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。

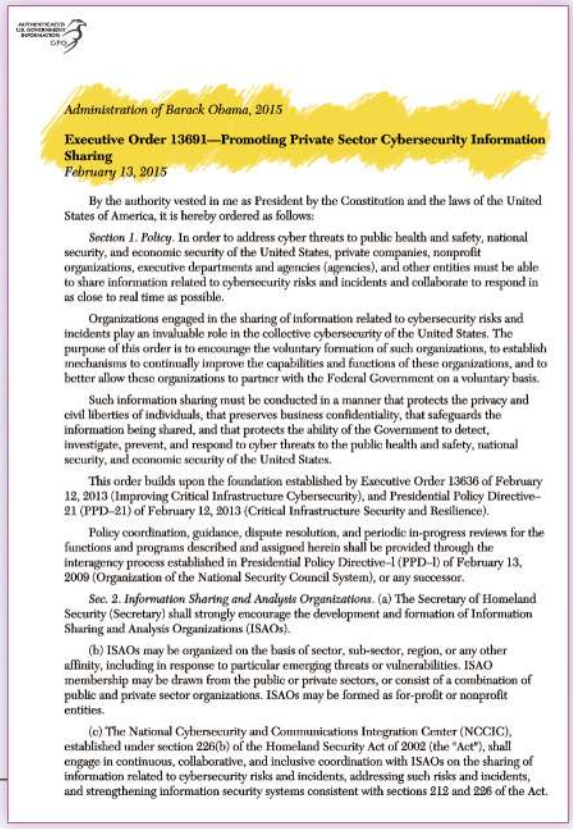
情資共享目的在於提升網路安全

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。



Administration of Barack Obama, 2015

Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing

February 13, 2015

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive–21 (PPD–21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 (PPD–1) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

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]？

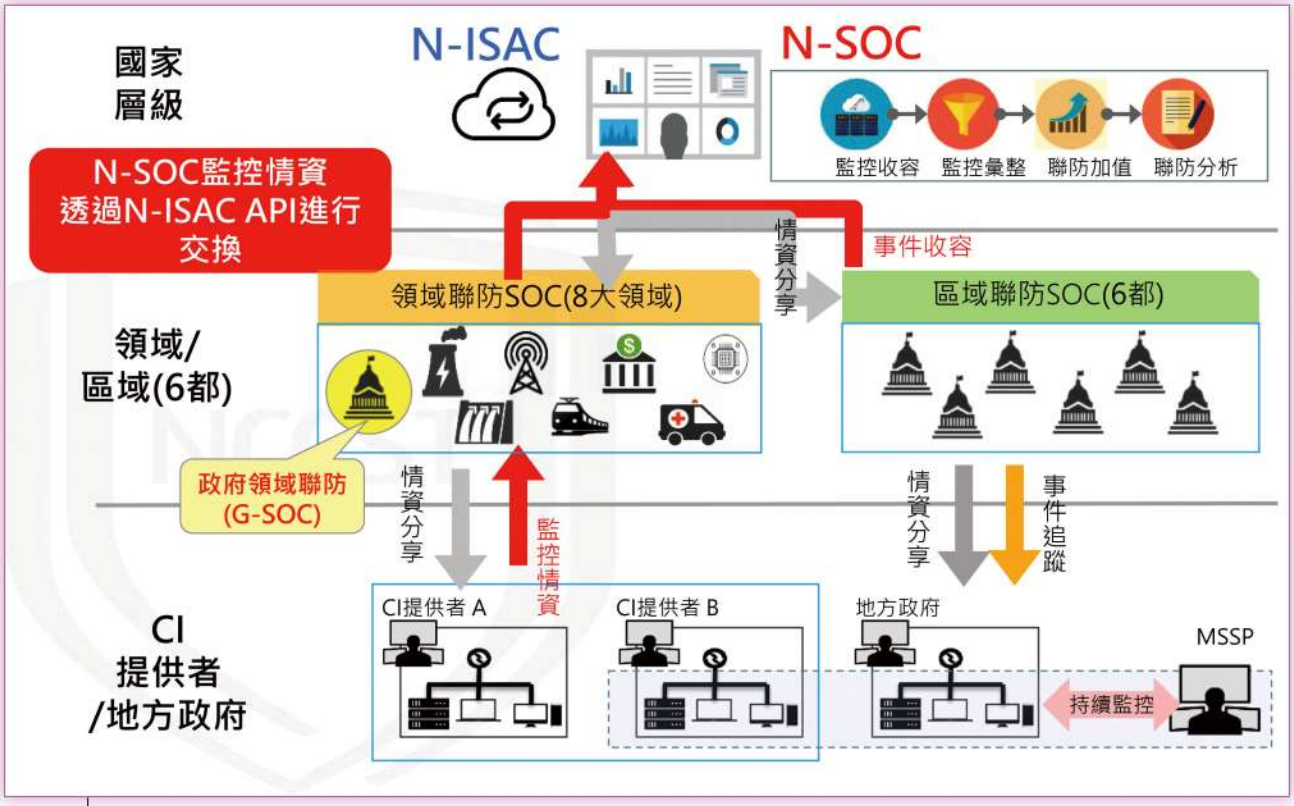
四、社群組織會員如何獲得分享情資[2]？

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，及盤點現有的技術來達成能快速分享「威脅指標」的目標。



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月掛牌，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。

