醫療器材網路安全評估分析參考範本

「通用範本」

衛生福利部食品藥物管理署

110 年 12 月

本範本不具法規強制性，僅提供業者建議或參考使用。

引言

本醫療器材網路安全評估分析參考範本係以衛生福利部食品藥物管理署公告之「適用於製造業者之醫療器材網路安全指引」為基礎，協助業者制定醫療器材網路安全評估報告。

本範本不具法規強制性，僅提供業者建議或參考使用。醫療器材業者如有既定網路安全評估格式，只要能涵蓋本署「適用於製造業者之醫療器材網路安全指引」範圍皆可適用。另範本所列各式文字僅供參考，醫療器材業者仍需視產品本身特性及實際操作流程擬訂，並以其為基礎執行網路安全評估。

OO醫材股份有限公司

醫療器材網路安全評估報告
Cybersecurity Risk Assessment Report for Medical Device

產品名稱

報告基本資訊(Basic Information of the Report)

報告編號 (Report No.)		報告版本 (Report Version)	
公司名稱 (Company Name)			
電話(TEL)		傳真(FAX)	
製造業者地址 (Factory Address)			
審查者 (Review By)	報告製作者 (Prepared By)	評估日期 (Evaluation Period)	報告日期 (Report Date)

目 錄

1. 簡介(Introduction)

1.1 報告概述(Document Overview)

[填寫重點：簡要說明該份報告內涵項目與內容，做一統整性整理]

[填寫範例如下]
本報告包括醫療器材「XXXX」之醫療器材組成元件、軟體物料清單、軟體設計暨發展、網路安全風險評鑑報告、網路安全自我檢核與檢測報告等。(This document covers the security risk assessment report of Product name device, designed in Product name software development project.)因此，本報告包括：

- 風險分析 The risk analysis,
- 風險評鑑報告 The risk assessment report,
- 風險追蹤矩陣 The risk traceability matrix with software requirements.

1.2 評估團隊(Evaluation Team)

[填寫重點：列出進行網路安全分析評估的人員清單，評估團隊相關經驗與專長需要具有資安相關教育訓練、經驗與資格如表1.2.1，若網路安全分析評估工作是公司委外團隊進行，團隊人員清單亦需於此部分列出]

表1.2.1、網路安全分析評估人員清單

姓名 Name	部門 Dept.,	職稱 Title	學歷 Education	經歷 Experience	專長 Specialty	工作年資 Seniority	責任 Responsibility
王 0 明	R&D	系統分析師	OO 大學資工系 碩士	OO 公司研發工程師	ICCP 認證	9 年	產品安全評估
張 0 宏	MIS	MIS 工程師	OO 大學電機系 碩士	OO 電腦網路管理工程師	SSCP 認證	8 年	網路安全評估
陳 0 君	法務	醫療器材法規專員	OO 大學法律系 學士	OO 生技法規助理	OO 證照	5 年	醫療法規符合性評估

1.3 引用文件(Document References)

[填寫重點：若有參照其他文件可在此列出，方便做參照使用，同時表明措施都是有所依據與法源，下面將分專案文件與標準法規兩部分]

1.3.1 引用的專案文件(Project References)

[填寫重點：若有參照技術文件，例如需求文件或設計文件，可在此列出，方便做參照使用如表1.3.1.1，而後有用到可用編號形式連結]

表1.3.1.1、參照技術文件

序號 #	文件編號 Document Identifier	文件標題 Document Title
1		Software Requirements Specification

1.3.2 引用的標準與法規(Standard and Regulatory References)

[填寫重點：列出有參照使用的法規，需要跟網路安全與風險分析相關，確保所作的方式是有所依據的，如表1.3.2.1，建議使用最新國際標準與法規，並標註引用標準的年份、編號、標準全名]

表1.3.2.1、參照標準與法規

序號 # 	文件編號 Document Identifier	文件標題 Document Title
1	ISO 14971:2019	Medical devices -- Application of risk management to medical devices
2	IEC 62304:2015	Medical device software - Software life cycle processes
3	AAMI TIR 57:2016	Principles for medical device security—Risk management
4	IEC 80001-2-8:2016	Application of risk management for IT-networks incorporating medical devices
5	NIST SP 800	

1.3.3 網路安全評估結果摘要(Summary of Cybersecurity Assessment Results)

[填寫重點：對該產品的資安評估結果進行總結，說明對該醫療器材產品分析到的資安風險進行措施降低風險至無或可接受狀態以及需要的追蹤項目]

2. 一般要求(General Requirement)

2.1 產品簡介(Product Introduction)

2.1.1 簡介與發展程序(Development Process)

[填寫重點：說明該醫療器材的分類分級以及網路安全執行措施[1]，用以確保產品網路安全。可作為建議寫法，如更換公司名稱、產品名稱以及開發時的管制措施，意即填入product name, software design and development plan (document No.)即可。業者可自行參酌，在此部分加入此醫療器材相關描述資訊，包括硬體版本、軟(韌)體版本及器材外觀照片。]

[填寫範例如下]

ABC公司已實施合理的管理、技術和實質保護措施，防止ABC公司產品的安全事件和隱私洩露，前提是產品是按照ABC公司的使用說明所操作。然而，隨著系統和威脅的發展，沒有任何系統可以保護所有漏洞。我們認為我們的客戶是維護安全和隱私保護的最重要合作夥伴，在適當的情況下，我們將通過產品變更、技術公告或是披露相關資訊給客戶和主管機關。 ABC公司透過以下措施不斷努力提高整個產品生命週期內的安全性和隱私性：

