十一、研究計畫中英文摘要：請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

（一）計畫中文摘要。（五百字以內）

總計畫：支援在企業雲環境BYOD 應用之資訊安全技術研發

隨著雲端服務與行動終端設備日漸普及，企業員工自帶設備的趨勢逐漸成形。在這樣的趨勢下，行動終端設備的資料安全議題已成為大多數企業需要面臨的課題。因此，符合企業需求之行動終端管理方案需求日益漸增。然而，目前的Mobile Application Management 作法都針對單一應用程式進行權限控管，此方法容易藉由Collude Issue 產生安全的漏洞。此外，目前行動終端設備使用者身分認證仍以

帳號密碼為主，易有肩窺等密碼被盜取之疑慮。為此，本研究計畫案將研究內容分為三大區塊；首先，子計畫一將提供結合靜態與動態分析的應用程式安全檢測機制及提出Data Centric-Information Flow Control 機制防止Collude Issue 的解決方案。其次，子計畫二將針對行動終端設備的使用者身分認證機制相關研究分析，提出以行為特徵為基礎之使用者認證技術輔以現有的認證技術。此外，子計畫二的使用者身分認證機制將整合至子計畫一，建構一個整合應用程式管理與身分認證管理之行動終端設備管理平台，讓行動終端管理機制更便利與安全，以達到支援企業雲環境BYOD 應用之資訊安全目標。最後，因應企業大多數的應用服務(如ERP)都建置在企業雲上，為了讓雲端平台上的應用服務穩定不中斷及支援本研究計畫之行動終端設備管理平台，子計畫三將提出高可用性服務技術確保企業雲端服務的可用性。

關鍵字：企業雲；自帶設備；使用者認證；行動終端設備管理；高可用性服務

子計畫二: 以行為特徵為基礎之可適應多重操作姿勢的行動裝置使用者認證技術研發

網際網路與資訊技術的迅速成長，促使行動裝置(例如：智慧型手機)成為存取各種數位資訊的重要裝置。因此，行動裝置存取資訊的安全性，成為產官學界矚目的研究焦點。根據提案團隊的觀察，目前於行動裝置或資訊服務平台的使用者認證機制，仍然是以數字、文字或圖行密碼進行存取控制；然而，此類型的安控模式一直存在著密碼容易被忘記或被盜用的問題，進而讓使用者對以行動裝置進行資訊存取的安全性產生疑慮。根據提案團隊於近年來的研究，除發現使用者會採用獨特習慣方式操作與持握行動裝置外，亦發現行動裝置內建之方位與觸控螢幕感測器可用來擷取這些行為特徵；此外，本團隊亦發現，不同的靜態操作姿勢(例如:站姿與坐姿)會對使用者的行為特徵模式造成影響，進而降低安全機制的識別能力。因此，研究團隊預計於為期二年之計畫執行期間，利用智慧型手機內建之方位與觸控螢幕感測器，研發一系列可處理多重靜態操作姿勢的非侵入式使用者識別機制。此外，團隊會將研發成果實作一「行動魔鎖」雛型，其功能可應用於自攜裝置(Bring Your Own Device, BYOD)或資訊系統上，透過整合密碼與「行動魔鎖」的使用者認證，建構一個雙因子或多因子認證機制以提升系統安全性。

關鍵字：行動裝置；行為特徵；非侵入式認證機制; 多因子認證；多重操作姿勢