出國報告（出國類別：開會）

出席2019年不請自來網路組織（UCENet）國際會議出國報告

服務機關：國家通訊傳播委員會
姓名職稱：吳銘仁簡任技正
周金賢技正
派赴國家/地區：加拿大/蒙特婁
出國期間：**108**年**10**月**12**日至**10**月**19**日
報告日期：**108**年**12**月**19**日

摘要

Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG，或稱 M3AAWG)是一個以科技為主且中立的國際非政治性組織，在全球擁有二百多名成員，主要關注網際網路資源濫用問題，涵蓋科技、產業合作和公共政策，致力於降低機器人（Bot）、惡意軟體（Malware）、垃圾郵件（Spam）、病毒（Virus）、阻斷服務攻擊（DoS）和廣告推銷所造成的各種網路威脅或攻擊，並制定濫用網際網路資源的有效方法。

本次會議由不請自來網路組織（The Unsolicited Communications Enforcement Network，“ UCENet“）組織，及「反濫用訊息、惡意軟體、行動通訊工作群組」(Message Malware Mobile Anti-Abuse Working Group，“ M3AAWG “)兩大組織共同舉辦，本會係 UCENet 組織之會員國，UCENet 的會員國主要為各國在垃圾郵件防制上的主政機關，M³AAWG 最初名為 M（Message）AAWG，為訊息反濫用工作組織，但隨著垃圾郵件的興起，該組織在 2012 年將其名稱變更為訊息、惡意軟體和移動裝置反濫用工作組織，M³AAWG 本著互助合作之精神，組織範圍已擴及電子郵件服務提供者（Email Service Providers）和對保護線上生態系統感興趣的審查方。

參加這次會議，除了在參與之會議中說明我國在防制垃圾郵件上的努力及最新進度，並且安排了臺日雙邊會談，這個會談已經持續了幾年，對於雙邊在防制垃圾郵件上的合作已累積相當多的經驗，值得繼續維持下去，以獲得更多的成果。

目次

壹、前言

Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG，或稱M3AAWG)是一個以科技為主且中立的國際非政治性組織，在全球擁有二百多名成員，主要關注網際網路資源濫用問題，涵蓋科技、產業合作和公共政策，致力於降低機器人（Bot）、惡意軟體（Malware）、垃圾郵件（Spam）、病毒（Virus）、阻斷服務攻擊（DoS）和廣告推銷所造成的各種網路威脅或攻擊，並制定濫用網際網路資源的有效方法。

M³AAWG 由網際網路服務供應商（Internet Service Providers，ISP）、移動網路運營商（Mobile Network Operators）、電信公司（Telecommunications Companies）和基礎設施供應商（Infrastructure Vendors），以及反垃圾郵件技術供應商（Anti-Spam Technology Vendors）所組成。M³AAWG 最初名為 M（Message）AAWG，為訊息反濫用工作組織，但隨著垃圾郵件的興起，該組織在 2012 年將其名稱變更為訊息、惡意軟體和移動裝置反濫用工作組織（Messaging Malware Mobile[1] Anti-Abuse Working Group），M³AAWG 本著互助合作之精神，組織範圍已擴及電子郵件服務提供者（Email Service Providers）和對保護線上生態系統感興趣的審查方。

各國可在 M3AAWG 會議上，針對訊息濫發提出討論、作法、法規制訂與執行現況，並依照不同的領域性（垃圾郵件、廣告簡訊、廣告電話、Do Not Call、RoboCall），再區分為技術面、政策面、各國現況等不同主題舉行各別會議。在M³AAWG（The Messaging, Malware and Mobile Anti-Abuse Working Group）的組織中，本會加入的會員組織為 UCENET（THE UNSOLICITED COMMUNICATIONS ENFORCEMENT NETWORK），其前身為 LAP（THE LONDON ACTION PLAN），

[1] Messaging：解決任何訊息傳遞平臺上的濫用問題，從電子郵件到簡訊系統；Malware：垃圾郵件和許多其他形式的濫用只是真正疾病的症狀，它們的主要目的是利用病毒、惡意代碼或是蠕蟲等惡意行為秘密地感染使用者系統。如果我們阻止惡意程式入侵系統，對使用者造成的傷害或影響就會消失；Mobile：保護這個無處不在的平臺，免受惡意程式和訊息傳遞濫用的影響，包括文字和語音服務。

組織成員主要為各國在垃圾郵件防制上的主責機關，共同交流與垃圾郵件有關之「情報」、「法規」、「溝通」、「訓練」等議題。

本會及財團法人電信技術中心皆有派員參加本次會議，出席人員如下：

本會基礎設施事務處 吳簡任技正銘仁

本會基礎設施事務處 周技正金賢

財團法人電信技術中心資通安全組 林副主任高裕

財團法人電信技術中心資通安全組 呂副工程師敏漢

圖 1 M³AAWG 出席人員

由左至右分別為林高裕（TTC）、周金賢（NCC）、吳銘仁（NCC）、呂敏漢（TTC）

貳、會議目的與議程安排

一、會議目的

M3AAWG（Messaging Malware Mobile Anti-Abuse Working Group）是各國聯合起來共同打擊殭屍網路（Botnets）、惡意程式（Malware）、垃圾郵件（Spam）、病毒（Viruses）、服務的阻斷（DoS）攻擊和其他在線攻擊而合作的國際組織。也是一個以科技為主且中立的非政治性國際組織。

本次會議由不請自來網路組織（The Unsolicited Communications Enforcement Network，“UCENet“）組織，及「反濫用訊息、惡意軟體、行動通訊工作群組」(Message Malware Mobile Anti-Abuse Working Group，“M3AAWG “)兩大組織共同舉辦，本會係 UCENet 組織之會員國，UCENet 的會員國主要為各國在垃圾郵件防制上的主政機關，M³AAWG 最初名為 M（Message）AAWG，為訊息反濫用工作組織，但隨著垃圾郵件的興起，該組織在 2012 年將其名稱變更為訊息、惡意軟體和移動裝置反濫用工作組織。

參加這次會議，除了在參與的會議中說明我國在防制垃圾郵件上的努力及最新進度，並且安排了臺日雙邊會談，這個會談已經持續了幾年，對於雙邊在防制垃圾郵件上的合作已累積相當多的經驗，值得繼續維持下去，以獲得更多的成果。

二、議程安排

議程說明：10 月 16 下午之議程「Caller Identification Authentication and Network Level Call Blocking -OPEN」與 10/17 下午之議程「Phone Numbers and the Global Regulation Landscape」具高度相依與關聯性，後續將針對此二議程進行合併說明。

會議行程與議程安排		
日期	上午	下午
10 月 14 日 星期一	• Public Speaking Survival	• Playing with paste: Linux for beginners • OPEN UCENet Members (ALL) Meeting
10 月 15 日 星期二	• (LE Only) Current State of SMS and Email Spam in Korea - CLOSED	• UCENet/M³AAWG Abusive Material Takedown Best Practices
10 月 16 日 星期三	• Bilateral meeting between NCC/TTC and JADAC 臺日雙邊會談	• Caller Identification Authentication and Network Level Call Blocking -OPEN • Robocall and Do Not Call Enforcement - OPEN
10 月 17 日 星期四	• Taking NOTICE: Identifying Vulnerable IoT Devices in Japan • (LE Only) Unlawful Messaging and Consumer Protection: The Intersection of Enforcement and Regulatory Regimes - CLOSED	• Phone Numbers and the Global Regulation Landscape

參、重要議題討論過程

一、Public Speaking Survival（公開場合演說生存之道）

本會議主持人為 Facilitation First, Inc. 的 Kevin Quinn，分為上午及下午兩場次。M³AAWG 會議為各國資安人員互相交流之場合，藉由發表演說與主持小組會議，期望能達到國際合作之最大效益。

與會者可在小組中做快速的模擬練習並達成下列幾個目的：強化演講之表達能力、控制自己在臺上的表現、如何與觀眾互動，並將這些技巧運用在下一次的演講或是會議主持。議程中 Kevin Quinn 多以互動的方式進行說明，因篇幅有限，以下節錄議程的整體結構與部分重點說明，不針對互動環節多作著墨。

Kevin Quinn 在其提供的資料中(詳附錄)說明本次會議期望能達到下述四種效益，分別是如何利用最佳的方式完成一場屬於自己的演講；如何完成最棒的演講稿以吸引觀眾；如何利用聲音、儀態與動作等強化個人的影響力，最後則是利用輕鬆的心態面對觀眾的壓力。

