資通安全管理法遵與實務的兩難？（上）

資安法歷經五年 順應時事修法完善

資安法公布歷經五年，相關時空背景變化下，亦進行數次修訂，本系列文章將陸續針對修法過程出現在法遵與實務上的難處進行探討。

文／林逸塵（國立政治大學資訊管理博士）

有鑑於資通安全是維護國家安全和公共利益上非常重要之議題，資通科技之發展蓬勃隨之資通安全風險也逐漸增大，國際間多以訂立專法方式對資通安全之保護加以規範，因此我國早自107年順應整體資通環境制定資通安全管理法（資安法），將公務機關及特定非公務機關之資安防護措施進行納管，以降低並防範資通安全的風險。

從資安法的規範對象觀之，所謂公務機關指依法行使公權力之中央、地方機關（構）或公法人（不含軍事機關及情報機關），特定非公務機關指關鍵基礎設施提供者、公營事業及政府捐助之財團法人，透過機關責任等級分級、資通系統分級、資安事件分級，藉由資通安全維護計畫的執行，對於資安事件在事前、事中、事後各階段的管控，進行內外稽核、事件通報應變、情資分享等作為，納管機關執行應辦事項及系統控制措施。

立法主要取自資訊安全管理系統（ISMS）的精神，由規劃（Plan）、執行（Do）、查核（Check）、行動（Act）進行資安風險管理，透過法遵避免資通訊系統、服務或網路違反安全政策或保護措施失效，影響資通系統機能運作，構成資通安全政策之威脅，藉以強化我國資安整體防護能量。

