IoT-2005-1

消費性網路攝影機資安測試規範

V1.0

經濟部工業局

中華民國 110 年 6 月

目錄

引言

經濟部工業局於 2017 年率先提出符合安控需求之影像監控系統資安標準，在安防產業上奠定了資訊與網路安全的重要基礎；然而，近年來一般消費市場對於消費性網路攝影機的需求大增，世界各國對於個人隱私的議題亦愈趨重視，其中發生多起個人私密影像外洩，及消費性網路攝影機受到有心人士掌控作為惡作劇或攻擊跳板的問題，多數原因皆指向消費性網路攝影機的資安防護不足。

消費性網路攝影機的設計與使用者區隔有別於影像監控系統之網路攝影機，在資安防禦基礎上應有所區別，因此在工業局與網路攝影機產業的支持下，制定我國消費性網路攝影機資安產業標準。

「IoT-1005-2 消費性網路攝影機資安測試規範」(以下簡稱本測試規範)，依據「IoT-1005-1 消費性網路攝影機資安標準」[1]訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法與測試結果等事項，俾利消費性網路攝影機製造商、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

本標準規定消費性網路攝影機之網路安全要求與檢測項目。該產品設置於消費者欲監看環境中，透過 IP 直接連接網際網路，可將影像與聲音傳送至指定之網路服務平台，消費者透過網際網路在該網路服務平台與欲監看的設備間進行聲音、影像與控制指令傳輸。消費性網路攝影機之適用情境包括但不限於寵物關懷、幼兒照護、長輩照顧和居家安全等應用。

本標準的適用範圍如下圖 1 所示，但不包括下列項目：

(a) 電信網路與消費性網路攝影機網路服務平台間之網路傳輸安全。

(b) 消費性網路攝影機雲端管理平台。

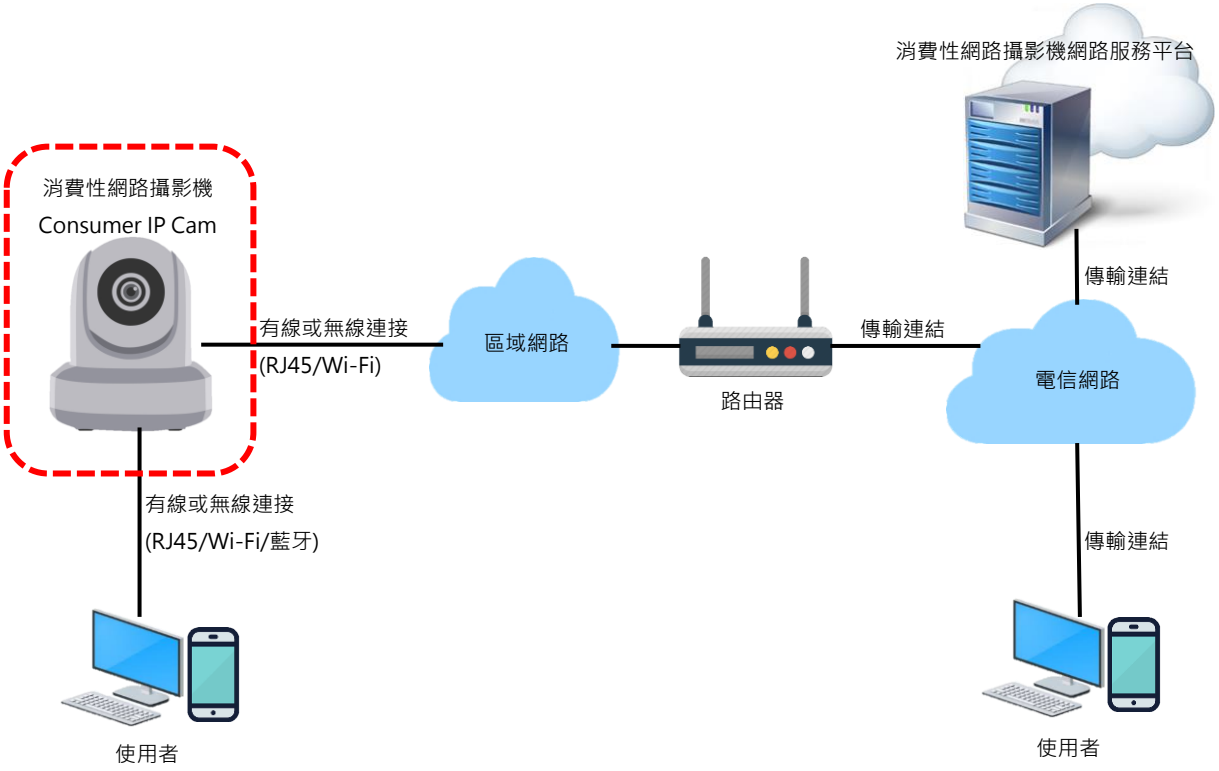

圖 1 適用範圍示意圖

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] IoT-1005-1 v1.0 消費性網路攝影機資安標準

[2] IoT-2001-2 v1.0 影像監控系統資安測試規範-第二部：網路攝影機

3. 用語及定義

「IoT-1005-1 消費性網路攝影機資安標準」所規定及下列用語及定義適用於本規範。

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。

3.3 本地端管理介面(Local Management Interface)

消費者直接存取與控制產品的操作介面，不應連接網際網路經由消費性網路攝影機平台操控產品，例如產品應用程式或透過與電腦連接並以 IP 地址開啟的網頁管理頁面等。

4. 測試項目分級

本節依據「IoT-1005-1 消費性網路攝影機資安標準」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)身分鑑別與權限控管、(2)已知漏洞安全、(3)軟韌體更新、(4)資料機密性與完整性、(5)系統完整性、(6)資源可用性、(7)隱私保護及(8)警示與紀錄；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；第三欄為安全測試細項，為各安全測試項目所做之測試標準。

表 1 實機測試標準等級總表

安全構面	安全測試項目	安全測試細項
5.1 身分鑑別與權限控管	5.1.1 鑑別機制	5.1.1.1 5.1.1.2 5.1.1.3
	5.1.2 權限控管	5.1.2.1 5.1.2.2
	5.1.3 通行碼鑑別	5.1.3.1
5.2 已知漏洞安全	5.2.1 作業系統與網路服務	5.2.1.1
	5.2.2 網路服務連接埠安全	5.2.2.1
	5.2.3 資訊安全管理	5.2.3.1 5.2.3.2 5.2.3.3 5.2.3.4
5.3 軟韌體更新	5.3.1 更新安全	5.3.1.1 5.3.1.2 5.3.1.3 5.3.1.4
5.4 資料機密性與完整性	5.4.1 安全敏感性資料儲存	5.4.1.1 5.4.1.2
	5.4.2 傳輸資料保護	5.4.2.1 5.4.2.2
5.5 系統完整性	5.5.1 實體入侵防護	5.5.1.1
	5.5.2 輸入驗證	5.5.2.1
5.6 資源可用性	5.6.1 資源管理	5.6.1.1
5.7 隱私保護	5.7.1 隱私保護能力	5.7.1.1 5.7.1.2
5.8 警示與紀錄	5.8.1 安全事件警示	5.8.1.1

