立法報導

外國法案介紹—資通安全管理法

概述

隨著網際網路及資通科技快速發展與普及，資通科技相關應用，已被世界各國視為協助產業經濟轉型、提升國家競爭力及有效解決社會發展議題之關鍵，各國亦紛紛致力於資通政策之規劃，建構公開、有效率之數位環境，希望藉由科技化服務，進而提升民眾生活品質、維護公共利益、帶動產業發展及國家整體競爭力。然而，網路頻繁傳輸與公開消費者使用管道給人們日常生活帶來便利的同時，貫通系統或服務之應用所引發之網路犯罪、個人資料保護等資通安全課題，逐漸成為影響社會安定、國家安全之隱憂。具有惡意目的之網路駭客已跨越國界範圍，對全球之公用設施、運輸網絡、醫療機構與其他的關鍵基礎設施為攻擊目標，企圖竊密、破壞或癱瘓各國之基礎服務，因而各國之資安管理部門應對定義與分析攻擊並發展各樣的防禦機制，保護當地的關鍵基礎設施並予以迅速對威脅和事件作出反應，俾促進關鍵部門的信息共享，實施定期的風險評估，遵守執業守則等防範措施。顯然資通安全威脅型態之瞬息萬變已使得全球資通部門面臨嚴峻之考驗。

當然每一個政府都希望民眾能從網際網路連接裝置市場的巨大潛力中受益，但利益的前提條件是它們必須是安全的，並對人們的生活產生積極的影響，因此與資通產業相關之業者須對使用者負責，遵守政府安全設計審查原則的各項規則，以便從現在開始就將強大的安全措施導入產品的日常技術研發中，有助於確保我國民眾免受網路犯罪傷害，且讓我國成為領先世界的創新數位經濟體。

人工智慧（Artificial Intelligence, AI）是物聯網及工業 4.0 發展的核心。

AI 與機器學習技術可造福諸如翻譯、醫學影像分析等應用，同時也可能遭到濫用，隨著 AI 能力愈來愈強大及普及，除了會擴大既有的威脅之外，也將帶來新的威脅，各種 AI 應用可能衍生犯罪、實體攻擊或政治破壞等負面影響，威脅數位安全、實體安全，以及政治安全。在數位安全上，自動化的網路攻擊行動將擴大現有的攻擊規模與效率，亦預期會出現專門軟體漏洞與 AI 系統漏洞的新型態攻擊行動，並預期將會藉由無人機或其它系統所展開的實體攻擊，或是顛覆傳統攻擊的新模式。另 AI 還能被用來破壞政治安全，以 AI 分析大量資料以進行監控，建立有特定目的的宣傳活動或欺騙行為，或者發展出新型態的攻擊，像是分析人類的行為、情緒及信仰以發動攻擊，也極會破壞民主國家的公共論壇。

基此，AI 新科技的演進，帶給勒索軟體有更進階的攻擊威脅。為此 AI 產業聯盟主動發起自律原則，承諾將負責任地推進技術發展，在現行法規下研發人工智慧技術，植入高度自主的系統必須考慮維護人的尊嚴、權利和自由，防止技術的濫用與潛在的倫理問題，並要求系統開發者必須確認 AI 系統的安全性，應具備安全保障措施，確保系統的可控制性。除此之外，資安業者亦開始布局 AI 系統安全維護開發，試圖切入 AI 資安新興市場，而且許多國家的法規也開始正視 AI 產業所引發的資安問題，開始制定各項規範資料保護措施。

新科技引發新的網路安全問題，近年國際間對各種互聯網、人工智慧採取更嚴謹的保護資通安全政策，各先進國家已將各種資安議題提升至國家安全層次，並制定專法加以規範。基本上，各國資通專法立法之目的在於實現「防止、檢測、反擊或調查」網絡安全威脅或事件。據聯合國旗下的國際電信聯盟（International Telecommunication Union, ITU）於 2017 年 7 月發表了全球網路安全指數（Global Cybersecurity Index, GCI）報告顯示，全球 193 個國家中，有 50%的國家部署了網路安全戰略，或正在制定當中。面對日益嚴峻複雜的國內外網路安全形勢，美國、德國、日本及歐盟等主要國家和地區均高度重視網路安全立法，一方面加快立法網路安全基本法，另一方面強化政府資訊安全、資訊監控與內容安全、數據保護、關鍵基礎設施保護等多方面立法，為網路安全保護各項措施的具體實施提供法律依據。並倡議於資通安全法規內採取積極主動的措施，以捍衛國家關鍵的基礎設施和包括許可選定的資通安全提供者。除此，亦專注於保護關鍵基礎設施，創造公平競爭環境，以提高國家所有行業的成熟度和防範能力為首要宗旨。例如：美國制定

有「聯邦資訊安全現代化法」;日本則制定「網路安全基本法」;德國依據 2011 年提出的「網路安全策略」制定有「資通安全法」。在國際組織部分，歐盟訂定「網路與資訊系統安全指令」讓其規範範圍更已涵蓋至數位服務之範疇。

以上各國或地區透過專法之制定，讓政府機關得以採取適當法律手段，以逐步提升資通安全能量及協助關鍵基礎設施提供者在內之非公務機關，其營運或提供之服務，得以認知自身資通安全責任與因應資通安全風險，增進自身資通安全能力。爰就美、德、日等三國資通安全立法主要涵蓋內容敘述如下：

