行政院及所屬各機關出國報告
(出國類別：考察)

「資訊分享及分析中心暨重要基礎建設保護」考察報告

出國人員：林培謙 經濟部資訊中心主任
鄭春光 經濟部國營事業委員會科長
蔡文隆 台灣電力公司經理
連香樹 台灣中油股份有限公司組長
曾沛聰 台灣自來水公司組長
出國地區：美國
出國期間：97 年 12 月 3 日至 97 年 12 月 10 日
執行機關：經濟部國營事業委員會

「資訊分享及分析中心暨重要基礎建設保護」考察報告

目次

1 序言

行政院於 93 年 2 月研擬自 94 年至 97 年的第二期「建立我國通資訊基礎建設安全機制計畫」，計畫目標中涵蓋「建置政府及重要基礎建設之資訊分享及分析中心，提升國家競爭力」一項，要求於 97 年完成 1~3 個領域的資訊分享與分析中心（ISAC），並選定經濟、外交、國防、交通四個領域爲首要建置目標。

由於經濟部爲前述目標的協辦單位之一，因此配合政府政策於 97 年進行「經濟部國營事業委員會資安資訊分享與分析中心」之建置，爲轄下維運重要基礎建設的國營事業（台電、台灣中油、台灣自來水三家公司）提供安全保護與資安資訊分享的機制。由於資安資訊分享與分析中心（簡稱 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、威脅燈號設計、工業控制系統安全、威脅與脆弱性分析等諸多技術議題，且國內過去並無相關建置、維運之經驗，因此安排本次參訪行程，針對國外相關單位目前發展的技術與維運制度進行深入瞭解，作爲後續維運、功能強化之依據。

本次共參訪美國三個單位，包括位於西雅圖的波音公司（Boeing）、微軟公司（Microsoft）以及位於華盛頓的北美電力可靠度公司（North American Electricity Reliability Corporation，NERC）。

2 波音公司之基礎建設保護與資訊分享

波音公司爲全球知名的飛機製造公司，本次我們參訪的地點爲西雅圖，由波音公司負責企業 IT 安全研發部門的黃明昱資深研究員負責接待，參訪主題包括重要基礎建設保護（Critical Infrastructure Protection，CIP）之研發和安全性資訊分享機制。

2.1 重要基礎建設保護之研發

黃研究員認爲在重要基礎建設保護的研發上，最具有價值的方向包括：

- 建立共通性的基礎建設維運藍圖。
- 發展下一代的 Internet 技術，並於其中各元件在設計時就加入資安之考量。
- 發展具存活能力、具自我診斷能力、具自我治療能力的網際空間基礎建設相關系統。

他並更進一步的說明各項相關研發主題的詳細內容，可供我們在未來規劃、執行重要基礎建設保護相關計畫的參考。以下各節分別說明之。

2.1.1 偵測與感知器系統

在偵測與感知器系統方面之研發重點將包括：

- 研訂新一代事故偵測與報告的框架，涵蓋所有相關資產與參與者的狀況、條件、需求、顧慮、行動、行爲的認知。

- 發展網路上監督安全和偵測事故的軟體，可以針對網路入侵者進行偵測、降低能力、隔離與剖析。
- 發展具存活能力、具自我治療能力、具自我診斷能力的基礎建設，這包括可整合資料的感知器和系統層面的檢查，以及下一代可分享責任、可重新分配工作負荷的資料獲取與監督管制系統（Supervisory Control And Data Acquisition，SCADA）。
- 對於感知器必須提升其能力，包括更高的速度、更低的誤報率、更低的耗能、更高的環境容忍度、GPS 同步的廣域感知量測系統。此外，先進的 SCADA 加密模組和符合美國氣體協會 AGA-12 的標準也是值得建議的。

2.1.2 保護與防禦

在保護重要基礎建設相關資產的系統、工具、方法與權限管理方面，研發重點將包括：

- 如何即時的導入保護和控制機制的狀態。
- 如何達成主動式保護的威脅減緩機制或對策。
- 研發爲了達成存活或防護的目的而設計的防護罩系統（Shielding System）或犧牲系統（Sacrificial System），以及具備破裂自動修補的極度強韌材料。

2.1.3 安全性存取入口

在防範非法存取重要地方和系統方面，研發重點將包括：

- 系統可清楚知道誰在哪裡、他們的角色、權限、以及他們攜帶的東西，並具備自動化巡邏和消除誤報的機制。
- 系統可對所有網際空間角色的習慣、活動、身份的監控，並能消除非法角色的能力。
- 系統在辨識與控制方面具備自動化學習、驗證、演化的能力，並可依據環境進行角色控制的客製化。

