全球政治評論　*Review of Global Politics*

第七十期（2020）No.70 頁 105-148

學術論文

日本網路安全戰略調整與組織變革[1]

Strategic Adjustments and Organizational Changes of Japan's Cybersecurity

古涵詩 *Han-Shih Ku*
中山大學中國與亞太區域研究所博士候選人
Ph.D. Candidate of Institute of China and Asia-Pacific Studies
National Sun Yat-sen University

摘要 / Abstract

日本為了因應網路威脅，於 2013 年公佈第一版《網路安全戰略》，將網路安全拉高到國家層次，朝向構建「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」的目標努力。同年 5 月，美日第一次舉行網路安全對話，聯合成立「美日網路防衛政策工作小組」，進一步推動美日在網路安全領域上的合作。2015 年根據《網路安全基本法》規定，將「資訊安全政策會議」及「內閣官房資訊安全中心」升格為「網路安全戰略本部」與「內閣網路安全中心」，組織調整的目的在於增強網路安全主責機關的監督權限，提高政策制定與執行單位間的效率。本文將探討日本因應網路威脅所進行的戰略調整，首先探討日本面臨的網路威脅與案例分

[1] 本文初稿曾發表於國立政治大學及當代日本研究學會舉辦之「亞太、日本與明治維新 150 年：日本研究的變與不變」學術研討會議（臺北：國立政治大學，2018 年 12 月 2 日）。

析，接著探討中央省廳對於網路安全組織積極調整與日本的網路安全國際合作。

In responding to cyber threats, Japan published the first Cybersecurity Strategy in 2013 and worked towards the goal of a “Cybersecurity Nation” with a “world-leading, resilient and vigorous cyberspace”. In May of 2013, the United States and Japan held their first cybersecurity dialogue and established the U.S.-Japan Cyber Defense Policy Working Group for prompting cybersecurity cooperation. According to Basic Act on Cybersecurity, Information Security Policy Conference and National Information Security Center were upgraded to Cybersecurity Strategic HQs and National Center of Incident Readiness and Strategy for Cybersecurity in 2015. The Japanese organizational adjustments were to strengthen the supervision authority of chief cybersecurity institutions and to raise policy formulation and efficiency between execution units. This study explores Japan’s strategic adjustments in response to cyber threats. At first, it discusses the Japanese cyber threats and case studies. Furthermore, the Central Government focusing on organizational adjustments and Japan’s international cooperation in cybersecurity are included in this paper.

關鍵字：網路安全戰略、網路安全基本法、美日同盟、美日防衛合作指針

Keywords: Cybersecurity Strategy, Basic Act on Cybersecurity, U.S.-Japan Alliance, Guidelines for U.S.-Japan Defense Cooperation

壹、前言

網際網路為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有組織甚至是由國家發起，以經濟或政治為目的之入侵行為。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。日本獨立行政法人情報通信研究機構（National Institute of Information and Communications Technology, NICT）於 2015 年 2 月 17 日的統計資料顯示，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] 此外，網路攻擊也擴大到國會、國防承包商，網路攻擊形式更為多樣化，如：2011 年 9 月，日本最大國防承包商三菱重工（Mitsubishi Heavy Industries, MHI）證實，許多工廠伺服器與電腦遭駭客植入惡意程式；[3] 再者，2011 年 10 月，《朝日新聞》報導指出，日本眾議院的公務電腦與伺服器遭中國大陸駭客入侵，部分國會議員的帳號密碼遭到破解，日本外交與國防等國政機密情報可能外洩；[4] 日本宇宙航空研究開發機構（JAXA）於 2013 年 4 月 23 日宣稱，伺服器遭到外部非法訪問，而洩漏的資訊是用於國際空間站—日本實驗艙「希望號」所使用的參考資料等。[5]

---

[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〉，《ITPRO》，2016 年 3 月 8 日，*http://itpro.nikkeibp.co.jp/atcl/column/14/346926/030700469/*。

[3] 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*。

[4] 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*。

[5] 〈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*。

以上網路安全事件對日本來說造成相當大的影響，五角大廈的公開報告中，透漏了某些遭到中國大陸間諜活動所竊取的武器設計資料，包括：愛國者三型（PAC-3）飛彈系統設計、反彈道飛彈終端高空防禦系統（Terminal High Altitude Area Defense, THAAD）、美國海軍神盾彈道飛彈防禦系統（Navy's Aegis ballistic-missile defense system）、F/A-18 型戰鬥機（F/A-18 fighter jet）、V-22 鶚式斜旋翼機（V-22 Osprey）、黑鷹直升機（Black Hawk helicopter）、美國海軍新型近岸作戰艇（Navy's new Littoral Combat Ship）、F-35 聯合打擊機（F-35 Joint Strike Fighter）等。[6] 倘若這些先進科技武器為中國大陸所用，意味著中國大陸能省下相當多武器研發時間，得以獲得作戰優勢。

2018 年 2 月，美國國家情報總監（National Intelligence）柯茲（Daniel Coats）表示，大部分偵測到中國大陸對產業所發動的網路攻擊中，目標通常是國防承包商及支援政府網路系統的科技公司。[7] 開發網路防禦產品的 FireEye 公司董事長達夫・德瓦爾特（Dave DeWalt）表示，在捲入網路戰爭的國家中，日本是特別危險的！因為日本企業擁有豐富的智慧財產權，成了重要的網路攻擊目標。[8] 美國網路安全學者龔培德（David C. Gompert）與李比奇（Martin Libicki）表示，雖然美國全球軍力遠勝於中國大陸，但中國大陸極可能利用網路戰來避免軍事失敗和削弱敵方的軍事系統，同時亦對雙方間的衝突施加影響力。目前，中國大陸發動的網路戰呈

---

[6] Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013, *https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html*.

[7] Steve Ranger, "Cyberattacks: China and Russia can disrupt US power networks warns intelligence report," *ZDNet*, January 30, 2019, *https://www.zdnet.com/article/cyber-attacks-china-and-russia-can-disrupt-us-power-networks-warns-intelligence-report/*.

[8] 日川佳三，〈為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*。

現升級狀態，目標不僅針對國家、政府機關及關鍵基礎設施，更大的目標乃是破壞敵方的軍事系統。[9] 縱使中國大陸一概否認這些行為，但美國仍感到來自中國大陸的網路威脅具有多面性，最顯著的特徵則是由國家主導網路攻擊，這與普通的網路犯罪不同之處在於，網路攻擊對象通常是針對一些非常具體且重要的戰略性目標。中國大陸的軍事科技有如此迅速的發展，無疑與從美日國防承包商竊取數量驚人的武器設計資料有直接的關聯性。

綜上所述，日本面臨的網路安全問題是複雜且嚴峻的，網路安全防護已成為日本國家安全和社會穩定的重要課題。本研究在探討日本網路安全之發展與啟示，日本針對網路攻擊態勢如何有效掌握？政府單位作了哪些調整與變動？研究結果可使讀者對日本網路安全防護機制有一個總體的認識，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能力提供啟示和借鑒。

貳、文獻回顧與探討

21 世紀的競爭是科技和資訊實力的競爭，資訊化程度的高低直接影響一國的綜合國力和國際地位。隨著資訊技術普及應用和網路發展，資訊安全問題便應運而生，成為非傳統安全領域的新課題。破壞力強、傳播速度更快的駭客攻擊、電腦病毒威脅、日益氾濫的網路犯罪等，使得全球資訊安全形勢更為嚴峻。一直以來人們皆是從技術層面來理解資訊安全，資訊安全就是保障資訊的保密性、完整性、可用性和可控性，其實質就是要保證資訊系統和網路中的資訊免受各種類型的破壞。隨著資訊技術的進

[9] David C. Gompert & Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability,” *Survival*, Vol. 56, No. 4, August-September 2014, pp. 7-22, *http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc*.

步，資訊和網路安全的內涵也不斷發展，人們更多地從綜合層面和廣義角度來理解資訊安全。認為現代的資訊安全包括經濟、政治、科技、軍事、思想文化及社會等各個領域，沒有資訊安全就沒有真正的政治安全、軍事安全和經濟安全，也沒有完全意義上的國家安全。

國家主權的發展，在網際網路時代似乎遇到了瓶頸。然而，基於主權演進的經驗，文化、經濟也非具備固定的實體要件。定義網路空間的國家主權，可以從構成網路空間之資訊平台的角度出發，發展出新的國家主權意涵。學者奈伊（Joseph S. Nye）更將國家因關鍵技術掌握而獲得的權力稱為「資訊權力」，並且表示在未來資訊時代將較傳統所關注的權力來源更為重要。[10] 虛擬空間的範疇比起其他環境更加變化不定，進入的門檻低，造成虛擬空間的權力擴散，權力向非國家行為者與網路中心擴散的趨勢，資訊權力是 21 世紀權力的關鍵面向。資訊革命導致權力擴散，網路創造的虛擬空間縮小了行為者之間的權力歧異，強權無法宰制虛擬領域，為權力擴散提供鮮明例證；然而，權力擴散並不表示權力均等，亦無法剝奪政府身為世界政治最有權力行為者的角色。[11] 因此，資訊革命和全球化為非國家行為者提供了新的權力資源。

詹姆斯（James A. Lewis）指出，由於技術的創新與國家之間缺乏協調，造成網路間諜和網路犯罪的猖獗，而這種不穩定的環境也使得誤解與衝突升高，應當透過制度、規範與法律加以限制。在網路安全改善的同時，政府應思考在網路空間中，國家行為如何能夠被大眾所接受並採納。[12]

---

[10] Joseph S. Nye, "The Information Revolution and Soft Power," *Current History*, No. 113 (2014), pp. 19-22, *https://dash.harvard.edu/bitstream/handle/1/11738398/Nye-InformationRevolution.pdf?sequence=1*.

[11] Joseph S. Nye 著，李靜宜譯，《權力大未來：軍事力、經濟力、網路力、巧實力的全球主導》（臺北：天下文化，2011 年），頁 163-164。

[12] James A. Lewis, "Conflict and Negotiation in Cyberspace," *Center for Strategic and International Studies*, February, 2013, *https://www.csis.org/analysis/conflict-and-negotiation-cyberspace*.

最後提出六個原則，說明了網路空間並非是一個獨特的環境，在網路空間中無法選擇「棄械」（disarm），網路攻擊不會有「全球倖免」（global zero）的情況。阿里斯德（Leigh Armistead）提及資訊力量的本質已產生重大變化，有別於軍事、外交和經濟等傳統力量可由政府掌握，資訊行動已非政府所能影響。易言之，政府已不再能完全控制資訊。阿里斯德在建議事項中指出，美國政府應運用資訊時代的新作戰領域，以最有效的方式因應目前及未來的威脅。[13] 由於關鍵基礎設施的防護屬於資訊行動措施的一部分，而資訊科技的互通有無仰賴於網路空間的便利性，如何確保網路空間的安全勢必成為國家重要目標。

李德（Thomas Rid）強調網路戰爭的弱暴力性和不確定性。[14] 弱暴力性是指一般戰爭行為即存在暴力行為，它以摧毀人身安全為目的，而網路中的戰爭行為是一種不針對任何人身安全行為的戰爭行為，因此它和以往戰爭不同的是，具有弱暴力性；而不確定性是指對客觀世界造成損失的不確定性，網路戰爭以破軟體系統從而間接影響客觀世界，因此在此方面存在不確定性。北約卓越合作網路防禦中心（NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE）自 2009 年開始研議《塔林手冊》（Tallinn Manual），[15] 《塔林手冊》試圖將網路戰之非傳統安全的攻擊行為傳統安全化。北約召集大量的學者、網路、國際法專家進行編撰，宣稱該手冊是符合國際戰爭法規範。姑且不論成效如何，以國際慣例而言，《塔林手冊》極有可能是未來用來參照網路戰適法性的依據。雖然整份手冊只是將概括規範成文，稱不上巨細靡遺，但對於參與編撰的專家學者，針對有異議的部分，會列出不同的觀點或是援引慣例。本研究認為該手冊主要

---

[13] Leigh Armistead，國防部史政編譯局譯，《資訊作戰》(Information Operation Matters)（臺北：國防部史政編譯室，2012 年）。

[14] Thomas Rid, “More Attacks, Less Violence,” *Journal of Strategic Studies*, Vol. 36, No. 1 (February 6, 2013), pp. 139-142.

