個人資安防護與資安法因應

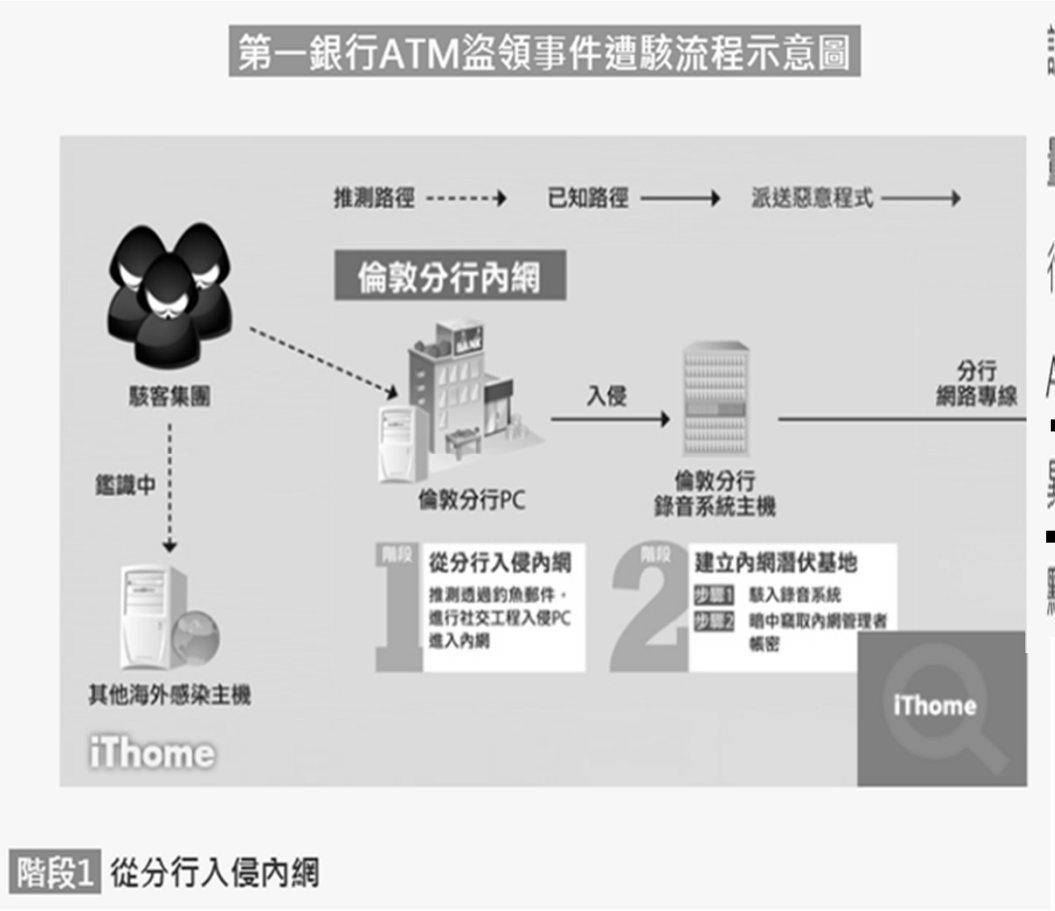
鍾沛原

成大資通安全研究與教學中心
TWISC@NCKU

Outline

- 資通安全管理法之因應
- 個人資安防護
- 結論

當防火牆與內網不再可靠

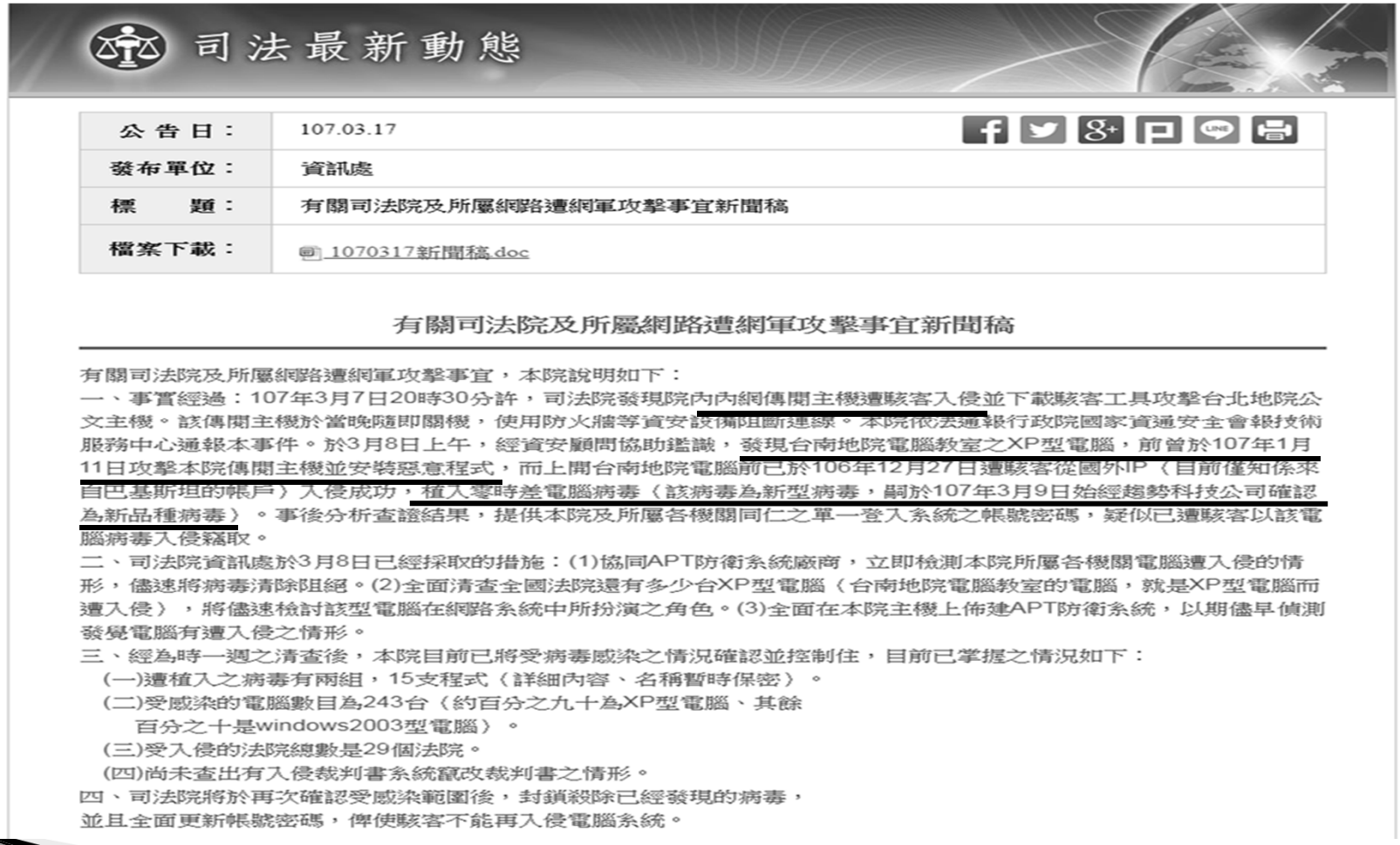


資料來源：iThome

調查局轉而聚焦於清查一銀內網的各種異常連線記錄，終於找到了在7月9日時大量來自海外一銀倫敦分行連線到臺灣ATM的記錄，發動大量連線的系統是倫敦分行的電話錄音伺服器。但是，一銀這家倫敦分行沒有ATM業務，不需連線回臺灣ATM，不應出現任何連線記錄，而對位於臺灣的ATM設備，也不應該出現對外的異常連線。調查局因此而能推斷，一銀倫敦分行就是造成這次事件的駭客入侵端點之一，駭客入侵了這臺伺服器做為跳板，再進一步攻入總行的ATM。