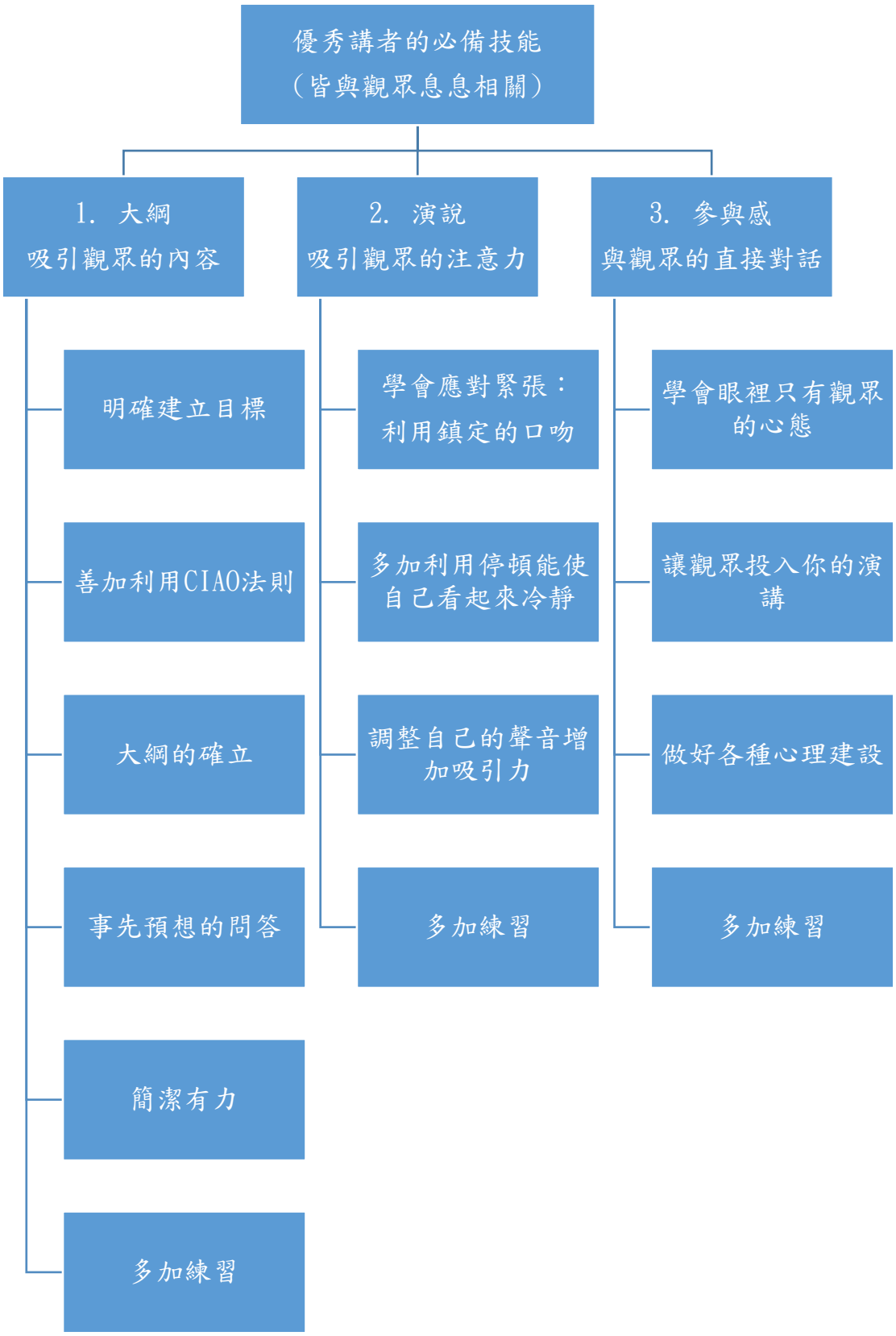

圖 2 優秀講者必備技能樹狀圖

表達能力與正確傳遞訊息是整場會議之重點，若沒有優秀出色的表達能力，縱使你的想法、方案再優秀，都得不到應有的關注，絕佳機會將會離你遠去，甚至是危險的警告會被忽視，值得提出的想法將會胎死腹中，對任何人都有實質影響。當你有更好的表達能力，將能獲得更多的機會展示你的想法與計畫視，無論是個人職涯所需、領導統御能力，或想參與更頂尖團隊以解決問題，如國際行動組織會議，優秀的表達能力將是關鍵之一。

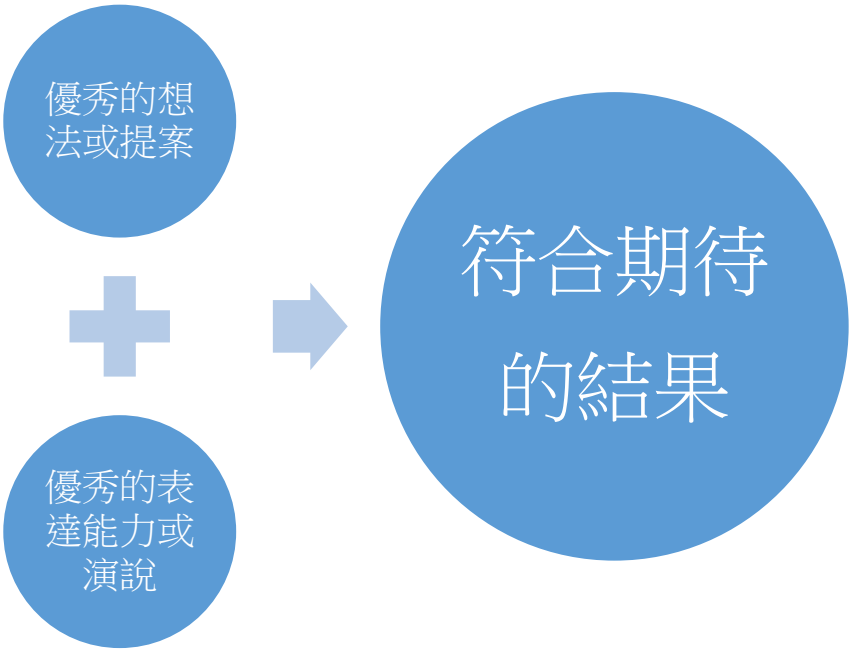

圖 3 完美結果的要件

前段敘述了一場優秀的演說或是符合期待的結果，其必備條件需要特別的想法或內容，以及極佳的表達能力，但若在內容或想法幾乎完美的前提下，仍有可能因為表達方式的不同，而造成不同結局，我們將兩者作一個比較：

表 1 演說效益之比較

效果不彰的演說	有效益的演說
● 觀眾對此主題無興趣或對其沒有益處 ● 提議的目的或結果不夠明顯 ● 過於冗長 ● 演講者的聲音風格單調、冷漠或是沒有誠意 ● 沒有具體的例子 ● 造成觀眾不舒適的簡報呈現	● 為滿足觀眾需求而客製的主題 ● 目的足夠明確的 ● 結果具體且對觀眾有利 ● 符合邏輯並吸引觀眾 ● 演講者對主題的熱情是顯而易見的一信心的呈現 ● 善用例子、故事、證據或問題來強化想呈現的資訊

● 未能嘗試吸引聽眾	● 觀眾是持續的保持互動

開場的最佳方式就是“CIAO”法則，有什麼強而有力的理由能讓聽眾在你說第一句話的時候就立刻被吸引？以下是 Kevin Quinn 建議的方式:

表 2 CIAO 要素說明

要素	描述	目的
Context 內容	內容的背景	讓觀眾可以快速進入狀況
Important 重要性	主題的重要性	與觀眾建立起關聯
Ask 要求	要求某些特定事項	請觀眾執行某些特定事項並確立演講的目的
Outcome 效益	執行的好處或效益	針對你對觀眾的要求回覆觀眾相對應的期待

這四個詞的第一個字母構成了縮寫“CIAO”(發音為 CHEE OW)。CIAO 是義大利問候語或告別語的表達方式，應在所有演講的開始(和結束)時使用，以本次 M³AAWG 為例：

表 3 CIAO 要素舉例

要素	舉例：此訓練議程	舉例：M³AAWG
Context 內容	演講或分享會議對教育他人至關重要	惡意“Bot”已被證明是許多備受關注之濫用案件的關鍵
Important 重要性	許多人致力於研究此議題的解決方法，但遲遲無法解決	M33AAWG 成員幫助 ISP 創建了一個新的反 bot 行為準則(Anti-Bot Code，ABC)，並在全球被採用
Ask 要求	利用下述的方式可以幫助你達到需求	與您的連絡人和利益相關人一起推廣此代碼
Outcome 效益	成功的舉例或演示會給觀眾或是其組織帶來具體的回報	如果我們現在就採取行動，並採納這一準則，我們就能遏制這一愈演愈烈的濫用行為

二、OPEN UCENet Members (ALL) Meeting（UCENet 成員大會）

此議程的主講者是加拿大廣播電視與電信委員會的高級顧問 Dana-Lynn Wood，與會人員包含所有的成員國，M³AAWG 的宗旨是通過國際合作、資訊分享和實際行動促進全球對消費者的保護。M³AAWG 的使命是透過網路最大限度地加強國際間的合作與資訊的分享，並加強單邊、雙邊和多邊的合規和執法方法和行動。

Dana-Lynn Wood 在其提供的資料中(詳附錄)說明 UCENet 由一般成員和執行委員會組成。為了實現使命，UCENet 有三個主要的優先任務。每個項目都由一個委員會專責的委員負責支援。

成員則包括監管機構、執法機構和其他政府機構，其職責是推廣與法規的執行，以及致力於防止未經請求的通訊或其他通訊的濫用行為。新成員的入會資格主要在於委員會的審查，在審查評估欲入會成員所屬角色、活動和對網路的潛在貢獻後，再決定是否可以入會。執行委員會由至少五名成員組成，他們必須承諾投入更多的時間和資源來支援網路的活動。每個工作小組會由至少兩名成員共同負責。委員會亦鼓勵各級人員和相關機構參與工作小組，以確保參與成員和專業知識的多樣性。

