電腦資安事件處理程序之研究-以陸軍ASOC資安防護管理中心為例

作者／李建億

提要

一、電腦緊急應變小組為針對資安事件提供緊急應變與應置，以降低資安事件發生時伴隨的損害，儘速恢復正常營運。

二、陸軍原電腦緊急應變小組因應實需，於近年成立「資安防護管理中心(ASOC)」期提升資安防護管理監控機制與編組。

三、藉國際資安認證電腦資安事件處理程序，檢視陸軍ASOC緊急應變作業程序，進而提出「資安鑑識應處能力」「人員資安防護技術」及「跨軍種情資分享」等相關建議。

關鍵詞：緊急應變小組、資安防護管理中心、數位鑑識、資安聯防

前言

鑑於陸軍通資部門建立「資料中心暨異地備援」各項資訊系統，強化資安防護能力，整合陸軍緊急應變小組(Army Computer Emergency Response Team， ACERT)成立陸軍資安防護管理中心(Army Security Operation Center， ASOC)，[1]提升資安防護管理監控機制及危機處理能力，並在處理資安事件流程中加入數位鑑識程序。

我國有關數位事務的最高主管機關數位發展部資通安全署(以下簡稱資通安全署)明定「資通安全事件通報及應變辦法」規範公務機關與非公務機關需訂定通報及應變機制(如圖1)，[2]並持續鏈結民間資源與國際合作，增加實務經驗、創新技術與解決方案來提升資安能量。本研究結合國際電子商務顧問公司(The InternationaCouncil of Electronic Commerce Consultants， EC-Council)，[3]所提出的藍隊資安事故處理(EC-Council Certified Incident Handler， ECIH)，[4]該項證照已遍布超過60個國家，並獲得美國政府、聯合國及我國數發部認可。[5]

本研究主要探討ECIH與ASOC電腦資安事件處理程序，並進行分析與探討，研究範圍不包括陸軍體系中專屬網路(簡稱專網)、國軍資訊網路(MINET，簡稱軍網)、

1 陸軍司令部〈陸軍司令部資安防護管理中心(ASOC)作業規定〉，民國 111 年 03 月 25 日。
2 全國法規資料庫〈資通安全事件通報及應變辦法〉，民國 110 年 08 月 23 日。
3 UCOM 恆逸《EC-Counil 教育訓練中心》，https://www.uuu.com.tw/Course/Partner/EC-Council。
4 EC-Council Certified Incident Handler Copyright by EC-Council, EC-Council Certified Incident Handler v2 – Vol 1 (2019)。
5 數位發展部通資安全署，〈資通安全專業證照清單〉，民國 112 年 2 月 14 日 1，頁 3。

行政民網(單一閘口民網)等整合管理議題，此外，研究結果將針對ASOC資安鑑識應處能力、人員資安防護技術及跨軍種情資分享等面向提出建議以強化組織發展。

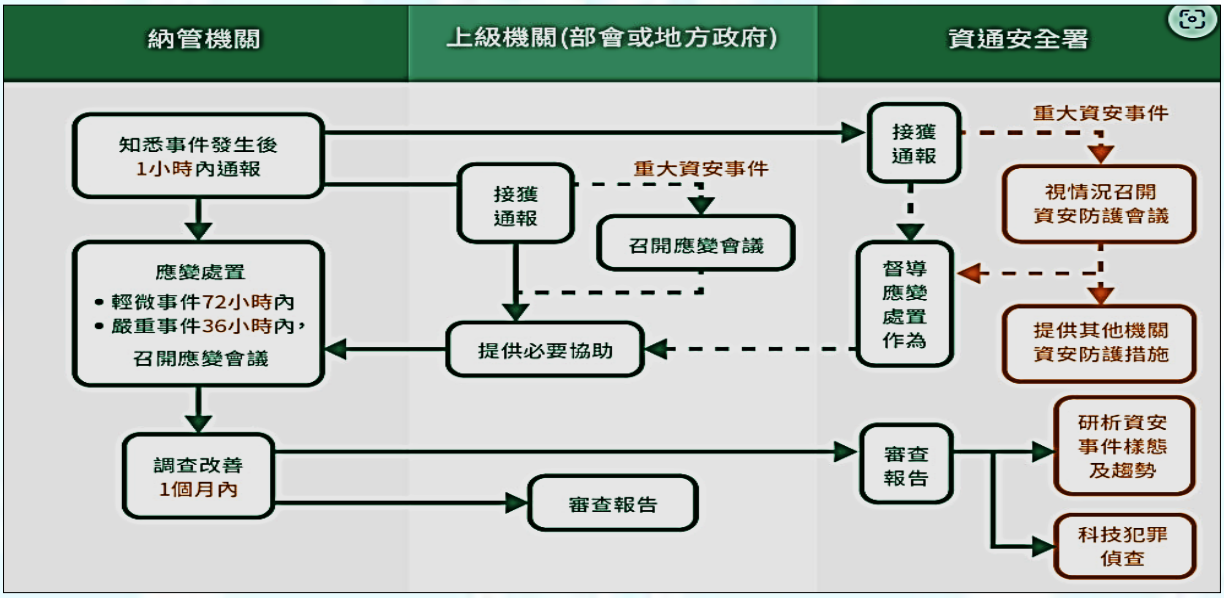

圖 1 資通安全事件通報及應變流程圖

資料來源：數位發展部資通安全署〈資安事件通報應變〉，https://moda.gov.tw/ACS/operations/notification-and-response/656，檢索日期2024年6月15日。

資安防護單位概述

一、電腦緊急應變小組(CERT)沿革與宗旨

1988年美國聯邦政府最先成立緊急應變小組，後續因科技發展資安事件層出不窮，於2003年美國國土安全部成立國家層級的US-CERT，強化資安事件應處能力。[6] 鑒於CERT資安防護與應變的重要性，我國於民國90年成立「行政院國家資通安全會報」，積極推動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，以達成即時資安事件通報。

依照國家資通安全防護整合服務計畫中對電腦緊急應變小組一詞，定義為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；同時建立跨體系之區域聯防整合運作機制，提供完整資安情資分享，防範未來可能的資安事件。

(一)角色權責與分工

為配合我國關鍵資訊基礎設施保護(Critical Information Infrastructure Protection

6 國家資通安全防護整合服務計畫〈領域 CERT 實務建置指引〉，民國 106 年 3 月，頁 1。

，CIIP)基本政策，電腦緊急應變小組區分國家層級(N-CERT)、各關鍵基礎設施領域層級(領域CERT)及關鍵基礎設施(Critical Infrastructure，以下簡稱CI)提供者層級(事件通報單位)等3個階層(如圖2)。對比於我陸軍通資體系中，N-CERT角色為陸軍司令部緊急應變小組、各領域CERT角色為軍團通資組緊急應變小組，最後CI提供者則為各單位緊急應變小組。[7]

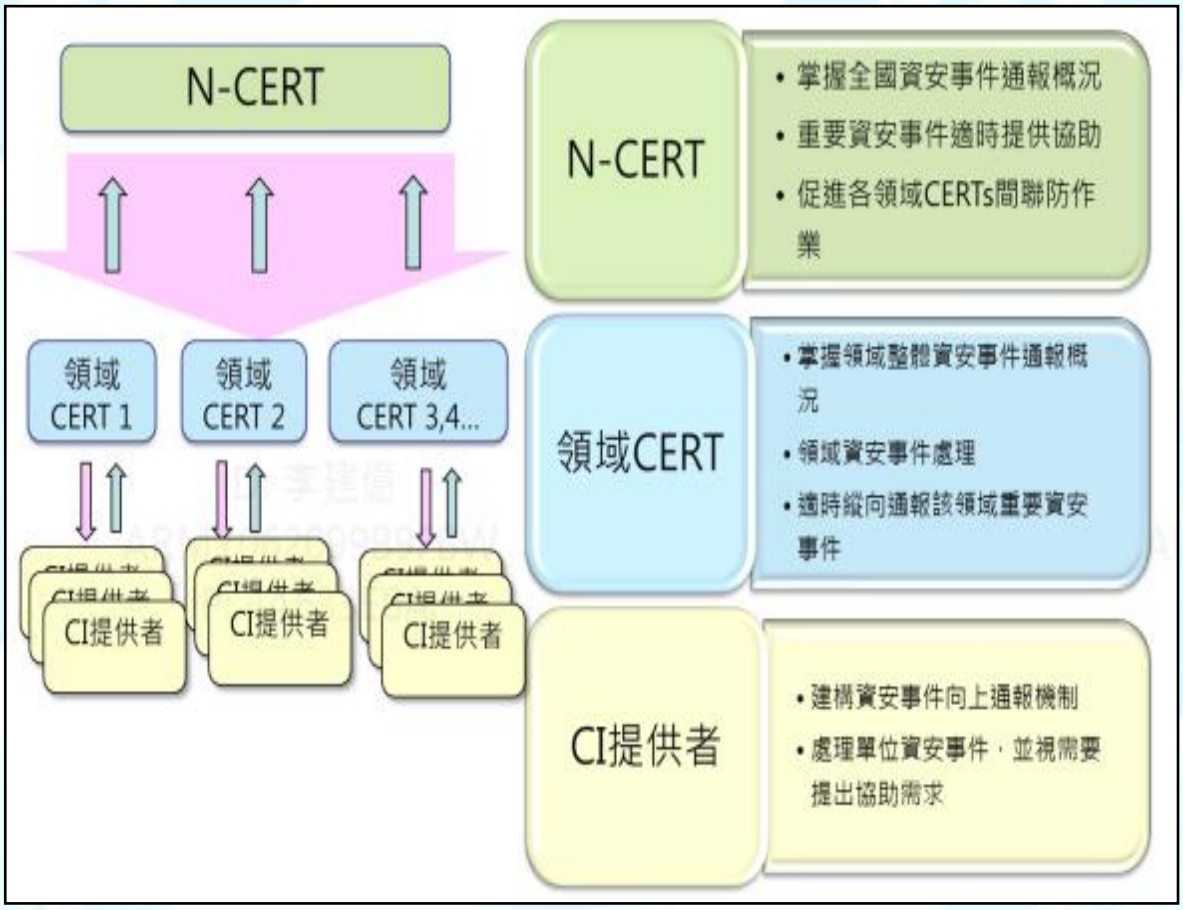

圖 2 CERT 角色權責與分工示意圖

資料來源：國家資通安全防護整合服務計畫〈領域CERT實務建置指引〉《數位發展部資通安全署》，https://moda.gov.tw/ACS/operations/ciip/650，檢索日期2023年10月17日。