5. 資安測試規範

5.1 身分鑑別與權限控管測試

檢視產品有關身分鑑別與權限控管部份之送審資料是否符合 IoT-1005-1 之安全要求，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 產品識別碼唯一性測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.1.1

(b) 測試資料：

無。

(c) 測試目的：

查驗產品之識別碼具唯一性。

(d) 測試條件：

(1) 應提供可與產品相連之消費性網路攝影機網路服務平台。

(2) 應提供產品至少 2 件。

(3) 應提供產品識別碼編碼機制說明文件。

(e) 測試佈局：

如圖 2。

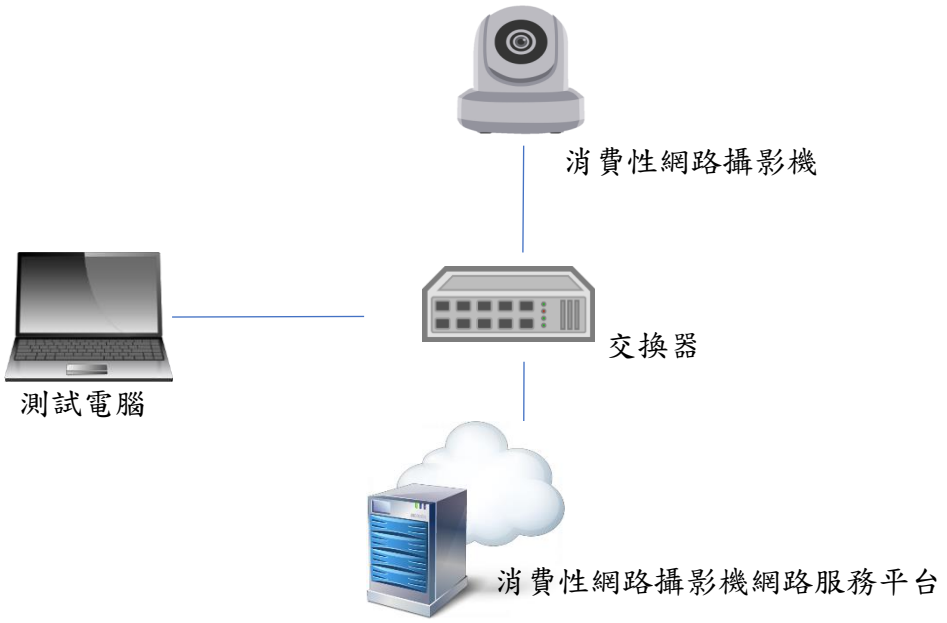

圖 2 測試示意圖

(f) 測試方法：

(1) 審閱具備此程序說明之書面資料。

(2) 檢視產品識別碼之編碼機制。

(3) 將測試電腦與產品連結在同一個區域網路中。

(4) 將產品與消費性網路攝影機網路服務平台對連。

(5) 設定中間人攔截熱點，於安全通道建立階段，開啟封包側錄工具進行側錄。

(6) 側錄封包並檢視識別碼是否與產品識別碼編碼機制一致。

(7) 將另一件產品與伺服器對連，重複步驟(3)~(4)。

(g) 測試結果：

(1) 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) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.1.1.2 金鑰唯一性測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.1.2