[15] NATO Cooperative Cyber Defence Centre of Excellence, “Tallinn Manual,” *CCDCOE*, May 23, 2015, *https://ccdcoe.org/tallinn-manual.html*.

是針對國家做出規範，雖然有定義個人或團體的攻擊行為，不過網路本身的匿名性已經讓追查攻擊來源困難重重，遑論還要找到攻擊者本身。《塔林手冊》本身立意良善，但或許是因為考量傳統安全中的行為者—國家，不得不將非傳統安全的網路戰套用在傳統安全的框架之下。

2012 年 4 月 26 日，外務省的資訊安全會議上決定國際法適用於網路空間，因此，網路攻擊可以被視為「武力攻擊」（armed attack）。那麼，行使自衛權即是可能的。2013 年 10 月 23 日安倍晉三在眾議院預算委員會上表示，「當網路攻擊作為武力攻擊的一環時，即可行使自衛權。」[16] 但問題是，什麼樣的網路攻擊等同於武力攻擊？北約卓越合作網路防禦中心（Cooperative Cyber Defense Centre of Excellence, CCDCOE）研議的《塔林手冊》（Tallinn Manual）中明確指出，網路攻擊相當於「國際法戰爭」及「武力攻擊」，但需要從網路攻擊的「規模」及所受到的「影響」來認定。美國國務院法律顧問高洪柱（Harold Hongju Koh）表示：「網路攻擊造成直接死亡、受傷及重大的故意破壞行為，視為武力攻擊，如：1.網路攻擊使核設施遭到熔毀；2.網路攻擊造成水壩潰堤；3.針對航管系統的網路攻擊視為武力攻擊。」[17]

川口貴久在《昨今のサイバー安全保障政策の課題：サイバー攻撃と自衛権》一文中將網路攻擊類型與武力攻擊認定進行分類，認為破壞型攻擊（Destructive attack）工業控制系統的網路攻擊與軍事行動結合的網路攻擊，是較高認定為武力攻擊。[18] 如：2009 年在伊朗所發現的震網（Stuxnet）病毒，是利用西門子（Siemens）製造的工業控制系統存在漏洞，進而感染

---

[16] 衆議院予算委員会，〈予算の執行状況に関する調査〉，《議事録》，2013 年 10 月 23 日，*https://yoshikawasaori.com/html/kokkai/2013/1023_08.pdf*。

[17] Harold Hongju Koh, "International Law in Cyberspace," *USCYBERCOM Inter-Agency Legal Conference*, September 18, 2012, *https://2009-2017.state.gov/s/l/releases/remarks/197924.htm*.

[18] 川口貴久，〈昨今のサイバー安全保障政策の課題：サイバー攻撃と自衛権〉，《グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題》（東京：公益財団法人日本国際問題研究所，2014），頁 2。

資料採集與監控系統（Supervisory Control and Data Acquisition, SCADA），造成伊朗的布什爾（Bushehr）核電廠延遲啟動。如果此事件後續造成物理傷害，並有人死亡的話，這樣就可能被視為武力攻擊；如果僅是單純的經濟損失，認定為武力攻擊的可能性則較低。另外，暫時停止服務之分散式阻斷服務攻擊（DDoS）及竊取型攻擊（Exploitation）較難被認定為武力攻擊，這樣的網路攻擊不能算是立即的「武力攻擊」與「國際法戰爭」，而是屬於「灰色事態」。

飯田將史認為網路攻擊對防衛省安全政策產生重大影響。日本網路防衛隊並不是保護整個國家的網路安全系統，而是只保護自衛隊內部的網路系統。日本今後所要面對的是中國大陸或者北韓發動的大規模網路攻擊，日本應該要有相對應的防禦措施及提升網路攻擊能力。憲法修正與網路安全在廣義上是有關係的，但由於憲法的約束，造成日本的網路攻擊能力非常薄弱，可是面對日新月異的網路攻擊與威脅，日本不可能再視若無睹，日本未來不只會提高網路防禦能力，而是網路防禦及攻擊能力都將會全面提升。[19]

山口昇則是認為若是網路攻擊造成人員死亡，這樣就和武力攻擊沒有什麼差別，在這樣的情況下就可以使用自衛權進行反擊。[20] 但是，網路攻擊較為麻煩的是，很難明確認定攻擊方是誰。小谷哲男表示，憲法並沒有明確條文規定網路空間的部分，目前日本政府非常謹慎的討論網路空間是否能主動發動網路攻擊。[21] 山田敏弘指出，日本政府還未對「網路攻擊」做出明確定義。[22] 對此，防衛省的說法是，由於國際上也還未對網路攻擊作出明確定義，今後日本將針對網路攻擊及自衛範圍積極展開討論。日本應以國際視野，自主獨立地提升該國網路技術能力，並推進法制建制等相關

[19] 古涵詩，當面訪談，飯田將史，防衛省防衛研究所（東京），2017 年 9 月 4 日。
[20] 古涵詩，山口昇，公益財團法人笹川平和財團（東京），2017 年 9 月 27 日。
[21] 古涵詩，當面訪談，小谷哲男，日本國際問題研究（東京）。2017 年 9 月 21 日。
[22] 山田敏弘，〈中露と米欧が主導権を争うサイバー空間の未来〉，《nippon.com》，2015 年 6 月 24 日，*https://www.nippon.com/ja/column/g00288/*。

工作。

土屋大洋（Motohiro, Tsuchiya）指出，2015 年 5 月日本年金機構遭受網路攻擊，導致伺服器內 125 萬筆之個人資料外洩，此事件沒有造成人員傷亡或物理上的破壞，可算是「廣義」的網路攻擊。[23] 不過，網路攻擊者真正的目的，可能不僅於此，有可能從入侵日本年金機構的資訊系統，順藤摸瓜式的侵入政府機關資料庫。因此，網路攻擊者的攻擊態樣可能更深、更廣。由國家築起一座網路屏障，實施網路審查與控管，並不是維護網路安全所應採取的對策。唯有倡議網路的自由開放，才能發揮網路社會的真正價值。最重要的是，培養網路安全人才，並跨越部門障礙，實現資訊共享，並藉著人與人、組織與組織間的協同合作來執行網路安全對策，如此才是日本的解決之道。

川島真表示，一旦發生事關國家安全的網路攻擊時，各省廳能否順利合作存在疑慮，如何克服各省廳「垂直管理」成為一大課題。網路攻擊對日本來說基本上屬於「網路犯罪」，由日本警察廳來處理，而網路防衛隊於則負責 24 小時監視防衛省內部網路系統，但是，警察廳與防衛省兩者並未在網路攻擊與安全防護上進行合作，若兩者能減少本位主義立場，加強合作並交換網路攻擊情資的話，相信更能建構安全、安心與便捷的網路科技社會。[24]

在網路安全人才培育方面，角南篤表示，日本的網路安全人才仍然相當不足。為了解決這個問題，日本政府開始對網路駭客進行招募，經過培訓後，表現優異者可以進入政府機關任職。另外，由文部科學省與經濟產業省聯合推動產官學共同對話機制，讓大學與企業的網路安全合作成為常態，並在 IoT、大數據、機器人及人工智慧等方面增加研發預算，期望建

[23] 土屋大洋，〈年金情報流出とサイバーセキュリティ戦略ー「共有」と「連携」の新戦略〉，《nippon.com》，2015 年 9 月 3 日，*https://www.nippon.com/ja/currents/d00195/*。

[24] 古涵詩，當面訪談，川島真，日本東京大學（東京），2017 年 9 月 14 日。

立吸引及留才的就業環境。[25] 松原實穗子表示，日本政府為迎接 2020 年東京奧運與殘奧會，針對網路安全實施以下措施：（一）政府大量投入人才培育；（二）在網路安全演習上加大力度；（三）更加重視情報共有與分享。[26] 總而言之，2020 年東京奧運會是日本整體提升網路安全的重要契機。

參、日本面臨的網路威脅與案例分析

一、日本面臨的網路威脅類型

2017 年 5 月，日本獨立行政法人情報處理推進機構（独立行政法人情報処理推進機構；Information-technology Promotion Agency, IPA）公布《2017 資訊安全十大威脅》，[27] 以下將對此十大資訊安全威脅闡述如下：

（一）針對性鎖定目標攻擊（Targeted attack）

此種網路攻擊是今日網路環境中對組織最大的威脅之一。[28] 網路攻擊目標鎖定某個政府機關、民間企業或特定團體，攻擊者利用電子郵件裡的附加檔案和網頁外部儲存媒體（external storage），使電腦感染病毒（Virus），此類網路攻擊的最終目的，在於竊取電腦裡高價值的資訊和智慧財產權等重要情報。日本經濟團體聯合會（經團聯）的電腦受到進階持

---

[25] 古涵詩，當面訪談，角南篤，政策研究大學院大學（東京），2017 年 9 月 12 日。

[26] 古涵詩，當面訪談，松原實穗子，Palo Alto Networks（東京），2017 年 10 月 2 日。

[27] 独立行政法人情報処理推進機構，〈情報セキュリティ 10 大脅威─2017〉，《独立行政法人情報処理推進機構》，2017 年 5 月 30 日，頁 46-67，*https://www.ipa.go.jp/security/vuln/10threats2017.html*。

[28] 當網路攻擊滿足三個主要條件時，就可以被認為是針對性攻擊／鎖定目標攻擊（Targeted attack），1.攻擊者有具體目標，顯然花費相當長的時間、資源和精力來設置或進行針對性攻擊/鎖定目標攻擊；2.此攻擊的主要目的是滲透目標網路和竊取伺服器資訊；3.針對性攻擊／鎖定目標攻擊是持久不間斷的，攻擊者花費相當大的努力，確保攻擊在一開始能滲透網路，一旦獲得資料存取權限後，絕非只是進來再出去而已，渠等會希望長期使用此管道越久越好。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.

續性威脅（Advanced Persistent Threat, APT）攻擊。[29] 2016 年 10 月底至 11 月初，經團聯事務局中的 23 台電腦被判斷出有 10 台電腦與外部電腦進行可疑通信。經事後調查發現，網路攻擊者使用惡意軟體「PlugX」（EI Plex）和「Elirks」（Erics）這兩個惡意程式來進行網路攻擊。

（二）透過勒索病毒（Ransomware）向企業或組織勒索高額贖金

勒索病毒是一種特殊的惡意軟體，透過鎖住電腦或智慧型手機，讓人失去對系統或資料的控制權，進而勒索被害人，若要恢復系統或存取資料就必須支付贖金作為交換的犯罪手段。勒索病毒從 2005 至 2006 年間首次在俄羅斯出現，[30] 2012 年勒索病毒從俄羅斯開始擴散到其他歐洲國家，[31] 2013 年「加密勒索病毒」開始浮出檯面，最有名的就是「CryptoLocker」病毒。2015 年發現有 29 個勒索病毒家族，2016 年發現的勒索病毒家族來到 247 個，足足增長 752%。[32] 此種勒索病毒不單將檔案加密，還會在受害者付不出贖金的期間逐批刪除檔案，受害者為了救回檔案還必須支付比特幣（Bitcoin）來換取解密金鑰。[33] 2016 年日本國內偵測出勒索病毒的被害

---

[29] 経団連事務局〈経団連事務局コンピュータのマルウェア感染〉《経団連事務局》，2016 年 11 月 15 日，*http://www.keidanren.or.jp/announce/2016/1115.html*。

[30] The Global Technical Support & R&D Center of TREND MICRO, “Ransomware: Past, Present and Future,” *Trend Micro*, 2017, pp. 2-7, *https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.*

[31] Roland Dela Paz, “Ransomware Attacks Continue to Spread Across Europe,” *Trend Micro*, March 8, 2012, *http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-attacks-continue-to-spread-across-europe/*.

