106年

國家資通安全防護整合服務計畫

領域CERT實務建置指引

(V1.0)

中華民國106年3月

修訂歷史紀錄表

項次	計畫資訊			發行紀錄		說明
	年度	版次	修訂日期	版次	日期	
1	106	V1.0	106/3	V1.0	106/3	新編
2						
3						

資料來源：技服中心整理

目　次

圖 目 次

表 目 次

1. 前言

為了落實推動國家關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)，特制定領域電腦緊急應變團隊(Computer Emergency Response Team, CERT)實務建置指引，作為關鍵基礎設施領域層級與關鍵基礎設施提供者，於執行領域 CERT 建置與維運的作業參考。各領域層級可依循本指引，再根據各領域特性，調整為各領域實務上適用的規範。

1.1. 目的

CERT 主要目的係針對資安事件提供緊急應變與處置，以降低資安事件發生時伴隨的損害，儘速恢復正常營運；同時，建立跨體系之整合運作機制，提供完備的通報機制，以期防範未來可能的資安事件。

綜觀國際上 CERT 發展，因莫里斯蠕蟲大規模感染，影響全球百分之十的網際網路系統後，了解資安事件處理需藉由專家組織緊急合作協調與應變，美國聯邦政府於 1988 年資助成立第一個電腦緊急應變團隊 CERT® Coordination Center(CERT/CC)，並由卡耐基大學負責營運，目的在於針對資安事件協助緊急應變、協助其他組織建立電腦緊急應變團隊及擔任協調中心進行資訊分享，陸續其他國家亦紛紛效法成立電腦緊急應變團隊。2003 年美國國土安全部成立 US-CERT，建立國家體系之預警系統，以強化國家資安事件緊急應變與協調能力，並於 2006 年起定期執行政府機關與私人產業大規模演練，稱為網路風暴(Cyber Storm)演習，其中演練範圍包括能源、交通及電信等關鍵基礎建置，顯見網路威脅已擴大至關鍵基礎設施。

我國於民國 90 年成立「行政院國家資通安全會報」，積極推動我國資通安全基礎建設工作，建立國家層級之資訊安全指揮機制，推動政府機關(構)對於資訊安全管理共識，以提升國家整體資訊安全品質，並於民國 92 年建立通報系統，以達成及時資安事件通報，強化通報應變機制。鑒於 CERT

的重要性，我國政府陸續成立相關組織，包括台灣電腦網路危機處理暨協調中心(TWCERT/CC)、政府網路危機處理中心(GSN-CERT/CC)、國家電腦事件處理中心(TWNCERT)、國家資通安全應變中心(NCERT)、國家通訊傳播委員會電腦危機處理中心(NCC-CERT)及經濟部電子商務資安通報服務中心(EC-CERT)，並擴及教育機構台灣學術網路危機處理中心(TACERT)等領域，其目的在於針對資安事件能即時做出對應的處置，彼此交換訊息以達到區域聯防的效果。

根據各國關鍵基礎設施處理經驗與評估，網路威脅已擴及關鍵基礎設施，且其資安事件影響範圍廣泛，未來仰賴各領域間公私部門的合作，以強化整體資安事件的防護與應變。此外，為利於領域內的 CERT、SOC 及 ISAC 的協同合作，需建立信任的傳輸管道與統一的交換格式，以提升資訊交流，因此各領域建立關鍵基礎設施領域 CERT 有助於迅速通報及緊急應變處置。

1.2.適用對象

本指引適用對象為行政院「國家資通安全會報」於網際防護體系下設「關鍵資訊基礎設施安全管理組」，並依 8 大領域區分之主政機關，詳見圖 1。

如有建置領域 CERT 需求之政府機關(構)或民間企業組織，亦可使用本指引做為建置領域 CERT 之參考資料。

●8 大領域，共計 7 個主政機關

– 通訊傳播分組，主政機關：通傳會

– 衛生醫療分組，主政機關：衛福部

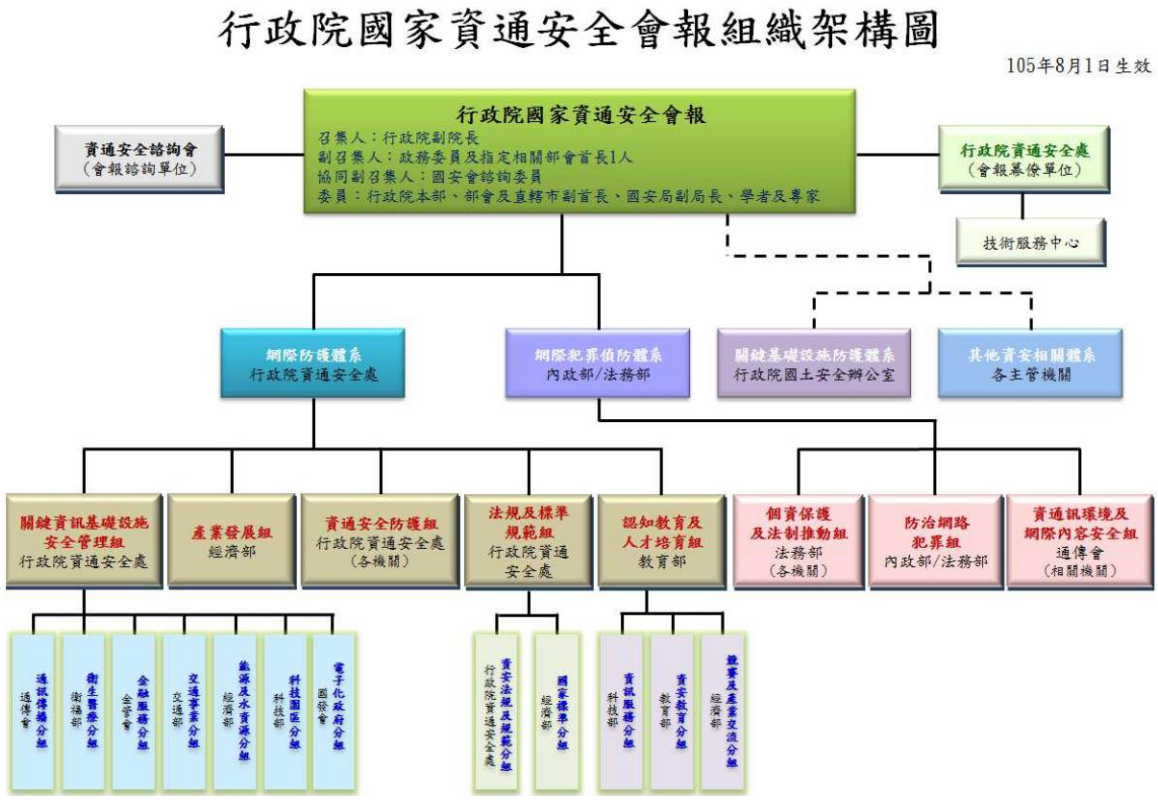
– 金融服務分組，主政機關：金管會

– 交通事業分組，主政機關：交通部

– 能源及水資源分組，主政機關：經濟部

– 科技園區分組，主政機關：科技部

– 電子化政府分組，主政機關：國發會

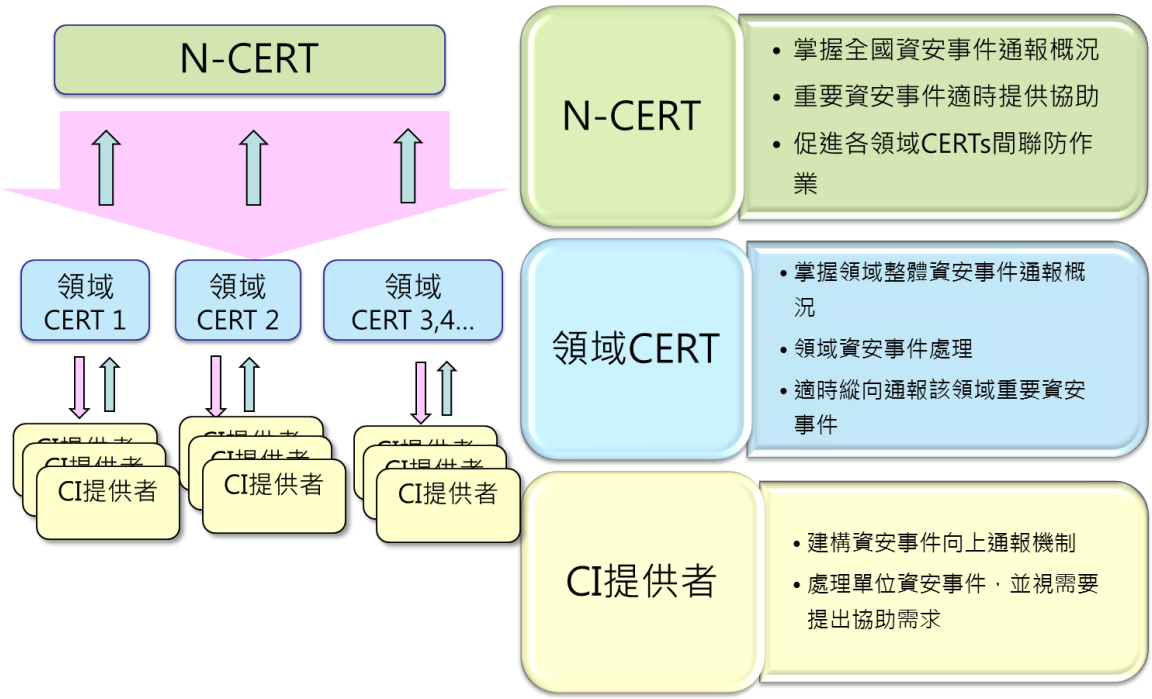


資料來源：行政院國家資通安全會報[3]

