資安攻擊與防範

顧 問 王高義

WHITE HAT RHINO

2025.09.25

資安概述

常見資安攻擊方式

近期案例

資安防護

WHITE HAT RHINO

方便、快速與危險

未來趨勢

縱深防禦 日趨增嚴的防護要求

資安防禦所需資源

- 防禦設備 (軟、硬體)
- 人員
- 預算

> > 以被攻破為前提思考資安措施

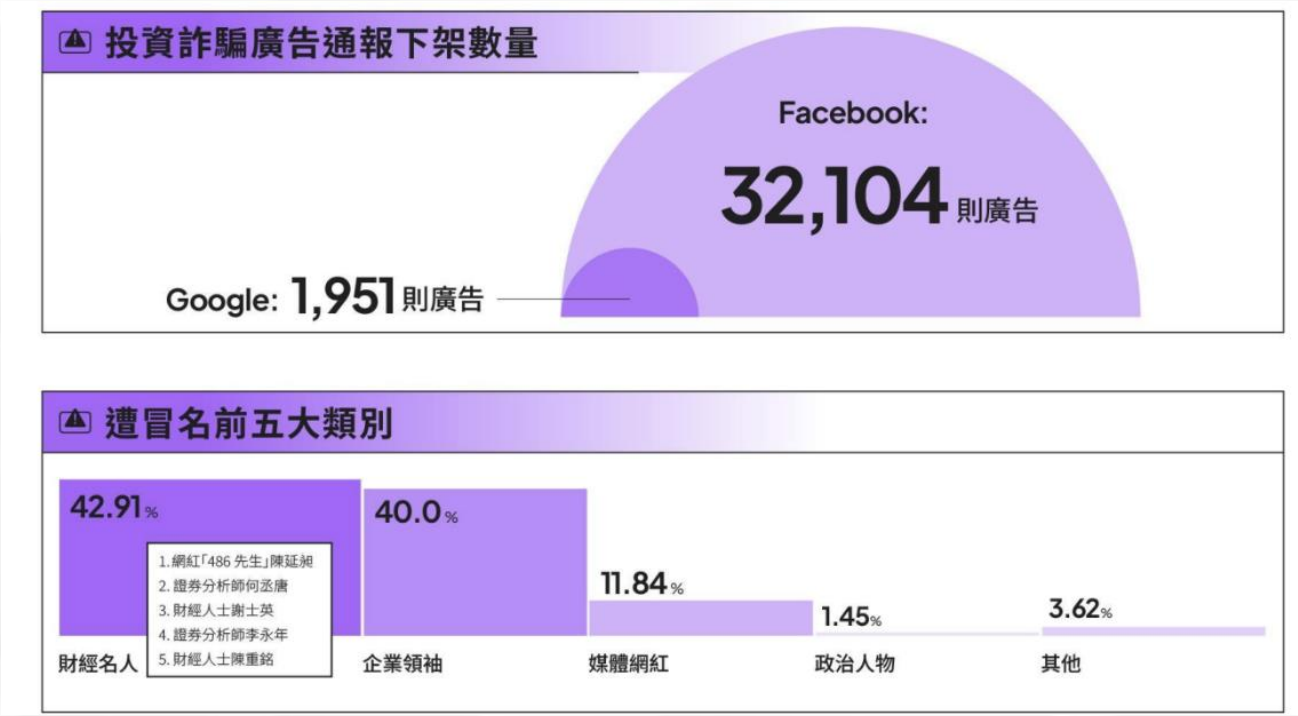
>

WEF 2025 全球風險報告

短期（2年）	長期（10年）
1. 錯誤訊息與假消息傳播	1. 極端氣候事件
2. 極端氣候事件	2. 生物多樣性喪失和生態系統崩潰
3. 以國家為基礎的武裝衝突	3. 地球系統的重大改變
4. 社會兩極化	4. 自然資源短缺
5. 網絡間諜活動與戰爭	5. 錯誤訊息與假消息傳播
6. 污染	6. 人工智慧技術的不利後果
7. 不平等	7. 不平等
8. 非自願移民或流離失所	8. 社會兩極化
9. 地緣經濟對抗	9. 網絡間諜活動與戰爭
10. 人權和/公民自由的侵蝕	10. 污染

來源：2025 台灣資安大會

錯誤訊息與假消息傳播



來源：2024 企業冒名事件報告書、刑事警察局

未來攻擊方向

AI驅動威脅	描述與機制	主要業務衝擊
超個人化釣魚/社交工程	GenAI利用抓取的資料創建極具說服力、針對性的電子郵件/簡訊/語音訊息	憑證竊取、金融詐騙、惡意軟體傳播
深度偽造	AI生成冒充高階主管或可信來源的虛假音訊/影片	金融詐騙（如電匯詐騙）、聲譽損害、繞過身份驗證
AI輔助惡意軟體/勒索軟體	AI協助創建惡意軟體變種、改進規避技術、增強勒索軟體誘餌	資料外洩、營運中斷、財務損失
自動化攻擊系統	AI工具自動化偵察、漏洞利用和橫向移動	更快的入侵速度、更廣泛的系統受損、攻擊量增加
敘事攻擊/假訊息	AI規模化創建/傳播針對品牌或信任的虛假資訊	聲譽損害、股價操縱、社會動盪關聯

來源：2025 台灣資安大會 中華資安

資安管理思維

- 要做甚麼措施

  (密碼長度、複雜度、定期變更、注意釣魚郵件、軟體更新...等)

資安管理思維

- 要做甚麼措施

  (密碼長度、複雜度、定期變更、注意釣魚郵件、軟體更新...等)

  - 可能有甚麼風險?
  - 防範風險要怎麼做?

