國際電子證據管理標準於犯罪偵查知識工程之應用探討

◎ 林宜隆／大同大學資訊工程學系教授、王林展／大同大學資訊工程學系在職碩士

隨知識工程迅速發展，網路犯罪手段不斷演變，犯罪偵查工作產生前所未有的挑戰。數位證據在現代犯罪偵查中扮演著愈加關鍵的角色，建立一套完善的數位犯罪偵查知識工程化框架顯得尤為重要。本文探討國際標準 ISO / IEC 27050 電子證據管理系列在犯罪偵查知識工程化的應用，尤其在建立鑑定化（Identification, I）、概念化（Conceptualization, C）、正規化（Normalization, N）、實作及測試（Implementation & Testing, I）、證實（Validation, V） ICNIV 模型的五個階段的具體流程 SOP 與實際步驟。

犯罪偵查知識工程化探討

犯罪偵查知識工程化ICNIV模型可分成五個階段：鑑定化（Identification ,I）、概念化（Conceptualization, C）、正規化（Normalization, N）、實作及測試（Implementation & Testing, I）、證實（Validation, V）。在數位犯罪偵查的知識工程領域中，國際標準ISO / IEC 27050系列從數位證據的鑑別，到最終的法律驗證等各個重要環節，為執法人員和法證專家提供多面向的參考指標[1]。

1 吳昆霖、林宜隆及趙涵捷「建立數位犯罪偵查知識工程雛型之研究－以DEFSOP、ISO 27037及ISO 27041為例」，2019年12月1日

為深入瞭解ISO / IEC 27050國際標準在犯罪偵查知識工程化中的實際具體應用，其流程如圖 1 所示。

在鑑定化階段，ISO / IEC 27050–1:2019和ISO / IEC 27050–2:2018標準幫助確定電子證據的範圍和關鍵利害關係人。接著進入概念化階段，ISO / IEC 27050–2:2018和ISO / IEC 27050–3:2020標準提供了開發調查模型和建立證據處理框架的指導。而在正規化階段，這些標準則確保了調查過程的合規性和證據處理的完整性。在實作與測試階段，ISO / IEC 27050–3:2020和ISO / IEC 27050–4:2021標準強調了工具和技術的實施和測試方法。最後在證實階段，這些標準確保了對調查結果進行審查與驗證，確保證據完整性與可信度，並生成法律訴訟報告，以確保證據具法律效力並能在法庭上提升其證據能力和有效性。

ISO / IEC 27050電子證據管理系列標準，為數位犯罪偵查知識工程化提供了一個高度系統化且具備全球認可的框架。透過整合及應用這些標準，能有效提高數位證據的管理水平，確保在跨國犯罪偵查過程蒐集到證據的合法性與可操作性。不僅有助於提高偵查的效率與精確性，更能在法庭上增強證據能力和有效性，為數位犯罪偵查提供技術支援和法律保障。

國際電子證據標準ISO 27050探討

探討ISO / IEC 27050電子證據管理系列標準過程，可從圖 2 瞭解ISO / IEC 27050

圖 1 ISO / IEC 27050 標準在犯罪偵查知識工程化各階段的具體應用流程

資料來源：本研究整理

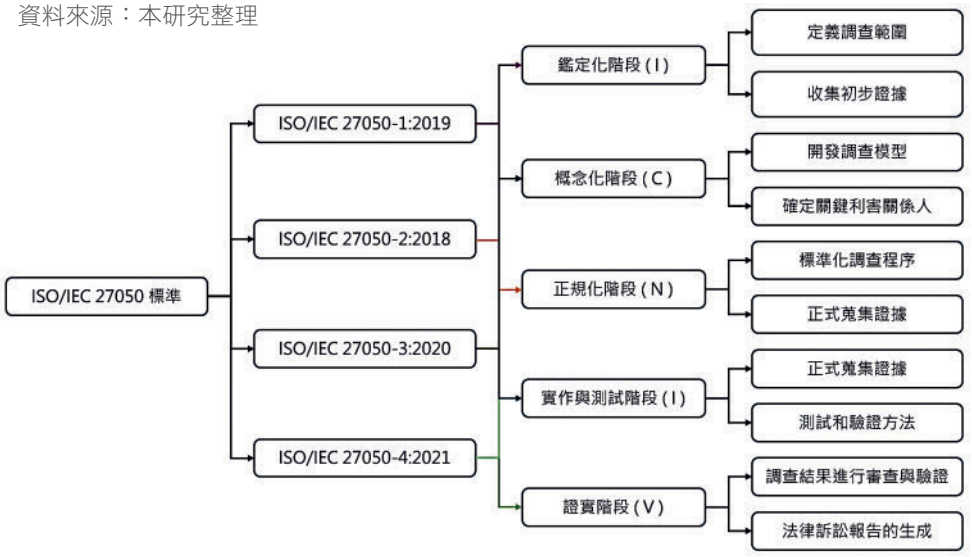


圖 2 ISO / IEC 27050 電子證據管理架構圖階段的具體應用流程

系列的四個區分概念，及其間的相互關聯性，在當前數位化的環境中，電子證據管理和分析十分重要。

為更全面地理解ISO / IEC 27050電子證據管理系列的功能適用範圍，將 ISO / IEC 27050電子證據管理系列標準與其他標準（如ISO / IEC 27037、ISO / IEC 27041、ISO / IEC 27042、ISO / IEC 27043、ISO / IEC 30121）之對應關係整理如表 1：