圖1　行政院國家資通安全會報組織架構

2. 角色權責與分工

配合我國關鍵資訊基礎設施保護基本政策，其所要求關鍵資訊基礎設施保護原則，規劃 CERT 體系將分為國家層級(N-CERT)、各 CI 領域層級(領域 CERT)及 CI 提供者層級(CI 提供者)等 3 個階層，CERT 體系角色與分工詳見圖 2。



資料來源：技服中心整理

圖2　角色權責與分工示意圖

2.1. 國家層級(N-CERT)

國家層級 N-CERT 目的係統整各領域 CERT 通報情況，以掌握全國資安事件，並針對重要資安事件適時提供協助處理，促進各領域 CERT 間聯防作業。

2.2.各 CI 領域層級(各領域 CERT)

各領域 CERT 由關鍵基礎設施領域層級主責,以協助領域內資安事件處理，掌握領域內整體資安事件通報概況，適時縱向通報該領域重要資安事件。

2.3.各 CI 提供者層級(事件通報單位)

關鍵基礎設施領域提供者應掌握單位內資安事件，建構資安事件向上通報機制，處理單位資安事件，並視需要提出協助需求。

3. 建置實務

本指引將以領域 CERT 之建置作業為模型，逐步說明建置 CERT 之參考步驟，以 Plan-Do-Check-Act(PDCA)循環之各階段作業項目進行，詳見圖 3。

●規劃階段(Plan)

領域 CERT 應規劃建置團隊，確認領域 CERT 之服務項目與內容，並擬定建置計畫。

●執行階段(Do)

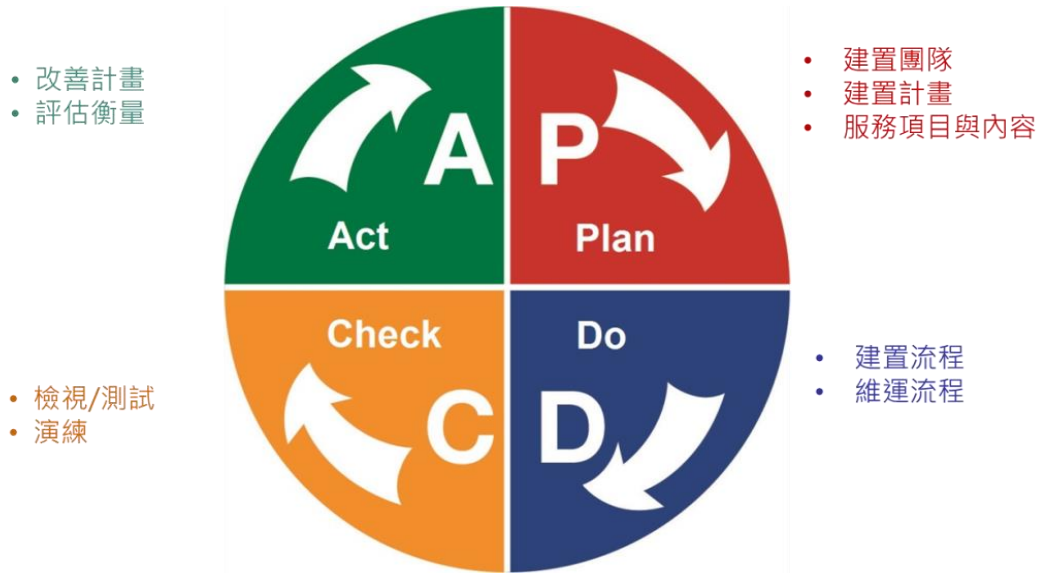
領域 CERT 應就建置時期與後續維運作業，訂定與實作相關規範與作業程序。

●查核階段(Check)

領域 CERT 應訂定檢視與測試相關程序，並定期執行。此外，應落實業務項目之演練作業，以利執行人員熟悉相關作業項目與程序。

●改善階段(Act)

領域 CERT 應規範管理審查機制，確保領域 CERT 之運作符合預期目標。此外，應依據管理審查內容訂定改善計畫，並落實追蹤。



資料來源：技服中心整理

圖3　PDCA 建置循環

3.1.規劃階段

本指引將以領域 CERT 為適用對象，依建置需求進行各項規劃事項說明。

3.1.1. 建置團隊

建置領域 CERT 應組成明確之建置團隊，並定義成員角色與職掌，以利後續建置規劃與控管工作。其組成可參考 CERT 建置團隊參考架構，詳見圖 4，建議建置團隊應包含決策管理、建置執行及執行查核等分組，分別說明如下：

●決策管理

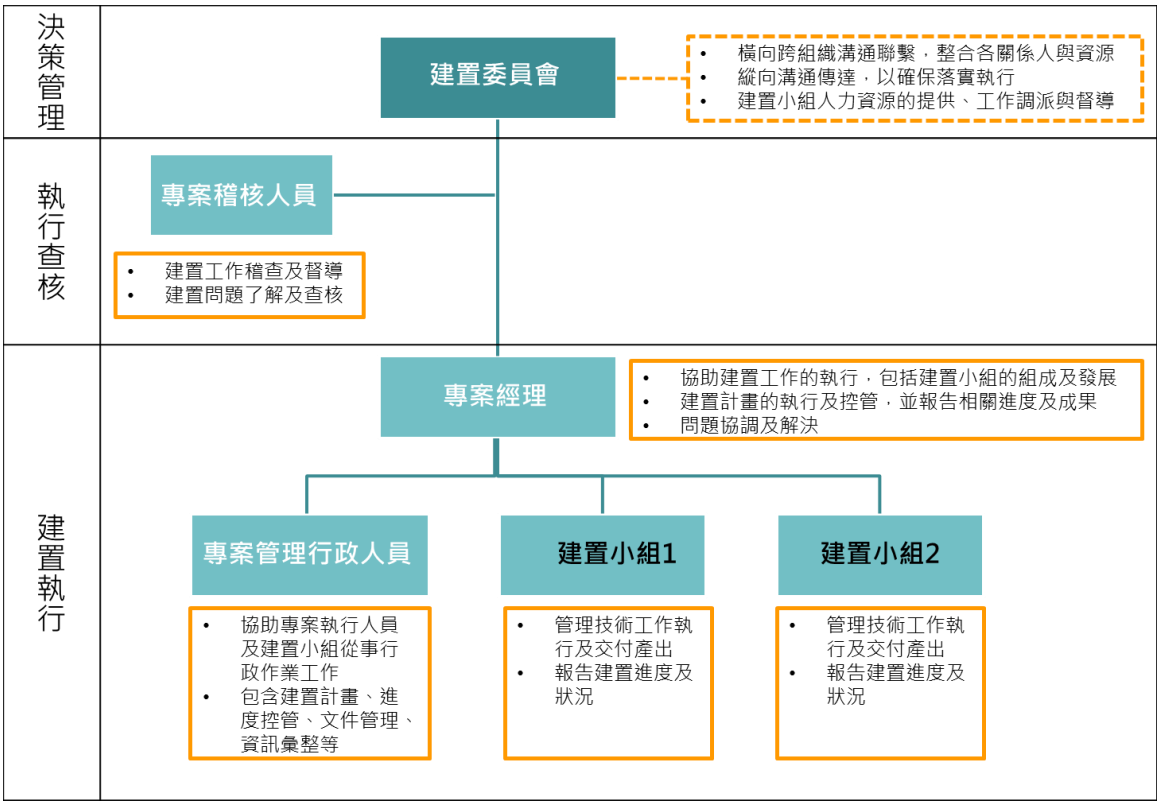
決策管理應包含領域關鍵角色代表，以確保建置方向與後續運作均符合目的需求。透過良好的協調機制(如定期召開會議)，以促進橫向跨組織的聯繫，整合各關係人與資源，並縱向溝通傳達確保落實情形。

●執行查核

藉由稽核人員於建置過程適時稽查及督導，以確保建置過程執行方向並符合相關法規規範。

●建置執行

實際執行建置計畫人員並依工作項目分組，適時報告執行進度及狀況。



資料來源：技服中心整理

圖4　CERT 建置團隊參考架構

3.1.2. 建置計畫

建置領域 CERT 應先進行需求分析，以了解所在 CI 領域之業務對於資安事件通報的相關需求，以妥善配置相關資源。

3.1.2.1. 需求分析

藉由內/外部環境分析了解組織外部環境對於資安事件通報的相關需求，並識別與分析和組織間往來活動之外部利害關係人，確認組織內部現行資安事件通報有關的管理制度內容、應用範圍、單位或人員等資訊。