資安概述

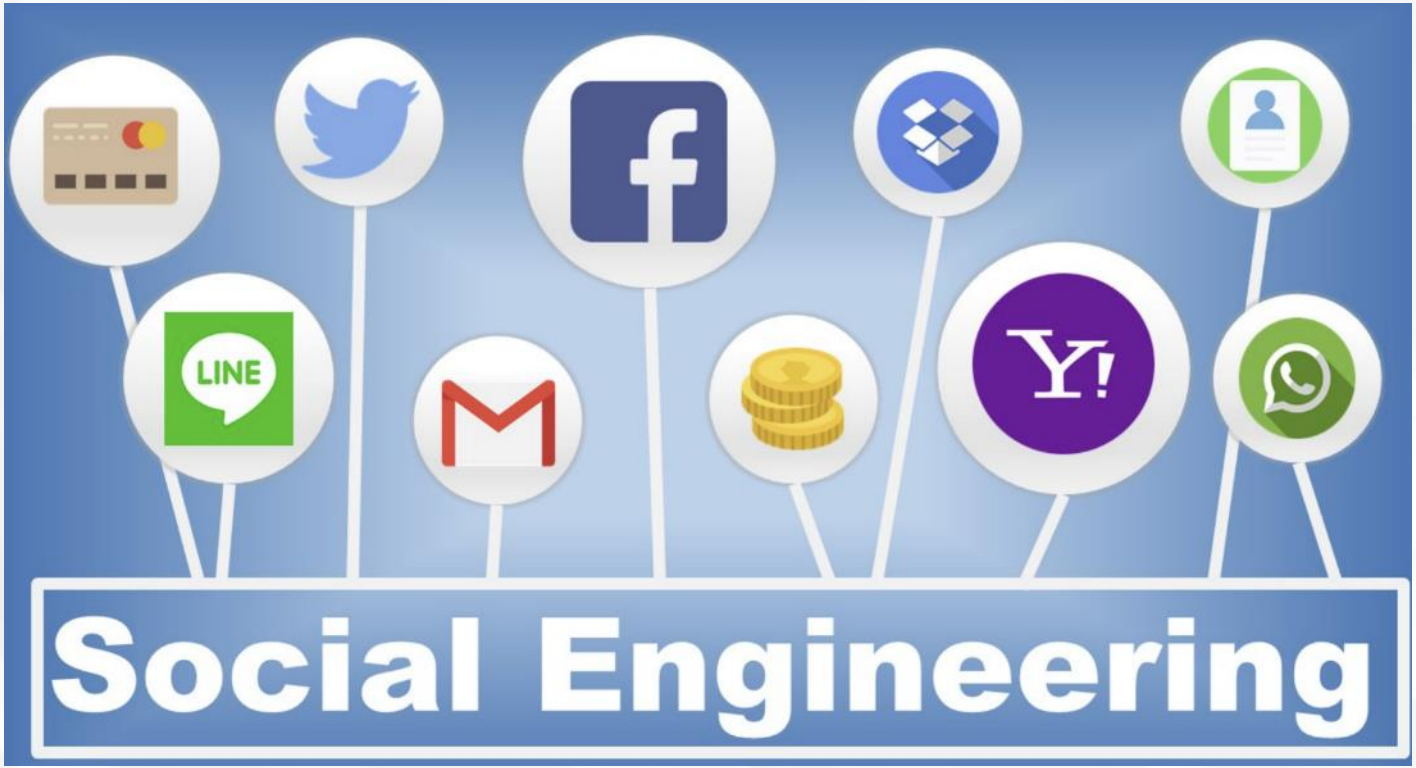
常見資安攻擊方式

近期案例

資安防護

WHITE HAT RHINO

社交工程



社交工程

WCERT/CC近期接獲外部情資，駭客社交工程手法更為精細，為取信於收件者，將依據收件者輸入公司域名，動態產生相應的登入頁面，進一步提高網站的可信度。建議企業與使用者加強社交工程防護措施。

情資顯示，攻擊者寄送包含釣魚連結於附檔之惡意電子郵件，當收件人開啟附件並點擊連結後，會被引導至釣魚網站。為了規避自動化沙箱檢測，攻擊者利用Captcha進行驗證，經人工確認後才會顯示頁面內容。此時，攻擊者採用將網頁背景模糊化的頁面，誘導收件人輸入個人資料，再根據收件人所輸入的公司域名，動態生成相應的登入頁面，包含公司商標和相關背景圖，以增加網頁真實性，欺騙收件人是合法的系統登入介面。

社交工程


①駭客發送釣魚信件
②收件人點擊附件連結
規避自動化檢測
③誘使收件人在模糊化的網頁輸入資料
④偽造公司的帳密登入頁面

社交工程

- 常見易混淆文字：「.g0v」「.gov.tw1」」「.corn」
- 確認信件來源
- 檢視來源信箱，非名稱

勒索病毒

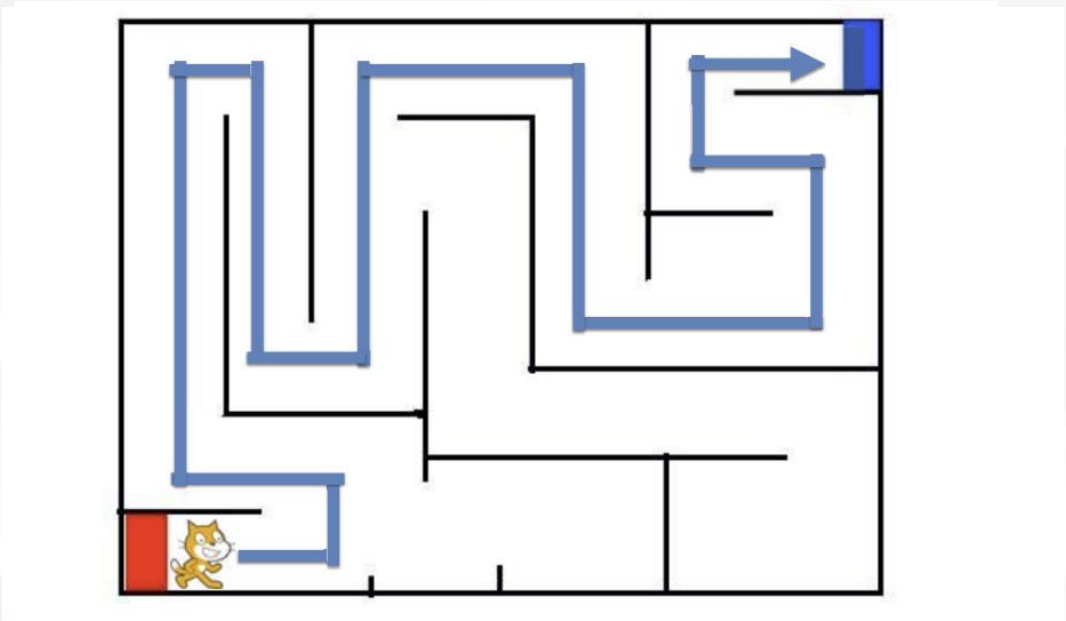

Ooops, your files have been encrypted!
xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx
xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx
xxxxxxxxxx?
xxxxxxxx xxxxx xxxxx xxxxxxxxx xx xxxxxxxxxxx
xxxx xxxxx xxxxxx xxxxxxxxxx xxxxxx xxxx xxxx
Payment will be raised on
xx/xx/xx xx:xx:xx
Time Left
XX:XX:XX:XX
Your files will be lost on
xx/xx/xx xx:xx:xx
Time Left
XX:XX:XX:XX
About Bitcoin
How to buy Bitcoin?
Contact Us
bitcoin
ACCEPT HERE
Copy
Check Payment
Decrypt

資安漏洞

(含軟、硬體)

資安漏洞

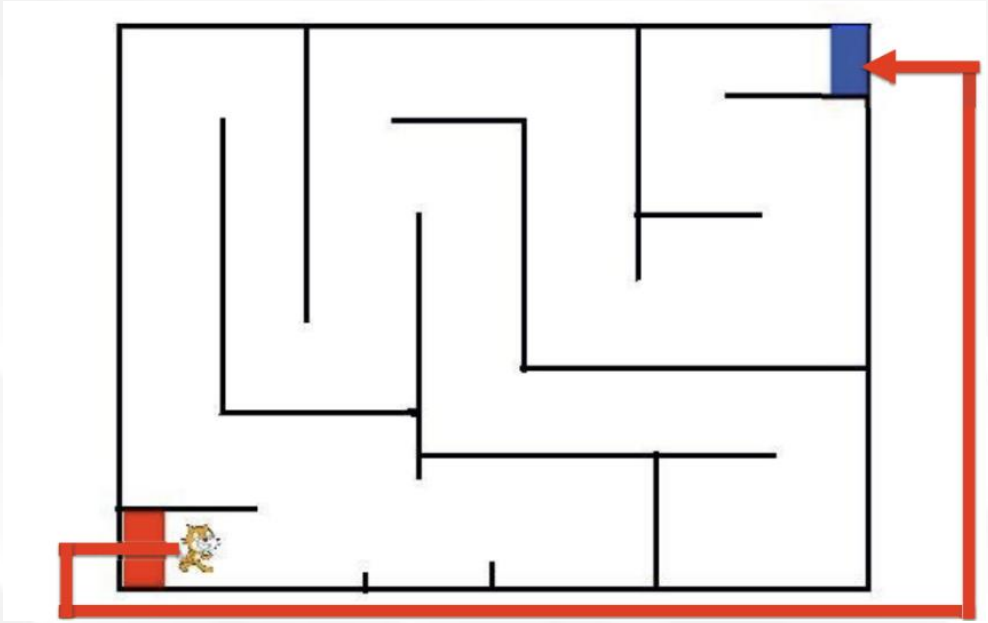
(含軟、硬體)



