2017 年度 公益財団法人日本台湾交流協会フェローシップ事業成果報告書

日本網路安全之發展與啟示

国立中山大学 中国與亞太区域研究所
古涵詩
招聘期間（2017 年 7 月 31 日～9 月 28 日）
2018 年
公益財団法人日本台湾交流協会

日本網路安全之發展與啟示*

古涵詩

（中山大學中國與亞太區域研究所博士候選人）

摘要

日本的網路安全政策目標為確保一個自由、公平與安全的網路空間。除了制定《網路安全基本法》之外，內閣網路安全戰略本部明訂需要藉由產、官、學合作，共同提升國家社會的網路安全防護能力。此外，日本政府為了提升國家的競爭力與維持社會的穩定發展，將著重改善網路商業環境、強化資訊系統的防護能力、增加網路安全教育、與各國合作培育世界級的網路安全人才等。本文將探討日本網路安全之組織架構、網路安全政策之發展歷程、相關政策分析並總結日本網路安全發展之啟示，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

* 感謝日本台灣交流協會慨予獎助本研究計畫經費，感謝中山大學中國與亞太區域研究所林教授文程及郭副教授育仁的不吝指導，並感謝受訪之專家學者慷慨提供各種知識與情感上的支持，於此一併致謝。

The Development and Enlightenment of Japan's Cybersecurity

Han-Shih Ku

Ph.D. Student, Institute of China and Asia-Pacific Studies, NSYSU

Abstract

The Japanese government has developed a target of cybersecurity strategy on a free, fair, secure network space. Except for Basic Act on Cybersecurity, Cybersecurity Strategic Headquarter expressly promotes projects and action programmes to enhance the national and social cybersecurity defensive capabilities through cooperation of industry-government. Moreover, the government emphasizes on the improvement of business cybersecurity environments, strengthens defensive capabilities of information systems, advances cybersecurity education, and works with other countries to develop world-class cybersecurity human resources in order to promote national competitiveness and maintain national security and social stability. This research explores the evolution of Japan's cybersecurity strategy, relates to Japanese strategic analyses, and discusses construction of its network security organizations. In conclusion, the characters of the Japanese cybersecurity strategy provide us with references on Taiwan's development of cybersecurity strategy.

Keywords: Network security, Cybersecurity strategy, Basic Act on Cybersecurity, Cybersecurity Strategic Headquarter, Key infrastructure

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。[1]

常見的網路安全威脅有：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，為了竊取個人隱私資料，與犯罪集團合作進行金融詐騙，例如：2011 年 4 月，日本 Sony PSN（PlayStation Network）網路帳戶遭駭客入侵，導致將近 8,000 萬筆個資外洩；[2]二、關鍵基礎設施（Critical Infrastructure, CI）遭受破壞，勢必影響經濟、民生及整個政府運作，例如：2011 年 3 月 11 日東日本大地震，日本在關鍵基礎設施之核能、電力、糧食、飲水設施防護及政府危機處理能力方面，都受到嚴厲考驗與挑戰；[3]三、進階持續性威脅（Advanced Persistent Threat, APT）[4]增加，由於 APT 的攻擊特徵為針對特定目標、低調、隱匿、手法多元、客製化等，日本、台灣及美國是遭受 APT 攻擊最為嚴重的國家。[5]

日本作為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。[6]在此之前，開發網路攻

---

[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 >。

[2] 黃彥棻，〈索尼影業遭駭事件始末大剖析〉，《iThome》，2015 年 1 月 9 日，<http://www.ithome.com.tw/news/93457 >。

[3] 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 >。

[4] 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，透過歲到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.

[5] 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》，<http://www.ringline.com.tw/zh-tw/article_info.php?id=78 >。

[6] 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/>。

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！」因為日本的企業富於創新，並且擁有豐富的智慧財產權，因此成了網路攻擊的重要目標。根據該公司的調查報告，惡意軟體的回呼（Callback）[7]通信對象，日本高達 87%，遠遠高於不到 47%的美國。[8]

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，現今國防承包商已成為駭客的主要攻擊目標之一。[9]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。[10]日本宇宙航空研究開發機構（JAXA）於 2013 年 4 月 23 日宣稱，檢測到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。[11]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？政府組織作了哪些調整與變動？不同時期的網路安全發展如何轉變？推動的成效與影響是什麼？研究結果可使讀者對日本網路安全有一個總體的認識，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、相關文獻回顧

一、何謂網路安全？

由於網路安全（cyber security）具有多種不同面向的複雜問題，因此，並沒有一個明確、精準且全球公認的定義。美國國家安全系統委員會（Committee on National Security Systems, CNSS）對網路安全的定義是：「保護或防止網路空間在

[7] 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。

[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 >。

[9] 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>。

[10] 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>。

[11] 〈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 >。

使用上不受網路攻擊的能力。」[12]而「網路空間」的定義則為：「資訊系統基礎設施網路所構成之資訊環境內的一個全球性領域，該網路包含網際網路、電信網路、電腦系統、內建處理器及控制器。」[13]聯合國負責資訊與通信科技的專門機構「國際電信聯盟」(International Telecommunication Union, ITU)在2008年4月針對網路、數據與電信安全的建議事項中，針對網路安全作出以下定義：「網路安全是可以用於保護網路環境、組織和使用者資產的所有工具、政策、安全概念、安全保障措施、指導方針、風險管理方式、行為、訓練、最佳作法、防護手段和技術。組織與使用者資產包含連結之計算裝置、人員、基礎設施、應用程式、服務、電信系統和所有網路環境中傳遞或儲存之資訊。網路安全則致力於確保組織和使用者資產，皆能建立並保持防止網路環境中相關安全風險之安全特質。一般性安全目標包含以下各項：可使用性、整體性(包含身分驗證和無可否認證明)、保密性。」[14]薩托拉（David Satola）和茱蒂（Henry Judy）指出，網路安全概念「會隨著不同管轄權可用的實體、教育和經濟資源而有所差異。其差別依所需保護之資料敏感性而有所不同，而且必須反應不同文化期望和優先順序，以及諸多其他因素。」[15]

日本政府則將網路安全（サイバーセキュリティ）定義為：「為了防止無法被自然人感官知覺之電子、電磁方式所發送、傳送，或對接收的資訊出現洩漏、滅失或毀損等情形，與其他為確保此類資訊之安全管理，及確保資訊系統與網路通訊環境之安全性與信賴性的必要措施。」[16]中國大陸學者俞曉秋認為資訊安全重在資訊本身，即資訊的處理、製作、獲得、傳播、交換、應用、儲存等方面的安全；網路安全則重在網路，即生產控制、公共服務、資訊傳播以及數據系統平台及網路基礎設施的安全。[17]

臺灣學者彭慧鸞指出，「數位安全」基本上涵蓋了國家安全層次的「網絡安全」(Network security)以及以網際網路為核心的「網路安全」。至於「網路安全」的意涵，可以引用 2003 年聯合國資訊社會高峰會（World Summit on the Information Society, WSIS）總結報告曾對網路安全作出範圍的界定，「凡在一國之內受到來自境外電腦病毒、木馬程式等病毒碼破壞網路系統，造成網路或資料

---

[12] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015, pp. 45, <https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf >.

[13] Committee on National Security Systems, "National Information Assurance (IA) glossary," April 2010, <https://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf>.

[14] International Telecommunication Union, "Overview of cybersecurity," *ITU-T X.1205*, April 2008, <http://www.itu.int/itu-t/recommendations/index.aspx?ser=X>.

[15] David Satola & Henry Judy, "Electronic Commerce Law: Toward a dynamic approach to enhancing international cooperation and collaboration in cybersecurity legal frameworks: reflections on the proceedings of the workshop on cybersecurity legal issues at the 2010 United Nations Internet Governance Forum," *William Mitchell Law Review*, Vol. 37, No. 1745, September 3, 2010, pp. 141.

[16] 《サイバーセキュリティ基本法》（平成 28 年 4 月 22 日法律第 31 號）第 2 條，<http://law.e-gov.go.jp/htmldata/H26/H26HO104.html>。

[17] 俞曉秋，〈信息安全與網絡安全辨析〉，《中國信息安全》，第 8 期，2014 年 8 月，頁 111-112。

上的破壞，則稱之為網路安全。」[18]因此，網路安全只是網絡安全中的一環。[19]梁德昭及朱治平指出，美國與中國大陸面臨網路安全問題之最大差異在於，雙方對網路空間認知的差異，美國試圖確保在網路空間行動自由之餘，亦可繼續擁有對國際網路空間之控制權；中國大陸則是確認網路空間與國家主權的關係。換言之，中國大陸在確定網路空間的主權歸屬時，相關公共政策問題的決策權屬於國家主權。此外，對於美中雙方而言，美國的網路安全利益主要聚焦在關鍵基礎設施、網路空間自由及商業機密的網路安全；中國大陸的網路安全利益則關注在政治社會穩定、資訊基礎設施及網路資訊與數據安全，雙方所關切的安全利益有所不同。[20]

二、網路戰爭

在網路戰爭方面，W. Alexander Vacca在《Military Culture and Cyber security》一文中，以美國所關注的新戰爭疆域—網路空間之無政府狀態說起，以認知心理學的角度，闡釋軍事文化對網路新戰場疆域形成的影響與作用。[21]Thomas Rid在其著作《More Attacks, Less Violence》中強調網路戰爭的弱暴力性和不確定性，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，網路戰爭以破壞軟體系統，從而間接影響客觀世界，因此在此方面存在不確定性。[22]

有學者從網路戰爭事件進行網路戰的分析，如《Cyclones in Cyberspace Information Shaping and Denial in the 2008 Russia–Georgia War》一文探討2007年愛沙尼亞（Estonia）與2008年喬治亞（Georgia）的政府網站遭受疑似俄羅斯官方的攻擊，[23]此事件促使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）。[24]《塔林手冊》的全稱是《適用於網路戰爭的塔林國際法手冊》（Tallinn

---

[18] WSIS Executive Secretariat, “Report of the Geneva Phase of the Summit on the Information Society” Document WSIS-03/GENEVA/9(Rev.)-E, 18 February, 2004, <http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1532|1191>.

[19] 彭慧鸞，〈數位時代的國家安全與全球治理〉，《問題與研究》，第 43 卷第 6 期，2004 年 11、12 月，頁 32。

[20] 朱治平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 17 卷第 2 期，2016 年 4 月，頁 8-9。

[21] W. Alexander Vacca, “Military culture and cyber security,” S*urvival,* Vol. 53, No. 6, December 1, 2011, pp. 159-176.

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

[23] Ronald J. Deibert, Rafal Rohozinski, Masashi Crete-Nishihata, “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war,” *Security Dialogue,* Vol. 43, No. 1 , February 15, 2012, pp. 3-24.

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

Manual on the International Law Applicable to Cyber Warfare），總編輯施密特（Michael N. Schmitt）強調，編纂手冊的國際專家小組是獨立的學術組織。《塔林手冊》的基本立場是：現有國際法規範完全可以適用於「網路戰爭」，國際社會無需創制新的國際法規範以管轄網路行為。[25]國際專家小組宣稱《塔林手冊》詳盡地參照了現行國際條約、國際慣例、被文明國家公認的一般法律原則、司法判決等廣義的國際法淵源。但作者認為該手冊主要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爭套用在傳統安全的框架之下。

理查・克拉克（Richard A. Clarke）、羅伯・柯納克（Robert K. Knake）所編著《網路戰爭：下一個國安威脅及因應之道》（Cyber War: The Next to National Security and What to Do About It），作者指出網路方面之政策急迫性，並提出警告，隨著大規模網路攻擊的可能性提高，網路911事件在可預見的未來可能會發生，政府應儘速通過網路安全相關的立法措施。此外，作者在對網路武器併入軍事規劃層面的論述、對各國秘密進行網路軍備競賽的說明，以及對美國網路安全在私部門基礎設施脆弱性的評估，均有精闢的分析。[26]最後在議題探討部分提出六個值得關注的議題：（一）思考網路戰爭看不見的層面。（二）防禦鐵三角概念。（三）網路犯罪。（四）網路戰爭限制條約。（五）研究更多保障網路安全的設計。（六）總統的介入。

阿里斯德（Leigh Armistead）編著的《資訊作戰》（Information Operation Matters），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控，易言之，政府已不再能完全控制資訊。在第四章「資訊行動近期變革」中則仔細檢討了美國近期資訊行動政策和組織變革，包含911事件前對美國關鍵基礎設施防護政策與事件後的影響。此外，作者在建議事項中指出，美國政府應運用資訊時代的新作戰領域，以最有效方式因應目前及未來所面臨之網路安全威脅。[27]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，如何確保網路空間安全勢必成為國家的重要目標之一。

與此同時，有學者認為網路戰爭爆發的可能性逐漸降低，甚至沒有可能，如：Adam P. Liff 在《Cyberwar: A New Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War》文中認為隨著網路戰爭能力的減弱，

---

[25] Oliver Kessler and Wouter Werner, "Expertise, Uncertainty and International Law: A Study of the Tallinn Manual on Cyber Warfare," *Leiden Journal of International Law*, Vol.26, No. 4 , 2013, pp.793-810.

[26] Richard A. Clarke, Robert K. Knake 著，王文勇譯，《網路戰爭:下一個國安威脅及因應之道》(Cyber War: The Next to National Security and What to Do About It)（臺北：國防部史政編譯室，2014 年）。

[27] 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）。

網路戰爭爆發的可能性越來越小，但是網路攻擊可能會變得越來越頻繁。[28]Thomas Rid在另一篇文章《Cyber War Will Not Take Place》中也認為網路戰爭不可能爆發，他從網路戰爭必備的要素談起，認為潛在的致命性、可操作性、具有政治意義上強制行動的惡意程式是構成網路戰爭必備的三大要素。[29]接下來他又從許多事件上說明網路攻擊不等於網路戰爭，因此他所得出的結論是網路戰爭不會爆發。

三、網路安全治理

在《Cyber-attacks and International Law》一文以國家安全層面探討網路攻擊的危害，並指出網路攻擊缺乏有效的國際法規範，如何在國際間制訂國際法原則，加以約束網路攻擊仍有相當大的難度。[30]Jeff J. McNeil的博士學位論文《Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem》，針對網路攻擊無法確定、網路安全難於監管等情況下，想要有效應對網路攻擊、維護網路安全，國際間的合作勢在必行。[31]Eneken Tikk在《Ten Rules for Cyber Security》一文中，[32]針對網路攻擊問題日益嚴重，尤其在愛沙尼亞網路攻擊事件出現之後，提出十條有關網路安全國際合作的原則。

美國智庫戰略暨國際研究中心（Center for Strategic and International Studies, CSIS）資深研究員詹姆斯（James A. Lewis），於2013年2月發表的《網路空間的衝突與談判》（Conflict and Negotiation in Cyberspace），報告著重於網路安全的政治軍事方面，並試圖置於國際安全的背景之下。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日益猖獗，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，而在網路安全改善的同時，政府應思考在網路空間中，國家行為如何能被社會大眾所接受並採納。作者最後提出六個原則，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

---

[28] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyber warfare Capabilities and Interstate War," *The Journal of Strategic Studies*, Vol. 35, No. 3, June 2012, pp. 401-428, <http://indianstrategicknowledgeonline.com/web/Proliferation%20of%20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf >.

[29] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, October 5, 2012, pp. 5-32.

[30] G. Grove, S. Goodman & S. Lukasik, "Cyber-attacks and International Law," *Survival*, Vol. 42, No. 3, December 7, 2010, pp. 89-103.

[31] McNeil, Jeff J., *Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem* (Ph. D. diss., Old Dominion University, USA, 2010), pp. 1-10.

[32] Eneken Tikk, "Ten Rules for Cyber Security," *Survival*, Vol. 53, No. 3 , June/July 2011, pp. 119-132, <http://citizenlab.org/cybernorms2011/rules.pdf>.

械」（disarm），網路攻擊不會有「全球倖免」（global zero）的情況。[33]

Robert J. Domanski的博士論文《Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace》一文，針對網際網路的絕對自由提出質疑，並提出當前網路仍處於政府管理之下，並且隨著時間的推移，政府將加強網際網路的監管。[34]作者在文中針對網際網路大眾—個人的特點提出四層的分析框架，以便政府加強網路政策監督與管理，妥善處理國家網路安全與個人隱私權的問題。

四、網路安全之主權與邊界

Kristell G. Havens的碩士論文《Borders Without Boundaries: Analysis of Cyber Security Policy and Changing Notions of Sovereignty》[35]首先探討國家主權的內涵，國家主權會隨著歷史、主體的可變更性及行使的範圍而演變。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、經濟也並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。而學者Joseph S. Nye更將國家因掌握關鍵技術而獲得的權力稱為「資訊權力」，並且表示「資訊權力」較傳統所關注的權力更為重要。[36]虛擬空間的範疇比起其他環境更加變化不定，虛擬空間可以靠著開關電源這個動作而打開或關上，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，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。[37]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。

從美國國家安全研究網路安全議題，比較有代表性的如Michael Chertoff在

---

[33] 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>.

[34] Robert J. Domanski, *Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace*, (Ph. D. diss., The City University of New York, 2013), pp. 1-30, <http://academicworks.cuny.edu/cgi/viewcontent.cgi?article=2512&context=gc_etds>.

[35] Kristell G. Havens, *Borders Without Boundaries: Analysis of Cyber Security Policy and Changing Notions of Sovereignty*, (Master's thesis., Utica College, 2014), pp. 1-12, <file:///C:/Users/C640/Dropbox/%E7%B6%B2%E8%B7%AF%E5%8F%B8%E4%BB%A4%E9%83%A8/%E5%8F%83%E8%80%83%E6%96%87%E7%8D%BB20170223/Borders%20Without%20Boundaries.pdf>.

[36] 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>.

[37] 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。

《Homeland Security Assessing the First Five Years》[38]一書中提到網路安全，並分析網路安全的脆弱性，由於控制領域分散、擁有分散、受益分散、用戶分散，這些分散導致網路攻擊對國家網路安全造成嚴重威脅。文中最後指出由於網路涉及公共與私人領域，想要有效解決網路安全問題，需要政府、企業、地方及個人共同配合。Bridgette Braxton在《Critical Infrastructure Protection》[39]一文中界定關鍵基礎設施，分析當前全球關鍵基礎設施網路安全的脆弱性，並指出脆弱性的原因所在，文中最後指出唯有保護這些關鍵基礎設施與國際合作，才能有效解決網路安全的問題。

此外，還有其他課題也涉及網路安全領域。Ian Bremmer在其著作《Democracy in Cyberspace: What Information Technology Can and Cannot Do》[40]中分析中美對網路空間的自由持不同的態度，因此實施不同的網路民主政策，並以客觀中立的視角得出結論：每個國家所採取的戰略與政策符合本國政府和人民的價值取向。Jacob A. Mauslein的博士論文《Three Essays on International Cyber Threats: Target Nation Characteristics, International Rivalry, and Asymmetric Information Exchange》[41]則是探討1999年到2011年之間的網路安全威脅，通過數理統計方法，分別探討政治、經濟、社會等傳統因素、國際競爭以及國際談判理論與網路威脅的關係。

Joseph House在《Internet Censorship in China》一文中，針對中國大陸網路審查制度進行研究與探討，[42]文章中有別於主流的觀點，認為中國大陸其實並沒有實施最為嚴格的網路審查制度，從歷史、政治手段、參與者等三方面進行研究，得出中國大陸政府通過監管系統來控制網路的發展。值得注意的是，中國大陸政府對於這種監管已經非常熟練，最後告誡企圖想要通過網際網路對中國大陸進行民主的人要持謹慎的態度。

美國布魯金斯基學會中國研究中心（John L. Thornton China Center at Brookings）學者 Kenneth Lieberthal 和 Peter W. Singer 於 2012 年撰寫的

---

[38] Michael Chertoff, *Homeland Security Assessing the First Five Years*, (Philadelphia: University of Pennsylvania Press, 2011), pp. 95-103.

[39] Bridgette Braxton, *Critical Infrastructure Protection.* (Master's thesis., A Capstone Project Submitted to the Faculty of Utica College, 2013), pp. 1-14, <http://search.proquest.com/docview/1501662605>.

[40] Ian Bremmer, "Democracy in Cyberspace: What Information Technology Can and Cannot Do," *Foreign Affairs*, Vol. 89, No. 6, November/December 2010, pp. 86-92.

[41] Jacob A. Mauslein, *Three Essays on International Cyber Threats: Target Nation Characteristics, International Rivalry, and Asymmetric Information Exchange*, (Ph. D. diss., Department of Security Studies College of Arts and Sciences, Kansas State University, Manhattan, Kansas, 2014), pp. 1-30, <http://krex.k-state.edu/dspace/bitstream/handle/2097/18147/JacobMauslein2014.pdf?sequence=1&isAllowed=y>.

[42] Joseph House, *Internet Censorship in China*, (Master's thesis., American University, Washington, DC, 2011), pp. 1-12, <file:///C:/Users/C640/Downloads/PDF.pdf >.

