米国におけるサイバーセキュリティ政策の最近の動向（後編）

和田恭＠JETRO/IPA New York

1．はじめに

世界規模でサイバー攻撃が多発する中、米国では、政府機関やマスコミ、関係機関が標的になるケースが非常に多く、サイバーセキュリティ確保に向けた取り組みが加速してきた。オバマ大統領は政権発足後、サイバーセキュリティを重要な政権課題の一つと位置づけ、サイバー政策レビューやそれに基づくサイバーセキュリティ調整官ポストの創設や各種サイバー戦略の策定など、取り組みを強化してきた。

特に、近年の特徴として、サイバー攻撃が通常の IT システムから、ライフラインやネットワークを含めた広範囲の社会システムに及ぶようになってきたことがあげられる。一方で、ライフラインや金融など、国民生活の基盤となる重要インフラは、その運営事業者が主として民間事業者であることから、セキュリティ確保に向けては、官民の情報交換や連携体制をいかに確立するが重要な課題である。これに関しては、これまでも多数のサイバーセキュリティ法案が議会に提出されたものの、利害の対立などから立法化に至っておらず、現行法を前提とした取組みのみでは、関係機関間での円滑な情報交換を行う上で限界も生じていたことから、オバマ大統領が 2013 年 2 月の一般教書演説でも議会の協力を働きかけたところである。

本稿では、先月の前編に引き続き、重要インフラのサイバーセキュリティに関する取組みや、近年のサイバーセキュリティ関連法案の動向について報告する。

2．重要インフラ保護に向けた国土安全保障省の取組み

(1) これまでの取組み

「重要インフラ」とは、ライフラインや金融機関など、他に代替することが著しく困難な国民生活及び社会生活活動の基盤であり、その機能が停止、低下又は利用不可能な状態になった場合に、わが国の国民生活又は社会経済活動に多大な影響を及ぼしうるものである。これまで見たとおり、近年のサイバー攻撃は、特定の企業の IT システムだけではなく、工場やライフラインの維持管理システムをも対象とするようになってきている。一方、重要インフラに属する設備･工場を運営する事業者の IT システムは、ファクトリーオートメーション（FA）やプロセスオートメーション（PA）といった、生産活動に直接関連する部分は旧式の PC や IT システムをそのまま利用していることが多く、サイバー攻撃に対して脆弱な場合が多い。さらに、管理部門、一般的な情報システムは、インフラの制御システム＝独立システムであるためサイバー攻撃に対して安全と考えられる傾向にあったもの

の、実態的にオープン・クローズドによらずネットワークで接続されることが多くなっていることから、従来の考えは当てはまらなくなってきている。これに加え、前編でとりあげたとおり、重要インフラを狙ったサイバー攻撃も多くなってきたことから、重要インフラの防護が喫緊の課題となってきている。

米国においても、クリントン大統領時代の 1993 年にはすでに重要インフラ防護に関する大統領令 PDD63 が発出され、重要インフラに対する物理・サイバー攻撃に対する取組みが開始されている。同大統領令では、脅威・脆弱性に関する情報共有を行う Information Sharing and Analysis Center（ISAC）の設置が行われ、以降、段階的に国家的なインフラ防護計画策定などが行われてきたところである。最近策定された主な重要インフラ防護関連の計画を紹介する。

①国家インフラ防護計画（NIPP）（2006 年）

ブッシュ政権後、9/11 同時多発テロを踏まえて創設された国土安全保障省（DHS）には、重要インフラ保護に関する対策を総括する役割が与えられ、2003 年に発出された国土安全保障令（ブッシュ政権時に発出された大統領令）Homeland Security Presidential Directive （HSPD）7 号により、国家インフラ防御計画（National Infrastructure Protection Plan: NIPP）策定が指示された。2006 年に取りまとめられた NIPP では、17 の重要インフラ分野が指定され、分野ごとに官民パートナーシップで重要インフラの物理・サイバー防御を図るという分野別モデルが形成された。具体的には、それぞれの重要インフラ分野に対応する分野別担当政府機関（Sector Specific Agency: SSA）が指定され、民間事業者は Sector Coordinating Council （SSC）、政府側は Government Coordinating Council （GCC）を組織し、分野ごとの情報連絡・調整をおこなうものとされた。また、これらの分野毎の SSC、GCC を統括する組織として、重要インフラパートナーシップ諮問委員会（Critical Infrastructure Partnership Advisory Council : CIPAC）が設置されている。

一方で、これらの SCC、GCC は、民間分野に従前から設けられている ISAC（Information Sharing and Analysis Center）とは異なる。ISAC は、クリントン大統領時代の 1998 年に大統領令（EO）127472 号及び重要インフラ防護に関する大統領指令（PDD）63 により設けられた、サイバー脅威・脆弱性に関する情報共有を行うセンターである。現在、ISAC は、16 分野についておかれており[1]、オペレーション上の情報、具体的にはサイバー脅威情報や脆弱性情報の収集、分析、普及に当たっている。

[1] National Council of ISACs （NCI）のホームページ上に掲載されている 15 機関と、2012 年 10 月の CSSP で登場した ICS-ISAC の計 16 機関とした。Chemical ISAC も活動を継続しているようであり、正式な ISAC 数は 17 以上と思われる。
これとは別に、州レベル以下でサイバーに限定されない情報集約機関として ISAC が置かれている例がある。

②国家サイバーインシデント対応計画（NCIRP）（2010 年 9 月）

米国の災害に対する対応を取りまとめた災害対策基本計画（National Response Framework: NRF）[2]のサイバー攻撃対応特別版として、国土安全保障省（DHS）は、サイバー攻撃に対する計画（NCIRP）の暫定版を 2010 年 9 月に策定している。NCIRP は、サイバーセキュリティに関する情報を集約するための全米サイバーセキュリティ・通信統合センター（NCCIC）と情報共有体制の構築、それに用いられるサイバー攻撃の影響度評価尺度（National Cyber Risk Alert Level（NCRAL）の導入、関係機関の分担の明確化（Cyber Unified Coordination Group（Cyber UCG）の設置）を盛り込んだものとなっている。

NRF 自体は、自然災害・テロなどに対する Prevention、Protection、Response、Recovery の 4 段階にわたる対応を規定した計画であるが、NCRIP はそのうちサイバー攻撃への Response に重点を置いているのが特徴である。ただし、NCRIP で規定されている NCCIC や Cyber UCG は、これに関わらず、この全 4 段階にわたり活動することが想定されている。

【図表１：NCIRP と NIPP、NRF との関係】

出典：DHS 発表資料から

[2]全米国土安全保障戦略（National Strategy for Homeland Security）の一環として、2008 年 3 月に策定された。

(2) 重要インフラ保護に関する大統領令（2013 年 2 月）

2013 年 2 月 12 日、オバマ大統領は、サイバーセキュリティ強化のための立法が進まず、議会がここ数年機能不全に陥っていることを踏まえ、一般教書演説において「サイバー対策の議会による迅速な法制化」を求めた。また同日、重要インフラのサイバーセキュリティ強化に向けた大統領令（Executive Order ：EO） 13636 号と大統領指令（Presidential Decision Directive ：PPD）21 号[3]を発出し、重要インフラ保護強化に向けて、官民でのサイバーセキュリティ関係の情報共有体制構築に向けた課題の洗い出し、必要な法制度の検討、技術的なソリューション（Cybersecurity Framework）の策定等にむけた作業期限を設定、DHS、DOD や NIST に作業を指示した。