來源： SHIELDXTREME

資安漏洞

(含軟、硬體)

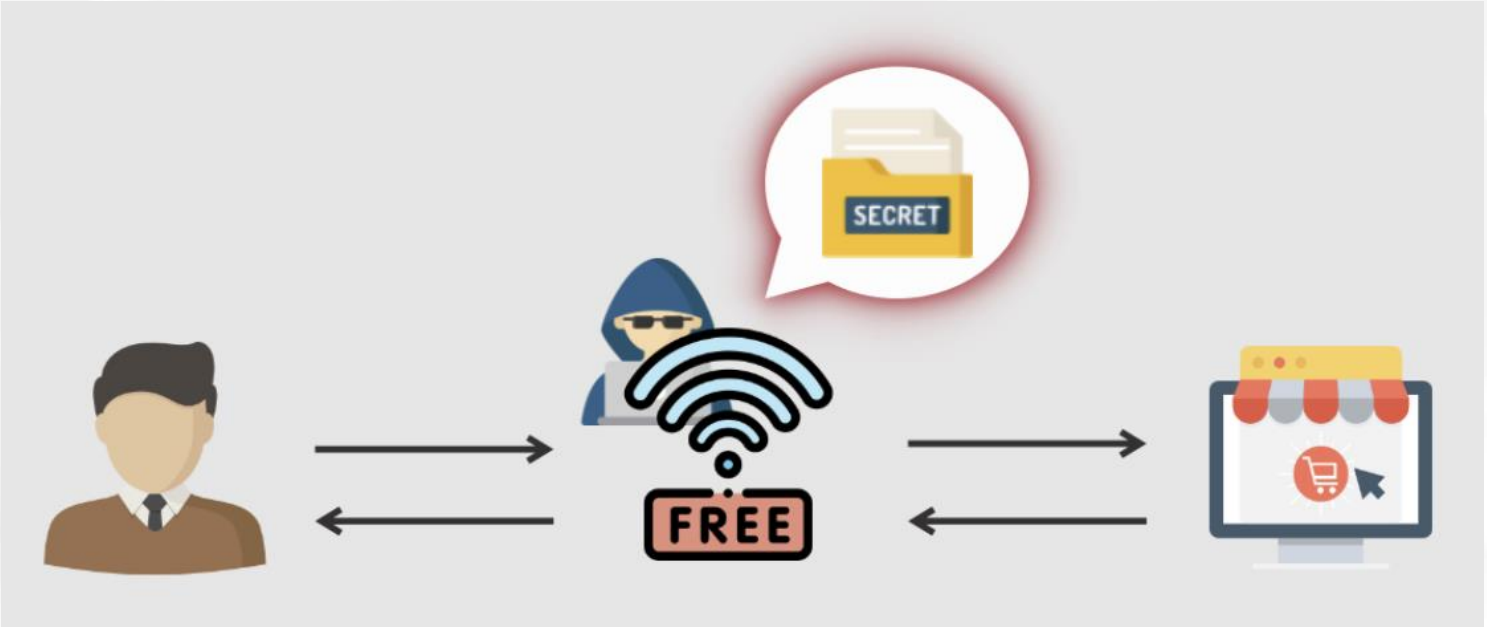


來源： SHIELDXTREME

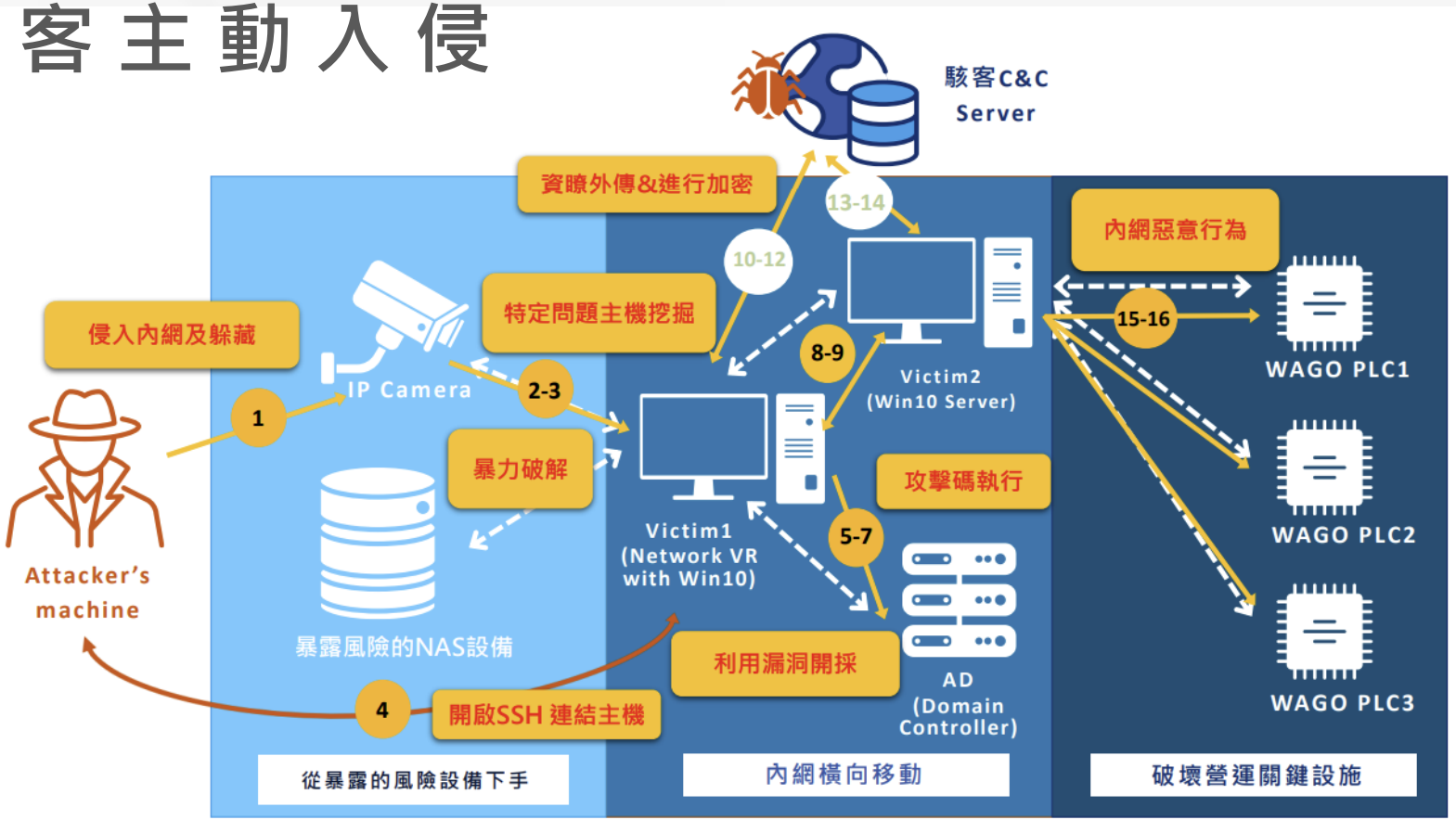
阻斷服務攻擊(DDoS)

