



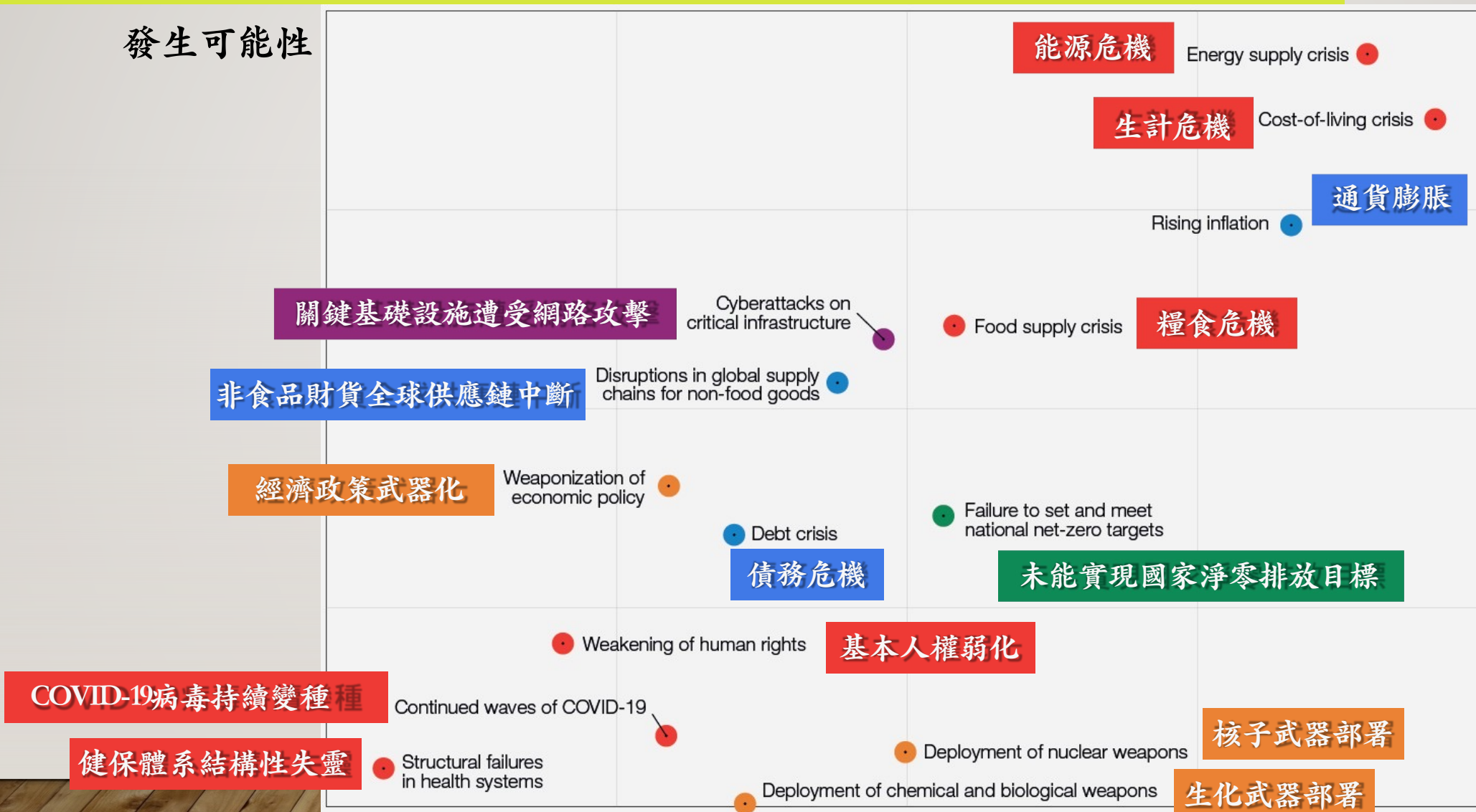
中央警察大學 一般人員教育訓練課程 資安威脅趨勢及防護策略

劉朝華

- 資安威脅趨勢
 - WEF 2023全球風險報告
 - 全球資安威脅趨勢
 - 政府資安威脅趨勢
 - 政府資安事件案例
- 資安管理原則
- 資安防護重點

2023年全球重大風險

發生可能性



全球短、長期預期風險

短期(2年)

長期(10年)

1	生計危機
2	自然災害與極端天氣事件
3	地緣經濟對峙
4	未能減緩氣候變遷
5	社會凝聚力削弱與兩極化
6	大規模環境破壞事件
7	未能適應氣候變遷
8	大型網路犯罪與危機
9	自然資源危機
10	大規模非自願遷徙

1	未能減緩氣候變遷
2	未能適應氣候變遷
3	自然災害與極端天氣事件
4	喪失生物多樣性及生態系崩潰*
5	大規模非自願遷徙
6	自然資源危機*
7	社會凝聚力削弱與兩極化
8	大型網路犯罪與危機
9	地緣經濟對峙
10	大規模環境破壞事件

政府與企業對於短期風險預測差異

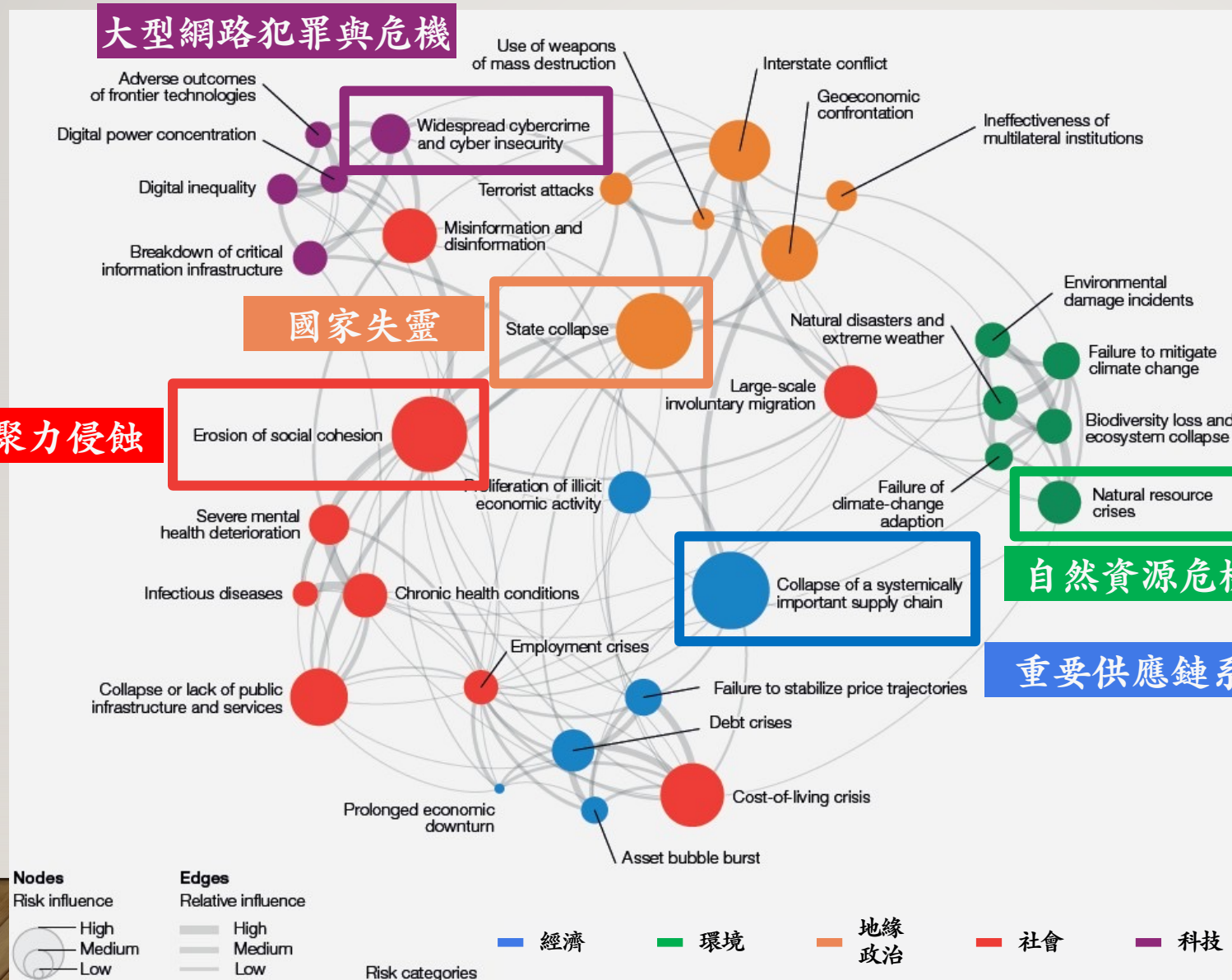
政府

1	生計危機
2	自然災害與極端天氣事件
3	未能減緩氣候變遷
4	地緣經濟對峙
5	未能適應氣候變遷
6	債務危機
7	社會凝聚力削弱與兩極化
8	市場價格波動*
9	大型網路犯罪與危機
10	長期經濟衰退*

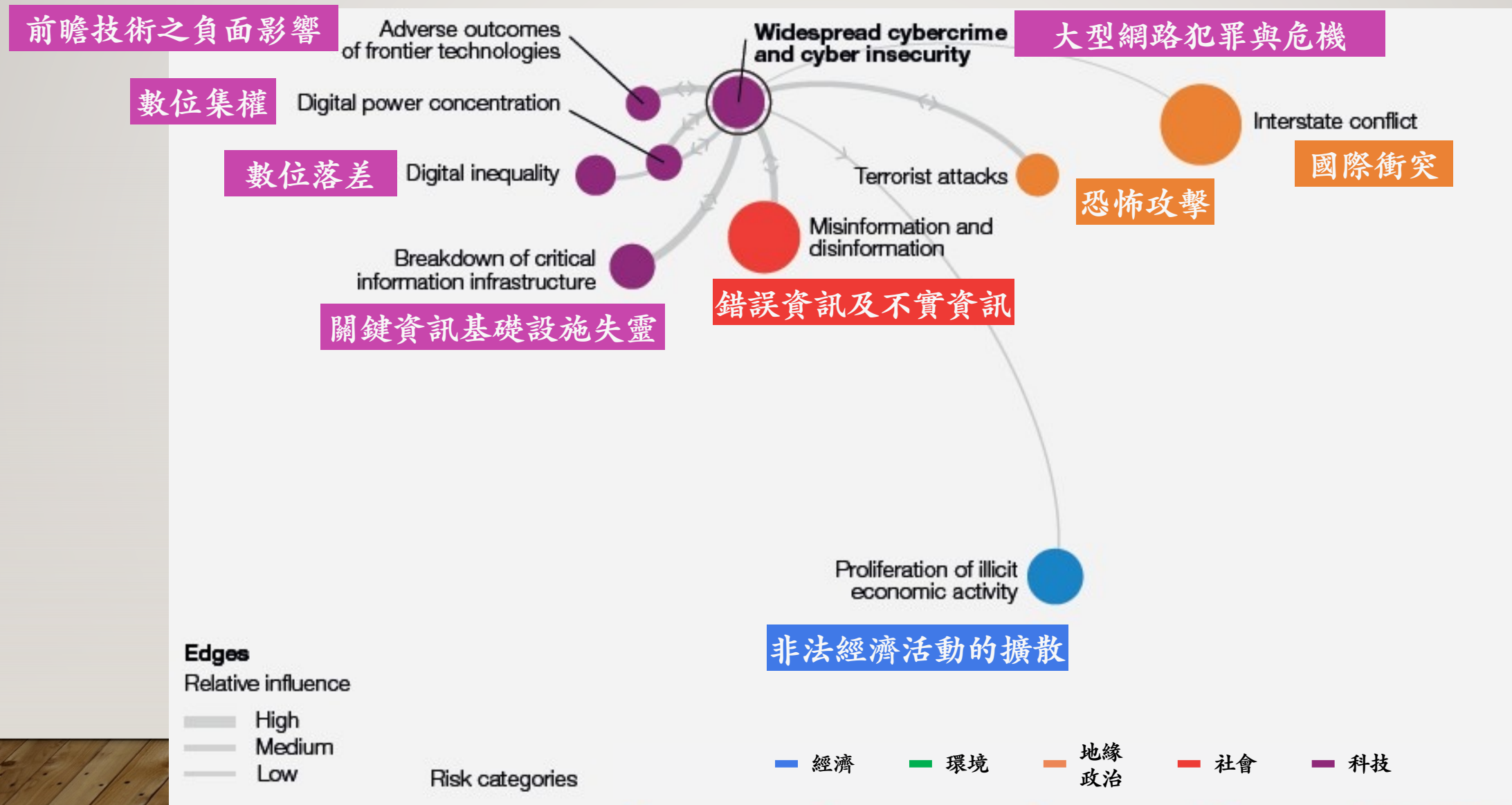
企業

1	生計危機
2	自然災害與極端天氣事件
3	地緣經濟對峙
4	大型網路犯罪與危機
5	大規模環境破壞事件*
6	社會凝聚力削弱與兩極化
7	未能減緩氣候變遷
8	自然資源危機*
9	債務危機
10	未能適應氣候變遷

全球風險之關聯性



- WEF篩選出32項風險因子
- 節點愈大表示該風險影響愈大
- 關連線愈粗表示兩個風險間之交互影響越顯著





大型網路犯罪與危機

- 由於喪失隱私、數位詐欺、數位竊盜及網路間諜活動之盛行，導致網路犯罪行為日趨複雜、嚴峻



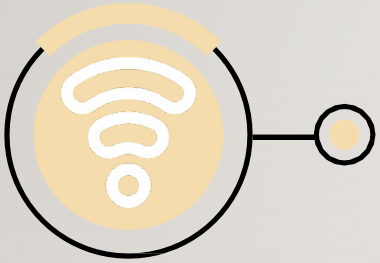
前瞻科技之負面影響

- 由於人工智慧、人機介面、生化科技、地球工程及量子電腦運算等技術之發展，對於個人、企業、環境及經濟所導致之負面影響



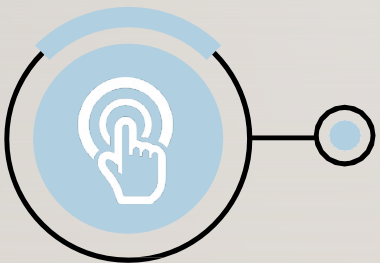
關鍵資訊基礎設施失靈

- 由於惡意網路攻擊、物理損壞或太陽風暴等因素，導致網際網路、移動裝置、公用事業及衛星等關鍵實體及數位基礎建設、服務之功能衰退、過載或失靈



數位集權

- 由於反壟斷之監理措施失效，新創產業之不當投資或國家對於關鍵科技發展之限制等因素，導致關鍵數位資產、能力或知識集中由少數個人、企業或國家掌控，且其可控制前述科技之使用，並操縱其定價



數位落差

- 由於投資不足、數位能力低下、購買力不足或政府對於科技發展限制等因素，導致數位網路與科技之使用出現不平等情形

大綱

- 資安威脅趨勢

- WEF 2023全球風險報告
- 全球資安威脅趨勢
- 政府資安威脅趨勢
- 政府資安事件案例

- 資安管理原則

- 資安防護重點

● 參考全球資安威脅與相關研究案例，歸納全球資安威脅趨勢



網路釣魚為主要攻擊媒介

隨著人工智慧(AI)與新興技術出現，112年社交工程攻擊顯著增長，**網路釣魚**仍是最主要攻擊媒介



物聯網/網通設備漏洞利用

- 網通設備零時差攻擊約**4萬台**設備遭感染
- Gafgyt殭屍網路針對路由器漏洞CVE-2017-18368進行**數千次**攻擊



供應鏈攻擊持續發展中

- Gartner預測，**114年**全球**45%組織**將遭受軟體供應鏈攻擊
- **112年**軟體供應鏈攻擊是**108年至111年**總和之**2倍**



勒索軟體技術多樣化

- 勒索軟體跨**Windows**、**Linux**及**macOS**作業系統進行攻擊
- Veeam指出，**93%**以上攻擊以**備份主機**為目標



Vivian Mendez

FTC消費者和商業教育部律師

一旦你的所谓意中人向你要钱

FTC專家提醒民眾謹防利用人工智慧和網路釣魚詐騙

全美電視台記者採訪報導

AMTV TODAY

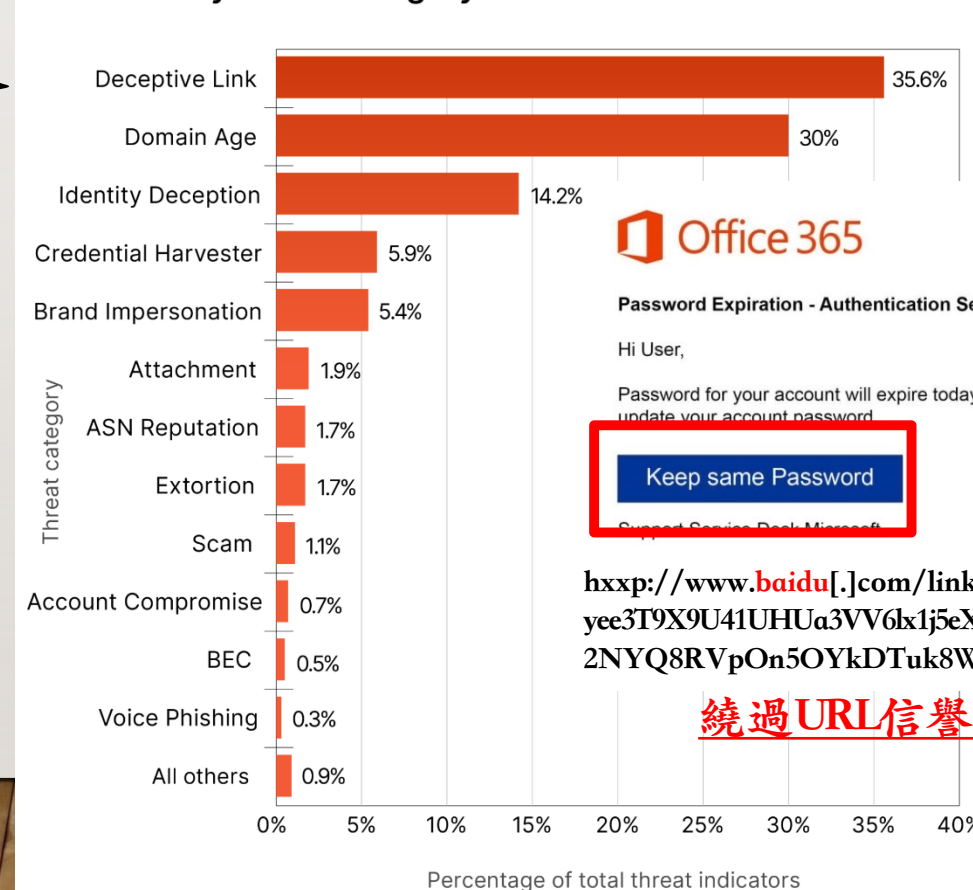
news

www.amtvusa.tv

網路釣魚為主要攻擊媒介

- CISA指出，**90%**以上網路攻擊都是從**網路釣魚**開始
 - 冒充受信任的電子郵件或訊息，以詐騙收件人**洩漏個人資訊、帳號密碼或執行惡意附件**
- 駭客使用**欺騙性連結**做為網路釣魚策略
 - Cloudflare報告指出，**欺騙性連結**占網路釣魚威脅**35.6%**
 - 寄發看似合法URL，使用者點擊該URL可能會**導向惡意網站或開啟應用程式(如PDF)**，使得駭客可以植入惡意程式或竊取資訊

Detections by threat category



Office 365

Password Expiration - Authentication Service

Hi User,

Password for your account will expire today. Please follow the link to update your account password

Keep same Password

hxxp://www.baidu[.]com/link?url=-
yee3T9X9U41UHUa3VV6lx1j5eX2Eol6XpZqfDgDcf-
2NYQ8RVpOn5OYkDTuk8Wg<4OY

繞過URL信譽檢查偵測機制



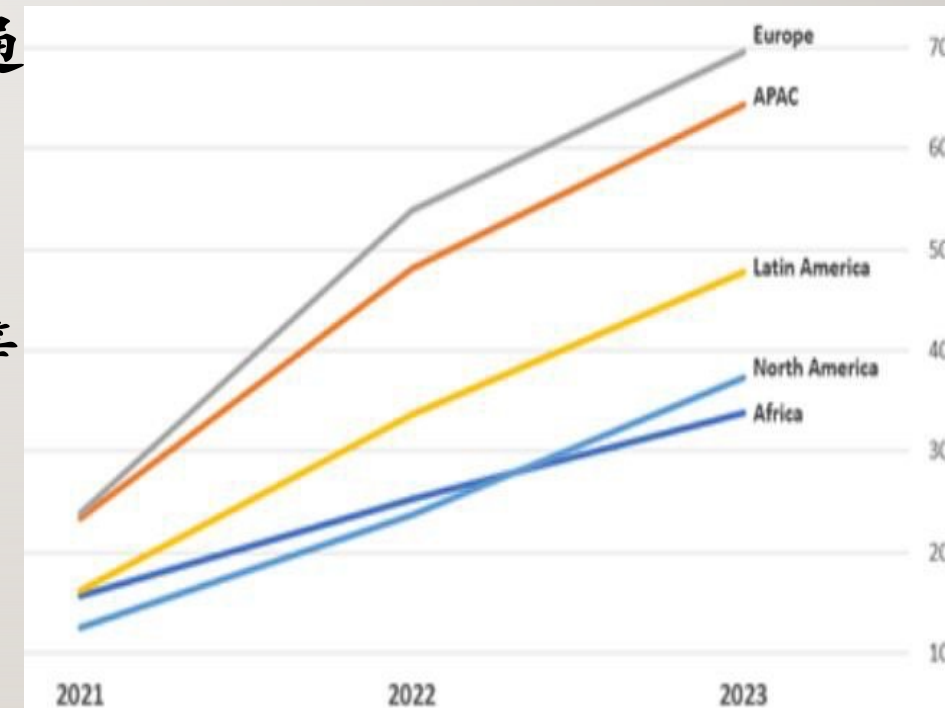
全城守網

cyberdefender.hk

物聯網攻擊

物聯網/網通設備漏洞利用

- CheckPoint指出，針對**物聯網設備**網路攻擊急遽增加
 - 112年與111年相比，物聯網設備平均**每週攻擊次數增加41%**，平均**每週有54%組織遭受攻擊**
- 物聯網設備多未有適當的保護或管理，普遍存在**注入攻擊**
 - 常見受攻擊物聯網設備，如**路由器**、**IP攝影機**、**DVR(數位錄影機)**、**NVR(網路錄影機)**及**印表機**等





2020年美國華府州西雅圖

供應鏈攻擊持續發展中

- 供應鏈攻擊係以**第三方供應商與服務提供者**為目標，以取得對其**客戶系統與資料存取權限**
 - **零時差/軟體漏洞**：針對供應商使用**韌體/軟體**進行攻擊
 - **憑證竊取**：透過網路釣魚或系統漏洞等攻擊取得**供應商系統存取憑證**
 - **資料竊取**：入侵供應商系統取得**營運或客戶機敏資料**



ALERT

Supply Chain Attack Against 3CXDesktopApp

Release Date: March 30, 2023

Mandiant: JumpCloud breach led to supply chain attack

Mandiant researchers attribute the supply chain attack to a North Korean threat actor that abused JumpCloud's commands framework to gain access to a downstream customer.

