醫療資安政策

衛生福利部資訊處處長龐一鳴

從公共衛生的口號看資安

- 病從口入
- 隔離檢疫/零信任
- 預防勝於治療
- 早期診斷早期治療

公共衛生與預防醫學的三段五級策略

醫療資安的三段五級策略

無症狀/
被刺探

出現弱點
資安事件

資料遺失
橫向擴散
系統癱瘓

健全體質
情資蒐集

弱點掃瞄
特殊防護

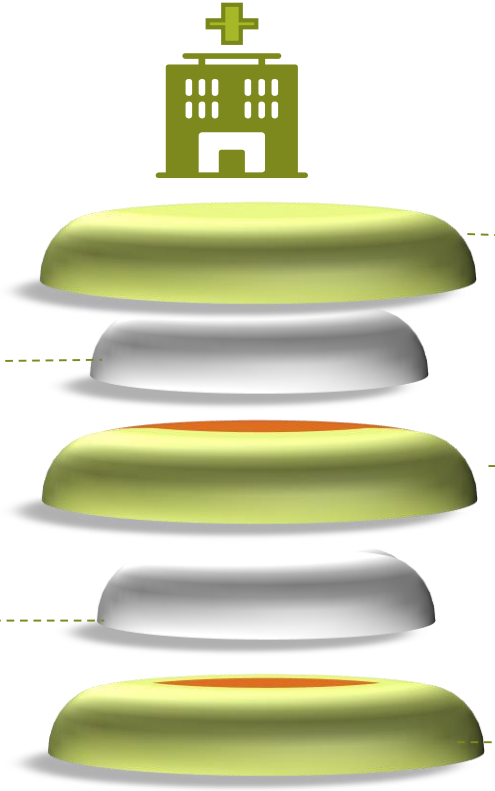
資安健檢
監控機制(SOC)
即時修補

通報應變機制
(ISAC,CERT)

復原
鑑定

醫院保護的範疇

醫院



設施

實體環境安全
儀器合於規範
儀器維護安全
系統運作正常
系統備援與緊急應變

健保

健保資料傳輸安全
健保IC卡合規與隱私保護
健保VPN專網

人

人員職照有效
儀器與設備安全操作
病人就醫安全
病人隱私維護

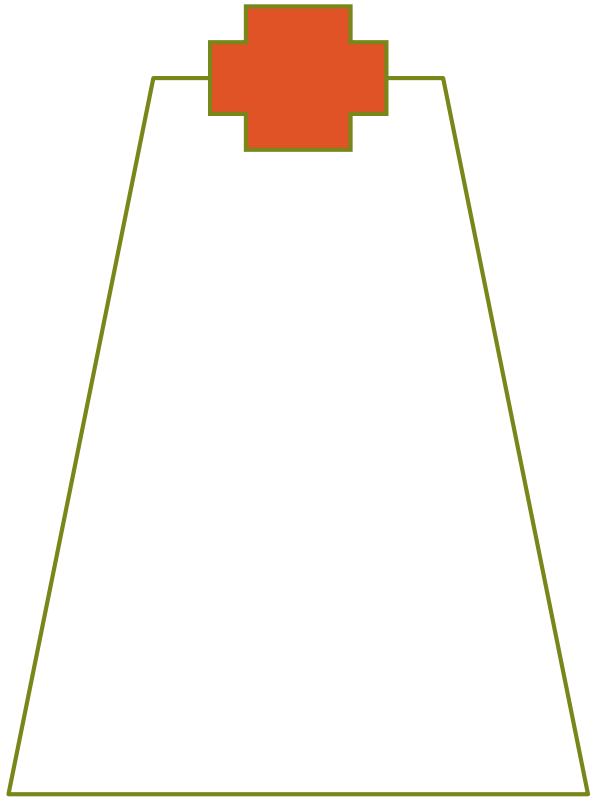
服務流程

服務流程不中斷
流程安全有效
有效的緊急應變處理流程

資料

保護資料安全
確保資料的正確性
確保資料處理及利用符合蒐集的目的
資料備份處理

是白色巨塔還是巴黎鐵塔?