《Cybersecurity and U.S.-China Relations》，[43]探討網路安全合作所存在的問題，進而闡述網路安全合作的困難之處，並分析了中美關係的特殊性對中美網路安全合作的負面影響。文章最後得出結論，中美的網路安全合作是可能存在的，但是需要加強戰略對話與雙邊互信，注意避開彼此紅線、談大原則而不應該細究分歧等建議。以下表1為上述網路安全相關文獻整理表。

表1　網路安全相關文獻整理表

主題	作者	著作名稱	出版年	主要論述
網路戰爭	W. Alexander Vacca	Military Culture and Cyber security	2011 年	以認知心理學角度，闡釋軍事文化對網路新戰場形成的影響與作用。
	Thomas Rid	More Attacks, Less Violence	2013 年	強調網路戰爭的弱暴力性和不確定性。
		Cyber War Will Not Take Place	2012 年	認為網路戰爭不可能爆發，網路攻擊不等於網路戰爭。
	Ronald J. Deibert、Rafal Rohozinski、Masashi Crete-Nishihata	Cyclones in Cyberspace Information Shaping and Denial in the 2008 Russia–Georgia War	2012 年	探討 2007 年 Estonia 與 2008 年 Georgia 政府網站受到俄羅斯官方網路攻擊，此事件促使北約卓越合作網路防禦中心（NATO Cooperative Cyber Defence Centre of , CCDCOE），並從 2009 年開始研議《塔林手冊》（Tallinn Manual）。
	Richard A. Clarke、Robert K. Knake	Cyber War: The Next to National Security and What	2014 年	作者指出網路安全相關政策的急迫性，認為大規模網路攻擊的

[43] Kenneth Lieberthal & Peter W. Singer, *Cybersecurity and U.S.-China Relations*, (Washington, D.C.: The Brookings Institution, 2012), pp. 31-33, <https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf>.

		to Do About It		可能性提高，網路911 事件在可預見的未來可能會發生，政府應儘速通過網路安全相關的立法措施。
	Leigh Armistead	Information Operation Matters	2012 年	作者認為資訊力量的本質已產生重大改變，有別於軍事、外交和經濟等傳統力量可由政府掌控，政府已經不再能完全控制資訊。關鍵基礎設施防護屬於資訊行動措施的一部分，如何確保網路空間安全，勢必成為國家的重要目標。
	Adam P. Liff	Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War	2012 年	作者指出網路戰爭爆發的可能性較小，但是網路攻擊可能會變得越來越頻繁。
網路安全治理	G. Grove、 S. Goodman、 S. Lukasik	Cyber-attacks and International Law	2010 年	指出網路攻擊缺乏有效的國際法規範，如何在國際間制訂國際法原則，加以約束網路攻擊仍有相當大的困難。
	Jeff J. McNeil	Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem	2010 年	針對網路攻擊無法確定、網路安全難以監管等情況下，要有效應對網路攻擊、維護網路安全，國際間的合作勢在必行。
	Eneken Tikk	Ten Rules for	2011 年	針對網路攻擊問題日

		Cyber Security		益嚴重，提出十條有關網路安全國際合作的原則。
	James A. Lewis	Conflict and Negotiation in Cyberspace	2013 年	著重於網路安全的政治、軍事方面，由於技術創新與國家之間缺乏協調聯繫，造成網路間諜和網路犯罪日益猖獗，政府應當透過制度、規範與法律加以限制，思考在網路空間中，國家行為如何能夠被社會大眾所接受並採納。
	Robert J. Domanski	Who Governs the Internet? The Emerging Policies, Institutions, and Governance of Cyberspace	2013 年	針對網際網路的絕對自由提出質疑，提出當前網路仍處於政府的管理之下，主張政府應加強網際網路的監管。
	Michael Chertoff	Homeland Security Assessing the First Five Years	2011 年	由於網路涉及公共與私人領域，想要有效解決網路安全問題，需要政府、企業、地方及個人的相互配合。
	Bridgette Braxton	Critical Infrastructure Protection	2013 年	分析當前全球關鍵基礎設施網路安全的脆弱性，指出唯有保護關鍵基礎設施與國際合作，才能有效解決網路安全問題。
網路安全之主	Kristell G. Havens	Borders Without Boundaries: Analysis of Cyber Security Policy and Changing Notions of	2014 年	探討國家主權的內涵會隨著歷史、主體的變更性及行使範圍而演變。國家主權的發展，在網際網路時代似乎遇到了瓶頸。主

權與邊界		Sovereignty		張定義新的國家主權意涵，並發展網路空間的國家主權。
	Joseph S. Nye	權力大未來：軍事力、經濟力、網路力、巧實力的全球主導	2011 年	奈伊將國家掌握關鍵技術而獲得的權力稱為「資訊權力」，表示「資訊權力」的重要。由於虛擬空間進入門檻低，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。
其他相關文獻	Ian Bremmer	Democracy in Cyberspace: What Information Technology Can and Cannot Do	2010 年	分析中美兩國對網路空間自由所持不同的態度，國家所採取的戰略與政策符合該國政府和人民的價值取向。
	Jacob A. Mauslein	Three Essays on International Cyber Threats: Target Nation Characteristics, International Rivalry, and Asymmetric Information Exchange	2014 年	探討 1999 年到 2011 年之間的網路安全威脅，通過數理統計方法，分別探討政治、經濟、社會等傳統因素、國際競爭及國際談判理論與網路威脅的關係。
	Joseph House	Internet Censorship in China	2011 年	針對中國大陸網路審查制度進行研究與探討。認為中國大陸政府通過監管系統控制網路的發展，最後告誡企圖想要通過網際網路對中國大陸進行民主的人要持謹慎的態度。

	Kenneth Lieberthal、Peter W. Singer	Cybersecurity and U.S.-China Relations	2012 年	探討網路安全合作所存在的問題，分析中美關係的特殊性，中美需要加強網路安全對話與建立互信，如此才可能在網路安全上進行合作。

參、日本網路安全發展之背景—ICT 政策發展

日本網路安全的發展奠基於日本資通訊政策的推動，日本政府於1999年開始正視資訊安全的議題。2000年7月7日，第26屆八大工業國集團（G8高峰會）前夕，日本政府在內閣會議上宣佈，正式成立「高度資訊通信網路社會推進戰略本部（高度情報通信ネットワーク社会推進戦略本部）」（以下簡稱「IT戰略本部」（IT Strategic Headquarters）），由時任首相森喜朗擔任部長，成立宗旨為全面推動日本的資訊化革命，並成立由資訊技術等相關產業人士組成「IT戰略會議」。7月21日，G8高峰會在日本沖繩縣舉行，主要議題為資訊技術及產業革命，隨後會議發表《關於全球資訊社會的沖繩憲章》（グローバルな情報社会に関する沖縄憲章），簡稱《IT憲章》，[44]希望能促進資訊技術產業的發展及縮小各國資訊技術的發展落差，好建立資訊化社會。

內閣官房（Cabinet Secretariat）在2000年7月建立《資訊安全對策指導方針》（情報セキュリティポリシーに関するガイドライン），[45]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。同年11月，「IT戰略會議」發表了《IT基本戰略》（ＩＴ基本戦略），[46]宣稱要在5年內將日本建設成世界上最先進的IT國家。2001年1月，日本政府公佈了《高度資訊通信網路社會形成基本法》（高度情報通信ネットワーク社会形成基本法），簡稱《IT基本法》，[47]正式提出「IT立國戰略」，為日本資訊技術發展提供了法律根據。同時，《IT基本法》將原本的「IT戰略本部」與「IT戰略會議」合併為新的IT戰略本部，由首相擔任部長，負責國家IT計

[44] 外務省，〈グローバルな情報社会に関する沖縄憲章〉，《外務省》，<http://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/it1.html>。

[45] 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》，平成 17 年 7 月 14 日，<http://www.nisc.go.jp/conference/suishin/ciso/pdf/konkyo.pdf>。

[46] ＩＴ戦略会議，〈ＩＴ基本戦略〉，《ＩＴ戦略本部》，平成 12 年 11 月 27 日，<https://www.kantei.go.jp/jp/it/goudoukaigi/dai6/6siryou2.html>。

[47] 〈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》，平成十二年法律第百四十四号，<http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000144&openerCode=1>。

畫的制定與實施工作。以下探討日本IT戰略本部與總務省推動資通訊相關政策措施，在這些政策推動上，可看出日本政府不僅重視國家社會的資訊化建設，亦強調資訊科技的安全應用，期望實現電子化政府，並促進國家的經濟發展。

一、《e-Japan戰略》（e-Japan Strategy）

新的IT戰略本部成立後，以《IT基本戰略》為藍圖，於2001年1月公佈《e-Japan戰略》（e-Japan Strategy），正式將IT戰略提升為日本的國家戰略。[48]該戰略闡述IT革命的歷史意義及日本制定IT戰略的必要性，要求在5年內將日本建設成世界最先進的IT國家，進而提出推動日本資訊化社會發展的四個優先政策領域：（一）建設超高速網路基礎設施；（二）完善電子商務制度與規則；（三）實現電子行政；（四）加強人才培養。

同年3月，IT戰略本部在《e-Japan戰略》提出的四個重點領域上發表《e-Japan重點政策計畫》（e-Japan Priority Policy Program），進一步制定各個領域所要達成的目標。其中，該計畫的第六部分《確保高度資訊通信網路的安全性與可靠性》探討日本面臨的資訊安全問題，並且點出日本無論在資訊安全政策的制定上，還是在防火牆等網路安全基礎設施上，均與美國存在較大的差距。

在《確保高度資訊通信網路的安全性與可靠性》中提出八項具體的改善措施，分別是：（一）完善資訊安全相關的制度與基礎設施，制定相關法律，推動加密技術標準化、設立資訊安全管理標準；（二）強化政府內部的資訊安全管理，實行資訊安全認證、評價與檢討制度，推廣使用高保密性的辦公用品；（三）加強保護個人資訊，制定完善相關法律規範；（四）提高民間機構的資訊安全意識，加強官民合作，推廣使用高安全性的電子通信設備，建立資訊安全評估標準，落實網路安全問題呈報；（五）政府與關鍵基礎設施相關企業建立聯絡與合作機制，改善政府機構的應急處理能力；（六）推動資訊安全相關技術的研究開發；（七）培育資訊安全人才，提升政府機構內部相關人員的業務素質，建立資格考察與認證制度；（八）加強資訊安全領域的國際合作，共同應對高科技跨國網路犯罪，與各國資訊安全部門建立資訊交換機制。[49]

《e-Japan重點政策計畫》、《e-Japan2002計畫》（e-Japan 2002 Program）[50]與《e-Japan重點政策計畫—2002》（e-Japan Priority Policy Program - 2002）[51]，以上三個計畫內容同為五個重點政策及五個橫斷面課題，五個重點政策為：（一）世界最高水準之資通訊網路的建立；（二）教育學習的振興與人才培育；（三）

[48] IT Strategy Headquarters, “e-JAPAN Strategy,” *IT Strategy Headquarters*, January 22, 2001, <http://japan.kantei.go.jp/it/network/0122full_e.html>.
[49] IT Strategy Headquarters, “e-JAPAN Priority Policy Program,” *IT Strategy Headquarters*, March 29, 2001, <http://japan.kantei.go.jp/it/network/priority-all/index.html>.
[50] IT Strategy Headquarters, “e-JAPAN 2002 Program,” *IT Strategy Headquarters*, June 26, 2001, <http://japan.kantei.go.jp/it/network/0626_e.html>.
[51] IT Strategy Headquarters, “e-JAPAN Priority Policy Program - 2002,” *IT Strategy Headquarters*, June 18, 2002, <http://japan.kantei.go.jp/policy/it/0618summary/01_e.html>.

電子商務的促進；（四）行政與公共領域資訊化；（五）資訊網路安全性與信賴性的確保。五個橫斷面課題為：（一）促進ICT的研究開發；（二）ICT之國際協調與貢獻；（三）矯正數位落差；（四）因應ICT所造成社會經濟結構的變動；（五）加深國民對ICT的理解措施。

總而言之，《e-Japan戰略》是IT戰略本部的第一個ICT發展政策，其目的是希望日本能在五年內成為最先進的ICT國家，並建立ICT積極應用的智慧型社會（知識創発型社会）。《e-Japan重點政策計畫》是IT戰略本部的第一個ICT執行計畫，且《e-Japan2002計畫》與《e-Japan重點政策計畫—2002》都是延續並補充《e-Japan戰略》。[52]

由於原訂目標希望在 2005 年達到日本 3,000 萬家庭可寬頻上網及 1,000 萬家庭超寬頻（30Mbps-100Mbps）上網的環境，此目標在 2003 年提前達成，因此，日本進入第二期 IT 革命。IT 戰略本部提出《e-Japan 戰略 II》，以活用資通訊科技為目標，[53]推動內容包括兩大主軸，包括七大優先應用領域：醫療、食、生活、中小企業金融、知識／學習、就業／勞動、行政服務的資訊應用，以及新加入五項基礎網路環境整備：建設新世代 IT 網路建設、發展安心及安全的資訊應用環境、促進研究發展、培育資通訊應用人才、應用資訊科技發展新國際關係，以此擴大資訊應用的範圍。

無論是《e-Japan戰略II》與《e-Japan重點政策計畫—2003》（e-Japan Priority Policy Program - 2003），其目的為透過ICT的有效利用，來建立「元氣、安心、感動、便利」的社會。[54]為了加速《e-Japan戰略II》的落實，IT戰略本部於2004年執行《e-Japan戰略II加速計畫》（e-Japan Strategy II Acceleration Package）、[55]《e-Japan重點政策計畫—2004》（e-Japan Priority Policy Program - 2004）[56]及《IT政策整合—2005》（IT Policy Package - 2005），目標皆是要達到「日本於2005年成為世界最先進的ICT國家」，並使日本民眾能更常應用ICT，並推動政府各行政機關間的合作。[57]

《e-Japan重點政策計畫—2003》之內容包括上述ICT七大優先應用領域、五項重點政策與五個橫斷面課題；《e-Japan戰略II加速計畫》（e-Japan Strategy II Acceleration Package）內容包括：亞洲地區國際ICT政策的實施（A：Asia）、資訊安全的強化（B：Block and Back-up: Security）、數位內容政策的推動（C：Contents）、ICT法規改革的推動（D：Deregulation）、ICT政策的評價（E：Evaluation）、

---

52 黃偉倫，〈日本與新加坡的國家資訊通信科技發展計畫〉，《全球政治評論》，第 41 期，2013 年，頁 77-113。

53 IT Strategy Headquarters, “e-JAPAN Strategy II,” *IT Strategy Headquarters*, July 2, 2003, < http://japan.kantei.go.jp/policy/it/0702senryaku_e.pdf>.

54 IT Strategy Headquarters, “e-JAPAN Priority Policy Program - 2003,” *IT Strategy Headquarters*, August 8, 2003, <http://japan.kantei.go.jp/policy/it/0808summary/030808gaiyo_e.pdf>.

55 IT Strategy Headquarters, “e-JAPAN Strategy II Acceleration Package,” *IT Strategy Headquarters*, February 6, 2004, <http://japan.kantei.go.jp/policy/it/040318senryaku_e.pdf>.

56 IT Strategy Headquarters, “e-JAPAN Priority Policy Program - 2004,” *IT Strategy Headquarters*, June 15, 2004, <http://japan.kantei.go.jp/policy/it/040615summary/040615gaiyo_e.pdf>.

57 IT Strategy Headquarters, “IT Policy Package - 2005,” *IT Strategy Headquarters*, February 24, 2005, <http://japan.kantei.go.jp/policy/it/itpackage2005.pdf>.

更友善的電子化政府服務（F：Friendly e-government and e-local government）等六項加速應用領域。

《e-Japan重點政策計畫—2004》之內容包括2005年目標達成的重點對策（五項基礎網路環境整備、七大優先應用領域）、2006年後的ICT布局政策（國際政策、資訊安全、人才教育、電子商務、數位內容、電子政府、研究開發、基礎設施）、五個重點政策與五個橫斷面課題。以下表2為2001年到2004年日本的資通訊發展政策。

表2　2001-2004年日本的資通訊發展政策

時間	政策名稱
2001 年 1 月 22 日	《e-Japan 戰略》（e-Japan Strategy）
2001 年 3 月 29 日	《e-Japan 重點政策計畫》（e-Japan Priority Policy Program）
2001 年 6 月 26 日	《e-Japan2002 計畫》（e-Japan 2002 Program）
2002 年 6 月 18 日	《e-Japan 重點政策計畫—2002》（e-Japan Priority Policy Program - 2002）
2003 年 7 月 2 日	《e-Japan 戰略 II》
2003 年 8 月 8 日	《e-Japan 重點政策計畫—2003》（e-Japan Priority Policy Program - 2003）
2004 年 2 月 6 日	《e-Japan 戰略 II 加速計畫》（e-Japan Strategy II Acceleration Package）
2004 年 6 月 15 日	《e-Japan 重點政策計畫—2004》（e-Japan Priority Policy Program - 2004）

資料來源：作者自行整理。

二、《u-Japan政策》（u-Japan Policy）

日本經歷《e-Japan戰略》後，社會的資訊化得到提升，但與先進國家相比，仍然存在一定的差距。2003年日本的寬頻使用人口為1,495萬人（如圖1），全國普及率為11.7%；而同時期的韓國、香港、加拿大都比日本要高，分別達到了23.3%、18%和14.7%，日本只排名世界第7名（如圖2）。從數據上可知，日本資訊化雖然有了一定的發展，但還有更大的進步空間。

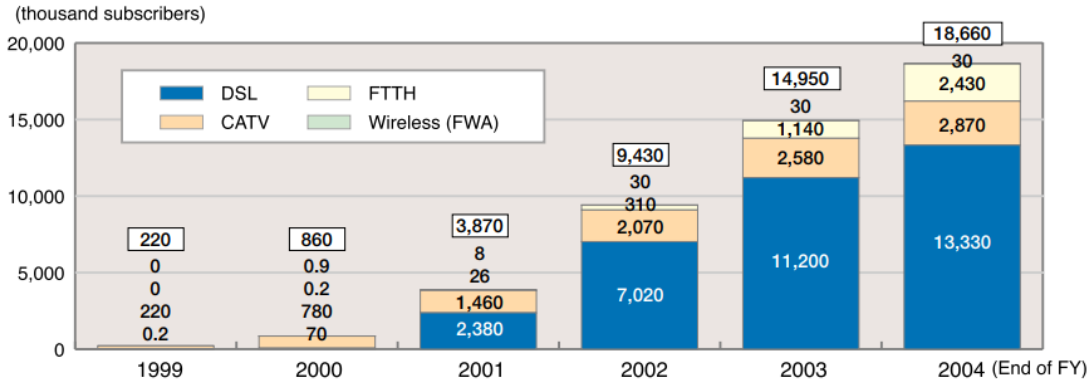

圖1　日本1999-2003年之寬頻使用人口數

資料說明：寬頻包括數位用戶線路（Digital Subscriber Line, DSL）、光纖到家（Fiber to the home, FTTH）、有線電視網路（Cable Television, CATV）與固定無線網路(Fixed Wireless Access, FWA)。

資料來源：Ministry of Internal Affairs and Communication, “Information and Communication in Japan 2005 summary,” pp. 26, <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2005/chapter1-4.pdf>.

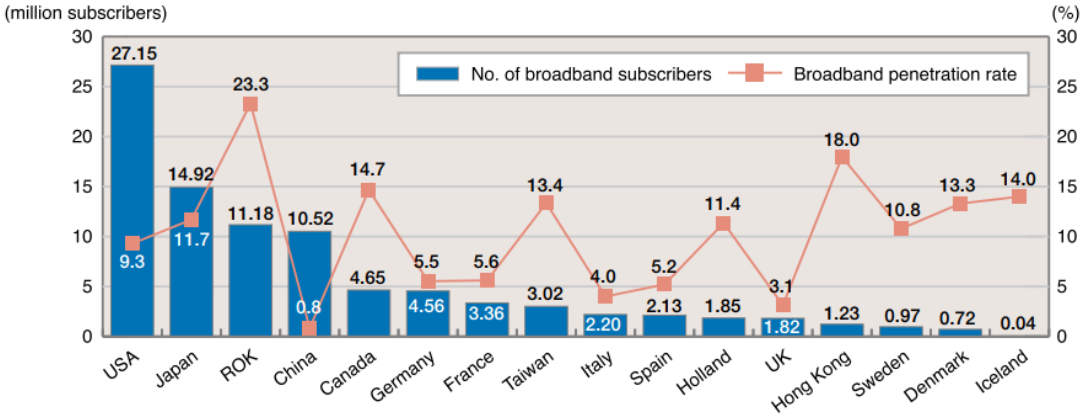

圖 2　2003 年世界各國寬頻網路普及率

資料來源：Ministry of Internal Affairs and Communication, “Information and Communication in Japan 2005 summary,” pp. 27, <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2005/chapter1-4.pdf>.

為了建構無所不在的網路社會，2004 年 3 月日本總務省（Ministry of Internal Affairs and Communications, MIC）召開了「實現無所不在（Ubiquitous）網路社會政策懇談會」，並於同年 5 月正式向日本經濟財政諮詢會議提出「u-Japan 構想」，此構想在 6 月 4 日被日本內閣通過，把原本的 IT 進一步擴展成為資訊通信科技（Information Communication Technology, ICT），直到同年 8 月，總務省

公布以發展無所不在網路社會為中心的《平成 17 年度 ICT 政策大綱》後，[58]正式確認執行的中心思想，並規畫出未來願景，直到 12 月 17 日，懇談會終於提出《u-Japan 政策》的最終報告，確立該政策之詳細執行方針。

《u-Japan 政策》的目標是要能達到無所不在（Ubiquitous）的網路社會，在 2010 年將日本建構成 Anytime、Anywhere、Any device、Anyone 都可以上網的環境，透過非常方便的網路和低廉的費用來促進資訊交流，將 ICT 運用到經濟、社會各方面，以期 ICT 能解決日本社會所面臨的問題。《u-Japan 政策》的理念可以用 4U 來概括：（一）無所不在（Ubiquitous），即連接所有人事物，使任何人在任何時間、任何地點都能透過任何方式方便上網，實現人與人、人與物、物與物的資訊溝通；（二）普及性（Universal），即交流的廣泛性，任何人，包括高齡者和身心殘障者，不必擔心設備和網路問題，利用 ICT 參加各種活動，使人與人的交流可超越語言和地域的限制，形成親密無間的溝通；（三）使用者導向（User-oriented），技術與服務必須緊貼使用者的需求，運用網路的力量，讓使用者參與產品的生產中；（四）獨特的（Unique），透過 ICT 讓個人和社會充滿活力，創造新的商務型態及服務，藉由創意使資源活化，促進區域再生。[59]

從《e-Japan 戰略》到 2006 年日本 IT 戰略本部於 1 月所提出的《IT 新改革戰略》（New IT Reform Strategy ）中，可見過去《e-Japan 戰略》著重於 E 化的推動，到後來《u-Japan 政策》則是積極使用 ICT，來解決社會可能會發生的問題，如：環境汙染、醫療照護、行動汽車管理、經濟成長與創造工作機會、提升人力資源、公共風險與行政服務等。《u-Japan 政策》的發展主軸更著重於生活和福利層面，希望能提升生活品質與生活價值。

《u-Japan 政策》主要以如何應用資通訊科技來解決社會問題及促進社會發展為主要方向。日本面臨出生率下降及人口老化等兩大問題，而上述現象代表著，日本未來將要面對勞動力減少、消費力下降、總體經濟力下滑等問題。日本政府認為網路化的社會可以累積和釋放民眾的潛在力量，進而激發民眾創新研發，透過經濟發展及創新的社會價值來解決上述問題。故日本以發展一個便於使用網路的社會為政策推動的主要目標。

然而《u-Japan 政策》在規劃中面臨了幾個問題：（一）網路基礎設施從有線升級為無線網路，這種無所不在的網路環境，會對未來的生活帶來什麼樣的衝擊？（二）未來的生活科技將滲透每一個生活細節，該如何解決這種無所不在的網路社會，因使用 ICT 而衍生的各種社會問題？（三）當網路環境涉入生活的每一部份時，如何提升民眾使用 ICT 的信任程度，好降低可能產生的負面態度？為了解決上述問題，進而實現《u-Japan 政策》所設定的目標，日本總務省提出未來社會

[58] 総務省，〈平成１７年度ＩＣＴ政策大綱―ユビキタスネット社会の実現へ向けて〉，《WARP》，平成 16 年 8 月，<http://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/s-news/2004/040827_7.html>。

[59] Ministry of Internal Affairs and Communication, “Information and Communication in Japan 2005 summary,” pp. 6-11, <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2005/chapter1-4.pdf>.

