從證券商內部利害關係人的視角檢視與資通安全部門的協作方式

中華民國證券商業同業公會業務電子化委員會副召集人

鄭嘉慶

1 資安部門和前線業務單位的關係與彼此眼中的自己

越來越危險的網路環境_不是因為它太陌生，而是因為它越來越懂我們

2026資安威脅預測

基於 2025 年全球資安趨勢觀察與預判2026年各行各業加速數位轉型，使網路威脅不再是 IT 部門的專屬課題，而是直接關係到企業的生存命脈。

隨數位轉型深化，攻擊面擴大與數據洩露風險增加。根據 IBM Security 最新發布的《數據外洩成本報告》顯示，2024 年全球數據外洩的平均成本已高達 450 萬美元，這一數字預計在 2025 年仍將持續攀升。這不僅是直接的財務損失，更包含了聲譽損害、客戶流失和合規罰款等「隱形成本」。尤其是在遠距辦公常態化、雲端環境複雜化的背景下，傳統的網路邊界防禦已顯不足，數據洩露的風險無孔不入。

地緣政治的緊張局勢已全面延伸到網路空間。在2025年國家級駭客 (Nation-State Hackers) 活動的數量與複雜性顯著提升。這些由國家支持的攻擊者，擁有雄厚的資源、頂尖的技術和極高的耐心，其發動的進階持續性威脅 (APT) 不僅旨在竊取情報、進行經濟間諜，更可能對目標國家的關鍵基礎設施發動偵察與破壞。
根據 Microsoft Threat Intelligence 於 2025 年發布的報告，過去一年中，針對關鍵基礎設施的國家級網路攻擊嘗試已增加 60%。

勒索軟體與供應鏈攻擊進化

勒索軟體 (Ransomware) 已從早期的廣撒網式攻擊，演變為高度組織化、精準打擊的「產業鏈模式」，更進化出「雙重勒索 (Double Extortion)」手法。此外，供應鏈攻擊 (Supply Chain Attack) 的威脅在 2025 年持續加劇，並預計在 2026 年達到新的高峰。如同 Gartner 所預警，到 2025 年，預計將有 45% 的全球組織遭受軟體供應鏈攻擊，相較 2021 年增加了三倍。

AI 驅動型攻擊

人工智慧的飛速發展，無疑是 2026 年資安領域的焦點。一方面，AI 正被資安廠商廣泛應用於威脅偵測、自動化響應和漏洞分析，大幅提升了防禦效率和精準度。另一方面，駭客也正加速將 AI 整合到其攻擊工具和策略中，使得攻擊更具自動化、個人化和隱蔽性。
據 Deep Instinct 的預測未來一年 AI 驅動型網路攻擊將大幅增加。 例如，AI 可以自動生成高度客製化的釣魚郵件，其語法和內容幾乎完美無瑕，顯著提高詐騙成功率；亦能加速零日漏洞的發現與利用，甚至透過深度偽造 (Deepfake) 技術進行身份詐騙和勒索。

資料來源:https://new-wp.effectstudio.com.tw/2026-數位安全新格局別再單打獨鬥！沒有資安部門，/

資安部門與和前線業務單位的關係

決戰境外，境外決戰

世上哪有歲月靜好，只不過有人為你負重前行。

資安部門眼中的前線業務單位看起來可能像.....

憨憨技術小麻瓜

+

恐怖噴火大怒神

前線業務單位眼中的資安部門看起來可能像.....

