國科會「雲端計算與資訊安全技術」研發專案補助申請要點

本會為配合行政院推動雲端運算及資訊安全產業發展，鼓勵學術界投入雲端及資安關鍵技術與創新應用研發，培育產業所需高階科技人才，並促進台灣學術界與國內外產學研機構合作研發，特規劃本研發專案補助辦法，鼓勵學術界積極提案申請。

壹、 專案補助範圍說明

本專案徵件範圍涵蓋二個分項：

一、「雲端計算及雲端資安技術研發」分項：補助範圍為雲端計算、雲端資安或結合二者之學術研究計畫（詳細說明請參考第貳項說明）。

二、「資訊安全技術研發」分項：凡非屬前項「雲端計算及雲端資安技術」補助範圍而與資通安全有關之學術研究計畫請申請本分項補助（詳細說明請參考第貳項說明）。

相關細項說明，請參閱國科會工程處網站(http://www.nsc.gov.tw/eng/)-最新消息，或資訊學門網站(http://cs.nsc.ncku.edu.tw/news/)-國科會「雲端計算與資訊安全技術」研發專案補助辦法。

計畫申請作業，請依國科會補助專題研究計畫辦法，研提正式計畫申請書(採線上申請，並請於計畫名稱後括弧備註申請之分項)，申請類別：一般型研究計畫。計畫歸屬請點選「工程處」、學門代碼名稱請點選「E08 資訊」，以利作業。並由計畫主持人所任職之機構於 ***99 年 12 月 20 日***前函送國科會申請（請彙整造冊後專案函送）逾期恕不受理。

貳、 「雲端計算及雲端資安技術研發」/「資訊安全技術研發」分項說明

一、 專案要點（請填具附件 1A：參與相關活動承諾書及附件 1B：申請計畫契合優先補助原則檢核表，並附於申請書中繳交）

(一).本專案優先補助多年期整合型研究計畫（有研究中心運作機制者尤佳，並請於申請書中載明研究中心名稱、組織架構及運作機制、研究方向、參與團隊、學校資源投入情形）。優質計畫將採預核方式通過多年期計畫，惟每年皆須通過成果審查，必要時將中止下年度計畫之補助。本案亦鼓勵由 45 歲（含）以下青年學者擔任整合型研究總主持人之計畫，以培養新生代學術領導團隊。

(二).本專案重視研發成果之價值創造潛力，優先補助具有明確之合作研發企業或法人機構，且有具體成果應用規劃之計畫（合作研發可以為學產或學產研合作模式；除了計畫書內容具體說明研究標的與產業需求的關聯外，應填寫合作研發企業或法人機構合作意願書（附件 2A）。無具體合作對象或由大學本身主導成果運用者請填寫成果運用規劃表（附件 2B））。

(三).本專案鼓勵具國際合作研究關係之計畫（請於申請書中載明合作對象、合作研究內容、合作模式、智財分享模式、合作對象資源投入情形、成果導入應用規劃等，並提出國外合作研究機構明確表達合作意願之佐證）。

(四).為提昇研發品質，本專案優先補助執行過程採用具體計畫流程管理及系統品質管理規範之計畫。本專案亦規定受補助計畫須繳交需求規格分析報告書及系統測試報告書兩文件，且應到中央研究院自由軟體鑄造場網路平台開啓專案計畫，及運用相關專案管理工具記錄研發歷程。

(五).本專案重視研發成果之開放性及分享交流，將優先補助願意依自由軟體授權精神公開原始碼，可跨校、跨組織整合運用現有雲端或資安運算資源及研究成果，或長期開放其研究成果提供服務之計畫。

(六).本專案重視研發成果之創新性及應用效益，計畫申請審查及成果審查時，將落實下列績效指標之評估，並做為國科會後續計畫核定之重要依據（以當年計畫成果或本專案補助之前期計畫成果為基準）：

