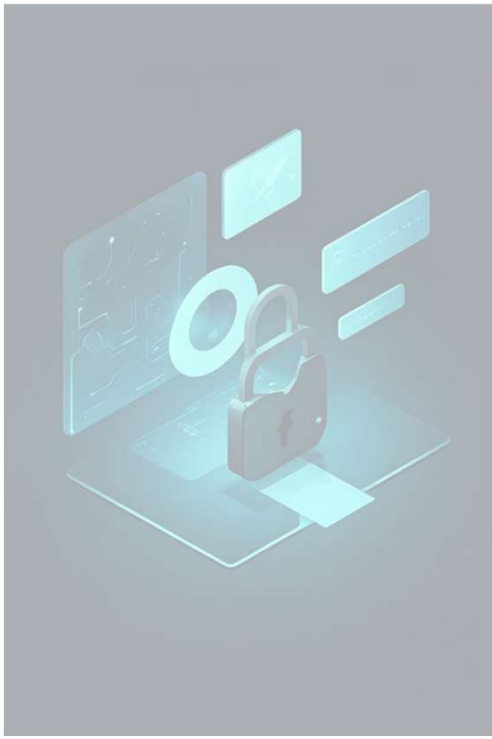
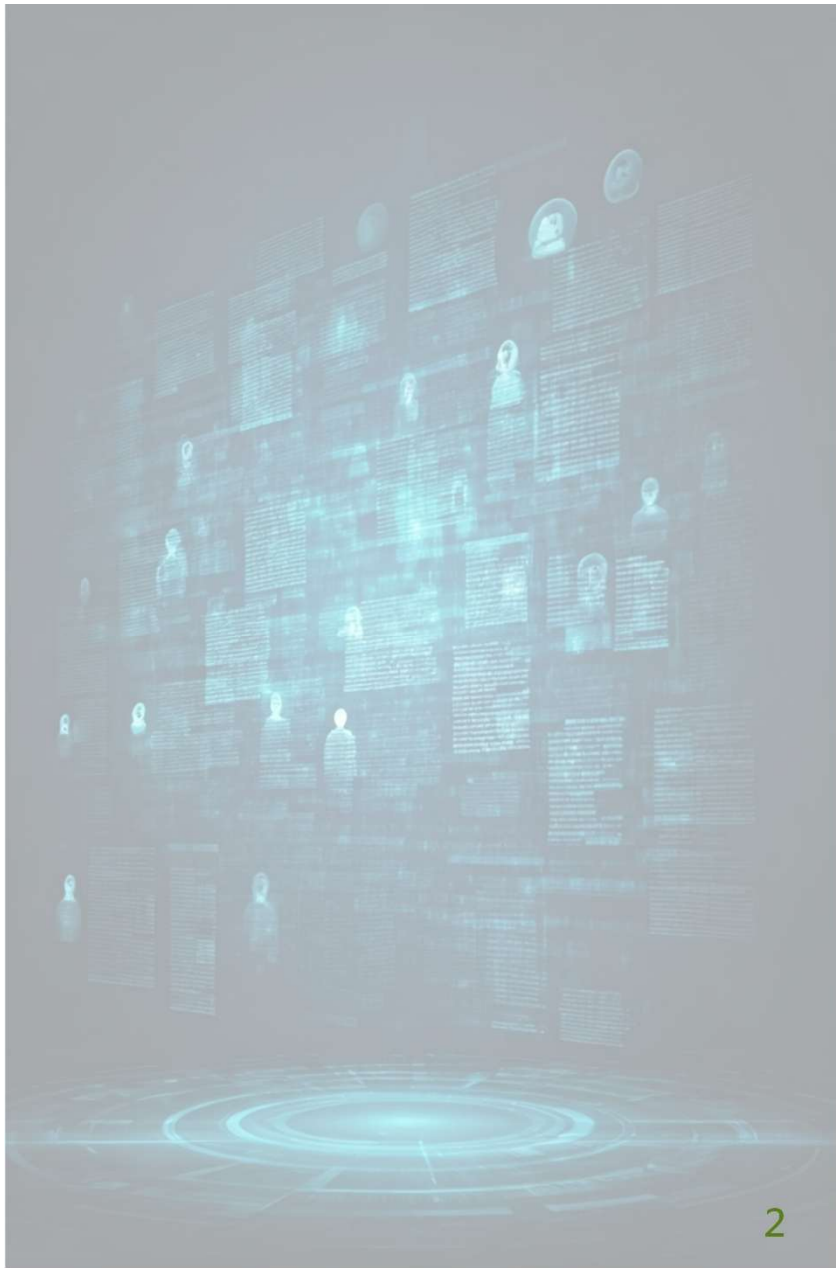
觀光署-114年度行政檢查計畫資安顧問服務案

