第八章　米国におけるサイバーセキュリティ政策

土屋大洋

はじめに

第一期バラック・オバマ政権は、成立当初からサイバーセキュリティ政策を重要な安全保障政策の一環としてきた。例えば、2009 年 5 月に「60 日レビュー」と呼ばれる報告書が出され、「サイバーセキュリティのリスクは、21 世紀の最も深刻な経済的・安全保障的挑戦」だと指摘された。2010 年には統合軍（STRATCOM）の下にサイバー軍（USCYBERCOM）が設置された。2010 年の「四年ごとの国防計画見直し（QDR）」ではサイバースペースが、陸、海、空、宇宙に続く第五の作戦空間として位置づけられた。そして、2012 年 6 月には、米国とイスラエルが共同でイランに対するサイバー攻撃を行っていたという報道がなされた[1]。セキュリティ（安全保障）を「攻撃」と「防衛」の両方を含むと解釈すれば、サイバー攻撃を国家が行うというサイバー戦争の局面に近づいてきていることが分かる。

冷戦の終結後、新たな安全保障上の懸念・脅威として「非伝統的安全保障」の重要性の高まりが指摘されてきたが、しかし、なぜオバマ政権になってから急速にサイバーセキュリティが非伝統的な安全保障政策の一つとして浮上してきたのかは必ずしも明らかではない[2]。本章では、第一に、国際的なサイバー攻撃の発生について検討し、第二に、米国のオバマ政権がこれにどう対応してきたか、そして、米国連邦議会がどう反応したのかを見ていきたい。オバマ政権はサイバー攻撃の脅威に対し積極的な対応をとっているが、議会は適切な法案を可決することができずにいる。

サイバーセキュリティは日本にとっても対岸の火事ではない。2011 年 9 月には日本の防衛産業を狙ったサイバー攻撃が明らかになり、米国の軍事機密が日本を通じて漏洩した可能性もある。リチャード・アーミテージ（Richard L. Armitage）とジョセフ・S・ナイ（Joseph S. Nye, Jr.）が 2012 年 8 月に米戦略国際問題研究所（CSIS）から発表した日米関係に関する報告書でも、サイバーセキュリティは「新しい安全保障戦略」の一つとして挙げられ、米国と日本の役割と旗幟を鮮明にする必要がある戦略的な分野だとされている[3]。

１．非伝統的安全保障としてのサイバーセキュリティ

軍隊がこれまで戦場としてきた陸、海、空、さらに宇宙が自然空間であるのに対して、サイバー空間はコンピュータと通信ネットワークによって作り出された人工的な空間である。したがって、それらを停止させれば究極的なサイバーセキュリティは可能になる。し

かし、軍事革命（RMA）とも呼ばれた装備のハイテク化を経た米軍では、コンピュータと通信ネットワークは不可欠の要素になっている。米国の装備の優位性を保つためにはサイバーセキュリティの確保が必要になる。

映画などの影響もあって、これまでサイバー攻撃の被害としては、飛行機の墜落やダムの破壊などがイメージされてきた。しかし、サイバー攻撃が本質的にこれまでと違う点は、攻撃があったことすら分からないようにする形で相手に被害を与えられることである。最も成功したスパイがその名を知られることがないように、成功したサイバー攻撃はその痕跡を残さないまま機密情報を盗んだり、相手のシステムにダメージを与えたりする。

パスワード破りなどによるウェブサイトの改ざんなどが原始的なサイバー攻撃だとすれば、近年のサイバー攻撃には大別して三つある。第一に、不特定多数のコンピュータをコンピュータ・ウイルスに感染させ、特定の日時にターゲットをめがけてアクセスさせるという分散型サービス拒否（DDoS）攻撃がある。第二に、標的となった人物やシステムに対してコンピュータ・ウイルスを密かに仕込んだ偽のメールを送りつけるなどして、システムを乗っ取ったり、その内容を盗み見たりする標的型電子メール攻撃（APT）がある。これは機密情報を盗むサイバー・エスピオナージ（スパイ活動）の一環となっている。

第三のタイプは、まだ事例はそれほど多くないが、通常兵器などの使用と組み合わせて行われるサイバー攻撃である。通常兵器による開戦と同時にサイバー攻撃を仕掛けて敵のシステムを不能にしたり、事前にサイバー攻撃を仕掛けて社会システムを麻痺・混乱させておいてから通常兵器による攻撃を仕掛けたりする。

また、サイバー攻撃の目的から整理すれば、個人的なものから国家による戦争行為にまで及ぶ。大別してそれらは、(1) 物理的な破壊（ダムの決壊や飛行機の衝突など）、(2) 金銭的な詐取（銀行口座への不正アクセスや証券詐欺など）、(3) 心理的操作や示威的行為（ウェブの書き換えやサービス障害など）、(4) 秘密裏の工作活動、に分けられるだろう。

