本所零信任資安防護探討(1/2)—技術與成本分析

運輸科技及資訊組 張益城 童志浩

研究期間113年2月至113年12月

摘要

隨著網路攻擊手法日益精進，傳統邊界防禦模式已無法有效應對現代資安威脅，促使零信任架構成為當前資安防護的重要策略。本研究聚焦於零信任架構的技術可行性與成本效益，並探討其在本所資訊安全環境中的適用性。零信任架構以「永不信任，持續驗證」為核心原則，透過嚴格的身份驗證與權限管控，減少內部威脅與資料外洩風險。本研究分析本所導入零信任架構的必要性與挑戰，並評估關鍵技術方案，如多因子驗證（MFA）、微分割（Micro-Segmentation）、端點偵測與應變（EDR）、身份與存取管理（IAM）等，從技術成熟度、安全性與成本效益等角度進行比較。研究結果顯示，透過漸進式導入與策略性部署，零信任架構可顯著提升本所資安防禦能力，降低潛在風險，並促進數位轉型，為政府資安治理提供實務參考應用。

關鍵詞：

零信任架構，身份與存取管理，微分割，多因子驗證

一、緒論

隨著資訊科技的快速發展和網路攻擊的日益猖獗，本所面臨的資安威脅也日趨嚴峻。傳統的邊界防禦模式，如同「築牆圍城」，僅著重於外部防護，而忽略內部網路安全，已不足以應對現今複雜多變的網路攻擊。政府資料、民眾個資一旦遭到竊取或破壞，將造成難以估計的損失，甚至影響國家安全和社會穩定。

零信任資安架構的出現，為本所的資安防護帶來新的啟發。零信任的核心原則是「永不信任，持續驗證」，無論使用者或設備位於何處，每次存取請求都必須經過嚴格的身份驗證和授權，才可存取相應的資源。此架構打破了傳統的信任邊界，將安全防護的重心轉移到身份識別和存取控制，有效降低了內部威脅和資料外洩的風險，提升了本所的資安防禦能力。

然而，零信任的導入對於本所而言，仍面臨諸多挑戰。例如，如何選擇符合政府規範和本所需求的技術方案？如何評估和控制導入和維護成本？如何兼顧安全性和使用效率？本研究旨在探討零信任資安防護在本所的應用，分析其技術可行性和成本效益，為政府單位的資安建設提供參考依據。

二、導入零信任架構的必要性和挑戰

(一)導入零信任架構的必要性

在資訊科技發展日新月異的時代，本所面臨的網路安全威脅也日趨複雜。傳統的「邊界防禦」模式，假設內部網路是安全的，僅著重於外部防護，已不足以應對現今多樣化的攻擊手段。本所掌握大量敏感資料，包括國家機密、民眾個資等，一旦遭到洩露或破壞，將造成難以估計的損失，甚至影響國家安全和社會穩定。零信任架構的「永不信任，持續驗證」原則，無論使用者或設備位於何處，都需經過嚴格的身份驗證和授權，才可存取資源。此架構能有效降低內部威脅和資料外洩風險，提升本所的資安防禦能力，保障國家機密和民眾個資安全。此外，零信任架構可促進本所數位轉型，提升行政效率。透過集中化身份管理和存取控制，簡化繁瑣的授權流程，並實現更彈性的遠距辦公模式。

隨著數位轉型的推進，本所越來越依賴科技來提供公共服務、處理機密數據。然而，這也使得本所成為高度吸引網路攻擊的目標。傳統的周邊式安全模型以「信任但驗證」為核心，假設內部網路比外部網路更安全。然而，隨著雲端運算、遠端工作及物聯網（IoT）設備的普及，這種模型已

顯得過時且不堪一擊。零信任架構（Zero Trust Architecture, ZTA）因此成為新時代資訊安全的必要策略，其核心理念是「永不信任，隨時驗證」，即無論內外部使用者或設備，都必須經過嚴格的驗證流程才能獲得存取權限。

首先，零信任架構有助於應對現代化威脅，例如勒索軟體攻擊、內部人員濫用權限及供應鏈攻擊等。零信任架構要求對每次數據請求進行存取控制，並結合多因子驗證（MFA）和動態安全政策，有效降低內部與外部威脅的成功率。

其次，導入零信任架構有助於提升整體網路安全彈性。本所面臨的威脅態勢日益複雜，攻擊者不僅針對技術漏洞，更利用社交工程滲透內部網路。零信任架構的另一個核心要素是持續監控與風險評估，藉由即時分析使用者行為和網路流量，本所能迅速檢測異常活動並做出回應。例如，當某位使用者嘗試從不尋常的地理位置登入系統，或其存取模式異於常態時，系統將能自動觸發安全警報並限制該使用者的權限。此種即時反應能力對於保護本所的數位基礎設施至關重要。因此，從數據安全、威脅應對的角度來看，零信任架構對本所的重要性不言而喻。