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。

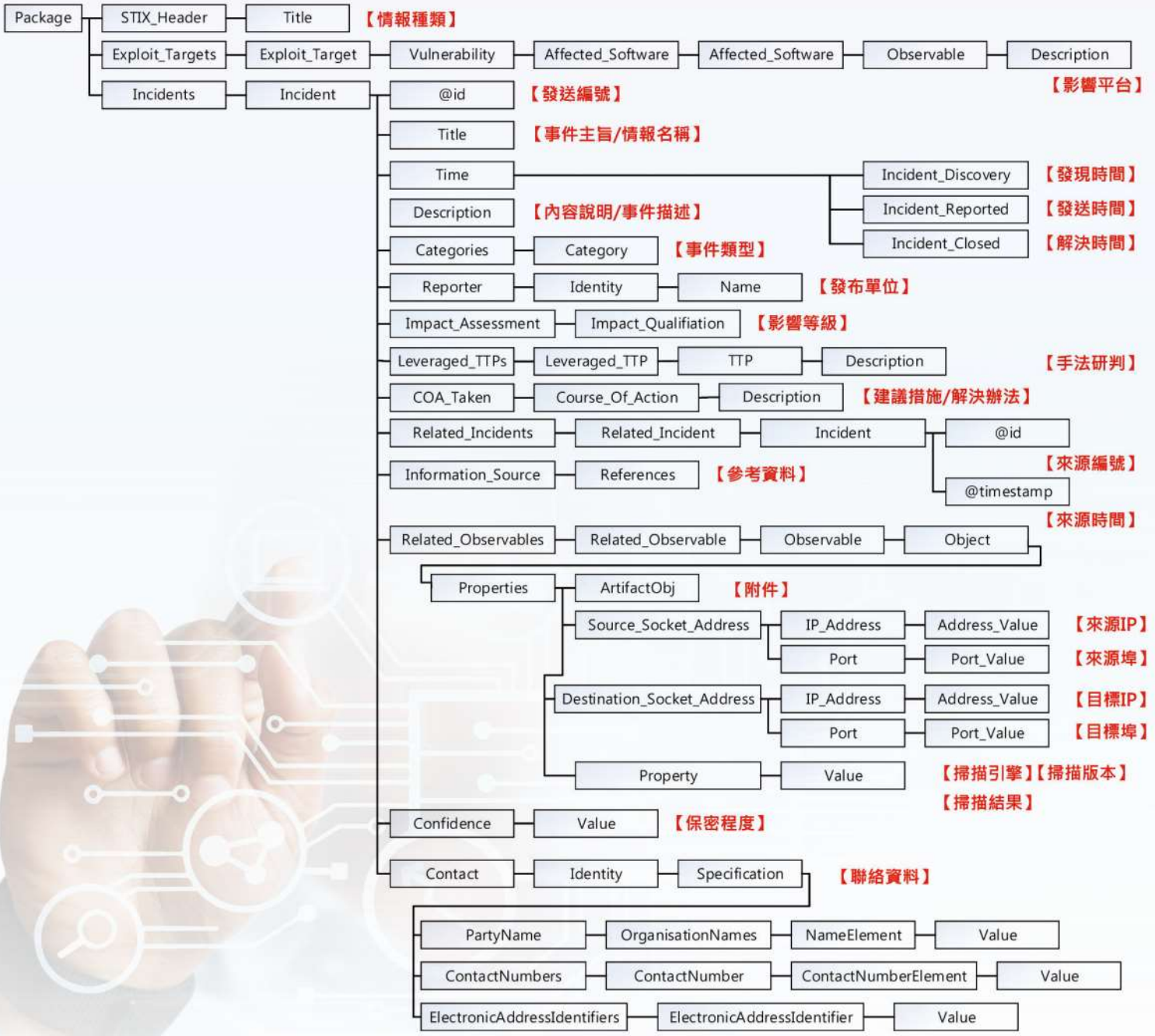
[6] 包含疑似存在系統弱點或可疑程式、疑似進行惡意或攻擊行為與進行可疑連線行為或活動。

