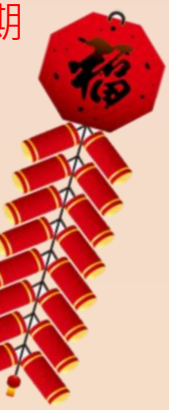
No. 179
Jan. 2022

政風電子報



淺談資安情資分享與分析

◆ 華梵大學資管系特聘教授 — 朱惠中

當公私部門妥善收集與共享網路威脅情資，將能協助各機關組織更快識別出威脅並找出解決方法。「資安即國安」，無煙硝的戰爭已啟動，各領域 ISAC 的成熟運作，才能建構完整之國家資安聯防體系。

背景

美國前總統歐巴馬於 2015 年 2 月 13 日簽署第 13691 號行政命令—「促進私營部門網路安全情資共享」，要求發展 ISAO（Information Sharing and Analysis Organizations）組織，以促進政府與私有部門之間更好的網路安全與情資共享，並加強私有部門之間的合作。

根據總統的第 13691 號行政命令，美國政府要求各關鍵基礎設施部門籌組 ISAC（Information Sharing and Analysis Centers）中心，基本上 ISAO 與 ISAC 的目標均是蒐集、分析、傳送網路威脅情資，而二者不同點在於 ISAC 分成若干層級部門，彼此間有從屬關係，而各 ISAO 間則沒有從屬關係。

情資共享目的在於提升網路安全

情資共享之目的為幫助管理及操作單位來降低網路安全（Cybersecurity）之風險，其具有下列特色：

一、各個 ISAO 為獨立個體。

二、須依據網路安全的場景、新型態的攻擊與需求而調整。

三、新設置 ISAO 所提供網路安全情資共享計畫的內容，須與已設置 ISAO 的內容保持一致。

(接續次頁)

Administration of Barack Obama, 2015

Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing

February 13, 2015

美國前總統歐巴馬於 2015 年 2 月 13 日簽署第 13691 號行政命令—「促進私營部門網路安全情資共享」，要求發展 ISAO 組織，促進公私部門之間更好的網路安全與情資共享。（Source: U.S. Government Publishing Office, https://www.govinfo.gov/content/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf）

威脅情資可分為分享與共享兩類，前者為將所獲得的威脅情資提供給特（指）定（如已參加 ISAC 的電力部門）的關鍵基礎設施部門擁有者、使用者，而後者則是將所獲得的威脅情資提供給所有（跨領域）關鍵基礎設施部門的擁有者、使用者或普羅大眾。

