日本網路安全政策發展與限制

古涵詩

摘　要

日本為了強化網路安全防護能力，於 2015 年設置「網路安全戰略本部」及「內閣網路安全中心」，開始重視跨領域及公私部門的網路安全合作。日本積極與各國進行網路威脅情報交流，訂定相關國際規則及展開雙邊、多邊網路安全對話。可見日本除了增加自身在網路空間的話語權外，更積極運用網路安全外交，強化國際合作與連結。本文將探討日本網路安全推進體制、網路安全政策發展與限制，並總結日本網路安全發展之特色與對臺灣之啟示，以作為我國網路安全政策之參考。

關鍵字：網路安全、網路安全戰略、網路安全基本法、網路安全戰略本部、關鍵基礎設施

壹、前言

網際網路爲人類帶來便捷與快速，然而，伴隨著網路全球化所引發的網路犯罪及個人資料保護問題，已逐漸影響一國的國家安全與社會穩定，全球正面臨嚴峻的網路安全威脅！網路安全威脅從個人之網路犯罪演變成由組織，甚至是由國家發起，以經濟或政治爲目的之入侵行爲。近年來，網路犯罪組織趨於高度專業化分工，加上網路攻擊的三種特性：多樣性、匿名性、隱密性，已造成國家安全之概念及範圍產生實質變化[1]。日本作爲網路及資訊科技領先的國家，在享受網路帶來便利的同時，卻也面臨著各式各樣的網路安全問題，例如：日本情報通信研究機構（National Institute of Information and Communications Technology, NICT） 於 2015 年 2 月 17 日發表的統計資料顯示，2014 年一整年日本遭到約 256.6 億次境外網路攻擊，其中有四成 IP 位址在中國大陸，比起 2013 年約 128.8 億次網路攻擊次數，整整增加一倍，顯示日本網路攻擊情況越來越激烈[2]。在此之前，開發網路攻擊防禦產品的 FireEye 公司，該公司董事長達夫 · 德瓦爾特（Dave DeWalt）表示：「網路戰爭已經開始，擁有豐富智慧財產權的日本，在敵人眼中是重要的網路攻擊對象。在捲入網路戰爭的國家中，日本是特別危險的。」根據該公司的調查報告，惡意軟體的回呼（Callback）[3] 通信對象，日本高達 87%，遠遠高於不到 47% 的美國[4]。

日本常見的網路威脅有：

一、個人資料被盜與金融詐騙事件。駭客透過電子郵件或利用網站應用程式漏洞、網頁掛木馬等方式，在受害電腦植入惡意程式，目的是爲了竊取個人隱私與犯罪集團合作進行金融詐騙；

二、關鍵基礎設施（Critical Infrastructure, CI）遭到破壞，進而影響經濟、民生及整個政府運作，如：2011 年 3 月 11 日日本東北地方大地震，日本在關鍵基礎設施之核能、電力、糧食、飲

《註 1》行政院國家資通安全會報，〈國家資通安全發展方案 102 年至 105 年〉，《行政院國家資通安全會報》，2013 年 12 月，頁 2-7，http://www.nicst.ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=918F43FED41196D2，最後瀏覽日期：2021 年 2 月 24 日。

《註 2》井上英明，〈2015 年のサイバー攻撃関連通信は 2 倍に急増、IoT 機器からが 2 割占める〉，2016 年 3 月 8 日，《ITPRO》，http://itpro.nikkeibp.co.jp/atcl/column/14/346926/030700469/，最後瀏覽日期：2021 年 2 月 24 日。

《註 3》一種安全性功能，能讓主機在成功連線後與遠端呼叫者切斷連線，然後再回呼遠端電腦，以起到安全性驗證或承擔經濟責任的作用。

《註 4》日川佳三，〈爲什麼駭客特別愛攻擊日本〉，《商周 .COM》，2013 年 6 月 25 日，http://www.businessweekly.com.tw/article.aspx?id=3945&type=Blog&p=0，最後瀏覽日期：2021 年 2 月 24 日。

水設施防護及政府危機處理能力等方面，都受到嚴厲的考驗與挑戰[5]；

三、進階持續性威脅（Advanced Persistent Threat, APT）[6]增加，由於APT的攻擊特徵爲針對特定目標、低調、隱匿、手法多元、客製化等，日本、臺灣及美國是遭受APT攻擊最爲嚴重的國家[7]。日本發生網路攻擊事件層出不窮，而且呈現擴大化與多樣化的趨勢。受到網路攻擊的目標不僅是政府、軍事單位，也擴大到國會、企業、教育及科技等相關部門；攻擊形式更爲多樣化，如：日本最大國防承包商三菱重工（Mitsubishi Heavy Industries, MHI）的工廠伺服器與電腦遭駭客植入惡意程式，國防承包商已成爲駭客的主要攻擊目標之一[8]。再者，英美兩國譴責俄羅斯軍事單位針對日本東京奧運發動一連串的網路攻擊，包括鎖定奧運主辦單位、物流供應商及贊助商等[9]。綜上所述，日本面臨的網路安全問題是複雜且嚴峻的，網路安全防護已成爲日本國家安全和社會穩定的重要課題。

本研究探討日本網路安全之發展與限制，爲了強化國家整體的網路安全防護能量，日本負責網路安全的有關機關做了哪些調整？不同時期的網路安全政策發展如何轉變？過程中面臨哪些挑戰與限制？研究結果可使讀者對日本網路安全有一個總體認識，歸納總結日本網路安全發展的特點，以期對我國的網路安全防護提供啓示和借鑑。

貳、日本網路安全政策發展趨勢

日本政府於2013年6月發布《網路

《註5》防災科技研究中心，〈關鍵基礎設施安全防護〉，《防災科技研究中心》，2012年2月15日，http://dptrc.sinotech.org.tw/chinese/03_news/022_detail.php?pid=7，最後瀏覽日期：2021年2月24日。

《註6》是一種讓未授權人員獲得網路存取權限，並保持長期不受偵知狀態的精密網路攻擊方式。進階持續性威脅的企圖是要竊取資料而非造成損害。進階持續性威脅包含以下步驟：階段一：透過滲透系統開始入侵；階段二：將惡意軟體安裝於遭滲透的系統；階段三：建立對外連結；階段四：橫向展開攻擊；階段五：透過隧道協議和加密等方式竊取資料；階段六：攻擊者會隱匿存取記錄，以免遭偵知。Steve Piper, *Definitive Guide to Next-Generation Threat Protection: Winning the War Against the New Breed of Cyber Attacks*. Annapolis, MD: CyberEdge Group, LLC., 2013, pp.5-9.

《註7》林威邑，〈企業何時會被駭客攻陷 回朔式掃描與預警機制的重要性〉，《麟銳科技》，2016年，http://www.ringline.com.tw/zh-tw/article_info.php?id=78，最後瀏覽日期：2021年2月24日。

《註8》陳曉莉，〈日本最大國防承包商三菱重工證實遭駭〉，《iThome》，2011年9月20日，http://www.ithome.com.tw/node/69808，最後瀏覽日期：2021年2月24日。

《註9》〈「民主主義揺るがす」東京五輪団体へのサイバー攻撃——加藤官房長官〉，《JIJI.COM》，2020年10月20日，https://www.jiji.com/jc/article?k=2020102000515&g=pol，最後瀏覽日期：2021年2月24日。

安全戰略》，從國家層次對網路安全進行架構設計和指導。該戰略提出日本要建構成「世界領先，強大而充滿活力的網路空間」，並實現「網路安全立國」的目標。戰略內容分爲四個部分，網路安全環境變化、基本方針、實施領域、推進體制與評價機制。首先指出，網路空間與實體空間不斷融合，網路空間存在的風險越來越大。其次探討日本網路安全防護機制，指出日本當前的體制已經不足以應付網路安全的環境變化。接著提到日本在今後對網路安全問題的基本思考，爲了確保資訊自由流通，將針對不斷增加的網路風險採取新型態應對措施、強化對網路安全風險資料庫的運用、促進產官學間的互動。第三部分爲構築強韌、有活力及領先世界的網路空間等三個層面，詳細指出今後確保網路安全的具體措施、網路空間防範對策及研發相關技術、人才培育與國際合作等。第四部分就推進體制與評價機制的改革做了詳細討論，包括在 2015 年度將「內閣官房資訊安全中心」（National Information Security Center, NISC）改組爲「內閣網路安全中心」（National Center of Incident Readiness and Strategy for Cybersecurity, NISC）及每年公布年度計畫等內容。

2014 年 6 月日本公布實施《網路安全基本法》，其目的爲擬訂全國性的網路安全對策，明確中央與地方政府的職責。「網路安全戰略本部」（Cybersecurity Strategic HQs, CSSHQ）除了協調各政府單位的網路安全對策外，並搭配《IT 基本法》，全面推動網路安全措施，提高日本經濟社會的活力及可持續發展，爲國民創造安全、安心生活的社會 [10]。《網路安全基本法》從法律層面確定了《網路安全戰略》施行的行政主體、架構內容及基本措施。在行政主體方面，主要確立「網路安全戰略本部」爲負責網路安全的專責機關，須與「國家安全保障會議」、「IT 戰略本部」有關機關合作。該法規定關鍵基礎設施營運商、民間企業和行政機關有義務提供網路資訊；在戰略規劃方面，主要確定《網路安全戰略》架構與內容。

2016 年 2 月日本參議院對於僅實施一年多的《網路安全基本法》提案進行修正，向國會提交《網路安全基本法及促進情報資訊處理法之修正法案》[11]，除了設立「資訊處理安全確保支援士」外，更擴大了「內閣網路安全中心」對政府機關、行政法人

《註 10》電子政府の総合窓口，〈サイバーセキュリティ基本法〉，《e-Gov》，2016 年 10 月 21 日，https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104，最後瀏覽日期：2021 年 2 月 24 日。

《註 11》內閣サイバーセキュリティセンター，〈サイバーセキュリティ政策に係る年次報告（2016 年度）〉，2017 年 7 月 13 日，頁 2-5，https://www.nisc.go.jp/conference/cs/dai14/pdf/14shiryou01.pdf，最後瀏覽日期：2021 年 2 月 24 日。

及特殊法人的網路安全監視。由於 2015 年 5 月日本發生年金機構遭駭客入侵，造成 125 萬筆之個人資料外洩[12]，此事件促使《網路安全基本法》修法，將中央省廳、行政法人的網路系統納入監視範圍[13]。《網路安全基本法》公布以前，各省廳採取自律方式對內部的網路系統進行監測，自《網路安全基本法》實施後，乃是強制各省廳要向「網路安全戰略本部」主動回報網路安全問題，而「網路安全戰略本部」也會向各省廳機關發出正式的網路安全建議。

2015 年 9 月 4 日日本公布 2015 年版《網路安全戰略》[14]，內容分別爲制定宗旨、網路空間相關認知、目的、基本原則、爲了達成目的的手段、推進體制、今後的應對等七個部分。主要延續 2013 年版《網路安全戰略》內容，亦針對 2015 年 5 月日本發生年金機構遭駭客入侵，造成資訊洩露等重大網路安全事件進行檢討。該戰略目的爲，說明日本政府有責任發展自由且公平的網路空間，提供人民安全與安心的生活，亦即保障 Safe 和 Security 兩種安全情境，並確保國際社會和平與穩定，提高社會經濟活力與可持續發展。該戰略有五大基本原則：

