以服務導向設計之教育學術資安資訊分享與分析中心

曾龍[1] 劉育佐[2] 陳麒元[2] 趙涵捷[2,3]
[1]崑山科技大學資訊工程學系
[2]國立東華大學電機工程學系
[3]國立宜蘭大學資訊工程研究所
E-mail：btseng@mail.ksu.edu.tw; yutso.liu@msa.hinet.net; chiyuan.chen@gmail.com; hcc@niu.edu.tw

摘要

資安資訊分享與分析中心（Information Sharing and Analyzing Center, ISAC）具有建立資安事件與情報蒐集、分析並產生對策能力的特性，它陳述資訊對於預防網路安全事件能提供預警功能，而且也可經由不同的組織與機構來共同分享，進而進行資訊分析研判的一個機制。本研究針對臺灣學術網路(TANet, Taiwan Academic Network)，提出教育學術資安資訊分享與分析中心(Academic Information Sharing and Analyzing Center，A-ISAC)，並應用服務導向架構之設計以改善作業流程與分享機制。

***關鍵詞**：資訊安全、資安資訊分享與分析中心、服務導向架構*

Abstract

Security Information Sharing and Analysis Center (ISAC) is an integrated mechanism to improve network security through information collection, analysis, dissemination, early warning, and response. It also provides the security information sharing platform between different organizations. In this paper, we proposed an Academic Information Sharing and Analyzing Center (A-ISAC) for Taiwan Academic Network (TANet). Furthermore, we design A-ISAC based on the Service Oriented Architecture (SOA) to improve workflow and sharing mechanism.

***Keywords**: Information Security、Information Sharing and Analysis Center、Service Oriented Architecture*

1. 前言

近年來資訊安全迅速成為網管的重要工作之一，臺灣學術網路(TANet, Taiwan Academic Network)[12][13]連接國內教育單位與研究單位的骨幹網路，擁有廣大的使用者群，資訊安全更是首要工作。過去因缺乏一套完整的資安資訊分享機制，各單位需要依靠少數的資安人員進行資安防護工作。本文提出教育學術資安資訊分享與分析中心(Academic Information Sharing and Analyzing Center， A-ISAC）[9]建置，其主要可分成兩大主軸，第一個將以教育機構資安通報平台為主軸之內部分享平台。第二個則關注於和其他單位之資訊分享平台(ISAC 外部分享平台)。

由於 ISAC 涉及資安資訊分享與分析平台之建置、分享安全機制、外部單位與系統之介面設計、風險評鑑、評分燈號設計、威脅與脆弱性分析等諸多議題[1-6]，本文針對 TANet 上經常受關注之資安相關議題，逐步建立具教育體系特色之資安資訊交換及分析防護機制。我們利用 A-ISAC，結合區域和縣網路中心，在 TANet 創建一個統一的防禦系統，實現資訊安全的多層次的縱向防禦系統。在本篇論文中，我們的設計注重在 TANet 上建置 A-ISAC，以改進在教育系統中的資訊和通信技術安全環境為主。本論文後續編排如下，第 2 章介紹本研究之相關背景，包含台灣學術網路現況與國內外 ISAC 發展狀況，第 3 章呈現本研究之服務導向 ISAC 系統設計，並分析本系統設計之目標、需求。最後則是結論和致謝。

2. 背景介紹

臺灣學術網路(TANet)於 1990 年 7 月建置以來，由教育部發起，邀集 13 所學校建立區域網路骨幹及結合 25 個縣市地方政府所組成一個階層式的學術網路架構[13]，是國際上少數完整教育體系的網路架構，目前所連接的學校及學術機構約有 4,108 個連線單位，使用人數超過 4 百萬人，藉由臺灣學術網路(TANet)的網路基礎建設，可以有效的發展校園資訊技術及培育資訊人才。校園網路資訊安全與政府機關及民間企業不同，必須兼顧校園學術自由發展，其中對於學生成績及師生個人資料的保護、保持研究實驗室的自由性、維持電腦教室及學生宿舍網路使用流暢性等都是重要的議題，目前高中職以下校園資訊環境、技術人力、經費普遍不足，又須抵禦外界駭客入侵、網路病毒攻擊，校園網路安全推動實屬不易。