一、強化資安統合機關，提出資通安全法

日本於 2014 年制定「網路安全基本法」，明確設立網路安全戰略總部並將網路安全戰略總部的權限大幅提升，以統一協調各部門的網路安全政策，並對電力、金融等基礎設施業者落實網路安全相關措施提出了要求。美國於 2014 年通過「聯邦資訊安全現代化法」，強化國土安全部維護國家網路安全的重要作用，賦予國土安全部（DHS）部長得隨時與管理及預算局（OMB）局長互相磋商，共同進行監督管理聯邦各機關資通安全措施。德國於 2009 年 8 月通過之「加強聯邦資通安全法」賦予聯邦資訊科技安全局為全國 IT 安全通報中央辦公室，蒐集並分析安全漏洞及新攻擊模式相關資訊，以建立可靠之情勢概覽，及早發現攻擊並採取對策。

二、加強政府資訊安全立法，保護政府網路與資訊安全

美國於 2002 年制定全面規定聯邦政府資訊安全保護要求的「聯邦資訊安全管理法」，強調對電腦網路進行實時、自動監控，加強聯邦政府網路安全保護。日本的「網路安全基本法」強制各政府單位要向網路安全戰略總部稟報資安相關問題，總部也會向各單位提出資安建議；國家安全委員會則要協助各政府單位落實網路安全審核，也要在發生重大資安事件時，第一時間介入調查，以確保政府網路的安全。德國「資通安全法」之立法宗旨，在於提升資通安全並加強保護 IT 系統與服務，尤其對於供給能源、糧食、水、資訊、電信、金融、醫療、運輸及交通等各領域之關鍵基礎設施產業，確保其資通安全至關重要，並且提升聯邦政府及企業之資通安全管理，強化確保民眾網路環境之安全。

三、加強數位資源安全，保護民眾個人資訊

數位安全是各國資訊安全立法保護的重點，從各國相關立法具體內容來看數位安全的實質意義，一是強調數據資訊資源安全，包括以商業秘密為代表的經濟資訊和政府部門受保護資訊。二是注重個人數位安全保護，包括禁止攔截和竊取個人數據、個人數據保存和處理的安全保護要求。

現階段日本於發展物聯網系統上，於建置過程中要求應具備安全性的設計。為促進物聯網安全，日本政府亦祭出多項規範與安全標準，包括要求廠商在研發物聯網功能時，要同等注重機密性、整合性、可用性以及安全性，也要求在資安事故發生時，有一套安全的備援措施，並且明訂事件發生後的責任歸屬。日本「網路安全基本法」則在意於每位國民能否對資通安全之認識，促其自發性處理資安問題，建立迅速復原機制，並要求政府為確保資訊系統及資通網路之安全性與信賴性而採取必要措施，以求適切管理，其基本措施在於防制網路犯罪及防止受害擴大，並防範處置嚴重影響國家安全之虞的情事。

在美國「聯邦資訊安全現代化法」要求各機關應向有關監督機關提出年度報告，內容必須為重大資安事件之情形與處理狀況以及涉及個人資料受侵害之重大資安事件之相關情形。

德國「資通安全法」則要求數位服務業者包括網站營運業者、線上購物網站、搜索引擎及雲運算服務提供者等相關業者應強化預防客戶資料及所使用之 IT 系統遭受攻擊之技術及行政措施，並應及時並定期更新或修補應用程式及操作系統。另為了應對網路犯罪，德國立法對資料保護方面有著嚴格的規定。一是，對於在網路上傳播病毒的駭客有著嚴格的取締規定，傳播惡意程式碼竊取個人資料的行為在德國是違反刑法的。二是，對在網路上濫用個人資料有著嚴格的處罰規定，如果將部分使用者資訊放到黃色網站上，在德國是必須受到法律追究的。三是，禁止違法內容在互聯網上傳播。

四、聚焦國土安全資產，保護國家關鍵基礎設施

在關鍵基礎設施保護立法方面，美國走在了世界前列。作為全球資訊技術最為發達、應用最為廣泛的國家，美國明確將數位化基礎設施作為國家戰略資產，2002 年「聯邦資訊安全管理法」以及依「聯邦資訊安全管理法」修正後更名之「聯邦資訊安全現代化法」，對關鍵基礎設施實體與資訊安全系統的風險管理，規定須整合相關部門與業者共同合作，以強化國家關鍵基礎設

施的安全性。日本「網路安全基本法」則將促進關鍵基礎建設事業及地方政府等確保資通安全之相關事項列為網路安全戰略必須記載的內容。德國「資通安全法」之核心宗旨則明確指出應對於供給能源、糧食、水、資訊、電信、金融、醫療、運輸及交通等各領域之關鍵基礎設施產業，加強保護 IT 系統與服務，確保其資通安全，而其關鍵基礎設施業者必須遵守相關 IT 安全標準營運，並向聯邦資訊科技安全局通報重要資安事件。

五、研擬訂定資安標準，以達資訊安全目標

美國「聯邦資訊安全管理法」為聯邦資訊系統創建一套能夠提供實現有效資訊安全控制措施之聯邦運作模式，及其綜合性資訊安全框架之資產規範，同時以實作計畫，奠定美國聯邦政府對資訊安全管理及保護之基礎，責成國家標準與技術研究院必須為資訊安全管理定義、政策與評鑑等作業，制定標準及指南，以達成資訊安全管理之目標。德國聯邦資訊科技安全局須為聯邦政府制定統一及嚴格之安全標準，並於必要時開發、採購或提供適合之產品。如此可以預防聯邦政府及政府網絡誤用具有安全漏洞或受到惡意操控之不合適 IT 商品及組件，且「資通安全法」復有規定，關鍵基礎設施業者必須提出符合最新資通安全標準之證明。一旦發現安全缺失，聯邦資訊科技安全局得與相關主管機關協商，下令廠商改善。日本「網路安全基本法」規定，中央政府應對其行政機關及獨立行政法人之網路安全，訂立統一資安標準，針對資訊系統之不法行為進行監視、分析，並與國內外相關機構合作，協力處理資安威脅。

