對本書的讚譽

零信任不只是一種安全策略，而且是一種假設、質疑的心態，要仔細審度每一次互動，以防數位系統遭受未知的敵人所侵害。本書可作為技術長（*CTO*）、工程師和資訊技術專業人員的實用指南，協助他們踏上零信任之旅。

—*Ann Johnson*，微軟安全部門企業副總裁

本書用易於理解的言語封裝零信任安全的基本概念，是初學者和專業人士必讀的權威之作。

—*Karan Dwivedi*，谷歌的資安工程經理

本書對零信任安全模型的精采闡述，著實令人嘆為觀止。除了介紹零信任安全的重要支柱，也涵蓋 *NIST*、*DoD*、*CISA* 和其他機構所開發的零信任框架，對於任何想要瞭解如何實施零信任安全模型的人，這是一份務必擁有的無價之寶！

—*Andrew Cameron*，汽車業界的技術專家

讀者可能沒有意識到我們天天都依賴電腦，不管你搭飛機、上醫院、乘火車，甚至在家裡打開電燈，這些都會用到電腦，一旦發生安全事件就可能造成一片混亂，因此，保護基礎設施的安全是刻不容緩的事。零信任網路為我們提供保護資產的基本原則和思維模式，值得我們去瞭解。本書對開發人員、基礎設施工程師和管理人員來說，都是一項令人讚嘆的資源，它清楚明白地告訴我們為什麼需要，以及如何實作零信任。

—*Sahil Malik*，資訊界的安全工程師

目標讀者

是否感受到集中式防火牆的維運預算受到限制，甚至無法有效管理？是否為了惱人的 VPN 管理、跨眾多應用系統及程式語言的 TLS 設定，或者繁瑣的法遵和稽核規定而痛苦掙扎？這些只是零信任模型要解決的一小部分問題，讀者若正在找尋解決前述問題的良方，只能說你太幸運了，這本書就是你的處方箋。

網路管理員、資安工程師、技術長（CTO），以及置身其中的任何人，皆可因學習零信任網路管理而受益。本書內容淺顯易懂，即使沒有相關專業技能也能理解作者介紹的各類原理，進而引領讀者在實現零信任模型的過程中做出正確決策，逐步改善機構的整體資安局勢。

此外，具備組態管理系統（CMS）維運經驗的讀者，將發現使用相同概念建構更安全和可維運網路的契機，網路中的資源在預設條件下就能得到安全保護。他們將意識到自動化系統能幫助實現新的網路設計型態，可以更輕鬆地完成細緻的安全控制。本書還會探討成熟的零信任網路設計，對已吸收基本原理的人，促使他們更進一步提升安全系統的強度。

撰寫目的

在 2014 年的同業會議上，筆者開始介紹規劃系統和網路的新手法，當時是透過組態管理嚴格定義系統狀態，以程式化方式回應網路拓撲的變動。利用自動化工具處理的過程中，自然而然採用程式化方式處理網路架構實作的細節，而不是手動管理設備的組態，我們發現使用自動化獲取系統設計資訊的方式，能夠比以往更輕鬆地部署和管理系統的安全特性，例如設定存取權限控制和資料加密等。更棒的，與一般系統相比，這些作為讓我們大大降低對網路信任的依賴，這是維運公有雲或跨雲環境安全時的關鍵考量。

撰寫本書時，筆者訪談了數十家公司的相關人員，聽取他們對網路安全設計的看法，發現有許多公司都已開始降低對內部網路的信任。儘管這些機構在各自系統裡採行的手法略有不同，但很明顯都在相同的威脅模型下作業，發展出來的解決方案也有多處相同特質。

本書目的並非提供一兩種建構此類系統的特定方案，而是制定一套不以信任為基礎的網路通訊系統模型，因此，不會專門使用特定廠商的軟體或實作方法，而是探討建構零信任網路的理念和原則。期望讀者從本書得到啟示，在建構自己的系統時能有清晰思路，瞭解如何建構安全的系統，甚至針對書中描述的問題，找到更佳、可重複使用的解決方案。

本書內容概要

本書各章主題安排如下：

- 第 1 章和第 2 章會討論零信任安全模型的基本概念。
- 第 3 章和第 4 章探討成熟零信任網路中常見的新觀念：具情境感知的網路代理和信任引擎。
- 第 5 章至第 8 章詳細介紹網路上的各種參與者如何建立信任，特別是針對設備、個人、應用程式和網路流量之間的信任關係，內容主要聚焦在現有技術上，這對傳統的網路安全模型可能很有用。另外，每章結尾的情境推演，可協助讀者瞭解如何將零信任的核心原理應用於真實的世界場景中。
- 第 9 章則融合前面幾章的內容，討論如何建構自己的零信任網路，並提供兩個研討案例。
- 第 10 章將從攻擊者角度看待零信任安全模型，探討此模型的潛在弱點之防治手段，以及哪些弱點不是零信任網路可以處理的。
- 第 11 章會探討來自 NIST、CISA、DoD 等機構的零信任架構、標準和框架，希望藉由業界權威機構的角度，協助讀者理解零信任安全模型。
- 第 12 章摘要說明實施零信任計畫時，可能遭遇的各種功能和技術障礙，並從高階角度提供因應這些挑戰的實用考量因素。此外，也研究人工智慧（AI）、量子運算和隱私增強技術對零信任安全模型的影響，這些都是值得瞭解的重要科技進展。既然知道人工智慧、量子運算和隱私增強技術會對零信任安全模型造成影響，並在資安策略中扮演重要角色，就更應該去關注這些科技發展趨勢。

