出國報告（出國類別：不定期會議）

2025 日本 IT Week 資安產業拓銷

單位名稱：數位發展部數位產業署
姓名職稱：杜欣怡 簡任技正
盛郁雁 專案規劃師

派赴國家：日本(東京)
出國期間：114 年 4 月 22 日~114 年 4 月 25 日
報告日期：114 年 7 月 3 日

摘要

數位發展部數位產業署(以下簡稱本署)為推動臺灣資安產業發展，協助資安產業拓銷國際市場，於 114 年 4 月 23 日至 25 日與臺灣資安大聯盟成員「臺灣資訊安全協會(以下簡稱 TWISA)」合作，匯集 9 家臺灣資安業者共同參展「Japan IT Week 2025 Spring」，並以「Cybersecurity Team Taiwan」為主題設立臺灣資安館，展現臺灣自主研發解決方案；本次訪日拓銷行程中，亦同步拜會日本經濟產業省所屬「獨立行政法人情報處理推進機構(以下簡稱 IPA)」以及日本伊藤忠集團旗下大型系統整合商伊藤忠科技解決方案公司(以下簡稱 CTC)，針對半導體設備資安標準(SEMI E187)及後量子密碼(PQC)資安議題進行深度交流。

本次「臺灣資安館」開幕式由我國駐日代表處李逸洋大使及 TWISA 理事長涂睿珅開幕致詞，並邀請日本防衛協會等貴賓出席，展現我國政府對於日本資安產業市場重視，參展廠商包含智慧資安、關楗、眾至資訊、杜浦、全景、優內控、如梭、奧義智慧及叡廷等 9 家公司，針對零信任架構、AI 防禦、供應鏈資安、工控防護與後量子密碼等技術領域，展現我國多元資安技術量能。

為協助廠商拓銷，本署亦與 TWISA 合作，帶領 10 家臺灣資安廠商前往拜會 CTC。除了向 CTC 介紹半導體設備資安標準 SEMI E187 內容與推動現況外，也由臺灣資安廠商分享協助設備廠商導入 SEMI E187 之實務經驗，並展示資安相關創新解決方案，凸顯臺灣在半導體產業及各產業中資安的豐富實力與技術實踐能力，以促成臺日雙邊合作機會並帶動資安產業發展。CTC 對於我國推動 SEMI E187 之合規檢核表、解決方案及檢測對象提出詢問，後續將持續追蹤 CTC 需求及媒合成果。

此外，為了解日本資安推動作法，本署及 PQC 聯盟代表（匯智安全鄭嘉信總經理）一同拜訪 IPA，介紹本署透過成立 PQC-CIA 推動資安業者布局 PQC 遷移商機的做法。另經 IPA 分享，日方刻正以「密碼演算法評鑑」及「推薦清單」等方式以協助日本各政府單位了解資安風險，惟 PQC 議題尚未有明確策略與推動做法，對於我國廠商已有 PQC 相關解決方案印象深刻，後續待日本有具體政策時，期可協助台廠佈局日本市場。

在物聯網資安標章的推動上，IPA 分享日本今年三月發布之 JC-STAR IOT 產品資安標章，共分四星等級，1-2 星係自評、3-4 星則需由第三方認證，惟實驗室規範尚未推出，後續將持續與 IPA 交流，探討雙邊互相承認可行性或協助我國實驗室

成為合格實驗室進行討論。

最後，前往拜訪工研院日本辦公室就臺日技術合作經驗進行交流，本署分享因台積電於熊本設廠，期待由 SEMI E187 標準帶動之資安需求，可作為臺灣資安業者的拓銷機會，可共同思考如何創造臺日在資安技術上的合作機會 ，工研院日本辦公室表示過去曾協助臺灣區電機電子工業同業公會(TEEMA)、TWISA 等公協會在日本拓銷，本署將持續透過工研院日本辦公室協助關注日本半導體供應鏈之資安需求。

未來本署將持續與相關公協會合作，建立自主資安研發能量、擴大資安產業規模與國際接軌等策略支持我國資安產業發展。

目錄

圖目錄

壹、目的

為推動臺灣資安產業發展，協助資安產業拓銷國際市場，本署積極協助業者了解各國政府的資安發展政策，並爭取臺灣資安業者在國際重要展會曝光的機會，同時也籌組拓銷團，積極拜會國際知名系統整合業者，推動臺灣資安業者與國際知名系統整合業者合作的機會。本次出國目的，包含：

一、了解日本資安政策

拜訪日本經濟產業省所屬「獨立行政法人情報處理推進機構(IPA)」，了解日本在物聯網設備資安標章的推動進度，並交流在半導體資安標準，如 SEMI E187 及 PQC 後量子加解密資安等議題。

二、打造臺灣資安館參與日本最大 IT 展會 2025 IT Week Spring

為加速提升臺灣資安業者國際知名度，與 TWISA 臺灣資訊安全協會合作，匯集 9 家臺灣資安業者共同參展「2025 IT Week Spring」，並以「Cybersecurity Team Taiwan」為主題設立臺灣資安館，展現臺灣自主研發解決方案。

三、協助臺灣資安業者爭取與國際知名資安系統整合業者合作機會

帶領 10 家臺灣資安廠商前往拜會 CTC。除了向 CTC 介紹半導體設備資安標準 SEMI E187 內容與推動現況外，也由臺灣資安廠商分享協助設備廠商導入 SEMI E187 之實務經驗，並分享資安相關創新解決方案，展現臺灣在半導體產業及各產業中資安的豐富實力與技術實踐能力，期待吸引更多商業合作機會，以帶動資安產業發展。

貳、行程

日期	時間	行程
4/22 (二)	06:50-07:00	華航櫃台報到
	09:00-13:10	台北松山機場→日本東京羽田機場 (華航 CI220)
	13:20-14:20	出關及領行李
	14:20-15:00	搭車移動至飯店
	15:20-15:50	移動至高輪 Gateway
	16:00-17:30	參觀「高輪 Gateway City」
	17:30-18:00	返回住宿飯店
4/23 (三)	09:00-10:00	飯店移動至日本科學未來館 Miraikan
	10:00-12:00	參觀日本科學未來館 Miraikan
	12:15-13:00	移動至東京國際展示場(東京 Big Sight)
	13:30-14:30	參加 IT Week Cybersecurity Team Taiwan 開幕式
	14:30-16:00	導覽臺灣資安館及參觀雲服務館
	16:00-17:00	參觀展場攤位
	17:00-18:00	移動至住宿飯店
4/24 (四)	0820-0850	從飯店移動至伊藤忠科技解決方案公司(CTC)
	0910-1115	拜會伊藤忠科技解決方案公司(CTC)
	1115-1200	從 CTC 移動至澀谷機器人餐廳 Pepper Parlor
	1200-1520	午餐+觀摩機器人餐廳
	1520-1600	移動至獨立行政法人情報處理推進機構(IPA)
	1600-1700	拜會獨立行政法人情報處理推進機構(IPA)
	1700-1740	返回住宿飯店
4/25 (五)	1000-1030	從飯店移動至工研院日本辦公室
	1030-1130	與工研院日本辦公室進行交流活動
	1130-1200	從工研院日本辦公室移動至東京羽田機場
	1200-1435	機場報到與準備出境
	1430-1655	日本東京羽田機場→台北松山機場(華航 CI221)
	1655-	入境、賦歸

參、團員名單

一、數位發展部

	姓名	單位	職稱
1	杜欣怡	數位發展部數位產業署	簡任技正
2	盛郁雁	數位發展部數位產業署	專案規劃師

二、隨隊成員

	姓名	單位	職稱
1	雷穎傑	工業技術研究院資訊與通訊研究所	技術副組長
2	張懷文	工業技術研究院資訊與通訊研究所	專案人員
3	蕭榮興	資訊工業策進會資安科技研究所	主任

肆、執行過程及內容

一、拜訪「高輪 Gateway City」

（一）日期：2025 年 04 月 22 日(二)

（二）地點：東京都江東區青海 2 丁目 3-6

（三）參訪摘要：

高輪 Gateway City 是由 JR 東日本（東日本旅客鐵道）主導的大型都市再開發計畫，地點位於東京港區高輪地區，緊鄰 2020 年啟用的高輪 Gateway 車站。這項開發案是「品川站與田町站之間」舊車廠地帶重生的核心項目。高輪 Gateway City 的開發主題是：「100 年後依然豐富人心的都市」，目標是打造一座集智慧科技、永續設計、文化交流與歷史保留於一體的未來型都市實驗場域。

圖 1：高輪 Gateway City 基地

資料來源：本計畫整理

高輪 Gateway City 是日本推動智慧城市（Smart City） 理念的標竿之一，導入多種機器人與自動化技術， JR 東日本計劃在這座未來城市中部署約 50 台各類型機器人，包括送餐、保全、清潔，以及最新的館內物流機器人，打造人機協作的創新生活空間。在這次參訪中，已經可以看到即將搬遷至「THE LINKPILLAR 1」北樓的 KDDI，在公司入口處進行將實施的清潔機器人、安保機器人、送貨機器人等的服務。KDDI 也與 JR 東日本合作開發一個平台，連結列車運行數據、配送機器人、Suica 卡等資訊，開發多功能的應用 App，可以查詢即時列車資訊、預訂活動、網路下單、餐點外賣以及查看商店和設施的資訊。而在「Gateway Park」周圍提供自動駕駛移動車輛「iino」，任何人都可以自由上下車。最多可容納五人。民眾可以每小時 5 公里的步行速度體驗這座城市。另外在北樓和南樓之間的大樓梯旁，展示了 ASKA 公司製造的可在陸地和空中使用的飛行汽車縮小比例模型，未來計劃利用這款四人座飛行汽車實現旅遊服務。

圖 2：高輪 Gateway City－相關科技設施與服務

資料來源：本計畫整理

高輪 Gateway City 站內也設有 Touch to Go 無人便利商店，其合作開發單位包括日本 FamilyMart、KDDI、ANA FESTA、JR 東日本的零售事業 JR-Cross 與滑雪場 GALA 等。這家無人便利商店天花板上的攝影機和貨架上的感應器會記錄消費者拾取的物品，當消費者帶著欲結帳的商品走到自動收銀機前面時，商品和價格會顯示在監視器螢幕上。如果顯示的商品內容有誤，消費者可以在確認付款前手動調整。另外，由於消費者在拾取物品的同時就開始被便利商店的系統紀錄下來（並非要到收銀時才確認），所以商店系統會自動識別出消費者是否改變主意並退回物品。結帳時除了 Suica 等智慧票卡外，也可以用信用卡或現金，全程無店員。

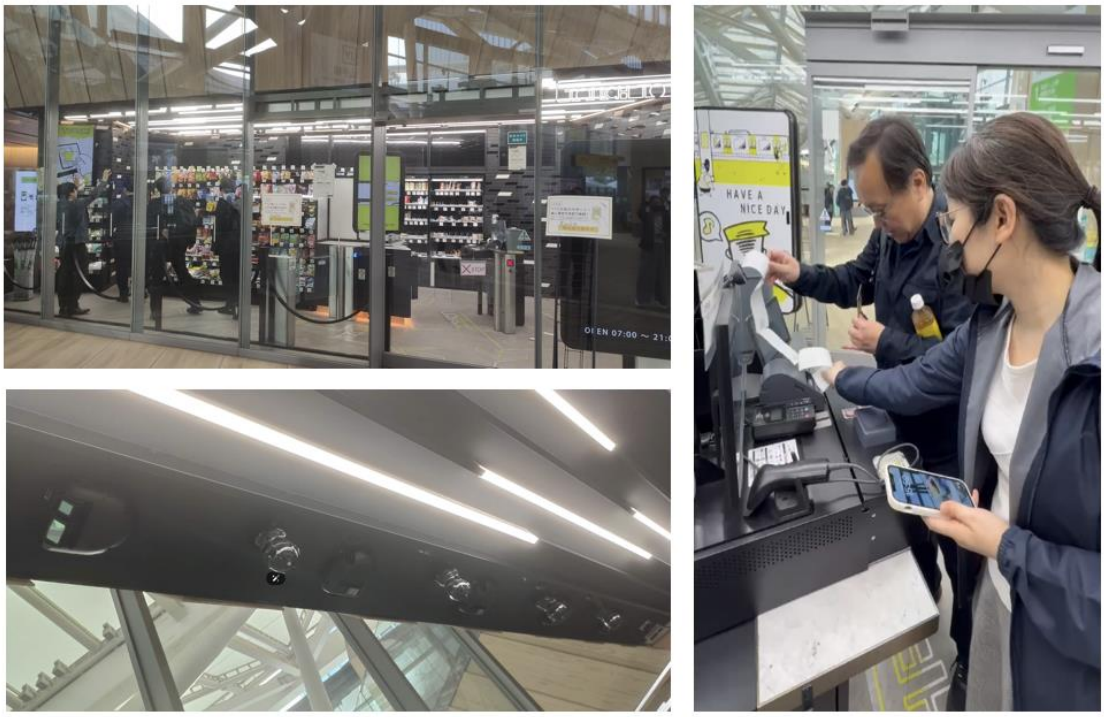


圖 3：高輪 Gateway City－Touch to Go 無人便利商店

資料來源：本計畫整理

高輪 Gateway City 作為日本新型智慧城市典範，其科技整合模式與資安治理架構，可為推動數位轉型提供以下啟發，特別是場域營運者可建立跨域協作平台，本次可以看到高輪以開放式數據平台串聯交通、能源、醫療等系統，顯示場域實證關鍵角色是「生態系整合者」，制定統一數據標準與介接規範，破除跨平台間的資料孤島。而在資安部分，建議可建立數位分身（Digital Twin）監控機制，例如透過即時模擬城市運作的模式，建立常態化風險預警系統，透過虛實互動偵測基礎設施潛在漏洞，此外，在資料蒐集階段即應實施匿名化或去識別化處理，並將隱私始於設計（Privacy by design）列為公共服務數位化的必要條件。

二、觀摩「日本科學未來館」

（一）日期：日期：2025 年 04 月 23 日(三)

（二）地點：東京都江東區青海 2 丁目 3-6

（三）日本科學未來館簡介

日本科學未來館坐落於東京台場核心區域，由日本國立研究開發法人科學技術振興機構（JST）直接運營。該館成立於 2001 年 7 月，扣合日本「科技立國」策略轉型與配合日本「科學技術基本計畫」第二期（2001-2005）政策，旨在透過提升全民科學素養重振國家創新動能，突破「失落的十年」經濟困境。有別於傳統博物館單向展示模式，該館定位為「社會共創型科學平台」，核心使命在於建構科學與社會的對話介面，聚焦太空探索、全球環境、生命科學及機器人技術四大主題。

（四）常設展區的深度解析

在常設展區裡，有許多與機器人相關的策展內容，以開放給民眾直接進行互動，包含：

1.「你好！機器人」科技劇場

此展區以「連結人類社會與科技發展的前瞻性對話」為核心理念，徹底顛覆靜態陳列模式。展場設計成動態互動場域，配置三款具突破性技術的機器人：

(1) Talking Bones：是一款設計用來講故事的互動機器人，透過刻意設計語言停頓與記憶缺失特性，觸發人類對「不完美智能體」的情感共鳴。當機器人對參觀者經歷表現興趣時，會建立共同成就感的心理連結機制。參訪團隊實際測試，Talking Bones 是現場少數可以透過對話（日文）互動的機器人，但互動不是非常的流暢，與一般人型機器人被設計精準達成某項功能的模式非常不同，Talking Bones 有著日本動漫卡通人物迷糊可愛的特性，常有歪著頭說：「嗯……

然後是什麼來著？」的舉動，引導互動者不由自主地想幫它接話，體驗時真的感受到了一種「被需要」的感覺，反而貼近人與人互動的真實模式。

圖 4：日本科學未來館－Talking Bones 聊天機器人

資料來源：本計畫整理

(2) Keparan：日本科學未來館內的原創夥伴機器人，設計理念為「大家一起培養」，意在讓參訪者與機器人共同成長，思考未來人與機器人的關係，Keparan 搭載 30 組精密馬達，模擬生物生長曲線實現雙足動態平衡，使 Keparan 能夠完成雙足行走、單腳站立及節奏感強烈且流暢的舞蹈動作。這種多自由度的機械結構結合高精度的動作控制系統，讓 Keparan 的動作不僅靈活自然，還能與音樂節奏完美同步，呈現出極具生命力的舞蹈表演。其情感表達系統能依據觀眾反應，自主調整動作複雜度與情緒反饋強度。參訪團隊實際測試，當靠近 Keparan，它會自主調整姿態，而舉起展區準備的看板，Keparan 會表現出喜歡或厭惡的反應，讓人感覺它真的有自己的脾氣和喜好並以跳舞方式回應，透過 30 多個馬達協調產生的流暢動作，配合輕快的音樂，可以表現出雙足行走、單腳站立，不像傳統人形機器人那樣呆板。

圖 5：日本科學未來館－Keparan 夥伴機器人

資料來源：本計畫整理

(3) Aibo 伴侶機器狗：採用「不完美生命體」設計哲學，背部觸覺感應器觸發踏地動作與 OLED 心形眼睛，忽視狀態下則啟動低鳴懲戒機制，重構人機情感依附邊界。參訪團隊實際測試，Aibo 可從遠方觀察到呼叫它們的手勢，緩慢的移動到參訪團隊前面，不斷的以鼻子觸摸團員的手，而在撫摸其背部時，Aibo 也會慢慢的轉換為坐姿，呈現依順的樣態，另外，不同的 Aibo 之間也會互相靠近，模擬小狗互相磨蹭的動作，顯示和平友好的態度，與實際人類與小狗互動的方式極為類似。

圖 6：日本科學未來館－Aibo 伴侶機器狗

資料來源：本計畫整理

展區另有解說機器人整合多層次技術，我們從現場展示的圖表中作(見下圖)可以觀察到，包含：外觀採用動態適應型仿生毛皮包覆，眼部配置多點觸控 OLED 微型顯示器。內部架構包含頭部中央處理單元、胸部馬達驅動模組（控制 30 組電動馬達）、傾斜感測器（精度±0.05°）與三軸腳底力量傳感器，散熱系統採用鋁合金翅片與微型渦輪風扇協同運。

圖 7：日本科學未來館－機器人展區關鍵技術說明

資料來源：本計畫整理

根據本次觀察日本科學未來館的機器人展示，其關鍵技術展現了新一代人形機器人領域的核心突破，特別是人工智慧結合機器人的關鍵技術，使得新一代機器人具備更擬真的能力，其技術分析如下：

(1) 語音識別與合成：機器人需要理解參觀者的問題並以語音回應，展場中的機器人多已可以透過語音互動，這部分涉及自然語言處理（Natural Language Processing, NLP）中的語音識別（Automatic Speech Recognition, ASR）和語音合成（Text-To-Speech, TTS）技術，這些技術的發展目前都與人工智慧技術脫不了關係，在 NLP 中，電腦需要對語言進行斷詞、詞性標記、句法分析和語義理解等，以便有效處理和理解文本，大型語言模型（Large language model, LLM）可以應用在各種 NLP 任務中，包含：語言生成、語言理解、依文本內容進行情感分析或主題分類、自動偵測拼字錯誤或語法錯誤等，這些都對於語音識別與合成能力有具體的提升。

(2) 骨骼結構與運動控制：機器人具有類似人類的骨骼結構，這需要精密的機械設計和運動控制算法，以實現自然的動作，而人工智慧技術可以協助發展更有效的機器人運動控制系統，包含提高神經信號解碼能力，提早預測使用者肢體運動意圖，降低外骨骼響應延遲時間，而電子皮膚檢測到意外碰撞時，AI 控制系統可提早預測因應，達成安全交互運作。新一代的機器人也開始採用大型行為模型（Large Behavior Model, LBM）整合物理規律與任務知識庫，使機器人更具備動態場景的任務應變能力。

(3) 視覺運算技術：機器人可能需要識別參觀者的位置、姿態或表情，以便進行互動，其關鍵是影像識別和圖像處理運算技術，目前卷積神經網絡（Convolutional Neural Network, CNN） 已經逐漸成為支援物體識別主流技術，能從複雜場景中精準定位目標，如果使用專用

AI 晶片（如 Google TPU、NVIDIA Jetson），可降低識別延遲至毫秒級，使機器人能在資源受限環境執行即時視覺任務。

(4) 人工智慧對話系統：機器人需要理解問題並生成有意義的回答，這需要使用更先進的深度學習模型，對機器人對話系統的影響主要在提升語言理解能力、增強生成回應的自然度和擴展系統的多功能性，特別是大型語言模型，能從龐大且多樣化的語料中自動學習語言規律，實現對自然語言的深度理解與生成，理解上下文和語境，生成流暢且符合語境的回應，提升人機交互的自然度和親和力。而深度學習模型不僅處理文字，還能整合影像、音訊等多模態數據，擴展對話系統的應用場景，例如，結合視覺輔助的對話機器人能根據用戶上傳的圖片進行分析和回應，不過深度學習模型對硬體資源需求高，需結合專用 AI 晶片（如 NVIDIA RTX GPU）和優化技術，才能實現低延遲的對話運算。

(5) 感測器技術：新一代機器人多可配備多種感測器（如觸覺感測器、距離感測器等）來感知環境，而人工智慧技術使機器人能夠將來自多種感測器（如壓力、應力、影像、環境感測器等）的異構數據進行融合分析，自動識別物體形狀、大小及環境變化，顯著提升感知的精度與可靠性，特別是機器學習演算法，能直接在感測層面進行數據篩選、雜訊過濾和特徵提取，提升數據處理效率，支持機器人自主判斷與行動。

整體來說，人工智慧技術雖已逐步解決了機器人的關鍵技術瓶頸，但仍有許多挑戰需要逐步解決，包含對控制器的即時算力和軟硬體協同的嚴苛要求，算力瓶頸限制了即時反應能力和普及應用，因此短期內難以在單台機器人上達成運算能力，目前多需結合雲端與邊緣運算架構輔助。AI 模型的性能依賴大量高質量數據，數據收集、標註成本高，且模

型在實際環境中的即時適應性仍有限。而人型機器人追求通用性，能執行多種任務，系統整合複雜度遠超過傳統的工業機器人，這些都需要我國未來持續投入資源進行研發。

2. 「七彩城」共生社會模擬

日本科學未來館常態展中的「七彩城」展館係透過建構一個機器人活躍的未來城市情境，將體驗者置入虛擬與實體交織的敘事脈絡中。展覽的故事情境以「共生社會」為核心，模擬一座名為七彩城的都市，其中機器人已融入日常生活的各個層面，從街道清潔、醫療照護到藝術創作，機器人不再僅是工具，而是具備自主學習能力的社會成員。本展覽是一個體驗型展覽，每組體驗者都會提供平板終端，體驗者以藉助這些設備探索在展示空間中再現的「未來城市」，這片虛擬的空間，有餐廳、便利商店、公寓、花屋、快遞員，體驗者會在不同關卡與不同的機器人互動，依據互動時取得線索，尋找下一個場景與角色，最終達成任務，在過程中，體驗者沈浸在與機器人共生的世界中，逐步體驗並認可未來共生的社會，此設計試圖打破傳統人機對立的框架，引導體驗者重新定位「以人類中心」的思維模式。

「七彩城」的核心技術是互動式沉浸體驗技術，讓參觀者以遊戲化的方式參與未來城市的探索，體驗機器人技術如何融入日常生活，提升參觀的沉浸感與教育效果。互動式體驗強調參觀者與展品或機器人之間的雙向交流，如與人形機器人的對話、模擬電腦訊號傳遞的操作體驗，甚至是模擬衰老視力與聽力的感官體驗，通過即時反饋增強參與感與學習效果。

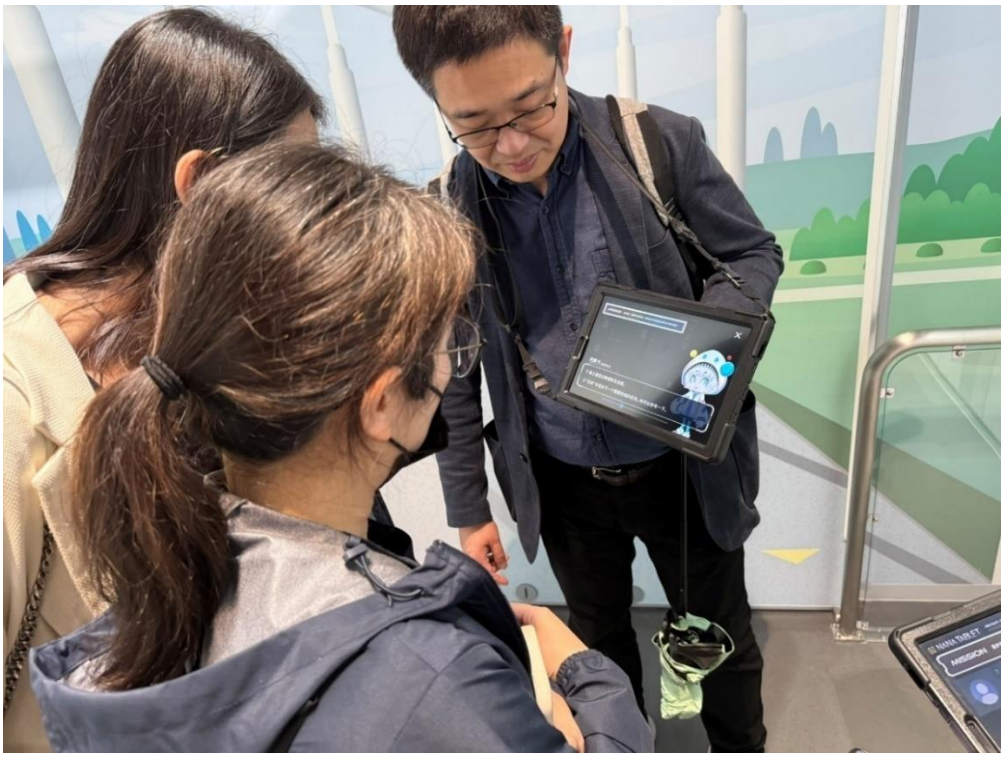


圖 8：日本科學未來館－七彩館互動體驗

資料來源：本計畫整理

圖 9：日本科學未來館－於七彩館以以平板與場域進行互動

資料來源：本計畫整理

圖 10：日本科學未來館－於七彩館以平板與場內機器人互動

資料來源：本計畫整理

過去虛擬實境技術（Virtual Reality, VR）與擴增實境技術（Augmented Reality, AR）在沉浸體驗中扮演重要的角色，VR 通過頭戴式顯示器

（Head-Mounted Display, HMD）將使用者帶入一個完全由電腦生成的虛擬環境，讓使用者感官被全方位包圍，結合視覺、聽覺甚至觸覺反饋，VR 讓使用者能在虛擬世界中自由移動與操作物件，適合用於訓練模擬、娛樂遊戲及設計創作等需要高度專注的場景；AR 將數位資訊（影像、文字、聲音）疊加到使用者的現實世界視野中，增強對現實環境的感知，根據使用者位置和環境動態調整內容，AR 利用感測器和相機辨識現實場景，根據使用者位置和環境動態調整內容，VR、AR 如能結合自然語言技術處理、視覺識別與行為決策，使機器人能理解環境與人類需求，實現自主行動與協助，可增強互動的自然性和智慧性，即能使得互動式沉浸體驗的效果更好。

圖 11：日本科學未來館－七彩城機器人互動展示館全景

資料來源：本計畫整理

3. 「量子電腦迪斯可」展館

2025 年是量子力學誕生 100 週年，聯合國教科文組織將其定為「國際量子科學技術年」，因此這次的展覽以過去到未來的計算機為概念，讓體驗者能夠了解這些艱深的計算原理，特別是最新的量子電腦，它很巧妙的以 DJ 混音的概念來解釋量子電腦的運算方式，以同時播放多首

歌曲來呈現「量子疊加」計算能力，以改變透過耳機聽到的聲音的位置來呈現「量子相位」，以實現改變音量等操作「量子機率幅度」。另也透過四部短片解釋量子電腦的工作原理，包含什麼是量子位元（量子電腦中最小的資訊單位）、五種實際應用方法（超導、半導體、中性原子、離子阱和光）以及糾錯的工作原理。而日本研發的 144 量子位元晶片，通常在研究機構之外很難見到，也是首次在本展覽中公開亮相。

圖 12：日本科學未來館－日本最新的 144 量子位元晶片展品

資料來源：本計畫整理

為了讓參觀者能夠以科普的方式了解量子電腦，展館中以多媒體形式循環播放短片，內容介紹量子計算機的原理與發展情況，幫助參觀者理解量子位元的基本概念及其在量子計算中的作用，量子計算機如何利用量子力學原理（如量子疊加和量子糾纏）實現強大計算能力，以及量子位元（qubit）作為量子信息的最小單位的基本介紹；影片中透過音樂混音的比喻（如同時播放多首樂曲、調節音量等）形象

化量子態的疊加和相位等量子特性，使抽象的量子概念更易理解。這些影片配合展覽中的 DJ 互動體驗、漫畫、電影和遊戲，形成多感官的學習環境，讓參觀者能從視覺、聽覺和操作中深入體會量子計算的核心原理及其科技意義，其簡易、科普的方式很值得台灣在量子電腦認知宣導方法上作為參考。

展館中也建立了量子疊加的體驗區，參觀者可透過將手邊的模塊擺放至圓形溝槽中，對《威風堂堂》和帕赫貝爾的《卡農》等 8 首經典曲目進行混音創作，模塊及其組合在量子計算中有特定含義，例如同時播放多首樂曲表現「量子疊加」的特性，透過耳機調整聲音方位（如左右環繞效果）來表現「相位」的特性，以控制音量大小（振幅愈大，音量愈強）來表現「機率振幅」的特性，都是試圖讓參觀者容易了解這些艱深的技術特徵。這種透過生活中的音樂來類比量子電腦的運作，其創意也很值得參考。

（五）營運模式啟示

日本科學未來館成功實踐三大創新策略：科研機構成果落地、常設公民科學論壇促進 AI 倫理對話，以及串聯東大、索尼、本田等產學研網絡。其「科技劇場」概念將博物館角色從知識儲藏庫轉型為社會創新實驗場。

三、打造臺灣資安館參與 IT Week 春季展

（一）2025 IT Week Spring 簡介

1. 展覽期間：114 年 4 月 23 日至 25 日
2. 展覽時間：每日 10:00~18:00
3. 展會地點：東京 Big Sight（Ariake 有明 3-21-1）
4. 主辦單位：RX Japan 株式會社

5. 展會介紹

2025 IT Week Spring 是日本乃至亞洲最具規模與影響力的綜合性 IT 展覽會，由 RX Japan 株式會社主辦，已有超過 30 年的歷史。該展會每年春季於東京國際展示場（Tokyo Big Sight）舉行，吸引來自全球的 IT 企業、專業人士及買家參與。2025 年展會共有 1,033 家參展商，吸引 57,802 名專業觀眾參與。展會涵蓋以下主要 IT 領域：

