物聯網設備檢測執行方法

行政院國家資通安全會報技術服務中心
中華民國110年6月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	110/6/1	新編
2			
3			

目　次

1. 前言 1
1.1 適用對象 2
1.2 使用建議 2
1.3 章節結構 3
2. 檢測作業流程 5
3. 前置階段 6
3.1 基本資訊蒐集 6
3.2 確認檢測範圍 7
3.3 確認資安檢測項目 7
3.4 編成檢測團隊 8
3.5 通知配合事項 8
3.6 準備檢測工具 9
4. 執行階段 12
4.1 網路印表機檢測 13
4.2 網路攝影機檢測 22
4.3 門禁設備檢測 31
4.4 無線網路基地台/無線路由器檢測 39
4.5 環控系統檢測 50
5. 結案階段 59
5.1 檢測結果 59
5.2 改善建議 62
6. 結論 63
7. 參考文獻 64
8. 附件 65
8.1 附件 1 物聯網設備基本資訊蒐集表範本 65

圖 目 次

圖 1　物聯網設備技術檢測重點 2
圖 2　物聯網設備檢測作業流程 5
圖 3　檢測結果彙整表範例 60

表 目 次

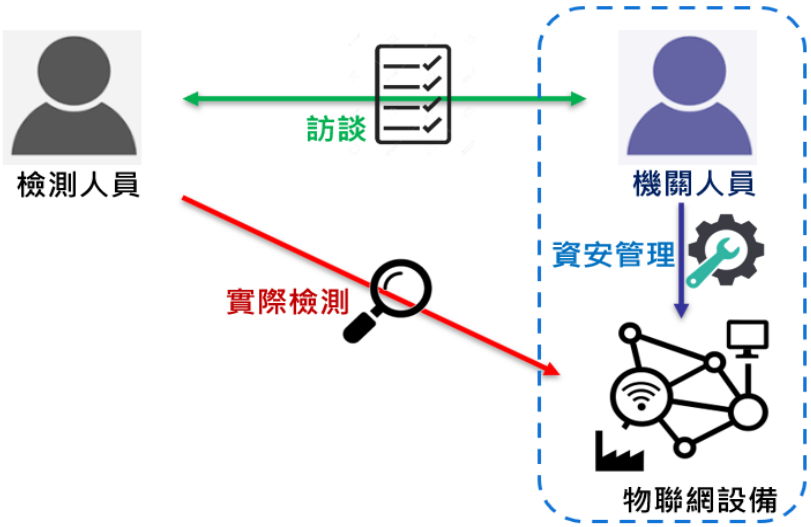
表 1　物聯網設備類型之定義與範例 6
表 2　物聯網設備檢測配合事項 8
表 3　物聯網檢測時參考使用之工具 9
表 4　檢測項目匯總 12
表 5　網路印表機之資安檢測項目 1-1 13
表 6　網路印表機之資安檢測項目 1-2 14
表 7　網路印表機之資安檢測項目 1-3 15
表 8　網路印表機之資安檢測項目 1-4 16
表 9　網路印表機之資安檢測項目 1-5 17
表 10　網路印表機之資安檢測項目 1-6 18
表 11　網路印表機之資安檢測項目 1-7 19
表 12　網路印表機之資安檢測項目 1-8 20
表 13　網路印表機之資安檢測項目 1-9 21
表 14　網路攝影機之資安檢測項目 2-1 22
表 15　網路攝影機之資安檢測項目 2-2 23
表 16　網路攝影機之資安檢測項目 2-3 24
表 17　網路攝影機之資安檢測項目 2-4 25
表 18　網路攝影機之資安檢測項目 2-5 26
表 19　網路攝影機之資安檢測項目 2-6 27
表 20　網路攝影機之資安檢測項目 2-7 28
表 21　網路攝影機之資安檢測項目 2-8 29
表 22　網路攝影機之資安檢測項目 2-9 30
表 23　門禁設備之資安檢測項目 3-1 31
表 24　門禁設備之資安檢測項目 3-2 32
表 25　門禁設備之資安檢測項目 3-3 33
表 26　門禁設備之資安檢測項目 3-4 34
表 27　門禁設備之資安檢測項目 3-5 34
表 28　門禁設備之資安檢測項目 3-6 35
表 29　門禁設備之資安檢測項目 3-7 36
表 30　門禁設備之資安檢測項目 3-8 38
表 31　門禁設備之資安檢測項目 3-9 39

表 32　無線網路基地台/無線路由器之資安檢測項目 4-1 40
表 33　無線網路基地台/無線路由器之資安檢測項目 4-2 41
表 34　無線網路基地台/無線路由器之資安檢測項目 4-3 41
表 35　無線網路基地台/無線路由器之資安檢測項目 4-4 42
表 36　無線網路基地台/無線路由器之資安檢測項目 4-5 43
表 37　無線網路基地台/無線路由器之資安檢測項目 4-6 44
表 38　無線網路基地台/無線路由器之資安檢測項目 4-7 45
表 39　無線網路基地台/無線路由器之資安檢測項目 4-8 46
表 40　無線網路基地台/無線路由器之資安檢測項目 4-9 48
表 41　通行碼演算法 48
表 42　無線網路基地台/無線路由器之資安檢測項目 4-10 49
表 43　環控系統之資安檢測項目 5-1 50
表 44　環控系統之資安檢測項目 5-2 51
表 45　環控系統之資安檢測項目 5-3 52
表 46　環控系統之資安檢測項目 5-4 53
表 47　環控系統之資安檢測項目 5-5 54
表 48　環控系統之資安檢測項目 5-6 54
表 49　環控系統之資安檢測項目 5-7 55
表 50　環控系統之資安檢測項目 5-8 57
表 51　環控系統之資安檢測項目 5-9 58
表 52　物聯網設備檢測結果彙整表範本 59
表 53　物聯網設備檢測評分表範本 61
表 54　物聯網設備檢測配分計算方式 61

1. 前言

物聯網(Internet of Things)之廣泛應用，不論是在辦公環境、金融交易、交通運輸或醫療保健等，已進入百家爭鳴時代。物聯網之興起，帶給人們許多便利與縮短了彼此距離，同時為追求連網便利或發展應用服務之商機，以往封閉系統與環境也紛紛加入物聯網之懷抱。然而在物聯網快速發展與設備安全性不足情況下，提供惡意人士更多元之入侵管道，造成層出不窮之資安事件，由於物聯網設備無所不在且已運用於日常生活中，一旦被入侵，所造成之影響規模將相當龐大，甚至直接影響政府機關之運作與民眾基本生活[1]。

為增進物聯網安全，執行物聯網資安檢測實為必要，常見物聯網設備資安檢測類型，包含源碼檢測、弱點掃描及滲透測試等，除源碼檢測為白箱測試外，其餘皆為黑箱或灰箱測試，此外物聯網設備資安檢測亦可從實體安全面向切入，針對設備進行韌體拆解與逆向工程等系統安全檢測，惟源碼檢測及實體安全檢測較不適用於一般政府機關環境。本文件中所提之物聯網設備檢測係以「檢測機關使用中之物聯網設備其資安管理落實程度與設備弱點」為檢測重點(詳見圖 1)，其非以檢測數量眾多且繁雜與之物聯網設備檢測標準為主體，而在於提供政府機關必要之基本檢測項目，以讓政府機關人員能具備基本且重要之資安檢測知識與技術以自行依循操作，或掌握委外檢測之要求重點。



資料來源：本中心整理

圖1　物聯網設備技術檢測重點

本文件藉由說明物聯網設備檢測流程，並詳述包含「網路印表機檢測」、「網路攝影機檢測」、「門禁設備檢測」、「無線網路基地台/無線路由器檢測」及「環控系統檢測」等 5 項檢測項目執行方式，以及提醒結果報告撰寫重點，做為政府機關自我檢測或第三方檢測之參考，以協助政府機關提升物聯網設備防護能力。

1.1 適用對象

本文件適用於政府機關(構)資訊人員執行機關自我檢測或第三方檢測之參考。

1.2 使用建議

本文件主要針對物聯網設備檢測各階段作業重點進行說明，提供執行設備檢測之參考，進而掌握各檢測項目與執行上需考量重點，以及執行作業中應留下之紀錄重點。建議先閱讀技術檢測流程，掌握整體執行工作與重點，再接續了解各階段細部工作內容與檢測步驟，以確保可如期如質完成

