資通安全查核重點及缺失案例分享

金融監督管理委員會
證券期貨局 黃仲豪組長
2025.2.21

簡報大綱

01 近期重要資安政策

02 資安缺失態樣

03 案例分享

04 近期宣導事項

1 近期資安政策

強化資訊安全管理

設置資安長

- 背景：進一步推動本會「金融資安行動方案」所定「型塑金融機構重視資安的組織文化」措施，提升證券期貨市場各服務事業對資安議題之決策能量，要求各服務事業符合一定條件者，應指派**副總經理以上或職責相當之人兼任資訊安全長**，綜理資訊安全政策推動及資源調度事務。
- 各服務事業若已指派專任資訊安全長有益於所任職務之有效執行，亦未違本項之立法目的。
- 各服務事業之一定條件授權由主管機關另定之。

強化資訊安全管理

設置資安專責單位

- 背景:提升證券期貨各服務事業對資安之重視，明定業者應設置資訊安全專責單位及主管，負責資安相關工作，並針對不同規模、業務及組織特性事業，命令設置資訊安全專責單位及主管，以利進行差異化管理。
- 證券商應依下列分級標準設置

分級標準	資安單位暨人力編制
資本額200億以上	應設資安專責單位，資安主管及至少3名資安人員不得兼辦資訊或其他與職務有利益衝突之業務。
資本額100億以上，未達200億	資訊安全主管及至少3名資訊安全人員。但已設置資訊安全專責單位者，得配置專責主管及2名專責人員。
資本額40億以上，未達100億	資安主管及至少2名資安人員。
資本額未達40億	至少1名資安人員。

強化資訊安全管理

整併資安聲明書納入內控聲明書

各服務事業每年應將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過。

資安主管及人員應持續接受課程訓練

各服務事業負責資訊安全之主管及人員，每年應至少接受十五小時以上資訊安全專業課程訓練或職能訓練。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程（證券暨期貨市場各服務事業內控處理準則§ 36-2）。

強化資訊安全管理

資安通報機制

證券商發生影響客戶權益或正常營運之資訊服務異常事件或資安事件，應依本會「證券期貨市場資通安全事件通報應變作業注意事項」規定於知悉事件 30 分鐘內至「證券期貨市場資通安全通報系統」辦理事件通報，以利主管機關及相關單位有效掌握事件資訊。

資安執行情形納入業務准駁之考量

證券商申請增加業務種類、增加營業項目、設置分支機構及轉投資國內外事業等事項，申請書件應包括資安自評表。

強化資訊安全管理

- 為強化證券商持續營運不中斷，證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。(證交所113.02.25修正)

等級	第一級(A級)證券商(註) (市占率1%以上且自然人客戶數達公司客戶數50%以上)	第二級(B級)證券商 (市占率未達1%或自然人客戶數未達公司客戶數50%以上)	應辦事項完成日
應辦事項	核心系統可容忍中斷時間為1小時	核心系統可容忍中斷時間為2小時	113年7月底

證券商作業委外應注意事項重點

委外內部作業規範應載明事項(董事會核定)

1.作業委外之政策及原則

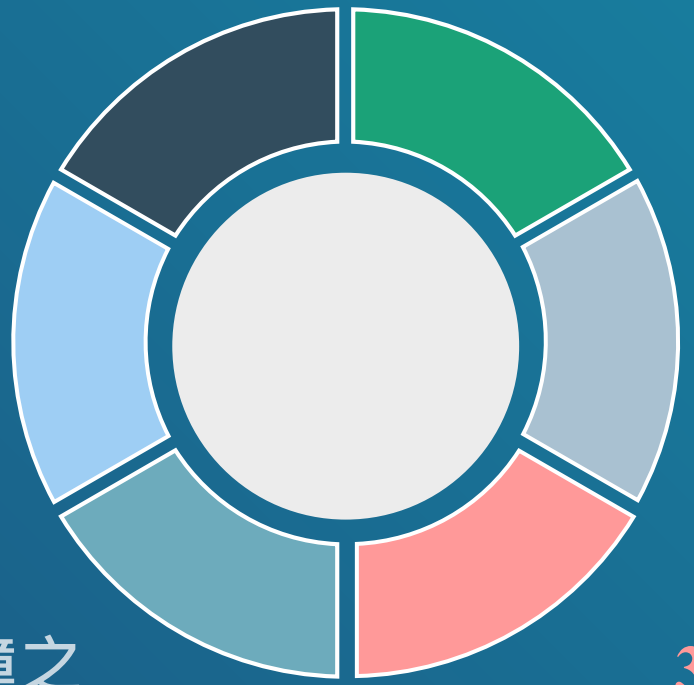
2.專責單位及相關單位對委外事項之權責分工

3.委外事項範圍及委外程序

4.客戶權益保障之作業及程序

5.風險管理原則及程序

6.內部控制原則及程序



資安查核簡介

年度資安例查

- 檢視證券商資安防護辦理情形

選案查核

- 投資人檢舉、資通安全事件、主機共置服務

專案查核

- 特定議題對 證券市場之影響 或 檢視 整體辦理情形

資安查核簡介

資通安全檢查機制

- 辨識資安風險
- 訂定資安政策
- 配置組織資源
- 清查資訊資產
- 強化人員管理
- 監控環境設備
- 管理通訊作業
- 落實存取控制
- 控管開發維運
- 提升營運韌性
- 實作規範相符
- 納管新興科技

資安查核作業

14個 資安 控制領域

依嚴重程度扣分

(每年查核約50間)

☑未制定 規範
嚴 重 缺 失（扣 10 分）

☑未依規定 執行
中 等 缺 失（扣 5 分）

☑未留下 操作記錄
輕 微 缺 失（扣 2 分）

追蹤改善

最近3年
150份查核報告
(736項缺失)

資料治理
合併成(65種 缺失態樣)

2 欠失態様分析

3 案例分享

資安事件因應作為-證券商遭駭客撞庫攻擊事件

◆110年11月下旬，3家證券商通報其複委託下單系統遭駭客撞庫攻擊，且有客戶帳戶遭偽冒下單港股(深藍科技)情事。證券商以錯帳處理，投資人權益不受影響。

遭駭券商緊急應變	全面清查	加強客戶APP登入及取得憑證之安控措施	宣導措施	完備資安規範
• 關閉港股電子交易改採人工接單 • 提醒客戶立即變更密碼，封鎖可疑來源IP • 向刑事警察局及法務部調查局報案 • 強化憑證申請機制 • 於公開資訊觀測站及公司官網公告提醒投資人提高警覺	• 函請證券商清查使用下單系統之安全性	• 證券商下單APP登入落實**採多因子認證** • 客戶申請或更新憑證，應增加與登入雙因子之**不同因子驗證機制** • 未落實者，督導證交所要求業者應即修改系統或暫停服務	• 向業者宣導強化資安措施，落實資安內控規範 • 提醒投資人妥善保管投資帳號及密碼	• 督導證交所研修「建立證券商資通安全檢查機制」及「證券商、期貨商電子憑證交付作業要點」有關密碼管理及憑證交付等規定

近期資安重大事件案例

基礎設施服務商異常

事件原因：複委託之上手證券商網路異常，致無法進行交易

影響範圍：造成相關證券商投資人之複委託無法正常下單

處理措施：要求上手證券商強化持續營運作業

近期資安裁罰事件案例

電子下單平台無法登入

事件原因：期貨行情劇烈震盪，大量投資人登入下單平台，
欲確認持有部位，並進行委託，人數達平日之２倍，
造成系統服務異常

影響範圍：查詢帳務資料回應緩慢、投資人登入異常

強化措施：評估整體資源配置（前、中、後台、憑證系統、資料庫）
優化程式效能（放寬可允許連線數、調整資料庫連線機制）
加強故障復原程序 與 壓力測試
提高警戒標準

近期資安裁罰事件案例

委外廠商管理不當

事件原因：證券商對測試系統與正式系統未隔離，並提供廠商高權限帳號及遠端登入功能，廠商於盤中進行系統下單測試。

影響範圍：造成1.4億元鉅額錯帳，回補後虧損113萬

處理措施：落實網段區隔
加強上線管控作業

近期資安裁罰事件案例

未落實資安防護致惡意程式攻擊

事件原因：證券商對外系統遭受攻擊。

影響範圍：部分內網主機遭植入惡意程式。

處理措施：停用多部內部主機上特定高權限帳號
落實網段區隔
加強異常連線監控
弱點程式修補

US financial regulation + Add to myFT

Robinhood to pay biggest fine among more than $100mn imposed by SEC

Broker agrees $45mn settlement as part of data breach while Blackstone and KKR among those penalised by US regulator

The penalties imposed by the SEC stem from a crackdown on Wall Street over use of 'off-channel' messaging systems © Kent Nishimura/Bloomberg

4 近期宣導事項

推動證券商導入零信任架構相關規劃

先行機構導入分享研討會	挑選之導入零信任先行示範單位，將零信任架構導入經驗與其他證券商分享。
參考指引解析說明會	依金管會發布「金融業導入零信任架構參考指引」，對框架概念、導入策略、建議實作參考原則分級進行說明。
零信任系列說明會	根據五大支柱共36個參考原則，分享導入實務及案例，並提供導入零信任架構相關諮詢常見問題及解決方向。

證券期貨市場資通安全事件通報應變作業注意事項

初步通報	應於知悉事件 30 分鐘內進行初步通報。
正式通報	查明事實後，應於24小時內轉為正式通報。
解除通報	事件處理完成後，應於3日內解除通報。

謝謝聆聽

生成式AI對於資安的挑戰

Presenter 吳乙南

Feb 21th , 2025

安碁資訊(股票代號: 6690)
Acer Cyber Security Inc.

講師簡介

吳乙南

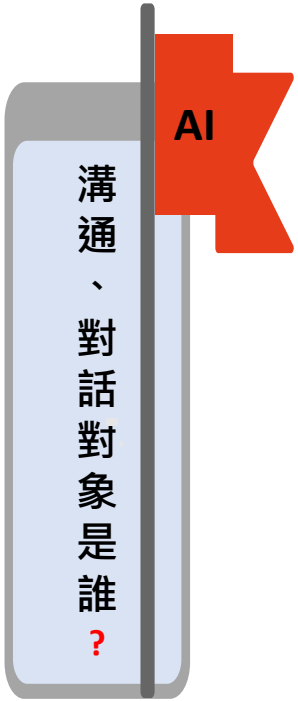
職務	安碁資訊股份有限公司 總經理 宏碁雲架構股份有限公司總經理，安碁學苑董事長
學歷	美國Syracuse University電腦資訊科學碩士 國立交通大學計算機工程學士
經歷	■ 交通大學資訊工程學系109年傑出系友 ■ 安碁資訊(ACSI)(股)公司 業務協理、副總經理、總經理 ■ BMC, Taiwan業務協理、總經理 ■ IBM, Taiwan 行銷經理
專長	■ 公司營運策略規劃 ■ 業務市場開發與銷售策略研擬 ■ 產品規劃暨市場行銷企畫 ■ 軟體工程

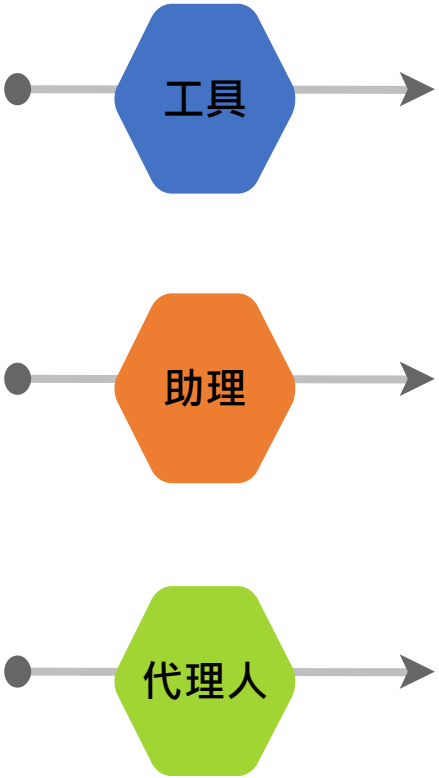
議程

- AI進程
- 地緣政治競爭
- GPT風險&對於資安威脅的影響
- 現今攻擊手法案例
- 資安管理基本面

AI取代人力?

AI進化論





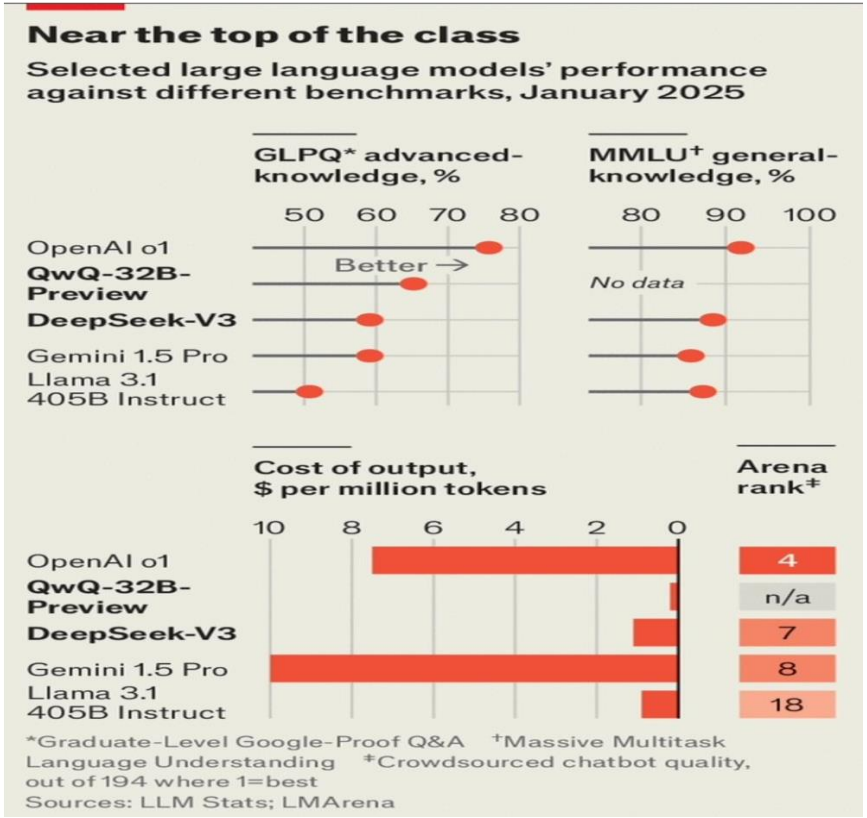
Layer 1 Embedding
- 人類Prompt 設定目標
- 請AI提供建議，文字、影音、程式、畫像…
- 人類完成絕大部分工作。
- 人類自主結束工作。

Layer 2 CoPilot
- 人類設定任務目標
- AI主動提供資訊或建議，錯字、文法修正…
- 人類和AI協作。
- 人類自主結束工作。

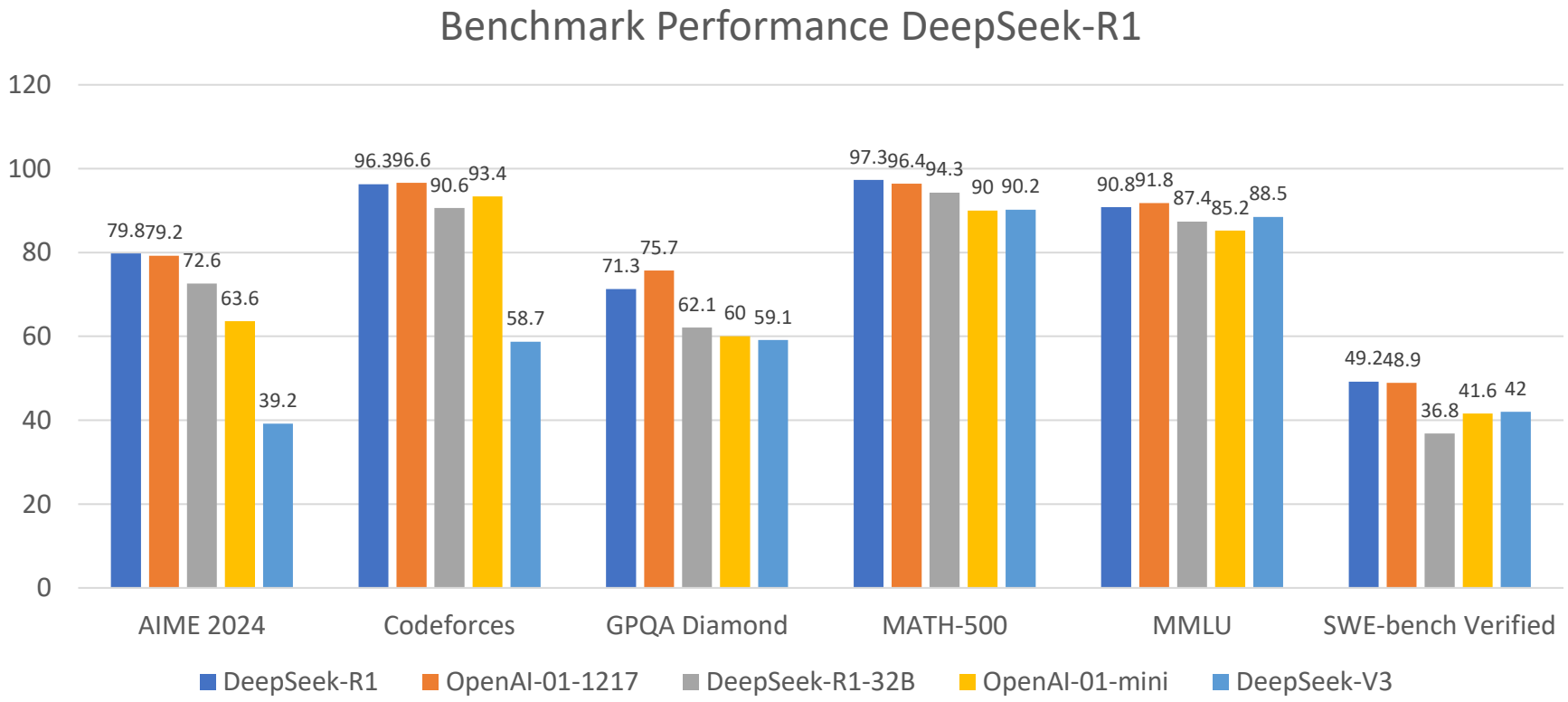
Layer 3 AI Agent
- 人類設定目標(給機器人下指令)
- AI拆分任務選擇工具，觀察和改善
- AI完成絕大部分工作。
- AI結束工作。

