경별 **최적화 및 표준화** 연구 필수 수행, 사업성과에 대한 **활용성 제고**

<그림 51> 연구개발 및 사업 범위(상세)

❑ 수혜 대상

ㅇ 대국민 공공 서비스·인프라 및 국가주요기반시설 운영기관·정부기관

- 사업 참여 대상 부처의 대국민 공공 서비스·인프라
- 국가정보보안지침에 따른 국가·공공 부문 보안관제센터
- 발전소, 공항, 항만 등을 포함한 국가주요기반시설의 ICT 인프라
- 각 정부부처에서 추진 중인 디지털뉴딜정책의 대표 ICT 서비스

ㅇ 정보보호 산업계를 포함한 민간 분야

- 네트워크 보안장비(IDS, IPS 등) 및 보안 솔루션 제조업체
- 대학교, 직업교육기관 등 정보보호 인력 육성 기관 등

제2절 성과목표 및 지표

❑ 사업 성과목표

구분	내용
최종목표	○ 암호화 사이버공격 대응 원천기술 개발 및 공유·협력 체계 구축 – 암호화통신 기반 악성·공격 행위 탐지 및 분석 원천기술 개발 ※ (과기정통부) 실시간 악성·공격 행위 분석 및 탐지·대응 기술 ※ (국토부) 지능형교통체계에 최적화된 분석·탐지 기술 개발 및 실증 ※ (해수부) 지능형해상교통망에 최적화된 분석·탐지 기술 개발 및 실증 ※ (세종시) 스마트 City 환경에 최적화된 분석·탐지 기술 개발 및 실증 – 악성·공격 행위정보 표준화 및 공유·협력 플랫폼 구축 ※ (과기정통부) 행위정보 표준화 포맷 제정 및 공유·협력 플랫폼 개발 ※ (국토부, 해수부, 세종시) 암호화 트래픽 전용 표준탐지규칙 정의 및 공유·협력 ○ 연구개발 결과물 – AI기반 암호화 공격 탐지·대응 모델 (S/W) – 암호화 공격 탐지·대응 솔루션 (H/W, S/W) – 악성·공격 행위 표준데이터 및 공유·협력 플랫폼 시스템 (H/W, S/W 및 활용 매뉴얼)
성과목표	○ 주요 기능(또는 규격) – 암호화 트래픽·디바이스 행위 데이터셋 ※ 각 환경별 암호화된 정상행위 수집 ※ 각 환경별 암호화된 악성행위 수집(랜섬웨어, 스파이웨어 등 주요 악성코드 포함) ※ 각 환경별 디바이스 행위 정보 수집(PC, 서버, IoT 등) ※ 암호화 악성·공격행위 탐지기술 개발을 위한 수집정보 가공 및 데이터셋화 – 암호화 악성·공격 행위 탐지·대응 기술(비복호화) ※ 메타정보 기반 악성·공격 행위 탐지 모델 개발 ※ 행위정보를 활용한 악성·공격 행위 탐지 모델 개발 ※ 환경별 대표적 악성코드 탐지 모델 개발 ※ 각 환경별 악성·공격 행위 탐지 및 분석 모델 최적화 ※ 암호화 악성·공격행위 탐지모델 운영용 차세대 IDS 개발 – 암호화 기반 악성·공격 행위정보 설명 표준화 포맷 및 행위 탐지규칙 ※ 악성·공격 행위특징 기반 표준화 모델 개발 ※ 악성·공격 행위특징 기반 차세대 IDS용 탐지규칙 개발 – 공유·협력 플랫폼 기반 데이터 전송·공유·저장 ※ 암호화 기반 악성·공격 행위정보 공유·대응을 위한 국가·공공 플랫폼 개발 ※ 악성·공격 행위정보 공유 플랫폼 활성화 및 대응력 강화 추진

	○ 주요 성능치 - (400종, 5억건 이상) 탐지모델 구축을 위한 대용량 데이터셋† - (복호화 탐지 대비 90%이상) 악성·공격 행위 탐지 모델 정확도†† ※ 복호화(가시화) 적용 후 평문기반 IDS/IPS 장비 활용 기준 - (세션 종료 후 5분 이내) 악성·공격 행위 탐지 신속도‡ ※ 세계최고 수준의 ETA장비인 Cisco사 Catalyst 9K series 성능 기준 - (400개 규칙 이상) 암호트래픽 전용 표준탐지규칙 수‡‡ - (8개소 이상) 악성·공격 행위 탐지 기술 실증 및 유효성 검증 환경‡‡‡ ○ 적용 범위(또는 서비스) – 국가과학기술연구망 및 과기정통부 산하 연구기관 – 부처별 대국민 공공 서비스 · 인프라 환경 – 공공분야 각급 보안관제센터 – 국가기반시설 및 주요정보통신기반시설 등

※ 주요 성능 지표 정의 및 목표치 근거

† (데이터 셋) 국내 최대 수준의 KISA ‘사이버보안 인공지능 데이터셋 구축 사업 (2021)’ 구축 목표인 380종, 4.1억건(침해사고 예 · 탐지, 백신 진단 악성코드 및 최신 사회이슈 악성코드 분야 시뮬레이션) 수준 이상

†† (탐지 정확도) 기존 복호화 솔루션(평문기반)과 유사한 수준의 기술개발 목표 수립

‡ (신속도) CISCO 社: Anderson, Blake, and David McGrew. "Identifying encrypted malware traffic with contextual flow data." Proceedings of the 2016 ACM workshop on artificial intelligence and security. 2016.

‡‡ (탐지 규칙 수) 대응 목표 악성행위 400종에 대한 각각 탐지규칙 1개 이상

‡‡‡ (실증처) 참여부처 4곳에서 각각 2개소 이상의 실증환경 제공 및 테스트 수행

❑ 정량적 목표

부처 (차수)	목표	평가항목	단위	현재기술수준 TRL 단계 (As-Is)	개발 목표치 TRL 단계 (To-Be)	평가방법
과학기술 정보통신부 (1차,2차)	구축	레거시 네트워크 환경에서의 정상/악성 암호트래픽 원천 데이터 수집	식	2	5~6	자체평가
과학기술 정보통신부 (2차)	구축	레거시 네트워크 기반 정상/악성 암호트래픽 학습/테스트 데이터셋 구축	식	2	5~6	자체/공인
과학기술 정보통신부 (2차)	개발	암호화된 위협징후 탐지 및 분석 모델	종	1	5~7	자체/공인
과학기술 정보통신부 (3차)	적용, 실증	탐지 가능한 암호화된 위협징후의 종류	종	2 ~ 3	5~7	자체/공인
과학기술 정보통신부 (4차)	적용	위협 암호화 트래픽 탐지 모델 실증을 위한 환경	SITE	2	5~6	자체/공인
과학기술 정보통신부 (4차)	개발	암호화 트래픽 특징 분석을 통한 표준화 포맷 정의	종	0	5~7	자체/공인
과학기술 정보통신부 (5차)	개발	암호화 악성행위 공동대응을 위한 공유·협력 플랫폼 구축	조	1	5~7	자체/공인
과학기술 정보통신부 (5차)	개발, 실증	포괄적 탐지 매커니즘(엔진) 개발 및 최적화	식	1	5~7	자체/공인
국토교통부 (1차,2차)	구축	지능형교통 인프라 통신에서의 정상/악성 암호트래픽 원천데이터 수집	식	2	5~6	자체평가
국토교통부 (1차,2차)	구축	지능형교통 인프라 통신에서의 디바이스/센서 정보 수집	식	2	5~6	자체평가
국토교통부 (2차)	구축	지능형교통 인프라 기반 정상/악성 암호트래픽 학습/테스트 데이터셋 구축	식	2	5~6	자체/공인

국토교통부 (3차)	적용, 실증	위협 암호화 트래픽 탐지 모델 성능	종	2 ~ 3	5~7	자체/공인
국토교통부 (4차)	개발	암호화 트래픽 특징 분석을 통한 표준화 포맷 정의	종	0	5~7	자체/공인
해양수산부 (1차,2차)	구축	LTE-M 인프라 통신에서의 정상/악성 암호트래픽 원천 데이터 수집	식	2	5~6	자체평가
해양수산부 (1차,2차)	구축	LTE-M 인프라 통신에서의 디바이스/센서 정보 수집	식	2	5~6	자체평가
해양수산부 (2차)	구축	LTE-M 인프라 기반 정상/악성 암호트래픽 학습/테스트 데이터셋 구축	식	2	5~6	자체/공인
해양수산부 (3차)	적용, 실증	위협 암호화 트래픽 탐지 모델 성능	종	2 ~ 3	5~7	자체/공인
해양수산부 (4차)	개발	암호화 트래픽 특징 분석을 통한 표준화 포맷 정의	종	0	5~7	자체/공인
세종특별자치시 (1차,2차)	구축	스마트 City 서비스·인프라의 정상/악성 암호트래픽 원천데이터 수집	식	2	5~6	자체평가
세종특별자치시 (1차,2차)	구축	스마트 City 서비스·인프라의 IoT 센서 디바이스/센서 정보 수집	식	2	5~6	자체평가
세종특별자치시 (2차)	구축	스마트 City 인프라 기반 정상/악성 암호트래픽 학습/테스트 데이터셋 구축	식	2	5~6	자체/공인
세종특별시 (3차)	적용, 실증	위협 암호화 트래픽 탐지 모델 성능	종	2 ~ 3	5~7	자체/공인
세종특별시 (4차)	개발	암호화 트래픽 특징 분석을 통한 표준화 포맷 정의	종	0	5~7	자체/공인
전부처 공통 (5차)	개발	포괄적 탐지 매커니즘(엔진) 상용화 시제품	식	1	5~7	자체/공인

제3절 사업내용

❑ 총괄

번호	부처	사업목표	사업주요내용
1	과학기술정보통신부	악성 암호화 트래픽 분석·탐지·대응 핵심 원천기술 개발과 데이터 공유 체계 구축을 위한 통합 플랫폼 구축	• 지능형 ICT환경에서의 악성 · 공격 암호트래픽 탐지 모델 개발을 위한 학습/테스트 데이터셋 수집 · 구축 • 암호화된 위협징후 탐지 기술 개발 • 악성행위 트래픽 특징 분석을 통한 표준화 포맷 정의 • 암호화 악성행위 공동대응을 위한 공유 · 협력 플랫폼 구축 • 포괄적 탐지 매커니즘(엔진) 개발 및 최적화
2	국토교통부	지능형교통 환경에서의 암호트래픽/악성코드 수집·공유 및 개발된 원천기술 적용 및 최적화	• 지능형교통 환경에서의 암호화 트래픽 수집, 공유 및 데이터셋 구축 • 탐지·대응 기술 최적화 및 실증 • 암호화 악성행위 공동대응을 위한 공유 · 협력 플랫폼 참여 • 포괄적 탐지 매커니즘(엔진) 상용화 시제품 개발 협력
3	해양수산부	LTE-M 기반 스마트 선박·항만 환경에서의 암호트래픽/악성코드 수집·공유 및 개발된 원천기술 적용 및 최적화	• LTE-M 환경에서의 암호화 트래픽 수집, 공유 및 데이터셋 구축 • 탐지·대응 기술 최적화 및 실증 • 암호화 악성행위 공동대응을 위한 공유 · 협력 플랫폼 참여 • 포괄적 탐지 매커니즘(엔진) 상용화 시제품 개발 협력
4	세종특별자치시	스마트 City 환경에서 발생하는 암호트래픽/악성코드 수집·공유, 實환경 테스트 베드 제공 및 기술 검증·최적화	• 스마트 City 서비스 · 인프라 환경에서의 암호화 트래픽 수집, 공유 및 데이터셋 구축 • 탐지·대응 기술 최적화 및 실증 • 개발 기술검증을 위한 實환경 테스트 베드 제공 • 암호화 악성행위 공동대응을 위한 공유 · 협력 플랫폼 참여 • 포괄적 탐지 매커니즘(엔진) 상용화 시제품 개발 협력

❑ 세부 연구 목표

○ **(정보 수집)** 대국민 공공 서비스·인프라 기반 암호화통신·디바이스 전주기 정보 수집

- 정상 및 악성행위 암호화·평문 네트워크 트래픽 정보 수집(프로토콜 헤더, 메타데이터 등)
- 통신 디바이스 행위 정보 수집(어플리케이션, 게이트웨이, 활성화 정보 등)
- 공공·민간 위협 인텔리전스 기반 데이터 수집(MITRE ATT&CK, NCTI 등)
- 오픈 데이터 소스를 활용한 최신 공개 데이터 수집(APCERT/CTA 등)

○ **(분석·탐지)** 암호화기반 공격·악성행위 분석·탐지 원천기술 개발

- 네트워크 메타정보*를 활용한 공격·악성행위 분석·탐지 모델 개발

* 암호화 트래픽에도 통신 절차 수립을 위한 일부 메타(평문)정보 포함

- 디바이스·네트워크 행위 기반의 공격·악성행위 탐지 모델 개발

※ 악성·정상·이상 행위별 모델링 및 화이트·블랙리스트 데이터베이스 구축

- 암호화기반 악성코드(멀웨어) 공격·악성행위 분석·탐지 모델 개발

※ 랜섬웨어, 백도어, 스파이웨어, 웜 등 주요 악성코드 분석 · 탐지 기술 확보

○ **(최적화·실증)** 부처별 서비스·인프라 대상 자동탐지 시스템 설계·최적화 및 실증·성능평가

- 상용망, C-ITS, LTE-M 및 스마트 City 환경의 탐지시스템 구축 및 성능 최적화
- 상용망, C-ITS, LTE-M 및 스마트 City 환경의 테스트베드 구축 및 실증 수행

○ **(표준화)** 다양한 암호화 공격·악성행위 통합 대응 및 협력을 위한 행위 표준화 기술 개발

- 암호화 통신 기반 네트워크 트래픽 특징·행위 정보 모델링 및 표준포맷 정의

- 네트워크 보안장비와의 연동을 위한 행위 기반 표준 모델의 탐지 패턴화

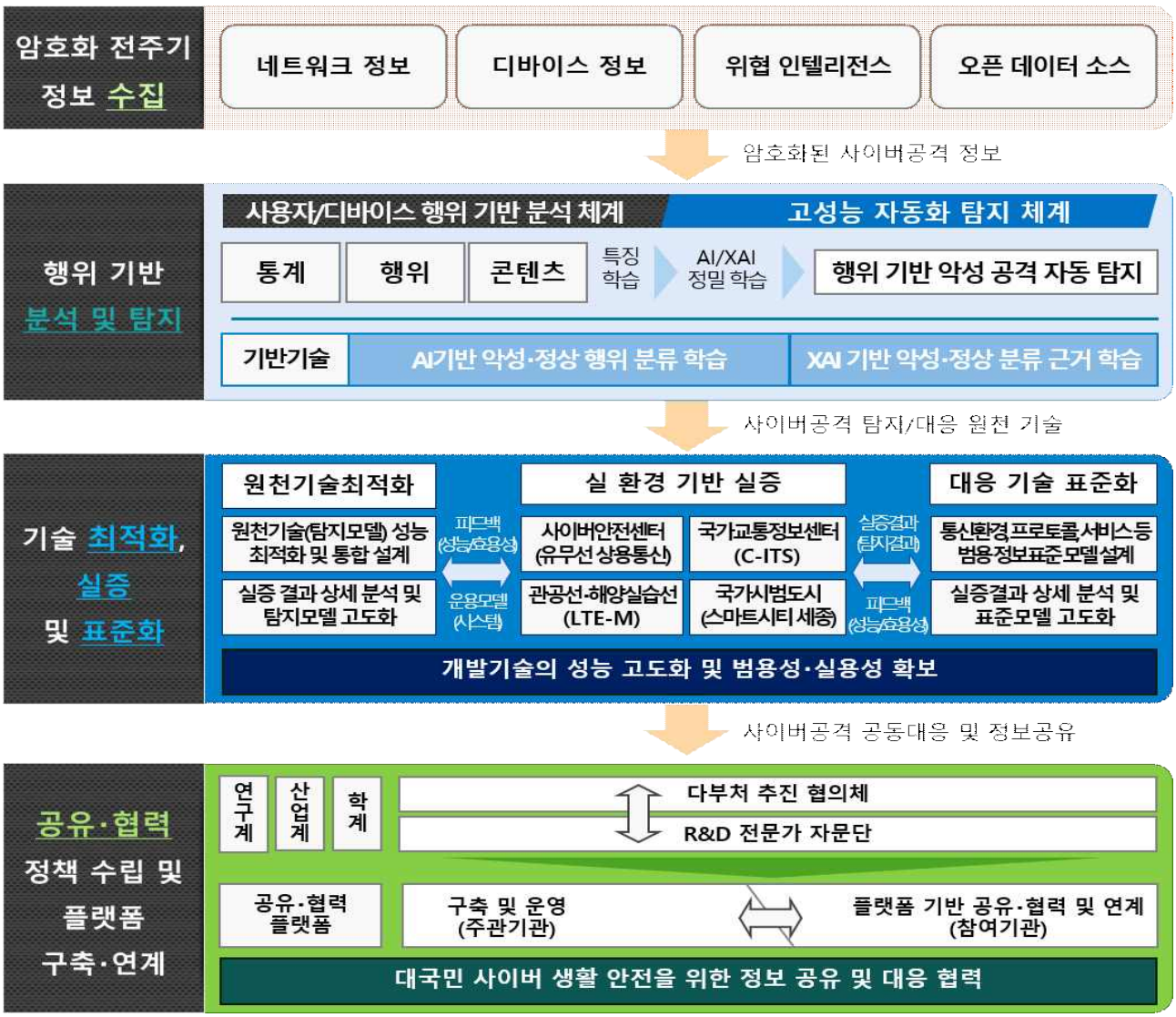
※ 암호화 트래픽 분석 보안장비의 상용화를 고려한 탐지 패턴 개발 · 구축

○ **(공유·협력)** 국가·공공 분야 암호화 공격 대응을 위한 공유·협력 체계 구축

- 암호화 통신 기반 공격·악성행위 공유 및 대응, 협력 플랫폼 개발 및 구축

- 공유·협력 플랫폼 기반 정보공유 활성화 및 위협 공동 대응 추진

- 국가·공공 분야를 비롯한 민간 분야를 포함한 공유, 협력 체계 확산 추진



<그림 52> 연구개발 단계별 사업 세부 내용

1 과학기술정보통신부

1. 목표 및 연구개발 내용

❑ 연구개발 목표

ㅇ **지능형 ICT환경 기반 암호화 사이버공격 탐지·대응 기술 및 위협정보 공유·협력 플랫폼 개발**

❑ 연구개발 내용

ㅇ **원천기술 연구 개발**

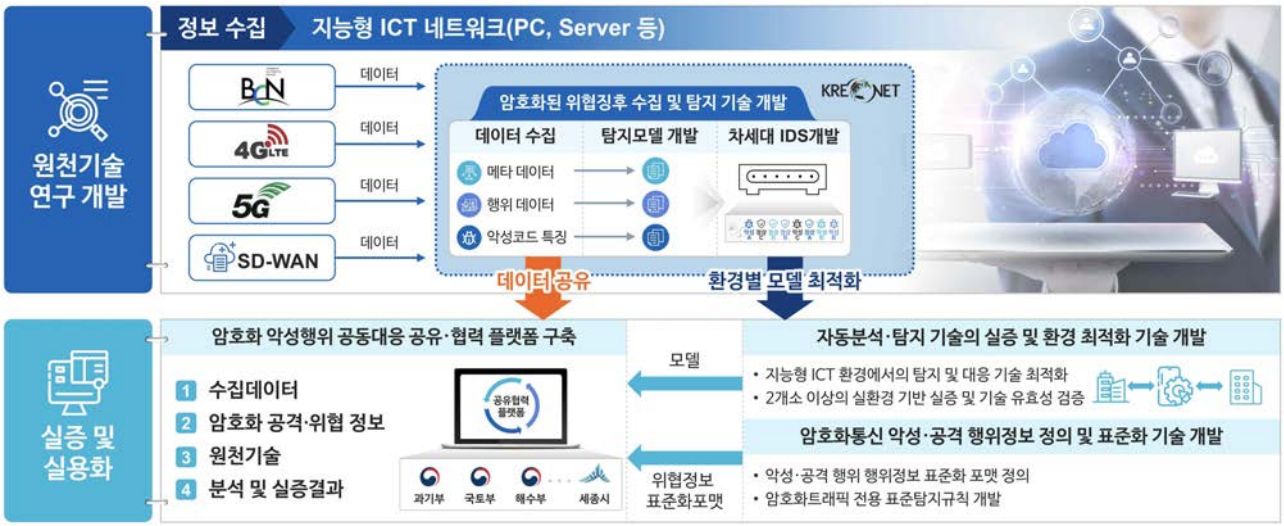
- (정보 수집)지능형 ICT환경 기반 악성·공격 행위 암호화·평문 트래픽 수집 기술 개발
- (정보 수집)자동탐지·대응 모델 구축을 위한 레거시 트래픽 특징 분석 기반 데이터셋 구축
- (분석·탐지)메타정보를 활용한 악성·공격 행위 분석 기술 및 탐지 모델 개발
- (분석·탐지)행위기반 암호화 트래픽 분석 기술 및 탐지 모델 개발
- (분석·탐지)대표적 암호화 악성코드 분석 기술 및 탐지 모델 개발
- (분석·탐지)AI/XAI를 통한 행위기반 자동화 분석, 탐지 및 대응 기술 개발

ㅇ **실증 및 실용화**

- (최적화·실증)지능형 ICT환경의 실환경 테스트베드를 활용한 실증 및 탐지 기술 최적화
- (표준화)악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의

기술 개발

- (공유·협력)위협 확산 방지 및 대응 방안 공유를 위한 정보 공유·협력 플랫폼 구축



<그림 53> 과학기술정보통신부 연구개발 세부 내용

2. 추진내용

❑ 과학기술정보통신부 사업 RFP(안)

