보안 솔루션의 새 길을 여는 제너시스템의 다중영역 네트워크 보안 솔루션 IEUMnet



[다중영역 네트워크 보안 기반]

CCTV망 통신망 보안강화

★"국정원 보안요구사항 V3.0 규격"인증 솔루션

JENER SYSTEM

CONTENTS

IoT 환경 단말(CCTV, IP카메라 등) 침입/해킹 차단 솔루션



01 CCTV망 보안강화 개요

02 CCTV망 보안강화 배경

03 CCTV망 보안강화 IEUMnet

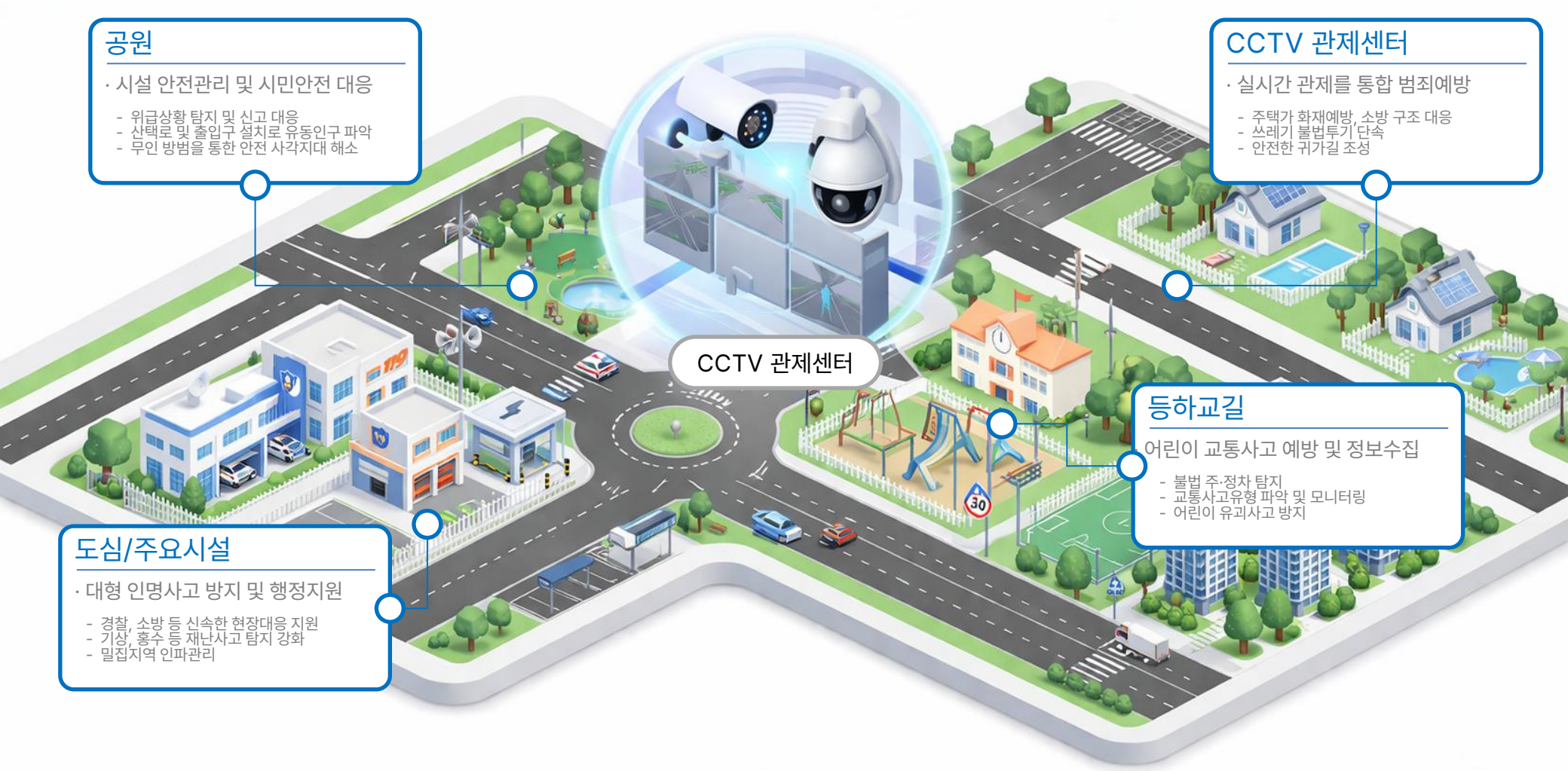
04 CCTV망 보안강화 구축실적

05 CCTV망 취약점 모의침투 테스트

01 CCTV망 보안강화 개요

01 CCTV 통신망 보안강화

CCTV는 우리의 일상 속에서 **국민의 안전**을 책임지고 있습니다.



02 CCTV 통신망 보안강화

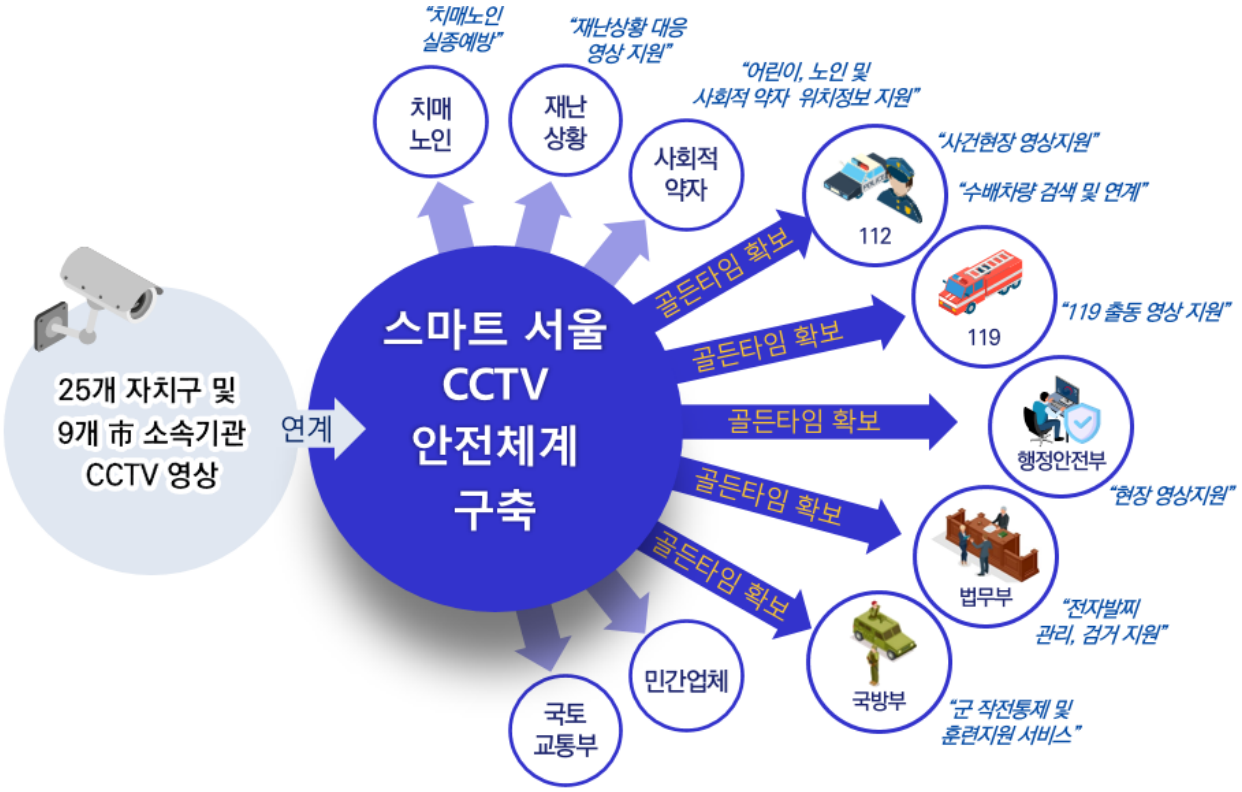
개요

CCTV는 우리의 일상 속에서 **국민의 안전**을 책임지고 있습니다.

국민의 안전을 위해 운영중인 CCTV 영상정보는 방범과 어린이 보호, 도시공원·놀이터, 쓰레기 투기단속, 교통단속 및 교통 정보 수집·분석뿐만 아니라, AI기반 지능형 선별관제를 통해서 범죄예방과 폭행, 배회, 쓰러짐 등 긴급 상황을 신속 감지하고 즉각 대응함으로써 시민의 안전을 위해 중요한 역활을 하고 있습니다.

