「醫療資安論壇」
醫院資訊安全防護現況與精進之道

臺灣資安大會
CYBERSEC 2019

衛生福利部關鍵基礎設施資安工作推動專案辦公室
范仲玫 主任

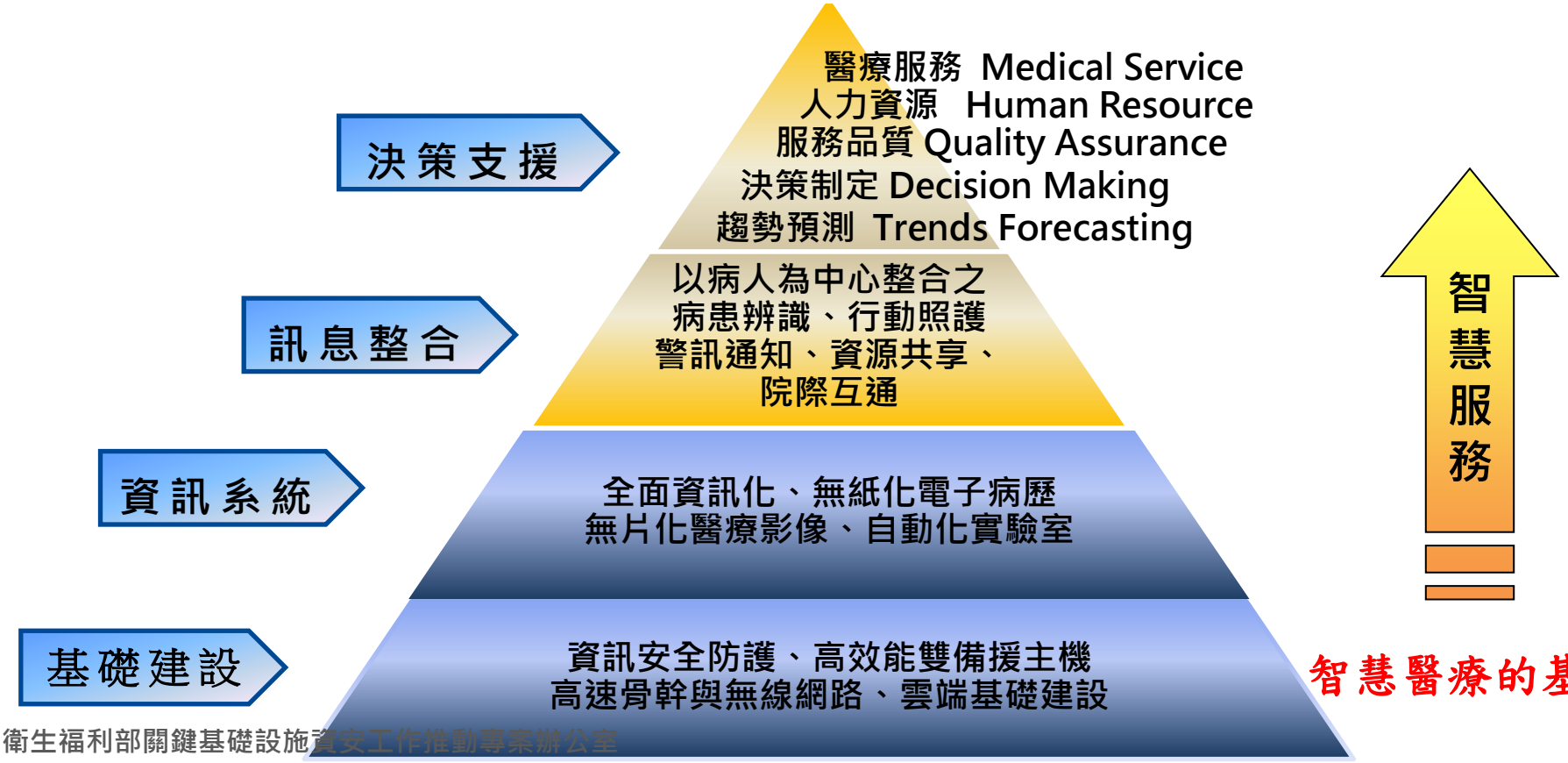
2019.03.19

PRESENTED BY iThome

醫療健康趨勢下之
醫院資訊發展

智慧醫療

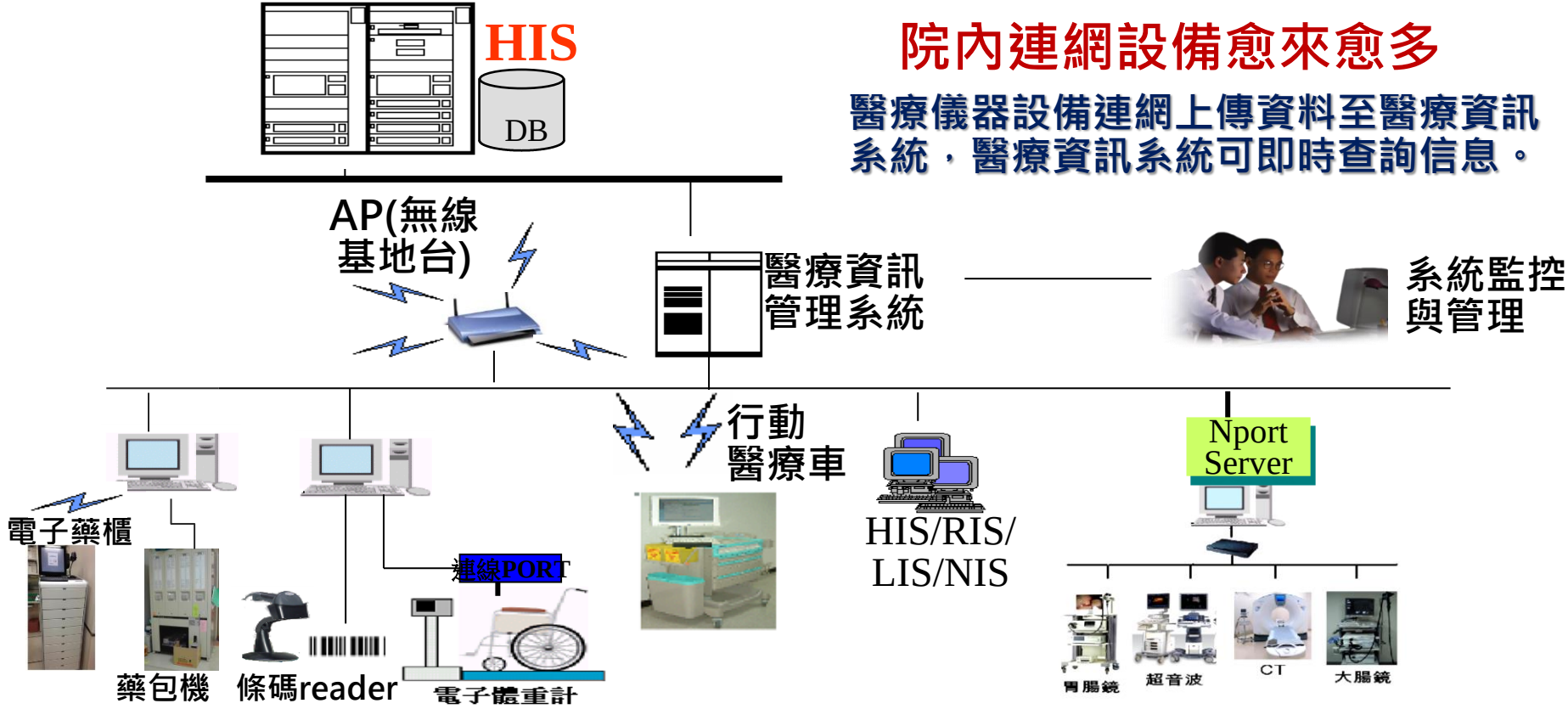
高效率、智慧化、資訊化的醫院



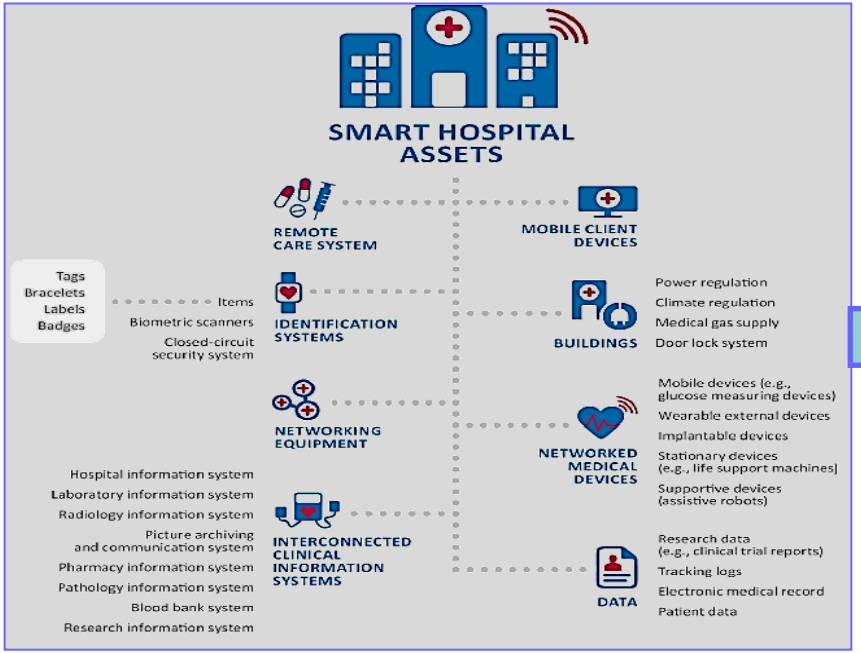
智慧醫療與電子病歷發展，加速資訊需求

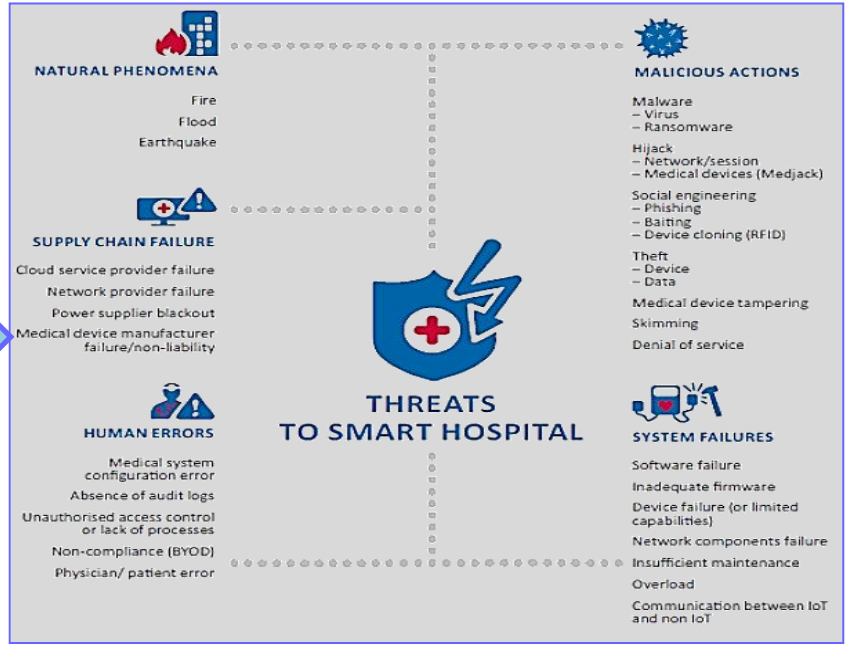
院內連網設備愈來愈多

醫療儀器設備連網上傳資料至醫療資訊系統，醫療資訊系統可即時查詢信息。



e化設備增加資安風險與威脅





ENISA, European Union Agency for Network and Information Security, "Cyber security and resilience for Smart Hospitals," 2016/11/24, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

醫療設備潛在風險威脅

- 依據勤業眾信（Deloitte）針對MDSLs（Medical Device Security Leaders）的一項訪談指出，針對聯網醫療設備的主要威脅包括：
  1. 駭客行為者（例如匿名的個人）希望導致該項服務中斷
  2. 希望出售個人醫療健康資訊，對個人和/或醫療機構實施財務欺詐的小偷。
  3. 懷有惡意的團體或個人，試圖對患者造成傷害（可能針對VIP患者）或尋求損害醫療機構名聲
  4. 並非針對醫療設備，但會逃避現有防病毒引擎和規則的惡意軟體

ECRI 每年發表十大醫療技術危害

美國急救醫學研究所
ECRI(Emergency Care Research Institute)

- 全球醫界知名度頗高擁有40年歷史的非營利機構
- 每年發表十大醫療技術危害，提供醫療機構重要的安全議題做為參考，以進行預防與應對，進而減少醫療技術危害對病患造成的傷害。

ECRI 十大醫療技術危害

2018年「勒索軟體和其他威脅醫療保健服務網絡安全的軟體危害」排名第一

	2018
1	**Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients (IT)** **勒索軟體和其他威脅醫療保健服務網絡安全的軟體，可能會危及患者安全**