(一)智慧與合作

合作向成員國收集、分析、交流和傳播情報和資訊，包括探索創新的合作方式和途徑。工作小組負責確定成員感興趣的領域，協調聯合情報收集和交流活動，並審查分享現有資訊的創新方法。工作小組還將酌情考慮與其他國際執法網路和組織協調共用的機會。

(二)溝通和參與

推廣 UCENet 的相關活動並促使其成功，借助成員的優勢，促進對各自司法管轄區的理解和協助，以加強合作和協調。工作組負責制定一項溝通策略，鼓勵成員

之間的資訊流動，對外促進成員資格和 UCENet 活動，吸收新成員和不活躍的成員，並克服參與的語言和其他障礙。

(三)培訓和發展

為會員組織提供或推廣有意義的培訓，瞭解並善加利用會員的專業知識，包括各國法規調查、執行方法和技術。工作小組會負責確定或協調培訓機會，並與成員夥伴合作，以促進、開發和提供創新的培訓課程，如 M³AAWG 年會就是最好的例子。

藉由每年度的 M³AAWG 會議，委員與成員會互相討論目前組織或各單位遇到的瓶頸與困境，並藉由討論提供彼此最佳的解決方式。已近兩年為例，年會遇到一個很大的問題便是如何擴大組織的規模，讓願意參與此國際組織或合作的國家與會員增加。以非洲地區的國家而言，不論在文化、語言、經濟或制度等，都讓主辦方面對極大的困難與相關單位進行溝通合作。又例如數年前有位杜克大學的安德列先生提出的價值主張的論點，認為對於企業或是組織而言，利益與價值是至關重要的，這影響了企業或是組織調度使用員工的考量，大家寧願將重點人力或資源放在這些有形的利益或是成效上面，對於短期內不會有成效或是意義的事物不聞不問。這會是此年會所遭遇很大的瓶頸與困境。但對於 M³AAWG 在近幾年也不是完全沒有任何成效，仍然陸續有些許美洲或是拉丁美洲國家的成員陸續加入。

委員們從這幾年的規劃與活動中得到的不外乎是經驗教訓和聯繫的技巧，許多國家有其聯繫上與溝通的難度，但對於委員們來說，他們希望強調一件事情，這些事情不全然是委員的責任，而是所有成員國需要一起面對的問題，某些特定國家或許對於委員們來說不好親近或是介入，但對於某些成員國而言卻是很親近的國家，此時的成員國又何嘗不是一個有利的推手呢？

後來各會員國與委員之間亦針對每年度舉辦會議的地點進行了討論，對於每年在固定的幾個國家（歐洲或美洲）進行會議的召開頗有微詞，成員國提出在不

同的國家進行會議，是個非常好的機會去深入不同的國家瞭解其風俗民情，對於會員國的招募也很有利，衍生的好處是對於他國也有一些經濟上的發展效益，這對於未加入 M³AAWG 的國家而言都會是一個吸引他們加入的好切入點。委員們則認為這是一個非常好的出發面向，但對於時程上的規劃必須進行一些討論，且當初規劃美洲與歐洲等相關國家，其實對於各國的距離而言，評估取得了一個最佳的中間值，所以委員們覺得，這個中間值也是讓眾多國家願意前來與會的一個考量。而且在同一個地點建立起會議的威信也是至關重要的，以往年的紐約會議為例，去年便有了電視台的採訪與對外媒體播出，這是需要一段時間或是更長的時間去進行建立與維護的，雖然短期有短期的效益，但我們更希望長期效益所帶來的組織成場。五至六年前，一開始只有二十七位會員國，到現在的成長，其實組織花了很長的時間去維護信譽與價值，對於其他未加入的國家而言，要吸引他們加入不是一朝一夕，而是長遠的讓他們知道我們做到了哪些事情，具備哪些價值，才有說服他們加入的理由，所以回到最初的信念，長期的價值是委員們目前統一認同的發展面向。

三、(LE Only) Current State of SMS and Email Spam in Korea - CLOSED（韓國垃圾簡訊與郵件之現狀）

此會議的主講者為韓國網際網路安全局（Korea Internet & Security Agency，以下簡稱 KISA[2]）的 JEESOO JEON，JEESOO 一開始即開宗明義的說明 KISA 的組織定位以及目標。

JEESOO JEON 在其提供的資料中(詳附錄)說明 KISA 的成立有五大目標，包含：改善網路環境、資訊安全產業的訊息推廣、網路攻擊（犯罪）的應對、個資的防護與非法垃圾郵件的處置，期望能有效的針對網路犯罪、網路詐騙、垃圾郵件或惡意程式等侵權違法的行為進行防制。

對於非法垃圾郵件的處置，KISA 成立了「非法垃圾郵件應對中心(Illegal Spam

圖 4 KISA 組織營運目標

Response Center)」，並從五個面向發展強化韓國對於垃圾郵件防制的能量，分別

[2] KISA 成立於 1996 年 6 月，是韓國科學技術情報通信部(Ministry of Science and ICT，MSIT)的轄下組織，主要任務除了分配與維護韓國的 IPv4 及 IPv6 位址，亦包含自治系統編號（Autonomous system number，ASN）和.kr 的國家/地區代碼頂級域名，並負責韓國境內互聯網的網路安全性（整理自維基百科 Wikipedia）

為：向民眾宣導如何防制垃圾郵件、接收民眾對於垃圾郵件的陳情、提高民眾的警覺、發展對垃圾郵件防制的技術能量與積極強化與國際間垃圾郵件防制組織的合作。

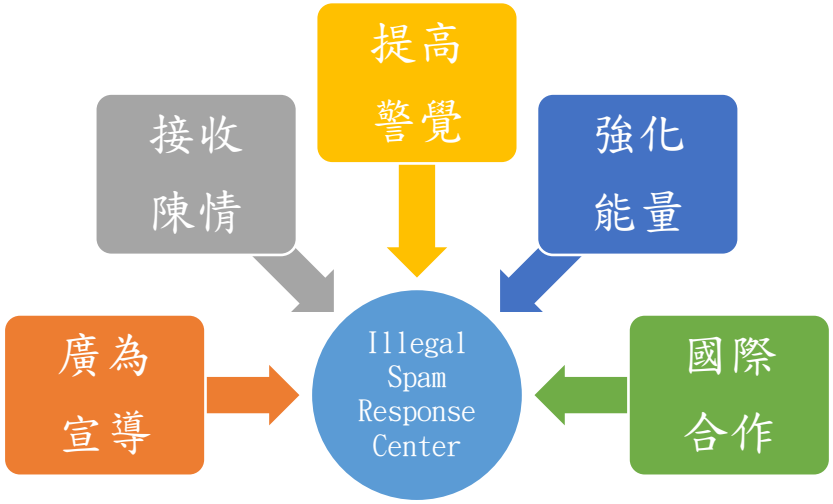

圖 5 KISA-非法垃圾郵件應對中心發展面向

韓國亦針對垃圾郵件成立了相關法案，法案規定了五大準則如下：必須經過使用者同意才能推送廣告訊息、廣告訊息會被強制性的加上相關標籤、使用者具取消接收廣告訊息的權利、不得於晚間九點至早上八點期間重複推播廣告訊息以及提高廣告訊息在晚間傳送的限制，期望藉由法律的強制力與約束力，有限度地杜絕廣告訊息的濫發情形。

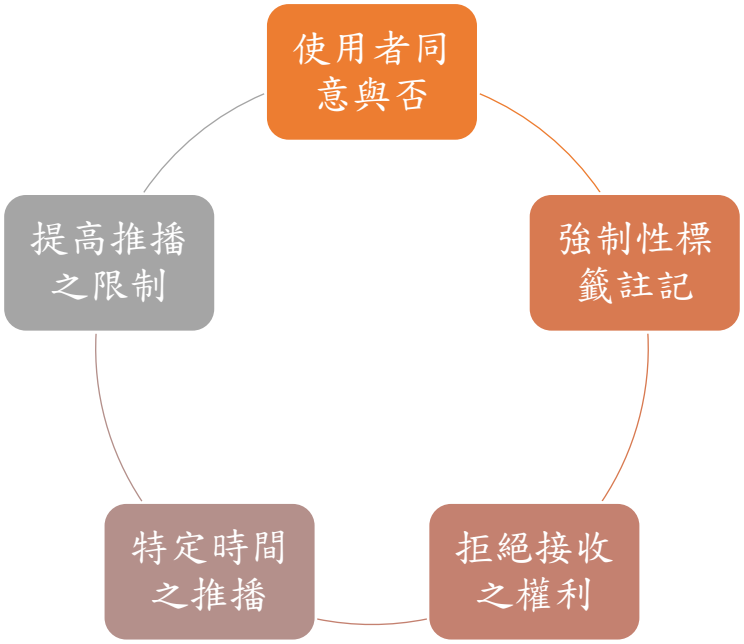

圖 6 KISA 垃圾郵件法規五大準則

韓國代表亦針對其國內垃圾郵件狀態做了相關的統計與回報，垃圾郵件是違背使用者意圖而傳播的廣告資訊。通過對商業廣告資訊的調查報告，確認其違法使用資訊通信網路的目的、管理辦法或根據廣告的類型進行調查。由圖 7 中可以得知每年收到超過 3000 萬份垃圾郵件報告，其中手機垃圾郵件報告占比更高比總數的 99%還要多。