季簡報

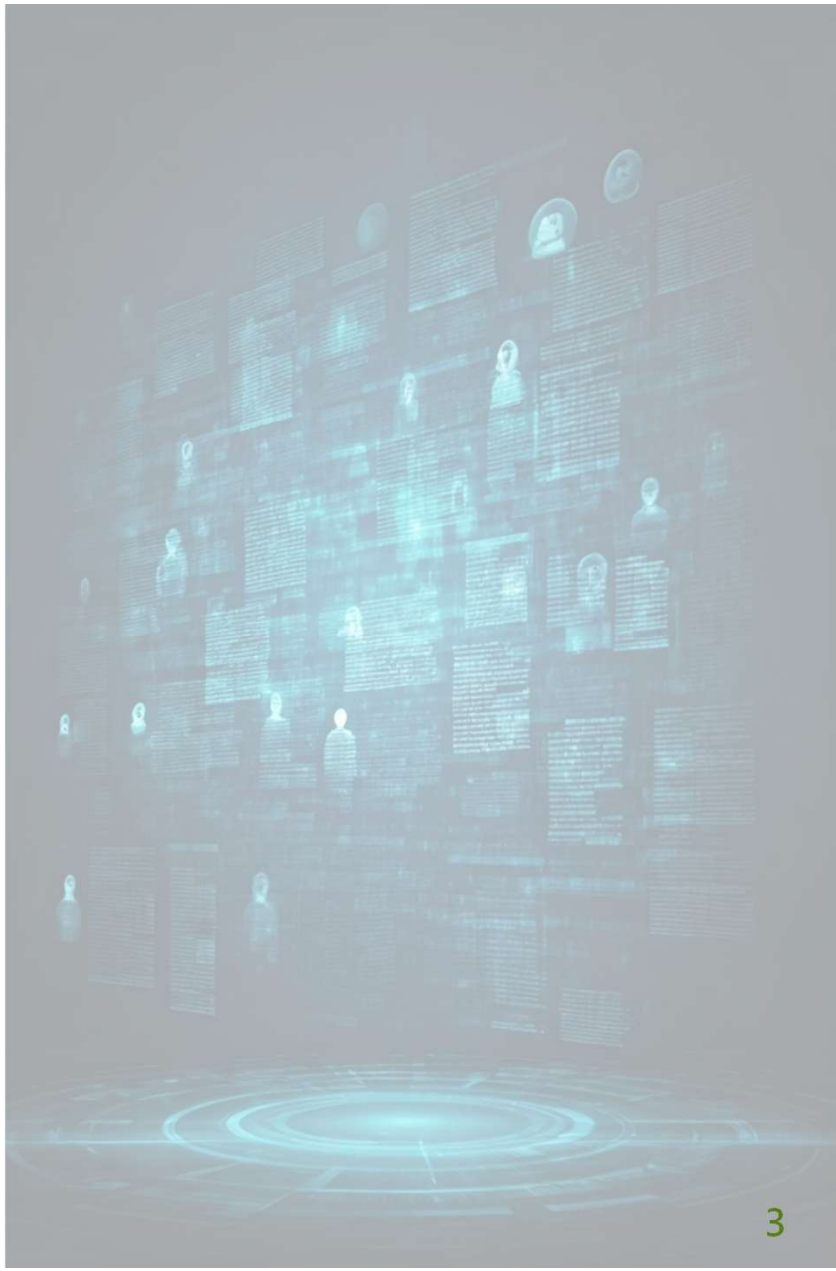
114年6月



目錄



一、共通性問題



一、共通性問題

- 查核家數35家，共21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？

- 法規依據
  - 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。
- 建議作法
  - 建議業者應明確界定與盤點組織蒐集個人資料相關之系統、資料庫與服務(有蒐集個人資料之系統或檔案是否都盤點)。
  - 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。

一、共通性問題

- 查核家數35家，共26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？

- 法規依據
  - 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。
- 建議作法
  - 建議每年應進行組織個資風險評估以識別相關可能之風險。
  - 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。

一、共通性問題

- 查核家數35家，共15間須進行改善。

查核項目	查核內容
5.事故之預防、通報及應變機制	5.4是否就個資事件之重大事故定義，及重大事故之通報流程為何？

- 法規依據
  - 依觀光署112年11月20日觀宿字第1120601160號函定義重大事故及其通報流程。
- 建議作法
  - 建議將個資事故應變機制，其中包含個資事件之重大事故定義，及重大事故之通報流程納入個人資料檔案安全維護計畫。

一、共通性問題

- 查核家數35家，共13間須進行改善。

查核項目	查核內容
6.蒐集、處理、利用作業	6.4是否依規定取得當事人同意（當事人同意之情形）？

- 建議作法
  - 建議單位應建立個人資料當事人同意之作業流程。內容應包含蒐集客戶個資並取得當事人同意之紀錄，並檢附告知同意書範本。

一、共通性問題

- 查核家數35家，共18間須進行改善。

查核項目	查核內容
6.蒐集、處理、利用作業	6.5是否履行告知義務（未履行告知義務時，是否符合免告知之情形）？

- 建議作法
  - 應檢附告知同意書範本或已執行之告知內容，免告知之內容可參考個資法第8條第2項相關項目

一、共通性問題

- 查核家數35家，共21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？

- 建議作法
  - 依個人資料檔案清冊盤點，識別那些人員處理個資，針對資料夾、系統權限進行帳號權限清查。
  - 應檢附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35家，共14間須進行改善。

查核項目	查核內容
9. 設備安全管理措施	9.2是否妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備？

- 建議作法
  - 確認是否**定期檢查或維護更新設備**，如系統主機、防火牆、個人電腦等，並應檢附定期檢查及維護紀錄。
  - 針對存放個資主機其作業系統是否已停止服務的支援，不再提供安全更新、非安全更新或技術支援，如作業系統使用Windows Server 2008-R2 2023/1/10停止支援，則建議進行作業系統升版。