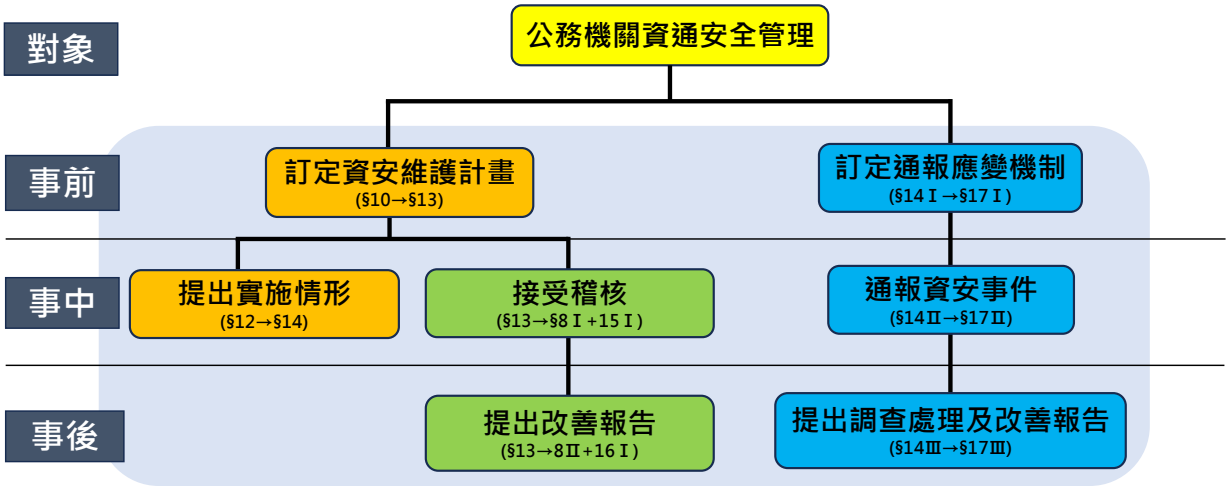

圖 1，資通安全管理法之公務機關法遵義務及條次調適示意。

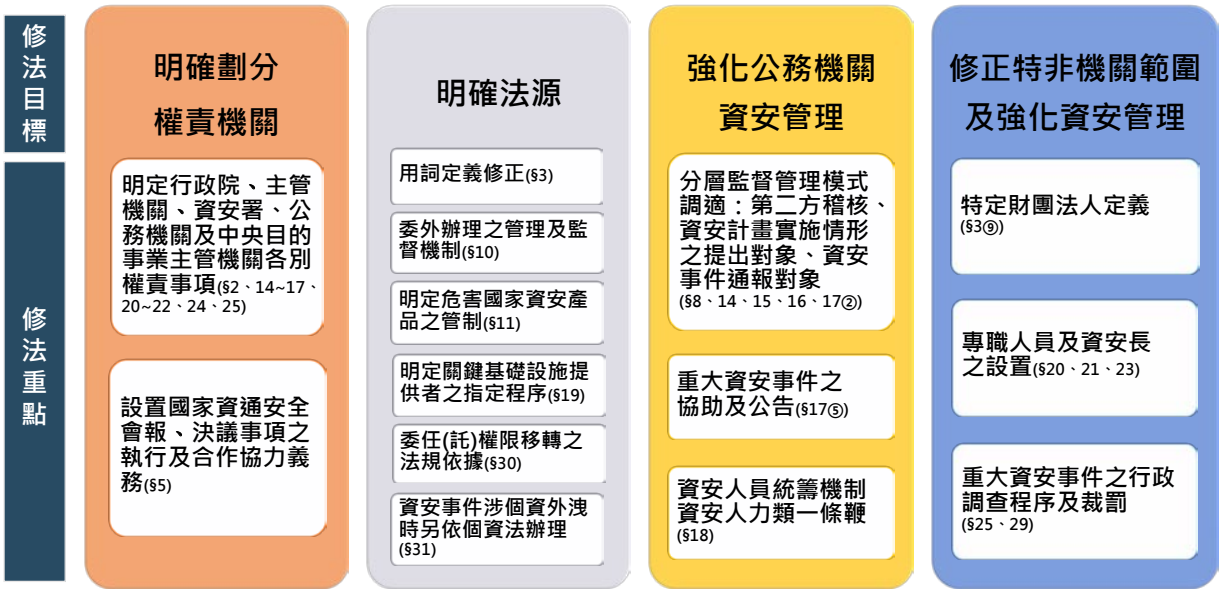

圖 2，數位發展部於 112 年 9 月 22 日預告修正草案重點條文。

蛻變中的資通安全管理法

我國資安法在107年6月6日經立法院三讀通過，該法自108年1月1日施行以來未曾修訂，而其授權制定的六大子法（包含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、公務機關所屬人員資通安全事項獎懲辦法）歷經108年8月26日、110年8月23日的修訂，反應出因資安環境變遷的法規調適。

除了強化納管機關的應辦事項，例如在技術面加入資通安全弱點通報機制（VANS）、端點偵測及應變機制（EDR），以結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資產盤點及風險評估應辦事項之作業，並在端點強化主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。並對資通安全專業證照及職能訓練證書進行規範等，這些措施有效加大資通安全管理的守備範圍。

然而資通安全管理法為母法，施行迄今已近五年，法遵工具在執行機關資安人員的實務操作下，經過充份磨合已可轉化為法規蛻變的動力，本次調修草案以維持原有法遵義務為基礎，將因調適而變動相關的條次內容，見（圖1）。

回溯到母法調修的歷程，早從行政院資通安全處時代，即已開始蓄積修法能量，在數位發展部資通安全署（資安署）111年8月27日正式成立時，致力推動國家整體資安在法制與實務的融合，以收納各機關在資安維護工作上的心聲，資安署積極盤點問題及推動修法，以期法規能更貼近實務運作。為此，數位發展部（數位部）於112年9月22日提出預告修正草案總說明及條文對照表，並提供資安法修法懶人包於公共政策網路平台，提供各利害關係人檢視及蒐集意見，草案重點條文如（圖2）。

此外，自112年8月起，資安署陸續舉辦了6 場修法工作坊，並自同年10～11月在全省舉辦了16場修法說明會，期望透過廣泛討論及交流，確保能充分反映社會各界期待，綜合調修後將送數位部及行政院審查，最後程序為送請立法院審議，以精進現有資安管理機制，提高國家整體資安水準。

本次資安法修法納入各界關切議題，因會對納管機關造成影響，資安署也持續進行綜整及規劃，期以妥適方式推動我國資安防護作業。依據112年9月22日預告資安法修正草案觀之，本系列文章將擇要就現行法遵及實務上難題進行解析。

