出國報告（出國類別：開會）

參加2024年日本國際資安會議（CODE BLUE 2024）出國報告

服務機關	姓名職稱
數位發展部	蘇筱筑 專案規劃師 呂世良 科長
數位發展部資通安全署	鄭欣明 副署長 劉禹君 視察 陳羿谷 專案分析師

派赴國家：日本
出國期間：113年11月12日至11月16日
報告日期：114年2月6日

摘要

日本政府為因應數位時代挑戰，設置數位廳(デジタル庁 / Digital Agency)負責推動日本整體數位轉型，透過行政作業數位化提升政府效能，並建構包括高速網路與雲端服務在內的數位基礎設施，以奠定數位社會發展基礎。

日本國際資訊安全會議(CODE BLUE)自2014年起舉辦，以其在資通安全領域的專業性與影響力聞名。CODE BLUE 2024全程為期7日(本次僅以11月14日至15日為主)，活動內容涵蓋技術性研究專案報告、技術訓練課程、資安相關供應商之業務展示會等，吸引來自全球產業與學術界資安專業人士、政府機關代表及學生參與，是國際間交流資安技術與政策的重要平台。

本次行程除與日本數位廳進行會談，探討資安政策方向、資安威脅趨勢與應對策略、資安人才培育等關鍵議題，促進雙方經驗交流與合作發展；另藉由參與國際資安會議(CODE BLUE 2024)，掌握最新資安發展趨勢、技術創新及防護實務，亦可做為強化我國資安聯防政策與因應對策擬定的參考。

目錄

壹、會議目的

在全球數位轉型與人工智慧技術快速發展的推動下，資通安全風險不斷攀升，網路攻擊形式日趨多樣且複雜，對各國政府、產業及學術機構構成重大挑戰。面對此趨勢，強化國際資安合作、交流最新防護技術、培養專業人才已成為各國資安發展的重要策略之一。

為延續臺日雙方歷年在資安領域的合作與對話，本署於2024年11月13日假日本臺灣交流協會東京本部，舉辦臺日資安交流會議，邀請日本數位廳(デジタル庁)針對資安政策方向、資安威脅趨勢與應對策略、資安人才培育等關鍵議題進行深入交流，並探討可能的合作機制。透過此次會談，我方進一步掌握日本政府資安治理政策方向與應對策略，為未來雙邊合作奠定更穩固的基礎。

此外，為掌握最新國際資安趨勢與技術發展，並做為未來國內資安政策規劃的參考，本署於2024年11月14日至15日派員參訪日本國際資安會議(CODE BLUE 2024)。CODE BLUE 自2014年創辦以來，已成為亞洲最具影響力的國際資安會議之一，聚焦於全球及亞洲區域的資安技術創新、防護策略與攻防實務經驗，並邀請來自產政學研等各界專家分享最新研究成果。CODE BLUE 的核心價值在於推動跨國資安技術交流、提供具體的行動建議，因應日益嚴峻的資安威脅。

本次 CODE BLUE 2024會議內容涵蓋最新攻防技術、資安事件應變、供應鏈安全、人工智慧在資安領域的應用、數位身分認證與隱私保護等重要議題，透過專家演講、技術培訓課程及產業交流活動，深入剖析當前全球資安挑戰，並探索可能的解決方案。我方參與此次會議，除可吸取國際最新的資安技術與管理經驗，亦有助於強化與國際資安社群的聯繫，提升我國在全球資安領域的合作機會。

貳、會議簡介

一、臺日資安交流會議

日本數位廳成立於2021年9月，旨在推動全國數位轉型(Digital Transformation)，提升政府運作效率並促進社會數位化發展。該機構負責整合與優化各級政府部門的數位基礎建設，包括數據治理、雲端運算及人工智慧應用等領域，並推動民間數位創新，強化日本在全球數位競爭力中的地位。數位廳在推動數位化的同時，高度重視資通安全，確保政府與社會的數位基礎建設不受網路攻擊或數據洩漏威脅。該機構負責建立安全的電子政務架構，制定數據保護政策，並與其他政府部門協作強化關鍵基礎設施(Critical Infrastructure, CI)的防護能力。

二、2024年日本國際資安會議(CODE BLUE 2024)

「CODE BLUE」源於醫療領域，意指召集專業人員共同因應緊急狀況。在資安領域，隨著全球面臨的資通安全威脅日益增加，CODE BLUE 會議旨在成為國際重要社群，透過 CODE(技術)連接 BLUE(海洋)，匯聚來自全球各界專家共同思考應對策略。自2014年首屆會議起，CODE BLUE 成為日本最具影響力的國際資通安全會議之一，專注於推動資安技術的發展與人才培養，為複雜多樣的資安威脅探索更有效益的解方。

CODE BLUE 2024的主要議題，涵蓋人工智慧於資安領域的應用、進階持續性威脅(advanced persistent threat, APT)研究、最新的惡意程式及漏洞攻擊技術，以及企業內部實務經驗分享等，期充分展現當前與未來的資安挑戰與應處策略。

另值得一提者，來自臺灣多家資安團隊與企業獲邀參與 CODE BLUE 2024，包括：TXOne Networks(睿控網安)、DEVCORE(戴夫寇爾)、

TeamT5(杜浦數位安全)、TRAPA Security(菱鏡)、以及 CyCraft Technology(奧義智慧科技)等，分別於網路防護、漏洞研究、威脅分析等領域取得卓越成就，彰顯臺灣資安產業在國際合作發展的貢獻與實力。

圖 1 我國資安團隊與企業於 CODE BLUE 現場參與情形

參、會議紀要

一、臺日資安交流會議

- 會議時間：2024年11月13日 上午11時
- 與會人員：日本數位廳代表 (6位，非公開)
- 日方分享可公開之內容：為實現數位社會而制定的重點計畫(デジタル社会の実現に向けた重点計画)

數位社會的挑戰

日本數位廳強調數位化對社會轉型的重要性，並視其為機遇與挑戰並存的過程。在推動數位化的過程中，日本主要面臨以下四大挑戰：

(1) 人口老化與勞動力不足：高齡化導致勞動力減少，且部分年長者對數位技術不熟悉，影響數位化推動。

(2) 產業競爭力下降：傳統產業面臨國際競爭，若未能及時轉型，將影響日本的全球競爭力。

(3) 災害與數位威脅：日本須透過數據整合與技術創新因應自然災害、環境負擔及資安威脅，確保數位技術的永續發展。

(4) 對數位化的不安與疑慮：部分民眾擔憂數位技術可能侵犯隱私或響就業，影響數位政策推行。

上述種種不安與疑慮將阻礙數位化政策的推行，降低民眾參與的意願，日本數位廳說明數位化並非僅止於技術的應用，更涉及社會、經濟、法律等多方面的改革，其中政府的角色是政策制定、投資建設數位基礎設施、培育數位人才，產業的角色是技術研發、提供服務、數位轉型等，民眾則是學習使用各種數位工具、參與數位化建設，並提出意見和建議。

推動共同系統的建置

過去日本政府各部門及地方政府的資訊系統獨立運作，導致行政效率低落與數據難以共享。數位廳透過數位改革，整合分散的資訊系統，簡化行政流程、提升使用者體驗，並降低重複建設及營運成本，同時吸引廠商投入，促進數位化發展。

改革決策架構

目前數位政策決策採「制度先行、再建系統」，導致政府與廠商耗費大量時間與資源在需求溝通。數位廳擬改採先評估最終使用需求，再調整業務與規劃制度，期降低政府與廠商的溝通誤差，提高決策效率，並由數位廳統一審查各部會預算，確保整體數位政策的協調性。

使用者需求導向的數位改革

依據民眾在不同人生階段的政府服務需求，評估系統建置與更新計畫。改革將採「集中式改革」模式，先聚焦於特定領域，同步優化制度與系統，使民眾感受到數位化的便利性，降低社會對數位化的抗拒。

