Deloitte.

勤業眾信

證券暨期貨市場各服務事業網路安全防護參考指引說明

Deloitte Risk Advisory、2022/05

Agenda

- 目的 & 總說明
- 條文說明
- 問題與討論

目的 & 總說明

目的 & 總說明

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。

總說明

本參考指引係參考 ISO 27001、資通安全管理法、證券暨期貨市場各服務事業建立內部控制制度處理準則、建立證券商資通安全檢查機制、建立期貨商資通安全檢查機制、證券商內部控制制度標準規範、期貨商內部控制制度標準規範、金融機構資通安全防護基準、行政院國家資通安全會報技術服務中心共通規範、期貨商因應嚴重特殊傳染性肺炎(COVID-19)事件申請居家辦公指引、金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法等，經蒐集實務做法併邀集業者共同研議相關參考指引，以維護網路安全防護資訊安全。

本指引共十九條，其要點如下：

一、 說明本指引之立法意旨。(第一條)

二、 說明本指引之適用範圍。(第二條)

三、 明訂本指引提及之名詞解釋。(第三條)

四、 明訂網路架構與網路安全管理要求。(第四條至第八條)

五、 明訂網路設備安全管理要求。(第九條至第十二條)

六、 明訂網路安全連線要求。(第十三條至第十五條)

七、 明訂網路攻擊防護機制及安全性檢測要求。(第十六條至第十七條)

八、明訂事件偵測及管理要求。(第十八條至第十九條)

條文說明

網路安全防護參考指引適用對象

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用對象分類		
第一類	**第二類**	**外資**
（一）「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）「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商。 （三）「建立期貨商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級期貨商。	非屬第一類範圍之組織。	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。

「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36條之2條文

一、 證券商實收資本額達新臺幣(以下同)一百億元以上或電子下單達一定比率；電子下單一定比率為網際網路下單加計電子式專屬線路下單(Direct Market Access，以下簡稱DMA)成交金額達公司成交金額百分之六十，經紀業務成交金額市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

二、 期貨商實收資本額達二十億元以上，且電子下單達一定比率；電子下單一定比率為網際網路下單加計DMA下單成交口數達公司成交口數百分之六十，經紀業務成交口數市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

三、 證券投資信託事業及證券投資顧問事業前一年度月平均境內外管理資產規模達六千億元以上者。

註1：參考資料為「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36條之2條文

註2：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。

網路安全防護參考指引-第一、二、三條

條文	內容
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） 詳前頁說明。
第三條	（名詞解釋） 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）。

網路安全防護參考指引-第四、五、六條

條文	內容
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，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」。

網路安全防護參考指引-第七、八條

條文	內容
第七條	（無線網路） 一、組織如有提供無線網路供內/外部人員使用，無線網路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。 二、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） 組織如允許內/外部人員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。

網路安全防護參考指引-第九、十、十一、十二條

條文	內容
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) 資訊服務供應商需存取組織資訊資產、營業秘密時，專案負責人應考慮以下各項因素評估風險： 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) 組織於專案進行中應注意下列事項： 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外部廠商維運或管理應依「證券暨期貨市場各服務事業供應鏈風險管理參考指引」。

網路安全防護參考指引-第十三、十四、十五條

條文	內容
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。

網路安全防護參考指引-第十六、十七條

條文	內容
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、進階持續性威脅攻擊防禦措施等防護機制。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。

網路安全防護參考指引-第十八、十九條

條文	內容
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。

條文內容說明

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。

內容說明

- 應定義各個工作區之網段，並確保網段隔離(如，邏輯隔離、實體隔離)。
- 網路架構圖提供組織人員能夠簡單快速了解組織網路架構、線路狀態、備援狀態、重要節點網路設備、重要伺服器、區域分隔與對應IP網段、重要設備實體位置標註，以協助管理者進行組織網路的維運。
- 組織應使用適當方式隔離限制存取與特定服務(參閱第五點)