一、共通性問題

- 查核家數35家，共26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？

- 法規依據
  - 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。
- 建議作法
  - 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，並應檢附最近一次之評估報告。

一、共通性問題

- 查核家數35家，共20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？

- 建議作法
  - 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35家，共16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？

- 建議作法
  - 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35家，共17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？

- 法規依據
  - 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。
- 建議作法
  - 單位應定期召開會議並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35家，共12間須進行改善。

查核項目	查核內容
13.委託作業	13.2委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件明確約定適當之監督事項及方式

- 法規依據
  - 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。
- 建議作法
  - 與委外廠商之合約中是否有約定個人資料適當之監督事項及方式，如每月報告、實地/書面稽核。
  - 應檢附個資委外之廠商清單及合約文件。

一、共通性問題

- 查核家數35家，共16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？

- 法規依據
  - 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。
- 建議作法
  - 建議於委外合約中約納入階段性驗收，在履約期間的監督是否有執行。
  - 可敘明單位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35家，共13間須進行改善。

查核項目	查核內容
13.委託作業	13.5是否要求受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關？

- 法規依據
  - 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。
- 建議作法
  - 提出個資委外之廠商清單及合約文件或其他地方有告知委外廠商之作業方式與佐證資料。

一、共通性問題

- 查核家數35家，共21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？

- 建議作法
  - 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(包含資安設備佈署)。
  - 應檢附系統演練紀錄，紀錄中包含演練檢討。