縱觀我國網路發展，可以粗分為政府網際服務網(GSN)、臺灣學術網路(TANet)、台灣高品質學術研究網路(TaiWan Advanced Research and Education Network, TWAREN)以及許多國內網際網路服務提供者(Internet Service Provider, ISP)，一旦發生大量資安攻擊源自於國外網路，尚可透過國內網路主管機關以邊界閘道及資安機制加以限制，倘若資安攻擊源自於國內網路將使得防禦工事相當棘手，因為

必須在抵禦攻擊的同時兼顧網路的可用性，因此國內各網的基礎資安防禦工事不容小覷。

為打造TANet安全信賴的學術資通訊環境，根據行政院國家資通安全會報「建立我國通資訊基礎建設安全機制計畫(98-101年)」—推動教育體系資通安全計畫(教育部)，97年起教育部規劃建置教育學術資安資訊分享與分析中心(Academic Information Sharing and Analyzing Center)。

資訊分享與分析中心（Information Sharing and Analyzing Center，以下簡稱 ISAC）[10][11][14]，具有建立資訊安全事件與情報蒐集、分析並產生對策能力的特性，ISAC 陳述的資訊對於預防網路安全事件能提供預警功能，而且也可經由不同的組織與機構來共同分享，進而進行資訊分析研判的一個機制。ISAC 源起於 1988 年 63 號美國總統決策令（PD633），該決策要求各政府部門需與相關民間產業間建立夥伴關係以分享資訊(ISACs)，共同協助保護美國個別關鍵基礎建設，進行資訊安全相關資訊的蒐集、分析、判斷與傳遞給產業界與國家基礎設施保護中心(National Infrastructure Protection Center, NIPC)，並供關鍵基礎設施確保部門(Critical Infrastructure Assurance Office, CIAO)據以發展出減少對可辨識脆弱點之蓄意探索的修補計畫。在美國政府的推動下，2001 年 1 月 16 日由 AT&T、Cisco、CA、HP、IBM、Intel、KPMG、Microsoft、Oracle 等 16 家知名資訊技術業者各自出資 65 萬美元，建立一個非盈利性組織。其目的是針對系統的弱點對網際網路的影響等問題，相互交流資訊分析問題尋求解決方法。

圖 1 美國 IT-ISAC

美國民間企業部門已遵照第 63 號總統決策令的建議，成立相關協會以從事資訊分享工作，目前美國現有重要基礎建設的 ISAC，涵蓋 IT、金融、電力、能源、運輸、供水等產業，並成立美國 ISAC 服務機構，其重點在建立及維護 ISAC 之間和政府的互動架構，ISAC 機制架構也包含建立身份辨識、安全通道、資訊過濾等功能及審查核准程序，著重資訊保護，包含來源確認(Authenticity)與不可否認(Non-repudiation)、責任聲明(Disclaimers)、來源保護(可能需至無法辨識來源 ISAC 的程度)、依事先定義的保護層級進行有限定對象的發佈，以及發佈授權。美國學界的 Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)[7]，REN-ISAC 建置的目的是為了進行資訊安全訊息的蒐集、分析、發佈通知或作為資安預警防護之設計用途，以提供分享給高等教育和研究網路。隨著各種資訊的投入其中處理分析，從各個骨幹網路之設備蒐集訊息，從各連結和校園提供者分享之事件報告，並結合政府和執法機構，以及橫向擴展及其他行業 ISAC 互動合作。有了上述的運作，再加上這些適當的整合和分析工具，及經驗豐富的資安事故應變團隊，以至於 REN-ISAC 在當前美國的高等教育界肩負著整合、分享與處理應變資安問題一個相當重要的角色。REN-ISAC 現在主要提供以下服務:

