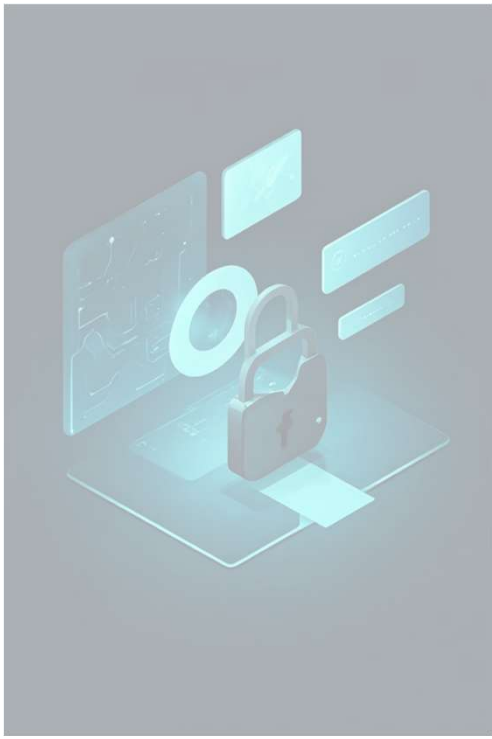
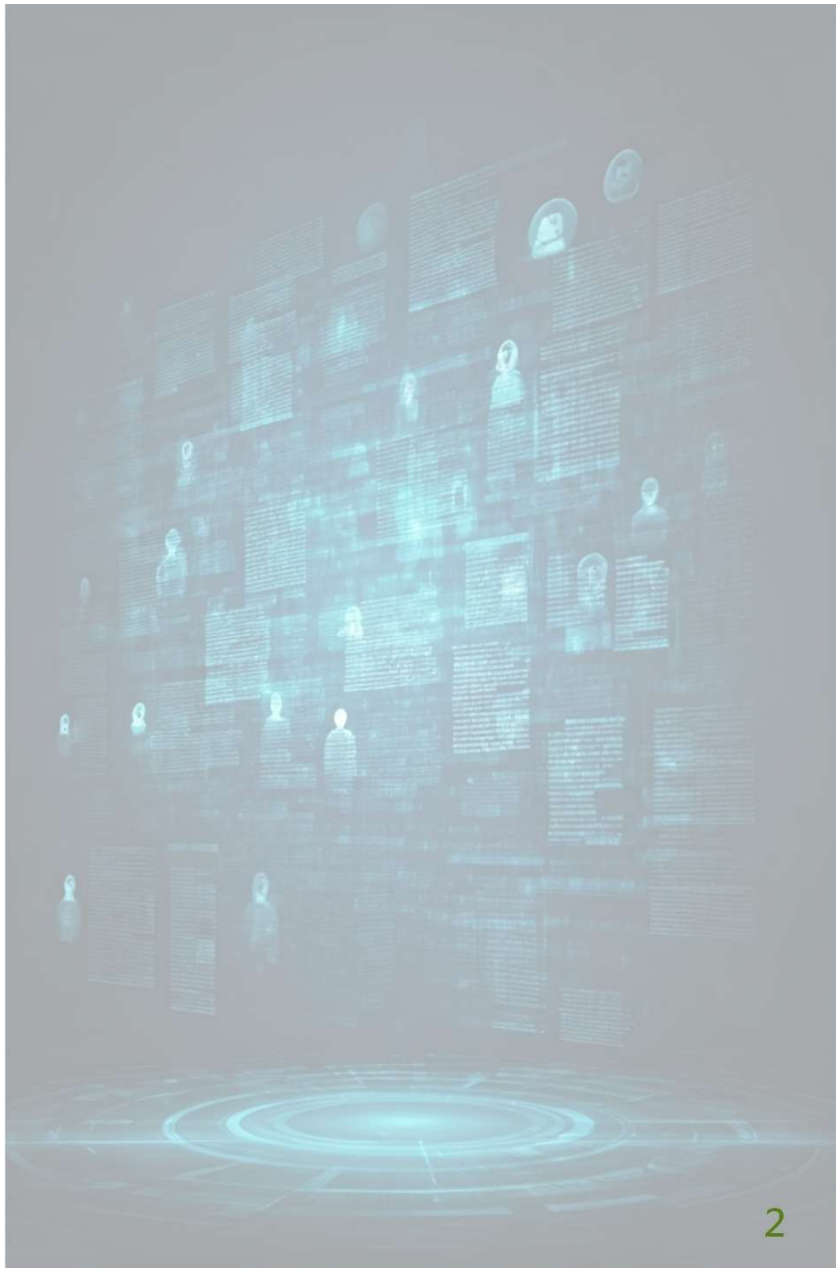
觀光署
114年度行政檢查計畫資安顧問服務案