的發展架構，嘗試就五個方向的政策，推動 u-Japan 所需要的基礎環境，這些政策內容包括：提升無所不在的網路整備程度、強化民眾對於 ICT 的使用程度、發展優質的網路使用環境、關注國際上網路安全的相關議題、從研發上的努力取得技術上的創新領先。[60]

在《u-Japan 政策》中所關注的各個社會議題，分類如下：社會與居住、勞動與雇用、醫療及福利、教育及人力資本、公共行政管理、交通運輸、公共安全及災難預防、國際事務參與、環境與能源問題、經濟及產業發展等，從上述議題可知，《u-Japan 政策》較 2000 年初期發展的《e-Japan 戰略》，更關注資訊科技的發展應用，幫助解決各種社會議題。

《e-Japan 戰略》改變日本政府、企業及個人的樣貌，進而推動日本的經濟社會走向資訊化。從 2001 年到 2005 年，日本雖然實現了成為世界最先進的 IT 國家之目標，但無論在行政服務、醫療、教育的資訊化，或是充分利用資訊化提高國民滿意度、消除數位落差、資訊安全、電子商務、提高國際競爭力、為國際社會做出貢獻等方面，都還存在著亟待解決的問題。為此，IT 戰略本部於 2006 年提出，2006 年到 2010 年 ICT 的發展政策—《IT 新改革戰略》。而《重點政策計畫—2006》（Priority Policy Program 2006 ）是執行方案，使日本在 2010 年成為世界 ICT 革命的領導者，並推動日本社會成為隨時、隨地、任何人都能真實感受 ICT 便利的社會。《重點政策計畫—2006》之三個重點政策為：ICT 社會結構改造力追求（ＩＴ構造改革力の追求）、ICT 基礎建設整備（ＩＴ基盤の整備）、國際競爭力與國際貢獻的提高（世界への発信）。[61]

經濟財政諮詢會議（経済財政諮問会議）[62]於2007年提出日本經濟發展方向與戰略《日本経済の進路と戦略について）》，並認為ICT可協助經濟社會的創造與成長，所以IT戰略本部於2007年4月5日公佈《IT新改革戰略政策綱要》（IT新改革戦略政策パッケージ），其中三個目標為：效率與產量提升等新價值的創

---

[60] 曾淑芬，《網路社會發展政策整合研究─總綱計畫「整合規劃未來 4 年我國網路社會發展」》（台北：行政院研究發展考核委員會編印，2007 年），頁 78-79。

[61] 資策會電子商務組，〈電子商務現況─各國電子商務及網路發展政策〉，《2014 電子商務觀察》，2014 年 11 月 12 日，<http://2014ecommerce.blogspot.jp/2014/11/blog-post_29.html>。

[62] 日本在 1990 年代所推動行政改革時，將過去由大藏省獨占預算編列的權限轉移至直屬於首相的內閣府之「經濟財政諮詢會議」，該會議於 2001 年 1 月成立，2009 年 9 月因日本民主黨執政，該會議停止運作，自 2012 年安倍政權開始運作後，也重新啟動自民黨時代的「經濟財政諮詢會議」。首相可以透過經濟財政諮詢會議的運作，主導預算編列與各 種經濟政策的決定。經濟財政諮詢會議是基於內閣法第 18 條明文規定的合議制機關，委員含擔任主席的首相在內共 11 人，除了首相以外，明文規定的委員只有內閣官房長官、負責經財會議運作的經財大臣，民間委員最少要占 11 人之中的 4 成，也會依議題邀請負責相關政策的大臣以臨時委員的身分出席。經財會議的功能有三點，第一是基於首相的要求，針對總體經濟、財政與預算編列的基本方向等關於經濟財政政策的重要事項進行研究與討論；第二是基於首相與相關政策的負責大臣的要求，對與「國土形成計畫法」所規定的計畫有關聯的經濟政策、整體經濟政策的一貫性與整合性進行研究與討論；第三是針對上述事項對首相提出建言。請參閱：黃偉修，〈日本民主黨的政治主導決策模式與鳩山首相的領導能力〉，《問題與研究》，第 50 卷第 2 期，2011 年 6 月，頁 75-84；內閣府経済財政諮問会議，〈経済財政諮問会議議員の変遷〉，《経済財政諮問会議》，<http://www5.cao.go.jp/keizai-shimon/kaigi/about/successive_memberlist.pdf >。

造、健全且安心社會的建設、創造性發展之基礎建設整備。[63]《重點政策計畫—2007》（Priority Policy Program 2007）的內容為《重點政策計畫—2006》及《IT新改革戰略政策綱要》之三個重點政策及三個目標的延續。

根據「IT新改革戰略評價專門調查會」於2008年對《IT新改革戰略》成效的評價[64]及經濟財政諮詢會議於2008年所建議日本經濟發展方向與戰略，IT戰略本部於2008年執行《IT政策藍圖》(IT政策ロードマップ)與《重點政策計畫—2008》（Priority Policy Program 2008），其目的是規劃ICT政策時程表，進而實現《IT新改革戰略》在2010年的目標，並探討2010年以後的ICT政策發展方向。

其中，《IT政策藍圖》將加強推動三個重點領域，（一）國民為導向的電子政府、醫療與社會保障服務（国民本位のワンストップ電子行政、医療・社会保障サービスの実現）；（二）ICT能安心且有效運用之環境的先進社會（ＩＴを安心して活用でき、環境に先進的な社会の実現）；（三）ICT關聯力發揮的經濟成長（「つながり力」発揮による経済成長の実現）。[65]

根據總務省研究，ICT產業對經濟成長的貢獻度而言，相較於其他產業來得貢獻更高（如圖3），若能有效利用ICT，將能帶動整體經濟成長。[66]圖4中可明顯看出，相較於其他產業而言，有高達35個縣市的ICT產業對經濟成長的貢獻度超過50%。因此，若能有效建立一個整合性的ICT政策，將能帶動整體經濟的成長，並降低縣市間的發展差距。

---

63 經濟財政諮問會議，〈日本経済の進路と戦略について〉，《經濟財政諮問會議》，2007 年 1 月 25 日，<http://www.kantei.go.jp/jp/singi/keizai/kakugi/070125kettei.pdf>。

64 「IT新改革戰略評價專門調查會」利用PDCA（由四個部分組成：制定計畫（Plan）、實施計畫（Do）、評價結果（Check）、改善計畫（Act））循環程序確認2006-2007年之《IT新改革戰略》的實際成效且提出改善意見，改善重點從使用者觀點探討ICT被徹底活用的方式。而《重點政策計畫─2008》的內容則為計畫目標實現的具體政策，二則為改善IT結構、重視使用者、強化競爭力等，三則利用PDCA循環程序評估計畫目標之成效及達成期限等，進而選擇與集中執行哪些重點政策。請參閱：黃偉修，〈日本民主黨的政治主導決策模式與鳩山首相的領導能力〉，《問題與研究》，第50卷第2期，2011年6月，頁86。

65 IT 戰略本部，〈ＩＴ政策ロードマップ〉，《IT 戰略本部》，2008 年 6 月 11 日，<http://www.kantei.go.jp/jp/singi/it2/kettei/080611honbun.pdf>。

66 ICT 成長力懇談會，〈ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて〉，《ICT 成長力懇談會報告書》，2008 年 7 月 3 日，<http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/vigor/pdf/080630_2_si1.pdf>。

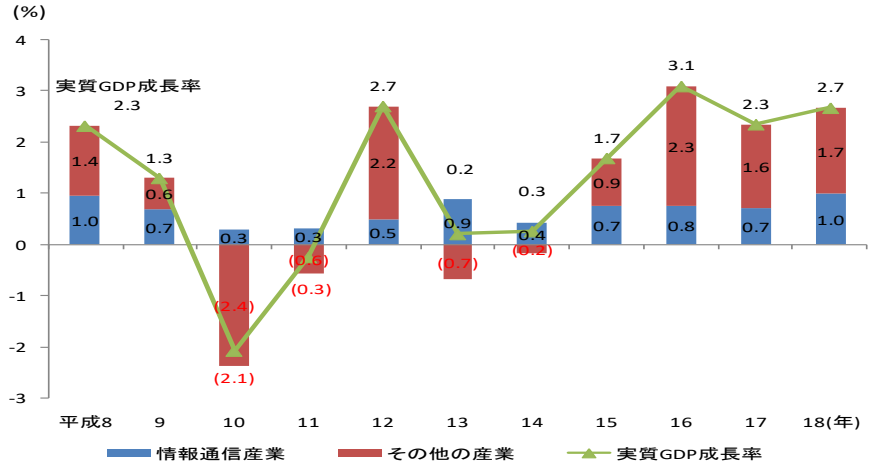

圖 3　ICT 產業對 GDP 成長的貢獻程度

資料來源：ICT 成長力懇談會，〈ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて〉，《ICT 成長力懇談會報告書》，2008 年 7 月 3 日，<http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/vigor/pdf/080630_2_si1.pdf>。

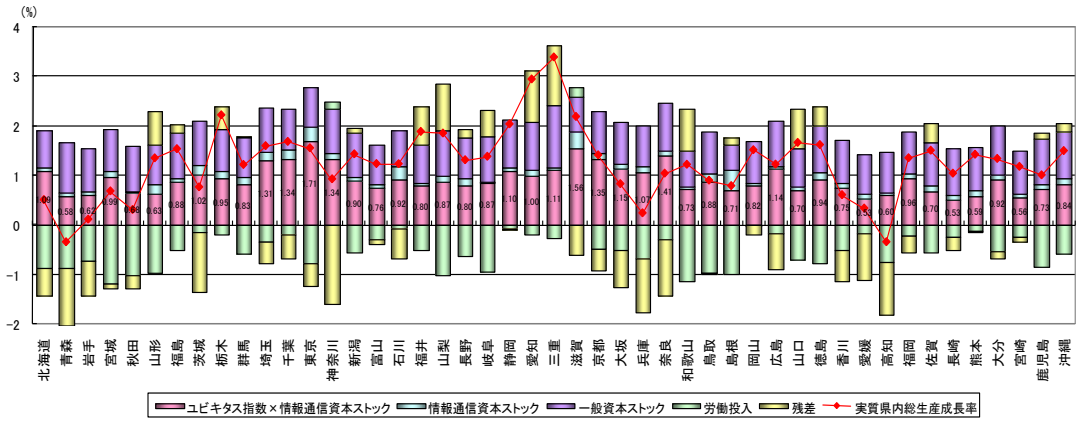

圖 4　各縣市生產成長率之因素分析圖

資料來源：ICT 成長力懇談會，〈ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて〉，《ICT 成長力懇談會報告書》，2008 年 7 月 3 日，<http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/vigor/pdf/080630_2_si1.pdf>。

總務省在 2008 年 2 月成立 ICT 發展專案小組，開始制定相關發展策略，並於該年 7 月 3 日發表《xICT Vision：產業及區域與 ICT 的深層融合》（ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて）報告，說明日本當時所面臨的問題，如：國家成長趨緩與區域間數位落差等問題，並指出

ICT 扮演的角色與影響。基本上，《xICT Vision》並非是一個全新的政策，而是針對《u-Japan 政策》內容進行調整。在《xICT Vision》中除了保留《u-Japan 政策》的相關工作之外，更迎合最新的全球趨勢，納入產業及區域兩個部分，總務省更將其定位為《u-Japan II 政策》。[67]

從「xICT」政策的架構來看，共分成三個部分，一是「產業 xICT=新融合市場」，也就是有效應用 ICT 達到產業變革，促進新融合市場的發展，如：傳統媒體產業在過去 e 化社會，透過紙張、電視、網路等媒介來閱讀收看，但在 u 化的社會中，則可透過隨身攜帶的電子 paper 收看新聞節目；二是「地區 xICT=電緣社會」，也就是透過 ICT 連結力，將地緣、血緣社會，以電子方式連結人與地區，如：觀光客與觀光導遊志工在未來 u 化的社會中，則是透過內嵌電子標籤的地區貨幣，提供多國語言的觀光導覽服務；三是「生活（人）xICT=無所不在的網路社會」，也就是有效應用 ICT 達到生活變革，達到無所不在的網路社會環境。[68] 如下圖 5 實現無所不在的網路服務社會藍圖。

[67] 郭仁宗、賴明豐、簡逸菁，〈日本 xICT Vision 政策內涵與發展方向〉，《國家實驗研究院科技政策研究與資訊中心》，2009 年 12 月 14 日，<https://portal.stpi.narl.org.tw/index/history>。

[68] 莊順斌，〈日本 xICT 政策總務省定位為 u-Japan II〉，《資策會創新應用服務研究所 FIND》，2008 年 12 月 11 日，<https://www.find.org.tw/market_info.aspx?n_ID=4747>。

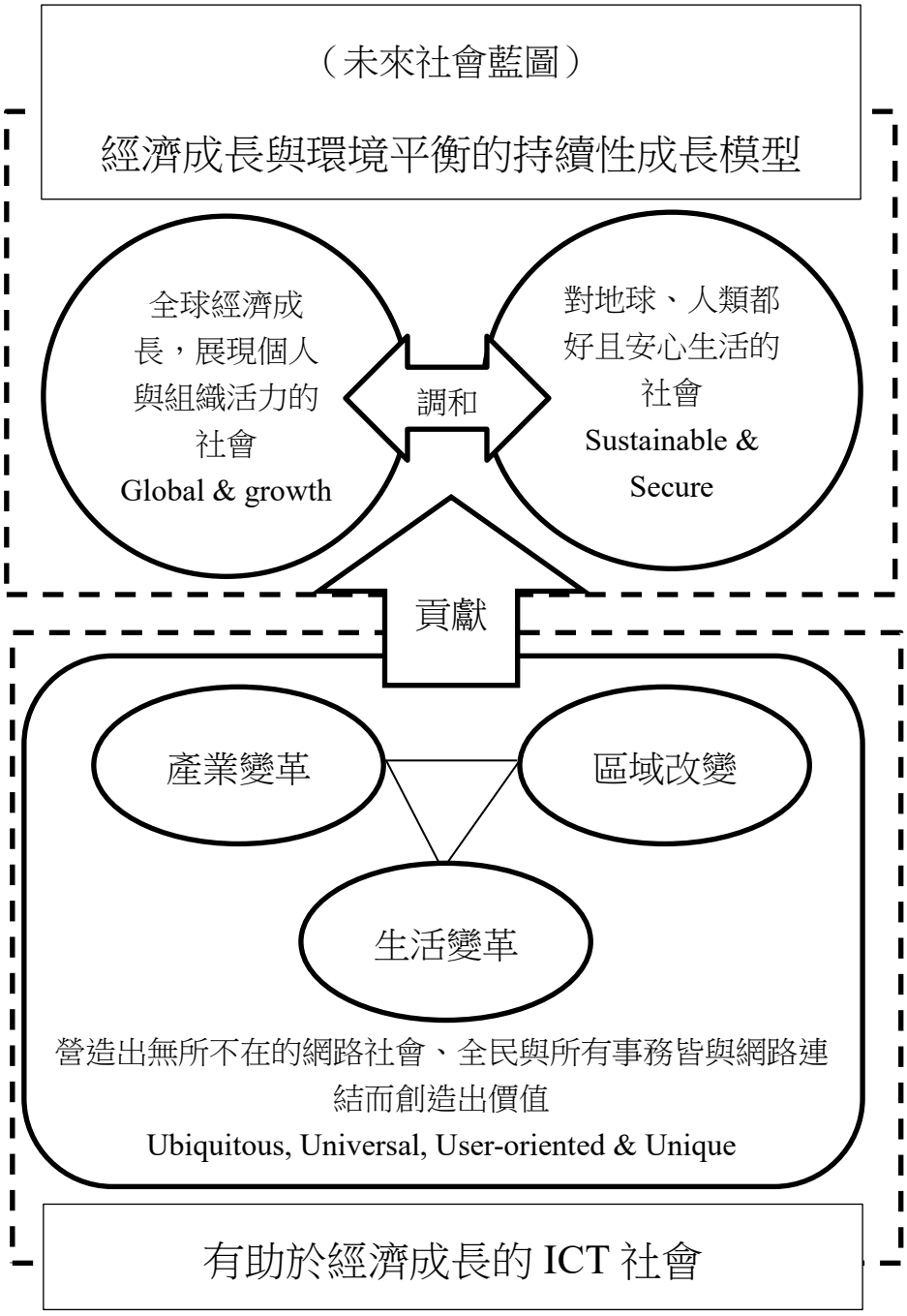

圖 5　無所不在的網路服務社會藍圖

資料來源：ICT 成長力懇談會，〈ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて〉，《ICT 成長力懇談會報告書》，2008 年 7 月 3 日，<http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/vigor/pdf/080630_2_si1.pdf>。

表 3　2005-2009 年日本的資通訊發展政策。

時間	政策名稱
2004 年 12 月 17 日	總務省公布《u-Japan 政策》
2005 年 2 月 24 日	《IT 政策整合—2005》（IT Policy Package - 2005）
2006 年 1 月 19 日	《IT 新改革戰略》（New IT Reform Strategy ）
2006 年 7 月 26 日	《重點政策計畫─2006》（Priority Policy Program 2006 ）
2007 年 4 月 5 日	《IT 新改革戰略政策綱要》（IT 新改革戦略政策パッケージ）
2007 年 7 月 26 日	《重點政策計畫─2007》（Priority Policy Program 2007）
2008 年 6 月 11 日	《IT 政策藍圖》（IT 政策ロードマップ）
2008 年 7 月 3 日	總務省公布《xICT Vision：產業及區域與 ICT 的深層融合》（ｘＩＣＴビジョン～あらゆる産業・地域とＩＣＴとの深化した融合に向けて）
2008 年 8 月 20 日	《重點政策計畫─2008》（Priority Policy Program 2008）
2009 年 4 月 9 日	《數位新時代新戰略—三年緊急計畫》（デジタル新時代に向けた新たな戦略～三か年緊急プラン～）

資料來源：作者自行整理。

三、《i-Japan2015戰略》（i-Japan Strategy 2015 ）

回溯日本資通訊政策推動歷程，《e-Japan 戰略》的核心是網路基礎設施；《e-Japan 戰略 II》的重點，強調利用數位技術推動經濟社會的結構改革。雖然資訊基礎設施不斷完善，但大多數民眾依然覺得應用層面不明顯。2009 年日本受到美國金融海嘯波及，導致經濟發展呈現停滯狀態，加上低生育率和社會活力衰弱，迫使日本政府重新思考 ICT 對日本經濟發展之意義。

日本原訂 2010 年 IT 發展目標為，以 IT 打造日本的資訊競爭力，讓日本成為世界級的資訊供應者。但是當時日本電子政府的管理架構屬於中央、地方兩層式的管理架構，不但應變速度緩慢，中央與地方的本位主義造成彼此溝通協調不易，更讓人力和資源無法充分發揮效用，導致政策無法落實。 為了盡快從經濟衰退中復原，日本政府認為，資訊管理架構的變革勢在必行。因此，在 2009 年 4 月到 7 月間，日本 IT 戰略本部與總務省提出，以增加 ICT 投資等相關振興經濟方案措施，提出為期三年的短期經濟因應對策《數位新時代新戰略—三年緊急計畫》（デジタル新時代に向けた新たな戦略—三か年緊急プラン）及中長期資通訊政策《i-Japan2015 戰略》（i-Japan Strategy 2015 ），希望能帶領日本克服經濟危機，朝向重視民眾生活資訊的應用，朝向發揮日本經濟實力的數位新時代邁進。

《三年緊急計畫》是《i-Japan2015 戰略》的執行方案，[69]該計畫目的是將 IT 投資金額在 2009 年到 2011 年 3 年間增加 3 兆日圓，並增加約 50 萬人的工作機會，並宣布設立國家級的資訊長（Chief Information Officer, CIO），職稱是「政府 CIO」，採專人專任制，希望透過制度化的國家級 CIO 角色，打破各級政府行政本位主義，建立一個整合中央和地方政府的資訊管理架構，由中央統籌各級政府的 IT 人才和資源運用，以提高政府行政運作效率。[70]

《i-Japan2015 戰略》從「以人為本」的理念出發，創造使國民安心且有活力的社會，大力發展項目有：（一）電子政府；（二）推動醫療健康資訊服務；（三）教育與人才培育。欲達成電子政府之目標有下列三項，1.電子窗口改革，目標為民眾可以透過電視、個人電腦、手機或電子窗口等管道，進入電子政府的行政、24 小時裡在家裡或便利商店等，可以隨時得到必要的證明文件、即使是不習慣數位科技的老年人也可以使用點擊率較少的操作畫面，得到國家和地方行政的資訊和服務；2.改善行政程序，目標是透過行政機關之行政程序的數位結合，進行無紙化的資訊交換，相關行政部門從國民和企業的角度，徹底進行業務流程重組（Business Process Reengineer, BPR）及推廣普及「國民個人電子信箱（国民電子私書箱）」，如此可以減少行政成本三成以上；[71]3.改善行政資訊的可得性措施，改善內容為人民和企業想要了解行政程序的處理狀況時，可以隨時且確實的得知資訊。[72]

為了加速推動電子政府的制度與法規，其執行方法為下列三項：（一）為了推動電子政府的指揮中心，透過各部會資訊長（CIO）的任命來推動電子政府，改革重點為預算調整和分配、行政程序與資料數據標準化、政府地方再造及合併廢除現有的各部會組織，並且政府的資訊長與地方政府的資訊長需充分溝通。[73]

---

[69] IT 戦略本部，〈デジタル新時代に向けた新たな戦略―三か年緊急プラン〉，《IT 戦略本部》，平成 21 年 4 月 9 日，<http://www.kantei.go.jp/jp/singi/it2/kettei/090409plan/090409honbun.pdf>。

[70] 王宏仁，〈用國家級 CIO 領導次世代 e 政府〉，《iThome》，2009 年 7 月 24 日，<https://www.ithome.com.tw/news/98888>。

[71] 所謂的「國民個人電子信箱」(「国民電子私書箱」)，每個人擁有自己的帳號，希望人民能在個人電子信箱中建立屬於自己的醫療資訊和保險資訊等，使用者能一致性的管理自己的資訊之外，醫療機關和保險公司各種詳細表格的成本也能削減及地址變更和納稅申報等的手續也能簡化，請參閱：丸山橋生，〈国民電子私書箱（仮称）〉，《株式會社日立總合計畫研究所》，<http://www.hitachi-hri.com/keyword/k056.html>。

[72] IT Strategy Headquarters, “i-Japan Strategy 2015,” *IT Strategy Headquarters*, July 6, 2009, <http://japan.kantei.go.jp/policy/it/i-JapanStrategy2015_full.pdf>.