- 為美國高等教育提供預警和相對網路的威脅和相關弱點，提升資訊的分享與相互彼此的溝通。
- 整合正式加入美國ISAC的產業夥伴和US - CERT 公司，美國國土安全部門等，一同透過互助分享的模式，來有效防護美國國家關鍵網路基礎設施。
- 接收、分析和通報網路安全威脅、警告和攻擊等訊息。
- 24×7運作監控平台。

目前全球除了美國以外，日本對於國家整體的資訊安全建置亦規劃的相當完整，有 NISC (National Information Security Center)[8]國家資安組織以外，也有 ISAC，但其 ISAC 功能與美國之 ISAC 較為不同，日本之 ISAC 類似美國 SOC 加 ISAC。而日本的 CEPTOAR 則與美國的 ISAC 較為相似。美國 ISAC 推動與日本 T-ISAC 的建置成效在安全防護的工作中已留下良好成效的案例，值得我國借鏡。關鍵基礎網路設施的安全問題關係到整體國家的運作，而 TANet 為整體學術發展的重要網路骨幹，且在資安技術評估新攻擊方法發展趨勢和設計防護機制上，也需仰賴資訊分享與分析機制之建立來邁進更新的研究發展。

3. 服務導向 A-ISAC 系統設計

3.1 A-ISAC分享平台

教育學術資安資訊分享與分析中心(A-ISAC)之設計，其主要可分成兩大主軸，第一個將以 TANet 資安通報應變平台為主軸，包含弱點與威脅資料庫之建置、內部分享平台(資訊分享/討論/社群網站與資安研發分享網站)與 TANet 資安通報/應變/公告/教育平台。第二個則關注於和其他單位之資訊分享平台(ISAC 外部分享平台)，此部份將援用行政院研考會所制訂之 G-ISAC 格式，並以 Web Service 技術進行開發。

為使教育機構所使用之資安通報平台能更有效率，並能提供更多服務，因此，A-ISAC 教育學術資安資訊分享與分析中心整合下列六大子平台，如圖 2 所示：

(1) 教育機構資安通報平台

(2) 資安資料庫平台(包含弱點與威脅資料庫)

(3) 資安論壇

(4) 資安分析報告

(5) TANet資安教育訓練平台

(6) 教育機構資安分享與分析中心

圖 2 教育機構資安分享與分析中心與其子平台

3.2 教育機構資安通報平台

教育機構資安通報平台(後續簡稱為資安通報平台)為本研究核心所在。資安通報平台主要是透過建立完善之資安事件通報流程，以期當校內資訊及網路系統在遭受到破壞或不當使用等緊急資通安全事故發生時，能在第一時間內迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害。此資安通報平台功能包括:

- 提供不同角色(Role:各校網路管理人員)之權限，如圖3所示。
- 建置可線上填寫資安通報內容之網站。
- 建置符合教育部規範的資安標準作業程序之自動化通知與提醒的電子化工作流程。

使用角色	工作事項
教育部人員	➢ 監督下屬機關資安通報
營運團隊	➢ 審核下屬機關資安通報 ➢ 追蹤與提醒下屬機關資安通報
區縣市網資安人員	➢ 協助第一線人員資安通報 ➢ 自行通報資安事件
第一線人員	➢ 資安事件通報與處理 ➢ 資安聯絡人資料填寫

圖 3 角色與工作事項

本項目重點在於通報格式與通報流程的設計，設計通報格式之目的在於提供網管人員輸入完整的資訊，讓通報的內容更具參考價值。資安通報平台目的在於當資安聯絡人提出進行通報後，需符合本項目所規劃之教育部標準資安流程來處理與應對後續的事項，以期能在第一時間內迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害。

本項目以 Java EE/J2EE 架構進行相關流程開發。首先完成不同等級(0-4 級)、不同種類(自行通報、告知通報)之通報應變流程。再根據這些流程之SOP(標準作業程序)進行程式實作。為確保網路之可行性(Availability)，我們以叢集技術加以開發，並為避免 SQL Inject 攻擊，使用 MD5 編碼與圖形驗證碼技術。