季簡報

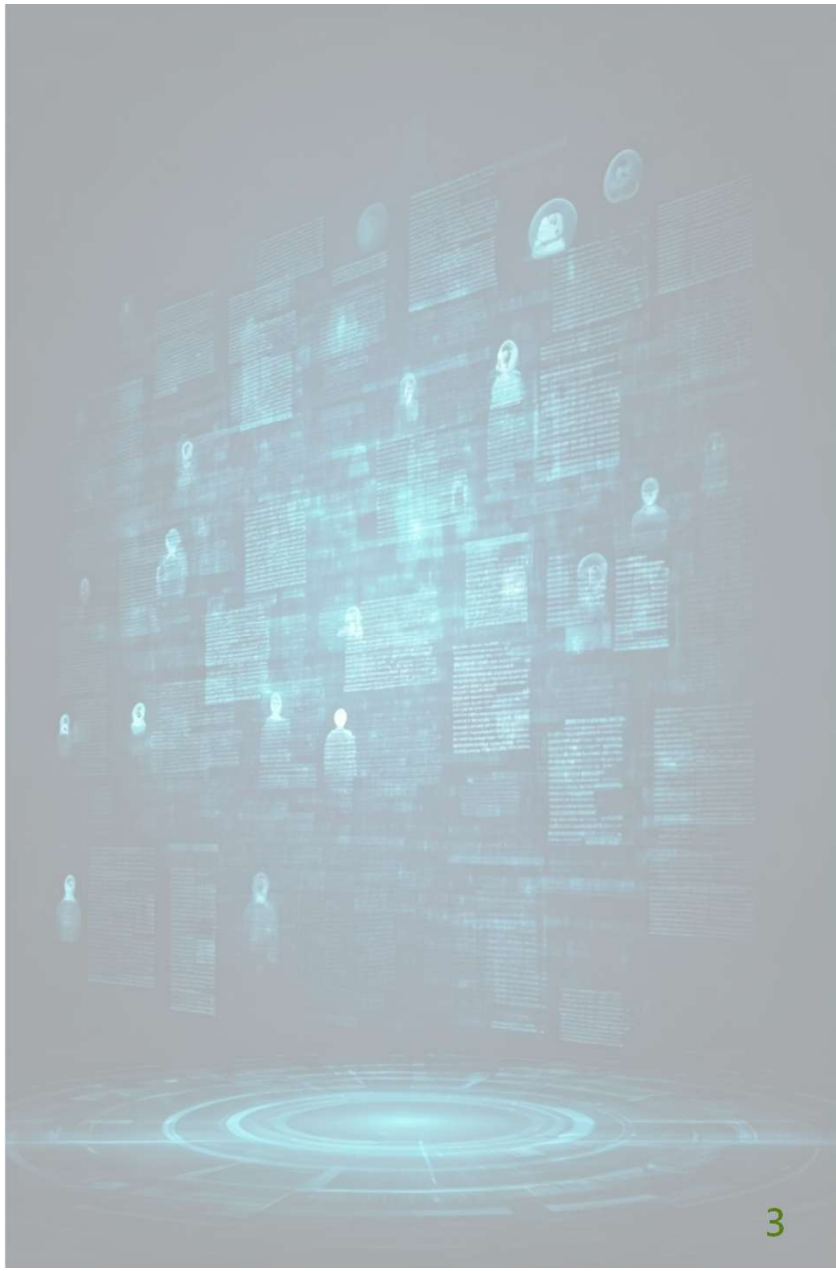
114年9月



目錄



一、共通性問題



一、共通性問題

- 截至114年8月31日，總共已完成51家業者稽核，應稽核家數共67家業者。
- 針對超過26家業者(比率超過50%)應改善之題項，納入後續共通性問題進行改善建議說明。

一、共通性問題

- 查核家數51家，共32間須進行改善。

查核項目	查核內容
3.界定個人資料之範圍	是否每年定期清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第2條界定蒐集、處理及利用個人資料之範圍。
- 業者應檢附「 個人資料檔案清冊」及個人資料作業流程說明文件，並經權責主管核定之紀錄，其個人資料之範圍界定之作法建議寫在「安全維護計畫」中。
- 可參考經濟部「個資作業手冊」(https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。

