三甲科技
AAA Security Technology

企業IT資安 內部管理整合
AI防禦應用

魏國瑞 Ray
kjwei@aaasec.com.tw

魏國瑞 Ray

- 三甲科技-營運總監
- 逢甲大學資工系 -兼任助理教授
- 專長領域：電子商務安全、資訊安全管理、資安攻防演練、...
- 專業證照：
  - ISC2 Certified Information Systems Security Professional(CISSP)
  - CompTIA Security+ Certified Professional
  - EC-Council Ethical Hacking and Countermeasures(CEH)
  - ISO 27001 ISMS Lead Auditor Course/Auditor
  - IEC62443-2-1 Lead Auditor Course/Auditor
  - Certificate of Cloud Security Knowledge(CCSK)
  - PMI Project Management Professional(PMP)
  - iPAS資訊安全工程師-初級、中級能力鑑定

公司簡介

三甲科技是由一群擁有資訊安全背景的工程師所共同創立，內部工程師皆具備資安相關專業證照。服務團隊經驗相當豐富，主要服務對象擴及學校單位、政府機關、科技產業、房產集團、金融企業和第三方支付產業等機構。

「三甲」取名於「AAA Security」，代表著資訊安全當中的三大面向，認證(Authentication)、授權(Authorization)、紀錄(Accounting)。另外一方面也意味著我們期望：

透過 A級專業 → 提供 A級服務 → 達到 A級安全

資訊安全管理系統驗證 ISO/IEC 27001

TAF測試實驗室認證 ISO/IEC 17025

通過數位發展部數位產業署
資安能量登錄
資通安全自主產品認定
SecPaas 資安整合服務平臺 合作夥伴

核心服務

- ✓ISMS導入/驗證
- ✓資安管理制度導入
- ✓教育訓練服務
- ✓源碼安全檢測服務
- ✓精準資安規劃服務
- ✓其他資安服務
  - 資安顧問服務
  - 紅隊演練服務
  - DDoS攻擊演練服務
  - 攻防演練服務

找出企業
漏洞風險

輔導企業
進行改善

強化資安
防護水準

分享大綱

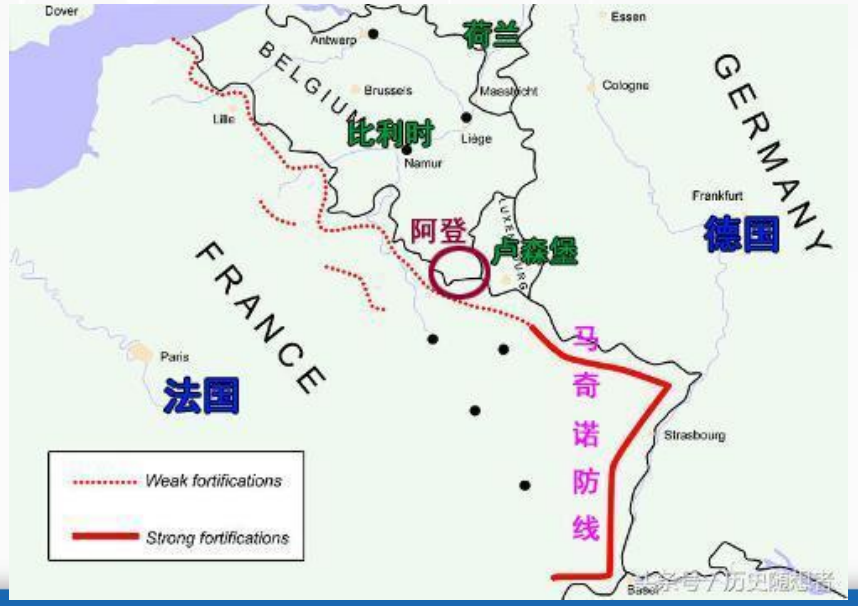
- 從資安威脅看風險
- 從風險到安全政策
- 當企業踏上AI路途

綜觀看資安

其實許多企業單位
非常重視資訊安全

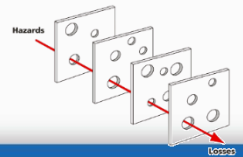
各種築牆計畫不在話下

但...光築牆就夠嗎



從二戰看築牆計畫
號稱完全防禦
馬奇諾防線

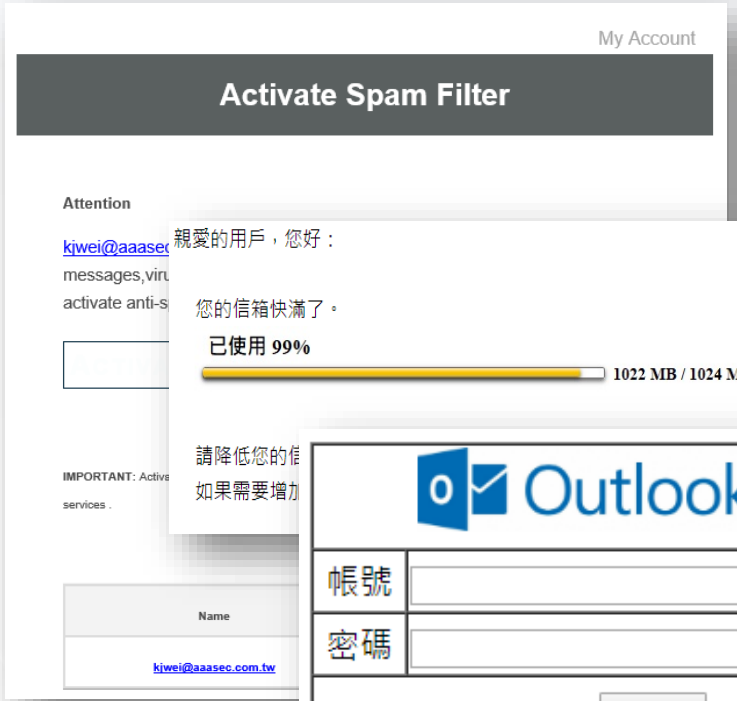
缺乏機動力、疏於練兵
→ **縱深防禦**

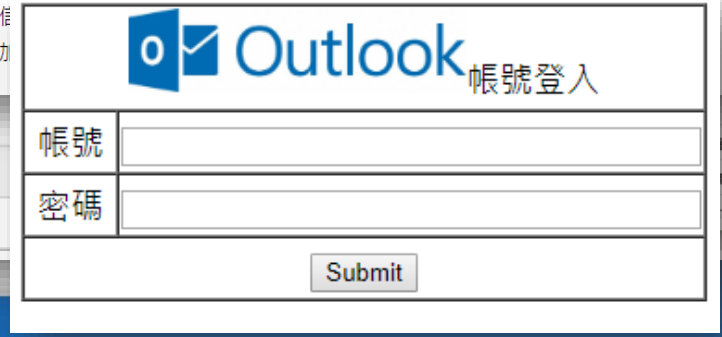


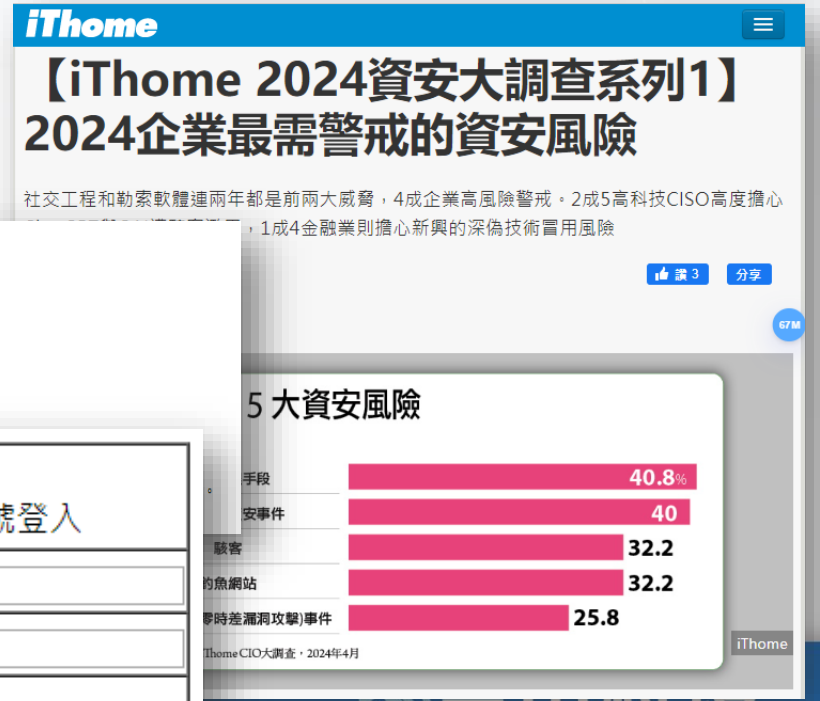
迂迴繞過預防機制

你說企業不會中獎嗎?

- 有沒有聽過**社交工程**?!
  - 簡單來說就是，利用人性弱點，應用簡單的溝通和 欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破資通安全防護，遂行其非法的存取、破壞行為。





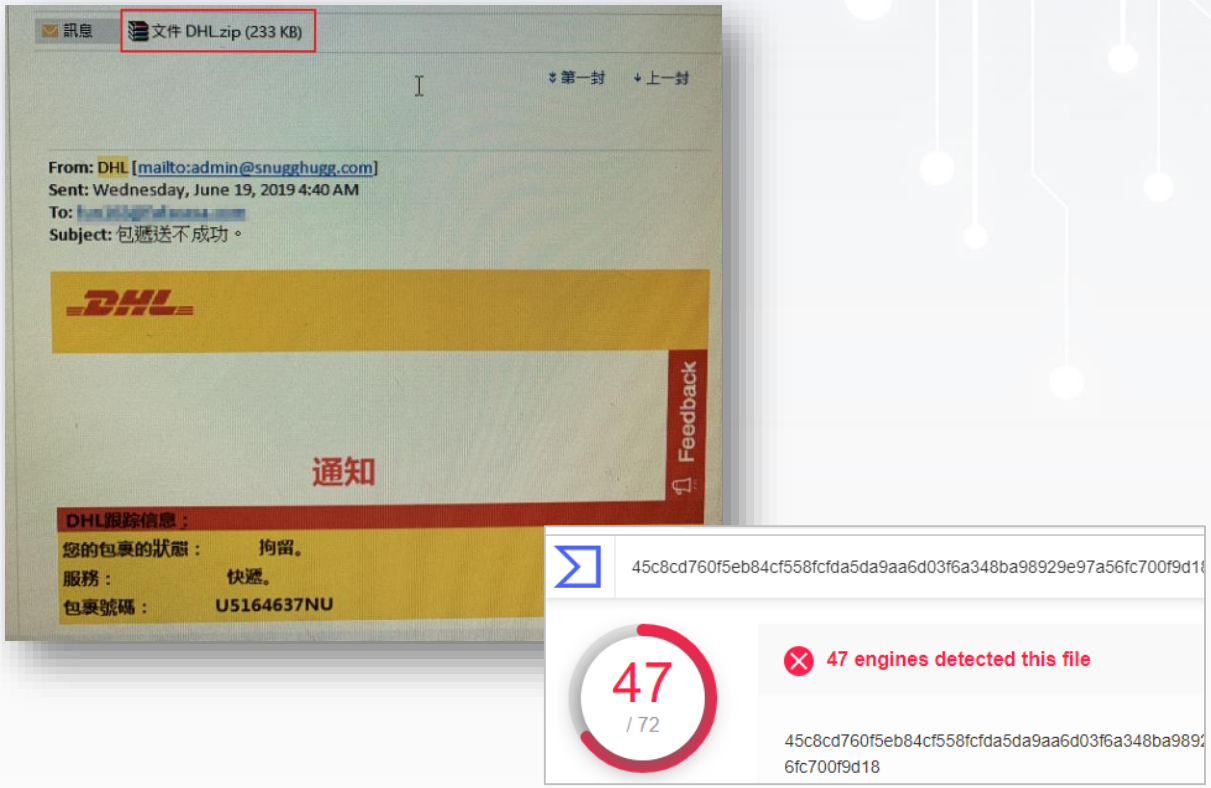


實際案例-勒索軟體

- 檔案陸續加密， 但不知為什麼?
- 發現加密後，網路隔離
  (第一步絕對是止血)
- 諮詢：可疑下載?可疑信件?可以執行?
  (一般感染會有兩個步驟：取得&執行)
- 同仁：無特殊程式安裝，也沒什麼可疑信件。

實際案例-勒索軟體(續)

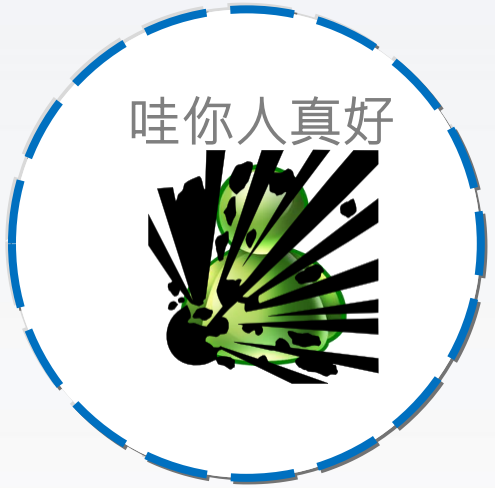
- 附件檔案DHL.zip
- 諮詢：是否開啟過物件？
- 找事件軌跡及可能路徑
  - 重現確認
  - 多軟體檢視執行序...
  - 加密時間、檔案還原
  - 開啟紀錄
- 確認事件路徑
- 經典型，將惡意程式封裝在壓縮檔，逃避防毒軟體偵測
- 啟示：小心可疑信件，預覽也是一種開啟



為什麼要透過社交?

禮物送你

經過適當的偽裝



防火牆、入侵防禦系統

(心理層面)
想要什麼？
需要什麼？

+

(攻擊層面)
想要做什麼？
攻擊手法？

串聯手法包裝

你真的不會中社交?