六、培育資安人才，維護網路安全

根據美國網路安全教育中心（CCSE）的調查，2015 年全球資安人才需求約為 150 萬人，估計至 2022 年時，需求將會擴大 20%，達到 180 萬人，資安人才短缺問題是各國網路安全建設面臨的共同難題。各國政府重視資安人才的理由，乃在於渠等人才與網路安全產品的量產與出口有關。

美國強調發展網路安全科技產品與人才培育，網路安全人力資源建設重點關注 4 個方面：一是，在高等教育體系培育人才。通過獎學金計畫，鼓勵學生從事網路安全相關領域的工作。二是，選拔與吸引優秀人才為政府部門工作。三是，政府機關關鍵職位人員培育。設計培訓認證制度，提高人員能力，並對人員實施技能的持續性評估。四是，在職人員的網路安全意識訓練。

日本「網路安全基本法」則將人才培育列為國家基本措施，2016 年 3 月，

網路安全戰略總部基於日本復甦計畫以及網路安全戰略，制定了網路安全人才培育發展計畫，主要是在政府、企業以及學界三者間培育並媒合資安人才，目標是建立起一個良善、人力供需平衡的生態圈。

德國由於高齡化發展趨勢，使得德國未來也將面臨人才缺口的問題，因此在高科技戰略中，對於全球人才的引進有更為開放之態度，目的是要強化對於人才培育之投入，以為未來產業發展建立基礎。德國將人才的引進視為提升網路安全的政策方針，在推動作法上主要有幾個方向，第一，鼓勵職業教育取得優秀畢業成績的學生，能再進一步攻讀大學文憑。其次，是吸引學生學習科學、技術、工程與數學的研究領域，以彌補未來產業在特定領域的人才缺口。三是，吸引高科技人才進入德國就業。為吸引國際人才，德國強化其科研領域對全球的吸引力，補助大學院校科技研究活動，也給予學校在人才聘用上的彈性，並放寬技術移民政策。

網路威脅是全球性的議題，隨著網路犯罪日趨頻繁，各國政府採取措施加強網路安全生態環境建設，以減少犯罪威脅，提高人們對使用網路服務的信心。全球產業隨著物聯網市場的快速增長，正處於受網路攻擊目標呈指數級增長的危機邊緣，我國身處國際產業供應鏈之一環，故同時亦是網路駭客攻擊威脅的目標之一。政府為推動改進應對網路安全威脅的措施，促進網路安全的國際合作，必須設立專責部門負責國家資安基本方針、政策及重大計畫、法規制定、通報應變和關鍵基礎設施的管理等事宜，爰行政院於 2016 年 8 月 1 日於院本部成立「資通安全處」。另為防範資通安全風險並逐步提升自身資通安全能量，以及達成資通安全環境最有效率的政策選擇目的，行政院擬透過制定資通安全專法，統籌分配資源、整合民間力量，提升我國整體資通安全環境及資通安全意識，保障國家安全與公共利益，爰於 106 年 4 月 28 日以院臺護字第 1060172497 號擬具「資通安全管理法草案」函請立法院審議。資通安全與經濟成長、國民福祉、科技服務息息相關，必須要維持網路互聯秩序及要求關鍵基礎設施應行配合的資通安全標準的專屬法律，為使本院委員及各界瞭解各國資通安全立法歷程及條文，爰蒐集美國、德國及日本等諸國相關資通安全資料予以簡述，以供立法及研究之參考。

美國

聯邦資訊安全法制

聯邦資訊安全管理法

Federal Information Security Management Act of 2002

聯邦資訊安全現代化法

Federal Information Security Modernization Act of 2014

法案簡介：

美國資訊安全之相關法制可追溯至 1929 年之「聯邦檔案法」(Federal Record Act of 1929)，而 1942 年修正之「聯邦檔案法」闡明資訊資源管理由白宮「管理及預算局」(Office of Management and Budget, OMB) 之前身「預算局」(Bureau of Budget) 負責。依據 1946 年「原子能法」(The Atomic Energy Act of 1946) 及 1947 年「國家安全法」(The National Security Act of 1947)，美國政府開始關注國家安全與特種資訊間所衍生之問題，更意味著對資訊安全意識之覺醒。

1966 年制定之「資訊自由法」(Freedom of Information Act of 1966)，於 1974 年、1986 年及 1996 年進行修正，主要內容包括對政府資訊之獲取、公開、可分割性及相關訴訟事宜等加以規定。另外，為因應 1952 年起「國家安全局」(National Security Agency, NSA) 對「機密性」之要求與規範，1985 年 12 月 24 日，「管理及預算局」以 A-130 公告之附件 III，正式啟動資訊安全管理法制化工作。1987 年制定之「電腦安全法」(Computer Security Act of 1987)，規定國家標準與技術研究院 (National Institute of Standards and Technology, NIST) 負責開發聯邦電腦系統之安全標準。除國家安全系統被應用於國防及情報任務外，商務部則負責公布安全標準，並加強聯邦電腦系統安全保護之培訓責任，以提高聯邦電腦系統之安全性及保密性。

1991 年「高性能計算法」(High Performance Algorithms Act of 1991)，規定建立滿足安全需求之聯邦高性能計算程式，提供跨部門間之協調，並向國會遞交年度執行報告。此外，要求國家標準與技術研究院為聯邦系統建立高效能計算之安全與隱私標準。1996 年頒布「克林格-科恩法」(Clinger-Cohen Act of 1996)，又名「資訊技術管理改革法」(Information Technology Management