2.1.4 內賊防範

在防範具有權限的合法人員進行破壞活動方面，研發重點將包括：

- 如何在可信賴的環境偵測非法或異常行爲。
- 發展動態的、以角色爲基礎（Role-Based）的存取控制機制和異常行爲偵測系統。
- 如何在監控時依據角色所進行的控制與逮捕。

2.1.5 分析與決策支援

針對複雜且困難的問題進行分析與決策支援方面，研發重點將包括：

- 如何即時將多方面的偵測資料蒐集以匯入決策支援系統。
- 發展協助應變人員和指揮官處理事故的工具。
- 如何對於發展中的材料和創新的設計進行先進的塑模（Modeling），且不受持續進步的威脅所影響。

2.1.6 應變與回復

在事故之應變處理方面，研發重點將包括：

- 發展應變人員所需之工具、方法和計畫，包括受害者搜尋、3D 受災狀況評估、安全進入與逃生等。
- 發展災後重建與攻擊減緩的機制，建立下一代的複置（Redundancy）和安全性故障復原。
- 於回復與重建工程發展整合跳躍式替換技術（Replacement Leap Technology）。
- 發展可控制的崩坍以控制損失，加速破壞與重建的速度。

2.1.7 新的威脅與弱點

如何發展工具與方法在威脅與弱點出現的第一時間即發現，研發重點將包括：

- 從攻擊意圖、監控和大量原始資料中搜尋發現威脅模式的方法。
- 將感知、發展針對新威脅的防禦能力內建於日常維運之中。

2.1.8 進階的基礎建設架構和系統設計

如何建立可避免過去系統或技術常見安全缺陷的新系統，研發重點將包括：

- 動態狀況認知與即時解譯的研究。
- 發展新一代高容量通訊系統。
- 發展安全性計算基礎、無法入侵的計算核心。
- 發展光學、有機、量子等新一代的計算系統。
- 發展可自行設計自我替代機制的系統。
- 發展聰明材料、可內嵌感知器的材料、具適應性的監控架構。

2.2 安全性資訊分享機制

黃研究員以飛機製造爲例，從飛機內部的各系統與飛行員之資訊分享，延伸到飛機起降時與控制塔台之間的資訊分享，都須要安全的設計才能保障飛航安全。在使用者、角色、存取分享之資源三者間，存在複雜的冪次關係如下圖。

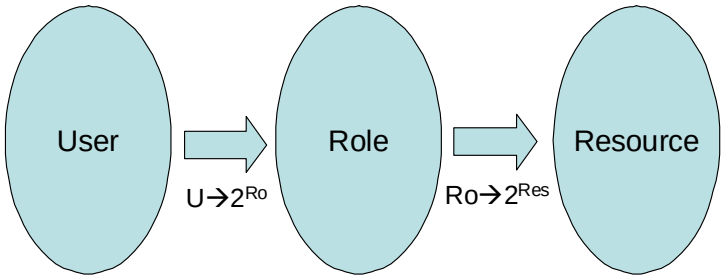

圖 1 使用者、角色與分享資源之關係

他建議資訊分享的生命週期如下圖，應從政策、法規的制訂到業務程序的成形，之後賦予使用者取得某角色的權限，並進一步依據該角色所有的權限來存取可分享的資訊。在此過程中，當然須要有稽核的機制和異常存取偵測、分析的機制予以監督。此外，透過定期或不定期的風險分析與資產保護方案的檢討，可以回頭修正資訊分享的政策和法規，進一步強化資訊分享的安全保護。這其中的關鍵即爲以角色爲基礎的存取權限管制，值得作爲我們在 ISAC 分享機制設計時之參考與借鏡。