(二)導入零信任架構的挑戰

儘管零信任架構在概念上具有吸引力，但對於本所而言，實際導入過程中仍面臨諸多挑戰，包括技術、組織和文化層面的困難。這些挑戰可能在短期內影響架構落地的成效，甚至導致推動過程受阻。

首先，技術上的複雜性是導入零信任架構的一大挑戰。本所的資訊基礎設施往往歷史悠久，存在許多傳統系統（Legacy Systems）。這些系統可能無法輕易與現代零信任技術（如多重身份驗證）整合，甚至缺乏必要的更新能力。此外，本所的業務系統高度專業化，涉及各類專屬軟體與硬體設備，導致零信任策略的部署需要額外的技術支援及調適。例如，實施持續監控功能時，需要將分散在不同平臺和應用程式中的數據流量整合到統一的安全管理框架中，這不僅耗費大量資源，還可能因部署錯誤而引發系統中斷或性能下降。

其次，零信任架構需要具備強大的身份管理能力，而這對本所來說是一項艱鉅的任務。零信任要求對所有使用者進行身份驗證和行為追蹤，但許多本所的使用者資料系統可能仍然不夠精確或統一，導致在身份驗證過程中容易出現錯誤。例如，一些同仁可能擁有多個身份或重複的系統帳號，而部分舊系統無法支援現代身份驗證技術。解決這些問題需要本所對使用者資料進行全面的清理和統整，這不僅需要投入大量時間和人力，也可能

引發內部摩擦。

在組織層面，零信任的導入過程可能遭遇來自內部的阻力。零信任架構的「最小權限」原則要求重新評估和限制使用者對資源的存取權限，這可能導致同仁感到工作流程受到干擾。例如，某些單位可能需要頻繁存取其他單位的資料庫或共用檔案，而零信任的限制政策可能增加存取的複雜性。此外，零信任的實施需要跨單位的協作，例如資訊單位與政風、秘書室等單位需共同制定適用的政策和規範，然而各單位間可能因缺乏溝通或責任不明而延誤程式。

最後，文化層面的挑戰同樣不可忽視。零信任架構要求所有使用者改變既有的使用習慣，例如頻繁進行多因子驗證或遵守嚴格的密碼政策，而這對於慣用簡化流程的本所同仁來說可能難以接受。此外，零信任的持續監控功能可能被誤解為侵犯隱私，進而引發內部的反對聲浪。本所需要投入大量精力進行內部教育和溝通，讓同仁瞭解零信任的目的是保護整體安全，而非針對個人。

三、適合本所的零信任技術方案

零信任架構並非單一技術，而是一套整合性的資安策略和解決方案。本所在導入零信任時，需考量自身需求和資訊環境，選擇合適的技術方案。以下列舉幾項適合本所的零信任技術：

(一)多因子身份驗證(MFA, Multi-factor authentication)

MFA 要求使用者提供多種身份驗證因素，例如密碼、生物特徵、一次性密碼(OTP)等，才能存取系統和資料。相較於單一密碼驗證，MFA 更能有效抵禦密碼竊取和帳號盜用等攻擊。本所可採用符合 FIDO2 標準的無密碼驗證技術，提升安全性及使用者體驗。技術方案如下：

1.硬體 Token：

YubiKey：

YubiKey 提供了高強度的安全性，其運作原理是基於公開金鑰加密技術。當使用者插入 YubiKey 時，裝置會產生一個隨機的加密簽名，並將其傳送給伺服器。伺服器會驗證簽名，以確認使用者的身份。這種方式的安全性極高，即使密碼被破解，攻擊者也無法偽造 YubiKey 的簽名。

初始部署成本：

(1) 需要購買 YubiKey 硬體裝置，每個使用者需配備一支，單價相對較高。

(2) 伺服器端需整合 FIDO2 標準，可能涉及額外的開發與部署成本。

維運成本：

(1) 裝置可能遺失或損壞，需要額外採購備用設備。

(2) 需要管理 YubiKey 的註冊、更新及回收機制，增加資訊部門工作量。

(3) 用戶可能需要支援與培訓，特別是非技術使用者。

表 1　硬體 Token 優缺點

優點	缺點
(1) 安全性高： 採用物理密鑰，不易被破解。 (2) 多因子驗證： 結合密碼和實體設備，強化安全性。 (3) 廣泛支援： 支援多種網路服務和協議。	(1) 成本較高： 相較於軟體 Token，硬體 Token 的成本較高。 (2) 攜帶不便： 使用者需要隨身攜帶 YubiKey。