- **魚叉式攻擊**

  想捕捉特定的魚，會使用特定魚叉進行捕捉

  社交工程的魚叉式攻擊也是一樣道理

這攤鹹酥雞超狂！要吃？至少要等3小時

【有片】這種米好厲害7成都被天龍人買走

沉在水底3年韓船難「世越號」重見天日

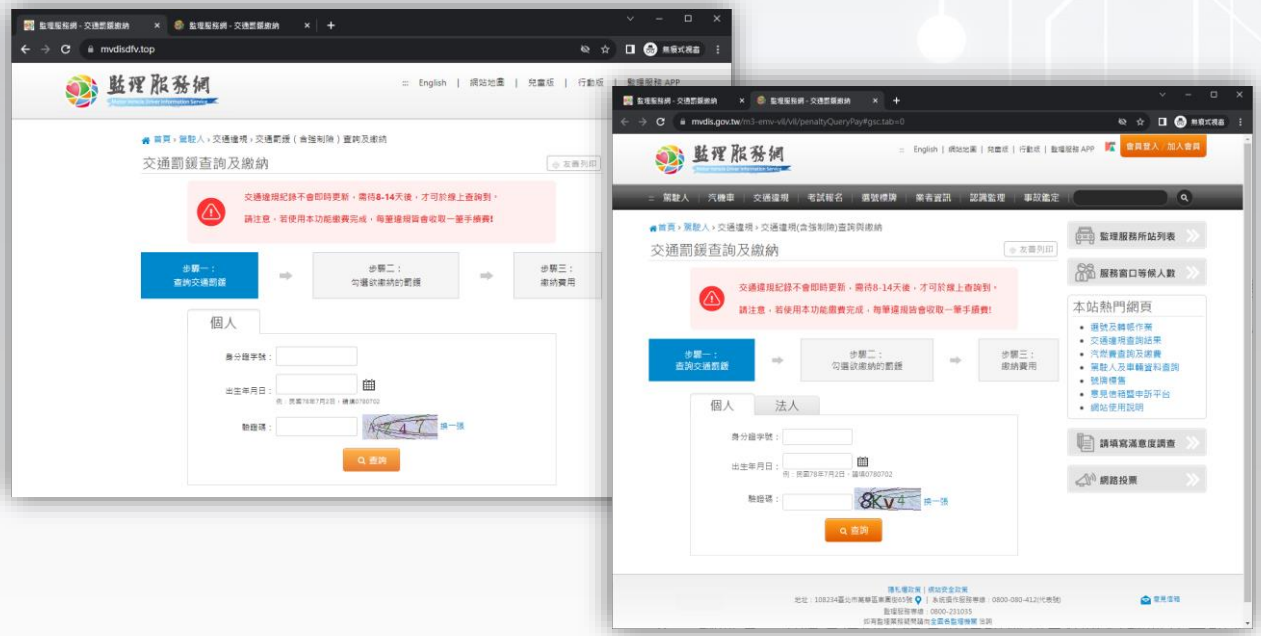
【緊急通知】09/04「企業IT資安內部管理整合AI防禦應用」 **課程延期通知**

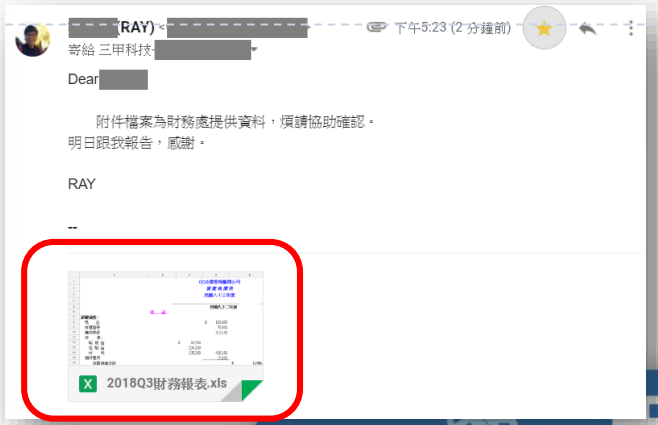
【緊急疏散】今早**台中世貿中心**發生氣爆，死傷數十人...

免費補助資安檢測服務**開始申請**囉！

信中的千百種可能?!

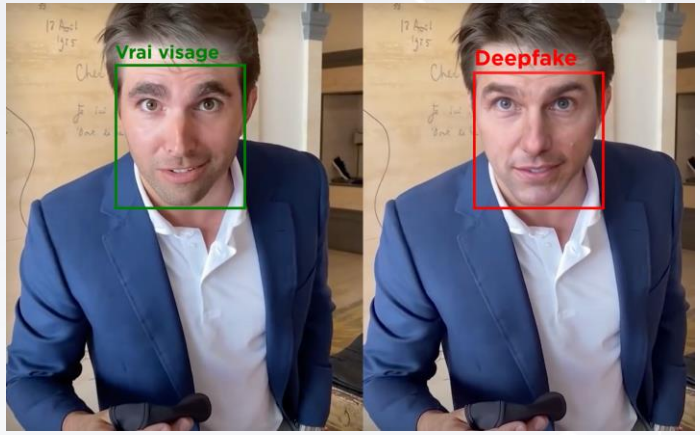
- 依攻擊者喜好！
  - 夾帶惡意連結
    - 釣魚網站
    - 偷你資料
    - 偷你權限
    - 偷你錢
    - 偷你...
  - 夾帶惡意檔案
    - 勒索軟體
    - 惡意程式
    - 入侵企業
    - 埋下後門程式
    - ...

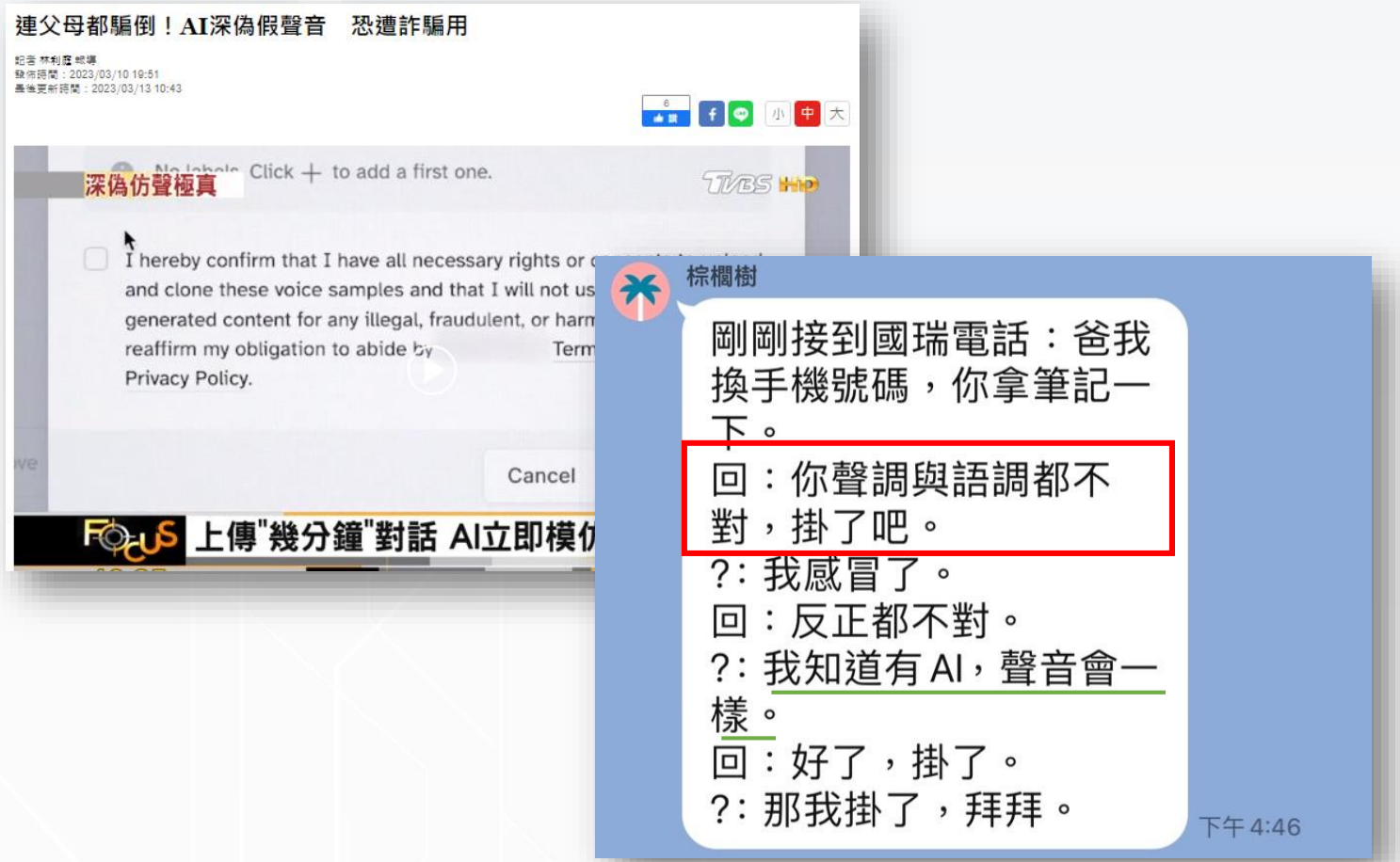


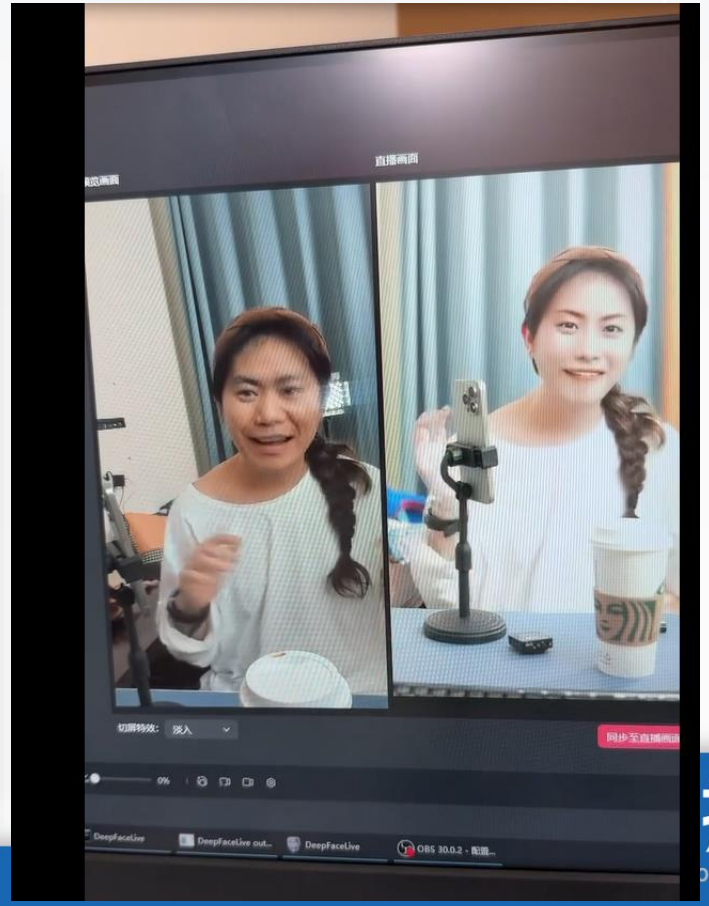


詐騙手法結合現代技術

- DeepVoice、DeepFake



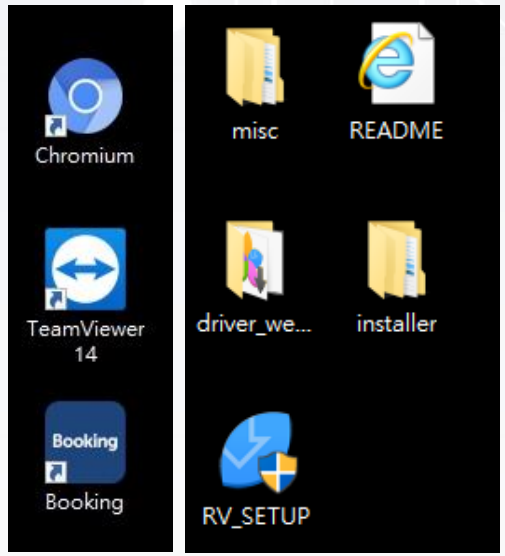


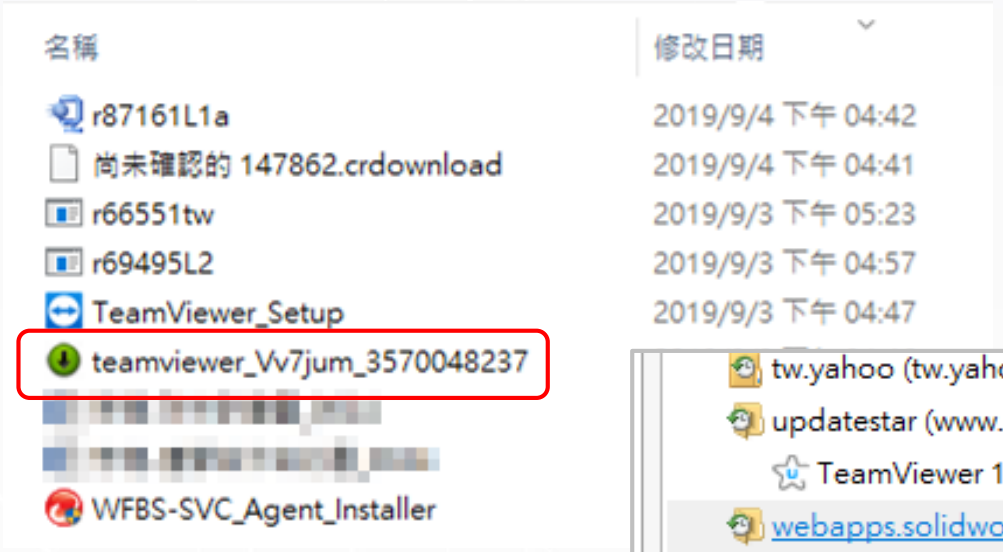


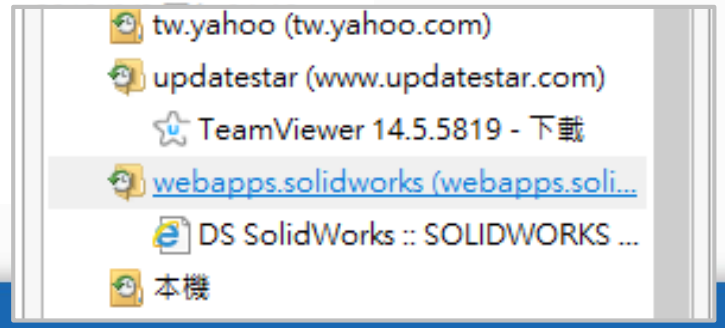
https://news.tvbs.com.tw/focus/2064534

不會有人來騙我們小公司吧?!

