米国連邦政府のサイバーセキュリティ政策を巡る最近の動向

和田恭＠JETRO/IPA　NY

1. はじめに

情報技術（IT）は経済成長には不可欠の基盤であり、情報化社会の構築を背景に、IT の安全確保が経済成長の前提となっているといえる。米国においては、近年、知的財産やライフラインを狙った攻撃や、企業等の機密漏えいが急増する中、特に悪意のある第 3 者からのインターネットを通じたサイバー攻撃への対策が遅れているとの指摘もある。また、ホワイトハウス主導によるサイバーセキュリティ体制の確立が遅れている、サイバー攻撃を受けた場合のリーダーシップの所在が不明瞭とする意見が多い。オバマ政権はこのような状況の改善に向けて動き始めており、サイバーコーディネーターの設置や様々な連邦省庁や民間も含めたサイバーセキュリティ体制の構築を目指している。

以上のような問題意識のもと、本稿では、米国における直近のサイバーセキュリティ政策を巡る動向について報告する[1]。

2. 米国連邦政府のサイバーセキュリティ政策について

(1) 概要

オバマ政権は、サイバーセキュリティ強化に向けた包括的な指揮体制の確立を、政権の重要政策の 1 つとして掲げている[2]。

サイバーセキュリティ政策については、ブッシュ政権時代に策定され、2010 年 3 月にその一部が発表された「包括的サイバーセキュリティ・イニシアティブ（Comprehensive National Cybersecurity Initiative、CNCI）」（NSPD54／HDPD23）によって枠組みが規定されているが、CNCI に関する文書の大部分は機密情報という扱いになっており、公開文献から得られる情報はきわめて限定的である。大統領府が昨年公開した CNCI の概要[3]によれば、同文書には以下の3つの綱領が掲げられている。

- サイバー攻撃に備える「前線基地」を構築する。ネットワーク上の脆弱性や、サイバー脅威に関する意識を連邦政府内で向上させ、サイバー攻撃を未然に防ぐ

[1] 2010 年 3 月以前のサイバーセキュリティ政策動向については、ニューヨークだより 2010 年 3 月号参照のこと。
[2] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[3] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

- サイバー教育の拡大や連邦省庁間での共同研究開発を促進することによって、強固なサイバーセキュリティ環境の構築を目指す
- 防諜機関の能力を強化し、重要な IT 技術に関する情報セキュリティを確保することで、様々な種類の脅威に対抗できる体制を整備する

このうち、わが国との関係で参考になると考えられるものとして、①サイバー攻撃未然防止、②ネットワーク上の脆弱性を防ぎつつ重要インフラの保護・継続運用を行うこと、③サイバーセキュリティに関する研究開発、普及啓発等を取り上げる。以下、オバマ政権によるサイバーセキュリティ政策の方向性について、この 3 つの観点から概説する。

① 攻撃未然防止

米国のサイバーセキュリティ政策においては、特に政府機関の IT インフラに対する攻撃を未然に防ぐことに重点を置いたイニシアティブが存在する。これは、国土安全保障省（Department of Homeland Security、DHS）の傘下組織 National Cyber Security Division（NCSD）の一部門である United States Computer Emergency Readiness Team（US-CERT）によって統括されるもので、Einstein プログラムと呼ばれている[4]。

同プログラムは、Homeland Security Act および Federal Information Security Management Act（いずれもブッシュ政権時代の 2002 年に発効）、そして大統領令 Homeland Security Presidential Directive（HSPD）7（2003 年に発令）に基づくもので、その内容は「各連邦政府機関における IT ネットワーク上の活動に関する情報を収集、類型化、分析」することで、「サイバー攻撃の事前探知、ネットワークセキュリティの向上、オンライン公共サービスの稼働率上昇」を実現するための IT システムである、とされている[5]。

なお、EINSTEIN プログラムは、2009 年から 2010 年頃に「EINSTEIN 2」という名のもとで機能の補強が施されている。EINSTEIN 2 では、各省庁および重要インフラを保有する企業のネットワークにおけるインターネット・アクセスポイントに、データトラフィックを監視するセンサ類を設置し、以前の EINSTEIN プログラムに比べ、より能動的に悪意のあるサイバー活動を探知することができるようになっているとのことである[6]。EINSTEIN 2 は、2011 年度中に全省庁によって導入される予定である他[7]、米 ISP（インターネット・サービス・プロバイダ）大手の AT&T 社、Qwest 社および Sprint 社は既に導入済みであるという[8]。また、現在、後継となる「EINSTEIN 3」の開発も進められて

[4] http://www.us-cert.gov/federal/analytical.html
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf
[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf
[6] http://www.upi.com/Top_News/Special/2008/03/03/Analysis-Einstein-and-US-cybersecurity/UPI-23431204569280/
[7] http://www.fiercegovernmentit.com/story/napolitano-einstein-2-be-fully-deployed-2011/2011-01-31
[8] http://www.networkworld.com/news/2010/021110-cybersecurity-einstein-2.html

いるとされ、EINSTEIN 3 では、ネットワークへの不正アクセスを未然に防ぐことに重点が置かれているというが、その詳細については不明な部分が多い[9]。

また、2010 年 7 月頃の報道によると、国防省（Department of Defense、DOD）傘下の国家安全保障局（National Security Agency、NSA）によるサイバー攻撃を未然に阻止するためのイニシアティブも存在するようであり、これは主に従来型の、インターネット接続が想定されていなかった時代に開発された IT インフラの保護を意図したものであるという。このイニシアティブは Perfect Citizen と名付けられており、同イニシアティブでは連邦政府機関のみならず、重要インフラを運営する民間企業も保護対象に入っているという[10]。

② 重要インフラ対策

重要インフラをサイバー攻撃から守るための対策についても、DHS を中心とした取り組みが行われている。同省では、National Infrastructure Protection Plan（NIPP）と呼ばれる、重要インフラ保護に関する枠組みを発表しており、2006 年に第 1 版が作成された後、2009 年に改訂が加えられたものが現在も使用されている。なお、NIPP 自体は、各種重要インフラに対するあらゆる形態（物理的、サイバー問わず）の脅威について対策を策定するものであり、重要インフラを 18 分野に分類した上で、各分野において責任を負う省庁を指定している。このうち、特に IT インフラの保護に関しては、DHS 傘下の Office of Cybersecurity and Communications（CS&C）が担当部署となっている。

③ 研究開発、啓蒙活動

研究開発、啓蒙活動に関しては、サイバーセキュリティに関する意識向上を狙いとして、国立標準技術研究所（National Institute of Standards and Technology、NIST）により統括される教育プログラム National Initiative for Cybersecurity Education（NICE）が 2009 年から開始されている。同プログラムでは、連邦政府関係者に限らず、初等以降の教育段階の生徒に対して、コンピュータを安全に取り扱うための多角的な教育プログラム及び普及啓発体制の整備を目指している[11]。

その他にも、NSA が大統領令 NSD42[12]に基づき実施している、情報セキュリティ専門家の育成を目的とした National IA Education and Training Program（NIETP）という教育プログラムも存在する。同プログラムは、民間企業や大学などと共同で実施され

[9] http://articles.latimes.com/2009/jul/14/opinion/oe-radack14
[10] http://www.eweek.com/c/a/Security/NSA-Cyber-Security-Program-Details-Revealed-275248/
[11] http://csrc.nist.gov/nice/aboutUs.htm
[12] http://www.fas.org/irp/offdocs/nsd/nsd42.pdf

るものであり、将来的にサイバーセキュリティ対策の重要性が更に増大することを見込み、新たな脅威や課題に対応できるだけの人材を育成することを目指している[13]。

また、サイバーセキュリティに関する研究開発は DHS が中心となって行っているようであるが、ほかに、中央情報局（CIA）、DOD なども民間委託等の形で研究開発を実施している。（研究開発については後述。）

(2) 体制

まず、現政権になってからの米国連邦政府におけるサイバーセキュリティ政策の主要動向を以下にまとめた。

（ブッシュ政権）	2002 年 12 月：E-government Act of 2002 成立。うち、Title III は、Federal Information Security Management Act (FISMA)。 2003 年 1 月：国家安全保障省（DHS）業務開始。 2008 年 1 月：包括的サイバーセキュリティ・イニシアティブ（NSPD54/HDPD23）策定。
オバマ政権	2009 年 2 月：Cyber Security 政策の 60 日間での見直しを指示。 2009 年 5 月：Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure 発表。 2009 年 12 月：Cyber Security Coordinator の任命。 2010 年 2 月: Cybersecurity Enhancement Act が下院を通過[14]。 2010 年 3 月: Comprehensive National Cybersecurity Initiative（CNCI）に関する機密文書の一部が一般公開[15]。 2010 年 5 月: サイバー司令部の司令官に Keith B Alexander 元帥が就任[16]。 2010 年 7 月: NSA が Perfect Citizen と称するイニシアティブを開始するとの報道[17]。 2010 年 12 月: Protecting Cyberspace as a National Asset Act が、2011 年度議会会期中に再審査されることが決定[18]。