サイバー攻撃の主体は国家だけではない。高度な技術があれば、非政府組織や個人、テロ集団でもサイバー攻撃に参加することができる。そうした多様化する攻撃主体への対応をサイバーセキュリティは求める。不正アクセスを犯罪として捉えるのか、戦争行為とするのか、テロなのか。宣戦布告のない攻撃が無数に始まる可能性がある。それに対して、大きな組織はそれだけでサイバーセキュリティ上の欠陥を潜在的に持ち、脆弱である。サイバー攻撃への備えが今後の非伝統的な安全保障の枠組みの中で整備されていかなくてはならない。核ミサイルの抑止では、ある程度互いの手の内を見せ合うことで相互抑止が成り立つ。しかし、サイバー戦争においては全てを隠すことになり、さらには抑止対象の主体がはっきりしないため、抑止が成り立ちにくい。

ナイは、近年の情報通信技術がもたらす特徴は「パワーの分散」であると指摘している。サイバースペースは単純にパワーを平準化するのではなく、複雑にする。その上で、「サイバー・パワー」と呼べる新しいパワーが出てきているという。それは行動論的に言えば「サイバー・ドメインの電子的に相互接続された情報資源の利用を通じて望ましい目的を達成する能力」である。ドメインという点から見れば、サイバー・パワーは、シー・パワー、エア・パワー、スペース・パワーに続く第四のパワーである。サイバースペースでは政府に限らず、ネットワーク型の組織が台頭し、スモール・アクターが力を持つという点でパワーの分散が進んでいくという[4]。

パワーの分散は平均的に行われるわけではない。情報通信のためのインフラストラクチャを持たない国ではサイバー・パワーを持ちにくい。しかし、ある程度のインフラストラクチャがあれば、小国の個人でも大国政府のサーバーを狙うことはできる。十分な知識と技能があれば、ある程度の被害を与えることができる。そうすると、パワーが米ソ二国に集中していた時代、あるいはその後の一極集中ともいわれる米国優位の世界において、パワーの分散が起こることで相対的に「損」をするのは米国だといえるだろう。米国が生み出した情報通信技術によってグローバリゼーションが加速し、その結果、米国にとっては必ずしも望ましくはないパワーの分散が進み始めている。そして、それが安全保障上の脅威となりつつあるとすれば、米国はこの問題への対処をどの国にもまして早く進めなくてはいけないと考えることができる。

今のところサイバー攻撃による直接の死者は世界でも例がないだろう。しかし、それは安全保障政策として軽視してよいということではない。国家安全保障から見て、サイバー攻撃は、(1) 戦闘行為を行う前に敵を戦闘不能にする、(2) 心理的・社会的な影響を敵に与えることができる、という点で脅威である。

２．国際的なサイバー攻撃の発生

（１）オバマ政権以前の米国に対するサイバー攻撃

現実的にインパクトのあるサイバー攻撃が行われるようになったのは最近のことだが、サイバー攻撃の可能性自体は 1980 年代から指摘されていた。1983 年に作られた映画『ウォー・ゲーム』ではコンピュータ制御の戦争のリスクが提起された。当時はロナルド・レーガン（Ronald Reagan）政権の時代であり、1983 年に発表された「スター・ウォーズ計画（戦略防衛構想）」は、夢物語として当時は受け止められた。しかし、現在ではミサイル防衛構想は現実に展開されるようになっている。映画『ウォー・ゲーム』のようにコンピュータが暴走するというシナリオは必ずしも現実的ではないが、コンピュータへの依存がいっ

そう高まっている現在、コンピュータを敵の操作からいかに守るかは重要な防衛課題になっている。

ビル・クリントン（Bill Clinton）政権で中央情報局（CIA）長官だったジョン・ドイチ（John Deutsch）は、1996 年 6 月 26 日の議会公聴会における証言で、「電子的パール・ハーバー（Electronic Pearl Harbor）」の可能性を警告した。

国際的なサイバー攻撃の例としては、1998 年 2 月に大量破壊兵器をめぐって米国とイラクの緊張が高まった際に米軍のコンピュータが攻撃された「ソーラー・サンライズ（Solar Sunrise）」事件、1998 年 3 月に国防総省、航空宇宙局（NASA）、エネルギー省のコンピュータへの不正侵入とデータのダウンロードが行われた「ムーンライト・メイズ（Moonlight Maze）」事件、2003 年に中国からと思われる侵入者がロッキード・マーチン社、サンディア国立研究所、NASA などを攻撃した「タイタン・レイン（Titan Rain）」事件がある。さらに、2008 年には、利用者のコンピュータ入力を記録する不正ソフトウェアが仕込まれた電子メールが防衛産業関係者などに送られた「ポイズン・アイビー（Poison Ivy）」事件が起きるなど、数多くの事例がある。