資料來源：TVBS

當電腦教室電腦成為攻擊小尖兵



司法最新動態

公告日：	107.03.17
發布單位：	資訊處
標　　題：	有關司法院及所屬網路遭網軍攻擊事宜新聞稿
檔案下載：	1070317新聞稿.doc

有關司法院及所屬網路遭網軍攻擊事宜新聞稿

有關司法院及所屬網路遭網軍攻擊事宜，本院說明如下：

一、事實經過：107年3月7日20時30分許，司法院發現院內內網傳閱主機遭駭客入侵並下載駭客工具攻擊台北地院公文主機。該傳閱主機於當晚隨即關機，使用防火牆等資安設備阻斷連線。本院依法通報行政院國家資通安全會報技術服務中心通報本事件。於3月8日上午，經資安顧問協助鑑識，發現台南地院電腦教室之XP型電腦，前曾於107年1月11日攻擊本院傳閱主機並安裝惡意程式，而上開台南地院電腦前已於106年12月27日遭駭客從國外IP（目前僅知係來自巴基斯坦的帳戶）入侵成功，植入零時差電腦病毒（該病毒為新型病毒，嗣於107年3月9日始經趨勢科技公司確認為新品種病毒）。事後分析查證結果，提供本院及所屬各機關同仁之單一登入系統之帳號密碼，疑似已遭駭客以該電腦病毒入侵竊取。

二、司法院資訊處於3月8日已經採取的措施：(1)協同APT防衛系統廠商，立即檢測本院所屬各機關電腦遭入侵的情形，儘速將病毒清除阻絕。(2)全面清查全國法院還有多少台XP型電腦（台南地院電腦教室的電腦，就是XP型電腦而遭入侵），將儘速檢討該型電腦在網路系統中所扮演之角色。(3)全面在本院主機上佈建APT防衛系統，以期儘早偵測發覺電腦有遭入侵之情形。

三、經為時一週之清查後，本院目前已將受病毒感染之情況確認並控制住，目前已掌握之情況如下：

(一)遭植入之病毒有兩組，15支程式（詳細內容、名稱暫時保密）。

(二)受感染的電腦數目為243台（約百分之九十為XP型電腦、其餘百分之十是windows2003型電腦）。

(三)受入侵的法院總數是29個法院。

(四)尚未查出有入侵裁判書系統竄改裁判書之情形。

四、司法院將於再次確認受感染範圍後，封鎖殺除已經發現的病毒，並且全面更新帳號密碼，俾使駭客不能再入侵電腦系統。

資安威脅已趨嚴峻

公部門防駭 今起資安演練到年底

2017-04-05

17

A+

〔記者李欣芳／台北報導〕近一年來中央與地方政府各公務機關不斷發生遭駭客攻擊的重要資安事件，甚至導致涉及洩漏民眾個資高達十三萬筆，引發各界的重視，行政院將從今天清明節連假後的第一天上班日起，展開全國各公務機關的資安演練，這項演練行動將持續到今年底。

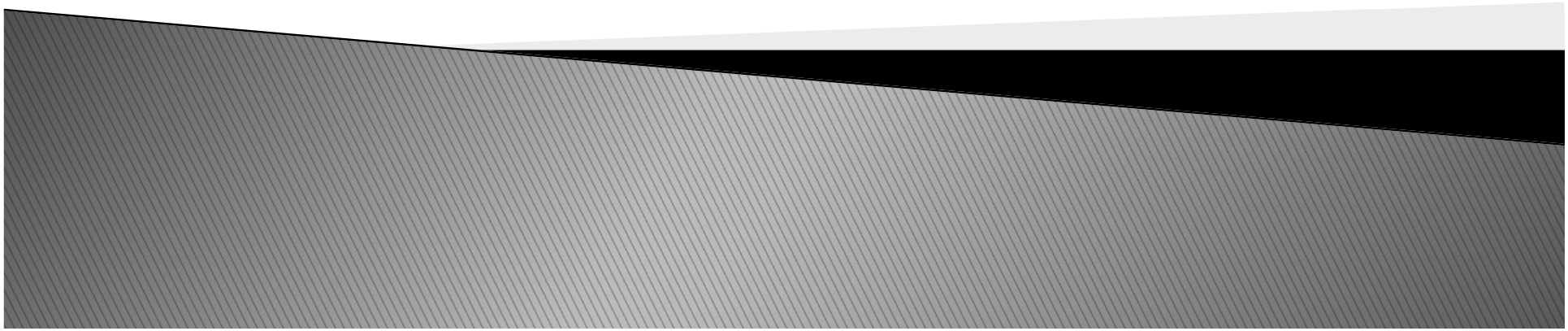
行政院相關官員表示，演練包括中央與地方政府的公部門，將由負責這次演練的官員擔任攻擊手，測試資安應變能力，因此不便透露由哪個部門開始進行演練。

由於民眾向公務機關申請相關業務時，依法必須提供個人資料才能申辦業務，不過，中華郵政去年五月發生個資遭竊，造成消費者個資外洩一萬七千多筆，勞動部去年十月被駭外洩三萬四千筆個資、台北市資訊局今年一月也外洩七萬筆個資，外交部今年二月更發生不明來源ＩＰ成功駭入我數十個外館領務信箱，導致國人登錄出國資料的一萬五千多筆個資外洩，外交部領務局更因此召開記者會致歉。

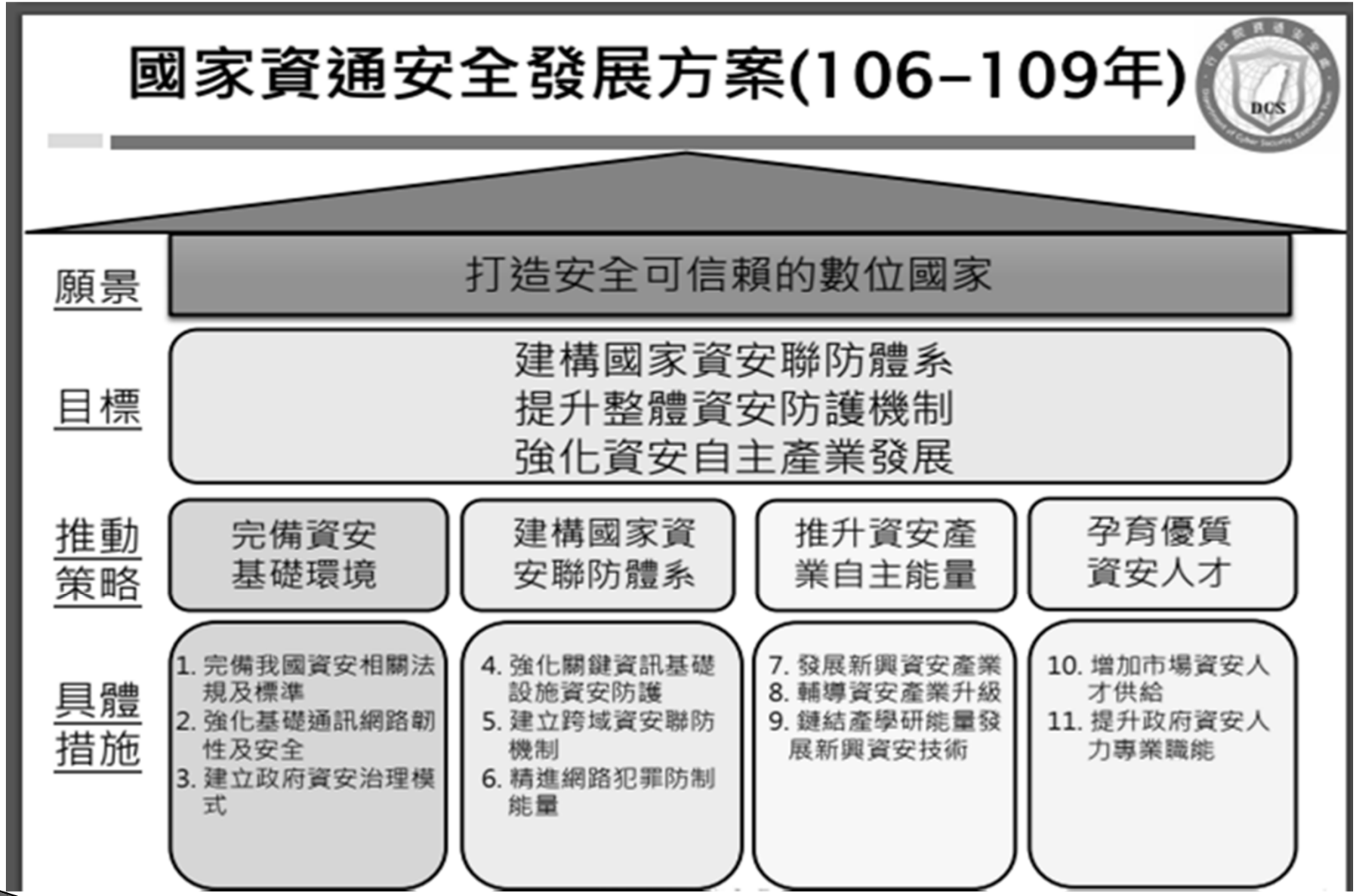
行政院官員表示，近期政府機關發生重大資安事件，行政院立即啟動個別專案資安查核進行檢討，並補強資安防護，這次資安演練也盼提升公部門的資安防護能量。