[73] 在電子化政府的發展方面，小尾敏夫（Toshio Obi）教授指出十個電子化政府發展的重要因素，分別是：國家主導權（Leadership）、電子治理（e-Governance）、人力資源（Human-Resource Development）、全球網絡（National/Global Network）、科技發展（Technology）、內容及應用（Content／Application）、系統管理（Solution／System）、核心能力（Core Competence）、安全（Security）及電子民主（e-Democracy）。日本政府逐漸認知在電子化政府的推動過程中，需要中央、地方政府乃至全球間的通力合作。尤其除了中央政府的政策規劃外，地方政府的積極介入是將資通訊科技應用推展至全體民眾及提升生活品質不可或缺的力量。以日本的公共設施網路為例，便結合了市政府、學校、社區中心、車站、圖書館以及公共醫療中心等不同的單位，形成彼此之間的共通網路。在這些指標中，小尾教授特別指出未來無所不在的網路社會發展趨勢下，政府資訊長（GCIO, government chief information

（二）各部會資訊長（CIO）的職責為電子政府項目的負責人，其工作內容包含行政程序改革、資訊、財務及人事的管理、資訊長活動及成果呈現以及資訊保密制度的建立。（三）根據上述需要，修正相關法令，建立必要的基本法制，好加速推動電子化政府。以下圖 6 為日本電子政府的推進體制。

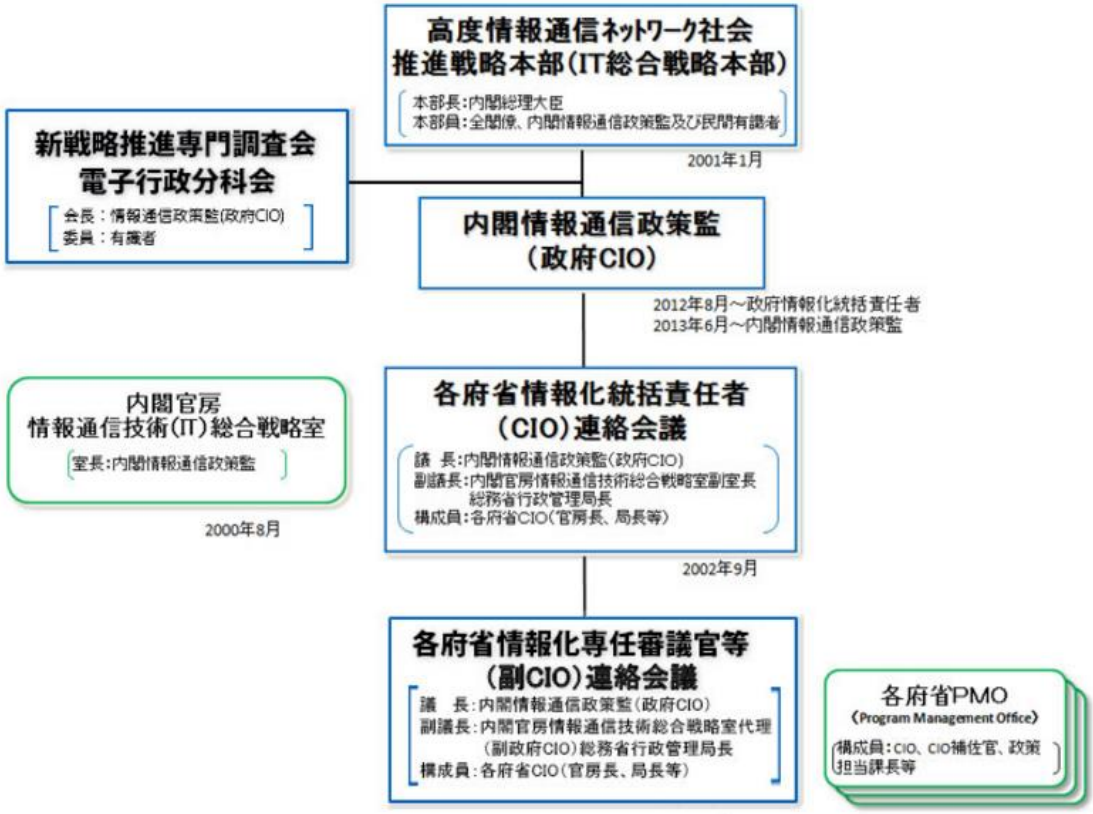

圖 6　日本電子政府的推進體制

資料來源：電子政府的總合窗口，〈日本の電子政府の推進体制〉，《電子政府的總合窗口 e-Gov》，<http://www.e-gov.go.jp/doc/promote/>。

《i-Japan2015 戰略》的第二個發展項目為推動醫療健康與資訊服務，目標為改善醫療體系，解決少子化、高齡化、醫生不足等相關問題。透過 IT 技術發展遠距醫療系統，並且建立「日本版的電子健康記錄」（日本版 EHR），[74]將民眾健

officer）的角色日漸趨重，資訊長的引進指標在未來的電子化政府評比的重要性亦相對增加。資訊長在電子化政府中扮演的角色包括政策的制訂者、IT 的策略規劃、IT 預算規劃、危機管控、產業創新的宣導者、e 化流程重整及位居溝通整合的關鍵位置等角色。請參閱：小尾敏夫，〈Development of e-Government and CIO toward Ubiquitous Society in Japan in Comparison with USA〉，《資訊社會研究》，第 12 期，2007 年 1 月，頁 49-55。

[74] 電子化的健康記錄（Electronic Health Record, EHR）為電子病歷（Electronic Medical Record, EMR）的最佳階段，將電子病歷做到個人化的健康紀錄。電子健康記錄是將醫院、健檢中心與藥局所掌握個人的健康資訊加以整合，提供給患者本身、醫護人員、研究人員、主管國民健康的政府機關等，其優點為：提高醫療品質與減少醫療過失，患者可根據過去就療紀錄繼續接受治療並且減少不必要的檢查，透過第二意見等選擇適合的醫療或健康服務；二是增加醫療與健康之研究品質，研究人員可透過大量的個人醫療與健康資料進行流行病或慢性病的

康資訊集中，減少因病歷資訊遺漏所衍生醫療誤診等情形。最後一項為教育與人才培育，將資訊科技融入教學，鼓勵學校在課堂教學中多加利用 IT 技術，例如導入電子白板等。以下表 4 為 2010 年之後日本的資通訊發展政策。

表 4　2010 年後日本的資通訊發展政策。

時間	政策名稱
2009 年 7 月 6 日	《i-Japan 戰略》（i-Japan Strategy 2015）
2010 年 5 月 11 日	《新資訊通信技術戰略》（A New Strategy in Information and Communications Technology）
2013 年 6 月 14 日	《世界最先端 IT 國家創造宣言（Declaration to be the World's Most Advanced IT Nation）》（分別於 2014 年 6 月 24 修定、2015 年 6 月 30 修定、2015 年 5 月 20 修定）。

資料來源：作者自行整理。

四、《世界最先端 IT 國家創造宣言》（Declaration to be the World's Most Advanced IT Nation）

2013 年日本政府又提出《世界最先端 IT 國家創造宣言》（Declaration to be the World's Most Advanced IT Nation），預期透過 IT 技術促進社會成長、活化城市與國民、建構全方位的社會、打造一站式的公共服務，同時持續強化人才培育、基礎建設、網路安全等基礎能量，提升日本 IT 技術與服務的國際競爭力。[75]其中，建構全方位社會納入了許多不同領域的 IT 應用發展，如：地方醫療照護、農業知識化、智慧交通、災害應對、能源管理等。根據 2016 年 5 月的修正版，三大推行重點為：（一）國家與地方的 IT 化與業務改革；（二）安全且安心的資料流通及多元應用之環境整備；（三）解決少子高齡化的社會問題。因此，相較於過去的政策發展，伴隨日本推動「個人編號（My Number）」制度，[76]及大數據

研究；三是增加醫療資源的分配效率，政府可根據各地居民的健康狀況分配醫療資源或加強特定的醫療項目。陳文欽，〈淺談電子病歷實務〉，《IT's 通訊》，2009 年，<http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1753>。

[75] IT Strategy Headquarters, "Declaration to be the World's Most Advanced IT Nation," *IT Strategy Headquarters*, June 13, 2013, <http://japan.kantei.go.jp/policy/it/2013/0614_declaration.pdf>.

[76] 日本從 2016 年 1 月起實施統一的社會保障與稅務號碼（My number，即個人身分識別號碼、個人編號）制度。政府依據居民基本資訊登記本，為每一位國民賦予一組 12 位數字終身不變的個人編號，用於社會保障、稅務、防災以及地方政府處理法律條例規定的各類事務等場合。此外，政府為提出申請的人發行個人編號卡（My number card），使用個人編號卡可以上網訪問「資訊提供記錄閱覽系統」上設置的個人主頁。在這個「資訊提供記錄閱覽系統」上，用戶可以 1.確認與自己個人編號相關的個人資訊操作記錄；2.確認資訊保管機構所保管有關個人編號的個人資訊；3.進行電子申請；4.確認行政機關等單位發送的通知。這是從以本人申請為前提的傳統行政服務模式轉變為政府通知個人的推播型行政服務模式。具體可以

（Big Data）時代的來臨，日本更強化政府的 IT 治理，希望能擴大 IT 範圍與產業競爭力。[77]以下表 5 為日本《世界最先端 IT 國家創造宣言》之目標與實施措施。

表 5　日本《世界最先端 IT 國家創造宣言》之目標與實施措施

目標	實施措施
成為一個鼓勵創新產業與服務成長之國家	1. 鼓勵開放資料與巨量資料之利用，包括促進私部門使用公部門資料、支持使用巨量資料發展新事業或服務。 2. 促進日本農業及相關產業運用 IT 將其轉化為智慧型產業並國際化，包括強化農業及相關產業競爭力、強化市場管理與發展。 3. 鼓勵創業及開放式創新。 4. 利用 IT 與資料活化地方。 5. 透過次世代廣播與電信服務之推動，提升影視產業之國際競爭力與發展新事業。 6. 2020 年東京奧運與殘奧會上運用強大 IT，以擴大 IT 範圍與產業競爭力。
成為一個民眾可以安心生活的國家	1. 提供適當的在地醫療與照護服務，以打造一個長壽的健康社會。 2. 打造一個世界最安全與最具抗災能力的社會，包括建立災難回應與損害降低系統、運用 IT 建立世界最安全與最經濟的社會基礎設施。 3. 針對家庭與社區推動有效率與穩定的能源管理機制。 4. 運用智慧運輸系統（Intelligent Transport Systems, ITS）發展全世界最安全、環境友善與經濟的道路運輸。

實現以下目標：1.中央和地方政府準確、高效地追蹤和共享社會保障所發放和負擔的資訊，從而避免少付、多付或雙重支付等問題，實現符合個人和家庭狀況、細緻周到的社會保障；2.稅務部門可以利用個人編號，高效匹配各種收入和扶養資訊，準確掌握個人收入情況；3.國民可使用自家電腦等終端便捷地閱覽自己的社會保障和稅收資訊記錄及利用相關服務的資訊，更易於接受各種必要的服務；4.中央和地方政府之間可適時交流申請手續所必需的資訊，這樣就減少了收入納稅證明、住所登記證明等資料附件，有利於簡化文書處理等手續工作，減輕國民、中央和地方政府的負擔，改善行政效率；5.標有「號碼」的智慧型個人編號卡，可以整合目前養老金手冊、醫療保險證、看護保險證的不同功能，提高國民生活的便利性。森信茂樹，〈マイナンバー制度：導入の意義と今後の活用〉，《nippon.com》，2015 年 10 月 28 日，<http://www.nippon.com/ja/currents/d00201/>。

[77] IT Strategy Headquarters, “Declaration to be the World's Most Advanced IT Nation,” *IT Strategy Headquarters*, May 20, 2016, <http://japan.kantei.go.jp/policy/it/2016/20160520_full.pdf>.

	5. 運用雲端運算及其他服務促進就業多元化與促成生活與工作之平衡。
成為一個可隨時隨地使用一站式公共服務的國家	1. 提供高度便利的電子政府服務。 2. 在中央與地方政府層級改善政府資訊系統。 3. 強化政府的 IT 治理。

資料來源：作者自行整理。

肆、日本面臨之網路安全威脅

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》（情報セキュリティ 10 大脅威—2017），[78]將此十大資訊安全威脅闡述如下：

一、針對性攻擊／鎖定目標攻擊（Targeted attack）。

此種攻擊可說是今日網際網路環境中對組織最大的網路威脅之一，[79]攻擊目標為鎖定在某個政府機關、民間企業或團體組織等，網路攻擊者常利用電子郵件裡的附加檔案和網頁外部儲存媒體（external storage）等方式，使電腦感染病毒（Virus），再透過遠端操作該電腦，使得其他電腦也遭受感染，此攻擊的最終目的，在於竊取電腦裡的高價值資訊和智慧財產權等重要情報。一旦針對性攻擊成功達到目的，將對組織造成極其嚴重的損害。攻擊者可能為情報人員、產業間諜或犯罪團體；被攻擊者為組織，如：政府機關、民間團體、企業或研究智庫等單位。

針對性攻擊／鎖定目標攻擊造成的影響，會因為目標和網路攻擊者的意圖而有所不同。最常見的是該組織或企業面臨業務中斷，企業無法進行日常作業和交易，因為此攻擊可能造成網路系統當機，企業必須緊急調派人手處理。另外，組織或企業所擁有的智慧財產權可能會被竊取、客戶資料外洩，甚至導致客戶陷於身份竊盜、敲詐、勒索或其他危險之中。不僅如此，企業或組織的信譽也會受到損害，財物上也可能遭受損失等等。針對性攻擊／鎖定目標攻擊常依循以下的步

[78] 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>。

[79] 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.

驟執行網路攻擊：

（一）擬訂網路攻擊計畫。

（二）調查攻擊標的，準備攻擊。

（三）初期潛入使電腦感染病毒。

（四）擴大病毒感染。

（五）內部侵入，調查或搜索重要資訊和情報。

（六）達成目的，向外傳送重要情報資料。

特別是在第三步驟「初期潛入使電腦感染病毒」中，網路攻擊者會為了成功感染目標電腦而使用非法手段，如：網路攻擊者會利用偽造簽名，透過電腦病毒攻擊目標電腦。案例一、日本大型旅行社（JTB）被駭，導致客戶資料外洩。2016 年 6 月，JTB 這間大型旅行社遭到針對性攻擊／鎖定目標攻擊，造成客戶的姓名、出生年月日、電子信箱、地址、電話號碼、護照號碼等個資外洩，約 678 名客戶受到影響。[80]此事件的開端為 2016 年 3 月，旅行社員工在使用電子信箱時，開啟了以客戶為署名的電子郵件中之附加檔案。在此之後，電腦遭到惡意病毒感染，網路攻擊者也透過遠端操作電腦，入侵該旅行社保管個人資料的伺服器。

案例二、日本經濟團體聯合會（經團聯）的電腦受到進階持續性威脅（APT）的攻擊。[81]2016 年 10 月底至 11 月初，經團聯事務局的 23 台電腦中，被判斷出有 10 台電腦與外部有可疑的通信情況。事後經調查，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。

案例三，日本富山大學受到針對性攻擊／鎖定目標攻擊。[82]網路攻擊者針對日本富山大學氫同位素科學研究中心進行針對性攻擊，個人情報和核能發電廠污水處理等相關研究成果可能已經外洩，而情報外流的原因為研究人員的電腦遭到病毒感染所致。

二、透過勒索／綁架病毒（Ransomware）向企業或組織勒索高額贖金。

所謂的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螢幕，或將裝置裡的資料進行加密，讓個人失去對系統或資料的控制，進而用來勒索被害人，被害人若要恢復系統或資料就必須被迫支付贖金以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，[83]2012 年勒索病毒從俄羅斯開

[80] 株式会社ジェイティービー，〈不正アクセスによる個人情報流出の可能性について―現状報告と再発防止策〉，《JTB Corp.》，2016 年 8 月 24 日，<https://www.jtbcorp.jp/jp/160824.html>。

[81] 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>。

[82] 富山大学，〈富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について〉，《富山大学》，2016 年 10 月 11 日，<https://www.u-toyama.ac.jp/news/2016/1011.html>。

[83] The Global Technical Support & R&D Center of TREND MICRO, “Ransomware: Past, Present and

始擴散到其他歐洲國家，[84]2013 年，「加密勒索病毒」開始浮出檯面，最有名的就是「CryptoLocker」病毒。到 2016 年新的勒索病毒家族數量爆增，2015 年發現有 29 個勒索病毒家族，2016 年所發現的勒索病毒家族來到 247 個，足足增長 752%，並且全都具備檔案加密的能力。[85]此種勒索病毒不單單將檔案加密而已，還會在受害者遲遲交不出贖金的期間逐批逐批的刪除檔案，受害者為了救回檔案，必須支付比特幣（Bitcoin）來換取解密金鑰。[86]

勒索病毒的散布方式會經由多種途徑進入電腦或各項裝置，如：（一）來自電子郵件附加檔案的感染。在電子郵件中的附加檔案附上勒索病毒，使被害人在開啟檔案時遭受感染；（二）精心特製的惡意網站。在電子郵件裡附上網頁連結使被害者連結並瀏覽遭到入侵的網站或竄改的網頁；（三）使被害者連結非法廣告而遭受惡意病毒感染，亦有直接將非法廣告顯示在電子郵件裡而受到病毒感染。

電腦防毒與網路安全廠商—趨勢科技，在 2016 年所偵測及封鎖的勒索病毒中，有 79%都是經由垃圾郵件散布；為了預防這種情況發生，除了平常要更新軟體之外，資料要定期備份，盡可能地作異地備份，也需要隨時掌握垃圾郵件所使用的社交工程技巧，如：一些熱門的節日、運動賽事、政治新聞、有趣的話題，或者與企業相關的新聞，都很可能成為歹徒引誘使用者下載勒索病毒的誘餌。未來勒索病毒可能演變成足以癱瘓所有基礎架構的惡意程式，不僅對企業營運造成威脅，很可能威脅一個城市，甚至一個國家，直到受害者支付贖金為止。網路攻擊者在不久的將來，很可能會攻擊工業控制系統（Industrial Control Systems, ICS）及其他關鍵基礎設施，不但可能癱瘓網路，甚至癱瘓整個產業生態體系。網路攻擊者最大的攻擊目標就是金融支付系統，如：2016 年美國舊金山灣區捷運系統（Bay Area Transit）自助付款機遭到勒索病毒感染的案例。[87]

案例一、勒索病毒被害案件爆增。2016 年和 2015 年相比，遭受勒索病毒威脅的被害者正在急遽增加當中。2016 年在日本國內偵測出勒索病毒的被害案件數為 6 萬 5 千件，比 2015 年的被害案件數 6 千 7 百件，高出 9.8 倍之多。[88]在這

Future," *Trend Micro*, 2017, pp. 2-7, <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>.

[84] 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/>.

[85] 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>.

[86] 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, pp. 6, <https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf>.

[87] Kristen Holland, "Update on SFMTA Ransomware Attack," *SFMTA*, November 28, 2016, <https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack>.