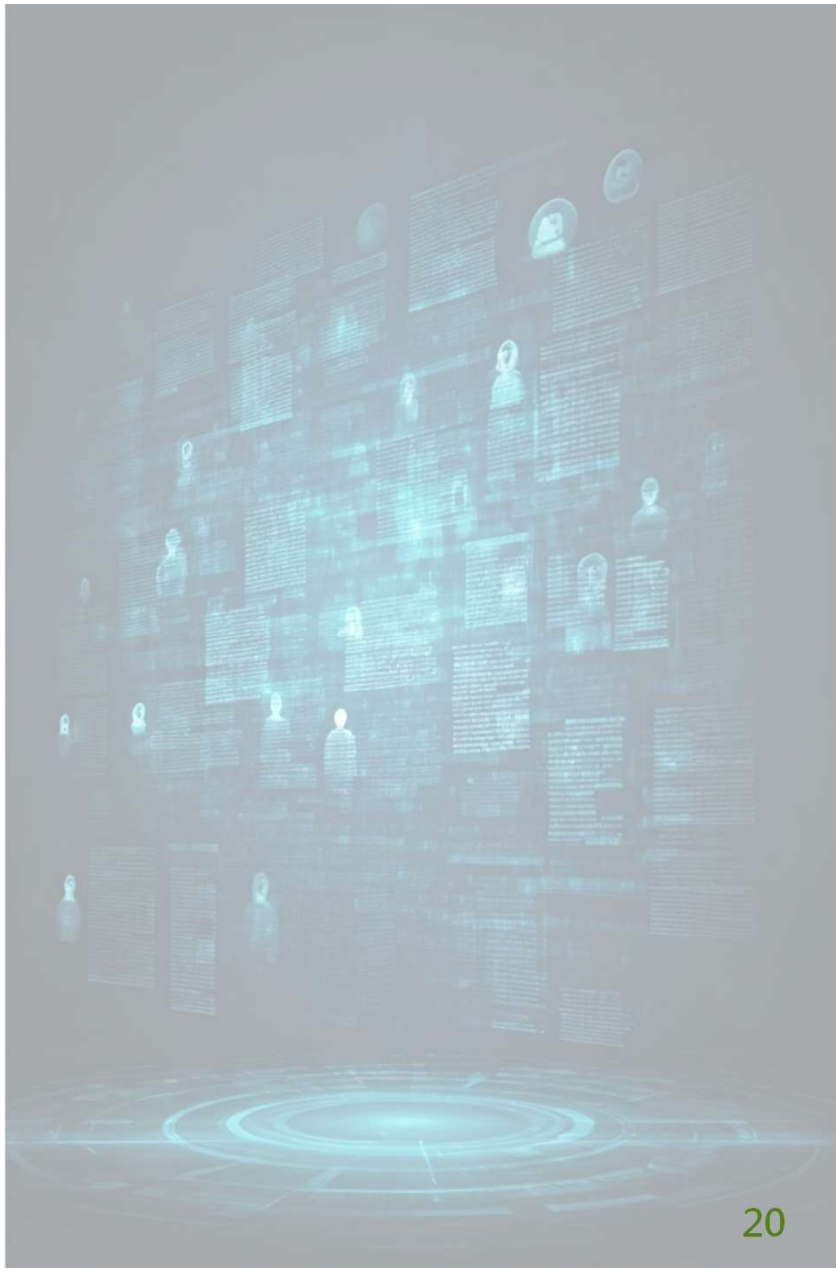
一、共通性問題

- 查核家數35家，共25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？

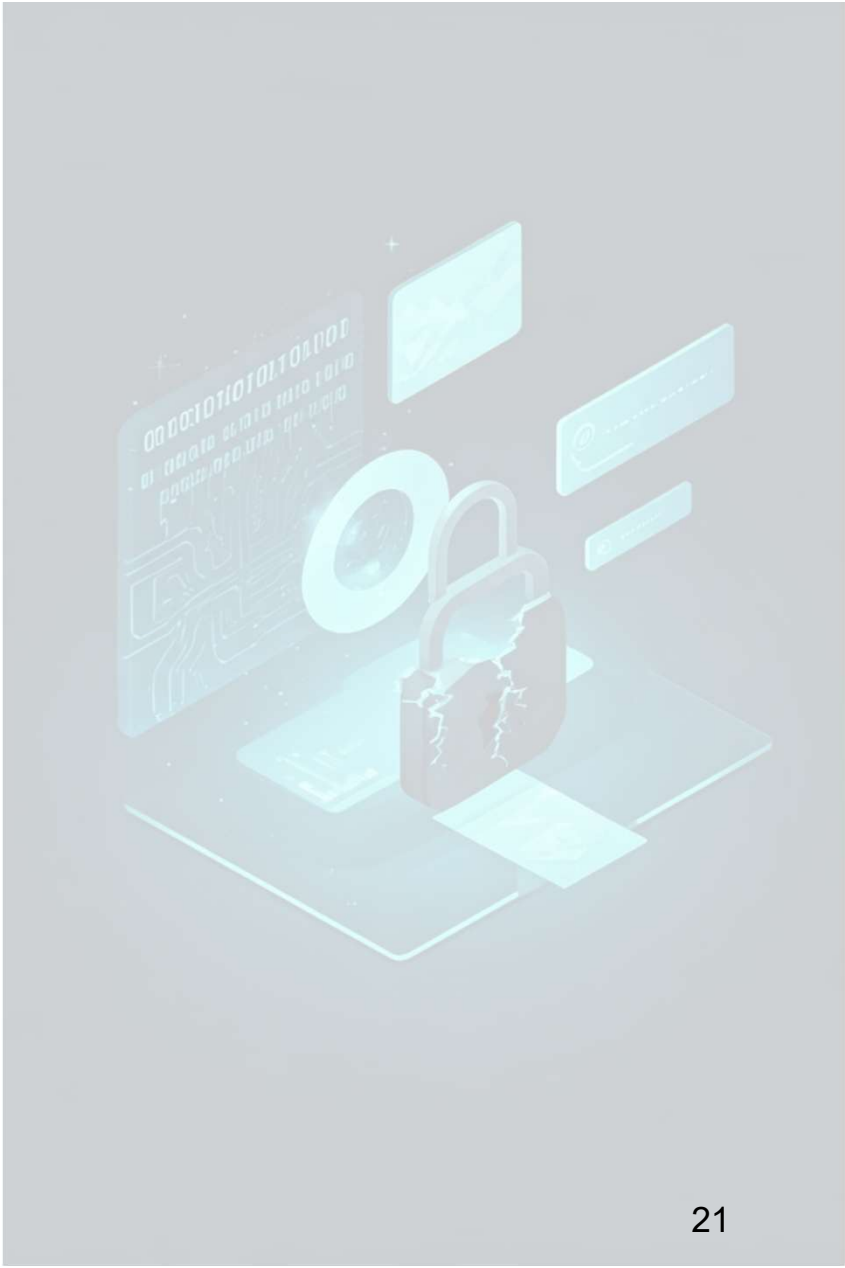
- 建議作法
  - 確認是否完成技術性檢測（弱點掃描、滲透測試），並針對檢測完成後之結果進行追蹤修補。

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A個資外洩說明

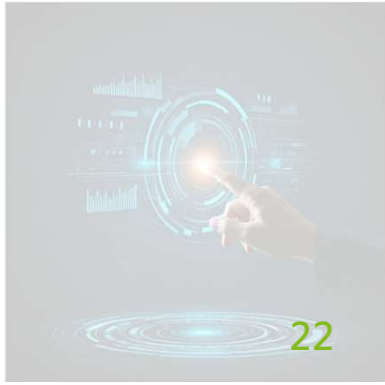
觀光業者A個資外洩原因及後續處理情形



觀光業者A個資外洩說明-事故說明

- 事故根因：公司員工個人電腦中存在惡意程式，在公司外部環境連線VPN，透過側錄方式取得訂單資訊。經調查後找出異常VPN連線之裝置，基於其意願及隱私權利，該裝置無法進行數位鑑識掃描。

- 因應措施：在事故發生當下，公司進行主機系統重建、切斷VPN連線、導入WAF系統，並請資安公司針對公司內部網路系統進行偵防工作（無發現侵入軌跡），並調整內部政策，僅允許公司派發之筆電，透過三重驗證方式建立VPN連線，驗證成功後才可存取內部系統。