次に、米国におけるサイバーセキュリティ政策の実施体制、及び関連主要省庁（NSA、DOD、DHS、OMB、NIST）の取り組みについて紹介する。

---

[13] http://www.nsa.gov/ia/news/2010/cyber_security_education.shtml
[14] http://www.govtrack.us/congress/bill.xpd?bill=h111-4061
[15] http://www.itworld.com/security/98614/obama-administration-partially-lifts-secrecy-classified-cybersecurity-project
[16] http://securitywatch.eweek.com/cyber-war/serious_challenges_await_head_of_cyber_command.html http://securitywatch.eweek.com/cyber-war/serious_challenges_await_head_of_cyber_command.html
[17] http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225702741
[18] http://thomas.loc.gov/cgi-bin/bdquery/z?d111:SN03480:@@@X

① ホワイトハウス

ホワイトハウスにおける主要 IT 関連ポストとしては、最高技術責任者（Chief Technology Officer、CTO）、最高情報責任者（Chief Information Officer、CIO）、そしてサイバーセキュリティコーディネータ（Cybersecurity Coordinator、CSC）の 3 つがあげられる。これらはすべてオバマ政権になって初めて設立されたポストであり、それぞれ Aneesh Chopra 氏、Vivek Kundra 氏、そして Howard Schmidt 氏が就任している。

各ポストが担う役割であるが、まず CTO は「連邦省庁間の連携を深め、IT の観点から国土安全保障、医療費の削減、雇用の創成などの重要課題について大統領を補佐する」とされている[19]。CIO は、「連邦省庁間での情報共有の仕組み、IT システムの相互互換性、および情報セキュリティとプライバシーを確立すること」とされている[20]。CSC については、省庁間のサイバーセキュリティ対策を取りまとめ、政府全体が指針とすべき方向性を示す、などのいわば事務的な役割が期待されているようである[21]。

これらのポストの関係については、CIO と CTO は、サイバーセキュリティ政策についてのみならず、IT 関連政策全般について大統領を補佐するポストであるのに対して、CSC はサイバーセキュリティ政策に特化したポジションであるといえる。このため、CIO と CTO は、IT 政策全般の一部としてサイバーセキュリティ政策に関連する技術的な助言を行い、CSC はそのような意見を取りまとめ情報セキュリティ政策の統括に活かすとの役割分担がされていると考えられる。

② NSA

国家安全保障局（NSA）は、「外国からの暗号通信を収集・分析し、国防政策を支援する」ことが設立目的であったことからも、活動実態には不明な点も多く[22]、NSA の情報セキュリティ体制についても、得られるのは断片的な情報のみとなっている。

この中で、最近報道された NSA の取り組みとして、Perfect Citizen と称する重要インフラ保護対策がある。これは、2010 年 7 月に Wall Street Journal 紙が最初に報道したもので、政府機関および重要インフラを運営する民間企業の IT システムに監視装置を設置し、不審なネットワーク活動を探知することで、サイバー攻撃の検知や対処方法の開発を行う活動として紹介されている[23]。しかし、従来は米国外からの脅威に対処

---

[19] http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff/chopra
[20] http://www.whitehouse.gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/
[21] http://www.pcworld.com/article/165756/obama_cybersecurity_coordinator_wont_be_czar.html
[22] http://www.wired.com/dangerroom/2010/10/doc-of-the-day-nsa-dhs-trade-players-for-net-defense/
[23] http://www.pcworld.com/businesscenter/article/200824/nsas_perfect_citizen_program_what_you_need_to_know.html

することに専念していると思われていた NSA が、このように国内でも監視活動を行う、という Perfect Citizen の内容には、NSA の秘密主義も相まって、各界より多くの懸念が寄せられている[24]。

なお、2010 年 10 月には、NSA と DHS の間で情報セキュリティ対策について協力体制を築くことを確認する覚書が交換されている。この協力体制についても、多くの情報が公開されているわけではないが、少なくとも両省庁の間で人材の交換が行われることが判明している[25]。これは、NSA が情報セキュリティに関してより多くのノウハウを持っており、そのようなノウハウを、米国市民に対する行動権限がより明確に定義されている DHS に吸収させることによって、市民のプライバシー権利が侵害されないようにするためとの指摘もある[26]。

③ DOD

国防総省（DOD）において情報セキュリティに関する中心的な業務を行うのは、サイバー司令部（Cyber Command）である。これは、2010 年 5 月に設立が発表されたもので、同年 11 月に正式に活動を開始している。Cyber Command の活動内容は、主に DOD の IT システムを外部の脅威から保護する、ということに重点が置かれたものとなっている。つまり、DOD は米軍全体を統治する立場にあることから、その延長として Cyber Command が米軍全体の IT インフラ保護を支援する役目を担っているといえる[27]。なお、米軍の指令系統において Cyber Command は、Strategic Command（戦略軍）の傘下と位置づけられている。

また、Cyber Command の活動指針には、「サイバースペースにおいて、米国および同盟国が自由に行動できることを保証する」という記述がある一方で、「敵対勢力がサイバースペースにおいて自由に行動できないようにする」こともあげられていること[28]などを考えると、いわゆる「サイバー戦争」が発生した場合において、国防総省の情報通信経路を確保し、サイバースペースへの安全なアクセスを確保するという受動的な役割にとどまらず、Cyber Command の主導で、米国に敵対する勢力の IT システムに対しサイバー攻撃を仕掛ける、などの能動的な活動を行う可能性も想定されているようである[29]。なお、Cyber Command の具体的な活動動向についてはほとんど明らか

---

[24] http://www.theregister.co.uk/2010/07/08/perfect_citizen/
[25] http://www.wired.com/dangerroom/2010/10/doc-of-the-day-nsa-dhs-trade-players-for-net-defense/
[26] http://www.huffingtonpost.com/leslie-harris/dhs-nsa-in-cybersecurity_b_764289.html
[27] http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf
[28] http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf
[29] http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

にされていないが、一部の報道によると、Cyber Command は「約 15,000 のコンピュータネットワークを管理し、1 日当たり約 90TB のデータをスキャン（検査）」している、とされることから、大規模な IT システムを運営していると考えられる[30]。

なお、Cyber Command は、ホワイトハウスが主導し、DHS によって統括されている民間 IT インフラ向けのサイバーセキュリティ政策とは別の指令系統にて運営されていると考えられる。この根拠としては、上述のように Cyber Command は大統領ではなく Strategic Command に報告する立場とされていることや[31]、DOD 高官自身が「DOD のサイバーセキュリティ対策は Cyber Command に、それ以外の連邦政府機関のサイバーセキュリティ対策は DHS に」よって責任が負われるべきである、と言及していることがあげられる[32]。

もちろん、米国においては大統領が米軍最高司令官という立場を兼任している以上、間接的には連邦政府のサイバーセキュリティ指針が Cyber Command においても遵守される。しかし、実際の運営面や役割分担という面では、DOD はホワイトハウスから独立した指令系統を維持していると推測できる。

④ DHS

国土安全保障省（DHS）において主に情報セキュリティに関する業務を担当するのは、DHS 長官直属の National Cyber Security Center（NCSC）と呼ばれる組織である。DHS のプレスリリースによると、NCSC の任務は、サイバーセキュリティにおける課題についての意見調整、情報共有、意識向上などの事項について、省庁間の連携を促進することとされているものの[33]、プレスリリースを除いて DHS のウェブサイト上には NCSC に関する記述はほとんどない他、その行動指針についても公開されておらず、NCSC の活動内容には不透明な点が多い[34]。