Reform Act of 1996），規定設立首席資訊官（CIO）職位；授予商務部發布安全標準之權利；要求各個機構開發及維護資訊技術架構；要求管理及預算局監督主要資訊技術之收購，並與國土安全部長協商，公布國家標準與技術研究院制定之強制性聯邦電腦安全標準。

隨著資訊化日益普及面對隨之而來之網路威脅議題，1998 年 5 月 22 日，柯林頓總統以第 63 號總統決策令（Presidential Decision Directive），將以「機密性」為主之電腦系統安全擴增為需具備「機密性」、「完整性」及「可用性」之資訊安全系統。在聯邦政府以身作則指導下，於 2000 年另頒布「政府資訊安全改革法」（Government Information Security Reform Act of 2000），規定聯邦政府部門對保護資訊安全方面之責任，並要求商務部、國防部、司法部、總務管理局、人事管理局等部門維護資訊安全之具體職責，建立聯邦政府部門資訊安全監督機制。2002 年國會通過「聯邦資訊安全管理法」（Federal Information Security Management Act of 2002），並於同年 12 月 17 日頒布施行，以做為統合聯邦資訊安全管理之基準法。以下僅就 2002 年「聯邦資訊安全管理法」內容簡述如下：

一、立法宗旨及目的

2002 年「聯邦資訊安全管理法」（FISMA）係為 2002 年「電子化政府法」（E-Government Act of 2002）之一環，置於該法第 3 篇（Title III）「資訊安全」，主要立法宗旨為提供一完整架構，以確保維護聯邦資訊及相關資產安全之綜合性措施，且具體規範美國聯邦政府對資訊安全管理之任務。其立法目的在為聯邦資訊系統創建一套能夠提供實現有效資訊安全控制措施之聯邦運作模式，及其綜合性資訊安全框架之資產規範，同時以實作計畫，奠定美國聯邦政府對資訊安全管理及保護之基礎。該法強調風險管理，規定 OMB、NIST、CIO（首席資訊官）、CISOs（首席資訊安全官）、IGs（聯邦機構監察長）之具體職責；倡導由「管理及預算局」監督建立中央聯邦事件中心負責分析安全事件，並且提供技術協助，通知資安業者關於現有及潛在之安全威脅與漏洞。

二、簡述

「聯邦資訊安全管理法」分成：1.資訊安全（第 301 條）；2.資訊技術之管理（第 302 條）；3.國家標準與技術研究院（第 303 條）；4.資訊安全與隱私諮詢委員會（第 304 條）；5.技術與遵循之修正（第 305 條），共計 5 條文。

主要內容包括：1.資訊安全與國家安全系統之定義；2.聯邦各機關之責任；3.資訊安全管理之運作評鑑及年度報告；4.國家標準與技術研究院之定位；5.國家標準與技術研究院之修正。

（一）資訊安全與國家安全系統之定義

資訊安全管理之標的為「資訊與資訊系統」，同時將資訊安全管理定義為「保護資訊及資訊系統，避免未經授權之存取、使用、洩漏、破壞、修改或銷毀，以確保資訊之機密性、完整性及可用性」。機密性係指對保護個人隱私與私人資訊之存取及揭露之授權限制；完整性係指防止不恰當之資訊鑑別性、可歸責性及不可否認性；可用性係指對資訊之即時及可靠之存取與利用。

國家安全系統之定義為「涉及情報工作與國家安全相關之密碼工作、軍隊之指揮及控制、武器或武器系統之裝備、國防或外交作業中之機密資訊」。

（二）聯邦各機關之責任

「管理及預算局」之責任為制定資訊安全政策、標準與指南，並監督其實作；要求聯邦各機關資訊安全工作之基本狀況及監督聯邦資訊安全事故中心等。聯邦各機關之責任則為評估各該單位之資訊安全風險，確定其等級，並提供相關資訊安全防護；部署資訊安全工作之負責人；遵循相關政策規定，並將資訊安全工作融入其機關之策略與規劃運作之過程中。

（三）資訊安全管理之運作評鑑及年度報告

「聯邦資訊安全管理法」規定各機關每年定期對資訊安全計畫與運作之結果進行一次獨立評鑑，並將評鑑報告送交管理及預算局，該局再將報告結合從其他通路獲得之資訊，編製成年度實作報告，提交國會審查，據以判斷資訊安全計畫與實作之成效。該法還要求評鑑報告中，所有聯邦各機關所使用之資訊與資訊系統必須分類，針對相應之風險等級提供適當資訊安全防護，每一類資訊及資訊系統均應滿足最低之資訊安全要求；所有資訊系統運行前必須進行驗證與認證，通過後方可投入業務之運作。

（四）國家標準與技術研究院（NIST）之任務

聯邦資訊安全管理法責成國家標準與技術研究院必須為前述資訊安全管理之定義、政策與評鑑等作業，制定標準及指南，以達成資

訊安全管理之目標。該項標準化作業於 2009 年完成第 1 階段工作，該法之實作計畫自 2010 年起，亦已正式進入 FISMA2.0，成為新的實作計畫典範。

（五） 國家標準與技術研究院（NIST）之修正成果

將國家標準與技術研究院中之「電腦系統安全與隱私諮詢委員會」（Computer System Security and Privacy Advisory Board）修正為「資訊安全與隱私諮詢委員會」（Information Security and Privacy Advisory Board）；電腦或電訊技術及裝置修正為資訊技術；電腦系統修正為資訊系統；電腦系統安全修正為資訊安全。

2009 年歐巴馬總統簽署「網路空間政策評估報告」，強調保障美國政府之網路系統安全。2001 年 911 事件後，為因應恐怖攻擊，美國成立「國土安全部」（Department of Homeland Security,DHS）。「聯邦資訊安全管理法」配合「網路空間政策評估報告」及「國土安全部」之成立，分別於 2012 年與 2014 年進行兩次修正，將該法納入「國土安全部」為管理角色之一，要求其對資安事件進行通報，並修正法名稱為「聯邦資訊安全現代化法」（Federal Information Security Modernization Act of 2014，FISMA）。以下僅就該法內容簡述如下：