(二)建置實務與維運程序

我國CERT與SOC均採納PDCA (Plan-Do-Check-Act， PDCA)作為組織建構的作業建置模型(如圖3)，從模型中訂定出CERT政策程序與維運作業，其中將模型區分為四個區塊，分別為規劃階段(Plan)、執行階段(Do)、查核階段(Check)及改善階段(Act)。透過模型訂定出程序與流程，適時回顧政策改善計畫，並落實追蹤。[8]

7 同註6，頁4。
8 同註6，頁7。

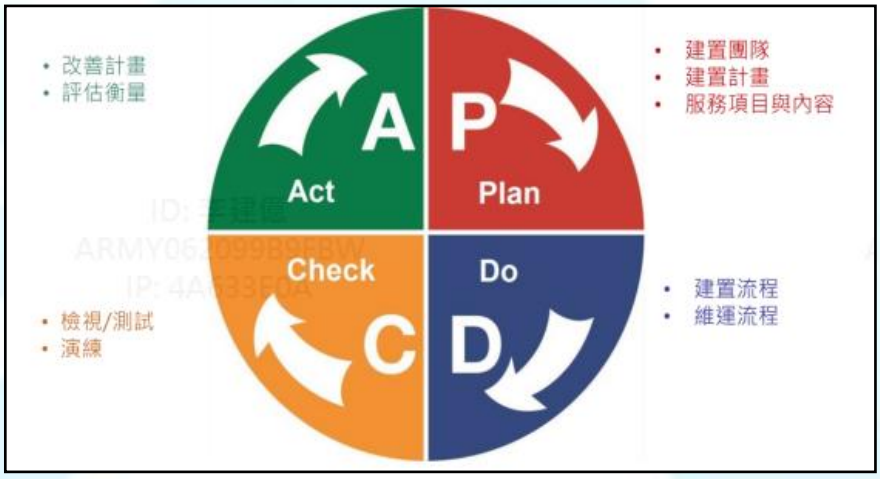

圖3 PDCA建置流程

資料來源：國家資通安全防護整合服務計畫，〈領域CERT實務建置指引〉《數位發展部資通安全署》，https://moda.gov.tw/ACS/operations/ciip/650，檢索日期2023年10月17日。

二、資安防護管理中心(SOC)沿革與宗旨

我國於民國90年成立「行政院國家資通安全會報」，積極推動資通安全基礎建設防護，於民國93年核定「建立我國通資訊基礎建設安全機制計畫(94年至97年)」第二期機制計畫，建置國家資通安全防護管理平臺(National Secruity Operation Center，N-SOC)針對重要核心政府機關提供監測等預警服務。[9]後續於民國108年依資通安全管理法要求，政府領域聯防監控中心(Government Security Operation Center，G-SOC)重新收容各公務機關威脅偵測機制之資安情資並與資安服務託管廠商建立公司協同關係提供資安聯防情資。

資安防護管理中心一詞依國家資通安全防護整合服務計畫中的定義，為協助CERT領域主管機關相關人員，評估整體網路環境及設施安全現況，有效掌握關鍵基礎設施資訊安全之運行，預防資安事件發生並協助CERT強化領域資安監控作業之運作管理，以符合關鍵基礎設施領域資安監控與資訊回傳管理規範之要求。[10]

(一)角色權責與分工

資安防護管理中心(Security Operation Center，以下簡稱SOC)在資安組織架構中區分三個級別(如圖4)。第一個級別為國家層級N-SOC主要負責制定CI資安威脅情蒐規範與領域內CI情資，掌握我國整體資安現況與趨勢。第二個級別為各CI領域層級，主要負責領域內資安監看情資與威脅，並縱向與N-SOC通報整體資安概況。第三個級別為各CI提供者層級，主要掌握該單位資安情資狀況與建構事件情資向上回

9 數位發展部資通安全署，〈資安政策與法規〉，https://moda.gov.tw/ACS/operations/policies-and-regulations/648，民國 96 年 02 月 15 日，檢索時間：民國 113 年 5 月 28 日。

10 國家資通安全防護整合服務計畫〈領域 SOC 實務建置指引〉，民國 106 年 3 月，頁 1。

傳機制。

整體SOC主要以資安威脅情蒐分析與掌握整體網路安全為主，另提供CERT在技術方面的支援，協助掌握資安事件並縱向回報資訊分享與分析中心(Information Sharing and Analysis Center， ISAC)對比陸軍通資部門所成立的ASOC為司令部層級屬領域內SOC，由ASOC協助各軍團CERT層級及旅級CERT處理資安事件與事件分析，掌握各式資安監控機制。[11]

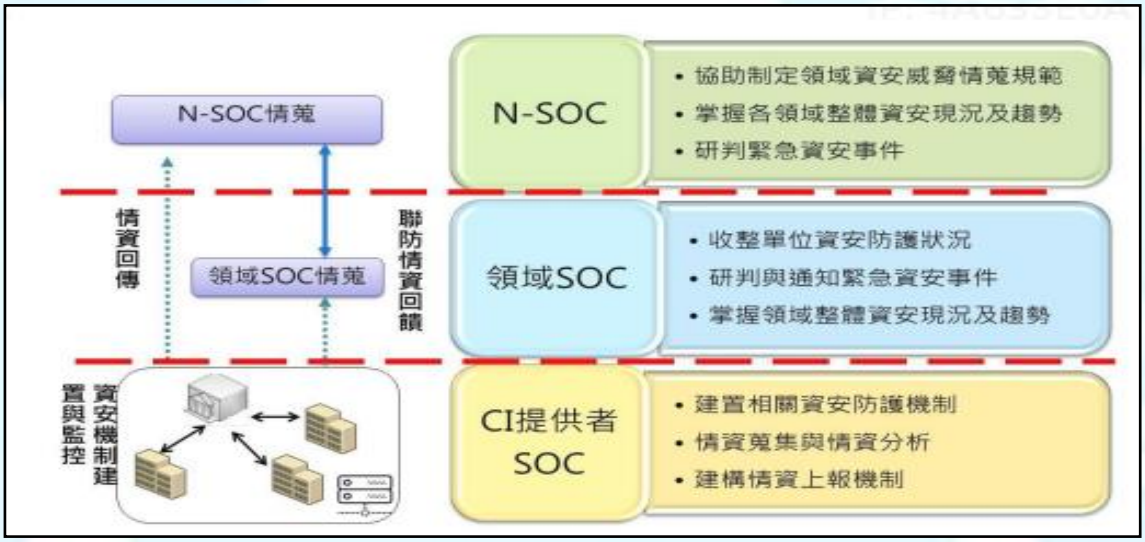

圖 4 SOC 角色分工與權責

資料來源：國家資通安全防護整合服務計畫〈領域SOC實務建置指引〉《數位發展部資通安全署》，https://moda.gov.tw/ACS/operations/ciip/650，檢索日期2023年10月17日。

(二)建置實務與維運程序

我國SOC與CERT均採納PDCA作為組織建構模型，建置各項作業與政策訂定、定期檢視實施計畫並落實追蹤改善計畫內容，使政策合乎實況及提供CERT政策與技術支援。[12]

(三)組織團隊領域劃分

團隊中主要有3個團隊組成依專業分責分工進行，由決策團隊來擬訂政策與管控計畫，建置團隊則負責網路環境監控項目、監控範圍定義、報告格式範例制定及執行政策並檢視現況適時回饋給決策團隊來改善計畫，維運團隊負責監看資料進行實際收容與分析、資安事件研判與回傳(如表1)。[13]

11 同註 10，頁 3。
12 同註 10，頁 5。
13 同註 10，頁 7。

表1 SOC建置項目分析

作業項目	國家層級 (N-SOC)	各SOC領域層級	SOC提供者層級
資安防護機制建置與資安監控處理	必要建置	必要建置	必要建置
情蒐威脅分析	必要建置	必要建置	配合事件成立
N-SOC資訊介接	必要建置	必要建置	必要建置
領域聯防情資回饋	必要建置	必要建置	配合事件成立
設置特定資安工作小組	配合事件成立	配合事件成立	配合事件成立