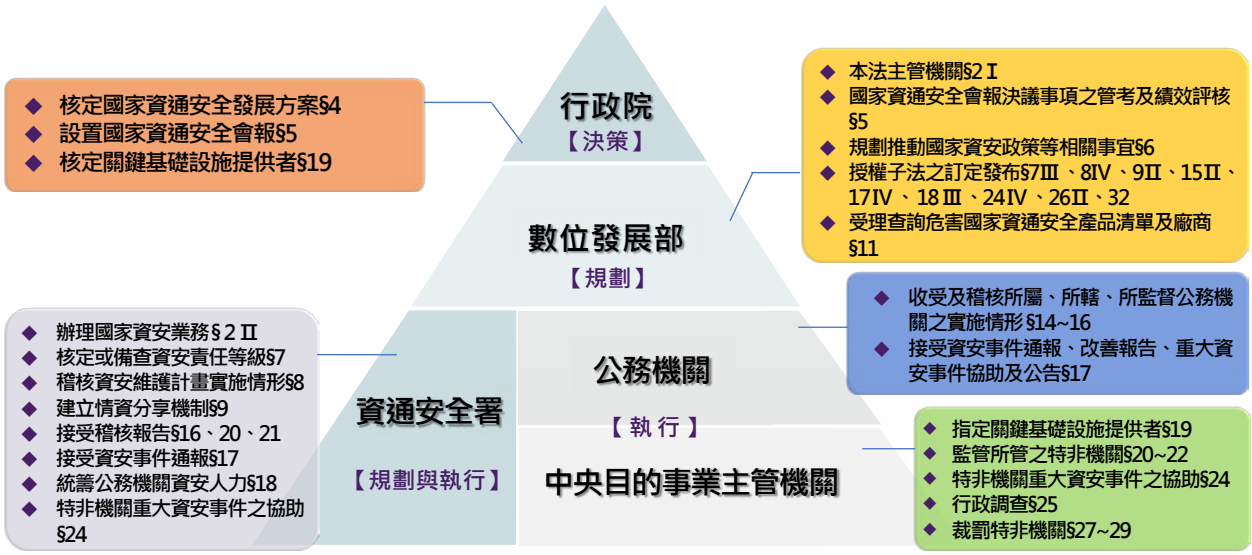

圖 3，主管機關及機關層級權責劃分與條文對照。

主管機關層級及上下權限區分

在本次資安法修法草案中，明確國家整體資安運行機制層級，詳細定義行政院、數位部、資安署、公務機關、中央目的事業主管機關的分工及職掌，以清晰界定納管機關的執行任務。機關的上下權限區分就如同金字塔形的權責事項劃分（**圖3**），行政院側重在上位決策權，沿襲自90年迄今陸續推動六個階段（各為期四年）之重大資通安全計畫或行動方案，即由行政院核定國家資通安全發展方案；數位部、資安署成立後，資安法的主管機關明訂在該部，主要側重國家資安政策方向，並進行統籌規劃

而資安署側重在實質規劃及執行，依組織任務辦理國家資通安全各項業務，包含辦理國家資通安全政策規劃、計畫核議及督導考核，執行國家資通安全防護、演練與稽核業務及關鍵基礎設施防護等。

在資安法修法草案第 14～17 條、第 19～22 條、第 24 條、第 25 條、第 27～29 條中，明訂公務機關應向上級機關或監督機關提出資通安全維護計畫實施情形，賦予資安署、上級機關或上級政府監督所屬、所轄機關或無上級機關者，因此監督單位有收受資安維護計畫實施情形、稽核報告、改善報告及接受資安事件通報、重大資安事件協助及公告的權責。

中央目的事業主管機關針對所監督的特定非公務機關，權限包含指定關鍵基礎設施提供者（CIP）、監督所管之特定非公務機關、重大資安事件協助及公告，以及賦予行政調查及裁罰等權責。

在資安法修法草案第5條中，明定行政院設置的國家資通安全會報（中央）及各政府機關（地方）合作協防機制，現行資通安全會報下設網際防護及網際犯罪偵防二個體系，屬於行政院的任務編組，由各相關部會主責，**見（圖4）**。

本次修正主要將國家資通安全會報提升為法律位階，希更強化與各政府機關的協防關係，不論中央、地方及各層級的政府機關都可致力配合，執行國家資通安全相關措施，進而建構國家資通安全環境。資通安全會報除辦理國家資通安全政策、應變機制與重大計畫之諮詢審議，協調中央及地方間之資通安全相關事務，強化跨機關間資通安全事件應處能力。

