

智慧路燈系統資安測試規範 —第一部：一般要求

**Intelligent Streetlight System Cybersecurity Test Specification
- Part 1: General Requirements**

智慧路燈系統資安測試規範-

第一部：一般要求

Intelligent Streetlight System Cybersecurity Test Specification -Part 1: General Requirements

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)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-物聯網設備安全基本要求測試.....	12
5.1 身分識別、鑑別、權限控管要求測試.....	12
5.2 資料機密性與完整性測試.....	56
5.3 系統完整性測試.....	65
5.4 軟韌體更新測試.....	66
5.5 警示與紀錄測試.....	73
5.6 已知漏洞安全測試.....	83
5.7 軟體應用程式測試.....	89
6. 資安測試規範-後台監控伺服器測試.....	93
6.1 身分識別、鑑別、權限控管要求測試.....	93
6.2 資料機密性與完整性測試.....	147
6.3 警示與紀錄測試.....	160
6.4 已知漏洞安全測試.....	169
6.5 軟體應用程式測試.....	173
6.6 資源可用性測試.....	176
6.7 隱私保護測試.....	180
6.8 雲端平台安全測試.....	186
7. 資安測試規範-燈桿開道器安全特殊要求測試.....	188



7.1 身分識別、鑑別、權限控管要求測試	188
7.2 資料機密性與完整性測試	214
7.3 系統完整性測試	216
7.4 軟韌體更新測試	219
7.5 警示與紀錄測試	219
7.6 已知漏洞安全測試	220
7.7 軟體應用程式測試	220
附錄 A (規定) 安全通道建議使用之密碼套件	221
參考資料	222
版本修改紀錄	223

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系統。而智慧路燈為奠定智慧城市的基石，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；2017 年美國駭客透過網路發動攻擊，控制德州達拉斯 156 座警報器大作。有鑑於社會安全的資安事件頻傳，經濟部工業局自 2017 年起，始推動我國物聯網產業資安規範與制定標準，打造我國安全的聯網產業生態系統。

「TAICS TS-0028-1 智慧路燈系統資安測試規範-第一部：一般要求」(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-0027-1 智慧路燈系統資安標準-第一部：一般要求」[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。俾利智慧路燈系統裝置製造商、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路燈及其附掛具有聯網功能之智慧城市相關應用。智慧路燈是由後台監控伺服器、燈桿閘道器及燈桿附掛設備所組成，如下圖 1 所示。

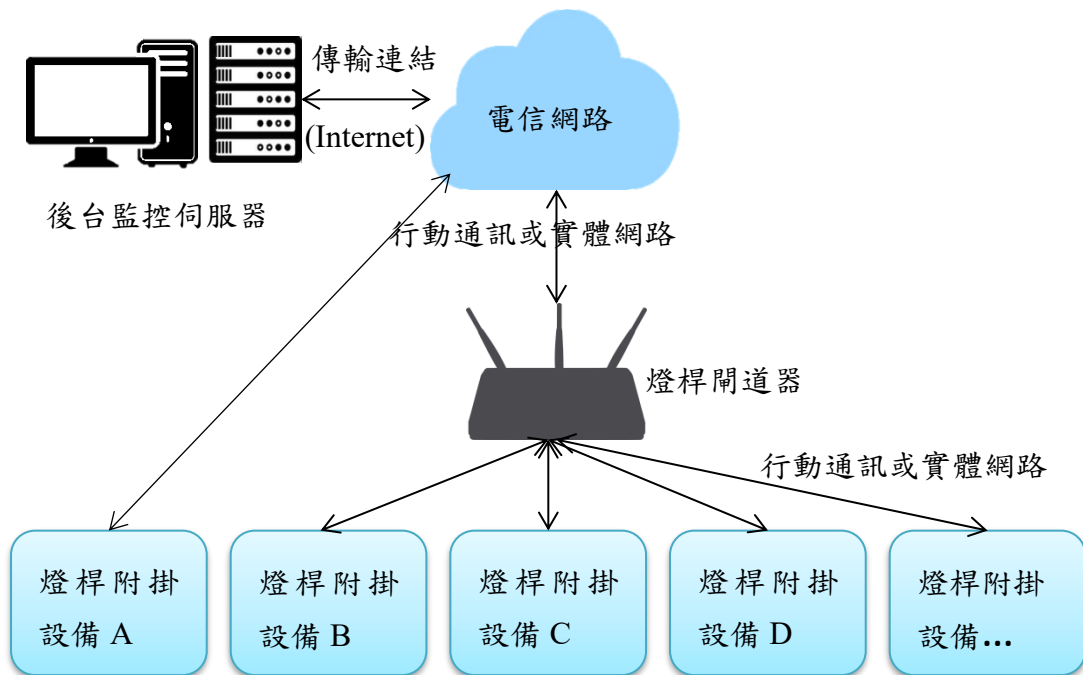


圖 1 適用範圍示意圖

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-0027-1:2019 智慧路燈系統資安標準-第一部：一般要求

3. 用語及定義

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」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-0027-1「智慧路燈系統資安標準-第一部：一般要求」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、(7)軟體應用程式測試，及後台監控伺服器安全要求與燈桿開道器特定資安要求之安全構面(8)資源可用性測試、(9)隱私保護測試及(10)雲端平台安全測試；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. 資安測試規範-物聯網設備安全基本要求測試				
5.1 身分識別、鑑別、權限控管測試	5.1.1 鑑別機制測試	5.1.1.1	-	5.1.1.6
		5.1.1.2		
		5.1.1.3		
		5.1.1.4		
		5.1.1.5		
	5.1.2 權限管控測試	5.1.2.1	-	-
5.1.2.2				
5.1.3 通行碼鑑別測試	5.1.3.1	-	-	
	5.1.3.2			
	5.1.3.3			
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	5.2.1.1(a)	5.2.1.1(b) 5.2.1.2	-
	5.2.2 傳輸資料保護測試	5.2.2.1	5.2.2.2	-
5.3 系統完整性測試	5.3.1 實體入侵防護測試	-	5.3.1.1	-
5.4 軟韌	5.4.1 更新安全測試	5.4.1.1	5.4.1.3	-
		5.4.1.2		

安全構面	安全測試分項	安全等級		
		1 級	2 級	3 級
體更新測試		5.4.1.4		
5.5 警示與紀錄測試	5.5.1 日誌檔與警示測試	5.5.1.1 5.5.1.2 5.5.1.3 5.5.1.4 5.5.1.5	-	-
5.6 已知漏洞安全測試	5.6.1 作業系統與網路服務測試	5.6.1.1	5.6.1.2	-
	5.6.2 網路服務連接埠測試	5.6.2.1	-	-
5.7 軟體應用程式測試	5.7.1 應用程式安全測試	5.7.1.1 5.7.1.2	-	-
6. 資安測試規範-後台監控伺服器測試				
6.1 身分識別、鑑別、權限控管測試	6.1.1 鑑別機制測試	6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.5	-	6.1.1.4 6.1.1.6
	6.1.2 權限控管測試	6.1.2.1 6.1.2.2	-	-
	6.1.3 通行碼鑑別測試	6.1.3.1 6.1.3.4 6.1.3.5 6.1.3.6	-	6.1.3.2 6.1.3.3
6.2 資料機密性與完整性測試	6.2.1 安全敏感性資料儲存測試	6.2.1.3(a)	6.2.1.1 6.2.1.3(b) 6.2.1.4	6.2.1.2
	6.2.2 傳輸資料保護測試	6.2.2.1 6.2.2.2	6.2.2.3	-
6.3 警示與紀錄測試	6.3.1 日誌檔與警示測試	6.3.1.1 6.3.1.2 6.3.1.3 6.3.1.4 6.3.1.5	-	-
6.4 已知漏洞安全測試	6.4.1 作業系統與網路服務測試	6.4.1.1	-	-
	6.4.2 網路服務連接埠測試	6.4.2.1	-	-
6.5 軟體應用程式測試	6.5.1 網路管理介面安全測試	6.5.1.1 6.5.1.2	-	-
6.6 資源可用性測試	6.6.1 備份測試	6.6.1.1 6.6.1.2	-	-

安全構面	安全測試分項	安全等級		
		1 級	2 級	3 級
6.7 隱私保護測試	6.7.1 隱私保護能力安全測試	6.7.1.2 6.7.1.3	6.7.1.1	-
6.8 雲端平台安全測試	6.8.1 雲端安全測試	-	-	6.8.1.1
7. 資安測試規範-燈桿開道器安全特殊要求測試				
7.1 身分識別、鑑別、權限管控測試	7.1.1 鑑別機制測試	7.1.1.1	-	-
	7.1.2 權限管控測試	-	-	-
	7.1.3 通行碼鑑別測試	7.1.3.1	-	7.1.3.2 7.1.3.3
7.2 資料機密性與完整性測試	7.2.1 安全敏感性資料儲存測試		7.2.1.2	7.2.1.3
	7.2.2 傳輸資料保護測試	-	-	-
7.3 系統完整性測試	7.3.1 實體入侵防護測試	-	7.3.1.2	7.3.1.3
7.4 軟體更新測試	7.4.1 更新安全測試	-	-	-
7.5 警示與紀錄測試	7.5.1 日誌檔與警示測試	-	-	-
7.6 已知漏洞安全測試	7.6.1 作業系統與網路服務測試	-	-	-
	7.6.2 網路服務連接埠測試	-	-	-
7.7 軟體應用程式測試	7.7.1 應用程式安全測試	-	-	-

5. 資安測試規範-物聯網設備安全基本要求測試

5.1 身分識別、鑑別、權限控管要求測試

檢視智慧路燈系統之身分識別、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 遠端指令介面安全

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之遠端指令介面是否關閉，或者具備身分鑑別機制。

(e) 測試條件：

產品須聲明其遠端指令介面連結方式。

(f) 測試佈局：

見下圖。



圖 2 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具網路埠掃描功能之工具。
- (3) 對產品執行 TCP 埠 0~65535 之掃描。
- (4) 檢視掃描結果所呈現之網路服務與對應埠。
- (5) 對產品執行 UDP 埠 0~65535 之掃描。
- (6) 檢視掃描結果所呈現之網路服務是否存在 SSH 或 telnet。
- (7) 根據產品聲明之遠端指令介面連結方式，開啟遠端指令介面。

(h) 檢測結果：

- (1) 產品不存在 SSH 或 telnet 網路服務。
- (2) 開啟遠端指令介面前，產品要求身分鑑別。

- (3) 通過: (1)~(2)二項結果符合其一。
- (4) 不通過: (1)~(2)二項結果皆不符合。
- (5) 不適用: 無。

5.1.1.2 鑑別機制強度測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

產品須支援網頁介面。

(6) 測試佈局：

見下圖。



圖 3 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 於未登入的狀況下，存取身分鑑別頁面外之頁面，確認是否要求身分鑑別。
- (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，開啟網頁介面。
- (v) 以產品之系統管理員帳密登入，執行身分鑑別操作。
- (vi) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。
- (vii) 檢視鑑別結果是否成功。

(8) 檢測結果：

- (i) 產品於網頁介面能正常執行身分鑑別機制。
- (ii) 身分鑑別機制具備抵抗重送攻擊的能力。
- (iii) 通過: (i)~(ii)二項結果皆符合。
- (iv) 不通過: (i)~(ii)二項結果不符合其一。
- (v) 不適用: 產品無支援網頁介面。

(b) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(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) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。
- (iii) 根據產品使用說明，開啟遠端指令介面。
- (iv) 以產品之系統管理員帳密登入，執行身分鑑別操作。
- (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。

(8) 檢測結果：

- (i) 產品於遠端指令介面能正常執行身分鑑別機制。
- (ii) 身分鑑別機制具備抵抗重送攻擊的能力。
- (iii) 通過: (i)~(ii)二項結果皆符合。
- (iv) 不通過: (i)~(ii)二項結果不符合其一。
- (v) 不適用: 產品無支援遠端指令介面。

(c) 射頻介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

無。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

- (i) 產品須支援射頻介面。
- (ii) 產品須提供使用說明並宣告其安全敏感性功能。
- (iii) 後台監控伺服器不適用。

(6) 測試佈局：

見下圖。



圖 5 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，執行安全敏感性功能或身份鑑別。
- (iii) 使用軟體定義無線電(SDR)，側錄無線電波訊號。
- (iv) 使用 SDR 重新播放側錄之無線電波訊號。
- (v) 確認產品是否有進行相同行為。

(8) 檢測結果：

- (i) 通過: 經 SDR 重新播放後，產品無進行相同行為。
- (ii) 不通過: 經 SDR 重新播放後，產品有進行相同行為。
- (iii) 不適用: 後台監控伺服器。

(d) Web API 介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

產品須支援 Web API 介面。

(6) 測試佈局：

見下圖。

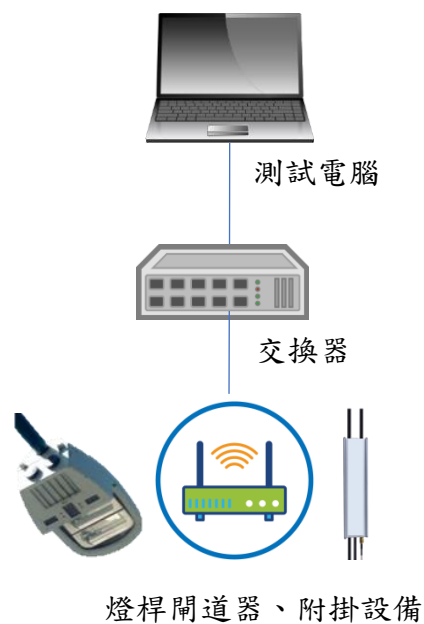


圖 6 測試示意圖

(7) 測試方法：

- (i) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (ii) 將產品連結後台監控伺服器。
- (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，執行身分鑑別操作。
- (v) 執行具 Web API 功能之操作。
- (vi) 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。
- (vii) 檢視鑑別結果是否成功。

(8) 檢測結果：

- (i) 產品於 Web API 介面能正常執行身分鑑別機制。
- (ii) 身分鑑別機制具備抵抗重送攻擊的能力。
- (iii) 通過: (i)~(ii)二項結果皆符合。
- (iv) 不通過: (i)~(ii)二項結果不符合其一。
- (v) 不適用: 產品無支援網頁介面。

5.1.1.3 金鑰唯一性測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證產品之金鑰是否唯一。

(e) 測試條件：

- (1) 產品須存在金鑰。
- (2) 根金鑰(Root Key)不在此測試範圍。

(f) 測試佈局：

見下圖。



圖 7 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 輸入產品之系統管理者帳密以執行身分鑑別。
- (4) 側錄封包並擷取產品之憑證，檢視其指紋碼(fingerprint)。

(5) 重置產品至出廠預設狀態。

(6) 重覆步驟(2)~(4)。

(h) 檢測結果：

(1) 若測試設備透過圖形化管理介面連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(2) 若測試設備透過安全外殼協定(SSH)連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(3) 若測試是產品與其它後台監控伺服器互連，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(4) 通過: (1)~(3)三項結果皆符合。

(5) 不通過: (1)~(3)三項結果不符合其一。

(6) 不適用: 產品不存在金鑰。

5.1.1.4 產品識別碼唯一性測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

(1) 驗證產品之識別碼是否唯一。

(e) 測試條件：

(1) 產品須提供可與其相連之智慧路燈裝置。

(2) 產品須提供識別碼機制之設計說明文件。

(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) 通過：產品唯一識別碼採用通用唯一識別碼同等或以上重覆概率的編碼方式。