說話內容像天書

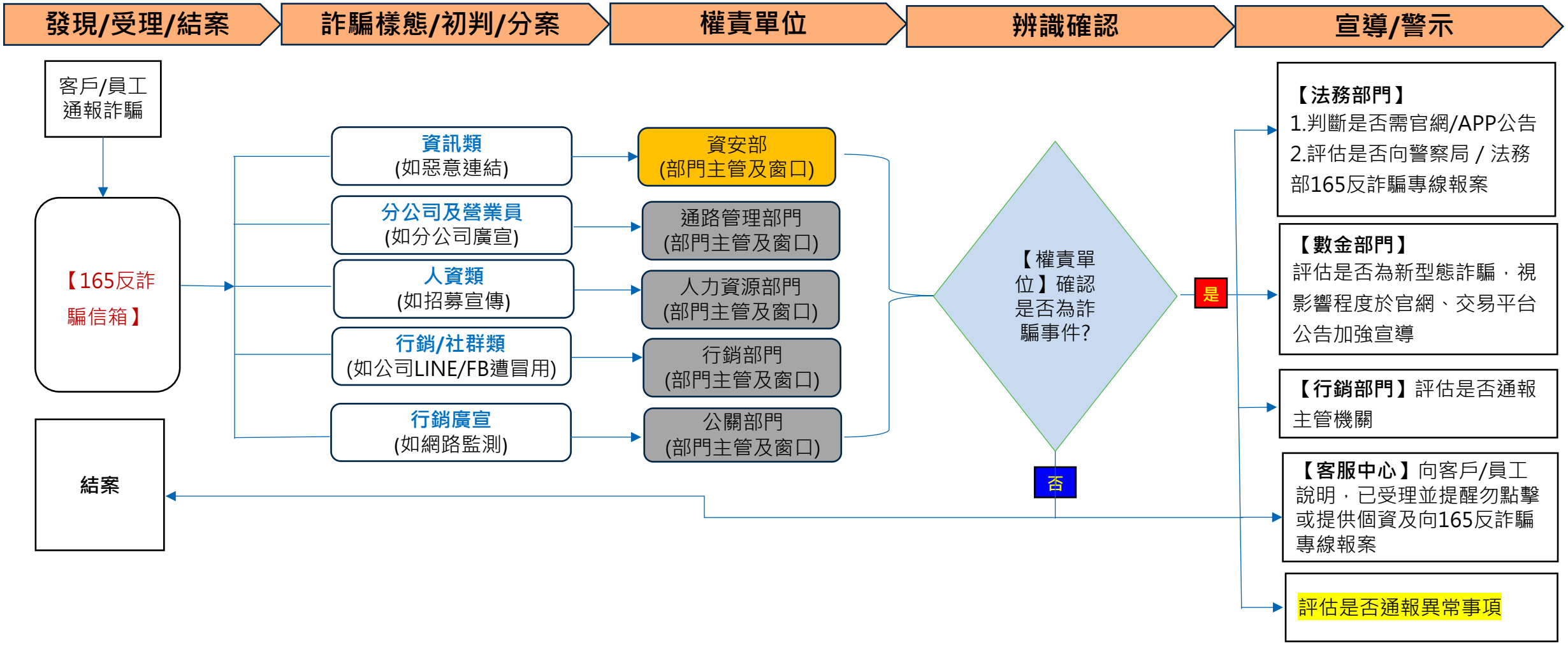
+

機櫃與主機

2 從實際案例中找到彼此高效率的溝通模式

案例1: 反詐騙

必須妥善設計工作流程SOP



資安部門是公司的防空鐵穹系統

資安部：

RSA偵測到以下釣魚網頁，已申請下架。

E7800746 (C7800745) hxxps :// kkpp [.] kgi357 [.] com / index / login 89.106.207.153
E7800753 (C7800752) hxxps :// kkpp [.] kgi379 [.] com / index / login 89.106.207.153
E7800748 (C7800747) hxxps :// kkpp [.] kgi599 [.] com / index / login 89.106.207.153
E7800744 (C7800743) hxxps :// kkpp [.] kgi69 [.] com / index / login 89.106.207.153
E7800741 (C7800740) hxxps :// kkpp [.] kgi359 [.] com / index / login 89.106.207.153
E7800750 (C7800749) hxxps :// kkpp [.] kgi257 [.] com / index / login 89.106.207.153
E7801179 (C7801178) hxxps :// kkpp [.] kgi237 [.] com / index / login 89.106.207.153
E7801181 (C7801180) hxxps :// 89 [.] 106 [.] 207 [.] 153 / index / login