3.3 資安資料庫平台

資安資料庫平台包括弱點資料庫與威脅資料庫。弱點資料庫主要的目的在記錄與整理程式或系統本身造成安全漏洞的原因，例如某個特定的埠不正常的開啟或不適當地運作，或是某個特定版本的程式可能存在某種程度的安全漏洞，有進一步造成入侵危害之虞。威脅資料庫主要的目的在記錄國內外已有發生的重要資安事件的處理經驗。

威脅與弱點資料庫不同在於，威脅是已有實際的攻擊案例發生或 Toolkit 工具的釋出，由於網際網路的便利性，容易讓有心人士輕易取得這些方法或工具，進而對系統造成威脅和危害。建置弱點與威脅資料庫，我們著重於下列幾個面向：

- 弱點與威脅資訊的更新與維護
- 最新弱點的補充
- 弱點與威脅描述、修補方法等內容實用性與正確性
- 弱點與威脅來源的確認 (符合軟體廠商或國際安全組織所公佈)

3.4 資安論壇

資安論壇功用在提供一個開放性的架構讓任何加入平台的會員都能夠透過連上網際網路的人在同一個網站上與各個參與者，針對同一主題發表意見、互動交流，及傳播與瀏覽不同主題的「內容」。參與者可以根據各種主題張貼訊息或讀取其他參與者所張貼的訊息，形成一個交流經驗、專家間分享知識，從中找到問題的解答、分享最新的資安技術，以及最新資訊安全警訊的管道平台。上述的開放性架構必需建置在權限存取的管理基準上，用以達到享受越多權利，就需盡更多義務的角色關係。最主要之設計與開發為以下兩個面向為要點：

- 提供不同角色(Role:一般會員,站長,系統管理員)的存取權限

- 提供多種主題及討論之實際案例

3.5 資安分析報告

資安分析報告(如圖 4)旨在提供國內外重要資安技術與研究成果之分析報告，現階段已提供三大類分析文件，包括：(1)資安分析文件、(2)綜合分析文件、(3)威脅趨勢文件。資安分析文件強調國內外學術界重要資安研究成果，現階段已完成包含：Conficker 行為模式分析與偵測技巧、Spyware 惡意軟體之偵測與防禦、SQL Injection 的自動化預防：CANDID、Torpig Botnet 行為分析、多型混合攻擊 Polymorphic Blending Attacks 技術分析、惡意 Flash 廣告之偵測與分析、整合 one-class SVM 的 Payload-based 異常入侵偵測系統、應用資料行為模型的入侵偵測系統等 7 篇文獻報告；綜合分析文件強調重要資安主題的多方面綜合性報告，將以長期的追蹤與彙整為主軸，現階段已完成包含：(1)BufferOverflow 攻擊、偵測與防禦、(2) Payload-based 資料探勘演算法應用到網路安全研究等兩篇文件，此部分文件將每半年更新其最新發展。威脅趨勢文件則彙整國內外重要資安廠商與研發單位所完成之資安趨勢報告為主，現階段已完成 OWASP 2010 TOP10 Web 應用弱點威脅。

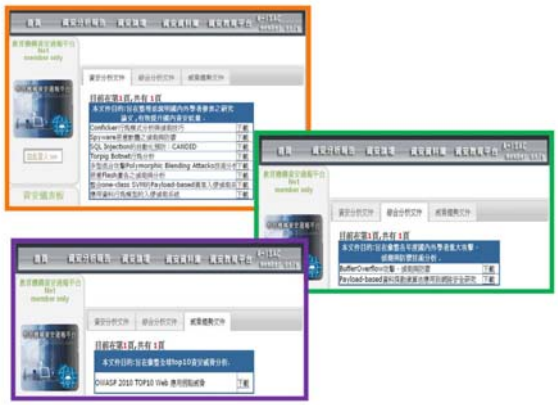

圖 4 資安分析報告

3.6 TANet資安教育訓練平台

TANet 資安教育訓練平台針對各級資安與網管人員製作訓練教材、針對各層級提出訓練計畫及辦理教育訓練課程，如圖 5 之管理人才與技術人才。

對於不同權限人員，應提供不同層次之訓練內容，課程內容與訓練對象可依主辦單位之需求加以調整，且教育訓練方式須採線上電子教材。其設計重點為：

- 建置以時事性、重大性、新聞性之資安事件教育訓練平台。
- 提供資安事件實際處理之教學影片。

本項目以 moodle 建置 TANET 資安教育平台，最主要工作在於課程教材之設計，本項目已完成三大類型(網路管理、資安技術、攻擊測試) 十門課程，以提高各級資安人員於資安事件處理之效率與準確。