(2) 不通過：產品唯一識別碼其編碼的重覆概率小於通用唯一識別碼。

(3) 不適用：無。

5.1.1.5 受信任根憑證測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

產品是否具備驗證相連裝置所發送之憑證是否為受信任之根憑證所發行的能力。

(e) 測試條件：

產品須列出使用到憑證的功能。

(f) 測試佈局：

見下圖。



圖 8 測試示意圖

(g) 測試方法：

- (1) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (2) 將產品與其對連之終端裝置，如：後台監控伺服器或燈桿附掛設備。
- (3) 設定中間人攔截熱點，於身分鑑別階段，開啟封包側錄工具進行側錄。
- (4) 當其對連終端裝置發送憑證予產品之間時攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
- (5) 發送已竄改之憑證予產品，檢視產品是否接受此憑證。

(h) 檢測結果：

- (1) 通過：產品不接受此憑證。
- (2) 不通過：產品接受此憑證。
- (3) 不適用：無。

5.1.1.6 終端設備身分證明測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.1.6

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證照明監控系統是否具有遠端證明燈桿閘道器與照明設備身分的能力。

(e) 測試條件：

(1) 產品須提供遠端證明之設計文件。

(2) 產品須提供對接的後台監控伺服器、燈桿閘道器及照明設備。

(f) 測試佈局：

見下圖。



圖 9 測試示意圖

(g) 測試方法：

- (1) 審閱具備遠端證明功能之設計文件。
- (2) 將燈桿開道器與後台監控伺服器建立連線。
- (3) 使用測試電腦側錄之間的封包。
- (4) 檢視燈桿開道器證明身分之機制是否符合遠端證明設計。
- (5) 將照明設備與後台監控伺服器建立連線。
- (6) 重複步驟(3)~(4)。

(h) 檢測結果：

- (1) 通過：產品支援遠端證明之功能。
- (2) 不通過：產品不支援遠端證明之功能。
- (3) 不適用：無。

5.1.2 權限管控測試

5.1.2.1 權限管控機制

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.2.1

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(5) 測試條件：

(i) 產品須具備創建多個不同權限使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

(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) 開啟網頁介面。
- (iii) 以一般使用者帳密登入。
- (iv) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (v) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 進行登出，並以系統管理者帳密登入。
- (vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(viii)嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(8) 檢測結果：

(i) 通過：於網頁介面的身分授權與產品自我宣告相符。

(ii) 不通過：於網頁介面的身分授權與產品自我宣告不相符，或產品無支援創建多個不同權限使用者之功能。

(iii) 不適用：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.2.1

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(5) 測試條件：

(i) 產品須具備創建多個不同權限使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

(iii) 產品須支援實體介面。

(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) 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) 以一般使用者帳密登入。
- (v) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 以系統管理者帳密登入。
- (vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (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)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)步驟。

(8) 檢測結果：

(i) 通過: 於 UART、USB 及 JTAG 介面的身分授權與產品自我宣告相符。

(ii) 不通過: 於 UART、USB 或 JTAG 介面的身分授權與產品自我宣告不相符，或產品無支援創建多個不同權限使用者之功能。

(iii) 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.2.1

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(5) 測試條件：

(i) 產品須具備創建多個不同權限之使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

(iii) 產品須支援遠端指令介面。

(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) 開啟遠端指令介面。
- (iii) 以一般使用者帳密登入。
- (iv) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (v) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 以一般系統管理者帳密登入。

(vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(viii) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(8) 檢測結果：

(i) 通過：於遠端指令介面的身分授權與產品自我宣告相符。

(ii) 不通過：於遠端指令介面的身分授權與產品自我宣告相符，或產品無支援創建多個不同權限之使用者之功能。

(iii) 不適用：產品無支援遠端指令介面。

5.1.2.2 權限有效時間

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證產品是否存在有限的授權時間長度。

(e) 測試條件：

產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(f) 測試佈局：

見下圖。



圖 13 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 透過網頁管理介面登入產品。
- (3) 檢視產品之網頁管理介面，閒置時限是否存在供使用者設定的操作介面。
- (4) 閒置產品直到超過閒置時限值。
- (5) 檢視是否需要重新鑑別方可存取產品。

(h) 檢測結果：

- (1) 產品之授權行為，存在閒置時限供使用者設定。
- (2) 遠端連線閒置逾時，須經過身分鑑別方可存取產品。
- (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。

5.1.3 通行碼鑑別測試

5.1.3.1 預設通行碼測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品提供之網頁介面預設通行碼。

(4) 測試目的：

(i) 狀況 1：

驗證產品是否有相同的預設通行碼。

(ii) 狀況 2：

驗證產品預設通行碼是否會於首次上線後，具強制要求更改預設通行碼之功能。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制，且須提供預設通行碼。

(ii) 產品須保持出廠具強制要求更改預設通行碼之功能。

(iii) 後台監控伺服器不適用。

(iv) 產品須支援網頁介面。

(6) 測試佈局：

見下圖。



圖 14 測試示意圖

(7) 測試方法：

(i) 狀況 1:

1. 準備 2 台以上產品。
2. 將測試電腦連接第一個產品。
3. 開啟網頁管理介面。
4. 於登入頁面輸入產品提供之預設通行碼。
5. 將測試電腦連接第二個產品。
6. 重複 3~4 之步驟。

(ii) 狀況 2:

1. 將測試電腦連接產品。
2. 開啟網頁介面。
3. 確認產品是否會於首次上線後，強制要求更改通行碼之功能。
4. 取消輸入通行碼。

(8) 檢測結果：

(i) 狀況 1:

1. 通過: 任 2 台產品的預設通行碼相異。
2. 不通過: 任 2 台產品的預設通行碼相同。
3. 不適用: 產品不支援通行碼鑑別機制。

(ii) 狀況 2:

1. 通過: 未經設定新通行碼前無法存取產品。
2. 不通過: 未經設定新通行碼前仍可存取產品。
3. 不適用: 產品不支援通行碼鑑別機制。

(iii) 通過: (i)~(ii)二項狀況符合其一。

(iv) 不通過: (i)~(ii)二項狀況皆不符合。

(v) 不適用: 後台監控伺服器。

(vi) 不適用: 產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品提供之實體介面預設通行碼。

(4) 測試目的：

(i) 狀況 1：

驗證產品是否有相同的預設通行碼。

(ii) 狀況 2：

驗證產品預設通行碼是否會於首次上線後，具強制要求更改預設通行碼之功能。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制，且須提供預設通行碼。

(ii) 產品須保持出廠具強制要求更改預設通行碼之功能。

(iii) 後台監控伺服器不適用。

(iv) 產品須支援實體介面。

(6) 測試佈局：

見下圖。



圖 15 測試示意圖

(7) 測試方法：

(i) 狀況 1:

1. 準備 2 台以上產品。
2. 若產品支援 UART，將測試電腦連接第一個產品之 UART。
3. 透過 UART 埠存取作業系統之除錯模式。
4. 輸入產品提供之預設通行碼。
5. 將測試電腦連接第二個產品之 UART。
6. 重複 3~4 之步驟。
7. 若產品支援 JTAG，將測試電腦連接第一個產品之 JTAG。
8. 透過 JTAG 埠存取作業系統之除錯模式。
9. 輸入產品提供之預設通行碼。
10. 將測試電腦連接第二個產品之 JTAG。



11. 重複 8~9 之步驟。
12. 若產品支援 USB，將測試電腦連接第一個產品之 USB。
13. 透過 USB 埠存取作業系統之除錯模式。
14. 輸入產品提供之預設通行碼。
15. 將測試電腦連接第二個產品之 USB。
16. 重複 13~14 之步驟。

(ii) 狀況 2:

1. 若產品支援 UART，將測試電腦連接第一個產品之 UART。
2. 透過 UART 埠存取作業系統之除錯模式。
3. 確認產品是否會於首次上線後，強制要求更改通行碼。
4. 取消輸入通行碼。
5. 將測試電腦連接第二個產品之 UART。
6. 重複 2~4 之步驟。
7. 若產品支援 JTAG，將測試電腦連接第一個產品之 JTAG。
8. 透過 JTAG 埠存取作業系統之除錯模式。
9. 確認產品是否會於首次上線後，強制要求更改通行碼。
10. 取消輸入通行碼。
11. 將測試電腦連接第二個產品之 JTAG。
12. 重複 8~10 之步驟。
13. 若產品支援 USB，將測試電腦連接第一個產品之 USB。
14. 透過 USB 埠存取作業系統之除錯模式。
15. 確認產品是否會於首次上線後，強制要求更改通行碼。
16. 取消輸入通行碼。

17. 將測試電腦連接第二個產品之 USB。

18. 重複 14~16 之步驟。

(8) 檢測結果：

(i) 狀況 1:

1. 通過: 任 2 台產品的 UART、USB 及 JTAG 預設通行碼相異。
2. 不通過: 任 2 台產品的 UART、USB 及 JTAG 預設通行碼相同。
3. 不適用: 產品不支援通行碼鑑別機制。

(ii) 狀況 2:

1. 通過: 未經設定新通行碼前無法存取產品。
2. 不通過: 未經設定新通行碼前仍可存取產品。
3. 不適用: 產品不支援通行碼鑑別機制。

(iii) 通過: (i)~(ii)二項狀況符合其一。

(iv) 不通過: (i)~(ii)二項項狀況皆不符合。

(v) 不適用: 後台監控伺服器。

(vi) 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-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品提供之遠端指令介面預設通行碼。

(4) 測試目的：

(i) 狀況 1：

驗證產品是否有相同的預設通行碼。

(ii) 狀況 2：

驗證產品預設通行碼是否會於首次上線後，具強制要求更改預設通行碼之功能。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制，且須提供預設通行碼。

(ii) 產品須保持出廠具強制要求更改預設通行碼之功能。

(iii) 後台監控伺服器不適用。

(iv) 產品須支援網遠端指令介面。

(6) 測試佈局：

見下圖。

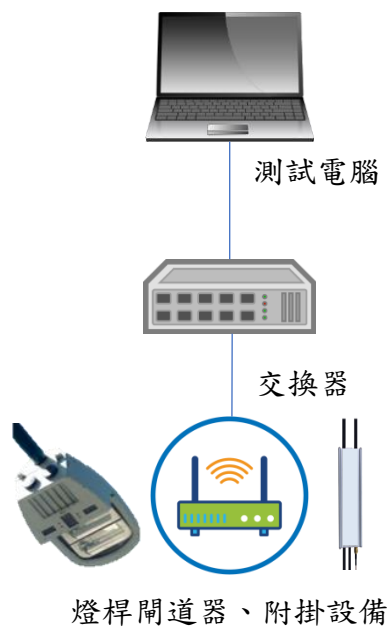


圖 16 測試示意圖

(7) 測試方法：

(i) 狀況 1:

1. 準備 2 台以上產品。
2. 將測試電腦連接第一個產品。
3. 開啟遠端指令介面。
4. 於登入介面輸入產品提供之預設通行碼。
5. 將測試電腦連接第二個產品。
6. 重複 3~4 之步驟。

(ii) 狀況 2:

1. 將測試電腦連接產品。
2. 開啟遠端指令介面。
3. 確認產品是否會於首次上線後，強制要求更改通行碼之功能。
4. 取消輸入通行碼。

(8) 檢測結果：

(i) 狀況 1:

1. 通過: 任 2 台產品的預設通行碼相異。
2. 不通過: 任 2 台產品的預設通行碼相同。
3. 不適用: 產品不支援通行碼鑑別機制。

(ii) 狀況 2:

1. 通過: 未經設定新通行碼前無法存取產品。
2. 不通過: 未經設定新通行碼前仍可存取產品。
3. 不適用: 產品不支援通行碼鑑別機制。

(iii) 通過: (i)~(ii)二項狀況符合其一。

(iv) 不通過: (i)~(ii)二項項狀況皆不符合。

(v) 不適用: 後台監控伺服器。

(vi) 不適用: 產品無支援遠端指令介面。

5.1.3.2 通行碼長度

(a) 網頁介面:

(1) 測試依據:

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部: 一般要求」 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密。

(4) 測試目的:

驗證產品的通行碼長度是否足夠, 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 17 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，建立或變更通行碼。
- (iii) 輸入小於 8 個字元長度之通行碼。
- (iv) 檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過：無法建立或變更小於 8 個字元長度之通行碼。
- (ii) 不通過：可建立或變更小於 8 個字元長度之通行碼。
- (iii) 不適用：產品須無支援通行碼鑑別機制。
- (iv) 不適用：產品須無支援網頁介面。

(b) 實體介面：

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 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密。

(4) 測試目的：

驗證產品的通行碼長度是否足夠，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。

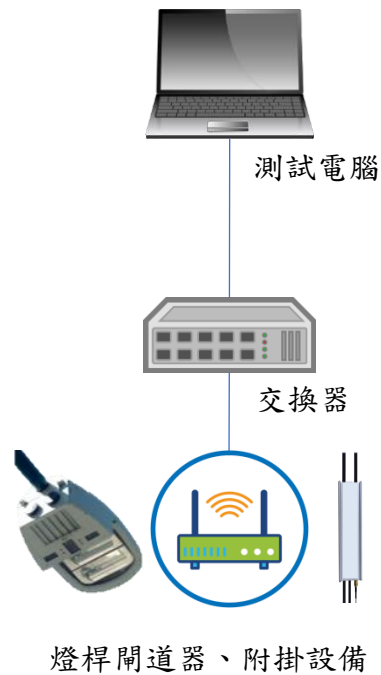


圖 18 測試示意圖

(7) 測試方法：

- (i) 若產品支援 UART，將測試電腦連接產品之 UART。
- (ii) 透過 UART 埠存取作業系統之除錯模式。
- (iii) 建立或變更通行碼。
- (iv) 輸入小於 8 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。
- (v) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (vi) 透過 JTAG 埠存取作業系統之除錯模式。
- (vii) 重複(iii)~(iv)之步驟。
- (viii) 若產品支援 USB，將測試電腦連接第一個產品之 USB。
- (ix) 透過 USB 埠存取作業系統之除錯模式。
- (x) 重複(iii)~(iv)之步驟。

(8) 檢測結果：

- (i) 通過：無法於 UART、USB 及 JTAG 介面建立或變更小於 8 個字元長度之通行碼。
- (ii) 不通過：可於 UART、USB 或 JTAG 介面建立或變更小於 8 個字元長度之通行碼。
- (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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 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密。

(4) 測試目的：

驗證產品的通行碼長度是否足夠，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 19 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) 輸入小於 8 個字元長度之通行碼。
- (v) 檢查通行碼是否能成功建立或變更。
- (8) 檢測結果：
 - (i) 通過：無法建立或變更小於 8 個字元長度之通行碼。
 - (ii) 不通過：可建立或變更小於 8 個字元長度之通行碼。
 - (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。

5.1.3.3 通行碼複雜度

(a) 網頁介面

- (1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.3.3
- (2) 安全等級：

1 級。
- (3) 測試資料：

產品之系統管理者帳密。
- (4) 測試目的：

驗證產品的通行碼複雜度是否足夠，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 20 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 從網頁管理介面，建立或變更通行碼。
- (iii) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過：無法於網頁介面建立或變更通行碼。
- (ii) 不通過：成功於網頁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：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.3.3

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(4) 測試目的：

驗證產品的通行碼複雜度是否足夠，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 21 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) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，檢查通行碼是否能成功建立或變更。
- (vi) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (vii) 透過 JTAG 埠存取作業系統之除錯模式。
- (viii) 重複(iv)~(v)之步驟。
- (ix) 若產品支援 USB，將測試電腦連接產品之 USB。

- (x) 透過 USB 埠存取作業系統之除錯模式。
- (xi) 重複(iv)~(v)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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.1.3.3
 - (2) 安全等級：

1 級。
 - (3) 測試資料：

產品之系統管理者帳密。
 - (4) 測試目的：

驗證產品的通行碼複雜度是否足夠，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 22 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) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，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。

5.2 資料機密性與完整性測試

檢視智慧路燈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 安全敏感性資料權限管控測試

(a) 初階測試：

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.2.1.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品所提供之安全敏感性資料保存方式。