本書編排慣例

本書編排慣例如下：

斜體字（*Italic*）

表示首次出現的術語、URL、電子郵件位址、檔案名稱及延伸檔名（副檔名）。中文以楷體表示。

定寬字（`Constant width`）

用於程式碼清單及書寫於段落的程式元素，例如變數或函式名稱、資料庫、資料類型、環境變數、敘述句和關鍵字等。

關於零信任網路

零信任網路的概念是基於五項主張：

- 網路始終受到對手覬覦。
- 網路隨時面臨外部和內部的安全威脅。
- 不能單單以網路的位置作為決定網路信任度的依據。
- 必須對所有設備、使用者和網路流量進行身分驗證及管理存取授權。
- 安全政策必須可動態調整，並盡可能以各種資料來源作為評估依據。

傳統的網路安全架構會部署一套或多套防火牆，將網路（或某個網段）劃分成不同區域，每個區域被授予某種程度的信任，藉以決定存取網路資源的權限，此模型可提供強大的縱深防禦。例如，面向網際網路的 Web 伺服器被視為具高度風險的資源，應部署在可嚴格監控和控制流量的繳械區（通常稱為 DMZ；非軍事區），讀者可能看過類似這種架構的安全手法，如圖 1-1 所示。

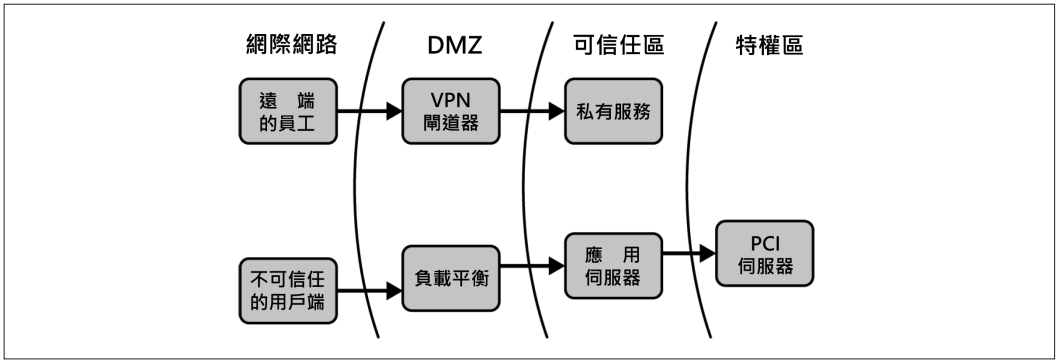

圖 1-1　傳統的網路安全架構

在昔日看來堅實的措施，如今不過是一時權宜，面對現代的網路攻擊型態，已然捉襟見肘、力有未逮，而零信任模型則完全翻轉這種架構。傳統架構主要缺點有：

- 缺乏內部區域的流量檢查。
- 主機的實體或邏輯部署都缺乏彈性。
- 存在單點失效（SPOF）全軍覆沒的缺陷。

注意，若打破網路的區域性，就不再需要虛擬私有網路（VPN）。通過身分驗證的使用者可以經由 VPN 收到遠端網路所分配的 IP 位址，之後，本地設備透過隧道（加密通道）將封包送到遠端網路，遠端網路解開加密的封包後，再將它轉送到目的地，這是一扇沒有人會質疑的最大後門。如果網路位置不再具有安全的評斷價值，則 VPN 和其他網路安全設備也就變得不重要了，因此，這種防護手段必須將安全控制點盡可能推向網路活動的邊緣，與此同時也減輕核心設備的安全責任。此外，主流作業系統都具備狀態防火牆（stateful firewall）功能，而網路交換和路由技術的進步，也為網路邊緣提供安裝高階功能的機會，將這些優點集合在一起，可得出一個結論：是該進行網路安全模式轉換的時候了。我們勾勒出類似圖 1-2 的設計架構，也就是實施分散式安全政策及應用零信任原則。