(1) 軟體與應用程式開發：展示最新的軟體開發工具與應用程式。

(2) 嵌入式系統與邊緣運算：探討嵌入式技術與邊緣運算的應用。

(3) 資訊安全：涵蓋資安防護、零信任架構、後量子密碼等。

(4) 雲端運算與資料中心：展示雲端解決方案與資料中心技術。

(5) 物聯網（IoT）與 M2M 解決方案：探討物聯網與機器對機器通訊的應用。

(6) AI 與業務自動化：展示人工智慧在業務流程中的應用。

(7) 數位行銷與電子商務：涵蓋數位行銷策略與電子商務解決方案。

(8) 商店 IT 解決方案：探討零售業的 IT 應用與創新。

此外，展會期間還舉辦多場高品質的研討會，深入探討 IT、AI、數位轉型、銷售策略和電子商務等最新趨勢。鑑於 IT Week 春季展為日本重要 IT 展會，本署率領我國資安業者組團參展，希望能藉此推廣臺灣資安解決方案至國際市場，同時建立與日本企業的交流與合作機會。

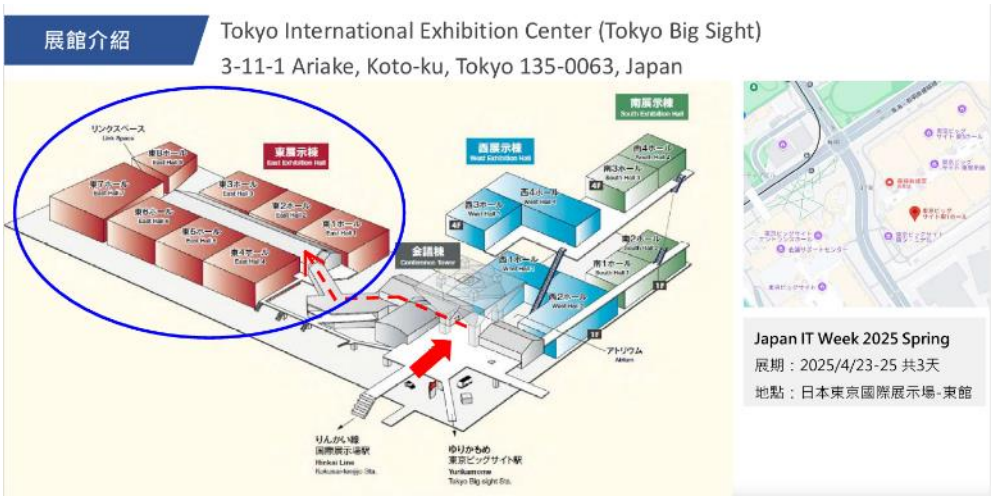


圖 13：IT Week 春季展區位置圖

資料來源：本計畫整理

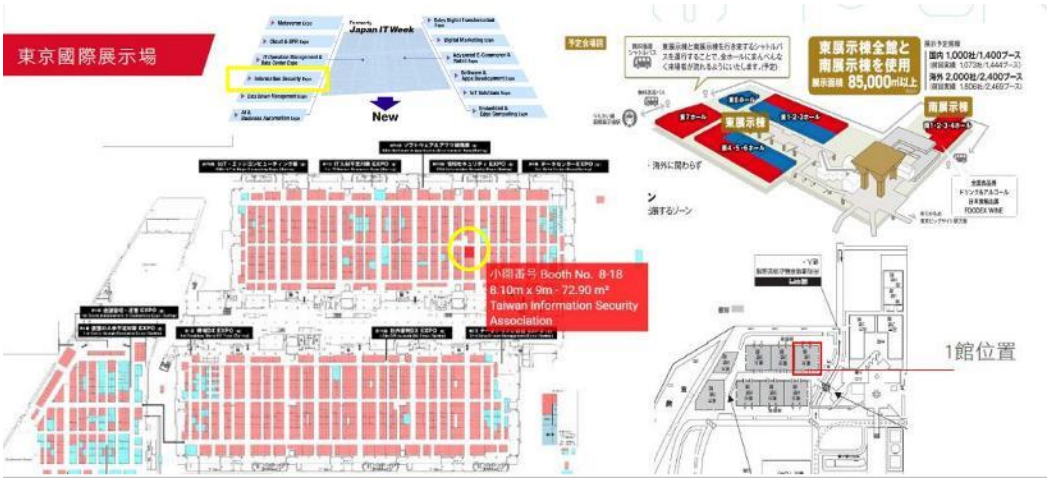


圖 14：臺灣資安館展區位置圖

資料來源：本計畫整理

（二）臺灣資安館 Cybersecurity Team Taiwan

1. 展館名稱：Cybersecurity Team Taiwan
2. 展覽期間：114 年 4 月 23 日至 25 日
3. 展館地點：2025 IT Week Spring 東 1 館 8-18 號
4. 展館介紹：

為推動臺灣資安產業發展，協助資安產業拓銷國際市場，本署於 114 年 4 月 23 日至 25 日與臺灣資安大聯盟成員「臺灣資訊安全協會(TWISA)」合作，匯集包含智慧資安、關楗、眾至資訊、杜浦、全景、優內控、如梭、奧義智慧及叡廷等 9 家公司，共同參展「2025 IT Week Spring」，並以「Cybersecurity Team Taiwan」為主題設立臺灣資安館，展現臺灣自主研發解決方案。

圖 15：以 Cybersecurity Team Taiwan 為主題之牆面設計

資料來源：本計畫整理

館內除各家業者皆有獨立展示區域，亦設有舞台專區，於展覽第一天以「SEMI E187」、「PQC」、「零信任」等主題發表演講，分享臺灣於上述議題上推動經驗與成果。展覽第二天及第三天，舞台區也安排資安廠商進行示範展示（PITCH）演講活動，由各業者輪流發表自家產品與解決方案實績，除增加曝光機會外，也透過與現場參與者進行互動以提高媒合機會；現場並另設有媒合專區，讓參展廠商可以即時與潛在客戶進行進一步的商談。

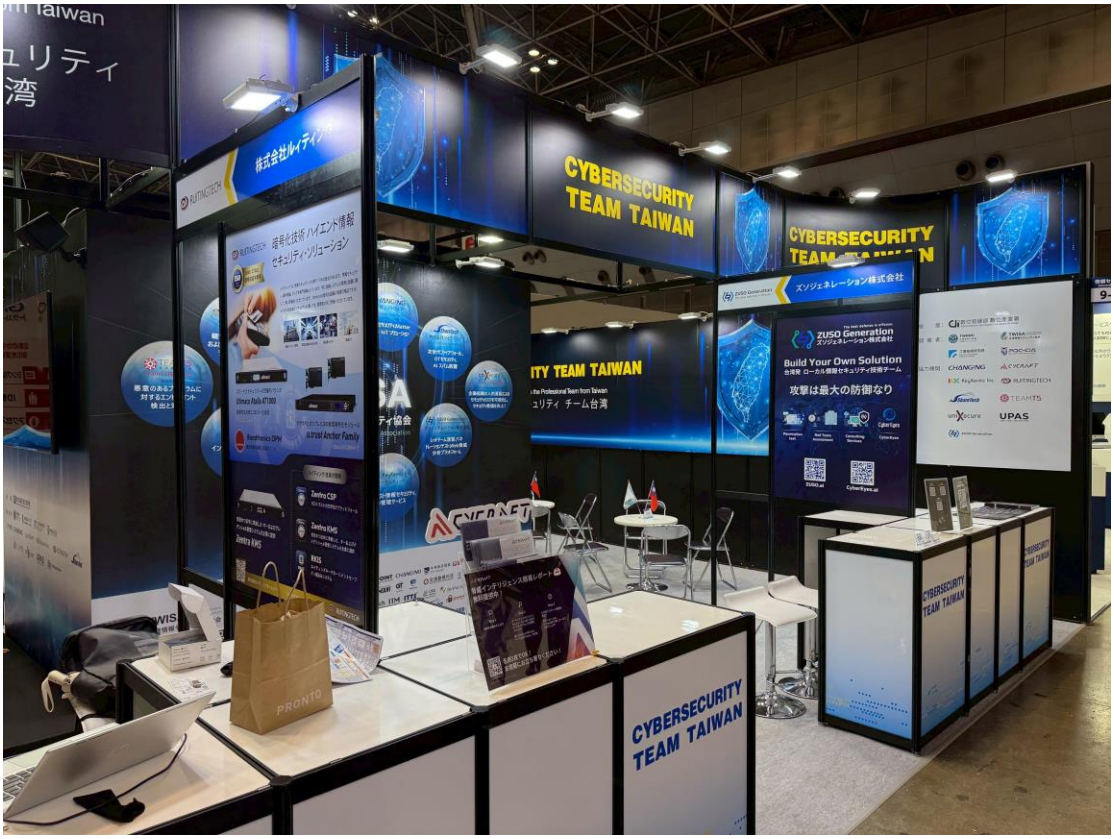


圖 16：臺灣資安館現場照片

資料來源：本計畫整理

5. 參與廠商介紹

(1) 奧義智慧 crycraft：奧義智慧科技 (CyCraft Technology)公司成立於 2017 年，是一家專注於 AI 自動化技術的資安科技公司，研發自動化威脅曝險管理平台「XCockpit」，整合「端點偵測與回應」、「身份攻擊面管理」、「外部攻擊面管理」三大防禦構面，提供一站式的全方位自動化資安防護。公司結合團隊多年來處理資安事件調查之深厚經驗以及針對人工智慧技術之深入研究，將 AI 與機器學習技術應用在資安實務工作中，持續為全球各地的政府機關、銀行和高科技製造產業提供專業資安服務。曾獲得國際頂尖研究機構 Gartner、IDC、Frost & Sullivan 的多項認可，以及海內外大獎的多次肯定。

圖 17：奧義智慧人員與其展示攤位

資料來源：本計畫整理

(2) 智慧資安 uniXecure：成立於 2022 年，為「精誠資訊」關係企業，原為集團資深資安團隊過往以專業資安顧問服務，成功協助超過 400 家以上客戶保護其核心競爭力，而智慧資安科技成立至今亦已擁有近百家的豐富建置經驗，服務產業橫跨公部門、傳產、製造、高科技與金融等，除代理引進國際知名先進資安技術，協助客戶依其商業流程量身打造資訊安全防護架構外，更提供由專業資安團隊建立資訊資產防護機制的角度，讓政府機關、企業能以訂閱制方式，享有事前預防、事中偵測、事後應處等一站式資安服務，全力防堵潛在威脅。

圖 18：奧義智慧人員與其展示攤位

資料來源：本計畫整理

(3) 優內控 UPAS：成立於 1993 年，從研發 IP 管理與 NAC 網路存取控制系統產品開始，多年來在資訊安全及網路管理的領域深耕，協助客戶建立全方位內網安控系統，解決企業內網安全性與管理效率的問題。獨立研發出擁有多國專利的 IP/MAC 管理核心技術—ARPScanner，十多年來不斷擴充其功能，建構出符合企業網路安全需求的完善系統，系統以高相容性、高智能化與高維持率等優勢獲得許多客戶信賴。 持續研發與提供服務，UPAS 在市場上累積超過 3800 家客戶群的產品使用見證，客戶行業領域遍及政府單位、電子業、製造業、科技業、金融業、銀行業、證券業、醫療機構、學校單位等。

圖 19：優內控人員與其展示攤位

資料來源：本計畫整理

(4) 全景軟體：成立於 1998 年，隸屬於緯創集團，是一家專業的資安企業。致力於幫助各行各業的客戶打造更安全、高效的網路業務流程，並優化保護和管理數據與資源。從零信任架構的數位認證，到金融科技安全解決方案及物聯網設備的強健安全性，目標是為客戶提供有效的安全保護、卓越的服務品質以及無縫的系統擴展能力。全景軟體與元大銀行合作，採用 FIDO 多因素驗證技術，為元大集團提供更高安全性和便捷性的金融服務，這解決了跨金融機構間的身分驗證和資料傳遞的問題。另外，全景軟體亦與日本的 Cybertrust 合作，針對歐盟和日本的物聯網（IoT）和操作技術（OT）安全標準，聯合開發資安解決方案，協助企業應對歐盟網路韌性法案（CRA）的合規要求。

圖 20：全景軟體人員與其展示攤位

資料來源：本計畫整理

(5) 關楗 KeyXenti：成立於 2017 年，由一支專注於硬體、安全元件與軟體整合的資訊安全專家團隊領導。核心專業涵蓋生物識別、多因素身份驗證、治理與公共金鑰基礎設施（PKI）技術。為各類資訊服務提供先進的安全加密技術，致力於解決遺忘或被盜密碼所帶來的安全漏洞問題。關楗的智慧金鑰解決方案結合了硬體和生物辨識技術，專為銀行和軍事等高安全需求的客戶設計。他們的技術提供了無密碼的身分認證系統，通過指紋識別來增強安全性，已經獲得了金融機構和軍方的採用。關楗不僅限於台灣市場，更積極進軍國際市場，特別是在東南亞地區的金融業務中，通過其零信任身分認證解決方案來保護用戶的數據安全，從而打開了國際商機。

圖 21：關楗人員與其展示攤位

資料來源：本計畫整理

(6) 睿廷：擁有近 13 年的資訊安全經驗，專注於資訊安全、密碼學及晶片技術。特別是在金融業務系統的開發與實施方面，獲得了業界與客戶的高度讚譽。睿廷不僅是 Utimaco 加密設備的獨家代理商，還在物聯網（IoT）與電動車安全領域展現出領先的創新能力。

圖 22：睿廷人員與其展示攤位

資料來源：本計畫整理

(7) 眾至資訊 ShareTech：成立於 1999 年，總部位於台中，是一家廣為人知的資訊安全公司。專注於網路安全及電子郵件安全管理，致力於保護企業和機構的信息及內部網絡免受各種威脅與攻擊。ShareTech 在日本、印度、泰國及印尼等地進行全球拓展，提供強大的 UTM（統合威脅管理）系統，為企業抵禦網路威脅提供有力的保護。

圖 23：眾至資訊人員與其展示攤位

資料來源：本計畫整理

(8) 如梭世代 ZUSO Generation：成立於 2019 年，是一家專注於資訊安全服務的新創公司。致力於為企業用戶打造量身定制的資訊安全服務方案，提升組織的資訊安全韌性，並以提供靈活且高安全性的解決方案為核心目標，從而提升企業的可持續商業價值。期望不斷深化自身能力，為各產業鏈的企業用戶創造更多附加價值。如梭世代的主要服務包括滲透測試、紅隊演練、資安顧問等專業服務，致力於透過攻防兩端的多維度技術，解決企業面臨的各類資安挑戰。他們的資安威脅研究團隊（ZUSO ART）已獲得美國 MITRE 公司授權，成為 CVE 編號管理者之一，這使他們能夠及時發現並揭露產品資安問題，幫助企業修補漏洞。

圖 24：如梭世代人員與其展示攤位

資料來源：本計畫整理

(9) 杜浦數位安全 TeamT5：成立於 2017 年，團隊具備超過 20 年的惡意程式、勒索軟體與進階持續性滲透攻擊 APT 的研究經歷，基於地理位置和語言優勢，有效掌握亞太地區的駭客攻擊。更經常受邀參加世界級資安會議演講，包括美國 Black Hat、日本 Code Blue/ AVTokyo、德國 Troopers，及國際組織辦理的 Hack In The Box 與 FIRST 等。另亦專精於亞太地區網路威脅研究，長期研究網路攻擊，追蹤攻擊者，專精類別如進階持續性攻擊(APT)、勒索軟體。我們以精準的威脅情資與獨特的端點威脅狩獵技術，提供反制網路間諜、勒索軟體之資安解決方案。客戶來自美國、日本、臺灣，產業別涵蓋政府機關、金融、科技、電信、資安服務提供商，持續保護機密文件，阻斷網路攻擊。

圖 25：杜浦數位安全人員與其展示攤位

資料來源：本計畫整理

6. 臺灣館展示攤位亮點

廠商名稱	技術亮點
奧義智慧科技股份有限公司	AI 技術、自動化威脅曝險管理平台
智慧資安科技股份有限公司	全域聯防、MOC 資安監控
全景軟體股份有限公司	IoT 資安、符合 Matter 安全架構的 IoT 方案
關楗股份有限公司	零信任資安、身分驗證管理平台
叡廷股份有限公司	金鑰管理系統與加解密平台、資料庫加密
眾至資訊股份有限公司	新世代防火牆、工控資安、AI SPAM 郵件防護
優內控股份有限公司	UPAS ZTA 零信任內網安全管理
杜浦數位安全股份有限公司	EDR 反制惡意程式端點偵測與回應
如梭世代股份有限公司	紅隊演練、滲透測試、Web 威脅分析平台

7. 舞台活動

(1). 主題演講

A. 活動日期：114 年 4 月 23 日（三）

B. 活動時間：15:00-16:00

C. 活動地點：臺灣資安館 Cybersecurity Team Taiwan 主舞台

D. 主題演講議程：(各廠商主題演講簡報詳見附件一)

時間	主題	單位	演講題目
15:00 | 15:20	SEMI	工業技術研究院 Industrial Technology Research Institute (ITRI)	SEMI E187 及其符合性驗證 (VoC) 簡介
15:20 | 15:40	PQC	匯智安全科技股份有限 WiSECURE Technologies Corporation	為後量子時代做好準備：PQC 轉型與重建安全基礎設施
15:40 | 15:48	ZTA	全景軟體股份有限公司 CHANGING Information Technology Inc.	零信任架構下的智慧家庭設備安全新思考
15:48 | 15:56	ZTA	關楗股份有限公司 KeyXentic Inc.	台灣政府的網路安全與零信任計劃
15:56 | 16:04	ZTA	優內控股份有限公司 UPAS Technology Corp.	一站式實現零信任，全面保護您的內部網路安全

(2). 廠商技術成果發表會

A. 活動日期：114 年 4 月 24 日（四）~ 4 月 25 日（五）

B. 活動時間：14:00-15:40、10:00-11:40

C. 活動地點：臺灣資安館 Cybersecurity Team Taiwan 主舞台

D. 成果發表會議程：(技術成果發表會簡報詳見附件二)

時間	廠商	發表主題
10:00 10:10	CYCRAFT 奧義智慧科技股份有限公司	XASM 360 度網路安全威脅監控
10:10 10:20	uniXecure 智慧資安科技股份有限公司	HEIS 針對性攻擊電子郵件訓練服務
10:20 10:30	UPAS 優內控股份有限公司	採用 UPAS NAC + ITAM 的下一代安全架構 — 實現完全可視、零信任、零盲點的安全可靠的 IT 環境
10:30 10:40	CHANGING 全景軟體股份有限公司	安全晶片、藍牙模組和 PKI 加速 Matter 合規性和智慧家庭市場部署
10:40 10:50	KeyXentic Inc. 關楗股份有限公司	台灣政府的網路安全與零信任計劃
10:50 11:00	BULWARETECH CO., LTD. 叡廷股份有限公司	加密技術高端資訊安全解決方案
11:00 11:10	ShareTech 眾至資訊股份有限公司	台灣針對日本優化的網路前沿專業知識 - 中小企業的資訊安全策略 台灣測試的安全，專為日本製造 Taiwan-Tested Security, Made for Japan
11:10 11:20	ZUSO Generation The best defense is offense. 如梭世代股份有限公司	真慶幸自己還活著！紅隊演習後，安全強化戰略直擊。
11:20 11:30	TEAMT5 杜浦數位安全股份有限公司	領先亞太地區網路威脅！ TeamT5 提供持續威脅追蹤和威脅情報

圖 26：臺灣資安館技術發表會現場照片

資料來源：本計畫整理

四、參加臺灣資安館 Cybersecurity Team Taiwan 開幕式

（一） 活動時間：114 年 4 月 23 日（三）13:30~15:00

（二） 活動地點：2025 IT Week Spring 東 1 館 8-18 號

（三） 出席人員：

1. 台方出席人員名單

No.	單位/Organization	姓名/Name	職稱/Title
1.	駐日代表處	李逸洋	大使
2.	數位發展部數位產業署	曾碧雲	組長
		杜欣怡	簡任技正
		盛郁雁	專案規劃師
3.	中華經濟研究院東京事務所	丁心嵐	所長
		許家芳	陪同人員
4.	工業技術研究院	雷穎傑	技術副組長
		張懷文	專案人員
5.	工研院日本辦公室	施虹宇	代理部長
6.	資訊工業策進會	蕭榮興	主任
7.	臺灣資訊安全協會	涂睿珅	理事長
		洪伯岳	秘書長
8.	匯智安全科技股份有限公司	鄭嘉信	創辦人兼執行長
9.	來毅數位科技股份有限公司	林政毅	董事長
10.	叡廷股份有限公司	趙翌有	總經理
11.	全景軟體股份有限公司	東田将真	駐在員事務所代表
12.	奧義智慧科技股份有限公司	荻原博	策略與營運高級經理
13.	智慧資安	黃之應	事業部長
14.	關楗股份有限公司	古館侑樹	營業部長
15.	眾至資訊股份有限公司	洪嘉鎂	副理
16.	優內控股份有限公司	梁容蓉	銷售經理
17.	杜浦數位安全股份有限公司	橫田智成	資深銷售工程師
18.	如梭世代股份有限公司	何宜霖	首席技術長

2. 日方出席人員名單

No.	單位/Organization	姓名/Name	職稱/Title
1.	日本防衛協會	不揭露	不揭露
		不揭露	不揭露
2.	警視廳	不揭露	不揭露
		不揭露	不揭露
		不揭露	不揭露
3.	Aillumission (智慧資安日本合作夥伴)	辻 高志	社長
		水本政宏	
4.	Y'S corporation (眾至日本合作夥伴)	川田 信人	業務部長代理
5.	GMO cybersecurity by Ierae Inc.	Shinichi Kan	Acting General Manager
6.	NSW 株式会社 (關楗日本合作夥伴)	扇 達也	經理

（四） 開幕式議程

時間	流程
1300-1325	開幕貴賓報到
1325-1330	主持人進行開幕活動暖場預告
1330-1340	開幕式開始
1340-1345	TWISA 理事長致詞
1345-1350	與會貴賓介紹
1350-1400	嘉賓代表致詞~~再~~
1400-1405	台灣館介紹影片
1405-1410	啟動儀式 上台單位人員代表： 1. 臺灣駐日代表李逸洋 2. 數位產業署杜欣怡 3. 臺灣資安大聯盟洪伯岳 4. 台灣資訊安全協會涂睿珅 5. 工業技術研究院雷穎傑 6. PQC 產業聯盟鄭嘉信
1410-1415	活動合影

（五） 臺灣資安館 Cybersecurity Team Taiwan 開幕式活動重點摘述

為展現我國政府對於日本資安產業市場重視，今年首次以臺灣主題館方式參加 IT Week Spring 展會，並於「臺灣資安館」開幕式邀請我國駐日代表處李逸洋大使出席。

駐日代表李逸洋大使於現場強調，臺灣與日本同處亞太資安戰略重心，雙方皆為全球供應鏈重要一環，深化彼此合作，不僅能強化區域聯防，更可提升產業韌性與競爭力，也盼藉由本次參展促成臺灣資安業者與日本大型企業、系統整合商合作，共同開發產品推廣市場。

開幕式活動並由我國駐日代表大使李逸洋、本署簡任技正杜欣怡、臺灣資訊安全協會理事長涂睿珅、臺灣資安大聯盟副秘書長兼發言人洪伯岳、後量子資安產業聯盟代表匯智安全科技創辦人暨執行長鄭嘉信等人進行啟動儀式，共同將手上的御守貼上資安守護神盾，為本次臺灣資安館 Cybersecurity Team Taiwan 正式揭開序幕。

圖 27：臺灣資安館啟動儀式

資料來源：本計畫整理

圖 28：臺灣資安館出席貴賓合影

資料來源：本計畫整理

啟動儀式結束後便開始進行導覽，導引李大使與貴賓們巡視我國資安廠商的攤位以了解各家廠商的解決方案，大使對臺灣資安廠商表現出極高的興趣，也對我國業者積極拓展日本商機努力給予肯定及勉勵。

（六） 臺灣資安館展攤導覽流程

活動時間	14:15-15:00
活動地點	臺灣資安館各展出攤位
導覽人	臺灣資安大聯盟洪伯岳
參與導覽人員	1.臺灣駐日代表李逸洋 2.數位產業署曾碧雲、杜欣怡、盛郁雁 3.台灣資訊安全協會(TWISA)涂睿珅 4.工業技術研究院雷穎傑、張懷文 5.資訊工業策進會蕭榮興 6.PQC 產業聯盟鄭嘉信(匯智安全)
導覽順序	智慧資安→關楗→眾至→杜浦→全景→優內控→如梭→奧義→叡廷

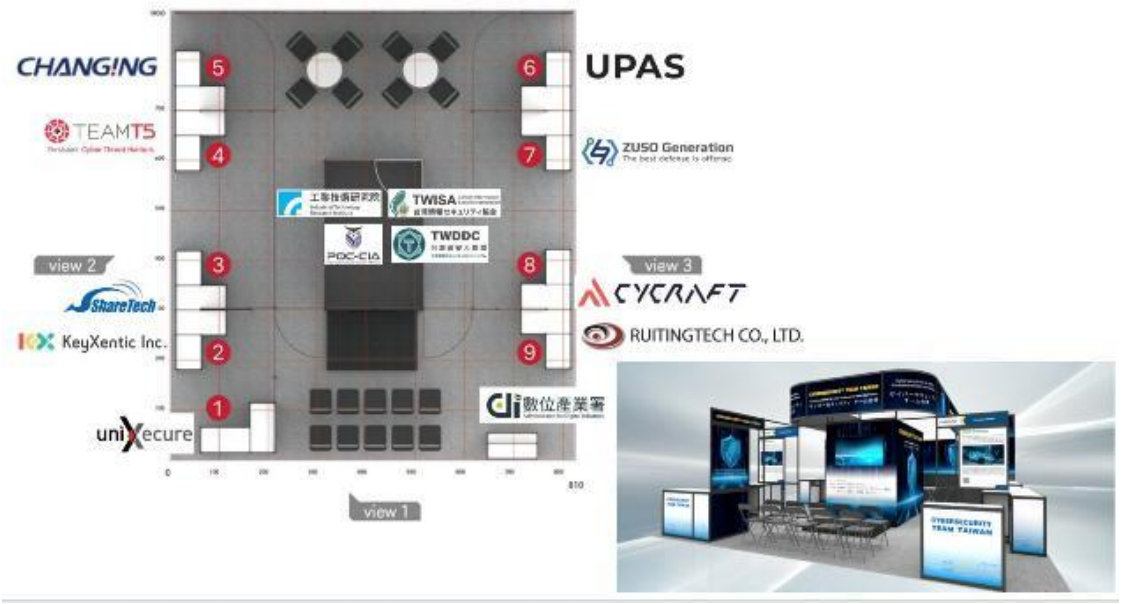


圖 29：臺灣資安館展攤導覽順序示意圖

資料來源：本計畫整理

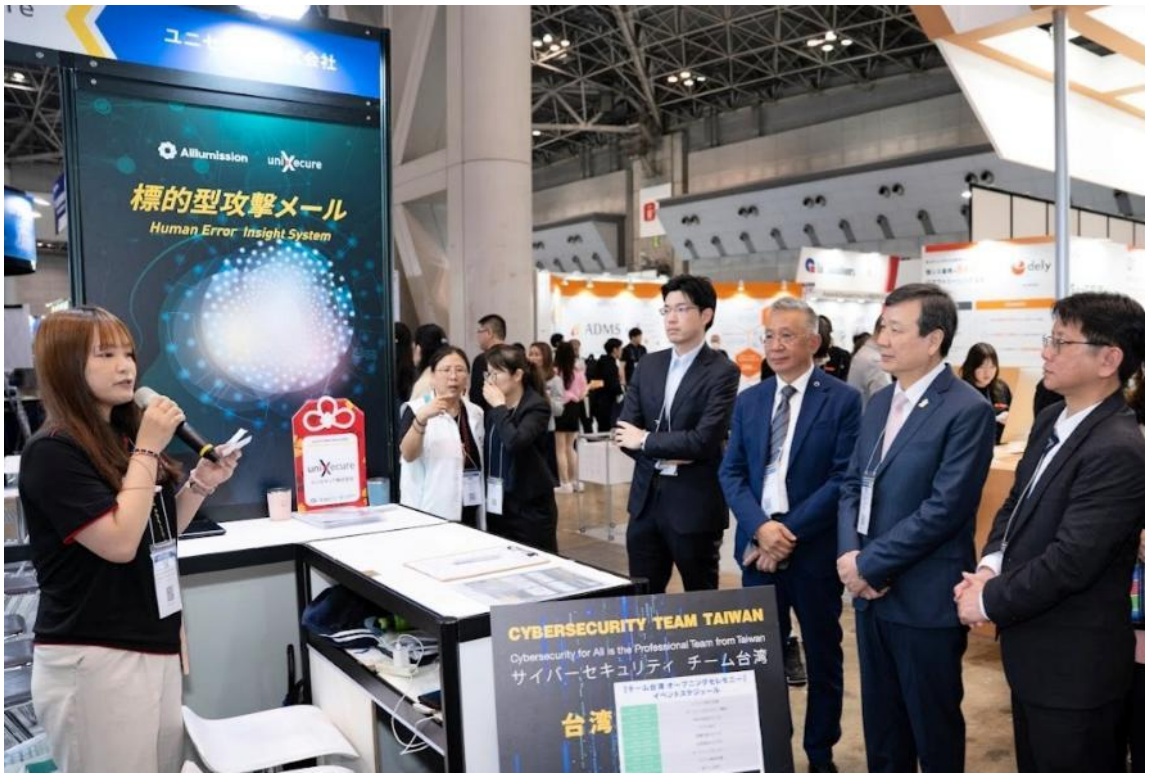


圖 30：李逸洋大使聽取臺灣資安廠商介紹

資料來源：本計畫整理

五、參訪臺灣雲服務館 Cloud Service Team Taiwan

（一）活動時間：114 年 4 月 23 日（星期三）15:00~15:30

（二）活動地點：2025 IT Week Spring 東 1 館 11-6 號

（三）出席人員

No.	單位/Organization	姓名/Name	職稱/Title
1.	數位發展部數位產業署	杜欣怡	簡任技正
		盛郁雁	專案規劃師
2.	工業技術研究院	雷穎傑	技術副組長
		張懷文	專案人員
3.	資訊工業策進會	蕭榮興	主任

（四）活動介紹

為推動我國雲端服務業者拓展海外市場，本署協助我國 8 家臺灣具代表性的雲服務業者參與日本規模最大的 ICT 專業展會，共同打造「Cloud Service Team Taiwan」主題專館，向國際展示臺灣在數位轉型、AI 應用、行銷科技、資安等雲端解決方案的創新能量與實戰經驗。