資安部：

確認【23111915.ec66.tw】非公司網站，已請委外廠商RSA下架。

案例2:
網頁防護大廠Cloudflare全球系統異常

Cloudflare事件說明

2025/11/18

■ 原因：

資料庫的權限調整讓數據庫吐出一個2倍大的特徵檔案（Feature File），新的特徵檔案（Feature File）同步到全球每一個節點後開始出現崩潰

■ 歷程：

- 11/18 19:20 開始產生異常特徵檔，客戶端出現第一波錯誤
- 11/18 19:32~21:05 問題調查以及提供暫時方案，部分網站正常，仍然不穩定
- 11/18 21:37 團隊確認問題來自 Bot Management 的特徵檔，開始著手回滾
- 11/18 22:24 停止產生與同步新的（壞的）特徵檔
- 11/18 22:30 推送上一版正常的特徵檔，主要流量恢復正常
- 11/19 01:06 全系統恢復正常營運

■ 改善機制：

- 強化內部設定檔驗證，避免異常檔案被同步到全球
- 增加全域 Kill Switch，發生異常可立即停用相關模組
- 改善 Feature File 大小與結構防呆，加入異常偵測
- 強化資料庫權限變更流程，避免查詢行為被意外改變

2025/12/5

■ 原因：

Cloudflare 為防範 React 框架重大漏洞 CVE-2025-55182，調整 Workers 執行環境的緩衝區設定，將邊緣節點的記憶體緩衝區由 128KB 擴增至 1MB。在完成此調整後，Cloudflare 為解決與測試工具的相容性問題，進行了第二次停用測試工具的操作。然而，此變更在部分邊緣節點觸發錯誤狀態，導致 Workers 回應 HTTP 500 錯誤。