佐證資料範例

- 組織訂定之網路管理使用程序
- 網路架構圖
- 防火牆規則或ACL檢視紀錄

第五條-網路區域劃分

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。

內容說明

- 組織應依據業務運作劃分不同屬性之網段(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)，作為存取控制與安全規劃的基準群組。

- 不同區域應限制所能存取的服務、應用程式、資料庫等，以保護營運區環境系統及資料安全。

佐證資料範例

- 組織訂定之網路管理使用程序
- 網路架構圖
- 防火牆規則或ACL檢視紀錄

第五條-網路區域劃分

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，避免非允許的服務進入。

內容說明

- 外部網路係指連接網際網路；內部網路係指組織人員與內部服務的伺服器配置區域。
- 組織對外網路區域，連接外部網路至內部網路，需要經過存取控制(如防火牆)，非允許的服務與來源不能進入其他區域。
- 實務上經常於外部網路與內部網路之間規劃DMZ(非軍事區)，以配置對外服務伺服器。DMZ至內部網路亦需經過存取控制。除特殊因素外，來自於外部網路之連線建議僅允許其連接至網站主機、郵件主機或其他提供對外服務之主機。

佐證資料範例

- 組織訂定之網路管理使用程序
- 網路架構圖
- 防火牆規則或ACL檢視紀錄

第五條-網路區域劃分

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。

內容說明

- 建議組織VLAN的劃分應該依據實際的需求，依據內部單位、部門、業務性質等作為依據並進行適當的劃分，劃分的目的主要將不同屬性的群體做分隔，分隔後除了可以限定特定服務的傳遞外，也可以進一步進行不同VLAN間的存取控制。

佐證資料範例

- 組織訂定之網路管理使用程序
- 網路架構圖
- 防火牆規則或ACL檢視紀錄

第五條-網路區域劃分

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）。

內容說明

- 組織區域間的存取控制檢測時，需要確認區域間的設備狀況(如透過防火牆、核心交換器等)。
- 確認區域間管理規則有正確設定啟動，同時檢測條例是否有過多之現象、條例是否妥善控管、未使用的規則定期檢討刪除，並刪除不必要規則，以免累積後難以維護。
- 建議備註說明此規則建立原因、用途、需求單位、使用期間等等，以利管理。

佐證資料範例

- 組織訂定之網路管理使用程序
- 網路架構圖
- 防火牆規則或ACL檢視紀錄

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。

內容說明

- 使用生命週期終止(EOS/EOL) 之網路設備，因原廠不再提供更新與支援服務，可能增加資安風險，且提高維護成本。
- 應依據組織業務，避免生命週期終止(EOS/EOL) 之網路設備。
- 若無法立即汰除生命週期終止(EOS/EOL)之網路設備(如，可能造成業務中斷等情況)，應擬定汰除相關計畫。

佐證資料範例

- 組織訂定之資訊資產管理作業程序
- 資訊資產汰除計畫

第六條-網路設備防護基準

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。

內容說明

- 網路設備版本更新會修正功能、更新驅動程式、修補已發現的安全漏洞等等，協助最佳化設備並防止設備漏洞遭惡意人士利用。
- 網路設備應定期檢視官方發布之軟體、韌體、弱點修補程式版本，若有釋出之最新版或廠商建議版本，應評估該版本相關內容、受影響程度、更新方式及更新時程等。
- 若發現網路設備廠商已公開揭露且已被駭客利用之重大資安弱點，應評估該弱點之相關內容、受影響程度修補方式及修時程。
- 進行修補程式更新時，建議先於測試環境進行相關修補測試 ，確認系統功能正常後部署於正式環境。

佐證資料範例

- 組織訂定之網路設備管理辦法

第六條-網路設備防護基準

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。

內容說明

- 組織可能因使用需求，使用者(如管理人員、外部廠商等)需利用遠距連線或遠端登入軟體等，透過網際網路登入遠端伺服器主機或個人電腦之設備進行維護作業。遠距維護時應落實身分驗證機制(如AD驗證)，建議採雙因子驗證機制。

