開創資安解決方案新道路的 JENER SYSTEM 多重領域網路安全解決方案 IEUMnet



【基於多重領域網路安全】

CCTV通訊網路安全強化

★「國家情報院安全要求事項 V3.0 規範」認證解決方案

JENER SYSTEM

CONTENTS

IoT 環境終端（CCTV、IP攝影機等）入侵／駭客攻擊阻斷解決方案



01 CCTV網路安全強化概要

02 CCTV網路安全強化背景

03 CCTV網路安全強化 IEUMnet

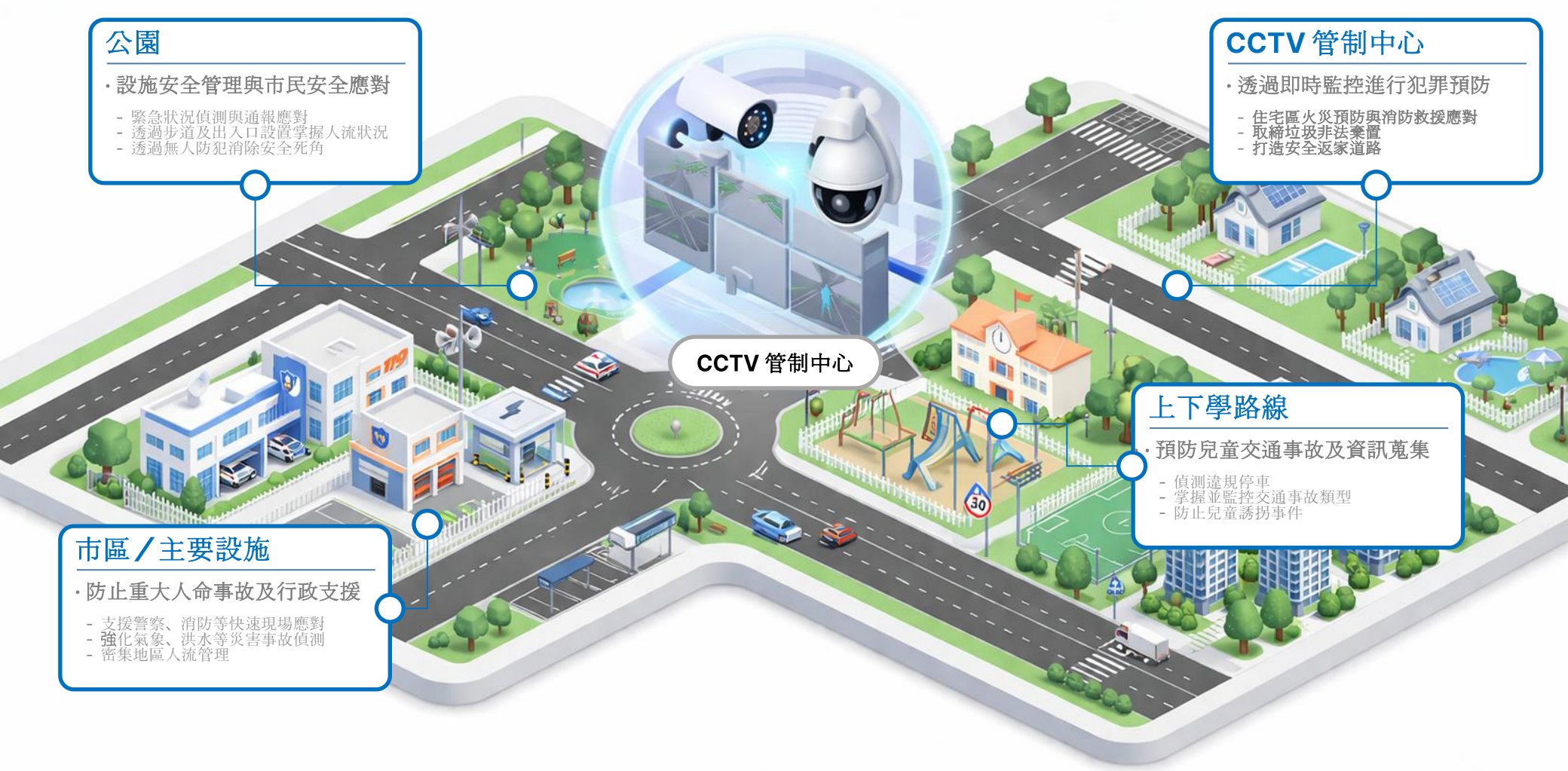
04 CCTV網路安全強化建置實績

05 CCTV網路弱點模擬滲透測試

01 CCTV網路安全強化概要

01 CCTV 通訊網路安全強化

CCTV 在我們的日常生活中肩負著守護國民安全的責任。



02 CCTV 通訊網路安全強化

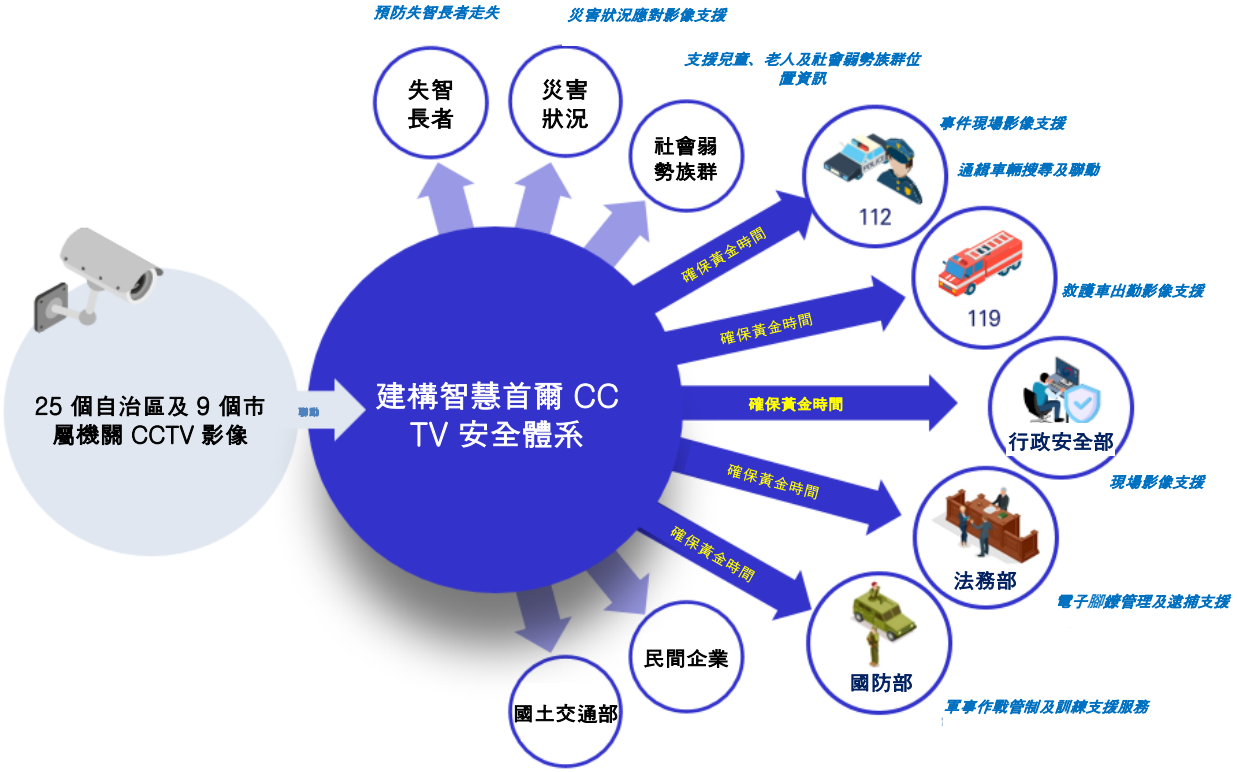
概要

CCTV 在我們的日常生活中肩負著守護國民安全的責任。

為了保障國民安全而運作中的 CCTV 影像資訊，不僅應用於防犯、兒童保護、都市公園與遊樂場、垃圾非法棄置取締、交通取締及交通資訊蒐集與分析，還透過 AI 基礎智慧型篩選監控，迅速偵測並即時應對犯罪預防、暴力、徘徊、跌倒等緊急狀況，對市民安全發揮重要作用。