2	Endoscope Reprocessing Failures Continue to Expose Patients to Infection Risk 內視鏡再處理失敗會持續使患者曝露於感染風險中
3	Mattresses and Covers May Be Infected by Body Fluids and Microbiological Contaminants(感控問題) 床墊和床罩可能會遭病人體液和微生物污染所引發的感染問題
4	**Missed Alarms May Result from Inappropriately Configured Secondary Notification Devices and Systems** **設定失當的警報轉發通知系統可能導致錯誤或遺漏的警報(使用者操作因素)**
5	Improper Cleaning May Cause Device Malfunctions, Equipment Failures, and Potential for Patient Injury 不適當的清潔程序可能導致設備故障，失效和患者受傷(使用者操作因素)

	2018
6	Unholstered Electrosurgical Active Electrodes Can Lead to Patient Burns 手術使用電燒時，電燒筆置放未適當套住絕緣，可能會因誤觸開關，導致患者灼傷
7	Inadequate Use of Digital Imaging Tools May Lead to Unnecessary Radiation Exposure 數位成像工具使用不當可能導致不必要的輻射照射(使用者操作因素)
8	Workarounds Can Negate the Safety Advantages of Bar-Coded Medication Administration Systems(使用者操作因素) 條碼藥物管理系統的安全優勢可能因現場過度變通使用方法，造成安全性下降。
9	**Flaws in Medical Device Networking Can Lead to Delayed or Inappropriate Care** **醫療設備網路的缺陷可能會導致延遲或不當護理(IT)**
10	Slow Adoption of Safer Enteral Feeding Connectors Leaves Patients at Risk(器材因素) 未使用專用的腸內餵食連接器會使患者面臨誤接輸液的風險

