IEUMnet, a Multi-Zone Network Security Solution by JENERSYSTEM,
leading a new paradigm in security



IEUMnet
Zero Trust Network Security

[Multi-Zone Network Security-Based]

# CCTV Network Security Enhancement

★ Certified Solution compliant with NIS Security Requirements V3.0

JENER SYSTEM

# CONTENTS

Intrusion and Hacking Prevention Solution for IoT Devices
(CCTV, IP Cameras, etc.)




01 Overview of CCTV Network Security Enhancement

02 Background of CCTV Network Security Enhancement

03 IEUMnet for CCTV Network Security

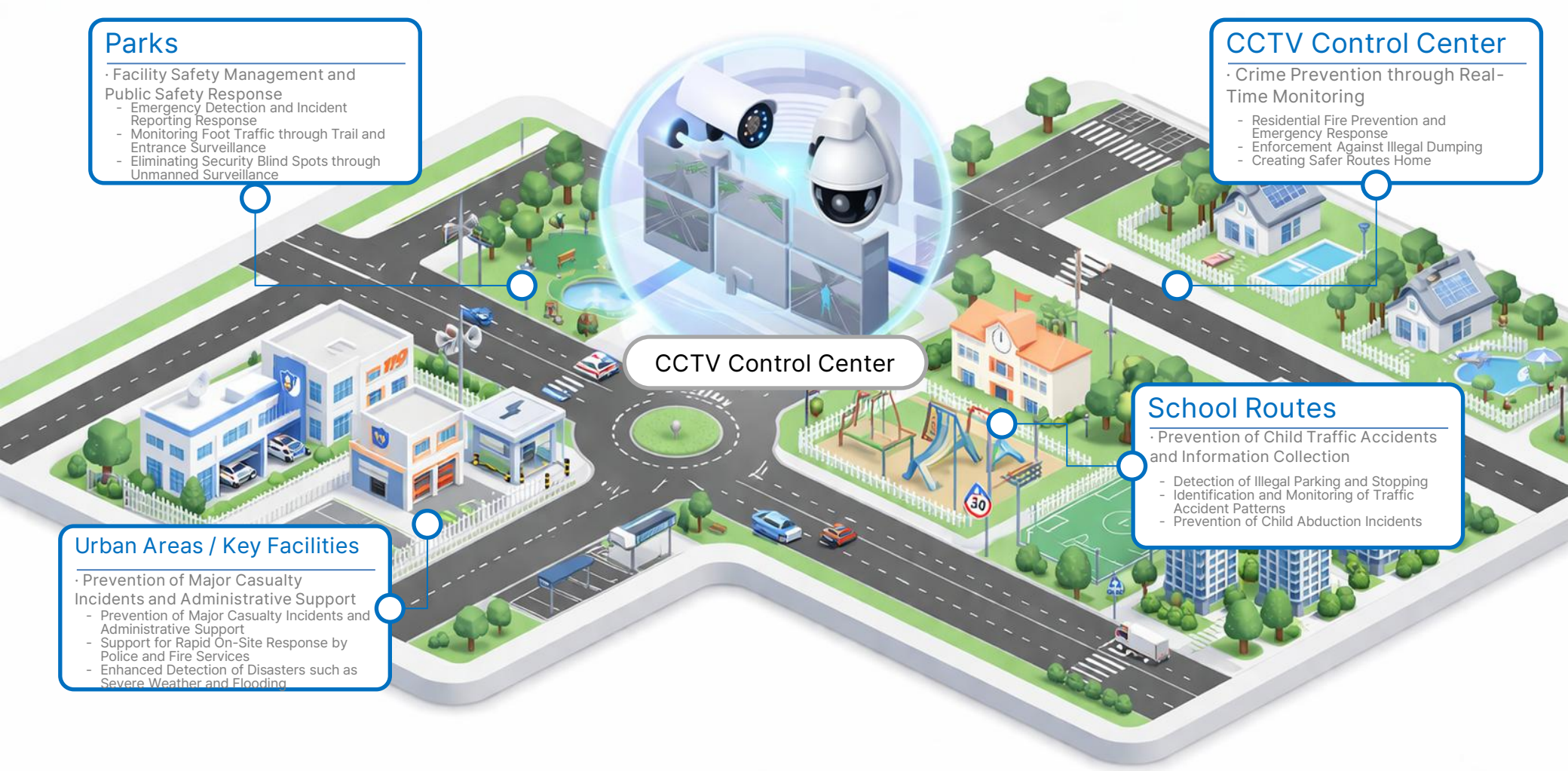
04 Implementation Cases

05 Penetration Testing for CCTV Network Vulnerabilities

# 01 Overview of CCTV Network Security Enhancement

# 01 CCTV Network Security Enhancement

CCTV plays a critical role in ensuring public safety in everyday life.



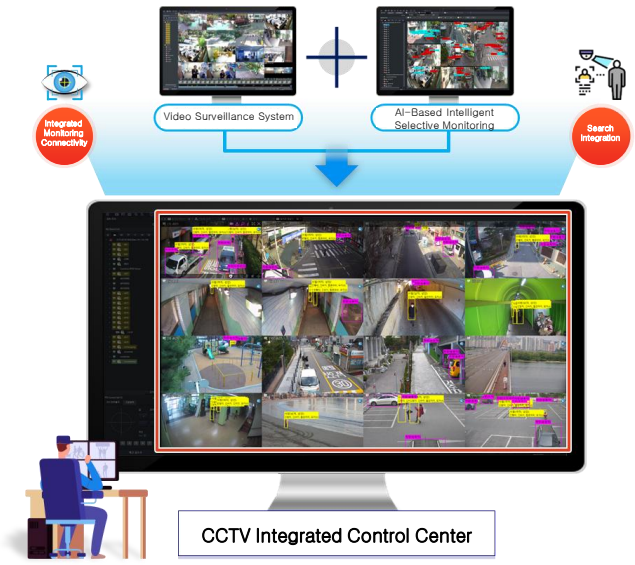
# 02 CCTV Network Security Enhancement

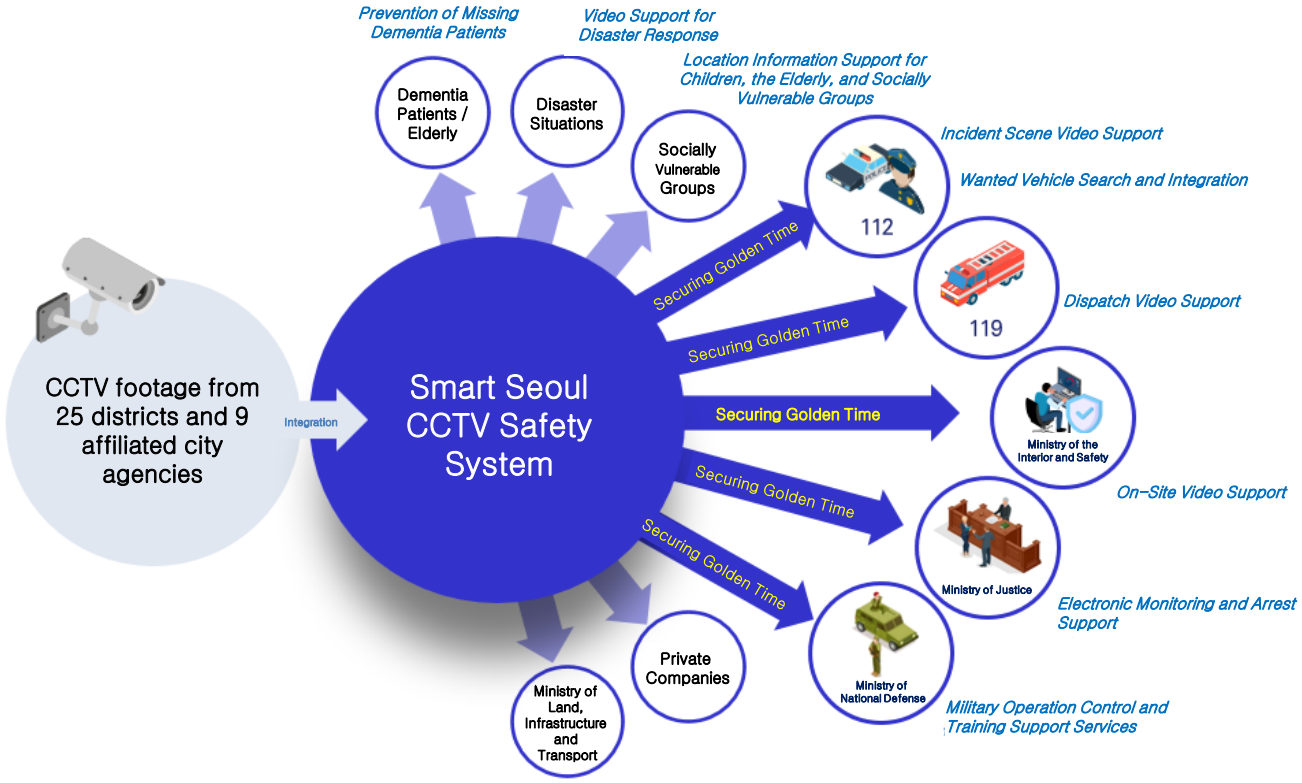
## Overview

CCTV plays a critical role in ensuring public safety in everyday life.