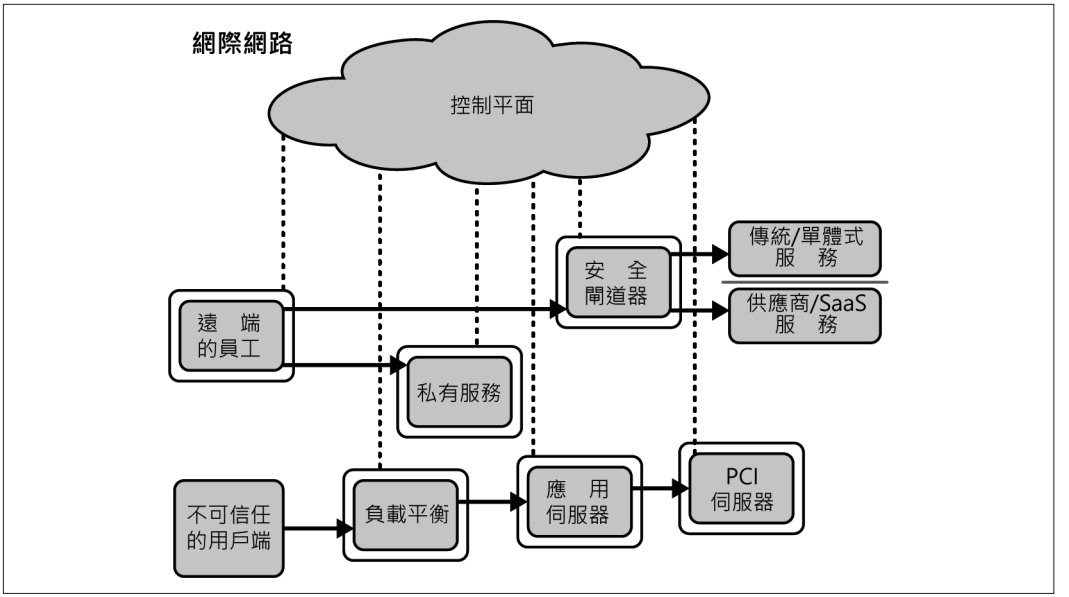

圖 1-2　零信任架構

零信任控制平面

支撐零信任架構的系統稱為控制平面（*control plane*），而其他由控制平面統籌協調和配置的部分則稱為資料平面（*data plane*）。存取受保護資源的請求會先經由控制平面處理，同時對設備和使用者進行身分驗證，並按照請求者在機構中的角色、不同時段、發動請求時的地理位置或設備類型給予適當授權。控制平面可以提供細緻的管理政策，對於存取更高安全性的資源，還能額外要求更高強度的身分驗證。

一旦控制平面允許該項請求，將動態設定資料平面以接受來自該用戶的流量。此外，控制平面還可以協調請求者和資源之間的加密隧道之詳細參數，包括短暫的一次性身分憑據（credential）、金鑰和臨時端口。

注意，控制平面決定放行此請求的決策是具有時效性，而非持久。也就是說，當控制平面在前次允許此請求之後，發現決策因素產生了變化，它可能會與資料平面協調，撤銷對該資源的請求權限。

雖然這些控制措施的強度不見得盡善盡美，但基本思維是：由一個可信賴的來源或受信任的第三方，依照各種輸入資訊，對請求者即時進行身分驗證、授權及協調存取項目。第 2 章會更深入探討控制平面和資料平面。

邊界安全模型的演進

本書所指的傳統安全架構，通常稱作邊界安全模型，這種手法就像使用城牆保護實物安全一般，藉由建立幾層的防線，入侵者必須先滲透防線才能接觸到機敏物件。不幸的是，面對電腦網路環境，這種方法天生就存在缺陷，並不能滿足安全需求。回顧這種模型的進化過程，有助於釐清這些缺陷的成因。

管理全球的 IP 位址空間

成就邊界安全模型的歷程，要從 IP 位址分配說起，網際網路興起之初，網路相連的成長速度不斷增加，若不是連接到網際網路（當時網際網路尚不普及），就是連線到另一個業務部門、另一家公司或某個學術網路。然而，在任何一個 IP 型網路裡，IP 位址必須是唯一的，若網管人員不幸使用範圍重疊的 IP 位址，將耗費許多心力來修正 IP 配置，如果讀者要連線到網際網路，就必須使用全球唯一的 IP 位址。顯然，這需要一些協調機制。

網際網路編號分配機構（IANA；*https://oreil.ly/A0rHj*）於 1998 年正式成立，是當今提供 IP 位址分配的協調機構。在成立 IANA 以前，負責 IP 位址分配的任務由 Jon Postel 負責，是 IP 位址所有權紀錄的權威來源，圖 1-3 的網際網路地圖就是他設計的，在當時，想確保擁有全球唯一的 IP 位址，可以向他註冊。在那個年代，就算不連接網際網路，仍然慫恿人們去註冊 IP 位址空間，因為大家認為現在不連接網際網路，說不定在某個時點也會連接到別人的網路。

第二章

管理信任關係

信任管理可能是零信任網路的最重要元素。大家多少知道什麼是信任，你可能信任家人，但大概不會信任街上的行人，當然更不可能信任目露凶光或具有威脅性的陌生人。何以如此？

首先是因為認識家人，知道他們的相貌、居住地，甚至一輩子都住在一起，他們是怎樣的人，你再清楚不過了。面對重要抉擇時，更可能相信他們，而不是其他人。

另一方面，陌生人是一個完全未知的個體，也許曾見過他們的臉，或許對他們也有一些基本瞭解，但不知道他們住在哪裡，也不清楚他們的成長歷程，表面看起來也許很和善，但面對重要抉擇時，你不會找他們商量。或許上廁所時會拜託他們幫忙看著行李，但絕不會請他們幫你到 ATM 提款。