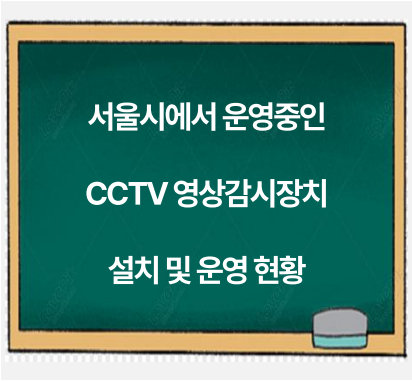
디지털 안전도시 CCTV 안전망 서비스

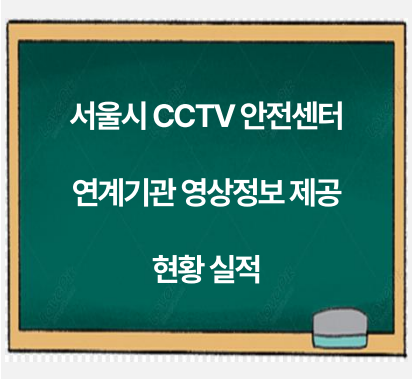




03 CCTV 통신망 보안강화

사업 배경





서울시에 설치된 CCTV 영상감사장치는 2023년 12월말 17만 7,000여대 설치 운영하고 있으며, 서울시 CCTV 안전센터 통합플랫폼을 통해서 414만 5,582건의 영상정보를 유관기간과 연계하여 제공함으로써 시민안전에 힘쓰고 있습니다.

서울시 CCTV 설치 현황(단위 : 대, 2025년 12월 31일 기준)

구 분	CCTV 총계	범죄예방 및 수사					시설안전·화재예방	교통단속	교통정보수집·분석	기타 다른법령
		소 계	방범	어린이 보호구역	공원·놀이터	쓰레기 무단투기				
자치구	122,613	108,947	80,885	8,874	18,327	861	4,426	8,811	153	276

서울시 CCTV 설치 현황(단위 : 대, 2024년 12월 31일 기준)

구 분	CCTV 총계	범죄예방 및 수사					시설안전·화재예방	교통단속	교통정보수집·분석	기타 다른법령
		소 계	방범	어린이 보호구역	공원·놀이터	쓰레기 무단투기				
자치구	113,273	99,758	74,807	8,704	15,417	830	4,482	8,648	18	367

02 CCTV망 보안강화 배경

01 IEUMnet 개발배경

사업의 필요성_CCTV망 보안강화

"공공기관의 보안 시스템은
유연성과 효율성 유지
내부자 위협과
외부 공격에 대응할 수 있는
강력한 보안솔루션이 필요합니다"

AS-IS

보안 취약점(원격지, 무인개소)

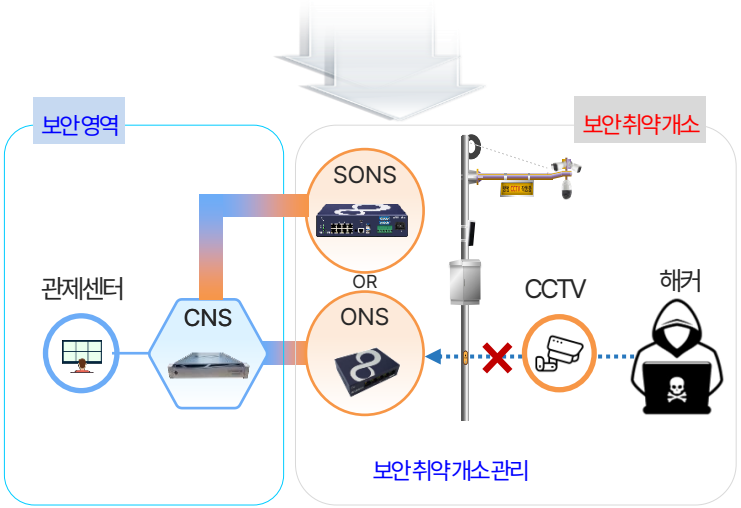
- 다수의 CCTV망내 현장시설물 보안의 빈틈 발생
- 보안 취약 개소 관리의 어려움
- 보안 취약경로를 통한 접근시도 가능성 존재



TO-BE

보안 취약개소 관리

- 불법 보안 취약경로 완전 차단 **안전한 관리**
- CCTV망 구간 데이터의 신뢰성, 무결성 보장
- 비보안/보안영역의 **폐쇄성, 독립성 유지**



※ CCTV → ONS → SWITCH → 방화벽 → CNS
※ CCTV → SONS → 방화벽 → CNS

01 IEUMnet 개발배경

사업의 필요성_CCTV망 보안강화(계속)

"공공기관의 보안 시스템은

유연성과 효율성 유지

내부자 위협과

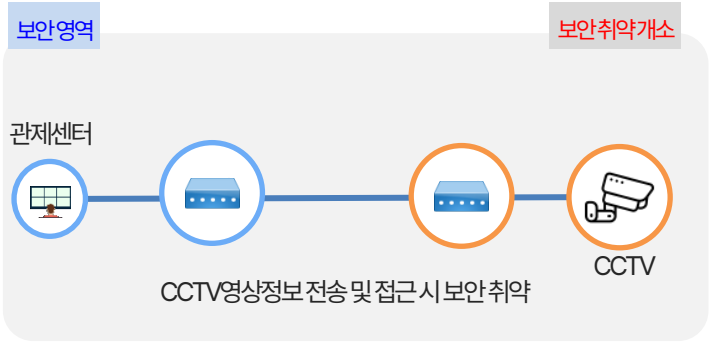
외부 공격에 대응할 수 있는

강력한 보안솔루션이 필요합니다"

AS-IS

영상데이터의 안전성 신뢰성 보안 필요

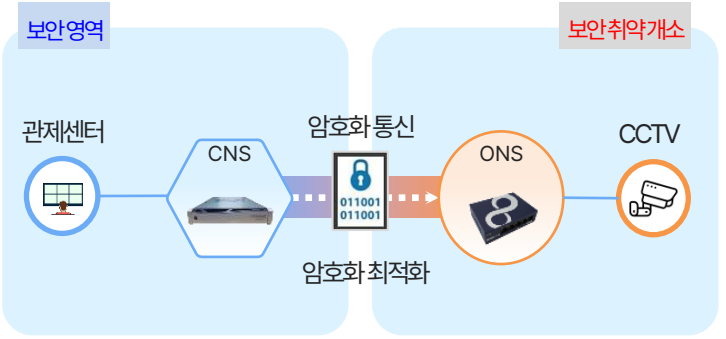
- 폐쇄망 운영에 따른 네트워크 구간 보안 취약점 발생
- CCTV영상정보 전송 시 무결성, 신뢰성 확보 필요
- CCTV망 네트워크 구간 보안에 대한 인식 저하



TO-BE

CCTV 영상정보의 무결성 및 신뢰성 확보

- CCTV망 보안성이 검증된 암호화 통신
- 단방향 통신의 장점 극대화로 폐쇄성 확보
- 성능 저하 최소화를 위한 최적의 설계



01 IEUMnet 개발배경

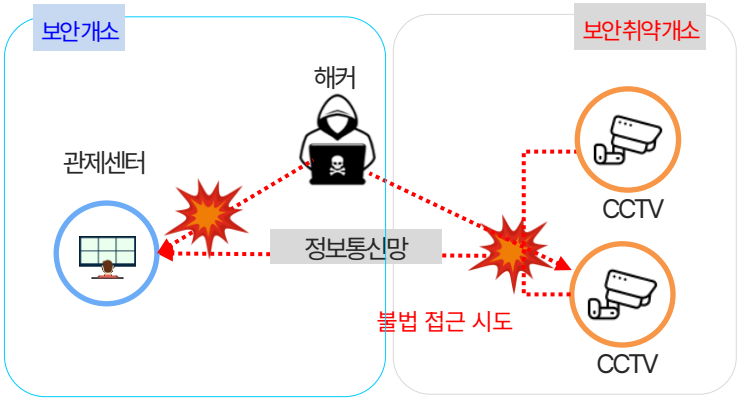
사업의 필요성_CCTV망 보안강화(계속)

"공공기관의 보안 시스템은
유연성과 효율성 유지
내부자 위협과
외부 공격에 대응할 수 있는
강력한 보안솔루션이 필요합니다"

AS-IS

보안 취약점(원격지, 무인개소)