數位安全城市 CCTV 安全網服務





03 CCTV 通訊網路安全強化

事業背景

首爾市營運中的CCTV影像監控設備設置及營運現況

首爾市CCTV安全中心聯動機關影像資訊提供現況實績

設置於首爾市的 CCTV 影像監控設備截至 2023 年 12 月底已安裝並營運約 17 萬 7,000 台，並透過首爾市 CCTV 安全中心整合平台，向相關機關聯動提供 414 萬 5,582 件影像資訊，致力於保障市民安全。

首爾市 CCTV 設置現況（單位：台，截至 2025 年 12 月 31 日）

區分	CCTV總計	犯罪預防及調查					設施安全・火災預防	交通取締	交通資訊蒐集・分析	其他法令
		小計	防犯	兒童保護區	公園・遊樂場	垃圾非法棄置				
自治區	122,613	108,947	80,885	8,874	18,327	861	4,426	8,811	153	276

首爾市 CCTV 設置現況（單位：台，截至 2024 年 12 月 31 日）

區分	CCTV總計	犯罪預防及調查					設施安全・火災預防	交通取締	交通資訊蒐集・分析	其他法令
		小計	防犯	兒童保護區	公園・遊樂場	垃圾非法棄置				
自治區	113,273	99,758	74,807	8,704	15,417	830	4,482	8,648	18	367

02 CCTV網路安全強化背景

01 IEUMnet 開發背景

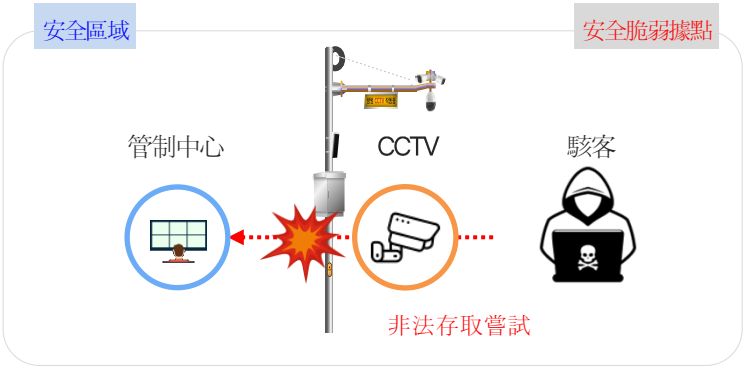
事業必要性_CCTV 網路安全強化

"公共機關的安全系統需要能維持靈活性與效率，並可應對內部威脅與外部攻擊的強大安全解決方案。"

現況（AS-IS）

安全弱點（遠端地區、無人據點）

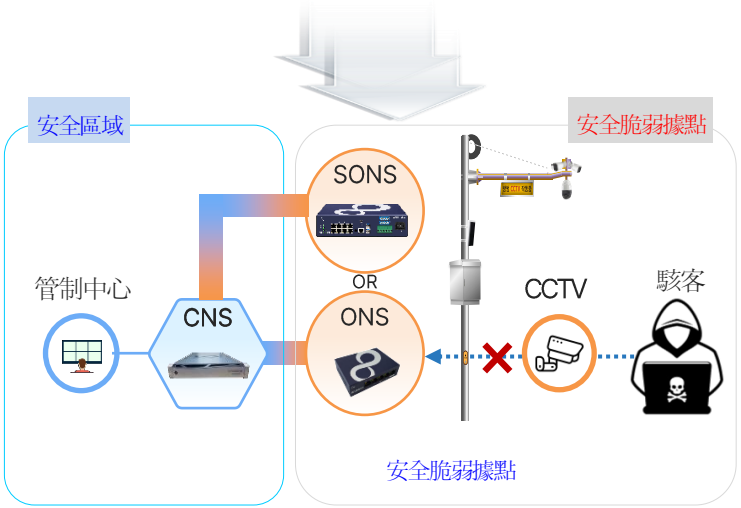
- 多數 CCTV 網路現場設施出現安全漏洞
- 安全脆弱據點管理困難
- 存在透過安全脆弱路徑進行存取嘗試的可能性



改善方案（TO-BE）

安全脆弱據點管理

- 完全阻斷非法安全脆弱路徑並進行安全管理
- 確保 CCTV 網路區段資料的可靠性與完整性
- 維持非安全／安全區域的封閉性與獨立性



※ CCTV → ONS → SWITCH → 防火牆 → CNS
※ CCTV → SONS → 防火牆 → CNS

01 IEUMnet 開發背景

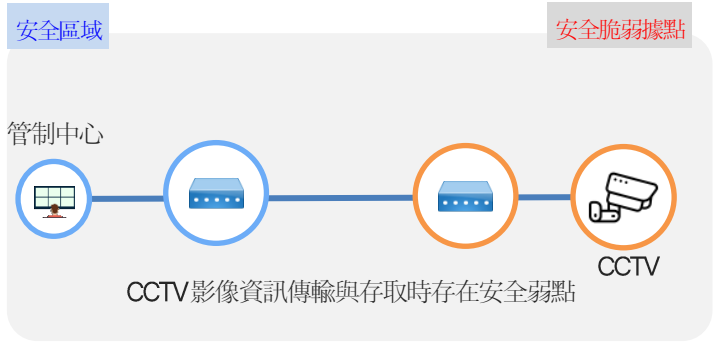
事業必要性_CCTV 網路安全強化（續）

"公共機關的安全系統需要能維持靈活性與效率，並可應對內部威脅與外部攻擊的強大安全解決方案。"

現況（AS-IS）

需要確保影像資料的安全性、可靠性與安全防護

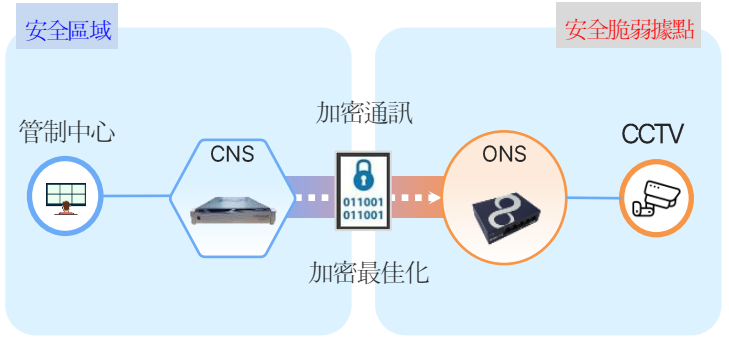
- 因封閉網路運作導致網路區段出現安全弱點
- CCTV 影像資訊傳輸時需要確保完整性與可靠性
- 對 CCTV 網路區段安全的認知不足