- 實務上常透過VPN建立安全通道，以保護連線過程的機密性與完整性，惟此種遠端連線行為因具備高度資安風險，很可能被惡意攻擊者利用作為系統入侵管道，故組織宜使用網路安全監控設備(如Firewall、WAF及IPS/IDS等)或服務(如SOC監控等)，監控遠端存取組織內部網段或資通系統後臺之連線，以及時發現異常連線或惡意攻擊行為。

佐證資料範例

- 組織訂定之遠距工作作業辦法
- 遠端連線申請

第七條-無線網路

一、組織如有提供無線網路供內/外部人員使用，無線網路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。

內容說明

- 無線網路係指不需要實體線路即可傳輸訊號之網路傳輸環境。
- 如有提供無線網路連線服務時，組織應制定相關規範，已符合最低必要之安全規則 ，降低發生資訊安全事件之風險，並維護無線網路使用連線安全。
- 應避免使用WEP、WPA等已知弱點之加密模式
- 無線網路環境應依組織規範進行網段區隔。
- 建議隱藏無線網路SSID，並依組織規定進行控管(如存取帳號控制、綁定MAC等)

佐證資料範例

- 組織訂定之無線網路管理辦法

第七條-無線網路

二、組織應建立無線網路密碼原則，以降低密碼破解之風險。

內容說明

- 無線網路使用者應以組織規範申請無線網路使用，使用者應使用專屬帳號並落實帳號密碼原則，避免帳號密碼予非授權人員使用。

佐證資料範例

- 組織訂定之無線網路管理辦法

第八條-外部設備存取內部網路

組織如允許內/外部人員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。

內容說明

- 外部設備係指非組織提供之設備(如，自攜設備、自攜行動裝置、外部供應商設備等)
- 如允許內/外部人員使用外部設備存取內部網路，應依組織規範進行申請與授權，並限制存取範圍。
- 安全性檢視如經掃毒後無病毒存在、防毒軟體病毒碼更新、作業系統為妥適版本等。
- 建議外部設備非必要盡量不接觸伺服器主機、連結內部網路、傳輸或儲存正式環境資料。

佐證資料範例

- 組織訂定之設備管理作業程序
- 外部設備存取申請單

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。

內容說明

- 應建立網路設備帳號管理機制，以適切管理提供網路服務之硬體、軟體及相關網路服務帳號(如路由器、交換器等)。
- 應訂定符合組織之網路設備帳號管理程序，包含帳號之申請、建立、修改、啟用、停用及刪除等作業規範並落實執行。帳號異動流程，一般可透過紙本或電子化系統完成，填寫相關表單(如系統帳號/權限異動申請單等)。
- 網路設備管理帳號應依據組織規劃，僅限管理相關人員使用，且不得共用帳號，以防止未授權操作與確保可歸責性。
- 網路設備管理帳號之密碼設定原則應依據組織身分驗證管理規範(如密碼複雜度、最短效期、最長效期等)

佐證資料範例

- 組織訂定之網路設備管理辦法
- 帳號異動申請單
- 網路設備管理使用者檢視記錄

第九條-網路設備管理

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。

內容說明

- 應建立網路設備帳號管理機制，以適切管理提供網路服務之硬體、軟體及相關網路服務帳號。網路設備管理人員、設備、IP、網段，應進行最小範圍限制，避免未授權存取。
- 例如，除內部許可之IP可使用加密方式(如SSL)連接登錄管理外，其餘IP一概不得登錄防火牆系統本身設備。
- 若無法進行上述限制，應採用一次性密碼（One-time password, OTP）、短暫性存取（Temporary Privileged Access）等措施。
- 應保留網路設備人員操作紀錄(如防火牆開啟適當稽核功能，記錄連線狀況)。