資料來源：國家資通安全防護整合服務計畫〈領域SOC實務建置指引〉《數位發展部資通安全署》，https://moda.gov.tw/ACS/operations/ciip/650，檢索日期2023年10月17日。

三、陸軍資安防護管理中心(ASOC)沿革與宗旨

陸軍通資部門為有效掌握各單位通資與資訊網路、資通安全事件及監控各類資安管控軟體等系統服務，於民國95年由國防部陸軍司令部下轄通信電子資訊處成立ACERT組織團隊(如圖5)，ACERT下轄單位成立資訊中心(如圖6)共同推動資安政策與維護等作業，ACERT在轉型前，任務為整體陸軍資安監控防護、硬體維護及各類系統維運管理，並協助資訊中心資安事件、資安違規及各類系統技術支援。

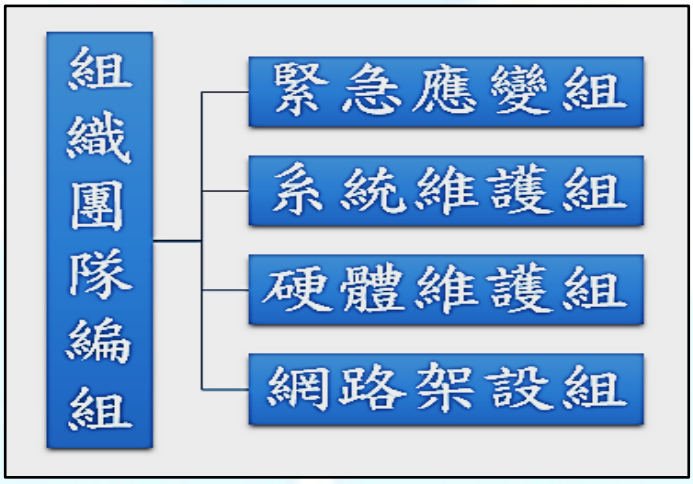

圖 5 ACERT 組織團隊編組

資料來源：作者整理，參考陸軍司令部，〈陸軍109年通資勤務管理實施計畫〉。

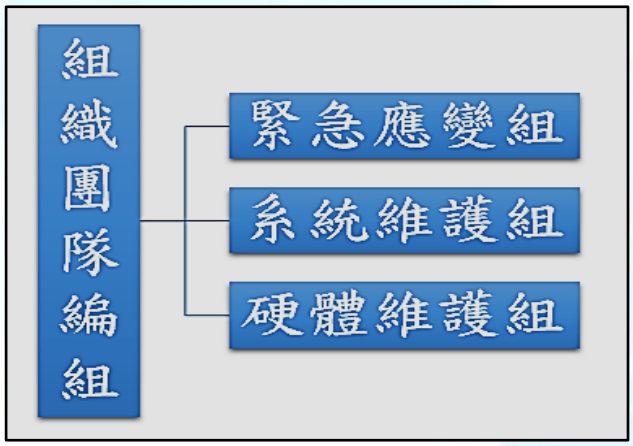

圖6 資訊中心組織團隊編組

資料來源：作者整理，參考陸軍司令部，〈陸軍113年通資勤務管理實施計畫〉。

後續因陸軍通資部門建立「資料中心暨異地備援」各項資訊系統，強化資安防護能力，於民國109年由陸軍通資部門統籌整合ACERT成立ASOC，提升資安防護管理監控機制與編組，[14]協助管制官掌握整體陸軍單位資安情資、通報與應變、技術支援及鑑識分析等相關應變作為。

ASOC與ACERT不同之處在於資通安全威脅偵測與防禦機制、資通安全事件鑑識工作及關鍵基礎設施資通安全管理與防護機制之規劃、推動等執行作業，提升資通電系統於關鍵基礎設施維護與運作更有韌性。

(一)角色權責與分工

ASOC組織團隊編組依照陸軍資安防護管理中心值勤作業規定，將團隊編組(如圖7)區分為管制官、系統分析士、系統監控士、事件分析士及事件監控士等5個席位，[15]負責整體系統服務、資安事件及應變通報等作業。

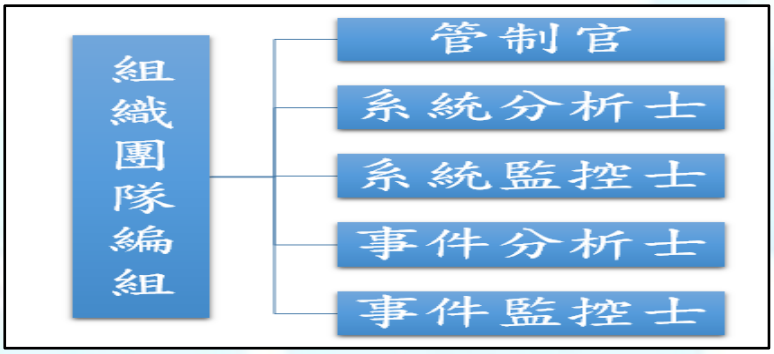

圖7 ASOC組織團隊編組

資料來源：作者整理，參考陸軍司令部，〈陸軍司令部資安防護管理中心(ASOC)作業規定〉。

14 同註1，頁9。

15 陸軍司令部〈陸軍資安事件通報應變實施計畫〉，民國112年12月06日，頁10~11。

(二)建置實務與維運程序

ASOC團隊負責資安防護管理中心組織維運(如圖8)、監看陸軍、民網資安防護動態、緊急應變處置、分析異常個案、彙整及肇因分析、技術諮詢、弱點掃描及系統漏洞修補、網路巡查及數位鑑識等工作。

圖8 組織維運

資料來源：作者整理，參考陸軍司令部，〈資安防護管理中心(ASOC)作業規定〉。

(三)組織團隊領域劃分

ASOC組織協助管制官掌握整體陸軍資安事件處置、通報、ASOC維運工作、規劃資安健檢及教育訓練等全般工作，並向上聯繫陸軍通資部門及國防部通次室(資安區隊)ASOC組織團隊主要由兩個編組組成，第一個編組為系統分析組，第二個編組為事件監控組，[16]編組席位監管分配(如表2)依專業各司其職掌握通資安違規事件管理系統與事件，構成完整的防禦體系。

16 同註1，頁11。

表2 監管分配表

陸軍「通資安違規事件管理系統」席位監管分配表			
項次	系統名稱	系統功能	備考
一	資安事件管理系統(SIEM)	收集各系統紀錄(log)，並設定條件過濾及分析異常事件，即時推播至網頁平臺。	系統分析士
二	網頁式硬體防火牆	管理網頁服務(HTTP、HTTPS)白名單設定，異常紀錄(log)回傳SIEM。	系統監控士
三	次世代防火牆	針對軍網所有連線設定白名單，異常紀錄(log)回傳SIEM。	
四	進階持續性威脅(APT)防禦模組	針對軍網所有異常行為(如阻斷服務、網段掃描等)，異常紀錄(log)回傳SIEM。	
五	通資安違規事件管理系統	網頁平臺顯示「資安事件管理系統(SIEM)」過濾後之異常事件，由ASOC研判再實施通報。	事件分析士
六	電子郵件過濾系統	電子郵件服務(POP3、IMAP)設定關鍵字及惡意程式等條件過濾異常郵件，紀錄(log)回傳SIEM。	事件監控士
七	網路支援管理系統(含流量監管)	監管路由器、防火牆上線情形及網路流量，異常紀錄(log)回傳SIEM。	
八	端點防護系統	部署於端點電腦，回傳端點電腦資訊(如漏洞修補編號、服務埠狀況等)，異常紀錄(log)回傳SIEM。	
九	弱點掃描系統	就本軍所屬網段實施弱點掃描，異常紀錄(log)回傳SIEM。	

資料來源：作者整理，參考陸軍司令部，〈資安防護管理中心(ASOC)作業規定〉。

電腦資安事件流程規範

為確保資通安全管理法納管之公務機關及特定非公務機關於發生資通安全事件時，依「資通安全事件通報及應變辦法」相關規定即時通報及應變，特訂定通報及應變處理作業程序。此外，政府部門提倡整合民間及產業能量，提升資通安全意識，通過各界資源合作，不僅加強防護措施，防範潛在威脅，更能打造安全、可靠的環境。以下就國際資安認證ECIH電腦資安事件處理程序與陸軍ASOC緊急應變處理程序實施說明。

一、ECIH電腦資安事件處理程序

商業機密對於企業或組織來說是最重要的資產，這些資訊對於企業競爭力和業務營運至關重要，如果遭受侵害，可能導致重大損失或商譽損害等影響，面對網路不確定性與威脅破壞，做好資訊網路安全防護對企業來說相當重要。以下就ECIH內容敘

述各階段程序(如圖9)。[17]

第一階段為「準備階段」，此階段中提出對組織或單位進行完整網路環境風險評估與系統復原計畫，分析出網路安全威脅並在實際環境進行模擬與演練，這期間必須考慮涉及人員、流程、技術與資訊的影響層面，檢視組織對網路安全事件應變準備程度。

第二階段為「應變階段」，接獲事件時，識別是否為資安事件，若是，由領域內人員控制當前狀況，保留當下所有證據並著手進行鑑識調查，在實驗室內還原當下資訊環境或系統，分析出威脅與漏洞根源找出滲透手法，記錄威脅分析報告提供後續決策者下達政策時之分析建議並適時修改資安政策，確認威脅根除已確實執行完畢，定時監控對外流量或系統工作是否有異常，事件結束後開始展開復原計畫，在第一階段時，單位必須備妥一份詳細的復原計畫，並確認所有復原程序都在涵蓋範圍內，確保能儘速恢復系統功能。

