<2015 臺灣資訊安全大會報名簡章>

一、會議日程

2015 年 4 月 1 日(三)至 4 月 2 日(四)

二、會議地點

台北國際會議中心（台北市信義路 5 段 1 號，會議室 101、102、103）

三、活動目的

臺灣資訊安全大會是由 iThome 企劃的大型資訊安全會議，旨在喚起臺灣各界對於資訊安全(資安)的重視，提倡全民資安時代的重要性，強化國家資訊安全政策、完備資安防護管理、培養資安技術能量、擴大資安人才培育及加強國際資安交流。

臺灣資訊安全大會將藉由大型會議的型式，集結臺灣資訊安全相關的產官學研等各界人士，共同探討臺灣最重要的資安課題、最新的資安趨勢與資安技術，期能廣泛探討資訊安全各個層面的議題，從而提升臺灣各界的資訊安全意識與整備度。

四、辦理單位

指導單位：行政院資通安全辦公室
主辦單位：iThome 電腦報周刊

五、大會主題

將探討臺灣當下及近程重要、熱門且急迫的資訊安全議題，並針對資安七大面向提供最齊全的專家建言與解決方案，搭建資安領域國際領導品牌，集結專家學者、法務人士、白帽駭客以及企業用戶等相關人員，一年一度擴大交流，創造學習的絕佳良機。

議程訴求：

- 強化國家資安政策，建立安全資安環境
- 完備資安防護管理，分享多元資安情報
- 奠基資安技術能量，整合科技實務應用
- 擴大資安人才培育，加強國際資安交流

七大議題主軸：

- IT 基礎建設安全
- APT 攻擊與防禦
- 法規遵循與資安治理
- 產業專屬議題
- 資料與隱私安全
- Web 與行動應用安全
- 雲端與虛擬化安全

六、議程

4月1日(三)					
08:00~09:00	報到				
09:00~09:10	開場致詞 (iThome 電腦報總編輯 / 吳其勳)				
09:10~09:30	大會主題演講 (行政院副院長兼國家資通安全會報召集人 / 張善政)				
09:30~10:10	打擊網路威脅：駭客攻擊現況大揭露 - 2014 駭客入侵之年 (FireEye 副總裁暨全球政府業務部門技術長 / Tony Cole)				
10:10~10:50	結合巨量資料分析的次世代資安雲端服務 (中華電信數據通信分公司 資通安全處負責人 / 謝東明)				
10:50~11:00	中場休息				
11:00~11:40	企業防洩密，雲端控管不可少 (精品科技 資訊安全顧問兼資安部經理 / 陳伯榆)				
11:40~12:20	決戰 APT 實例：駭客最怕你用的必殺技 TPS (台灣威瑞特系統總經理 / 吳明蔚 博士)				
12:20~13:30	中場休息				
Tracks	**Track A** **IT 基礎建設安全**	**Track B** **APT 攻擊與防禦 I**	**Track C** **法規遵循與資安治理**	**Track D** **企業熱門資安議題**	**Track I** **資安論壇**
13:30~14:10	企業網路安全缺口何在？ (Arbor Networks 亞太區技術總監 / 張泰興)	由最新 APT 攻擊手法探討層出不窮的 APT 攻擊事件 (趨勢科技 技術顧問 / 吳宗霖)	營業秘密管理制度與資安稽核聯防剖析 (中華數位科技 企業資料保護研究小組顧問 / 吳毅勛)	看百大企業如何抵禦 APT 與 DDoS 攻擊 (瑞奇數碼 技術副理 / 呂建鋒)	2015 國際資安標準趨勢與內涵 (BSI 總經理 / 蒲樹盛)
14:10~14:30	中場休息				
14:30~15:10	重新定義網路安全-持續性的安全監測 (Tenable 大中華區總經理 / 莊昊龍)	資安就是競爭力 - 2015 Blue Coat 進階威脅防護策略與實務分享 (Blue Coat 亞太地區資訊長 / Matthias Yeo)	稽核漏攔與誤判，真能安心？符合國際 e-Discovery，最佳化整合 DLP 與 HTTPS/ PDF/ZIP 郵件閘道加密 (碩琦科技 總經理 / 鄭志文博士)	揭開最新資安挑戰！虛擬化伺服器安全機制核心技術拆解 (F-Secure 翔偉資安亞洲區病毒威脅室訊息安全技術顧問 / 吳樹謙)	阿碼創業時的大膽假設與成功關鍵：八年後回顧 (阿碼科技 創辦人兼執行長 / 黃耀文博士)
15:10~15:30	中場休息				
15:30~16:10	Xceedium~ 遠端連線控管、側錄、防止蛙跳 與特權帳號密碼管理方案 (商丞科技 產品經理 / 李舒玄)	百分之百的安全？ (思科台灣安全事業部產品經理 / 郭旭傑)	《全球資安剖析》，您做確實了嗎？ (Barracuda 亞太區技術顧問 / 翁學良)	虛擬化環境內的微切分安全防護技術架構 (VMware 資深技術顧問 / 饒康立)	打造新一代安全財政系統 (財政部財政資訊中心 主任 / 蘇俊榮)