佐證資料範例

- 組織訂定之網路設備管理辦法
- 帳號異動申請單
- 網路設備管理使用者檢視記錄
- 網路設備稽核軌跡

第九條-網路設備管理

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。

內容說明

- 若發現網路設備廠商已公開揭露且已被駭客利用之重大資安弱點，應評估該弱點之相關內容、受影響程度修補方式及修補時程。

- 進行修補程式更新時，建議先於測試環境進行相關修補測試 ，確認系統功能正常後部署於正式環境。

佐證資料範例

- 組織訂定之網路設備管理辦法
- 修補紀錄

第十條-網路設備規則管理

資訊服務供應商需存取組織資訊資產、營業秘密時，專案負責人應考慮以下各項因素評估風險：

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。

內容說明

- 網路設備規則異動時，應依據組織訂定之流程(如經由使用單位主管、網管人員、資安人員等評估核准)，評估規則適當性、正確性、資安風險等(評估項目如：使用需求、來源位址、目標位址、埠號、服務、使用期間等)。

- 網路設備規則異動應留存相關紀錄，保留年限應依組織訂定之規範。

佐證資料範例

- 組織訂定之防火牆管理作業程序
- ACL/防火牆規則異動申請單
- 組織部署之防火牆規則、ACL

第十條-網路設備規則管理

資訊服務供應商需存取組織資訊資產、營業秘密時，專案負責人應考慮以下各項因素評估風險：

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。

內容說明

- 網路設備規則正面表列(Implicit Deny all , or White-listing)只允許合規網路傳輸通過，應依據組織需求採最小授權原則評估規則啟用。

- 多數網路設備規則有其順序性，由第一條策略往下比對，合乎比對條件即動作後不再往下比對，故建議最後一條規則阻斷不合規的所有連線(Deny all)。

佐證資料範例

- 組織訂定之防火牆管理作業程序
- ACL/防火牆規則異動申請單
- 組織部署之防火牆規則、ACL

第十條-網路設備規則管理

資訊服務供應商需存取組織資訊資產、營業秘密時，專案負責人應考慮以下各項因素評估風險：

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。

內容說明

- 應至少**每年檢視一次**網路設備規則。
- 可評估實際執行需求，並依組織規定清查不必要之規則，如：未使用之規則、開放範圍過大、系統效能、邏輯重複問題等。
- 建議備註說明此規則建立原因、用途、需求單位、使用期間等等，以利管理。

佐證資料範例

- 組織訂定之防火牆管理作業程序
- ACL/防火牆規則異動申請單
- 組織部署之防火牆規則、ACL
- 網路設備規則檢視記錄

第十一條-網路設備日誌

組織於專案進行中應注意下列事項：

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。

內容說明

- 應訂定相關管理辦法以妥善留存網路設備日誌(如防火牆系統所產生之稽核紀錄) ，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。
- 考量網路設備日誌有滅失之可能，應依據組織訂定之規範進行定期備分(如備份至儲存媒體、受控管設備或集中化稽核日誌儲存主機(Log Server))。
- 網路設備日誌留存期限應至少保留**六個月**。

佐證資料範例

- 組織訂定之防網路設備管理作業程序
- 網路設備日誌備分紀錄
- 網路設備日誌檢視紀錄

第十一條-網路設備日誌

組織於專案進行中應注意下列事項：

二、網路設備日誌應予以保護以防止未經授權存取。

內容說明

- 為避免網路設備日誌遭竄改之風險，應設置權限存取控管機制。網路設備日誌應依據組織訂定之規範僅限定相關人員檢視及調閱(如只能由網路管理人員、權責主管、資訊安全人員等)。