ECRI 十大醫療技術危害

2019年「黑客可以利用遠端訪問醫院資訊系統，破壞醫療保健服務」排名第一

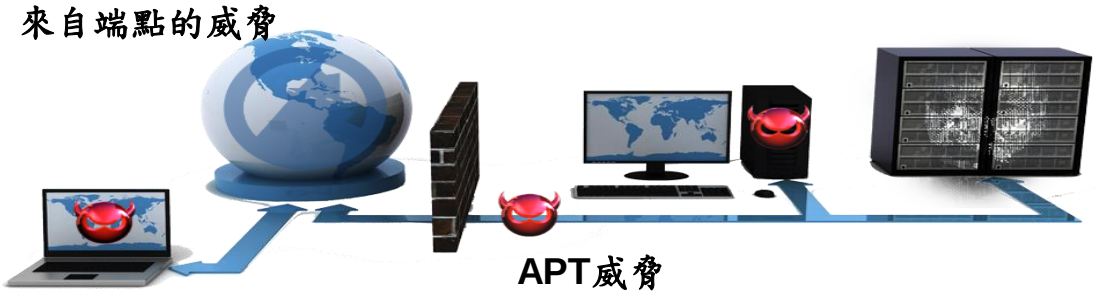
	2019
1	**Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations** **黑客可以利用遠端訪問醫院資訊系統，破壞醫療保健服務**
2	"Clean" Mattresses Can Ooze Body Fluids onto Patients "乾淨"的床墊可以將體液滲透到患者身上
3	Retained Sponges Persist as a Surgical Complication Despite Manual Counts 儘管人工清點，手術遺留海綿（紗布等異物）仍然是一手術併發症
4	Improperly Set Ventilator Alarms Put Patients at Risk for Hypoxic Brain Injury or Death 不正確設定呼吸機警報引數，置患者於缺氧性腦損傷或死亡的風險之中
5	Mishandling Flexible Endoscopes after Disinfection Can Lead to Patient Infections 消毒後的軟鏡（內窺鏡）操作不當會導致患者感染

	2019
6	Confusing Dose Rate with Flow Rate Can Lead to Infusion Pump Medication Errors 將藥物劑量率與流速混淆會導致輸液泵給藥物錯誤
7	Improper Customization of Physiologic Monitor Alarm Settings May Result in Missed Alarms 不適的生理監測儀警報個性化設定可能導致警報遺漏
8	Injury Risk from Overhead Patient Lift Systems 軌道式患者移位系統的傷害風險
9	**Cleaning Fluid Seeping into Electrical Components Can Lead to Equipment Damage and Fires** 裝置清潔液滲入電器元件可能導致裝置損壞和火災
10	Flawed Battery Charging Systems and Practices Can Affect Device Operation 電池充電系統缺陷和充電故障會影響裝置正常執行

2018年10月1日在網站釋出《2019年十大醫療技術危害》

IT環境開放且迅速由院內擴展到院外

資安威脅變的
越來越多樣化



APT威脅
Advanced Persistent Threats

醫院資訊安全管理與防護

醫院為何建置資安管理制度

達成目標：

- 資訊服務不中斷
- (特種)資料保護

建立 — 組織規範
內部控制

確保 — 資訊安全及
個資保護管理能力

遵守 — 法遵能力

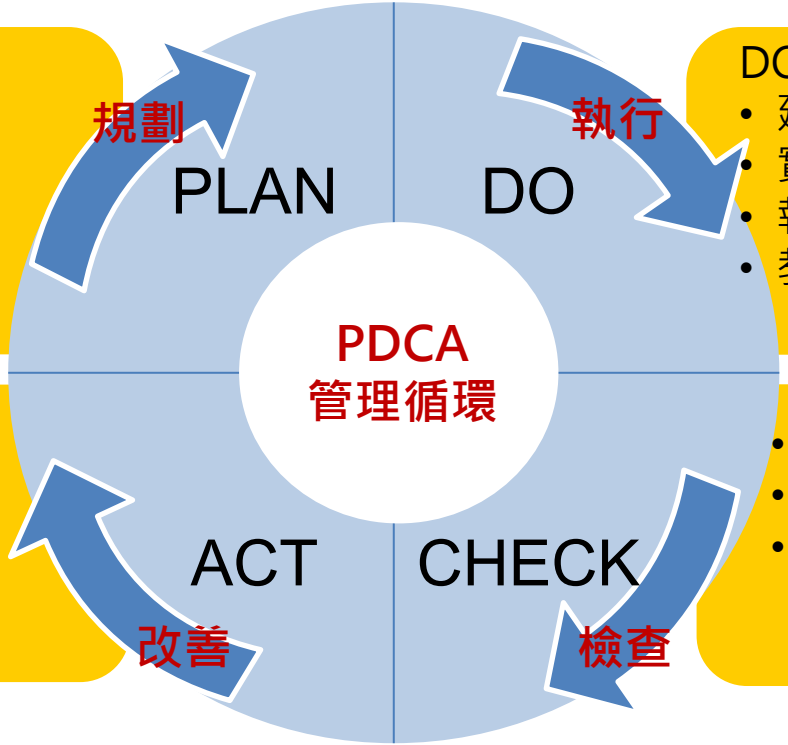
降低 — 營運風險
訴訟風險

提升 — 人員
管理能力

PDCA的管理循環

PLAN
- 確認範圍及目標
- 風險評估
- 選擇控制目標與措施

DO
- 建立管理程序
- 實施風險評鑑
- 執行管理程序
- 教育訓練及宣導



ACT
- 執行適當修正
- 實施成果報告
- 確認目標達成
- 持續改善

- CHECK
- 績效評估量測
- 紀錄追蹤及檢討

醫院資訊安全與個資保護規範

國內法規

- 醫療法與醫療相關法規
- 個人資料保護法與相關子法
- 資通安全管理法與相關子法 (新法上路)

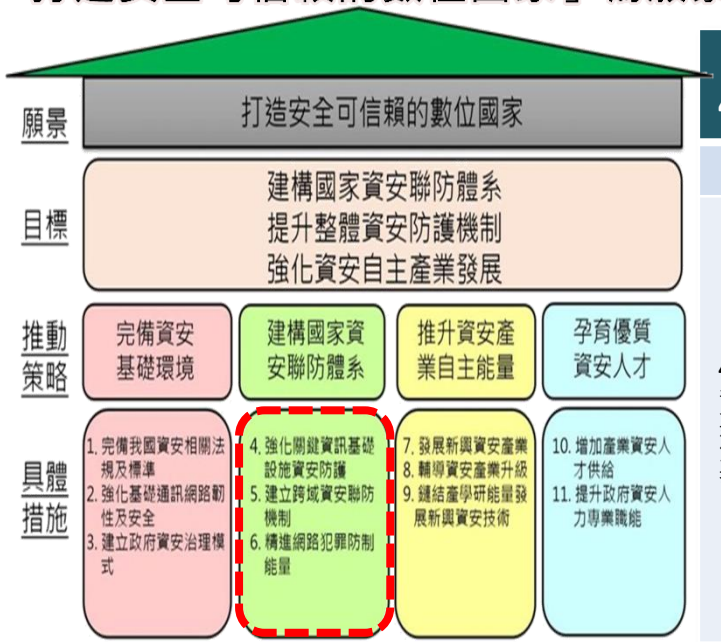
醫院評鑑與管理驗證

- 醫院評鑑基準，列入評量項目
- ISO 27001 資訊安全管理系統(ISMS) 認證
- BS 10012 個人資訊管理制度(PIMS) 認證

新的議題
須遵循中央目的事業主管機關資安政策

衛生福利部資安工作政策

國家資通安全發展方案 (106年至109年)
「打造安全可信賴的數位國家」為願景



國家資通安全發展方案(106年至109年)具體措施
4.強化關鍵資訊基礎設施資安防護

工作項目	分年重要進程
4.2輔導各關鍵資訊基礎設施落實資安防護基準	1.106年底前完成關鍵基礎設施領域資訊分享與分析中心(H-ISAC)建置，107年底前擴大納 管範圍。 2.108年底前完成： (1)所管關鍵基礎設施全數納管加入H-ISAC。 (2)建立關鍵基礎設施領域電腦緊急應變小組(H-CERT)。 (3)建立關鍵基礎設施資安防護策略與防護基準。 (4)完成關鍵基礎設施領域資訊資產盤點與風險評估。 3.109年底前建置關鍵基礎設施領域資訊安監控中心(H-SOC) 。