(4) 測試目的：

產品安全敏感性資料的存取是否具有權限控管機制。

(5) 測試條件：

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。

(6) 測試佈局：

無。

(7) 測試方法：

審閱能證明符合此安全要求之書面資料。

(8) 檢測結果：

(i) 產品通行碼資料之權限管控與產品自我宣告相符。

- (ii) 產品之加解密金鑰的權限管控與產品自我宣告相符。
- (iii) 該權限管控機制至少擁有二個以上不同權限的角色。
- (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: 產品無存放安全敏感性資料。

(b) 中階測試：

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.2.1.1

(2) 安全等級：

2 級。

(3) 測試資料：

- (i) 產品之一般使用者帳密。
- (ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品安全敏感性資料的存取是否具有權限控管機制。

(5) 測試條件：

- (i) 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。
- (ii) 產品須提供系統管理者權限供測試用。
- (iii) 產品須提供能進入作業系統層之介面。

(6) 測試佈局：

見下圖。



圖 23 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 以產品之一般使用者身分登入。
- (iii) 確認通行碼資料存取權限。
- (iv) 確認加解密金鑰存取權限。
- (v) 登出後以產品之系統管理者身分登入。
- (vi) 確認通行碼資料存取權限。
- (vii) 確認加解密金鑰存取權限。

(8) 檢測結果：

- (i) 產品通行碼資料之權限管控與產品自我宣告相符。
- (ii) 產品之加解密金鑰之權限管控與產品自我宣告相符。

(iii) 該權限管控機制至少擁有二個以上不同權限的角色。

(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: 產品無存放安全敏感性資料。

5.2.1.2 安全敏感性資料加密儲存測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.2.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之安全敏感性資料於儲存狀態下是否加密保護。

(e) 測試條件：

(1) 產品須提供安全敏感性資料儲存保護之演算法書面資料作為審查依據。

(2) 產品須提供系統管理者權限供測試用。

(3) 產品須提供能進入作業系統層之介面。

(4) 根金鑰(Root Key)不在此測試範圍。

(f) 測試佈局：

見下圖。



圖 24 測試示意圖

(g) 測試方法：

- (1) 審閱能證明符合此安全要求之書面資料。
- (2) 將測試電腦連接產品。
- (3) 若產品支援 UART，將測試電腦連接產品之 UART。
- (4) 透過 UART 埠存取作業系統之除錯模式。
- (5) 透過搜尋工具，查找安全敏感性資料位置。
- (6) 檢視保護通行碼資料所採用的雜湊演算法。
- (7) 檢視保護加解密金鑰所採用的保密機制。
- (8) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (9) 過 JTAG 埠存取作業系統之除錯模式。
- (10) 重複(5)~(7)之步驟。

- (11) 若產品支援 USB，將測試電腦連接產品之 USB。
- (12) 過 USB 埠存取作業系統之除錯模式。
- (13) 重複(5)~(7)之步驟。
- (14) 若產品支援遠端指令介面，開啟並連接遠端指令介面。
- (15) 重複(5)~(7)之步驟。
- (h) 檢測結果：
 - (1) 通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之雜湊函數。
 - (2) 加解密用金鑰的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。
 - (3) 通過: (1)~(2)二項結果符合其一。
 - (4) 不通過: (1)~(2)二項結果皆不符合。
 - (5) 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 身分鑑別因子傳輸安全測試

- (a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.2.2.1
- (b) 安全等級：

1 級。
- (c) 測試資料：

產品之系統管理者帳密。
- (d) 測試目的：

驗證遠端控制介面之身分鑑別因子於傳輸中是否加密。
- (e) 測試條件：

產品須保持出廠預設環境狀態。

(f) 測試佈局：

見下圖。

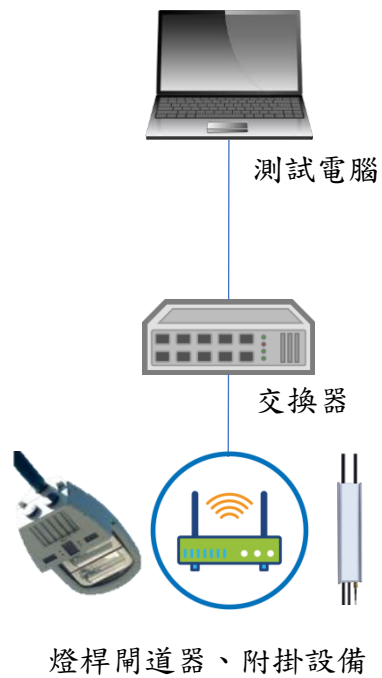


圖 25 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 對產品使用安全通道掃描工具。
- (3) 比對掃描結果是否為附錄 A 中所包含之密碼套件。
- (4) 於相應之管理介面輸入產品之系統管理者帳密，同時側錄封包。
- (5) 檢視所側錄之封包是否採用安全通道。

(h) 檢測結果：

- (1) 安全通道僅支援「附錄 A」中所建議之密碼套件。

(2) 與測試電腦之間的帳號密碼資訊傳輸，預設採用安全通道。

(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：產品無傳輸身分鑑別因子。

5.2.2.2 資料之傳輸保護測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.2.2.2

(b) 安全等級：

2 級。

(c) 測試資料：

後台監控伺服器之 IP 位址。

(d) 測試目的：

驗證產品資料之傳輸，預設是否採用強度足夠之安全通道。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供後台監控伺服器。

(f) 測試佈局：

見下圖。



圖 26 測試示意圖

(g) 測試方法：

- (1) 開啟安全通道掃描工具，對後台監控伺服器進行掃描。
- (2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。
- (3) 將測試電腦連接產品。
- (4) 將產品與後台監控伺服器連線，同時側錄封包。
- (5) 檢視所側錄之封包是否採用安全通道。

(h) 檢測結果：

- (1) 產品與後台監控伺服器之資料傳輸，預設採用安全通道。
- (2) 安全通道僅支援「附錄 A」中所建議之密碼套件。
- (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。

5.3 系統完整性測試

檢視智慧路燈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 實體介面安全管控測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.3.1.1

(b) 安全等級：

2 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證是否可透過產品實體介面，存取作業系統之除錯模式，或具身分鑑別。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須於文件中說明進入作業系統除錯模式之方法。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據文件所述連接相應之實體介面。

(2) 測試電腦連接產品之 USB 埠，並開啟相應之管理介面連接工具。

(3) 透過 USB 埠存取作業系統之除錯模式。

- (4) 測試電腦連接產品之 UART 埠，並開啟相應之管理介面連接工具。
- (5) 透過 UART 埠存取作業系統之除錯模式。
- (6) 測試電腦連接產品之 JTAG 埠，並開啟相應之管理介面連接工具。
- (7) 透過 JTAG 埠存取作業系統之除錯模式。
- (h) 檢測結果：
 - (1) 產品透過 USB、UART 及 JTAG 存取作業系統之除錯模式時，產品要求身分鑑別。
 - (2) 產品不存在進入作業系統除錯模式之介面。
 - (3) 通過: (1)~(2)二項結果符合其一。
 - (4) 不通過: (1)~(2)二項結果皆不符合。
 - (5) 不適用: 無。

5.4 軟體更新測試

檢視智慧路燈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 備援更新功能測試

- (a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.4.1.1
- (b) 安全等級：

1 級。
- (c) 測試資料：

無。

(d) 測試目的：

驗證當更新作業異常中斷時，產品仍可恢復正常運作狀態。

(e) 測試條件：

- (1) 產品須支援線上更新。
- (2) 廠商須負責觸發線上更新。

(f) 測試佈局：

見下圖。

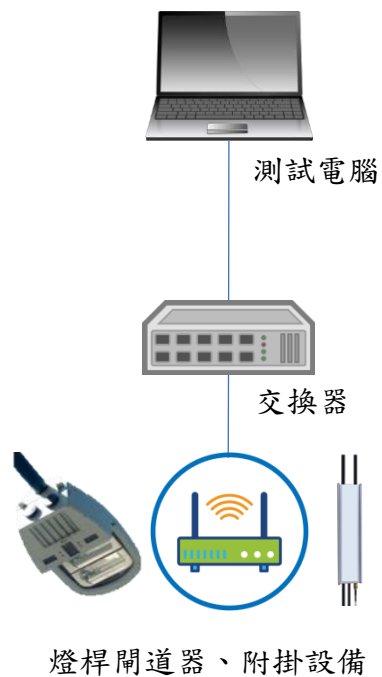


圖 27 測試示意圖

(g) 測試方法：

- (1) 啟動線上更新。
- (2) 於更新過程中(非韌體檔案下載階段)，觸發更新中斷。

(h) 檢測結果：

- (1) 通過: 更新中斷後，系統仍可回復正常運作狀態。

(2) 不通過: 更新中斷後, 系統無法回復正常運作狀態, 或無支援線上更新功能。

(3) 不適用: 無。

5.4.1.2 韌體更新路徑的保護

(a) 測試依據:

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部: 一般要求」5.4.1.2

(b) 安全等級:

1 級。

(c) 測試資料:

測試用假憑證。

(d) 測試目的:

驗證產品的韌體線上更新是否採用安全通道, 以確保韌體之機密性、正確性及完整性, 同時是否具有鑑別安全通道所使用憑證之合法性及有效性。

(e) 測試條件:

(1) 產品須支援線上更新。

(2) 產品須提供所有相連伺服器之宣告。

(3) 受測廠商須協助觸發產品之線上更新。

(f) 測試佈局:

見下圖。



圖 28 測試示意圖

(g) 測試方法：

- (1) 將測試電腦、產品與更新伺服器連結在同一個區域網路中。
- (2) 啟動韌體更新。
- (3) 使用工具側錄更新伺服器與產品之間的封包。
- (4) 檢視所側錄之封包。
- (5) 再次啟動更新。
- (6) 於更新伺服器發送憑證予產品之間，攔截更新伺服器憑證。
- (7) 置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
- (8) 發送已竄改之憑證予產品。
- (9) 於安全通道建立的交握過程中監聽封包。
- (10) 檢視所側錄之封包。

(h) 檢測結果：

- (1) 產品之線上更新路徑通過安全通道，且安全通道僅支援「附錄 A」中所建議之密碼套件。
- (2) 更新伺服器之憑證公鑰或憑證資訊其一被竄改，安全通道建立失敗。
- (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或不支援線上更新功能。
- (5) 不適用: 產品無支援線上更新。

5.4.1.3 韌體檔案安全測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.4.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

產品所提供之韌體檔案。

(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) 產品須提供所使用之韌體檔案。
- (2) 產品須提供所使用之加密演算法書面資料作為審查依據。
- (3) 產品須提供所有相連伺服器之宣告。

(f) 測試佈局：

無。

(g) 測試方法：

- (1) 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。
- (2) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。
- (3) 檢視該韌體更新檔是否可被解析出檔案系統目錄。
- (4) 審閱可證明所使用加密演算法之書面資料。
- (5) 確認系統通行碼資料的保密機制是否採用 FIPS 140-2 Annex A 所核可之雜湊函數。
- (6) 確認金鑰是否可被擷取。
- (7) 確認是否存在非公開之 email 資料。
- (8) 確認是否存在產品所宣告之相連伺服器外之 IP 資料。
- (9) 確認是否存在產品所宣告之相連伺服器外之 URL 資料。

(h) 檢測結果：

- (1) 韌體無法解析出安全敏感性資料或安全敏感性資料保密機制採用 FIPS 140-2 Annex A 所核可之雜湊函數。
- (2) 系統之更新來源應與廠商自我宣告中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。
- (3) 通過：(1)~(2)二項結果皆符合。
- (4) 不通過：(1)~(2)二項結果不符其一。
- (5) 不適用：無。

5.4.1.4 系統降版安全測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.4.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證系統是否可降為較舊之系統版本。

(e) 測試條件：

(1) 產品須支援線上更新。

(2) 廠商須負責觸發線上更新。

(f) 測試佈局：

見下圖。



圖 29 測試示意圖

(g) 測試方法：

- (1) 廠商使用舊韌體版本觸發更新。
- (2) 啟動線上更新。

(h) 檢測結果：

- (1) 通過：更新失敗。
- (2) 不通過：更新成功。
- (3) 不適用：無。

5.5 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。

5.5.1 日誌檔與警示測試

5.5.1.1 安全事件日誌檔測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.5.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品是否有安全事件紀錄供查詢。

(e) 測試條件：

無。

(f) 測試佈局：

見下圖。



圖 30 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 以產品之系統管理者帳密登入。
- (3) 根據產品使用說明，開啟相應之管理介面連接工具。
- (4) 瀏覽安全事件日誌。
- (5) 確認日誌內容是否記載使用者的登入紀錄。
- (6) 檢視該日誌之登入紀錄是否提供正確時間、使用者身分及執行結果。
- (7) 將產品重新開機。
- (8) 根據產品使用說明，開啟相應之管理介面連接工具。
- (9) 瀏覽安全事件日誌。

(10) 檢視重開機前之日誌資料是否仍然可視。

(h) 檢測結果：

(1) 產品具有安全事件日誌功能。

(2) 安全事件日誌的資料包含正確時間(包括年、月、日、時、分、秒)、使用者身分及執行結果。

(3) 重開機前之安全事件紀錄仍可查詢。

(4) 通過: (1)~(3)三項結果皆符合。

(5) 不通過: (1)~(3)三項結果不符合其一。

(6) 不適用: 無。

5.5.1.2 日誌紀錄安全敏感性資料外洩測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.5.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證日誌紀錄是否會洩露安全敏感性資料。

(e) 測試條件：

(1) 產品須支援安全事件日誌功能。

(2) 產品須提供系統管理者權限之身分。

(f) 測試佈局：

見下圖。



圖 31 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 若產品支援網頁介面，開啟並以產品之系統管理者身分登入。
- (3) 瀏覽安全事件日誌。
- (4) 檢視安全事件日誌是否存在安全敏感性資料。
- (5) 若產品可存取作業系統層之介面，開啟該介面並以產品之系統管理者身分登入。
- (6) 重複(3)~(4)之步驟。

(h) 檢測結果：

- (1) 通過：日誌記錄無安全敏感性資料。
- (2) 不通過：安全敏感性資料以明文或甚至可被回復成明文的方式顯示在安全事件日誌中。

(3) 不適用：產品無支援安全事件日誌功能。

5.5.1.3 安全事件日誌檔存取權限管控測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.5.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之安全事件日誌紀錄是否具備權限控管。

(e) 測試條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 產品須提供安全事件日誌檔存取權限說明。

(f) 測試佈局：

見下圖。



圖 32 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 以產品之系統管理者帳密登入。
- (4) 瀏覽安全事件日誌。
- (5) 登出後以產品之一般使用者帳密登入。
- (6) 瀏覽安全事件日誌。
- (7) 檢視帳號之身分類型對安全事件日誌檔的存取權限是否與產品自我宣告相符。

(h) 檢測結果：

- (1) 安全事件日誌檔的身分授權與產品自我宣告相符。
- (2) 至少有二個以上不同權限的角色。

- (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: 產品無提供日誌紀錄。

5.5.1.4 安全事件日誌檔之日誌滾動功能測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.5.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品是否具備處理日誌儲存空間不足之異常狀況。