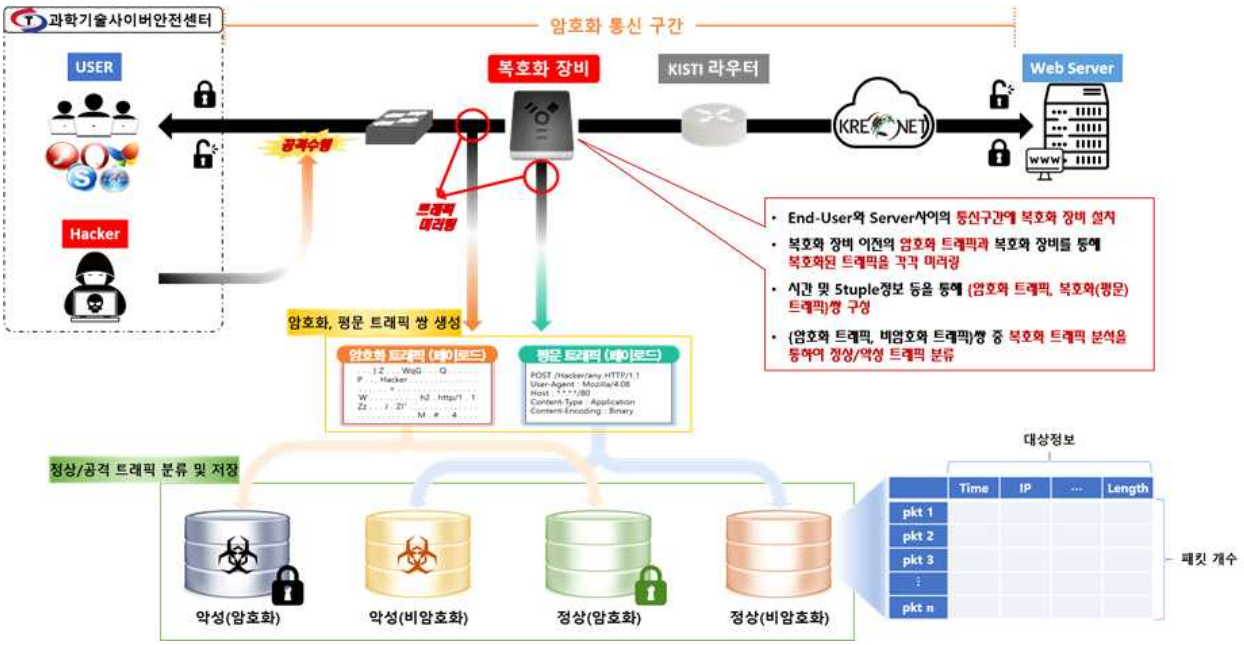
주요사업명	암호화통신 기반 사이버공격 탐지·대응 기술 및 위협정보 공유·협력 플랫폼 개발	부처	과학기술정보통신부
사업개요	○ 암호화통신 기반 사이버공격에 대한 탐지·대응 원천기술 개발 및 국가·공공분야 암호화 공격 대응을 위한 공유·협력 플랫폼 개발		
현황 및 필요성	<현황> ○ 최근 개인정보보호 및 보안성 강화를 목적으로 암호화 트래픽을 의무화하는 정부정책이 수립되고 있으며, 이미 대부분의 네트워크 통신은 암호화 트래픽을 활용 중 (웹 통신 95% 이상) ○ 암호화 트래픽의 확산은 정상 서비스의 데이터 보호뿐만 아니라 멀웨어 또는 해커들의 위협행위들을 보안장비로부터 은닉하는데도 활용되고 있어 사이버 위협으로 인한 피해가 폭발적으로 증가 중 ○ 암호화 트래픽 복호화(가시화) 기술개발 등의 대응책이 활용 중에 있으나, 네트워크 병목 현상, 한정된 복호화 대상, 개인정보를 포함한 민감정보 유·노출과 같은 문제점을 내포하고 있음		

	<필요성> ㅇ 대규모·대용량·초고속 네트워크 환경으로의 변화에 따라 복호화기반 암호화 공격 대응에는 한계가 존재하므로, 비복호화 기반의 사이버공격 분석·탐지로의 대응 정책·기술 패러다임 변화 필요 ㅇ 사이버보안 사각지대로 분류되고 있는 암호화(지능화·은닉화·난독화)된 사이버 공격으로부터의 사전 피해 방지 및 국가적 대응 체계 수립 필요
사업목표	ㅇ 암호화통신 기반 사이버공격에 대한 탐지 및 대응 원천기술 개발 ㅇ 국가·공공 분야 암호화 공격 대응을 위한 공유·협력 플랫폼 개발
연구개발내용	ㅇ 원천기술 연구 개발 - 지능형 ICT환경 기반 악성·공격 행위 암호화·평문 트래픽 수집 및 데이터셋 구축 기술 개발 - 메타정보를 활용한 악성·공격 행위 분석 기술 및 탐지 모델 개발 - 행위기반 암호화 트래픽 분석 기술 및 탐지 모델 개발 - 대표적 암호화 악성코드 분석 기술 및 탐지 모델 개발 - AI/XAI를 통한 행위기반 자동화 분석, 탐지 및 대응 기술 개발 ㅇ 실증 및 실용화 - 악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의 - 지능형 ICT환경의 실환경 테스트베드를 활용한 실증 및 탐지 기술 최적화 - 위협 확산 방지 및 대응 방안 공유를 위한 정보 공유·협력 플랫폼 구축 - 원천기술 실용화 추진을 위한 포괄적 탐지 매커니즘(엔진) 개발 및 최적화 - 협력 플랫폼 활용을 통한 수집데이터·분석기술·실증결과 공유 (전부처 공통)
기대효과	ㅇ 암호통신에 따른 사이버공격 탐지기술 부재로 인한 보안문제를 해결할 수 있는 핵심 원천기술 확보 ㅇ 비복호화 기반 사이버공격 탐지·대응 기술 개발을 통해 사회적 혼란을 초래할 수 있는 암호화 통신 기반 사이버공격을 조기에 탐지·대응함으로써 국민생활 안정 및 디지털 안심국가 실현 ㅇ 암호화 통신 기반 사이버공격에 대한 대응력을 강화함으로써 경제적·사회적 피해 최소화 및 복구비용 절감
소요예산/기간	190억/5년 (*1차년도 데이터 수집장비 및 4차년도 실증·시제품 비용증가 예상분 반영)
중복성 검토	해당사항 없음

❑ 세부추진 내용

○ (정보 수집) 지능형 ICT환경에서의 암호문·평문 트래픽 수집 및 데이터셋 구축 기술

- 암호화 트래픽에 대한 메타정보(평문) 수집 기술 개발
- 암호화 트래픽의 악성·공격 행위 수집 기술 개발
- 데이터셋 구축을 위한 복호화기반 평문-암호트래픽 쌍 수집 기술 개발
- 암호화 트래픽 기반의 악성코드 행위 정보 수집 기술 개발
- 자동 탐지·대응 모델 개발을 위한 수집데이터의 학습·검증 데이터셋화



<그림 54> 지능형 ICT환경(레거시 네트워크 환경)에서의 시스템 구축 및 트래픽 수집 방안

○ (분석·탐지) 암호화 트래픽 기반 악성·공격 행위 분석·탐지 기술 개발

- 메타정보를 활용한 공격행위 탐지기술

※ 네트워크 세션 생성 시 패킷 길이, 전달 시간 및 순위, 바이트 분포, Cipher suit 등의 메타정보 수집 및 저장 기술 개발

※ 수집된 메타정보 분석을 통한 암호화 기반 공격 트래픽 분류모델 개발

※ 메타정보를 활용한 공격행위 탐지모델 검증시스템 개발

- 네트워크 행위기반 암호화 트래픽 탐지기술

※ 네트워크 플로우(flow) 분석을 통한 임계치 기반의 공격 트래픽 탐지 및 대응기술 개발

※ 암호화 통신 중 부가적으로 발생하는 행위정보 분석을 통한 분류모델 개발

※ 행위기반 암호화 트래픽 탐지모델 검증시스템 개발

- 암호화 트래픽 기반의 악성코드 탐지기술 개발

※ 지능형 ICT환경에서 암호화 통신을 사용하는 대표적인 멀웨어 패밀리 수집

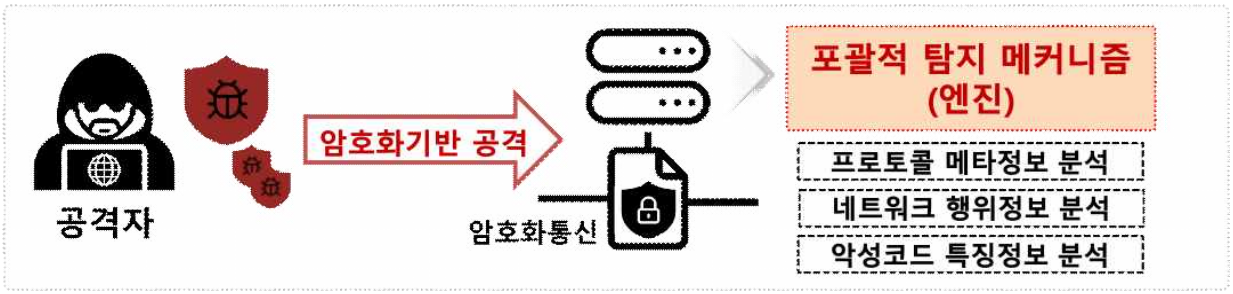
※ 멀웨어 패밀리의 네트워크 행위 모니터링 및 분석기술 개발

※ 멀웨어 패밀리의 네트워크 행위 학습 및 검증 시스템 개발

- AI/XAI 기술 기반의 행위기반 자동분석·탐지 기술 개발

※ 다양한 악성 · 공격 행위에 신속 탐지 · 대응 가능한 자동분석 · 탐지 기술 개발

※ XAI 기술을 활용한 행위정보 설명기반의 탐지 모델 성능 고도화 기술 개발



<그림 55> 암호화 트래픽 악성 · 공격 행위 탐지 접근 방법

ㅇ (최적화·실증) 자동분석·탐지 기술의 실증 및 환경 최적화 기술 개발

- 지능형 ICT환경의 실환경 테스트베드를 활용한 실증 및 탐지 기술 최적화

※ 2개소 이상 상이한 환경의 실증 테스트베드 확보 및 기술 최적화 수행

ㅇ **(표준화) 암호화통신 악성·공격 행위정보 정의 및 표준화 기술 개발**

- 악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의

※ 다양한 환경의 서비스 · 인프라에 적용을 위한 행위정보 표준포맷 개발

- 탐지·분석기술 실용·제품화를 위한 암호화 트래픽 전용 표준탐지규칙 개발

※ 네트워크에 인입 탐지 · 분석용 H/W를 위한 표준 탐지규칙 정의

ㅇ **(공유·협력) 위협 확산 방지 및 대응 방안 공유를 위한 정보 공유·협력 플랫폼 구축**

- 국가·공공분야 각 주체간 암호화 트래픽 악성·공격 행위정보·탐지규칙·위험 징후·공격자정보 등의 공유 및 공동 대응·협력을 위한 플랫폼 개발

- 협력 플랫폼 활용을 통한 수집데이터·분석기술·실증결과 공유 (전부처 공통)

- 원천기술 실용화 추진을 위한 포괄적 탐지 매커니즘(엔진) 개발 및 최적화

<그림 56> 국가 · 공공 분야 암호화 공격 · 위협정보 공유 · 협력 플랫폼 활용 방안

2 국토교통부

1. 목표 및 연구개발 내용

❑ 연구개발 목표

ㅇ **차세대 지능형교통체계의 사이버재난·재해 예방 및 확산 방지를 위한 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발**

❑ 연구개발 내용

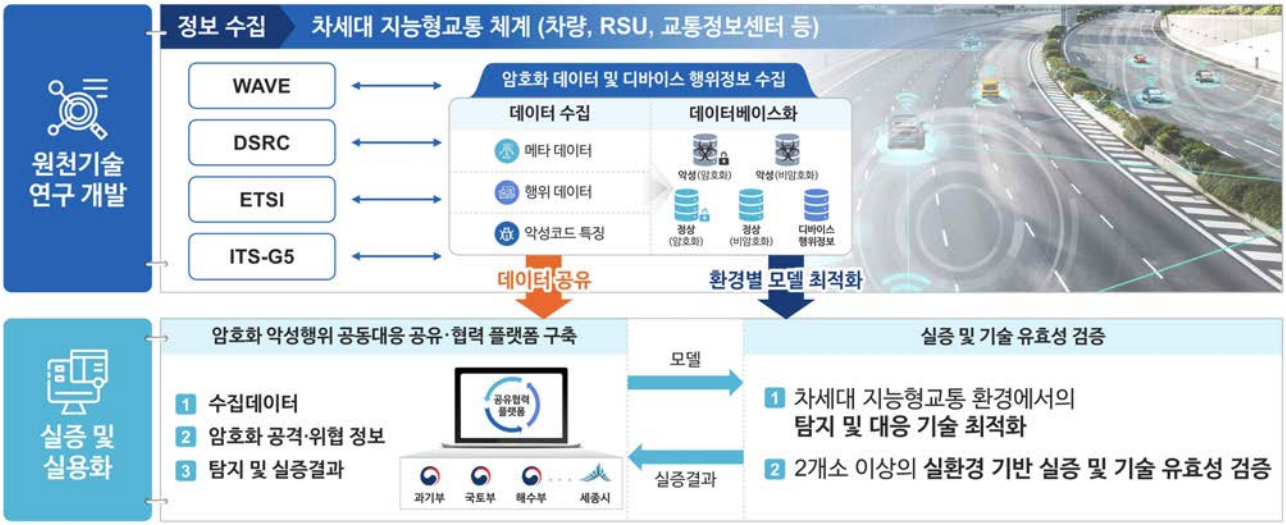
ㅇ **원천기술 연구개발 단계**

- (정보 수집)차세대 지능형교통체계(C-ITS)기반 악성·정상행위 암호문·평문 트래픽 수집
- (정보 수집)차세대 지능형교통체계(C-ITS)기반 디바이스·센서 행위정보 수집
- (정보 수집)자동탐지·대응 모델 구축을 위한 차세대 지능형교통체계 트래픽·디바이스 특징 분석기반 데이터셋 구축

ㅇ **실증 및 실용화 단계**

- (최적화·실증)차세대 지능형교통체계(C-ITS)환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화
- (최적화·실증)차세대 지능형교통체계의 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증
- (표준화) 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화

- (공유·협력) 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력



<그림 57> 국토교통부 연구개발 세부 내용

2. 추진내용

❑ 국토교통부 사업 RFP(안)

주요사업명	차세대 지능형교통체계의 사이버재난·재해 예방 및 확산 방지를 위한 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발	부처	국토교통부
사업개요	○ 암호화통신 기반 사이버공격으로부터 대국민 공공 서비스·인프라인 차세대 지능형 교통체계 보호를 위한 공격·악성행위 탐지·대응 기술 최적화 및 실증 서비스 개발		
현황 및 필요성	<현황> ○ 일방적으로 정보를 수신하던 전통적인 교통환경에서 상호 교통정보를 송·수신하는 차세대 지능형교통체계가 구축되고 있으며, 이러한 교통환경 변화에 따라 교통정보 위·변조, 교통정보 불법도청, 차량 위치정보 무단 획득, 거짓교통상황정보 전송 등과 같은 다양한 사이버 위협이 발생 ○ 교통정보보호를 위해 주요 국가 및 기관에서 중요 교통정보 암호화 및 전송 기술 적용을 검토 중 ○ 교통정보 암호화 시 이를 악용한 암호화통신 기반의 사이버 공격 사례가 증가할 수 있으며, 이에 대한 대비가 필요한 상황 <필요성> ○ 지능형교통체계를 구축하는 차량 및 노변기지국에서 수집되는 네트워크 트래픽의 양은 대규모·대용량이기 때문에 복호화기반 암호화공격 대응에는 한계가 존재하므로,		

	비복호화 기반의 사이버공격 분석·탐지로의 대응 정책·기술 패러다임 변화 필요 o 차세대 지능형교통체계의 사이버 재난·재해 예방 및 확산 방지를 위해 암호화통신 기반 사이버공격 탐지·대응 기술 개발 필요 o 지능형교통체계에서의 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발을 통한 안전성과 신뢰성이 보장된 지능형교통체계 구축 필요
사업목표	o 차세대 지능형교통체계 환경에서의 암호트래픽·악성코드 수집·공유 및 암호화통신 기반 사이버공격 탐지·대응 원천기술 최적화 및 실증
연구개발내용	o 원천기술 연구개발 단계 - 차세대 지능형교통체계(C-ITS)기반 악성·정상행위 암호문·평문 트래픽 수집 - 차세대 지능형교통체계(C-ITS)기반 디바이스·센서 행위정보 수집 - 자동탐지·대응 모델 구축을 위한 차세대 지능형교통체계 트래픽·디바이스 특징 분석기반 데이터셋 구축 o 실증 및 실용화 단계 - 차세대 지능형교통체계(C-ITS)환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화 - 차세대 지능형교통체계의 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증 - 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 - 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력
기대효과	o 차세대 지능형교통체계에 최적화된 암호통신 기반 사이버공격 탐지기술의 핵심 원천기술 확보 o 지능형교통체계의 사이버재난·재해로부터 야기되는 사회적·경제적 혼란 예방 및 재난·재해 복구비용 절감 o 암호통신 기반 사이버공격 탐지·대응 기술 개발 및 적용을 통한 안전성·신뢰성이 보장된 차세대 지능형교통체계의 구축 및 운영
소요예산/기간	115억/ 5년 (*1차년도 데이터 수집장비 및 4차년도 실증·시제품 비용증가 예상분 반영)
중복성 검토	“해당사항 없음”

❑ 세부추진 내용

ㅇ (정보 수집) 차세대 지능형교통체계(C-ITS)기반 악성·정상행위 암호문·평문 트래픽 수집 기술

- C-ITS 환경에서의 암호화 트래픽에 대한 메타정보(평문) 수집 기술 개발

- C-ITS 환경에서의 암호화 트래픽의 악성·공격 행위 수집 기술 개발

- 데이터셋 구축을 위한 복호화기반 평문-암호트래픽 쌍 수집 기술 개발

※ 통합교통정보센터와 차량(OBU)/노변기지국(RSU) 간의 통신 트래픽 수집 등

- C-ITS 환경에서의 암호화 트래픽 기반의 악성코드 행위 정보 수집 기술 개발

<그림 58> 차세대 지능형교통체계 인프라 현황 및 트래픽 수집 방안

ㅇ (정보 수집) 차세대 지능형교통체계(C-ITS)기반 디바이스·센서 정보 수집 기술

- C-ITS 인프라(노변기지국 등)의 각종 디바이스·센서들의 정보 및 디바이스 내 동작 중인 프로세스 정보들의 주기적인 수집 기술 개발

- C-ITS 인프라(노변기지국 등)의 디바이스·센서 비정상행위 정보 수집

기술 개발

※ 디바이스·센서 모니터링을 통한 비인가 접근 및 비정상 프로세스 실행 등의 Blacklist·Whitelist 구축 기술 개발

ㅇ **(정보 수집) 자동탐지·대응 모델 구축을 위한 차세대 지능형교통체계 트래픽·디바이스 특징 분석기반 데이터셋 구축**

- 지능형교통체계 트래픽 수집 데이터 특징 분석을 통한 데이터 정규화 기술 개발

- 자동 탐지·대응 모델 개발을 위한 수집데이터의 학습·검증 데이터셋화 기술 개발

ㅇ **(최적화·실증) 차세대 지능형교통체계(C-ITS)환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 최적화 기술 개발**

- C-ITS 환경(시뮬레이션 또는 실환경)에서의 원천기술 테스트 및 성능 최적화 기술 개발

ㅇ **(최적화·실증) 차세대 지능형교통체계의 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증**

- C-ITS 국가 실증 테스트베드(국가교통정보센터, 스마트 City 등) 기반의 실환경 테스트베드를 활용한 탐지 기술의 실증 기술 개발

※ 2개소 이상 상이한 환경의 실증 테스트베드 확보 및 기술 실증·검증

ㅇ **(표준화) 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 기술 개발**

- 악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의

※ 다양한 환경의 서비스 · 인프라에 적용을 위한 행위정보 표준포맷 개발 지원

- 탐지·분석기술 실용·제품화를 위한 암호화 트래픽 전용 표준탐지규칙 개발지원

※ 네트워크에 인입 탐지 · 분석용 H/W를 위한 표준 탐지규칙 정의 지원

ㅇ (공유·협력) 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력

- 협력 플랫폼 활용을 통한 수집데이터·분석기술·실증결과 공유 (전부처 공통)

- 원천기술 실용화 추진을 위한 포괄적 탐지 매커니즘(엔진) 최적화 기술 지원

3 해양수산부

1. 목표 및 연구개발 내용

❑ 연구개발 목표

ㅇ 지능형 해상교통정보서비스(e-Nav) 및 해상무선통신망(LTE-M)의 사이버 재난·재해 예방 및 확산 방지를 위한 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발

❑ 연구개발 내용

ㅇ 원천기술 연구개발 단계

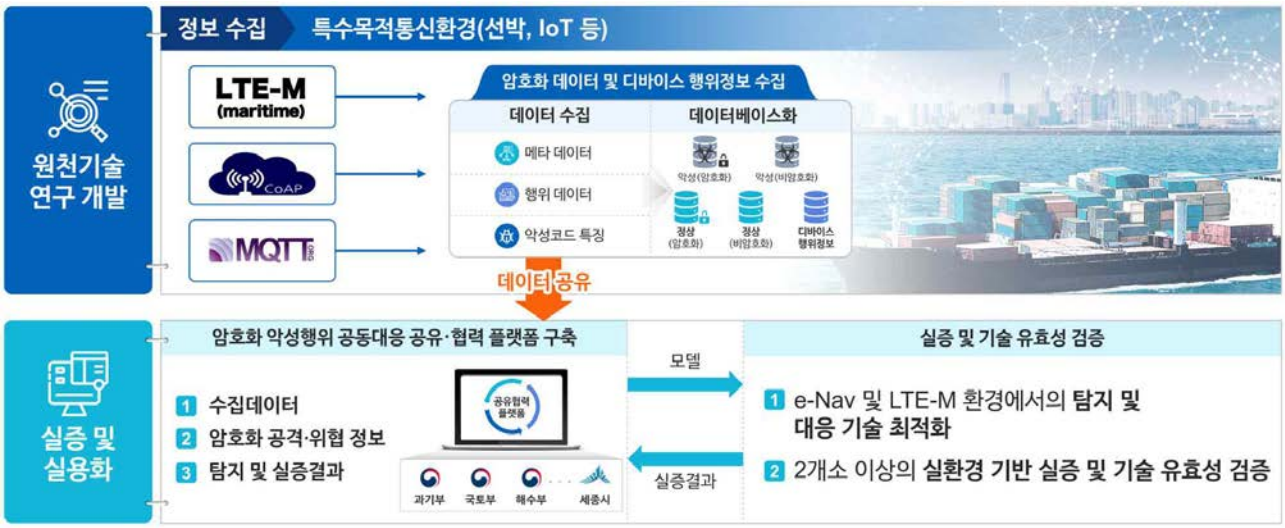
- (정보 수집)해상무선통신망(LTE-M) 환경 악성·정상행위 암호문·평문 트래픽 수집
- (정보 수집)지능형 해상교통정보서비스(e-Nav)환경 디바이스·센서 행위 정보 수집
- (정보 수집)자동탐지·대응 모델 구축을 위한 지능형 해상교통정보서비스 및 해상무선통신망 트래픽·디바이스 특징 분석기반 데이터셋 구축