總之，只需單純依照處境、個人及對這些人事物的理解，便能決定可信任程度。到 ATM 提款需要極高信任，看管行李就不需太多信任，但也絕非毫無信任。

或許你不會完全信任自己，但可以確認所採取的行動絕對是你自己所為，依照這種邏輯，零信任網路的信任往往源自網管人員，在零信任網路中談信任似乎有些矛盾，有個重點要瞭解，信任不是與生俱來的，必須從某個地方獲取並謹慎管理。這裡還有個小問題：無法一直要求網管人員提供授權和賦予信任！想增加網管人員數量也很困難。還好，可如圖 2-1 所示，透過信任委派方式解決這些問題。

信任評分

如圖 2-4，零信任網路利用信任評分來定義網路內部的信任度，它不是以二分法的政策決定參與者的信任，而是持續監視網路參與者的行為，不斷更新其信任分數，之後，依照違反信任的嚴重性，為不同分數訂定信任政策（參考圖 2-5）。使用者從不受信任的網路查看行事曆，所需信任分數相對較低；若同一位使用者嘗試更改系統組態，需要更高的分數，若分數不足，該次請求將被拒絕或需要通過審查。即使這樣簡單的例子，也能看出採用信任評分的優勢，可以進行更細緻的判斷及確保信任得到充分維護。

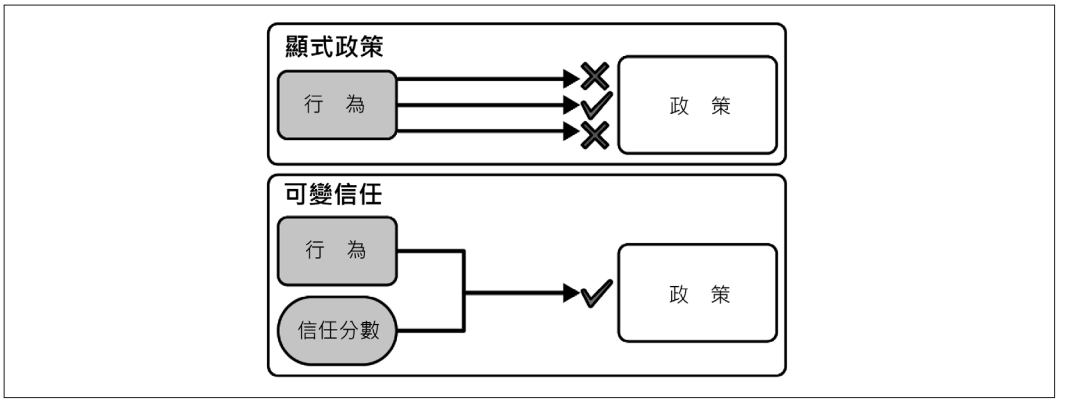

圖 2-4　使用信任評分可以讓更少的政策提供相同數量的存取管制

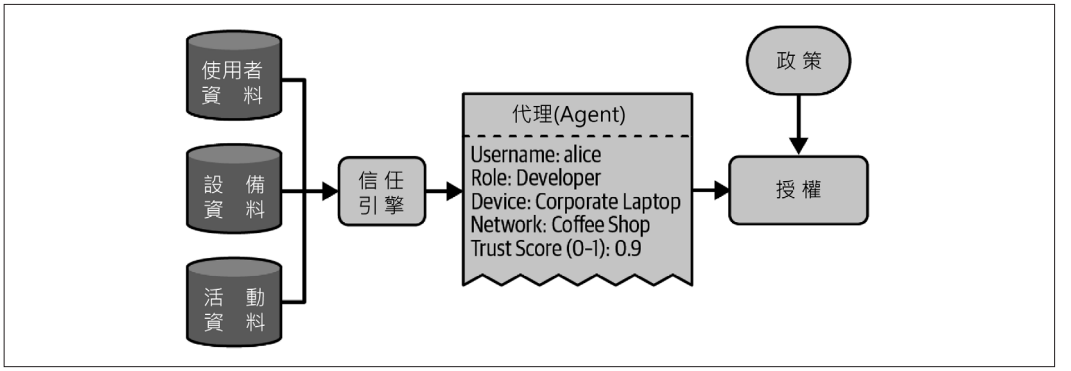

圖 2-5　信任引擎計算分數及形成代理，代理再與政策進行比較以得到授權。第 3 章會進一步討論代理機制

當需要符合如歐盟一般資料保護規則（GDPR）或聯邦政府風險與授權管理計畫（FedRAMP）等法規標準的要求時，會影響政策引擎分析請求的決策過程。機構通常會部署版本管理系統，以滿足法規標準要求，透過系統來產生政策，最好是能夠完全自動化，但通常在發行政策之前會由人工進行最終審查，最終可以建立一套強大的系統，讓政策引擎可以查詢符合法規標準的儲存系統，以便判斷是否授予或拒絕該請求。