また、DHS の傘下組織としては National Cyber Security Division（NCSD）も情報セキュリティに関する業務を行っている。NCSD の業務は、連邦政府外の行政組織、民間企業および外国の関連組織と協力して米国のサイバーセキュリティ対策を改善することとされている。NCSD は、このような行動指針のもと、各省庁における情報セキュリティリスクマネジメントの支援を行う他、一般市民を対象とした啓蒙活動や、Cyber Storm と呼ばれる、サイバー攻撃を想定した演習なども行っている[35]。また、US-CERT も NCSD に所属している。なお、NCSD は上述の CS&C に所属する部署という扱い

http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html
[30] http://www.v3.co.uk/v3/news/2274867/rsa-cyber-command-nsa
[31] http://www.stratcom.mil/factsheets/Cyber_Command/
[32] http://www.defense.gov/speeches/speech.aspx?speechid=1399
[33] http://www.dhs.gov/xnews/releases/pr_1206047924712.shtm
[34] http://news.cnet.com/8301-13578_3-10004266-38.html
[35] http://www.dhs.gov/xabout/structure/editorial_0839.shtm

になるが[36]、CS&C は NIPP によって国家の IT インフラを保護する責任を負わされていることから、NCSD は情報セキュリティの観点から IT インフラを守るための組織であるといえる。

また、2009 年 10 月には DHS 内部で National Cybersecurity and Communications Integration Center（NCCIC）という組織が新たに設立されている。これは、サイバー脅威に関して「監視と警告」を行うための IT システムを収容する施設であり、US-CERT、NCSD、National Coordinating Center for Telecommunications（NCC）[37]などの組織を「運営面」で統括することを目的としている[38]。このため、NCCIC とは、これらの組織間で IT リソースを共有することで、よりシームレスな情報共有・連携体制を目指すものであるといえる。

情報セキュリティ関連の研究開発活動については、2004 年に設立された Cyber Security Research and Development Center[39]のほか、自主研究開発及び民間委託を行っている Homeland Security Advanced Research Projects Agency (HSARPA) が担当している。（研究開発については後述。）

このように、DHS 内にはサイバーセキュリティ業務を担当する部署が複数存在し、研究開発からサイバー攻撃を想定した演習まで、様々な活動を行っている。DOD のプレスリリースにおいても、「DHS が米国の情報セキュリティ対策を事実的にリードしている」とする記述があり、投入リソースの面からも DHS がサイバーセキュリティ政策遂行の中心となっていると考えられる[40]。少なくとも連邦政府内においては、DHS が情報セキュリティ対策を統括する機関とする共通認識が存在するようである[41]。

⑤ OMB

行政管理予算局（OMB）の情報セキュリティ関連活動は、主に情報セキュリティ対策に関する予算策定の面から、関連省庁をサポートすることに重点が置かれている。つまり、毎年大統領が予算教書を議会に提出するに当たって、情報セキュリティ対策費が占める割合や各省庁への配分を決定するのが OMB の主要な役割とされている[42]。

---

[36] http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm
[37] サイバー・物理的攻撃を問わず、国家の非常事態時に連邦省庁間での円滑な連絡を確保するための組織 http://www.ncs.gov/ncc/
[38] http://ctovision.com/2009/10/dhs-opens-the-national-cybersecurity-and-communications-integration-center-nccic/
http://www.continuitycentral.com/news04845.html
[39] http://www.cyber.st.dhs.gov/
[40] http://www.defense.gov/news/newsarticle.aspx?id=61356
[41] http://broadbandbreakfast.com/2010/07/omb-and-dhs-clarify-cybersecurity-responsibility-and-activities-within-the-executive-branch/
[42] http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf

また、OMB が責任を負うその他の情報セキュリティ関連業務としては、連邦省庁に情報セキュリティを確保するための体制確保を求める連邦情報セキュリティマネジメント法（Federal Information Security Management Act, FISMA）に基づく、同法遵守状況の議会への報告がある。なお、同法に基づく各省庁の報告は、年間 23 億ドルものコストを要していたと指摘されており[43]、効率化の観点から 2010 年からオンライン化されている[44]。このように、OMB の情報セキュリティ関連活動は、予算策定や、アカウンタビリティの確保という面から、運営面での支援を行うことが中心となっている[45]。

⑥ NIST

国立標準技術研究所（NIST）は、商務省（Department of Commerce、DOC）所属の一部署ということもあり、情報セキュリティに関して、直接的に治安維持や国防に関わる活動を行っているわけではない。しかし、NIST は、FISMA に基づき、連邦政府におけるセキュリティ関連の規格、標準、ガイドライン策定について統括しており、実質的に連邦政府におけるセキュリティ関連ツール・サービス類の採用基準を規定している他、NIST が発行する暗号化技術標準についての文書は、この分野において、世界中でデファクトスタンダードとして参照されている。このような活動を行っていることから、NIST は、DOC の一部門という位置づけながらも、米国連邦政府のサイバーセキュリティ政策立案・実行において、大きな役割を担っていると言える。

サイバーセキュリティ関係の技術標準に関しては、NIST では、OMB、NSA、Government Accountability Office（GAO）を始めとする連邦政府機関、および民間企業・団体と協力して策定に当たっている。また、OMB と協力し、技術面から連邦政府機関が FISMA 準拠を達成できるように支援することも NIST の任務の 1 つとなっている[46]。その具体例としては、FIPS や SP 800 シリーズが挙げられる[47]。

まず、FIPS であるが、これは正式名称を Federal Information Processing Standard（連邦政府の情報処理に関する標準）とするもので、米軍以外のすべての連邦組織、および連邦政府の下請け業者の IT システムにおいて採用されるべき技術標準、と位置づけられている。FIPS によって定義される技術標準の分野には、例えば暗号化やハッシュ化、認証、デジタル署名および LAN のセキュリティなどがあり、NIST は情報セキュリティに関わる事項について、広範囲に標準策定の活動を行っている[48]。

---

[43] http://www.meritalk.com/pdfs/FISMA-Facelift-CyberScope-Report.pdf
[44] この報告実施のため、OMB は 2009 年に報告ツール CyberScope を開発している。
http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
[45] http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf
[46] http://csrc.nist.gov/groups/SMA/index.html
[47] http://www.ipa.go.jp/security/publications/nist/index.html
[48] http://csrc.nist.gov/publications/PubsFIPS.html

次に、SP 800 シリーズであるが、これは連邦政府での情報セキュリティ対策を支援する目的で、NIST が発行する様々な文書群のことを指す。SP 800 シリーズに含まれる文書は、情報セキュリティ対策を講じる上での心構えについて記した小冊子から、クラウドコンピューティングの仕組み導入時におけるセキュリティガイドラインなど多岐にわたっている[49]。また、SP 800 シリーズを参照する組織としては連邦政府が想定されているとはいえ、同シリーズに含まれる文書の多くは、普遍性が高く、官民関係なしに適用可能な内容であるものが多くなっている。従って、同シリーズは、民間企業の IT 担当者が情報セキュリティ方策を考える上でも参考になるものである。

⑦ 州政府

米国の一部の州では、独自のサイバーセキュリティに関する州法を持っている。このような州法の代表例としては、Notice of Security Breach Act（カリフォルニア州、2003 年成立）や Information Security Breach and Notification Act（ニューヨーク州、2005 年成立）がある。これらは、いずれも類似した内容の法案であり、個人情報を管理・利用する企業などがサイバー攻撃を受け、個人情報が流出した可能性があると考えられる時に、それら個人に対してサイバー攻撃を受けた旨を通知しなければならない、とするものである。なお、両州とも、「個人情報」の定義を「社会保障番号（Social Security Number、SSN）、運転免許証（またはそれに準ずる ID カード）、銀行口座番号（あるいはデビット・クレジットカード番号）と PIN 番号の組み合わせ、のいずれか」と定めており、何をもって重要な個人情報とするか、については、ある程度のコンセンサスが見られる[50]。

[49] http://csrc.nist.gov/publications/PubsSPs.html
[50] http://www.cscic.state.ny.us/security/securitybreach/
http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=2668

3. 最近の政策動向

本章では、米国のサイバーセキュリティ政策の最近の動向について紹介する。

(1) 2010 年以降の動向

① NCIRP

2010 年 9 月に、「サイバー攻撃の脅威にいかに対処するか」という問題意識のもと、その対処に向けた体制の枠組みを定める National Cyber Incidence Response Plan（NCIRP）という計画が策定されている。NCIRP は、元々2009 年 5 月にホワイトハウスによって発表された白書（サイバーセキュリティ政策レビュー報告書）においてその策定が想定されていたものであり、その策定は、同文書において連邦政府が達成すべき短期的な目標の 1 つとして挙げられていた[51]。