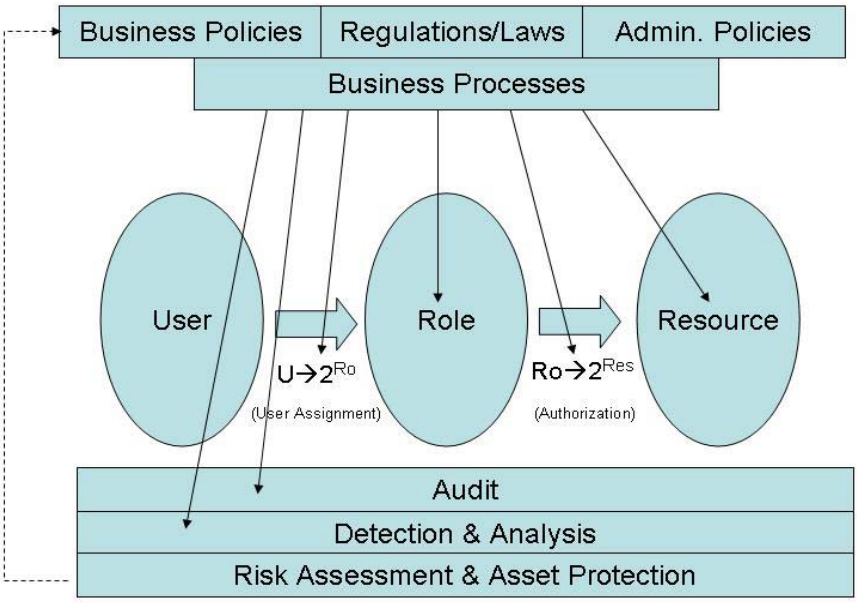

圖 2 資訊分享的生命週期

3 微軟公司重要基礎建設保護與存活演練

本次參訪對象主要包括微軟的主要安全策略師（Principal Security Strategist）Paul Nicolas 和其部門成員 Angela McKay，Paul Nicolas 同時也是微軟重要基礎建設計畫（Critical Infrastructure Protection Project）的主持人。微軟目前共有 6 位

主要安全策略師。

3.1 重要基礎建設保護

微軟的重要基礎建設計畫，其目標是傾聽外部單位有關於重要基礎建設保護的聲音且尋找潛在的需求，並於內部發展外部單位所需要的解決方案，因此對於重要基礎建設的保護有深刻的瞭解。

3.1.1 重要基礎建設保護的內涵

就重要基礎建設的組成架構來看，微軟將其分爲軟硬體與服務、重要網際空間系統、關鍵性系統與服務功能等，如下面圖 3。

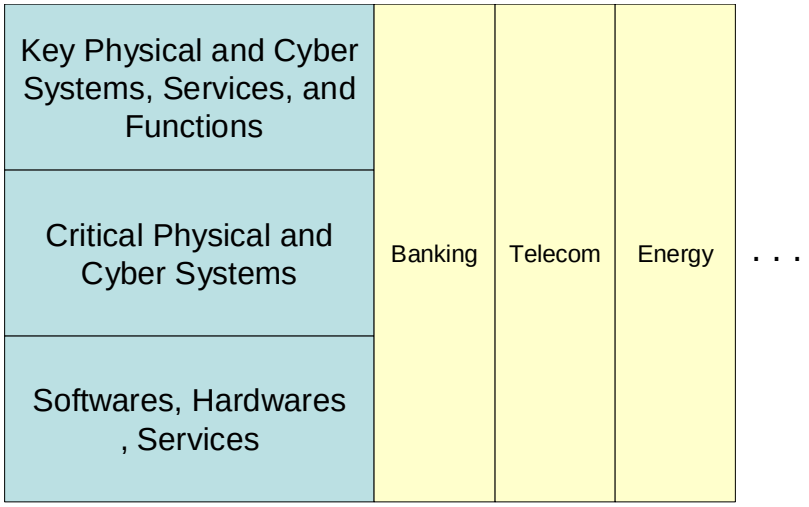

圖 3 重要基礎建設組成架構

微軟認爲對於決策者來說，於規劃重要基礎建設的保護時，必須要考慮的因素如下面圖 4，包括：

- 氣候變遷
- 移民與都市化
- 基礎建設的狀況
- 分化的技巧（如社交工程）
- 網際空間的存活
- 無所不在的狀況警示
- 模糊的國界
- 能力強化的個人與團體
- 法規環境

