金融業導入零信任架構參考指引

2024.7.15

一、緣起

因應疫情帶動異地/居家辦公模式，亦隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求。國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國「國家資通安全發展方案(110 年至 113 年)」，將發展零信任網路資安防護環境，推動政府機關導入零信任網路納為推動策略及主要工作項目。本會於 2022 年 12 月發布「金融資安行動方案 2.0」，將「鼓勵零信任網路部署、強化連線驗證與授權管控」列為推動重點之一，期鼓勵金融機構導入零信任網路機制，並搭配網路及資源存取的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。

零信任架構涵蓋整體資安防護框架，於各資安研究組織、提供零信任方案之諮詢顧問或產品供應商間，因存在從不同角度切入而有不同觀點；另其實務上涉及龐大且複雜的資訊與資安架構，導入過程不可能一次到位，並將與既有資安管理機制並存，於達成度亦尚無明確績效指標可參。考量金融機構於資安防護均已有一定基礎量能，於推動及導入零信任過程中已凝聚各方共識，以零信任思維漸進強化資安防護，爰訂定本參考指引供金融機構參考。

二、零信任架構概念

零信任架構的主要精神，是基於「永不信任、持續驗證」的方式，透過持續、多種類的驗證手段，持續強化對系統或資料存取控制的安全性。目前主要參考文件如下：

(一)2020 年美國國家標準技術研究院(NIST)發布 SP 800-207 文件[1]，提出身分鑑別、設備鑑別及信任推斷等 3 大核心組件，並且以身分鑑別為優先導入範圍。

(二)2021 年美國總統發布指令[2]，要求美國聯邦政府採用零信任架構，作為資通安全現代化策略之一。2022 年 1 月，美國預算與管理辦公室制定備忘錄[3]，要求各機構在 2024 財年(FY) 年底前，於身分識別、設備、網路、應用程式與工作負載、資料等 5 個面向滿足特定的安全標準和目標。

(四)2023 年 4 月美國網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)發布零信任成熟度模型 2.0[4]，依身分識別、設備、網路、應用程式與工作負載、資料等五支柱；至自動化與協調、可視性及分析則內含於各支柱中。因應逐步漸進之導入過程，區分傳統、起始、進階、最佳化等四個等級。

(五)我國行政院第六期「國家資通安全發展方案(110 年至 113 年)」之推動策略，數位部資安署將發展零信任網路資安防護環境，並優先推動 A 級公務機關導入試辦。規劃自 111 年起，分年依序導入身分鑑別、設備鑑別、信任推斷等階段，並陸續訂定身分鑑別、設備鑑別、信任推動等產品標準並受理廠商申請產品驗測[5]。

三、零信任架構導入策略

現行銀行、保險、證券等業別多已於高風險應用場域具有一定基礎之資安防護，如採用高強度密碼或雙因子身分驗證，

[1] https://csrc.nist.gov/pubs/sp/800/207/final
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[3] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[4] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
[5] https://www.nics.nat.gov.tw/ZeroTrustMain.htm?lang=zh

並就設備建有作業系統更新及防毒碼更新機制、網段區分外部網路、DMZ、營運環境及其他如內部辦公區，定期進行應用程式安全檢測及資料加密儲存等。建議金融機構以既有資安管理機制為基礎，參採零信任架構概念，為分階段之補強及優化。

考量零信任架構於實務上不可能一步到位，可與既有資安管理機制並存，建議以關鍵保護標的為核心，盤點資源存取路徑（身分、設備、網路、應用程式、資料），由外而內縮小攻擊表面並增進防禦深度、由內而外擴大防護表面；並參採美國 CISA 零信任成熟度模型區分傳統、起始、進階、最佳化等四階段，依據我國金融業屬性及既有資安防護能量調適如下：

(一) 傳統：以靜態指標為主 ，建議優先盤點既有資安防護機制之完整性，規劃防禦深度之優化及整合，不以導入新產品/解決方案為必要。

(二) 起始：以動態指標為主，建立具基於屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點、健康狀況、合規性等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警；並應辨識存取標的之關鍵數據與資源，及其被存取之交易流程，進而定義保護關鍵數據與資源之防護表面(Protect Surface)及對應之零信任政策。

(三) 進階：以即時指標為主，整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制。事件日誌應涵蓋依據起始階段定義之動態屬性及零信任政策產生之行為紀錄。相關日誌可集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如透過 SOC 事件單、SOAR Playbook 等)，建議參考 F-ISAC 資安威脅情資及金融資安監控組態基準。

(四) 最佳：整合指標，建立可依資安政策快速調適之一致性且自動化之管理機制，確保安全性及合規性。

四、零信任架構實作建議

(一)風險導向，擇高風險場域先行

初期導入以規模於可控範圍、減少影響面並可獲致實質補強效益為原則，建議以高風險、低衝擊之場域為優先，並得依風險基礎方法進行適當評估，擇定其導入優先序及範圍。高風險場域例舉如下：

1. 遠距辦公：使用者及設備位於傳統資安防護邊境外。
2. 雲端存取：雲端資源位於傳統資安防護邊境外。
3. 系統維運管理：含重要主機設備及系統軟體(作業系統、資料庫等)之特權帳號管理。
4. 應用系統管理：重要應用系統之管理者(如帳號管理員)或高權限使用者帳號(如可接觸大量個資或機敏資料者)。
5. 服務供應商：如委外廠商之遠端維運管理。
6. 跨機構協作：如重要應用系統開放予外部使用者從外部存取，其人員到離或使用設備非屬本機構管控範圍者。