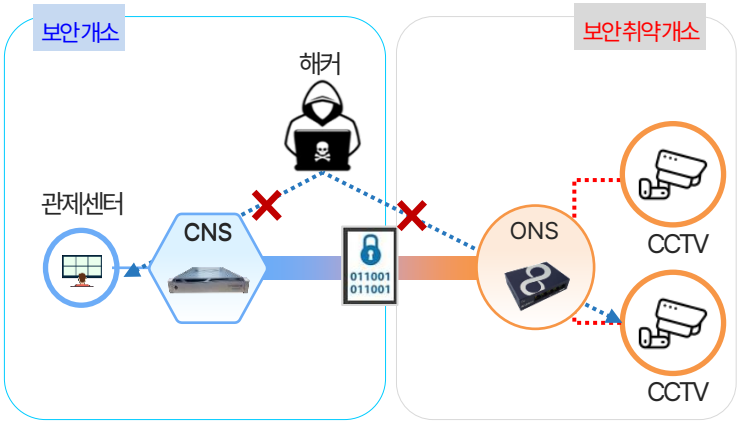
- 정보통신망(임대망, 자가망) 보안의 빈틈 발생
- 다수의 보안 취약 개소 관리의 어려움
- 보안 취약경로를 통한 접근시도 가능성 존재



TO-BE

보안 취약개소 관리

- 보안 취약개소의 **안전한 관리**
- 다수의 취약개소의 1: N 중앙 통제 보안 관리
- 데이터의 신뢰성, 무결성 보장
- 비보안/보안영역의 **폐쇄성 유지**



02 CCTV 설치 현황

배경

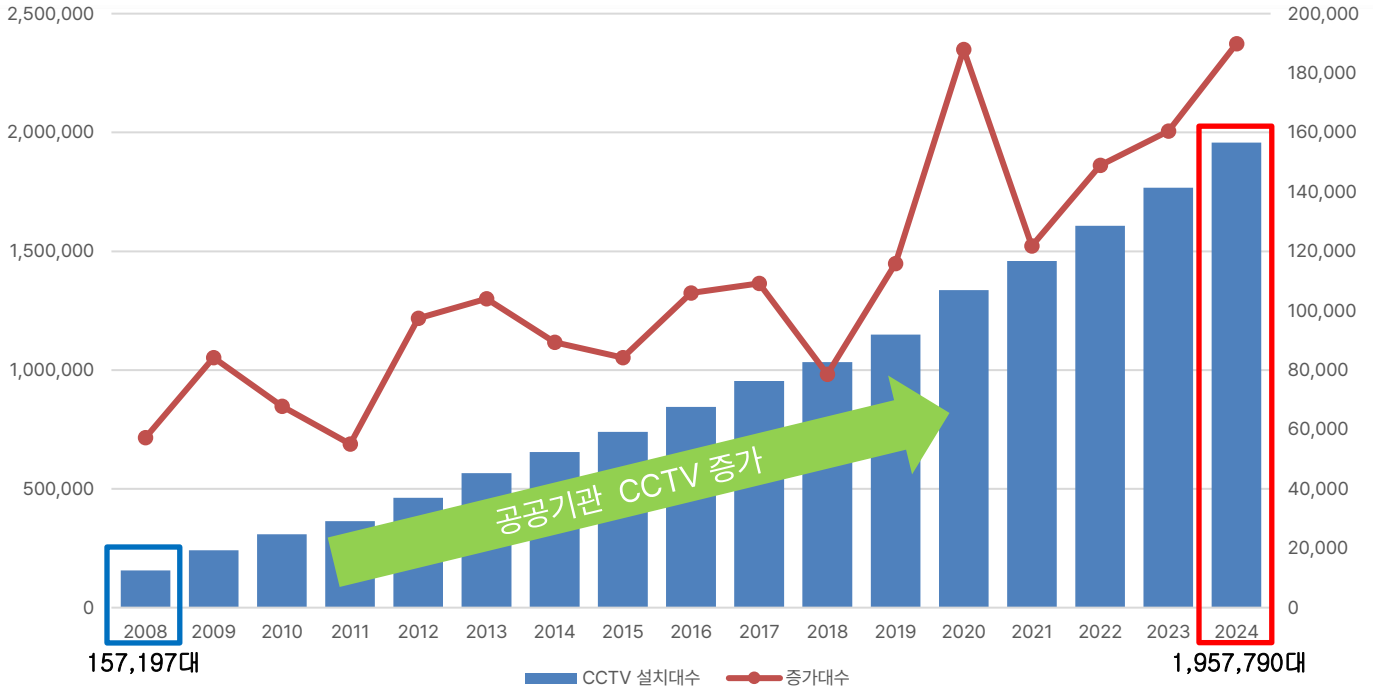
출처 : e-나라지표

(지표서비스Ie나라지표

(index.go.kr))



공공기관 CCTV 설치 및 증가대수



출처 : 실태조사 및 개인정보보호 종합지원시스템 현황자료

연간 평균 CCTV 10%이상 증설 및 성능개선

(단위 : 대)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
총 CCTV 설치대수(대)	157,197	241,415	309,227	364,302	461,746	565,723	655,030	739,232	845,136	954,261	1,032,879	1,148,770	1,336,653	1,458,465	1,607,388	1,767,894	1,957,790
전년대비 증가대수(대)	57,240	84,170	67,812	55,075	97,444	103,977	89,307	84,202	105,904	109,125	78,618	115,891	187,883	121,812	148,923	160,506	189,896
전년대비 증감비(%)	57.3	53.6	28.1	17.8	26.7	22.5	15.8	12.9	14.3	12.9	8.2	11.2	16.4	9.1	10.2	10	10.7

출처: 실태조사 및 개인정보보호 종합지원시스템 현황자료

주석: 공공기관 CCTV 설치 및 운영현황은 2011년(2010년 자료)까지는 공공기관별로 조사 · 수합하였으나, 2012년(2011년 자료)부터는 공공기관이 매년 3월말까지 개인정보보호종합지원시스템에 현황을 등록함

02 CCTV 설치 현황

배경

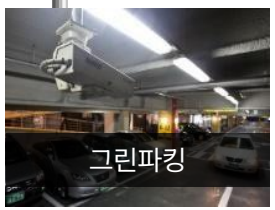


연간 평균 CCTV 10%이상 증설 및 성능개선











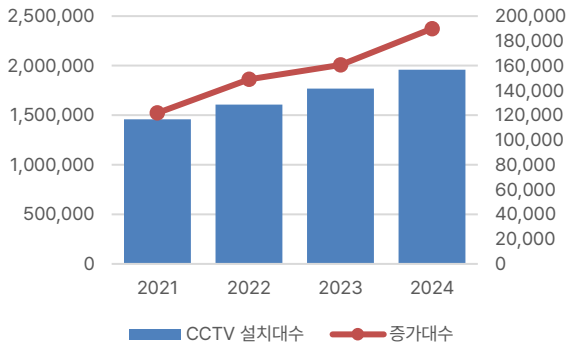




공공기관 CCTV 설치대수

	2021	2022	2023	2024
총 CCTV 설치대수(대)	1,458,465	1,607,388	1,767,894	1,957,790
전년대비 증가대수(대)	121,812	148,923	160,506	189,896
전년대비 증감비(%)	9.1	10.2	10	10.7

공공기관 CCTV 증가 차트

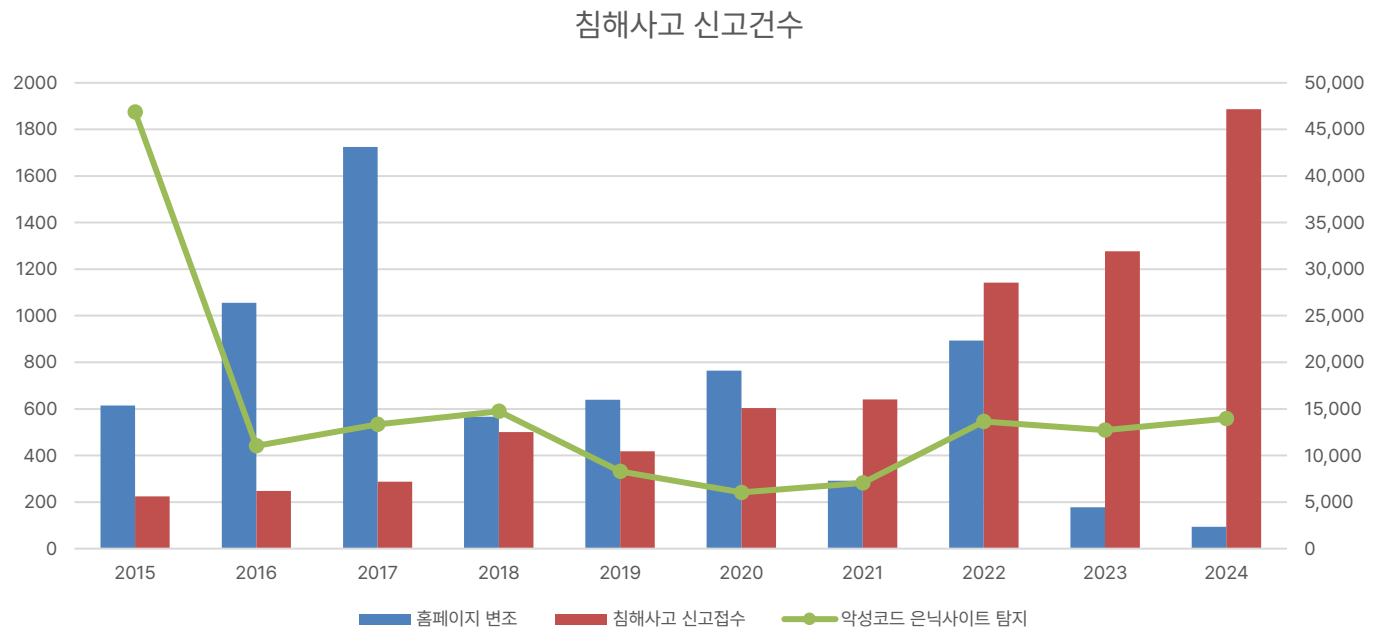


출처 : e-나라지표
(지표서비스 : I e-나라지표(index.go.kr)

