米国におけるサイバーセキュリティ法制の示唆

(The Suggestions from US Cyber Security Legislations)

Pauline C. Reich[1]、高橋郁夫[2]、有本真由[3]

１　序

2012 年 10 月 11 日、米国国防長官レオン・パネッタは、「サイバー分野での脅威の重要な増大」があったと警告した[4]。

ここ数年間、たびたびの警告がなされているにもかかわらず、米国議会は、サイバーセキュリティ問題に関する包括法を定めることができていない。本稿は、テーマ、概念、時系列の観点から、それらを分類して、提案された法律を分析するものである（2012 年 11 月現在）。両院が包括的なサイバーセキュリティ法案を可決できないために、大統領令が発令される可能性があり、それも分析の対象とされる。

２　議論されるべき論点[5]

サイバーセキュリティの問題の解決に対しては、法、ポリシー、技術の各分野が協力をなして対応していかなければならないことはいうまでもない。しかしながら、十分に、協働しているとは思えない点も多々あり、特に米国に比較して、他の国においては、その度合いが低いといわざるをえない。さらに、そのような協働作業がなされたとしても、誰が、サイバーセキュリティの問題に対して責任をもって対処すべきなのかという点については、同意できないという問題が存在している。

---

[1] 早稲田大学法学部教授、 Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute 理事(cyberasia2@gmail.com)

[2] 弁護士（BLT 法律事務所）、株式会社 IT リサーチ・アート代表取締役社長(ikuo@comit.jp)

[3] 弁護士（小川綜合法律事務所）(arimoto@ogawalaw.com)

[4] 具体的には、イランによる米国、そして、外国の銀行に対する最近のサイバー攻撃、2012 年 8 月のサウジアラビアアラムコに対するサイバー攻撃を指す。

[5] なお、本稿のこの部分については、Pauline C. Reich 編著 “LAW, POLICY AND TECHNOLOGY: INFORMATION WARFARE, CYBERTERRORISM AND INTERNET IMMOBILIZATION “（IGI Global, 米国,2012）に記載があり、参照されたい。

国内問題について見るとき、十分なセキュリティ手段を採用していない国内民間会社や個人に責任を課して、外部の侵入者に対応することなく、自国のネットワーク部分を保護するのが望ましいのだろうかという問題がある。 民間企業は、国内において、政府機関、軍部機関、諜報機関との間において、攻撃情報の共有に協力すべきかという問題もある。また、それらの懈怠に刑事罰をもって臨むべきかという議論もありうる。

さらに国際的な問題について見るとき、重要情報インフラに対するサイバー攻撃の加害者を特定できないとき、グローバルなサイバーセキュリティに関する条約や国内法が、国際的に役に立つのか、国内法もしくは国際法に基づいて防衛的行為をなすのに十分なサイバー攻撃の源を特定しうるのか、そのような防衛的行為は、警察行為なのか、軍事行為なのか、はたまた、諜報機関の仕事なのか、政府か、民間の行為か、といった問題がある。

上記の問題は、米国において議会での議論の際に検討された問題のいくつかを列挙したものである。

３　米国議会における議論の経緯

米国議会におけるサイバーセキュリティ法案の提案とその議論経過を以下、分析する。2012 年 7 月 25 日に発刊された議会調査局のレポート[6]は、「50 以上の法令が直接または間接的にサイバーセキュリティのいろいろな面について触れているが、すべてを包含する枠組みの法律は、存在しない。過去数年間にわたり、いろいろな法の改正が提案されているが、2002 年以来主要なサイバーセキュリティに関する法律は制定されていない」と述べている。また、上記レポートは、第 111、112 会期議会は、主に 10 の広い領域（国家戦略と政府の役割）に焦点を合わせていると論じている。具体的には、連邦情報セキュリティ管理法(FISMA)の改革、 重要インフラの防護(配電網と化学産業を含む)、 情報共有とセクター間のコーディネート、 財務情報などの個人情報の窃取や暴露をもたらす情報漏えい、 サイバー犯罪、 電子商取引のプライバシー、 国際的な努力、 研究開発、サイバーセキュリティ担当部門（workforce）である。

メリッサハザウェイ(ホワイトハウスの元国家安全保障会議サイバー空間担当上級部長)は第 111 会期議会において提出された法案を分析している。その分析は、様々な提出法案

[6] Eric A. Fischer, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS, Congressional Research Service, Summary, July 25, 2012.

を、組織的責任、法令順守及び説明責任、データ説明責任、アイデンティティ窃取、教育、認知及び研究開発、重要インフラ、電気にそれぞれ分類するというものであった[7]。

もう一つ大きな論争を巻き起こした法案は、2009 年に上院議員ロックフェラーとスノウによって提出されたいわゆる「Kill Switch」という法案であった[8]。その法案は、大統領が「連邦政府ないし合衆国の重要インフラ情報システムないしネットワークが危険にさらされた際には、サイバーセキュリティ危機を宣言し、インターネットトラフィックを制限ないしシャットダウンを命じることができる」権限を付与するものであった[9]。大統領にそのような権限を付与することに疑問を抱く者も多く、その法案は通らなかった。