[32] TrendLabs, “A Record Year for Enterprise Threats,” *Trend Micro*, February 28, 2017, *https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2016-roundup-record-year-enterprise-threats.*

[33] 到 2016 年為止，勒索病毒所要求的贖金其實不高，大多在 0.5 至 5 比特幣之間，因為某些變種勒索病毒會隨著時間過去而再提高贖金，第二是比特幣仍不斷在升值，2016 年 1 月，1 比特幣大約值 431 美元。然而 2017 年的匯率卻已經翻了將近三倍，來到 1 比特幣兌換 1,076.44 美元（2017 年 3 月 31 日之匯率）。The Global Technical Support & R&D Center of TREND MICRO, “Ransomware: Past, Present and Future,” *Trend Micro*, 2017, p. 6, *https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf.*

案件數為 6 萬 5 千件，比 2015 年的 6 千 7 百件，高出 9.8 倍之多。[34] 這些案件內文大多是以英文記載，用日文記載的亦有被偵測出來。

（三）漏洞攻擊

此種攻擊為利用網站服務（Web Services）的漏洞竊取個人資料。許多個人資料會註冊在各式各樣的網站裡，如：購物網站或社交網路服務（Social Networking Service, SNS），除了有個人註冊資料外，更記載著親朋好友或其他社群資料，由於社交網站常有大量的資訊分享、外部連結或廣告，無疑為駭客提供更多引誘和犯罪途徑，進而達到網路攻擊或竊取用戶個人資料。由於程式開發過程中的疏失，許多網站都存在安全漏洞，像是資料隱碼（SQL Injection）攻擊和跨網站指令碼（Cross-Site Scripting）攻擊，已成為最好利用的攻擊手法，隨著網站服務的應用程式愈來愈多，網站應用程式漏洞的攻擊相當普遍，也是造成許多重大網路安全事件的原兇之一。案例如：日本電視局網站發生資料存取不當問題，網路攻擊者利用「作業系統命令植入攻擊」（OS Command Injection）突破軟體的安全漏洞，使得高達 43 萬筆的個人資料遭到外洩。[35]

（四）分散式阻斷服務攻擊（Distributed Denial of Service, DDoS）

為「阻斷服務攻擊」（Denial of Service, DoS）的延伸，[36] 主要是利用殭屍網路（Botnet）與系統弱點，對特定目標發送大量合法或偽造連線請求，造成占用大量網路及系統資源，達到癱瘓對方網路，阻斷特定服務及通訊目的。分散式阻斷服務攻擊的目的並非是竊取資料，而是要影響網路

---

[34] トレンドマイクロ株式会社，〈ランサムウェアビジネス」が法人にもたらす深刻な被害〉，《2016 年年間セキュリティラウンドアップ》，2017 年 3 月 2 日，頁 1-4，*https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20170301-01.html*。

[35] 〈日テレに不正アクセス―最大 43 万件の個人情報が漏洩した可能性〉《Security NEXT》，2016 年 4 月 21 日，*http://www.security-next.com/069154*。

[36] 阻斷服務攻擊（Denial of Service, DoS），又稱洪水攻擊，目的在於使目標電腦的頻寬或系統資源耗盡，使服務暫時中斷或停止；分散式阻斷服務攻擊（Distributed Denial of Service, DDoS）是駭客利用網路上 2 台或以上被攻陷的電腦作為攻擊平台，向特定目標發動「阻斷服務」式攻擊。

運作，導致使用者無法存取網路資源，此攻擊會造成企業或政府機關形象受損、用戶信心降低、智慧財產權損失等。近期大型的 DDoS 攻擊大多為混合式攻擊，發動來源以物聯網（Internet of Things, IoT）裝置為主，因為物聯網裝置普遍不具資安防護，對於網路攻擊者來說成本便宜，不需透過網路釣魚（Phishing）取得控制權。[37] 所有物聯網攻擊中 60%起源於亞洲，21%源於歐洲、中東和非洲，19%則來自美洲。[38] 網路攻擊者不僅利用物聯網裝置，還會盡可能尋找不同類型的裝置發動 DDoS 攻擊。2016 年 2 月 19 日，日本國際協力機構（Japan International Cooperation Agency, JICA）、日本信用評級機構（Japan Credit Rating Agency, JCR）、日本住宅金融支援機構（Japan Housing Finance Agency）等官網受到「國際駭客組織」匿名者（Anonymous）的網路攻擊，攻擊理由與日本重啟南極捕鯨活動有關，在官網上提到「捕鯨並非文化特權」，[39] 網路攻擊者為了宣揚特定理念，遂發動網路攻擊。

（五）人為因素

近年來各式各樣雲端服務、新興網路與通訊軟體蓬勃發展，雖然強化了人與人之間的聯繫，但一不小心就可能在彈指間洩漏了公司或政府機關機密文件，包括：重要客戶名單、商業機密等。為了防止內部員工不當行為，除了設立法律規章和懲罰條例對策外，更應建立專業自動化的管控查核機制，這樣才能降低企業在資料管理上的風險。案例如：日本外匯經紀商ワイジェイ FX 株式会社（YJFX）前員工竊取 18 萬件的客戶資料。該

---

[37] 行政院國家資通安全會報技術服務中心，〈資安趨勢與案例宣導〉，《國家資通安全會報技術服務中心》，2017 年 5 月，頁 5-7，*https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1267*。

[38] Dimension Data, "2017 Global Threat Intelligence Report: Cybersecurity insights for protecting your digital business," *Dimension Data*, 2017, *https://www2.dimensiondata.com/microsites/global-threat-intelligence-report.*

[39] 田尻浩規〈JICA などのサイトが閲覧しづらい状態―またアノニマスの DDoS 攻撃か〉，《IT media Inc.》，2016 年 2 月 19 日，*http://www.atmarkit.co.jp/ait/articles/1602/19/news078.html*。

公司離職職員不當攜出公司客戶資料，並將資料放在網路上使第三者能查看，一部分的客戶資料已經被證實遭到閱覽。[40]

（六）水坑式攻擊（Watering Hole）

為最精巧的網路攻擊形式，攻擊者首先滲透完全合法的網站，植入惡意程式碼，接著靜待目標登入該網站，並監控遭滲透網站的活動紀錄。網路攻擊者可以觀察潛在目標使用網路的情況，選擇某些受害者感興趣的網站，這種攻擊技巧在於受害者不會對合法網站存有戒心。[41] 2013 年最受矚目的網路安全事件為 Twitter、Facebook、Apple、Microsoft 等知名網路服務公司受到水坑式網路攻擊。[42] 案例如：日本高松機場的網站首頁遭到竄改，飛機時刻表顯示付款頁面後，網路攻擊者透過一連串文字，引誘客戶連結到指定的外部網站。[43]

（七）非法登入攻擊

遭到非法登錄的案件中多數是使用整合式清單（List-Based Attack）攻擊手法，網路攻擊者利用其他網路服務取得帳號密碼組合，不斷重複登入。為了防範這類身分驗證的網路攻擊，網路服務提供者應善用多因素身分認證（Multi-Factor Authentication, MFA），[44] 如此可以防止非法登入攻擊，妥善保護資料與網路系統。案例如：日本大型連鎖電器行 Big Camera

---

[40] ワイジェイ FX 株式会社（YJFX），〈顧客情報などの持ち出しに対する弊社対応のご報告〉，《YJFX》，2016 年 5 月 31 日，*https://www.yjfx.jp/20160202news/0531release/*。

[41] Symantec, “Internet Security Threat Report 2014,” *Symantec*, April 2016, pp. 34-35, *https://www.certisur.com/sites/default/files/docs/20140411_ISTR_v19.en_us.pdf.*

[42] F-Secure, “Threat Report H1 2013,” *F-Secure*, pp. 11-12, *https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2013.pdf.*

[43] 〈高松空港ＨＰ改竄され閉鎖　不正アクセスか〉，《産経 WEST》，2016 年 8 月 20 日，*http://www.sankei.com/west/news/160820/wst1608200020-n1.html*。

[44] 身分認證（authentication）在資訊安全防護上是一項重要的基本防禦機制。透過一定手段，確認使用者的身分，用以判別身分的因素可分為三種：所知之事（something you know），如：通行密碼、暗號；所持之物（something you have），如：RFID 感應卡、鑰匙；所具之形（something you are），如：指紋（Fingerprint）辨識、臉部辨識。而多因素身分認證（Multi-Factor Authentication, MFA）即使用兩個以上的因素進行驗證，因為要同時具有多個因素難度較高，因此能提高身分認證的安全性。

購物網站，曾發生網路攻擊者進行非法登錄，造成客戶的紅利點數被不當使用。[45] 此外，客戶姓名、地址、電子郵件、購買紀錄等資料已被第三者所閱覽。

（八）透過物聯網裝置發動的網路攻擊

許多連網的裝置就像蟄伏的間諜一樣，直到被攻擊前都不具威脅。隨著越來越多不安全的物聯網裝置，加劇了 DDoS 網路攻擊。通常物聯網裝置的使用說明書上會要求使用者，在首次使用前應先更改帳號、密碼，但使用者可能會覺得變更帳號、密碼手續繁複、操作流程麻煩因此不願重新設定，此時物聯網裝置的安全漏洞就會隨之增加。另外，全球數十億台的物聯網裝置中，約有五十萬台的裝置使用無法變更帳號、密碼的硬式編碼，[46] 使用者想要更改帳號、密碼，也無法自行重新設定。此外，車聯網（Connected Car）的安全漏洞則持續被公開。案例如：網路安全研究人員 Troy Hunt 發現 Nissan Leaf 的電動汽車易受到駭客攻擊，原因是車載系統漏洞，允許駭客遠端操控汽車溫度控制系統，雖然此漏洞不會給車主帶來生命危險，但是駭客能利用此漏洞來耗盡電力，帶給車主不必要的麻煩與損失，問題的根源在於 Nissan Connect 的應用程式，僅需要輸入汽車車輛識別碼（Vehicle Identification Number, VIN）就能遠端控制該車輛。[47]

（九）網路攻擊走向商業化

---

[45] 株式会社ビックカメラ，〈当社インターネットショッピングサイトでの会員ＩＤ、パスワード不正使用被害について〉，《BICCAMERA.COM》，2016 年 3 月 3 日，*https://www.biccamera.com/bc/c/info/report/20160303.jsp?160303*。

[46] Krebs on Security, “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage,” *Krebs on Security*, October 21, 2016, *https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/*.