上記 2 大統領令で規定された具体的な作業項目、分担省庁などは以下のとおりである。

【図表 2：大統領令 13636 号の主要項目】

項目	関係機関	求められる対応
サイバーセキュリティに関する情報共有	DHS、DOJ、IC	非機密情報を適切なタイミングでおこなうためのマニュアル作成。
		重要インフラ運営事業者間で機密情報を共有・管理するための手続き確立。
	DHS、DOD	連邦政府と重要インフラ事業者間でサイバー脅威に関する機密情報を共有するための（Enhanced Cybersecurity Services Program：ECS）の対象範囲拡大。
	DHS	重要インフラ事業者のセキュリティ担当者に対するクリアランスプロセス促進。
		サイバーリスクを低減するため重要インフラ事業者への情報提供内容、情報構造、種類について助言を行う臨時職員の登用拡大。
プライバシーと市民権保護	全関係省庁	連邦取引委員会（FTC）のオンライン上での「公正な情報取り扱い規則」に基づいて、プライバシーと市民権の保護を行う。
利害関係者との調整	DHS	重要インフラのサイバーセキュリティに関しステークホルダー（利害関係者）との協議体制を確立する。
サーバーセキュリティフレームワーク	NIST	重要インフラのサイバーリスクを低減するためのフレームワークを 1 年以内に策定する。フレームワークは、政策、ビジネス実態及び技術に基づきサイバーリスクに対応するための基準、方法論及び手続きからなるものである。 ● 自主基準やベストプラクティスを盛り込むこと ● 産業分野横断的な基準やガイドラインの特定 ● 参加する産業分野と基準策定機関間の将来的な協力可能分野の特定 ● フレームワークを実施する組織のパフォーマンスを測るためのガイダンスを盛り込むこと

[3] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0
http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

		● 営業機密と個人のプライバシー保護に対する影響を緩和するための方法論の特定
自主的な重要インフラサイバーセキュリティプログラム	DHS、SSAs	(おおよそ 6 ヶ月以内に)フレームワーク導入に向け、以下の自主的なプログラムの策定。 ● セクター特定のリスクに対応するための実施ガイダンス又は補足資料の作成 ● 民間分野の参加状況について大統領への年次報告 ● 参加を促すためのインセンティブの分野間での調整 ● セキュリティ基準の導入することの実現可能性、セキュリティ上の効果ほか利益を理解させる
最大のリスクの特定	DHS、SSAs	リスクベースのアプローチによりサイバー攻撃が米国の公衆衛生、経済又は国家安全保障に対するインパクトが最大となる重要インフラを特定するために、リスクベースのアプローチを 7 ヶ月以内に採用する。

【図表 3:大統領令 13636 号に基づく各省庁の作業項目】

項目名及び関係省庁	始期	期間	終期
非機密情報を適切なタイミングでおこなうためのマニュアル作成(DOJ、DHS、DNI)	2013 年 2 月	120 日	2013 年 6 月
重要インフラ分野での情報共有体制の確立(DHS、DOD 協力)	2013 年 2 月	120 日	2013 年 6 月
サイバーセキュリティフレームワークの第一次版作成(NIST)	2013 年 2 月	240 日	2013 年 10 月
サイバーセキュリティフレームワークの最終版作成(NIST)	2013 年 2 月	1 年	2014 年 2 月
プログラムに参加するためのインセンティブ確保に向けた提言(DHS、Treasury、DOC)	2013 年 2 月	120 日	2013 年 6 月
調達及び契約役務にセキュリティ基準を盛り込むことについて、DHS、FARC と協力して大統領への提言を策定する(DOD、GSA)	2013 年 2 月	120 日	2013 年 6 月
重要インフラの特定(DHS)	2013 年 2 月	150 日	2013 年 7 月
サイバーリスクに適切に対応するため、サイバーフレームワークに基づく要求事項を課すために必要な権限を持っているか、大統領へ報告(各省庁)	2013 年 10 月	90 日	2014 年 1 月
規制が不十分とみなされる場合、サイバーリスクを低減するために必要な取組み(各省庁)	2014 年 2 月	90 日	2014 年 5 月
重要インフラの中で特に非効率、矛盾、負担の大きいサイバーセキュリティに関する規制が課せられているものについて、行政管理予算局(OMB)へ報告	2014 年 2 月	2 年間	2016 年 2 月

【図表 4:大統領決定 21 号の主要項目】

項目	関係機関	求められる対応
重要インフラのセキュリティと柔軟性の強化	DHS	重要インフラに関する 2 つのオペレーションセンターを運用する。
	DHS ほか	DHS 内部及び関係省庁間にわたり、重要インフラのセキュリティ機能と柔軟性機能との関係について、120 日以内に取りまとめる。
情報交換の実施	全省庁	データや情報フォーマット、アクセシビリティ、システム相互運用性、冗長性及び代替機能に関する要求事項の特定。
	DHS、SSA ほか	連邦政府機関が効率的な情報交換を行うための、ベースラインデータとシステム要求を 180 日以内に特定する。
重要インフラに関する情報集約と分析機能の導入	IC、DOD、DOJ、DHS ほか	脆弱性と影響情報に関する隔離、評価、統合により、脅威・危険情報の情報集約と分析を行う機能を導入する。 重要インフラの優先付けとリスク管理を支援する。 独立・連鎖反応を想定し、重要インフラにサイバー事象が発生する事前、途中、事後の各段階におけるセキュリティと柔軟性を確保するための提言の策定。 重要インフラにおけるサイバー事象のマネジメント及び復旧作業を支援する。
既存の官民パートナーシップモデルの評価	DHS、SSA ほか	既存の官民パートナーシップを評価し、150 日以内に連携改善に向けた提言を取りまとめる。
状況把握能力	DHS	重要インフラに関する状況把握能力向上策を 240 日以内に策定する。
国家インフラ防護計画(NIPP)	DHS	現行の国家インフラ防護計画(NIPP)を 240 日以内に改定する。
重要インフラのセキュリティと柔軟性に関する研究開発	DHS、OSTP、SSA、DOC ほか SSAs	重要インフラのセキュリティと柔軟性に関する研究開発について、国家計画を 2 年以内に策定する。
		連邦政府の研究開発方針と合致させるために、重要インフラのセキュリティと柔軟性のために行っている研究開発へのインプットを提供する。

上記の大統領令に基づき様々な作業が今後並行的に進められていることとなるが、特に注目されるのが、国立標準技術研究所(NIST)が担当するサイバー関連情報を関係者で共有し、重要な情報をフィードバックすることを目的とした官民での情報連携制度 Cybersecurity Framework の創設である。Cybersecurity Framework は、現行法令を前提として、重要インフラに対する攻撃が行われた場合の事案の情報、それに基づく分