(b) 測試資料：

產品之安全通道的憑證。

(c) 測試目的：

查驗產品之金鑰具唯一性。

(d) 測試條件：

(1) 產品應存在金鑰。

(2) 根金鑰(Root Key)不在此測試範圍。

(e) 測試佈局：

如圖 3。

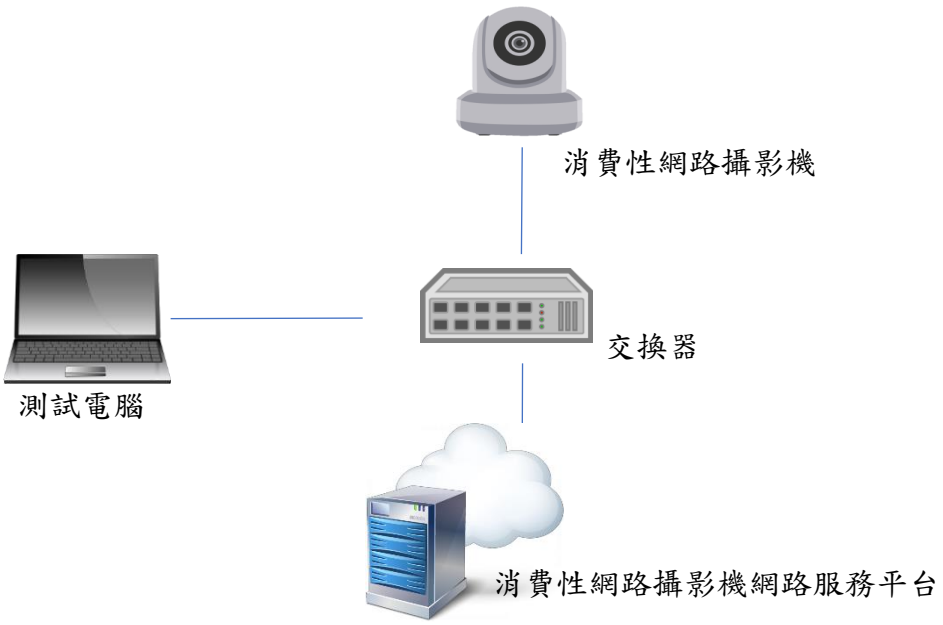

圖 3 測試示意圖

(3) 測試方法：

(1) 將測試電腦與產品連結在同一個區域網路中。

(2) 將產品與消費性網路攝影機網路服務平台對連。

(3) 設定中間人攔截熱點，於安全通道建立階段，開啟封包側錄工具進行側錄。

(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)~(5)。

(f) 測試結果：

(1) 產品重置出廠預設狀態前後，憑證之指紋碼是相異的。

(2) 通過：(1)項結果符合。

(3) 不通過：結果不符合。

(4) 不適用：產品不存在金鑰。

5.1.1.3 鑑別機制強度測試

(a) 本地端管理介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.1.3

(2) 測試資料：

產品之系統管理員帳密。

(3) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(4) 測試條件：

產品應支援本地端管理介面。

(5) 測試佈局：

如圖 4。

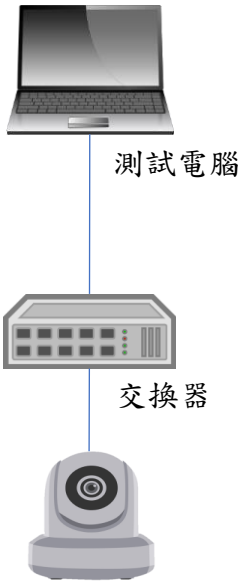

圖 4 測試示意圖

(6) 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，開啟本地端管理介面。

(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。

(7) 測試結果：

(i) 產品於本地端管理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: 產品不支援本地端管理介面。

(b) 網路協定與 API 介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.1.3

(2) 測試資料：

產品之系統管理員帳密。

(3) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(4) 測試條件：

(i) 產品應支援網路協定介面。

(ii) 產品應支援 API 介面。

(5) 測試佈局：

如圖 5。

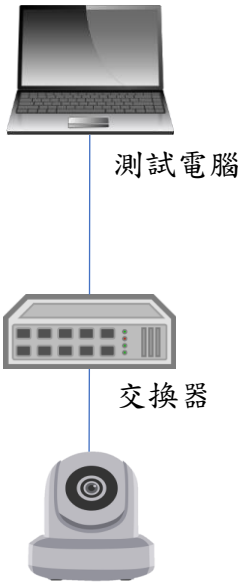

圖 5 測試示意圖

(6) 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，開啟所支援網路協定介面。

(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。

(vii) 根據產品使用說明，開啟所支援 API 介面。

(viii) 以產品之 API 驗證連接方式，執行身分鑑別操作。

(ix) 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。

(x) 檢視鑑別結果是否成功。

(7) 測試結果：

(i) 產品於網路協定介面能正常執行身分鑑別機制。

(ii) 產品於 API 介面正面能正常執行身分鑑別機制。

(iii) 身分鑑別機制具備抵抗重送攻擊的能力。

(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: 產品不支援網路協定介面。

(c) 實體介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.1.3

(2) 測試資料：

產品之系統管理員帳密。

(3) 測試目的：

查驗不可透過產品實體介面，直接存取產品之除錯模式。

(4) 測試條件：

(i) 產品應保持出廠預設組態。

(ii) 產品若存在除錯模式介面，應於文件中說明進入除錯模式之方法。

(5) 測試佈局：

如圖 6。

圖 6 測試示意圖

(6) 測試方法：

(i) 檢查產品是否存在可進入除錯模式之介面。

(ii) 若存在可控制除錯模式介面，則執行以下步驟。

(iii) 根據文件所述連接相應之實體介面。

(8) 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。

(i) 透過 UART 埠存取之除錯模式。

(ii) 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。

(iii) 透過 JTAG 埠存取之除錯模式。

(iv) 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。

(v) 透過 USB 埠存取之除錯模式。

(7) 測試結果：

(i) 產品不存在進入除錯模式之介面。

(ii) 產品透過 UART 及 JTAG 及 USB 存取除錯模式時，產品要求身分鑑別。

(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：產品不支援實體介面。

(d) 測試結果：

(1) 測試依據：通過: (a)~(c)三項結果皆符合。

(2) 不通過：(a)~(c)三項結果不符合其一。

(3) 不適用：(a)~(c)三項介面產品皆不支援。

5.1.2 權限管控測試

5.1.2.1 權限管控機制

(a) 本地端管理介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.2.1

(2) 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。

(3) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(4) 測試條件：

(i) 產品應提供角色存取權限之宣告。

(ii) 產品應支援本地端管理介面。

(9) 測試佈局：

如

圖 7。

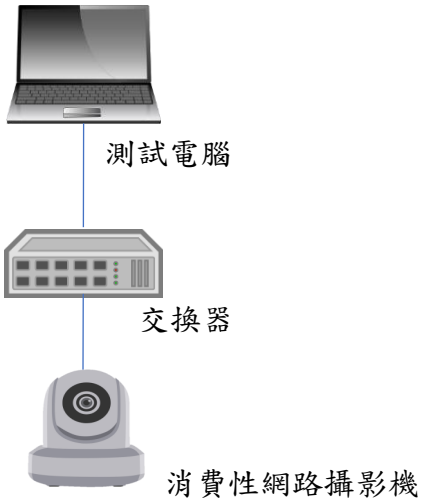

圖 7 測試示意圖

(5) 測試方法：

(i) 將測試電腦連接產品。

(ii) 開啟本地端管理介面。

(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。

(6) 測試結果：

(i) 於本地端管理介面的身分授權與產品自我宣告相符。

(ii) 產品應具備多個不同權限角色之功能，若此功能會對營運產生不利影響，產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項任一結果不符合。

(v) 不適用：產品不支援本地端管理介面。

(b) 網路協定介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.2.1

(2) 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。

(3) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(4) 測試條件：

(i) 產品應提供角色存取權限之宣告。

(ii) 產品應支援網路協定介面。

(5) 測試佈局：

如圖 8。

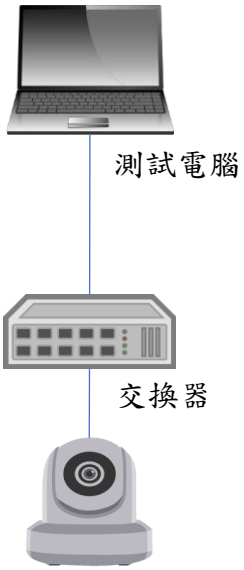

圖 8 測試示意圖

(6) 測試方法：

(i) 將測試電腦連接產品。

(ii) 開啟網路協定介面。

(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。

(7) 測試結果：

(i) 於網路協定介面的身分授權與產品自我宣告相符。

(ii) 產品應具備多個不同權限角色之功能，若此功能會對營運產生不利影響，產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。