第三階段為「經驗學習階段」，事發過程會將整體概況記錄在安全事件調查報告，被視為最重要之一環，從經驗中學習可以防範未來安全事件，此階段包括事後檢視，確認復原過程所採取所有行動、修正或更新管控作業與安全事件應變計畫，從中學習相關的利害關係並且分享情資[18]。

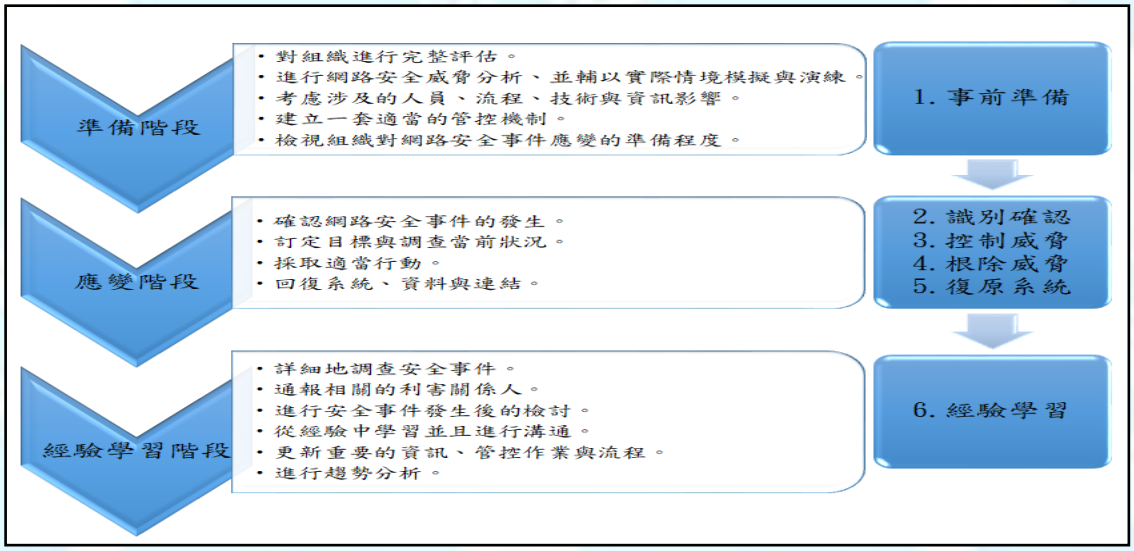

圖9 階段程序圖

資料來源：作者整理，參考BSI Group，網路安全事件應變step by step，https://www.bsigroup.com/LocalFiles/zh-tw/news/NO164/Cyber-Incident-Response-Step-by-Step.pdf，檢索日期113年4月22日。

17 臺北精誠資訊股份有限公司復興分公司〈藍隊資安事故處理-EC-Council ECIH 認證課程〉《UCOM 恆逸》，https://www.uuu.com.tw/Course/Show/698/EC-Council-ECIH 資安危機處理員認證課程，檢索時間 113 年 4 月 19 日。

18 〈網路安全事件應變 step by step〉《bsi》，https://www.bsigroup.com/LocalFiles/zh-tw/news/NO164/Cyber-Incident-Response-Step-by-Step.pdf，檢索時間 113 年 4 月 22 日。

此外針對應變階段通報流程，ECIH細分為六大階段分別探討事件處理回應程序，以下依階段敘述說明(如圖10)。[19]

第一階段為「事件紀錄與團隊分工」領域團隊接獲通報時，由專業領域應變小組記錄事件屬性及威脅程度，同時判別事件是否為資安事件。

第二階段為「事件分類與分析階段」。若事件成立後，由領域團隊分工進行事件分類與蒐證，並將蒐整的數位證據進行分析，依照事件影響程度決定優先順序。

第三階段為「通報階段」由領域緊急應變小組通報至資安防護管理中心記錄與掌握，資安防護管理中心負責指導統籌領域專業團隊相關技術與事件管制。

第四階段為「鑑識階段」。此階段將事故現場行動裝置或電腦系統保留，這部分須注意到電力系統不能突然中斷，導致硬體損壞，並留意若軟體正在運行，須由鑑識技術團隊進行勘查系統工作記錄等相關技術設定，避免直接關閉電力系統造成數位證據遺失。當實驗室還原事故現場的軟硬體運作，鑑識團隊須進行證據蒐整與分析，若超出領域技術範圍由防護管理中心編組進駐到事發地點協助處理，實施證據分析找出威脅手段與威脅程式進行根除，根除威脅後，在復原系統前要再次確認系統是否完成漏洞修補、更新系統及更新病毒碼，確保無慮後再將系統上線。

第五階段為「事件分析與政策修訂階段」鑑識團隊分析出事件威脅等級後進行分類，並且評估事件影響層面與損害計算記錄，整理完整證據資訊製作安全事件調查報告，提供後續決策層面在政策修改之建議。

第六階段為「事件情資分享階段」領域團隊結束調查後將安全調查報告資訊充分周知，公開資訊要避開商業機密，針對處理程序、通報程序、事件威脅分析、事件威脅分類、評估損害程度、入侵指標及鑑識報告實施揭露，並將威脅情資分享至ISAC透過跨領域資安聯防分析與回饋，提供威脅指標與手法，產製聯防情資報告，掌握整體資安現況及趨勢。

ECIH事件處理與回應程序中，鑑識階段是重要且繁瑣的過程，以下就數位鑑識準備程序說明(如圖11)。[20]

第一階段為「準備階段」此階段涉及實際調查開始之前執行的所有任務，包括建立電腦鑑識實驗室、建立取證工作站、調查工具包、成立調查小組及獲得有關當局批准，規劃流程等步驟、定義任務目標、保護案件周邊和涉及設備。

第二階段「調查階段」被認為是取得電腦數位犯罪證據的主要階段，它涉及取得、保存、分析數據資料並確認犯罪來源和攻擊者。這個階段具有技術知識、尋找證據、檢查記錄和保存結果以及證據資訊，為了確保數位證據完整性必須由訓練有素的專

19 同註 5，pp.161~167。
20 同註 5， pp.287~294

業人員執行。

第三階段「事後調查階段」此階段涉及報告和記錄，調查過程中採取的行動和調查結果，需確保分析報告能夠讓決策者理解並可以充分提供可接受之證據，且調查報告必須符合當地法規政策，才能成為法庭證據。

