Special Issue in Communications of the CCISA — Call For Paper

「資訊安全通訊雜誌」係由中華民國資訊安全學會發行，並定期於每年一月、四月、七月及十月出版與資訊安全相關領域有關之研究論著，每一期將邀請 Guest Editor 針對當期主題進行規劃與邀稿，且為了讓更多的研究者、同好共同開創資訊安全領域研究的天地，將在每一期中刊載下一期 Guest Editor 之規劃主題與論文徵稿方向，供研究者共襄盛舉，以豐富資訊安全研究之園地。

2016年度一月份主題為「新型態網路服務應用的安全防護機制(Security Mechanisms for Innovative Network Services)」。近年來，隨著通訊技術的演進，許多不同於以往環境的新型態網路應用架構紛紛被制定出來以符合新時代服務應用發展的需求，且雲端運算(Cloud Computing)與物聯網(Internet of Things)概念的出現更引領了一波創新服務應用的熱潮。然而，在使用者享受著創新服務所帶來的便利性的同時，其系統安全與個人隱私防護也面臨著新型態網路應用架構所帶來的潛在風險，例如傳統密碼學機制就不完全適用於如物聯網架構下的新型態輕量化感測元件，在無法使用具備足夠安全性的密碼學機制此一前提下，如何避免物聯網服務應用遭受惡意攻擊便成為了新一代物聯網架構下的一個新的研究主軸。由此可知，如何設計出一套適用於新型態網路服務應用架構的安全防護機制將成為未來數年內學研界的研究發展趨勢之一。

資訊安全通訊雜誌的本期主題將聚焦在新型態網路服務應用的安全防護機制，舉凡如系統檢測與分析等安全驗證機制開發，乃至於可完整維護服務應用安全的防護理論、架構、方法、工具等，皆可成為本期資訊安全通訊想要探討的議題。

以下僅列舉部分的相關主題，但徵稿論文不受此限：

＊新型態網路服務應用的系統安全設計
＊新型態網路服務應用的個人隱私防護機制
＊新型態網路服務應用的安全通訊機制
＊新型態網路服務應用的網路檢測工具
＊新型態網路服務應用的信賴運算架構設計

投稿須知：

1. 對於論文主題有任何問題，請以 E-mail 聯絡 Guest Editor。
2. 論文請不要有智慧財產與一稿多投之爭議，刊登論文之文責由作者自負。
3. 本刊物只接受電子檔投稿，稿件需以 Microsoft Word 編輯，字體為 12 點標楷體(中文)或 times (英文)，總頁數在 20 頁以內，並請參閱資安通訊雜誌論文格式 http://140.127.40.50/download/isc2.doc
4. 投稿稿件請將含作者服務單位、聯絡地址、電話、傳真、email 信箱等之基資料及投稿論文(論文內請勿含基本資料)email 至 Guest Editor 及本期刊編輯部。

重要日期：

論文投稿截止：104 年 12 月 10 日

論文接受通知：104 年 12 月 20 日

期刊發行日期：104 年 1 月

Guest Editor 聯絡方式

姓名：葉國暉

單位：國立東華大學資訊管理學系

地址：97401 花蓮縣壽豐鄉大學路二段一號

電子郵件：khyeh@mail.ndhu.edu.tw

本期刊編輯部聯絡方式

主編：王智弘 (wangch@mail.ncyu.edu.tw)

助理編輯：吳玉冰 (ccisa.editor@gmail.com)

CCISA: http://www.ccisa.org.tw/