醫院配合安全防護政策

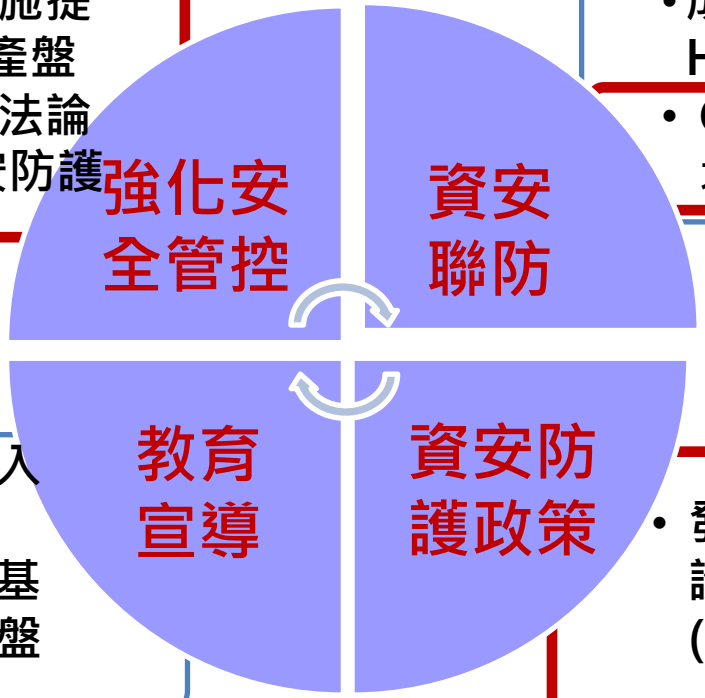
- 建立關鍵基礎設施提供者(CI)資訊資產盤點與風險評估方法論
- 落實CI醫院資安防護

執行

- 成立H-ISAC, H-CERT, H-SOC
- CI醫院加入醫療領域的資安聯防

執行

政策



- 教育訓練醫院加入H-ISAC聯防
- CI醫院執行關鍵基礎設施資訊資產盤點與風險評估

- 發展專屬之資安防護政策與防護基準(遵循資安法)

醫療領域 關鍵基礎設施 資產分類

- 以網絡安全(Cybersecurity)觀點,評估關鍵基礎設施之資通訊安全風險

緊急醫療部門(醫院)
關鍵基礎設施

關鍵基礎設施重點：
- 中斷或停頓影響醫療核心業務
- 中斷或停頓衝擊病人安全

盤點設施

網路安全危害：
- 醫療核心業務
- 病人安全

106
107

Information Technology

Operational Technology

其他設施

關鍵基礎設施
資訊資產(IT)

關鍵基礎設施
醫療儀器設備(OT)