2.軟體 Token：

Google Authenticator、Microsoft Authenticator：

這些 App 運用時間同步演算法，產生不斷變化的六位數一次性密碼。使用者在登入時，除了輸入帳號密碼外，還需輸入 App 上顯示的動態密碼。

初始部署成本：

(1) 應用程式本身免費，無需額外硬體設備，因此初始成本較低。

(2) 伺服器端需整合 TOTP（Time-based One-Time Password）驗證機制，可能涉及一定的開發成本。

維運成本：

(1) 主要成本來自資訊支援，例如使用者手機遺失或更換時的帳戶恢復問題。

(2) 需定期檢查與更新驗證機制，以確保安全性。

表 2　軟體 Token 優缺點

優點	缺點
(1) 免費： 多數軟體 Token App 為免費提供。 (2) 易用性高： 操作簡單，使用者體驗佳。 (3) 跨平台： 支援多種行動裝置平台。	(1) 安全性相對較低： 相較於硬體 Token，軟體 Token 的安全性較低，容易受到釣魚攻擊。 (2) 依賴網路： 需要手機有網路連線才能獲取驗證碼。

3.生物特徵驗證：

指紋辨識、臉部辨識為例：

這些技術利用人體獨有的生理特徵進行身份驗證。

初始部署成本：

(1) 需要搭配支援生物辨識的設備，如指紋辨識器、紅外線攝影機等，設備成本較高。

(2) 伺服器端需儲存及管理生物特徵數據，涉及隱私保護與安全加密技術的開發成本。

維運成本：

(1) 生物辨識系統可能受到環境影響（如濕度、光線），需要定期維護與校正。

(2) 需要確保數據庫的安全性，避免生物數據外洩風險，可能需要更強的加密與存取控制機制。

表 3　生物特徵驗證優缺點

優點	缺點
(1) 便利性高： 不需要額外攜帶任何裝置。 (2) 安全性高： 生物特徵難以偽造。	(1) 成本高： 建置生物辨識系統需要較高的硬體和軟體成本。 (2) 隱私疑慮： 生物特徵數據的安全性備受關注。 (3) 環境影響： 指紋辨識容易受到濕度、溫度等環境因素影響。

(二)微分割

微分割將網路切割成更小的隔離區域，限制使用者只能存取其工作所需的資源，在舊式的邊界防護環境中，駭客一旦進到本所內部，就能存取整個網路。微分割可縮小受攻擊面，降低每一次駭客入侵所造成的損害。技術方案如下：

1.軟體定義網路(Software-Defined Networking, SDN)

傳統網路架構中，每台網路設備（例如路由器、交換器）都擁有獨立的控制平面(Control Plane)和資料平面(Data Plane)，這使得網路管理變得繁瑣，變更配置時需要逐一調整設備，難以應對快速變化的需求。SDN 透過集中式控制器(SDN Controller)來管理網路設備的資料平面，可動態調整流量路由，提高網路的靈活性與自動化程度。SDN 採用開放標準，如 OpenFlow 協議，允許管理員透過程式碼定義網路行為，而非手動配置硬體設備。此外，SDN 允許組織根據業務需求自動化配置 QoS（服務品質）、負載平衡和安全策略，提升整體網路效能與安全性。