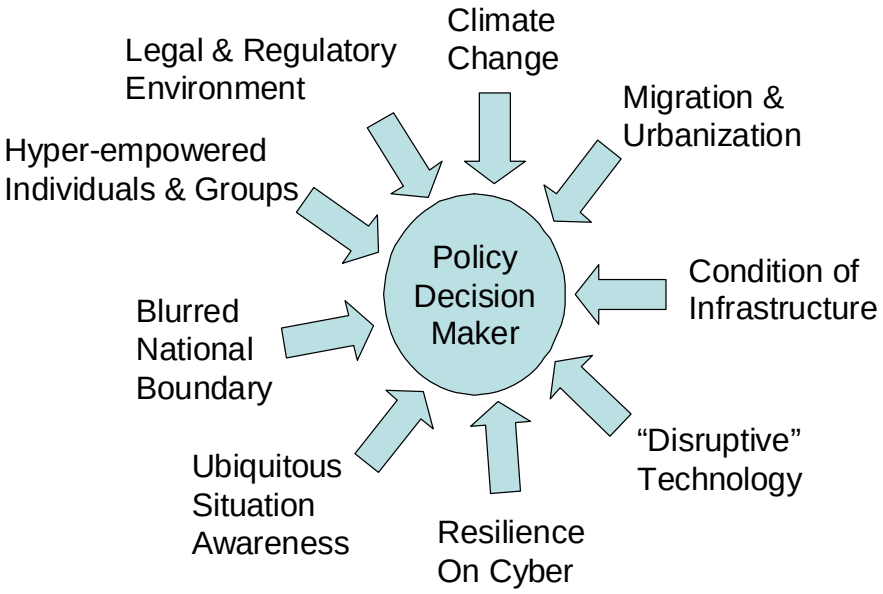

圖 4 重要基礎建設保護的考慮因素

從微軟的觀點，重要基礎建設的保護必須涵蓋可信賴的規劃與政策、可存活的維運、對於創意的投資等三方面，並透過資訊分享與可信的協同運作來強化這三方面的協同運作，最終達到重要基礎建設保護的目的。

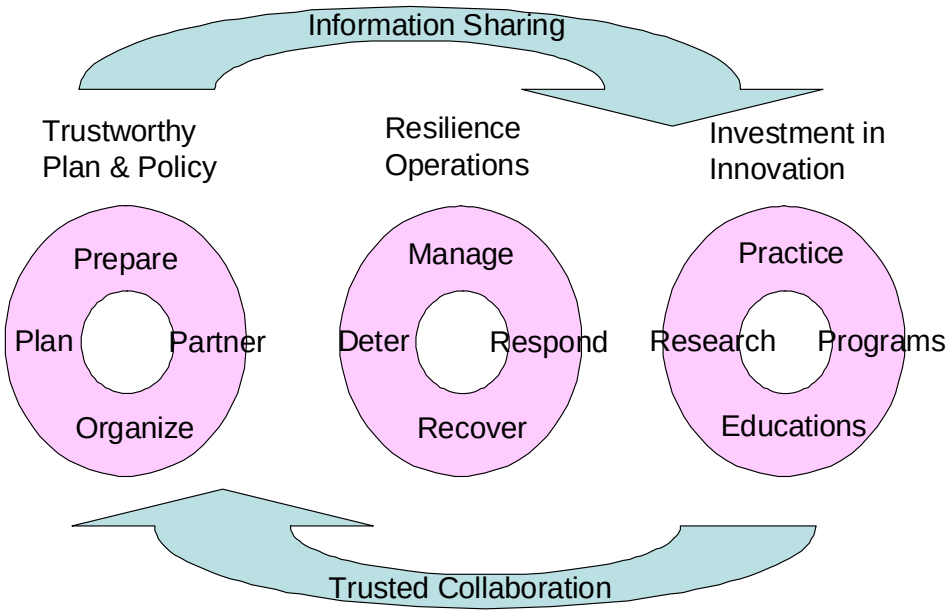

圖 5 重要基礎建設保護的內涵

在前述內涵中，Paul Nicolas 還特別強調與利益相關者成爲合作伙伴的重點，包括與政府單位、內部客戶、外部客戶、業界、有影響力的人士等，在各方

有利益、能力、成本等考量因素下，如何從利益與專業能力去整合出合作的能量實爲關鍵。此經驗很值得國內從事重要基礎建設保護與 ISAC 建置、維運之參考。

3.1.2 美國 ISAC 現況

由於微軟也積極參與美國 ISAC 相關組織與活動，因此對於美國各 ISAC 的狀況也有下列深入的瞭解：

- 依據微軟的瞭解，美國供水、能源、電力等 ISAC 的維運模式都不盡相同，以北美電力可靠度公司所維運的電力 ISAC 爲例，其會員數量不多（僅含發電業者，不含代銷、代配送業者），且對電力 ISAC 具有極強的信賴感。在 2003 年美東大停電時，電力 ISAC 即發揮相當有用的功能，有效扮演政府與業界的溝通橋樑，即時分享災情、回復狀態等有用的資訊給相關人員。另外除了政府法規的要求之外，發電業者自己也有相關的安全規範需遵守。
- 能源 ISAC 雖然沒有正式的 ISAC 名稱，但是實質上具有 ISAC 的功能，且與政府單位具有密切合作的關係。
- 由於微軟目前也主導美國 IT-ISAC 的董事會（Paul Nicolas 的主管擔任董事會召集人），因此可以從 IT-ISAC 這個 34 家重量級軟、硬體供應商所組成的資訊分享組織，取得許多有關 IT 領域的資訊分析與分享結果。IT-ISAC 的會員就比較獨立，不像電力 ISAC 的會員本質上是同業兼競爭者，但在系統重大漏洞發生時確實能協同進行即時的改善，化解可能發生的災難。以 Dan Kaminsly 於今年所發現的 DNS 重大漏洞爲例，IT-ISAC 透過一般通訊管道之外的 Out-of-band Security Bulletin，即時推播（Push）正確的資訊給政府單位和相關業者，針對該漏洞於極短期間內完成必要的修補程式並公告，將可能的危害減到最低。
- 各產業之相關業者，其各自的風險管理多半做得不錯。政府單位各自的風險管理也做得很好。但從整個國家的觀點來看關鍵基礎建設的風險管理，風險模型是不同且更複雜的，必須加上許多整合與協同運作的功夫才能控制整體風險。