1. 專利、技轉及產學合作等價值創作成效。
2. 優質期刊及國際會議論文之發表情形。
3. 產出之開放軟體元件被下載率及評價。

(七).本專案依據推動目標決定計畫錄取標準，受補助計畫納入每位主持人之國科會計畫件數計算。

(八).附件 3A/B 所列為本專案重點推動之研發主題，附件 4A/B 為法人機構推薦之研究主題，有興趣之主持人可先與其聯絡。

(九).受補助計畫主持人及執行團隊有參加推動辦公室所舉辦之說明會、

研討會、審查會及成果發表會之義務。

二、 推動時程及申請資格

(一).重要時程

1. 計畫書收件截止日：***99 年 12 月 20 日***。
2. 計畫開始執行日：***100 年 8 月 1 日***。

(二).申請資格：所有大專校院教師，且符合國科會專案研究計畫主持人資格者，皆可提出申請。

(三).計畫書格式

1. 計畫書：同國科會專題研究計畫申請書格式。
2. 應填寫附件：附件 1A/1B、附件 2A/2B，其中附件 1A/1B 為必備之附件，不得缺漏。

(四).執行規範

1. 本專案計畫主持人及參與研究人員必須參加本專案所舉辦之相關活動。各計畫開始執行後至 Open Foundry 專案平台開啓專案計畫。
2. 繳交各階段報告書（請依據推動小組規定之格式及規範撰寫），共包含：

a. 系統分析與流程規劃階段：繳交專案執行與系統需求規格書。

b. 系統測試階段：繳交系統測試報告書。

c. 驗收與結案階段：繳交成果報告書至國科會(依國科會格式)。

詳細作業流程將另行公告,並擇期舉辦說明會向研究計畫之主持人說明。

(五).成果評估：

1. 國科會將於每年計畫執行期間分二階段邀請執行團隊報告相關進度，並聘請學者專家擔任審查委員，提供專業建議。
2. 研究計畫結案時將由推動小組以現場展示及詢問方式評估各計畫執行成果，並向國科會報告（計畫成果報告主要審查項目包括：需求規格完成度、成果可應用性、技術方案優越性、測試完整性、各期報告完整性) 。
3. 本案各研究計畫之執行成效將送交國科會，做為以後核定國科會各類計畫

(附件1A)

承諾書

本人承諾針對所主持「雲端運算及資訊安全技術」專案之研究計畫，願意依照推動辦公室所規定之作業流程執行計畫(包含參與活動、繳交報告書等)，詳細內容如下：

日 期	進行事項	附 註
2011/8	計畫主持人座談會	計畫主持人參加
2011/9~10	「Light-Weight CMMI」研討會	計畫主持人及所有參與計畫學生都需參加 (若已參加以前年度課程者，本年度得免參加；不曾上過課者皆須參與)
2011/9~10	開放軟體鑄造場Open Foundry專案開發平台暨開放軟體授權說明會	
2011/9~2012/7	計畫執行過程，請使用開放軟體鑄造場所提供 SVN 系統進行專案管理	專案管理紀錄列為執行成效之一
2011/12	繳交專案執行規劃與系統需求規格書	依據推動小組規定之格式及規範撰寫
2012/1	期中查訪	所有群體計畫皆需報告，個別型計畫則不用
2012/6	繳交系統測試報告書	依據推動小組規定之格式及規範撰寫
2012/7	上傳計畫成果原始碼 (在計畫書承諾者需執行)	七月底前上傳至自由軟體鑄造廠
2012/7	繳交系統安裝使用手冊 (在計畫書承諾者需執行)	七月底前上傳至自由軟體鑄造廠
2012/8	「計畫成果發表會」	現場展示與報告、評審委員進行評選
2012/8~2012/10	上傳計畫成果報告書至國科會	依國科會規定上傳計畫成果報告書