情境推演

結束本章之前，先來看看一個簡單但真實的情境，將有助於理解本章和之前章節所探討的組件，以及它們之間的互動方式。後續章節進一步探討零信任的各個面向，如使用者、設備、應用程式和網路流量時，會延續這裡所探討的情節。

Bob 是 Wayne 公司的業務經理，典型的工作流程是他打算存取某項資源，比如某部印表機。圖 4-5 是從高階角度所描繪有關此情境的零信任組件。

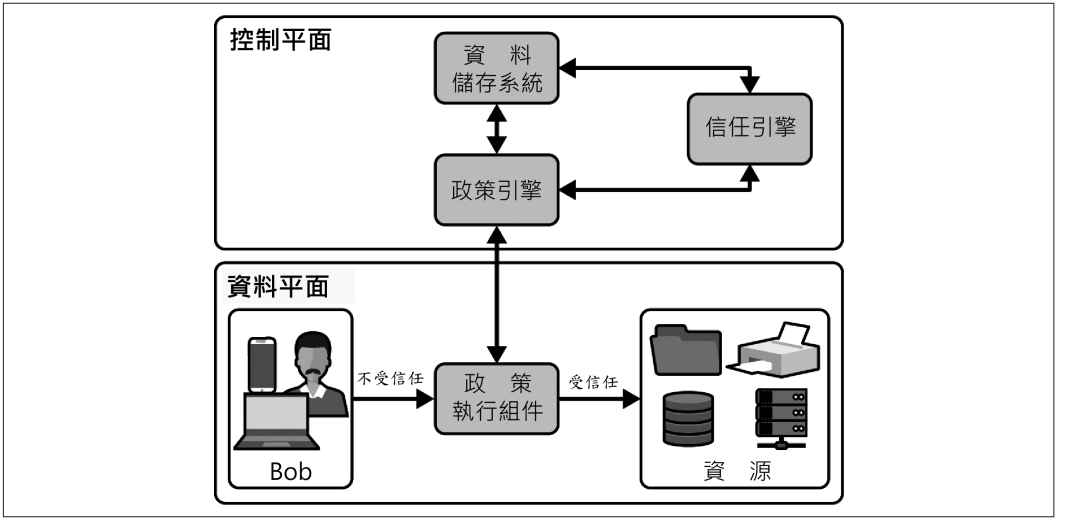

圖 4-5　具有控制平面、資料平面、使用者和資源的零信任安全模型之邏輯視圖

首先，檢視控制平面裡的組件（圖 4-6）。Bob 的個人資訊，如姓名、IP 位址和位置等是保存在使用者儲存區；這部設備的詳細資訊包括作業系統、是否已完成最新的安全修補；活動日誌會記錄 Bob 的每次互動資訊，包括時間戳記（Unix 格式）、IP 位址和地理位置。

