出國報告（出國類別：國際會議）

出席「Meridian 2013 年會」報告

服務機關：行政院 資通安全辦公室
姓名職稱：吳　副 主　任　啟　文
派赴國家：阿根廷(布宜諾斯艾利斯)
出國期間：102 年 11 月 2 日 至 9 日
報告日期：103　年　1　月　23 日

摘要

「Meridian 2013 年會」於 102 年 11 月 4 日至 6 日在阿根廷布宜諾斯艾利斯舉行，本次年會由阿根廷內閣長官辦公室(Chief Cabinet Office)規劃主辦，參加對象包括 Meridian 各會員國主責關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之政府高階主管及專業人員，本次年會亦邀請關鍵資訊基礎設施防護相關之民間專業代表(如：微軟、賽門鐵克等)與會。

Meridian 組織係針對各國關鍵資訊基礎設施防護政策制訂者所設置之經驗分享、交流、溝通平台。本次年會行政院國家資通安全會報技術服務中心劉主任培文受邀於 11 月 5 日下午 4 時至 5 時，針對「政府資訊分享與分析中心：公私夥伴關係之資訊分享實務」(G-ISAC: The Information Sharing of Public-Private Partnership Practice)進行專題報告，分享我國政府 CIIP 策略規劃及實務經驗。

我國為 Meridian 組織指導委員會成員之一，除透過參與「Meridian 2013 年會」與各會員國在 CIIP 議題交換意見與交流合作外，亦將持續參與指導委員會相關活動，以維持我國在 Meridian 組織之影響力。

目次

圖目次

表目次

壹、目的

「Meridian 2013 年會」於 102 年 11 月 4 日至 6 日在阿根廷布宜諾斯艾利斯舉行，本次年會由阿根廷內閣長官辦公室(Chief Cabinet Office)規劃主辦，參加對象包括 Meridian 各會員國主責關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之政府高階主管及專業人員，本次年會亦邀請關鍵資訊基礎設施防護相關之民間專業代表(如：微軟、賽門鐵克等)與會。

Meridian 組織係針對各國關鍵資訊基礎設施防護政策制訂者所設置之經驗分享、交流、溝通平台。本次年會行政院國家資通安全會報技術服務中心劉主任培文受邀於 11 月 5 日下午 4 時至 5 時，針對「政府資訊分享與分析中心：公私夥伴關係之資訊分享實務」(G-ISAC: The Information Sharing of Public-Private Partnership Practice)進行專題報告，分享我國政府 CIIP 策略規劃及實務經驗。透過參與「Meridian 2013 年會」除與各會員國在 CIIP 議題交換意見與交流合作外，同時可瞭解各國 CIIP 最佳實務經驗，以提升我國在資通訊、能源、交通、金融、政府等領域之關鍵資訊基礎設施防護能力，更可提高我國國際能見度。

本次年會中有關美國目前草擬中之網際安全框架、日本網際安全國際合作計畫、歐盟針對網安事故通報流程立法與國際網安演習舉辦經驗、美國與加拿大推動國家網安覺知提升計畫等，均可作為我國推動關鍵資訊基礎設施防護業務之參考。

貳、過程

一、議程

「Meridian 2013 年會」由阿根廷內閣長官辦公室(Chief Cabinet Office)主辦，於 102 年 11 月 4 日至 6 日為期三天，假阿根廷布宜諾斯艾利斯 San Martin Palace 舉行，三天議程詳如表 1、表 2 及表 3。

表1 102 年 11 月 4 日議程

時間	議程	報告人	主持人
09:30 – 10:30	Registration		
10:30 – 11:00	Group photo		
11:00 – 11:10	Welcome and Opening Speech	Lic. Facundo Nejamkis, Secretary of Cabinet and Administrative Coordination, Chief Cabinet Office Lic. Mariano Greco, Undersecretary of Management Technologies, Chief Cabinet Office Mr. Pedro Janices, National Director, Chief Cabinet Office, Argentina	
11:10 – 11:30	The Meridian Process and its contribution to worldwide CIIP	Dr. Rainer Mantz, head of section IT-Security at the Federal Ministry of the Interior, Germany	
11:30 – 12:10	Current Cybersecurity and CIIP landscape and technological prospective	Ms. Cristin Flynn Goodwin, Senior Attorney, Microsoft Corporation Mr. Ilias Chantzos, Senior Director EMEA, Global CIP and Privacy Advisor, Government Affairs, Symantec Corporation	Mr. Robert Gordon
12:10 – 12:25	Round of questions/debate		
12:25 – 13:20	Lunch		
13:25 – 14:40	New CIIP scenarios	Ms. Iris Gonzalez, Director of Information Technology, Ministry of the Presidency (CSN), Panama Mr. Carlos Landero Cartes, Chief of Information, Ministry Internal	Mr. Pedro Janices