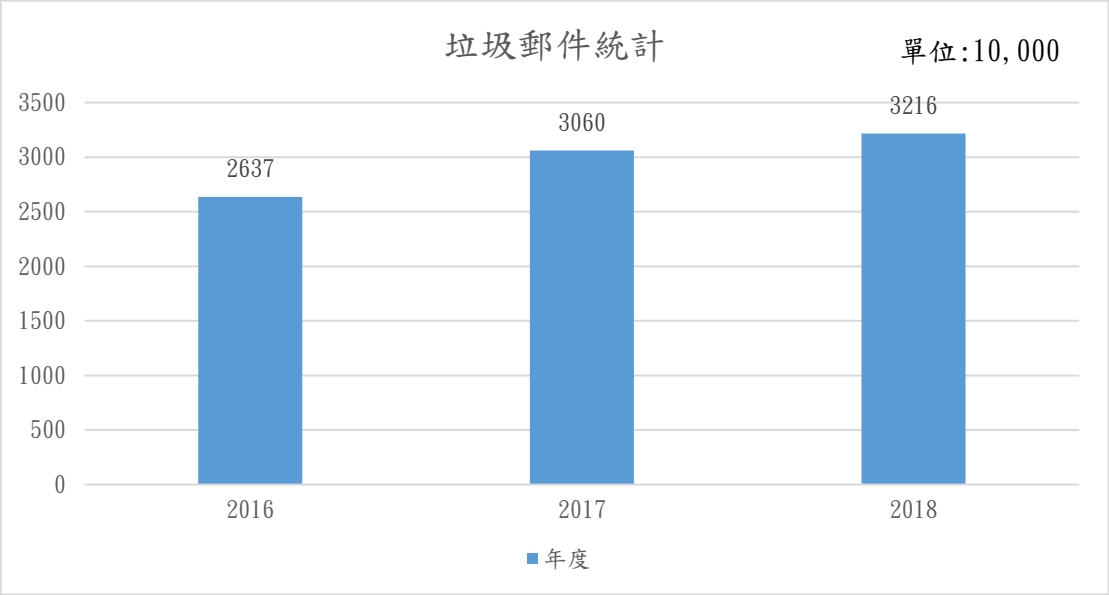

圖 7 KISA-近年垃圾郵件統計

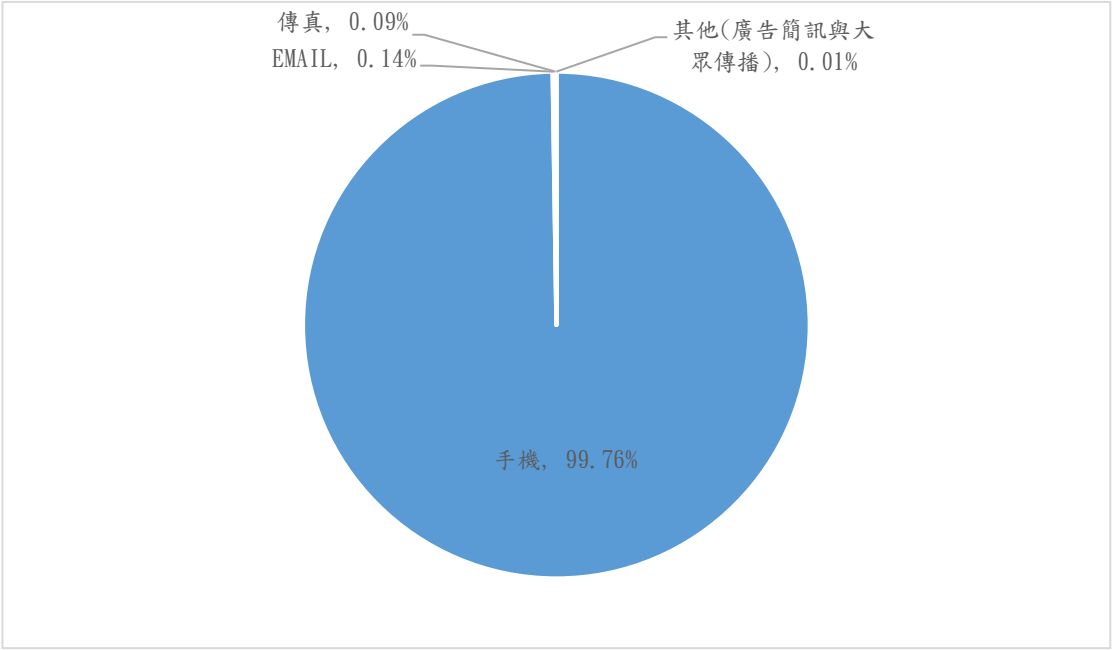

圖 8 KISA-垃圾郵件類型比例

在所有的手機垃圾郵件中，統計 2019 年 1 月至 5 月區間，其中約 490,000 宗與股票垃圾郵件有關。占總數的 7.1%，排名第三，其次是賭博(41.4%)以及非法貸款(11.5%)。大多數報告都會推薦高回報的股票（績優股）資訊並請使用者回覆請求，隨後將引導使用者連結到 Kakaotalk、線上俱樂部或其他惡意網址。

KISA 亦透過國際間的合作，防堵 SPAM 的氾濫，在 2018 年所有國外的電垃圾郵件數量統計中，12 個合作國夥伴約佔了 88%-92%，但在今年 2019 年的統計，

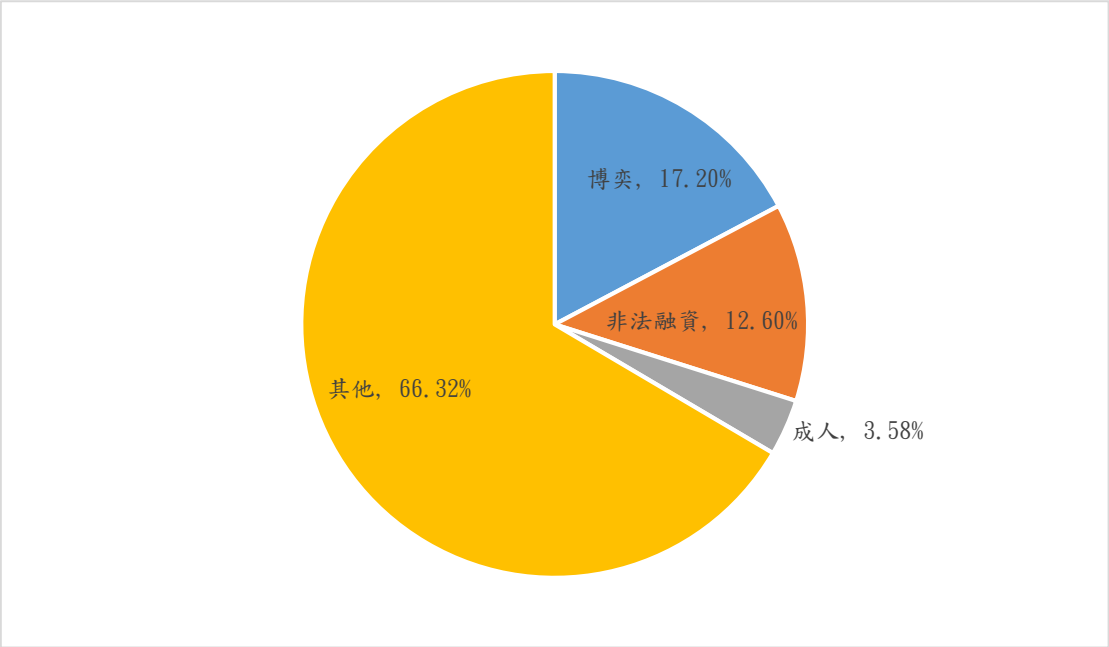

圖 9 KISA-垃圾郵件（手機）類型比例

來自合作國夥伴的垃圾郵件數量約降至了 62.3%。與往年相比有非常顯著的效益。（12 個合作國夥伴分別為：臺灣（NCC）日本 (JADAC)、中國(12321 Center)、紐西蘭(DIA)、澳洲(ACMA)、 加拿大(CRTC)、香港(OFCA)、英國(ICO)、馬來西亞(MCMC)、印度 (Cert In)與巴西(Cert)）。

對於垃圾郵件的防制，KISA 提出了他們的防制方式與手段，其中包含了：手機回報機制的優化、監控機制（Spamtrap）的輔助、預防機制（手機號碼的顯示）。另外，亦建立定期現場檢查制度，針對可疑的運營商或違反行為，並與大韓民國廣播通訊委員會（Korea Communications Commission，KCC[3]，等同於臺灣NCC）以及檢調單位合作針對其違反程度執行行政處罰或刑事處罰。

圖 10 韓國垃圾郵件防制之國內合作

[3] 廣播通訊委員會是韓國有關通訊與廣播事務的最高主管機關，也是韓國總統直屬機關之一。其機構是仿照美國聯邦通訊委員會的架構，以 2008 年 2 月 29 日的《廣播通訊委員會設置以及運作相關法律》為基礎而設立。除了是來研究、管理廣播、通訊、頻譜，也是建立相關政策的機構，其下另設置廣播通訊審議委員會，以審議、決議上述政策。（參考自維基百科 Wikipedia）

四、UCENet/M³AAWG Abusive Material Takedown Best Practices

（有效防制資源濫用的最佳實踐）

此議程的主講者為紐西蘭內政部的 Jolene Armadoros，旨在探討今年 3 月發生的「基督城清真寺槍擊案[4]」，並在後續 5 月所召開的「基督城行動呼籲高峰會[5]」的相關議題延伸。

