證券暨期貨市場各服務事業

網路安全防護參考指引

第一章 總則

第一條 （目的）

為強化證券商、期貨商及投信投顧業者之資通安全，依據金融監督管理委員會「金融資安行動方案」強化金融業資安防護能力，針對網路安全之風險議題，擬定網路安全防護參考指引。

第二條 （適用範圍與對象）

本指引適用之組織包括證券商、期貨商、證券投資信託事業及證券投資顧問事業。適用對象分為以下兩類說明：

一、第一類：

依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之組織。

二、第二類：

非屬第一類範圍之組織。

三、外資集團在台子公司或分公司，其資安管理政策由外國母公司或總公司控制與建置者，如其母公司或總公司已建置或設立相關控制措施，且有較佳之規範，則從其規範；若無，則應遵循本國法令法規規範。

四、以下參考指引如無特別說明，皆為第一類及第二類組織應遵循之事項。

第三條 （名詞定義）

一、資通系統：

係指用以蒐集、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。

二、存取：

係指存取資訊資產的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。

三、網路設備：

係指傳輸資料、應用程式、服務和多媒體所需的網路通訊元件，如防火牆、路由器、交換器...等，亦為組織的網路架構圖包含的項目。

四、資通安全事件：

係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

五、資訊資產：

係指與資訊處理相關之資產，包括硬體、軟體、資料、文件及人員等（如：伺服器主機及使用者電腦之作業系統及應用程式等軟體資訊）。

六、 資訊服務供應商

係指符合「證券暨期貨市場各服務事業資通系統與服務供應鏈風險管理參考指引」遴選條件之廠商。

第二章 網路架構與網路安全管理

第四條 （網路架構定義）

一、透過網路架構規劃協助組織在規劃業務運作系統架構時能夠更加全面性考量業務維運與資通安全。

二、網路架構圖應呈現組織維持業務運作之必要網路環境設備(如：防火牆、路由器、交換器、系統設備、線路配置、伺服器與服務、無線網路)，另針對網段、路由規劃、主機 IP 位址、備援線路應有相關檔案紀錄。

第五條 （網路區域劃分）

一、為確保網路架構安全，應獨立劃分各工作區域並落實網段隔離。

二、網段應以維持業務運作劃分區域：如非軍事區（Demilitarized Zone, DMZ）、營運區（Production, Prod.）、測試區（Unit Test, UT 或 User Acceptance Test, UAT）及其他等網段。

三、組織應定義外部網路與內部網路，外部網路連接網際網路，內部網路區域為組織人員與內部服務的伺服器配置區域。由外部網路到內部網路的流量需要經過存取控制，僅限於組織內人員公務用或資訊服務供應商申請核准後使用，避免非允許的服務進入。

四、組織之內部網段宜規劃以虛擬區域網路（Virtual Local Area Network, VLAN）區隔，區域劃分方式可依據組織內部單位、部門、業務性質等，並限制不同 VLAN 間的存取。

五、組織應使用適當方式隔離限制存取與特定服務，且資訊人員應視區隔方式，定期檢視防火牆規則或存取控制清單（Access Control List, ACL）。

第六條 （網路設備防護基準）

一、組織應避免使用生命週期終止（End of Service, EOS/End of Life, EOL）之網路設備，並針對 EOS/EOL 之網路設備擬定汰除相關計畫。

二、組織應定期檢視官方發布之軟體、韌體、弱點修補程式之更新，經過評估後將網路設備更新至最新版本或廠商建議版本。

三、組織經由網際網路連線至內部網路進行遠距之系統維護，應落實身份認證機制。

四、組織所有網路設備之防護基準應依「證券暨期貨市場各服務事業資通系統安全防護基準參考指引」。

第七條 （無線網路）

一、組織如有提供內部無線網路使用，其存取保護應採用現行公開資訊已認可且無弱點之安全協定，並比照組織內部網路管理程序，僅限於組織內人員公務用或資訊服務供應商申請核准後使用。

二、組織如有提供外部無線網路使用，其存取保護應採用現行公開資訊已認可且無弱點之安全協定。

三、組織應建立無線網路密碼原則，以降低密碼破解之風險。

第八條 （外部設備存取內部網路）

組織如允許組織人員或資訊服務供應商使用外部設備存取內部網路，應提出申請並檢視設備安全性與相關授權，並限制存取範圍。

第三章 網路設備安全管理

第九條 （網路設備管理）

一、網路設備管理人員之管理帳號應僅限管理人員使用且不得共用帳號，管理帳號之密碼設定原則應遵循組織之身份驗證管理規範。

二、組織應限制網路設備管理使用之人員、設備、IP、網段，或採用一次性密碼（One-time password, OTP）、短暫性存取（Temporary Privileged Access）等措施，並留存使用人員操作紀錄。

