

「米国連邦政府のサイバーセキュリティ政策を巡る動向」

市川類@JETRO/IPA NY

1. はじめに

米国においては、情報化が進展している半面、悪意ある活動が活発であり、したがって、情報セキュリティ全体の中でも、インターネットを通じた悪意ある活動を対象とするサイバーセキュリティが大きな課題となっている。

特に、近年にサイバー攻撃が急増する中、主要な攻撃対象となる連邦政府における対応が喫緊の課題となっており、連邦政府におけるサイバーセキュリティ対策においても、重要インフラの保護から近年さらに包括的なサイバーセキュリティを目指す方向にある。

このような中、オバマ政権においては、サイバーセキュリティ対策を重視する方向を示しているものの、ホワイトハウス主導による体制整備は遅れている。一方、サイバー攻撃が増加する中、米国全体においては、今後、来るべきサイバー戦争に向けて体制整備も念頭に、国防総省（DOD）や、国土安全保障省（DHS）においては、その対策の強化に努めつつある。

このような問題意識の下、本報告書においては、米国におけるこれまで及びオバマ政権下におけるサイバーセキュリティ政策を巡る最近の動向について、報告する。（なお、最近のグーグルへのサイバー攻撃と中国との関係については、別途報告する。）

2. サイバーセキュリティの位置づけと現状

（1）情報セキュリティとサイバーセキュリティ

本稿においては、情報セキュリティの中でも、特に米国において関心が高く、喫緊の課題となっているサイバーセキュリティに係る政策動向について報告する。

① 情報セキュリティ（広義）とサイバーセキュリティの関係

<情報セキュリティの定義>

一般的に、情報セキュリティとは、「情報の機密性、完全性、可用性を保持すること」と定義される。これは、もともと、1992年にOECDが発表した情報セキュリティ・ガイドラインの序文において、情報セキュリティを、これらの三要素

を維持・管理することとして定義しており¹、その後、国際的な情報セキュリティ・マネジメント・システム (ISMS) 標準であるISO/IEC 27001²においても、上記の三要素によって定義している³。また、米国のFederal Information Security Management Act (FISMA) of 2002においても、同様に、「情報セキュリティ」を、以下のように定義している。

FISMAによる情報セキュリティの定義⁴

○「情報セキュリティ」とは、以下の3項目を提供することによって、情報及び情報システムを、不正なアクセス、利用、開示、破壊、改ざんから保護すること。	
①完全性 (Integrity)	不適切な情報の改竄・破壊から守ること (情報の否認防止と真正性の確保を含む)
②機密性 (Confidentiality)	情報へのアクセス・開示について権限ある制限を守ること (個人のプライバシーや機密情報を守ることを含む。)
③可用性 (Availability)	情報へのタイムリーで信頼性の高いアクセス及び利用を確実にすること。

<情報セキュリティにおけるサイバーセキュリティの位置づけ>

一方、サイバーセキュリティとは、明確な定義はないものの、一般的には、サイバースペースと呼ばれるインターネット等のネットワークで接続された空間において、悪意ある第三者による不正侵入、情報の流出またはシステムの破壊、から保護することを指すものとされる⁵。

すなわち、サイバーセキュリティとは、情報セキュリティの中でも、

- ・ 「ネットワーク (オンライン) 経由の行為」
- ・ 「悪意ある者の行為」

に対する対応であると位置づけられる。したがって、サイバーセキュリティには、一般的に、非ネットワーク経由のもの (例えば、USBでの無断コピーなど) や、悪意のないもの (例えば、メールミスによる情報流出など) は含まれない⁶。

¹ Organization for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems*, 1992,

http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1,00.html

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity”;

² ISO/IEC 27001 は、情報セキュリティマネジメント・システム (ISMS) を構築、運用、監視、検査、維持、改善するためのモデルを提供する標準。

³ “preservation of confidentiality, integrity and availability of information”;

<http://www.iso27001security.com/html/27002.html#Section2>

⁴ *Federal Information Security Management Act (FISMA)*,

<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> ; Chapter 35, Title 44 U.S.C. § 3542(b)-(1)

⁵ <http://www.weblio.jp/content/%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%83%B%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3>

⁶ ただし、例えば、ファイルシェアソフトを通じた情報流出などは、両面を有するなど、完全には分離して議論できない面はある。(いずれにせよ、リスク管理であるとも言える。)

このうち、一般的には、情報セキュリティにおける情報流出等の事例の大半は、「非サイバー」の要因に依るものとされるが、今後、ITシステムのネットワーク化が進む中で、情報セキュリティにおけるサイバーセキュリティの位置づけは大きくなるものと考えられる。

サイバーセキュリティ・情報セキュリティに係る整理⁷

	政府（国防）	一般政府、重要施設（民間）	一般民間企業	個人
情報セキュリティ（広義）				
サイバーセキュリティ（悪意ある者によるオンラインを通じた行為からの保護）				
完全性	サイバー攻撃、サイバーテロ、クラッキング等			米国の関心
可用性				日本の関心
機密性	サイバースパイ、不正アクセス、ハッキング等			
（非サイバーの）情報セキュリティ（非悪意的、又は、非オンラインにかかるリスク低減）				
完全性	（非オンライン）内部犯行によるシステム改竄等			
可用性	（非悪意的）システム障害、バグ等			
機密性	（非オンライン）物理的情報流出、内部犯行による情報流出等 （非悪意的）情報流出ミス等			
cf.機密性の対象情報	国防機密情報	政府機密情報	企業機密情報	ID、個人情報

<情報セキュリティ対策におけるサイバーセキュリティへの重点の違い>

一般的に、企業等の各主体における情報セキュリティ対策とは、問題が生じることによって被害が生じるリスクを全体として如何に軽減するか、という一種のリスク管理対策であり⁸、個々の技術的対策に加え、（特に非サイバーのセキュリティに対しては）組織としてのマネジメント対策が重要になる。

このような中で、情報セキュリティ対策において、サイバーセキュリティに重点が置かれるか否かは、当該各主体におかれている状況によって異なるものと考えられる。一般的に、米国においては、政府・重要施設を中心としたサイバーセキュリティ対策に関心が高いのに対し、日本では、民間を中心とする（非サイバーの）情報セキュリティ対策に関心が高いように見受けられる。

- ・ 米国においても、一般的に、「非サイバー」による事案は、日本以上に多いとされる。しかしながら、米国では、サイバー攻撃等に係る被害がそれ以上に多く、特に、米国の連邦政府・重要施設は世界の中でも多く狙われており、これらを対象としたサイバーセキュリティ対策・政策に関心の重点がある。
- ・ 一方、日本においては、官民ともに、相対的にサイバー攻撃等を受ける事例は少なく、このため、システム障害も含め「非サイバー」の事案に相対的に関心

⁷ 出典：筆者作成。図の「米国の関心」「日本の関心」はあくまでも相対的なものであり、例えば、米国においても、システム障害や、情報流出の事例等は多数存在する。（ただし、日本と比べて、相対的に、社会の関心は薄い。）

⁸ したがって、情報セキュリティに係るリスクを、完全にゼロにすることは困難である。

がある。特に、プライバシー問題への関心が相対的に高い⁹こともあり、非サイバーを中心とした個人情報保護対策に重点が置かれているように見える。

② サイバー攻撃者・スパイ（悪意ある者）の動機と手段

＜サイバー攻撃者・スパイ（悪意ある者）に係る動機＞

サイバーセキュリティに係る事案（主としてサイバー犯罪）は、悪意ある者（サイバー攻撃者・スパイ等）によって行われる。その動機としては、一般的に、国家・安全保障的動機、経済的動機、個人的動機があるとされ、いずれにせよ、システムの破壊等（完全性、可用性関連）、あるいは、情報の不正入手（機密性関連）を目的とする。

従来においては、個人的動機に注目されていた面もあるが、サイバー犯罪の組織化が進む中で、今後、経済的動機（組織レベル）に加え、国家・安全保障的動機（国レベル）のものが増加することも想定される。

サイバー犯罪に係る主な動機とその対象¹⁰

動機	主な対象主体	例	主な目的
国家・安全保障的動機	国防・重要施設 一般政府	・テロリストによる危害の付与 ・各国による諜報活動 ¹¹	システム破壊 機密・個人情報入手

⁹ なお、米国においては、日本のような広範な個人情報保護法は、連邦レベルでは制定されていない。

＜情報セキュリティとプライバシー政策の関係＞

なお、個人情報に関して、情報セキュリティにおける情報の機密性に関しては、基本的には、当該主体が機密と考える個人情報に対して、許可を得ない者が不正にアクセスすることを防止することを意味する。

しかしながら、その際、その機密とする個人情報の範囲は何か（例えば公に得られる情報は、個人情報か）、あるいは、その個人情報は誰がどのように利用できるか（アクセス・利用権限）などといった利用に係るルール（プライバシー政策）を確定することが、情報セキュリティの検討にあたっての前提となる（これらは、社会及び時代によって変化しうるものと考えられる）。また、これらのルールは、企業のリスク回避行動を通じて、企業における情報セキュリティ行動、また、企業の IT 利用に関しても大きな影響を影響を与える。

なお、企業の知的財産・著作権政策においても、同様のことが言える。

情報セキュリティとプライバシー政策・知的財産政策（ルール）との関係

対象情報	情報セキュリティの問題 (サイバー、非サイバー)	利用ルールの問題 (範囲の問題、アクセス・利用権限の問題)
個人情報	個人情報の漏洩	プライバシー問題（対象範囲、企業における利用権限等）
知的財産	企業秘密・著作権作品の漏洩	企業情報公開ルール、著作権問題（Fair Use・私的利用の範囲等）

出典：筆者作成。

¹⁰ 出典：筆者作成。ただし、実際には、これらの分類に曖昧な部分もある。（Hackivists など）

¹¹ ＜諜報活動とセキュリティ、また、検閲、有害情報規制との関係＞

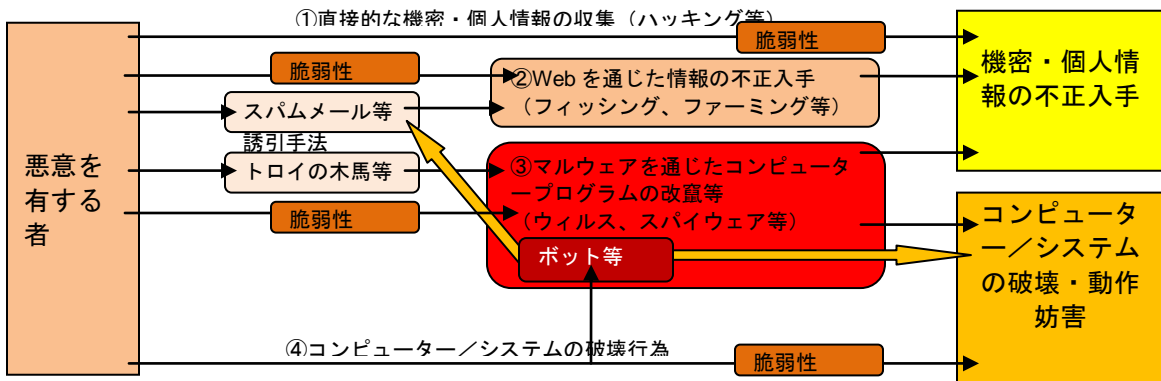
なお、米国を始め、世界各国においては、諜報（Intelligence）活動・犯罪捜査活動等の中で、盗聴（Wiretrapping）を行っている。これらは、少なくとも国内では、原則合法的に行われものであり、また、一般的には、通信上の情報を傍受（場合によっては暗号を解読）することによって行われる。（ただし、通信を傍受できない海外では、下記のようなマルウェアによる手法等も利用されているものと考えられる。）しかしながら、諜報活動は、（特に、国内においては）実際にプライバシーの侵害であると批判されることも多く、また、海外から見れば、セキュリティ上の問題となる。

