

智慧路燈系統資安測試規範 — 第二部：智慧照明

**Intelligent Streetlight System Cybersecurity Test Specification
- Part 2: Intelligent Lighting**

智慧路燈系統資安測試規範-

第二部：智慧照明

Intelligent Streetlight System Cybersecurity Test Specification - Part 2: Intelligent Lighting

出版日期: 2019/12/06

終審日期: 2019/09/27

此文件之著作權歸台灣資通產業標準協會所有，
非經本協會之同意，禁止任何形式的商業使用、重製或散佈。

Copyright© 2019 Taiwan Association of Information
and Communication Standards. All Rights Reserved.

誌謝

本標準由台灣資通產業標準協會—TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：安華聯網科技股份有限公司 洪光鈞 總經理

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 副主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 博士

T5C 物聯網資安工作組：財團法人資訊工業策進會 賴怡伶、劉濬銘、王勤為

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

中華電信股份有限公司、台灣德國萊因技術監護顧問股份有限公司、安華聯網科技股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣電子檢驗中心、財團法人資訊工業策進會、財團法人電信技術中心、國立交通大學、優力國際安全認證有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、台達電子工業股份有限公司、台灣 LED 照明產業聯盟、台灣飛樂喜萬年有限公司、光宇股份有限公司、安謀國際科技股份有限公司、威力工業網絡股份有限公司、思納捷科技股份有限公司、研揚科技股份有限公司、神通資訊科技股份有限公司、國立雲林科技大學、晶復科技股份有限公司、億光電子工業股份有限公司。

本標準由經濟部工業局支持研究制定。

目錄

誌謝.....	1
目錄.....	2
前言.....	4
引言.....	5
1. 適用範圍.....	6
2. 引用標準.....	7
3. 用語及定義.....	8
4. 測試項目分級.....	9
5. 資安測試規範-照明設備測試.....	11
5.1 身分識別、鑑別、權限控管測試.....	11
5.2 資料機密性與完整性測試.....	39
5.3 系統完整性測試.....	41
5.4 軟韌體更新測試.....	44
5.5 警示與紀錄測試.....	44
5.6 已知漏洞安全測試.....	44
5.7 軟體應用程式測試.....	45
6. 資安測試規範-照明監控伺服器測試.....	46
6.1 身分識別、鑑別、權限控管要求測試.....	46
6.2 資料機密性與完整性測試.....	46
6.3 警示與紀錄測試.....	46
6.4 已知漏洞安全測試.....	47
6.5 軟體應用程式測試.....	47
6.6 資源可用性測試.....	47
6.7 隱私保護測試.....	48
6.8 雲端平台安全測試.....	48
7. 資安測試規範-照明監控閘道器安全特殊要求測試.....	49

7.1 身分識別、鑑別、權限控管要求測試.....	49
7.2 資料機密性與完整性測試.....	49
7.3 系統完整性測試.....	49
7.4 軟韌體更新測試.....	50
7.5 警示與紀錄測試.....	50
7.6 已知漏洞安全測試.....	50
7.7 軟體應用程式測試.....	51
附錄 A (規定) 安全通道建議使用之密碼套件.....	52
參考資料.....	53
版本修改紀錄.....	54

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業規範。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

隨著物聯網與雲端運算技術的廣泛應用，在經濟部工業局發展智慧城市計畫與能源局擴大補助 LED 路燈計畫的帶動下，路燈燈桿上開始附加各種感測器，透過其連網功能將收集到的交通及環境資料回傳雲端分析，進而衍生出智慧路燈照明系統。根據 2016 年 Philip 市場調查報告指出，全球路燈市場規模約 3 億盞，目前全球具備聯網功能的路燈平均每年複合成長率達 16%；IEK 預估 2020 年全球智慧路燈市場規模達 34.3 億美元。台灣在各地地方政府投入的智慧照明路燈公共工程及億光、光寶、台達電等大廠的帶領下，單以台北市為例，過去每年路燈照明電費約 3 億元，路燈升級後電費降至 1.7 億元。在帶來節能與生活便利的同時，伴隨而來的網路攻擊對資訊安全與隱私造成極大的威脅，如 2016 年白帽駭客發現透過 ZigBee 的 Touchlink 控制系統的漏洞，利用 Philips 智慧燈泡更新韌體時植入蠕蟲發動 DDoS 攻擊，成功掌控城市路燈並癱瘓城市照明。

「TAICS TS-0028-2 智慧路燈系統資安測試規範-第二部：智慧照明」(以下簡稱本測試規範)，依據台灣資通產業標準協會所制定之「TAICS TS-0027-2 智慧路燈系統資安標準-第二部：智慧照明」[1]訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法與檢測結果等事項。俾利智慧照明系統裝置製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。

1. 適用範圍

本系列標準適用於智慧照明系統，智慧照明是由照明監控伺服器、照明監控閘道器及照明設備所組成，如下圖 1 所示。

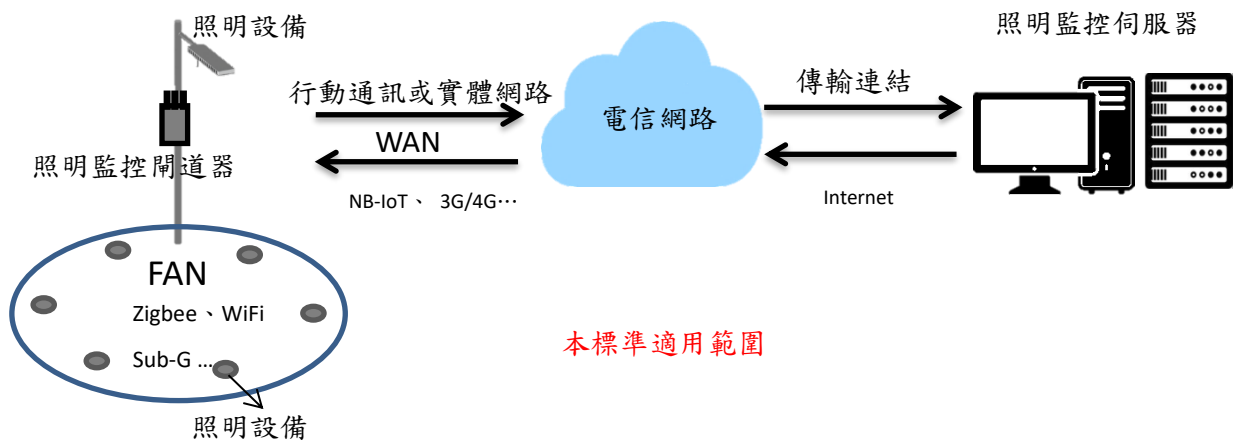


圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] TAICS TS-0027-2：2019 智慧路燈系統資安標準-第二部：智慧照明

3. 用語及定義

TAICS TS-0027-2「智慧路燈系統資安標準-智慧照明」所述，及下列用語及定義適用於本標準。

3.1 密碼套件(Cipher Suite)

係指使用於安全通道(SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(MAC)和金鑰交換演算法。

3.2 網路埠(Port)

網路埠，又稱為通訊埠或者連接埠，作為連網裝置與外部來源之間傳送/接收通訊資料的端口。

3.3 網路埠掃描(Port Scan)

使用網路掃描工具對網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，以此確認可使用的埠口，進一步探尋其漏洞，藉此找到未經授權的存取點。