ㅇ 실증 및 실용화 단계

- (최적화·실증)지능형 해상교통정보서비스(e-Nav) 및 해상무선통신망(LTE-M) 환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화
- (최적화·실증)지능형 해상교통정보서비스(e-Nav) 및 해상무선통신망(LTE-M) 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증

- (표준화) 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화

- (공유·협력) 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력



<그림 59> 해양수산부 연구개발 세부 내용

2. 추진내용

❑ 해양수산부 사업 RFP(안)

주요사업명	지능형 해상교통정보서비스의 사이버재난·재해 예방 및 확산 방지를 위한 해상무선통신망 중심 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발	부처	해양수산부
사업개요	○ 암호화통신 기반 사이버공격으로부터 대국민 공공 서비스·인프라인 지능형 해상교통정보서비스(e-Nav)·해상무선통신망(LTE-M)의 보호를 위한 공격·악성행위 탐지·대응 기술 최적화 및 실증 서비스 개발		
현황 및 필요성	<현황> ○ 최근 낚시 및 레저용 선박에 대한 수요 증가로 인해 해양에서의 활동이 급증, 이에 따른 해양 네트워크 및 데이터 통신에 대한 보안성 강화가 시급한 과제로 대두됨 ○ 기존의 VHF무전기의 거리 및 속도의 한계를 극복하기 위해 LTE기술 기반의 초고속 해상 무선통신망(LTE-M) 및 지능형 해상교통정보서비스를 구축 및 운영 중		

	○ LTE-M은 연안 100Km까지의 서비스를 목표로 개발 및 운영됨에 따라 인접국가(일본, 중국, 북한, 러시아)들과의 전파 중첩이 발생하며, 이로 인해 주요 정보노출, 무선 네트워크 해킹 등의 사이버 위협에 대한 리스크가 매우 높은 상황 ○ 특히, 암호화된 통신을 활용한 사이버공격 발생 시 이에 대한 대응방법이 부재하기에 효과적인 위기대응 수행이 불가한 상황 <필요성> ○ 지능형 해상교통정보서비스의 전자해도, 어선, 운반선, 여객선 등의 무선 통신 디바이스들에서 수집되는 네트워크 트래픽은 매우 광범위한 지역에서 수집되기 때문에 복호화 장비 기반의 대응 체계에서는 트래픽 전송 시간 및 복호화 시간으로 인한 네트워크 지연 현상이 발생하여 원활한 서비스가 불가 ○ 지능형 해상교통정보서비스의 사이버 재난·재해 예방 및 확산 방지를 위해 암호화 통신 기반 사이버공격 탐지·대응 기술 개발 필요 ○ 지능형 해상교통정보서비스에서의 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발을 통한 안전성과 신뢰성이 보장된 지능형교통체계 구축 필요
사업목표	○ 지능형 해상교통정보서비스 환경에서의 암호트래픽/악성코드 수집·공유 및 암호화통신 기반 사이버공격 탐지·대응 원천기술 적용 및 최적화
연구개발내용	○ 원천기술 연구개발 단계 - 해상무선통신망(LTE-M) 환경 악성·정상행위 암호문·평문 트래픽 수집 - 지능형 해상교통정보서비스(e-Nav)환경 디바이스·센서 행위정보 수집 - 자동탐지·대응 모델 구축을 위한 지능형 해상교통정보서비스 및 해상무선통신망 트래픽·디바이스 특징 분석기반 데이터셋 구축 ○ 실증 및 실용화 단계 - 지능형 해상교통정보서비스(e-Nav) 및 해상무선통신망(LTE-M) 환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화 - 지능형 해상교통정보서비스(e-Nav) 및 해상무선통신망(LTE-M) 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증 - 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 - 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력
기대효과	○ 지능형 해상교통정보서비스 환경에 최적화된 암호통신 기반 사이버공격 탐지기술의 핵심 원천기술 확보 ○ 지능형 해상교통정보서비스의 사이버재난·재해로부터 야기되는 사회적·경제적 혼란 예방 및 재난·재해 복구비용 절감 (어업인, 낚시 스포츠인, 해상물류·운송 등) ○ 암호통신 기반 사이버공격 탐지·대응 기술 개발 및 적용을 통한 안전성·신뢰성이 보장된 지능형 해상교통정보서비스 구축 및 운영
소요예산/기간	115억/ 5년 (*1차년도 데이터 수집장비 및 4차년도 실증·시제품 비용증가 예상분 반영)
중복성 검토	해당사항 없음

❑ 세부추진 내용

○ (정보 수집)해상무선통신망(LTE-M) 환경 기반 악성·정상행위 암호문·평문 트래픽 수집 기술

- LTE-M 환경에서의 암호화 트래픽에 대한 메타정보(평문) 수집 기술 개발

- LTE-M 환경에서의 암호화 트래픽의 악성·공격 행위 수집 기술 개발

※ 국가 해상무선통신망 통신센터 및 기지국 인프라 활용 고려

- 데이터셋 구축을 위한 복호화기반 평문-암호트래픽 쌍 수집 기술 개발

- LTE-M 환경에서의 암호화 트래픽 기반의 악성코드 행위 정보 수집 기술 개발

<그림 60> 지능형 해상교통정보서비스 인프라 현황

○ (정보 수집)지능형 해상교통정보서비스(e-Nav) 기반 디바이스·센서 정보 수집 기술

- e-Nav 서비스 및 LTE-M 통신 인프라의 각종 디바이스·센서들의 정보 및 디바이스 내 동작 중인 프로세스 정보들의 주기적인 수집 기술 개발

- e-Nav 서비스 및 LTE-M 통신 인프라의 디바이스·센서 비정상행위 정보 수집 기술 개발

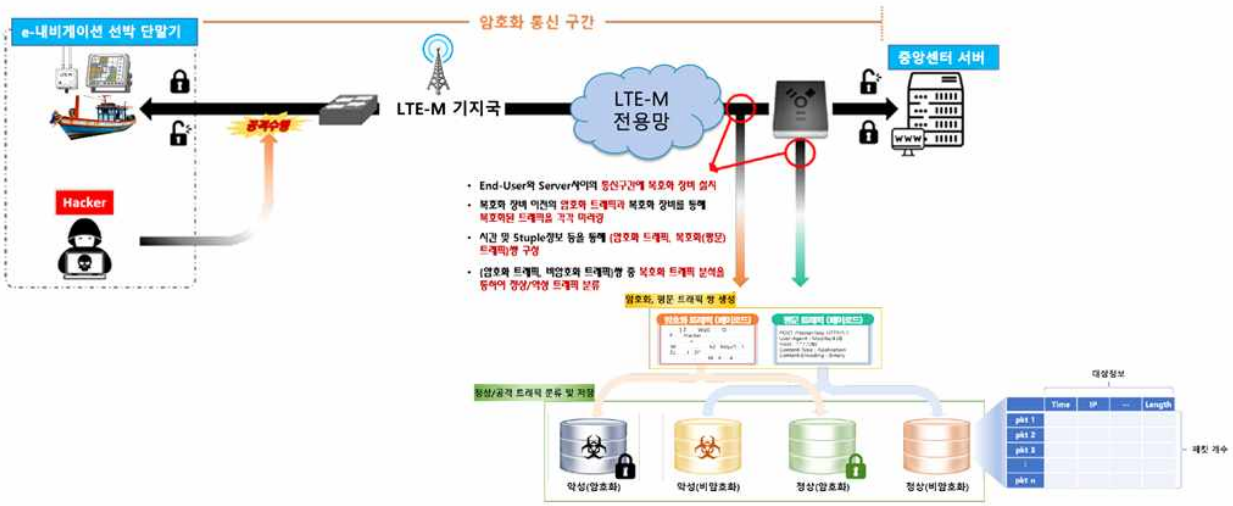
※ 국가 관공선, 해양 실습선(한국해양대,한국선급 등)의 디바이스 · 센서 활용 고려

※ 디바이스 · 센서 모니터링을 통한 비인가 접근 및 비정상 프로세스 실행 등의 Blacklist · Whitelist 구축 기술 개발

ㅇ **(정보 수집)자동탐지·대응 모델 구축을 위한 차세대 지능형 해상교통정보서비스 트래픽·디바이스 특징 분석기반 데이터셋 구축**

- 지능형 해상교통정보서비스 트래픽 수집 데이터 특징 분석을 통한 데이터 정규화 기술 개발

- 자동 탐지·대응 모델 개발을 위한 수집데이터의 학습·검증 데이터셋화 기술 개발



<그림 61> 지능형 해상교통정보서비스 환경에서의 공격 및 정상 트래픽 수집 방안

ㅇ **(최적화·실증)e-Nav 서비스 및 LTE-M 인프라 환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 최적화 기술 개발**

- e-Nav 서비스 및 LTE-M 인프라 환경(시뮬레이션 또는 실환경)에서의

원천기술 테스트 및 성능 최적화 기술 개발

ㅇ **(최적화·실증)e-Nav 서비스 및 LTE-M 인프라의 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증**

- LTE-M 실운용 환경(해수부 중앙센터, 해상통신 제1센터 등) 기반의 실환경 테스트베드를 활용한 탐지 기술의 실증 기술 개발

※ 2개소 이상 상이한 환경의 실증 테스트베드 확보 및 기술 실증·검증

ㅇ **(표준화)위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 기술 개발**

- 악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의

※ 다양한 환경의 서비스·인프라에 적용을 위한 행위정보 표준포맷 개발 지원

- 탐지·분석기술 실용·제품화를 위한 암호화 트래픽 전용 표준탐지규칙 개발지원

※ 네트워크에 인입 탐지·분석용 H/W를 위한 표준 탐지규칙 정의 지원

ㅇ **(공유·협력)암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력**

- 협력 플랫폼 활용을 통한 수집데이터·분석기술·실증결과 공유 (전부처 공통)

- 원천기술 실용화 추진을 위한 포괄적 탐지 매커니즘(엔진) 최적화 기술 지원

4 세종특별자치시

1. 목표 및 연구개발 내용

❑ 연구개발 목표

ㅇ **스마트 City 대국민 공공 교통·치안·생활 서비스·인프라의 사이버재난·재해 예방 및 확산 방지를 위한 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발**

※ 교통(대중교통, 신호체계 등), 치안(방범CCTV, 가로등 등), 생활(교통상황, 병원 · 약국 정보 등)

❑ 연구개발 내용

ㅇ **원천기술 연구개발 단계**

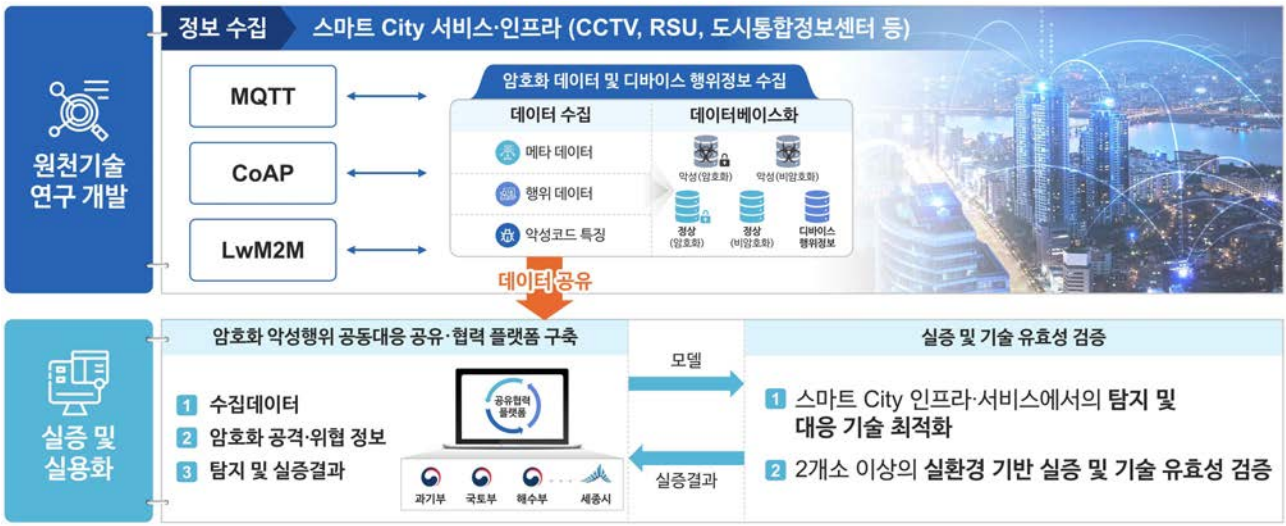
- (정보 수집)스마트 City 교통·치안·생활 서비스·인프라 기반 악성·정상행위 암호문·평문 트래픽 수집
- (정보 수집)스마트 City 교통·치안·생활 서비스·인프라 기반 디바이스·센서 행위정보 수집
- (정보 수집)자동탐지·대응 모델 구축을 위한 스마트 City 교통·치안·생활 서비스·인프라 트래픽·디바이스 특징 분석기반 데이터셋 구축

ㅇ **실증 및 실용화 단계**

- (최적화·실증)스마트 City 교통·치안·생활 서비스·인프라환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화
- (최적화·실증)스마트 City 실환경 테스트베드를 활용한 실증 및 기술

유효성 검증

- (표준화) 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화
- (공유·협력) 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력



<그림 62> 세종특별자치시 연구개발 세부 내용

2. 추진내용

❑ 세종특별자치시 사업 RFP(안)

주요사업명	스마트 City 사이버재난·재해 예방 및 확산 방지를 위한 암호화통신 기반 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발	부처	세종특별자치시
사업개요	○ 암호화통신 기반 사이버공격으로부터 대국민 공공 서비스·인프라인 스마트 City 교통·치안·생활 서비스·인프라의 보호를 위한 공격·악성행위 탐지·대응 기술 최적화 및 실증 서비스 개발		
현황 및 필요성	<현황> ○ 최근 정부 4차 산업혁명 위원회에서 '도시혁신 및 미래 성장 동력 창출을 위한 스마트 City 추진전략'을 발표, 인공지능, 빅데이터, 클라우드, 5G등의 기술을 활용한 도시문제 해결 및 편의성 향상을 목적으로 하는 서비스들이 개발 및 운영 중 ○ 스마트 City는 빅데이터, 인공지능, IoT등 ICT기술이 종합적으로 적용되어 만들어지므로 개별기술에서 발생할 수 있는 보안 위협 및 취약점들이 발생 가능함		

	ㅇ 이중에서도 암호화통신을 활용한 사이버 공격들은 탐지 자체가 어려워 월패드, 스마트 가전, CCTV, 빌딩제어 시스템 해킹 등 보안사고를 유발하고 있음 ㅇ 스마트 City 인프라들은 모두 독립된 네트워크를 사용 중이므로 모든 네트워크 환경에 암호화 트래픽 복호화(가시화) 장비를 설치 및 대응하는 것은 경제적인 어려움이 있음 <필요성> ㅇ CCTV, 교통정보수집, 의료, 도시정보 등의 스마트 City 서비스·인프라를 구축하는데 사용되는 IoT장비들의 사이버 침해 예방 및 사고 확산 방지를 위해 암호화통신 기반 사이버공격 탐지·대응 기술 개발 필요 ㅇ 스마트 City 서비스·인프라에서의 사이버공격 탐지·대응 기술 최적화 및 실증 서비스 개발을 통한 안전성과 신뢰성이 보장된 스마트 City 구축 및 운영 필요
사업목표	ㅇ 스마트 City 서비스·인프라에서의 암호트래픽/악성코드 수집·공유 및 암호화통신 기반 사이버공격 탐지·대응 원천기술 적용 및 최적화
연구개발내용	ㅇ 원천기술 연구개발 단계 - 스마트 City 교통·치안·생활 서비스·인프라 기반 악성·정상행위 암호문·평문 트래픽 수집 - 스마트 City 교통·치안·생활 서비스·인프라 기반 디바이스·센서 행위정보 수집 - 자동탐지·대응 모델 구축을 위한 스마트 City 교통·치안·생활 서비스·인프라 트래픽·디바이스 특징 분석기반 데이터셋 구축 ㅇ 실증 및 실용화 단계 - 스마트 City 교통·치안·생활 서비스·인프라환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 기술 최적화 - 스마트 City 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증 - 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 - 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력
기대효과	ㅇ 스마트 City 서비스·인프라 환경에 최적화된 암호통신 기반 사이버공격 탐지기술의 핵심 원천기술 확보 ㅇ 스마트 City 서비스·인프라의 사이버재난·재해로부터 야기되는 사회적·경제적 혼란 예방 및 재난·재해 복구비용 절감 ㅇ 암호통신 기반 사이버공격 탐지·대응 기술 개발 및 적용을 통한 안전성·신뢰성이 보장된 스마트 City 서비스·인프라 구축 및 운영
소요예산/기간	65억/ 5년 (스마트 City 기구축 IoT 서비스·인프라 활용으로 장비구축 등 예산 절감)
중복성 검토	해당사항 없음

❑ 세부추진 내용

○ (정보 수집)스마트 City 교통·치안·생활 서비스·인프라환경 기반 악성·정상행위 암호문·평문 트래픽 수집 기술

- 스마트 City 교통·치안·생활 서비스·인프라 환경에서의 암호화 트래픽에 대한 메타정보(평문) 수집 기술 개발

- 스마트 City 교통·치안·생활 서비스·인프라 환경에서의 암호화 트래픽의 악성·공격 행위 수집 기술 개발

※ 세종스마트 City 국가시범단지(5-1생활권) 및 도시통합정보센터 인프라 활용 고려

- 데이터셋 구축을 위한 복호화기반 평문-암호트래픽 쌍 수집 기술 개발

- 스마트 City 교통·치안·생활 서비스·인프라 환경에서의 암호화 트래픽 기반의 악성코드 행위 정보 수집 기술 개발

<그림 63> 스마트 City 서비스 · 인프라 현황 및
도시통합정보센터를 통한 트래픽 수집 방안

○ (정보 수집)스마트 City 교통·치안·생활 인프라·서비스의 대규모 IoT 네트워크 기반 디바이스·센서 정보 수집 기술

- 스마트 City 인프라의 각종 디바이스·센서들의 정보 및 디바이스 내 동작

중인 프로세스 정보들의 주기적인 수집 기술 개발

- 스마트 City 인프라의 디바이스·센서 비정상행위 정보 수집 기술 개발

※ 스마트폴(Smart pole)에 설치된 교통 · 치안 · 환경 등의 각종 디바이스 · 센서 활용

※ 미세먼지, 기온, 습도 센서 등, CCTV, 신호등, LoRa통신 단말기 등

ㅇ (정보 수집)자동탐지·대응 모델 구축을 위한 스마트 City 인프라·서비스 트래픽·디바이스 특징 분석기반 데이터셋 구축

- 스마트 City 대규모 IoT 네트워크 트래픽 및 지능형 서비스* 수집 데이터 특징 분석을 통한 데이터 정규화 기술 개발

* 세종엔, 셔클, 어울링, 세종안심이 등 다양한 스마트 City 기반 서비스

- 자동 탐지·대응 모델 개발을 위한 수집데이터의 학습·검증 데이터셋화 기술 개발

ㅇ (최적화·실증) 스마트 City 교통·치안·생활 인프라·서비스 환경 행위기반 암호화 트래픽 보안관제 탐지 및 대응 최적화 기술 개발

- 스마트 City 도시통합정보센터 인프라 환경(시뮬레이션 또는 실환경)에서의 원천기술 테스트 및 성능 최적화 기술 개발

ㅇ (최적화·실증) 스마트 City 교통·치안·생활 인프라·서비스 실환경 테스트베드를 활용한 실증 및 기술 유효성 검증

- 스마트 City 서비스·인프라 실운용 환경(도시통합정보센터 등) 기반의 실환경 테스트베드를 활용한 탐지 기술의 실증 기술 개발

※ 2개소 이상 상이한 환경의 실증 테스트베드 확보 및 기술 실증 · 검증

ㅇ (표준화) 위협 확산 방지 및 대응 방안 공유를 위한 분석정보 표준화 기술 개발

- 악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 정의

※ 다양한 환경의 서비스 · 인프라에 적용을 위한 행위정보 표준포맷 개발 지원

- 탐지·분석기술 실용·제품화를 위한 암호화 트래픽 전용 표준탐지규칙 개발지원

※ 네트워크에 인입 탐지 · 분석용 H/W를 위한 표준 탐지규칙 정의 지원

ㅇ (공유·협력) 암호화 공격·위협정보의 공유 및 공동 대응을 위한 플랫폼 활용 정보 공유 및 협력

- 협력 플랫폼 활용을 통한 수집데이터·분석기술·실증결과 공유 (전부처 공통)

