計畫名稱：雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究(總計畫暨子計畫四)

執行單位：成功大學/電機工程學系暨電腦與通信工程研究所
主持人：楊竹星教授

計畫編號：MOST 103-2221-E-006-145-MY3

一、摘要

雲端運算環境日漸成熟，為傳統資訊基礎建設帶來革命性的改變，然而在新的環境 架構及科技的應用下，我們亦面臨著與以往全然不同之網路與資訊安全之威脅。本整合型計畫將以利用以虛擬機器為基礎之測試平台，研發雲端平台上多層次防禦機制，與多元化攻擊之偵測技術。透過子計畫間之分工合作，建立網路與雲端系統多層次防禦機制，可作為防禦網路與雲端攻擊之防線，提供高安全度的網路環境。

子計畫四的主要目的是要在雲端環境之下建立一套可靠的網路流量監控系統，透過建置於虛擬機器管理平台中的流量辨識模組截取網路環境的封包，產生Netflow資訊，並結合深層封包探測技術(DPI, Deep Packet Inspection)與網路攻擊之時間與空間概念之多層次分析，進行協同防禦，可捕抓於系統中之潛藏攻擊者及未知受害者。

關鍵字：雲端運算，目標性攻擊，關聯分析，多層次防禦，。

三、技術特色

總計畫在本計畫中角色為一資料共享之平台，以建構多層次防禦機制為基礎，發展雲端網路活動日誌收集分析、異常雲端網路流量特徵分析、智慧型僵屍網路偵測、以及多階段目標攻擊之偵測與預測，進而建構多層次關聯分析雲端攻擊之防禦系統。

子計畫四利用Netflow格式的原始資料做統計和分類，歸納出特徵以辨別惡意行為及嫌疑行為。惡意行為將會直接進行阻擋動作，針對嫌疑行為，則會進行時間(分散流量)及空間(攻擊手法)上之偵測。