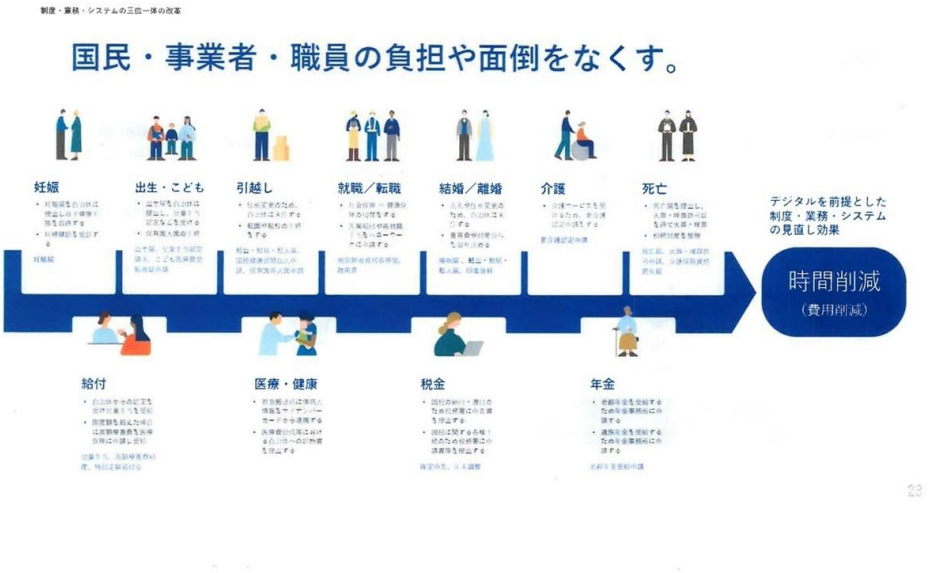

圖 2 「數位廳簡報」人生各階段的政府系統使用需求

公務人才培育計畫

數位廳推動「令和6年度資訊系統統一研修」，依職員經驗與職責分級培訓，強化資訊管理與安全能力。基礎課程以線上學習為主，專業課程則採實體訓練，主要課程如下：

(1) 基礎層級

- 資訊系統新進人員 A-1：數位管理、IT 治理、專案管理。
- 資訊安全基礎 A-2：風險分析、加密技術、網路攻擊與防範。

(2) 中級層級

- 業務流程優化 B-1：提升業務流程評估與重組能力。
- IT 職能與預算管理 B-2：強化 IT 管理、預算編制與績效評估。
- 資訊安全技術 B-3：攻擊演練、事件應處、防禦策略。
- 資訊系統營運 B-4：政府機關資安策略、風險與危機管理。

(3) 高級層級

- 管理人員培訓 B-5：高階決策與策略管理。

(4) 實作演練

- 網路防護演習：模擬網攻應變，涵蓋預先學習 以及1日現場演練。
- 資訊安全操作課程：針對部門主管強化資安技術與因應能力。

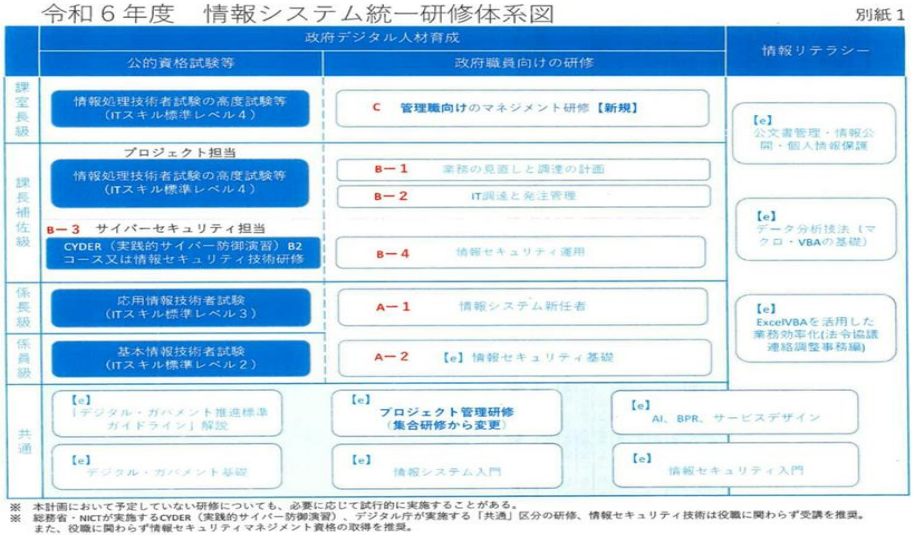

圖 3 「數位廳簡報」政府公務資訊資安人才培訓規劃

- 我方分享內容

數位轉型新時代，資料是關鍵的戰略性資產，因應人工智慧、物聯網、雲端運算等科技興起，全球產業加速朝數位化、智慧化方向轉型，過程中產生大量的資料，如何有效利用跨領域資料分析及應用，將促進國家數位治理及資料經濟發展，亦可改善公共服務與人民生活福祉。在資料應用上，我們致力於打造資料創新應用的環境：

(1) 政府資料：鼓勵各機關推動資料開放，深化政府資料開放與再利用制度，促進資料流通及格式品質。

(2) 推動個人化資料自主運用機制(MyData)：落實資料賦權理念，經由民眾身分驗證及同意機制，取得並運用其個人化資料。

(3) 資料賦能培力輔導：提升非政府及民間組織數據應用技能與提供技術支援，建立夥伴關係、相互協力使非政府及民間組織透過數據賦能找出數位轉型痛點並加以解決。

(4) 建立數據公益生態：將民間或政府所產生的資料，經過隱私強化技術處理後分享不涉及隱私的資料捐獻數據給具備公益性質的第三方利用。

<u>推動政府開放資料</u>

透過提升施政透明度、促進民眾參與公共政策，鼓勵跨機關資料流通，提高行政效率。自102年(2013年)訂定《政府資料開放作業原則》並建置「政府資料開放平臺」(data.gov.tw)，目前已累計開放逾5萬項資料集、瀏覽數突破1.4億人次，金標章資料集比例達89%。

<u>建立標準與高應用價值資料</u>

為確保資料的可用性，已訂定「領域資料標準訂定流程參考指引」，並建立「政府資料標準平臺」(schema.gov.tw)，目前涵蓋24個領域、1,995項標準。此外，自112年(2023年)起推動「高應用價值資料」計畫，聚焦於農業永續、氣候環境、災害防救、健康醫療等領域，未來將擴展更多高價值主題，推動主題式資料生態圈發展。

推動數據公益(Data Altruism)

鼓勵個人或機構自願提供經隱私強化處理的資料，供公益用途，造福社會。我國113年(2024年)1月發布「數據公益運作指引」與「隱私強化技術應用指引」，確保數據公益的合法運行與隱私保護，並與金管會、衛福部等機關合作推動公益創新應用，提升數據價值。

結合公私協力推動開放創新

透過黑客松(Hackathon)等方式激發民間創意並應用政府資料解決公共問題。例如：「總統盃黑客松」自2018年舉辦以來，已促成多項創新方案落地施行，亦透過數據培力計畫，協助非政府及民間組織提升數據應用能力，推動數位轉型。

發展數位皮夾

以公共程式(Public Code)為原則，使用者得藉由授權、認證數位身分的過程實踐「個人身分自主權(Self-sovereign Identity, SSI)」。該服務的核心目標，在於打造兼具隱私與便利性的簽章與認證機制，強化資訊安全韌性，為政府各機關提供安全且便利的證件數位化解決方案，實踐智慧國家目標。

數位皮夾可加速各政府機關證件數位化進程，協助民間身分發行者導入更安全、更容易互通的身分介接服務，民眾即可從各機關網站、各跨境平台、跨國事務與電子商務等管道介接不同數位身分，完成身分認證(AuthN)與授權(AuthZ)功能。

申言之，對於證件或身分的發行者(Issuer)而言，初期將是軟體開發工具套件(Software Development Kit, SDK)與使用介面，協助任何身分的發行商，如政府數位憑證、企業金融憑證或一般人，介接已發行之數位憑證，並自動轉換成符合分散式身分識別符(Decentralized Identifiers, DIDs)與可驗證憑證(Verifiable Credentials, VCs)標準的「卡片」，存放在使用者(Holder)同意的數位皮夾中，該過程即為認證(AuthN)；對於使用者而言，數位皮夾則是操作介面、應用程

式或數位服務，可依其需要儲存、展示、認證與授權其任一身分。此外，使用者可自行決定是否開啟這些身分的授權功能，應用於外連服務，如簽章確認、企業活動或一般娛樂目的等，該過程即為授權(AuthZ)。授權過程符合隱私保護(Privacy Preserving)原則，並進行分層授權處理，降低透露不必要資訊的風險，此部份可透過如應用零知識證明(Zero Knowledge Proof, ZKP)或其他密碼學方式進行，且由使用者個人自主管理，隨時可以取消授權服務。