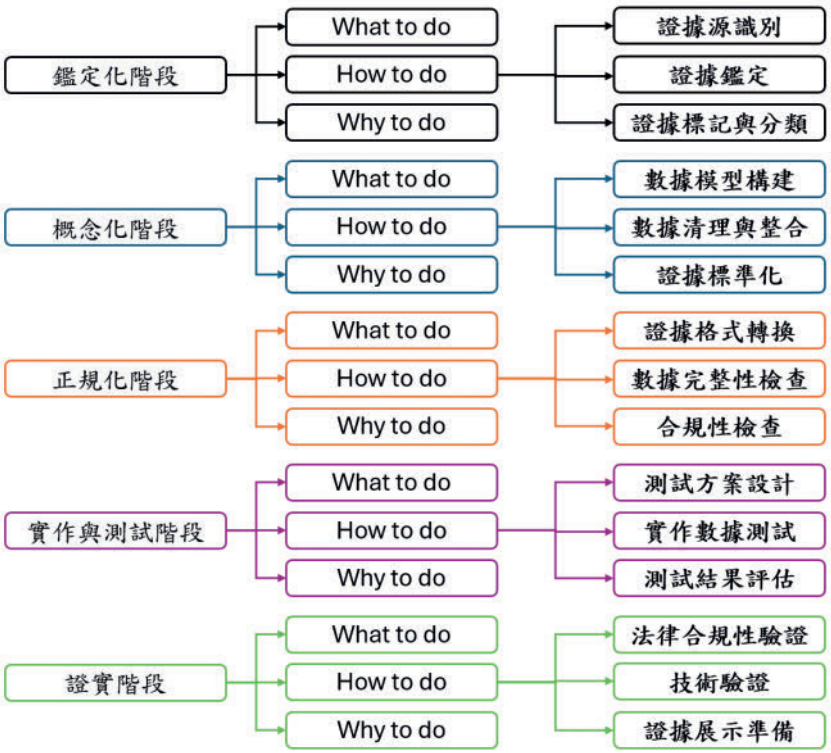
表 1 ISO / IEC 27050 電子證據管理系列與其他相關標準的功能適用範圍

資料來源：本研究整理

功能/標準	識別	保存	收集	處理	審查	生產	分析
ISO/IEC 27050-1:2019	✔	✔			✔		
ISO/IEC 27050-2:2018		✔	✔	✔		✔	
ISO/IEC 27050-3:2020	✔		✔				✔
ISO/IEC 27050-4:2021			✔			✔	
ISO/IEC 27037:2012	✔	✔	✔				
ISO/IEC 27041:2015		✔		✔	✔		
ISO/IEC 27042:2015					✔		✔
ISO/IEC 27043:2015	✔	✔	✔				✔
ISO/IEC 30121:2015				✔		✔	

圖 3 犯罪偵查知識工程化各階段流程圖

資料來源：本研究整理



建構犯罪偵查知識工程 ISO 27050 框架之必要與內涵

為更有效將ISO / IEC 27050 電子證據管理標準應用在犯罪偵查知識工程化ICNIV模型之鑑定化、概念化、正規化、實作及測試、證實等五大階段，有必要建立一個符合該標準的框架（圖3）。此框架能幫助調查人員遵循SOP標準化流程，確保調查過程的合法性和技術準確性。前開標準應用在ICNIV各階段之內涵說明如下：

鑑定化階段 （Identification Phase）

鑑定化階段主要任務是識別與犯罪案件相關的數位證據，這階段的證據識別將直接影響後續的調查和分析，故需要確保可能的證據來源都被充分考慮及初步篩選。依據 ISO / IEC 27050-2:2018 規範，鑑定化階段應包括以下步驟：

- 證據源識別：分析案件背景，識別所有潛在的數位證據來源，例如電腦、手機、網路伺服器、雲端存儲等。
- 證據鑑定：根據證據的相關性、可靠性和合法性進行篩選，初步確定哪些證據具有調查價值。
- 證據標記與分類：對鑑定出的證據進行標記和分類，以便於後續的處理和分析。

概念化階段（Conceptualization Phase）

概念化階段涉及將已鑑定的證據進行結構化處理，將其轉化為可操作的數據模型，以支持後續的分析和推理。在此階段，需將證據的多樣性和複雜性轉化為清晰的數據表示。根據 ISO / IEC 27050–3:2020 規範，應包括以下步驟：

- 數據模型構建：將數位證據轉化為可分析的數據模型，例如建立時間線、關聯圖表等，以顯示證據之間的關聯性。
- 數據清理與整合：對證據中的雜訊進行清理，整合多源數據，確保數據的一致性和準確性。
- 證據標準化：根據案件的需求和法律要求，對數據進行標準化處理，確保其符合相關規範。