- 發現時間
- 檢視近期安裝程式(TeamViewer)
- 確認安裝軟體的取得(官網)
- 檢視下載紀錄與瀏覽紀錄







你說企業不會中獎嗎?

- 有沒有可能企業**還**存在很多弱密碼、預設密碼?!

1	123456
2	123456789
3	Picture1(新進榜)
4	password
5	12345678
6	111111
7	123123
8	12345
9	1234567890
10	Senha(葡語,密码)

11	1234567
12	qwerty
13	abc123
14	Million2
15	000000
16	1234
17	iloveyou
18	aaron431
19	password1
20	qqww1122

不進榜、但也...

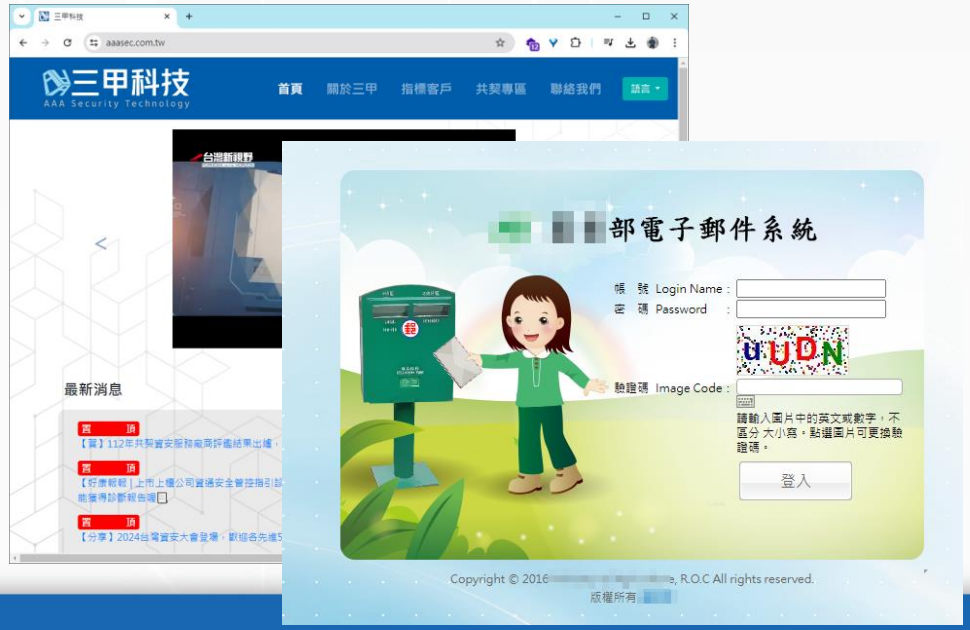
- P@55W0RD
- zaq12wsx
- ZAQ!2wsx
- 統編/電話
- 分機
- Ji32k7au4a83

Google

- admin/admin
- admin/password
- root/root
- monitor/!monitor (HP)
- root/calvin (Dell iDARC)
- admin/dh123456 (監視器)

那...

- 對外服務系統?
  - 官方網站
  - 供應鏈系統
  - 郵件伺服器
  - ...



- 容易被遺忘卻有能力的資產?
  - 網路攝影機
  - 網路印表機
  - 掃地機器人
  - 機聯網設備
  - 碳排測試設備
  - ...

都安全嗎?

沒事都沒事，一有事就...

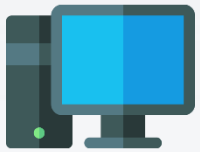
- 沒認知到漏洞被惡意使用?!

- WinRAR 嚴重漏洞，開啟壓縮檔可讓駭侵者遠端執行任意程式碼
- CVE 編號：CVE-2023-40477
- 影響產品：WinRAR 6.23 先前版本。
- 解決方案：立即更新 WinRAR 至 6.23 與後續版本。

演練案例

1. 掃描取得資訊

9. 發現伺服器
主機弱點



10. 成功使用
Microsoft弱點
控制伺服器

額外目標
取得主機控制權

8. 使用其內員工信箱，
設計偽裝的系統警告信

額外目標
使用員工信箱資
訊進行社交工程

2. 不需密碼
存取之資訊

6. 發現網站

7. **SQL injection**
取得資料庫中資訊

主要目標
取得機敏資料

3. **發現敏感**
網段相關資訊

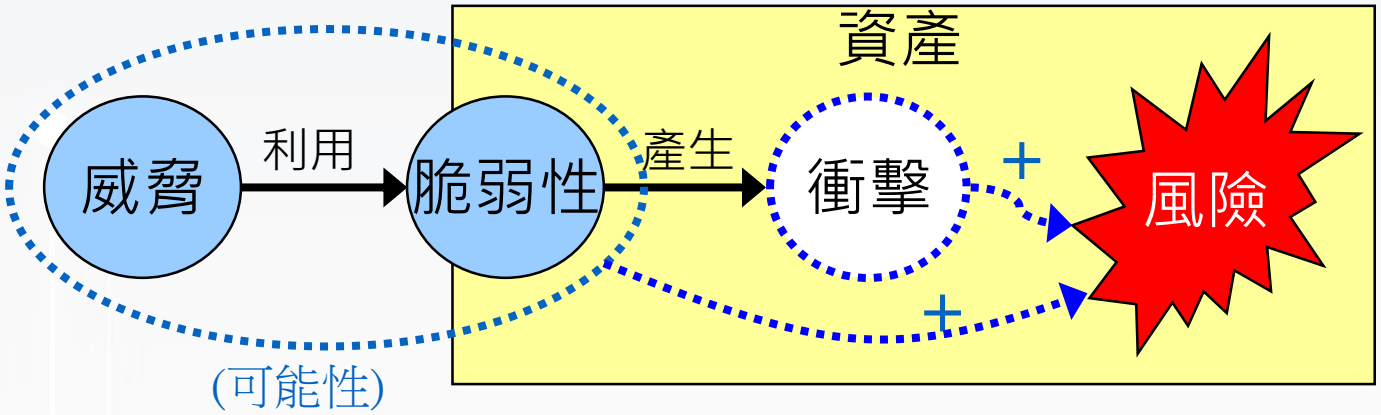
4. 於網段
發現網域控制站

5. 於共享資料夾發現**產品規格書、工作進度報告、敏感往來信件、產品報價單與客戶資訊**

主要目標
取得機敏資料

風險

- 「風險」是指「威脅」利用其相對應「脆弱性」造成企業資訊資產受到「衝擊」的「可能性」

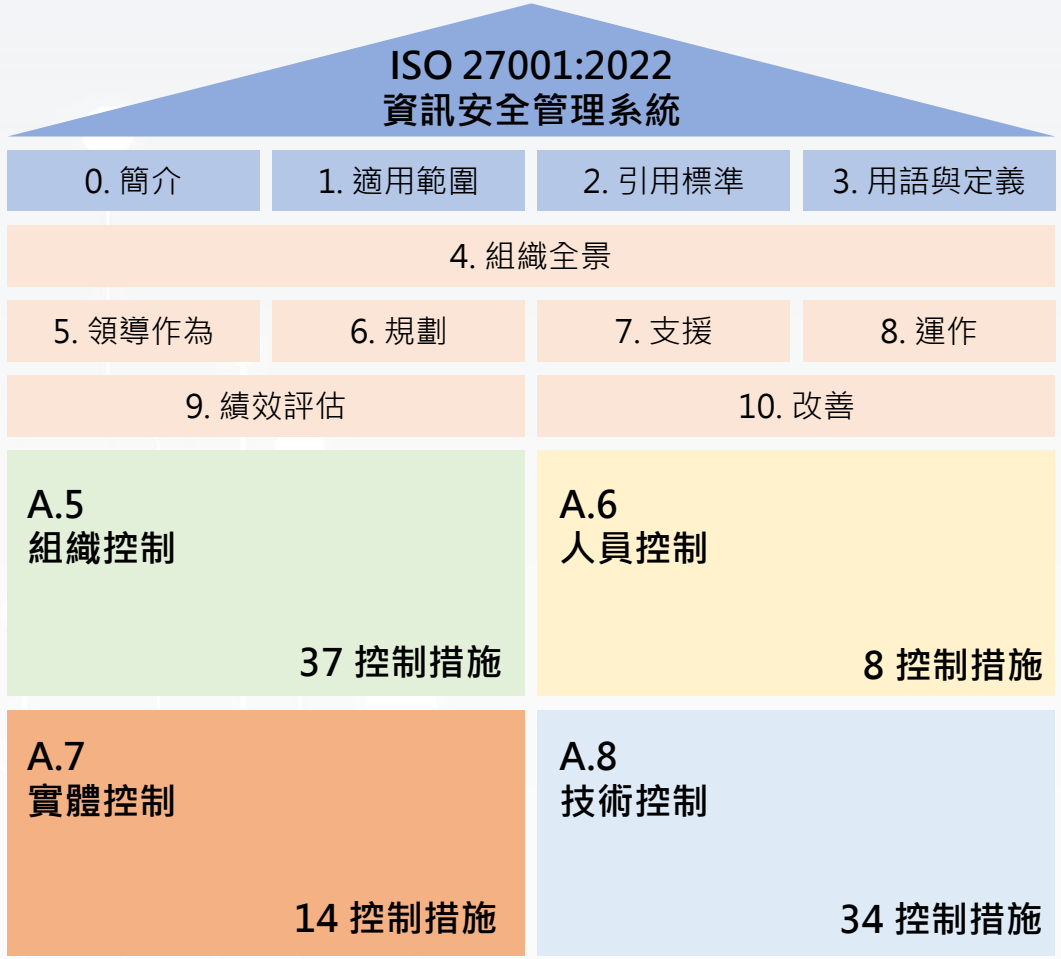


- 風險透過「衝擊」與其「可能性」兩個因素的結合來定義其影響程度或損害程度
- 風險管理的目標：最低的防護成本投入下獲得最優化的安全性(最優化非最強固，而是最合適)