情資分（共）享之處理原則

情資分享之處理原則（STEPS）需考量如下列事項：

一、社群組織（ISAO）會員需要哪些情資（如威脅情資或弱點）？

二、社群組織需要哪些情資來支持與達成其任務或願景？

三、社群組織會員如何使用社群組織所提供的分（共）享情資[1]？

四、社群組織會員如何獲得分享情資[2]？

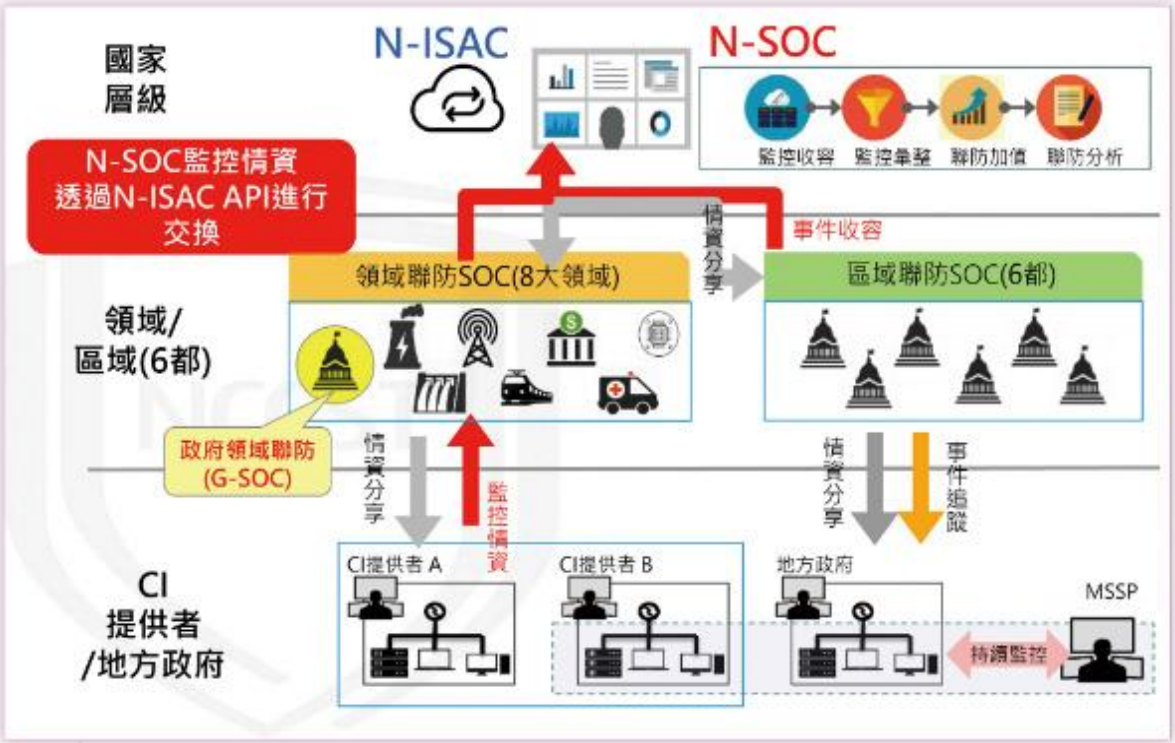
五、會員如何與其他會員共享情資（初期）[3]？

[1] 需再考量：1. 會員使用此等共享情資來降低威脅（直接），如安裝防毒軟體；2. 會員將此等分享情資列入風險管理決策之考量（間接），如機敏資料須加密或使用燈號控制協議（Traffic Light Protocol, TLP）來對資料做分類及決定其可以分享的對象與程序。

[2] 分為：1. 會員經由社群組織獲得由該社群組織的會員提供給其他成員之情資；2. 會員經由政府或工業網路安全情資供應商，如 CERT（Computer Emergency Response Team），提供給社群組織 ISAO 會員。

[3] 方式包含：1. 社群組織會員與會員直接交換情資（非正式，如見面交談）；2. 經由線上入口網站執行人工（非自動化）分享作業；3. 利用情資共享平臺執行自動化分享作業；4. 初期會採取非正式的分（共）享方法，及盡點現有的技術來達成能快速分享「威脅指標」的目標。

(接續次頁)



ISAO與ISAC的目標均是蒐集、分析、傳送網路威脅情資，ISAC分成若干層級部門，彼此間有從屬關係，而各ISAO間則沒有從屬關係；圖為我國資安情資分享的體系架構。（資料來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1282）

六、社群組織會員是否有能力及資源使用社群組織或其他會員提供的共享情資？

七、社群組織如何確保其所獲得之分（共）享的情資是可運用的？如無法滿足獲得此共享情資的成員需求時，則如何精進或調整以滿足其需求？

八、社群組織如何蒐集其他會員對所提供之共享情資的回饋意見？

九、社群組織如何提供共享情資？匿名分享或公布來源歸屬？

十、社群組織是否要對共享情資（分享和接收）做機密等級分類？

分（共）享情資之類別

依金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）[4] 情資分享管理辦法之定義，威脅情資的分類原則及類別如次：

[4] 係針對金融業所設立，於2017年12月揭牌，為聯手臺灣金融業者共同打造之金融圈的資安聯防體系。https://www.ithome.com.tw/news/119886。

(接續次頁)

一、原則

1. ISAO 和其成員如希可與其他 ISAO 成員及各級政府單位共享情資，則須有一致性的技術標準、框架及資料格式。
2. 建置框架來達成不同來源之情資的完整性與可分析性。

二、類型

包括資安訊息情資（ANA）[5]、資安預警情資（EWA）[6]、網頁攻擊情資（DEF）[7]、入侵攻擊情資（INT）[8]與回饋情資（FBI）[9]等。

分（共）享情資之技術標準與資料格式

情資交換平臺應配合國家資安資訊分享與分析中心（National Information Sharing and Analysis Center, N-ISAC）[10]情資交換格式與系統架構，採用 STIX（Structured Threat Information eXpression）格式與 TAXII（Trusted Automated eXchange of Indicator Information）傳輸架構，其中情資內容描述宜採用 CybOX（Cyber Observable eXpression），以利跨組織之情資傳遞與交流（圖 1）。