03 피해사례

침해사고 신고건수 통계

해킹사고 건수 지표는 한국인터넷진흥원 국내 홈페이지 변조가 발생한 사이트를 탐지하여 조치 한 건수, 국내 홈페이지를 대상으로 악성코드 은닉사이트를 탐지하여 조치한 건수, "정보통신망법" 에 근거 하여 민간분야 (기관 및 기업)에서 발행한 침해사고에 대한 신고 받은 건수들의 합입니다.



침해사고 신고건수

출처 : 한국인터넷진흥원

구 분	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
홈페이지 변조	615	1,056	1,724	567	639	764	292	893	178	94
침해사고 신고접수	225	247	287	500	418	603	640	1,142	1,277	1,887
악성코드 은닉사이트 탐지	46,850	11,044	13,347	14,754	8,299	6,034	7,043	13,661	12,731	13,967

04 도입 필요성

도입 필요성

CCTV 통신망 보안강화를 통해 기술적 보안문제를 해결해야 합니다.

- 24시간 365일 무인 원격지로 운영중인 CCTV망(**CCTV 카메라** ⟷ **통합관제센터 네트워크 구간)**에 대해
  - 비인가 및 불법 보안 취약경로를 통한 접근 통제
  - 암호화 통신을 통한 긴밀성 보장과 안전한 네트워크 구간 확보
  - AI 기반의 CCTV 영상데이터에 대한 신뢰성 무결성 보장
- 안전한 CCTV 운영에 대한 보안 취약점 개선

강력한 보안 시스템 도입을 통한 기술적 보안 강화로 침해 보안 사고 방지



물리적/기술적/관리적 보안 강화로
보안유출사고 방지

CCTV망 + IEUMnet

- 침입/해킹방어시스템 확충
- 보안취약점 해소

1 Step 물리적 보안강화

건물, 설비와 같은 물리적 정보 시스템 자산을 보호

- 시스템실 장비보안
- 출입 통제감시
- 서버 접근통제 및 시스템 보안대책
- 각종 장비 및 설비 시건 장치 보호

2 Step 기술적 보안강화

침해 및 해킹 등으로부터 보호하기 위한 기술적 통제

- 네트워크 구간 암호화
- AI기반 트래픽 이상탐지
- 네트워크 구간 불법접근 통제
- 관리 취약개소 보안강화

3 Step 관리적 보안강화

물리적, 기술적 보안을 수행하기 위한 관리적 보안체계

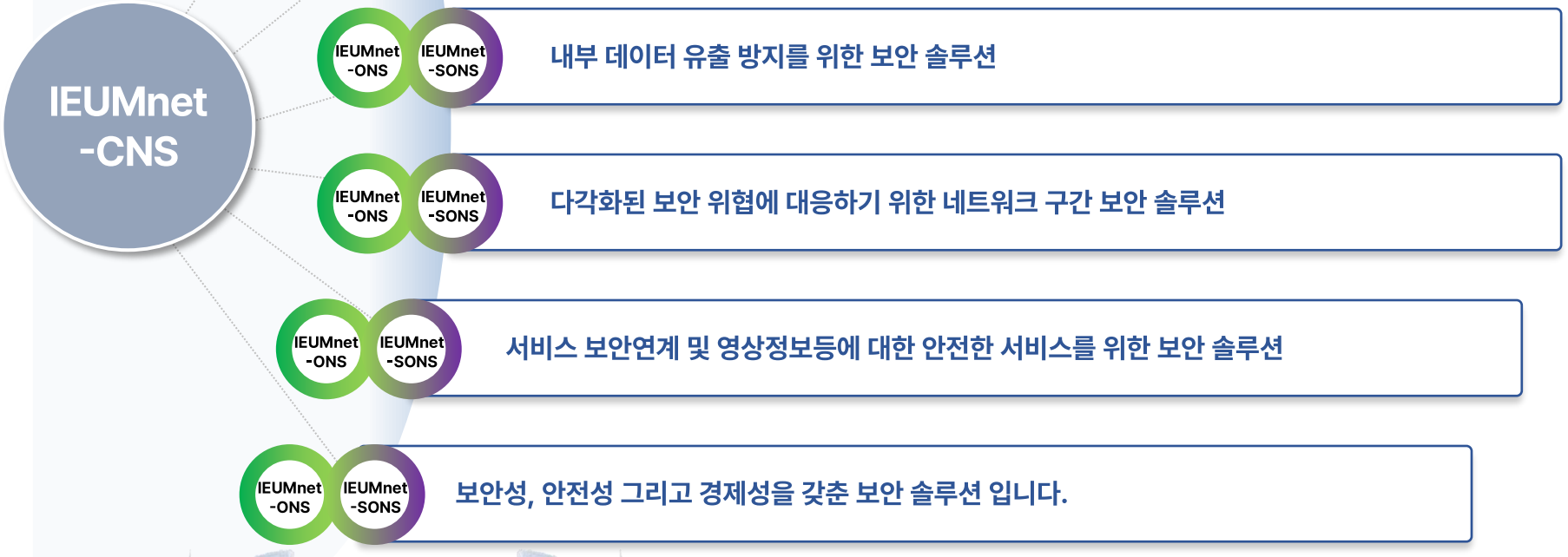
- 내부 직원 및 외주 인력관리
- 정보 보호 문서화
- 개인정보보호법 교육 및 훈련
- 보관, 변조 대비 주기적인 백업