檢測作業。

1.3 章節結構

本文件共分為「前言」、「檢測作業流程」、「前置階段」、「執行階段」、「結案階段」、「結論」、「參考文獻」及「附件」等 7 個章節，各章節架構與工作項目說明如下：

- 第 1 章：前言

  說明目的、適用對象、使用建議及章節架構，以對檢測重點與本文件架構有全盤性認知。

- 第 2 章：檢測作業流程

  說明物聯網設備檢測前置階段、執行階段及結案階段等各階段之整體流程。

- 第 3 章：前置階段

  說明檢測前需準備之項目，包含基本資訊蒐集、檢測範圍與項目確認、團隊編成、檢測工具及雙方配合事項等。

- 第 4 章：執行階段

  說明「網路印表機檢測」、「網路攝影機檢測」、「門徑設備檢測」、「無線網路基地台/無線路由器檢測」及「環控系統檢測」等 5 項之執行重點。

- 第 5 章：結案階段

  說明結果報告中各檢測項目應撰寫之重點。

- 第 6 章：結論

說明結論與效益。

- 第 7 章：參考文獻

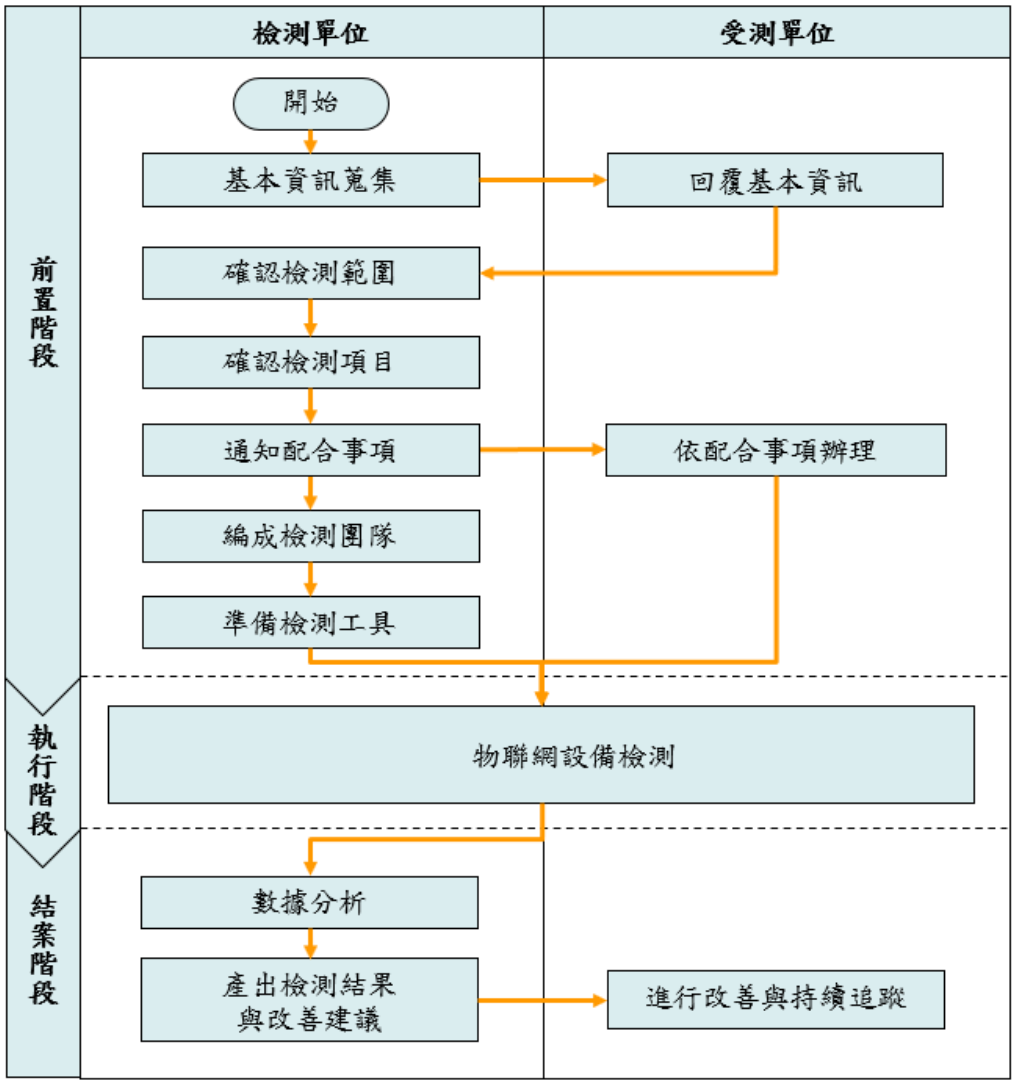
  說明本文件所參考之文獻資料。

- 第 8 章：附件

  提供物聯網設備檢測所需之基本資訊蒐集表範本。

2. 檢測作業流程

物聯網設備檢測作業流程分為「前置階段」、「執行階段」及「結案階段」等 3 個階段，各階段作業內容詳見圖 2，依據此執行流程對受測物聯網設備進行資料蒐集與資訊分析，接續執行檢測作業，最後進行數據分析與產出檢測結果，並提供相關改善建議。



資料來源：本中心整理

圖2　物聯網設備檢測作業流程

3. 前置階段

物聯網設備檢測執行前須調查受測單位基本資訊，以確認檢測範圍、規劃資安檢測項目、編成檢測團隊及準備檢測工具。此外，受測單位亦須依檢測配合事項，備妥檢測所需環境，俾利後續檢測作業執行。

3.1 基本資訊蒐集

為了解受測單位現行之物聯網設備資訊，受測單位需確認符合檢測範圍之物聯網設備，建議於檢測前完成受測單位之物聯網設備基本資訊蒐集，如網址(內部 IP)、廠牌型號、作業系統及放置位置等，以利評估檢測範圍。物聯網設備類型之定義與範例詳見表 1，基本資訊蒐集表範本詳見附件 1。

表1　物聯網設備類型之定義與範例

項次	物聯網設備類型	設備名詞定義說明	範例
1	網路印表機	▪可使用 RJ45 進行控制之相關設備、後端管控平台及伺服器主機 ▪提供紙張列印輸出功能	網路印表機、多功能事務機、影印機等
2	網路攝影機	▪可使用 RJ45 進行控制之相關設備、後端管控平台及伺服器主機 ▪提供影像錄製或影像顯示/儲存功能	網路攝影機、網路影像錄影機(NVR)、影像管理主機等
3	門禁設備	▪可使用 RJ45 進行控制之相關設備、後端管控平台及伺服器主機 ▪提供門禁開關或設定功能	指紋機、門禁卡機等、門禁管理伺服器等
4	無線網路基地台/無線路由器	▪可使用 RJ45 進行控制之相關設備、後端管控平台及伺服器主機 ▪提供無線網路分享或控制功能	無線網路基地台、無線路由器、無線區域

項次	物聯網設備類型	設備名詞定義說明	範例
			網路控制器、Thin AP 等
	環控系統	▪可使用 RJ45 進行控制之相關設備、後端管控平台及伺服器主機 ▪提供監控機房溫度或溫度功能	▪智慧溫度計、智慧溼度計、環控設備及環控主機等

資料來源：本中心整理

3.2 確認檢測範圍

本文件所述之物聯網設備檢測標的為可直接使用 RJ45 進行連線之相關設備、後端管控平台及伺服器主機，並提供列印、門禁開關、攝影、無線網路分享、監控機房溫度或濕度等功能，包含但不僅限於網路印表機、網路攝影機、網路影像錄影機(NVR)、影像管理主機、指紋機、門禁卡機、門禁管理伺服器、無線網路基地台、無線路由器、無線區域網路控制器、Thin AP、智慧溫度計、智慧溼度計、環控系統及環控主機等，當收到受測單位回覆之調查表後，除依此原則完成檢測範圍確認外，亦可考量檢測時程與人力決定受測設備數量，當受測設備數量有限之情況下，應儘量檢測不同廠牌與不同型號之設備，以增進發掘所管理之各項物聯網設備潛在資安風險機會。

3.3 確認資安檢測項目

依據擬定之檢測範圍與數量進行資安檢測項目確認，原則上「網路印表機」、「網路攝影機」、「門禁設備」、「無線網路基地台/無線路由器」及「環控系統」等 5 類物聯網設備，各類設備建議應至少檢測 1 組，並依 5 類設備之 10 項安全基準為資安檢測項目，若非 5 類設備都具備時，則以

擁有之設備類型之 10 項安全基準為資安檢測項目，例如僅具備網路印表機與網路攝影機等 2 類物聯網設備，則以網路印表機與網路攝影機對應之安全基準為資安檢測項目。

3.4 編成檢測團隊

為確保檢測作業可如期順利完成，依照各資安檢測項目之需求進行任務編組，考量物聯網設備檢測屬性，建議由具備系統滲透測試能力與經驗之人員編成物聯網設備檢測團隊，負責執行技術資安檢測項目，並指派 1 位統籌與管理執行進度。

3.5 通知配合事項

檢測範圍與項目確認後，可針對資安檢測項目配合事項通知受測單位預先準備，針對檢測 IP、系統測試帳號及通行碼組數，則視檢測人力需求進行申請，物聯網設備檢測之配合事項列表詳見表 2。

表2　物聯網設備檢測配合事項

檢測項目	配合事項說明
物聯網設備檢測	▪請受測單位提供可連線至受測物聯網設備之檢測 IP，或於各設備網段提供檢測 IP ▪請確認檢測 IP 可連線至物聯網設備，檢測 IP 未受網路設備阻擋(如防火牆或 WAF 等) ▪受測設備如有白名單機制，請將檢測 IP 加入白名單 ▪各設備之相關管理者配合訪談與實際檢測作業，並備妥設備管理者帳號，於檢測執行期間協助相關問題，並視檢測情形提供予檢測人員 ▪為避免檢測過程發生預期外情況，導致設備發生當機或資料毀損情況，在執行前應備份設備相關資料