一、STIX

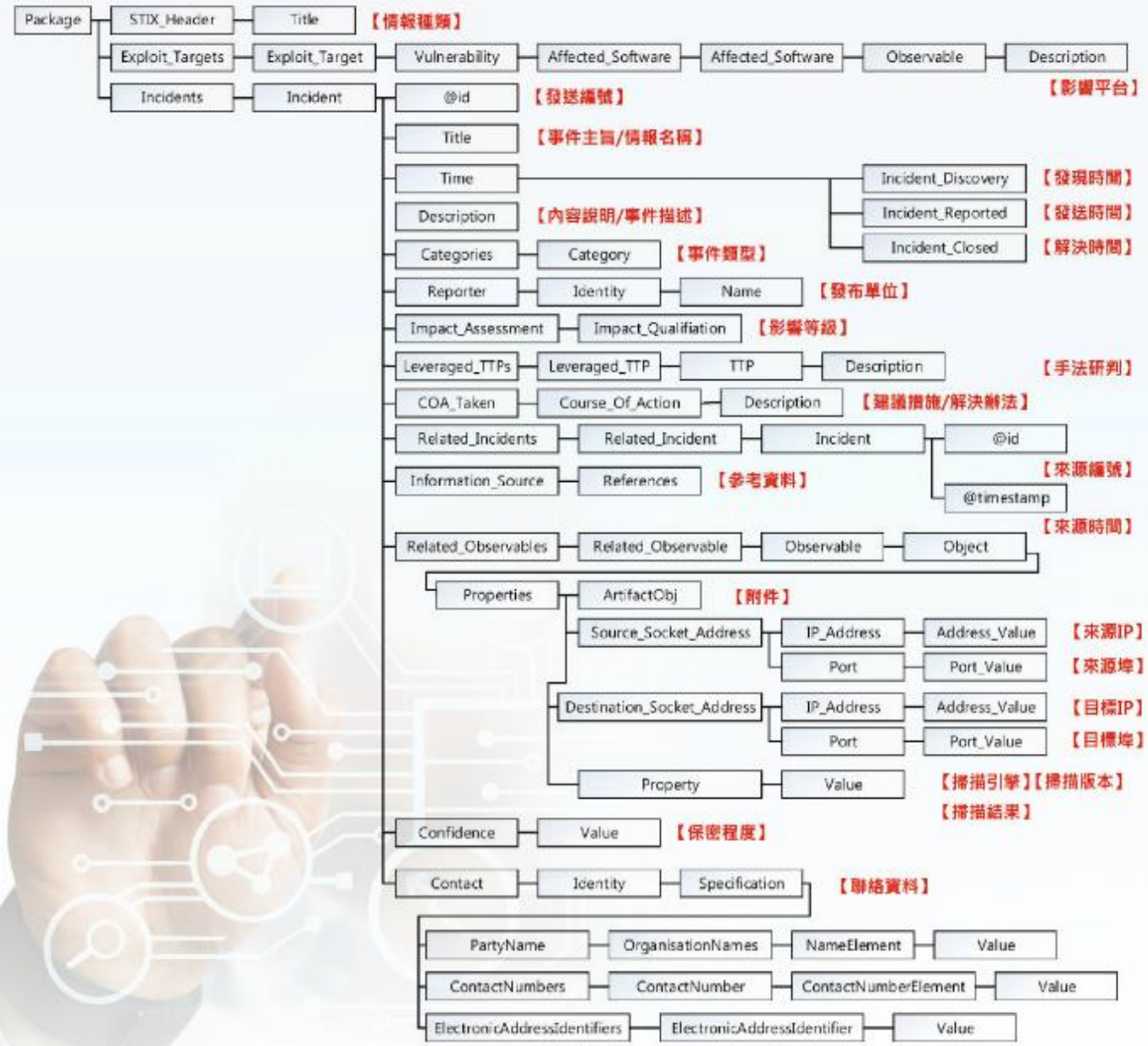
STIX 格式是一個共同合作開發的標準結構化語言，用於規範、獲取、描述和傳達標準化網路威脅資訊，使用擴展標記語言（Extensible Markup Language, XML）格式進行撰寫，便於封裝情資資訊，並且具有高度的可解讀性，方便人類與機器進行解讀，同時 XML 也有良好的擴展性，能透過編寫將既有資訊進行擴展。

情資交換格式 STIX	情資傳輸架構與機制 TAXII	情資內容描述（Schema）CybOX
● 情資封裝（Package）格式 ● 提供規範的資料模型來描述威脅情資	● 傳輸協定 ● XML Web Service 用來作為交換情資的標準	● 描述觀察到行為的特徵、屬性等

圖 1　技術標準與資料格式

[5] 包含重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告與資安相關技術或議題之經驗分享。
[6] 包含疑似存在系統弱點或可疑程式、疑似進行惡意或攻擊行為與進行可疑連線行為或活動。
[7] 包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確。
[8] 包含特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確。
[9] 包含情資使用或處理情形回饋、分享資安事件統計資料。
[10] 為國家級的資安資訊分享與分析平臺，於 2018 年 1 月正式營作。

(接續次頁)



STIX 格式是一個標準結構化語言，用於規範、獲取、描述和傳達標準化網路威脅資訊，便於封裝情資資訊，且具高度可解讀性；圖為 STIX 情資格式架構。（資料來源：行政院國家資通安全會，https://nicst.ey.gov.tw/Page/7CBD7E79D558D47C/74feb851-7f16-4e72-925e-3a041d898ce3）

(接續次頁)

STIX 情資除了便利封裝，能將情資進行儲存、傳遞、分享與分析，目前美國國土安全部旗下的資通安全辦公室（Office of Cybersecurity and Communications）、國家網路安全和通訊整合中心（National Cybersecurity and Communications Integration Center）及美國電腦緊急應變小組（US-CERT）均使用此架構進行情資分享。STIX 架構分為 12 大模組[11]，其模組本身或相互之間可具有關聯性與上下關係（Context-Sensitive）。

二、TAXII

TAXII 是一套網路威脅情資交換傳輸機制，其功能為提供組織與合作夥伴傳遞與共享情資，其功能模組包含網路連接、訊息處理及後端管理等功能單元，並包含數種服務功能[12]。

三、CybOX

CybOX 是一個標準化的方法（schema），用以編碼和傳達高精確度的結構化語言，描述所有可以從電腦系統和操作上觀測到的事件內容、行為或狀態特性。CybOX 支援許多網路安全領域[13]。

情資分享模型架構

情資分享模型架構可略分為以下模式：

一、點對點型（Peer-to-Peer）

1. 任何一個社群中之會員均可與其他會員互動及分享資訊。
2. 適合於較小的社群或僅需與部分的會員互動（Small/Asymmetrical Trust）。
3. 分享模式見圖 2。