●環境分析

– 外部環境分析：確認外部法規資安事件通報標準與原則，以符合相關規範。為掌握我國政府機關及公民營事業機構資安事件，行政院於 98 年 2 月 5 日頒布「國家資通安全通報應變作業綱要」[2]，以期迅速通報及緊急應變處置。為強化公私協同合作機制，並擴展至關鍵基礎設施的提供者，建議可參考現行制度「國家資通安全通報應變作業綱要」制定通報應變機制，並詳見「政府機關（構）資通安全責任等級分級作業規定」[4]及「資訊系統分級與資安防護基礎作業規定」[7]作為評估原則。

– 內部環境分析：確認內部現行制度，評估調整需求。部分領域層級已陸續或已建置 CERT 機制，包括建構縱向資安通報機制與橫向資安共同聯防，評估項目包括但不限於內部資安通報應變平台功能擴充之必要性、縱向資安通報機制、現行適用範圍、資安事件影響等級及資安事件應變處理，是否符合或相容國家資通安全通報應變作業綱要。

●領域 CERT 有關之利害關係人清單

依據關鍵基礎設施範圍，盤點 CERT 領域有關之利害關係人清單，以政府領域縱向資安通報機制為例，採階層式管理包括各級政府機關通報人、協助事件處理之 CI 領域層級及掌握所有政府機關資安事件之行政院國家資通安全會報 3 階層。此外，政府機關遵循行政院國家資通安全會報制訂之「政府機關（構）資通安全責任等級分級作業規定」[4]，針對政府機關、學研機關(構)及各事業分組進行分級，以評估通報範圍，若為基層業務單純者，則由上層機關代為執行通報作業。

●界定各領域內 CI 提供者服務範圍

領域CERT應就所識別之核心服務項目，檢視領域內業務項目或服務流程，以釐清劃分服務範圍與對象，俾利 CI 領域內之 CI 提供者遵循。服務項目可參考 CERT 服務項目表，詳見表 1。

表1　CERT 服務項目表

服務作業項目	國家層級 (N-CERT)	各領域 CI 層級 (領域 CERT)	各 CI 提供者層級 (CI 提供者)
資安事件通報	必要項目	必要項目	必要項目
協助資安事件處理	必要項目	必要項目	配合事件處理
建置平台接收通報	必要項目	必要項目	-
辦理通報演練	必要項目	可選擇項目	-
辦理教育訓練	可選擇項目	可選擇項目	-

資料來源：技服中心整理

彙整內外部環境與利害關係人之分析結果，擬定建置 CERT 應辦事項。建置 CERT 應辦事項，詳見表 2。

表2　建置 CERT 應辦事項

應辦事項	說明
建立資安事件通報程序	CI 提供者發生資安事件時，須向領域 CERT 進行通報。事件等級建議詳見國家資通安全通報應變作業綱要等級劃分原則，依「機密性」、「完整性」及「可用性」由輕至重分為 1 至 4 級資安事件。若該筆資安事件為 3、4 級資安事件，領域 CERT 須上報至國家層級 N-CERT。
建立資安事件處理程序	CI 提供者發生資安事件時，若需請求外部技術支

應辦事項	說明
	援，領域 CERT 得視需求提供事件處理協助。若該筆資安事件為 3、4 級資安事件，且領域 CERT 需外部協助，可向國家層級 N-CERT 申請支援。
CI 提供者資料維護管理	領域 CERT 需提供管道供 CI 提供者進行資料維護與更新。
建立資安事件通報平台	領域 CERT 應建置自動化平台，以協助管理資安事件通報、事件處理及 CI 提供者資料維護。

資料來源：技服中心整理

3.1.2.2. 建置資源

依據需求分析結果，領域 CERT 業務項目應包含事件通報管理、事件處理管理、教育訓練管理及 CERT 平台維運/開發管理，領域 CERT 建置維運組織參考架構詳見圖 5，說明如下：

●事件通報管理

事件通報管理需維護事件通報內容與 CI 提供者聯繫資料之正確性與完整性，並提供諮詢服務以協助 CI 提供者解決問題，相關說明如下：

– 事件通報

領域 CERT 負責接收 CI 提供者資安事件通報，並追蹤了解事件處理情形。當接獲 CI 提供者通報 3、4 級事件時，應通報至國家層級 N-CERT，以協助 N-CERT 及時掌握重要資安事件並適時提供協助。

– CI 提供者資料維護

領域 CERT 應維護 CERT 平台帳號使用與管理，審視 CI 提供者帳號申請資料，並不定期檢視資料正確性，確保聯繫管道暢通以完備通報機

制。

– 諮詢服務

領域 CERT 應設置諮詢管道，提供 CI 提供者詢問相關資安事件或通報應變問題，以協助 CI 提供者解決問題。服務執行時間可評估資源與執行情形，以排班制安排 7x24 制或 5x8 制。

●事件處理管理

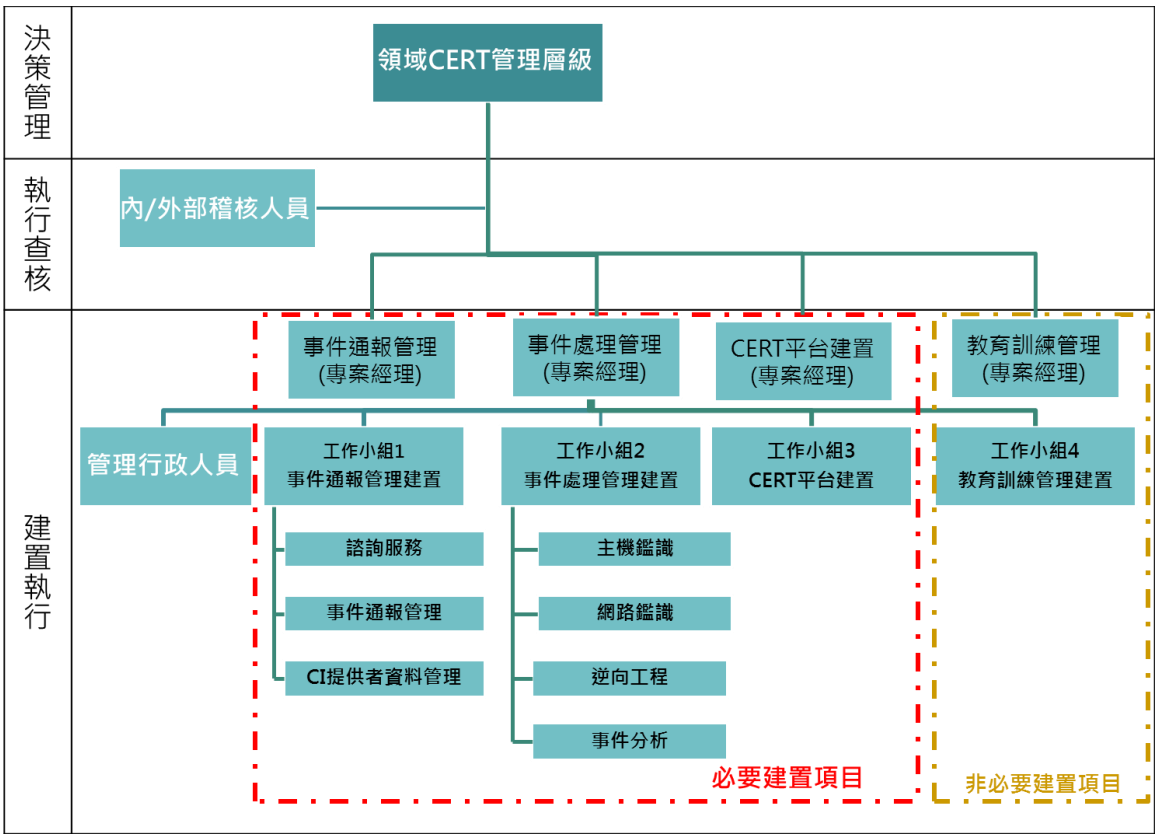
事件處理人員依據鑑識範疇，基本需涵蓋主機鑑識人員、網路鑑識人員及逆向工程人員，進行相關數位鑑識資料蒐集與分析，並由事件分析人員綜整各項分析結果，確認資安事件發生情形與影響範圍，提供補強建議與處置措施。服務執行時間可評估資源與執行情形，以排班制安排 7x24 制或 5x8 制。

●教育訓練管理

教育訓練人員主要以宣導或提升 CI 提供者資安意識，並教導 CERT 平台使用為主，適時進行政策宣導，以強化資安防護。

●平台維運/開發管理

平台維運/開發人員係當平台功能不敷需求或使用時，需進行調整與開發，以維持系統正常營運之可用性。



資料來源：技服中心整理

圖5　領域 CERT 建置維運組織參考架構

3.1.2.3. 規範與規格

建置領域 CERT 平台應制定信任的傳輸管道與統一的交換格式，並與領域 SOC、領域 ISAC 達到資訊交流，以完備領域 CERT、SOC 及 ISAC 間的協同合作，因此建議領域層級建置 CERT 平台可配合系統彈性，於系統建置時宜採用 Structured Threat Information eXpression(STIX)與 Trusted Automated eXchange of Indicator Information(TAXII)，以建置資安事件傳輸格式與傳輸架構。