安全政策制定

三甲科技
AAA Security Technology

熟悉的ISO/IEC 27001



4 Domians ; 93 Controls

營運安全

A5.30 營運持續之資通訊準備

資料安全

A8.10 資訊刪除
A8.11 資料遮罩
A8.12 防範資料外洩

雲安全

A5.23 雲服務之資訊安全

資訊安全

A5.7 威脅情報
A7.4 實體安全監控
A8.9 組態管理
A8.16 活動監控
A8.23 網頁安全防護
A8.28 程式開發安全

ISMS 資訊安全政策

外部法規

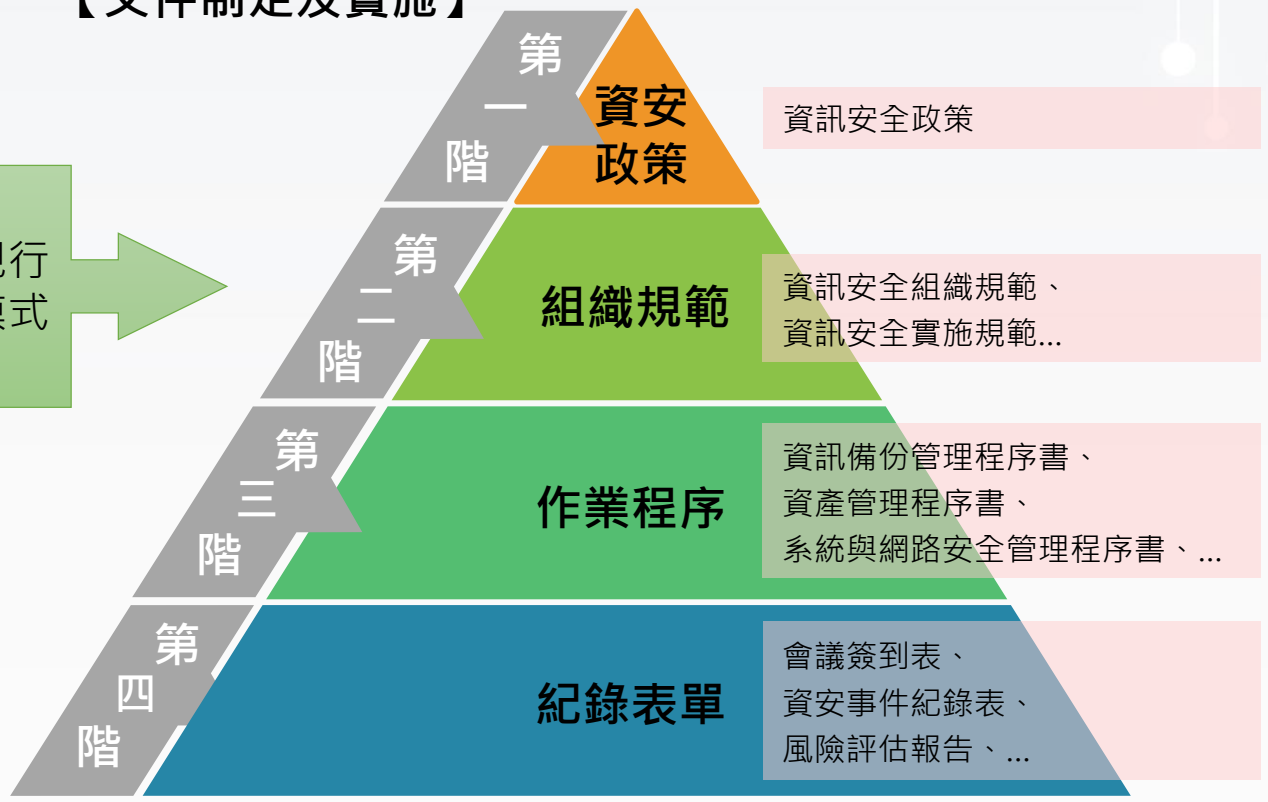
- 相關法令及法規
- ISO 27001:2022
- 個人資料保護法

內部文件

- 風險評鑑報告
- 現有文件及表單
- 相關作業流程

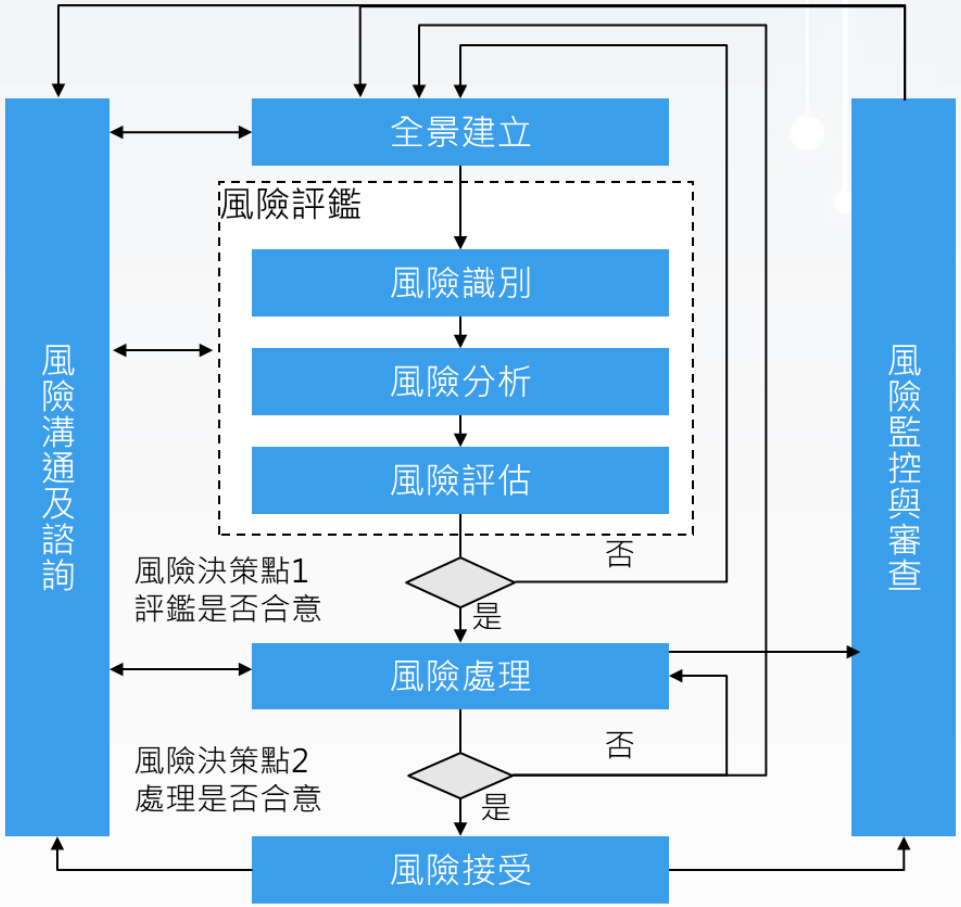
整合現行作業模式

【文件制定及實施】



風險管理


範圍、全景及準則
風險評鑑
風險識別
風險分析
風險評估
風險處理
記錄與報告
溝通及諮詢
監視與審查

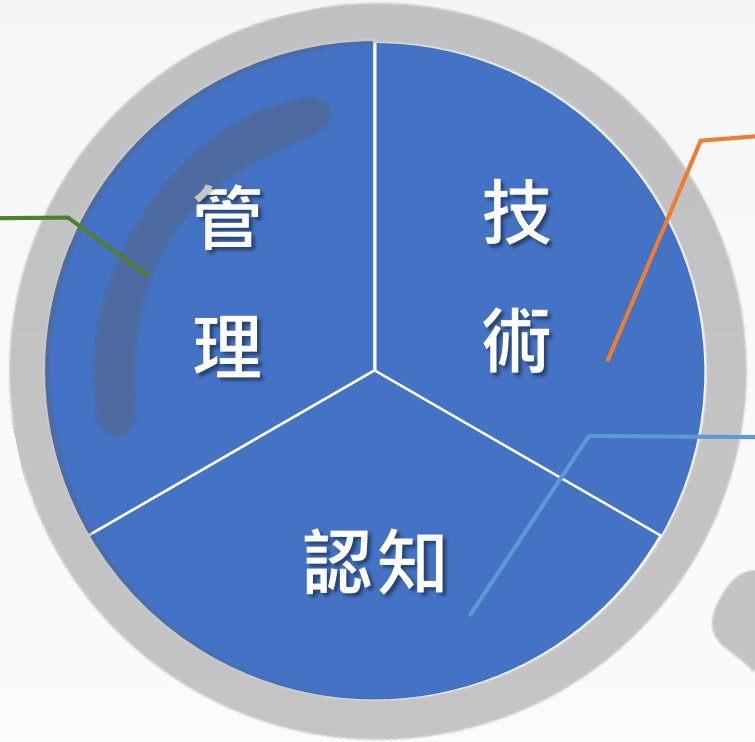

全景建立
風險評鑑
風險識別
風險分析
風險評估
風險決策點1
評鑑是否合意
否
是
風險處理
風險決策點2
處理是否合意
否
是
風險接受
風險溝通及諮詢
風險監控與審查

殘餘風險

觀察資安怎麼做?

從「**資通安全管理法**」看資安

- ISMS輔導
- 持續運作演練
- 內部稽核輔導



- 網站安全弱點檢測
- 系統滲透測試
- 資通安全健診
- …

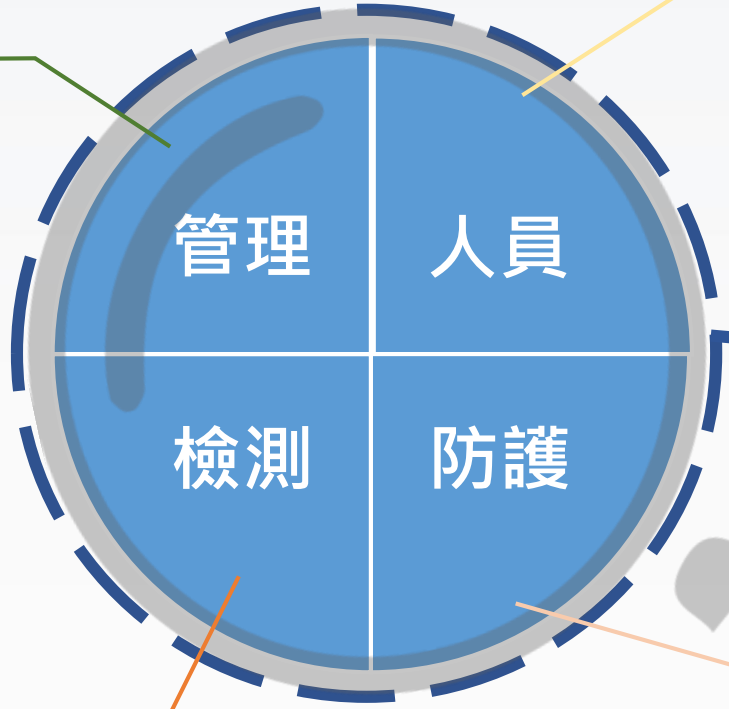
- 資通安全教育訓練[一般、資訊]
- …

事前防護 事中應變 事後復原

觀察資安怎麼做?

從「上市上櫃公司資通安全管控指引」看資安

- 資訊資產盤點
- 風險評估
- 資訊安全管理制度



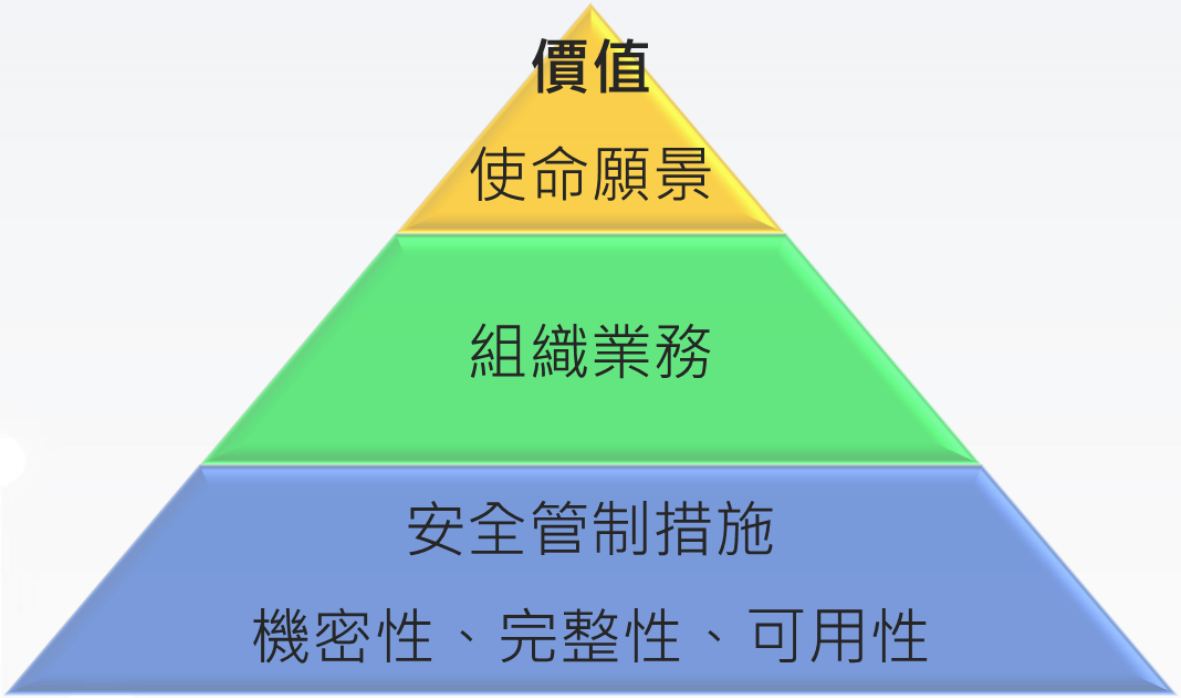
- 郵件社交工程演練
- 資通安全教育訓練
- 加入情資分享組織

- **精準資安規劃服務**

- 須具備資安防護措施
- 依需求區隔網段

- 核心系統弱點掃描
- 核心系統滲透測試
- 系統上線前源碼掃描

資訊安全?



