第五章

結論

在無線網路與行動網路佈建環境完整與互補的今日，無線行動上網已成為全球科技發展一大重要方向。不論是固定接線式的上網方式或是其他單一上網方式早已不滿足行動用戶對於資訊移動性之需求。而外在無線應用環境之成熟，使得大小型企業紛紛投入公司M化之導入。移動式的工作環境伴隨著M化的工作模式，企業相信透過自由與彈性的商務行動應用能夠降低資產成本，提升公司競爭優勢。

行動工作者透過整合式的上網服務，可以在任何時間與地點即時地取得資訊，進行遠端存取資料。無線行動網路雖然延伸現有網路之連結規模，但卻也因為網路環境之特性暴露更多安全性漏洞。因此要如何在這動態的環境下，針對這些衝擊與威脅提出一個具有高度擴充性、彈性並滿足複雜安全性需求之無線網路解決方案，便成為企業所迫切關心的議題。

5.1 結論

本研究首先設計一個整合在AAA架構下的情境感知授權系統雛型，提出利用情境感知之機制來增進無線網路安全。結合情境的概念定義屬於安全授權系統中『行動用戶、資源服務、虛擬網路位址』等面向的安全性情境資訊，藉以描述一個動態的網路環境，並用來驅動不同授權評估決策，調整系統安全設定。另外透過跨網域環境中的情

境偵測服務(CDS)、情境處理器(CH)與AAA伺服器之間相互合作，將所偵測到的情境參考存取控制政策來推論資源授權之決策。因此不同的行動用戶、目標動作或資源的屬性或環境使用上的差異，會產生不同的授權範圍與連線設定。

然而行動工作者的工作環境並不會只侷限在特定的地方，他們可以根據所處地點的現況彈性地選擇網路形態與連線方式；同樣地，遠端的資源也會隨著時間的變化改變資源使用狀態，因此情境資訊會持續地發生改變。本研究所設計的授權系統，因為具備情境感知的能力，當連線對話中的情境改變時，系統便能夠自發性地針對這些改變來調整安全設定以適應新的環境型態。

為了要使本研究所設計的授權系統能夠動態的根據週遭環境與使用者情境來執行授予或拒絕資源存取權，我們透過一個以情境為定義設計原則的情境感知存取控制政策來加強系統彈性授權的能力。首先參考遠端存取規則與各種型態的無線行動網路環境來定義一個具有階層關係的存取控制政策之情境模型。管理人員能夠以此模型來設計資源的授權政策，根據使用者的角色、目標資源與動作與當時的網路環境等來決定不同安全等級的授權範圍。以多樣化的情境資訊取代傳統帳號/密碼來做為驗證與授權決策之評估依據，因此在提供工作之移動性與靈活度的同時，亦能夠充分為企業建構安全的網路存取環境。

此外，本研究選擇以Web Ontology Language(OWL)的方式來表達系統的存取控制政策。希望藉由OWL豐富的類別與屬性關係以滿足在情境塑模(modeling)上建立一個完整的政策模型；透過標準的表達方式，使得安全性情境資訊能在分散式的網路環境下被分享(sharing)與溝通(communication)；最後則利用OWL本身的推論規則來達到推論(reasoning)上的需求，以推論出適當的網路資源存取決策。

5.2 研究貢獻

Mostéfaoui and Brézillon (2003) 於"A Generic Framework for Context-Based Distributed Authorizations" 中，提出情境導向安全政策的概念，藉此能根據動態環境中所蒐集到的資訊來調整系統安全政策；並設計一個概念性的架構作為情境導向安全系統之基礎。而本研究則以此概念為基礎，將授權系統延伸至跨網域AAA 架構下。用來解決在無線網路環境下有關漫遊、遠端存取等安全問題。另外根據系統目的與整體執行環境定義所需要的安全性情境資訊，包括AAA 伺服器所支援的屬性、行動用戶個人資訊、存取資源狀態與目前網路環境等。希望透過一個較結構化的分類方式，將安全性情境資訊作有效的整理與分類，並有利於日後情境之管理與擴充。

至於存取控制政策的表達上，無論是以XML 語言或是利用情境關聯圖 (contextual graph) (Mostéfaoui and Brézillon, 2004; Mostefaoui et al., 2004) 中所產生的路徑來表達，都是較靜態且固定形式的。管理人員必須考量到各種可能的存取行為來設計不同的存取控制政策。但是網路環境之複雜與多變的特性，若是要完整地定義所有的存取控制政策是很困難的。正因如此，本研究採用 ontology 的概念，將存取控制中的組成元件描述成各個類別 (class)，並定義不同屬性 (property) 使得類別之間產生複雜的關連。因此利用元件之間的階層或屬性上的關係及 ontology 之推論能力，以簡化存取控制政策的定義與描述。

另外本研究又延伸XACML 中對於存取控制政策組成元件之定義。另外附加個人設定一類別於政策中，藉以滿足在AAA 架構中，遠端伺服器為了保障連線的品質、頻寬或加密行為，而在授權連線後對於特定行動用戶所執行的連線限制等。