●STIX

STIX 是標準結構化語言，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，並提供資安事件評估範例格式供開發者使用，詳見附件 4。STIX 情資除了便利封裝，能將情資進行儲存、傳遞、分享及分析，目前美國國土安全部旗下的資通安全辦公室(Office of Cybersecurity and Communications)、國家資通安全集成中心(National Cybersecurity and Communications Integration Center)及美國電腦緊急應變小組(US-CERT)目前正在使用其架構進行情資分享，也努力推廣架構與相關技術[11]。

●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。TAXII 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(Collection Management Service)，詳見附件 5。

3.1.2.4. 建置前準備

建置領域 CERT 應完成擬訂建置計畫，包含作業項目細部執行內容，並訂定各階段執行時程，工作項目範例請詳見表 3。

表3　工作項目執行表範例

工作項目		主責人員	執行時程	執行進度	產出項目
事件通報管理	定義通報範圍與準則			完成/未完成	通報作業要點
	定義通報機制中各角色權責			完成/未完成	
	定義通報項目與類別			完成/未完成	

工作項目		主責人員	執行時程	執行進度	產出項目
	建置諮詢服務管道			完成/未完成	諮詢服務管理程序
I 提供者資料建立/維護	CI 提供者盤點			完成/未完成	CI 提供者盤點清冊
	CI 提供者資料登錄/異動			完成/未完成	CI 提供者資料維護程序
事件處理	定義事件處理範圍			完成/未完成	事件處理程序
	組成團隊人員			完成/未完成	
	建置事件處理工具			完成/未完成	
CERT 平台建置	事件通報管理功能			完成/未完成	CERT 平台建置報告
	資安事件處理管理功能			完成/未完成	
	CI 提供者資料維護功能			完成/未完成	
	CERT 平台管理維護功能			完成/未完成	
	CERT 平台功能測試			完成/未完成	

資料來源：技服中心整理

3.1.3. 服務項目與內容

根據前述需求分析彙整之服務項目應包括核心服務有資安事件通報與資安事件處理；附加服務有通報演練與教育訓練，詳細內容可參考領域 CERT 服務項目說明表，詳見表 4。

表4　領域 CERT 服務項目說明表

類型	服務項目	說明
核心服務	資安事件通報	▪管理領域內資安事件，即時掌握轄下單位資安現況 ▪追蹤資安事件原因、處理進度及損害範圍
	資安事件處理	▪設置諮詢管道，提供防護建議，協助轄下單位進行事件處置 ▪視事件情形與需求，派員提供技術支援
附加服務	通報演練	▪強化轄下機關緊急應變、系統復原、協調管控等能力 ▪協助資安人員熟悉通報流程與平台 ▪確保轄下相關資安人員聯絡管道暢通，驗證人員資料正確性
	教育訓練	定期提供資安通報宣導，強化資安人員資安防護能量

資料來源：技服中心整理

3.2.執行階段

依建置計畫執行設計、建置、測試及上線營運等作業，進行各項執行事項說明。

3.2.1. 建置流程

建置領域 CERT 應考量工作項目之相依性，依序或併行工作執行順序，因此建議先行完成相關規範擬定與 CERT 通報平台，並公告至 CI 提供者使其有所遵循，以協助完備相關資料填寫。因此建置流程依序為建立通報機制、建立事件處理團隊、建立 CERT 通報平台及建立 CI 提供者資料維護機制，詳見圖 6。

資料來源：技服中心整理

圖6　領域 CERT 建置流程圖

●建立通報機制

領域CERT應制定通報作業要點相關文件與規範，說明其目的、適用範圍、通報管道、資安事件影響等級及通報內容，以供 CI 提供者遵循，詳見附件 1 與附件 2。

●建立事件處理團隊

領域 CERT 應建置事件處理團隊以協助 CI 提供者進行事件處理，定義事件處理範疇，依服務範疇組成或培訓團隊人員，並循事件處理流程進行電腦檢測，詳見附件 3。

●建立 CERT 通報平台

依循通報機制、CI 提供者資料建立/維護及事件處理之功能加以系統化，

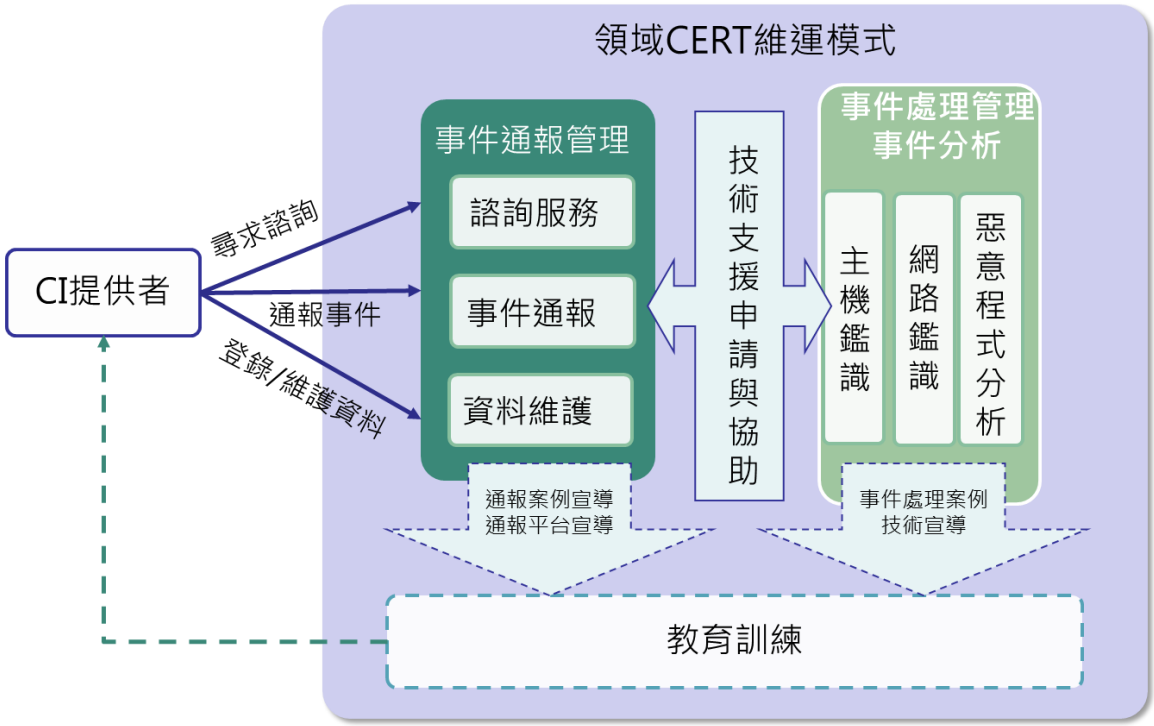
透過自動化平台協助通報管理、CI 提供者資料管理及事件支援管理，請詳見詳見附件 6。平台開發與測試可參考「安全軟體設計參考指引」[8]與「安全軟體測試參考指引」[9]，如有委外需求可參考「資訊作業委外安全參考指引」[10]。

●CI 提供者資料建立/維護

依照 CI 提供者盤點清冊確認資料登錄情形，應定期進行資料維護與確認，以確保資安事件發生時，能及時並正確傳達資訊。維護管道不限電話、紙本、電子郵件或建置系統自動化更新維護。

3.2.2. 維運流程

領域 CERT 主要藉由 CERT 通報平台接收與管理 CI 提供者事件通報與資料維護，並提供諮詢服務以協助 CI 提供者解決問題。當事件通報管理人員接獲 CI 提供者事件通報並提出技術支援申請時，得視事件需求，由事件處理人員提供技術支援協助事件處理，業務維運關係可詳見圖 7。



