本所零信任資安防護探討(2/2)—導入與維運分析

運輸科技及資訊組 張益城 童志浩

研究期間 114 年 2 月至 114 年 12 月

摘要

延續「本所零信任資安防護探討(1/2)—技術與成本分析」所建立之技術基礎，本研究聚焦於零信任架構的實際導入策略與長期維運規劃。零信任架構的成功導入不僅需要完善的技術方案，更需要周全的執行計畫、組織變革管理及持續性的維運機制。本研究提出分階段導入策略，從風險評估、試點部署到全面推廣，並針對身份管理、網路架構、端點安全及監控機制等面向，制定具體的實施步驟與時程規劃。在維運層面，本研究探討零信任架構的日常管理需求，包括政策維護、效能監控、事件應變、使用者教育訓練等關鍵要素，並建立持續改進機制，確保零信任架構能夠適應不斷演變的資安威脅。此外，本研究亦分析導入過程中可能面臨的組織挑戰與技術障礙，提供風險緩解措施及變革管理建議。研究成果將協助本所建立完整的零信任實施藍圖，提升資安治理成熟度，為政府機關資安轉型提供實務參考。

關鍵詞：
零信任導入策略、資安維運管理、分階段部署、變革管理

一、緒論

本研究為「本所零信任資安防護探討」系列研究之第二部分，延續第一部分「技術與成本分析」的研究成果，進一步探討零信任架構的實際導入策略與長期維運規劃。

在第一部分研究中，本所已系統性地分析了零信任資安防護的核心概念、技術架構與成本效益。該研究首先闡述零信任架構的必要性，指出傳統邊界防禦模式已無法有效應對現代資安威脅，而零信任的「永不信任，持續驗證」原則能有效降低內部威脅與資料外洩風險。研究中深入探討了適合本所的零信任技術方案，包括：

1. 多因子身份驗證：分析了硬體 Token（如 YubiKey）、軟體 Token（如 Google Authenticator）及生物特徵驗證等方案，從安全性、成本及使用者體驗等面向進行比較。
2. 微分割技術：評估軟體定義網路、網路存取控制及防火牆等技術方案，探討如何透過網路分割降低攻擊面。
3. 行為分析：研究安全資訊與事件管理、使用者和實體行為分析及端點偵測與回應等技術，以建立異常偵測與威脅監控能力。
4. 身份與存取管理：分析目錄服務與權限管理系統，探討如何實現集中化的身份管理與精細化的存取控制。

第一部分研究亦詳細分析各項技術方案的初始部署成本與維運成本，並評估其優缺點，為本所提供技術選擇的參考依據。然而，技術方案的確立僅是零信任轉型的第一步，如何有效導入這些技術、建立完善的維運機制，以及如何克服組織與文化層面的挑戰，都是確保零信任架構成功落地的關鍵因素。

因此，本研究將在前期技術分析的基礎上，聚焦於導入策略與維運管理兩大主軸。在導入策略方面，本研究提出分階段、漸進式的實施路徑，從現況評估、基礎建置、試點部署到全面推廣，並針對組織準備、變革管理等面向提供具體建議。在維運管理方面，本研究探討日常管理需求、威脅監控、事件應變及持續改進等機制，確保零信任架構能夠長期有效運作。此外，本研究亦分析導入過程中可能面臨的技術、組織及預算風險，並提供相應的緩解策略。

透過第一部分的技術與成本分析，以及本研究的導入與維運規劃，將形成完整的零信任實施藍圖，協助本所系統性地推動資安轉型，建立符合現代資安需求的防護體系。

二、導入策略與規劃

零信任架構的導入是一項複雜且長期的資訊安全轉型工程，需要審慎的規劃與執行。本所應採取分階段、漸進式的導入策略，確保在轉型過程中維持業務連續性，同時逐步提升整體資安防護能力。

(一)現況評估與差異分析

在正式導入零信任架構前，本所須先進行全面的現況評估，了解現有資訊環境與零信任架構標準之間的差距。此階段的主要工作包括：

1.資訊資產盤點

全面清查本所的資訊資產，包括實體設備（伺服器、網路設備、個人電腦、行動裝置等）、軟體系統（應用程式、資料庫、雲端服務等）及資料資產（機密文件、個人資料、業務資料等）。針對每項資產進行分類與風險評級，確認其重要性與敏感程度，作為後續保護措施的優先順序依據。