		Affairs, Chile	
		Mrs. Johanna Carolina Orjuela Parra, SCADA Coordinator, Ecopetrol/ Mr. Leonardo Huertas Calle, Coordinador colCERT, Ministry of Defense, Colombia	
		Ing. Santiago Vazquez, CERT-Py Director, Senatics, Paraguay	
		Mr. Jorge Colin, Technical Secretary, Mexcio	
14:40 – 14:55	Round of questions/debate		
14:55 – 15:55	International cooperation in CIIP	Ms. Jessica Smith, Senior Policy Advisor, Cabinet Office - UK	Mr. Peter Burnett
		Dr. Reiko Kondo, Counselor for International Strategy, NISC, Japan	
		Ms. Jordana Siegel, Director, International Affairs Program, Office of Cybersecurity and Communications, Department Of Homeland Security, USA	
15:55 – 16:10	Round of questions/debate		
16:10 – 16:30	Coffee break		
16:30 – 17:30	Government and Private Sector approaches to addressing CIIP Risks	Mr. Omar Sherin, CIIP Manager, Qatar CERT	Mr. Pedro Janices
		Ms. Mara Misto Macías, Senior Manager Information Security, Central Bank of Argentina	
		Eng. Manuel Pedroso de Barros, ANACOM - Portugal	
17:30 – 17:45	Round of questions/debate		
17:45 – 18.05	Conclusion day 1	Argentina	

表2　102 年 11 月 5 日議程

時間	議程	報告人	主持人
09:00 – 10:00	Registration/Coffee		
10:00 – 10:40	CIIP: A vision of international organization	Mr. Belisario Contreras, Program Manager Secretary of the Inter-American Committee against Terrorism CICTE – OAS	Mr. Jessica Smith
		Mr. Konstantinos Moulinos, security expert of the European Network and Information Security Agency - ENISA	
10:40 – 10:55	Round of questions/debate		
10:55 – 11:55	Country approaches	Mr. Fernando Sanchez Gomez, Director of the National Centre for the Protection of Critical Infrastructures.- Spain	Mr. Jorge Colin
		Ing. Santiago Paz, IT Area, AGESIC, Uruguay	
		Mr. Antonio Augusto Muniz De Carvalho, Director for Technology, ABIN/ Mr. João Pincovscy, Head of research in information, ABIN, Brazil	
11:55 – 12:10	Round of questions/debate		
12:10 – 13:10	Lunch		
13:10 – 14:10	CIIP: Lessons learnt and future challenges	Mr. Samuel Linares, Director at Industrial Cybersecurity Center, Spain	Mr. Ake Holmgren
		Mr. Ryan Kimmitt, Operations Integration Chief of the Industrial Control Systems CERT, Office of Cybersecurity and Communications, Department of Homeland Security, USA	

時間	議程	報告人	主持人
		Capitan Pablo Daniel Sorrentino, Head of Information Security of the Navy, Argentina	
14:10 – 14:25	Round of questions/debate		
14:25 – 15:25	Awareness Campaigns	Mr. Robert W. (Bob) Gordon , Special Advisor, Cyber Security , Public Safety Canada	Mr. Belisario Contreras
		Mr. Pedro Janices, National Director, National Office for Information Technologies, Chief cabinet Office	
		Mr. Marcos Gomez Hidalgo, Operations deputy Manager of National Institute of Communications Technologies (INTECO)	
15:25 – 15:40	Round of questions/debate		
15:40 – 16:00	Coffee break		
16:00 – 17:00	Public & Private Partnership, lessons learnt	Mr. Hans Oude Alink, senior policy advisor at the National Cyber Security Centre - NL	Mr. Mark Henauer
		Dr. Pei-Wen Liu, Director of Information & Communication Security Technology Center, Taiwan	
		Dr. Michael Pilgermann, Technical Advisor at the Federal Ministry of the Interior, Germany	
17:00 – 17:15	Round of questions/debate		
17:15 – 17:35	Conclusion day 2	Argentina	

表3 102 年 11 月 6 日議程

時間	議程	主持人
09:00 – 10:00	Meeting at Venue Place / Coffee	
10:00 – 12:30	Depart for site visit	Federal Administration Of Public Revenue (AFIP)
12:30 – 14:00	Lunch	
14:00 – 14:30	Conference Closing	Mr. Pedro Janices, National Director, Chief of the Cabinet Office, Argentina
	Handover to Meridian 2014	Dr. Reiko Kondo, Counselor for International Strategy, NISC, Japan
14:30 – 15:00	Coffee break	
15:00 – 17:00	Close meeting	By invite only