03 CCTV망 보안강화 IEUMnet

01 CCTV보안 IEUMnet

IEUMnet

Zero Trust Network Security



02 IEUMnet 핵심특징

핵심특징



IEUMnet 은

검증된 보안솔루션
- 국정원 보안기능확인서 인증
- GS 1등급 소프트웨어 품질 인증
- 서울시 지자체 등 현장 검증 완료

다중영역 네트워크 보안
- 비 보안 영역을 1:N 다중영역 연계 구성
- 다수 외부 단말의 안전한 보안 연결
- 유연한 확장 연계성 보장

망분리
- 분리된 다중영역 네트워크 보안 환경 구현
- 외부 해킹 원천 차단
- 전용 암호화 프로토콜 사용

보안 강화된 VPN 구성
- 보안 강화된 VPN 구현 가능
- 국정원 보안 지침 준수
- 보안성 강화와 세션, 보안정책 취약점 해소

내부 정보시스템 보호
- 데이터 전송 전 악성코드 사전 검출
- 단방향 통신, 세부화 정책 해킹 방지
- 내부자 보안정책을 통한 자료 유출 방지

안전한 관리 / 서비스 연속성
- 보안 개소별 독립성, 폐쇄성 운영 환경
- 외부 공격 원천 차단 준수
- 통합 정책 운영 및 관리

국내최초



망간자료전송제품 부문
보안기능 확인서
인증

국정원 보안요구사항
V 3.0
만족 제품

1등급 GOOD Software

GOOD Software
GS 1등급
소프트웨어 품질 인증



02 IEUMnet 핵심특징

핵심특징

보안이 취약 또는 필요한 다수의

현장 개소의 통합 보안관리를

위해서

IEUMnet 은

CCTV 현장개소 원격지

무인개소 등

폐쇄적 독립적 구성 운영으로

외부접근 차단

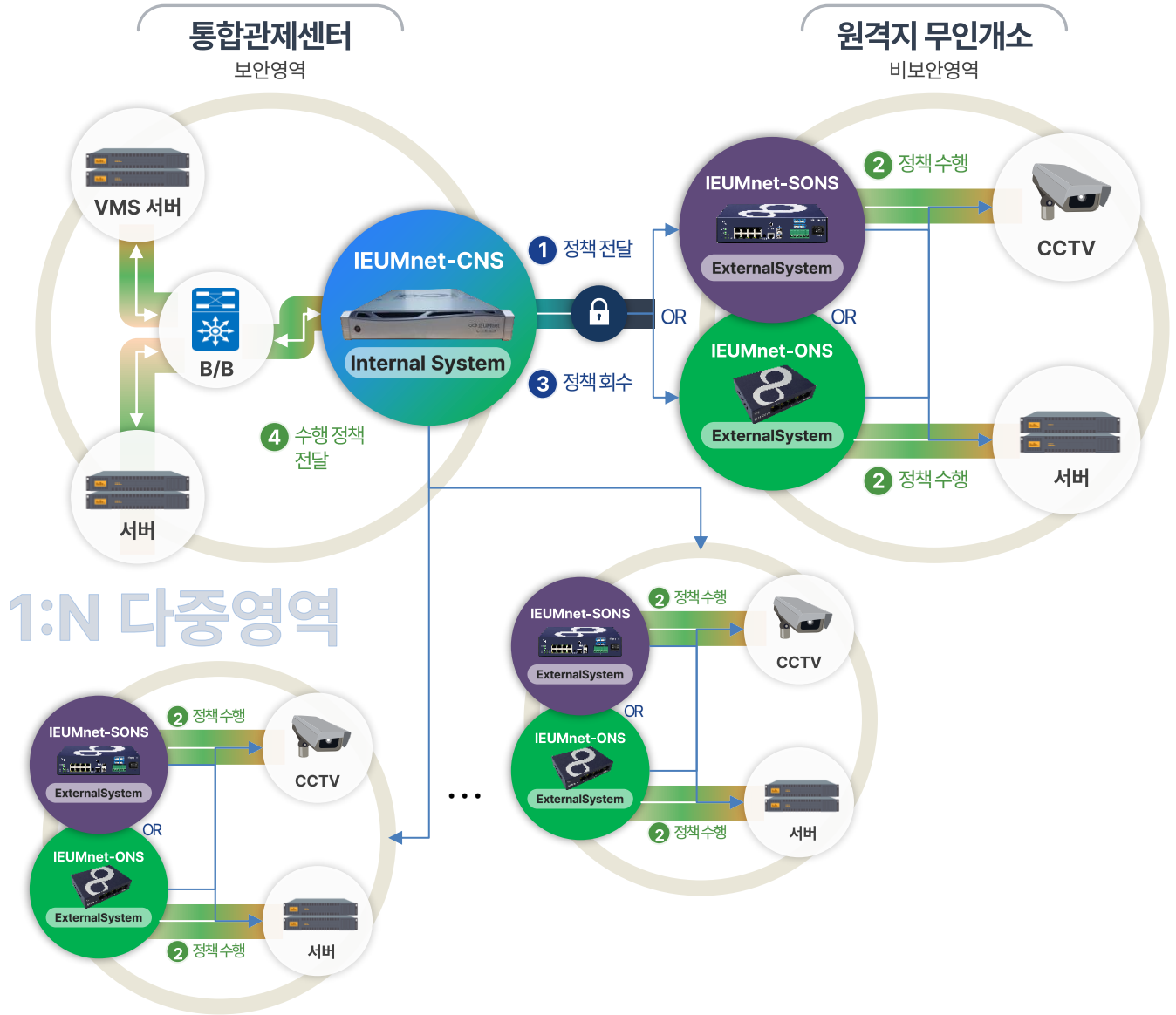
검증된 암호화 통신으로

안전한 데이터 전송 구현

보안성을 높이고

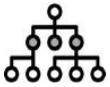
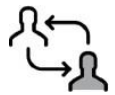
안전한 서비스 연속성을

제공하는 솔루션



03 CCTV망 보안강화 적용 시스템

IEUMnet 적용분야

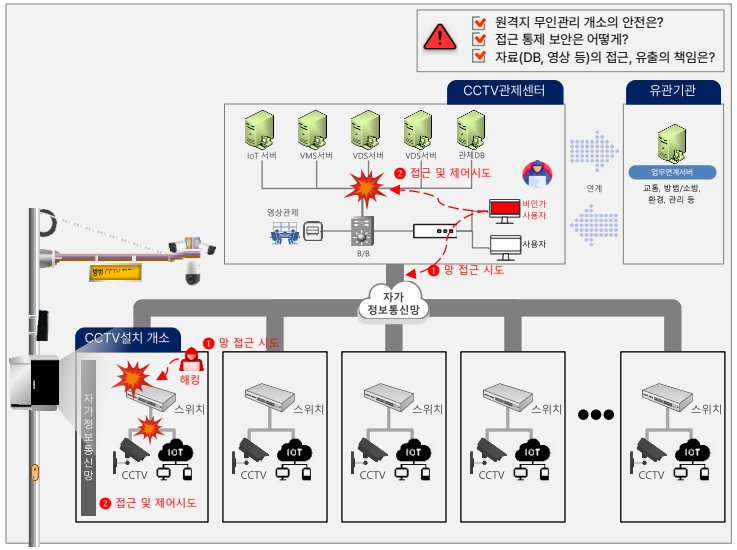
 재택 근무	재택근무 시 불안한 VPN 말고 물리적인 이음넷을 이용해 집에서 내부 업무시스템에 접근하여 관리 및 이력 등 로그를 남김으로 써 안전 사용	 유무선 통합	LTE망 등 무선망과 유선망에서 유연하게 사용할 수 있습니다.
 지점 연계	본점과 지점간 네트워크 연결 시 VPN 보다 보안레벨이 더 높은 이음넷 사용	 해외근무자	해외 근무 중 내부 업무 시스템에 접근시 이음넷을 사용함으로써 관리의 명확성 보안의 안전성을 높일 수 있습니다.
 민원발급	민원 발급 시스템이 불안한 VPN으로 네트워크 구성되어 있는 점을 이음넷으로 대체할 수 있습니다.	 제어망	저수지, 한전망 등 원격 제어망에서 단방향 통신하는 이음넷으로 구성하여 보안성을 높일 수 있습니다.
 ATM 기기	전국의 ATM 기기 시스템이 불안한 VPN으로 네트워크 구성되어 있는 점을 이음넷으 로 대체할 수 있습니다.	 보안시스템 및 인프라 구축	통합망등의 인프라 구축시 서로 다른 망간 보안의 벽을 세울 시 이음넷으로 구성할 수 있습니다.

03 CCTV망 보안강화 적용 시스템

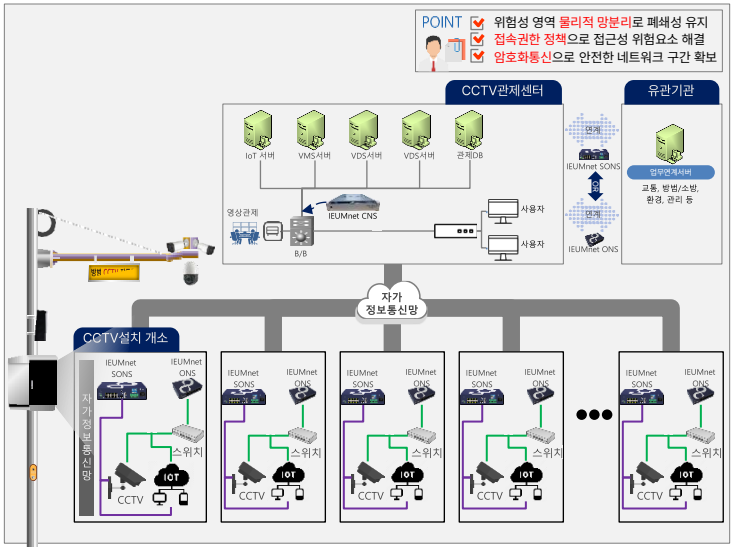
CCTV망 보안강화 구성도

CCTV 구간과 내부망 사이 망을 분리해 줌으로써 CCTV 구간에서 유입되는 바이러스 및 해킹을 원천 차단하여 지자체 전산자원을 보호할 수 있습니다.