3.2 重要基礎建設存活演練

重要基礎建設在面臨災難時，是否能存活進而發揮穩定社會與國家安全的力量，除了平時就規劃災難應變與業務、系統的回復等作業之外，演練是進行有效性驗證最基本的手段。依據微軟的建議，下面分別說明各類型演練的焦點與演練的步驟，這些資訊對於國內 ISAC 與重要基礎建設後續進行相關演練甚有參考價值。

3.2.1 演練焦點

重要基礎建設存活演練依據其規模與範圍，可概分爲國家級或跨國性、地區性或跨領域、領域內等三種。

對於國家級或是國際級的重要基礎建設存活演練，其價值包括：

- 提升安全意識與認知存活演練的重要性。
- 檢視可能發生的災難對於政府任務、業務服務、人民生命財產、國家經濟的衝擊。
- 發現資訊分享、決策等相關的協調合作可能出現的問題。
- 測試應變計畫或作業程序的有效性。
- 評估災難可能的預防或緩解措施。

此類國家級或是國際級的演練所能得到的經驗，主要集中於發現缺點並針對下列各項進行改善：

- 跨過邊界和領域進行狀況的認知與敏感資訊的分享，以便在不影響國家利益的前提之下因應多個事故。
- 應變計畫、風險評估、事故管理、公開資訊、共通的通訊架構等相關程序與作業步驟。
- 須要強化應變、角色、政策、程序的必要教育訓練。
- 國家、地方政府、各類組織進行應變與回復的協調工作。
- 有關網際空間安全與災難應變的工具與技術。

對於地區性或跨領域的重要基礎建設存活演練，其價值包括：

- 提升參與演練者對於地區性基礎建設之相依性與弱點、某些情境的後果、應變準備的缺失等之認知程度。
- 針對應變與回復作業，鑑別跨領域或跨管轄範圍之協調、溝通問題。
- 鑑別出可以整合進地方政府和組織之作業與業務回復計畫。
- 對於利益相關者，建立聯繫網路與信賴感，並擴展他們的相關知識。
- 促進地區性聯盟或社群組織之建立與合作，共同發展地區性的應變計畫與程序、經濟有效的災難預防與緩解措施。

此類地區性或跨領域的演練所能得到的經驗，主要集中於發現下列缺點：

- 缺乏對地區相依性的認知，包括電子化的相互連結和網際空間攻擊的相關衝擊。
- 應變與回復過程中，公部門與私人企業、組織之間欠缺的協調與溝通管道。
- 對於角色、權責、任務之誤解與含糊不清。
- 欠缺對於稀有人力與設備之管理計畫。
- 欠缺大眾資訊傳播能力以緩和民眾的恐慌並提供必要、即時的資

訊。

- 針對地方政府與區域組織之應變、回復、互助計畫，欠缺審查、檢討的機制。
- 災難準備計畫所需之資訊，欠缺一個資訊彙整的資料庫及存取的通訊協定。
- 欠缺一個安全、可存活、互通的通訊管道和資訊系統以發佈威脅、應變、回復狀態相關資訊。

至於領域內的重要基礎建設存活演練，其價值主要在於讓政府與業界領導廠商瞭解可能造成主要服務或產品中斷供應的可能事故。這類演練讓廠商從過去僅思考內部可能的事故，進而思考外部與供應鏈可能的事故及其對生產、服務之衝擊。此類演練也可提升與供應商、消費者、公共設施（如水、電）、地方救災單位、社區學術單位等利益相關者之合作。領域內的重要基礎建設存活演練通常著重於發展最佳的營運持續計畫及與基礎建設相依性有關的要素。