本次參展廠商提供多元的雲端服務，包括以力科技與愛吠的狗展示結合 AI 與 VR 技術的 AI 雲端客服，雲發互動科技的 AI Agent 智慧助理，獵豹資訊、亞路科技與禾多移動推出的網紅媒合、社群行銷整合與流量生成等數位行銷方案，以及叡揚資訊推出知識管理系統和凌羣電腦開發的資安 IT 監控系統等，充分展現臺灣資服業者在數位創新量能。

在臺灣資安館開幕式後，亦邀請我國駐日代表李逸洋大使前往臺灣雲服務專館聽取參展業者介紹相關應用方案，大使對於業者在國際市場的表現與努力，也給予高度的肯定及勉勵。

圖 31：李逸洋大使與虛擬人物互動

資料來源：本計畫整理

圖 32：李逸洋大使與臺灣雲服務館團隊合影

資料來源：本計畫整理

六、參觀 IT Week 春季展資安相關展攤

本次訪團除了率領我國資安廠商主辦臺灣資安館 Cybersecurity Team Taiwan 外，也同步參觀其他廠商攤位，藉此了解日本資安業者相關方案。相關資訊如下：

（一）Soracom

Soracom 是一間專注 IoT 的行動虛擬網路營運商(Mobile Virtaul Network Operator)服務商，透過全球 SIM/eSIM 連接，到加密轉發、資料儲存與分析等服務，協助企業管理遍布全球的 IoT 設備，近年也因應生成式 AI 浪潮，提供免程式碼或簡易程式碼即可使用生成式 AI 工具的服務，讓企業可在不需要專業 AI 工程師的協助下，結合生成式 AI 服務加值 IoT 設備的管理，如 IoT 設備維運或健康狀況的報表。本次展出的 Soracom Air 服務，更支援了 LoRaWAN、Sigfox 通訊協定下的資料安全傳輸。

「ソラカメ」，英文服務名稱：Soracom Cloud Camera Services，是 Soracom 推出的雲端型 IoT 攝影機解決方案，主打低成本、無需工程即可快速部署的智慧監控服務，讓企業或個人能透過簡單操作，即可在 Soracom 本身安全的 IoT 傳輸網路及雲平台上，讓監視器安全的將影像傳送到雲端，進行影像管理、AI 影像分析及告警。此服務模式，對於需要遠端監視影像及加值分析，但又擔心監視器資安疑慮的業者來說，的確是一個方便實惠的方案。

Soracom 此次展會的資安展示重點在於端到端的 IoT 連接安全，從硬體 SIM 卡安全、加密通訊、裝置認證到雲端資料管理，形成完整的資安防護鏈。其強調與合作夥伴共建生態系，提供多元且安全的 IoT 解決方案，滿足企業在數位轉型過程中的資安需求。

對於台灣資安產業而言，與 Soracom 合作的重點可聚焦於 IoT 端點安全技術整合，提供裝置端的防護軟體、韌體安全及身份認證的零信任解決

方案；另日本今年剛公告物聯網資安標準 JC-STAR，這部分台安資安業者有相當多物聯網資安認證經驗，可以提供 Soracom 參考，加速其產品的資安合規認證

總體而言，Soracom 是物聯網整體解決方案供應商，與台灣產業可以相互搭配，推動雙方技術與產品的深度整合與推廣。

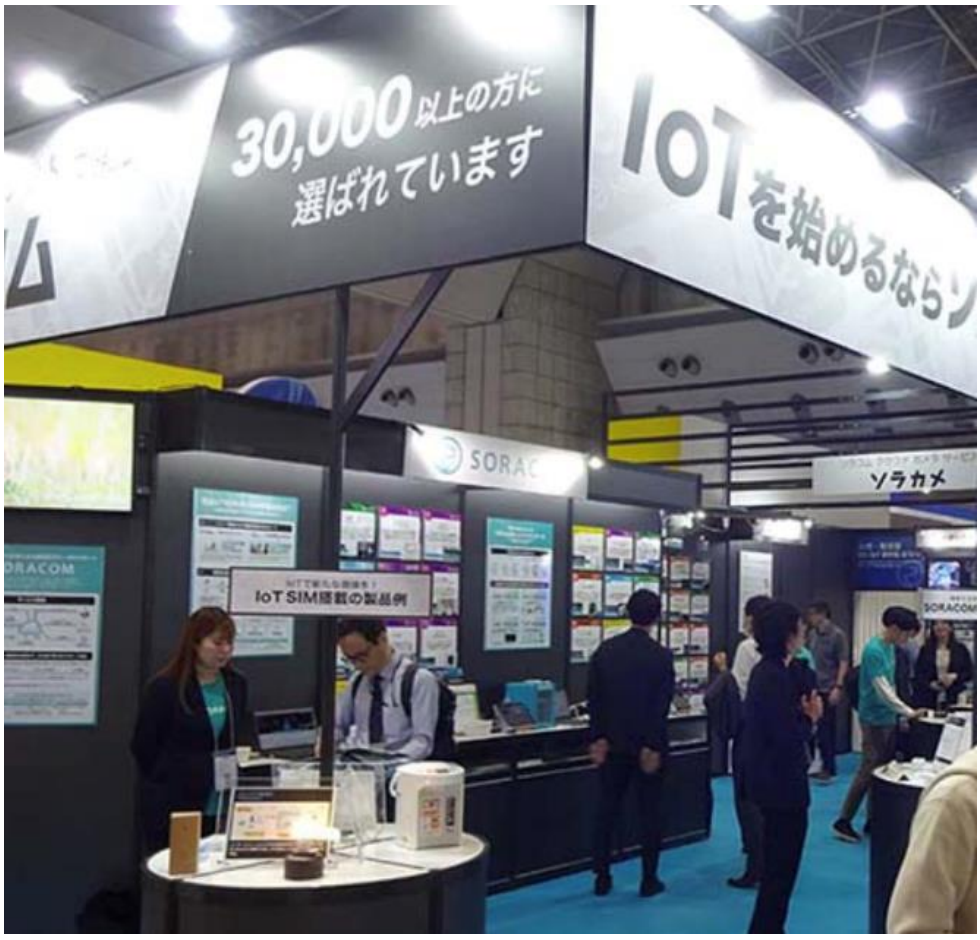


圖 33：Soracom 展攤與物聯網整體解決方案

資料來源：本計畫整理

（二）GMO Internet Group

GMO Internet Group, Inc.(簡稱 GMO)，是日本領先的網際網路企業集團， 2023 年起轉為控股公司體制，旗下擁有超過 100 家子公司，事業橫跨網路基礎設施、網路金融科技、數位行銷與媒體：廣告平台、SEO/SEM、內容網站、資安與雲端信任等，旗下有多家資安相關科技公司，如 GMO

GlobalSign，為日本最大 SSL/TLS 憑證與電子簽章供應商，市佔率超過 80%；GMO Cybersecurity by Ierae 曾在 2023～2024 年連續兩年的 Cloud Village CTF(雲端安全奪旗賽)獲得冠軍；GMO Flatt Security，專注產品安全與自動化資安工具提供者；Shisho Cloud 針對 Web 應用與公有雲環境提供的自動化漏洞掃描 SaaS 服務；KENRO 是一個 Secure Coding 學習平台，為一款幫助開發者強化資安意識與技術力的 SaaS 平台；Takumi 提供 AI 資安稽核助理服務，形成完整且多元的資安生態系。這使 GMO 不僅在日本資安市場具備強大競爭力，也展現出在推動企業數位轉型與資安技術創新方面的領導地位。

在 2025 年日本 IT Week 春季展中，GMO 旗下子公司 GMO Flatt Security 推出了其最新的 AI 資安產品「Takumi」，該產品定位為一款專為軟體開發與安全工程師設計的 AI 安全診斷代理人，以提升軟體開發過程中的安全性與效率。Takumi 能夠自動識別軟體中的安全漏洞，並協助工程師進行漏洞分級與優先處理，減少人工審查負擔，並且能將診斷結果進行有效分類與管理，確保團隊能針對最關鍵的安全問題迅速反應。透過與 Slack 等協作工具整合，開發團隊可直接向 Takumi 發出安全檢查請求，AI 代理人會自主進行多輪分析與回應，提升溝通效率。同時，Takumi 可設定在特定事件發生時自動啟動安全評估，實現軟體生命週期中的持續安全保障。

圖 34：GMO 展攤與 AI 開發助理：Takumi 解決方案

資料來源：本計畫整理

（三）Cybereason

Cybereason 成立於 2012 年，總部位於以色列特拉維夫，是全球資安領域的創新領導者，專注於端點安全、網路安全及跨平台威脅偵測。公司在全球 18 個國家設有營運據點，並擁有三個全球安全運營中心（東京、特拉維夫、波士頓），其解決方案已部署在超過 1200 萬個端點裝置上，廣受企業界肯定。Cybereason 以獨家研發的 MalOp™檢測技術與 AI 引擎著稱，能主動偵測並回應各種複雜的網路攻擊，並於 2022 年獲得 MITRE ATT&CK 評比為史上最佳資安平台。

本次展會中，Cybereason 重點展示了其 XDR（Extended Detection and Response）平台，該平台整合了預防、檢測、響應與調查功能，能夠快速識別並阻斷多樣化的資安威脅，特別強調 AI 技術在威脅偵測與自動回應中的應用。展區中還介紹了針對零日漏洞與勒索軟體攻擊的防禦策略，並分享了最新的資安威脅趨勢與案例分析，幫助企業提升整體防護能力。

現場的說明人員分享，隨著零日漏洞數量激增，傳統的管理模式已無

法完全防禦，必須依靠 AI 驅動的主動防禦技術來降低風險。此外，展會中也提及近期針對金融、建築等產業的社交工程攻擊案例，強調多層次防禦的重要性。

台灣資安產業也有許多 XDR 解決方案，這次 Cybereason 帶來的展示，對台灣資安產業而言，顯示加速 AI 技術整合的重要性，促使台灣廠商在資安產品中融入更多智能化、自動化功能，以應對日益複雜的網路攻擊。Cybereason 針對零日漏洞與勒索軟體的防禦策略，也提醒台灣資安業界必須強化對新型態威脅的快速識別與反應能力，台灣廠商應加強研發具備即時威脅分析與多層次防禦的解決方案，提升整體資安韌性。此外，Cybereason 強調多層次防禦與跨平台整合，對台灣資安產業推動零信任架構與端點安全管理具有借鑒意義。台灣資安團隊可借鑒其整合端點、網路與雲端資源的策略，打造更全面的防護體系，提升企業客戶的安全保障。綜合而言，Cybereason 在日本 IT Week 春季展的展示，可以提供台灣資安產業應積極推動 AI 智能化防禦、多層次安全策略與國際合作，以提升整體競爭力與應對未來資安挑戰的能力。

圖 35：Cybereason 展攤與 AI-XDR 解決方案

資料來源：本計畫整理

（四） Wisecure-tech Japan

為亞洲領先的硬體安全模組（Hardware Security Modules, HSM）製造商，透過臺灣 IKV-Tech 的 OEM/ODM 技術實力，以及多年的軍民兩用安全級別設計經驗，提供包含金融、雲端、IoT 市場的客製化 HSM 及 FIDO 安全工具及設計服務。

1. HSM 產品部分：從支援 PCIe 介面的高使用頻率的金融機構應用，USB 介面適用隨身裝置的加密應用，到 MicroSD 介面適用於 IoT 裝置的資料加密存取，完整滿足不同市場的需求。
2. 在身分認證設備產品部分：從單純支援 FIDO 身分認證到適用軍方的特規加密，如 PQC 後量子加解密安全金鑰
3. 檔案加密管理系統：除了軟體版本的檔案加密管理系統，亦提供結合 HSM 硬體安全模組及身分認證產品所打造的安全網路儲存裝置。

本次 Wisecure-tech Japan 在 IT WEEK 春季展曝光是該公司的 KV FDO Solution，鄭總經理親自為參訪團隊解說，FDO（FIDO Device Onboard）是由 FIDO 聯盟推動的一項開放標準，旨在提升物聯網設備的安全性與部署效率。Wisecure-tech Japan 針對這一標準，打造了一套自動化的安全認證流程，徹底改變了傳統物聯網設備在部署階段所面臨的挑戰。過去，物聯網設備往往需要手動進行複雜的設定，且普遍存在使用預設憑證的安全隱患，這些問題不僅增加了配置的難度，也大幅提升了遭受攻擊的風險。透過 Wisecure-tech Japan 的自動化認證方案，這些繁瑣的手動操作被大幅簡化，設備能夠自動完成安全註冊與身份驗證，有效杜絕預設憑證帶來的安全漏洞。此方案不僅提升了部署的便捷性與安全性，也協助廠商實現從設備生產、出廠到使用全階段的產品生命週期管理。藉由這套完整且高效的流程，廠商能夠更好地掌控設備安全狀態，確保物聯網生態系統的穩定與可靠，為智慧連網設備的廣泛應用奠定堅實的基礎。

圖 36：Wisecure-tech Japan 展攤與物聯網整體解決方案

資料來源：本計畫整理

（五）LANSCOPE

LANSCOPE 主打 IT 資產管理（ITAM）、操作監控（Operation Log）與端點安全防護。透過整合 IT 資產管理與端點安全應用，為企業提供一套全面且高效的資安管理方案。具體而言，LANSCOPE 自動化收集並管理 PC 與行動裝置的硬體與軟體資產資訊，讓企業能即時掌握設備狀態與使用情況，減少資產管理的人工成本與錯誤。同時，LANSCOPE 結合端點防護功能，如行為監控、應用程式操作管理、USB 與外接設備管控、網頁權限監控等，有效防範內部資料外洩與惡意軟體攻擊。此外，LANSCOPE 還整合 Microsoft Defender 等防毒工具，並提供即時威脅偵測與隔離功能，提升整體端點安全防護能力。其設備控制系統可靈活設定 USB、CD 等存儲設備的使用權限，防止機密資料透過外部設備外洩。網路流量側錄與異常偵測功能則能快速定位網路瓶頸與安全問題，補足企業資安最後一道防線。

在本次 Japan IT Week 春季展中，LANSCOPE 展示了其端點管理與資安防護的整合解決方案，LANSCOPE Endpoint Manager 可以統一管理 PC

與行動裝置，實現 IT 資產盤點與安全控管。LANSCOPE Cyber Protection 則結合 AI 技術的防毒與行為監控，強化惡意軟體防禦與內部威脅識別。LANSCOPE Security Auditor：針對 Microsoft 365 的安全審計工具，提升雲端服務安全管理。此外，LANSCOPE 也向參訪團隊分享他們的脆弱性診斷服務，可以協助企業進行系統與應用程式弱點掃描，提前修補安全漏洞。

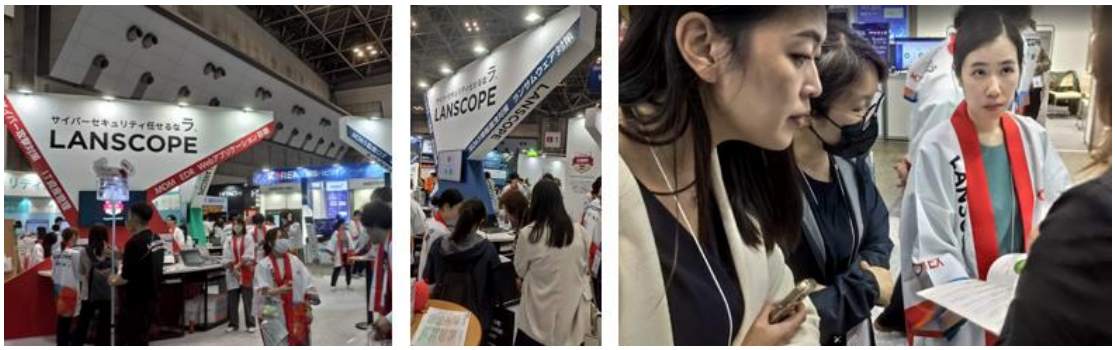


圖 37：LANSCOPE 展攤與資產管理資安解決方案

資料來源：本計畫整理

（六）MEEQ

MEEQ 是一家立足於日本的創新科技企業，專注於物聯網（IoT）與數位轉型（DX）領域的解決方案開發。公司致力於通過簡化技術門檻，推動企業快速實現智能化升級，特別強調無程式碼（NoCode）平台的開發，讓非技術用戶也能輕鬆部署 IoT 應用，促進數據驅動的決策與管理。

在 2025 年日本 IT Week 春季展中，MEEQ 展示了其創新的 NoCode IoT/DX Platform，該平台以簡便的操作介面和強大的管理功能，助力企業快速推動物聯網與數位轉型計畫。

NoCode IoT/DX Platform 是一款 SaaS 型物聯網通訊平台，平台提供無程式碼（NoCode）開發環境，企業無需自行開發即可快速實現 IoT 系統，降低技術門檻與開發成本，MEEQ Global SIM 支援約 180 個國家和地區，方便企業進行跨國 IoT 業務部署，其高安全性網路架構：支援雲端及

本地閉域網路，保障通訊安全與資料隱私，並提供通信量與連線狀態的即時監控，減少管理工時，提升運營效率。

經由展攤人員展示，日本 MEEQ 公司的 NoCode IoT/DX Platform 之所以能實現無程式碼開發，關鍵技術主要包括以下幾點：提供用戶友善的圖形化介面，透過拖拉元件與視覺化操作，讓使用者能輕鬆完成 IoT 設備的連接、通信服務的購買與管理，無需撰寫任何程式碼。另外後台部分，應該已經將各種內建多種通用的通信模組與數據處理模組，並支持自動化流程配置，使用者只需設定條件與動作，即可快速構建完整的 IoT 系統，實現數據收集、監控與告警等功能，無需自行開發底層程式。特別是其強調已經整合日本三大電信商的通信資源，應該是已經將各大平台的通訊模組部署完成。

圖 38：MEEQ 展攤與資產管理資安解決方案

資料來源：本計畫整理

（七）TREND

趨勢科技成立於 1988 年，由張明正董事長創立，總部設於日本東京，是全球跨國軟體公司。趨勢科技專注於電腦防毒軟體及網路安全服務，涵蓋行動裝置、端點、伺服器、雲端、5G 及物聯網等多元資安領域。公司持續透過全球威脅研究與創新技術，守護超過 250 萬企業客戶及超過 2.5 億個人用戶。

此次展會中，趨勢科技展示了多款資安產品，包含跨雲端與端點的資安平台，提供針對 AWS、Microsoft 及 Google 等雲端環境的最佳化防護，實現集中威脅偵測與快速回應。會場上也展示 AI 驅動的威脅防禦技術，利用人工智慧提升惡意軟體偵測效率，並強化對新型態攻擊的防禦能力。針對 AI 詐騙，內建視訊異常偵測功能，能在通話中即時警示假冒警察等詐騙行為，達到視訊偵測防詐功能。此外，物聯網與 5G 安全解決方案，可因應物聯網設備與 5G 網路普及，提供端對端的安全防護，降低攻擊風險。

趨勢科技展示了其整合 AI 技術的企業資安平台「Trend Vision One™」，該平台能集中管理威脅情報與系統狀況，並以 AI 驅動的安全代理人「Trend Cybertron」協助分析與預警，提升資安團隊的反應速度與準確性。福田也提醒企業在導入 AI 時須重視「Security for AI」，確保 AI 系統本身的安全性，避免成為新的攻擊目標。

從趨勢科技的展示觀察，此次展會中強調的是面對 AI 帶來的資安新挑戰，企業必須從被動防禦轉向主動預測與風險管理，結合 AI 技術打造更智慧、更全面的資安防護體系，以應對未來日益複雜的網路威脅。

圖 39：TREND 展攤與 Trend Vision One™資安解決方案

資料來源：本計畫整理

（八）Advantech Japan

研華科技成立於 1983 年，總部位於台灣台北，是全球物聯網智能系統與嵌入式平台的領導廠商，產品涵蓋工業電腦、智慧製造、工業自動化及物聯網解決方案。研華以「智能地球的推手」為企業願景，2023 年在工業電腦市場市佔率全球第一，並持續推動 AI 與邊緣運算技術的產業應用。研華在日本設有分公司（Advantech Japan Co., Ltd.），並於 2019 年收購了日本 OMRON 子公司，強化在地服務與技術支持。

本次展會中，研華聚焦於工業物聯網與資安解決方案，展現多項核心產品，包含智慧工廠與邊緣運算平台，為 WISE-IoT 平台與邊緣運算設備，強調 AI 與物聯網結合，協助製造業實現生產線智能監控、預防性維護與品質管理，提升生產效率與靈活性。資安部分，針對工業網路安全，研華推出整合式資安解決方案，涵蓋工業控制系統（ICS）防護與資產管理，確保工廠運營安全無虞。展區亦介紹與日本系統整合商 Nippon RAD 的合作案例，強化軟硬體整合與本地化服務。

研華科技以其深厚的技術底蘊與完整的物聯網生態系統，結合在地合

作夥伴的專業服務，在 2025 年日本 IT Week 春季展中展現了強大的市場競爭力與創新能力。透過智慧製造與資安解決方案，研華持續推動日本產業的數位轉型與智能升級，助力企業迎接未來挑戰。

圖 40：Advantech Japan 展攤與最新嵌入式平台產品

資料來源：本計畫整理

（九）MSI

MSI 成立於 1986 年，總部位於台灣，是全球知名的電競硬體與高效能運算設備製造商，產品涵蓋主機板、顯示卡、筆記型電腦、伺服器及工業用嵌入式系統等。MSI 積極布局 AI 運算與邊緣運算領域，致力於提供企業級解決方案，並在全球市場擁有廣泛影響力。

本次展會中，MSI 聚焦於 AI 運算、雲端工作負載與資安產品，MSI 推出多款專為次世代 AI 與雲端運算設計的伺服器，支援大型語言模型（LLM）與深度學習應用，提升運算效能與能效比， AI SmartLink 平台結合大型語言模型與 AI 聊天機器人技術，提升企業決策效率，並搭配 SysLink 遠端監控與預測性維護，強化生產運營效能。資安部分則結合 AI 技術的資安產品，強化威脅偵測與防禦能力，提升企業資訊安全防護層級。

在產業應用方面，本次包括智慧車載平板、智慧農業平板及自助點餐機等，MSI 提供 ODM/OEM 一站式客製化解決方案，滿足多元產業需求。

（十）GIGABYTE

技嘉科技成立於 1986 年，總部位於臺灣新北市，是全球領先的電腦主機板及顯示卡製造商之一。公司以「創新科技，美化人生」為企業使命，產品線涵蓋主機板、顯示卡、電腦系統、伺服器、筆記型電腦及網路通訊設備。技嘉在全球設有多個研發與製造基地，並積極推動 AI、AIoT 及 5G 等前瞻技術的應用，持續擴大企業市場版圖。

本次展區展出技嘉最新 GPU 伺服器及 AI 伺服器，提出資料中心及邊緣運算的解決方案。根據該負責人介紹，技嘉的 GPU 伺服器及 AI 伺服器已上市約一年，廣泛應用於半導體製造設備、醫療設備、火力發電廠等行業。這次展出了搭載 AMD EPYC 8004 系列的邊緣伺服器，以及搭載第四代、第五代至強可擴充處理器的伺服器。

同時，Advanet 自己的產品－使用 LoRaWAN 的物聯網通訊系統「Leyline」也在現場展出。本產品具有利用工廠設備的振動感測器進行異常檢測、省電的長距離通訊等功能，並以應用於鹿兒島縣大崎町的堆肥廠的溫度感應。

圖 41：GIGABYTE 展攤與最新最新 GPU 及 AI 伺服器產品

資料來源：本計畫整理

七、參訪伊藤忠科技解決方案公司（CTC）

（一）活動時間：4 月 24 日(星期四)，上午 9:30~11:15

（二）活動地點：東京都港區虎之門 4-1-1　神谷町信賴大樓 2 樓

（三）出席人員：

1. 台方出席人員名單（共 20 人）

No.	單位/Organization	姓名/Name	職稱/Title
1.	數位發展部數位產業署	杜欣怡	簡任技正
		盛郁雁	專案規劃師
2.	奧義智慧科技股份有限公司	張筑婷	Architecture Consultant Manager
3.	睿控網安股份有限公司	Toru Takahashi	技術工程部資深總監 Senior Director
4.	優內控股份有限公司	張本純 (Harimoto)	臺灣區經理
5.	關楗股份有限公司	洪伯岳	執行長
6.	叡廷股份有限公司	趙翌有	總經理
7.	眾至資訊股份有限公司	洪嘉鎂	專案部副理
8.	全景軟體股份有限公司	東田 将真	駐在員事務所　代表
9.	杜浦數位安全股份有限公司	宮本　明	日本法人經理
10.	智慧資安科技股份有限公司	林詩珊	產品專員
11.	匯智安全科技股份有限公司	鄭嘉信	總經理/TWISA 理事
12.		林蓉萱	業務經理
13.	來毅數位科技股份有限公司	林欣怡	總經理/TWISA 財務長
14.		青柳 正	日本分公司副總裁
15.	工業技術研究院	卓傳育	技術組長
16.		雷穎傑	技術副組長
17.		張懷文	專案人員
18.		施虹宇	部長代理
19.	資訊工業策進會	蕭榮興	主任
20.	臺灣資訊安全協會	葉晏伶	工作人員

2. 日方出席人員名單

No.	單位/Organization	職稱/Title	姓名/Name
1.	數位服務事業群 Digital Services Business Group	執行董事（副總）Managing Executive Officer	藤岡 良樹（FUJIOKA Yoshiki）
2.	數位服務事業群網路安全企劃・推廣本部 Digital Services Business Group Cyber Security Business Planning and Promotion Headquarters	技術總監 Chief Technical Officer	伊藤 英二（ITO Eiji）
3.	區域・社會基礎建設事業群中國地方九州業務本部 Regional and Social Infrastructure Business Group Chugoku Kyushu Sales Headquarters	—	浅野 周三（ASANO Shuzo）
		—	水川達也（MIZUKAWA Tatsuya）
4.	區域・社會基礎建設事業群中國地方九州業務第1部 Regional and Social Infrastructure Business Group Chugoku Kyushu Sales Headquarters Department 1	—	桑山裕介（KUWAYAMA Yusuke）
5.	技術戰略集團 創新戰略部 Technology Strategy Group, Innovation Strategy Department	資深專員 Senior Specialist	中川 裕路（NAKAGAWA Yuji）
		主任 Chief	住友 真穂子（SUMITOMO Mahoko）
6.	資訊系統集團 IT 安全整合部 Information Systems Group IT Security Division	課長 Section Manager	藤原 利行（FUZIWARA Toshiyuki）
		—	大畑 光介（OHATA Kosuke）
		—	加藤美穗（KATOU Miho）
7.	資訊系統集團 IT 基礎健設系統部 Information Systems Group IT Infrastructure Systems Department	課長 Section Manager	長井健太（NAGAI Kenta）
		—	鈴木利幸（SUZUKI Tosiyuki）
8.	區域・社會基礎建設事業群公共業務第二部 Regional and Social Infrastructure Business	—	岡田大翔（OKADA Hiroto）
		—	田島 瑛芝（TAZIMA Eishiba）

	Group, Public Sales Department 2		
9.	區域・社會基礎建設事業群 市場企劃部 Regional and Social Infrastructure Business Group, Public Sales Marketing Planning Department	高級專家 Senior Specialist	米澤政洋（YONEZAWA Masahiro）
10.	台湾代表者事務所 Taiwan Representative Office	事務所長 Head of Office	魏 海洪 (Wei Haihong)

（四）伊藤忠科技解決方案公司（CTC）基本介紹：

CTC 為伊藤忠旗下的科技解決方案公司，其下有幾個重要的單位：

1. 技術解決方案中心(TSC)

   TSC 是日本領先的綜合驗證中心之一，擁有全方位的開放資源。 除了驗證單個產品外，還建立了一個系統，可以與供應商合作夥伴合作，在多供應商環境中進行驗證。TSC 不僅在提高我們提供的系統的安全性方面發揮著重要作用，而且在更快地提供更優化的系統方面也發揮著重要作用。

2. 數據中心：日本全國 3 個地點的 5 個數據中心是日本最大的數據中心之一，除了符合 ISMS 認證和 FISC 的高度安全可靠的設備外，還部署了高品質的網路，以確保客戶資訊系統的穩定運行。

3. 遠端運作中心(ROC)：Remote Operation Center 提供一年 365 天、每天 24 小時遠端作和監控客戶 IT 系統的服務。

4. 維護據點：CTC 的維護和支援基地分佈在全國約 100 個地點，每個基地都提供一年 365 天、每天 24 小時的設備維護、運營服務、監控服務和資訊安全服務等各種服務。

（五）議程：

時間	當日流程
8:50~9:10	訪團人員集合
9:10~9:20	台灣廠商進場
9:20~9:30	雙方列隊互換名片
9:30-9:40	雙方致詞與交流儀式
9:40-9:50	CTC 公司介紹
9:50-10:10	工研院分享我國 SEMI E187 標準與合規相關作法
10:10-10:20	我國資安廠商技術分享 奧義智慧：SEMI E187 合規解決方案與經驗分享 TXOne：SEMI E187 合規解決方案與經驗分享
10:20-11:00	我國 8 家廠商資安技術分享：AI 應用、PQC、工控系統（ICS）資安實踐案例
11:00-11:10	Q&A
11:10~	自由交流時間

（六）CTC 交流摘要

CTC 於 114 年初曾拜訪本署，了解目前我國 SEMI E187 的推動狀況，並關注我國推動 SEMI E187 標準發展過程，爰本次參訪除向 CTC 分享更多 SEMI E187 的推動成果外，亦帶臺灣資安業者前往分享工控資安解決方案以推動商機媒合。

在 SEMI E187 的標準推動分享上，先由工研院卓傳育博士進行分享 SEMI E187 的推動背景，以及目前相容性驗證(Verification of Comformity, VoC)的具體內容與針對檢核清單進行介紹，續由臺灣廠商奧義及 TxOne 介紹相關的 SEMI E187 合規產品，最後再安排與會其他臺灣廠商以短講方式介紹公司及產品，本次交流活動相關簡報詳見附件三。

本次交流 CTC 表達對於 SEMI E187 合規的檢核清單以及如何成為檢驗機構表達興趣，並表達後續可與臺灣廠商共同推動日本 SEMI E187 合規相關事宜。