(e) 測試條件：

產品須提供系統管理者權限供測試用。

(f) 測試佈局：

見下圖。

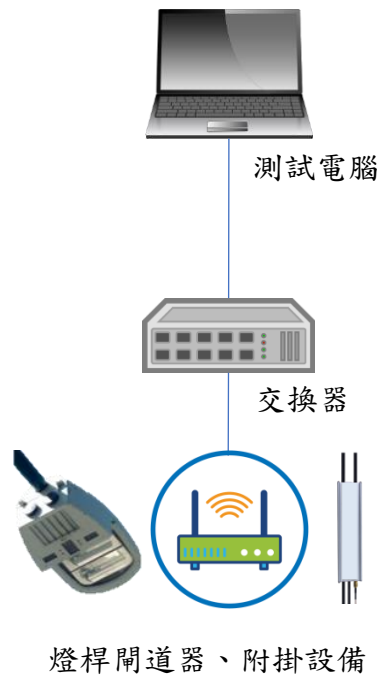


圖 33 測試示意圖

(g) 測試方法：

- (1) 不斷觸發安全事件。
- (2) 填充儲存容量，直到儲存空間不足。
- (3) 檢視產品是否無法正常記錄安全事件。

(h) 檢測結果：

- (1) 產品不會發生儲存空間不足的現象。
- (2) 產品仍可正常記錄安全事件。
- (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: 產品無提供日誌紀錄。

5.5.1.5 產品安全事件警示功能測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.5.1.5

(2) 安全等級：

1 級。

(3) 測試資料：

無。

(4) 測試目的：

驗證產品發生安全事件時，是否進行推播或告警等警示機制。

(5) 測試條件：

(i) 產品須支援使用者登錄。

(ii) 廠商須提供安全事件警示機制之說明。

(6) 測試佈局：

見下圖。

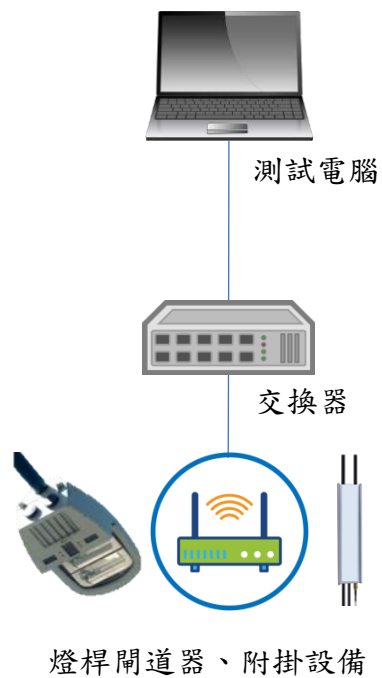


圖 34 測試示意圖

(7) 測試方法：

- (i) 觸發產品各種使用者登錄介面(包括: 網頁介面、遠端指令控制介面、應用程式介面、實體介面)之安全事件。
- (ii) 根據產品提供之說明文件，檢視警示狀態。

(8) 檢測結果：

- (i) 通過: 產品發生安全事件時，發出推播或告警等警示機制。
- (ii) 不通過: 產品發生安全事件時，無推播或告警等警示。

5.6 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。

5.6.1 作業系統與網路服務測試

5.6.1.1 測試作業系統與網路服務是否存在 CVSS v3 評分為 9.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.6.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品 IP 位址。

(2) 產品所提供之系統管理者帳密。

(d) 測試目的：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 重大資安風險之漏洞。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 後台監控伺服器不適用。

(3) 產品須支援作業系統與網路服務。

(4) 產品須提供系統管理者帳密。

(f) 測試佈局：

見下圖。



圖 35 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具作業系統及網路服務弱點掃描功能之工具。
- (3) 設定產品之 IP 位址及系統管理者帳密。
- (4) 對產品執行弱點掃描。

(h) 檢測結果：

- (1) 通過：作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。
- (2) 不通過：作業系統與網路服務存在國家弱點資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。
- (3) 不適用：產品無作業系統或網路服務之功能。

5.6.1.2 測試作業系統與網路服務是否存在 CVSS v3 評分為 7.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.6.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品 IP 位址。

(2) 產品所提供之系統管理者帳密。

(d) 測試目的：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 高資安風險之漏洞。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 後台監控伺服器不適用。

(3) 產品須支援作業系統與網路服務。

(4) 產品須提供系統管理者帳密。

(f) 測試佈局：

見下圖。



圖 36 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具作業系統及網路服務弱點掃描功能之工具。
- (3) 設定產品之 IP 位址及系統管理者帳密。
- (4) 對產品執行弱點掃描。

(h) 檢測結果：

- (1) 通過：作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。
- (2) 不通過：作業系統與網路服務存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。
- (3) 不適用：產品無作業系統或網路服務之功能。

5.6.2 網路服務連接埠測試

5.6.2.1 網路服務最小化測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 5.6.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

產品之 IP 位址。

(d) 測試目的：

驗證產品是否存在預期以外之網路埠。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供所啟用之網路服務與對應埠之宣告。

(f) 測試佈局：

見下圖。



圖 37 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具網路埠掃描功能之工具。
- (3) 對產品執行 TCP 埠 0~65535 之掃描。
- (4) 檢視掃描結果所呈現之網路服務與對應埠。
- (5) 對產品執行 UDP 埠 0~65535 之掃描。
- (6) 檢視掃描結果所呈現之網路服務與對應埠。

(h) 檢測結果：

- (1) 通過：產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

- (2) 不通過：產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」或「資料內容」不相符。
- (3) 不適用：產品無網路服務之功能。

5.7 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。

5.7.1 應用程式安全測試

5.7.1.1 網頁管理介面常見資安風險測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.7.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之 IP 位址。

(2) 產品之系統管者帳密。

(d) 測試目的：

驗證產品之網頁管理介面是否存在已知資安漏洞。

(e) 測試條件：

(1) 產品須提供系統管理者權限供測試用。

(2) 產品須支援網頁介面。

(f) 測試佈局：

見下圖。



圖 38 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 開啟網頁介面，檢視網頁是否使用超文本傳輸協定。
- (3) 啟動具備網頁弱點掃描功能之工具。
- (4) 設定產品 IP 位址，對產品網頁介面執行弱點掃描。
- (5) 檢視該弱點掃描工具所產生之報告，是否存在 OWASP web TOP 10 [4]之資安攻擊風險。

(h) 檢測結果：

- (1) 通過: 產品之網頁介面，不存在引發 OWASP web Top 10 之資安攻擊風險。
- (2) 不通過: 產品之網頁介面，存在引發 OWASP web Top 10 之資安攻擊風險。
- (3) 不適用: 產品無支援網頁介面。

5.7.1.2 應用程式權限控管測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」5.7.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證產品之應用程式是否存在超級使用者權限。

(e) 測試條件：

產品須提供具聯網功能之應用程式權限使用說明文件。

(f) 測試佈局：

見下圖。



圖 39 測試示意圖

(g) 測試方法：

- (1) 審閱產品所提供具聯網功能之應用程式權限使用說明文件。

(h) 檢測結果：

- (1) 通過: 產品之應用程式，不存在超級使用者權限。
- (2) 不通過: 產品之網頁介面，存在超級使用者權限。
- (3) 不適用: 產品無支援應用程式。

6. 資安測試規範-後台監控伺服器測試

6.1 身分識別、鑑別、權限控管要求測試

檢視智慧路燈系統之身分識別、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 身分鑑別錯誤訊息

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.1

(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) 不存在之使用者帳密。

(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。

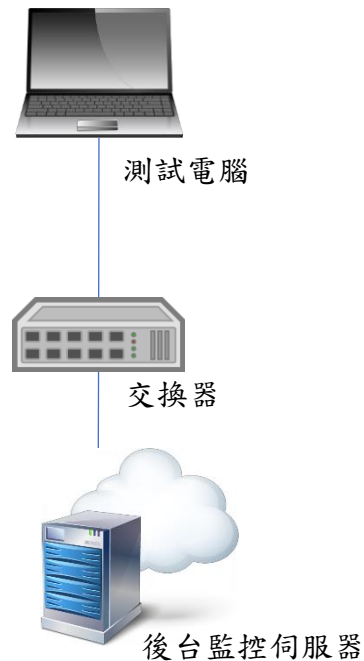


圖 40 測試示意圖

(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密。
- (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) 不適用：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.1

(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) 不存在之使用者帳密。

(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：

無。

(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密。

(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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.1.1

(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) 不存在之使用者帳密。

(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。

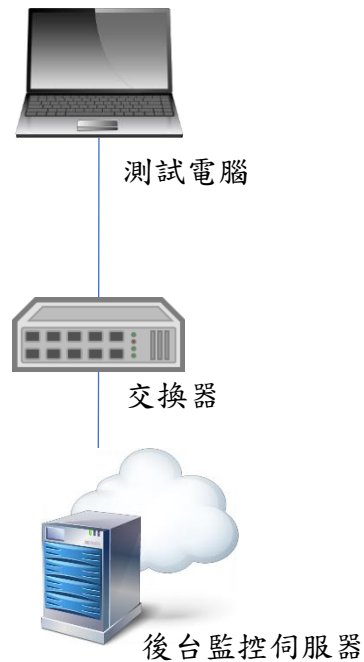


圖 41 測試示意圖

(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密。
- (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-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.1

(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) 不存在之使用者帳密。

(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。

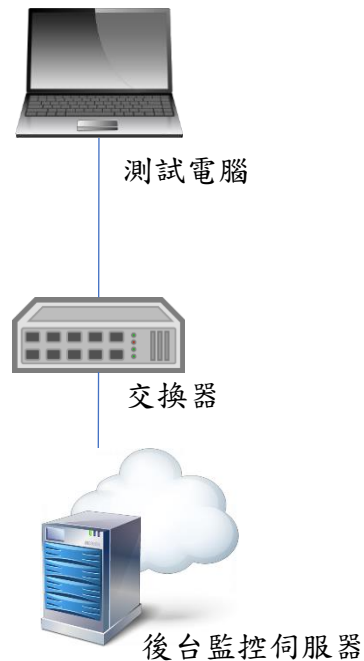


圖 42 測試示意圖

(7) 測試方法：

- (i) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (ii) 將產品連結後台監控伺服器。
- (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密。

(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。

6.1.1.2 鑑別機制強度測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

產品須支援網頁介面。

(6) 測試佈局：

見下圖。

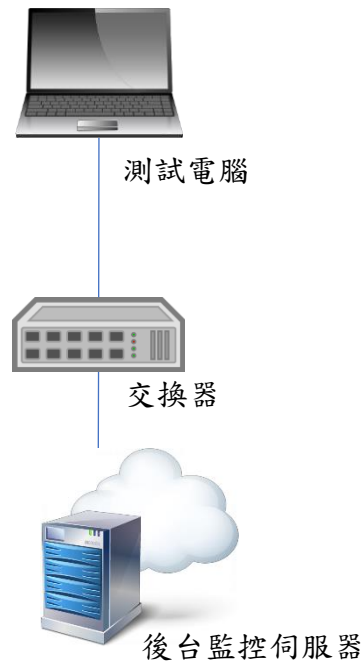


圖 43 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 於未登入的狀況下，存取身分鑑別頁面外之頁面，確認是否要求身分鑑別
- (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，開啟網頁介面。
- (v) 以產品之系統管理員帳密登入，執行身分鑑別操作。
- (vi) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。
- (vii) 檢視鑑別結果是否成功。

(8) 檢測結果：

- (i) 網頁管理介面具備身分鑑別。

(ii) 身分鑑別機制具備抵抗重送攻擊的能力。

(iii) 通過: (i)~(ii)二項結果皆符合。

(iv) 不通過: (i)~(ii)三項結果不符合其一。

(v) 不適用: 產品無支援網頁介面。

(b) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

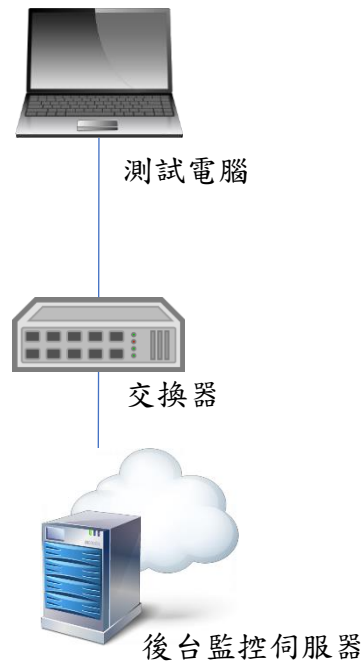


圖 44 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。
- (iii) 根據產品使用說明，開啟遠端指令介面。
- (iv) 以產品之系統管理員帳密登入，執行身分鑑別操作。
- (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。

(8) 檢測結果：

- (i) 產品於遠端指令介面能正常執行身分鑑別機制。
- (ii) 身分鑑別機制具備抵抗重送攻擊的能力。
- (iii) 通過: (i)~(ii)二項結果皆符合。

(iv) 不通過: (i)~(ii)二項結果不符合其一。

(v) 不適用: 產品無支援遠端指令介面。

(c) 射頻介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

無。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

(i) 產品須支援射頻介面。

(ii) 產品須提供使用說明並宣告其敏感性功能。

(iii) 後台監控伺服器不適用。

(6) 測試佈局：

見下圖。

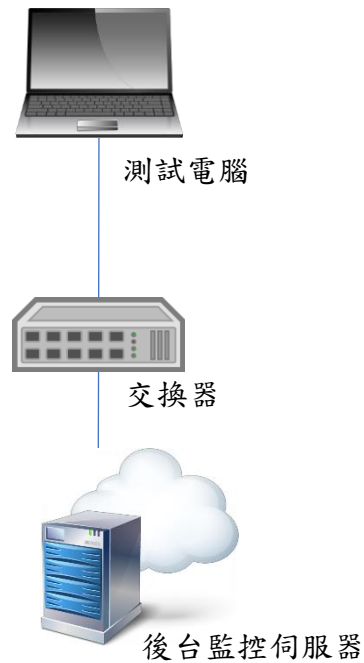


圖 45 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 根據產品使用說明，執行敏感性功能或身份鑑別。
- (iii) 使用軟體定義無線電(SDR)，側錄無線電波訊號。
- (iv) 使用 SDR 重新播放側錄之無線電波訊號。
- (v) 確認產品是否有進行相同行為。

(8) 檢測結果：

- (i) 通過: 經 SDR 重新播放後，產品無進行相同行為。
- (ii) 不通過: 經 SDR 重新播放後，產品有進行相同行為。
- (iii) 不適用: 後台監控伺服器。

(d) Web API 介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理員帳密。

(4) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(5) 測試條件：

產品須支援 Web API 介面。

(6) 測試佈局：

見下圖。

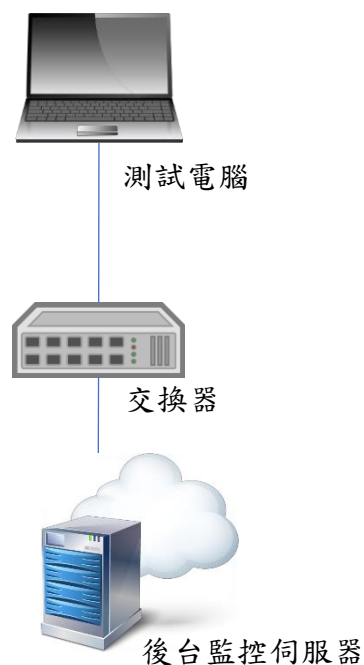


圖 46 測試示意圖

(7) 測試方法：

- (i) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (ii) 將產品連結後台監控伺服器。
- (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，執行身分鑑別操作。
- (v) 執行具 Web API 功能之操作。
- (vi) 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。
- (vii) 檢視鑑別結果是否成功。

(8) 檢測結果：

- (i) 產品於 Web API 介面能正常執行身分鑑別機制。
- (ii) 身分鑑別機制具備抵抗重送攻擊的能力。
- (iii) 通過: (i)~(ii)二項結果皆符合。
- (iv) 不通過: (i)~(ii)二項結果不符合其一。
- (v) 不適用: 產品無支援網頁介面。