3.2.2 演練步驟

對於重要基礎建設存活演練，微軟建議採取下面 7 個步驟：

- 針對重要組織與利益相關單位的領導者和重要維運人員，進行鑑別並確保其於災難發生時可投入支援活動。
- 於演練之前舉行適合參與者知識與能力的教育訓練活動，聚焦於網際空間、重要基礎建設的保護與存活等，並提供演練相關之必要背景知識與資訊。
- 協助主要的利益相關單位與人員，進行演練的設計與執行。
- 產出演練報告，指出與演練目標之差距和必要的改善方案。協調參與者進行演練檢討會議與相關活動。
- 依據演練報告產出因應策略草案，並提出應變與回復計畫之改善作法。
- 舉辦演練後之策略研討會，對行動方案進行微調，並決定其執行之優先順序。
- 與利益相關單位與人員共組工作團隊以定義計畫需求，取得財務支援和技術支援以進行實作，並建立一個可持續監督的治理架構。

4 電力資訊分享與分析中心

美國電力資訊分享與分析中心（簡稱 ES-ISAC）於 1998 年建立，是由美國政府授權北美電力可靠度公司（North American Electricity Reliability Corporation，NERC）負責維運。NERC 負責美國、加拿大、墨西哥共計 1847 個發電、輸電相關單位的協調、管理，該公司總部位於紐澤西，但於華盛頓特區亦有辦公室。

本次參訪係於華盛頓特區之辦公室進行，由 NERC 的資安長 Michael

Assante 負責接待。Michael Assante 過去曾擔任美國電力公司（American Electric Power，AEP）的副總裁兼資安長，也曾擔任愛達荷國家實驗室的基礎建設保護策略師。他於今年 9 月就任現職，除負責 NERC 重要民生基礎建設保護之相關業務之外，他也是電力業界、美國政府、NERC 電力推動委員會（Electricity Sector Steering Committee）的單一聯繫窗口。Michael Assante 在 2007 年也曾參與「連結石油與天然氣產業以改善網際空間安全計畫（Linking the Oil and Gas Industry to Improve Cyber Security Project，LOGIIC）」，因此對於工業控制系統的安全防護有深刻的瞭解。

4.1 CIP 核心方案

NERC 在電力相關重要基礎建設保護方面，已建置核心方案如下圖，以確保北美整體電力系統的可靠度。

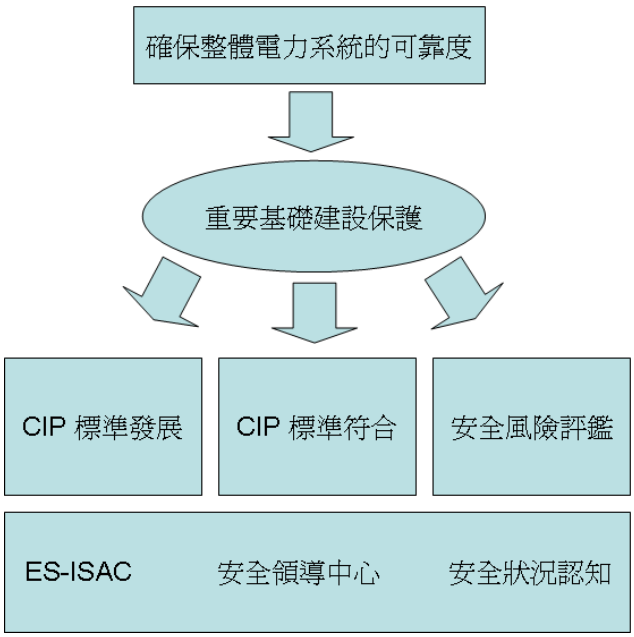

圖 6 電力重要基礎建設保護之核心方案

在事故防範準備上，NERC 的行動方案包括 CIP 標準發展、CIP 標準符合與安全風險評鑑三方面。

在 CIP 標準發展方面，NERC 目前共發展有 9 項標準並已經發佈實施：

- CIP-001-1 顛覆報告（Sabotage Reporting）：對於造成電力系統擾動或異常之限向活動，若疑為或確認是顛覆應該向適當的系統、政府單位或監督團體報告。
- CIP-002-1 重要網際空間資產之鑑別（Critical Cyber Asset Identification）：支援電力系統可靠維運的重要資產，其相關之網際空間資產必須鑑別並撰寫於文件。
- CIP-003-1 安全管理控制項（Security Management Controls）：負責