關鍵基礎設施
水、電、氣體等供應

風險評鑑

資安與風險管理
ISO 27001

風險評鑑

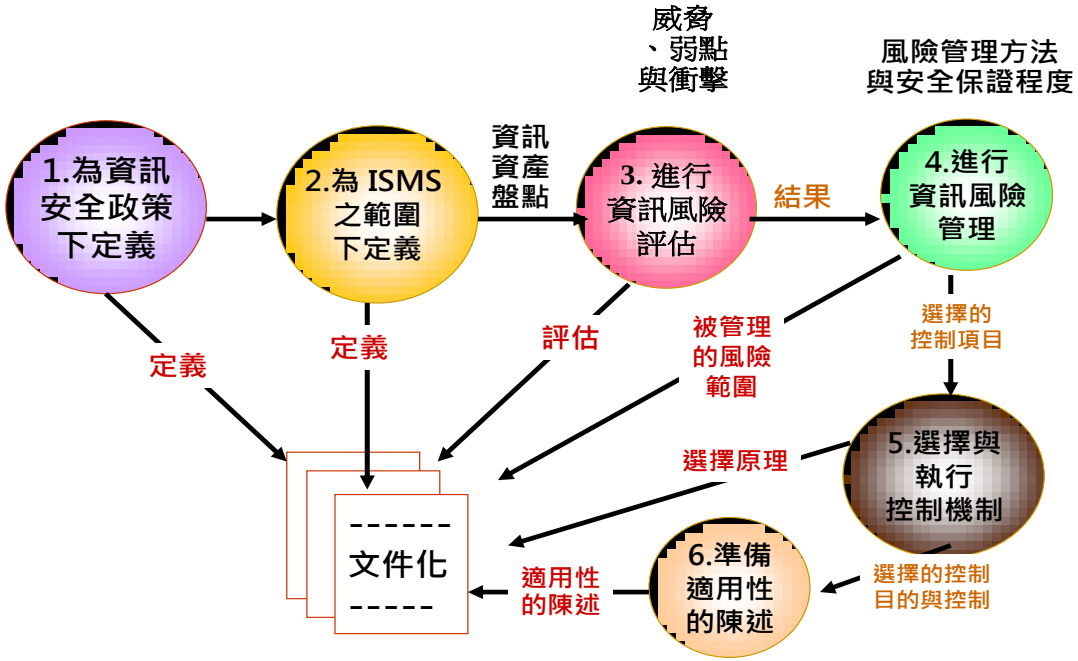
醫療儀器風險管理
TFDA對儀器供應商規範
美國醫療儀器網絡安全指引

風險評鑑

風險管理
醫院評鑑基準之
風險分析與危機管理

醫院資訊資產(IT) 納入 ISO27001 資安管理

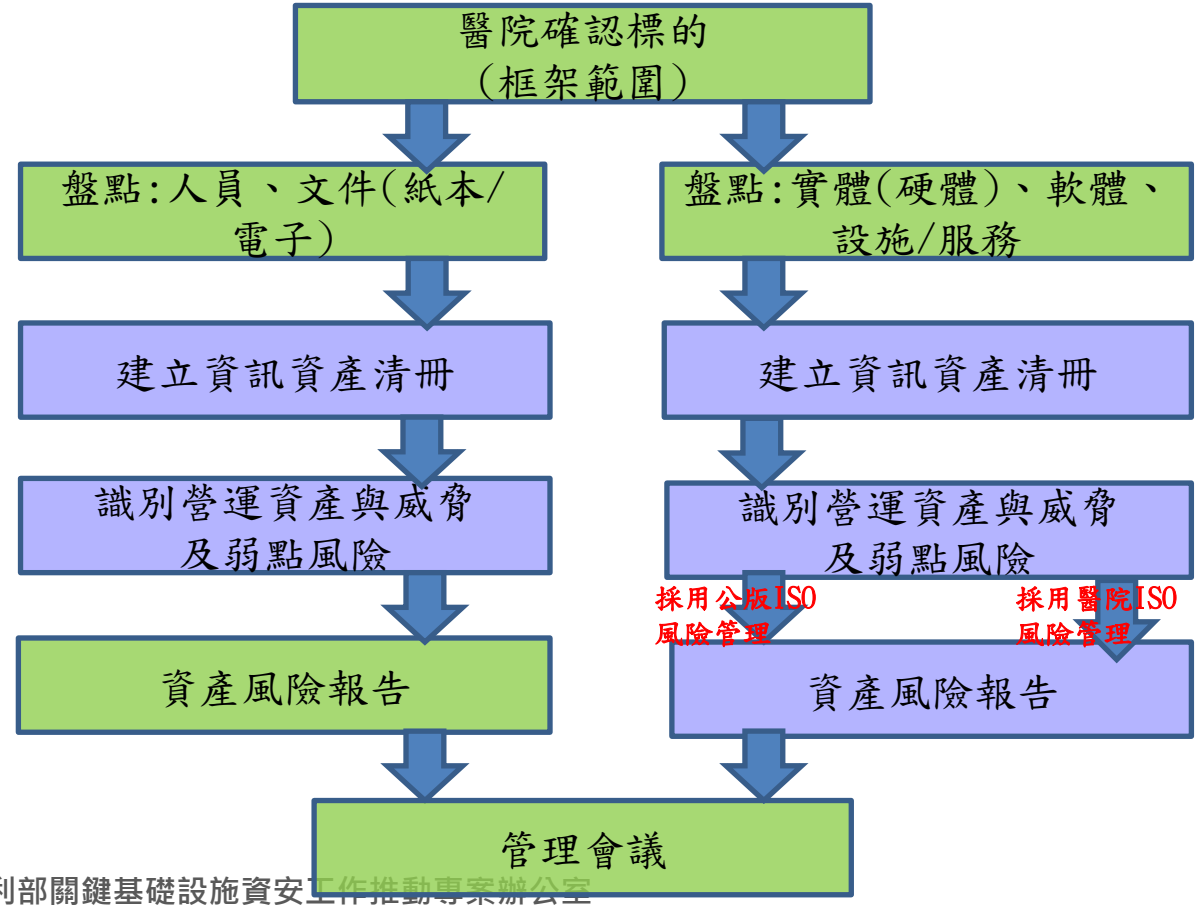
資訊安全管理架構



- 由資訊單位主導
- 驗證範圍以資訊室管轄範圍為主

自2009年起各醫院陸續導入 ISO27001資安管理政策

資訊單位 資訊資產(IT)盤點與風險評估



- 以網絡安全(Cybersecurity)觀點，評估關鍵基礎設施之資通訊安全風險

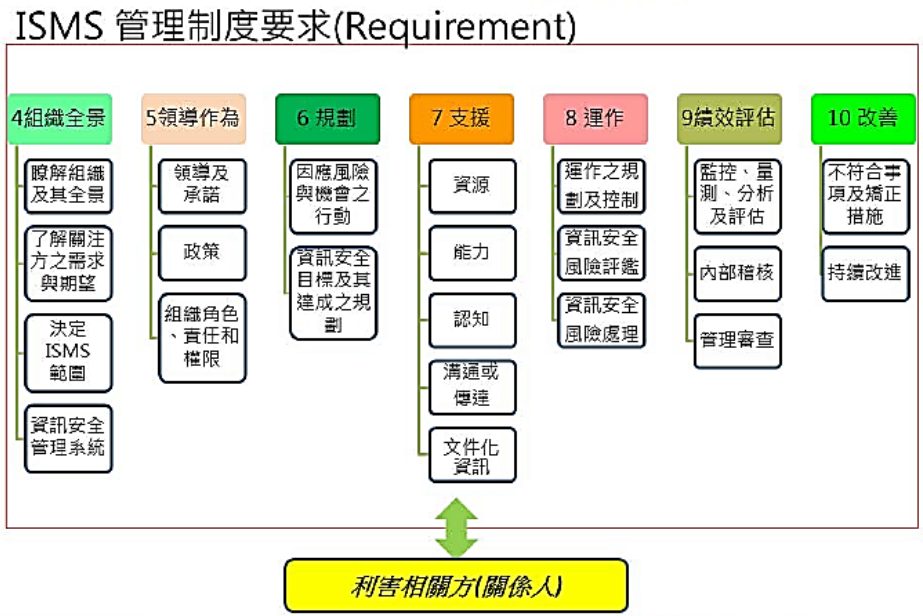
標準: ISO/ISMS 27001
量表: 資訊資產盤點表

標準: ISO/ISMS 27001
參考：威脅及弱點 ISO/IEC 13335
量表: 資產風險評估表

標準: ISO/ISMS 27001
量表: 資產風險評估上傳表一、二

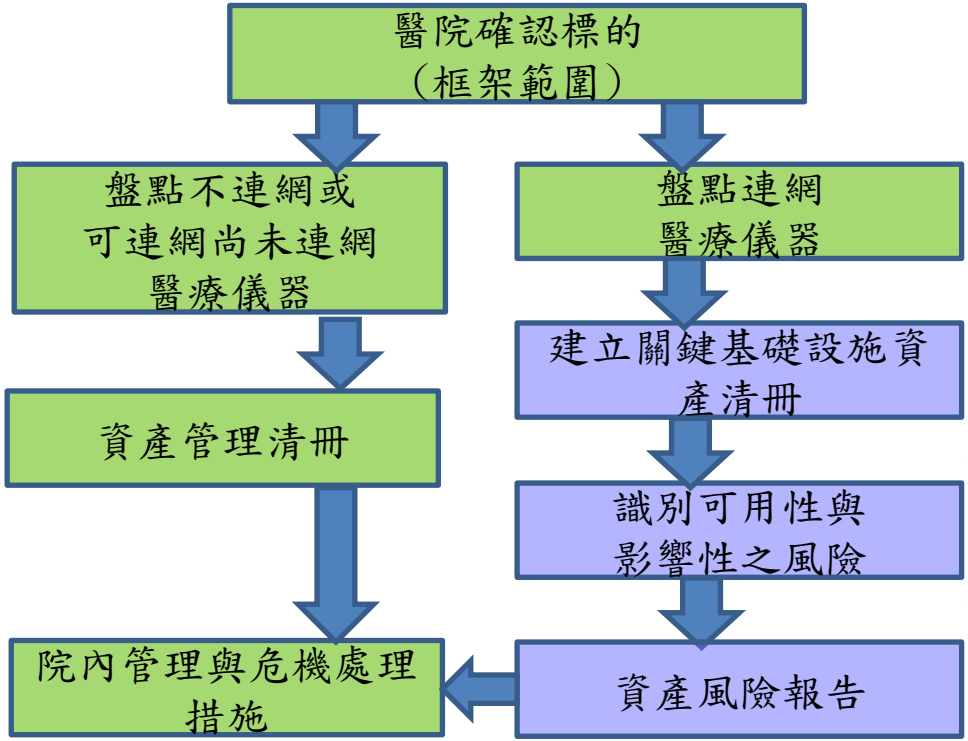
標準: ISO/ISMS 27001
系統: 輔助系統
量表: 資產風險報告表

資安防護遵循 ISO27001本文與附錄A之控制要求



資料來源: 財團法人資訊工業策進會 資安科技研究所

醫工單位 OT 醫療儀器 資產盤點與風險評估



- 現階段以可連網上傳HIS/RIS/LIS/NIS等資訊系統之醫療儀器

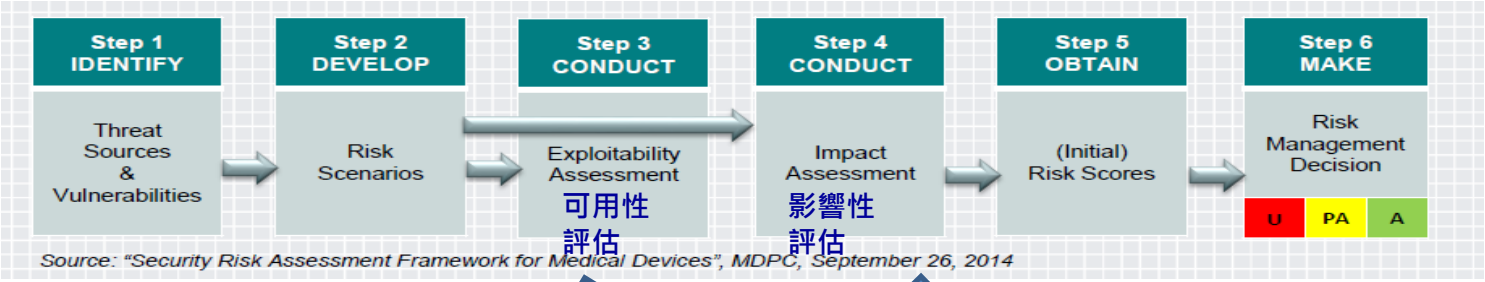
參考：量表：醫療儀器盤點表

可用性：NIST 800-30、ISO 14971之威脅與弱點
影響性：Cybathlon 風險管理病人安全影響
量表：醫療儀器風險評估表

標準：MDPC醫療儀器風險評估白皮書、
Cybathlon組織的風險管理文件
方法：
OWASP *Risk Rating Methodology and Common Vulnerability Scoring System*
系統：輔助系統
量表：資產風險報告表