立同意書人簽名: _____

中華民國　　年　　月　　日

(附件 1B) 申請計畫契合「雲端運算及資訊安全技術」專案優先補助原則檢核表

□申請計畫屬「雲端計算及雲端資安技術」範疇：請填寫下表查核項目 1-11。

□申請計畫屬「資訊安全技術」範疇：請填寫下表查核項目 2-11。

序號 查核項目 是■/否□ 說明（填■者須作答）

序號	查核項目	是■/否□	說明（填■者須作答）
1	是否符合雲端計算及雲端資安專案重點研究主題?	□	重點推動研究主題項目：
2	是否有國內合作企業?	□	國內企業名稱：
3	是否與國內企業及法人機構形成研發聯盟?	□	國內企業名稱： 國內法人名稱：
4	是否有國外合作對象?	□	國外機構名稱：
5	是否與國外機構、企業或法人機構形成研發聯盟?	□	國外機構名稱： 國外企業名稱： 國外法人名稱：
6	是否運用國內學界或政府單位現有雲端設備環境？	□	設備提供單位：
7	計畫執行是否採行計畫流程及系統品質管理規範?	□	採行之規範或標準名稱：
8	是否願意依自由軟體授權精神公開原始碼?	□	預期公開之自由軟體名稱 1. 2.
9	是否為整合型計畫?	□	子計畫件數： 總經費： 參與校數：
10	是否由 45 歲（含）以下青年學者擔任整合型研究總主持人？	□	總主持人： 年齡： 資歷：
11	是否具有研究中心運作機制?	□	研究中心名稱： 學校資源投入情形： 參與學者數量： 中心主持人：
12	是否有具體成果運用及價值創造構想?	□	成果運用及價值創造方式： 參與機構或企業： 預定期程：

附件 2A 合作研發企業或法人機構合作意願書

企業／機構名稱及地址：	
成立時間：	
員工人數及研發人員數：	
主要產品或業務：	
公司資本額：	
雙方合作方式及擬投入之資源：	
雙方合作內容及預期產出之規格：	
成果運用及價值創造方式：	
成果運用預定期程：	
企業／機構及負責人用印：	

附件 2B 成果運用規劃表

預定場域或導入機構	
成果運用內容	
成果運用對象	
成果運用期程	
價值創造模式及途徑	
導入機構投入資源規劃	
成果運用機構用印	

(附件 3A) 「雲端計算與雲端安全技術」重點推動研發主題

一、 雲端計算與應用安全關鍵技術

1. privacy protection
2. IaaS security:
   a. 虛擬機的獨立性(virtual machine independency)
   b. 檔案遺失防護，確保檔案資料在儲存系統上的可得性
   c. 資料保密：透過 block level 的資料切割技術分散儲存不同的區塊，讓惡意人士無法取得完整的資料
3. PaaS security:
   a. 雲端服務平台安全管理：雲端系統弱點診測監控、雲端服務平台資安事件分析、防毒等
   b. 身分與權限管理： AAA (Authentication, Authorization & Accounting)
   c. 終端裝置安全管理
4. SaaS security:
   a. 雲端應用層安全防禦：高效能 Web App 封包（XML, RIA）深層過濾、Web DB 存取行為監控、Behavior based 惡意軟體閘道偵測
   b. 身分與權限管理： AAA (Authentication, Authorization & Accounting)
   c. data integrity and protection
   d.雲端 SaaS 服務內容安全防護技術
5. 分散式雲架構之 CIA (Confidentiality, Integrity, Availability) 控管
6. 多雲之間的資安管理架構與 AAA 控管
7. Cross-layer security solutions

二、 雲端計算關鍵技術 (for container computer, elastic service device, open cloud OS and middleware)

1. 雲端計算平台技術
   a. virtualization
   b. service flow and workflow orchestration
   c. programming model
   d. world-wide distributed storage system
   e. dynamic resource management and provisioning
   f. energy-efficient infrastructure and platform
   g. availability and reliability
   h. data management
   i. cloud interoperability
   j. 平台資源整合（學術雲／大學雲）
   k. 虛擬系統惡意軟體萃析技術
   l. 雲端資料安全防護技術
2. 雲端計算服務技術
   a. web service and SOA
   b. web 2.0 and mashup
   c. privacy and trustworthiness management
   d. service quality guarantee
   e. universal access for heterogeneous client devices
   f. virtual enterprises and organizations