- 隱私和安全設計
- 產品和供應商風險評估
- 漏洞和更新管理
- 安全編碼原則和分析
- 漏洞掃描和測試
- 適用於客戶數據的存取控制
- 事件應變
- 確保雙向通訊暢通無阻

本文檔的目的是詳細說明ABC公司安全和隱私範例如何應用於本產品，及您應該如何維護該產品安全的知識，以及我們如何與您合作，以確保本產品整個生命週期的安全。

2.1.2 預期用途(Intended Use)

[填寫重點：醫療器材預期用途說明，該預期用途會影響資安分析範圍，例如無資料傳輸即資安風險僅存在設備本身是否有漏洞缺口。若有對外傳輸介面，其對外傳輸介面都需要分析是否有被攻擊的可能性]

2.1.3 軟硬體系統運作架構與軟體物料清單(System Operating Architecture And Software Bill Of Materials)

[廠商根據醫療器材的預期用途與使用情境說明其系統運作架構，提出測試結果，可以使用第三方報告，或是自行使用相關工具進行。例如，可參考美國國家電信暨資訊管理局(NTIA)提供之資訊，或是使用CyCloneDX[2]、SWID[3]、SPDX[4]等軟體建立軟體物料

[1] 西藥、醫療器材及化粧品許可證查詢. Available: https://info.fda.gov.tw/mlms/H0001.aspx
[2] CycloneDX. Available: https://cyclonedx.org
[3] Software Identification. (SWID) Available: https://pages.nist.gov/swid-tools/
[4] Software Package Data Exchange. Available: https://spdx.dev/

清單。[5]]

2.2 網路安全要求(Security Requirement Specification, SRS)

[填寫重點：廠商根據其醫療器材的預期用途以及使用情境回答下面表2.2.1的問題，若檢核表答案為“是“則必須要有對應的執行措施的規格(SRS) ，並對應到執行措施的方法(SDD)，處理該狀況以確保使用時的資訊安全]

本產品之網路安全要求乃參照衛生福利部食品藥物管理署「適用於製造業者之醫療器材網路安全指引」[6]及行政院國家資通安全會報技術服務中心[7]所規範之資通安全需求如下表2.2.1：

表2.2.1、網路安全要求檢核表

分類	問題	答案(是/否/不適用)	SRS
機密性	機敏資料傳輸時，採用加密機制	是	SRS-01
	機敏資料儲存時，採用加密機制	是	SRS-02
	使用公開、國際機構驗證且未遭破解的演算法	是	SRS-03
	使用該演算法支援的最大金鑰長度	是	SRS-04
	不使用自行創造的加密方式	是	SRS-05
	加密金鑰具有保護機制	是	SRS-06
	加密金鑰或憑證週期性更換	是	SRS-07
完整性	重要資料產生 HASH 值，確保其完整性	是	SRS-08
	重要資料傳輸過程，使用防止竄改的協定	是	SRS-09
	提供下載的資料，產生 HASH 值供比對其完整性	是	SRS-10
可用性	評估服務重要性，設定可用性要求	不適用	
	採用「高可用性」(High Availability) 架構或機制	不適用	
	重要資料定時同步至備援環境	不適用	
輸入驗證	採用過濾機制，以防止輸入惡意命令或資料	是	SRS-11
	驗證使用者輸入資料	是	SRS-12
	驗證外部取得的資料	不適用	
	驗證系統參數合理性	是	SRS-13

[5] SOFTWARE BILL OF MATERIALS Available: https://www.ntia.gov/SBOM
[6] 衛生福利部食品藥物管理署. (2021). 適用於製造業者之醫療器材網路安全指引. Available: https://www.fda.gov.tw/TC/newsContent.aspx?cid=3&id=27018
[7] 行政院國家資通安全會報技術服務中心. 系統安全發展流程實務.

	於伺服器端檢查輸入資料合法性	是	SRS-14
身分認證	除了允許匿名存取的功能外，所有功能都必須經過認證才允許存取	是	SRS-15
	身分認證機制位於伺服端且採用集中管理機制	是	SRS-16
	採用多重因素認證(兩種以上認證類型)	是	SRS-17
	採用 CAPTCHA 機制於身分認證或重要交易行為，以防範自動化程式之嘗試	不適用	
	身分認證相關資訊不以明文傳輸	是	SRS-18
	身分認證相關資訊不存於源碼中，並限制存取	是	SRS-19
	身分認證失敗達一定次數後鎖定該帳號	不適用	
	身分認證發生錯誤時，預設不允許存取任何非公開功能	不適用	
	密碼添加亂數資料(Salt)後進行雜湊函數(HASH)處理，才加以儲存	不適用	
	密碼須符合複雜度(長度限制、具備英文大小寫及特殊字元等)	不適用	
	限制需定期更換密碼	不適用	
	重要交易行為要求再次身分認證	不適用	
授權與存取控制	採用伺服端的集中管理機制檢查使用者授權	是	SRS-20
	執行功能或存取資源前，檢查使用者授權	是	SRS-21
	除特殊管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)	不適用	
	使用者/角色賦予所需的最小權限	不適用	
	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行	是	SRS-22
	重要行為由多人/角色授權後才得以進行	不適用	
日誌紀錄	認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行 Log 記錄	是	SRS-23