二、重點與發現

本次年會之主軸為「挑戰、機會及解決方案」(Challenges, Opportunites and Solutions)，除了首次邀請產業界代表從技術面分享資訊安全現況與關鍵資訊基礎設施所面臨挑戰外，也透過各國關鍵資訊基礎設施保護作法(Country Approaches)、國際組織(International Organization)、國際合作(International Cooperation)、認知推廣(Awareness Campaign)及公私夥伴關係(Public Private Partnership)等面向進行議題報告與討論。重點說明如後：

(一) 美國網際安全架構(Cybersecurity Framework)

為強化關鍵基礎設施之復原能力，美國歐巴馬總統於 102 年 2 月 12 日下達 13636 號”改善關鍵基礎設施網際安全”行政命令(Executive Order)。該行政命令要求發展一個志願性的網際安全框架，提供一個能夠區分優先順序、具彈性、可重複、重效能及具成本效益的方法，協助負責關鍵基礎設施服務的組織來管理網際安全風險。此框架強調依據現有的標準、指引及最佳實務，而不另行訂定新

的標準或指引。利用此框架與框架中的元件，企業組織可以使用共通的語言與機制，描述目前網際安全狀態、欲達成目標狀態、在風險管理內涵下找出改善的優先機會、評估朝向目標狀態的進展及促成內外利害關係人的溝通。此框架的設計並非要取代組織目前的業務與網際安全風險管理流程，而是與現有流程互補，讓組織可以找出改善的機會。而對尚未建立網際安全風險管理流程的組織，則可以參考此框架建立相關流程。網際安全框架以風險為基礎，包含框架核心(Framework Core)、框架剖繪(Framework Profile)及框架實作等級(Framework Implementation Tier)等三部分。

框架核心包含功能(Function)、分類(Category)、次分類(Subcategory)及提供參考資訊(Informative Reference)的表格(詳如圖 1)，以下分別說明表格內容。

- 功能：將網際安全活動概分為辨識(Identify)、保護(Protect)、偵測(Detect)、應變(Response)、復原(Recover)等五個高階部分。功能的組成與現今事故管理的方法論匹配，並幫助顯示網際安全活動的投資。

- 分類：分類是將一個功能中詳細的活動分群，例如辨識的分類可能包括資產管理(Asset Management)、業務環境(Business Environment)及資安治理(Government Governance)等，保護的分類可能包括存取控制(Access Control)、認知與訓練(Awareness and Training)及資料安全(Data Security)等。

- 次分類：次分類係依據提供參考資訊所描述的資安活動產出或結果，例如”組織內部的實體設備與系統被登記分類”等。

- 提供參考資訊：提供參考資訊係關鍵基礎設施領域所採用共通的標準、指引及實例，由這些資訊可說明各次分類完成活動的方法。要注意的是此方法論並未限定必須要參考何種標準，各組織也可以將自行施行的標準、指引及實例納入。

目前美國國家標準與技術研究院(National Institute of Standards and Technology, NIST)已於初版的網際安全框架文件(草案)[1]提出一個框架核心的範例(詳如該文件 Appendix A)，文件中特別強調該實例所列出的分類、次分類及提供參考資訊並非窮舉的結果，各組織可以自行修改或擴充。此外文件中亦針對框架核心中的功能、分類及次分類提供編碼參考以方便識別。

框架剖繪代表一個特定系統或組織實施的網際安全活動目前已經達成或期望達成結果。透過目前達成結果與目標剖繪比較，可進行差距分析，進而決定資安改善與投資的優先順序(詳如圖 2)。