二、軸輻型（Hub-and-Spoke）

1. 所謂「軸輻式系統」常用於貨運業、航空業、金融資訊業等之 ISAC 系統，即建立一個或數個轉運（或網路）中心，或可稱為「軸心」（HUB），先由各中心，結合該 HUB 的專業人員、流程及技術等來處理情資分享的相關事宜，再由各 HUB 的子系統向外「擴散」或「輻射」（spoke），而各 HUB 間可互相支援。
2. 分享模式見圖 3。
3. 我國 N-ISAC 採用軸輻型情資分享模型，作為情資管理與交流。

三、混和型（Hybrid）

[11] 12 模組包括：資安威脅觀察資料（Observables）、資安威脅模式（Indicator）、資安威脅事件（Incident）、資安威脅手法（Tactics, Techniques, and Procedures, TTP）、資安威脅活動（Campaign）、資安威脅者（Threat Actors）、資安威脅目標（Exploit Target）、資安威脅防護措施（Course of Action）、資安威脅報告（Reports）、資安通報與警示（Security Advisories and Alerts）、執行指引（Operational Practices）與弱點資訊（Vulnerabilities）等。

[12] 服務功能包含：接收服務（Inbox Service）、收取服務（Poll Service）、探索服務（Discovery Service）及訂閱管理服務（Collection Management Service）等。

[13] 包含威脅評估與描述（Threat assessment and characterization）、惡意軟體描述（Malware characterization）、操作事件管理（Operational event management）、安全性資訊與事件管理／記錄（Security information and event management / Logging）、網路情境感知（Cyber situational awareness）、事件應變（Incident response）、指標共享（Indicator sharing）及數位鑑識（Digital forensics）等。

(接續次頁)

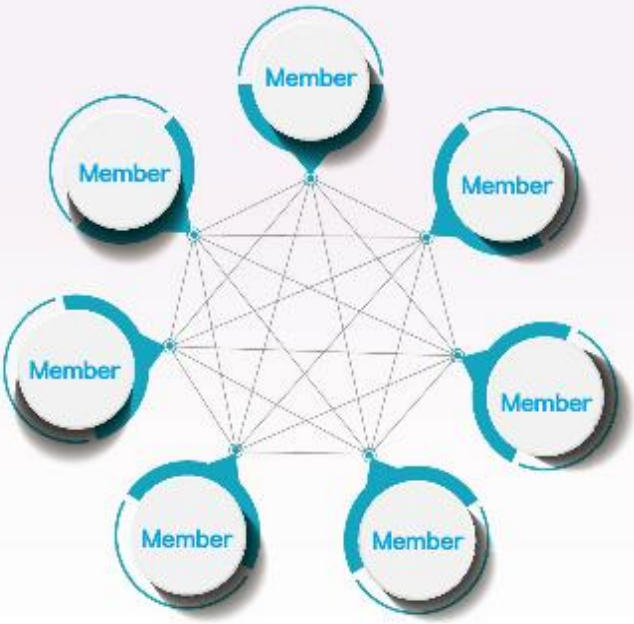


圖 2　點對點情資分享模式

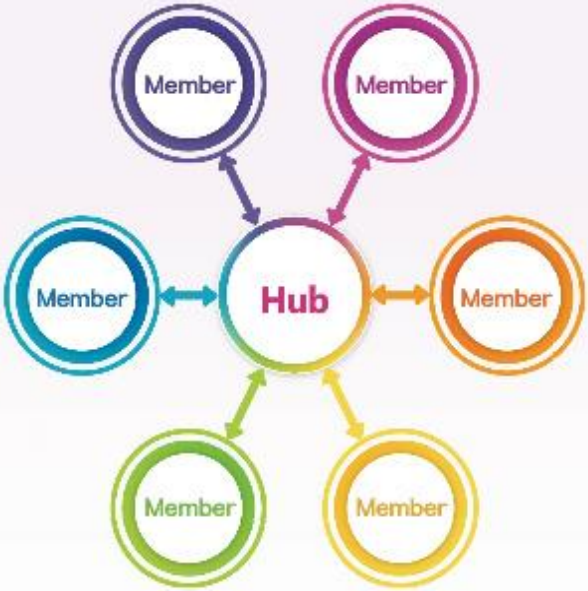


圖 3　軸輻型情資分享模式

威脅情資分析（Information Analysis）

一、情資分析的目的

先了解資料（data），然後再結合上下文及其他資料，獲得資訊（information），情資分析與情資分享基本上是 2 個獨立個體，彼此間沒有相互關係。

二、情資分析的步驟

1. 蒐集資料。應注意：（1）避免僅蒐集單個成員的資料；（2）資料如網路釣魚嘗試的次數、入侵企圖、成功的入侵、被入侵的帳戶數量以及分布式拒絕服務攻擊等。
2. 根據現有的數據來源進行解讀和操作學習。
3. 解讀相關的威脅數據以產生威脅組、資安威脅活動摘要或業務風險評估。包括：（1）什麼是感興趣的問題？（2）相關資料在哪裡？（3）分析是否可用（Available）、可以理解和適用（Applicable）。
4. 產出報告：包括樞軸報告（觀察跳躍點（hop）的 IP 位址）、惡意程式（蒐集惡意程式的雜湊值（HASH））與資安威脅活動[14]等。