- 建議針對使用者存取帳號僅限唯讀存取，禁止任何人具權限可刪除紀錄。

佐證資料範例

- 組織訂定之防網路設備管理作業程序
- 網路設備日誌存取權限

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。

內容說明

- TLS憑證(亦稱SSL憑證)服務，透過TLS加密傳輸協定建立瀏覽器與站台伺服器之間的安全通道。為避免TLS憑證被人惡意破解偽造，資通系統應設定憑證使用效期並定期更換。開對外服務站台應使用公正第三方所簽發之SSL憑證，以政府伺服器數位憑證管理中心(GTLSCA)為例，109年9月1日起所簽發之TLS憑證已調整為1年效期。組織內部使用之站台若使用自行簽發之TLS憑證，亦須避免使用萬年憑證，應評估資安風險及使用需求後，設定合理使用效期。

佐證資料範例

- 組織訂定之系統發展維護辦法
- 組織訂定之金鑰管理規範
- 系統憑證資訊

第十三條-網路連線安全憑證

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。

內容說明

- 組織如提供網路下單服務，應訂定憑證交付程序

- 多重認證技術係指採用兩種以上不同身分驗證因子，意即使用MFA (Multi-Factor Authentication)。身分驗證因子依類型，可分為所知之事、所持之物及所具之形等；所知之事係指利用限使用者知道的知識內容驗證身分，如密碼、PIN碼及安全問答等；所持之物則利用使用者擁有的實體或非實體物品，如憑證、晶片卡、SMS簡訊驗證碼、符記(Token)及一次性密碼(OTP)等；而所具之形為使用者具有的生物特徵辨識技術，如臉部、聲紋、指紋及虹膜等。

佐證資料範例
- 組織訂定之憑證作業管理程序

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。

內容說明

- 組織在不影響營運狀況下，內外服務可實作加密機制，如HTTPS、SSH、SFTP等加密傳輸協定，或透過應用程式等適當方式，先行將資訊加密後再傳輸，以保護資料機密性與完整性。

- 實務上常建立已加密之安全通道(如HTTPS與VPN等)保護傳輸資料之機密性。當站台啟用HTTPS，於瀏覽器網址列上會出現安全鎖頭圖示。

- 當無法使用加密連線時，另一種替代方案如將機敏資訊先以應用程式或其他軟硬體實作加密或編碼保護後，再進行網路傳輸。

佐證資料範例

- 組織訂定組織訂定之系統發展維護辦法
- 資通系統加密連線之測試報告

第十四條-網路傳輸與連線安全管理

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。

內容說明

- 組織如使用網路專線與合作第三方機構網路連線，應依據組織規範評估需求與風險，並依需求設立防火牆規則，僅允許授權之流量通過，關閉非約定之埠號或服務。

佐證資料範例

- 組織訂定之防火牆安全管理作業程序
- 部署之防火牆規則

第十四條-網路傳輸與連線安全管理

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（例如：TLS1.3）處理。

內容說明

- 為保護網際網路下單服務安全性，下單畫面應採用加密機制以建立安全通道(如啟用HTTPS TLS 1.3加密傳輸協定等)。

- SSL V3及TLS1.0皆已被視為安全性不足，若無相容性問題，建議停用。110年3月，RFC 8996標準正式棄用TLS1.0及TLS 1.1。對IE、Edge、Chrome、Safari及Firefox而言，目前皆建議網站採用TLS 1.3。另外，加密協定所使用的演算法(Ciphers)亦有安全考量，如RC2、RC4、DES及3DES等加密演算法已遭破解，建議可改用AES與RSA等尚未遭破解之加密演算法。

佐證資料範例

- 組織訂定之系統發展維護辦法
- 系統加密連線之測試報告，如Nmap檢測結果

第十四條-網路傳輸與連線安全管理

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。

內容說明

- 如有國際傳輸機敏資料時組織應實作加密傳輸機制，如HTTPS、SSH、SFTP等加密傳輸協定，或透過應用程式等適當方式，先行將資訊加密後再傳輸，以保護資料機密性與完整性，並保留相關文件與稽核軌跡。