初始部署成本：

(1) 需重新設計網路架構，可能涉及硬體升級與軟體整合。

(2) 資訊團隊需接受專門培訓，掌握 SDN 網路管理方式。

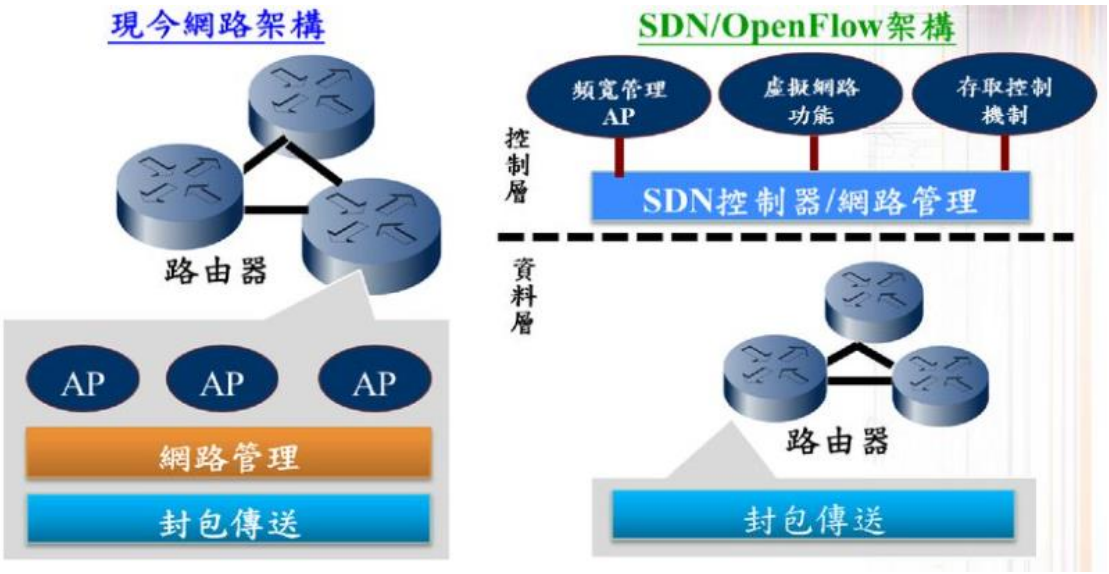
維運成本：

(1) SDN 控制器可能成為單點故障風險，因此需要高可用性方案（如備援控制器），增加維護成本。

(2) 定期更新 SDN 軟體，確保相容性與安全性，可能涉及授權費或開發成本。

表 4 軟體定義網路優缺點

優點	缺點
(1) 集中化管理： 透過 SDN 控制器可統一管理整個網路，簡化設備配置和管理流程。 (2) 靈活性與可程式化： 能透過軟體快速調整網路架構，支援自動化網路管理。 (3) 提升安全性： 能即時監控網路流量，並根據安全策略主動阻擋異常流量。 (4) 成本效益高： 可使用標準化網路設備，降低對高成本專有硬體的依賴。	(1) 單點故障風險： 控制器若發生故障，整個網路可能受到影響。 (2) 初始部署成本高： 需要重新設計現有網路架構，並培訓資訊人員。



圖一、SDN 網路

資料來源：國立屏東科技大學(https://slidesplayer.com/slide/17096461/)

2.網路存取控制(Network Access Control, NAC)

NAC 是一種存取控制機制，可根據使用者身份、設備類型與安全狀態，決定是否允許該設備存取網路。當一個設備（如筆電、手機）試圖連接本所內部網路時，NAC 會執行一系列的安全檢查，例如設備是否安裝最新的防毒軟體、作業系統是否更新、是否符合本所安全政策。如果設備未達到安全標準，NAC 可限制其網路存取權限或直接阻止連線，確保內部網路免受威脅。NAC 也能與身份存取管理(IAM)與 SIEM 系統整合，提供更精細的存取控制與即時威脅偵測。