[88] 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>。

些案件中威脅被害者的內文，大多是以英文記載，但用日文記載的亦有被偵測出來。

案例二、善用解密工具處理遭到加密的檔案。日本現在已有網路安全公司提供解密工具，來復原這些遭到勒索病毒加密的檔案。除此之外，受害者在處理勒索病毒時，亦有拒絕勒索病毒的網站可以使用，如：The No More Ransom Project，這個網站是由「荷蘭國家警察高科技犯罪小組」（The National High Tech Crime Unit of the Netherlands' police）、歐洲刑警組織之下的「歐洲網路犯罪中心」（European Cybercrime Centre, EC3）、卡巴斯基實驗室（Kaspersky Lab）和英特爾網路安全公司所推動的計畫，上面提供多項解密工具供被害者使用。[89]或許解密工具並非能全部有效的解決勒索病毒所帶來的問題，但提供檔案復原的可能性。

三、漏洞攻擊。

利用網站服務（Web Services）安全上的漏洞竊取個人資料。由於有許多個人資料會註冊在各式各樣的網站服務裡，如：在購物網站上註冊重要的個人資料，包括：姓名、性別、出生年月日、信用卡資料等，或者是「社交網路服務」（Social Networking Service, SNS），除了有個人的註冊資料外，也記載著朋友或其他社群的資料，由於社交網站常常有大量的資訊分享、外部連結或廣告等，無疑是為駭客提供更多的引誘和犯罪途徑，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，針對網站應用程式漏洞的攻擊已相當普遍，這也是造成許多重大資訊安全事件的原兇之一。

漏洞攻擊的方法有：（一）網路應用程式在開發時產生的安全漏洞。由於在撰寫網路應用程式時，沒有慎重考慮到安全問題，造成許多網站應用程式存在安全漏洞。如：資料隱碼攻擊，指的是 SQL 語法上的漏洞，藉由特殊字元，改變語法上的邏輯，駭客就能取得資料庫的所有內容，進而造成資料庫損毀或資料流失；（二）利用軟體的安全漏洞。由於網路服務是由作業系統（Operating System, OS）[90]、中介軟體（Middleware）[91]、內容管理系統（Content Management Systems, CMS）等多數的軟體所構成，網路服務中也有共通使用的軟體，如：加密軟體

[89] 〈サイバー犯罪者に不当な支払いをせずに、ロックされたデバイスや暗号化されたデータを取り戻すためのサポートが必要ですか？〉，《No More Ransom》，<https://www.nomoreransom.org/zh/about-the-project.html>。

[90] 電腦硬體和應用程式之間的介面。對於個人電腦而言，最常見的作業系統包含 MacOS、Windows、DOS 和 Linux。

[91] 連接兩個其他單獨應用程式的應用程式。

（OpenSSL）[92]、網頁應用程式（Apache Struts）[93]、部落格軟體（WordPress）等，網路攻擊者能利用以上這些軟體上的安全漏洞來竊取大量資料或影響網站營運。

案例一、民營廣播公司不當的資料存取，導致 43 萬筆個人資料遭到外洩。日本電視局的網站發生資料存取不當的問題，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。[94]

案例二、化妝品銷售網站約 42 萬筆個人資料外洩。網路攻擊者利用系統的安全漏洞，竊取化妝品公司資生堂（IPSA）在網路商店約 42 萬件的客戶註冊資料，[95]包括：姓名、性別、出生日期、電話、地址、職業、電子信箱、購買歷史資料等。

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，[96]主要利用殭屍網路（Botnet）與系統弱點，對特定目標之企業或政府機關的網站，發送大量合法或偽造的連線請求，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、通訊之目的。分散式阻斷服務攻擊的目的並非是要竊取資料，而是要影響網路運作，導致使用者無法存取網路資源，這樣的攻擊可能會造成企業或政府機關的形象受損、客戶信心降低、智慧財產權損失等影響。

---

[92] OpenSSL 是相當普遍的網路加密軟體，網路上的資料傳輸都會透過「安全插槽層」（Secure Sockets Layer, SSL）和「傳輸層安全」（Transport Layer Security, TLS）來加密，用來確保資料傳輸的安全與隱私性。由於使用 OpenSSL 作為加密工具的裝置和設備相當多，包括網站伺服器、郵件伺服器、即時通訊伺服器、視訊設備或是防火牆等產品，皆可能使用 OpenSSL 來確保資料傳輸的安全。但是，許多使用 OpenSSL 的嵌入式系統，因為平常漏洞修補的更新頻率較低，因此存在高風險漏洞，被稱為 Heartbleed 漏洞，網路攻擊者會利用此漏洞入侵伺服器，取得機敏資訊或發動阻斷服務攻擊（DoS）。請參閱：行政院國家資通安全會報技術服務中心，〈重大漏洞專區─Heartbleed〉，《行政院國家資通安全會報技術服務中心》，<https://www.nccst.nat.gov.tw/Heartbleed?lang=zh>；黃彥棻，〈記得要更新！OpenSSL 又爆罕見高風險漏洞，官網預告 7 月 9 日釋修補〉，《iThome》，2015 年 7 月 8 日，<https://www.ithome.com.tw/news/97287>。

[93] Apache Struts 為一開源的網頁應用程式框架，主要用來開發 Java EE 網路應用程式，但特定版本 Apache Struts 2 存在允許網路攻擊者遠端執行任意程式碼的安全漏洞，進而可能導致機敏資訊外洩或遠端程式攻擊等風險，請參閱：行政院國家資通安全會報技術服務中心，〈Apache Struts 存在遠端攻擊漏洞〉，《行政院國家資通安全會報技術服務中心》，2017 年 9 月 27 日，<https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16003>。

[94] 〈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>。

[95] 〈クレカ情報 5.6 万件含む個人情報 42 万件が流出した可能性─イプサ〉，《Security NEXT》，2016 年 12 月 2 日，<http://www.security-next.com/076305>。

[96] 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。

近期大型的 DDoS 攻擊案例大多為混合式攻擊，發動來源皆以物聯網（Internet of Things, IoT）裝置為主，因為 IoT 裝置普遍不具資訊安全的防護能力，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，而且 IoT 設備用途單純，長期不關機，因此，隨著 Mirai 殭屍病毒的釋出，將針對 IoT 裝置發起更複雜的 DDoS 攻擊。[97]所有 IoT 攻擊中有 60%源於亞洲，21%源於歐洲、中東和非洲，19%則來自美洲。[98]網路攻擊者不只利用物聯網裝置，還會盡可能尋找更多不同類型的裝置來發動 DDoS 攻擊。

DDoS 攻擊的手段有：（一）利用殭屍網路，網路攻擊者利用殭屍網路，將受感染的電腦在指定的日期和時間，對特定目標受害者、企業或政府機關發動攻擊，這樣大規模同步攻擊的結果，將造成目標網站伺服器緩衝區溢位問題（buffer overflow）[99]，導致整個網站和服務中斷運作；（二）反射性 DDoS 攻擊，是指網路攻擊者利用被控制的多台殭屍電腦，在成功偽照目標主機的 IP 位址後，對多台管理不夠嚴謹的主機，發出詢問封包並要求回覆，而這些被詢問的主機群，回覆大量封包給偽照 IP 位址時，造成真正的目標主機接收來自四面八方的回覆封包，進而造成放大且反射的攻擊效果。[100]這種網路攻擊方式也能達到 DDoS 放大攻擊的效果，造成目標主機無法正常存取網路資源，並增加網路攻擊者被追查到的難度；（三）DNS 洪水攻擊，網路攻擊者會對 DNS 伺服器，送出許多 DNS 快取資料的網域名稱解析請求，增加 DNS 伺服器與網路頻寬的負擔。[101]

案例一、特定訴求為目的之 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（日本格付研究所；Japan Credit Rating Agency, JCR）、日本住宅金融支援機構（Japan Housing Finance Agency）等單位的網站，受到「國際駭客組織」（国際的ハッカー集団）匿名者（Anonymous）的網路攻擊，攻擊的理由與日本重啟南極捕鯨活

---

97 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>。

98 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>.

99 緩衝區溢位（buffer overflow）是指應用程式會騰出一些記憶體區域，及緩衝區作為儲存空間，如果應用程式嘗試儲存更多資料，導致大小固定的緩衝區無法容納時，則會出現緩衝區溢位問題。當網路攻擊者所能傳送的資料超出應用程式緩衝區的限制，再加上應用程式又沒有採取安全檢查措施時，緩衝區溢位攻擊就此發生，請參閱：賽門鐵克（Symantec），〈詞彙查詢：緩衝區溢位〉，《安全機制應變中心》，<https://www.symantec.com/zh/tw/security_response/glossary/define.jsp?letter=b&word=buffer-overflow>。

100 李美雯，〈WordPress Pingback DDoS 攻擊分析〉，《臺灣大學計算機及資訊網路中心電子報》，2016 年 2 月 18 日，頁 3-5，<http://cert.ntu.edu.tw/Document/TechDoc/Analysis_of_WordPress_Pingback_DDoS_Attack.pdf>。

101 陳宏儒，〈阻斷式服務攻擊的演進與應對之道〉，《麟瑞科技》，2015 年 1 月 30 日，<http://www.isac.org.tw/spaw2/uploads/images/2.LR_0128.pdf >。

動有關，該匿名者在推特（Twitter）上提到「捕鯨並非文化的特權」。[102]網路攻擊者為宣揚特定理念，頻繁以日本為對象發動網路攻擊。

案例二、勒索金錢為目的之 DDoS 攻擊。有些 DDoS 攻擊是由激進駭客（Hacktivist）所為，如：比特幣勒索團體（DDos for Bitcoin, DD4BC）。他們威脅受害者必須支付相當金額的比特幣，否則將發動 DDoS 攻擊，一旦發動 DDoS 攻擊，受害者必須支付更高額費用給比特幣勒索團體。[103]該團體於 2014 年 7 月開始出現，初期以勒索線上遊戲及貨幣兌換平台為主，後來擴大勒索對象到金融服務業、媒體娛樂業及零售產業等。2016 年 1 月歐洲刑警組織（Europol）以代號「Operation Pleiades」的多國聯合調查行動中，逮捕 DD4BC 的核心成員。多國聯合調查行動中包括許多歐洲國家與美國、日本、澳洲等非歐洲國家也共同參與其中。[104]

案例三、殭屍網路的病毒擴散。DDoS 攻擊的規模、影響程度和發生頻率將逐年提高，成為具威脅性的網路攻擊。在 2013 年、2014 年與 2015 年，最大規模的網路攻擊分別達每秒 300Gb、400Gb 與 500Gb，[105]2016 年首次有兩波 Tb 等級的網路攻擊。[106]DDoS 攻擊所造成的威脅逐步提高，主要與三項發展趨勢有關：（一）不安全的物聯網裝置日益增加，如：連網的相機或數位攝影機，這些裝置較易遭到殭屍網路入侵，成為駭客攻擊目標；（二）網路上可以輕易取得惡意軟體，如：Mirai 的攻擊教學，業餘駭客只要透過不安全的物連網裝置，就可以發動網路攻擊；（三）頻寬速度增加，由於 GB 等級的網路速度提升，使用超高速寬頻的消費性電子產品增加，使殭屍網路入侵的裝置可以傳輸更多的垃圾資料。[107]日本獨立行政法人情報通信研究機構（NICT）調查，殭屍網路造成的攻擊案例，2015 年為 1,960 萬件，2016 年已經急速增加至 1 億 2,600 萬件，增長 6.4 倍之多，[108]案件急速增長被認為和殭屍病毒（Mirai）原始程式碼公開有極大的關聯。

---

[102] 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>。

[103] 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 58-67。

[104] 末岡洋子，〈ユーロポール、セブン銀行など攻撃の DDoS 攻撃グループ「DD4BC」を逮捕〉，《株式会社マイナビ》，2016 年 1 月 14 日，<https://news.mynavi.jp/article/20160114-a549/>。

[105] 電腦記憶容量單位 1TB= 1,024GB= 1,048,576 MB= 1,073,741,824KB。規模 1GB 的網路攻擊通常就足以癱瘓大部分企業組織的網際網路連線能力，迫使企業離線，造成網路中斷、收入損失或損害商譽等情事發生，請參考：Arbor Networks，〈DDoS：風險已激增，你知道嗎？〉，《Arbor 白皮書：真相揭露─關於 DDoS 攻擊的 3 個迷思》，頁 2-3，<https://www.g2easia.com/__novadocuments/344387?v=636262094744670000>。

[106] Cisco, “The Zettabyte Era: Trends and Analysis,” June 7, 2017, <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html#>.

[107] 陳明煇，〈2017 高科技、媒體及電信產業趨勢報告〉，《勤業眾信 Deloitte》，2017 年 1 月 12 日，頁 7-10，<https://www2.deloitte.com/tw/tc/pages/technology-media-and-telecommunications/articles/2017-tmt-predictions.html>。

[108] 〈ＩｏＴ製品乗っ取りサイバー攻撃１億２６００万件…家電や通信機器から発信 昨年、

五、人為因素。

近年來各式各樣的雲端服務、新興的網路與通訊軟體蓬勃發展，雖然強化了員工之間聯繫上的簡便，但一不小心，可能在彈指間就洩漏了公司或政府機關的機密文件，包括重要客戶名單、商業機密、重要文件等。為了防止內部員工的不當行為，除了設立法律規章和懲罰條例等對策外，更應建立專業自動化的管控稽核機制，這樣才能逐漸降低企業在資料管理上的風險。

企業或政府機關的內部威脅較容易發生在「不滿員工」的身上，有些員工不滿遭到解雇或降低薪資等原因，會產生竊取企業內部資料等報復行為。或者是企業不當地給予取得資料的權限，由於取得資料權限的管理愈趨複雜，有些企業可能對此掌握不佳，使原本沒有取得資料權限的員工竟能夠獲得企業重要情報或機敏資料，或者具有特殊權限的使用者，如：網路工程師、資料庫管理者、資訊安全人員能輕易取得企業的機敏資料等。因此，企業或政府機關需要更完善的管理規章或導入自動化的管控稽核機制來防範機敏資料的外洩。

案例一、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。[109]該公司的前職員不當攜出公司的客戶資料，並將資料放在網路上保存，使第三者能夠在網路上查看，而一部分的客戶資料已經被證實遭到閱覽。

案例二、員工攜出企業資料卻因醉酒不慎遺失。[110]員工不理會企業禁止攜出資料的安全條例，將保存個人資料的業務用硬碟（hard disk）攜出，在回家途中由於喝得爛醉，不慎將硬碟弄丟。該員工表示，是為了在自家工作才會將硬碟攜出。

六、水坑式攻擊（Watering Hole）。

水坑式攻擊為最精巧的針對性攻擊形式，攻擊者首先滲透完全合法的網站，植入惡意程式碼，接著靜靜等待目標登入該網站，即可監控遭到滲透網站的活動紀錄。攻擊者從觀察潛在目標的過程，得以選擇某些受害者感興趣的網站特質，並且經常造訪某些特定網站，這種攻擊技巧之所以能發揮效果，在於受害者不會對合法網站有戒心，而且完全不知道有人可能已在此網站內植入惡意程式碼。[111]2013 年最受矚目的網路安全事件為 Twitter、Facebook、Apple、Microsoft 等知

前年の６倍に〉，《産経 WEST》，2017 年 1 月 20 日，<http://www.sankei.com/west/news/170120/wst1701200014-n1.html>。

109 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/>。

110 Security NEXT，〈職員が持出データを酒に酔って紛失─川口市〉，《Security NEXT》，2016 年 10 月 14 日，<http://www.security-next.com/074773>。

111 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>.

名網路服務公司受到水坑式攻擊。[112]

水坑式攻擊好比在非洲大草原上，獅子會在水池附近靜待與觀察前來喝水的動物一般。首先駭客會觀察攻擊目標瀏覽哪些網站，鎖定這些網站後再入侵並植入惡意程式，等到攻擊目標瀏覽這些網站後就此被感染了。許多水坑式攻擊會結合零時差漏洞(Zero-day Vulnerabilities)[113]或是在網頁上插入 Java Script 或 HTML 碼，當攻擊目標瀏覽被感染的網頁時，電腦會自動下載一個惡意檔案，這個檔案會引導攻擊目標到 C&C 伺服器（Command and Control Server）下載真正的惡意程式，而且這個惡意程式會隨時作更新，避免被防毒軟體偵測到，進而提高攻擊的成功率。[114]

案例一、網路攻擊者竄改飛機時刻表網頁，導致受害者連結至外部網站。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，誘導客戶連結到指定的外部網站，[115]產生這樣的原因有以下兩點，（一）管理用的電腦受到病毒感染後，存在電腦中的帳號與密碼被竊取；（二）網頁應用程式存在著安全漏洞，讓網路攻擊者可以輕易取得管理權限。

案例二、網路攻擊者竄改動物園網頁。日本東京動物園・水族園的活動布告欄上寫著「你被駭客入侵了」和「給我讓動物恢復自由」等字樣，由於網頁受到竄改與攻擊，使動物園被迫暫時關閉網頁。[116]

七、非法登入攻擊。

2016 年有許多網路服務的帳號、密碼遭竊，因為使用者為了方便記憶，常會使用相同的帳號、密碼，一旦這些帳號、密碼被盜，就可以用來闖入其他系統。遭到非法登錄的案件中多數是使用整合式清單（List-Based Attack）的攻擊手段，網路攻擊者利用從其他網路服務取得的帳號密碼組合，不斷的重複嘗試登入。為因應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），[117]如此可以防止非法登入攻擊，能更妥善的保護資

---

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

113 所謂零時差漏洞（Zero-day Vulnerabilities, 0day）是指軟體程式中的未知弱點或漏洞，軟體開發人才得知此漏洞但來不及進行修補。

114 廖珮君，〈與其假造不如入侵合法網站，水坑式攻擊成 APT 最新手法〉，《資安人》，2013 年 4 月 29 日，<https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7413#ixzz2dp0QRIJE>。

115 〈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>。

116 東京動物園協会，〈都立動物園・水族園のホームページへの不正アクセスについて〉，《東京都庁》，2016 年 7 月 8 日，<http://www.metro.tokyo.jp/INET/OSHIRASE/2016/07/20q78600.htm>。

117 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

料與系統。

非法登入攻擊的手段有：（一）整合清單式攻擊（List-Based Attack），網路攻擊者利用在其他網站服務中取得的帳號與密碼組合，進行非法登入。在多個網站都使用相同帳號、密碼的情況下，只要有其中一組的帳號、密碼遭到外洩，其受害程度也會擴及其他網站；（二）推測密碼的攻擊行為，網路攻擊者可能推測使用者的密碼，並嘗試進行非法登錄，舉例來說，帳號和密碼一致，或者密碼是由一串單字組成，如：「123456」或「abcdef」這種連續使用阿拉伯數字或英文字母的情況下，都有可能被網路攻擊者推測出來。此外，密碼採用像是「qwerty」這樣鍵盤上鄰接的一列單字，也容易被網路攻擊者推敲出密碼。

案例一、部落格（Blog）網站遭到非法登錄。日本知名部落格網站「Ameba」，在 2016 年 5 月和 11 月時皆曾被網路攻擊者非法登錄，特別是在 11 月時，證實約有 59 萬件的非法登入情形。此外，調查發現，部落格網站的非法登錄很有可能是在其他網站服務中不慎外流密碼所導致。[118]

案例二、Big Camera 購物網站遭到非法登錄，紅利點數被不當利用。日本大型連鎖電器行 Big Camera 官方購物網站，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。[119]此外，客戶的姓名、地址、電子郵件、購買紀錄等資料已被第三者所閱覽。在此事件中，可能是客戶在瀏覽其他網站時，密碼不慎外流所導致。

案例三、社交網路服務網站「pixiv」遭到非法登錄。「pixiv」為日本插畫藝術作品的社交網路服務網站，由日本藝術家所組成的虛擬社群，可以投稿插畫、動漫等作品。不過，2016 年 11 月 29 日到 12 月 2 日遭到整合清單式攻擊（List-Based Attack），造成約 3,600 件帳號遭到非法登錄，而註冊在上面的電子郵件、出生年月日、性別等個人資料也可能已經被攻擊者瀏覽。[120]

八、物聯網裝置興起加劇網路攻擊。

許多連網的裝置就像蟄伏的間諜一樣，直到被網路攻擊者攻擊之前都不具威脅。但越來越多不安全的物聯網裝置，則加劇 DDoS 網路攻擊，這些裝置包括：攝影機、數位錄影機、路由器或其他裝置等。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、

（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。

118 山川晶之、飯塚直，〈「Ameba」で約 59 万件の不正ログイン--パスワードリスト型攻撃で〉，《CNET Japan》，2016 年 11 月 30 日，<https://japan.cnet.com/article/35092962/>。

119 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>。

120 pixiv 事務局，〈pixiv の一部アカウントに対する「なりすましログイン」の報告とパスワード変更のお願い〉，《pixiv》，2016 年 12 月 2 日，<https://www.pixiv.net/info.php?id=3897>。

密碼的手續繁複、操作流程麻煩，或者認為物聯網裝置沒有內建的螢幕或鍵盤，因此不願重新設定帳號、密碼，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，[121]即使使用者想要更改帳號、密碼，也無法自行重新設定。而車聯網（Connected Car）和聯網醫療裝置的安全漏洞則持續被公開，2015 年 8 月，研究人員 Charlie Miller 和 Chris Valasek 在美國黑帽大會（Black Hat show）上展示網路攻擊 Jeep Cherokee，透過汽車上的無線網路系統取得入侵途徑，並能夠遠端控制汽車引擎和剎車。[122]而滲透測試工程師 Mark Collao 在 Derbycon 2015 駭客會議上揭露，網路上可以搜尋到數百個可以公開存取的醫療系統，發現可聯網的醫療裝置存在安全漏洞，[123]這可能使救命的醫療裝置變成害命裝置，這不僅攸關病患的個人隱私，甚至還會對患者造成生命上的威脅。

雖然物聯網能讓工業環境更有效率，但駭客可能對工業控制系統（ICS）進行網路攻擊。[124]在 2017 年 10 月，美國國土安全部（U.S. Department of Homeland Security, DHS）與美國聯邦調查局（FBI）共同發出聯合聲明，證實工業控制系統（ICS）遭受駭客攻擊的案例已經擴大到能源、核能與供水等公用事業單位。針對工業控制的網路攻擊實例中，2010 年伊朗核設施遭受網路攻擊事件最具代表性，震網病毒（Stuxnet）是專門攻擊工業控制系統的電腦蠕蟲，針對伊朗核設施的工業控制軟體和設備進行攻擊，Stuxnet 感染伊朗國內 60%的個人電腦，癱瘓伊朗約 6 分之 1 的鈾濃縮工廠，伊朗首座核電站—布什爾核電站（GETTY IMAGES）數名員工的個人電腦遭到入侵，估計延緩伊朗的核武發展至少 18 到 24 個月左右。[125]另一個案例是，烏克蘭電廠的網路安全事件。2015 年 12 月 23 日烏克蘭電力網路受到駭客攻擊，造成約 22 萬人停電，[126]此為駭客攻擊造成大

---

121 KrebsonSecurity, “Hacked Cameras, DVRs Powered Today’s Massive Internet Outage,” KrebsonSecurity, October 21, 2016, <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>.

122 Cara West-Wainwright, “Is Your Car Connected or Protected,” *TREND MICRO*, August 4, 2015, <http://blog.trendmicro.com/is-your-car-connected-or-protected/>.

123 行政院國家資通安全會報技術服務中心，〈美國 FDA 發布醫療裝置網路安全準則草案〉，《行政院國家資通安全會報技術服務中心》，2016 年 2 月 2 日，<https://www.nccst.nat.gov.tw/NewsRSSDetail?seq=15455>。

124 工業控制系統（Industrial control systems, ICS）包括以下幾種系統，如：分散控制系統（Distributed Control systems, DCS）、監控和資料擷取系統（Supervisor Control And Data Acquisition, SCADA）、工業自動化系統（Industrial Automation system, IAS）、工業自動化和控制系統（Industrial Automation and Control Systems, IACS）、可程式設計邏輯控制器（Programmable Logic Controller, PLC）。工業控制系統主要是管理關鍵基礎設施，如：發電廠、自來水和污水處理廠、石油和瓦斯煉油廠、機場和捷運等交通運輸設施及與這些控制系統高度關聯的基礎設施或相互依賴之相關系統，請參閱：陳興忠、劉泰瑋，〈工業控制安全的現況與分析〉，《台網中心電子報》，2016 年 12 月，<http://www.myhome.net.tw/2016_12/p02_02.htm>。

125 行政院國家資通安全會報技術服務中心，〈關鍵基礎設施資安防護〉，《行政院國家資通安全會報技術服務中心》，2017 年 6 月 15 日，頁 2-8。

126 藍弋丰，〈烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論〉，《Tech News 科技新報》，2016 年 4 月 26 日，<https://technews.tw/2016/04/26/ukraine-power-system-phishing-information-security-protection/>。

規模停電事件，駭客攻擊的手法為，先對電廠員工進行魚叉式網路釣魚（Spear phising），取得員工登入權後，利用遠端登入電廠系統，啟動斷路器截斷電力，然後變更密碼，使電廠員工無法登入系統重啟電力。因此，工業物聯網（IIoT）的發展趨勢也將為企業和國家帶來前所未有的網路安全危機與影響。

案例一、日產（Nissan）Leaf 電動汽車的安全漏洞。2016 年 2 月，一位網路安全研究人員 Troy Hunt 發現 Nissan Leaf 電動汽車容易受到駭客攻擊，原因是車載系統的漏洞，允許駭客進行遠端操控汽車內部冷氣等溫度控制系統，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動汽車的電力，帶給車主不必要的麻煩與損失。Hunt 指出，這個問題的根源在於 NissanConnect 的應用程式，僅需要輸入汽車的車輛識別碼（Vehicle Identification Number, VIN），就能遠端控制該車輛。[127]

案例二、嬌生（Johnson & Johnson）公司生產的胰島素注射幫浦 Animas OneTouch Ping 存在安全漏洞。[128]這款胰島素注射幫浦是提供糖尿病患者隨身配戴，透過導管注射胰島素到病患體內，以維持體內正常血糖的醫療設備。由於這個注射幫浦配有無線遙控器，為了使病患能透過遙控器操控該設備，但因為該無線遙控器裝置出現安全漏洞，使得駭客有機會駭入該設備中。2016 年 10 月，嬌生對於該設備的安全漏洞發出警訊聲明，隔年 2017 年 10 月 Animas 公司即宣布停止生產和銷售此款胰島素幫浦設備。

九、網路攻擊走向商業化。

網路犯罪團體在黑市取得的攻擊技術已經越來越高超，甚至越來越商業化。像是使用勒索病毒的駭客集團，不但擁有廣泛的技術資源和高效率的團隊，甚至還建立客服中心，向受害者解釋如何付款解鎖，將整個犯罪行為提升到企業服務的等級。例如：俄羅斯的地下市場，聘雇一個駭客發動 DDoS 攻擊，一天約 30 到 70 美元，一個月約 1,200 美元；入侵團體組織的電子郵件 500 美元；植入 2,000 台殭屍電腦（bots）約 200 美元等；[129] 有些駭客組織推出各種月付方案，如：月付 69.99 美元，客戶即可使用 DDoS 攻擊服務。像是 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的目的，以吸引潛在客戶。[130]

---

[127] 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>。

[128] Japan Vulnerability Notes, “Animas OneTouch Ping に複数の脆弱性,” *JVN*, October 5, 2016, <https://jvn.jp/vu/JVNVU95089754/>.