供應鏈攻擊

中間人攻擊



駭客主動入侵



來源：2025 台灣資安大會 Forescout

遭受攻擊可能影響類型

- 服務中斷
- 資料加密
- 資料外洩
- 攻擊中繼站

資安概述

常見資安攻擊方式

近期案例

資安防護

WHITE HAT RHINO

現階段生成式AI最常被駭客用在：社交工程攻擊的強化

過去曾擔任美國國家情報總監辦公室資安事務情報長，現為Google Cloud國際資安合作負責人的Christopher B. Porter指出，這些發現並非理論推測，而是來自Google Cloud客戶與Mandiant全球事件應變團隊的實際觀察結果。

過去這些駭客雖然技術力強，但苦於語言障礙，難以理解或模仿目標組織內部的溝通語境，即使滲透後要找到關鍵敏感資料也很費工，如今這個障礙已不存在了。

駭客入侵公司組織電子郵件後的行動也更加容易，因為AI能幫助總結電子郵件的內容，因此可以更逼真地偽冒回應，並製作更容易引人誤信的郵件內容與對話。

WHITE HAT RHINO

假借Safari更新攻擊macOS用戶

FrigidStealer是在今年初首次現蹤，當時是由代號TA2727的駭客組織，使用代號TA2726的組織所運作的惡意流量散布系統（traffic distribution system，TDS）散布竊密程式。它們合作以JavaScript 注入程式注入網站中，冒充瀏覽器更新散布，而FrigidStealer則專門鎖定Mac用戶。

它冒充Safari瀏覽器更新程式，誘使用戶下載磁碟映像檔（disk image file, DMG）。下載該程式需要用戶手動在AppleScript程式中輸入密碼，這可繞過macOS內建防毒工具Gatekeeper。一旦安裝完成，FrigidStealer就會在Mac電腦上蒐尋敏感資料，並連向外部C2（command-and-controller）伺服器，經由DNS通道外洩資料。

惡意NPM套件濫用Google行事曆

該惡意套件起初在2025年3月19日上架，攻擊者利用Unicode字元來藏匿惡意程式碼，並且使用Google行事曆活動（event）邀請的短網址，來存取最終的有效酬載，使得這起多階段攻擊行動的蹤跡難以察覺。

首先，NPM套件安裝後，會取得Google Calendar短網址，此套件使用特定的功能函數追蹤，直到收到HTTP 200 OK的回應。接著此套件從Google Calendar活動標題取得經Base64演算法處理的網址並解碼，下載第二階段的惡意軟體有效酬載，此有效酬載同樣經過Base64處理。最終攻擊者解密有效酬載，並透過功能eval()執行。

台新爆重大疏失 個資外洩4年未覺察

台新銀在2020年5月1日及2024年5月9日調整信用卡系統地址欄位時，未同步調整催收系統；另外，2022年8月調整行動銀行地址變更功能時，寫入台幣核心系統的規則設計錯誤，導致催收系統產出之簽帳金融卡、信用卡及消金產品催收信函地址異常，可能誤寄而產生個資外洩，受影響客戶數共1089人。

金管會銀行局副局長王允中，台新銀對內是未確實執行測試及驗收的作業規範，針對委外也無有效督導受委託機構建立完善的內部控制制度。對此，金管會依銀行法第129條第7款規定對台新銀處600萬元罰鍰。

本次台新銀的缺失是有客戶收到錯誤的催收帳單，並向銀行反應，公司才去清查並發現錯誤。台新銀後續也回應客戶疑問或是主動透過簡訊、信函聯繫客戶。

首宗偽冒「111政府專屬簡訊」釣魚簡訊詐欺

有民眾在PTT分享收到偽冒「111」及高雄區監理所之釣魚詐騙簡訊，經研判為不法分子以偽造2G基地臺方式，發送竄改發送人門號之釣魚簡訊，案經刑事局電信偵查大隊、國家通訊傳播委員會與各電信事業組成非法訊號偵測小組，今年9月至11月初在新竹、高雄兩地區測得不明干擾訊號，在專案小組跟監埋伏，日前在高雄鼓山和雙北、新竹地區逮捕兩個不法集團共4名犯嫌，這也是警方首度查獲集團利用「111」簡訊行騙手法。

警方掌握，高雄中國籍林男（32歲、依親來台）後與郭男（69歲），自2024年10月31日至11月13日間在大高雄地區偽冒「111」簡訊，假冒「高雄市監理站」、「台灣自來水公司」等公部門，誘使民眾點擊釣魚連結後，續騙個資及盜刷信用卡，案經與電信業者合作定位下，順利將林郭兩人逮捕。

馬偕醫院遭勒索軟體Crazy Hunter攻擊

2025年2月上旬馬偕醫院遭到勒索軟體Crazy Hunter攻擊，當時他們表示只有臺北及淡水院區的急診室受到影響，如今傳出駭客已在駭客論壇兜售竊得資料。對於駭客聲稱握有馬偕醫院資料的情況，最早可追溯到3日衛生福利部資訊處長李建璋透露，馬偕事故發生之後，新竹馬偕兒童醫院也遭受攻擊，駭客宣稱掌握部分個資。

自稱是Crazy Hunter的人士於駭客論壇BreachForums聲稱，他們握有馬偕醫院所有病人的資料，這批資料包含1,660萬筆病人資訊，檔案大小為32.5 GB，涵蓋臺北、淡水、新竹、臺東院區，以及臺北與新竹的兒童醫院。呼籲曾經在馬偕看醫生的民眾要提高警覺，慎防外流的資料被用於詐騙。駭客表示這批資料包含姓名、身分證字號、手機號碼、Line ID、住家地址、生日，以及醫療記錄。

彰基醫院遭勒索軟體CrazyHunter攻擊

彰化基督教醫院在二二八連假遭勒索軟體攻擊的事件，受到最多的矚目，因為這次與上個月馬偕紀念醫院面臨的威脅相同，都遭遇CrazyHunter這支勒索軟體，也傳出AD伺服器都受影響，未來不排除還有其他醫院成為攻擊目標。在後續應變上，衛生福利部也舉行緊急資安會議，請遭遇攻擊事故的醫院分享其清除與防禦經驗，並發布醫院面對勒索軟體攻擊的應變指南。

- 彰化基督教醫院自3月1日遭受勒索軟體攻擊，衛福部資訊處指出此事件也是CrazyHunter這支勒索軟體的攻擊，因此定調為「系統性攻擊」事件。
- 攻擊者在入侵過程中會從AD管道下手，透過弱密碼嘗試取得帳號權限再透過內網發送至其他裝置。

WHITE HAT RHINO

美25歲駭客用AI繪圖外掛入侵迪士尼

駭客代號為「NullBulge」的25歲男子克雷默（Ryan Mitchell Kramer）目前，已同意就入侵迪士尼公司電腦系統的行為認罪，這起案件牽涉AI生成藝術工具的惡意操作與數據竊取。

這起案件的核心在於一款廣泛使用的AI圖像生成介面工具ComfyUI，該工具為開源平台Stable Diffusion的擴充套件，主要透過Github發布。克雷默在ComfyUI中植入一個特洛伊木馬，進而入侵安裝該工具的使用者電腦。透過這個後門，克雷默得以未經授權地存取多位使用者的系統，其中一人正是迪士尼公司的員工。他藉由該員工的電腦登錄迪士尼的Slack系統，並下載多達1.1TB的公司內部資料。