地緣政治競爭態勢(I)

QWQ:
Queen with Questions
(通義千問)

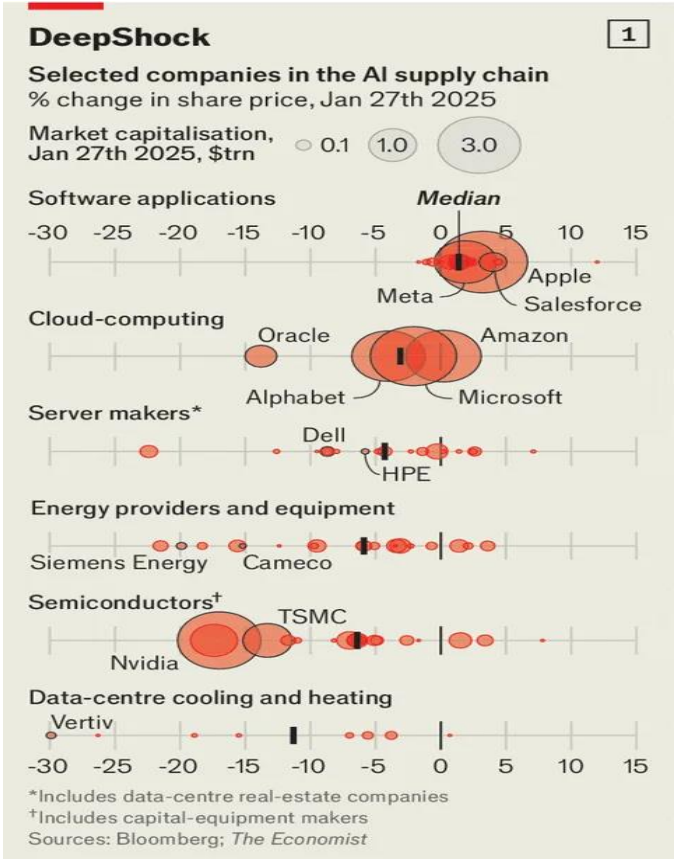


地緣政治競爭態勢(II)-iThome 2025-01-22



地緣政治競爭態勢(III)

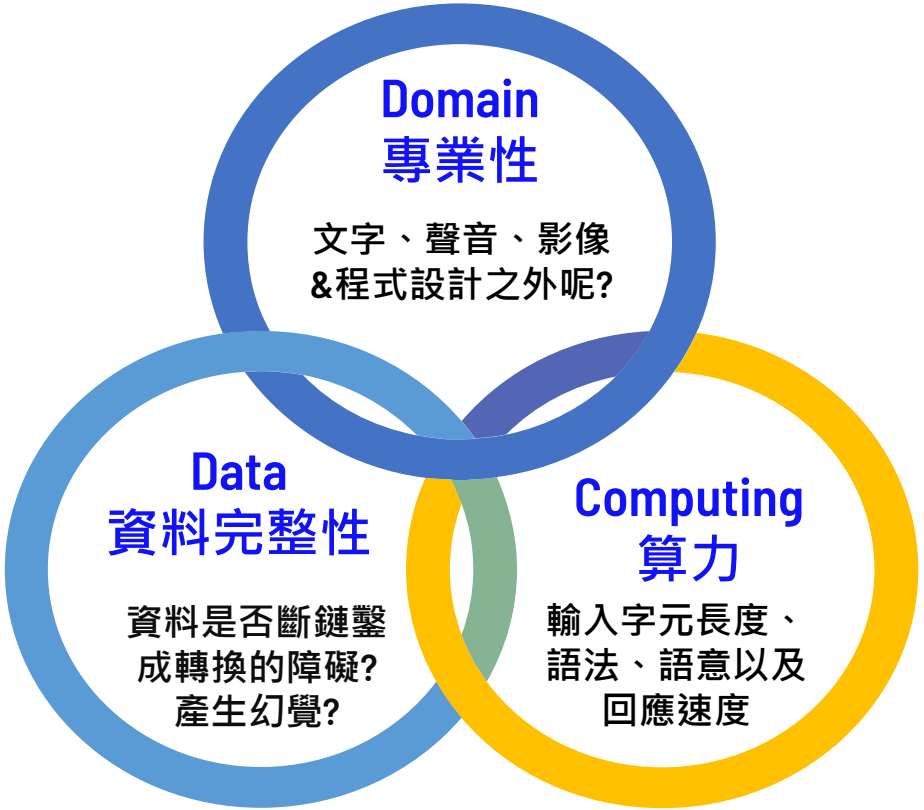
- **DeepSeek(深度求索)讓世界引起震撼，nVIDIA AI Chips引發疑慮**
  - AI生態系: AI Chips, Servers, Data Centers, 模型製作商(Model Makers: OpenAI & Anthropic…), 軟體公司(SAP&Salesforce…)，散熱系統…
  - 中國LLM模式最具成本優勢，V3僅需2000 CPUs vs世界一流16,000 CPUs，美國LLM花費數千萬美元，DeepSeek則不到6百萬美元，而且還是Open-Source，歡迎下載。
  - 另一說法來自SemiAnalysis，對沖基金High-Flyer(幻方量化)投入Nvidia A100GPU & H20GPU總金額超過USD$1.6B。



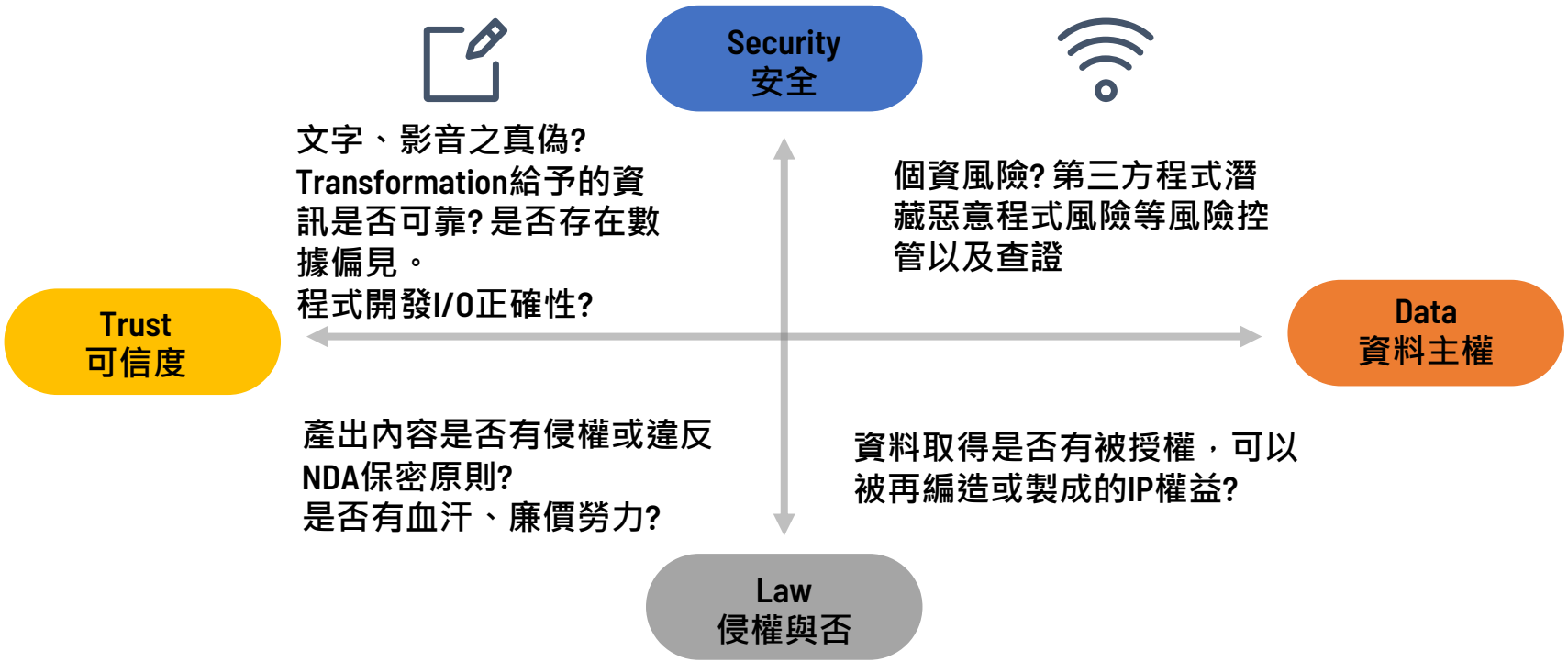
GPT的選擇性

GPT 應用場域

學術論文、簡報製作
置入性廣告搜尋
程式設計
Copilot, OpenAI, Bard, Claude…



GPT風險之所在


Security
安全
文字、影音之真偽?
Transformation給予的資訊是否可靠? 是否存在數據偏見。
程式開發I/O正確性?
個資風險? 第三方程式潛藏惡意程式風險等風險控管以及查證
Trust
可信度
Data
資料主權
產出內容是否有侵權或違反NDA保密原則?
是否有血汗、廉價勞力?
資料取得是否有被授權，可以被再編造或製成的IP權益?
Law
侵權與否

AI/GPT Pre-Trained Model

資料集

訓練過程運算資源可能被異常耗用
遭汙染的資料可能破壞模型可用性

Ingest data
準備與
萃取資料

Select algorithm
擇定演算法

Build and Train the model
建置與訓練模型

Deploy and Score the model
部署與評定模型

Maintain and re-train the model
維護及重複訓練模型

使用者輸入資料

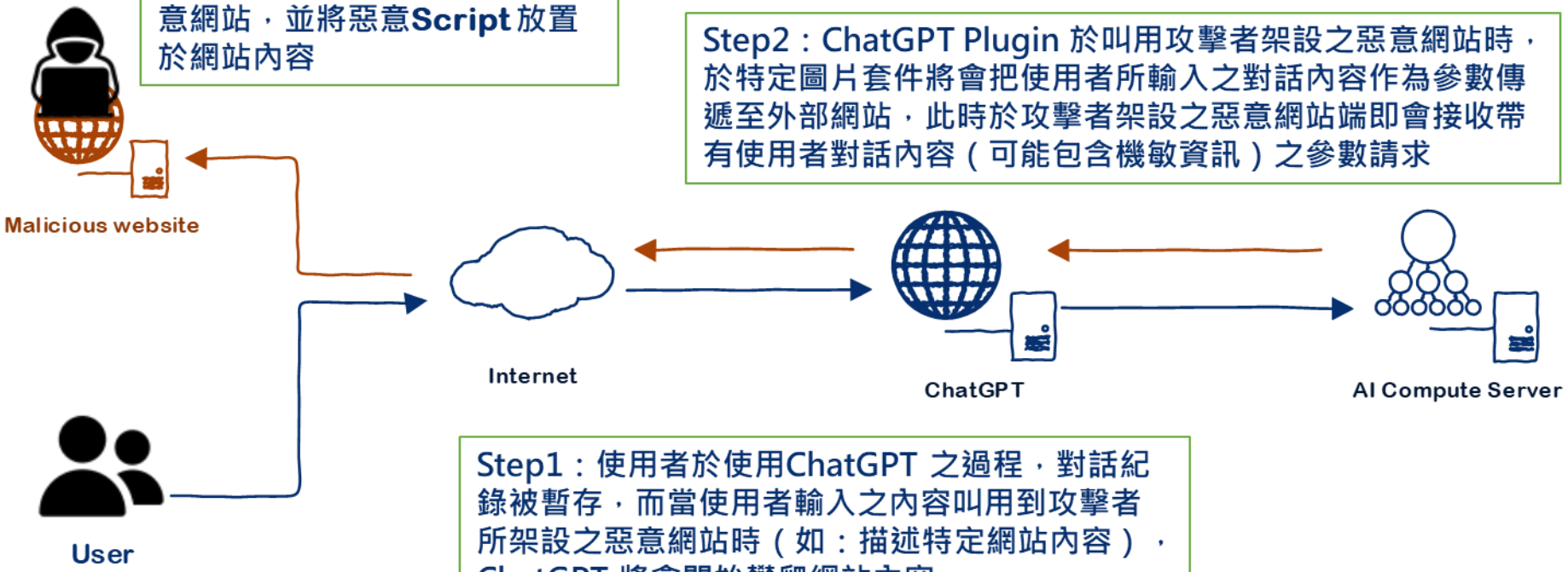
模型可能輸出預期外之結果
攻擊者可能利用演算法或合法途徑竊取模型
利用模型生成對抗資料持續破壞模型可用性

資料來源可能被汙染
攻擊者可能發動注入攻擊

AI/GPT Attack案例說明

Step0：攻擊者先於外部架設惡意網站，並將惡意**Script**放置於網站內容

Step2：ChatGPT Plugin 於叫用攻擊者架設之惡意網站時，於特定圖片套件將會把使用者所輸入之對話內容作為參數傳遞至外部網站，此時於攻擊者架設之惡意網站端即會接收帶有使用者對話內容（可能包含機敏資訊）之參數請求



Step1：使用者於使用ChatGPT 之過程，對話紀錄被暫存，而當使用者輸入之內容叫用到攻擊者所架設之惡意網站時（如：描述特定網站內容），ChatGPT 將會開始攀爬網站內容

對資安威脅的影響(I)

APT: Advanced Persistent Threat進階持續性威脅

從情報的收集，社群媒體的學習進而網路詐騙
勒索軟件攻擊目標明確化，具地緣性。

Deepfake深偽詐欺、語音詐騙

人臉識別、車牌辨識等技術轉移至詐欺
影響Fintech等相關金融業務。

不熟悉、使用不當造成資料外洩

LLM是經過類神經網路的大量資料學習，
封閉跟開放的黑盒子未經釋疑，使用不當
將造成巨大損失。

程式開發引用開放碼

程式開發隱藏漏洞未經檢測貿然上線
除錯(Debug)比開發將更費時

對資安威脅的影響(II)

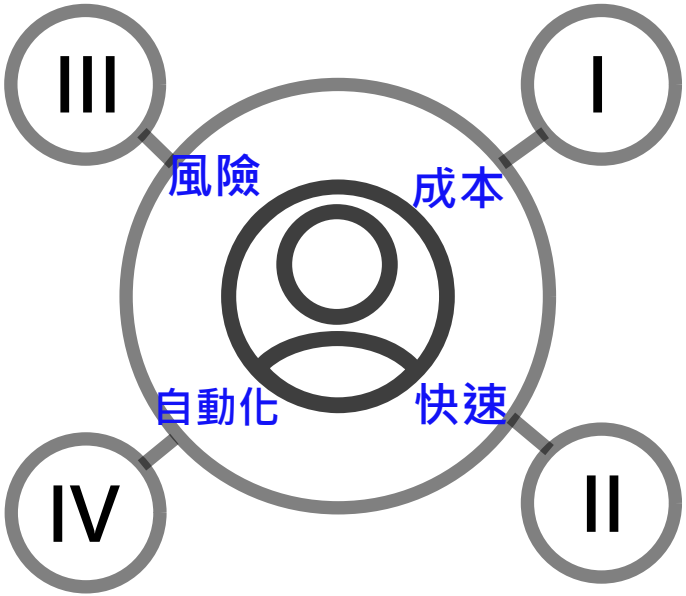
思考導入GPT的業務目的以及定位

錯誤資訊利用

公司必須明定使用政策跟範圍，限制Prompt字節的使用長度，並以權限控管做好內部稽核。

應用項目的導入

對外服務以及內部製造上線數據參數等，都必須要有嚴謹核可以及核對機制，並要有災損應對SOP。



內部資安議題

- 業務單位要求開放客戶資料查詢
- 系統龐大在設計上出現漏洞
- 內部人員使用GPT遭成資料洩漏之風險

內部資料外洩

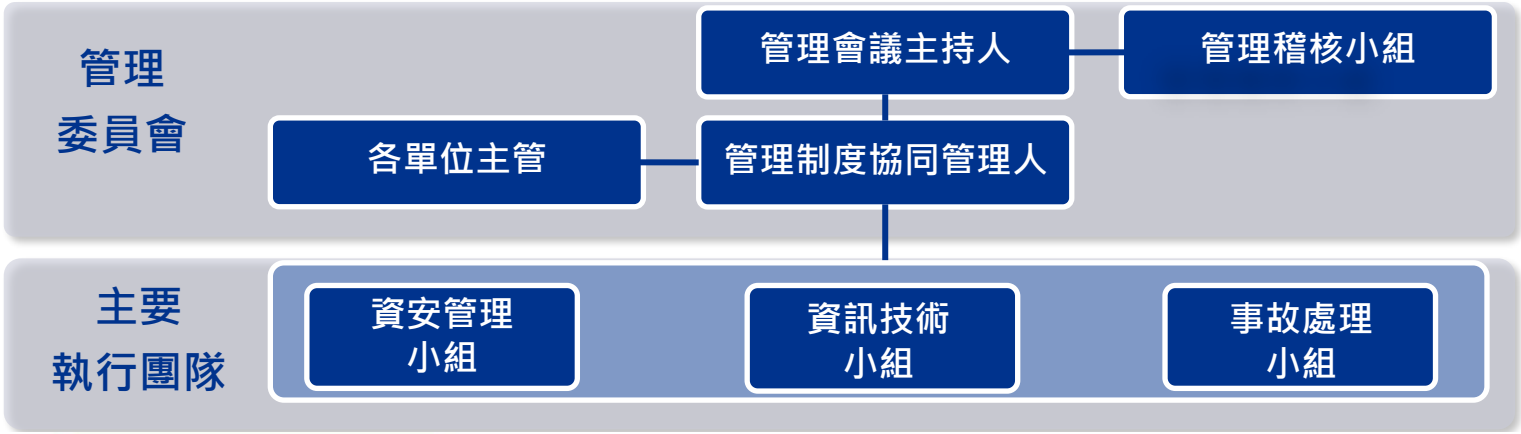
- 未經授權的人員可以存取並使用AI模型，進而導致內部資料的外洩。
- 訓練過程使用不當，造成機敏資料外洩