三、 雲端計算創新應用：本專案不限定特定應用領域，但所提計畫應能展現下列特性：

1. 能突顯有別於傳統的 IaaS, PaaS 或 SaaS 模式之價值
2. 具有驗證雲端計算關鍵技術或創新營運模式能否達成有效用戶規模需求的性質，並有具體驗證規劃者
3. 具有下列創新服務模式性質之一：
   a.展現企業內或跨企業流程改造或創新效益
   b.展現政府服務改造或創新效益
   c.展現電子商務市集流程改造或創新效益
   d.展現公共服務（如防災、環保、綠能等）流程改造或創新效益
   e.展現教育服務流程改造或創新效益
   f.展現促進創業育成效益（如數位內容、互動多媒體、社群網路服務等）
4. 具有應用技術或服務科學研發內涵

(附件 3B)資訊安全技術重點推動研發主題

1. 系統及應用程式安全
   A. 安全程式發展模式
   B. web 應用安全防護
   C. 程式行為追蹤控制
   D. 沙箱系統
   E. 系統異常行為塑模技術
   F. 密碼學與密碼協定設計
2. 安全測試
   A. 測試平台加值應用
   B. 網路即時攻擊資料收集與評估
   C.0-day 攻擊偵測與防護
3. 惡意軟體安全
   A. 殭屍網路偵測與防堵
   B. 惡意程式偵測與防禦
   C. 跨站腳本攻擊偵測與防禦
4. 數位鑑識
5. 行動資安與終端安全
   A.認證裝置防護
   B.小額付款及線上交易安全機制
   C. 終端裝置安全防護
6. 隱私保護
   A.個人資料運用控管及探勘整合防護
   B.企業資料過濾
   C.雲端運算之資料及運算保密
7.軟硬體及異質平台整合
   A. 跨平台分散式運算於資安偵測之應用
   B. 多核心處理器、繪圖處理器及嵌入式系統於資安偵測之應用

(附件 4)法人研究建議主題

A. 資策會

研究主題	內容簡要說明
1. 雲端資料安全防護技術	研究雲端虛擬環境中的資料安全防護機制，如資料運算(data in use)、資料儲存(data at rest)及資料傳遞(data-in-transit)等相關的解決方案。
2. 虛擬系統安全技術	發展虛擬系統安全技術，如：Hypervisor 安全監控、虛擬系統弱點診測及虛擬系統安全防護等技術。
3. Web 應用服務安全技術	分析 Web 服務存取行為之關聯，藉由如：Cookies 及 History 反查等資訊，解析惡意網站內容之行為狀態，協助應用內容解構技術之發展。
4. 雲端 SaaS 服務安全防護技術	研究 SaaS 服務資訊內容交換過程中之內容機敏資訊保護機制及管理機制，並進行可能的威脅攻擊研究。
5. 靜態數位鑑識分析技術	藉由記憶體、硬碟與系統日誌等主機或其它輔助資訊，自動化關聯分析出可能的受駭情境 (Attack Scenario)。
6. 動態數位鑑識分析技術	觸發軟體執行後，分析其系統呼叫(System Call)和系統行為（檔案操作、機碼值操作、網路連線），以辨識未知軟體是否屬於已知的惡意軟體類型甚或是新的變種。