的個體必須維持保護重要網際空間資產的最低安全管理控制項。

- CIP-004-1 人員與訓練（Personnel & Training）：對於被授權進出網際空間或實體空間進行重要網際空間資產存取的人員，必須有適當的風險評估、訓練和安全認知。
- CIP-005-1 電子安全邊界（Electronic Security Perimeter）：涵蓋重要網際空間資產的電子邊界及其上所有存取入口都必須有安全防護措施。
- CIP-006-1 重要網際空間資產的實體安全（Physical Security of Critical Cyber Assets）：確保具備保護重要網際空間資產的實體安全方案。
- CIP-007-1 系統安全管理（Systems Security Management）：負責的個體應定義方法、程序、步驟來保護重要網際空間資產之相關系統。
- CIP-008-1 事故報告與應變規劃（Incident Reporting and Response Planning）：確保與重要網際空間資產相關的安全事故被鑑別、分類、處置及報告。
- CIP-009-1 重要網際空間資產的回復計畫（Recovery Plans for Critical Cyber Assets）：確保重要網際空間資產具有適當的回復計畫，且這些計畫依循業務永續與災難回復的技術與實務作法。

NERC 除了針對這些標準進行維護與更新之外，也將提出新的標準來因應可能的安全顧慮。

在 CIP 標準之符合性查核方面，NERC 協同所屬區域性可靠度組織（Regional Reliability Organization）進行稽核、監督與事故調查。這些組織包括：

- 佛羅里達可靠度協調委員會（Florida Reliability Coordination Council，FRCC）
- 中西部可靠度組織（Midwest Reliability Organization，MRO）
- 東北電力協調委員會（Northeast Power Coordinating Counci，NPCC）
- 可靠度第一公司（ReliabilityFirst Corporation，RFC）
- SERC 可靠度公司（SERC Reliability Corporation）
- 西南電力池公司（SouthWest Power Pool Inc.，SPP）
- 德州地區個體（Texas Regional Entity）
- 西部電力協調委員會（Western Electricity Coordinating Counci，WECC）

至於在安全風險評鑑方面，NERC 除了必須評估對整體電力系統的威脅之外，也必須鑑別安全顧慮並進行整備評估（Preparedness Evaluation）。

在事故應變處理上，NERC 的行動方案包括建立與維運 ES-ISAC、建立資安領導中心、安全狀況認知等三方面。其中 ES-ISAC 的任務是事故通報與預警，並協調事故的應變處理；資安領導中心除了 NERC 已於 2008 年 9 月建立並任命安全官一職，也將積極與各種安全安全領導核心組織之活動與運作；安全狀況認知

則係監督可能衝擊電網的事件，並提供可幫助協調和提升可靠度的工具。

4.2 ES-ISAC 的功能與服務

ES-ISAC 的主要功能是擔任電力供應單位、政府和其他重要基礎建設之間的溝通樞紐，並即時發佈威脅徵兆、分析、警訊、解譯之資訊以協助電力相關業者採取防範因應措施。ES-ISAC 係由 NERC 負責維運，在 NERC 內部由電力領域推動群組（Electricity Sector Steering Group，ESSG）所管理，在外部則接受聯邦能源法規委員會（Federal Energy Regulatory Commission，FERC）的監管。