此外，對於國家資通安全會報作成的決議，相關政府部門應予執行，由數位部定期追蹤管考，並得辦理績效評核，並授權行政院對於其實質運作應另訂辦法。

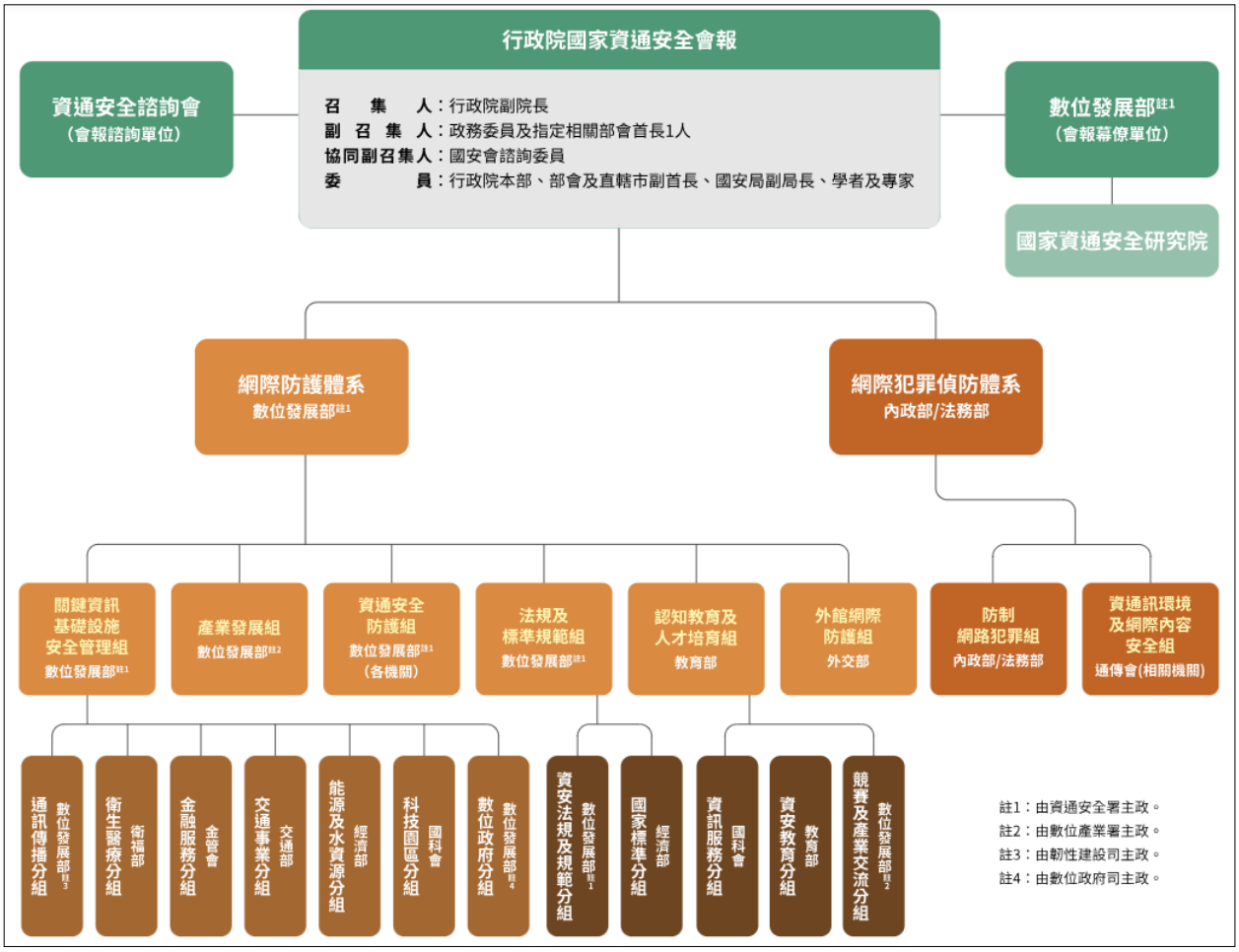

圖 4，行政院國家資通安全會報組織架構。

指定關鍵基礎設施提供者（CIP）程序

現行指定 CIP 程序係依行政院於 107 年 5 月 18 日修訂之「國家關鍵基礎設施安全防護指導綱要」辦理，由國土安全辦公室主責，行政院要先公告關鍵領域。關鍵領域為三層式架構，第一層為**主領域**，第二層為**次領域**，第三層為次領域下的**重要功能設施與系統，主領域依功能屬性分為能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區共八項**，再依功能業務區分各次領域，例如：能源領域下再區分為電力、石油、天然氣共三項次領域；交通領域下再區分為陸運、海運、空運、氣象共三項次領域；金融領域下再區分為銀行、證券、金融支付三項次領域等。

為協助中央目的事業主管機關指定關鍵基礎設施提供者，資安署特訂定關鍵基礎設施提供者指定程序，區分「**辨識關鍵領域**」、「**辨識關鍵服務**」、「**辨識關鍵（資訊）基礎設施**」及「**核定關鍵基礎設施提供者**」四大步驟，各步驟內之各分項工作依權責分由行政院、各中央目的事業主管機關及候選關鍵基礎設施提供者負責辦理，以落實推動國家關鍵資訊基礎建設防護（Critical Information Infrastructure Protection，CIIP）。

下一期針對民間單位的 CIP 認定會有更進一步的說明。