By **Rob Wright**, News Director

Published: 24 Jul 2023

Mandiant discovered a supply chain attack against a U.S. software company that stemmed from last month's data breach at JumpCloud.

駭客攻擊台灣

```
... size of py file: 2424 bytes  
ved as: snellcode.txt  
liakali:~/tools/SMBGhost_RCE_PoC$  
liakali:~/tools/SMBGhost_RCE_PoC$ msf  
py -o shell_reverse
```

台北



駭客善用"生成式AI技術" 攻擊複雜更難監控

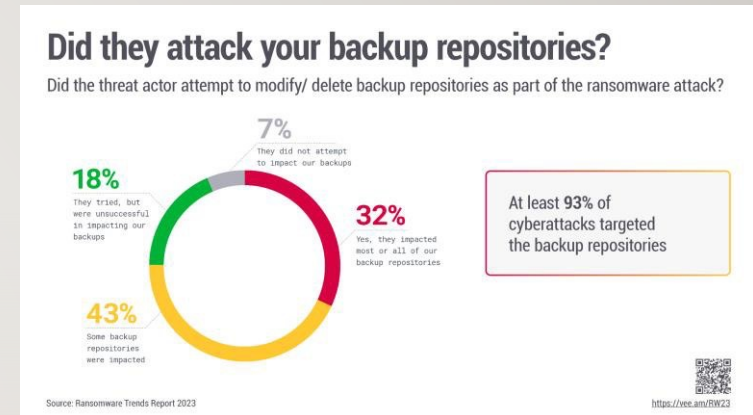
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道



更多新聞在這裡

勒索軟體技術多樣化

- Veeam指出，約**93%**攻擊以**備份檔**為目標，近**29%**無法完成復原
- 造成勒索軟體攻擊主要原因為**漏洞利用**，其次為**憑證洩漏**與**惡意電子郵件**
- 勒索軟體技術多樣化擴及影響平台與規避偵測機制
 - LockBit與Cyclops可感染**Windows**、**Linux**及**Mac**三大作業系統
 - Cactus透過**自我加密**，繞過防毒軟體偵測機制



AHA warns hospitals about data 'time bombs'

Giles Bruce - Monday, October 2nd, 2023

Save Post Tweet Share Listen Text Size Print Email

Hospitals and health systems should be on the lookout for data "time bombs" that could cause patient information to be destroyed by hackers, the American Hospital Association warned.

Ransomware gangs have been attacking victims twice within close proximity and using data deletion tools that lie dormant during which time the groups can negotiate for more ransom, the FBI said in a notice.

Cyber adversaries continue to evolve their tactics in a way to increase likelihood of ransom "said John Riggi, AHA's national advisor for cybersecurity and risk, in a Sept. 29 news release. The combination of multiple ransomware attacks on the same vulnerable victim organization

LockBit ransomware encryptors found targeting Mac devices

By Lawrence Abrams

April 16, 2023 01:31 PM 7

會自我加密的新型勒索軟體 Cactus，讓防毒軟體及網路監控工具偵測不到

作者 Evan | 發布日期 2023 年 05 月 12 日 8:20 | 分類 網路, 資訊安全

LINE 分享

分享

Follow

讚 64

分享

大綱

- 資安威脅趨勢

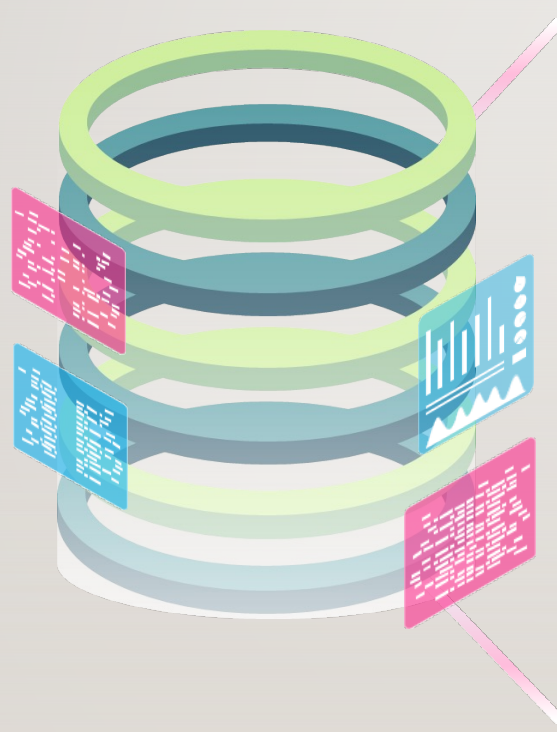
- WEF 2023全球風險報告
- 全球資安威脅趨勢
- 政府資安威脅趨勢
- 政府資安事件案例

- 資安管理原則

- 資安防護重點

政府資安威脅趨勢

- 綜整政府領域資安威脅偵測與機關事件通報資訊，主要威脅趨勢包含6大面向



1. 社交工程與APT惡意電子郵件仍為主要攻擊手法
2. 遠端服務探測與產品漏洞利用為主要網路威脅
3. 雲端服務中繼站盛行協助駭客隱匿惡意行為
4. 萬物聯網衍生應用造成資安風險
5. 供應鏈安全遭破壞成為入侵跳板
6. 人員資安意識不足導致資料外洩



資通安全署

關於資安署



資安法規專區



業務專區



訊息公告



- 政府資訊公開
- 最新消息
- 廉政專區
- 資安月報

相關連結



資通安全網路月報 (113年1月)



資通安全網路月報(113年1月)

<近期政策重點>

近來發現部分同仁使用公務信箱註冊於非公務網站，致遭帳密外洩案例，重申公務信箱勿註冊於非公務網站或外部服務，且不可使用相同通行碼，避免外部主機遭駭侵後，相關帳號、密碼及使用者個資等資料都將一起曝險；另使用者電腦系統及軟體亦應定期更新及掃毒，以維資通安全。

<整體威脅趨勢>

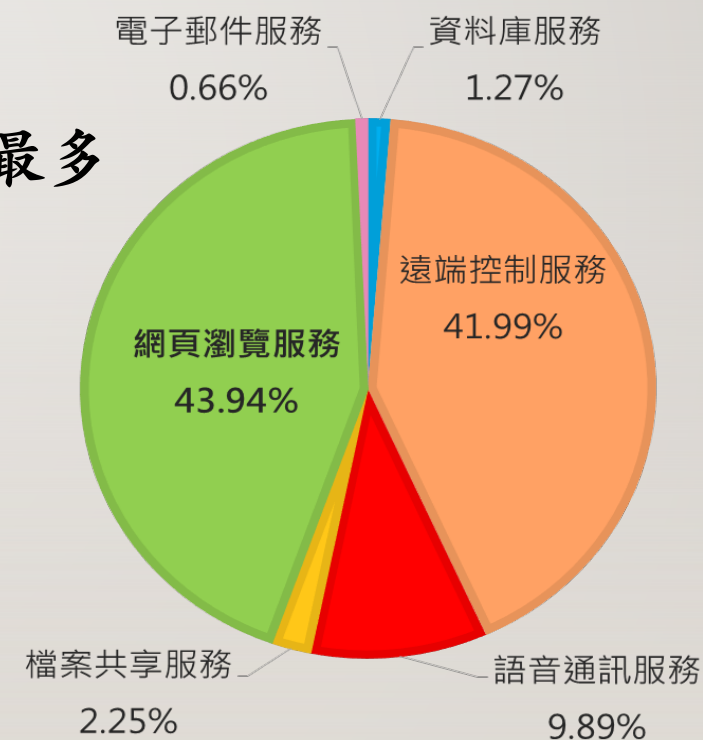
事前聯防監控

本月蒐整政府機關資安聯防情資共6萬2,578件（較上月增加1萬 2,997件），分析可辨識的威脅種類，第1名為資訊蒐集類(31%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(23%)，主要是嘗試入侵未經授權的主機；以及資訊內容安全類 (15%)，大多是系統遭未經驗證存取或影響資訊機敏性。另統計近1 年情資數量分布詳見圖1。

經進一步彙整分析聯防情資資訊，發現近期駭客利用微軟 Outlook電子郵件服務，針對政府機關人員寄送主旨為「投訴政府人員不作為」，內含惡意附檔之社交工程電子郵件，企圖誘騙收件人開啟惡意附檔以植入後門程式，進而竊取機敏資訊，相關情資已提供各機關聯防監控防護建議。



- 112年1月至10月，透過國內外外部署之蜜罐誘捕殭屍網路攻擊威脅，共捕獲11,399,806,680次攻擊連線
 - 前3名攻擊跳板來源國家分別為美國(31%)、中國(10%)及新加坡(7%)
 - 針對網頁瀏覽服務之攻擊最為嚴重
 - 捕獲114,054個惡意樣本，以Mirai殭屍網路與其變種最多



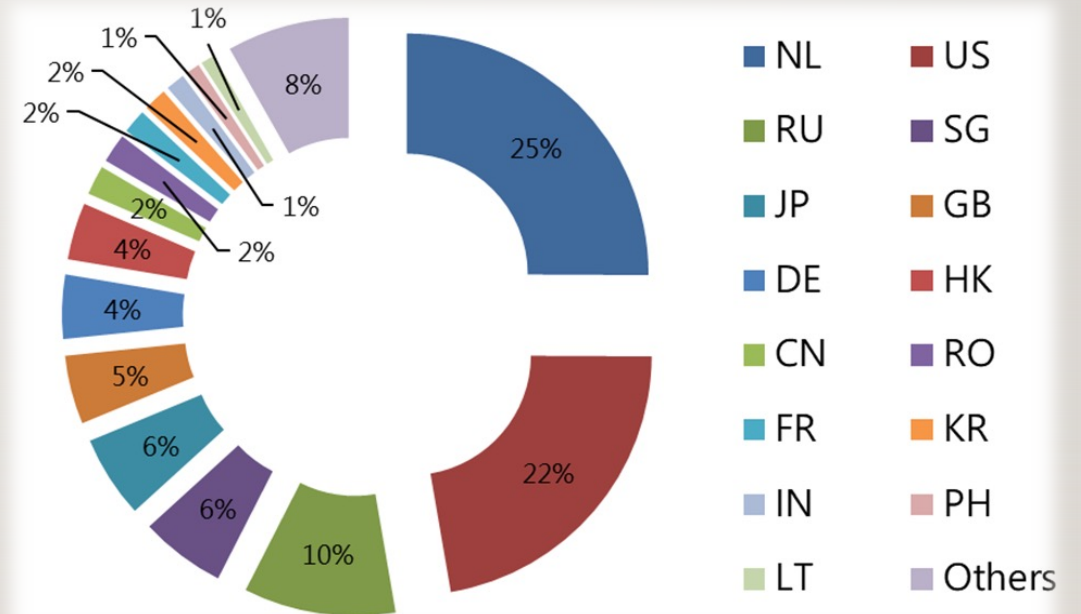
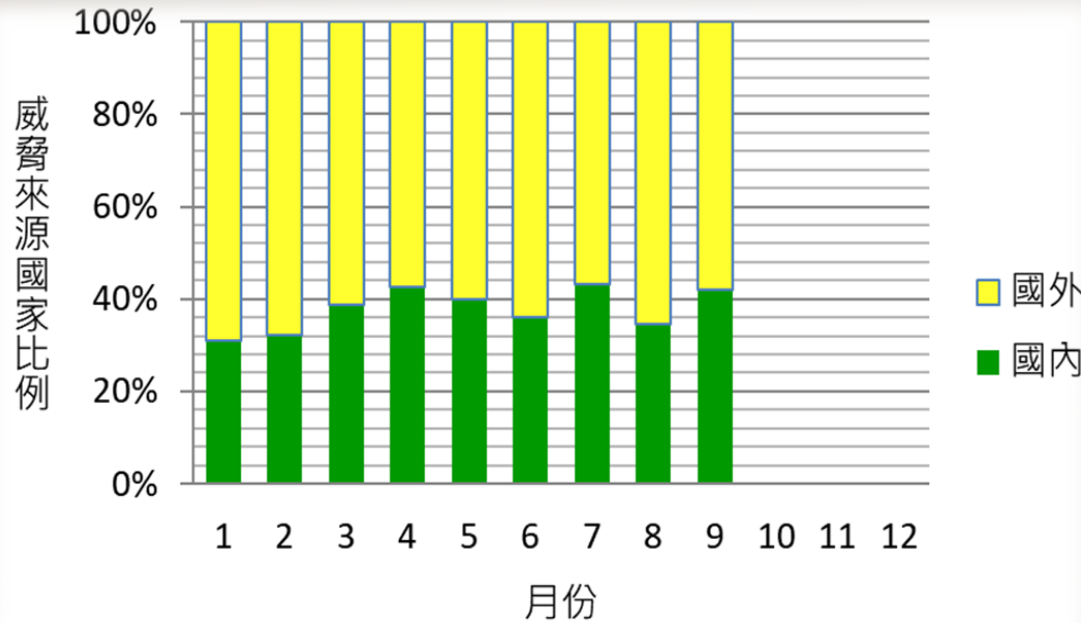
- 112年5月，AndoryuBot出現新型變種，針對物聯網裝置進行感染擴散
 - 不斷利用漏洞持續擴散殭屍網路，並可發起各種協定之**DDoS攻擊**
 - 駭客集團亦利用此殭屍網路進行營利，於**Telegram**銷售**DDoS攻擊服務**
- 駭客建立殭屍網路之動機，可能朝向營利目的之趨勢發展，**黑色產業鏈興起**，駭客攻擊活動將日益猖獗，升高對我國之資安威脅
 - 需持續宣導物聯網設備之相關威脅風險，提高使用者資安意識，避免設備遭殭屍網路感染

AndoryuBot殭屍網路

- 112年5月，AndoryuBot出現新型變種，以新型漏洞CVE2023- 25717進行感染擴散，以**Ruckus 無線路由器**為攻擊目標
- 另2種漏洞之攻擊，以DVR與路由器漏洞注入惡意指令
 - MVPower CCTV DVR之RCE漏洞 (CVE-2016-20016)
 - Dasan GPON路由器之RCE漏洞 (CVE-2018-10562)

聯防監控威脅情蒐(1/2)

- 112年1月至9月，SOC業者回傳有效資安監控情資共516,102件，依政府機關業務類別，前3名分別為**外交國防法務類之入侵攻擊68,042件**、**綜合行政類之資訊蒐集65,658件**及**外交國防法務類之資訊蒐集61,676件**
- 國外攻擊跳板來源前3名分別為荷蘭(25%)、美國(22%)及俄羅斯(10%)



聯防監控威脅情蒐(2/2)

● 政府領域網通設備為駭客攻擊目標之一

－ 可程式化邏輯控制器(PLC)暴露影響分析

漏洞編號	CVSS3分數	漏洞描述
CVE-2022-1161	9.8	屬Rockwell設備遠端程式執行漏洞
CVE-2022-1159	7.2	屬Rockwell設備注入攻擊漏洞
CVE-2022-38773	6.8	屬西門子設備資料完整性驗證漏洞

－ 機關考勤設備存在零時差漏洞並遭惡意利用

漏洞簡述	漏洞說明
不當的存取控制 (Improper Access Control)	系統存在登入驗證頁面，但未經授權之使用者，可不經身分驗證，存取系統網站頁面。
未限制檔案上傳 (Unrestricted Upload of File)	系統部分頁面存在檔案上傳功能，該功能未過濾特殊字元與驗證檔案類型，未經授權使用者存取該頁面即可上傳任意類型檔案。
危險功能暴露 (Exposed Dangerous Method or Function)	系統部分頁面可直接執行系統指令，未經授權之使用者可存取該頁面，執行任意系統指令。

受攻擊機關類別

資安責任等級 機關業務類別	B	C	D	總計
綜合行政	3	31	2	36
經濟能源農業	7	0	0	7
總計	10	31	2	43

受攻擊機關類別

資安責任等級 機關業務類別	B	C	D	E	總計
綜合行政	3	2	1	0	6
內政衛福勞動	0	1	17	2	20
教育科學文化	0	3	0	0	3
交通環境資源	0	0	0	2	2
總計	3	6	18	4	31

