資通安全管理法之簡介與因應

資通安全管理法之簡介與因應

資訊工業策進會科技法律研究所
2019年6月25日

壹、事件摘要

隨著網路科技的進步，伴隨著資安風險的提升，世界各國對於資安防護的意識逐漸升高，紛紛訂定相關之資安防護或因應措施。為提升國內整體之資通安全防護能量，我國於107年5月經立法院三讀通過「資通安全管理法」（以下簡稱資安法），並於同年6月6日經總統公布，期望藉由資通安全管理法制化，有效管理資通安全風險，以建構安全完善的數位環境。觀諸資通安全管理法共計23條條文外，另授權主管機關訂定「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」及「公務機關所屬人員資通安全事項獎懲辦法」等六部子法，建置了我國資通安全管理之法制框架。然而，資安法及相關子法於108年1月1日實施後，各機關於適用上不免產生諸多疑義，故本文擬就我國資通安全管理法之規範重點為扼要說明，作為各機關遵法之參考建議。

貳、重點說明

一、規範對象

資安法所規範之對象，主要可分為公務機關及特定非公務機關。公務機關依資安法第3條第5款之定義，指依法行使公權力之中央、地方機關（構）或公法人，但不包含軍事機關及情報機關。故公務機關包含各級中央政府、直轄市、縣（市）政府機關、依公法設立之法人（如農田水利會[1]、行政法人[2]）、公立學校、公立醫院等，均屬公務機關之範疇。惟考量軍事及情報機關之任務性質特殊，故資安法排除軍事及情報機關之適用[3]。

特定非公務機關依資安法第3條第6款之規定，指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。關鍵基礎設施提供者另依該法第16條第1項規定，須經中央目的事業主管機關於徵詢相關公務機關、民間團體、專家學者之意見後指定，報請行政院核定，並以書面通知受核定者。須注意者為該指定行為具行政處分之性質，如受指定之特定非公務機關對此不服，則可循行政救濟程序救濟之。目前各關鍵基礎設施領域，預計將於108年下半年陸續完成關鍵基礎設施提供者之指定程序[4]。

此外，政府捐助之財團法人，依該法第3條第9項之規定，指其營運及資金運用計畫應依預算法第41條第3項規定送立法院，及其年度預算書應依同條第4項規定送立法院審議之財團法人。故如為地方政府捐助之財團法人，則非屬資安法所稱特定非公務機關之範圍。公營事業之認定，則可參考公營事業移轉民營條例第3條之規定，指（一）各級政府獨資或合營者；（二）政府與人民合資經營，且政府資本超過百分之五十者；（三）政府與前二款公營事業或前二款公營事業投資於其他事業，其投資之資本合計超過該投資事業資本百分之五十者。目前公營事業如臺灣電力股份有限公司、中華郵政股份有限公司、臺灣自來水股份有限公司等均屬之。

二、責任內容

資安法之責任架構，可區分為「事前規劃」、「事中維運」及「事後改善」等三個階段，分述如下：

（一）事前規劃

就事前規劃部分，資安法要求各公務機關及特定非公務機關均應先規劃及訂定「資通安全維護計畫」及「資通安全事件通報應變機制」，使各機關得據此落實相關之資安防護措施，各機關並應依據資通安全責任等級分級辦法之規定，依其重要性進行責任等級之分級，辦理分級辦法中所要求之應辦事項[5]，並將應辦事項納入安全維護計畫中。

此外，在機關所擁有之資通系統[6]部分，各機關如有自行或委外開發資通系統，尚應依據分級辦法就資通系統進行分級（分為高、中、普三級），並就系統之等級採取相應之防護基準措施，以高級為例，從7大構面中，共須採取75項控制措施。

（二）事中維運

事中維運部分，資安法要求各機關應定期提出資通安全維護計畫之實施情形，上級或中央目的事業主管機關並應定期進行各機關之實地稽核及資通安全演練作業。各機關如有發生資通安全事件，應於機關知悉資通安全事件發生時，於規定時間內[7]，依機關訂定之通報應變機制採取資通安全事件之通報及損害控制或復原措施，以避免資通安全事件之擴大。

（三）事後改善

在事後改善部分，如各機關發生資通安全事件或於稽核時發現缺失，則均應進行相關缺失之改善，提出改善報告，並應針對缺失進行追蹤評估，以確認缺失改善之情形。

三、情資分享

為使資通安全情資流通，並考量網路威脅可能來自於全球各地，資安法第8條規定主管機關應建立情資分享機制，進行情資之國際合作。情資分享義務原則於公務機關間，就特定非公務機關部分，為鼓勵公私間之協力合作，故規定特定非公務機關得與中央目的事業主管機關進行情資分享。

我國已於107年1月將政府資安資訊分享與分析中心（G-ISAC）調整提升至國家層級並更名為「國家資安資訊分享與分析中心」（National Information Sharing and Analysis Center, N-ISAC）。透過情資格式標準化與系統自動化之分享機制，提升情資分享之即時性、正確性及完整性，建立縱向與橫向跨領域之資安威脅與訊息交流，以達到情資迅速整合、即時分享及有效應用之目的[8]。