6.1.1.3 金鑰唯一性測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證產品之金鑰是否唯一。

(e) 測試條件：

- (1) 產品須存在金鑰。
- (2) 根金鑰(Root Key)不在此測試範圍。

(f) 測試佈局：

見下圖。

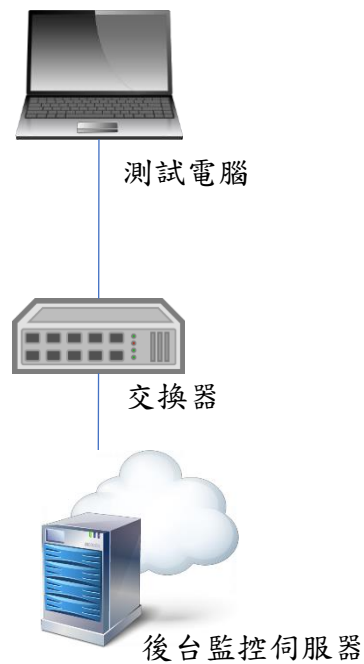


圖 47 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 輸入產品之系統管理者帳密以執行身分鑑別。
- (4) 側錄封包並擷取產品之憑證，檢視其指紋碼(fingerprint)。

(5) 重置產品至出廠預設狀態。

(6) 重覆步驟(2)~(4)。

(h) 檢測結果：

(1) 若測試設備透過圖形化管理介面連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(2) 若測試設備透過安全外殼協定(SSH)連接產品，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(3) 若測試是產品與其它後台監控伺服器互連，重置出廠預設狀態前後，憑證之指紋碼是相異的。

(4) 通過: (1)~(3)三項結果皆符合。

(5) 不通過: (1)~(3)三項結果不符合其一。

(6) 不適用: 產品不存在金鑰。

6.1.1.4 多因子鑑別機制測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.1.4

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之身分鑑別機制是否支援多因子認證或 FIDO 之強認證機制。

(e) 測試條件：

(1) 狀況 1：

- (i) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，且多因子鑑別功能已啟用。
 - (ii) 須提供具多因子鑑別操作之產品說明文件。
- (2) 狀況 2：
- (i) 產品若有支援 FIDO 機制，須提供通過證書。
- (f) 測試佈局：
- 見下圖。

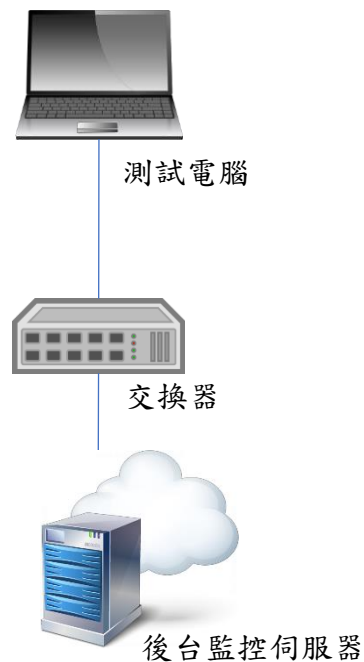


圖 48 測試示意圖

- (g) 測試方法：
- (1) 狀況 1：
 - (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) 執行第一項多因子身分鑑別操作。

- (iv) 檢查鑑別過程中是否採用短訊服務(Short Message Service, SMS)獲取通行碼。
- (v) 檢查鑑別過程中，使用行動裝置作為所持之物(something you have)之鑑別因子時，檢視是否僅可在 1 台行動裝置上獲取鑑別因子。
- (vi) 執行第二項多因子身分鑑別操作。
- (vii) 檢查是否與之前的身分鑑別都採用不同種類之鑑別因子。
- (viii)重複(iv)~(v)步驟。
- (ix) 若有第三項以上多因子身分鑑別操作，則執行多因子身分鑑別操作。
- (x) 檢查是否與之前的身分鑑別都採用不同種類之鑑別因子。
- (xi) 重複(iv)~(v)步驟。

(2) 狀況 2：

- (i) 產品若檢視 FIDO 證書

(h) 檢測結果：

(1) 狀況 1：

- (i) 產品透過多因子身分鑑別進行身分鑑別。
- (ii) 每一階段身分鑑別皆採用不同因素的鑑別因子。
- (iii) 當使用鑑別因子時，未採用短訊服務獲取通行碼。
- (iv) 當行動裝置作為所持之物之鑑別因子時，僅可在 1 台行動裝置上獲取鑑別因子。
- (v) 通過: (i)~(iv)四項結果皆符合。
- (vi) 不通過: (i)~(iv)四項項結果不符合其一。
- (vii) 不適用: 無。

(2) 狀況 2：

- (i) 通過: 產品具 FIDO 認證。

(ii) 不通過: 產品不具 FIDO 認證。

不適用: 無。

6.1.1.5 受信任根憑證測試

(a) 測試依據:

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部: 一般要求」 6.1.1.5

(b) 安全等級:

1 級。

(c) 測試資料:

無。

(d) 測試目的:

產品是否具備驗證相連裝置所發送之憑證是否為受信任之根憑證所發行的能力。

(e) 測試條件:

產品須列出使用到憑證的功能。

(f) 測試佈局:

見下圖。



圖 49 測試示意圖

(g) 測試方法：

- (1) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (2) 將產品與其對連之終端裝置，如：後台監控伺服器或燈桿附掛設備。
- (3) 設定中間人攔截熱點，於身分鑑別階段，開啟封包側錄工具進行側錄。
- (4) 當其對連終端裝置發送憑證予產品之間時攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
- (5) 發送已竄改之憑證予產品，檢視產品是否接受此憑證。

(h) 檢測結果：

- (1) 通過：產品不接受此憑證。
- (2) 不通過：產品接受此憑證。
- (3) 不適用：無。

6.1.1.6 終端設備身分證明測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.1.6

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證照明監控系統是否具有遠端證明燈桿閘道器與照明設備身分的能力。

(e) 測試條件：

- (1) 產品須提供遠端證明之設計文件。
- (2) 產品須提供對接的後台監控伺服器、燈桿閘道器及照明設備。
- (3) 相連設備須支援憑證認證方式。
- (4) 產品須提供安全通道加密之私鑰。

(f) 測試佈局：

見下圖。



圖 50 測試示意圖

(g) 測試方法：

- (1) 審閱具備遠端證明功能之設計文件。
- (2) 將燈桿開道器與後台監控伺服器建立連線。
- (3) 於安全通道建立後，攔截傳送至後台監控伺服器之封包。
- (4) 使用產品提供之安全通道私鑰，解開封包之內容。
- (5) 更改憑證內容後，以安全通道之公鑰進行加密，並傳輸至後台監控伺服器。
- (6) 檢視後台監控伺服器是否接受此封包。
- (7) 將照明設備與後台監控伺服器建立連線。
- (8) 重複步驟(3)~(6)。

(h) 檢測結果：

- (1) 通過:後台監控伺服器不接受遭竄改憑證之封包。
- (2) 不通過:後台監控伺服器接受遭竄改憑證之封包。

- (3) 不適用:相連設備不支援憑證認證方式。

6.1.2 權限控管測試

6.1.2.1 權限控管機制測試

(a) 網頁介面

- (1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.2.1

- (2) 安全等級：

1 級。

- (3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

- (4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

- (5) 測試條件：

(i) 產品須具備創建多個不同權限使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

- (6) 測試佈局：

見下圖。

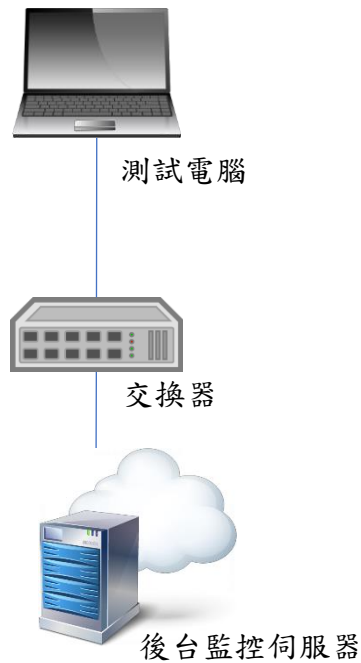


圖 51 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟網頁介面。
- (iii) 以一般使用者帳密登入。
- (iv) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (v) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 進行登出，並以系統管理者帳密登入。
- (vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。



(viii)嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(8) 檢測結果：

(i) 通過：於網頁介面的身分授權與產品自我宣告相符。

(ii) 不通過：於網頁介面的身分授權與產品自我宣告不相符，或產品無支援創建多個不同權限使用者之功能。

(iii) 不適用：產品無支援網頁介面。

(b) 實體介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.2.1

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(5) 測試條件：

(i) 產品須具備創建多個不同權限使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

(iii) 產品須支援實體介面。

(6) 測試佈局：

無。

(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) 以一般使用者帳密登入。
- (v) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 以系統管理者帳密登入。
- (vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (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)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)步驟。

(8) 檢測結果：

- (i) 通過：於 UART、USB 及 JTAG 介面的身分授權與產品自我宣告相符。
- (ii) 不通過：於 UART、USB 或 JTAG 介面的身分授權與產品自我宣告不相符，或產品無支援創建多個不同權限使用者之功能。
- (iii) 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.2.1

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(5) 測試條件：

(i) 產品須具備創建多個不同權限之使用者之功能。

(ii) 產品須提供角色存取權限之宣告。

(iii) 產品須支援遠端指令介面。

(6) 測試佈局：

見下圖。

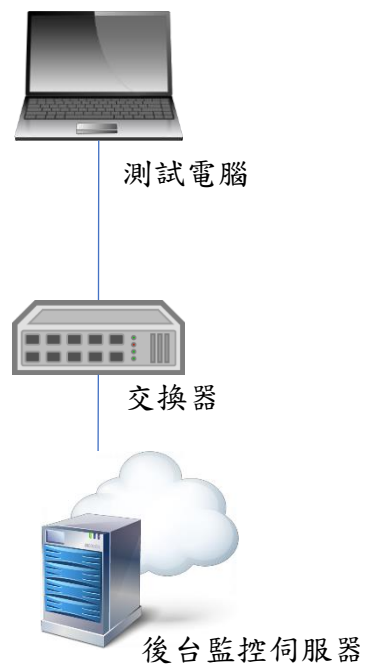


圖 52 測試示意圖

(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) 以一般使用者帳密登入。
- (iv) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (v) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (vi) 以系統管理者帳密登入。
- (vii) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。
- (viii) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(8) 檢測結果：

- (i) 通過：於遠端指令介面的身分授權與產品自我宣告相符。
- (ii) 不通過：於遠端指令介面的身分授權與產品自我宣告相符，或產品無支援創建多個不同權限之使用者之功能。
- (iii) 不適用：產品無支援遠端指令介面。

6.1.2.2 權限有效時間測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證產品是否存在有限的授權時間長度。

(e) 測試條件：

產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(f) 測試佈局：

見下圖。

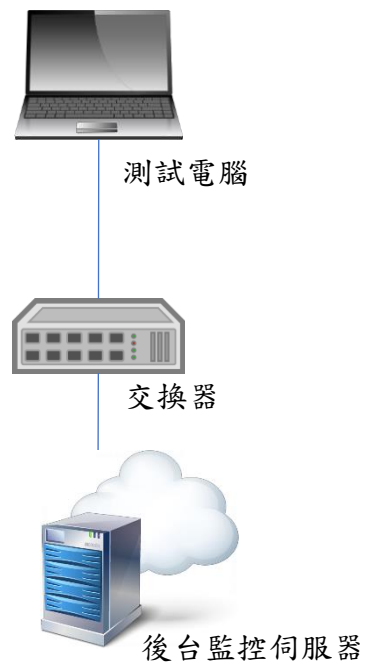


圖 53 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 透過網頁管理介面登入產品。
- (3) 檢視產品之網頁管理介面，閒置時限是否存在供使用者設定的操作介面。
- (4) 閒置產品直到超過閒置時限值。

(5) 檢視是否需要重新鑑別方可存取產品。

(h) 檢測結果：

- (1) 產品之授權行為，存在閒置時限供使用者設定。
- (2) 遠端連線閒置逾時，須經過身分鑑別方可存取產品。
- (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。

6.1.3 通行碼鑑別測試

6.1.3.1 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

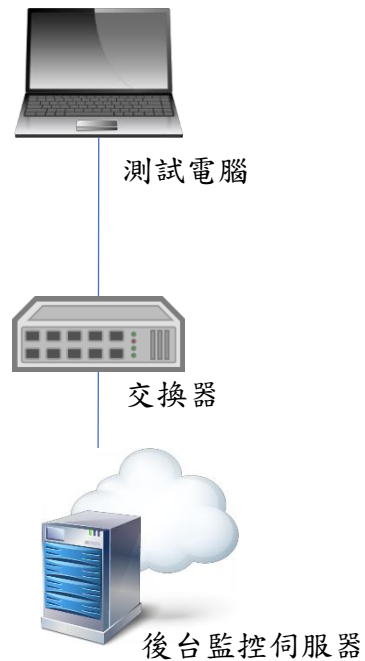


圖 54 測試示意圖

(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) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

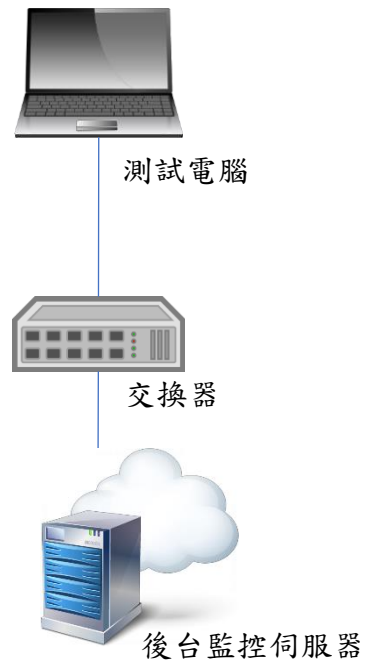


圖 55 測試示意圖

(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。

6.1.3.2 通行碼連續字元之避免測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.2

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

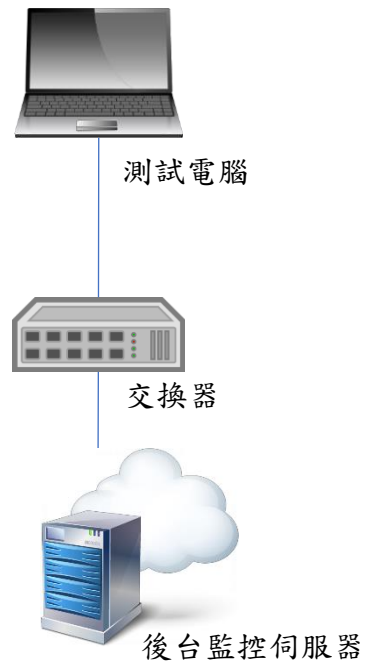


圖 56 測試示意圖

(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) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.2

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

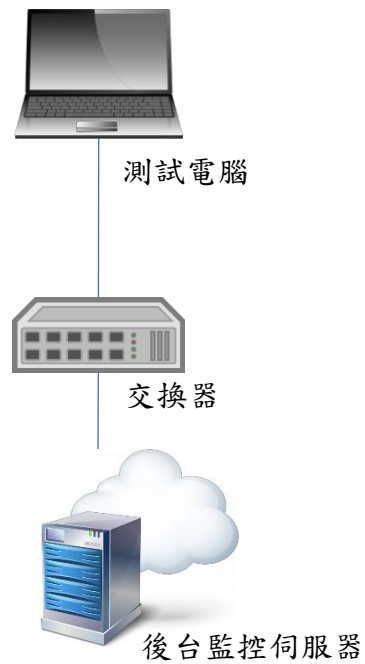


圖 57 測試示意圖

(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。

6.1.3.3 通行碼歷程記錄測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

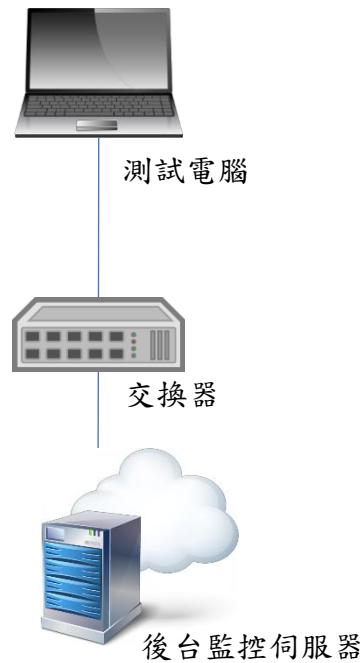


圖 58 測試示意圖

(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) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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。