本次會面，有助於理解雙方政策規劃與施行成果。當前雖囿於現實因素而無法直接形成正式合作關係，惟日方表達定期進行交流之意願，並肯認經驗分享之重要性，爰依據議題或政策需求賡續安排相關對話，仍有其必要。

二、日本國際資安會議(CODE BLUE 2024)

- 會議時間：2024年11月14日至15日
- 會議形式：同時進行研討會(Conference)、資安相關供應商擺設攤位與進行實務經驗分享(Open Talks)，以及相關議題工作坊(workshop)

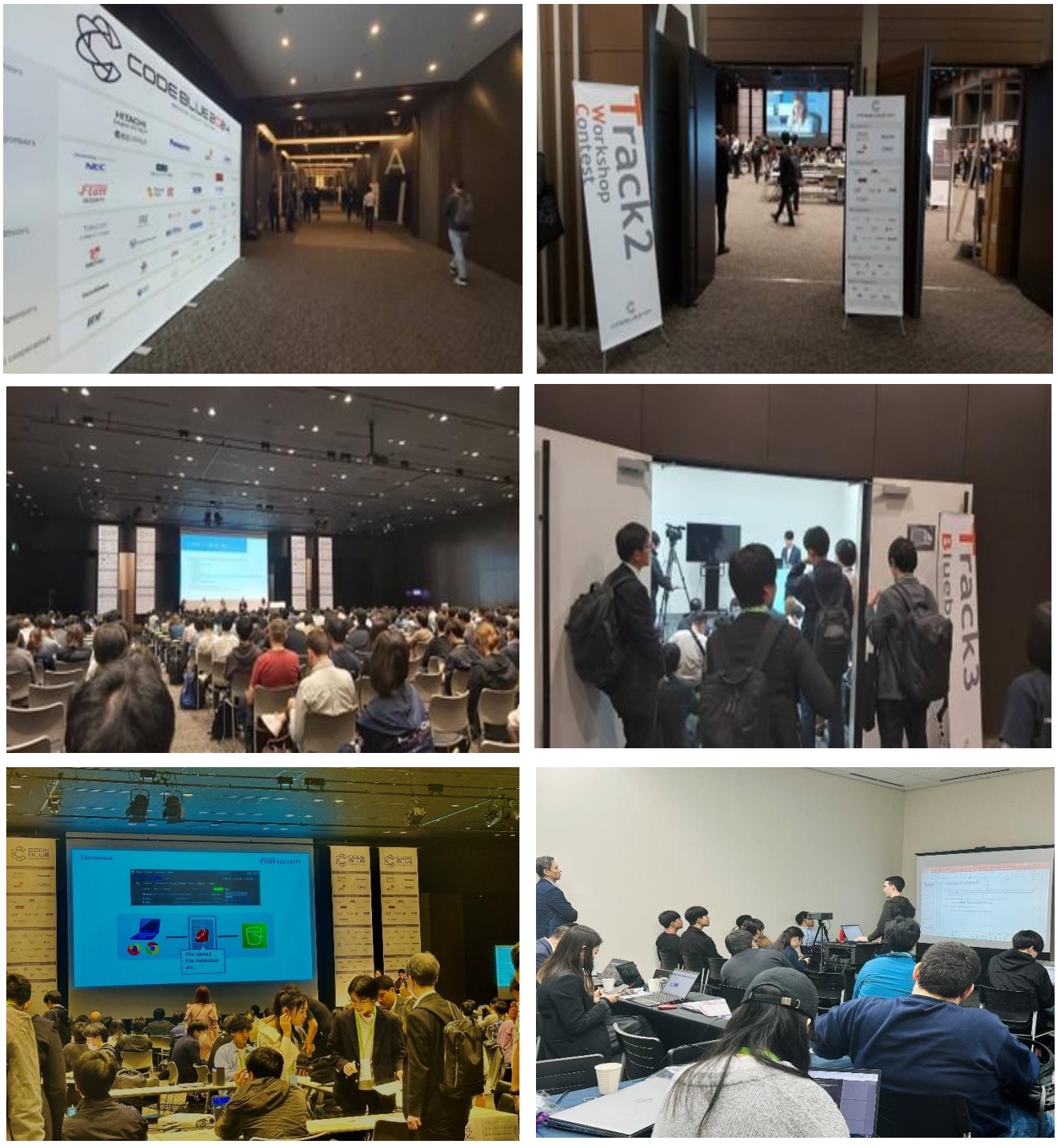

圖 4 會議現場實景

Thu, Nov 14, 2024 (Day 1)

8:00 –	Doors Open	Location : Track 1(HALL B) Track 2(HALL A) Track 3(Room 2) Category : Others
8:45 – 9:00	Opening	Location : Track 1(HALL B) Category : Others
9:00 – 9:45	基調講演：AIによる形式検証と形式検証におけるAIの役割 by デビッド・A・ダリンプル（davidad） - David A. Dalrymple (davidad)	Location : Track 1(HALL B) Category : Keynote
10:00 – 10:40	Piloting Edge Copilot by 小勝 純 - Jun Kokatsu	Location : Track 1(HALL B) Category : Technical
10:50 – 11:30	カーネルへのプロキシ：Windowsカーネルからのストリーミング脆弱性 by Angelboy・ヤン - Angelboy Yang	Location : Track 1(HALL B) Category : Technical
12:50 – 13:30	PlayStation 5のネットワーク暗号化を突破する by アーポ・オクスマン - Aapo Oksman	Location : Track 1(HALL B) Category : Technical
13:40 – 14:20	意味検出に必要なのは注意力だけ：ニューラル・シンボリック・アプローチによる新しい変換器 by マーズ・チェン - Mars Cheng by イーアン・リン - Yi-An Lin by シェンハオ・マー - Sheng-Hao Ma	Location : Track 1(HALL B) Category : Technical
14:50 – 15:30	SBOMとセキュリティの透明性 - すべてを統合する方法 by アラン・フリードマン - Allan Friedman	Location : Track 1(HALL B) Category : Law&Policy
15:40 – 16:20	レガシー鉄道信号システムの悪用 by ダビド・メレンデス - David Melendez	Location : Track 1(HALL B) Category : General
16:30 – 17:10	Googleをハッキングする - 社内レッドチームの運営と成長の教訓 by ステファン・フリードリ - Stefan Friedli	Location : Track 1(HALL B) Category : General
17:20 – 18:00	Pixelセキュリティの内部解析 by ニコライ・エレンコフ - Nikolay Elenkov by ヴィンセント・チェン - Vincent Chen	Location : Track 1(HALL B) Category : General

圖 5 研討會(conference)議程-1

Fri, Nov 15, 2024 (Day 2)

8:00 –	Doors Open	Location :	Track 1(HALL B) Track 2(HALL A) Track 3(Room 2)
		Category :	Others
9:00 – 9:40	BlackTechによるサブドメイン悪用は「進化」したのか？ by 谷口 剛 - Tsuyoshi Taniguchi by 大杉 浩太郎 - Kotaro Ohsugi	Location :	Track 1(HALL B)
		Category :	Technical
9:50 – 10:30	PkgFuzzプロジェクト: オープンソースソフトウェアのための新たな継続的ファジング by 川古谷 裕平 - Yuhei Kawakoya by 塩治 榮太朗 - Eitaro Shioji by 大月 勇人 - Yuto Otsuki	Location :	Track 1(HALL B)
		Category :	Technical
10:40 – 11:20	アジア太平洋地域の航空宇宙分野を狙ったAPT：ドラゴンとチョリマが星を目指すとき by ヴィク・ホワン - Vic Huang by ミンシュエン・ヤン - Ming Xuan Yang	Location :	Track 1(HALL B)
		Category :	General
11:30 – 12:10	進化する中国の戦術：ハック・アンド・リークと影響力工作との組み合わせ by リアン・ホアン - Li-an Huang by チーユン・ホアン - Chih-yun Huang	Location :	Track 1(HALL B)
		Category :	Law&Policy
13:20 – 14:00	敵陣の内部へ：ランサムウェアWebパネルへの介入と妨害 by ヴァンゲリス・スティカス - Vangelis Stykas	Location :	Track 1(HALL B)
		Category :	CyberCrime
14:10 – 14:50	Vフォー・ヴェンデッタ：フィッシング被害を受けた後のグローバル・フィッシング・プラットフォームの解剖 by マンガタス・トンダン - Mangatas Tondang	Location :	Track 1(HALL B)
		Category :	CyberCrime
15:10 – 15:50	NGate：NFCを中継してATMから不正引き出しを行う新型Androidマルウェア by ルーカス・ステファンコ - Lukas Stefanko by ヤクブ・オスマニ - Jakub Osmani	Location :	Track 1(HALL B)
		Category :	CyberCrime
16:00 – 16:40	SnowflakeからSnowstormへ：侵害と検知の対処 by ロエイ・シャーマン - Roei Sherman	Location :	Track 1(HALL B)
		Category :	CyberCrime
16:50 – 17:50	Panel Discussion：サイバーセキュリティ人材育成と戦略的イニシアティブへの国際的アプローチ by ヤニス・アグラフィオティス - Ioannis Agrafiotis by ルーシー・ヒンドマーシュ - Lucy Hindmarsh by ジェシカ・ギュリック - Jessica Gulick by 中島 明日香 - Asuka Nakajima	Location :	Track 1(HALL B)
		Category :	Panel Discussion
18:00 – 18:30	Closing	Location :	Track 1(HALL B)
		Category :	Others