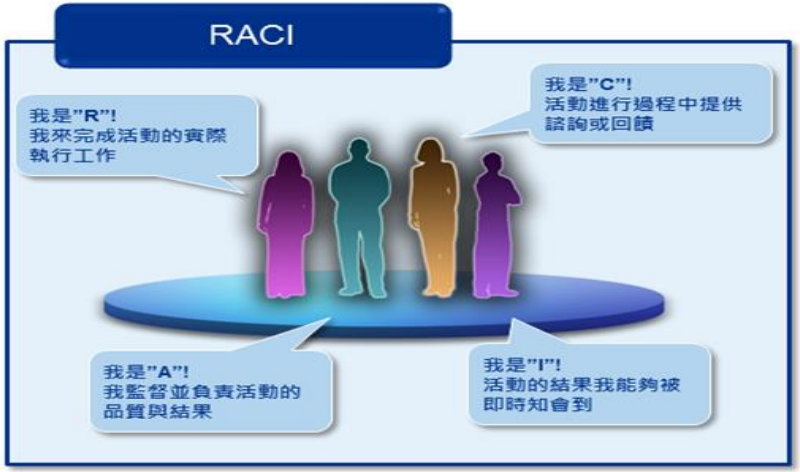
對資安防禦的強化

道高一尺，魔高一丈

- 爭取防禦空間及早發現、因應
- 事件分析加速
- 布局維運人員+BOT(Well-Trained)

基本:確認資訊安全管理組織架構





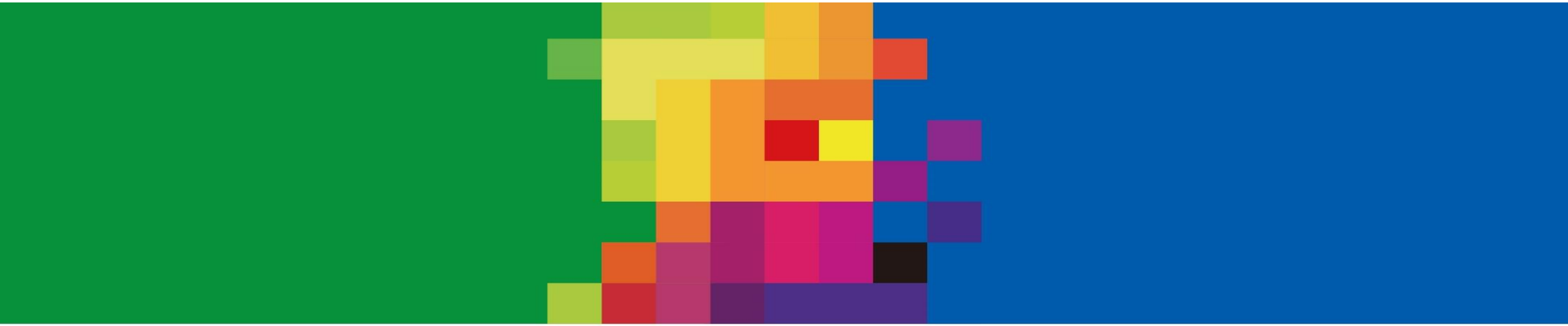
負責單位 / 資安工作事項	使用者	單位主管	承辦人	資訊單位主管
使用者帳號管理	R	A	I	I
管理者帳號管理	R	R	R	A
權限審查	R	R/A	C	C
使用者密碼保管	R/A	I	I	I
網路存取控制	R/I	R/I	R	A
作業系統存取控制	R/I	R/I	R	A

THE BEST IS YET TO COME

114 年度證券商資通安全會議

金融零信任架構及金鑰演算法升級

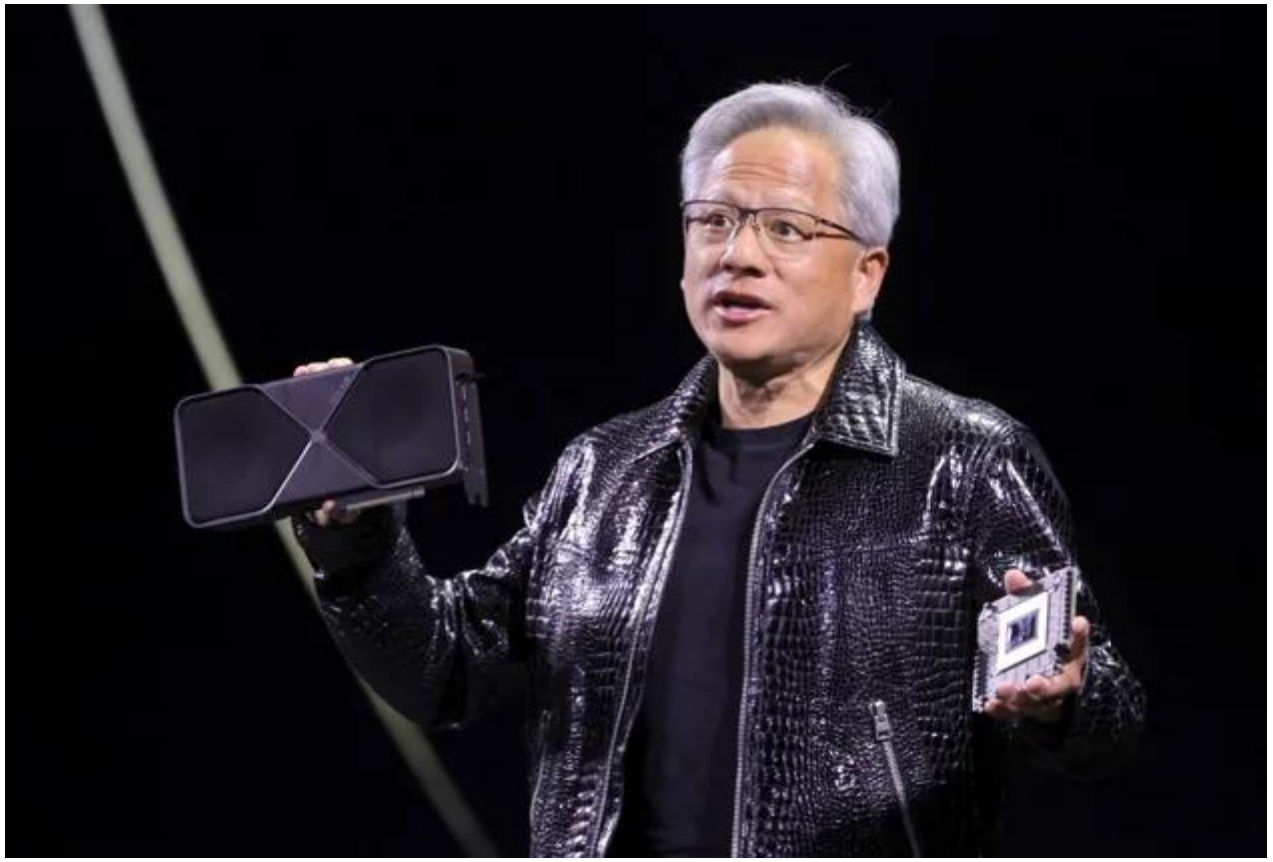
臺灣網路認證公司
連子清協理



TWCA 臺灣網路認證

TWID 身分識別中心

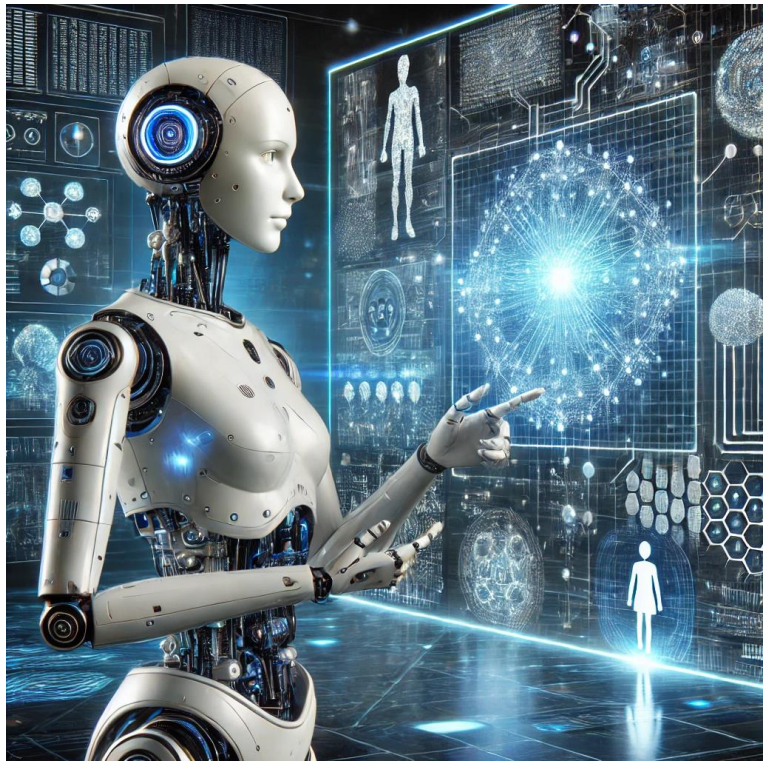
輝達CEO黃仁勳在國際電子消費展（CES 2025）發表主題演講。（路透）



Copyright of Oliver Lien

2024 年資訊界二大盛事

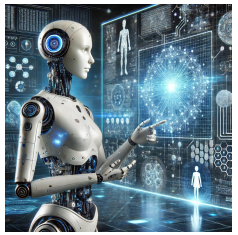
A 與 Z



AI 驅動的全面進化

Zero Trust 的全面落地

Copyright of Oliver Lien



AI

ZTA

- 在自動化、預測分析等場景幫助節約成本或創造價值。

花錢

- 避免資料外洩的高額罰款或減少因安全事件導致的營運中斷。

- 信任 AI；
- 透明的算法和可解釋性來提升用戶信心。

信任

- 從不信任，始終驗證；
- 要運用多種技術；和別人合作聯防。

- AI 可以做很多事
- 但如何在法規和隱私保護下實現？

無止境

- ZTA 要做很多事，
- 但如何確保零信任策略不影響用戶體驗？

Copyright of Oliver Lien

AI 和 ZTA 是 技術 還是 架構?

兩者的相輔相成→ 運用AI 做威脅檢測和行為分析。

- 人工智慧（AI, Artificial Intelligence）是一個廣義的概念，它既可以是一種架構，也可以是一種技術．
  - AI 作為技術定義：AI 作為一種技術，指的是用來模擬人類智能的算法、模型和工具。
  - AI 作為架構定義：AI 作為一種架構，指的是構建人工智能系統的整體框架和設計理念。

- 零信任架構（ZTA, Zero Trust Architecture）是一種架構，而不是一種單獨的技術。它是一種全面的安全設計理念，依靠多種技術和策略的整合來實現。
- 需要多種技術來支持實現
  - 技術： MFA、加密技術、軟體定義邊界（SDP）、行為分析（UBA）等。
  - 工具： 防火牆、SIEM（安全信息與事件管理）、EDR（端點檢測與響應）等。

Copyright of Oliver Lien

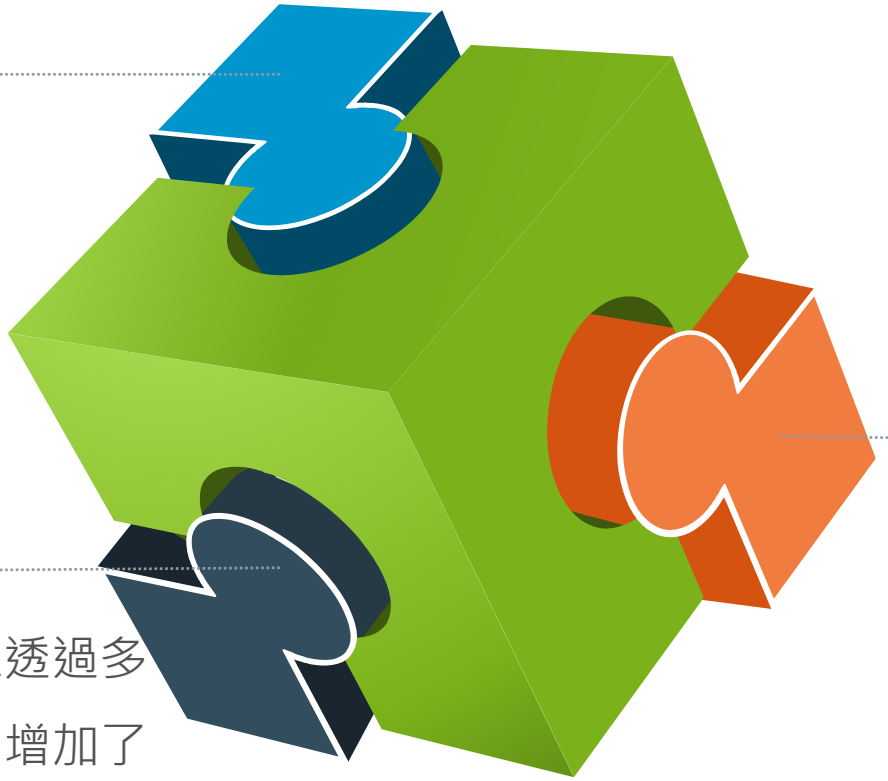
資安威脅 及 零信任基本理念

Copyright of Oliver Lien

為什麼談零信任?