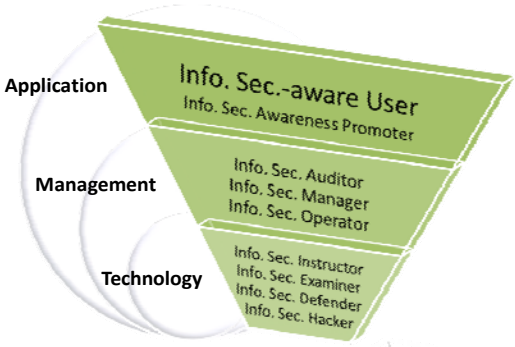

圖 5 TANet資安教育訓練架構

3.7 教育機構資安分享與分析中心

本項為第二個設計主軸，關注於和其他單位之資訊分享平台，此部份開發需符合行政院研考會所提之 G-ISAC 格式，並以 Service-Oriented Architecture(SOA)架構進行 Web service 的開發。外部分享平台的開發上，要考慮不同分享單位的資訊分享，因此需制定一套資料交換格式標準提供給分享單位，使其依照此標準開發分享平台。本項目主要是以 G-ISAC 情資交換格式為基礎，做為通報與威脅情資交換架構的標準規範。在此分享機制上架構如圖 6 所示。

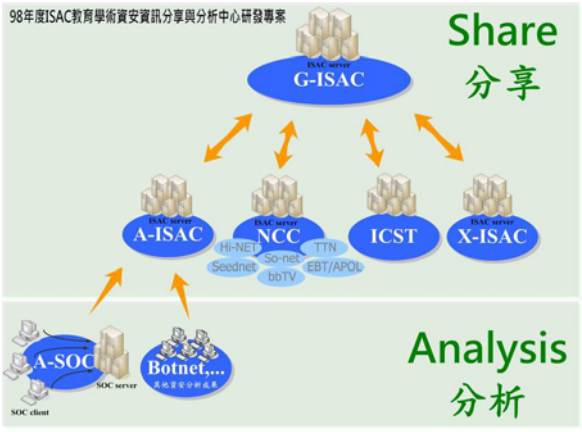

圖 6 分享機制架構圖

分享架構三個最核心的主題分別為:(1)分享的內容；(2)分享的格式；(3)分享的技術與架構。因此需完成下列之功能需求:

(1) 需可分享行政院技術服務中心所規範之情資內容。[(1)分享的內容]。

(2) 需可配合參與實作行政院技術服務中心制定之G-ISAC 共通規格。[(2)分享的格式]。

(3) 需參考與實作行政院技術服務中心所提之 web service 分享機制架構。[(3)分享的技術

與架構]。

資訊分享機制主要由行政院來提供整體的資訊分享，而這些資訊來源則是由國家各處所部署之 SOC 提供，另外，在於各家 SOC 廠商之警報資訊格式皆不相同，因此在進行資訊之分享前，需依據行政院所規範之標準交換格式來進行正規化之處理，以將其警報資訊格式進行統一，達到資訊可共享之目的。

行政院技術服務中心針對資安交換格式標準的制定上主要是以"事件物件描述和轉換格式--IODEF(Incident Object Description and Exchange Format)"為參考規格。電腦事件正在逐漸變為分散式和國際化的事件，許多事件突破了國界、語言和文化的約束。各國的電腦安全事件回應組(CSIRTs)瞭解到資訊轉換以及合作在處理、跟蹤和調查安全事件中的優勢所在，在所有這些事件中，資訊轉換的關鍵因素在於事件(物件)描述的通用格式方面。IODEF 主要目標是要解決過多人工產生的無結構安全事件通報(包括垃圾郵件的通報)，或是自動產生但屬於自行創建的專屬通報格式，造成不易分享與自動處理的問題。IODEF 定義了通報的通用資料格式，該資料格式用於 CSIRTs(計算機安全事件回應組)(包括：報警、事件調查、存檔、統計、報告等)之間事件資訊的描述、存檔和轉換。