	Log 紀錄考慮包含以下項目 1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型(例如，成功或失敗)。5.事件優先權(priority)。6. 事件詳細描述。7.事件代碼。8.網路位址	不適用	
	採用單一的 Log 機制，確保輸出格式的一致性	不適用	
	Log 進行適當保護及備份，避免未經授權存取	不適用	
會話管理	會話識別碼(Session ID)是隨機產生且不可預測	是	SRS-24
	使用者的會話階段，設定在合理的時間內失效	不適用	
	使用者的會話階段，使用者登出後失效	不適用	
	使用者重新登入後，會話識別碼(Session ID)會改變	不適用	
	不將會話識別碼(Session ID)或使用者 ID 顯示於使用者可以改寫處	不適用	
錯誤及例外管理	所有的功能都會進行錯誤及例外處理，並將資源正確釋放	是	SRS-25
	軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息	不適用	
	嚴重錯誤採用通知機制(例如電子郵件或簡訊)	不適用	
組態管理	管理者介面限制存取來源或不允許遠端存取	不適用	
	參數設定或系統設定存放處，限制存取或進行適當保護	不適用	
	依賴的外部元件或軟體，不使用預設帳號密碼	是	SRS-26
	作業平台定期更新、關閉不必要服務、注意安全設定	是	SRS-27
	依賴的外部元件或軟體，注意其安全漏洞通告，必要時評估更新	是	SRS-28

[填寫重點：根據檢核表答案為“是”的項目進行需求分析說明需要達成之功能，例如機密性中要求機敏資料傳輸時，採用加密機制，則此需求即為資料傳輸前須先完成加密以保障資料安全]

本產品根據上述自主檢查表，確認網路安全要求如表2.2.2：

表2.2.2、適用項目需求分析

SRS 編號 No. (SRS)	網路安全要求規格說明(Security Requirement Specification SRS Description)
SRS-01	資料傳輸的封包，送出前需要做加密
SRS-02	
SRS-03	

2.3 網路安全細部設計(Security Detail Design, SDD)

本產品網路安全細部設計(Security Detail Design, SDD)，根據SRS的要求落實於產品，確認本產品之網路安全要求。

[填寫重點：根據SRS內容進行細部設計說明如表2.3.1，例如機密性中要求機敏資料傳輸時，採用加密機制，則此需求即為資料傳輸前須先完成加密以保障資料安全，針對該需求說明設計一加密機制於資料傳輸前先行加密後才可送。建議可參考國際網路安全防護標準等級，針對網路安全要求(SRS)，加註安全防護等級之說明，例如:加密演算法AES 宜加註加密金鑰的長度，如 AES-128 或 AES-256，以確立是否符合產品的SRS要求]

表2.3.1、網路安全細部設計

SDD編號 No. (SDD)	網路安全設計規格說明(Security Detail Design, SDD Description)
SDD-01	將資料做傳輸前，需要做AES128 的加密
SDD-02	

2.4 網路安全驗證確效測試(Security Validation & Verification, SVV)

[填寫重點：根據SDD內容進行測試，每一個測試需要寫測試的方法做通過標準，並做測試確認規格，撰寫範例如表2.4.1所示。]

表2.4.1、網路安全驗證確效測試範例

測試編號	SVV-01
軟體版本	1.3.4
測試項目	傳輸封包做AES128加密
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	封包可以用AES128 解開後呈現明碼
測試結果	Pass

2.5 追溯性矩陣(Traceability Matrix)

[填寫重點：根據SRS、SDD、SVV 做矩陣表，清楚寫出每一個SRS 都有被滿足於SDD中，可以一個SRS 對應到多個SDD，每一個或多個SDD 可以整理成一個SVV，撰寫範例如表2.5.1所示]

表2.5.1、追溯性矩陣範例

軟體需求編號	軟體設計規格編號	軟體 V&V 測試編號
SRS-01	SDD-01	SVV-01

3. 網路安全評估(Cybersecurity Assessment)

3.1 網路安全評估計畫(Cybersecurity Assessment Plan)

本產品參照如 NIST SP 800 標準，針對產品進行：

- 本產品軟硬體元件之盤點與分類
- 本產品之網路安全威脅建模
- 本產品之網路安全風險評估
- 本產品之網路安全風險控制措施
- 本產品之網路安全檢測與報告

3.1.1 網路安全威脅建模方法(Security Requirement Specification & Threat Modeling)

網路安全威脅建模包括：

1 識別資產

2 產生資料流向圖（Data Flow Diagram, DFD）

3 分析網路安全威脅。在DFD中每一類部件都有對應STRIDE [假冒（Spoofing）、篡改（Tampering）、否認性（Repudiation）、資訊泄露（Information disclosure）、阻斷服務（Denial of service）、權限提高（Elevation of privilege）]模型威脅。輸出威脅列表，對每個威脅項進行評估處理。

3.1.2 識別資產(Assets Identification)

[填寫重點:醫療器材產品進行分析定義資產分級分類，其分類會影響其資料安全等級以及防護措施，以下表3.1.2.1為分類描述，直接呈現資產表]

針對系統的資產識別，可以將系統資產加以分類：

表3.1.2.1、識別資產分類描述

分類	描述
機敏資料	任何資料其機密性、完整性、可用性遭到破壞時，將會遭受重大不利影響者，如系統組態檔
外部實體	驅動軟體的某人或某物，且為軟體本身無法控制者
程序	處理輸入資料的工作或行為，並輸出資料者，如作業系統、韌體
資料流	資料於軟體或系統中移動的方法，如通訊協定
資料儲存庫	軟體中資料暫時或持續的儲存區，如日誌資料

3.2 資料流向圖(Data Flow Diagram, DFD)

[呈現DFD 圖，根據所識別的資產，可以產生資料流向圖（Data Flow Diagram, DFD），如下圖3.2.1，鑑於確保系統資料的安全性，可以進一步針對資料分級(Data Classification)，並產生資料流向圖（Data Flow Diagram, DFD）。資料的等級可以依據其資安防護需求及資料機敏性區分為高、中、低，如下表3.2.1。不同的資料安全等級，其應對投入的網路安全防護水準亦應有所不同，以降低風險。]

