出國報告（出國類別：出席國際會議）

參加 108 年第 15 屆 MERIDIAN 關鍵資訊基礎設施防護會議

服務機關：行政院
姓名職稱：徐嘉臨副處長
派赴國家/地區：瑞士
出國期間：108 年 10 月 13 日至 10 月 19 日
報告日期：108 年 12 月 18 日

摘要

本報告說明參加 108 年第 15 屆 MERIDIAN 關鍵資訊基礎設施防護會議之經過與發現，內容包含德國、瑞士、印尼、日本等國家之關鍵資訊基礎設施安全防護現況，及經濟合作發展組織（OECD）、歐盟資通安全局（ENISA）等國際組織在資通安全領域之發展近況，並提出心得與建議作為主管機關後續推動相關工作之參考。

目錄

一、 背景說明

MERIDIAN 會議係由英國政府於 2005 年倡議創立，自始每年召開 1 次年會，由參與國輪流主辦，會議定位以關鍵資訊基礎設施之安全防護為主，與會人員以政府公務員為限，本（108）年輪由瑞士主辦，會議以「Think Local, Act Global」為題，著重關鍵資訊基礎設施在公私與國際合作等議題之探討，透過出席本次會議，除了解各國在關鍵資訊基礎設施資安防護之發展趨勢並借鏡其經驗外，亦參與各項分組討論，分享我國作法，促進國際交流與合作。

二、 會議議程

本次會議於 108 年 10 月 15 日至 10 月 17 日在瑞士日內瓦舉行，議程（如附件）摘要如下：

（一） 108 年 10 月 15 日全日：上午為開場及歡迎儀式；下午由德國、美國、瑞士等國分享該國關鍵資訊基礎設施防護現況及由經濟合作發展組織（OECD）、歐盟資通安全局（ENISA）等國際組織分享該組織之近期資安發展重點。

（二） 108 年 10 月 16 日全日：上午由西班牙、瑞典、資安事件應變合作組織（FIRST）等分享利害關係人管理及由美國、愛沙尼亞等分享國際合作措施；下午進行 2 場分組討論。

（三） 108 年 10 月 17 日半日：上午安排參訪位於瑞士與法國邊境之 CERN 歐洲核子研究組織後結束本次會議。

三、 會議重點摘要

（一） 德國關鍵資訊基礎設施防護現況

1. 德國在歐盟國家中係屬較早透過立法推動關鍵資訊基礎設施防護之國家，該國自 2015 年制定 IT-Security Law 納管關鍵基礎設施提供者，目前該國之關鍵基礎設施計分政府機關、能源、健康、資通訊、交通、媒體與文化、水資源、金融與保險、食品等 9 個領域，納管對象數量計 1642 個，各領域納管對象之數量如下圖 1 紅框欄內所示，其中以金融及保險領域納管數量最多，另自立法施行至今，關鍵基礎設施提供者通報之資安事件數總計 358 件（如下圖 1 藍框欄內所示），其中以資通訊領域通報之件數最多，近期該國開始關注關鍵基礎設施之供應鏈安全，對於投資關鍵基礎設施之第三國已進行管制，後續規劃透過修法要求關鍵基礎設施之設備商負有弱點通報及產品需通過檢測之義務，另將調降納管關鍵基礎設施之門檻，擴大關鍵基礎設施納管

範圍，此外，值得一提的是，該國在 2007 年尚未立法納管關鍵基礎設施之前，即已透過 UP KRITIS 計畫以公私協作方式促進關鍵基礎設施提供者進行自我資安防護，該計畫至今仍持續運作與精進中。

Sector	Estimated (= 1650)	IS (= 1642)	Notifications since entry into force (= 358)
Energy	320	294	66
ICT	30	67	117
Food	150	107	13
Water	230	200	18
Health	368	332	63
Finance and Insurance	356	403	94
Transport and Traffic	196	239	58

圖 1 德國各領域關鍵基礎設施之納管數量及資安事件通報次數

2. 德國在本次會議中介紹該國辨識關鍵基礎設施之作法，其辨識關鍵基礎設施採三步驟進行，分別為從國家高度辨識關鍵服務（critical services）、接著自關鍵服務中辨識必要設施、最後再訂定篩選基準自必要設施中篩選出關鍵基礎設施，目前德國訂定之篩選基準為「50 萬人」，意即當設施失效影響民眾 50 萬人以上者，即認定為關鍵基礎設施，各領域主管機關可依據上述基準，換算成適用各該領域之基準（各領域轉換後之基準為 Thresholds of the BSI-Kritis Ordinance 公開文件），上述認定基準每 2 年檢討一次。