來源：自由時報，https://news.ltn.com.tw/news/world/breakingnews/1124148

醫療資安法規架構

醫療法、醫療器材法及相關法規

一、以專業為對象
二、對機構、人員、設備、業務、服務等進行管理
三、保障人民權益、安全、品質
四、評鑑

+

個資法

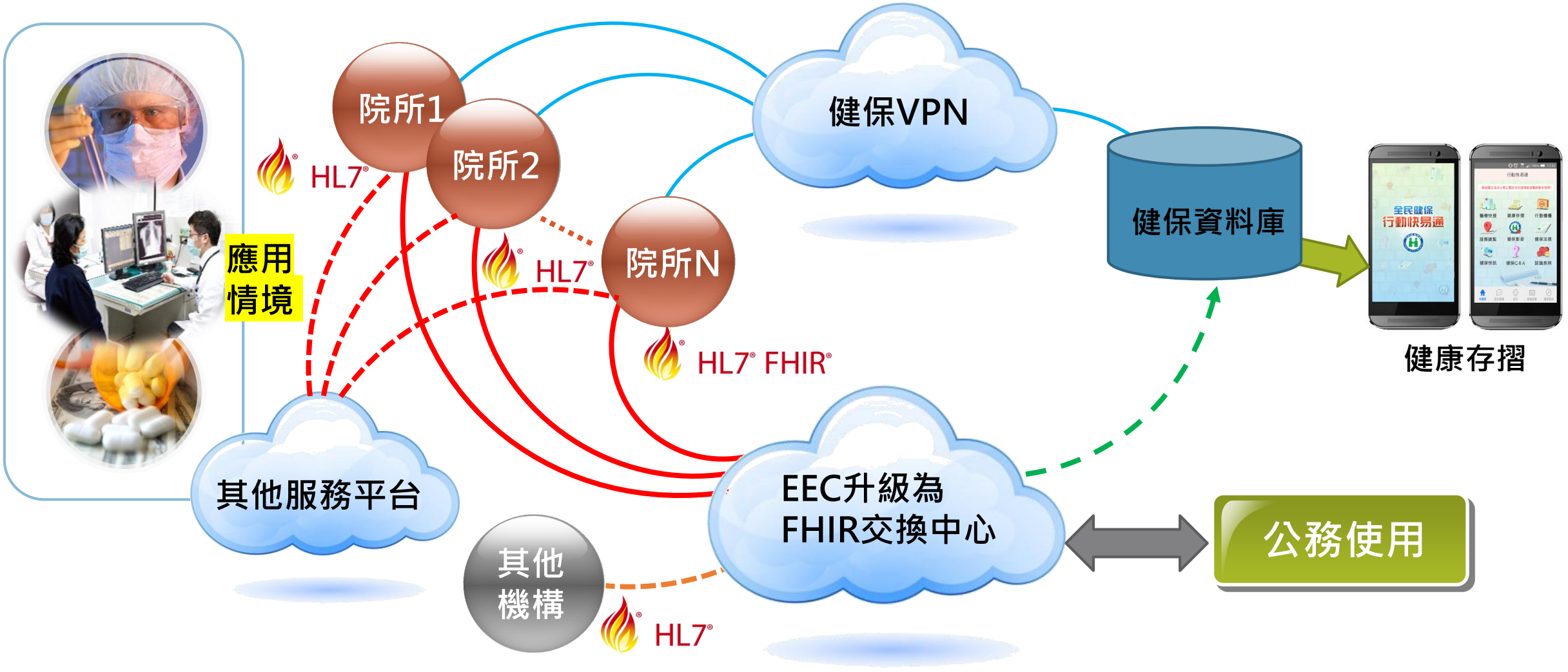
一、廣泛適用
二、定義特種個資
三、公務機構、非公務機關
四、安維辦法

+

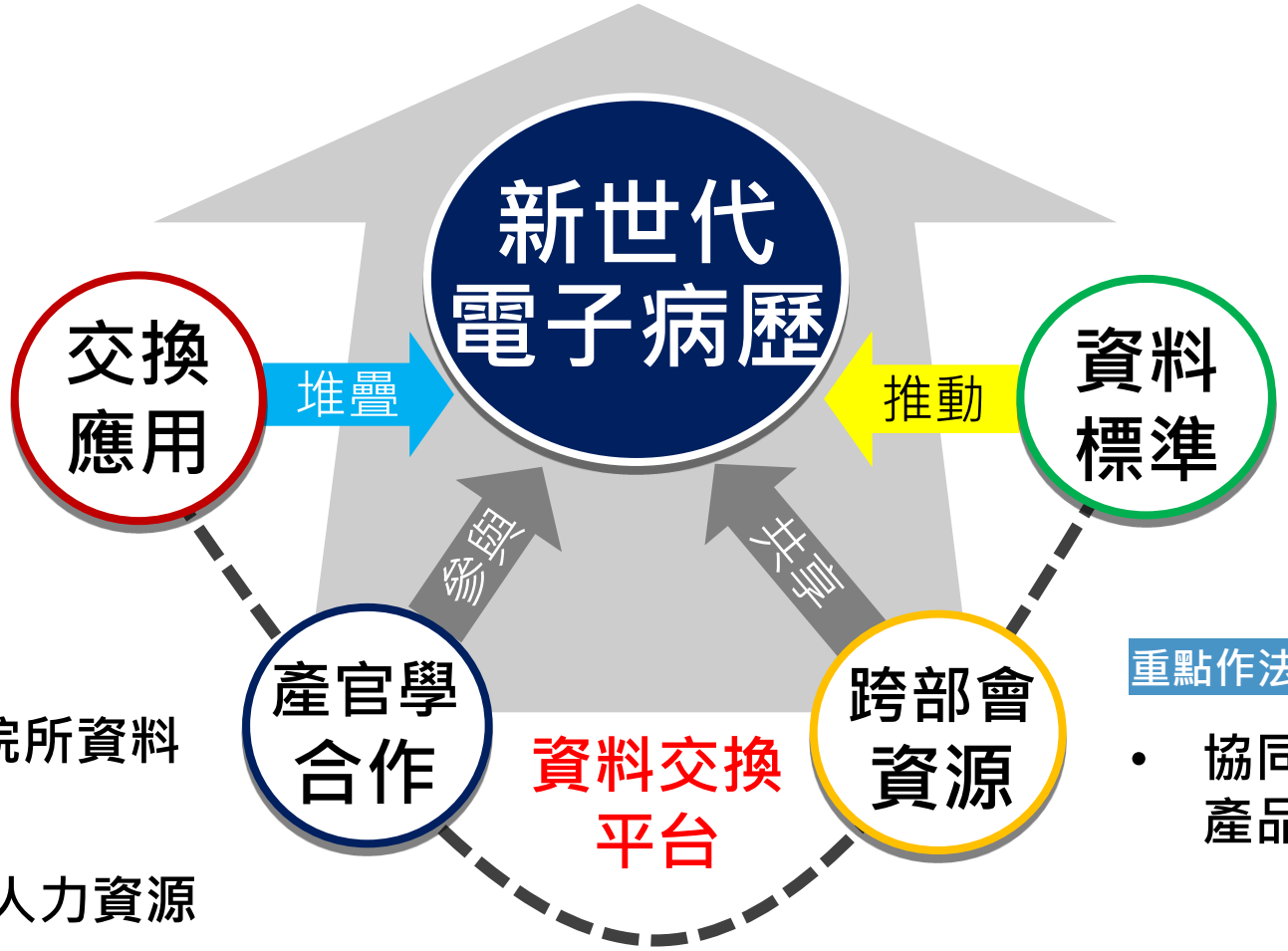
資安法

一、聯防體系、責任分級
二、公務機構、特定非公務機關
三、安維計畫、通報、稽核

電子病歷交換架構及平台的改革