NCIRP は、DHS が中心となって作成したもので、連邦政府内での連携体制の改善を目指す内容となっている。具体的には、同計画は、各連邦及び地方政府機関がサイバー攻撃時に負う責任や、それに基づいて果たすべき役割、また各機関がどのように連携を取るべきかについて規定している。また、非常時に各機関がそのような役割を果たせるかどうかをテストするための演習についても定めており、これが下記の Cyber Storm に相当する。また、連邦政府機関のネットワークを監視する仕組み（上述の EINSTEIN プログラム）や、万がーサイバー攻撃により損害を受けた場合の IT インフラの復旧方法などについても NCIRP によって言及されている[52]。

NCIRP は、以上のように、攻撃の未然防止と IT インフラの継続運用という両面から国家的なサイバーセキュリティ体制について定める計画であるといえる。また、これと同時に、米国軍隊及び諜報機関に直接関連性がない IT インフラについては、非常事態のリーダーシップが DHS に移管されることも定められており、より明確な指令体制の確立も図られている。

なお、このように幅広く連携体制について定めている NCIRP であるが、特に連邦政府機関による体制については、ブッシュ政権時代より維持されていた National Cyber Response Coordination Group（NCRCG）を置き換える形で、Cyber Unified Coordination Group（UCG）という体制について新たに言及している。元々NCRCG とは、「重大な」サイバー攻撃の脅威が発生した場合に、非常時権限を関連省庁に与え、それらの省庁を統括するための体制についてまとめたものであった[53]。

---

[51] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[52] http://www.helium.com/items/1988496-an-overview-on-the-national-cyber-incident-response-plan
[53] http://www.dhs.gov/xabout/structure/editorial_0839.shtm

UCG と NCRCG の間で、非常事態に備えて定められた基本的な枠組みについての構図は大差なく、いずれも DHS、DOD を始めとする関連省庁から派遣されたサイバー専門家によって構成される特別委員会（Coordination Group）が中心となる。しかし、その枠組みを統括する機関は異なっており、NCRCG では DHS、DOD、そして司法省（Department of Justice、DOJ）の共同体制であったのに対し[54]、UCG においては DHS のみがその役割を与えられている[55]。

また、NCRCG と UCG 間のもう 1 つの相違点として、前者はあくまでサイバー攻撃の脅威が高まった場合にのみ適用されるのに対し、後者はそのような脅威の程度に関わらず、恒久的に活動することが想定されていることがある。NCIRP によると、平常時でも「UCG 構成員は最低 1 か月に 1 回は会合を持ち、NCIRP に基づいて参加省庁間の円滑な連携を保証し」サイバー脅威に備えることが定められている[56]。

つまり、サイバーUCG とは、サイバー攻撃に備えた連邦政府機関の連携体制におけるリーダーシップをより明確にし、平常時から省庁間の情報共有を促進することで、より強固なサイバー攻撃対策を目指す体制であるといえる。

② Cyber Storm

前章で触れたように、DHS はサイバー攻撃を想定した演習も実施しており、これは Cyber Storm と呼ばれている。Cyber Storm は、2006 年 2 月に初めて実施され、2008 年 3 月には第 2 回目、そして 2010 年 9 月には第 3 回目が実施された。第 3 回目の Cyber Storm III においては、7 つの省庁（DOC、DOD、DOE、DHS、DOJ、運輸省、財務省）、ホワイトハウス、11 の州政府、12 か国の政府、そして重要インフラに関わる 60 の民間企業が演習に参加した[57]。また、Cyber Storm III は、上述の NCIRP によってその実行が規定された初めてのサイバーセキュリティ演習であり、I や II に比べ、より横断的かつ広範にサイバーセキュリティ対策の施策状況をテストするものであったといえる。

Cyber Storm の目的は、模擬サイバー攻撃を実施することによって、NCIRP によって定められたサイバー攻撃対策の達成度を測定し、各組織の対策における欠陥、脆弱性を発見することにある。また、Cyber Storm の最も中心的な目的は「国家機能の復元性」を監査することとされていることから[58]、重要インフラの継続運用・復旧を念頭に置いた演習内容となっていると考えられる。

---

[54] http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf
[55] http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf
[56] http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf
[57] http://www.dhs.gov/files/training/gc_1204738275985.shtm
[58] http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf

③ NIST

＜サイバーセキュリティ教育に向けた取り組み＞

NIST は、2010 年 4 月、サイバーセキュリティ人材の包括的な育成体制構築を目指すイニシアティブ（NICE）の開始を発表している[59]。（NICE の詳細については後述。）

＜スマートグリッドに関するサイバーセキュリティガイドラインの画定＞

NIST は、2010 年 9 月、現在米国で展開が進み始めているスマートグリッドについて、そのサイバーセキュリティ体制に関するガイドラインを発表している。これは、スマートグリッドが満たすべき情報セキュリティの要項について記述している他、スマートグリッド利用者の情報プライバシー、セキュリティに対するリスクを審査するための枠組み、あるいは送電網を運営する企業がどのように送電網を「スマート」化すべきかについての助言などの課題にも言及している。このガイドライン発表によって、官民を含めた国家全体で、スマートグリッド普及を促進する協力体制が整備されることも期待されている[60]。

＜情報セキュリティリスクマネジメントに関する文書＞

NIST は、2010 年 12 月、業務全体における情報セキュリティリスクマネジメントについて記述した文書（SP800-39）の最終ドラフトを発表している。これは、連邦政府機関やそのコントラクター（下請業者）が IT システムを業務に使用する中で、重要な情報のセキュリティに関するリスクマネジメントをどのように行うべきかについて助言するものである。なお、NIST は、同文書に関して 2011 年 1 月まで一般公衆からも意見を募集していた。同文書は、これらの意見を元に、2011 年をめどに最終化される予定となっている[61]。

＜個人のアイデンティティの信頼性向上に向けた動き＞

オバマ政権は、2011 年初頭より、e コマースや SNS など、オンラインサービスの利用時に使用される個人のアイデンティティ識別情報（ID）について、より信頼性の高いオンライントランザクションがより広範囲に行われることを目指し、客観的な第 3 者が ID を審査、認証を行う取り組みを提案している。これは、National Strategy for Trusted Identities in Cyberspace（NSTIC）と称するもので、NIST 主導でその実現に向けた体制が整備されつつある。NSTIC は、官民連携体制のもとでの推進が重要視されており、2011 年 2 月には、そのリーダーとして官民両方での経験を持つ Jeremy Grant 氏が任命されている[62]。これは、サイバーセキュリティ体制の強化の一環として、一般個人ユーザの観点からもセキュリティ確保の働きかけを進めている取り組みであると言える。

---

[59] http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224700519
[60] http://www.smartmeters.com/the-news/1171-nist-releases-grid-cyber-security-guidelines.html
[61] http://www.healthimaging.com/index.php?option=com_articles&article=25771
http://csrc.nist.gov/news_events/news_archive/index.html
[62] http://www.executivegov.com/2011/02/nist-names-industry-veteran-to-lead-identity-ecosystem/
http://www.nist.gov/nstic/

④ 産業界における対応

2010 年 12 月には、NIST、DHS および Financial Services Sector Coordinating Council（FSSCC）の間で、金融業界の IT インフラにおけるサイバーセキュリティ強化に向けて、共同で研究開発を進めることについて定めた覚書が交わされている[63]。この覚書の CNCI 上の位置づけについては不明であるが、金融機関という重要な国家インフラを保護するための方策であることは間違いなく、連邦政府機関に限らず、産業界も巻き込んだサイバーセキュリティ対策が進められていることがわかる。

なお、この覚書自体では、実際にどのような分野で研究開発活動が行われるのか、資金的な援助などに関して言及されておらず、あくまでもこれらの 3 者による研究開発に関する協力体制を確立することが目的となっている[64]。

この協力体制においては、(a)FSSCC が金融機関独自の IT システムについての研究開発、(b)NIST が業界における技術標準の策定に向けた研究開発、そして(c)DHS の科学・技術（Science and Technology、S&T）部門がサイバーセキュリティに特化した研究開発を行うことで、各者の強みを統合させ、ひいてはより包括的な研究体制の確立につなげることが図られているといえる[65]。具体的な研究開発の内容としては、まず高信頼性 DNS（Domain Name System）と、ユーザーID を管理・処理するための仕組み、の 2 つが対象とされているようである[66]。