資料來源：自由時報

資通安全管理法之因應

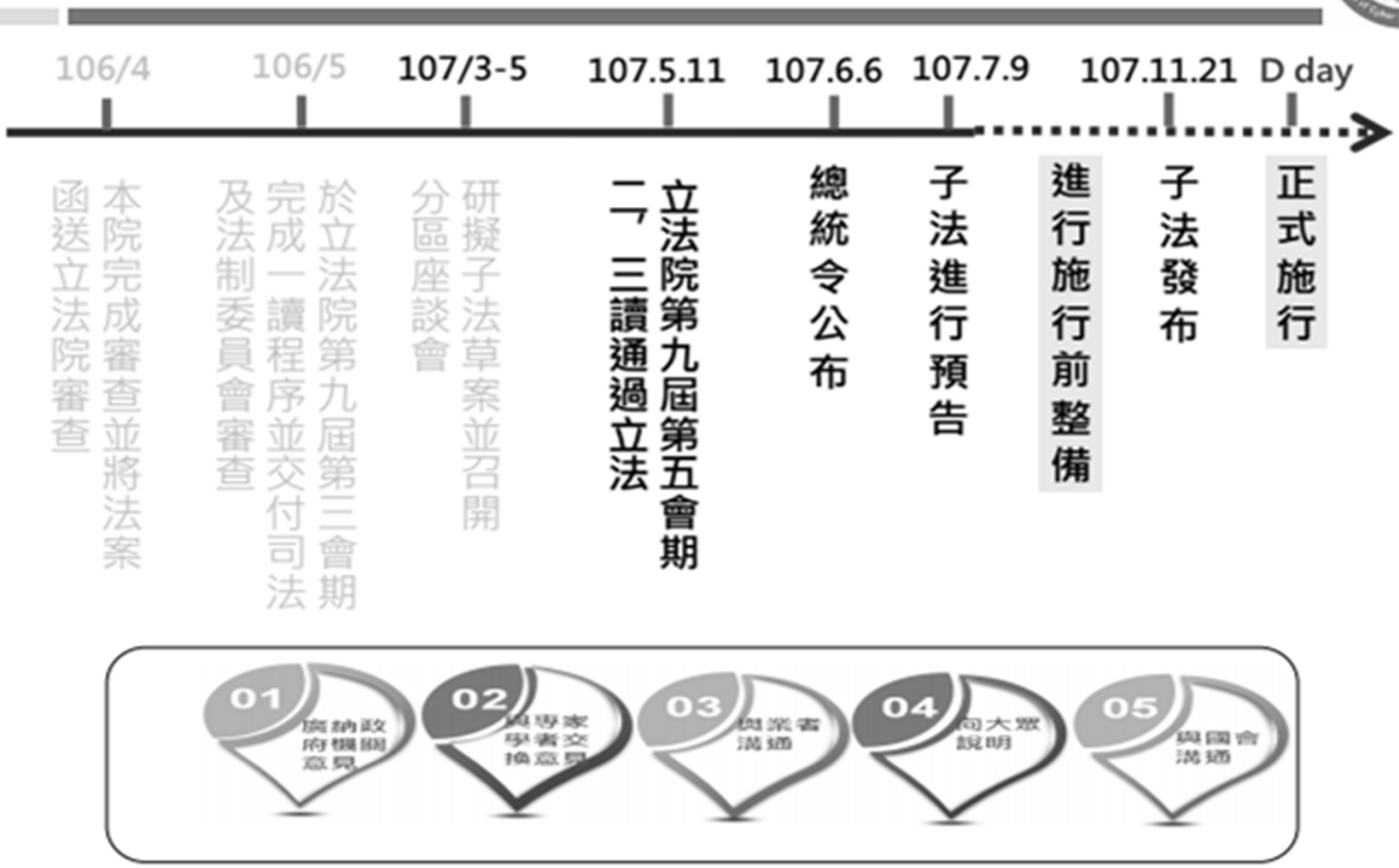


國家資通安全發展方案(106–109年)



資料來源：行政院資通安全處

資通安全法(資安法)立法歷程



資料來源：行政院資通安全處

公務機關資通安全管理

- 資安責任等級分級
- 資安維護計畫之制定與實施
- 資安長設置
- 年度資安維護計畫實施情形提出
- 資安稽核
- 改善報告
- 資安事件通報應變
- 公務機關人員獎懲標準

資通安全責任等級分級辦法

- 第六條 各機關維運自行或委外開發之資通系統者，其資通安全責任等級為 C 級。
- 第七條 各機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

資通安全責任等級 C 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		**每二年辦理一次。**
	業務持續運作演練		**全部核心資通系統每二年辦理一次。**

資通安全責任等級 C 級之公務機關應辦事項(con.)

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	網站安全弱點檢測	**全部核心資通系統每二年辦理一次。**
		系統滲透測試	**全部核心資通系統每二年辦理一次。**
	資通安全健診	網路架構檢視	**每二年辦理一次。**
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全防護	防毒軟體	初次受核定或等級變更後之**一年內**，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

資通安全責任等級 C 級之公務機關應辦事項(con.)

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年**至少一名人員各接受十二小時以上**之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者與主管	**每人每年接受三小時以上**之一般資通安全教育訓練
	資通安全專業證照及職能訓練證書	資通安全專業證照	**資通安全專職人員**總計應持有**四張以上**。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有一張以上，並持續維持證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

資通安全責任等級 D 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。

資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資 通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

資通系統防護基準

系統防護需求分級 控制措施		高	中	普
構面	措施內容			
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。

資通系統防護基準(con.)

稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。	一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三、應稽核資通系統管理者帳號所執行之各項功能。
	稽核紀錄內容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者

資通系統防護基準(con.)

				身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。
	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。		
	稽核處理失效之回應	一、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。	
	時戳及校時	一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二、等級「普」之所有控制措施。		資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
	稽核資訊之保護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。

資通系統防護基準(con.)

營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。		無要求。
識別與鑑別	內部使用者之	一、對帳號之網路或本機存取採取多重認證技術。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	

資通系統防護基準(con.)

	識別與鑑別	二、等級「中」及「普」之所有控制措施。	
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

資通系統防護基準(con.)

	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。	
	系統發展生命	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	無要求。

資通系統防護基準(con.)