（二） 瑞士關鍵資訊基礎設施防護現況

瑞士之關鍵基礎設施共分為 6 項領域，分別為食品（Food）、資通訊（ICT）、能源（Energy）、醫療（Health care）、物流（Logistic）、工業（Industry）等，目前並無專責機關負責資安管理事務，為解決日益嚴重之資安威脅及符合歐盟資安法規之要求，於本年成立 National Cyber Security Center（NCSC），負責擔任跨機關協調之角色，近年為提升關鍵資訊基礎設施防護能量，聯邦政府機關 Federal Office for National Economic Supply（FONES）參考美國國家標準暨技術研究院（NIST）所訂定之 Cyber Security Framework （CSF），透過公私合作方式，完成制定國內關鍵基礎設施之最低資安防護水準，供各界參考運用。

（三） 印尼關鍵資訊基礎設施防護現況

印尼主管關鍵資訊基礎設施之政府機關為 National Cyber & Crypto Agency（BSSN Indonesia），BSSN Indonesia 係於 2017 年成立並直接隸屬總理府，負責統籌及協調國家資安事務，近 2 年積極辦理關鍵資訊基礎設施之各領域演練工作，依據 Global Cybersecurity Index, ITU 所公布之各國資安評比報告，該國於 2017 年及 2018 年分別獲得 70 名及 41 名，成績進步可觀，該國近年來致力於發展數位經濟，為兼顧數位經濟發展與降低網路安全威脅，後續將以推動資安情資分享作為工作重點。

（四） 歐盟 ENISA 近期發展重點

歐盟於 2016 年及 2019 年分別訂定 NIS Directive 及 Cybersecurity act 之後，正式賦予歐盟資通安全局 The European Union Agency for Cybersecurity（ENISA）法律地位及授予該機構扮演提升歐盟網路安全之角色，並賦予其更多的資源和新任務，特別是在訂定歐盟會員國適用之資通安全認證產品、服務或流程等工作上，另外授命其擔任協調跨國資安應變之角色，當在歐盟國家遭遇大規模跨域網路攻擊或危機時，須協助各國進行應處。

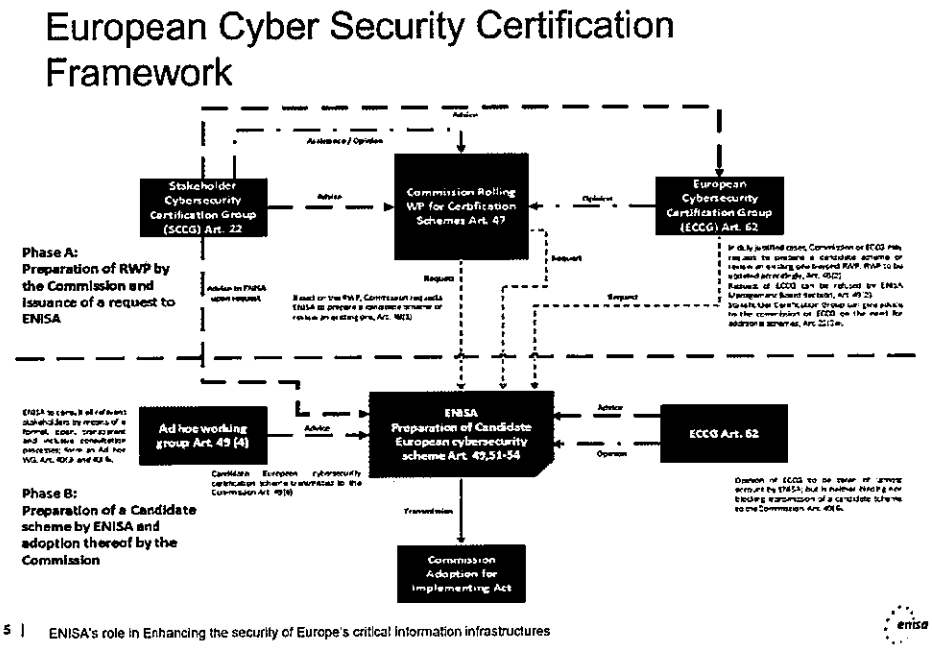

圖 2　ENISA 訂定資通安全認證標準之框架

面對與日俱增之物聯網資安威脅及供應鏈安全議題，加上歐盟各會員國對資通產品之安全標準認定不一，爰由 ENISA 統一訂定資通安全認證標準供各會員採用，上圖 2 為 ENISA 訂定資通安全認證標準之框架，說明 ENISA 與相關利害關係人間之協同合作關係。簡言之，歐盟建立資通安全認證標準之程序大致分為二階段，第一階段為需求確認階段，歐盟委員會藉由啟動 Rolling