析、関係者へのフィードバックを円滑に進めるための、ベストプラクティスやガイドライン類の集合体となることが想定されており、実際の運用は国土安全保障省（DHS）が担当することとなる。NIST は、Cybersecurity Framework を策定するため、2 月 25 日に Request for Comment（RFC）[4]を発出し一般からの意見聴取を開始するとともに、関係機関及びその他民間からの意見聴取のため、ワークショップを複数回開催することとしている。第 1 回目は 2013 年 4 月 3 日（ワシントン DC）、第 2 回目は 5 月 29-31 日（ピッツバーグ）開催予定である。第 1 回ワークショップでは、政府サイバーセキュリティ調整官の Michael Daniel 氏のほか、国土安全保障省・商務省両次官、IT、Water、National Health、Electricity、Communication 分野の情報分析センター（ISAC）、関連業界団体などが出席し、同 Framework の必要性が強調されたほか、同 Framework 策定に当たっては、多様なサイバー攻撃や分野別の特性を踏まえた柔軟性をもったものとすべきことなどが述べられた。今後、さらに 1 回のワークショップの後、NIST は 10 月に同 Framework 暫定版を取りまとめる予定としている。

ただし、同 Framework は現行法制下で実施されることから（つまりこれまでの権利義務関係を変更しないことから）、過去の官民情報連携制度（CIPAC、ISAC、IC－CERT）で情報連携が進まなかった根本的な原因を解決するものではなく、民間事業者側から任意の情報提供を促すための税額控除制度や経済的なインセンティブなどが予定されているものの、そもそも想定された情報連携を行うにたる法的権限が各省に与えられているか、与えられていたとして、従来の課題が解決されるかといった点が問題となる可能性がある。これについては、現行の官民情報連携体制下での課題抽出など、オバマ大統領が 2013 年の一般教書演説で議会に要請したサイバーセキュリティ立法を念頭に置いた作業項目も大統領令の中に含まれており、今回の一連の作業は、政権が求めているサイバーセキュリティ新立法への地ならしを行う位置づけにあるとも言える[5]。

今後、大統領令 EO13636 号と PDD21 号に基づき、重要インフラに関する情報共有に向けた各種課題（法改正事項を含む）の抽出や、サイバーセキュリティ情報共有のための枠組み（Cybersecurity Framework）の構築が国立標準技術研究所（NIST）を中心に進められることとなる。

(3) 国土安全保障省（DHS）内の体制

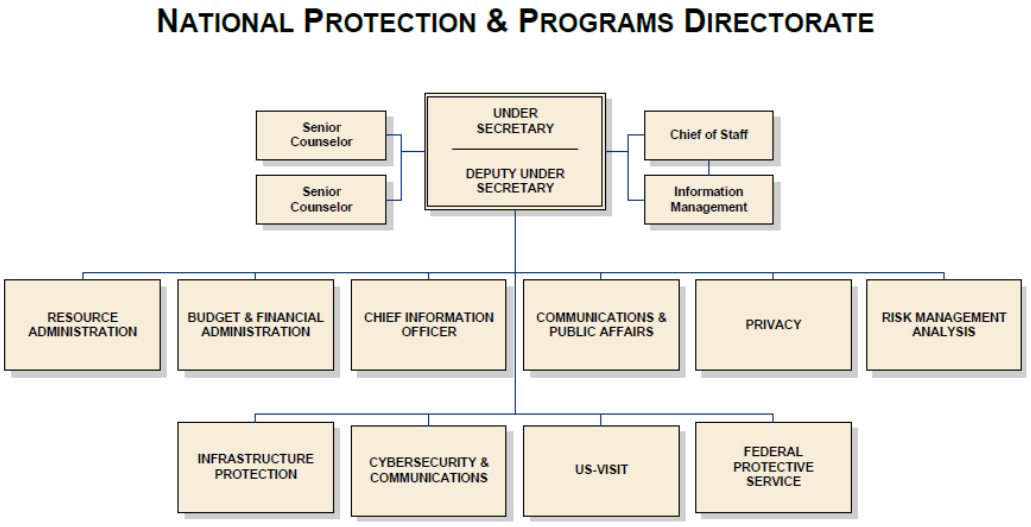
DHS においてサイバーセキュリティに関連する部門は、重要インフラや IT システムのサイバーセキュリティを担当する National Protection and Programs Directorate（NPPD）と、サイバー関係 R&D を担当する、Science& Technology Directorate の 2 つである。

[4] http://www.nist.gov/itl/csd/upload/fr_noticerfi_framework_cybersecurity_2-26-13.pdf
[5] NIST サイバーセキュリティフレームワーク策定責任者 Adam Sedgewick 氏へのインタビューより。

NPPD でサイバー・通信インフラのセキュリティや柔軟性の確保に中心的な役割を果たす部署として、Office of Cybersecurity & Communication（CS&C）が 2006 年に発足した。CS&C 内には、現在、The Office of Emergency Communications（OEC）、The National Cybersecurity and Communications Integration Center（NCCIC）（後述）、Stakeholder Engagement and Cyber Infrastructure Resilience（SECIR）、Federal Network Resilience、Network Security Deployment の 5 部門が置かれている[6]。

NPPD には、CS&C のほか、重要インフラのうち DHS 所管とされている重要インフラ 11 分野[7]のうち、化学産業、商業施設、重要な製造業、ダム、緊急サービス、原子力施設を所管する部局として Office of Infrastructure Protection（OIP）が置かれている。サイバー以外の重要インフラに関する脅威情報を集約する機関である National Infrastructure Coordinating Center（NICC）も、OIP 内におかれている。

【図表 5 国土安全保障省 NPPD の組織図[8]】

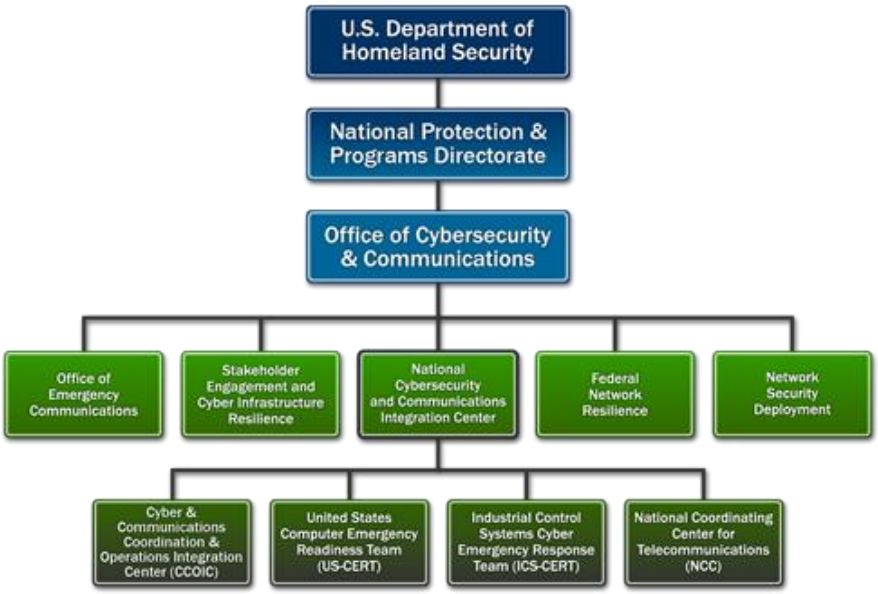


[6] ニューヨークだより 2011 年 3 月号で取り上げている NCSD、NCSC は廃止されているので注意のこと。
[7] DHS 所管の重要インフラ分野は、化学産業、商業施設、重要な製造業、ダム、緊急サービス、原子力施設（以上 OIP/NPPD/DHS 担当）、政府機能（ICS・FPS /DHS 担当）、通信、IT（以上 CS&C/NPPD/DHS 担当）、郵便、交通・物流（以上 TSA/DHS 担当）である。
[8] http://www.dhs.gov/xlibrary/assets/org-chart-nppd.pdf