「聯邦資訊安全現代化法」之立法宗旨係在不影響國防部、國安系統及國家情報局之權限下，確保支援聯邦政府資訊來源之安全、可靠、完整與機密，並增訂具有拘束力之作業指令及對情報界之定義。其修正重點包括：

一、賦與國土安全部長監督管理職掌

將 FISMA 監督管理聯邦各機關資安政策及實施者，由原本之「管理及預算局」（OMB）局長，改為與「國土安全部」（DHS）部長應隨時互相磋商，共同進行監督管理。職掌包括，1.DHS 部長協助 OMB 局長執行任務；2.訂定並監督綜合作業指令之實施；3.監督聯邦各機關資安政策及實施；4.召集各機關主管開會，以落實資安政策及實施；5.協調跨部門資安工作事項；6.提供各機關資安管理與技術上之協助。

當「聯邦資訊安全現代化法」生效兩年後，前述兩位監管最高負責人，應提出政府機構採用診斷式科技及其他精密安全儀器後之效果分析。

二、調整各機關提出年度報告之內容

對於各機關應向有關監督機關提出年度報告之要求，其內容由原本關於

資安政策及措施等執行情形，與預算及資源之運用狀況，調整為關於資安事件之報告。報告內容主要為：1.重大資安事件之情形與處理狀況；2.資安事件之統計數量及其影響程度；3.涉及個人資料受侵害之重大資安事件之相關情形。

三、增加對重大資安事件進行通報之要求與相關規定

為因應對重大資安事件進行通報之要求，2014 年「聯邦資訊安全現代化法」規定管理及預算局應訂定「重大資安事件指導原則」，並應向國會報告。此外，發生重大資安事件之機關應於相當確定事件發生後 7 天內，向國會相關權責委員會進行初次通報，並於合理時間內，再次提出詳細報告。

四、增加資訊安全系統測試及關於資訊受侵害時之相關規定

2014 年「聯邦資訊安全現代化法」除增訂資訊安全系統之定期測試，應包括使用符合標準之自動化儀器在內外，另要求當資訊系統內之資料受到侵害時，應有相當處置措施。管理及預算局應確認關於資料受侵害時之通報政策與指引是否適時更新。受侵害之聯邦機關發現資料遭到無權取得或存取後 30 日內，向國會報告下列事項，1.侵害發生之原因；2.預估受侵害影響之當事人數量；3.是否及何時告訴當事人，並說明可能延遲告知時間之原因。

條文要旨：

2002 **年電子化政府法**

第 3 **篇　資訊安全**

2002 **年聯邦資訊安全管理法**

第 301 條　　聯邦資訊管理法

美國法典第 44 **篇第** 35 **章**

第 3 分章　資訊安全

第 3541 條　立法目的

第 3542 條　定義

第 3543 條　管理及預算局局長之權限與職責

第 3544 條　聯邦機構之責任

第 3545 條　聯邦機構年度獨立評估

第 3546 條　聯邦資訊安全事件處置中心

第 3547 條　國家安全系統

第 3548 條　撥款之授權
第 3549 條　本法對現行法律之影響
第 302 條　資訊技術之管理
第 303 條　國家標準與技術研究院
第 304 條　資訊安全與隱私諮詢委員會
第 305 條　技術上與相對應之條文修正

2014 **年聯邦資訊安全現代化法**
第 1 條　簡稱
第 2 條　「聯邦資訊管理法」之修正

美國法典第 44 **篇第** 35 **章**
第 2 分章　資訊安全
第 3551 條　立法目的
第 3552 條　定義
第 3553 條　國土安全部部長與管理及預算局局長之權限與職責
第 3554 條　聯邦機構之責任
第 3555 條　聯邦機構年度獨立評估
第 3556 條　聯邦資訊安全事件處置中心
第 3557 條　國家安全系統
第 3558 條　本法對現行法律之影響

資料來源：

1. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
（最後瀏覽日：2018/04/10）
2. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
（最後瀏覽日：2018/04/10）

德國

提高資訊科技系統安全法（簡稱「資通安全法」）
Gesetz zur Erhöhung der Sicherheitinformationstechnischer Systeme
（IT-Sicherheitsgesetz）

法案簡介：

自從資訊科技（Information Technology，簡稱 IT）發展愈來愈深入人類生活，工作各領域漸趨網路化後，德國身為高度開發之工業國家，對於 IT 在經濟及社會方面之潛力開發自然不落人後。然而隨著數位化應用之成熟，連帶亦產生愈來愈多網路風險，尤其是針對政府機關、銀行、醫療機構及其他掌握重要珍貴資訊之企業等相關關鍵基礎設施業者，進行竊密、破壞或癱瘓行動，該等帶有惡意目的之網路駭客攻擊事件一旦得逞，足以對國家經濟社會產生巨大之影響，因此資通安全已成為德國國家安全核心議題之一。

為此，聯邦政府於 2011 年提出「德國網路安全策略」（Cyber-Sicherheitsstrategie für Deutschland），作為國家提升資通安全之政策方針。策略中訂出十大目標:(1)保護關鍵基礎設施，(2)強化德國公民與企業之 IT 系統，(3)加強公共行政系統內部資訊安全，(4)建立「國家資訊回應中心」，(5)建立「國家資訊安全理事會」，(6)提升資訊領域之犯罪控制效率，(7)進行資訊安全之歐洲區域及全球合作，(8)使用可靠之資訊科技，(9)聯邦機構之人力發展，(10)採取資訊攻擊之回應措施。這些目標於 2014 年納入聯邦政府賡續列管追蹤之數位項目，爰此 2015 年 7 月制定「資通安全法」（IT-Sicherheitsgesetz），則是實現目標之第一個具體成果。以下謹就德國「資通安全法」簡述如下：