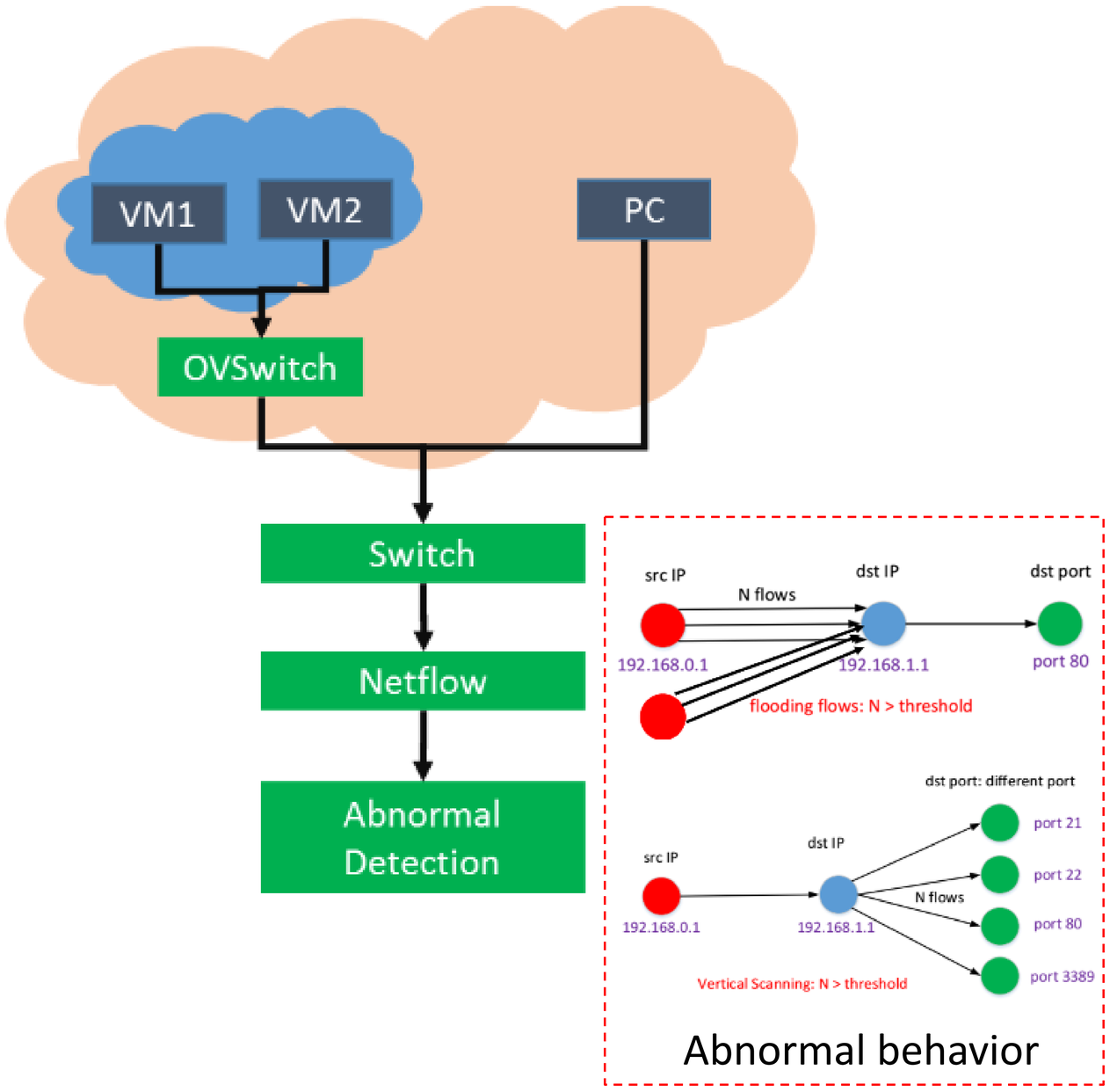
四、技術應用範圍

雲端運算被視為目前最火紅、高成長的產業，針對雲端平台使用者除其可靠度外，最重視即為其安全性。本研究將能提升重要營運中心之資安事件預警能力，舉凡資訊安全服務商、雲端服務供應商研究成果可應用於資訊安全相關產業，包含防毒程式廠商、資訊安全設備研發廠商等。供學術單位管理及分析流量，亦可部屬在國家或私人企業，供其管控資訊進出。

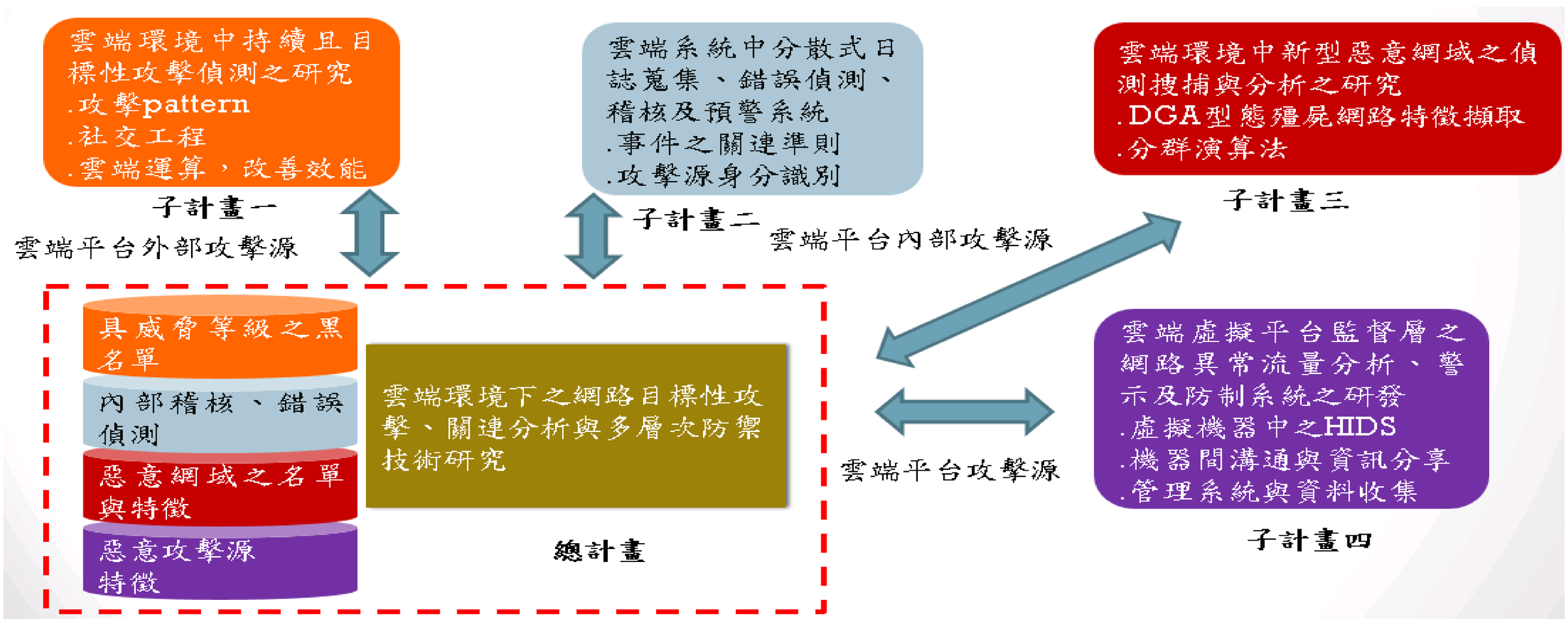
二、架構功能

總計畫之主要功能為建立中央控管之雲端安全防護系統，包含針對雲端主機進行進階持續性滲透攻擊、內部日誌稽核、惡意網域及雲端流量監控等，系統架構如圖一所示。

子計畫四針對網路流量分別以封包和網路流(flow)為單位，進行巨觀和微觀的流量觀察，來達到惡意行為之偵測，本年度除了偵測雲端網路外，針對架構雲端所處之網路環境亦可一併進行偵測。如圖二所示：



圖二、子計畫四系統架構



圖一、總計畫系統架構