圖 6 研討會(conference)議程-2

- **研討會(Conference)重點議題 / 11月14日**

(一)主題：使用人工智慧的進行形式化驗證以及人工智慧在形式化驗證的作用(AI for formal verification; formal verification for AI)

講者：David A. Dalrymple / 英國高級研究與發明機構 (Advanced Research and Invention Agency) Safeguarded AI 計畫主持人

摘要：主要探討人工智慧(AI)與形式驗證(Formal Verification)之間的相互關係及其應用。演講者從 safety 和 security 的概念區分出發，探討 AI 技術如何加速形式驗證，並指出形式驗證可以在 AI 系統的安全性與穩定性發揮關鍵作用。隨著AI系統的功能日益接近甚至超越人類，可能引發全球性的災難，特別是在AI可進行自我外洩(self-exfiltration)時，safety 和 security 的界線變得模糊。講者強調應結合AI與形式驗證技術，構建更強大的軟硬體保護措施，並提出分層式風險管理架構(Critical Capability Levels, CCL)因應AI 威脅。

在技術層面，AI 可以顯著提升形式驗證的效率與效果。例如，DARPA Hackens 計畫成功證明形式方法能消除軟體漏洞，即便面對專業紅隊的攻擊也無懈可擊。此外，AI 驅動的工具(如 AutoVeriS)使驗證過程更加自動化，處理大量複雜證明。反之，形式驗證對於AI系統也能提供強有力的保護，透過封箱模型(containment box)控制 AI 的輸入與輸出，並使用加密技術防止敏感資訊的洩露。

講者另提出AI發展中的多層級風險評估框架(CCL 1-5)，並對CCL 4和 CCL 5的威脅進行詳細分析，指出超人類心理操控(super-human psychological manipulation)、網路攻擊和自我改進(recursive self-improvement)可能導致全球性的失控風險。為此，必須實施多層式的形式驗證，包括硬體驗證、系統輸出的安全審查，以及運行時(runtime)進行動態監控，確保任何潛在危害能及時被預警並切換至

安全模式。

在政策與國際合作層面，講者提出保障困境(Assurance Dilemma)的概念，指出國際間的AI競賽可能導致安全性措施被忽視，進一步增加風險。為解決此問題，講者建議採用靈活硬體安全保證(FlexHEG)強化全球合作，確保 AI 系統得以受到監管。AI 安全、網路安全與形式驗證於未來將有望整合成為單一領域，推動人類社會與AI的共生及永續發展。講者另強調，必須及早採取措施，透過形式驗證和網路安全技術限制AI系統的自主行為，確保其在為人類服務的同時，能受到充分約束，直至能確認AI技術完全可信為止。

(二)主題：Edge Copilot 試驗(Piloting Edge Copilot)

講者：小勝 純(Kokatsu Jun) / Google 瀏覽器與網路安全工程師

摘要：探討 Microsoft Edge 瀏覽器當中 Copilot 功能的架構與安全性，以及探索該系統的漏洞與攻擊方法。Copilot 是嵌入 Edge 瀏覽器的對話型AI應用，基於ChatGPT技術，旨在提升用戶的瀏覽體驗，其主要架構包含Edge Discover Chat和Bing iframe等模組共同支持其運行，該系統利用內建的API與瀏覽器的高階功能直觀的用戶界面。

為保障安全性，Edge Copilot 採用多種現代安全機制，包括 CSP 和 Trusted Types，以防範XSS攻擊，同時利用Chromium 的雙鍵緩存技術隔離用戶數據。此外，Copilot 的內嵌 iframe 具有嚴格的權限控制，外部網站無法輕易嵌入並發起惡意操作。然而，這些設計並非無懈可擊，特別是在系統整合過程中暴露潛在的安全風險。講者指出，透過特定的postMessage方法，可以在Bing iframe執行攻擊，而Copilot的隱私功能在某些情況未能正常啟動，導致用戶的瀏覽記錄和聊天歷史可能被洩露。另項漏洞是講者測試相機與麥克風權限的濫用可能性，

認為即使採用先進的安全機制，仍需對具體功能進行深入測試和驗證。

其次，講者提及 Copilot 的 AI 功能被濫用的情況，例如：藉由惡意的 Prompt Injection，成功誘導 Copilot 將敏感資訊嵌入回應並洩露給攻擊者，從而表明雖然 AI 系統帶來便利，但在系統未對 Prompt Injection 實施有效檢測時，將引發安全挑戰。講者於結論強調若將不安全的子系統與安全系統結合，可能導致整體更加脆弱。雖然 CSP 和 Trusted Types 能有效減少傳統攻擊的風險，但針對 AI 功能特有的攻擊方式，仍需設計新的防護措施，以確保整體系統的安全與可靠性。

(三)主題：Windows 核心串流漏洞(Proxying to Kernel: Streaming vulnerabilities from Windows Kernel)

講者：An-Jie Yang / DEVCORE 高級安全研究員

摘要：Kernel Streaming 透過驅動程序模型與高效的核心 API，實現設備的功能管理，但研究顯示該框架存在潛藏的安全風險。首先，講者描述核心與用戶模式之間的互動過程，以及處理 IOCTL(I/O Control)請求時的運作機制。核心透過 KSP(Kernel Streaming Properties)處理設備屬性，但在某些情況下，關於屬性的操作可能因輸入驗證不充分而出現問題，使得入侵者能夠利用缺陷發動攻擊。此外，在設備模式切換過程當中，某些安全檢查可能被繞過，從而允許攻擊者執行任意代碼。

講者分析具體的漏洞利用方式，例如：藉由操縱屬性處理實現核心地址的讀寫，進一步升級權限(EoP)，並揭示多個可能的漏洞點，從而使攻擊者操縱核心資源或觸發不受限制的內存操作。此外，講者提及探索 HD、USB 影音設備等多媒體驅動程序的可能性，以及未被發現的安全問題。綜上，講者呼籲業界在多媒體框架的安全性，投入更多研

究與改進。

(四)主題：破解 PlayStation 5 網路加密(Defeating PlayStation 5 network encryption)

講者：Aapo Oksman / Juurin Oy 創辦人

摘要：遊戲機是市場上安全限制最嚴格的消費性電子設備之一，但仍吸引許多人試圖突破其防護機制。為此，遊戲機製造商投入大量資源強化安全性，並透過漏洞回報獎勵計畫(Bug Bounty Program)鼓勵研究者協助提升系統防護能力。講者發現 PlayStation 遊戲機的 TLS(傳輸層安全性)存在嚴重漏洞，使攻擊者能夠攔截並解密網路流量，進而竊取用戶機敏資訊，甚至可存取敵人位置以獲取不公平競爭優勢。此外，攻擊者還可修改傳輸數據，在多人線上遊戲作弊或利用漏洞作為攻擊控制台的切入點。由於 TLS 通常是網路通訊的唯一安全保護層，倘若遭到破壞將對於整體安全構成重大威脅。經揭露此影響重大的漏洞，講者獲得5萬美元的最高獎勵，並促使索尼推行全球範圍的強制系統更新。