ES-ISAC 對電力業者發佈的正式警訊通知（Formal Notifications），涵蓋網際空間、實體與各類災害之安全問題，依嚴重程度遞增包括下面三類：

- 通知（Advisories）
- 建議（Recommendations）
- 請求基本行動（Request for Essential Actions）

過去 ES-ISAC 曾經發佈過的通知和建議包括 Boreas 和 ABB、RealWin SCADA、GE Fanuc 之弱點建議等。

ES-ISAC 對於警訊之決策，主要是以風險評估爲基礎，利用下圖來決定是否發佈警訊：

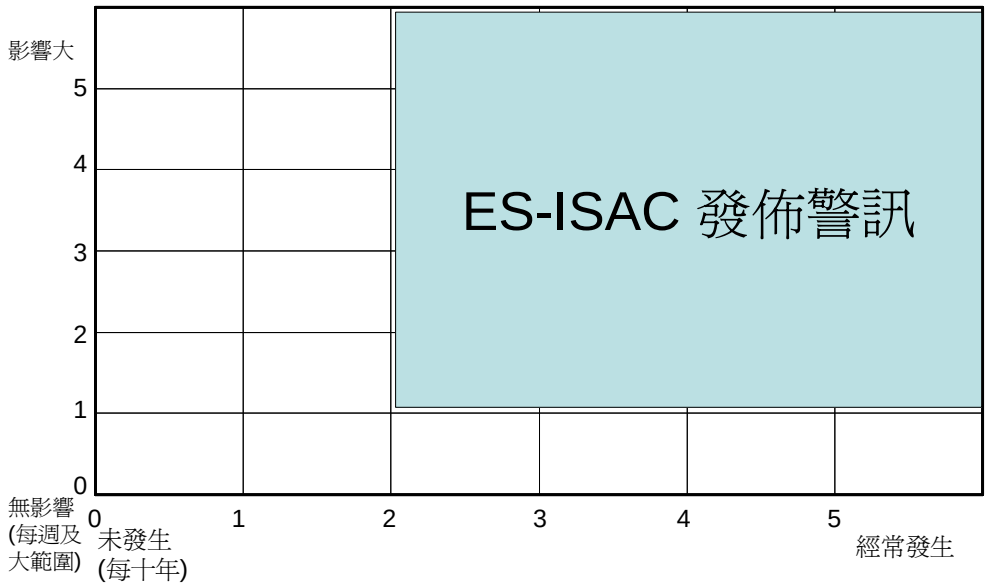

圖 7 ES-ISAC 發佈警訊之研判準則

就 IT 技術與系統之弱點所發佈的警訊，ES-ISAC 依技術領域分爲下表幾種，包括現行已發佈及未來考慮納入發佈的領域：

表 1 弱點警訊相關技術領域

技術領域	是否發佈弱點警訊
SCADA EMS	是
Field Control & Protection	是
Plant Control System	是
Market Systems	考慮中
Networking & Telecommunications	考慮中
Business Systems	否
Mobile Technology	否

在 2008 年，截至目前爲止，ES-ISAC 所發佈的關鍵基礎建設警訊包括：

- ABB PCU 400（瑞典），建議
- Citect（雪梨），通知
- RealWin（都柏林），通知
- Iconics（美國麻薩諸塞州），通知
- Boreas（美國華盛頓特區），通知
- GE Fanuc（美國維吉尼亞洲），通知
- Wonderware（美國加州），通知
- OSISoft（美國加州），通知
- BMS（全球），通知
- Microsoft（美國西雅圖），建議

在維運人力方面，ES-ISAC 現有 4 名全職員工，但另外約有 30 名的義工專家參與維運，這些義工都是電力業界熱心且具備專業知識與經驗的人員，自願由 ES-ISAC 安排輪值時段，並於事故或警訊徵兆發生時協助事故之分析與應變處理。

在警訊分析與發佈程序方面，ES-ISAC 依循下圖之作業流程：

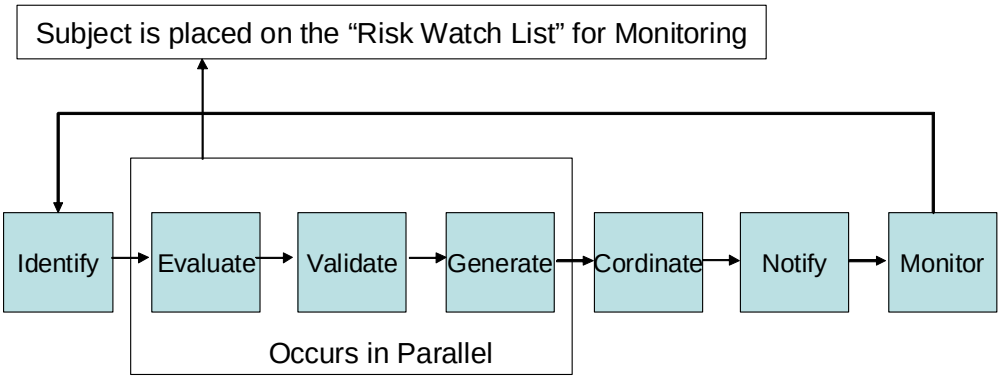

圖 8 警訊分析與發佈程序

目前的警訊分析與通報程序均爲人工作業，並無工作流程（Workflow）系統協助

事故之分析、追蹤與服務水準之管制。將來 ES-ISAC 於經費較充裕時，將導入工作流程系統及 Vedio Conference、Web-based Conference 等系統與機制。

5 結語

本次參訪，接觸了重要基礎建設保護與 ISAC 最爲先進的三家美國企業，對於重要基礎建設保護相關研究發展、作業標準、作業實務、ISAC 之維運實務等都有深刻的體悟，並取得相關文件資料，對於未來國內進行相關建置與維運計畫非常有幫助。

此外，此行也認識了多位在此領域具有關鍵地位與影響力的研究及維運人員，透過他們的人脈可進一步與其他重要單位接洽、交流，包括愛達荷國家實驗室、麻省理工學院林肯實驗室、SRI 國際公司等，對於瞭解技術發展趨勢和國際接軌將有極爲正面的幫助。