檢測項目	配合事項說明
	▪ 各設備之相關管理者備妥設備管理者帳號，於檢測過程協助相關問題，並針對受測設備提供 2 組設備一般使用者帳號

資料來源：本中心整理

3.6 準備檢測工具

執行物聯網設備檢測前，檢測人員可依「資訊蒐集」、「弱點掃描」、「弱點利用」及「權限跳脫與提升」等 4 個類別，準備相對應之檢測工具，常用工具詳見表 3。

表3　物聯網檢測時參考使用之工具

項次	類別	參考工具	簡介
1	資訊蒐集	Nessus	一款系統弱點掃描與分析工具，可針對系統或物聯網設備進行弱點掃描，產出風險報告等資訊，供檢測人員進一步分析與利用
2		Nmap	此為應用於網路發現與安全稽核之開放原始碼工具，主要利用發送 IP 封包方式來確認與列舉網路上主機，辨識主機提供之服務(應用程式名稱與版本)、主機作業系統及版本等資訊，並提供規避防火牆/IDS 與使用相關腳本(NSE)進行弱點掃描等功能
3		Binwalk	一款文件分析工具，旨在協助研究人員對文件進行分析、提取及逆向工程。在物聯網之檢測中，可用於分析目標裝置韌體封裝格式，以使用對應之工具進行反解
4		Wireshark	一套開放原始碼之網路封包分析軟體，用於擷取網路封包內容與分析封包摘要與詳細資訊

項次	類別	參考工具	簡介
5		Burp Suite	該工具用於檢視與攔截物聯網網站或行動軟體之網路行為，並可依據檢測需求，修改其網路請求內容
6		DIRB	該工具可用來執行目錄掃描，並藉由字典檔或暴力破解等方式尋找網站後台路徑
7		SQLite database browse	該工具為處理 SQLite3 資料庫文件之應用軟體，能夠打開 SQLite3 資料庫文件，用以檢視由 Android 模擬器或裝置所提取之資料庫文件
8		Metasploit	應用於開發、測試及漏洞利用之開放原始碼平台，該平台提供數千個資訊蒐集、漏洞利用及後滲透模組等，研究人員也可自行撰寫模組放置於 Metasploit 使用，執行攻擊時僅需依照模組所需資訊填入便可執行攻擊
9	弱點掃描	Web Application Attack and Audit Framework (W3AF)	該工具為網站弱點掃描軟體，透過該工具可快速找出網站弱點位置(如 Command Injection、CSRF、XSS 及 SQLi 等)並加以利用
10		Burp Suite	同項次 5
11		Metasploit	同項次 8
12	弱點利用	Burp Suite	同項次 5
13		THC-Hydra	一款暴力破解工具，可對多種類型系統，如 cisco、ftp、http[s]、ldap2[s]、mssql、mysql 及 oracle-listener 等進行帳號與通行碼猜測
14		Unshadow	該工具可合併/etc/passwd 與/etc/shadow 資訊，並創建 1 個含有使用者名稱與密碼詳細資訊之文件

項次	類別	參考工具	簡介
15		John the Ripper	該工具用於密碼分析與破解，在不知道密鑰之情況下，可針對多種加密協定訊息進行解密
16		Aircrack-ng	此為一款與 802.11 標準之無線網路分析有關之安全軟體，可用於支援監聽模式之無線網卡上，執行包含網路偵測、封包探測、WEP 與 WPA/WPA2-PSK 破解等功能
17		Hping3	一款用來製作封包之工具，可以生成 ICMP、UDP 及 SYN 等封包來測試網路之功能。除此之外該工具可利用偽造 IP 位址與設定封包送出頻率等方式達到執行阻斷服務攻擊(DoS)目的
18		SQLMap	該工具可用來測試 SQLi 漏洞，並利用此漏洞取得資料庫敏感資料
19		Metasploit	同項次 8
20	權限跳脫與提升	Metasploit	同項次 8

資料來源：本中心整理

4. 執行階段

物聯網設備檢測執行階段將依前置階段所擬定之檢測範圍與任務編組，於檢測時程內，依各資安檢測項目之執行方法展開檢測作業，並產出相關檢測紀錄。各類設備資安檢測項目詳見表 4。

表4　檢測項目匯總

項次	檢測項目	網路印表機	網路攝影機	門禁設備	無線網路基地台/路由器	環控系統
1	管理介面存取須具備並啟用身分鑑別功能	√	√	√	√	√
2	管理介面通行碼具備並啟用複雜度要求	√	√	√	√	√
3	管理介面通行碼須具備並啟用最小長度限制	√	√	√	√	√
4	管理介面須具備並啟用限制錯誤嘗試的機制	√	√	√	√	√
5	管理介面身分鑑別不得使用預設帳號通行碼	√	√	√	√	√
6	資料存取須進行權限控管，並以最小權限為原則	√	√	√	√	√
7	軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞	√	√	√	√	√
8	所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為	√	√	√	√	√
9	須具備並啟用日誌管理功能	√	√	√	√	√
10	若設備具 WPS 功能則須關閉	NA	NA	NA	√	NA

資料來源：本中心整理

檢測時注意事項如下：

- 檢測前需再次確認本次受測設備標的，並可透過內網 IP、無線網路或臨機操作方式，在無防護設備(如防火牆或 WAF 等)阻擋下進行檢測。
- 建議先針對受測設備進行相關資訊蒐集，透過自動化檢測工具掃描時，需注意物聯網設備運算能力是否能夠負荷，避免影響業務正常運作。
- 執行具侵入性質之檢測作業皆需與受測單位進行確認，並於雙方議定之適當時間且具備適當應變措施與風險評估後，始進行相關檢測作業。
- 檢測過程應留存相關檢測紀錄，並詳細記錄針對設備所做之變更，以便於檢測結束後請受測單位協助進行復原。

4.1 網路印表機檢測

- 資安檢測項目 1-1：網路印表機管理介面存取須具備並啟用身分鑑別功能

  與管理人員透過訪談或手動檢測方式，驗證網路印表機所有服務介面之身分鑑別功能，包含使用者、遠端、本地端、無線網路或實體設備端之介面，皆需經身分鑑別過程方可存取設備內非公開資源，檢測執行步驟詳見表 5。

表5　網路印表機之資安檢測項目 1-1

資安檢測項目 1-1	網路印表機管理介面存取須具備並啟用身分鑑別功能
檢測工具	弱點掃描工具：Nessus、Nmap
檢測執行步驟	▪ 步驟 1

資安檢測項目 1-1	網路印表機管理介面存取須具備並啟用身分鑑別功能
	透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋管理介面相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，確認網路印表機管理介面存取須具備並啟用身分鑑別功能

資料來源：本中心整理

●資安檢測項目 1-2：網路印表機管理介面通行碼具備並啟用複雜度要求

與管理人員透過訪談或手動檢測方式驗證通行碼之複雜度，檢視通行碼是否包含下列 4 種字元中之 3 種，檢測執行步驟詳見表 6。

– 英文大寫字元(A 到 Z)。

– 英文小寫字元(a 到 z)。

– 10 進位數字(0 到 9)。

– 特殊符號(例如：!、$、#、%)。

表6　網路印表機之資安檢測項目 1-2

資安檢測項目 1-2	網路印表機管理介面通行碼具備並啟用複雜度要求
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2

資安檢測項目 1-2	網路印表機管理介面通行碼具備並啟用複雜度要求
	透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題或請設備管理人員協助登入系統，由檢測人員確認是否有開啟通行碼複雜度原則之設定

資料來源：本中心整理

●資安檢測項目 1-3：網路印表機管理介面通行碼須具備並啟用最小長度限制

與管理人員透過訪談或手動檢測方式驗證通行碼之最小長度限制，檢視通行碼最小長度是否為 8 個字元以上，檢測執行步驟詳見表 7。

表7　網路印表機之資安檢測項目 1-3

資安檢測項目 1-3	網路印表機管理介面通行碼須具備並啟用最小長度限制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題，或請設備管理人員協助登入系統，由檢測人員確認是否有開啟通行碼最小長度之設定

資安檢測項目 1-3	網路印表機管理介面通行碼須具備並啟用最小長度限制

資料來源：本中心整理

●資安檢測項目 1-4：網路印表機管理介面須具備並啟用限制錯誤嘗試之機制

與管理人員透過訪談或手動檢測方式檢視帳號通行碼之輸入錯誤次數與頻率，並在達到特定輸入次數或頻率時，進行裝置或使用者名稱之鎖定，各端點規範如下，檢測執行步驟詳見表 8。

– 裝置端：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 通訊(端)網路：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 控制端：5 次連續不成功身分鑑別過程，須使連線失效或進行 15 分鐘之鎖定。

表8　網路印表機之資安檢測項目 1-4

資安檢測項目 1-4	網路印表機管理介面須具備並啟用限制錯誤嘗試之機制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2

資安檢測項目 1-4	網路印表機管理介面須具備並啟用限制錯誤嘗試之機制
	透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有弱通行碼問題 ▪ 步驟 3 確認手動輸入通行碼或使用工具暴力破解後，系統是否會出現帳號鎖住或是測試 IP 被鎖住之訊息

資料來源：本中心整理

●資安檢測項目 1-5：網路印表機管理介面身分鑑別不得使用預設帳號通行碼

與管理人員透過訪談或手動檢測方式驗證印表機是否仍能以預設帳號通行碼成功登入。檢測執行步驟詳見表 9。

表9　網路印表機之資安檢測項目 1-5

資安檢測項目 1-5	網路印表機管理介面身分鑑別不得使用預設帳號通行碼
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼進行登入，確認是否已變更預設帳號通行碼

資安檢測項目 1-5	網路印表機管理介面身分鑑別不得使用預設帳號通行碼

資料來源：本中心整理

●資安檢測項目 1-6：網路印表機資料存取須進行權限控管，並以最小權限為原則

與管理人員透過訪談方式驗證印表機之資料存取是否經權限控管，並必須存在至少 2 種角色，包含具有較高權限之角色(如 Administrator 或 System)與一般僅支援最低權限之角色(如 user)。此外，須對可以被身分鑑別之每一個授權角色或用戶，執行最小權限原則，檢測執行步驟詳見表 10。