４　2012 年における議会状況と大統領令の可能性

そして 2012 年、我々は一連の法案とさらなる論争に直面した。

「Cyber Intelligence Sharing and Protection Act」 (CISPA)法案[10]は、下院を通過したが、政府は上院に対し当該法案を通過させれば拒否権を行使すると圧力を加えた。この CISPA 法案は、National Security　Act　1947 に、Cyber Threat　Intelligence Sharing というものを追加しようとする法律案である 。その目的は、「インテリジェンスコミュニティと民間部門との脅威情報の共有」である。そこでは、機密とされた情報が、認可された組織、適切なセキュリティクリアランスを有している人物においてのみ共有されること、認可された組織の従業員等にセキュリティクリアランスが与えられること、などが議論されている。また、サイバーセキュリティ提供業者が、保護された組織のサイバー脅威情報を取得するため、サイバーセキュリティシステムを利用することができ、連邦政府などの保護された組織と情報共有することができること、共有された情報について、場合によっては、適切な匿名化や情報の最小化がなされなければならないこと、提供した主体に対して損害を与えるような使用がされてはならないこと、政府と共有される場合には、政府機関の情報開示から排除されること、プロプライエタリな情報だと認識され政府機関外には、開示されないこと、政府機関が規制目的では利用し得ないこと、が必要になることなどが議論されている。その内容からして、攻撃情報（およびそれに付随する民間の種々の情報）な

---

[7] Melissa E. Hathaway, “Cybersecurity: The U.S. Legislative Agenda,” Belfer Center for Science and International Affairs（2010 年 5 月 14 日） 9-11 頁, http://belfercenter.ksg.harvard.edu/files/legislative-]landscape-publish-final

[8]法案の原文については作業ドラフト（2009 年 3 月 31 日）を参照のこと。 https://www.cdt.org/security/CYBERSEC4.pdf

[9] Internet Governance Project, “A more detailed look at the proposed Cybersecurity Act of 2009,” http://www.internetgovernance.org/2009/04/03/a-more-detailed-look-at-the-proposed-

どが、政府機関との間で共有されることに批判が集まったものである。プライバシー及び自由を標榜する団体からは、国家安全保障局（NSA）による関与、及び、「サイバー脅威（cyberthreat）」の定義の漠然性に対し、強い懸念が表明された。

また、上院においては、“Cybersecurity Act of 2012”（2012 年サイバーセキュリティ法案という）が議論された。なお、関連法案として Cybersecurity Information Sharing Act of 2012[11]も議論された。2012 年サイバーセキュリティ法案は、重要インフラ防衛（１章）、政府ネットワークの保護（２章）、既存の仕組みの明確化および強化（３章）、教育、人材発掘、担当部門（４章）、調査および発展（５章）、リスクマネジメント（６章）、情報共有（７章）、公共啓発報告（８章）、国際協力（９章）からなる包括的なものである。しかしながら、この法案にたいしては、あまりにも幅広いものであるという批判[12]がなされるにいたった。結局、上院は、2012 年サイバーセキュリティ法案の票決に至ることはなかった。

そして、8 月には、議会の機能不全に対処するため、大統領令が発令されるとのうわさが上がった。大統領令の 1 つについては、プレスにリークされたが、未だ公式な命令は発令されていない[13]。

また最近になって、国土安全保障省長官が大統領令の最終的な草稿を準備していたと報道された。再選後も、議会はまだ法案を通過させることができないため、オバマ大統領が実際に大統領令を発令する可能性は高まっている。

なぜ上院は 8 月、さらには 11 月に法案を通過させることができなかったのか。それによって本年度の法案通過はほぼ絶望的となった。政府及びプライバシー及び自由を標榜するいくつかの団体は、上院の法案（2012 年サイバーセキュリティ法）に賛同していたものの、米国商工会議所が同法案に強く反対していた。その反対は、民間部門の過大な費用負担及び過剰規制を理由とする。経済的苦境に鑑みれば、かかる懸念は当然のことである。

---

[11] この法案は、民間企業が、自己もしくは第三者のシステムのモニターおよび反撃の権限を有することをさだめ（２条）、第三者との共有が法に違反しないこと（３条）、サイバーセキュリティに関するインディケーターの交換プロセス（４条）、交換機関への任意の開示（５条）などを定めている。

[12] Elinor Mills “Civil liberties groups: Proposed cybersecurity bill is too broad”（http://news.cnet.com/8301-27080_3-57384137-245/civil-liberties-groups-proposed-cybersecurity-bill-is-too-broad/）

[13] The White House, “Memorandum: Paper Deputies Committee Meeting on Executive Order on Improving Critical Infrastructure Cybersecurity Practices,” September 28, 2012, pages 9-15, http://www.lawfareblog.com/wp-content/uploads/2012/11/White-House-D

また、プライバシー及び自由を標榜する団体は、かかる懸念を前述の CISPA 法案が通過する前後から表明し続けている。

5　今後の展開

したがって、そろそろ大統領が議会の機能不全に介入し、大統領令を発令する可能性がある。ここで我々が直面しているのは、異なる政治哲学、前代未聞の国防の脅威への既存法の適用、国家安全のため妥協が許されないこと、国家安全を上回る新たな費用負担への民間部門の懸念といった、複雑なファクターである。

こうした米国の状況が、何故、その他の国でサイバーセキュリティに関する法律及び政策に関わる専門家にとっても意味があるのか。かかる状況の検討から、以下のような根本的に重要な疑問が生じてくる。例えば、どの政府部門がサイバー脅威情報の入手につき主導的役割を果たすべきか、またどの政府部門が民間部門に責任と負担を課すべきか。政府の監視はどの範囲まで許されるか、サイバー脅威をモニターしなければならない状況下において民主社会でどの範囲まで市民のプライバシー及び自由が保護されるべきか。サイバー攻撃に対処するための費用及び責任は誰が負うべきか。サイバー攻撃対応における民間部門の役割と責任、軍事部門、諜報機関の役割は何か、といった疑問である。

今後の動向に注目していく必要がある。今後なされうる決定は、サイバー脅威及びサイバー攻撃に対し政府がどのように対処すべきかという論点について大きな影響を及ぼしうるからである。