科技進步帶來的挑戰

5G網路、雲端服務、
行動設備的快速發展



傳統安全模式的局限性

傳統網路安全模式以邊界防護為主，但在邊界逐漸模糊的背景下，無法有效防範內部威脅與權限濫用，駭客可利用身分管理的漏洞進行攻擊，導致企業資產面臨更大的風險。

生活型態改變

疫情加速了遠距工作的推廣，員工透過多種連線設備進行遠端作業，無形中增加了企業安全邊界的複雜性，讓傳統的安全防護方式無法應對。

Copyright of Oliver Lien

為什麼需要導入零信任架構？

1 企業邊界模糊，場域外人員及設備安全控管不易

- 居家辦公、遠端工作
- 供應商、合作商
- 雲端平台

2 假設資安有缺口，攻擊者一定會進入內網

- 內網是資安防禦最脆弱的一環，已獲授權人員、設備等不可信
- 內網探測、滲透、橫向擴散

身分 → 設備 → 網路 → 應用程式 → 資料

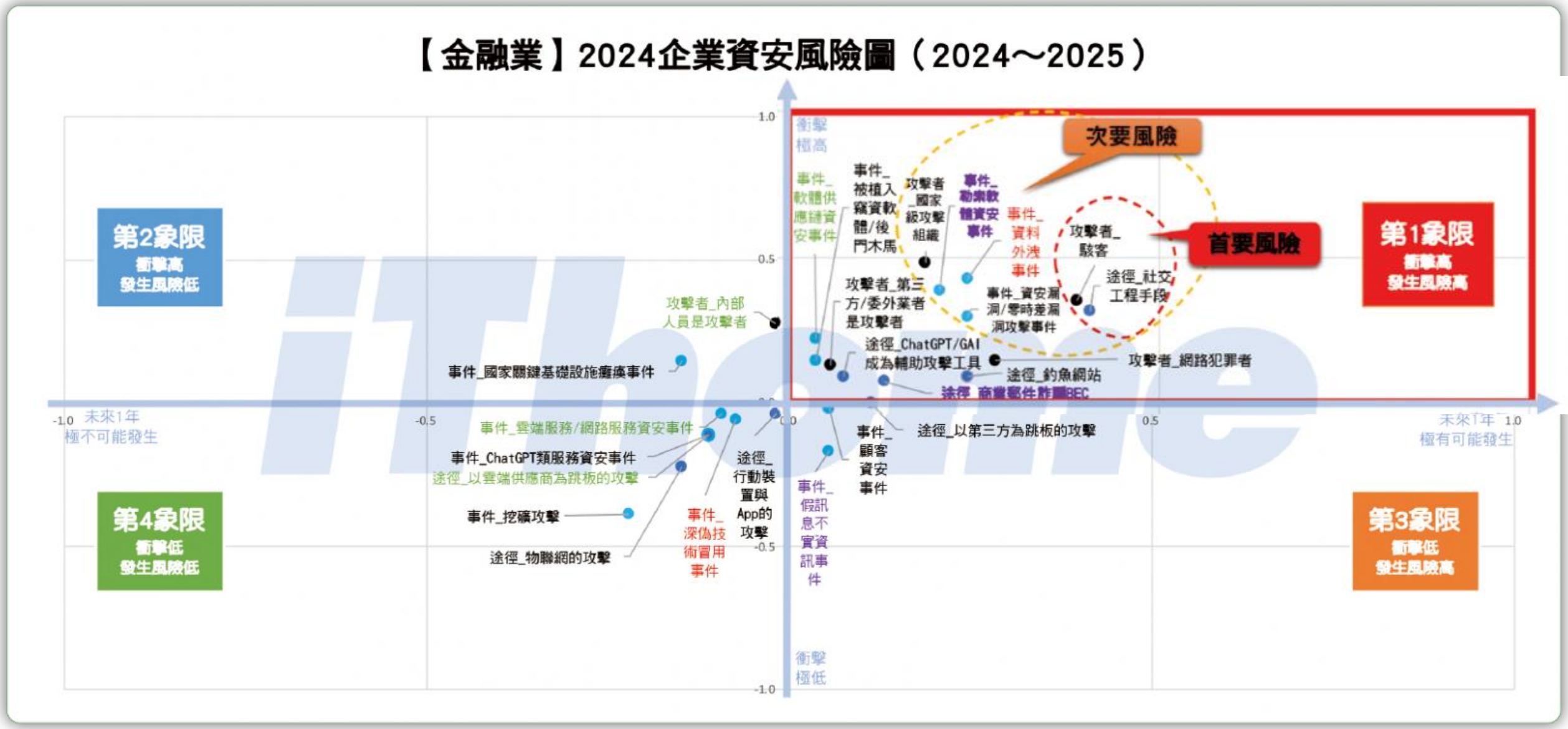
零信任思維重新檢視資安政策

- ☐ 整體資安防護框架
- ☐ 既有資安防護基礎

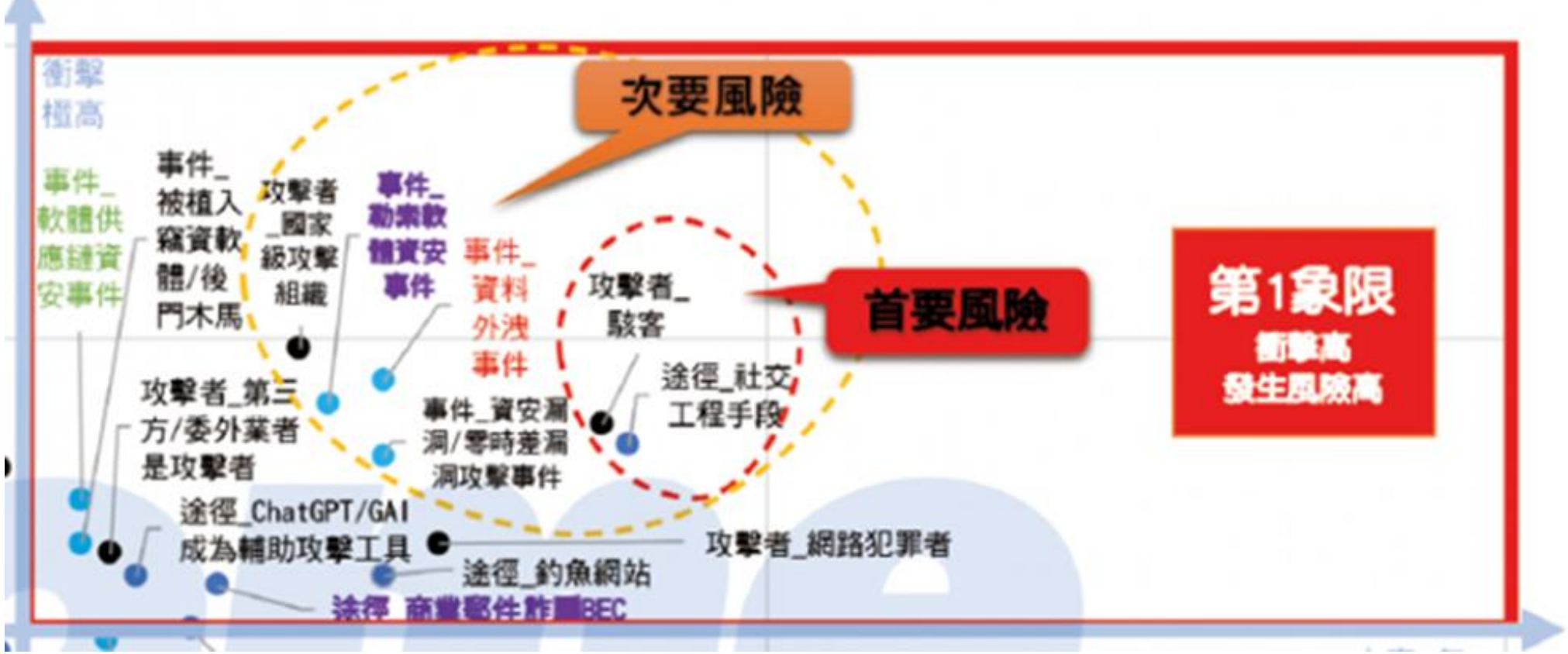
- 由外而內
  - ➢ 縮小攻擊表面、增加防禦深度
- 由內而外
  - ➢ 擴大防護表面、限縮損害衝擊
- 提高可視性
  - ➢ 持續監控與驗證

Copyright of Oliver Lien

IThome 2024 資安大調查



Copyright of Oliver Lien



- **社交工程**、 **駭客威脅**：連二年都是金融業的首要風險。
- 次要風險：去年只有**國家級攻擊組織**，今年新增 3 項：**資料外洩**、**勒索軟體**、**資安漏洞（零時差漏洞）攻擊**。
- 值得注意：
  - 紫色(衝擊及風險較去年高)：軟體供應商資安事件、商業郵件詐騙BEC(Business Email Comprosie)
  - 紅色(僅風險明顯提高)：資料外洩事件。
  - 綠色(僅衝擊明顯提高)：軟體供應商資安事件。

Copyright of Oliver Lien

零信任三個核心理念 (以 CIA 為例)

誰是總統?

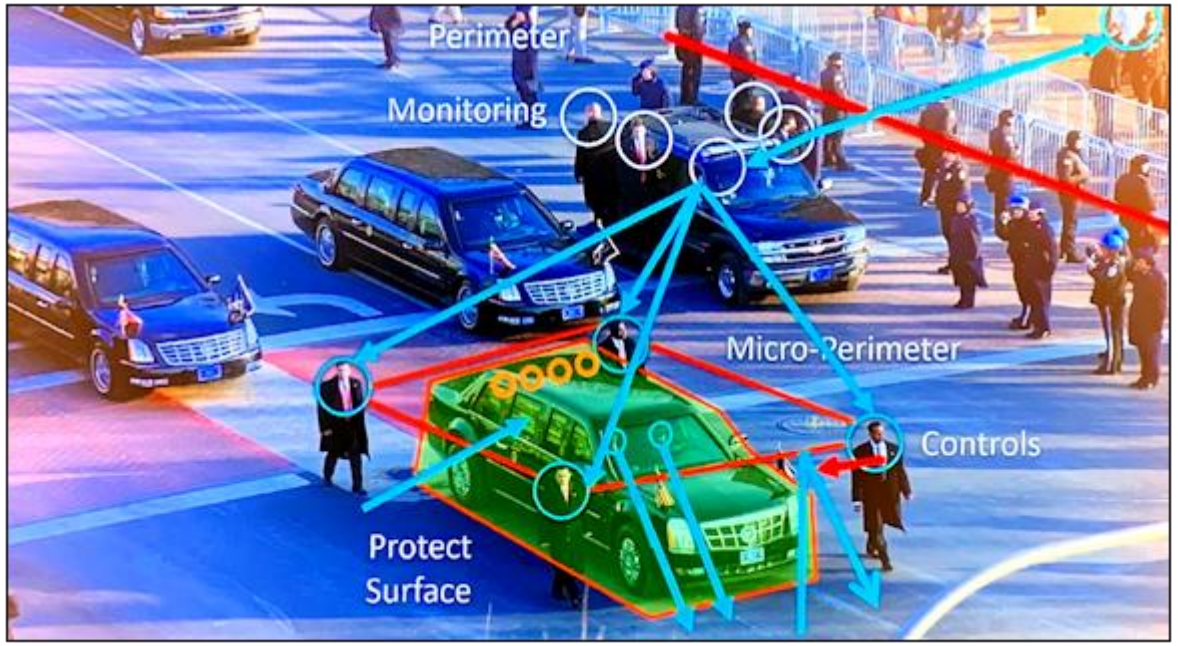
必須先清楚了解**需要保護的資產**對象，並且無需多次驗證其存在。

總統在哪裡?

對應的是資產的**可視性**，意即需要時刻掌握資料和關鍵資產的流向，並保證它們在預期的範圍內。

誰可以接近總統?

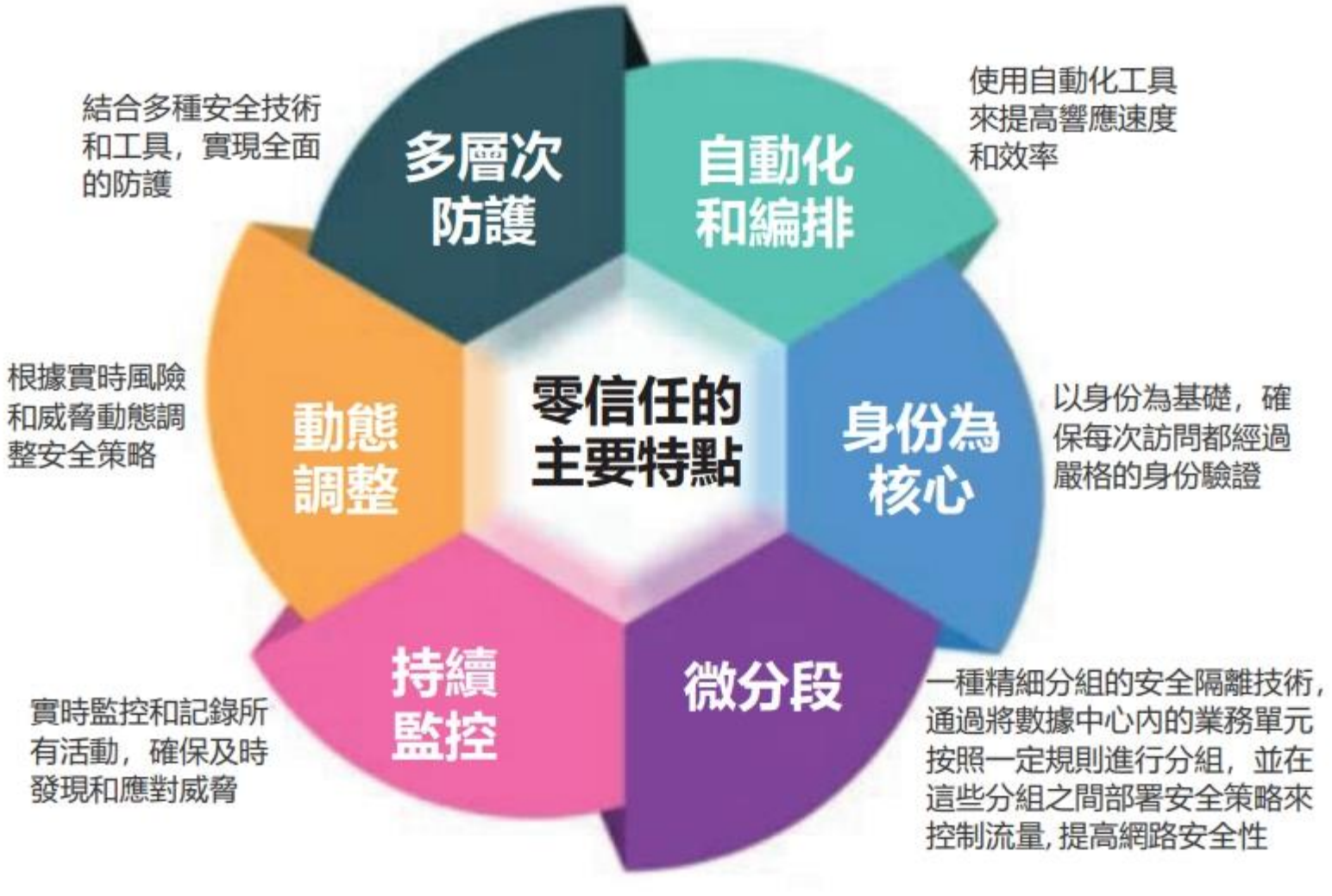
與零信任中的授權過程類似，強調**每個存取的請求都需要被精確審核**，並根據具體需求進行動態管理。



資料出處:https://www.ithome.com.tw/news/165397

Copyright of Oliver Lien

零信任核心原則：從不信任，始終驗證



資料出處:CIO Taiwan

Copyright of Oliver Lien

零信任基本架構

Copyright of Oliver Lien

零信任架構概念

國家資通安全研究院 (NIST)

- NIST 在2020年8月發佈了 SP 800-207 標準文件，提出身分識別、設備鑑別及信任推斷三大核心組件，並以身分鑑別為優先導入範圍。

美國總統指令

- 2021年 要求美國聯邦政府採用零信任架構，2022 年1月美國預算與管理辦公室制定備忘錄，於身分識別、設備、網路、應用程式與工作負載、資料五個面向滿足特定安全標準。

美國網路安全暨基礎設施安全局 (CISA)

- 2023 年 4 月發佈信任成熟度模型 2.0，依身分識別、設備、網路、應用程式與工作負載、資料等五大支柱；至自動化與協調，可視性及分析則內含於各支柱中。因應逐步導入過程，區分傳統、超始、進階、最佳化等四個等級。

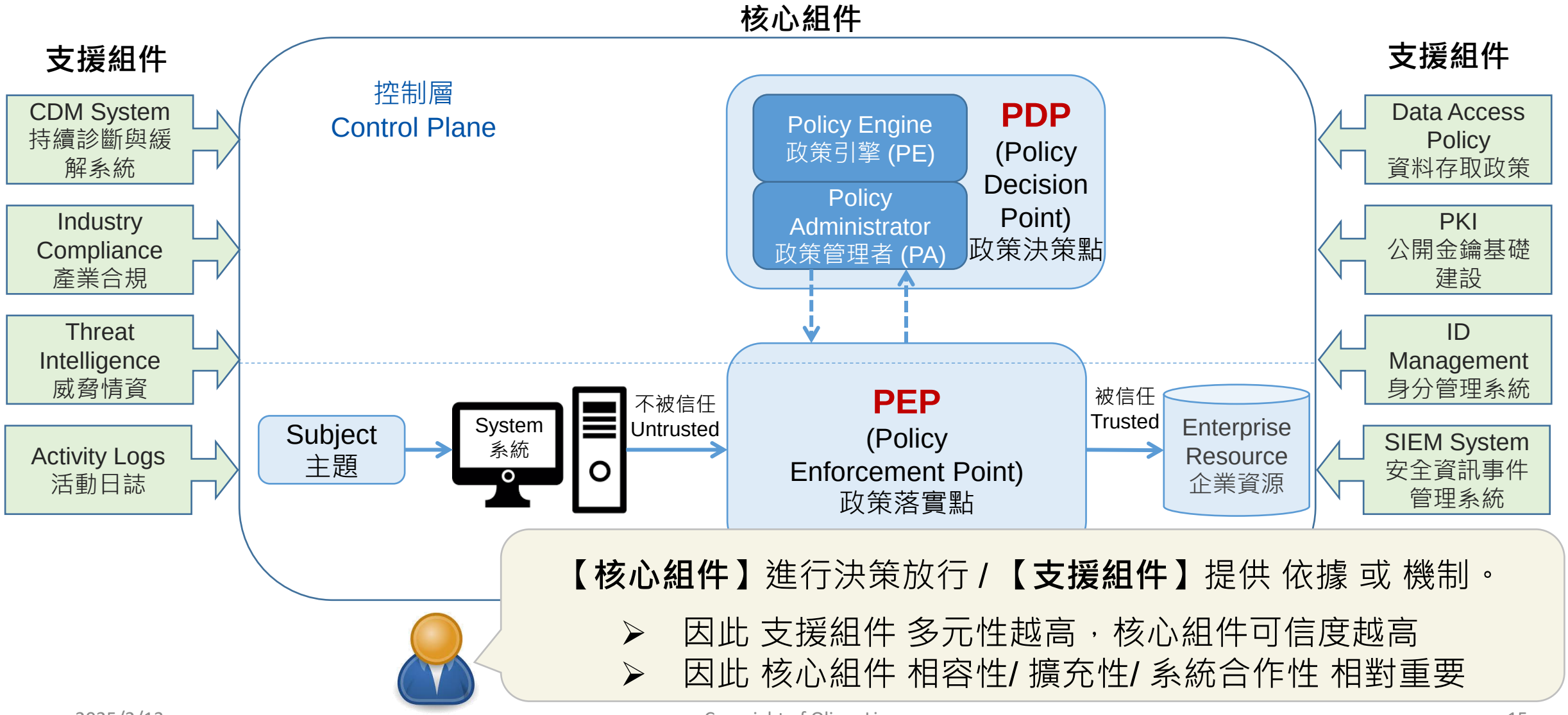
我國行政院第六期「國家資通安全發展方案 (110至113年) 之推動策略」

- 數位部資安署發展零信任網路資安防護環境，並優先推動 A 級公務機關導入試辦。自111年起，分年依序導入身分識別、設備鑑別及信任推斷等階段，也同時陸續訂定前述階段產品標準並受理廠商申請產品驗測。

