出國報告（出國類別：其他國際會議）

出席「2018 年美日合辦之工業控制系統網路安全聯合訓練」報告

服務機關：行政院資通安全處
姓名職稱：周智禾 科長
派赴國家：日本(東京)
出國期間：107 年 9 月 9 日至 107 年 9 月 16 日
報告日期：107 年 11 月 16 日

摘　　要

日本經濟產業省(METI)與美國國土安全部(DHS)共同舉辦，並邀請東南亞國家協會(簡稱東協)10 個成員國、澳洲、紐西蘭、南韓、印度及我國等與工控領域相關人員前往參與 Japan & US Joint Training for Industrial Control Systems Cybersecurity 2018，講授工業控制系統國際資安趨勢、檢測技術及防禦架構等資安相關課程。

本次課程包含「Introduction to Control Systems Cybersecurity (101) Training」、「Intermediate Industrial Control Systems Cybersecurity (201) Training-Part1」、「Intermediate Industrial Control Systems Cybersecurity (201) Training-Part2」、「Introduction of Recent Trends in Threats in Asian Region and Cooperation among CERTs」、「Introduction of Industrial Cybersecurity Measures in the United States」、「Overview and Demonstration of Facilities of ICS CoE」、「Introduction of Industrial Cybersecurity Policy」及「Introduction of Measures of Electric Utility Security by Electricity Company」等項目，均與工業控制系統資安議題有著密切關係。

目　　錄

壹、會議介紹

一、會議名稱

Japan & US Joint Training for Industrial Control Systems Cybersecurity 2018

二、會議時間

107 年 9 月 10 至 107 年 9 月 14 日

三、會議地點

9 月 10 日至 11 日：東京大學

9 月 12 日：IPA 行政法人情報處理推進機構 Bunkyo Green Count 8F

9 月 13 日：財團法人海外產業人才育成協會(AOTS)

9 月 14 日：IPA 行政法人情報處理推進機構(Akihabara UDX)

貳、參加會議目的

隨著近年來勒索軟體的猖獗、多種 API 重大漏洞被發現及 DDoS 攻擊規模的提升，資安議題逐年備受重視。而備受矚目的資安議題已不僅侷限於網站應用程式、系統服務或行動裝置中，工業控制系統與物聯網安全也成為全球性的課題之一。

日本經濟產業省(Ministry of Economy, Trade and Industry，以下簡稱 METI)與美國國土安全部(Department of Homeland Security，以下簡稱 DHS)共同舉辦，並邀請東南亞國家協會(以下簡稱東協)10 國、澳洲、紐西蘭、南韓、印度及我國等 15 國之工控領域相關人員前往參與 Japan & US Joint Training for Industrial Control Systems Cybersecurity 2018，講授工業控制系統國際資安趨勢、檢測技術及防禦架構等資安相關議題。

本次參與該課程除學習工業控制系統相關安全知識與技巧外，並可透過與各國參與人員進行工業控制領域相關資安趨勢與實驗經驗交流，培養工業控制系統檢測能力

參、會議過程及重點議題

一、會議議程

Japan & US Joint Training for Industrial Control Systems Cybersecurity 2018 分別於 9/10~9/11「東京大學」、9/12「IPA 行政法人情報處理推進機構 Bunkyo Green Count 8F」、9/13「財團法人海外產業人才育成協會(AOTS)舉行」及 9/14「IPA 行政法人情報處理推進機構 Akihabara UDX」舉行為期 5 天訓練課程，議程時間表與詳細議程詳見圖 1 與表 1。