4. 測試項目分級

本節依據 TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」制定相對應之安全測試項目與測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：(1)身分識別、鑑別、權限控管測試、(2)資料機密性與完整性測試、(3)系統完整性測試、(4)軟體更新測試、(5)警示與紀錄測試、(6)已知漏洞安全測試及(7)軟體應用程式測試，及照明監控伺服器安全要求的安全構面(8)資源可用性、(9)隱私保護及(10)雲端平台安全；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品須先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試標準等級總表

安全構面	安全測試分項	安全等級		
		1 級	2 級	3 級
5. 標準規範-照明設備				
5.1 身分識別、鑑別、權限控管測試	5.1.1 鑑別機制測試	5.1.1.2 5.1.1.3	-	-
	5.1.2 權限管控測試	-	-	-
	5.1.3 通行碼鑑別測試	5.1.3.2	-	5.1.3.3 5.1.3.4
5.2 資料機密性與完整性測試	5.2.1 安全敏感性資料儲存測試	-	5.2.1.2	5.2.1.3
	5.2.2 傳輸資料保護測試	-	-	-
5.3 系統完整性測試	5.3.1 實體入侵防護測試	-	5.3.1.2	5.3.1.3
5.4 軟韌體更新測試	5.4.1 更新安全測試	-	-	-
5.5 警示與紀錄測試	5.5.1 日誌檔與警示測試	-	-	-
5.6 已知漏洞安全測試	5.6.1 作業系統與網路服務測試	-	-	-
	5.6.2 網路服務連接埠測試	-	-	-

安全構面	安全測試分項	安全等級		
		1 級	2 級	3 級
5.7 軟體應用程式測試	5.7.1 應用程式安全測試	-	-	-
6. 標準規範-照明監控伺服器				
6.1 身分識別、鑑別、權限控管要求	6.1.1 鑑別機制	-	-	-
	6.1.2 權限控管	-	-	-
	6.1.3 通行碼鑑別	-	-	-
6.2 資料機密性與完整性	6.2.1 安全敏感性資料儲存	-	-	-
	6.2.2 傳輸資料保護	-	-	-
6.3 警示與紀錄	6.3.1 日誌檔與警示	-	-	-
6.4 已知漏洞安全	6.4.1 作業系統與網路服務	-	-	-
	6.4.2 網路服務連接埠	-	-	-
6.5 軟體應用程式	6.5.1 網頁管理介面安全	-	-	-
6.6 資源可用性	6.6.1 備份	-	-	-
6.7 隱私保護	6.7.1 隱私保護能力	-	-	-
6.8 雲端平台安全	6.8.1 雲端安全要求	-	-	-
7. 標準規範-照明監控閘道器安全特殊要求				
7.1 身分識別、鑑別、權限控管	7.1.1 鑑別機制	-	-	-
	7.1.2 權限管控	-	-	-
	7.1.3 通行碼鑑別	-	-	-
7.2 資料機密性與完整性	7.2.1 安全敏感性資料儲存	-	-	-
	7.2.2 傳輸資料保護	-	-	-
7.3 系統完整性	7.3.1 實體入侵防護	-	-	-
7.4 軟體更新	7.4.1 更新安全	-	-	-
7.5 警示與紀錄	7.5.1 日誌檔與警示	-	-	-
7.6 已知漏洞安全	7.6.1 作業系統與網路服務	-	-	-
	7.6.2 網路服務連接埠	-	-	-
7.7 軟體應用程式	7.7.1 應用程式安全	-	-	-

5. 資安測試規範-照明設備測試

5.1 身分識別、鑑別、權限控管測試

檢視智慧照明系統之身分識別、鑑別、權限控管測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.1.1 鑑別機制測試

5.1.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範—第一部：一般要求」第 5.1.1 節

5.1.1.2 身分鑑別錯誤訊息測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

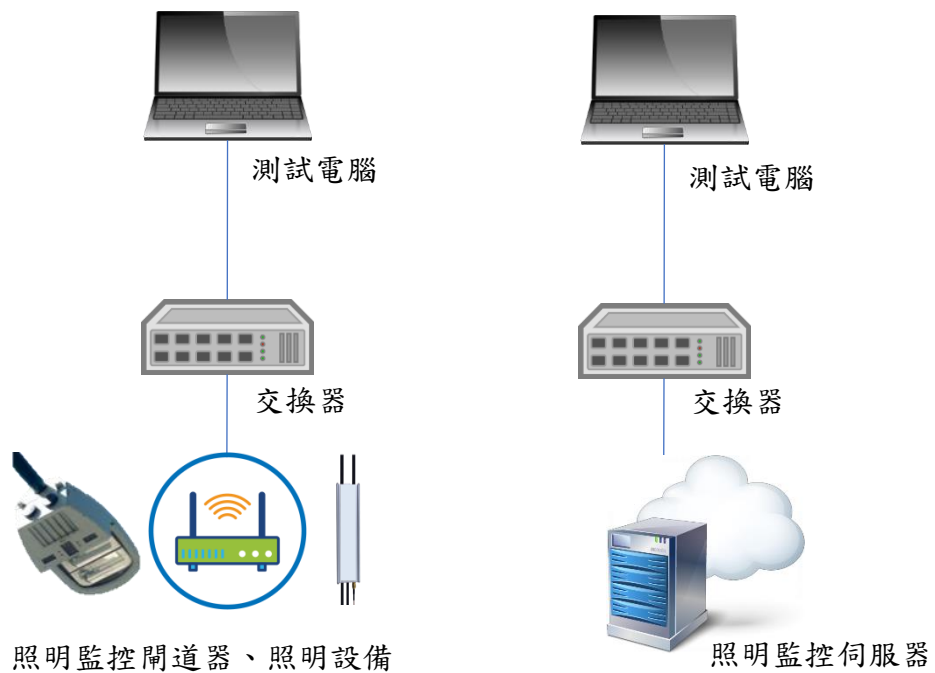
驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品須支援網頁介面。

(6) 測試佈局：

見下圖。



(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，開啟網頁介面。
- (iii) 輸入產品已存在之使用者搭配錯誤的通行碼。
- (iv) 檢視鑑別錯誤訊息。
- (v) 輸入不存在之使用者帳號、通行碼。
- (vi) 檢視鑑別錯誤訊息。

(8) 檢測結果：

- (i) 通過：從鑑別錯誤訊息無法推斷出合法使用者名稱。
- (ii) 不通過：從鑑別錯誤訊息可推斷出合法使用者名稱。
- (iii) 不適用：產品無身分鑑別機制。

(iv) 產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

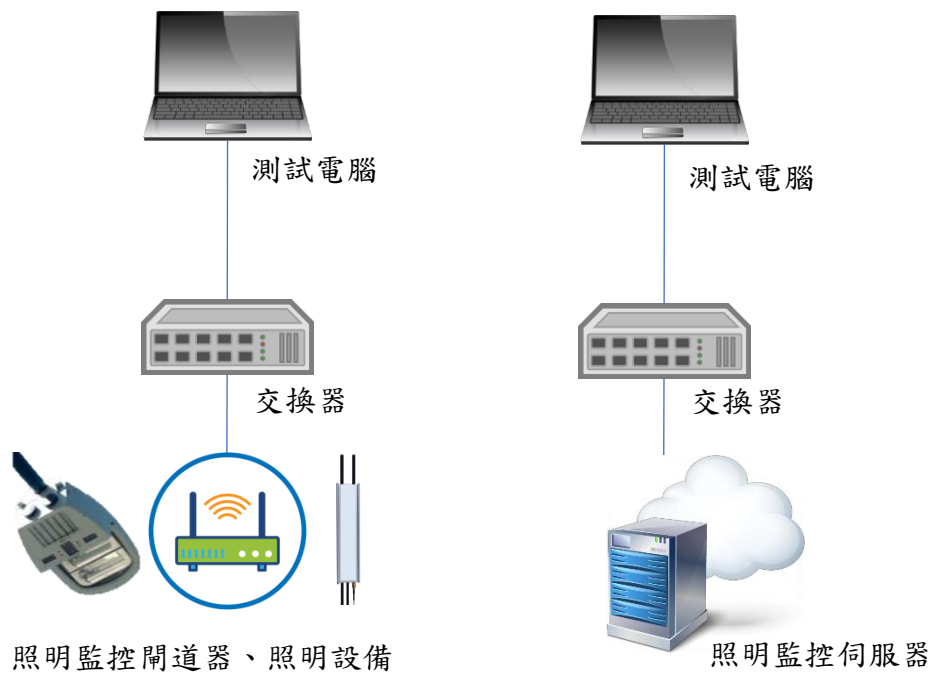
驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品須支援實體介面。