藉由查找 Bob 活動日誌裡的異常行為，信任引擎能夠利用機器學習模型動態計算信任分數。它的主要責任是計算信任分數，以及將分數通知政策引擎。

政策引擎是控制平面的核心，它使用信任分數和法遵規則來判定是否授予或拒絕 Bob 的請求。

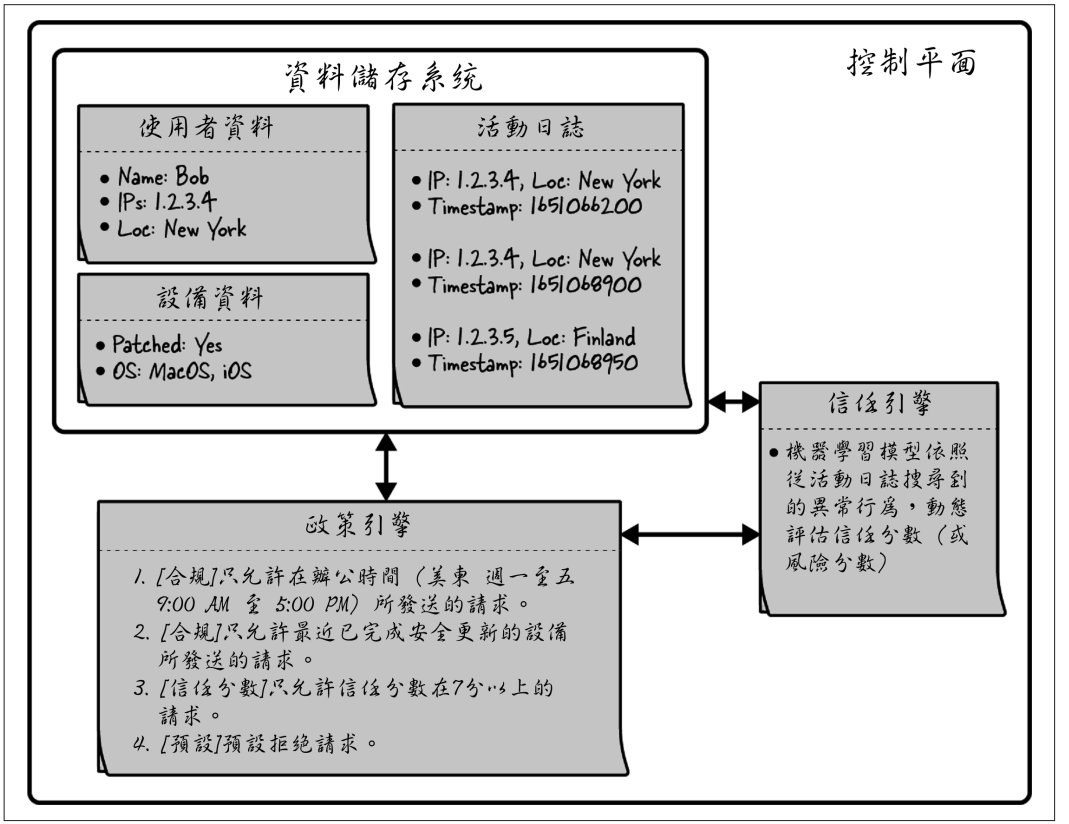

圖 4-6　政策引擎利用信任分數和法遵規則為存取請求進行授權決策

現在，近一步查看影響政策引擎行為的政策規則。前兩項與合規性有關，確保系統始終遵循法規和業務操作要求；第三項是將信任分數當作政策的動態輸入，確保僅在該分數超過一定閾值時才授予請求。最終，若沒有其他適用的政策規則，則將預設動作設為拒絕請求，確保只有在政策規則明確授予存取權時，使用者才能進行存取：

1、合規性

僅允許在辦公時間內的請求，亦即，北美東部時間（EST）星期一至星期五上午 9 點至下午 5 點之間。

2、合規性

僅允許已安裝最新安全修補的設備所發送之請求，目的是確保設備已完成弱點修補，降低惡意攻擊的成功率。

3、信任分數

僅允許信任分數大於等於 7 分（最高 10 分）的請求。亦即，較高的信任分數可提供較高的信任度，這裡以 7 為合格值。政策裡的信任分數通常是可設定的，可隨時間需要進行調整，以確保平衡；較低的分數閾值可能成為惡意請求可滑過的破口，而過高的分數可能對合理請求產生負面影響。

4、預設動作

如果沒有其他適用的政策規則，就使用這條萬用（預設）規則。這條規則很重要，建議設為拒絕請求。由於零信任系統裡沒有與生俱來的信任，每個請求預設都被視為惡意，再根據其自身價值進行評估，如此一來，這條政策規則就很實用。