CCTV video data operated for public safety plays a critical role not only in crime prevention, child protection, urban parks and playgrounds, illegal dumping enforcement, and traffic control and analysis, but also in rapidly detecting and responding to emergencies such as violence, loitering, and falls through AI-based intelligent selective monitoring, thereby ensuring citizen safety.

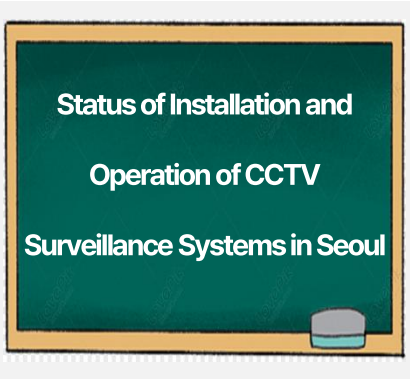
## Digital Safe City CCTV Safety Network Service

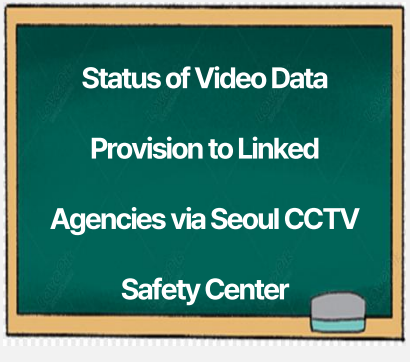


# 03 CCTV Network Security Enhancement

## Project Background




- As of the end of December 2023, approximately 177,000 CCTV surveillance systems are installed and operated in Seoul, and through the Seoul CCTV Safety Center integrated platform, 4,145,582 cases of video data have been provided in linkage with relevant agencies, contributing to public safety.

### CCTV Installation Status in Seoul (Unit: Units, as of December 31, 2025)

| Category | Total CCTV | Crime Prevention and Investigation | | | | | Facility Safety and Fire Prevention | Traffic Enforcement | Traffic Information Collection and Analysis | Others (Other Regulations) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Subtotal | Crime Prevention | Child Protection Zones | Parks and Playgrounds | Illegal Dumping | | | | |
| Local Governments | 122,613 | 108,947 | 80,885 | 8,874 | 18,327 | 861 | 4,426 | 8,811 | 153 | 276 |

### CCTV Installation Status in Seoul (Unit: Units, as of December 31, 2024)

| Category | Total CCTV | Crime Prevention and Investigation | | | | | Facility Safety and Fire Prevention | Traffic Enforcement | Traffic Information Collection and Analysis | Others (Other Regulations) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Subtotal | Crime Prevention | Child Protection Zones | Parks and Playgrounds | Illegal Dumping | | | | |
| Local Governments | 113,273 | 99,758 | 74,807 | 8,704 | 15,417 | 830 | 4,482 | 8,648 | 18 | 367 |

# 02 Background of CCTV Network Security Enhancement

# 01 Background of IEUMnet Development

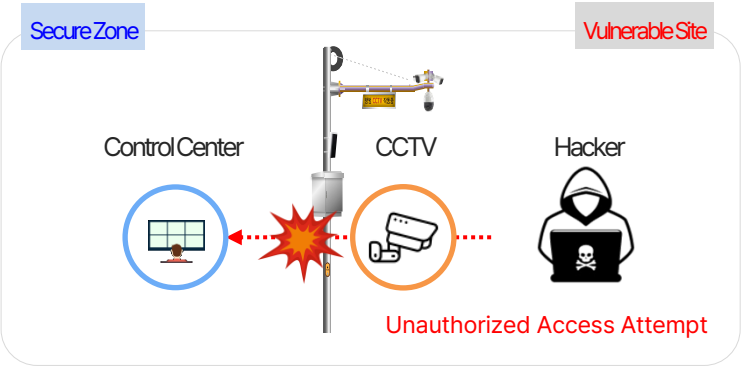
## Necessity of the Project_CCTV Network Security Enhancement

"Public security systems require a strong security solution that maintains flexibility and efficiency while responding to insider threats and external attacks."

### AS-IS

**Security Vulnerabilities**

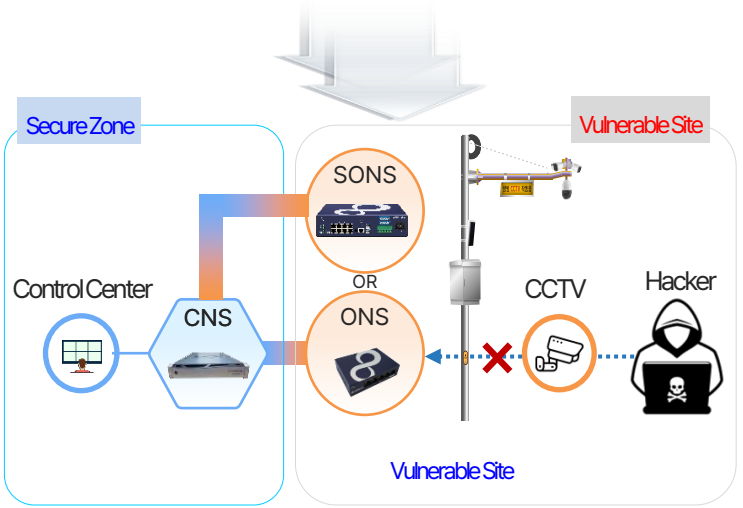
- Security gaps in multiple on-site facilities within the CCTV network
- Difficulty in managing vulnerable sites
- Possibility of access attempts through vulnerable paths




### TO-BE

**Management of Vulnerable Sites**

- Complete blocking of illegal vulnerable paths and secure management
- Ensuring reliability and integrity of data in the CCTV network
- Maintaining isolation and independence between non-secure and secure zones




※ CCTV → ONS → SWITCH → FIRE WALL → CNS
※ CCTV → SONS → FIRE WALL → CNS

# 01 Background of IEUMnet Development

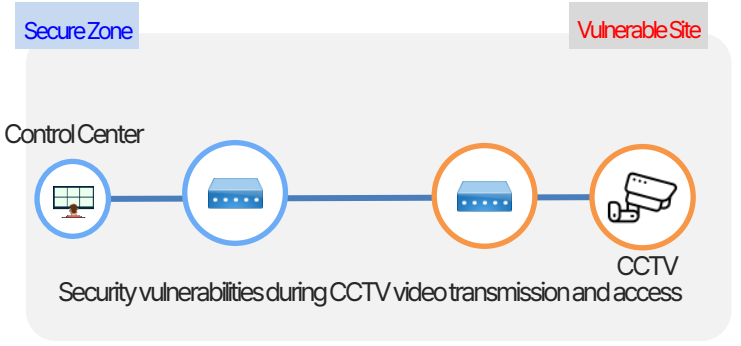
## Necessity of the Project_CCTV Network Security Enhancement

"Public security systems require a strong security solution that maintains flexibility and efficiency while responding to insider threats and external attacks."