(6) 測試佈局：

見下圖。



(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 若產品支援 UART，將測試電腦連接產品之 UART。
- (iii) 過 UART 埠存取作業系統之除錯模式。
- (iv) 輸入產品之已存在使用者搭配錯誤的通行碼。
- (v) 檢視鑑別錯誤訊息。
- (vi) 輸入不存在之使用者帳號、通行碼。
- (vii) 檢視鑑別錯誤訊息。
- (viii) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (ix) 透過 JTAG 埠存取作業系統之除錯模式。
- (x) 重複(iv)~(vii)之步驟。

(xi) 若產品支援 USB，將測試電腦連接產品之 USB。

(xii) 透過 USB 埠存取作業系統之除錯模式。

(xiii) 重複(iv)~(vii)之步驟。

(8) 檢測結果：

(i) 通過：從鑑別錯誤訊息無法推斷出合法使用者名稱。

(ii) 不通過：從鑑別錯誤訊息可推斷出合法使用者名稱。

(iii) 不適用：產品無身分鑑別機制。

(iv) 不適用：產品無支援實體介面。

(c) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

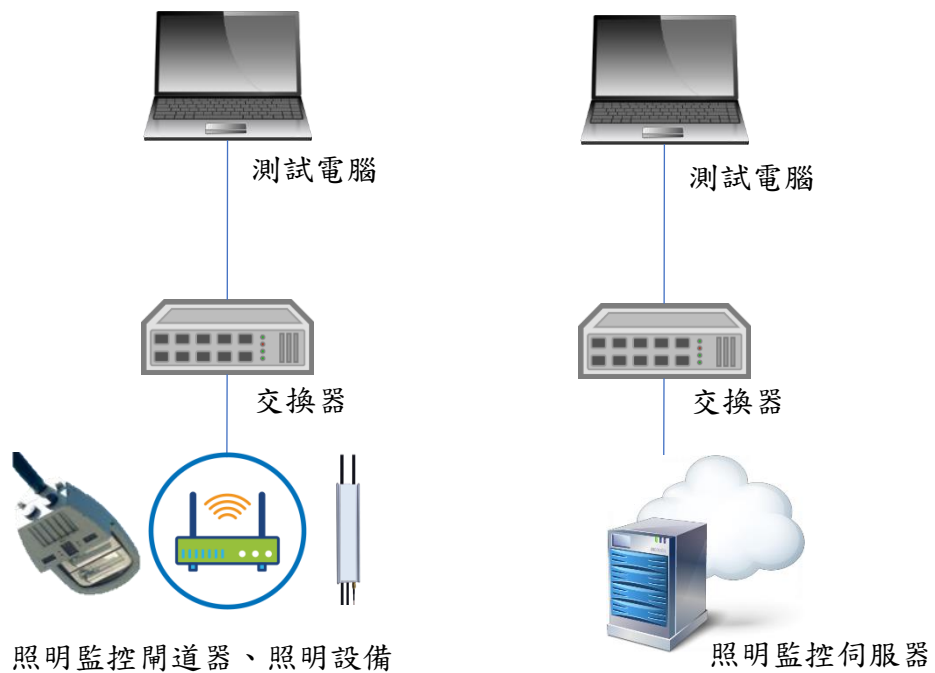


圖 4 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，開啟遠端指令介面。
- (iii) 輸入產品之已存在使用者搭配錯誤的通行碼。
- (iv) 檢視鑑別錯誤訊息。
- (v) 輸入不存在之使用者帳號、通行碼。
- (vi) 檢視鑑別錯誤訊息。

(8) 檢測結果：

- (i) 通過：從鑑別錯誤訊息無法推斷出合法使用者名稱。
- (ii) 不通過：從鑑別錯誤訊息可推斷出合法使用者名稱。
- (iii) 不適用：產品無身分鑑別機制。

(iv) 產品無支援遠端指令介面。

(d) Web API 介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品須支援 Web API。

(6) 測試佈局：

見下圖。

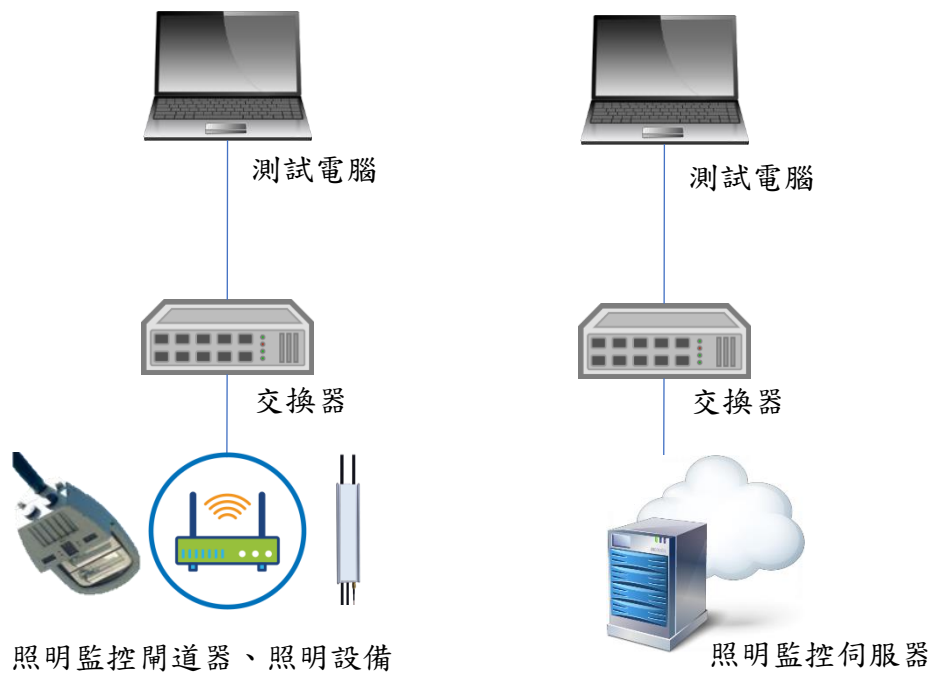


圖 5 測試示意圖

(7) 測試方法：

- (i) 將測試電腦與照明監控伺服器連結在同一個區域網路中。
- (ii) 將產品連結照明監控伺服器。
- (iii) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。
- (iv) 根據產品使用說明，執行具 Web API 功能之操作。
- (v) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至受測產品。
- (vi) 檢視鑑別結果是否成功。
- (vii) 將測試電腦連接產品。
- (viii) 根據產品使用說明，開啟遠端指令介面。
- (ix) 輸入產品之已存在使用者搭配錯誤的通行碼。