BEFORE



AFTER



CCTV망 보안 문제점

- CCTV 설치 개소 및 원거리 무인 관리 개소의 네트워크망 접근에 대한 보안 문제
  - CCTV 카메라 접근 및 제어를 통해 피해 발생
  - 취약지점 및 비업무시간대 불법 접근 통제에 때란 취약점 발생
- 악의적 내부 사용자 및 비인가 사용자의 내부 시스템 접근 보안 문제
  - 시스템 접근을 통해 내부정보(DB, CCTV 영상등) 유출 피해 발생
  - 운영중인 시스템의 의도적 장애 발생(시스템 Shut down, 정책 변경)으로 피해 발생

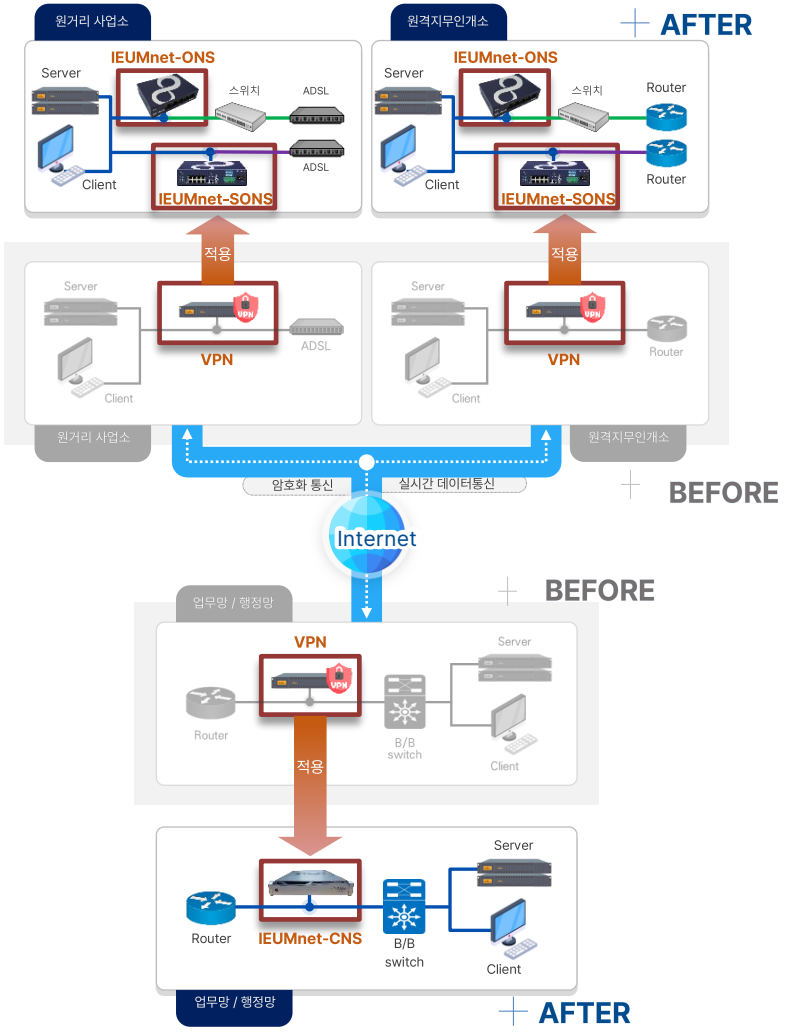
IEUMnet을 통한 CCTV망 보안 해결 방안

- CCTV 관제센터 및 원거리 무인 관리 개소간 검증필 암호화 통신 으로 네트워크 구간 안전성 확보
  - 화이트리스트 기반 관리로 등록 기기와 정책 통신으로 CCTV 카메라 접근 문제 해결
  - 비보안/보안 개소의 폐쇄성 유지로 통신망내 불법 CCTV 접속 및 접근 보안 원천 차단
- 내부통제시스템을 향상 시켜 운영중인 시스템 안정성 및 서비스 연속성 제공
  - 정책 변경 2차 인증을 통한 권한 강화를 통해 내부정보(DB, CCTV 영상등) 접근 및 유출 문제 해결
  - 비인가 연계/접속/차단에 대한 보안 감사 기록, 통합 정책, 통합관리로 안전한 운영관리 방안 확보

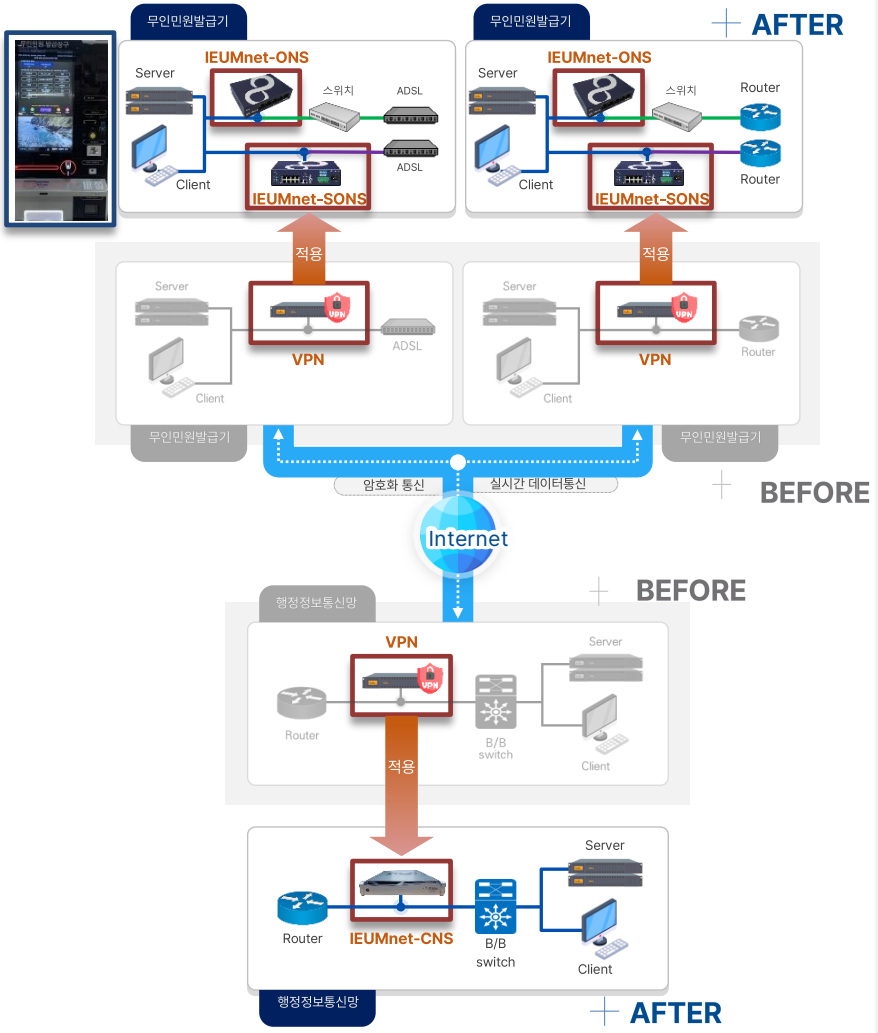
03 CCTV망 보안강화 적용 시스템

VPN 네트워크 구간 보안성 강화

VPN망 취약점 보안 강화를 위한 목표구성도



보안 강화된 무인민원발급기 구간 보안망 구성도



- 암호화 통신으로 안전한 네트워크 구간 확보
- TCP/IP 통신이 아닌 전용프로토콜 통신으로 물리적 폐쇄성 유지와 안전한 서비스 연속성 제공
- VPN 구간에서 인가 정책외 업무망 / 행정망으로 접속 불가 / 업무 서비스 연속성 보장
- 네트워크 접근 차단을 위해 화이트리스트 기반 관리로 등록된 기기와 정책을 통한 통신 유지
- 통합 정책 및 통합 관리로 안전한 운영관리 방안 확보

03 CCTV망 보안강화 적용 시스템

도입효과

Multi Area Network Security

IEUMnet 은

검증된 보안솔루션
IEUMnet -ONS / IEUMnet -SONS

- 검증필 암호화 통신 영상정보의 기밀성, 신뢰성 확보
- 국정원 보안 기능 확인서 인증으로 보안 지침 준수
- 현장 검증 솔루션 (서울시 및 지자체) 적용 실증 완료

보안 강화된 네트워크
IEUMnet -ONS / IEUMnet -SONS

- 물리적망분리구현으로보안강화된네트워크보안망구성가능
- 국정원 보안 지침 준수(보안기능확인서)
- 보안성 강화(OS, 개발언어) 및 보안정책으로 취약점 해소

보안 태세 강화
IEUMnet -ONS / IEUMnet -SONS

- 통합 보안 관리의 효율성 증대와 강력한 보안 제공
- 디지털 환경의 위험 구간 접근 제어, 통합 정책 관리, 최소화 정책 등으로 보안 취약점 제거를 통한 보안 태세 강화

중요한 자산 보호
IEUMnet -ONS / IEUMnet -SONS

- 통신 정책 체계 강화를 통해 외부와 연계되는 데이터, 내부 네트워크 구간의 주요관리 데이터등을 IEUMnet 핵심원칙 적용을 통해 안전하게 실시간 중요한 자산을 보호

