

## 美國資訊安全分析新挑戰：巨量資料（Big Data）之應用

在2013年的國際資訊安全會議（RSA Conference）上，資安專家紛紛表示，將Big Data技術應用於資訊安全分析的項目上，確實可以幫助企業建立更佳的情勢判斷能力，但在實際執行過程中是一大挑戰。

資安廠商如RSA和賽門鐵克公司，在會議上表示目前的策略是透過新的數據匯集、比對和分析協助企業篩選、過濾結構化和未結構化資料的威脅指標，這是傳統的特徵偵測（signature-based）安全工具無法做到的。

不像傳統的安全手段著重於阻斷攻擊，新的技術強調偵測並立即回應違犯行為，也就是提前遏止任何違犯行為，協助企業作全面性的偵測而不擔心有所遺漏。

由於越來越多的美國政府機關和民間企業遭受到針對性和持續性的攻擊，巨量資料技術的應用需求激增。企業內部都累積著大量的數據和多元的數據種類，而需要動新技術來保護這些數據資料免於惡意人士或對手的竊取或其他侵害行為。企業應該要因應實際面臨的威脅和所獲悉的威脅情報來建立安全模型，取代部署特定產品和外圍系統的防禦。

美國無論是政府機關或民間企業都被捲入了不對稱戰爭-對手是武器精良、準備充分並有嚴密組織的網路敵人。

「駭客只需要攻擊成功一次，但我們必須每次都是成功的」賽門鐵克的總裁deSouza表示。「因此與其專注的在阻擋所有威脅，更好的辦法是使用巨量資料技術偵測侵入行為並消解之」。而在會議中資安專家都肯認至少從理論上來說，以巨量資料技術強化資訊安全是很好的想法。

不過另有其他的說法，金融服務企業LSQ的首席安全及法務主管皮爾遜認為，許多人的電腦紀錄檔和所有的電子裝置都早就被侵入滲透了，這才是問題所在。他表示，目前現存的SIEM（安全性資訊及事件管理）工具可以讓企業聚集來自許多個安全設備的巨量登錄數據整合在同一系統內，但真正的問題是，SIEM工具必須要有能力分析數據並找出關聯性，如此才能偵測到駭客入侵的前兆證據和真實的入侵行為，這和彙整數據是不同的兩件事。許多企業所面臨的問題不是缺乏數據資料，而是要如何為資訊安全的目的建立關聯規則和應用方式，以有效率的方式找出有用的巨量數據並進行分析，和留下可供進行訴訟使用的證據。

### 相關連結

[Cyclone Interactive, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, Apr. 10, 2013](#)

[Jaikumar Vijayan, Applying big data approaches to information security a challenge, Computerworld, Apr. 10, 2013](#)

陳秭璇 編譯整理

上稿時間：2013年04月

#### 資料來源：

Jaikumar Vijayan, Applying big data approaches to information security a challenge, Computerworld, Apr. 10, 2013, [http://www.computerworld.com/s/article/9237212/Applying\\_big\\_data\\_approaches\\_to\\_information\\_security\\_a\\_challenge\\_](http://www.computerworld.com/s/article/9237212/Applying_big_data_approaches_to_information_security_a_challenge_) (last visited Apr. 15, 2013).

Cyclone Interactive, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, Apr. 10, 2013, <http://www.emc.com/leadership/digital-universe/view/information-security-2020.htm> (last visited Apr. 15, 2013)

文章標籤



## 你 可 能 還 會 想 看

### 從新一期發布之強化農業生產基礎計畫談日本智慧農業推動策略

從新一期發布之強化農業生產基礎計畫談日本智慧農業推動策略 資訊工業策進會科技法律研究所 劉宥好 副法律研究員 2020年11月13日 壹、日本內閣推動智慧農業政策之演進 日本內閣推動智慧農業相關政策，促使農林漁畜業及地方發展，首現於2013年「農林水產業地域活力創造計畫」（以下簡稱活力創造計畫）[1]，計畫指出日本預計透過活用機器人技術與農業ICT（資通訊技術），實現超省力、高品質生產的新農業，設置研究會以規劃智慧農業未來藍圖、確保保機器人技術安全性政策等，促進高等栽培技術知識外顯化，推動開發生產管理與農業經營指導等系統。活力創造計畫係由日本內閣設置之農林水產業地域活...

### 德國「促進智慧財產權保障落實法Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, Durchsetzungsgesetz」將於今年8月1日開始生效施行

歐盟「Enforcement-Richtlinie 2004/48/EG指令」於德國國內法，而採取所謂「條款立法Artikelgesetz」之綜合立法方式\*，包括「專利法」、「商標法」、「實用新型專利法」、「半導體保護法」、「外觀設計專利法」、「品種保護法」、「非訟事件費用法」以及「著作權法」等相關條文之修正。其中涉及「著作權法」相關重要修正條文包括「他人資訊提供請求權」，主要是賦予著作權人在主張權利侵害時，得向ISP業者要求提供可以辨明侵權者之身分資料 (§101 UrhG)，惟須符合特定條件，例如，侵權者須有營業行為 (in gewerblichem Ausmaß)。然而，就何謂「營業行為」在立法過程中爭議迭...

### 監視器無鉛製程 冠捷導入

歐盟RoHS、WEEE政策實施在即，出身歐洲第一大品牌的飛利浦 (Philips) 率先響應，今年所有LCD監視器符合RoHS全面無鉛化，代工夥伴冠捷 (AOC) 隨第二季正式合併飛利浦顯示器事業部，也將導入無鉛製程。國內兩大LCD監視器製造大廠明基、光寶也已防患未然，製程無鉛化製程提早開跑。飛利浦今年在臺灣LCD監視器策略，其中之一是全面推展無鉛化產品線，W、P、B、S四大系列全面符合歐盟RoHS規定，鉛含量在0.1% (1000ppm) 以下，可說領先各品牌率先推出無鉛產品。監視器製造大廠冠捷 (AOC) 已和飛利浦已簽訂顯示器事業部併購意向書，第二季起將正...

### 歐洲執委會公布安全，清潔，聯網式交通行動議程

歐盟執委會於2018年5月17日公布第三套安全，清潔和聯網式交通行動議程，該套行動也是最後一套實現歐洲運輸系統現代化的措施。在2017年9月的國情咨文中，歐盟主席容克提出歐盟產業成為創新，數位化和低碳化均能領先於全球地位的目標。基於此原因，在交通領域執委會2017年5月和11月的提出兩套歐洲行動措施，其目標係讓所有歐洲人都能從享受更安全的交通，更少污染的車輛和更先進的技術解決方案，並同時加強歐盟產業的競爭力。為此，本次議程聚焦包括未來車輛和基礎設施安全措施綜合政策;重型車輛的二氧化碳標準;歐洲發展和製造電池的戰略行動計畫以及關於車聯網和自駕車的前瞻性戰...

## 最 多 人 閱 讀

- 二次創作影片是否侵害著作權-以谷阿莫二次創作影片為例
- 美國聯邦法院有關Defend Trade Secrets Act的晚近見解與趨勢
- 何謂「監理沙盒」？
- 何謂專利權的「權利耗盡」原則？

▶ 隱私權聲明

▶ 聯絡我們

▶ 相關連結

▶ 徵才訊息

▶ 資策會

▶ 網站導覽