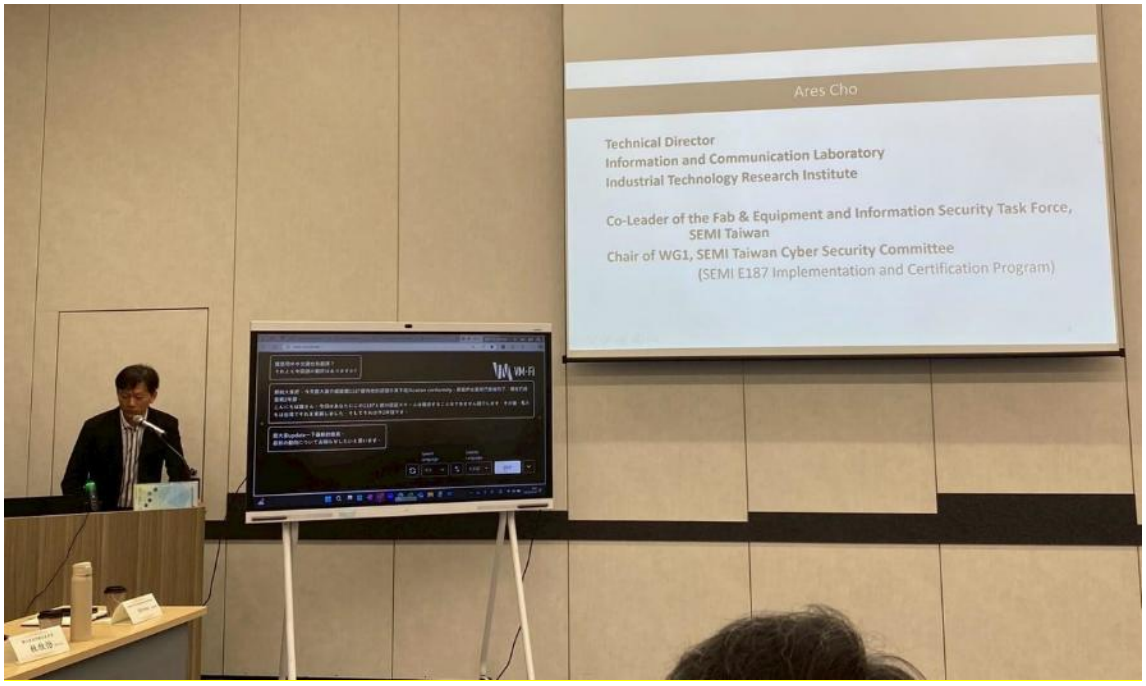


圖 42：工研院卓傳育博士介紹我國 SEMI E187 推動成果

資料來源：本計畫整理

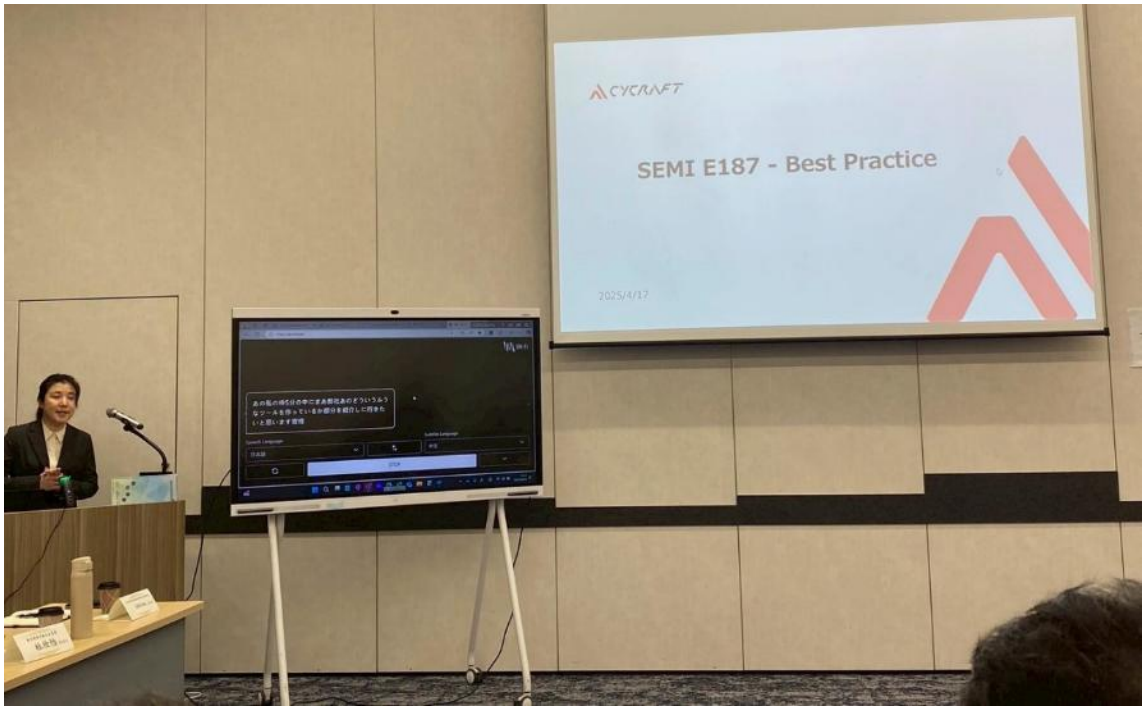


圖 43：奧義分享 SEMI E187 合規產品

資料來源：本計畫整理

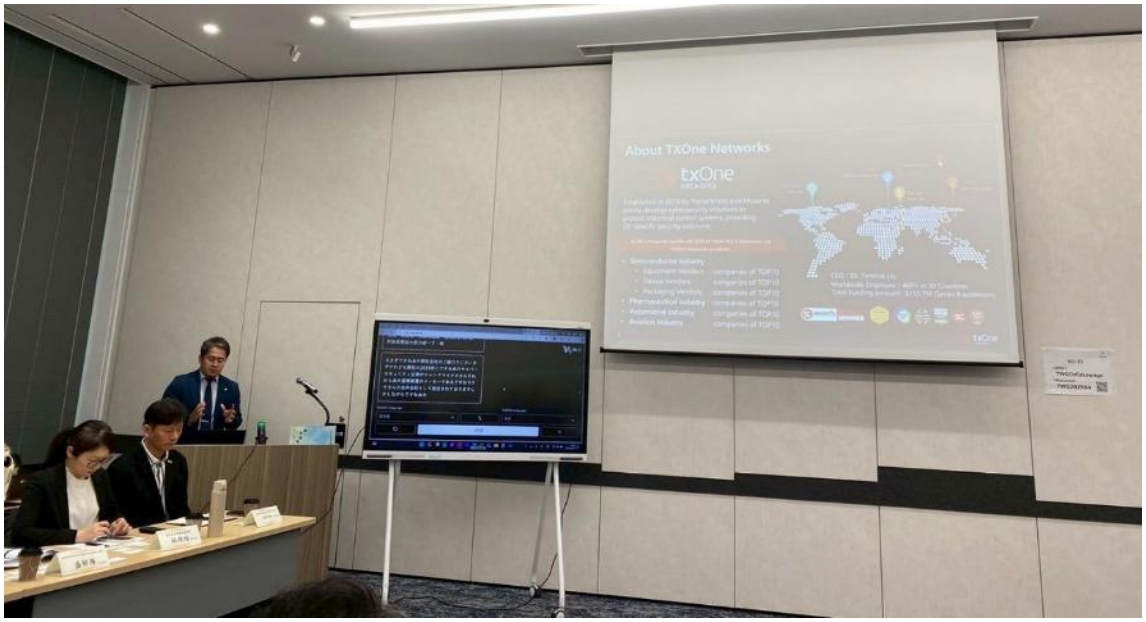


圖 44：TxOne 分享 SEMI E187 相關產品

資料來源：本計畫整理

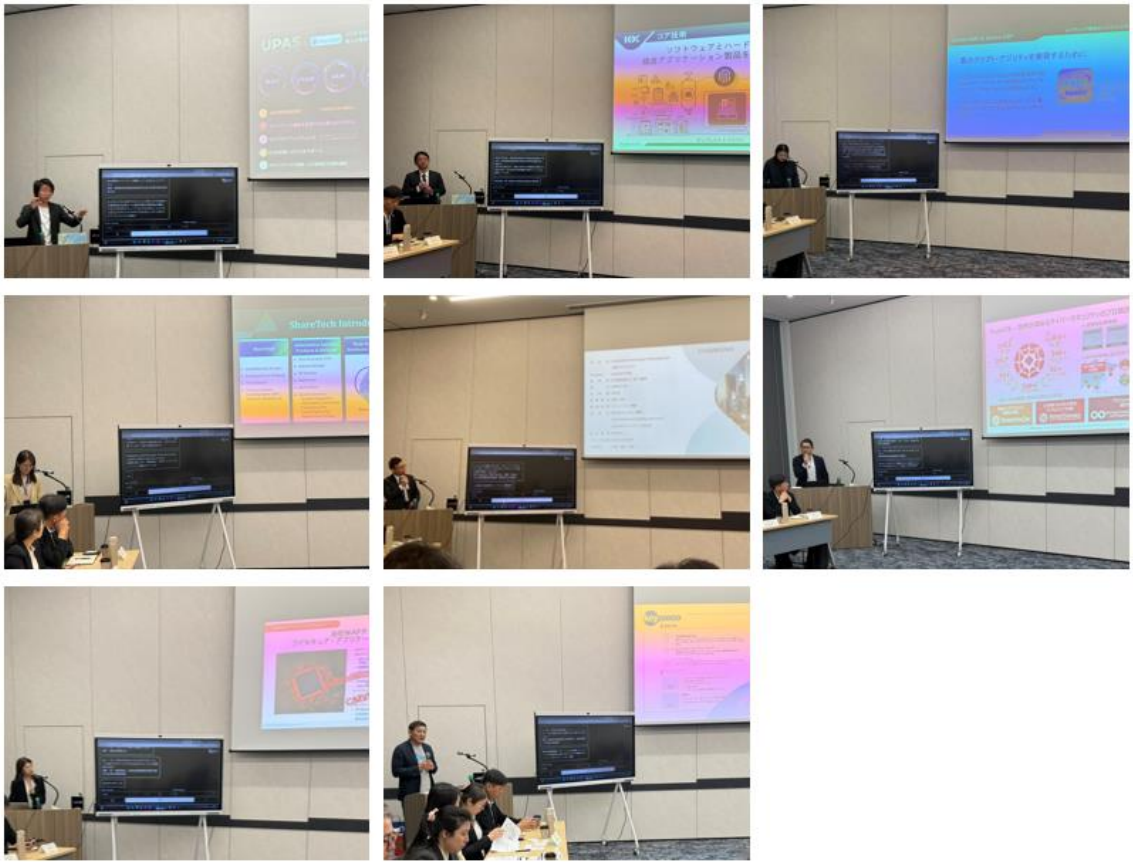


圖 45：各廠商向 CTC 分享資安解決方案

資料來源：本計畫整理

圖 46：數產署訪團與伊藤忠科技解決方案公司(CTC)團隊合影

資料來源：本計畫整理

八、觀摩「Pepper Parlor」機器人主題餐廳

（一） 地點：東京都澀谷區道玄坂 1-2-3 (東急 PLAZA 澀谷 5 樓)

（二） 簡介：

Pepper Parlor 坐落於東京澀谷東急 Plaza，為全球少數以「人機互動實境體驗」為核心的主題餐廳。店內部署 SoftBank 研發、鴻海製造的 Pepper 人型機器人，從迎賓帶位、送餐服務、桌邊互動到娛樂展演，完整呈現 AI 與機器人技術的商業化整合應用，堪稱日本服務型機器人實證場域之標竿案例。

1. 核心服務場景與技術亮點

店內機器人系統依功能分為四大模組。第一類為「智慧迎賓機器人」，搭載 3D 攝影機與紅外線感測器，可即時偵測顧客入店動線，透過頭部關節模擬鞠躬姿態，並以日英雙語問候。其胸前觸控螢幕同步顯示動態笑臉與促銷資訊，內建聲紋辨識系統能自動判別顧客年齡層——當偵測

到高頻童聲時，即刻切換為卡通音調與簡化版兒童菜單介面，展現高度情境適應能力。

「軌道送餐機器人」採用動態路徑規劃技術，運用即時 3D 環境建模與障礙物掃描功能，能在突發路徑阻斷（如移動中顧客）時自主繞行，相較傳統單線往返模式，有效降低碰撞風險。送達桌邊後，其螢幕自動顯示 QR 碼核銷介面，並透過語調頻譜分析模組偵測顧客情緒狀態。實測顯示，當系統判讀不耐煩語調時，將觸發三階段應對機制：即時語音道歉、訂單優先處理標記，以及後台管理系統警示，提升服務優化能力。

2. 深度互動與技術整合

「桌邊聊天機器人」已發展為全週期服務介面，整合多語種語意解析引擎（支援日文、英文、中文）與生成式 AI 對話模型。實測過程中，機器人不僅能流暢應答菜色問題，更可主動延伸話題，例如根據顧客點餐內容推薦搭配飲品，或結合占卜遊戲創造娛樂互動。其頭部視覺追蹤系統可模擬人類眼神接觸，頸部 12 軸關節則實現擬真點頭與側耳傾聽動作，提升對話臨場感。

「群體表演機器人」聚焦於運動控制技術驗證，中央舞台常態展演多機協作舞蹈。關鍵突破在於其分散式時序同步演算法，透過邊緣運算架構達成動作同步校準，即使單機臨時故障，系統仍能動態調整隊形維持演出完整性。此技術已取得 JIS 服務機器人安全認證，可擴展至大型展演場域應用。

3. 產業實證啟示與借鑑

Pepper Parlor 驗證多項關鍵技術整合，首先，建立「環境感知—語意解析—決策生成」的即時反饋迴路，解決傳統服務機器人指令延遲痛點；其次，開發情緒辨識資料庫，透過累計顧客微表情與語調樣本，提

高情感語音調變模型的準確率；最後，創新商業模式設計，將技術展示巧妙融入餐飲流程，創造體驗經濟收益。

對臺灣產業發展之啟示有三：(1)亟需建置開放式實證場域，促進大型語言模型與垂直領域知識庫（如餐飲 SOP、食安法規）對接；(2)強化「感測—決策—控制」技術鏈整合，特別是高噪環境下的語音接收與低延遲硬體響應；(3)借鏡日本產學研合作模式，該店技術骨幹來自早稻田大學人機互動實驗室與 SoftBank 的專利授權體系，以及鴻海製造，此種協作機制值得臺灣產學界參考。

圖 47：「Pepper Parlor」多機協作機器人實證環境

資料來源：本計畫整理

九、參訪獨立行政法人情報處理推進機構(IPA)

（一）日期：2025 年 04 月 24 日(四)

（二）地點：東京都文京區本駒込 2-28-8

（三）出席人員：

1. 台方出席人員名單

No.	單位/Organization	姓名/Name	職稱/Title
1.	數位發展部數位產業署	杜欣怡	簡任技正
		盛郁雁	專案規劃師
2.	PQC-CIA 資安產業聯盟	鄭嘉信	理事
3.	資訊工業策進會	蕭榮興	主任
4.	工業技術研究院	雷穎傑	技術副組長
		張懷文	專案人員

2. 日方出席人員名單

No.	單位/Organization	姓名/Name	職稱/Title
1.	安全中心 IT Security Center (ISEC)安全中心技術評測部 Security Technology Evaluation Department	神田　雅透	部長
		鷲見　拓哉	主任
		伊藤　忠彦	研究員
2.	安全中心 IT Security Center (ISEC)風險管理部控制系統組 Risk Management Department Industrial Control System Assessment	高見　穣	組長

（四）議程：

時間	當日流程
1600-1610	名片交換、雙方致詞
1610-1625	關心上次交流時的議題，分享後續狀況
1625-1635	工研院-PQC-後量子遷移的資安機會與挑戰
1635-1650	資策會-PQC 後量子遷移指引
1650-1705	PQC-CIA 分享 PQC 解決方案範例
1705-720	IPA 分享日本的 PQC 相關應對措施
1720-1755	意見交流 • 交流雙方 PQC 應用現狀 • 跨國合作交流可行性
1755-1800	交換禮品/合影

（五）參訪交流摘要：

本次會議主要針對物聯網產品安全功能進行交流與合作，包括對物聯網產品安全功能的推動、制定安全標準、與日本半導體廠商的合作，以及日本密碼安全的推動機制等方面進行深入探討，與 IPA 交流簡報詳見附件四。

1. 物聯網安全標準的跨境調和與產業生態共建

日本於 2025 年 3 月推出的物聯網產品安全標示制度「JC-STAR」，將通訊裝置與智慧設備分為四級資安認證體系，一二星級產品允許廠商自主宣告，高星級則需強化驗證機制。惟三星級以上需第三方實驗室檢測的規範，但目前檢測規範尚未公告。對於跨國實驗室認證的開放態度，為臺日合作創造技術接軌空間。臺灣方面提出兩大合作路徑：首先針對兩地物聯網資安標準的差異性，建議成立技術工作組進行測試項目對照與互認基準研擬；其次爭取臺灣檢測實驗室納入 JC-STAR 認證體系，待日方提供對接窗口後，將持續雙方標準的對接調和工作。

2. SEMI E187 標準的供應鏈協同與實務經驗輸出

隨著台積電九州廠量產時程逼近，日本半導體設備供應鏈面臨急迫的資安合規需求，此背景促使 SEMI E187 標準成為臺日技術合作焦點。日本 IPA 機構特別關注該標準的誕生歷程，尤其是 2018 年台積電機台中毒事件後，如何透過產業聯盟與國際組織協作，在 18 個月內完成從威脅分析到標準制定的全流程。IPA 預計將此過程轉化典範案例對日本設備供應商說明，協助日本業界理解供應鏈資安管理的核心要素。在實務層面，臺灣資安廠商已開發出符合 SEMI E187 的合規解決方案，此類解決方案能有效縮短日本設備商導入標準的學習曲線。因此雙方未來將規劃的線上技術交流會，由本署邀請臺灣的 SEMI E187 解決方案廠商分享，以支援日本在 SEMI E187 的導入。

3. 後量子密碼遷移的階段性協作策略

面對量子電腦威脅，臺灣在後量子密碼（PQC）發展腳步明顯領先日本。日本由 CRYPTREC 機構維持十年週期的密碼清單更新機制，雖在 2025 年啟動 PQC 部署環境建構計畫，但現行政策仍側重傳統密碼算法的持續使用，此保守態度源於日本金融與能源基礎設施的系統複雜性，以及主管機關對演算法替換風險的謹慎評估。相對地，臺灣透過工研院與資策會的推動，已建立從密碼盤點工具開發到產業聯盟組建的完整生態系，特別在中小企業導入層面累積實務經驗。

當前日本對 PQC 議題的重視程度仍低於臺灣技術發展進程，此落差創造潛在合作空間。臺灣業者可從三個層面切入：首先參與日方密碼盤點工具的開發專案，其次提供中小企業遷移解決方案，最後透過建立跨國應用案例提升技術能見度。隨著 2025 年日本啟動環境建構計畫，相關測試驗證與系統整合服務將成為關鍵商機所在。

圖 48：數產署訪團與獨立行政法人情報處理推進機構(IPA)交流情形

資料來源：本計畫整理

圖 49：數產署訪團與獨立行政法人情報處理推進機構(IPA)合影

資料來源：本計畫整理

這次與 IPA 在後量子密碼議題上的收穫非常豐盛，參訪團隊藉此瞭解了日本密碼安全的政策與做法，日本負責密碼安全議題的單位為密碼研究與評估委員會（Cryptography Research and Evaluation Committees, CRYPTREC），其任務為監測和評估日本政府推薦密碼清單的密碼安全性，並調查和審查密碼技術的適當實施和操作方法，旨在監測和評估電子政府採購應參考的密碼清單上所發布的密碼的安全性。由日本總務省（Ministry of Internal Affairs and Communications）和經濟產業省（Ministry of Economy, Trade and Industry）共同運營，它還有三個小組委員會，由日本資訊通信研究機構（National Institute of Information and Communications Technology, NICT）和日本資訊處理推進機構（Information-technology Promotion Agency, IPA）共同經營。

CRYPTREC 的主要目標是確保電子化政府的安全與可靠性，它會評估並監控密碼學的安全性，開發適用於電子政府採購的密碼清單（即 CRYPTREC 密碼清單），並針對電子政府推薦密碼的適當使用進行調查、檢查並發布相關指引

圖 50：日本密碼安全推動組織與其任務

資料來源：IPA 提供

CRYPTREC 密碼清單的第一版在 2003 年發布，第二版於 2013 年發布，而最新的第三版則是在 2023 年發布。CRYPTREC 密碼清單分為三個主要類別：「電子政府推薦密碼清單」，這些密碼在技術上安全高效且市場上易於取得；「候選推薦密碼清單」，這些密碼同樣技術上安全高效，但市場可用性較低；「監控密碼清單」，這些密碼在安全性上已存在技術弱點，但仍在市場上廣泛使用。最後，清單中的項目也可能會經歷一個檢視的程序後被移除。

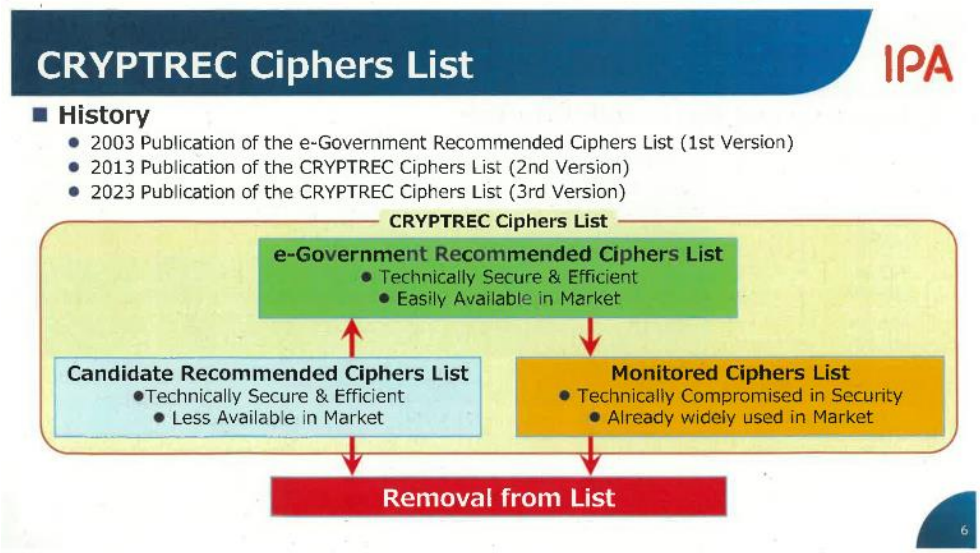


圖 51：日本密碼安全清單公告歷程與類型

資料來源：IPA 提供

我們在第三版 CRYPTREC 密碼清單中，可以在「電子政府推薦密碼清單」中，找到目前日本推薦的用於簽章的 DSA、ECDSA、EdDSA、RSA-PSS 等密碼演算法；用於加密的 RSA-OAEP，以及用於雜湊的 SHA 系列演算法等。值得注意的是，此清單中尚不包含任何剛公告的後量子密碼演算法。IPA 強調，雖然量子電腦對密碼學構成潛在威脅、日本官方也開始注意這個議題，但尚未納入第三版 CRYPTREC 密碼清單。

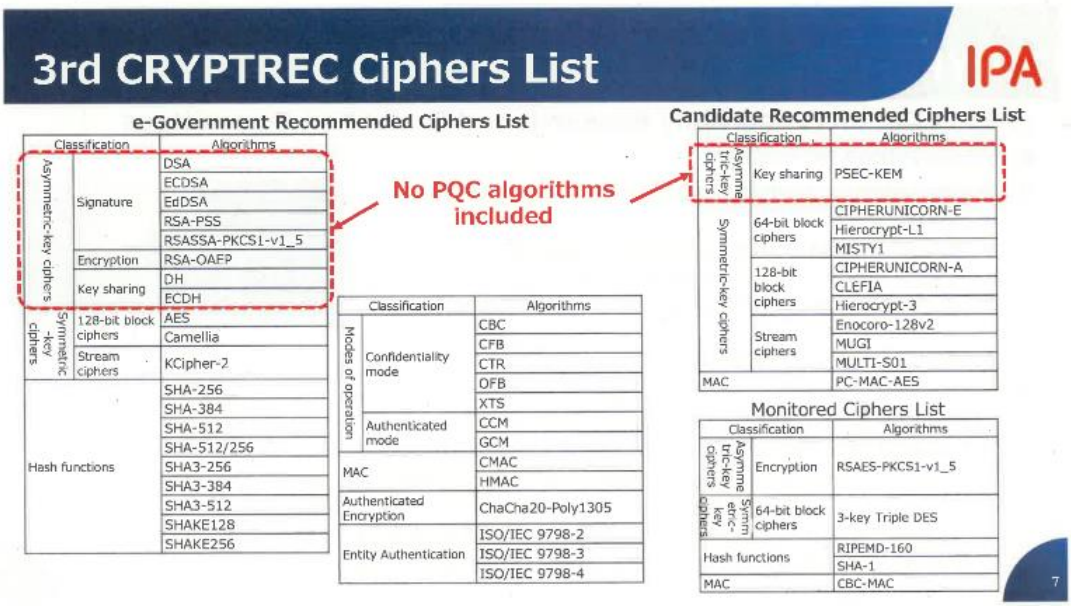


圖 52：日本最近一版安全密碼清單內容

資料來源：IPA 提供

本次交流也希望在後量子密碼議題創造合作機會，因此參訪團隊也特別以美國為例提醒日方，美國國家標準組織 NIST 已經預告 2030 年起禁用有風險的傳統加密簽章演算法，2035 年完成後量子密碼遷移，台灣數發部數產署也已經公佈了後量子密碼遷移指引，IPA 對此也表達興趣，並表示 CRYPTREC 正在關注包涵國際標準化進展和 PQC 遷移計畫在內的最新趨勢，2025 年 CRYPTREC 將開始為 PQC 部署準備環境，而每十年更新的安全密碼清單也預計於 2027 年啟動討論，因此可能會在下一個版本的安全清單中納入後量子密碼。我方也表達台灣已有後量子密碼的軟硬體解決方案供應商，後續將就如何支援日本的後量子密碼遷移持續交流討論合作機會。

整體來說，日本目前對 PQC 議題的重視程度尚未觸發，但可見的未來仍會啟動，我國則走得較前面，未來可思考如何在日本推動量子遷移過程中持續促成台日合作，讓臺灣業者有機會獲得商機。

十、參訪工研院日本辦公室

（一）活動時間：114 年 4 月 25 日(五)，上午 10:30~11:30

（二）活動地點：108-0073 東京都港區三田 1-2-18 TTD 大樓 3F

（三）出席人員：

1. 台方出席人員名單

No.	單位/Organization	姓名/Name	職稱/Title
1.	數位發展部數位產業署	杜欣怡	簡任技正
2.		盛郁雁	專案規劃師
3.	工業技術研究院	雷穎傑	技術副組長
4.		張懷文	專案人員
5.	資訊工業策進會	蕭榮興	主任

2. 工研院日本辦公室席人員名單

No.	單位/Organization	職稱/Title	姓名/Name
1.	工業技術研究院 日本辦公室	國際長	楊馬田
2.		部長代理	張璧伊
3.		部長代理	施虹宇(Jason)

（四）議程：

時間	當日流程
10:30-10:32	工研院日辦致詞（楊馬田國際長）
10:33-10:35	台灣方面致詞（杜欣怡簡任技正）
10:36-10:56	工研院日辦業務介紹（施虹宇部長）
10:56-11:25	交流與 Q&A
11:25-11:30	紀念合影

（五）參訪摘要：

ITRI 日本辦公室成立於 1987 年，以創新研發合作及產業鏈結為主軸，主動積極擔任臺日產官學研機構合作的有效橋梁，近年來配合院內的發展主軸，聚焦四個應用領域：智慧生活、健康樂活、永續環境及韌性社會。在執行策略上，期望透過：

1. 以技術、人才、制度國際化思維進行布局
2. 成為各單位的臺日業務的合作夥伴，接軌國際
3. 長期經營日本在地產官學研網脈
4. 以 2035 技術藍圖為依據，策略性促成臺日實質合作

因資安為打造韌性社會的重要一環，從 2023 年開始 ITRI 日本辦公室亦協助臺灣資訊安全協會(TWISA)來日本從事產學交流活動，包含參加 CEATEC 展會、拜會 CBC 商社、日本 TCI 研究創新中心等。

圖 53：工研院日本辦公室協助 TWISA 與日本產學交流記錄

資料來源：工研院日本辦公室提供

臺灣在半導體先進製程與 AI 硬體具全球領先地位，日本則在材料、設備與品質管理方面實力雄厚。九州地區則是日本半導體重鎮，隨著台積電在熊本設廠，工研院日本辦公室也開始參與大九州相關的活動，包含每年二月的熊本復興展、九月的福岡半導體展，以及包含跟日本北九州產業學術推進機構(FAIS)的交流。而我們的半導體資安標準 SEMI E187 也是跟台積電合作一起推動，後續相關的半導體資安合規產品的推動上，可朝大九州的市場方向規劃。

圖 54：工研院日本辦公室分享日本產學合作經驗

資料來源：本計畫整理

圖 55：數產署訪團與工研院日本辦公室合影

資料來源：本計畫整理

伍、心得及建議

(一) 重點成果

1. 本次活動為我國首次以臺灣資安館名義參展 IT Week Spring，開幕式由我國駐日代表李逸洋大使親臨會場開幕致詞，並匯集包含智慧資安、關楗、眾至資訊、杜浦、全景、優內控、如梭、奧義智慧及叡廷等 9 家公司共同參展，展出本土資安廠商所研發之零信任架構、AI 防禦、供應鏈資安、工控防護與後量子密碼等技術領域之資安產品與服務，展現我國多元資安技術量能。
2. 除參與前述展館活動外，也率領我國資安廠商拜訪日本大型系統整合商伊藤忠科技解決方案公司，除了分享臺灣推動半導體資安標準 SEMI E187 的經驗，也藉由每家資安業者的短講分享，讓 CTC 更了解我國資安業者的能量，創造後續我國資安廠商與日本大型系統商媒合機會。
3. 此外，本次訪團行程拜會 IPA 活動中，除掌握日本 IoT 設備資安標章的進度外，亦就 PQC 量子遷移議題進行意見交換，除分享我國量子遷移推動作法外，亦偕同 PQC-CIA 聯盟業者展示研發成果。IPA 對於臺灣已投入 PQC Ready 解決方案印象深刻，後續或可就此議題進行交流。
4. 另安排參訪高輪 Gateway City、日本科學未來館與 Pepper Parlor 等代表性智慧場域活動中，從高輪 Gateway City 展現城市層級資料平台與數位分身（Digital Twin）風險預警體系，未來可作為我國智慧場域佈建的參考樣板。科學未來館則將博物館轉型為社會創新與科技倫理實驗場，可做為我國未來沙崙基地升級規畫時參考；而 Pepper Parlor 實證場域結合機器人互動、AI 決策與商業場景融合，提供我國 AI 業者打造高互動應用場域之具體參照。

依據前述三項重點工作，均有助於提升我國資安產業在國際的能見度，且不論是日本大型系統業者 CTC 抑或是行政法人機構 IPA，均對於我國資安技術能

量給予正面評價。面對日本政府開始推動中小企業資安強化，我國資安業者相較日本大型商社具有更高性價比的技術方案，此為我國資安業者進入日本市場之優勢，可作為後續拓銷時參考。而最後一項場域觀摩，則進一步補足對日本資安應用實境與創新推動策略的理解。從高輪 Gateway City 所展現的智慧城市整合治理，到日本科學未來館將科技展示場域轉型為社會參與平台，以及 Pepper Parlor 結合 AI 技術與人機互動的商業應用模式，皆提供我國在智慧城市建構、AI 落地實證與公民科技推廣等層面寶貴的參考依據，也為未來深化臺日資安合作開啟更多跨域連結的可能性。