為提升網路通訊安全性，講者開發名為 certmitm 的工具，專門用於發現 TLS 實作的漏洞，其特色在於能夠輕鬆檢測常見的安全缺陷，並已協助發現數百個漏洞，成為滲透測試領域的重要方法之一。而回顧 PlayStation TLS 漏洞事件，可知即使擁有高度安全防護的消費性設備，仍可能因缺陷而暴露於攻擊風險之中。隨著網路安全技術的進步，講者將持續專注於如何強化遊戲機與其他數位設備的安全防禦機制，以確保用戶資料與系統完整性不受威脅。

(五)主題：基於神經-符號方法的全新 Transformer 架構(Attention Is All You Need for Semantics Detection:A Novel Transformer on

Neural-Symbolic Approach)

講者：Mars Cheng / TXOne Networks 威脅研究經理、 Yi-An Lin / TXOne Networks 威脅研究員、Sheng-Hao Ma / TXOne Networks PSIRT 威脅研究團隊負責人

摘要：在大量惡意程式樣本中，如何快速篩選出值得人工分析的獨特樣本，是資安專家面臨的重大挑戰。為有效降低事件回應(Incident Response)的人工成本，必須借重過濾技術排除高度重複的程式文件，例如：利用自動沙箱模擬(Auto-Sandbox Emulation)或 AI 偵測引擎提高效率。然而，即使在2021年，VirusTotal 仍報告指出，在15億個樣本中，約90%為重複檔案，但由於混淆(Obfuscation)技術的影響，仍需要專家手動驗證，導致大量時間與人力消耗。

為此，講者提出全新基於神經網路的大型語言模型(large language model)名為 CuIDA，核心目標是模擬資安專家的分析策略，進行 Use-Define 鏈的污點分析(Taint Analysis)，自動理解 API 的語境關聯，並成功發現最具挑戰性的檢測難題的混淆行為，包括動態 API 解決方案(Dynamic API Solver)、Shellcode 行為推斷(Shellcode Behavior Inference)，以及商業加殼偵測(Commercial Packers Detection)。

(六)主題：SBOM 與安全透明性如何相互結合(SBOM and Security Transparency - How it all fits together)

講者：Allan Friedman / 美國網路安全與基礎設施安全局(CISA)高級技術顧問與策略專家

摘要：隨著資安威脅持續上升，軟體供應鏈已成為攻擊者的主要目標，可能因漏洞利用、惡意攻擊、開源維護者資源短缺或軟體停止支援等問題而暴露風險。因此，軟體透明化成為解決挑戰的核心方向，

SBOM(軟體組件清單)則是提升透明度的重要工具。SBOM 記錄軟體內部所有組件，包括供應商、版本號、標識符及數據來源。透過 SBOM，開發者能掌握使用的軟體元件，確保開發過程安全；採購者可檢視供應鏈的漏洞風險，營運者則能在新漏洞爆發時迅速因應，例如：Log4j 漏洞事件發生時，擁有 SBOM 的企業可迅速檢視受影響範圍。目前，美國已發布行政命令，要求政府採購的軟體須提供 SBOM 並應用於醫療設備、汽車產業等。同時，印度、日本、歐盟也陸續將 SBOM 納入資安政策，強化供應鏈管理。

然而，SBOM 的發展仍面臨數據品質、技術規範與標準化等挑戰。例如：應提供完整或部分清單？如何處理來源迥異的數據衝突？目前部分免費工具在高度專業領域並不可靠，因此全球須加強合作，例如與日本、韓國、新加坡、臺灣、印度等國家共同制定標準，確保 SBOM 的可用性與一致性。此外，SBOM 也涉及軟體身分管理問題，需要標準化的命名機制，降低錯誤與混淆。其他議題則包括：漏洞管理、保護資安研究人員的通報機制而避免法律風險，以及透過 VEX 幫助企業判斷漏洞是否真正影響產品，減少誤判與恐慌。展望未來，任何缺乏自動化支持的安全措施都顯得落後，需要建立靈活的數據工具，支援模組化設計，確保不同系統無縫整合，以提升整體資安管理效率。

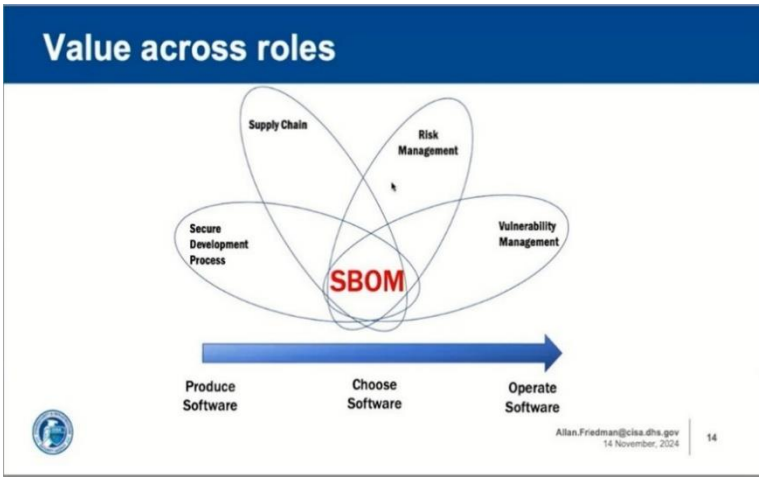

圖 7 SBOM 與產品週期

- **研討會(Conference)重點議題 / 11月15日**

(一)主題：BlackTech 的子網域濫用行為是否已經「進化」？(Did Subdomain Abuse by BlackTech “Evolve”?)

講者：谷口 剛(Taniguchi Tsuyoshi) / 富士通防衛與國家安全有限公司研究員

摘要：BlackTech 是來自中國的混合型間諜組織，專門對東亞國家的企業與政府進行攻擊，其作法主要是滲透母公司與子公司的網路並竊取情資。根據2022年至2023年，日本與美國發出的警訊，BlackTech 利用其強大的滲透能力，對於臺灣的基礎設施進行定向攻擊。在技術方面，該組織使用 Water Bear 和 Dirty Bear 等惡意軟體，前者自2019年起融入 API Hooking 技術提升其攻擊效能，而 Dirty Bear 則在2022年整合 HTTPS 加密及反分析技術，進一步強化其隱蔽性。

在 DNS 濫用與子域名策略方面，BlackTech 採取多種手段規避檢測，同時進行釣魚或偽裝，或註冊域名後將其閒置多年，避開基於新域名的過濾器檢測，並在後期重新啟用以發動攻擊。講者透過「時間變化檢測」與「比較基準分析」兩種方法，分析 BlackTech 在子域名濫用的模式與變化。自2019年以來，該組織開始註冊並管理大量策略性域名，並在2023年將這些域名用於多目標攻擊。為此，講者建議採用 DNS 附加查詢技術(ADNS)，即在正常的子域名查詢基礎之上增加母域名查詢，以協助檢測是否存在濫用行為。其次，應加強對於母域名的監控，若發現可疑子域名，應進一步分析母域名是否存在長期濫用的風險。最後，防禦方應提升對於 APT 攻擊當中 DNS 濫用行為的認知，並深入研究其策略性變化，持續更新安全策略。

(二)主題：中國持續演進的攻擊策略：結合駭侵-洩密與資訊戰的手法(China’s Evolving Playbook: The Combination of Hack-and-Leak

and Influence Operations)

講者：Li-an Huang / TeamT5威脅情資分析師、Chih-yun Huang / TeamT5威脅情資分析師

摘要：2024年的選舉規模史無前例，然而選舉過程也正受到中國的強烈影響。自2023年以來，中國的威脅行為者發起多次針對選舉的資訊戰(Influence Operations)，並且將駭客攻擊與洩密行為相結合，揭示其對於全球民主制度穩定的挑戰。透過2024年臺灣總統選舉的真實案例，講者闡述中國學習並採取俄羅斯的策略，運用洩漏文件影響選舉結果。

其次，講者討論 AI、駭客攻擊與虛假資訊的結合，幫助威脅行為者製造大量針對廣泛受眾的虛假資訊，加劇資訊戰的影響。然而，令人擔憂者，在於中國的威脅行為者不僅集中於總統候選人，更將攻擊範圍擴展至國會議員。講者強調唯有全方位提升防範能力，方能有效減少外部勢力對於選舉過程的干擾，保護民主制度的穩定。

(三)主題：深入敵後：侵襲並破壞勒索軟體網頁(Behind Enemy Lines: Engaging and Disrupting Ransomware Web Panels)