觀光業者A個資外洩說明-後續處理情形

- 建立系統及資料庫日誌，以保全操作軌跡紀錄：
  - 針對資料庫(DB)、作業系統(OS)，AD伺服器及應用系統(AP)、防火牆及WAF等實施日誌保存。

- 非業務需要之機敏個人資料庫欄位應加密後再儲存：
  - 資料庫個資欄位進行加密，如業務執行人員需確認訂單明細資訊，需點選功能鍵解密。

- 應用系統應針對機敏個人資料庫欄位改以隱碼顯示：

(1) 員工登入AD驗證成功，以及ERP驗證成功後，才得以存取內部系統。

(2) 在個資頁面內，機敏個人資料預設隱藏，須按下顯示才會跳出詳細資料。

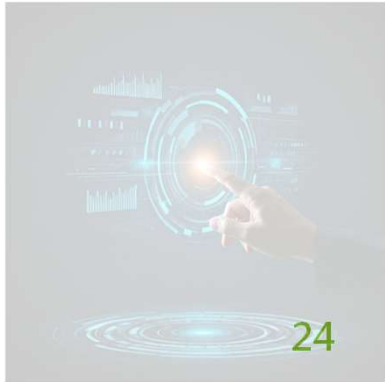
(3) 系統對應紀錄按下顯示聯絡人資料及取件方式之員工編號，存為記錄檔。

觀光業者A個資外洩說明-後續處理情形

- 提供員工使用VPN 服務，訂定相關管理措施（含終端使用設備資安防護政策等）：

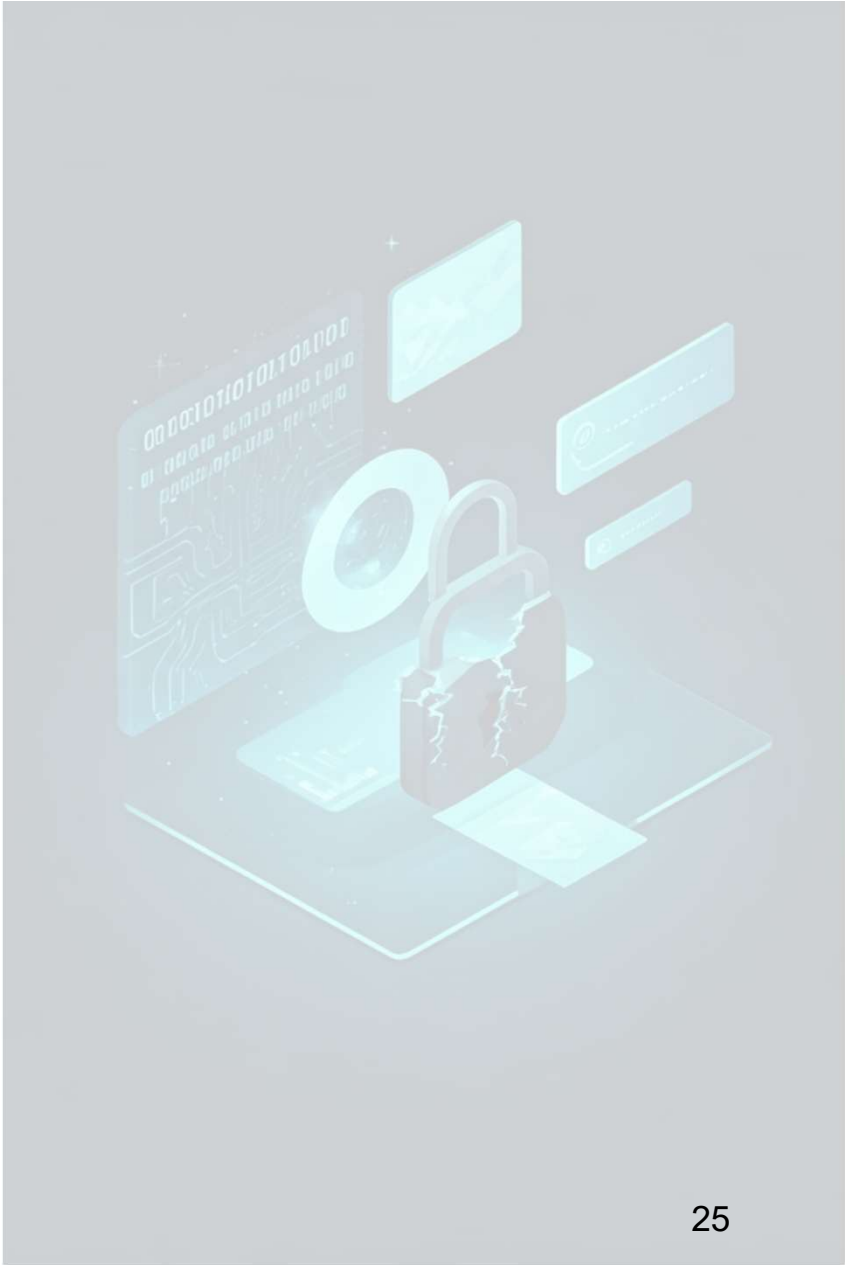
  身分審核、設備管控、三重身分驗證、登入時段

- 針對公司對外提供服務之應用系統，訂定每年進行資安檢測（如弱點掃描及滲透測試等）相關規劃。



觀光業者 B 個資外洩說明

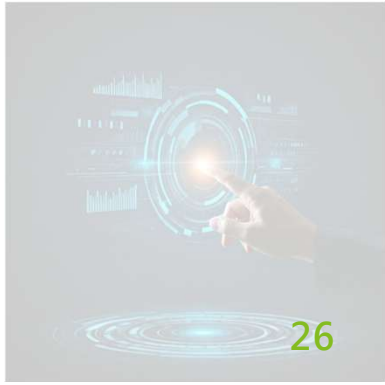
觀光業者B個資外洩原因及後續處理情形



觀光業者 B 個資外洩說明-事故說明

- 事故根因：攻擊者透過post/graphql，且利用getMemberData函數輸入custNo參數的漏洞以取得會員資料。

- 因應措施：事故發生當下判斷為個資外洩事件並追查及調整可能外洩位置，並主動透過簡訊通知受影響會員，於官網設置防詐騙頁面提醒消費者，且向警局進行報案動作 。針對系統進行以下調整：強化加解密機制、個資相關功能API及非法或異常使用行為警示機制、個資隱碼處理強化。