[47] 鈴木聖子，〈日産「リーフ」のアプリに脆弱性、他人の車を遠隔操作可能に〉，《ITmedia》，2016 年 2 月 25 日，*http://www.itmedia.co.jp/enterprise/articles/1602/25/news067.html*；〈日產 Nissan Leaf 電動汽車漏洞曝光〉，《每日頭條》，2016 年 2 月 25 日，*https://kknews.cc/zh-tw/car/lpl3a2g.html*。

網路犯罪團體在黑市取得的攻擊技術已越來越商業化，像是使用勒索病毒的駭客集團，不但擁有廣泛的技術資源，更能將整個犯罪行為提升到商業服務等級，例如：俄羅斯地下市場聘雇一個駭客發動 DDoS 攻擊，一天花費約 30 到 70 美元一個月約 1,200 美元、入侵特定組織電子郵件 500 美元、植入 2,000 台殭屍電腦（bots）約 200 美元等。[48] 更甚者，有些駭客組織推出各種月付方案，月付 69.99 美元，客戶即可使用 DDoS 攻擊服務。2014 年聖誕節爆發 Sony PSN 及 Xbox Live 遭到 DDoS 攻擊，駭客組織「蜥蜴部隊」（Lizard Squad）聲稱，只是為了展現攻擊實力來達到行銷目的並吸引潛在客戶。[49]

（十）網路金融犯罪

網路銀行的使用日益普遍，網路銀行提供許多便利性和行動性，但安全是許多用戶最大的顧慮。網路攻擊者可以利用病毒和網路釣魚（Phishing）方式，竊取客戶在網銀的認證資訊，進而盜取個人資料或執行任意轉帳等。網路攻擊者使用許多方式竊取客戶網銀資料，如：植入木馬病毒（Trojan Horse）。木馬病毒能攻擊受害者電腦，在電腦上顯示出對話視窗或圖片再假冒成網銀官網，進而要求用戶輸入帳號和密碼。或者，「鍵盤側錄」程式監視客戶使用電腦行為，客戶一旦登入木馬列表中的網銀時，病毒就會開始擷取使用者在鍵盤上輸入的資料，網路攻擊者就能夠竊取用戶的個人資料或執行非法轉帳。根據日本警察廳調查指出，2016 年網路銀行非法轉帳案件為 1,291 件，整體受害金額約 16 億 8,700 萬日圓，個人帳戶的受害金額為 12 億 5,200 萬日圓，公司團體帳戶的受害金額為 4 億 3,500 萬日圓。[50] 網路銀行遭駭客入侵盜領客戶存款事件頻

---

[48] 聞美晴，〈2015 年(ISC)^2 Security Congress 考察紀要〉，《金融聯合徵信》，第 28 期（2016 年 6 月），頁 61-63。

[49] 陳曉莉，〈駭客集團 Lizard Squad 推出 DDOS 服務，攻擊 Sony PSN 與 Xbox Live 只為了展示〉，《iThome》，2014 年 12 月 31 日，*https://www.ithome.com.tw/news/93322*。

[50] 警察庁，〈平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について〉，《警察庁》，2017 年 3 月 23 日，頁 1-2，

傳，顯示出網路金融問題的嚴重性，如滾雪球般越演越烈。

二、三菱重工遭受網路攻擊案例分析

2011 年 9 月 19 日日本媒體報導三菱重工有關製造潛艦、飛彈和核電廠零組件的電腦受到網路攻擊。三菱重工表示，大約有 11 個製造及研發基地，包括三菱重工東京總部、三菱重工旗下神戶造船廠（神戶市）、長崎造船廠（長崎市）、名古屋引導推進系統製作所（愛知縣小牧市）等大約 83 台伺服器和個人電腦受到惡意程式感染。[51] 三菱重工表示，網路攻擊可能是針對專業技術的工業間諜活動，病毒感染地點集中在國防產業和核能研發中心，是針對特定公司和目標的網路攻擊行為。[52] 不僅三菱重工遭到駭客攻擊，日本軍備與機械界頗負盛名的 IHI、[53] 川崎重工等企業亦遭到有目的的伺服器攻擊。IHI 表示從 2009 年 7 月以來，外部有特定人士持續向公司員工發送帶有病毒的電子郵件，由於公司員工沒有打開，因此沒有受到病毒感染。川崎重工也表示，有人向公司多次發送用於網路伺服器攻擊的電子郵件。[54] 因此，可以推測網路攻擊的對象可能是日本防衛產

---

https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf。

[51] 三菱重工東京總部、三菱重工旗下神戶造船廠（神戶市）、長崎造船廠（長崎市）、下關造船廠（山口縣下關市）、相模原工廠（相模原市）、高砂工廠（兵庫縣高砂市）、名古屋冷卻廠（愛知縣清州市）、橫濱研究所（橫濱市）、長崎研究所（長崎市）、名古屋引導推進系統製作所（愛知縣小牧市）、岩塚工廠（名古屋市）等 11 個製造及研發基地，其中神戶造船廠主要建造潛艦，並生產核能發電廠相關零組件；長崎造船廠生產護衛艦；名古屋引導推進系統製作所主要生產飛彈和火箭推進器，請參閱：日本經濟新聞，〈三菱重工にサイバー攻撃　防衛･原発関連など 11 拠点 産業スパイの可能性も〉《日本經濟新聞》，2011 年 9 月 19 日，*https://www.nikkei.com/article/DGXNASDG1900N_Z10C11A9000000/*。

[52] 内閣官房情報セキュリティセンター（NISC），〈情報セキュリティ対策推進会議第３回会合の開催について―官民連携の強化のための分科会の設置等について〉，《内閣官房情報セキュリティセンター》，2011 年 10 月 14 日，*https://www.nisc.go.jp/press/pdf/ciso_3_press.pdf*。

[53] IHI 的全名為 IHI Corporation，位於日本石川縣，主要為防衛省生產戰鬥機引擎、護衛艦和鍋爐等軍工用品，2007 年以前稱為石川島播磨重工業株式會社。

[54] 日本经济新闻，〈ＩＨＩ・川重にもサイバー攻撃、防衛産業狙い撃ち、情報管理、対

業全體。

同年 2011 年 5 月 28 日，美國國防武器承包商洛克希德馬丁公司（Lockheed Martin Corp）也發生網路攻擊情事，駭客首先入侵負責資訊儲存資料 EMC 公司旗下的 RSA 網路安全系統後，複製「Secur ID」金鑰技術，再突破層層網路金鑰，進入與美國國防部合作廠商的網路系統。洛克希德馬丁公司表示，已偵測到資訊系統遭到「明顯且持續」攻擊，但並未發現有任何客戶、程式或員工的資料外洩。[55] 巧合的是，無論是洛克希德馬丁公司還是三菱重工遭駭，皆為 2011 年所發生針對國防承包商的網路攻擊。NSS Labs 資訊安全公司 Rick Moy 表示，入侵 RSA 金鑰系統的駭客，是帶有目標鎖定 RSA 特定客戶，如：政府機關或軍事單位，或者其他擁有重要智慧財產權的企業。澳洲戰略政策研究所（Australian Strategic Policy Institute, ASPI）主任 Andrew Davies 表示：「這可能是日本首起被發現此類的網路攻擊，與美國國防企業遭遇網路攻擊的情況可能有關。由於日本製造大型傳統潛艦擁有全球尖端的技術，這些技術與機械、電子和控制系統的一體化相當完備，因此竊取日本潛艦設計方案對駭客來說相當具有吸引力。」[56]

2011 年 8 月中旬三菱重工發現部分伺服器中毒時，趨勢科技公司先從中毒的伺服器和個人電腦進行分析，在存有核能、國防數據的伺服器裡發現電腦系統有資訊洩漏的情況，其它伺服器資料有被移動過，部分檔案失

策後手に〉，《日本经济新聞》，2011 年 9 月 21 日，*https://messe.nikkei.co.jp/ss/news/92934.html*。

[55] Mike Lennon, “Lockheed Martin Acknowledges ‘Tenacious’ Cyber Attack,” *Security Week*, May 29, 2011, *https://www.securityweek.com/lockheed-martin-acknowledges-tenacious-cyber-attack*.

[56] Jim Finkle, Andrea Shalal-Esa, “Exclusive: Hackers breached U.S. defense contractors,” Reuters, May 28, 2011, *https://www.reuters.com/article/us-usa-defense-hackers/exclusive-hackers-breached-u-s-defense-contractors-idUSTRE74Q6VY20110527*.

竊。總共發現 8 種病毒，[57] 其中包括「特洛伊木馬」病毒，駭客從外部透過電腦操作，窺視電腦螢幕並將資訊送到外面；有病毒從中毒的麥克風裡竊聽對話，藉由隱藏式攝影機進行監視；有的病毒甚至刪除入侵資訊的痕跡，在員工不知情的情況下，駭客透過操控電腦，訪問 14 個外部網站，其中至少有 4 個網站伺服器登記地點位於中國大陸、香港、美國和印度。[58] 雖然三菱重工表示沒有丟失任何機密資訊，但美國仍對此事相當敏感。當時美國駐日大使館發言人 Karen Kelley 表示：「美方關切並持續注意，對於每個國家而言，此類的入侵可能帶來長期負面的影響，因此必須嚴肅看待。這也是為什麼網路安全必須是公私部門密切合作。」[59]

三菱重工於 2011 年 8 月 11 日內部監控系統即發現網路伺服器異常，9 月 19 日在日本讀賣新聞報導下，此事件才曝光。防衛大臣一川保夫於 9 月 20 日命令三菱重工要對此網路攻擊事件進行徹底調查，防衛省於 9 月 21 日對三菱重工表達嚴正抗議，宣稱三菱重工沒有在第一時間內主動向防衛省通報網路攻擊情況，並警告三菱重工，由於沒有提早揭露可能已經違反數十億美元的供應合約。[60] 以下表為三菱重工遭網路攻擊的時間發生序列。

---

[57] 病毒包括：TSPY_DERUSBI.A、TROJ_PIDIEF.EED、BKDR_ZAPCHAST.QZ、BKDR_HUPIG.B、BKDR_HUPIGON.ZXS、BKDR_HUPIGON.ZUY，請參閱 Nart Villeneuve, “Japan, US Defense Industries Among Targeted Entities in Latest Attack,” *Trend Micro*, September 19, 2011, *https://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/.*

[58] 三柳英樹，〈三菱重工を含む防衛産業 8 社が標的型攻撃の被害に、Trend Micro が分析〉，《INTERNET Watch》，2011 年 9 月 20 日，*https://internet.watch.impress.co.jp/docs/news/478766.html*。

[59] Hiroko Tabuchi, “U.S. Expresses Concern About New Cyberattacks in Japan,” *Star News Online*, September 21, 2011, *https://www.starnewsonline.com/news/20110921/us-expresses-concern-about-new-cyberattacks-in-japan.*

[60] Dean Wilson, “Japanese government slams Mitsubishi for not disclosing a cyber attack,” *the INQUIRER*, September 2011, *https://www.theinquirer.net/inquirer/news/2110452/japanese-government-slams-mitsubishi-disclosing-cyber-attack.*

表一 三菱重工遭網路攻擊事件之時間表

時間	內容
2011 年 4 月	川崎重工、IHI 員工表示收到可疑的電子郵件。
2011 年 8 月 11 日	三菱重工內部監控系統檢測到網路伺服器異常。
2011 年 8 月 22 日	三菱重工證實網路伺服器與電腦遭到病毒感染。
2011 年 8 月 27 日	三菱重工要求趨勢科技進行調查。
2011 年 9 月 19 日	・日本讀賣新聞報導三菱重工遭受到網路攻擊。 ・三菱重工下午四點發布新聞稿表示，系統資訊如：IP 位址等可能已經洩露，但機密資訊還在確認。 ・三菱重工向防衛省通報遭受到網路攻擊。
2011 年 9 月 20 日	・日本讀賣新聞報導標題「攻擊三菱重工伺服器，病毒當中包括中文簡體字。」 ・防衛大臣一川保夫表示，三菱重工未有重要機密外洩，並指示三菱重工徹底調查。 ・美國駐日大使館發言人 Karen Kelley 表達針對此三菱重工網路攻擊事件感到擔憂。 ・IHI 和川崎重工發現受到目標式電子郵件攻擊。