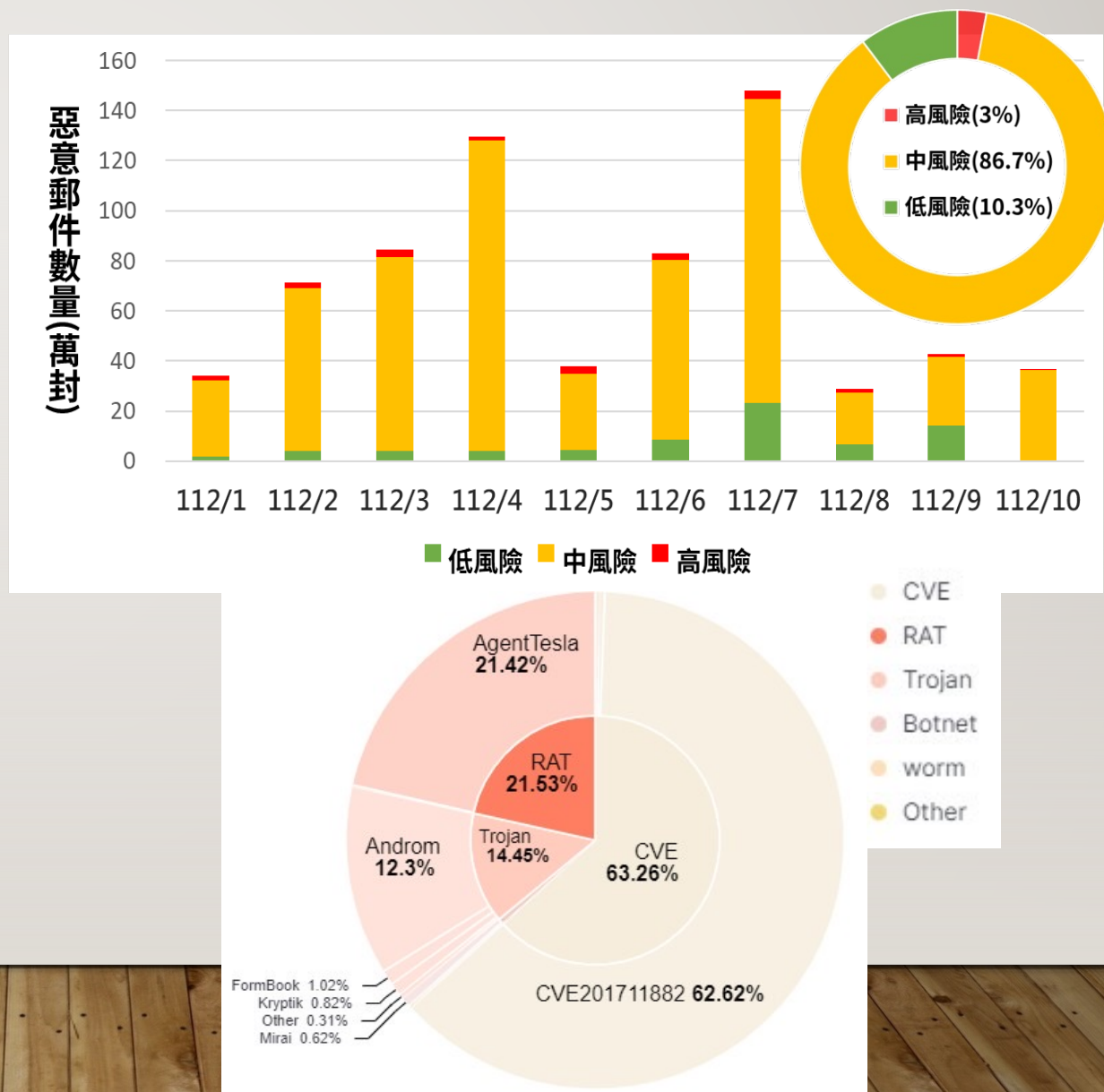
2013



來到人人皆是低頭族的網路世代

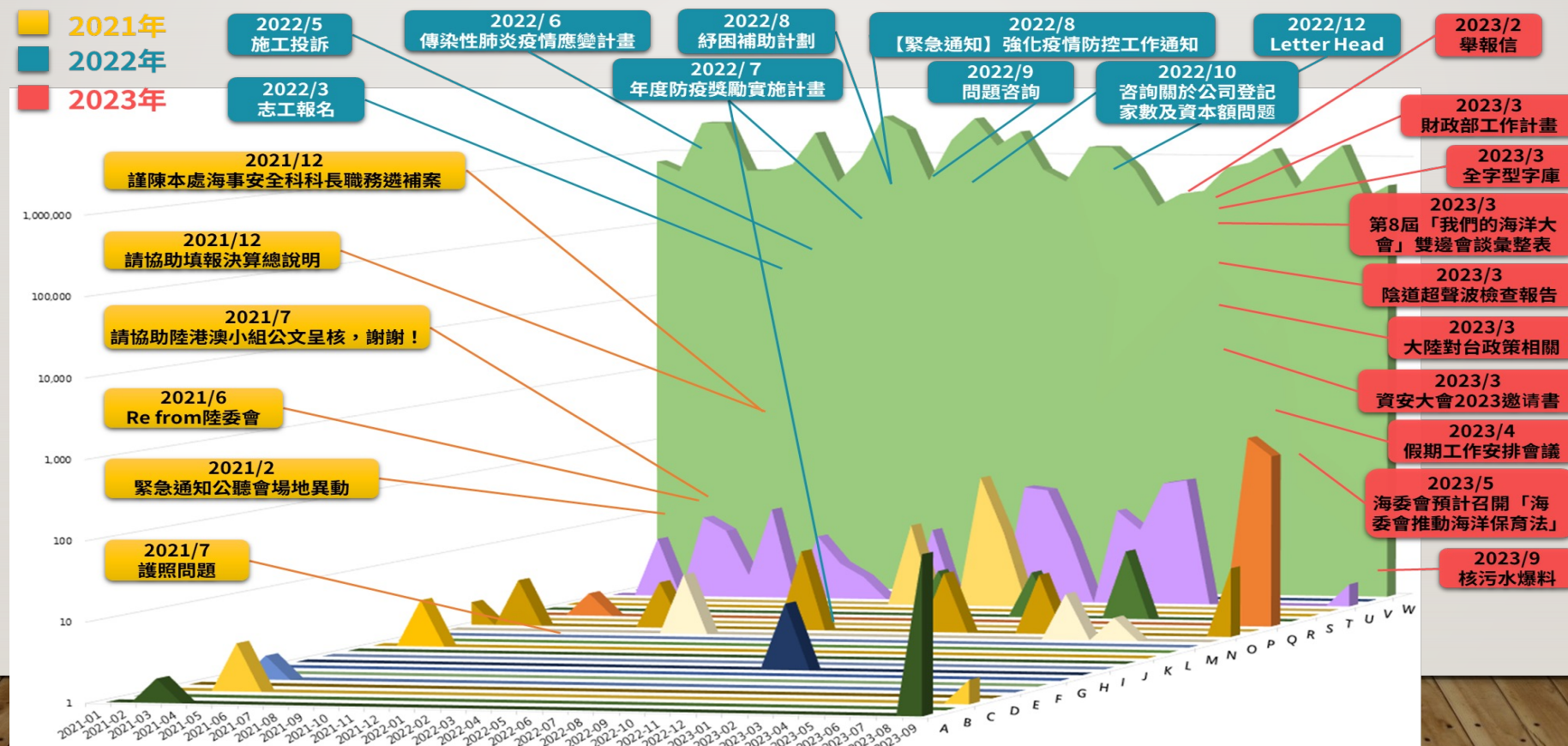
惡意電子郵件分析(1/2)

- 112年共檢測2.8億餘(289,896,041)封電子郵件，偵測發現**696萬餘**(6,963,081)封可疑惡意電子郵件占2.4%
- 殭屍網路惡意電郵(MalSpam)，以**CVE-2017-11882 弱點**利用攻擊為大宗，占整體惡意程式62.62%，其次偵測之威脅，為**AgentTesla**遠端木馬與**Androm**後門木馬等



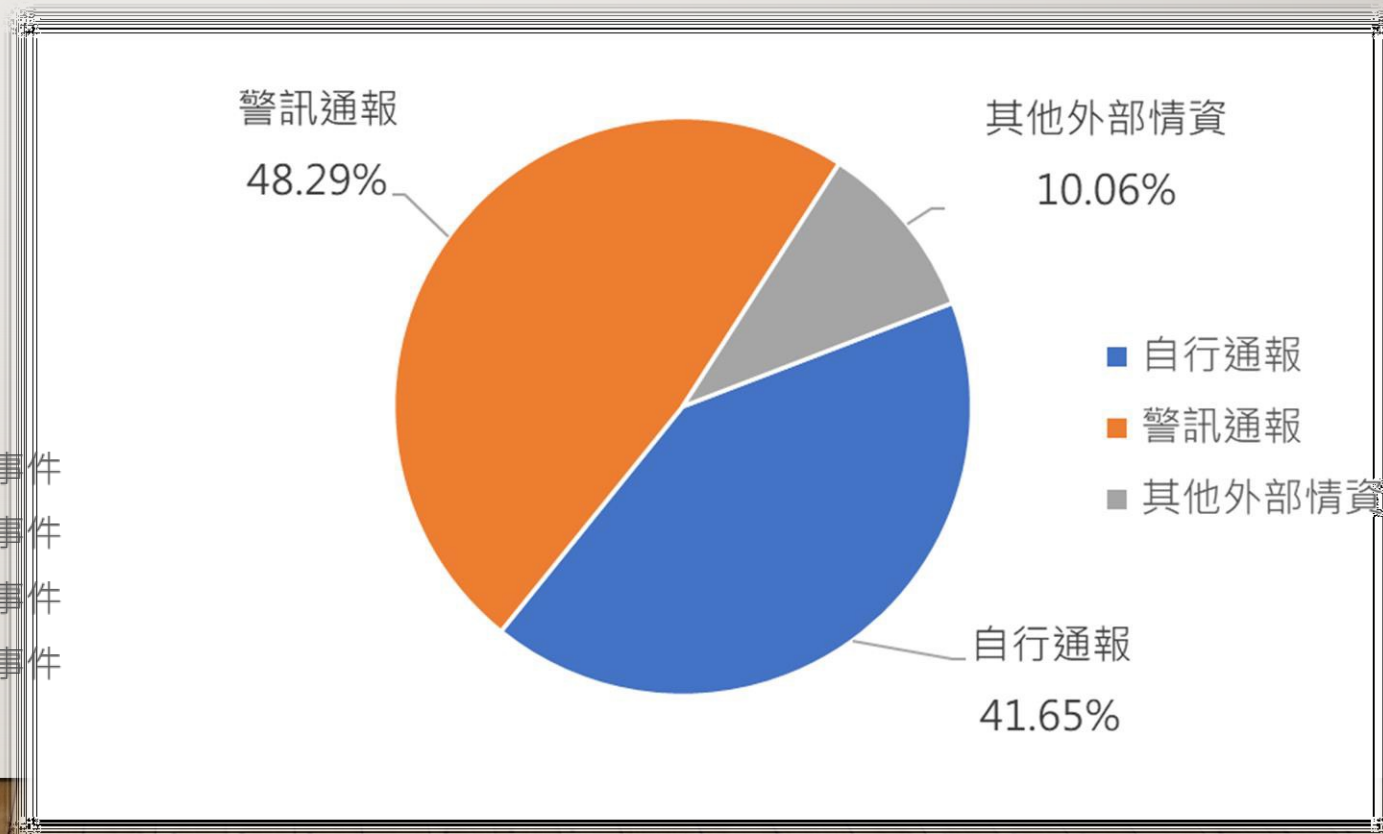
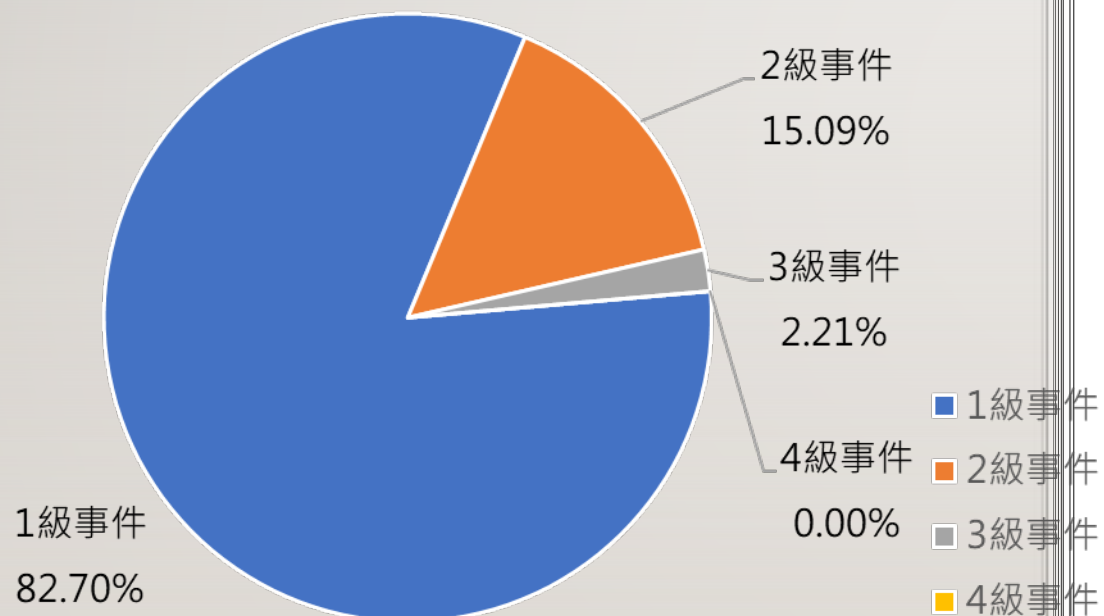
惡意電子郵件分析(2/2)

- 112年政府領域APT郵件攻擊趨勢，可歸納為**5波攻擊行動**，計**208封針對性社交工程郵件**，其中駭客分別利用政府機關工作業務、會議邀請、健檢報告及檢舉爆料等主旨，對政府機關人員發動攻擊



通報事件分析(1/2)

- 112年1月至9月，共接獲497件政府機關資安事件通報
- 事件影響等級以**1級事件為主**占82.70%，3級事件僅占2.21%
- 48%為機關接獲資安院警訊通告後所進行之通報



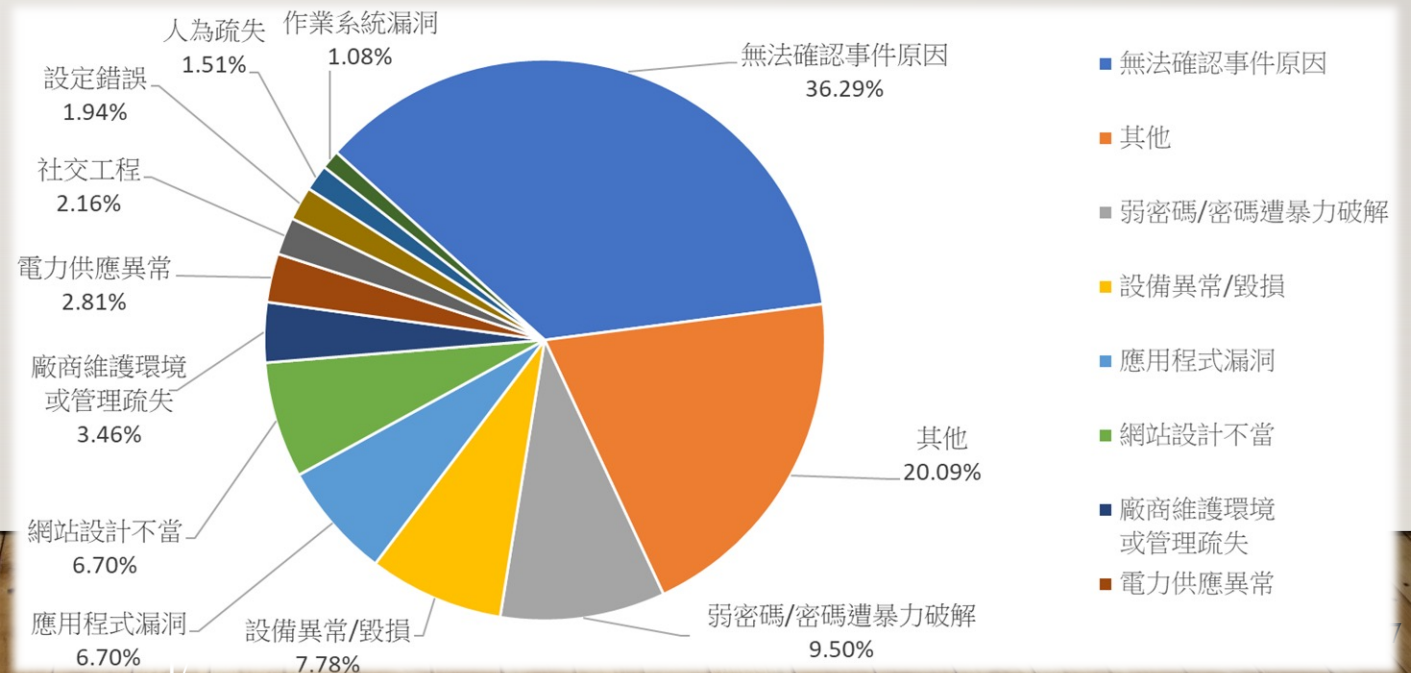
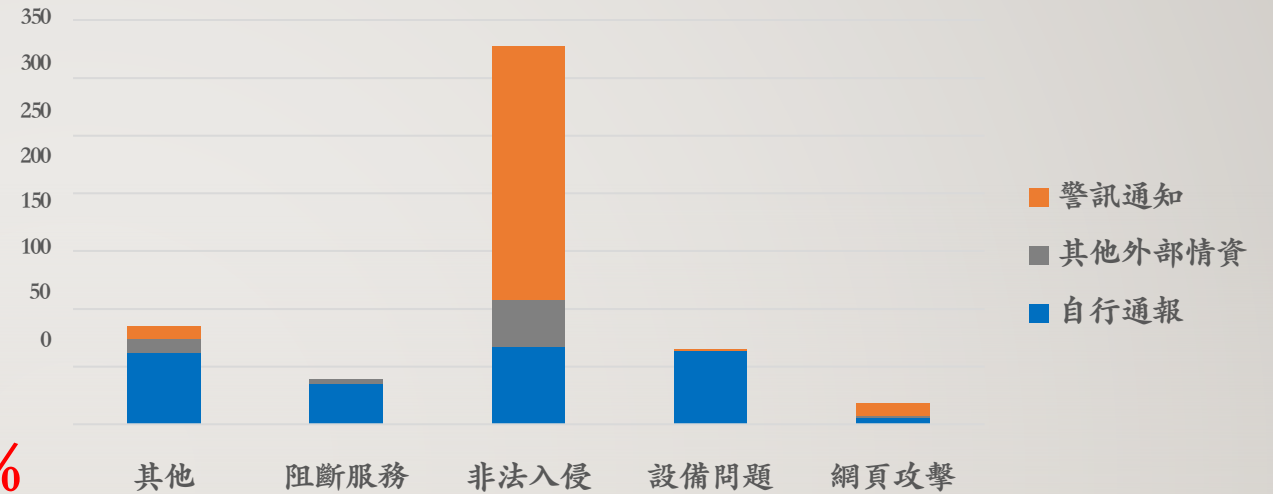
※統計區間：112年1月1日至9月30日

通報事件分析(2/2)

- 事件類型以**非法入侵為大宗**，其中又以機關接獲資安院警訊通知後進行通報為主

- 可識別之事件原因

- 「弱密碼/密碼遭暴力破解」 9.50%
- 「設備異常/毀損」 7.87%
- 「應用程式漏洞」 6.70%



大綱

- 資安威脅趨勢

- WEF 2023全球風險報告
- 全球資安威脅趨勢
- 政府資安威脅趨勢
- 政府資安事件案例

- 資安管理原則

- 資安防護重點



案例



人員資安意識不足，開啟惡意郵件，或瀏覽網頁點擊惡意連結



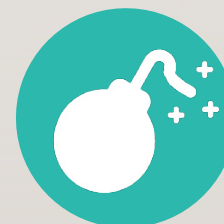
網通設備弱點遭開採利用，增加調查難度



供應鏈廠商遭駭，導致機關出現異常連線

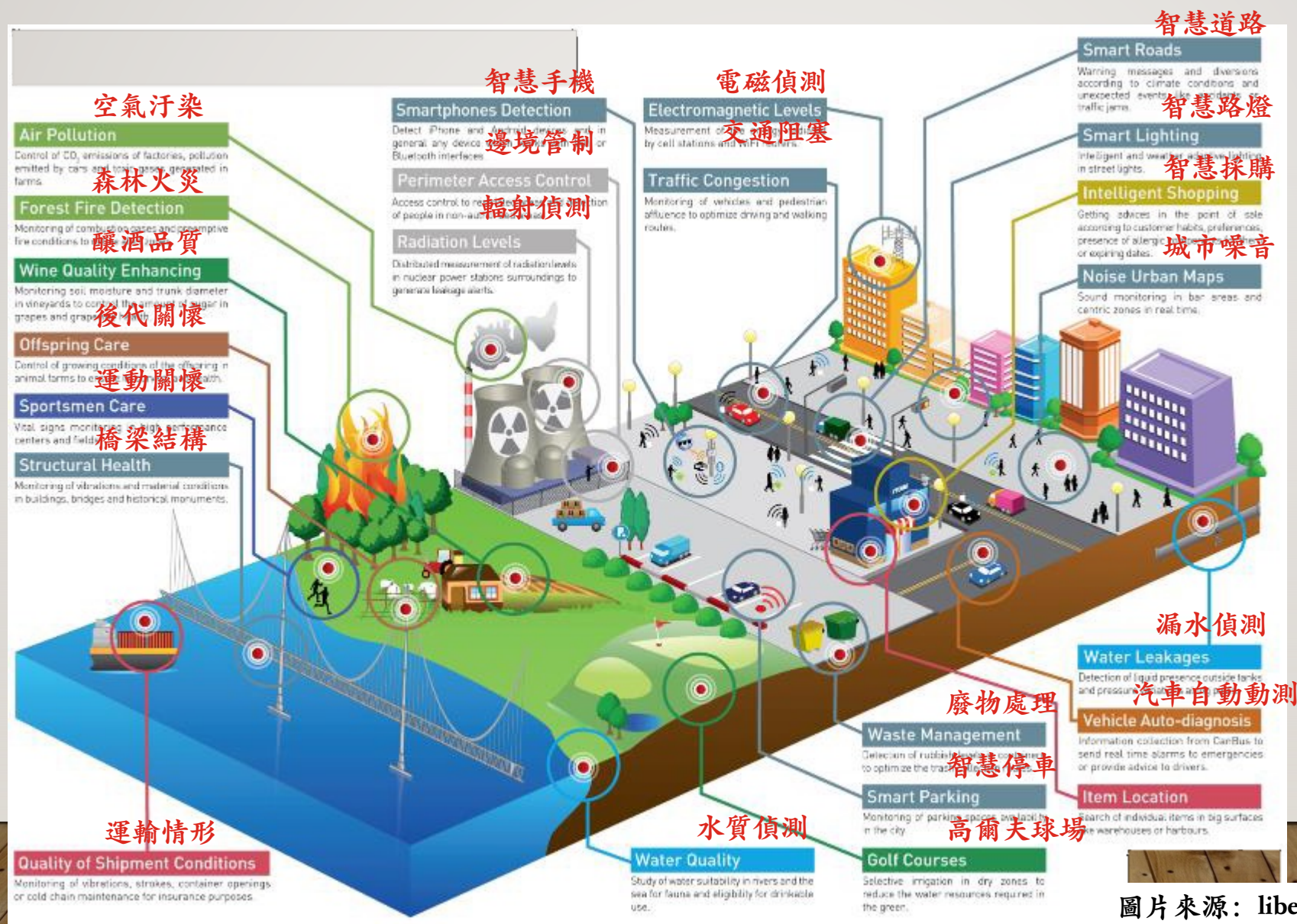


利用產品漏洞發動攻擊，導致帳密外洩



DNS遭DDoS攻擊，無法正常提供服務

萬物聯網時代、資安威脅升高



行動化(M)
雲端化(C)
IOT(I)
+
AI(A)
大數據(B)
+
5G

案情提要

- 駭客利用日本民間公司之郵件帳號，透過VPN服務以核污水爆料為由，**寄送夾帶惡意壓縮檔之社交工程郵件**，對政府機關進行社交工程郵件攻擊
- 駭客事先將惡意壓縮檔上傳至匿名文件託管服務，並將下載連結與惡意壓縮檔附於惡意郵件中，**壓縮檔則經通行碼保護以規避偵測**
- 惡意壓縮檔可觸發近期公告之**WinRAR漏洞(CVE-2023-38831)**，若使用者點擊誘餌文件，將觸發執行同名資料夾內之惡意批次執行檔
- 經分析，該後門程式為遭駭客濫用之紅隊攻防演練工具Cobalt Strike