正規化階段（Normalization Phase）

本階段目的是確保數據模型的合法性和技術準確性，為證據的合法性提供保障，將概念化的數據模型進一步精煉和優化，使其符合技術和法律的雙重標準，並確保數據模型能夠在不同情境下被有效應用。在 ISO / IEC 27050–3 和 27050–4 規範，應包括以下步驟：

- 證據格式轉換：將數據模型轉換為標準化格式，例如將非結構化數據轉化為結構化數據，以便於後續的處理和分析。
- 數據完整性檢查：驗證數據模型的完整性和一致性，確保所有關鍵資訊均被正確包含和處理。
- 合規性檢查：根據相關法律和標準，檢查數據模型是否符合規範要求，並進行必要的修正。

實作及測試階段（Implementation and Testing Phase）

本階段是將正規化後的數據模型應用於實際情境並進行各種測試，以確保其在現實環境中的有效性和可靠性。這階段是驗證數據模型是否能夠支持實際案件的關鍵。根據 ISO / IEC 27050–3 和 27050–4 要求，應包括以下步驟：

- 測試方案設計：制定測試計劃，包括測試目標、測試方法、測試數據和測試環境，確保測試的全面性和有效性。
- 實作數據測試：在模擬或真實環境中進行數據模型的測試，評估其在不同情境下的表現，檢查是否存在數據丟失、錯誤或其他問題。
- 測試結果評估：對測試結果進行分析，確定數據模型的有效性和可靠性，並根據測試結果進行必要的修正和優化。

證實階段 （Validation Phase）

證實階段是犯罪偵查知識工程化的最後階段，旨在通過法律或技術手段對數據模型的合法性和有效性進行最終驗證，確保其能夠作為法律證據使用。在 ISO / IEC 27050-4 規範下，證實階段應包括以下步驟：

- 法律合規性驗證：根據相關法律規範，對數據模型進行最終驗證，確保其在法律訴訟中具有可接受性。
- 技術驗證：通過技術手段驗證數據模型的準確性和可靠性，確保其能夠支持法律程序中的各項需求。
- 證據展示準備：準備證據展示資料，確保在法庭上能夠清晰、準確地呈現數據模型及其分析結果。

結論

將ISO / IEC 27050電子證據管理系列標準與犯罪偵查知識工程化五個階段相結合，能建立既符合國際標準，又具備實用性的犯罪偵查知識工程化框架，不僅提升了電子證據處理的規範性和可靠性，還大幅增強了犯罪偵查的效率與準確性，為司法人員提供了有效的工具來應對複雜的數位證據挑戰，並能確保提供的數位證據具有更強的法律證據能力和有效性。

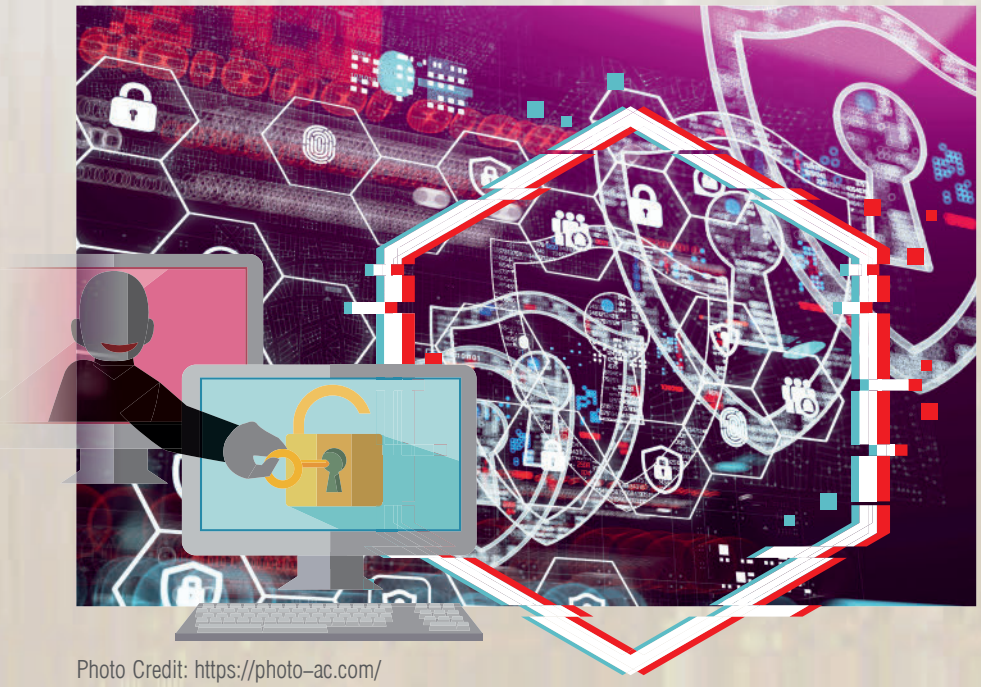


Photo Credit: https://photo-ac.com/