2.現有安全架構評估

檢視本所現行的資安防護機制，包括防火牆配置、身份驗證方式、存取控制政策、網路架構設計、監控與稽核機制等。分析現有架構的優劣勢，辨識安全缺口與潛在風險，並評估與零信任原則的相容性。特別需要關注舊有系統的整合難度，以及是否需要進行升級或汰換。

3.使用者行為與權限分析

分析各類使用者的存取需求與行為模式，包括內部同仁、外包人員、合作夥伴等。檢視現有權限配置是否符合最小權限原則，識別過度授權或閒置帳號等安全隱患。此分析將有助於後續建立適切的存取控制政策與角色劃分。

4.合規性與政策檢視

確認本所需遵循的資安法規與政策要求，包括資通安全管理法及相關子法、行政院資通安全責任等級分級辦法等。評估零信任架構的導入如何協助本所達成合規要求，並確保導入過程不違反現有規範。

(二)分階段導入計畫

考量本所業務的複雜性與資源限制，建議採用三階段導入模式，逐步推進零信任架構的建置：

第一階段：基礎建置期（6-9 個月）

此階段著重於建立零信任架構的核心基礎，包括：

1. 強化身份驗證機制：導入多因子驗證(Multi-Factor Authentication,MFA)，優先針對高權限帳號（如系統管理員、資料庫管理員）及遠端存取進行部署。選擇適合本所的 MFA 方案（如硬體 Token、軟體 Token 或生物辨識），並制定使用規範。
2. 建立集中化身份管理：整合或升級現有目錄服務（如 Active Directory），建立統一的身份管理平台。清理冗餘帳號，規範帳號生命週期管理流程（包括帳號申請、審核、停用、刪除等）。
3. 網路可視化與監控：部署或強化安全資訊與事件管理(Security Information and Event Management, SIEM）系統，收集關鍵系統的日誌資料，建立基本的威脅偵測規則。實施網路流量監控，建立使用者與設備的正常行為基線。
4. 政策與流程制定：制定零信任相關的資安政策，包括存取控制政策、密碼政策、設備管理政策等。建立事件應變程序與責任歸屬。

第二階段：試點部署期（6-9 個月）

在完成基礎建置後，選擇特定業務單位或系統作為試點，進行零信任架構的實際部署：

1. 選定試點範圍：建議選擇業務重要性高但規模相對可控的單位或系統作為試點，例如運輸科技及資訊組或特定核心業務系統。試點範圍應具代表性，能夠涵蓋不同類型的使用者與存取場景。
2. 實施微分割：在試點範圍內導入網路微分割，將網路劃分為更小的安全區域。實施基於身份的存取控制，確保使用者只能存取其工作所需的特定資源。可採用軟體定義網路或網路存取控制技術實現。
3. 部署端點安全：在試點範圍的端點設備上部署 EDR 解決方案，實施持續監控與威脅偵測。建立端點設備的安全基線，確保所有設備符合資安要求才能存取網路。
4. 精細化權限管理：實施角色型存取控制或屬性型存取控制，根據使用者角色、時間、地點等因素動態調整存取權限。定期檢視與調整權限配置，確保符合最小權限原則。

5. 效果評估與調整：在試點期間密切監控系統運作狀況，收集使用者回饋，評估安全性提升效果與對業務的影響。根據試點經驗調整技術方案與部署策略，為全面推廣做好準備。

第三階段：全面推廣期（12-18 個月）

基於試點經驗，將零信任架構擴展至全所：

1. 分批推廣：根據單位或系統的重要性與複雜度，制定推廣時程表。優先處理高風險或高價值的系統，逐步擴展至所有單位與系統。
2. 舊有系統整合：針對無法直接支援零信任技術的舊有系統，評估升級、替換或採用中介方案（如應用層代理）的可行性。確保所有關鍵系統都能納入零信任框架。
3. 完善監控與分析：持續擴展安全資訊與事件管理與使用者與實體行為分析的涵蓋範圍，實現全網路的可視化與威脅偵測。建立完整的資安儀表板，提供即時的安全態勢感知。
4. 持續優化：根據運作經驗持續調整安全政策與技術配置，確保零信任架構能夠適應組織變化與新興威脅。建立定期檢討機制，評估架構效益並規劃進一步改進。