- 원천기술 실용화 추진을 위한 포괄적 탐지 매커니즘(엔진) 최적화 기술 지원

제3장 사업 추진방법

제1절 사업 추진전략

❑ 기존 사업과의 중복성 검토 및 기술개발 차별화 전략

○ 기존기술의 문제점 및 한계점을 면밀히 분석하여 제안 사업의 기술적 차별화 전략 수립 및 핵심 원천기술 개발 추진

- 악성·공격 행위 탐지에 관한 기존사업과 제안사업의 정부 R&D사업, 산업계·연구계 기술동향 비교 분석

[표 20] 기존사업과 제안사업의 정부정책 및 산 · 학 · 연 측면의 차별점 분석

구분		기존 사업	제안 사업
정부 사업		·**평문데이터**에 대한 보안관제 기술 개발 ·**암호화데이터 복호화(평문)** 및 잠재적 위협 탐지 기술 개발 ·초연결 기반 ICT 서비스 **보안 정책수립 및 적용**, **인증기술** 개발 중심	·**암호화데이터**에 대한 보안관제 기술 개발 ·**암호통신 기반** 다양한 ICT 서비스에서 발생하는 **사이버위협 탐지 · 대응 기술** 개발 ·**비복호기반** 공격 · 악성 **'행위 분석'** 연구개발 중심
산업계		·**암호화 트래픽의 복호화**를 통한 사이버공격 탐지 솔루션 개발 * 복호화에 따른 네트워크/시스템 성능이슈, 개인정보/사생활 침해, 사용자 거부감 등 문제 발생	·**암호화 트래픽의 비복호화**를 기반으로 사이버공격 탐지 기술 개발 * 암호화된 트래픽 자체의 **행위분석**을 통해 **정상행위와 비정상(공격행위) 탐지**
연구계	국내	·AI/XAI 기반 기술개발 동향조사 및 **선행연구 수행 단계** * KISTI, 고려대학교 등	·**알려진/잠재적 모든 사이버공격을 대상**으로 탐지 가능한 기술 개발 추진 * (알려진 공격) 공개된 위협 인텔리전스 및 AI 데이터 활용 * (잠재적 공격) 부처별 스마트 서비스의 네트워크 트래픽, 디바이스/응용프로그램 정보 등을 활용하여 비정상행위 탐지 ·**IoT, 5G 등 초연결 기반 스마트 서비스**를 포함한 모든 네트워크/시스템의 암호화 트래픽을 활용 * 각 부처의 스마트 서비스 환경에서 수집한 데이터, 디바이스, 응용프로그램 등에 대한 공유 · 협력
	국외	·ETA 중심의 암호화된 트래픽분석 연구 수행 * CISCO, Juniper에서 전용장비 판매 및 기술고도화 진행 중 ·응용프로그램 분류, 일부 공격(Bruteforce, 봇넷 등) 탐지만 가능 ·일반 인터넷 및 시스템/서비스에서 발생하는 암호화 트래픽을 활용	

※ 비복호화 기반의 악성 암호트래픽 탐지 원천기술 연구를 통한 實보안관제에 적용 가능한 기술 확보 추진

※ 원활한 기술연계를 위한 공격 · 악성행위 모델링 및 표준화 기술 확보 추진

ㅇ **旣 사업들은 개인정보 유·노출, 한정된 복호화 대상, 대용량·초고속 네트워크 환경에서의 네트워크 병목현상 유발 등의 현실적인 문제점으로 인해 보안관제에 적용하는 것이 불가능하므로, 본 사업에서는 비복호화 기반 원천기술 연구에 초점을 맞춤**

- 복호화의 경우 현재 1~10Gbps 수준의 환경을 지원하고 있으며, 물리적·비용적으로 100Gbps 이상의 통신을 수행 중인 대국민 서비스·인프라 전체 환경에 복호화 장비 설치 불가

- 기존사업과의 연계 및 암호화 기반 공격·악성 트래픽 원천 행위 분석을 위해 복호화 수행을 통한 {암호문, 평문} 형태의 공격행위 연구 데이터 셋 구축 추진

※ 참여부처별 다양한 환경의 서비스 · 인프라 테스트베드 상에 복호화(가시화) 장비 설치 및 연구 데이터 수집 예정

❑ **다부처 공동 사업수행 전략**

ㅇ **공동기획연구 목표 달성을 위한 기술정보 수집, 전문가 확보, 관련부처 협의 및 공청회 개최 등 추진 전략 수립**

- 부처별 서비스·인프라 운영기관 및 규제 전문가, 원천기술 전문기관 및 전문가 자문단 등과 주기적인 워크숍, 자문회의 및 공청회 개최

- IoT, 5G 등 초연결 기반 공공 스마트 서비스를 대상으로 사회 전 방위적 발생 가능한 사이버 보안사고 예방·대응 및 협력 체계 마련

ㅇ **성과 관리 및 과제평가 방안**

- 부처간 공통목표 해결을 위한 연구개발·성과관리를 수행하므로, 부처·실무수행 기관 등과 긴밀한 협력 및 주기적인 사업성과 공유·논의

※ 참여부처 이외에 공공 서비스 · 인프라를 운영하는 기간시설 부처 · 기관을 수요처로 섭외하여 실제 수요 환경에서의 사업성과 유효성 검토 · 관리

- 범국가적 보안체계 향상을 위한 핵심 원천기술 개발을 수행하므로, 산업계·학계·연구계 등 기술분야, 법·제도 등 규제분야, 국가·공공·지차체 등 행정분야의 각계 전문가 및 수요자의 정성적·정량적 평가 수행

※ 지속적인 국내외 선도기술 현황 조사를 통하여 정밀하고 현실적인 범위에서의 국내외 최고수준 성능지표 및 목표치 설정

※ 사이버안전 유관기관(국가정보원, 국가사이버안보센터, 부처별 사이버안전센터 등)과 협조 추진

ㅇ 규제 이슈 및 대응방안

- 통신트래픽 분석을 통한 보안관제 기술 개발을 목표로 하므로, '국가 정보보안 기본지침'을 중심으로 각 부처별 규정 준수 필요

※ 개인정보 및 민감정보가 포함된 데이터 수집 · 처리를 수행하므로 개인정보보호법, 정보통신망법 등 '데이터 3법' 준용 예정

※ 정보시스템 구축 시 기본지침에 따라 수행하며, 관리적 · 기술적 · 물리적 보호 조치를 포함한 종합적 관리체계(이하 '정보보호 관리체계') 인증 준수

- 방송통신위원회의 '정보보호 및 개인정보 관리체계 인증' 제도 및 데이터 보안관리를 위한 '정보통신단체표준' 지침을 준수하여 데이터 수집·처리 예정

- 각 부처별 기본법 검토 및 유의사항, 법적 근거 미비사항 확보 등 부처간 지속적인 협력·논의 추진

※ 과기정통부(정보보안기본지침 등), 국토부(국가통합교통체계효율화법 등), 해수부(지능형해상교통정보법 등), 세종시(스마트도시법 등) 등의 검토 및 상호 협력

- 기술규제툴킷 작성 및 검토 컨설팅(KISTEP, 중소벤처기업연구원)을 통한 규제 이슈 및 대응 방안의 면밀한 검토 수행

[표 21] 규제 이슈 검토 및 애로사항별 해결전략

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
네트워크 행위 빅데이터 구축 (정상/공격 행위의 암호화/평문 트래픽 수집)	레거시 인터넷망 통신 트래픽 수집	5~7	법령·고시	국가 정보보안 기본지침 - 제72조(빅데이터 보안) - 제134조(공격정보 탐지·수집)	-	- 지침에 따라 정보시스템 구축 및 운영 예정
				과학기술정보통신부 정보보안 기본지침 - 제72조(빅데이터 보안) - 제112조(공격정보 탐지·수집)		
				국가 정보보안 기본지침 - 제131조(보안관제센터 설치·운영)	- 보안관제 설치·운영 시 국가보안관제 체계와의 연계만 가능	- 다부처 공동기획연구와 관련된 민간 분야 인프라 트래픽 수집 시 해당 법령 확대 적용 여부 검토 필요
				과학기술정보통신부 정보보안 기본지침 - 제109조(보안관제센터 설치·운영)		
				행정안전부 개인정보보호위원회 개인정보보호법 - 제16조 (개인정보의 수집 제한)	- 트래픽 수집 중 불가피하게 수집되는 개인정보를 처리 및 보관하기 위한 적절한 법령 및 고시 필요	- 정보주체의 동의가 필요없는 비식별화 처리 후의 데이터 수집 예정 - 연구목적으로 활용할 수 있도록 비식별화 처리된 네트워크 데이터 사용
				과학기술정보통신부, 방송통신위원회 정보통신망법 - 제47조(정보보호 관리체계의 인증)	-	- 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계") 인증 준수
			표준·인증·규격	방송통신위원회 - 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) (https://isms.kisa.or.kr/main/ispims/intro/) - 정보통신망법 제47조 - 정보통신망법 시행령 제47조~54조 - 정보통신망법 시행규칙 제3조 - 개인정보보호법 제32조의2 - 개인정보보호법 시행령 제32조의2~제34조의8 - 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시	-	- ISMS-P 인증제도를 준수하여 트래픽 수집 예정
				정보통신기술협회 정보통신단체표준 - 데이터 생애주기 기반 빅데이터 도입 및 활용 지침(TTAK.KO-10.0900)	- 데이터 보안 관리 기술 고려 - 개인정보보호 처리 기술 고려 - 빅데이터 품질 관리 고려	- 데이터 보안관리의 표준지침을 준수하여 진행

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
			국내외 인허가	없음 (잠재적 가능성 존재)	- 현재 특별히 필요한 국내외 인허가 사항은 없으나, 다부처 사업 특성상 공동 정보 수집 및 활용에 대한 잠재적인 제약/법령 등의 제고 필요	- 다부처간 트래픽 수집 공유/활용이 가능하도록 (잠재적) 법/제도 및 규제 지속 검토
	스마트 City 센서 기반 통신 트래픽 수집	5~7	법령·고시	국토교통부 스마트도시 조성 및 산업진흥 등에 관한 법률 - 제21조(개인정보 보호)	- 개인정보의 수집 및 이용 등에 대해 관계 법령에 따라 적법하고 안전하게 취급 필요	스마트도시 조성 및 산업진흥 등에 관한 법률 제37조(익명처리된 개인정보의 활용에 대한 다른 법령의 배제) - 익명처리된 개인정보 사용 예정이므로 개인정보 보호법의 적용을 받지 않음
				행정안전부 개인정보보호위원회 개인정보보호법 - 제15조(개인정보의 수집·이용) - 제16조(개인정보의 수집 제한) - 제19조(개인정보를 제공받은 자의 이용·제공 제한)	- 개인정보 수집은 정보주체의 동의를 받거나 기타 특수한 상황에서만 가능	개인정보 보호법 제28조의2(가명정보의 처리 등) - 과학적 연구를 위하여 가명정보 사용 예정이므로 정보주체의 동의 없이 사용가능 자율주행자동차 상용화 촉진 및 지원에 관한 법률 제20조(익명처리된 개인정보 등의 활용에 대한 다른 법령의 배제) - 익명처리된 개인정보 사용 예정이므로 개인정보 보호법의 적용을 받지 않음
				행정안전부 개인정보보호위원회 개인정보보호법 - 제25조 (영상정보처리기기의 설치·운영 제한) - 제28조의7(적용범위)	- 영상정보처리기기 관련 트래픽 수집 및 활용을 허가받을 수 있는 항목이 존재하지 않음 (가명정보 활용 시 허가되는 대상이 아님)	- 영상정보처리기기의 트래픽 수집 및 활용이 관계 법령 위반이 되지 않도록 법적 근거 마련 필요 - 영상정보처리기기의 데이터 유형(이미지, 영상 등)이 개인정보보호법의 영향을 받는지 여부 확인 필요
				방송통신위원회 위치정보법 - 제15조(위치정보의 수집 등의 금지) - 제18조(개인위치정보의 수집)	- 개인위치정보 수집, 이용, 제공 시 개인위치정보주체의 동의 및 이용약관 명시 필수	위치정보의 보호 및 이용 등에 관한 법률 제21조(개인위치정보 등의 이용·제공의 제한 등) - 학술연구를 위하여 특정 개인을 알아볼 수 없는 형태로 가공된 데이터 사용 예정이므로 주체의 동의 없이 사용가능
				법무부, 과학기술정보통신부 통신비밀보호법 - 제3조(통신 및 대화비밀의 보호) - 제14조(타인의 대화비밀 침해금지)	- 암호화된 통신데이터의 수집 및 활용에 대한 법/제도 미비 (잠재적 문제 발생 소지 有)	- 암호화된 통신데이터의 수집 및 활용이 관계 법령에 위반되지 않도록 법적 근거 마련 필요

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
				과학기술정보통신부, 방송통신위원회 정보통신망법 - 제48조(정보통신망 침해행위 등의 금지)	- 데이터 수집을 위한 센서 설치는 정보통신망의 접근 권한을 넘는 침입 행위가 될 가능성 존재	- 데이터 수집을 위한 센서 설치가 관계 법령 위반이 되지 않도록 공공 분야 보안관제 체계에서 접근 또는 추가적인 법적 근거 마련 필요
	스마트 교통(C-ITS) 인프라 통신시설 기반 트래픽 수집	5~7	법령·고시	행정안전부 개인정보보호위원회 개인정보보호법 - 제15조(개인정보의 수집·이용) - 제16조 (개인정보의 수집 제한)	- 트래픽 수집 중 불가피하게 수집되는 개인정보를 처리 및 보관하기 위한 적절한 법령 및 고시 필요	- 정보주체의 동의가 필요없는 비식별화 처리 후의 데이터 수집 예정 - 연구목적으로 활용할 수 있도록 비식별화 처리된 네트워크 데이터 사용
				방송통신위원회 위치정보법 - 제15조(위치정보의 수집 등의 금지) - 제16조(위치정보의 보호조치 등) - 제17조(위치정보의 누설 등의 금지) - 제17조의2 (개인위치정보주체에 대한 위치정보 처리 고지 등) - 제18조(개인위치정보의 수집) - 제21조(개인위치정보 등의 이용・제공의 제한 등)	- 자동차, RSU 등으로부터 수집되는 위치정보를 처리 및 보관하기 위한 적절한 법령 및 고시 필요	- 위치정보의 유출·오용 및 남용으로부터 사생활 보호를 위한 위치정보의 안전한 활용 조치 및 이용환경 구축 예정이며, 제16조에 따라 사전 동의를 받고 진행 예정
				과학기술정보통신부 정보통신공사업법 시행령(정보설비 공사)	-	-
				국가정보원 - 국가·공공기관 정보시스템 구축·운영 지침	-	- 가이드를 준수하여 구축 예정
				행정안전부 - 행정기관 및 공공기관 정보시스템 구축·운영 지침	-	- 지침에 따라 정보시스템 구축 및 운영 예정
				국토교통부 국가공간정보기본법 - 제37조(공간정보 등의 침해 또는 훼손 등의 금지)	- 차량 네비게이션 등의 지도(공간정보 데이터) 등의 통신상 트래픽 수집으로 인해 사생활 침해 위험	- 공간정보의 관리기관 승인을 통해 트래픽 수집의 정당성 확보 및 사용목적에 따라 익명처리 후 활용
				국토교통부 국가통합교통체계효율화법 - 제14조(정보통신수단 등을 통한 교통조사)	- 트래픽 수집 시, 해당 법령 제14조제2항에서 휴대전화를 활용한 교통조사 시 사용자 동의 필요	- 트래픽을 휴대전화 대상이 아닌 차량의 통신정보로 한정
				국토교통부	- 교통정보에 대해	- 연구목적의 교통정보

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
				국가통합교통체계효율화법 - 제88조 (지능형교통체계를 활용한 교통정보의 제공 등)	일반인 및 교통정보의 수집·가공 및 제공 등을 업으로 하는 자에 대해서만 제공 명시(규제부재)	수집대상 확대를 위해 사전에 지능형교통체계관리청 및 교통체계지능화사업시행자와 협의
				과학기술정보통신부 통신비밀보호법 - 제3조(통신 및 대화비밀의 보호) - 제14조(타인의 대화비밀 침해금지)	- 통신정보에 대한 수집 및 활용을 법령에서 금지	- 제12조 (통신제한조치로 취득한 자료의 사용제한)에서 제1호의 범죄를 예방(보안사고 예방 등)하기 위해 사용하는 경우에 해당하므로 법령에 대한 해석 확대
			표준·인증·규격	과학기술정보통신부(한국인터넷진흥원) - 정보보호시스템 구축을 위한 실무가이드	-	- 가이드를 준수하여 구축 예정
	LTE-M 인프라 및 활용 선박 통신 트래픽 수집	5~7	법령·고시	해양수산부 지능형해상교통정보법 - 제20조(보호조치) - 제21조(비밀 유지) - 제22조(방해 금지)	-	- 선박 통신 트래픽 수집 시 지능형 해상교통정보서비스에 침해 및 장애가 발생하지 않도록 수집 예정
				해양수산부 지능형해상교통정보법 - 제17조(해상교통정보의 제공 등)	- 학술연구 및 통계작성 등의 목적으로 해상교통정보를 활용 할 수 있지만, 정보제공 수수료 발생 가능	- 공익성 또는 공공사업 목적인 경우에 대한 해당 법·제도 개선 필요
				해양수산부 지능형해상교통정보법 - 제7조(관계 행정기관 등의 해상무선통신망 이용)	- 시행령에 따라 해상무선통신망의 이용 목적/기간, 전송될 정보의 내용/용량과 해상교통정보서비스 제공에 미치는 영향 등 해양수산부장관에게 협의 요청 필요	- 시행령을 준수하여 해상교통정보서비스 트래픽 수집 예정
				방송통신위원회 위치정보법 - 제15조(위치정보의 수집 등의 금지) - 제18조(개인위치정보의 수집)	- 해상무선통신망 LTE-M. 송수신기 기술 요구사항(국내 표준)에 따라 선박에 대한 위치정보를 주기적으로 선박위치정보시스템으로 송신하므로 개인위치정보주체의 동의 및 이용약관 명시 필요	방송통신위원회 위치정보법 제21조(개인위치정보 등의 이용·제공의 제한 등) - 학술연구를 위하여 특정 개인을 알아볼 수 없는 형태로 가공된 데이터 사용 예정이므로 주체의 동의 없이 사용가능
				법무부, 과학기술정보통신부 통신비밀보호법 - 제3조(통신 및 대화비밀의 보호)	- LTE-M 통신 트래픽 수집 및 활용 불가	- 관계법령 확인을 통한 수집/활용 가능성 확인 필요 (개인정보보호법 등) - 연구목적으로 수집 및 활용

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
				- 제14조(타인의 대화비밀 침해금지)		이 가능하도록 통신 트래픽 내 민감정보 비식별화 조치 등 관련 법령을 준수한 방식을 사용하여 데이터 수집 예정
	위협인텔리전스 및 오픈데이터 소스 기반 데이터 수집	5~7	법령·고시	행정안전부 개인정보보호위원회 개인정보보호법 - 제15조(개인정보의 수집·이용) - 제16조 (개인정보의 수집 제한)	- 트래픽 수집 중 불가피하게 수집되는 개인정보를 처리 및 보관하기 위한 적절한 법령 및 고시 필요	- 정보주체의 동의가 필요없는 비식별화 처리 후의 데이터 수집 예정 - 연구목적으로 활용할 수 있도록 비식별화 처리된 네트워크 데이터 사용
			표준·인증·규격	정보통신기술협회 정보통신단체표준 - 데이터 생애주기 기반 빅데이터 도입 및 활용 지침(TTAK.KO-10.0900)	- 데이터 보안 관리 기술 고려 - 개인정보보호 처리 기술 고려 - 빅데이터 품질 관리 고려	- 데이터 보안관리의 표준지침을 준수하여 진행
디바이스 행위 빅데이터 구축 (어플리케이션, 활성화, 게이트웨이 정보 등)	레거시 네트워크 연결 디바이스 및 센서 행위 데이터 수집	5~7	표준·인증·규격	과학기술정보통신부(고시 제2018-66호) - ICT융합품질인증 : 정보통신융합 기술·서비스 등의 품질인증기준	-	- 침해 사고에 대한 원인 분석을 위해 네트워크 트래픽을 수집하고 저장, 보존하는 등의 표준 가이드라인을 준수하여 행위 분석 기술 개발 예정
	스마트 City 활용 디바이스 및 센서 행위 데이터 수집	5~7	법령·고시	법무부, 과학기술정보통신부 통신비밀보호법 - 제3조(통신 및 대화비밀의 보호)	- 통신사실확인자료에 대한 수집 및 활용은 현재 국가안보, 범죄수사를 위한 경우에만 사용이 가능	- 연구를 위한 통신사실확인자료의 수집 및 활용이 관계 법령 위반이 되지 않도록 법적 근거 마련 필요
				과학기술정보통신부, 방송통신위원회 정보통신망법 - 제48조(정보통신망 침해행위 등의 금지)	- 데이터 수집을 위한 센서 설치는 정보통신망의 접근권한을 넘는 침입행위가 될 가능성 존재	- 데이터 수집을 위한 센서 설치가 관계 법령 위반이 되지 않도록 법적 근거 마련 필요
	C-ITS 활용 디바이스 및 센서 행위 데이터 수집	5~7	법령·고시	국토교통부 교통안전법 - 제38조 (교통시설안전진단지침)	- 디바이스 및 센서 행위 데이터 수집을 위한 장치·장비 등에 대한 진단지침 미비(규제미비)	- 국토교통부 발간 자동차 사이버보안 가이드라인 적용 및 국제기준 사이버보안(UNECE-WP29 등) 국내 적용 가능성 확인
	LTE-M 활용 디바이스 및 센서 행위 데이터 수집	5~7	법령·고시	과학기술정보통신부 정보통신기반 보호법 - 제12조(주요정보통신기반시설 침해행위 등의 금지)	- 디바이스 데이터 수집 시 주요정보통신기반시설에 대한 접근 권한을 초과하여 데이터 수집 가능성 존재	- 데이터 수집 단말에 대한 접근통제 및 보안조치를 고려하여 수집 예정
				해양수산부 지능형해상교통정보법 - 제3조(지능형 해상교통정보서비스 단말기)	- 디바이스 데이터 수집 모듈 개발 시 선박안전법 제18조제1항 및 제9항에 따른 형	- 해당 시행규칙을 준수하여 개발 예정