[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 月正式運作。



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）

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。

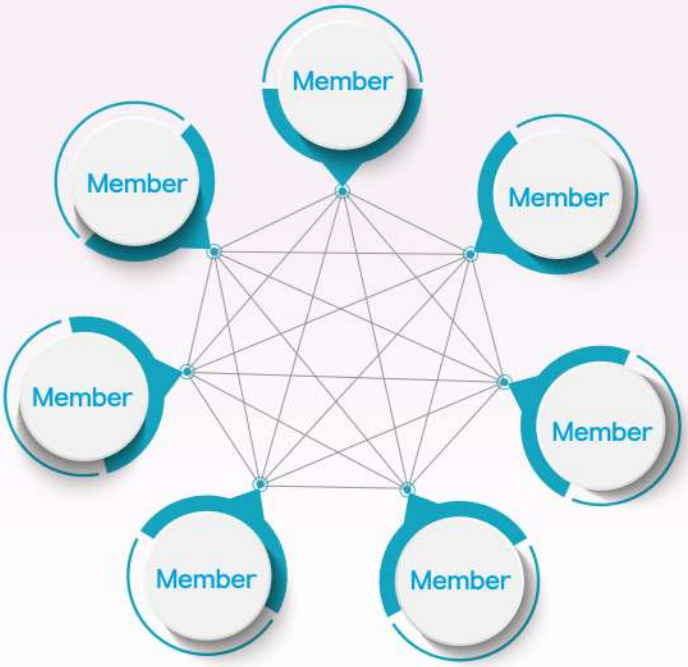


圖 2　點對點情資分享模式

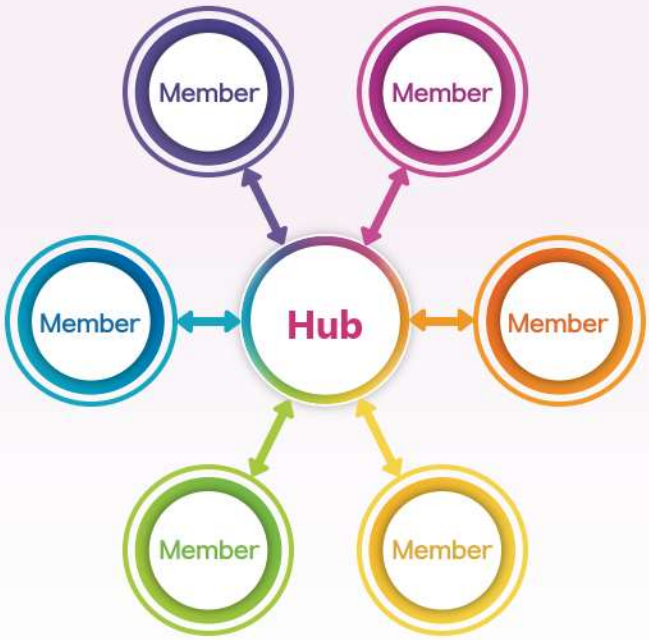


圖 3　軸輻型情資分享模式

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。

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。

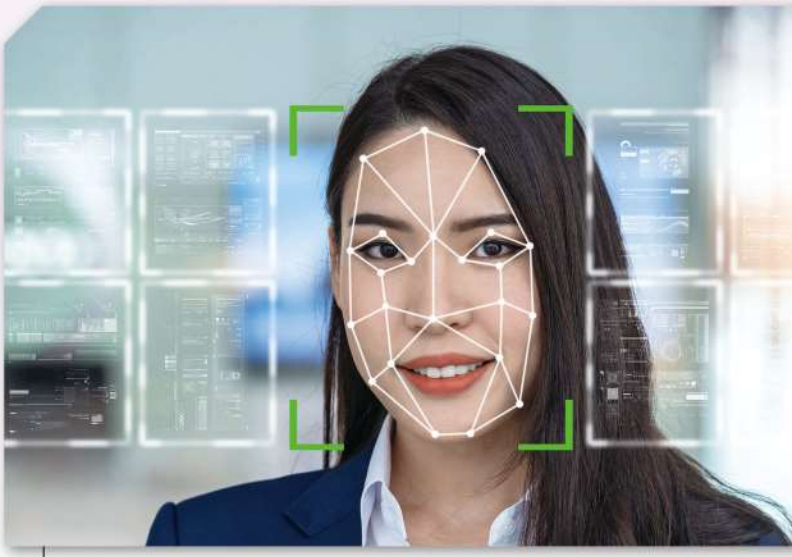
二、需評估因與資安威脅模式有關的個資外洩所造成之影響。當資安威脅模式為個人識別資訊（Personally Identifiable Information, PII）時，需判斷此個人識別資訊是否與資安威脅有關，以及 ISAO 或其成員是否視需要刪除相關個資。

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。