表10 網路印表機之資安檢測項目 1-6

資安檢測項目 1-6	網路印表機資料存取須進行權限控管，並以最小權限為原則
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認是否有進行權限管控 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認權限相關設定

資料來源：本中心整理

●資安檢測項目 1-7：網路印表機之軟/韌體、作業系統及相關應用程式須不能存在 CVSS v3 高於 7 分(含)之 CVE 漏洞

透過實際檢測方式，針對設備體/韌體、作業系統及相關應用程式進行檢測，須不能存在已揭露之 OWASP TOP 10、CVE、NVD 或 CVSS 評分為 7 以上之資安漏洞，且原始碼掃描須不能存在 CWE/SANS on the cusp list 或 CWE/SANS TOP 25 最危險之程式設計錯誤。

為協助檢視物聯網「系統安全」之「弱點測試」，特針對「軟/韌體、作業系統及相關應用程式應保持更新，不得存在已揭露漏洞」資安檢測項目訂定相關作業程序，檢測範圍包含「網站與系統服務」、「行動軟體 APP」及「傳輸服務」，執行步驟詳見表 11。

表11 網路印表機之資安檢測項目 1-7

資安檢測項目 1-7	網路印表機之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、PRET、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或受測標的型號搜尋弱點資訊 ▪ 步驟 2 確認受測標的系統或服務之版本是否存在已揭露漏洞，並嘗試進行弱點驗證與利用

資料來源：本中心整理

●資安檢測項目 1-8：網路印表機所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現如下之非預期異常行為：

– 產品設定重新初始化。

– 在測試結束後 2 分鐘內，程式中斷或強制失敗且無法回復至前一狀態。

– 程式凍結或停止回應。

– 測試所使用之資源在測試後仍被綁定。

– 軟體顯示無法處理之例外。

– 儲存資料毀壞。

– 產品對異常輸入測試失去連線。

– 針對特定行為所造成產品中斷運行，沒有在製造商所指定時間內恢復運行。

– 產品在任何介面下揭露任何個人資料或敏感資料，包含所有遠端介面、本地端介面、無線介面、外部檔案輸入接口及所有通訊協定等。

– 產品在輸入測試以外之外部介面，無法正常運作或回應。

檢測執行步驟詳見表 12。

表12 網路印表機之資安檢測項目 1-8

資安檢測項目 1-8	網路印表機所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、PRET、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 瀏覽目標網站，並於登入前與登入後，嘗試在參數內容輸入功能意料外之字串(如 SQL 語法、Script 語法及 XML 語法等)

資安檢測項目 1-8	網路印表機所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
	▪ 步驟 2 確認產品正常運作，且不應顯示非預期之異常行為

資料來源：本中心整理

●資安檢測項目 1-9：網路印表機須具備並啟用日誌管理功能

與管理人員透過訪談或手動執行檢測方式，檢視設備如具備此功能是否被啟用。記錄設備所發生之重要事件，並儲存於非快閃記憶體中，包含時間、使用者身分及操作行為，如成功或不成功之登入嘗試、修改身分鑑別資訊、修改使用者帳號、成功或不成功之軟體更新及相關警示或通知內容。此外若日誌紀錄檔無法正常儲存時，須發出警示或通知。

此外須將安全紀錄檔儲存於非快閃記憶體中，直到檔案儲存至外部磁碟，並且不允許非授權之使用者移除或修改。日誌檔須具備保存期限之設計，如須符合 NIST SP 800-92[2]中 high impact systems 之日誌資料維護長度，檢測執行步驟詳見表 13。

表13 網路印表機之資安檢測項目 1-9

資安檢測項目 1-9	網路印表機須具備並啟用日誌管理功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2

資安檢測項目 1-9	網路印表機須具備並啟用日誌管理功能
	使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認設備是否有開啟日誌管理功能 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認日誌管理相關設定

資料來源：本中心整理

●資安檢測項目 1-10：若設備具 WPS 功能則須關閉

此項目不適用網路印表機設備。

4.2 網路攝影機檢測

●資安檢測項目 2-1：網路攝影機管理介面存取須具備並啟用身分鑑別功能

與管理人員透過訪談或手動驗證方式，驗證網路攝影機所有服務介面之身分鑑別功能，包含使用者、遠端、本地端、無線網路或實體設備端之介面，皆需經身分鑑別過程方可存取設備內非公開資源。檢測執行步驟詳見表 14。

表14 網路攝影機之資安檢測項目 2-1

資安檢測項目 2-1	網路攝影機管理介面存取須具備並啟用身分鑑別功能
檢測工具	弱點掃描工具：Nessus、Nmap 影像串流工具：VLC、CVLC
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊

資安檢測項目 2-1	網路攝影機管理介面存取須具備並啟用身分鑑別功能
	▪ 步驟 2 透過網路針對開啟之服務進行連線，確認是否存在管理介面，並確認該網路攝影機管理介面存取須具備並啟用身分鑑別功能

資料來源：本中心整理

●資安檢測項目 2-2：網路攝影機管理介面通行碼具備並啟用複雜度要求

與管理人員透過訪談或手動執行驗證通行碼之複雜度，檢視通行碼是否包含下列 4 種字元中之 3 種，檢測執行步驟詳見表 15。

– 英文大寫字元(A 到 Z)。

– 英文小寫字元(a 到 z)。

– 10 進位數字(0 到 9)。

– 特殊符號(例如：!、$、#、%)。

表15 網路攝影機之資安檢測項目 2-2

資安檢測項目 2	網路攝影機管理介面通行碼具備並啟用複雜度要求
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊，如管理介面之預設 IP ▪ 步驟 2

資安檢測項目 2	網路攝影機管理介面通行碼具備並啟用複雜度要求
	透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題，亦可請管理人員使用管理者身分登入系統，確認設備安全性設定是否有開啟通行碼複雜度原則

資料來源：本中心整理

●資安檢測項目 2-3：網路攝影機管理介面通行碼須具備並啟用最小長度限制

與管理人員透過訪談或手動驗證方式驗證通行碼之最小長度限制，檢視通行碼最小長度是否為 8 個字元以上，檢測執行步驟詳見表 16。

表16 網路攝影機之資安檢測項目 2-3

資安檢測項目 2-3	網路攝影機管理介面通行碼須具備並啟用最小長度限制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題，亦可請管理人員使用管理者身分登入系統，確認設備安全性設定是否有開啟通行碼最小長度原則

資安檢測項目 2-3	網路攝影機管理介面通行碼須具備並啟用最小長度限制

資料來源：本中心整理

- 資安檢測項目 2-4：網路攝影機管理介面須具備並啟用限制錯誤嘗試之機制

  與管理人員透過訪談或手動驗證方式檢視帳號通行碼之輸入錯誤次數與頻率，並在達到特定輸入次數或頻率時，進行裝置或使用者名稱之鎖定，各端點規範如下，檢測執行步驟詳見表 17。

  – 裝置端：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

  – 通訊(端)網路：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

  – 控制端：5 次連續不成功身分鑑別過程，須使連線失效或進行 15 分鐘之鎖定。

表17 網路攝影機之資安檢測項目 2-4

資安檢測項目 2-4	網路攝影機管理介面須具備並啟用限制錯誤嘗試之機制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2

資安檢測項目 2-4	網路攝影機管理介面須具備並啟用限制錯誤嘗試之機制
	透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題 ▪ 步驟 3 確認手動輸入通行碼或使用工具暴力破解後系統是否會出現帳號鎖住或是測試 IP 被鎖住之訊息

資料來源：本中心整理

●資安檢測項目 2-5：網路攝影機管理介面身分鑑別不得使用預設帳號通行碼

與管理人員透過訪談或手動驗證方式，驗證網路攝影機是否仍能以預設帳號通行碼成功登入，檢測執行步驟詳見表 18。

表18 網路攝影機之資安檢測項目 2-5

資安檢測項目 2-5	網路攝影機管理介面身分鑑別不得使用預設帳號通行碼
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼進行登入，確認是否已變更預設帳號通行碼

資料來源：本中心整理

●資安檢測項目 2-6：網路攝影機資料存取須進行權限控管，並以最小權限

為原則

與管理人員透過訪談或手動驗證方式驗證資料存取是否經權限控管，並必須存在至少 2 種角色，包含具有較高權限之角色(如 Administrator 或 System)與一般僅支援最低權限之角色(如 user)。此外，須對可以被身分鑑別之每一個授權角色或用戶，執行最小權限原則，檢測執行步驟詳見表 19。

表19 網路攝影機之資安檢測項目 2-6

資安檢測項目 2-6	網路攝影機資料存取須進行權限控管，並以最小權限為原則
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認是否有進行權限管控設定 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認使用者權限相關設定

資料來源：本中心整理

●資安檢測項目 2-7：網路攝影機之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞

透過實際檢測方式，針對設備體/韌體、作業系統及相關應用程式進行檢測，須不能存在已揭露之 OWASP TOP 10、CVE、NVD 或 CVSS 評分為

7 以上之資安漏洞，且原始碼掃描須不能存在 CWE/SANS on the cusp list 或 CWE/SANS TOP 25 最危險之程式設計錯誤。檢測執行步驟詳見表 20。

表20 網路攝影機之資安檢測項目 2-7

資安檢測項目 2-7	網路攝影機之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或受測標的型號搜尋弱點資訊 ▪ 步驟 2 確認受測標的系統或服務之版本是否存在已揭露漏洞，並嘗試進行弱點驗證與利用