圖1 框架核心結構

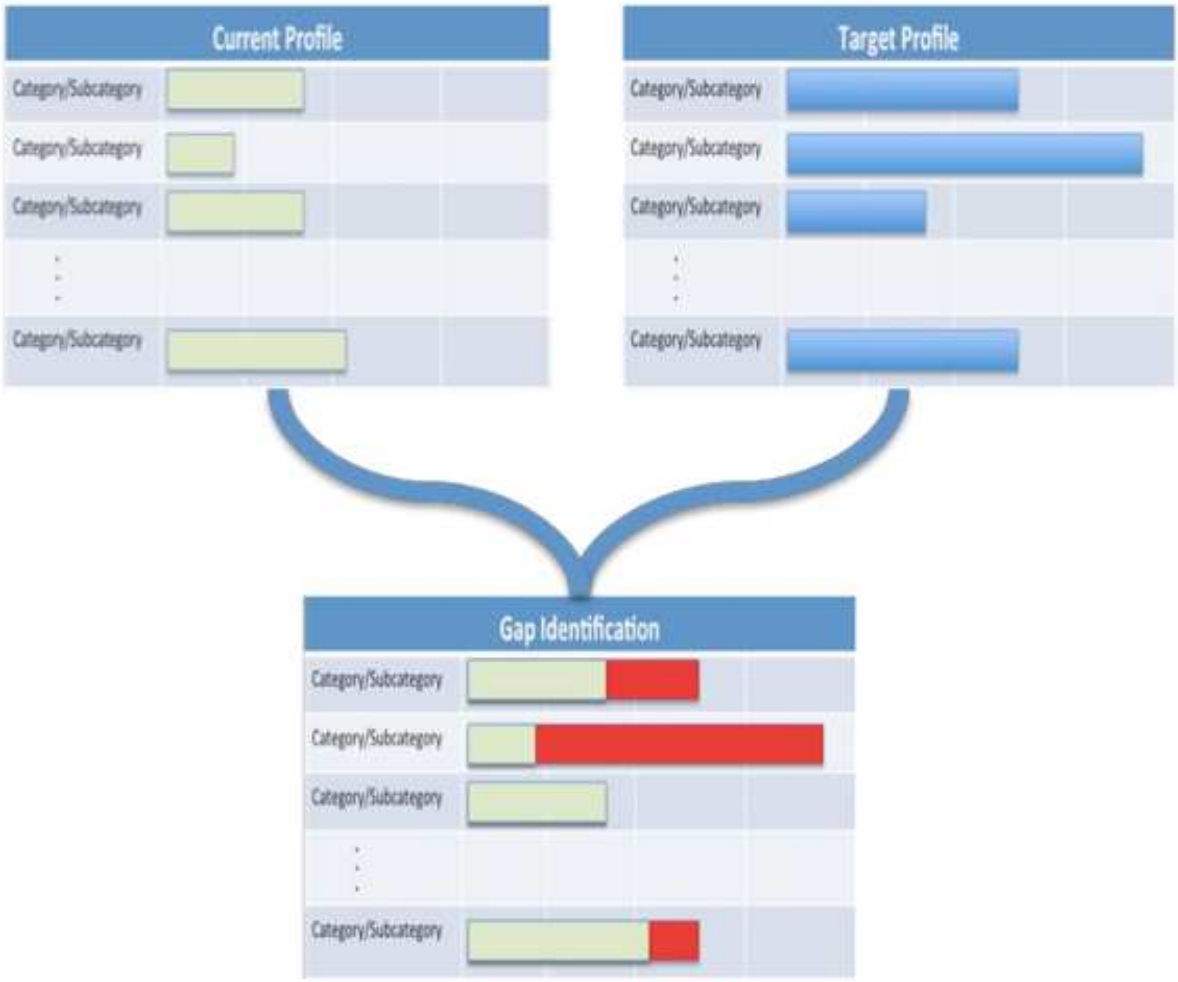

圖2 框架剖繪比較示意圖

框架實作等級描述一個企業組織如何管理它的網際安全風險。企業組織應該利用外部指導、資訊(例如來自聯邦政府部門或資訊分析分享中心的資訊等)或現有的成熟度模型，決定期望等級。確保所選擇的等級能夠符合組織目標、降低關鍵基礎設施風險，且實作是具體可行且具經濟效益的。框架實作等級由等級 1 至 4 分別為局部實作(Partial)、能提供風險資料實作(Risk-informed)、能提供風險資料且可重複實作(Risk-informed and Repeatable)及可適性的實作(Adaptive)。文件中針對 4 個等級在風險管理流程、整合計畫及外部參與等三個面向說明等級

應該達成的程度。

企業組織內部資訊安全的資訊與決策如何在資深管理、業務/流程及實作/作業三個階層間流動，詳如圖 3。資深管理階層首先與業務/流程階層溝通任務優先順序、可取得資源及風險忍受程度。業務/流程階層將這些資訊作為風險管理流程的輸入，並與實作/作業階層合作製作剖繪。實作/作業階層實作剖繪後，與業務/流程階層溝通實作資訊。實作/作業階層利用剖繪實作資訊進行衝擊評估，再將衝擊評估結果向資深管理階層報告，以利企業組織整體風險管理。

●第一步、識別(Identify)：企業組織辨識列出任務目標、相關系統與資產、法規需求與整體風險管理做法。

●第二步、製作目前剖繪(Create Current Profile)：由框架核心中列出的分類開始，企業組織發展出目前的剖繪。此剖繪反映出企業組織對目前依據提供參考資訊的標準、指引及實務進行實作網際安全活動產出的了解。