Jolene Armadoros 在其提供的資料中(詳附錄)說明 M³AAWG 正在研究分析一種避免資源濫用的協議與執行方式，並嘗試推廣以支持基督城行動呼籲和任何未來的提倡的相關目標，希望能以 Crisis Protocol[6]為基礎，致力於打擊網上恐怖主義和暴力極端主義的內容或文章，並推廣促使全球進行合作。由 M³AAWG 和

[4] 基督城清真寺槍擊案（Christchurch mosque shootings）發生於 2019 年 3 月 15 日紐西蘭夏令節約時間下午 1 時 40 分（協調世界時 0 時 40 分），一名槍手闖入紐西蘭基督城的光明清真寺和林伍德伊斯蘭中心，共造成 51 人死亡。紐西蘭總理傑辛達·阿德恩定性該事件為恐怖襲擊。其中一名槍手行兇時通過 Facebook 進行現場直播。當局確認其中一名兇手為在澳洲出生的 28 歲男子布倫頓·塔蘭特。該兇手在其槍枝和社交媒體投稿上展示有新納粹主義符號、基督徒打敗穆斯林戰役的名稱，以及歐洲恐襲中恐怖分子的姓名。目擊者看到多人受槍擊倒地，受害人不分性別年紀。報導亦指司直蘭街（英語：Strickland Street）一被撞毀的車內發現一枚炸彈。是次槍擊案為 1997 年華利姆大屠殺（Raurimu Massacre）後紐西蘭首宗大型槍擊案，亦是 1809 年的博依德大屠殺之後發生在紐西蘭最嚴重的屠殺事件。該槍手持有半自動步槍及簡易爆炸裝置施襲，武器使用也相當熟練；加上當地學生於同日發生罷課遊行呼籲關注全球暖化議題，事件引起各方高度關注。紐西蘭採用較為寬鬆的槍支控管政策，2017 年全國槍證申請通過率達到 99.6%，另據警方估計，2019 年紐西蘭僅半自動軍用武器持有人接近 7000 人(參考自維基百科 Wikipedia)。

[5] 基督城行動呼籲高峰會（Christchurch Call to Action Summit 或 Christchurch Call）是由紐西蘭總理傑辛達·阿德恩發起的政治峰會，於 2019 年 5 月 15 日在法國巴黎舉行，召開的兩個月前，克賴斯特徹奇清真寺於 2019 年 3 月 15 日發生槍擊事件。此次峰會由阿德恩和法國總統埃馬紐埃爾・馬克龍(Emmanuel Macron)共同主持，旨在「讓各國和科技公司走到一起，試圖終結利用社交媒體組織和宣傳恐怖主義和暴力極端主義的能力」。世界各國領導人和科技公司承諾「消除網路上的恐怖主義和暴力極端主義內容」；最初有 17 個國家簽署了不具約束力的協定，于同年 9 月 24 日與另外 31 個國家簽署了不具約束力的協定。該承諾包括三個部分或承諾：一個針對政府，一個針對線上服務提供者，一個針對兩者之間合作的方式。(整理自維基百科 Wikipedia)

[6] Crisis Protocol（危機管理）是一個組織處理破壞性和意外事件的過程，這些事件威脅到組織或其利益相關者。危機管理的研究始於 20 世紀 80 年代的大規模工業和環境災難。危機有三個共同的要素：(a)對組織的威脅，(b)出其不意，(c)決策時間短。Venette 認為“危機是舊體制無法再維持的轉型過程”。因此，第四個定義品質的因素是變化的需要。如果不需要更改，則可以更準確地將事件描述為失敗或事件。與風險管理不同，風險管理涉及評估潛在的威脅並找到避免這些威脅的最佳方法，而危機管理涉及在威脅發生之前、期間和之後對其進行處理。它是在更廣泛的管理背景下的一門學科，包括識別、評估、理解和處理嚴重情況所需的技能和技巧，特別是從第一次發生到恢復程式開始的那一刻。(整理自維基百科 Wikipedia)

UCENet 參與者組成的工作小組已經成立，紐西蘭政府內務部數位安全部門主任 Jolene Armadoros 擔任領導機構與負責人。本議程是關於這個工作小組日後發展面向的公開討論。

Charles 提出了三個歷年來具爭議的面向進行討論，第一點涉及言論自由的問題上存在分歧，第二點是強調隱私政策和長期隱私原則之間的關係。第三個是網際網路的本質，這是一個極具挑戰性的邊緣問題。

他認為保護自己的聲譽並不是什麼新鮮事，但隨著社交媒體的興起，在一些科技與通訊技術中，大家都必須經歷聲譽方面的評定，比如各位的信用評分。這基本上就像你信用價值，你的信用價值決定你在社會的價值，可應用在貸款等行為的評定，這是非常系統化的東西，在各個國家，有規定誰可以取得這些資訊並應用。這種制度立意良善，避免一些社會亂象或是糾紛產生。但極端的例子也存在著，我們可以發現，隨著時間的推移，實踐的發展，愈來愈多生活上的事物與信用息息相關。以看到最近的例子而言，中國在社會信用體系的應用便是極佳的佐證案例。

最近的一項調查顯示有近 25%的加拿大人認為網路搜索是一種公共記錄。網路空間通常被稱為數位公共廣場，在這裡，思想是一個市場，思想需要被公開討論，以便發現真相，進行公平和公開的討論，而不需要對思想進行審查。所以，這些與隱私是相互衝突的價值觀。它與長期存在的隱私原則有很強的聯繫，為什麼這些原則如此重要，在前面的信用報告的案例中，留下的支票資訊可能會在你不知道的情況下被用來損害你的利益。80%的加拿大人關心公司如何利用資訊來做決策（包含面試或是投資等等行為）。這些都說明了聲譽的重要性。不僅僅是一個作出決定的問題，也影響人們的就業能力，只用信用評分、聲譽會影響評斷你是否得到抵押貸款或是代表你在社會的價值，其實隱私與信用是脫離不了關係的存在。

另一個問題是，各國的法律對於彼此間定義的界線與衝突，舉例來說，虐待

的定義是什麼，以及程度到什麼境界便構成虐待的要件。這些都取決於各國的文化背景、地理背景與宗教背景，綜合種種不同的因素，每個國家甚至國家內部的許多區域對於虐待的構成要素與定義都是不同的，同樣的道理也套用在「Christchurch Call to Action」協議上，所以這是擺在我們面前的一個真正的挑戰。另外還有一個問題是版權問題。舉個極端的例子是如果你把自己的裸照放到網上。事實上，版權是屬於你的，但是如果你的配偶或是其他人拍了那張照片，然後把它貼在網路上，你會認為那是虐待或令人反感的內容，但在某些法律下，版權實際上是屬於他們的，我們在美國已經看到這種情況發生過好幾次了，你沒有拍視頻或者你沒有拍圖像，那麼你就沒有任何權利。又例如雖然我們不是歐盟的一部分，但 GDPR 在美國確實有著舉足輕重的影響。或許你並不在歐洲生活，但若是你在歐洲做事情，或者收集適用於我的法律資料，我可能會因此蒙受相關的損失。

委員在最後仍然再次強調，M³AAWG 的各位委員都會陸續討論更多關於解決方案的內容，但是仍然需要各位會員的積極參與，這是非常重要的。

五、Caller Identification Authentication and Network Level Call Blocking -OPEN （身分驗證與封鎖網路電話）與 Phone Numbers and the Global Regulation Landscape（電話號碼與全球控管機制之關聯）

本場次議程的主講者有五名，分別為：Huw Saunders、Brent Strothers、Linda Vandeloop、Will Maxson 與 John，旨在為了減少來電顯示欺騙，電信供應商正在開發驗證來電顯示號碼的工具。這個名為 STIR/ Shaken 的協定驗證發出呼叫的人有權使用顯示的呼叫者 ID。在美國，這一自願機制的部署才剛剛開始，預計將在 2019 年底由大型航空公司實施。在加拿大，加拿大廣播電視及通訊委員會（Canadian Radio-television and Telecommunications Commission，CRTC[7]）要求在 2019 年 3 月 31 日前實施，美國聯邦傳播委員會最近也授權 ISP 攔截可疑的垃圾郵件和詐欺電話。特定行業將被要求執行 STIR/Shaken[8]技術並回報相關的執行現狀。UCENet 成員將描述他們國家的法律框架、實施的影響，以及如果 ISP 若執行的順利，阻止詐騙行為，則這些集團成員下一步會去哪裡。STIR/Shaken 是人們期待已久的改變，它改變了電話和 Robocall 的流行，但這協定目前僅在美國實行。在美國以外，有 600 多種不同的規章制度來管理電話號碼的使用。STIR/Shaken 面對的挑戰是如何去理解或與這些規定達到最佳的執行平衡。許多國家已將其電話

[7] 加拿大廣播電視及通訊委員會是專責規管加拿大國內所有廣播及電訊市場的機構。CRTC 的前身是加拿大廣播電視委員會，於 1968 年成立並取代廣播委員會的功能。CRTC 的管轄範圍再於 1976 年擴充至包括電訊公司，並改為現稱。（參考自維基百科 Wikipedia）