金管會2022年12月發佈「金融資安行動方案 2.0」,鼓勵零信任網路部署，強化連線驗證與授權管控

Copyright of Oliver Lien

ZTA SP 800-207 邏輯架構圖



【**核心組件**】進行決策放行 / 【**支援組件**】提供 依據 或 機制。

- 因此 支援組件 多元性越高，核心組件可信度越高
- 因此 核心組件 相容性/ 擴充性/ 系統合作性 相對重要

Copyright of Oliver Lien

CISA 零信任成熟模型

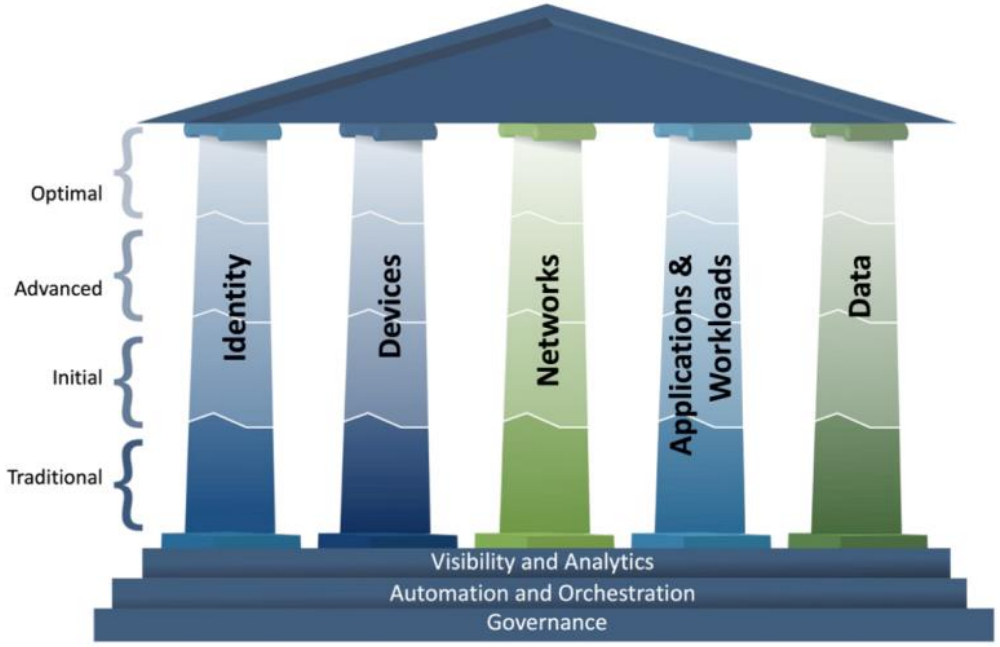


Figure 3: Zero Trust Maturity Evolution

模型評估

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

評估細節可於 CISA.gov 的官方公告
Zero Trust Maturity Model Version 2.0 查詢

Copyright of Oliver Lien

金管會零信任導入策略

Copyright of Oliver Lien

金管會 零信任架構

金管會發布「金融業導入零信任架構參考指引」
2024.07.18

國家資通安全研究院 (NIST)

- 參考 NIST SP800-207，逐步導入身分鑑別，設備鑑別及信任推斷三大核心。(2020)
- 公布「NIST SP 1800-35實施零信任架構相關資安實務指引」(2022)

資安院

- 參考 NIST SP800-207，分三年逐步導入三大核心並建立標準及提供產品檢測。

美國國防部 (Department of Defense : DoD)

- ZTA七大支柱：以**使用者**，**設備**，**應用程式與工作負載**，**網路**，**自動化與協調**，**可視性及分析**七大支柱為零信任導入基礎。
- 成熟度三階段：分為目標，目標與進階與進階三階段。

美國網路安全暨基礎設施安全局 (CISA)

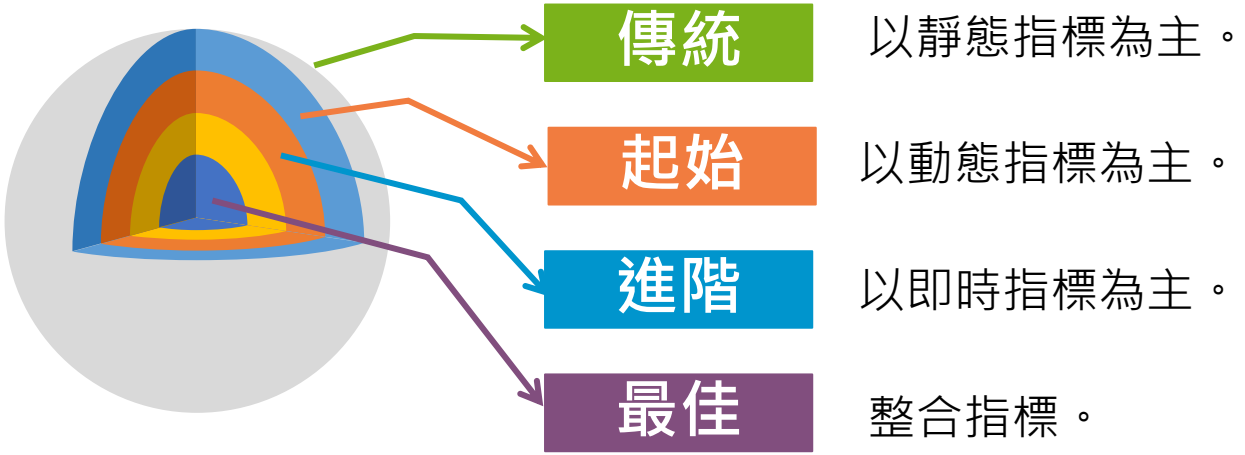
- ZTA 五大支柱：以**身分，設備，網路，應用程式與工作負載，資料**五大支柱為基礎，**自動化與協調**，**可視性及分析**已涵蓋各支柱中。
- 成熟度四階段：依五支柱成熟度，分為**傳統，初始，進階**與**最佳化**四個階段。

Copyright of Oliver Lien

金管會 零信任架構 導入策略

- 不可能一步到位，可與既有資安管理機制並存，
- 建議以關鍵保護標的為核心，盤點資源存取路徑（身分，設備，網路，應用程式，資料），
- 由外而內縮小攻擊表面並增進之防禦深度。

依據我國金融業屬性及既有資安防護能量調適如下：



Copyright of Oliver Lien

零信任成熟度指標

1 傳統

- **以靜態指標為主**，建議優先盤點既有資安防護機制之完整性，規劃防禦深度之優化及整合，不以導入新產品 / 解決方案為必要。

2 起始

- **以動態指標為主**，建立具基於屬性存取控制 (ABCD) 機制，可將每個工作階段 (Session) 之動態屬性(如:時間,地點,健康狀況,合規性)納為授權審條件。
- 動態撤銷，限銷存取授權或即時告警。
- 應辨識存取標的之關鍵數據與資源，及其被存取之交易流程，進而保護關鍵數據與資源之防護表面 (Protect Surface) 及對應之零信任政策。

3 進階

- **以即時指標為主**，整合或容事件日誌，建立定期審查及異常行為之偵測，告警及回應機制。
- 事件日誌應涵蓋依據起始階段定義之動態屬性及零信任政策產生之行為紀錄。
- 相關日誌可集中收容於 SIEM 平或並與資安監控機制 (SOC) 整合，針對入侵指標(IOC) 或攻擊行為樣態進行即時的判斷與應處(如:透過 SOC事件單, SOAR Playbook 等)，建議參考 F-ISAC 資安威脅情資及金融資安監控組態基準。.

4 最佳

- **整合指標**，建立可依資安政策決策快速調適之一致性且自動化之管理機制，確保安全性及合規性。

Copyright of Oliver I

金管會導入零信任架構實施原則

導入零信任架構實施原則

- 風險導向
- 循序漸進
- 目標導向
- 技術中立

NIST 800－27 Operative Definition:
Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised.

Copyright of Oliver Lien

風險導向→由高風險場域先行(例舉)

金管會發布「金融業導入零信任架構參考指引」，鼓勵深化資安防護
2024.07.18

遠距辦公

- 使用者及設備位於**傳統資安防護邊境外**

雲端存取

- 雲端資源位於**傳統資安防護邊境外**

系統維運管理

- 含重要**主機設備及系統軟體**之**特權帳號**管理

應用系統管理

- 重要**應用系統之管理者**(如:帳號管理員)或**高權限使用者帳號**(如:可接觸大量個資或機敏資料者)

服務供應商

- 如委外廠商之**遠端維運**管理

跨機構跨作

- 如重要應用系統開放予**外部使用者**從外部存取，其人員到離或使用設備非屬本機構管控範圍者。

Copyright of Oliver Lien

循序漸進→依分級指標分階段導入

金管會發布「金融業導入零信任架構參考指引」，鼓勵深化資安防護
2024.07.18

I 傳統

靜態指標

- **RBAC基於角色存取控制**
- 優先盤點既有資安防護機制之完整性，規劃**防禦深度之優化及整合**。

II 起始

動態指標

- **ABAC基於屬性存取控制**
- 將**動態屬性(如時間、地點, 設備合規性等)**納為授權審核條件，動態撤銷、限縮存取授權。

III 進階

即時指標

- **SIEM/SOC**
- 整合或收容事件日誌，建立定期審查及異常行為**(IOC、MitreATT&CK TTP)**之偵測、告警及回應機制。
- **UEBA**使用者和實體行為分析。

IV 最佳

整合指標

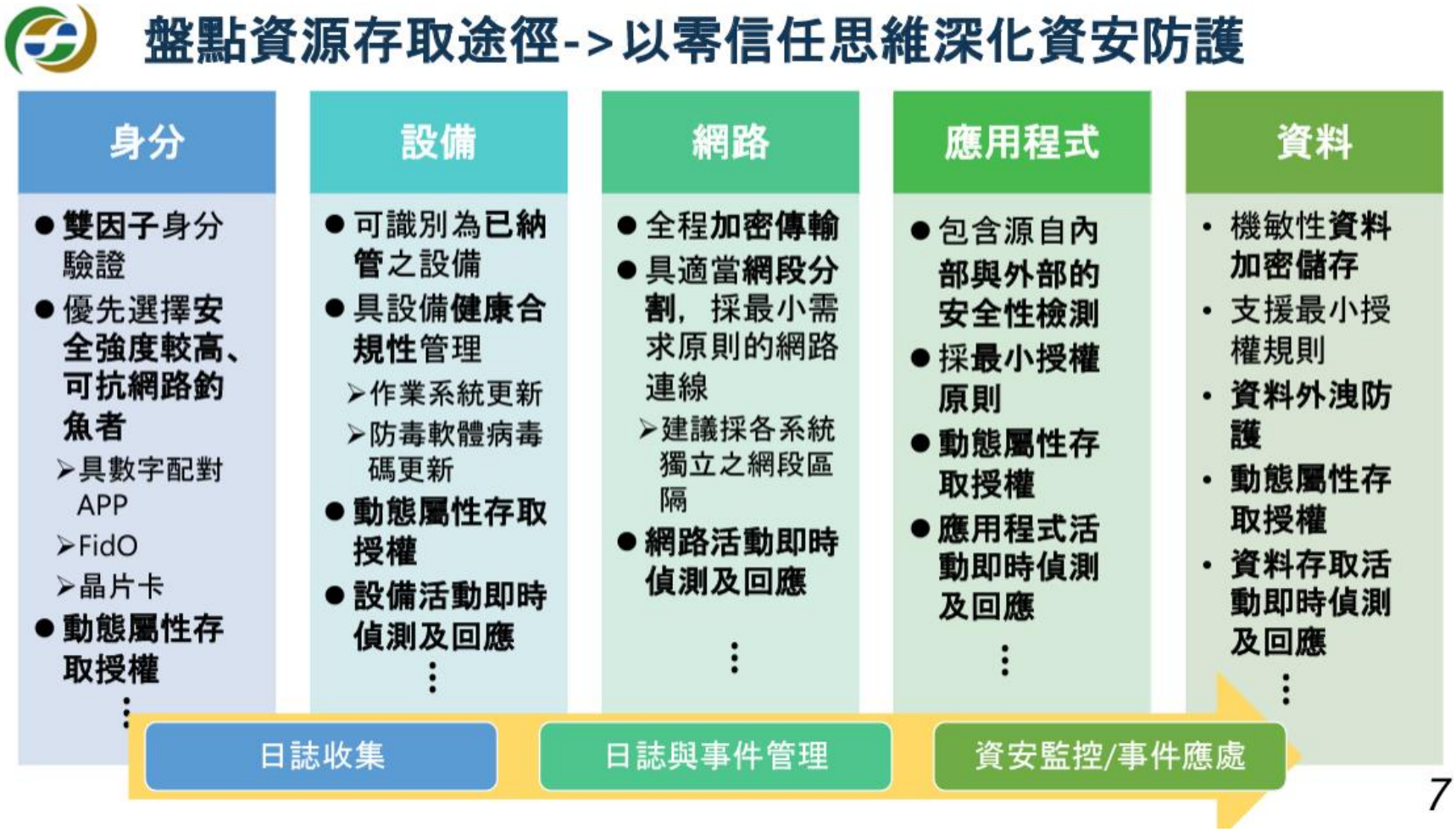
- 建立可依資安政策快速調適之一致性且自動化之管理機制，確保安全性及合規性。
- **點▸線▸面**

Copyright of Oliver Lien

金管會 零信任架構導入策略

金管會發布「金融業導入零信任架構參考指引」，鼓勵深化資安防護
2024.07.18

參考美國網際安全暨基礎設施安全局(CISA)



Copyright of Oliver Lien

零信任架構實作參考原則分級

等級 I 傳統

支柱	功能
身分	身分認證
	身分互通
設備	設備合規
	供應鏈風險
網路	網路區隔
	流量加密
應用程式	存取授權
資料	外洩防護
	資料分類
	資料可用性
	資料加密

等級 II 起始

支柱	功能
身分	身分認證
	權限存取
設備	設備合規
	資源存取
網路	網路區隔
	流量管理
應用程式	存取授權
	程式安全
	程式部署
資料	資料存取

等級 III 進階

支柱	功能
身分	可視性分析
設備	威脅防護
	可視性分析
網路	網路韌性
	可視性分析
應用程式	威脅防護
	可視性分析
資料	外洩防護
	可視性分析

等級 IV 最佳

支柱	功能
身分	可視性分析
設備	威脅防護
	可視性分析
網路	網路韌性
	可視性分析
應用程式	威脅防護
	可視性分析
資料	外洩防護
	可視性分析

儘可能在規劃及盤點朝越高等級思考

Copyright of Oliver Lien

零信任架構實作參考原則分級表—身分支柱

項次	支柱	功能	原則	等級
1.1	身份	身份認證	採用多因子驗證機制，降低依賴密碼破解、竊取或竄改等風險。	I
1.2	身份	身份認證	採用包含綁定裝置載具(如 FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對 APP 或排除指訊、語音或電子郵件 OTP)的多因子驗證機制，可抗網路釣魚威脅風險。	II
1.3	身份	身份互通	對外部使用者(如服務供應商或跨機構協作)提供或採用不同於內部使用者信賴等級之身份識別機制。(參照 ISO 29115 評估身份登錄、信物管理與身份驗證三階段)	II
1.4	身份	身份互通	如具多元身份驗證機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身份登錄、信物管理與身份驗證三階段)	I
1.5	身份	權限存取	完成身份驗證後，依「最小存取原則」落實角色存取控制(RBAC)或屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷，限縮存取授權或即時告警。	II
1.6	身份	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，分析指標指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或 SOAR Playbook 等)。(參照 F-ISAC 成員情資及金融資安監控處置基準)	III
1.7	身份	自動化治理	建立可依資安政策快速調適之一致性且自動化之管理機制，確保於帳號生命週期之安全性及合規性。	IV

1.1 身分認證：採用多因子驗證。

通常是指 所持之物 (What you have), 所知之事 (What you know), 所具之形 (What you are)。

1.4 身分互通：如多元身分識別機制會跨應用互通，其信賴等級應相同（參照 ISO 29115)。

ISO 29115 可透過身分登錄, 信物管理, 個體驗證三階段評估信賴等級 (LoA)

Copyright of Oliver Lien

零信任架構實作參考原則分級表—身分支柱

項次	支柱	功能	原則	等級
1.1	身份	身份認證		
1.2	身份	身份認證	1.2 身份認證 採用包含綁定實體載具 (如 FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對 APP ，排除簡訊、語音或電子郵件 OTP)的多因子驗證機制，可抗網路釣魚威脅風險。	
1.3	身份	身份互通	1.3 身分互通：外部使用者身分鑑別機制採用不低於內部使用者之信賴等級（參照 ISO 29115)。	
1.4	身份	身份互通	如具多元身份驗證機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身份登錄、信物管理與身份驗證三階段)	I
1.5	身份	權限存取	1.5 權限存取：完成身份驗證後，應依據「最小存取原則」來分配權限，確保用戶只能接觸到執行其工作所需的資源和資料。這可以透過以下兩種方式來實現： **1.角色存取控制 (RBAC)**：根據用戶的角色來定義其權限範圍，例如管理員和普通用戶擁有不同的權限。 **2.屬性存取控制 (ABAC)**：根據特定條件（如用戶的工作時間、所在位置等）來動態調整其權限。	
1.6	身份	可視性分析		
1.7	身份	自動化治理		