⑤ WikiLeaks への対応

米国においては、2010 年半ばから後半にかけて、連邦政府所属の機密文書の一部が告発サイト WikiLeaks によって無断で一般公開されたことが話題となっており、これらの書類には、DOD が保管していたイラクおよびアフガニスタン戦争に関わる機密文書も含まれていた。

本件は、サイバーセキュリティの仕組みに不備があったために発生したものではない、とする見方が支配的であるが、今回の文書流出を機に、DOD はその情報セキュリティ体制の更なる改革に着手している。これを機に、DOD では複数の取り組みが行われているが、その代表的な例として、Host-Based Security System（HBSS）と呼ばれる仕組みの導入が加速されることが予想されている[67]。

---

http://arstechnica.com/security/news/2011/01/identity-ecosystem-inside-uncle-sams-trusted-identity-proposal.ars

[63] http://www.cybersecuritymarket.com/2010/12/12/new-public-private-cybersecurity-partnership-nist-dhs-and-financial-sector/

[64] http://www.whitehouse.gov/sites/default/files/microsites/ostp/FSSCC_DHS_NIST_MOU_12062010.pdf

[65] http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation

[66] http://publish.ndia.org/Divisions/Divisions/HomelandSecurity/Documents/NDIA-149C-Maughan%20Proceedings.pdf

[67] http://homelandsecuritynewswire.com/pentagon-revamps-security-wake-wikileaks?page=0,1

HBSS とは、DOD が機密情報通信用に使用する専用ネットワーク（Secret Internet Protocol Router Network、SIPR）に接続されているコンピュータ端末にセンサ類を設置することで、そのネットワークに対する不正アクセスや、悪意ある活動を検知することを目指す仕組みである。HBSS は、2010 年末時点で SIPR 上コンピュータの約 6 割に導入されていたようであるが、DOD では、その導入を更に加速させていく方針であるという。また、DOD では、HBSS の導入を加速化させていく他にも、SIPR 上のコンピュータにおけるリムーバブルディスクの使用を禁止する方針を打ち出しており、機密情報管理の体制を改善させるように努めている[68]。

(2) 研究開発活動

次に、米国政府機関によって行われているサイバーセキュリティ関連研究開発業務のうち、中央情報局（Central Intelligence Agency、CIA）および DOD によって主導されているものについて紹介する。

① CIA

米国連邦政府の対外諜報機関である CIA は、1998 年に In-Q-Tel 社という非営利ベンチャーキャピタルを設立し、民間企業による情報セキュリティ関連の研究活動を資金面から支援している。In-Q-Tel 社は様々な分野における研究事業に投資しているが、情報セキュリティに関しては、以下の分野における活動を行う企業を援助対象としている[69]。

- ID マネジメント
- アクセス管理
- リスク分析能力
- IT システムデザインおよび分析ツール類
- セキュリティポリシーの規定と管理

In-Q-Tel 社の目的は、「諜報コミュニティにおけるニーズ」と「民間における科学技術の発展」の間を仲介し、前者が必要とするセキュリティ関連製品・サービスにおいて、民間の研究開発活動の最新成果が反映されるように努めること、とされている。このような意識のもと、同社は積極的に投資を行っており、民間からビジネスプランの募集も行なっている。同社は、設立以来約 7,500 件に上るビジネスプランを審査しており、そのうち約 150 に対して資金援助を行ったという。また、このように In-Q-Tel 社が投資を行った民間企業によって今までで約 300 件の技術が開発され、CIA やその関連組織による採用に至ったという[70]。

---

[68] http://homelandsecuritynewswire.com/pentagon-revamps-security-wake-wikileaks?page=0,1
[69] http://www.iqt.org/technology-portfolio/index-security.html
[70] http://www.iqt.org/mission/IQT%20Corporate%20Fact%20Sheet.pdf

② DOD

CIA が対民間投資をもって研究開発活動を促進しているのに対し、DOD では、国防高等研究計画局（Defense Advanced Research Projects Agency、DARPA）という省内の部署を中心に研究開発を実施している。DARPA は、軍事転用可能な先端技術について広範に渡る分野で研究を行っている[71]。DARPA は、そのような研究成果の 1 つとして、一般的にインターネットの原型とされている ARPANET という仕組みを開発した組織として知られていることからも、情報セキュリティに関する研究開発活動も積極的に行っていると見られる。

DARPA が現在行っている研究プロジェクトの中でも、特に情報セキュリティとの関連性が高いものとしては、Cyber Defense というプロジェクトがある。同プロジェクトで集中的に行われている研究のトピックは、「DOD の機密情報、省内情報インフラ、およびミッションクリティカルな IT システムを保護するために、その中核となる情報通信技術の開発を行うこと」であり、例えばネットワーク上のマルウェアなどを自動的に探知する仕組みや、ネットワーク上の通信トラフィックを監視する仕組みが同プロジェクトにおいて開発されており、このような技術の活用によって、高い費用効率を維持しつつ DOD の IT インフラが（サイバー攻撃時にも）継続運用可能となることを目指している[72]。

なお、DARPA は、2010 年度に合計で約 4,979 万ドルを CNCI に基づいたプロジェクトに投入していたとされているものの、2011 および 2012 年度にはこれが約 1,000 万ドルにまで削減される予定であるという[73]。また、DARPA は機密情報扱いのプロジェクトも行っており、これらの予算額は一般公開されていないため、DARPA 全体の予算については確認できなかった。

③ DHS

DHS も、上記の DARPA に相当する部署を省内に持っており、これは Homeland Security Advanced Research Projects Agency（HSARPA）と呼ばれている。同部署の目的は、「国土安全保障に関する研究開発を行い、DHS の業務に大きく貢献するための革新的な技術を生み出すこと」とされており、自前で研究開発活動を行う他にも、民間企業や大学などと共同研究を行う体制も整えているという。実際に、HSARPA は公募を行うポータルサイトも設置しており、複数の研究プロジェクトについて、一般企業・団体から研究開発活動のアウトソース先を募集している[74]。なお、HSARPA が直属するのは、DHS 内の Office of the Director of Innovation という部門であり、同部

---

[71] http://www.darpa.mil/our_work/

[72] http://www.darpa.mil/Our_Work/I2O/Programs/Cyber_Defense_(Cyber_Genome,_Dynamic_Quarantine_of_Computer_Based_Worm_Attacks,_and_Scalable_Network_Monitoring).aspx

[73] http://www.fiercegovernmentit.com/story/cybersecurity-runs-deep-fiscal-2012-budget-request/2011-02-16

[74] https://baa.st.dhs.gov/index.asp

門の 2010 年度における予算額は、約 4,400 万ドルとなっている。また、2011 年度には、これが約 5,500 万ドルに増額されると想定されている[75]。

(3) サイバーセキュリティ関係人材育成

現在の米国におけるサイバーセキュリティ業界は比較的小規模に留まっており、2009 年の CNN 社による報道によると、全米で約 13,000 人が同業界で雇用されているに過ぎない。

しかし、今後サイバーセキュリティ関係の人材需要は増える傾向にあると予想される。同報道では、2006 年から 2016 年までの 10 年間にサイバーセキュリティ業界における雇用数が約 27%増加する、との予測を立てており、今後サイバーセキュリティ関係人材に対する需要が急速に伸びるとしている[76]。また、民主党所属の Dutch Ruppersberger 下院議員は、2011 年 2 月に出身の Maryland 州で行った演説において、「10 年後には、シリコンバレーよりも、（連邦政府機関が集中する）Washington DC 都市圏の方が多くの IT 技術者を雇用していることだろう」と述べており、将来的に連邦政府によって多くの情報セキュリティ関連人材が求められるようになる、という見解を示している[77]。

米国では、このような状況を踏まえ、サイバーセキュリティ人材の育成を目指す複数のプログラムが運営されている。その代表例について以下に紹介する。

① NICE

「サイバーセキュリティに関する国家イニシアティブ（National Initiative for Cybersecurity Education、NICE）」とは、連邦政府機関によるサイバーセキュリティ専門家育成のみならず、一般国民に対してもサイバーセキュリティ教育を行い、サイバー空間におけるベストプラクティスの遂行を奨励することで、国家全体でサイバーセキュリティ体制の強化を目指す取り組みである。

同イニシアティブも、元々は 2009 年 5 月発表のサイバーセキュリティ政策レビューにて、その開始がとりあげられていたものである。具体的には、同レビューにおいて「サイバーセキュリティの向上に向け、世論の意識を高めるための PR 活動や、教育プログラムを実施すること」が短期的な課題の 1 つとして挙げられており[78]、NICE がこのような課題の解決に向けた方策として位置づけられているといえる。