接著來看資料平面，它包括政策執行、資源（印表機、檔案共享等），以及請求存取資源（本例為檔案共享）的使用者 Bob。圖 4-7 指出控制平面和資料平面的關係。

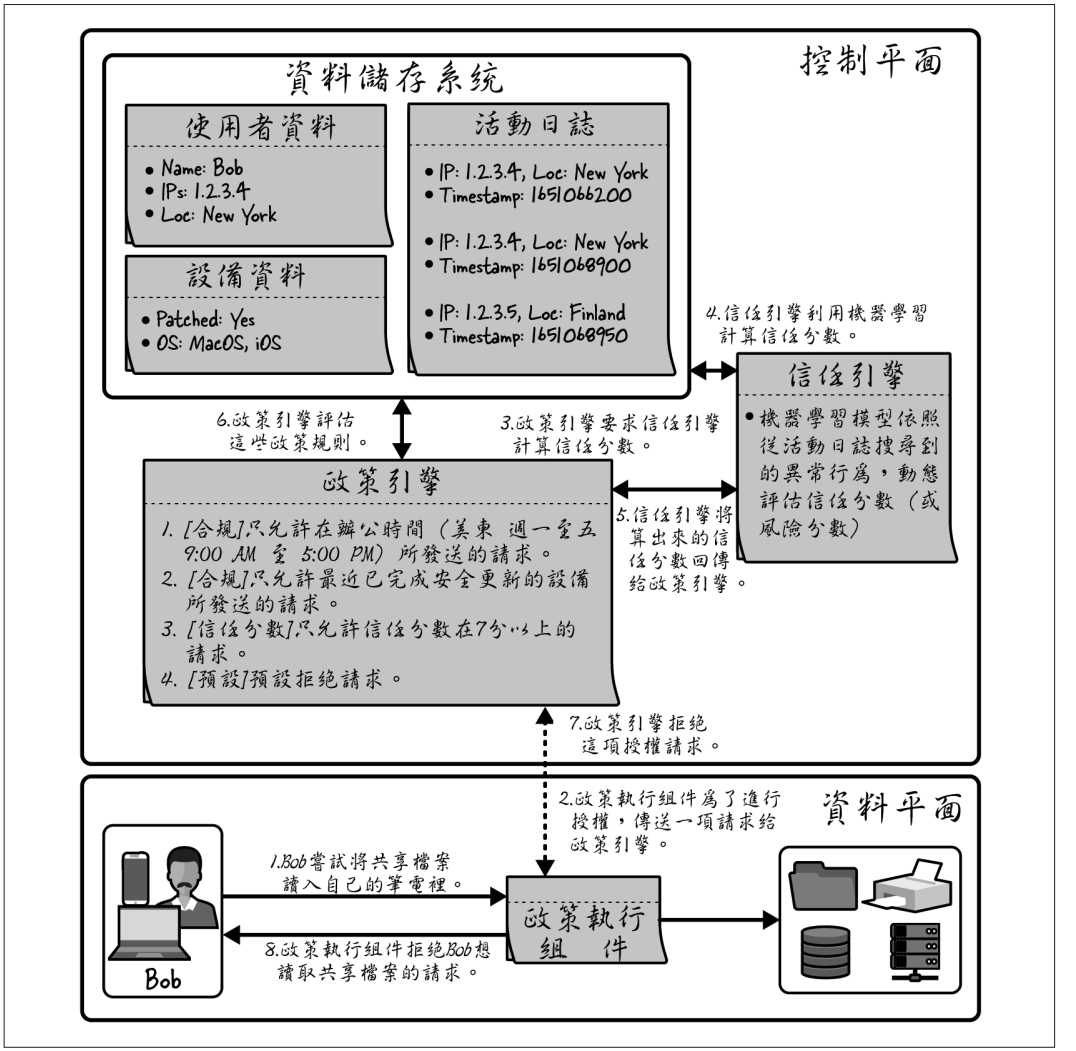

圖 4-7　經信任分數和其他政策規則評估之後，拒絕了 Bob 存取共享檔案的請求

我們來逐步分析 Bob 的請求：

1. 在北美東部標準時間（EST）星期一上午 9:30，Bob 以筆記型電腦要求存取檔案共享資源，這部筆電已完成安全修補，它的作業系統為 MacOS。
2. 政策執行組件攔截此請求，再將它發送給政策引擎進行授權。
3. 政策引擎收到請求後，與信任引擎協商，確認此請求的信任分數。

第十章

駭客眼中的零信任網路

以敵對的觀點，假設所有數位系統都可能存在漏洞，惡意攻擊者會不斷嘗試入侵系統。從這個視角理解敵方的手法，能夠評估系統遭受攻擊的機率和衝擊程度，以及找出潛在弱點，最終建立堅固、具韌性的安全系統。

要在零信任網路中有效防禦可能的入侵行為，機構必須瞭解攻擊者會如何試圖繞過安全措施，並積極找出可能成為攻擊目標的漏洞，以降低被成功入侵的機會。

面對與日俱增的複雜網路攻擊，機構必須轉向採用零信任模型來保護系統免受惡意活動的侵襲。儘管這種方法能夠大幅提升防止資料外洩的能力，但機構仍應注意與該模型相關的潛在陷阱、風險和攻擊向量。

本章將詳細探討與零信任模型相關的弱點風險，若打算滲透零信任網路，你會採取什麼行動？

潛在的陷阱與危機

實施零信任模型可能帶來複雜性、時間和成本方面的問題。

機構的身分驗證措施不夠周全，就可能被駭客突破，進而繞過其管制功能。若身分驗證系統及驗證政策設置不完善，可能妨礙使用者體驗和工作效率，錯誤組態甚至會造成安全漏洞，例如使用不正確的存取協定和驗證標準，或缺乏稽核動作而導致未經授權的存取。另一個問題是，只依賴身分驗證措施，卻未清晰觀測使用者的活動，可能會產生安全假象。此外，駭客也會不斷利用社交工程和釣魚攻擊，以便繞過身分驗證協定而獲得未經授權的系統存取權限。

零信任模型並非萬無一失的方案，攻擊者會不斷尋找方法來繞過機構所部署的安全控制措施。

與零信任網路相關的重大風險之一，是利用軟體漏洞或濫用系統權限來建立未經授權的存取管道。我們將這些入侵手法稱為攻擊向量（attack vector）。

攻擊向量

有許多攻擊向量可以繞過零信任網路，包括社交工程和竊取身分憑據、特權升級及橫向移動、分散式阻斷服務（DDoS）攻擊、零時差（zero-day）漏洞，以及應用程式破解技術。表 10-1 摘要介紹這些攻擊向量及因應對策。

這些攻擊向量可能擾亂機構的運作，最終目的是破壞整體安全。為了深入瞭解這些威脅，下一節會更詳細探討每個攻擊向量。

表 10-1　常見的攻擊向量和建議的防禦對策

分類	攻擊向量	方法說明	因應對策
身分識別、存取權限和身分驗證	內部人員的威脅	利用擁有合法網路存取權限的個人進行攻擊，進而取得高等特權。	持續監控、行為分析、存取控制。
身分識別、存取權限和身分驗證	竊取身分憑據，並冒用	使用被盜的身分憑據存取系統。	採用多因子驗證機制、定期更換密碼、強制要求密碼複雜度。
身分識別、存取權限和身分驗證	竊取身分憑據，並冒用	使用已知的使用者帳號和密碼組合。	採用多因子驗證機制，並監控失敗的系統登入嘗試。
雲端安全	雲端安全	挑戰零信任保護雲端環境的能力。	實作正確的雲端組態、身分識別和存取管理（IAM）政策，並使用雲端原生的安全工具。
雲端安全	組態設定錯誤	因不正確的組態設定，造成資料暴露或授予過多存取權限。	施行安全稽核、組態管理工具、自動化漏洞掃描。
資料處理	資料外洩	從網路中竊取機敏資料的技術。	部署資料外洩防護（DLP）工具，並監控出站流量。
設備信任	不可信的運算平台	利用基礎平台的漏洞。	在授予存取權限之前，確保設備已符合安全標準。