経済的動機	一般企業、個人	・ 経済的利益を狙った犯罪	機密・ID情報入手
個人的動機	各主体	・ ハッキングによる自己達成、 覗き見、いやがらせ他	システム改竄、 個人情報入手

＜サイバー攻撃・スパイの手法＞

これらの悪意ある者が、セキュリティを突破する目的を達成する手法は、時代によって深化しつつあるものの、ソフトウェアや Web サイトの脆弱性等を突いて、直接情報を入手したり、直接的にコンピューターを破壊したりする手法に加え、ネット（Web）を通じた詐欺的手法、PC へのウィルス感染等を通じた手法がある。

サイバー攻撃の全体像（イメージ）と代表的なサイバー攻撃の種類¹²



種類	名称	概要
手直接情報入	辞書攻撃	辞書に載っている単語を延々と試し、パスワードを解読する解析方法
	ブルートフォース攻撃	実在する可能性のあるパスワードを次々と試すことで、パスワードを解読する方法
	中間者攻撃	認証処理（公開鍵の交換）に攻撃者が介入し、偽の公開鍵を送信する方法。当事者が気付かないまま、攻撃者に情報を送信することになる

なお、国による諜報活動に関連して、検閲、及び、有害情報規制がある。
 ・諜報活動や犯罪捜査活動は、検閲・有害情報規制とは異なり、直接的に情報公開を規制するものではなく、原則、直接的には、表現の自由との関係はない。しかしながら、諜報活動等によって入手した情報に基づき、国が関与・規制することは否定できず、そのような意味で表現の自由にも関係する。
 ・検閲・有害情報規制は、事前規制によるものか、事後規制かという違い。なお、その対象範囲は、性的な情報などに加え、国家安全保障的なもの（犯罪予告に係る情報なども含む）など国によって異なるが、程度の問題という見方も一方ではされる。（米中の比較については、NYだより2009年3月号参照）

諜報活動、検閲、有害情報規制の関係

	非公開・機密情報の収集 (情報セキュリティに関連)	情報の公開に対する規制
事前チェック（オンタイム）	諜報活動（通信の盗聴）	検閲（事前規制）
事後活動	司法・犯罪捜査活動	有害情報規制（事後規制）

(出典)筆者作成。

¹² 出典: イメージ図については、筆者作成(実際には、更に複合的な攻撃も多く想定される)。

代表的な種類については、<http://www.sophia-it.com/>、<http://e-words.jp/> より筆者作成。

ネット詐欺	スパムメール	営利目的のメールを無差別かつ大量に送りつけること。多くは、架空請求、フィッシング詐欺目的。
	フィッシング詐欺	信頼できる機関のウェブサイトを装って詐欺を働くこと。信頼して個人情報を入力することにより、情報が窃盗される。
	ファーミング詐欺	フィッシング詐欺の発展版。ユーザーが正しいURLを入力しても、自動的に偽のサイトに誘導される。
	ワンクリック詐欺	ウェブ上での契約が成立していない段階で、契約が成立したと勝手に見なし、不当な架空請求を繰り返し行うこと。
マルウェア ¹³	トロイの木馬	コンピューターへの侵入にあたって、無害なプログラムを装ってユーザー自らにダウンロードさせることで侵入するタイプのウイルス。
	ウイルス	コンピューターに感染して、破壊活動を行ったり、問題を引き起こしたりするプログラム。
	ワーム	ウイルスのうち、ユーザーに気づかれないまま、インターネットを通じて自己増殖を行う性質を持つもの。
	スパイウェア	ウイルスのうち、ユーザーが気付かない間に、ユーザーの行動や個人情報を収集したり、プログラムを実行したりするもの。
	ボット	ウイルスのうち、攻撃者からの指令を待ち、指令どおりの処理を、感染者のコンピューター上で実行するもの。DoS攻撃の発信源となったり、スパムメールの踏み台となったりする。
	バックドア	次回も侵入できるようされたプログラム。ウイルスを通じて一旦バックドアが設けられると、いつでも不正侵入され、他のコンピューターの攻撃等に利用される。
Dos攻撃	F5攻撃	サーバーに大量のリクエストを送り、付加を与えてシステムダウンを起こさせること。人海戦術的な手法。
	DDoS (Distributed Denial of Service)	標的となるコンピューターに対し、複数のコンピューターから大量の処理負荷を与えること。攻撃にはマルウェアに侵入された一般のコンピューターが踏み台にされる。

この中でも、特に、ボット等は、感染者（被害者）が、各種サイバー攻撃の踏み台とされ、攻撃者となりうるということで重要な位置づけとなる。

また、それが故に、サイバー攻撃源の特定にあたって、直接攻撃した当該コンピューターを特定したとしても、その裏で実際に操作している攻撃者の特定は困難を極めることが多い（特に、国境を越えて司法権のない国を源とする場合）¹⁴。

（2）米国のサイバーセキュリティと情報セキュリティ投資の現状

米国においては、ITシステム・ネットワーク化が発展している反面、悪意ある活動が活発であり、情報セキュリティの中でも、サイバーセキュリティが大きな課題となっている。

¹³ マルウェアとは、コンピュータウイルス、ワーム、スパイウェア等「悪意のこもった」ソフトウェアのこと。

¹⁴ また、更に、攻撃源となるコンピューターを特定したとしても、実際にそれを操作したのは誰か、また、それは誰の指示によってなされたのか、については、オンライン上では特定できない。

なお、このような中、FBIは、最近、（悪質な活動が活発である、）ウクライナ、オランダ、エストニアに職員を送っている。<http://www.computerworld.jp/topics/vs/176089.html>

その中でも、米国連邦政府は、世界の中でも標的にされやすく、このため、連邦政府等におけるサイバーセキュリティ対策は喫緊の課題となっている。

① 米国における悪質な活動の状況

＜悪質な活動に係る世界における米国の位置づけ＞

米国においては、他国と比較して、一般的に悪質な活動が活発であり、したがって、被害も大きいものと想定される。

実際に、各種の調査によると、米国は、世界の23%~38%と、概ね、世界のトップを占めており、その他の国としては、中国が多い。ただし、これらの国では、そもそものブロードバンド利用者が大きいこと（中国21%、米国20%、ドイツ6%）を考慮すると、必ずしも飛びぬけて高い訳ではない¹⁵。また、これらの米国での悪意ある活動の全てが、米国を起源とする訳でもない。

インターネットにおける悪意ある活動の国別比較¹⁶
(Symantec Global Internet Security Threat Report: Trends for 2008 総合評価)

順位	国	合計割合	悪意	Spam	Phising	Bot	攻撃源
1	米国(1)	23% (26%)	1	3	1	2	1
2	中国(2)	9% (11%)	2	4	6	1	2
3	ドイツ (3)	6% (7%)	12	2	2	4	4
4	英国 (4)	5% (4%)	4	10	5	9	3
5	ブラジル (8)	4% (3%)	16	1	16	5	9
6	スペイン (6)	4% (3%)	10	8	13	3	6
7	イタリア (7)	3% (3%)	11	6	14	6	8
8	フランス (5)	3% (4%)	8	14	9	10	5
9	トルコ (15)	3% (2%)	15	5	24	8	12
10	ポーランド (12)	3% (2%)	23	9	8	7	17

¹⁵ ただし、日本は、全く上位に入っておらず、特に、ブロードバンド人口等を考慮すると、サイバーセキュリティに係る悪質な活動は、世界の中でも飛びぬけて低いとも言える。

¹⁶ 出典：総合評価と、Webベースの攻撃源については、Symantec Global Internet Security Threat Report: Trends for 2008(2009年4月)より。(なお、総合評価のうち、括弧内は、2007年の順位と割合。また、それぞれの活動は、「悪意」: Malicious Code、「Spam」: Spam Zombies、「Phising」: Phishing Websites Host Ranking、「Bot」: Bot、「攻撃源」: Attack Origin。)

http://www.symantec.com/connect/sites/default/files/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

また、マルウェア感染サイトの割合については、Sophos(2010年2月)の資料より。

<http://www.sophos.com/pressoffice/news/articles/2010/02/malware-hosting-countries.html>

なお、これ以外にも、McAfeeがの2009年第4四半期における報告書(2009年2月)によると、
・ゾンビPC(マルウェアの感染により、外部から不正操作できる状態のままに放置されたコンピューター)の多い国:これまでトップだった米国が2位に後退する一方、中国が1位(12%)となった。

・SQLインジェクション攻撃の発信源:中国が過半数の54%を占めるなどの統計がある。<http://www.computerworld.jp/topics/vs/174310.html>
http://newsroom.mcafee.com/article_display.cfm?article_id=3621

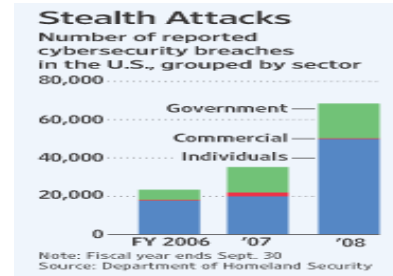
ウェブベースの攻撃源の割合（同上）マルウェア感染サイトの割合（Sophos）

順位	国	合計割合	順位	国	合計割合
1	米国	38%	1	米国	37.4%
2	中国	13%	2	ロシア	12.8%
3	ウクライナ	12%	3	中国	11.2% ¹⁷
4	オランダ	8%	4	ペルー	3.7%
5	ロシア	5%	5	ドイツ	2.6%

<サイバーセキュリティ事案における政府の位置づけ>

一方、米国の中では、サイバーセキュリティによる情報漏洩に係る事案数（WSJ 記事¹⁸；右記図参照）で見た場合、個人に加えて、政府部門における事案数が非常に多いのが特徴である。

ただし、民間企業における被害事案数が少ないのは、多くの場合、報告・公表を行っていないためではないかと推測される。



② 米国の情報セキュリティ投資の状況

<情報セキュリティに係る市場規模>

米国における（サイバーセキュリティ対策、非サイバーセキュリティ対策の両方を含む）情報セキュリティに係る投資は、他の地域と比較して比較的多く¹⁹、かつ、近年増加傾向にある。

具体的には、日本ネットワークセキュリティ協会の調査²⁰によると、2009年の米国の情報セキュリティ市場は約266億ドルであり、世界全体の46%を占める。また、世界の情報セキュリティ投資は、近年の経済危機に関わらず、着実に伸びているとされる。

主要地域の情報セキュリティ市場の規模と対GDP比²¹

¹⁷ なお、中国に関しては、前々年の51.4%、前年の27.7%から急激に減少している。

¹⁸ <http://online.wsj.com/article/SB123914805204099085.html>

¹⁹ なお、日本は、サイバーセキュリティに係る悪意ある活動が少ない割には、投資額は多いとの見方も可能である。（非サイバー事例対策に係る投資が多い可能性もある。）

²⁰ 情報セキュリティ市場調査報告書（2009年3月）
<http://www.meti.go.jp/policy/netsecurity/h20fymarketresearchreport.pdf>

²¹ 出典：セキュリティ市場の投資額は、情報セキュリティ市場調査報告書（2009年3月）のデータを利用。（情報セキュリティ市場には、アプライアンス（機器）、ソフトウェア、サービスを含む。）

2008年は見込値、2009年は予測値。（なお、欧米については、IDCによる経済危機直後の見込みであり、経済危機の影響が十分に反映されていない可能性がある。）

<http://www.meti.go.jp/policy/netsecurity/h20fymarketresearchreport.pdf>

	規模 (単位: 億円)				対 GDP 比			
	2006	2007	2008	2009	2006	2007	2008	2009
北米	20,279	24,422	24,951	28,185	0.120%	0.136%	0.150%	0.172%
西欧	11,778	14,564	15,022	17,040	0.090%	0.105%	0.118%	0.137%
日本	5,972	6,847	7,268	6,874	0.109%	0.122%	0.131%	0.131%
世界	44,103	53,306	55,153	61,181				