觀光業者 B 個資外洩說明-後續處理情形

- 個人資料檔案與資料庫的存取管理與控制：
  - 定期進行個資盤點，並設置存取控制限制非授權人員接觸。
  - 建立嚴格的存取記錄，確保所有存取行為可追溯。

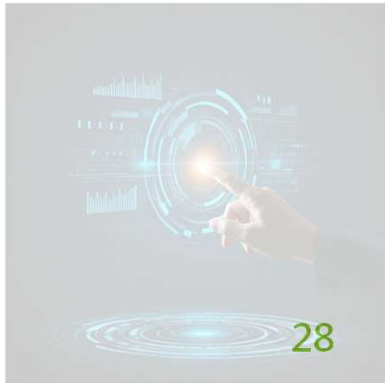
- 強化加解密機制：更新加密及解密使用加密標準SHA-512/AES-256保護敏感資料。

- 個資相關功能API及非法或異常使用行為警示機制：偵測使用行為，若有異常行為時進行阻擋，並設置警報及黑名單機制。

觀光業者 B 個資外洩說明-後續處理情形

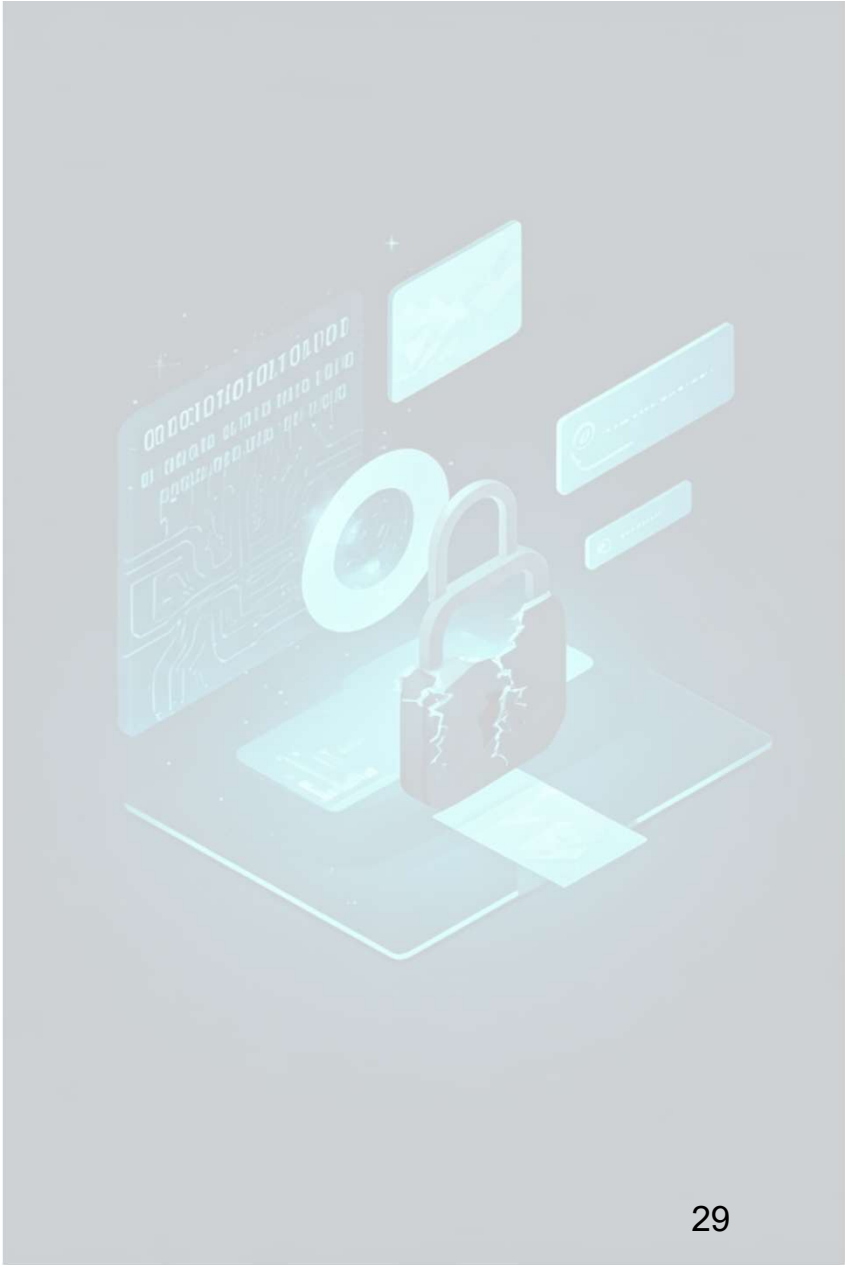
- 個資隱碼處理強化：針對有敏感資料的API進行盤點，盤點完成後進行個資隱碼處理。