IEUMnet-CNS



Internal System

악성 행위자의 영향 최소화
IEUMnet -ONS / IEUMnet -SONS

- 모든 액세스 요청을 명시적으로 확인하는 계층형 방어로 내외부 위험으로부터 데이터 보호
- IEUMnet 핵심원칙으로강력한보안태세, 접근성세분화, 최소화정책 적용을 통한 접근 방식으로 업무 피해 최소화의 이점

규정 준수 및 선도
IEUMnet -ONS / IEUMnet -SONS

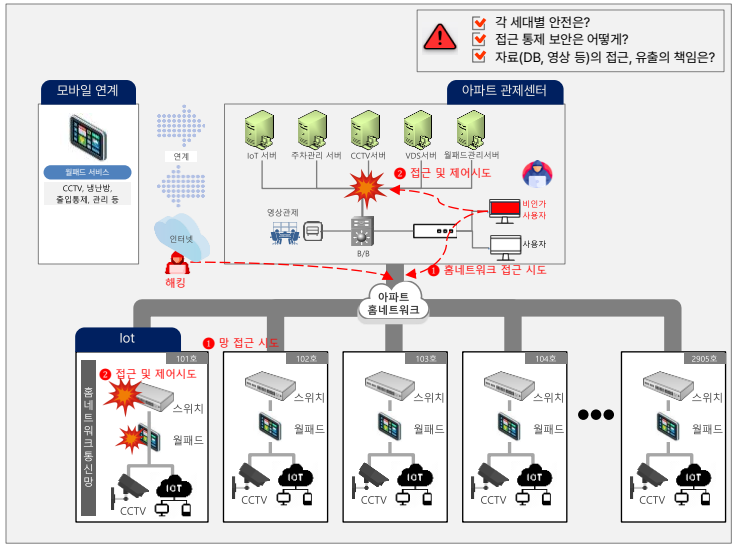
- 실시간 서비스 연계, 데이터 보호를 위해 변화하는 규정에 대한 준수 강화, 규제 요구사항 대응
- IEUMnet의 도입은 " Network Security 서비스 구현 " 을 위한 선도적 보안 강화와 선제적 보안 대응 이다

04 월패드망 보안강화 적용 시스템

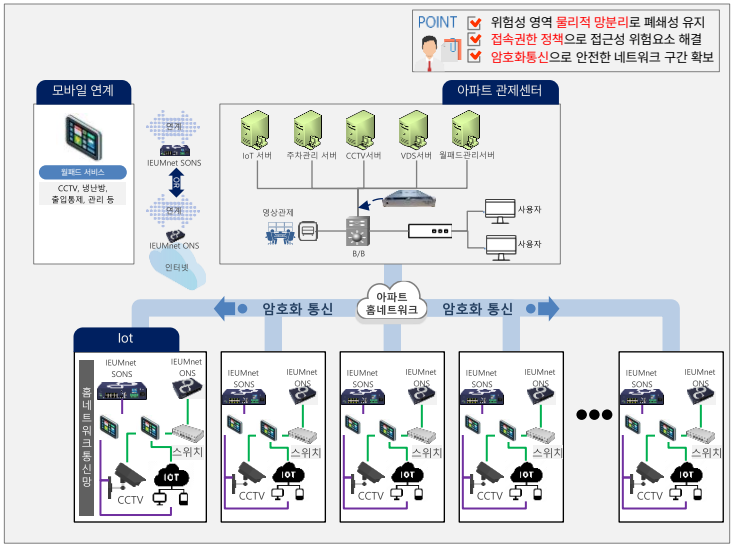
홈네트워크 구간 보안강화

홈네트워크 구간과 각세대별 네트워크를 분리하여 독립적 운영으로 홈네트워크 구간으로 유입되는 내/외부 바이러스 및 해킹을 원천 차단, 개인의 자산 및 개인정보를 보호할 수 있습니다.

BEFORE



AFTER



홈네트워크망 보안 문제점

- 홈네트워크망 및 각 세대별 월패드 시스템 접근에 대한 보안 문제

  해킹 및 악성코드 등으로 홈네트워크 통신시스템 접근에 대한 보안 문제 발생
  운영 중인 각 세대별 월패드 시스템 접근 및 제어를 통해 피해 발생

- 악의적 내부 사용자 및 비인가 사용자의 내부 시스템 접근 보안 문제

  홈네트워크 운영시스템 접근을 통해 내부정보(CCTV, 주차관제, 월패드 등) 유출 피해 발생
  운영 중인 시스템의 의도적 장애 발생 (시스템 Shut down, 정책 변경)으로 피해 발생

IEUMnet을 통한 홈네트워크 및 월패드 보안 해결 방안

- 홈네트워크와 각 세대별 국정원 검증필 암호화 통신으로 네트워크 구간 안전성 확보

  - 화이트리스트 기반 관리로 등록 기기와 정책 통신으로 각 세대별 월패드 접근 문제 해결
  전용 프로토콜 통신으로 물리적 폐쇄망 유지, 각 세대별 독립적 운영으로 보안 문제 해결

- 내부통제 시스템을 향상시켜 운영 중인 시스템 안정성 및 서비스 연속성 제공

  정책 변경 시 2차 인증을 통한 권한 강화로 내부정보(CCTV, 주차관제, 월패드 등) 접근 및 유출 문제 해결
  비인가 연계 / 접속 / 차단에 대한 보안 감사 기록과 통합 정책, 통합 관리로 안전한 운영관리 방안 확보

05 조달청 구매

제품구매

· 조달청 디지털서비스몰

· 보안소프트웨어

· 업체명 :
주식회사 제너시스템

· 제품 구매 구성

- IEUMnetV1.0, 서버CNS
(서버S/W + 하드웨어)

- IEUMnetV1.0, 스위치SONS
(스위치 + 클라이언트SW)

- IEUMnetV1.0, 클라이언트ONS
(단말기 + 클라이언트 S/W)

· 다량납품 가능

IEUMnet-CNS



센타장비

구분	시스템규격
인터페이스	• SPC621D8U-2T C621A
CPU	• Xeon Silver 4310 12 Core 2 Thread
메모리(RAM)	• 16GB x 4EA
HDD	• 1TB * 2EA(Raid 1)
전원	• 전원이중화

규격명 : 보안소프트웨어, 제너시스템, IEUMnet V1.0, 망연계보안솔루션, 1Package, **서버CNS**

조달식별번호 25342306
금액(VAT포함) 38,500,000원

IEUMnet-ONS



CCTV 함체내 단말 장비

구분	시스템규격
인터페이스	• 4Port 10/100/1000 Base-TX
CPU	• MTK MT7621A, Dual-core MIPS1004Kc
메모리(RAM)	• 256MB
HDD	• 32MB
전원	• 싱글전원

규격명 : 보안소프트웨어, 제너시스템, IEUMnet V1.0, 망연계보안솔루션, 1Package, **클라이언트ONS**

조달식별번호 25342307
금액(VAT포함) 500,000원

IEUMnet-SONS



CCTV 함체내 스위치 장비

구분	시스템규격
이더넷	• Gigabot Ethernet 2ea
CPU	• Quad-core ARM Cortex-A55
메모리(RAM)	• 1GB LPDDR4 / 2GB LPDDR4X
HDD	• eMMC 32GB (Optional)
전원	• 싱글전원

규격명 : 보안소프트웨어, 제너시스템, IEUMnet V1.0, 망연계보안솔루션, 1Package, **스위치 SONS**

조달식별번호 26050514
금액(VAT포함) 2,400,000원

04 CCTV망 보안강화 구축실적

01 CCTV 통신망 보안 사업 실적

IEUMnet 실적

순번	도입년도	사이트	사업명
1	2024년	서울특별시 동대문구청	CCTV 구간보안 시스템 도입
2	2024년	경기도 안양시청	CCTV 구간보안 시스템 도입(자율주행 버스구간)
3	2024년	서울특별시 송파구청	CCTV 구간보안 시스템 도입
4	2025년	서울특별시 동대문구청	CCTV망 보안강화 시스템 구매 설치(확대설치)
5	2025년	서울특별시 성북구청	CCTV망 보안강화 시스템 구매 설치
6	2025년	서울특별시 양천구청	CCTV망 보안강화 시스템 구매 설치
7	2025년	서울특별시 은평구청	CCTV망 보안강화 시스템 구매 설치
8	2025년	경기도 안양시청	둘레길 등산로 방범시설물 취약지 개선(확대설치)
9	2025년	서울특별시 서대문구청	CCTV망 보안강화 시스템 구매 설치
10	2025년	서울특별시 종로구청	CCTV망 보안강화 시스템 구매 설치

05 CCTV망 취약점 모의침투 테스트

01 CCTV망 취약점 모의침투 테스트 (적용전)

1. 프로젝트 명

- ㅁㅁ구 CCTV 네트워크 모의침투테스트

2. 수행 개요

2.1 목 적

본 모의침투테스트 수행은 ㅁㅁ구 CCTV 네트워크에 대하여, 시스템의 특성 및 환경에 맞게 모의 침투테스트 시나리오를 선정하여 모의침투테스트를 수행하고, **수행 이후 발견된 보안상 취약한 부분에 대하여 알려 드림으로써, 보안상 안전한 운영과 서비스의 안정성을 확보하는데 그 목적**이 있습니다.