一、確保資訊自由流通，保護隱私及智慧財產權；

二、制定法律：網路空間需要完整適切的法令規章，一如實體空間一般，並參考國際規範制定；

三、開放性：開放帶來參與、分享與創新，任何使用網路的個人都不應該被阻擋；

四、自律性：自主管理爲網路空間管理之核心，須落實在各種資訊系統中；

五、協同合作：與關鍵資訊基礎設施（Critical Information Infrastructures, CII）之利害關係人共同協作，政府扮演協調與資訊分享角色。

《註 12》サイバーセキュリティ.com 編集事務局，〈日本年金機構情報漏洩事件のすべて〉，《サイバーセキュリティ.com》，2016 年 6 月 10 日，https://cybersecurity-jp.com/security-incident-case/9146，最後瀏覽日期：2021 年 2 月 24 日。

《註 13》日本《網路安全基本法》第 13 條提到之指定法人單位，包括以下 9 個法人單位，分別是：地方公共團體資訊系統機構（地方公共団體情報システム機構）、地方公務員共濟組合連合會、地方職員共濟組合、都職員共濟組合、全國市町村職員共濟組合連合會、國家公務員共濟組合連合會、日本私立學校振興・共濟事業團、公立學校共濟組合、日本年金機構，請參閱サイバーセキュリティ戦略本部，〈サイバーセキュリティ基本法第 13 條の規定に基づきサイバーセキュリティ戦略本部が指定する法人〉，《サイバーセキュリティ戦略本部》，2016 年 10 月 21 日，https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou01.pdf，最後瀏覽日期：2021 年 2 月 24 日。

《註 14》情報セキュリティ政策会議，〈サイバーセキュリティ戦略〉，《内閣サイバーセキュリティ センター》，2015 年 9 月 4 日，https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf，最後瀏覽日期：2021 年 2 月 24 日。

日本總務省於 2017 年 10 月 3 日公布《物聯網安全綜合對策》，政策項目有：防止物聯網設備之安全缺陷、推動研發、促進民間企業對網路安全進行投資、人才培育之強化及加強國際合作。以下簡述如下：

一、防止物聯網設備之安全缺陷：物聯網設備在設計、製造、銷售、安裝、運送和維護等流程都需要採取相關安全措施，從製造階段就要考量產品的安全性，並給予安全認證標誌，進而鼓勵消費者使用安全的物聯網設備，並定期進行認證檢查；

二、推動研發：日本政府鼓勵針對網路安全進行基礎研究，如：「情報通信研究機構」開發安全驗證平台、密碼技術，模擬、監測政府及企業受到網路攻擊的情形，並且開發「STARDUST」技術來掌握網路攻擊行爲[15]，此技術可進一步監測持續性威脅攻擊活動；

三、促進民間企業對網路安全進行投資：總務省及經產省合作，希望對中小企業採取租稅優惠，促進民間企業對於網路安全進行投資；

四、人才培育：爲因應 2020 年東京奧運會可能發生的網路攻擊，2018 年 2 月「情報通信研究機構」開始模擬在奧運會官網、賽事運作系統的網路環境下，進行網路攻擊・防禦演習「Cyber Colosseo」[16]，其目的在於培育能應對高度網路攻擊的網路安全人才；

五、加強國際合作：爲了創造安全的網路空間，並發展網路安全生態系，有必要強化網路安全的國際連結與合作。2016 年 5 月在日本伊勢志摩的七大工業國集團（G7）高峰會上，表示要共同致力於加強網路安全合作。於 2016 年 10 月七大工業國共同訂定《網路安全指導方針》（G7 Fundamental Elements for Cyber Security）[17]。日本積極與德國共同訂定類似國際標準化

《註 15》國立研究開発法人情報通信研究機構，〈サイバー攻撃誘引基盤 “STARDUST”（スターダスト）を開発〉，《國立研究開発法人情報通信研究機構》，2017 年 5 月 31 日，https://www.nict.go.jp/press/2017/05/31-1.html；臺北駐日本經濟文化代表處科技組，〈日本情報通信研究機構開發解析網路「標的型攻擊」之法〉，臺北駐日本經濟文化代表處科技組，2017 年 9 月 22 日，https://www.most.gov.tw/japan/ch/detail?article_uid=7b55a278-b4f4-44cc-90b4-b3725dd68287&menu_id=a0a402e3-4dd6-4411-a21b-9ecdf4f5af66&content_type=P&view_mode=gridView，最後瀏覽日期：2021 年 2 月 24 日。

《註 16》國立研究開発法人情報通信研究機構，〈Cyber Colosseo〉，《NICT》，https://colosseo.nict.go.jp/，最後瀏覽日期：2021 年 2 月 24 日。

《註 17》HM Treasury, “G7 fundamental elements for cyber security,” GOV.UK, October 11, 2016, pp.1-3, https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security.，最後瀏覽日期：2021 年 2 月 24 日。

組織（ISO）的物聯網國際標準[18]，希望日本的相關技術能更容易被採納，以開創更大的商機。

2018 年 7 月 27 日發布 2018 年版《網路安全戰略》，主要是延續 2015 年版，整體而言，2018 年版提出要達成戰略目標的相關措施要更具操作性，從事後的應變轉爲先發制人、從被動的網路安全防護轉變爲積極主動預測、從網路空間朝向融合空間來發展。日本爲了解決網路攻擊者及攻擊手法，將加強蒐集網路攻擊資訊，並與國際合作，進行國家間的網路威脅資訊共享[19]。爲了確保關鍵基礎設施和其他社會系統運作，擬透過自衛隊保護重要關鍵資訊基礎設施，並提高網路防衛隊的網路攻擊能力。在提高威懾能力方面，密切與同盟國家合作，利用政治、經濟、技術、法律和外交手段，對破壞國家安全的網路威脅實施響應。一面加強政府部會間的協調，增強執法機關和自衛隊網路防護能力，另一面，與各國建立網路安全信任措施，避免不必要的衝突和誤會。在加強網路態勢感知能力方面，政府機關提高資訊蒐集與分析的能力，包括開發和保護技術人才，促進政府內部與同盟國家建立網路威脅資訊共享，有效掌握網路空間態勢。爲強化網路攻擊防禦對策，日本於 2019 年 4 月 1 日成立「網路安全協議會」。協議會爲因應網路攻擊、官民共用資訊的新組織，由關鍵基礎設施事業體、政府機關、資安產業及大學和教育單位組成。當會員受到網路攻擊時，「內閣網路安全中心」會進行分析，再將結果通知會員企業，以防止受害範圍持續擴大。由於網路攻擊常以關聯企業或以特定單位爲攻擊對象，即時的資訊共用與通報將對防止受害範圍擴大十分重要，爲使企業願意坦承且主動向「內閣網路安全中心」通報，「網路安全協議會」規定所有成員必須履行保密義務，即使公布受害情況時也能不具名企業名稱。

參、日本網路安全推進體制

以下介紹日本政府與網路安全之機關單位及受其管轄之組織，其中「內閣網路安全中心」爲其相關組織運作之總部（Headquarter）。2015 年 1 月 9 日日本政府根據《網路安全基本法》，將「資訊安全政策會議」及「內閣官房資訊安全中心」分別升格爲「網路安全戰略本部」與「內閣

《註 18》八時島綾平，〈日本在國際標準制定上追趕德國，中韓在後〉，《日經中文網》，2017 年 3 月 30，https://zh.cn.nikkei.com/politicsaeconomy/economic-policy/24424-2017-03-30-04-52-14.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 19》情報セキュリティ政策会議，〈サイバーセキュリティ戦略〉，《内閣サイバーセキュリティ センター》，2018 年 7 月 27 日，https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf，最後瀏覽日期：2021 年 2 月 24 日。

表 1　日本《網路安全戰略》之內容比較

版本	2013 《網路安全戰略》	2015 《網路安全戰略》	2018 《網路安全戰略》
目的	一、提升經濟社會活力與永續發展 二、實現國民安全且安心生活之社會 三、維持國際社會和平、安定及保障日本安全		
重點對策	一、網路安全環境變化：網路與實體空間不斷融合，並朝一體化的方向發展，當前體制已經不足應付。 二、基本方針：爲確保資訊自由流通、將針對網路風險採取新型態應對措施、強化對風險資料庫的運用、促進產官學民間的互動。 三、實施領域：研發相關技術、人才培育與國際合作。 四、推進體制與評價機制。	一、提升經濟社會活力與永續發展 1. 創建安全的物聯網系統。 2. 加強企業的網路安全意識。 3. 提高企業之網路安全環境整備。 二、提供人民安全與安心的生活 1. 提供保護國民與社會之措施。 2. 關鍵基礎設施防護。 3. 政府機關之安全防護。 三、確保國際社會和平與穩定 1. 確保國家安全。 2. 維護和平與穩定之國際社會。 3. 加強與周邊國家和全球之合作。	一、提升經濟社會活力與永續發展 1. 推動可以支援創造新價值之網路安全措施。 2. 實現可以創造價值之網路安全供應鏈。 3. 架構安全物聯網（IoT）系統。 二、實現國民安全且安心生活之社會 1. 訂定網路犯罪之因應對策。 2. 官民一體共同防護關鍵基礎設施。 3. 強化與充實政府機關之網路安全。 4. 確保大學能建構安全與安心之教育與研究環境。 5. 強化 2021 年東京奧運與未來之措施。 6. 強化情資共享與合作體制。 7. 強化應變大規模網路攻擊事態之能力。 三、維持國際社會和平、安定及保障日本安全 1. 堅持自由、公平且安全之網路空間。 2. 建立支配網路空間之法律秩序。 3. 強化日本網路防禦力、抑制網路攻擊能力與掌握狀況之能力。 4. 強化掌握網路空間狀況之能力。 5. 國際合作。

資料來源：作者自行整理。

網路安全中心」[20]。網路安全戰略本部部長由官房長官擔任，副部長由網路安全戰略本部有關事務擔當國務大臣擔任，成員包括國家公安委員會委員長、總務大臣、外務大臣、經濟產業大臣、防衛大臣、情報通信技術政策擔當大臣、東京奧運會擔當大臣及數名專家學者等[21]；內閣網路安全中心主任由「國家安全保障局」（National Security Secretariat, NSS）次長擔任，下轄兩位副主任、首席網路安全分析官及網路安全補佐官，成員來自於外務省、總務省、防衛省、經產省、警察廳等各省廳派駐人員及 IT 企業成員[22]。