世界のセキュリティソフトウェア市場とその伸び²²

	2007	2008	2009	2010
市場規模	11.4	13.5	14.5	16.3
対前年度伸び	20%増	19%増	8%増	13%増

<米国の連邦政府の情報セキュリティ予算>

この米国の情報セキュリティ市場において、連邦政府の役割は非常に大きいものと考えられる。

実際に、統計が異なるため必ずしも同じ評価はできないものの、米国連邦政府における 2009 年の予算要求時点での情報セキュリティ予算は、約 73 億ドルであり、また、このうち国防総省 (DOD) が約半分強 (約 42 億ドル) を占める。

米国連邦政府における IT 投資予算と IT セキュリティ予算の割合²³

	2007 年 実績	2008 年 実績	2009 年 実績	2010 年 推定額	2011 年 要求額(割合)	IT Security 割合(09)
DOD	34,384	36,980	34,523	34,288	36,534 (46%)	12.2%
DHS	4,455	5,252	6,532	6,541	6,412 (8%)	7.5%
HHS	5,526	5,692	5,683	6,165	6,212 (8%)	4.0%
VA	1,735	2,526	2,843	3,373	3,356 (4%)	4.7%
DOT	2,769	2,830	3,034	3,134	3,351 (4%)	25.7%
Treasury	2,673	2,896	2,995	3,164	3,263 (4%)	7.4%
DOJ	2,405	2,299	2,856	2,991	3,017 (4%)	8.3%
USDA	2,086	2,000	2,425	2,584	2,704 (3%)	4.7%

GDP に関しては、欧米に関しては、同報告書の為替レート(1ドル当たり 2006 年: 116.3310 円、2007 年: 117.8145 円、2008 年: 105.8768 円、2009 年: 105.8768 円)で割り戻した上で、以下の数字を利用 (2009 年は推定値)。 <http://www.oecd.org/dataoecd/48/4/37867909.pdf> 一方、日本については、以下の数字を利用。 http://ecodb.net/country/Jp/imf_gdp.html

なお、北米は、アメリカ合衆国およびカナダの合計。西欧は、欧州内の OCED の統計諸国(英国、フランス、ドイツ、オランダ、ベルギー、イタリア、スペイン、ポルトガル、デンマーク、アイスランド、ルクセンブルグ)のうち、アイスランドを除く 10 カ国の合計。

²² 出典: 以下の Gartner の資料。(ソフトウェアのみを対象。単位: 10 億ドル)

<http://www.gartner.com/it/page.jsp?id=1031712>

2009 年以降の見込み。 <http://www.gartner.com/it/page.jsp?id=1184713>

2007 年の対前年度伸び率 <http://www.gartner.com/it/page.jsp?id=697307>

²³ 出典: 以下より作成。(IT Security 割合は、2009 年要求における各省庁の IT 投資予算における割合)

<http://www.whitehouse.gov/omb/asset.aspx?AssetId=2321>

<http://www.whitehouse.gov/omb/e-gov/docs/> なお、IT Security 予算については、2009 年要求資料に掲載されているデータを採用。(それ以降はデータなし。)

DOC	1,704	1,983	3,791	6,572	2,437 (3%)	7.7%
DOE	1,995	2,086	2,135	2,192	2,200 (3%)	12.1%
その他	8,428	8,233	9,318	9,614	9,889 (12%)	
合計	68,160	72,777	76,135	80,645	79,375 (100%)	9.4%
IT Security	約 5,900	6,631	7,278			

3. 連邦政府におけるサイバーセキュリティ政策・体制を巡る動向

このような中、米国連邦政府の政策においては、情報セキュリティの中でも、サイバーセキュリティ対策を中心に動いてきている。

(1) これまでの連邦政府におけるサイバーセキュリティ政策と体制

米国連邦政府のサイバーセキュリティ政策は、クリントン政権後期から、テロ対策／重要インフラ保護の観点から中心に進められてきたが、サイバー攻撃の増加に対応して、包括的な対策が求められるようになってきている。

① 連邦政府のサイバーセキュリティ政策の推移

<テロ対策／重要インフラ対策としてのサイバーセキュリティ対策>

米国連邦政府のサイバーセキュリティ政策は、クリントン政権期において、重要インフラ保護のための政策を打ち出したことに端を発する²⁴。

その後、2001年9月の同時多発テロを経て、米国側からの報復に対して、テロリストがサイバー攻撃で逆報復するであろうとの認識から、重要インフラ保護に係る取り組みを強化し、その後、2003年に、国家サイバー戦略の発表と併せて、サイバーセキュリティ政策に係る権限を、新たに設置された国土安全保障省(DHS)に移管した。

米国連邦政府におけるサイバーセキュリティ政策の経緯²⁵

クリントン 政権	1996年6月：大統領令(Executive Order) 13010号を発令。 ・ PCCIP (President's Commission on Critical Infrastructure Protection) の設置。 ・ 重要インフラの定義と防護策の検討。 1997年10月：PCCIPは、報告書(勧告)を発表。
-------------	---

²⁴ 当時において、DODによる模擬試験により、重要インフラのITシステムが攻撃に対して非常に脆弱であることが判明したことがきっかけとされる。

<http://www.nistep.go.jp/achiev/ftx/jpn/stfc/stt007j/feature2.html>

²⁵ 出典：以下等より作成。(なお、黄色部分は、主要報告書、イニシアティブ)

NYだより2004年12月、<http://www.jipdec.jp/chosa/kiban/03/security.html>、

<http://www.nistep.go.jp/achiev/ftx/jpn/stfc/stt007j/feature2.html>

	<p>↓</p> <p>1998年5月：<u>大統領決定指令（PDD：Presidential Decision Directive）63</u>を発表。</p> <ul style="list-style-type: none"> ・国家調整官、国家インフラ保証会議（NIAC）の設置 ・国家インフラ保護センター（NIPC：FBI内）の設置（サイバー攻撃の監視等） ・重要インフラ保証局（CIAO：商務省内）、重要インフラごとの情報共有分析センター（ISAC）の設置等 <p>↓</p> <p>2000年1月：<u>National Plan for Information Systems Protection²⁶</u>発表。</p>
ブッシュ政権	<p>2001年9月：同時多発テロ発生。</p> <p>↓</p> <p>2001年10月：<u>大統領令（Executive Order）13231</u>を発令。</p> <ul style="list-style-type: none"> ・PCIPB（President’s Critical Infrastructure Protection Board）設立。 <p>↓</p> <p>（2002年11月：Cyber Security R&D Act成立。）</p> <p>（2002年12月：E-government Act of 2002成立。）</p> <ul style="list-style-type: none"> ・うち Title IIIは、FISMA（Federal Information Security Management Act） <p>（2003年1月：国土安全保障省（DHS）業務開始。）</p> <p>2003年2月：<u>大統領令 13286</u>を発令（PCIBP事実上廃止）。</p> <p>2003年2月：<u>National Strategy to Secure Cyberspace²⁷</u>発表。</p>
DHS	<p>2003年6月：DHS内にNational Cyber Security Division (NCSD)を設置。</p> <ul style="list-style-type: none"> ・NIPC、CIAOその他の他省の部局を統合。 <p>2003年9月：US-CERT設立（カーネギーメロン大学内のCERT/CCとも連携）。</p> <ul style="list-style-type: none"> ・2004年1月National Cyber Alert Systemの運用開始。 <p>2003年12月：<u>HSPD（Homeland Security Presidential Directive）-7</u>を発表。</p> <ul style="list-style-type: none"> ・PDD 63の改訂版。 <p>↓</p> <p>2005年2月：National Infrastructure Protection Plan（NIPP）暫定版策定。</p> <p>2006年6月：NIPP策定。2009年改定²⁸。</p> <p>2008年1月：<u>Comprehensive National Cyber Security Initiative（CNCI）²⁹（NSPD54/HDPD 23）</u>を策定。</p> <p>2008年3月：DHS内にNational Cyber Security Center（NCSC）設立。</p>
オバマ政権	<p>2009年2月：Cyber Security政策の60日間での見直しを指示。</p> <p>2009年5月：<u>Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure</u>発表。</p> <p>2009年12月：Cyber Security Coordinatorの任命。</p>

<重要インフラ保護に係る取り組み>

このような中、DHSにおいては、（同省設置法に基づく）HSPD-7³⁰に基づいて、重要インフラ（Critical Infrastructure and Key Resources: CIKR）の保護に係る計

²⁶ <http://clinton4.nara.gov/media/pdf/npisp-execsummary-000105.pdf>

<http://cryptome.org/cybersec-plan.htm>

²⁷ http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

²⁸ http://www.dhs.gov/files/programs/editorial_0827.shtm

²⁹ http://www.dhs.gov/files/programs/gc_1234200709381.shtm

³⁰ NYだより2005年11月号参照。

画（NIPP）を策定するとともに、各担当省庁及び地域・産業界等との連携のもとで、セクター別プランをとりまとめ、策定してきている。

National Infrastructure Protection Plan (2009)に示される 18 セクター³¹

担当省庁	重要インフラ分野
農水省（DOA）／健康保健省（HHS）	農業・食料
国防総省（DOD）	国防産業基盤
エネルギー省（DOE）	エネルギー
健康保健省（HHS）	医療・公衆安全
内務省（DOI）	国家モニュメント・アイコン
財務省（Treasury）	銀行・金融
環境保護庁（EPA）	水
国土安全保障省（DHS）	
インフラ保護室	化学、商業施設、重要製造業、ダム、緊急サービス、原子炉・核燃料・廃棄物
サイバーセキュリティ・通信室	情報技術、通信
運輸安全局（TSA）	郵便・海運
運輸安全局（TSA）／沿岸警備局（USCG）	運輸システム
移民税関局（ICE）連邦保護サービス	政府施設

② ブッシュ政権のサイバーセキュリティ対策の取り組み（CNCI）

<DHS の能力に対する批判と連邦政府への攻撃の増大>

しかしながら、サイバーセキュリティ政策全体に係る連邦政府全体のとりまとめを DHS に移管したことについては、格下げであるとして、その後トップの辞任が相次いだ³²。実際に、DHS においては、（上記重要インフラのレポートのとり

http://www.hitachi.co.jp/Prod/comp/Secureplaza/sec_trend/ls/is/isac01.html

³¹ http://www.dhs.gov/xlibrary/assets/nipp_executive_summary_2009.pdf

http://www.dhs.gov/files/programs/gc_1189168948944.shtm

http://www.dhs.gov/files/programs/gc_1179866197607.shtm

³² 具体的に、米国連邦政府のサイバーセキュリティに係るトップを巡る就任・辞任は、以下の通り。

- ・9/11直後の2001年10月、大統領重要インフラ防護委員会（President's Critical Infrastructure Protection Board: PCIPB）をホワイトハウスに設立。Richard Clarke氏委員長。（Clarke氏は、PDD63に基づく、初代の国家調整官。）

- ・2003年2月、PCIPBの廃止とDHSへの移行を決定。Richard Clarke氏は格下げを批判して2月に辞任。副委員長であったHoward Schmidt氏（後のCyber Security Coordinator. 後述）が後任に就任したが、同じ理由で、4月に辞任。

- ・2003年6月、DHSはNCSD（National Cyber Security Division）を新設。初代DirectorにAmit Yoran氏就任。しかしながら、2004年9月、十分な権限が与えられていないとして辞任。その後、副DirectorのAndy Purdy氏が、2年間暫定を勤める。なお、2005年7月、DHSは、NCPDよりも格上げのCS&C（Cyber Security & Communications）に、ポストを設立。2006年9月、DHSのCS&CポストにGreg Garcia氏が就任。その後、Bush政権終わり（2008年末）まで就任。