	・中國大陸外交部發言人洪磊表示，對於指責中國大陸是網路攻擊發源地的說法表達抗議，否認中方與此事有關。
2011 年 9 月 21 日	・防衛省對三菱重工未盡通報義務表達抗議。 ・日本警察廳證實約有 890 封有關企業的電子郵件遭到網路攻擊。
2011 年 9 月 22 日	網路安全公司趨勢科技發現，遠端操控感染病毒的電腦畫面使用中文，並包含「計算機」和表示伺服器的「主機」等中文用語。
2011 年 9 月 27 日	為了回應該事件，內閣官房長官在新聞記者會上宣佈將召開「資訊安全政策會議」。
2011 年 9 月 30 日	三菱重工表示，已向防衛省報告，截至目前為止，尚未確認產品與重要技術資訊是否洩漏，將繼續與警方配合調查。
2011 年 10 月 7 日	內閣官房長官召開資訊安全政策會議，敦促三菱重工加強網路安全舉措。
2011 年 10 月 14 日	日本警察廳調查，網路攻擊是從日本航空宇宙工業會（SJAC）向川崎重工發送具有針對性的電子郵件攻擊。
2011 年 10 月 24 日	三菱重工表示某些產品與技術數據在伺服器內移動，但無法確認遺失的資料是否為敏感的國防資訊，其中包括日本防衛省訂購的戰機、直升機和其他設備的資訊。

2011 年 11 月 9 日	三菱重工表示未有重要的機敏資訊洩露。

資料來源：三菱重工業株式会社，〈コンピューターウイルス感染に関する調査状況についてーその 1〉，《三菱重工》，2011 年 9 月 30 日，*https://www.mhi.com/jp/notice/notice_110930.html*；三菱重工業株式会社，〈コンピューターウイルス感染に関する調査状況についてーその 2〉，《三菱重工》，2011 年 10 月 24 日，*https://www.mhi.com/jp/notice/1504034_14475.html*；三菱重工業株式会社，〈コンピューターウイルス感染に関する調査状況についてーその 3〉，《三菱重工》，2011 年 11 月 9 日，*https://www.mhi.com/jp/notice/notice_111109.html*。

三菱重工輕忽此次網路攻擊所造成的影響，[61] 三菱重工未即時向防衛省通報，不願對外聲張也不與同業分享網路攻擊情報，以致成為駭客眼中的攻擊目標。日本知名資安顧問 Toshio Nawa 表示：「美國的資安人員一旦發現公司網路系統異常就必須通報；反之，日本的資安人員卻認為，一旦通報就會暴露自己的失職。」[62] 反觀 2011 年 5 月受到網路攻擊的洛克希德馬丁公司，在網路攻擊發生後即向美國聯邦政府報告，[63] 並在一周後發布新聞稿，但三菱重工的反應和通報卻相當延遲，其聲譽嚴重受損。[64] 由於企業基層的資安人員擔憂通報上級可能自身會被懲處，在此認知下，反應出日本企業高階主管普遍不瞭解網路安全的本質，當網路攻擊事件發生時，有必要去探究與追蹤到底什麼樣的資訊會被竊取或網路攻擊者的目的與手段，如此才有正確且有效的網路防護措施。

針對日本三菱重工遭到網路攻擊事件，中國大陸外交部發言人洪磊表

---

[61] Gerry Shih, "Japan its own enemy in push to improve cybersecurity," *Business Insider*, November 2015, *https://www.businessinsider.com/ap-japan-its-own-enemy-in-push-to-improve-cybersecurity-2015-11*.

[62] 松田辰雄，〈標的型攻撃に備えよ：人間のぜい弱性を突いた第一撃を察知するための一方策〉，《海上自衛隊幹部學校》，2014 年 8 月 6 日，*https://www.mod.go.jp/msdf/navcol/SSG/topics-column/col-053.html*。

[63] 名和利男，〈サイバー脅威の背景と実状理解〉，《サイバーディフェンス研究所》，2012 年 5 月，頁 26-28，*https://www.riis.or.jp/symposium/vol.16/nawa_shirahama.pdf*。

[64] 〈三輪信雄氏インタビュー：低いレベルの攻撃に合わせてはダメ、三菱重工のサイバー攻撃から得られる教訓〉，《ビジネス+IT》，2011 年 10 月 17 日，*https://www.sbbit.jp/article/cont1/23983*。

示：「中方否認與此事有關，強調中國大陸也是受害國，聲稱希望與各國積極合作，打擊網路犯罪。」[65] 日本警視廳則認為，此事件為國際性的間諜事件。[66] 美國則是對中國大陸大規模竊取智慧財產權有所批評。美國網路安全公司曼迪恩集團（Mandiant Group）公布《進階持續性威脅 1 號報告》中指出，中國大陸的網路間諜單位進行大量網路攻擊，[67] 共有 20 多個進階持續性威脅團體從事網路間諜活動，這些團體從 2006 年以來，透過設在上海和浦東地區的四個大型網路，入侵 150 個受害單位電腦系統。[68] 共軍 61398 部隊的任務、能力與資源，與此進階持續性威脅團體雷同，且位在同一棟建築物內，並鎖定中國大陸第十二五計畫所列的七大新興戰略產業為目標。[69] 該團體從美國 20 大主要產業中共有 141 個組織和企業有系統地竊取了數百兆位元組的資料。如前文所述，進階持續性威脅主要目的並非破壞系統，而是在竊取資料，盡可能長時間隱藏於目標組織的網路系統中。進階持續性威脅團體在某特定組織中隱藏時間平均高達 365 天，時間最長者高達四年之久。在某個案中發現，進階持續性威脅團體在十個月內竊取某組織 6.5 兆位元的壓縮檔資料，所使用的 937 個指揮管制伺服器，分別設在 13 個國家 849 個不同 IP 位址，其中 709 個 IP 位址設在中國大陸，109 個設在美國。[70] 儘管中國大陸當局多次否認任何從事不法的網

---

[65] 劉詩雨，〈日本最大軍工企業遭駭客襲擊 中共否認網路戰〉，《阿波羅新聞》，2011 年 9 月 21 日，*http://tw.aboluowang.com/2011/0921/219315.html*。

[66] 〈三菱重工サイバー攻撃、中國の反論〉，《Newsweek》，2011 年 9 月 21 日，*https://www.newsweekjapan.jp/stories/world/2011/09/post-2270.php*。

[67] Mandiant Group, "APT-1：Exposing One of China's Cyber Espionage Units," *Mandiant*, February 2013, *https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf*.

[68] Mandiant Group, "M-Trends: The Advanced Persistent Theat," *Mandiant*, January 2010, pp. 21-22, *https://content.fireeye.com/m-trends/rpt-m-trends-2010*.

[69] 中國大陸推動的十二五計畫，聚焦並整合七大領域，並以七大新興戰略產業稱之，分別是：環保節能產業、新一代資訊技術產業、生物產業、高端裝配製造業、新能源、新材料、新能源汽車。

[70] Mandiant Group, "APT-1：Exposing One of China's Cyber Espionage Units," *Mandiant*, February 2013, pp, 3-6,

路間諜活動，但曼德恩集團和其他研究機構皆已蒐集充分證據，讓美國司法部於 2014 年 5 月起訴五名中國大陸籍嫌犯，並指控多項非法網路間諜罪名。[71]

澳洲戰略政策研究所（Australian Strategic Policy Institute）在一份探討中國大陸情報機關能力的專案報告中，列舉出中共情報人員所發動的國際網路攻擊行為。這些網路攻擊個案，與曼德恩集團的報告內容大致相符，亦呼應中共軍委會聯合參謀部副參謀長戚建國中將認為，對於奪取並維持網路空間優勢，比第二次世界大戰中奪取制海權和制空權更為重要。[72]中國大陸的軍事科技有如此迅速的發展，無疑從美日國防承包商竊取武器設計文件有直接的關聯性。中國大陸運用進階持續性威脅網路攻擊，得以獲得相當數兆位元的機密文件。同時，美日國防承包商在網路安全防護能量不足，更凸顯這些國防承包商毫無保護資訊網路系統的能力，進而造成龐大的財務損失。

表二 共軍總參第三部門所進行的網路攻擊行為

時間	內容	產業	網路攻擊類型
2007 年 6 月	五角大廈	政府機關	
2009 年 3 月	英國航太系統集團（BAE Systems）	國防承包商	進階持續性威脅（APT）
2011 年 3 月	RSA 公司	保全公司	魚叉式網路釣魚攻擊

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[71] Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," *The United States Department of Justice*, May 19, 2014, *https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.*

[72] Tobias Feakin, "Enter the Cyber Dragon: Understanding Chinese intelligence agencies cyber capabilities," *Special Report*, Vol. 50, June 5, 2013, pp.5-7.

2011 年 4 月	L-3 通信集團（L-3 Communications）	國防承包商	SecurIDs 毀損
2011 年 5 月	洛克希德馬丁公司（Lockheed Martin）	國防承包商	SecurIDs 毀損
2011 年 5 月	諾斯諾普格魯集團（Northrop Grumman）	國防承包商	SecurIDs 毀損
2011 年 8 月	三菱重工（Mitsubishi Heavy Industries）	國防承包商	進階持續性威脅（APT）
2011 年 10 月	日本外務省及駐外使館 (10 countries	政府機關	進階持續性威脅（APT）
2012 年 1 月	歐洲航空國防與航空公司（EADS）	國防承包商	
2013 年 1 月	紐約時報	媒體業	進階持續性威脅（APT）

資料來源：作者自行整理。

肆、日本網路安全發展與組織調整

日本的網路安全發展是持續演進的。從 2000 年至今，日本的網路安全發展經歷了起始階段（2000-2004 年）、形成階段（2005-2014 年）及升級階段（2015 年至今），主要體現在網路安全相關政策和網路安全體制之變化。

一、起始階段（2000-2004 年）

2000 年 2 月日本內閣官房成立「資訊安全對策推進室」和「資訊安全對策推進會議」，此為日本網路安全發展之起點。2000 年 1 月，日本連續發生數起駭客攻擊中央省廳網頁，[73] 暴露出日本政府在網路安全方面的漏洞。當時首相小淵惠三於 2000 年 2 月 29 日發布命令，在內閣官房的「內閣安全保障和危機管理室」下設立「資訊安全對策推進室」，[74] 作為網路安全政策之執行單位。同日，在「高度情報通信社會推進本部」下設立「資訊安全對策推進會議」，[75] 為日本網路安全政策之制定部門。雖然相繼成立政策及執行單位，但這兩個單位的成立時間過於倉促，形式大於實質，政策的制定與執行缺乏一致性。為改善此種情況，日本在 2001 年 1 月根據《IT 基本法》，[76] 成立「IT 戰略本部」，由首相兼任 IT 戰略本部部長，為全面推動日本的資訊化革命，負責國家 IT 計畫的制定與實施工作。