①NCCIC（National Cybersecurity and Communication Integration Center）

NPPD 傘下の CS&C のうち、特に重要インフラを中心としたサイバー情報の集約機関として重要な役割を果たすのが NCCIC である。NCCIC は、国家サイバー事故対応計画（NCIRP）に基づき、それまでの National Cyber Security Center（NCSC）を置き換える形で発足した機関であり、US-CERT（米国内のサイバー脅威情報の集約や警戒情報や注意喚起情報の発信を行う実働部隊）や、ICS-CERT（制御システムに関するサイバーセキュリティを担う）などを統括している。NCCIC には、この United States Computer Emergency Readiness Team（US-CERT）、Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）のほか、24 時間体制でサイバー空間の監視をおこなう Cyber & Communications Coordination & Operations Integration Center（C3OIC）、DHS 所管の重要インフラ中、IT 分野の政府側調整機関である National Coordinating Center for Telecommunications（NCC）の4部門が存在する。

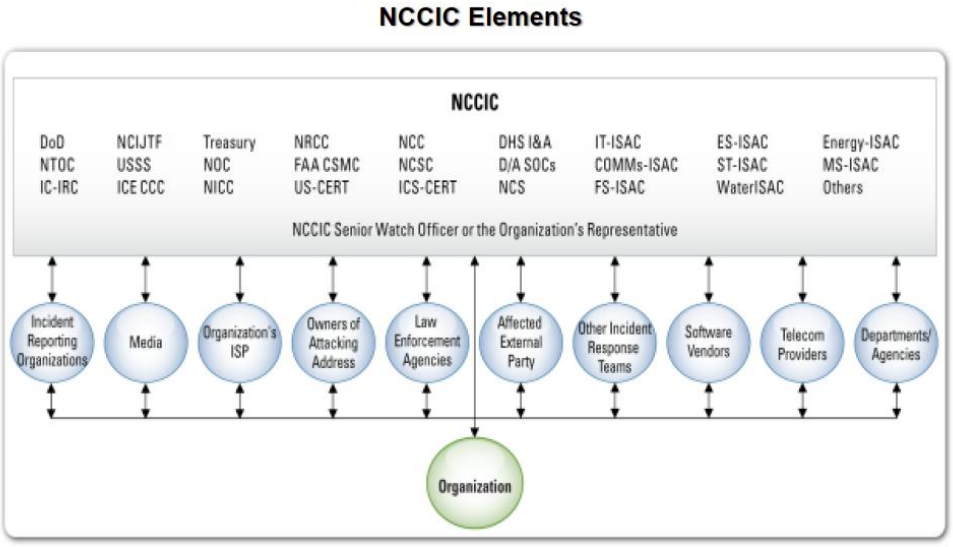
【図表 6：NCCIC の組織構成[9]】



C3OIC では、NCCIC 傘下の US-CERT、ICS-CERT のほか、各種 ISACs、安全保障情報（NOC）、防衛・軍事情報（サイバー司令部、NTOC）、インテリジェンス（IC-IRC）、法執行部門（FBI、NCI-JEF、シークレットサービス USSS）などを通じた情報交換をおこなっている。

[9] http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

【図表 7：C3OIC（NCCIC）における情報共有体制[10]】



上図で Organization's Representative とあるのは、C3OIC 内のオペレーションルーム内に職員を派遣して、情報共有している US-CERT、ICS-CERT、ISAC、地方政府機関などを指す。また、集約される情報はサイバーセキュリティ情報だけではなく、場合によりインテリジェンス、法執行（司法）、国防情報なども含まれる。

【図表 8：C3OIC（NCCIC）のオペレーションルームの風景[11]】

[10] http://northalabama.issa.org/sites/default/files/Scurlock%20%28for%20ISSA%20website%29.pdf 13 ページ。

[11] http://ics-cert.us-cert.gov/icsjwg/downloads/final-slicksheet-ncicc-v2-012411.pdf

②US-CERT

US-CERT（United States Computer Emergency Readiness Team）は、国家のサイバーセキュリティに対する能力を高め、集約されるサイバー関係情報の調整や、サイバーリスク管理に貢献するための組織である。その具体的な活動としては、US-CERT は、サイバーセキュリティ関連情報を共有するためのメーリングリストやフィードを提供するポータル「国家サイバー状況把握システム（National Cyber Awareness System（NCAS））」を通じたサイバー脅威情報の共有と、脆弱性データベース（VND）の運営をおこなっている。また、インフラ運営者、連邦政府機関、研究機関、ISAC と連携して、マルウェア分析、被害復旧支援、司法捜査支援業務をおこなっている。2011 年単独で、10 万件のサイバーインシデント情報が報告され、US-CERT から 5,000 件のサイバーセキュリティ警告と情報提供をおこなっている。

US-CERT に対するサイバーインシデント情報は、CS-CERT インシデント報告システムに基づいておこなわれ、そこに含まれる情報は通報者、報告機関の種別、インシデントによる被害規模、対象インフラ種類、インシデント解決策、救援要請の有無、インシデント発生時間、詳細、データ暗号化の有無などである。この情報提供は任意でおこなわれている。このために用いられる自動情報収集システムは Einstein プログラムと呼ばれ、関係省庁の拡大、機能強化が順次行われており、現在、Einstein3 が導入テスト中である。

また、インシデント情報とは別に、US-CERT は脆弱性情報も収集しており、この情報は VND を管理している Carnegie Mellon 大学 Software Engineering Institute（SEI）内におかれた民間部門対象の情報集約組織 CERT/CC に送られる。なお、US-CERT 職員のかなりの割合が CERT/CC からの出向者とされている。

そのほか、US-CERT は、フィッシングサイトに関する情報も収集しているが、これは該当サイトの URL をメールアドレス phishing-report@us-cert.gov に送るという非常にシンプルなものである。

③ICS-CERT

ICS-CERT（The Industrial Control Systems Cyber Emergency Response Team）は、重要インフラを対象としたサイバーセキュリティ情報の集約、分析を行う機関であり、US-CERT と同様、法執行機関やインテリジェンスコミュニティと連携して活動を行っている。

3. サイバーセキュリティ情報に関する官民連携強化に向けた取組み

(1) 米国の全体像

これまで、米国ではサイバーセキュリティに関して、さまざまな情報共有を官民で図る試みがなされてきた。また、その情報集約機関としては、サイバー攻撃の内容を分析し、防御プログラムを提供する ISAC、セクター別にサイバー情報（サイバー事象、政策動向、技術動向など）を共有するための SCC、GCC、サイバー攻撃の情報を集約し国際的な協力体制を構築している US-CERT など、さまざまな組織が存在する。米国におけるサイバー情報の官民連携制度の全体像は明らかになっていないが、筆者が把握している範囲で以下のとおりである。