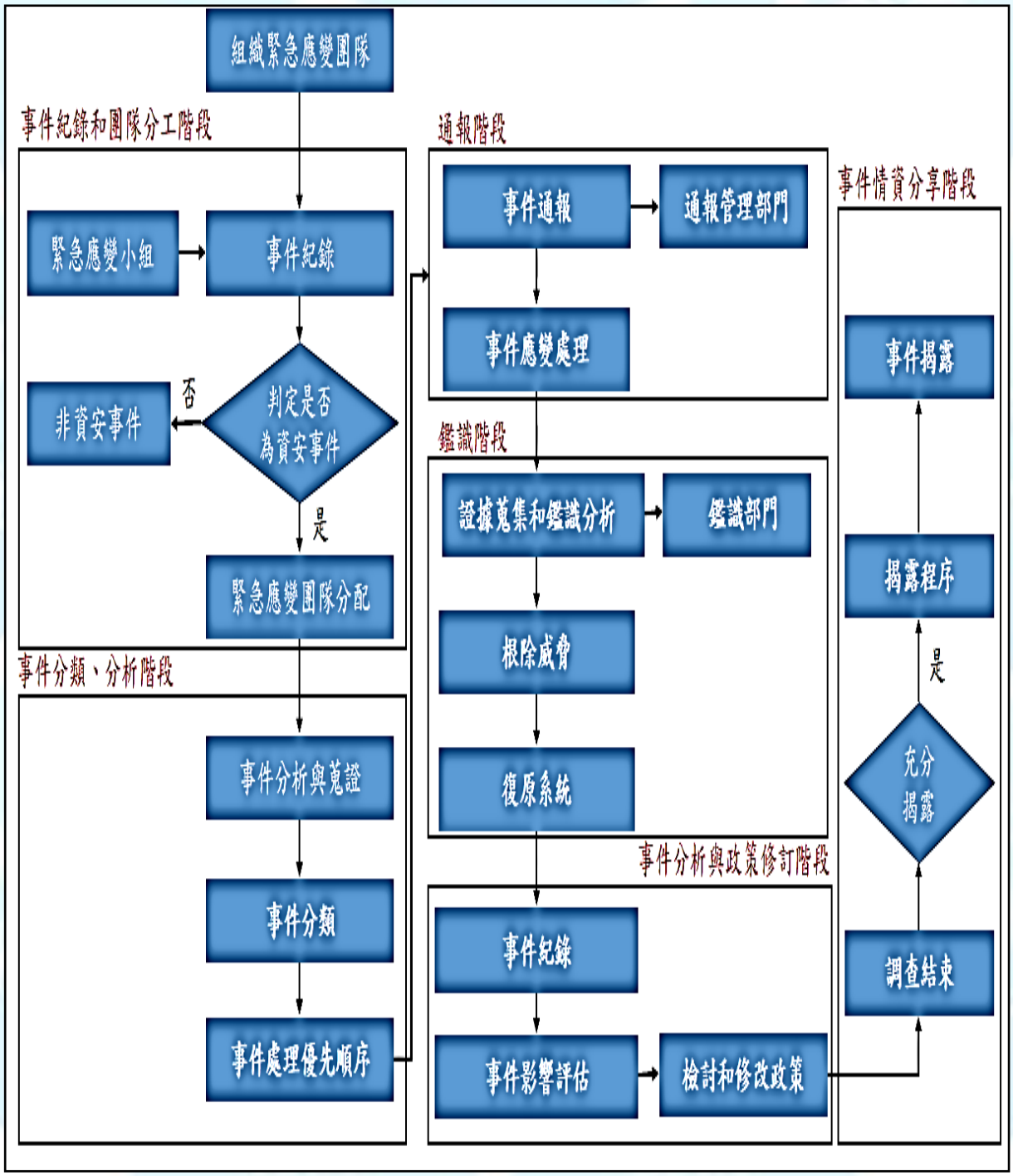

圖10 事件處理與回應程序圖

資料來源：作者整理。

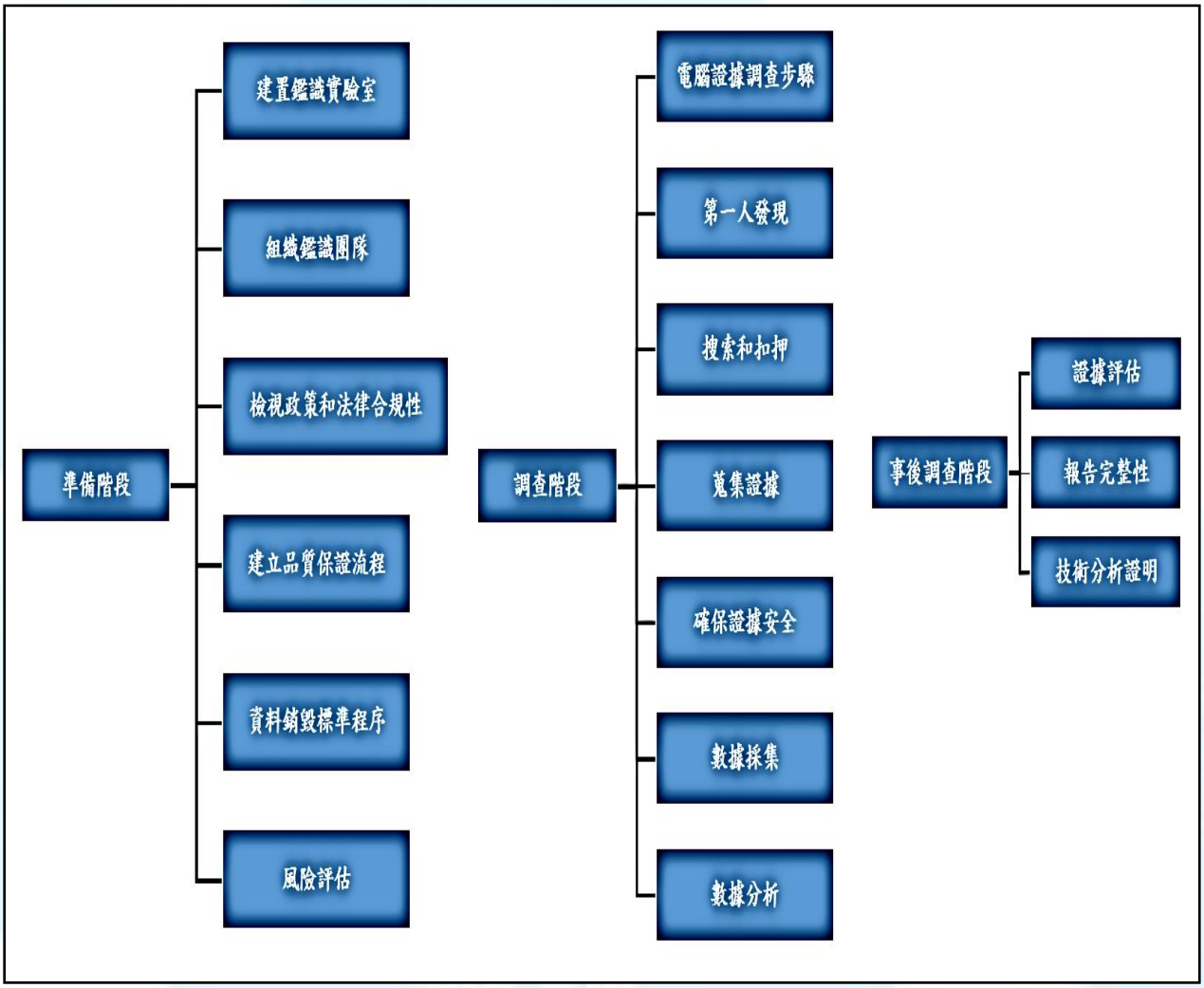

圖 11 數位鑑識準備程序

資料來源：作者整理。

二、陸軍資安防護管理中心緊急應變處理程序

承國防部政策指導與規範，陸軍通資部門訂定相關資安政策來應對體系內的資安事件，藉以達到事前安全防護、事中緊急應變、事後復原作業等相關措施，在陸軍資安事件通報應變實施計畫明確定義資安事件等級、資安違規、核心資訊系統以及資安責任權責與等級劃分。資安事件等級區分四個級別，事件由輕至重分別為「一級」、「二級」、「三級」、「四級」，[21]判定原則從嚴認定，資安違規事件則是屬於未達資安事件等級但仍對單位有影響，例如：資安管控軟體違規告警案件等。

核心資訊系統依重要性來區分成作戰指管類、戰備訓練類、管理資訊類及行政教育類等四大類(如表3)，[22]資安事件發生時會依照資安事件等級判斷基準來作重要性分類，進行優先順序搶修工程，若資安事件肇生會影響到公務機密洩漏、敏感資訊洩漏

[21] 同註 15，頁 5~6。

[22] 陸軍司令部〈陸軍資訊資產管理作業規定〉，民國 111 年 11 月 03 日，頁 39。

、基礎設施運作、核心業務系統停頓或終止運作，則依照資安事件來應變處置，事件等級則由領域緊應變小組視當下影響程度來判斷事件等級，確認實屬資安事件等級，限30分鐘內通報至ASOC，通報過程由旅級R-CERT循體系通報至軍團C-CERT後，並彙整所有資安違規初步報告及佐證，向ASOC回報資安事件狀況及處置情形。整體資安事件由ASOC管制處理情形，事件處理期間若遇旅級R-CERT無法處理，則限時2小時內向ASOC提出技術協助。

資安事件若屬「三級」、「四級」必須在24小時內恢復系統運作，「一級」、「二級」則在36小時內完成恢復，資安事件發生時由陸軍通資部門統籌相對應的部門來進行責任分工，資安事件發生時由事件指揮官(通資部門)掌握新聞官(政戰部門)、事件分析執行單位(通資部門)、情資及計畫組(通資部門)、應變執行組(領域專業編組)、後勤調度組(鑑識團隊)及財務行政組(主計部門)，透過各編組掌握事件發生期間所有威脅情資報告、損害評估、鑑識分析、年度政策修訂及事件揭露等相關資訊，使整體事件資訊和數據能夠充分掌握(通報與應變作業流程如圖12)。

表3 國軍核心資訊系統分類及適用範圍說明表

國軍核心資訊系統分類及適用範圍說明表		
名稱	類別	說明
資訊資產 核心系統	作戰指管	一、 用於作戰指管系統。 二、 包含各類指管系統、電子戰、網路戰、情報系統及監偵系統及其他等。
	戰備訓練	一、用於戰備或演訓系統。 二、戰備系統主要為人事戰備系統、用兵後勤系統及通資電戰力系統等。 三、演訓系統為兵棋裁判系統、戰術模擬系統及武器模訓系統等。 四、戰演訓專屬系統主機及終端設備。
	管理資訊	一、用於作業管理系統。 二、包含政戰、人事、主財、後勤、計畫、行政、醫療、採購及通資電系統等。
	行政教育	一、用於行政作業或一般教育訓練之資訊資產。 二、民網電腦及其相關管理設備歸屬於本類。 三、訓練教室等非機敏之內網電腦歸屬於本類。 四、備用資訊資產歸屬於本類。