除了分享的格式外，研考會也針對分享之內容進行相關標準之制定。目前依據研考會規劃的情報種類有 5 大類型(資安訊息情報(ANA) ，資安預警情報(EWA) ，網頁攻擊情報(DEF) ，入侵事件情報(INT) 與回饋情報(FBI)，包含 22 種事件分類。由於本項目著眼於不同平台之自動化分享，因此 G-ISAC 與 A-ISAC 的分享流程需透過共通格式加以規範。本項目針對不同情報類型分別使用符合 IODEF 規範的 XML 檔，並於接收與傳送不同格式的資安情資前進行格式驗證，以確保資安情資的正確性。

就技術而言 ISAC 外部分享平台，現階段主要根據 G-ISAC 情報交換格式標準來進行資訊分享，A-ISAC 伺服器端主要透過 Web Services 技術，提供 A-ISAC 客戶端傳輸分享情資之交換中心，由客戶端將其分享情資給予標準化後傳回伺服器端，再由伺服器端進行後續分享之處理。

在實作上，本項目使用基於服務導向架構(SOA)進行設計，其目標為透過「服務元件」結合「流程」以提供更多樣的自動化分享服務。要達到一個自動化的分享行為，需以跨系統的資料交換與傳遞的規範與方法(方法論)，以利分享資訊交換，並實作負責資訊的交換與傳遞的模組(服務元件)。我們採用 Web Services 技術來進行開發(如圖 7 所示)，並部屬於 JBoss (JavaEE AP server) 平台[15]，其中使用到 Jboss-WS 元件與 Eclipse 開發工具來進行 Web Services 之系統研發。Web service 是新型分散式系統的技術，特別適合大型異質性整合型系統之架構。其優點在於透過 Web Services 技術的使用，系統使用者不必擔心服務建構在甚麼平台，或使用甚麼技術實作，亦可更快速及低負擔地將服務更換或更新。

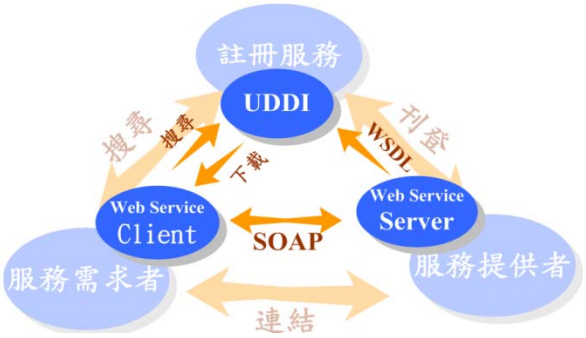

圖 7 Web Service架構

根據圖 8 所示，外部資安資訊分享上，主要涵蓋三個處理模組：

傳送資安分享訊息：A-ISAC 客戶端需根據 G-ISAC 情報交換格式進行資訊正規化，將其欲分享之資訊，依據欄位進行正規化，並透過 Web Services 回傳至 A-ISAC 伺服器端。