【図表 9：サイバーセキュリティ関連の情報共有のための官民連携制度】

分野	連携組織	統括組織	参加機関（政府）	参加機関（民間）
全般 政策枠組	包括的国家サイバーセキュリティイニシアティブ（CNCI）、FISMA、GSA procurement rules、NIST SP-800、FIPS			
情報連携体制	GFIRST	US-CERT/DHS	CIRCs	
	NCCIC	CS&C/DHS	US-CERT, ICS-CERT, NICC, NCC-Telecom, DOD, 地方政府	CIRCs（JC3-CIRC など）、各種 ISACs
	NOC	OIP/DHS	Intelligence Watch and Warning, NRCC, NICC	
重要インフラ 政策枠組	国家インフラ防護計画（NIPP）、国家サイバー事故対応計画（NCRIP）			
情報連携体制	（政策レベル） セクター別パートナーシップモデル	CIPAC	GCC	PCIS 、 16 SCCs (CSCC, ESCC,)
	CyberUCG	CS&C/DHS	NCCIC members	CI/KR 事業者, NGOs
	Cybersecurity Framework	DHS	連邦政府関係機関	CI/KR 事業者
	（運用レベル） ISAC	National Council of ISACs	Communication ISAC, Multi State ISAC	16 ISACs (IT-ISAC, ES-ISAC, etc.)
	InfraGard	FBI Cyber Div.	FBI	電磁気、農業、化学等分野別 InfraGard

用語
FIPS: Federal Information Processing Standardization ITシステムに関する連邦政府標準規格
US-CERT: United States Computer Emergency Response Team
NCCIC: National Cybersecurity and Communication Integration Center
NICC: National Infrastructure Coordinating Center
NOC: National Operations Center
NRCC: National Response and Coordination Center
CI/KR: Critical Infrastructure/Key Resource
CIRC: Computer Incident Response Capability
CIRT: Computer Incident Response Team
GCC: Government Coordinating Council
SCC: Sector Coordinating Council
ISAC: Information Sharing and Analysis Center

ただし、これらとは別に、司法（法執行）やインテリジェンス、国防といった別の法目的による情報収集体制も別途存在し、情報集約組織はそれぞれ別個に、あるいは重複して情報集約を行っていることから、組織や法目的間の連携の必要性も以前から指摘されている。

以下、サイバーセキュリティの情報共有に向けた主要な枠組みについて説明する。

(2) 情報共有に向けた枠組み・統括組織

① GFIRST

政府機関の各分野に設けられた緊急時対応組織 CIRC、緊急時対応チーム CIRT 間の情報連携組織として、GFIRST（Government Forum of Incident Response and Security Team）が US-CERT 内に設けられ、年次会合も開かれている。GFIRST ポータルサイトでは、最新のサイバー脅威情報、脆弱性情報（ベンダー製品ごとに提供）などが提供されている。

② NCCIC（National Cybersecurity and Communication Integration Center）

NCCIC は、US-CERT、 ICS-CERT、地方政府、ISAC などからのサイバー情報を集約するため、NPPD 傘下に設置された機関である。詳細は前章参照のこと。

③ Network Operations Center（NOC）

DHS では 20 以上の部門にわたる機関が状況把握（Common Operating Pictures（COPS））を共有することが大きな課題となっている。その一つの解決方法が National Operations Center（NOC）の設置である。NOC は、以前から設置されてい

た Homeland Security Operation Center を再編する形で 2006 年に設置され、Intelligence Watch and Warning、 国家防災対応センター（National Response Coordination Center ：NRCC）、国家インフラ調整センター（National Infrastructure Coordination Center: NICC）の 3 実働部隊と監視、企画部門の合計 5 部門からなる組織とされた。NOC 自体は OIP の the Office of Operations Coordination and Planning（OPS）の傘下にあるが、情報共有 3 組織は DHS 内で複数部にまたがっており、Intelligence Watch and Warning は Office of Intelligence and Analysis（I&A）、NRCC は FEMA、NICC は NPPD が所管している[12]。

NICC は 2004 年に設置され、重要インフラ（CI/KR）の運営状況を 24 時間体制で監視している。重要インフラ分野の SCC、GCC（Government Coordinating Council）、ISAC や、担当省庁 SSA（Sector Specific Agency）とも連絡調整を行っている。NICC は、重要インフラのオペレーション状況を監視するユニット Watch and Warning のほか、DHS 幹部に状況をブリーフィングするユニット Executive briefing team（EBT）があり、2013 年 2 月には上記 2 ユニットを支援できる民間ベンダーを募集している[13]。

④ セクターパートナーシップモデル（分野別連携モデル）

国家インフラ防護計画（NIPP）によって提言された重要インフラ防護における分野別の官民連携体制をセクターパートナーシップモデル（分野別連携モデル）と呼び、その統括組織が重要インフラパートナーシップ諮問委員会 CIPAC（Critical Infrastructure Partnership Advisory Council）である。これは、重要インフラの分野ごと（金融、電力、IT、通信など）に政府側機関、民間機関が多数存在する中、政府側と民間側に情報集約・調整のための協議体を置き、集約化を図るものである。政府側に設置される協議体を GCC（Government Sector Coordinating Council）、民間側に設置される協議体と SCC（Sector Coordinating Council ）[14]と呼ぶ。また、政府との連携・情報共有を目的とした CIRC（Computer Incident Response Capability）/CIRT（Computer Incident Response Team）により、分野ごとの情報が交換される。例えば DOE が運営するエネルギーセクターの JC3-CIRC[15]などが該当する。CIPAC は GCC/SCC 間のコンセンサス形成をおこなう。

---

[12] http://itlaw.wikia.com/wiki/National_Operations_Center
[13] http://www.gsnmagazine.com/article/28446/dhs_wants_hear_prospective_vendors_can_support_its
[14] なお、政府機関内でも縦割りの Government Coordinating Council が複数存在する。
[15] http://www.doecirc.energy.gov/aboutus.html
DOE 傘下の行政機関・研究機関については、コンピューター関連のインシデント情報を同プログラムに対して報告することが義務付けられている。報告までの時間はセキュリティ上の重要性に応じ、1時間から 1 週間以内まで。

GCC や SCC 内で共有される情報は、2002 年重要インフラ情報法（CII Act、国家安全保障法の一部）に基づいて、連邦政府諮問委員会法（Federal Advisory Committee Act）における免責条項が適用され、一般向けの情報公開請求に基づく開示が免除される。この手続きは、重要インフラ情報保護プログラム（Protected Critical Infrastructure Information（PCII）Program）と呼ばれる。PCII の取り扱いを求める事業者は、電子メール、物理媒体、電子媒体（暗号化の有無を問わず）の形態の情報を直接又は PCII Management System（PCIIMS）を通じて担当部局に提出することができる。ただし、PCII に基づき政府や他機関と情報を共有することが民間損害賠償の対象外となるかが不明確であることや、情報公開請求に対する保護手続きが明確でないことにより、本パートナーシップモデルにおいては、情報連携が必ずしも円滑に行われていないとの指摘も見られる。