(二) 心得與建議

針對本次訪團參加 IT Week Spring 展會、場域觀摩與日本重要單位參訪交流相關討論等相關成果，綜整後續本署推動業務建議如下：

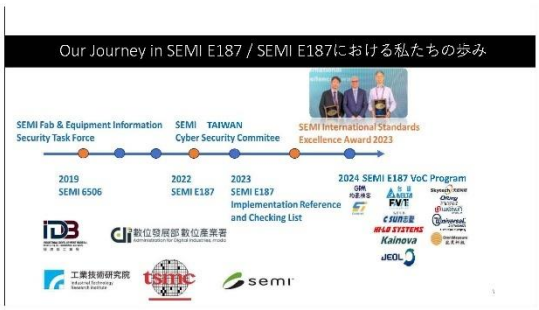
1. 持續參與日本資安相關展會：本次 IT Week Spring 以臺灣資安館名義展出，並由我國駐日代表李逸洋大使親臨會場主持開幕，有效提升我國國際能見度，另外，因 IT Week 為日本 IT 產業重要展會，吸引眾多買家前來，有助於臺灣資安業者開拓日本市場，並提升我國資安產業的國際能見度，建議未來可持續規劃辦理。
2. 半導體資安標準交流：因臺灣半導體產業佈局大九州，且半導體資安標準 SEMI E187 合規已逐漸落實於臺灣半導體業者，因此日本相關企業對此標準非常有興趣，建議可持續輔導臺灣資安業者投入 SEMI E187 標準合規產品開發，並持續辦理臺日半導體資安標準交流活動，據以協助推動臺灣資安業者進入當地市場。
3. PQC 量子遷移議題交流：本署推動產業投入 PQC 後量子加解密技術研發，於今(114)年資安大會展出相關解決方案，日本對於我國積極推動量子遷移且已有相關解決方案印象深刻，後續可規劃臺日交流媒合活動，

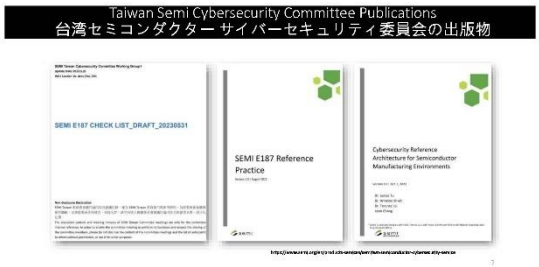
由我國資安業者分享 PQC 相關解決方案，讓日本更了解台灣資安業者的技術方案內容。

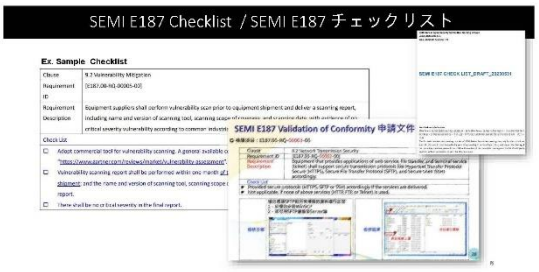
上述合作建議後續可評估透過臺日辦公室或工研院日本辦公室作為在地推動窗口，協助連結政策、廠商與技術實證資源，加速臺日資安與智慧應用產業之合作深化。

附件一、開幕式舞臺主題演講簡報

（一）SEMI E187 介紹－工業技術研究院







Quick Highlights of SEMI E187 Checklist
SEMI E187 チェックリストの注目ポイント

Category	Requirement ID	Document Verification
7.2 Operational System	[E187.00 RQ 00001 00]	OS Life Cycle Management
	[E187.00-RQ-00002-00]	Operational Manuals for System Patch/Update
8.2 Network Security	[E187.00-RQ-00003-00]	Network Protocol for Data Transmission
8.3 Network Configuration	[E187.00-RQ-00004-00]	Network Hardening
9.2 Vulnerability Management	[E187.00 RQ 00005 00]	Application Vulnerability Scanning and Mitigation
9.3 Malware Mitigation	[E187.00-RQ-00006-00]	Antivirus Scanning and Mitigation
9.4 Anti malware protection	[E187.00-RQ-00007-00]	Endpoint Protection Mechanism
	[E187.00-RQ-00008-00]	Peripheral I/O Control
9.5 Access Control	[E187.00-RQ-00009-00]	Authentication Methods
	[E187.00-RQ-00010-00]	Least Privilege Authorization
10.2 Security Logging	[E187.00-RQ-00011-00]	System and Security Logs last for one month
	[E187.00-RQ-00012-00]	Log Fields

Systematic Verification of Conformity (VoC)
適合性確認の体系的アプローチ

Case Study (Preface of VoC) / ケーススタディ（VoC序章）

[E187.00-RQ-00001-00]

Clause	7.2 Support for Operating System
Requirement ID	[E187.00-RQ-00001-00]
Requirement Description	Equipment supplier shall not ship equipment with OS that are not supported by the OS vendor (e.g., end of life).
Check List	

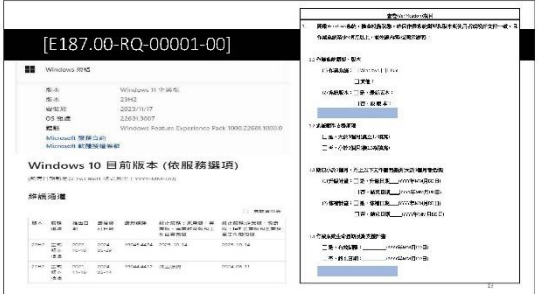
☐ Version number and scree shot to proof the OS support is valid for at least 12 months by the time of product release.

Some commonly used OSes could be found in the following links:

- Microsoft Windows: https://learn.microsoft.com/en-us/lifecycle/products/
- Redhat: https://access.redhat.com/support/policy/updates/errata/
- Ubuntu: https://wiki.ubuntu.com/Releases

☐ If OS support is valid less than 12 months, list the date to be end of support and the upgrading and patching plans accordingly.

[E187.00-RQ-00001-00]



The Checklist

- Baseline, Simple to implement
- Focus on security checks before shipment.
- This may lead to improvements in product design, manufacturing, and verification processes to ensure compliance.
- Introduce security scanning tools for vulnerability and malware detection, along with reporting tools

- ベースライン、実装が簡単
- 出荷前のセキュリティチェックに焦点を当てる。
- これにより、製品設計、製造、検証プロセスの改善が進み、コンプライアンスを確保できる可能性があります。
- 脆弱性およびマルウェア検出のためのセキュリティスキャンツールと、レポーティングツールを導入する。

SEMI E187 Compliance Toolkit / SEMI E187準拠ツールキット

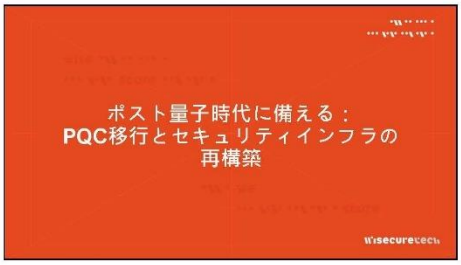
SEMI E187 Verification of Conformity (VoC)

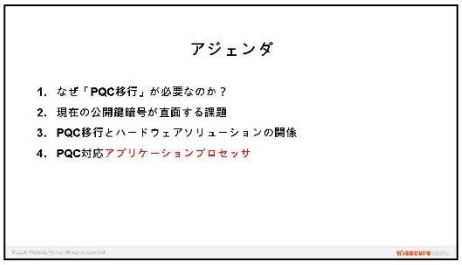

Prepare for your journey
to SEMI E187
工業技術研究院
Industrial Technology Research Institute
工研院量測技術發展中心
The National Measurement Laboratory

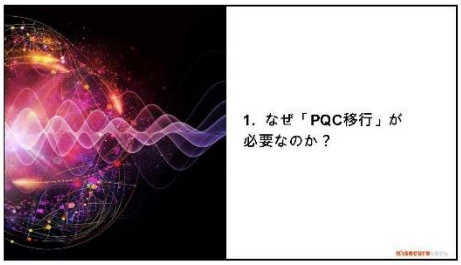

GMOサイバーセキュリティ byイエラエ、
台湾・工業技術研究院 情報通信研究ラボラトリと業務提携
～半導体業界サイバーセキュリティ標準「SEMI E187」の認証サービスを提供予定～
SC3 国際WG 半導体業界標準SEMI E187セミナーの開催を支援しました
GMO CYBER SECURITY
IERAE
https://www.gmo.jp/news/article/9382/

（二）後量子資安產業聯盟－匯智安全股份有限公司代表

2025/6/26







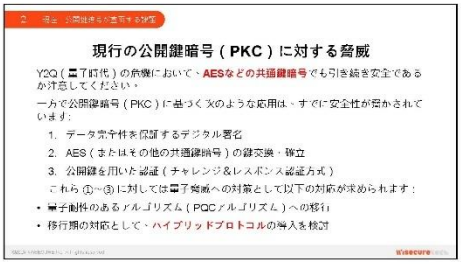
1

2025/6/26

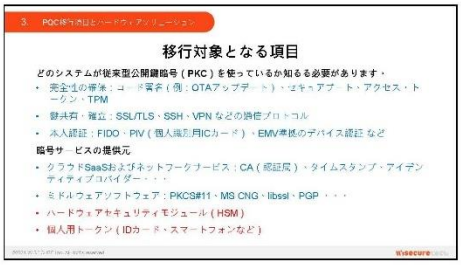
2

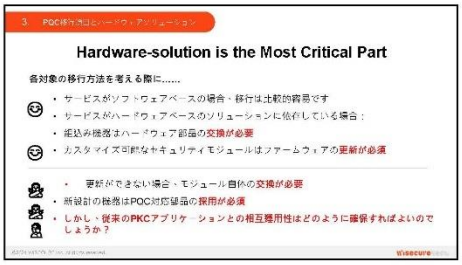

2. 現在、公開鍵暗号が直面する課題
公開鍵暗号（PKC）はあらゆる領域に活用されている
https
マイナンバーカード
MOICA
（共通用途身分証明用ICカード）
FIDO, FIDO2
スマートフォンアプリのダウンロード


2. 現在、公開鍵暗号が直面する課題
公開鍵暗号（PKC）のアプリケーションには
ハードウェアが不可欠
データ機密の安全確保
DRM
安全なコード署名
Code Signing
電子文書のデジタル署名
Document Signing
Regulation Compliance
HSM
アプリケーション
クラウドサービスの保護
Cloud Server
暗号化データの保護
Encryption (Data-at-rest)
通信伝送のセキュリティ保護
Secure Communication
ブロックチェーンにおけるデジタル署名の応用
Blockchain
IoTデバイスのセキュリティ保護
IoT Device


2. 現在、公開鍵暗号が直面する課題
現行の公開鍵暗号（PKC）に対する脅威
Y2Q（量子時代）の脅威において、AESなどの共通鍵暗号でも引き続き安全であるか注意してください。
一方で公開鍵暗号（PKC）に基づく次のような応用は、すでに安全性が脅かされています：
1. データ完全性を保証するデジタル署名
2. AES（またはその他の共通鍵暗号）の鍵交換・確立
3. 公開鍵を用いた認証（チャレンジ&レスポンス認証方式）
これら①～③に対しては量子脅威への対策として以下の対応が求められます：
• 量子耐性のあるアルゴリズム（PQCアルゴリズム）への移行
• 移行期の対応として、ハイブリッドプロトコルの導入を検討

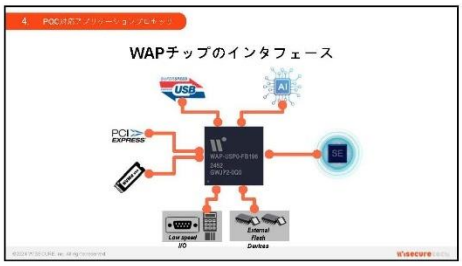

1. Y2Q…なぜ「PQC移行」が必要なのか？
2. 現在、公開鍵暗号が直面する課題
3. PQC移行項目とハードウェアソリューション

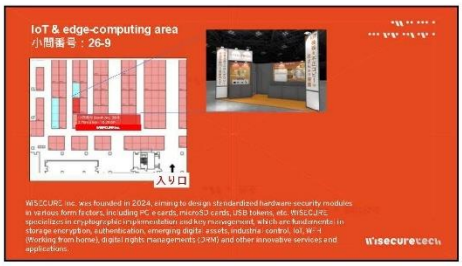

3. PQC移行項目とハードウェアソリューション
移行対象となる項目
どのシステムが従来型公開鍵暗号（PKC）を使っているか知る必要があります。
• 完全性の確保：コード署名（例：OTAアップデート）・セキュアブート・アクセス・トークン・TPM
• 鍵共有・確立：SSL/TLS・SSH・VPNなどの通信プロトコル
• 本人認証：FIDO・PIV（個人識別用ICカード）・EMV準拠のデバイス認証など
暗号サービスの提供元
• クラウドSaaSおよびネットワークサービス：CA（認証局）・タイムスタンプ・アイデンティティプロバイダー・・・
• ミドルウェアソフトウェア：PKCS#11・MS CNG・libssl・PGP・・・
• ハードウェアセキュリティモジュール（HSM）
• 個人用トークン（IDカード・スマートフォンなど）


3. PQC移行項目とハードウェアソリューション
Hardware-solution is the Most Critical Part
各対象の移行方法を考える際に……
• サービスがソフトウェアベースの場合、移行は比較的容易です
• サービスがハードウェアベースのソリューションに依存している場合：
• 組込み機器はハードウェア部品の交換が必要
• カスタマイズ可能なセキュリティモジュールはファームウェアの更新が必須
• 更新ができない場合、モジュール自体の交換が必要
• 新設計の機器はPQC対応部品の採用が必須
• しかし、従来のPKCアプリケーションとの相互運用性はどのように確保すればよいのでしょうか？


1. Y2Q…なぜ「PQC移行」が必要なのか？
2. 現在、公開鍵暗号が直面する課題
3. PQC移行とハードウェアセキュリティモジュール（HSM）
4. PQC対応アプリケーションプロセッサ


4. PQC対応アプリケーションプロセッサ
当社WAPチップ：
ワイセキュア・アプリケーション・プロセッサ
Submitting FIPS 140-3
CAVP
CMVP (Level 3)

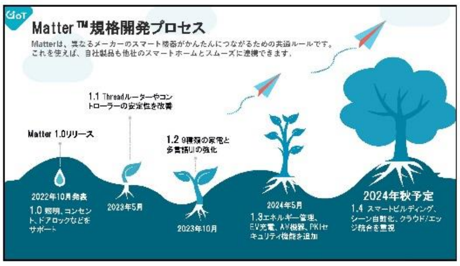




（三）零信任

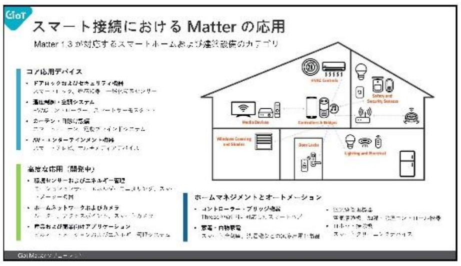
1. 全景軟體股份有限公司

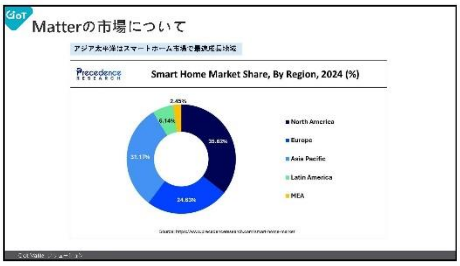

cybertrust CHANGING
Matterソリューション
スマート市場の動向
New Thinking on Smart Home Device Security under Zero Trust

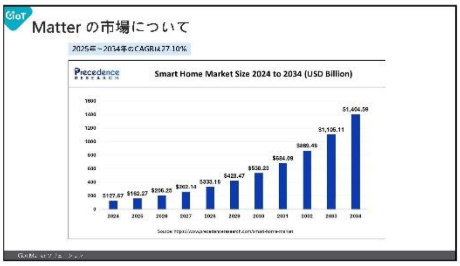

Matter™規格開発プロセス
Matterは、異なるメーカーのスマート機器がかんたんにつながるための共通ルールです。
これを使えば、自社製品も他社のスマートホームとスムーズに連携できます。
1.1 Threadルーターやコントローラーの安定性を改善
Matter 1.0リリース
1.2 9種類の家電と多言語UIの強化
2022年10月発表
1.0 照明、コンセント、ドアロックなどをサポート
2023年5月
2023年10月
2024年5月
1.3エネルギー管理、EV充電、AV機器、PKIセキュリティ機能を追加
2024年秋予定
1.4 スマートビルディング、シーン自動化、クラウド/エッジ統合を重視


目次
1.Matterの規格と日本の制度
2.Matterの市場について
3.スマート家電の課題
4.Matterソリューション


Japan Cyber STAR (JC-STAR)
日本版サイバーセキュリティ技術評価基準に基づくラベリング制度「JC-STAR」
JC-STAR
Scheme logo
Conformance labels
Japan Cyber STAR (JC-STAR): "Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements" is a Japanese labeling scheme that confirms the conformance of IoT products to conformance requirements (security technical requirements) based on its own standards, while also harmonizing with domestic and international standards such as ETSI EN 303 645 and NISTIR 8425.


スマート接続における Matter の応用


Matterの市場について
アジア太平洋はスマートホーム市場で最速成長地域
Precedence Research
Smart Home Market Share, By Region, 2024 (%)
2.45%
6.54%
39.63%
25.17%
24.63%
North America
Europe
Asia Pacific
Latin America
MEA


Matter の市場について
Precedence Research
Smart Home Market Size 2024 to 2034 (USD Billion)
$127.67
$162.27
$206.25
$262.14
$333.18
$423.47
$538.23
$684.09
$869.48
$1,105.11
$1,404.59
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034


Matterの市場について
Google
SmartThings
Apple Home
amazon alexa

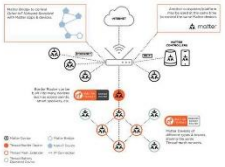
Matterの市場について

2025年に起きる変化

1. スマートスピーカーの専用スマートホームハブの重要性が低下
2. MATTERがスマートホームの接続プロセスを簡素化
3. MATTERのCRA対応が可能かウォッチする企業が増える

matter 安全なスマート接続

- **ローカル接続、クラウド依存なし**
- **Threadプロトコルによるシームレス通信**
- **シンプルなセットアップでスムーズな自動化**



スマート家電の課題

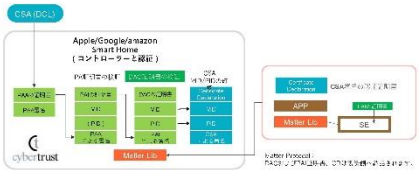
主要な課題

1. 相互運用性の問題

2. セキュリティ脅威

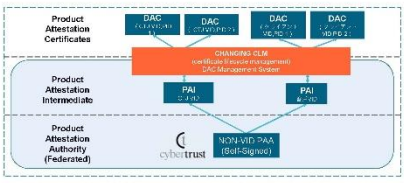
3. 法規制のプレッシャー

CSA Matterプロトコルにより実現されるセキュリティと相互運用性



Non-VID PAAソリューション

2つの方法：

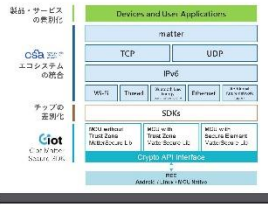


MATTER関連で対応可能なサービス

-DACセキュアプロビジョニング
-Matter Secure SDK
-セキュリティチップ内蔵DACまたは委託書き込み
-Matter over Threadソリューション

Matterはエコシステム統合を促進し、製品の差別化を可能にする

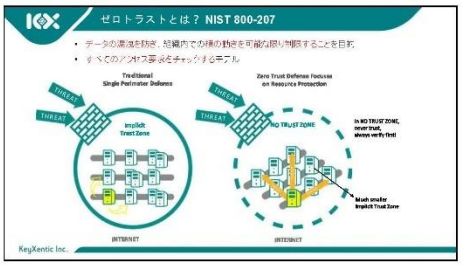
Ciot Matter Secure SDK がこの実現を支援します

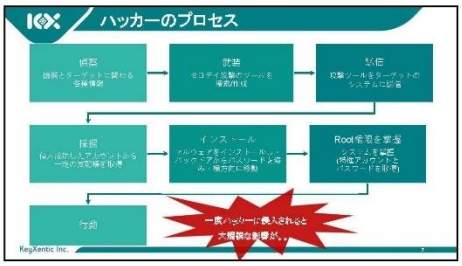


2. 關楗股份有限公司

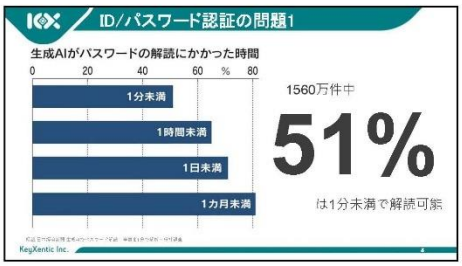
2025/6/26

1


ゼロトラストとは？ NIST 800-207
KeyXentic Inc.

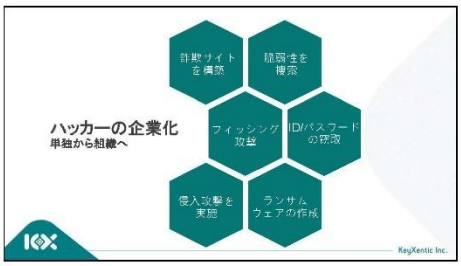

ハッカーのプロセス
KeyXentic Inc.

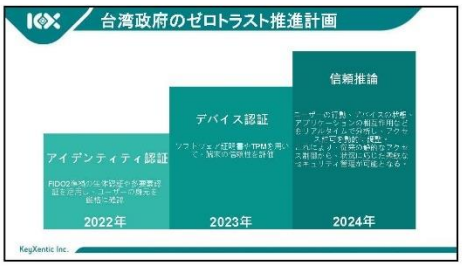

2
ハッカーはすぐ近くに

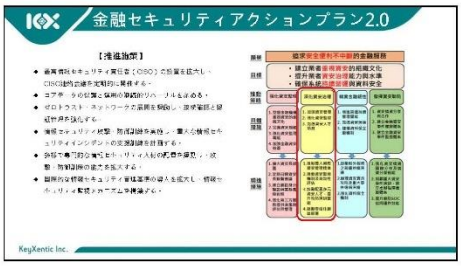

ID/パスワード認証の問題1
生成AIがパスワードの解読にかかった時間
1分未満
1時間未満
1日未満
1カ月未満
1560万件中
51%
は1分未満で解読可能
KeyXentic Inc.


ID/パスワード認証の問題2
ダークウェブで
① 確認されている認証情報
120億件以上
② 82% は重複利用
KeyXentic Inc.

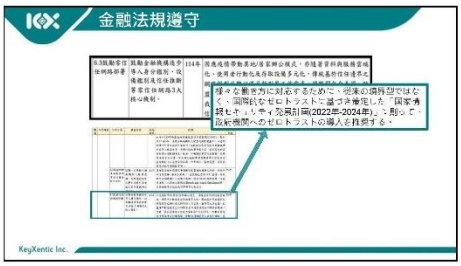

3
台湾政府による
ゼロトラストの取り組み


ハッカーの企業化
単独から組織へ
詐欺サイトを構築
脆弱性を探索
フィッシング攻撃
ID/パスワードの窃取
侵入攻撃を実施
ランサムウェアの作成
KeyXentic Inc.

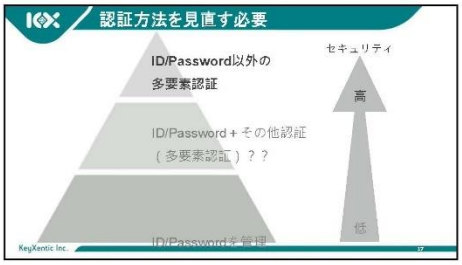

台湾政府のゼロトラスト推進計画
アイデンティティ認証
2022年
デバイス認証
2023年
信頼推論
2024年
KeyXentic Inc.


金融セキュリティアクションプラン2.0
【推進施策】
KeyXentic Inc.


まとめ


金融法規遵守
KeyXentic Inc.


現状
IDパスワードは
流出している
使い回されている
前提での運用が必要
KeyXentic Inc.


認証方法を見直す必要
ID/Password以外の
多要素認証
ID/Password + その他認証
（多要素認証）？？
ID/Passwordを管理
セキュリティ
高
低
KeyXentic Inc.


導入企業
金融
企業
政府
軍
LINE Bank
NSW
TAIPEI
MEDIATEK
FATC
KeyXentic Inc.


KeyXenticについて
全製品Made in Taiwan、開発製品の現地PSD

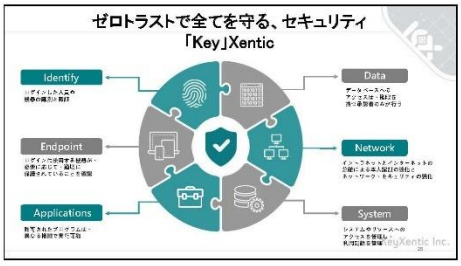

KeyXentic Inc.
Achievement
License
KeyXentic Inc.


コア技術
ソフトウェアとハードウェアの
統合アプリケーション製品を独自に研究開発
オンプレミス & クラウド


KeyXentic プロダクト KX701
KX701 FIDO2 NFCトークン
KX701
SMART
TOKEN


プロダクト Keyper–総合的な管理プラットフォーム
Keyper


KeyXentic プロダクト KX901
KX901 FIDO2 指紋認証トークン

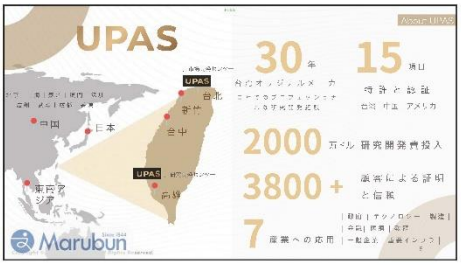

ゼロトラストで全てを守る、セキュリティ
「Key」Xentic
Identify
Data
Endpoint
Network
Applications
System


Thank you
CEO
Sean Hung
営業部長
古舘 侑樹
お問合せ先
東1ホール
ブース番号 8-18
KeyXentic


日本での期待
台湾と日本は
地政学的に似ている
力を合わせて
日本を守る
日本の
ビジネスパートナー
を募集

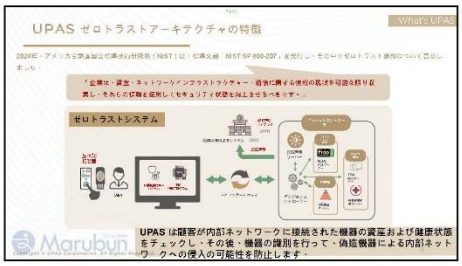
3. 優內控股份有限公司

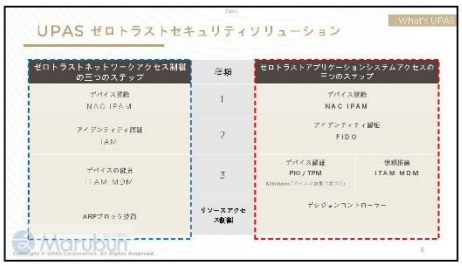
2025/6/26



1

2025/6/26





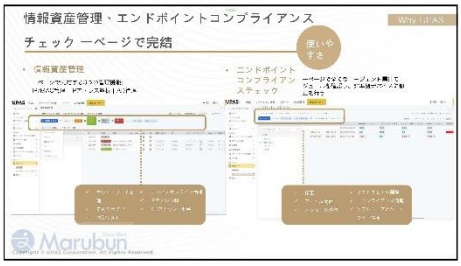
2


UPASゼロトラストセキュリティソリューション
NAC
IPAM
IAM
ITAM
MDM
一括で解決
Why UPAS


ホームダッシュボード 内部ネットワーク
デバイス情報の可視化
使いやすさ
Why UPAS

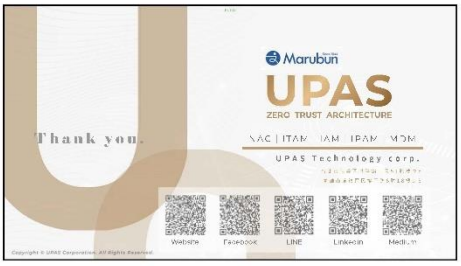

UPASゼロトラストセキュリティソリューション
Why UPAS


基本設定 ポリシー設定 一ページで完結
簡単インストール
Why UPAS


情報資産管理・エンドポイントコンプライアンス
チェック 一ページで完結
使いやすさ
Why UPAS


WHY CHOOSE US?
他社
ネットワークアクセス制御製品
+
他社
資産管理製品
=
UPAS
価格が安い
導入が簡単
効率的な運用・保守

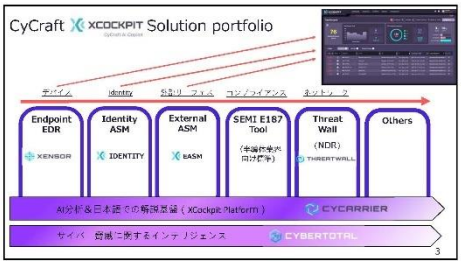

UPAS ZTAトリプル防御ライン
情報漏洩防止
ハッキング防御
運用保守
100%の資産インベントリを実現＋98%以上のAgentカバレッジ率
企業の情報漏洩防止・ハッキング防御・運用保守能力を全面的に向上

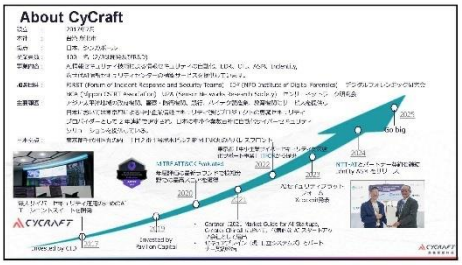

Thank you.
UPAS
ZERO TRUST ARCHITECTURE
NAC | ITAM | IAM | IPAM | MDM
UPAS Technology corp.