資料來源：作者整理，參考陸軍司令部，〈資安防護管理中心(ASOC)作業規定〉。

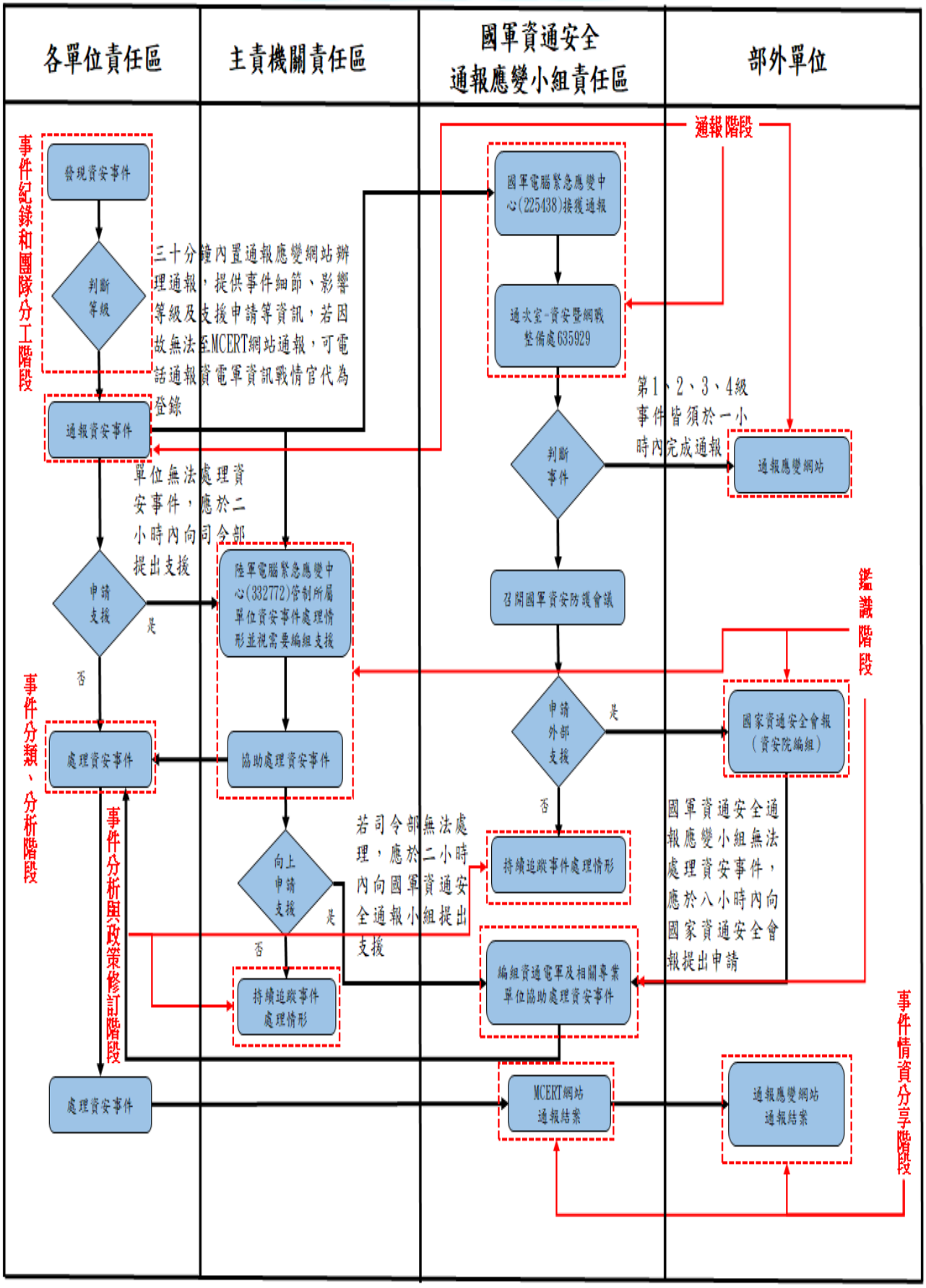

圖12 通報流程圖

資料來源：作者整理，參考陸軍司令部，〈資安事件通報應變實施計畫〉。

層級關係與程序差異分析

一、電腦緊急應變小組與資安防護管理中心層級關係

對於資安事件處理程序而言，CERT屬於第一線資安事件的處理人員，負責關鍵基礎設施領域系統維運、處理資安事件、提供緊急應變處置及降低資安事件發生的角色。當單位內部發生資安事件時，由緊急應變小組研判與掌握事件處理狀況，彙整相關資安事件資料蒐整，向領域SOC通報。

而SOC則是以掌握整體網路安全、資安威脅情蒐分析、訂定關鍵基礎設施資安監控與評估關鍵基礎設施安全政策為主軸，屬於整體網路規劃、安全評估、情資蒐集及情資分享的角色，透過公私部門情資分享掌握資安威脅情資，協助CI強化資安監控機制，預防資安事件發生。

整體而言，CERT負責快速反應並採取措施，以降低資安事件影響，解決正在發生的事件。與此同時，SOC則負責更高層次管理和規劃資安防禦策略，透過監控和情報分享來提升整體安全。這兩個單位密切合作和協調至關重要，能夠有效應對資安挑戰，確保組織的資訊系統和數據得到適當保護(層級界定關係如圖13)。

圖13 層級關係圖

資料來源：作者繪製。

二、ECIH電腦資安事件處理程序與陸軍資安防護管理中心緊急應變流程差異

企業網路環境與軍事網路環境架構有所不同，但在整體資訊網路安全上有一致性的目標，就是確保網路運作安全，依圖10事件處理與回應程序及圖12通報與應變作業流程來分析ECIH與ASOC電腦資安事件處理程序。現階段陸軍通報與應變流程以單位責任實施區分，企業則是以階段性區分，為使兩個通報與應變程序能在同一個階段比較，將陸軍單位責任區以階段區分並與企業六大階段做對比，以下就通報與應變作

業程序差異實施分析。

(一)事件紀錄與團隊分工階段(如表4)

在本階段ECIH於接獲事件通報時，由應變團隊先行判別事件屬性及威脅程度後才進行任務分配，使資訊人員通報與應變作業流程能更進一步掌握威脅資訊。而陸軍ASOC則是接獲事件通報時，先進行人員任務分配再進行事件屬性分析。

顯見兩者在應處程序差異上，對判斷事件屬性與威脅程度的先後順序有所不同，但對於事件威脅情資來說，情資的掌握是有助於團隊判斷方向與應處工具運用，這樣才能快速又準確的根除威脅，所以在這個階段中，優先判別情資威脅屬性及程度是最重要的。

表 4 事件紀錄和團隊分工階段

權責單位	應變處理程序	差異性
陸軍	事件發生，由 ASOC 判定一般違規或資安事件，若是資安違規，則依資安事件等級判斷基準進行判斷後，[23]再由 ASOC 依席位職掌進行分工。	■陸軍 事先席位任務分配，再進行屬性與威脅程度評估作業。 ■ECIH 企業先依屬性與威脅程度評估作業，再進行團隊任務分配。
ECIH	事件發生時，由領域內 CI 識別與記錄事件屬性及威脅程度，若判定屬資安事件，領域 CI 則依緊急應變團隊任務分配應處。	

資料來源：作者整理。

(二)事件分類與分析階段(如表5)

ECIH平時已編組鑑識團隊能即時介入數位犯罪調查。陸軍在資安事件成立後會編組鑑識團隊支援CERT。若以數位鑑識團隊的投入與分析能力來說，陸軍在數位鑑識準備程序與團隊整體鑑識能量較不足。數位環境強調的是蒐集數位證據的完整性與可用性，鑑識能量則攸關於分析能力與情資報告，能量不足恐導致人員對事件造成誤判或是低估危害程度。例：刑事警察在鑑識數位作業準備階段會先訂定編組與專責分工項目來進行後續現場證據蒐整作業。[24]

23 同註 1，頁 15。

24 林宜隆，〈建構數位證據鑑識標準作業程序(DEFSOP)與案例實證之研究〉《司法新聲》，第 101 期，出版社，民國 101 年 1 月，頁 59。

表 5 事件分類與分析階段差異表

權責單位	應變處理程序	差異性
陸軍	資安事件成立，由 ASOC 依照資安事件等級判斷基準分類。	■陸軍 ▲未具備事件分類與分析能力且數位鑑識團隊視狀況編組支援。 ▲明定核心資訊資產系統分類及適用範圍。 ■ECIH 具備數位鑑識團隊與事件分類與分析能力。
ECIH	資安事件成立，由領域團隊分工進行事件分類與蒐證，並將蒐整到的數位證據進行分析，依照事件影響程度來作優先處理。	

資料來源：作者整理。

(三)通報階段(如表6)

ECIH在通報階段未說明時間管制節點作為，僅就階段程序說明，陸軍在處置資安事件有明確規定通報與申請技術支援的時效，若以通報時效差異來說，陸軍在通報時效上較具優勢，其原因在於掌握事件初步通報時間，但因組織架構關係時效與技術申請恐會延長。例：申請國家資通安全技術支援應於8小時內申請。

表 6 通報階段差異表

權責單位	應變處理程序	差異性
陸軍	▲判定屬資安事件，通報過程由旅級 R-CERT 通報至軍團 C-CERT 再向上通報制 ASOC。 ▲資安事件限 30 分鐘內通報至 ASOC，資安違規事件限於 24 小時內回覆違規查察。 ▲申請技術支援應於 2 小時內向 ASOC 提出。	■陸軍 明確通報節點，但逐層通報時效性較低。 ■ECIH 未說明通報時效作為，僅內部通報管制。
ECIH	領域 CI 通報至領域 SOC 記錄與掌握，SOC 負責指導統籌領域專業團隊相關技術與事件管制	

資料來源：作者整理。

(四)鑑識階段(如表7)

ECIH鑑識階段上有明確規範出鑑識三階段的作業程序(圖11)，有助於團隊在整體鑑識的蒐集與調查。陸軍在鑑識作業程序上較不明確，然而鑑識團隊是提出技術申請後再進行編組投入，時效上恐延誤應處的最佳時間，兩者差異在於前、中、後的準備工作與鑑識團隊投入時間，其影響整體事件評估與分析報告的完整性。例：刑事警察在數位鑑識作業程序的準備階段時研擬作業流程，並提供第一線鑑識編組在操作階段能夠有規範來進行作業。[25]