佐證資料範例

- 組織訂定之資料傳輸作業規範
- 傳輸稽核軌跡

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。

內容說明

- 應控管所有允許的遠端連線行為，其中包含對於應用程式及作業系統資源的存取控制，應通過授權檢查後始可放行。應建立相關使用限制、組態需求及連線需求，其中包含使用者身分類型、來源位址、連線人數上限、網路連線類型、開放時段、允許存取的功能資源及任何先備條件等限制。

- 使用情境如為因應遠距辦公之需求而開放VPN連線存取，但限制使用者須為組織同仁透過AD帳號登入，並使用組織配發之OA電腦，檢測已安裝及更新防毒軟體後始可連線，連線後僅允許存取特定系統功能。

佐證資料範例

- 組織訂定之網路管理規範
- 防火牆規則、存取控制列表(ACL)
- 存取控制功能之測試紀錄
- 系統連線日誌

第十五條-遠端連線

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。

內容說明

- 應訂定相關管理辦法以妥善留存遠端連線日誌，，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。
- 存取控制資訊應文件化，有助於日常維運遵循與日後稽核查檢作業。
- 建議啟動稽核功能與安全性監控，並須依據組織所規定之檢核頻率要求，進行檢視，以確保無未經授權之連線使用。

佐證資料範例

- 組織訂定之網路管理規範
- 組織部署之防火牆規則、ACL
- 存取控制功能測試紀錄
- 系統連線日誌

第十五條-遠端連線

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。

內容說明

- 遠端存取行為應通過授權後始可放行，若有必要允許外部遠端存取之系統功能時，應限制遠端存取控制點以降低遭受攻擊機會，如識別來源主機、來源端IP位址、目的端IP位址、埠口及通訊協定等連線限制，避免全面性開放存取。

- 為保護遠端存取連線的機密性與完整性，應採用加密機制以建立安全通道(如啟用HTTPS TLS 1.3加密傳輸協定等)。

- 實務上組織可能因居家辦公等使用需求，而允許同仁或系統維護人員遠端存取內部網段之服務或後臺，此時常會建立VPN安全通道，並可限制遠端來源以降低存取風險，VPN遠端存取資通系統服務。如網路設備允許管理人員透過遠端桌面服務登入系統進行維護操作，為降低被駭客利用遠端桌面服務入侵的機率，亦應啟用加密連線機制。

佐證資料範例

- 組織訂定之網路管理規範
- 組織部署之防火牆規則、ACL
- 存取控制功能測試紀錄
- 系統連線日誌

第十五條-遠端連線

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。

內容說明

- 遠端存取行為應通過授權後始可放行，若有必要允許外部遠端存取之系統功能時，應限制遠端存取控制點以降低遭受攻擊機會，如識別來源主機、來源端IP位址、目的端IP位址、埠口及通訊協定等連線限制，避免全面性開放存取。

- 應檢查使用者存取權限，禁止未經系統授權存取行為。

佐證資料範例

- 組織訂定之網路管理規範
- 組織部署之防火牆規則、ACL
- 存取控制功能測試紀錄
- 系統連線日誌

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、進階持續性威脅攻擊防禦措施等防護機制。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。

內容說明

- 爲維護組織網路及資訊系統使用品質與安全，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、進階持續性威脅攻擊防禦措施等防護機制。應依據組織業務，將風險較高之網際網路進出閘道口、DMZ等，與重要資通系統，納入網路攻擊防護機制範圍，以偵測異常攻擊與違反資安政策之違規事件，確保Internet、Intranet 與 DMZ區域中個人電腦、伺服器及網路設備的安全與正常運作。