聯絡人：林志鴻 組長
e-mail：chlin@iii.org.tw
連絡電話：(02) 66000100 #711

B. 工研院

B1: 「雲端計算_安全技術」重點推動研發主題

一、 雲端計算與應用安全關鍵技術

1. privacy protection。
2. IaaS security:
   a. 虛擬機的獨立性(virtual machine independency)。
   b. 檔案遺失防護，確保檔案資料在儲存系統上的可得性。
   c. 資料保密：透過 block level 的資料切割技術分散儲存不同的區塊，讓惡意人士無法取得完整的資料。
3. PaaS security:
   a. 雲端服務平台安全管理：雲端系統弱點診測監控、雲端服務平台資安事件分析、防毒等。
   b. 身分與權限管理： AAA (Authentication, Authorization & Accounting)。
   c. 終端裝置安全管理。
4. SaaS security:
   a. 雲端應用層安全防禦：高效能 Web App 封包（XML, RIA）深層過濾、Web DB 存取行為監控、Behavior based 惡意軟體閘道偵測。
   b. 身分與權限管理： AAA (Authentication, Authorization & Accounting)。
   c. data integrity and protection。
   d. 2. 雲端 SaaS 服務內容安全防護技術
   e. static/dynamic code analysis for web applications
5. 分散式雲架構之 CIA (Confidentiality, Integrity, Availability) 控管。
6. 多雲之間的資安管理架構與 AAA 控管。
7. Cross-layer security solutions。

二、 雲端計算關鍵技術 (for container computer, elastic service device, open cloud OS and middleware)

1. 雲端計算平台技術
   a. virtualization
   b. service flow and workflow orchestration
   c. programming model
   d. world-wide distributed storage system
   e. dynamic resource management and provisioning
   f. energy-efficient infrastructure and platform
   g. availability and reliability
   h. data management
   i. cloud interoperability
   j. 平台資源整合(學術雲／大學雲)
   k. 虛擬系統惡意軟體萃析技術
   l. 雲端資料安全防護技術
2. 雲端計算服務技術
   a. web service and SOA
   b. web 2.0 and mashup
   c. privacy and trustworthiness management
   d. service quality guarantee
   e. universal access for heterogeneous client devices
   f. virtual enterprises and organizations
   g.high performance computation environment for security analysis and

cryptography

3. 大型資料中心網路架構與安全技術
   a. virtual layer2 network for data-center
   b. network packet analysis over large scale layer 2 network
   c. large scale network flow monitoring
   d. availability for large scale virtual scale layer 2 network

三、 雲端計算創新應用：本專案不限定特定應用領域，但所提計畫應能展現下列特性：

1. 能突顯有別於傳統的 IaaS, PaaS 或 SaaS 模式之價值。
2. 具有驗證雲端計算關鍵技術或創新營運模式能否達成有效用戶規模需求的性質，並有具體驗證規劃者。
3. 具有下列創新服務模式性質之一：
   a.展現企業內或跨企業流程改造或創新效益。
   b.展現政府服務改造或創新效益。
   c.展現電子商務市集流程改造或創新效益。
   d.展現公共服務（如防災、環保、綠能等）流程改造或創新效益。
   e.展現教育服務流程改造或創新效益。
   f.展現促進創業育成效益（如數位內容、互動多媒體、社群網路服務等）。
4. 具有應用技術或服務科學研發內涵。

B2: 資訊安全技術重點推動研發主題

1. 系統及應用程式安全
   A. 安全程式發展模式
   B. web 應用安全防護
   C. 程式行為追蹤控制
   D. 沙箱系統
   E. 系統異常行為塑模技術
2. 安全測試
   A. 測試平台加值應用
   B. 網路即時攻擊資料收集與評估
   C.0-day 攻擊偵測與防護
3. 惡意軟體安全
   A. 殭屍網路偵測與防堵
   B. 惡意程式偵測與防禦
   C. 跨站腳本攻擊偵測與防禦
4. 數位鑑識
5. 行動資安與終端安全
   A.認證裝置防護
   B.小額付款及線上交易安全機制
   C. 終端裝置安全防護
6. 隱私保護
   A.個人資料運用控管及探勘整合防護
   B.企業資料過濾
   C.雲端運算之資料及運算保密
   D.社群網路隱私保護

7.軟硬體及異質平台整合

A. 跨平台分散式運算於資安偵測之應用

B. 多核心處理器、繪圖處理器及嵌入式系統於資安偵測之應用

8. Web 2.0 網路應用安全技術

A. Cross-site attack and prevention

B. XML poisoning

C. RSS/Atom injection

D.Mallicious script code analysis

E. RIA thick client (e.g., Flash, ActiveX, Applet,.....) binary manipulation

---

聯絡人：宋振華 經理

e-mail：chsong@itri.org.tw

連絡電話：03-5915745