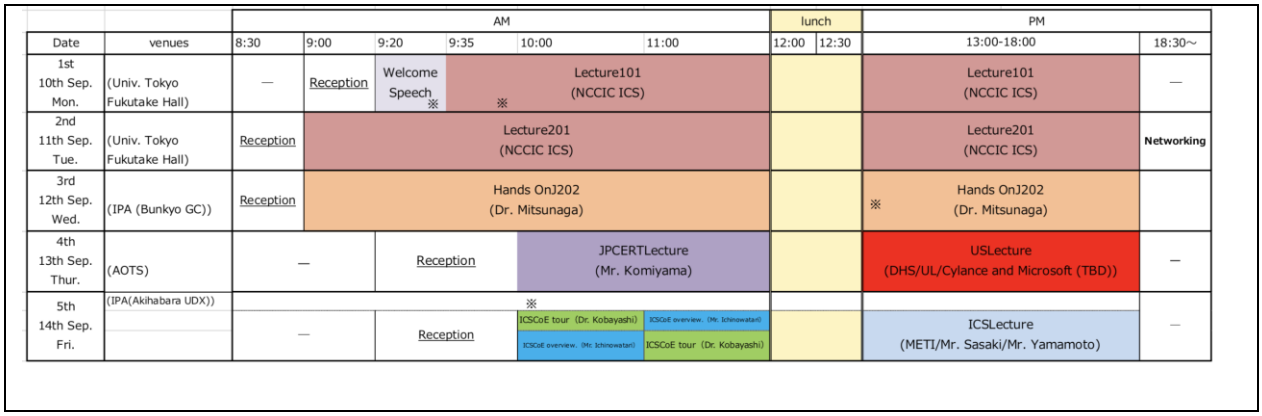

圖1　議程時間表

表1　詳細議程

日期	議程	講師
9/10	Introduction to Control Systems Cybersecurity (101) Training	Gary Finco (NCCIC)
9/11	▪ Intermediate Industrial Control Systems Cybersecurity (201) Training-Part1 ▪ Networking	▪ Gary Finco (NCCIC) ▪ Melinda Cebull (NCCIC) ▪ Chris Johnson (NCCIC)
9/12	▪ Intermediate Industrial Control Systems Cybersecurity (201) Training-Part2	Takuho Mitsunaga (Tokyo

日期	議程	講師
		University)
9/13	▪ Introduction of Recent Trends in Threats in Asian Region and Cooperation among CERTs ▪ Introduction of Industrial Cybersecurity Measures in the United States	▪ Koichiro Komiyama (JPCERT) ▪ Yukako Uchida (JPCERT) ▪ Ken Katayama (Microsoft Japan) ▪ Jeff Gray (DHS) ▪ Nathaniel Jones (DHS) ▪ Abel Torres (UL)
9/14	▪ Overview and Demonstration of Facilities of ICS CoE ▪ Introduction of Industrial Cybersecurity Policy ▪ Introduction of Measures of Electric Utility Security by Electricity Company	▪ Yoshiaki Ichinoatrai (IPA) ▪ Toshikazu Okuyu (METI) ▪ Hiroshi Sasaki (McAfee) ▪ Keiji Shinohara(TEPCO Power)

二、重點議題

(一)開幕式

本次訓練課程開幕式由日本副經濟產業大臣武藤容治、美國駐日大使 William Hagerty 及獨立行政法人情報處理推進機構(Information-technology Promotion Agency，以下簡稱 IPA)理事長富田達夫致詞，內容提及美日首次共同舉辦聯合訓練，顯見美日對於工業控制系統資安之高度重視。參與國家與其組織詳見表 2，致詞資料照片詳見圖 2 與圖 3。

表2　參與國家與組織

項次	國家	組織
1	柬埔寨	MPTC (Ministry of Posts and Telecommunication)
2	印尼	NCEA (National Cyber Encryption Agency)
3	寮國	MPTC (Ministry of Posts and Telecommunication)
4	馬來西亞	NACSA (National Cyber Security Agency)
5	緬甸	MTC (Ministry of Transportation and Communications)
6	菲律賓	DCST (Department of Information and Communications Technology Office)
7	泰國	ETDA (Electronic Transactions Development Agency)
8	越南	AIS (Authority Information Security)
9	澳洲	CERT Australia
10	汶萊	BruCERT
11	紐西蘭	CERT NZ
12	印度	CERT-In
13	中華民國	TWNCERT
14	韓國	KrCERT/CC
15	新加坡	SingCERT

