標　　題	**Adaptive Access Control「自適應存取控制」(註1)：如何在 AI(人工智慧)和 Zero Trust(零信任)(註2)時代中，引導網路安全**
類　　別	訊息新知 (May 2025)
內　　容	人工智慧（AI）正在重新定義企業實現網路安全的方式。傳統的存取控制機制依賴於靜態的、基於信任的模型，越來越不足以應對複雜的網路威脅。 解決方案是甚麼？由傳統管理邁向**「自適應存取控制」**(Adaptive Access Control)機制的轉變，這是一種基於 **Zero Trust(零信任)**原則的動態 AI 驅動型的安全方法。**AAC「自適應存取控制」**機制能即時評估上下文的所涵蓋的風險因子，確保只有合法的使用者，才能在適當的情況下獲得存取許可權。 本篇文章將探討 **AAC「自適應存取控制」**如何改變存取管理，為什麼傳統方法無法滿足要求，以及企業如何利用 AI 驅動的情境感知，來加強其網路安全態勢。 **什麼是「自適應存取控制」(AAC)？** **「自適應存取控制」(AAC)** 超越了”**靜態角色和預先定義規則**”，能持續地即時評估上下文的所涵蓋的風險因子，例如： ■**使用者行為**（例如，登錄模式、打字速度） ■**設備運行狀況**（例如，系統修補狀態、惡意軟體檢測） ■**地理位置**（例如，從可信賴的位置存取點與從公共 Wi-Fi 網路存取位置） ■**網路安全狀況**（例如，連接到安全的 VPN 網路） 通過 integrated AI(整合式人工智慧)和機器學習，**「自適應存取控制」(AAC)**可以檢測異常情況，動態調整安全策略，並確保僅在符合安全協定時，才授予存取許可權。這種適應性使得**「自適應存取控制」(AAC)**能成為在日益互聯的世界中，企業尋求增強網路安全的強大工具。 **為什麼傳統的存取控制模型無法滿足需求** 為何傳統存取控制模型，在目前環境的需求是不足夠的，是因為其基於角色的存取控制(Role-Based Access Control)和基於屬性的存取控制(Attribute-Based Access Control)等傳統存取控制模型，歷來僅提供結構化的安全框架，這些模型太依賴於靜態規則，這使得它們，在應對現代網路動態威脅方面缺乏靈活性。攻擊者經常利用被盜的憑證或受損的端點的這些弱點，能順利進入系統。 例如，如果醫療保健專業人員的憑證被盜，傳統模型可能僅僅因為憑證與預定義的角色配對符合，就允許其能夠存取敏感的病患數據。相較之下，**「自適應存取控制」(AAC)**會檢測異常情況（例如:來自不熟悉的位置，或設備的存取的嘗試），並實施額外的驗證措施或完全拒絕存取。 **情境感知在存取控制中的作用** **「自適應存取控制」(AAC)** 的核心是情境感知的監測 – 評估圍繞存取嘗試的情境因素的能力，包括基於人類和機器的因素。

想像一下，醫院員工從他們日常使用的工作站登錄內部系統。此預期行為將導致最低的身份驗證要求。但是，如果同一名員工嘗試從另外一個城市的公共 Wi-Fi 網路登錄，AAC 會將其標記為異常，並強制執行其他安全措施，例如生物識別身份驗證，或多重因子身份驗證 Multi-Factor Authentication (MFA)。
根據其風險狀況制定**「自適應存取控制」(AAC)** 策略，企業可以最大限度地減少合法使用者的摩擦，同時增強高風險場景中的安全性。

AI 驅動的情境感知的關鍵要素

有效的**「自適應存取控制」(AAC)**實施，需要 AI 驅動的情境感知，和即時分析靜態和動態的信號：

■**靜態信號**：提供安全管理基礎資料的固定元素，例如：
- ❍用戶的憑證
- ❍經核准的設備
- ❍應用程式的許可權

■**動態信號**：AI 分析的即時資料，包括：
- ❍行為模式和異常資料
- ❍地理位置跟蹤
- ❍網路運行狀況和威脅情報
- ❍設備安全狀況
- ❍存取請求的頻率和時間