Work Program（RWP）向 ENISA 提出認證需求，ENISA 於接受需求建議後，即進入第二階段，透過徵詢各界意見方式草擬認證標準，認證標準通常訂有不同之保證級別（如基本、重要或高，basic, substantial or high）供不同情境及需求使用。

（五） OECD 近期發展重點

該組織正著手草擬 economic and social risk management approach to digital security 文件供會員國參考，本文件制定之目的在協助各國於轉型數位國家之過程中，能同時降低數位安全（digital security）對各國之經濟及社會活動之衝擊，特別是在雲端服務、物聯網、人工智慧、5G 等新興科技日漸發達的未來，本文件提出風險管理方法如下圖 3，首先係以國家層級之高度辨識關鍵活動及營運者，再逐步辨識關鍵功能及產生相對之風險控制措施，本文件預定於 2019 年底定稿。

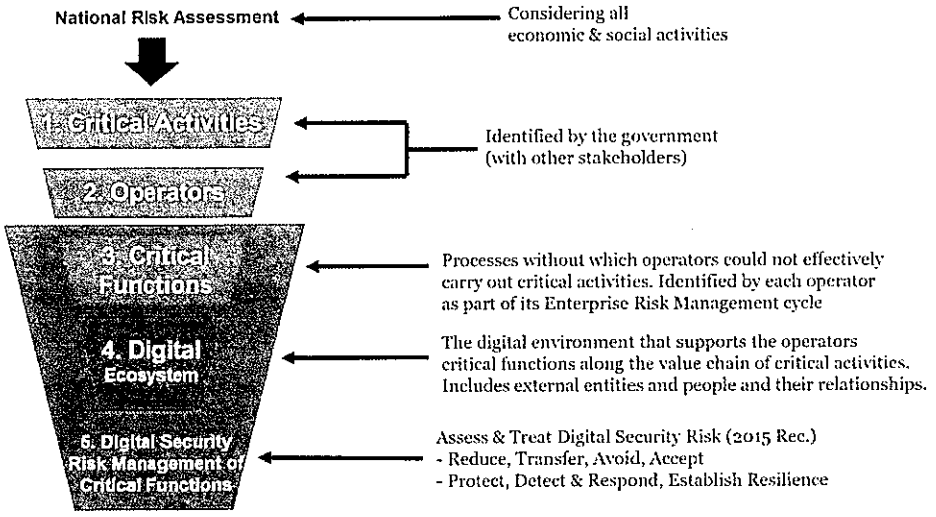

圖 3　OECD 數位安全風險控制流程

（六） 日本政府推動關鍵資訊基礎設施防護之公私合作做法

日本政府 National Center of Incident Readiness and Strategy for Cybersecurity in Japan（NISC）於本次會議分享該國在關鍵資訊基礎設施公私合作之作法，其作法主要有三，分別為公私部門共同訂定應遵守之防護政策、建立情資分享機制、定期執行資安事件應變演練等，為了防範 2020 年該國舉辦東京奧運所可能遭受之資安威脅，特地在本年進行公私跨領域聯合演練，測試情資分享作業之有效性及動員應變能力。

（七） 供應鏈安全（Supply Chain Management–Trustworthy IT-Components and Services）議題

隨著物聯網時代的來臨，物與物及物與人透過網路相互連結將更為緊密，而隨之而來的是上下游產品間之供應鏈安全議題，如何避免因單一節點存在安全弱點，而影響整體系統之安全，已漸受重視，歐盟雖已責成 ENISA 進行資通產品之安全認證工作，但如德國等歐盟國家仍在思考除認證產品外，是否仍有其他有效防堵措施可供進一步強化供應鏈安全，會中提出之解決方式包含透過立法對產品訂定最低安全要求、對產品中之不信任元件採取預防管控措施、要求供應商主動公布產品弱點等，多數參與本次會議之國家認為供應商對主動公布產品弱點之態度普遍較不積極，建議各國政府集結力量以聯合要求方式，較有利於提高供應商之配合度。