三、網路設備修補程式發布時，網路設備管理人員應取得修補程式，並經評估後進行網路設備修補程式更新作業。

第十條 （網路設備規則管理）

一、網路設備規則（例如：網路存取規則、防火牆規則等）新增、異動、刪除應審核使用者需求，經評估資通安全風險程度後進行規則變更，並保留相關紀錄備查。

二、網路設備規則設立應以使用者角色最小授權及正面表列為原則。

三、組織應至少每年檢視一次網路設備規則，並評估規則適切性，移除不必要之規則。

第十一條（網路設備日誌）

一、組織應留存網路設備日誌，遵循內部備份規範，並定期檢視以確保可用性。日誌應至少保留六個月，供留存備查。

二、網路設備日誌應予以保護以防止未經授權存取。

第十二條 （網路設備委外管理）

組織所有網路設備若委由資訊服務供應商維運或管理應依「證券暨期貨市場各服務事業資通系統與服務供應鏈風險管理參考指引」。

第四章 網路連線安全

第十三條（網路連線安全憑證）

一、組織應確保 SSL/TLS 憑證之有效性及合法性，以維持網路連線之安全性。

二、組織如提供網路下單服務，應訂定憑證交付程序，避免非本人取得憑證，並搭配與登入雙因子之不同因子（例如：OTP、SIM 認證）驗證機制交付憑證，及全面使用認證機制。

第十四條（網路傳輸與連線安全管理）

一、組織在不影響營運狀況下應使用較安全的加密連線提供內/外服務。

二、組織如使用網路專線與合作第三方機構網路連線，應架設防火牆，關閉非約定之埠號以確保組織內部網域安全。

三、證券期貨業者如提供網際網路下單服務，畫面應採加密方式處理。

四、如有國際傳輸機敏資料時，組織應建立加密傳輸機制，當涉及客戶資訊，傳輸前應取得當事人授權且不違反主管機關對國際傳輸之限制，並留存完整稽核紀錄。

第十五條（遠端連線）

一、組織應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求及文件化，並建立安全的遠距連線機制，包含：採多因子身分驗證機制（員工帳號密碼、動態密碼、一次性帳密）、加密連線、採最小授權原則、留存完整使用者操作稽核軌跡、監控與警示異常操作行為、執行安全性漏洞更新等安控措施，並留存相關紀錄由權責主管定期覆核。

二、組織須限制僅能由組織內人員登入連線，設備操作軌跡應保有完整紀錄，並依據職掌作業時間訂定可開放連線時段相關規範。

三、組織須透過安全的連線機制來阻擋惡意或未經授權之連線，並以最小權限原則設定規則及關閉非必要之埠號，並應監控網路流量及異常警告及中斷連線機制。

四、組織須以最小授權原則，對使用者進行存取系統權限之差異化管理，僅能有執行業務之必要功能權限，關閉非必要之系統功能授權。

第五章 網路攻擊防護機制及安全性檢測

第十六條（網路攻擊防護機制）

一、第一類組織應建立維持業務運作之網路攻擊防護機制，如：入侵偵測及防禦機制。第二類組織應評估建立維持業務運作之網路攻擊防護機制。

二、具網路下單服務或設有官方網站之證券業者及期貨業者應建立分散式阻斷服務之防護機制。

三、具有對外服務之資通系統者，應建置應用程式防火牆。

第十七條（安全性檢測）

一、組織應定期評估自身網路環境安全（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等）。

二、組織應定期修補網路環境之安全漏洞，並留存相關文件。

三、第一類組織之資通系統應每年辦理一次系統滲透測試。第二類組織應評估定期辦理系統滲透測試。

四、第一類組織應每年辦理一次資通安全健診，包含網路架構檢視、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及目錄伺服器設定及防火牆連線設定檢視。第二類組織應評估定期辦理資通安全健診。

第六章 事件偵測及管理

第十八條（事件偵測）

一、組織應建立網路環境安全威脅偵測管理機制，包含事件收集、異常分析、偵測攻擊並判斷攻擊行為。

二、組織應偵測釣魚網站及惡意網站連結並提醒使用者防範網路釣魚。

第十九條（事件通報及應變）

一、組織應訂定資通安全事件內部通報機制，包含正式之通報程序及資通安全事件通報聯絡人。

二、於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件應依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當應變程序及留存紀錄。

三、組織遇有重大個人資料安全事故者，應立即通報主管機關。前項所稱重大個人資料安全事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及組織正常營運或大量當事人權益之情形。