通過利用 AI，企業***可以主動識別風險***，並根據全面的威脅評估做出明智的安全決策。

AAC「自適應存取控制」的核心優勢

1.靈活性：AAC 根據不斷變化的用戶行為、網路狀況和設備運行狀況動態調整安全策略。

2.智慧決策：AI 驅動能即時分析評估上下文風險因子，確保安全決策與業務目標保持一致。

3.增強的用戶體驗：「AAC 自適應策略」可減少對合法使用者的干擾，同時阻止未經授權的嘗試。

4.可擴展性：AI 支援跨混合環境、雲應用程式和遠端員工進行無縫的安全存取。

5.法規合規性：AI 產生的日誌和分析，可以增強透明度和可稽核性，支援和遵循監管標準。

零信任(Zero Trust)安全中的 AI 增強型 AAC

零信任框架遵循**“從不信任，全部驗證”**的原則。每個存取請求，都必須經過上下文的即時分析，以驗證其合法性。AI 是這種方法的關鍵，它使用演算法來評估風險參數、檢測異常並動態調整存取策略。
例如，如果員工試圖從不安全的設備存取敏感資料庫，AI 增強的**「自適應存取控制」(AAC)**會將該嘗試標記為高風險，並強制執行額外的身份驗證或完全拒絕存取。

克服建置的挑戰

雖然 AI 增強的**「自適應存取控制」(AAC)** 提供了巨大的優勢，但由於策略配置和資源需求，實施可能很複雜。企業可以通過以下方式緩解這些挑戰：

■**逐步推出**：優先考慮高風險領域並逐步擴展 AAC
■**自動化**：利用 AI 簡化決策並減少人工干預
■**持續學習**：使用最新的威脅情報和行為資料更新 AI 模型

AI 和零信任(Zero Trust)在存取控制中的未來

隨著 AI 的不斷發展，「**自適應存取控制**」(AAC) 將演變成一種更具預測性和主動性的安全機制。機器學習、行為分析和威脅情報方面的未來創新將進一步建置完善存取系統，使得企業從被動防禦，轉變為先發制人的安全措施。

在這種未來環境中，每個存取請求，都將以無與倫比的精度和效率進行審查，確保只有合法使用者才能在適當的條件下獲得存取許可權。

更好、更具適應性的網路戰略

「**自適應存取控制**」AAC 代表了網路安全的重大進步，提供了一種動態、智慧和彈性的存取管理方法。通過利用 AI 驅動的情境洞察，企業可以增強對現代網路威脅的防禦，同時保持強大的安全態勢。

隨著 **AI 和零信任(Zero Trust)**方法的不斷發展，AAC 仍將是**自適應網路安全戰略**的基礎組成重要部份。

備註 1：

自適應存取管理:根據使用者存取系統時，當下評估的風險以調整存取安全等級。雖然成熟的存取管理基礎設施可以透過身份驗證和授權安全性提供服務，但自適應存取管理，會調整這些保護措施以適應當前的風險。這些調整風險的決策標準，評估包括上下文訊息、使用者是否正在存取高度敏感的資訊、使用已知設備、使用前所未有的設備、在安全設施範圍內、從指定範圍或區域內的遠端位置、來自遙遠或未知的遠端（IP 位址範圍、地理位置等）。

備註 2：

零信任的定義:零信任是一種雲端安全性模型，藉由移除隱含的信任，並強制實行嚴格的身分驗證和授權機制，來保護現代企業。在零信任機制下，不論使用者是屬於企業網路內部或外部，一律將所有使用者、裝置和元件視為不受信任。

更多詳細的內容，可以參考底下的連結:
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/adaptive-access-control-navigating-cybersecurity-in-the-era-of-ai-and-zero-trust