改善方案（TO-BE）

確保 CCTV 影像資訊的完整性與可靠性

- 採用經過驗證具安全性的 CCTV 網路加密通訊
- 最大化單向通訊優勢以確保封閉性
- 為將效能降低最小化而進行最佳化設計



01 IEUMnet 開發背景

JENER SYSTEM

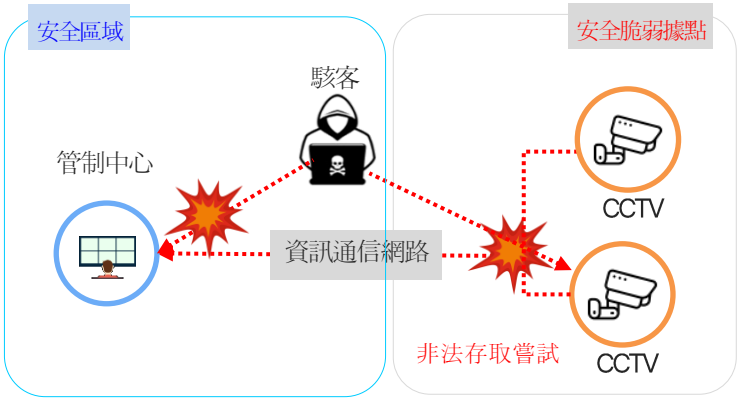
事業必要性_CCTV 網路安全強化（續）

"公共機關的安全系統需要能維持靈活性與效率，並可應對內部威脅與外部攻擊的強大安全解決方案。"

現況（AS-IS）

安全弱點（遠端地區、無人據點）

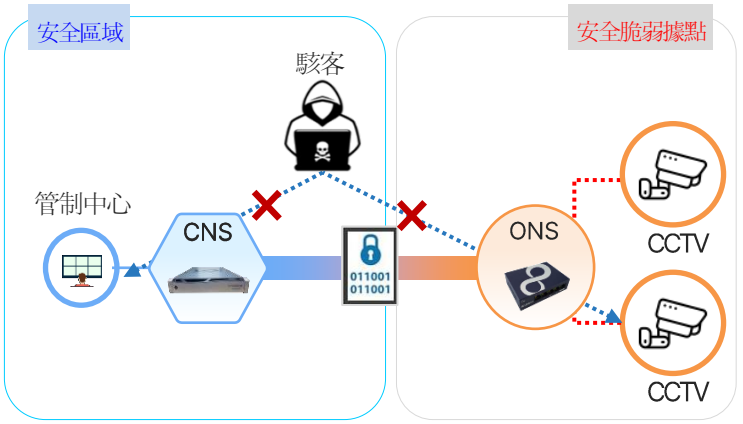
- 資訊通信網路（租用網、自建網）出現安全漏洞
- 多數安全脆弱據點管理困難
- 存在透過安全脆弱路徑進行存取嘗試的可能性



改善方案（TO-BE）

對安全脆弱據點進行安全管理

- 對安全脆弱據點進行安全管理
- 對多數脆弱據點進行 1:N 中央統合安全管理
- 確保資料的可靠性與完整性
- 維持非安全／安全區域的封閉性



02 CCTV 設置現況

JENER SYSTEM

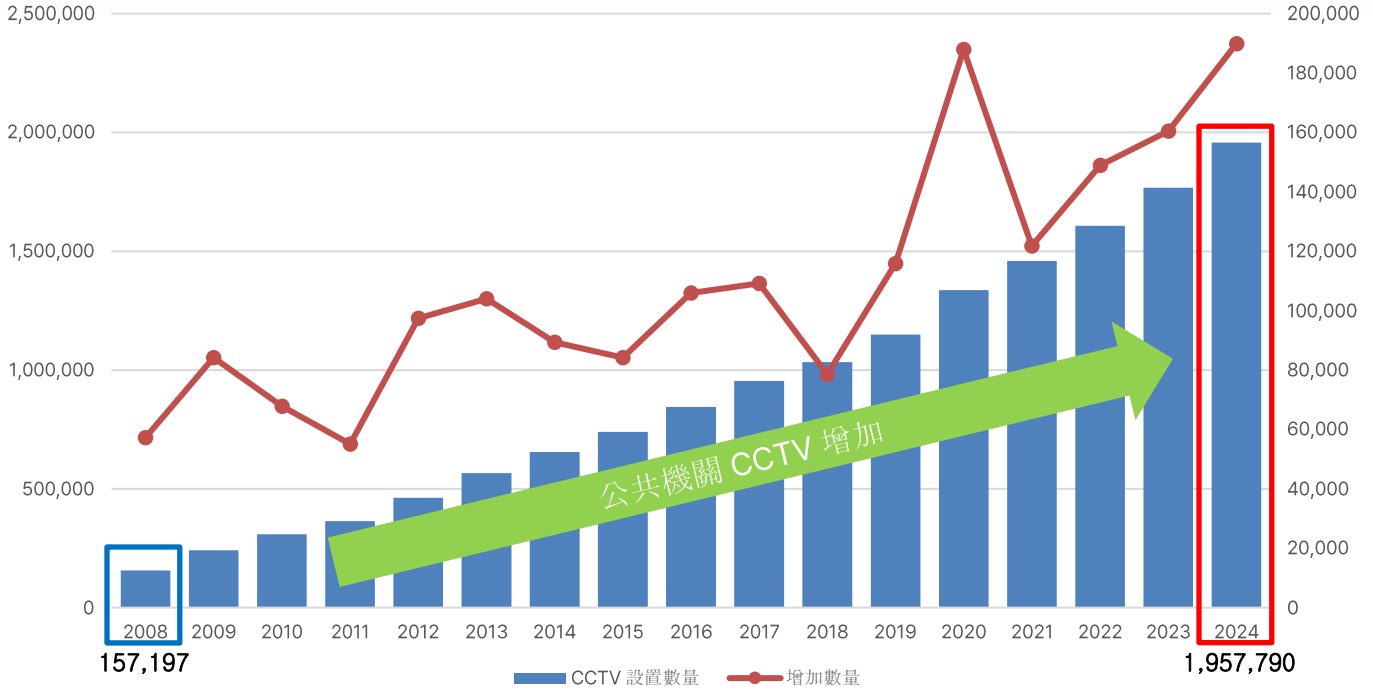
背景

資料來源：e-나라指標

(指標服務e나라指標 (index.go.kr))



公共機關 CCTV 設置及增加數量



資料來源：實態調查及個人資訊保護綜合支援系統現況資料

每年平均 CCTV 增設超過 10% 並進行性能改善

(Unit: Units)

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
CCTV 總設置數量（台）	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
較前一年增加數量（台）	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
較前一年增減比率（%）	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

註釋：公共機關 CCTV 設置及營運現況截至 2011 年（2010 年資料）為止，由各公共機關個別調查與彙整；自 2012 年（2011 年資料）起，公共機關需於每年 3 月底前將現況登錄於個人資訊保護綜合支援系統。

02 CCTV 設置現況

背景



每年平均 CCTV 增設超過 10% 並進行性能改善











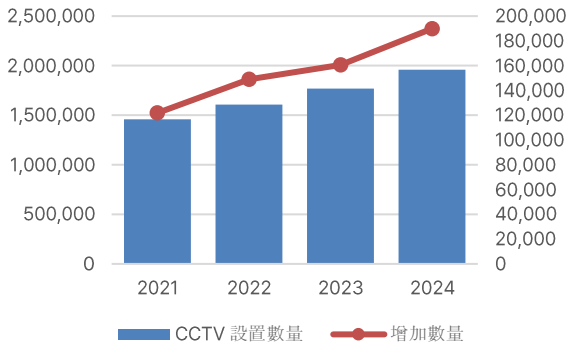




公共機關 CCTV 設置數量

	2021	2022	2023	2024
CCTV 總設置數量(台)	1,458,465	1,607,388	1,767,894	1,957,790
較前一年增加數量(台)	121,812	148,923	160,506	189,896
較前一年增減比率(%)	9.1	10.2	10	10.7