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
					식승인 및 검정을 받아야 함	
			표준·인증·규격	해상무선통신망 LTE-M. 송수신기 기술 요구사항 (TTA) - S/W 관련 요구사항	- LTE-M 망 통신을 위한 전용 단말이 존재하여 기기의존성 및 호환성 문제 발생 가능	- 해당 표준 요구사항을 만족하도록 개발 예정
사용자 및 디바이스 행위 분석 기술 개발 (암호화 트래픽 상의 악성, 정상, 이상 행위 특징 모델링)		5~7	법령·고시	국가정보원 국가정보보안기본지침 - 제2장 <정보화사업 보안> 과학기술정보통신부 정보보안기본지침 - 제85조~88조 <보안성 검토>	-	- 기술 개발 및 설치 시 '기타 외부망(인터넷) 연동이 요구되는 모든 정보화 사업 등'에 해당함으로 사업계획 단계에서 보안성 검토 관련 문서 작성 후 사전에 과학기술정보통신부 또는 국가정보원에 보안성 검토 요청 필요
				과학기술정보통신부 지능정보화 기본법 - 제58조 (정보보호시스템에 관한 기준 고시 등) 과학기술정보통신부 지능정보화 기본법 시행령 - 제51조(정보보호시스템에 관한 기준 고시 등)	-	- CC인증(정보보호제품의 보증수준을 측정 하기위한 공통평가기준)을 준수하여 개발예정
				과학기술정보통신부 정보보호시스템 평가·인증 지침 - 과학기술정보통신부고시 제2017-7호		
				과학기술정보통신부 정보보호시스템 공통평가기준 - 미래창조과학부고시 제2013-51호		
			표준·인증·규격	과학기술정보통신부(고시 제2018-66호) - ICT융합품질인증 : 정보통신융합 기술·서비스 등의 품질인증기준	-	- 침해 사고에 대한 원인 분석을 위해 네트워크 트래픽을 수집하고 저장, 보존하는 등의 표준 가이드라인을 준수하여 행위 분석 기술 개발 예정
				정보통신기술협회 정보통신단체표준 - 사이버 침해 사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구 사항(TTAK.KO-12.0280)	-	-
암호화 트래픽 공격 행위 실시간 자동 탐지 기술 개발		5-6	법령·고시	국가정보원 국가정보보안기본지침 - 제2장 <정보화사업	-	- 기술 개발 및 설치 시 '기타 외부망(인터넷) 연동이 요구되는 모든

연구개발과제		관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module	TRL	구 분	내 용		
(정상, 악성, 이상 행위 분류)			보안> 과학기술정보통신부 정보보안기본지침 - 제85조~88조 <보안성 검토>		정보화 사업 등'에 해당함으로 사업계획 단계에서 보안성 검토 관련 문서 작성 후 사전에 과학기술정보통신부 또는 국가정보원에 보안성 검토 요청 필요
			과학기술정보통신부 지능정보화 기본법 - 제58조 (정보보호시스템에 관한 기준 고시 등) 과학기술정보통신부 지능정보화 기본법 시행령 - 제51조 (정보보호시스템에 관한 기준 고시 등)	-	- CC인증(정보보호제품의 보증수준을 측정 하기위한 공통평가기준)을 준수하여 개발예정
			과학기술정보통신부 정보보호시스템 평가·인증 지침 - 과학기술정보통신부고시 제2017-7호		
			과학기술정보통신부 정보보호시스템 공통평가기준 - 미래창조과학부고시 제2013-51호		
		표준·인증·규격	과학기술정보통신부(고시 제2018-66호) - ICT융합품질인증 : 정보통신융합 기술·서비스 등의 품질인증기준	-	- 침해 사고에 대한 원인 분석을 위해 네트워크 트래픽을 수집하고 저장, 보존하는 등의 표준 가이드라인을 준수하여 행위 분석 기술 개발 예정
			정보통신기술협회 정보통신단체표준 - 사이버 침해 사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구 사항(TTAK.KO-12.0280)	-	-
암호화/평문 트래픽의 네트워크 행위정보 모델링 및 표준화	5~7	법령·고시	국가정보원 국가정보보안기본지침 - 제2장 <정보화사업 보안> 과학기술정보통신부 정보보안기본지침 - 제85조~88조 <보안성 검토>	-	- 기술 개발 및 설치 시 '기타 외부망(인터넷) 연동이 요구되는 모든 정보화 사업 등'에 해당함으로 사업계획 단계에서 보안성 검토 관련 문서 작성 후 사전에 과학기술정보통신부 또는 국가정보원에 보안성 검토 요청 필요
			과학기술정보통신부 지능정보화 기본법 - 제58조(정보보호시스템에	-	- CC인증(정보보호제품의 보증수준을 측정 하기위한 공통평가기준)을 준수하여

연구개발과제		관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module	TRL	구 분	내 용		
			관한 기준 고시 등) 과학기술정보통신부 지능정보화 기본법 시행령 - 제51조(정보보호시스템에 관한 기준 고시 등)		
			과학기술정보통신부 정보보호시스템 평가·인증 지침 - 과학기술정보통신부고시 제2017-7호		개발예정
			과학기술정보통신부 정보보호시스템 공통평가기준 - 미래창조과학부고시 제2013-51호		
		표준·인증·규격	과학기술정보통신부(고시 제2018-66호) - ICT융합품질인증 : 정보통신융합 기술·서비스 등의 품질인증기준	-	- 침해 사고에 대한 원인 분석을 위해 네트워크 트래픽을 수집하고 저장, 보존하는 등의 표준 가이드라인을 준수하여 행위 분석 기술 개발 예정
			정보통신기술협회 정보통신단체표준 - 사이버 침해 사고 분석을 위한 네트워크 데이터 수집 및 보존 도구 요구 사항(TTAK.KO-12.0280)	-	-
암호화 악성행위 정보 공유 및 대응 협력 플랫폼 개발 및 구축	5~7	법령·고시	국가 정보보안 기본지침 - 제146조(정보공유시스템 운영) 1항	- 국가 정보보안 기본지침에 명시된 국가사이버위협정보공유시스템은 국정원만 구축·운영할 수 있으며, 그 밖의 공공부문 정보공유시스템 관련 법령·고시가 존재하지 않음	- 암호화 악성행위 정보 공유 및 대응 협력 플랫폼 개발 및 구축을 위한 별도의 법적 근거 규정 마련 필요
		표준·인증·규격	개인정보보호위원회 개인정보 보호법 - 제15조(개인정보의 수집·이용) - 제16조(개인정보의 수집 제한) - 제19조(개인정보를 제공받은 자의 이용·제공 제한)	- 개인정보 수집은 정보주체의 동의를 받거나 기타 특수한 상황에서만 가능	개인정보보호위원회 개인정보 보호법 - 제28조의2(가명정보의 처리 등) - 과학적 연구를 목적으로 가명정보 사용 예정이므로 정보주체의 동의 없이 사용가능
		국내외 인허가	방송통신위원회 위치정보의 보호 및 이용 등에 관한 법률 - 제15조(위치정보의 수집 등의 금지)	- 개인위치정보 수집, 이용, 제공 시 개인위치정보주체의 동의 및 이용약관 명시 필수	방송통신위원회 위치정보의 보호 및 이용 등에 관한 법률 - 제21조(개인위치정보 등의 이용·제공의 제한 등)

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
				- 제18조(개인위치정보의 수집)		- 학술연구를 목적으로 특정 개인을 알아볼 수 없는 형태로 가공된 데이터 사용 예정이므로 주체의 동의 없이 사용가능
자동화 탐지 기술 최적화 및 실증	레거시 인터넷 환경	5~7	법령·고시	과학기술정보통신부, 방송통신위원회 정보통신망법 - 제45조의2(정보보호 사전점검)	- 정보통신서비스 제공 시 계획 또는 설계에 정보보호에 관한 사항을 고려해야 함	정보통신융합법 제38조의2(실증을 위한 규제특례) - '신규 정보통신융합 사업 시, 해당 기술·서비스에 대한 제한적 시험·기술적 검증을 위해 관련 규제의 전부 또는 일부를 적용하지 않는 실증을 위한 규제특례를 신청할 수 있음'을 활용
	C-ITS 인프라 환경	5~7	법령·고시	국토교통부 국가통합교통체계 효율화법 시행령 - 제68조 2항 4조	-	- 지능형교통체계를 활용하여 교통과 관련된 정보(암호화된 C-ITS관련 정보)를 수집·처리·보관 시 관계 행정기관·공공기관 또는 정부출연기관의 장에게 지능형교통체계와 관련된 정보나 자료의 제공 또는 지원을 요청하여 수행 예정
				국토교통부 국가통합교통체계효율화법 - 제17조의2 (교통빅데이터플랫폼의 구축·운영)	- 국토교통부는 교통빅데이터플랫폼을 구축·운영하면서 데이터 수집·관리할 수 있으나, 개인정보의 경우 포함 불가	- 데이터3법 개정안을 통해 개인정보는 가명정보로 변환하여 활용 가능
				행정안전부 개인정보보호위원회 개인정보보호법 - 제29조(안전조치의무)	- C-ITS 인프라 환경에서 실증 시 개인정보가 부득이하게 포함될 수 있으므로 조치 필요	- 암호화 트래픽 전체에 대한 안전성 확보에 기술적, 관리적, 물리적 조치 수행
			표준·인증·규격	IEEE X.1372 IEEE 1609.2	-	- X.1372에 정의된 차량통신에서의 메시지 암호화 방법에 따라 암호화된 트래픽을 수집 - RSU의 보안요구사항을 준용하여 암호화 트래픽 수집
				기타	-	- 국내 자율협력주행산업발전협의회의 보안분과위원회를 통해 안전한 C-ITS환경 구축을 위한 보안관제 방법 및 체계 수립
				국토교통부 - 자동차 사이버보안 가이드라인	-	- 가이드를 준수하여 구축 예정
				한국인터넷진흥원 - 스마트교통 사이버보안 가이드		

연구개발과제			관련 기술규제		애로사항	해결전략
연구 핵심 프로세스 or Module		TRL	구 분	내 용		
			국내외 인허가	- 국토교통부 및 유관부처(도로교통공사 등) 협력	-	- 국토교통부 및 유관부처(도로교통공사 등)와 협력하여 C-ITS에서 발생하는 암호화 통신 수집 및 활용에 대한 인허가 필요
	LTE-M 네트워크 환경	5~7	법령·고시	과학기술정보통신부 지능정보화 기본법 - 지능정보화 기본법 제57조(정보보호 시책의 마련 등)	-	- 자동화 탐지기술 실증 중 탐지정보의 수요기관 에의 제공 과정에서 자동화 탐지기술의 안전을 도모할 수 있도록 관련 지침을 준수하여 구축 예정
	스마트 City IoT 네트워크 환경	5~7	법령·고시	국토교통부 스마트도시 조성 및 산업진흥 등에 관한 법률 - 제49조의2(규제의 신속확인)	-	- 실증사업을 위해 개선이 필요한 규제에 대해 스마트 City 규제 샌드박스 제도의 '스마트실증사업'을 통해 해소 가능

❑ 참여 부처 및 기관, 전문가 자문단 협의 내용

ㅇ 부처(과기정통부, 국토부, 해수부, 세종시) 참여 협의 및 진행상황 논의

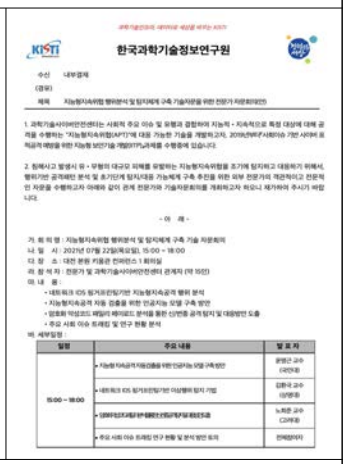
- 각 부처별 사전·중간·최종 협의를 포함한 15회 이상 관련 내용 공유 및 협의 수행

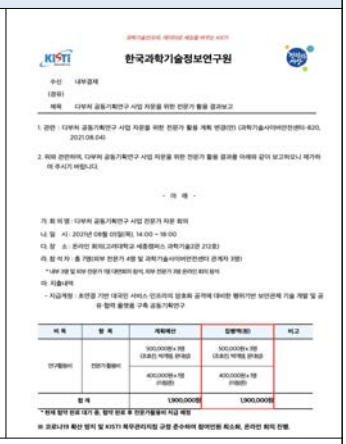
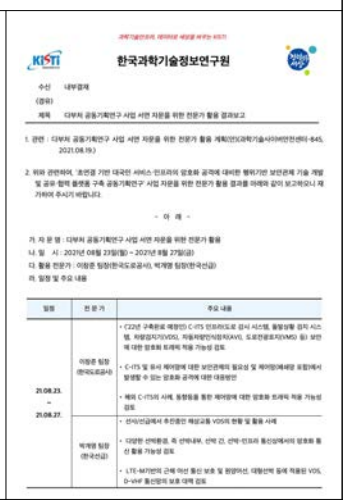
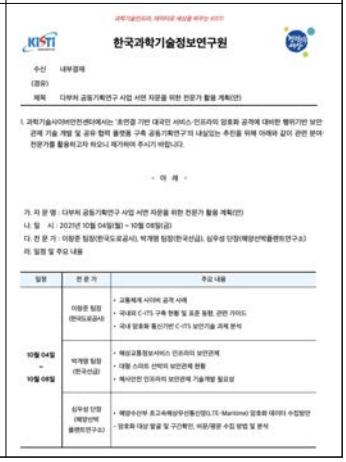
ㅇ 전문가 자문단 및 관계 기관 담당자를 통한 기술적 타당성 검토 및 연구계획 수립

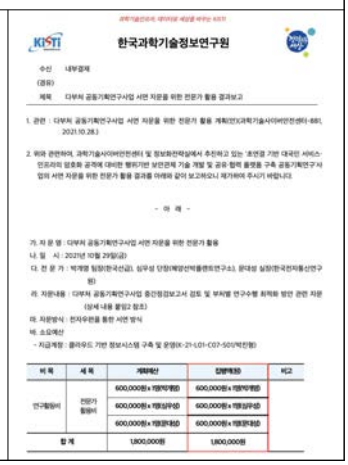
- 오프라인·온라인 회의 및 서면자문을 포함한 10회 이상 면밀한 관련내용 검토

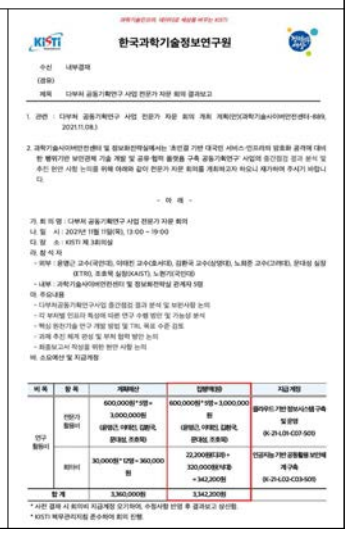
[표 22] 참여 부처 및 기관, 전문가 자문단 협의 현황

협의 기관 (날짜)	협의 및 자문 내용
과학기술정보통신부 (21.05.03)	○ 주요 협의자 – 과기정통부 정보보호담당관실 최준순 사무관, 박순재 사무관, 유지형 주무관 – KISTI 송중석 센터장, 김규일 팀장, 이준 선임 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 추진 가능여부 확인 – 공동기획연구 제안서 내용 검토 – 정보보호담당관실에서 정보보호기획과로 이관 추진

협의 기관 (날짜)	협의 및 자문 내용
과학기술 정보통신부 (21.05.06)	○ 주요 협의자 – 과기정통부 정보보호기획과 박태성 사무관, 배영준 주무관 – 정보통신기획평가원 정현철 차세대보안PM, 보안블록체인기획팀 박인성 팀장 – KISTI 송중석 센터장, 김규일 팀장, 이준 선임 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 추진 가능여부 확인 – 공동기획연구 제안서 내용 타당성 검토 – 과학기술정보통신부 기획연구 제안 승인 – 관련 부처 및 기관 선정, 향후 추진 방향 논의
해양 수산부 (21.07.19)	○ 주요 협의자 – 해양수산부 첨단해양교통관리팀 홍순배 팀장, 최은진 서기관, 이치경 사무관, 한성의 주무관 – 해양선박플랜트연구소 심우성 단장 – KISTI 송중석 센터장, 이준 선임, 고영민 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 참여여부 타진 – 공동기획연구 제안서 내용 공유 및 타당성 검토 – 해양수산부 적극 참여 및 지원 확약
전문가 자문단 (KISTI, 21.07.22)	○ 주요 협의자 – 국민대 윤명근 교수, 호서대 이태진 교수, 고려대 노희준 교수, 상명대 김환국 교수 – KISTI 송중석 센터장 및 과학기술사이버안전센터 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 안내 및 선정 결과 공유 – 공동기획연구 제안서 내용의 기술적 타당성 검토 – 연구내용 수립 방안 및 향후 계획 논의 
경찰청 (21.07.30)	○ 주요 협의자 – 경찰청 과학치안정책팀 김경오 경감, 이준행 빅데이터정책기획계장 외 3인 – KISTI 송중석 센터장, 이준 선임, 권태웅 연구원, 박건량 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 참여여부 타진 – 공동기획연구 제안서 내용 공유 및 타당성 검토 – 경찰청 사업 불참 확정 (대국민 치안관련 서비스의 민감성 고려)

협의 기관 (날짜)	협의 및 자문 내용	
관계기관 담당자 및 전문가 자문단 (고려대학교, 21.08.05)	○ 주요 협의자 – 한국도로공사 이창준 팀장, 한국선급 박개명, 유진호 책임 – 숭실대 조효진 교수, 고려대 김희석, 노희준 교수 – KISTI 송중석 센터장 외 3인 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 안내 및 선정 결과 공유 – 공동기획연구 각 부처별 내용의 실무적 타당성 검토 – 연구내용 수립 방안 및 향후 계획 논의	
세종특별자치시 (21.08.27)	○ 주요 협의자 – 세종특별자치시 임채식 사무관, 박혜연 주무관 – KISTI 송중석 센터장, 이준 선임, 권태웅 연구원, 김태용 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 참여여부 타진 – 공동기획연구 제안서 내용 공유 및 타당성 검토 – 세종특별자치시 스마트 City 인프라 현황 공유 및 안내 – 세종특별자치시 적극 참여 및 지원 확약	
전문가 자문단 (서면, 21.09.10)	○ 주요 협의자 – 한국도로공사 이창준 팀장, 한국선급 박개명 팀장, 해양선박플랜트연구소 심우성 단장 – KISTI 송중석 센터장 외 과학기술사이버안전센터 연구원 ○ 협의 내용 – 각 인프라(C-ITS, LTE-M)에서 고려할 수 있는 암호화 데이터 수집대상 – 암호문 · 평문 데이터의 페어셋 수집 가능 방안 – 데이터 수집을 위한 H/W 및 S/W구축 비용 등 소요 예산	
관계기관 담당자 (서면, 21.10.04)	○ 주요 협의자 – 한국도로공사 이창준 팀장, 한국선급 박개명 팀장, 해양선박플랜트연구소 심우성 단장 – KISTI 송중석 센터장 외 과학기술사이버안전센터 연구원 ○ 협의 내용 – 각 인프라 환경 (LTE-M, C-ITS) 환경에서의 데이터 수집 방안 및 실증 환경 검증 – 각 환경별 테스트베드(관공선 및 해양실습선, C-ITS 실증센터) 활용방안 검토 – C-ITS 및 LTE-M 통신 인프라 세부 Specification 검토	

협의 기관 (날짜)	협의 및 자문 내용
전문가 자문단 (서면, 21.10.20)	○ 주요 협의자 – 국민대 윤명근 교수, 호서대 이태진 교수, 고려대 노희준 교수, 상명대 김환국 교수 – KISTI 송중석 센터장 및 과학기술사이버안전센터 연구원 ○ 협의 내용 – 공격·악성행위 분석과정에 활용할 수 있는 통신 데이터 특징 검토 – 암호화 트래픽을 통한 사이버공격 사례 분석 및 규모 검토 – 각 환경별 데이터 수집 방안의 기술적인 적정성 및 데이터의 품질 향상 방안 검토 
해양 수산부 (21.10.25)	○ 주요 협의자 – 해양수산부 최은진 사무관, 한성의 주무관 – KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 중간컨설팅 결과 보고 및 현재 진행상황 검토 – 해양수산부 서비스·인프라 세부 현황 공유 및 연구 타당성 논의 – 예산 수립 및 투입 분야 적정성 검토
국토교통부 (21.10.28)	○ 주요 협의자 – 국토교통부 정보보호담당관실 김미희 주무관 – KISTI 송중석 센터장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 안내 및 선정 결과 공유 – 공동기획연구 제안서 내용 공유 및 타당성 검토 – 국토부 참여의사 타진 및 인프라·서비스 운용과로 이관 추천
관계기관 담당자 (서면, 21.10.29)	○ 주요 협의자 – 해양선박플랜트연구소 심우성 단장, 한국선급 박개명 팀장 – ETRI 문대성 실장 – KISTI 송중석 센터장 외 과학기술사이버안전센터 연구원 ○ 협의 내용 – 각 부처별 중간컨설팅 보고서 내용 점검 – 부처별 연구수행 최적화 방안 검토 – 원천기술의 부처 인프라·서비스 적용 방안 검토 

협의 기관 (날짜)	협의 및 자문 내용
한국 도로공사 (21.11.02)	○ 주요 협의자 – 한국도로공사 스마트도로연구단 차세대도로팀 이창준 팀장, 윤원재 차장 – KISTI 송중석 센터장, 이준 선임 ○ 협의 내용 – 지능형교통시스템(C-ITS) 인프라 소개 및 실증센터 환경 검토 – 자율주행차량 및 네트워크 기지국 인프라간 암호화 통신 구간 확인 – C-ITS 보안체계에 따른 암호화 구간 보안필요성 검토
과학기술 정보통신부 (21.11.03)	○ 주요 협의자 – 과학기술정보통신부 정보보호기획과 박태성 사무관, 배영준 주무관 – KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 중간컨설팅 결과 보고 및 현재 진행상황 검토 – 과기정통부 서비스·인프라 세부 현황 공유 및 연구 타당성 논의 – 예산 수립 및 투입 분야 적정성 검토 – 주관기관으로 연구진행시 연구사업관리 총괄기관 선정 논의
국가 정보원 (21.11.04)	○ 주요 협의자 – *** 담당관 – KISTI 송중석 센터장, 이준 선임 ○ 협의 내용 – 국가·공공 보안관제분야 연구개발 필요성 논의 – 암호화 트래픽 기반 공격의 위험성 검토 및 국가사이버안보센터 협력 타진 – 기타 법적 규제 및 기술적 이슈사항 논의
세종특별 자치시 (21.11.11)	○ 주요 협의자 – 세종특별자치시 임채식 사무관, 박혜연 주무관 – KISTI 송중석 센터장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 중간컨설팅 결과 보고 및 현재 진행상황 검토 – 스마트 City 센서네트워크 구축 세부 현황 공유 및 연구 타당성 논의 – 예산 수립 및 투입 분야 적정성 검토
전문가 자문단 (KISTI, 21.11.11)	○ 주요 협의자 – 국민대 윤명근 교수, 호서대 이태진 교수, 고려대 노희준 교수, 상명대 김환국 교수 – ETRI 문대성 네트워크시스템보안연구실장, KAIST 조호묵 실장 – KISTI 송중석 센터장 및 과학기술사이버안전센터 연구원 ○ 협의 내용 – 중간컨설팅 결과 공유 및 코멘트 내용 검토 – 각 인프라별 데이터 수집의 구체적인 방안 및 소요 예산 수립 – 암호화 악성행위 탐지를 위한 해외기술동향 공유 및 연구개발 현실 가능성 검토 