### AS-IS

**Need for security to ensure the safety and reliability of video data**

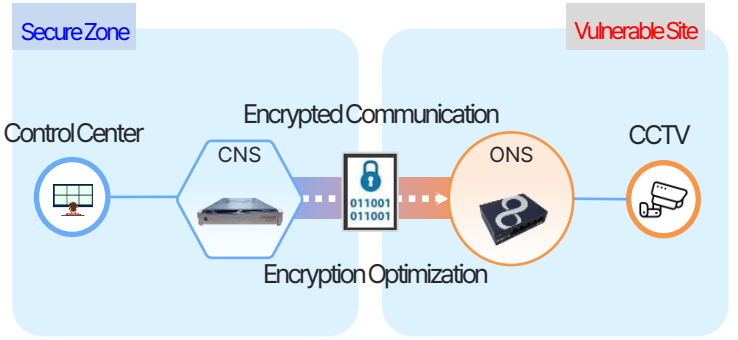
- Security vulnerabilities in network segments due to closed network operation
- Need to ensure integrity and reliability during CCTV video transmission
- Low awareness of network segment security in CCTV networks




### TO-BE

**Ensuring integrity and reliability of CCTV video data**

- Encrypted communication verified for CCTV network security
- Maximizing one-way communication advantages to ensure isolation
- Optimized design to minimize performance degradation



# 01 Background of IEUMnet Development

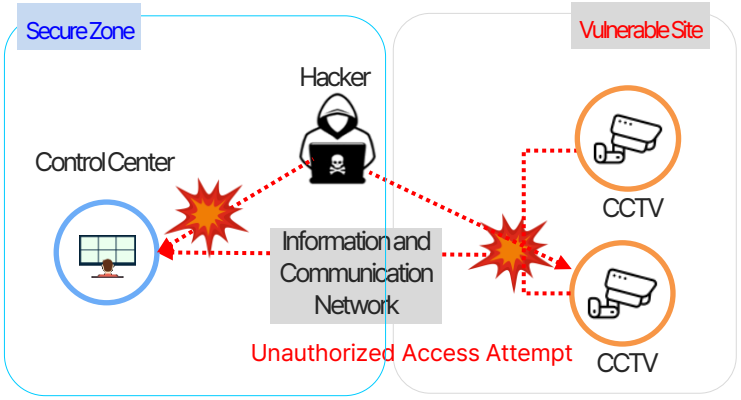
## Necessity of the Project_CCTV Network Security Enhancement

"Public security systems require a strong security solution that maintains flexibility and efficiency while responding to insider threats and external attacks."

### AS-IS

**Security Vulnerabilities**

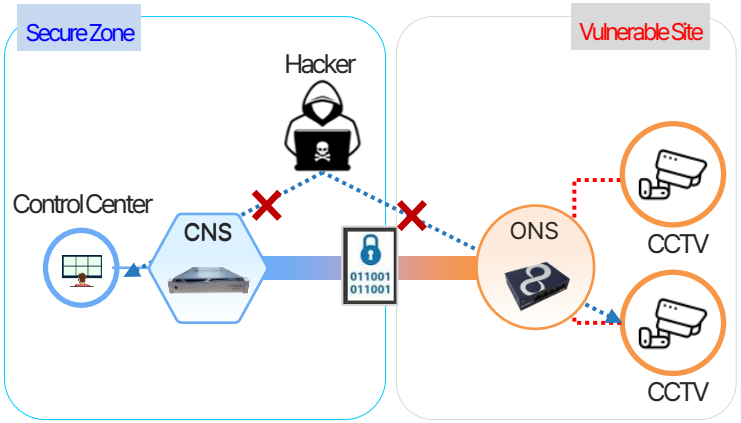
- Security gaps in information and communication
- Difficulty in managing multiple vulnerable sites
- Possibility of access attempts through vulnerable paths




### TO-BE

**Management of Vulnerable Sites**

- Secure management of vulnerable sites
- 1:N centralized security control management of multiple vulnerable sites
- Ensuring data reliability and integrity
- Maintaining isolation between non-secure and secure zones



# 02 CCTV Installation Status

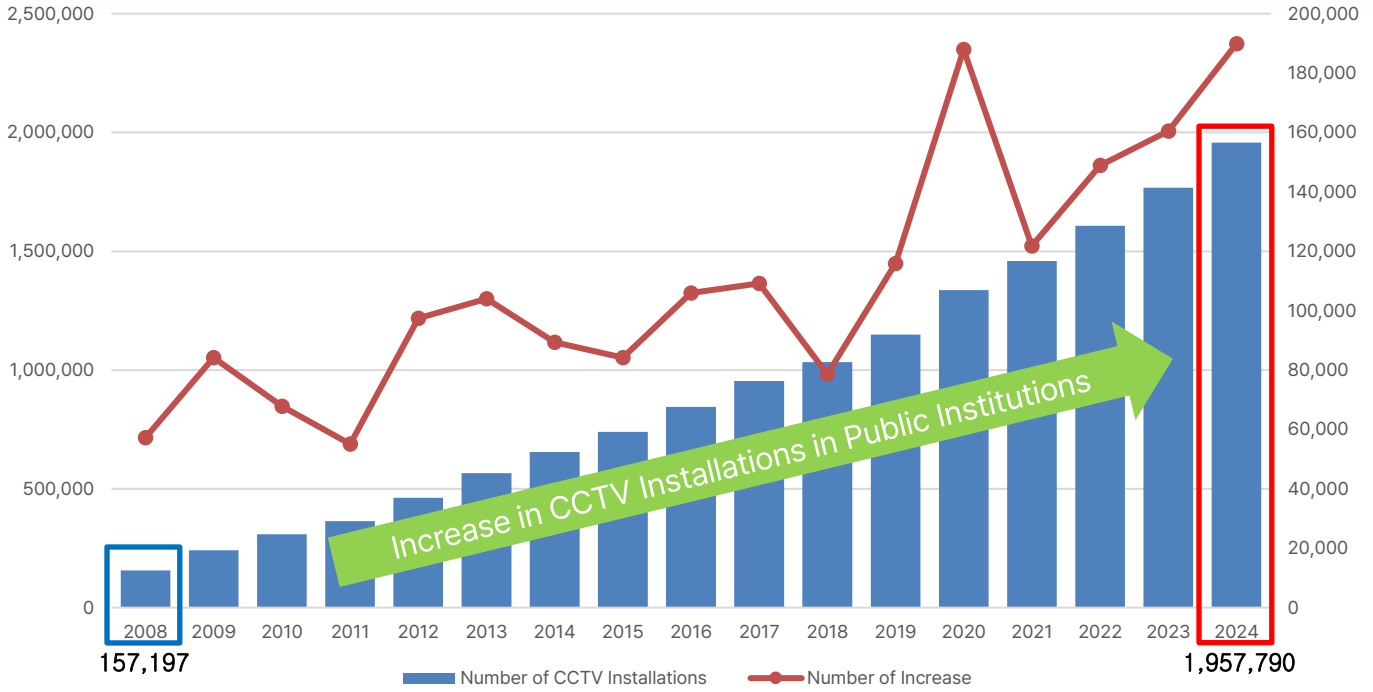
## Background

Source: e-Nara Index

(Indicator Service | e-Nara Index (index.go.kr))



CCTV Installation and Increase in Public Institutions




Source: Survey and Personal Information Protection Comprehensive Support System Data

**Annual average increase of over 10% in CCTV installations and performance improvement**

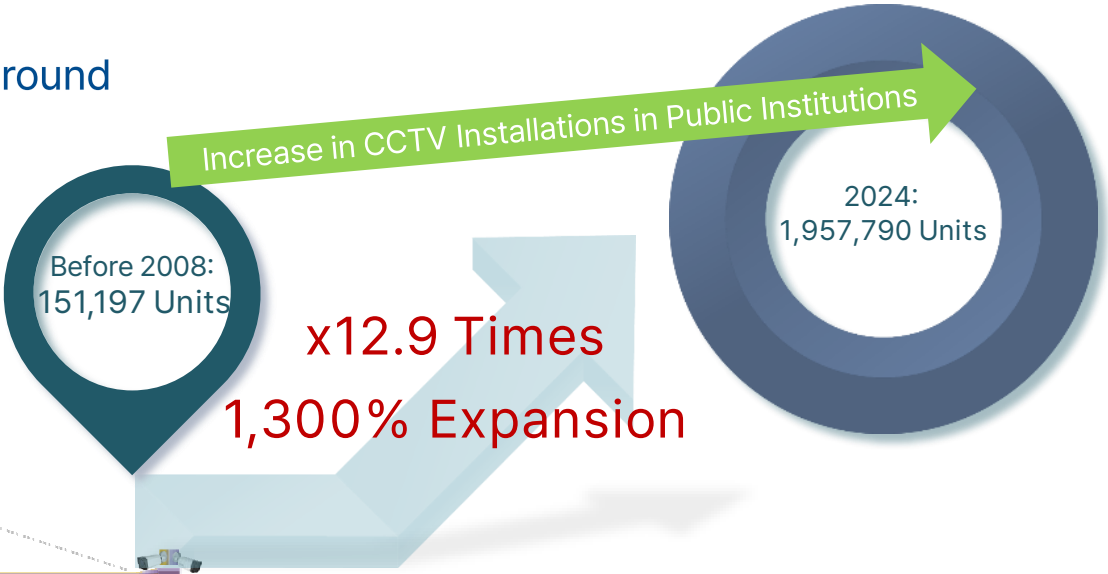
(Unit: Units)

| | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total Number of CCTV Installations (Units) | 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 |
| Year-on-Year Increase (Units) | 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 |
| Year-on-Year Growth Rate (%) | 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 |