日本網路安全相關單位的組織調整，其意義在於：

一、獲得法律授權：網路安全戰略本部可以根據《網路安全基本法》，具有法律授權；

二、職能擴大：網路安全戰略本部的任務爲（一）訂定《網路安全戰略》並推動實施;（二）訂定網路安全標準;（三）對網路安全重大事件進行調查；

三、權限提升：根據《網路安全基本法》第 30 條規定，當網路安全戰略本部做出決定後，行政機關負責人「必須」即時提供網路安全資訊及情報，協助行使職能；

四、行政級別提升：根據《網路安全基本法》第 34 條規定，網路安全戰略本部的主管大臣是日本首相；

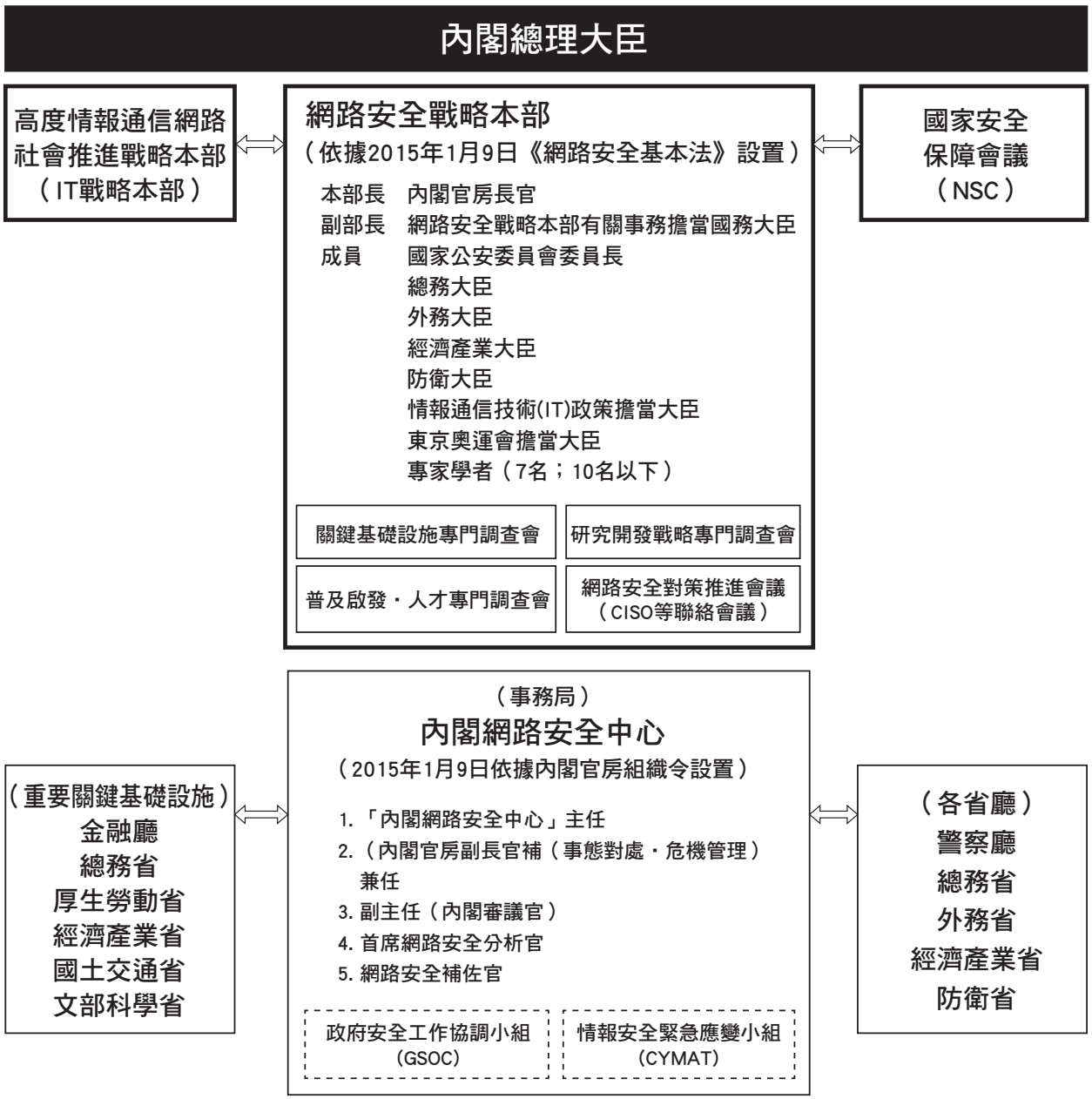
五、增加發布行政命令的職能：《網路安全基本法》第 35 條規定，網路安全戰略本部發布的行政命令稱爲「網路安全本部令」。而內閣網路安全中心除了承擔內閣官房的日常計畫、綜合協調事務外，還負責網路安全戰略本部的行政事務，特別是對各省廳進行網路安全監管和調查。下頁圖 1 爲日本網路安全推進體制。

日本各省廳亦不遺餘力加強網路安全措施，總務省（Ministry of Internal Affairs and Communications, MIC）主要負責訂定有關通信與網路安全政策。從 2001 年起每年公布《資訊通信白皮書》，內容載明資

《註 20》内閣サイバーセキュリティセンター，〈内閣サイバーセキュリティセンター（NISC）設置までの経緯〉，《内閣サイバーセキュリティセンター》，2015 年 1 月，https://www.nisc.go.jp/about/details.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 21》サイバーセキュリティ戦略本部，〈サイバーセキュリティ戦略本部名簿〉，《内閣サイバーセキュリティセンター》，2016 年 4 月 1 日，https://www.nisc.go.jp/conference/cs/pdf/meibo.pdf，最後瀏覽日期：2021 年 2 月 24 日。

《註 22》内閣サイバーセキュリティセンター，〈内閣サイバーセキュリティセンター（NISC）の組織体制〉，《内閣サイバーセキュリティセンター》，2015 年 1 月，https://www.nisc.go.jp/about/organize.html，最後瀏覽日期：2021 年 2 月 24 日。



資料來源：內閣サイバーセキュリティセンター，〈我が國のサイバーセキュリティ政策の概要〉，《內閣サイバーセキュリティセンタ》，2017 年 1 月 30 日，http://www.soumu.go.jp/main_content/000463592.pdf。

圖 1　日本網路安全推進體制

訊安全威脅近期動向、國民對於資訊安全意識調查、日本對於資訊安全的行動方針等。此外，設有「國民資訊安全網」，定期舉辦主題式的調查研究會[23]，如:互聯網、雲端安全研究會等；經產省（Ministry of Economy, Trade and Industry, METI）主要負責：

一、協助企業建立網路安全管理機制；
二、針對國民進行網路安全教育；
三、執行《電子簽章及認證業務法》規定[24]；
四、評價 IT 產品的安全性；
五、指導應處網路威脅事件，定期舉辦網路攻擊解析協議會、網路安全與經濟產業研究會等。

經產省於 2012 年 3 月設立「控制系統安全中心」（Control System Security Center, CSSC），定期舉辦關鍵基礎設施領域之網路安全演習[25]。

外務省（Ministry of Foreign Affairs of Japan, MOFA）主要負責日本網路安全國際合作。日本將網路安全視爲外交的重要討論議題，其三大支柱爲：

一、訂定網路安全國際規則；
二、提高透明度並與各國建立信心措施；
三、能力構築[26]。

爲了能有效對抗跨國的網路攻擊，日本積極參與不同功能與屬性的網路安全國際組織，如：聯合國政府專家小組（The Group of Governmental Experts, GGE）、網路空間國際會議（The Global Conference on Cyber Space, GCCS）、《歐洲理事會網路犯罪公約》（Budapest Convention）等。日本希望透過參與網路安全國際組織，建立網路安全的國際合作框架。日本亦與各國「電腦安全事件應變小組」（Computer Security Incident Response Team, CSIRT）合作，交換網路犯罪與數位鑑識情報分

《註 23》総務省，〈「国民のための情報セキュリティサイト」のリニューアル〉，《総務省》，2013 年 4 月 5 日，http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000045.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 24》経済産業省，〈電子署名及び認証業務に関する法律電子署名及び認証業務に関する法律〉，《経済産業省》，2000 年 5 月 31 日，http://www.meti.go.jp/policy/netsecurity/docs/esig/H12HO0102.txt，最後瀏覽日期：2021 年 2 月 24 日。

《註 25》経済産業省，〈電力・ガス・ビル・化学分野のサイバーセキュリティ演習を実施します〉，《経済産業省》，2014 年 1 月 17 日，http://www.meti.go.jp/press/2013/01/20140117005/20140117005.html，最後瀏覽日期：2021 年 2 月 24 日；王家宜，〈日本控制系統安全中心〉，《行政院國家資通安全會報技術服務中心》，2015 年 7 月 27 日，https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1377，最後瀏覽日期：2021 年 2 月 24 日。

《註 26》外務省，〈外務省のサイバー分野における取組——日本のサイバー外交〉，《外務省》，2017 年 11 月 1 日，http://www.mofa.go.jp/mofaj/annai/page5_000250.html，最後瀏覽日期：2021 年 2 月 24 日。

享，共同打擊網路犯罪。

警察廳（National Police Agency, NPA）負責偵辦網路犯罪案件。由於網路犯罪日漸猖獗，警察廳於 1998 年 6 月發布《高科技犯罪對策重點推進計畫》，並成立「網路警察」，負責蒐集網路恐怖主義攻擊情報[27]。警察廳除了定期舉辦偵查員的講習訓練外，亦加強與產業界或國外警察機關合作交流，共同對抗網路不法入侵、網路詐欺及非法買賣等網路犯罪行爲[28]。防衛省（Japan Ministry of Defense, MOD）於 2014 年 3 月 26 日成立「網路防衛隊」，初期建置共約 90 人[29]。網路防衛隊直接隸屬防衛大臣，由統合幕僚監部幕僚長指揮，主要負責網路威脅情報蒐集、網路防護、網路安全訓練、調查研究與技術支援等。自衛隊應處網路攻擊的六大支柱爲：

一、提高情報通信系統的安全性，如：導入防火牆及防毒軟體；
二、防護系統整備，建立網路監控系統，分析網路攻擊來源；
三、規則整備；
四、人才培育；
五、促進情報共用，網路防衛隊與內閣網路安全中心及美國等其他國家進行網路威脅通報與合作；
六、最新網路攻擊技術研究，舉行網路安全演習等[30]。

接著介紹日本總務省及經產省轄下有關之網路安全組織（參見下頁圖 2），包括：情報通信研究機構（National Institute of Information and Communications Technology, NICT），爲總務省下轄的行政法人，成立於 2004 年 4 月 1 日，主要業務爲資訊、通信及電波技術的研究開發及放送事業振興等。其中，網路安全研究所主要是針對網路攻擊建構視覺化（visualization）監測系統，對可能的網路攻擊進行監視及攻擊分析，並能將偵測到的網路攻擊行爲即時回報系統管理者，以加強資訊系統的安全性。

日本資通訊科技資訊分享與分析中心

《註 27》警察庁情報通信局，《警察のサイバーセキュリティ施策——における技術的対応》，警察庁情報技術解析課，2015 年 10 月 22 日，https://www.npa.go.jp/cyberpolice/material/pdf/20151022_CSS2015.pdf，最後瀏覽日期：2021 年 2 月 24 日。

《註 28》陳文哲，〈日本警方因應網路恐怖攻擊對策〉，《刑事雙月刊》，第 49 期，2012 年 8 月，頁 58-63；林賢參，〈從社會治安的角度探討反恐應有的措施——以日本反恐對策爲考察對象〉，2008 警學與安全管理研討會，臺北：臺灣警察專科學校，2008 年 6 月 18 日，頁 15-17。