また、分野横断的な連絡調整機関もおかれている。国家インフラ防護計画（NIPP）による分野別連携モデルのうち、民間サイドの SCC 間のコーディネーションを行う組織は、重要インフラ保護パートナーシップ PCIS（Partnership for Critical Infrastructure Security）である。

⑤ Cyber UCG（User Coordination Group）

Cyber UCG は、NCIRP により設置された政府機関の重大インシデント対応をサポートするための各政府機関の代表者及びサイバー専門家からなるグループ組織である。サイバー専門家からなる NCCIC に対し、NCCIC の所属機関の上級職も参加していることが特徴となっている。

DHS が全体を統括し、非常時のみだけではなく平常時の連携体制強化に向けた情報交換も行っている。NCCIC からのオペレーション情報のほか、国際機関、NGO からの情報なども集約する。ブッシュ政権時代に 13 の連邦政府機関からなる National Cyber Response Coordination Group（NCRCG）が設置されていたが、これを置き換える形で設置された。

⑥ Cybersecurity Framework に基づく情報連携

2013 年 2 月に発出された大統領令に基づき、現在国家標準技術研究所（NIST）が策定中の重要インフラに関するサイバー情報交換枠組みである（上述）。昨年来、国防総省と国土安全保障省が、重要インフラの一分野である防衛産業基盤（DIB）を対象として行ってきた任意の情報連携制度 Enhanced Cybersecurity Program（ECS）を拡張したものとなると見込まれる。制度運営は国土安全保障省（DHS）が担当する。

⑦ 情報共有分析センター ISAC（Information Sharing and Analysis Center）

ISAC は、重要インフラ分野に対する物理・サイバー攻撃に対する脅威・脆弱性に関する情報共有を行うセンターであり、もともと 1998 年制定の PDD63（Presidential Decision Directive、重要インフラ防護に関する大統領令）に基づき設立された。金融、エネルギー等セクターごと 17 分野に ISAC がおかれており、一部分野の ISAC（IT-ISAC）は DHS が運営している。

ISAC に対する情報は、政府内（US-CERT の National Cyber Alert System）、民間（NICC ＝ISAC と各工業界メンバーからなる調整機関）から提供される。また、CERT/CC からは特定業界の連絡先（Point of Contact）あて直接情報提供される場合もあるとのことである。ISAC を通じて流通しているサイバー情報の例としては、ハッカーの攻撃メトリクス情報、TCP/UDP 等のネットワーク統計情報、アラート（e-mail 含む）が上げられる。これらは、ウェブサイト・電子メール等の手段によりメンバー内で共有されるとのことである。

＜HSIN（Homeland Security Information Network）＞
HSIN は、連邦政府、州政府及び自治体、重要インフラ事業者、国際機関との間で、非公開であるが機密とは明確に分類されていない情報（Sensitive but Unclassified Information :SBU）を交換するために構築されたウェブベースのプラットフォームである。もともとは国内の様々な脅威に対する防護・対応・復旧活動等の支援を行うための情報ネットワークを統合するためのセキュアなプラットフォームとして開発されたとのこと。DHS が運用しており、制御システムに関するワーキンググループ ICSJWG における情報交換にも利用されている（HSIN-CS ICSJWG と呼ばれている。）

⑧ InfraGard[16]

InfraGuard は、サイバー空間におけるインシデント対処能力向上のために情報共有、調査及びサイバー犯罪の起訴手続き等に関して、FBI、IT 企業、大学等で 1996 年に開始された官民パートナーシッププログラムである。関連情報は暗号化されて National Infrastructure Protection Center （NIPC）に送られ、FBI と関係機関・者で共有される。2001 年に物理犯罪に関する情報もスキームに追加されて以降、参加機関は拡大しており、現在、54,000 の関係機関・者（参加者は対外秘）、FBI の 56 事務所が参加している。なお、NIPC は 2003 年に DHS に移管されており、現在の InfraGuard の活動は、重要インフラ保護に関するものは DHS が、犯罪捜査に関する

[16] http://www.infragard.net/about.php?mn=1&sm=1-0

ものは FBI が中心となっているようである。個々の構成員等は非公開であり、活動内容は一定のガイドラインにしたがったもののみ公開可能とのことである。

(3) 州・地方自治体との情報共有

国土安全保障省（DHS）は、2010 年 8 月に発表された大統領令 13549 に基づき、州や自治体、民間企業（State、Local、Tribal、Private sector: SLTPS partners）、コントラクタ、連邦政府との間で、脅威に関する機密情報を共有する際のセキュリティ基準について、2012 年 3 月 9 日、新しいガイダンスを発表した[17]。Classified National Security Information Program for State、Local、Tribal and Private Sector Entities Implementing Directive[18]は、DOS、CIA、FBI、ODNI、DOD、DOJ の協力により運営される。

(4) 司法（法執行）、インテリジェンスなどの観点からの情報連携

上記に掲げた情報連携体制は、サイバーセキュリティに関するものであるが、サイバーセキュリティ以外に連邦政府内で機密情報あるいは（非機密）機微情報に関する情報連携が行われてきた分野として、国防、司法（法執行）、インテリジェンス、外交などがあげられる。これらは、その目的や参加機関、情報連携組織もそれぞれ異なっており、一般的にはそれぞれの情報連携体制間で情報のやり取りは行われない。

一方で、例えば US-CERT が扱う情報をみても、その背後に特定国の支援があるサイバー犯罪、安全保障上の問題がある事案、犯罪の一環としてのサイバー利用などの事例があり得ることからも分かるように、重要インフラに関するサイバー関連情報を官民で連携して共有していく体制を構築しても、そこで取り扱われる情報は「サイバー」として切り分けられるものではない。したがって、サイバー情報に関する官民連携体制の構築にあたっては、法目的を異にするこれらの分野における情報連携体制との整合・協力が長期的な課題となろう。ここでは、その代表的なものとして、法執行とインテリジェンス情報の情報連携体制について紹介する。

① 法執行情報

規制の遵守状況調査や刑事上の捜査活動など、法執行に関する情報は、民事に関する情報とは隔離されて取り扱われている。また、連邦捜査局（FBI）では、犯罪捜査の観点から重要インフラに関する脅威情報の収集を行っているが、サイバー攻撃に関する情報でみた場合、軍事活動に関連するものか、安全保障に関連するものかといった

[17] http://fcw.com/articles/2012/03/12/dhs-information-sharing-state-local.aspx
[18] http://www.dhs.gov/xlibrary/assets/mgmt/mgmt-classified-national-security-program-implementation-directive.pdf

背景まで明らかになることは極めて少ないことから、FBI のインフラガードを通じて得られる情報と、DHS 内で収集される重要インフラに関するサイバー情報が共有されることはあまりないようである。

② インテリジェンス情報

国家の安全保障の目的で情報収集を行う機能がインテリジェンスである。米国内では、中央情報局（CIA）、国家安全保障局（NSA）、国防情報局（DIA）などがその情報収集の任務に当たっているが（US－CERT のように国防、法執行、インテリジェンスの分野にわたる情報の収集・分析を行っている組織も存在する。）、関係機関間で集約した情報を調整するための連携組織として、Intelligent Community （IC）がおかれている。インテリジェンス情報の共有体制としては、上記各機関を通じた情報が、その重要性に応じて、Joint Worldwide Intelligence Communications System （JWICS）（最重要機密情報）、Secret Internet Protocol Routed Network （SIPRNET）（機密情報）、Open Source Information System（OSIS）（非機密情報）という異なる 3 つのネットワーク経由で集約されている[19]。