Source: Survey and Personal Information Protection Comprehensive Support System Data
Note: CCTV installation and operation status in public institutions was collected by each institution until 2011 (2010 data), but from 2012 (2011 data), institutions are required to register the status annually by the end of March in the Personal Information Protection Comprehensive Support System

# 02 CCTV Installation Status

## Background



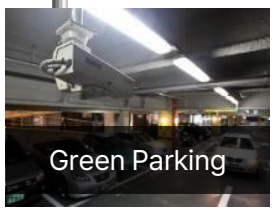

Annual Average Increase of Over 10% in CCTV Installations and Performance Improvement

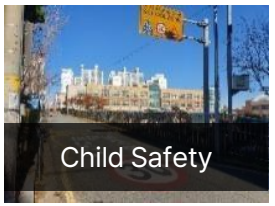










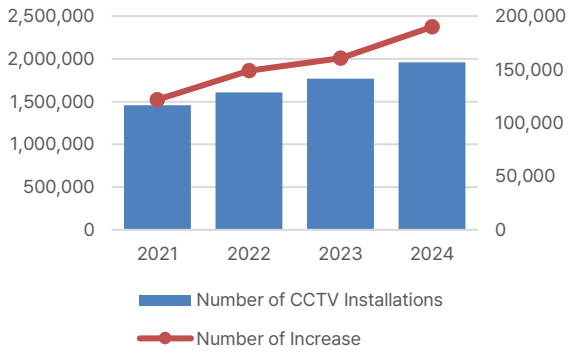





### Number of CCTV Installations in Public Institutions

| | 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 |

### CCTV Increase Chart in Public Institutions

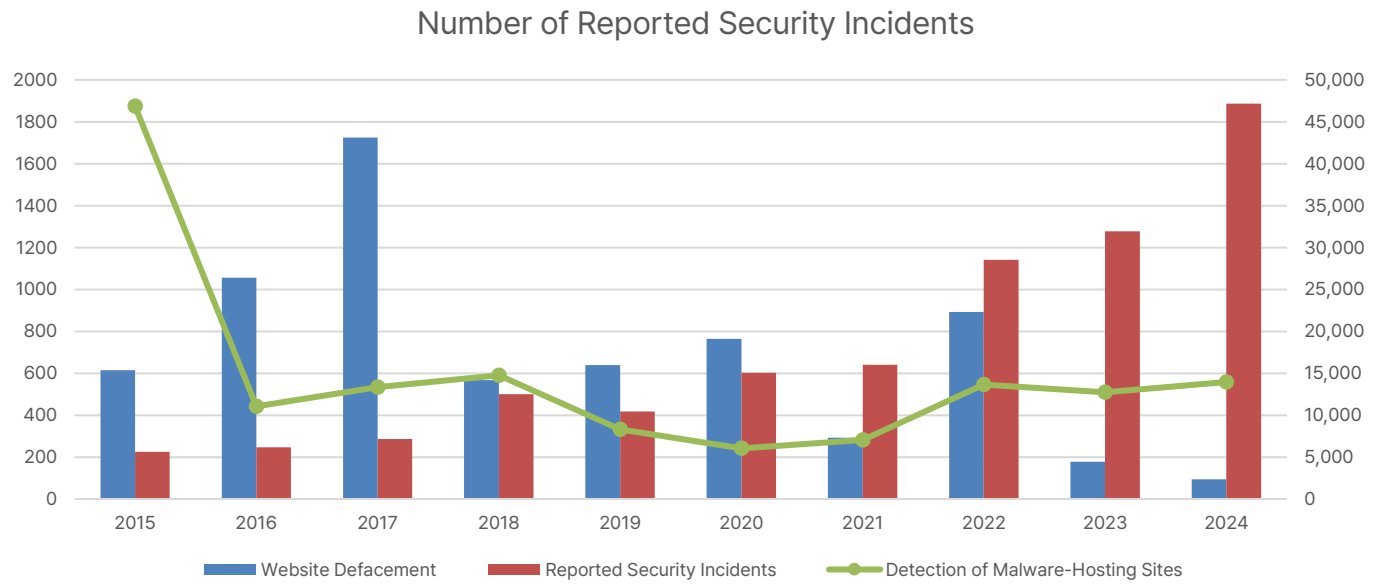



Source: e-Nara Index
(Indicator Service: e-Nara Index (index.go.kr))

# 03 Damage Cases

## Statistics on Reported Security Incidents

The hacking incident index represents the total number of cases detected and handled by KISA, including website defacement incidents, detection and response to malware-hosting sites targeting domestic websites, and reported security incidents from private sectors (institutions and companies) based on the Information and Communications Network Act.




### Number of Reported Security Incidents

Source: Korea Internet & Security Agency (KISA)

| Category | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|---|
| Website Defacement | 615 | 1,056 | 1,724 | 567 | 639 | 764 | 292 | 893 | 178 | 94 |
| Reported Security Incidents | 225 | 247 | 287 | 500 | 418 | 603 | 640 | 1,142 | 1,277 | 1,887 |
| Detection of Malware-Hosting Sites | 46,850 | 11,044 | 13,347 | 14,754 | 8,299 | 6,034 | 7,043 | 13,661 | 12,731 | 13,967 |

# 04 Necessity of Implementation

## Necessity of Implementation

**Technical security issues must be resolved through CCTV network security enhancement.**

- For CCTV networks operated 24/7 in remote unmanned locations network segments between CCTV cameras and integrated control centers
  - Control of unauthorized access through illegal and vulnerable security paths
  - Ensuring confidentiality and securing network segments through encrypted communication
  - Ensuring reliability and integrity of CCTV video data through AI-based systems
- Improvement of security vulnerabilities for safe CCTV operation

Preventing security breaches through strengthened technical security by adopting a robust security system



**Preventing data leakage through enhanced physical, technical, and administrative security**

CCTV Network + IEUMnet

- Expansion of Intrusion and Hacking Defense Systems
- Elimination of Security Vulnerabilities

### 1 Step Physical Security Enhancement

**Protection of physical information system assets such as buildings and equipment**

- Server Room Equipment Security
- Access Control Monitoring
- Server Access Control and System Security Measures
- Protection of Locking Devices for Equipment and Facilities

### 2 Step Technical Security Enhancement

**Technical controls to protect against intrusion and hacking**

- Network Segment Encryption
- AI-Based Traffic Anomaly Detection
- Control of Unauthorized Access to Network Segments
- Strengthening Security of Vulnerable Management Areas

### 3 Step Administrative Security Enhancement

**Administrative security framework to support physical and technical security**

- Internal Staff and Outsourced Personnel Management
- Information Security Documentation
- Personal Information Protection Training and Education
- Regular Backups for Storage and Tampering Prevention

# 03 IEUMnet for CCTV Network Security

# CCTV Security IEUMnet



## IEUMnet

**Zero Trust Network Security**



# 02 Key Features of IEUMnet

## Key Features




IEUMnet ..