The figure consists of four screenshots illustrating the attack process:

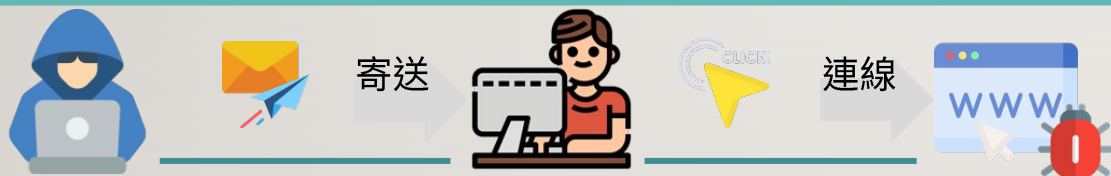
- 1. 經通行碼保護之壓縮檔，以規避偵測**: A WinRAR window showing a ZIP archive named "資料.zip" (Zi料.zip) with an unpacked size of 182,692 bytes. The file is highlighted with a red box.
- 2. 利用WinRAR漏洞之壓縮檔**: A WinRAR window showing a ZIP archive named "1.zip" with an unpacked size of 182,692 bytes. The file is highlighted with a red box.
- 3. 含同名之資料夾與正常文件**: A Windows Explorer window showing a folder named "資料" (Zi料) containing a file named "資料.pdf" (Zi料.pdf). The file is highlighted with a red box.
- 4. 資料夾內含同名之惡意批次檔**: A Windows Explorer window showing a folder named "資料" (Zi料) containing a file named "資料.pdf.cmd" (Zi料.pdf.cmd). The file is highlighted with a red box.

Red arrows indicate the flow of the attack: from the ZIP file in WinRAR to the folder in Windows Explorer, and from the PDF file to the PDF command file.

漏洞利用社交工程攻擊案例(2/2)

防護建議

- 建議清查與更新WinRAR版本至6.23以上
- 加強內部宣導，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔及連結



利用WinRAR漏洞
製作惡意附檔

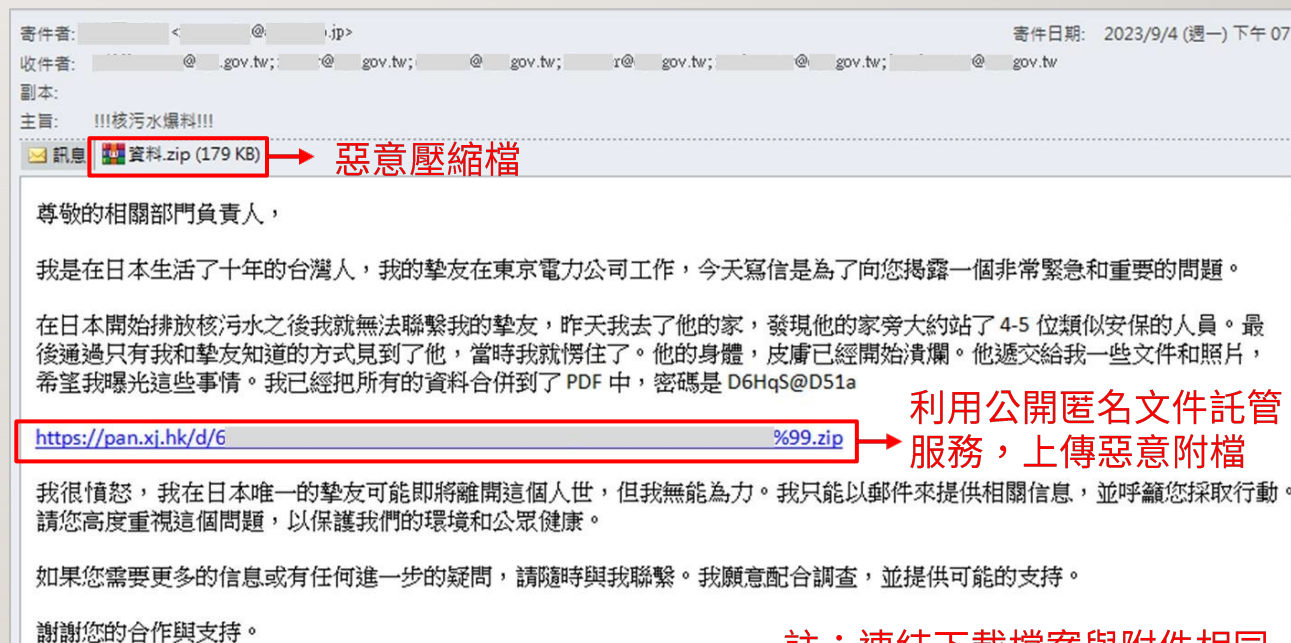
核污水爆料

Cobalt Strike

利用VPN服務寄送
社交工程郵件

利用匿名文件託管
服務上傳惡意檔案

竊取利用日本民間
科技公司郵件帳號



註：連結下載檔案與附件相同

偽冒機關散布惡意電郵案例

案情提要

- 駭客偽冒台電名義與郵件帳號，利用**繳交台電費用相關主旨**，模仿台電寄送予民眾之繳費通知郵件內文做為誘餌
- 發送以**pdf.zip命名之惡意附檔**，大量散布惡意程式垃圾郵件，攻擊機關與民眾
- 利用Google雲端空間放置二階NanoCore遠端木馬惡意程式躲避偵測



- 偽冒台電名義
- 竊取過往郵件

攻擊者



社交工程郵件

連至雲端空間下載二階惡意程式



雲端下載站

中繼站報到



駭客中繼站



偽冒台電名義與電子郵件帳號

副檔名以pdf.zip形式發送

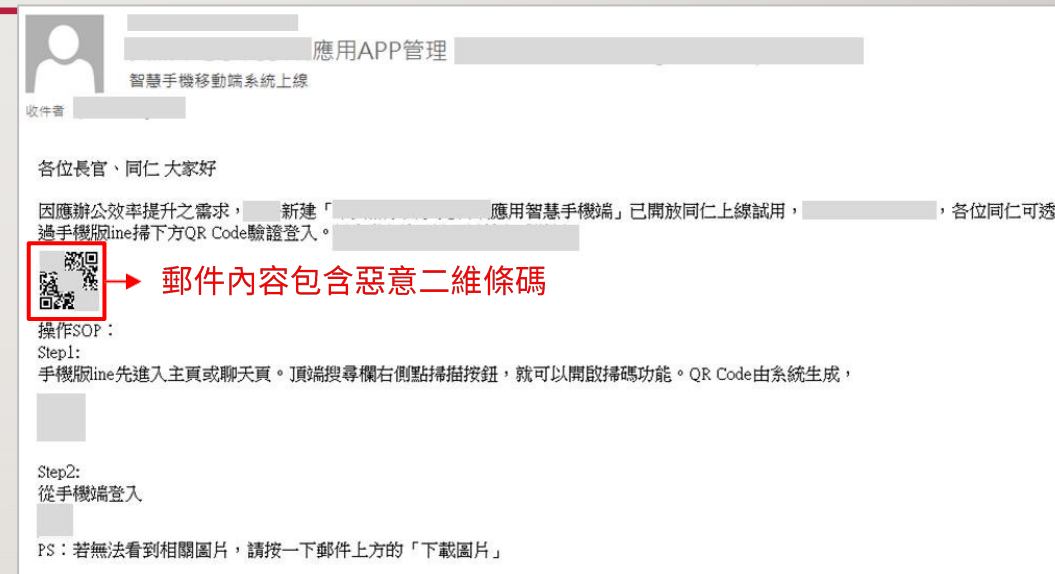
防護建議

- 確認郵件附檔屬性或檔名後才點擊檔案，若檔名存在異常字元(如pdf.zip, pdf.exe, lnk)，請提高警覺

釣魚郵件社交工程攻擊案例

案情提要

- 駭客偽冒政府機關電子郵件，利用智慧手機系統上線等主旨，引誘收件者以**行動裝置掃描惡意二維條碼**(QR Code)
- 掃描後將**連線至偽冒之登入頁面**，要求收件人輸入帳號與通行碼
- 釣魚網頁無論輸入正確與否，皆**跳轉至合法網站頁面**，以降低收件人戒心



防護建議

- 加強宣導提升人員資安意識，勿掃描未知來源之二維條碼
- 多加注意透過二維條碼訪問之網站，可能包含利用漏洞或竊取資料之惡意程式碼

案情提要

- 機關同仁瀏覽線上**免費影音網站(楓X網)**時，出現「我不是機器人」視窗，顯示「**如果你不是機器人，請點擊下面按鈕**」等資訊，點擊後即觸發惡意程式下載並執行
- 同仁執行程式後，即遭植入勒索軟體，導致個人電腦及NAS分享目錄檔案遭勒索軟體加密
- 機關立即將受害駭電腦中斷連線與封存，並將同業務組室斷網、關閉NAS分享目錄，並還原至前一天備份檔案



防護建議

- 加強宣導提升人員資安意識，勿隨意瀏覽與公務無關之網站
- 採「3-2-1原則」定期備份檔案，3份備份檔、2種不同備份方法及1份異地存放

網通設備產品漏洞攻擊(1/4)

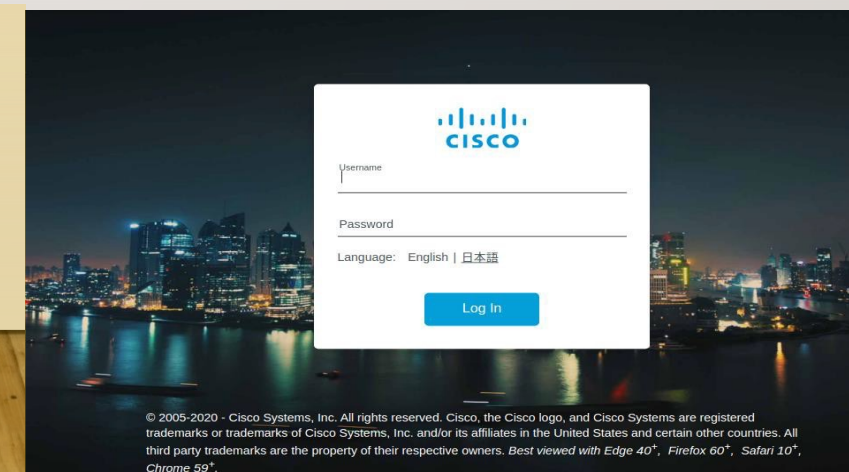
案情提要

- 資安院偵測發現多個公務機關Cisco設備存在嚴重漏洞(CVE-2023-20198)
- 透過原廠釋出之檢測方式，確認已遭駭客利用，共發佈9筆警訊
- 10/20發佈漏洞預警(NICS-ANA-2023-0000453)通知各機關應處



漏洞說明

- Cisco IOS XE之網頁介面允許遠端攻擊者在未經身分鑑別之情況下，新增高權限帳號，以此控制受影響之系統
- 若啟用網頁介面(Web UI)功能皆會受到影響，包含交換器、無線網路控制器、無線基地台及路由器等



防護建議

- 思科官方網站已針對部分型號設備公告修補程式，須儘速安裝
- 採用非網頁UI介面(關閉HTTP Server、HTTPS SERVER，或設定存取白名單)

官方檢測資訊

- Cisco官方與其所屬威脅情報組織Talos，釋出3種檢測方式

1

傳送一個特定HTTP POST至Cisco設備，若設備conf遭竄改，就會回傳16進位字串

```
D:\>curl -k -X POST "https://[redacted]/webui/logoutconfirm.html?logon_hash=1"  
[redacted]45c815c4cc5f4
```

```
D:\>curl -k -X POST "https://[redacted]/webui/logoutconfi  
/1010202301/
```

異常回傳畫面

網通設備產品漏洞攻擊(3/4)

2

由原檢測方式改進，於Http請求標頭新增授權驗證碼，以因應變種惡意程式規避原始檢測方式

```
> curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "http://210.241.22.254:80/webui/logoutconfirm.html?logon_hash=1"
```

```
<!DOCTYPE html>  
<html>
```

正常回傳畫面

```
> curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "http://210.241.72.119:80/webui/logoutconfirm.html?logon_hash=1"
```

```
adcbf66a5aada0f8de
```

異常回傳畫面

3

使用者存取設備網頁根路徑時，惡意程式會偽照並回應 404Not Found 頁面，而正常未被植入程式設備會自動載入javascript程式跳轉至網頁登入路徑

```
> curl -k "http://2[REDACTED]:80/%25"
```

```
<script>window.onload=function(){ url = '/webui';window.location.href=url;}</script>%
```