(接續次頁)

隱私原則

情資分享與分析所須遵守或符合的隱私原則如次：

一、ISAO 本身需要有規劃及處理資訊隱私相關問題的能力。

二、需評估因與資安威脅模式有關的個資外洩所造成之影響。當資安威脅模式為個人識別資訊（Personally Identifiable Information, PII）時，需判斷此個人識別資訊是否與資安威脅有關，以及 ISAO 或其成員是否視需要刪除相關個資。

三、制定防止共享之個資或與資安威脅模式無關的機敏資料外洩之政策。

資訊安全

情資分享與分析所須遵守的資安規範為：

一、資訊安全是任何一個 ISAO 須面對的挑戰，資安政策須與資料的機敏程度同步，且安全通訊做法要確實，包括：1. 定期審查個別成員的資安等級及能力；2. 定期審查情資共（分）享計畫的資安要求是否合宜；3. 存取控制規劃（Access Control）的精進。

情資分享與分析仍須遵守隱私原則，防止共享之個資或機敏資料外洩。

二、網路攻擊與資料外洩須通報。

三、資料須分級、傳輸及標籤。

四、保障主機、伺服器及端點設備記憶體之安全性。

ISAC 的成熟運作是完整國家資安聯防體系的核心

我國對於關鍵基礎設施防護，已經逐步推動，亦有相當成果。運作良好且精準之威脅情資分享與分析中心，以及各領域之 ISAC 的成熟運作，將是建構完整之國家資安聯防體系的核心。

[14] 即分享有關資安威脅活動和 TTPs 的資訊。TTPs 為一個數學公式，用以偵測惡意行為的手法、技術與程序（Tactics, Techniques, and Procedures），包含攻擊特徵、惡意軟體、暴露之弱點、使用工具、事件架構、受害目標等），並認為此套理論可以被利用在各種不同使用情境及規模，這樣的防禦方式稱為碎形防禦（Fractal Defense），亦即行為模式。已有越來越多資安產品強調以「行為模式」偵測並防禦攻擊行為，Joseph Zadeh 認為，透過機器學習機制，掌握攻擊者的行為特徵（包含手法、技術與過程），比起利用變動頻率越來越大的 IP 及域名黑名單或特徵（Signature）之偵測，無論攻擊或應用的規模大小皆可達到有效防禦。

(資料來源:清流雙月刊111年1月號)

涉侵占民眾平板電腦 新北警遭清查 送辦自請離職

內政部警政署保一總隊支援新北市中和警分局偵查隊的陳姓員警，協辦拾得遺失物業務，未依規定入庫，還私自將民眾撿到的平板電腦帶回家，7月底已自請離職。（記者闕敬倫翻攝）

〔記者闕敬倫／新北報導〕內政部警政署保一總隊支援新北市中和警分局偵查隊的陳姓員警，今年6月協助辦理拾得遺失物業務，不僅未依規定入庫，還私自將民眾撿到的平板電腦帶回家，經分局內部清查，由新北市政府警察局政風室依法送辦，陳員7月底已自請離職。

據了解，前陳姓警員為保一支援中和分局偵查隊員警，平時主要業務為協助校園安全及犯罪宣導工作，今年5、6月期間，國內遭逢武漢肺炎疫情，警察機關實施分流上班，陳員被指派協助辦理民眾拾得遺失物業務。

6月中旬，陳員受理一台民眾拾獲的平板電腦，竟製作不實書函稱已發還物主，還將平板私帶回家，之後拾獲人去電中和偵查隊，詢問平板電腦的發還狀況；經偵查隊承辦人查詢，發現該平板電腦竟尚未發還，且陳員未依規定將遺失物入庫保管，後續向單位主管通報，偵查隊也展開內部調查，並調閱駐地監視器，確認陳員涉嫌違法，遂陳報警察局督察室及政風單位。

新北市政府警察局政風室後續調查，依《貪汙治罪條例》竊取或侵占職務上持有之非公用私有器材、財物及刑法《公務員登載不實罪》，將陳員移送新北地檢署偵辦；而陳員涉案遭送後，7月底已向中和警分局提出報告，主動請辭。