---

[75] http://www.dhs.gov/xlibrary/assets/budget_bib_fy2010.pdf
[76] http://money.cnn.com/magazines/moneymag/bestjobs/2009/snapshots/8.html
[77] http://www.hometownannapolis.com/news/sch/2011/02/14-29/form_engagements.html
[78] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

NIST によると、NICE は、(a)サイバーセキュリティに関する意識向上（DHS が統括）、(b)公式のサイバーセキュリティ教育プログラム（教育省及び Office of Science and Technology Policy が統括）、(c)連邦機関におけるサイバーセキュリティ専門家採用（Office of Personnel Management が統括）、そして(d)連邦機関内部でのサイバーセキュリティ教育（DOD、DHS、Office of the Director of National Intelligence）、4つのトラックにより構成される[79]。

まず、(a)であるが、これは DHS の分担により、一般国民に対する PR 活動を行い、サイバーセキュリティに対する大衆の意識向上を図るイニシアティブである。このイニシアティブによって、一般個人による「責任感のある（responsible）」インターネットの使用が推進され、結果的に一般個人のオンラインプライバシーが守られることが想定されている。この一環として、DHS は「Stop. Think. Connect.」という啓蒙活動を行っており、各一般ユーザがオンラインで情報の送受信・共有などを行う前に、「一旦立ち止まって、その行動の結果について考える」、つまり一人一人がオンラインでの行動について責任をもつことの重要性を強調する内容となっている[80]。

次に、(b)は、教育省（ED）及び Office of Science and Technology Policy（OSTP）の分担で、幼稚園・保育園レベルから大学・大学院・職業訓練学校のレベルまで、包括的にサイバーセキュリティ教育を行うためのカリキュラム作成が計画されている。このイニシアティブにおいては、特に科学、ハイテク、工学、数学などの分野での教育改革を行うことで、将来的にサイバーセキュリティ人材が恒久的に育成されることが目指されている[81]。

(c)は、Office of Personnel Management（OPM）の分担で、連邦政府機関が有能なサイバーセキュリティ人材にとって魅力的な就職・転職先となることを目指すイニシアティブである。同イニシアティブでは、連邦政府機関において必要とされるサイバーセキュリティ関連職種の明確化や、人材に求められる資質・資格の規定が実施されることとなっている。これらによって、必要な人材像が明確に定義されることで、最終的に連邦政府機関が有能な人材を採用できるようになることが期待されている[82]。

最後に、(d)は、連邦政府機関内部でのサイバーセキュリティ人材教育制度の作成を念頭においたイニシアティブである。DOD、DHS 及び Office of the Director of National Intelligence の分担で、以下のサブトラックに分かれて連邦政府職員の教育を行うことが想定されている。

---

[79] http://csrc.nist.gov/nice/aboutUs.htm
[80] http://csrc.nist.gov/nice/awareness.htm
[81] http://csrc.nist.gov/nice/education.htm
[82] http://csrc.nist.gov/nice/workforce.htm

- 一般職員によるインターネット利用時のベストプラクティス（DHS、Federal CIO Council 主導）
- IT インフラ運用・メンテナンス及び情報の取り扱い（DOD、DHS 主導）
- 治安維持及び防諜活動（DOJ 主導）
- その他特別活動（NSA 主導）

以上、NICE は一般国民の啓蒙、専門家の育成、専門家の連邦機関による採用、そして連邦機関内部での教育、という包括的な教育体制の構築を目指しているといえる。また、充実した教育体制の実現をもって、米国に対するサイバー攻撃の可能性を低減する、という目的達成も期待されている。

② US Cyber Challenge

US Cyber Challenge（USCC）とは、官民共同体制で設立された組織であり、主に大学院生・学部生・高校生を対象に、全米の有能なサイバーセキュリティ人材を発掘し、これらの人材に専門教育を行い、政府機関、大学あるいは民間企業への就職活動を支援することを目的としている[83]。

USCC は、IT に関する知識・技能を問う競技大会を複数実施することで人材の発見を図っている。これらの競技大会には、(a)DOD 主催の Forensics（犯罪科学）Challenge、(b)同じく DOD（空軍）主催の CyberPatriot、(c)非営利団体 SANS Institute 主催の NetWars Capture-the-Flag などがある。

(a)では、主に防諜活動による活用を目的に、革新的な科学捜査の方法や仕組みが考案されることが期待されており、25 の異なる大会が主催されているという。これらの大会の勝者には、DOD 主催のサイバーセキュリティ会議に無料参加できる他、International Council of Electronic Commerce Consultants 主催のサイバーセキュリティ教育プログラムを無料で受けられるなどの特典が与えられる[84]。

(b)は、全米の高校生を対象に、サイバーセキュリティに対する課題を与える大会を主催することで、「サイバーセキュリティに対する関心を高め、高校から大学を経由するキャリアパスを提示し」、結果的にサイバーセキュリティ人材の充実を図るもの、とされている。このような意向のもとに、一部の参加者に対しては奨学金、専門家による特別教育、あるいは就職先の紹介などのサポート体制も用意されているといい、高校卒業時という比較的早い段階から将来的な人材の確保を目指していることが特徴であるといえる[85]。

---

[83] http://www.uscyberchallenge.org/
[84] http://www.uscyberchallenge.org/competitions/dc3-digital-forensics-challenge.cfm
[85] http://www.uscyberpatriot.org/about/Pages/FAQ.aspx

また、(c)は、不特定の参加者を対象に、IT システムの脆弱性やセキュリティホールなどを発見する知識・技量を問う内容の大会となっている。同大会の参加者には、Capture-the-Flag（旗取りゲーム）という名前の通り、脆弱性のあるコンピュータを発見、侵入した上で、他参加者からの攻撃を防ぎ、乗っ取られないようにする、という課題が課せられている。これによって、特にコンピュータに関して高い技能を持つ者が、自らの技能を、ハッキングといった悪用の形ではなく、国家のサイバーセキュリティ対策に有効活用することが期待されているという[86]。

③ 奨学金制度

Cyber Challenge とは別に、指定大学・大学院に所属する一部の学生を対象に、奨学金を提供するイニシアティブも行われている。これは National Science Foundation（NSF）がスポンサーとなっているもので、奨学金受給者は、卒業後、連邦政府機関にサイバーセキュリティ関連職で最低 1～2 年勤務することが要求されている。なお、具体的な就職先としては、NSA や DHS などが想定されている[87]。この他にも、大学などの教育機関に対し、サイバーセキュリティ人材育成のための奨学金と称して、私企業が資金提供を行っているケースなども散見される[88]。

④ その他

大学等教育機関のサイバーセキュリティ教育の修了者ではなく、サイバーセキュリティに関する知識を有するものを途中採用する動きもある。例えば、ハッカーを対象とした会議で、同種のものとしては世界最古・最大のイベントの 1 つである DEF CON が毎年米国で開かれているが、この提唱者である Jeff Moss 氏は、2010 年 6 月に DHS 長官直属組織の Homeland Security Advisory Council（HSAC）に登用されている。HSAC とは、国土安全保障に関する事項について、DHS 長官に直接助言を行う有識者の会合であり、Jeff Moss 氏については、サイバーセキュリティに関して「政府とのしがらみがない、第三者の視点から」意見を述べることが期待されているという[89]。

また、DEF CON 自体についても、2001 年 9 月に発生した同時多発テロを機に多くの連邦政府関係者がハッカーを雇用する目的で訪れるようになっており、その一例として、2008 年には米空軍が 60 人の DEF CON 参加者を雇用したという[90]。このように、限定的とはいえ、従来と異なるルートでの人材確保も行われ始めているようである。

---

[86] http://edition.cnn.com/2009/TECH/12/21/cyber.challenge.hackers/?iref=polticker
[87] https://www.sfs.opm.gov/AgencyToolkit.pdf
https://www.sfs.opm.gov/default.asp
[88] http://www.businesswire.com/news/home/20101202005307/en/IID-Launches-Cyber-Security-Scholarship-University-Alabama
[89] http://news.cnet.com/8301-1009_3-10258634-83.html?tag=mncol;txt
[90] http://www.pcworld.com/article/169462/defense_department_eyes_hacker_con_for_new_recruits.html