	週期設計階段	二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，須注意版本控制與變更管理。 二、等級「普」之所有控制措施。	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	
	獲得程序	開發、測試及正式作業環境應為區隔。	無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。	

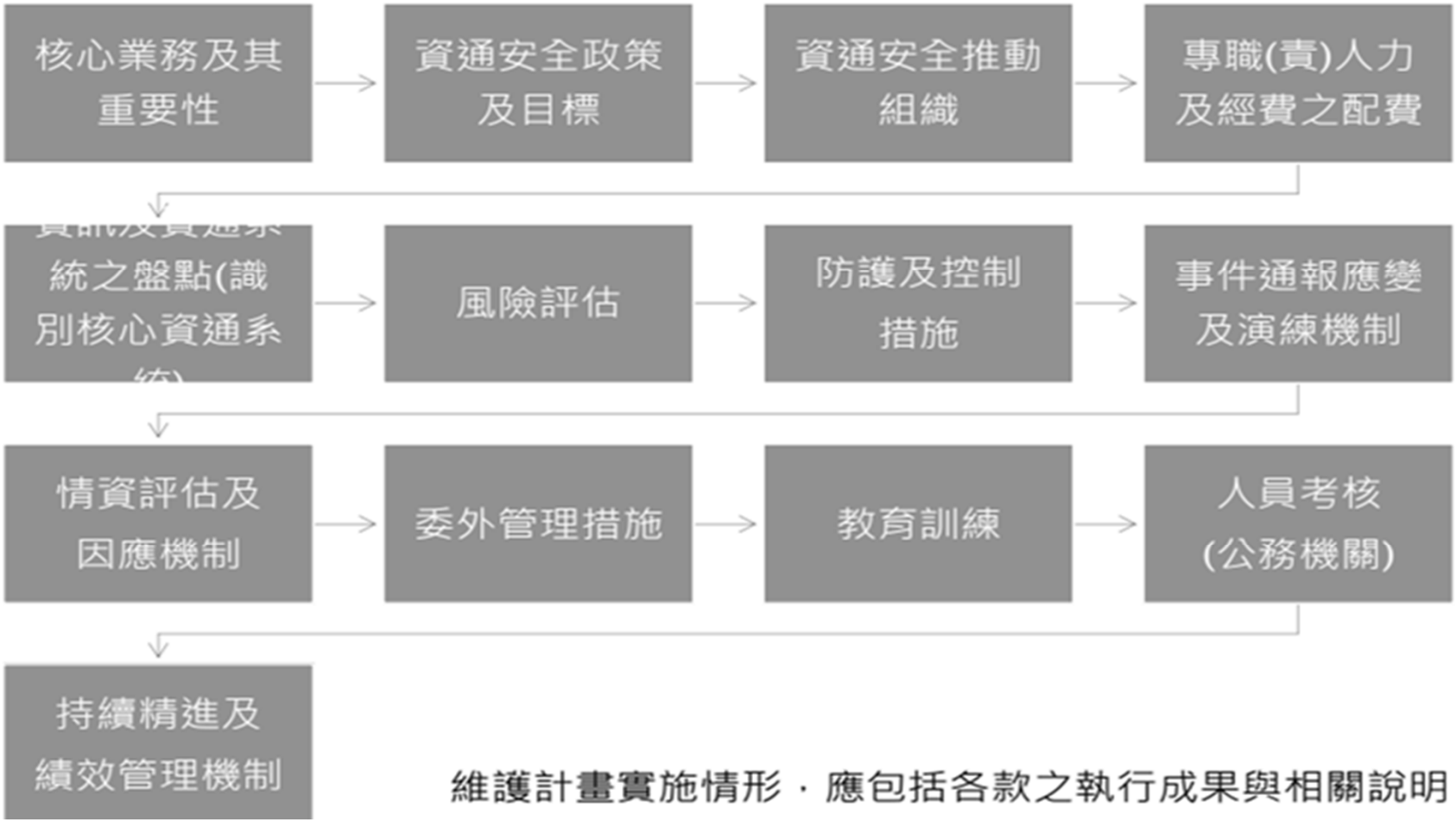
資通系統防護基準(con.)

系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。	無要求。	無要求。
		四、加密金鑰或憑證週期性更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。		
	資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。

資通系統防護基準(con.)