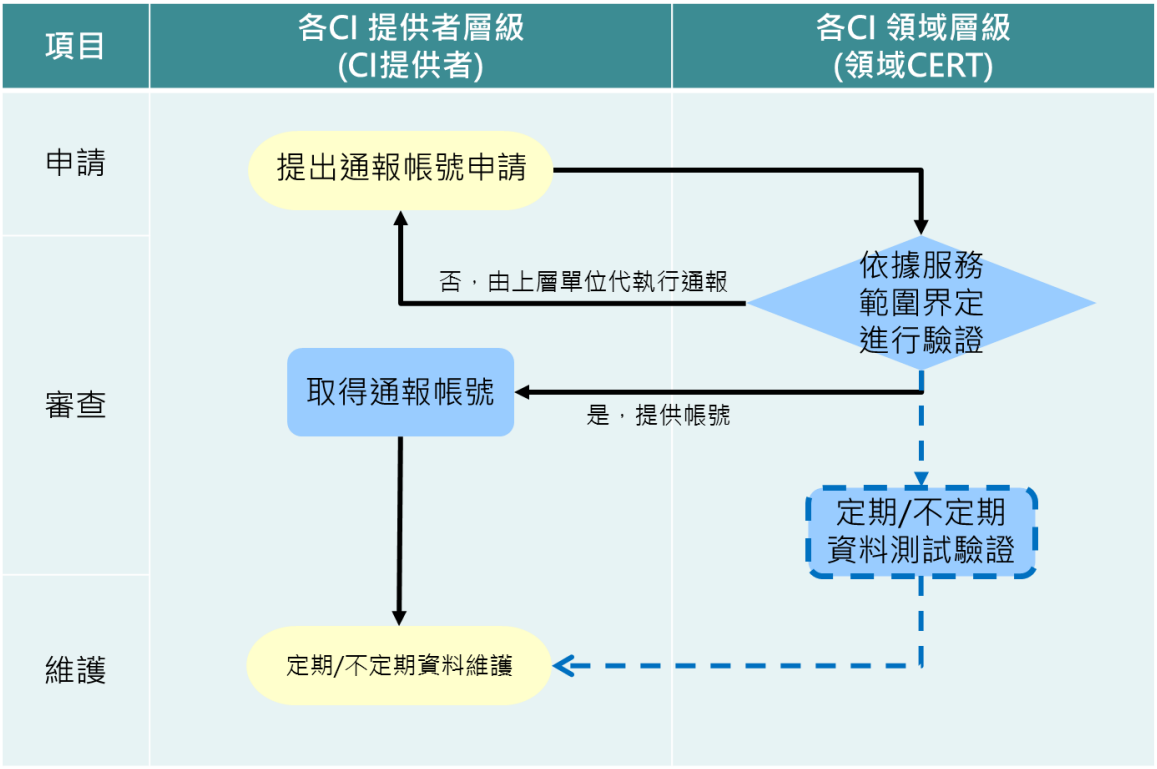
資料來源：技服中心整理

圖7　領域 CERT 維運模式示意圖

事件通報管理與事件處理管理主要維運項目分別為：CI 提供者資料申請與核定作業、事件通報管理程序及資安事件處理程序，說明如下：

●CI 提供者資料申請與核定作業

領域 CERT 應建立該領域 CERT 通報帳號申請管道，並定期確認 CI 提供者聯絡資料正確性與完整性，落實 CI 提供者登錄情形，以完善通報機制詳見圖 8。



資料來源：技服中心整理

圖8　CI 提供者資料申請與核定作業示意圖

●事件通報管理程序

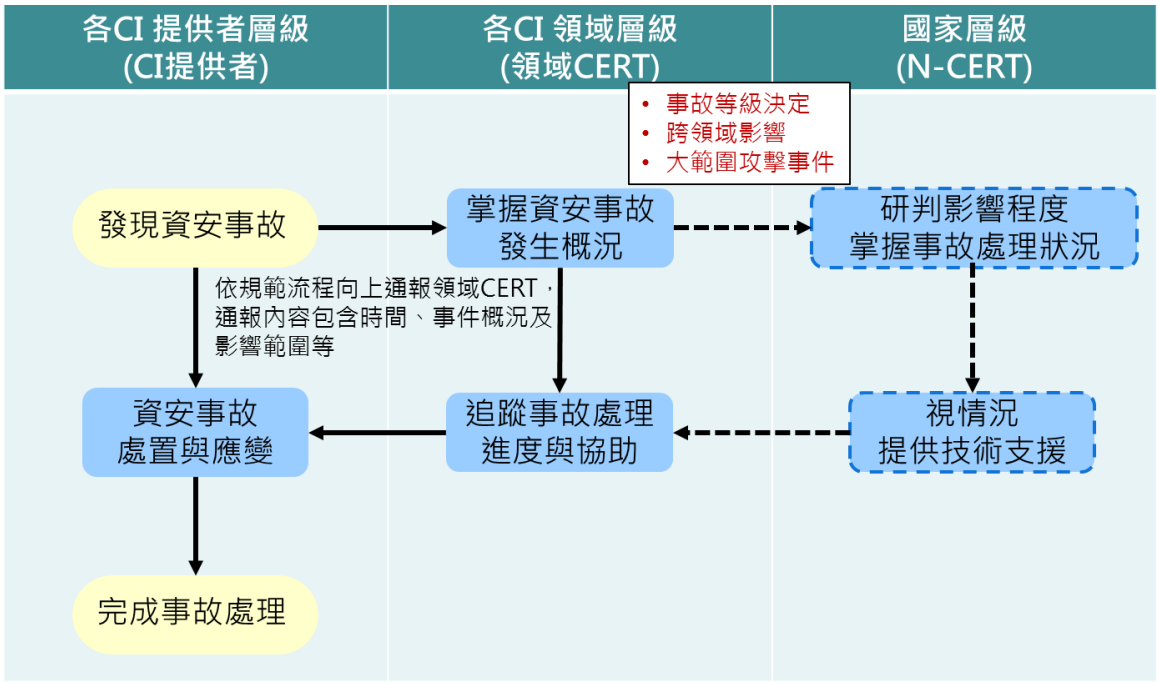
領域 CERT 需制定資安事件通報作業要點，以供 CI 提供者發現資安事件時，可依照配合辦理通報應變。此外，領域 CERT 應視資安事件影響情形，適時提供 N-CERT，以協助 N-CERT 掌握資安事件情形詳見圖 9。

– 領域 CERT 層級向上互動

領域 CERT 接獲資安事件通報時，經評估符合 3、4 級資安事件通報、影響範圍擴及跨領域或大範圍攻擊事件時，應彙整相關資料通報至 N-CERT，以利 N-CERT 掌握全國整體通報現況。

– 領域 CERT 層級向下互動

領域 CERT 接收 CI 提供者資安事件通報時，應追蹤了解 CI 提供者事件處理情形，確保資安事件處理完善。



資料來源：技服中心整理

圖9　資安事件通報流程示意圖

●資安事件處理程序

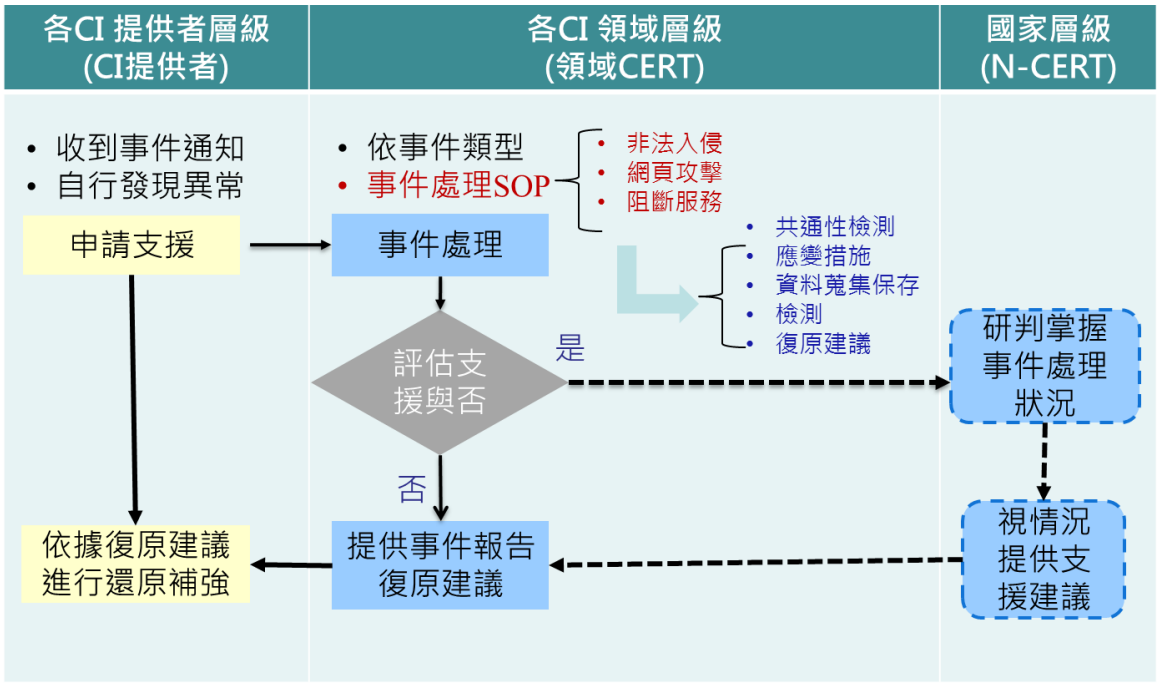
領域 CERT 接獲 CI 提供者申請事件處理支援時，需掌握事件發生概況，適時提供適當之支援協助，以協助 CI 提供者完成事件處理進行後續補強，詳見圖 10。

– 領域 CERT 層級向上互動

領域 CERT 層級接獲 CI 提供者事件處理需求時，經評估符合 3、4 級資安事件通報、影響範圍擴及跨領域或大範圍攻擊事件時，得向 N-CERT 申請資源協助。

– 領域 CERT 層級向下互動

領域 CERT 接獲 CI 提供者申請事件處理支援時，應評估事件類型以判斷是否符合支援範圍，並循資安事件處理程序協助進行技術支援(如電腦鑑識)，並提供事件處理報告與復原建議，協助 CI 提供者進行復原與補強措施。