表3.2.1、資料分級之參考

資料安全等級	等級	資安防護特性		
		機密性	完整性	可用性
	高	只有限制性的系統角色才能揭露資料	資料遭到竄改會造成嚴重危害	資料遭到毀壞會造成嚴重危害
	中	系統角色可揭露資料	資料遭到竄改會造成中度危害	資料遭到毀壞會造成中度危害
	低	資料可以公開揭露	資料遭到竄改會造成輕度危害	資料遭到毀壞會造成輕度危害

以從資料的角度來描述一個系統。元素如下：

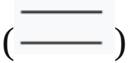
- Flow()
- File/Database ()：表示文件、資料庫
- Function（  ）
- Input/Output（  ）：系統的端點，例如人。
- 信任邊界（  ）：表示可信元素與不可信元素之間的邊界。

圖3.2.1顯示以簡單案例來呈現資料流向圖的結果：

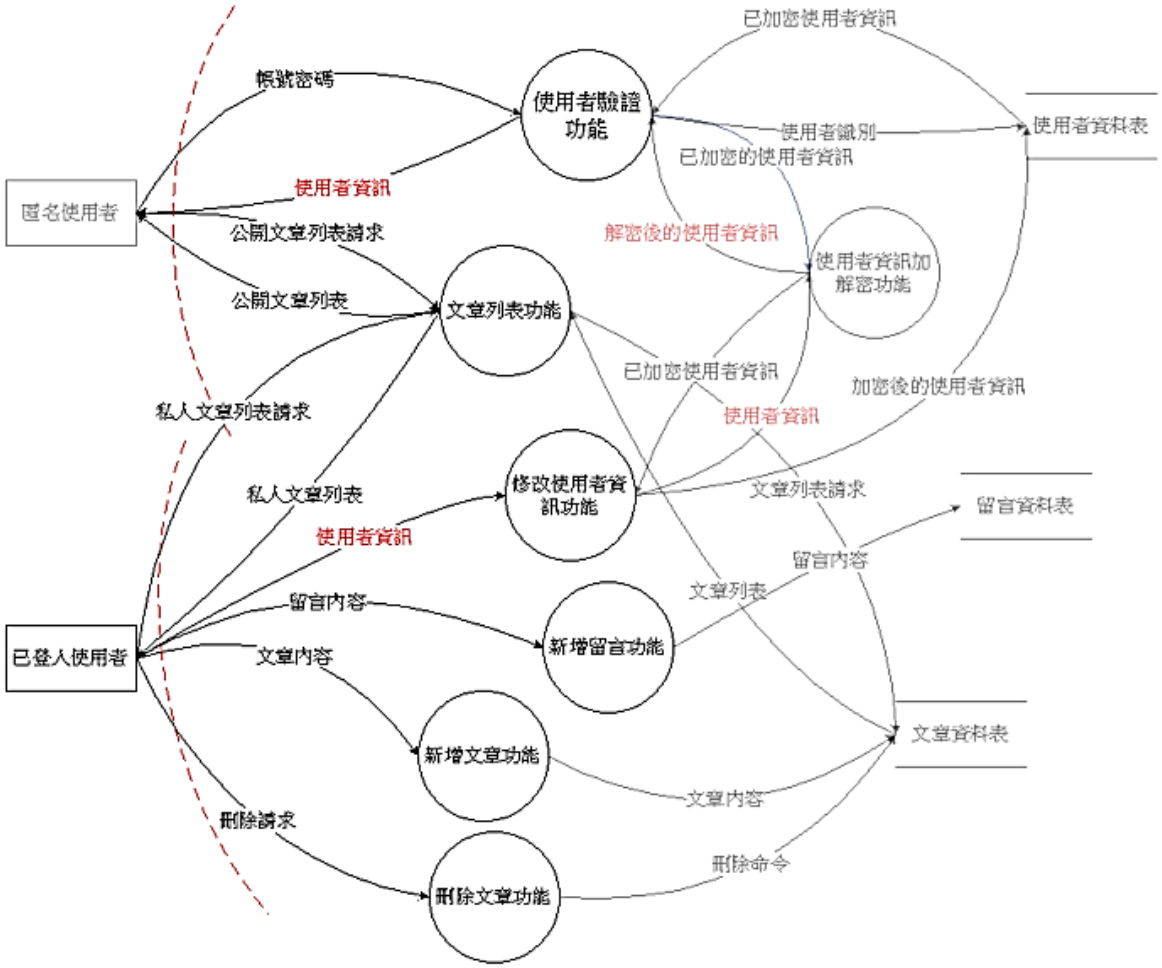


圖3.2.1、資料流向簡單案例圖

3.3 分析網路安全威脅(Cybersecurity Threat Analysis)

[填寫重點：對醫療器材產品進行網路安全威脅分析，其中威脅建模是分析和解決問題的結構化方法，用以識別、量化並應對威脅，利用抽象的方法來幫助思考風險。市面上已有多套工具協助完成威脅建模，例如Microsoft Threat Modeling Tool[8]。Microsoft Threat Modeling Tool套用STRIDE模型，它會將不同類型的威脅分類，可參考表3.3.1。威脅建模工具風險降低措施可參考The Open Web Application Security Project(OWASP) Web應用程式安全性架構來分類，其包含類別詳如表3.3.2「風險降低類別」[9]。威脅建模之前，可依據STRIDE模型威脅分類以及風險降低措施，來完成「網路安全需求檢核表」，以確安全需求，詳細說明如表3.3.3所示。]

[8] Microsoft 威脅模型化工具. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-threats

[9] Microsoft 威脅模型化工具風險降低. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-mitigations