＜IC（Intelligent Community）＞
IC は、Intelligence Reform and Terrorism Prevention Act （IRTPA） of 2004 により、16 の政府機関が参加する安全保障情報の意思決定組織として大統領府に置かれている。情報共有や外交まで含めた情報の収集、分析を行い、その統括機関は ODNI（Office of Director of National Intelligence）である。ODNI は、各省庁の情報機関の予算を一括計上、執行している。

2001 年の同時多発テロを防げなかったことの反省から、国際的なテロ・犯罪組織への対応能力を強化すべく、2001 年の米国愛国者法により、法執行機関の情報収集権限強化、外国人に対する情報収集制限の緩和などが行われている[20]。これにより、法執行情報とインテリジェンス情報は、かなりの部分共有が進みつつあるものと考えられる。

また、並行的に、政府機関間で機密又は機微情報の交換を円滑化する取組みも進められており、その代表例として ISE があげられる。

＜Federal Information Sharing Environment（ISE）＞
2001 年の同時多発テロ以降、縦割りの情報管理体制に対する反省から、国防、法執行、インテリジェンス、外交などの様々なコミュニティ関係省庁間で機密（又は機微）情報の共有を行うためのフレームワークとして、Federal Information Sharing Environment（ISE）が 2006 年に構築されている。ISE は、もともとは Intelligence Reform and Terrorism

[19] http://www.dtic.mil/ndia/2003interop/Lunch.pdf
[20] http://www.fas.org/sgp/crs/intel/RL33873.pdf

Prevention Act of 2004 に基づき、テロ対応能力強化のため設けられた制度であり、国家安全保障上重要な情報（疑わしい活動情報（Suspicious Activity Reporting: SAR）などの安全保障関連、インテリジェンス、外交、防衛関連情報など）を政府、地方政府、関係企業間で共有するメカニズムである[21]政府機関の見直しと合わせて構築が求められていたものである。

インテリジェンス情報を国家安全保障（テロ対策）にも活用するとの観点から、大統領府におかれた国家インテリジェンス長官（Director of National Intelligence）を中心としてISE の検討が進められてきたが、安全保障情報を取り扱う観点から、ISE の事務局である Project Manager of ISE（PM-ISE）は国土安全保障省内におかれている。ただし、ISE は、メタデータ構造、ボキャブラリ・API 整備などにより関係機関間での情報共有に向けた環境整備を行うものであり、現状では、法執行情報とインテリジェンス情報間での個別具体的な調整を図ったりするものではない。

[21] http://www.ise.gov/background-and-authorities

4. サイバーセキュリティ関連法案の状況

本章では以下、最近の米国議会におけるサイバーセキュリティ関連法案やサイバーセキュリティ関連の大統領令に関する状況についてまとめる。

(1) サイバーセキュリティ関連法案

2012 年以降のサイバーセキュリティ関連の主要な法案としては、①4 月に下院を通過した Cyber Intelligence Sharing and Protection Act（CISPA）、②Cybersecurity Act of 2012（廃案）、③上院に提出された SECURE IT Act、④下院に提出された Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act、などがある。以下、それぞれの法案の概要をまとめる。

＜Cyber Intelligence Sharing and Protection Act＞

「Cyber Intelligence Sharing and Protection Act（CISPA）」とは、第 112 議会において可決直前までいったサイバーセキュリティ法案である。同法案は、民間企業と DHS（国土安全保障省）がサイバースペースにおける脅威情報を共有することで、より効果的なサイバーセキュリティを実現しようとするものであるが、民間側による政府との情報共有においてプライバシー侵害が危惧された。実際、AT&T 社、Verizon 社、Microsoft 社、Facebook 社などの一部企業は賛同したものの、消費者の個人情報が政府の諜報機関や NSA（国家安全保障局）の手に渡るのではないかとの懸念から、プライバシー保護を訴える人権団体や多くのウェブサービス事業者から強い反対があり、大反対キャンペーンが繰り広げられた。結果、2012 年 4 月に下院を通過したものの、オバマ政権も「同法案が可決された場合、大統領は拒否権を発動する用意がある」という姿勢（veto threat）を明確にしたことや、上院で別途同様の法案（以下参照）を検討中であったことから、会期中に成立せず廃案となっている。

しかし、この CISPA は 2013 年 2 月、オバマ大統領によるサイバーセキュリティ強化に向けた大統領令（EO 13636 および PPD-21）の発令を受けて、共和党の Mike Rogers 下院議員と民主党の Dutch Ruppersberger 下院議員による超党派法案として、現在開催中の第 113 議会に再提出されている。Ruppersberger 議員は法案の再提出に関して、ホワイトハウスとの調整はとても順調であることを明らかにし、「今回は、政権側が前回の法案よりも協力的になることを期待している」と述べている[22]。また、法案の再提出には、新政権の CIA 長官として指名された John Brennan 氏の影響も指摘されている。Brennan 氏は、オバマ政権のサイバーセキュリティアドバイザを務めた経歴があり、今回の法案にも好意的とのことから[23]、CISPA の立法化を期待する声が改めて出てきている。

[22] http://thehill.com/blogs/hillicon-valley/technology/281309-ruppersberger-intelligence-committee-to-re-introduce-cispa-this-year
[23] http://www.dailytech.com/article.aspx?newsid=29866

ただし、CISPA の議会への再提出を受け、反対運動も再び始まっている。CISPA のプライバシーへの影響を懸念する数多くのウェブサービス事業者は 2013 年 3 月、ウェブサイト上に「CISPA is back（CISPA が復活した）」とするメッセージを一斉に掲載するという一大キャンペーンを展開したのである[24]。報道によると、インターネット上での権利保護に向けた団体 Electronic Frontier Foundation と Internet Defense League が主導したこのキャンペーンには、3 万にのぼるウェブサイトが参加したほか、法案反対へのオンライン署名活動への賛同者も 2 月に 30 万、3 月も 10 万を超えたとされている。

CISPA は 2013 年 4 月に下院を通過したが、4 月 22 日の週に他の研究開発促進等のサイバーセキュリティ関連法が集中的に上程、審議された一方で、上院では CISPA の採決について見送りとなった。政権側も、引き続き veto threat の方針を維持していると見られており、当面 CISPA の成立は困難になった[25]。

＜Cybersecurity Act of 2012＞

「Cybersecurity Act of 2012」とは、第 112 議会で上院に提出されたサイバーセキュリティ法案であり、オバマ政権が成立を目指していたものである[26]。特にライフラインや経済基盤となる重要インフラ（電力網や航空管制システムなど）に対するサイバーセキュリティ強化を狙ったものであり、官民が連携しながら、重要インフラへのサイバー攻撃に対する防御能力を高めるため、重要インフラを運営する民間企業に対して、必要十分なサイバーセキュリティ対策をとっているかどうかを DHS（国土安全保障省）に報告する義務を課すというものであった。しかし、この法案は米国商工会議所および産業界と手を組んだ上院共和党の反対に遭い、結果的に廃案へと追い込まれている[27]。産業界が政府による監視を警戒し、政府が民間企業のセキュリティを規制することを嫌ったことが原因で、特に DHS が民間を監視するという仕組みが法案成立の障害になったとされている[28]。