(x) 檢視鑑別錯誤訊息。

(xi) 輸入不存在之使用者帳號、通行碼。

(xii) 檢視鑑別錯誤訊息。

(8) 檢測結果：

(i) 通過：從鑑別錯誤訊息無法推斷出合法使用者名稱。

(ii) 不通過：從鑑別錯誤訊息可推斷出合法使用者名稱。

(iii) 不適用：產品無身分鑑別機制。

(iv) 不適用：產品無支援 Web API 或 Web API 無支援通行碼認證。

5.1.1.3 安全敏感性功能安全操作測試

(a) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之安全敏感性功能操作於異常狀態下是否具備身分鑑別機制。

(e) 測試條件：

(1) 產品須聲明所擁有之安全敏感性功能。

(2) 產品須聲明安全敏感性功能的啟動時機與條件。

(3) 產品需聲明異常狀態之內容及條件。

(f) 測試佈局：

無。

(g) 測試方法：

- (1) 依據產品聲明之安全敏感性功能，啟動安全敏感性功能。
- (2) 確認安全敏感性功能能正常運行。
- (3) 關閉安全敏感性功能。
- (4) 依據產品需聲明異常狀態之內容及條件，觸發異常狀態。
- (5) 開啟安全敏感性功能。
- (6) 檢視啟動時是否要求身分鑑別。

(h) 檢測結果：

- (1) 通過：於異常狀態下啟動，產品之安全敏感性功能要求身分鑑別。
- (2) 不通過：於異常狀態下啟動，產品之安全敏感性功能無要求身分鑑別。
- (3) 不適用：無。

5.1.2 權限管控測試

5.1.2.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.1.2 節

5.1.3 通行碼鑑別測試

5.1.3.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.1.3 節

5.1.3.2 通行碼的輸入頻率及次數限制測試

(a) 網頁介面

- (1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」5.1.3.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證通行碼鑑別機制是否有防止暴力破解之能力。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(iii) 產品須提供帳戶鎖定機制之設計說明。

(iv) 產品須支援網頁介面。

(6) 測試佈局：

見下圖。

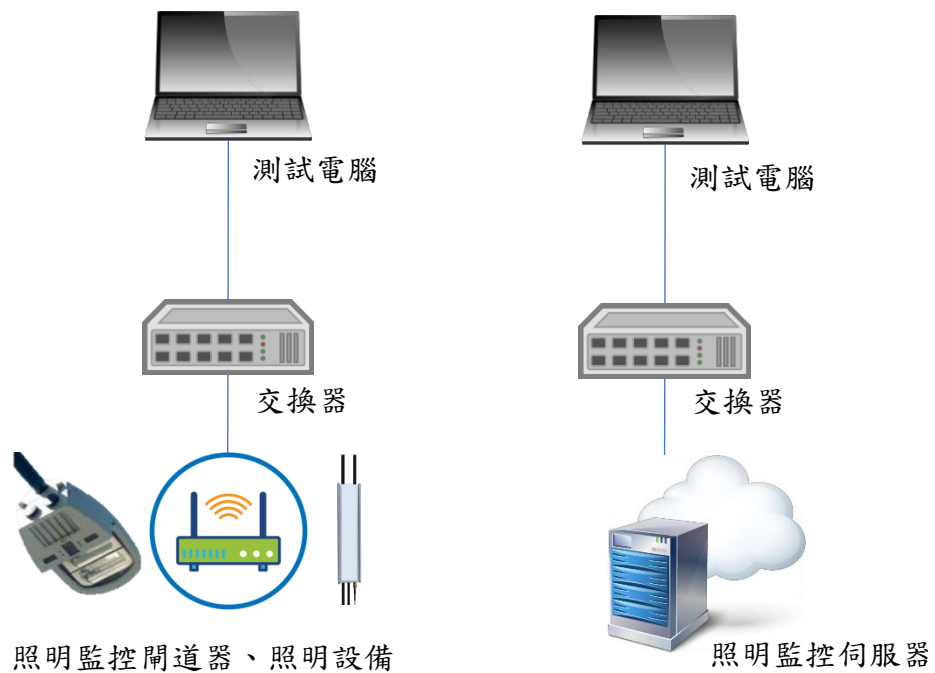


圖 6 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。
- (iii) 不斷輸入錯誤且相異的通行碼。
- (iv) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。
- (v) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。
- (vi) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(8) 檢測結果：

- (i) 輸入次數 5 次以內，會鎖定帳戶。
- (ii) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。
- (iii) 於廠商宣告計數器重設時限內，失敗次數未重新計算。
- (iv) 通過：(i)~(iii)三項結果皆符合。
- (v) 不通過：(i)~(iii)三項項結果不符合其一。
- (vi) 不適用：產品無支援通行碼鑑別機制。
- (vii) 不適用：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.3.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證通行碼鑑別機制是否有防止暴力破解之能力。

(5) 測試條件：

- (i) 產品須支援通行碼鑑別機制。
- (ii) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。
- (iii) 產品須提供帳戶鎖定機制之設計說明。
- (iv) 產品須支援實體介面

(6) 測試佈局：

見下圖。

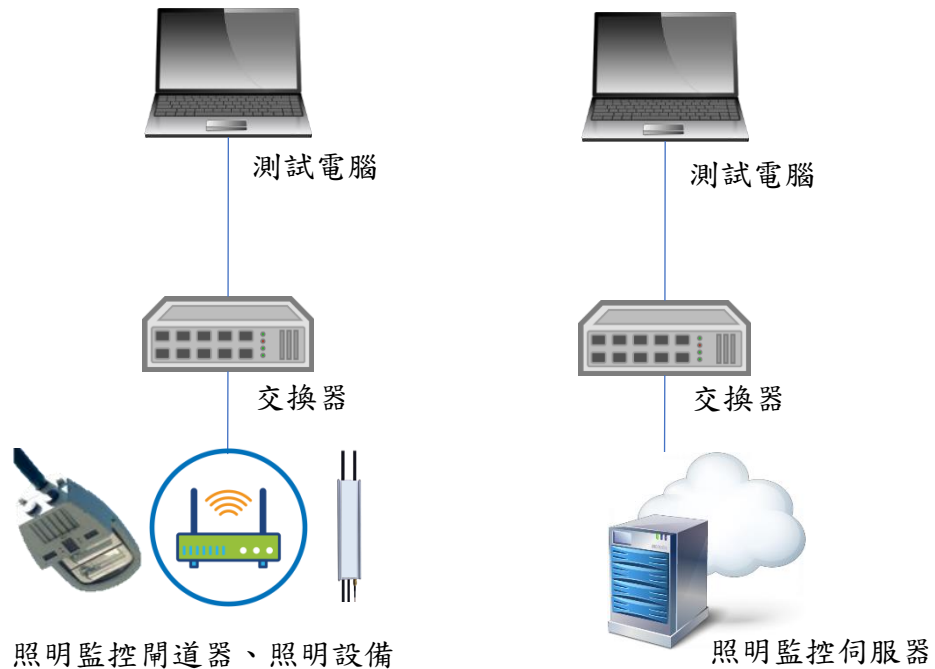


圖 7 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 若產品支援 UART，將測試電腦連接產品之 UART。
- (iii) 透過 UART 埠存取作業系統之除錯模式。
- (iv) 不斷輸入錯誤且相異的通行碼。
- (v) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。
- (vi) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。



(vii) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(viii) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。