- ・2008年3月、DHSにNational Cyber Security Center（NCSC）設立。トップにRod Beckstrom氏就任。し

まとめは行っているものの)、サイバーセキュリティに係る技術的知見を十分に有さず、そのため、サイバーセキュリティに強く関与する国防総省(DOD)を含め、全省庁をとりまとめきれていないという批判は多い³³。

また、その後、概ね2007年以降から、連邦政府等に対するサイバー攻撃が多く発生・報道されているが³⁴、これらに対して、ブッシュ政権は、サイバーセキュリティに積極的に取り組んでいないという批判も多くなされた。

<包括的国家サイバーセキュリティイニシアティブ(CNCI)の策定>

このような中、2008年1月、ブッシュ大統領(当時)は、Comprehensive National Cyber Security Initiative(CNCI)に係る大統領令(NSPD64/HSPD23)に署名をした³⁵。

本大統領令に係る詳細は、機密情報として公表されていないが、基本的には、連邦政府に対するサイバー攻撃から保護するため、DOD/NSA(National Security Agency)の能力を強化する一方、それらを活用してDHSで全体のとりまとめを行うという体制を目指しているように見受けられる。すなわち、報道によると、

- ・ DODのNSA等の諜報機関における侵入等に係るモニタリングを強化。
- ・ DHSにおいては、NSAを含む連邦政府全体におけるモニタリングデータの収集・分析、民生系省庁でのサイバーセキュリティ対策の促進等。

などを中心とし³⁶、具体的には、EINSTEINプログラム、Trusted Internet Computingなど12分野の取り組みを含む³⁷と報道されている。

これを踏まえて、DHSにおいては、NSA、FBI等と連携して政府全体のサイバーセキュリティの全体像の把握を行う、National Cyber Security Center(NCSC)

かしながら、2009年3月、同氏は、NCSCは、NSAに牛耳られていると批判して辞任。

・2009年3月、DHSのNPPDのDeputy Under Secretary(CS&Cよりちょっと格上)に、Philip Reitering氏就任。同氏は、2009年6月、NCSCのトップも兼任。

・2009年2月、Obama大統領はMerissa Hathawayに60日レビューを実施、4月報告、5月発表。2009年8月辞任。

NYだより2004年12月号参照。また、http://e-public.nttdata.co.jp/f/repo/452_u0702/u0702.aspx

³³ 例えば、以下のGAOの報告。

GAO-08-1157T, September 16, 2008: **Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities**

GAO-08-588, July 31, 2008: **Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability**

³⁴ 例えば、NYだより2009年3月号参照。

³⁵ <http://openocrs.com/document/R4027/>

³⁶ <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html>

³⁷ http://www.nextgov.com/nextgov/ng_20080801_9053.php

具体的に、12分野としては、Trusted Internet Computing, Intrusion detection, Intrusion prevention, R&D, Situational awareness, Cyber counter intelligence, Classified network security, Cyber education and training, Implementation of information security technologies, Deterrence strategies, Global supply chain security, Public/private collaboration が報道されている。

が設置されており、2008年3月には、そのトップにシリコンバレーの企業家のRod Beckstrom氏を任命している³⁸。また、DHSにおいては、CNCIに基づいて、以下のようなサイバーセキュリティ対策に取り組んでいるとしている。

CNCIに関するDHSにおける対応（2008年4月時点³⁹）

項目	概要
US-CERTの人員拡充	US-CERTは、官民連携による、連邦政府のインターネットインフラの監視・警告センター。（.govを対象）
EINSTEINプログラムの拡充	全ての連邦省庁へ対象。連邦政府の職員に対し、状況把握のための早期警戒システム、悪意ある活動の早期明確化、包括的なネットワーク防衛を提供するもの。
外部接続の統合	OMBのTrusted Internet Connection Initiativeの一環として実施。連邦政府の外部インターネット接続ポイントを統合する。（.gov対象。）
National Cyber Security Centerの創設	連邦政府の他のサイバーセキュリティ組織と連携し、連邦政府のネットワークに係るサイバーセキュリティの全体像を把握する。
National Cyber Investigative Joint Task Force（NCIJIF）の他省庁への拡充	FBIによって管轄され、サイバー脅威の捜査に係る複数省庁による調整、統合、情報共有。
サプライチェーン防衛の強化	IT・通信機器が、米国に輸入される前に捜査されることによる悪影響の低減。このため、連邦政府の調達におけるプロセスの見直し。
NIPPに基づく官民での情報共有	NIPPの枠組みによる官民での連携。例えば、DHSは制御システムに係る脆弱性評価ツールを作成。
Cyber Storm IIの実施	官民の参加によるサイバーセキュリティに係る模擬試験の実施。
サイバー教育の拡充	連邦政府職員のための官民連携によるサイバー教育の拡充。
連邦のIT予算の拡充	2009年予算要求において、72億ドル要求（前年は66億ドル） ⁴⁰ 。

③ 米国連邦政府におけるサイバーセキュリティに係る主要な組織

上述のとおり、ブッシュ政権下においては、DHSが、連邦政府のサイバーセキュリティ政策をまとめとなっているが、DHSは、サイバーセキュリティに係る知見を十分有さず、一方、連邦政府内では、国防総省（DOD）の特にNSAが、圧倒的な知見を有するとされる。

以下、米国連邦政府機関において、サイバー（情報）セキュリティに関係する主な機関について記述する。

³⁸ http://www.dhs.gov/xnews/releases/pr_1206047924712.shtm
<http://www.washingtonpost.com/wp-dyn/content/article/2008/03/19/AR2008031903354.html>

³⁹ http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm
 なお、2009年6月時点については、以下を参照。（大きくは変化していない。）

http://www.dhs.gov/files/programs/gc_1234200709381.shtm
⁴⁰ http://www.usatoday.com/news/washington/2008-03-13-cybersecurity_N.htm

米国連邦政府における主要なサイバーセキュリティ関連組織

担当分野	組織	概要
国防	DOD/NSA (National Security Agency) ⁴¹	<ul style="list-style-type: none"> ・米国の暗号解析機関であり、具体的には、米国の（国防用の）情報インフラの保護を目的とした情報アシュアランス（Information Assurance）と、外国からの各種信号情報の収集・分析（Signals Intelligence：SIGINT）を主要ミッションとする。 ・メリーランド州の Fort Meade に本部を置く。
諜報	ODNI ⁴² (Office of Director of National Intelligence)	<ul style="list-style-type: none"> ・2004年の Intelligence Reform and Terrorism Prevention Act によって設立された、Intelligence Community（諜報機関）のとりまとめ機関。Defense Intelligence Agency, NSA, CIA, FBI, DHS の Office of Intelligence and Analysis などが主要メンバー。 ・大統領や NSC（National Security Council）に諜報関連の報告を行うことになる。
連邦政府（一般） 民間インフラ	DHS (NCSD、NCSC 等)	<ul style="list-style-type: none"> ・National Protection and Programs Directorate（NPPD）⁴³内の Office of Cyber Security and Communications の下の、National Cyber Security Division（NCSD）⁴⁴では、National Cyber Alert System、US-CERT の運用、Cyber Exercises、普及啓発月間等を実施。 ・NPPD 内の、Office of Infrastructure Protection では、2003年の PDD63 に基づき、重要インフラ保護対策（ITセキュリティ対策を含む）を、各所管省庁、関連業界等と連携しつつ、実施。 ・CNCI に基づき、2008年3月、National Cyber Security Center（NCSC）を設置⁴⁵。直接、NSA、FBI、DOD などとも連携しつつ、直接長官に報告する立場。 ・その他、Science and Technology Directorate のもとに、2004年、Cyber Security R&D Center を設立（SRI が運営）⁴⁶。
連邦政府（一般：情報セキュリティ）	OMB NIST	<ul style="list-style-type: none"> ・OMB は、2002年電子政府（e-gov）法に基づき、情報セキュリティを含む連邦政府の IT システム全体について管轄。 ・2002年連邦情報セキュリティマネジメント法（FISMA：Federal Information Security Management Act）により、各省庁は、DOC の NIST（国立標準技術研究所）が作成したガイドライン等に基づき、情報セキュリティ対策をとることが義務付けられている。

DHS におけるサイバーセキュリティ関連の組織の位置づけ⁴⁷

⁴¹ http://www.nsa.gov/home_html.cfm

⁴² <http://www.dni.gov/>、<http://www.dni.gov/overview.pdf>

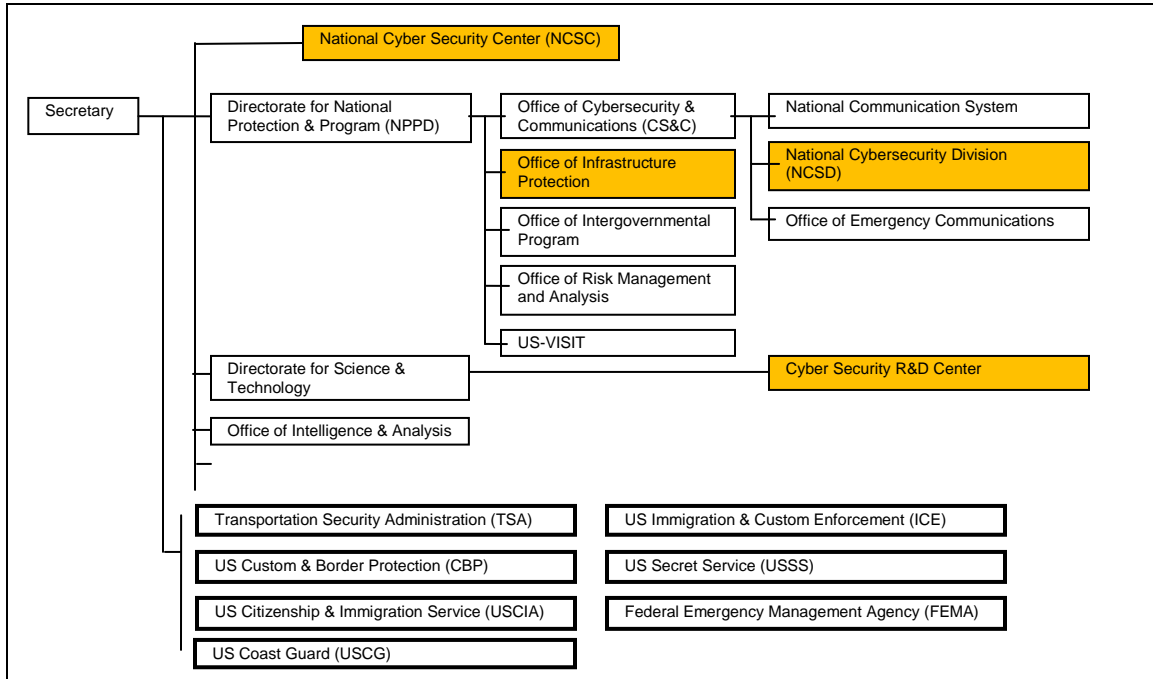
⁴³ http://www.dhs.gov/xabout/structure/editorial_0794.shtm

⁴⁴ http://www.dhs.gov/xabout/structure/editorial_0839.shtm

⁴⁵ http://www.dhs.gov/xprevprot/programs/gc_1234200709381.shtm

⁴⁶ <http://www.cyber.st.dhs.gov/>

⁴⁷ 出典：http://www.dhs.gov/xabout/structure/editorial_0644.shtm 等より作成。（色印がサイバーセキュリティ関連の組織）