表 7 鑑識階段差異表

權責單位	應變處理程序	差異性
陸軍	▲ASOC 團隊視狀況成立鑑識編組進駐到 CERT 協助。 ▲CERT 無法處置，應於 2 小時內向 ASOC 提出技術支援，ASOC 無法處置，應於 2 小時內向國軍資通安全通報應變小組申請技術支援。 ▲若需向國家資通安全研究院申請技術支援，應於 8 小時內提出申請。	■陸軍 ▲案發單位未具備鑑識能力，需仰賴上級數位鑑識團隊。 ▲犯罪現場數位證據受影響。 ▲組織需新增鑑識階段流程。 ■ECIH ▲具數位鑑識準備程序等三階段。 ▲具數位鑑識能力，直接對犯罪現場採集數位證據。 ▲實驗室可還原犯罪現場數位證據進行數據分析。 ▲明確訂定鑑識階段處理事項。
ECIH	▲數位鑑識準備程序區分準備階段、調查階段及事後調查三階段。 ▲領域 CI 編組內具有鑑識團隊進行證據蒐整與分析，若超出領域技術範圍由資安防護管理中心編組進駐到事發地點協助處理。 ▲採集數位證據後，在實驗室還原現場數位狀況，進行後續數位鑑識調查釐清病毒屬性或是滲透手法。 ▲釐清滲透手法或是病毒程式，立即將潛藏於復原系統內部檔案根除，實施復原系統。	

資料來源：作者整理。

25 同註 24，頁 60。

(五)事件分析與政策修訂階段

ECIH本身具備鑑識團隊，面對數位犯罪證據、損害威脅評估及數位調查報告能直接掌握，應變程序也能即時審視與修訂。陸軍CERT團隊本身不具備鑑識能量，必須由ASOC編組鑑識團隊介入整體事件調查，分析結果會由ASOC發布資安通報來即時修訂(表8)。例：刑事警察在數位鑑識實驗室訂定鑑識標準作業程序，提供第一線執勤與教育訓練有所依循，[26]面對作業程序不符也能適時修訂。

表 8 事件分析與政策修訂階段差異表

權責單位	應變處理程序	差異性
陸軍	資安事件發生時由陸軍通資部門統籌，透過各編組掌握事件發生期間所有威脅情資報告、損害評估、鑑識分析、政策修訂及事件揭露等相關資訊，使整體事件資訊和數據能夠充分掌握。	■陸軍 ▲事件進度、技術支援及數位調查報告須上級鑑識團隊協助。 ▲政策修訂以資安通報發布。 ■ECIH ▲直接掌握鑑識事件進度、損害威脅及數位調查報告。 ▲政策或應變處置流程可依調查報告即時進行內部政策修訂後頒布。
ECIH	CI 鑑識團隊分析事件威脅等級後進行分類，並評估事件影響層面與損害計算記錄，整理完整證據製作安全事件調查報告，提供後續決策層面在政策修改之建議。	

資料來源：作者整理。

(六)事件情資分享階段(如表9)

ECIH事件分析後所產生的安全調查報告，將充分揭露整體事件的分析結果，透過分享資安情資與分析報告，進行有效的預防措施與聯合防禦機制。陸軍在整體資安事件結束後，必須由軍種司令部通報至國防部MCERT辦理結案，若以情資分享差異來說，企業界與公部門分析的結果都會交換到ISAC來作分享，使整體都能預防類似的事件，並非單一群體掌握情資。例：我國八大關鍵基礎設施與民營企業均

26 同註 24，頁 61。

會將威脅情資回傳到ISAC共享到各機關領域。

表 9 事件情資分享階段差異表

權責單位	應變處理程序	差異性
陸軍	通報與應變作業流程以完成處理並通報 MCERT 當作事件結案節點。另於一個月內完成相關調查報告及佐證資料回傳 ASOC 登錄。	■陸軍 ▲情資分享僅於軍種體系資安通報。 ▲資安事件通報至國軍資安防護管理中心辦理結案。 ■ECIH ▲SOC 情資透過 ISAC 分享至跨領域 SOC。 ▲ISAC 提供各領域資安情資分析、回饋、威脅指標及滲透手法調查報告。
ECIH	調查結束後，將安全調查報告資訊充分揭露，揭露資訊要避開商業機密，針對處理程序、通報程序、事件威脅分析、事件威脅分類、評估傷害程度、入侵指標及鑑識報告作揭露，並將威脅情資分享至 ISAC 透過跨領域資安聯防分析與回饋，提供威脅指標與手法，產製聯防情資報告。	

資料來源：作者整理。

三、小結

在資安防護層級關係中，CERT專注於資安事件的即時處理，負責應急反應與控制，SOC則偏重整體資安策略之規劃，強調情資分析與預防能力的提升。兩者功能各有其重點，CERT著眼於事件後處置效率，而SOC則專注於事件前預警與防禦。透過密切協同合作，使兩個單位有效整合應急處置與預防措施，將全面強化資訊系統的安全性與穩定性。

陸軍資安事件應變流程中，雖然通報階段已有初步規範，能迅速通知通資部門掌握事件，惟結案時僅通報國防部MCERT，未能如ECIH向ISAC進行情資分享，導致橫向交流與聯防機制不足。此外，陸軍在事件紀錄與團隊分工上，因優先分配任務後再進行威脅評估，會導致評估延遲。數位鑑識準備程序與能量不足，可能造成威脅程度低估和情資分析不足，而現行ASOC鑑識團隊支援需申請後進駐，延誤鑑識時效，增加證據破壞風險，相較於ECIH三個階段之鑑識流程則較完善。

後續陸軍政策單位可參考 ECIH 鑑識階段來加強鑑識準備與情資分享機制，並

結合實驗室模擬網攻，運用內部教育及外部委託培訓，全面提升應變能力，達成情資整合與資安聯防目標。

結論

我國自民國90年起，陸續推動資通安全基礎建設工作，為配合關鍵基礎設施保護的基本政策，政府制定CERT實務建置指引與SOC實務建置指引，以提供公部門及各領域關鍵基礎設施參考，進一步發展出專屬於各領域的緊急應變與資安防護管理機制。

陸軍通資部門於民國109年因應「資料中心暨異地備援」資訊系統的實際需求，強化資安防護能力，將原CERT緊急應變小組升級為資安防護管理中心(ASOC)。此項升級不僅提升編組分工及應變作為，更進一步擴展資安防護單位的層級與職能。

由於陸軍資安單位成立時間尚短，在電腦資安事件處理流程與應變程序上存在不足，分析其原因，主要在於資安鑑識應處能力不足、人員資安防護技術有限，以及跨軍種情資分享機制尚不完善，為改善上述問題，本文提出三個建議，期望作為陸軍組織發展與教育訓練的長期營運目標之參考。

一、提升資安鑑識應處能力

電腦資安事件和危機事件的應對與處理，其中鑑識是不可或缺的一部分。在上一章程序差異分析中，事件分類與分析階段、通報階段以及鑑識階段都提出數位鑑識的重要性，當前ASOC所面臨的問題是數位鑑識經驗不足以及第一線資訊人員面對資訊犯罪現場不知如何處置，導致在現場已經破壞數位證據的完整性，政策單位可參考圖11建置數位鑑識準備程序，提供人員在數位鑑識當中有所依循，同時強化通報機制和緊急應變流程，確保事件可以即時被發現、報告和應處，以最大限度地減少損失並恢復正常運作，在事件擴大損害前，應於事前建立完善的資安政策和程序，包括風險評估、資產管理、系統權限控制、系統監控等處理程序以預防資安事件發生。陸軍通報與應變作業流程當中以責任區劃分權責並沒有針對事件的階段來區分，建議參考圖12將階段修訂到通報流程圖中也能明確了解單位責任區所負責的處置階段，處置階段細節可參考圖10，提供CERT在應變處置中能夠清楚階段內需負責項目。

若資安事件影響達到「一級」、「二級」、「三級」、「四級」時，鑑識須由ASOC編組專責團隊介入調查，負責蒐整證據、保全資料和分析資料以及事件報告，利用軟體工具重建資安事件發生的情況，進行數據恢復和重建，以數據分析，追蹤事件來源和傳播路徑，進行詳細調查和分析，找出事件來源、影響範圍和受影響資訊資產，及攻擊者身份和行為軌跡，以便釐清事件全貌和影響。鑑識報告應詳細記錄證據和分析結果及專業意見並符合當地法律法規和相關標準，確保整體證據的合法性和可用性，以