(ix) 透過 JTAG 埠存取作業系統之除錯模式。

(x) 重複(iv)~(vii)之步驟。

(xi) 若產品支援 USB，將測試電腦連接產品之 USB。

(xii) 透過 USB 埠存取作業系統之除錯模式。

(xiii) 重複(iv)~(vii)之步驟。

(8) 檢測結果：

(i) 於 UART、USB 及 JTAG 介面輸入次數 5 次以內，會鎖定帳戶。

(ii) UART、USB 及 JTAG 介面於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。

(iii) UART、USB 及 JTAG 介面於廠商宣告計數器重設時限內，失敗次數未重新計算。

(iv) 通過：(i)~(iii)三項結果皆符合。

(v) 不通過：(i)~(iii)三項結果不符合其一。

(vi) 不適用：產品無支援通行碼鑑別機制。

(vii) 不適用：產品無支援實體介面。

(c) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.3.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證通行碼鑑別機制是否有防止暴力破解之能力。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(iii) 產品須提供帳戶鎖定機制之設計說明。

(iv) 產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

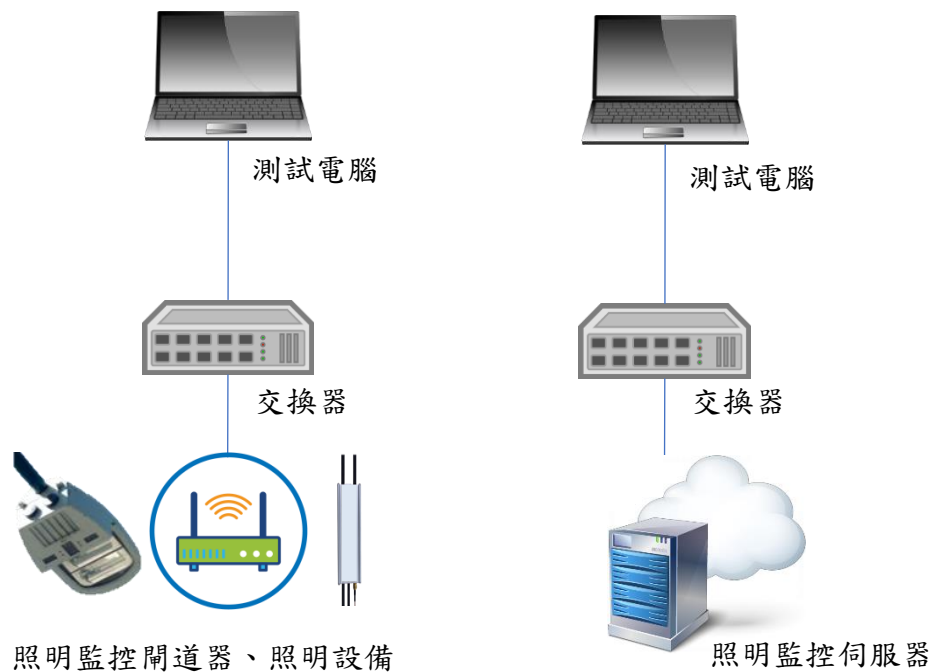


圖 8 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，開啟遠端指令介面以執行身分鑑別。
- (iii) 不斷輸入錯誤且相異的通行碼。
- (iv) 檢視產品於帳戶鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳戶。
- (v) 帳戶鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶鎖定時限內，檢視帳戶是否解除鎖定。
- (vi) 同一帳戶任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(8) 檢測結果：

- (i) 輸入次數 5 次以內，會鎖定帳戶。
- (ii) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。
- (iii) 於廠商宣告計數器重設時限內，失敗次數未重新計算。
- (iv) 通過：(i)~(iii)三項結果皆符合。
- (v) 不通過：(i)~(iii)三項項結果不符合其一。
- (vi) 不適用：產品無支援通行碼鑑別機制。
- (vii) 不適用：產品無支援遠端指令介面。

5.1.3.3 通行碼連續字元之避免測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否存有連續字元，以確保其強度。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品須支援網頁介面。

(6) 測試佈局：

見下圖。

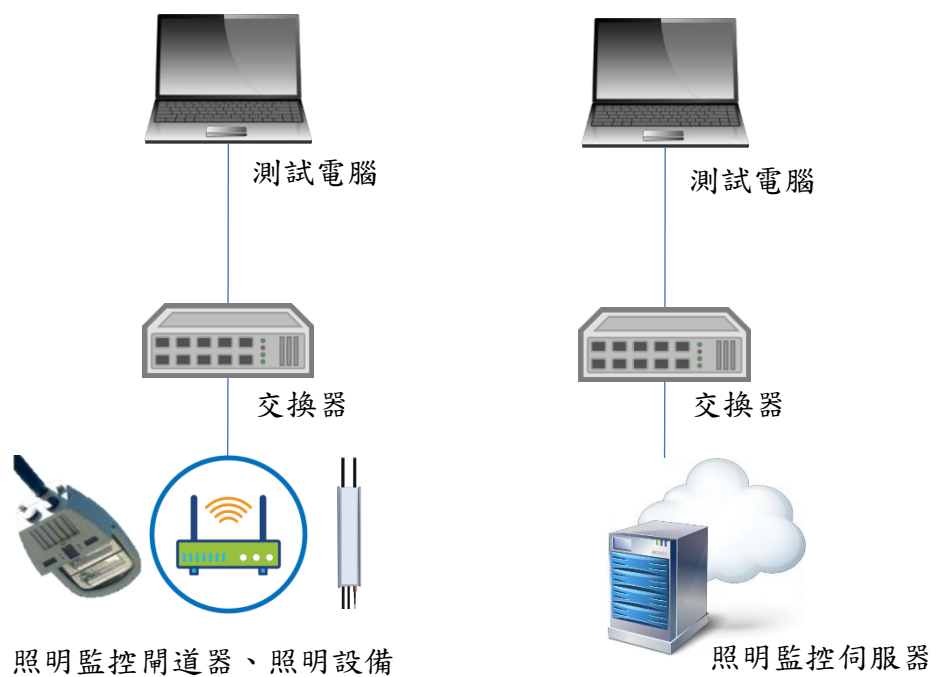


圖 9 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟網頁管理介面。
- (iii) 建立或變更通行碼。
- (iv) 輸入含使用者的帳戶名稱全名中，3 個以上的連續字元。
- (v) 檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過： 無法建立或變更通行碼。
- (ii) 不通過： 成功建立或變更通行碼。
- (iii) 不適用： 產品無支援通行碼鑑別機制。
- (iv) 不適用： 產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否存有連續字元，以確保其強度。