根據資安公司vpnMentor指出，克雷默所修改的ComfyUI版本不僅植入惡意代碼，還能入侵用戶的加密貨幣錢包、注入木馬程式並大量竊取個人資料。

勒索軟體駭客Akira轉向網路攝影機下手

資安業者S-RM指出是透過遠端存取系統得逞，這次駭客使用的是AnyDesk，以便在外傳竊得資料之前能夠持續存取受害組織的網路環境。

遭到利用的網路攝影機存在以下特點，使得駭客有機可乘。首先，就是該攝影機存在多項重大漏洞，攻擊者能在未經授權的情況下存取鏡頭、部署Shell工具。再者，該設備執行精簡版的Linux作業系統，而能執行多種Linux命令。此外，因為儲存空間極為有限，該設備完全無法部署EDR系統而不受保護。在確認網路攝影機是符合條件的利用對象後，駭客隨後就對其部署Linux版勒索軟體，並藉由網路攝影機存取SMB共享資料夾，而能對受害網路加密檔案。

全錄（Xerox）印表機漏洞

2025年1月底全錄（Xerox）宣布修補Versalink系列多功能印表機（MFP）的資安漏洞。攻擊者能竄改LDAP服務的IP位址，並觸發LDAP使用者與系統帳號對應（LDAP User Mapping）的搜尋，接著可監聽特定連接埠而得知印表機使用的LDAP身分帳密。

攻擊者可經由這該弱點進行回傳攻擊（Pass-Back Attack），從而取得印表機的LDAP、SMB、FTP組態，隨後就能在受害組織的內部網路環境進行橫向移動，並且破壞其他Windows伺服器或是檔案系統。

WHITE HAT RHINO

D-Link部分NAS設備存在重大漏洞

2024年10月底遭接露，這個編號為CVE-2024-10914的弱點屬於命令注入漏洞，此事也得到D-Link證實，但由於設備的生命週期已經結束，他們不會進行修補。

此為重大層級的CVE-2024-10914漏洞，屬於命令注入漏洞，存在於NAS設備名為account_mgr.cgi的URI，發生在CGI指令碼cgi_user_add處理name參數的過程，未經身分驗證的攻擊者有機會利用偽造的HTTP GET請求，藉由漏洞注入任意的Shell命令，估計至少約有6.1萬臺設備曝險。根據漏洞資料庫VulDB的評估，此漏洞的4.0版CVSS風險評分為9.2（滿分10分）。

事隔不到一週威脅情報業者GreyNoise、Shadowserver基金會證實，已有攻擊嘗試利用此漏洞的跡象。

惡意廣告透過臉書轉傳

駭客挾持臉書企業帳號濫用Meta廣告平臺散布竊資軟體的情況，不時有事故傳出，最近有研究人員提出警告，他們發現有人冒用使用者相當信賴的品牌，佯稱提供遊戲、破解軟體等內容，意圖散布惡意程式的新一波攻擊行動。

資安業者Bitdefender指出，他們看到駭客透過Meta的廣告平臺散布惡意廣告，自9月開始為期超過1個月，而且，每天都會上架新的廣告，這些廣告的最終目的，就是散布名為SYS01stealer的竊資軟體。

在這波攻擊行動當中，對方運用Electron應用程式來散布惡意程式。研究人員指出，攻擊者的廣告內容，通常帶有指向雲端檔案共享服務（如MediaFire）的連結，一旦使用者點選，就會下載內含Electron應用程式的ZIP壓縮檔。

臺灣企業臉書粉專管理員遭鎖定

思科旗下的威脅情報團隊Talos指出，他們發現自今年7月開始，有人針對臺灣的臉書企業用戶及廣告帳號，發動相關攻擊，攻擊者以侵犯版權為由，假冒企業的法律部門，寄送帶有偽裝成PDF檔案附件的釣魚信，意圖引誘使用者下載及執行惡意程式。

在這波攻擊行動裡，對方濫用Google的Appspot[.]com網域名稱，以及短網址服務、雲端檔案共享服務Dropbox，藉此迴避網路資安系統的偵測，而能成功將竊資軟體LummaC2（Lumma Stealer）、Rhadamanthys，傳送到受害電腦。

針對這起攻擊行動發生的過程，研究人員提及，這些釣魚郵件夾帶惡意軟體下載連結，而郵件內容及偽裝成PDF檔案的誘餌，都使用了正體中文，顯然是針對這種語言的使用者而來。

Hitcon Zeroday公開資安院系統漏洞

該攻擊嘗試於2024年10月10日公開，對象為資安院電子郵件社交工程演練系統。

在這波測試攻擊行動裡，查看網頁根頁面發現是資安院電子郵件社交工程演練系統。發現可透過錯誤訊息取得伺服器版本 Apache Tomcat/9.0.80，其中存在CVE-2023-45648 HTTP請求走私漏洞。

由於Tomcat未能正確解析HTTP Trailer標頭，超出標頭大小限制的特製Trailer標頭可能會導致Tomcat將單個請求視為多個請求，從而可能導致在反向代理之後出現請求走私。成功利用漏洞可能導致繞過安全控制，未經授權存取敏感資料等。

WHITE HAT RHINO

美國醫療服務供應商遭到勒索軟體攻擊

今年2月美國醫療服務供應商Change Healthcare遭到勒索軟體攻擊，母公司UnitedHealth Group因為這起資安事故，在Q3財報中已認列超過20億美元的網路攻擊損失，如今美國衛生及公共服務部（HHS）的公開資料顯示，Change Healthcare所外洩的用戶資料高達1億筆，成為美國醫療領域最嚴重的資料外洩事件。

該公司在今年2月遭到勒索軟體BlackCat的攻擊，駭客利用竊來的憑證入侵了Change Healthcare的Citrix遠端存取服務，盜走了6TB的資料，也加密了Change Healthcare系統。隨後Change Healthcare並未說明外洩的筆數，僅說使用者的健康資訊、健保資訊、支付資訊，或是社會安全碼與駕照號碼等資訊外洩了。