資料來源：技服中心整理

圖10 資安事件處理流程示意圖

3.2.3. 應用情境

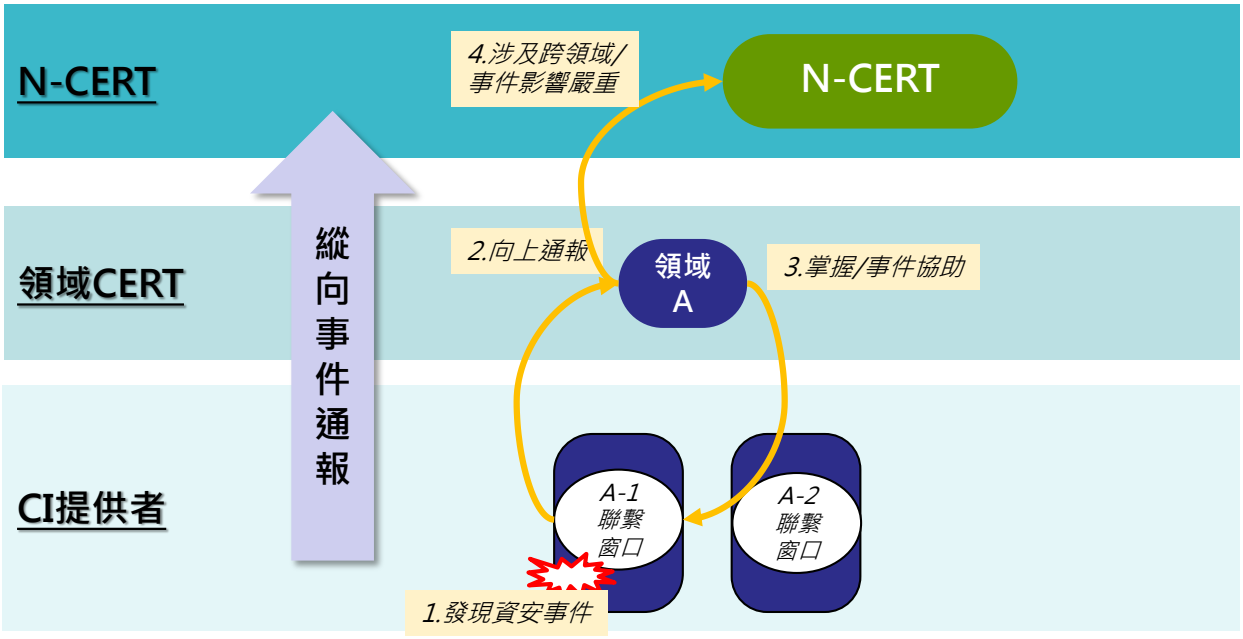
領域 CERT 負責接收領域內 CI 提供者事件通報，彙整相關資安事件資訊，依據向上呈報準則適時提報至 N-CERT，可參考下列之應用情境範例說明，以了解事件通報之運作模式與流程。此應用情境處理流程分為 4 個步驟，應用情境詳見圖 11，並說明如下：

●步驟一：CI 提供者發現資安事件，且機密性、完整性及可用性實際受害之情形。

●步驟二：CI 提供者依循領域 CERT 制定之通報作業要點，於限定時間內至 CERT 平台進行通報作業。

●步驟三：領域 CERT 接獲 CI 提供者通報後，即連繫 CI 提供者以了解事件概況，並視 CI 提供者處理需求提供協助。

●步驟四：領域 CERT 經了解該通報事件影響程度符合 3、4 級資安事件通報、影響範圍擴及跨領域或大範圍攻擊事件後，彙整相關資料提報至 N-CERT 協助處理。



資料來源：技服中心整理

圖11 縱向事件通報示意圖

3.3.查核階段

查核階段為確保 CERT 建置執行，透過測試、與演練活動之進行，檢測應辦事項執行之有效性。本節將以領域 CERT 為適用對象，說明查核階段所

進行之各查核事項。

3.3.1. 檢視/測試

CI 領域層級於建置領域 CERT 後，建議檢視或測試的項目與內容，作為後續改善的依據。

●執行情形統計

針對服務執行項目定期檢視與彙整運作情形，並提供報表供管理審查(詳見表 5)，項目包括：

– CI 提供者資料維護報告檢視：依據組織目標與政策，定期與不定期檢視 CI 提供者資料維護活動與紀錄，針對尚未完成申請或更新聯絡資料之 CI 提供者，適時提出矯正行動方案。

– 通報事件追蹤處理：定期與不定期檢視通報事件活動與紀錄，以發掘潛在改善之機會。

– 資安事件處理追蹤報告：定期與不定期檢視資安事件處理報告，針對特殊攻擊手法進行了解，以增進資安事件處理程序。

表5　執行情形報表審查檢核表範例

工作項目		主責人員	統計區間	執行情形(統計/件數)
CI 提供者資料維護報告	CI 提供者平台帳號申請/裁撤異動統計		季/年	
	CI 提供者平台帳號申請率統計		季/年	
	CI 提供者資料經測試驗證不正確比率		季/年	
通報事件追	通報事件通報統計		季/年	

工作項目		主責人員	統計區間	執行情形(統計/件數)
蹤處理	通報事件通報類型/等級統計		季/年	
	通報事件平均結案所需天數		季/年	
資安事件處理追蹤	資安事件處理申請件數		季/年	
	資安事件處理類型統計		季/年	
	資安事件處理平均所需天數		季/年	

資料來源：技服中心整理

●功能測試

因應外部環境改變或使用者需求，平台功能調整或開發，需進行對應之測試，以確保平台之可用性，並符合使用需求，並以季/年為統計區間檢視平台功能異動情形，提供參考之檢核表，詳見表 6。

表6　功能異動紀錄檢核表範例

功能項目	異動狀態(新增/修改/刪除)	申請時間	預計上線時間	測試情形	完成/未完成	主責人員

資料來源：技服中心整理

3.3.2. 演練

透過演練方式以查核建置領域 CERT 後執行狀況，演練項目包含：

●通報演練：確認領域 CERT 通報聯繫管道暢通與強化權責人員了解並知悉通報作業。

●事件處理情境演練：確認事件處理人員了解事件處理程序。

3.4.改善階段

3.4.1. 改善計畫

領域 CERT 應依據組織內部管理審查之結果，訂定改善計畫，並落實執行追蹤複核，確保各項工作項目完成建置與執行。

3.4.2. 評估衡量

藉由組織內部定期/不定期管理審查會議，以確認組織運行方向是否符合組織願景與目標。

4. 結論

本指引主要針對領域 CERT 建立過程中，CI 領域層級與 CI 提供者對應之角色權責進行說明。此外，針對建置規劃過程或建置執行中，說明需考量之相關項目，並提供相關檢核項目與改善方式供作後續維運參考，惟仍需考量下列議題：

●推動 CI 提供者參與

領域 CERT 仰賴 CI 提供者主動通報與積極的事件處理，唯目前國內尚未有相關安全政策及相關法規，律定 CI 提供者須進行資安事件通報之義務，因此需加強 CI 提供者的參與，以強化整體通報機制。

●強化 CI 提供者資訊安全意識

當 CI 提供者受限於人力或是組織資源時，往往會缺乏資訊安全相關背景的人員，當發生資安事件時，較為缺乏事件處理能量。因此領域 CERT 適時適地以適當方式，提供應變程序或處置策略，可提升 CI 提供者資安事件處理能量。

領域 CERT 營運期間將遭遇許多當初在規劃建置時未能事先預料之問題，須於維運期間收集相關問題以精進通報機制與流程，以及需與所有成員進行有效率的溝通，如定期召開會議或進行問卷調查以取得寶貴反饋，持續改善通報機制與流程，以達成有效益及效率之事件處理的終極目標。

5. 參考文獻

[1]行政院資通安全處(106 年 2 月)。「106 年國家資通安全防護整合服務計畫」需求說明書。未出版。

[2]行政院資通安全處(105 年 8 月)。「行政院國家資通安全通報應變作業綱要」。

[3]組織架構(民 105 年 8 月 1 日)。行政院國家資通安全會報。民 106 年 3 月 7 日，取自：https://www.nicst.ey.gov.tw/。

[4]行政院資通安全會報。「政府機關（構）資通安全責任等級分級作業規定」。

[5]行政院資通安全會報。「資訊系統分類分級與鑑別機制參考手冊」。

[6]行政院資通安全會報。「資訊系統風險評鑑參考指引」。

[7]行政院資通安全會報。「資訊系統分級與資安防護基準作業規定」。

[8]行政院資通安全會報。「安全軟體設計參考指引」。

[9]行政院資通安全會報。「安全軟體測試參考指引」。

[10]行政院資通安全會報。「資訊作業委外安全參考指引」。

[11]US-CERT, Information Sharing Specifications for Cybersecurity(https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity)

[12]STIX Project by the MITRE Corporation(2017). The MITRE Corporation. Retrieved March 7, 2017, from the World Wide Web: https://stixproject.github.io/

[13]TAXII Project by the MITRE Corporation(2017). The MITRE Corporation. Retrieved March 7, 2017, from the World Wide Web: https://taxiiproject.github.io/