正常回傳畫面

```
> curl -k "http://[REDACTED]:49:80/%25"
```

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>openresty</center>
</body>
</html>
```

異常回傳畫面

案情提要

- 資安院偵測發現多個公務機關設備對外下載**木馬程式HiatusRAT**，因設備**紀錄保存不足或無紀錄功能**導致難以進行根因調查
- 經機關調查後發現連線設備多為**網通設備(路由器、防火牆)**，受駭設備多**久未進行韌體/軟體更新**，舊版本存在漏洞遭利用

設備類型	廠牌數量	通報件數
路由器	1	3
防火牆	1	15
無線基地台	2	2
郵件伺服器	1	1

※112年統計資料

防護建議

- 定期檢視並更新設備系統/韌體版本
- 採購具有紀錄功能之設備
- 建立健全日誌保存機制，以利異常事件發生時之根因調查

產品漏洞攻擊導致帳密外洩(1/2)

案情提要

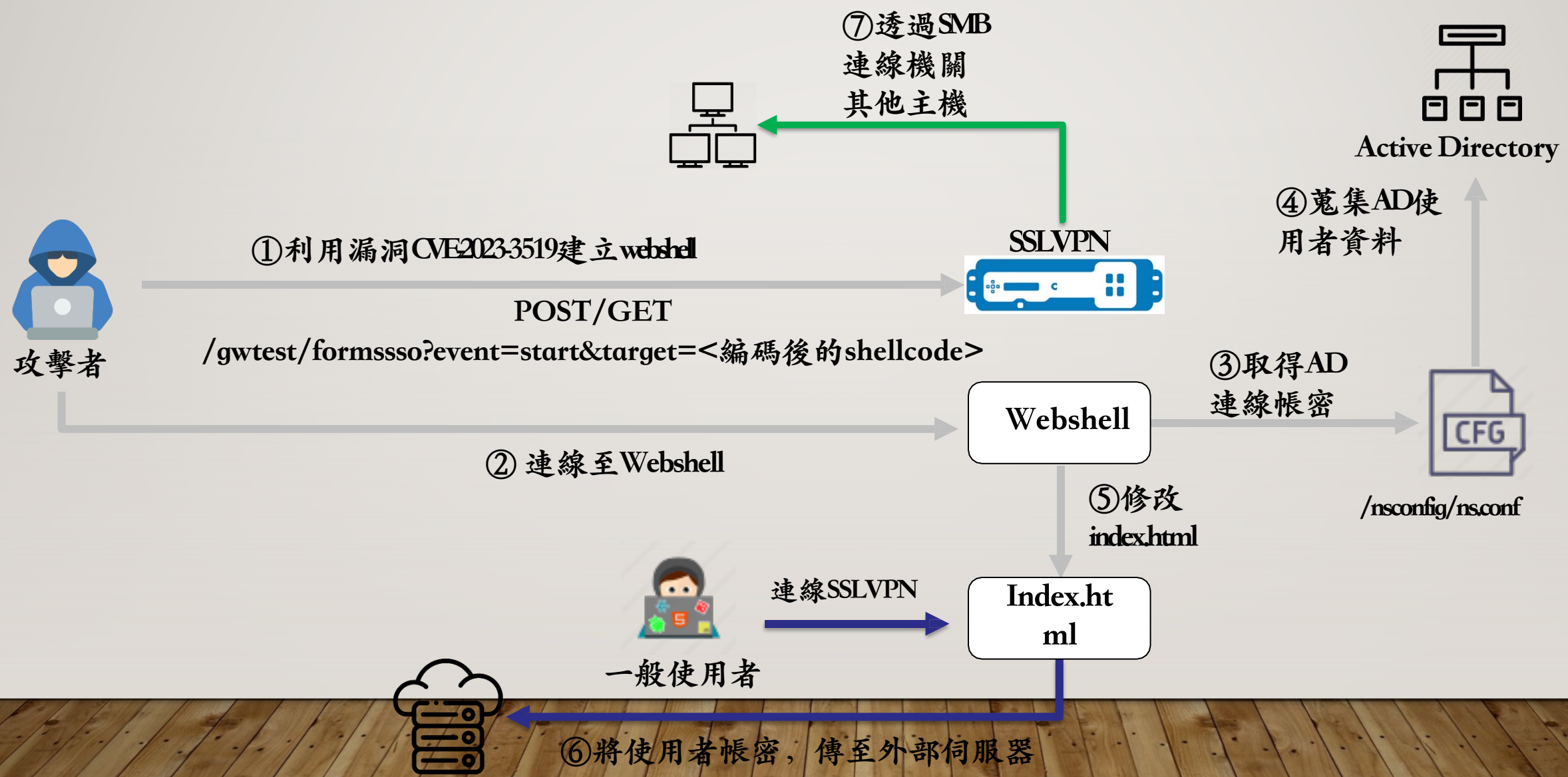
- 機關**防火牆發現大量異常連線**，SSL VPN設備發送大量SMB封包
- 經查SSL VPN設備存在安全性漏洞(CVE2023-3519)，攻擊者可利用漏洞**上傳Webshell、探測腳本**
- 在設備中取得可以連線到**AD帳密檔**，並透過ldapsearch查詢使用者訊息
- 竊取被駭期間連線SSLVPN使用者帳密

防護建議

- 及時更新或套用相關修補程式
- 及時更新特徵碼，透過防護設備阻擋攻擊
- 隔離外部設備網段，避免攻擊擴散

產品漏洞攻擊導致帳密外洩(2/2)

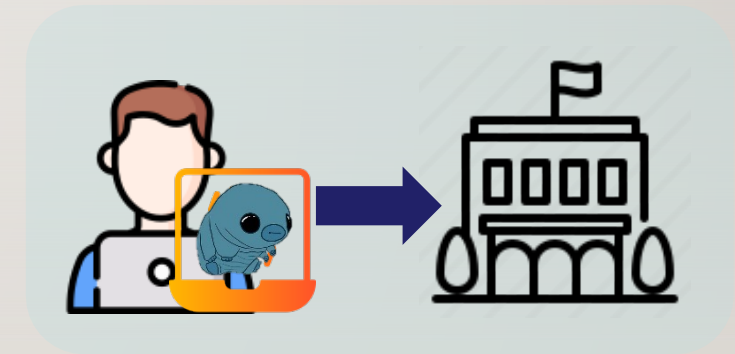
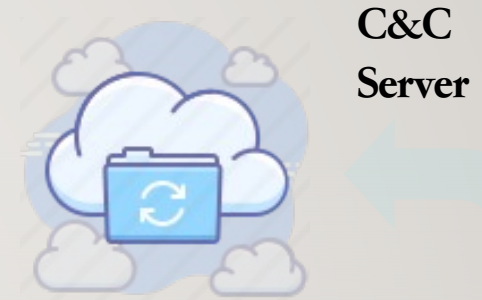
4
6



供應鏈廠商維護環境或管理疏失(1/3)

案情提要

- 廠商攜帶設備至機關進行維護作業，機關允許該設備連線至機房網路，待設備接上網路並操作一段時間後，資安院即發現**符合特定惡意程式行為之連線**
- 機關收到通知後，**即時將廠商設備斷網**，經查後未對機關設備造成進一步為害

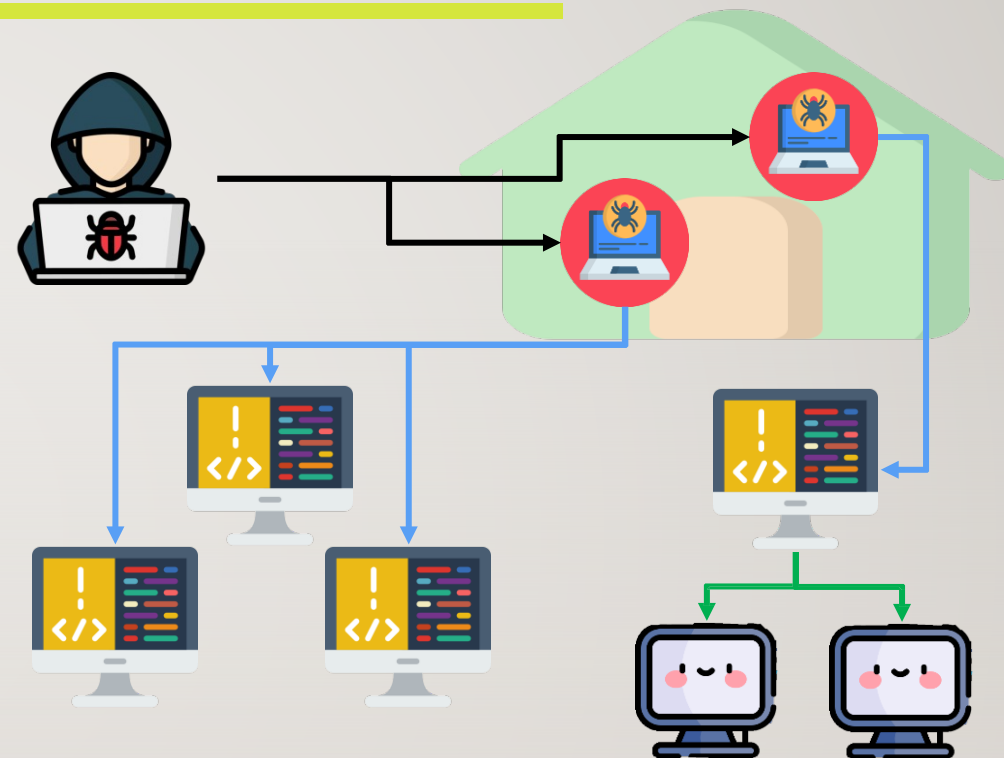


防護建議

- 廠商應恪守機關資通安全政策及委外廠商管理相關規範要求
- 攜帶之設備或工具應確保安全無虞，方可連線至機關內部網路

案情提要

- 機關發現多個外部觀測站設備，被維護廠商IP/帳號遠端桌面登入後執行勒索軟體，造成資料被加密無法存取使用
- 遭感染的觀測站又連結到其他觀測站，以致被加密範圍擴大



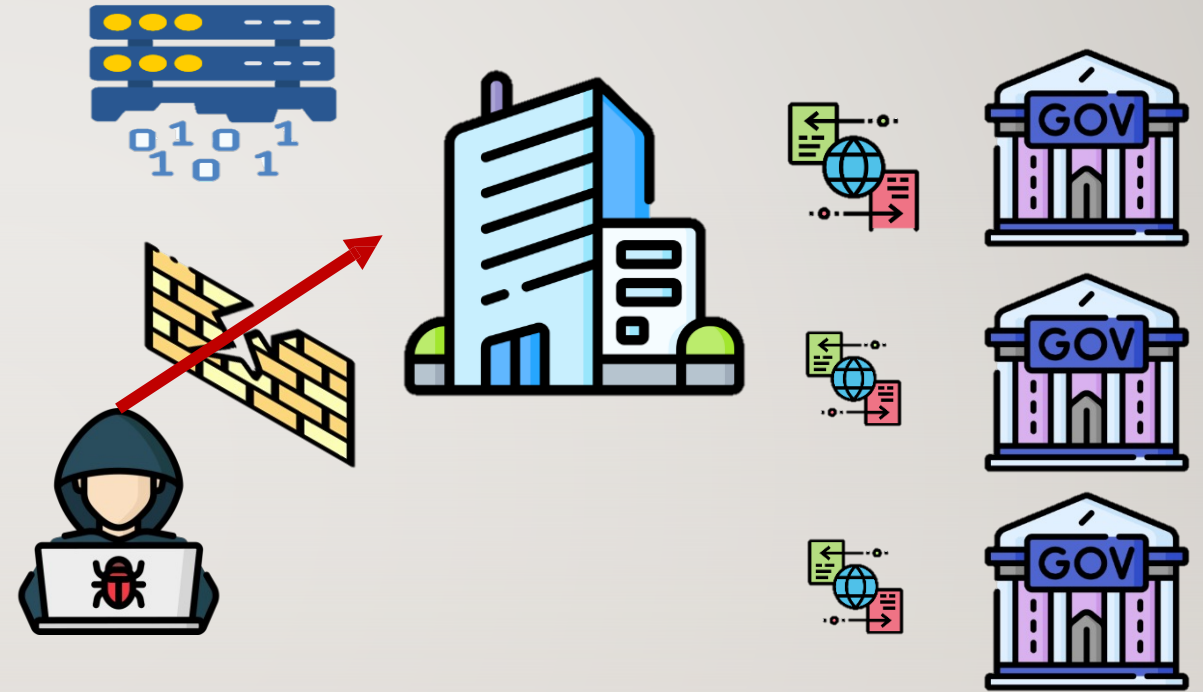
防護建議

- 遠端維護作業應採「原則禁止、例外允許」方式進行，如開放遠端存取，應以短天期為限，並建立連線行為管理機制
- 維護廠商使用之密碼，亦應依照機關資通安全相關程序，定期變更

供應鏈廠商維護環境或管理疏失(3/3)

案情提要

- 機關因委請廠商執行系統開發作業，以致廠商持有機關相關業務資料
- 廠商端防護作業未落實，導致位於廠商端之機關資料外洩



防護建議

- 廠商如欲於其場域內建置測試環境，應依機關之資安責任等級，設置對應之防護、必要檢測及採白名單限制存取來源及帳號
- 所收集之資料使用完畢，應依機關程序要求，徹底刪除並留存刪除過程

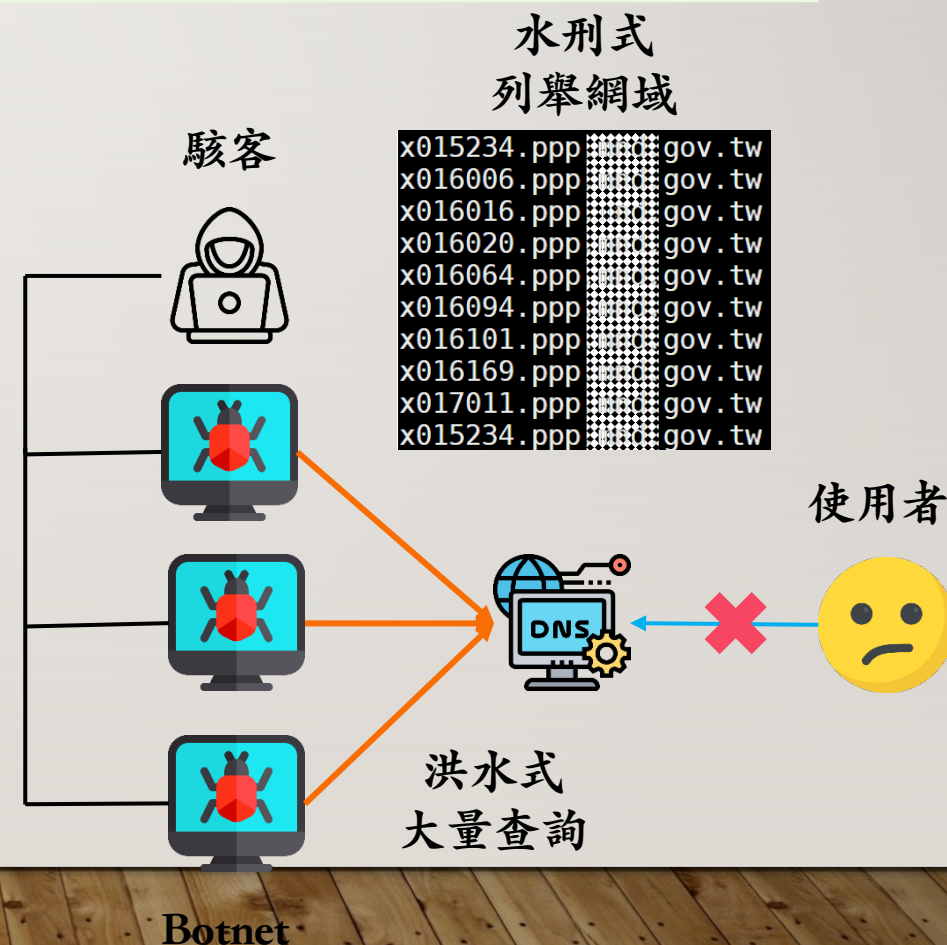
政府機關DNS遭DDoS攻擊案例

案情提要

- 機關對外服務網站無法正常提供服務，經分析DNS遭受DDoS攻擊
- 遭受混合式DNS攻擊
 - 洪水攻擊(Flood Attack)
 - 水刑式攻擊(DNS Water-torture)
- 攻擊期間共查詢約1000萬(10,160,541)個網域名稱，14小時內共計查詢次數約1億5千400萬次

防護建議

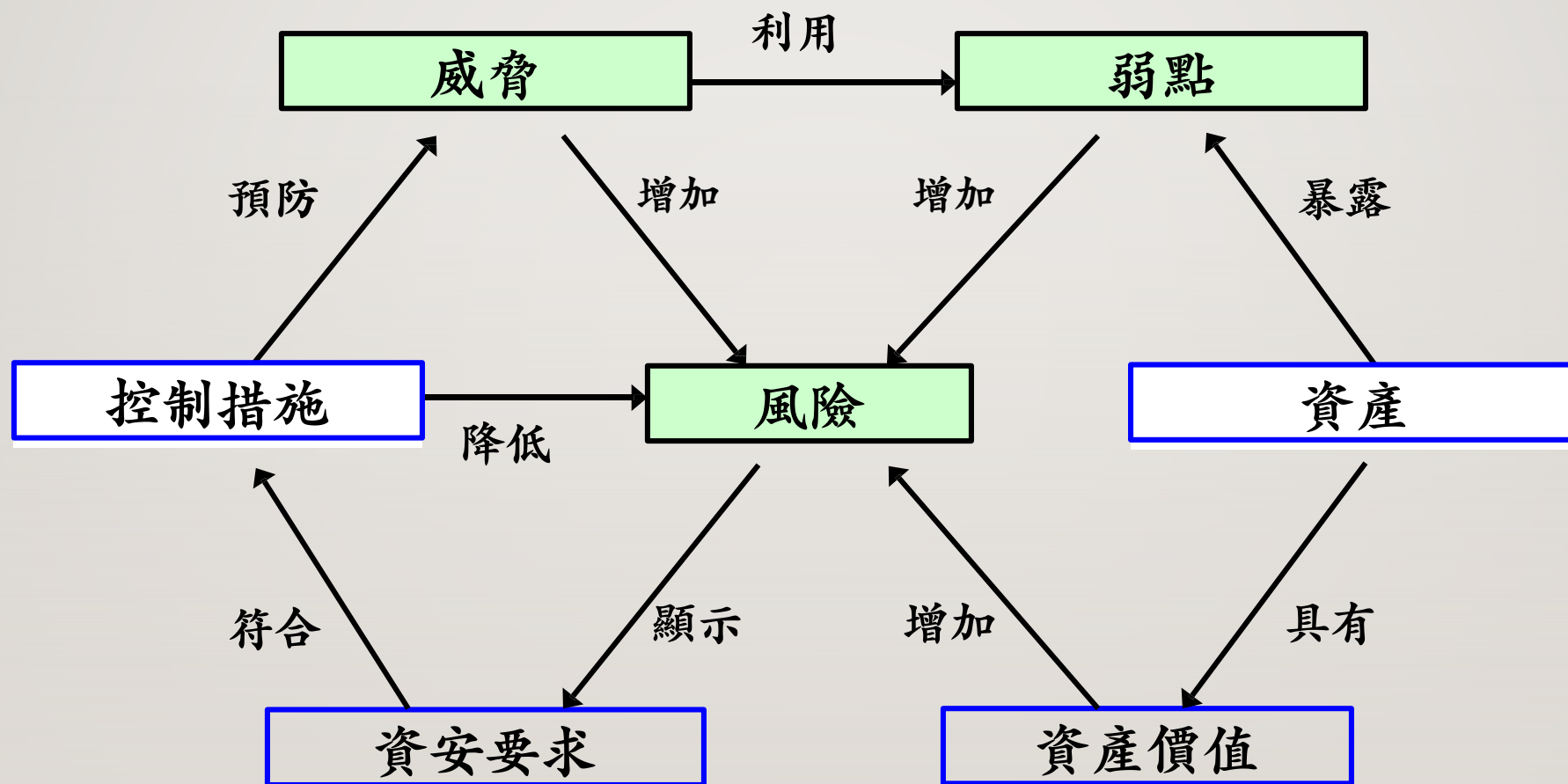
- 採購流量清洗服務
- 限制查詢次數，並避免成為Open Resolver



大綱

- 資安威脅趨勢
- 資安管理原則
 - 資安管理要素
 - 資安治理架構
- 資安防護重點

資安風險之形成



資安管理要素(1/4)

- 資安管理範圍包括資料、系統、設備、網路及實體安全等，需採行適當及充足之資安防護措施以降低風險

Non-repudiation (不可否認性)

CIA + N + 3A

Confidentiality (機密性)

Integrity (完整性)

Availability (可用性)

Authentication (身分鑑別)

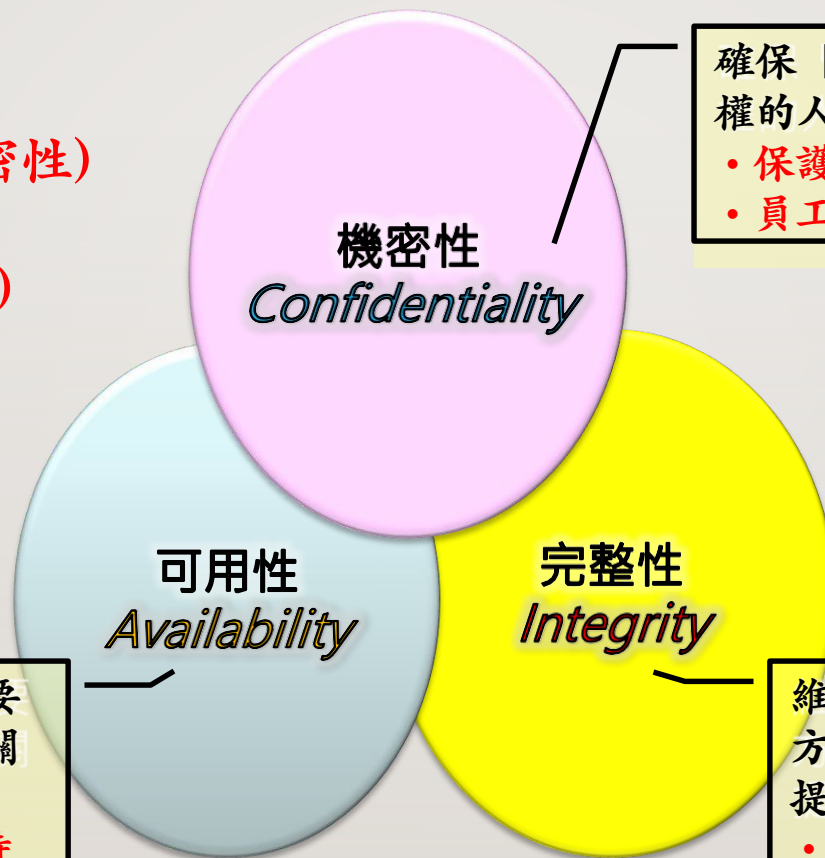
Authority (存取權限控制)

Accountability (可歸責性)

資安管理要素(2/4)

CIA:

- Confidentiality (機密性)
- Integrity (完整性)
- Availability (可用性)



確保「資訊」只能被經過授權的人員使用

- 保護智慧財產(程式原始碼)
- 員工個人資料

確保經過授權的人員在需要時可以存取「資訊」及相關資產

- 確保金融轉帳服務24小時可存取使用