(iii) 通過：(i)(ii)項結果皆符合。

(iv) 不通過：(i)(ii)項任一結果不符合。

(v) 不適用：產品不支援網路協定介面。

(c) 測試結果：

(1) 通過：(a)(b)二項結果皆符合。

(2) 不通過：(a)(b)二項結果不符合其一。

(3) 不適用：(a)(b)二項介面產品皆不支援。

5.1.2.2 通行碼的輸入頻率及次數限制

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.2.2

(b) 測試資料：

產品之系統管理者帳密。

(c) 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。

(d) 測試條件：

(1) 產品應支援通行碼鑑別機制，否則此測項不適用。

(2) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(3) 產品應提供帳戶鎖定機制之設計說明。

(4) 產品應支援本地端管理介面。

(e) 測試佈局：

如圖 9。

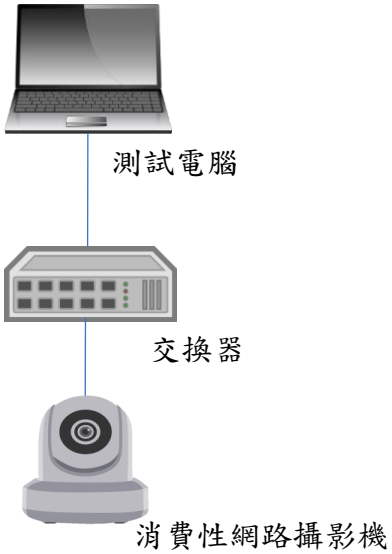

圖 9 測試示意圖

(f) 測試方法：

(1) 將測試電腦或行動裝置連接產品。

(2) 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。

(3) 不斷輸入錯誤且相異的通行碼。

(4) 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，超出廠商宣告可連續登入失敗的次數，是否會鎖定帳戶。

(5) 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。

(6) 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。

(10)測試結果：

(1) 輸入次數超出廠商宣告可連續登入失敗的次數，會鎖定帳戶。

(2) 於廠商宣告之帳戶鎖定時限內，帳戶未解除鎖定。

(3) 於廠商宣告計數器重設時限內，失敗次數未重新計算。

(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：產品應支援本地端管理介面。

5.1.3 通行碼鑑別測試

5.1.3.1 預設通行碼測試

(a) 本地端管理介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.3.1

(2) 測試資料：

產品提供之本地端管理介面預設通行碼。

(3) 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。

(4) 測試條件：

(i) 產品應支援通行碼鑑別機制，且應提供預設通行碼。

(ii) 產品應保持出廠及重置後具強制要求更改預設通行碼之功能。

(iii) 產品應支援本地端管理介面。

(5) 測試佈局：

如圖 10。

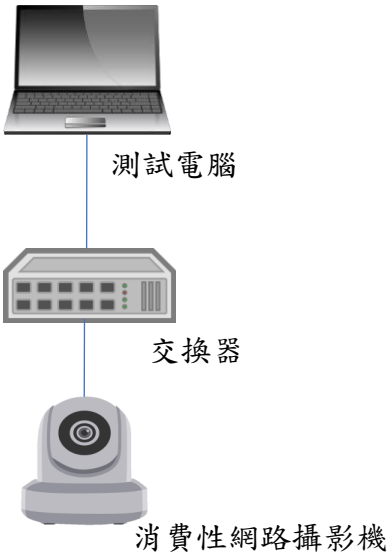

圖 10 測試示意圖

(6) 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. 開啟本地端管理介面。
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. 開啟本地端管理介面。
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。

(7) 測試結果：

(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：產品不支援本地端管理介面。

(b) 實體介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.3.1

(2) 測試資料：

產品提供之實體介面預設通行碼。

(3) 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。

(4) 測試條件：

(i) 產品應支援通行碼鑑別機制，且應提供預設通行碼。

(ii) 產品應保持出廠具強制要求更改預設通行碼之功能。

(iii) 產品應支援實體介面。

(5) 測試佈局：

如圖 11。

圖 11 測試示意圖

(6) 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。

(7) 測試結果：

(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：產品不支援實體介面。

(c) 網路協定介面

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.1.3.1

(2) 測試資料：

產品提供之網路協定介面預設通行碼。

(3) 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。

(4) 測試條件：

(i) 產品應支援通行碼鑑別機制，且應提供預設通行碼。

(ii) 產品應保持出廠具強制要求更改預設通行碼之功能。

(iii) 產品應支援網路協定介面。

(5) 測試佈局：

如圖 12。

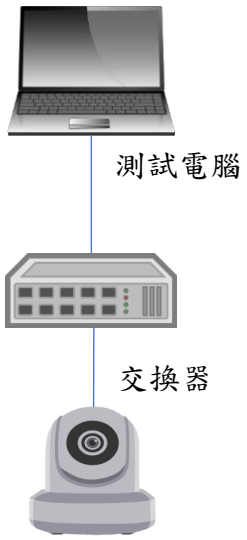

圖 12 測試示意圖

(6) 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. 開啟網路協定介面。
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. 開啟網路協定介面。
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。

(7) 測試結果：

(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：產品不支援網路協定介面。

(d) 測試結果：

(1) 通過：(a)~(c)三項結果皆符合。

(2) 不通過：(a)~(c)三項結果不符合其一。

(3) 不適用：(a)~(c)三項介面產品皆不支援。

5.2 已知漏洞安全測試

檢視產品有關已知漏洞安全部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.2.1 作業系統與網路服務測試

5.2.1.1 測試作業系統與網路服務不存在 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：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.1.1

(b) 測試資料：

(1) 產品 IP 位址。

(2) 產品所提供之系統管理者帳密。

(3) 廠商應提供產品所使用之作業系統與網路服務及所使用第三方套件之說明。

(c) 測試目的：

查驗產品之作業系統與網路服務不存在已知 CVSS v3 高資安風險之漏洞。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應支援作業系統與網路服務。

(3) 產品應提供系統管理者帳密。

(e) 測試佈局：

如圖 13。

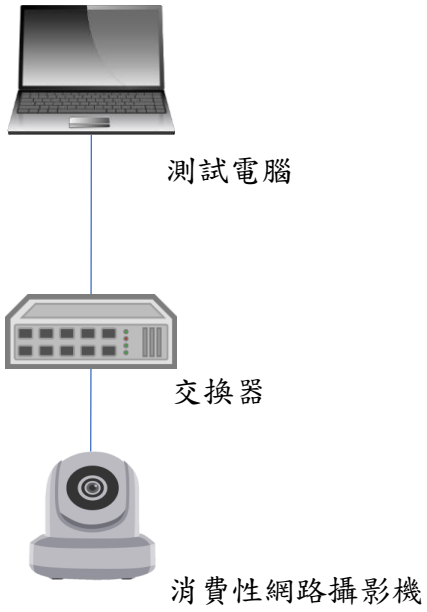

圖 13 測試示意圖

(f) 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。

(5) 根據廠商提供之說明驗證結果。

(g) 測試結果：

(1) 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。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.2 網路服務連接埠測試

5.2.2.1 網路服務最小化測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.2.1

(b) 測試資料：

產品之 IP 位址。

(c) 測試目的：

驗證產品是否存在預期以外之網路埠。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供所啟用之網路服務與對應埠之宣告。