[129] 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。

[130] 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>。

有些駭客集團會利用黑市銷售或出租「漏洞攻擊包」（Exploit Kit），漏洞攻擊包就像潘朵拉的盒子一般，裡面包括許多網路攻擊所需使用的惡意軟體，如：網路銀行木馬 Zeus、Vawtrak、勒索軟體 Nymaim、Ransomware、比特幣病毒 CTB-Locker 等，漏洞攻擊包的出租費用區分為：24 小時 30 美元、一周 150 美元、一個月 500 美元不等。[131]當受害者的瀏覽器被引導到存有漏洞攻擊包的網站後，漏洞攻擊包就會攻擊瀏覽器及其應用程式，如：Microsoft Silverlight、Adobe Flash 及 Reader 等，造成系統感染惡意程式，以致使用者的資料被盜或電腦檔案遭到強行加密進行勒索，甚至成為殭屍電腦發動網路攻擊等情況。

案例一、銀行木馬（Shifu）針對日本銀行發動攻擊。IBM 安全研究團隊 X-Force 公布 Shifu 是一個高度精密的銀行木馬，此命名為日語的「小偷」，因為攻擊目標鎖定日本的 14 家銀行。[132]這個銀行木馬能竊取大量受害者用於認證的各種資訊，利用鍵盤紀錄程式紀錄密碼，竊取用於銀行應用程式的私密憑證，讓網路攻擊者使用客戶的銀行憑證進行認證，並接管這些銀行帳戶進行非法轉帳。

案例二、13 個歐美國家共同執法，聯手逮捕付費使用 DDoS 攻擊的服務者。歐洲網路犯罪中心（EC3）與 13 個國家跨國合作，針對 DDoS 攻擊服務使用者進行跨國聯合犯罪打擊行動，一共逮捕 34 名付費使用 DDoS 攻擊服務的使用者，這些使用者大多為二十歲以下的年輕人，他們針對政府機關、遊戲服務商或學校單位的網站發動洪水攻擊。歐洲刑警組織（Europol）表示，希望藉由這次逮捕行動，可對付費使用網路攻擊服務的人而言，達到警告的效果。[133]

十、網路金融犯罪。

由於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，但安全方面是許多用戶對於網路銀行最大的顧慮。網路攻擊者可能利用病毒感染和網路釣魚（Phishing）的方式，竊取客戶在網路銀行的認證資訊，進而盜取個人資料或執行任意轉帳等非法行為。

網路攻擊者會使用許多方式竊取客戶的網路銀行資料，如：（一）植入木馬病毒（Trojan Horse）。木馬病毒能攻擊受害者的電腦，在電腦上顯示出對話視窗或圖片，這個對話視窗或圖片會假冒成網路銀行網站，進而要求用戶輸入個人的帳號和密碼。或者，「鍵盤側錄」程式會監視客戶使用電腦的行為，客戶一旦登入木馬列表中的網路銀行網站時，木馬病毒就會開始擷取使用者在鍵盤上輸入的資料，這樣網路攻擊者就能夠竊取用戶的個人資料或執行非法轉帳，盜取客戶的

---

131 Cale Guthrie Weissman, “Some hackers make more than $80,000 a month - here's how,” Business Insider, July 14, 2015, <http://www.businessinsider.com/we-found-out-how-much-money-hackers-actually-make-2015-7>.

132 Denis Laskov, “Shifu: ‘Masterful’ New Banking Trojan Is Attacking 14 Japanese Banks,” *Security Intelligence*, August 31, 2015, <https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/>.

133 蘇文彬，〈美、法、英等歐美 13 國大執法，聯手打擊 DDoS 攻擊服務使用者〉，《iThome》，2016 年 12 月 28 日，<https://www.ithome.com.tw/news/110677>。

財務；（二）網路釣魚（Phishing）。網路釣客常常會模仿知名網路服務公司的網站，架設以假亂真的山寨網頁或使用變造的網址，如：www. yhaoo.com.tw，再發送主旨為緊急通知的電子郵件，要求使用者執行電子郵件的連結，進而更改帳號、密碼或信用卡密碼等資料。為了引誘使用者輸入自己的個人資料，電子郵件內會聲稱，如果不輸入相關資訊，帳號就會被凍結。一旦用戶按下此連結，連結到假網站的同時，很可能會啟動惡意軟體，惡意軟體即開始記錄使用者登入的帳戶資料並立即回傳給釣客，以獲取不當利益。

案例一、網路銀行存款盜轉事件層出不窮。根據日本警察廳調查指出，2016年網路銀行非法轉帳的案件為 1,291 件，整體受害金額約為 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。[134]網路銀行遭駭客入侵盜領客戶存款事件頻傳，顯示出網路金融問題的嚴重性，如滾雪球般越演越烈。

案例二、惡意電子郵件（Malicious Email）癱瘓電腦系統。惡意電子郵件通常被稱為垃圾郵件（SPAM）或廣告信，泛濫的垃圾郵件已是各國所重視的重要問題。根據 SPAMHAUS 統計，到 2017 年 11 月 28 日為止，全球垃圾郵件量前五大國家，依序為美國、中國大陸、俄羅斯、烏克蘭、日本。[135]駭客最常使用電子郵件來發動網路攻擊，透過一次網路攻擊，即可對外發出 400 封以上夾帶病毒的電子郵件。[136]由此可見，網路攻擊者認為電子郵件是阻力最小的攻擊途徑，因為可以避開許多網路安全防護，達到攻擊效果。

伍、日本網路安全發展之對策

一、日本網路安全之組織體制

（一）中央政府

日本負責網路安全的組織機關分為三大部分，包括中央政府、各省廳及行政法人等三個層次。其中，負責網路安全之中央機關出現數次變革。2000 年 2 月 29 日，日本政府成立「資訊安全對策推進會議」（情報セキュリティ対策推進会議），議長為內閣官房副長官，成員包括各省廳官房長；同時，作為「資訊安全對策推進會議」的事務性機關，日本內閣官房設立「資訊安全對策推進室」（情報セキュリティ対策推進室）。「資訊安全對策推進會議」和內閣官房「資訊安全對策推進室」在這段時間內，為日本網路安全重要的中央主管機關，負責制定

134 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，<https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf>。

135 SPAMHAUS, “The World's Worst Spam Enabling Countries,” *SPAMHAUS*, November 28, 2017, <https://www.spamhaus.org/statistics/countries/>.

136 岡本勝之，〈2016 年個人の三大脅威：ネットバンキングを狙う「オンライン銀行詐欺ツール」〉，《TREND MICRO》，2017 年 1 月 13 日，<http://blog.trendmicro.co.jp/archives/14247>。

網路安全等政策法規、分析網路安全態勢、組織協調各省廳的網路安全相關事務等。[137]2004 年 12 月 7 日，日本「IT 戰略本部」通過《重新審視政府在資訊安全問題方面的作用與機能》（情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて），[138]決議方案指出要在「IT 戰略本部」下設置「資訊安全政策會議（臨時名稱）」（情報セキュリティ政策会議（仮称）），同時重組現有的內閣官房「資訊安全對策推進室」，在內閣官房下設置「國家資訊安全中心（臨時名稱）」（国家情報セキュリティセンター（仮称））。2005 年 4 月 21 日，日本正式成立內閣官房「資訊安全中心」（情報セキュリティセンター（NISC）），[139]相應廢止內閣官房「資訊安全對策推進室」。2005 年 5 月 30，日本「IT 戰略本部」正式設置「資訊安全政策會議」（情報セキュリティ政策会議），並規定議長由內閣官房長官擔任，代理議長由資訊通信技術擔當大臣擔任，其成員包括國家公安委員會委員長、防衛廳長官、總務大臣、經濟產業大臣、厚生勞動大臣、國土交通大臣及專家學者等，同時廢止「資訊安全對策推進會議」。[140]由以上整理發現，在議長及成員級別方面，「資訊安全政策會議」高於「資訊安全對策推進會議」。自此，「資訊安全政策會議」及內閣官房「資訊安全中心」成為負責日本網路安全的中央主管機關。

2015 年 1 月 9 日，日本政府根據《網路安全基本法》（サイバーセキュリティ基本法）的規定，將「資訊安全政策會議」及內閣官房「資訊安全中心」分別升格為「網路安全戰略本部」（サイバーセキュリティ戦略本部；Cybersecurity Strategic HQs, CSSHQ）與「內閣網路安全中心」（内閣サイバーセキュリティセンタ；National Center of Incident readiness and Strategy for Cybersecurity, NISC）。[141]「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、資訊通信技術大臣、東京奧運會擔當大臣及專家學者等。[142]「內閣網路安全中心」主任由「國家安全保障局」（National Security Secretariat,

---

137 情報セキュリティ基本問題委員会，〈第 1 次提言の概要─情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて〉，《内閣サイバーセキュリティセンタ》，平成 16 年 11 月 16 日，<https://www.nisc.go.jp/conference/kihon/index.html>。

138 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），〈情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて〉，《ＩＴ戦略本部》，平成 16 年 12 月 7 日，<https://www.kantei.go.jp/jp/singi/it2/kettei/041207minaosi.html>。

139 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》，平成 17 年 4 月 20 日，<http://www.nisc.go.jp/about/pdf/050420-kisoku.pdf>。

140 第三次「資訊安全政策會議」出席者名單中，議長為內閣官房長官安倍晉三、代理議長為資訊通信技術擔當大臣松田岩夫。情報セキュリティ政策会議，〈第３回情報セキュリティ政策会議出席者名簿〉，《内閣サイバーセキュリティセンタ》，平成 17 年 12 月 13 日，<https://www.nisc.go.jp/conference/seisaku/dai3/pdf/3siryou01.pdf>。

141 内閣サイバーセキュリティセンタ，〈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》，<https://www.nisc.go.jp/about/details.html>。

142 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

NSS）次長擔任，下轄 2 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、經濟產業省、警察廳等各省廳派駐人員及相關 IT 企業的職員。[143]相較於「資訊安全政策會議」設置於「IT 戰略本部」之下，「網路安全戰略本部」則直接設置於內閣之中，其位階因此得到提升；而「內閣網路安全中心」主任由「國家安全保障局」次長、內閣官房副長官補兼任，其地位也由內閣官房下屬提升為內閣直屬，因此，再次顯示首相官邸對日本網路安全的重視。[144]下圖 7 為日本網路安全政策的推進體制。

セキュリティセンタ》，平成 28 年 4 月 1 日，<https://www.nisc.go.jp/conference/cs/pdf/meibo.pdf>。

143 内閣サイバーセキュリティセンタ，〈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》，<https://www.nisc.go.jp/about/organize.html>。

144 内閣官房，〈内閣官房の組織図〉，《内閣官房》，平成 29 年 8 月 8 日，<http://www.cas.go.jp/jp/gaiyou/pdf/h290808_sosikizu.pdf>。

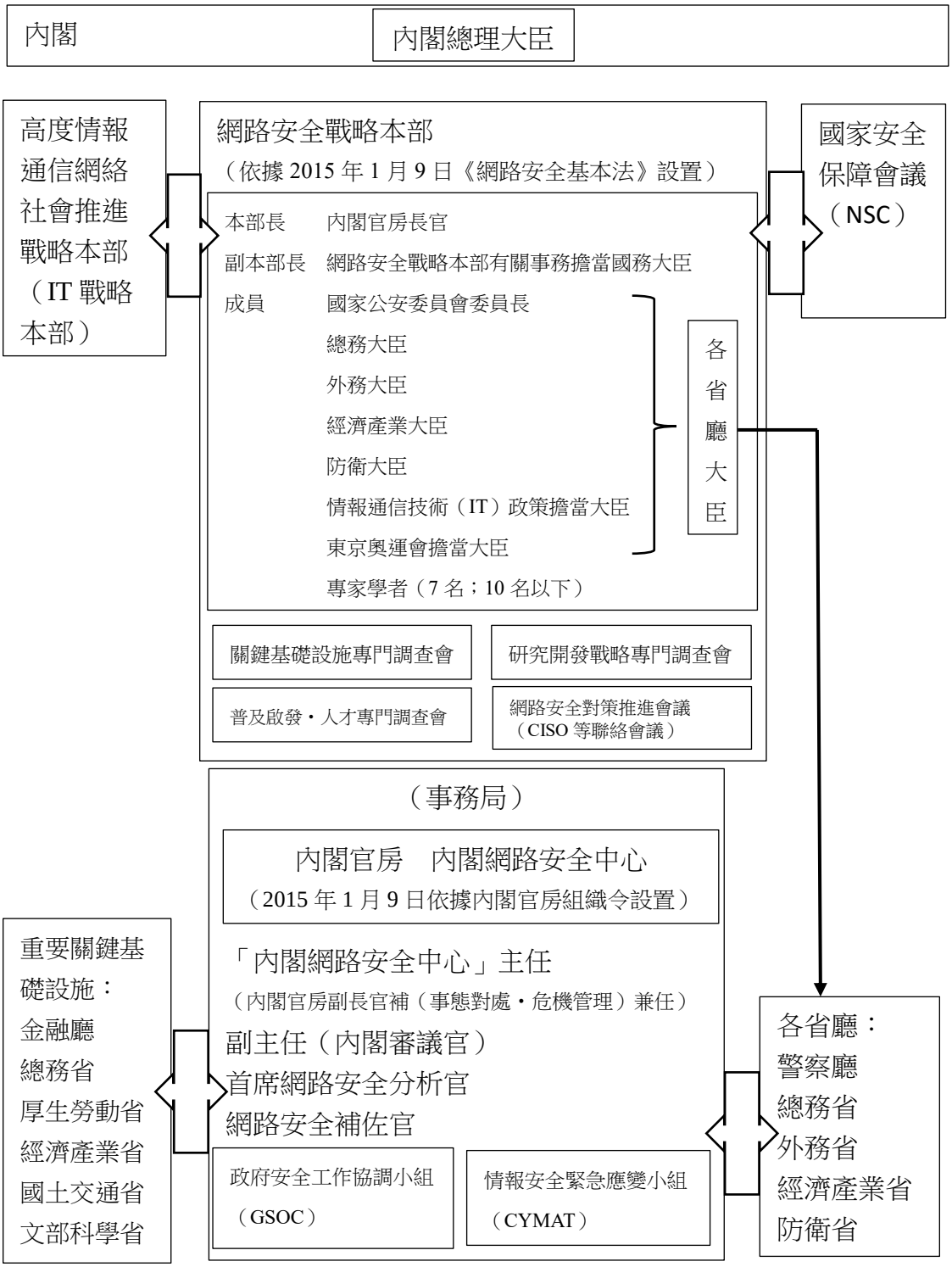

圖 7　日本網路安全政策的推進體制

資料來源：作者自行繪製自，内閣サイバーセキュリティセンタ，〈我が国のサイバーセキュリティ政策の概要〉，《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>。

（二）各省廳

日本各省廳亦不遺餘力加強網路安全。**總務省**（Ministry of Internal Affairs and Communications, MIC）主要負責制定有關通信與網路安全相關政策。從 2001 年起總務省每年公布《資訊通信白皮書》（情報通信白書），內容載明資訊安全威脅的近期動向、國民對於資訊安全的意識調查、日本對於資訊安全的行動方針等。此外，總務省設有「國民的資訊安全網」（国民のための情報セキュリティサイト），也會定期舉辦各式各樣的調查研究會，如：互聯網、雲端安全研究會等。[145]

經濟產業省（Ministry of Economy, Trade and Industry, METI）負責網路安全的單位為，2001 年 1 月成立「商務資訊政策局」（商務情報政策局）的「網路安全課」（サイバーセキュリティ課），除了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常設會議外，並於 2012 年 3 月設立「控制系統安全中心」（技術研究組合制御システムセキュリティセンタ；Control System Security Center, CSSC），舉辦電力、天然氣、大樓自動化及化工流程自動化等關鍵基礎設施的網路安全演習（サイバーセキュリティ演習）。[146]在網路安全上，經產省主要負責 1.協助企業經營者建立資訊安全管理機制；2.針對國民進行網路安全教育；3.執行《電子簽章及認證業務法》（電子署名及び認証業務に関する法律）之相關規定；[147]4.評價 IT 產品的安全性能；5.實施資訊安全管理與檢查制度；6.密碼技術；7.處理軟體與網站漏洞；8.指導應處網路釣魚事件。

外務省（Ministry of Foreign Affairs of Japan, MOFA）主要負責日本網路安全的國際合作。網路外交的三大支柱為，1.制訂國際規則；2.提高透明度及與各國建立信心措施；3.能力構築。[148]為了能有效對抗跨國的網路攻擊和網路犯罪，日本積極參與不同功能與屬性的網路國際組織，如：聯合國政府專家小組（国連における政府専門家会合；The Group of Governmental Experts, GGE）、網路空間國際會議（サイバー空間に関する国際会議；The Global Conference on Cyber Space, GCCS）、《歐洲理事會網路犯罪公約》（又稱《布達佩斯網路犯罪公約》（Budapest Convention））等，日本希望能參與網路安全的國際建制，以建立網路安全的國際合作框架。不僅如此，日本也與其他國家，如：美國、澳洲、英國、法國、以色列、愛沙尼亞、俄羅斯、歐盟和東協等國加強網路安全防護能量，建立共通平

---

145 **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**》，平成 25 年 4 月 5 日，<http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000045.html>。

146 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》，<http://www.meti.go.jp/press/2013/01/20140117005/20140117005.html>；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》，<https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1377>。

147 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》，平成 12 年 5 月 31 日，<http://www.meti.go.jp/policy/netsecurity/docs/esig/H12HO0102.txt>。

148 外務省，〈外務省のサイバー分野における取組ー日本のサイバー外交〉，《外務省》，平成 29 年 11 月 1 日，<http://www.mofa.go.jp/mofaj/annai/page5_000250.html>。

台及對網路威脅的分析能力。此外，日本也與各國的「電腦安全事件應變中心」（Computer Security Incident Response Team, CSIRT）合作，交換網路犯罪與數位鑑識情報分享，共同打擊網路犯罪。以下表 6 為日本網路外交之國際會議與雙邊對話。

表 6　日本網路外交之國際會議與雙邊對話

時間	會議名稱
2016 年 10 月 14 日	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）
2015 年 4 月 16-17 日	海牙網路空間會議（サイバー空間に関するハーグ会議）
2013 年 10 月 17-18 日	首爾網路空間會議（サイバー空間に関するソウル会議）
2012 年 10 月 4-5 日	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）
2011 年 11 月 1-2 日	倫敦網路空間會議（サイバー空間に関するロンドン会議）
2017 年 2 月 1 日（第 3 回） 2016 年 12 月 7-8 日（第 2 回） 2014 年 12 月 17-18 日（第 1 回）	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）
2017 年 1 月 27 日	日歐網路對話（日 EU サイバー対話の開催）
2016 年 11 月 11 日（第 2 回） 2015 年 3 月 24 日（第 1 回）	日俄網路協議（日露サイバー協議）
2016 年 10 月 26 日	日韓網路協議（日韓サイバー協議）
2016 年 10 月 13 日（第 3 回） 2014 年 12 月 15 日（第 2 回） 2012 年 6 月 19-20 日（第 1 回）	日英網路協議（日英サイバー協議の開催）
2016 年 9 月 9 日	日德網路協議（日独サイバー協議）
2016 年 8 月 2 日（第 2 回） 2015 年 2 月 13 日（第 1 回）	日澳網路政策協議（日豪サイバー政策協議）
2016 年 7 月 27 日（第 4 回） 2015 年 7 月 22 日（第 3 回） 2014 年 4 月 10 日（第 2 回） 2013 年 5 月 10 日（第 1 回）	美日網路對話（日米サイバー対話の開催）
2016 年 6 月 21-22 日（第 2 回）	日本—以色列網路協議（日イスラエ

2014 年 11 月 17 日（第 1 回）	ル・サイバー協議）
2015 年 10 月 15 日（第 2 回） 2014 年 10 月 21 日（第 1 回）	中日韓網路協議（日中韓サイバー協議）
2014 年 12 月 12 日	日法網路協議（日英サイバー協議の開催）
2012 年 11 月 5 日	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。

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 月公佈「高科技犯罪對策重點推進計畫」（ハイテク犯罪対策重点推進プログラム），並成立「網路警察」。1999 年 4 月，警察廳在「情報通信局」下設置「技術對策課」，2004 變更名稱為「情報技術解析課」，為指導解決各都道府縣警察本部在偵破網路犯罪中所面臨的技術問題。在「情報技術解析課」下設置「先進資訊技術分析中心」（高度情報技術解析センター）及「網路恐怖主義控制小組」（サイバーテロ対策技術室），負責蒐集分析網路恐怖主義攻擊情報及研發反制技術。警察廳內負責網路安全的另外兩個部門，分別為「網路犯罪對策部門」之「情報技術犯罪對策課」及「網路攻擊對策部門」之「警備企劃課」，負責指導及協調全國各都道府縣警察本部之網路恐怖攻擊對策，對提供關鍵基礎設施之企業進行訪問和教育訓練，並建立官民合作之網路攻擊應處對策。[149]同時，日本 47 個都道府縣的警察本部均設立「網路犯罪對策室」（サイバー犯罪対策室），並安排相應的「網路犯罪搜查官」（サイバー犯罪捜査官），為指導及協調地方警察本部偵辦網路犯罪案件。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的合作交流機會，共同對抗網路不法入侵、色情網站、網路詐欺及非法買賣等網路犯罪行為。[150]下圖 8 為日本警察廳的網路安全體制。