資料來源：自由時報〔記者闕敬倫／新北報導〕

針對勒索病毒事件建議強化措施

一、 高權限帳號存取管控

1.確認高權限帳號近期登出入記錄是否有異常狀況。

2. 更改高權限帳號密碼，確保密碼設定符合複雜性原則，避免字符轉換情況發生。

3. 限定帳號使用範圍，或利用群組原則設定僅能登入特定主機，例如網域管理員帳號僅能登入網域管理伺服器進行管理。

4. 採用多因子驗證，高權限帳號要透過兩種以上的認證機制之後，才能得到授權。

二、 遠端連線、委外廠商、網路硬碟與移動裝置存取管控

1.針對相關系統連線與遠端存取透過防火牆設備嚴謹控管，僅允許固定來源連線，避免遭駭客藉由跳板嘗試入侵。

2.外部網路透過 VPN 連線內部網路以達到安全加密的連線。

3.依據各單位不同業務考量提供不同資料檔案存取權限與連線網段，確保機敏資料安全性。

4.限定委外廠商外部連線存取機制，限縮其連線來源與目標，竊強烈建議僅允許限定時段作業，於作業完成後關閉連線許可，同時管控與監視其對內部的存取行為。

5.檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。

6. 針對移動設備進行存取管控，限定僅能使用授權裝置與鎖定非授權存取，使用移動設備前應先檢查是否感染惡意程式。

7. 針對移動設備進行存取管控，限定僅能使用授權裝置與鎖定非授權存取。

三、 資通訊系統排程設定與派送機制

1. 檢視近期排程設定與派送紀錄是否有異常狀況。

2. 針對新增特權帳號（事件識別碼：576 / 4672）、GPO 的新增異動（事件識別碼：566 / 5136、5137）、排程的新增異動（事件識別碼： 602 / 4698）、稽核紀錄服務停止（事件識別碼： 6006）、稽核記錄刪除（事件識別碼：517 / 1102）強化監控。

(接續次頁)

四、 資料備份與企業營運持續計畫（BCP）

1.檢視重要系統備份頻率，建議遵循 3-2-1 原則來定期備份檔案。此原則要求以兩種不同格式建立三個備份，並在異地儲存一個備份。同時重要機密的資料備份，應使用加密方式來保護。

2. 確認企業營運持續計畫（BCP）執行完善化，確保重要核心系統可達到高可用性、業務持續與災難恢復之能力。

五、 程式版本與弱點修補

1.確認作業系統及應用程式更新情況，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。

2.確認所有主機防毒軟體是否安裝以及更新狀況，未安裝與更新者應即時處理。

六、 資安意識宣導

1.強化相關人員網路安全認知，避免點選釣魚郵件，同時使員工具備保護數據資產、辨識安全威脅和高風險行為的能力。

2.針對網芳之共享資料夾建議盡量不使用，如要使用應設定密碼存取，避免遭惡意程式存取利用。

3.宣導若發現疑似遭受勒索病毒感染時，應立即關閉電腦並切斷網路。

4.若發現疑似遭受勒索病毒感染時，建議重新安裝作業系統與應用程式，且確認已安裝至最新修補程式後，再還原備份的資料。備份資料在還原至電腦之前，應以防毒軟體檢查，確保沒有殘存的惡意程式。

5. 宣導同仁重要資料採用離線備份。

(資料來源:臺北市政府資訊局)

公事家辦之風險暨春節期間加強注意事項

一、案情概述

「公事家辦無人問，一旦洩密天下知」某政府機關主管習慣將經手（包含屬下陳核及 其他課室會辦文件）公文之電子檔拷貝留存備用，並經常以隨身碟再將其拷貝至家中電腦硬碟儲存運用。孰料，其家用電腦早遭駭客植入後門程式而不 自知，以致長期大量經手之機密文書陸續外洩，直至情治單位查獲上情且依法偵辦時，方知事態嚴重卻為時已晚。事發後某民意代表召開記者會對其所屬機關嚴 詞抨擊，經各媒體大幅報導，損害政府機關形象。

二、案例解析

近年資訊安全漸獲各政府機關之重視，相繼購置更新資訊系統之防火牆及防毒軟體等設備，並加 強實施各項資訊稽核、宣導及訓練，因此各機關資 訊系統之防護能力也相對提昇。然而，公務員將公事攜回家中處理之情形仍屢 見不鮮，惟家中個人電腦畢竟防護力較低，且與其他成員共用容易遭駭客入侵而不自知。 本案中該主管私下將機密文書攜離辦公處所，實已具行政責任，嗣因家中電腦遭駭客入侵致機密文書外洩，更須負刑事責任，對機密維護及機關形象造成極大之傷害。

三、相關法規

(一)文書處理手冊第76點第7項「一般保密事項規定如下：(七) ...因職務而持有之機密文書，應保存於辦公處所，並隨時檢查，無繼續保存之必要者，應繳 還原發單位；無法繳回者應銷毀之。」

(二)刑法第132條第1、2項「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品 者，處3年以下有期徒刑、拘役或3百元以下罰金。 因過失犯前項之罪者，處1年以下有期徒刑、拘役或3百元以下罰金。」

(三)個人資料保護法第18條「公務機關保有個人資料檔 案者，應指定專人辦理安全維護事項，防止個人資 料被竊取、竄改、毀損、滅失或洩漏。」

(接續次頁)

四、策進作為

由本案例可知，無論係故意或過失洩漏公務機密，其所承擔之刑事責任及行政責任皆極為沈重。 如今網路駭客無所不在，防不勝防，而電腦、網路又係現今不可或缺的公務必需品，因此更應審 慎使用。如需另為備份時，請以光碟燒錄儲存，勿將檔案資料暫存於家用電腦中，以防止駭客入侵竊取機密資料，導致須背負洩漏公務機密之罪責。