(二)循序漸進，擇基礎原則先行

美國 NIST、CISA 及國家資通安全研究院雖有各自訂定之導入框架、原則或標準，惟考量實務可行性，建議依前揭高風險場域之完整存取路徑(即身分、設備、網路、應用程式、資料 5 大支柱)，評估既有資安防護機制之完備度，依傳統、初始、進階及最佳等四階段導入相關控制措施。

零信任架構 5 大支柱建議實作功能及原則等，依導入階段分級（Level Ⅰ, Ⅱ, Ⅲ, Ⅳ）如附表。

五、零信任架構推動路徑

本參考指引為漸進導入零信任架構路徑之一，金融機構於導入實務仍得考量既有資訊與資安環境、資安防護水準、資源及人力、業務風險、相關解決方案成熟度等因素調適；或另為適切之規劃，不以本參考指引為限。本會並將依據金融機構導入進程，滾動修訂整體推動策略及分階段推動指標，主要推動路徑如下：

(一) 鼓勵分享實務案例，帶動持續深化及擴散

本會鼓勵金融機構導入零信任架構，於 113 年研擬導入規劃，本會並將自各業別擇金融機構先行，分享導入經驗作為示範，供金融同業交流研討最佳實務。

(二) 建立導入實務共識，漸進納入基礎規範

本會定期調查各金融機構於零信任架構之導入規劃及進程，召集相關周邊單位、同業公會共同依據各金融業別屬性、規模及業務風險等，衡量實際資安防護需求及執行可達性，滾動修訂推動策略及實施進程，並評估將實作參考原則漸進納入資安基礎規範，提升整體資安防禦水準。

附表：零信任架構實作參考原則分級表

項次	支柱	功能	原則	等級
1.1	身分	身分認證	採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。	Ⅰ
1.2	身分	身分認證	採用包含綁定實體載具(如 FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對 APP 等，排除簡訊、語音及電子郵件 OTP)的多因子驗證機制，可抗網路釣魚風險。	Ⅱ
1.3	身分	身分互通	對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者信賴等級之身分鑑別機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	Ⅰ
1.4	身分	身分互通	如具多元身分鑑別機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	Ⅰ
1.5	身分	權限存取	完成身分鑑別後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並具基於屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警。	Ⅱ
1.6	身分	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或 SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
1.7	身分	自動化治理	建立可依資安政策快速調適之一致性且自動化之管理機制，確保於帳號生命週期之安全性及合規性。	Ⅳ

項次	支柱	功能	原則	等級
2.1	設備	設備合規	具有效盤點且可唯一識別(如 TPM 等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	Ⅰ
2.2	設備	設備合規	具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。	Ⅱ
2.3	設備	供應鏈風險	對外部設備(如 BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道(如 VDI 等)存取。	Ⅰ
2.4	設備	資源存取	可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道(如 VDI 等)存取。	Ⅱ
2.5	設備	威脅防護	對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應處(如發出事件單即時追蹤處置)。	Ⅲ
2.6	設備	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
2.7	設備	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於設備生命週期之安全性及合規性。	Ⅳ

項次	支柱	功能	原則	等級
3.1	網路	網路區隔	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。	Ⅰ
3.2	網路	網路區隔	具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	Ⅱ
3.3	網路	流量管理	呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。	Ⅱ
3.4	網路	流量加密	於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。	Ⅰ
3.5	網路	網路韌性	對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。	Ⅲ
3.6	網路	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook 等)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
3.7	網路	自動化治理	具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。	Ⅳ

項次	支柱	功能	原則	等級
4.1	應用程式	存取授權	以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身分及設備鑑別之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。	Ⅰ
4.2	應用程式	存取授權	可將帳號動態屬性(如 MFA 強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。	Ⅱ
4.3	應用程式	威脅防護	對應用程式活動紀錄具有即時偵測及回應機制，並可依據使用者行為或使用模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警。	Ⅲ
4.4	應用程式	程式安全	從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經 Internet 存取之防護能力。	Ⅱ
4.5	應用程式	程式部署	為應用程式開發、測試及部署建立持續整合及部署(CI/CD) 通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實權責分離。	Ⅱ
4.6	應用程式	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
4.7	應用程式	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於應用程式生命週期之安全性及合規性。	Ⅳ

項次	支柱	功能	原則	等級
5.1	資料	外洩防護	針對機敏資料部署防止資料外洩防護機制，如依據資料特徵之 DLP、資料不落地等。	Ⅰ
5.2	資料	外洩防護	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警，偵測及阻止疑似資料外洩之行為。	Ⅲ
5.2	資料	資料分類	建立資料盤點、分類及、標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	Ⅰ
5.3	資料	資料可用性	建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。	Ⅰ
5.4	資料	資料存取	可將資料存取的動態屬性(如 MFA 強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可動態撤銷、限縮存取授權或即時告警。	Ⅱ
5.5	資料	資料加密	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	Ⅰ
5.6	資料	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照 F-ISAC 威脅情資及金融資安監控組態基準)	Ⅲ
5.7	資料	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於資料生命週期之安全性及合規性。	Ⅳ