(三)組織與人力準備

零信任架構的成功導入不僅是技術問題，更需要組織層面的支持與準備：

1.成立專案推動小組

組成跨部門的專案團隊，成員應包括運輸科技及資訊組、業務單位代表、資安專家及高層主管。明確定義專案目標、範圍、時程與預算，建立決策機制與溝通管道。指派專案經理負責整體協調，並定期向高層報告進度。

2.人力培訓與能力建置

資訊人員需要接受零信任相關技術的專業訓練，包括身份管理、網路安全、威脅偵測等領域。可透過內部培訓、外部課程、廠商技術支援或聘請顧問等方式提升團隊能力。此外，所有同仁都需要接受資安意識教育，了解零信任架構的目的與使用方式，培養良好的資安習慣。

3.變革管理

零信任架構可能改變現有的工作流程與習慣，導致內部阻力。需要透過充分的溝通，說明導入零信任的必要性與好處，爭取同仁的理解與支持。建立回饋機制，及時處理同仁在使用過程中遇到的問題。對於影

響較大的變更，應給予足夠的緩衝期與支援。

三、維運管理與持續改進

零信任架構的導入並非一勞永逸，而是需要持續的維運與優化。本所應建立完善的維運管理機制，確保零信任架構能夠長期穩定運作，並隨著環境變化持續改進。

(一)日常維運管理

1.帳號與權限管理

建立標準化的帳號生命週期管理流程，確保新進同仁能及時獲得適當權限，離職同仁的帳號能立即停用。定期檢視帳號使用狀況，清理閒置帳號，審查權限配置是否符合最小權限原則。針對高權限帳號應特別加強管理，實施定期審核與多重授權機制。

2.政策維護與更新

隨著組織架構調整、業務需求變化或新威脅出現，需要定期檢視並更新資安政策與存取控制規則。建立政策變更管理流程，確保所有變更都經過適當的審核與測試，避免影響業務運作或造成安全漏洞。維護完整的政策文件與版本記錄，方便追蹤與稽核。

3.系統監控與效能管理

持續監控零信任架構相關系統的運作狀況，包括身份驗證服務、網路設備、安全工具等。建立效能基準與告警機制，當系統負載異常或效能下降時能及時發現並處理。定期進行系統維護，包括韌體更新、軟體補丁、容量擴充等，確保系統穩定運作。

4.日誌管理與留存

確保所有關鍵系統的活動日誌都被妥善收集、儲存與保護。日誌應包括身份驗證記錄、存取活動、系統變更、安全事件等。建立日誌留存政策，符合法規要求與稽核需求。定期檢查日誌收集的完整性與可靠性，確保在需要時能夠進行有效的調查與分析。

(二)威脅偵測與事件應變

1.持續威脅監控

運用 SIEM、EDR 等工具，對網路、系統及使用者行為進行 24/7 全天候監控。建立多層次的偵測規則，包括已知威脅簽名、異常行為模式、基於機器學習的異常偵測等。定期調整偵測規則，降低誤報率，提高威脅識別的準確性。

2.資安事件分級與應變

建立資安事件分級機制，根據事件的嚴重程度、影響範圍與緊急性，訂定不同的應變流程與時限。制定詳細的事件應變程序手冊，明確規範各類事件的處理步驟、責任分工與通報機制。定期進行事件應變演練，確保團隊能在真實事件發生時快速有效地應對。

3.威脅情報整合

訂閱並整合外部威脅情報來源，包括政府資安單位（如國家資通安全研究院、台灣電腦網路危機處理暨協調中心）、資安廠商、資安社群等提供的威脅資訊。將威脅情報整合至 SIEM 與防禦系統，提升對新興威脅的偵測與防禦能力。建立內部威脅情報分享機制，促進與其他政府機關或相關單位的資安協作。

4.事後分析與改進

每次重大資安事件後，應進行詳細的事後分析，檢討事件發生原因、應變過程的得失、造成的影響等。將分析結果轉化為改進措施，包括技術強化、流程優化、人員訓練等。建立知識庫，累積事件處理經驗，供未來參考。

(三)持續改進機制

1.定期評估與稽核

每季或每半年進行零信任架構的全面評估，檢視架構運作效能、安全事件統計、政策遵循狀況等。邀請外部專家或稽核單位進行獨立評估，提供客觀的改進建議。根據評估結果制定改進計畫，持續優化架構。

2.技術更新與升級

關注零信任相關技術的發展趨勢，評估新技術或新方案的導入可行性。規劃系統升級路徑，確保採用的技術能夠與時俱進，不會因過時而影響防護效果。建立技術評估機制，對新引入的技術進行充分的測試與驗證。