五、春節期間加強注意事項

(一)加強注意保密規定，公務機密資料非經權責主管人員核准，不得複製及攜出辦公處所，且切勿將機敏公文存於隨身碟攜回家中辦理。

(二)實施公文收發、檔案管理稽核抽查作業，並針對機密文書傳遞過程可能產生疏漏環節，加強維護措施。

(三)保密通訊設備應實施檢核，機敏文件內容應避免電子傳輸，以杜絕公務機密外洩情事。

(四)就電腦週邊設備實施保密安全檢查，積極蒐報網路安全情資及影響國家安全之資安事件，加強資 安宣導及檢測。

(五)機關資訊部門請加強委外廠商之監督，並注意連續假日期間電腦機房門禁管制措施及監視設備是 否正常。

(六)遇有重大資安異常案件，應立即通報資訊單位，並循行政院國家資通安全會報資安事件通報應變 作業流程辦理。

(七)遇有重大疑似洩漏一般公務機密案件，應立即查明洩密管道，迅謀補救，防堵危害擴大。

(資料來源:花蓮縣政府消防局)

情書

壹、案例故事

添財是泰國人，在102年的時候以移工名義來臺工作並且居留，但是後來在104年間，因為不滿雇主的管理方式，添財未告知雇主就自己離開了服務處所，並且一直在外違法打工。移民署依照雇主的通報，將添財註參為行方不明，再依勞動部廢止聘僱公文，廢止了居留許可。添財在外違法工作期間，結交了一名同樣是在臺灣工作的泰國籍女友，兩人經過2年交往，互相扶持，情深義重。後來在106年間，添財女友不幸車禍住院，添財又遭到移民署查獲歸案，添財因為是失聯移工身分，所以被依規定收容在收容所，等待遣返出國。添財難擋對女友思念之情，遂寫了一封充滿愛意的情書給女友，並交由收容所寄發，收容所專責管理人員阿華因為深諳泰文，開拆信件檢查，並利用檢查添財信件時機，細細閱讀情書內容，事後不斷向人稱讚添財文情並茂。添財得知收容所專責管理人員將自己信件開拆並充分閱讀，心中不斷納悶，管理人員閱讀收容人信件，是對收容人隱私權的嚴重侵害，管理人員詳細閱讀自己信件之行為是否合法？臺灣法令對此有無相關規 定？

貳、爭點

管理人員檢查收容人信件，是否包括詳細閱讀信件內容？在何種條件下才能詳細閱讀信件內容？添財如對管理人員閱讀其信件一事不服，有無相關救濟管道，以避免日後寫的情書再被他人閱覽？

參、人權指標

一、《公民與政治權利國際公約》第17條第1項規定，任何人之私生活、家庭、住宅或通信，不得無理或非法 侵擾，其名譽及信用，亦不得非法破壞。

二、《公民與政治權利國際公約》第2條第3項第 1 款規定，確保任何人所享本公約之權利或自由如遭受侵害，均獲有效之救濟，公務員執行職務所犯之侵權行為，亦不例外。

(接續次頁)

肆、國家義務

一、各締約國的報告往往都沒有顧及締約國都必須保證「在其領土內和受其管轄的一切個人，都享有《公民與政治權利國際公約》所承認的權利。一般而言，本公約所訂各項權利適用於每個人，不論國家間對等原則，亦不論該個人的國籍或無國籍身分(人權事務委員會第15號一般性意見第1段)。

二、各締約國在其報告內應該注意外國人的法定地位和實際地位。《公民與政治權利國際公約》已在內載的權利方面給予外國人一切保護；各締約國在其立法上和實踐上均應適當遵守本公約的規定。這樣才能大大改善外國人的地位。各締約國均應確保在其管轄範圍內的外國人都能知道本公約的條款和所規定的權利 (人權事務委員會第15號一般性意見第4段)。

伍、解析

依據內政部移民署「寄發受收容人書信標準作業流程」 規定，受收容人申請寄發中文書信由收容區管理員實施檢查、外文書信則轉請戒護人員洽通譯協助譯讀檢查後陳報執勤官複檢。書信內容經檢查有妨害管理秩序或收容安全之虞者，不予寄發。又內政部移民署「收容管理工作手冊」規定，一般書信、賀卡由專責管理人員初審送收容管理中心（專勤隊）執勤官複審後，造冊登記寄發，檢查內容應注意有無消極厭世、脫逃意圖、所內勤務安排、舍房位置或妨害單位信譽及影響戒護安全等情形。準此，案例中收容所專責管理人員阿華，利用檢查添財信件有無自戕、脫逃傾向及洩漏機敏資訊之時機，仔細閱讀添財的情書內容，似難謂違反上開規定。

(接續次頁)

又依監獄行刑法第74條第1項及第2項規定：「受刑人寄發及收受之書信，監獄人員得開拆或以其他適當方式檢查有無夾藏違禁物品。前項情形，除法律另有規定外， 有下列各款情形之一者，監獄人員得閱讀其書信內容。但屬受刑人與其律師、辯護人或公務機關互通之書信，不在此限：1、受刑人有妨害監獄秩序或安全之行為，尚在調查中。2、受刑人於受懲罰期間內。3、有事實而合理懷疑受刑人有脫逃之虞。4、有事實而合理懷疑有意圖加害或騷擾他人之虞。5、矯正機關收容人間互通之書信。6、有事實而合理懷疑有危害監獄安全或秩序之虞。」，依司法院釋字第756號解釋意旨，監獄未斟酌受刑人個案情形，一律閱讀書信之內容，顯已對受刑人及其收發書信之相對人之秘密通訊自由，造成過度之限制。故修正草案第74條第2項明定有該條項各款情形之一者，監獄人員始得閱讀書信內 容，以符比例原則。