UnitedHealth Group在今年5月坦承支付贖金予駭客，惟並未證實金額是否為外傳的2,200萬美元。

資安概述

常見資安攻擊方式

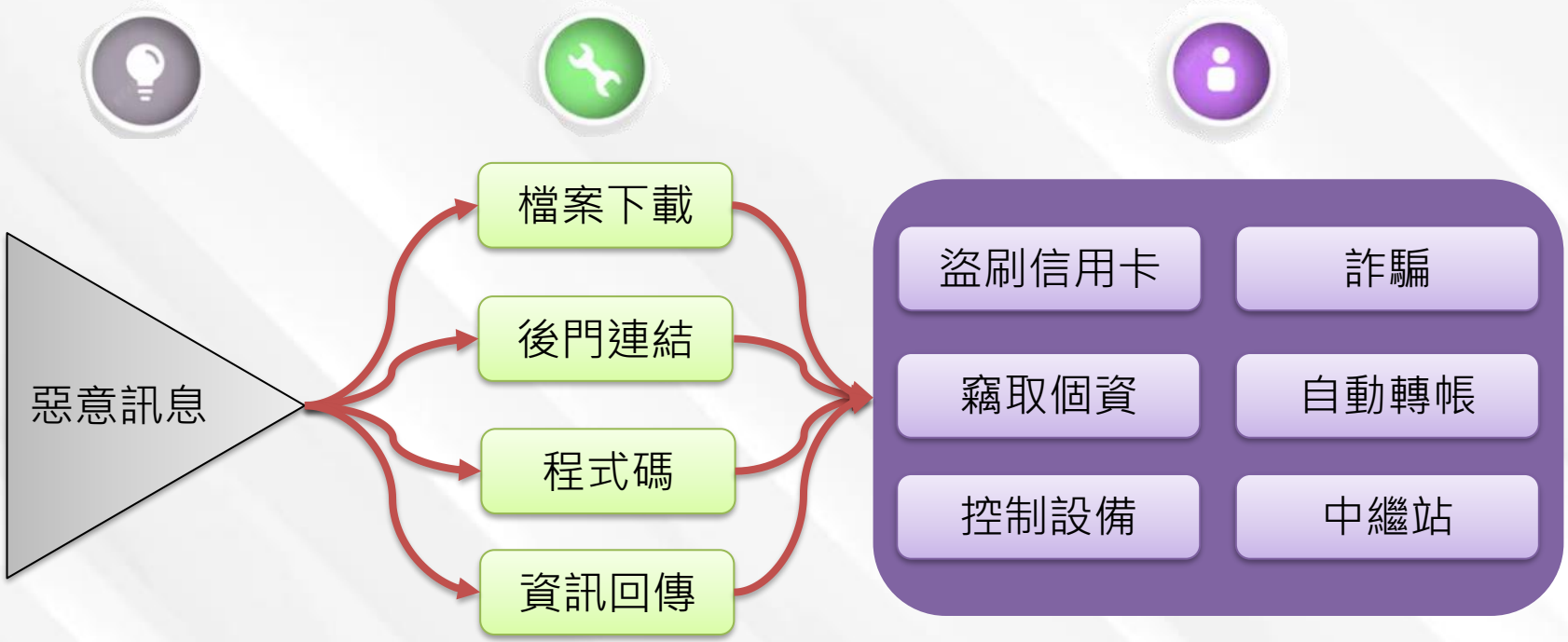
近期案例

資安防護

惡意訊息來源

- 電子郵件
- 簡訊
- 社群軟體
- 網頁廣告、連結
- 電話

影響流程



電子郵件

- 確認來源 勿直接開啟
- 可先與對方聯繫
- 關閉預覽功能
- 不任意開啟連結
- 下載檔案須注意

電子郵件

- 高雄市政府標準
- 開啟率 5%
- 連結、附件點擊率 2%

資料洩漏預防

資料分類

檢視業務流程

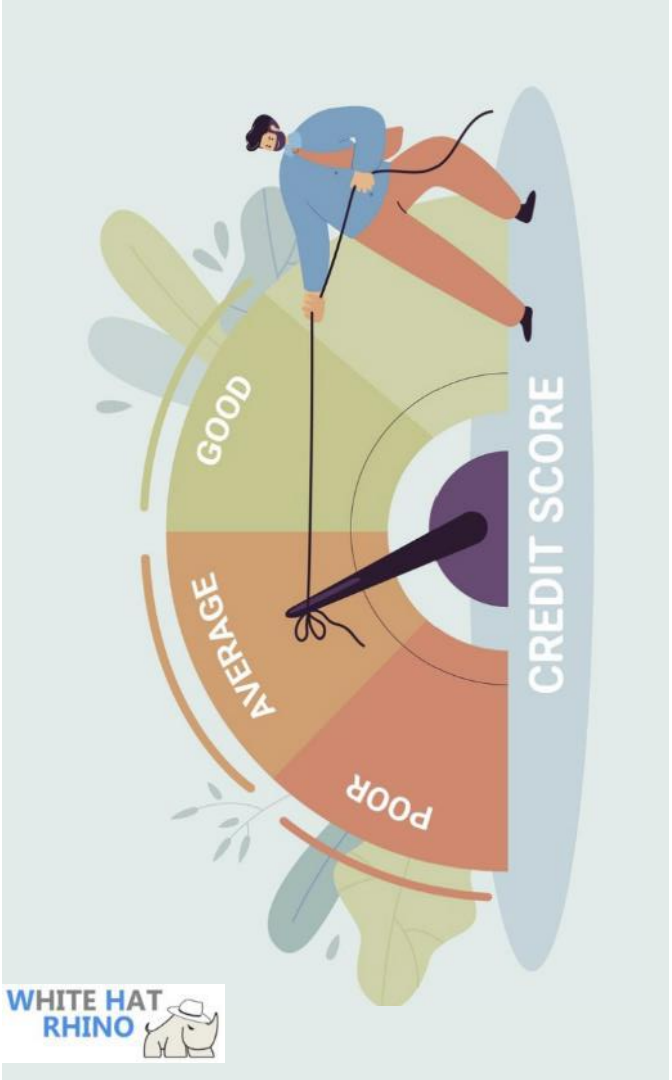
確認流程風險

資訊分類

- 是否為機敏性資料
- 有無包含個資
- 內部限定閱覽
- 開放資料

檢視業務流程

- 資料傳遞流程
- 過程經手人員
- 傳遞方式
- 資訊類型



確認流程風險

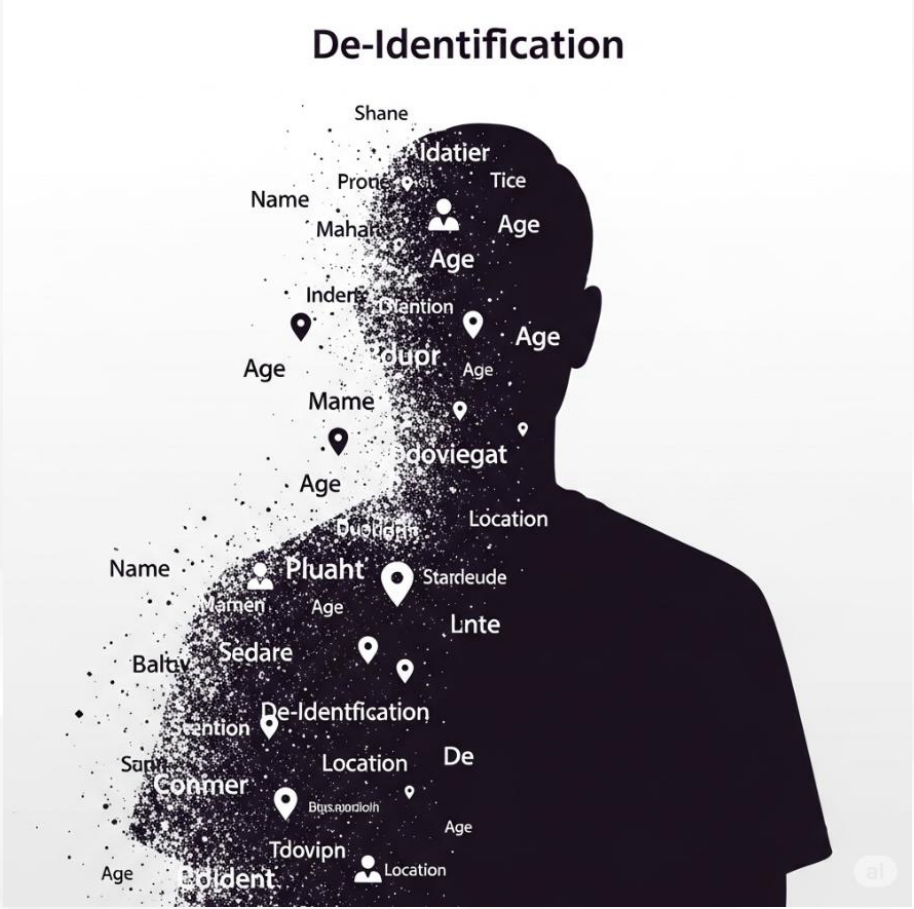
- 內、外部人員作業不熟悉
  - 教育訓練、檔案閱覽權限
- E-mail遭入侵或釣魚郵件
  - 社交工程演練、取消帳密記憶、檔案加密
- USB中毒或有後門程式
  - 防毒軟體、定期更新
- 雲端資料外洩
  - 檔案加密、資料分類、存取權限
- 系統遭入侵
  - 系統技術檢測、防火牆、帳密要求、權限設定