附件二、技術成果發表會簡報

（一）奧義智慧科技股份有限公司

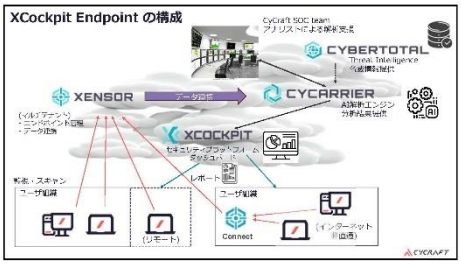
2025/6/26





1

2025/6/26



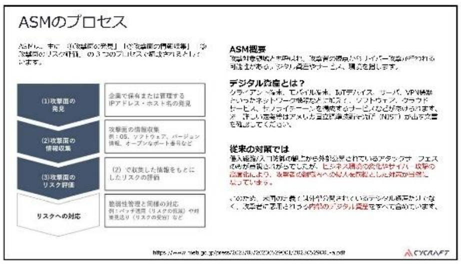
EDR：Endpoint Detection & Response

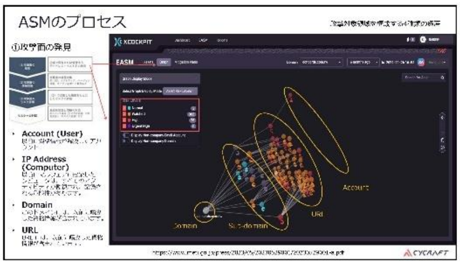
EASM：External Asset Management

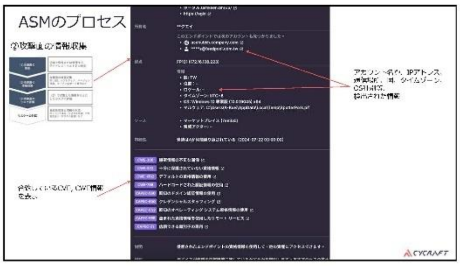
アタックサーフェスマネジメント

2

2025/6/26

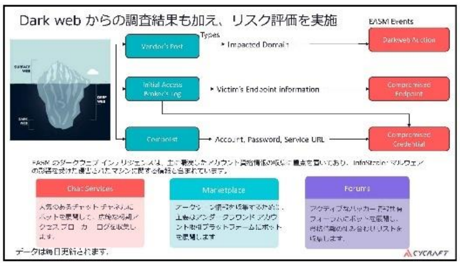


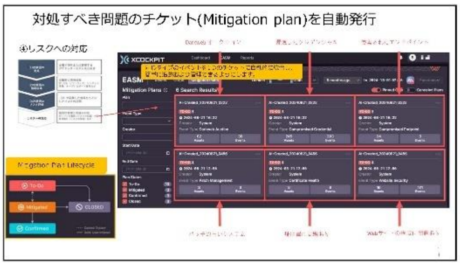




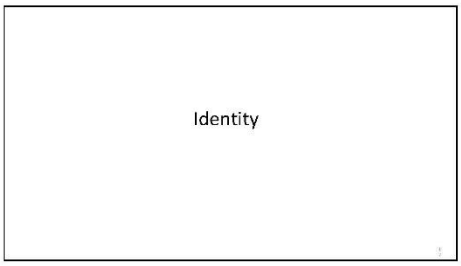
3

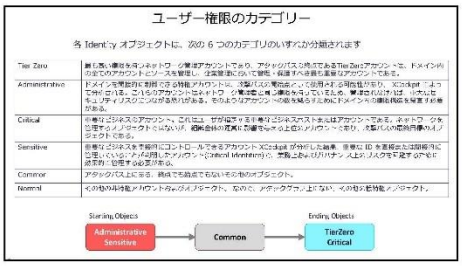
2025/6/26



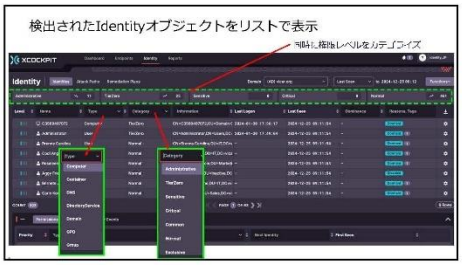


4

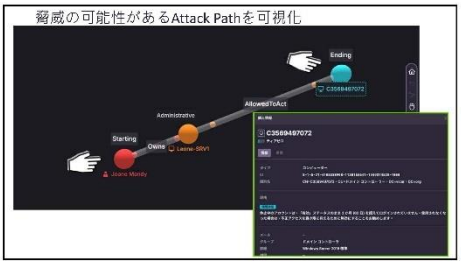

Identity


ユーザー権限のカテゴリー
各 Identity オブジェクトに、次の 6 つのカテゴリのいずれかが分類されます
Tier Zero
Administrative
Critical
Sensitive
Common
Normal
Starting Objects
Administrative
Sensitive
Common
Ending Objects
TierZero
Critical

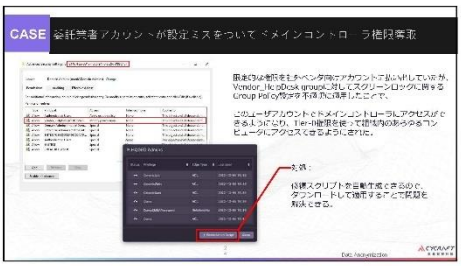

AD関連のサイバー被害
KADOKAWAサイバー攻撃の概要
Active Directoryを悪用した事例（2/3）
セキュリティ対策Lab
今「AD」を絶対見直すべきワケ。“侵害は前提前”攻撃者がこぞって狙う「恐怖の実態」


検出されたIdentityオブジェクトをリストで表示
可視化、権限レベルをカテゴライズ
Identity

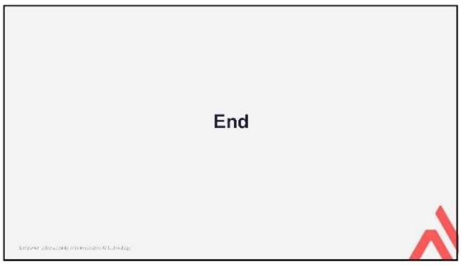

脅威の可能性があるAttack Pathを可視化
Identity
Attack Paths


脅威の可能性があるAttack Pathを可視化
Ending
AllowedToAct
Administrative
Starting
Owns
C3569497072


脅威の可能性があるAttack Pathを可視化
Attack Paths


CASE
委託業者アカウントが設定ミスをついてドメインコントローラ権限奪取

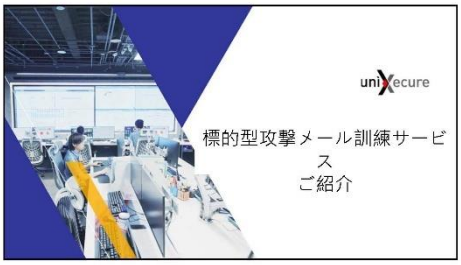

XCOCKPIT IDENTITY
Active Directory, Entra ID のセキュリティを強化します。
CyCraftが支援するADの運用の特徴
- アカウントセキュリティ設定の診断、ISMS監査を支援
30日間のトライアルで、導入効果を確認
2通りのデプロイ方法
エージェントレス
エージェント
インストール先
AD Server
スキャンタイミング
任意でScan アプリを実行、CyCraft Cloud にアップロード
1/Day
評価タイミング
アップロード後
1/Day
契約形態
One Time(30 days), Annual(1 Year)
Annual(1 Year)
キャンペーン内容及び、条件
- ユーザーライセンス数による設定となります。
- ライセンス費用
100ユーザーの場合 ¥158,800
200ユーザーの場合 ¥317,600
500ユーザーの場合 ¥794,000
評価お申し込みはこちらから ↓
https://www.cycraft.com/ja/contact-us


End

7

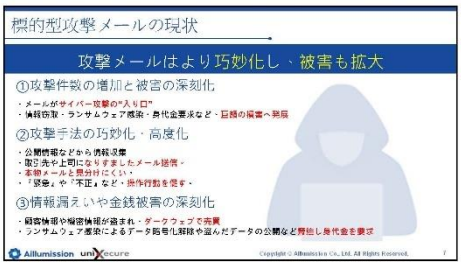
（二）智慧資安科技股份有限公司

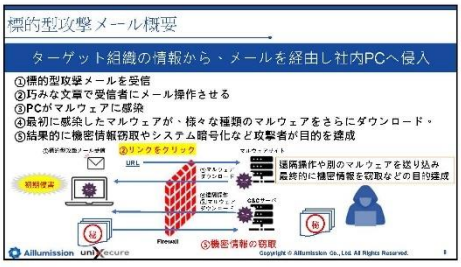
2025/6/26



1

2025/6/26

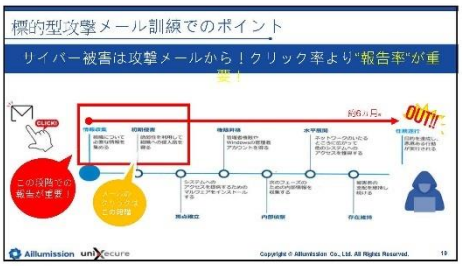




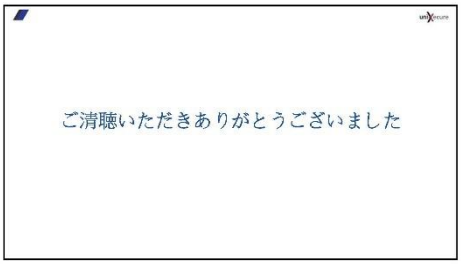
2


標的型攻撃メール訓練の目的
リイバー攻撃はツールだけでは防げない・人への継続教育が重要！
脆弱性の把握
セキュリティ意識の向上
インシデント対応力の強化
セキュリティ文化の醸成
Ailumission uniXecure
Copyright © Ailumission Co., Ltd. All Rights Reserved.


標的型攻撃メール訓練フロー
訓練プラットフォーム＋講習により、受講者のセキュリティ意識を向上
配信準備
メール配信
Ailumission uniXecure
標的型攻撃メール
Human Error Insight System
PLATFORM
Ailumission uniXecure
Copyright © Ailumission Co., Ltd. All Rights Reserved.

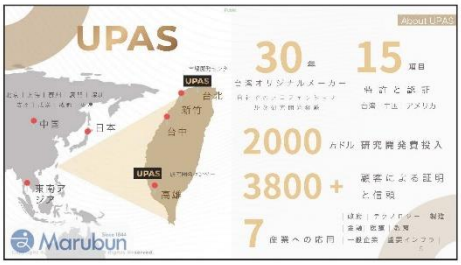

標的型攻撃メール訓練でのポイント
リイバー被害は攻撃メールから！クリック率より"報告率"が重要！
CLICK!
OUT!!
Ailumission uniXecure
Copyright © Ailumission Co., Ltd. All Rights Reserved.


ピンポーン!!
クイズ


ご清聴いただきありがとうございました

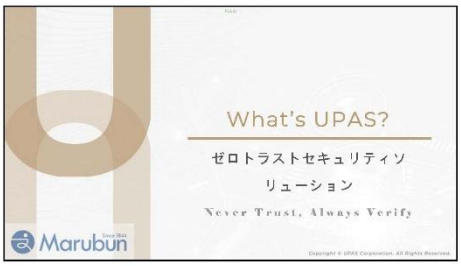
（三）優内控股份有限公司

2025/6/26

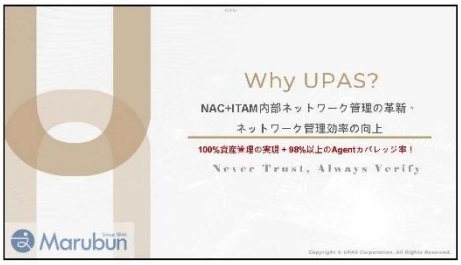


1

2025/6/26



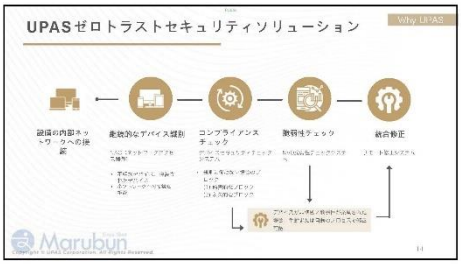
2

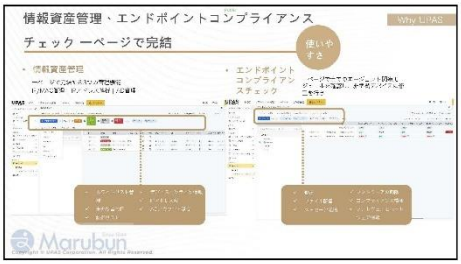

Why UPAS?
NAC+ITAM内部ネットワーク管理の革新、
ネットワーク管理効率の向上
100%資産※理の実現＋98%以上のAgentカバレッジ率！
Never Trust, Always Verify
Marubun

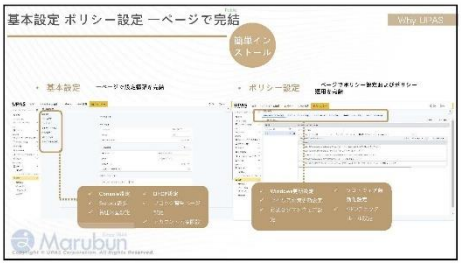

Why UPAS
UPAS NAC+ITAM統合管理 境界防御の更なる強化
NAC
ITAM
100%
98%
Agent-based
ハッキング防御
80% 98%
情報漏洩防止
80% 95%
端同保守
90% 98%
Marubun


Why UPAS
内部ネットワーク管理の革新！NAC+ITAMの2つの管理 vs 単一プラットフォームによる統合管理
NAC・ITAMの2つの管理
NAC+ITAM 統合管理
単一平台 集中管理
自動化された精密管理・隙間のない防御
Marubun


Why UPAS
UPAS 98% Agent 完璧な防御
UPAS
Agentless
100%
80%
20%
脆弱性修正技術
全体のAgent展開成功率
98%
Marubun


Why UPAS
UPASゼロトラストセキュリティソリューション
設備の内部ネットワークへの接続
柔軟なデバイス類別
コンプライアンスチェック
脆弱性チェック
統合修正
Marubun


Why UPAS
情報資産管理、エンドポイントコンプライアンスチェック ーページで完結
使いやすさ
Marubun


Why UPAS
基本設定 ポリシー設定 ーページで完結
簡単インストール
Marubun


Why UPAS
ホームダッシュボード 内部ネットワークデバイス情報の可視化
使いやすさ
Marubun

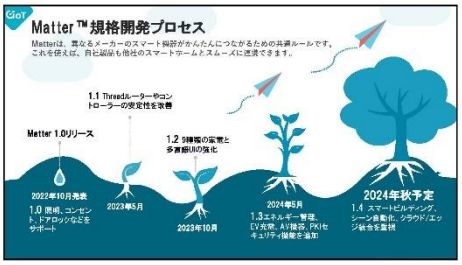

UPAS ZTAトリプル防御ライン
情報漏洩防止
機密データの流出防止
ハッキング防御
ハッキング侵入の防止
運用保守
全面的なデバイス運用管理
✓ 100%の資産インベントリを実現＋98%以上のAgentカバレッジ率
✓ 企業の情報漏洩防止、ハッキング防御、運用保守能力を全面的に向上


Thank you.
Marubun
UPAS
ZERO TRUST ARCHITECTURE
NAC | ITAM | IAM | IPAM | MDM
UPAS Technology corp.
Website
Facebook
LINE
LinkedIn
Medium


WHY CHOOSE US?
他社
ネットワークアクセス制御製品
＋
他社
資産管理製品
＝
UPAS
価格が安い
導入が簡単
効率的な運用・保守

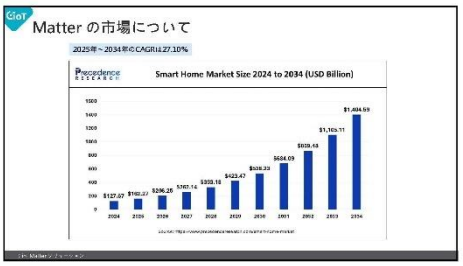
（四）全景軟體股份有限公司

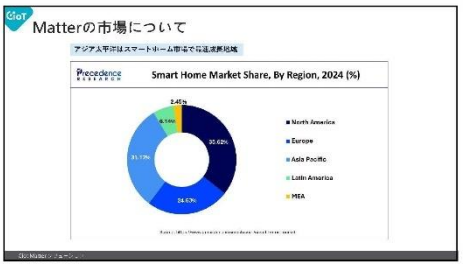
2025/6/26

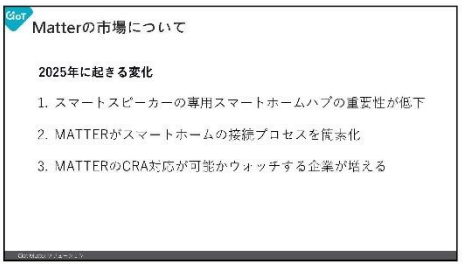


1

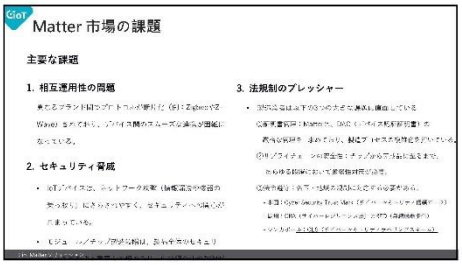
2025/6/26

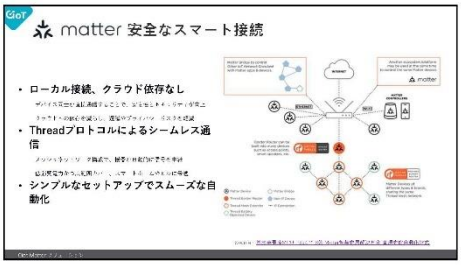




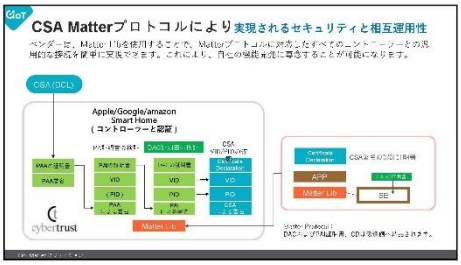


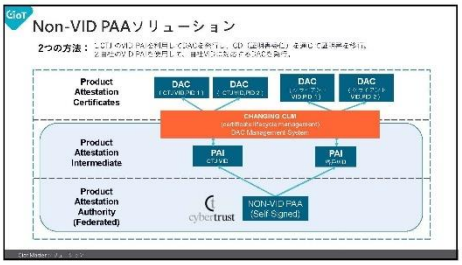
2


Matter 市場の課題
主要な課題
1. 相互運用性の問題
2. セキュリティ脆弱
3. 法規制のプレッシャー

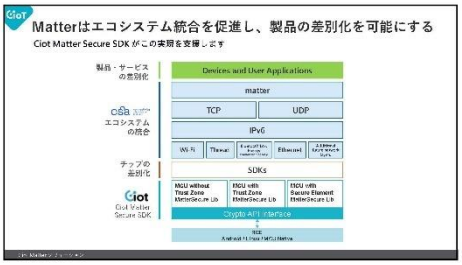

matter 安全なスマート接続
• ローカル接続、クラウド依存なし
• Threadプロトコルによるシームレス通信
• シンプルなセットアップでスムーズな自動化


スマート接続における Matter の応用
Matter 1.3 が対応するスマートホームおよび医療機器のカテゴリ
コア応用デバイス
高度な応用（開発中）
ホームネットワーク接続デバイス
ホームマネジメントとオートメーション


CSA Matterプロトコルにより実現されるセキュリティと相互運用性
CSA (DCL)
Apple/Google/amazon
Smart Home
（コントローラーと開発）
cybertrust
Matter Lib
SE


Non-VID PAAソリューション
2つの方法：
Product Attestation Certificates
DAC
CHANGING CLM
Product Attestation Intermediate
PAI
Product Attestation Authority (Federated)
cybertrust
NON-VID PAA (Self-Signed)


Ciot
共に創る、安全・高品なMatter製品
THANK YOU !
CHANGING

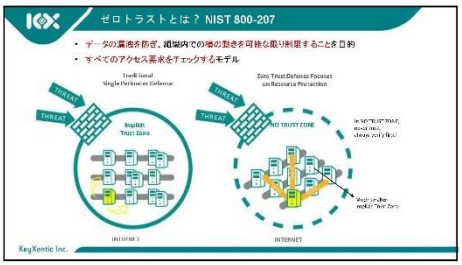

Matterはエコシステム統合を促進し、製品の差別化を可能にする
Ciot Matter Secure SDK がこの実現を支援します
製品・サービスの差別化
エコシステムの統合
チップの差別化
Ciot Matter Secure SDK
Devices and User Applications
matter
TCP
UDP
IPv6
SDKs
Crypto API Interface

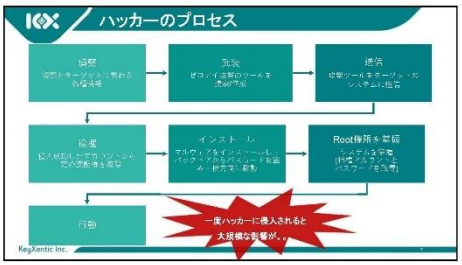
（五）關健股份有限公司

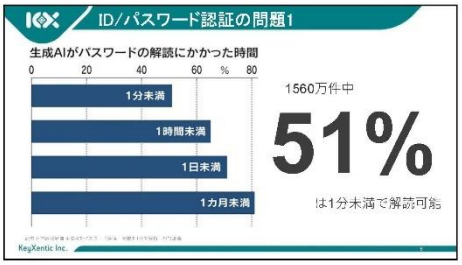
2025/6/26

1

2025/6/26







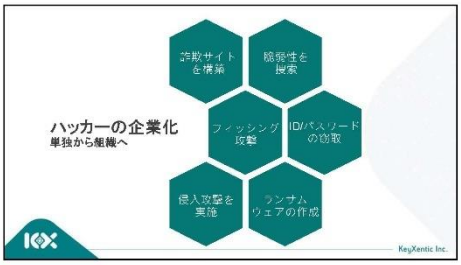
2

ID/パスワード認証の問題2

ダークウェブで

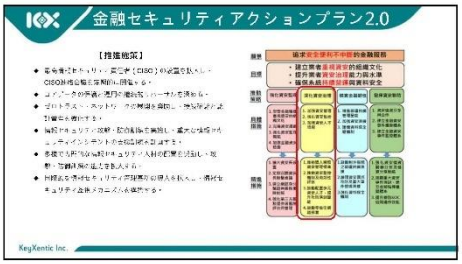
① 確認されている認証情報
120億件以上

② **82%** は重複利用

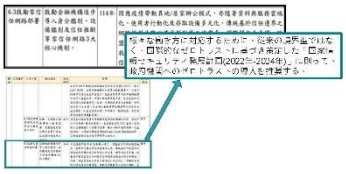


台湾政府のゼロトラスト推進計画

金融セキュリティアクションプラン2.0



金融法規遵守

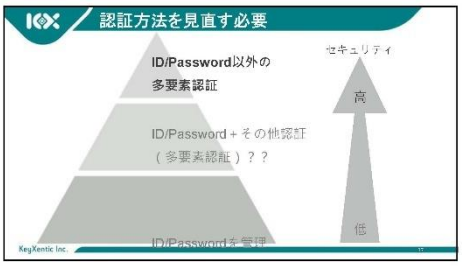


現状

ID/パスワードは

流出している
使い回されている

前提での運用が必要


認証方法を見直す必要
ID/Password以外の
多要素認証
ID/Password＋その他認証
（多要素認証）？？
ID/Passwordを管理
セキュリティ
高
低
KeyXentic Inc.


導入企業
企銀
企業
政府
軍
LINE Bank
NSW
TAIPEI
MEDIATEK
HongLeong Bank
FATC
KeyXentic Inc.


KeyXenticについて
全製品Made in Taiwan、開運製品の開発R&D

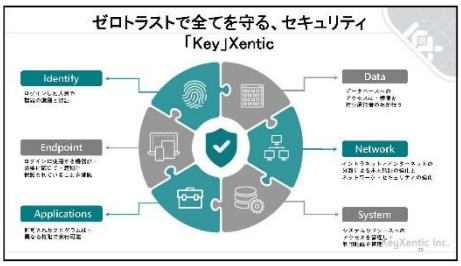

KeyXentic Inc.
2017年設立
資本金
2億7000万円
ID認証
権限授与
データ暗号
生体認証
FIDO
20年
IT関係領域
での実績
全シリーズ
Made in Taiwan
Achievement
License
2019ゴールデンリップルアワード
スマートアプリケーション部門チャンピオン
2019アジア太平洋ITアワードでダブル銀賞を受賞
台湾経済部工業証充局認定情報セキュリティサービス機関
2023 日本 シリーズA 投資を受け入れ
KeyXentic Inc.


コア技術
ソフトウェアとハードウェアの
統合アプリケーション製品を独自に研究開発
BYOK
PKI
AAIT
HSM
E-Signature
CA
Authentication
MFA
SSO
Encryption
e-KYC Integration
オンプレミス & クラウド
KeyXentic Inc.


KeyXentic プロダクト KX701
KX701 FIDO2 NFCトークン
KX701
SMART
TOKEN
fido
CERTIFIED
KeyXentic Inc.


プロダクト Keyper–総合的な管理プラットフォーム
Keyper
KeyXentic Inc.


KeyXentic プロダクト KX901
KX901 FIDO2 指紋認証トークン
fido
CERTIFIED
KeyXentic Inc.


ゼロトラストで全てを守る、セキュリティ
「Key」Xentic
Identify
Endpoint
Applications
Data
Network
System


Thank you
CEO
Sean Hung
営業部長
古舘　侑樹
お問合せ先
東1ホール
ブース番号 8-18
KeyXentic

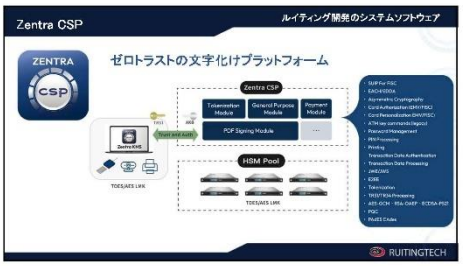

日本での期待
台湾と日本は
地政学的に似ている
力を合わせて
日本を守る
日本の
ビジネスパートナー
を募集

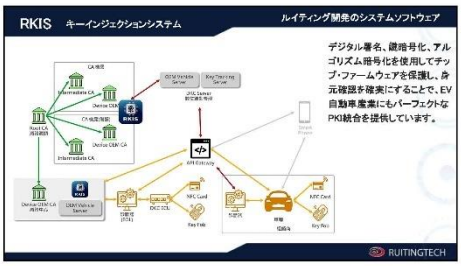
（六）叡廷股份有限公司

2025/6/26

1

2025/6/26





2


▪ビデオご覧ください
私たちの技術は、未来のデジタル
セキュリティを塗り替えています。
RUITINGTECH
RUITINGTECH

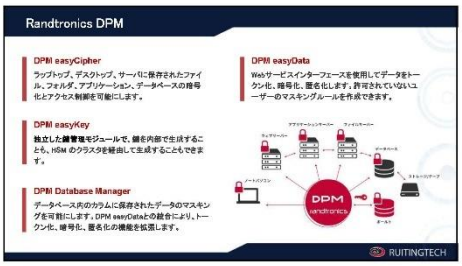

u.trust Anchor
RUITINGTECH


utimaco
Utimaco HSM
Hardware security module


Atalla AT 1000
FIPS
Level 3 Validated
140-3
スピードとセキュリティの究極のバランス
効率的な決済エコロジーを実現
Key use cases
PIN Processing
PIN Translations and Authorization
Card/User Verification
3-D Secure
Payment Card Verification
Data Encryption/ Decryption
E-Wallets
Key Generation and Injection
EMV Transaction Processing
UTIMACO Atalla AT1000は、電子決済業界において、速度が最も早く、国際的なFIPS 140-3 Level 3認証を受けたペイメント・ハードウェア・セキュリティ・モジュールです。非現金小売決済取引、カード会員認証、暗号鍵の機密データと関連鍵を保護し、電子決済業界のお客様から高く評価いただいています。
RUITINGTECH


Randtronics DPM
Randtronics DPM
機密情報の保護に最適なツール
DPMはアメリカのデータベース、会社の機密情報の漏洩を心配する必要がなくなります。Mailとデータベースを保護でき、暗号化のためにプログラムを変更する必要はありません。
Randtronics Data Privacy Manager
RUITINGTECH


統合された完全なアーキテクチャ
utimaco HSM
Payment HSM
General Propose HSM
u.trust 360
Maintenance
Ruiting Solutions
HSMs
Zentra KMS
Zentra CSP
RKIS
Randtronics DPM
Ruiting Solutions
RUITINGTECH

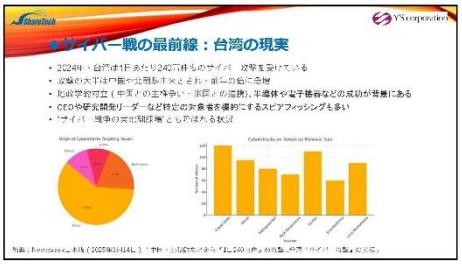

Randtronics DPM
DPM easyCipher
ラップトップ、デスクトップ、サーバに保存されたファイル、フォルダ、アプリケーション、データベースの暗号化とアクセス制御を可能にします。
DPM easyKey
独立した鍵管理モジュールで、鍵を内部で生成するとも、HSM のクラスタを経由して生成することもできます。
DPM Database Manager
データベース内のカラムに保存されたデータのマスキングを可能にします。DPM easyDataとの統合により、トークン化、暗号化、匿名化の機能を拡張します。
DPM easyData
Webサービスインターフェースを使用してデータをトークン化、暗号化、匿名化します。許可されていないユーザーのマスキングルールを作成できます。
DPM
RUITINGTECH


実績
LINE Bank
Chelpis
FUJITSU
BT
htc
RUITINGTECH


THANK YOU
本日はご清聴いただき、ありがとうございました。
ご質問等ございましたら、どうぞ当社ブースへお
気軽にお問い合わせください。
ありがとうございました！
株式会社ルイテック
ホームページ
Mail : sales@ruitingtech.com.tw
TEL +886-2-2627-6340
RUITINGTECH 株式会社ルイテック

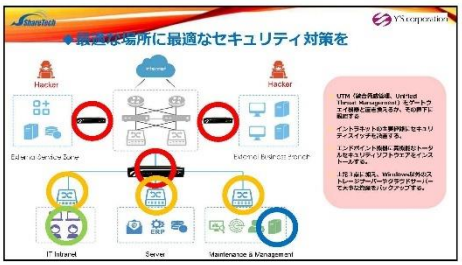
（七）眾至資訊股份有限公司

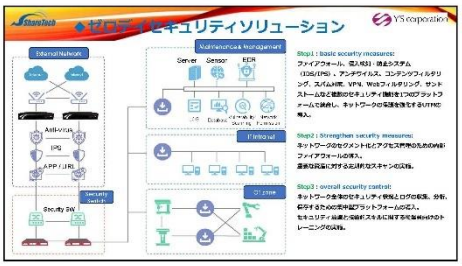
2025/6/26



1

2025/6/26

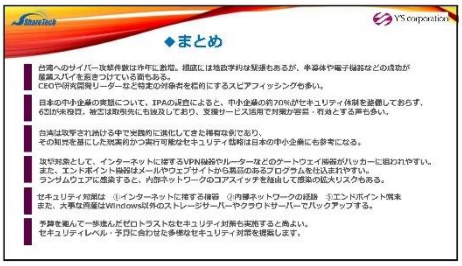




2


ShareTech
Y'S corporation
◆STEALTHONE Sシリーズ(UTM)のご紹介
1. オールインワンネットワークセキュリティ機能
2. ネットワーク通信を可視化する分析・レポート機能
日本で企画・設計
台湾のセキュリティ知見
防御ノウハウを最適化
台湾の各企業と連携
ZYXEL NETWORKS
AXIOMTEK
台湾で開発・製造