在此基礎上，有許多階段性措施，主要包括：（一）首次將「網路安全」概念寫入法律。在 2000 年版《IT 基本法》第 22 條中提到「要保護先進資訊和通信網路的安全與可靠」；[77] （二）開始出台許多網路安全相關政策。日本於 2000 年 7 月推出《資訊安全對策指導方針》、[78] 2000 年 12

---

[73] 〈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/*。

[74] 〈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（NISC）》，2000 年 2 月 29 日，*https://www.nisc.go.jp/conference/suisinkaigi/dai1/0229kisoku.html*。

[75] 〈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（NISC）》，2000 年 2 月 29 日，*https://www.nisc.go.jp/conference/suisinkaigi/0229suisinkaigi.html*。

[76] 〈高度情報通信ネットワーク社会形成基本法〉，《電子政府の総合窓口》，2000 年法律第 144 号，*http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000144&openerCode=1*。

[77] 〈高度情報通信ネットワーク社会形成基本法（「IT 基本法」）〉，《首相官邸》，2000 年 11 月 29 日，*https://www.kantei.go.jp/jp/it/kihonhou/pdfs/honbun.pdf*。

[78] 內閣官房（Cabinet Secretariat）在 2000 年 7 月建立《資訊安全對策指導方針》（情報セ

月《關鍵基礎設施網路反恐怖主義特別行動計畫》、[79] 2003 年 10 月《資訊安全綜合戰略》[80] 等網路安全相關政策；（三）在資通訊政策中，均將網路安全列為重要前提。2001 年 1 月公佈《e-Japan 戰略》，強調要保護先進資訊與電信網路的安全與可靠，通過資通訊技術實現高度安全的資訊社會，從根本上強化資訊安全，切實保護個人資訊及提高軟體的安全性與可靠性。[81] 2003 年 7 月 2 日公布之《e-Japan 戰略 II》，[82] 日本進一步強調「開發安全可靠的電信環境」，作為政策優先順序；（四）意識到統籌管理機制的重要性。日本在 2003 年版的《資訊安全綜合戰略》中提到，強化資訊安全不能只強化政府作為，需要有官民合作，對有限的網路安全人才及預算進行合理的分配與管理。」具體而言，需要擴大內閣官房在網路安全方面的權限，使內閣官房可以對網路安全進行整體的規劃與推動。

キュリティポリシーに関するガイドライン），主要發展重點為建立資訊安全管理政策、維持政府安全等級、建立專責的資安機構、發展資安因應對策、建立資安處理程序等，請參閱：内閣サイバーセキュリティセンタ，〈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》，2005 年 7 月 14 日，*http://www.nisc.go.jp/conference/suishin/ciso/pdf/konkyo.pdf*。

[79] 就關鍵基礎設施防護而言，從 2000 年 12 月起，日本就開始著手相關的防護措施。為了防止藉由資通訊網路或資訊系統的網路攻擊，進而影響國民的生計和社會經濟活動，日本「資訊安全對策推進會議」於 2000 年 12 月決議以《關鍵基礎設施網路攻擊對策特別行動計畫》（重要インフラのサイバーテロ対策に係る特別行動計画），作為日本對於關鍵基礎設施資訊安全最起始的施政根據。，請參閱：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》，2000 年 12 月 15 日，*https://www.nisc.go.jp/active/sisaku/2000_1215/1215actionplan.html*。

[80] 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*。

[81] IT 戰略本部，〈e-Japan 戰略〉，《IT 總合戰略本部》，2001 年 1 月 22 日，*https://www.kantei.go.jp/jp/it/network/dai1/pdfs/s5_2.pdf*。

[82] IT 戰略本部，〈e-Japan 戰略 II〉，《IT 總合戰略本部》，2003 年 7 月 2 日，*https://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf*。

二、形成階段（2005-2014 年）

2005 年 5 月，日本決定在 IT 戰略本部下設立「資訊安全政策會議」，替代原來的「資訊安全對策推進會議」；「內閣官房資訊安全中心」（National Information Security Center, NISC）成為「資訊安全政策會議」的事務局。[83] 與起始階段相比，最大的變化在於：（一）將網路安全的問題提升至國家層面來考量；（二）網路安全的主責機關級別升高，權力增強。「資訊安全政策會議」議長從原本內閣官房副長官擔任，改由內閣官房長官直接擔任。同時，「內閣官房資訊安全中心」由內閣官房的二級單位升格為直屬部門，可充分實施管理職能，提高政策制定單位與執行單位間的效率。

除上述組織調整外，日本從政府單位、關鍵基礎設施、企業和個人等方面加強網路安全整備，並制定 2013 年版《網路安全戰略》，內容提到：（一）加強政府單位的網路安全整備。2005 年 12 月 13 日，「資訊安全政策會議」發布《政府機關資訊安全對策統一標準》，[84] 開始統一政府機關的資訊安全標準，於 2011 年 4 月 21 日進一步推出四個標準規範，分別為：《政府機關資訊安全對策統一規範》、《政府機關資訊安全統一管理標準》、《政府機關資訊安全統一技術標準》和《政府機關資訊安全統一管理標準及政府機關統一技術標準制定和實施指南》。特別的是，日本政府於 2008 年 4 月正式啟動「政府機關資訊安全跨部門監視及緊急處理小組」（Government Security Operation Coordination team, GSOC），[85] 開始對政府機關的資通訊網路進行即時監控與分析；（二）加強關鍵基礎設施網

---

[83] 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》，2005 年 4 月 21 日，*https://www.nisc.go.jp/press/pdf/nisc_press.pdf*。

[84] 情報セキュリティ政策会議，〈政府機関の情報セキュリティ対策のための統一基準群（旧版）〉，《内閣サイバーセキュリティセンタ》，2005 年 12 月 13 日，*https://www.nisc.go.jp/conference/seisaku/2005.html#seisaku03*。

[85] 情報セキュリティ政策会議，〈セキュア・ジャパン 2008─情報セキュリティ基盤の強化に向けた集中的な取組み〉，《内閣サイバーセキュリティセンタ》，2008 年 6 月 19 日，*https://www.nisc.go.jp/active/kihon/pdf/sjf_2008.pdf*。

路安全。2005 年 12 月，第一版《關鍵基礎設施資訊安全對策行動計畫》中揭示四大主軸，分別為：安全基準的準備及散布、強化資訊共享體制、相互依賴性解析、跨類別演習，並於各關鍵基礎設施領域下設置「情報分享與分析中心」（Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response, CEPTOAR），作為關鍵基礎設施事業體間的情報共享平台。2009 年 2 月 26 日再創立各 CEPTOAR 間的資訊共享聯絡協議會（CEPTOAR-Council）。2009 年 2 月 3 日「資訊安全政策會議」公布《關鍵基礎設施資訊安全對策第二次行動計畫》，除了延續第一版行動計畫的相關政策外，此版以「因應環境變化」為重點；（三）加強個人對網路安全的重視。2010 年 5 月 11 日，出台《保護國民資訊安全戰略》，該戰略提出要保護日本國民日常生活不可或缺的關鍵基礎設施安全，降低民眾在使用資通訊技術時所面臨的風險。[86]

三、升級階段（2015 年至今）

2015 年 1 月日本設置「網路安全戰略本部」（Cybersecurity Strategic HQs, CSSHQ）及「內閣網路安全中心」（National Center of Incident readiness and Strategy for Cybersecurity, NISC），[87] 並推出 2015 年版《網路安全戰略》。該階段的特色為組織機構升級，「資訊安全政策會議」升格為「網路安全戰略本部」;「內閣官房資訊安全中心」升格為「內閣網路安全中心」，意

[86] 情報セキュリティ政策会議，〈国民を守る情報セキュリティ戦略〉，《内閣サイバーセキュリティセンタ》，2010 年 5 月 11 日，*https://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf*。

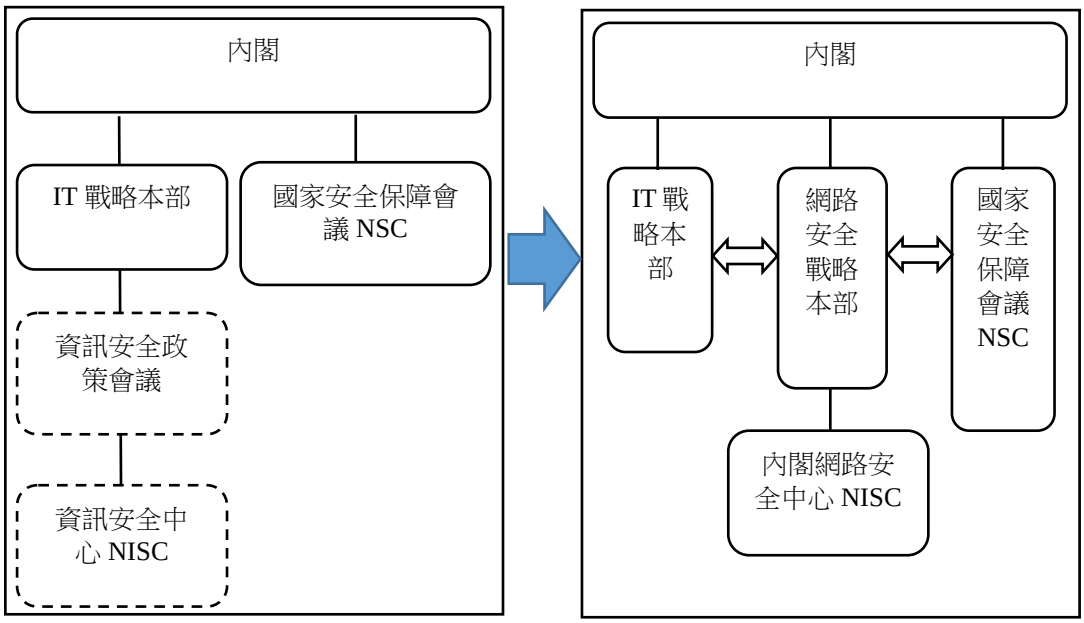
[87] 「內閣網路安全中心」是由「內閣官房資訊安全中心」升格並擴大職權而來。除了資訊安全變成網路安全外，兩者在日語上最重要的變化，是由「內閣官房」轉變為「內閣」，顯示出組織級別與和服務對象的變化，即從內閣官房下屬單位變成內閣直屬機關，過去服務內閣官房長官轉變成直接對日本首相和內閣負責。另外，兩者的英文簡稱雖然都為「NISC」，但英文全稱發生極大變化，「內閣官房資訊安全中心」的英文為「National Information Security Center, NISC」;「內閣網路安全中心」的英文名稱為「National Center of Incident readiness and Strategy for Cybersecurity, NISC」（國家網路安全事件防護和應變中心），後者著重在加強緊急事件的應變及網路系統的恢復能力，其組織內涵已發生深刻變化。

義在於：（一）獲得法律授權。「資訊安全政策會議」沒有獲得明確的法律授權能對政府各部門進行指導，[88] 升格後的「網路安全戰略本部」是根據《網路安全基本法》設立，具有法律授權；[89] （二）職能擴大。「網路安全戰略本部」的任務為：1.制定《網路安全戰略》並推動實施；2.制定網路安全標準措施；3.對網路安全重大事件進行查察；（三）權限提升。《網路安全基本法》第 30 條對行政機關負責人之約束規定。「網路安全戰略本部」做出決定後，相關行政機關的負責人「必須」即時向「網路安全戰略本部」提供資訊及情報，並協助行使職能。該法中強調「必須即時」提供協助，凸顯行政機關的責任與義務；（四）行政級別提升。《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」具有發布行政命令的職能，發布的行政命令稱為「網路安全本部令」。「內閣網路安全中心」（NISC）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，組織升級能促進網路安全對策的落實與執行。