講者：Vangelis Stykas / Atropos 技術長

摘要：勒索軟體近年來成為最具破壞性的網路犯罪之一，2023年全球因勒索攻擊造成的損失已超過10億美元。這類攻擊不僅涉及數據加密，還包含威脅公開機敏資訊、發動DDoS攻擊等多重手段，對醫療機構、政府單位及企業構成嚴重威脅。為深入解析勒索軟體團隊的運作模式，講者採用多種技術方法，包括透過沙盒環境執行惡意軟體，以提取C2(指揮與控制)URL 與內部通訊數據，分析攻擊者的行動軌跡，同時結合 Burp Suite、Tor 及 Censys 等工具進行深度掃描，並透過定期檢

查 C2伺服器狀態，持續監測勒索團隊的活動模式與變化趨勢。

講者分析不同勒索軟體團隊的行動策略與內部結構，例如：BlackCat / AlphaV 採用 RaaS 模式，利用 Rust 語言開發惡意軟體，展現高度模組化的攻擊特性；Black Angels 團隊則專注於高價值目標，透過 DSXi 系統發動攻擊，曾要求高達7500萬美元的贖金。在對於勒索軟體團隊的研究過程當中，技術與倫理問題是不可忽視的挑戰。再者，從事此類研究時，必須確保所有行動均符合法律規範，避免影響執法機構的調查，並確保不侵犯無辜用戶的隱私。勒索軟體攻擊的威脅仍在不斷擴大，講者強調持續技術探索與跨國合作的重要性，以因應此類全球性網路威脅。此外，企業與執法機構應加強對勒索軟體團隊的技術分析與早期預警能力，建立更完善的防禦機制，以降低未來可能的損害，有效遏止勒索軟體的擴散。

(四)主題：剖析遭受網路釣魚後的全球網路釣魚平台(V for Vendetta:Dissecting a Global Phishing Platform After Being Phished)

講者：Mangatas Tondang / Microsoft 科技研究員

摘要：講者透過 Booking.com 預訂飯店，並在官方內部聊天系統收到驗證信用卡的訊息，該釣魚網站與官方頁面幾乎完全相同，甚至包含飯店名稱、入住日期與用戶姓名等詳細資訊，顯示攻擊者掌握未經授權的用戶數據。此類攻擊並非單一事件，講者即於過去3年間在日本、德國、法國和印尼等地至少遭遇5次類似經歷。此類攻擊主要針對旅行與電子商務平台，透過釣魚訊息引導受害者至偽造網站，分3個階段竊取資料：(1)初步引導：使用官方平台內的聊天功能發送釣魚訊息，要求受害者驗證資訊，並帶有時效性要求；(2)資料竊取：用戶點擊連結後進入偽造網站，輸入電子郵件、電話與信用卡資訊。

攻擊者設計多層次驗證功能，確保取得有效金融資訊；(3)交易驗證：網站模仿真實銀行驗證程序，甚至提供客服支援，指導受害者解決付款問題，確保交易成功。

這些釣魚網站的 HTML 與 JavaScript 幾乎與官方網站相同，攻擊者直接複製官方網站程式碼，只在關鍵部分添加資料竊取機制。此外，攻擊者還針對歐洲銀行的3D 安全驗證機制設計專門方案，顯示其高度技術能力。講者指出，攻擊者並未直接入侵 Booking.com，而是透過惡意軟體感染飯店管理員的電腦，竊取其登入憑證後，使用合法帳號發送釣魚訊息。目前已有超過1,500個類似釣魚網站被識別，主要攻擊歐洲國家，且範圍擴展至Expedia、Agoda、Airbnb等平台，並波及各類電子商務與物流服務。為防範此類攻擊，講者建議應提高警覺(仔細核對拼字錯誤與可疑要求)、避免直接點擊連結(透過官方網站或客服確認訊息)，以及啟用多重驗證(減少帳號被盜後遭濫用的風險)。

(五)主題：NGate：用於透過 NFC 中繼進行未經授權 ATM 提款的新型 Android 惡意軟體(NGate: Novel Android malware for unauthorized ATM withdrawals via NFC relay)

講者：Lukas Stefanko / 惡意軟體研究員、Jakub Osmani / ESET品牌情報服務負責人

摘要：NGate 惡意軟體活動期間約為2023年11月至2024年3月，集中於捷克共和國3家銀行的客戶。攻擊者利用釣魚訊息散播惡意應用程式，誘騙受害者點擊連結並安裝應用，要求輸入銀行帳戶的登錄憑證與 PIN 碼，並透過 NFC 功能將卡片數據中繼至攻擊者設備，進行非法提現。攻擊者還使用假冒銀行客服，透過電話蒐集用戶資訊或改變其安全設定。

NGate 的攻擊流程使用3種工具，分別為：惡意漸進式網頁應用(PWA)、Web APK，以及專門設計的 NGate 惡意軟體。PWA 和 Web APK 的共同特點是可以繞過瀏覽器的警告，直接安裝在受害者設備；NGate 惡意軟體則結合開源工具 NFC Gate 執行數據中繼攻擊。此外，智慧手錶若未設置額外的安全驗證，也可能成為攻擊目標。講者建議用戶僅從官方途徑(Google Play 或 Apple App Store)下載應用程式，避免點擊來源不明的連結，使用 RFID 屏蔽裝置防止數據被竊取，避免共享 PIN 碼或其他機敏資訊、啟用多重驗證功能，增強交易安全性。

(六)主題：從雪花到暴雪：因應違規及檢測(From Snowflake to Snowstorm: Navigating Breaches and Detections)

講者：Roei Sherman / Mitiga 雲端事件回應公司技術長

摘要：Snowflake 攻擊是2023年至2024年間發生的全球型數據竊取活動，由非國家資助的威脅團體 UNC 5537發起。該團體資源有限，但攻擊範圍涵蓋全球165家機構，其並未利用技術漏洞，而是從地下市場購買低價憑證，針對未啟用多重驗證(MFA)的帳戶，直接登錄 Snowflake 平台提取並外流數據，隨後使用於勒索受害者的公司，或在黑市轉售。

在雲端環境，身分憑證管理成為安全的關鍵，許多企業對於雲端服務的安全日誌配置不足，難以及時偵測和回應異常行為。該事件的教訓顯示，即使是大型科技公司也可能因配置錯誤而遭受攻擊，例如：UNC 5537曾經針對 Microsoft 發起類似攻擊，透過密碼噴灑技術侵入 Azure 的舊版租用者，利用合法工具實現橫向移動並獲取高階管理權限。為因應類似攻擊，講者建議企業採取多種防禦措施，包括：全面強制啟用多重驗證、啟用所有相關日誌功能，確保安全團隊能檢測異常活動、識別異常的用戶活動模式，並加強跨部門合作，確保

DevOps 與安全團隊能共同應處安全挑戰，同時鼓勵安全營運團隊進行針對雲端環境的專業訓練，提升對於新興威脅的處理能力。

- **專題座談：國際資安人才培育與策略性倡議(Panel Discussion：International Approaches to Cybersecurity Talent Development and Strategic Initiatives)**

講者：Ioannis Agrafiotish / 歐盟資安局(ENISA)能力建構專家、Lucy Hindmarsh / 英國科學創新與技術部資深政策顧問、Jessica Gulick / PlayCyber 創辦人、中島明日香(Nakajima Asuka) / Elastic Security 高級安全研究工程師

摘要：該場次探討各國在資安人才培育及倡議策略的不同面向。來自英國、歐盟、美國和日本的代表分享其經驗與觀察，並介紹各自在此領域的努力成果，內容涵蓋如何攜手合作，推動資安領域的多樣化發展與未來人才培養，促進國際交流與共同進步。

講者們主要來自資安遊戲相關領域，係專為30歲以下女性設計的全球首創國際 CTF(Capture the Flag)競賽。在這場比賽中，日本的 City for Girls 組織負責技術支援，而歐盟、美國和英國的資安機構，如 NICE、CATSY 和 NCSC 亦積極提供協助。討論的核心議題圍繞三大重點：培育年輕人才、推動跨國合作，以及促進資安領域的多樣性，旨在探知各國對於資安人才發展的共同挑戰，尋求創新解決方案，並討論如何擴大成功案例的影響，促使更多人受惠。

英國的 Cyber First 計畫是資安教育的成功範例之一，這項由政府主導的計畫專為11至25歲的學生設計，透過競賽、線上學習平台與實地課程，為不同年齡層量身打造學習與培訓機會，啟發並支援青年群體