(2) オバマ政権の選挙公約とサイバーセキュリティ政策レビュー

オバマ大統領は、公約段階からサイバーセキュリティの強化を謳うとともに、就任直後から政策のレビューを開始したものの、その後ホワイトハウス主導の政策立案・実施は停滞している。

① オバマ大統領の選挙公約

オバマ大統領は、選挙時から、サイバーセキュリティを連邦政府のトッププライオリティと位置付け⁴⁸、大統領に直接報告する立場で、各省庁の取り組みを調整し、国家のサイバー政策を立案する権限を有する「国家サイバーアドバイザー（National Cyber Adviser）」を設置することを公約としていた⁴⁹。

実際に、2009年1月21日にホワイトハウスが発表した Homeland Security に係るアジェンダ⁵⁰においてあげられた、6項目からなる情報セキュリティに係る項目の中でも、サイバーインフラは戦略的資産であると宣言するとともに、ホワイトハウスによるリーダーシップの強化を同項目の一番にあげている。

⁴⁸ <http://media.washingtonpost.com/wp-dyn/content/article/2008/07/16/AR2008071601474.html>

⁴⁹ http://www.barackobama.com/2008/07/16/fact_sheet_obamas_new_plan_to.php

⁵⁰ http://www.whitehouse.gov/agenda/homeland_security/

情報セキュリティ政策に係るアジェンダの概要（国土安全保障政策より抜粋）⁵¹

④ 情報ネットワークの保護
<ul style="list-style-type: none"> • サイバーセキュリティに係る連邦政府のリーダーシップの確保（サイバーインフラを戦略資産と宣言、National Cyber Adviser の設置） • 安全なコンピューティング研究開発の取り組みの開始と国家のサイバーインフラの強固化 • 米国経済を安全にする IT インフラの保護 • 企業に対するサイバースパイの防止 • 犯罪利益に係る機会を最小にするためのサイバー犯罪に係る戦略の策定 • 個人情報保護に係る強制基準の策定と、個人情報流出に係る企業の開示義務

なお、民間企業から見たオバマ政権のサイバーセキュリティのあり方については、例えば、国防や国際問題に係るシンクタンクである Center for Strategic and International Studies（CSIS）は、2008年12月8日、オバマ政権におけるサイバーセキュリティ政策に関する提言集である『Securing Cyberspace for the 44th Presidency』を発表している⁵²。同執筆者は、上記オバマ大統領の取り組み姿勢を評価している。

② サイバーセキュリティ政策レビュー

<60日間のレビューの開始>

オバマ政権は、同政権発足後、すぐにサイバーセキュリティ政策の見直しを開始した。具体的には、2009年2月9日、オバマ政権は、連邦政府内のサイバーセキュリティについて、60日間のレビューを行うことを発表した⁵³。このレビューは、ODNIのCyber Coordination Executiveを務めていたMelissa Hathaway氏が、期間中、ホワイトハウス内のSenior Director for Cyberspace 代行として、取り組むことになった。

同氏は、その後、上記のレビューを行うため、多くの利害関係者等へのヒアリングを実施しているが、この時期、サイバーセキュリティへの高い関心の中で、議会での法案策定の動き⁵⁴と合わせて、後述のNSA、国防総省を巡る動きも含めて、サイバーセキュリティに係る議論が活発化した。

⁵¹ http://www.barackobama.com/issues/homeland_security/index.php

⁵² http://csis.org/files/media/csispubs/081208_securingcyberspace_44.pdf

<http://www.washingtonpost.com/wp-dyn/content/article/2008/12/08/AR2008120801944.html>

<http://www.computerworld.jp/news/trd/133129.html>

http://news.cnet.com/8301-1009_3-10148263-83.html?part=rss&subj=news&tag=2547-1_3-0-20

<http://japan.cnet.com/news/media/story/0,2000056023,20386954,00.htm>

⁵³ <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/09/AR2009020903222.html>

http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/

⁵⁴ 具体的には、例えば、以下の通り。

・2009年3月11日、米国下院サイバーセキュリティ小委員会委員長は、サイバーセキュリティ法の必要性を指摘し、ヒアリングを開始。

<http://www.computerworld.jp/topics/gov/138169.html>

<http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=215801708>

なお、このレビューの結果は、2009年4月17日には、ホワイトハウスに提出されたと発表されている⁵⁵。

<レビューの公表>

このレビューを踏まえて、ホワイトハウスは、2009年5月29日付けで、「Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communication Infrastructure」という報告書を発表した⁵⁶。

本発表に際し、オバマ大統領は、サイバーセキュリティを、経済繁栄、安全保障の基盤であると明確に位置付けたことが特徴である⁵⁷。その上で、公約通り、組織面については、国家のサイバーセキュリティ政策・活動の調整に責任を有する担当者（Cyber Security Coordinator）を新設することを発表した。その際、同担当者は、ホワイトハウスの国家安全保障会議（NSC）と国家経済会議（NEC）⁵⁸のスタッフも兼務とするとともに、また、NSC内に省庁間でのサイバーセキュリティ関連の戦略・政策を調整するための担当部局も設置することとしている。

・Rockfeller 上院議員は、2009年3月20日、法案作成、4月1日提出。具体的には、Office of National Cybersecurity Adviser、Cybersecurity Advisory Panel、情報共有のための Clearinghouse の設置、NIST によるサイバーセキュリティ標準等の設置。4年毎にサイバーセキュリティプログラムの見直し、など。
http://news.cnet.com/8301-13578_3-10200710-38.html
http://news.cnet.com/8301-13578_3-10209406-38.html

・また、他の議員（Carper 上院議員）も、2009年4月30日、FISMA の改定法案提出。具体的には、「U.S. Information and Communications Enhancement Act」で、FISMA をアップデートするもの。National Office of Cyberspace の設立。（他の法案と同じ。）

<http://www.informationweek.com/news/government/technology/showArticle.jhtml?articleID=217201046>

⁵⁵ http://www.whitehouse.gov/the_press_office/Statement-by-the-Pres-Secretary-on-Conclusion-of-the-Cyberspace-Review/

⁵⁶ <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/29/AR2009052900350.html>

<http://www.nytimes.com/2009/05/30/us/politics/30cyber.html>

<http://online.wsj.com/article/SB124362745408767285.html>

http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

http://www.whitehouse.gov/the_press_office/Cybersecurity-event-fact-sheet-and-expected-attendees/、<http://www.whitehouse.gov/CyberReview/>

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

⁵⁷ オバマ大統領は、「サイバー空間は我々が日々の生活に必要な不可欠なものとなっているのが現実であるとの認識を、各種事例を挙げて示した上で、サイバーセキュリティは、米国の 21 世紀の経済的な繁栄及び国家安全保障の確保の前提となるものとして位置づけられる」とした。

⁵⁸ 当初は、National Security Council (NSC) のみの管轄であったのが、National Economic Council (NEC) との兼任となった背景に関し、2009年5月1日付けの WSJ は、ホワイトハウス内でも、権限争いを生じていると報道されている。具体的には、NEC の Summers 氏は、サイバーセキュリティの管轄は、Red Tape にならないよう、また、経済回復に影響を与えないようチェックする観点から、NSC だけでなく、NEC も所管し、引率すべきと主張したとされる。

<http://online.wsj.com/article/SB124113159891774733.html>

また、その上で、オバマ大統領は、ホワイトハウスにおける上記担当者⁵⁹の設置に加えて、今後の取り組みの方向として、以下の5点を上げている。

サイバースペースレビューの発表にあたってのオバマ大統領のポイント

- | |
|--|
| <ul style="list-style-type: none"> ① 新たな包括的なサイバーセキュリティ戦略を確立すること。同戦略は、先日指名を発表した、最高技術責任者（CTO）と最高情報責任者（CIO）と連携して策定する。 ② 将来のサイバーセキュリティ事案に対して、組織的、統一的に対応するために、州・地方政府、民間企業等と協力して対応すること。 ③ これらのインフラの大半は民間企業が有していることを踏まえ、官民連携を強化すること。ただし、民間企業に対して、セキュリティ標準を強制することはない。 ④ 最先端の研究開発に投資をし続けること。 ⑤ サイバーセキュリティに係る普及啓発活動を開始すること。 |
|--|

ただし、Cyber Security Cordinator を設置し、サイバーセキュリティ政策の取りまとめを DHS からホワイトハウスに移管し直すということ自体は、規定路線であり、また、戦略自体は、必ずしも目新しいものではなく、今後、これらの課題を実際にどう執行するかが鍵となるとの意見も多くなされた。

③ その後の動きと Cyber Security Cordinator（Howard Schmidt 氏）の就任

<Hathaway 氏の辞任と Cordinator の不在>

しかしながら、レビュー終了後、報告書の発表までに多くの時間を要したことに加え、報告書発表後（2009年5月末以降）も、上記報告書に記載された Cyber Security Cordinator はなかなか任命されず、ホワイトハウス主導のサイバーセキュリティ政策は、足踏みをすることになる。

⁵⁹ なお、同報告書においては、当面の具体的な課題としては、以下の10点をあげている。

- ① 国家のサイバーセキュリティ政策・活動の調整に責任を有する担当者の指名。当該担当者の元での省庁間でのサイバーセキュリティ関連の戦略・政策を調整するための、強力な国家安全保障会議（NSC）担当部局の設置。当該担当者は、NSC と国家経済会議（NSE）を兼務。
- ② 情報・通信インフラの安全を確保するための国家戦略の見直し。
- ③ サイバーセキュリティを、大統領のマネージメント優先事項の一つとして位置付けるとともに、パフォーマンスの評価手法の確立。
- ④ NSC 内のサイバーセキュリティ部局において、プライバシー・市民自由権担当者を指名。
- ⑤ サイバーセキュリティ関連の優先課題に係る省庁横断的な法的分析を実施するために必要な、適切な省庁横断的なメカニズムの構築。
- ⑥ サイバーセキュリティを促進する国家的な啓発活動や教育キャンペーンの開始。
- ⑦ 国際的なサイバーセキュリティに係る枠組みでの米国政府の位置付けの強化と、各種イニシアティブを実施するための国際的なパートナーシップの強化。
- ⑧ サイバーセキュリティ事案に対する対応計画の準備、官民パートナーシップ強化を図るための対話の開始。
- ⑨ 他の大統領行政府との連携のもと、サイバーセキュリティに係る研究開発戦略の枠組みの策定。
- ⑩ サイバーセキュリティに基づく ID マネージメントに係るビジョンと戦略の構築。

なお、その間、同職の代行を務めていた Melissa Hathaway 氏は、2009年8月3日、もう十分仕事を行ったとして、同職を辞任することを発表⁶⁰しており、その後、Cyber Security Coordinatorになる適切な人材がそもそもいないのではなどの報道が繰り返しなされている⁶¹。

<OMB (CIO) /NIST等の動き>

一方、ホワイトハウスにおいては、連邦CIO(OMB所属)のVivek Kundra氏が、同氏の担当である、連邦政府における情報セキュリティ政策の観点から、FISMAが実際の各省庁のセキュリティ強化につながっていないとの認識⁶²を踏まえて、就任以降これまでの施策の見直しに着実に取り組んでいる。

具体的には、政府説明責任局(GAO)は、2009年7月に、「連邦政府の情報セキュリティについては、コンプライアンスを強化したとの報告がなされているが、実際に、各省庁のセキュリティ管理強化につながっていない」との指摘を内容とする報告書⁶³を発表しているが、この本報告のドラフトに対して、Vivek Kundra氏

⁶⁰ <http://online.wsj.com/article/SB124932480886002237.html>

<http://journal.mycom.co.jp/news/2009/08/05/071/>

⁶¹ http://www.computerworld.com/s/article/9136306/The_cybersecurity_job_no_one_really_wants
<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221400243>