- 技術檢測：針對對外服務定期執行源碼掃描、網頁弱點掃描、滲透測試。



觀光業者C個資外洩說明

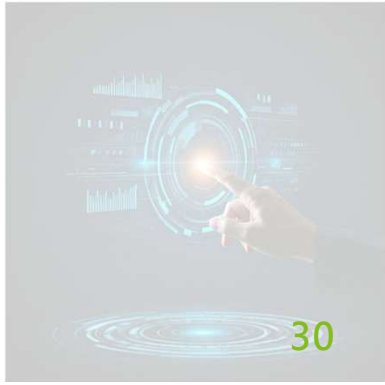
觀光業者C個資外洩原因及後續處理情形



觀光業者C個資外洩說明-事故說明

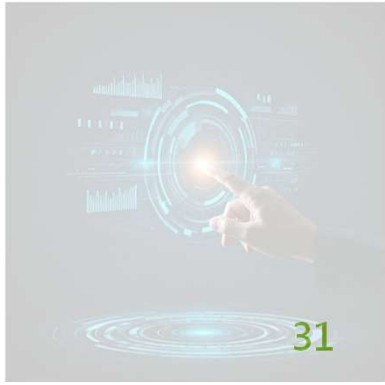
- 事故根因：經由WAF發現攻擊者透過正常管道登入使用者帳號，查看訂單資訊，並透過改變請求路徑URL中OrderNo參數後，即可以獲取他人使用者訂單資訊。

- 因應措施：業者自行發現特定IP存取數量異常而發出告警，並確認為惡意攻擊後立即阻擋惡意來源IP、限制存取頻次、更換密鑰及更新APP版本、強化API驗證機制及加強行為監控，並進行報案動作。後續以簡訊及墊子郵件方式提醒消費者避免受騙。



觀光業者C個資外洩說明-後續處理情形

- 前、後台訂單個資欄位遮罩
  - 資料庫機敏欄位加密、訂單欄位遮罩
- 帳號及權限管理：
  - 資料庫帳號定期盤點
  - 資料庫存取來源定期盤點
- 加強異常存取行為監控&阻擋：
  - 個資相關API 存取監控，初步設定同一IP 200 次 /10分鐘於WAF阻擋30分鐘，並依相關資料分析訂定合理閥值、滾動式檢討增修監控規則
- 進行弱點掃描、滲透測試、源碼檢測作業



共同根因分析

- 內部員工端安全防護不足，惡意程式感染且缺乏有效監控與數位鑑識（業者A）。
- 員工隱私權與安全調查的矛盾，影響事故調查完整性（業者A）。
- 權限與授權控管不足，導致未授權存取發生（業者B、C）。
- 系統設計缺乏嚴謹的參數驗證與授權檢查（業者B、C）。

建議措施

- 強化授權與存取控制
  - 系統端對所有敏感資料存取進行嚴格的身份驗證與授權驗證，避免只靠單一參數識別資料。
  - 對API及網頁參數採用間接參考（如Token或加密ID），防止IDOR(不安全的直接物件參照)攻擊。
- 加強系統參數驗證與安全設計
  - 對所有輸入參數進行嚴格驗證與過濾，避免攻擊者透過修改參數取得非授權之資料。
- 提升內部端點安全與監控
  - 強化員工端電腦防毒與惡意程式偵測，定期掃描與更新安全軟體。
  - 建立VPN連線行為監控與異常偵測機制，及早發現異常裝置與連線。

建議措施

- 數位鑑識與事件響應能力建置
  - 建立標準化的數位鑑識流程，提升調查效率與完整性。
  - 員工端設備若涉及資安/個資事件，應有明確政策與合約規範，避免因隱私問題阻礙調查。
- 教育訓練與安全意識提升
  - 定期對員工進行資安教育，強調惡意程式風險與安全操作規範。
  - 強化開發團隊安全設計能力，避免設計漏洞。
- 綜合來看，這三起個資外洩事故均反映出組織在授予權限控管、系統設計安全及內部端點防護上的不足，建議從技術、管理與人員三方面同步強化，才能有效降低個資外洩風險。