《註 29》防衛省，〈サイバー防衛隊の新編について〉，《防衛省》，2014 年 3 月 25 日，http://www.mod.go.jp/j/press/news/2014/03/25d.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 30》防衛省運用企画局情報通信研究課，〈防衛省のサイバーセキュリティへの取組〉，《防衛省》，2014 年 4 月，https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf，最後瀏覽日期：2021 年 2 月 24 日。

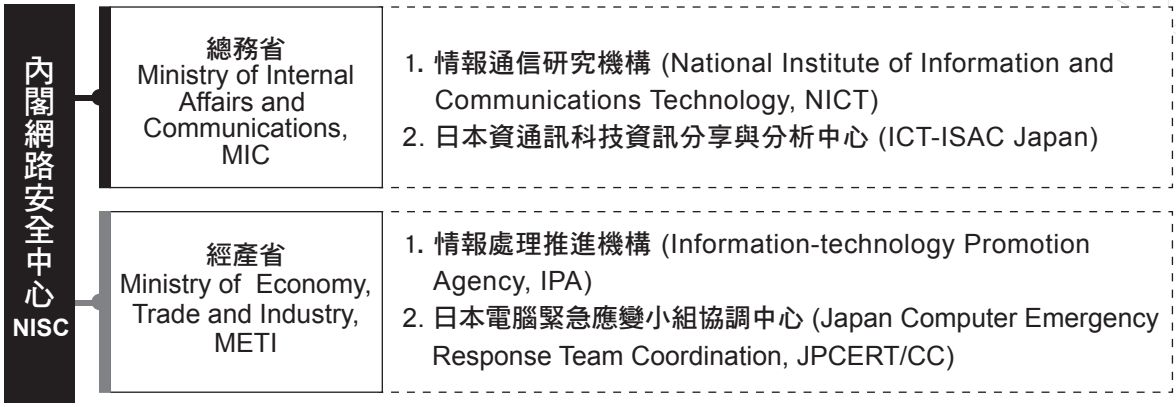


圖 2　日本總務省、經產省轄下之網路安全組織

（ICT-ISAC Japan）成立於 2016 年 3 月 9 日，其前身爲日本電信資訊分享與分析中心（Telecom-ISAC），後來納入資通訊科技（ICT）領域，包括電信、廣播、系統整合、網路安全等廠商，目前共有 40 家企業會員。該中心的主要任務爲，蒐集、調查和分析與網路安全有關資訊、會員之間的資訊共用與合作、訂定網路安全準則、舉辦教育訓練與人才培育等，並且共有網路攻擊對應演習、路由器漏洞問題、Wi-Fi 改進、物聯網安全、資訊共用、人才培育等 10 個工作小組。

「情報處理推進機構」（Information-technology Promotion Agency, IPA）爲經產省下轄的行政法人，推廣 IT 有關的國家戰略，主要任務包括 IT 安全、軟體工程、IT 人才培育及軟體開放等，並受理電腦病毒、不當存取及脆弱性關聯情況等申報，與日本電腦緊急應變小組協調中心合作，定期公開調查情報及緊急對策訊息。另於 2011 年 10 月 25 日成立「日本網路安全資訊分享夥伴協議會」（Initiative for Cyber Security Information Sharing Partnership of Japan, J-CSIP），目的爲加強公私部門的資訊共用與合作，共有 11 個關鍵基礎設施領域之特別小組（Special Interest Group, SIG），如：電力、工業、化學、石油、能源、自動車、物流業、航空、鐵道、金融等產業及 190 個組織參與此情報共有體制[31]。另外，「產業網路安全中心」（Industrial Cyber Security Center of Excellence, ICSCoE）從 2017 年 7 月起開

《註 31》情報処理推進機構技術本部セキュリティセンター，〈サイバー情報共有イニシアティブ（J-CSIP）運用状況〉，《情報処理推進機構》，2017 年 10 月 26 日，https://www.ipa.go.jp/files/000062172.pdf，最後瀏覽日期：2021 年 2 月 24 日。

始培育關鍵基礎設施領域之網路安全人才，除了學習網路攻擊技術外，也進行網路攻防演練。

「日本電腦緊急應變小組協調中心」（Japan Computer Emergency Response Team Coordination, JPCERT/CC）爲一般社團法人，自 1992 年起開始處理網路安全事件，於 1996 年 10 月正式成立。該中心與網際網路服務提供者、網路安全設備供應商、關鍵基礎設施營運商、政府單位及其他產業密切合作，共同協調處理網路安全事件緊急應變 [32]。同時該中心也是亞太地區電腦緊急事件回應小組（Asia Pacific Computer Emergency Response Team, APCERT）、事件回應及安全小組論壇（Forum of Incident Response and Security Team, FIRST）成員，負責協調並整合有關網路安全防護資訊。

肆、日本網路安全發展的限制

日本的網路安全政策雖然取得一定成效，但仍然遭遇到許多限制，包括：一、企業因網路攻擊事件造成巨額損失；二、企業網路安全意識低落；三、資通訊產業對政策缺乏主動性；四、缺乏網路安全人才；五、網路安全預算分散；六、網路安全戰略本部與 IT 戰略本部權限之爭等，茲分述如下：

一、企業因網路攻擊事件造成巨額損失

在亞太地區，網路攻擊所導致的財物損失呈現上升趨勢。其中，日本企業因網路安全漏洞造成的財物損失最爲突出 [33]。2019 年 3 月思科（Cisco）提出的《2019 年首席資訊安全官（CISO）基準研究報告》指出 [34]，網路攻擊導致企業超過 500 萬美元財務損失的亞太地區企業比率高於全球平均水準。此項調查以澳洲、中國大陸、印度和日本爲主，其中日本和澳洲的企業在此指標中增幅最大，12% 的日本受訪者和 47% 的澳洲受訪者表示成本超過 500 萬美元。日本企業面臨最大的挑戰在於，很難跨越多家廠商來協同處理網路攻擊警訊，企業通常在遇到特別的網路威脅時，會採用不同的解決方案來應對，並沒有一

《註 32》一般社団法人 JPCERT コーディネーションセンター，〈JPCERT/CC 事業概要〉，《一般社団法人 JPCERT コーディネーションセンター》，2016 年 10 月 3 日，http://www.jpcert.or.jp/profile.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 33》香港經濟日報，〈網絡漏洞致財務損失 澳洲日本重災區〉，《香港經濟日報》，2019 年 3 月 7 日，https://www.cisco.com/c/zh_cn/about/press/2019/03-07.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 34》思科，〈預見未知情況：資安長（CISO）基準研究〉，《2019 年思科網路安全系列》，2019 年 3 月，https://www.cisco.com/c/zh_cn/about/press/2019/03-07.html，最後瀏覽日期：2021 年 2 月 24 日。

套完整且通用的網路安全解決方案，此現象造成企業在建構網路安全能力時相當碎片化。個別的單點網路安全解決方案雖然可以修補個別的網路安全漏洞，但駭客正不斷合作發動新的網路攻擊，造成特定目標損失。

二、企業網路安全意識低落

2019 年 7 月日本行動支付 7 Pay 的資安風暴事件中，凸顯日本的 IT 產業發展相對落後，特別是軟體產業 [35]。日本企業普遍缺乏數位素養，而且大多數企業爲中小企業，對資訊科技的導入與採用通常謹慎且保守，由於以價格導向爲考量，因此中小企業的網路安全防護能力普遍不足。此外，日本企業普遍缺乏專職的首席資訊安全官。由於設立專職的首席資訊安全官（Chief Information Security Officer, CISO）對於企業來說相當重要，企業設置首席資訊安全官意味著將網路和資訊安全納入營運風險來考量，若是首席資訊安全官能獲得公司高層的授權和重視，將更能發揮實質影響力。當前日本企業中少有設立首席資訊安全官一職。根據「情報處理推進機構」公布的《2017 年關於公司 CISO 和 CSIRT 實際調查報告》顯示，日本有 63% 的企業設立首席資訊安全官，其中有 35% 爲「兼任」角色，而美國和歐洲企業設置首席資訊安全官的比率，分別高達 95% 和 85%，其中，兼任的比率爲 17% 和 18% [36]。日本企業傾向以兼任的方式聘僱首席資訊安全官，由於日本的企業管理高層對於資安的認知未達一定高度，因此，對於設置專職的首席資訊安全官的態度較爲保守。另外，歐美企業對於從外部招聘首席資訊安全官的態度較能敞開接受，但日本保守的企業文化較難接受從外部招聘高階管理人士，因此，美國或歐洲企業對於外部招聘和指定首席安全官的做法不一定在日本可行。

三、資通訊產業對政策缺乏主動性

由於日本 90% 的資通訊技術歸行業所有，大部分的技術都掌握在產業界手中，政府部門只占了 6% [37]。日本行業的被動態度造成社會和經濟的負面影響，特別是在

《註 35》降旗淳平，〈7pay 事件から見えた　サイバーセキュリティーの盲點〉，《日経 X TREND》，2019 年 7 月 22 日，https://xtrend.nikkei.com/atcl/contents/watch/00013/00537/，最後瀏覽日期：2021 年 2 月 24 日。

《註 36》獨立行政法人情報処理推進機構，〈企業の CISO や CSIRT に関する実態調査 2017〉，《独立行政法人情報処理推進機構》，2017 年 4 月 13 日，頁 22-25，https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html，最後瀏覽日期：2021 年 2 月 24 日。

《註 37》経済産業研究所，〈JIP データベース 2015〉，《独立行政法人経済産業研究所》，2015 年 12 月 8 日，https://www.rieti.go.jp/jp/database/JIP2015/index.html，最後瀏覽日期：2021 年 2 月 24 日。

網路安全方面[38]。日本的大型企業在面對國家政策要求上，常抱持著傳統的態度，甚至是被動等待政府機關下達指令。相較而言，美國大型企業本著參與政策訂定與監管政策的目的，會透過企業的政策團隊或行業協會，主動公開地與政府單位進行接觸與遊說，如今，少有日本企業在內部設立公共政策宣傳團隊。雖然企業部門以非正式方式進行討論，但要訂定影響日本政府、社會大眾，甚至是全球消費者、客戶和業務合作夥伴的權力仍掌握在政府手中。但是，政府機關卻往往缺乏私部門所具備的網路安全專業技術和操作知識。

四、缺乏網路安全人才

網路安全人才短缺是日本多數企業共同關注的問題。根據經產省於 2016 年 6 月公布的調查結果顯示，2016 年只有約 28 萬 870 人可以填補約 41 萬 2,930 個網路安全有關職缺，網路安全人才缺乏約 13 萬 2,060 人。2020 年日本的網路安全人才缺口將達到 19 萬 3,010 人[39]。日本網路安全人才的短缺，是因爲日本企業高度依賴外包的 IT 和網路安全技術人員。在美國，大約 71.5% 的 IT 專業人士爲企業職員；在日本僅有 24.8% 的 IT 人員是企業職員[40]，這些職員相對缺乏網路安全所需具備的專業知識。不僅如此，企業文化的差異也會影響企業職員對於網路安全專業技能的培養，歐美企業重視的是員工的專業技能，透過專業技能的互補，進而建立專業的網路安全團隊；相反的，日本企業傾向尋找通才及文化適應者，企業較關注員工的整體技能[41]。此外，日本企業大多認爲網路安全問題是技術問題，用技術就能夠克服，但是網路安全防護除了須具備基礎的專業技術外，尚須搭配企業整體的網路安全規劃與企業高層的承諾與重視[42]。總體來說，缺乏訓練有素且技術精湛的網路安全人才是各個產業正在面對的問題，隨

《註 38》Shinichi Yokohama, “Business Management and Cybersecurity: Digital Resiliency for Executives,” NTT Group, March, 2018, pp.111-114, http://www.ntt.co.jp/topics_e/CfBE2018/img/201803_Business_Management_and_Cybersecurity.pdf.