[8] STIR/Shaken 是一套協定和程式，旨在打擊公共電話網路上的來電顯示欺騙（Spoofing）。來電顯示欺騙技術被 Robocalls 用來掩蓋他們的身份，或者讓人覺得電話來自一個合法的來源，通常是一個附近的電話號碼，或者來自一些知名機構，比如國稅局(Internal Revenue Service)或安大略省警察局(Ontario Provincial Police)。這種類型的欺騙對於來自 IP 語音(VOIP)系統的呼叫來說很常見，VOIP 可以位於世界上的任何地方（整理自維基百科 Wikipedia）。

系統收歸國有，由政府管控，從而對一些不法集團採取了更嚴格的監管和行動。

STIR/Shaken 被 FCC 定義為一個相互連接的標準框架。它基於公共金鑰加密技術，本質上為保證 IP 電話的真實性提供了基礎。該框架被認為是打擊非法和 Robotcalls 重要的第一步。此機制已於網際網路上使用多年，為安全網站提供身份驗證，最大限度地減少惡意者對網際網路地址的欺騙。最近，政府、服務提供者和企業安全專家都逐漸重視對於非法呼叫的影響以及相關改善的機制。

美國參議院於 2019 年中通過了「電話 Robocall 濫用刑事執法和威懾法（Telephone Robocall Abuse Criminal Enforcement and Deterrence Act，TRACED Act」，這項新立法將提高聯邦通信委員會 FCC 對自動呼叫者徵收的罰款，同時將違規行為的時效延長至 3 年。該法案還將創建一個跨部門工作小組來解決這個問題，其中一項關鍵要求是 ISP 營運商須配合實現呼叫認證技術，而 STIR/Shaken 可能是首選的方法。2018 年，加拿大廣播電視和電信委員會引入了 CRTC 2018-32，要求到 2019 年 3 月，所有加拿大電信服務提供者必須實施網際網路協定(IP)語音呼叫的來電顯示資訊認證和驗證。CRTC 2018-32 將 STIR/shake 作為識別資訊的主要驗證方法。

John 也提到 STIR/Shaken 本身是減少騷擾電話數量的一個重要環節，但這機制本身有許多更強大的應用可以執行。通過添加呼叫處理選項或細節，服務提供者和訂閱者甚至可以配置自己的呼叫處理規則，以強化各組織對於防制 Robocalls 的效益。

六、Taking NOTICE: Identifying Vulnerable IoT Devices in Japan

（驗證日本境內脆弱之物聯網設備）

NOTICE，全稱為 National Operation Towards IoT Clean Environment 是日本對其境內的脆弱物聯網設備進行掃描調查後，並針對有弱密碼或漏洞的設備，通知其用戶的一項計畫，此計畫於 2019 年 2 月開始執行，由日本總務省（Ministry of Internal Affairs and Communications，MIC[9]）、日本國立研究開發法人情報通信研究機構（National Institute of Information and Communications Technology，NICT[10]）與日本境內電信營運商三方進行密切合作。

圖 11 NOTICE 計畫組織關係圖

在這個暢談物聯網與人工智能的時代，所有東西都被連接到網路上。網路安全是一個當今社會大眾都必須關注的議題，針對物聯網設備的網路攻擊近年來呈上升趨勢。物聯網設備具備幾項特點，如功能有限、維護困難與生命週期長，容易成為網路攻擊的目標。事實上，在其他國家也持續有嚴重的災情或損失出現，如先前極為盛行的 Mirai 攻擊事件。

[9] 總務省是日本中央省廳之一，所管業務相當廣泛，包括地方自治監理、行政機關事務統籌、消防、選舉管理、通訊傳播管理、國勢與施政統計等，功能類似其他國家的內政部。（參考自維基百科 Wikipedia）

[10] 國立研究開發法人情報通信研究機構是隸屬於日本總務省的獨立行政法人機構。該機構成立於 2004 年 4 月，目前總部位於日本東京都小金井市，主要進行資訊技術領域的研究和開發，同時對資訊通信提供業務支持。（參考自維基百科 Wikipedia）

本議程的主講者為在 NICT 擔任 Research Manager 的 Dr. Takahiro Kasama，Takahiro Kasama 在其提供的資料中(詳附錄)提到，日本境內 IoT 設備造成的危害近年有增加的趨勢，NICT 將某些特定且未使用的 IP 位址定義為 Darknet，NICT 認為這些沒有在使用的 IP，既然不屬於任何主機或是安裝任何服務，便不應該存在任何的使用流量，亦即不該有任何的封包被傳送過去。若是出現了封包或是使用流量，NICT 認為有如下可能：惡意程式之掃描行為、駭客惡意存取行為或是錯誤的網路設定等等……。因此這些可疑的封包便被 NICT 認為是非常值得參考的惡意行為指標（欄位資訊包含有：時間、設備 ID、來源 IP、傳輸協定、來源 Port、目標 IP 與目標 Port 等資訊），同樣適用於 IoT 行為分析上。

NICT 利用這些 IP 蒐集到相關的資訊並進行分析後，確認有問題的 IP 會主動透過合作組織 JPCERT/CC[11]並通報至相關電信營運商（ISPs）。另外也會由 NICT 定期發布分析報告供相關單位進行參考研究。藉由主動與被動的兩套機制，期望達到最佳效益。

Takahiro Kasama 指出 NICT 近年對於 IoT 掃描作業的技術成長與機制有逐年的進步，2016 僅針對預設的連線帳號密碼進行掃描；2017 新增了常見脆弱的漏洞進行掃描；2018 對於連線 IoT 設備的行動裝置也可以進行掃描偵測。

圖 12 NICT 掃描目標之演進

配合日本的相關法規[12]與技術，NICT 可以執行與達成下述目標：端口掃

[11] JPCERT/CC 是在日本建立的第一個 CSIRT(電腦安全事件回應小組)。該組織與網路服務提供商、安全供應商、政府機構以及行業協會進行協調。(參考自 JPCERT 官網)

[12] 《電信商業法》和《國家資訊和通信技術研究所法》修正案（the amendment of the Telecommunications Business Act and the Act on the National Institute of Information and

描、帶有開放端口的 IP 掃描、利用 Banner 識別行動裝置（搭配 NICT 本身的特徵資料庫）、確認設備與惡意行為是否吻合、限制用戶存取並進行通知，流程可參照下圖。

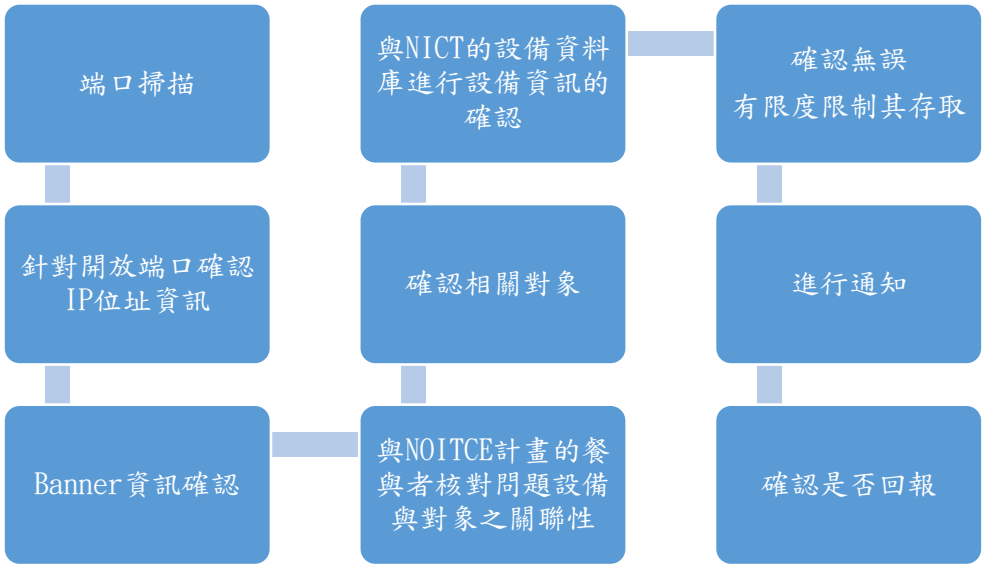

圖 13 NOTICE 運作流程圖

NICT 針對其認為優秀的密碼原則建立了以下規範：不得少於 8 碼、過去的網路攻擊中未被使用、非預設以及 NICT 會定期更新其認為危險的一百組弱密碼。目前 NICT 一次掃描的範圍約落於 34 家 ISP 中的 1 億組 IP。

Takahiro Kasama 最後也指出，雖然 NICT 致力於 NOTICE 的推廣，也得到了一定的成效，但執行近一年的現今，仍然面臨著許多挑戰，他認為目前的通知機制效果有限，必須有更積極的方式去進行用戶的通報。目前通知用戶的方式僅限於電子郵件，但從過往的數據中可以發現，用戶閱讀此類電子郵件的比例低於 40%，而這 40%更是極少數會主動與客服中心聯繫進行下一步的處置，NICT 正在研擬是否可以採用更具效益的方式如明信片或電話通知已取得更顯著的回報，也不排除搭配使用一些獎勵的機制，鼓勵使用者對於此類的防制作業能有更進一步的協助。

Communications Technology）。

七、Robocall and Do Not Call Enforcement - OPEN （電話行銷與相關之強制規範）

本次會議講者有 Ian Barlow、Adam Stevens、Anneqa Khan、與 Evert Jan Hummelen，主講者為為 FTC 的 Ian Barlow 與 Anneqa Khan。主要在探討 Robocall[13]、Do not call[14]、Telemarking[15]與 Spoofing 的議題，針對上述議題監管和執法機構已加強執法行動，將責任人繩之以法。