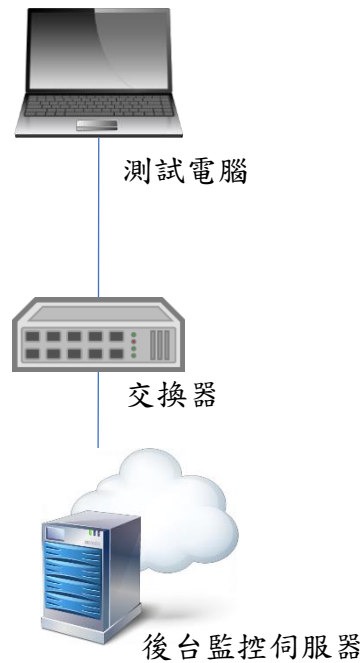


圖 59 測試示意圖

(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。

6.1.3.4 預設通行碼測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.4

(2) 安全等級：

1 級。

(3) 測試資料：

產品提供之網頁介面預設通行碼。

(4) 測試目的：

(i) 狀況 1：

驗證產品是否有相同的預設通行碼。

(ii) 狀況 2：

驗證產品預設通行碼是否會於首次上線後，具強制要求更改預設通行碼之功能。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制，且須提供預設通行碼。

(ii) 產品須保持出廠具強制要求更改預設通行碼之功能。

(iii) 後台監控伺服器不適用。

(iv) 產品須支援網頁介面。

(6) 測試佈局：

見下圖。

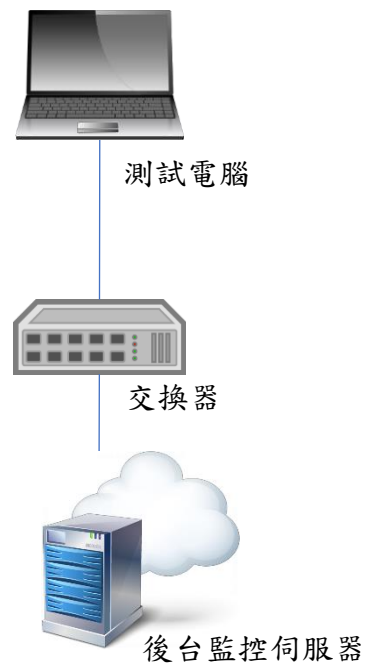


圖 60 測試示意圖

(7) 測試方法：

(i) 狀況 1:

1. 準備 2 台以上產品。
2. 將測試電腦連接第一個產品。
3. 開啟網頁管理介面。
4. 於登入頁面輸入產品提供之預設通行碼。
5. 將測試電腦連接第二個產品。
6. 重複 3~4 之步驟。

(ii) 狀況 2:

1. 將測試電腦連接產品。
2. 開啟網頁介面。

3. 確認產品是否會於首次上線後，強制要求更改通行碼之功能。
4. 取消輸入通行碼。

(8) 檢測結果：

(i) 狀況 1:

1. 通過: 任 2 台產品的預設通行碼相異。
2. 不通過: 任 2 台產品的預設通行碼相同。
3. 不適用: 產品不支援通行碼鑑別機制。

(ii) 狀況 2:

1. 通過: 未經設定新通行碼前無法存取產品。
2. 不通過: 未經設定新通行碼前仍可存取產品。
3. 不適用: 產品不支援通行碼鑑別機制。

(iii) 通過: (i)~(ii)二項狀況符合其一。

(iv) 不通過: (i)~(ii)二項狀況皆不符合。

(v) 不適用: 後台監控伺服器。

(vi) 不適用: 產品無支援網頁介面。

(b) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.3.4

(2) 安全等級：

1 級。

(3) 測試資料：

產品提供之遠端指令介面預設通行碼。

(4) 測試目的：

(i) 狀況 1：

驗證產品是否有相同的預設通行碼。

(ii) 狀況 2：

驗證產品預設通行碼是否會於首次上線後，具強制要求更改預設通行碼之功能。

(5) 測試條件：

(i) 產品須支援通行碼鑑別機制，且須提供預設通行碼。

(ii) 產品須保持出廠具強制要求更改預設通行碼之功能。

(iii) 後台監控伺服器不適用。

(iv) 產品須支援網遠端指令介面。

(6) 測試佈局：

見下圖。

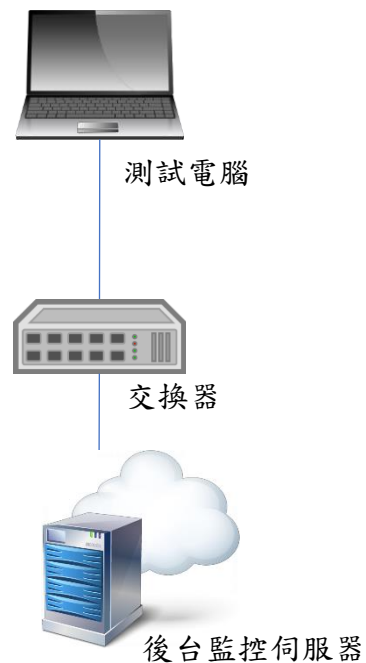


圖 61 測試示意圖

(7) 測試方法：

(i) 狀況 1:

1. 準備 2 台以上產品。
2. 將測試電腦連接第一個產品。
3. 開啟遠端指令介面。
4. 於登入介面輸入產品提供之預設通行碼。
5. 將測試電腦連接第二個產品。
6. 重複 3~4 之步驟。

(ii) 狀況 2:

1. 將測試電腦連接產品。
2. 開啟遠端指令介面。
3. 確認產品是否會於首次上線後，強制要求更改通行碼之功能。
4. 取消輸入通行碼。

(8) 檢測結果：

(i) 狀況 1:

1. 通過: 任 2 台產品的預設通行碼相異。
2. 不通過: 任 2 台產品的預設通行碼相同。
3. 不適用: 產品不支援通行碼鑑別機制。

(ii) 狀況 2:

1. 通過: 未經設定新通行碼前無法存取產品。
2. 不通過: 未經設定新通行碼前仍可存取產品。
3. 不適用: 產品不支援通行碼鑑別機制。

(iii) 通過: (i)~(ii)二項狀況符合其一。

(iv) 不通過: (i)~(ii)二項項狀況皆不符合。

(v) 不適用: 後台監控伺服器。

(vi) 不適用: 產品無支援遠端指令介面。

6.1.3.5 通行碼長度測試

(a) 網頁介面:

(1) 測試依據:

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部: 一般要求」 6.1.3.5

(2) 安全等級:

1 級。

(3) 測試資料:

產品之系統管理者帳密。

(4) 測試目的:

驗證產品的通行碼長度是否足夠, 以確保其強度。

(5) 測試條件:

(iii) 產品須支援通行碼鑑別機制。

(iv) 產品須支援網頁介面。

(6) 測試佈局:

見下圖。

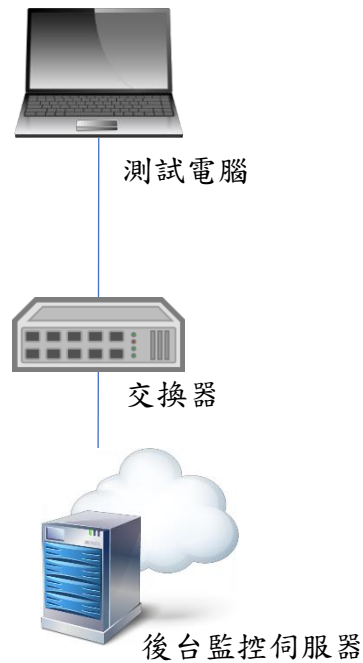


圖 62 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 開啟網頁管理介面，建立或變更通行碼。
- (iii) 輸入小於 8 個字元長度之通行碼。
- (iv) 檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過：無法建立或變更小於 8 個字元長度之通行碼。
- (ii) 不通過：可建立或變更小於 8 個字元長度之通行碼。
- (iii) 不適用：產品須無支援通行碼鑑別機制。
- (iv) 不適用：產品須無支援網頁介面。

(b) 遠端指令介面：

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.5

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(4) 測試目的：

驗證產品的通行碼長度是否足夠，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。

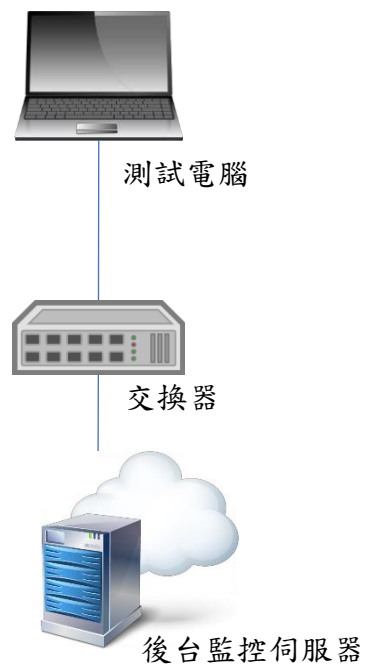


圖 63 測試示意圖

(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) 輸入小於 8 個字元長度之通行碼。
- (v) 檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

- (i) 通過：無法建立或變更小於 8 個字元長度之通行碼。
- (ii) 不通過：可建立或變更小於 8 個字元長度之通行碼。
- (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。

6.1.3.6 通行碼複雜度測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.1.3.6

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(4) 測試目的：

驗證產品的通行碼複雜度是否足夠，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。

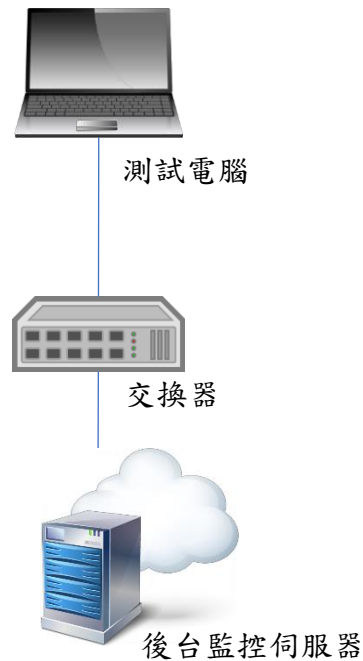


圖 64 測試示意圖

(7) 測試方法：

(i) 將測試電腦連接產品。

(ii) 從網頁管理介面，建立或變更通行碼。

(iii) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，檢查通行碼是否能成功建立或變更。

(8) 檢測結果：

(i) 通過: 無法於網頁介面建立或變更通行碼。

(ii) 不通過: 成功於網頁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：產品無支援網頁介面。

(b) 遠端指令介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.1.3.6

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(4) 測試目的：

驗證產品的通行碼複雜度是否足夠，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。

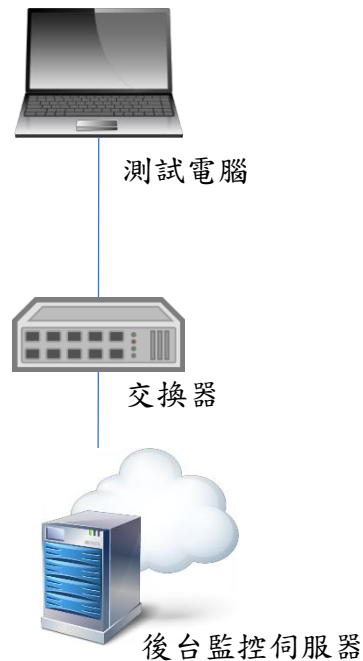


圖 65 測試示意圖

(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) 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，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。

6.2 資料機密性與完整性測試

檢視智慧路燈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 金鑰管理程序測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.2.1.1

(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[3]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。

6.2.1.2 安全敏感性資料隔離保護測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.2.1.2

(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。

6.2.1.3 安全敏感性資料權限管控測試

(a) 初階測試：

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.2.1.3

(2) 安全等級：

1 級。

(3) 測試資料：

產品所提供之安全敏感性資料保存方式。

(4) 測試目的：

產品安全敏感性資料的存取是否具有權限控管機制。

(5) 測試條件：

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。

(6) 測試佈局：

無。

(7) 測試方法：

審閱能證明符合此安全要求之書面資料。

(8) 檢測結果：

(i) 產品通行碼資料之權限管控與產品自我宣告相符。

(ii) 產品之加解密金鑰的權限管控與產品自我宣告相符。

(iii) 該權限管控機制至少擁有二個以上不同權限的角色。

(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: 產品無存放安全敏感性資料。

(b) 中階測試:

(1) 測試依據:

TAICS TS-0027-1「智慧路燈系統資安標準-第一部:一般要求」6.2.1.3

(2) 安全等級:

2 級。

(3) 測試資料:

(i) 產品之一般使用者帳密。

(ii) 產品之系統管理者帳密。

(4) 測試目的:

驗證產品安全敏感性資料的存取是否具有權限控管機制。

(5) 測試條件:

(i) 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。

(ii) 產品須提供系統管理者權限供測試用。

(iii) 產品須提供能進入作業系統層之介面。

(6) 測試佈局:

見下圖。

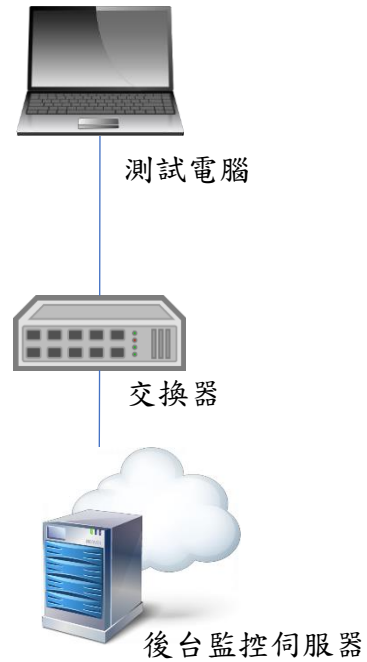


圖 66 測試示意圖

(7) 測試方法：

- (i) 將測試電腦連接產品。
- (ii) 以產品之一般使用者身分登入。
- (iii) 確認通行碼資料存取權限。
- (iv) 確認加解密金鑰存取權限。
- (v) 登出後以產品之系統管理者身分登入。
- (vi) 確認通行碼資料存取權限。
- (vii) 確認加解密金鑰存取權限。