資料來源：本中心整理

- 資安檢測項目 2-8：網路攝影機所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現以下非預期異常行為：
  - 產品設定重新初始化。
  - 在測試結束後 2 分鐘內，程式中斷或強制失敗且無法回復至前一狀態。
  - 程式凍結或停止回應。
  - 測試所使用之資源在測試後仍被綁定。
  - 軟體顯示無法處理之例外。
  - 儲存資料毀壞。

– 產品對異常輸入測試失去連線。

– 針對特定行為所造成產品中斷運行，沒有在製造商所指定時間內恢復運行。

– 產品在任何介面下揭露任何個人資料或敏感資料，包含所有遠端介面、本地端介面、無線介面、外部檔案輸入接口及所有通訊協定等。

– 產品在輸入測試以外之外部介面，無法正常運作或回應。

檢測執行步驟詳見表 21。

表21 網路攝影機之資安檢測項目 2-8

資安檢測項目 2-8	網路攝影機所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、PRET、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 瀏覽目標網站，並於登入前與登入後，嘗試在參數內容輸入功能意料外之字串(如 SQL 語法、Script 語法及 XML 語法等) ▪ 步驟 2 確認產品是否正常運作，且不應顯示非預期之異常行為

資料來源：本中心整理

●資安檢測項目 2-9：網路攝影機須具備並啟用日誌管理功能

與管理人員透過訪談方式，檢視設備如具備此功能是否被啟用。須記錄設備所發生之重要事件，並儲存於非快閃記憶體中，包含時間、使用者

身分及操作行為，如成功或不成功之登入嘗試、修改身分鑑別資訊、修改使用者帳號、成功或不成功之軟體更新及相關警示或通知內容。此外，若日誌紀錄檔無法正常儲存時，須發出警示或通知。

此外，須將安全紀錄檔儲存於非快閃記憶體中，直到檔案儲存至外部磁碟，並且不允許非授權之使用者移除或修改。日誌檔須具備保存期限之設計，例如須符合 NIST SP 800-92[2]中 high impact systems 之日誌資料維護長度，檢測執行步驟詳見表 22。

表22 網路攝影機之資安檢測項目 2-9

資安檢測項目 2-9	網路攝影機須具備並啟用日誌管理功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認設備是否有開啟日誌管理功能 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認日誌管理相關設定

資料來源：本中心整理

●資安檢測項目 2-10：若網路攝影機具 WPS 功能則須關閉

此項目不適用網路攝影機設備。

4.3 門禁設備檢測

●資安檢測項目 3-1：門禁設備管理介面存取須具備並啟用身分鑑別功能

與管理人員透過訪談或手動驗證方式，驗證門禁設備所有服務介面之身分鑑別功能，包含使用者、遠端、本地端、無線網路或實體設備端之介面，皆需經身分鑑別過程方可存取設備內非公開資源，檢測執行步驟詳見表 23。

表23 門禁設備之資安檢測項目 3-1

資安檢測項目 3-1	門禁設備管理介面存取須具備並啟用身分鑑別功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，確認門禁設備管理介面存取須具備並啟用身分鑑別功能 ▪ 步驟 3 亦可請設備管理人員陪同至門禁設備所在處，手動操作設備確認是否需要身分鑑別才可進入系統

資料來源：本中心整理

●資安檢測項目 3-2：門禁設備管理介面通行碼具備並啟用複雜度要求

與管理人員透過訪談或手動驗證方式驗證通行碼之複雜度，檢視通行碼是否包含下列 4 種字元中之 3 種，檢測執行步驟詳見表 24。

– 英文大寫字元(A 到 Z)。

– 英文小寫字元(a 到 z)。

– 10 進位數字(0 到 9)。

– 特殊符號(例如：!、$、#、%)。

表24 門禁設備之資安檢測項目 3-2

資安檢測項目 3-2	門禁設備管理介面通行碼具備並啟用複雜度要求
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題，或請設備管理人員協助登入系統，由檢測人員確認是否有開啟通行碼複雜度原則之設定

資料來源：本中心整理

●資安檢測項目 3-3：門禁設備管理介面通行碼須具備並啟用最小長度限制

與管理人員透過訪談或手動驗證方式驗證通行碼之最小長度限制，檢視通行碼最小長度是否為 8 個字元以上，檢測執行步驟詳見表 25。

表25 門禁設備之資安檢測項目 3-3

資安檢測項目 3-3	門禁設備管理介面通行碼須具備並啟用最小長度限制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有最小長度限制，或請設備管理人員協助登入系統，由檢測人員確認是否有開啟通行碼最小長度原則之設定

資料來源：本中心整理

●資安檢測項目 3-4：門禁設備管理介面須具備並啟用限制錯誤嘗試之機制

與管理人員透過訪談或手動驗證方式，檢視帳號通行碼之輸入錯誤次數與頻率，並在達到特定輸入次數或頻率時，進行裝置或使用者名稱之鎖定，各端點規範如下，檢測執行步驟詳見表 26。

– 裝置端：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 通訊(端)網路：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 控制端：5 次連續不成功身分鑑別過程，須使連線失效或進行 15 分鐘之鎖定。

表26 門禁設備之資安檢測項目 3-4

資安檢測項目 3-4	門禁設備管理介面須具備並啟用限制錯誤嘗試之機制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有弱通行碼問題 ▪ 步驟 3 確認手動輸入通行碼或使用工具暴力破解後系統是否會出現帳號鎖住或是測試 IP 被鎖住之訊息

資料來源：本中心整理

●資安檢測項目 3-5：門禁設備管理介面身分鑑別不得使用預設帳號通行碼

與管理人員透過訪談或手動驗證方式，驗證門禁設備是否仍能以預設帳號通行碼成功登入，檢測執行步驟詳見表 27。

表27 門禁設備之資安檢測項目 3-5

資安檢測項目 3-5	門禁設備管理介面身分鑑別不得使用預設帳號通行碼
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1

資安檢測項目 3-5	門禁設備管理介面身分鑑別不得使用預設帳號通行碼
	透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入預設帳號通行碼，確認是否已變更預設帳號通行碼

資料來源：本中心整理

●資安檢測項目 3-6：門禁設備資料存取須進行權限控管，並以最小權限為原則

與管理人員透過訪談方式驗證門禁設備之資料存取是否經權限控管，並必須存在至少 2 種角色，包含具有較高權限之角色(如 Administrator 或 System)與一般僅支援最低權限之角色(如 user)。此外須對可以被身分鑑別之每一個授權角色或用戶，執行最小權限原則，檢測執行步驟詳見表 28。

表28 門禁設備之資安檢測項目 3-6

資安檢測項目 3-6	門禁設備資料存取須進行權限控管，並以最小權限為原則
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2

資安檢測項目 3-6	門禁設備資料存取須進行權限控管，並以最小權限為原則
	使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認是否有進行權限管控 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認相關設定

資料來源：本中心整理

●資安檢測項目 3-7：門禁設備之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞

透過實際檢測方式，針對設備體/韌體、作業系統及相關應用程式進行檢測，須不能存在已揭露之 OWASP TOP 10、CVE、NVD 或 CVSS 評分為 7 以上之資安漏洞，且原始碼掃描須不能存在 CWE/SANS on the cusp list 或 CWE/SANS TOP 25 最危險之程式設計錯誤。檢測執行步驟詳見表 29。

表29 門禁設備之資安檢測項目 3-7

資安檢測項目 3-7	門禁設備之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或受測標的型號搜尋弱點資訊 ▪ 步驟 2

資安檢測項目 3-7	門禁設備之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
	確認受測標的系統或服務之版本是否存在已揭露漏洞，並嘗試進行弱點驗證與利用

資料來源：本中心整理

- 資安檢測項目 3-8：門禁設備所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現以下非預期異常行為：
  - 產品設定重新初始化。
  - 在測試結束後 2 分鐘內，程式中斷或強制失敗且無法回復至前一狀態。
  - 程式凍結或停止回應。
  - 測試所使用之資源在測試後仍被綁定。
  - 軟體顯示無法處理之例外。
  - 儲存資料毀壞。
  - 產品對異常輸入測試失去連線。
  - 針對特定行為所造成產品中斷運行，沒有在製造商所指定時間內恢復運行。
  - 產品在任何介面下揭露任何個人資料或敏感資料，包含所有遠端介面、本地端介面、無線介面、外部檔案輸入接口及所有通訊協定等。
  - 產品在輸入測試以外之外部介面，無法正常運作或回應。

檢測執行步驟詳見表 30。

表30 門禁設備之資安檢測項目 3-8

資安檢測項目 3-8	門禁設備所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 瀏覽目標網站，並於登入前與登入後，嘗試在參數內容輸入功能意料外之字串(如 SQL 語法、Script 語法及 XML 語法等) ▪ 步驟 2 確認產品是否正常運作，且不應顯示非預期之異常行為

資料來源：本中心整理

●資安檢測項目 3-9：門禁設備須具備並啟用日誌管理功能

與管理人員透過訪談或手動檢測方式，檢視設備如具備此功能是否被啟用。須記錄設備所發生之重要事件，並儲存於非快閃記憶體中，包含時間、使用者身分及操作行為，如成功或不成功之登入嘗試、修改身分鑑別資訊、修改使用者帳號、成功或不成功之軟體更新及相關警示或通知內容。此外，若日誌紀錄檔無法正常儲存時，須發出警示或通知。