初始部署成本：

(1) 需要購買 NAC 伺服器或 NAC 雲端服務，視本所規模可能需額外部署多台設備，成本較高。

(2) 網路設備升級需求：若現有網路設備（交換器、路由器）不支援 NAC 功能，需更換或升級，增加硬體成本。

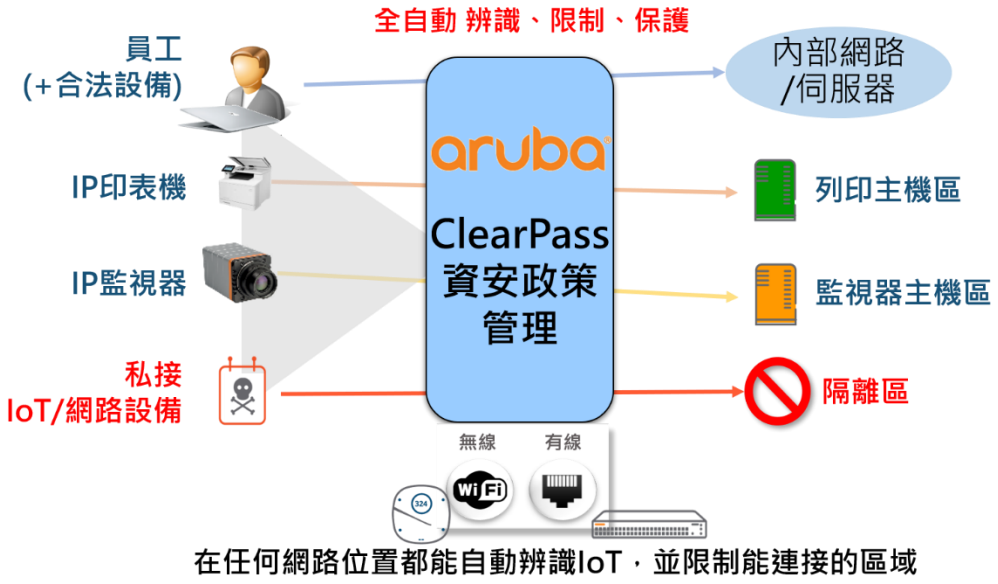
維運成本：

(1) 需定期調整 NAC 安全政策，以適應組織變化（如新同仁加入、新設備連線），增加管理負擔。

(2) NAC 伺服器與相關軟體需定期更新，以防範新型態攻擊，並確保與其他資安工具相容。

表 5 網路存取控制優缺點

優點	缺點
(1) 強化網路安全： 可防止未經授權或受感染的設備存取本所網路，降低惡意軟體傳播風險。 (2) 合規性管理： 確保連線設備符合安全政策，滿足本所資安規範。 (3) 動態存取控制： 可根據使用者角色與設備狀態，自動調整存取權限。	(1) 部署與維護複雜： 需要建立完整的設備識別與存取策略，初期設定成本較高。 (2) 影響使用者體驗： 可能因設備不符合安全標準而導致使用者無法順利連線，影響工作效率。 (3) 整合需求高： 需與 IAM、EDR、SIEM 等安全系統整合，確保完整的安全機制。



圖二、網路存取控制方案

資料來源：網聯資訊(https://www.wantnetinfo.com/system-integration/Secur 資訊 y/arubacleapass)

3.防火牆(Firewall)

防火牆是網路安全的第一道防線，主要負責監控和控制內外部網路之間的流量，以防止未經授權的存取和攻擊。傳統防火牆主要使用基於 IP 和埠號的存取控制，而現代防火牆則結合應用層過濾、深度封包檢測、入侵防禦等技術，能夠更精確地識別與攔截惡意流量。防火牆還可與微分割技術結合，將內部網路劃分為多個隔離區域，防止駭客在受感染設備之間橫向移動，進一步提升安全性。

初始部署成本：

(1) 防火牆處理大量封包時，可能影響網路效能，若需升級頻寬或搭配負載平衡設備，會進一步增加成本。

(2) 需設計防火牆存取規則，防範內外部威脅，若設定錯誤可能影響業務運作，專業人員需求提高。

維運成本：

(1) 防火牆韌體與規則庫需定期更新，以確保防禦能力，部分廠商可能需額外收取授權費。

(2) 若本所需要 24/7 不間斷防護，需購買雙機備援方案 (Active-Standby)，以防止防火牆設備故障導致業務中斷。

表 6 防火牆優缺點

優點	缺點
(1) 流量過濾與存取控制： 能有效阻擋未經授權的存取，防止惡意攻擊。 (2) 深度檢測與應用層防護： 次世代防火牆能夠檢測惡意流量，攔截潛在威脅。 (3) 阻擋 DDoS 攻擊： 具備防禦 DDoS（分散式阻	(1) 規則配置複雜： 需要詳細設計存取規則，若設定錯誤可能影響正常業務運作。 (2) 無法完全防禦內部攻擊： 防火牆主要防禦外部威脅，對於內部攻擊的防禦能力有限。

斷服務攻擊）的能力，可降低網路中斷風險。	(3) 維護與升級成本高： 需要定期更新安全規則與防火牆韌體，以應對新型態攻擊。

(三)行為分析

行為分析是重要的資安技術，它利用機器學習建立使用者行為模型，如同為每位使用者建立專屬的「行為指紋」。系統會持續監控使用者的網路活動，例如登入時間、地點、存取的檔案等，並與基準模型進行比對。一旦發現異常行為，例如在非上班時間登入系統或嘗試存取未經授權的檔案，系統就會立即發出警報，甚至阻擋可疑操作，有效防止潛在的資安威脅。技術方案如下：

1.安全資訊與事件管理(SIEM, Security Information and Event Management)

SIEM 是一種集中化的安全監控與事件管理解決方案，其核心功能包括即時監控、日誌收集、威脅偵測與事件應對。SIEM 會收集來自各種資安設備（如防火牆、入侵偵測系統、端點安全工具等）以及資訊基礎設施（如伺服器、應用程式和資料庫）的大量日誌數據，並透過規則引擎與機器學習分析異常行為，協助資安團隊識別潛在攻擊。當 SIEM 偵測到異常行為時，例如異常登入、異常網路存取或惡意軟體活動，會自動發送警報，讓資安人員能夠迅速應對。