近期事件分享

將分析近期國內外備受關注的重大個資外洩事件，涵蓋醫療、社群平台與科技產業等領域。

AA醫院個資外洩事件

1 攻擊發生

2025年2月，遭CrazyHunter勒索軟體攻擊。

2 攻擊手法

駭客入侵AD主機並派送惡意程式。

3 資料販售

3月，BreachForums出現32.5GB AA醫院個資兜售訊息。

4 影響範圍

傳出高達1660萬筆個資遭竊，開價10萬美元。

BB醫院洩個資

2025年5月，事件起因於院內一名B姓呼吸治療師，

盜用多名醫護人員帳號投票，

又被查出利用遠端連線進入醫院資料庫，

瀏覽病患及醫護人員個資，包括知名人士在內，

上萬筆資料疑似有外洩風險，

但截至目前官方調查結果顯示，

尚未發現有病患或醫護人員個資實際外洩。

CC平台用戶資料外洩

28億

受影響用戶數

2025年3月爆發，史上最大規模社群媒體資料外洩之一。

6+

外洩資料類型

帳戶建立日期、用戶ID、個人簡介、位置等資訊。

1

可能原因

據報導，這起事件可能與內部員工有關。

DD 公司隱私資料外洩

2013至2018年間發生，2024年6月曝光。

數千起用戶隱私資料外洩事件。

包括兒童聲音音訊、共乘行程、已刪除的YouTube紀錄等。

發生原因為軟體問題讓外部開發商有機會存取 DD 公司用戶個資。

EE公司個資外洩

事件時間

2024年6月爆發。

影響範圍

20萬筆求職者個資遭駭客於國外論壇販售。

外洩資料

包含姓名、身分證、電話、地址等敏感資訊。

社會影響

事件引發台灣社會高度關注。

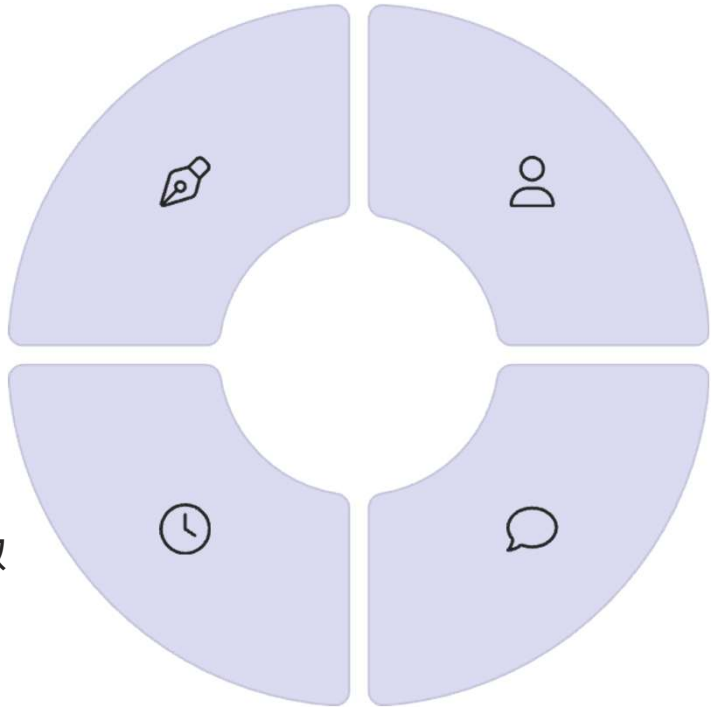
資安威脅趨勢分析

勒索軟體攻擊

成為主要威脅，醫療、金融、科技等產業均受波及。

攻擊速度加快

部分攻擊者能在1小時內完成資料竊取。



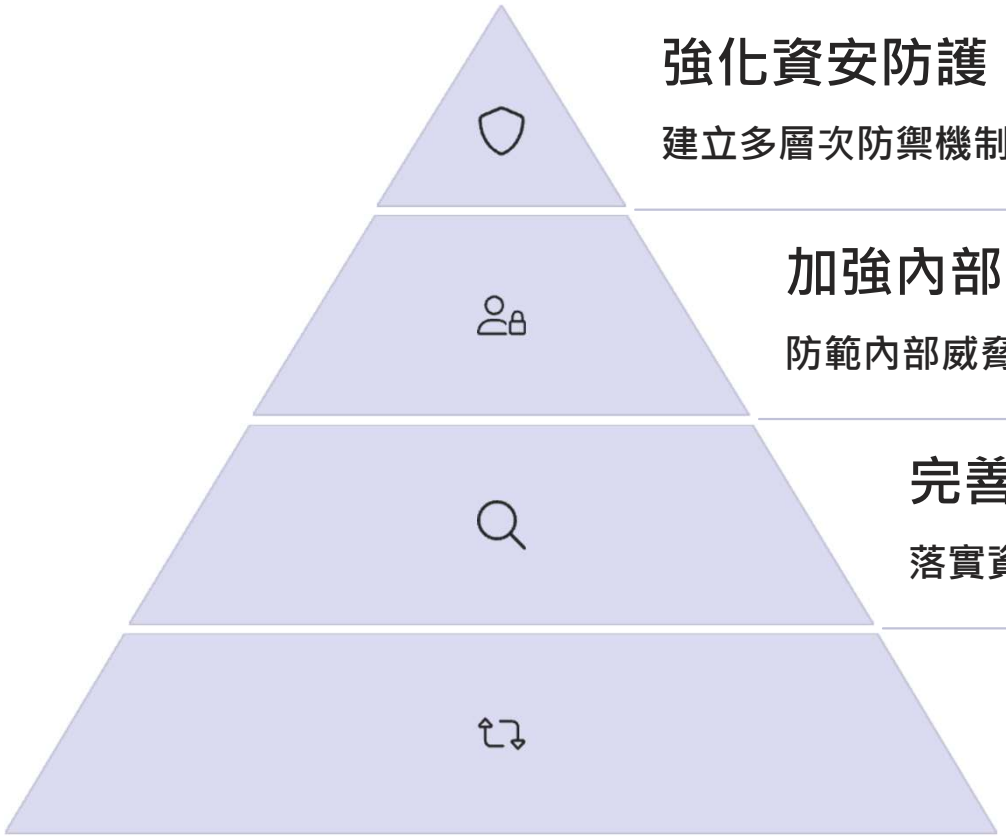
內部人員威脅

管理疏失導致大型平台出現大規模資料外洩。

台灣成為重災區

政府與企業部門仍為駭客攻擊目標，個資外洩事件頻傳。

資安防護關鍵建議



強化資安防護

建立多層次防禦機制

加強內部控管

防範內部威脅與人為疏失

完善個資保護

落實資料加密與存取控制

定期安全演練

提升應變能力與復原速度