(4) サイバー空間上のプライバシー保護に関する政策

2010 年 7 月、上院に所属する民主党議員によって、オンラインでの個人プライバシー保護法案の策定に向けた聴聞会が行われた。同聴聞会には、Apple 社、AT&T 社、Google 社、Facebook 社などの大手 IT 企業も参加しており、これらの企業は、業界主導の自主的な個人プライバシー保護体制を確立するのが望ましいと主張したと見られているものの、同聴聞会に参加した John Kerry 上院議員は、2011 年中には法案が提出されるであろう、と述べていた[91]。

また、同時期の 2010 年 7 月に、サイバースペースにおける個人アイデンティティ（ID）の信頼性向上を目指すための戦略（National Strategy for Trusted Identities in Cyberspace）のドラフトが、ホワイトハウスによって公開されている。これによると、将来的には、機密性の高い情報が交換されるオンライントランザクション（例えば、オンラインバンキングや、自身の電子健康情報へのアクセスなど）が行われる際に、トランザクションに関わるステークホルダー（消費者、消費者と取り引きを行う企業など）の ID の信頼性を第 3 者があらかじめ確認しておくことで、安全にトランザクションが行われる環境（ecosystem）づくりが目指されているという[92]。なお、この文書は、2011 年初頭に最終化される予定であり、それに伴って DOC の傘下に専門部署が設立される計画もあるという[93]。

これを受け、2011 年 2 月には、Jackie Speier 下院議員（民主党）が「Do Not Track」と一般的に呼ばれている法案を提出している。同法は、一般個人のオンライン訪問・購入履歴などの個人情報（ライフログ）について、個人の許可なしに、広告目的などでの民間企業の利用を禁じる内容となっている。この法案は、連邦取引委員会（Federal Trade Commission、FTC）に対し、個人が自らのライフログについて、事業者の利用を「効果的で簡素な方法で」拒否することができるよう 18 ヶ月以内に必要な規則の制定を行うよう求めている[94]。

今後の議論によっては、同法案は議会で内容に修正が加えられる可能性もあり、最終的に両院で可決されるかどうかは不透明である。しかし、オンラインプライバシーの保護については、共和党・民主党共に強い関心を示しているとされ、何らかの形でオンラインプライバシーに規定した法案が議会を通過する可能性は十分にあると見られる。

---

[91] http://www.politico.com/news/stories/0710/40304.html
[92] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
[93] http://www.pcworld.com/businesscenter/article/216143/white_house_officials_push_online_trusted_ids.html
[94] http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=229218521&cid=RSSfeed_IWK_All
http://www.latimes.com/business/la-fi-do-not-track-20110212,0,66573.story

以上は、ライフログ事業者のユーザに対する情報開示が十分に行われていないとする問題意識に起因するものであり[95]、一般ユーザの啓蒙という観点からサイバーセキュリティの強化を目指す動きといえる。

(5) セキュリティ機能の評価

民間を含め、強固な情報セキュリティ体制を構築するためには、関連製品・サービスについて、その信頼性や確実性の評価を公正に行うための枠組みの確立も必要である。

このため、情報セキュリティ評価に関する国際技術標準（ISO/IEC 15408）が策定されており、これは一般的にコモンクライテリア（Common Criteria、CC、「共通基準」の意）と呼ばれている。CC によって、「情報セキュリティ製品の設計、実装、および評価の際に必要とされる各プロセスが、厳格かつ基準に沿った形で行われること」の保証が図られている。なお、CC はあらゆる情報セキュリティ関連製品・サービスを意識したものであり、ハードウェア、ソフトウェア製品のみならず、「システム全体」といった抽象的な概念もカバー対象になっている[96]。

米国連邦政府機関では、NSA と NIST が CC の適用促進に当たっており、この 2 省庁が National Information Assurance Partnership（NIAP）と呼ばれる共同パートナーシップを設置し、NIAP が CC による審査と認定に関する枠組み（Common Criteria Evaluation and Validation Scheme、CCEVS）を管理している。このイニシアティブのもとで、情報セキュリティ製品およびサービスの審査を行うための試験場[97]の認定、試験場における審査が行われ、これまで認定された製品・サービスは情報公開されている。なお、最近の動きとして、NIAP は 2010 年 1 月に CCEVS に一部変更を加えており、これによって各製品・サービスの審査にかけられる最大期間が規制されるようになった。具体的には、米国連邦政府によって規定される保護プロファイル（Protection Profile、PP）[98]に準拠している製品については 12 か月以内、これに対し、PP 非準拠、あるいは PP 準拠であっても、より厳密な評価レベル（Evaluation Assurance Level）にて再評価が必要な製品については、24 か月以内に CCEVS に基づいた審査を完了することが定められている[99]。

---

[95] http://www.latimes.com/business/la-fi-do-not-track-20110212,0,66573.story
[96] http://www.ipa.go.jp/security/jisec/about_cc.html
[97] Common Criteria Testing Laboratories（CCTLs）と呼ばれる。
http://www.niap-ccevs.org/ccevs/defined/
[98] PP とは、情報セキュリティ製品カテゴリ別（ファイアウォール、OS、WiFi、など）に、各製品・サービスが達成すべきセキュリティ目標を設定する文書のこと。なお、PP ごとにレベル 1 から 7 までの評価レベル（Evaluation Assurance Level、EAL）が設定されており、評価レベルが高いほど要求されるセキュリティ目標の水準も高くなる。
http://www.niap-ccevs.org/pp/
[99] http://www.niap-ccevs.org/policy/ccevs/policy-ltr-18-update1.pdf

なお、情報セキュリティ製品を調達する際に CC の適用を必須条件としている連邦政府機関は、DOD および諜報・防諜機関などの機密性の高い国防上の情報を扱う機関のみであり、その他の省庁においては、調達基準内に CC を要求していることは稀であるという。この背景には、1990 年代前半に NSA が CC を上述の FIPS に組み込むことを要求したものの、NIST がこれを拒否したため、それら省庁が CC を重視しなかった、との経緯があるとされている[100]。

[100] http://gcn.com/Articles/2010/11/17/Commentary-common-criteria-changes.aspx?Page=2

4. サイバーセキュリティ関係法案の状況

本章では、サイバーセキュリティ関連法案の最近の状況について概説する。

(1) 2010 年度以降に議会提出された主要法律

サイバーセキュリティは国家的な優先事項と認識されているにも関わらず、関連する分野の広さから、米国議会においてさまざまな委員会がサイバーセキュリティに関する権限を求め、多数の重複する法案を提出するも、包括的なサイバーセキュリティ法案の成立にはいたっていない[101]。2010 年以降提出されてきた法案の内容は、サイバーセキュリティ研究開発のための資金提供、サイバー攻撃に対する重要インフラ保護、個人識別情報（ID）盗難対策および関連する消費者保護対策、新たな監督機関の設置など多岐にわたる。以下に、2010 年以降に米国議会に提出された主要サイバーセキュリティ法案について表記する。

【2010 年以降に提出された主要法案】

法案名	提出年月	概要
Cybersecurity Enhancement Act	2009 年 11 月	サイバーセキュリティに関する研究開発や、技術標準画定を促進する法案。2010 年 2 月に下院で可決も、12 月に議会会期満了に伴い廃案。2011 年中に再提出の見込み[102]。
Homeland Security Cyber and Physical Infrastructure Protection Act	2011 年 1 月	Homeland Security Act of 2002 を一部修正し、Cybersecurity Compliance Division の設立や、DHS の権限強化をもって、米国のサイバー及び物理的インフラを保護するための法案。現在 Emerging Threats, Cybersecurity, and Science and Technology 小委員会にて諮問中。2010 年 11 月にも提出されたが、議会会期満了により廃案。
Cyber Security and American Cyber Competitiveness Act	2011 年 1 月	米国のサイバーセキュリティ体制の強化や、IT産業における競争力向上と、米国民及び企業の機密性の高い情報を守るための法案。現在 Homeland Security and Governmental Affairs 委員会にて諮問中。

[101] NIST コンピューターセキュリティ部によると、2009-2010 年の第 111 期国会に提出されたサイバーセキュリティ関係法案は 44 本とのことである（そのほとんどが未成立）。本数の数え方は機関により異なるが、例えば以下の民間サイトではサイバーセキュリティ法案 33 本の一覧が掲載されている。
http://www.govtrack.us/congress/billsearch.xpd?PostFormID=billsearch&session=111&q=cybersecurity&sponsor=&cosponsor=&status=&sort=