(5) 測試條件：

- (i) 產品須支援通行碼鑑別機制。
- (ii) 產品須支援實體介面。

(6) 測試佈局：

見下圖。

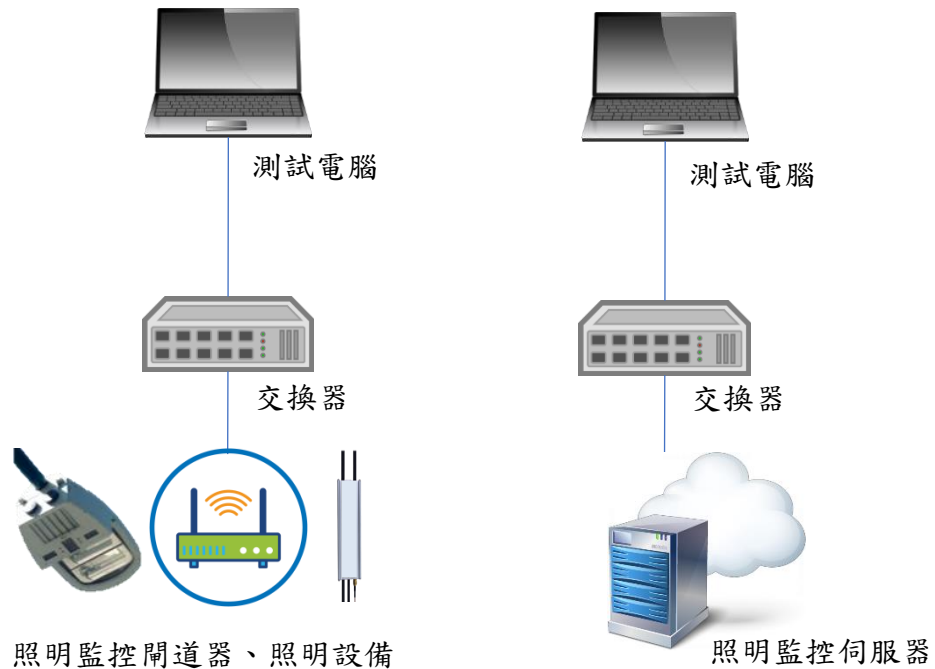


圖 10 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 若產品支援 UART，將測試電腦連接產品之 UART。
- (iii) 透過 UART 埠存取作業系統之除錯模式。
- (iv) 建立或變更通行碼。
- (v) 輸入含使用者的帳戶名稱全名中，3 個以上的連續字元。
- (vi) 檢查通行碼是否能成功建立或變更。
- (vii) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (viii) 透過 JTAG 埠存取作業系統之除錯模式。

(ix) 重複(iv)~(vi)之步驟。

(x) 若產品支援 USB，將測試電腦連接產品之 USB。

(xi) 透過 USB 埠存取作業系統之除錯模式。

(xii) 重複(iv)~(vi)之步驟。

(8) 檢測結果：

(i) 通過：無法於 UART、USB 及 JTAG 介面建立或變更通行碼。

(ii) 不通過：成功於 UART、USB 或 JTAG 介面建立或變更通行碼。

(iii) 不適用：產品無支援通行碼鑑別機制。

(iv) 不適用：產品無支援實體介面。

(c) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否存有連續字元，以確保其強度。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

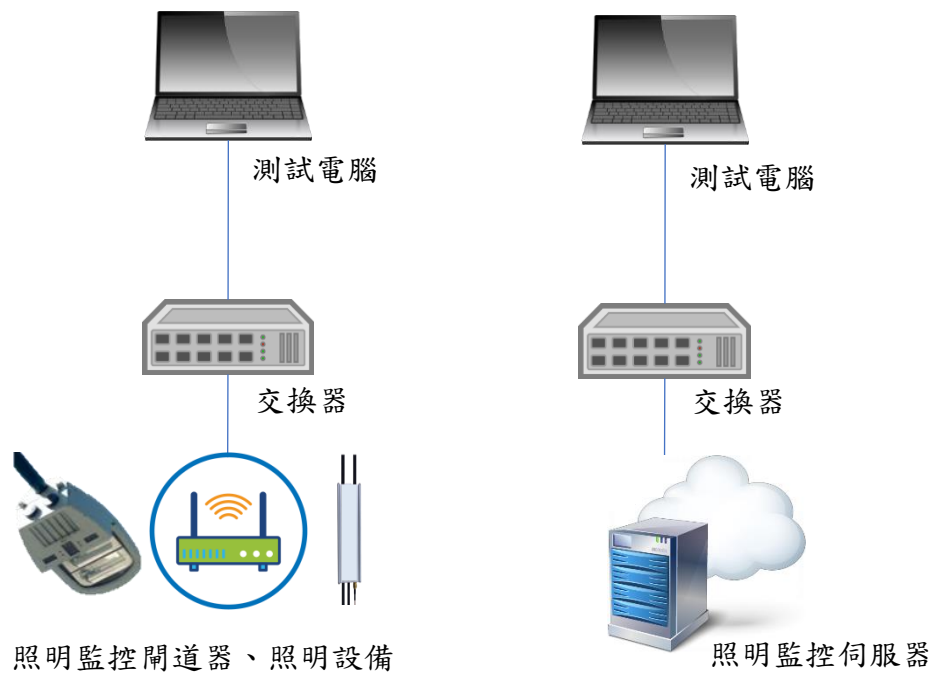


圖 11 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟遠端指令介面。
- (iii) 建立或變更通行碼。
- (iv) 輸入含使用者的帳戶名稱全名中，3 個以上的連續字元。
- (v) 檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過：無法建立或變更通行碼。
- (ii) 不通過：成功建立或變更通行碼。
- (iii) 不適用：產品無支援通行碼鑑別機制。
- (iv) 不適用：產品無支援遠端指令介面。

5.1.3.4 通行碼歷程記錄測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.3.4

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否執行通行碼歷程記錄功能，以確保其強度。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品須支援網頁介面。

(6) 測試佈局：

見下圖。

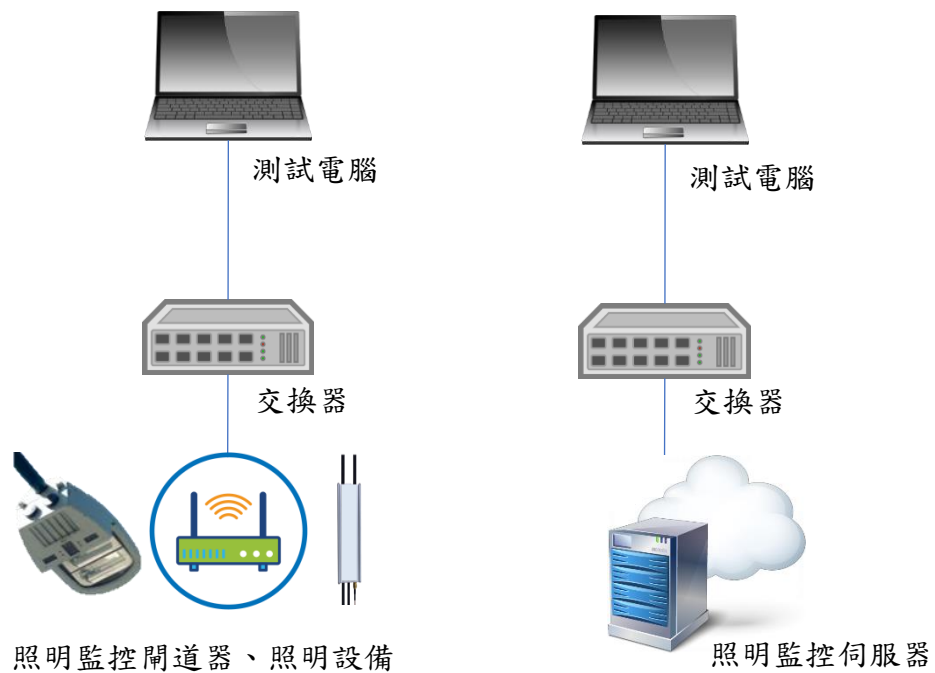


圖 12 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟網頁管理介面。
- (iii) 建立或變更通行碼。
- (iv) 再次變更通行碼，輸入產品曾經使用過之通行碼。
- (v) 檢查通行碼是否能成功變更。

(8) 檢測結果：

- (i) 通過：無法變更通行碼。
- (ii) 不通過：成功建立或變更通行碼。
- (iii) 不適用：產品無支援通行碼鑑別機制。
- (iv) 不適用：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.1.3.4

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否執行通行碼歷程記錄功能，以確保其強度。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品須支援實體介面。