圖2　日本副經濟產業大臣武藤容治致詞

圖3　美國駐日大使 William Hagerty 致詞

(二)基礎工控資安簡介

第 1 日課程由美國 DHS National Cybersecurity and Communications Integration Center (NCCIC)的 Gary Finco 先生講授「Introduction to Control Systems Cybersecurity (101) Training」，內容包含工業控制系統基本元件、架構、風險及工控資安事件案例等項目，大綱詳見表 3。

表3　Introduction to Control Systems Cybersecurity (101) Training 大綱

項次	大綱
1	Describe ICS deployments, components, and information flow

2	Differentiate cybersecurity within IT and ICS domains
3	Discuss cyber risk to ICSs
4	Explain a cyber exploit in an ICS infrastructure
5	Recognize sector dependencies

(三)中階工控資安簡介

第 2 日課程由美國 DHS NCCIC 的 Gary Finco 先生、Melinda Cebull 小姐及 Chris Johnson 先生共同講授「Intermediate Industrial Control Systems Cybersecurity (201) Training-Part1」，內容包含實際演示較深入的 PLC 梯形邏輯圖，並說明滲透路徑、檢測手法及使用 NIST 框架執行網路偵測方法及防禦與事件回應等項目，大綱詳見表 4，相關課程照片詳見圖 4 與圖 5。

表4　Intermediate Industrial Control Systems Cybersecurity (201) Training-Part1 大綱

項次	大綱
1	Describe ladder logic
2	Describe network discovery
3	Discuss the three main stages of an attack
4	Create a baseline using CSET
5	Describe network defense, detection, and response using the NIST cybersecurity framework

圖4　簡易控制系統演示

圖5　簡易控制系統內部元件

(四)工控檢測實作課程

第 3 日課程由日本東京大學 Takuho Mitsunaga 教授講授「Intermediate Industrial Control Systems Cybersecurity (201) Training-Part2」，將參與人員分為 7 組，每組配置一組水力模擬環境並做為攻擊標的進行檢測實作課程，以任務形式完整演示攻擊者由外而內如何進行滲透，並對 PLC 與 HMI 執行弱點攻擊，大綱詳見表 5，相關課程照片詳見圖 6、圖 7 及

圖 8。

表5　Intermediate Industrial Control Systems Cybersecurity (201) Training-Part2 大綱與實作說明

項次	大綱	實作說明
1	Industrial control systems overview	工控簡介與實作環境設定
2	Network discovery and mapping	▪ 操作 Nmap 工具(任務 1) ▪ 操作 Wireshark 工具(任務 2) ▪ 操作 Nessus 工具(任務 3)
3	Exploitation and using Metasploit	▪ 操作 Metasploit 工具執行 MS17-010 攻擊(任務 4)
4	Network attacks and exploits	▪ 執行 SQL Injection(任務 5) ▪ 操作 Mimikatez 工具(任務 6)
5	Lateral movement across ICS networks	▪ 針對控制網路進行資訊蒐集(任務 7) ▪ 攻擊網路攝影機(任務 8) ▪ 攻擊 Gateway 伺服器(任務 9) ▪ 竊取 OPC 伺服器密碼(任務 10) ▪ 針對 PLC 執行重送攻擊 1(任務 11) ▪ 針對 PLC 執行重送攻擊 2(任務 12) ▪ 針對 PLC 執行重送攻擊 3(任務 13) ▪ 攻擊 OPC 伺服器 1(任務 14) ▪ 攻擊 OPC 伺服器 2(任務 15) ▪ 攻擊 OPC 伺服器 3(任務 16)
6	Network defense, detection, and response	操作 NetworkMiner 工具(任務 17)