なお、Melissa Hathaway氏の辞任後は、Chris Painter氏(FBIからの出向)が、暫定的にCoordinator的な役割を努めている。

⁶² <http://govconexecutive.com/2009/05/vivek-kundra-fisma-does-not-meet-federal-security-needs/>

⁶³ http://www.computerworld.com/s/article/9135733/OMB_eyes_new_metrics_for_security_at_federal_agencies?taxonomyId=82

<http://www.gao.gov/new.items/d09546.pdf>

なお、GAOは、連邦政府の情報セキュリティに関して、ほぼ毎年以上の報告書を発表している。例えば、毎年主な報告は、以下の通り。(<http://www.gao.gov/docsearch/pastweek.html> より検索。なお、これら以外に、個別の省庁・機関や、個別課題に係る報告書も含めて、情報セキュリティ、サイバーセキュリティにかかわる報告書は多数ある。)

GAO-10-159T, October 29, 2009: **Information Security**: Concerted Effort Needed to Improve Federal Performance Measures

GAO-09-546, July 17, 2009: **Information Security**: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses

GAO-09-661T, May 5, 2009: **Information Security**: Cyber Threats and Vulnerabilities Place Federal Systems at Risk

GAO-08-571T, March 12, 2008: **Information Security**: Progress Reported, but Weaknesses at Federal Agencies Persist

GAO-07-837, July 27, 2007: **Information Security**: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses

GAO-07-751T, April 19, 2007: **Information Security**: Persistent Weaknesses Highlight Need for Further Improvement

GAO-06-527T, March 16, 2006: **Information Security**: Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

GAO-05-552, July 15, 2005: **Information Security**: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements

は、既に、各省庁による報告の評価基準（Metrics）を見直しすべく、各省庁の CIO や NIST とともに連携を進めているとするとともに、報告書の形式を全てインターネットベースで行うようにするとのコメントを提出している。

その後、実際に、OMB は、2009年8月には、FISMA に基づく各省庁から OMB への報告は全てオンライン（Web ベース）で提出するよう変更する⁶⁴とともに、NIST は、OMB との連携のもと、2009年11月、これまでのコンプライアンス中心の評価基準を変更すべく⁶⁵、連邦政府の IT システムのセキュリティ認証と認可に関するガイドラインである SP800-37 の改正案のドラフトを提示している⁶⁶。また、この直前の2009年8月、NIST は、連邦政府の情報セキュリティ管理策の基本に係る SP800-53 の改正版（Rev3）の最終版を発表している⁶⁷⁶⁸

また、レビュー開始以降現時点までの間、DOD・NSA や、DHS などの各省庁においては、独自に、サイバーセキュリティに係る取り組みを積極的に進めている（第4章参照）。

<Cyber Security Coordinator の任命>

このようにホワイトハウスにおける任命が待たれる中、報告書発表後約7カ月後の2009年12月22日、ようやく、Howard A. Schmidt が Cyber Security Coordinator として指名された⁶⁹。同氏は、ブッシュ政権時代において、Critical Infrastructure Protection Board の副議長、サイバースペースセキュリティの特別アドバイザーをしていたベテランである⁷⁰。なお、報道によると、彼は、当初想定されていた NSC と NEC の両方に報告する立場ではなく、NSC のみに報告する立場となっている。

Howard Schmidt 氏は、2010年1月から、実際にホワイトハウスでの活動を開始しているが、最近の主だった動きとしては、2010年3月2日、同氏は、民間の

⁶⁴ <http://www.fiercegovernmentit.com/story/agencies-must-submit-fisma-reports-online/2009-08-25>

⁶⁵ http://www.nextgov.com/nextgov/ng_20091214_7738.php

⁶⁶ <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=22190072>
2 同案は、2010年2月の最終版発行。

<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

⁶⁷ <http://www.physorg.com/wire-news/10767054/nist-releases-final-version-of-new-cybersecurity-recommendations.html>

<http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

なお、本版は、DOD、諜報当局等とも連携して作った初めてのもの。（3年間協力して作られた。）

⁶⁸ なお、FISMA に基づく、NIST の各種ガイドラインは、以下を参照。

<http://www.ipa.go.jp/security/publications/nist/>

<http://csrc.nist.gov/publications/PubsSPs.html>

⁶⁹ <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator>

<http://www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122201429.html>

<http://www.nytimes.com/2009/12/22/technology/internet/22cyber.html>

⁷⁰ 当時、Information Security Forum（在ロンドンの NPO）の CEO。以前においては、eBay の CISO、Microsoft の CSO を努める。空軍、陸軍でのセキュリティ対策、FBI での Forensics の経験もあり。

会議において、これまで機密とされてきたブッシュ政権の策定したイニシアティブである CNCI について、その一部を公表する方針を発表している⁷¹。

4. DOD/DHS における動きとサイバー戦争に向けた対応の動き

ホワイトハウス主導のサイバーセキュリティへの取り組みが停滞する一方、連邦政府等へのサイバー攻撃が大きな問題となる中、国防総省（DOD）及び国土安全保障省（DHS）は、サイバー戦争（Cyber Warfare）に向けた対応も含めて、独自にサイバーセキュリティ政策の強化を着実に図りつつある。

（1）NSA との連携を含む DHS を巡る動向

一般（非国防・民生用）政府のネットワークインフラの保護に関しては、一時期、現在担当する DHS ではなく NSA の機能を強化しようとする議論があったものの、その後は、DHS は、再度 NSA との連携を進めつつも、サイバーセキュリティ人材の抜本的拡充を図り、その能力を強化しようとする方向にある。

① NSA と DHS との連携の状況／NSA の機能強化の動き

<NSA と DHS の関係の状況>

前述の通り、ブッシュ政権の CNCI においては、NSA によるネットワークへの侵入等のモニタリング（盗聴等）能力等を強化するとともに、新たに設置した DHS/NCSC を通じて、DHS が、一般（非国防、民生用）政府関連のネットワークインフラの保護の取り組みを行うことを支援するとしている。

これらに係る、その後の具体的な状況としては、以下の話が報じられている。

- ・ **Einstein 3** : 2009 年 4 月 17 日の WP によると⁷²、関係者の話として、NSA は、国防に係るネットワーク保護技術（Einstein3）を、民生用の政府ネットワークの保護に利用すべく、DHS に出向した NSA の従業員が、民生用政府ネットワークに侵入する悪意あるコードを探知するセンサー技術をインターネットの中に送り込むソフトウェアを試験したとしている⁷³。
- ・ **NSA の主導** : 1 年前に NCSC のトップについた Beckstrom 氏は、2009 年 3 月 5 日、連邦政府のサイバーセキュリティ政策は NSA に牛耳られている

⁷¹ <http://www.nytimes.com/2010/03/02/science/02cyber.html>

<http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030202113.html>

⁷² <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/16/AR2009041604291.html>

⁷³ なお、本試験は機密扱い。なお、Einstein プログラムについては、以下を参照。

[http://en.wikipedia.org/wiki/Einstein_\(US-CERT_program\)](http://en.wikipedia.org/wiki/Einstein_(US-CERT_program))

との批判をして、同職を辞任している⁷⁴。同氏によると、彼のオフィスは、過去1年間においてたった5週間分の資金と5人の職員しか割り当てられなかったとしている。

<NSAの機能強化の動きとプライバシーに係る批判>

このような中、特にサイバーレビューにおいてサイバーセキュリティの体制が検討されている時期において、NSA側において、(国防だけでなく)民生用の政府系ネットワークの保護にまで権限を与えるべきとの発言があり、波紋を広げた⁷⁵。

なお、この時期、2009年4月10日、安全保障関連の高官の話として、(DHSの管轄する)米国の電力網が中国またはロシアのスパイによって侵入されたとの報道が大きくなされている⁷⁶。なお、本件の探知は、電力企業ではなく、米国の諜報機関によってなされたものであり、侵入にあたってインフラを破壊することのできるソフトウェアが残されていたとしている。

一方で、このようなNSAへの権限強化については、NSAの権限が強大化しすぎることに対する懸念⁷⁷に加え、市民の権限やプライバシー侵害の観点から、批判を浴びることになる(2009年4月16日付のNYT⁷⁸参照)。

特に、(CNCIに基づき)議会が2008年に設定した広大な権限を越えて、NSAが、外国の諜報活動と併せて、米国人の電話や電子メールを盗聴したことが2009年4月15日報じられ、議会関係者、市民団体から批判を浴び、問題になった⁷⁹。

⁷⁴ <http://online.wsj.com/article/SB123638468860758145.html>
<http://www.washingtonpost.com/wp-dyn/content/article/2009/03/09/AR2009030901213.html>
<http://www.computerworld.jp/topics/gov/138129.html>

⁷⁵具体的には、2009年2月26日、国家情報長官(Director of National Intelligence)のDennis Blair氏は、議会において、NSAは、国防用と政府のネットワークの保護に係る権限を有するのに適していると発言。NSAはサイバーセキュリティに係る有能な人材を多く有しており、この能力は国防・諜報用だけではなく、連邦政府全体あるいは重要インフラに拡大していくべきとしている。

<http://cyberstrategies.wordpress.com/2009/02/28/nsa-should-oversee-cybersecurity-intel-chief-says/>

なお、NSA長官(Director)のKeith Alexander氏は、2009年3月半ばに、スタンフォード大学で開催されたコンファレンスでの演説で、

- ・NSAは国防ネットワークのみを担当とするつもりであり、一般政府はDHSが担当すべき
- ・NSAは政府のネットワーク保護にしか関心がなく、そのためには、NSAの能力を利用して、政府のネットワークに侵入しようとするサイバー脅威を探知するために利用することが必要、と述べている。

<http://www.washingtonpost.com/wp-dyn/content/article/2009/04/16/AR2009041604291.html>

<https://365.rsaconference.com/blogs/tim-mather/2009/03>

⁷⁶ <http://online.wsj.com/article/SB123914805204099085.html>

<http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040803904.html>

http://news.cnet.com/8301-1009_3-10216702-83.html

<http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=216403524>

⁷⁷前述のDHS/NCSCを辞任したBeckstrom氏は、NSAが政府の従業員の全ての電子メール、テキストメッセージ、検索を収集・分析する能力を有すること、また、一つの機関に巨大な権力が集中することを懸念すると述べている。<http://www.nytimes.com/2009/04/17/us/politics/17cyber.html>

⁷⁸ <http://www.nytimes.com/2009/04/17/us/politics/17cyber.html>

また、プライバシー擁護団体である CDT (Center for Democracy and Technology) は、2009年4月15日、当時計画中のサイバーセキュリティ政策に関して、プライバシーと透明性の観点から (DHS から権限を剥奪することはともかく)、NSA には権限を与えるべきではないとしている⁸⁰。

このような中、NSA 長官 (Keith Alexander 氏) は、2009年4月21日、民間のコンファレンスの中で、NSA は、国防用のネットワークに対するサービスの提供は行うが、民生用のサイバーセキュリティの運営を行うつもりはないと再度発言している⁸¹。

② DHS における体制強化の動き

<DHS 内の体制強化の動きと最近の NSA との関係>

その後、前述の通り、サイバーレビューの結果、サイバーセキュリティに係るとりまとめ体制に関しては、ホワイトハウスに Coordinator を設置するとともにその機能を強化⁸²することとなった。しかしながら、これまでとりまとめであった DHS 内の体制を今後どうするかについては、全く触れていない⁸³。

このような中、DHS においては、DHS の機能は従来どおり引き続き残るとのホワイトハウスの指示のもと⁸⁴、DHS 内部のサイバーセキュリティに係る体制の統合を図っている。具体的には、以下の通り⁸⁵。

- ・ DHS は、2009年6月2日、National Cyber Security Center (NCSC) のヘッドに、2009年3月に新たに任命していた NPPD の Philip Reitering 氏 (Deputy undersecretary) を兼任として任命し⁸⁶、両者の権限を統合。