(6) 測試佈局：

見下圖。

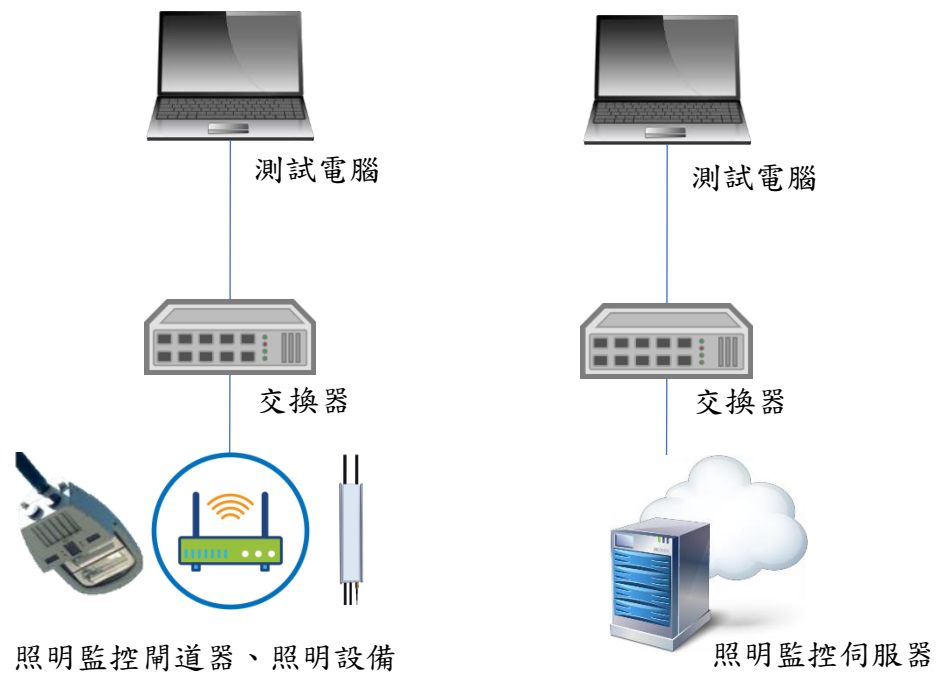


圖 13 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 若產品支援 UART，將測試電腦連接產品之 UART。
- (iii) 透過 UART 埠存取作業系統之除錯模式。
- (iv) 建立或變更通行碼。
- (v) 再次變更通行碼，輸入產品曾經使用過之通行碼。
- (vi) 檢查通行碼是否能成功變更。
- (vii) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (viii) 透過 JTAG 埠存取作業系統之除錯模式。
- (ix) 重複(iv)~(vi)之步驟。
- (x) 若產品支援 USB，將測試電腦連接產品之 USB。

(xi) 透過 USB 埠存取作業系統之除錯模式。

(xii) 重複(iv)~(vi)之步驟。

(8) 檢測結果：

(i) 通過：無法於 UART、USB 及 JTAG 介面變更通行碼。

(ii) 不通過：成功於 UART、USB 及 JTAG 介面建立或變更通行碼。

(iii) 不適用：產品無支援通行碼鑑別機制。

(iv) 不適用：產品無支援實體介面。

(c) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.1.3.4

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳號、通行碼。

(4) 測試目的：

驗證產品的通行碼是否執行通行碼歷程記錄功能，以確保其強度。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制。

(ii) 產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

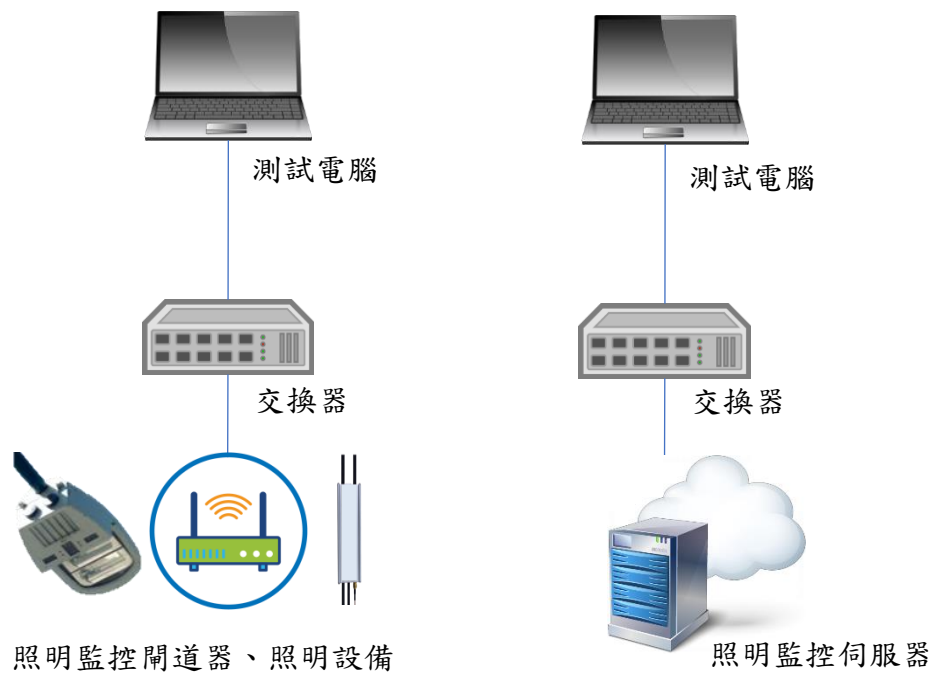


圖 14 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟遠端指令介面。
- (iii) 建立或變更通行碼。
- (iv) 變更通行碼，輸入產品曾經使用過之通行碼。
- (v) 檢查通行碼是否能成功變更。

(8) 檢測結果：

- (i) 通過：無法變更通行碼。
- (ii) 不通過：成功建立或變更通行碼。
- (iii) 不適用：產品無支援通行碼鑑別機制。
- (iv) 不適用：產品無支援遠端指令介面。

5.2 資料機密性與完整性測試

檢視智慧照明系統之資料機密性與完整性測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.2.1 安全敏感性資料儲存測試

5.2.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範—第一部：一般要求」第 5.2.1 節

5.2.1.2 金鑰管理程序測試

(a) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」 5.2.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

產品所提供之金鑰管理程序。

(d) 測試目的：

確認產品的金鑰管理是否建立可靠管控程序。

(e) 測試條件：

產品須提供金鑰管理程序之說明文件。

(f) 測試佈局：

無。

(g) 測試方法：

審閱具備此程序說明之書面資料。

(h) 檢測結果：

- (1) 產品有制定金鑰生成、交換、儲存、使用、銷毀及更替之程序，且該程序須以達到監督、保證和證明金鑰得到妥善管理為目標。
- (2) 金鑰生成所需之亂數產生器採用 FIPS 140-2 Annex C[4]所核可之隨機亂數產生器。
- (3) 通過：(1)~(2)二項結果皆符合。
- (4) 不通過：(1)~(2)二項結果不符合其一。
- (5) 不適用：無。

5.2.1.3 安全敏感性資料隔離保護測試

(a) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.2.1.3

(b) 安全等級：

3 級。

(c) 測試資料：

產品所提供之安全區域設計資料。

(d) 測試目的：

確認產品安全敏感性資料之存放與正常作業系統隔離。

(e) 測試條件：

- (1) 產品須提供安全敏感性資料保存方式之書面資料作為審查依據。
- (2) 產品須聲明哪些資安功能使用到安全區域之書面資料作為審查依據。

(f) 測試佈局：

無。

(g) 測試方法：

審閱具備此功能證明之書面資料。

(h) 檢測結果：

(1) 通過：書面資料證實產品之安全敏感性資料存放於安全區域。

(2) 不通過：書面資料無法證實產品之安全敏感性資料存放於安全區域或無證明資料。

(3) 不適用：產品無存放安全敏感性資料。

5.2.2 傳輸資料保護測試

5.2.2.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.2.2 節

5.3 系統完整性測試

檢視智慧照明系統之系統完整性是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.3.1 實體入侵防護測試