16:10~16:30	中場休息				
16:30~17:10	線上模擬-奪回你的網路安全主控權（Intel Security 資深技術經理 / 沈志明）	萬物皆聯網，危機四處藏 - 如何因應甚囂塵上的 DNS 攻擊！（Infoblox 達友科技 技術顧問 GCC / 張哲綱）	中芯數據 技術議程	你必須認識駭客的三大原因 & 從 VulReport 談漏洞揭露與企業資安漏洞管理（HITCON /蔡松廷 (TT)、Sylphid）	邁向電子病歷時代的醫療安全（衛生福利部資訊處處長 / 許明暉）

4 月 2 日(四)					
08:00~09:00	報到				
09:00~09:10	開場致詞 (iThome 電腦報總編輯 / 吳其勳)				
09:10~09:50	從 **Sony** 遭駭事件的教訓，談數位隱私和物聯網（F-Secure 芬安全 首席資安研究長/ Mikko Hypponen）				
09:50~10:30	重大資料竊案，現場忠實呈現（趨勢科技全球技術處 資深處長 / 張裕敏）				
10:30~10:40	中場休息				
10:40~11:20	顛覆 **2015**：威脅與防禦新趨勢（阿碼科技 創辦人兼執行長 / 黃耀文博士）				
11:20~11:50	**2015** 企業資安全面防護策略 - 打造從閘道到端點的縱深防禦機制（Palo Alto Networks 總經理 / 陳宗祈）				
11:50~12:30	對策直擊！日本關鍵基礎建設資安防護大揭露（日本電腦網路危機處理暨協調中心 JPCERT/CC 資安分析師 / 林永熙）				
12:30~13:30	中場休息				
Tracks	**Track E** 資料與隱私安全	**Track F** Web 與行動應用安全	**Track G** 雲端與虛擬化安全	**Track H** APT 攻擊與防禦 II	**Track J** 資安論壇
13:30~14:10	合作夥伴精彩議程 **(Akamai)**	**Protect your apps from the bad guys**（HP 資訊安全事業處 北亞區技術總監 / 蕭松瀛）	讓我們一起，看雲，聽故事（Openfind 雲端服務副總經理 / 張嘉淵）	APT 攻擊無所不在，小心！威脅就在您身邊!（ESET 亞太區總代理 台灣二版有限公司 高級產品經理 / 盧惠光）	臺灣資安人才培育（國立臺灣科技大學 資訊管理系特聘教授 / 吳宗成）
14:10~14:30	中場休息				