---

[88] 高度情報通信ネットワーク社会推進戦略本部，〈情報セキュリティ政策会議の設置について〉，《内閣官房情報セキュリティセンター》，2005 年 5 月 30 日，*https://www.nisc.go.jp/press/050530seisaku-press.html#b1*。

[89] 日本《網路安全基本法》第 24 條至第 35 條規範「網路安全戰略本部」相關組織及權責事項，如：資料提供等協力義務。請參閱：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，*http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC1000000104&openerCode=1*。



資料來源：作者自行繪製。

圖 1 《網路安全基本法》實施後之組織調整

另外，2015 年出台《網路安全戰略》，與 2013 年版相比，最大的變化有以下四個方面：（一）網路安全議題被納入日本《國家安全保障戰略》中，提高到國家安全層次。[90] 新修訂的《防衛計畫大綱》及《中期防衛力量整備計畫》[91] 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《特定秘密保護法》，該法通過後，可以促進同盟友好國家的重要情報交換與分享，並且得以強化機密情報的保護機制；[92] （四）2015

[90] 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*。

[91] 內閣官房，〈平成 23 年度以降に係る防衛計画の大綱について〉，《防衛省》，2010 年 12 月 17 日，*http://www.mod.go.jp/j/approach/agenda/guideline/2011/taikou.html*。

[92] 〈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/*。

年版《網路安全戰略》的目標及基本原則更加明確。提及要確保資訊自由流通、法治、開放性、自律性及協同合作等五項基本原則。整體而言，2015 年版《網路安全戰略》提出要達成該戰略的目標，其相關措施要更具操作性，從事後應變轉為先發制人、從被動的網路安全防護轉變為積極主動預測、從網路空間朝向融合空間來發展。日本為了解網路攻擊者及攻擊手法，將加強收集網路攻擊資訊，並與國際合作進行國家間的網路威脅資訊共享。

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》提案進行修訂，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》，[93] 修正法案除了設立「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、獨立行政法人及特殊法人的資訊安全監控。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，[94] 此事件促使《網路安全基本法》修法，將日本中央省廳、獨立行政法人及特殊法人的網路系統納入監視範圍。[95] 因此，《網絡安全基本法》公佈以前，各省廳機關採取自律方式對內部的網路系統進行檢測，自《網絡安全基本法》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

[93] 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〉，2017 年 7 月 13 日，頁 2-5，*https://www.nisc.go.jp/conference/cs/dai14/pdf/14shiryou01.pdf*。

[94] 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*。

[95] 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*。

機關發出正式的網路安全建議。日本政府為強化網絡攻擊的防禦對策，於 2018 年 12 月進行《網路安全基本法》修正，決定於 2019 年 4 月 1 日成立「網絡安全協議會」，此協會為因應網路攻擊、官民共用資訊的新組織。協議會由關鍵基礎設施事業體，如：通信、金融、航空、電力、醫療等、政府機關、地方政府、網路安全企業及大學和教育研究單位所組成。當成員企業及會員受到網路攻擊時，「內閣網路安全中心」將收到通報並進行分析，再將分析結果通知會員企業，以防止受害範圍持續擴大。

2018 年 7 月 27 日「網路安全戰略本部」發布 2018 年版《網路安全戰略》，[96] 主要是延續 2015 年版，戰略目標是希望能實現提高日本經濟社會活力與永續發展、實現國民安全且安心生活的社會、維持國際社會和平、安定與保障日本安全。針對以上三大目標簡述重要的網路安全舉措：

（一）提高日本經濟社會活力與永續發展：1.推動可支援創造新價值的網路安全措施。日本政府將與私部門合作，幫助企業高層提高網路安全風險管理意識，並推廣使用網路安全保險，激勵企業進行網路安全投資，進而促進企業利用先進技術支持網路安全業務創新；2.建立可創造價值的網路安全供應鏈。政府與私部門合作，共同制定供應鏈的網路安全框架，使供應鏈中的企業盤點網路安全防護範圍，無論是網通設備、大數據或相關應用服務等；3.官民合作建構安全的物聯網系統。針對物聯網設備脆弱性建立解決方案，透過官民合作，制定涵蓋物聯網設備全生命週期（從設計、製造、應用到廢棄）的網路安全對策。並根據各物聯網設備列出網路安全要求，鼓勵民眾使用符合安全標準的物聯網設備。另外，檢查、識別網路上易受攻擊的物聯網設備機制，透過電信營運商迅速向用戶發出警報。

（二）實現國民安全且安心生活的社會：1.制定網路犯罪因應對策。與

---

[96] 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*。

網路服務業者合作推行「積極的網路防禦」措施，包括利用技術誘導攻擊方式收集網路攻擊者的資訊、促進網路威脅資訊共享利用、與加密貨幣服務提供者合作，建構安心安全的網路空間使用環境。另外，強化打擊網路犯罪措施，包括加強網路犯罪情資掌握、提高取證能力、提高分析惡意軟體的技術能力；2.官民一體共同防護關鍵基礎設施。日本政府將推廣資訊安全標準制定指南，將網路安全措施定位為相關法令規定，透過公私部門聯合演習、共同促進工業控制系統人才開發等，促進關鍵基礎設施業者的網路安全防護能力，並定期更新安全策略指導、開發網路安全人才和預算保證等，增強地方政府的網路安全；3.強化與充實政府機關之網路安全。政府將監控資訊系統、推廣可信賴的雲端服務、利用先進技術，跨組織分析各機關的數據資訊等，致力於提高政府機關的網路安全水準；4.大專院校建構安全與安心的教育和研發環境。政府將根據高等教育與研發環境的多樣性推動網路安全措施，包括制定指導方針促進大專院校自主實施網路安全、促進校際合作共同應對網路攻擊和資訊共享等；5.確保 2020 東京奧運會的安全。日本政府建立「東京奧運會網路安全事件應變小組」（政府オリンピック・パラリンピック CSIRT），目的是希望能促進網路安全風險管理與評估、網路威脅資訊共享等措施，確保東京奧運會之網路安全，並於賽事結束後擴大網路安全的適用範圍；6.強化情資共享與合作體制。日本政府將開發新的資訊共享系統、鼓勵資訊共享誘因，促進各利害關係者安心共享網路安全資訊；7.強化應對大規模網路攻擊事態之能力。包括展開網路攻擊培訓與演習、加強公私部門的網路資訊共享，以及推動網路監控等措施。

（三）維持國際社會和平、安定及保障日本網路安全：1.堅持自由、公平及安全的網路空間。與網路安全業者發展網路安全生態系，並向國際社會傳遞自由、公平及安全的網路空間理念，主張國際法適用於網路空間，並與國外執法單位合作，共同打擊網路犯罪；2.強化日本網路防禦、威懾和

態勢感知能力。**在強化網路防禦方面**，為了確保關鍵基礎設施和其他社會系統所提供的民生服務，需要保護先進技術，並加強防衛省和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，同時，加強蒐集恐怖組織在網路空間中所發布的活動資訊，並與國際社會合作，共同打擊恐怖組織惡意使用網路空間。**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；3.國際合作。利用雙邊對話或國際組織會議，分享網路安全專業知識和威脅資訊，與戰略夥伴國加強網路安全政策協調，透過聯合演訓和培訓，提高網路安全事件響應能力，並協助發展中的國家建構網路安全防護能力。4.跨領域措施。加強網路安全人才開發和保障。政府與產業界、學術界合作，加強管理階層、業務層級及技術人員對網路安全之重視，並促進中小學的師資培訓、學生基礎教育及高等教育網路安全人才開發，並與主要國家建立人才合作機制；促進技術研發。包括設備和軟體安全檢查技術、網路攻擊檢測與防禦技術、加密技術等；培養國民網路安全意識和參與。制定培養日本國民網路安全意識的綜合戰略與行動計畫，建立有效促進各利益相關方的分工協作機制等。

伍、日本網路安全國際合作

日本積極推動網路安全國際合作。2013 年版《網路安全戰略》指出，要以創造「世界領先的網路空間」為目標，並制定網路安全的國際規則。[97] 2013 年 10 月「資訊安全政策會議」公佈《網路安全國際合作方針》，[98] 闡述日本進行網路安全國際合作的方向與領域。該戰略指出，為了強化網路安全國際合作，日本致力建構全球網路安全意識、促進國際間的資訊交流與普及安全技術等，[99] 重點發展項目為：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情報交流；針對網路犯罪調查能力進行培訓，提供各種最新的網路安全趨勢與技術解決方案；並制定相關國際規則、開展雙邊、多邊協商機制與對話。日本的網路安全國際合作有「一個中心」和「三大支柱」。「一個中心」是以歐美等西方國家為中心；「三個支柱」為推動和制訂網路空間國際規則、與各國建立信心措施、建構網路安全防護能力，簡言之，日本以歐美國家的網路安全概念為核心，透過三大支柱來開展網路安全外交。[100] 在此基礎上，日本積極與國際組織、同盟國家和發展中國家進行網路安全合作，以此建構自身的網路安全能力。目前已與美國、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雙邊對話。[101]

---

[97] 情報セキュリティ政策会議，〈サイバーセキュリティ戦略：世界を率先する強靭で活力あるサイバー空間を目指して〉，《内閣サイバーセキュリティ センター（NISC）》，2013 年 6 月 10 日，*https://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf*。

[98] 情報セキュリティ政策会議，〈サイバーセキュリティ国際連携取組方針〉，《内閣サイバーセキュリティ センター（NISC)》，2013 年 10 月 2 日，*http://www.nisc.go.jp/conference/seisaku/dai37/pdf/37shiryou0102.pdf*。

[99] 栗碩，〈日本網絡安全建設析論〉，《國際研究參考》，第 12 期（2015 年），頁 33。

[100] 外務省，〈サイバーセキュリティ日本のサイバー外交〉，《外務省》，2018 年 10 月 25 日，*https://www.mofa.go.jp/mofaj/annai/page5_000250.html*。

[101] 外務省，〈日本のサイバー外交　多国間会議等〉，《外務省》，2018 年 4 月 26 日，*https://www.mofa.go.jp/mofaj/fp/nsp/page24_000686.html*。

2011 年 6 月 21 日「美日安全保障協議委員會」(「2+2」會議）上，網路安全成為美國與日本加強同盟關係的重要內容。美國國防部長蓋茲（Robert Gates）在美日聯合記者會上表示：「美日雙方將加強網路安全合作，進一步擴大美日安保合作新舉措。」[102] 2012 年 4 月 29 至 5 月 2 日，日本首相野田佳彥（Yoshihiko Noda）訪問美國，與美國總統歐巴馬一致認定 2011 年 6 月、2012 年 4 月兩次「2+2」會議上所達成的共識，特別重申網路安全合作對美日同盟的重要性。[103] 2013 年 10 月 3 日「2+2」會議上發表《美日共同聲明》，強調網路安全是美日同盟的新領域，特別是在保密及網路系統裝備上的合作，並將相關合作納入新修訂的《美日防衛合作指針》中，並設立美日網路安全協調機制「美日網路防衛政策工作小組」(Cyber Defense Policy Working Group, CDPWG）共同應對網路威脅。該工作小組是美日網路安全合作的主要平台，[104] 任務是共同研發網路防禦技術並推動網路安全政策、協助日本培育網路安全人才、加強日本自衛隊與美軍的網路防衛合作。此外，美日網路安全合作朝向機制化及常態性發展，共有「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，目的在於透過美日同盟來深化雙方的網路安全合作，包括：協商合作、共享網路安全情資、共同制定推動網路空間國際規則、建立互信機制、共同應對網路威脅及對發展中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。透過以上相關對話機制，達成美日在政治、經濟及軍事上的網路安全合作。