系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。

資通安全維護計畫



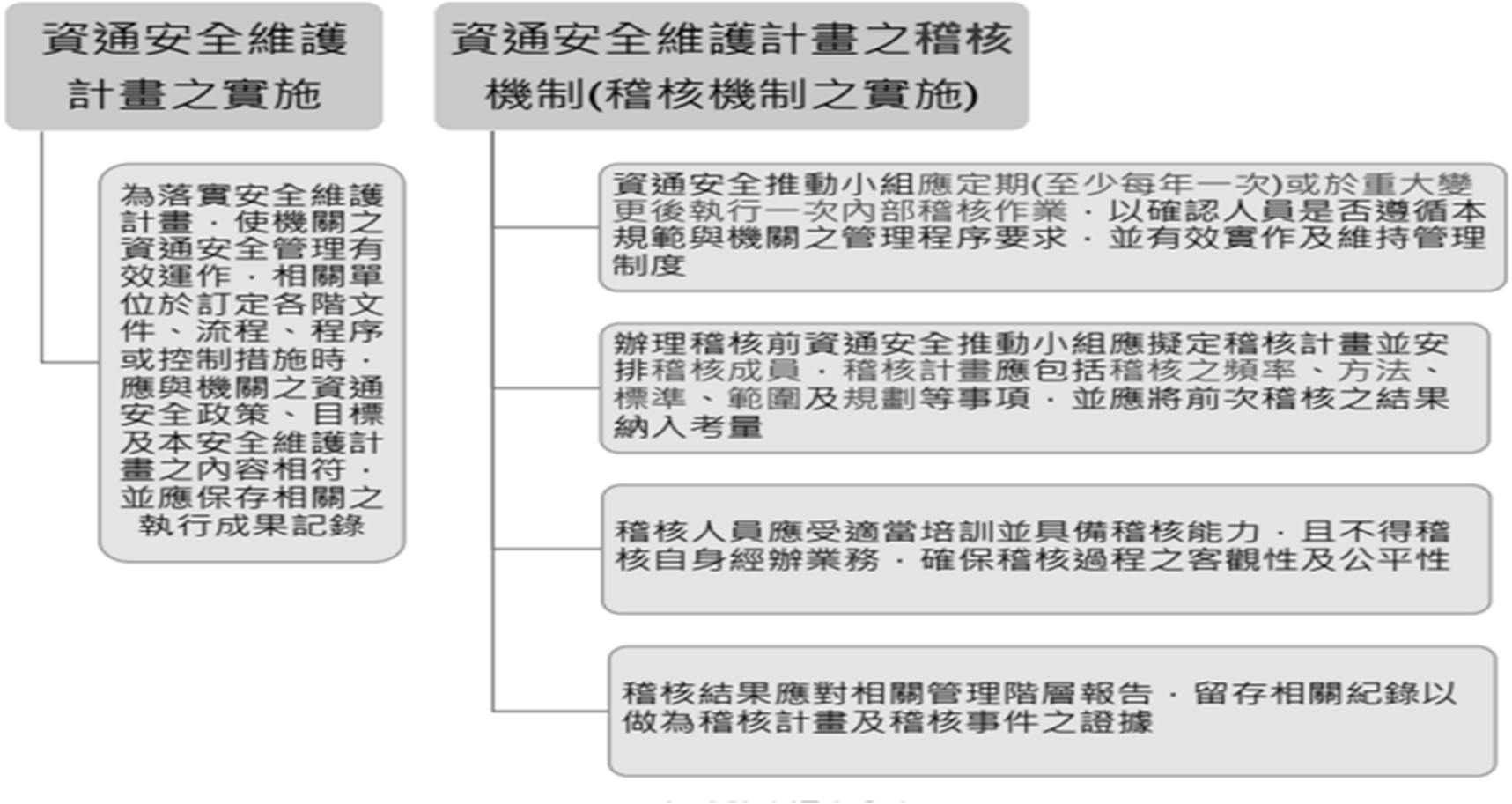
維護計畫實施情形，應包括各款之執行成果與相關說明。

資料來源：行政院資通安全處

資通安全維護計畫注意事項

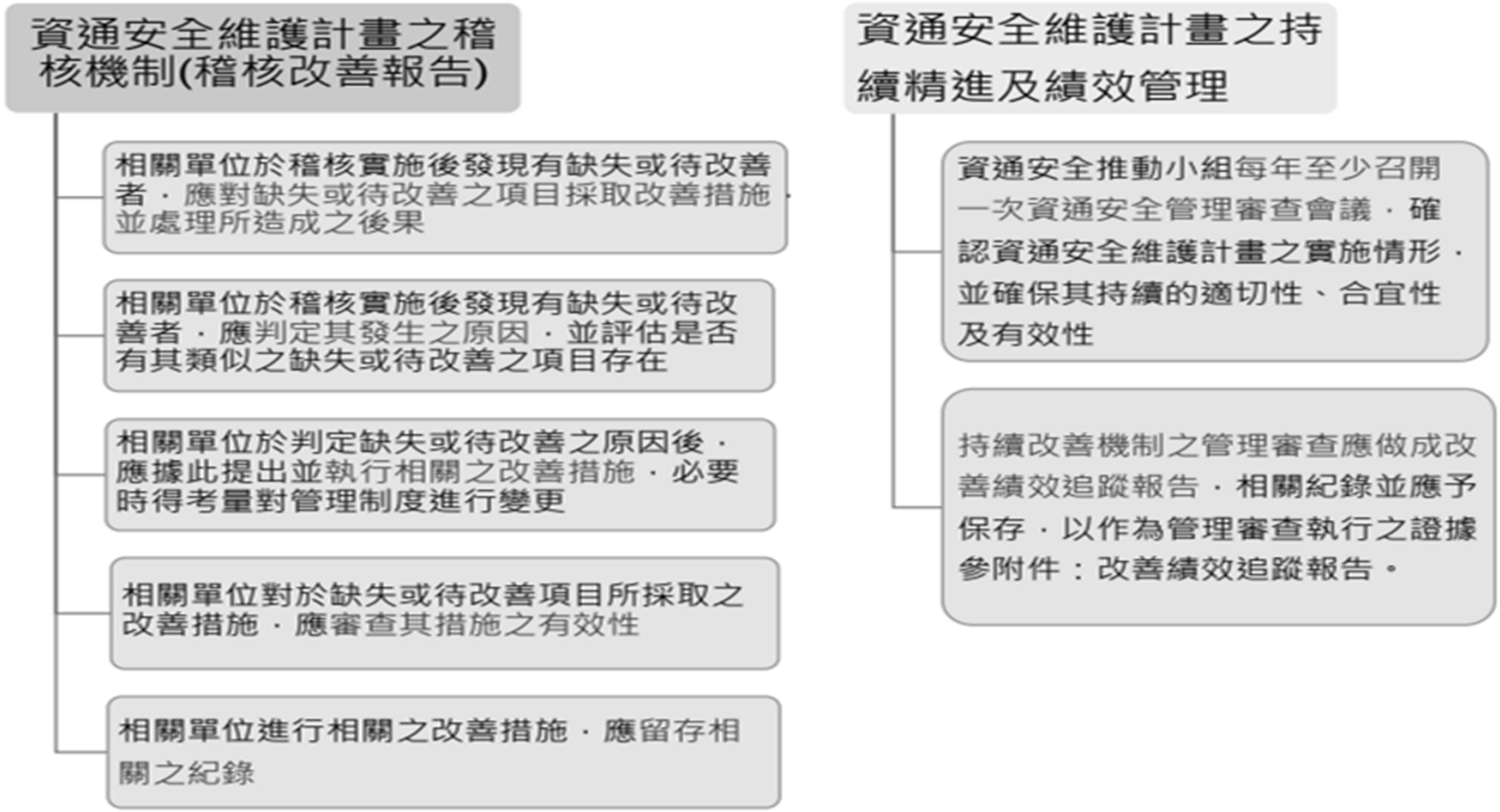
- 資通安全維護計畫內容，應包括資通安全管理法施行細則第6條規定之項目。另外，資通安全責任等級分級辦法之應辦事項亦應納入其中。
- 資通安全維護計畫內容，其適用範圍得包含本機關與所屬機關，惟內容應載明各自應遵循項目。
- 機關如已有資安規定與程序者，資通安全維護計畫內之項目，得直接引述內部文件編號及名稱。

資通安全維護計畫及實施情形之持續精進及績效管理



資料來源：行政院資通安全處

資通安全維護計畫及實施情形之持續精進及績效管理(con.)



資料來源：行政院資通安全處

資通安全維護計畫及實施情形之持續精進及績效管理(con.)

- 管理審查議題應包含下列討論事項
  - 過往管理審查議案之處理狀態
  - 與資訊安全管理系統有關之內外部議題變更，如法令變更、上級機關要求、資通安全推動小組決議事項等
  - 資通安全維護計畫內容之適切性
  - 資訊安全績效之回饋，包括：
    - 資通安全政策及目標之實施情形
    - 資通安全人力及資源之配置之實施情形
    - 資通安全防護及控制措施之實施情形
    - 內外部稽核結果
    - 不符合項目及矯正措施
  - 風險評鑑結果及風險處理計畫執行進度
  - 重大資通安全事件之處理及改善情形
  - 利害關係人之回饋
  - 持續改善之機會

資通安全維護計畫實施情形之提出

- 機關依據資通安全管理法第12(16,17)條之規定，應向上級或監督機關、中央目的事業主管機關，提出資通安全維護計畫實施情形，使其得了解機關之年度資通安全計畫實施情形
- 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項

資安事件等級綜合評估表

	機密性 資訊洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作遭中斷	
	資訊性質	影響程度	業務資訊/資通系統	影響程度	業務	可否於可容忍中斷時間回復
1級	非核心業務	輕微	非核心	輕微	非核心業務	可
2級	非核心業務	嚴重	非核心	嚴重	非核心業務	不可
	核心業務 (未涉及CI維運)	輕微	核心 (未涉及CI維運)	輕微	核心/資通系統 (未涉及CI維運)	可
	核心業務 (未涉及CI維運)	嚴重	核心 (未涉及CI維運)	嚴重	核心/資通系統 (未涉及CI維運)	不可
3級	核心業務 (涉及CI維運)	輕微	核心 (涉及CI維運)	輕微	核心/資通系統 (涉及CI維運)	可
	一般公務機密、敏感資訊	輕微	一般公務機密、敏感資訊	輕微		
	核心業務 (涉及CI維運)	嚴重	核心 (涉及CI維運)	嚴重	核心/資通系統 (涉及CI維運)	不可
4級	一般公務機密、敏感資訊	嚴重	一般公務機密、敏感資訊	嚴重		
	國家機密	-	國家機密	-		