發展醫療儀器類資安風險評估

- 醫療儀器類風險評鑑方法



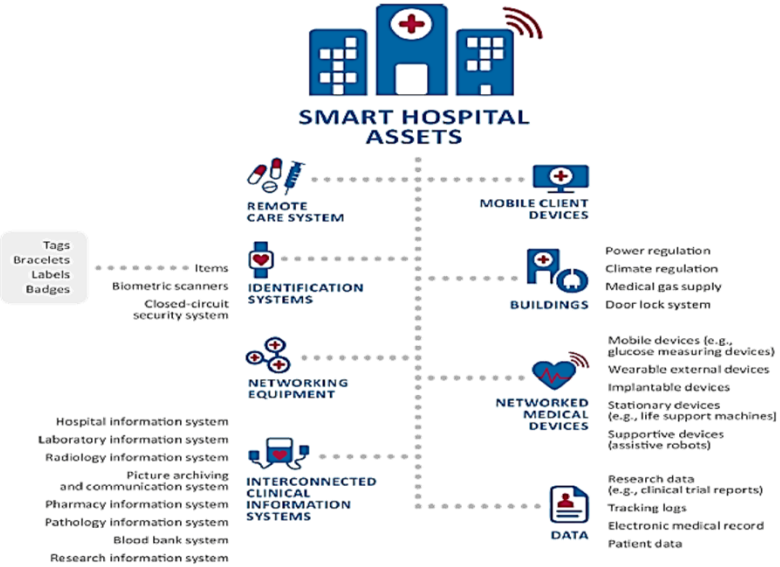
Threat Agent Factors 威脅因素			Vulnerability Factors 弱點因素		
Skill level 技能等級	Motive 動機	Opportunity & Resources 機會與資源	Ease of Discovery & Awareness 發現的難易度	Ease of Exploiting 可用性	Intrusion Detection 入侵偵測
入侵者當下所具備的能力技能。	入侵者成功入侵時，所能獲得的財務或其他可識別的利益(例如成名機會)。	權限等級分類是否夠複雜完備，或入侵者能否輕易取得各類權限與入侵工具資源。	能否輕易察覺安全漏洞	入侵者使用/開發入侵工具的難易度	能否確實記錄、察覺入侵者相關行動資訊。

Impact	Criteria: Severity of effect
權值	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

- 威脅為外部因素，評估因子有技能等級、動機、機會與資源3項。
- 弱點為內部因素，評估因子有發現難易度、可用性與入侵偵測3項。

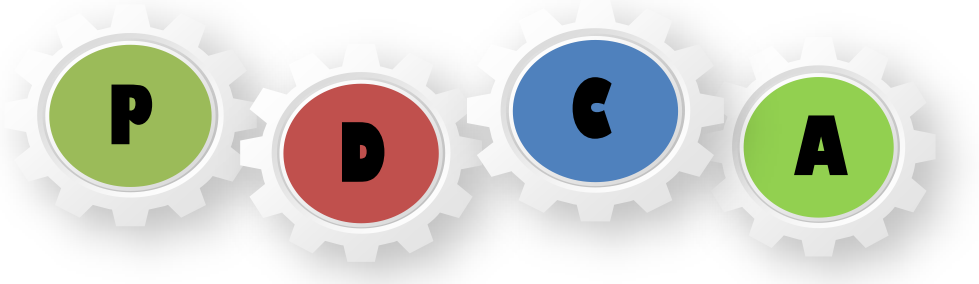
醫療領域 關鍵基礎設施 OT連網分類

- **連網醫療儀器**
  - Physiologic monitors and system (生理監視器與系統)
  - Defibrillators (除顫器)
  - Infusion pumps (輸液泵)
  - Anesthesia units (麻醉機)
  - Ventilators (呼吸機)
  - Extracorporeal Assist (體外輔助儀器)
  - Vital sign monitors (生命徵象監視器)
  - Digital Radiographic X-Ray System(數位X光攝影系統)
  - CT & MRI scanners (CT和MRI掃描儀器)
  - Nuclear Machine (核子醫學設備)
  - Fetal monitors (胎兒監視器)
  - Laboratory analyzers (實驗室分析儀器)
  - Diagnostic ultrasound (超音波診斷儀器)
  - Electrocardiographs (心電圖儀器)
  - Injectors, contrast media (注射器，造影劑)
  - DIALYSIS MACHINE(透析機)
  - Others (其他)



ENISA, European Union Agency for Network and Information Security, "Cyber security and resilience for Smart Hospitals," 2016/11/24,

各個醫院的資訊安全防護進度概況



IT 資產 (資訊單位管理) ISO 27001 資訊管理

PDCA持續管理循環檢討改善

OT 資產(醫工單位管理) 風險評估

在盤點與風險評估階段

現況醫療儀器資安風險評估的瓶頸

- 資產清單取得難易度

  保養工時系統、HIS系統資產下載或其他，盤點困難醫工人力不足

- 盤點及評估人力

  醫療儀器本身的作業系統調查—花時間

  風險評估須會同三方：

  廠商提供系統資訊+資訊單位資安專業+ 醫工單位整合評估

- 資訊醫工部門取得共識(資訊作為窗口，醫工落實評估)

  資訊安全及病人安全兼得

醫療領域關鍵基礎設施(CI)醫院安全管理進度

- 關鍵基礎設施指定醫院 64家

CI醫院加入H-ISAC

42家 65.6%

CI醫院完成 IT資產資訊安全防護

42家 65.6% (餘22家尚未加入執行情形待追蹤)

CI醫院完成 OT資產資訊安全防護

執行情形待追蹤

CI醫院完成其他類資產資訊安全防護

執行情形待追蹤

註: 關鍵基礎設施醫院由衛生福利部指定並完成核定程序公告。
醫療照護的關鍵基礎設施為：
1. 醫療核心業務不能中斷或停頓。
2. 醫療核心業務不能危及病人安全。

資訊安全防護之未來進展與醫療領域持續關注之議題

辦理法遵事項：擬定資通安全維護計畫

- 資通安全管理法施行細則 第六條明訂應包含事項：
  - 一、 核心業務及其重要性。
  - 二、 資通安全政策及目標。
  - 三、 資通安全推動組織。
  - 四、 專責人力及經費之配置。
  - 五、 公務機關資通安全長之配置。
  - 六、 資訊及資通系統之盤點，並標示核心資通系統及相關資產。
  - 七、 資通安全風險評估。
  - 八、 資通安全防護及控制措施。
  - 九、 資通安全事件通報、應變及相關機制。
  - 十、 資通安全情資之評估及因應機制。
  - 十一、資通系統或服務委外辦理之管理措施。
  - 十二、 公務機關所屬人員辦理業及資通安全事項之考核機制。
  - 十三、 資通安全維護計畫及實施情形之持續精進及績效管理機制。