在歐洲地區，日本與歐盟主張共同創造一個開放、安全且可靠的網路

---

[102] 外務省，〈日米安全保障協議委員会（「2+2」）共同記者会見〉，《外務省》，2011 年 6 月 21 日，*https://www.mofa.go.jp/mofaj/area/usa/hosho/kaiken1106.html*。

[103] 外務省，〈日米安全保障協議委員会共同発表〉，《外務省》，2012 年 4 月 27 日，*https://www.mofa.go.jp/mofaj/area/usa/hosho/pdfs/joint_120427_jp.pdf*。

[104] 外務省，〈日米安全保障協議委員会（「2+2」）共同発表ーより力強い同盟とより大きな責任の共有に向けて〉，《外務省》，*https://www.mofa.go.jp/mofaj/files/000016026.pdf*。

空間，同時建立日歐網路對話（EU-Japan Cyber Dialogue），共同打擊網路犯罪、網路恐怖主義、建構網路空間能力等，強調《網路犯罪公約》（Convention on Cybercrime）的重要，持續在「全球網路專業論壇」上（Global Forum for Cyber Expertise, GFCE）對網路安全、資料保護（Data Protection）及電子化治理（E-Governance）等進行相關專業知識交流；[105] 在中東地區，日本與以色列展開網路協議（Dialogue on Cyber issues between Japan and Israel），雙方對於網路安全問題，如：關鍵基礎設施資訊安全防護、網路犯罪、政府體制與戰略、網路空間國際規則與規範進行討論。2017 年 5 月，在以色列訪問的日本經濟產業大臣世耕弘成與以色列簽署網路安全合作備忘錄，日以兩國加強人才培育、聯合演習、專家互訪等。[106] 世耕弘成表示，以色列企業擁有先進的網路安全防禦技術能力與市場運作，加上日本企業擁有強大的執行力，雙方能形成良性的互補關係。2017 年 11 月日本、以色列舉行第三屆網路安全對話，雙方決議在網路防禦與技術革新上加強合作，除了舉行網路攻擊聯合演習外，促成以色列與日本企業搭建合作平台，雙方定期交換網路安全資訊與企業交流；[107] 作為「准同盟」關係的延伸，日本與澳洲在網路安全領域上展開對話，2014 年 4 月日本首相安倍晉三與澳洲總理艾波特（Tony Abbott）舉行會談，會後發布聯合聲明，對於網路安全政策磋商會議達成一致。2015 年 2 月、2016 年 8 月，日澳分別召開第一屆、第二屆日澳網路政策協議（Japan-Australia Cyber Policy Dialogue），[108] 雙方就情報共享、關鍵基礎設施資訊安全防護、建立相互信任措施、打擊網路犯罪、提升網路空間防護能力及共同演習等議題上進

---

[105] 外務省，〈第 3 回日ＥＵサイバー対話 共同ステートメント〉，《外務省》，2018 年 3 月 5 日，*https://www.mofa.go.jp/mofaj/files/000344033.pdf*。

[106] 大治朋子，〈世耕弘成経産相 イスラエル、パレスチナと経済協力拡大へ〉，《每日新聞》，2017 年 5 月 4 日，*https://mainichi.jp/articles/20170504/k00/00m/030/128000c*。

[107] 外務省，〈第 3 回日・イスラエル・サイバー協議〉，《外務省》，2017 年 11 月 29 日，*https://www.mofa.go.jp/mofaj/me_a/me1/il/page23_002331.html*。

[108] 外務省，〈第 2 回日豪サイバー政策協議〉，《外務省》，2016 年 8 月 8 日，*https://www.mofa.go.jp/mofaj/a_o/ocn/au/page4_002218.html*。

行深入探討，並加強區域內網路安全能力建構，強化 2020 年東京奧運會的網路安全合作。

在亞洲地區，日本與印度較早時就展開網路安全對話，2012 年 4 月第六屆日印外長戰略對話於印度召開，兩國外長表示，為了保障網路空間安全使用，將在國際行動規範上進行合作，同年 11 月，第一次日印網路協議（The 1st Meeting of Japan-India Cyber Dialogue）在東京召開，雙方就安全保障領域、打擊網路犯罪、網路安全系統防護及所面臨之相關問題進行探討。直到 2017 年 8 月 17 日，日印舉行第二次網路安全對話，[109] 兩國重申致力於打造一個開放、安全的網路空間，並探討網路安全對策、所面臨的網路威脅，一致認為，現有《國際法》普遍適用於網路空間；東南亞地區，日本與東協（ASEAN）展開網路安全合作，2013 年 9 月「日本—東協關於網路安全合作之部長級政策會議」（ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation）在東京召開，[110] 這是雙方首次就網路安全問題舉行部長級會議。會後雙方發表共同聲明，表示將把合作重心放在構築安全放心之商業環境與通訊網路上，並且提出多項具體實施計畫。另外，2014 年 11 月，「日本—東協元首高峰會」在緬甸首都內比都召開，會後日本與東協各國元首共同發表了《日本—東協打擊恐怖主義和跨國犯罪聯合宣言》，[111] 日本與東協首次將網路安全議題提升到國家元首級別，聲明內容包括雙方將建立網路犯罪資訊共享機制、強化執法單位合作，並且與「國際刑警全球綜合性創新總部」（Intelpol Global Complex for Innovation，IGCI）共同發展基礎與進階網路犯罪調查能力培訓計畫，預測

---

[109] 外務省，〈第 2 回日インド・サイバー協議の開催（共同プレスリリースの発出）〉，《外務省》，2017 年 8 月 18 日，*https://www.mofa.go.jp/mofaj/press/release/press4_004917.html*。

[110] Prime Minister of Japan and His Cabinet, "ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation," *Prime Minister of Japan and His Cabinet*, September 12, 2013, *https://japan.kantei.go.jp/96_abe/actions/201309/12asean_e.html*.

[111] 外務省，〈テロ及び国境を越える犯罪と闘う協力のための日 ASEAN 共同宣言〉，《外務省》，2014 年 11 月 12 日，*https://www.mofa.go.jp/mofaj/files/000059327.pdf*。

及打擊國際化的網路犯罪趨勢。以上綜整可知，日本在網路安全國際合作方面，累積了豐富經驗。以下表為日本網路安全國際合作與雙邊對話。

表三 日本參與網路安全國際會議與雙邊對話

會議名稱
G7 伊勢志摩網路集團第一次會議（G7「伊勢志摩サイバーグループ（Ise-Shima Cyber Group, ISCG）」第 1 回会合）
海牙網路空間會議（サイバー空間に関するハーグ会議）
首爾網路空間會議（サイバー空間に関するソウル会議）
布達佩斯網路空間會議（サイバー空間に関するブダペスト会議）
倫敦網路空間會議（サイバー空間に関するロンドン会議）
日本─愛沙尼亞網路協議（日・エストニアサイバー協議の開催）
日歐網路對話（日 EU サイバー対話の開催）
日俄網路協議（日露サイバー協議）
日韓網路協議（日韓サイバー協議）
日英網路協議（日英サイバー協議の開催）
日德網路協議（日独サイバー協議）
日澳網路政策協議（日豪サイバー政策協議）
美日網路安全對話（日米サイバー対話の開催）
日本─以色列網路協議（日イスラエル・サイバー協議）
中日韓網路協議（日中韓サイバー協議）
日法網路協議（日英サイバー協議の開催）
日印網路協議（日インド・サイバー協議）

資料來源：作者自行整理。

陸、結論

網路空間使國家利益的邊界得以延伸和擴展。網際網路日益成為國家安全、政治、經濟、文化和社會發展的重要命脈。基於對網路安全的認識與需要，日本提出要建構「世界領先的、堅強的、充滿活力的」的網路空間。2014 年日本公布《網路安全基本法》，其目的為擬定全國性的網路安全對策，明確中央與地方政府的職責，主要確立「網路安全戰略本部」為負責網路安全的專責機關，其核心任務包括：制定《網路安全戰略》、制定網路安全標準措施、對網路安全重大事件進行查察，並與「國家安全保障會議」（NSC）及「IT 戰略本部」緊密聯繫與合作。同時，將隸屬於 IT 戰略本部下的「內閣官房資訊安全中心」調整為「內閣網路安全中心」，該中心為「網路安全戰略本部」事務局，負責政策具體落實與執行，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。以上組織調整的目的在於增強網路安全主責機關的監督權限，提高政策制定與執行單位間的效率。

從《網路安全戰略》可看出日本政府施行「積極網路防禦」戰略，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「事後因應轉變為事前防禦」、被動轉變為主動態勢；2018 年版《網路安全戰略》明確指出，為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搜集攻擊者的背景及相關資訊，進而增進威脅資訊共同使用。此外，要提高網路威懾力，日本《網路安全戰略》以美日同盟為基礎，日本認為美日同盟應遵循美國在網路空間推行網路威懾戰略。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。以上呼應 2018 年 12 月公佈新版《防衛計畫大綱》，強調自衛隊需具備「網路反擊能力」。

網路空間成為影響國家安全的重要因素，日本除了強化自身網路安全防護能力，更將網路空間納入美日同盟的合作範圍。所謂的網路安全國際

合作，其基礎仍然是美日安保體制，美日將軍事合作擴及到網路空間與太空，並針對網路威脅資訊進行共享，共同監視和實施網路安全聯合演習等，透過相關知識及技術上的交流，共同因應網路威脅。除此之外，日本更致力於建構全球網路安全意識、促進國際間資訊交流、普及安全技術等。除了建構應對網路攻擊事件的全球動態體制外，更加強與各國調查機關的情報交流，針對網路犯罪調查能力進行培訓，並提供各種最新的網路安全趨勢與技術解決方案，此外，制定相關國際規則並展開雙邊、多邊的網路安全協商機制與對話。由此可見，日本除了增加自身在網路空間的話語權外，更聯合其他國家積極建構應對網路攻擊的全球動態體制。總體來說，日本在面臨網路威脅時，積極運用網路安全外交，以強化溝通、增進國際合作等概念來處理網路安全議題。

日本有國家級的網路安全戰略方針，訂定網路安全產業發展方向，我國國家安全會議國家資通安全辦公室於 2018 年 9 月發布《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」之政策，亦具備國家級的政策規劃，不過需要再將整體的推動方向和範圍明確加以宣導，讓各界清楚部會相關權責。為發揮國家整體的網路安全政策，各政府單位應落實分級管理政策，設置緊急應變小組，加強內部網路安全策略與跨部會協調合作，並進行策略執行前後的績效評估。對於國家層級的網路攻擊，我國亦應培養應變能力，建議可擴大民間參與，延攬白帽駭客協助進行滲透測試、弱點掃描，甚至編組紅隊攻擊，提高政府機關的網路安全強度與防護能力。另外，由於網路攻擊無國界，單一國家難以應付層出不窮的駭客攻擊，因此網路安全需要國際聯防。在應對中國大陸所發動的網路攻擊中，台灣可透過美日的網路安全合作框架增強自身的角色，在網路安全方面推動三邊合作，台、日在網路安全方面應投入更多資源，以便未來與美國在網路安全事務上展開全面的合作關係。為此，台美日可在以下領域上進一步合作：一、在定義和實施網路空間集體防衛方面

達成共識；二、建立網路威脅資訊共享機制，共同研發網路防禦技術；三、發展健全且實用的聯合訓練和演習；四、擴大民用關鍵基礎設施網路安全防護及反間諜活動；五、建構台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。

責任編輯：劉冠彤