(e) 測試佈局：

如圖 14。

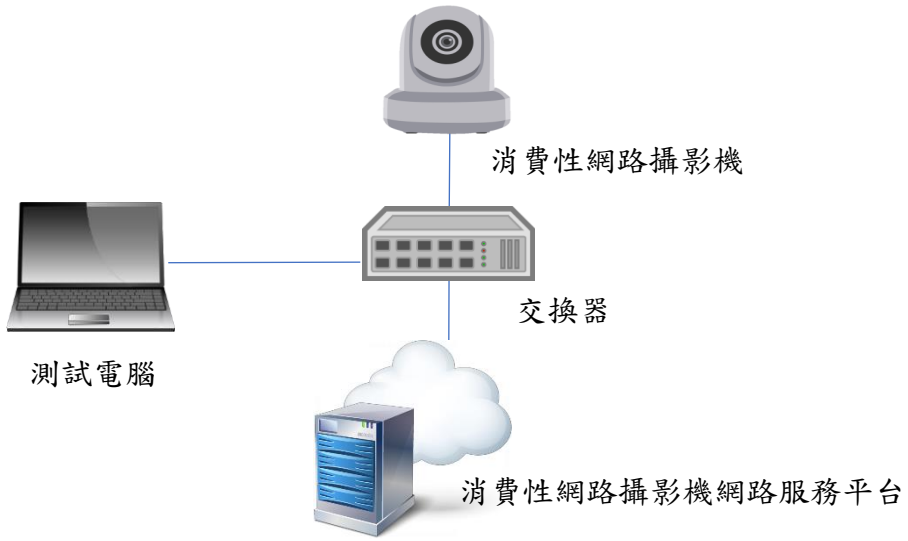

圖 14 測試示意圖

(f) 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。

(g) 測試結果：

(1) 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) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無網路服務之功能。

5.2.3 資訊安全管理測試

5.2.3.1 隱私政策宣告測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.3.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否具有隱私政策宣告。

(d) 測試條件：

(1) 廠商應提供隱私政策文件。

(2) 產品應提供隱私政策之連結。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供隱私政策文件。

(2) 驗證產品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，應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。

(g) 測試結果：

(1) 隱私政策之內容應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) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.3.2 安全開發驗證測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.3.2

(b) 測試資料：

無。

(c) 測試目的：

查驗產品開發流程是否符合安全開發要求。

(d) 測試條件：

廠商應提供相關說明文件(見附錄 C 所述)作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱具備此功能證明之書面資料。

(g) 測試結果：

(1) 書面資料證實產品符合安全開發之規定。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.3.3 安全指南測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.3.3

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否具有產品設置安全指南。

(d) 測試條件：

廠商應提供產品設置安全指南之使用手冊或網頁連結作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱產品設置安全指南之使用手冊或網頁連結。

(2) 使用手冊應含安全指南說明，包括但不限於：

(i) 產品安全功能的涵蓋範圍。

(ii) 設置安全的使用環境（網路安全設定）。

(iii) 安全功能的設置（安裝、身分驗證、授權、加密、更新等）。

(iv) 刪除儲存於產品的資料或檔案。

(v) 警示與通知。

(g) 測試結果：

(1) 產品設置使用手冊應包括安全指南說明。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.3.4 產品標示測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.2.3.4

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否載明產品型號或產品名稱於設備外觀。

(d) 測試條件：

廠商應提供產品出廠之完整包裝作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

檢查產品實體外觀與包裝。

(g) 測試結果：

(1) 產品實體外觀印有產品型號或名稱。

(2) 產品備有型號或名稱之標籤，以供消費者自行黏貼。

(3) 通過：(1)、(2)項結果符合其一。

(4) 不通過：(1)、(2)項結果皆不符合。

(5) 不適用：無。

5.3 軟韌體更新測試

檢視產品有關軟韌體更新部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 更新安全測試

5.3.1.1 備援更新功能測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.3.1.1

(b) 測試資料：

無。

(c) 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。

(d) 測試條件：

(1) 產品應支援更新功能，包括但不限於線上更新或手動更新方式。

(2) 支援線上更新：廠商應負責觸發線上更新。

(e) 測試佈局：

如圖 15。

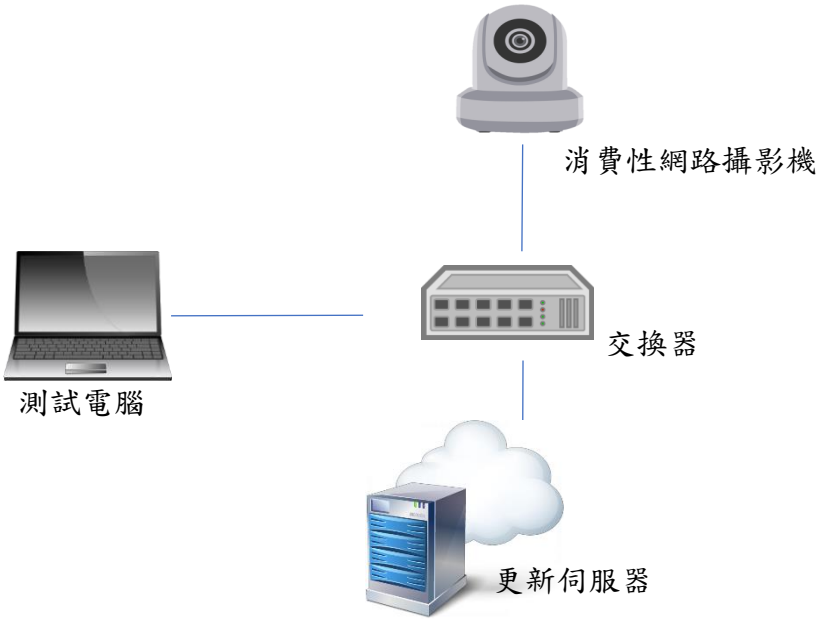

圖 15 測試示意圖

(f) 測試方法：

(1) 啟動更新。

(2) 於更新過程中(非韌體檔案下載階段)，觸發更新中斷。

(g) 測試結果：

(1) 支援更新功能。

(2) 更新中斷後，系統仍可回復正常運作狀態。

(3) 產品更新過程會自動關機執行者，應於更新開始前提示消費者。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：無。