此外，須將安全紀錄檔儲存於非快閃記憶體中，直到檔案儲存至外部磁碟，並且不允許非授權之使用者移除或修改。日誌檔須具備保存期限之設計，如須符合 NIST SP 800-92[2]中 high impact systems 之日誌資料維護長度，檢測執行步驟詳見表 31。

表31 門禁設備之資安檢測項目 3-9

資安檢測項目 3-9	門禁設備須具備並啟用日誌管理功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認設備是否有開啟日誌管理功能 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認日誌管理相關設定

資料來源：本中心整理

●資安檢測項目 3-10：若門禁設備具 WPS 功能則須關閉

此項目不適用門禁設備。

4.4 無線網路基地台/無線路由器檢測

●資安檢測項目 4-1：無線網路基地台/無線路由器管理介面存取須具備並啟用身分鑑別功能

與管理人員透過訪談或手動檢測方式，驗證無線網路基地台/無線路由器所有服務介面之身分鑑別功能，包含使用者、遠端、本地端、無線網路或實體設備端之介面，皆需經身分鑑別過程方可存取設備內非公開資源。檢測執行步驟詳見表 32。

表32 無線網路基地台/無線路由器之資安檢測項目 4-1

資安檢測項目 4-1	無線網路基地台/無線路由器管理介面存取須具備並啟用身分鑑別功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，確認無線網路基地台/無線路由器管理介面存取須具備並啟用身分鑑別功能

資料來源：本中心整理

●資安檢測項目 4-2：無線網路基地台/無線路由器管理介面通行碼具備並啟用複雜度要求

與管理人員透過訪談或手動檢測方式驗證通行碼之複雜度，檢視通行碼是否包含下列 4 種字元中之 3 種。

– 英文大寫字元(A 到 Z)。

– 英文小寫字元(a 到 z)。

– 10 進位數字(0 到 9)。

– 特殊符號(例如：!、$、#、%)。

檢測執行步驟詳見表 33。

表33 無線網路基地台/無線路由器之資安檢測項目 4-2

資安檢測項目 4-2	無線網路基地台/無線路由器設備管理介面通行碼具備並啟用複雜度要求
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題，或請設備管理人員協助登入系統，由檢測人員確認是否有開啟通行碼複雜度原則之設定

資料來源：本中心整理

●資安檢測項目 4-3：無線網路基地台/無線路由器管理介面通行碼須具備並啟用最小長度限制

與管理人員透過訪談或手動檢測方式驗證通行碼之最小長度限制，檢視通行碼最小長度是否為 8 個字元以上，檢測執行步驟詳見表 34。

表34 無線網路基地台/無線路由器之資安檢測項目 4-3

資安檢測項目 4-3	無線網路基地台/無線路由器設備管理介面通行碼須具備並啟用最小長度限制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1

資安檢測項目 4-3	無線網路基地台/無線路由器設備管理介面通行碼須具備並啟用最小長度限制
	透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有最小長度限制

資料來源：本中心整理

●資安檢測項目 4-4：無線網路基地台/無線路由器管理介面須具備並啟用限制錯誤嘗試之機制

與管理人員透過訪談或手動檢測方式，檢視帳號通行碼之輸入錯誤次數與頻率，並在達到特定輸入次數或頻率時，進行裝置或使用者名稱之鎖定，各端點規範如下，檢測執行步驟詳見表 35。

– 裝置端：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 通訊(端)網路：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 控制端：5 次連續不成功身分鑑別過程，須使連線失效或進行 15 分鐘之鎖定。

表35 無線網路基地台/無線路由器之資安檢測項目 4-4

資安檢測項目 4-4	無線網路基地台/無線路由器設備管理介面須具備並啟用限制錯誤嘗試之機制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra

資安檢測項目 4-4	無線網路基地台/無線路由器設備管理介面須具備並啟用限制錯誤嘗試之機制
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有弱通行碼問題 ▪ 步驟 3 確認手動輸入通行碼或使用工具暴力破解後系統是否會出現帳號鎖住或是測試 IP 被鎖住之訊息

資料來源：本中心整理

●資安檢測項目 4-5：無線網路基地台/無線路由器管理介面身分鑑別不得使用預設帳號通行碼

與管理人員透過訪談或手動檢測方式，驗證無線網路基地台/無線路由器是否仍能以預設帳號通行碼成功登入。檢測執行步驟詳見表 36。

表36 無線網路基地台/無線路由器之資安檢測項目 4-5

資安檢測項目 4-5	無線網路基地台/無線路由器設備管理介面身分鑑別不得使用預設帳號通行碼
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2

資安檢測項目 4-5	無線網路基地台/無線路由器設備管理介面身分鑑別不得使用預設帳號通行碼
	透過網路針對開啟之服務進行連線，手動輸入預設帳號通行碼，確認是否已變更預設帳號通行碼

資料來源：本中心整理

- 資安檢測項目 4-6：無線網路基地台/無線路由器資料存取須進行權限控管，並以最小權限為原則

與管理人員透過訪談或手動檢測方式，驗證無線網路基地台/無線路由器之資料存取是否經權限控管，並必須存在至少 2 種角色，包含具有較高權限之角色(如 Administrator 或 System)與一般僅支援最低權限之角色(如 user)。此外，須對可以被身分鑑別之每一個授權角色或用戶，執行最小權限原則。檢測執行步驟詳見表 37。

表37 無線網路基地台/無線路由器之資安檢測項目 4-6

資安檢測項目 4-6	無線網路基地台/無線路由器設備資料存取須進行權限控管，並以最小權限為原則
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認是否有進行權限管控 ▪ 步驟 3

資安檢測項目 4-6	無線網路基地台/無線路由器設備資料存取須進行權限控管，並以最小權限為原則
	透過訪談或是請管理設備人員登入系統，確認相關設定

資料來源：本中心整理

- 資安檢測項目 4-7：無線網路基地台/無線路由器之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞

透過實際檢測方式，針對設備體/韌體、作業系統及相關應用程式進行檢測，須不能存在已揭露之 OWASP TOP 10、CVE、NVD 或 CVSS 評分為 7 以上之資安漏洞，且原始碼掃描須不能存在 CWE/SANS on the cusp list 或 CWE/SANS TOP 25 最危險之程式設計錯誤。檢測執行步驟詳見表 38。

表38 無線網路基地台/無線路由器之資安檢測項目 4-7

資安檢測項目 4-7	無線網路基地台/無線路由器之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或受測標的型號搜尋弱點資訊 ▪ 步驟 2 確認受測標的系統或服務之版本是否存在已揭露漏洞，並嘗試進行弱點驗證與利用

資料來源：本中心整理

- 資安檢測項目 4-8：無線網路基地台/無線路由器所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現以下非預期異常行為：
  - 產品設定重新初始化。
  - 在測試結束後 2 分鐘內，程式中斷或強制失敗且無法回復至前一狀態。
  - 程式凍結或停止回應。
  - 測試所使用之資源在測試後仍被綁定。
  - 軟體顯示無法處理之例外。
  - 儲存資料毀壞。
  - 產品對異常輸入測試失去連線。
  - 針對特定行為所造成產品中斷運行，沒有在製造商所指定時間內恢復運行。
  - 產品在任何介面下揭露任何個人資料或敏感資料，包含所有遠端介面、本地端介面、無線介面、外部檔案輸入接口及所有通訊協定等。
  - 產品在輸入測試以外之外部介面，無法正常運作或回應。

檢測執行步驟詳見表 39。

表39 無線網路基地台/無線路由器之資安檢測項目 4-8

資安檢測項目 4-8	無線網路基地台/無線路由器所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite

資安檢測項目 4-8	無線網路基地台/無線路由器所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
	無線封包利用工具：airmon-ng、airodump-ng、aircrack-ng、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 瀏覽目標網站，並於登入前與登入後，嘗試在參數內容輸入功能意料外之字串(如 SQL 語法、Script 語法及 XML 語法等) ▪ 步驟 2 確認產品是否正常運作，且不應顯示非預期之異常行為

資料來源：本中心整理

●資安檢測項目 4-9：無線網路基地台/無線路由器須具備並啟用日誌管理功能

與管理人員透過訪談或手動檢測方式，檢視設備如具備此功能是否被啟用。須記錄設備所發生之重要事件，並儲存於非快閃記憶體中，包含時間、使用者身分及操作行為，如成功或不成功之登入嘗試、修改身分鑑別資訊、修改使用者帳號、成功或不成功之軟體更新及相關警示或通知內容。此外，若日誌紀錄檔無法正常儲存時，須發出警示或通知。

此外，須將安全紀錄檔儲存於非快閃記憶體中，直到檔案儲存至外部磁碟，並且不允許非授權之使用者移除或修改。日誌檔須具備保存期限之設計，如須符合 NIST SP 800-92[2]中 high impact systems 之日誌資料維護長度。檢測執行步驟詳見表 40。

表40 無線網路基地台/無線路由器之資安檢測項目 4-9

資安檢測項目 4-9	無線網路基地台/無線路由器設備須具備並啟用日誌管理功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊。 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認設備是否有開啟日誌管理功能 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認日誌管理相關設定

資料來源：本中心整理

●資安檢測項目 4-10：若無線網路基地台/無線路由器具 WPS 功能則須關閉

與管理人員透過訪談或手動檢測方式，檢視設備是否關閉此功能。WPS 功能須預設為關閉，且須提供使用者身分鑑別功能(例如：WPS PIN)與 WPS Lock 之開/關功能設定，並使用安全加密演算法(詳見表 41)連線。檢測執行步驟詳見表 42。

表41 通行碼演算法

項次	通行碼演算法
1	ISO/IEC 9796 (all parts), Information technology – Security techniques – Digital signature scheme giving message recovery.