- 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。

佐證資料範例

- 組織訂定之網路攻擊防護作業程序
- 組織訂定之入侵偵測防禦管理作業程序
- 資安設備組態設定

第十六條-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。

內容說明

- 分散式阻斷服務攻擊(Distributed Denial of Service ,DDoS)係指利用分散於不同地方的資訊設備(多數為跨國之殭屍網路)進行多對一的攻擊，透過發送難以追查且大量的封包，癱瘓目標資訊設備，使之無法提供服務而導致服務中斷等現象。

- 組織應建立DDoS相關防護處理規範，並落實防護機制(如建置流量清洗服務、網路流量及資源監控機制、啟用網路防護設備DDoS防禦功能、DDoS演練等)

佐證資料範例

- 組織訂定之DDoS應變處理作業程序
- 組織訂定之資訊作業故障應變處理作業程序
- DDoS演練紀錄

第十六條-網路攻擊防護機制

三、具有對外服務之資通系統者，應建置應用程式防火牆。

內容說明

- 具有對外服務之資通系統者應建置應用程式防火牆(Website Application Firewall , WAF)保護網站應用程式，透過監控及過濾網站傳輸的流量，避免網站遭受惡意攻擊、XSS攻擊、資料外洩等應用層(Layer 7)攻擊。

- 建議地端WAF部屬在外部防火牆之後、網站伺服器之前，流量先經由外部防火牆，流量通過WAF分析過濾後，再至網站伺服器。

佐證資料範例

- 組織訂定之網路管理規範
- 組織部署之WAF規則

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）。

內容說明

- 為維持網路環境之可用性與安全性，應依據組織規範定期評估網路相關系統與設備之使用、異動及管理等（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等），避免因不當的使用或管理，導致可能的資訊安全破壞及網路資源浪費。

佐證資料範例

- 組織訂定之資訊設備管理程序
- 組織訂定之網路管理作業程序
- 定期檢視紀錄

第十七條-安全性檢測

二、組織應定期修補網路環境之安全漏洞，並留存相關文件。

內容說明

- 為確保組織業務相關網路環境之安全及降低可能導致之資訊安全風險，組織應訂定相關作業程序。
- 安全漏洞係指因系統組態設定錯誤、通訊協定或系統程式設計不當等，而導致使用者得以未經合法授權取得資源，或惡意使用者致使癱瘓系統等。
- 應依據組織規範定期進行網路安全檢測報告(如弱點評估報告、滲透測試報告)。經確認弱點項目存在者，應先評估修補作業之可行性，而後進行修補作業。建議於修補後追蹤辦理結果並執行複測作業。
- 若評估無法修補安全漏洞，應依組織規範執行例外項目作業，並由主管核准。

佐證資料範例

- 組織訂定之弱點管理程序
- 漏洞修補紀錄

第十七條-安全性檢測

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。

內容說明

- 滲透測試是一種特殊類型評鑑，由技術熟練的資安專家模擬敵人行動，執行之白、灰、黑箱測試及分析等各種檢測活動，對資通系統或個別系統元件辨識可能被敵人利用的弱點。這種測試可用於驗證弱點，或驗證資通系統防護程度已達某種特定限制條件下(如時間、資源或技能等)能力。開始測試前，各方應協調及同意滲透測試場景與規則，宜將滲透測試規則與預期敵人進行攻擊所採用工具、技術及程序相互關聯，並依風險評鑑結果與等級需求進行滲透測試，並在定義之廣度/深度及限制因素下執行滲透測試。

- 第一類組織之資通系統皆應執行滲透測試安全性檢測活動，並提供檢測結果報告或執行紀錄以供查檢，檢測活動之執行週期應符合資安法(如應辦事項等)與組織資安政策之規範。為避免檢測活動流於形式，應確實進行弱點修補作業，並追蹤修復狀況。

- 第二類組織應評估定期辦理系統滲透測試。

佐證資料範例

- 滲透測試檢測報告
- 滲透測試複測報告
- 弱點修補紀錄

第十七條-安全性檢測

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。

內容說明

- 資通安全健診服務係透過整合各項資通安全項目的檢視服務作業，提供受檢單位資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力。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。