健康資料在HL7-FHIR架構下，加速資料交換互通，增進加值應用



重點作法

- 發展交換平台
- 試作疫苗護照等應用

重點作法

- 新舊標準平行轉移
- 部內資料交換電子病歷化

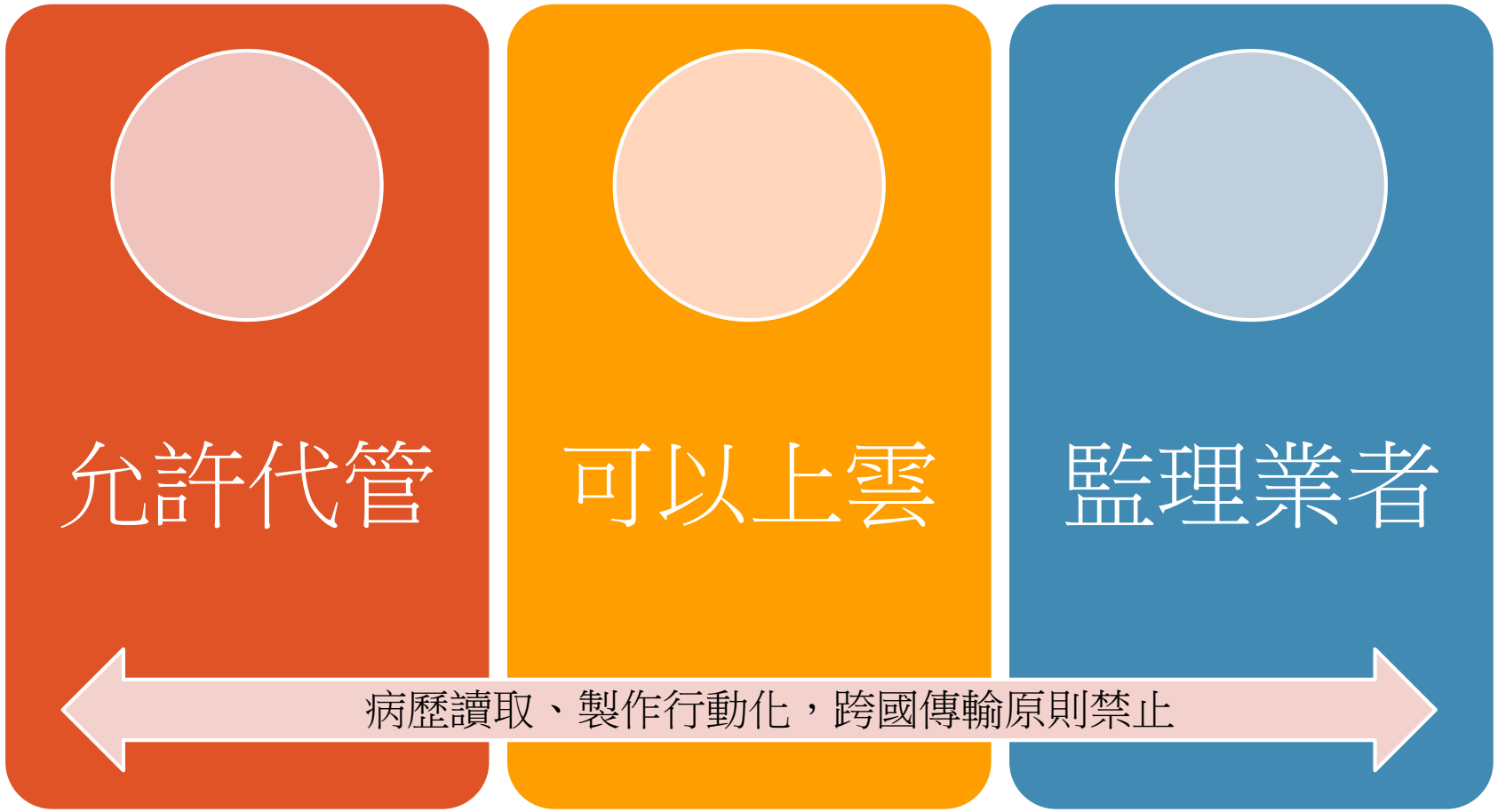
重點作法

- 發展醫療院所資料轉換工具
- 建構FHIR人力資源

重點作法

- 協同經濟部補助聯測及產品服務等資源

電子病歷存取的改革



持續推醫院資安改善及法遵事項

1. 以資通安全管理法無法推動全面醫療聯防與資安防護，擬推動醫院評鑑制度納入相應要求，建議提供更多誘因吸引更多醫療院所加入聯防機制 (Membership expansion)
2. 逐步要求醫療資訊供應業者有資安防護措施或說明防護機制，提升醫療資訊業者之資安意識 (Increasing cybersecurity awareness of both members and their vendors)
3. 投入資源協助更多醫療院所提升資安能力，特別是人才的培訓 (Add more resource to enhance members' cyber threat defense capability, especially for personnel training)
4. 積極與其他部會及地方政府協商加強聯防機制 (Cross-domain alliance)
5. 辦理**資安稽核**，修改評鑑標準

辦理
醫療資安事件通報應變處理、社交工程防制模擬演練

- 警訊發布與回覆

  H-ISAC發布演練警訊(需回覆)