●第三步、進行風險評估(Conduct a Risk Assessment)：組織需針對作業環境進行分析以區分資安事件與衝擊的可能性。關鍵基礎設施的機構必須將意外的風險與外在的威脅資料考慮進來，以便對資安事件的可能性有充分的了解。

●第四步、製作目標剖繪(Create Target Profile)：組織應針對框架中的元件(例如分類與次分類等)進行評估以建立目標剖繪。該剖繪描述組織期望的網際安全活動產出。

●第五步、缺口決定、分析及區分優先(Determine, Analyze, and Prioritize Gaps)：組織應該比較目前剖繪與目標剖繪決定其間的差距，以決定應投入的資源。組織應建立一個區分優先序的行動計畫(Action Plan)，列出任務驅動力、成本效益分析及達成目標剖繪存在的風險。

●第六步：實施行動計畫(Implement Action Plan)：組織應依據行動計畫逐步實施，並根據目標剖繪監控計畫執行狀況。

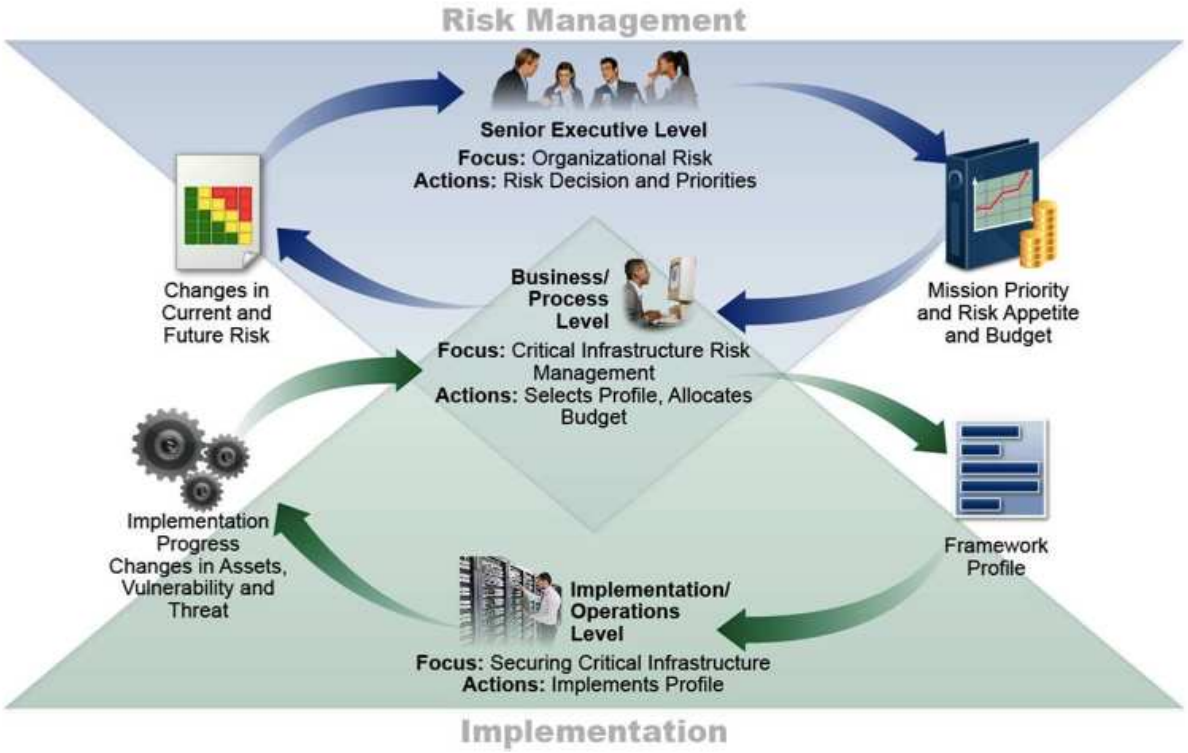

圖3 組織內部資安資訊與決策流示意圖

(二)日本網際安全合作國際策略(j-initiative for Cybersecurity)

日本於 102 年 10 月由內閣官房的資訊安全政策委員會依據 102 年 6 月制訂的日本復興戰略(Japan Revitalization Strategy)與網際安全策略(Cybersecurity Strategy)，制訂網際安全合作國際策略(International Strategy on Cybersecurity Cooperation,簡稱 j-initiative for Cybersecurity)。此國際合作策略在制訂時依循四項基本原則：確保資訊自由流通、應變逐漸嚴重之風險、強化以風險為基礎之做法及依據社會責任扮演夥伴關係，以及三大基本政策：逐步培養全球共識、強調日本對全球社群之貢獻及在全球擴展尖端技術。依據上述的基本原則與政策，日本訂定國際合作的三大優先領域，包括網際事故動態應變實作