一開始便由來自澳洲通訊媒體局（Australian Communications and Media Authority，ACMA）的 Anneqa Khan 針對澳洲現在國內太陽能板產業所衍生的 Telemarketing 議題進行探討。由下圖可以窺見，澳洲內部電話銷售投訴的情形在 2015 至 2017 年間增長，又於 2017-2020 期間呈現下降的趨勢。

[13] 一種通過電話來達到宣傳目標的形式，通過電腦控制實施自動撥號，播放預先錄製好的音訊。這種方式大大提高了傳統電話宣傳效率，通常用於電話銷售，總統選舉等。(參考自維基百科 Wikipedia)

[14] 美國謝絕來電計劃（英語：National Do Not Call Registry）旨在讓美國消費者少收到錄音電話促銷。消費者可撥打 1-888-382-1222 註冊該計劃。謝絕來電計劃從 2003 年開始設立，但因有異議延誤至 2004 年實行。(參考自維基百科 Wikipedia)

[15] 電話銷售是一種直銷模式，一般是銷售人員通過電話向潛在的客戶推銷商品和服務。電話銷售有時候也使用電話自動撥號，然後錄音播放錄音的方式。電話銷售的消極方面是經常和各種詭計和詐騙聯繫在一起，比如層壓式推銷、價格不合理的劣質貨品或假貨，亦有電話行銷者經常致電目標顧客，令對方感到滋擾。(參考自維基百科 Wikipedia)

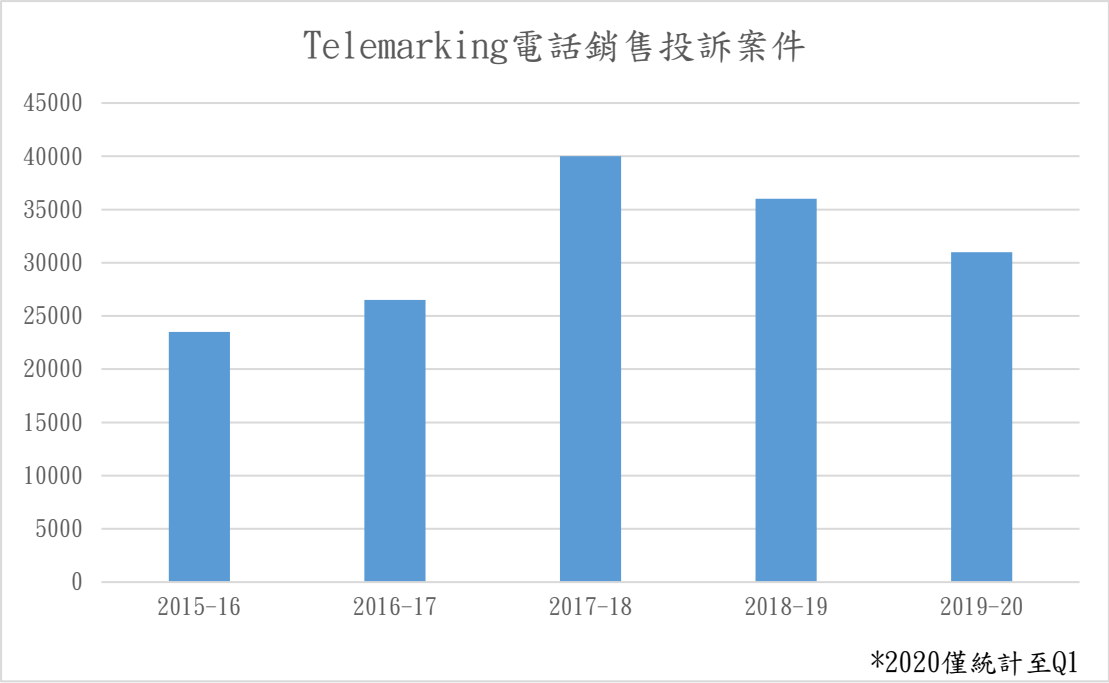

圖 14 澳洲 Telemarking 電話銷售投訴案件

Anneqa Khan 認為這種下降的趨勢跟以下澳洲的執法現況有關，像是近幾年執法動作有逐年加強的趨勢，如：有爭議或是調查中的案件，至少 18 個月內不得調用或調整其註冊碼；針對持續違反規定或侵權的對象，更積極地進行通知；亦利用法律強制力，確認廠商或企業已投入足夠的心力與具備足夠的專業知識。針對那些被廣為投訴的或是領頭的業者優先執行這些政策。Anneqa Khan 認為這些太陽能產業的 Telemarketing 有以下特色：不明確的規定將導致服務的濫用與騷擾用戶的情形氾濫；服務大多外包至國外，相對不容易受國內相關的法規或是統一。Anneqa Khan 亦提出其國內解決的方式，如明確的提出相關規範並遵守執行；不明確的規定則透過教育訓練的方式進行相關訓練，並定期稽核相關單位是否符合標準，強調違法的相關後果。對於外包的部分，可針對發包的公司進行查驗與稽核，且根據澳洲相關法律，對於外包的電話行銷公司，其相關責任與義務須由簽訂合約的發包公司承擔。

Anneqa Khan 指出，目前這些策略的執行雖然效果尚不顯著但也已經有初步的成效，在過去的 18 個月間電話投訴的案件已有顯著的減少，並提到這些策略日後亦可能在能源產業、電信產業與金融產業執行。

八、(LE Only) Unlawful Messaging and Consumer Protection: The Intersection of Enforcement and Regulatory Regimes - CLOSED（非法訊息與消費者的保護：強制力與監控機制的交叉應用）

本次會議主講者為英國資訊專員辦公室(Information Commissioner’s Office)負責情報部門的 Adam Stevens 等人。委員們提到，使用者未注意或不在乎的一些資訊分享，都可能造成其他使用者的危害，但其實有一些具有強制力的機構可打擊不符合規範的行為，我們該如何利用這些機構來防堵資訊漏洞？

Adam 舉例，以往我們發送電子賀卡給親朋好友，但在發送電子賀卡的同時，也洩漏了對方的電子郵件等相關資訊，我們在不知不覺中造成了他人的困擾而不自知，同樣的道理，由於通訊軟體的盛行，多數使用者對於資料蒐集的模式更是習以為常。Adam 提及，除了訊息洩漏，甚至有不法集團利用這些資訊從事非法行為，例如電話行銷雖然是定義模糊的騷擾，但有時推銷的產品也有不實的廣告效果，將衍生出後續問題，例如消費衍生的法律糾紛也極為常見。

Adam 又舉美國某個小農村為例，其人口不到五千人，卻被對外宣稱有十萬以上的人口數，因此，當地某些企業便被許多推廣業務的業者打了數百、甚至數千通，為期三周的騷擾電話，慶幸的是 Adam 雖然阻止了這件事引起的風暴，但因為農村並沒有資安犯罪的知識與能量，所以能蒐集到的資訊非常有限。

最後 Adam 提及，以上的犯罪行為乃 FCC 等組織或委員致力改善的目標，對他們來說，打擊犯罪無法靠一己之力，必須藉由每年辦理的大會，積極與各會員國達成共識，即便在沒有召開大會的情形下，也有足夠默契互相合作。

肆、臺日雙邊會談（Bilateral meeting between NCC/TTC and JADAC）

1. 日期：2019/10/16

2. 地點：Av.Laurier, Hotel Fairmont Queen Elizabeth, Montreal, Canada

3. 日方代表：

隸屬日本數據通信協會（Japan Data Communications Association，下稱 JADAC）反垃圾電子郵件諮詢中心（Anti-Spam Consultation Center）的 Deputy Director-谷原秀彥（Hidehiko TANIHARA）。

4. 臺灣代表：

中華民國國家通訊傳播委員會（National Communications Commission，下稱 NCC）的吳簡任技正銘仁與周技正金賢。財團法人電信技術中心（Telecom Technology Center，下稱 TTC）的林副主任高裕與呂副工程師敏漢。

5. 會議目的：臺灣與日本近年的垃圾郵件交換議題上合作關係日益密切，不論是在 Honeypot 技術或是情資的交流都有很大的突破與發展，是故我方與日方也期望藉由每年度的 M³AAWG 場合，進行一次面對面的雙邊面談。本次會晤結束後，由本會基礎處吳簡任技正銘仁致贈日方代表紀念品，以表示友好關係。

圖 15 臺日雙邊會談與談人員

由左至右依序為吳銘仁(NCC)、林高裕(TTC)、周金賢(NCC)、谷原秀彥(JADAC)