一、共通性問題

- 查核家數51家，共39間須進行改善。

查核項目	查核內容
4.個人資料之風險評估及管理機制	是否每年定期評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定適當之管控及因應措施？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第3條個人資料之風險評估及管理機制。
- 應檢附風險評估過程底稿、「風險評鑑報告」及「風險處理計畫」，其風險評估及管理機制作法建議寫在「安全維護計畫」中。
- 可參考經濟部「個資作業手冊」(https://www.moea.gov.tw/mns/colr/content/SubMenu.aspx?menu_id=7783)。

一、共通性問題

- 查核家數51家，共33間須進行改善。

查核項目	查核內容
7. 資料安全管理及人員管理	7.2是否依其業務特性、內容及需求，設定所屬人員接觸消費者個人資料之權限，並定期檢視其適當性及必要性？

- 依「個人資料檔案清冊」盤點，了解是誰會碰到個資，針對資料夾、系統權限進行帳號權限清查，應檢附個資資料夾、個資系統權限申請表單以及帳號權限審查紀錄。

一、共通性問題

- 查核家數51家，共40間須進行改善。

查核項目	查核內容
10. 資料安全稽核機制	10.1是否每年定期由適當組織執行資料安全內部稽核並提出評估報告？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點第8條個人資料安全維護稽核機制。
- 資料安全稽核機制之作法建議寫在「安全維護計畫」中，且應包含稽核之頻率及執行方式，並檢附最近一次之評估報告。

一、共通性問題

- 查核家數51家，共33間須進行改善。

查核項目	查核內容
10. 資料安全稽核機制	10.2是否採取改善措施以持續改善資料安全維護？

- 持續改善之作法建議寫在「安全維護計畫」中，應檢附檢視或修正之紀錄，如矯正單/追蹤紀錄。

一、共通性問題

- 查核家數51家，共28間須進行改善。

查核項目	查核內容
11. 使用紀錄、軌跡資料及證據保存	11.3是否保存個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄？

- 依「個人資料檔案清冊」盤點，清冊上的資料若有進行刪除、停止處理、利用或銷毀，應檢附個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。
- 如電子檔案銷毀、紙本檔案碎紙等之執行紀錄，登記在「 個人資料銷毀紀錄表」 。

一、共通性問題

- 查核家數51家，共27間須進行改善。

查核項目	查核內容
12. 個人資料安全維護之整體持續改善	12.1是否定期就個人資料安全維護議題召開會議並提出持續改善報告？

- 依照交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第5條第1項第2點10條個人資料安全維護之整體持續改善。
- 應檢附相關個人資料安全維護議題會議之記錄。

一、共通性問題

- 查核家數51家，共26間須進行改善。

查核項目	查核內容
13.委託作業	13.3委託他人蒐集、處理或利用個人資料之全部或一部時，是否確實執行監督？

- 依據個人資料保護法施行細則第8條&交通部指定觀光產業類非公務機關個人資料檔案安全維護計畫及處理辦法第21條。
- 呈13.2，於合約中約定後，在履約期間的監督是否有執行。
- 請說明對委外廠商之監督方式或檢附委外稽核報告以及稽核缺失追蹤情形。

一、共通性問題

- 查核家數51家，共26間須進行改善。

查核項目	查核內容
14. 使用資通訊系統蒐集、處理或利用個人資料-消費者個人資料達8千筆，且具對外電子商務服務系統者	14.7前2項之防止外部網路入侵對策及非法或異常使用行為之監控與因應機制，是否定期演練及檢討改善？