### Proven Security Solution

- Certified with NIS Security Function Verification
- GS Grade 1 Software Quality Certification
- Field-Proven in Seoul and Local Governments

### Multi-Zone Network Security

- 1:N Multi-Zone Integration of Non-Secure Areas
- Secure Connection of Multiple External Devices
- Flexible Scalability and Connectivity

### Network Segmentation

- Implementation of Isolated Multi-Zone Network Security Environment
- Fundamental Blocking of External Hacking
- Use of Dedicated Encryption Protocol

### Enhanced VPN Configuration

- Implementation of Enhanced VPN
- Compliance with NIS Security Guidelines
- Strengthened Security and Resolution of Session and Policy Vulnerabilities

### Internal Information System Protection

- Pre-Detection of Malware before Data Transmission
- One-Way Communication and Granular Policy-Based Hacking Prevention
- Prevention of Data Leakage through Insider Security Policies

### Secure Management / Service Continuity

- Independent and Isolated Operation Environment per Security Site
- Compliance with Blocking External Attacks
- Integrated Policy Operation and Management

**First in Korea**




Security Function Verification Certification in the Private Data Transmission Product Sector

Product Compliant with NIS Security Requirements V3.0

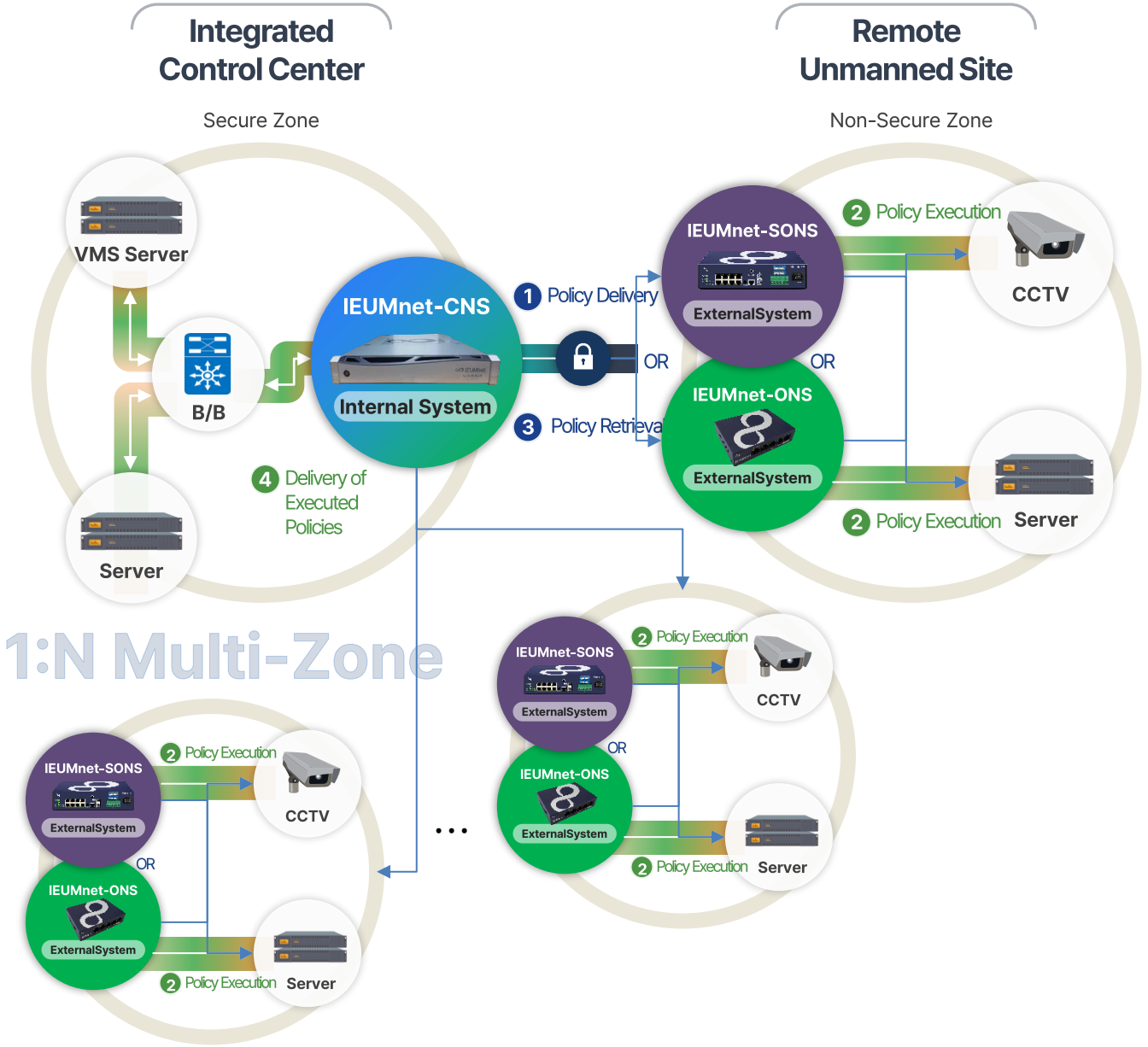
GOOD Software GS Grade 1 Certification



# 02 Key Features of IEUMnet

## Key Features

IEUMnet is a solution that provides integrated security management for multiple vulnerable or required sites by operating CCTV sites and remote unmanned locations in an isolated and independent configuration, blocking external access, enabling secure data transmission through verified encrypted communication, enhancing security, and ensuring safe service continuity.



# 03 CCTV Network Security Enhancement Application System

JENER SYSTEM

## IEUMnet Application Areas

| | | | |
|---|---|---|---|
| Remote Work | Instead of using insecure VPN for remote work, IEUMnet enables secure access to internal systems from home while maintaining management records and logs | Wired and Wireless Integration | Can be flexibly used across wireless networks such as LTE and wired networks |
| Branch Connectivity | Provides higher security than VPN for network connections between headquarters and branches | Overseas Workers | Enhances management clarity and security when accessing internal systems from overseas using IEUMnet |
| Civil Service Issuance | Replaces insecure VPN-based civil service systems with IEUMnet for enhanced security | Control Network | Improves security in remote control networks (e.g., reservoirs, power grids) through one-way communication with IEUMnet |
| ATM Systems | Replaces insecure VPN-based ATM networks nationwide with IEUMnet | Security System and Infrastructure | IEUMnet can be used to establish secure boundaries between different networks when building integrated infrastructures |

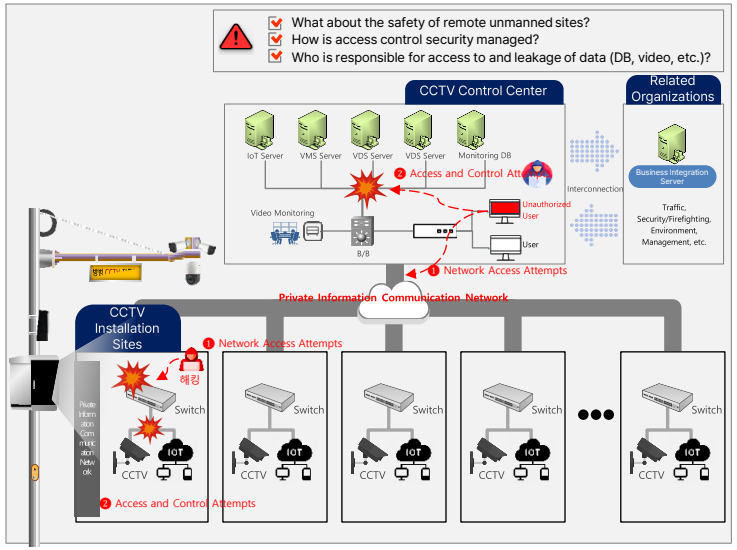
# 03 CCTV Network Security Enhancement Application System

JENER SYSTEM

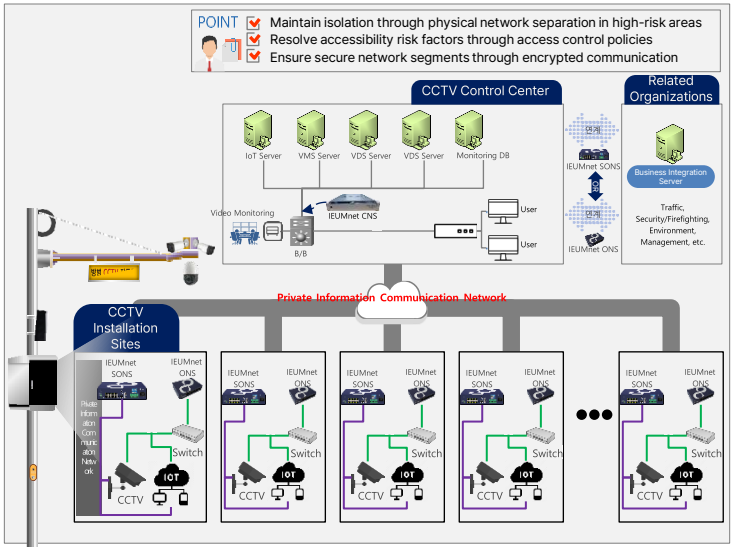
## CCTV Network Security Reinforcement Architecture

By separating the network between the CCTV segment and the internal network, viruses and hacking attempts originating from the CCTV segment can be fundamentally blocked, protecting municipal IT resources.