透過安全管制措施，
保護資產免於受到危害，
以達到C、I、A的目標，
進而支持組織業務，創造價值、
實現組織的使命與願景

-資安專家 Wentz Wu

- 無論各個行業都需要資安(數位轉型、ESG、AI導入)
- 抓住**企業核心**、**盤點命脈**

資安，我們該怎麼做

- 透過**現況盤點**了解須要做什麼？

  盤點組織資訊資產/威脅，了解組織**資訊命脈**，更有效益規劃

- 配合**企業目標**與期望調整

  挖掘**企業痛點**與期望短中長程**改善目標**

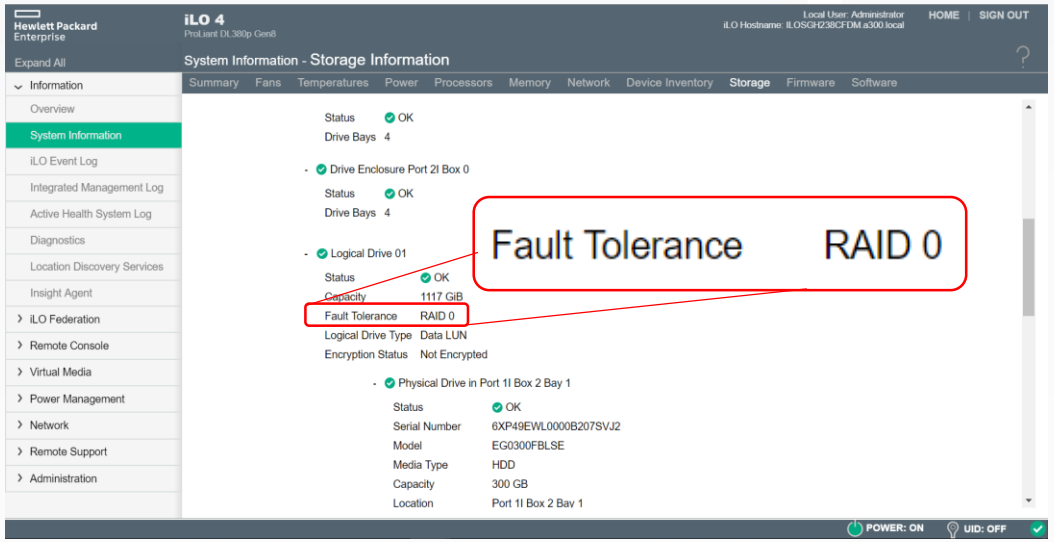
- 因應**防護需求**作好準備

  透過基礎防護、安全存取、管理制度，建立有效控管

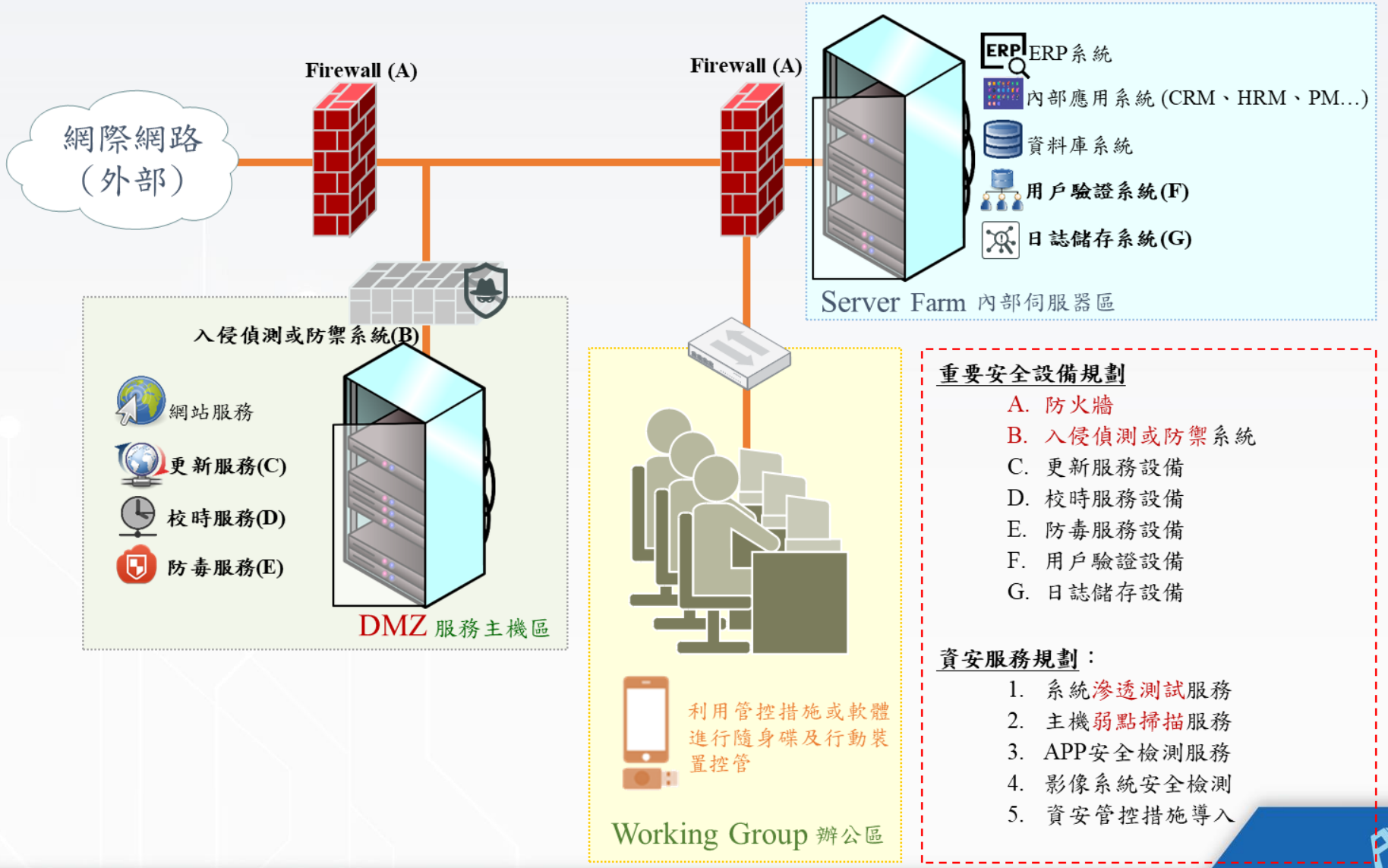
從了解做起

實務案例分享

- 案例背景：企業導入智慧化卓有成效，資訊主責 MIS*1，以需求導向
- 初步盤點了解狀況，逐步改變
  - 內網大通透、訪客區即可全看透
  - 核心伺服器潛在問題未發現
  - 事件即搶救、無備援機制
  - 同仁無資安意識概念
  - 系統管理較無文件化(網路拓樸圖)
  - 設備掌握度低、系統穩定性不佳
  - 高階設備執行低階工(防護設定)



從基礎鞏固



重要安全設備規劃

A. 防火牆
B. 入侵偵測或防禦系統
C. 更新服務設備
D. 校時服務設備
E. 防毒服務設備
F. 用戶驗證設備
G. 日誌儲存設備

資安服務規劃：

1. 系統滲透測試服務
2. 主機弱點掃描服務
3. APP安全檢測服務
4. 影像系統安全檢測
5. 資安管控措施導入

萬一的萬一，反思一下

- 如果被攻擊了，我們能偵測到嗎? → 偵測機制、...
- 如果偵測到了，我們能即時阻擋嗎? → 阻擋機制、...
- 如果阻擋失敗，我們能怎樣快速救援嗎? → 備援機制、...
- 如果資料遺失，我們能怎樣復原回來? →備份機制、還原機制
- 如果有阻擋了，看到相關紀錄軌跡嗎? → 日誌機制、...
- 如果有軌跡了，我們能探查發生經過嗎? → 調查機制、...
- 如果知道過程，我們能找出根因、能解決嗎?
- 如果...

我們不是要最強，而是要能對抗制衡

-常常問題處理成本，遠高於前置防禦-

萬一不幸

備份與還原

- 檢視內部重要服務之備份還原機制是否具有紀錄或是實際演練，當災難發生時才能減少復原時間。
  - ERP：異地備份、還原演練
  - 資料庫：除了異機備份還有離線備份
  - 網路儲存裝置(NAS)：有做同步備份
  - OT設備：透過無線網路進行連結以達到智慧監控
  - OT監控資訊：異機備份

如果是資料外洩？

自我檢視 - 政策規則對應

- 美國國家標準技術研究院(NIST)
- 網路安全框架 v2.0 (Cybersecurity Framework v2.0, CSF v2.0)

功能	治理(GOVEM)	
類別	● 組織全景 ● 風險管理策略 ● 角色、職責與權限	● 政策 ● 監督 ● 網路安全供應鏈風險管理

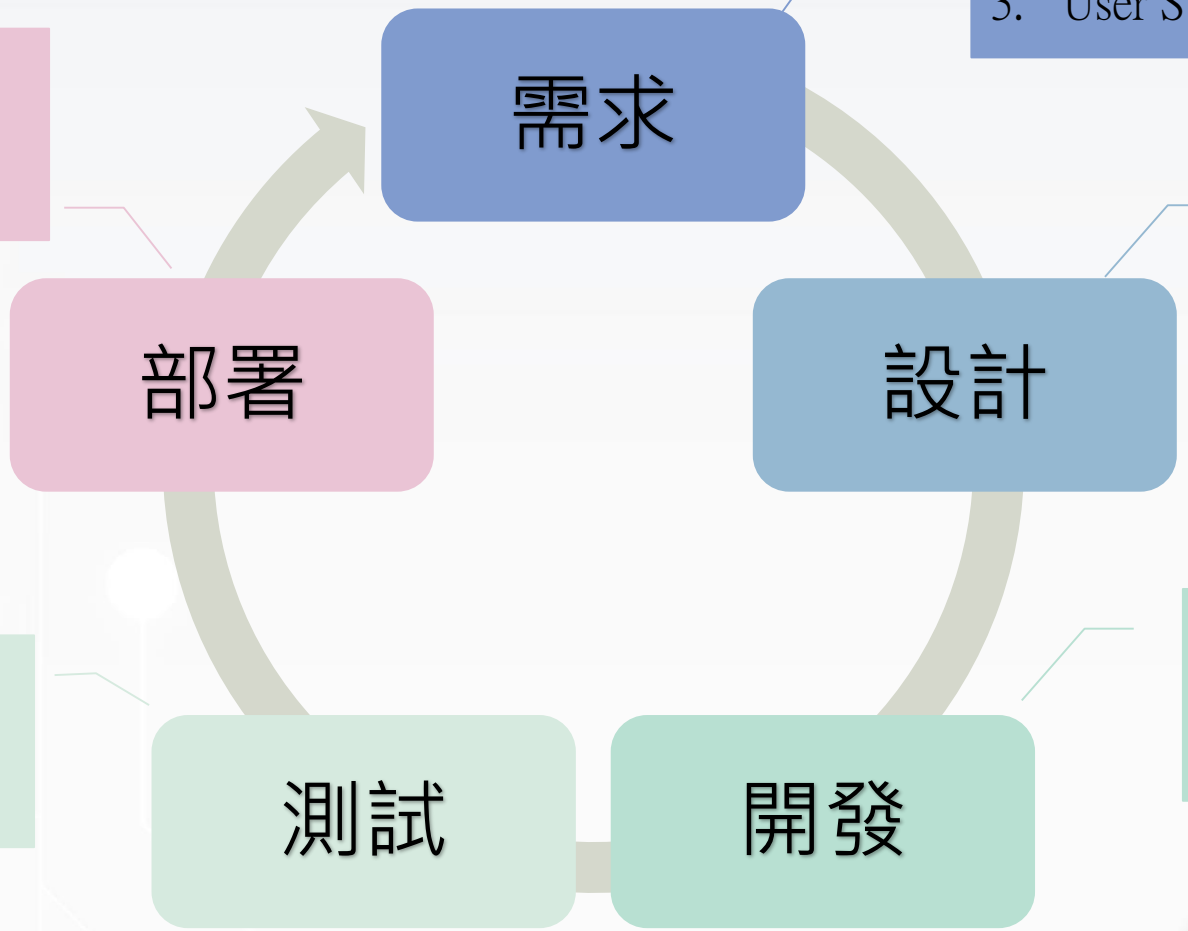
功能	辨識 (IDENTIFY)	保護 (PROTECT)	偵測 (DETECT)	應變 (RESPOND)	復原 (RECOVER)
類別	● 資產管理 ● 風險評鑑 ● 改善	● **身分管理、驗證及存取控制** ● 認知與訓練 ● 資料安全 ● 平台安全技術架構韌性	● 持續監控 ● 不良事件分析	● 事故管理 ● 事故分析 ● 事故應變報告與溝通 ● 事故減緩	● 事故復原計畫執行 ● 事故復原溝通