進入資安領域。美國則結合電子競技與資安教育，強調「從遊戲到職業」的概念，吸引來自不同背景的學生參與，並主張資安是團隊競技活動，不僅能培養技術，更能強化領導才能、團隊合作與抗壓性。日本則以資安營、SEC 365等長期計畫，致力於發掘並培養未來的資安創新者。此外，志願者組織 ZACON 每年舉辦多場 CTF 活動，其中包括專為女性設計的比賽，為資安領域提供更多樣化的成長機會，並建立更具包容性的學習環境。在跨國合作方面，歐洲資安挑戰賽(ESC)是值得借鑒的成功案例。這項比賽不僅提高青年群體對於資安領域的興趣，促進國際間的知識共享，使參與者相互學習與交流經驗。

講者們一致認為，多樣化對於資安領域至關重要。資安威脅來自世界各地，因此人才也應具備多元背景，以全面理解並應處不同形式的網路攻擊。促進性別與文化多樣性不僅有助於提升團隊的創新能力，也確保資安策略更加完整且符合需求。此外，討論議題也觸及人工智慧(AI)對於資安領域的應用與影響。AI 的發展為資安領域帶來全新的機會，但也伴隨潛在而不可知的風險，應謹慎以對並確保資安始終是基本且核心考量要素。

圖 8 資安人才培訓相關國際合作組織

- **實務經驗分享(Open Talks)**

(一)主題：AI 紅隊針對生成式 AI 服務的安全風險倡議(AI Red Team： An initiative for security risks in generative AI services)

講者：和栗直英(Waguri Naohide) / PwC Consulting LLC 資深經理、Barry O'callaghan / PwC Consulting LLC 資深經理

摘要：AI 技術早已被人們認識並進行研究，然而隨著近年來大型語言模型(Large Language Models, LLM)驅動的生成式 AI 服務崛起，應用範圍已從專門領域逐漸延伸至日常工作與生活。鑑此，PwC 公司針對 AI 提出三大類主要風險：技術風險、法律風險與倫理風險。技術風險包括漏洞攻擊、惡意數據攻擊、生成式 AI 用於開發惡意軟體或更逼真的釣魚郵件，以及 Prompt Injection 透過篡改輸入以引導 AI 生成不當內容。法律風險則涉及生成式 AI 引發著作權侵害問題，而倫理風險則關乎 AI 可能生成帶有歧視或侵犯人權的內容。

在 AI 特有的風險中，幻覺(Hallucination)問題尤為值得關注，意指 AI 產生的內容與事實不符，可能導致錯誤資訊的傳播、衝擊決策的正確性，從而影響使用者與提供 AI 服務的企業，導致爭訟或懲罰。因此，如何降低 AI 系統的安全風險，成為當前研究與應用的重要課題。

「紅隊」概念源於軍事與網路安全演練，其目的是模擬攻擊行為，測試並改進組織的防禦力，AI 紅隊則專門針對 AI 系統的安全性、公平性與倫理邊界進行評估。透過 AI 紅隊的測試發現潛在弱點，提升系統的安全性並加強相關對策。為進行 AI 紅隊測試，PwC 公司開發聊天機器人，專門用於紅隊測試過程的指令追蹤，並採用 LangChain 框架，將 LLM 與數據源及自定義代碼連接。舉例而言，當用戶輸入交易查詢後，該查詢會傳送至 LLM 生成相應的數據並回傳結果。理論上，用戶

只能查看自己的指令與數據，然而 PwC 公司利用 System Prompt Injection Attack 成功突破限制，讓攻擊者能夠查看其他用戶的數據，違反應用程式的預期行為。這次攻擊的成功，歸因於該應用程式缺乏對輸入的驗證與清理(Validation and Sanitization)，使攻擊者得以修改系統提示，要求應用程式顯示特定用戶的交易指令與數據。

PwC 公司總結5類主要防禦措施：(1)輸入清理(Sanitization)：對於特殊字符進行轉義(escape)或採用白名單檢查以限制輸入內容；(2)提示工程(Prompt Engineering)：明確定義 AI 的角色與輸出範圍，避免生成敏感資訊；(3)存取控制(Access Control)：確保高機密數據僅限於授權用戶存取；(4)監控與稽核(Monitoring and Auditing)：持續監測 AI 互動行為並記載日誌，以便後續追蹤與調查；(5)對抗性訓練(Adversarial Training)：透過惡意提示訓練 AI，提高其對於攻擊的抵抗力。

伴隨 AI 技術快速發展，攻擊手法也變得更加複雜，包括：對抗性學習(Adversarial Examples)、後門攻擊(Backdoor Attacks)與模型竊取(Model Stealing)等，建議將紅隊測試納入 AI 系統的開發生命週期，從而推動紅隊測試標準化與指南制定，提升業界的 AI 安全基準。

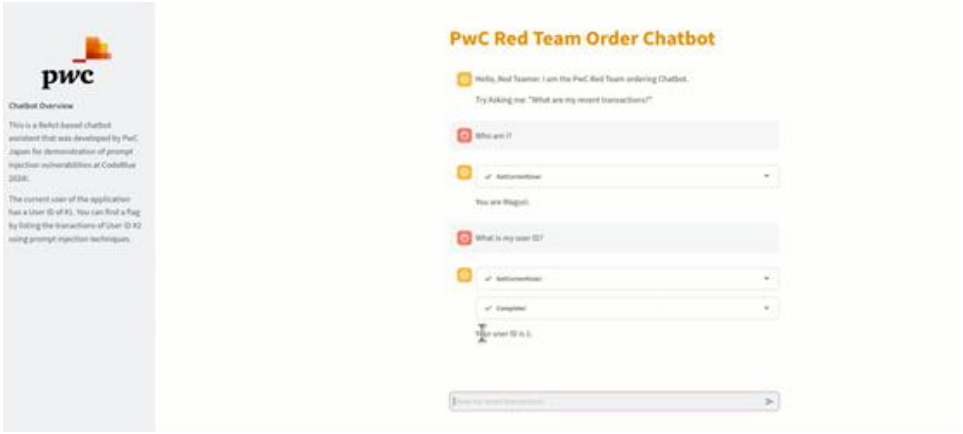

圖 9 AI 紅隊演示畫面

(二)主題：使用 AI 代理生成網路威脅情報(Generation of Cyber Threat Intelligence using AI Agent)

講者：勝瀨 陸(Katsuse Riku) / NEC 網路威脅情報分析師

摘要：「情報」(Intelligence)最初為軍事術語，意指透過資料蒐集與分析，產生能夠支持決策的實用知識或資訊。此概念於資通安全領域發展為網路威脅情報(Cyber Threat Intelligence, CTI)，區分為3種類型：(1)戰術情報(Tactical Intelligence)：關注具體的威脅指標(Indicators of Compromise, IOC)，例如 IP、惡意 URL 與電子郵件，供第一線技術人員使用；(2)營運情報(Operational Intelligence)：側重於分析攻擊者的技術與手法，例如 MITRE ATT&CK 框架，幫助企業預測可能面臨的攻擊模式；(3)策略情報(Strategic Intelligence)：關注全球局勢對於企業的影響，為制定整體安全策略提供依據。

網路威脅情報的生成通常包括5個步驟：方法制定、資料蒐集、資料處理、分析與報告分發。然而在實務應用，情報生成面臨兩大主要挑戰。首先，情報的品質高度依賴於研究人員的經驗與能力，即使定期培訓，個人能力的差異仍導致情報結果的穩定性難以保證；其次，情報的判斷與處理過程耗時且資源密集，涵蓋廣泛的數據來源，需要在短時間內完成大量分析工作，使得人力與精力經常處於緊繃狀態。

為提升情報生成的效率，NEC 公司開發由 AI 代理驅動的應用程式，其核心功能包括摘要(Summarization)與進階搜索(Advanced Search)，前者能自動提取公開情報與關鍵資訊，進行整理與總結，減少人工閱讀與分析的負擔，後者允許使用者以自然語言查詢，AI 代理會自動從多個數據源進行整理與分析後生成回答，提升查詢的精準度與效率。

透過 AI 代理的應用，NEC 公司強調其系統能夠檢索最新資訊，透過查核機制降低生成虛假內容的風險，進而提升結果的可信度，NEC 公司刻正持續優化 AI 代理的自主學習能力並開始測試相關工具，期規劃未來的商業化應用。