- 確保保全監控系統24小時運作

維護「資訊」和其「處理方法」之真確性和完整性提供防護措施

- 稅務資料送出後不被變更
- 銀行交易資料傳輸過程不被第三者竄改

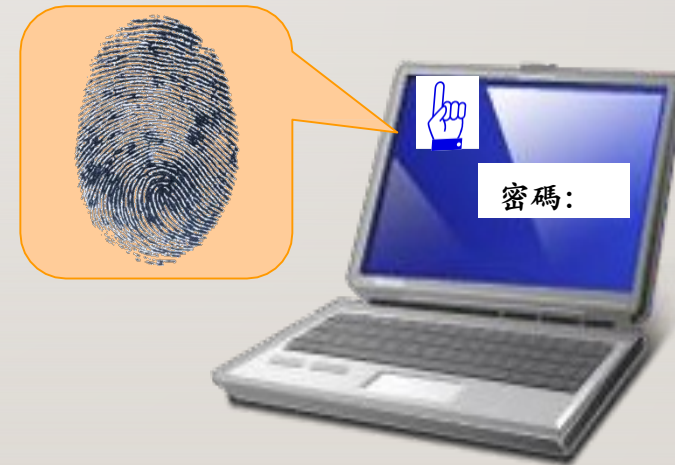
資安管理要素(3/4)

● 不可否認性(Non-repudiation)

- 防止存心不良的使用者否認其所做過的事，包括送出信件，接收文件，存取資料等。即交易的收發雙方無法否認執行過的交易
- 如【數位簽章】就具備不可否認性

● 身分鑑別(Authentication)

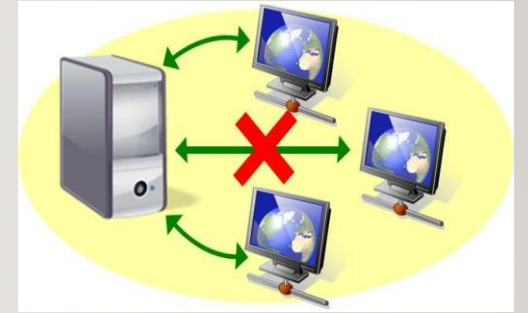
- 辨別資訊使用者的身份
- 可記錄資訊是被誰使用過
- 如帳號、身份字號、員工編號等



資安管理要素(4/4)

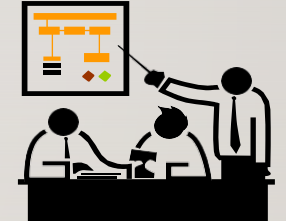
● 存取權限控制(Authority)

- 依照職務或階級身份給予適當的權限
- 如銀行的櫃臺是不被允許進入保險櫃，僅有組長以上的權限才能進入



● 可歸責性(Accountability)

- 所有主要的資訊資產應有人負責，並指定資產的所有人負責保護，管理紀錄必須是可追溯的



資安管理制度

- 資訊安全管理制度係依循CNS/ISO 27001標準，以風險評估管理為架構，涵蓋所有與資安相關議題，是一套完整的資安應用與稽核標準
- 政府機關於建置時，可透過規劃(Plan)、執行(Do)、改善(Check)及行動(Act)之管理循環，確保資訊安全管理制度的有效性，並落實資訊安全工作，持續有效控管資安風險，維持政府機關正常運作

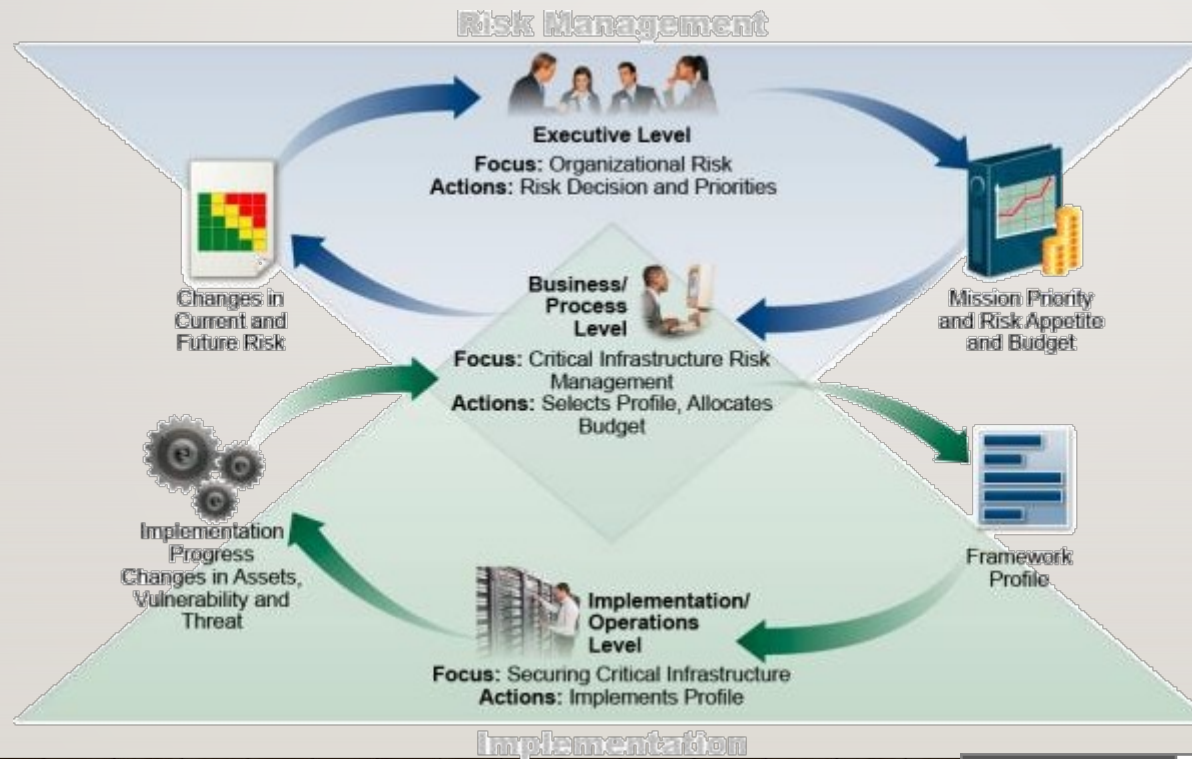
大綱

- 資安威脅趨勢
- 資安管理原則
 - 資安管理要素
 - 資安治理架構
- 資安防護重點

國際資安治理趨勢

● 美國國家標準技術研究所(NIST)

- NIST建議組織應透過由上而下且持續回饋的資安治理架構，以降低資安風險



管理層

管理階層應關注組織所面臨的威脅，並針對存在的風險決定因應措施及優先順序

業務層

應鑑別關鍵的業務與系統，確保重要業務所存在之潛在風險得以被完善的管控

維運層

依據管理階層的意向以及業務關鍵性，確保重要的資訊資產得以受到全面性的保護

資料來源

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

資安治理與資安管理差異(1/2)

● 資安治理定義

- 資安治理定義為建立與維護框架、支援管理之結構及程序，以及提供下列保證的過程：在努力管理風險下，使資安策略與業務目標一致、支援業務目標，藉由嚴守政策與內部控制以符合相關法規，以及提供職責之指派

資料來源

NIST SP800-100

- 資安治理為指導及控制組織資安活動之系統，目標在於確保資安目標及策略承接組織營運目標及策略

資料來源

CNS/ISO 27014

● 資安管理定義

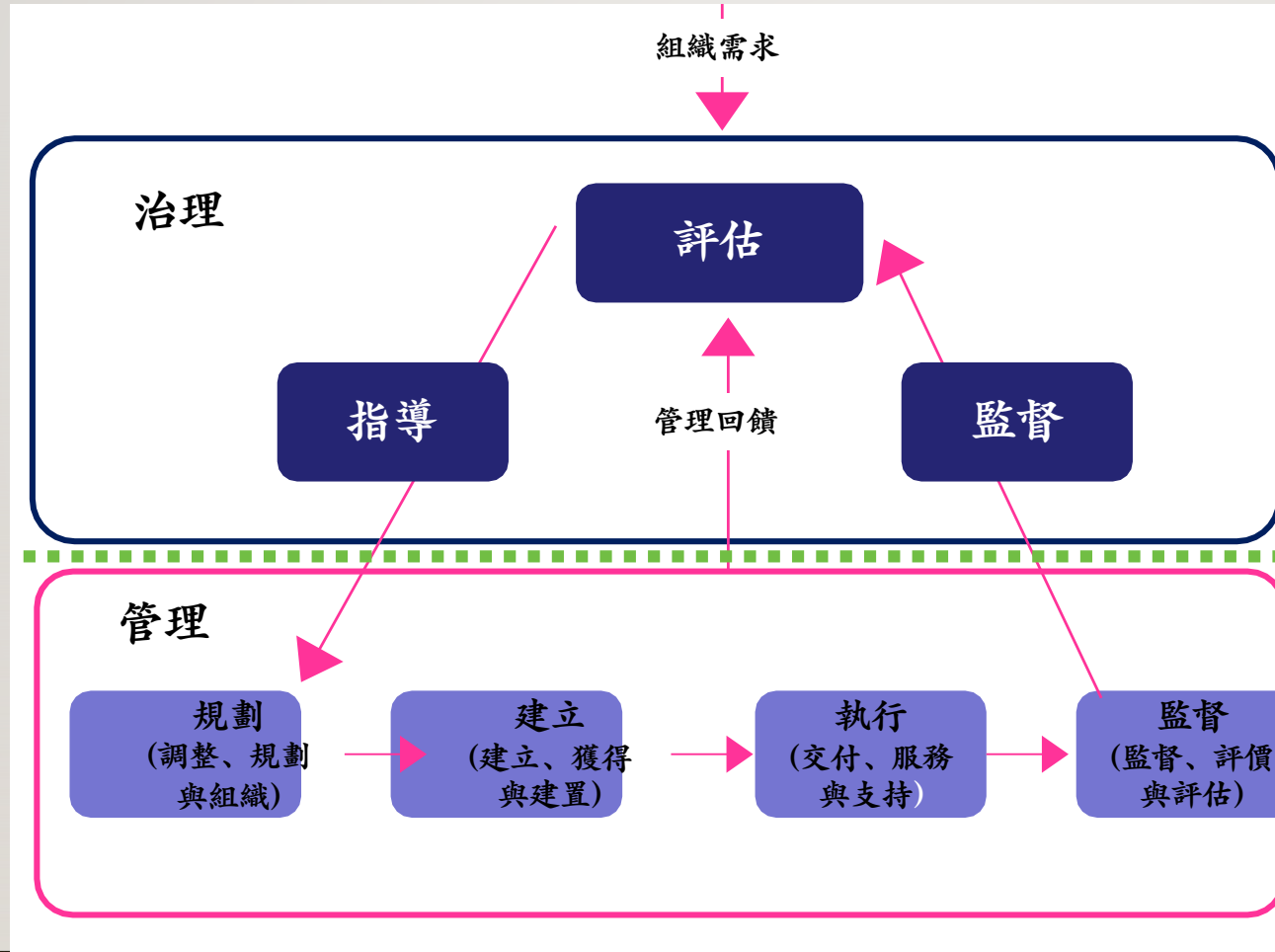
- 資安管理目的在於透過規劃、建立、執行及監督(PDCA)機制，保護資訊資產的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)

資料來源

CNS/ISO 27001

資安治理與資安管理差異(2/2)

● 治理與管理的關鍵領域



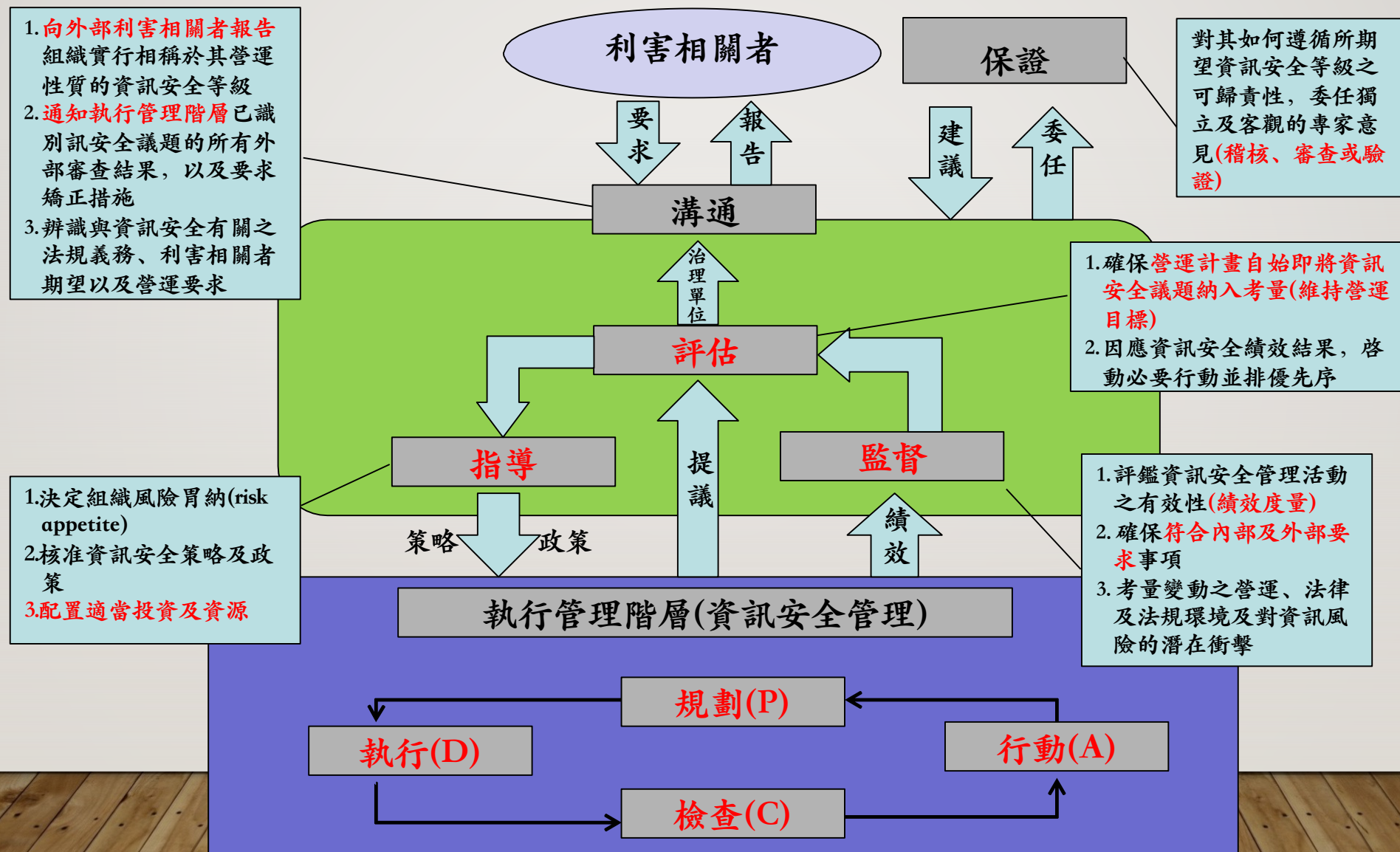
以 評估 (Evaluate)、指導 (Direct)、監督 (Monitor) 建立 治理架構，向下監督、管理資安管理執行機制，並透過 治理架構 向上溝通，回應組織利害關係人之要求

遵循治理架構所形成之 指導原則，規劃與建立組織適用之 管理機制，並透過日常維運執行與監督的過程確保其持續改善，並提供組織得以再次評估之管理回饋

CNS/ISO 27014資安治理六大原則



CNS/ISO 27014資安治理模型



大綱

- 資安威脅趨勢
- 資安管理原則
- 資安防護重點
 - 主動式防禦策略
 - 零信任架構推動
 - 資安防護建議

MITRE ENGAGE(1/2)

- 著重於於阻斷(Denial)、欺敵(Deception)及對手交戰(Adversary Engagement)，包括5大目標、9大交戰方法

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

MITRE ENGAGE(2/2)

- 9大交戰方法中，前2大方法主要以**警示與防護**為主，適合所有企業組織進行資安防禦，後續7大方法則以**欺敵與情蒐**為主

方法		說明
規劃	Plan	協助防禦者釐清目標，確保每項操作能有效率且安全
蒐集	Collect	蒐集攻擊者情資，可供其他防禦機制參考
偵測	Detect	針對攻擊者行為，透過偵測機制進行警示通知
預防	Prevent	限制攻擊者進入不可控環境，如阻止攻擊者橫向移動
指引	Direct	引導攻擊者移向或遠離預期路徑
破壞	Disrupt	阻止攻擊者執行部分或全部任務，增加其攻擊難度
擬真	Reassure	增加欺敵技術之真實性，如於假環境中，創建真實帳號使攻擊者認為此環境為真實使用環境
動機	Motivate	釋出假訊息或系統，測試是否引起攻擊者興趣，並透過取得系統控制權之難易度，測試攻擊者能力