一、立法目的

「資通安全法」全稱為「提高資訊科技系統安全法」（Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme），其立法目的在提升資訊安全並保護德國關鍵基礎設施。該法採包裹立法制定，又稱為條款法，其條文內容主要為個別法律之修正法，包含修正「聯邦資訊科技安全局」、「核能法」、「能源法」、「電信媒體法」、「電信法」等。修正重點在加強公用事業及關鍵基礎設施相關業者、電信業以及網站服務業之 IT 安全規範以及通報義務。

二、立法宗旨

「資通安全法」之核心宗旨在提升資通安全並加強保護 IT 系統與服務，尤其對於供給能源、糧食、水、資訊、電信、金融、醫療、運輸及交通等各領域之關鍵基礎設施產業，確保其資通安全至關重要。其次，則是要提升聯邦政府及企業之資通安全管理，並強化確保民眾網路環境之安全。為提升網路安全，該法亦要求網路業者及電信業者均應符合更高標準之 IT 系統規格。

為達成上述目標，「資通安全法」再度擴大聯邦資訊科技安全局之職掌與職權。

三、適用對象應盡之義務

（一）關鍵基礎設施業：

「資通安全法」主要適用於現代社會最無法承受失誤之處，即關鍵基礎設施之資訊系統。關鍵基礎設施之提供者是指能源、糧食、水、資訊、電信、金融、醫療、運輸及交通等領域之重要設施業者，其營運必須遵守相關 IT 安全標準，並向聯邦資訊科技安全局通報重要事件。具體規定如下：

1. 如無其他特別規定，關鍵基礎設施相關業者應根據當前最先進科技標準保護其 IT 系統，並且每 2 年進行安全檢測。安全事故應通報聯邦資訊科技安全局，而聯邦資訊科技安全局則應向通報業者提供因應解決意見。
2. 如無其他特別規定，在符合當前最先進科技標準之情形下，業者得自行設定其基礎設施之安全值。
3. 如無其他特別規定，業者得根據當前最先進技術水準，設計各自行業之安全標準。
4. 對於足以影響關鍵基礎設施正常供應之 IT 系統重大干擾事件，業者必須向聯邦資訊科技安全局通報。
5. 關鍵基礎設施業者之營業夥伴、服務提供商及供應商亦須適用「資通安全法」之規範。

（二）數位服務業：

1. 包括網站運營業者、線上購物網站、搜索引擎及雲運算服務提供者等相關業者應強化預防客戶資料及所使用之 IT 系統遭受攻擊之技術及行政措施，例如：及時並定期更新或修補應用程式及操

作系統。

2. 個人或團體所架設之私人且非營利性質網站並不在「資通安全法」規範範圍內。但如私人網站涉及廣告並有營業收入，則應適用之。

（三）電信業：

1. 電信業者一旦發現客戶連線被用於 IT 攻擊時，應即對客戶示警，同時亦應對客戶提供排除干擾之可能途徑。
2. 電信業者根據最先進技術水準採用之 IT 安全措施，不僅應用於保護個人資料，亦應保護基礎設施免於遭受未經授權之干擾。
3. 業者應向聯邦網路局通報之事項，包含重大 IT 安全事故。

四、資安管理機關─聯邦資訊科技安全局

聯邦資訊科技安全局係依據 1990 年 12 月 17 日通過之「聯邦資訊科技安全局組織法」（Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik）而成立，為聯邦內政部之下設機關。其職掌如下：

1. 研究資通科技安全風險並制定安全措施。
2. 制定檢驗及評估資通系統或組件安全性之安全標準、程序及工具。
3. 檢驗並評估資通系統或組件之安全性，並頒發安全證書。
4. 核准用於處理或傳輸聯邦政府各機關機密資訊，或聯邦所屬事業之資訊科技系統或組件。
5. 支援並負責資通安全諮詢或管控之聯邦單位。
6. 支援警察、執法機關及憲法保護機關執行法定且必要之任務。
7. 提供資訊科技生產廠商、經銷商及使用者有關資安漏洞可能後果之諮詢。

2009 年 8 月通過之「加強聯邦資通安全法」（Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes）賦予聯邦資訊科技安全局更多對抗資安威脅方面之職權：

1. 作為全國 IT 安全通報中央辦公室，蒐集並分析安全漏洞及新攻擊模式相關資訊，以建立可靠之情勢概覽，及早發現攻擊並採取對策。
2. 收集、分析、存儲、使用並處理紀錄數據以及在聯邦通信界面產生之數據，使 IT 攻擊之跡象可以被偵測到，並迎面對抗。
3. 將 IT 產品及服務之系統漏洞及惡意程式相關資訊及警訊通知相關單位或消費大眾。原則上，聯邦資訊科技安全局應先通知廠商，其次才告知消費大眾。

4. 為聯邦政府制定統一及嚴格之安全標準，並於必要時開發、採購或提供適合之產品。如此可以預防聯邦政府及政府網絡誤用具有安全漏洞或受到惡意操控之不合適 IT 商品及組件。

2015 年制定並開始實施之「資通安全法」再度擴增聯邦資訊科技安全局之職權，俾能有效應付聯邦政府外部之 IT 安全攻擊，該局原本擔任國家資通安全事務中心之角色因此更形強化。新增職權如下：