협의 기관 (날짜)	협의 및 자문 내용
정보통신 기획평가원 (21.11.15)	○ 주요 협의자 – 정보통신기획평가원 정현철 차세대보안PM, 보안블록체인기획팀 류승한 수석, 박성연 수석 – KISTI 송중석 센터장, 이준 선임 ○ 협의 내용 – 다부처공동기획연구 사업 및 추진체계 안내 – 진행상황 공유 및 과기부 주관 선정 시 향후 사업관리 가능여부 확인 – 정보보호원천기술 확보를 위한 과제내용 적절성 검토 및 논의
국토 교통부 (21.11.23)	○ 주요 협의자 – 국토교통부 디지털도로팀 장유진 사무관 – KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 제 11차 상향식 다부처공동기획연구 안내 및 선정 결과 공유 – 공동기획연구 제안서 내용 공유 및 타당성 검토 – 국토부 측 사업기간 축소 의견 제시(6년 –> 5년) – 국토부 참여 및 지원 최종 확인 (21.11.30)
세종특별 자치시 (21.12.21)	○ 주요 협의자 – 세종특별자치시 임채식 사무관, 박혜연 주무관 – KISTI 송중석 센터장, 이준 선임, 권태웅 연구원 ○ 협의 내용 – 최종보고서 세부 내용 검토 및 논의 – 현재 · 향후 연구사업에 활용 가능한 스마트 City 인프라 목록 최신화 – 향후 일정 안내 및 선정 시 부처 역할 검토 (과제수립 및 예산검토)  
전문가 자문단 (KISTI, 21.12.21)	○ 주요 협의자 – 국민대 윤명근 교수, 호서대 이태진 교수, 고려대 노희준 교수, 상명대 김환국 교수 – ETRI 문대성 네트워크시스템보안연구실장, KAIST CSRC 조호묵 실장 – KISTI 송중석 센터장 및 과학기술사이버안전센터 연구원 ○ 협의 내용 – 최종보고서 세부 내용 검토 및 논의 – 구체적인 연구내용 및 방향의 타당성 최종 검토 – 사회문제 해결을 위한 기여방안 및 연구개발 현실성 검토

<table>
<tr><th>협의 기관
(날짜)</th><th>협의 및 자문 내용</th></tr>
<tr><td></td><td>   </td></tr>
<tr><td rowspan="2">해양
수산부
(21.12.22)</td><td>○ 주요 협의자
– 해양수산부 최은진 서기관, 김근영 주무관
– KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원
○ 협의 내용
– 최종보고서 세부 내용 검토 및 논의
– 현재 · 향후 연구사업에 활용 가능한 LTE-M 서비스 · 인프라 목록 최신화
– LTE-M 및 항행실습선의 테스트베드 활용여부 최종 확인
– 향후 일정 안내 및 선정 시 부처 역할 검토 (과제수립 및 예산검토)</td></tr>
<tr><td>   </td></tr>
<tr><td>국토
교통부
(21.12.22)</td><td>○ 주요 협의자
– 국토교통부 디지털도로팀 장유진 사무관
– KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원
○ 협의 내용
– 최종보고서 세부 내용 검토 및 논의
– 현재 · 향후 연구사업에 활용 가능한 C-ITS 네트워크 및 디바이스 최신화
– 한국도로공사와 연계한 실증 테스트베드 활용 가능 여부 최종 확인
– 향후 일정 안내 및 선정 시 부처 역할 검토 (과제수립 및 예산검토)</td></tr>
</table>

<table>
<tr><th>협의 기관
(날짜)</th><th>협의 및 자문 내용</th></tr>
<tr><td></td><td>   </td></tr>
<tr><td rowspan="2">과학기술
정보통신부
(21.12.22)</td><td>○ 주요 협의자
– 과기정통부 박태성 사무관, 배영준 주무관
– KISTI 송중석 센터장, 김규일 팀장, 이준 선임, 권태웅 연구원
○ 협의 내용
– 최종보고서 세부 내용 검토 및 논의
– 향후 일정 안내 및 선정 시 부처 역할 검토 (과제수립 및 예산검토)
– 국가과학기술연구망 및 과기정통부 과학기술사이버안전센터 실증 테스트베드 활용 방안 논의</td></tr>
<tr><td>   </td></tr>
</table>

❑ 주관·참여 부처 협의 및 확정

○ 과학기술정보통신부, 국토교통부, 해양수산부, 세종특별자치시에서 본 연구에 대한 주관·참여 의사를 확인하고 적극지원을 확약

사 업 명	초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술개발 및 공유·협력 플랫폼 구축			
부처 (주관/참여부처 표기)	과기정통부 **(주관)**	국토교통부 (참여)	해양수산부 (참여)	세종시 (참여)
부서	정보보호기획과	디지털도로팀	첨단해양교통관리팀	통합정보센터
이름	박태성	장유진	최은진	임채식
직급	사무관	사무관	서기관	사무관
연락처 (이메일, 휴대폰)	sealiker15@korea.kr ********	upjang80@korea.kr ********	ejchoi0418@korea.kr ********	lcs2426@korea.kr ********
참여여부 및 협의현황	O 참여 및 예산투입 적극지원	O 참여 및 예산투입 적극지원	O 참여 및 예산투입 적극지원	△ 인프라 활용 및 실증·테스트 적극지원
총예산 (사업기간)	190억 (5년)	115억 (5년)	115억 (5년)	(컨소시엄 참여 및 민간 매칭펀드)
회계	일반회계	일반회계	일반회계	-
세부사업명	차세대 사이버위협 대응 기술 개발 사업 (가제)	차세대 사이버위협 대응 기술 개발 사업 (가제)	차세대 사이버위협 대응 기술 개발 사업 (가제)	–

○ 부처별 참여·지원 확약서

(주관) 과학기술정보통신부

과학기술정보통신부「다부처공동기획사업 공동기획연구」
'초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축'

과학기술정보통신부는 「제11차 상향식 다부처공동기획사업 공동기획연구」로 추진되는 '초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축' 연구사업의 **주관기관**으로서 향후 본 과제 선정 시 사업 추진 **적극 지원** 예정.

2021년 12월 22일

과학기술정보통신부
정보보호기획과
사무관 박 태 성 (인)

(참여) 국토교통부

과학기술정보통신부「다부처공동기획사업 공동기획연구」
'초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축'

국토교통부는 「제11차 상향식 다부처공동기획사업 공동기획연구」로 추진되는 '초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축' 연구사업의 **참여 확약** 및 향후 본 과제 선정 시 사업 추진 **적극 지원** 예정.

2021년 12월 22일

국토교통부
디지털도로팀
사무관 장 유 진 (인)

(참여) 해양수산부

과학기술정보통신부「다부처공동기획사업 공동기획연구」
'초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축'

해양수산부는 「제11차 상향식 다부처공동기획사업 공동기획연구」로 추진되는 '초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축' 연구사업의 **참여 확약** 및 향후 본 과제 선정 시 사업 추진 **적극 지원** 예정.

2021년 12월 22일

해양수산부
첨단해양교통관리팀
서기관 최 은 진 (인)

(참여) 세종특별자치시

과학기술정보통신부「다부처공동기획사업 공동기획연구」
'초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축'

세종특별자치시는 「제11차 상향식 다부처공동기획사업 공동기획연구」로 추진되는 '초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축' 연구사업의 **참여 확약** 및 향후 본 과제 선정 시 사업 추진 **적극 지원** 예정.

2021년 12월 21일

세종특별자치시
도시성장본부 통합정보센터
사무관 임 채 (인)

❑ 연구 성과물 결과 검증 및 실증 테스트베드 확정

○ 주무부처 및 개발·수요기관의 성과 적용·검증 대상으로 활용 구간 확정

[표 23] 부처별 연구 성과 적용 및 활용 구간

주무부처	개발·수요기관	성과 적용·활용 구간
과학기술정보통신부	한국과학기술정보연구원	국가과학기술연구망(KREONET)* 보안관제 대상기관
국토교통부	한국도로공사	C-ITS 시범운영 구간 중 실증 구간 선정(논의 중)
해양수산부	선박해양플랜트연구소	LTE-M 활용 국가 관공선 및 해양대학교 항행실습선
세종특별자치시	도시성장본부	세종시 內 스마트 City 통신망 관제 영역
기타 국가공공 분야 全부처	부문보안관제센터	각 부처의 보안관제센터가 담당하고 있는 관제 네트워크

* 국내·외 연구자들에게 첨단과학 및 응용연구 수행을 지원하는 국가 R&D 연구망

○ 정보보호 장비·솔루션 개발 민간기업 원천기술 상용화·실용화 지원 협력

㈜SK쉴더스
(보안관제 및 종합정보보안서비스제공)

과학기술정보통신부 「다부처공동기획사업 공동기획연구」
협 력 의 향 서
(Letter of Intent)

본 의향서는 상호협력 내용을 기초로 한 전략적 제휴를 통하여 잠재적인 공동연구 기회를 발굴함과 동시에 이를 실현하고 확대하기 위한 상호 협력 의사를 명문화 하는데 그 목적이 있음.

'한국과학기술정보연구원' 과 '(주)SK쉴더스' 는 성공적인 연구 성과 달성 및 검증을 위한 다음과 같은 사항에 대해 상호 협력하기로 합의함.

- 다 음 -

가. 하기 연구수행과제* 수행시 개발기술의 검증 및 평가를 위한 적극적인 실증 환경 구축 협력, 기술 개발 지원, 정보제공 및 국내·외 기술교류 등
* 초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축

나. 기타 연구결과를 기반으로 암호화기반 사이버공격 탐지·대응 공동연구 등

본 의향서와 관련하여 상호 교류하는 자료 및 정보는 사업 목적 달성을 위해서만 사용하고, 제 3자에게 이를 제공하거나 누설하지 않으며, 신의를 바탕으로 협의 내용을 충실히 이행할 것을 확인 함.

2021년 12월 20일

한국과학기술정보연구원
과학기술사이버안전센터장
송 중 석 (인)

㈜SK쉴더스
그룹장
김 덕 수 (인)

㈜윈스
(네트워크 보안장비·솔루션 개발)

과학기술정보통신부 「다부처공동기획사업 공동기획연구」
협 력 의 향 서
(Letter of Intent)

본 의향서는 상호협력 내용을 기초로 한 전략적 제휴를 통하여 잠재적인 공동연구 기회를 발굴함과 동시에 이를 실현하고 확대하기 위한 상호 협력 의사를 명문화 하는데 그 목적이 있음.

'한국과학기술정보연구원' 과 '(주)윈스' 는 성공적인 연구 성과 달성 및 검증을 위한 다음과 같은 사항에 대해 상호 협력하기로 합의함.

- 다 음 -

가. 하기 연구수행과제* 수행시 개발기술의 검증 및 평가를 위한 적극적인 실증 환경 구축 협력, 기술 개발 지원, 정보제공 및 국내·외 기술교류 등
* 초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축

나. 기타 연구결과를 기반으로 암호화기반 사이버공격 탐지·대응 공동연구 등

본 의향서와 관련하여 상호 교류하는 자료 및 정보는 사업 목적 달성을 위해서만 사용하고, 제 3자에게 이를 제공하거나 누설하지 않으며, 신의를 바탕으로 협의 내용을 충실히 이행할 것을 확인 함.

2021년 12월 20일

한국과학기술정보연구원
과학기술사이버안전센터장
송 중 석 (인)

㈜윈스
부사장
조 학 수 (인)

㈜이스트시큐리티
(바이러스 백신 및 EDR 보안솔루션 개발)

과학기술정보통신부 「다부처공동기획사업 공동기획연구」
협 력 의 향 서
(Letter of Intent)

본 의향서는 상호협력 내용을 기초로 한 전략적 제휴를 통하여 잠재적인 공동연구 기회를 발굴함과 동시에 이를 실현하고 확대하기 위한 상호 협력 의사를 명문화 하는데 그 목적이 있음.

'한국과학기술정보연구원' 과 '(주)이스트시큐리티' 는 성공적인 연구 성과 달성 및 검증을 위한 다음과 같은 사항에 대해 상호 협력하기로 합의함.

- 다 음 -

가. 하기 연구수행과제* 수행시 개발기술의 검증 및 평가를 위한 적극적인 실증 환경 구축 협력, 기술 개발 지원, 정보제공 및 국내·외 기술교류 등
* 초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축

나. 기타 연구결과를 기반으로 암호화기반 사이버공격 탐지·대응 공동연구 등

본 의향서와 관련하여 상호 교류하는 자료 및 정보는 사업 목적 달성을 위해서만 사용하고, 제 3자에게 이를 제공하거나 누설하지 않으며, 신의를 바탕으로 협의 내용을 충실히 이행할 것을 확인 함.

2021년 12월 20일

한국과학기술정보연구원
과학기술사이버안전센터장
송 중 석

㈜이스트시큐리티
상무
김 의 탁

㈜와이즈넛
(인공지능·빅데이터 솔루션 개발)

과학기술정보통신부 「다부처공동기획사업 공동기획연구」
협 력 의 향 서
(Letter of Intent)

본 의향서는 상호협력 내용을 기초로 한 전략적 제휴를 통하여 잠재적인 공동연구 기회를 발굴함과 동시에 이를 실현하고 확대하기 위한 상호 협력 의사를 명문화 하는데 그 목적이 있음.

'한국과학기술정보연구원' 과 '(주)와이즈넛' 은 성공적인 연구 성과 달성 및 검증을 위한 다음과 같은 사항에 대해 상호 협력하기로 합의함.

- 다 음 -

가. 하기 연구수행과제* 수행시 개발기술의 검증 및 평가를 위한 적극적인 실증 환경 구축 협력, 기술 개발 지원, 정보제공 및 국내·외 기술교류 등
* 초연결 기반 대국민 서비스·인프라의 암호화 공격에 대비한 행위기반 보안관제 기술 개발 및 공유·협력 플랫폼 구축

나. 기타 연구결과를 기반으로 암호화기반 사이버공격 탐지·대응 공동연구 등

본 의향서와 관련하여 상호 교류하는 자료 및 정보는 사업 목적 달성을 위해서만 사용하고, 제 3자에게 이를 제공하거나 누설하지 않으며, 신의를 바탕으로 협의 내용을 충실히 이행할 것을 확인 함.

2021년 12월 20일

한국과학기술정보연구원
과학기술사이버안전센터장
송 중 석 (인)

㈜와이즈넛
성장기술연구소 상무
장 정 훈 (인)

❑ 전문가 자문위원회 구성

ㅇ 공동기획연구 자문위원회 명단 전문가들을 기반으로 본 연구의 R&D 전문가 협의체를 구성 예정 (산·학·연 및 수요기관 등)

참여전문가				
소속	담당부서	성명	직위/직급	비고
고려대학교	사이버보안전공	김희석	부교수	핵심 원천기술 자문
고려대학교	사이버보안전공	노희준	조교수	
국민대학교	소프트웨어융합대학	윤명근	교수	
상명대학교	정보보안공학과	김환국	조교수	
호서대학교	컴퓨터공학부	이태진	조교수	
한국과학기술원	사이버보안연구센터	조호묵	실장	
고려대학교	정보보호대학원 사이버법정책	권헌영	교수	법·제도 및 정책 자문
한국전자통신연구원	네트워크·시스템보안연구실	문대성	실장	세종시 스마트 City 서비스·인프라 자문
가천대학교	컴퓨터공학과	서정택	부교수	
숭실대학교	소프트웨어학부	조효진	조교수	국토부(C-ITS) 서비스·인프라 자문
한국도로공사	스마트도로연구단	이창준	팀장	
		윤원재	차장	
선박해양플랜트연구소	해양안전환경연구본부	심우성	단장	해수부(LTE-M) 서비스·인프라 자문
한국선급	사이버인증팀	박개명	팀장	
		유진호	책임	

❑ 공청회 개최

○ 참여 부처 및 관계 기관 담당자 및 산·학·연 전문가를 초청하여 공청회 개최 (2021년 12월 1일)

- 공청회 의견을 수렴하여 추진 계획 및 최종 보고서에 반영 완료

<table>
<tr><td>과 제 명</td><td colspan="4">초연결 기반 대국민 공공 서비스·인프라의 암호화 공격에 대한 행위 기반 보안관제 기술개발 및 공유·협력 플랫폼 구축</td></tr>
<tr><td>일 시</td><td colspan="4">2021년 12월 01일(수요일) 오후 14:00~18:00</td></tr>
<tr><td>장 소</td><td colspan="4">한국과학기술정보연구원 키움관 컨퍼런스-1</td></tr>
<tr><td>주요 논의사항
(간략히 작성)</td><td colspan="4">○공청회 세부 일정
<table>
<tr><th>순번</th><th>시간</th><th>일 정</th><th>발표자</th></tr>
<tr><td>1</td><td>14:00~14:10</td><td>개회사</td><td>박태성 사무관
(과학기술정보통신부)</td></tr>
<tr><td>2</td><td>14:10~14:30</td><td>연구 소개 및 진행 상황</td><td>송중석 센터장
(과제 책임자)</td></tr>
<tr><td>3</td><td>14:30~14:50</td><td>DNA 시대의 보안관제 패러다임 변화</td><td>윤명근 교수
(국민대)</td></tr>
<tr><td>4</td><td>14:50~15:10</td><td>암호화 트래픽 분석 연구 필요성 및 최신 연구동향</td><td>이태진 교수
(호서대)</td></tr>
<tr><td>5</td><td>15:10~15:30</td><td>세종시 스마트 City 인프라 구축 현황 및 계획</td><td>임채식 사무관
(세종특별자치시)</td></tr>
<tr><td>6</td><td>16:00~17:00</td><td>패널토론</td><td rowspan="2">좌장: 서정택 교수 (가천대)
패널:
김익균 본부장 (ETRI),
심우성 단장 (KRISO),
노희준 교수 (고려대),
조학수 부사장 (㈜ Wins),
김의탁 상무 (㈜ 이스트시큐리티)</td></tr>
<tr><td>7</td><td>17:00~17:20</td><td>방청객 의견 개진</td></tr>
</table>
○논의사항
- 연구개발 현황 및 현 연구의 차별성/필요성 논의
- 행위기반 암호화 공격 탐지 기술 연구 수행에 대한 코멘트 및 질의응답 수행
- 부처 및 관련 기관과의 논의 내용 공유</td></tr>
</table>

- 본 연구의 참여/수요기관 현황 공유
- 향후 일정 논의

ㅇ주제발표

전문가	주요 내용
윤명근 교수 (국민대학교)	전통적인 방식의 보안관제부터 현재의 진화된 보안관제까지의 주요 내용에 대해 소개하고, 특히 기존의 평문 중심에서 **암호화된 사이버 공격 탐지·대응**을 위한 **보안관제 패러다임의 전환의 시급성 및 AI를 활용한 최신 보안관제 기술** 소개
이태진 교수 (호서대학교)	비복호화 기반 암호트래픽 분석의 필요성, TLS Inspection 및 ETA 기술동향, Tor환경에서의 ETA 구현/검증 현황을 소개함으로써 **비복호화 기반의 암호트래픽 분석 가능성 시사 및 분석방법** 소개
임채식 사무관 (세종특별자치시)	세종시에서 구축·운영되고 있는 스마트 City 인프라에 대한 소개 및 **보안성 강화를 고려한 인프라 운영 계획** 소개

ㅇ전문가 의견

전문가	주요 의견
서정택 교수 (가천대학교)	◦ 본 과제의 핵심 목표는 “초연결 기반으로 대국민 공공 서비스 인프라의 **암호화 공격에 대비한 행위기반**으로 보안 관제를 수행”하는 것임. ◦ 이를 위해서는 **‘탐지’와 관련된 기술개발**과 참여 기관 간에 **정보를 공유·협력하는 플랫폼을 구축**하는 것이 가장 중요함. ◦ 금일 주제발표를 통해 **암호화 트래픽에 대한 분석 및 탐지 가능성을 확인**하였으며, 이를 바탕으로 과제 수행 기간 동안 관련된 기술들을 발전시켜 주도적인 연구를 수행한다면 성공적인 과제 수행이 가능할 것임.
김익균 본부장 (ETRI)	◦ **네트워크 트래픽이 암호화됨에 따라 보안관제에 많은 어려움**을 겪음. 기존에도 이를 극복하기 위한 시도들은 존재하였으나 다양한 측면의 **기술적 한계로 인해 사업화하기 어려웠음**. ◦ 그러나, 현재는 AI기술, 빅데이터 처리, 대용량 로우(raw)트래픽 수집 및 처리할 수 있는 기술들이 발전함에 따라 **암호**