⁷⁹ <http://www.nytimes.com/2009/04/16/us/16nsa.html>

これに対して、4月16日、国家情報長官 (Director of National Intelligence) の Dennis Blair 氏は、盗聴は安全保障にとって必要不可欠だとしつつ、誤って米国内の盗聴を一部行ってしまった (また、その割合は少ない) と釈明している。

⁸⁰ <http://www.computerworld.jp/topics/gov/142509.html>

⁸¹ http://news.cnet.com/8301-13578_3-10224579-38.html

⁸² ホワイトハウスは、上記レビュー報告書の発表直前の5月25日に、ホワイトハウスの Homeland Security に係る体制の見直しを発表している。この中で、サイバーセキュリティについては、ホワイトハウス内の National Security Staff 内で新たな Directorate と Position を作り、機能強化を図るとしている。

http://www.whitehouse.gov/the_press_office/Statement-by-the-President-on-the-White-House-Organization-for-Homeland-Security-and-Counterterrorism/

<http://www.washingtonpost.com/wp-dyn/content/article/2009/05/25/AR2009052502104.html>

<http://www.informationweek.com/news/government/federal/showArticle.jhtml?articleID=217700171>

⁸³ なお、CSIS の報告書においては、NCSC を、ホワイトハウスに移行すべきと提言していた。

⁸⁴ これに関し、2009年6月3日、DHS の NPPD の Undersecretary は、Cyber security Coordinator 設立後も、DHS の機能は引き続き残ると、ホワイトハウスの John Brennan 氏から指示があったとしている

<http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=217701655>

⁸⁵ なお、それに加えて、2009年6月、DHS のアドバイザーの一人に、ハッカーを新たに任命したことが話題になっている。http://news.cnet.com/8301-1009_3-10258634-83.html

- ・ DHS は、2009年10月30日に、NCCIC（National Cybersecurity and Communication Integration Center）をオープン⁸⁷。同センターはUS-CERTと、National Communication Systems 内の NCC（National Coordination Center for Telecommunications）を統合するものであり、また NCSC の成果も統合する。

実際に、DHS の Napolitano 長官は、2009年8月4日、民間コンファレンスにおいて、当初就任したときは、DHS のサイバーセキュリティ体制は全く組織化されていなかったと発言している⁸⁸。

一方で、最近の NSA との関係では、2010年3月4日、DHS の高官（Greg Schaffer 氏）は⁸⁹、CNET 誌のインタビューにおいて、EINSTEIN を、重要インフラに延長できるかどうか検討中としており、今後インターネットのセキュリティ確保に向けて NSA と DHS との連携強化の方向性を示している。

<DHS におけるサイバー人材の雇用強化と連邦政府全体の動き>

連邦政府に対するサイバー攻撃の増大に対応し、対策を図るためには、セキュリティ人材を如何に確保するかが重要であり、特にサイバーセキュリティの能力が弱いとされるDHSにおいては、クリティカルである。

このような中、DHSは、2009年10月1日、サイバーセキュリティ普及啓発月間に際して、サイバーセキュリティの専門家を大幅に採用すると発表した⁹⁰。この採用計画は、DHSとOPM（Office of Personal Management）、OMBの合意によるもので、具体的には、今後3年間にわたって最大1,000名を採用する権限を得ている⁹¹。

一方で、セキュリティ関連人材は、DHSだけでなく、連邦政府各省庁においても不足している。例えば、最近の連邦政府のセキュリティマネージャーに対するアンケート調査の結果（2010年3月発表⁹²）では、約8割がセキュリティ人材を見

⁸⁶ <http://www.informationweek.com/news/government/federal/showArticle.jhtml?articleID=217701278>

⁸⁷ http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm

⁸⁸ http://www.nextgov.com/nextgov/ng_20090805_9634.php

その上で、同氏は、引き続き、DOD は.milを、DHS は、.govに加えて、民間(.org 及び.com)のインターネットインフラの保護に責任を有するとしている。

⁸⁹ http://news.cnet.com/8301-13578_3-10463665-38.html

⁹⁰ http://www.dhs.gov/ynews/releases/pr_1254411508194.shtm

http://voices.washingtonpost.com/securityfix/2009/10/dhs_seeking_1000_cyber_security.html

⁹¹ なお、人材とは異なるが、最近において、DHS は、2010年3月3日、個人または企業に対して、サイバーセキュリティに係る普及啓発を促すための競争資金 National Cybersecurity Awareness Campaign Challenge Competition を募集することを発表している。

<http://www.dhs.gov/files/cyber-awareness-campaign.shtm>

<http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=223101441>

⁹² 国際情報システムセキュリティ認証コンソーシアム((ISC)2)による調査。

つけるのに大変苦勞しているとしている。

このような中、民間団体においても、サイバーセキュリティの専門家を育成しようとする動きがある。具体的には、CSISとSANS Instituteは、2009年7月、連邦政府と連携し、サイバーセキュリティの専門家を10,000人育成すべく、US Cyber Challengeを立ち挙げている⁹³。

また、連邦議会においても、下院は、2010年2月4日、Cybersecurity Enhancement Act法案を圧倒的多数で可決した⁹⁴。同法案の多くはCybersecurity R&D Actを改正するものであるが、省庁ごとが必要とするサイバーセキュリティ労働力の評価を行うことや、将来的に連邦政府で働くことを前提にした大学生、大学院生に対するスカラーシップなどの項目が含まれている。

(2) DODにおけるサイバー司令部設立とサイバー戦争への対応に向けた動き

一方、連邦政府、特に国防関連のネットワークに対するサイバー攻撃が増大する中、DODにおいては、サイバー攻撃からの防御だけでなく、攻撃能力も強化することを目的に、NSAを中心にサイバー司令部(Cyber Command)を設立している。実際に、米国においては、サイバー戦争に向け、対応できる能力を確保すべきとの議論が、最近多くなされている。

① DODにおけるCyber Command設立に向けた動き

<DODにおけるサイバー攻撃の増大>

近年DODに対するサイバー攻撃は近年急増してきているされている。具体的には、DODのCISO(Chief Information Security Officer)は、2009年5月6日、議会での公聴会において⁹⁵、国防のネットワークへの侵入の試みが、2006年には6

<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=223101596>
回答者の56%が新たに見つけるのが困難、23%が非常に困難、としている。

⁹³ <http://csis.org/uscc>

なお、同US Cyber Challengeを報道しているUS Newsは、中国では軍が60,000人の”information troops”を訓練しているのに対し、米国では、DODでさえ年間たった80人しか訓練していないとしている。
<http://www.usnews.com/articles/news/national/2009/08/06/government-recruits-geeks-to-blunt-cybersecurity-threats.html>

なお、別の情報では、DODは2010年においては年間200人訓練する予定であり、一方、DHSは現在100人しか在籍していないとの報道もある。<http://online.wsj.com/article/SB124579956278644449.html>

⁹⁴ 同法案は、もともと2009年11月に提出された法案であり、主として、Cyber Security R&D Actを改正する法律案であるが、2010年1月、Googleのサイバー攻撃、議会のハッキング等を背景に採決された。

<http://thecaucus.blogs.nytimes.com/2010/02/04/house-passes-cybersecurity-bill/>

<http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.4061:>

⁹⁵ <http://online.wsj.com/article/SB124153427633287573.html>

なお、同様にDODの情報システムが脆弱であるという指摘は、3月17日にもなされている。

<http://www.washingtonpost.com/wp-dyn/content/article/2009/03/17/AR2009031702715.html>

百万件であったが、昨年（2008年）には、360百万件に増えているとしており、このため、被害から改修するための費用として、過去半年で100百万ドルを費やしたと証言している（その多くは、中国とロシアからではないかとしている）。

また、2009年4月21日、WSJは、事情に詳しい政府関係者の話として、次世代戦闘機であるF35の情報がハッキングされたことが報道され、大きな話題になるとともに、国防インフラにおけるサイバー攻撃からの防御の必要性の認識が高まっていた⁹⁶。なお、本攻撃は、前政府関係者の話によると、確定は困難であるものの、中国からのものとされ、また、Lockheed Martin等のコントラクターのネットワークの脆弱性を破って侵入したとされる。

<Cyber Command の設立>

上述のNSAの機能強化の議論が収束した直後、また、上記F35の報道の翌日の2009年4月22日、WSJは、DODは、DODのネットワークの保護に係る各機関の調整を行うとともに、サイバー戦争における米国の攻撃能力を強化するため、NSAを中心に新たな司令部（Cyber Command）を設置する計画であると報じた⁹⁷。

このCyber Commandのアイデアは、もともと、2008年秋⁹⁸、当時の国家情報長官（Director of National Intelligence）のMike McConnell氏⁹⁹がRobert Gates国防長官に宛てたレターに基づくものであるとされる¹⁰⁰。同氏は、DODにおけるサイバーセキュリティに係る取り組みが、NSAや情報システムを担当するDISA（Defense Information Systems Agency）などに分断されていることに問題視していたとされ、これを踏まえてGates長官は、当時ホワイトハウスによるレビューが終わったあとに、同Commandを設置する意向であると報道されている¹⁰¹。

⁹⁶ <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/21/AR2009042103938.html>
<http://online.wsj.com/article/SB124027491029837401.html>
http://news.cnet.com/8301-1009_3-10224637-83.html

⁹⁷ <http://online.wsj.com/article/SB124035738674441033.html>
<http://www.informationweek.com/news/government/technology/showArticle.jhtml?articleID=217000202> なお、同日付けのWPでも、国防総省の広報官は、サイバー攻撃に対応するための組織見直しについて確認している。

<http://www.washingtonpost.com/wp-dyn/content/article/2009/04/22/AR2009042202742.html>
<http://www.washingtonpost.com/wp-dyn/content/article/2009/04/22/AR2009042200029.html>

⁹⁸ なお、国防長官の諮問機関である国防科学評議委員会が、2008年11月4日に発表した報告書においても、サイバー戦争への対応の必要性について触れている。

<http://www.itmedia.co.jp/enterprise/articles/0811/07/news060.html>
http://www.ndia.org/Divisions/Divisions/SOLIC/Documents/SOLIC_DSB_DefenseImperatives_Nov2008.pdf

⁹⁹ 彼の前職は、NSA長官。

¹⁰⁰ <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/05/AR2009050504342.html>
<http://online.wsj.com/article/SB124035738674441033.html>

¹⁰¹ その後、5月5日には、NSA長官も、DODにCyber Command設置を検討していると発言したとの報道がなされている。なお、その際、同氏は、同Commandは、軍のコンピューターシステムの保護だけでは

このような中、2009年6月24日、国防総省（DOD）は、前日の6月23日にゲーツ国防長官が、サイバーセキュリティに焦点を当てた Subcommand である Cyber Command の設立に係るメモに署名したことを、正式に発表した¹⁰²。同発表によると、

- ・ 詳細はまだ公開されないが、新たな Cyber Command は、Strategic Command¹⁰³に報告する立場となる。
- ・ Gates 長官は、現在の NSA 長官（Director）である Keith B. Alexander 氏（現在3つ星ランク）を4つ星ランクにし、Cyber Command を指揮する責任を追加する予定。
- ・ 現在のところ、本部は、（NSA のある）Fort Maede, MD に設置する方向で検討中。

としている¹⁰⁴。なお、報道によると、Cyber Command は、2009年10月に活動を開始し、2010年10月から完全に活動を行う予定とされているが、詳細は明らかにされていない¹⁰⁵。

② サイバー戦争への対応に向けた動き

<サイバー戦争に係る認識の高まり（各種報告書等）>

このような流れの中で、1年ほど前より、サイバー戦争（Cyber War）関連の記事が大きく報道されるようになってきている。多くは、サイバー戦争に向けて米

なく、同 Command を通じて、NSA は、民生用のネットワークや電力網その他の重要インフラの保護を担う DHS を支援するとしている。

<http://www.washingtonpost.com/wp-dyn/content/article/2009/05/05/AR2009050504342.html>