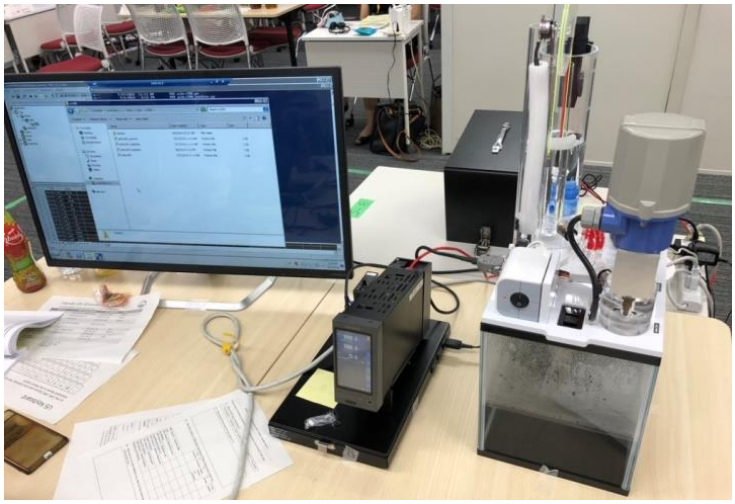

圖6　水力模擬環境

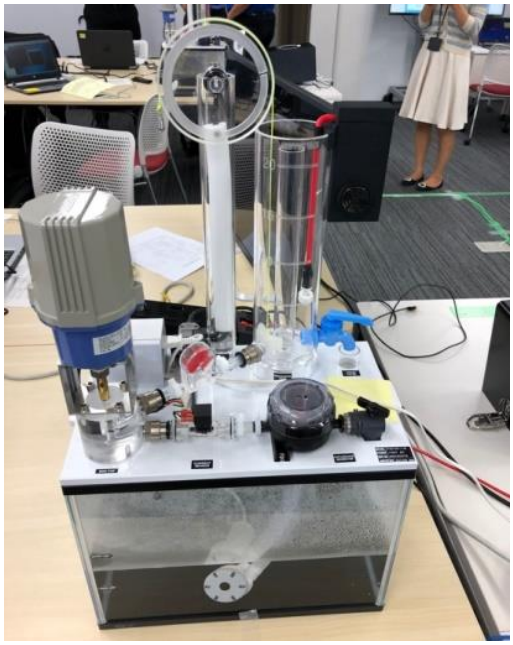

圖7　水力模擬環境感測器

圖8　實作課程解題平台紀錄

(五)工控資安威脅趨勢與防禦措施

第 4 日課程分上下午兩場，上午場由日本 JPCERT Koichiro Komiyama 先生與 Yukako Uchida 小姐講授「Introduction of Recent Trends in Threats in Asian Region and Cooperation among CERTs」;下午場由美國 DHS Jeff Gray 先生與 Nathaniel Jones 先生、微軟 Ken Katayama 先生及 UL Abel Torres 先生講授「Introduction of Industrial Cybersecurity Measures in the United States」，上午場議程大綱詳見圖 9，下午場議程大綱詳見表 6。

圖9　上午場議程大綱

表6　下午場議程大綱

項次	主題	講者
1	National Cybersecurity & Communications Integration Center Overview	Jeff Gray (DHS)
2	ICS Malware/DHS IoT Principles, Priorities and Challenges	Nathaniel Jones (DHS)
3	IoT Baseline Security and Policy	Abel Torres (UL)
4	The realization of Society 5.0 Cybersecurity Policy for a Safe and Secure Cyberspaces	Ken Katayama　(Microsoft Japan)

(六) 參觀 IPA ICS CoE

第 5 日課程由 IPA 安排「Overview and Demonstration of Facilities of ICSCoE」，The Industrial Cybersecurity Center of Excellence (ICSCoE)建置諸多與真實環境軟硬體規格相同之模擬場域，以利 IPA 進行更完善與真實的工控資安研究，據以建立相關檢測與防禦策略。模擬場域包含建築管理系統、電力控制系統、機械製造系統及交通控制系統，模擬環境資料照片詳見圖 10、圖 11 及圖 12。其中除介紹模擬環境外，更以建築管理系統為標的，演示下列 4 種攻擊手法：