14:30~15:10	文件保護型態轉換與文件加密不得不說的故事（優碩資訊科技 Trustview 技術行銷部產品經理 / 陳品翰）	**Mobile x 資安 x 挑戰 剖析行動安全的必要性**（AhnLab 原廠專業講師）	不可遺忘的最後一塊拼圖 - 監控、側錄、風險分析各類操作行為（漢領國際 產品技術經理 / 黃漢宙）	全面啟動點線面 APT 防護網（FireEye 技術經理 劉俊雄）	我國網路安全防護願景與推動策略芻議（國家發展委員會 管制考核處處長 / 何全德）
15:10~15:30	中場休息				
15:30~16:10	**Varonis 檔案儲存記錄稽核、權限控管理、機敏資料搜尋、權限申請批核盤點**（商丞科技 產品經理 / 李舒玄）	**Enterprise Mobility Management: Secure, Manage, and Empower**（VMware AirWatch 事業部大中華區總監 / 徐謙）	雲端與虛擬化安全的新思維（優利資安顧問總監 / 李逸元 博士）	從資料竊取看 APT 複合進階攻擊（Websense 台灣區技術經理 / 陳志遠）	日本如何培育資安人才（日本電腦網路危機處理暨協調中心 JPCERT/CC 資安分析師 / 林永熙）
16:10~16:30	中場休息				
16:30~17:10	資安治理與資訊犯罪預防（東吳大學法律研究所兼任助理教授；中央警察大學刑事系兼任教官 / 李相臣）	你知道駭客怎麼看你嗎？ - 從滲透測試談企業常見資安風險（戴夫寇爾 DEVCORE 執行長 / 翁浩正）	雲端與虛擬化安全技術議程	如何因應 APT 攻擊 - 從預防、偵測到應變（勤業眾信聯合會計師事務所 企業風險管理協理 / 舒世明）	政府資安管理與資安治理（行政院資通安全辦公室副主任/ 吳啟文）

＊主辦單位保留議程變動之權利

七、國際資安大師師資介紹

1. Tony Cole /

職稱： FireEye 副總裁暨全球政府業務部門技術長

簡介：曾是美國五角大廈將軍，負責五角大廈後端網路資安防護工作，管理過 24 小時資安維運團隊、弱點評估團隊、資安工程團隊和五角大廈電腦事件應變團隊等。於美國陸軍服役超過 30 年，參與多項軍方通訊、情報和加密研發等資安事務。退役後曾任職於 McAfee，負責全球政府資安顧問服務團隊，也曾在 Symantec 負責大型技術研發專案。目前在 FireEye 負責協助各國政府和企業了解各種新式先進威脅技術和影響。他將帶來美國最新資安事件進展和趨勢。

2. Mikko Hypponen /

職稱：芬安全首席資安研究長

簡介：從 1991 年就和病毒為伍，協助歐美調查網路犯罪，並參與北約卓越合作防禦中心任務，幾次全球性資安事件，都扮演關鍵角色，被媒體喻為資安傳奇。2003 年事先關閉連微軟都沒輒、透過垃圾郵件全球散布的 SoBig.F 變種病毒的傀儡網路；2004 年率先針對會造成電腦自動開機關機的 Sasser 殺手病毒提出警告，迫使微軟在 17 天內完成漏洞修補；更是 2007 年，全球第一個時事垃圾郵件感染風暴蠕蟲的發現者；連鎖定核電廠的 Stuxnet 病毒，都在發現初期就對運作進行分類，降低後遺症。他將介紹最新資安威脅，揭露物聯網或穿戴式裝置隱藏的風險。

3. 林永熙 /

職稱：日本電腦網路危機處理暨協調中心（JPCERT/CC）資安分析師

簡介：在 JPCERT/CC 任職至今近 10 年，是日本派赴海外支援各國當地資安事件的國際級專家之一。在 JPCERT/CC 則負責協調資安漏洞事件處理、資安新團隊籌設與培訓，也負責日本相關資安事件緊急因應。曾於 2009 擔任日本國際合作機構（JiCA）專家，派遣至柬埔寨王國國家資訊通信技術開發局。2012 年時則擔任日本一般財團法人海外產業人才培育協會（HIDA）專家，派遣至緬甸聯邦共和國郵電部。近年以都市安全為主要研究方向，將來臺介紹日本關鍵基礎設施資安防護經驗。

八、報名方式：

各項課程，即日起開放報名（額滿為止），請上官方網站報名:

http://infosec.ithome.com.tw/

- 免報名費，食宿、交通自理，
- 因座位有限，主辦單位保留報名資格審核權，
- 收到報名資料後，系統將發出確認信告知已收到資料，並於資料審核後，於會前一周內以 email 及手機簡訊發出會前通知及報到編號。

聯絡人: 賴小姐，(02)2562-2880#3631
guan@mail.ithome.com.tw