《註 39》経済産業省商務情報政策局情報処理振興課，《IT 人材の最新動向と將來推計に関する調査結果——報告書概要版》，2016 年 6 月 10 日，頁 12，http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf，最後瀏覽日期：2021 年 2 月 24 日。

《註 40》Cynthia Brumfield, “Why NIST is so popular in Japan,” Cyberscoop, November 8, 2018, https://www.cyberscoop.com/nist-japan-workforce/, last visited: February, 24, 2021.

《註 41》E 安全，〈日本網路安全現狀：企業文化制約安全發展〉，《安全內參》，2018 年 7 月 6 日，https://www.secrss.com/articles/3766，最後瀏覽日期：2021 年 2 月 24 日。

《註 42》Mihoko Matsubara, “The Cybersecurity Canon: Cybersecurity for Business Executives Toward an Era When Everything Is Connected,” paloalto, June 5, 2017, https://researchcenter.paloaltonetworks.

著網路威脅不斷增加，網路安全人才短缺將成爲更加緊迫的問題。

五、網路安全預算分散

政府的經費預算是推動網路安全政策的重要推動力。《網路安全基本法》從法律上規定「網路安全戰略本部」掌管日本網路安全經費預算分配。根據日本「網路安全戰略本部」的經費預算數據顯示，2014年投入567.2億日圓，2015年投入839.6億日圓，2016年度投入570.5億日圓，2017年投入619.9億日圓，2018年投入634.1億日圓，2019年投入764.9億日圓，2020年投入881.1億日圓[43]（參見下頁表2）。日本網路安全相關計畫在部門分配和執行方面，呈現以內閣網路安全中心、經產省、總務省、防衛省的網路安全預算經費最多。2014年防衛省的網路安全預算爲184.2億日圓，比2015-2019年來得高，防衛省於2014年3月26日成立網路防衛隊，比起2013年防衛省的網路安全預算85.1億日圓，增加了99.1億日圓[44]。2020年預算最高的項目爲防衛省的新措施，除了以176.5億日圓增強網路安全系統外，更投入44.6億日圓運用最新的網路有關技術。防衛省表示，目的是爲了集中管理自衛隊的網路安全系統及運用AI技術進行網路防禦。不過，日本的網路安全預算呈現零碎化現象，其計畫執行和項目是分散在各省廳，由於資訊的不對稱會影響網路安全預算和經費的完整性，也容易降低財政支出的效率。

六、網路安全戰略本部與IT戰略本部權限之爭

網路安全戰略本部是由IT戰略本部隸屬之資訊安全對策推進會議中獨立升格而來，兩者從上下隸屬關係轉變爲同級別合作關係，網路安全戰略本部在推動網路安全政策的同時，必須注意不涉及IT戰略本部的職權事務。而兩部門在有些領域上交叉重疊，但在日本官僚長期存在互相掣肘、各自爲政的傳統下，兩部門如何緊密合作將成爲課題。此外，《網路安全基本法》與《IT基本法》的制定背景與理念存在差異，也就是網路安全與資訊自由化的

com/2017/06/cybersecurity-canon-candidate-book-review-cybersecurity-business-executives-toward-era-everything-connected/, last visited: February, 24, 2021.

《註43》〈政府のサイバーセキュリティに関する予算〉，《内閣サイバーセキュリティセンター》，2020年1月30日，https://www.nisc.go.jp/conference/cs/dai23/pdf/23shiryou04.pdf，最後瀏覽日期：2021年2月24日。

《註44》情報セキュリティ政策會議，〈政府の情報セキュリティ予算について〉，《内閣サイバーセキュリティセンター》，2013年5月21日，https://www.nisc.go.jp/conference/seisaku/index.html，最後瀏覽日期：2021年2月24日

表 2　日本 2014-2020 年各省廳網路安全預算經費分配表（億日圓）

部門＼億日圓	2014 年	2015 年	2016 年	2017 年	2018 年	2019 年	2020 年
網路安全預算總計	567.2	839.6	570.5	619.9	634.1	764.9	881.1
內閣網路安全中心	17.2	84.6	21.5	23.9	61.9	24.9	40.5
警察廳	9.5	8.8	6	12.8	12.6	4.5	20.5
總務省	17.6	277.6	20.3	22.1	23.5	30.5	32.6
外務省	4.5	5	4.2	6.2	7.4	6	6.4
經產省	54.8	138.2	93.1	78.7	100.9	43.8	50.3
防衛省	184.2	41.2	91.1	14	46.3	-	221.1
個人資訊保護委員會	-	1.9	2.6	13.3	12.4	11.7	17.8
厚生勞動省	-	12.7	41.4	42.1	46.5	40.4	34.1
文部科學省	-	1.9	11.6	12.4	23.3	11.4	12.2
金融廳	-	-	0.3	0.5	0.6	0.7	0.9
國土交通省	-	-	0.3	0.6	1.1	0.5	0.7

資料來源：作者自行整理。

衝突問題，《IT 基本法》制定於 2000 年，希望能促進資訊自由流通；而《網路安全基本法》則是提到，要在網路安全爲前提的情況下促進資訊自由流通。從《網路安全基本法》第 3 條中提到網路安全與資訊化問題，在第 1 款中強調幾點，要確保資訊自由流通、網路空間自由、鼓勵創新、促進社會經濟活力等重要性。在第 3 款中則寫明，關於推動網路安全，必須不斷採取措施，以推動互聯網及其他資通訊網路的完善和技術的廣泛應用，來促進社會經濟活力。在第 5 款中也寫明，推動網路安全措施，必須要兼顧《IT 基本法》的理念。第 6 款則提到，對於實施網路安全措施，必須注意不能侵犯國民的權利。但以上這些條款缺乏詳細的實施細則，在網路安全政策推動上難以操作。由於《網路安全基本法》注重安全保障和危機管理等強制性規定，因此自然會限制資訊的自由流通。因此，日本同時面臨如何在確保公民隱私、言論自由等前提下來加強網路安全的難題。

伍、日本網路安全發展之特色

一、日本積極建構國家級網路安全聯防體系

爲了統籌建構國家層級的網路安全聯防體系，日本在 2015 年 1 月設置「網路

安全戰略本部」及「內閣網路安全中心」。根據日本《網路安全基本法》規定，「網路安全戰略本部」的任務爲：訂定《網路安全戰略》並推動實施；訂定政府機關、獨立行政法人之網路安全標準；對網路安全重大事件進行調查，爲日本網路安全戰略的最高決策單位。此外，「網路安全戰略本部」與「國家安全保障會議」（NSC）及「IT戰略本部」緊密聯繫與合作，共同處理網路安全相關重大事件。「內閣網路安全中心」則由「內閣官房資訊安全中心」升格而來，爲「網路安全戰略本部」事務局，負責政策具體落實與執行。該中心的任務是透過「政府機關資訊安全跨部門監視及緊急處理小組」（GSOC），監視分析政府機關的資訊系統是否有網路異常情形。當發生大規模網路安全事件，由內閣危機管理監、內閣官房副長官助理、緊急事件應對室來應對；發生武力攻擊時，由國家安全保障局因應；日常的網路安全危機管理，則由內閣網路安全中心應對。

爲因應持續升高的網路威脅，防衛省於 2014 年 3 月成立「網路防衛隊」，該隊直接隸屬於防衛大臣，由統合幕僚監部幕僚長負責指揮，主要負責自衛隊內部之網路安全防護、威脅情報蒐集、網路安全演訓、調查研究與技術支援等。2013 年 7 月防衛省成立網路防禦委員會（Cyber Defense Council, CDC），提高防衛省與國防產業間的網路安全合作，目的在於促進國防產業間的情報分享。在網路威脅日益嚴峻下，日本進行組織調整與創新，旨在強調職能擴大，避免網路空間所造成的嚴重損害，進而影響國家安全與經濟發展。本文認爲，組織調整並非重新建立新的單位，而是在網路安全政策倡議的過程中，打破制式的傳統觀念，可在現有的組織體系下做變動，並跨越政府機關、公私部門間的合作障礙。

二、建立網路安全資訊共享機制

日本在網路安全積極建立資訊共享機制，重要法人機關有：「情報通信研究機構」、「情報處理推進機構」、「日本電腦緊急應變小組協調中心」、「網絡安全協議會」等。其中，2019 年 4 月成立的「網絡安全協議會」是目前資訊共享機制中級別最高的，由「內閣網路安全中心」主導，由政府機關、地方政府、關鍵基礎設施營運商、網路安全企業及大學和教育研究單位所組成。由於網路攻擊常以關聯企業或以特定單位爲攻擊對象，即時的資訊共享與互相通報將對防止受害範圍擴大十分重要，因此，當成員企業或會員受到網路攻擊時，「內閣網路安全中心」會收到通報並進行分析，再將網路攻擊分析結果通知會員企業，防止受害範圍持續擴大。

每個共享機制都有各自的成立目的和任務，如：「情報通信研究機構」爲總務省下轄的獨立行政法人，該機構針對網路攻擊建構視覺化的監測系統，有三種網路攻擊視覺化平台，分別爲「網路攻擊監測系統」（NICTER）、「網路攻擊防禦告警系統」

（DAEDALUS）及「NIRVANA 改」[45]。透過這些網路攻擊監測系統，能對攻擊者進行監視及分析，並能將偵測到的網路攻擊行爲即時回報給系統管理者，以加強系統的安全。另，「情報處理推進機構」爲經濟產業省下轄的獨立行政法人，於 2011 年 10 月成立「日本網路安全資訊分享夥伴協議會」（J-CSIP），設立目的爲加強公私部門的資訊共享與合作，共設 11 個關鍵基礎設施領域 SIG 小組，可以促進領域情資分享，掌握各領域整體資安現況，並強化各關鍵基礎設施提供者進行合作。「情報處理推進機構」亦積極與「內閣網路安全中心」及「日本電腦緊急應變小組協調中心」密切合作，對於影響關鍵基礎設施的重大網路事件做出反應。