公共機關 CCTV 增加圖表

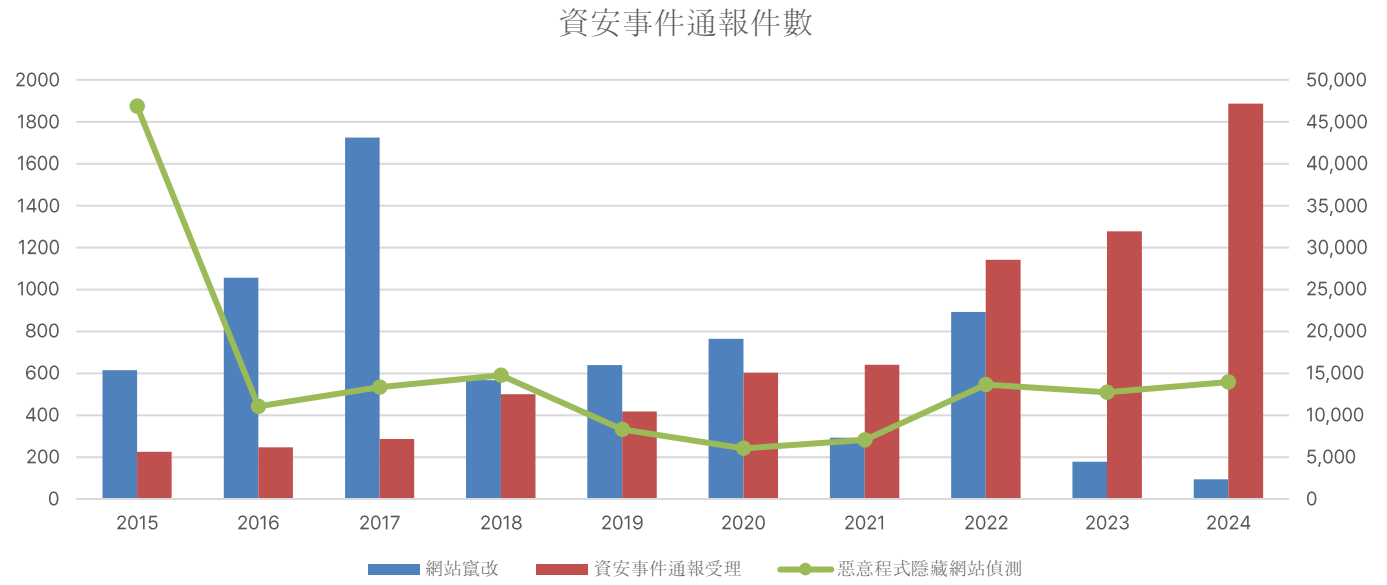


資料來源：e-나라指標
(指標服務：e-나라指標 (index.go.kr))

03 損害案例

資安事件通報件數統計

駭客攻擊事件件數指標，是指韓國網際網路振興院偵測並處理國內網站遭竄改的案件數、針對國內網站偵測並處理惡意程式隱藏網站的案件數，以及依據《資訊通信網法》由民間領域（機關及企業）通報的資安事件件數總和。



資安事件通報件數

資料來源：韓國網際網路振興院

區分	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
網站竄改	615	1,056	1,724	567	639	764	292	893	178	94
資安事件通報受理	225	247	287	500	418	603	640	1,142	1,277	1,887
惡意程式隱藏網站偵測	46,850	11,044	13,347	14,754	8,299	6,034	7,043	13,661	12,731	13,967

04 導入必要性

導入必要性

必須透過強化 CCTV 通訊網路安全來解決技術性安全問題。

- 針對 24 小時全年無休於無人遠端地區運作中的 CCTV 網路（CCTV 攝影機 ↔ 綜合管制中心網路區段）
  - 控制透過未授權及非法安全脆弱路徑的存取
  - 透過加密通訊確保機密性並保障安全網路區段
  - 確保 AI 基礎 CCTV 影像資料的可靠性與完整性
- 改善安全 CCTV 營運中的安全弱點

透過導入強大安全系統來強化技術性安全，防止資安事故發生



透過強化實體／技術／管理安全來防止資安外洩事故

CCTV 網路 + IEUMnet

- 擴充入侵／駭客防禦系統
- 消除安全弱點

1 Step 實體安全強化

保護建築物、設備等實體資訊系統資產

- 系統室設備安全
- 出入口管制監控
- 伺服器存取控制及系統安全對策
- 各類設備及設施鎖定裝置保護

2 Step 技術性安全強化

為防止入侵及駭客攻擊等所進行的技術性控制

- 網路區段加密
- AI 基礎流量異常偵測
- 網路區段非法存取控制
- 管理脆弱據點安全強化

3 Step 管理性安全強化

為執行實體與技術安全所建立的管理性安全體系

- 內部員工及外包人力管理
- 資訊保護文件化
- 個人資料保護法教育與訓練
- 定期備份以防止資料保存與竄改

03 CCTV網路安全強化 IEUMnet

01 CCTV 安全 IEUMnet

零信任網路安全

IEUMnet



02 IEUMnet 核心特點

核心特點

IEUMnet



IEUMnet ..