（２）国際的なサイバー攻撃の発生

米国では、サイバーセキュリティは、ブッシュ政権末期の 2008 年頃から米国政府の安全保障政策においてトップ・プライオリティの一つになった。2008 年度の米国の国防予算の目玉の一つは、「包括的全米サイバーセキュリティ・イニシアチブ（CNCI）」であった。ところが、このイニシアチブの予算に関する情報は機密扱いとされていて公表されていない。米国議会下院の常設インテリジェンス委員会は、この機密措置が「行き過ぎ」だとして批判した。

こうした動きを刺激したのはロシアと中国である。ロシアは、2007 年のエストニア、2008 年 6 月のリトアニア、そして 2008 年のグルジアでも実際にサイバー攻撃を行ったとされている。2007 年 4 月のエストニアにおけるサイバー攻撃では、ロシアと緊張関係にあったエストニアに対して、ロシアの記念日に当たる 4 月 27 日に攻撃が仕掛けられ、エストニアの議会、省庁、メディアや金融機関が麻痺に近い状況に置かれた[5]。

ロシアに加えて米国政府と米国防総省が懸念しているのは中国である。米国と中国は恒常的なサイバー戦争状態に入っているという見方もある。サイバー戦争は物理的な被害を伴わない限り、外部には被害が分かりにくい。仮に被害があったとしても、それを発表しないことも多い。さらには、やられたことすら気づかない場合もある。例えば、機密情報を盗み出すことが狙いだとすれば、盗まれたことが分かるようにするよりも、盗まれたこ

とすら気づかないようにして情報をコピーするのが最もスマートなやり方ということになる。

2007 年 9 月 8 日付けの英国のタイムズ紙（オンライン版）は、中国が破壊的なサイバー攻撃により米軍の輸送航空隊を妨害する詳細な計画を用意しているとする米国防総省の報告書について報じている。中国の人民解放軍の二人の技術者によって書かれたという報告書は、2050 年までに中国は、米国、英国、ロシア、韓国といったライバルたちに対して「電子的な優勢（electronic dominance）」を獲得することを目指しているという[6]。

2009 年 1 月のオバマ政権成立後、特に日本にとって大きなインパクトを与えたのが 2009 年 7 月の米韓に対する大規模サイバー攻撃である（米国では「インディペンデンス事件」、韓国では「7.7 DDoS 大乱」と呼ばれる）。2009 年 7 月 4 日、米国の独立記念日に何者かが米国の政府機関のサイトや商業サイトへの DDoS 攻撃を始めた。ホワイトハウスや国務省、財務省、国防総省、ヤフー、アマゾンなど少なくとも 20 以上のサイトが狙われた。続いて 7 日から 9 日にかけて、韓国でも大規模なサイバー攻撃が行われ、国防省や国会、国家情報院、オークションサイト、銀行など 28 機関が被害を受けた。ウイルスで乗っ取られたコンピュータは韓国を中心に 19 カ国に及び、数日にわたって波状的に行われる大規模な攻撃だった。その後の解析で、米韓両国の攻撃には同じプログラムが使われていることが分かり、攻撃は北朝鮮によるものとの疑いが強い。

サイバー攻撃は、「使いやすい第一撃」として使われる可能性も否定できない。サイバー攻撃の匿名性が高いことから、仮に政府が関与していたとしても、関与を否定しやすい。サイバー攻撃で防空システムや重要インフラストラクチャに被害を与えられれば、その後の通常兵器による攻撃は格段にやりやすくなるだろう。2009 年の米韓へのサイバー攻撃が行われているさなかに北朝鮮による軍事侵攻が韓国に対して行われていれば、被害は大きくなった可能性がある。

日本政府はこの米韓への攻撃を受けて、2010 年 5 月に「国民を守る情報セキュリティ戦略」を策定し、サイバー攻撃が国家安全保障に関わる問題であると規定し、対処を進めることになった。同盟国である米国が大規模な攻撃を受けており、隣国の韓国も攻撃を受けたことで、日本に対するサイバー攻撃の蓋然性が高まった。

３．オバマ政権とサイバーセキュリティ

（１）オバマ政権とサイバーセキュリティ

オバマ大統領が 2008 年の大統領選挙で情報通信技術を駆使したことは広く知られている。本章の冒頭で述べたように、第一期オバマ政権は成立直後からサイバーセキュリティ