另外，網路安全演習在資訊共享中扮演著重要的角色。爲了增強關鍵基礎設施網路安全部門應對緊急事態的響應能力，日本政府每年都會舉辦各式網路安全演習。從 2006 年開始，由內閣官房主導，聯合日本國內關鍵基礎設施所屬省廳、營運商等相關單位，實施關鍵基礎設施跨域演習。網路安全演習一般會預設一個突發事件，關鍵基礎設施行業間會針對此一突發事件共同展開對策，最終要使關鍵基礎設施恢復到正常運作的目標。演習的目的是要考察各設施間的資訊共享能力，以及與「內閣網路安全中心」、「情報處理推進機構」、「日本電腦緊急應變小組協調中心」情報傳遞與應急處理能力。網路安全演習可以對資訊共享機制的運作狀況進行驗證，在演習中出現的問題可以暴露和反映現行機制中實際存在的問題和漏洞，爲事後共享機制的完善和訂定提供建議。網路安全演習類別，包括：「內閣網路安全中心」針對情報分享與分析中心聯絡協議會（CEPTOAR-Council）舉辦大規模的網路攻擊演訓；經產省則主導電力、工業控制系統網路安全演習；總務省則負責「資通訊科技資訊分享與分析中心」（ICT-ISAC）的網路攻擊演習；國土交通省則舉辦有關航空、鐵路、物流等各種關鍵基礎設施領域的網路安全演習，透過建構縱向之情資分享機制，來促進該領域內相關成員之合作。

三、日本《網路安全戰略》升級與演進

隨著網際網路的迅速發展，網路威脅變得日益嚴重，過去的資訊安全戰略已無法應對網路威脅的挑戰。爲因應網路威脅，美、英、德、法、韓等國家紛紛提出國家級的《網路安全戰略》。在此背景下，日本政府於 2013 年 6 月、2015 年 9 月、2018 年 7 月陸續公布《網路安全戰略》，從國家層面對網路安全進行架構設計和指導。相較於 2013 年版《網路安全戰略》，

《註 45》「NIRVANA 改」爲專注於從資安監控中心（Security Operation Center, SOC）收集之 Log 進行視覺化分析，主要針對 APT 攻擊之 Log 資料。

2015 年版的《網路安全戰略》更加強調網路安全防護機制的主動性，從事後應變轉爲先發制人、從被動的網路安全防護轉變爲積極主動預測、從網路空間朝向融合空間來發展，最大的變化主要有以下四個方面：（一）網路安全議題被納入日本《國家安全保障戰略》中，提高至國家安全層次，2013 年底日本公布《國家安全保障戰略》，並以此爲基礎重新訂定《防衛計畫大綱》及《中期防衛力量整備計畫》，以上文件皆提到網路安全的重要；（二）《網路安全戰略》建立在《網路安全基本法》之上；（三）強化情資共享與交換，2013 年 12 月 6 日日本政府通過《特定祕密保護法》，該法案通過後，可以推進與同盟友好國家重要的情報交換與分享，並且得以強化機密情報的保護機制；（四）2015 年版《網路安全戰略》目標及基本原則更加明確，除了要遵循 2013 年版本外，其他五項基本原則爲：確保資訊自由流通、法治、開放性、自律性及協同合作。

從 2015 年版及 2018 年版《網路安全戰略》可看出，日本政府施行「積極網路防禦」戰略：一是更強調事前積極防禦。2015 年版《網路安全戰略》指出，達成戰略目標的各項舉措必須符合從「事後因應轉變爲事前防禦」、被動變爲主動之態勢；2018 年版《網路安全戰略》明確指出，爲了實施積極網路防禦戰略，政府將與網路企業合作，利用技術誘導網路攻擊方式蒐集攻擊者的背景及相關資訊，進而增進威脅資訊共同使用。二是重視提高網路威懾力。日本網路安全戰略以美日同盟爲基礎，日本認爲美日同盟應遵循美國在網路空間推行網路威懾戰略。另外，日本將透過增強執法機關與自衛隊的網路安全防護能力，提高日本的網路威懾力。此外，日本政府於 2018 年 12 月公布的新版《防衛計畫大綱》也強調，自衛隊須具備「網路反擊能力」。

四、美日網路安全合作朝向機制化及常態化

美日網路安全合作逐漸朝向機制化及常態性發展。美國戰略與國際問題研究中心（CSIS）2015 年 11 月發表《U.S.-Japan Cooperation in Cybersecurity》報告，內容強調爲應對中國大陸、俄羅斯與北韓所發動的網路攻擊，美日須加強網路安全合作的重要性。鑑於日本鄰近這三個最活躍的網路攻擊國家，日本與美國深化網路安全合作顯得至關重要。日本自身需要提高網路防護能力，以便未來與美國在國防事務上展開全面的夥伴關係。美日同盟需要在網路安全上進一步合作，分別是：（一）日本需要在網路安全領域上分配足夠的資源；（二）在定義和實施網路空間集體防衛方面達成共識；（三）建立網路威脅資訊共用雙邊合作機制，共同研發削弱網路攻擊技術；（四）發展健全實用的聯合訓練和演習；（五）擴大民用關鍵基礎設施防護、反間諜活動方面的雙邊合作；（六）協調各方努力，建構網路安全框架，在東北亞建立網路互信等措施。

2011 年 6 月、2012 年 4 月兩次「美日安全保障協議委員會」達成的共識，皆強調網路安全合作對於美日同盟的重要性，明確指出雙方將積極展開政府間的合作。另，2013 年 10 月 3 日「美日安全保障協議委員會」強調網路安全是美日同盟的新領域，特別要在保密及網路系統裝備上合作，並納入修正的《美日防衛合作指針》。除了設立共同目標外，更設立新的美日網路安全協調機制「美日網路防衛政策工作小組」（CDPWG），共同應對網路威脅。截至 2016 年底，美國和日本在網路安全方面已形成「美日網路安全對話」、「美日網路防衛政策工作小組會議」與「美日網路經濟政策合作對話」等三個政府間常態性對話機制。這些對話機制的目標爲，透過美日同盟來深化雙方的網路安全合作，內容包括：協商合作、共用網路安全情報、共同推動訂定網路空間國際規則、建立互信機制、共同應對網路威脅、美國協助日本訂定《網路安全戰略》、共同對第三國家實施網路安全支援、共同防護重要關鍵基礎設施、研討美日網路安全防衛合作事項等。

2015 年 4 月 28 日「美日安全保障協議委員會」發布新版《美日防衛合作指針》，重新定義美日軍事合作，取消了美日軍事合作的地理限制範圍，將美日軍事合作推向「全球」，甚至擴及網路與太空領域，強調美日政府間的「無縫」合作。爲了進一步凸顯美日同盟的「全球性質」，美日兩國擴展太空與網路等新戰略領域之合作。美日將針對各自與太空系統強化情監偵性能，如：早期預警、情監偵（Intelligence, Surveillance and Reconnaissance, ISR）、方位測定、導航等任務能量。在網路空間合作上，美日政府針對網路空間威脅，進行監視、防護演練、網路安全及相關知識交流，共同提高網路及系統堅固性。2015 年 4 月「美日國防部長會談」決議設立「太空合作工作小組」（SCWG），並透過「美日網路防衛政策工作小組」（CDPWG）推動太空政策協議、深化情報共用機制、合作培育太空領域專門人才、實施兵棋推演等事項。

五、日本強化網路安全國際合作

國際合作是日本網路安全政策的重點項目。2013 年版《網路安全戰略》提出以創造「世界領先的網路空間」爲目標，將訂定網路安全相關國際規則。2013 年 10 月「資訊安全政策會議」正式公布《網路安全國際合作方針》，內容闡述日本網路安全國際合作的政策方向與合作領域，以及在世界各地的合作計畫。爲了強化網路安全問題國際合作，日本致力於建構全球網路安全意識、促進國際網路安全資訊交流、普及網路安全技術等三方面。重點項目爲建構應對網路攻擊事件的全球動態體制，加強與各國調查機關的情報交流；致力於構築對網路安全問題之國際合作能力，與各國調查機關共同發展網路犯罪調查能力培訓，提供各種最新的網路趨勢與技術解決方案；訂定網路安全國際規則並

開展雙邊、多邊的國際合作協商機制。截至 2016 年底，日本已經與美國、英國、法國、俄羅斯、德國、澳洲、以色列、愛沙尼亞、歐盟、中國大陸、韓國、印度等 12 個國家簽署雙邊網路安全協議或展開網路安全對話。日本亦積極參加國際會議推動網路安全合作，如在七大工業國集團（G7）高峰會、東協——日本論壇（ASEAN-Japan Forum）、G7 網路工作小組、聯合國政府專家小組（GGE）、東協區域論壇網路安全專家會議（ARF-ISM on ICTs Security）等國際場合上積極推動合作。

日本的網路安全國際合作主要有「一個中心」和「三大支柱」。「一個中心」是以歐美等西方國家爲中心；「三個支柱」爲推動和訂定網路空間國際規則、與各國建立信心措施、建構網路安全防護能力；簡而言之，以歐美國家的網路安全概念爲核心，透過三大支柱來開展網路外交。首先，日本積極與國際組織和同盟國家展開網路安全合作，透過多邊的網路安全合作架構來增強日本在國際組織中的角色，同時參與訂定國際網路安全標準和規則。日本主要是以聯合國政府專家小組（The Group of Governmental Experts, GGE）爲平台，在聯合國內展開多邊的網路安全合作，同時積極參與國際電信聯盟（International Telecommunication Union, ITU）、國際電工委員會（International Electrotechnical Commission, IEC）等組織活動，進而參與網路安全技術標準的訂定。同時，日本還展開與歐盟、以色列、澳洲、印度、東協等國家的網路安全合作對話。日本在網路安全國際合作方面，累積了豐富經驗，一是日本積極致力建構應對網路攻擊事件的全球動態體制，透過多種管道，串聯各國負責網路犯罪執法部門、全球各個研究網路犯罪與趨勢的資安研究單位，發揮資訊互通有無的功能，並能即時掌握最新網路犯罪趨勢。爲了強化合作能力，日本與各國調查機關共同發展網路犯罪調查能力培訓計畫，掌握最新的鑑識與犯罪偵查技術。二是日本積極致力於建構網路犯罪與資安趨勢研究單位，提供各種最新的趨勢與技術解決方案，強化國際合作中的研究開發活動。三是日本積極訂定關於網路安全國際規則，展開雙邊、多邊的國際合作機制。

陸、結論：對臺灣的啓示與借鏡

爲了因應政府推動數位國家與創新經濟發展所面臨的網路安全威脅和挑戰，2018 年 9 月國家安全會議公布《國家資通安全戰略報告》，推動總統所宣示「資安即國安，打造安全可信賴的數位國家」政策，亦是將資安提升至國家層級的政策規劃。行政院國家資通安全會報則於 2001 年 1 月成立，積極推動國家資通安全之基礎建設工作。資安會報自 2001 年迄今，陸續推動 5 大階段、各爲期 4 年之重大資通安全計畫或方案。同時，爲了強化我國八大關鍵基礎設施之資安防護能力，於 2018 年 5 月推動並通過《資安管理法》，並且搭配投入「資安旗艦計畫」及「前瞻基礎建設

計畫」。臺灣由於政經環境特殊，經常面臨國家級的駭客組織威脅，雖然有其相關的資通安全計畫或發展方案，但臺灣的資安發展仍面臨產業規模小、產值較低、國家整體資安聯防機制仍待深化，且欠缺資安核心技術，缺乏實戰經驗等資安人才等。