分析	Analyze	分析可用於將數據轉化為關於攻擊者之動機、行為、策略及技術等可操作情資

主動式防禦推動策略

網路攻擊狙殺鏈(Cyber Kill Chain)

偵查

(Reconnaissance)

研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境。

武裝

(Weaponization)

針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝。

遞送

(Delivery)

設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道。

攻擊

(Exploitation)

惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊。

安裝

(Installation)

於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中。

發令與控制

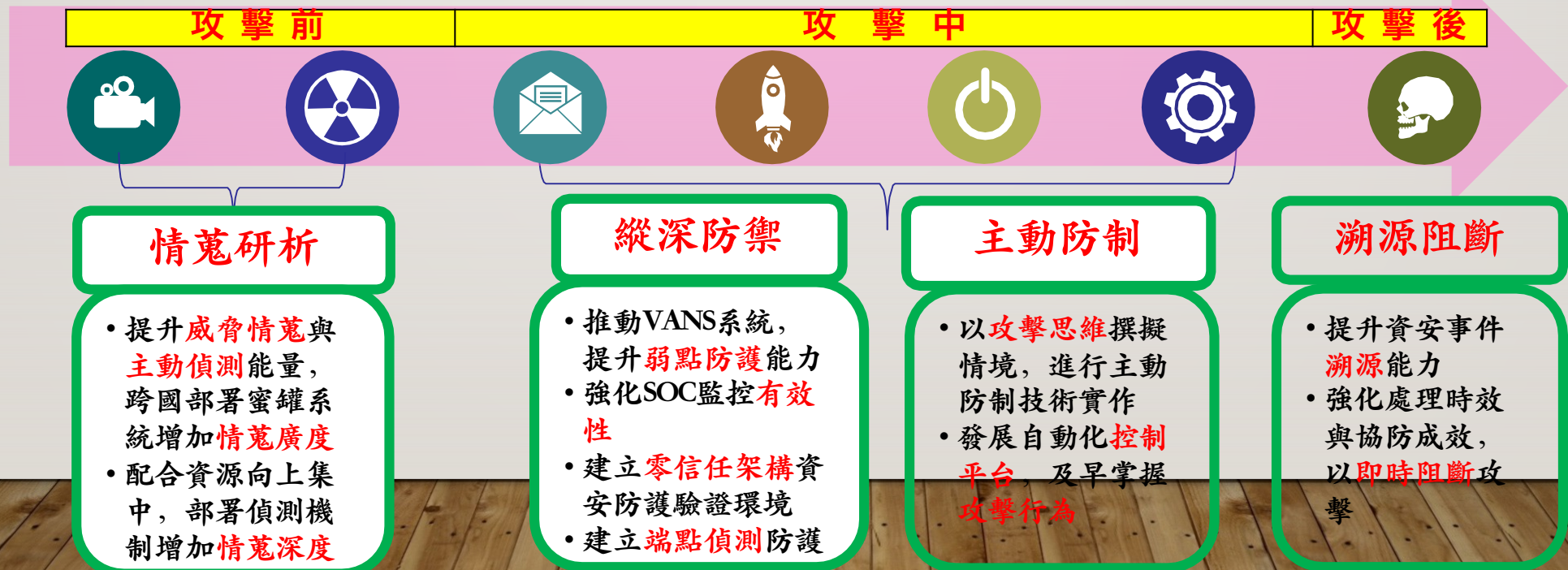
(Command and Control)

受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機。

採取行動

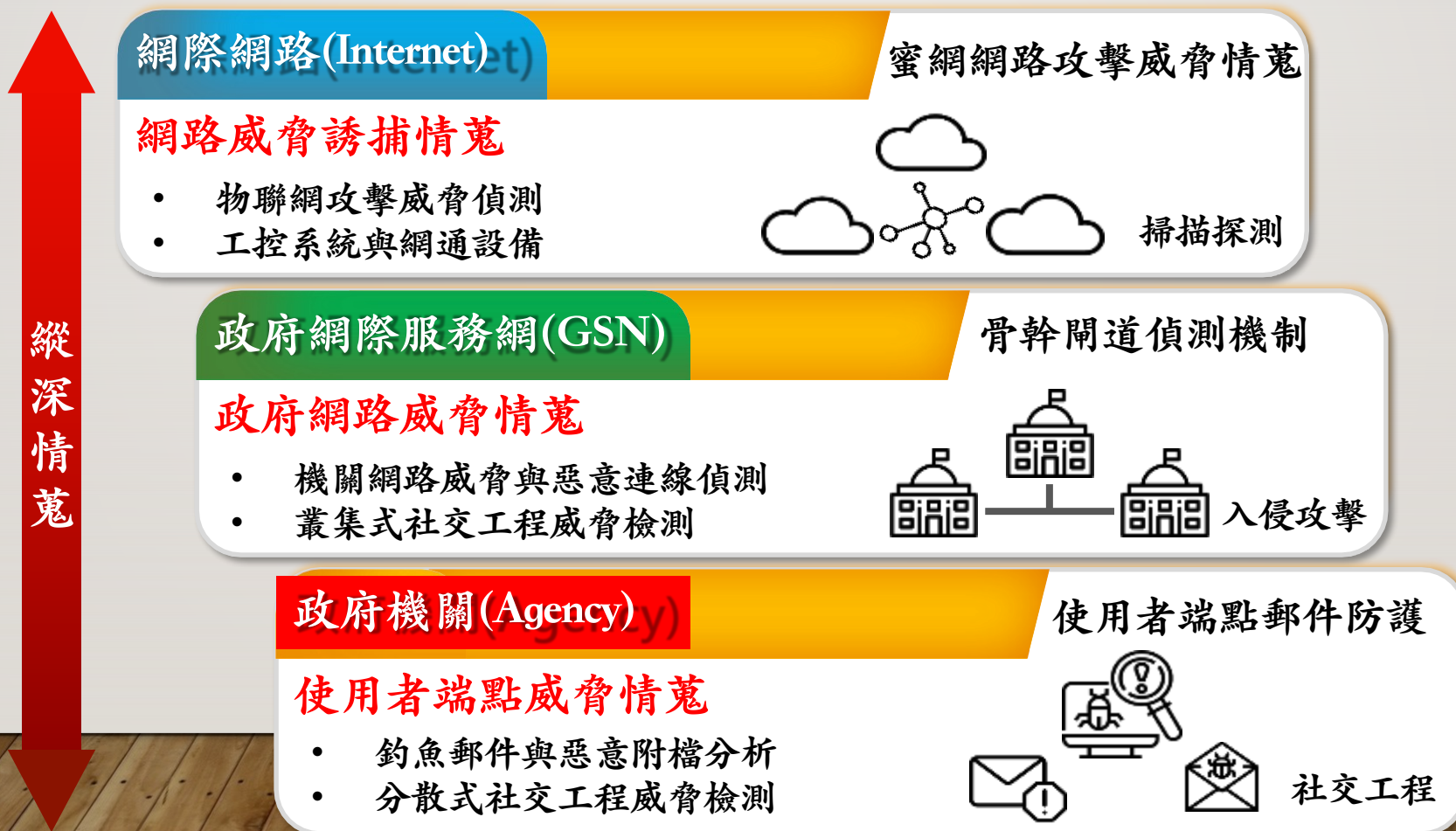
(Actions on Objectives)

攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板。

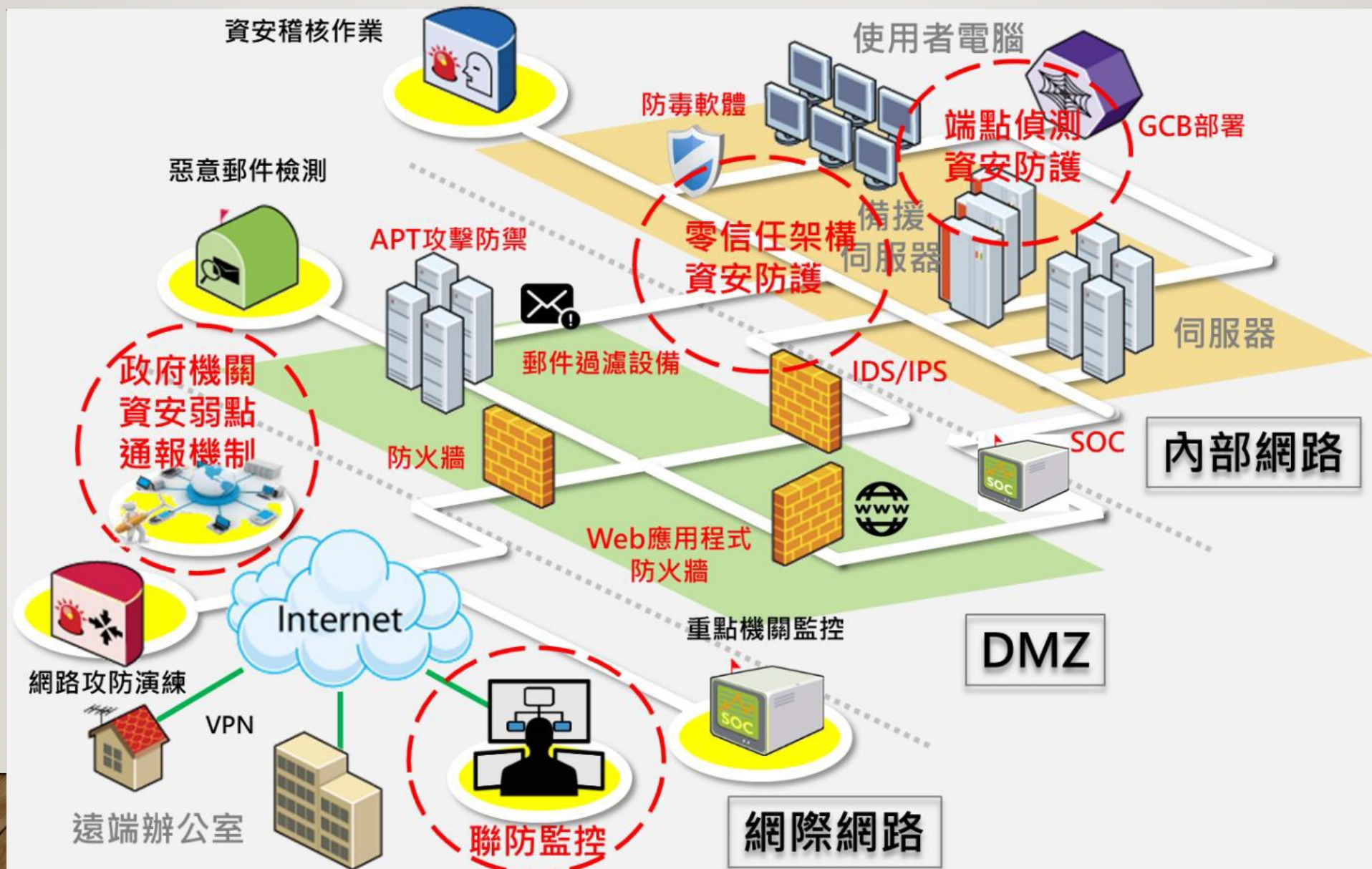


情資研析

- 從網際網路、政府網際服務網及政府機關3個面向，蒐集各種威脅資訊，並提供預防性情資，以達早期預警



縱深防禦



資通安全弱點通報(VANS)機制

- 結合資訊資產管理與弱點管理，將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊，並依風險情形完成安全性更新



註：VANS：Vulnerability Alert Notification System

政府領域資安聯防監控

SOC監控有效性驗證

- 政府機關：推動完善監控範圍
- SOC業者：依回傳能力、偵測能力及情資品質，驗證監控成效

政府機關資安監控範圍

- 「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄

資通 安全 防護	• 防毒軟體
	• 網路防火牆
	• 電子郵件過濾機制
	• 入侵偵測及防禦機制
	• 應用程式防火牆
	• 進階持續性威脅攻擊防禦措施

回傳能力

- 資安監控情資格式與回傳率
- 資安防護項目回傳率

偵測能力

- 網路攻防演練驗證
- 技服中心資安警訊驗證
- 機關通報資安事件驗證

情資品質

- 資安監控情資品質分析
- 資安監控情資回饋能量

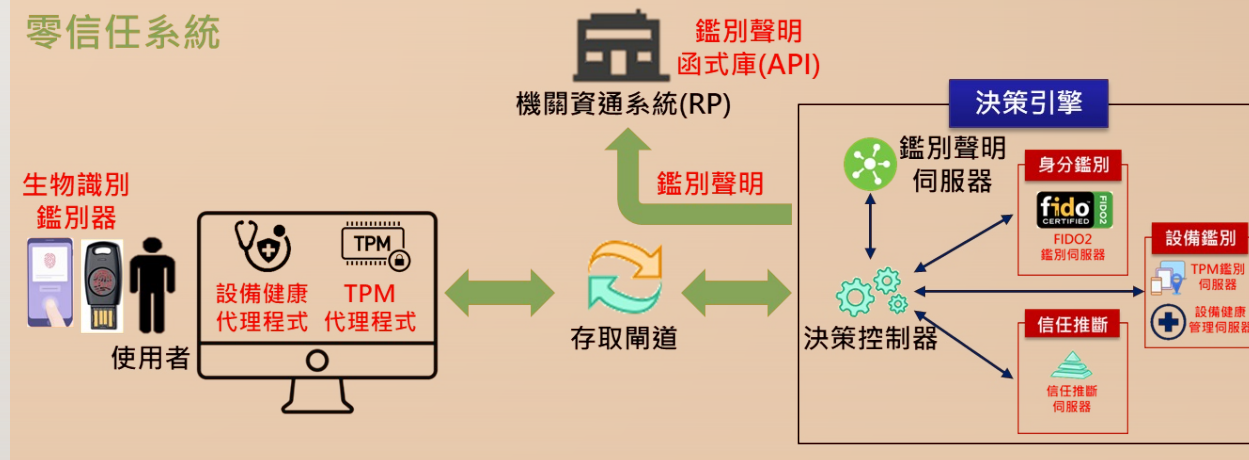
政府零信任架構

- 參考NIST零信任架構，採取資源門戶之部署方式 (Resource Portal-Based Deployment)，包含3大核心機制
 - - 身分鑑別：多因子身分鑑別與鑑別聲明
 - - 設備鑑別：設備鑑別與設備健康管理
 - - 信任推斷：使用者情境信任推斷機制

現有系統

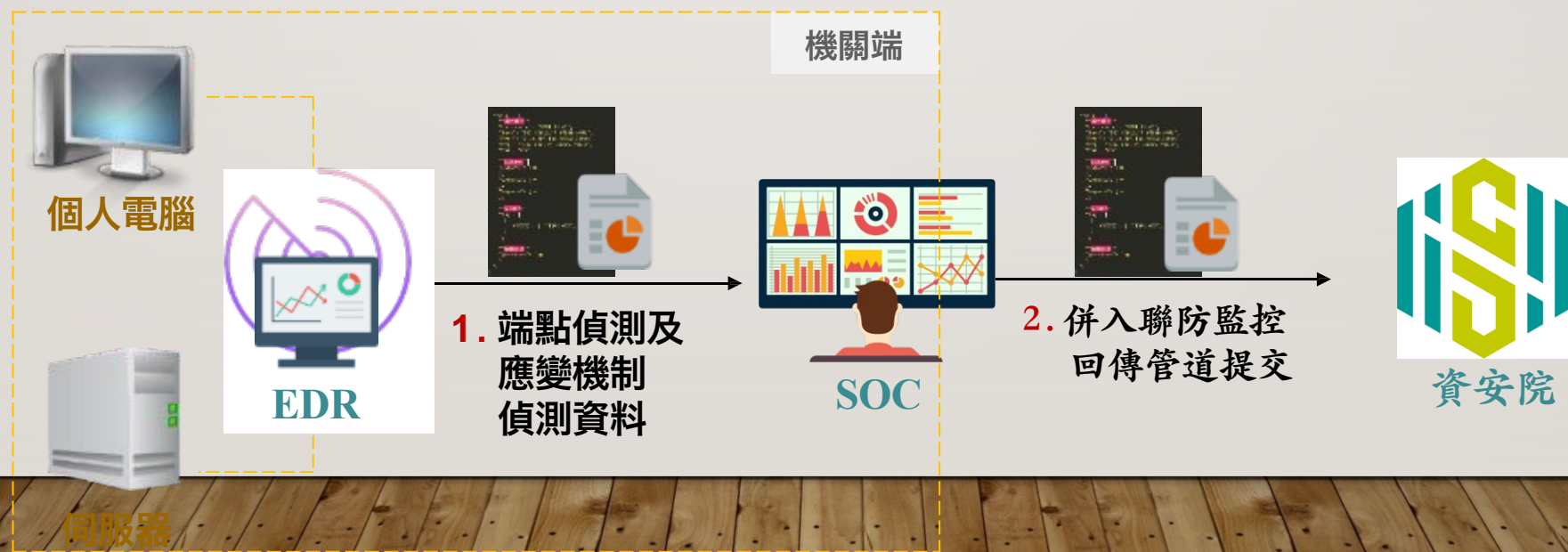


零信任系統



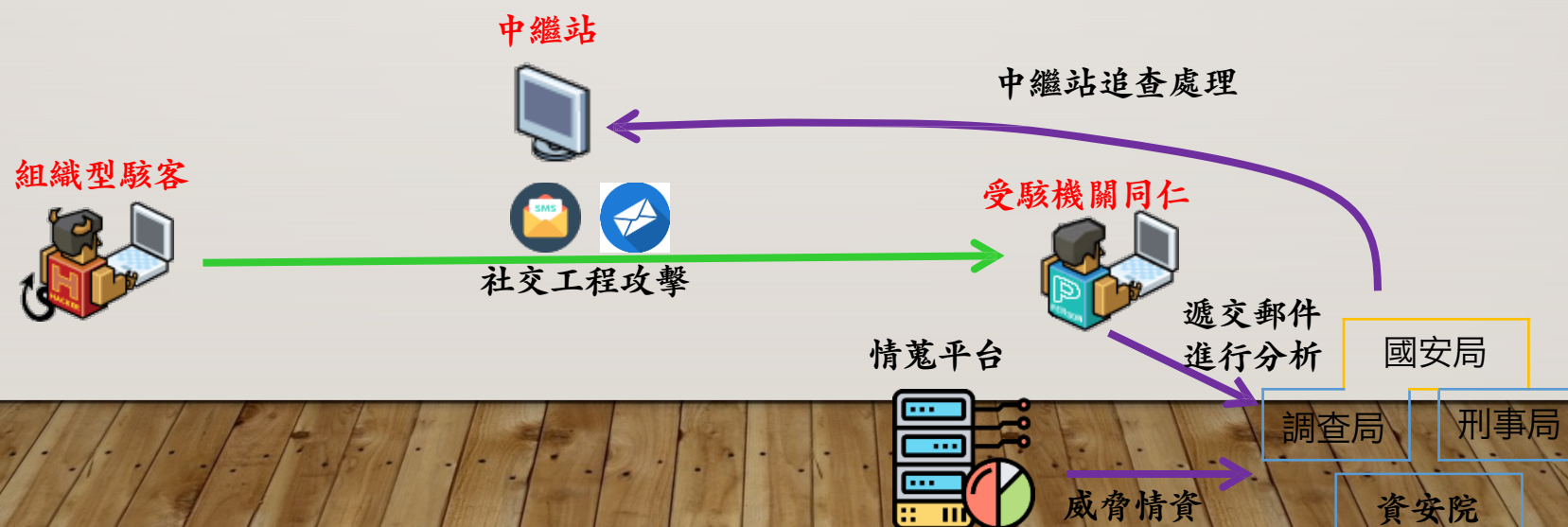
端點偵測及應變(EDR)機制

- EDR偵測到異常行為或惡意程式活動，並確認成為**資安事件**時，由機關SOC依特定格式，透過現有**聯防監控資料回傳管道**提交至主管機關
 - － 非遭入侵類型通報(如DDoS、停電等)則不需回傳



主動防制

- 透過**主動出擊**，減弱與破壞駭客相關資源，協助政府機關防護
 - 109年4月微軟偕同台灣在內之35國執法單位，摧毀Necurs殭屍網路
- 進行**主動防制技術研究與合作**
 - 針對駭客常用之攻擊手法進行分析
 - 透過威脅情資，及時掌握駭客活動
 - 搭配適時處理與應變防制，降低政府機關資安風險



溯源阻斷

- 當資安事件發生，啟動**聯防作業**，透過**鑑識調研**，掌握**攻擊來源**，並阻斷**攻擊行為**
 - 針對發現之國內外**中繼站**，協同相關單位共同調研取證，進一步追查攻擊來源，達到**追蹤溯源**目的
 - 配合**端點鑑識**即時告警，達到**連線阻斷**目的

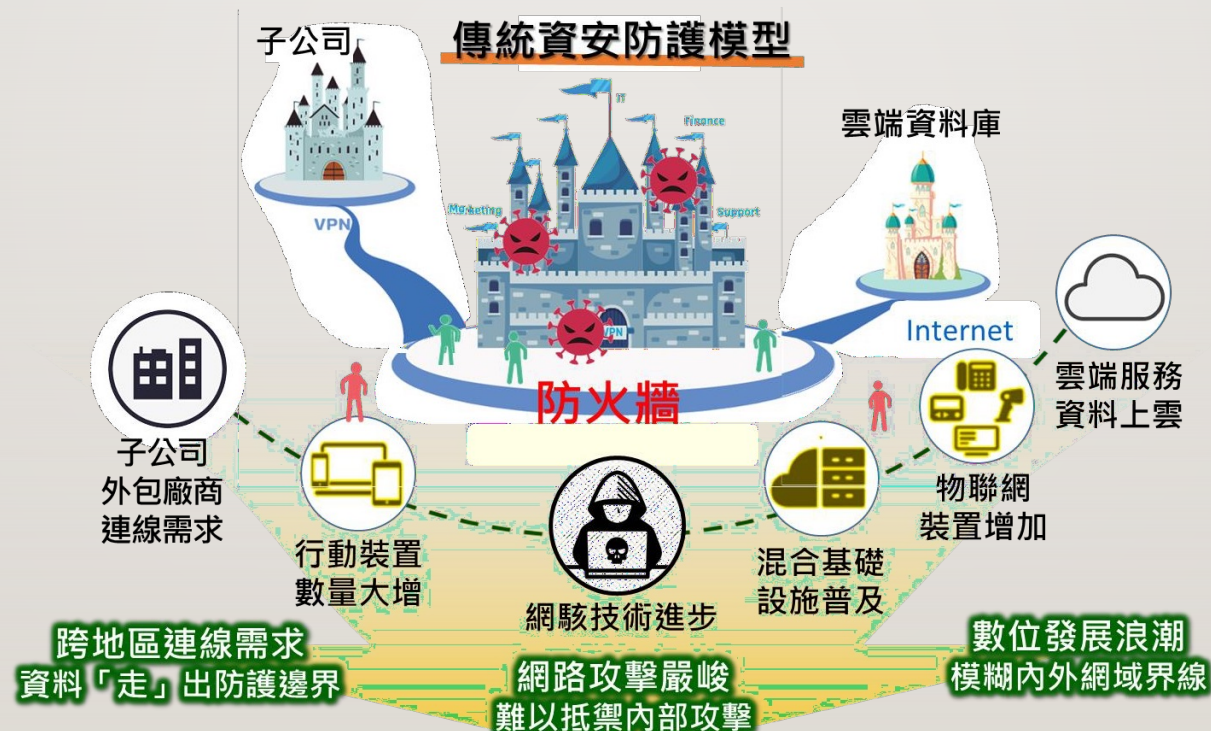


大綱

- 資安威脅趨勢
- 資安管理原則
- 資安防護重點
 - 主動式防禦策略
 - 零信任架構推動
 - 資安防護建議

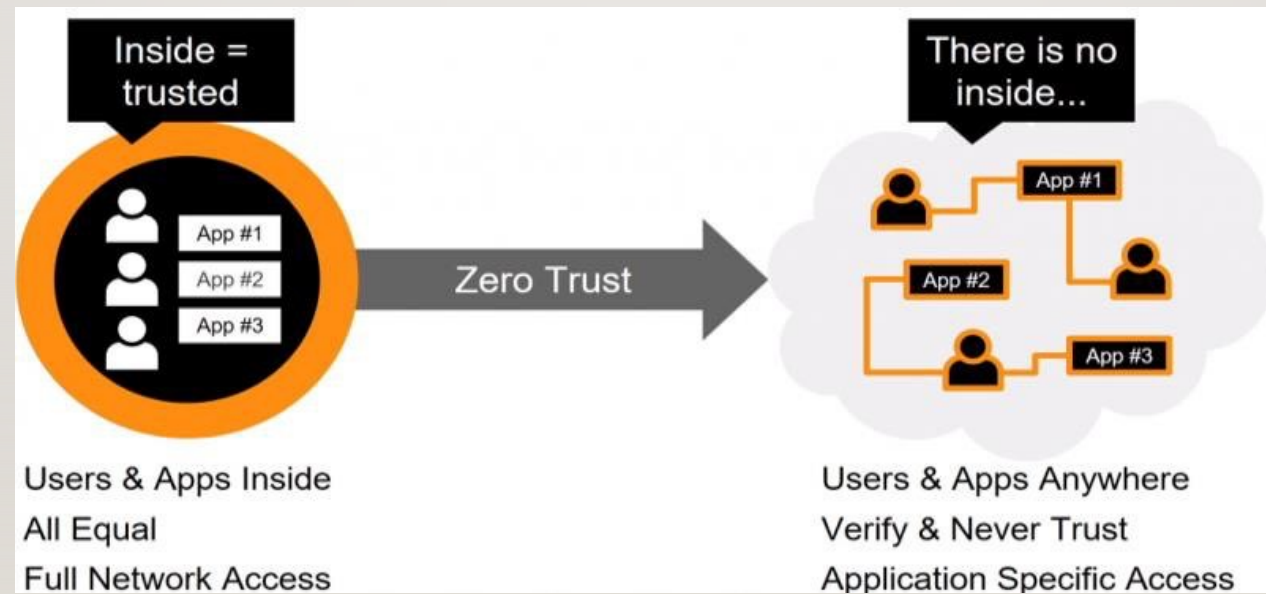
傳統網路模型之資安窘境

- 隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已現資安窘境，難以滿足新形態工作需求



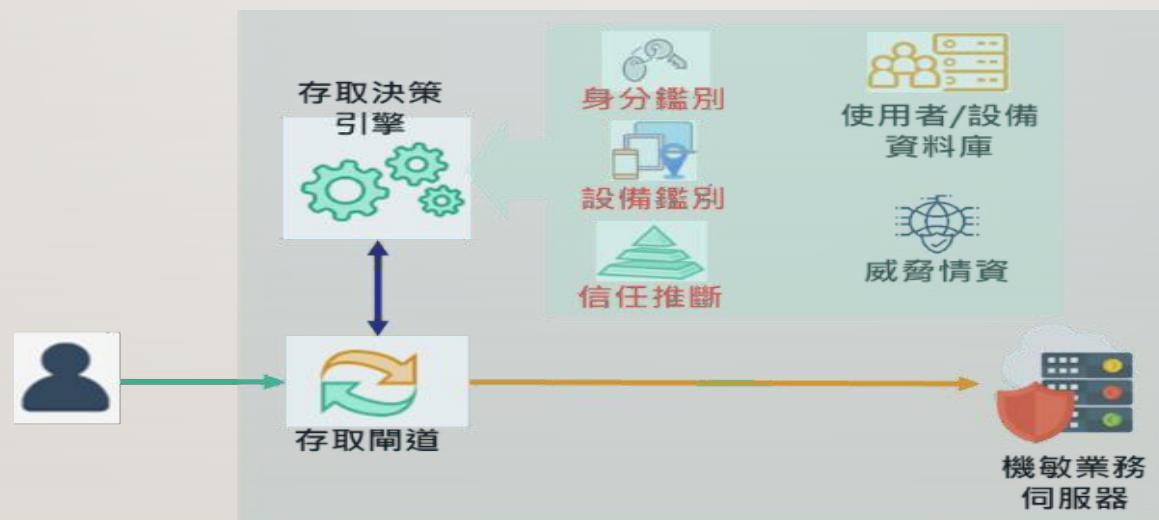