表3.3.1、STRIDE模型之類別說明

類別	描述	資安防護特性
假冒 (Spoofing)	涉及非法存取然後使用其他使用者的驗證資訊，例如使用者名稱和密碼。	身分認證 (Authentication)
竄改 (Tampering)	涉及惡意修改資料。例如在未經授權的狀況下變更資料庫中保存的持續性資料，以及修改在兩部電腦之間透過開放式網路(例如網際網路) 流動的資料。	完整性 (Integrity)
否認性 (Repudiation)	與拒絕執行動作但沒有其他任何一方有辦法另外證明的使用者有關，例如使用者在無法追蹤違禁作業的系統中執行非法作業。不可否認性是指系統對抗否認性威脅的能力。例如，購買商品的使用者可能必須在收到商品時簽名。然後，廠商可以使用簽名收據做為使用者已收到包裹的證據。	不可否認性 (Non-repudiation)
資訊洩漏 (Information Disclosure)	涉及將資訊暴露給不應具有其存取權的個人，例如，使用者可以讀取其未被授權可存取的檔案，或入侵者能夠讀取在兩部電腦之間傳輸的資料。	機密性 (Confidentiality)
阻斷服務 (Denial of Service, DoS)	阻斷服務攻擊可阻斷對有效使用者提供的服務，例如，藉由讓網頁伺服器暫時無法存取或無法使用。您必須防止特定類型的DoS威脅，以便提升系統的可取得性和可靠性(availability and reliability)。	可用性 (Availability)
權限提高 (Elevation of Privilege)	未授權的使用者取得授權的存取權，因此有足夠存取權危害或摧毀整個系統。提高權限威脅包含攻擊者已有效地滲透所有系統防禦，並成為受信任系統本身的一部分，這確實是危險的情況。	授權 (Authorization)

表3.3.2、風險降低類別[10]

類別	描述
稽核和記錄	誰在何時做了什麼？稽核和記錄是指應用程式記錄安全性相關事件的方式
驗證	您是誰？驗證是某實體證明另一個實體身分識別的程序 (通常透過使用者名稱和密碼等認證)
授權	您可以做什麼授權是應用程式針對資源和作業提供存取控制的方式
通訊安全性	您在與誰對話？通訊安全性可確保所有通訊是在最安全的情況下進行的
組態管理	應用程式的執行身分為何其所連線到的資料庫為何？應用程式的管理方式為何如何保護這些設定？ 組態管理指的是應用程式處理這些作業問題的方式
密碼編譯	如何保護機密資料(機密性)？如何防止資料或程式庫遭到竄改(完整性)如何為必須是密碼編譯增強式的隨機值提供種子？密碼編譯是指應用程式強制執行機密性與完整性的方式
例外狀況管理	當應用程式中的呼叫失敗時，應用程式會如何處理？ 您要顯示多少資料？您要對使用者傳回容易理解的錯誤資訊嗎？ 您要將重要例外狀況資訊傳回給呼叫者嗎？應用程式會呼叫失敗嗎？
輸入驗證	您如何知道應用程式收到的輸入是有效且安全的？ 輸入驗證指的是應用程式如何先篩選、消除或拒絕輸入再進行其他處理。請考慮透過進入點限制輸入並透過退出點編碼輸出。您是否信任來源的資料，例如來自資料庫和檔案共用？
機敏性資料	應用程式如何處理機敏性資料？ 機敏性資料指的是應用程式如何處理記憶體中、透過網路或持續性存放區中必須受到保護的任何資料
會話管理	應用程式如何處理和保護使用者工作階段？ 工作階段是指使用者與 Web 應用程式之間的一系列相關互動

[10] Microsoft 威脅模型化工具風險降低. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-mitigations

表3.3.3、網路安全威脅分析表

資產名稱	假冒(S)	竄改(T)	否認行為(R)	資訊洩露(I)	拒絕存取服務(D)	權限提高(E)	威脅列表
作業系統					V	V	D1：透過入侵作業系統關閉相關服務或應用系統 E1：作業系統遭到入侵後，可透過創建帳號並提權。
韌體		V		V			T1：內部不法人員竄改韌體，植入相關木馬或後門程式 I1：透過韌體的偵測或側錄，揭露資訊
系統組態檔		V			V		T2：透過組態設定變更，更改系統服務。 D2：透過組態設定開啟相關通訊介面，以揭露資訊。患者的植入式心律器之脈搏產生器之設定遭受未經授權的變更。植入式心律器之脈搏產生器無法正常運作，對患者造成傷害。
機敏性資料							I2：針對未保護的機敏性資料進行揭露
日誌資料		V	V				T3：竄改日誌資料，隱匿不法行為 R1：竄改日誌資料，修改相關存取記錄
通訊協定	V						S1：透過重送攻擊來進行假冒攻擊 I3：針對未保護的通訊管道揭露資訊
外部實體A							
資料流B							