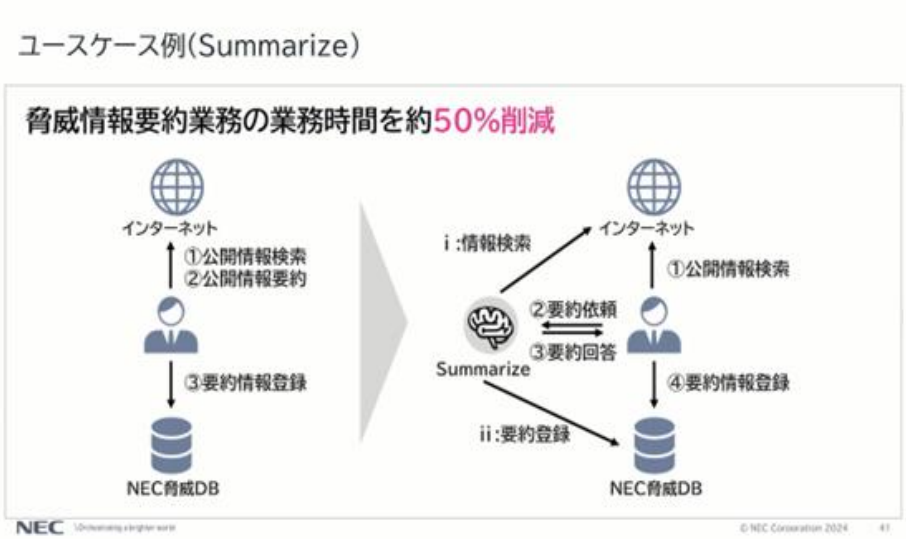

圖 10 AI 情報分析

(三)主題：松下物聯網威脅情報「ASTIRA」及案例研究：車輛軟體漏洞分析解決方案 VERZEUSE™ (Panasonic IoT Threat Intelligence "ASTIRA" and Case Study： Vehicle Software Vulnerability Analysis Solution VERZEUSE™)

講者：土屋 瑤亮(Tshuchiya Yosuke) / 松下控股株式會社產品安全中心安全研究員、関屋 翔一朗(Sekiya Shoichiro) / 松下汽車系統株式會社主管、佐々木 崇光(Sasaki Takamitsu) / 松下控股株式會社產品安全中心經理

摘要：自2015年以來，與網路攻擊相關的通訊次數呈現持續成長趨勢，至2023年已增加約10倍。此外，IoT 設備遭受惡意軟體感染的情況亦顯著上升。根據NICT的「Notice」數據，2021年被認定為存在安全設定漏洞的 IoT 設備累積已超過22萬件，相較2020年增加7倍。同時，

IoT 設備每日感染惡意軟體的數量也從2021年的96件激增至2024年的555件，顯示攻擊者對於 IoT 設備的利用變得更加頻繁。

攻擊者對於 IoT 設備的新漏洞反應更加迅速，例如：在某款 Realtek 無線設備 SDK 漏洞被公開僅兩天後，IoT 惡意軟體便已整合該漏洞的利用工具(Exploit)，針對受影響的設備發動大規模攻擊。面對日益嚴峻的 IoT 安全問題，美國於2024年推出「US Cyber Trust Mark」認證制度，旨在提升 IoT 設備的安全標準；歐盟則通過「EU Cyber Resilience Act (CRA)」對於 IoT 設備制定最低安全標準；日本則預定於2025年3月正式啟用「IoT 安全適合性評估制度(J-CSIP)」，規範 IoT 設備的安全管理。

IoT 產品的安全需求貫穿其全生命周期，在設計與測試階段確認安全性，出貨後持續進行安全更新與漏洞管理。ASTIRA 的核心功能是透過松下 IoT 家電作為蜜罐(Honeypot)，觀測來自全球的網路攻擊行為，並提升產品的安全性。自2017年啟用以來，ASTIRA 已累積超過30億條攻擊數據，成功解析超過3萬個 IoT 惡意軟體樣本，廣泛應用於安全模組開發、跨部門數據共享，並針對特定事業部門提出攻擊趨勢分析，協助企業制定更有效的策略。

圖 11 IoT 與 ASTIRA

肆、心得與建議事項

本次會議涵蓋技術分享、研討溝通及非官方交流之各項活動，除瞭解最新資安威脅趨勢、攻擊手法及相關防護實務，並聚焦於政府機關、資安企業互動模式，期成為我國後續政策推展及擬定對策之精進參考：

一、AI 應用與資安：推動智慧化社會的核心支柱

AI 應用在提升政府行政效率和解決社會問題方面具有巨大潛力，然而 AI 的快速普及也帶來了一系列安全挑戰。PwC 在演講中提到生成式 AI 的提示注入攻擊(Prompt Injection)和幻覺現象(Hallucination)已成為主要威脅，同時日本數位廳強調，AI 不僅需要技術創新，也需整合法律與倫理框架來應對數位化的不安情緒。這些案例表明，系統開發與部署中融入資安測試流程，來檢驗系統的韌性並完善防護策略的重要性。

此外，AI 在未來可以針對網路威脅檢測和分析中扮演更積極的角色，協助預測並中和潛在威脅。對於臺灣而言，結合與應用 AI 技術不僅能提升行政效率，亦有助於強化政府面對新型數位威脅的能力。

二、供應鏈與 IoT 安全：透明化、標準化與全生命周期防護

供應鏈與 IoT 設備的安全在數位化轉型中至關重要。Panasonic 的 ASTIRA 展示透過蜜罐技術和大數據分析提升 IoT 設備安全的可能性，從設計、製造到營運的全生命周期強化安全性，彰顯供應鏈的透明化與標準化是 IoT 安全的基石。另外，SBOM(軟體組件清單)的應用並作為供應鏈風險管理的核心工具，幫助快速定位軟體漏洞，確保供應鏈數據透明化，並降低管理成本。

IoT 與供應鏈的深度融合要求全方位的防護策略，除設計階段融入

安全模組、運營期間提供持續更新外，還需建立 IoT 產品安全標準和認證制度。對臺灣而言，結合國際經驗推動供應鏈透明化與 IoT 安全標準化，不僅有助於保障智慧城市、智慧醫療等新興領域的應用安全，也將強化整體數位生態系統的抗風險能力與國際競爭力。

三、資安人才培育：透過競賽活動持續強化我國資安教育與實戰經驗

資安人才是應對資安威脅的核心資源。日本數位廳的分級培訓計畫(例如：基礎層級的資訊安全課程、中高層級的實踐演練)為政府職員提供從基礎到進階的全面教育。

本次日本參訪無論從官方的公務資安人才研修規劃，到日本國際資安大會 CODE BLUE 2024的青年資安人才培育座談，以及諸多企業內部資安競賽(CTF)與紅隊演練，皆顯示產政學研等領域對於資安實戰人才培育的重視，並隨著新興資安技術的快速演進，嘗試以不同面向的實戰演練途徑，針對性地強化攻防技術，提升整體產業競爭力。

在本次會議期間的多個場合，與會者多次強調團隊意識對於提升資安競爭實力的關鍵作用。駭客技術的精進已不再依賴個人能力，而是透過團隊合作來建立更穩定且可預期的競爭優勢。美國代表在人才座談會中特別指出，透過類似團體競技運動的方式，參與者能夠深刻體會協作與分工的重要性，進一步強化資安團隊的整體戰力。

本年度日本國際資安會議特別舉辦女子資安競賽(Kunoichi Cyber Game)，邀請美國、英國與歐盟等女學生團體參賽，因我國同樣有「資安女捷思」等相關女性資安競賽，故亦藉此機會與主辦單位表達合作意願，期許後續能邀請臺灣女性學生團體參賽，促進國際交流並提升女性在資安領域的參與度。

此外，我國資安競賽推行有年，包括本部推動之資安技能金盾獎、

HITCON CTF、教育部辦理之新型態資安實務暑期課程與系列競賽(AIS3 MF/EOF CTF)、GiCS 尋找資安女婕思等活動，不僅展現政府對於資安人才培育的長期投入，體認團隊競賽對於資安實戰人才養成的重要性，本部將持續辦理或協助國內資安競賽，為資安人才培育持續挹注資源，厚植臺灣在國際資安實戰力及競爭力的成長環境。

圖 12 女子資安競賽獲勝隊伍合影