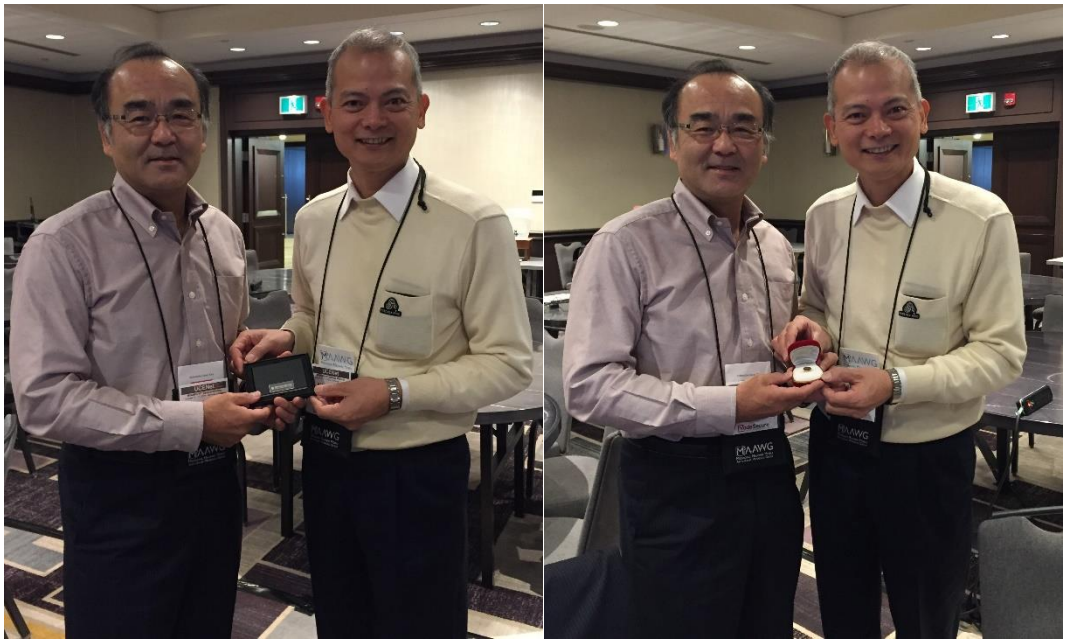

圖 16 吳簡任技正銘仁致贈日方代表紀念品

6. 會議內容：本次的臺日雙邊會談主要探討的議題有四，以下列出日方所提議題以及我端回覆：

6.1 NCC/TTC 提供垃圾郵件資料時，資料格式發生與以往不同，JADAC 無法順利解析現有的檔案格式，並請求 NCC/TTC 考慮是否同意使用可以上傳至 JADAC 系統的格式。

我方回覆：工程師團隊針對格式調整的部分將協助配合，若完成新的格式，我端將試行發送新舊格式的檔案，並確認新格式檔可正常執行解析後，將舊的格式檔案進行下架的動作。

6.2 以往 JADAC 收到的垃圾郵件以 HINET 為大宗，最近發現有一家業者為 HSINYEONGANC(新永安有線電視公司)的單位發出大量的垃圾郵件，甚至超過了 HINET，是否屬於異常情形並可以協助調查？

我方回覆：我們已經通知提供新永安有線電視公司網路服務業務之 ISP 業者 NCIC (新世紀資通公司)這些資訊，並與其保持聯繫，將持續追蹤相關資訊與確認問題是否有被解決。(後經洽詢新世紀資通公司，該公司回復已處理完成，後續也未再收到日方提出此問題，本會將持續與日方維持合作關係，確保類似問題不再發生)

6.3 與巴西的垃圾郵件交流，2018 年 8 月，巴西至日本的垃圾郵件數量激增(約為 2018 年 6 月與 7 月的 10 倍)，JADAC 想知道從巴西到臺灣的垃圾郵件是否也有增加的趨勢？

我方回覆：以我端蒐集到的資訊作確認，巴西來的垃圾郵件並未有增加的趨勢，但我們仍可以提供您端巴西 Cert 的聯絡視窗，以利您端與其進行進一步的確認。

表 4 巴西垃圾郵件交流數量統計

Month	The number of spam
2018/6	1
2018/7	1

2018/8	1
2018/9	44,014
2018/10	525,098
2018/11	316,212
2018/12	42,617
2019/1	142,724
2019/2	447,630
2019/3	184,543
2019/4	1
2019/5	8,924
2019/6	0
2019/7	0
2019/8	0

6.4 臺灣對於資訊安全相關法案的目前進度或現況如何？

我方回覆：因法案的推動與審議需經過較為嚴謹且繁複的流程，像是一讀、二讀與三讀等過程，中間也有可能被退回重審與協商討論。目前我國的數位通訊傳播法（草案）立法進度為立法院仍在審議中。

伍、心得及建議

一、 會議心得

垃圾訊息（SPAM）氾濫成災的情況在近二十年極為嚴重，如何有效阻擋垃圾郵件一直是各國資安管理的首要目標。目前垃圾訊息已從單純的資料蒐集與洩漏(如電子賀卡的濫發)，進化為造成人民驚慌的恐怖暴力訊息，急需各國主管機關擬定「反垃圾郵件法令」以遏止錯誤訊息擴散。目前許多國際組織與相關單位已發現濫發垃圾訊息所造成的危害，主動促成許多跨國單位合作，積極參與類似 M³AAWG 的國際會議，並藉由柔性的教育訓練與勸導，或是具強制力的法律規範，共同防堵垃圾訊息。

訊息濫發在國際上已是急需被重視的議題，政府單位針對制定法律規範與強制執行（如此次 UCENet/M³AAWG Abusive Material Takedown Best Practices 議程提及的基督城行動呼籲條款）；學術界針對相關技術（如此次 Caller Identification Authentication and Network Level Call Blocking 提及的 STIR/Shaken 技術）進行相關研究並瞭解訊息濫用之相關趨勢（如 KISA 所分享的國內外垃圾郵件影響趨勢）；民間單位或企業配合資安防護工作，不再侷限於特定組織或單位，共同打擊濫發訊息，並針對防制、法規與技術情報進行交流，藉由與國際各組織互動合作，才能降低濫發訊息所造成的危害。

藉由參與 M³AAWG 此類的國際大型會議進行跨國交流，如與日本或韓國進行垃圾郵件的資訊與技術交流，可累積我國的技術專業聲望，以獲得國際上對我國執行成效的認可，並獲取新知，法規、技術、管理等經驗，皆是參加本次會議之收穫。以 KISA 推動韓國內部防制垃圾郵件的手段而言，即使 KISA 本身屬於無強制力規範之組織，但藉由與主管機關及檢調單位之合作，亦強化了本身之強制力，搭配其專業能量，如手機系統回報機制與 Spamtap 誘捕系統，與韓國各單位通力合作並相輔相成，獲得極為顯著的防制效益。

本次參與 M³AAWG 會議所獲得之新知與內容，將分享予我國相關產業或內部同仁進行交流，以達到 M³AAWG 會議之目的。面對垃圾訊息，政府及產業界需要全面檢討網路及系統安全性，針對漏洞追蹤改善，提升系統管理人員資訊安全管理能力，以及加強一般民眾對資訊安全的認知，唯有採取更積極、主動的資安防護，才能有效抵禦網路犯罪引發的國安危機。

二、 建議事項

近年來有關物聯網設備的網路攻擊事件有上升的趨勢，所以關於物聯網設備的網路安全議題也成了各國關注的另一個焦點，在「Taking NOTICE: Identifying Vulnerable IoT Devices in Japan」的議程主講者 Dr. Takahiro Kasama 說明下，讓我們了解由日本總務省（MIC）、日本國立研究開發法人情報通信研究機構（NICT）及日本境內電信營運商三方進行密切合作的 NOTICE 計畫與成果，此計畫是由 NICT 使用某些特定的 IP 位址蒐集到相關的資訊並進行分析，在確認有問題的 IP 後，會主動透過合作組織 JPCERT/CC 並通報至相關電信營運商（ISPs），另外也會由 NICT 定期發布分析報告供相關單位進行參考研究，藉由主動與被動的兩套機制，期望達到最佳效益。Takahiro Kasama 也說明 NICT 近年對於 IoT 掃描作業的技術進步成果，由 2016 年僅能針對預設的連線帳號密碼進行掃描，發展到 2018 年對於連線 IoT 設備的行動裝置也可以進行掃描偵測。我國目前正積極推動 5G 行動寬頻業務，有關如何做好物聯網設備的資安防護也將會是愈來愈重要的議題，建議可仿效日本 NOTICE 計畫的做法，結合產官學 3 方的力量，針對有問題的 IP 進行分析及通報，協助相關電信營運商（ISPs）做好物聯網設備的資安防護工作，以達到網路安全的目標。

附錄、參考資料

1. Public Speaking Survival 簡報(2019)：Kevin Quinn (Facilitation First, Inc.)。
2. OPEN UCENet Members Meeting 簡報(2019)：Dana-Lynn Wood(加拿大廣播電視與電信委員會)。
3. Current State of SMS and Email Spam in Korea 簡報(2019)：JEESOO JEON（韓國網際網路安全局）。
4. UCENet/M³AAWG Abusive Material Takedown Best Practices 簡報(2019)：Jolene Armadoros (紐西蘭內政部)。
5. Phone Numbers and the Global Regulation Landscape 研討資料(2019)：由 Huw Saunders、Brent Strothers、Linda Vandeloop、Will Maxson 與 John 等 5 人口述，周金賢紀錄。
6. Taking NOTICE: Identifying Vulnerable IoT Devices in Japan 簡報(2019)：Dr. Takahiro Kasama (NICT)。
7. Robocall and Do Not Call Enforcement 簡報(2019)：Anneqa Khan（Australian Communications and Media Authority，ACMA）。
8. Unlawful Messaging and Consumer Protection: The Intersection of Enforcement and Regulatory Regimes 簡報(2019)：Adam Stevens(Information Commissioner’s Office，英國資訊專員辦公室)。