綜上所述，依據監獄行刑法第74條第1項及第2項規定，監獄人員對於受刑人寄發之信件原則上僅得「檢查有無夾藏違禁物品」；倘受刑人信件有同法第74條第2項各款規定之情形時，監獄人員方得閱讀受刑人之書信內容。在監獄服刑之受刑人，尚受有秘密通訊自由之保障，則受收容處分之外國人，更無剝奪其通信隱私權之理。是以內政部移民署似應修正收容相關法令，規範收容管理人員閱讀收容人寄發信件內容之時機及要件，以確保受容人之秘密通訊自由。

(資料來源:內政部移民署108年人權教材)

泰國列入非洲豬瘟疫區 海關強化邊境查緝防範疫情

財政部關務署表示，根據非洲豬瘟中央災害應變中心最新消息，泰國政府於111年1月11日宣布發現非洲豬瘟，歐洲地區之義大利及北馬其頓也在近日確認發生非洲豬瘟。面對國際疫情蔓延，且農曆春節即將到來，海關持續加強查驗來自非洲豬瘟疫區等高風險國家之貨物、郵包及旅客行李，與行政院農業委員會動植物防疫檢疫局(下稱防檢局)等查緝機關強化合作，阻絕疫情於境外。

關務署指出，海關自110年8月24日至111年1月10日，查獲並經防檢局確定為豬肉製品計527件569.489公斤。以運輸管道區分，郵包查獲437件418.882公斤最多，其次為空運快遞貨物查獲52件131.897公斤。以查獲來源地區分，則以中國大陸(含香港)查獲304件268.976公斤最多，其次為泰國查獲94件94.974公斤。查獲物品以豬肉香腸、月餅等含豬肉烘培製品及炸豬皮為大宗。

關務署強調，海關近三年來於中秋及春節前查獲豬肉製品件數及數量均明顯增加，且自110年12月中迄今已連續查獲3件泰國進口郵包夾藏豬肉香腸，移送防檢局檢驗確認帶有非洲豬瘟病毒。為因應疫情威脅加劇，海關持續與中華郵政合作將泰國、越南及中國大陸等自疫區等高風險來源地進口郵包分流查核，落實執行100%X光檢視，並於春節前加強郵包查驗比率，如查獲豬肉製品等應施檢疫物，均移送防檢局依動物傳染病防治條例相關規定處分。

關務署籲請民眾不要上網購買境外肉製品等應施檢疫物，自國外返鄉探親也不要攜帶應施檢疫物，更要提醒境外親友絕對不能寄送含應施檢疫物之快遞或郵包。民眾如收到郵遞寄送輸入之應施檢疫物，應即送交防檢局及其轄區分局銷毀，未送交者將依動物傳染病防治條例第45條規定，處以新臺幣3萬元以上15萬元以下罰鍰。請勿以身試法，全民共同守護臺灣農畜產業。

(資料來源:行政院消費保護會)

泰國列入非洲豬瘟疫區
海關強化邊境查緝防範疫情

海關將持續與防檢局及中華郵政合作，加強查緝非洲豬瘟疫區等高風險國家進口貨物、郵包及入境旅客行李，請民眾勿以身試法。

(資料來源：財政部關務署)

嘟～

嘟～

嘟～

喂～老公～
郵差送來一個包裹，說是高級洋酒，寄件人是「一路發資訊有限公司」，可是我不認識什麼一路發啊，是你業務往來對象嗎？

對！老婆～
快，郵差還在嗎？
趕快退回，這不能收。

為什麼？
看起來很不錯，而且是署名給我的，有關係嗎？

1 2
3 4

一旦收了，你老公就要丟飯碗啦！
公務員和他的配偶，是不能收受相關業務往來對象的禮物啊。

公務員應依法公正執行職務，不得收受與其職務有利害關係者之餽贈，除有公務員廉政倫理規範第4條所訂例外情形，且係偶發而無影響特定權利義務之虞時，才得例外收受。並應於受贈日起3日內，簽報長官，及知會政風機構。

蛤～
那我趕快退回去。
郵差先生～
郵差先生～等一下～

內政部移民署
政風室關心您

飲宴應酬應避免
利害關係不參加
受贈財物想仔細
知會政風免爭議

內政部移民署政風室　關心您

政風電子報

刊名 / 政風電子報
出版機關 / 內政部移民署政風室
地址 / 10066臺北市中正區廣州街15號7F
出版年時間 / 中華民國111年1月
頻率 / 月刊
編輯總召 /卓明偉
主編 / 簡國樑
本室編輯小組 /張文山、 陳安莉、蘇承玉、蔡雅雯、
謝瑋哲