初始部署成本：

(1) SIEM 需要專用伺服器或雲端服務來處理日誌數據，可能需支付 一次性授權費或訂閱費用。

(2) 因 SIEM 需長期儲存大量日誌，可能需額外添購高容量儲存設備或雲端儲存空間，增加硬體成本。

維運成本：

(1) 需持續調整 SIEM 規則，避免誤報與漏報，可能影響資安團隊工作負擔。

(2) SIEM 平台需定期更新與維護，以確保支援最新的安全威脅偵測功能，可能需支付額外維護費用。

表 7 安全資訊與事件管理優缺點

優點	缺點
(1) 集中管理安全資訊： 提供跨系統、跨設備的統一視角，提升可見性。 (2) 即時威脅偵測與回應： 能夠迅速識別異常行為，並提供可行的應對措施。 (3) 支援自動化應對： 與 SOAR（安全編排與自動化回應）工具整合，能自動處理某些威脅事件。	(1) 初期部署成本高： 需要大量的基礎設施與設定，且不同來源的日誌整合可能較為複雜。 (2) 高誤報率： 若規則設定不當，可能導致過多警報，影響資安人員的效率。 (3) 數據存儲需求大： 需長期保存大量日誌數據，對於儲存與計算資源的需求較高。

圖三、安全資訊與事件管理方案

資料來源：北祥資訊(https://www.pershingdata.com.tw/tw/secur 資訊 y_qradar_siem.aspx)

2.使用者和實體行為分析(UEBA, User and Entity Behavior Analytics)

UEBA 是一種透過機器學習與行為分析技術，來識別潛在威脅的安全方案。傳統的安全解決方案（如 SIEM 和防火牆）主要基於規則與簽名來偵測威脅，而 UEBA 專注於使用者和裝置的行為模式，透過建立正常行為基線，來識別異常活動。例如，UEBA 會分析使用者的登入時間、地點、存取的系統與資料行為，當偵測到異常（如使用者在異地登入、異常下載大量機敏資料、或嘗試存取平時不會使用的系統），即會發送警報，協助資安團隊發現內部威脅，例如同仁帳號被盜用、內部人員惡意洩密、或裝置遭受攻擊。相較於傳統規則式偵測，UEBA 更具適應性，能夠有效識別新的、未知的資安威脅。

初始部署成本：

(1) UEBA 依賴 AI 與行為分析技術，需購買或開發 AI 模型與行為分析系統，導入成本較高。

(2) UEBA 需收集大量歷史行為數據來建立「正常行為基線」，建置初期可能需數週或數月 來進行數據訓練。

維運成本：

(1) UEBA 可能涉及使用者行為監控，需符合數據隱私法規，可能帶來額外的法律與技術成本。

(2) 隨著時間推移，UEBA 需儲存大量使用者行為數據，可能需購買 雲端儲存或高效能運算資源。

表 8 使用者和實體行為分析優缺點

優點	缺點
(1) 識別內部威脅： 能夠檢測內部同仁濫用權限或帳號遭竊取的行為，防範內部攻擊。 (2) 降低誤報率： 相較於傳統規則式偵測，UEBA 透過行為基線來識別異常，降低誤判可能性。	(1) 依賴大量數據訓練： UEBA 需要長期監測使用者行為，建立行為基線，才能有效偵測異常。 (2) 隱私問題： 持續追蹤使用者行為可能涉及隱私問題，需符合隱私保護法規。

3.端點偵測與回應(EDR, Endpoint Detection and Response)

EDR 主要負責監控、記錄並分析端點設備（如個人電腦、伺服器、行動裝置）上的活動，以即時偵測與回應潛在攻擊。相較於傳統防毒軟體，EDR 不僅能掃描已知惡意軟體，還能透過行為分析與威脅情報，偵測未知或零時差攻擊。當端點設備上出現可疑行為（如異常程式執行、檔案加密行為、未授權存取系統），EDR 會自動記錄該活動，並可根據威脅等級自動阻斷攻擊、隔離受感染的設備，或通知資安團隊進行。此外，EDR 也支援事件調查與回溯分析，協助資安團隊追蹤攻擊來源與影響範圍，進一步強化整體資安能力。