四、 心得及建議

（一） 透過公私合作方式推動關鍵資訊基礎設施安全防護，仍是各國當前工作重點，而建立公私夥伴間之信任關係仍是最大挑戰，多數國家多採循序漸進方式，在逐步建立互信關係之基礎上，深化各項聯防工作。整體而言，邀請關鍵基礎設施提供者聯合辦理攻防演練及主動提供威脅情資，常為公部門搭建公私協同合作關係之起點，當逐漸建立互信關係後，再逐步發展合作模式，如共同研擬防護法規或標準、就最佳防護典範或實務進行交流、公部門主動佈署威脅偵測與協防機制等，我國雖自今年起透過資通安全管理法納管關鍵基礎設施提供者，然徒法不足以自行，仍待透過公私夥伴關係之建立，逐步引導關鍵基礎設施提供者強化自身資安防護能量，部分歐美國家之發展進程相較我國已較成熟，相關推動經驗殊值本處參考借鏡。

（二） 歐盟 ENISA 刻正訂定資通產品、服務及流程等資安認證標準工作，此作法與我國近年來配合 5+2 產業創新所積極建立之物聯網資安驗證標準不謀而合，如二者能銜接相容，對我國資通產業進入歐洲市場將有絕對優勢，後續我方仍應持續密切觀察 ENISA 之進度與動向，並持續爭取合作制定認證標準之機會。

（三） 識別關鍵基礎設施係進行關鍵資訊基礎設施防護管理之首要步驟，依據歐盟 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75)指令，各國應基於基礎設施遭破壞之影響及嚴重性，訂定識別關鍵基礎之基準值（cross-cutting criteria），反觀我國目前在識別關鍵基礎設施之作法上並未就衡量指標統一訂定跨領域之基準值，而係由各領域主管機關自行訂定標準，以致產生不同

領域間之納管認定標準不一之情形，建議於二年後定期檢視關鍵基礎設施納管範圍時，可就上述問題參考歐盟國家做法進行適度調整。

五、 附件

108 年第 15 屆 MERIDIAN 關鍵資訊基礎設施防護會議議程。

MERIDIAN
Connecting and Protecting

SWITZERLAND
2019

DAY 1 – FUNDAMENTALS

October 15, 2019

Morning **9:00 – 10:00** **(Break 30')**	Opening Report Meridian 2018 (KOREA)		
10:30 – 11:15 **(Break 15')**	Keynote – Think Local, Act Global Federal Delegate for Cyber-Security		
11:30 – 12:30 **(Lunch 90')**	Ice Breaker/Speed Dating		
Afternoon **14:00 – 15:00** **(Break 15')**	Panel 1 – National fundamentals GERMANY, USA, SWITZERLAND - CI and economic policy - National strategies - Minimal Standards adapted for CI-Sectors		
15:15 – 16:15 **(Break 15')**	Work-Shop 1a GERMANY Identifying your NCI	Work-Shop 1b SINGAPORE Protecting your ICS	Workshop 1c SPAIN National Guide for Cyber Incident Management & Reporting
16:30 – 17:30	Round Table – International Frameworks and (Standardization) Initiatives GFCE, OECD, ENISA - CIIP Capacity, Framework and Collaboration - International Standardization - Activities in the field of CIIP		

MERIDIAN
Connecting and Protecting

SWITZERLAND
2019

DAY 2 – STAKEHOLDERS

October 16, 2019

Morning **9:00 – 10:00** **(Break 15')**	Panel 2 – Identifying your relevant stakeholders SPAIN, SWEDEN, FIRST/ITU - Implementation of NIS Directive - Regional Experiences - Tech for policy makers		
10:15 – 11:15 **(Break 15')**	Work-Shop 2a JAPAN/SPAIN Approaches to PPP	Workshop 2b SWEDEN Center of Competence – Setting up the administration	Workshop 2c SWITZERLAND Stakeholder Management
11:30 – 12:30 **(Lunch 90')**	Panel 3 – International Initiatives/Collaborations WEF, USA, ESTONIA - Regional Approaches to Managing Stakeholders - Regional Initiatives - Cyber 4 Development		
Afternoon **14:00 – 15:00** **(Break 15')**	Work-Shop 3a GERMANY Supply Chain Management: Trustworthy IT-Components and Services	Workshop 3b SWITZERLAND International Initiatives and what they bring to CIIP Policy makers	Workshop 3c WEF Vendor, Buyer and the State
15:15 – 16:15 **(Break 15')**	Wrap – Up Information about Changes to the Meridian Secretariat and the Meridian Website		
16:30 – 17:00 **(Refresh 60')**	End of Conference		