[149] 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>。

[150] 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─以日本反恐對策為考察對象〉，發表於「2008 警學與安全管理研討會」（台北：台灣警察專科學校，2008 年 6 月 18 日），頁 15-17。

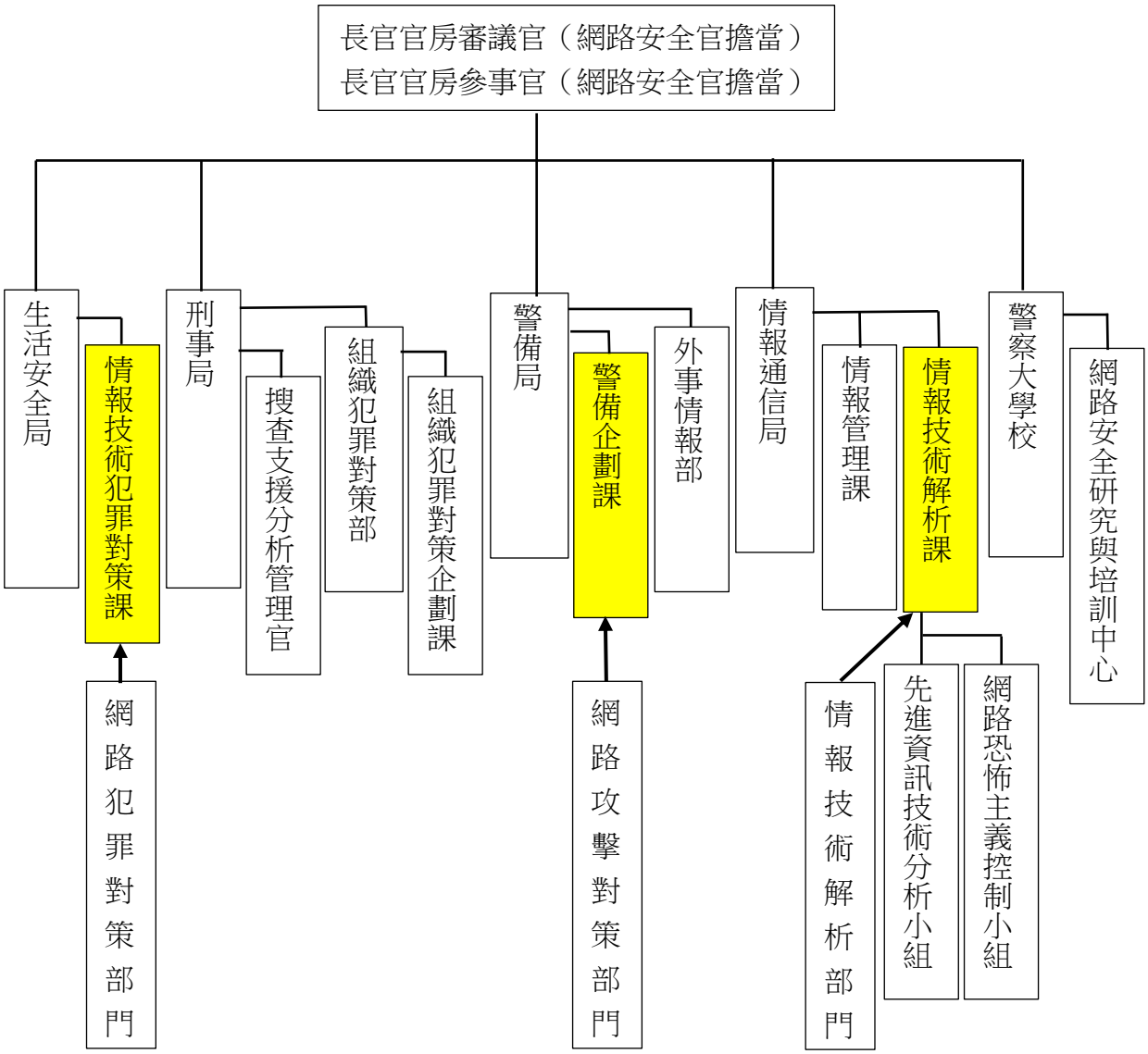

圖 8　日本警察廳的網路安全體制

資料來源：作者自行繪製。

防衛省（Japan Ministry of Defense, MOD）負責網路安全的單位為「網路防衛隊」（サイバー防衛隊），於 2014 年 3 月 26 日成立，前身為 2008 年 3 月成立的「自衛隊指揮通信系統隊」（自衛隊指揮通信システム隊），該系統隊由統合幕僚監部指揮通訊系統部的「指揮通訊系統運用課」（指揮通信システム運用課）改編而成。「網路防衛隊」成員來自陸上自衛隊的「系統防護隊」（システム防護隊）、海上自衛隊的「保全監察隊」、航空自衛隊的「系統監察隊」（システム監查隊）與相關技術人員組成，初期共約 90 人，[151]未來的目標直到 2020 年將逐年

[151] 防衛省，〈サイバー防衛隊の新編について〉，《防衛省》，平成 26 年 3 月 25 日，<http://www.mod.go.jp/j/press/news/2014/03/25d.html >。

擴增為 1,000 人的編制。[152]「網路防衛隊」直接隸屬於防衛大臣，由統合幕僚監部幕僚長負責指揮，主要任務為負責網路威脅情報蒐集、網路防護、網路安全訓練及調查研究與技術支援等。在平成 30 年（2018 年）的防衛預算中，與網路安全有關之預算為 145 億日圓，「網路防衛隊」的編制將從現有約 110 名擴增為 150 名，並加強基礎設施的安全調查研究、網路攻擊技術之研析等。[153]自衛隊全面應處網路攻擊的六大支柱為，1.提高情報通信系統的安全性，如：導入防火牆及防毒軟體；2.防護系統的整備，建立網路監控系統、分析網路攻擊等裝備；3.規則整備；4.人才培育；5.促進情報共享，「網路防衛隊」與「內閣網路安全中心」、及美國等其他國進行網路攻擊通報與合作；6.最新網路攻擊技術的研究，建立網路演習環境等。[154]

美日兩國在 2012 年 4 月 26 日的「美日安全保障協議委員會」（日米安全保障協議委員会，泛稱「2+2 會議」）上，宣布將針對網路安全議題建立戰略性的雙邊「政府一元化」對話，因此在 2013 年 5 月，首次舉行「美日網路對話」（日米サイバー対話），2013 年 10 月，聯合成立「美日網路防衛政策工作小組」（日米サイバー防衛政策ワーキンググループ；（Cyber Defense Policy Working Group, CDPWG）。此小組作為美日防衛部門間的基本框架，進一步推動美日在網路安全領域上的防衛合作，包括 1.促進網路安全政策的協議；2.緊密的情報共享；3.針對網路攻擊進行聯合訓練；4.共同培育專業人才。[155]此外，日本與英國、澳洲、愛沙尼亞等國建立戰略性的網路安全對話，就網路威脅進行情報分析與交換。不僅如此，日本也積極參與北約卓越合作網路防禦中心（NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE）舉辦之「國際網路衝突會議」（サイバー紛争に関する国際会議；Cyber Conflict, CyCon），並且日本也是「鎖定盾牌」（Locked Shields）網路防禦演習之觀察員。[156]

2013 年 7 月，防衛省成立了網路防禦委員會（サイバーディフェンス連携協議会；Cyber Defense Council, CDC），旨在提高防衛省與國防產業共同應對網路攻擊的能力，主要以防衛省為中心，促進國防產業間的情報分享與聯合訓練。以下表 7 為 2012-2016 年防衛省在網路安全上的舉措。

---

152 共同通信社，〈防衛省、サイバー部隊千人規模へ攻撃手段も研究〉，《共同通信 47》，2017 年 7 月 17 日，<https://this.kiji.is/259364402415468548>。

153 防衛省，〈サイバー空間における対応〉，《我が国の防衛と予算─平成 30 年度概算要求の概要》，頁 16，<http://www.mod.go.jp/j/yosan/2018/gaisan.pdf>。

154 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》，平成 26 年 4 月，<https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf>。

155 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>。

156 CCDCOE, “Japanese Delegation: Cyber Defence Calls for Cooperation,” CCDCOE, 23 July, 2014, <https://ccdcoe.org/japanese-delegation-cyber-defence-calls-cooperation.html>.

表 7　2012-2016 年防衛省網路安全之舉措

時間	政策內容
2012（平成 24）年	4 月：「美日安全保障協議委員會」上，雙方同意建立網路安全問題之戰略性對話。 6 月：「內閣官房資訊安全中心」（情報セキュリティセンタ；National Information Security Center, NISC）設置「情報安全緊急應變小組」（情報セキュリティ緊急支援チーム；Cyber Incident Mobile Assistant Team，CYMAT）。 9 月：制定「防衛省自衛隊穩定且有效使用網路空間」（防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」）政策。
2013（平成 25）年	5 月：在「美日安全保障協議委員會」上舉行「第一次美日網路對話」（第 1 回日米サイバー対話）。 7 月：成立「網路防禦委員會」（サイバーディフェンス連携協議会；Cyber Defense Council, CDC）。 8 月：在美日國防部長會談上，同意進一步推動在合資網路安全領域上的合作，並建立新的合作框架。 10 月：美日聯合成立「美日網路防衛政策工作小組」（日米サイバー防衛政策ワーキンググループ；（Cyber Defense Policy Working Group, CDPWG）。
2014（平成 26）年	3 月：「自衛隊指揮通信系統隊」（自衛隊指揮通信システム隊）改編為「網路防衛隊」（サイバー防衛隊）。 11 月：「網路安全基本法」（サイバーセキュリティ基本法）成立
2015（平成 27）年	1 月：內閣「網路安全戰略本部」（サイバーセキュリティ戦略本部）。 1 月：內閣官房設立「內閣網路安全中心」（內閣サイバーセキュリティセンタ；National Center of Incident readiness and Strategy for Cybersecurity, NISC）」。 5 月：CDPWG 共同發表聲明。 9 月：閣議決定「網路安全戰略」（サイバーセキュリティ戦略）。
2016（平成 28）年	4 月：防衛省設立「網路安全與資訊畫審議官」（サイバーセキュリティ・情報化審議官）一職。

資料來源：作者自行整理。

（三）行政法人

日本有關網路安全之法人機構主要包括「獨立行政法人情報通信研究機構」（国立研究開発法人情報通信研究機構；National Institute of Information and Communications Technology, NICT）、「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）、「日本電腦緊急應變小組協調中心」（一般社団法人JPCERTコーディネーションセンター；Japan Computer Emergency Response Team Coordination, JPCERT/CC）等。

「獨立行政法人情報通信研究機構（NICT）」為總務省下轄的獨立行政法人，成立於2004年4月1日，主要業務為關於資訊、通信及電波技術的研究開發及放送事業的振興等。其中，NICT網路安全研究所的「網路安全研究室」（サイバーセキュリティ研究室）主要是針對網路攻擊建構視覺化（Visualization）的監測系統。透過這個監測系統，對可能的網路攻擊進行監視及分析，並能將偵測到的網路攻擊行為即時回報給系統管理者，以加強維護系統的安全。NICT發展出三種網路攻擊視覺化平台，分別為「網路攻擊監測系統」（Network Incident analysis Center for Tactical Emergency Response, NICTER）、「聯合網路攻擊防禦告警系统」（Direct Alert Environment for Darknet And Livenet Unified Security, DAEDALUS」及「NIRVANA」（Nicter Real-time Visual Analyzer）。[157]

「網路攻擊監測系統」（NICTER）是利用暗網（Dark Net）的流量與圖形化，監控合作單位的網路系統，若是合作單位受到網路攻擊，該系統會立即告警並提供網路攻擊資訊給合作單位，此系統也監視物聯網（IoT）的網路攻擊，這對物聯網資訊安全有極大的助益。

網路攻擊防禦告警系统」（DAEDALUS）同樣利用視覺化圖像技術，收集暗網資料，解讀系統 log 檔或網路封包內容，即時對網路攻擊者與被攻擊者發出告警通知。

[157] 情報通信研究機構（NICT），〈サイバー攻撃観測・分析・対策システム NICTER〉，《サイバーセキュリティ研究所》，<http://www.nict.go.jp/cyber/research.html>。

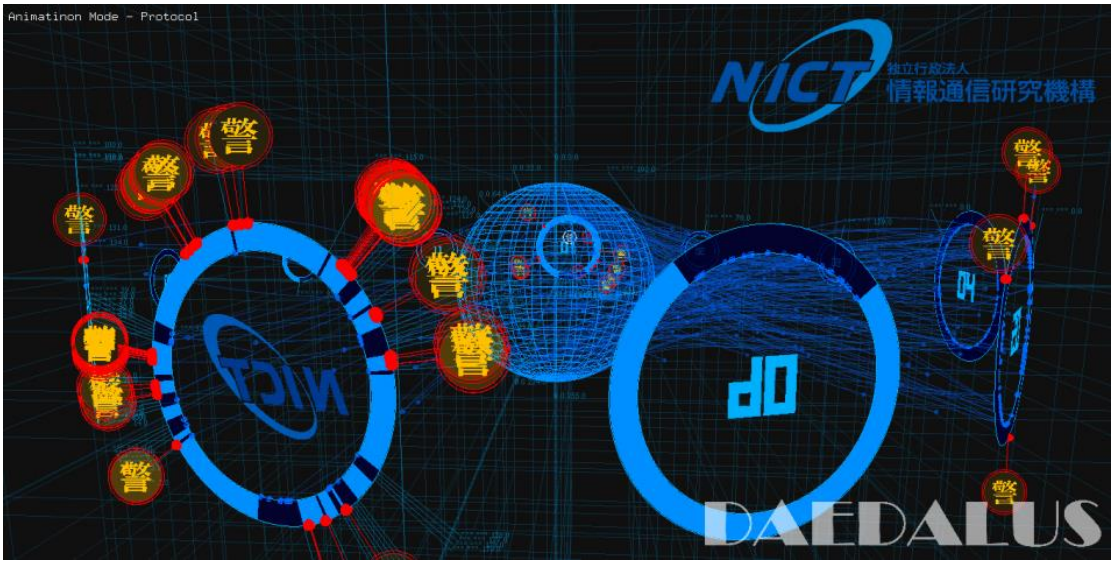

圖 9　DAEDALUS 可視化網路監測

圖片說明：每一個圓圈代表一個組織的網段，中間的球體代表網際網路，藍色圓圈代表一個組織的網路流量，當流量越大，圓圈的轉速會越快，表示越多人連線到這個組織；藍色圓圈代表正在使用的 IP，因此，當中間球體連線到圓圈的暗處（暗網（Dark Net）），意味著有人正連接到無人使用的網域，那可以推論這極有可能是一個網路攻擊。

資料來源：情報通信研究機構（NICT），〈対サイバー攻撃アラートシステム“DAEDALUS”（ダイダロス）の外部展開を開始〉，《情報通信研究機構（NICT）》，2012 年 6 月 6 日，<http://www.nict.go.jp/press/2012/06/06-1.html>。

「NIRVANA」是一套能監控網路流量及使用狀況的系統，它可以對每個不同的通訊協定，或是不同 IP 位址所使用的流量作即時的紀錄，讓管理者能確實掌控網路流量，並在任何異常發生時迅速找出原因。[158]

[158] 山下達也，〈サイバーセキュリティの今（国立研究開発法人 NICT～求められているのは可視化と教育）〉，《さくらインターネット株式会社》，2016 年 11 月 7 日，<https://knowledge.sakura.ad.jp/6430/>；林子煒，〈日本物聯網及資訊安全科技發展現況〉，《IT's 通訊》，第 10 期，2017 年，<http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=3832>。

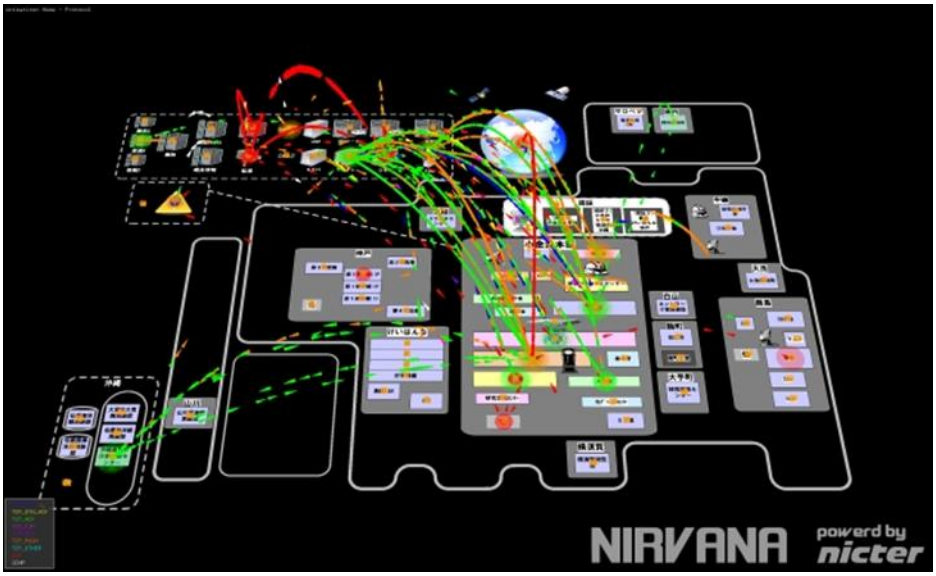

圖 10　NIRVANA 網路流量可視化

資料來源：情報通信研究機構（NICT），〈リアルトラフィックの可視化ツール "NIRVANA"を開発〉，《情報通信研究機構（NICT）》，2011 年 6 月 2 日，<http://www.nict.go.jp/press/2011/06/02-1.html>。

「獨立行政法人情報處理推進機構（IPA）」為經濟產業省下轄的獨立行政法人，前身為「情報處理振興事業協會」，於 2004 年 1 月 5 日改組，推廣 IT 有關的國家戰略，主要任務包括 IT 安全、軟體工程、IT 人才培育及開放軟體等，並受理資訊病毒、不當存取及脆弱性關聯情報等申報，與日本電腦緊急應變小組協調中心（JPCERT/CC）合作，定期公開調查情報及緊急對策等訊息。該機構下設的一個單位「IPA 安全中心」（IPA/ Information-technology SEcurity Center, ISEC）負責資訊安全防護、技術開發、標準制定、操作系統的安全認證、收集及分析不當入侵的電腦病毒，定期公佈電腦病毒報告及網路安全相關資訊，對日本國民進行網路安全教育與使用建議。[159]

情報處理推進機構（IPA）於 2011 年 10 月 25 日成立「日本網路安全資訊分享夥伴協議」（サイバー情報共有イニシアティブ；Initiative for Cyber Security Information sharing Partnership of Japan, J-CSIP），為加強公私部門的資訊共享與合作，設置 11 項關鍵基礎設施領域之特別小組（Special Interest Group, SIG），如：關鍵基礎設施製造商、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。此外，「情報處理推進機構」（IPA）也與「經濟產業省」（METI）、「內閣網路安全中心」（NISC）及「日本電腦緊急應變小組協調中心」（JPCERT/CC）密切合作，對影響關鍵基礎設施的重大網路事件作出反應。[160]以下圖 11 為「日本網路安全資訊分享夥伴

[159] 情報処理推進機構，〈IPA セキュリティセンターの事業概要〉，《情報処理推進機構》，<https://www.ipa.go.jp/security/outline/isecabst.html>。

[160] 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

協議」（J-CSIP）之體制。

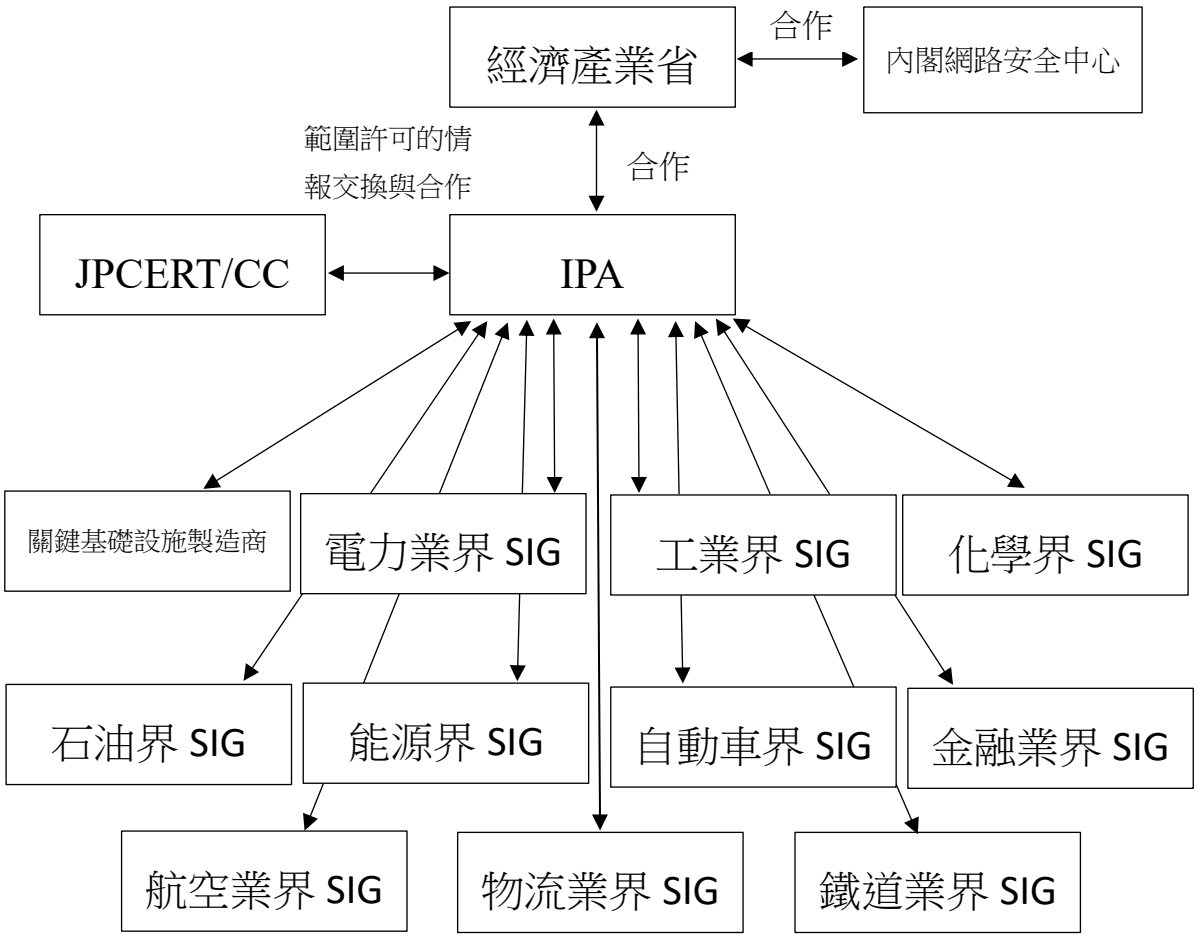

圖 11　「日本網路安全資訊分享夥伴協議」（J-CSIP）之體制
資料來源：作者自行繪製。

情報處理推進機構（IPA）也成立「產業網路安全中心」（産業サイバーセキュリティセンター；Industrial Cyber Security Center of Excellence, ICSCoE），此安全中心主要為培育網路安全人才，該中心計畫從 2017 年 7 月起開始培育 100 名關鍵基礎設施領域（電力、天然氣、鋼鐵、石油、化學、汽車、鐵路、廣電通訊）的網路安全人才，除了學習網路攻擊技術外，也模擬網路攻擊的兵棋推演（ウォーゲーム・セッション）。該中心主任由日立製作所董事長中西宏明擔任，顧問為美國國家安全局（National Security Agency, NSA）前局長、美國網路司令部（U.S. Cyber Command）首任司令亞歷山大（Keith B. Alexander）擔任。[161]中西表示：