Copyright of Oliver Lien

零信任架構實作參考原則分級表—設備支柱

項次	支柱	功能	原則	等級
2.1	設備	設備合規	具有錨點且可唯一識別(如 TPM 等)納管設備機制，並針其安全要求(如防病毒、作業系統補丁等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	I
2.2	設備	設備合規	對納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控是否合規設備並採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警)。	II
2.3	設備	供應鏈風險	對外部設備(如 BYOD、服務供應商或跨機構協作筆電)，應建立不同於內部設備防護基準之管控措施；或限制需曲可控之合規中繼間道(如 VDI 等)存取。	I
2.4	設備	資源存取	可將設備動態屬性(如是否合規及合規、設備位置、是否納入納管設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具設備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼間道(如 VDI 等)存取。	
2.5	設備	威脅防護	對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威[illegible](IOC)時，可自動隔離或即時應處(如發布事件單即時追蹤處置	
2.6	設備	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資處基準)	
2.7	設備	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於週期之安全性及合規性。	

2.1 設備合規：可以清楚地盤點設備，並且每個設備都有獨一無二的身分標識（例如：TPM晶片）。此外，這些設備能根據安全需求（例如病毒檢測、操作系統狀態）進行分析與應對。對於未經管理的設備，也可以即時偵測風險，並採取措施，例如強制隔離。

2.3 供應鏈風險：對於外部設備（例如自帶的個人設備 BYOD），應該設置一套防護標準，至少要和內部設備的安全防護標準一樣高。如果無法達到標準，則應限制這些設備，並要求它們透過受控且符合規範的中繼通道（例如 VDI 虛擬桌面架構）來存取系統。

Copyright of Oliver Lien

零信任架構實作參考原則分級表—設備支柱(續)

項次	支柱	功能	原則	等級
2.1	設備	設備合規	具有錨點且可唯一識別(如 TPM 等)納管設備機制，並針其安全要求(如防病毒、作業系統補丁等)之判斷及應處機制；對未納管設備具有即時	I
2.2	設備	設備合規		
2.3	設備	供應鏈風險	對外部設備(如 BYOD、服務供應商或跨機構協作筆電)，應建立不同於內部設備防護基準之管控措施；或限制需曲可控之合規中繼間道(如 VDI 等)存取。	I
2.4	設備	資源存取		
2.5	設備	威脅防護		
2.6	設備	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對候指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組處基準)	III
2.7	設備	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於設備生命週期之安全性及合規性。	IV

2.2 設備合規：對納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控是否合規設備並採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警)。

2.4 資源存取：在設備存取資源時，要考慮設備的動態屬性（像設備是否合規、位置是否正常、是否屬外部設備）。根據這些屬性在每個工作階段 (Session) 決定是否授權、限制權限，或發出即時警告。如果發現不合規的設備，應阻斷它們的連線，並限制它們的存取路徑，讓它們只能透過可控制的合規中繼閘道（例如 VDI）存取資源。

Copyright of Oliver Lien

零信任架構實作參考原則分級表—網路支柱

項次	支柱	功能	原則	等級
3.1	網路	網路區隔	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。	I
3.2	網路	網路區隔	具軟體定義網路(SDN)或網路微分段 (Micro-Segmentation) 機制，可依使用裝務需求或動態屬性(如人員身份、設備動態及連線時間等)調整網路防護邊界，並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	II
3.3	網路	流量管理	呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備異常監控及應處機制。	II
3.4	網路	流量加密	於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。	I
3.5	網路	網路韌性	對網路連線紀錄具有即時偵測及回應機制(如 NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。	III
3.6	網路	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	III
3.7	網路	自動化治理	具可依資安政策、工作流程情境及網絡態勢快速調適之網絡管理機制。	IV

3.1 網路區隔：按照最低需求的原則來限制網路連線，只允許必要的資源存取。同時，也要限制同一網段內的設備彼此之間的連線和資源存取，避免攻擊者利用已被入侵的設備作為跳板來進行橫向擴散攻擊。

3.4 流量加密：於資源存取路徑之資料傳輸加密(如採https等加密協定)。

Copyright of Oliver Lien

零信任架構實作參考原則分級表—網路支柱(續)

項次	支柱	功能	原則	等級
3.1	網路	網路區隔	具	
3.2	網路	網路區隔	具	
3.3	網路	流量管理	呈	
3.4	網路	流量加密	於	
3.5	網路	網路韌性		
3.6	網路	可視性分析	資及金融資安監控組態基準)	
3.7	網路	自動化治理	具可依資安政策、工作流程情境及網絡態勢快速調適之網絡管理機制。	IV

3.2 網路區隔：結合軟體定義網路 (SDN) 或網路微分段 (Micro-Segmentation)機制，讓網路區隔結合「智慧調控」和「精準分割」。

- **SDN** 將網路的控制層和數據層分離，讓網路管理者能使用網路控制網路，不須依賴硬體設備配置；
- **微分段**是將網路細分為更小，更獨立的區隔的安全策略，如:定義每個應用，工作負載的安全策略；或基於上下文進行分段(設備屬性或使用者身分)等。

3.3 流量管理：可以把所有系統、設備（像電腦、伺服器）、和網路連線之間的依賴關係完整地描繪出來。這樣一來，如果某個設備有問題，我們可以馬上知道它會影響到哪些系統或連線，並監控這些設備或系統的異常情況，然後迅速採取應對措施。

Copyright of Oliver Lien

零信任架構實作參考原則分級表—應用程式支柱

項次	支柱	功能	原則	等級
4.1	應用程式	存取授權	以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身份及設備鑑別之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。	I
4.2	應用程式	存取授權	可將帳號動態屬性(如 MFA 強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。	II
4.3	應用程式	威脅防護	對應用程式活動紀錄具有即時偵測及回應機制，並可依據使用者行為或使用模式等因素評估風險(如雖屬授權範圍但于符作業常規等)，動態撤銷、限縮存取授權或即時告警。	III
4.4	應用程式	程式安全	從網際網路及防護邊界內對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經 Internet 存取之防護能力。	II
4.5	應用程式	程式部署	為應用程式開發、測試及部署建立可持續整合及部署(CI/CD)通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實權責分離。	II
4.6	應用程式	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組處基準)	III
4.7	應用程式	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於應用程式生命週期之安全性及合規性。	IV

4.1存取授權：根據工作的性質和風險，把角色區分開來，然後依照角色的風險等級來設定授權條件（例如，身份驗證和設備驗證的等級）。按照最少授權的原則，只允許角色能接觸到需要的資源。針對特權操作，設置獨立的角色授權，不與普通操作混合使用，這樣可以減少特權帳號被濫用的風險。

零信任架構實作參考原則分級表—應用程式支柱

項次	支柱	功能	原則	等級
4.1	應用程式	存取授權		
4.2	應用程式	存取授權		
4.3	應用程式	威脅防護		
4.4	應用程式	程式安全		
4.5	應用程式	程式部署		
4.6	應用程式	可視性分析		
4.7	應用程式	自動化治理		

4.2 存取授權：

- 可以根據使用者的帳號情況（例如多重驗證的強度、設備是否符合安全要求、連線的時間和地點等），來動態調整每次工作階段（Session）的授權條件。
- 對於有特別權限的操作，採用「即時存取」的方式，只在需要的時候授權，並可以隨時取消或限制授權，甚至立即發出警告。

4.4 程式安全：

- 對應用程式執行資安檢測(如:源碼檢測、弱點掃描、滲透測試)，確保應用程式本身安全性。
- 具開放經 Internet 存取之防護能力。
  - 如：透過部署 WAF(應用程式防火牆)；啟用 DDOS 保護服務；配置 HTTPS。

4.5 程式部署：

- 在應用程式的開發、測試和部署過程中，我們可以建立一個自動化的流程（稱為 CI/CD 通道），讓每個階段的操作都遵循最小授權原則（只給執行任務所需的最低權限）。
- 同時，評估是否能用自動化工具來減少人員介入帶來的錯誤，或者讓不同的團隊分工合作，確保權限管理清楚，避免一個人負責所有敏感操作。

零信任架構實作參考原則分級表—資料支柱

項次	支柱	功能	原則	等級
5.1	資料	外洩防護	針對機敏資料部屬防止資料外洩防護機制，如依據資料特徵之 DLP、資料不落地等。	I
5.2	資料	外洩防護	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理樣式等因素評估風險(如雖符合授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。	III
5.2	資料	資料分類	建立資料盤點、分類及標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	I
5.3	資料	資料可用性	建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如啟動線備份、儲存於隔離環境、防止寫入等)及有效還原。	I
5.4	資料	資料存取	可將資料存取的動態屬性(如 MFA 強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。	II
5.5	資料	資料加密	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	I
5.6	資料	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組處基準)	III
5.7	資料	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於資料生命週期之安全性及合規性。	IV

5.1 外洩防護：針對重要的敏感資料，要部署防止資料外洩的保護措施，例如根據資料特性進行的DLP（資料外洩防護）系統，或者確保資料不會被存放到本地裝置的機制。

5.2資料分離：建立一套系統來清點資料，對資料進行分類和加上標籤，確保按照資料的分類和重要性執行相應的保護政策，並支援最小授權原則，只讓必要的人或角色存取所需

5.3 資料可用性：建立一套可靠的本地備份系統，並在異地進行備份，確保備份的資料受到妥善保護。例如，可以採用離線備份、儲存在隔離的環境中，或防止資料被改寫的措施。同時，也要確保備份資料能夠在需要時有效還原。

資料加密：依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。

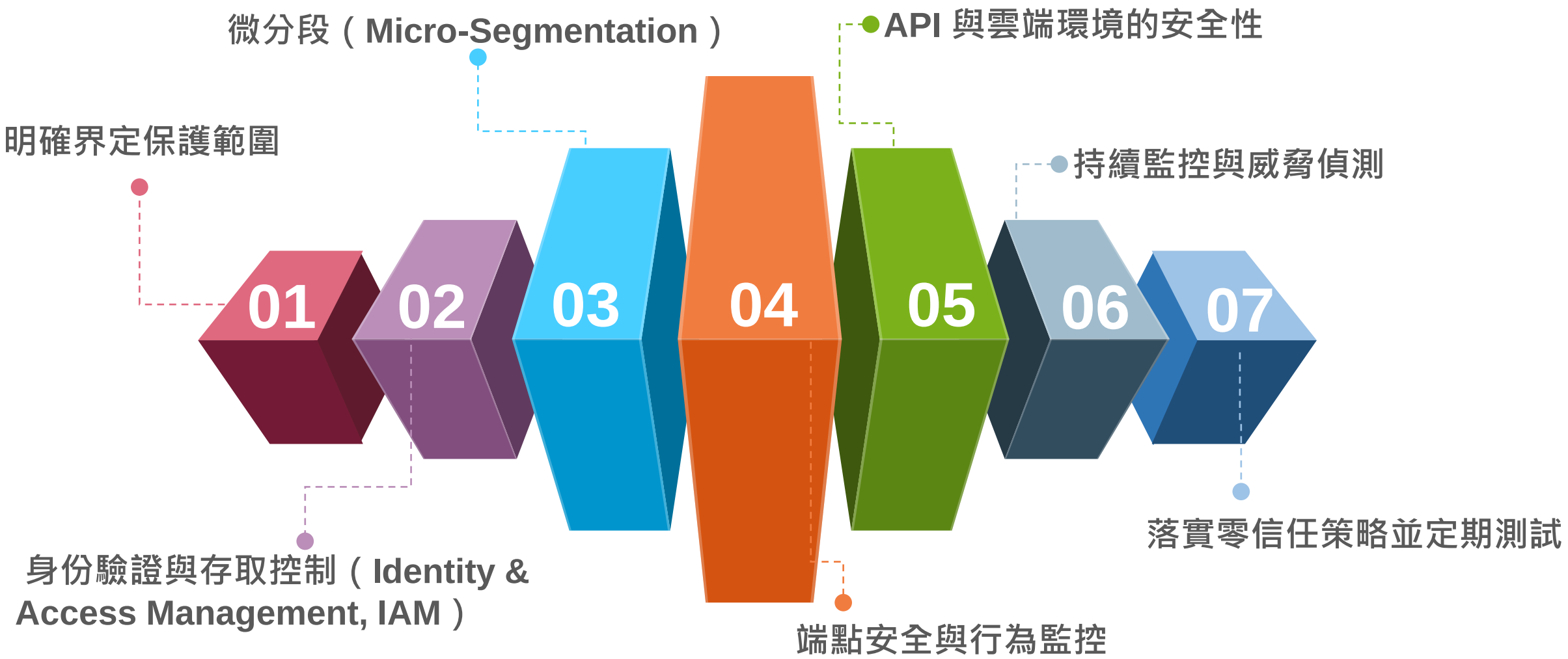
零信任架構實作參考原則分級表—資料支柱(續)

項次	支柱	功能	原則	等級
5.1	資料	外洩防護	針對機敏資料部屬防止資料外洩防護機制，如依據資料特徵之 DLP、資料不落地等。	I
5.2	資料	外洩防護	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理樣式等因素評估風險(如雖符合授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。	III
5.2	資料	資料分類	建立資料盤點、分類及標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	I
5.3	資料	資料可用性	建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如啟動線備份、儲存於隔離環境、防止寫入等)及有效還原。	I
5.4	資料	資料存取	可將資料存取的動態屬性(如 MFA 強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。	II
5.5	資料	資料加密	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	I
5.6	資料	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組處基準)	III
5.7	資料	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於資料生命週期之安全性及合規性。	IV

5.4 資料存取：可以根據使用者在每次登入或工作階段的情況（例如多重驗證的強度、設備是否符合要求、登入的時間和地點等），來動態審核他的資料存取權限。

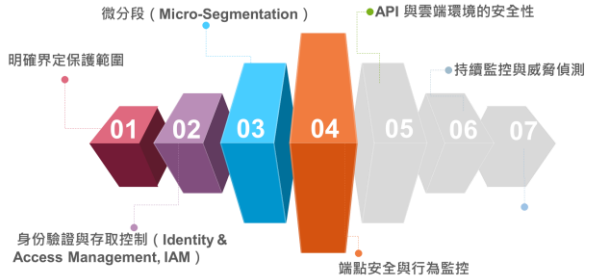
- 如果發現異常，可以要求重新驗證，並根據情況撤銷、限制存取權限，甚至立即發出警報。

導入零信任的步驟建議



Copyright of Oliver Lien

導入零信任的步驟建議



1.明確界定保護範圍（Protect Surface）

- 確定需保護的關鍵資產（如交易系統、客戶數據、API）。
- 依據 **台灣金管會「金融業零信任參考指引」** 設定保護目標。

2. 身份驗證與存取控制（Identity & Access Management, IAM）

- 強化身份驗證：採用多因素驗證（MFA），包括 FIDO、生物辨識、OTP 。
- 最小權限原則（Least Privilege）：使用 RBAC（角色型存取控制） 或 ABAC（屬性型存取控制） 限制存取權限。
- 持續驗證：導入 持續風險評估（Continuous Authentication & Authorization），根據用戶行為變化動態調整存取權限。

3.微分段（Micro-Segmentation）

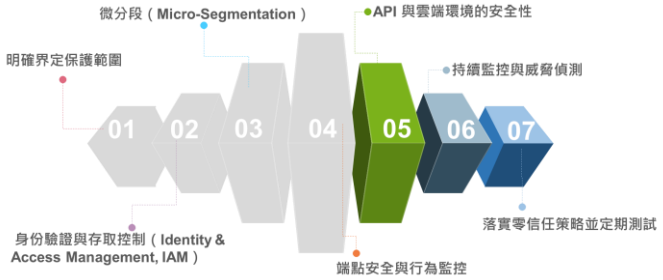
- 透過 SDP（Software Defined Perimeter） 和 網路微分段 控制內部流量。
- 交易與客戶數據應與一般 IT 環境隔離，確保攻擊影響最小化。

4.端點安全與行為監控

- 端點檢測與回應（EDR/XDR）：即時監控交易員、經紀商的端點裝置，偵測異常行為。
- 設備信任管理：對 BYOD（自攜設備）設定合規要求，如 MDM（行動裝置管理）或 ZTNA（零信任網路存取）。
- 行為分析（UEBA）：異常交易行為檢測，如不尋常的大額交易、異地登入等。

Copyright of Oliver Lien

導入零信任的步驟建議(續)



5.API 與雲端環境的安全性

- API 安全：使用 OAuth 2.0、JWT（JSON Web Token），並對 API 存取進行動態風險評估。
- 雲端資安控制：如採用 AWS/Azure/GCP 等雲端服務，應確保 Cloud Security Posture Management（CSPM）與 Cloud Access Security Broker（CASB）整合。

6.持續監控與威脅偵測

- 建立 SOC（Security Operation Center），透過 SIEM（安全資訊與事件管理）整合日誌分析。
- 導入 SOAR（安全編排與自動化應變），提升事件回應速度。