初始部署成本：

(1) EDR 需在每台電腦、伺服器、行動裝置上安裝代理程式，可能涉及大量裝置授權費用。

(2) 初期需設計惡意行為偵測規則與應對策略，可能需專家顧問協助，增加初始成本。

維運成本：

(1) 端點設備需定期更新 EDR 代理程式，確保相容性與防禦能力，增加管理成本。

(2) 部分 EDR 方案可能會影響端點裝置效能，需優化設定，避免影響業務運作，可能增加資訊團隊維護工作量。

表 9 端點偵測與回應優缺點

優點	缺點
(1) 即時威脅偵測： 能夠即時識別端點上的異常活動，減少攻擊影響。 (2) 自動應對能力： 可自動隔離受感染設備、終止惡意程式，降低攻擊擴散風險。 (3) 深入調查與回溯分析： 記錄完整端點活動，協助資安團隊進行事後分析。	(1) 需大量運算資源： 持續監控端點可能會影響系統效能，尤其是在高負載環境下。 (2) 無法防範網路層攻擊： EDR 主要針對端點設備，對於網路層的攻擊無法直接防禦。

(四)身份和存取管理(IAM, Identity and Access Management)

IAM 提供集中化的身份管理和存取控制，讓管理者可以有效地管理使用者帳號、角色和權限，並實現單一登入(SSO, Single Sign-On)等功能。技術方案如下：

1.目錄服務（Directory Service）

目錄服務是一種集中式的身份與存取管理解決方案，主要用於儲存、組織與管理本所內部的使用者、裝置與應用程式的身份資訊。其中，AD (Active Directory)是微軟的目錄服務，負責身份驗證與存取控制，讓資訊管理員能夠統一管理使用者帳號、群組與權限，確保資源存取的安全性。此外，LDAP(Lightweight Directory Access Protocol)是一種開放標準的協議，可用於跨平台的身份管理，支援 Linux、Windows 及雲端應用，讓不同系統能夠透過統一的介面存取身份資訊。透過目錄服務，本所能夠實現單一登入(SSO, Single Sign-On)，使用者只需登入一

次，即可安全存取多個系統，提升使用體驗並降低管理負擔。此外，目錄服務可與多因子驗證(MFA)整合，進一步提高安全性，防止帳號被竊取或未經授權存取的風險。

初始部署成本：

(1) 若採用 Microsoft Active Directory，需購買 Windows Server 授權與 CAL 授權，成本較高。若使用 LDAP，則可能需額外部署開源或商業版本的目錄伺服器。

(2) 若本所要求 24/7 高可用性，需建立目錄服務備援架構(如 AD 多站台同步)，可能增加硬體與網路設備成本。

維運成本：

(1) 需持續管理使用者帳號、群組與權限，確保帳號生命周期符合安全政策，增加資訊團隊的管理負擔。

(2) 目錄服務需定期更新，以修補安全漏洞，確保與新應用相容，可能需額外聘請專業資訊人員或顧問支援。

表 10 目錄服務優缺點

優點	缺點
(1) 集中化管理： 統一管理使用者帳號與權限，減少手動配置錯誤的風險。 (2) 提升安全性： 透過身份驗證與存取控制，確保只有授權使用者能存取敏感資源。 (3) 支援 SSO： 減少使用者登入不同系統時需要記住多組密碼的困擾，提升效率。	(1) 部署與維護成本高： 需專業資訊人員進行設定與管理，對於小型本所可能負擔較重。 (2) 單點故障風險： 如果目錄服務發生異常，可能影響整個本所的身份驗證與存取，需搭配高可用性架構。 (3) 權限管理需謹慎設定： 若設定不當，可能造成過多權限暴露，導致資安風險。 (4) 異質系統整合需額外配置： 不同系統（例如 Windows 與 Linux）可能需要額外的中介軟體或 API 來確保互通性。

2.權限管理系統（Access Control System）

負責確保使用者只能存取符合其角色與權限範圍的資源，從而降低未經授權存取的風險。權限管理系統通常採用角色型存取控制或屬性型存取控制來定義存取權限。例如，Open Policy Agent(OPA)是一款開源的存取控制引擎，可應用於 API Gateway、雲端服務等場景，根據使用者身份、裝置狀態、網路來源等條件動態決定存取權限。在 API 保護方面，OPA 可根據請求來源 IP、使用者角色或請求內容來決定是否允許存取特定 API，這有助於減少潛在的攻擊面。此外，相較於傳統的靜態權限管理，OPA 提供更靈活且可擴展的策略管理機制，讓本所能夠根據需求快速適應變更，確保資源安全性。