(8) 檢測結果：

- (i) 產品通行碼資料之權限管控與產品自我宣告相符。
- (ii) 產品之加解密金鑰之權限管控與產品自我宣告相符。

(iii) 該權限管控機制至少擁有二個以上不同權限的角色。

(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: 產品無存放安全敏感性資料。

6.2.1.4 安全敏感性資料加密儲存測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.2.1.4

(c) 安全等級：

2 級。

(d) 測試資料：

無。

(e) 測試目的：

驗證產品之安全敏感性資料於儲存狀態下是否加密保護。

(f) 測試條件：

(1) 產品須提供安全敏感性資料儲存保護之演算法書面資料作為審查依據。

(2) 產品須提供系統管理者權限供測試用。

(3) 產品須提供能進入作業系統層之介面。

(4) 根金鑰(Root Key)不在此測試範圍。

(g) 測試佈局：

見下圖。

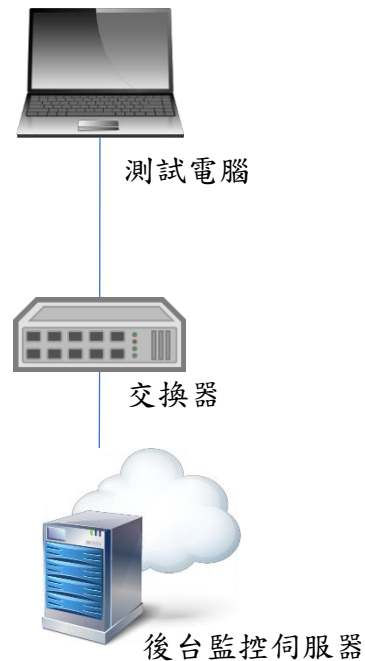


圖 67 測試示意圖

(h) 測試方法：

- (1) 審閱能證明符合此安全要求之書面資料。
- (2) 將測試電腦連接產品。
- (3) 若產品支援 UART，將測試電腦連接產品之 UART。
- (4) 透過 UART 埠存取作業系統之除錯模式。
- (5) 透過搜尋工具，查找安全敏感性資料位置。
- (6) 檢視保護通行碼資料所採用的雜湊演算法。
- (7) 檢視保護加解密金鑰所採用的保密機制。
- (8) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。
- (9) 過 JTAG 埠存取作業系統之除錯模式。
- (10) 重複(5)~(7)之步驟。
- (11) 若產品支援 USB，將測試電腦連接產品之 USB。

- (12) 過 USB 埠存取作業系統之除錯模式。
- (13) 重複(5)~(7)之步驟。
- (14) 若產品支援遠端指令介面，開啟並連接遠端指令介面。
- (15) 重複(5)~(7)之步驟。
- (i) 檢測結果：
 - (1) 通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之雜湊函數。
 - (2) 加解密用金鑰的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。
 - (3) 通過: (1)~(2)二項結果符合其一。
 - (4) 不通過: (1)~(2)二項結果皆不符合。
 - (5) 不適用: 產品無存放安全敏感性資料。

6.2.2 傳輸資料保護測試

6.2.2.1 接收前端資料的完整性與不可否認性測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.2.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證後台監控伺服器是否檢驗與其相連設備所傳送資料的完整性與不可否認性。

(e) 測試條件：

產品須提供照明設備。

(f) 測試佈局：

見下圖。



圖 68 測試示意圖

(g) 測試方法：

- (1) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (2) 將前端設備連結後台監控伺服器並開啟服務。
- (3) 攔截傳送中之資料。
- (4) 竄改攔截到的資料內容，並轉發給後台監控伺服器。
- (5) 檢視竄改過之資料是否可被接受。
- (6) 攔截傳送中之資料。
- (7) 調換簽章，並轉發給後台監控伺服器。
- (8) 檢視竄改過之封包是否可被接受。

(h) 檢測結果：

- (1) 通過：竄改過內容及簽章的資料皆不可被接收。
- (2) 不通過：後台監控伺服器接收竄改過內容或簽章的資料，或資料無使用簽章。
- (3) 不適用：無。

6.2.2.2 身分鑑別因子傳輸安全測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.2.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳密。

(d) 測試目的：

驗證遠端控制介面之身分鑑別因子於傳輸中是否加密。

(e) 測試條件：

產品須保持出廠預設環境狀態。

(f) 測試佈局：

見下圖。

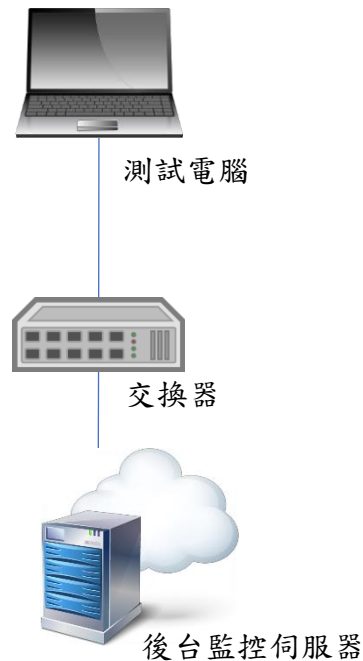


圖 69 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 對產品使用安全通道掃描工具。
- (3) 比對掃描結果是否為附錄 A 中所包含之密碼套件。
- (4) 於相應之管理介面輸入產品之系統管理者帳密，同時側錄封包。
- (5) 檢視所側錄之封包是否採用安全通道。

(h) 檢測結果：

- (1) 安全通道僅支援「附錄 A」中所建議之密碼套件。
- (2) 與測試電腦之間的帳號密碼資訊傳輸，預設採用安全通道。
- (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：產品無傳輸身分鑑別因子。

6.2.2.3 資料之傳輸保護測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.2.2.3

(b) 安全等級：

2 級。

(c) 測試資料：

後台監控伺服器之 IP 位址。

(d) 測試目的：

驗證產品資料之傳輸，預設是否採用強度足夠之安全通道。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供後台監控伺服器。

(f) 測試佈局：

見下圖。

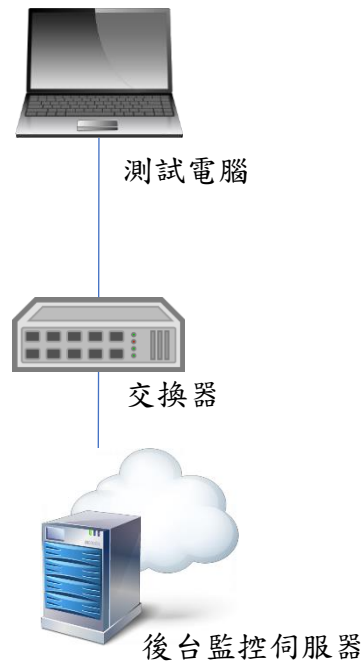


圖 70 測試示意圖

(g) 測試方法：

- (1) 開啟安全通道掃描工具，對後台監控伺服器進行掃描。
- (2) 比對掃描結果是否為附錄 A 中所包含之密碼套件。
- (3) 將測試電腦連接產品。
- (4) 將產品與後台監控伺服器連線，同時側錄封包。
- (5) 檢視所側錄之封包是否採用安全通道。

(h) 檢測結果：

- (1) 產品與後台監控伺服器之資料傳輸，預設採用安全通道。
- (2) 安全通道僅支援「附錄 A」中所建議之密碼套件。
- (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。

6.3 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。

6.3.1 日誌檔與警示測試

6.3.1.1 安全事件日誌檔測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.3.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品是否有安全事件紀錄供查詢。

(e) 測試條件：

無。

(f) 測試佈局：

見下圖。

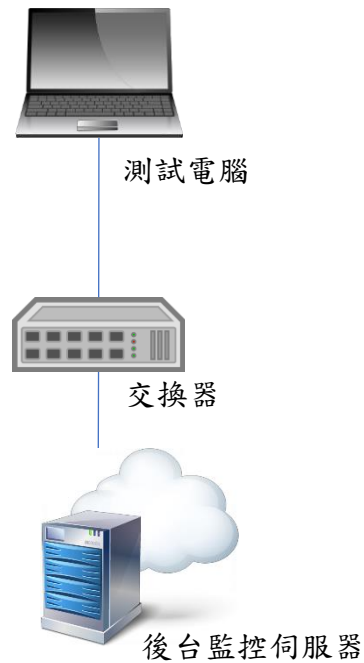


圖 71 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 以產品之系統管理者帳密登入。
- (3) 根據產品使用說明，開啟相應之管理介面連接工具。
- (4) 瀏覽安全事件日誌。
- (5) 確認日誌內容是否記載使用者的登入紀錄。
- (6) 檢視該日誌之登入紀錄是否提供正確時間、使用者身分及執行結果。
- (7) 將產品重新開機。
- (8) 根據產品使用說明，開啟相應之管理介面連接工具。
- (9) 瀏覽安全事件日誌。
- (10) 檢視重開機前之日誌資料是否仍然可視。

(h) 檢測結果：

- (1) 產品具有安全事件日誌功能。
- (2) 安全事件日誌的資料包含正確時間(包括年、月、日、時、分、秒)、使用者身分及執行結果。
- (3) 重開機前之安全事件紀錄仍可查詢。
- (4) 通過: (1)~(3)三項結果皆符合。
- (5) 不通過: (1)~(3)三項結果不符合其一。
- (6) 不適用: 無。

6.3.1.2 日誌紀錄安全敏感性資料外洩測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.3.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證日誌紀錄是否會洩露安全敏感性資料。

(e) 測試條件：

- (1) 產品須支援安全事件日誌功能。
- (2) 產品須提供系統管理者權限之身分。

(f) 測試佈局：

見下圖。

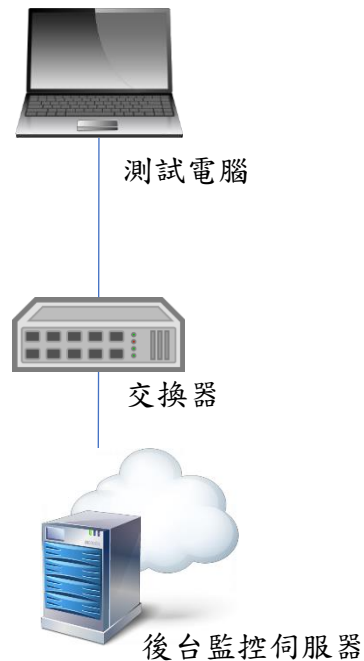


圖 72 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 若產品支援網頁介面，開啟並以產品之系統管理者身分登入。
- (3) 瀏覽安全事件日誌。
- (4) 檢視安全事件日誌是否存在安全敏感性資料。
- (5) 若產品支援遠端指令介面，開啟並以產品之系統管理者身分登入。
- (6) 重複(3)~(4)之步驟。

(h) 檢測結果：

- (1) 通過：日誌記錄無安全敏感性資料。
- (2) 不通過：安全敏感性資料以明文或甚至可被回復成明文的方式顯示在安全事件日誌中。
- (3) 不適用：產品無支援安全事件日誌功能。

6.3.1.3 安全事件日誌檔存取權限管控測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.3.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之安全事件日誌紀錄是否具備權限控管。

(e) 測試條件：

(1) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立，並且存在系統管理者及一般使用者二類帳號。

(2) 產品須提供安全事件日誌檔存取權限說明。

(f) 測試佈局：

見下圖。

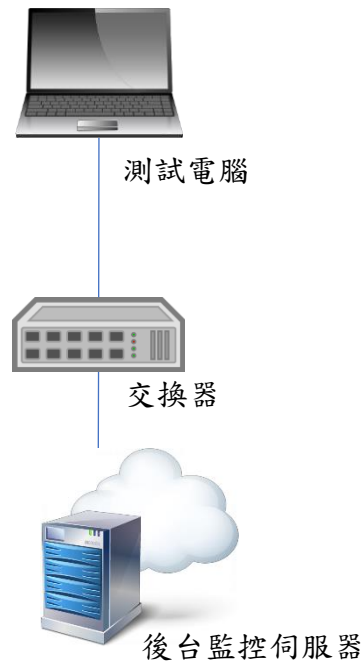


圖 73 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 以產品之系統管理者帳密登入。
- (4) 瀏覽安全事件日誌。
- (5) 登出後以產品之系統管理者帳密登入。
- (6) 瀏覽安全事件日誌。
- (7) 檢視帳號之身分類型對安全事件日誌檔的存取權限是否與產品自我宣告相符。

(h) 檢測結果：

- (1) 安全事件日誌檔的身分授權與產品自我宣告相符。
- (2) 至少有二個以上不同權限的角色。

- (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: 產品無提供日誌紀錄。

6.3.1.4 安全事件日誌檔之日誌滾動功能測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.3.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品是否具備處理日誌儲存空間不足之異常狀況。

(e) 測試條件：

產品須提供系統管理者權限供測試用。

(f) 測試佈局：

見下圖。

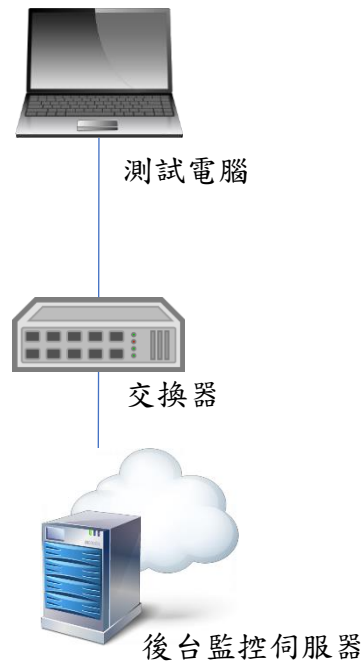


圖 74 測試示意圖

(g) 測試方法：

- (1) 不斷觸發安全事件。
- (2) 填充儲存容量，直到儲存空間不足。
- (3) 檢視產品是否無法正常記錄安全事件。

(h) 檢測結果：

- (1) 產品不會發生儲存空間不足的現象。
- (2) 產品仍可正常記錄安全事件。
- (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: 產品無提供日誌紀錄。

6.3.1.5 產品安全事件警示功能測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.3.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品發生安全事件時，是否進行推播或告警等警示機制。

(e) 測試條件：

廠商須提供安全事件警示機制之說明。

(f) 測試佈局：

見下圖。

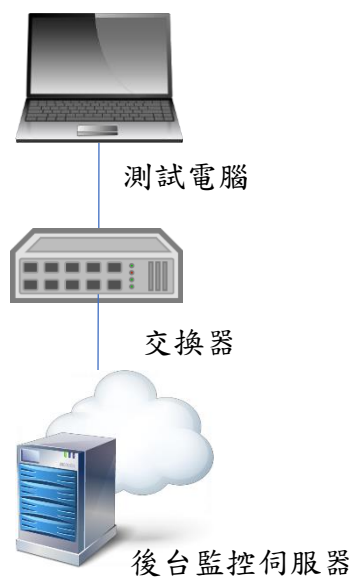


圖 75 測試示意圖

(g) 測試方法：

- (1) 觸發產品定義之安全事件。
- (2) 根據產品提供之說明文件，檢視警示狀態。

(h) 檢測結果：

- (1) 通過：產品發生安全事件時，發出推播或告警等警示機制。
- (2) 不通過：產品發生安全事件時，無推播或告警等警示。
- (3) 不適用：無。

6.4 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。

6.4.1 作業系統與網路服務測試

6.4.1.1 測試後台監控伺服器之作業系統與網路服務是否存在 CVSS v3 評分為 7.0 分以上之常見資安弱點與漏洞

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.4.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

- (1) 產品 IP 位址。
- (2) 產品之系統管理者帳密。

(d) 測試目的：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 高資安風險之漏洞。

(e) 測試條件：

- (1) 產品須保持出廠預設環境狀態。
- (2) 僅照明監控伺服器適用。
- (3) 產品須支援作業系統與網路服務。
- (4) 產品須提供系統管理者帳密。

(f) 測試佈局：

見下圖。

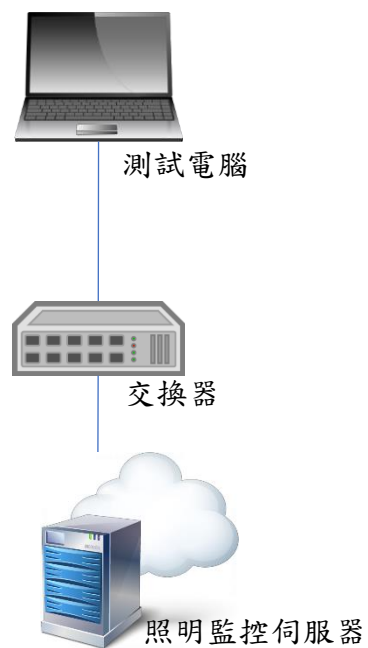


圖 76 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具作業系統及網路服務弱點掃描功能之工具。
- (3) 設定產品之 IP 位址及系統管理者帳密。