(Implementation of dynamic responses to cyber incidents)、建立動態應變基本法則(Building up fundamentals for dynamic responses)及網際安全國際規則制訂(International rulemaking for cybersecurity)。以下分別說明這三大優先領域的詳細內容。

1. 網際事故動態應變實作

(1) 強化多層次資訊分享機制

日本認為多層次包括電腦緊急應變團隊作業層級且採取實際行動的資訊交換，執法機關間為行使犯罪調查與預防的資訊交換，政府層級為進行政策合作相互瞭解的資訊交換，在外交層次避免政治衝突的資訊交換，以及研發機構間針對前瞻技術進行之合作交流等。

(2) 網際犯罪適切反應

日本透過八大工業國 G5 之羅馬-里昂組織，參與高科技犯罪小組及反犯罪技術調查會議(Counter-cybercrime Technology Investigation Symposium, CTINS)等國際組織，與各國執法機關合作。日本也參與推動網路犯罪公約(亦即一般俗稱之布達佩斯公約)，協助其他國家建立能量成為公約會員國。此外日本政府也支持其政府官員參與國際刑警組織(INTERPOL)，為打擊全球網路犯罪確保數位世界安全，並擔任 2014 年在新加坡成立的國際刑警全球創新總部(INTERPOL Global Complex for Innovation, IGCI)之執行官員(Executive Director)。

(3)建立網際空間之安全合作國際架構

日本擬透過參與東南亞國協區域論壇(ASEAN Regional Forum)、為強化美日安保協議(Japan-U.S. Security Arrangement)的美日軍方資訊技術論壇(Japan-U.S. IT Forum)及美日政府部會的網際對話(Japan-U.S. Cyber

Dialogue)等，建立一個全球性的國際合作架構。

2. 建立動態應變基本法則

(1)協助建立網際保健全球架構

針對資安事故應變合作的基礎需由各國先建立資安偵測、分析及應變機制。日本承諾將以自身建立電腦緊急應變團隊、殭屍電腦網路偵測及關鍵基礎設施防護的經驗，來協助其他國家建立能量。此外日本認為協助每個國家針對網路攻擊與網際安全倡議訂定量化的評估指標(indicator)，對建立全球性的網際保健架構相當重要，因此日本將持續參與 OECD 與其他國際組織制訂資安指標相關工作。

(2)推廣認知活動

日本將以自身在認知與人員能力建立的經驗協助其他國家，並持續參與國際性的認知推廣活動。

(3)透過國際合作強化研發

日本將透過 PRACTICE(Proactive Response Against Cyber-attacks Through International Collaboration Exchange)計畫，與各國建立合作網路，以發展資安預警與應變技術。

3. 網際安全國際規則制訂

(1)國際技術標準規劃

在國際技術標準推動方面，日本於 2013 年設立控制系統安全中心(Control System Security Center, CSSC)，由該中心建立控制系統安全評估與驗證技術。日本將建立控制系統安全與驗證體系，並將其建議為國際標準。日本也積極推動設備採購依循之共通準則認證協議(Common Criteria

Recognition Agreement)。同時日本亦於國際電信聯盟(International Communication Union, ITU)推動制訂網際安全資訊交換架構(Cybersecurity Information Exchange Framework, CYBEX)，並在 ISO 與 ITU 參與雲端運算安全標準之制訂。

(2)國際規則制訂

日本參與聯合國大會第一委員會下設立之政府專家組(Group of Government Expert, GGE)於 102 年 6 月發佈報告，該報告建議各國使用資通訊技術規範。日本也參與 OECD 所制訂之資訊系統與網路安全指引(Guidelines for the Security of Information Systems and Networks)。

在國際合作的區域性倡議方面，日本在亞太地區特別重視與東協的合作，包括東協-日本資訊安全政策會議、東協日本網際安全合作部長會議及日本-東協安全夥伴專案(Japan-ASEAN Security PartnERship, JASPER)。日本與美國及歐盟的合作包括美日安保協議、美日網際對話(Japan-U.S. Cyber Dialogue)、美日網際網路經濟政策合作對話(Japan-U.S. Policy Cooperation Dialogue on the Internet Economy)、英日雙邊網際對話(Japan-UK Cyber Dialogue)及日本歐盟網際網路安全論壇(Japan-EU Internet Security Forum)。