5.3.1.2 韌體更新路徑的保護

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.3.1.2

(b) 測試資料：

測試用假憑證。

(c) 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。

(d) 測試條件：

(1) 產品應支援線上更新。

(2) 產品應提供所有相連更新伺服器之宣告。

(3) 受測廠商應協助觸發產品之線上更新。

(e) 測試佈局：

如圖 16。

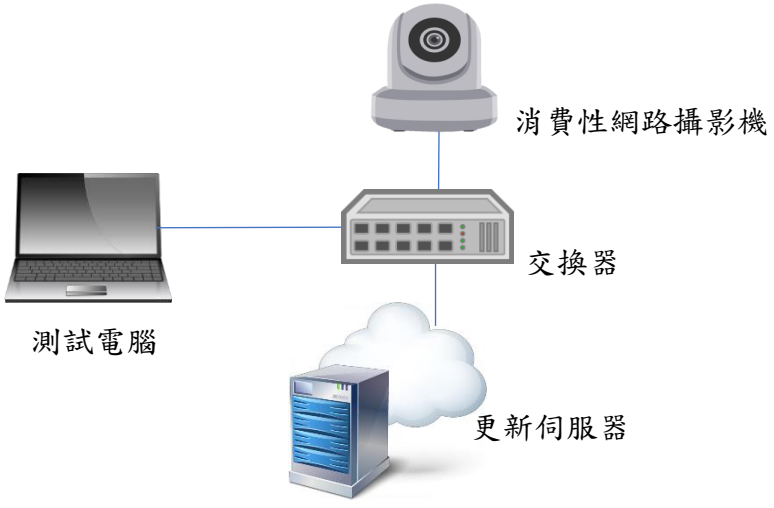

圖 16 測試示意圖

(f) 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。

(g) 測試結果：

(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：產品不支援線上更新功能。

5.3.1.3 更新通知測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.3.1.3

(b) 測試資料：

無。

(c) 測試目的：

驗證產品具有更新訊息提醒消費者進行軟韌體更新。

(d) 測試條件：

(1) 產品應支援更新功能，包括但不限於線上更新或手動更新方式。

(2) 支援線上更新：廠商應提供較現有產品版本更新之版本，且負責觸發線上更新。

(e) 測試佈局：

如圖 17。

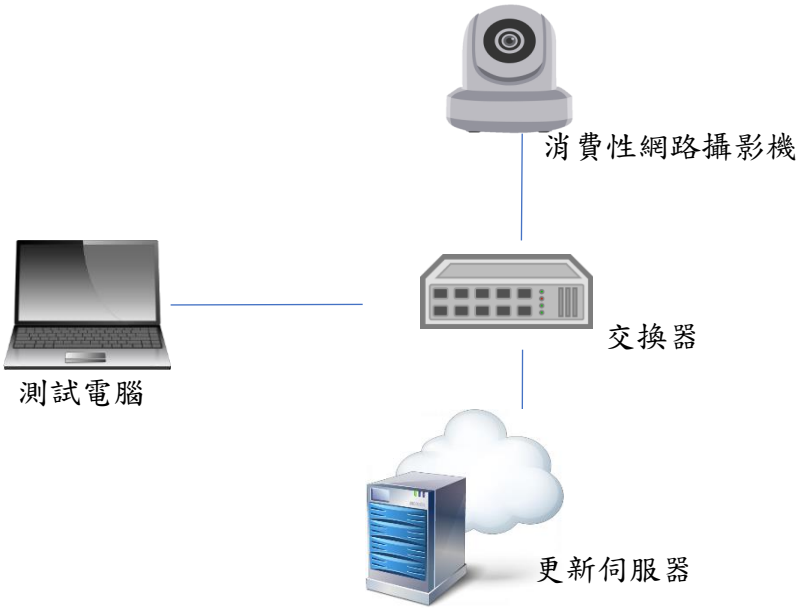

圖 17 測試示意圖

(f) 測試方法：

檢查產品管理介面之產品韌體版本顯示狀態。

(g) 測試結果：

(1) 產品管理介面應顯示韌體版本資訊及顯示有可用更新。

(2) 廠商應於產品官網上發佈韌體更新資訊與說明。

(3) 通過：(1)、(2)項結果符合其一。

(4) 不通過：(1)、(2)項結果皆不符合。

(5) 不適用：無。

5.3.1.4 支援更新期限測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.3.1.4

(b) 測試資料：

無。

(c) 測試目的：

查驗產品具有韌體更新期限之說明宣告。

(d) 測試條件：

(1) 產品應支援更新功能。

(2) 廠商應提供支援更新期限之宣告作為審查依據，包括但不限於使用手冊、網頁等發布方式。

(e) 測試佈局：

無。

(f) 測試方法：

查驗廠商所提供之產品宣告文件或網頁連結。

(g) 測試結果：

(1) 產品於支援宣告更新期限

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4 資料機密性與完整性測試

檢視產品有關資料機密性與完整性部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.4.1 安全敏感性資料儲存測試

5.4.1.1 韌體安全測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.4.1.1

(b) 測試資料：

產品之韌體檔案。

(c) 測試目的：

查驗產品之韌體不存在明文或可被解密回復之安全敏感性資料。

(d) 測試條件：

(1) 應提供產品之韌體燒錄工具與方法。

(2) 產品應提供所使用之加密演算法書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 檢視受測廠商之官網是否存在產品韌體可供下載。

(2) 若廠商之官網不存在產品韌體，則執行以下步驟。

(3) 審閱可證明所使用加密演算法之書面資料。

(4) 若燒錄接腳存在，使用廠商提供之工具，嘗試進行韌體萃取。

(5) 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；若韌體不可萃取，由廠商提供產品之韌體。

(6) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(7) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(8) 確認系統通行碼資料的保密機制是否採用 NIST SP 800-140C[(1)]所核可同等或以上強度之雜湊函數。

(9) 確認金鑰是否可被擷取。

(10) 確認是否存在非公開之 email 資料。

(11) 確認是否存在產品所宣告之相連伺服器外之 IP 資料。

(12) 確認是否存在產品所宣告之相連伺服器外之 URL 資料。

(g) 測試結果：

(1) 韌體檔案不應置於公開存取之位置。

(2) 韌體應加密保護且採用 NIST SP 800-140C[(1)]所核可同等或以上強度之加密演算法。

(3) 韌體無法解析出安全敏感性資料。

(4) 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。

(5) 通過：(1)(2)(4)三項結果皆符合，或(1)(3)(4)結果皆符合。

(6) 不通過：(1)(2)(4)三項結果不符其一，或(1)(3)(4)結果不符合其一。

(7) 不適用：無。

5.4.1.2 安全敏感性資料加密儲存測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.4.1.2

(b) 測試資料：

無。

(c) 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。

(d) 測試條件：

(1) 產品應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) 產品應提供系統管理者權限供測試用。

(3) 產品應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。

(e) 測試佈局：

如圖 18。

圖 18 測試示意圖

(f) 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) 若產品支援網路協定介面，開啟並連接網路協定介面。

(15) 重複(5)~(7)之步驟。

(g) 測試結果：

(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。

5.4.2 傳輸資料保護測試

5.4.2.1 資料之傳輸保護測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.4.2.1

(b) 測試資料：

無。

(c) 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。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供消費性網路攝影機網路服務平台。