5.3.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.3.1 節

5.3.1.2 韌體萃取安全測試

(a) 測試依據：

TAICS TS-0027-2 「智慧路燈系統資安標準-第二部：智慧照明」5.3.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之韌體是否能被拆解分析。

(e) 測試條件：

(1) 廠商須提供韌體燒錄的介面操作工具及方法。

(2) 韌體若加密，廠商須提供韌體加密之方式。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 依照廠商自我宣告表之燒錄方法及接腳，目視晶片燒錄接腳是否存在。

(2) 若燒錄接腳存在，使用廠商提供之工具，嘗試進行韌體萃取。

(3) 若韌體可萃取，使用具二進制檔案字串搜尋功能之工具，查找是否具有安全敏感性資料。

(4) 若韌體可萃取，使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(5) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(6) 審閱可證明所使用加密演算法之書面資料。

(h) 檢測結果：

(1) 接腳不存在。

(2) 無法成功讀取韌體內資料。

(3) 韌體有用 FIPS 140-2 Annex A [3]所認可加密演算法加密。

(4) 通過：(1)~(3)三項結果符合其一。

(5) 不通過：(1)~(3)三項結果皆不符合。

(6) 不適用：無。

5.3.1.3 測試產品是否支援安全啟動功能

(a) 測試依據：

TAICS TS-0027-2「智慧路燈系統資安標準-第二部：智慧照明」5.3.1.3

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品於開機階段是否能確保產品之完整性及可信度。

(e) 測試條件：

產品須提供安全啟動功能之設計文件。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能證明之書面資料。

(2) 確認產品在開機過程中是否驗證韌體與作業系統的簽章。

(h) 檢測結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 書面資料證實產品在開機過程中驗證韌體與作業系統的簽章。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.4 軟體更新測試

檢視智慧照明系統之軟體更新需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.4.1 更新安全測試

5.4.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.4.1 節

5.5 警示與紀錄測試

檢視智慧照明系統之警示與紀錄安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.5.1 日誌檔與警示測試

5.5.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.5.1 節

5.6 已知漏洞安全測試

檢視智慧照明系統之已知漏洞安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.6.1 作業系統與網路服務測試

5.6.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.6.1 節

5.6.2 網路服務連接埠測試

5.6.2.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.6.2 節

5.7 軟體應用程式測試

檢視智慧照明系統之軟體應用程式安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.7.1 應用程式安全測試

5.7.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 5.7.1 節

6. 資安測試規範-照明監控伺服器測試

6.1 身分識別、鑑別、權限控管要求測試

檢視智慧照明系統之身分識別、鑑別、權限控管測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.1.1 鑑別機制測試

6.1.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.1.1 節

6.2 資料機密性與完整性測試

檢視智慧照明系統之資料機密性與完整性測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.2.1 安全敏感性資料儲存測試

6.2.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.2.1 節

6.3 警示與紀錄測試

檢視智慧照明系統之警示與紀錄安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.3.1 日誌檔與警示測試

6.3.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.3.1 節

6.4 已知漏洞安全測試

檢視智慧照明系統之已知漏洞安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.4.1 作業系統與網路服務測試

6.4.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.4.1 節

6.5 軟體應用程式測試

檢視智慧照明系統之軟體應用程式安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.5.1 網路管理介面安全測試

6.5.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.5.1 節

6.6 資源可用性測試

檢視智慧照明系統之資源可用性安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.6.1 備份測試

6.6.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.6.1 節

6.7 隱私保護測試

檢視智慧照明系統之隱私保護安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.7.1 隱私保護能力安全測試

6.7.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.7.1 節

6.8 雲端平台安全測試

檢視智慧照明系統之雲端平台安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

6.8.1 雲端安全測試

6.8.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 6.8.1 節

7. 資安測試規範-照明監控閘道器安全特殊要求測試

7.1 身分識別、鑑別、權限控管要求測試

檢視智慧照明系統之身分識別、鑑別、權限控管測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.1.1 鑑別機制測試

7.1.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 7.1.1 節

7.2 資料機密性與完整性測試

檢視智慧照明系統之資料機密性與完整性測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.2.1 安全敏感性資料儲存測試

7.2.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 7.2.1 節

7.3 系統完整性測試

檢視智慧照明系統之系統完整性是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.3.1 實體入侵防護測試

7.3.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 7.3.1 節

7.4 軟體更新測試

檢視智慧照明系統之軟體更新需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.4.1 更新安全測試

7.4.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 7.4.1 節

7.5 警示與紀錄測試

檢視智慧路燈系統之警示與紀錄安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.5.1 日誌檔與警示測試

7.5.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範－第一部：一般要求」第 7.5.1 節

7.6 已知漏洞安全測試

檢視智慧路燈系統之已知漏洞安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.6.1 作業系統與網路服務測試

7.6.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範—第一部：一般要求」第 7.6.1 節

7.7 軟體應用程式測試

檢視智慧路燈系統之軟體應用程式安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

7.7.1 應用程式安全測試

7.7.1.1 測試須依循 TAICS TS-0028-1 「智慧路燈系統資安測試規範—第一部：一般要求」第 7.7.1 節

附錄 A (規定) 安全通道建議使用之密碼套件

根據 Mozilla wiki [6]網站建議之密碼套件建議如下：

A.1 安全通道應使用下述幾種密碼套件：

- 0xC0,0x2C-ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH
Au=ECDSA Enc=AESGCM(256) Mac=AEAD
- 0xC0,0x30-ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA
Enc=AESGCM(256) Mac=AEAD
- 0xCC,0x14-ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH
Au=ECDSA Enc=ChaCha20(256) Mac=AEAD
- 0xCC,0x13 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA
Enc=ChaCha20(256) Mac=AEAD
- 0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH
Au=ECDSA Enc=AESGCM(128) Mac=AEAD
- 0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA
Enc=AESGCM(128) Mac=AEAD
- 0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AES(256) Mac=SHA384
- 0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA
Enc=AES(256) Mac=SHA384
- 0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AES(128) Mac=SHA256
- 0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA
Enc=AES(128) Mac=SHA256

參考資料

- (1) TAICS TS-0027-2 智慧路燈系統資安標準-第二部：智慧照明
- (2) TAICS TS-0027-1 智慧路燈系統資安標準-第一部：一般要求
- (3) National Institute of Standards and Technology, FIPS 140-2 Annex A： Approved Security Functions, available at URL： [http：//www.nist.gov/cmvp](http://www.nist.gov/cmvp).
- (4) National Institute of Standards and Technology, FIPS 140-2 Annex C： Approved Random Number Generators, available at URL： [http：//www.nist.gov/cmvp](http://www.nist.gov/cmvp).
- (5) OWASP, OWASP Top 10 – 2017, [https：](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)
[//www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)
- (6) [https：](https://wiki.mozilla.org/Security/Server_Side_TLS) [//wiki.mozilla.org/Security/Server_Side_TLS](https://wiki.mozilla.org/Security/Server_Side_TLS)

版本修改紀錄

版本	時間	摘要
v1.0	2019/12/06	出版



台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地 址 • 台北市中正區重慶南路二段51號8樓之一

電 話 • +886-2-23567698

Email • secretariat@taics.org.tw

www.taics.org.tw