[102] http://www.govinfosecurity.com/articles.php?art_id=3340

Cybersecurity and Internet Freedom Act	2011 年 2 月	Homeland Security Act of 2002 や関連法案を一部修正し、米国のサイバー及び IT インフラを強化するための法案。現在 Homeland Security and Governmental Affairs 委員会にて諮問中。2010 年 6 月に Protecting Cyberspace as a National Asset Act の名称で議会に提出されたが、議会会期満了により廃案。

(2) 議会の状況

次に、2010 年 11 月の中間選挙の結果を受けた、サイバーセキュリティ法案に関する上下両院の状況を概説する。

① 上院

中間選挙の結果、与党民主党は上下両院で議席数を減らしたものの、上院では依然として民主党が多数政党となっている。上院においてサイバーセキュリティ関連法案の諮問を中心的に行うのは、Homeland Security and Governmental Affairs 委員会である。同委員会は、8 人の民主党議員、8 人の共和党議員及び 1 人の無党派議員によって占められており、委員長は無所属の Joseph Lieberman 議員が務めている。同委員会は 5 つの小委員会によって構成されるもので、このうち Oversight of Government Management, the Federal Workforce, and the District of Columbia 小委員会と Disaster Recovery and Intergovernmental Affairs 小委員会が特にサイバーセキュリティ関連法案と関連性が深い小委員会であり、それぞれ Daniel Akaka 議員、Mark Pryor 議員（いずれも民主党所属）が委員長を務める[103]。いずれにせよ、米国上院が下院と異なる点として、より党派の壁を超えた議論が行われることが知られている他、Homeland Security and Governmental Affairs 委員長は 2007 年より Lieberman 議員が務めていることからも、上院においてサイバーセキュリティ法案に関する主導権や論調が大きく変化する可能性は低いと考えられる。

② 下院

中間選挙の結果、下院は、上院と異なり、野党の共和党が多数を占めている。下院においてサイバーセキュリティ関連法案の諮問を中心的に行うのは、Homeland Security 委員会である。同委員会の委員長は、共和党所属の Peter T King 議員が務めている他、同委員会は 6 つの小委員会も傘下に入れており、この中で特にサイバーセキュリティ法案と関連性があるのは、Counterterrorism and Intelligence 小委員会（Patrick Meehan 委員長）、Cybersecurity, Infrastructure Protection, and Security Technologies 小委員会（Dan Lungren 委員長）、Emergency Preparedness,

[103] http://hsgac.senate.gov/public/

Response, and Communications 小委員会（Gus Bilirakis 委員長）、そして Oversight, Investigations, and Management 小委員会（Michael McCaul 委員長）の 4 つであるといえる[104]。いずれの小委員会も共和党所属の委員長の下で活動しており、下院におけるサイバーセキュリティ対策の支配権は、中間選挙の結果共和党に渡ったといえる。

[104] http://homeland.house.gov/about/history-jurisdiction

5. 現在の課題及び今後の方向性

本章では、米国連邦政府のサイバーセキュリティ政策に関して、今後考えうる動きや課題について考察する。

(1) グローバルコモンズとしてのサイバーセキュリティ確保

今後考えられる議論の方向性として、サイバー空間を人類共通のリソースであるグローバルコモンズ（global commons）と見なし、国際的にサイバー空間における活動の自由を保証するための枠組みづくりが行われる可能性がある。これは、グローバライゼーションに伴い、例えば海上、空中、または宇宙空間における行動の自由や安全保障が各国の健全な経済活動に大きく影響してきており、国際的な管理体制が求められているように、サイバー空間にも同じような概念を適用しようという考え方に基づくものである[105]。

このような考え方を実現に移すための動きとして、国連傘下組織である国際電気通信連合（International Telecommunication Union、ITU）によって 2007 年に設立された Global Cybersecurity Agenda（GCA）というイニシアティブがある。GCA は、サイバー空間における情報の信頼性とセキュリティの向上に向けた国際協力体制構築のため、国際的な議論の場を提供することを目的としている。また、GCA においては、以下の 5 項目を重要事項として捉えているようである[106]。

- 国境を超えたサイバー犯罪に対処するための、法的な枠組みづくり
- 情報セキュリティに関する国際的な技術標準の画定
- サイバー犯罪が起きた場合、これに対処するための国際的な連携体制の構築
- サイバーセキュリティに関する国際的な教育・啓蒙活動の実施
- 国連他組織との連携体制の構築

米国は、ITU 加盟国であり、（当然ながら）以上の GCA の活動にも何らかの形で関与していると想定できる。

また、GCA との直接的な関連性はないものの、第 3 章で触れた Cyber Storm III においては、米国連邦政府以外にも 12 か国の政府が参加していたが、これはサイバーセキュリティ対策は 1 国では成し得ないものである、との認識を示したものと考えられる。このように、米国内外において、サイバー空間がグローバルコモンズであるとの認識が広がり、サイバー空間における信頼性・セキュリティ向上に向けた国際協力体制構築の動きが加速化することが考えられる。

---

[105] http://yalejournal.org/2010/07/security-challenges-in-the-21st-century-global-commons/
[106] https://www.unibw.de/.../ensuring-cyberpeace-in-a-new-world-order-2010
http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf

(2) キルスイッチを巡る議論

サイバーセキュリティ確保のため、行政機関にどの程度の権限を与えるべきかの議論で登場するのが、緊急時にインターネットの一部を遮断する権力を大統領に与える「キルスイッチ」条項である。例えば、第 4 章で触れた Cybersecurity and Internet Freedom Act（CIFA）の前身である Protecting Cyberspace as a National Asset Act が 2010 年に議会提出された際に、同法が大統領に対してキルスイッチ権限を与えているとして、多くのメディアで話題になった。しかし、同法は 2010 年 12 月に廃案となり、その後継として新たに提出された CIFA においては、「大統領を始め、米国連邦政府に勤める何者もインターネットを遮断する権限を持たない」という記述が加えられている[107]。CIFA とその前身を起草した Lieberman、Collins および Carper 議員は、キルスイッチに関する議論は根拠なきものである、と反論しているものの、CIFA には「サイバー非常時に、連邦政府は、（インターネット関連企業に対して）強制力のある命令を出すことができる」などという意味の記述があることから、CIFA に対して依然強い警戒感を示す論調も一部には見られる[108]。

また、2011 年 1 月以来発生しているアラブ世界での抗議活動において、抗議活動を抑圧する目的でエジプトなどにおいてインターネットが一時遮断された、という直近の経緯があったことからも、このキルスイッチを巡る議論は再び最活発化の動きをみせている。

このように、サイバー空間上における行動の自由と秩序の維持を両立させる上での課題は、デリケートな問題となることが多く、今後も検討課題として取り扱われる可能性が高い。

[107] http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=3623b3da-5056-8059-7644-0dcbd7558317
[108] http://www.washingtontimes.com/news/2011/mar/7/the-internet-kill-switch-rebooted/

【参考】 用語集

CC	コモンクライテリア（Common Criteria）
CIFA	Cybersecurity and Internet Freedom Act（法案）
CIA	中央情報局（Central Intelligence Agency）
CSC	サイバーセキュリティコーディネーター（Cybersecurity Coordinator）
DARPA	（国防総省）国防高等研究計画局（Defense Advanced Research Projects Agency）
DHS	国土安全保障省（Department of Homeland Security）
DOC	商務省（Department of Commerce）
DOD	国防総省（Department of Defence）
FIPS	連邦政府の情報処理に関する標準（Federal Information Processing Standard）
FISMA	連邦情報セキュリティマネジメント法（Federal Information Security Management Act of 2002）
GCA	（国際電気通信連合）Global Cybersecurity Agenda
HSARPA	（国土安全保障省）Homeland Security Advanced Research Projects Agency
ITU	国際電気通信連合（International Telecommunication Union）
NCCIC	（国土安全保障省）National Cybersecurity and Communications Integration Center
NCSC	（国土安全保障省）National Cyber Security Center
NCSD	（国土安全保障省）National Cyber Security Division
NICE	サイバーセキュリティに関する国家イニシアティブ（National Initiative for Cybersecurity Education）
NIPP	National Infrastructure Protection Plan
NIST	国立標準技術研究所(National Insititute of Standards and Technology)
NSA	国家安全保障局（National Security Agency）
OMB	行政管理予算局（Office of Management and Budget）
PP	保護プロファイル（Protection Profile）
US-CERT	United States Computer Emergency Readiness Team
USCC	US Cyber Challenge

本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。

なお、このレポートに対するご質問、ご意見、ご要望がありましたら、takashi_wada@jetro.go.jp までお願いします。