1. 關鍵基礎設施業者必須提出符合最新資通安全標準之證明。一旦發現安全缺失，聯邦資訊科技安全局得與相關主管機關協商，下令廠商改善。
2. 聯邦資訊科技安全局成為全國關鍵基礎設施之 IT 安全通報中心。相關設施業者必須向其通報足以影響服務之 IT 系統重大干擾。反之，該局亦須收集及評估與防護關鍵基礎設施 IT 安全有關之所有信息，並提供予業者及其目的事業主管機關。
3. 一旦發現某一關鍵基礎設施 IT 系統出現應通報之干擾，聯邦資訊科技安全局亦得同時要求產品及系統製造商共同參與解決方案。
4. 賦予聯邦資訊科技安全局檢測 IT 產品安全之權限。
5. 擴大聯邦資訊科技安全局分析聯邦政府所屬網站界面及紀錄資料之職權，要求各政府機關必須支援聯邦資訊科技安全局之分析作業。
6. 為提升聯邦政府網路之安全性，聯邦資訊科技安全局有義務為聯邦政府資訊技術制定最低標準。

條文要旨：

第 1 章　修正聯邦資訊科技安全局法
第 2 章　修正核能法
第 3 章　修正能源法
第 4 章　修正電信媒體法
第 5 章　修正電信法
第 6 章　修正聯邦薪資法
第 7 章　修正聯邦刑事局法
第 8 章　（刪除）
第 9 章　修正聯邦規費法結構改革法
第 10 章　評估報告
第 11 章　生效日期

資料來源：

1.https://www.jurion.de/gesetze/itsg/（最後瀏覽日：2018/04/10）

2.http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf（最後瀏覽日：2018/04/10）

日本

網路安全基本法

サイバーセキュリティ基本法

（平成二十六年十一月十二日法律第 104 號）

（最新修正：平成二十八年四月二十二日法律第 31 號）

法案簡介：

一、立法經緯

近年拜資通科技發展迅速之賜，產業結構與民眾生活發生極大變革。依日本「平成 25 年（2013 年）通信利用動向調查結果」，該國網際網路之人口普及率約達 8 成，網路就其社會經濟活動已是不可或缺。日本為促進網際網路之應用，曾於 2000 年制定「高度資訊通信網路社會建構基本法」（簡稱「IT 基本法」），惟欠缺網路安全保護之法規架構。嗣後隨著智慧型手機、行動裝置、雲端服務等新興科技普及，所衍生之跨國網路攻擊、政府機關或私人企業之機密或資料遭竊取，甚至金融、電力、交通等關鍵基礎設施遭駭客入侵等威脅資通安全情事遽增，致使該國防範網路犯罪、保護個人資料等資安風險管理議題面臨嚴竣考驗。

再者，鑑於 2012 年倫敦奧會期間曾發生數量龐大之網路攻擊事件，為免東京於 2020 年舉辦奧林匹克運動會期間，出現網路攻擊情事影響賽事進行，而斲喪國家威信，爰確保資通安全成為東京奧運最重要課題之一。

此外，為解決網路安全課題，強化政府資訊安全政策會議之功能，以及促成各級政府機關之資安情資的共享，要求關鍵基礎設施業者應配合資安措施及推動資安人才培育，充實資安維護能量等事項，均為當務之急。

基於上揭因素，自民黨之網路安全對策會議草擬「強化網路安全體制之建言」，並依據此建言擬具「網路安全基本法草案」。該草案於 2014 年 6 月 11 日，由自民黨、民主黨、公明黨、日本維新會等跨黨派國會議員共同提出，並於同年 12 月 6 日完成立法，期與「IT 基本法」相輔相成，營造健全之網路應用環境。該法明定，於內閣設置「網路安全戰略總部」，以促進與 IT 戰略總部及國家安全保障會議之合作。

該法施行之後，物聯網、無線網路等資通科技更為盛行，在享受新興科技為經濟活動、日常生活帶來便捷之同時，由於網路攻擊型態變幻莫測，資安危機也悄然而至。2015 年日本年金機構因遭外來可疑電子郵件不當存取，導致 125 萬件個人資料外洩，促使日本政府更深切體認資通安全威脅之嚴重性，遂於 2016 年修法，將特殊法人納入規範對象，期建構完善資安風險防禦體制。

二、「網路安全基本法」概要

（一）定義

本法所稱之網路安全為：

1. 防止數位資訊洩漏、消失或毀損等數位資訊安全管理之必要措施。
2. 為確保資訊系統及資通網路之安全性與信賴性而採取必要措施，以求適切管理。

（二）基本理念

推動網路安全措施時，應依循下揭基本理念：

1. 與多個單位合作，就資安威脅積極處理。
2. 加強每位國民對資通安全之認識，促其自發性處理資安問題，並建立迅速復原機制。
3. 致力建構善用資通技術之經濟社會。
4. 發揮先導之功能，協助國際秩序之建立與發展。
5. 參酌 IT 基本法之基本理念。
6. 切勿不當侵害國民之權利。

（三）網路安全戰略

為有效落實資安管理措施，本法賦予政府擬訂「網路安全基本計畫」（簡稱「網路安全戰略」）之義務，且須向國會報告戰略之內容，並以網路等方法公布之。該「戰略」應記載之內容如下：

1. 網路安全措施之基本方針。
2. 行政機關等確保網路安全之相關事項。
3. 促進關鍵基礎建設事業及地方政府等確保資通安全之相關事項。

（四）基本措施

明定政府應採行下揭措施：

1. 中央行政機關應確保網路安全

   中央政府應對其行政機關及獨立行政法人之網路安全，訂立統一資安標準，針對資訊系統之不法行為進行監視、分析，並與國內外相關機構合作，協力處理資安威脅。
2. 要求關鍵基礎建設產業及地方政府等應確保網路安全
3. 促進民間企業及教育研究機構等之自發性致力維護網路安全
4. 政府與民間應密切合作，致力推動網路安全措施
5. 防制網路犯罪及防止受害擴大
6. 有嚴重影響國家安全之虞情事之處置
7. 振興產業及強化國際競爭力
8. 促進研究開發
9. 人才培育等
10. 教育宣導及加強資安知識
11. 促進國際合作等