(三) 指導委員會(Steering Committee)會議重點

Meridian 指導委員會是在大會結束後，以閉門會議方式進行。列席指導委員會的國家以主辦過 Meridian 會議的國家為當然成員，並納入未來可能主辦的國家。本次參加指導委員會的國家包括歷年會議主辦國：英國、美國、日本、瑞典、德國、台灣、新加坡及阿根廷，匈牙利與卡達並未參加此次 Meridian 會議，因此未出席指導委員會。此外加拿大、墨西哥、挪威、西班牙及瑞士為未來主辦候選國，因此也受邀參加指導委員會。Meridian 另設有議程委員會(Programme Committee)，係由當年度的會議主辦國指派議程委員會主席，以規劃與準備當年

度會議，指導委員會的成員都有資格參與議程委員會。本次指導委員會會議討論議題包括未來主辦國、Meridian 新網站、聯絡窗口目錄(Directory Point of Contacts)、秘書處(Secretariat)角色與經費及 2014 年會議等項目。

1.未來主辦國

指導委員會決定會議舉辦地點按區域輪流辦理，若 2015 年在歐洲舉辦，2016 年則移到美洲或中東，2016 年再移到東南亞。未來若可能也希望能在非洲與印度半島舉辦，但一些熟悉 Meridian Process 的主辦國可優先考慮。墨西哥、挪威及西班牙表示未來可考慮主辦，而加拿大與瑞士則表示若 2015 年沒有國家願意主辦則兩國願意擔任主辦國。墨西哥表示由於該國 2015 年為大選年，希望能排除 2015 主辦國，2016 年確定能夠主辦。西班牙與挪威代表均表示 2016 年確定能夠主辦，2015 年的主辦權則需要與國內權責部會討論，並將討論結果在今年底前回復。

2.Meridian 新網站

Meridian 新網站係由瑞典建置，在指導委員會上大家均對瑞典的貢獻表示致意。針對網站內容的存取權限，指導委員會決議對所有進入網站區域限制的使用者顯示警告訊息，讓使用者知道網頁中包含 Meridian 社群會員的機敏資訊(TLP:Green)。阿根廷將負責依一項新的流程倡議(Process Initiative)，協助將網站的資源區英文內容翻譯為西班牙文，並將此次會議西班文簡報翻譯為英文，並放置在 2013 年會議摘要區。明年會議的日文資料也將會做類似雙語的安排。此外網站中會建立一個獨立的聯絡窗口目錄(Directory Point of Contacts)存取分類，讓沒有適當權限的使用者無法取得限制區域完整目錄。指導委員會決議應訂定網站存取政策，此政策初稿將由 Peter Burnett 與瑞典共同協商制訂，並將包含下列議題：每個國家註冊用戶的上限、如何替換已註冊但已離開 Meridian 業務之用戶、尚未加入 Meridian 組織等，俾利有意願了解更多資

訊的國家及 Meridian 相關國際組織加入。

在指導委員會上有國家提出網站內容所有權或版權議題，經澄清目前網站內容沒有法定的擁有人(除了商標與品牌是註冊在英國)。考量到過去所有的內容均沒有考量版權，等同於捐贈給 Meridian 網站，且此議題牽連甚廣，因此目前也無任何計畫要改變此現況。考量上述相關議題與改變所帶來的衝擊與評估，新網站預計於 102 年 12 月 1 日上線。

3.聯絡窗口目錄(Directory Point of Contacts)

瑞典已將此目錄改版為可以線上查詢服務。指導委員會決議目錄中並不需要增加國際組織單元，但會提供一個”資源”項目內含積極參與 Meridian 事務的國際組織連結(例如 ENISA、OAS)。目錄搜尋服務與結果將以英文呈現，但未來將於適當時機提供西班牙文翻譯。指導委員會鼓勵所有參加 2013 年會議的國家都加入聯絡窗口目錄，並可尋求列名指導委員會國家協助。

4.秘書處(Secretariat)角色與經費

指導委員會認可永久秘書處對協助會議永續性與歷史知識，以及年度會議間活動促進的貢獻。目前秘書處的經費是由英國贊助，該經費預計於 2014 年 3 月結束，英國正在嘗試爭取延長贊助經費 1 年。若英國無法順利爭取贊助經費，指導委員會討論幾種可能替代選擇，包括民間廠商贊助(但應避免演變成供應商支配的狀況)、研討會收費(對新加入國家會造成妨害因此不予考慮)、由指導委員會或所有國家共同分攤(會衍生管理成本)或是將此費用納入每年會議主辦國的成本中(等同於支付給專業的會議主辦組織)。

上述選項都會產生不同的未決事宜，例如秘書處選擇的競爭、超過一年以上的延續性、秘書處對資金進行轉帳的法定地位、可能被大型顧問公司把持的可能性以及成立國際法人組織的可能性(未來會考慮，但目前尚不考慮此選項因爲可能會產生大量的管理成本)。此外尚有其他公共性的資源需求要納入考