以開發為例

三甲科技
AAA Security Technology

以企業開發 - 軟體開發生命週期

- System Development Life Cycle



1. 需求訪談
2. RFP
3. User Story

1. 軟體架構設計
2. 資料庫設計
3. …

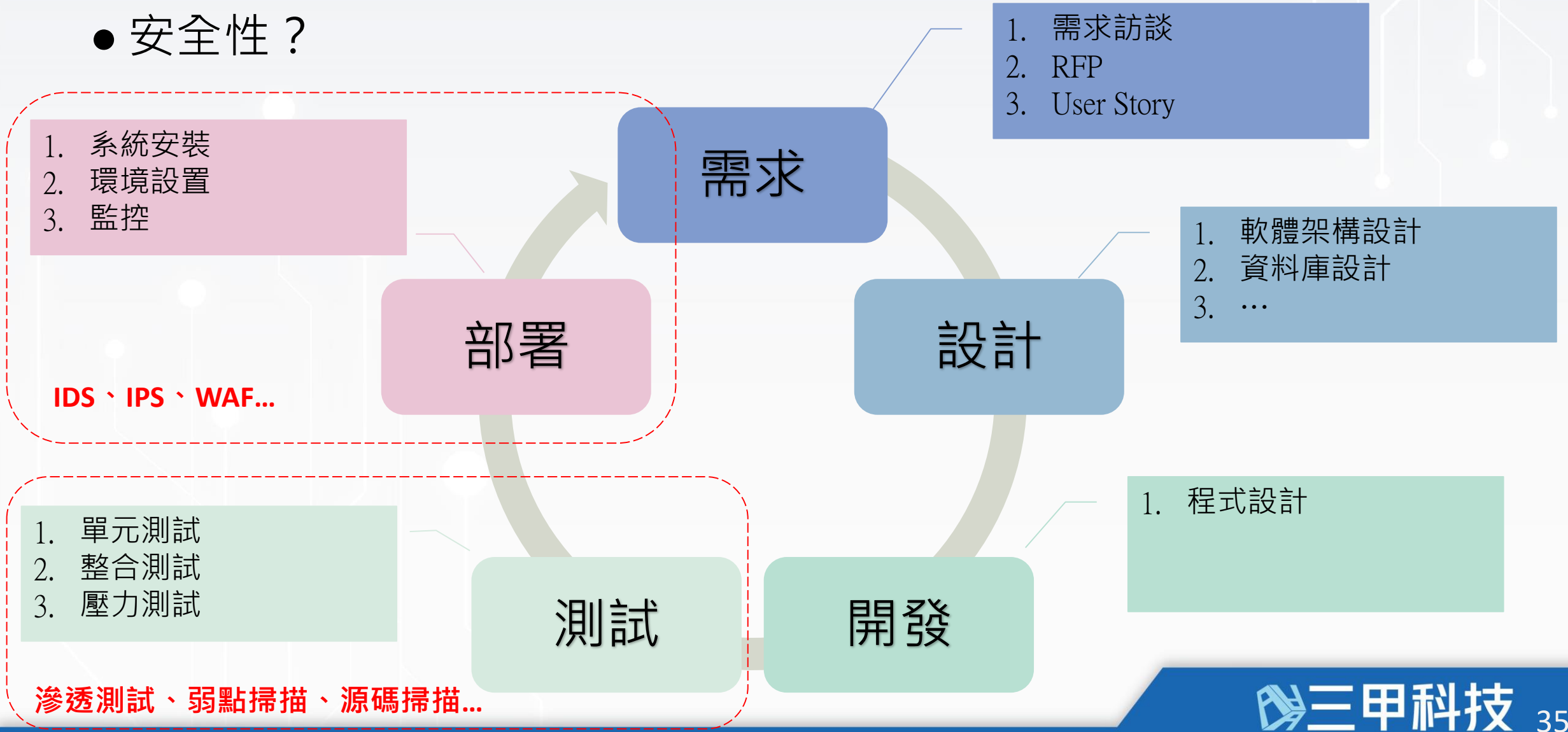
1. 程式設計
2. 修正實作
3. …

1. 單元測試
2. 整合測試
3. 壓力測試

1. 系統安裝
2. 環境設置
3. 監控

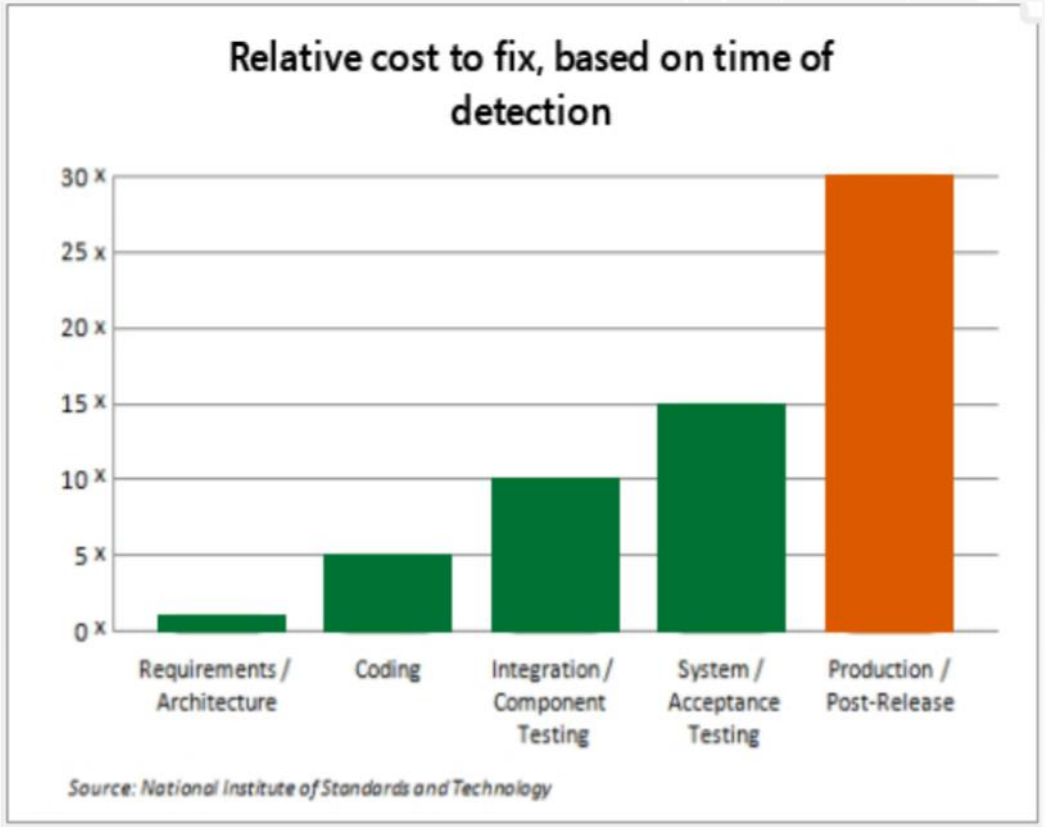
軟體開發生命週期

- 安全性？



軟體開發生命週期

- 若程式設計不當時，測試階段可能找出什麼弱點？
  - SQL Injection
  - 密碼可能使用明文儲存
  - 登入機制於前端驗證而非後端
  - 水平/垂直越權
- 要修復測試階段找出的弱點可能會...
  - 延宕上線時間
  - 核心架構異動
  - 修復成本高 (時間、難度)

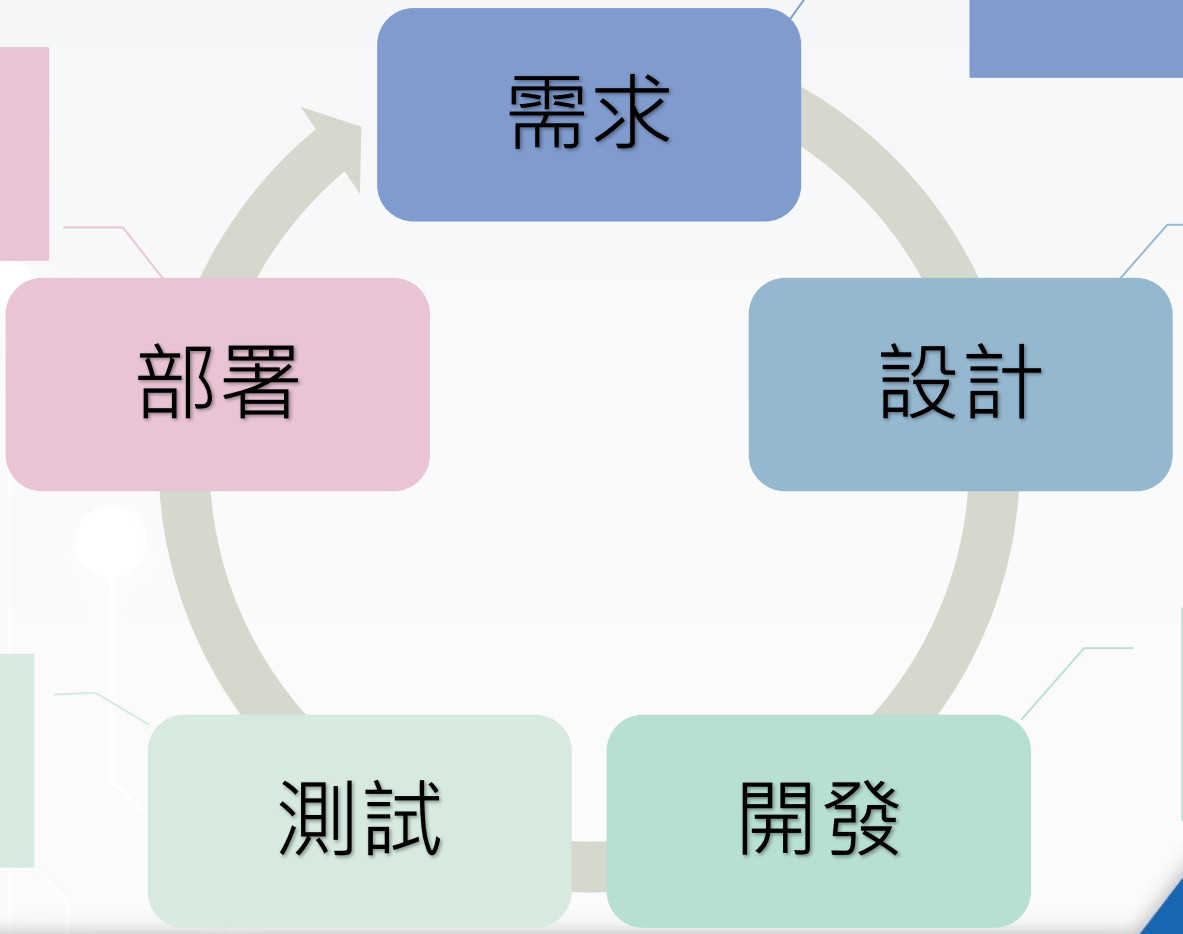


反思一下

- 傳統軟體開發之特性
  - 功能性導向，在最短的時間，完成系統的開發與上線
  - 缺乏安全性考量的設計，面對日新月異的攻擊手法，難以建立有效的防護方法保護系統的安全，例如:資料隱碼攻擊(SQL Injection)等便是因此而崛起
  - 實務上，問題修正??
- 資安左移
  - （Shift Left Security）是一種在軟體開發生命周期中將安全性考量提前到更早階段的策略。
  - 將安全性工作提前到開發初期，甚至是需求分析和設計階段，雖開發時程長，但可以更早地發現並解決潛在的安全問題，從而減少修復成本並提高整體的軟體安全性。

安全軟體開發生命週期

- 何不一開始就考量資安？
  - Secure SDLC



1. 安全分級
2. 安全性需求

1. 威脅建模
2. 威脅風險評估
3. 架構風險分析

1. Secure Code Review
2. 源碼掃描
3. Source SBOM

1. 弱點掃描
2. 滲透測試
3. 安全性需求驗證

1. 組態管理
2. 安全存取控管
3. SBOM建立與查驗

踏上AI路途

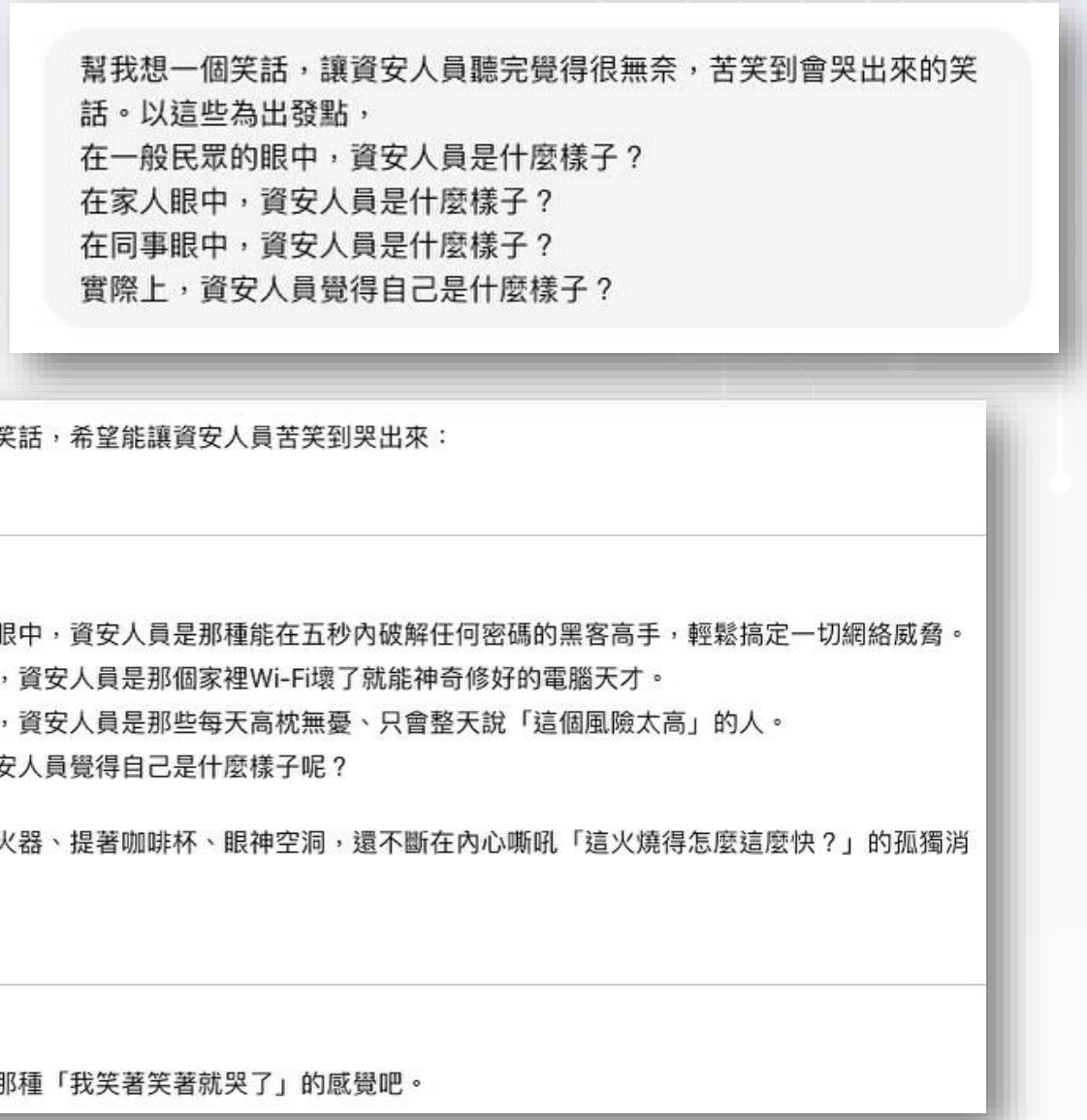
三甲科技
AAA Security Technology

當你踏上AI路途...

- 你用AI來幹嘛?
- AI使用提升工作效率計畫書?

【AI應用】

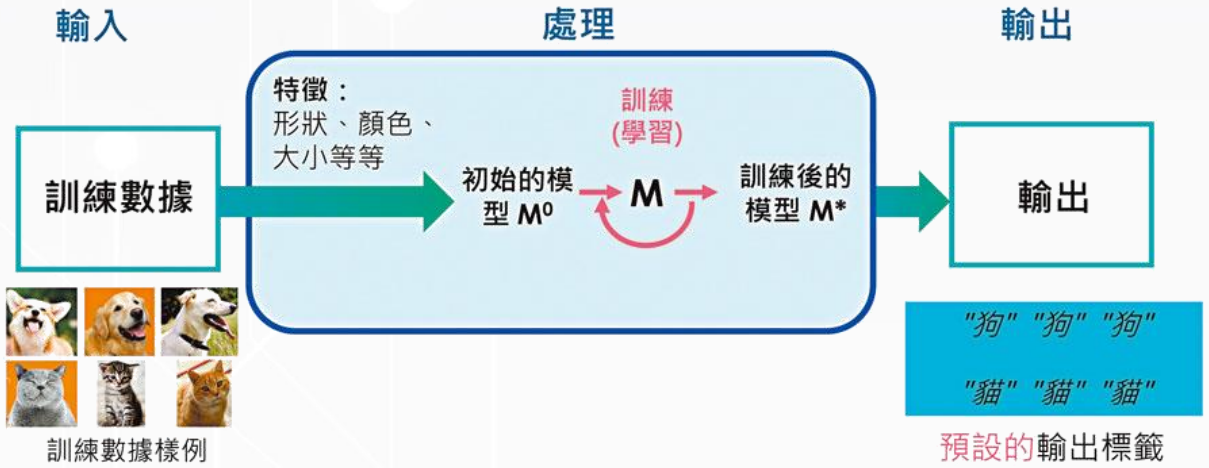
- 會議記錄、語音錄音自動紀錄
- 程式解題協助開發
- 資料彙整
- 自動寫信
- ~~聽笑話~~



圖片來源：資安同好者

當你踏上AI的路上...

優 與 憂



圖片來源:香港文匯報 百科啟智

【訓練模組】

- 訓練模組來源
- 訓練模組限制

AI 風險管理

導入AI之前，應該先建立AI風險管理，避免AI帶來負面影響

相關資料：

- 行政院及所屬機 關（構）使用生成式 AI 參考指引
- 政府**預告**制定「人工智慧基本法」草案
- 金融業運用人工智慧(AI)指引
- ...