基於STRIDE與DFD結果，便可以針對系統組成元素分析其網路安全威脅，以及可能的攻擊樹(Attack Tree)，如下圖3.3.1所示：

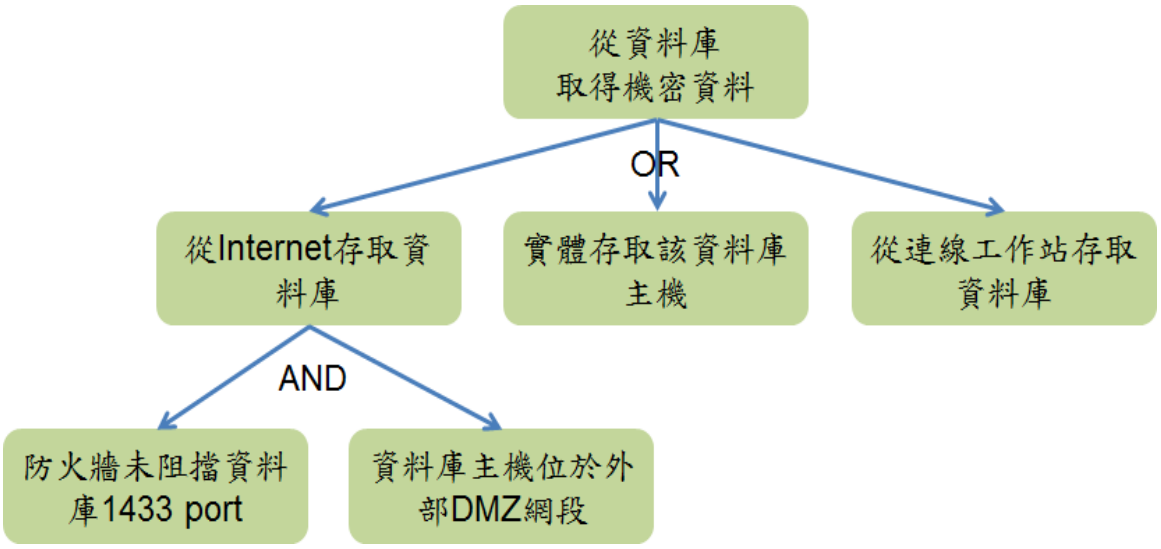


圖3.3.1、攻擊樹狀圖簡單案例圖

3.4 網路安全風險評鑑方法(Cybersecurity Risk Assessment Methodology)

[醫療器材業者根據產品的組成元件來分析是威脅或弱點，並分析可利用性及發生機率。建議可以加入殘餘風險的描述及可接受殘餘風險的鑑別。]

醫療器材的風險評鑑方法，可以參考醫療器材的網路安全風險評鑑框架：

1. 識別威脅來源與弱點
2. 網路安全威脅/風險情境分析
3. 可用性評估
4. 影響性評估
5. 風險評分
6. 風險管理與控制措施

上述步驟1 (識別威脅來源與弱點)以及步驟2 (網路安全風險情境分析)即為第2.2.4節分析網路安全威脅的結果。本章節主要來針對前述網路安全威脅列表的所有威脅進行各別的網路安全風險評鑑。醫療器材之網路安全風險因素主要可分為以下兩種，詳細網路安全因素與風險值由表3.4.1所示：

- 威脅(外部因素)：主要從攻擊者的角度，來探討其針對醫療器材造成網路安全威脅的風險狀況，其評估因子有技能等級、動機、機會與資源3項。
- 弱點(內部因素)：主要從防禦方以及醫療器材本身的安全漏洞，來探討醫療器材之網路安全漏洞可被利用而造成網路安全風險的狀況，其評估因子有發現難易度、可用性與入侵偵測3項。

威脅來源可能來自於使用者、維護廠商、醫院醫工、其他可能碰觸者或網路惡意攻擊者。

表3.4.1、表3.4.2、表3.4.3分別描述了影響醫療器材網路安全的可用性、影響性與發生可能性的相關數值，並經由表3.4.4中的計算公式，將上述所提及的數值合併成代表醫療器材的整體風險值。

表3.4.1、醫療器材的網路安全因素與風險值[11]

可利用性	Threat Agent Factors 威脅因素			Vulnerability Factors 弱點因素		
風險因素與風險值	**T1** Skill level 技能等級	**T2** Motive 動機	**T3** Opportunity & Resources 機會與資源	**V1** Ease of Discovery & Awareness 發現的難易度	**V2** Ease of Exploiting 可用性	**V3** Intrusion Detection 入侵偵測
說明	**就已知現狀電腦技能選最高**	**資料有價值或量大可轉賣獲利/新上市高貴儀器可出名**	**權限管理、實體環境/系統運作介面之控管**	**視使用作業系統，若為主流設備(設備市佔高)或作業系統廠商較能支援**	**若為主流作業系統, 網路上可搜尋到較多的入侵工具**	**是否有安全偵測、有入侵日誌、能自動偵側**
1	無技術性技能或具一般電腦能力	低度或無獎勵或無誘因, 如無個資為一般性設備	實體環境/系統運作介面有加以控管且有特殊權限	1.設備市佔高或設備之作業系統為大宗, 廠商能支援程式修補, 2.作業系統客製化攻擊意願較低	非大宗、非主流作業系統或設備市佔低，網路入侵工具較少	有檢附防護機制或人員對入侵能即時偵測
2	具備部分技術性技能或具備網路與程式撰寫能力	可能有獎勵與誘因, 如檢查量大設備且有醫療資訊	僅有權限管理但無人員/角色管理	使用的作業系統非大宗或較舊作業系統但廠商仍支援程式修補	使用的作業系統非大宗或較舊作業系統，但網路入侵仍有工具	人員對入侵後知後覺
3	具備資安滲透技能	高度獎勵與誘因, 如尖端設備可成名, 具價值的醫療資訊	實體環境/系統運作介面有加以控管，但不需任何權限或資源可達成入侵目的	舊作業系統之弱點廠商已不支援程式修補	設備市佔高、設備作業系統為大宗或主流，網路入侵工具較多	人員對入侵不知不覺

[11] 行政院衛生福利部關鍵基礎設施資安工作推動專案辦公室. 醫療器材的網路安全因素與風險值.