包括院內通報處理程序及院外通報規定

擴大醫療領域關鍵基礎設施資產盤點與風險評估範圍

- 以網絡安全(Cybersecurity)觀點,評估關鍵基礎設施之資通訊安全風險

緊急醫療部門(醫院)關鍵基礎設施

關鍵基礎設施重點：
- 中斷或停頓影響醫療核心業務
- 中斷或停頓衝擊病人安全

全院

盤點設施

網路安全危害：
- 醫療核心業務
- 病人安全

108

Information Technology

Operational Technology

其他設施

擴大IT與OT範圍

106~107年

關鍵基礎設施
資訊資產(IT)

關鍵基礎設施
醫療儀器設備(OT)

關鍵基礎設施
水、電、氣體等供應

風險評鑑

資安與風險管理
ISO 27001

風險評鑑

醫療儀器風險管理
TFDA對儀器供應商規範
美國醫療儀器網絡安全指引

風險評鑑

風險管理
醫院評鑑基準之
風險分析與危機管理

醫療領域關鍵基礎設施(CI)醫院安全管理目標

- 關鍵基礎設施醫院指定 64家

CI醫院加入H-ISAC
42家

100%醫院加入

CI醫院完成 IT資產資訊安全防護
42家

100%醫院達成

CI醫院完成 OT資產資訊安全防護

完成盤點與風險評估並逐步導入資安防護措施

CI醫院完成其他類資產資訊安全防護

完成盤點與風險評估並逐步導入資安防護措施

註: 關鍵基礎設施醫院由衛生福利部指定並完成核定程序公告。

資安合規應檢視項目與內涵

- 資訊架構檢視
  - 評估網路架構之配置、資訊設備的管理方式和單點故障的風險承擔能力，以及組織對於營運持續採取的相關措施
- 網路活動檢視
  - 包括網路相關設備的帳號權限管理和存取記錄、設備的監控與異常事件的處理，以及檢視網路封包是否存在網路異常連線和惡意行為
- 網路設備、伺服器及終端機等設備檢測
  - 檢測設備的存取和連線機制、是否定期實施弱點掃描和修補作業，以及檢測是否存在惡意程式程後門程式
- 網路安全檢測
  - 包括網站和客戶端軟體的弱點掃描、程式源碼的檢測、滲透測試，以及評估網站日誌權限設定的適當性檢視系統是否存在可能易遭連線挾持程資源消耗等影響系統可用的情況
- 安全設定檢視
  - 包括系統存取限制和特權管理、伺服器的設定原則、軟體更改、防火牆的連線設定以及金鑰的儲存保護和存取機制等
- 合規檢視
  - 檢視整體的電腦系統是否符合標準或法令法規要求之要求

技術面問題

醫療儀器面臨

資料來源: 財團法人資訊工業策進會 資安科技研究所

醫療儀器資安合規的難題

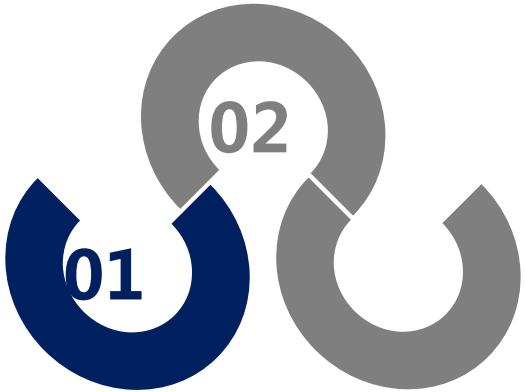
醫療儀器以可用性、穩定性為首要

資料來源: 財團法人資訊工業策進會 資安科技研究所

醫院現行提出資安風險改善建議作法

- 加裝防毒軟體
  → 透過資訊部門或儀器廠商提供
- 單機或區域加裝硬體防火牆
  → 醫工部門申請裝設
  → 資訊部門協助設定
- 汰舊換新
  → 考量使用單位汰換時程、預算
- 其他措施
  → 如門禁管制、人員帳密、儀器使用管理、強化人員資安認知教育宣導等

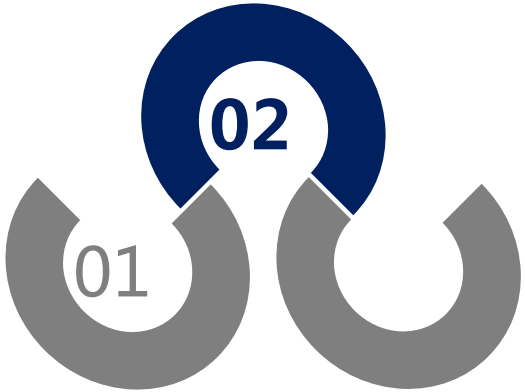
醫療領域持續關注 儀器安控議題



1 醫療儀器類資安控制措施受限

- 醫療儀器為支援醫療診斷、治療與處置，以可用性為主要考量，資安控制措施須遷就實務開題調整：
  - 設備使用年限可達10~15年，作業系統如為舊作業系統，升級後無法確保原設備之效能與穩定時多選擇維持原狀態，尋求其他可行防護措施
  - 大型設備多為國外進口，受限原廠或代理商維護合約，醫院等待配合原廠提供上PATCH、安裝防毒軟體或系統升級