爲了強化臺灣網路安全發展，有以下建議：（一）公私協力深化合作，加強關鍵基礎設施聯防機制，建置模擬場域，進行網路安全演習，此部分可邀請民間業者加入網路攻防演練隊伍，強化網路安全演習成效；（二）促進資安產業的跨領域交流與合作，包括推動跨領域聯防計畫，結合資安業者與臺灣優勢產業，如：半導體、物聯網等共同組成團隊，開發資安的整體解決方案；（三）積極推動網路安全外交。臺灣可借鏡日本將網路安全視爲重要的外交政策議題與工具，在應對國家級的網路攻擊中，可透過美日的網路安全合作框架增強自身的角色，臺灣在網路安全方面也應投入更多資源，以便與美國在網路安全事務上展開更全面的合作關係。

《2020 美國國防授權法案》中，特別以專節授權與臺灣在網路安全領域中進行合作，凸顯臺灣在全球網路安全戰略的重要角色。爲此，臺美日可在以下領域上進一步合作：1. 在定義和實施網路空間集體防衛方面達成共識；2. 建立網路威脅資訊共享機制，共同研發網路防禦技術；3. 展開健全且實用的聯合網路安全演習；4. 擴大重要關鍵基礎設施網路安全防護，包括公部門、金融業、醫療產業等；5. 建構臺美日網路安全合作框架，在亞太區域共同建立網路互信措施等，與亞太區域國家共同維護網路安全合作能量；（四）強化與國際資安研發機構合作，進行技術或人才的交流，合作的對象可從資安重點學校、國家智庫或實驗室到標準訂定等相關機構；（五）培育資安創新人才，透過舉辦資安競賽，可以吸引白帽駭客社群挖掘企業產品資安漏洞，持續優化產品的安全設計。此外，爲扶植資安新創，可加強資安新創與 ICT 業者交流，強化業者的可信度，目標使資安社群產業化。

（作者古涵詩為國立中山大學中國與亞太區域研究所博士候選人）

參考文獻

一、中文部分

專書

電信總局、台灣經濟研究院，《因應技術匯流發展，相關法規之修訂研究》。臺北：

交通部電信總局，2004 年，頁 110-114，https://www.ncc.gov.tw/chinese/files/07051/474_13.pdf。

期刊論文

陳文哲，2012 年 8 月，〈日本警方因應網路恐怖攻擊對策〉，《刑事雙月刊》，第 49 期，頁 58-63。

研討會論文

林賢參，2008 年 6 月 18 日，〈從社會治安的角度探討反恐應有的措施——以日本反恐對策爲考察對象〉，2008 警學與安全管理研討會，臺北：臺灣警察專科學校。

網際網路

〈「民主主義揺るがす」東京五輪団体へのサイバー攻撃——加藤官房長官〉，《JIJI.COM》，2020 年 10 月 20 日，https://www.jiji.com/jc/article?k=2020102000515&g=pol，最後瀏覽日期：2021 年 2 月 24 日。

E 安全，〈日本網路安全現狀：企業文化制約安全發展〉，《安全內參》，2018 年 7 月 6 日，https://www.secrss.com/articles/3766，最後瀏覽日期：2021 年 2 月 24 日。

nippon.com，〈日本通過特定秘密保護法〉，《nippon.com》，2014 年 1 月 20 日，https://www.nippon.com/hk/features/h00044/，最後瀏覽日期：2021 年 2 月 24 日。

八時島綾平，〈日本在國際標準制定上追趕德國，中韓在後〉，《日經中文網》，2017 年 3 月 30 日，https://zh.cn.nikkei.com/politicsaeconomy/economic-policy/24424-2017-03-30-04-52-14.html，最後瀏覽日期：2021 年 2 月 24 日。

日川佳三，〈爲什麼駭客特別愛攻擊日本〉，《商周 .COM》，2013 年 6 月 25 日，http://www.businessweekly.com.tw/article.aspx?id=3945&type=Blog&p=0，最後瀏覽日期：2021 年 2 月 24 日。

日經 BP 社，〈JAXA 伺服器遭非法訪問 希望號運行準備資訊洩漏〉，《日經 BP 社報導》，2013 年 4 月 25 日，http://big5.nikkeibp.com.cn/news/mobi/65809-20130424.html，最後瀏覽日期：2021 年 2 月 24 日。

王家宜，〈日本控制系統安全中心〉，《行政院國家資通安全會報技術服務中心》，2015 年

7 月 27 日，https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1377，最後瀏覽日期：2021 年 2 月 24 日。

行政院科技顧問組，2011 年 12 月 31 日。〈關鍵資訊基礎建設保護政策指引〉，《臺南市政府地政局》，頁 74，http://land.tainan.gov.tw/FileDownLoad/FileUploadList/744.pdf，最後瀏覽日期：2021 年 2 月 24 日。

行政院國家資通安全會報，〈國家資通安全發展方案 102 至 105 年〉，《行政院國家資通安全會報》，2013 年 12 月，頁 2-7，http://www.nicst.ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=918F43FED41196D2，最後瀏覽日期：2021 年 2 月 24 日。

行政院國家資通安全會報，〈國家資通安全發展方案 106 至 109 年〉，《行政院國家資通安全會報》，2017 年 11 月，https://www.nicst.ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=5582A0F79672DAD9，最後瀏覽日期：2021 年 2 月 24 日。

防災科技研究中心，〈關鍵基礎設施安全防護〉，《防災科技研究中心》，2012 年 2 月 15 日，http://dptrc.sinotech.org.tw/chinese/03_news/022_detail.php?pid=7，最後瀏覽日期：2021 年 2 月 24 日。

林威邑，〈企業何時會被駭客攻陷 回朔式掃描與預警機制的重要性〉，《麟銳科技》，2016 年，http://www.ringline.com.tw/zh-tw/article_info.php?id=78，最後瀏覽日期：2021 年 2 月 24 日。

思科，〈預見未知情況：資安長（CISO）基準研究〉，《2019 年思科網路安全系列》，2019 年 3 月，https://www.cisco.com/c/zh_cn/about/press/2019/03-07.html，最後瀏覽日期：2021 年 2 月 24 日。

施慧中，〈IT 先進大國 日電子支付因高齡化推動困難〉，《公視新聞網》，2019 年 8 月 27 日，https://news.pts.org.tw/article/443702，最後瀏覽日期：2021 年 2 月 24 日。

香港經濟日報，〈網絡漏洞致財務損失 澳洲日本重災區〉，《香港經濟日報》，2019 年 3 月 7 日，https://www.cisco.com/c/zh_cn/about/press/2019/03-07.html，最後瀏覽日期：2021 年 2 月 24 日。

陳淑娟，〈日本眾院疑遭中國大陸駭客入侵〉，《中央日報網路報》，2011 年 10 月 25 日，http://cdnews.com.tw/cdnews_site/docDetail.jsp?coluid=109&docid=101705110，最後

瀏覽日期：2021 年 2 月 24 日。
陳曉莉，〈日本最大國防承包商三菱重工證實遭駭〉，《iThome》，2011 年 9 月 20 日，http://www.ithome.com.tw/node/69808，最後瀏覽日期：2021 年 2 月 24 日。
臺北駐日本經濟文化代表處科技組，2017 年 9 月 22 日。〈日本情報通信研究機構開發解析網路「標的型攻擊」之法〉，《臺北駐日本經濟文化代表處科技組》，https://www.most.gov.tw/japan/ch/detail?article_uid=7b55a278-b4f4-44cc-90b4-b3725dd68287&menu_id=a0a402e3-4dd6-4411-a21b-9ecdf4f5af66&content_type=P&view_mode=gridView，最後瀏覽日期：2021 年 2 月 24 日。

二、日文部分

專書譯著

Crandall, Robert W & Waverman, Leonard 著，福家秀紀、栗澤哲夫譯，《IT 時代のユニバーサル・サービス 効率性と透明性》（Who Pays for Universal Service? When Telephone Subsidies Become Transparen）（東京：NTT 出版社，2001 年），頁 21-22。

網際網路

IT 戦略本部，〈e-Japan 戦略〉，《IT 総合戦略本部》，2001 年 1 月 22 日，https://www.kantei.go.jp/jp/it/network/dai1/pdfs/s5_2.pdf，最後瀏覽日期：2021 年 2 月 24 日。
IT 戦略本部，〈e-Japan 戦略 II〉，《IT 総合戦略本部》，2003 年 7 月 2 日，https://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf，最後瀏覽日期：2021 年 2 月 24 日。
サイト引越し屋さん，〈国内であった Web サイト乗っ取り（改ざん）事例 5 件〉，《サイト引越し屋さん》，2017 年 8 月 8 日，https://site-hikkoshi.com/824/，最後瀏覽日期：2021 年 2 月 24 日。
サイバーセキュリティ.com 編集事務局，〈日本年金機構情報漏洩事件のすべて〉，《サイバーセキュリティ.com》，2016 年 6 月 10 日，https://cybersecurity-jp.com/security-incident-case/9146，最後瀏覽日期：2021 年 2 月 24 日。
サイバーセキュリティ戦略本部，〈サイバーセキュリティ基本法第 13 條の規定に基づきサイバーセキュリティ戦略本部が指定する法人〉，《サイバーセキュリティ戦略

本部》，2016 年 10 月 21 日，https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou01.pdf，最後瀏覽日期：2021 年 2 月 24 日。

サイバーセキュリティ戦略本部，〈サイバーセキュリティ戦略本部名簿〉，《内閣サイバーセキュリティセンター》，2016 年 4 月 1 日，https://www.nisc.go.jp/conference/cs/pdf/meibo.pdf，最後瀏覽日期：2021 年 2 月 24 日。

一般社団法人 JPCERT コーディネーションセンター，〈JPCERT/CC 事業概要〉，《一般社団法人 JPCERT コーディネーションセンター》，2016 年 10 月 3 日，http://www.jpcert.or.jp/profile.html，最後瀏覽日期：2021 年 2 月 24 日。

井上英明，〈2015 年のサイバー攻撃関連通信は 2 倍に急増、IoT 機器からが 2 割占めるへ〉，《ITPRO》，2016 年 3 月 8 日，http://itpro.nikkeibp.co.jp/atcl/column/14/346926/030700469/，最後瀏覽日期：2021 年 2 月 24 日。

內閣サイバーセキュリティセンター，〈サイバーセキュリティ政策に係る年次報告（2016 年度）〉，2017 年 7 月 13 日，頁 2-5，https://www.nisc.go.jp/conference/cs/dai14/pdf/14shiryou01.pdf，最後瀏覽日期：2021 年 2 月 24 日。

內閣官房，〈国家安全保障戦略について〉，《內閣官房》，2013 年 12 月 17 日，http://www.cas.go.jp/jp/siryou/131217anzenhoshou.html，最後瀏覽日期：2021 年 2 月 24 日。

內閣官房，〈平成 31 年度以降に係る防衛計画の大綱〉，《內閣官房》，2018 年 12 月 18 日，https://www.cas.go.jp/jp/siryou/h31boueikeikaku.html，最後瀏覽日期：2021 年 2 月 24 日。