### BEFORE




### AFTER




### CCTV Network Security Issues

- Security issues related to network access at CCTV installation sites and remote unmanned management locations
  - Damage caused through unauthorized access and control of CCTV cameras
  - Vulnerabilities arising from inadequate control of illegal access at weak points and during non-working hours
- Security issues from internal system access by malicious insiders and unauthorized users
  - Leakage of internal data (DB, CCTV footage, etc.) through system access
  - Damage caused by intentional disruption of operating systems (system shutdown, policy changes)

### CCTV Network Security Solution through IEUMnet

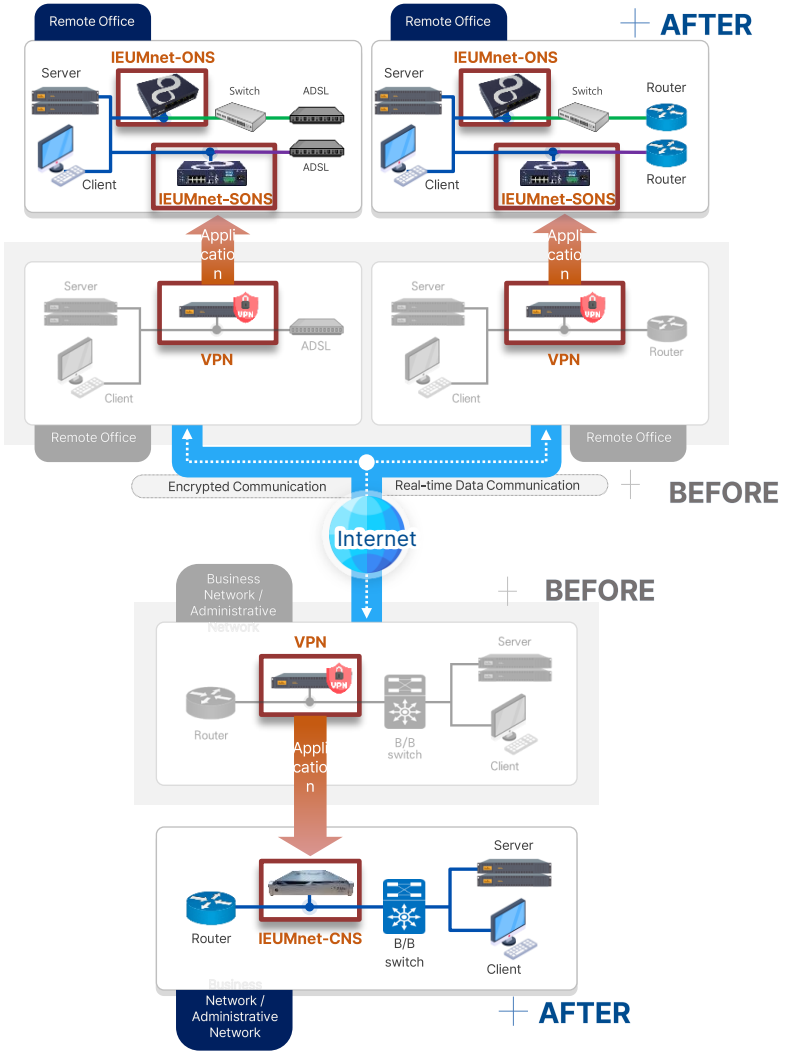
- Ensure network segment security through verified encrypted communication between CCTV control centers and remote unmanned sites
  - Resolve CCTV camera access issues through whitelist-based management and policy-based communication with registered devices
  - Fundamentally block illegal CCTV access within the network by maintaining isolation between secure and non-secure zones
- Enhance internal control systems to ensure system stability and service continuity
  - Strengthen authority through secondary authentication for policy changes to prevent access and leakage of internal data (DB, CCTV footage, etc.)
  - Secure operation management through security audit logs for unauthorized connections/access/blocking, integrated policies, and unified management