		화 트래픽에 대한 분석을 현실화할 수 있는 단계가 된 것 같음. ◦ **Cisco를 포함한 글로벌 주요 기업**들이 암호화 트래픽 분석에 관한 백서를 작성 및 공개하는 것은 **암호화 트래픽에 대한 분석가능성을 시사**한 것. ◦ 이번 다부처공동기획연구를 통해 **비복호화 기반의 암호화 트래픽 분석 기술**을 체계적으로 발전시킨다면, **네트워크 보안 측면에서 아주 큰 성과**가 될 것임.
	심우성 단장 (KRISO)	◦ 최근 낚시 및 레저용 선박에 대한 수요 증가로 인해 해양에서의 활동이 급증, 이에 따른 **해양 네트워크 및 데이터 통신에 대한 보안성 강화가 시급**한 과제로 대두됨. ◦ 기존의 VHF무전기의 거리 및 속도의 한계를 극복하기 위해 **LTE기술을 활용한 초고속 해상 무선통신망을 구축**함. ◦ LTE-M은 연안 100Km까지의 서비스를 목표로 개발 및 운영됨에 따라 **인접국가(일본, 중국, 북한)들과의 전파 중첩**이 발생하며, 이들 국가에 의한 **사이버공격 발생 및 보안위협에 대한 리스크가 매우 높은 상황**으로 특히 **암호화된 통신에 의한 해킹 발생 시 신속·정확한 대응**을 통해 **국민의 안전한 삶을 제공할 필요가 있음** ◦ 본 사업을 통해 **비복호화 기반의 원천기술이 성공적으로 개발되어 LTE망에서 수행되는 해킹 및 보안위협들을 탐지**할 수 있길 바람.
	노희준 교수 (고려대학교)	◦ 본 사업의 성공적인 수행을 위해서는 **다양한 데이터셋 확보 및 데이터 표현이 중요함.** ◦ 다양한 환경에서의 데이터셋 수집·구축한다면 충분히 **암호화 트래픽 분석(ETA : Encrypted Traffic Analytics)연구를 선도** 가능함. ◦ 또한, 최근 TiPS에서 발표된 연구에 따르면 패킷간의 관계를 단순히 1차원 배열의 형태로 데이터를 표현한 것보다 그래프 기반의 표현 방법 등을 활용했을 때 유의미한 결과들을 도출함. ◦ 따라서, **데이터에 대한 다양한 형태의 표현**을 통해 기존에는

		불가능했던 **암호화된 공격을 행위기반으로 탐지가 가능함**
	조학수 부사장 (㈜ Wins)	◦ 네트워크 보안 분야의 1위 업체로서, 기존의 평문 중심의 통신 환경이 **암호문 중심의 통신환경으로 급격하게 변화함**에 따라 보유하고 있는 **솔루션의 활용도가 현저히 떨어질 것으로 판단**하고 있음. ◦ 윈스에서도 2000년 중반을 전후해서 **암호화된 형태의 공격을 탐지하기 위해 프로젝트를 진행**한 경험이 있으나, 당시에는 **시장의 니즈가 높지 않아 중단**되었지만 암호화된 트래픽이 급증하고 있는 지금의 네트워크 환경을 고려할 때, 본 사업을 통한 **원천기술을 선도적으로 확보**하고 **해외 기업에 의한 기술 종속 회피** 및 **제2의 화웨이 사태를 미연에 방지**할 필요가 있음. ◦ 윈스에 추진했던 프로젝트를 통해 **분석의 트리거 및 위협정보 탐지에 활용하기 위한 CTI의 필요성**을 인지하였으며, 본 사업이 진행될 경우 이에 대한 충분한 고려가 필요함. ◦ 하지만, 실시간으로 네트워크 트래픽 패킷 획득 후 **헤더 및 페이로드 분석을 처리하여 데이터를 추출하고 저장하는 모든 과정이 기술적으로 어려움**. ◦ 암호화 통신을 위한 핸드셰이킹 과정에서 발생하는 키 교환, Cipher suite 교환, 인증서 교환 등에서 파악할 수 있는 공격자 및 피해자 정보를 모아 DB화한다면 **세션 內 트래픽의 악성 여부를 조기 식별 가능**할 것.
	김의탁 상무 (㈜이스트시큐리티)	◦ **네트워크에서 암호화 패킷 분석**을 통해 나온 악성/정상행위 결과 및 근거를 **엔드포인트(단말)에서 해당 패킷이 복호화 된 정보와 연계**한다면 암호화 패킷에 대한 **검증 및 종합적인 솔루션 및 해결방안 제시가 가능**할 것. ◦ 또한, 여러 기관에서 발생한 이벤트, 관제 관련 기술 등을 활발히 **공유하고 연계한다면 경쟁력 있는 연구 개발 수행 및 원천기술 확보가 가능**할 것.

ㅇ방청객 의견 개진

최간호 소장 (㈜시스메이트)	◦ **본 과제에서 대상으로 삼고 있는 암호화 프로토콜의 종류가 무엇인가? 현재 상용되는 암호화 프로토콜별 사용량을 분석해보면 TLS가 약 70%, 약 QUIC 30%임. QUIC은 높은 비율로 사용되는 암호화 프로토콜이기 때문에 분석 대상으로 선정이 필요하나 핸드쉐이크 과정조차 암호화가 되어 있어 분석이 매우 어려울 것이 예상됨. 또한, 산업제어시스템등과 같은 환경에서의 암호화 트래픽도 감안하고 있는가?**
송중석 센터장 (KISTI)	◦ 비복호화 기반의 암호화 트래픽 분석을 제안하는 이유 중 하나는 모든 암호화 통신을 복호화할 수는 없기 때문임. ◦ 아직 암호화 프로토콜 대상이 정확히 확정된 것은 아니나 **TLS는 가장 기본이 되는 암호화 프로토콜이기 때문에 대상**으로 수행 예정. ◦ 만약, **TLS를 대상으로 유의미한 결과를 도출할 수 있다면 이를 기반으로 他암호 프로토콜 역시 분석이 가능할 것**으로 예상 중임. ◦ 제안단계까지 모든 제반사항들을 고려하여 대상 암호화 프로토콜을 선정할 것임.

하수헌 이사 (㈜샌즈랩)	◦ **다부처공동기획 연구개발이 성공적으로 진행되어 실제 기술이 상용화가 되었을 때, 멀티 피쳐로 구성되는 암호화 트래픽의 행위를 실시간으로 탐지 가능한 하드웨어의 성능 구현이 현실적으로 가능한 부분인지?**
조학수 부사장 (㈜ Wins)	◦ 암호화 트래픽을 하나의 패킷으로 정의하는 것은 불가능. ◦ 최소 하나의 세션을 모두 기록·모니터링 해야 하는데, 해당 과정에서 소요되는 비용이 매우 크기 때문에 현실적으로 불가능함 (100Gbps에서 64k사이즈의 패킷 1억 4천만개 분석 필요). ◦ 따라서. **CTI를 기반으로 공격 트래픽을 선별하고 분석 범위를 확대하는 것이 필요함.** ◦ 제한된 하드웨어 자원에서의 효율적 분석을 위해 선택과 집중이 필요함.

박건량 연구원 (KISTI)	◦ **상용 클라우드 혹은 메일서버를 C2서버로 활용할 때, CTI 정보를 활용할 수 있는 방법이 있는지?**
조학수 부사장 (㈜ Wins)	◦ 정상 서비스를 통해 악성행위가 전파되었다 해서 해당 서비스를 차단하는 것보다는 **이후에 발생하는 행위들을 통해 판단하는 것이 옳음**. ◦ C2서버에 접속해서 진행되는 핸드셰이크와 같은 부분에서 CTI가 활용될 수 있는 여지가 있다고 생각됨. ◦ 또한, 악성파일이 실행되었을 때 C2 혹은 외부 사이트에 접속 후 Cipher suite 등을 교환하는 부분, 피싱의 경우 접속 사이트의 도메인 네임의 제작 시기, 제작 출처, 다른 사이트와의 유사도 등의 부분에서 CTI를 활용할 수 있을 것으로 생각함.
김의탁 상무 (㈜이스트시큐리티)	◦ 일반적인 해커의 경우 C2 서버를 통해 데이터 전송을 하는데, 올해 구글 계정을 생성해 구글 블로그 쪽으로 데이터를 전송하는 일반적이지 않은 방식을 찾은 바가 있음. ◦ 이렇게 국내 보안 업체 및 보안 담당자를 우회하는 다양한 방식이 등장하고 있음 ◦ **특정 서비스를 통해 파일이 전파되는 행위뿐만 아니라 파일 전송 시 사이즈 및 특정 확장자 전송 여부 등 전반적인 모니터링이 필요**할 것임. ◦ **모니터링 후 정보를 수집·분석하여 차후에 보안정책 제작까지도 가능**할 것임.

문대성 실장 (ETRI)	◦ **본 사업은 기획연구이기 때문에 다부처 사업 심의 통과 및 他 다부처사업과 비교하여 경쟁력을 갖추는데 필요한 점을 제시해 주시면 좋을 것 같음.**
김익균 본부장 (ETRI)	◦ **기존 현황 및 기술의 발전 등을 고려하여 3~4년 이후에 어떠한 전략을 통해 어떤 청사진(목표 및 계획)을** 사전에 작성할 수 있다면 좋은 결과를 도출할 수 있을 것
노희준 교수 (고려대학교)	◦ 트래픽 수집·분석 시 발생하는 **부처별 공통점 및 차별점을 파악하는 것이 중요**함. ◦ 여러 부처 및 기관에서 운영하는 시스템 및 수집 가능한 정보들은

		매우 상이함. ◦ 상이한 환경 및 시스템에서 공통적으로 수집 가능한 정보들을 파악하고 각 부처별 특성이 반영된 특징들을 가미한다면 더욱 유의미한 연구가 될 것임.
	조학수 부사장 (㈜ Wins)	◦ 본 사업의 기간(6년)을 고려했을 때 **경제성은 의사결정에서 중요한 요소**가 될 것임. ◦ 현재 국내에 구축된 관제센터들은 다양한 보안 장비들을 설치·운영 중이나 **암호화 트래픽으로 인해 해당 보안 장비들의 역할 축소 및 신규 장비 증가, 분석 및 운영 인력 부족, 성과하락 등의 문제점들이 존재**. ◦ 따라서 **다부처 사업을 통해 경제적 비용 및 사회적 중복 비용을 최소화하고 효율적인 운영이 필요함을 강조**. ◦ 또한, 국가적으로 공유할 수 있는 CTI체계를 구축하고, CTI 정보들을 실시간으로 추출 및 공유하여 旣구축된 보안 장비에 적용 및 운영함으로써 그 활용률을 향상시킬 수 있음을 강조한다면 해당 과제가 더욱 유의미하게 받아드려질 것임.
	김의탁 상무 (㈜이스트시큐리티)	◦ 엔드포인트 업체들이 개별 IoT시장을 개척하지 않는 이유 중 하나는 개별 IoT 시장이 너무 작아 시장성 및 경제성이 부족하기 때문임. ◦ IoT는 저마다 다른 프로토콜과 통신방식을 활용하기 때문에 범용성이 부족함. ◦ 본 사업을 통해 **프로토콜 및 통신환경과 독립적으로 운영 및 사이버 위협 탐지가 가능한 장비 개발** 및 환경 구축은 **해당 과제를 성공적으로 수주하기 위한 선제조건**이 될 수 있음.
	심우성 단장 (KRISO)	◦ 기존 데이터를 학습함으로써 암호화된 공격들을 찾을 수 있다면 탐지률에 대한 **정량적 목표가 확률적 또는 통계적으로 제시돼야함**. ◦ 만약 목표치를 제시할 수 없다면, **제시할 수 없는 사유에 대한 내용이라도 반영함으로써 과제 목표치를 현실적이며 상세히 제시**하는 것이 필요.

[다부처공동기획연구 지원사업 공청회 포스터]

[개회사 - 박태성 사무관]

[과제 브리핑 - 송중석 센터장]

[전문가 주제 발표 - 윤명근 교수]

[전문가 주제 발표 - 임채식 사무관]

[패널토론-1]

[패널토론-2]

제2절 사업 추진체계

❑ 사업 운영 체계

○ **(역할정립·협력체계 구축)** 부처, 개발·수요 기관, 연구수행·지원 기관별 역할 정립 및 긴밀한 협조·추진체계 구축

- **주관·참여 부처**: 부처 內 개발·수요 기관들의 요구사항을 수렴하고 다부처 사업 수행을 지원함으로써 연구개발 성과창출 추진

- **개발·수요 기관**: 부처 및 연구 수행·지원 기관들과 상호협력을 통한 원활하고 주도적인 사업 추진 및 성과 확산 방안 수립

- **연구 수행·지원 기관**: 산·학·연을 포함한 전문성·관련성 있는 기관간의 공유·협력을 통해 원천기술연구, 일자리 창출지원 및 인력양성 등 사회문제해결에 기여

※ 효율적인 부처협업사업 추진을 위하여 '통합관리형'으로 관리체계 수립

<그림 64> 사업 추진 · 운영 체계도

○ **(협의체 구성·운영)** 사업 추진 범위 및 연구방향 정립을 위한 다부처 추진 협의체 및 R&D 전문가 협의체 구성

- **다부처 추진 협의체** : 사업간 지속적인 공동연구 계획·방법·추진 체계 수립을 위해 부처 담당자, 사업 주관 부서, 실무기관 관계자 등으로 구성

- R&D 전문가 협의체 : 암호기술, 네트워크, AI 등 사업 관련 각 분야의 전문가들로 구성된 R&D 전문가 협의체 구성을 통해 구체적인 연구방향 수립·검토 및 원천기술 개발 자문 수행

○ **(실증 사전협의)** 사업성과의 원활한 검증 및 적용을 위해 협업 부처 및 수요처 등과 연계한 현장 실증 사전 협의 추진

- 현장 실증의 범위, 실증 시 필요한 디바이스, 디바이스 설치 시 필요한 기술적·제도적 요구사항 정의 등을 부처 및 실증 주체와 협의

- 국가·공공 분야 '부문보안관제센터'와 연계·협력을 추진함으로써 사업성과 및 원천기술 유효성 평가와 더불어 성과 확산 도모

❑ 부처 역할분담 및 연계방안

○ **(역할 세분화)** 성공적인 다부처사업 추진이 가능하도록 기술개발 체계를 고려하여 주관부처와 참여부처간 역할을 세분화

- **주관부처(과학기술정보통신부)** : ICT환경 기반 데이터 수집, 최적화 기술 개발 및 실증, 행위기반 자동화 분석·탐지 원천기술 및 공유·협력 플랫폼 개발 주도

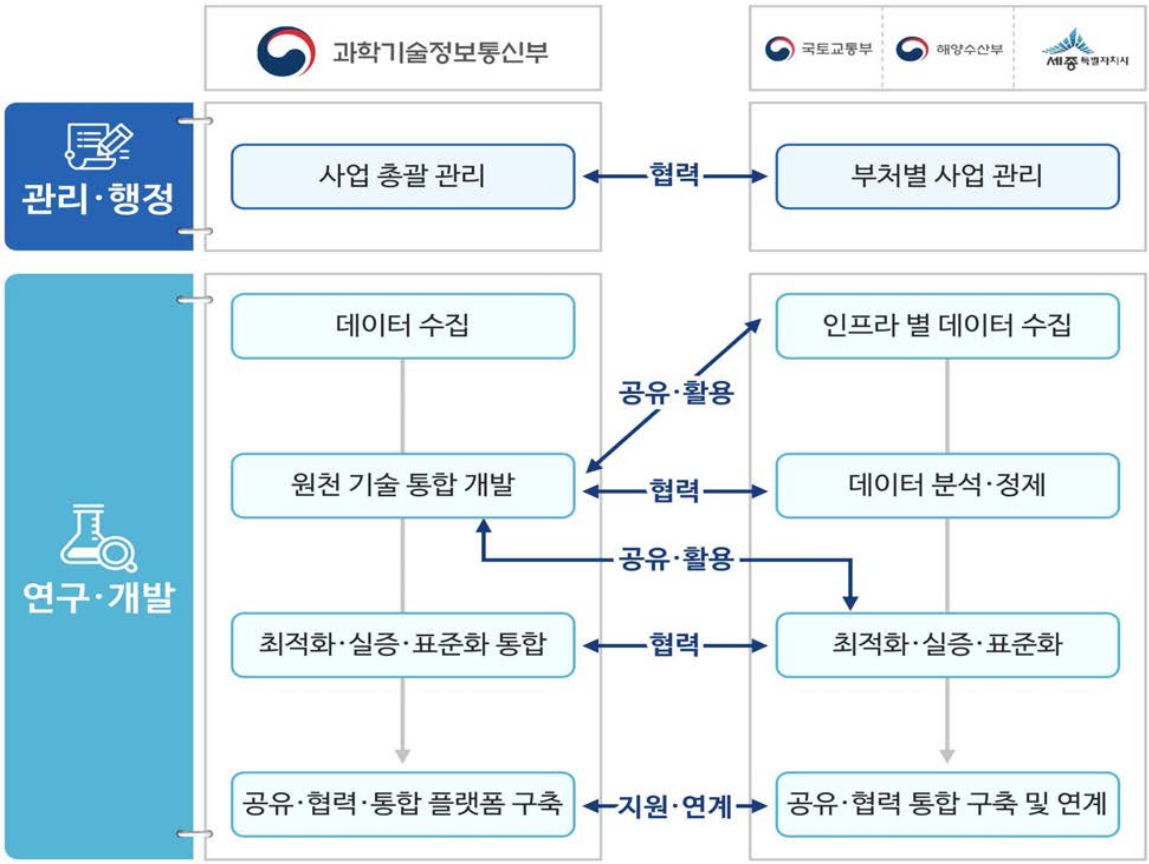
- **참여부처(국토교통부, 해양수산부, 세종특별자치시)** : 환경 및 데이터 특수성을

고려하여 데이터 수집, 최적화 기술개발 및 실증을 부처별 상황에 따라 각각 수행

- **전체부처** : 위협정보 표준포맷 개발 및 표준화 작업 공동 수행

○ **(연구 모듈화)** 각 부처별 업무범위 정립 및 연구수행 단계별 추진목표와 연차별 연구내용의 명확화를 위해 연구개발 단계를 대분류 2단계(원천기술 연구개발, 실증·실용화), 소분류 5단계(수집, 분석·탐지, 최적화·실증, 표준화, 공유·협력)로 구분하고 단계별 모듈화 수행

○ **(특수성 고려)** 다양한 환경에 대한 고려가 필수적인 암호화 기반 사이버 공격 대응의 특수성을 반영하여 서로 다른 유형의 대국민 공공서비스·인프라를 운용 중인 각 부처가 기술 수요처이자 공급처로서 참여하고, 긴밀한 연계 협력 추진



<그림 65> 주관 및 참여부처간 주요역할 분담

※ 기술개발 성공을 위해서는 주관기관을 중심으로 각 서비스·인프라 운용 기관, 통신환경별 기술연구 전문기관, 주요기반시설 대상 사이버 보안연구 전문기관 등 각 부처에서 보유하고 있는 전문기관들 간의 협력이 필수적으로 요구됨

※ 이를 위해서, 연구개발 간 부처간 원활한 협력 및 연구개발내용의 성격을 고려하여 혼합형 또는 공동추진 형태로 운영방식 구성 필요

○ **(공급처·수요처 역할)** 대국민 서비스·인프라를 운영, 보유한 참여부처는 본 사업의 공급처이자 수요처로써, 부처별 운용 환경을 고려한 최적화된 원천기술 개발 및 즉각적인 협력체계 구축이 가능

- **과학기술정보통신부** : 악성 암호화 트래픽 분석·탐지·대응 핵심 원천기술 개발과 데이터 공유 체계 구축을 위한 통합 플랫폼 구축 주도

- **국토교통부** : C-ITS 환경에서의 암호트래픽/악성코드 수집·공유 및 개발된 원천기술 적용 및 최적화 수행

- **해양수산부** : LTE-M 기반 스마트 선박·항만 환경에서의 암호트래픽/악성코드 수집·공유 및 개발된 원천기술 적용 및 최적화 수행

- **세종특별자치시** : 스마트 City 환경에서 발생하는 암호트래픽/악성코드 수집·공유, 實환경 테스트 베드 제공 및 기술 검증·최적화 수행

○ **(부처간 연계방안)** 구성된 협의체를 통해 정기적인 회의를 바탕으로 기술적 이슈에 대한 마일스톤 방식의 개발관리 협의 및 조정

- 요구사항, 기능, 설계 검토 및 기본·상세 설계, 시험방안, 운영방안 검토 등 수행

- 다부처 추진 협의체를 통한 정기 점검회의를 기반으로 각 세부과제별 문제점 도출 및 해결방안 수립

- 부처별 운영요구사항 부합성 평가 등을 실시하여 수요처 니즈 충족 및 사업 완성도 향상 추진

❑ 사이버 재난 대비 요구사항 분석 및 실용기술 발굴

ㅇ 사이버 공격을 통한 재난환경을 가정한 각 서비스·인프라 현장 중심의 요구사항을 도출하고, 이를 반영한 세부기술 도출을 위한 연구 추진

- 사이버 공격 징후 포착 및 사고발생 전주기간 현장상황의 시뮬레이션을 통한 기술적 한계 및 극복 시나리오 도출

- 보안관제 요원 및 정보보호 솔루션·장비 운용 인력 등 사이버공격 대응 요원들의 개선사항과 요구사항을 수집하고 이를 반영한 기술 개발을 통해 사이버 재난 발생 시 현장에 적용 가능한 실용적 연구 추진