- 資通安全健診報告內容建議包括：執行結果摘要說明(依照檢測類別各別摘要說明)、執行計畫(執行期間/執行項目/執行範圍/專案成員)、執行情形(需包含所有服務項目執行結果，不可直接以工具產生之原始結果交付)、改善建議、結論。

佐證資料範例

- 資通安全健診報告
- 辦理資通安全健診之評估

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。

內容說明

- 應建立網路環境安全威脅偵測管理機制加強網路環境設備之安全，包含但不限於安全監控管理系統、威脅偵測系統等，達到資訊安全監控之目的。

- SIEM系統(常見如Arcsight、Qradar)係指透過即時收集並儲存正規化後之各式來源資料(如網路設備、網路使用行為紀錄檔等)，以監控規則(policy)執行關聯分析，提高資訊安全警訊之偵測效率及有效性，以期發現潛在資訊安全風險，俾利適時採取因應之防護措施，以防範可能之駭客攻擊與確保資訊安全。

- 威脅偵測系統(TDS)(包含內網威脅偵測系統、動態沙箱分析系統等)係透過分析所收錄的網路流量，以發現可能威脅(如已知的惡意程式、可疑程序、可疑傳輸行為等)，進行告警或收錄於報表，俾利適時採取因應之防護措施，以防範可能之駭客攻擊與確保資訊安全。

- 宜採用自動化工具(包含基於主機、基於網路、基於傳輸，或基於儲存的事件監控工具或安全事件/資訊管理(SIEM)技術)，以提供即時分析警示或通知。

佐證資料範例

- 組織訂定之監控作業程序
- 錯誤處理功能測試紀錄

第十八條-事件偵測

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。

內容說明

- 網路釣魚係指利用社交工程 (操縱使用者以取得機密資訊)的網路犯罪活動。駭客藉由手動方式發動攻擊，或利用某種工具將攻擊流程自動化，亦或兩者互相搭配，一開始先用腳本工具來突破防線，之後再用手動方式完成攻擊。

- 偵測網路釣魚之機制，例如使用一套電子郵件閘道來攔截垃圾郵件、過濾掉含有可疑連結或附件檔案的郵件、DMARC電子郵件認證工具來防止駭客偽造電子郵件寄件人地址、定期對員工實施網路釣魚模擬攻擊訓練等。

佐證資料範例

- 提醒使用者防範釣魚之警訊或信件
- 網路釣魚演練紀錄

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。

內容說明

- 應建立資通安全通報機制，飽含正式之通報程序及資安事件通報聯絡人等。當發現系統遭不當存取、竄改、毀損等疑似入侵攻擊跡象時，可透過當面告知、電話、簡訊、電子郵件訊息等適當聯絡方式，通知相關人員進行適當處理，人員通知如網路管理者、系統管理者、系統擁有者或各級資安人員等。

佐證資料範例

- 組織訂定之通報應變處理程序
- 組織訂定之資通安全事件管理規範

第十九條-事件通報及應變

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。

內容說明

- 請參閱「證券期貨市場資通安全事件通報應變作業注意事項」

佐證資料範例

- 組織訂定之通報應變處理程序
- 組織訂定之資通安全事件管理規範
- 事件處理紀錄單

第十九條-事件通報及應變

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。

內容說明

- 組織遇有重大個人資料安全事故者，應立即通報主管機關。
- 重大個人資料安全事故包含但不限於外部入侵事件導致個人資料侵害(如駭客入侵竄改、電腦病毒攻擊或資料遭竊等事件)、內部事件導致個人資料侵害(如故意或無故意之資料洩漏、不適當個人資料分享、可攜式儲存媒體遺失等)。

佐證資料範例

- 組織訂定之通報應變處理程序
- 組織訂定之資通安全事件管理規範
- 事件處理紀錄單

問題與討論

Deloitte.

勤業眾信