6. 附件

附件 1　通報單範例格式

附件 2　通報作業要點範例說明

附件 3　資安事件處理程序

附件 4　STIX 模組說明

附件 5　TAXII 模組說明

附件 6　CERT 通報平台功能說明

附件1 通報單範例格式

資安事件通報單

◎通報單位：_____ □通報 □解除通報單

◎聯繫電話：_____ E-mail：_____

◎填報時間：____年____月____日____時____分

一、發生資通安全事故之單位聯絡資料：

◎單位名稱：_____◎主政機關名稱：_____

◎通報人：_____ ◎電話：_____ 傳真：_____

◎電子郵件信箱：_____

◎是否代其他單位通報：□是，該單位名稱_____ □否

二、發生資安事件基本資訊：

1.◎事件發生時間：____年____月____日____時____分

2.設備資料：

◎受害主機數量：_____臺：伺服器_____臺

IP 位址（IP Address）： 內部 IP：_____

(無；可免填)

外部 IP：_____

網際網路位址（Web-URL）： (無；可免填)

◎作業系統名稱：□Windows 系列 □Linux 系列 □其他作業平台 版本：_

◎已裝置之安全機制：□防火牆 □防毒軟體 □入侵防禦系統 □其他：__

◎資安監控中心(SOC)：□無□機關自行建置□委外建置 _____(請提供廠商名稱)

◎受害系統是否通過資安管理認證：□是□否

◎資安維護廠商：_____(請提供廠商名稱)

3.事故影響等級：

◎請分別評估資安事故造成之機密性、完整性以及可用性衝擊：

資安事故影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)

－機密性衝擊：（單選）

□國家機密資料遭洩漏 (4 級)

□密級或敏感公務資料遭洩漏 (3 級)

□核心業務 (含關鍵資訊基礎設施)一般資料遭洩漏 (2 級)

□非核心業務一般資料遭洩漏 (1 級)

□無資料遭洩漏 (無需通報)

－完整性衝擊：（單選）

□關鍵資訊基礎設施系統或資料遭嚴重竄改 (4 級)

□核心業務系統或資料遭嚴重竄改；抑或關鍵訊基礎設施料遭輕微竄改 (3 級)

□非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改 (2 級)

□非核心業務系統或資料遭竄改 (1 級)

□無系統或資料遭竄改 (無需通報)

－可用性衝擊：（單選）

□關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作 (4 級)

□核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施遭影響或系統停頓，於可容忍中斷時間內回復正常運作 (3 級)

□非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務遭影響系統停頓，於可容忍中斷時間內回

復正常運作 (2 級)

□非核心業務運作遭影響或短暫停頓，於可容忍中斷時間內回復正常運作 (1 級)

□無系統或設備運作受影響 (無需通報)

◎事故分類與異常狀況：(事故分類為單選項；異常狀況為複選項)

○ 網頁攻擊

□網頁置換 □惡意留言 □惡意網頁 □惡意網頁 □釣魚網頁 □網頁木馬 □網站個資外洩

○ 非法入侵

□系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件 □資料外洩

○ 阻斷服務 (DoS/DDoS) □服務中斷 □效能降低

○ 設備異常 □設備毀損 □電力異常

○ 其他：_____

◎事故說明：

◎可能影響範圍及損失評估：

◎是否影響其他關鍵基礎設施運作：□是 □否

◎應變措施：

◎此事故通報來源：□自行發現 □事件通知，事件編號：_____

三、期望支援項目：

◎是否需要支援：□是（請續填期望支援內容） □否（免填期望支援內容） 期望支援內容：
四、通報結案： 解決辦法與後續補強措施：
五、 已解決時間：____年___月___日____時____分

附件2 通報作業要點範例說明

建議可參考現行制度「國家資通安全通報應變作業綱要」制定領域通報作業要點，供 CI 提供者遵循。通報作業要點應載明目的、適用對象與時機、資安事件影響等級及通報作業，可參考下列表格。

通報作業要點項目說明

目的	為利領域 CERT 及所轄領域 CI 提供者於遭遇資通安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保各機關（構）各項業務之正常運作，依據「國家資通安全通報應變作業綱要」特訂定本要點。
適用對象與時機	▪ 適用對象：領域 CERT 及所轄領域 CI 提供者 ▪ 適用時機：各領域 CI 提供者於發生資通安全事件或其他災害涉及資通安全事件時應立即依本要點辦理。
資安事件影響等級	4 級事件：符合下列任一情形者，屬 4 級事件： ▪ 國家機密資料遭洩漏。 ▪ 關鍵資訊基礎設施系統或資料遭嚴重竄改。 ▪ 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。
	3 級事件：符合下列任一情形者，屬 3 級事件： ▪ 密級或敏感資料遭洩漏。 ▪ 核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改。 ▪ 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

	2 級事件：符合下列任一情形者，屬 2 級事件： ▪ 核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。 ▪ 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改。 ▪ 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。	
	1 級事件：符合下列任一情形者，屬 1 級事件： ▪ 非核心業務一般資料遭洩漏。 ▪ 非核心業務系統或資料遭輕微竄改。 ▪ 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。	
通報作業	通報	通報範圍應包含自建或委外之資通訊系統。 CI 提供者於發現資通安全事件時，如符合資安事件影響等級，除循內部程序上報外，並依下列規定通報： ▪ 於限定時間內至通報平台填寫事件資訊(填寫內容請附件 1 詳見)，並評估該事件是否影響其他關鍵資訊基礎設施運作。 ▪ 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於限定時間內，聯繫提供事件細節，待網路通訊恢復正常後，仍須至通報平台填報。
	審核	領域 CERT 應於接獲各 CI 提供者通報，即檢視通報內容，並評估該事件是否影響其他關鍵資訊基礎設施運作與事件影響等級之合理性，視需要請求外部支援。

	結案	▪事件處理完成後CI提供者應至通報平台登錄事件處理辦法與完成時間，通報結案以解除列管。 ▪如遇資安事件危及人員生命或設備遭到破壞等涉及民、刑事案件時，經首長核定後，立即通報檢調單位請求處理。
應變作業	事前	▪應依資訊系統分級作業相關規定，判定資訊系統安全防護等級，並據以落實資安防護基準。 ▪應規劃建置資通安全整體防護環境，做好單位及委外廠商內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。 ▪應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。 ▪應依資通安全防護需要，執行入侵偵測、安全檢測及弱點掃描等安全檢測工作，並訂定系統與資料備份管理辦法，以做好事前防禦準備。 ▪應實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。 ▪應保留資安紀錄與備份，如資訊系統屬委外建置管理者，應於合約內要求承商保留相關資安紀錄。 ▪應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實

		施內部稽核，以儘早發現系統安全弱點並完成修復補強。 ▪應建置並保存相關設備之系統日誌。
	事中	▪應就資安事件發生原因、影響等級、可能影響範圍、可能損失及是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。 ▪依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。 ▪查詢系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，以尋求解決方案；如無法解決，應迅速向領域 CERT 反應，請求提供相關技術支援。 ▪評估資安事件對業務運作造成之衝擊，並進行損害管制。 ▪視資安事件損壞程度，遵循單位及委外廠商內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。 ▪資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。 ▪各單位如發生重大(「3」、「4」級)資安事件，應主動提供相關設備系統日誌予領域 CERT，俾提供相關協助。

	事後	▪在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份及資料復原等相關事宜。 ▪在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。 ▪全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。 ▪資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊，並提送領域 CERT 檢討，以強化資通安全防護機制。

附件3 資安事件處理程序

資安事件處理程序係為資安事件處理人員於資安事件發生時，能有效執行事件處理調查，並依據調查情形，進行事件處置應變、損壞管制及復原，以減輕資安事件造成的影響， 後續進而強化資安事件防範措施。事件處理流程概分為計劃準備階段、檢測分析階段、處理復原階段及檢討改進階段，各階段執行項目可參考「資安事件處理程序工作項目範例」。

- 計劃準備階段係當資安事件發生時，根據組織網路環境架構、權限控管、調查目的及受害情形等，以判斷事件類型與界定調查範圍，作為資安事件處理小組人員遴選依據，並依循預先定義資安事件類型，採取對應的處理作業程序，確保投入正確且足夠資源處理資安事件。

- 檢測分析階段係資安事件處理小組人員，依據不同資安事件類型，決定資料蒐集範圍與類型，如資安監控系統警示紀錄(入侵偵測與防禦系統、防毒軟體、誘捕系統及日誌監控系統等)、網路監控系統警示紀錄(防火牆、網路流量分析紀錄及網頁內容過濾等)、資訊設備日誌紀錄(系統登入/登出紀錄、事件檢視器紀錄、應用程式紀錄及網站日誌紀錄等)，確保完整蒐集數位證據以供處理人員分析。

- 處理復原階段係依據檢測分析結果，採取對應損壞管制或復原，並適當將處置過程文件化加以記錄，作為後續檢討改進依據。若資安事件尚未獲得控制或是對組織營運造成嚴重衝擊，則應循內部營運持續管理計畫進行危機處理，以確保組織正常營運。

- 檢討改進階段係於事件處理結束後，審視、驗證，以及改善相關作業程序，包括現存的資安風險評鑑的適宜性、現行資安事件處理程序的有效性、現行資安政策的落實，防範措施與資源是否充足。