經驗證的安全解決方案

- 國家情報院安全功能確認書認證
- GS 一級軟體品質認證
- 已完成首爾市等地方自治團體現場驗證

多重區域網路安全

- 將非安全區域構成 1:N 多重區域聯動架構
- 多數外部終端的安全連接
- 保障靈活的擴充聯動性

網路隔離

- 實現分離式多重區域網路安全環境
- 從根本阻斷外部駭客攻擊
- 使用專用加密協定

強化安全性的 VPN 架構

- 可實現強化安全性的 VPN
- 遵循國家情報院安全指引
- 強化安全性並消除 Session 與安全政策弱點

內部資訊系統保護

- 資料傳輸前預先偵測惡意程式
- 單向通訊與細部化政策防止駭客攻擊
- 透過內部安全政策防止資料外洩

安全管理／服務持續性

- 各安全據點具獨立性與封閉性運作環境
- 遵循從源頭阻斷外部攻擊
- 整合政策營運與管理

韓國首創

網間資料傳輸產品部門安全功能確認書認證



符合國家情報院安全要求事項 V3.0 的產品

GOOD Software GS 一級軟體品質認證



02 IEUMnet 核心特點

核心特點

為了對多個安全脆弱或需要安全防護的現場據點進行整合安全管理

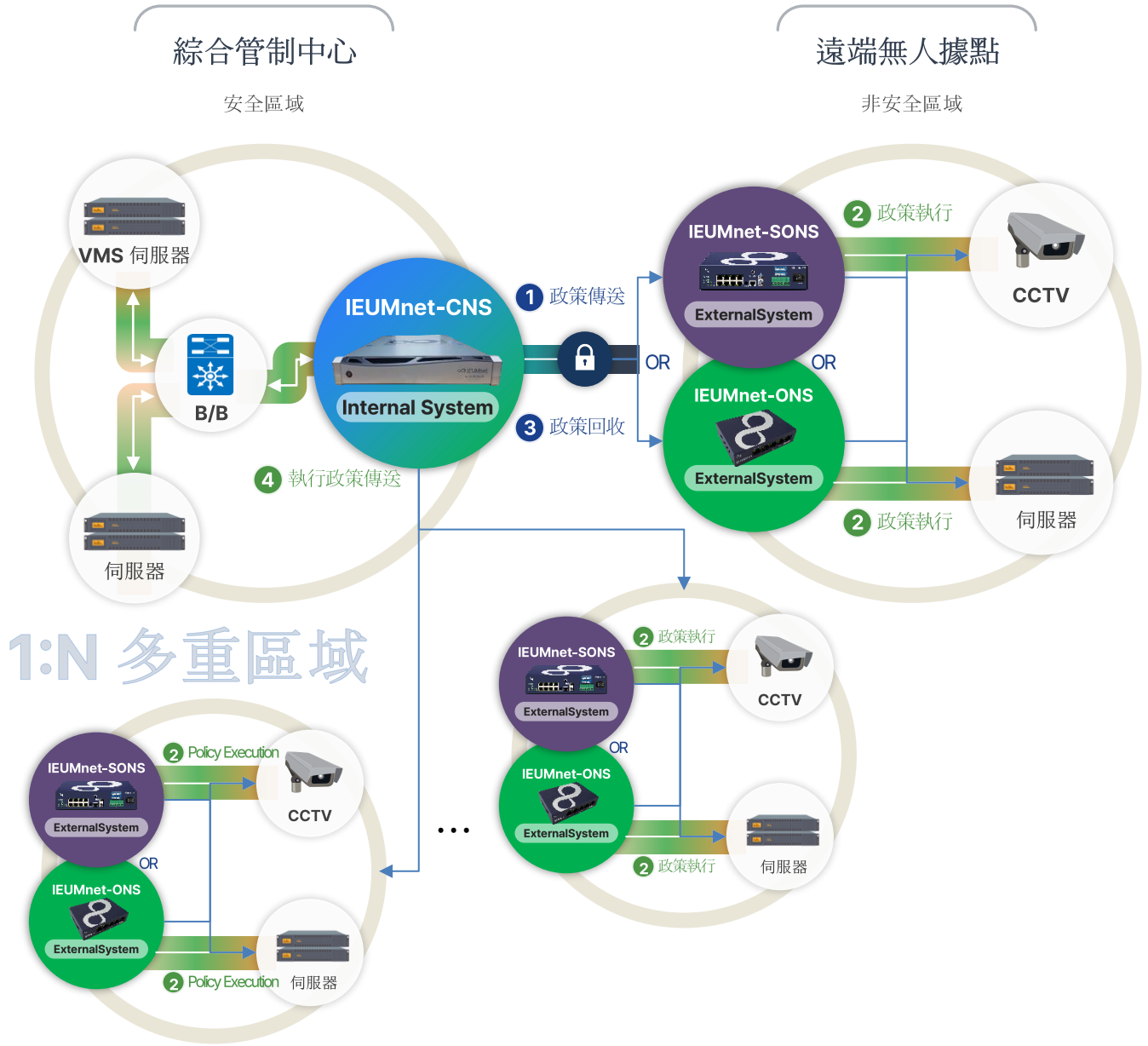
IEUMnet 是

適用於 CCTV 現場據點、遠端地區及無人據點等

透過封閉且獨立的架構運作來阻斷外部存取

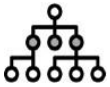
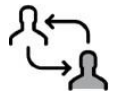
透過經驗證的加密通訊實現安全資料傳輸

提升安全性並提供安全服務持續性的解決方案



03 CCTV 網路安全強化應用系統

IEUMnet 應用領域

 居家辦公	居家辦公時，可不使用安全性較低的 VPN，而是透過實體 IEUMnet 從家中存取內部業務系統，並留下管理與操作紀錄等日誌，以實現安全使用。	 有線／無線整合	可靈活應用於 LTE 等無線網路與有線網路環境。
 分支據點聯動	總公司與分公司之間進行網路連接時，可使用安全等級高於 VPN 的 IEUMnet。	 海外工作人員	海外工作期間存取內部業務系統時，可透過 IEUMnet 提升管理明確性與安全性。
 民眾文件申請發放	民眾文件申請發放系統目前若使用安全性較低的 VPN 架構網路，可改由 IEUMnet 取代。	 控制網路	水庫、韓電網等遠端控制網路可透過單向通訊的 IEUMnet 架構提升安全性。
 ATM 設備	全國 ATM 設備系統若使用安全性較低的 VPN 架構網路，可改由 IEUMnet 取代。	 安全系統及基礎建設構建	建構整合網路等基礎設施時，如需在不同網路間建立安全隔離牆，可採用 IEUMnet 架構。

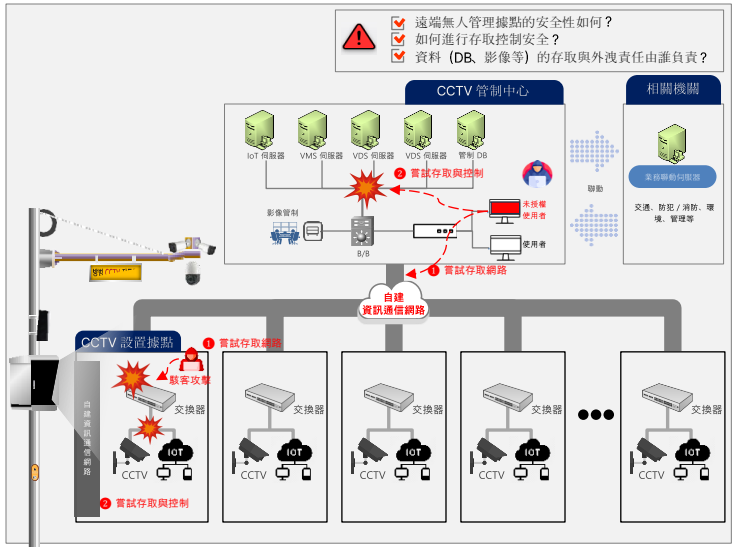
03 CCTV 網路安全強化應用系統

JENER SYSTEM

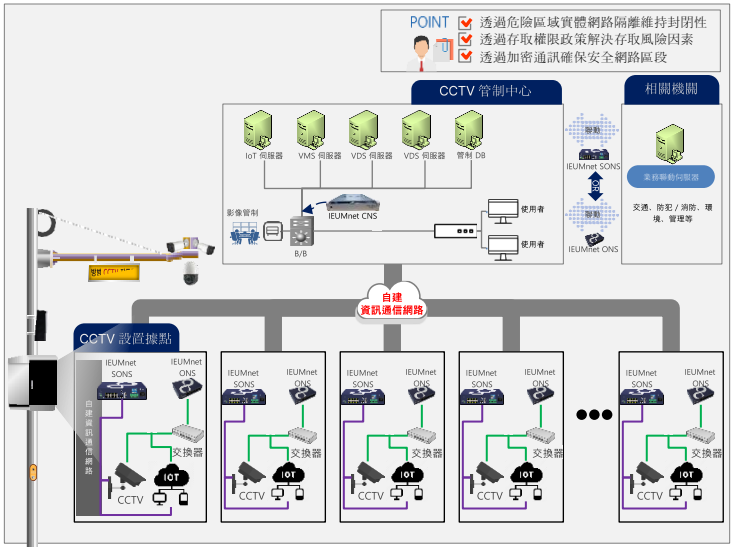
CCTV 網路安全強化架構圖

透過分離 CCTV 區段與內部網路，可從源頭阻斷由 CCTV 區段流入的病毒與駭客攻擊，進而保護地方政府電算資源。

改善前



改善後



CCTV 網路安全問題點

- CCTV 設置據點及遠端無人管理據點在網路存取上的安全問題
  - 透過存取及控制 CCTV 攝影機造成損害
  - 因脆弱據點及非工作時段非法存取控制不足而產生弱點
- 惡意內部使用者及未授權使用者存取內部系統的安全問題
  - 透過系統存取導致內部資訊（DB、CCTV 影像等）外洩
  - 因蓄意造成系統障礙（系統 Shut down、政策變更）而導致損害

