前瞻科技與管理　5卷2期，23-40頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 23-40 (November, 2015)
DOI: 10.3966/222014242015110502002

建構整合式雲端威脅之數位證據鑑識標準作業程序雛形之探討

陳靜玉[1,*]　吳乙南[2]　林宜隆[3]

[1]宏碁股份有限公司主任工程師
[2]宏碁股份有限公司副總經理
[3]元培醫事科技大學資管系暨數位創新管理研究所教授

摘 要

本文就雲端安全管理概念從事數位證據鑑識標準化，且為讓資安事件發生後，能有足夠的能力應付各種新興的犯罪型態以及因應各項潛在訴訟之需求，所蒐集之證據均具備有效性，希望能藉此提升數位鑑識資安能量，將美國國家標準研究所（National Institute of Standards and Technology, NIST）所提出之IaaS、PaaS、SaaS（Software）3層增列DaaS、MaaS、SaaS（Security），期藉由國際標準CSA、ISO27001: 2013、《個人資料保護法》之安全控制措施加於應用面進行探討，並套用林宜隆所提出之DEFSOP，衍生出一套符合現況雲端架構之標準作業流程，目的除了在減輕人工對雲端管理的成本浪費，並包含自動化之要件，以及整體網路使用上的資訊安全監控能力之完善管理流程——建立整合式雲端威脅之數位證據鑑識標準作業程序雛形。本文期將儲存設備空間加以整合利用，解決使用者的困擾，並進而落實資料保全與資訊安全，以完整掌握在私有雲內之資料動向，藉以提升我國私有雲之資安能量，進而達成BYOS（Bring Your Own Security）理念。

關鍵詞：BYOS、CSA、DEFSOP、ISO 27001、NIST

* 通訊作者：陳靜玉
電子郵件：cyc7986@gmail.com

前瞻科技與管理　5卷2期，23-40頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 23-40 (November, 2015)

Discussion on Digital Integrated Cloud Threat Forensic Evidence Standard Operating Procedures of the Construction of the Prototype

Jewel Chen[1,*], Rex Wu[2], and Yi-Long Lin[3]
[1]Principal Engineer, ACER INCORPORATED
[2]Vice President, ACER INCORPORATED
[3]Professor, Yuanpei University of Medical Technology Departement of Information Management
Master's Program in Digital Technology Innovation and Management

Abstract

In this paper, the concept of cloud security management, Standardization in digital evidence forensics, to make information security incident, have sufficient capacity to cope with emerging crime patterns and response to the potential demand litigation, Which have gathered evidence of effectiveness, hoping to enhance the digital forensics owned energy security, the NIST raised the IaaS, PaaS, SaaS (Software) additional three item DaaS, MaaS, SaaS (Security), by international standards CSA, ISO27001: 2013, Security controls Personal Data Protection Act applied to the application surface to be explored, and apply to the DEFSOP application that were put forward by Professor Yi-Long, Lin, in line with the current situation put forward a set of standard operating procedures cloud architecture, aim to reduce the labor costs in addition to waste management to the cloud, and it contains elements of automation, overall information security and network monitoring capabilities on the use of a better management process-the establishment of an integrated Cloud threat of digital evidence forensics prototype standard operating procedures, if by this study will be to integrate the use of space for storage equipment,

* Corresponding Author: Jewel Chen
E-mail: cyc7986@gmail.com

to solve user problems, the further implementation of information preservation and information security, a complete grasp trends in the data within a private Cloud, funding in order to enhance the energy security of the private cloud, and then reached the BYOS (Bring your own safety) concept.

Keywords: BYOS, CSA, DEFSOP, ISO 27001, NIST