3.使用者回饋與體驗優化

建立使用者回饋管道，收集同仁對零信任架構使用體驗的意見與建議。分析回饋內容，識別影響使用者體驗的問題，例如驗證流程過於繁瑣、權限配置不當等。在維持安全性的前提下，優化使用流程，提升便利性，降低同仁的抗拒感。

4.資安意識持續強化

定期舉辦資安教育訓練，更新訓練內容以反映最新的威脅態勢與安全實務。透過多元化的方式提升同仁資安意識，例如電子郵件宣導、社

交工程演練等。培養全體同仁的資安文化，使資安成為每個人工作中的自然考量，而非額外負擔。

四、風險管理與挑戰應對

零信任架構的導入與維運過程中，本所可能面臨多種風險與挑戰。提前識別這些風險並制定應對策略，是確保專案成功的關鍵。

(一)技術風險與應對

1.舊有系統相容性問題

風險：本所可能存在無法支援現代身份驗證協議或無法整合零信任技術的舊有系統，影響整體架構的完整性。

應對策略：在導入前期進行詳細的系統盤點與相容性測試。對於關鍵但無法升級的舊系統，考慮採用應用層代理或虛擬專用網路(VPN)等中介方案，在不修改系統本身的情況下納入零信任框架。規劃長期的系統汰換計畫，逐步淘汰過時的系統。

2.效能影響

風險：多因子驗證、流量檢查、行為分析等機制可能增加系統負載，影響回應速度與使用者體驗。

應對策略：在導入前進行充分的效能測試與容量規劃，確保基礎設施能夠承受額外負載。採用快取、負載平衡等技術優化效能。對於影響較大的驗證流程，考慮採用單一登入或無密碼驗證等方式改善使用者體驗。持續監控系統效能，及時發現並解決瓶頸。

3.單點故障風險

風險：集中化的身份驗證服務或控制器若發生故障，可能導致大範圍的服務中斷。

應對策略：對關鍵系統實施高可用性架構，包括備援伺服器、負載平衡、容錯移轉機制等。建立災難復原計畫，確保在重大故障時能快速恢復服務。定期進行備份並測試復原程序。考慮採用多雲架構或混合雲，降低對單一基礎設施的依賴。

(二)組織與人員風險

1.內部阻力與接受度

風險：零信任架構改變既有工作方式，可能遭遇同仁的抗拒，影響導入進度與效果。

應對策略：在專案啟動初期即進行充分的溝通與宣導，說明導入零

信任的必要性與預期效益。讓各單位代表參與規劃過程，聽取意見並適度調整方案。提供完善的教育訓練與技術支援，協助同仁適應新流程。設立試用期與回饋機制，讓同仁的意見能被重視與採納。

2.技術人力不足

風險：本所資訊人員可能缺乏零信任相關技術的經驗，影響導入品質與後續維運。

應對策略：及早規劃人力培訓，透過內外部訓練提升團隊能力。在導入初期考慮引入外部顧問或技術支援，提供專業協助與知識轉移。評估是否需要增補人力或將部分工作外包。建立內部知識庫與標準作業程序，降低對特定人員的依賴。

3.跨部門協調困難

風險：零信任的導入需要多個部門的配合，但各部門可能因優先順序不同而缺乏配合意願。

應對策略：取得高層主管的明確支持，將零信任專案列為組織重點任務。建立跨部門專案小組，明確各單位的責任與權限。定期召開協調會議，及時處理跨部門問題。建立激勵機制，鼓勵各單位積極參與。

(三)預算與資源風險

1.成本超支

風險：專案執行過程中可能因需求變更、技術問題或其他因素導致成本超出預算。

應對策略：在規劃階段進行詳細的成本估算，並預留適當的預算彈性（建議 10-20%）。採用分階段導入策略，每階段完成後評估效益與成本，再決定下一階段的投入。優先選擇投資報酬率高的項目，避免不必要的開支。建立嚴格的預算控管機制，定期檢討支出狀況。

2.資源排擠效應

風險：零信任專案可能占用大量人力與預算，影響其他資訊專案的推動。

應對策略：在年度資訊規劃中統籌考量所有專案的優先順序與資源分配。評估是否可將零信任與其他專案整合，發揮綜效。對於非緊急的專案，考慮延後或調整範圍，確保零信任專案有足夠資源。