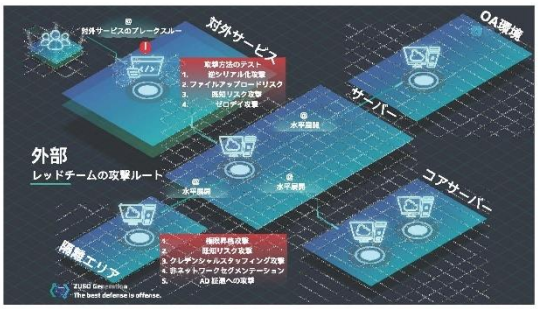

会社紹介
ShareTech Information Co., Ltd.
ShareTech
株式会社ワイズ
Y'S corporation
■ パートナービジネスについて
総合お問合せ窓口
株式会社ワイズ　ビジネスパートナー営業部
03-5297-5470

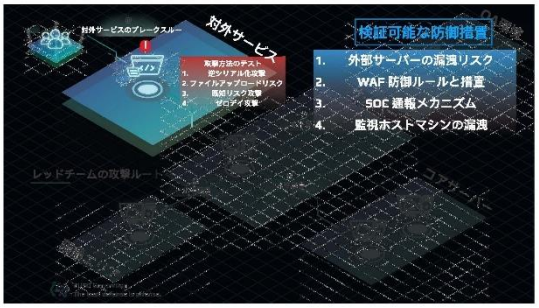

ShareTech
Y'S corporation
◆まとめ
台湾へのサイバー攻撃件数は昨年に激増。根底には地政学的な緊張もあるが、半導体や電子機器などの成功が産業スパイを惹きつけている面もある。
CEOや研究開発リーダーなど特定の対象者を標的にするスピアフィッシングも多い。
日本の中小企業の実態について、IPAの調査によると、中小企業の約70%がセキュリティ体制を整備しておらず、6割が未投資。被害は取引先にも波及しており、支援サービス活用で対策が容易・有効とする声も多い。
台湾は攻撃され続ける中で実践的に進化してきた稀有な例であり、
その知見を基にした現実的かつ実行可能なセキュリティ戦略は日本の中小企業にも参考になる。
攻撃対象として、インターネットに接するVPN機器やルーターなどのゲートウェイ機器がハッカーに狙われやすい。
また、エンドポイント機器はメールやウェブサイトから悪意のあるプログラムを仕込まれやすい。
ランサムウェアに感染すると、内部ネットワークのコアスイッチを経由して感染の拡大リスクもある。
セキュリティ対策は　①インターネットに接する機器　②内部ネットワークの経路　③エンドポイント端末
また、大事な資産はWindows以外のストレージサーバーやクラウドサーバーでバックアップする。
予算を組んで一歩進んだゼロトラストなセキュリティ対策も実施すると尚よい。
セキュリティレベル・予算に合わせた多様なセキュリティ対策を提案します。

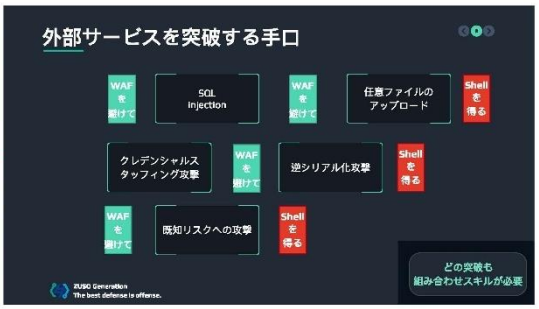

Sharetech セキュリティソリューション導入実績
行政機関
医療機関
教育機関
企業
インフラ業界
TSMC
tsmc
win
Chenergy
中龍鋼鐵 DRAGON STEEL
金居開發
長庚大學

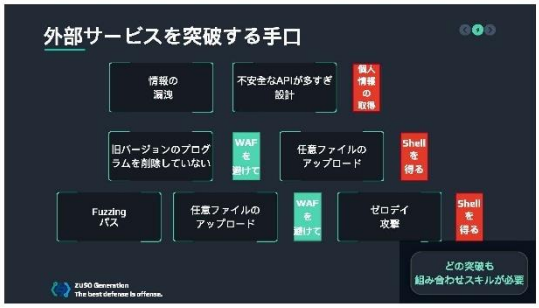

ご清聴ありがとうございました

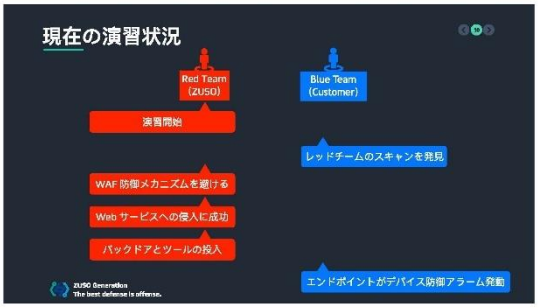
（八）如梭世代股份有限公司

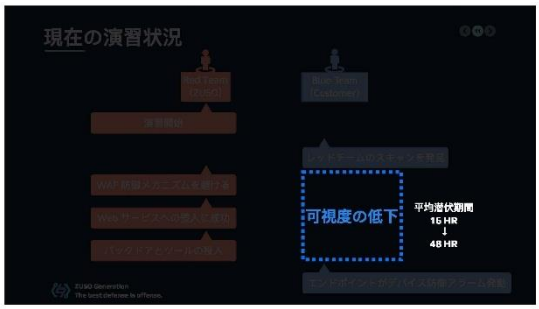







外部サービスを突破する手口
情報の漏洩
不安全なAPIが多すぎ設計
個人情報の取得
旧バージョンのプログラムを削除していない
WAFを避けて
任意ファイルのアップロード
Shellを得る
Fuzzing パス
任意ファイルのアップロード
WAFを避けて
ゼロデイ攻撃
Shellを得る
どの突破も組み合わせスキルが必要
ZUSO Generation
The best defense is offense.


現在の演習状況
Red Team (ZUSO)
Blue Team (Customer)
演習開始
レッドチームのスキャンを発見
WAF 防御メカニズムを避ける
Web サービスへの侵入に成功
バックドアとツールの投入
エンドポイントがデバイス防御アラーム発動
ZUSO Generation
The best defense is offense.


現在の演習状況
可視度の低下
平均潜伏期間
16 HR
↓
48 HR
ZUSO Generation
The best defense is offense.


Webログ
分析の重要性
ZUSO Generation
The best defense is offense.

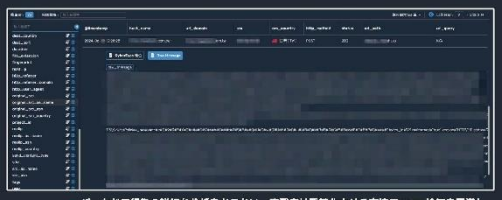

ZUSO Generation
CyberEyes 情報セキュリティの可視度
ネットワーク攻撃はどこにでもあり、対外ウェブサイトはすでにハッカーの最新攻撃目標であり、クレデンシャルスタッフィング攻撃、注入攻撃、アプリケーションプログラム層別攻撃などの脅威に曝されています。
CyberEyes ガードソリューションは外部ウェブサイト侵入アラーム、セキュリティホールへの攻撃、セキュリティイベントアラームなどを提供します。
CyberEyes
CyberEyes ソリューションプランの特徴
✓ Web ログへの脅威に対する検知と分析をおこないアラームを発します
✓ 企業情報の漏洩がないか検査します
✓ 重要なサーバーに対する危険 Cmd アラームを実行します
✓ 企業の情報セキュリティデバイスへの投資の有効性を検証します
✓ 完璧な情報セキュリティイベントログトラックを提供します
ZUSO Generation
The best defense is offense.


CyberEyes 攻撃スタイルの分析
異常なブラウズアクセスを検知し、かつ最新のリソースを保ちます
ZUSO Generation
The best defense is offense.


CyberEyes 攻撃スタイルの分析
Drill Down 機能によりマークを付けた後のアラームログにジャンプします
ZUSO Generation
The best defense is offense.


CyberEyes 攻撃スタイルの分析
行為アラームは Webshell の特徴です
ZUSO Generation
The best defense is offense.

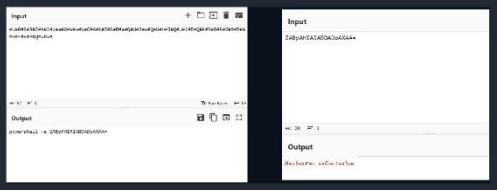
CyberEyes 攻撃スタイルの分析



- バックドア行為の詳細な分析をおこない、攻撃者は難読化させる方法で WAF 検知を回避し、被害ホストマシンへのコマンド埋め込みに成功します

ZUSO Generation
The best defense is offense.

CyberEyes 攻撃スタイルの分析

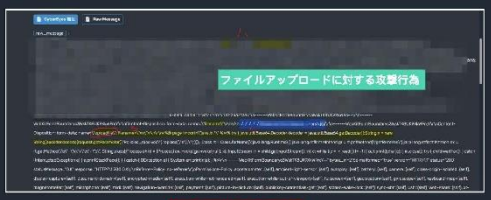


ZUSO Generation
The best defense is offense.

CyberEyes 攻撃スタイルの分析

ZUSO Generation
The best defense is offense.

CyberEyes 攻撃スタイルの分析



WAF ルールの強化が必要

ZUSO Generation
The best defense is offense.

CyberEyes 攻撃スタイルの分析

その後攻撃者はバックドアを通じて機密情報をウェブサイトディレクトリに置き、直接アクセスしダウンロードします

ZUSO Generation
The best defense is offense.

CyberEyes 成功例

ZUSO Generation
The best defense is offense.

Future

CyberEyes
Cloud Base

- Deploy in Minutes
- Prepared to Stop Attacks
- Focus on Real Threats
- Simple Forensic Investigation

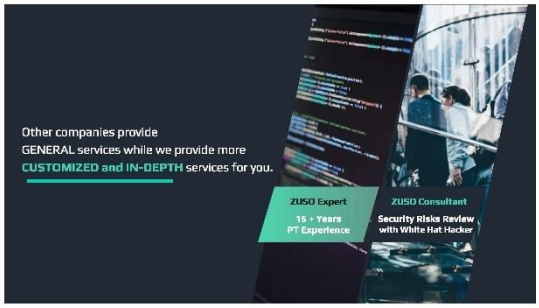
Cybersecurity isn't Difficult, it's just getting Easier

ZUSO Generation
The best defense is offense.

防御者が抱いている攻撃者の態度

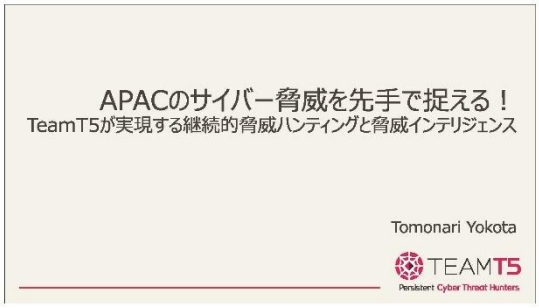
受け身の防御が攻めの防御を徐々に高める

ZUSO Generation
The best defense is offense.


Other companies provide
GENERAL services while we provide more
CUSTOMIZED and IN-DEPTH services for you.
ZUSO Expert
15 + Years
PT Experience
ZUSO Consultant
Security Risks Review
with White Hat Hacker


Contact Us
Email
sales@zuso.ai
Facebook
https://FB.com/ZUSOGeneration
Website
https://zuso.ai
ZUSO Generation
The best defense is offense.

（九）杜浦數位安全股份有限公司



高度なサイバー脅威への対処

攻撃者を見極め、脅威を発見し、専門家とともに対処する

脅威インテリジェンス
敵に関する知識に基づく、より優れた対策
ThreatVISION
165+ 脅威アクター
2,600+ マルウェア

脅威ハンティングテクノロジー
エンドポイント保護、攻撃者のツール、バックドア、足跡の発見
ThreatSonar ANTI-RANSOMWARE
90% MSSP
3M+ エンドポイント

プロフェッショナルな管理と専門的な対応
攻撃の監視、対応、分析の支援
Managed Detection and Response / Incidient Response
1,000+ インシデント対応
100+ テクニカルエキスパート

ThreatVision

APACを中心とした、包括（戦略・運用・戦術）的なサイバー脅威インテリジェンスプラットフォーム

- **侵害の痕跡（IoC）**：TeamT5 の詳細な調査に基づいた指標を提供
- **脅威ハンティングツール**：マルウェアと脆弱性の脅威ハンティングツール
- **インテリジェンスレポート**：多様なユーザーと業界向けの各種レポート
- **脅威アクター、マルウェアギャラリー**：それぞれの特徴をまとめたプロファイル
- **RFIサービス**：レポート/ツールのカスタマイズ
- **API Service**：TeamT5 とシステムを統合して生産性を最適化

ThreatVISION
A Portal to See Through the Chaos

2024年下半期APT脅威レポート - マルウェア技術分析

脅威アクターはセキュリティ製品の検知を回避するために、マルウェアの機能を強化し続けている

中国系APTグループのEDR回避手法

- **主なEDR回避ツール**
  - ClientEnd、ChatLoader、HelloKety、SharpAgent、EDRSilencer、sn0wldr、ScareCrow
- **ClientEndの特徴**
  - ウイルス対策ソフトやEDR製品をスキャン
  - ファイアウォールルールを新規作成し、通信を遮断・保護機能を無効化
  - 中国系APTグループ5LIME63が台湾の航空宇宙産業、韓国の組織を標的
- **ChatLoader/HelloKetyの特徴**
  - Windowsのイベントトレース（ETW）を回避してログ収集を妨害し、EDR検知を回避
- **SharpAgentの特徴**
  - WindowsのAntimalware Scan Interface（AMSI）を回避し、EDRのマルウェア検出能力を無効化

ThreatSonar

メモリフォレンジックを含む総合的な分析で脅威を可視化し、迅速対応を実現するプラットフォーム

- **業界トップクラスの脅威ハンティング：APT（高度な継続的標的攻撃）**を高精度に検出し、潜伏を逃さない
- **高い検知率**：他社製品未検知の**1,000件超**の脅威を摘発
- **幅広い導入実績：300万台以上**に導入、**300以上のクライアント**を支援
- **インテリジェンス駆動型**：数千のAPT/バックドア情報を内蔵し、外部IoC取り込みも可能
- **総合フォレンジック分析：メモリフォレンジック・挙動分析**で感染経路を再現し、根本原因を追跡
- **簡単&自動化された導入：実行ファイル形式**で展開しやすく、**オフライン**端末もカバー

ThreatSonar
Threat Forensics Analysis Platform

事例紹介：セキュリティ対策済み大手企業における導入効果

10,000台のエンドポイントを2週間で調査し、感染経路と影響範囲を迅速に特定

高度な脅威への備え
- AVやEDRを導入済みにもかかわらず、APTや未知の脅威への懸念から、ThreatSonarによる定期健診評価を実施

定期評価で発見
- 10,000台のスキャンで、EDRをすり抜けた潜伏中のマルウェアを検出
- パブリッククラウドを利用した約1年にわたる情報漏洩が明らかに

迅速な対処で把握
- 初期調査として、感染端末・侵入経路・影響範囲を2週間で特定
- 攻撃者の行動全体を把握し、対処方針を明確化

早期把握と封じ込め
- マルウェア解析の結果、APIフックの悪用、攻撃者の痕跡などを確認し、再発防止へ活用

グローバルでの信頼と評価

国際的な受賞歴と豊富な防御実績が、高度な専門性を証明

世界的な受賞歴
- 台湾脅威インテリジェンス年間最優秀企業賞2024、2023（Frost & Sullivan）
- ベストチョイスアワード最優秀賞 2024（Computex Taipei）

10+ 国際カンファレンス登壇
- Black Hat（米国）
- CODE BLUE/AVTokyo/JSAC（日本）
- Troopers（ドイツ）
- Hack In The Box、FIRST など

300+ 世界各国のクライアント
- 台湾：300社以上
- 日本：50社以上
- ASEAN：30社以上
- 政府、金融、テクノロジー、電気通信、情報セキュリティなど

TeamT5との連携で未来を守る

脅威分析のプロフェッショナルと実践的なソリューションで、組織のセキュリティを強化

お問い合わせ・ご相談
- まずはお問い合わせ・ご相談いただき、現状の課題を一緒に解決

パートナー協業
- エンドポイント保護やインシデント対応、脅威ハンティングを高度化し、顧客満足度の向上や競合差別化を実現

製品トライアルご相談（ThreatSonar/ThreatVision）
- 導入前から運用後まで、TeamT5の専門家が継続的にフォロー

ご清聴ありがとうございました

TeamT5.jp

@TeamT5_JP

横田 智成 Tomonari Yokota
Email: t.yokota@teamt5.jp

TEAMT5
Persistent Cyber Threat Hunters

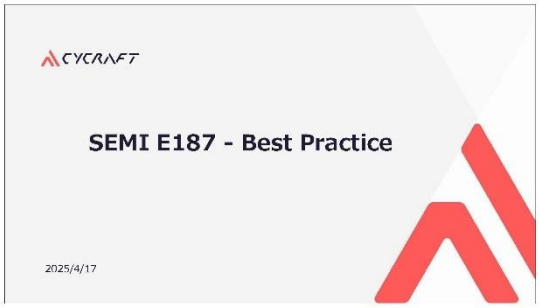
TeamT5 Seminar の開催

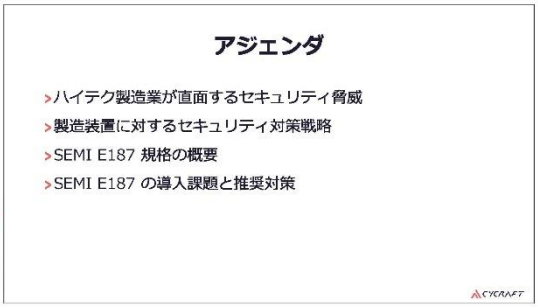
セキュリティスペシャリストが解説！
「EDR回避攻撃の最新実態」と「迅速インシデント対応」の最前線
2025-5-28 (水)
住所：〒108-0075 東京都港区港南1-6-31 品川東急ビル 8F
会場名：AP品川 A&ーム、B&ーム

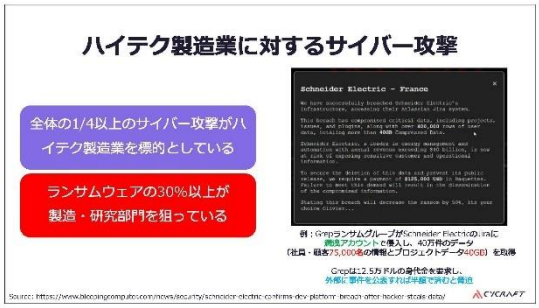
附件三、參訪伊藤忠科技解決方案公司各廠商分享簡報

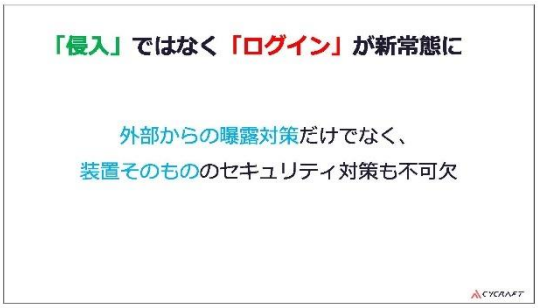
（一）SEMI E187 相關分享

1. SEMI E187 商品合規－奧義智慧科技股份有限公司

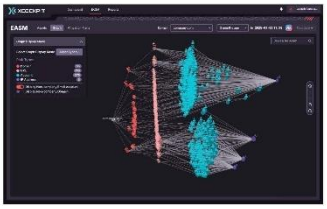




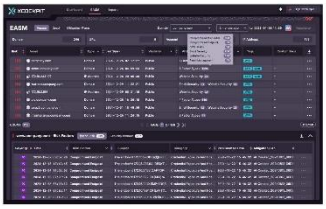




外部からの曝露対策には……
CyCraft XCockpit EASM



外部からの曝露対策には……
CyCraft XCockpit EASM



装置そのものは……？　E187！

製造装置のライフサイクルに基づいた セキュリティ戦略

導入 (Onboarding) → 構成 (Staging) → 運用 (Production) → 保守 (Maintenance)

#	セキュリティ対策	実施内容
1	身元・装置認証	装置の唯一性と真正性を確保
2	マイクロセグメンテーション	ネットワークを小分けし、許可通信のみ許容
3	最小権限の原則	特定アカウントが指定条件で操作可能
4	行動分析・監視	異常な挙動を継続的に監視・検知
5	セキュリティ強化と脆弱性管理	不要なサービス・インターフェースを無効化
6	ログ管理と監査機能	イベントログの記録と分析

SEMI E187規格の概要

ランサムウェア被害が契機	規格化の検討開始	SEMI E187正式発表	企業が調達要件に導入	バージョン2の検討が進行中
2018	2019	2022	2023	2024

SEMI E187の12項目

#	管理項目	チェック内容
001	OSサポート状況の確認	使用しているOSがベンダーのサポート対象であるかを確認し、サポートライフサイクルの証明を提出
002	セキュリティ更新情報の登録	アップデート情報源（脆弱性、他社動向の評価を含む）を登録し、更新記録の例を提示
003	暗号化通信の対応	HTTPS、SFTP、SSHなどの暗号化通信に対応しているか確認し、パケット分析ツールで検証
004	ネットワーク設定管理	使用中のプロトコルとポート番号を定義したドキュメントを整備し、不必要なサービスを停止が可能であること
005	脆弱性スキャンの実施	資料構成ツールによる最新の脆弱性スキャン結果を提出し、重大な脆弱性がないことを確認
006	マルウェアスキャン結果と対応策	マルウェアスキャンの対象とその対応方法を提示
007	AVソリューションの互換性	推奨されるウイルス対策ソフトとその設定、および機能との互換性を説明
008	システム強化とセキュリティ設定	入出力インターフェース（例：USB）やシステムサービスの使用を制限し、不要な初期値を無効化
009	認証機能（ユーザー分類）	ログイン時の本人認証、および管理者と一般ユーザーの区別があること
010	権限管理と最小権限原則	アカウントを職務に応じて分類し、最小権限原則に基づいた設定を行い、文書で証明
011	ログ出力機能	セキュリティイベントをログに記録し、APIまたは手動で外部ユーザーにエクスポート可能
012	イベントの分類と内容	ログにアクセス試行、設定変更、システムエラー等のイベントを分類して記録（イベント種別、説明、アカウント、タイムスタンプを含む）

SEMI E187の導入課題と推奨対策

課題
- リソース不足・専任チーム不在
- 規格知識の不足
- 装置がセキュリティ対象外
- チェックツールの未整備

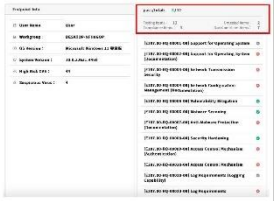
対策
- 部門横断チームの設置
- 専門家の導入と支援
- 自己評価・ギャップ分析の実施
- 自動診断ツールの活用

SEMI E187を支えるエコシステム

CyCraftのツールを使った適合性確認

CYCRAFT

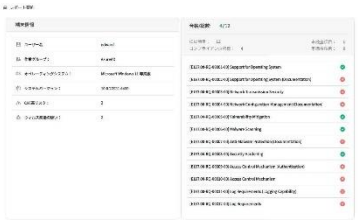
CyCraftのツールを使った適合性確認



CYCRAFT

Confidential

サンプルレポート：設備情報と適合度



CYCRAFT

Confidential

サンプルレポート：OS分析結果

CYCRAFT

Confidential

サンプルレポート：設備分析結果と改善点

ウイルス発見の場合

E187対応項目:006

脆弱性発見の場合

E187対応項目:005

CYCRAFT

Confidential

サンプルレポート：ネットワーク分析結果

暗号化通信を利用していない場合

E187対応項目:003

CYCRAFT

Confidential

サンプルレポート：監査に関する情報

E187対応項目:012

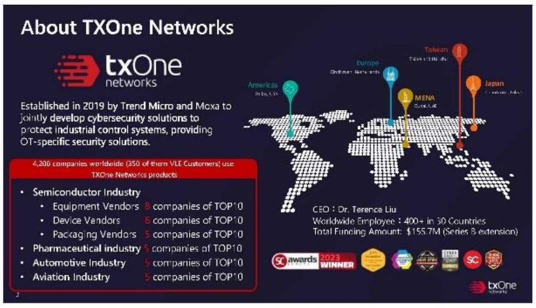
CYCRAFT

製造装置セキュリティの継続的な検証

CYCRAFT

2. SEMI E187 商品合規－睿控網安股份有限公司


txOne networks
The Leader of OT Zero Trust
TXOne's activities for Semiconductor Industry
TXOne Networks Japan

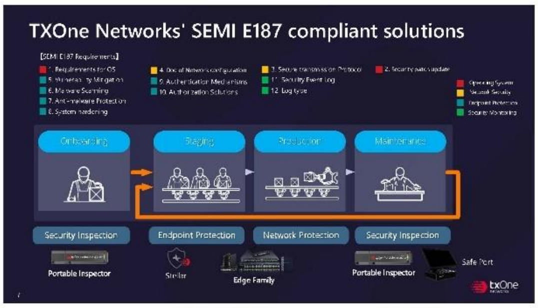

About TXOne Networks
txOne networks
Established in 2019 by Trend Micro and Moxa to jointly develop cybersecurity solutions to protect industrial control systems, providing OT-specific security solutions.
Semiconductor Industry
Equipment Vendors companies of TOP10
Device Vendors companies of TOP10
Packaging Vendors companies of TOP10
Pharmaceutical industry companies of TOP10
Automotive Industry companies of TOP10
Aviation Industry companies of TOP10
Taiwan
Europe
Americas
MENA
Japan
CEO : Dr. Terence Liu
Total Funding Amount: $155.7M (Series B extension)

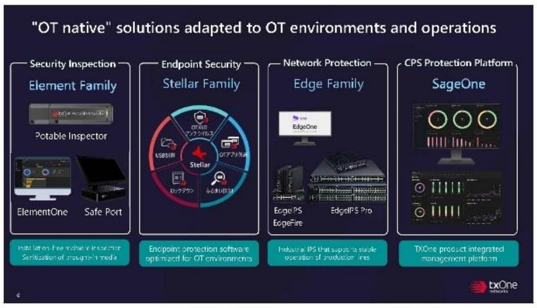

Achievements at leading global companies
Confidential
Semiconductor
Automotive
Manufacturing
Pharmaceutical
Foods & Beverages
Power
Aviation
Oil & Gas
ASML
infineon
intel
Lam
onsemi
Powerchip
Rapidus
ROHM
tsmc
TEXAS INSTRUMENTS
UMC
BRIDGESTONE
DENSO
Ferrari
HONDA
HYUNDAI
KYB
MARELLI
Mercedes-Benz
SUZUKI
TOYOTA
BOSCH
HITACHI
KOMATSU
KYOCERA
MITSUBISHI ELECTRIC
NIPPON STEEL
Panasonic
SHIMADZU
SIEMENS
TOSHIBA
Lonza
NOVARTIS
Roche
sanofi
Alsea
Carlsberg
FEMSA
Heineken
AIRBUS
BOEING
GE Aviation
SAFRAN
txOne


Thesis Validated by Industry's Most Important Player
tsmc
TSMC's Success Story with TXOne Networks
Growing OT Security Threat
TXOne Has the Most Suitable OT Solution
Land and Expand Strategy
Winning Industry Large Customers
Penetrate Across Supply Chain
TSMC disclosed number of foundry tools were infected by computer virus and shut down may cost up to US$1/1mm of revenue
TXOne's solutions beat out other competitors after going a rigorous testing process. TSMC began deploying TXOne's solutions
TSMC increases deployment of TXOne solutions to more foundries across Taiwan & globally
TSMC set the standard, and many foundries in the world began deploying TXOne's solutions
TSMC pushing the standard across supply chain, and many major suppliers began deploying TXOne's solutions
Outstanding Supplier Award


SEMI TAIWAN Cybersecurity Committee
FOCUS 01
Promotion of SEMI Standards
Study of reference architectures
FOCUS 02
Cyber security awareness
(SEMICON Events held quarterly)
SEMI TAIWAN Cybersecurity Committee
FOCUS 03
Study on how to evaluate supply chain cybersecurity
FOCUS 04
Supply Chain based on NIST CSF Cyber Security Risk Assessment Study
Group Leader
Dr. Terence Liu
CEO, TXOne Networks
txOne


SEMI TAIWAN Cybersecurity Committee
Standards and reference guides published and provided under the initiative of SEMI Taiwan
Security Standard for Fab Equipment
SEMI E187 published
SEMI E187 Reference Practice
SEMI Semiconductor Cybersecurity Risk Rating Service
Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments
Jan 2022
Oct 2022
Jan 2023
Oct 2023
txOne


TXOne Networks' SEMI E187 compliant solutions
[SEMI E187 Requirements]
Onboarding
Staging
Production
Maintenance
Security Inspection
Endpoint Protection
Network Protection
Security Inspection
Portable Inspector
Stellar
Edge Family
Portable Inspector
Safe Port
txOne


"OT native" solutions adapted to OT environments and operations
Security Inspection
Element Family
Portable Inspector
ElementOne
Safe Port
Endpoint Security
Stellar Family
Stellar
Network Protection
Edge Family
EdgeOne
EdgeIPS
EdgeFire
EdgeIPS Pro
CPS Protection Platform
SageOne
Endpoint protection software optimized for OT environments
TXOne product integrated management platform
txOne

E-187 Certification of Conformity by a Certification Body

- Gallant Precision Machining and Contrel Technology, both of Taiwan, receive the world's first SEMI E187 Certificate of Conformity (VoC). (2023 Aug)
- JEOL was the first company in Japan to receive the E187 certificate of conformity in Japan (2024 Dec)

TXOne supported each company with solutions and advisory to help them achieve certification.