內閣官房情報セキュリティセンター，〈セプターカウンシルの創設について〉，《內閣サイバーセキュリティセンター》，2009 年 5 月 8 日，頁 1-6。

內閣官房情報セキュリティ対策推進室，〈情報セキュリティ対策推進室の設置に関する規則〉，《內閣サイバーセキュリティセンター》，2000 年 2 月 29 日，https://www.nisc.go.jp/conference/suisinkaigi/dai1/0229kisoku.html，最後瀏覽日期：2021 年 2 月 24 日。

內閣サイバーセキュリティセンター，〈內閣サイバーセキュリティセンター（NISC）の組織体制〉，《內閣サイバーセキュリティセンター》，https://www.nisc.go.jp/about/organize.html，最後瀏覽日期：2021 年 2 月 24 日。

內閣サイバーセキュリティセンター，〈内閣サイバーセキュリティセンター（NISC）設置までの経緯〉，《内閣サイバーセキュリティセンター》，https://www.nisc.go.jp/about/details.html，最後瀏覽日期：2021 年 2 月 24 日。

内閣サイバーセキュリティセンター，2000 年 2 月 29 日。〈情報セキュリティ対策推進会議の設置について〉，《内閣サイバーセキュリティセンター》，https://www.nisc.go.jp/conference/suisinkaigi/0229suisinkaigi.html，最後瀏覽日期：2021 年 2 月 24 日。

内閣サイバーセキュリティセンター，〈情報セキュリティ対策推進会議〉，《内閣サイバーセキュリティセンター》，2005 年 7 月 14 日，http://www.nisc.go.jp/conference/suishin/ciso/pdf/konkyo.pdf，最後瀏覽日期：2021 年 2 月 24 日。

内閣サイバーセキュリティセンター，〈我が國のサイバーセキュリティ政策の概要〉，《内閣サイバーセキュリティセンター》，2017 年 1 月 30 日，http://www.soumu.go.jp/main_content/000463592.pdf，最後瀏覽日期：2021 年 2 月 24 日。

内閣官房情報セキュリティ対策推進室，〈内閣官房情報セキュリティセンター（NISC）の設置について〉，《内閣サイバーセキュリティセンター》，2005 年 4 月 21 日，https://www.nisc.go.jp/press/pdf/nisc_press.pdf，最後瀏覽日期：2021 年 2 月 24 日。

外務省，〈外務省のサイバー分野における取組——日本のサイバー外交〉，《外務省》，2017 年 11 月 1 日，http://www.mofa.go.jp/mofaj/annai/page5_000250.html，最後瀏覽日期：2021 年 2 月 24 日。

防衛省，〈サイバー防衛隊の新編について〉，《防衛省》，2014 年 3 月 25 日，http://www.mod.go.jp/j/press/news/2014/03/25d.html，最後瀏覽日期：2021 年 2 月 24 日。

防衛省，〈サイバー空間における対応〉，《平成 29 年版防衛白書》，2017 年 8 月 31 日，http://www.mod.go.jp/j/publication/wp/wp2017/html/n3127000.html，最後瀏覽日期：2021 年 2 月 24 日。

防衛省運用企画局情報通信研究課，〈防衛省のサイバーセキュリティへの取組〉，《防衛省》，2014 年 4 月，https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf，最後瀏覽日期：2021 年 2 月 24 日。

〈政府のサイバーセキュリティに関する予算〉，《内閣サイバーセキュリティセンター》，2020 年 1 月 30 日，https://www.nisc.go.jp/conference/cs/dai23/pdf/23shiryou04.pdf，

最後瀏覽日期：2021 年 2 月 24 日。

降旗淳平，〈7pay 事件から見えた　サイバーセキュリティーの盲點〉，《日経 X TREND》，2019 年 7 月 22 日，https://xtrend.nikkei.com/atcl/contents/watch/00013/00537/，最後瀏覽日期：2021 年 2 月 24 日。

高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）。〈高度情報通信ネットワーク社会形成基本法〉，《首相官邸》，2020 年 11 月 29 日，https://www.kantei.go.jp/jp/singi/it2/hourei/honbun.html，最後瀏覽日期：2021 年 2 月 24 日。

国立研究開発法人情報通信研究機構，〈Cyber Colosseo〉，《NICT》，2020 年 7 月，https://colosseo.nict.go.jp/，最後瀏覽日期：2021 年 2 月 24 日。

国立研究開発法人情報通信研究機構，〈サイバー攻撃誘引基盤“STARDUST”（スターダスト）を開発〉，《国立研究開発法人情報通信研究機構》，2017 年 5 月 31 日，https://www.nict.go.jp/press/2017/05/31-1.html，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ対策推進会議，〈重要インフラのサイバーテロ対策に係る特別行動計画〉，《内閣サイバーセキュリティセンター》，2000 年 12 月 15 日，https://www.nisc.go.jp/active/sisaku/2000_1215/1215actionplan.html，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ対策推進会議，〈情報セキュリティ対策推進室の設置に関する規則〉，《内閣サイバーセキュリティセンター》，2005 年 4 月 20 日，http://www.nisc.go.jp/about/pdf/050420-kisoku.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈サイバーセキュリティ戦略〉，《内閣サイバーセキュリティ センター》，2015 年 9 月 4 日，https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈サイバーセキュリティ戦略〉，《内閣サイバーセキュリティ センター》，2018 年 7 月 27 日，https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈重要インフラの情報セキュリティ対策に係る行動計畫〉，《内閣サイバーセキュリティ センター》，2005 年 12 月 13 日，https://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈重要インフラの情報セキュリティ対策に係る第 2 次行動計畫改定版〉，《内閣サイバーセキュリティセンター》，2012 年 4 月 26 日，https://www.nisc.go.jp/active/infra/pdf/infra_rt2-2.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈政府の情報セキュリティ予算について〉，《内閣サイバーセキュリティセンター》，2013 年 5 月 21 日，https://www.nisc.go.jp/conference/seisaku/index.html，最後瀏覽日期：2021 年 2 月 24 日。

情報セキュリティ政策会議，〈重要インフラの情報セキュリティ対策に係る第 3 次行動計畫（改訂版）〉，《内閣サイバーセキュリティセンター》，2015 年 5 月 25 日，https://www.nisc.go.jp/active/infra/pdf/infra_rt3_r1.pdf，最後瀏覽日期：2021 年 2 月 24 日。

情報処理推進機構技術本部セキュリティセンター，〈サイバー情報共有イニシアティブ（J-CSIP）運用状況〉，《情報処理推進機構》，2017 年 10 月 26 日，https://www.ipa.go.jp/files/000062172.pdf，最後瀏覽日期：2021 年 2 月 24 日。

経済産業省，〈電子署名及び認証業務に関する法律電子署名及び認証業務に関する法律〉，《経済産業省》，2000 年 5 月 31 日，http://www.meti.go.jp/policy/netsecurity/docs/esig/H12HO0102.txt，最後瀏覽日期：2021 年 2 月 24 日。

経済産業省，〈情報セキュリティ総合戦略〉，《経済産業省》，2013 年 10 月 10 日，http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_body.pdf，最後瀏覽日期：2021 年 2 月 24 日。

経済産業省，〈電力・ガス・ビル・化学分野のサイバーセキュリティ演習を実施します〉，《経済産業省》，2014 年 1 月 17 日，http://www.meti.go.jp/press/2013/01/20140117005/20140117005.html，最後瀏覽日期：2021 年 2 月 24 日。

経済産業省商務情報政策局情報処理振興課，《IT 人材の最新動向と將來推計に関する調査結果——報告書概要版》，2016 年 6 月 10 日，頁 12，http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf，最後瀏覽日期:2021年2月24日。

経済産業研究所，〈JIP データベース 2015〉，《独立行政法人経済産業研究所》，2015 年 12 月 8 日，https://www.rieti.go.jp/jp/database/JIP2015/index.html，最後瀏覽日期：

2021 年 2 月 24 日。

電子政府の総合窓口，〈サイバーセキュリティ基本法〉，《e-Gov》，2016 年 10 月 21 日，https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104，最後瀏覽日期：2021 年 2 月 24 日。

総務省，〈情報通信白書〉，《総務省》，2003 年 7 月，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h15/summary/summary01.pdf，最後瀏覽日期:2021 年 2 月 24 日。

総務省，〈「国民のための情報セキュリティサイト」のリニューアル〉，《総務省》，2013 年 4 月 5 日，http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000045.html，最後瀏覽日期：2021 年 2 月 24 日。

独立行政法人情報処理推進機構，〈企業の CISO や CSIRT に関する実態調査 2017〉，《独立行政法人情報処理推進機構》，2017 年 4 月 13 日，頁 22-25，https://www.ipa.go.jp/security/fy29/reports/ciso-csirt/index.html，最後瀏覽日期：2021 年 2 月 24 日。

警察庁情報通信局，〈警察のサイバーセキュリティ施策――における技術的対応〉，《警察庁情報技術解析課》，2015 年 10 月 22 日，https://www.npa.go.jp/cyberpolice/material/pdf/20151022_CSS2015.pdf，最後瀏覽日期：2021 年 2 月 24 日。

三、英文部分

專書

Steve Piper, *Definitive Guide to Next-Generation Threat Protection: Winning the War Against the New Breed of Cyber Attacks*. Annapolis, MD: CyberEdge Group, LLC, 2013, pp. 5-9.

網際網路

Cynthia Brumfield, “Why NIST is so popular in Japan,” Cyberscoop, 2018/11/8, https://www.cyberscoop.com/nist-japan-workforce/, last visited: February, 24, 2021.

HM Treasury, “G7 fundamental elements for cyber security,” GOV.UK, October 11, 2016, pp.1-3, https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security, last visited: February, 24, 2021.

Mihoko Matsubara, “The Cybersecurity Canon: Cybersecurity for Business Executives Toward an Era When Everything Is Connected,” paloalto, 2017/6/5, https://researchcenter.paloaltonetworks.com/2017/06/cybersecurity-canon-candidate-book-review-cybersecurity-business-executives-toward-era-everything-connected/, last visited: February, 24, 2021.

Shinichi Yokohama, “Business Management and Cybersecurity: Digital Resiliency for Executives,” NTT Group, 3, 2018, pp.74-75, http://www.ntt.co.jp/topics_e/CfBE2018/img/201803_Business_Management_and_Cybersecurity.pdf, last visited: February, 24, 2021.

Developments and Limitations of Japan's Cybersecurity Policy

Ku, Han-Shih

Abstract

In order to strengthen the capabilities of cybersecurity protection, Japan in 2015 established CSSHQ and NISC to attach important to cross-domain and public-private cooperation in cybersecuirty. Japan has reinforced intelligence exchanges with countries on Internet threats, formulated relevant international rules, and developed bilateral or multilateral cybersecurity dialogues. Consequently, Japan not only increases discourse power in the cyberspace but also actively practices cybersecurity diplomacy toward international collaboration and links. The purpose of this paper is to discuss a promotion system of the Japanese cybersecurity and developments and limitations of its policy. Furthermore, it summarizes the characters of and inspiration from the development of Japan's cybersecurity as a reference for Taiwan's cybersecurity policy.

Keywords: Cybersecurity, Cybersecurity Strategy, Basic Act on Cybersecurity, Cybersecurity Strategic HQs, Critical Infrastructure