附件 1 威脅/脆弱性範例

形式	脆弱性的範例	威脅的範例
硬體	儲存媒體的維護不足/錯誤安裝	危害資訊系統可維護性
	缺乏定期更換概要	設備或媒體的破壞
	對濕度、灰塵、土壤的敏感性	灰塵、腐蝕、凍結
	對電磁輻射的敏感性	電磁輻射
	缺乏有效的組態變更管理	使用上的誤用
	對電壓變化的敏感性	電力供應喪失
	對溫度變化的敏感性	氣象現象
	未保護的儲存庫	媒體或文件的盜竊
	處置時不小心	媒體或文件的盜竊
	未控制的複製	媒體或文件的盜竊
	欠缺寄送或接收訊息的證明	否認行動
	未保護的傳輸線	偷聽
	未保護的敏感性電信	偷聽
	不良的電纜接合	電信設備故障
	單點失誤	電信設備故障
	欠缺寄送者或接收者的識別與授權	偽造權限
	不安全的網路架構	遠端暗中監視
	以明碼傳送通行碼	遠端暗中監視
	不充分的網路管理(路由的彈性)	資訊系統飽和
	未保護的公用網路連接	未經授權的使用設備
軟體	無或不充分的軟體測試	濫用權限
	軟體上知名的缺點	濫用權限
	離開工作站時未'登出'	濫用權限
	處置或再使用儲存媒體未適當地消磁	濫用權限
	欠缺稽核軌跡	濫用權限
	錯誤的存取權限分配	濫用權限
	廣泛散佈的軟體	資料的訛用

形式	脆弱性的範例	威脅的範例
	在時間方面將應用系統程式應用至錯誤的資料	資料的訛用
	複雜的使用者介面	使用上的誤用
	欠缺文件	使用上的誤用
	不正確的參數設定	使用上的誤用
	不正確的日期	使用上的誤用
	欠缺像使用者授權的識別與授權機制	偽造權限
	未保護的通行碼	偽造權限
	不良的通行碼管理	偽造權限
	啟動不必要的服務	非法的處理資料
	不成熟或新的軟體	軟體機能失常
	對開發者不清楚或未完成的規格	軟體機能失常
	欠缺有效的變更控制	竄改軟體
	未控制的下載與使用軟體	竄改軟體
	欠缺備份複本	竄改軟體
	欠缺對建築物、門窗的實體保護	媒體或文件的盜竊
	未能產出管理報告	未經授權的使用設備
人員	缺乏人員	人員可利用性的違反
	不充分的招募程序	設備或媒體的破壞
	不足的安全訓練	使用上的誤用
	不正確的使用硬體和軟體	使用上的誤用
	欠缺安全認知	使用上的誤用
	欠缺監控機制	非法的處理資料
	外部或清潔人員未經監督的工作	媒體或文件的盜竊
	欠缺正確使用電信媒體和訊息的政策	未經授權的使用設備
場地	對建築物與房間不充分或草率的實體存取控制	設備或媒體的破壞
	位置位於易於有水災的區域	水災
	不穩定的電源格網	電力供應喪失
	欠缺建築物、門窗的實體保護	設備的盜竊

形式	脆弱性的範例	威脅的範例
組織	欠缺使用者註冊與撤銷註冊的正式程序（軟體）	濫用權限
	欠缺存取權限審查(監督)的正式程序	濫用權限
	欠缺或未充分提供(在安全方面)和客戶及/或第三方的聯絡	濫用權限
	欠缺監控資訊處理設施的正式程序	濫用權限
	欠缺一般的稽核(監控)	濫用權限
	欠缺風險識別與評鑑的程序	濫用權限
	欠缺記錄於管理員與操作員日誌的錯誤報告	濫用權限
	不充分的服務維護回覆	危害資訊系統可維護性
	欠缺或不充分的服務等級協議	危害資訊系統可維護性
	欠缺變更控制程序	危害資訊系統可維護性
	欠缺 ISMS 文件控制的正式程序	資料的訛用
	欠缺 ISMS 記錄監督的正式程序	資料的訛用
	欠缺公開資訊授權的正式程序	來自不可信賴來源的資料
	欠缺資訊安全職責的適當配置	否認行動
	欠缺持續計畫	設備故障
	欠缺電子郵件使用政策	使用上的誤用
	欠缺引進軟體至業務系統的程序	使用上的誤用
	欠缺管理員與操作員日誌的記錄	使用上的誤用
	欠缺機密資訊處理的程序	使用上的誤用
	欠缺在工作說明的資訊安全職責	使用上的誤用
	欠缺或未充分提供(在資訊安全方面)和受雇人員的聯絡	非法的處理資料
	欠缺已定義的資訊安全事故懲戒程序	設備的盜竊
	欠缺行動電腦使用的正式政策	設備的盜竊
	欠缺場所外資產的控制	設備的盜竊
	欠缺或不充分的”桌面淨空和螢幕淨空”政策	媒體或文件的盜竊
	欠缺資訊處理設施的授權	媒體或文件的盜竊