四、罰則

為使資安法之相關規範得以落實，資安法就公務機關部分，訂有公務機關所屬人員資通安全事項獎懲辦法以資適用。公務機關應依據獎懲辦法之內容，配合機關內部之人事考評規定訂定獎懲基準，而獎懲辦法適用之人員，除公務人員外，尚包含機關內部之約聘僱人員。就特定非公務機關部分，資安法則另訂有相關之罰則，針對未依資安法及相關規定辦理應辦事項之特定非公務機關，中央目的事業主管機關得令限期改正，並按情節處10萬至100萬元之罰鍰。惟就資通安全事件通報部分，因考量其影響範圍層面較廣，故規定特定非公務機關如未依規定進行通報，則可處以30萬元至500萬元之罰鍰。

參、事件評析

公務機關及特定非公務機關為落實資安法之相關規範，勢必投入相關之資源及人力，以符合資安法之要求。考量公務機關或特定非公務機關之資源有限，故建議可從目前組織內部所採用之個人資料保護或資訊安全管理措施進行盤點與接軌，以避免資源或相關措施重複建置，以下則列舉幾點建議：

一、風險評估與安全措施

資安法施行細則第6條要求安全維護計畫訂定風險評估、安全防護及控制措施機制，與個人資料保護法施行細則第12條要求建立個人資料風險評估及管理機制之規定相似，故各機關於適用上可協調內部之資安與隱私保護機制，共同擬訂單位內部之風險評估方式與管理措施規範。

二、通報應變措施

資安法第18條要求機關應訂定資通安全事件通報應變機制，而個人資料保護法第12條亦規定有向當事人通知之義務，兩者規定雖不盡相同，惟各機關於訂定通報應變機制上，可將兩者通報應變程序進行整合，以簡化通報流程。

三、委外管理監督

資安法第9條要求機關負有對於委外廠商之監管義務，個人資料保護法施行細則第8條亦訂有委託機關應對受託者為適當監督之規範。兩者規範監督之內容雖不同，惟均著重對於資料安全及隱私之保護，故各機關可從資料保護層面著手，訂定資安與個人資料保護共同之檢核項目，來進行委外廠商資格之檢視，並將資安法及個人資料保護法之相關要求分別納入委外合約中。

四、資料盤點及文件保存

資安法施行細則第6條要求於建置安全維護計畫時，須先進行內部之資產盤點及分級，而個人資料保護法施行細則第12條中，則要求機關須訂有使用記錄、軌跡資料及證據保存之安全措施。故各機關於資產盤點時，可建立內部共同之資料盤點清單及資料管理措施，並增加資料使用軌跡紀錄，建置符合資安與個人資料之資產盤點及文件軌跡保存機制。

[1] 參水利法第12條。
[2] 參中央行政機關組織基準法第37條。
[3] 軍事及情報機關依資通安全管理法施行細則第2條規定，軍事機關指國防部及其所屬機關（構）、部隊、學校；情報機關指國家情報工作法第3

條第1項第1款（包含國家安全局、國防部軍事情報局、國防部電訊發展室、國防部軍事安全總隊）及第2項規定之機關。另須注意依國家情報工作法第3條第2項規定，行政院海岸巡防署、國防部政治作戰局、國防部憲兵指揮部、內政部警政署、內政部移民署及法務部調查局等機關（構），於其主管之有關國家情報事項範圍內，視同情報機關。

[4] 羅正漢，〈臺灣資通安全管理法上路一個月，行政院資安處公布實施現況〉，iThome，2019/02/15，https://www.ithome.com.tw/news/128789（最後瀏覽日：2019/5/13）。

[5] 公務機關及特定非公務機關之責任等級目前分為A、B、C、D、E等五級，各機關應依據其責任等級應從管理面、技術面及認知與訓練面向，辦理相應之事項。

[6] 資通系統之定義，依資通安全管理法第3條第1款之規定，指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

[7] 公務機關及特定非公務機關於知悉資通安全事件後，應於1小時內依規定進行資通安全事件之通報；如為第一、二級資通安全事件，並應於知悉事件後72小時內完成損害控制或復原作業，第三、四級資通安全事件，則應於知悉事件後36小時內完成損害控制或復原作業。

[8] 〈國家資安資訊分享與分析中心(N-ISAC)〉，行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/NISAC（最後瀏覽日：2019/5/14）。

相關連結

- 臺灣資通安全管理法上路一個月，行政院資安處公布實施現況
- 國家資安資訊分享與分析中心(N-ISAC)

你可能會想參加

- → 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- → 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- → 供應鏈資安國際法制與政策趨勢分享會
- → 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
- → 商業服務業個資保護宣導說明會
- → 個人資料保護新思維企業法遵論壇
- → 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 中部場–商業服務業個資保護工作坊
- → 南部場–商業服務業個資保護工作坊
- → 北部場–商業服務業個資保護工作坊
- → 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會
- → 電商零售業法制宣導說明會暨產學研座談會
- → 數位海盜時代來臨–抵禦海上資安威脅的實踐與挑戰
- → 零售業個資保護宣導暨座談會
- → 零售業個資保護及資訊安全教育講習
- → 零售業個資保護及資訊安全教育講習

施弘文
專案經理 編譯整理

上稿時間：2019年06月

文章標籤

個人資料　資訊安全

推薦文章