支援事件調查和法律程序(如圖14)。

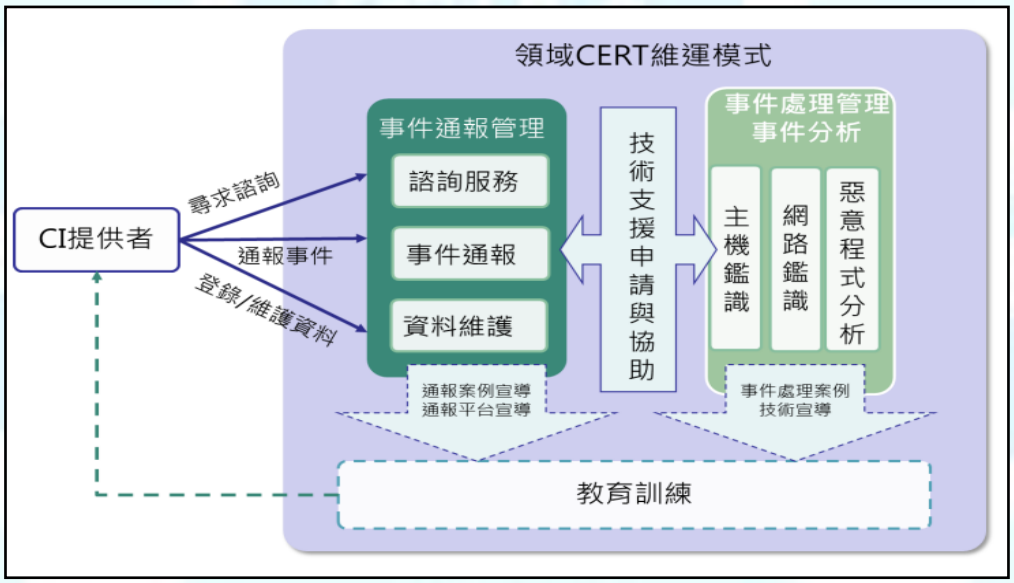

圖 14 危機事件與處理原則圖

資料來源：國家資通安全防護整合服務計畫〈領域 CERT 實務建置指引〉《數位發展部資通安全署》，https://moda.gov.tw/ACS/operations/ciip/650，檢索日期 2023 年 10 月 17 日。

二、強化人員資安防護技術

檢視關鍵基礎設施的安全風險時，除了法規、管理與技術設備外，不能忽略「人」的角色。企業安全專家徐子文強調「科技存在的目的是協助執行程序，人，才是所有事件的根本」。[27]人員培育必須重視，組織人才除專業培訓課程外，建立資安人員資料庫更為關鍵，尤其在數位化和資訊化程度日益提高的年代。資安教育訓練的目的是確保組織內部人才具備足夠技術和意識來保護敏感資訊和資源，才能有效應對日益複雜的安全威脅。

人才培育方面陸軍應制定明確的職業發展計畫並鼓勵支持所屬資訊人員持續提升資安技能和知識，以下提供陸軍培訓資訊人員的國際資安證照參考方向，新進人員建議參考入門「資訊安全管理」思科認證網路工程師(CCNA)或Comp TIASecurity+國際網路資安認證班。

各階層資訊官或資訊人員需管理網路存取與資訊機房者，建議參考中階證照「事故應變」、「資安防護技術」及「網路存取管控」，證照分別為資安災害復原專家認證課程(EC-Council EDRP)、威脅情資分析專家認證課程(EC-Council CTIA)及安全最佳化-網路設備與遠端存取(SONDRA)。

鑑識團隊、各階層資訊官建議參考高階證照「應變鑑識」與「資訊安全管理」，

27 資安人編輯部〈資安即國安與日常生活密不可分關鍵資訊基礎設施保護〉《資安人》，http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=8456，(民國 106 年 06 年 19 日)，下載時間：民國 112 年 11 月 15 日。

證照分別為資安危機處理員認證課程(EC-Council ECIH)與資安系統專家認證(CISSP)，資訊人員取得證照後，將課程知識與管理經歷融入後，在日後的教育課程訓練上可針對如何識別常見威脅類型、漏洞攻擊、社交工程攻擊、釣魚郵件、惡意軟件等常見的風險態樣說明，提升人員安全意識(如表10)。

整體來說，人才培育與教育訓練是一個持續不斷的過程，需要陸軍和個人共同努力，以應對快速變化的安全威脅和挑戰。通過投資於這方面，陸軍可以提高自身的安全防禦能力，減少安全事件的風險，並確保組織持續安全性。

表 10 國際資安證照

國際資安證照		
	類別	項目
入門	「資訊安全管理」	1.思科認證網路工程師 (CCNA) 2.CompTIA Security+國際網路資安認證班
中階	「事故應變」 「資安防護技術」 「網路存取管控」	1.資安災害復原專家認證課程 (EC-Council EDRP) 2.威脅情資分析專家認證課程 (EC-Council CTIA) 3.安全最佳化-網路設備與遠端存取 (SONDRA)
高階	「應變鑑識」 「資訊安全管理」	1.資安危機處理員認證課程 (EC-Council ECIH) 2.資安系統專家認證 (CISSP)

資料來源：作者整理。

三、提升跨軍種情資分享

依據國家關鍵基礎設施(CI)發展運作與政策制定區分能源、水資源、通訊傳播、交通、金融、醫療、中央與地方機關，與高科技園區等八大領域，各領域會設置領域專長內的CI-CERT、CI-SOC及ISAC，形成資安聯防與網路合作，組成國家資安聯防體系。[28]在上一章差異分析中事件情資分享階段，也提到資訊分享與分析中心(ISAC)，各領域情資蒐整後彙整到ISAC統一作跨領域的資安分析與回饋，形成聯防情資，[29]達到有效的資安防護網。若將SOC建置到各軍種軍團或大隊層級，由作戰區擔任SOC角色掌握作戰區內資訊網路系統與系統監控等服務，除減少通報時效外，還能在作戰區資訊編組新增鑑識小組，即時應處資安事件的擴大。作為軍種司令部層級可擔任ISAC來掌握各軍種內部情資來針對政策修訂、系統預防、系統偵測等應變措施來做改

28 國家資通安全研究院〈國家資安聯防監控中心 N-soc〉，《國家資通安全研究院》，https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/，(民國 113 年 03 年 13 日)，下載時間：民國 113 年 04 月 15 日。

29 歐柏昇，〈嚴密監控戰情！資安組織聯手構築防禦陣線〉，《科技魅隱-談觀點》，https://www.charmingscitech.nat.gov.tw/post/perspective10-soc，(民國 112 年 06 月 09 日)，下載日期：113 年 2 月 13 日。

善。另一層面的跨軍種的資安領域機構，除情資相互共享外，共同協防的資安縱深防禦會更加嚴密。

參考文獻

一、官方文件：

(一)數位發展部資通安全署：〈領域cert實務建置指引〉，民國106年03月。

(二)數位發展部資通安全署：〈領域soc實務建置指引〉，民國106年03月。

(三)數位發展部資通安全署：〈領域isac實務建置指引〉，民國106年03月。

(四)數位發展部資通安全署：〈資通安全專業證照清單〉，民國106年03月。

(五)國家資通安全研究院：〈政府領域聯防監控作業規範〉，民國112年06月13日。

(六)國家資通安全研究院：〈國家資安聯防監控中心N-soc〉，民國113年3月24日。

(七)陸軍司令部：〈陸軍資訊資產管理作業規定〉，民國111年11月03日。

(八)陸軍司令部：〈陸軍資安事件通報應變實施計畫〉，民國112年06月13日。

(九)陸軍司令部：〈陸軍資安防護管理中心(ASOC)值勤作業規定〉，民國111年03月25日。

(十)陸軍司令部：〈陸軍113年通資勤務管理實施計畫〉，民國112年12月1日。

二、書籍

(一)EC-Council Certified Incident Handler Copyright by EC-Council, EC-Council Certified Incident Handler v2 – Vol 1(2019)。

三、期刊

(一)林宜隆、周彥霖，〈軍事院校資安管制措施之探討─以數位證據鑑識標準作業程序為例〉《電腦稽核期刊》，第28期，民國102年7月。

(二)林宜隆，〈建構數位證據見識標準作業程序(EDFSOP)與案例實證研究〉，《司法新聲》，第101期，民國101年1月。

四、學位論文

(一)陳恒鈞，〈我國國軍資訊安全政策探討：危機管理觀點〉(淡江大學公共行政學系公共政策碩士在職專班/碩士論文，民國97年6月)，http://dx.doi.org/10.6846/TKU.2008.00640。

(二)吳嘉龍，〈資訊安全風險管理與電腦緊急應變發展研究探討〉，民國104年09月。

五、網路

(一)數位發展部資通安全署，〈資安政策與法規〉，https://moda.gov.tw/ACS/operations/policies-and-regulations/648，(民國96年02月15日)，下載時間：民國113年5月28

日。

(二)全國法規資料庫：〈資通安全事件通報及應變辦法〉，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305，(民國110年08月23日)，下載時間：民國113年6月15日。

(三)歐柏昇，〈嚴密監控戰情！資安組織聯手構築防禦陣線〉，《科技魅隱-談觀點》，https://www.charmingscitech.nat.gov.tw/post/perspective10-soc，(民國112年06月09日)，下載日期：民國113年2月13日。

(四)編輯部，〈資安即國安與日常生活密不可分關鍵資訊基礎設施保護〉，《科技魅隱-談觀點》，https://www.charmingscitech.nat.gov.tw/post/perspective10-soc，(民國106年06月19日)，下載日期：民國113年2月13日。

(五)臺北精誠資訊股份有限公司復興分公司〈藍隊資安事故處理-EC-Council ECIH認證課程〉《UCOM恆逸》，https://www.uuu.com.tw/Course/Show/698/EC-Council-ECCIH資安危機處理員認證課程，檢索時間：民國113年4月19日。

(六)BSI〈網路安全事件應變step by step〉《bsi》，https://www.bsigroup.com/LocalFiles/zh-tw/news/NO164/Cyber-Incident-Response-Step-by-Step.pdf，下載時間：民國113年4月22日。

作者簡介

李建億上士，儲備士官103年班、士官高級班107年班；曾任資訊士、組長，現任職於通訓中心網路作戰組教官。