接收資安分享訊息：A-ISAC 伺服器取得 A-ISAC 客戶端分享資訊後先通過格式驗證確認後再進行判斷內部分享與外部分享等分類儲存

分享資訊：A-ISAC 伺服器將欲提供分享之資訊定時將其資訊填入 XML 對應的元素中，藉此建立統一格式之 XML 分享檔案，藉以分享給其他外部分享單位。

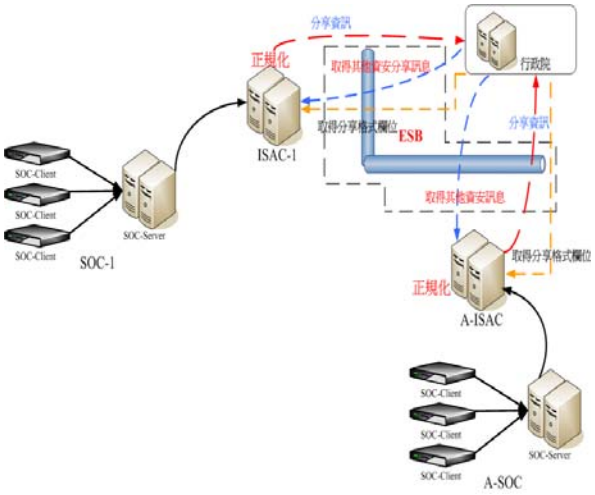

圖 8 分享機制架構圖

4. 結論

TANet教育學術網路被視為整體學術發展的重要網路骨幹，其 TANet 網路上的攻擊層出不窮，因此在資安技術評估新攻擊方法發展趨勢和設計防護機制上，也需仰賴資訊分享與分析機制之建立以

更進一步強化安全機制。承上之考量，藉由整合各學術機構 (如國小、國中、高中、大學等)提供資訊，再將其資訊彙總、分析，並進一步在 G-ISAC 架構下來與相關機構的成員分享，將有助於國家關鍵基礎網路設施的防護。

透過所教育機構資安通報平台,建立完善之資安事件通報流程，做為校內資訊及網路系統在遭受到破壞或不當使用等緊急資通安全事故發生時，能在第一時間內迅速進行必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害。藉由此研究設計中之各子平台之建置與部署，得以培養國內高階資安處理與管理人才，並提升各教育單位網站負責人員的資安處理應變能力，藉此提升教育單位資安防護水平，以有效降低外來之攻擊所造成之損失。透過建置『ISAC 外部分享平台』，可藉此與國家資通安全監控中心(G-SOC)進行資安資訊分享之整合，以建立具有共通規格之線上資安自動通報作業平台，完成國家交付之重大資安建置與研發計劃。

5. 致謝

本研究感謝教育部電算中心對於 ISAC 教育學術資安資訊分享與分析中心研發專案之補助。

6. 參考文獻

[1] 梁文典。2009。從資訊分享看 DDoS。行政院國家資通安全會報。

[2] 行政院科技顧問組。2009。國家資通訊安全發展方案(98 年至 101 年)。行政院國家資通安全會報。

[3] 行政院科技顧問組。2009。國家資通訊發展方案(2007-2011 年)修訂核定版。行政院國家資通安全會報。

[4] 傅雅萍、樊國楨、楊中皇。2008。CORAS 用於 ISAC 之研究。國立高雄師範大學資訊教育研究所碩士論文。

[5] 樊國楨、林樹國、歐崇明。2006。資安監控中心之終極目標:資訊分享與分析中心初探。資通安全專論。

[6] 劉江龍、韓康年、曾子軒、楊棋堡。2009。應用於資訊分享決策支援之資安事件管理技術。資訊管理實務研討會。

[7] Research and Education Networking Information Sharing and Analysis Center。http://www.ren-isac.net。

[8] National Information Security Center。http://www.nisc.go.jp/index.html。

[9] 教育部全球資訊網。2010/01/31 即時新聞。http://140.111.34.54/PDA/news.aspx?news_sn=3098&pages=0。

[10] D. Constant, S. Kiesler, and L. Sproull, “What’s Mine Is Ours, or Is It? A Study of Attitudes about Information Sharing,” Information Systems Research, Vol. 5, No. 4, pp. 400-421, 1994.

[11] D. Heimbigner, and D. McLeod, “A federated architecture for information management,” ACM Transactions on Information Systems, Vol. 3, pp.253-278, 1985.

[12] S. S. Tseng, L. Su, and E. Chao, “TANet: Taiwan Academic Network,” INET96.

[13] A brief Introduction to Taiwan Academic Network。http://english.moe.gov.tw/content.asp?cuItem=11616&mp=2。

[14] Information Sharing and Analyzing Center 。https://www.it-isac.org。

[15] JBoss Community。http://www.jboss.org。