治理及問責機制

系統穩健性與安全性

人為可控性

透明性與可解釋性

資料保護

永續發展

行政院及所屬機 關（ 構 ）使用生成式 AI 參考指引

行政院及所屬機關（構）使用生成式 AI 參考指引

近年來生成式 AI 快速發展，影響遍及全球產官學研各界。其中 ChatGPT 於 2022 年底發布後，更掀起全球熱潮，且功能極為多元，已被視為人工智慧之一項重大突破。參考歐盟之定義，生成式 AI 模型是一種電腦程式，旨在創建類似於人類製作（human-made）之新內容；其大量蒐集、學習與產出之資料，可能涉及智慧財產權、人權或業務機密之侵害，且其生成結果，因受限於所學習資料之品質與數量，有可能真偽難辨或創造不存在之資訊，須客觀且專業評估其產出資訊與風險。

考量行政院及所屬機關（構）（以下簡稱各機關）利用生成式 AI 協助執行業務或提供服務，有助於行政效率之提升，且為保持執行公務之機密性及專業性，並促使各機關使用生成式 AI 有一致之認知及基本原則，爰參考各國政府之審慎因應作法，研訂「行政院及所屬機關（構）使用生成式 AI 參考指引」（以下簡稱本參考指引），供各機關依循。各機關得視使用生成式 AI 之業務需求，參酌本參考指引另訂使用規範或內控管理措施。

衡酌 AI 發展具重要性且與資訊安全及國家安全息息相關，本參考指引明確揭示各機關人員使用生成式 AI 時，應秉持負責任及可信賴之態度，掌握自主權與控制權，並秉持安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊。因 AI 之發展日新月異，後續將觀察全球 AI 發展趨勢與因應作為，及各機關於人工智慧應用之推動情形，持續滾動修正本參考指引。

本參考指引共計十點如下：

一、為使行政院及所屬機關（構）（以下簡稱各機關）使用生成式 AI 提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式 AI 應注意之事項，訂定本參考指引。

二、生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

三、製作機密文書應由業務承辦人親自撰寫，禁止使用生成式 AI。

前項所稱機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。

四、業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式 AI 模型，於確認系統環境安全性後，得依文書或資訊機密等級分級使用。

五、各機關不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據。

六、各機關使用生成式 AI 作為執行業務或提供服務輔助工具時，應適當揭露。

七、使用生成式 AI 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施。

八、各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各機關依前點所訂定之規範或內控管理措施。

九、公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式 AI，得準用本參考指引。

十、行政院及所屬機關（構）以外之機關得參照本參考指引，訂定使用生成式 AI 之規範。

政府預告制定「人工智慧基本法」草案

力，爰擬具「人工智慧基本法」草案，其要點如下：

一、本法之制定目的。（草案第一條）

二、人工智慧定義。（草案第二條）

三、人工智慧研究發展及應用之基本原則。（草案第三條）

四、政府應推動人工智慧研究發展與應用。（草案第四條）

五、政府應完善法規調適。（草案第五條）

六、政府應建立或完備人工智慧創新實驗環境。（草案第六條）

七、政府應推動人工智慧公私協力與國際合作。（草案第七條）

八、政府應推動人工智慧人才培育與素養教育。（草案第八條）

九、政府應評估驗證人工智慧防止違法應用。（草案第九條）

十、政府應推動人工智慧風險分級規範。（草案第十條）

十一、政府應強化人工智慧人為可控性（草案第十一條）

十二、政府應建立人工智慧應用負責機制。（草案第十二條）

十三、政府應保障勞工權益。（草案第十三條）

十四、政府應保障個資隱私。（草案第十四條）

十五、政府應提升資料利用性與國家文化價值。（草案第十五條）

十六、政府公務使用人工智慧之原則。（草案第十六條）

十七、政府應檢討主管法規。（草案第十七條）

十八、本法施行日。（草案第十八條）

條文	說明
第一條 為促進以人為本之人工智慧研發與應用，維護國民生命、身體、健康、安全及權利，提升國民生活福祉、維護國家文化價值及國家競爭力，增進社會國家之永續發展，特制定本法。	一、本法之立法目的。 二、人工智慧為攸關國家發展之戰略性科技，為積極發展與應用人工智慧，強化與深耕以人為本之人工智慧技術，促進技術應用與產業發展，同時維護人民安全、國家安全及保障人民權利，以期人工智慧可回應人文與社會發展所需，邁向社會永續發展。因此，發展與應用人工智慧之同時，有賴於制定具有指標與引導性原則之立法，以作為發展人工智慧之規範與促進應用之法源基礎。
第二條 本法所稱人工智慧，係指以機器為基礎之系統，該系統具自主運行能力，透過輸入或感測，經由機器學習與演算法，可為明確或隱含之目標實現預測、內容、建議或決策等影響實體或虛擬環境之產出。	參考美國國家人工智慧創新法案（National AI Initiative Act of 二〇二〇）美國法典(U.S. Code)第九四〇一章、國際標準化組織（ISO）及國際電工委員會（IEC）聯合制定技術規範(ISO/IEC)四二〇〇一：二〇二三人工智慧管理系統、美國國家標準暨技術研究院(National Institute of Standards

金融業運用人工智慧(AI)指

總則章　共通事項

一、人工智慧(AI)相關定義[2]

(一)AI 系統定義：係指透過大量資料學習，利用機器學習或相關建立模型之演算法，進行感知、預測、決策、規劃、推理、溝通等模仿人類學習、思考及反應模式之系統。

(二)生成式 AI 定義：係指可以生成模擬人類智慧創造之內容的相關 AI 系統，其內容形式包括但不限於文章、圖像、音訊、影片及程式碼等。

二、AI 系統生命週期

AI 系統的生命週期主要包括以下 4 個階段：

(一)系統規劃及設計：設定明確的系統目標及需求。

(二)資料蒐集及輸入：資料蒐集、處理並輸入資料庫之階段。

(三)模型建立及驗證：選擇與建立模型演算法及訓練模型，並對模型進行驗證以確保模型效能、安全性與機密性。

(四)系統部署及監控：將系統應用於實際環境中，且關注模型是否已完備，並持續監控以確認系統所帶來之潛在影響。

金融機構運用 AI 系統，可能為自行研發[3]並使用，因此包含上述 4 階段。金融機構亦可能委託第三方業者研發或購入 AI 系統後，再部署該系統並監控，因此金融機構不盡然均會經歷上開 4 階段。金融機構運用 AI 系統時宜辨識 4 個階段中可自行監控風險之程度，並得對自身較無控制權的部分或事項，透過契約或其他方式與合作廠商明訂風險監控責任之分工。為簡化文字，本指引以「導入(introduce)」AI，表示前述(一)、(二)及(三) 3 階段，以「使用(use)」AI 表達第(四)階段。至本指引之「運用(apply)」AI 則係整體性概念，包含上述 4 階段。

三、風險評估考量因素

金融機構運用 AI 系統時，宜就個別使用情境所涉相關風險進行評估，

[2] 人工智慧相關定義參考自銀行公會「金融機構運用人工智慧技術作業規範」。

[3] 自行研發除包含金融機構完全獨立開發外，亦包含與其他金融機構共同合作、聯合開發 AI 系統，以及以市場上既有之開源 AI 模型為基礎，進一步自行訓練或微調(fine-tuning)所研發之 AI 系統。

並宜多分配資源於高風險的 AI 系統，以有效地管理風險。風險評估所需考量之因素如下：(以下所舉例子係為協助說明風險評估情境，非就相關使用情境之風險等級加以規範，運用 AI 系統之風險高低仍由金融機構綜合考量各風險評估因素後自行判斷)

(一)是否直接提供客戶服務或對營運有重大影響

1. 提供客戶服務(面對客戶)之 AI 系統：AI 決策結果對客戶權益或營運有重大影響之 AI 系統，通常有較高之風險性，例如用於信用評分、機器人理財等系統；AI 決策結果僅係提升客戶服務品質者之 AI 系統，風險性可能較低，例如智能客服系統。

2. 用於內部作業(不面對客戶)之 AI 系統：AI 決策結果涉及監理規範之 AI 系統，通常有較高之風險性，例如用於法定資本適足率評估、洗錢防制等系統；AI 決策結果不涉及監理規範之 AI 系統，風險性可能較低，例如用於提升內部行政作業效率之系統。

(二)使用個人資料的程度：AI 系統使用個人原始資料[4]或機敏性個資程度越高者，可能具有較高之風險性。

(三)AI 自主決策程度：取代人類決策程度較高，或自動化學習程度較高的 AI 系統，可能會增加未預期之系統性負面影響，或減少即時人工干預的機會，而有較高之風險性。

(四)AI 系統的複雜性：運算模型的複雜性較高或使用參數數量與類型較多的 AI 系統，可能降低可解釋性，而有較高之風險性。

(五)影響不同利害關係人(stakeholder)的程度及廣度：AI 系統決策結果對內、外部利害關係人(stakeholder)影響程度較深或影響類型及數量較多者，可能具有較高之風險性。

(六)救濟選項[5]之完整程度：針對 AI 系統決策結果，如未提供利害關係人(stakeholder)救濟選項或救濟選項較不完整者，可能具有較高之風險性。

四、以風險為基礎落實核心原則

金融機構宜根據 AI 系統風險評估結果，決定採用之風險控管措施及程度，並確保與其現行實務作法相符。針對風險較高之 AI 系統，除在導入及使用時注意第一章至第六章所列重點及措施外，並評估是否

[4] 個人原始資料係指未經去識別化、隱私強化技術處理或其他方式處理之個人資料。

[5] 救濟選項(remedies)可能包括申訴或補救管道、爭議處理機制等。

採用下列措施：

(一)記錄：運用高風險系統宜有較完整之書面或數位紀錄。

(二)監控機制：運用高風險系統宜建立較高頻率及廣泛層面之監控機制。

(三)審查及核准：運用高風險系統宜有較嚴格之審查及核准過程，且提高決策層級。

(四)稽核或評測機制：經評估 AI 系統風險、內部資源及專業程度後，如有需要得由第三方稽核或評測單位進行獨立驗證。如導入之 AI 系統由同集團(包含其關係企業)開發或管理，相關稽核得以集團提供之資料替代。

五、第三方業者之監督管理

金融機構委託第三方業者導入 AI 系統相關作業時，宜採行以下監督管理措施：

(一)金融機構宜先進行檢視，評估該第三方業者是否具備相關知識、專業及經驗等，並判斷委託其導入可能衍生之集中度風險(金融機構自身委託該機構之集中度風險)，再根據評估結果採取適當之監督策略與管理作為，以防止可能之風險或問題。

(二)金融

(三)金融

(四)金融

(五)金融

(六)金融機構委託第三方業者導入事項如涉及金融業作業委外事項，應符合各業別相關委外規範。

- 人工智慧(AI)相關定義
- AI系統生命週期
- 風險評估考量因素
- 以風險為基礎落實核心原則
- 第三方業者之監督管理

整合 AI 進行資安管理的基本工作

資安基礎設施建置

資料收集

資安策略流程確立

AI 於資安管理應用

提升可視性

AI 能即時分析大量網絡數據和設備日誌，生成直觀的威脅檢測報告，提高威脅識別的效率。

增強主動性

AI 透過持續學習使用者和系統的行為模式，主動識別異常威脅，提前預警防範。

自動化防禦

自動執行例行資安任務，如威脅偵測、事件回應和日誌分析，降低人力成本並提高反應速度。

各領域服務供應上的防禦應用

【思考風險】

- 洩漏風險?
- 依賴風險?
- 限制與政策
- 監測與確保
- 事件與搶救

2024 台灣企業AI 準備度調查報告

數據力
企業已具備資料策略，且能發揮資料價值。

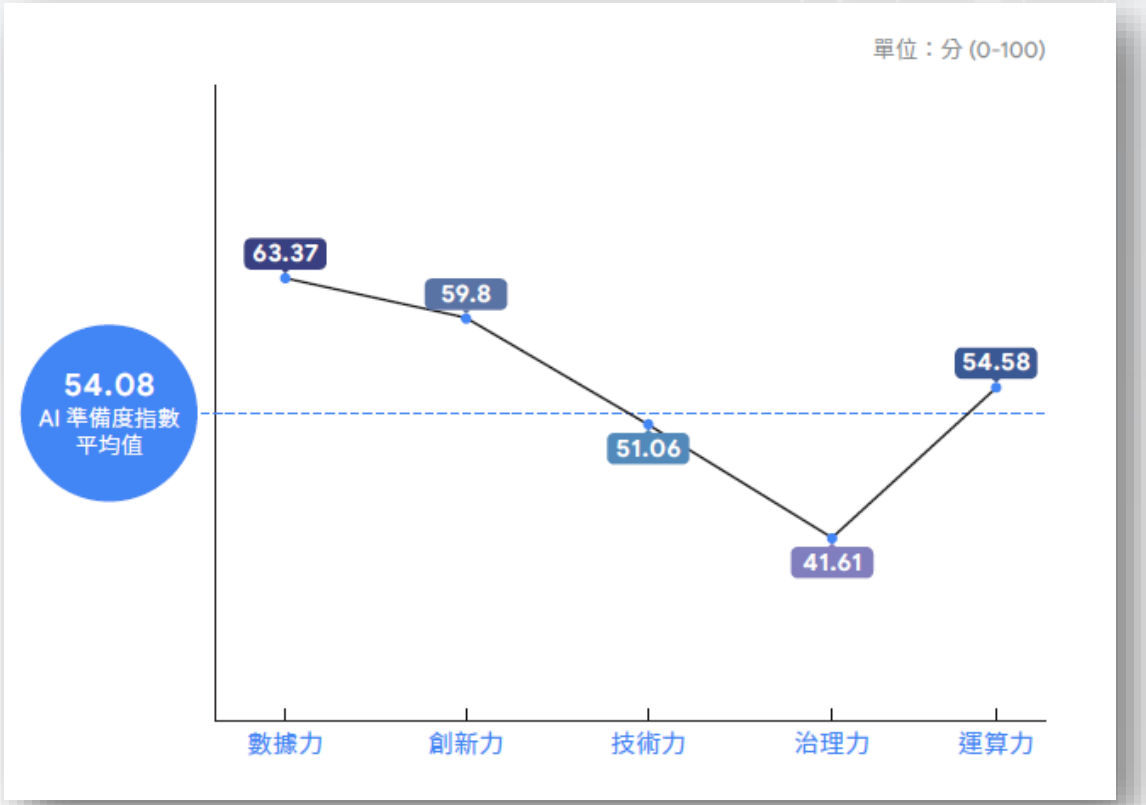
創新力
企業已具備接受 AI 技術的文化，且能靈活進行組織調整以因應新的分工。

技術力
企業已能將 AI 應用於工作流程中，具備足夠 AI 人才，並擁有建置與維護 AI 模型的能力。

治理力
企業對於發展的 AI 應用具備一定的掌握度，能確保 AI 的安全性與隱私，並了解 AI 的風險。

運算力
對於發展 AI 的運算環境已有妥善策略與規劃。

AI 準備度
完善的 AI 發展需要五大能力的均衡發展和協同運作。



問

目前我正在幫老闆擬一封信，請幫我用下面書信習慣寫一封，一樣的寄件者，但內容主要是跟"林院長"告知，近期因為疫情關係，6/15，13:10的演講"小心駭客就在你身邊"取消了，資料如附件。