分類	攻擊向量	方法說明	因應對策
設備漏洞	物聯網（IoT）漏洞	利用缺乏強固安全性的 IoT 裝置。	更改 IoT 裝置的預設憑據，並定期更新韌體。
漏洞利用	零時差漏洞	因未知漏洞沒有可用的修補程式而遭到入侵。	定期更新、部署入侵偵測和防禦系統、實作網路分段保護。
網路和基礎設施的安全	DDoS 攻擊	利用極高流量壓垮網路或站點頻寬。	使用先進的 DDoS 防禦服務，並維護多元的網路資源。
網路和基礎設施的安全	MitM 攻擊	利用攔截通訊內容來竊取或竄改資料。	使用端點到端點的加密技術和安全的通訊協定。
網路和基礎設施的安全	控制平面的安全	藉由入侵路由控制來操縱網路流量。	部署網路監控工具，保護及監視控制平面
網路和基礎設施的安全	枚舉可用的終端設備	識別網路裡的設備或使用者。	實施網路隱形手段、網路分段保護，限制對未知查詢的回應內容。
社交工程和人為因素	實體脅迫	利用實體威脅，強迫某人執行不願意做的事。	實施實體保護措施、培養人員的安全意識和建立緊急代號。
社交工程和人為因素	釣魚和社交工程	利用詐術讓人透露機敏資料或執行駭客想要的動作。	培養人員的安全意識、實施多因子驗證、確保電子郵件的安全。
session 和資料處理	利用已失效資訊	利用已失效的身分符記（token）或 session 來繞過安全管制。	限制 session 的效期，對於重要操作，應要求使用者再次驗證身分。
session 和資料處理	連線劫持	攻擊者接管有效的使用者連線 session。	使用加密的 session、定期更新 session 符記，對於重要操作，應要求使用者再次驗證身分。
來自第三方的風險	供應鏈攻擊	入侵第三方供應商或軟體以取得目標系統的存取權限。	定期執行供應商風險評估、實施安全稽核、建立允許的應用程式清單。

零信任的關鍵原則總結如下：

- 始終假設存在漏洞 / 遭到入侵。
- 總是實施最小權限存取。
- 總是管制每個請求 / 連線的存取活動。
- 始終授予精確 / 恰好足夠的存取權限。
- 始終應用具有動態特性的存取政策。
- 始終將系統裡的所有運算服務及資料源，皆視為需被保護的資源。
- 始終持續監控所有資源及評估其安全狀態，並根據威脅情況動態調整存取政策。
- 永遠不要只根據網路位置就授予存取權限。

整體考量資源存取權限

NIST 的指南強調從更廣泛角度思考如何保護資源的存取，包括保護對設備、服務、身分等的存取，零信任不應只限於保護資料。

零信任架構的邏輯組件

ZTA 的邏輯架構分為兩個基本區塊：核心組件和資料源。核心組件在圖 11-1 中間的框框裡，透過控制平面和資料平面的組合來進行通訊。值得注意的是，這個模型有許多種轉換成實體基礎設施的方式，因此，這些組件可根據企業對基礎設施的需求而建置於地端、雲端或兩者兼有。

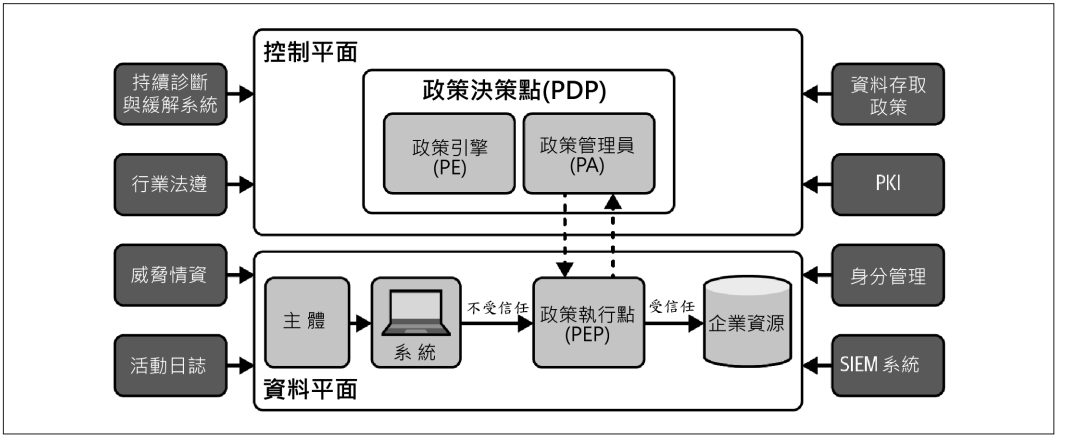

圖 11-1　ZTA 的邏輯組件