また、その後も、オバマ大統領の報告書発表時においても、同 Cyber Command の話が報道されている。

<http://www.nytimes.com/2009/05/29/us/politics/29cyber.html>

なお、6月12日は、Cyber Command に関して、プライバシーの問題があると報道されている。

<http://www.nytimes.com/2009/06/13/us/politics/13cyber.html>

¹⁰² <http://www.defenselink.mil/news/newsarticle.aspx?id=54890>

<http://online.wsj.com/article/SB124579956278644449.html>

¹⁰³ 現在、国防総省の司令部（Command）には、地域別に6つの司令部（アフリカ、中央、欧州、太平洋、北部、南部）に加え、機能別に4つの司令部（Joint Force, Special Operations, Strategic Command, Transportation Command）がある。

¹⁰⁴ なお、この発表にあたって、本件は、国防のネットワークに係るもののみを対象とするものであり、サイバースペースを国防化するものでもなく、（DHS 責任下にある）民生用のネットワークに係る責任を乗っ取るものでもないことを強調している。

¹⁰⁵ <http://www.democracypartisan.org/2009/10/us-cyber-command-goes-online-.html>

なお、実際に、その後もいくつかの断片的な動きはあるが、正式な動きはほとんど公表されていない。

<http://www.thenewnewinternet.com/2009/10/05/navy-to-create-cyber-command/>

<http://uscybercom-watch.blogspot.com/2009/10/marine-consider-cyber-command.html>

<http://www.af.mil/news/story.asp?id=123186689>

国は体制を強化すべきとの論調ではあるが、サイバー戦争はいずれにせよニッチな部分にしか過ぎないとの意見もある¹⁰⁶。具体的は、以下の通り。

- ・ 2009年4月27日付けのNYT¹⁰⁷は、「サイバー戦争—サイバー兵器の競争の中で、米国の攻撃能力に対する疑念が増加」と題する記事を報道。
- ・ 同4月30日、National Academy of Scienceは、「Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities」とのレポートを発表¹⁰⁸。同レポートでは、米国はサイバー攻撃に対する明確な国防政策をもっておらず、攻撃能力も含めて、その明確化を図るべきとしている。
- ・ 2009年11月のMcAfeeの報告書¹⁰⁹は、特に、政治的な目的のためのサイバー攻撃が増加しており、特に、米国、ロシア、フランス、イスラエル、中国の5ヶ国において、「サイバー兵器」の軍拡競争が急速に進みつつあるとしており、サイバー戦争が現実のものとなりつつあるとしている。
- ・ 公共政策のシンクタンクのRAND Corpが、2009年10月に発表した空軍向けの報告書¹¹⁰では、実践的なサイバー戦争はニッチな位置づけにしか過ぎず、それ以上のものではないとして、サイバー戦争に重点を置くべきではないとしている。

また、特にサイバー攻撃の多くの起源であると見られている中国との関係に関し、2009年11月に発表された米中経済・安全保障レビュー委員会の報告書¹¹¹では、前年の報告書と比較しても¹¹²、中国のサイバースパイ、サイバー戦争の能力増強に対する脅威をより明確に指摘している。具体的には、以下の通り。

¹⁰⁶ なお、既に Cyber Warfare が行われたこともあるとの記事もある。

http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php

¹⁰⁷ <http://www.nytimes.com/2009/04/28/us/28cyber.html>

¹⁰⁸ <http://www.nytimes.com/2009/04/30/science/30cyber.html>

¹⁰⁹ http://newsroom.mcafee.com/article_display.cfm?article_id=3594

<http://japan.cnet.com/news/sec/story/0,2000056024,20403744,00.htm>

¹¹⁰ “Cyber Deterrence and Cybwe War”

http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=220600297>

¹¹¹ http://www.uscc.gov/pressreleases/2009/09_11_10pr.pdf

http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf

<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221900505>

http://news.cnet.com/8301-13639_3-10381621-42.html

<http://online.wsj.com/article/SB125616872684400273.html>

同報告書は、第1章：米中貿易・経済関係、第2章：米国の安全保障に直接的な影響を与えている中国の活動、第3章：アジアにおける中国のプレゼンス、第4章中国のメディアと情報情報統制、の4章立てとなっており、このうち、第2章の第4節「米国を攻撃対象とし、米国の国家安全保障に影響を与えている中国のサイバー活動について」において、中国のサイバー活動に関する報告がなされている。

¹¹² NYだより2009年3月号参照。

米中経済安全保障レビュー委員会報告書での中国のサイバー能力に係る記述¹¹³

- ・米国に対する悪意あるコンピューター上の活動量は、2008年に増加し、2009年は急増した。これらの大半は、中国を起源とするもののように思われる。
- ・ハッカーは、場所を隠しているため、それらの攻撃者の特定は困難であるが、状況及び鑑識の証拠によると、中国政府又は政府関連機関が関与していることが強く示唆される。
- ・中国政府は、人民解放軍の中においてコンピューター・ネットワーク運用（CNO）能力の組織化を行っている。また、人民解放軍はサイバー能力を強化するため、民間からも含めて技術的に能力ある人材を雇用しており、「情報戦闘軍」部隊に送り込んでいる。
- ・中国の平和時におけるコンピューター開拓能力は、主に米国、及び海外にいる中国の反体制派に対する諜報活動に焦点が当てられている。
- ・紛争の初期段階においては、人民解放軍は、対立する政府及び軍の情報システムに対するコンピューター・ネットワーク運用（CNO）を行うであろう。
- ・米国の重要インフラは、悪意あるサイバー活動に脆弱である。中国は軍のドクトリンにおいて、紛争時には、これらの脆弱性を活用するように求めている。

<今後のサイバー攻撃、戦争に向けた懸念の高まり>

このような中、米国に対するサイバー攻撃に係る事例については、上述の電力網に対するサイバースパイ侵入、次世代戦闘機 F35 の情報窃盗以外にも、現時点までに引き続き多くの報道がなされている¹¹⁴。また、それ以外にも、近年はインターネットサービス企業に対する攻撃も多く報道されており¹¹⁵、また、世界各国において、政治的なハッキング活動が広がってきていると報告もある¹¹⁶。

¹¹³ なお、本報告書に作成にあたって、Northrop Grumman 社は、2009年10月に、中国のサイバー戦闘能力について評価分析を行った報告書「Capability of People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation」を上記委員会に提出している。

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approve%20Report_16Oct2009.pdf

<http://jpress.ismedia.jp/articles/-/2705?page=3>

同報告書では、中国は情報戦争における優位性の拡大に向け、情報技術やコンピューター・ネットワークの包括的な近代化プログラムを進めており、これまでの陸海空における軍事活動に加え、サイバー空間においてもその能力向上を図っているとの問題意識の下、平時・戦時における中国のコンピューター・ネットワーク作戦（computer network operation: CNO）の遂行能力の評価結果を取りまとめられている。

¹¹⁴ 例えば、2009年7月：ホワイトハウス他政府機関、民間企業、韓国政府等に対する DDoS 攻撃。

<http://www.afpbb.com/article/environment-science-it/it/2619675/4347469>

www.google.com/hostednews/afp/article/ALeqM5hM1x-CC9vCIHGSq6RSvkKHZAz5sg

また、経済犯罪では、2009年夏、ロシアのハッカー組織が Citigroup 等の大手銀行から数千万ドルを盗難。（FBI が、2009年12月、捜査を開始）

<http://online.wsj.com/article/SB126145280820801177.html>

¹¹⁵ 例えば、以下の通り。

・2009年8月、Twitter, Facebook が DoS 攻撃により、一時アクセスできなくなった。これは、グルジアのプロガーを狙ったものと報道されている。<http://www.securityfocus.com/brief/992>

<http://www.networkworld.com/news/2009/080709-twitter-dos-attack-targeted-georgian.html>

・2010年10月、MS Hotmail, Google Gmail などのアカウント／パスワード情報が、Phishing により流出。被害は、3万件以上。http://news.cnet.com/8301-17939_109-10367348-2.html

http://news.cnet.com/8301-17939_109-10368361-2.html

実際、2010年に入ってから、米国におけるサイバー攻撃に対する脆弱性に対する報道、発表が多くなされている。その中でも、2010年1月にGoogleがサイバー攻撃を受けたとの発表は、民間企業が自ら積極的にその内容を公表したことに加え、中国における検閲問題（インターネットの自由）と中国でのビジネスの問題のあり方も含めて、大きな話題となっている（本件については、別途報告する）¹¹⁷。それ以外には、以下の通り。

- ・ ネットワークへの脅威の探知等を事業とする Netwitness 社は、2010年2月18日、大規模なハッキングの事例を発見したと発表した¹¹⁸。同発表によると、2500の組織における75,000のコンピューターが新たなタイプのボットによって感染しているとしており、18ヶ月にわたって、政府・民間における企業秘密・個人情報等が盗難された（75GB相当）としている。
- ・ 一方、超党派政策センター（Bipartisan Policy Center）は、2010年2月17日サイバー攻撃を受けた場合のシミュレーション（Cyber ShockWave）を実施したところ、現行の連邦政府の体制では、サイバーテロに対応できないことが判明したとの発表を行っている¹¹⁹。

このような中、米国連邦政府においては、最近、諜報当局を中心に、今後のサイバー攻撃への対応の喫緊の必要性を指摘する発言が相次いでいる。

- ・ 国家情報長官（Director of National Intelligence : DNI）の Dennis Blair 氏は、2010年2月2日、上院の公聴会において、今後6ヶ月以内に、アルカイダからの米国への大規模攻撃がありうると発言した¹²⁰。その際、同氏は、通信やコンピューター・ネットワークへの攻撃の脅威は非常に高まっておおり、“Cyber Pearl-Harbor”の可能性を指摘している。また、その上で、今回、Googleの件は、サイバー戦争への脅威を無視してきた人への wake-up call となるであろうとしている。

・2009年12月、Twitterのサイトがハッキングされ、「このサイトは Iranian Cyber Army に乗っ取られた」というサイトにリダイレクトされた。<http://www.cnn.com/2009/TECH/12/18/twitter.hacked/index.html>

¹¹⁶ <http://www.computerworld.jp/topics/vs/174310.html>
http://newsroom.mcafee.com/article_display.cfm?article_id=3621

¹¹⁷ ただし、本件については、サイバーセキュリティ関連当局からは、ほとんど正式なコメントがなされていない。

¹¹⁸ <http://www.netwitness.com/resources/pressreleases/feb182010.aspx>
<http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html>
<http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html>
<http://www.informationweek.com/news/services/data/showArticle.jhtml?articleID=223000140>

¹¹⁹ <http://www.bipartisanpolicy.org/news/press-releases/2010/02/cyber-shockwave-shows-us-unprepared-cyber-threats>、<http://www.bipartisanpolicy.org/events/cyber2010>

<http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html>
<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222900723>

¹²⁰ <http://www.nytimes.com/2010/02/03/us/politics/03intel.html>

- ・ 前 DNI 長官の Mike MicConnell 氏は、2010 年 2 月 28 日付けの WP に寄稿した記事の中で¹²¹、（Google の事例などに見られるように、）我々は既にサイバー戦争に負けているが、その上で、サイバーセキュリティ対策の強化の必要性を述べている。
- ・ FBI 長官の Robert Mueller 氏は、2010 年 3 月 4 日、民間のコンファレンスにおいて、サイバーテロは、既に現実のものとなりつつあり、また、急速に拡大しつつあると発言している¹²²。

なお、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的一切について、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。

¹²¹ <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>

¹²² <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html>