零信任概念

- 突破傳統網路模型之資安窘境，保護資料存取
 - 非保護網路存取，聚焦**保護資料/應用存取**
 - 無具體邊界，使用者/設備與資料/應用無處不在
 - 任何資料存取**永不信任**(Never Trust)且**持續驗證**(Always Verify)



NIST零信任推動建議

- 2020年美國國家標準技術研究院(NIST)正式頒布標準文件SP 800- 207**零信任架構**(Zero Trust Architecture, ZTA)，成為各界採用基礎
 - 零信任網路以**決策引擎**為核心，包含**身分鑑別**、**設備鑑別**及**信任推斷**3大關鍵技術
 - 實施零信任會是一段**過程**，而不是一次大規模替換基礎架構，且與傳統模式會同時**混合運作**



零信任架構

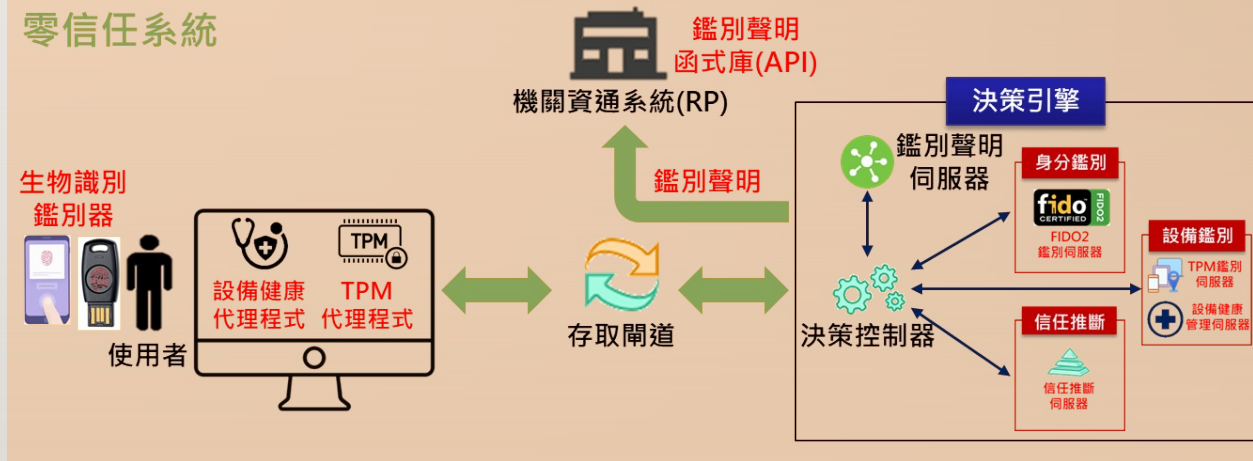
政府零信任架構

- 參考NIST零信任架構，採取資源門戶之部署方式(Resource Portal-Based Deployment)，包含3大核心機制
 - - 身分鑑別：多因子身分鑑別與鑑別聲明
 - - 設備鑑別：設備鑑別與設備健康管理
 - - 信任推斷：使用者情境信任推斷機制

現有系統



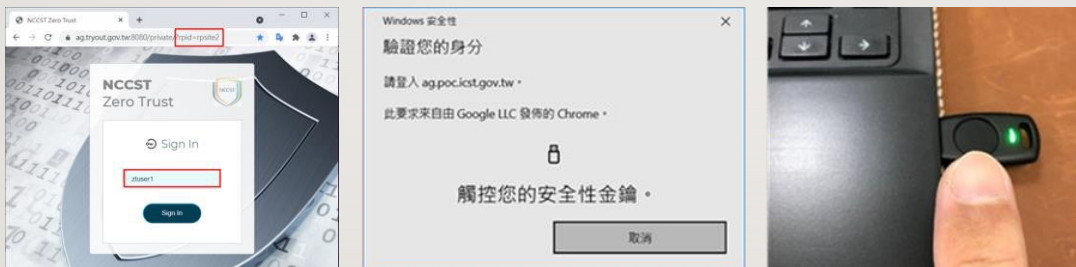
零信任系統



身分鑑別

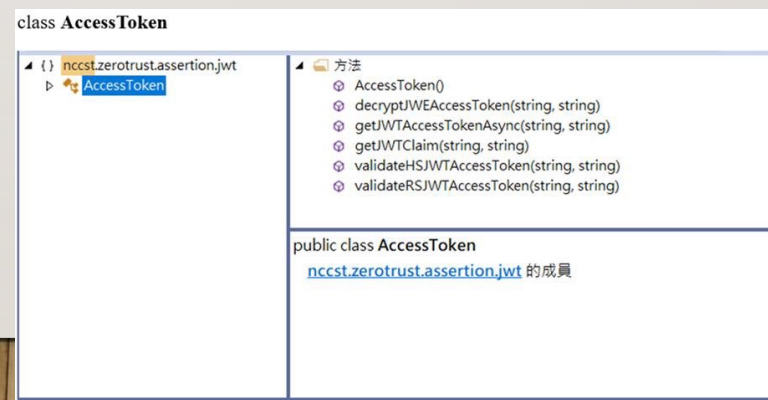
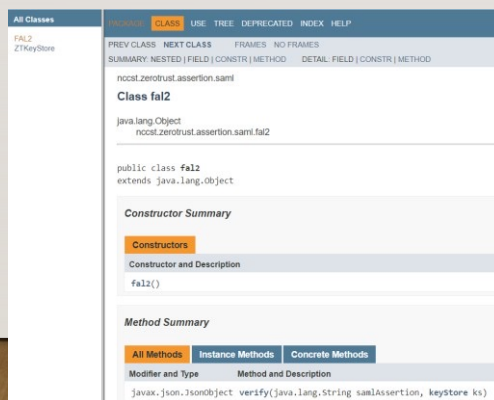
- 以無密碼雙因子方式達成身分鑑別

- 運用如FIDO2相關技術鑑別使用者之身分



- 提供具備簽章與加密之鑑別聲明

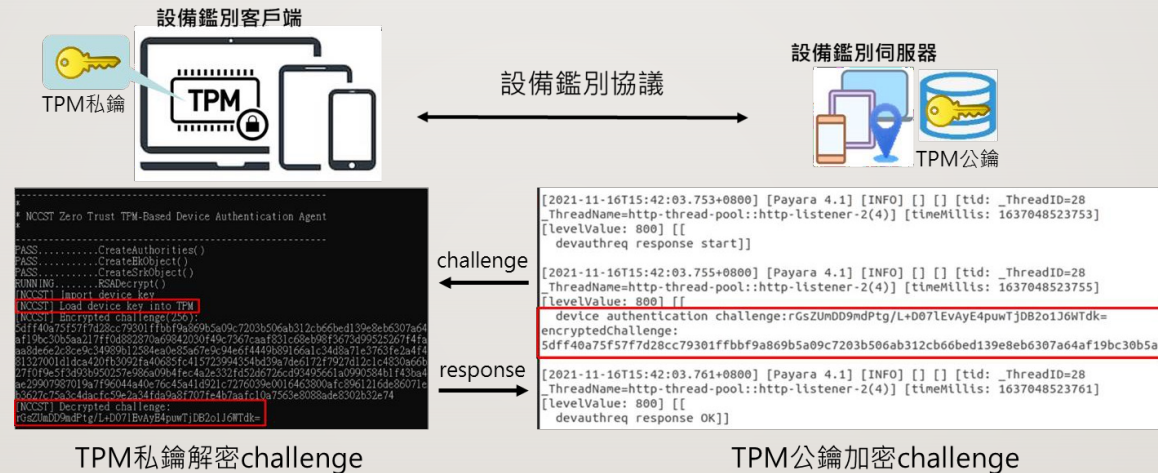
- 提供API函式庫，使機關之資通系統(RP)可解密並驗證鑑別聲明以確保其機密性與完整性



設備鑑別

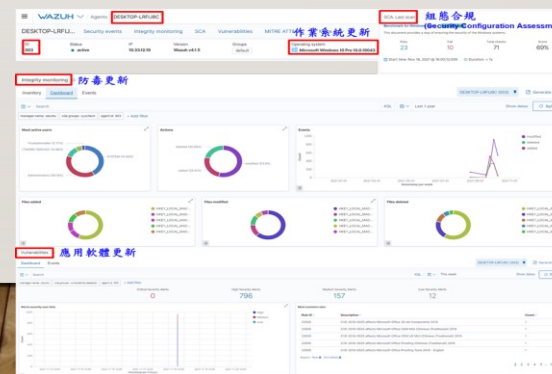
● 基於公開金鑰技術之設備鑑別方法

- 透過TPM或Agent產生金鑰與憑證，完成設備註冊與鑑別



● 設備健康管理

- 持續性設備健康狀態監控
- 依設備健康狀態計算設備健康信任等級



設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

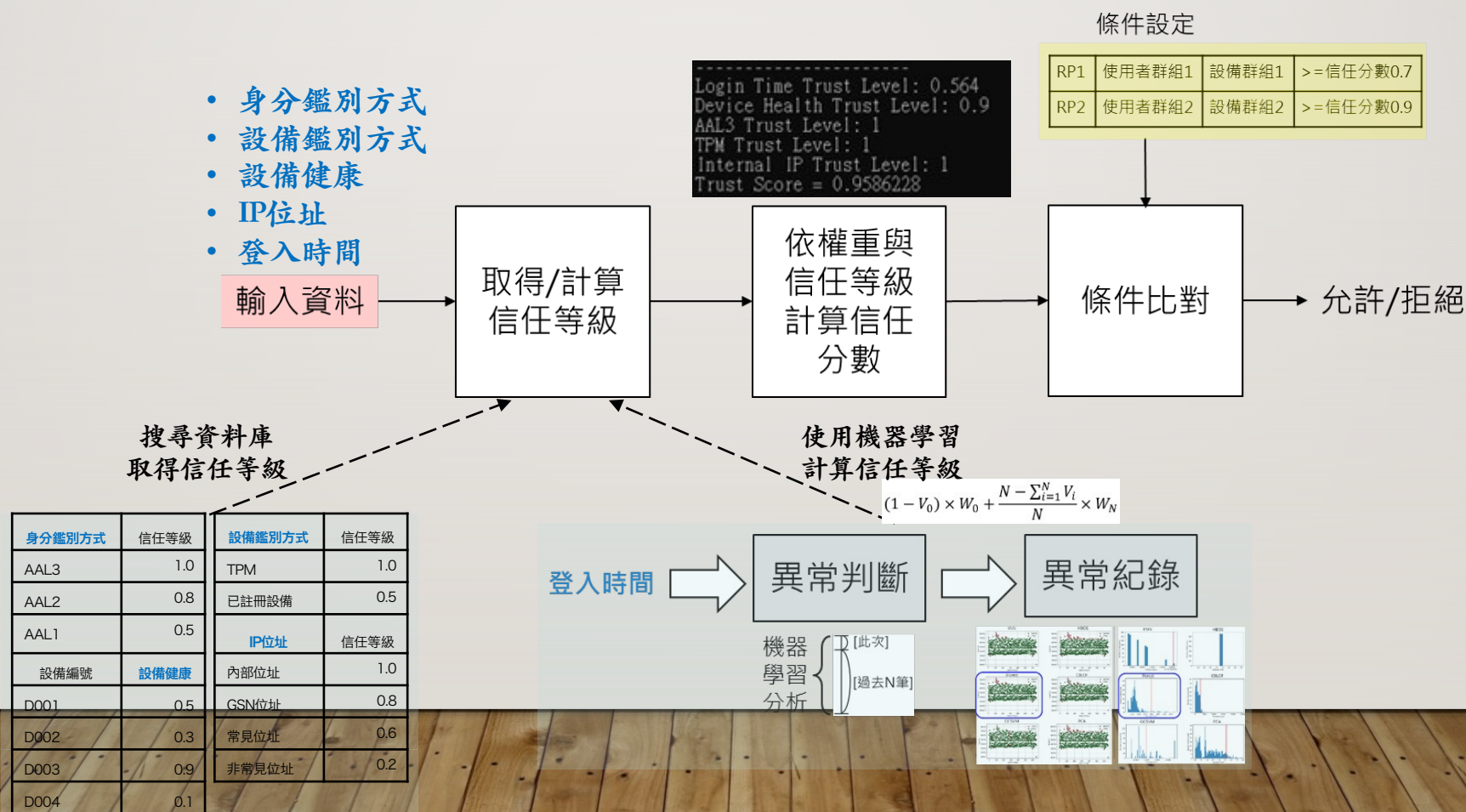
健康狀態/等級分配

- (A)作業系統更新：0.4
- (B)防毒更新：0.3
- (C)應用軟體更新：0.2
- (D)組態合規：0.1

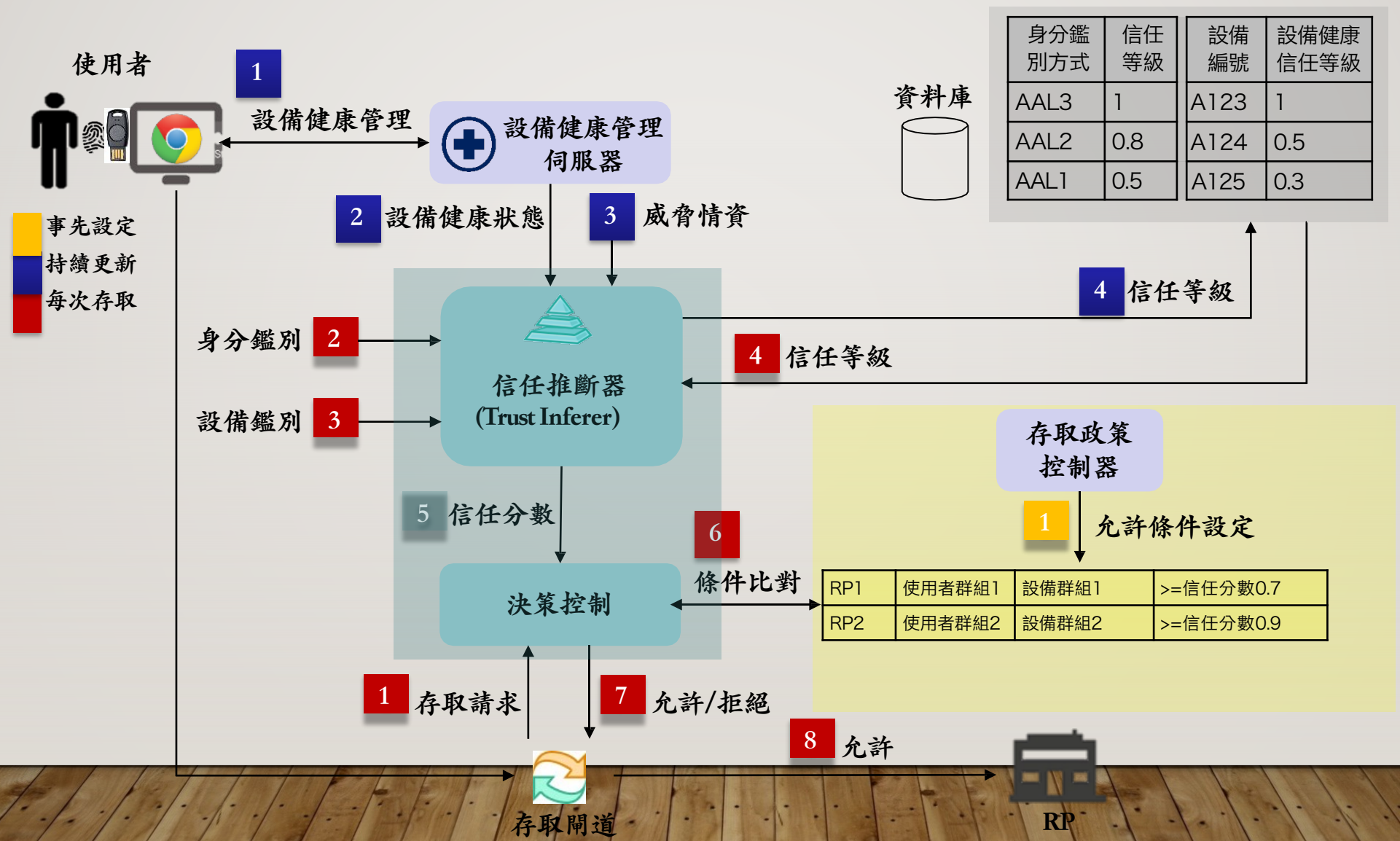
信任推斷

● 基於信任推斷機制決定存取權限

- 依使用情境計算每次存取之信任分數作為判斷依據



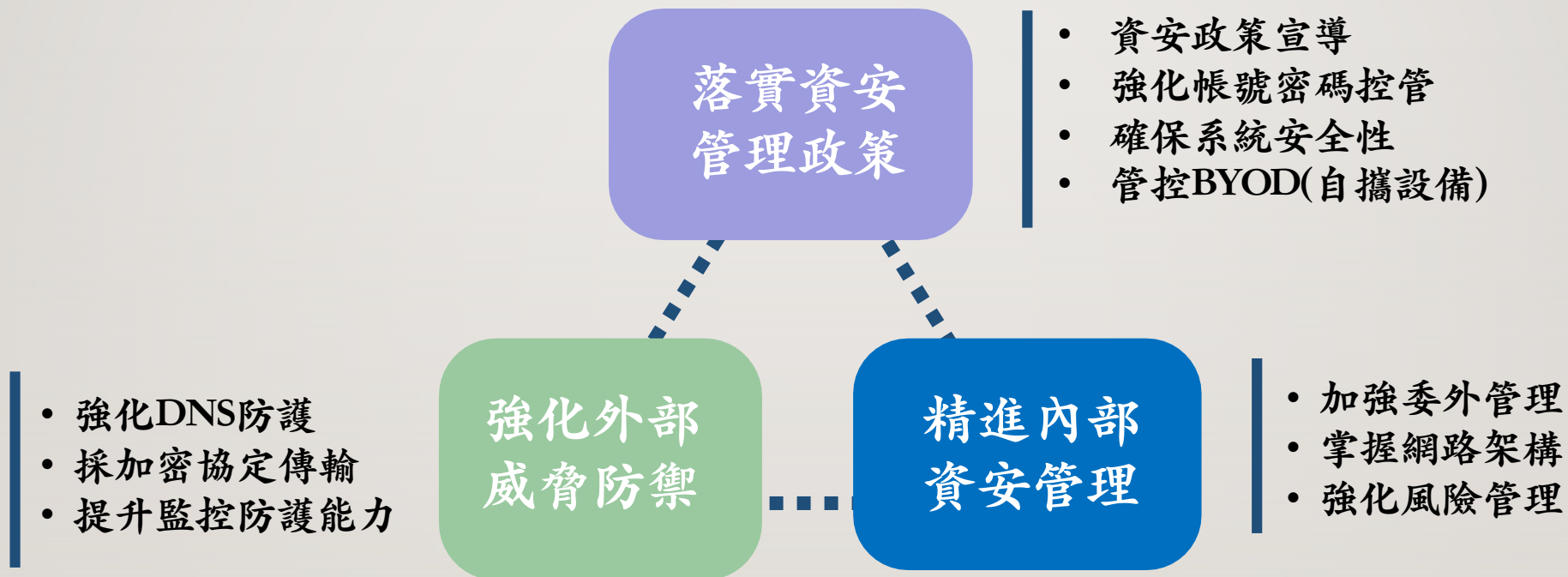
完整零信任登入流程



大綱

- 資安威脅趨勢
- 資安管理原則
- 資安防護重點
 - 主動式防禦策略
 - 零信任架構推動
 - 資安防護建議

提升資安防護能力



落實資安管理政策

資安政策宣導

- 政策訂定及宣導
- 政策定期檢討
- 認知與訓練

強化帳號管控

- 提升密碼強度
- 身分驗證加密傳輸
- 最小權限原則
- RBAC、GCB

落實資安管理政策

確保系統安全

- 安全性檢測
- 網頁內容過濾
- 事件日誌管理

管控BYOD

- BYOD政策審查
- 資安防護措施
- 流量管控

強化外部威脅防禦



精進內部資安管理

加強委外管理

- ◆ 確保履約服務水準
契約SLA
- ◆ SOC納入驗證範圍
納入機關ISMS驗證
範圍
- ◆ 落實委商資安稽核
每年應擇商辦理
- ◆ VPN管理
確實審查、導入雙
因子認證

掌握網路架構

- ◆ 落實資產盤點(VANS)
主機數量、服務目的、存取
控制
- ◆ 繪製網路架構圖
有助於整體安全性評估
- ◆ 納入行動裝置
需考量動態架構資安問題
- ◆ 定期辦理資安健診
共同供應契約-資安健診服
務-網路架構檢視

實施風險管理

- ◆ 常見漏洞揭露CVE
評估
N-ISAC情資分享
- ◆ 定期更新惡意中繼
站清單
至少每週至技服中
心下載更新
- ◆ Patch管理
定時更新

結論與建議(1/2)

- 社交工程攻擊仍為常見攻擊手法，機關應持續加強內部宣導，提升人員資安意識
 - 注意郵件來源正確性，慎防異常附件與連結
 - 注意個別系統之安全修補(含應用程式)與病毒碼更新
- 機關應落實資訊作業委外安全管理，敦促委外廠商遵守資安規範
 - 配合辦理系統防護需求分級原則與資通系統防護基準
 - 避免未經管制設備於機關環境中使用
 - 遠端維護作業應採「**原則禁止、例外允許**」方式進行
 - 如須開放遠端存取，應以**短天期為限**，並應建立**連線行為管理機制**

結論與建議(2/2)

- 關注資通訊設備漏洞情資，提升弱點防護能力，落實資安監控
 - 應隨時**關注資通訊設備之情資(漏洞資訊、零日攻擊)**，適時更新韌體版本或採行必要之防護設定
 - **導入端點偵測及應變機制**，強化資安監控與防護，落實資安防禦縱深
 - **落實日誌保存作業**，以利資安事件之鑑識分析

謝謝聆聽