# 03 CCTV Network Security Enhancement Application System

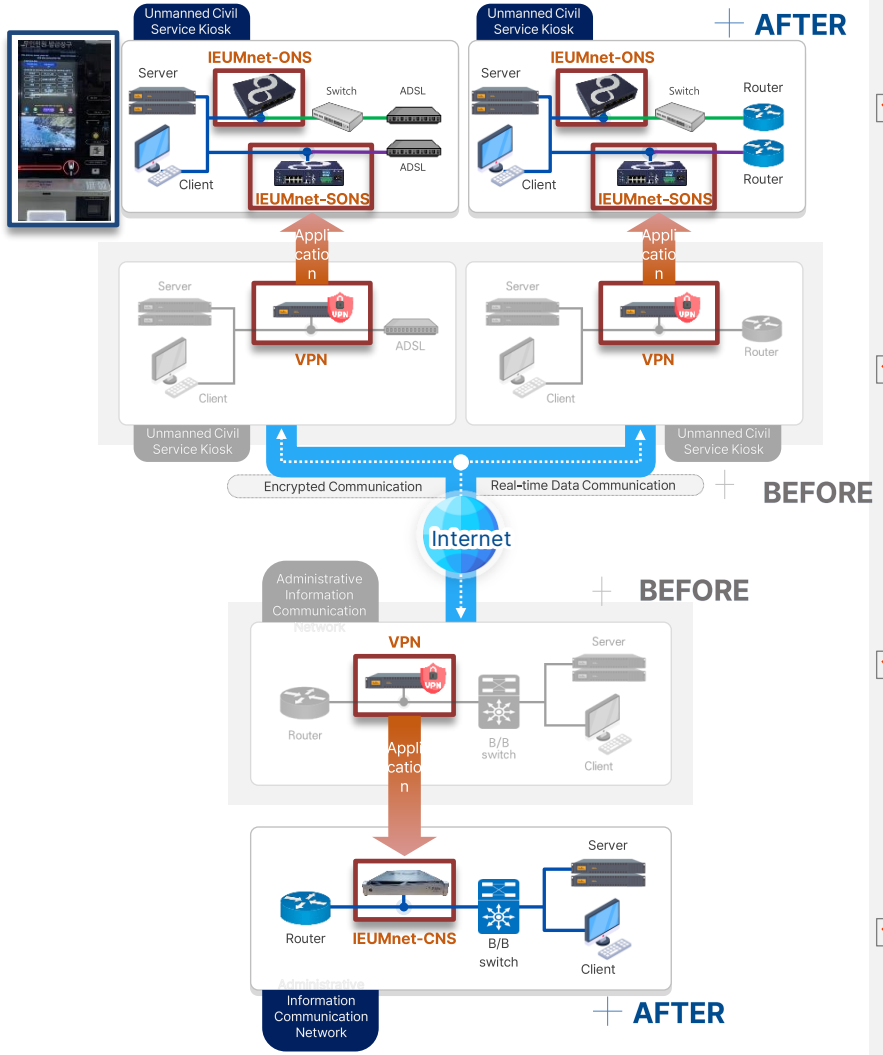
JENER SYSTEM

## Enhanced Security for VPN Network Segments

### Target Architecture for Strengthening VPN Network Security Vulnerabilities




### Security Architecture for Reinforced Unmanned Civil Service Kiosk Network



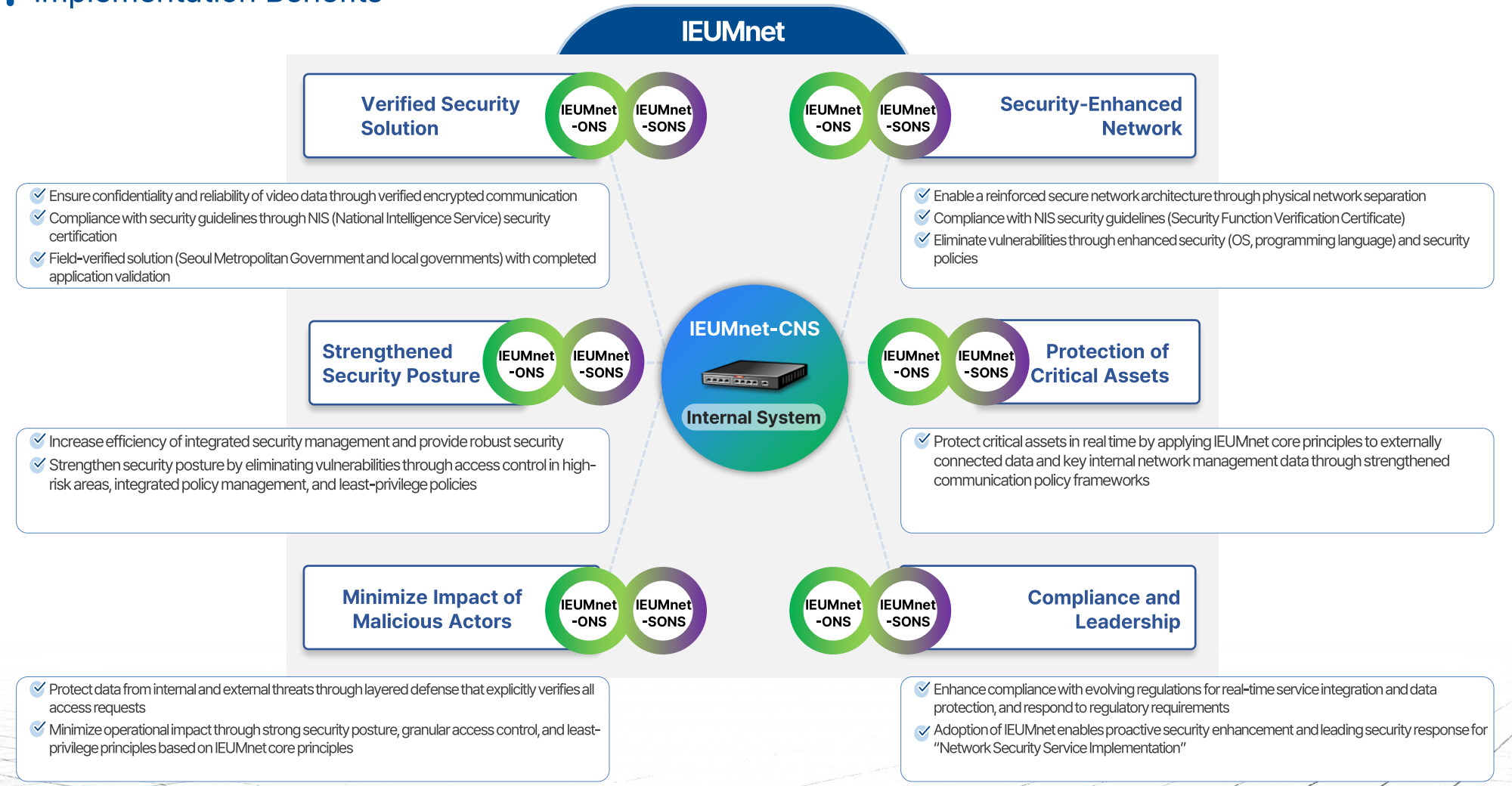

- Ensure secure network segments through encrypted communication
- Maintain physical isolation and ensure service continuity using proprietary protocol communication instead of TCP/IP
- Prevent access to business/administrative networks outside authorized policies within VPN segments while ensuring service continuity
- Maintain communication only between registered devices and policies through whitelist-based management to block network access
- Ensure secure operations through integrated policies and unified management

# CCTV Network Security Enhancement Application System



## Implementation Benefits

## Multi Area Network Security



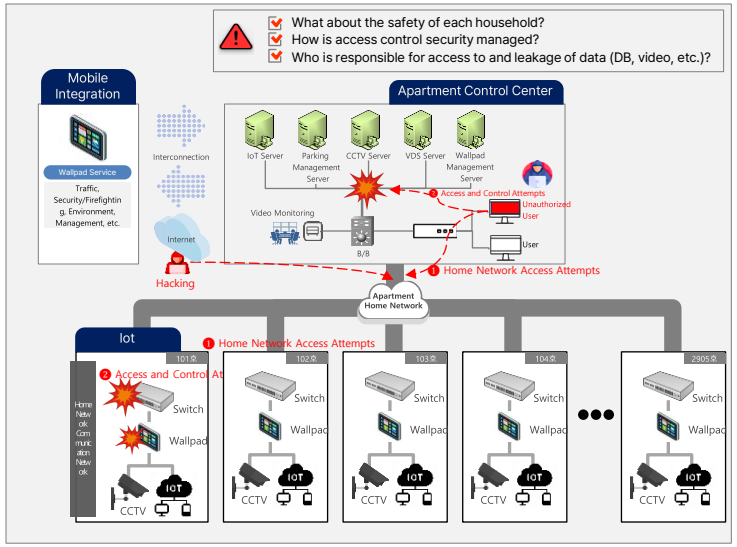
# 04 Wallpad Network Security Enhancement Application System

JENER SYSTEM

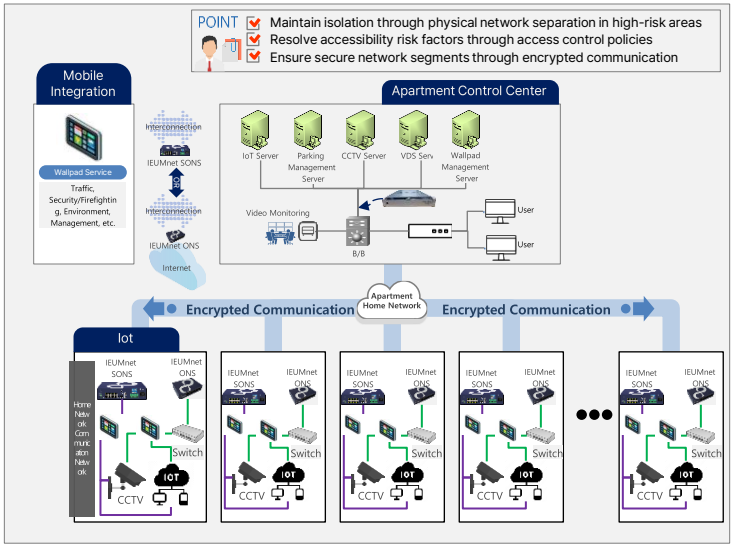
## Enhanced Home Network Segment Security

By separating the home network segment and each household network for independent operation, internal and external viruses and hacking attempts entering the home network can be fundamentally blocked, protecting personal assets and privacy.

### BEFORE




### AFTER




## Home Network Security Issues

- Security issues related to access to the home network and each household's wallpad system
  - Security issues arising from access to the home network communication system due to hacking and malware
  - Damage caused through access and control of wallpad systems in each household
- Security issues from internal system access by malicious insiders and unauthorized users
  - Leakage of internal data (CCTV, parking control, wallpad, etc.) through access to the home network operating system
  - Damage caused by intentional disruption of operating systems (system shutdown, policy changes)

## Home Network and Wallpad Security Solutions through IEUMnet

- Ensure network segment security through NIS-verified encrypted communication between the home network and each household
  - Resolve wallpad access issues for each household through whitelist-based management and policy-driven communication with registered devices
  - Maintain a physically isolated network using proprietary protocol communication and resolve security issues through independent operation per household
- Enhance internal control systems to ensure system stability and service continuity
  - Strengthen authority through secondary authentication for policy changes to prevent access and leakage of internal data (CCTV, parking control, wallpad, etc.)
  - Ensure secure operation management through security audit logs for unauthorized connections/access/blocking, integrated policies, and unified management

# 05 Public Procurement Service Purchase

## Product Purchase

· Public Procurement Service Digital Service Mall
· Security Software
· Company Name: JenerSystem Co., Ltd.
· Product Purchase Configuration
- IEUMnet V1.0, Server CNS (Server S/W + Hardware)
- IEUMnet V1.0, Switch SONS (Switch + Client S/W)
- IEUMnet V1.0, Client ONS (Device + Client S/W)
· Available for Bulk Supply

### IEUMnet-CNS



Central Equipment

| Category | System Specifications |
|---|---|
| Interface | • SPC621D8U-2T C621A |
| CPU | • Xeon Silver 4310 12 Core 2 Thread |
| Memory | • 16GB x 4EA |
| HDD | • 1TB * 2EA(Raid 1) |
| Power | • Redundant Power |

Specification Name: Security Software, Jenersystem, IEUMnet V1.0, Network Interconnection Security Solution, 1 Package, Server CNS

Identification Number 25342306
Amount (Including VAT) ₩38,500,000

### IEUMnet-ONS



CCTV Enclosure Terminal Equipment

| Category | System Specifications |
|---|---|
| Interface | • 4Port 10/100/1000 Base-TX |
| CPU | • MTK MT7621A, Dual-core MIPS1004Kc |
| Memory | • 256MB |
| HDD | • 32MB |
| Power | • Single Power |