(e) 測試佈局：

如圖 19。

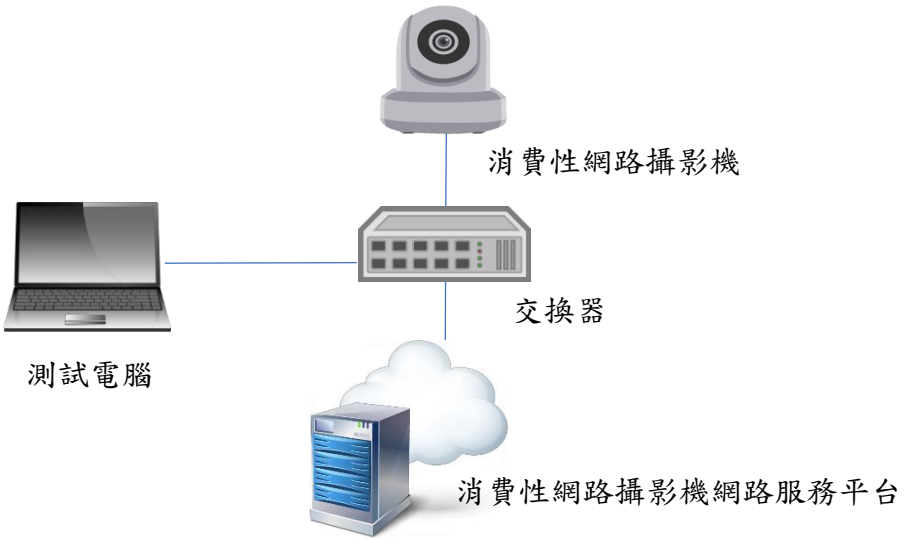

圖 19 測試示意圖

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 將產品與消費性網路攝影機網路服務平台連線，同時側錄封包。

(3) 檢視所側錄之封包是否採用安全通道。

(4) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(g) 測試結果：

(1) 產品與消費性網路攝影機網路服務平台之資料傳輸，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。

5.4.2.2 身分鑑別因子傳輸安全測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.4.2.2

(b) 測試資料：

產品之系統管理者帳密。

(c) 測試目的：

驗證本地端介面之身分鑑別因子於傳輸中是否加密。

(d) 測試條件：

產品應保持出廠預設環境狀態。

產品應提供本地端管理介面。

(e) 測試佈局：

如圖 20。

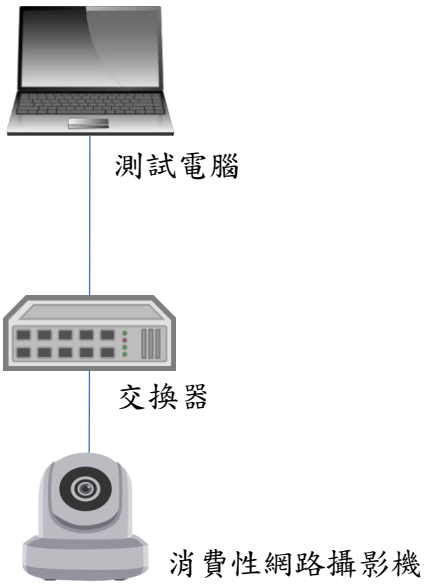

圖 20 測試示意圖

(f) 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) 於相應之本地端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。

(g) 測試結果：

(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：產品不支援本地端管理介面。

5.5 系統完整性測試

檢視產品有關系統完整性部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.5.1 實體入侵防護測試

5.5.1.1 實體介面安全管控測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.5.1.1

(b) 測試資料：

無。

(c) 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。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應於文件中說明進入作業系統除錯模式之方法。

(e) 測試佈局：

如圖 21。

圖 21 測試示意圖

(f) 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。

(g) 測試結果：

(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。

5.5.2 輸入驗證測試

5.5.2.1 輸入驗證功能測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.5.2.1

(b) 測試資料：

無。

(c) 測試目的：

驗證本地端管理介面任何輸入的語法和內容不應對產品功能造成損壞，或存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞。

(d) 測試條件：

產品支援本地端管理介面。

(e) 測試佈局：

如圖 22。

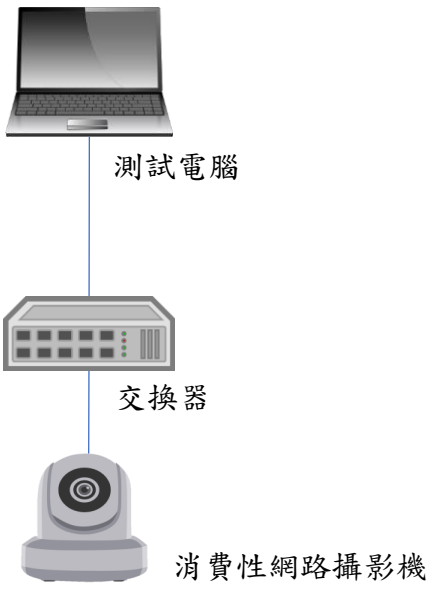

圖 22 測試示意圖

(f) 測試方法：

(1) 將測試電腦與連接產品。

(2) 開啟本地端管理介面。

(3) 進行輸入驗證測試。

(g) 測試結果：

(1) 產品之測試結果不存在國家弱點資料庫評分 CVSS v3 為 7.0 分以上的資安漏洞。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援本地端管理介面。

5.6 資源可用性測試

檢視產品有關資源可用性部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.6.1 資源管理測試

5.6.1.1 備援功能測試

(a) 通訊網路中斷

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.6.1.1

(2) 測試資料：

無。

(3) 測試目的：

驗證當通訊網路異常中斷恢復後，系統能回復正常運作。

(4) 測試條件：

無。

(5) 測試佈局：

無。

(6) 測試方法：

(i) 啟動遠端連線監看功能。

(ii) 於遠端監看過程中，觸發網路連線中斷(例:拔除網路線)。

(iii) 恢復產品網路連線。

(7) 測試結果：

(i) 恢復產品網路連線，遠端監看功能回復正常運作狀態。

(ii) 通過：(1)項結果符合。

(iii) 不通過：(1)項結果不符合。

(iv) 不適用：無。

(b) 電源中斷

(1) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.6.1.1

(2) 測試資料：

無。

(3) 測試目的：

驗證當電源異常中斷恢復後，系統能回復正常運作。

(4) 測試條件：

無。

(5) 測試佈局：

無。

(6) 測試方法：

(i) 啟動遠端連線監看功能。

(ii) 於遠端監看過程中，觸發斷電(例:拔除電源線)。

(iii) 恢復產品供電。

(7) 測試結果：

(i) 恢復產品供電後，遠端監看功能回復正常運作狀態。

(ii) 通過：(1)項結果符合。

(iii) 不通過：(1)項結果不符合。

(iv) 不適用：無。

(c) 測試結果：

(1) 通過：(a)~(b)二項結果皆符合。

(2) 不通過：(a)~(b)二項結果不符合其一。

(3) 不適用：無。

5.7 隱私保護測試

檢視產品有關隱私保護部分之送審資料是否符合IoT-1005-1之安全要求，並依下列各測試項目進行實機測試。

5.7.1 隱私保護能力測試

5.7.1.1 敏感性個人資料收集最小化測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.7.1.1

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否存在收集預期以外的敏感性個人資料，且敏感性個人資料是否可被刪除。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 廠商應提供產品所收集之敏感性個人資料之使用目的與刪除方法之宣告(包括但不限於產品使用手冊、包裝說明、本地端管理介面、網頁等介面)。