形式	脆弱性的範例	威脅的範例
	欠缺已建立的安全危害監控機制	媒體或文件的盜竊
	欠缺一般的管理階層審查	未經授權的使用設備
	欠缺通報安全弱點的程序	未經授權的使用設備
	欠缺遵循智慧財產權規定的程序	使用偽造或複製的軟體

威脅/脆弱性相關資訊

附錄（一）資產類別：資訊紀錄

威脅	脆弱性
火災	使用易燃性之材質，如紙或盒子。
未授權存取資料	網路存取規劃不當。
	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。
作業失能	備份失效
	保存不當
委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
冒充	未保護通行碼(password)檔。
	缺乏身份鑑別與辨識機制。
	通行碼易被人識破/取得。
破壞	存取權限不對。
	缺少實體安控。
	缺少變更管理控制。
	缺少邏輯上(技術或系統)的存取安控。
	對有計畫的破壞行動缺乏懲戒處分。
竊聽	未規範行動與遠端裝置之使用。
	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺乏交換資訊協議。
	通訊未加密。
	資料通訊室或中心缺少實體安控。
偷竊	未控制資料及/或軟體複製。

威脅	脆弱性
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。
通訊失能	未規劃與建置通訊線路。
	缺少備援與備份設備。
	缺乏意外處理機制。
惡意破壞資料與設施	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未規劃與建置通訊線路。
	沒有防毒軟體。
	對人員在軟體病毒的教育不足。
	未實施程式碼檢驗。
	對有計畫的破壞行動缺乏懲戒處分。
詐欺	缺乏應用系統控管導致不實的付款。
傳輸錯誤	佈線不當。
	缺乏意外處理機制。
資料外洩	資料分級錯誤或處理不當。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。

附錄（二）資產類別：電腦系統

威脅	脆弱性
入侵	未更新或安裝作業系統/軟體的修補程式。
	開發或設定標準不足。
阻斷服務攻擊	網路管理不足。
	缺乏備援系統。
未授權軟體變更	缺少軟體變更管理規範與程序。
	缺少備份。
	缺少變更管理軟體。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
未授權撥接存取	缺少使用者身份辨識。
作業人員或使用者錯誤	使用者認知不足。
	缺少有效的型態管理控制。
技術失能	使用者認知不足。
	變更管理流程失誤。
使用盜版軟體	未限制複製軟體。
	缺少人員使用合法軟體的規範。
	缺少軟體稽核。
	軟體派送安裝機制不足。
委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
破壞	存取權限不對。
	缺少變更管理控制。
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未控制由網際網路下載及使用軟體。
	沒有防毒軟體。
	資通安全政策不足。

附錄（三）資產類別：實體設備

威脅	脆弱性
水災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
火災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用易燃性之材質，如紙或盒子。
	缺少火災偵測設備。
	缺少自動滅火系統。
	缺少實體安控。
	備份檔案或系統無法使用。
未授權存取資料	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
地震	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
有害動物(蟲、鳥、獸)	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
污染	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
污染(放射線)	設備與設施缺乏維護。
	備份檔案或系統無法使用。
作業人員或使用者錯誤	使用者認知不足。
技術失能	由於不當的規劃或維護而導致網路容量不夠。
	技術設施維護不恰當。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用者認知不足。
	缺少備份設施或流程。
	缺乏環境保護。
	變更管理流程失誤。
委外作業失能	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
破壞	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。

威脅	脆弱性
偷竊	缺少實體安控。
通訊服務失能	網路管理不足(路徑彈性)。
惡意破壞資料與設施	缺少實體安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
極端的溫濕度	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	環境監控不足。
電力供給失能	電力供應設備容量不足。
電子干擾	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
電源不穩	位於易有電源不穩定地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	沒有電力調節設備。
暴風雨(土石流,颱風)	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。

附錄（四）資產類別：服務

威脅	脆弱性
干擾	傳輸介面易遭破壞或干擾。
中斷	缺乏應變計劃。
	容量不足。
	未釐清委外協議的權責。
	維護不當。
誤用	缺乏線路圖或標示不明。
	未釐清委外協議的權責。
	缺乏使用規範。

附錄（五）資產類別：人員

威脅	脆弱性
未授權存取資料	未規劃與建置通訊線路。
	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	傳輸機密資料未加適當防護。
	對有計畫的破壞行動缺乏懲戒處分。
罷工	沒有回復資訊與資訊資產的營運持續管理與程序。
	缺乏勞資協議。
未授權軟體變更	缺少接收訊息證明。
	缺少軟體變更管理規範與程序。
	缺少備份。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
	傳輸機密資料未加適當防護。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。
否認	未使用數位簽章。
	缺少收送訊息證明。
使用盜版軟體	未限制複製軟體。
委外作業失能	未釐清委外協議的權責。
社交工程	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
	缺乏交換資訊協議。
	通訊未加密。
	資訊相關辦公室或機房缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
破壞(偷竊,詐欺,竄改)	對有計畫的破壞行動缺乏懲戒處分。
偷竊	未控制資料及/或軟體複製。
詐欺	缺乏應用系統控管導致不實的付款。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。