項次	通行碼演算法
2	ISO/IEC 9797 (all parts), Information technology – Security techniques – Message Authentication Codes (MACs).
3	ISO/IEC 9798 (all parts), Information technology – Security techniques – Entity authentication.
4	ISO/IEC 10118 (all parts), Information technology – Security techniques – Hash functions.
5	ISO/IEC 11770 (all parts), Information technology – Security techniques – Key management.
6	ISO/IEC 14888 (all parts), Information technology – Security techniques – Digital signatures with appendix.
7	ISO/IEC 15946 (all parts), Information technology – Security techniques – Cryptographic techniques based on elliptic curve.
8	ISO/IEC 18033 (all parts), Information technology – Security techniques – Encryption algorithms.
9	ISO/IEC 19772 (all parts), Information technology – Security techniques – Authenticated encryption.
10	NIST FIPS 140-2, Annex A: Approved Security Functions.
11	NIST FIPS 140-2, Annex D: Approved Key Establishment Techniques

資料來源：本中心整理

表42 無線網路基地台/無線路由器之資安檢測項目 4-10

資安檢測項目 4-10	若無線網路基地台/無線路由器設備具 WPS 功能則須關閉
檢測工具	弱點掃描工具：Nessus、Nmap

資安檢測項目 4-10	若無線網路基地台/無線路由器設備具 WPS 功能則須關閉
	密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 請系統管理人員登入或由檢測人員使用手動檢測方式登入設備之管理介面 ▪ 步驟 2 確認設備是否關閉 WPS 功能，如有開啟該功能，則需確認是否有開啟使用者身分鑑別功能(例如：WPS PIN)與 WPS Lock 功能設定

資料來源：本中心整理

4.5 環控系統檢測

●資安檢測項目 5-1：環控系統管理介面存取須具備並啟用身分鑑別功能

與管理人員透過訪談或手動檢測方式，驗證環控系統服務所有服務介面之身分鑑別功能，包含使用者、遠端、本地端、無線網路或實體設備端之介面，皆需經身分鑑別過程方可存取設備內非公開資源，檢測執行步驟詳見表 43。

表43 環控系統之資安檢測項目 5-1

資安檢測項目 5-1	環控系統管理介面存取須具備並啟用身分鑑別功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊

資安檢測項目 5-1	環控系統管理介面存取須具備並啟用身分鑑別功能
	▪ 步驟 2 透過網路針對開啟之服務進行連線，確認環控系統管理介面存取須具備並啟用身分鑑別功能 ▪ 步驟 3 亦可請設備管理人員陪同至環控系統所在處，手動操作設備確認是否需要身分鑑別才可進入系統

資料來源：本中心整理

●資安檢測項目 5-2：環控系統管理介面通行碼具備並啟用複雜度要求

與管理人員透過訪談或手動驗證方式驗證通行碼之複雜度，檢視通行碼是否包含下列 4 種字元中之 3 種，檢測執行步驟詳見表 44。

– 英文大寫字元(A 到 Z)。

– 英文小寫字元(a 到 z)。

– 10 進位數字(0 到 9)。

– 特殊符號(例如：!、$、#、%)。

表44 環控系統之資安檢測項目 5-2

資安檢測項目 5-2	環控系統管理介面通行碼具備並啟用複雜度要求
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2

資安檢測項目 5-2	環控系統管理介面通行碼具備並啟用複雜度要求
	透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解，確認是否有弱通行碼問題

資料來源：本中心整理

●資安檢測項目 5-3：環控系統管理介面通行碼須具備並啟用最小長度限制

與管理人員透過訪談或手動檢測方式驗證通行碼之最小長度限制，檢視通行碼最小長度是否為 8 個字元以上，檢測執行步驟詳見表 45。

表45 環控系統之資安檢測項目 5-3

資安檢測項目 5-3	環控系統管理介面通行碼須具備並啟用最小長度限制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有最小長度限制

資料來源：本中心整理

●資安檢測項目 5-4：環控系統管理介面須具備並啟用限制錯誤嘗試之機制

與管理人員透過訪談或手動檢測方式，檢視帳號通行碼之輸入錯誤次數與頻率，並在達到特定輸入次數或頻率時，進行裝置或使用者名稱之鎖

定，各端點規範如下，檢測執行步驟詳見表 46。

– 裝置端：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 通訊(端)網路：10 次連續不成功身分鑑別過程，須使連線失效或進行 30 分鐘之鎖定。

– 控制端：5 次連續不成功身分鑑別過程，須使連線失效或進行 15 分鐘之鎖定。

表46 環控系統之資安檢測項目 5-4

資安檢測項目 5-4	環控系統管理介面須具備並啟用限制錯誤嘗試之機制
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入通行碼，或使用 Burp Suite 利用字典檔進行暴力破解確認是否有弱通行碼問題 ▪ 步驟 3 確認手動輸入通行碼或使用工具暴力破解後系統是否會出現帳號鎖住或是測試 IP 被鎖住之訊息

資料來源：本中心整理

●資安檢測項目 5-5：環控系統管理介面身分鑑別不得使用預設帳號通行碼

與管理人員透過訪談或手動檢測方式，驗證環控系統是否仍能以預設帳

號通行碼成功登入，檢測執行步驟詳見表 47。

表47 環控系統之資安檢測項目 5-5

資安檢測項目 5-5	環控系統管理介面身分鑑別不得使用預設帳號通行碼
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，或是針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 透過網路針對開啟之服務進行連線，手動輸入預設帳號通行碼，確認是否已變更預設帳號通行碼

資料來源：本中心整理

●資安檢測項目 5-6：環控系統資料存取須進行權限控管，並以最小權限為原則

與管理人員透過訪談方式驗證資料存取是否經權限控管，並必須存在至少 2 種角色，包含具有較高權限之角色(如 Administrator 或 System)與一般僅支援最低權限之角色(如 user)。此外，須對可以被身分鑑別之每一個授權角色或用戶，執行最小權限原則，檢測執行步驟詳見表 48。

表48 環控系統之資安檢測項目 5-6

資安檢測項目 5-6	環控系統資料存取須進行權限控管，並以最小權限為原則
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra

資安檢測項目 5-6	環控系統資料存取須進行權限控管，並以最小權限為原則
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認是否有進行權限管控 ▪ 步驟 3 透過訪談或是請設備管理人員登入系統，確認相關設定

資料來源：本中心整理

●資安檢測項目 5-7：環控系統之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞

透過實際檢測方式，針對設備體/韌體、作業系統及相關應用程式進行檢測，須不能存在已揭露之 OWASP TOP 10、CVE、NVD 或 CVSS 評分為 7 以上之資安漏洞，且原始碼掃描須不能存在 CWE/SANS on the cusp list 或 CWE/SANS TOP 25 最危險之程式設計錯誤。檢測執行步驟詳見表 49。

表49 環控系統之資安檢測項目 5-7

資安檢測項目 5-7	環控系統之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit

資安檢測項目 5-7	環控系統之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或受測標的型號搜尋弱點資訊 ▪ 步驟 2 確認受測標的系統或服務之版本是否存在已揭露漏洞，並嘗試進行弱點驗證與利用

資料來源：本中心整理

- 資安檢測項目 5-8：環控系統所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現以下非預期異常行為：
  - 產品設定重新初始化。
  - 在測試結束後 2 分鐘內，程式中斷或強制失敗且無法回復至前一狀態。
  - 程式凍結或停止回應。
  - 測試所使用之資源在測試後仍被綁定。
  - 軟體顯示無法處理之例外。
  - 儲存資料毀壞。
  - 產品對異常輸入測試失去連線。
  - 針對特定行為所造成產品中斷運行，沒有在製造商所指定時間內恢復運行。
  - 產品在任何介面下揭露任何個人資料或敏感資料，包含所有遠端介面、本地端介面、無線介面、外部檔案輸入接口及所有通訊協定等。

– 產品在輸入測試以外之外部介面，無法正常運作或回應。

檢測執行步驟詳見表 50。

表50 環控系統之資安檢測項目 5-8

資安檢測項目 5-8	環控系統所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
檢測工具	弱點掃描工具：Nessus、Nmap 封包攔截工具：Burp Suite、SQLMap、Kali、Metasploit
檢測執行步驟	▪ 步驟 1 瀏覽目標網站，並於登入前與登入後，嘗試在參數內容輸入功能意料外之字串(如 SQL 語法、Script 語法及 XML 語法等) ▪ 步驟 2 確認產品是否正常運作，且不應顯示非預期之異常行為

資料來源：本中心整理

●資安檢測項目 5-9：環控系統須具備並啟用日誌管理功能

與管理人員透過訪談或手動檢測方式，檢視設備如具備此功能是否被啟用。須記錄設備所發生之重要事件，並儲存於非快閃記憶體中，包含時間、使用者身分及操作行為，如成功或不成功之登入嘗試、修改身分鑑別資訊、修改使用者帳號、成功或不成功之軟體更新及相關警示或通知內容。此外，若日誌紀錄檔無法正常儲存時，須發出警示或通知。

此外，須將安全紀錄檔儲存於非快閃記憶體中，直到檔案儲存至外部磁碟，並且不允許非授權之使用者移除或修改。日誌檔須具備保存期限之設計，如須符合 NIST SP 800-92[2]中 high impact systems 之日誌資料維護