醫療領域持續關注 人才議題



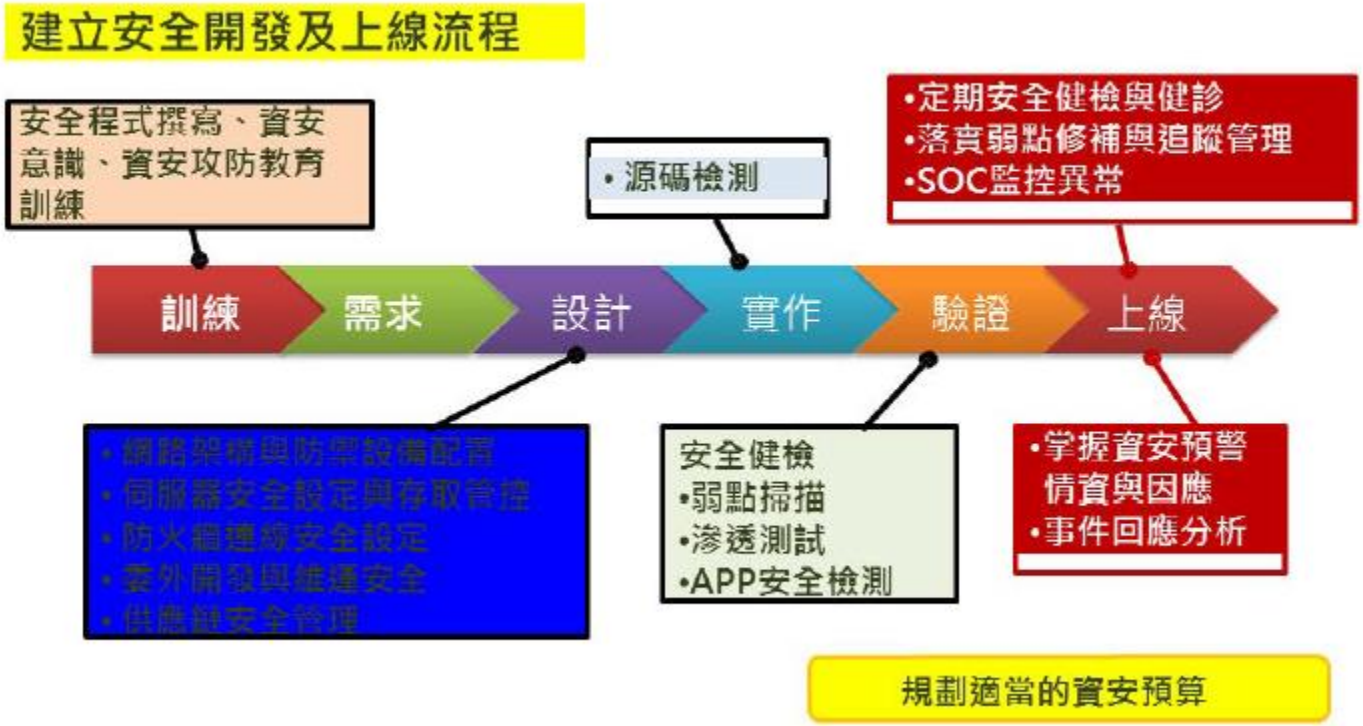
2 資訊單位資安人才不足

- 醫療領域包含CIP與CIIP。
- 醫院關鍵基礎設施涵蓋資訊、醫療設備、工務、藥劑等設施，各有不同領域的專業技術，除資訊有資安專業人員，其餘領域的專業人員對資安欠缺專業知識。
- 資訊單位的資安人員由原先CIIP，擴大涉及全院關鍵基礎設施之CIP，技術人員面將臨支援問題
- 資安情資判斷面將挑戰，未來跨領域須IT與OT合作，如何適當分工缺乏實務經驗待摸索

醫院資訊安全防護之建議

- 擴大執行資訊設備、儀器或應用軟體進行資安檢測
- 擴大資安人才培育、引進自動化偵測簡化人力監控
- 物聯網設備檢測 (如網路攝影機、門禁系統、網路印表機)
- 現有之醫療儀器建立合適且可行的資安防護措施
- 未來請購資訊設備、應用軟體、醫療儀器或行動裝置設備加入資安防護、資安檢測報告或相關文件之要

專家建議：關鍵防護之鑰1—建立安全開發週期



資料來源: 財團法人資訊工業策進會 資安科技研究所

專家建議：關鍵防護之鑰2—落實資產與弱點管理

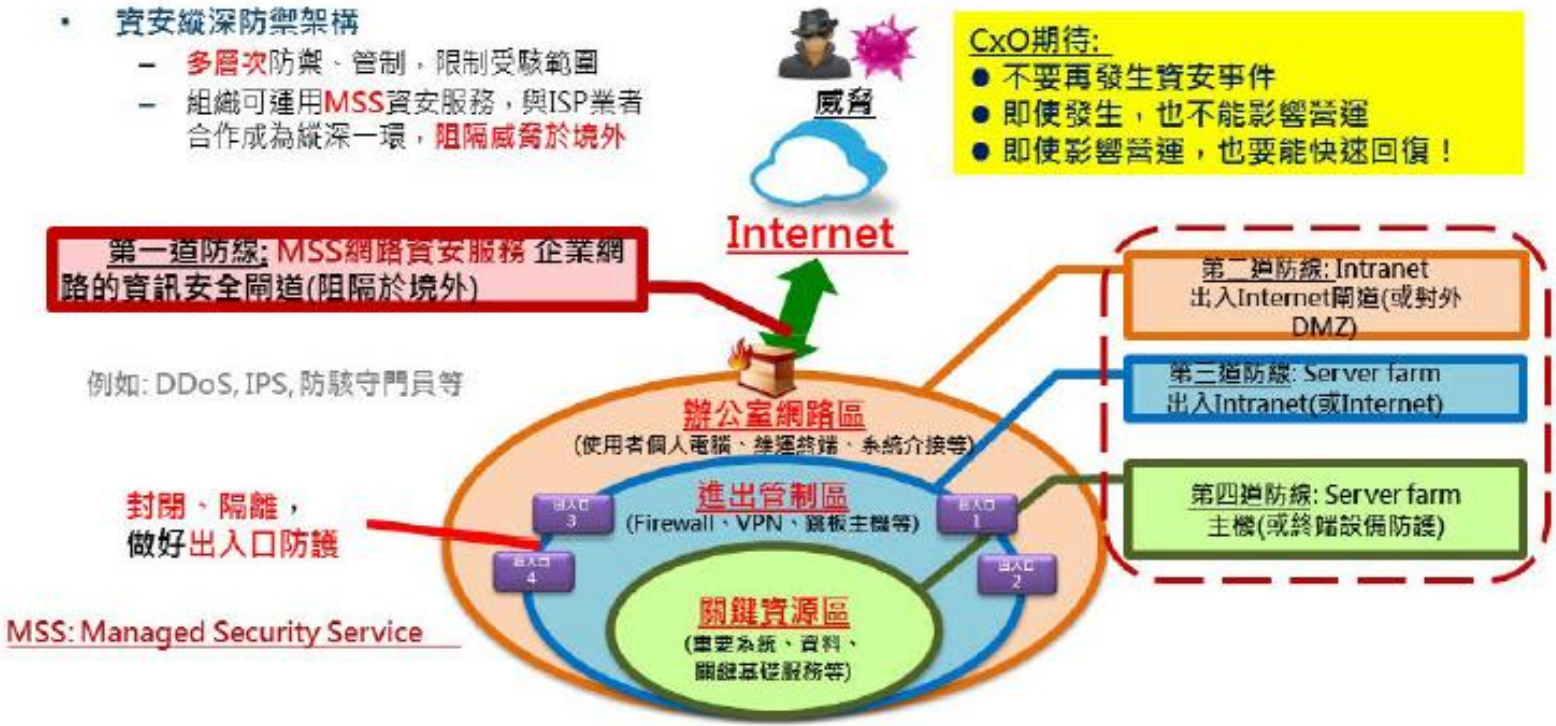
導入弱掃管理平台 –落實弱點修補有效性

- 整合系統/網頁掃描商用軟體，自動化排程弱點掃描
- 系統化追蹤管理各單位的弱點處理狀況，有效降低人力
- 可自動複檢落實弱點修補的有效性
- 系統管理者可隨時自檢，確認上線系統無已知弱點

資料來源: 財團法人資訊工業策進會 資安科技研究所

專家建議：關鍵防護之鑰3—資安縱深防禦架構

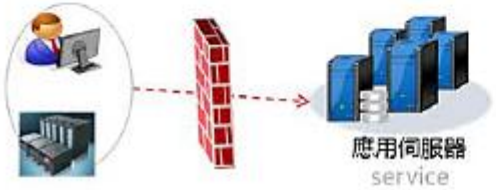
- 資安縱深防禦架構
  - 多層次防禦、管制，限制受駭範圍
  - 組織可運用MSS資安服務，與ISP業者合作成為縱深一環，阻隔威脅於境外



資料來源: 財團法人資訊工業策進會 資安科技研究所

專家建議：建構OT系統安全白環境

- 持續監控收集，即時探測，判斷、取證、溯源、修復；
- 被動解決方案，不影響OT系統的“可用性”和“穩定性”
- OT協議深度解析技術，具備高安全性，低時延影響
- 建構白名單
  - 可信任的設備才能接入控制網路
  - 可信任的資訊才能在網路上傳輸
  - 可信任的軟體才允許被執行



資料來源: 財團法人資訊工業策進會 資安科技研究所

結 語

醫療機構必須：

- 建立完整的防護系統來減輕管理、財務和道德風險
- 改善工作流程和提升員工效率，加強保護健康醫療隱私和網路安全，使照護的病人免於遭受資安攻擊導致危害

「以卑謙之敬畏
謀偉大之不畏」

— 認識自己的長處和不足，虛心聽取不同意見，學習不斷提升，
做事謹慎不懈怠，為尋求遠大的志向、見解而不畏懼。

臺灣資安大會
CYBERSEC 2019

PRESENTED BY iThome