Specification Name: Security Software, Jenersystem, IEUMnet V1.0, Network Interconnection Security Solution, 1 Package, **Client ONS**

Identification Number 25342307
Amount (Including VAT) ₩500,000

### IEUMnet-SONS



CCTV Enclosure Switch Equipment

| Category | System Specifications |
|---|---|
| Ethernet | • Gigabot Ethernet 2ea |
| CPU | • Quad-core ARM Cortex-A55 |
| Memory | • 1GB LPDDR4 / 2GB LPDDR4X |
| HDD | • eMMC 32GB (Optional) |
| Power | • Single Power |

Specification Name: Security Software, Jenersystem, IEUMnet V1.0, Network Interconnection Security Solution, 1 Package, **Switch SONS**

Identification Number 26050514
Amount (Including VAT) ₩2,400,000

# 04 Implementation Cases

# 01 CCTV Network Security Project Performance

## IEUMnet Performance

| No. | Year of Implementation | Site | Project Name |
|---|---|---|---|
| 1 | 2024 | Dongdaemun-gu Office, Seoul | Implementation of CCTV Section Security System |
| 2 | 2024 | Anyang City Hall, Gyeonggi-do | Implementation of CCTV Section Security System (Autonomous Bus Section) |
| 3 | 2024 | Songpa-gu Office, Seoul | Implementation of CCTV Section Security System |
| 4 | 2025 | Dongdaemun-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System (Expansion) |
| 5 | 2025 | Seongbuk-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System |
| 6 | 2025 | Yangcheon-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System |
| 7 | 2025 | Eunpyeong-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System |
| 8 | 2025 | Anyang City Hall, Gyeonggi-do | Improvement of Vulnerable Security Facilities on Trail Routes (Expansion) |
| 9 | 2025 | Seodaemun-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System |
| 10 | 2025 | Jongno-gu Office, Seoul | Purchase and Installation of CCTV Network Security Enhancement System |

# 05 Penetration Testing for CCTV Network Vulnerabilities

# 01 CCTV Network Vulnerability Penetration Test (Before Implementation)

JENER SYSTEM

## 1. Project Name

- ○○-gu CCTV Network Penetration Test

## 2. Project Overview

### 2.1 Objective

This penetration test is conducted on the ○○-gu CCTV network by selecting test scenarios tailored to system characteristics and environment. After performing the test, identified security vulnerabilities will be reported to ensure secure operation and service stability.

### 2.2. Scope and IP

The penetration test will be conducted on the following operational services.

| NO | Target(URL) | Category | Internal/ External | IP Address |
|---|---|---|---|---|
| 1 | ○○-gu CCTV Sample (1 Set)<br>(CCTV near the East Gate Entrance of ○○ Ri○○ Apartment) | Network Device | External | 168.XXX.12.187 |

# CCTV Network Vulnerability Penetration Test (Before Implementation)



## 3. Test Item

### 3.1 Test Scenario

A penetration test was conducted on the CCTV network by connecting an arbitrary LAN cable to the sampled CCTV, and the test was performed as a black-box test without any prior knowledge of the IT infrastructure.

| NO | Penetration Test Execution Scenario | Remarks |
|---|---|---|
| 1 | Attempt to scan the network and obtain IP information of the target CCTV | |
| 2 | Attempt unauthorized intrusion to nearby CCTV devices from the target CCTV | |
| 3 | Attempt to obtain administrator authentication page information through analysis of active service ports on CCTV | |
| 4 | Attempt to bypass authentication on the CCTV administrator page and gain control of management functions | |
| 5 | Attempt to extract video data and perform unauthorized manipulation after successful authentication bypass | |
| 6 | Attempt to take control of the integrated monitoring system via CCTV and network relay points | |

## 4. Summary of Results

As a result of the CCTV network penetration test, five types of security vulnerabilities were identified.

| NO | Penetration Test Execution Scenario | Inspection Result |
|---|---|---|
| 1 | Attempt to scan the network and obtain IP information of the target CCTV | Vulnerable |
| 2 | Attempt unauthorized intrusion to nearby CCTV devices from the target CCTV | Vulnerable |
| 3 | Attempt to obtain administrator authentication page information through analysis of active service ports on CCTV | Vulnerable |
| 4 | Attempt to bypass authentication on the CCTV administrator page and gain control of management functions | Vulnerable |
| 5 | Attempt to extract video data and perform unauthorized manipulation after successful authentication bypass | Vulnerable |
| 6 | Attempt to take control of the integrated monitoring system via CCTV and network relay points | Secure |

# CCTV Network Vulnerability Penetration Test (Before Implementation)



## 5. Overall Assessment

In summary, by simply connecting a LAN cable to the switching hub linked to a sampled CCTV, it was possible to move across and access different networks where thousands of CCTV devices are connected. Access to the CCTV management tool was easily achieved, and by bypassing authentication, most CCTV systems could be unlawfully controlled, with real-time video acquisition possible.

This indicates that the CCTV system is in a highly vulnerable security state, allowing the potential for various illegal and malicious activities.

Therefore, it is recommended to refer to this document and take necessary measures to ensure the secure operation of the CCTV systems.

# CCTV Network Vulnerability Penetration Test (After Implementation)



## 3. Test Items

### 3.1 Test Scenario

The penetration test on the CCTV network was conducted by connecting the sampled CCTV to the security solution and switch equipment, and it was performed as a black-box test without any prior knowledge of the IT infrastructure.

| NO | Penetration Test Execution Scenario |
|---|---|
| 1 | Attempt to scan the network and obtain IP information of the target CCTV |
| 2 | Attempt unauthorized intrusion to nearby CCTV devices from the CCTV equipped with the security solution |
| 3 | Attempt to obtain administrator authentication page information by analyzing active service ports on the CCTV equipped with the security solution |
| 4 | Attempt to bypass authentication on the administrator page of the CCTV equipped with the security solution and gain control of management functions |
| 5 | Attempt to extract video data and perform unauthorized manipulation after successfully bypassing authentication on the CCTV equipped with the security solution |

## 4. Summary of Results

As a result of the CCTV network penetration test, no security vulnerabilities were identified.

| NO | Penetration Test Execution Scenario | Inspection Result |
|---|---|---|
| 1 | Attempt to scan the network and obtain IP information of the target CCTV | Secure |
| 2 | Attempt unauthorized intrusion to nearby CCTV devices from the CCTV equipped with the security solution | Secure |
| 3 | Attempt to obtain administrator authentication page information by analyzing active service ports on the CCTV equipped with the security solution | Secure |
| 4 | Attempt to bypass authentication on the administrator page of the CCTV equipped with the security solution and gain control of management functions | Secure |
| 5 | Attempt to extract video data and perform unauthorized manipulation after successfully bypassing authentication on the CCTV equipped with the security solution | Secure |

## 5. Overall Assessment

The ○○-gu CCTV Network Penetration Test has been completed.

### Test Results

In the second penetration test conducted on the ○○-gu CCTV network with the security solution applied, all results were satisfactory, and no vulnerabilities were identified.

In the scenario “Attempt to scan the network and obtain IP information of the target CCTV,” no IP information could be obtained when connecting via LAN to the CCTV equipped with the security solution without any prior information, confirming it to be secure.

In the scenario “Attempt unauthorized intrusion to nearby CCTV devices from the CCTV equipped with the security solution,” scanning the entire network range revealed no other networks beyond the connected CCTV network, confirming it to be secure.

In the scenario “Attempt to obtain administrator page information by analyzing active service ports on the CCTV equipped with the security solution,” network scanning was not possible, and therefore service port analysis could not be performed, confirming it to be secure.

## 5. Overall Assessment

### Test Results (Continued)

In the scenario “Attempt to bypass authentication and gain control of the CCTV management page equipped with the security solution,” network scanning and service port analysis were not possible, preventing access to the management tool page, and it was confirmed to be secure.
In the scenario “Attempt to extract video data and perform unauthorized manipulation after successful authentication bypass on CCTV equipped with the security solution,” access to the management tool page was not possible, preventing authentication bypass and video extraction, confirming it to be secure.

In summary, from a sampled CCTV equipped with the security solution, it was not possible to discover nearby CCTV devices via LAN connection, and further attack attempts were difficult to proceed.

**This concludes the second penetration test of the ○○-gu CCTV network.**