初始部署成本：

(1) 需與目錄服務(AD/LDAP)、API Gateway、應用系統進行整合，確保能夠精細管理不同層級的存取權限，開發與設定成本較高。

(2) 存取控制系統需 即時判斷存取請求，若策略過於複雜，可能影響應用效能，需配置高效能伺服器

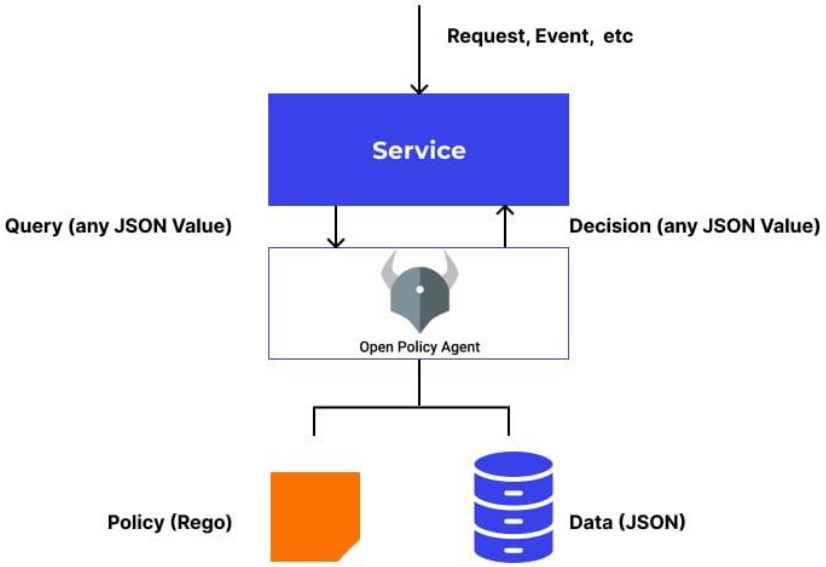
維運成本：

(1) 隨著組織架構變更、業務需求變動，權限規則需持續調整，資訊 部門需定期檢視與優化存取策略，確保安全性與靈活性。

(2) 使用者可能因權限不足導致存取問題，資訊部門需提供技術支援與培訓，以減少日常運作的干擾。

表 11 權限管理系統優缺點

優點	缺點
(1) 動態權限管理： 可根據使用者行為、設備狀態、時間等因素動態決定權限。 (2) 細緻存取控制： 可根據本所需求靈活設定不同層級的權限。 (3) 提升安全性： 降低超權限存取風險，確保敏感資源不會被未授權的使用者存取。	(1) 學習門檻高： 如 OPA 需要學習 Rego 語言，資訊人員需要額外培訓。 (2) 初期部署較為複雜： 需與現有身份驗證、存取管理機制整合，設定細緻權限策略可能需要較長時間。 (3) 需定期維護： 存取策略需隨組織需求調整，若未及時更新，可能導致存取異常或安全漏洞。 (4) 效能影響： 過於複雜的存取策略可能會影響系統執行效率，需要優化配置。



圖四、安全資訊與事件管理方案

資料來源：wallarm(https://www.wallarm.com/cloud-native-products-101/what-is-an-open-policy-agent-opa)

四、結論

實施零信任架構是一個逐步推進的過程。建議從評估現有資訊系統的安全狀況入手，識別潛在的風險和漏洞，然後制定詳細的實施計畫。在這個過程中，可能需要對現有的網路架構進行調整，甚至引入新的安全技術和工具。此外，成本也是一個不可忽視的因素。實施零信任架構可能需要一定的初期投資，包括技術設備的採購、系統整合以及人員培訓等。然而，從長遠來看，這項投資是值得的。因為它可以顯著降低因網路攻擊導致的損失，保護本所的重要數據和資訊資產。

總之，通過合理的規劃和堅定的執行，能夠有效防禦各種已知的網路攻擊，還能提高我們應對未來潛在安全威脅的能力。

參考文獻

1. cloudflare：https://www.cloudflare.com/zh-tw/learning/network-layer/what-is-sdn/
2. 網管人：https://www.netadmin.com.tw/netadmin/zh-tw/feature/4936786C813D4F8886724E95E3ACABA8
3. 網聯資訊(https://www.wantnetinfo.com/system-integration/Security/arubacleapass
4. FORTINET：https://www.fortinet.com/tw/resources/cyberglossary/access-control
5. 微軟：https://www.microsoft.com/zh-tw/security/business/security-101/what-is-siem
6. 微軟：https://www.microsoft.com/zh-tw/security/business/security-101/what-is-user-entity-behavior-analytics-ueba
7. Trend Micro：https://www.trendmicro.com/zh_tw/what-is/xdr/edr.html
8. 資安趨勢中心： https://www.trendmicro.com/zh-tw/security/resources/security-center/topics/zero-trust-network-architecture
9. 國家資通安全研究院：https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/
10. 資策會產業情報研究所：https://www.iii.org.tw/
11. Check Point：https://www.checkpoint.com/tw/solutions/zero-trust-security/
12. Forcepoint：https://www.forcepoint.com/zh-tw/resources/zero-trust-security