資安事件處理程序工作項目範例

執行項目				應蒐集/檢測	已完成
計劃準備階段	確認事件資訊	事件類型(非法入侵、網頁攻擊、阻斷服務) 受測設備資訊(用途、作業系統、數量) 調查目的		☐	☐
	檢測人員			☐	☐
檢測分析階段	資料蒐集	資安監控系統警示紀錄		☐	☐
		網路監控系統警示紀錄		☐	☐
		資訊設備日誌紀錄		☐	☐
	檢測項目	遭駭帳號檢測	自動啟動項目 網路活動	☐	☐
		惡意程序檢測	行程檢測 檔案時間線	☐	☐
		惡意網路活動檢測	事件日誌紀錄檢視 註冊表檢視	☐	☐
		惡意檔案檢測	惡意程式取樣	☐	☐
處理復原階段	移除異常項目	異常帳號		☐	☐
		惡意程序		☐	☐
		惡意檔案		☐	☐
	弱點修補			☐	☐
	確認已復原之設備運作正常	作業系統運作正常		☐	☐
		應用程式運作正常		☐	☐
		網路連線活動正常		☐	☐

執行項目			應蒐集/檢測	已完成
檢討改進階段	補強與改善計畫	網路架構調整	□	□
		存取權限控管	□	□
		作業程序改善	□	□

附件4 STIX 模組說明

STIX 第一版發行的官方白皮書詳細敘述其架構與相關技術，其架構主要可分為 9 大模組，模組之間或模組本身可具有關聯性與上下關係，詳細模組說明如下。

STIX 模組列表

項次	模組名稱	模組說明
1	資安威脅觀察資料 (Observables)	敘述資安威脅事件中所觀察到的相關資料，內容可包含資料來源、資料名稱、內容敘述、資料真實性及相關資安威脅事件等
2	資安威脅模式 (Indicator)	敘述資安威脅可能被觀察到的活動模式，內容可包含威脅模式名稱、模式描述、有效時間、攻擊手法、觀察資料及網際狙殺鍊階段(cyber kill chain)等
3	資安威脅事件 (Incident)	敘述資安威脅事件，內容可包含事件名稱、事件描述、事件類型、受害者、影響範圍與影響資產等
4	資安威脅手法 (Tactics, Techniques, and Procedures, TTP)	敘述資安威脅策略、技術與手法，內容可包含資安漏洞、攻擊模式、惡意程式、使用工具、受害者及網際攻擊狙殺鍊階段等
5	資安威脅活動 (Campaign)	敘述資安威脅活動資訊，內容可包含一群駭客、攻擊手法、威脅模式與相關事件，甚至可推演關聯至其他相關資安威脅活動
6	資安威脅者 (Threat Actors)	敘述資安威脅者的特徵與描述資訊，內容可包含相關基本描述、資安威脅活動、威脅手法、情資來源及動機等
7	資安威脅目標	敘述被惡意利用的資安漏洞、弱點及設定

項次	模組名稱	模組說明
	(Exploit Target)	檔，內容可包含目標名稱、目標描述、資安漏洞、資安弱點、因應措施、處理狀況及相關資安威脅手法等
8	資安威脅防護措施(Course of Action)	敘述面對資安威脅所做的應變與預防措施，內容可包含防護措施名稱、描述、效用、使用成本、應用範圍及相關防護措施等
9	資安威脅報告(Reports)	綜整各模組資訊而成資安威脅報告，也可處理難以單一套用至其他模組的資安資訊，設計此模組以文字格式彈性封裝資安資訊

資料來源：技服中心整理

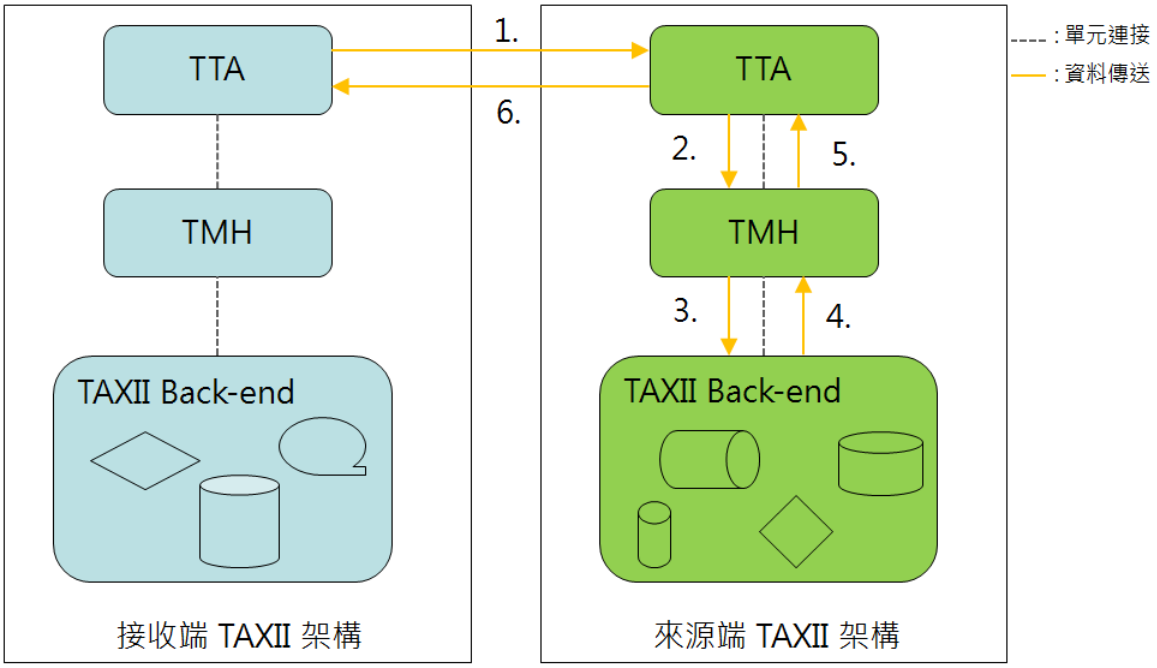
附件5 TAXII 模組說明

TAXII 針對網路威脅情資交換傳輸機制，定義一套服務和訊息交換機制，功能模組包含網路連接、訊息處理及後端管理等功能單元，相關功能單元說明與運作架構如下。

TAXII 功能單元列表

功能單元	說明
網路連接單元 TAXII Transfer Agent (TTA)	▪ 負責傳送/接收 TAXII 訊息 ▪ 透過網路與其他 TTA 通訊，處理協定需求的細節 ▪ 不處理 TAXII 訊息內容(由 TMH 處理)
訊息處理單元 TAXII Message Handler (TMH)	▪ 負責產生/解讀 TAXII 訊息，解析 TTA 收到的 TAXII 訊息，或建構一個可傳送的 TAXII 訊息 ▪ 與 TAXII Back-end 連接，將來自 Back-end 的訊息轉換為 TAXII 訊息，或基於 TTA 接收的 TAXII 訊息執行動作
後端單元 TAXII Back-end	後端單元，負責資料儲存、訂閱管理、存取控制決定、內容過濾及其他活動

資料來源：技服中心整理



資料來源：技服中心整理

圖1　TAXII 功能單元運作架構

附件6 CERT 通報平台功能說明

因應領域 CERT 建置需求，依循通報機制、CI 提供者資料建立/維護及事件處理之功能加以系統化，透過自動化平台協助通報管理、CI 提供者資料管理及事件支援管理。平台開發功能說明如下。

CERT 通報平台功能表

必要性	序號	功能項目	通報帳號 (CI 提供者)	審核帳號 (領域層級)
核心功能	1.	身分驗證與存取控管	CERT 通報平台應妥善規劃其帳號管理與身分識別機制，並考量存取系統資料之機密性與安全性。	
	2.	事件通報/審核作業	通報登錄： CI 提供者發生資安事件時進行通報填寫	通報審核： 領域層級接獲 CI 提供者通報時，應了解通報內容進行審核。
			通報列表/修改： 修改已填寫之通報內容	
			通報結案： 當完成事件損壞管制與復原時，即進行通報結案	追蹤結案： 領域層級應掌握 CI 提供者事件處理情況，當 CI 提供者通報結案或逾時未進行通報結案，應進行追蹤了解。
			歷史通報查詢： 查詢過去 CI 提供者已完成通報結案之通報事件	
			資安事件通報統計： 依據不同通報類型進行分類統計	資安事件通報統計： 依據不同通報類型進行分類統計。

必要性	序號	功能項目	通報帳號 (CI 提供者)	審核帳號 (領域層級)
	3.	事件處理管理	技術支援申請： CI 提供者於通報資安事件時，提出技術申請之需求。	事件處理派工與追蹤： 領域層級接獲 CI 提供者申請技術支援，依據事件處理程序評估是否符合支援標準與項目，並審核同意或不同意其申請需求。待事件處理完畢後，予以結案追蹤。
	4.	CI 提供者資料維護功能	修改 CI 提供者 CERT 平台帳號人員資料	維護 CI 提供者 CERT 平台帳號人員資料。
				修改 CERT 平台管理人員帳號資料。
附加功能	5.	通報演練功能	比照 CERT 通報平台功能，開放 CI 提供者練習熟悉 CERT 通報平台操作。	
	6.	網站訊息公告	重要公告事項： CI 提供者可檢視領域 CERT 發布之相關公告事項，如系統維護通知	

資料來源：技服中心整理