防 範 措 施

- 更新、漏洞修補
- 定期變更密碼
- 重要資料加密保存
- 判斷來源、不隨手開啟資訊

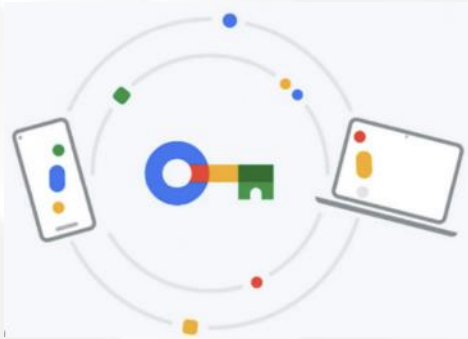
個資保護

- 去識別化可以怎麼做？
- PII極小化目標
- 暫存檔



密碼自動記憶功能

- 建議取消
- 盡可能避免紀錄重要系統密碼
- 避免紀錄信用卡資訊



密碼長度與複雜度

- 8碼已有風險
- 錯誤鎖定
- 多因子驗證

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	17 mins
7	Instantly	Instantly	2 hours	9 hours	20 hours
8	Instantly	30 mins	5 days	3 weeks	2 months
9	Instantly	13 hours	9 months	4 years	11 years
10	Instantly	2 weeks	40 years	232 years	779 years
11	Instantly	1 year	2k years	14k years	54k years
12	2 hours	26 years	107k years	889k years	3m years
13	1 day	684 years	5m years	55m years	267m years
14	1 weeks	17k years	291m years	3bn years	18bn years
15	3 months	462k years	15bn years	212bn years	1tn years
16	3 years	12m years	788bn years	13tn years	91tn years
17	28 years	312m years	40tn years	815tn years	6qd years
18	276 years	8bn years	2qd years	50qd years	449qd years

來源：Hive Systems

日 常 備 份

- 每日下班前
- 備份至不同硬碟
- 如使用隨身碟須注意
- 檔案放置於雲端空間須加密
- 機敏性資料本機加密保存

終端安全


雲端
FTP /IM
檔案傳輸
網站存取
Webmail
共用資料夾分享
應用程式連線
私人電腦
Peer 2 Peer
4G網路
手機熱點
WiFi AP
私接SIM卡

法規要求與修法

- 資安法
- 個資法

資安法草案修正重點鳥瞰圖

修法目標

修法重點

明確機關權責
強化合作協力

- 明定各機關權責事項
- 強化國家資通安全會報功能(§5)
- 委託權限移轉之法規依據(§32)

提升資安人力

- 公務機關：職能訓練、調度支援、適任性查核(§18、19)
- 特定非公務機關：
  1.設置專職人員及資安長(§20、21、23)
  2.對所屬人員獎懲(§26、28)

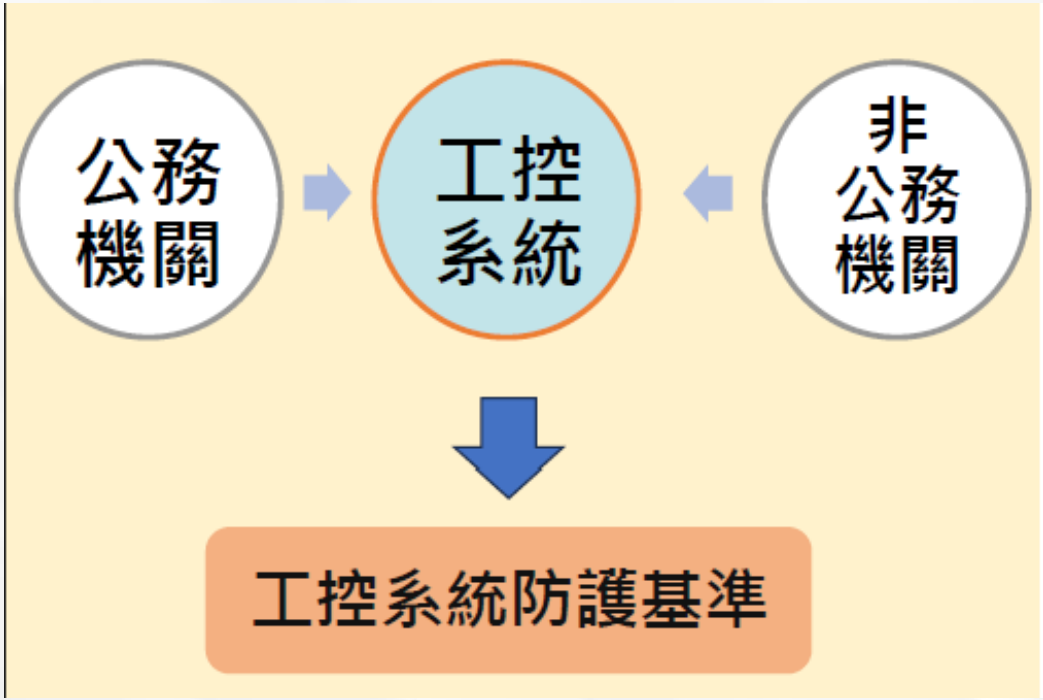
強化納管機關
資安管理

- 危害國家資安產品管制(§11、27)
- 公務機關：強化聯防體系，分層監督管理模式調適 (§8、14~17)
- 特定非公務機關：重大資安事件調查權限(§25、31)

明確法源

- 修正關鍵基礎設施提供者定義(§3⑧)
- 配合財團法人法施行，修正特非機關定義(§3⑨)
- 資安事件涉個資外洩時另依個資法辦理(§33)

工控系統須納入管控



附表10資通系統防護基準修正

構面	控制措施	修正/新增條文	備註
存取控制	帳號管理	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除	由「中級」修正為「普級」
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取	由「中級」修正為「普級」
	遠端存取	遠端存取之來源應為機關已預先定義及管理之存取控制點	由「中級」修正為「普級」
事件日誌與可歸責性	時戳及校時	系統內部時鐘應定期與基準時間源進行同步	由「中級」修正為「普級」
營運持續計畫	系統備援	應在與運作系統不同地點，由備援設備或其他方式取代並提供服務	高級 **增加異地備援**
識別與鑑別	內部使用者之識別與鑑別	對資通系統之存取採取多重認證技術	由「高級」修正為「中級」