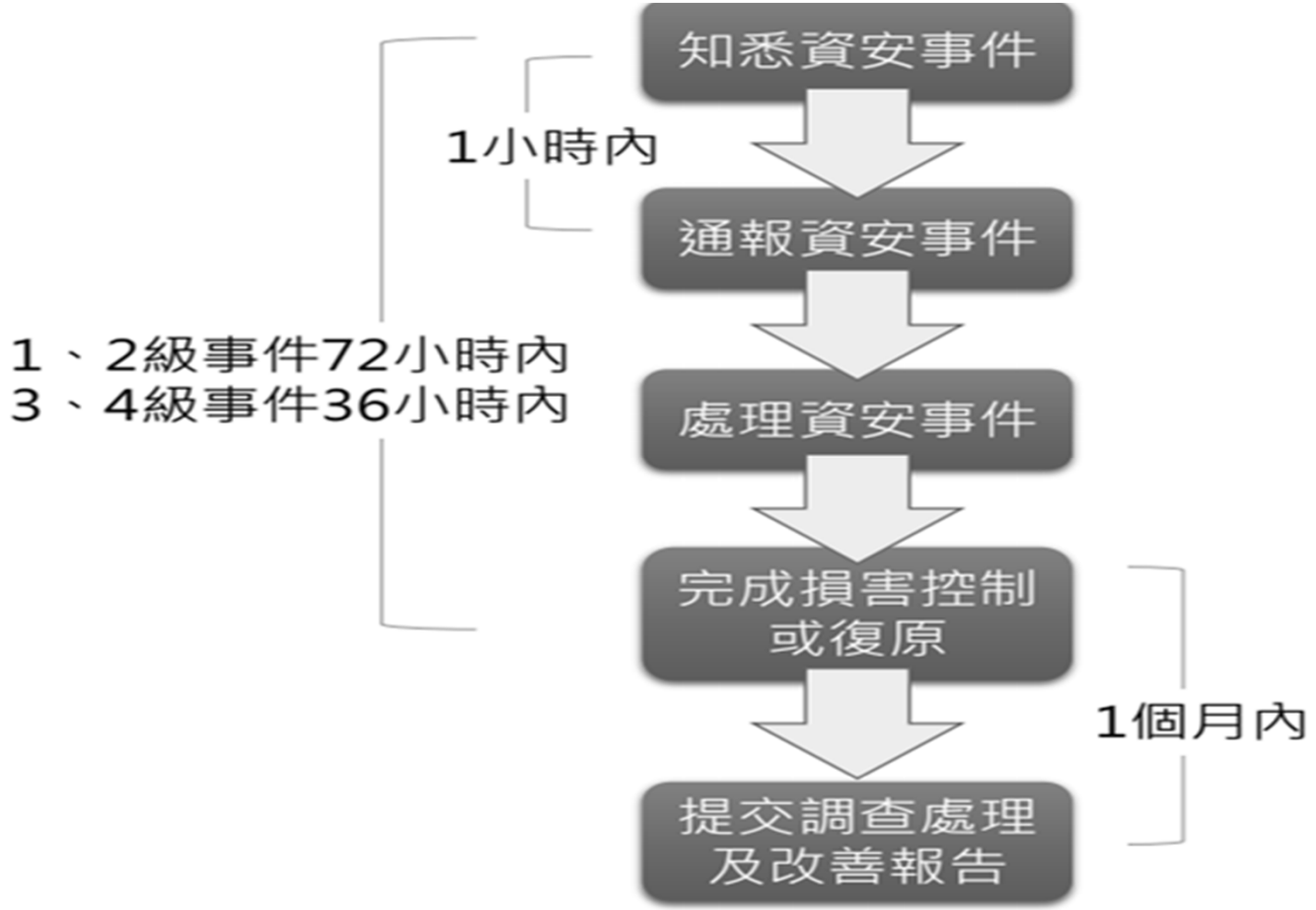
資料來源：行政院資通安全處

資安事件等級綜合評估表(con.)

	機密性 資訊洩漏		完整性 資訊/資通系統遭竄改		可用性 業務/資通系統運作遭中斷	
影響程度 業務性質/資通系統別	洩漏程度		竄改程度		可否於可容忍時間內回復	
	輕微	嚴重	輕微	嚴重	可	不可
非核心業務	1級	2級	1級	2級	1級	2級
非核心資通系統			1級	2級		
未涉及CI維運之核心業務	2級	3級	2級	3級	2級	3級
未涉及CI維運之核心資通系統			2級	3級	2級	3級
涉及CI維運之核心業務	3級	4級	3級	4級	3級	4級
涉及CI維運之核心資通系統			3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級		4級			

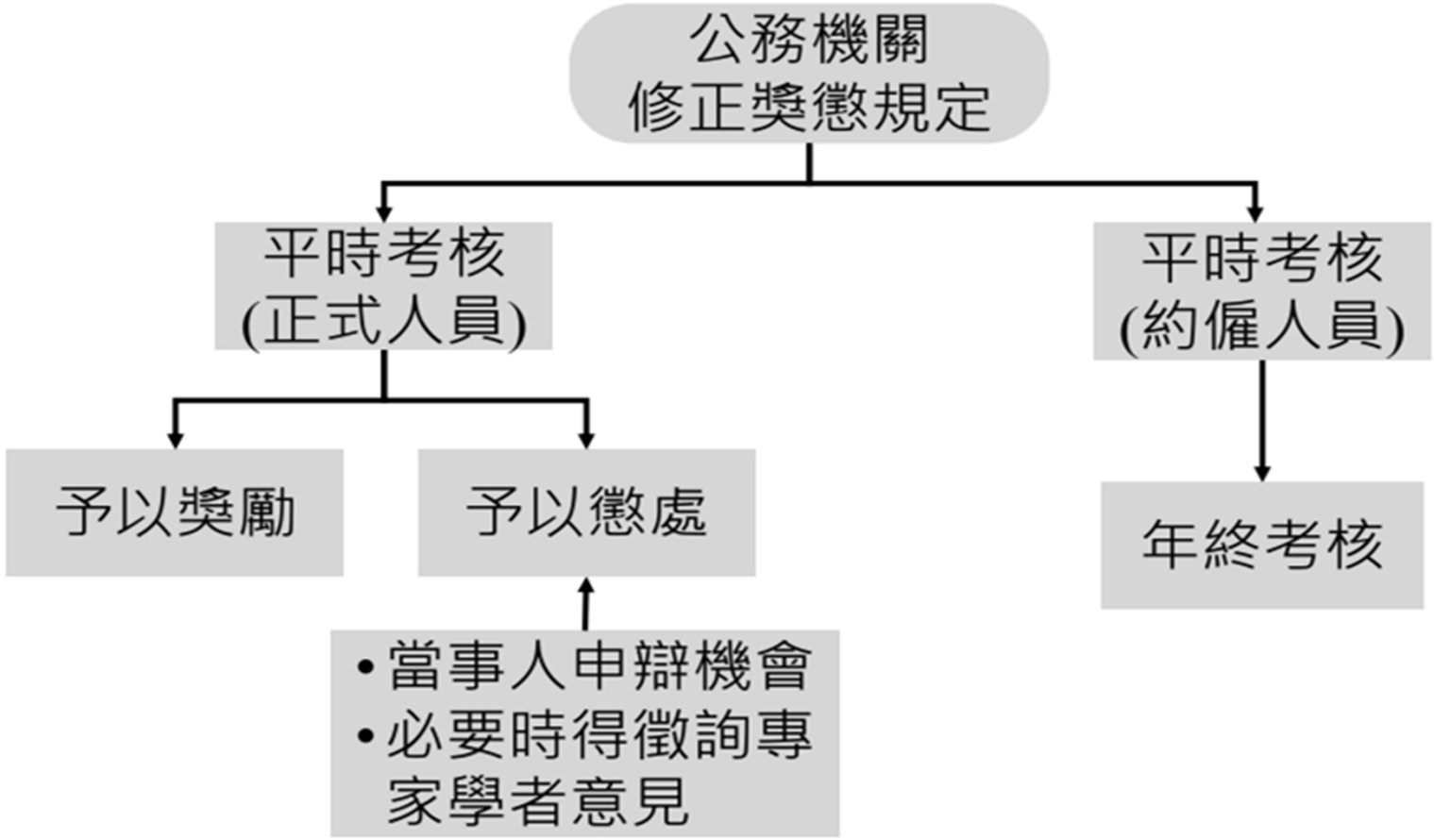
資料來源：行政院資通安全處

通報作業流程各項目時限



資料來源：行政院資通安全處

公務機關人員獎懲標準



資料來源：行政院資通安全處

公務機關人員獎懲標準(con.)