(4) 對產品執行弱點掃描。

(h) 檢測結果：

(1) 通過：作業系統與網路服務不存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

(2) 不通過：作業系統與網路服務存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

(3) 不適用：產品無作業系統或網路服務之功能。

6.4.2 網路服務連接埠測試

6.4.2.1 網路服務最小化測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.4.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

產品之 IP 位址。

(d) 測試目的：

驗證產品是否存在預期以外之網路埠。

(e) 測試條件：

(1) 產品須保持出廠預設環境狀態。

(2) 產品須提供所啟用之網路服務與對應埠之宣告。

(f) 測試佈局：

見下圖。

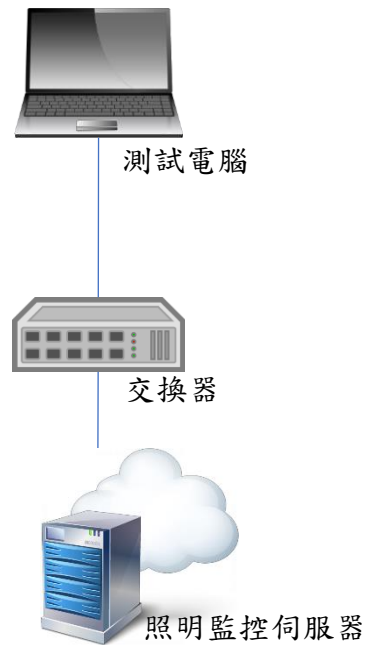


圖 77 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 啟動具網路埠掃描功能之工具。
- (3) 對產品執行 TCP 埠 0~65535 之掃描。
- (4) 檢視掃描結果所呈現之網路服務與對應埠。
- (5) 對產品執行 UDP 埠 0~65535 之掃描。
- (6) 檢視掃描結果所呈現之網路服務與對應埠。

(h) 檢測結果：

- (1) 通過：產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

- (2) 不通過：產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」或「資料內容」不相符。
- (3) 不適用：產品無網路服務之功能。

6.5 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。

6.5.1 網路管理介面安全測試

6.5.1.1 網頁管理介面常見資安風險測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.5.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之 IP 位址。

(2) 產品之系統管者帳密。

(d) 測試目的：

驗證產品之網頁管理介面是否存在已知資安漏洞。

(e) 測試條件：

(1) 產品須提供系統管理者權限供測試用。

(2) 產品須支援網頁介面。

(f) 測試佈局：

見下圖。

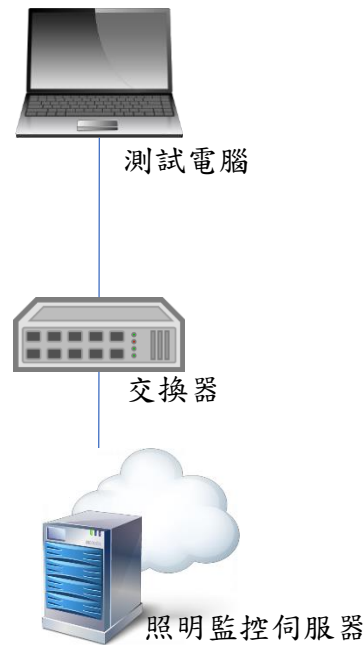


圖 78 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 開啟網頁介面，檢視網頁是否使用超文本傳輸協定。
- (3) 啟動具備網頁弱點掃描功能之工具。
- (4) 設定產品 IP 位址，對產品網頁介面執行弱點掃描。
- (5) 檢視該弱點掃描工具所產生之報告，是否存在 OWASP web TOP 10 [4]之資安攻擊風險。

(h) 檢測結果：

- (1) 通過: 產品之網頁介面，不存在引發 OWASP web Top 10 之資安攻擊風險。
- (2) 不通過: 產品之網頁介面，存在引發 OWASP web Top 10 之資安攻擊風險。
- (3) 不適用: 產品無支援網頁介面。

6.5.1.2 應用程式權限控管測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.5.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之系統管者帳密。

(d) 測試目的：

驗證產品之應用程式是否存在超級使用者權限。

(e) 測試條件：

(1) 產品須提供具聯網功能之應用程式權限使用說明文件。

(f) 測試佈局：

見下圖。

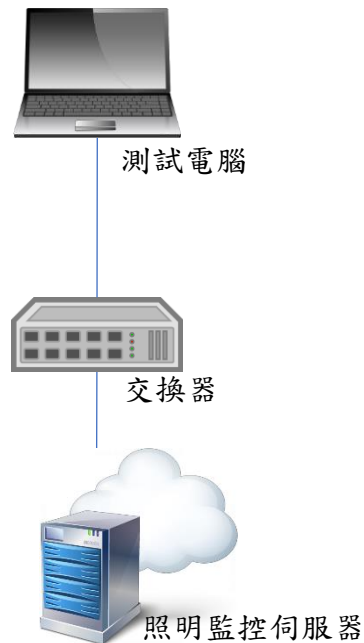


圖 79 測試示意圖

(g) 測試方法：

(1) 審閱產品所提供具聯網功能之應用程式權限使用說明文件。

(h) 檢測結果：

(1) 通過: 產品之應用程式，不存在超級使用者權限。

(2) 不通過: 產品之網頁介面，存在超級使用者權限。

(3) 不適用: 產品無支援應用程式。

6.6 資源可用性測試

檢視智慧路燈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 備份能力測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.6.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

確保產品支援備份功能。

(e) 測試條件：

(1) 產品應提供備份功能之使用說明。

(2) 僅適用於照明監控伺服器。

(f) 測試佈局：

見下圖。

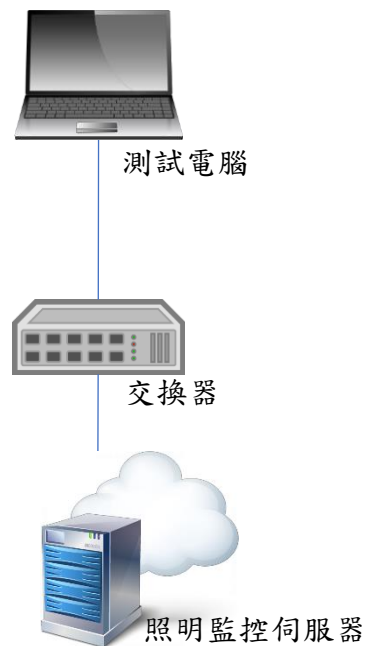


圖 80 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 啟動備份功能，檢視功能是否正常運行。

(h) 檢測結果：

- (1) 通過：備份功能正常運行。
- (2) 不通過：備份功能無法正常運行或無備份功能。
- (3) 不適用：產品非照明監控伺服器。

6.6.1.2 還原能力測試

(a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.6.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

確保產品之系統能被還原到正確的版本。

(e) 測試條件：

(1) 產品應提供備份還原功能之使用說明。

(2) 產品須支援備份功能。

(3) 僅適用於照明監控伺服器。

(f) 測試佈局：

見下圖。

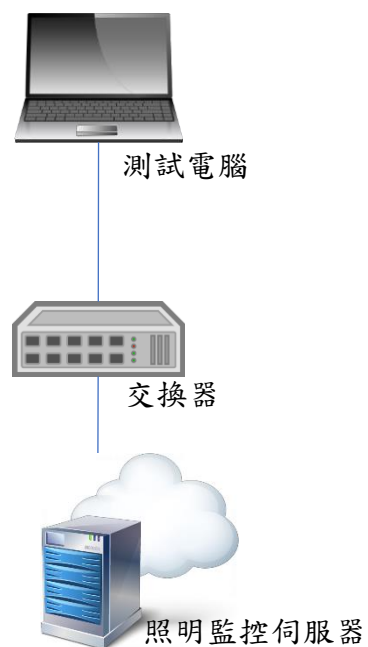


圖 81 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 根據產品使用說明，開啟相應之管理介面連接工具。
- (3) 竄改備份檔案。
- (4) 啟動還原功能，檢視功能是否正常運行。

(h) 檢測結果：

- (1) 通過：還原失敗。
- (2) 不通過：還原成功。
- (3) 不適用：產品無支援備份功能。
- (4) 不適用：產品非照明監控伺服器。

6.7 隱私保護測試

檢視智慧路燈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 隱私資料傳輸保護測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.7.1.1

(b) 安全等級：

2 級。

(c) 測試資料：

後台監控伺服器 IP 位址。

(d) 測試目的：

驗證隱私資料的傳送是否經由安全通道。

(e) 測試條件：

伺服器提供的服務含隱私資料。

(f) 測試佈局：

見下圖。



圖 82 測試示意圖

(g) 測試方法：

- (1) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (2) 將前端設備連結後台監控伺服器。
- (3) 側錄傳送中之封包。
- (4) 檢視封包中的隱私資料是否走安全通道。
- (5) 啟動安全通道掃描工具。

- (6) 設定後台監控伺服器 IP 位址，並進行掃描。
- (7) 比對掃描結果，檢視伺服器所支援的密碼套件，是否符合附錄 B 之要求。
- (h) 檢測結果：
 - (1) 通過: 隱私資料走安全通道，且安全通道之密碼套件符合附錄 B 之要求。
 - (2) 不通過: 隱私資料沒走安全通道，或安全通道之密碼套件不符合附錄 B 之要求。
 - (3) 不適用: 伺服器提供的服務不含隱私資料。

6.7.1.2 隱私資料存取管控測試

- (a) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 6.7.1.2

- (b) 安全等級：

1 級。

- (c) 測試資料：

- (1) 後台監控伺服器 IP 位址。
- (2) 後台監控伺服器之一般使用者帳密。
- (3) 後台監控伺服器之系統管理者帳密。

- (d) 測試目的：

驗證產品隱私權是否具有存取控制機制。

- (e) 測試條件：

- (1) 伺服器提供的服務含隱私。
- (2) 產品須提供隱私存取權限之宣告。
- (3) 產品必須能建立 2 個以上的帳號。

- (f) 測試佈局：

見下圖。



圖 83 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 透過網頁介面，以一般使用者帳密登入產品。
- (3) 存取資料，並檢視該帳號之身分類型與其對應之隱私存取權限是否與產品自我宣告相符。
- (4) 當產品提供網頁介面且已經有帳號登入的情況下，檢視是否無需透過帳號切換，即可存取該帳號權限之外的隱私資料。
- (5) 進行登出，並以系統管理者帳密登入產品。
- (6) 重複(3)~(4)步驟。

(h) 檢測結果：

- (1) 通過：使用者的隱私存取授權與產品自我宣告相符。
- (2) 不通過：使用者的隱私存取授權與產品自我宣告不相符。
- (3) 不適用：伺服器提供的服務不含隱私資料。
- (4) 不適用：產品無法建立 2 個以上的帳號。

6.7.1.3 隱私政策宣告測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.7.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

後台監控伺服器 IP 位址。

(d) 測試目的：

驗證產品是否具有隱私政策宣告。

(e) 測試條件：

- (1) 廠商須提供隱私政策文件。
- (2) 產品須提供隱私政策之連結。

(f) 測試佈局：

見下圖。



圖 84 測試示意圖

(g) 測試方法：

- (1) 將測試電腦連接產品。
- (2) 開啟至網頁介面的首頁，選擇隱私政策選項或連結。
- (3) 核對該頁面內容及廠商提供之隱私政策文件，須與世界經濟合作暨發展組織 (OECD) 個資保護基本原則之規定相符。

(h) 檢測結果：

- (1) 通過: 伺服器網頁介面首頁有宣告隱私政策，其隱私政策之內容須符合世界經濟合作暨發展組織 (OECD) 個資保護基本原則之規定。
- (2) 不通過: 伺服器網頁介面無隱私政策宣告，或不符合隱私政策內容與世界經濟合作暨發展組織 (OECD) 個資保護基本原則之規定。
- (3) 不適用: 無。

6.8 雲端平台安全測試

檢視智慧路燈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 雲端認證測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」6.8.1.1

(b) 安全等級：

3 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品之雲端平台是否有經過 ISO 27017[6]或 CSA STAR[7]認證。

(e) 測試條件：

廠商須提供 ISO 27017 或 CSA STAR 通過證明。

(f) 測試佈局：

無。

(g) 測試方法：

審閱 ISO 27017 或 CSA STAR 之通過證明文件。

(h) 檢測結果：

(1) 通過: 雲端平台有取得 ISO 27017 或 CSA STAR 認證。

(2) 不通過: 雲端平台未取得 ISO 27017 或 CSA STAR 認證。

(3) 不適用：無。

7. 資安測試規範-燈桿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

檢視智慧路燈系統之身分識別、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 身分鑑別錯誤訊息測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.1.1.1

(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) 不存在之使用者帳密。

(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。



圖 85 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密。
- (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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.1.1

(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) 不存在之使用者帳密。

(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。



圖 86 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) 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密。
- (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-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.1.1.1

(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) 不存在之使用者帳密。

(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 87 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密。
- (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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.1.1

(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) 不存在之使用者帳密。

(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 88 測試示意圖

(7) 測試方法：

- (i) 將測試電腦與後台監控伺服器連結在同一個區域網路中。
- (ii) 將產品連結後台監控伺服器。
- (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密。
 - (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。

7.1.2 權限管控測試

7.1.2.1 測試須依循第錯誤！找不到參照來源。節「資安測試規範-物聯網設備安全基本要求測試」第 5.1.2 節。

7.1.3 通行碼鑑別測試

7.1.3.1 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」7.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 89 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-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 90 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.1

(2) 安全等級：

1 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 91 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。

7.1.3.2 通行碼連續字元之避免測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.2

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 92 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.2

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 93 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」7.1.3.2

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 94 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。

7.1.3.3 通行碼歷程記錄測試

(a) 網頁介面

(1) 測試依據：

TAICS TS-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 95 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 96 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-0027-1 「智慧路燈系統資安標準-第一部：一般要求」 7.1.3.3

(2) 安全等級：

3 級。

(3) 測試資料：

產品之系統管理者帳密。

(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 97 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。

7.2 資料機密性與完整性測試

檢視智慧路燈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 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.2.1 節。

7.2.1.2 金鑰管理程序測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.2.1.2

(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[3]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。

7.2.1.3 安全敏感性資料隔離保護測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.2.1.3

(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。

7.2.2 傳輸資料保護測試

7.2.2.1 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.2.2 節。

7.3 系統完整性測試

檢視智慧路燈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 測試須依循第**錯誤! 找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.3.1 節。

7.3.1.2 韌體萃取安全測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.3.1.2

(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，查看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 [2]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。

7.3.1.3 測試產品是否支援安全啟動功能測試

(a) 測試依據：

TAICS TS-0027-1「智慧路燈系統資安標準-第一部：一般要求」7.3.1.3

(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。

7.4 軟韌體更新測試

檢視智慧路燈系統之軟韌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 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.4.1 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 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.5.1 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 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.6.1 節。

7.6.2 網路服務連接埠測試

7.6.2.1 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.6.2 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 測試須依循第**錯誤！找不到參照來源。**節「資安測試規範-物聯網設備安全基本要求測試」第 5.7.1 節。

附錄 A (規定) 安全通道建議使用之密碼套件

根據 Mozilla wiki [5] 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-0027-1 智慧路燈系統資安標準-第一部：一般要求
- (2) National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions, available at URL: <http://www.nist.gov/cmvp>.
- (3) National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators, available at URL: <http://www.nist.gov/cmvp>.
- (4) OWASP, OWASP Top 10 – 2017, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- (5) Mozilla wiki, Server Side TLS, https://wiki.mozilla.org/Security/Server_Side_TLS
- (6) ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- (7) CSA Security Trust Assurance and Risk (STAR), <https://cloudsecurityalliance.org/star/>

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