1. 攻擊 PLC，使建築管理系統中的照明功能關閉或燈光閃爍不定。
2. 攻擊網路攝影機，置換監視系統畫面，使操作者無法察覺遭受異樣。
3. 攻擊 HMI，使 HMI 呈現錯誤資訊導致操作者執行錯誤決策。
4. 預先於系統中植入硬體元件，並利用手機通話啟動 PLC 攻擊程式導致系統關閉，情境詳見圖 13。

圖10　建築管理系統

圖11　電力控制系統

圖12　機械製造系統

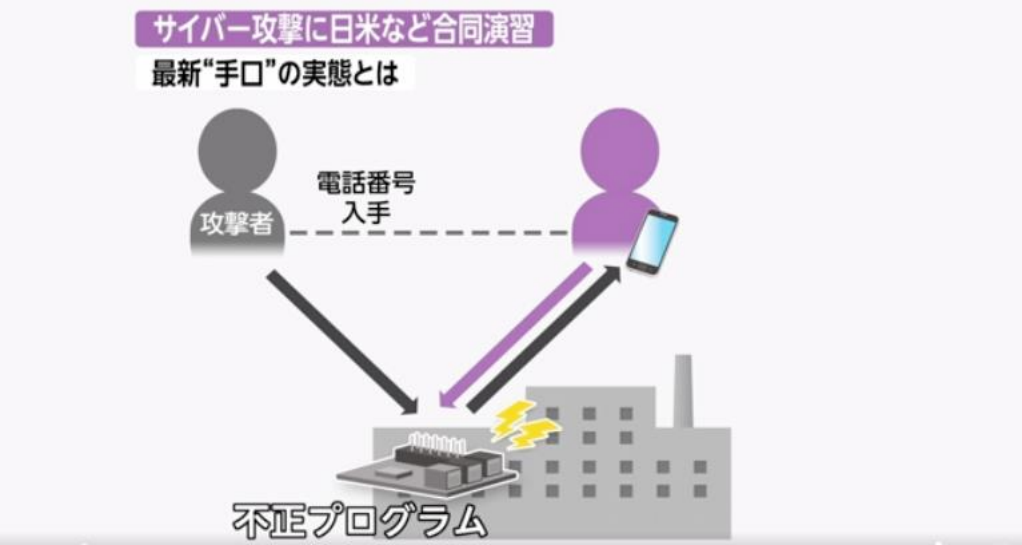

圖13　建築管理系統攻擊情境

肆、心得建議

本次參與 Japan & US Joint Training for Industrial Control Systems Cybersecurity 2018 訓練，除學習工業控制系統基礎內容、資安檢測與防禦相關知識之外，在第 2 日晚宴時，也與各國參與人員交流分享對於工控資安的觀點、看法及相關作為，也藉此機會向各國分享我國於工控檢測上的相關經驗。

參觀日本 IPA ICSCoE 時，觀摩到日本建立諸多領域的工控模擬環境供相關研究人員進行資安研究，並藉由模擬環境宣傳工控資安的重要性，實可為我國仿效用以推廣資安重要性的方式之一。日本 METI 與美國 DHS 藉由聯合辦理訓練課程，除了增加國際上的能見度，也是一種很有效的方式與各國工控相關組織/人員建立關係，以利往後國際交流。另外美國 DHS 也提供相關工控資安情資分享平台供參與人員申請使用，也是一個相當好的方式宣傳 DHS NCCIC 的相關作為。

我國除了網路攻防演練（CODE）與各國建立關係外，也可考慮利用提供訓練課程的方式與各國組織及授課講師建立關係，既可提升我國的能見度，也可增進後續國際交流的機會。