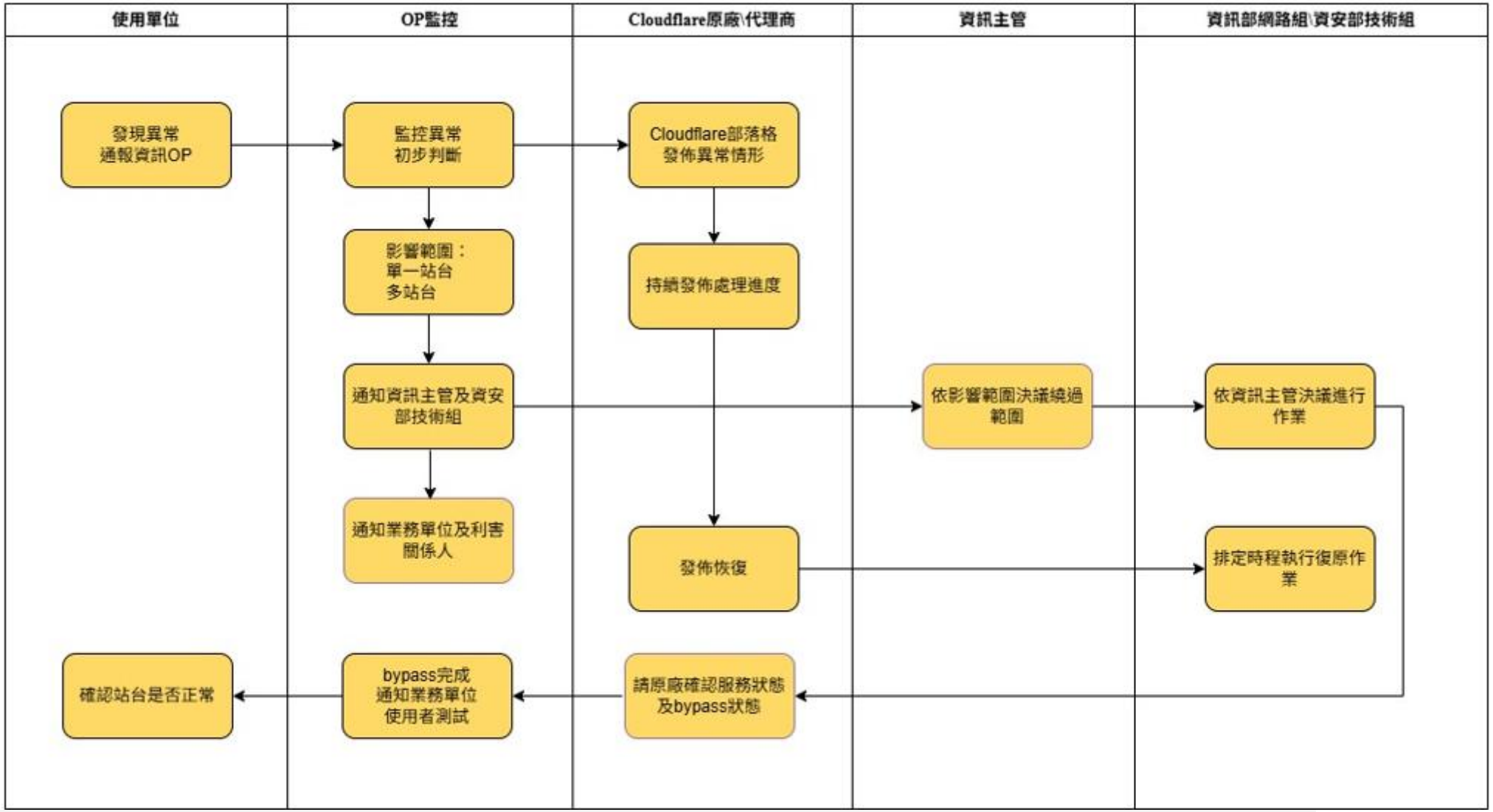
■ 歷程：

- 12/5 16:47 配置變更已部署並派送到網絡
- 12/5 16:48 變更已完全傳播
- 12/5 16:50 自動警報
- 12/5 17:11 配置變更已回復，派送開始
- 12/5 17:12 回復已完全生效，所有流量已恢復

■ 改善機制：

- 增強型部署和版本控制
- 精簡的緊急應變能力
- 「故障開放」錯誤處理

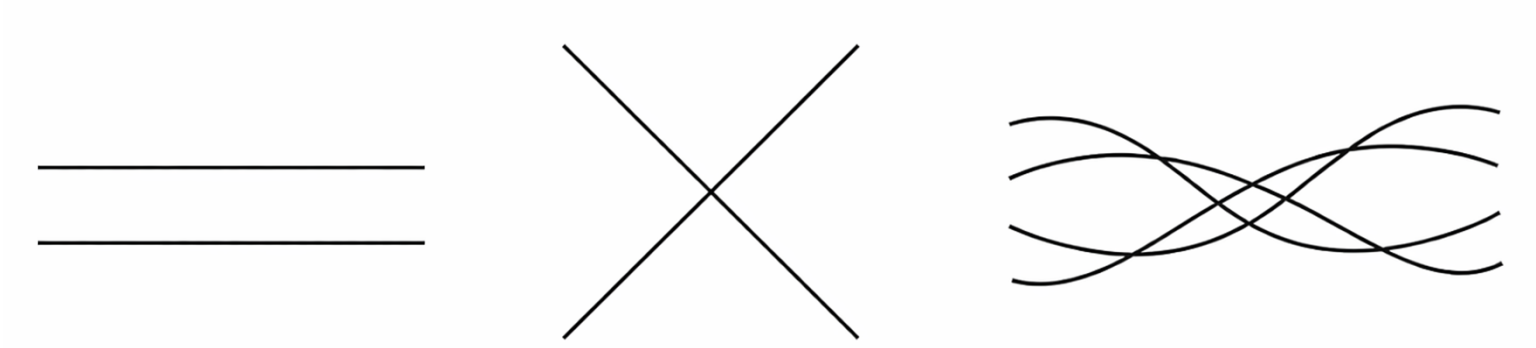
資安部門發動跨部門協同合作，爭搶時間降低業務衝擊



3 結論與思考

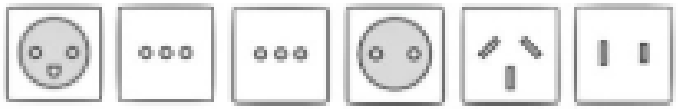
思考1：資安部門與和前線業務單位之間，現在處於什麼情況.....

平行線/偶而相交/纏繞共生前進???



思考2：如何避免資安部門與和前線業務單位之間有溝沒有通.....

找到自己的溝通轉接頭



國際萬用規格
各國幾乎通用

- 與前線業務單位共同商議SOP並落實執行
- 善用比喻的白話文運動
- 採用工具加強事前預警，遇到狀況隨時同步更新訊息