五、效益評估與成功指標

為了評估零信任架構導入的成效，本所應建立明確的評估指標與方法，從多個面向衡量架構的效益。

(一)安全性指標

1.資安事件數量與嚴重性：追蹤資安事件的發生頻率與影響程度，評估是否有下降趨勢。

2.平均偵測時間：衡量從攻擊發生到被偵測的平均時間，目標是持續縮短。

3.平均應變時間：衡量從事件偵測到完成應變的平均時間，目標是提升應變效率。

4.未授權存取嘗試次數：監控被阻止的未授權存取行為，評估存取控制的有效性。

5.漏洞修補時間：衡量發現漏洞到完成修補的時間，評估風險管理能力。

(二)運作效率指標

1.帳號管理效率：衡量帳號開通、變更、停用等作業的處理時間。

2.政策部署時間：評估新安全政策從規劃到完成部署的時間。

3.誤報率：監控安全告警中的誤報比例，目標是降低誤報以提升團隊效率。

4.系統可用性：追蹤零信任相關系統的正常運作時間比例，確保服務穩定。

(三)使用者體驗指標

1.使用者滿意度：透過問卷調查或訪談，收集同仁對零信任架構使用體驗的評價。

2.登入時間：監控使用者完成身份驗證的平均時間，評估對工作效率的影響。

3.求助單數量：追蹤與零信任相關的技術支援請求數量，評估系統易用性與訓練成效。

4.政策遵循率：衡量同仁對資安政策的遵循程度，例如定期更換密碼。

(四)成本效益指標

1.總擁有成本：計算零信任架構的建置與維運總成本，包括硬體、軟體、人力等。

2.避免的損失：估算因防止資安事件而避免的潛在損失，例如資料外洩賠

償、業務中斷成本等。

3.投資報酬率：比較投入成本與獲得效益，評估專案的經濟價值。

4.合規成本降低：評估零信任架構是否協助本所更有效地達成法規要求，降低合規成本。

六、結論與建議

本研究系列透過「技術與成本分析」及「導入與維運分析」兩階段，完整探討本所零信任資安防護建置藍圖。第一部分系統性分析多因子身份驗證、微分割、行為分析及身份與存取管理等關鍵技術方案與成本效益；第二部分提出分階段導入策略、維運管理機制及風險應對措施，為本所提供可操作的實施路徑。

零信任架構的成功導入需要技術、組織與文化三層面配合。建議採行 24 至 36 個月分階段導入策略，從基礎建置、試點部署到全面推廣。在維運層面，應建立完善的日常管理機制，包括帳號權限管理、政策維護、威脅監控及事件應變，確保架構長期穩定運作並適應演變的資安威脅。

基於研究成果，提出五項核心建議：一、確立高層承諾，將零信任列為未來 3 至 5 年核心資安策略；二、採務實漸進策略，從易實現項目著手建立成功案例；三、投資人力培訓，提升資訊團隊專業能力並強化全員資安意識；四、建立評估機制，設定明確成功指標並定期檢討調整；五、保持技術彈性，關注新技術發展並定期評估導入可行性。

零信任架構代表資安思維從「預設信任」轉向「永不信任，持續驗證」的根本轉變。透過本研究建立的完整藍圖，本所能系統性推動資安轉型，建立符合現代需求的防護體系，不僅提升資安防禦能力、降低風險，更為數位轉型奠定堅實基礎。作為政府機關，本所應發揮示範作用，透過成功導入零信任架構，保障國家機密與民眾權益，並為其他機關提供實務參考，推動整體政府資安能力提升。

參考文獻

1. 本所零信任資安防護探討(1/2)—技術與成本分析
2. 國家資通安全研究院：https://www.nics.nat.gov.tw/
3. 【ZTA 101】NIST SP 800-207第一章：簡介：https://www.ithome.com.tw/tech/152241
4. Microsoft：零信任指引中心—六大防禦支柱：https://learn.microsoft.com/zh-tw/security/zero-trust/zero-trust-overview
5. iThome：解析臺灣政府推動零信任架構的三大核心：https://www.ithome.com.tw/news/156499
6. Palo Alto Networks：實行零信任架構的五個步驟：https://www.paloaltonetworks.tw/cyberpedia/what-is-a-zero-trust-architecture
7. 勤業眾信：金融業導入零信任架構的挑戰與契機：https://www2.deloitte.com/tw/tc/pages/risk/articles/zero-trust-architecture-for-financial-services.html