長度，檢測執行步驟詳見表 51。

表51 環控系統之資安檢測項目 5-9

資安檢測項目 5-9	環控系統須具備並啟用日誌管理功能
檢測工具	弱點掃描工具：Nessus、Nmap 密碼破解工具：Burp Suite、Hydra
檢測執行步驟	▪ 步驟 1 透過弱點掃描工具 Nessus 或 Nmap 掃描受測標的之網路開啟服務狀態，並針對該型號搜尋預設帳號通行碼相關資訊 ▪ 步驟 2 使用預設帳號通行碼或嘗試使用暴力通行碼破解進行登入，如可登入，則進入系統後確認設備是否有開啟日誌管理功能 ▪ 步驟 3 透過訪談或是請管理設備人員登入系統，確認日誌管理相關設定

資料來源：本中心整理

●資安檢測項目 5-10：若環控系統具 WPS 功能則須關閉

此項目不適用環控系統。

5. 結案階段

完成各類設備檢測後，將針對檢測紀錄進行彙整與分析，並依分析結果提供改善建議，供機關提升物聯網設備安全性，檢測結果與改善建議內容重點說明如下。

5.1 檢測結果

針對受測物聯網設備未符合之檢測基準項目進行彙整，詳列受測物聯網設備名稱、未符合之基準項數與項目名稱，未符合之基準項目可簡述不符合之處(如登入頁面)、採用之檢測手法、可能產生之風險與可能洩漏之資訊內容，物聯網設備檢測結果彙整表範本詳見表 52，範例詳見圖 3。此外，如需以量化數字清楚呈現檢測結果，可依物聯網設備檢測評分表範本(詳見表 53)與配分計算方式說明(詳見表 54)進行分數計算。

表52 物聯網設備檢測結果彙整表範本

物聯網設備檢測			
不符合總數			
項次	設備名稱	不符合項數	不符合項目
1			
2			
3			

資料來源：本中心整理

物聯網設備檢測			
不符合總數		9	
項次	設備名稱	不符合項數	不符合項目
1	網路印表機 SHARP MX-2310U (10.10.22.201)	3	1-2：網路印表機管理介面通行碼具備並啟用複雜度要求
			1-3：網路印表機管理介面通行碼須具備並啟用最小長度限制
			1-5：網路印表機管理介面身分鑑別不得使用預設帳號通行碼
2	網路攝影機 HUNI 網路攝影機 (10.1.34.201)	2	2-3：網路攝影機管理介面通行碼須具備並啟用最小長度限制
			2-7：網路攝影機之軟/韌體、作業系統及相關應用程式應保持更新，不得存在 CVSS v3 高於 7 分(含)之 CVE 漏洞
3	門禁設備 ZKTECO (10.2.6.213)	1	3-3：門禁設備管理介面通行碼須具備並啟用最小長度限制
4	無線網路基地台 ASUS RT-AC88U (10.100.0.88)	2	4-2：無線網路基地台/無線路由器管理介面通行碼具備並啟用複雜度要求
			4-9：無線網路基地台/無線路由器須具備並啟用日誌管理功能
5	環控系統 工業主機(CIM) (10.3.101.49)	1	5-5：環控系統管理介面身分鑑別不得使用預設帳號通行碼

資料來源：本中心整理

圖3　檢測結果彙整表範例

表53 物聯網設備檢測評分表範本

受測機關(構)					
技術檢測日期		年　月　日~　年　月　日			
項次	技術檢測項目	技術檢測子項	檢測範圍	配分	得分
1	物聯網設備檢測	網路印表機檢測	5 組物聯網設備	10	
		網路攝影機檢測			
		門禁設備檢測			
		無線網路基地台/無線路由器檢測			
		環控系統檢測			

資料來源：本中心整理

表54 物聯網設備檢測配分計算方式

檢測項目	檢測範圍	配分	配分計算方式
物聯網設備檢測	5 組物聯網設備(網路印表機、網路攝影機、門禁設備、無線網路基地台/無線路由器、環控系統)	10	計算規則： 得分 / 檢測基準不符合率(X) 10 / 0% 9 / 0% < X≦11% 8 / 11% < X≦22% 7 / 22% < X≦33% 6 / 33% < X≦44% 5 / 44% < X≦55%

<table>
<tr><th>檢測項目</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>4</td><td>55% < X≦66%</td></tr>
<tr><td>3</td><td>66% < X≦77%</td></tr>
<tr><td>2</td><td>77% < X≦88%</td></tr>
<tr><td>1</td><td>88% < X<100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪檢測基準不符合率：
X=(不符合檢測基準之項數/檢測項目總數)*100%
▪計算公式：
本項得分=檢測基準不符合率(X)對應之得分
</td></tr>
</table>

資料來源：本中心整理

5.2 改善建議

物聯網設備檢測結果彙整與分析後，除說明各項不符合基準之內容與可能產生之風險外，應提出具體改善建議，以利受測單位快速掌握檢測結果與調整方向，此外，相同廠牌與型號之設備皆可能存在相同問題，故應提醒受測單位於後續改善時，應針對相同廠牌與型號之設備一併進行檢視與改善。

6. 結論

物聯網為現今資通訊科技發展常用設備之一，其無所不在之特性可廣泛地應用於不同場合，帶給人們生活上之便利，但也衍生出許多資安問題，為因應不同物聯網設備安全性不足所帶來之相關資安威脅，本文件發展 10 項物聯網設備資安檢測項目，同時選定 5 類物聯網設備做為檢測標的，並設計相對應之檢測方法與標準化作業程序，供政府機關自我檢測或第三方檢測時掌握各檢測項目執行重點與留下相關紀錄，以透過檢測物聯網設備之資安管理落實程度與弱點防護情形，協助機關提升物聯網設備安全性。

7. 參考文獻

[1]國家文官學院 T&D 飛訊，萬物聯網的資安威脅-談物聯網資安防護之道，取自：https://ws.csptc.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNy9yZWxmaWxlLzEyMjIwLzM0MTQ5LzdhNmM5OWJmLWQyNGEtNDkwMC04ZmY2LTNlY2NhM2E2NTZiZS5wZGY%3d&n=5ZCz5Li75Lu7LTEwOTAxKOi%2fvei5pOS%2fruiogikucGRm&icon=.pdf

[2]NIST. SP.800-92, Guide to Computer Security Log Management，取自：https://csrc.nist.gov/publications/detail/sp/800-92/final

8. 附件

8.1 附件 1 物聯網設備基本資訊蒐集表範本

物聯網設備檢測基本資訊蒐集表

物聯網設備檢測基本資訊蒐集表　※項次不足請自行增加
※請填復機關內「網路印表機」、「門禁設備」、「網路攝影機」、「無線網路基地台/無線路由器」、「環控系統」五類相關設備，項次不足請自行增加，若無某類型設備時，則不需填復該類型設備 ※檢測標的為下列可直接使用 RJ45 進行連線之設備、後端管控平台、控制器及伺服器主機: ➢ 網路印表機：提供紙張輸出功能 (範例:印表機、多功能事務機、影印機等) ➢ 網路攝影機：提供影像錄製或影像顯示/儲存功能 (範例:攝影機與網路影像錄影機(NVR)等) ➢ 門禁設備：提供門禁開關或設定功能 (範例:指紋機、指掌靜脈機、門禁卡機等、門禁管理伺服器等) ➢ 無線網路基地台/無線路由器：提供無線網路分享或控制功能 (範例:無線網路基地台、無線路由器、無線區域網路控制器等) ➢ 環控系統：提供監控機房溫度或濕度功能 (範例:溫度計、溼度計、機房溫度監控伺服器等)

編號	類別	無此類別設備	項次	設備名稱	網址（內部 IP）	廠牌型號/作業系統	放置位置
範例	網路印表機	□	1	HP 網路印表機	192.168.5.101	HP LaserJet 4300	資訊處 5 樓辦公室
			2	HP 網路印表機	192.168.5.102	HP LaserJet 4400	資訊處 6 樓辦公室
			3	HP 網路印表機	192.168.5.103	HP LaserJet 4500	資訊處 7 樓辦公室

	門禁設備	□	1	怡群科技門禁卡機	192.168.20.11	怡群科技 Bic-301	人事室 1 樓辦公室
			2	門禁管理伺服器	192.168.20.2	Windows 7	資訊處 1 樓辦公室
	網路攝影機	□	1	AXIS 網路攝影機	192.168.10.11	AXIS P1354	資訊處 6 樓機房
			2	AXIS 網路攝影機	192.168.10.12	AXIS M1033_W	1 樓電梯口
			3	網路影像錄影機	192.168.10.20	AXIS 262	1 樓監控室
	無線網路基地台/無線路由器	□	1	無線區域網路控制器	192.168.0.1	Cisco 2500	資訊處 1 樓辦公室
			2	Thin AP	192.168.0.2	Cisco 2602l -x-k9	第 1 會議室
			3	Thin AP	192.168.0.3	Cisco 2602l -x-k9	第 2 會議室
			4	一般型/SOHO 無線路由器	192.168.0.4	D-link DIR-618	第 3 會議室
	環控系統	□	1	Advantech 水位	192.168.140.55	Advantech WebAccess ver 2.1	資訊處 6 樓機房

				計伺服器			
13.1	網路印表機	□	1				
			2				
			3				
13.2	門禁設備	□	1				
			2				
			3				
13.3	網路攝影機	□	1				
			2				
			3				
13.4	無線網路基地台/無線路由器	□	1				
			2				
			3				
13.5	環控系統	□	1				
			2				
			3				