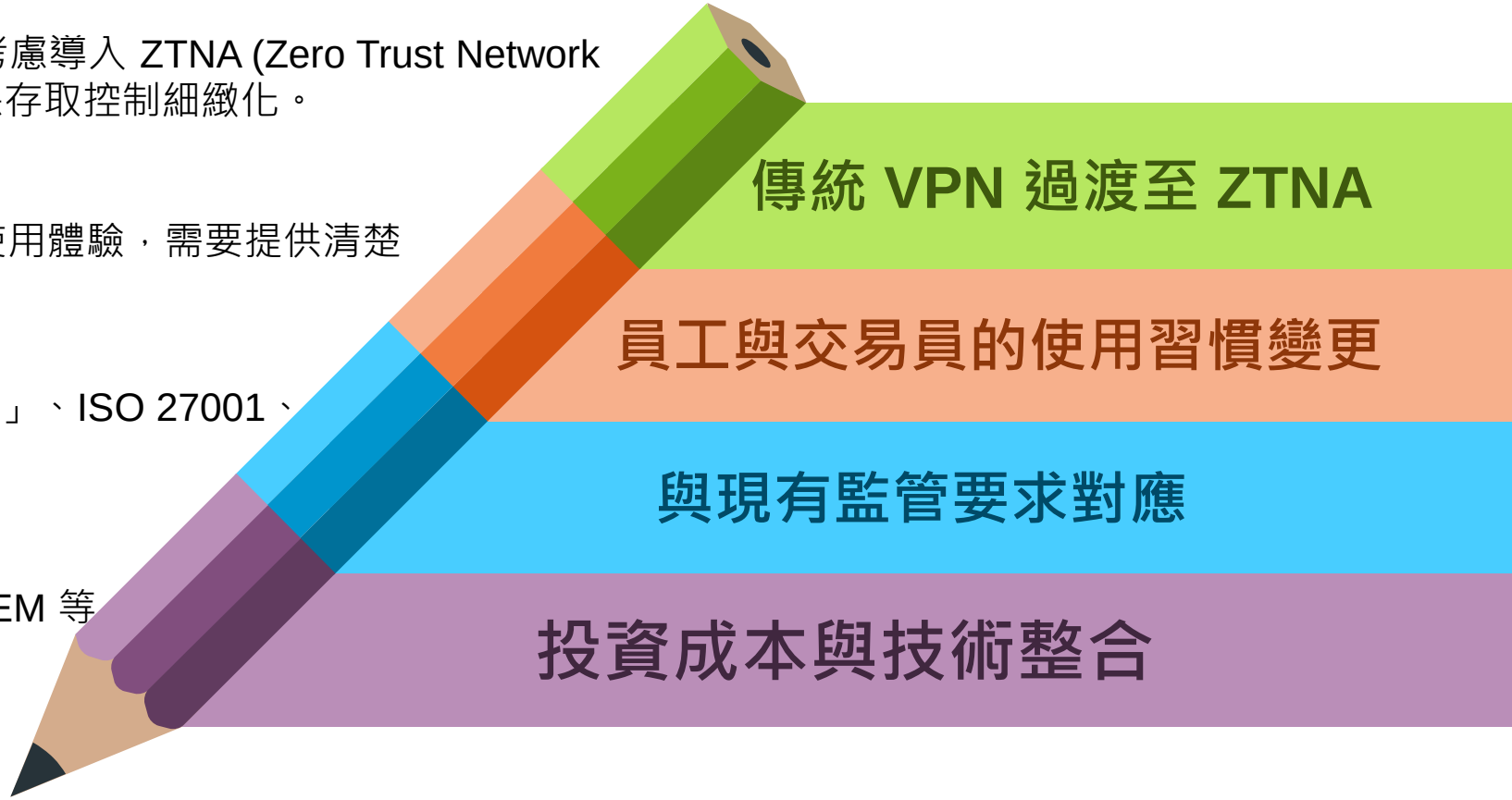
7.落實零信任策略並定期測試

- 資安演練（Red Team & Blue Team）測試零信任防禦效果。
- 定期進行滲透測試（Penetration Testing）與 威脅建模（Threat Modeling）。

Copyright of Oliver Lien

導入時的關鍵挑戰

- 企業需評估導入 ZTNA、IAM、EDR、SIEM 等技術的投資回報（ROI）。
  - 需符合 金管會「資通安全管理辦法」、ISO 27001、NIST 800-207 等資安標準。
    - VPN 容易被攻擊者利用，應考慮導入 ZTNA (Zero Trust Network Access) 取代傳統 VPN，確保存取控制細緻化。
      - 零信任導入可能影響使用體驗，需要提供清楚的使用者教育與引導。



Copyright of Oliver Lien

成功導入零信任架構的案例

- 背景：微軟在全球範圍內推行零信任架構，以應對現代化的安全挑戰。
- 措施：實施多因素驗證（MFA）、裝置管理和條件式存取等技術，確保所有員工和裝置在安全的環境中運作。

- 背景：作為零信任策略的先驅者，Google 推出了 BeyondCorp 計劃，旨在消除傳統的網路邊界。
- 措施：透過持續驗證和監控，確保所有存取請求的安全性。

南韓某大型金融機構

- 背景：員工帳號密碼設定過於簡單，或重複使用相同密碼，導致銀行內部權限控管失效，機密資訊遭未授權人員存取。
- 措施：導入人臉辨識解決方案，實現雙因子身分驗證，並部署符合韓國零信任架構的資安環境。

- 背景：面對日益增長的網路威脅和合規要求，花旗銀行開始實施零信任策略。
- 措施：強化身份驗證和存取控制，並實施持續監控。

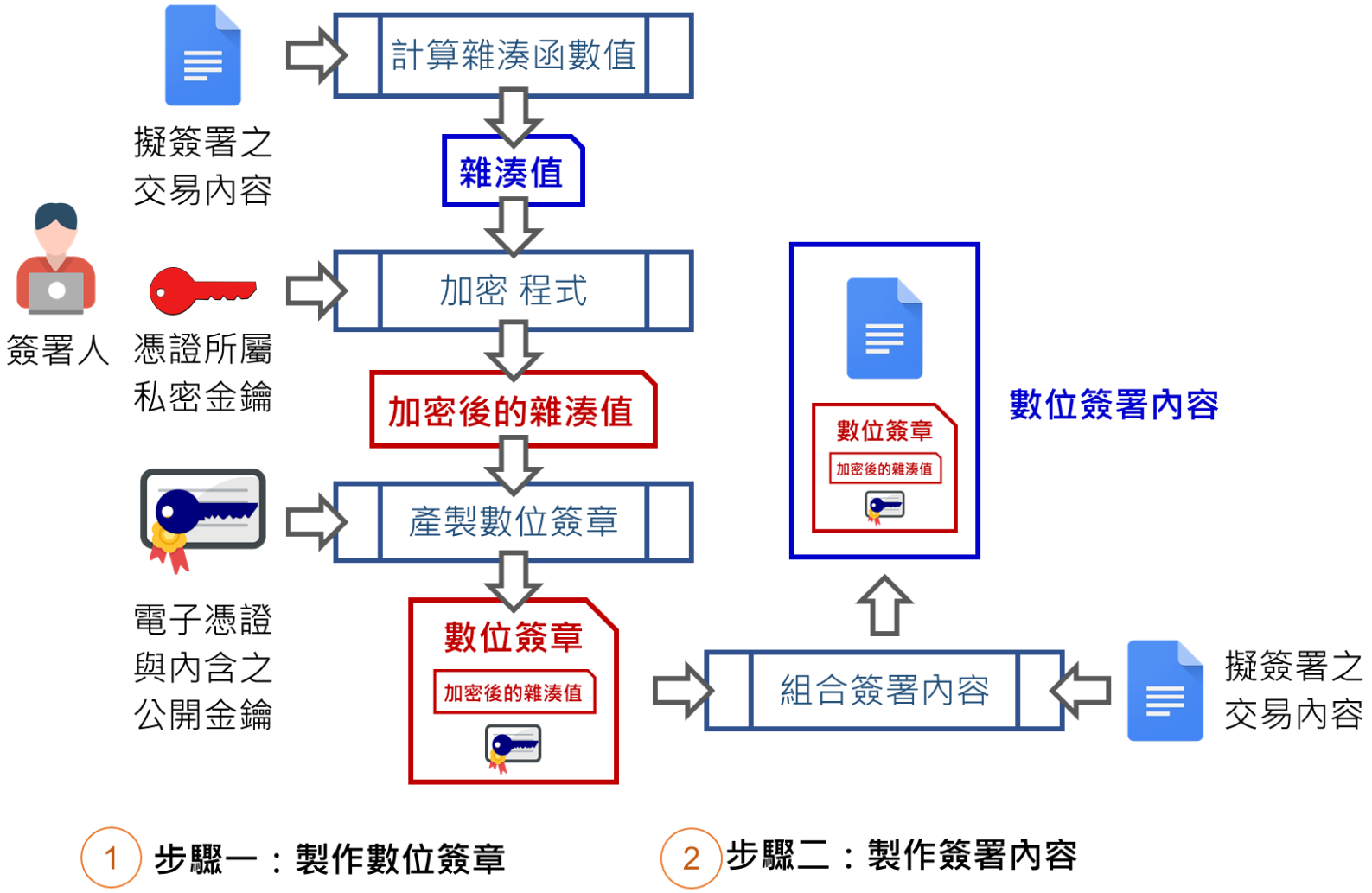
Copyright of Oliver Lien

金鑰演算法安全議題

Copyright of Oliver Lien

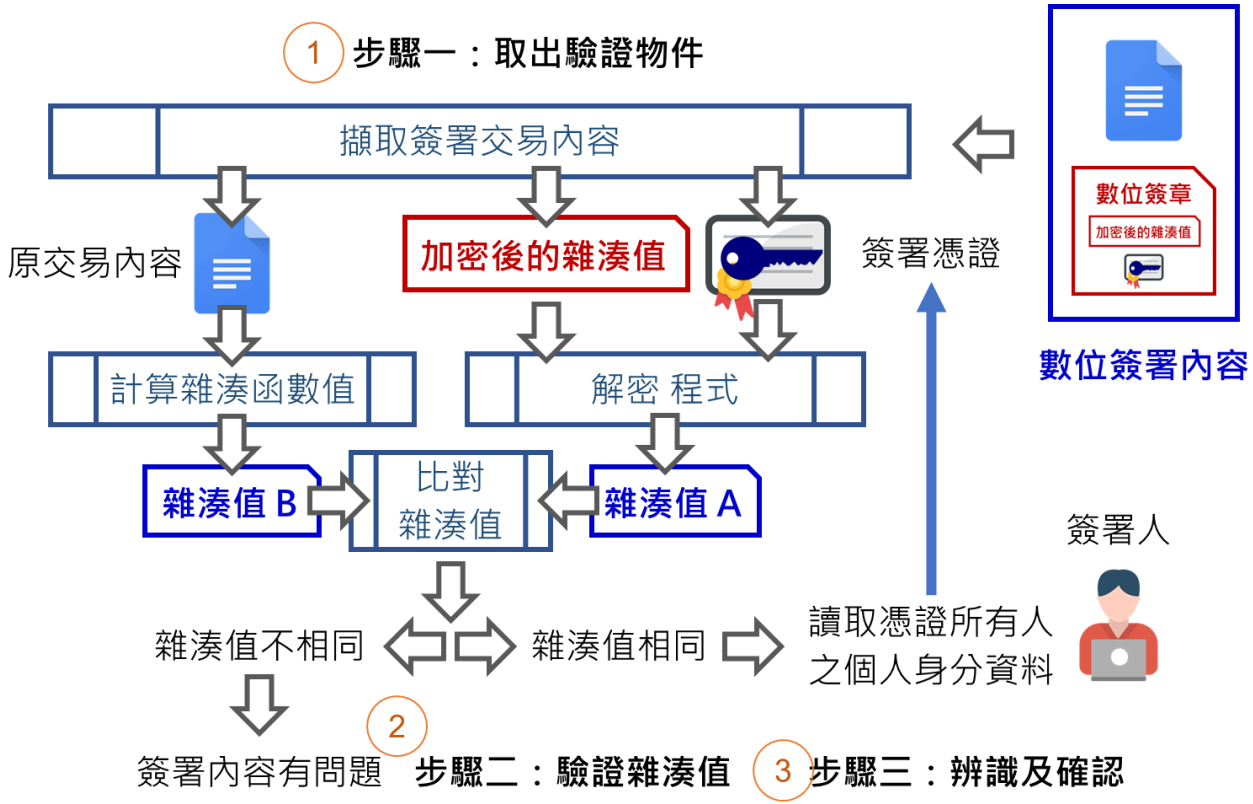
數位簽章的產製作業

- 簽署作業
  - 可以分為產製數位簽章以及製作簽署內容兩個步驟。
  - 當然，在執行簽署作業之前，簽署人必須準備好擬簽署的交易內容以及擬使用的電子憑證。



Copyright of Oliver Lien

數位簽章的驗證作業



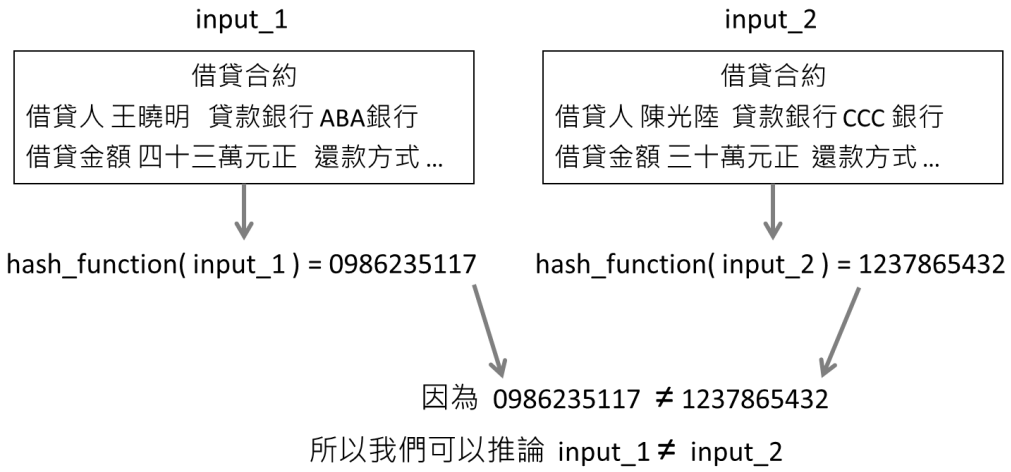
驗證作業包含三個步驟：

- 取出驗證物件
  - 從簽署的文件中提取：原始的電子文件簽署用的憑證加密後的雜湊值。
- 驗證雜湊值
  - 用憑證的公開金鑰解密簽章的雜湊值。比較解密後的雜湊值和原文件的雜湊值是否一致，確認文件是否被修改。
- 確認簽署人及內容真偽簽署人身分驗證：
  - 用憑證上的資訊（如姓名或帳號）確認簽署人。
  - 內容完整性檢查：確定文件沒有被竄改，並確認簽章屬於該文件。

Copyright of Oliver Lien

雜湊函數演算法 (hash function algorithm) 的概念

- 甚麼是雜湊函數 (hash function)？所謂雜湊函數就是一種變換數位資料的機制。概念如下：
- 將一組數位資料輸入「雜湊函數」，雜湊函數會將這組輸入資料轉換成一組固定長度的亂碼，稱之為「雜湊值 (hash value)」。
- 雜湊函數的特性：
  - 輸入一樣，輸出一定相同。
  - 輸出長度固定。(如：SHA 256雜湊函數輸出永遠是256位元。
  - 小變化，大不同。
  - 不可逆 (沒辦法反推)



Copyright of Oliver Lien

由於金鑰演算法涉及簽章安全性，目前各界對金鑰演算法升級之看法如下：

國際標準

- OWASP建議避免使用SHA-1，且應優先考慮更安全的雜湊函式[1]
- NIST SP 800-131A (關於演算法和金鑰長度的建議)及NIST SP 800-57 (金鑰管理的建議)兩項專業指引，均明確指出 SHA-1雜湊函式之安全強度不足[2]
- NIST 宣布 2030 年應完全停用 SHA-1 演算法[3]

國內要求

- 銀行公會金融 XML 憑證共通性規範已要求使用 SHA256 [4]
- 電子銀行業務安控作業基準建議雜湊函式使用 SHA256 [5]
- 國家資通安全研究院於資安檢測項目中建議避免使用 SHA-1 雜湊函式進行加密簽章[6]

市場實務

- 配合規範要求，現今銀行在電子憑證的使用皆已採用 SHA256 演算法。
- CA/Browser Forum公告不再支援 SHA-1 電子憑證，且至今各大瀏覽器皆已棄用[7] 。
- 內政部自然人憑證已不再採用 SHA-1 雜湊函式[8]

Copyright of Oliver Lien

SHA 的背景及安全性問題

- SHA-1 的背景與歷史
  - SHA-1 由 NIST 於 1995 年設計，用於數位簽章、SSL/TLS 憑證、密碼雜湊等。
  - 主要用途： HTTPS、Git、數位憑證（X.509）、密碼存儲。
  - 現代安全需求無法滿足，面臨重大風險
- SHA -1 的安全性問題
  - 🛑 碰撞攻擊（Collision Attack）已被證實
    - 2017 年：Google 與 CWI 研究院發布 SHA-1 SHAttered 攻擊。
    - 攻擊成本（2020 年估算）：約 4.5 萬美元，未來將更低。
    - 影響：惡意文件可偽造相同雜湊值，破壞完整性。
  - ⚠ 預像攻擊（Chosen-Prefix Collision Attack）
    - 2019 年出現更強攻擊，可針對特定內容製造碰撞。
    - 影響：數位簽章、HTTPS 憑證、密碼存儲安全性降低。