  -> 收到警訊之會員機構進行警訊回覆

- 通報作業

  H-ISAC發布演練警訊(需回覆)

  -> 進行通報作業

◆ 針對至少10間醫院進行社交工程模擬演練

◆ 各自出具社交工程模擬演練報告並提供綜整版本予部內

No.	類型	標題
1	財經	用貸款「零本金退休」？專家抱持質疑
2	休閒	嚴選全台10大「海水浴場」第1名竟然不是墾丁！
3	休閒	只要50元！這間冰店讓你隨意裝 吃完還能再加冰
4	保健	5種高熱量食物 但減肥的你更應該吃！
5	保健	青少年腰痛不是腎！小心是運動過度脊椎解離症
6	新奇	富爾地鐵「炸雞」拉環 網友：看到都餓了

資料來源：關鍵基礎設施資訊安全聯防機制與H-SOC建置計畫案

納入醫療儀器生命週期的資訊安全管理

Life Cycle of Medical Device Management
醫療儀器全生命週期資安管理

Recent Ransomware Events

	UK 2017/5/12	Taiwan 2019/8/29	Germany 2020/9/18	Taiwan 2020~now
Action	Blackmail, WannaCry	Blackmail, WannaCry deriver	Blackmail	Blackmail
Motivation	Financial	Financial	駭客的攻擊目標也許是杜塞道夫大學	
Victims	80/236 trusts, 603 organizations	**38 hospitals** (66 was said but unverified)	杜塞道夫大學醫院（Duesseldorf University Hospital）	2020/2 北部某區域醫院 2020/10北部某地醫院 2021/1 中部某區域醫院 2021/3 南部某醫學中心 2021/4某醫療體系
Affected	Cancel 20000 hospital appointments and procedures, close 5 emergency units	None reported	關閉急診室，使得該院必須將一名急診病患轉至20英里（32公里）外的醫院，造成該名病患死亡，而這很可能是全球首起因勒索軟體攻擊而致死的案件	None reported
Weakness	MS-Windows version and upgrade	Official: VPN management, assets management Individual: Weak code, remote services	Citrix ADC(VPN) CVE-2019-19781	
Lesson	Target of Modernization	Scope of ISMS, Policy of EEC		

面對勒索病毒的威脅

80%的攻擊

落實資安長制度

- 資安長親自主持資安會議
- 協調跨部門(資訊、醫工、工務)資安推動工作

拒絕釣魚郵件

- 社交工程攻擊是突破防守的最佳捷徑
- 切勿讓人員的不注意成為資安破口

網路防火牆

- 讓網路防火牆阻絕境外的惡意攻擊及試探
- 管理及監控遠端存取，包含供應商
- 應用白名單進行管制

USB管控

- 電子業受駭案例，殷鑑不遠
- USB隨身碟為病毒傳播媒介
- 有限使用USB並監控管理

20%的攻擊

IT防禦

- 善用H-ISAC情資分享—勒索軟體防護攻略，打造防駭狙擊封鎖線
- 以有效的管理杜絕大多數的攻擊嘗試，讓IT有餘力應付高明的駭客，不致因層出不窮的事件疲於奔命
- 支持IT採行各項資安縱深防禦工具及技術
- 導入資訊安全管理制度落實執行

醫院對抗網攻的夥伴– H-ISAC

- ✓ 資安事件通報[不限公務機關或CI提供者]
- ✓ 更多勒索軟體防護資訊，請參閱H-ISAC資安訊息情報
- ✓ 衛生福利部資安資訊分享與分析中心(H-ISAC)

網址 https ://hisac.nat.gov.tw/

電話：0809-070-166 (緊急通報專線)

電子郵件 : hisac-cs@mohw.gov.tw

衛生福利部資安資訊分享與分析中心
Hospital Cybersecurity Information Sharing and Analysis Center

資安訊息情報

5.0 ★★★★★

勒索軟體攻防戰！3分鐘讀完攻略，打造防駭狙擊封鎖線

發布單位 : 衛生福利部　日期 : 2021-03-16

發現時間 ：2020-05-19
影響等級 ：低

中油、台塑、力成等台灣大型企業去年接連遭到勒索軟體攻擊，不只是導致中油內部網路系統無法正常運作，所屬的捷利卡、中油PAY一度暫停使用，封測大廠力成的生產作業也因此一度停擺，而這些都還只是冰山的一角。