附表10資通系統防護基準修正

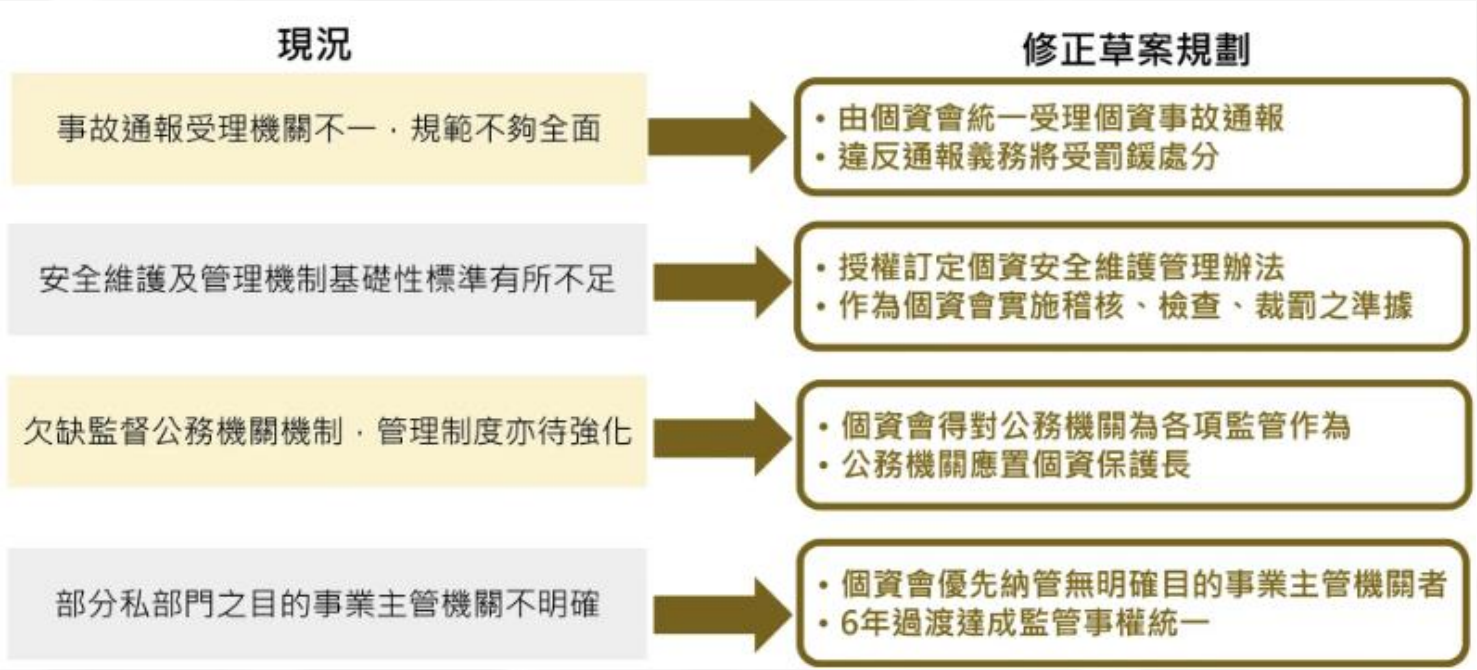
新增

構面	控制措施	修正/新增條文	備註
系統與服務獲得	獲得程序	資通系統使用第三方軟體、服務、函式庫或其他元件時，應識別其組件之來源	普級
系統與通訊保護	傳輸之機密性與完整性	一. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限 二. 使用公開、國際機構驗證且未遭破解之演算法 三. 加密金鑰或憑證週期性更換 四. 伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施	由「高級」修正為「普級」
系統與資訊完整性	軟體及資訊完整性	使用者輸入資料合法性檢查應置放於應用系統伺服器端	由「中級」修正為「普級」

資通安全管理法施行細則

第4條：
涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明

個資法修正草案

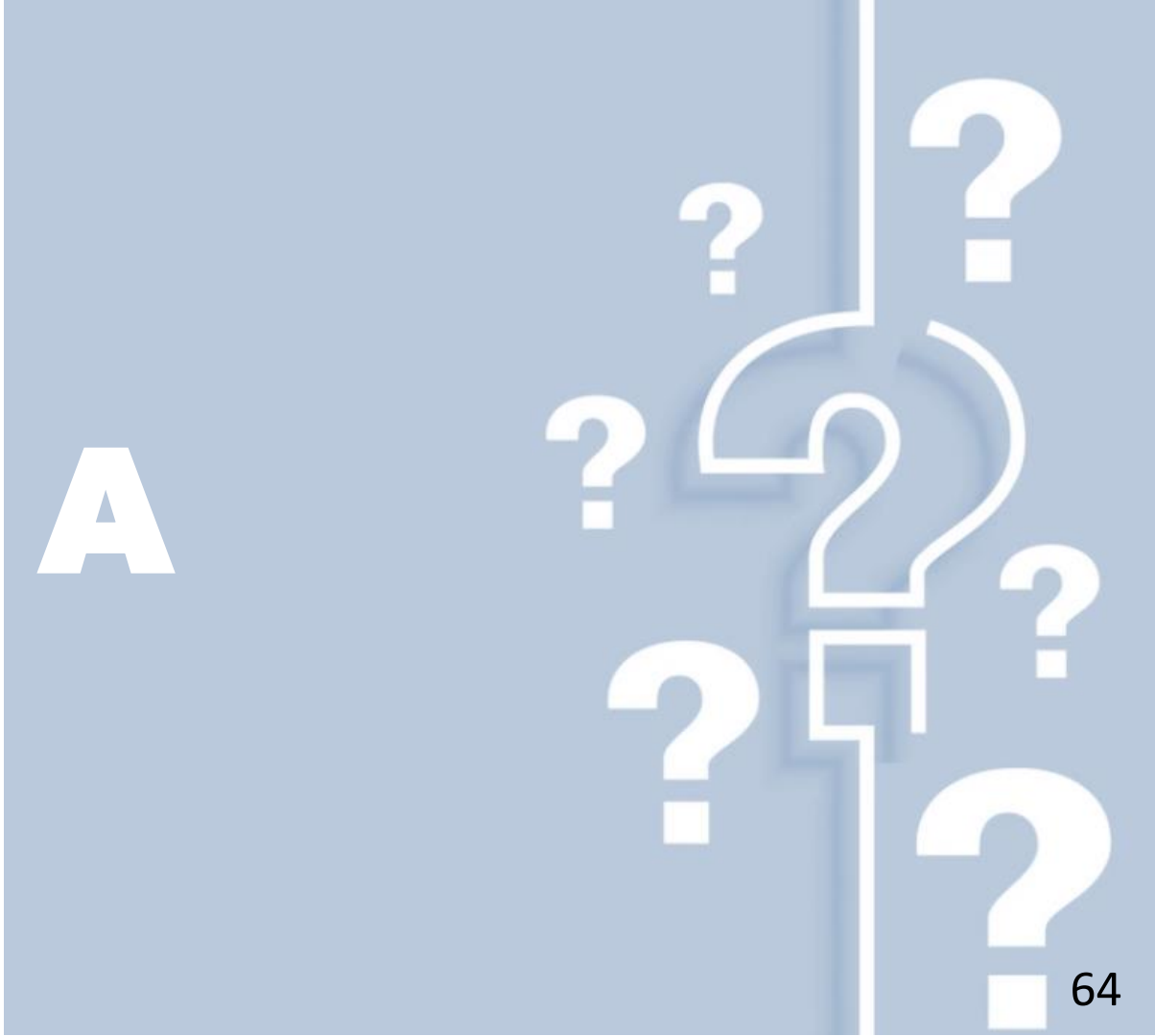

現況
修正草案規劃
事故通報受理機關不一，規範不夠全面
• 由個資會統一受理個資事故通報
• 違反通報義務將受罰鍰處分
安全維護及管理機制基礎性標準有所不足
• 授權訂定個資安全維護管理辦法
• 作為個資會實施稽核、檢查、裁罰之準據
欠缺監督公務機關機制，管理制度亦待強化
• 個資會得對公務機關為各項監管作為
• 公務機關應置個資保護長
部分私部門之目的事業主管機關不明確
• 個資會優先納管無明確目的事業主管機關者
• 6年過渡達成監管事權統一

結論

攻擊與資安防護

WHITE HAT RHINO

Q & A



WHITE HAT RHINO