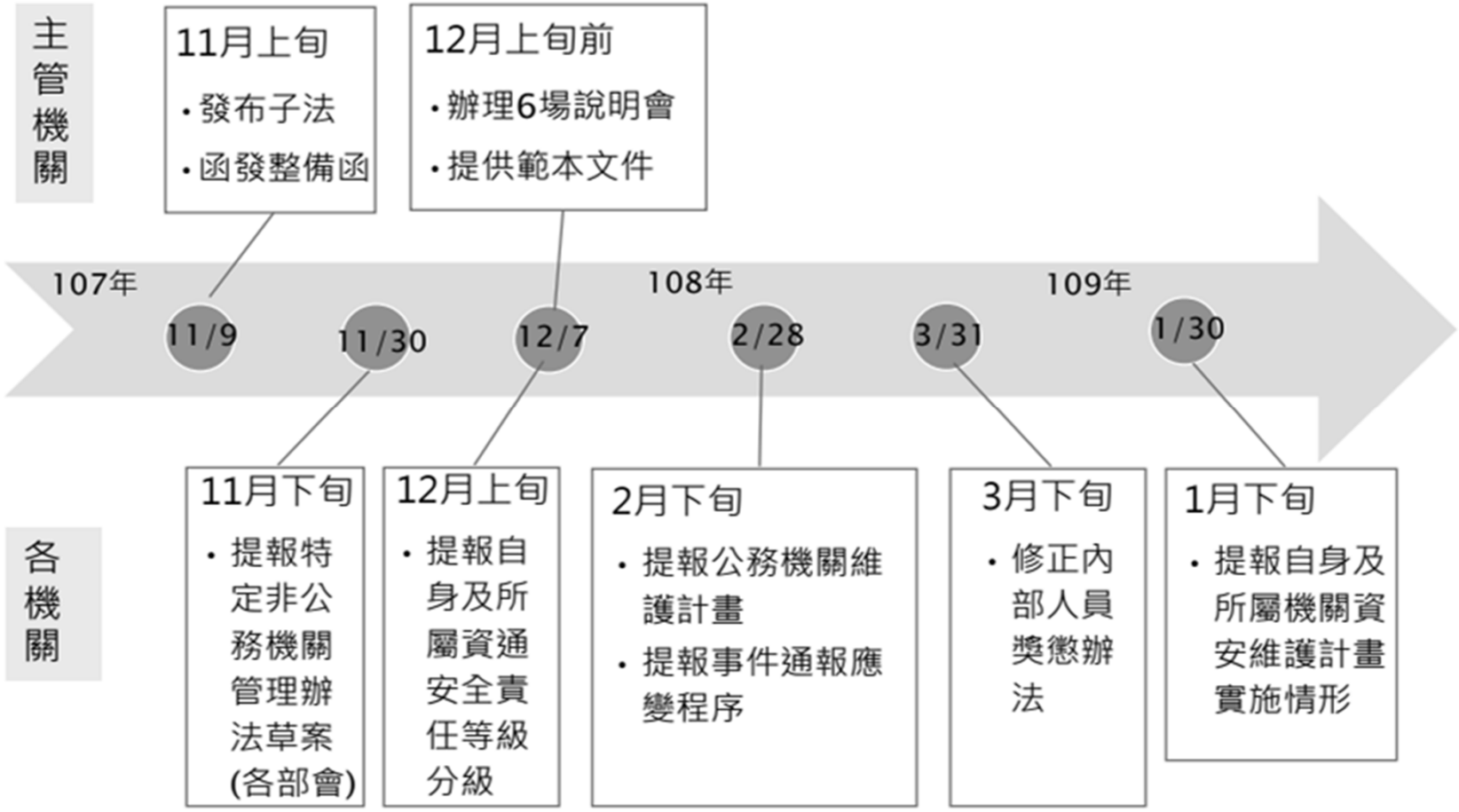
- 獎勵項目
  - 訂定、修正及實施資通安全維護計畫，績效優良
  - 稽核所屬或辦理資通安全演練作業，績效優良。
  - 配合主管機關、上級或監督機關辦理稽核或資通安全演練作業，經評定績效優良。
  - 積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。
  - 辦理其他資通安全業務有具體功績。

  (其餘可參考獎懲辦法第3條，共有12款事宜)

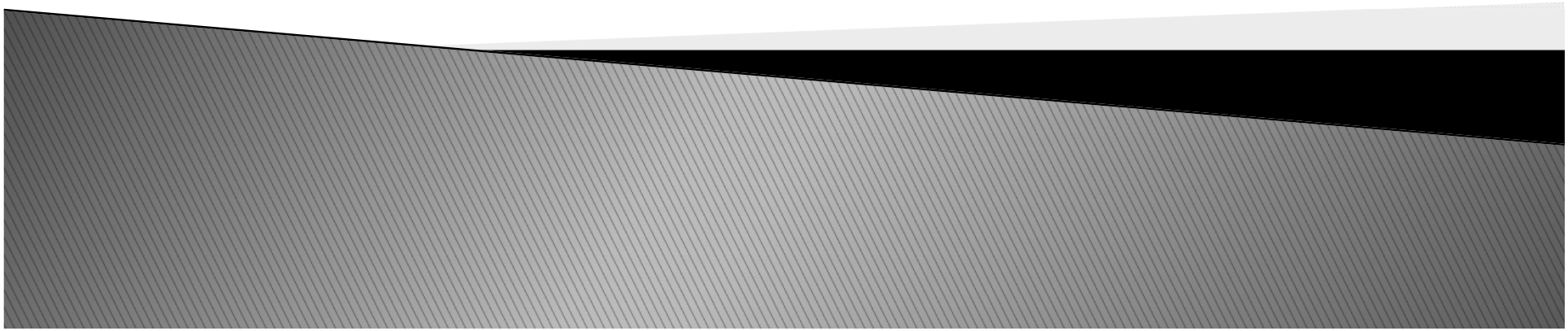
- 懲處項目
  - 未依本法、本法授權訂定之法規或機關內部規範辦理資通安全管理事項(維護計畫、事件通報應變、稽核、情資分享)，情節重大。
  - 辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。
  - 其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

資料來源：行政院資通安全處

後續施行時程


主管機關
11月上旬
・發布子法
・函發整備函
12月上旬前
・辦理6場說明會
・提供範本文件
107年
108年
109年
11/9
11/30
12/7
2/28
3/31
1/30
各機關
11月下旬
・提報特定非公務機關管理辦法草案(各部會)
12月上旬
・提報自身及所屬資通安全責任等級分級
2月下旬
・提報公務機關維護計畫
・提報事件通報應變程序
3月下旬
・修正內部人員獎懲辦法
1月下旬
・提報自身及所屬機關資安維護計畫實施情形

個人資安防護



個資外洩事件方興未艾

Quora遭駭客入侵！1億用戶個資裸奔　姓名、郵件全外洩

0:00 / 2:44

萬豪酒店集團遭駭　全球5億客戶資料恐外洩

0:00 / 2:10

資料來源：ETToday

個資被洩漏真的沒什麼大不了？

請輸入您的 MasterCard® SecureCodeTM 密碼。

特約商店: SHEN FAN
交易金額: TWD 24.00
交易日期: 12:08:22
卡 號: XXXX XXXX XXXX
請選擇認證密碼種類: 3D認證密碼 / 動態認證密碼
SecureCodeTM 密碼
送出 說明 取消

注意事項:

1. 已完成註冊設定認證密碼之客戶可直接輸入認證密碼
2. 忘記密碼或未完成註冊之客戶，請點選動態認證密碼後，按取『取得認證密碼』按鍵，本行將於一到二分鐘內以簡訊和E-Mail傳送交易認證密碼。
3. 若您無法完成交易或是未收到認證密碼，請與客服中

銀行還會為盜刷買單？

信用卡被盜刷上萬元！因為這設定...銀行要她先買單

2018-03-28 17:00 東森新聞

字級：字 字

▲（示意圖／翻攝自Pixabay）

桃園一位黃小姐去年12月遭盜刷1萬多元，她報案跟台中銀行反應，銀行查出她用3D驗證的自設固定密碼，認為黃小姐疏於保管，要她先付款，但事情鬧大後，銀行改列「爭議款項」免賠了，先等警方抓到凶手再求償。

資料來源：東森新聞

求償當事人！那被害使用者呢？

求職者個資被「轉送」　1111：將求償當事人、加強保護

2018/03/31 11:59:00　友善列印　加入好友　G+　A-　A　A+

記者葉立斌 / 台北報導

相信有使用過人力銀行的網友都知道，有項功能是關閉特定職業話，但如果你已經封鎖，卻又不斷接到這類的電話，就該當心。

30日驚爆人力銀行個資外流案件，而外流方式並非遭駭。調查發現徵才帳號密碼交給保險業務員，由保險業務蒐集求職者個資，另外並向檢方舉報，台北市調查處搜索該公司並依違反《個人資料保護談負責人與員工，而該保險業務不在國內，將擇期傳喚。