SMCC (Semiconductor Manufacturing Cybersecurity Consortium)

<Objective>

- Establish a robust cybersecurity framework
- Accelerate implementation of security solutions for the entire supply chain
- Modernize security protocols to incorporate best practices from industries such as automotive and healthcare

- 6 WGs discuss each theme
  - WG1 : Cybersecurity Implementation
  - WG2 : Compliance Readiness
  - WG3 : Supply Chain Cybersecurity
  - WG4 : Regulation & Other Specs
  - WG5 : Threat Sharing
  - WG6 : Cybersecurity Pre-Standards Engineering

Semiconductor Industry Activities in Japan

SEMICON JAPAN

Booth Exhibition

Cyber Security Forum

Semiconductor Cybersecurity Executive Roundtable

15 Semiconductor companies join
Tokyo Electron, RO-RI, Rapidus, DNP, Lbem, Itochu, JCSL, Livertec, NuFlare, Renesas, Kioxia, Tokyo Seimitsu, Screen Semiconductor, Japan Semiconductor, ULVAC

KYUSHU SEMICONDUCTOR HUMAN DEVELOPMENT CONSORTIUM

Collaboration with METI

経済産業省

txOne networks

Keep the Operation Running

TSMC's Supply Chain Security Initiative

In 2023, this standard was officially included as one of TSMC's procurement contract requirements to further enhance the security of semiconductor factory operations, and a verification mechanism was established to ensure compliance with the standards in four areas – computer operation system, network security, endpoint device protection, and security monitoring and information security auditing, before the introduction of new equipment."

source: TrendForce synthesis, Japan Forum for Cybersecurity of Semiconductor Equipment, Roadmap status, Industry Trends

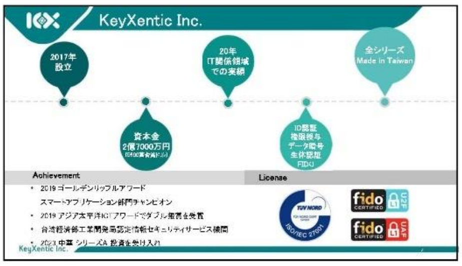
（二）廠商技術分享

1. 優內控股份有限公司

2. 關楗股份有限公司

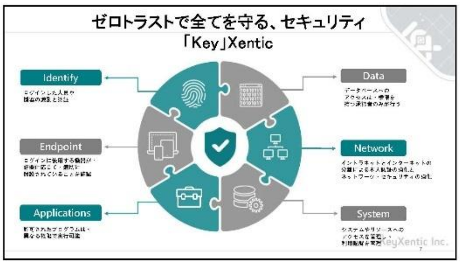

KeyXentic
-ID/パスワードからの脱却
Zero Trust Solution
KeyXentic Inc.


コア技術
ソフトウェアとハードウェアの
統合アプリケーション製品を独自に研究開発
BYOK
PKI
AATL
HDD
E-Signature
CA
Authentication
MFA
SSO
Encryption
e-KYC Integration
オンプレミス & クラウド
KeyXentic Inc.


KeyXentic Inc.
2017年 設立
資本金 2億7000万円
20年 IT関係領域での実績
ID認証 権限授与 データ暗号 生体認証 FIDO
全シリーズ Made in Taiwan
Achievement
• 2019 ゴールデンリッフルアワード スマートアプリケーション部門チャンピオン
• 2019 アジア太平洋ICTアワードでダブル報賞を受賞
• 台湾経済部工業開発局認定情報セキュリティサービス機関
• 2023 中華 シリーズA 投資を受け入れ
License
TÜV NORD ISO/IEC 27001
fido CERTIFIED U2F
fido CERTIFIED UAF
KeyXentic Inc.


KeyXentic プロダクト KX701
KX701 FIDO2 NFCトークン
KX701
SMART
TOKEN
SIMPLE PROTECTION
SMART ENCRYPTION
SECURE FIRST
fido CERTIFIED FIDO2
PKI および FIDO2 の２種類の標準認証モードに対応した、先進的な防水・防塵のNFC USB セキュリティキーです。
KeyXentic Inc.


KeyXentic プロダクト KX901
KX901 FIDO2 指紋認証トークン
fido CERTIFIED FIDO2
KeyXentic Inc.


ゼロトラストで全てを守る、セキュリティ
「Key」Xentic
Identify
Endpoint
Applications
Data
Network
System
KeyXentic Inc.


プロダクト Keyper–総合的な管理プラットフォーム
Keyper
Fido
Welcome to Keyper Manager
353
221
132
• パスワード不要のID認証管理：
• シングルサインオン（SSO）のシームレスな体験
• ID 認証のライフサイクルを包括的に管理


パートナー
visioneer
NET PEACE
NSW
NTT DATA
TURNCLOUD
中華電信
TWCA 臺灣網路認證
精誠軟體服務 SYSTEX Software & Service
uniXecure
ITTS
DXC TECHNOLOGY
Hwacom 華電聯網
峰儀科技
數聯資安
KeyXentic Inc.


導入企業
金融
企業
政府
LINE Bank
SHISEIDO
TAIPEI
MEDIATEK
FATC
HongLeong Bank
KeyXentic Inc.


Thank you.
KeyXentic Inc.

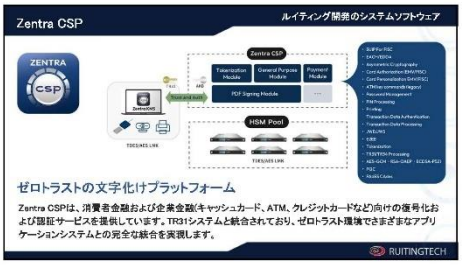
3. 叡廷股份有限公司

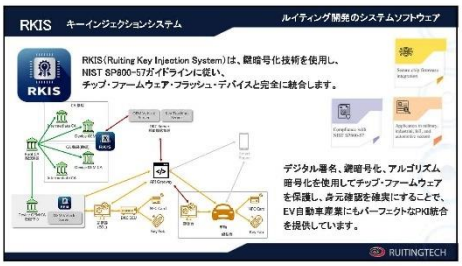

暗号化技術 ハイエンド情報
セキュリティ・ソリューション
RUITINGTECH 株式会社ルイティング

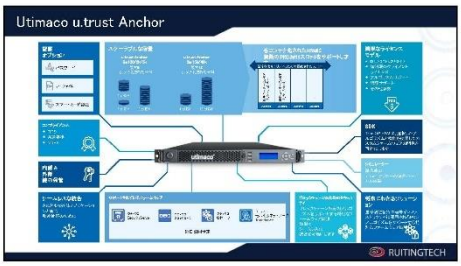

Zentra KMS & Zentra CSP
ルイティング開発のシステムソフトウェア
真のクリプト・アジリティを実現するために
当社は NIST CSWP39および国際標準に準拠したゼロ トラスト キー管理およびクリプト サービス プラットフォームを提供します。
PQC 移行メカニズムを組み込み、ポスト量子時代(PQC)における企業のセキュリティを確保します。
PQC READY
CRYSTALS-Kyber
CRYSTALS-Dilithium
Sphincs+
FALCON
RUITINGTECH


RUITINGTECH
ルイティング は、情報セキュリティの分野で13年の歴史があります。情報セキュリティ、暗号理論、チップを専門領域としています。特に金融システムの開発と設置に関して、高い評価をいただいています。
Utimacoの暗号化設備の専属代理店ですが、IoTとEV自動車のセキュリティに関しても、開発能力をご評価いただいています。

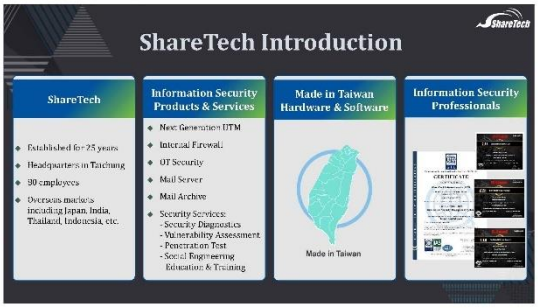

Zentra KMS
ルイティング開発のシステムソフトウェア
安全かつ法令に準拠した、キーおよびクレデンシャル管理システムを企業に提供
◆キーとクレデンシャルの生成、保存、更新、破棄、同期を含め、完全なライフサイクル管理を確保します。
◆標準化されたキー管理とクロスプラットフォームのキー変換のために、KMIPサービスを提供します。
◆クラウドHSMと、PKCS#をサポートするオンプレミスHSMのキーとの同期管理を実現します。
RUITINGTECH

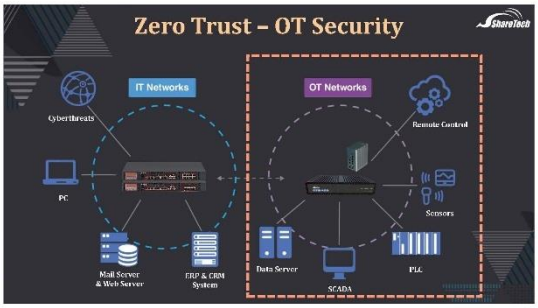






4. 眾至資訊股份有限公司





5. 全景軟體股份有限公司

CHANGING 全景ソフトウェアとCiotブランド紹介

会社概要

- 会社名: CHANGING Co., Ltd. 全景ソフトウェア
- 代表取締役社長: 楊朝明（ヤン・ルイミン）
- 資本金: 2.5億台湾ドル（約10億円）
- 設立: 1998年8月
- 社員数: 200名
- 事業拠点: 台湾・日本
- 主要市場: IoTセキュリティ・Matter対応ソリューション
- 親会社: Wistron Corporation

Ciot

Cyber ▲ Control ▲ Connect

Changingは、台湾でいくつかの企業の一連機器がISA/IEC 62443規格を満たすのを支援した実績があります。

生産機器のネットワーク接続に伴い、ISA/IEC 62443標準に基づくセキュリティ保護が必要。

1. **安全基盤の構築：**アクセス制御、認証、機密性、完全性、可用性の確保
2. **脆弱性低減：**設計・実装での弱点除去
3. **安全通信：**データ機密性・完全性保護
4. **システム完全性：**不正改変防止

ターゲット

生産機器はネットワーク接続が必要であるため、ISA/IEC 62443 という産業用自動化および制御システムの国際セキュリティ標準に準拠した機器セキュリティ対策が求められます。
これには、機器ファームウェアの保護（不正利用や改ざん防止）、ユーザー認証、機器自体の正当性検証、生産データの盗用・改ざん防止、ネットワーク通信の暗号化セキュアチャネルの構築などが含まれます。これらの対策の主な目的は、あらゆるネットワーク脅威に対して機器・システムの安全性を確保することです。

実施方法① 機器ファームウェア保護

- 完全性保護：ハッシュによる整合性検査
- 機密性保護：暗号化技術でロジック保護
- アクセス制御：認可ユーザーのみ更新
- 改ざん検知：デジタル署名による警告

実施方法② ユーザー認証

- ゼロトラスト原則に基づく多要素認証を導入。
- NIST準拠の多要素認証で継続的検証。

実施方法④ ネットワーク安全通道

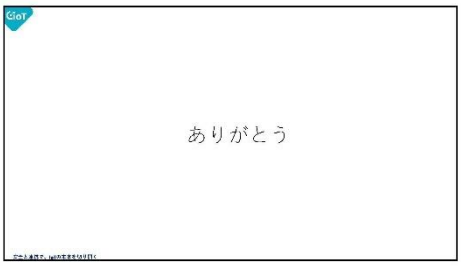
- TLS双方向認証による暗号化通信
- TLSの3要素：暗号化、認証、完全性

実施方法③ 機器認証 & データ防護

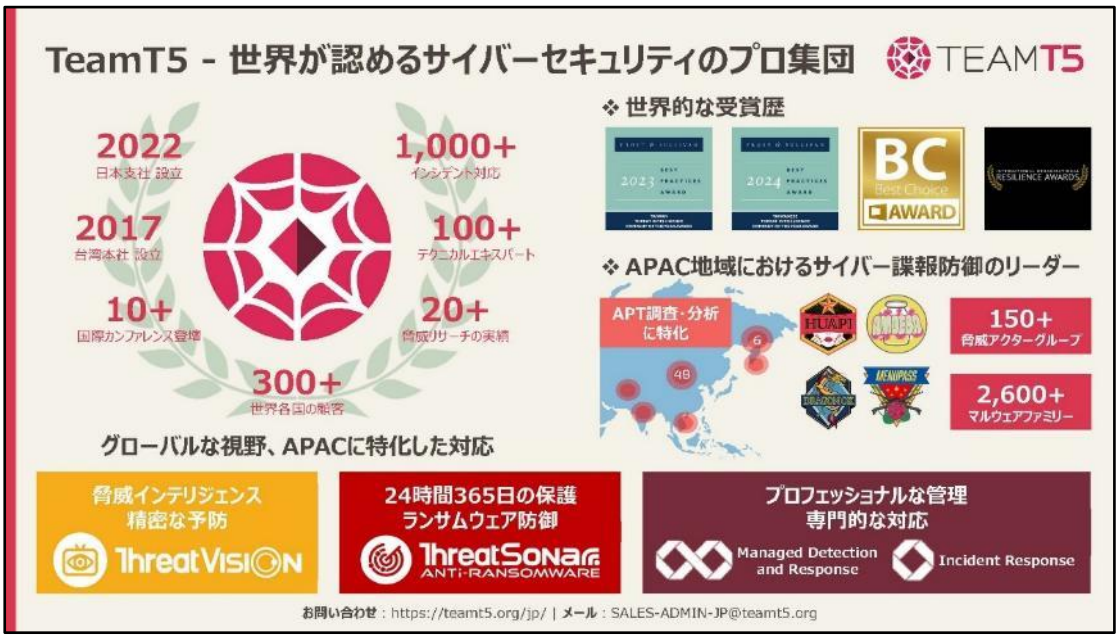
- PKI証明書管理：申請、撤回、更新、同期機能
- IEC 62443-4-2 Level2準拠
- 生産データ署名/暗号化で機密性・完全性確保

予期成果

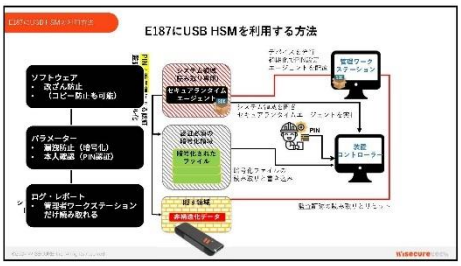
1. セキュリティ向上: IACS全体の防御強化
2. 脆弱性リスク低減
3. データ保護改善
4. コンプライアンス達成
5. 信頼性・評判向上

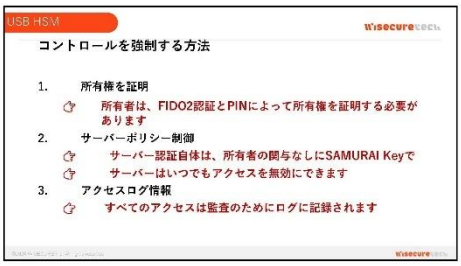


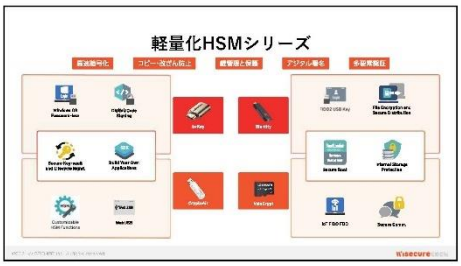
6. 杜浦數位安全股份有限公司

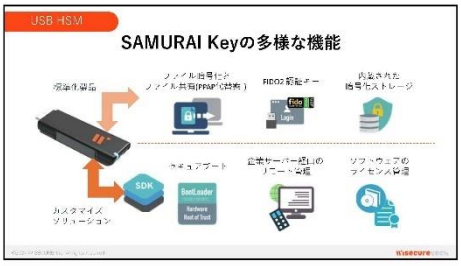


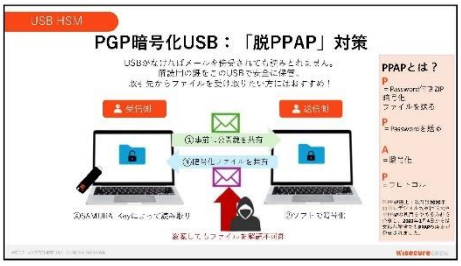
7. 匯智安全股份有限公司

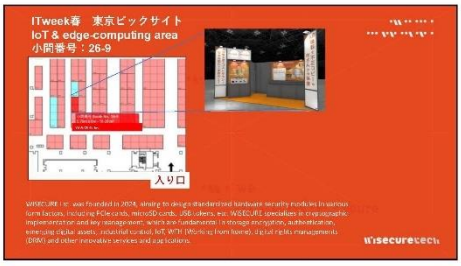








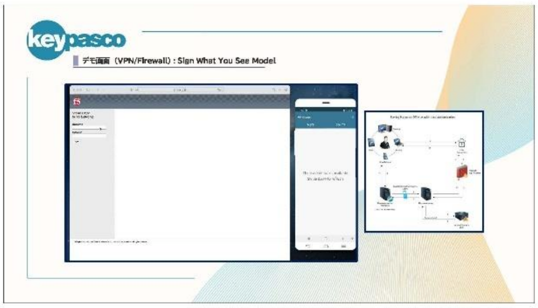




8. 來毅數位科技股份有限公司


keypasco
新しい手法の多要素認証ソリューション
Lydsec Digital Technology Japan
リーセックデジタルテクノロジージャパン


keypasco
事業の特長
3. ユーザーオリエント
マッチングニーズ
メガバンク、地方銀行、証券会社、ネットバンク
メーカー、プラットフォーマー
IT企業、商社
事業概要(サービス/製品)
Channel 1
Verifying channel
Channel 2


keypasco


keypasco
Keypasco 多要素認証ソリューションの5つの特徴
1
クレデンシャルを使用しない認証
2
2チャンネル構造で認証を行う
3
暗号化通信で認証を行う
4
アクティブ認証：変動型
5
ユーザーフレンドリー


keypasco
Keypasco によるSEMI E187対応項目
分野
要件
1.オペレーティングシステム
1. 装置搭載 OS に関する要求
2. パッチ適用手順の技術文書作成
2.ネットワークセキュリティ
3. 安全な通信転送プロトコルのサポート
4. ネットワーク構成の技術文書作成
3.エンドポイント保護
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
10. アクセス権の設定
4.セキュリティモニタリング
11. セキュリティイベントログ
12. ログタイプ


keypasco
受賞と特許
AWS Cloud Challenge 2019 トップテン
2022 Select USA Sumit サイバーセキュリティ部門 1位
特許一覧
会社情報
Lydsec Digital Technology Co. Ltd.
台湾
2012年
アメリカ、オランダ、スウェーデン等
ISO27001
GDPR
PSD2

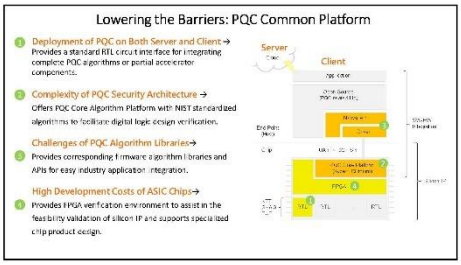
附件四、參訪獨立行政法人情報處理推進機構雙邊交流簡報

（一）後量子遷移的資安機會與挑戰

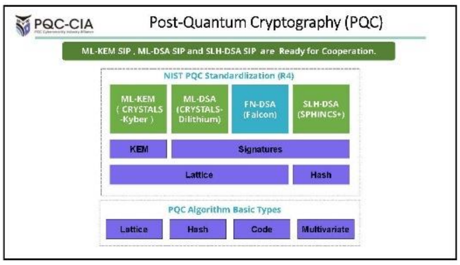
2025/6/26

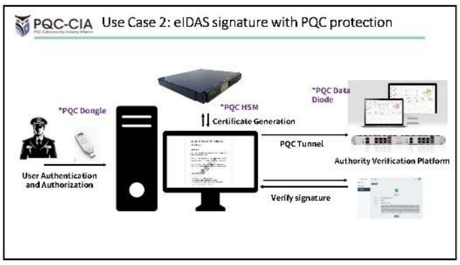
1

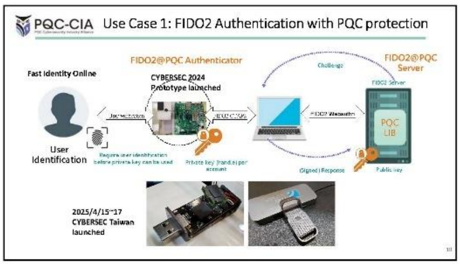
2025/6/26

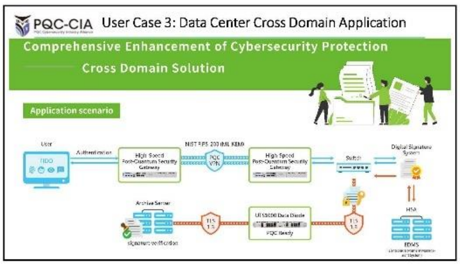


2









PQC-CIA Conclusion

The **Years-to-Quantum (Y2Q)** crisis will start in 2026.

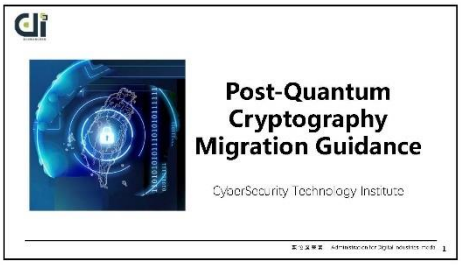
(Elena Yndurain, https://www.linkedin.com/pulse/y2q-and-current-cybersecurity-elena-yndurain)

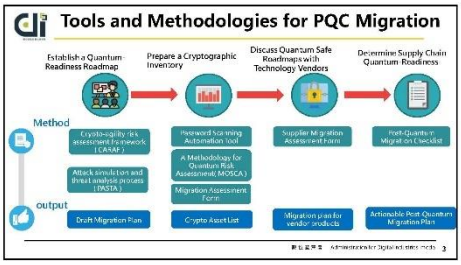
We all are facing the PQC Migration Issues
Hope that we can
(1)Share the strategy for PQC migration
(2)Share the case studies each other
(3)Share the PQC-ready ICs, devices and solutions partners

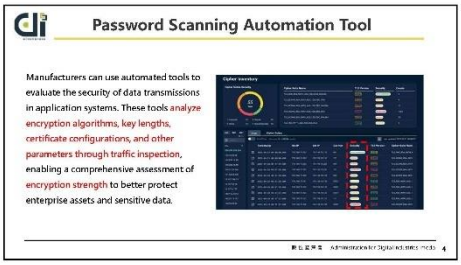
PQC-CIA
PQC Cybersecurity Industry Alliance

（二）後量子遷移指引

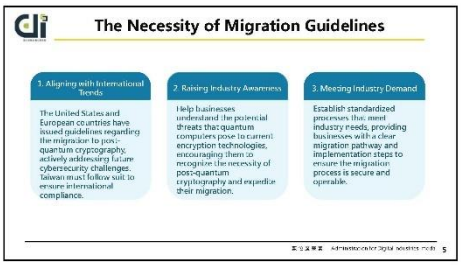
2025/6/26







2025/6/26



附件五、參訪工研院日本辦公室分享簡報

附件六、臺灣資安館展會執行記錄

執行紀錄(展館照片)

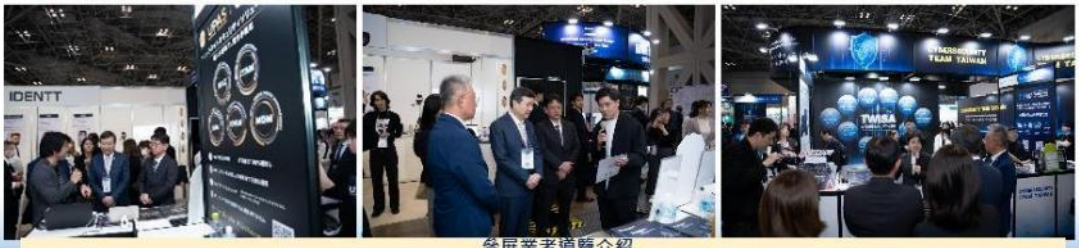
CYBERSECURITY TEAM TAIWAN

19

執行紀錄(展館照片)

CYBERSECURITY TEAM TAIWAN

參展業者導覽介紹



參展業者導覽介紹

執行紀錄(展館照片)

CYBERSECURITY TEAM TAIWAN

啟動儀式/大合影

大合影/參展業者導覽介紹

執行紀錄(展館照片)

CYBERSECURITY TEAM TAIWAN

開幕式準備

貴賓致詞

執行紀錄(展館照片)

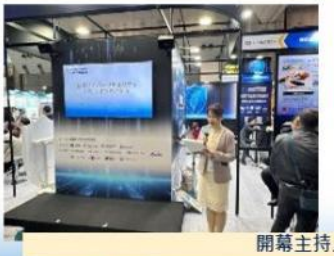
CYBERSECURITY TEAM TAIWAN

媒體採訪

執行紀錄(展館照片)

CYBERSECURITY TEAM TAIWAN

短講活動



開幕主持人/翻譯人員推廣

執行紀錄(媒體露出)

廣告換算價值
¥3,933,880

CYBERSECURITY TEAM TAIWAN

	刊登日	記錄日	媒體名	Title	URL	廣告換算價值
1	2025/4/24	2025/4/25	MSNニュース	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://www.msn.com/ja-jp/technology/cybersecurity/cybersecurity-team-taiwan%E3%81%8C-japan-it-week-%E6%98%A5-2025-%E3%81%AB%E5%87%BA%E5%B1%95-%E5%8F%B0%E6%B9%BE%E3%81%AE%E5%85%88%E9%80%B2%E7%9A%84%E3%81%AA%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%BD%E3%83%AA%E3%83%A5%E3%83%BC%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%92%E4%B8%96%E7%95%8C%E3%81%AB%E7%99%BA%E4%BF%A1/ar-AA1DiwF0	¥1,279,475
2	2025/4/24	2025/4/25	MSNニュース	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://www.msn.com/ja-jp/lifestyle/shopping/cybersecurity-team-taiwan%E3%81%8C-japan-it-week-%E6%98%A5-2025-%E3%81%AB%E5%87%BA%E5%B1%95-%E5%8F%B0%E6%B9%BE%E3%81%AE%E5%85%88%E9%80%B2%E7%9A%84%E3%81%AA%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%BD%E3%83%AA%E3%83%A5%E3%83%BC%E3%82%B7%E3%83%A7%E3%83%B3%E3%82%92%E4%B8%96%E7%95%8C%E3%81%AB%E7%99%BA%E4%BF%A1/ar-AA1DiwF0	¥1,279,475
3	2025/4/21	2025/4/25	ノアドット	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://nordot.app/1286945637714640937?c=414795408717890657	¥406,715
4	2025/4/19	2025/4/25	livedoor	「Japan IT Week 春 2025」に出展！TWISA	https://news.livedoor.com/article/detail/28591370/	¥1,159,294
5	2025/4/23	2025/4/23	South65	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://south65.jp/cybersecurity-team-taiwan%E3%81%8C-%E3%80%8Cjapan-it-week-%E6%98%A5-2025%E3%80%8D%E3%81%AB%E5%87%BA%E5%B1%95%E3%80%81%E5%8F%B0%E6%B9%BE%E3%81%AE%E5%85%88%E9%80%B2%E7%9A%84%E3%81%AA%E3%82%BB%E3%82%AD/	¥11,724
6	2025/4/22	2025/4/22	イチオシ	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://ichioshi.smt.docomo.ne.jp/articles/news/33055	¥7,227
7	2025/4/21	2025/4/22	@nifty ニュース	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://news.nifty.com/article/item/neta/12374-4039361/	¥359,958
8	2025/4/21	2025/4/22	Cubeニュース	CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信	https://news.cube-soft.jp/article/3974746	¥18,233

執行紀錄(媒體露出)

CYBERSECURITY TEAM TAIWAN

36	2025/04/18	2025/04/21	Newsweek	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://www.newsweekjapan.jp/press-release/2025/04/cybersecurity-team-taiwantwisa42325japan-it-week-2025.php	¥25,627
37	2025/04/18	2025/04/21	PC Watch	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://pc.watch.impress.co.jp/docs/release/atpress/2006158.html	¥22,884
38	2025/04/18	2025/04/21	SANSPO.COM	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://www.sanspo.com/pressrelease/atpress/Z2NZVBWEVBMKRBVG3MMIRTMT5M/	¥26,504
39	2025/04/18	2025/04/21	StartHome	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://home.kingsoft.jp/news/pr/atpress/433802.html	¥10,714
40	2025/04/18	2025/04/21	zakⅡ	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://www.zakzak.co.jp/pressrelease/atpress/Z2NZVBWEVBMKRBVG3MMIRTMT5M/	¥20,622
41	2025/04/18	2025/04/21	インターネットコム	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://pressrelease.internetcom.jp/release/4174579.html	¥2,291
42	2025/04/18	2025/04/21	徳島新聞Web	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://www.topics.or.jp/ud/pressrelease/6801fffba f6d3417ee000000	¥4,646
43	2025/04/18	2025/04/21	財経新聞	CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！	https://www.zaikei.co.jp/releases/2896293/	¥2,821

61

執行紀錄(媒體露出)

CYBERSECURITY TEAM TAIWAN

MSNニュース

CYBERSECURITY TEAM TAIWANが「Japan IT Week 春 2025」に出展、台湾の先進的なセキュリティソリューションを世界に発信

65

執行紀錄(媒體露出)

CYBERSECURITY TEAM TAIWAN

財経新聞

CYBERSECURITY TEAM TAIWANを率いる台湾情報セキュリティ協会(TWISA) 4月23日～25日開催の「Japan IT Week 春 2025」に出展！

102


自由時報專訪報導(平面/電子)
CYBERSECURITY TEAM TAIWAN
台灣資安館 前進日本IT展
台積電建高雄6廠?
水電有準備
平面報紙
電子新聞 https://ec.ltn.com.tw/article/paper/1703290


執行紀錄(媒體露出)
CYBERSECURITY TEAM TAIWAN
https://picsee0328.pse.is/7hw49a
台灣資安大聯盟赴日參展 展現資安實力、拓展國際合作新契機

展後效益報告

CYBERSECURITY TEAM TAIWAN

Japan IT Week | Japan DX Week | Sales x Digital Marketing Week | E-commerce x Store Week

Visitors Count

Tokyo Spring Show, 2025

Apr.23(Wed) - 25(Fri) 2025 | Tokyo Big Sight, Japan | 10:00-18:00 (until 17:00 on the last day)

April 30, 2025 RX Japan Ltd.

Apr.23 (Wed.)	Apr.24 (Thu.)	Apr.25 (Fri.)	3-days total
16,269	19,503	22,030	57,802

*The daily number of visitors is the number of visits a day. A person is counted only once per day.
*The total number of visits equals the number of visitors of that day plus the total number of repeat visits.
*Above number does not include exhibitors nor press attendees.

146

展館交流-總結數據

CYBERSECURITY TEAM TAIWAN

數據項目	筆數
展覽三天到訪總人數(RX提供)	57,802
台灣資安館到訪總人數(約估)	980
開幕觀眾總人數(約估)	60
App掃描到訪展館入場證總筆數	780
媒合商談紀錄筆數(廠商提供)	33
參展商名片搜集筆數(廠商提供)	56

日本警視廳至攤位

媒合商談桌

展覽首日開幕盛況

155