表3.4.2、醫療器材網路安全風險的影響等級

影響等級	嚴重程度
說明	**病人安全影響的嚴重程度**
1	無損害或造成病人稍微不舒服
2	間接傷害，指當下未造成病人直接傷害但病人有潛在傷害的風險
3	直接傷害，指當下即造成病人的損傷或傷害，嚴重者可能追成病人死亡

表3.4.3、醫療器材網路安全風險的發生可能性數值

發生可能性數值	可能由插槽/系統運作介面遭受的風險機會
1	設備無插槽另提供外接或 設備有插槽且有使用者管控措施
2	設備有插槽但無使用者管控措施

表3.4.4、醫療器材風險值的計算

風險值	**風險值 ＝可用性風險值 × 影響性風險值 × 發生可能性數值** （風險值最高值為 18，最低值為 1）
	● 可用性風險值 = 6項風險因素值的平均 (1~3) ● 影響性風險值 = 病人安全影響程度風險值 (1~3) ● 發生可能性數值= 可能由插槽/系統運作介面遭受的風險機會 (1~2)
風險等級	● **A級(高風險)**：風險值介於13.0 ~ 18.0 ，**不可接受(Unacceptable)** ● **B級(中風險)**：風險值介於7.0 ~ 12.9，**可能接受的(Potentially Acceptable)** ● **C級(低風險)**：風險值介於1.0 ~ 6.9，**可接受的(Acceptable)**

表3.4.5、醫療器材網路安全風險等級檢核表

醫療器材組成元件	威脅類型	(I) Impact factor 影響程度 (低:1~高:3)	可利用性						(R) 風險值 (低：1~高：3)	(P) 發生可能性 (低：1~高：2)	(E) 風險結果	(R) 風險等級 A:高風險 (不可接受) B:中風險 (可能接受的) C:低風險 (可接受)	風險編號	風險控制措施
			(T) Threat Agent Factors 威脅因素 (低：1~高：3)			(V) Vulnerability Factors 弱點因素 (低：1~高：3)								
元件	威脅	病人危害程等	(T1) 技能等級	(T2) 動機	(T3) 機會與資源	(V1) 發現的難易度	(V2) 可用性	(V3) 入侵偵測	R=avg(T+V) 平均值	由插槽/系統運作介面遭遇的風險機會	I*R*P	A:13~18 B:7.0~12.9 C:1.0~6.9	風險	控制措施
作業系統	D1	1	2	2	1	2	2	1	1.66	1	1.66	低風險 (可接受)	Risk-01	SDD-01：設定權限管理
作業系統	E1	1	2	1	2	2	2	1	1.66	1	1.66	低風險 (可接受)	Risk-02	SDD-02：針對特權帳戶定期盤點 SDD-03：權限管理
韌體	T1	1	2	1	1	1	2	1	1.33	1	1.33	低風險 (可接受)	Risk-03	SDD-04：軟體的完整性保護
韌體	I1	1	1	2	1	2	2	1	1.5	1	1.5	低風險 (可接受)	Risk-04	SDD-05：進行機敏性資料加密。

														SDD-06：設置加密的金鑰管理模組
系統組態檔	T2	1	1	2	3	2	1	1	1.66	1	1.66	低風險 (可接受)	Risk-05	SDD-07：自動化組態設定
系統組態檔	D2	1	2	1	1	2	2	1	1.5	1	1.5	低風險 (可接受)	Risk-06	SDD-08：自動化組態設定
機敏性資料	I2	2	1	1	1	1	1	1	1	1	2	低風險 (可接受)	Risk-07	SDD-09：進行機敏性資料加密。 SDD-10：設置加密的金鑰管理模組
日誌資料	T3	1	2	1	3	1	2	1	1.66	1	1.66	低風險 (可接受)	Risk-08	SDD-11：建置區塊鏈保護機制
日誌資料	R1	1	1	1	1	1	1	1	1	1	1	低風險 (可接受)	Risk-09	SDD-12：自動登出，以防止器材遭受未經授權人員存取。 SDD -13：使用帳號與密碼才能設定

通訊協定	S1	1	1	1	1	1	2	1	1.16	1	1.16	低風險 (可接受)	Risk-10	SDD -14：設備身分管理機制
通訊協定	I3	1	2	1	1	1	2	1	1.33	1	1.33	低風險 (可接受)	Risk-11	SDD -15：進行機敏性資料加密。 SDD -16：設置加密的金鑰管理模組
…	…	…	…	…	…	…	…	…	…	…	…	…		

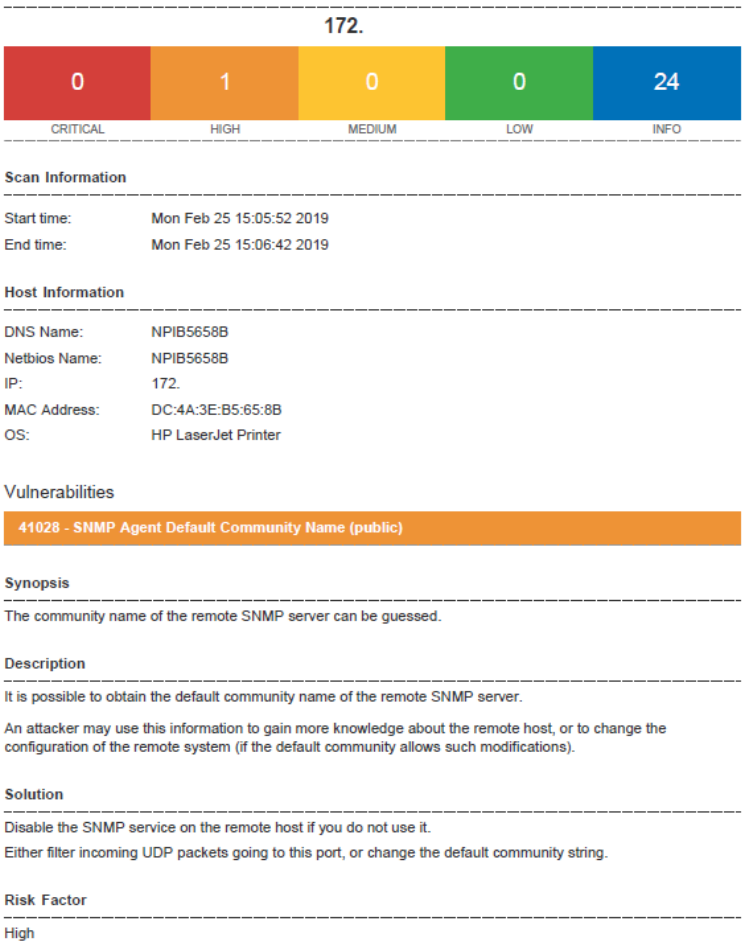
3.5 網路安全檢測方法(Cybersecurity Testing Methodology)