- 應針對防止外部網路入侵對策及非法或異常使用行為之監控與因應機制進行演練作業。
- 可檢附系統演練紀錄、防火牆政策檢討，紀錄中包含演練檢討。

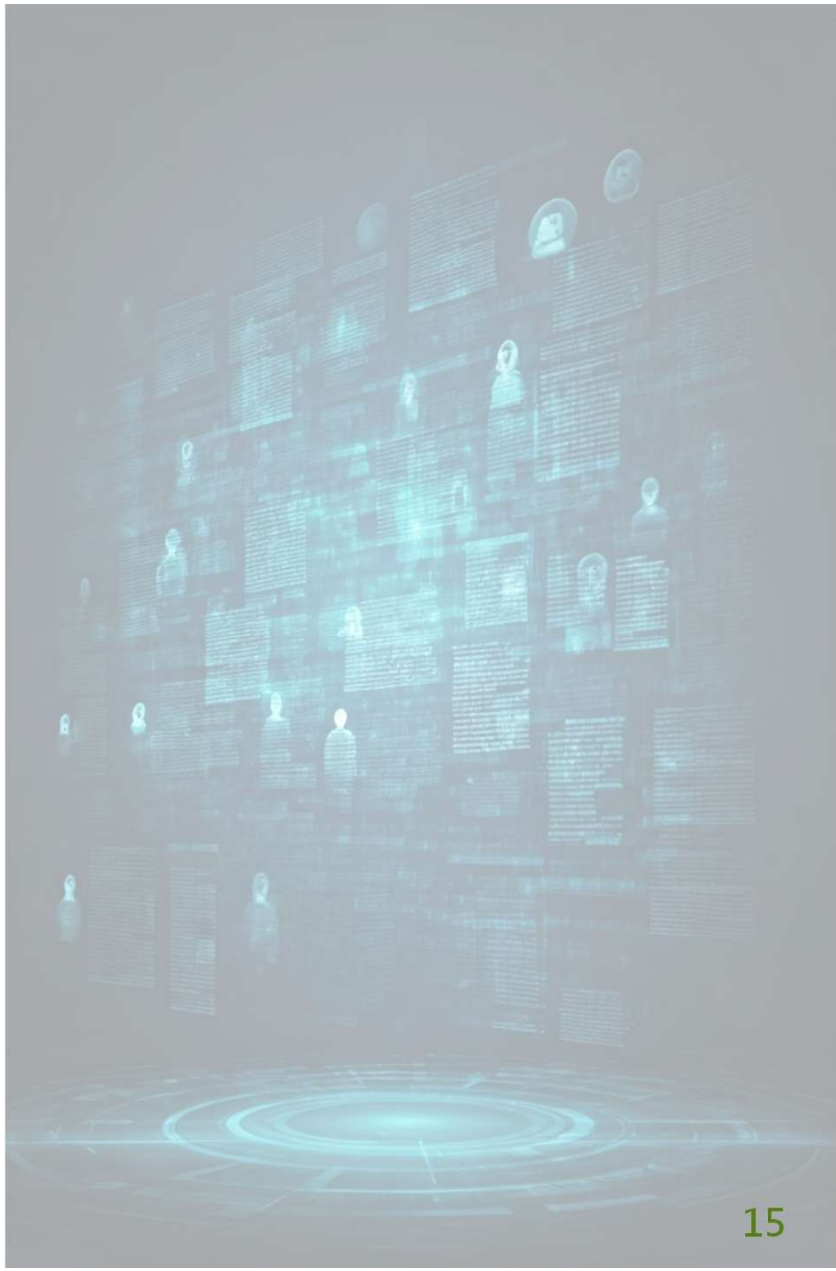
一、共通性問題

- 查核家數51家，共39間須進行改善。

查核項目	查核內容
18.其他	有存放個人資料之系統或伺服器是否已完成技術性檢測（弱點掃描、滲透測試），並針對檢測結果進行追蹤？

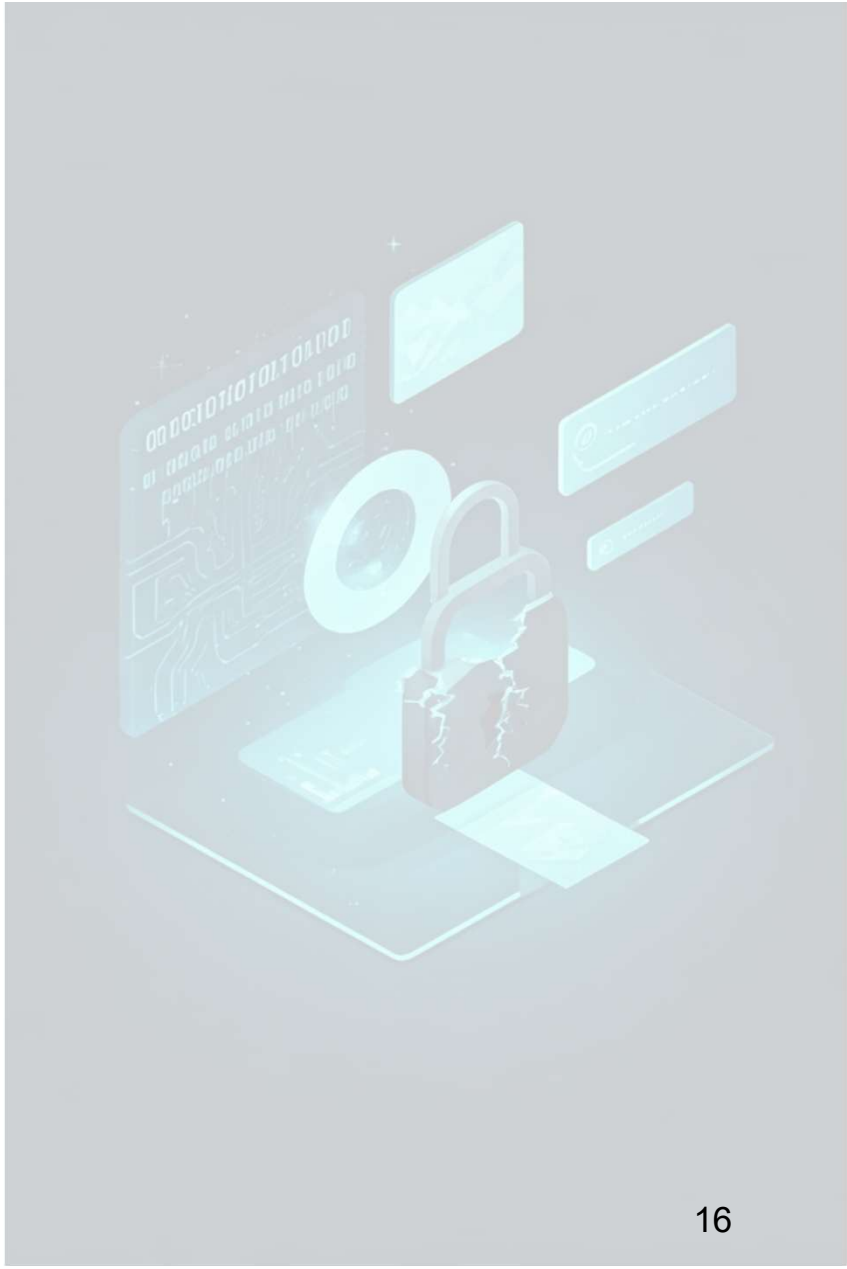
- 確認是否完成技術性檢測（弱點掃描、滲透測試），並針對檢測完成後之結果進行追蹤修補。

二、個案問題分析
-觀光業者個資外洩說明
-近期事件分享



觀光業者AA

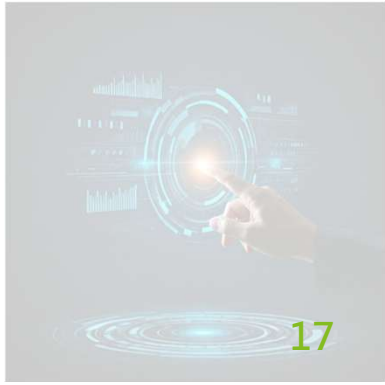
個資外洩原因及後續處理



AA個資外洩說明-事故說明

- 事故發生：AA於2025/07/23起接獲通知，發現遭到不肖人士偽冒對消費者進行詐騙，存在疑似資料外洩的跡象，為調查根因，故交付事件調查，調查後發現會員專區存在非授權大量存取訂單的紀錄。

- 事故根因：駭客使用多個Tor節點存取頁面/MemberV2/act/MemberLogin及/MemberV2/act/UpdateMember的紀錄，研判為嘗試大量登入並更新會員資料的行為，另程式碼內容中發現token值是利用3DES演算法將訂單號碼及會員ID加密後產生，為弱加密演算法。



AA外洩說明-後續處理建議

1. 程式碼中使用弱加密演算法(3DES演算法)，建議使用強加密演算法。
2. 建議評估強化現行會員驗證機制(如:導入雙因子驗證、登入失敗次數過多進行鎖定、登入失敗提醒、密碼定期變更、限制單一IP可同時建立的連線數等)。
3. 建議透過防火牆規則等方式，限縮可連線資料庫的主機。
4. 建議定期檢視並強化現有資安防護規則(如:資料庫稽核規則及網頁應用程式防火牆規則)。
5. 建議安裝作業系統與應用程式更新至最新版本。
6. 建議強化使用者資安意識。
7. 建議評估導入EDR解決方案(端點防護)或MDR監管(資安託管服務)。
8. 建議評估導入ISO27001資訊安全管理系統及ISO27701隱私資訊管理系統。