透過 IEUMnet 的 CCTV 網路安全解決方案

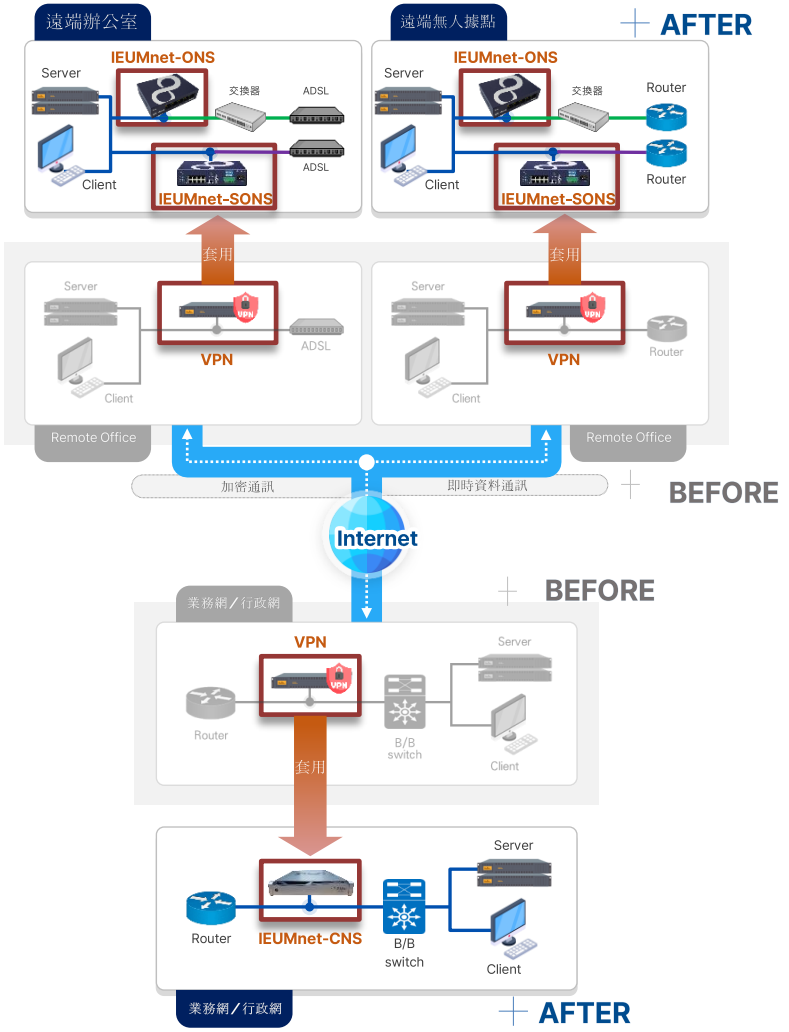
- 透過 CCTV 管制中心與遠端無人管理據點間經驗證的加密通訊，確保網路區段安全性
  - 透過白名單式管理，以已註冊設備及政策通訊解決 CCTV 攝影機存取問題
  - 透過維持非安全／安全據點的封閉性，從源頭阻斷通訊網路中的非法 CCTV 連線與存取
- 提升內部控制系統，提供運作中系統的穩定性與服務持續性
  - 透過政策變更雙重認證強化權限，解決內部資訊（DB、CCTV 影像等）的存取與外洩問題
  - 透過對未授權聯動／連線／阻斷的安全稽核紀錄、整合政策與整合管理，確保安全的營運管理方案

03 CCTV 網路安全強化應用系統

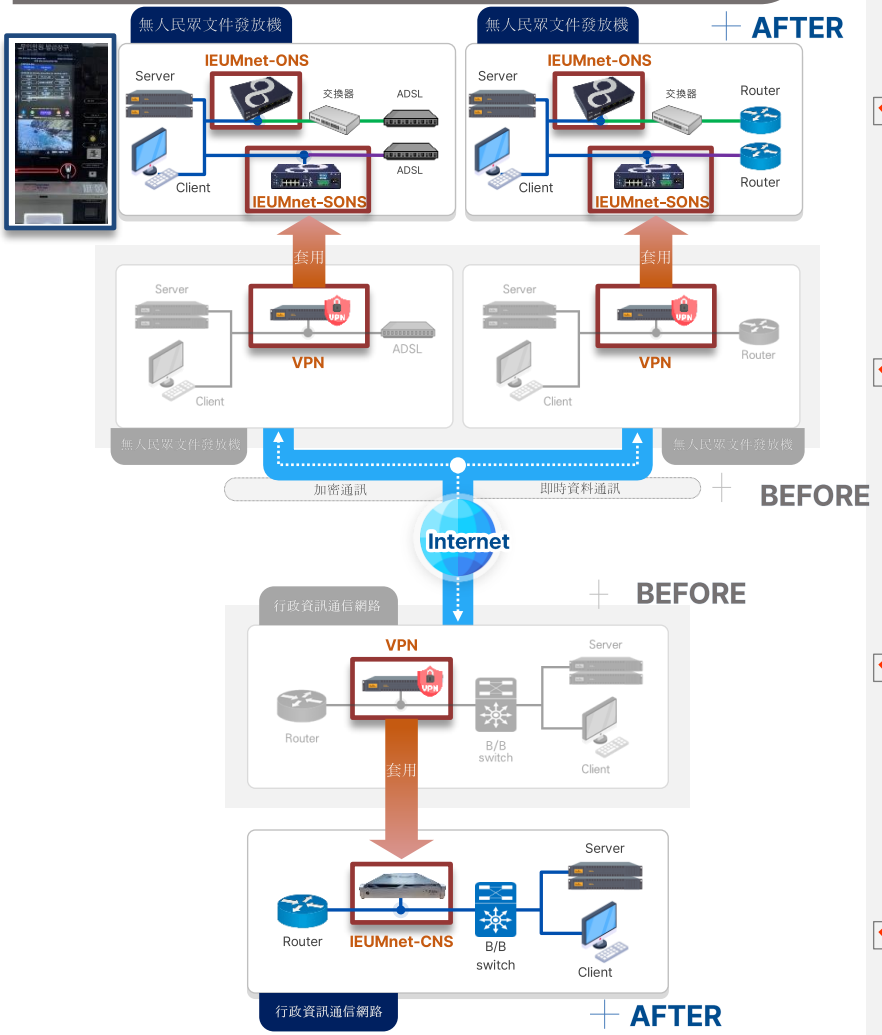
JENER SYSTEM

VPN 網路區段安全性強化

VPN 網路弱點安全強化目標架構圖



強化安全性的無人民眾文件發放機區段安全網路架構圖



- 透過加密通訊確保安全網路區段
- 透過非 TCP/IP 的專用協定通訊，維持實體封閉性並提供安全的服務持續性
- 在 VPN 區段中，除授權政策外無法存取業務網／行政網，並保障業務服務持續性
- 為阻斷網路存取，透過白名單式管理維持已註冊設備與政策通訊
- 透過整合政策與整合管理確保安全營運管理方案

03 CCTV 網路安全強化應用系統

導入效果

多重區域網路安全

IEUMnet 是

經驗證的安全解決方案

IEUMnet -ONS / IEUMnet -SONS

- 透過經驗證的加密通訊，確保影像資訊的機密性與可靠性
- 透過國家情報院安全功能確認書認證，遵循安全指引
- 已完成現場驗證解決方案（首爾市及地方自治團體）實證應用