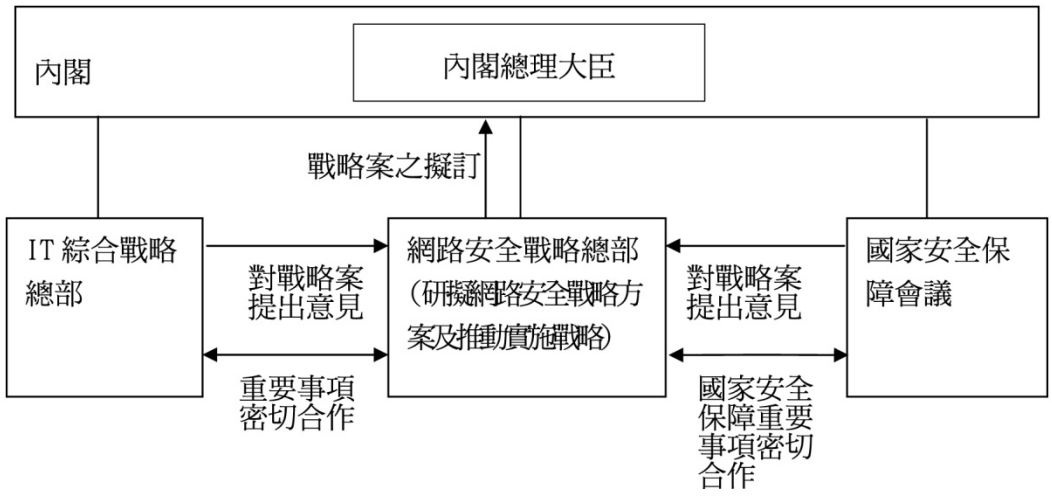
（五）網路安全戰略總部

1. 組織

   為有效推動網路安全措施，於內閣官房設網路安全戰略總部，並置總部長、副總部長及總部員。由內閣官房長官、國務大臣分別充任總部長、副總部長。至於總部員之成員，除與網路安全業務較相關之行政機關首長外，亦由民間遴選卓越學者專家充任之。
2. 掌理事項
   (1) 擬研網路安全戰略方案及推動實施戰略。
   (2) 擬訂國家行政機關及獨立行政法人之網路安全措施基準，並就依該基準訂定之措施進行評估（含監查）。
   (3) 國家行政機關發生之重大網路安全事件所採取措施之評估（含調查原因）。
   (4) 上揭事項之外，網路安全措施重要企劃之調查審議、跨部會

之計畫與相關行政機構之預算編列方針及措施執行方針之訂立等。

3. 總部長之權限
   (1) 總部長依據該總部完成之評估報告或行政機關提供之情資，於必要時，得對相關行政機關首長予以勸告。
   (2) 得要求相關行政機關首長針對依勸告而採取之措施，提出報告。
   (3) 針對所發出之勸告，如有必要，得向內閣總理大臣陳述意見。
4. 資料之提供等
   (1) 相關行政機關首長應適時提供必要之資料，以利總部執行業務。
   (2) 為遂行掌理事務而有必要時，總部得要求地方政府首長、獨立行政法人首長、國立大學法人之校長等提供必要之協助。
5. 保密義務
   受網路安全戰略總部委託處理資安業務者，不得洩漏或盜用從事業務獲悉之秘密，違者處一年以下有期徒刑、50 萬日圓以下罰金。
6. 網路安全戰略總部之權限



（六）2016 年修法重點

1. 擴大政府網路安全措施之適用對象

針對網路安全統一基準之訂立、資訊系統不當活動之監督及分析、網路安全演練，增列適用對象。

	中央省廳	獨立行政法人	特殊法人、認可法人
監查	修法前		增列
查明原因	修法前	增列	
監視(GSOC)	修法前	增列	

2. 網路安全戰略總部之部分業務得委託獨立行政法人資訊處理促進機構（Information-technology Promotion Agency）。

條文要旨：

第一章　總則

第　一　條　　目的
第　二　條　　用語定義
第　三　條　　基本理念
第　四　條　　國家之職責
第　五　條　　地方政府之職責
第　六　條　　重要社會基礎事業者之職責
第　七　條　　網路相關業者及其他業者之職責
第　八　條　　教育研究機構之職責
第　九　條　　國民之努力
第　十　條　　法制措施等
第十一條　　行政組織之建構等

第二章　網路安全戰略

第十二條　　網路安全基本計畫

第三章　基本措施

第十三條　　國家行政機關等確保網路安全
第十四條　　促進重要社會基礎事業者等確保網路安全
第十五條　　促進民間業者及教育研究機構等自發性致力網路安全

資料來源：

1. http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/viewContents?lawId=426AC1000000104_20161021（最後瀏覽日：2018/04/10）
2. https://www.nri.com/~/media/PDF/jp/opinion/teiki/chitekishisan/cs201504/cs20150408.pdf（最後瀏覽日：2018/04/10）

3. 川合将之「サイバーセキュリティに関する施策を総合的かつ効果的に推進」（時の法令 1975 号 2015/04）（最後瀏覽日：2018/04/10）

（國會圖書館簡任編纂趙俊人
簡派編審紀瑪玲
編譯助理研究員葉靜月
編譯助理研究員紀麗惠）