近期事件分享

蒐集5-8月國內外備受關注的重大個資外洩事件。

B公司機密洩密事件

2025 年 8 月， B公司爆出奈米製程機密洩密案，
疑似將先進製程技術外洩至競爭對手或境外組織。
此事件不僅引發國家安全法相關偵辦，
更讓企業界再次意識到：
資訊安全管理與隱私保護已不再只是 IT 部門的事，而是企業營運存亡的關鍵。

員工權限太寬鬆：
有些公司員工可以接觸到超過自己職務需求的資料，時間一久就成了安全破口。
資料沒分等級：
機密合約、設計檔和一般公文放在同一資料夾，誰都能打開，等於沒有鎖門。
沒有盯異常動作：
員工大量下載或複製資料，系統沒發警示，事後才發現早就外流。
合作夥伴的安全沒檢查：
把資料交給外包廠商，卻沒要求對方的資安標準，結果變成外面漏水，裡面遭殃。

ZZ爆資安危機

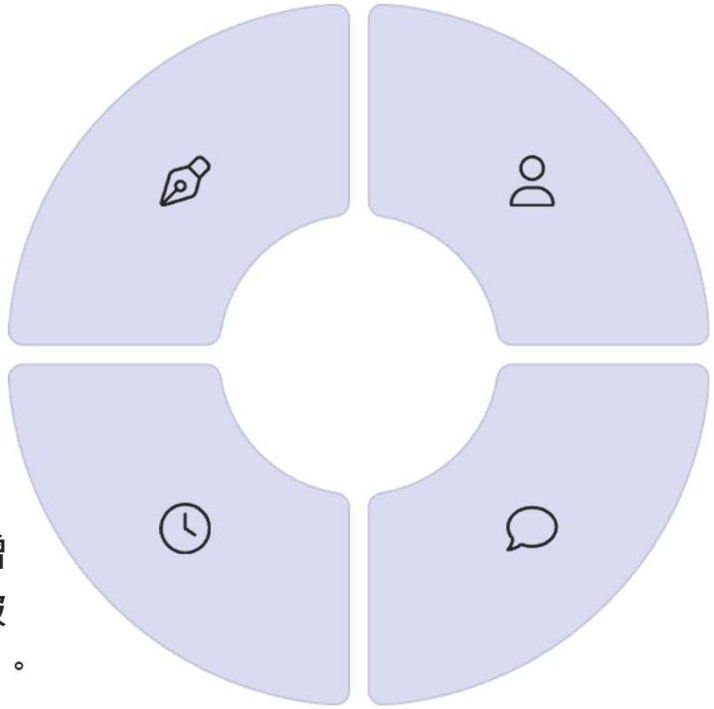
知名品牌ZZ台灣分公司於10號發布聲明，證實系統於7月2日遭駭客入侵，導致會員個資外洩，包含客戶姓名、電話、電子郵件、性別、國籍及購買偏好等資料。

ZZ強調未洩漏密碼及金融資訊，並已向受影響顧客發送警示電子郵件。

2025年個資外洩威脅趨勢

勒索軟體手法升級

勒索軟體結合資料外洩勒索，且能自動識別高價值目標，攻擊效率大增，造成企業及組織重大營運威脅。



人為因素

約60%的資料外洩事件與「人」有關，尤其是因為釣魚郵件、社交工程等操作失誤，儘管有資安教育，但員工仍因圖方便或其他因素成為資安防線薄弱點。

內部威脅與物聯網攻擊增多

由內部員工無意或故意洩漏資料的事件增加，且物聯網（IoT）及邊緣設備漏洞被大量利用，成為駭客入侵企業網路的跳板。

AI技術

駭客利用AI製作更難識破的釣魚郵件、語音偽造及深偽影片，讓攻擊更具欺騙性與規模化，使真實與虛假界線更加模糊。

總結....

2025年個資外洩威脅呈現技術複雜度提升、攻擊更具規模和智能化趨勢，「人為因素」及「AI技術濫用」依然是資安防護核心關鍵，組織需強化員工資安意識、採用先進防禦工具及構築零信任架構以減低風險。