強化安全性的網路

IEUMnet -ONS / IEUMnet -SONS

- 透過實體網路隔離實現強化安全性的網路安全架構
- 遵循國家情報院安全指引（安全功能確認書）
- 透過強化安全性（OS、開發語言）與安全政策消除弱點



強化安全態勢

IEUMnet -ONS / IEUMnet -SONS

- 提升整合安全管理效率並提供強大安全防護
- 透過數位環境危險區段存取控制、整合政策管理及最小化政策等方式，消除安全弱點並強化安全態勢

重要資產保護

IEUMnet -ONS / IEUMnet -SONS

- 透過強化通訊政策體系，將與外部連動的資料及內部網路區段的重要管理資料等，透過套用 IEUMnet 核心原則，安全地即時保護重要資產

最小化惡意行為者影響

IEUMnet -ONS / IEUMnet -SONS

- 透過對所有存取請求進行明確驗證的分層防禦，保護資料免受內外部威脅
- 透過 IEUMnet 核心原則所建立的強大安全態勢、細分化存取及最小化政策，將業務損害降至最低

法規遵循與領先

IEUMnet -ONS / IEUMnet -SONS

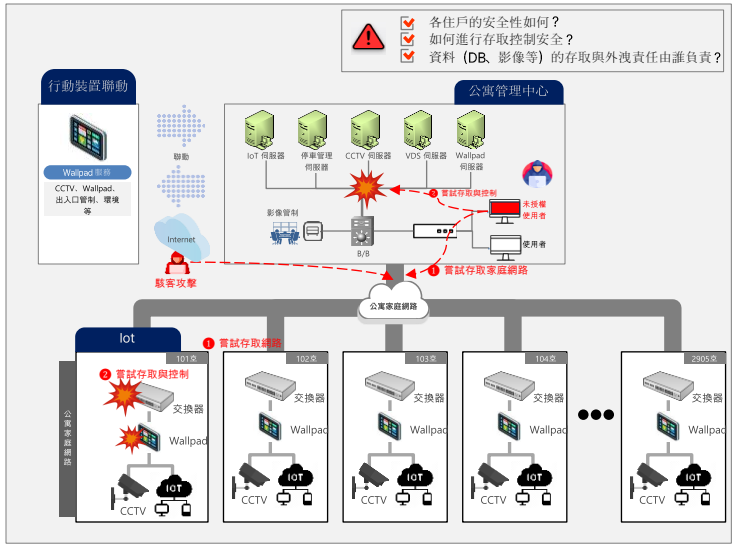
- 為即時服務聯動與資料保護，加強遵循持續變化的法規並因應監管要求
- 導入 IEUMnet 是為了實現「Network Security 服務」的領先安全強化與主動式安全應對

04 Wallpad 網路安全強化應用系統

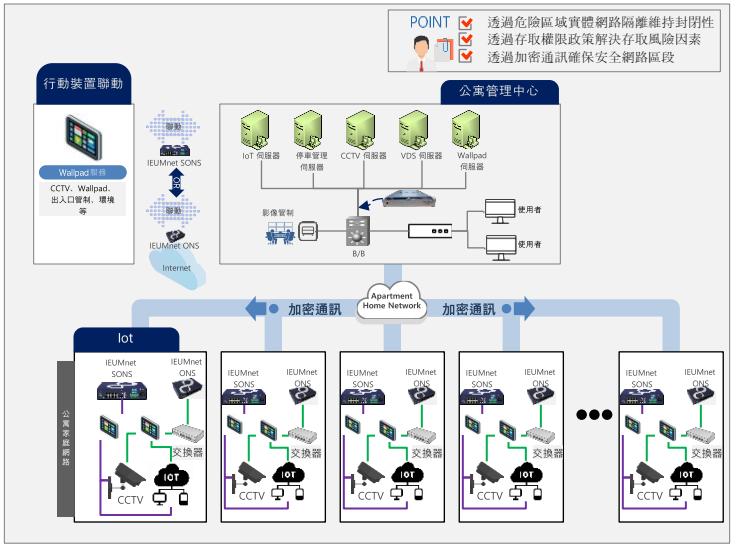
家庭網路區段安全強化

透過將家庭網路區段與各住戶網路分離並獨立運作，可從源頭阻斷流入家庭網路區段的內外部病毒與駭客攻擊，保護個人資產與個人資訊。

改善前



改善後



家庭網路安全問題點

- 家庭網路及各住戶 Wallpad 系統存取的安全問題
  - 因駭客攻擊及惡意程式等造成家庭網路通訊系統存取安全問題
  - 透過存取及控制運作中的各住戶 Wallpad 系統造成損害
- 惡意內部使用者及未授權使用者存取內部系統的安全問題
  - 透過存取家庭網路營運系統，導致內部資訊（CCTV、停車管理、Wallpad 等）外洩
  - 因蓄意造成系統障礙（系統 Shut down、政策變更）而導致損害

透過 IEUMnet 的家庭網路與 Wallpad 安全解決方案

- 透過家庭網路與各住戶間經國家情報院驗證的加密通訊，確保網路區段安全性
  - 透過白名單式管理，以已註冊設備與政策通訊解決各住戶 Wallpad 存取問題
  - 透過專用協定通訊維持實體封閉網路，並以各住戶獨立運作方式解決安全問題
- 提升內部控制系統，提供運作中系統的穩定性與服務持續性
  - 透過政策變更時的雙重認證強化權限，解決內部資訊（CCTV、停車管理、Wallpad 等）的存取與外洩問題
  - 透過對未授權聯動／連線／阻斷的安全稽核紀錄、整合政策與整合管理，確保安全營運管理方案

產品採購

· 採購廳數位服務商城

· 安全軟體

· 廠商名稱：JENER SYSTEM

· 產品採購構成

-IEUMnetV1.0, Server CNS
(伺服器軟體 + 硬體)

-IEUMnetV1.0, Switch SONS
(交換器 + 用戶端軟體)

- IEUMnetV1.0, Client ONS
(終端設備 + 用戶端軟體)

· 可大量供貨

IEUMnet-CNS



中心設備

區分	系統規格
介面	• SPC621D8U-2T C621A
CPU	• Xeon Silver 4310 12 Core 2 Thread
記憶體（RAM）	• 16GB x 4EA
HDD	• 1TB * 2EA(Raid 1)
電源	• 雙重電源

規格名稱：安全軟體，JENER SYSTEM，IEUMnet V1.0，網路聯動安全解決方案，1Package，Server CNS

採購識別編號 25342306
金額（含 VAT） ₩38,500,000

IEUMnet-ONS



CCTV 箱體內終端設備

區分	系統規格
介面	• 4Port 10/100/1000 Base-TX
CPU	• MTK MT7621A, Dual-core MIPS1004Kc
記憶體（RAM）	• 256MB
HDD	• 32MB
電源	• 單一電源

規格名稱：安全軟體，JENER SYSTEM，IEUMnet V1.0，網路聯動安全解決方案，1Package，**Client ONS**

採購識別編號 25342307
金額（含 VAT） ₩500,000

IEUMnet-SONS



CCTV 箱體內交換器設備

區分	系統規格
Ethernet	• Gigabot Ethernet 2ea
CPU	• Quad-core ARM Cortex-A55
記憶體（RAM）	• 1GB LPDDR4 / 2GB LPDDR4X
HDD	• eMMC 32GB (Optional)
電源	• 單一電源