3.5.1 漏洞掃描(Vulnerability Scanning)

[業者根據醫療器材的預期用途與使用情境提出掃描結果，可以使用第三方報告，或是自行使用相關工具進行。漏洞掃描報告原始結果應以附件的方式提供，並且在此章節裡面進行結果摘要說明。摘要內容建議可包含執行掃描時的網路架構、執行人員或單位、使用工具及掃描參數設定等相關資訊，避免在不熟悉弱點掃描作業的情況下，執行錯誤的掃描造成無法有效發現安全漏洞。]

漏洞掃描是針對已知的系統漏洞，對該系統進行掃描、攻擊、測試。漏洞掃描可瞭解現有環境中各種網路設備、系統與主機所存在之漏洞狀況，並透過漏洞掃描結果分析報告獲得有效的改善方案。漏洞通常因缺陷 (flaws) 或錯誤配置(misconfigurations)而產生。缺陷是由產品的設計缺陷造成，常見軟體缺陷是緩衝區溢出(buffer overflow)。錯誤配置例如薄弱的錯誤配置存取控制表、開放的埠和不必要的服務，OWASP網站(https://owasp.org/www-community/Vulnerability_Scanning_Tools)列舉漏洞掃描工具可供參考。

[附上測試報告，如下圖3.5.1.1所示]



172.

0	1	0	0	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Feb 25 15:05:52 2019
End time: Mon Feb 25 15:06:42 2019

Host Information

DNS Name: NPIB5658B
Netbios Name: NPIB5658B
IP: 172.
MAC Address: DC:4A:3E:B5:65:8B
OS: HP LaserJet Printer

Vulnerabilities

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

圖3.5.1.1、漏洞掃描測試報告範例圖

3.5.2 滲透測試(Penetration Testing)

[業者根據醫療器材的預期用途與使用情境提出測試結果，可以使用第三方報告，或是自行使用相關工具進行。撰寫時請注意以下兩點:
1. 滲透測試原始報告應以附件的方式提供，並且在此章節裡面進行結果摘要說明，摘要內容建議可包含執行單位、執行方法、測試項目、發現弱點清單及弱點詳細資訊，針對未修補完成之弱點，亦應於此章節說明未修補之原因與採取之緩解措施。
2. 評估人員應確認執行單位所採用的方法與測試項目是否符合我國醫療器材網路安全指引所要求的內容，例如:使用藍芽傳輸技術的醫療器材，在測試項目內應包括相對應的測試項目、針對通訊協定是否有執行模糊測試等。]

滲透測試(Penetration Test)通常是由資安團隊以駭客之思維與行為模式規劃測試內容，利用漏洞掃描軟體或其他的工具，從外部和內部網路進行模擬入侵，收集系統的相關資訊，探查漏洞。

[附上測試報告，如下圖3.5.2.1所示]

圖3.5.2.1、滲透測試報告範例圖

4. 參考資料(References)

[1] IEC 62304:2006 Medical device software — Software life cycle processes
[2] Manufacturer Disclosure Statement for Medical Device Security. Available: https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

附錄一：醫療器材網路安全評估—自我檢核表(Cybersecurity Self-Checklist)

使用附件“醫療器材網路安全之業者揭露聲明書”檔案

附錄二：本產品相關醫療器材之網路安全通報 (Related Cybersecurity Alerts)

[業者根據其醫療器材的品項, 預期用途與使用情境查詢先前的網路安全通報事件，可搜尋H-ISAC、ECRI、FDA以及TFDA上市後安全等資料庫，分析前例事項發生原因，並提出對應處置措施]

調查並呈現相關醫療器材網路安全通知、漏洞資料庫資訊及產品應對措施。

附錄三：本產品相關之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE)

[業者根據其醫療器材的品項，預期用途與使用情境查詢通用漏洞揭露，可搜尋CVE[12]、NVD[13]等資料庫，分析前例事項發生原因，並提出對應處置措施。若通用漏洞揭露與2.1.3所列之軟體物料清單相關，則建議在CVE後加註於2.1.3中所列之軟體物料清單。]

通用漏洞揭露(Common Vulnerabilities and Exposures, CVE)是資訊安全相關的資料庫，該資料庫收集各種資安漏洞並給予編號以便於查閱，讓資安管理人員有辦法針對部分CVE所條列的系統弱點逐項檢測。此資料庫現由美國非營利組織 MITRE所屬的National Cybersecurity FFRDC所營運維護。將open source可能已有其他應用之弱點被通報所獲得資訊羅列。

[12] https://cve.mitre.org/
[13] https://nvd.nist.gov/vuln/search