Hi All,

經討論確認，
我們HQ Q2 VA ReScan預計更改至06月12日 14:00開始執行。
另外，外點的Q2 VA ReScan亦將於同一天開始執行，
相關資料如附件所示。

造成困擾非常抱歉，感謝大家協助，
如果還有需要調整的地方再請不吝告知。

Best Regards,

by Ray Wei
2024/05/07

答

了解，以下是給林院長的通知信件：

Subject: 通知: 6月15日演講"小心駭客就在你身邊"取消及相關資料

Hi 林院長,

經討論確認，
由於近期疫情關係，原定於6月15日13:10的演講"小心駭客就在你身邊"已取消，
相關資料如附件所示。

造成困擾非常抱歉，感謝您的理解與配合，
如果還有需要調整的地方，請不吝告知。

Best Regards,

by Ray Wei
2024/06/07

回歸基礎管理

三甲科技
AAA Security Technology

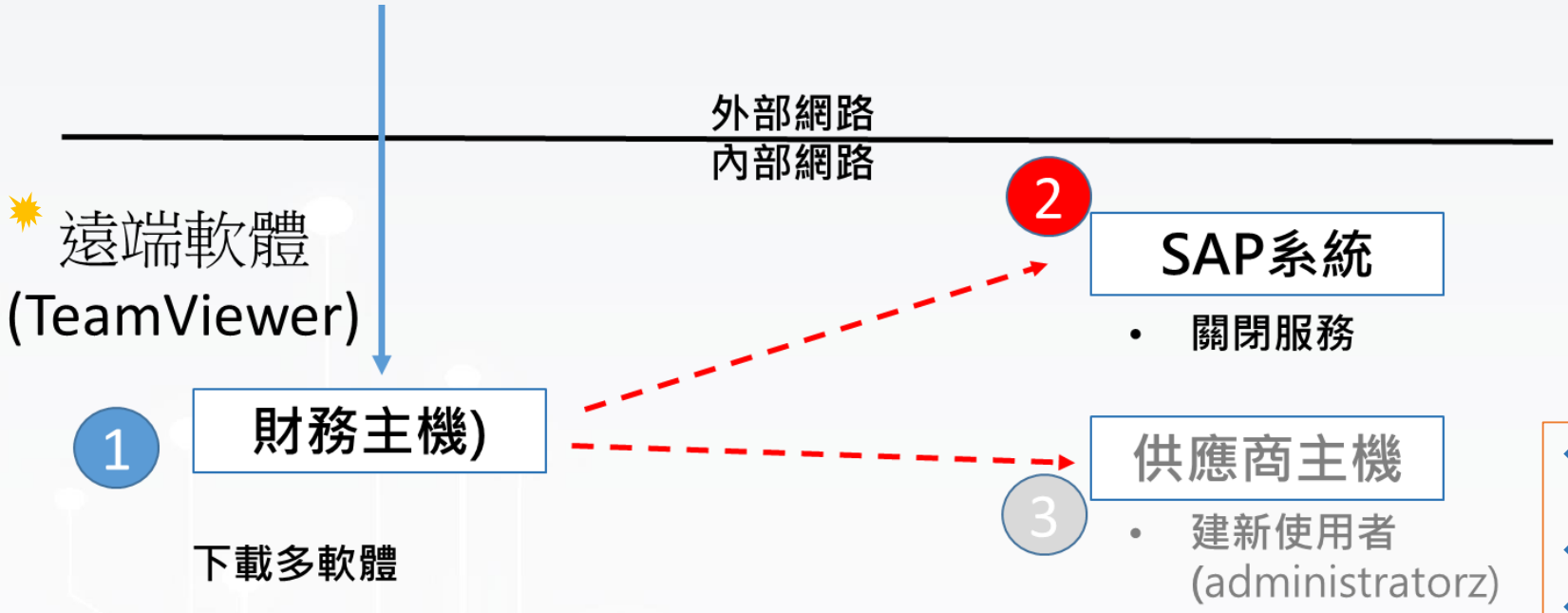
案例分享

- 第一階段
  - SAP停止服務事件發生、入侵軌跡描述、防護措施
- 第二階段
  - 螢幕監控事件發生、入侵軌跡描述、防護措施
- 第三階段
  - 資料刪除事件發生、入侵軌跡描述、防護措施
- 事件防護措施及建議
- 本次事件損害評估

第一階段

因為系統異常而進一步追查，才發現原來系統早有入侵痕跡

➢入侵軌跡



下載多軟體

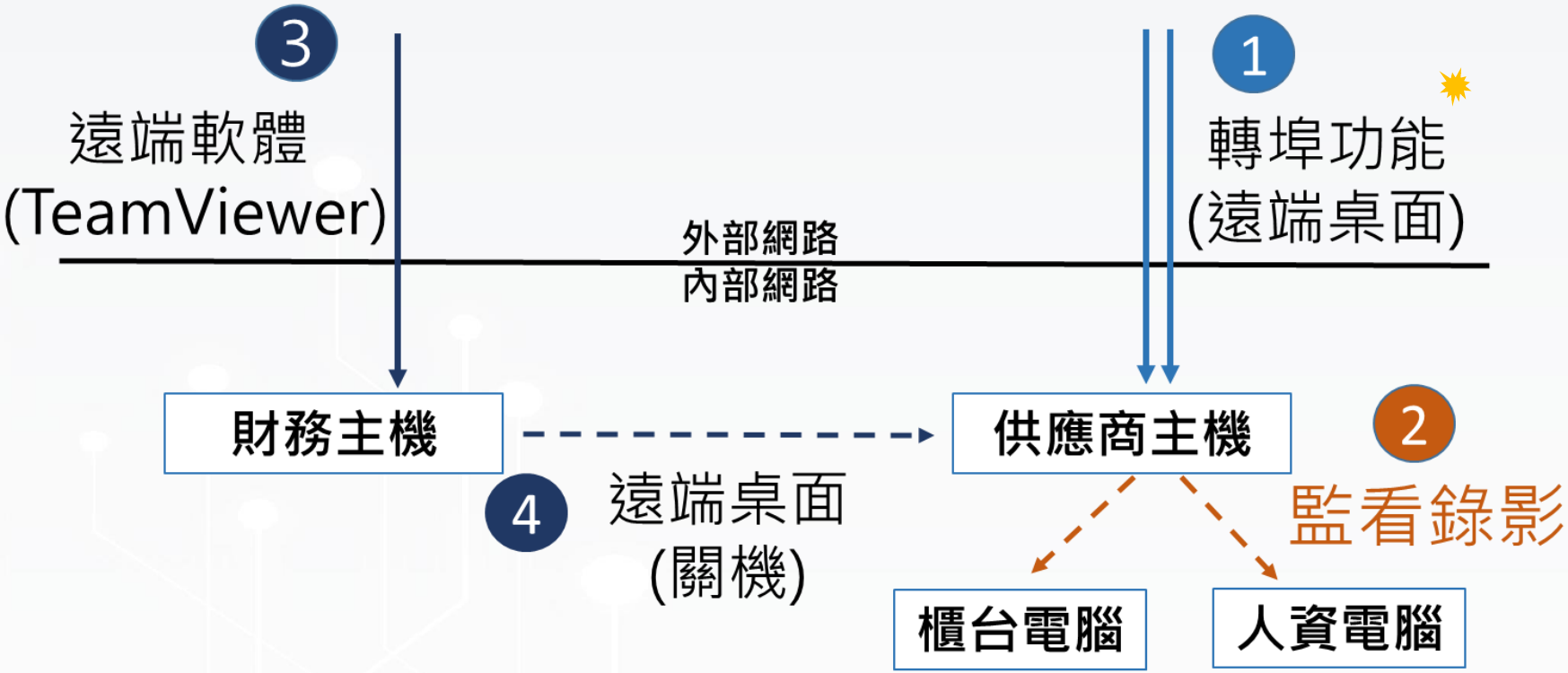
- **遠端控制軟體(Putty) → 關閉SAP服務**
- 遠端控制軟體(Radmin)
- **文件軟體(Libreoffice) → 查看共用槽文件**
- 螢幕錄影軟體(oCam)

- **關閉所有VPN**
  →於防火牆控管外部人員(廠商)進入內部網路
- **切割財務主機、伺服器網段與SAP間之存取權限**
- **停止並關閉遠端軟體、防火牆阻擋TeamViewer**
  →請資訊人員盤點並關閉同仁電腦使用之遠端軟體(包含TeamViewer、AnyDesk、Radmin、...)
- **持續觀察連線紀錄**
- **建立觀察區(財務主機)**

第二階段

平行調查其他主機系統，
發現也有入侵痕跡

➢入侵軌跡



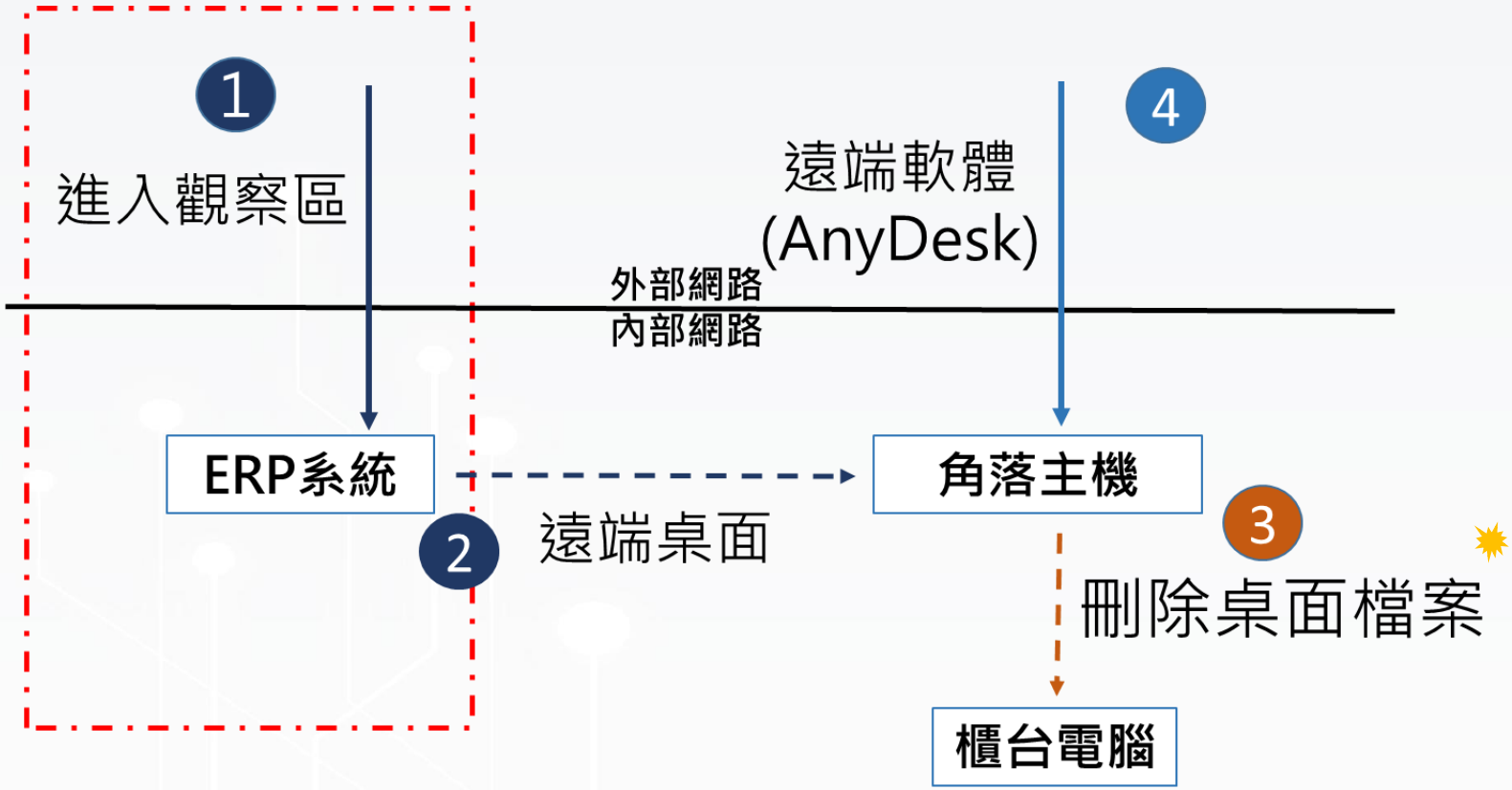
- 關閉供應商主機之遠端桌面
- 緊急關閉防火牆對供應商的轉埠功能
- 請MIS協助換掉核心系統使用者密碼

發現惡意IP：OO.OO.OO.OO、XX.XX.XX.XX

第三階段

追查事件入侵的軌跡時，
再次發現異常事件，逐步
向前探查出入侵來源點

➢入侵軌跡



過程防護措施

- 關閉VPN(除非必要透過MIS開通)
- 於防火牆全面審視轉埠功能保留必要服務
- 協助MIS全面更換主機密碼
- 限制使用遠端軟體、強制關閉TeamViewer存取

後續控管

- 確認所有電腦開啟網路芳鄰的需求性與必要性
- 限制遠端軟體使用
- 修改服務主機之管理密碼
- 資訊相關重要文件進行加密

發現惡意IP：找到真實來源

感謝聆聽

三甲科技
AAA Security Technology