規格名稱：安全軟體，JENER SYSTEM，IEUMnet V1.0，網路聯動安全解決方案，1Package，**Switch SONS**

採購識別編號 26050514
金額（含 VAT） ₩2,400,000

04 CCTV網路安全強化建置實績

01 CCTV 通訊網路安全建置實績

IEUMnet 實績

序號	導入年度	網站 / 機關	專案名稱
1	2024	首爾特別市 東大門區廳	導入 CCTV 區段安全系統
2	2024	京畿道 安養市廳	導入 CCTV 區段安全系統（自動駕駛巴士區段）
3	2024	首爾特別市 松坡區廳	導入 CCTV 區段安全系統
4	2025	首爾特別市 東大門區廳	CCTV 網路安全強化系統採購安裝（擴充安裝）
5	2025	首爾特別市 城北區廳	CCTV 網路安全強化系統採購安裝
6	2025	首爾特別市 陽川區廳	CCTV 網路安全強化系統採購安裝
7	2025	首爾特別市 恩平區廳	CCTV 網路安全強化系統採購安裝
8	2025	京畿道 安養市廳	環山步道登山路防犯設施脆弱區改善（擴充安裝）
9	2025	首爾特別市 西大門區廳	CCTV 網路安全強化系統採購安裝
10	2025	首爾特別市 鍾路區廳	CCTV 網路安全強化系統採購安裝

05 CCTV網路弱點模擬滲透測試

01 CCTV 網路弱點模擬滲透測試（套用前）

1. 專案名稱

- ○○區 CCTV 網路模擬滲透測試

2. 執行概要

2.1 目的

本次模擬滲透測試係針對 ○○區 CCTV 網路，依據系統特性及環境選定適當的模擬滲透測試情境進行測試，並於測試後告知所發現之安全弱點，以確保系統安全運作及服務穩定性為目的。

2.2. 執行對象及 IP

以下列正在運行中的服務為對象進行模擬滲透測試。

NO	執行對象(URL)	區分	內／外部	IP Address
1	○○區 CCTV 樣品 1式 (○○里○○公寓東門出入口附近 CCTV)	Network 設備	外部	168.XXX.12.187

3. 執行項目

3.1 執行情境

於抽樣之CCTV設備連接任意網路線後進行CCTV網路模擬滲透測試，並在未知任何IT基礎架構資訊的情況下，以黑箱測試方式進行。

NO	模擬滲透測試執行情境	-
1	嘗試搜尋目標CCTV網路並取得IP資訊	
2	嘗試透過目標CCTV非法入侵鄰近CCTV設備	
3	透過分析CCTV啟用中的服務埠，嘗試取得管理者認證頁面資訊	
4	嘗試繞過CCTV管理者認證頁面並取得管理功能控制權限	
5	於CCTV管理者認證繞過成功後，嘗試竊取影像資料及進行非法操作	
6	嘗試透過CCTV與網路中繼節點掌控整合管制系統	

4. 執行結果摘要

CCTV網路模擬滲透測試結果中，共檢測出5項安全弱點。

NO	模擬滲透測試執行情境	檢查結果
1	嘗試搜尋目標CCTV網路並取得IP資訊	脆弱
2	嘗試透過目標CCTV非法入侵鄰近CCTV設備	脆弱
3	透過分析CCTV啟用中的服務埠，嘗試取得管理者認證頁面資訊	脆弱
4	嘗試繞過CCTV管理者認證頁面並取得管理功能控制權限	脆弱
5	於CCTV管理者認證繞過成功後，嘗試竊取影像資料及進行非法操作	脆弱
6	嘗試透過CCTV與網路中繼節點掌控整合管制系統	良好

CCTV網路弱點模擬滲透測試（套用前）

5. 總評

簡而言之，僅需將網路線連接至抽樣之單一

CCTV所連接的交換器設備，

即可移動並存取周邊數千台以上**CCTV**所屬之不同網路區域，

且能輕易存取**CCTV**管理工具，

甚至可繞過認證功能，對多數**CCTV**進行非法操控及即時取得影像資料等行**為**。

此情況顯示CCTV系統目前處於高度安全脆弱狀態，存在遭受非法與惡意行**為**之風險。

因此，建議參考本文件內容，對CCTV系統進行安全性補**強**，以確保系統之安全運作。

01 CCTV網路弱點模擬滲透測試（套用後）

3. 執行項目

3.1 執行情境

於抽樣之CCTV分別連接安全解決方案與交換器設備後，進行CCTV網路模擬滲透測試，

並在未知任何IT基礎架構資訊的情況下，以黑箱測試方式進行。

NO	模擬滲透測試執行情境
1	嘗試搜尋目標CCTV網路並取得IP資訊
2	嘗試透過已安裝安全解決方案之CCTV非法入侵鄰近CCTV設備
3	透過分析已安裝安全解決方案之CCTV啟用中的服務埠，嘗試取得管理者認證頁面資訊
4	嘗試繞過已安裝安全解決方案之CCTV管理者認證頁面並取得管理功能控制權限
5	於已安裝安全解決方案之CCTV管理者認證繞過成功後，嘗試竊取影像資料及進行非法操作

4. 執行結果摘要

CCTV網路模擬滲透測試結果中檢測出安全弱點。

NO	模擬滲透測試執行情境	檢查結果
1	嘗試搜尋目標CCTV網路並取得IP資訊	良好
2	嘗試透過已安裝安全解決方案之CCTV非法入侵鄰近CCTV設備	良好
3	透過分析已安裝安全解決方案之CCTV啟用中的服務埠，嘗試取得管理者認證頁面資訊	良好
4	嘗試繞過已安裝安全解決方案之CCTV管理者認證頁面並取得管理功能控制權限	良好
5	於已安裝安全解決方案之CCTV管理者認證繞過成功後，嘗試竊取影像資料及進行非法操作	良好

5. 總評

已完成〇〇區CCTV網路模擬滲透測試。

執行結果

於安裝安全解決方案後進行之〇〇區CCTV網路第二次模擬滲透測試中，

所有測試結果皆為良好，未發現任何安全弱點。

於「嘗試搜尋目標CCTV網路並取得IP資訊」情境之安全診斷中，

在未取得任何事前資訊的情況下，僅將LAN連接至已安裝安全解決方案之CCTV時，

無法取得相關IP資訊，確認為安全狀態。

於「嘗試透過已安裝安全解決方案之CCTV非法入侵鄰近CCTV設備」情境之安全診斷中，

對已安裝安全解決方案之CCTV進行整體網路頻段掃描時，除筆記型電腦所連接之CCTV網路外，

無法搜尋到其他網路，確認為安全狀態。

於「透過分析已安裝安全解決方案之CCTV啟用中的服務埠，嘗試取得管理者頁面資訊」

情境之安全診斷中，由於無法對已安裝安全解決方案之CCTV進行網路掃描，

亦無法進行服務埠分析，因此確認為安全狀態。

5. 總評

執行結果

於「嘗試繞過已安裝安全解決方案之CCTV管理工具頁面認證並取得管理功能控制權限」情境之安全診斷中，
由於無法進行網路掃描與服務埠分析，因此無法存取管理工具頁面，
確認**為**安全狀態。

於「已安裝安全解決方案之CCTV在管理者認證繞過成功後，嘗試竊取影像及進行非法操作」情境之安全診斷中，
由於無法存取管理工具頁面，因此無法進行認證繞過及影像竊取，
確認**為**安全狀態。

簡而言之，於抽樣之已安裝安全解決方案的單一CCTV設備中，透過LAN連接後無法搜尋周邊CCTV，
並確認後續亦難以進行進一步攻擊。

以上為〇〇區CCTV網路第二次模擬滲透測試結果說明。