

# 整合國際數位證據鑑識標準 ISO27037、ISO27041~43 於數位證據標準作業程序-以 UFED 為例

林宜隆

元培醫事科技大學

數位創新管理碩士班 教授

[cyberpaul747@mail.ypu.edu.tw](mailto:cyberpaul747@mail.ypu.edu.tw)

賴群傑

元培醫事科技大學

數位創新管理碩士班 研究生

[a410131232@gmail.com](mailto:a410131232@gmail.com)

## 摘要

近年來，人們生活對行動互聯網及行動裝置的依賴度與日俱增，而在資安事件發生時，偵查人員對於案件數位證據之鑑識調查，往往忽視事前之準備程序及事後的鑑識報告及呈現程序，為希冀能在事件發生之前中後均能依數位鑑識程序處理，有關國際數位鑑識標準持續開發新的標準包含除了 ISO/IEC 27037 以外，開發新的 ISO/IEC 27041、ISO/IEC 27042 及 ISO/IEC 27043 等諸多作業程序，以因應現今虛擬世界中網路犯罪、關鍵基礎設施連結網路與現實世界所帶來之風險。如近期發生的台積電病毒事件，其為臺灣業界資安的資安生，都會犯錯。讓一個看似無害的違反 SOP 小疏忽，最後竟導致 52 億元的預估營收損失，創下臺灣資安史的紀錄。也顯現網路資訊安全的重要性是越來越強烈。

關鍵字：ISO/IEC 27037、ISO/IEC 27041、ISO/IEC 27042、ISO/IEC 27043 數位證據鑑識標準作業程序(DEFSOP)