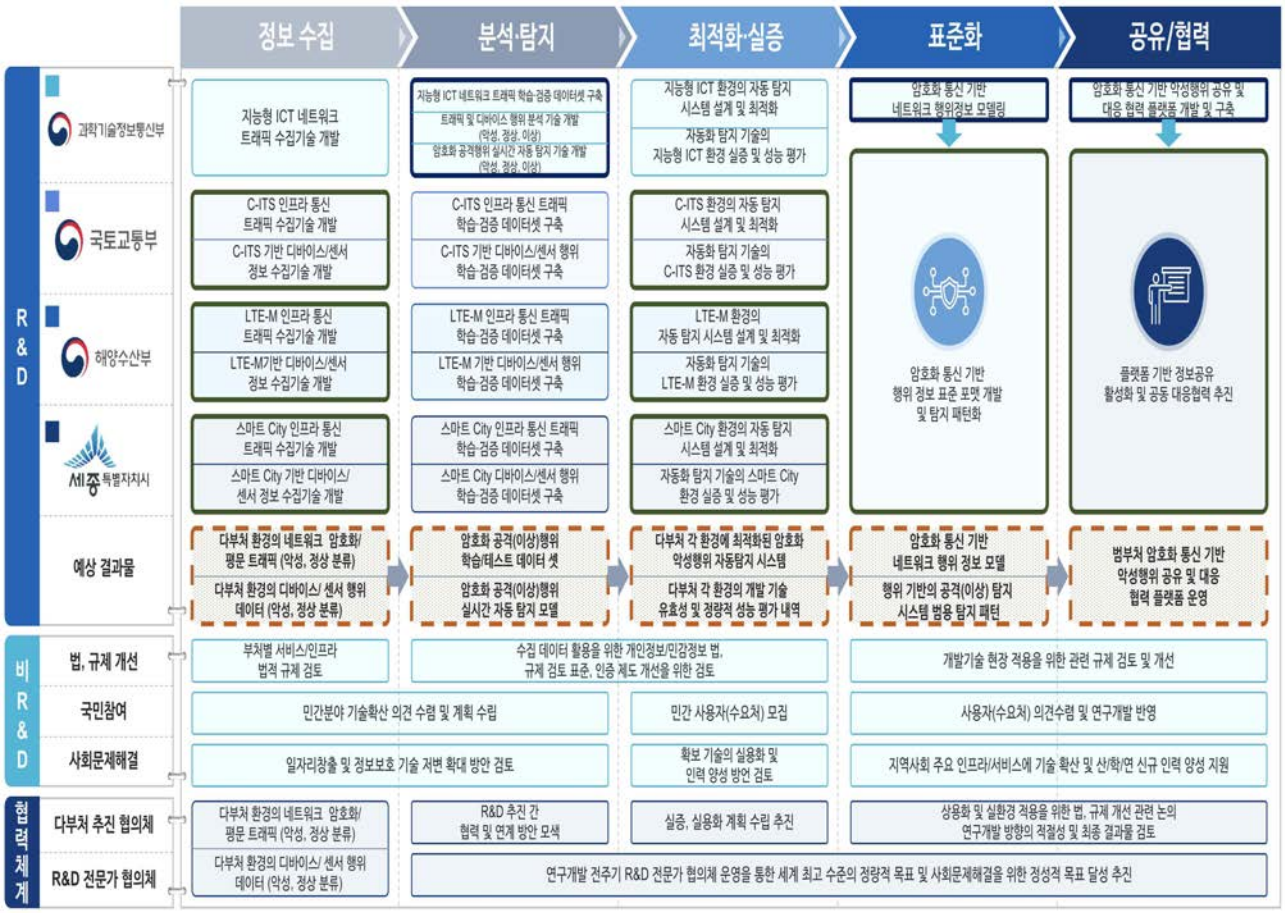
ㅇ 다양한 환경에 대한 고려가 필수적인 암호화 기반의 사이버공격 대응의 특수성을 반영하여, 서로 다른 유형의 대국민 공공서비스·인프라를 운용 중인 각 부처가 긴밀하게 연구개발 협력

- 각 인프라별 특성 및 취약점에 따른 연구개발 우선순위를 설정하고, 그에 따른 기술 성능 향상 방안 연구 추진

- 사이버보안 관련 유관기관(국가사이버안보센터 및 각급 보안관제센터) 들과 협력하여 사이버공격 징후 및 추가정보 수집·활용을 적극 추진하고, 이를 통합·공유할 수 있는 플랫폼에 적용할 수 있도록 연구 수행

❑ 다부처공동연구 추진 로드맵

○ 주관·참여부처, 수요기관, 협의체 등의 긴밀한 협조를 통해 각 연차별 결과와 최종 암호화통신 기반 악성·공격행위 탐지·대응 기술의 실증 및 실용화 추진



<그림 66> 연구개발 추진 로드맵

제3절 사업 기간 및 소요예산

❑ 연구기간 및 소요예산

○ 사이버보안 분야 인프라 기반 기술 발전 속도 및 암호화공격 대응 기술개발의 시급성을 고려하여 연구개발 기간 설정

- 수집, 분석·탐지, 최적화·실증, 표준화 및 공유·협력 5단계로 구분된 연구개발 과정을 5년에 걸쳐 수행 예정

[표 24] 부처별 연차 소요예산 (단위: 억원)

부처	사업내용	2023년	2024년	2025년	2026년	2027년	계
과학기술정보통신부	지능형 ICT환경 기반 악성·공격 행위 암호화평문 트래픽 수집 기술 개발	20	10	2	1	0	33
	자동탐지·대응 모델 구축을 위한 지능형 ICT환경 트래픽 특징기반 학습·검증 데이터셋 구축	15	10	3	2	0	30
	암호화 트래픽 악성·공격 행위 분석 및 탐지 기술 개발	5	20	20	10	0	55
	지능형 ICT환경의 실환경 테스트베드를 활용한 실증 및 성능 최적화 기술 개발	0	0	10	15	15	40
	악성·공격 행위 특징분석을 통한 행위정보 표준화 포맷 및 공유·협력 플랫폼 개발	0	0	0	12	20	32
	합계	**40**	**40**	**35**	**40**	**35**	**190**
국토교통부	차세대 지능형교통체계(C-ITS)기반 악성·정상행위 암호문평문 트래픽 수집 기술 개발	10	5	2	1	0	18
	차세대 지능형교통체계(C-ITS)기반 디바이스·센서 행위 정보 수집 기술 개발	10	5	2	1	0	18
	자동탐지·대응 모델 구축을 위한 차세대 지능형교통체계 트래픽·디바이스 특징 분석기반 데이터셋 구축	5	15	3	3	0	26
	차세대 지능형교통체계의 실환경 테스트베드를 활용한 실증 및 성능 최적화 기술 개발	0	0	13	10	10	33
	위협 확산 방지와 대응 방안 공유를 위한 분석정보 표준화 지원 및 공유·협력 기술 개발	0	0	0	10	10	20
	합계	**25**	**25**	**20**	**25**	**20**	**115**

부처	사업내용	2023년	2024년	2025년	2026년	2027년	계
해양수산부	지능형 해상교통정보서비스 및 해상무선통신망 기반 악성·정상행위 암호문평문 트래픽 수집 기술 개발	10	5	2	1	0	18
	지능형 해상교통정보서비스 및 해상무선통신망 기반 디바이스·센서 행위 정보 수집 기술 개발	10	5	2	1	0	18
	자동탐지·대응 모델 구축을 위한 해상무선통신망 트래픽·디바이스 특징 분석기반 데이터셋 구축	5	15	3	3	0	26
	해상무선통신망 실환경 테스트베드를 활용한 실증 및 성능 최적화 기술 개발	0	0	13	10	10	33
	위협 확산 방지와 대응 방안 공유를 위한 분석정보 표준화 지원 및 공유·협력 기술 개발	0	0	0	10	10	20
	합계	**25**	**25**	**20**	**25**	**20**	**115**
세종특별자치시	스마트 City 교통·치안·생활 서비스·인프라 기반 악성·정상행위 암호문평문 트래픽 수집 기술 개발	0	0	0	0	0	0
	스마트 City 교통·치안·생활 서비스·인프라 기반 디바이스·센서 행위 정보 수집 기술 개발	0	0	0	0	0	0
	자동탐지·대응 모델 구축을 위한 스마트 City 트래픽·디바이스 특징 분석기반 데이터셋 구축	0	0	0	0	0	0
	스마트 City 실환경 테스트베드를 활용한 실증 및 성능 최적화 기술 개발	0	0	0	0	0	0
	위협 확산 방지와 대응 방안 공유를 위한 분석정보 표준화 지원 및 공유·협력 기술 개발	0	0	0	0	0	0
	합계	**0**	**0**	**0**	**0**	**0**	**0**
총계		**90**	**90**	**75**	**90**	**75**	**420**

※ 1~2차년도의 경우 복호화장비 및 데이터 수집을 위한 스토리지 등의 H/W·S/W 구축비용 관계로 예산 증액 편성

※ 4차년도의 경우 실증·실용화 추진을 위한 테스트베드 구축·활용 및 시제품 제작 비용을 고려하여 예산 증액 편성

※ 세종특별자치시의 경우 기 구축된 스마트 City 서비스·인프라의 적극 활용 예정

❑ 부처별 재원 마련 방안

○ 총사업비는 485억원으로, 각 주관 및 참여부처는 자체 R&D 사업 예산, 국가연구개발사업 투자예산 등으로 재원 확보 예정

- 일부 민간 참여자의 경우 현물 등의 부담을 통하여 재원 충당 고려

[표 25] 부처별 재원 마련 방안

부처	세부사업명	참여여부 및 현황		회계	총 예산
과학기술 정보통신부	차세대 사이버위협 대응 기술 개발 사업 (가제)	O (주관)	연구개발 필요성 및 시급성이 높으므로 사업 참여와 예산투입 적극 지원	일반회계	190 (~2027년)
국토교통부	차세대 사이버위협 대응 기술 개발 사업 (가제)	O (참여)	연구개발 필요성 및 시급성이 높으므로 사업 참여와 예산투입 적극 지원	일반회계	115 (~2027년)
해양수산부	차세대 사이버위협 대응 기술 개발 사업 (가제)	O (참여)	연구개발 필요성 및 시급성이 높으므로 사업 참여와 예산투입 적극 지원	일반회계	115 (~2027년)
세종특별 자치시	–	△ (참여)	연구개발 필요성 및 시급성이 높으므로 인프라 활용 및 실증·테스트 적극지원	–	–

제4장 성과 활용방안 및 기대효과

제1절 사업 성과 활용방안

❑ 최종 연구개발 성과

ㅇ 암호화된 사이버공격 탐지·대응 기술 및 범부처 공유·협력 플랫폼

최종 연구개발 성과 형태	○ AI기반 암호화 공격 탐지·대응 모델 (S/W) ○ 암호화 공격 탐지·대응 솔루션 (H/W, S/W) ○ 데이터 및 공격 정보 공유·협력 플랫폼 시스템 (H/W, S/W 및 활용 매뉴얼)
최종 연구개발 성과 주요 용도 및 기능	○ 암호화 트래픽·디바이스 행위 데이터셋 ○ 암호화 악성·공격 행위 탐지·차단 (비복호화) ○ 암호화 기반 악성·공격 행위정보 설명 표준화 포맷 및 행위 탐지규칙 ○ 공유·협력 플랫폼 기반 데이터 전송·공유·저장
최종 연구개발 성과 목표 성능	○ 탐지모델 구축을 위한 대용량 데이터셋 - 악성·공격 행위 20종 · 디바이스 10종 이상 ○ 암호화 악성·공격 행위 탐지 모델 정확도 - 복호화 탐지 대비 90% 이상(복호화 적용 후 평문기반 IDS/IPS 장비 활용 기준) ○ 암호트래픽 전용 표준탐지규칙 수 - 80개 규칙 이상 (20종 대응 X 4개 환경) ○ 악성·공격 행위 탐지 기술 실증 및 유효성 검증 환경 - 8개소 이상 (4부처 X 2개 환경)
최종 사용자 (목표 수요처)	○ 국가과학기술연구망 및 과기정통부 산하 연구기관 - 과학기술연구망 활용 산·학·연 200여개소 및 과학기술사이버안전센터 관제 대상 62개소 ○ 부처별 공공 서비스·인프라 - C-ITS 통합관제센터 (국내 고속도로 및 시범운영 인프라 2개소) - LTE-M 제1, 2운영센터 및 기지국 263개소, 연안 선박 3천대 이상 - 스마트 City 도시통합정보센터 관제대상 CCTV(약 2000대), 교통장치 (약 500대) 등을 포함한 5-1생활권 국가시범도시 IoT 인프라 ○ 공공분야 각급 보안관제센터 - 국가 정보보호지침에 따라 운영되는 공공기관 보안관제센터 40여개소 ○ 국가기반시설 및 주요정보통신기반시설 등 - 행정안전부 국가정보자원관리원, 산업통상자원부 관할 발전소, 국토교통부 관할 공항 등 주요 국가기반시설 - 통신교환국, 정수장, 병원 등을 포함한 주요정보통신기반시설 통신망

생산 주체	○ 다부처 참여 기관: 탐지 원천기술 및 최적화 모델 ○ 다부처 참여 기업 및 용역: 관련 시스템 구성 S/W 및 H/W
전달 및 구매 체계	○ 공공분야 각급 보안관제 센터: 정부·부처 공공재로 조달하여 제공 ○ 대국민 공공 서비스·인프라 및 기반시설: 정부·부처 공공재로 조달하여 제공 ○ 민간 주요 대국민 서비스·인프라: 정부·부처가 일부 보조하여 시장구매 유도 ○ 민간 일반 서비스·인프라: 100% 민자 또는 시장구매(소비자 구매) 방식

❑ 공동사업 성과 관리 및 활용 방안

ㅇ 국가·공공 분야 대국민 서비스 및 기반 인프라의 사이버 공격 보호를 위해 원천기술 확산 및 플랫폼 현업화 추진

- 행위 기반 암호트래픽 보안관제 기술은 관계부처들이 수요처이자 연구·개발자이기 때문에 관계부처들이 운영하는 대국민 서비스·인프라에 실증 환경 구축 및 단계별 적용

- 주무부처 및 개발·수요기관의 성과 적용·검증 대상으로 활용 구간 확정

[표 26] 부처별 연구 성과 적용 및 활용 구간

주무부처	개발·수요기관	성과 적용·활용 구간
과학기술정보통신부	한국과학기술정보연구원	국가과학기술연구망(KREONET)* 보안관제 대상기관
국토교통부	한국도로공사	C-ITS 시범운영 구간 중 실증 구간 선정(논의 중)
해양수산부	선박해양플랜트연구소	LTE-M 활용 국가 관공선 및 해양대학교 항행실습선
세종특별자치시	도시성장본부	세종시 內 스마트 City 통신망 관제 영역
기타 국가·공공 분야 全부처	부문보안관제센터	각 부처의 보안관제센터가 담당하고 있는 관제 네트워크

* 국내·외 연구자들에게 첨단과학 및 응용연구 수행을 지원하는 국가 R&D 연구망

ㅇ 국내 유관기관 및 관계기업 기술지원

- 원천·요소기술 활용 방안: 본 사업은 공급·수요처 일원화 기반 실증 중심 연구를 수행 예정으로 실제 제품화 수준에 근접한 연구 성과를 창출할 것으로 기대

- 연구 성과를 기반으로 보안솔루션 개발 등에 활용 가능할 것으로 예상되며, 보안장비·솔루션 제작 관련 기업·연구소와의 연계를 통해 개발 과정에서 추가 기술개발 이슈 및 기능 고도화가 자연스럽게 이루어질 것으로 기대

- 개발 원천·요소기술 활용 상용화 모델 및 수요처(예상)

[표 27] 원천 및 요소기술 활용 상용화 및 예산 수요처

제품 및 요소기술	상용화 모델	예상 수요처
· 트래픽 수집 및 암호화 트래픽 식별 기술	H/W모듈 및 S/W library, 기술 이전 등	네트워크 장비 및 보안장비 · 솔루션 제작 업체
· 암호화 트래픽 분석 노하우		
· 비복호화 기반의 악성 암호화 트래픽 식별 기술		

ㅇ 암호화통신 기반 악성·공격 행위 탐지 원천기술 및 관련 제품 해외수출

- 신규 시장인 암호화통신 기반 정보보호 장비·솔루션의 국제적 기술선도 및 시장 선점 효과 기대

- 테스트베드 및 실증시험을 통해 검증된 기술을 본 사업에 참여하지는 않았으나 유사한 환경을 보유한 각 부처에 전파·공유 하여 국가적인 정보보호 역량 증대 추진과 이를 기반으로 한 수출시장 확대전략 확립

ㅇ 암호화통신 기반 악성·공격 행위 분석·탐지 인력양성 및 일자리 창출

- 국내 정보보호 업계로의 기술 지원·전파를 실시하여 관련 시장 활성화 및 신규 일자리 창출 효과 기대

- 보안관제 업무 인력의 역량 향상을 위한 기술 교육 및 신규 정보보호 인력 양성을 통한 공공·민간 분야 취업난·구직난 해소 기여

제2절 기대효과

❑ 기술적 측면

○ 폭발적으로 증가하는 암호통신에 따른 보안성 강화 및 사이버공격 탐지 기술 부재로 인한 보안문제를 해결할 수 있는 **핵심 원천기술 선도적 확보**를 통한 **'국가 사이버안보 자주권 확보'** 기여

- (**패러다임 전환 원천기술 확보**) 폭발적으로 증가하는 암호화된 사이버 공격을 선제적으로 분석·탐지·대응할 수 있는 **차세대 사이버보안 원천기술** 확보 및 국내 기업의 **글로벌 기술경쟁력** 확보

- (**기술 완성도 제고**) 부처 간 **긴밀한 협력을 기반으로 대규모 실제 인프라·데이터**를 활용한 R&D를 수행함으로써 개발된 기술의 **완성도 제고**

- (**국가 사이버안보 자주권 확보**) 사이버안보 패러다임 전환을 위한 **핵심기술을 국산화 및 조기 확보**함으로써 해외 기업의 기술종속에 따른 **제2의 화웨이 사태를 미연에 방지**하고 국산 장비를 활용한 **자주적 사이버안보 체계 구축·운영** 가능

<그림 67> 기술적 측면 기대효과

※ 특히 보안장비는 모든 기관에 설치·운영되고 송·수신되는 모든 데이터를 모니터링하기 때문에 해외 기업에 기술종속이 될 경우 국가 안보에 심각한 타격을 받음

※ 기존 평문기반 보안관제 체계와의 연동 및 공유·협력 체계를 바탕으로 한 **차세대 국가 보안관제 체계 선도** 기대

※ 암호화 트래픽의 비복호화 기반의 분석을 시도함으로써 **국민의 개인정보 유출 등 2차 피해 방지**

❑ 사회적 측면

ㅇ **대규모 재난·재해급의 사회적 혼란**을 초래할 수 있는 암호화통신 기반 사이버 공격을 조기에 탐지·대응함으로써 대국민 **'디지털 안심국가 실현'** 기여

- (**디지털 안심국가 실현**) 모든 사물이 네트워크로 연결되는 4차 산업혁명 시대의 **대국민 공공 인프라·서비스에 대한 보안성 및 안전성**을 확보함으로써 **디지털 안심국가를 실현**

- (**국민의 생명과 안전 보장**) **대규모 재난·재해급**의 사회적 혼란을 초래할 수 있는 암호화된 사이버공격을 조기에 탐지 및 대응함으로써 **국민의 생명과 안전을 보장**하고 **삶의 질 제고에 기여**

- (**코로나 시대 사이버안전 확보**) 암호화 통신 기반의 온라인 서비스가 폭증하는 코로나 시대에 재택근무, 화상회의, 원격접속 등 **대국민 업무·생활 서비스의 안전한 이용**환경 제공에 기여

※ 보안관제 업무 인력의 역량 향상을 위한 기술 교육 및 신규 정보보호 인력양성을 통한 공공·민간 분야 **취업난·구직난 해소 등 사회문제 해결에 기여** 가능

※ 악의적인 암호화기반 악성코드·랜섬웨어 유포 등을 사전에 방지하고 신종 범죄로 연결을 차단하는 등 **추가적인 피해 예방과 범죄율 감소 효과** 기대

<그림 68> 사회적 측면 기대효과

❑ 경제적 측면

○ 암호화통신 기반 사이버공격으로 발생 가능한 대규모 피해를 사전에 방비함으로써 경제적 **피해 최소화 및 복구비용 절감**, 유사 연구개발 중복투자를 원천 차단하여 **국가예산 절감 및 신규 일자리 창출** 기여

- (**예산 절감**) 다부처사업 추진을 통한 유사 R&D 사업 **중복투자를 원천 차단**하여 **국가 R&D 예산을 절감**하고 **연구수행 효율화 향상**

- (**경제적 피해 최소화**) 재난화·대형화되는 사이버위협을 사전에 차단 또는 조기에 탐지·대응함으로써 발생 가능한 **경제적 피해 규모를 최소화**하고 **복구비용을 절감**

- (**사이버안보 산업 발전**) 약 7조원 규모의 국내 **사이버안보 산업의 발전**에 기여하고 국내 기업의 **해외시장 진출을 통한 수출증대** 및 **글로벌 기업으로의 성장**을 위한 기반 마련

※ 국내 정보보안 솔루션·장비 시장 규모: 약 6조 414억원 (2021 국내외 보안시장 전망보고서, 보안뉴스)

※ 글로벌 정보보안 시장은 연평균 10%이상 성장 중이며, 특히 본 과제에서 주요 대상으로 선정한 **IoT 보안시장은 연평균 33.7%의 급속한 성장**을 기록중 (MarketsandMarkets, 2018.09.)

※ 현재 웹사이트 통신 중 암호화 트래픽 사용량 95% 이상 (2021, Google)으로 향후 평문통신이 더 이상 사용되지 않을 것으로 예상됨에 따라 **기존 보안장비 교체·대체 수요 발생 여지 충분**

<그림 69> 경제적 측면 기대효과

❑ 실용·사업화 측면

○ 국가·공공 분야를 비롯한 민간 분야로 원천기술 전파를 통해 암호화된 사이버 공격에 대한 **국가 차원의 대응력 향상 및 사이버안보 공동연구 체계 구축** 추진

- (**범국가적 대응체계 구축**) 대국민 공공 서비스·인프라에 대한 암호화된 사이버 공격을 선제적으로 분석·탐지·대응하기 위한 **범국가적 차원의 일원화된 공동대응 체계 구축** 및 **사이버안보 역량 강화**에 기여

※ 과학기술정보통신부 활용 예시 : 소관 보안관제센터(과학기술정보통신사이버안전센터, 우정사업사이버안전센터 등)에 선도적으로 적용·검증한 후, 민간분야(KISA 협력) 등에 보급

- (**기술·서비스 경쟁력 강화 및 일자리 창출**) 핵심 원천기술을 국내 보안장비 제조사, 보안솔루션 공급사, 보안관제 전문기업 등에 기술이전을

실시함으로써 **제품·서비스의 기술 경쟁력 강화** 및 새로운 **일자리 창출 기회** 마련

※ 현재 Cisco 社 Catalyst 9000 Series 제품군을 통해 암호화 트래픽 분석(ETA) 기반의 정보보호 솔루션 · 장비 분야 사실상 시장독점 체제

※ 정보보호 분야는 국가 주도의 공공수요가 필수적으로 존재하여 관련 기업의 성장 가능성이 높고, 원천기술의 spin-off화에 따른 신규 응용시장 및 부가가치 창출을 통한 기업들의 경쟁력 강화에 기여 가능

<그림 70> 실용 · 사업화 측면 기대효과