Copyright of Oliver Lien

預像攻擊 V.S. 碰撞攻擊

攻擊類型	預像攻擊（Preimage Attack）	碰撞攻擊（Collision Attack）
目標	反推出雜湊值的原始輸入	找到兩個不同的輸入，產生相同的雜湊值
難度	一般比碰撞攻擊更困難	相對較容易（Birthday Attack 原理）
應用場景	破解密碼、偽造數位簽章	破壞數位簽章、憑證安全性
攻擊影響	偽造特定內容的文件	創造兩份不同但具有相同 SHA-1 的文件
SHA-1 是否易受影響？	目前有可能	2017 年 SHAttered 攻擊成功

Copyright of Oliver Lien

SHA-1 風險影響

Chrome、Firefox、Edge 等瀏覽器已全面 停用 SHA-1 憑證。

- **Google Chrome**：自 **2017 年 1 月** 發行的 Chrome 56 版本起，停止支援 SHA-1 憑證。
- **Mozilla Firefox**：自 **2017 年 1 月** 發行的 Firefox 51 版本起，停止支援 SHA-1 憑證。
- **Microsoft Edge**：自 **2017 年 2 月 14 日** 起，停止支援 SHA-1 憑證。
- **Internet Explorer 11**：自 **2017 年 2 月 14 日** 起，停止支援 SHA-1 憑證。
- **Apple Safari**：自 **2017 年** 起，停止支援 SHA-1 憑證。
- **Opera**：自 **2017 年** 起，停止支援 SHA-1 憑證。

數位簽章

使用 SHA-1 進行文件驗證，可能被偽造。

密碼儲存

SHA-1 雜湊過於脆弱，容易遭到破解。

金融機構影響

金融監管機構（FSC）建議提升密碼雜湊標準。

Copyright of Oliver Lien

SHA-1 v.s. SHA-2

特性	SHA-1	SHA-2	SHA-256
發佈年份	1995 年	2001 年	SHA-2 家族中的一部分（2001）
雜湊長度	160-bit	224, 256, 384, 512-bit	256-bit
安全性	已被破解，不安全	目前無已知有效攻擊	目前無已知有效攻擊
碰撞攻擊	2017 年 SHAttered 攻擊成功	尚未有實際成功案例	尚未有實際成功案例
預像攻擊	2019 年已成功	目前無已知成功攻擊	目前無已知成功攻擊
應用場景	HTTPS（已淘汰）、Git、舊憑證	HTTPS、區塊鏈、金融、密碼存儲	區塊鏈（比特幣）、密碼雜湊、安全通信

Copyright of Oliver Lien

SHA 與金鑰長度的關聯

SHA 本身不是加密演算法，但它在**數位簽章與憑證（如 RSA、ECDSA）**中用來生成雜湊值。
因此，在選擇金鑰長度時，通常需要考慮 SHA 雜湊的強度。

演算法類型	建議 SHA 演算法	建議金鑰長度（bit）	適用場景
RSA	SHA-256 / SHA-384	2048-bit 以上	HTTPS、SSL/TLS、數位簽章
ECDSA（橢圓曲線簽章）	SHA-256 / SHA-384	256-bit 以上	金融、區塊鏈、數位簽章
AES（對稱加密）	SHA-256 / SHA-384	128-bit / 256-bit	資料加密
HMAC（雜湊訊息驗證碼	SHA-256 / SHA-512	N/A（基於雜湊長度）	API 金鑰驗證

金鑰長度與 SHA 雜湊長度的搭配

- RSA-2048：通常搭配 SHA-256 來確保足夠的安全性。
- RSA-3072：通常搭配 SHA-384 或 SHA-512。
- ECC-256（橢圓曲線加密）：通常搭配 SHA-256。
- ECC-384：通常搭配 SHA-384。

Copyright of Oliver Lien

因應方案建議

1. 資訊安全遵循業界標準

(1) 支援 SHA256 憑證演算法, 因應國際規範與資安需求

(2) 出貨之主程式皆經原始碼掃描與修正

(3) 舊框架與第三方函式庫經全面改寫與汰換以符合現有資安標準

2. 三階段逐步提升, 降低切換風險

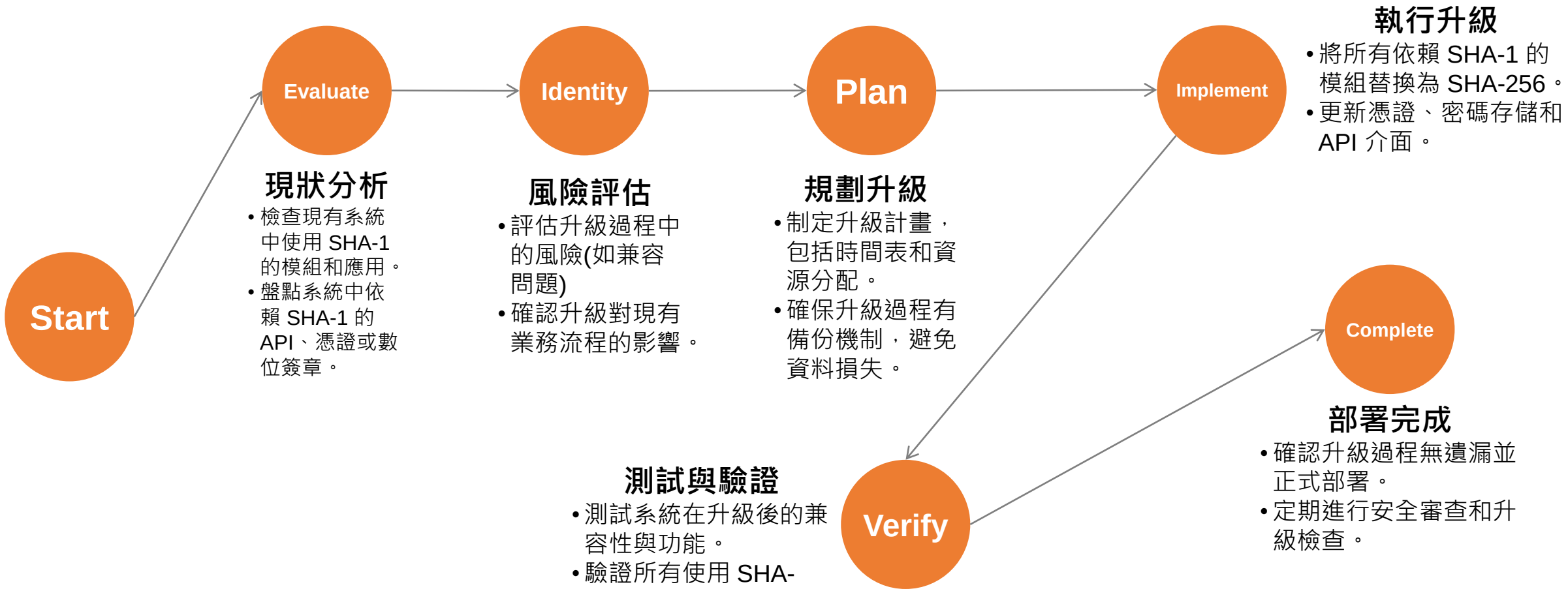
(1) 提升：提升新安控系統

(2) 移轉：交易 AP 整合安控元件與新安控系統, 逐步切換至新安控系統

(3) 切換：CA 待證券商安控系統全面備妥後進行 SHA2 憑證切換

Copyright of Oliver Lien

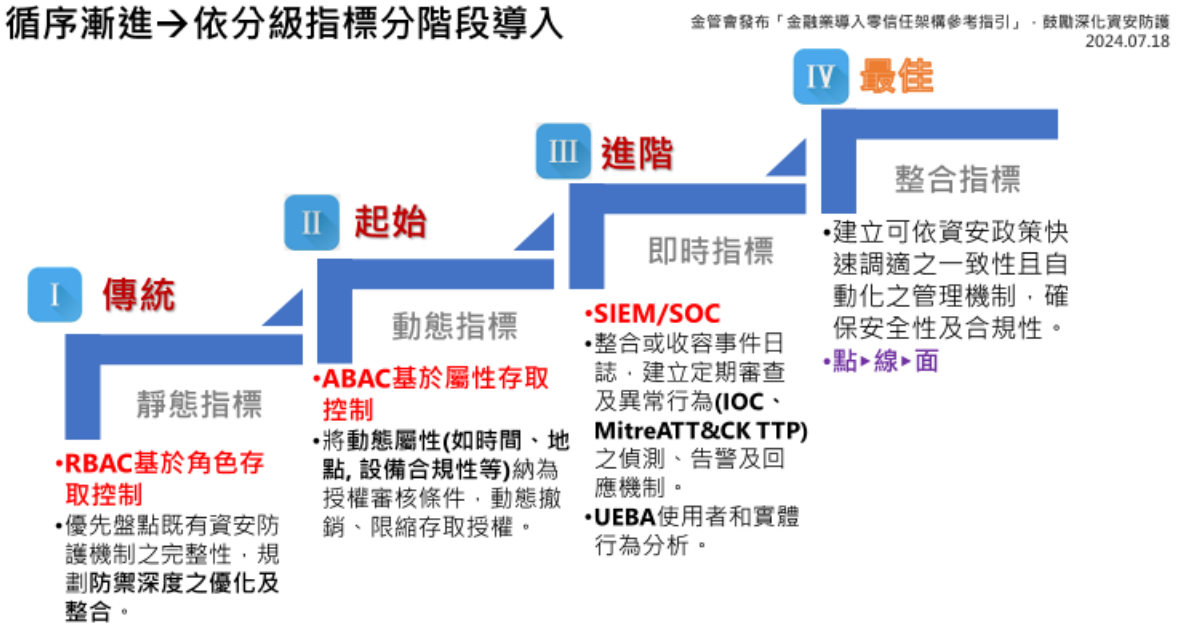
升級策略流程圖



Copyright of Oliver Lien

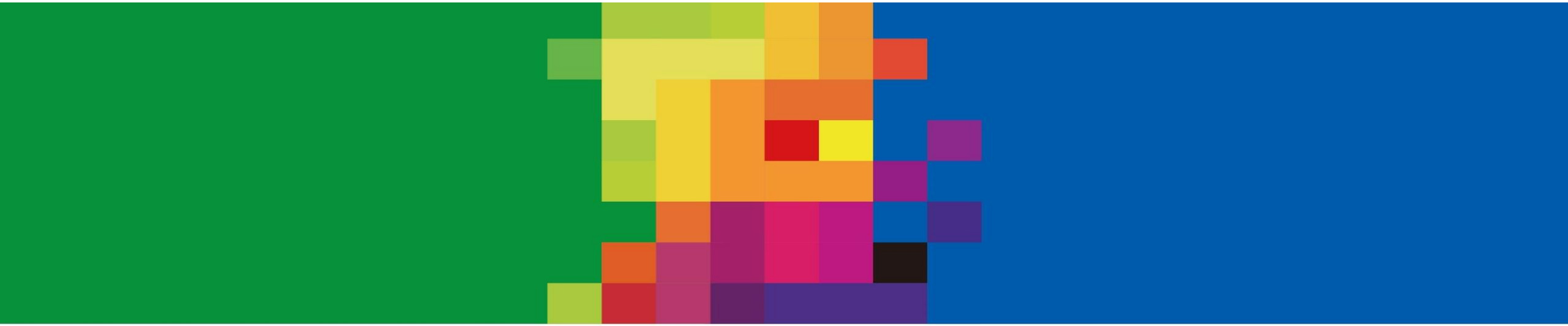
結論與因應

- 零信任落地是一個長期且持續的過程，過程必定需要專業的人員輔助，應尋找具強大服務能力及端點能力支撐的供應商。
- 高層支持，觀念分享，統一規劃，分步實施。



Copyright of Oliver Lien

感謝聆聽



TWCA 臺灣網路認證

TWID 身分識別中心

參考資料

1. **OWASP**
   - ① https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption
   - ② https://mas.owasp.org/MASTG/General/0x04g-Testing-Cryptography/#identifying-insecure-andor-deprecated-cryptographic-algorithms
2. NIST
   - ① NIST SP 800-131A Rev. 2：Transitioning the Use of Cryptographic Algorithms and Key Lengths, https://csrc.nist.gov/pubs/sp/800/131/a/r2/final
   - ② NIST SP 800-57 Part 1 Rev. 5：Recommendation for Key Management: Part 1 – General, https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
3. NIST 2030停用:
   - ① https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm
4. 銀行公會金融XML
   - ① https://fca.hinet.net/download/FUCA_XML_%20v1.2.pdf
5. 電子銀行業務安控作業基準:
   - ① https://www.ba.org.tw/FileDownload/Download?FileId=5ede5db7-e60b-4748-b6cc-bd5bd9d4dbcb&FileName=%E9%99%84%E4%BB%B61_%E9%87%91%E8%9E%8D%E6%A9%9F%E6%A7%8B%E8%BE%A6%E7%90%86%E9%9B%BB%E5%AD%90%E9%8A%80%E8%A1%8C%E6%A5%AD%E5%8B%99%E5%AE%89%E5%85%A8%E6%8E%A7%E7%AE%A1%E4%BD%9C%E6%A5%AD%E5%9F%BA%E6%BA%96.pdf
6. 國家資通安全研究院於資安檢測項目:
   - ① https://download.nics.nat.gov.tw/UploadFile/attachfilehandout/%E8%AD%B0%E9%A1%8C%E4%B8%89%EF%BC%9A112%E5%B9%B4%E7%B6%B2%E8%B7%AF%E6%94%BB%E9%98%B2%E6%BC%94%E7%B7%B4%E6%9A%A8%E8%B3%87%E5%AE%89%E6%AA%A2%E6%B8%AC%E9%87%8D%E8%A6%81%E7%99%BC%E7%8F%BE%E4%BA%8B%E9%A0%85_v0.7_1121030.pdf
7. CA/Browser Forum
   - ① https://cabforum.org/2014/10/16/ballot-118-sha-1-sunset-passed/
   - ② https://www.chromium.org/Home/chromium-security/education/tls/sha-1/
8. 自然人憑證
   - ① https://moica.nat.gov.tw/news_in_144c0560f9c00000a52e.html

Copyright of Oliver Lien

ZTA 的解決方案

ZTA解決方案示例	重點	方法
身份和訪問管理（IAM）	實施多因素身份驗證（MFA）和動態訪問控制	使用身份提供者（IdP）和訪問管理工具來確保每次訪問都經過驗證
設備安全	確保設備的健康狀況和合規性	使用端點檢測和響應（EDR）工具來監控和管理設備
網路分段	將網路劃分為更小的區域，限制攻堅者的橫向移動	使用虛擬局域網（VLAN）和软件定義網路（SDN）技術
資料保護	保護靜態和傳輸中的資料	使用加密技術和資料丟失防證（DLP）工具
應用安全	確保應用程序的安全性和完整性	使用應用程序安全測試（AST）和 Web應用防火牆（WAF）
威脅檢測和響應	實時檢測和智應威脅	使用安全信息和事件管理（SIEM）和安全運營中心（SOC）
荟安全：	保護雲環境中的資源	使用雲訪問安全代理（CASB）和要安全姿態管理（CSPM）
用戶行為分析（UBA）	監控和分析用戶行為以檢測異常活動	使用機械學習和行為分析工具
信任網路訪問（ZINA）	提供安全的遠程訪問	使用 LINA 解決方案來替代傳統的 VPN
動態策略管理	根據實時風險評估動態調整訪問策略	使用策略引擎和自動化工具
供應鏈安全	保護供應鏈中的資料和資源	使用供應鏈風險管理（SCRM）工具
內部威脅防護	檢測和防止內部威脅	使用內部威脅檢測和響應 (ITDR）工具
安全配置管理	確保系統和應用的安全配置	使用配置管理工具和基準檢查
持續監控和審計	持續監控和密計所有活動	使用監控和審計工具
安全事件管理	有效管理和響應安全事件	使用事件管理和響應平台
合規性管理	確保符合相關法規和標準	使用合規性管理工具
安全培訓和意識	提高員工的安全意識和技能	提供定期的安全培訓和模擬演練

資料出處:CIO Taiwan/NIST SP 1800-35

攻擊手法與可監控設備對應（節錄）

與各設備原廠合作，核對、增修可監控設備與方式

項次	ID	攻擊手法	Windows	Linux	AV	FW	IPS	WAF	Router	Switch	網域控制台	DNS	網站應用系統	資料庫系統
1	T1001	Data Obfuscation 資料混淆				V	V							
2	T1003	OS Credential Dumping 作業系統憑證擷取	V	V		V		V						
3	T1005	Data from Local System 本地系統的數據	V					V						
4	T1008	Fallback Channels 備援通道			V	V	V							
5	T1040	Network Sniffing 網路嗅探				V	V		V	V				
6	T1056	Input Capture 輸入擷取			V	V	V	V					V	
7	T1110	Brute Force 暴力破解	V	V		V	V	V	V	V				V
8	T1491	Defacement 網頁篡改				V		V					V	
9	T1498	Network Denial of Service 網路拒絕服務攻擊				V	V	V						
10	T1505	Server Software Component 伺服器軟體元件				V		V					V	

資料出處:金管會金融零信任架構策略思維與實作

Copyright of Oliver Lien