1111人力銀行副總經理何啟聖表示，徵才企業如在網站上有不符常態的動作，例如只開一個職缺，卻大量瀏覽求職者的履歷，便會嚴格監督。而近期有不少求職者反映，明明已經關閉「保險、直銷」兩種類型職業，卻仍頻繁接到電話。人力銀行立即向檢調舉發此事。

何啟聖表示，何啟聖表示，有時業者會用廠商徵才名義，將獲取的個人資料挪作他用，只要確定有此事，便會將該公司停權並求償。另外他強調，這是一項「官民聯手，打擊不法」的成功案例。未來1111人力銀行將會加強系統巡邏，揪出異常行為。

資料來源：三立新聞網

政府帶頭做示範真是好棒棒

為免愛滋患者二度傷害 沒告知個資外洩

中國廣播公司
發布時間 2018年6月20日 PM 3點52分
更新時間 2018年6月20日 PM 4點27分

♥ 0　💬 0

臺北市立聯合醫院2年前得知有3千多筆愛滋病患者資料外洩，卻沒有通知患者，可能有損患者權益。衛生福利部疾病管制署副署長羅一鈞表示，由於感染者名單和外洩的簡報檔案綁在一起，為避免患者被告後，到網路搜尋相關檔案，不排除可能因此刺激到還持有檔案的人，做出更不當的舉動，因此有關單位與專家討論後，沒有逐一通知個資外洩的患者。

羅一鈞：『在我們能夠處理的範圍之內，避免引起二度傷害跟資安更大的疑慮，所以我們當時跟市政府這邊也是決定，就是說他們沒有要逐筆通知當事人，也沒有採用對外公布的方式。因為網路時代其實個資外洩最可怕的，就是有一些好事者或有心人士，會就這個個資的持有跟散佈，去做一些匿名、大規模的動作。』

羅一鈞表示，不是每個愛滋感染者都希望被通知個資遭外洩，政府的處理已告一段落，再告知只會增添患者的擔憂，事件經媒體報導可能引起感染者恐慌，北市府已提供專線專人說明和權益諮詢，與心理諮商服務。

此外，公務機關洩露個資，依規定當事人若能舉證權益受損，可向政府求償，人數較多可提出團體訴訟，有需求的患者可向北市府或愛滋相關團體提出。

（圖：資料照片，戎華儀攝）

資料來源：Line Today

當使用者變成豬隊友時...

自由時報 Liberty Times Net

即時新聞 ▾ 報紙總覽 ▾ 影音 娛樂 汽車 時尚 體育 3C 評論 食譜 健康

首頁 > 即時 > 社會

高市警官網洩報案人個資 刑大懲處失職人員

讚 LINE

2017-06-25 11:02

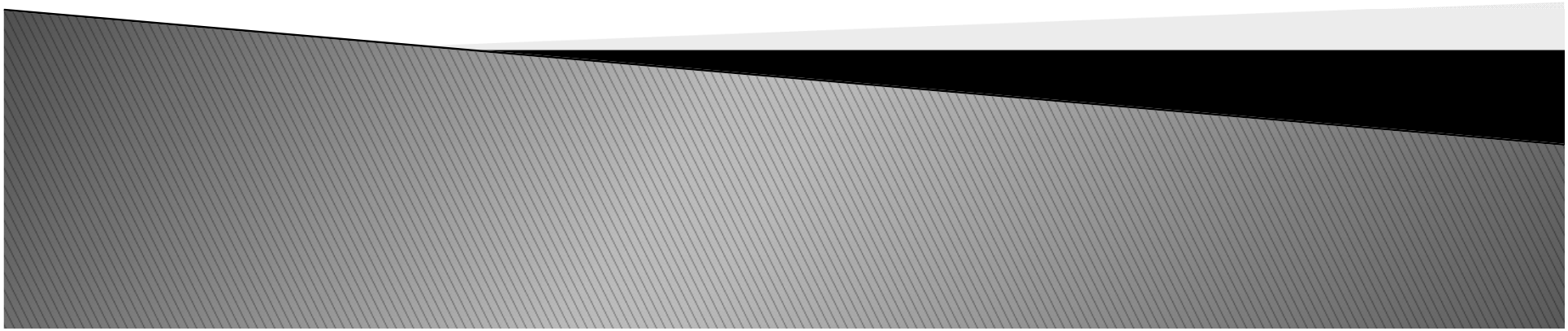
〔記者黃建華／高雄報導〕馬姓男子去年發現鄰居死亡多日，向警方報案，不料本月22日朋友瀏覽高雄市警局全球資訊網，赫見馬的名字、出生年月日、身分證字號、手機號碼等個資，都被高市警局官網公佈，馬姓男子因此向媒體投訴；對此，高雄市刑大司法組今天上午坦承承辦人員疏忽，已刪除相關民眾個資，同時將行政懲處失職人員。

負責管理高雄市警局全球資訊網的高雄市警局資訊室主任李德智表示，無名屍公告是開放給刑大司法組，由承辦人將相關資訊上傳到高雄市警局全球資訊網，22日才發現有洩露報案人個資的問題，晚間先下架公告，將報案人個資適當隱匿後，再重新上傳，日後也會加強審核，杜絕報案人的個資外洩。

高雄市刑大司法組則表示，當初是急於讓「無名屍」提供民眾認領，以利殯葬，將受理報案單位、時間上

真的不要輕易的以為資安事故處理完畢了！

結論



你願意接受多少錢出賣自己的個資？

劍橋分析給我們的省思.....

國際 國際焦點

祖克柏承認犯錯！ 「劍橋分析」竊臉書5千萬用戶資料 助川普贏大選

0:00 / 6:12

記者楊絡懸／綜合外電報導

美國臉書（Facebook）被英國數據分析公司「劍橋分析」（Cambridge Analytica）假借學術研究名義，利用心理測驗等應用程式，在2014到2015年間蒐集5000萬用戶個人資料，存取使用後，違法轉賣給第三方分析，針對用戶的政治立場投放特定廣告，企圖影響英國脫歐公投與美國總統大選選情。對此，臉書執行長兼創辦人祖克柏（Mark Zuckerberg）21日終於出面解釋，發表聲明承認犯錯。

資料來源：ETtoday

Google也無可倖免

Google+外洩50萬個資！用戶照片地址全曝光　谷歌刻意隱瞞才關閉

▶ 0:00 / 3:02

▲Google被爆出軟體漏洞。（圖／路透社）

國際中心／綜合報導

網路搜尋引擎「Google」8日承認因軟體漏洞，導致2015年至2018年期間，外部開發人員可以任意觀看Google+用戶的個人資料，導致50萬名用戶受到影響，這些資料都洩漏給外部開發商，嚴重的個資外洩。然而，Google內部開會卻決定在第一時間刻意隱瞞事件經過，不讓用戶知道詳細狀況，直到消息曝光後，Google才宣告要關閉Google+社群服務。

根據《華爾街日報》報導，2015年至2018年這段期間，Google出現軟體漏洞，外步開發人員可以任意訪問Google+用戶的個人資料數據，其中包括姓名、電子郵件地址、出生日期、性別、個人資料照片、居住地、職業和關係狀態等，將近有50萬Google+用戶受到影響，所幸個人通訊錄和電話號碼等資料沒有曝光。

資料來源：ETtoday

資安防護建議

- 使用者
  - 確保所有的安全軟體處於最新版本。
  - 將手機納入安全保護中。
  - 提高密碼複雜度並定期更改。
  - 定期確認自己的銀行帳戶和行動付費。
  - 永遠留意你的網路使用行為。
- 企業
  - 使用有效的解決方案保護你的企業。
  - 為客戶的利益做好把關。
  - 建立和落實有效的IT使用規範。

資料來源：資安人