2.2. 수행 대상 및 IP

아래 운영 중인 서비스를 대상으로 모의침투테스트를 수행합니다.

NO	수행대상(URL)	구분	내/외부	IP
1	ㅇㅇ구 CCTV 샘플 1식 (ㅇㅇ 리ㅇㅇ아파트 동문 출입구 근처 CCTV)	Network 기기	외부	168.XXX.12.187

01 CCTV망 취약점 모의침투 테스트 (적용전)

3. 수행 항목

3.1 수행 시나리오

샘플링 된 CCTV에 임의의 랜선을 연결하여 CCTV 네트워크 모의침투테스트를 진행하였으며, 어떠한 IT 인프라 정보를 알고 있지 않은 상태에서의 블랙박스 테스트로 수행하였습니다.

NO	모의침투테스트 수행 시나리오	비 고
1	분석 대상 CCTV의 네트워크 서칭 및 IP 정보 획득 시도	
2	분석 대상 CCTV의 인접한 주변 CCTV들로 불법적 침투 시도	
3	CCTV의 활성화된 서비스 포트 분석을 통한 관리자 인증 페이지 정보 획득 시도	
4	CCTV 관리자 인증페이지의 인증 우회 접근 및 관리 기능 장악 시도	
5	CCTV 관리자 인증 우회 성공 이후 동영상 탈취 및 불법적 조작 시도	
6	CCTV와 네트워크 경유지를 통한 통합관제 시스템 장악 시도	

4. 수행 결과 요약

CCTV 네트워크 모의침투테스트 수행 결과 5가지 경우의 보안 취약점이 검출되었습니다.

NO	모의침투테스트 수행 시나리오	점검 결과
1	분석 대상 CCTV의 네트워크 서칭 및 IP 정보 획득 시도	취약
2	분석 대상 CCTV의 인접한 주변 CCTV들로 불법적 침투 시도	취약
3	CCTV의 활성화된 서비스 포트 분석을 통한 관리자 인증 페이지 정보 획득 시도	취약
4	CCTV 관리자 인증페이지의 인증 우회 접근 및 관리 기능 장악 시도	취약
5	CCTV 관리자 인증 우회 성공 이후 동영상 탈취 및 불법적 조작 시도	취약
6	CCTV와 네트워크 경유지를 통한 통합관제 시스템 장악 시도	양호

01 CCTV망 취약점 모의침투 테스트 (적용전)

5. 총 평

요약하여 말씀드리자면, 샘플링 된 1개 CCTV에서 연결된 **스위칭 허브에**

간단히 랜선 연결만 하면,

주변의 수천대 이상의 CCTV가 속해져 있는 서로 다른 네트워크의 이동 및 접근이 가능하였으며,

CCTV의 관리툴에 손쉽게 접속이 가능하였고,

인증 기능 우회하여 **대다수의 CCTV를 불법적 조작, 동영상 실시간 취득** 등을 할 수 있는 상황이었습니다.

이는 CCTV 시스템이 매우 보안상 취약한 상태로써 어떠한 불법적인 행위, 악의적인 행위 등을 할 수 있는 가능성이 있는 상태입니다.

그러므로, 본 문서를 참고하시어 CCTV 시스템들에 대한 보안상 안전한 운영이 될 수 있도록 보완이 되시 길 권고 드리는 바입니다.

01 CCTV망 취약점 모의침투 테스트 (적용후)

3. 수행 항목

3.1 수행 시나리오

샘플링 된 CCTV에 보안솔루션과 스위치 장비에 각각 연결하여 CCTV 네트워크 모의침투테스트를 진행하였으며,

어떠한 IT 인프라 정보를 알고 있지 않은 상태에서의 블랙박스 테스트로 수행하였습니다.

NO	모의침투테스트 수행 시나리오
1	분석 대상 CCTV의 네트워크 서칭 및 IP 정보 획득 시도
2	보안솔루션이 장착된 CCTV의 인접한 주변 CCTV들로 불법적 침투 시도
3	보안솔루션이 장착된 CCTV의 활성화된 서비스 포트 분석을 통한 관리자 인증 페이지 정보 획득 시도
4	보안솔루션이 장착된 CCTV 관리자 인증페이지의 인증 우회 접근 및 관리 기능 장악 시도
5	보안솔루션이 장착된 CCTV 관리자 인증 우회 성공 이후 동영상 탈취 및 불법적 조작 시도

4. 수행 결과 요약

CCTV 네트워크 모의침투테스트 수행 결과 보안 취약점이 검출되었습니다.

NO	모의침투테스트 수행 시나리오	점검 결과
1	분석 대상 CCTV의 네트워크 서칭 및 IP 정보 획득 시도	양호
2	보안솔루션이 장착된 CCTV의 인접한 주변 CCTV들로 불법적 침투 시도	양호
3	보안솔루션이 장착된 CCTV의 활성화된 서비스 포트 분석을 통한 관리자 인증 페이지 정보 획득 시도	양호
4	보안솔루션이 장착된 CCTV 관리자 인증페이지의 인증 우회 접근 및 관리 기능 장악 시도	양호
5	보안솔루션이 장착된 CCTV 관리자 인증 우회 성공 이후 동영상 탈취 및 불법적 조작 시도	양호

01 CCTV망 취약점 모의침투 테스트 (적용후)

5. 총 평

ㅇㅇ구 CCTV 네트워크 모의침투테스트 수행을 완료 하였습니다.

수행 결과

보안솔루션이 장착된 상태의 ㅁㅁ구 CCTV 네트워크 모의침투테스트 2번째 수행에서는
수행 결과 모두 양호하였으며, 취약점이 확인되지 않았습니다.

‘분석 대상 CCTV의 네트워크 서칭 및 IP 정보 획득 시도’ 시나리오 부분의 보안진단의 경우,
어떠한 사전정보 없이 단지 보안솔루션이 장착된 CCTV에 LAN 연결 시 CCTV에 해당하는
IP 정보 취득이 되지 않았으며, 안전한 것으로 확인되었습니다.

‘보안솔루션이 장착된 CCTV의 인접한 주변 CCTV들로 불법적 침투 시도’ 시나리오 보안진단의 경우,
보안솔루션이 장착된 CCTV의 네트워크 전체 대역 스캔 시 노트북에 연결된 CCTV 네트워크 외의
다른 네트워크를 찾을 수 없었으며 안전한 것으로 확인되었습니다.

‘보안솔루션이 장착된 CCTV의 활성화된 서비스 포트 분석을 통한 관리툴 페이지 정보 획득 시도’
시나리오 보안진단의 경우, 보안솔루션이 장착된 CCTV의 네트워크 스캔이 되지 않아
서비스 포트 분석 또한 할 수 없었으므로 안전한 것으로 확인되었습니다.

01 CCTV망 취약점 모의침투 테스트 (적용후)

5. 총 평

수행 결과 (계속)

‘보안솔루션이 장착된 CCTV 관리툴 페이지의 인증 우회 접근 및 관리 기능 장악 시도’ 시나리오

보안진단의 경우, 네트워크 스캔과 서비스 포트 분석이 되지 않아 관리 툴 페이지에 접근이 불가하여 안전한 것으로 확인되었습니다.

‘보안솔루션이 장착된 CCTV의 관리자 인증 우회 성공 이후 동영상 탈취 및 불법적 조작 시도’ 시나리오

보안진단의 경우, 관리 툴 페이지의 접근이 불가하여 인증 우회 및 동영상 탈취가 되지 않아 안전한 것으로 확인되었습니다.

요약하여 말씀드리자면, 샘플링 된 1개의 보안솔루션이 장착된 CCTV에서는 LAN 연결을 통해 주변에 있는 CCTV를 검색할 수 없었으며 이후에 추가적인 공격 진행이 어려운 것을 확인하였습니다.

이상 ㅁㅁ구 CCTV 네트워크 모의침투테스트 2번째 수행을 마칩니다.