（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>。

[161] 独立行政法人情報処理推進機構，〈産業サイバーセキュリティセンター〉，《独立行政法人情報処理推進機構》，2017 年 10 月 27 日，
<https://www.ipa.go.jp/icscoe/index.html#section18>。

「希望能確實培養守護關鍵基礎設施的人才」，亞歷山大強調：「為了保護關鍵基礎設施不受到網路攻擊，相關訓練非常重要。」經濟產業大臣世耕弘成則認為：「需要建立跨領域、跨行業的網路安全合作，並重視人力資源的開發與培育。」[162]

「日本電腦緊急應變小組協調中心」（JPCERT/CC）為一般社團法人，自 1992 年起開始整理網路安全事件相關資訊，於 1996 年 10 月正式成立，為日本建立第一個「電腦安全事件應變小組」（Computer Security Incident Response Team, CSIRT），並在 2009 年 6 月正式更名。該協調中心與網際網路服務提供者（Internet Service Provider, ISP）、網路安全設備供應商、關鍵基礎設施部門、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的緊急因應。[163]JPCERT/CC 同時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）的成員，負責協調並整合有關網路安全的防護措施。以下圖 12 為「日本電腦緊急應變小組協調中心」（JPCERT/CC）之合作體制。

[162] 世耕弘成，〈業種の枠を越えた幅広い連携とサイバーセキュリティの強化・人材育成の重要性〉，《ICSCoE REPORT》，第一期，平成 29 年 10 月 2 日，頁 1-4，<https://www.ipa.go.jp/files/000062154.pdf>。

[163] 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>。

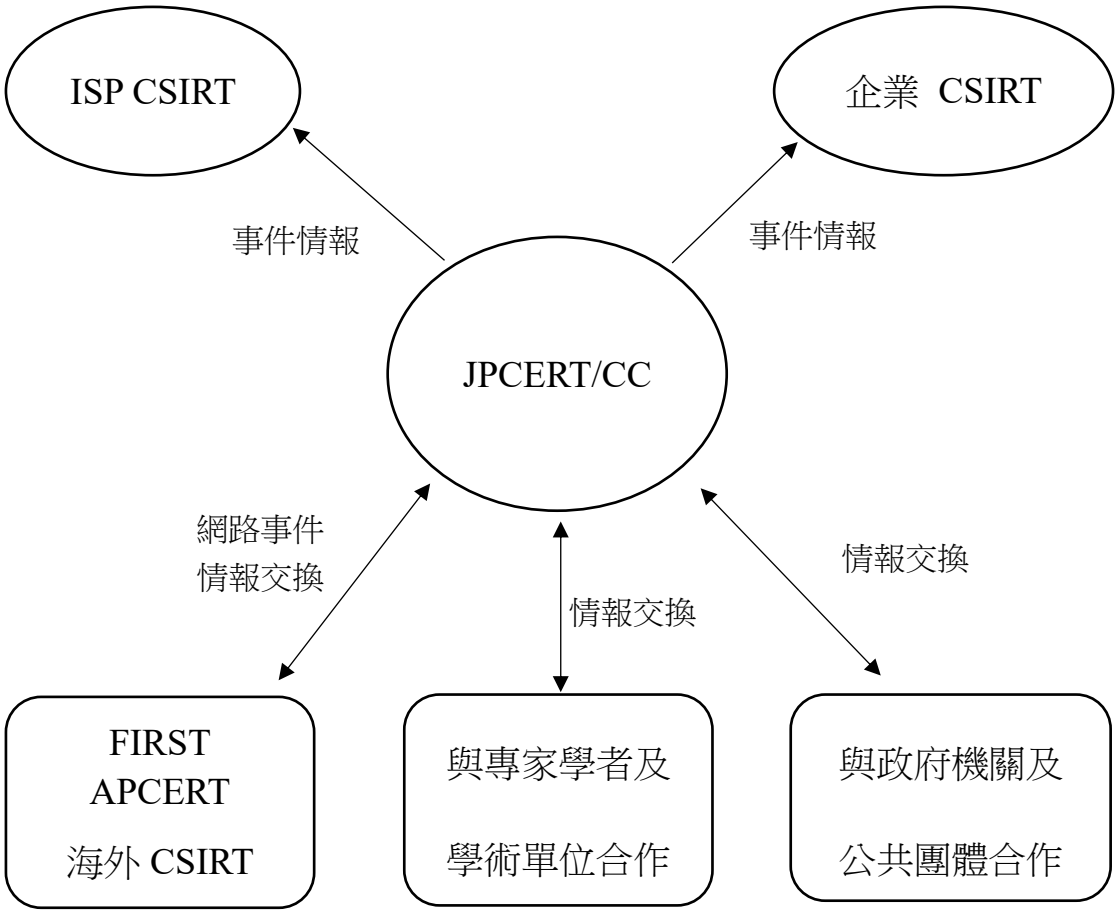

圖 12 「日本電腦緊急應變小組協調中心」（JPCERT/CC）之合作體制
資料來源：作者自行繪製。

二、日本網路安全之相關政策

21世紀後日本政府相繼出台許多與網路安全有關的政策。日本從2001年制定《e-Japan戰略》以來，希望能達到安全的網路交易環境與個人資料保護、建立資訊導向的企業、數位內容能受到智慧財產權法保護等目標。2005年日本正式實施《個人情報保護法》（Japanese Personal Information Protection Act, JPIPA），明文規定保有個人情報的企業有義務保護個人情報並避免洩漏。

2004 年 7 月 27 日，日本 IT 戰略本部在「資訊安全專門調查會」（情報セキュリティ専門調査会）下設置了「資訊安全基本問題委員會」（情報セキュリティ基本問題委員会）。該委員會歷時 10 個月，總共召開 5 次會議，提出共兩份建言，2004 年 11 月 16 日提出**《第一次建言—重新審視政府在應對資訊安全問題時的機能與作用》**（第 1 次提言—情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて），[164]內容表示日本政府在應對網路安全問題時的基

[164] 情報セキュリティ基本問題委員会，〈第 1 次提言─情報セキュリティ問題に取り組む政府

本態度，並建議設立「資訊安全政策會議」與「國家資訊安全中心」，同時就兩者的機能、結構及相互關係進行說明。2005 年 4 月 22 日「資訊安全基本問題委員會」發表**《第二次建言─強化我國重要基礎設施相關資訊安全對策》**（第 2 次提言─我が国の重要インフラにおける情報セキュリティ対策の強化に向けて），[165]針對通信、金融、航空、鐵路、電力、天然氣、行政服務等關鍵基礎設施領域的資訊安全進行討論。

2004 年 8 月總務省公布《平成 17 年度 ICT 政策大綱》，以實現無所不在（Ubiquitous）的網路社會。[166]在該政策大綱中，「資通安全政策之推動」共編列 49 億日圓預算，占總預算 733 億日圓的 7%，希望能實現任何人都可以安心且安全生活的社會。2005 年 5 月 30，IT 戰略本部設置「資訊安全政策會議」（情報セキュリティ政策会議），而「資訊安全基本問題委員會」被廢止，後續工作交由「資訊安全政策會議」下設的「安全文化專門委員會」（セキュリティ文化専門委員会）執行。2005 年 11 月 17 日「安全文化專門委員會」公布**《報告書─強化企業與個人相關資訊安全對策》**（セキュリティ文化専門委員会報告書─企業・個人の情報セキュリティ対策強化に向けて），[167]討論企業與個人的資訊安全對策。

依據上述文件，日本政府成立「內閣官房資訊安全中心」和「資訊安全政策會議」。2006年2月2日，「資訊安全政策會議」公布**《第一次資訊安全基本計畫》**（第1次情報セキュリティ基本計画─「セキュア・ジャパン」の実現に向けて），[168]此計畫設定時間為3年，由上而下從政府機關、關鍵基礎設施、企業與個人等四個領域強化資訊安全。

2009年2月3日，「資訊安全政策會議」公布**《第二次資訊安全基本計畫》**（第2次情報セキュリティ基本計画─IT時代の力強い「個」と「社会」の確立に向けて），[169]內容共有四章，分別為：第一次資訊安全基本計劃下的應對及2009年的狀況、第二次資訊安全基本計畫的基本思考與2012年的預測、今後三年的施政重

の機能・役割の見直しに向けて〉，《内閣サイバーセキュリティ センター（NISC）》，2004 年 11 月 16 日，<https://www.nisc.go.jp/conference/kihon/teigen/pdf/1teigen_hontai.pdf>。

165 情報セキュリティ基本問題委員会，〈第 2 次提言─我が国の重要インフラにおける情報セキュリティ対策の強化に向けて〉，《内閣サイバーセキュリティ センター（NISC）》，2005 年 4 月 22 日，<https://www.nisc.go.jp/conference/kihon/teigen/pdf/2teigen_hontai.pdf>。

166 総務省，〈平成 17 年度 ICT 政策大綱〉，《国立国会図書館：WARP》，2004 年 8 月，<http://warp.ndl.go.jp/info:ndljp/pid/235321/www.soumu.go.jp/s-news/2004/pdf/040827_7.pdf>。

167 セキュリティ文化専門委員会，〈セキュリティ文化専門委員会報告書─企業・個人の情報セキュリティ対策強化に向けて〉，《内閣サイバーセキュリティ センター（NISC）》，2005 年 11 月 17 日，<https://www.nisc.go.jp/conference/seisaku/bunka/common/pdf/bunka_sum.pdf>。

168 情報セキュリティ政策会議，〈第 1 次情報セキュリティ基本計画─「セキュア・ジャパン」の実現に向けて〉，《内閣サイバーセキュリティ センター（NISC）》，2006 年 2 月 2 日，<https://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf>。

169 情報セキュリティ政策会議，〈第 2 次情報セキュリティ基本計画─IT 時代の力強い「個」と「社会」の確立に向けて〉，《内閣サイバーセキュリティ センター（NISC）》，2009 年 2 月 3 日，< https://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf>。

點、政策推進體制與連續改善。兩次基本計畫建立了官民合作模式的基本構想，並以政府單位、關鍵基礎設施、企業及個人等四大部分為基礎，勾勒出日本網路安全戰略的發展脈絡。

2010年5月11日，「資訊安全政策會議」公布**《守護國民的資訊安全戰略》**（国民を守る情報セキュリティ戦略），[170]該報告在前言中指出：《第二次資訊安全基本計畫》公佈後，美國、韓國相繼發生大規模網路攻擊事件及個人隱私洩露等情事，特別是大規模網路攻擊事件，帶給日本非常大的警訊。日本當前的體制已經不足以應對網路安全風險的多樣化、高度化及複雜化的趨勢，因此，日本在《第二次資訊安全基本計畫》中確立以官民合作、共同應對網路威脅，並對政府的因應措施進行改革。簡單來說，《守護國民的資訊安全戰略》是兩次《資訊安全基本計畫》所確立的補充說明，表示日本強化對網路安全的重視，並凸顯對網路攻擊事態的應處及對新型態網路安全環境變化的因應。

2013年6月10日，「資訊安全政策會議」公布**2013年版《網路安全戰略》**，這是日本首次在相關政策中使用「網路安全」一詞。[171]新戰略在前言中指出：「資訊安全政策會議」成立八年多以來，相繼提出《第一次資訊安全基本計畫》、《第二次資訊安全基本計畫》、《守護國民的資訊安全戰略》等相關政策文件，希望在資訊自由流通與網路風險間取得平衡，並提高日本的資訊安全水準。《網路安全戰略》共分為四個部分，分別是：網路安全環境的變化、基本方針、實施領域、推進體制與評價機制，第一部分首先指出，網路空間與實體空間不斷融合，並朝一體化的方向發展。同時，網路空間中存在的風險越來越大。其次探討日本網路安全防護機制，並指出日本當前的體制已經不足以應赴網路安全環境的變化。隨後介紹美國、英國、法國、德國、韓國等對網路安全問題的應對態勢。第二部分提到日本在今後應對網路安全問題的基本思考，為確保資訊自由流通、將針對不斷增加的網路風險採取新型態應對措施、強化對風險資料庫的運用、促進產、官、學、民之間的互動。第三部分為構築強韌的網路空間、構築有活力的網路空間及構築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、網路空間的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作了詳細討論，包括在2015年度將內閣官房資訊安全中心改組為網路安全中心及每年公佈年度計畫等內容。

Yoko Nitta認為日本網路安全戰略的第一根支柱為，建立一個強健的網路空間，以強化保護網路空間的能力，即使遭遇攻擊，也能快速復原。要達成這個目標需要具備偵測與分析網路攻擊的能力，同時分享攻擊事件的資訊；第二根支柱為，建立有活力的網際網路空間，以增強在這方面的知識與創新能力。為擴大網

---

[170] 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 センター（NISC）》，2010 年 5 月 11 日，<https://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>。

[171] 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>。

路空間，要增強產業界在網路上的活力，以對抗網路攻擊，並發展新的網路防護技術、加強訓練、培育網路安全人才，如此才能獨立地對抗網路攻擊的風險；第三根支柱：為建立世界領導地位的網路空間，以強化對世界的貢獻及領導地位，日本積極參與國際性重要網路空間政策制訂會議，開拓海外市場，建立信心等措施。為了強化日本的網路安全，以因應2020年東京奧運與殘奧會所可能面臨的威脅，他提出以下三點建議：（一）建立政府層級資訊安全防護網，及早發現嚴重的網路安全事件，並對該事件加以分析，以擬定出處理的方法與程序，因為這可能牽涉到跨國合作，所以對各國的外交政策需要更深入的了解；（二）建立多功能的情資交換平台，改進資訊安全標準，制定可行的資訊安全政策更顯迫切；（三）強化國際間的合作及資訊分享，共同抵抗日益增強的網際網路威脅。在資訊安全事件的分析能力方面，擷取資訊的能力要提升，尤其是在政府機構與關鍵基礎設施的協同合作方面，要透明沒有障礙，整個策略可以視未來網際網路安全環境的變化而作調整。[172]

由於網路威脅日益增加，政府機關受到網路攻擊之數量倍增、網路攻擊範圍逐漸擴大，為了加強政府機關的應對能力、並強化公私部門及國際間的合作，日本眾議院於 2014 年 11 月 6 日表決通過**《網路安全基本法》**（サイバーセキュリティ基本法案），旨在加強日本政府與民間單位對網路安全的協調及運作，共同應對網路攻擊。該法的重點為：（一）公私部門對於網路安全應有的責任義務；（二）法制與行政組織之整備；（三）推動《網路安全戰略》；（四）基本政策。[173]內容簡述如下：

（一）公私部門對於網路安全應有的責任義務。中央基於本法的基本原則，訂定全國性的網路安全政策並負責推動，而地方政府亦基於本法的基本原則，與中央分擔責任，訂定地方自主的網路安全政策並負責推動；其次，關鍵基礎設施業者，應確保工業控制系統的網路安全，並配合中央與地方的政策為之；其他網際網路服務供應商及網路安全業者亦應配合中央與地方政府，確保網路安全；最後，大學等研究單位應致力培育網路安全人才並推廣相關研究成果，而每位國民也應了解網路安全的重要性，並保護個人隱私資訊。

（二）法制與行政組織之整備。為實施網路安全等相關政策，在法制、賦稅及行政效率改善等方面採取的配合措施。

（三）推動《網路安全戰略》。規範網路安全政策的基本方針、行政機關應確保網路安全、關鍵基礎設施業者與地方政府促進網路安全及其他相關必要之事項。

（四）基本政策。政府及有關單位應執行以下措施：1.政府機關及獨立行政

---

[172] Yoko NITTA, “Review of the Japan Cybersecurity Strategy,” *ISPSW Strategy Series: Focus on Defense and International Security,* No. 290, September 2014, pp. 2-8, <https://www.files.ethz.ch/isn/183668/290_Nitta.pdf>.

[173] 衆議院，〈サイバーセキュリティ基本法案：第 4 條至第 9 條〉，《議案本文情報一覽》，<http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm>；蘇柏毓，〈資訊安全法規國際最新發展舉隅〉，《科技法律透析》，第 27 卷第 6 期，2015 年 6 月，頁 30-32。

法人等應採取確保網路安全之必要措施，如：訂定網路安全措施之統一標準、共享資訊系統、對網路攻擊行為進行監視和分析、進行網路安全演習與訓練等；2.關鍵基礎設施業者應針對網路安全採取必要措施；3.促進民間企業及教育研究單位，自發性採取各種保護自身網路安全之措施；4.公私部門間的合作；5.網路犯罪防制並避免受害範圍擴大；6.對於產生重大影響之網路安全事件，應強化網路安全防護體制，明確有關機構之合作模式與責任分擔；7.產業振興強化國際競爭力，為了增加網路安全產業之就業機會，並健全其發展，推動網路安全之研究開發、技術升級與人才培育；8.加強網路安全技術的研究開發；9.人才培育；10.教育國民網路安全知識與意識；11.積極參與制定國際網路安全規範、促進國際合作、協助發展中國家網路安全技術的建立、合作取締跨國網路犯罪等。

2015 年 9 月 4 日，日本公佈 **2015 年版《網路安全戰略》**，[174]內容分別為制定的宗旨、網路空間相關認知、目的、基本原則、為了達成目的的手段、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》的內容，並針對 2015 年 5 月，日本發生年金機構資訊洩露等重大網路安全事件進行改革。戰略中說明日本政府有責任實現自由而公平的網路空間，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，並且維護日本高品質的產品與技術精良的國家形象及競爭優勢。該戰略有五大原則，（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，並參考國際規範來制定；（三）開放。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）自治。自主管理為網路空間管理的核心，並落實於網路空間的各種社會系統；（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並履行各自責任，政府則扮演好協調與分享資訊的角色。

為了達成上述目標相關措施如下：對於企業而言，為了建立安全物聯網系統（IoT Systems），日本政府向企業建議，在組織中設置「資訊安全長」的角色（Chief Information Security Officer, CISO），以增進網絡安全的管理技能，強化組織對商業機密的保護能力，讓企業能夠永續經營。在商業網路環境方面，日本政府提供中小企業安全的雲端運算服務，以保護企業的核心技術，促進日本企業全球營運的環境與發展。

在關鍵資訊基礎設施防護（Critical Information Infrastructures Protection, CIIP）上，除了強化作業人員對於安全的認知與標準外，並對關鍵資訊基礎設施進行定期審查，由政府安全工作協調小組（Government Security Operation Coordination Team, GSOC）擔任監督與資訊分享的角色，分享網絡安全事件與偵測資訊給關鍵資訊基礎設施等相關部門。同時為了在 2020 年建立世界級的網路安全防禦架構，由日本內閣網路安全中心（National Center of Incident Readiness and Strategy

[174] 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（NISC）》，2015 年 9 月 4 日，<https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf>。

for Cybersecurity, NISC）提供有效且及時的資訊，好阻擋針對關鍵資訊基礎設施的網絡攻擊。

為了確保全球化的網路安全與資訊自由流通，日本政府積極和擁有共同理念的國家建立網路安全合作，除了與美國共同探討網路安全議題、簽署雙邊合作協定之外，如：關鍵資訊基礎設施防護、網路犯罪防範、國土安全等；更積極協助東協國家提升資訊安全防護的能量，建立共通平台及對網路安全威脅的分析能力。同時，擴展日本網路安全的海外市場，及增加網路安全專業人才的來源。

在教育方面，為了培養與招募一流的人才，日本政府同時關注各國網路安全研發的情形與專業人員的動態，增進國際研發合作，建立高等教育與專業訓練外，並且規劃長期的網路安全 ICT 專業人力發展路徑圖，向下延伸擴大到中小學，使學生能具備基本的網路安全素養。以下表 8 為日本網路安全之相關政策。

表 8　日本網路安全之相關政策

時間	政策內容
2004 年 11 月 16 日	「資訊安全基本問題委員會」提出《第一次建言—重新審視政府在應對資訊安全問題時的機能與作用》（第 1 次提言—情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて）
2005 年 4 月 22 日	《第二次建言—強化我國重要基礎設施相關資訊安全對策》（第 2 次提言—我が国の重要インフラにおける情報セキュリティ対策の強化に向けて）
2005 年 11 月 17 日	「安全文化專門委員會」公布《報告書—強化企業與個人相關資訊安全對策》（セキュリティ文化専門委員会報告書—企業・個人の情報セキュリティ対策強化に向けて）
2006 年 2 月 2 日	「資訊安全政策會議」公布《第一次資訊安全基本計畫》（第 1 次情報セキュリティ基本計画―「セキュア・ジャパン」の実現に向けて）
2009 年 2 月 3 日	《第二次資訊安全基本計畫》（第 2 次情報セキュリティ基本計画―IT 時代の力強い「個」と「社会」の確立に向けて）
2010 年 5 月 11 日	《守護國民的資訊安全戰略》（国民を守る情報セキュリティ戦略）
2013 年 6 月 10 日	2013 年版《網路安全戰略》（サイバーセキュリティ 2013）
2014 年 11 月 12 日	公布《網路安全基本法》（サイバーセキュリティ基本法案）
2015 年 9 月 4 日	2015 年版《網路安全戰略》（サイバーセキュリティ

	2015）

資料來源：作者自行整理。