量，例如網站維護與發展每年約需 3 萬英鎊。

秘書處的角色分為兩個部分：對來年會議的支援與年度內活動的支援。年度內活動特別需要專用的資源，以提供可信任與持續性的支援，但期望單一國家長期支持是不可行的。因此指導委員會決議組成一個工作小組，針對上述可能選項進行評估並提出建議方案。指導委員會一致同意針對現行 Meridian Process 進行整理是一個沈重的負擔(包括將指導委員會/議程委員會角色、盤點現有倡議與未來方向、考慮年度內 Meridian Process 相關活動模式及會員會籍的記錄與統計等)。指導委員會也同意在年度會議後發展工作小組相關活動，對維持動能相當重要。

5.Meridain 2014 年會議

2014 年會議將在日本舉辦，日本表示會議地點可能選在仙台，因為仙台距離日本控制系統安全中心(Control System Security Center)所在的多賀城很近。日本將會指派議程委員會的主席，以便規劃與準備 2014 年會議，指導委員會的成員都有資格參與議程委員會。未來將會有文件陳述指導委員會與議程委員會的功能與章程。

日本將會提出議程委員會實體會議與電話會議的時程，其中實體會議可能於 2014 年 3 月在日本召開，此外日本也表示會在所有電話會議前將會議文件提供給參與國家，並尋求改善電話會議通話品質的解決方案。

參、心得與建議

一、 由 Meridian 2013 年會中各國的報告可以發現，包括美國、歐盟、日本及中南美洲等許多國家均已制訂國家網際安全策略(National Strategy for Cybersecurity)。2013 年 10 月 Hathaway Global Strategies 公司所發布的網際整備度指標(Cyber Readiness Index)除包括資安主管機關設置、國家電腦緊急應變團隊(National CSIRT)、網路犯罪公約、資訊分享、技術研發及經費統計資訊外，國家網際安全策略亦是其中一項重要指標[2]。我國雖已制訂行政院國家資通訊發展方案，但過去並未將發展方案翻譯為英文版，後續應以發展方案為基礎，製作國家網際安全策略與整備度英文簡介(廣宣資料)於各類國際會議上發表，另在行政院國家資通安全會報網站亦應即時更新英文簡介與資料，以呈現我國政府對資安之努力。

二、 美國依據歐巴馬總統 13636 號"改善關鍵基礎設施網際安全"行政命令發展的網際安全框架，雖未能透過立法成為對關鍵基礎設施業者的強制性要求，但由目前草案可以看出該框架希望提供一個能夠區分優先順序、具彈性、可重複、重效能及具成本效益的方法，協助負責關鍵基礎設施服務的組織來管理網際安全風險。此框架強調依賴現有的標準、指引及最佳實務，而不另行定義新的標準或指引。利用此框架與框架中的元件，企業組織可以用共通的語言與機制來描述目前網際安全的狀態、欲達成的目標狀態、在風險管理的內涵下找出改善的優先機會、評估朝向目標狀態的進展及促成內外利害關係人的溝通。因此後續應持續觀注此框架的發展，並思考如何與國內之作法整合。

三、 日本於 2013 年 10 月由內閣官房之資訊安全政策委員會依據 2013 年 6 月制訂的日本復興戰略(Japan Revitalization Strategy)與網際安全策略(Cybersecurity Strategy)，制訂網際安全合作國際策略，簡稱 j-initiative for Cybersecurity。根據該策略，日本將透過網際網路流量監控資料分享專案(TSUBAME)與 Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE)專案與其他國家強化網際安全技術合作，我國應積極規劃如何與日本之相關專案進行合作。

四、 我國過去曾經主辦過 Meridian 會議，因此目前為 Meridian 指導委員會成員國之一，具有資格參加 Meridian 會議結束後的閉門指導委員會會議。我國應持續積極參與 Meridian 會議與指導委員會會議，以維持我國在指導委員會的資格。此外也可思考積極參與 Meridian Process 與工作小組專案，例如維持更新聯絡窗口目錄、工業控制系統安全交流的小組委員會(Meridian Process Control Systems Info. Exchange, MPCSIE)等，讓其他國家可以感受到我國對 Meridian 國際社群之貢獻。

肆、參考資料

[1]Preliminary Cybersecurity Framework, http://www.nist.gov/itl/cyberframework.cfm

[2]Cyber Readiness Index,
http://belfercenter.ksg.harvard.edu/publication/23607/cyber_readiness_index_10.html

伍、附錄

一、附件 1 Meridian 2013 年會與會人員合照

附件1　Meridian 2013 年會與會人員合照