(e) 測試佈局：

無。

(f) 測試方法：

審閱敏感性個人資料收集與刪除方法之宣告文件。

(g) 測試結果：

(1) 產品宣告所列之收集項目符合該類產品必要之所需。

(2) 敏感性個人資料收集宣告中有說明敏感性個人資料刪除之方式。

(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。

5.7.1.2 遙測數據收集測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.7.1.2

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否存在預期以外資料之收集，且是否經消費者同意提供第三方利用。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 廠商應提供產品之遙測數據收集與利用宣告作為審查依據(包括但不限於產品使用手冊、包裝說明、本地端管理介面、網頁等介面)。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱遙測數據收集與利用之說明。

(2) 初次啟用產品，檢視各管理介面。

(g) 測試結果：

(1) 遙測數據收集與利用宣告中應詳細說明收集哪些個人資訊、使用目的、提供哪些廠商以外的第三方單位使用。

(2) 管理介面之遙測數據宣告頁面，應提供消費者選擇願意提供與否之選項。

(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。

5.8 警示與紀錄測試

檢視產品有關警示與紀錄部分之送審資料是否符合 IoT-1005-1 之安全要求，並依下列各測試項目進行實機測試。

5.8.1 安全事件警示測試

5.8.1.1 產品安全事件警示功能測試

(a) 測試依據：

「IoT-1005-1 消費性網路攝影機資安標準」5.8.1.1

(b) 測試資料：

無。

(c) 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。

(d) 測試條件：

(1) 產品應支援使用者登錄。

(2) 廠商應提供安全事件警示機制之說明。

(e) 測試佈局：

如圖 23。

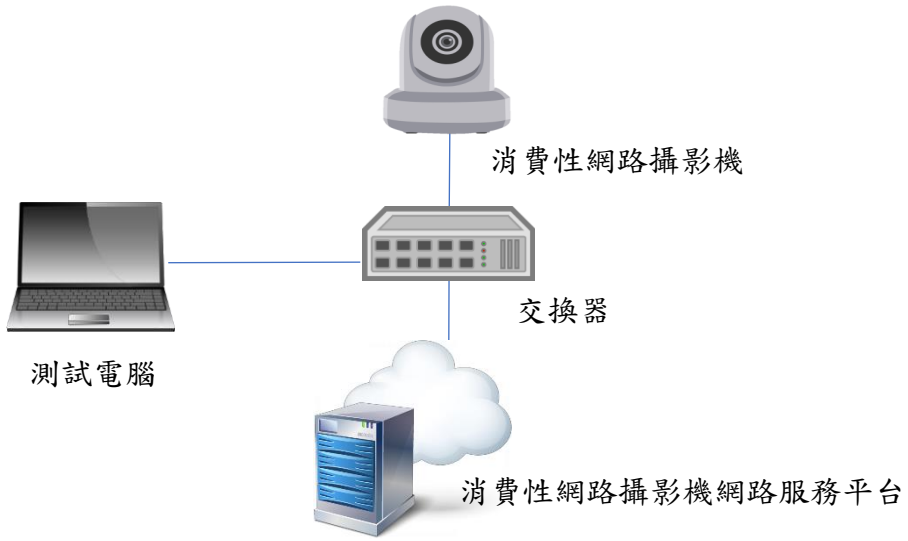

圖 23 測試示意圖

(f) 測試方法：

(1) 觸發產品各種使用者登錄介面(包括: 本地端管理介面、網路協定控制介面、應用程式介面、實體介面)之安全事件。

(2) 根據產品提供之說明文件，檢視警示狀態。

(g) 測試結果：

(1) 產品發生安全事件時，發出推播或告警等警示機制。

(2) 通過：(1)項結果符合。

(3) 不過：(1)項結果不符合。

(4) 不適用：無。

附錄 A
(規定)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
    - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
    - TLS_AES_128_CCM_SHA256
    - TLS_AES_128_CCM_8_SHA256

附錄 B
(參考)
產品概述說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 B.1 設備概述表

製造商	XX 公司
設備名稱	XXX
廠牌	XXX
型號	XX-XXX
韌(軟)體版本	XX.XXX.XX
通訊介面	XXX
網路服務(埠號)	https (443)
網路服務平台(IP)	xx 網路服務平台 (XX.XX.XX.XX)
日誌存取權限	User A : 唯讀
日誌檔保存期限	90 天
角色存取權限	Administrator : User A :
使用者帳密	Admin 帳號 : Admin 密碼 :
外觀	<picture>

附錄 C
(參考)
安全功能規格說明(範例)

送測之產品應提供下表供測試實驗室參閱：

表 C.1 安全功能規格表

項目	說明	申請者填寫內容
1. 除錯模式	詳細描述進入產品除錯模式之方法，或提供佐證文件。	
2. 網路協定	詳細描述產品支援之網路協定，或提供說明文件。	
3. 加密演算法	列出產品所提供之加密演算法及其應用，及提供佐證文件。	
4. 日誌與警示機制	說明安全事件警示機制與警示方式，或提供佐證資料。	
5. 安全通道憑證	驗證 2 級安全項目之產品應提供。	
6. 安全開發證明	出示相關認證證明，或以下文件：符合 SSDLC 各管理程序書面資料，包括: (1)安全管理、(2)風險評估、(3)安全要求、(4)安全開發(含設計、開發、驗證)、(5)安全維運(含監控、弱點管理、事件應變)。	
7. 敏感性個人資料收集	詳細描述收集哪些敏感性個人資料及其使用情境和提供誰利用、機密保護作法與存取/存放位置。	

8. 遙測數據收集	詳細描述收集哪些遙測數據及其使用目的和提供誰利用、個資/隱私資料保護作法與存取/存放位置。	

參考資料

(1) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program