なお、上記の通りオバマ政権はこの Cybersecurity Act of 2012 の成立を目指していたため、業界では、同法案廃案になったことが、2013 年 2 月の大統領令（EO 13636 および PPD-21）の発令につながったと見られている。実際、ホワイトハウスは Cybersecurity Act of 2012 が廃案になってからすぐ、大統領令の作成に着手、数ヶ月をかけて作成したとされている。

＜SECURE IT Act＞

「SECURE IT Act」についても共和党議員により上記の Cybersecurity Act of 2012 に対抗する形で上院に提出されたサイバーセキュリティ法案である[29]。官民連携で重要イン

[24] http://www.huffingtonpost.com/2013/03/20/cispa-cybersecurity_n_2915325.html

[25] http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html

[26] 2012 年 7 月には、Wall Street Journal に同法案の成立を期待する大統領の論説文を寄稿している。
http://www.whitehouse.gov/blog/2012/07/20/taking-cyberattack-threat-seriously?utm_source=related

[27] http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/

[28] http://www.cnn.com/2012/11/13/tech/innovation/obama-tech-policy

[29] http://www.networkworld.com/news/2012/030112-republican-senators-introduce-their-own-256874.html

フラへのサイバー攻撃に対処するという点では Cybersecurity Act of 2012 と同じであるが、同法案と比較すると、民間に求める行動が緩和されている点が特徴となっている。具体的には、民間からの政府への情報提供を義務化せず、官民の情報共有を基本的に任意としており、DHS の役割なども明確にされていない。また、重要インフラの保護に向けた情報共有・連携にフォーカスしていた Cybersecurity Act of 2012 と違い、潜在的なサイバー脅威についての官民情報共有しか謳っていない、サイバー犯罪で有罪となった者への懲罰の厳罰化を定義している、という特徴もあった。ただし、SECURE IT Act も会期中に成立しないまま廃案となっている。

＜ Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act＞

上記の CISPA を可決した下院には、「Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act（PrECISE Act）」と呼ばれるサイバーセキュリティ法案も提出された[30]。同法案についても、官民の情報共有に向けたものであり、これを調整・指揮する連邦政府組織を設立すること、DHS（国土安全保障省）に連邦政府のシステムおよび民間の重要インフラのリスク評価をし、インフラ保護に向けた取り組みを推進する権限をあたえることを謳っていた。PrECISE Act についても、成立に至らず廃案となっている。

(2) サイバーセキュリティ関連の大統領令

オバマ政権は 2012 年以降、サイバーセキュリティ関連の大統領令（Executive Order：EO）と大統領指令（Presidential Policy Directive： PPD）を発令している。以下、これら 2 つの大統領令をまとめる。

＜PPD-20[31]＞

PPD-20 は、オバマ大統領が 2012 年 10 月中旬に機密扱いで発令した大統領令である。2004 年 7 月に当時のブッシュ大統領が発令した国家安全保障大統領令（National Security Presidential Directives/NSPD-38）をアップデートする形のもので、機密扱いのため詳細は明らかになっていないが、米国に所在する者や組織が被害を被るようなサイバー攻撃が起こると確信できる場合、米国軍にサイバー攻撃者を先制攻撃できるという武力行使の権限を与えると共に、その際の行動規範を定めたものとされている。NSA 長官でもある Keith B. Alexander 将軍が司令官として率いる DOD 傘下のサイバー司令部では、防衛だけでなく攻撃までも視野に入れた組織体制を構築していると言われているが、この PPD-20 の方向性とも符合する。

30 http://thehill.com/blogs/hillicon-valley/technology/199929-house-members-introduce-cybersecurity-bill
31 http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html

＜EO 13636/PPD-21[32]＞

上記の通り、オバマ大統領が第二期政権後、一般教書演説と同じ日（2 月 12 日）に発令した大統領令である。サイバーセキュリティへの取り組み強化を目指した各種法案（特に Cybersecurity Act of 2012）が廃案となるなど、議会がサイバーセキュリティ関連の立法について機能不全に陥っていることを踏まえたもので、現行法の枠内で官民連携体制の構築に向けた課題の洗い出し、具体的なスキームの構築を DOD、DHS、NIST などの関連機関に指示する内容となっている。特に、ガイドライン、手続きやベストプラクティスをとりまとめた Cybersecurity Framework 作成を担当する NIST はパブリックコメントの聴取やワークショップの開催（2013 年 4 月、5 月）を開始し、関係者からの意見聴取を進めているところである。

また、一般教書演説でも、オバマ大統領が議会による迅速な法制化を求めたことからも明らかなように、官民連携体制の構築には、現行法内では対応しきれない問題点も存在することが明らかであることから、本大統領令の作業結果を踏まえたサイバーセキュリティ立法作業が今後加速する可能性がある。

[32] http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

用語集

CI/KR:	Critical Infrastructure/Key Resource
CIRC:	Computer Incident Response Capability
CIRT:	Computer Incident Response Team
CIPAC	Critical Infrastructure Partnership Advisory Council
Cyber UCG	Cyber User Coordination Group
CS&C	Office of Cybersecurity and Communication NPPD/DHS 内でサイバーセキュリティ情報の集約等を担当する。NCCIC 所管。
DHS	Department of Homeland Security 国土安全保障省
DOC	Department of Commerce 商務省
DOD	Department of Defense 国防総省
EO	Executive Order 大統領(指)令
FBI	Federal Investigation Bureau 連邦捜査局
FIPS:	Federal Information Processing Standardization IT システムに関する連邦政府標準規格
GCC	Government Coordinating Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive 国家安全保障令 ブッシュ政権下での大統領令の一形態
IC	Intelligence Community インテリジェンスコミュニティ
ICS-CERT	Industrial Control System Computer Emergency Response Team US-CERT の制御システム版。NCCIC/DHS 内に設置されている。
ISAC	Information Sharing and Analysis Center 情報共有分析センター
NCCIC	National Cybersecurity and Communication Integration Center 国土安全保障省におかれたサイバー脅威情報を監視集約する組織
NCIRP	National Cyber Incident Response Plan 国家サイバー事故対応計画
NICC	National Infrastructure Coordinating Center 全米インフラ調整センター
NIPP	National Infrastructure Protection Plan 国家インフラ防護計画
NIST	National Institute of Standard and Technology 国立標準技術研究所
NOC:	National Operations Center
NPPD	National Protection and Program Directorate DHS 内のサイバー担当局
NSA	National Security Agency 国家安全保障局
ODNI	Office of the Director of National Intelligence (大統領府)国家情報長官室
OSTP	Office of Science and Technology Policy (大統領府)科学技術政策室
PPD	Presidential Policy Directive オバマ政権下での大統領令の一形態
RAT	Remote Access Tool
SCC:	Sector Coordinating Council
SSA	Social Security Administration 社会保障庁
VPN	Virtual Private Network
US-CERT:	United States Computer Emergency Response Team