に積極的に取り組んだ。

オバマ候補が大統領に当選し、翌年の就任を控えた 2008 年 12 月、ワシントン D.C.の戦略系シンクタンクである CSIS が、次期大統領のためのサイバーセキュリティ政策について提言する報告書を発表した[7]。この報告書はオバマ政権誕生を控えた時期に発表されたことから、新政権に向けて発表された数々の政策提案の一つであるとしても、ワシントンの戦略系シンクタンク大手である同研究所がサイバーセキュリティ政策を取り上げたことは注目を集めた。提言のとりまとめの中心になったジェームズ・A・ルイス（James A. Lewis）は、クリントン政権で暗号ソフトウェアの輸出規制に関わるなど、情報通信技術の国際政治において知られており、サイバーセキュリティの第一人者となっている。

これも先述のように、政権成立から 4 カ月後の 2009 年 5 月末、オバマ政権は「サイバースペース政策レビュー（通称「60 日レビュー」）」と題する報告書を発表した[8]。この報告書は、ホワイトハウスの臨時サイバーセキュリティ補佐官で、元インテリジェンス機関職員のメリッサ・ハサウェイ（Melissa Hathaway）が取りまとめたもので、彼女のチームは数多くの専門家からヒアリングを行い、100 本以上の論文を精査したという。その報告書の中で次のような認識が示されている。

> サイバーセキュリティのリスクは、21 世紀の最も深刻な経済的・安全保障的挑戦を示している。デジタル・インフラストラクチャのアーキテクチャは、安全保障よりも、相互運用性と効率性を考えて運用されてきた。その結果として、多くの国家・非国家アクターが情報を危険にさらし、盗み、変換し、破壊し、そして米国のシステムに重大な破壊を引き起こすことができるようになっている[9]。

これに合わせて 5 月 29 日、オバマ大統領は、サイバーセキュリティを担当する最高責任者としての調整官ポストの新設を発表した。「サイバー皇帝（cyber czar）」と称されるこのポストは国家安全保障会議のメンバーとなり、ホワイトハウスの安全保障担当補佐官と経済担当補佐官の両方に報告する立場になるという。しかし、このポストの任命は遅れ、指名が行われたのは年末の 12 月になってからで、「サイバーセキュリティ調整官（cybersecurity coordinator）」にハワード・シュミット（Howard Schmidt）が就いた[10]。

しかし、サイバーセキュリティが政府の政策の中で重要性を増してくるにつれ、政府内のさまざまな省庁・部局が所管権限を主張するようになった。その結果、ホワイトハウス、国防総省、国土安全保障省（DHS）、司法省、連邦通信委員会（FCC）、商務省、国家安全保障局（NSA）、CIA、全米科学財団（NSF）、連邦捜査局（FBI）などが政策決定に関わる

ようになっている。

国防総省では 2009 年 6 月 24 日、ロバート・ゲイツ（Robert Gates）国防長官がサイバーテロ攻撃に対処する USCYBERCOM を設置する命令書に署名した。実動部隊編成を経て 10 月までに運用を開始するとし、司令部はメリーランド州のフォードミード基地に置くという。フォードミードには通信傍受や暗号解読などを行うインテリジェンス機関の NSA の本部があり、NSA 長官のキース・アレクサンダー（Keith Alexander）が司令官を兼務することになった。

こうした流れの中で、オバマ政権がサイバースペースにおける問題を直視したものとして認められているのが、2010 年 2 月発表の QDR である[11]。これは四年ごとに出されるものなので、前回はまだブッシュ政権の時代であった。オバマ政権になって力点がどう変わるか、発表前から注目された。発表された報告書の序文でゲイツ国防長官は、これが戦時の QDR であることを強調するとともに、新しい分野に焦点と投資が与えられるとしている。それは、空海戦闘（エア・シー・バトル）の概念、長距離爆撃（long-range strike）、宇宙とサイバースペースである。

エア・シー・バトルはこの後、米軍の戦略的転換を意味する言葉として注目を浴びることになった。エア・シー・バトルは、米国の前方展開能力に挑戦するような国として中国などが台頭していることを背景として、空軍と海軍の統合作戦を企図した概念として登場した。しかし、陸軍と海兵隊が置き去りにされたと反発したことから、さらにその上の概念として「統合作戦アクセス構想（JOAC）」が提示されている。いずれにせよ、QDR は、特に中国が海軍力を増強させている西太平洋を念頭に置きながら、米国の前方展開能力を維持するための各軍の統合運用を目指すようになった。そこで必須となる技術が指揮通信システムということになる。したがって、サイバーセキュリティが非常に重要な課題として改めて認識されることになった[12]。

QDR は、サイバースペースにおける能力を強化するための四つのステップをとるという。第一に、サイバースペースにおける米軍のオペレーションに対して包括的なアプローチを開発する。このアプローチは文化的・組織的なものであり、ダイナミック・ネットワーク防衛オペレーションといった新しいオペレーション概念が必要となる。

第二に、サイバースペースに関する専門知識と意識の向上を図る。もはや IT は単なるツールではなく、最高の成果を出すためにはネットワーク・セキュリティの保持に努めなくてはならない。

第三に、サイバースペースにおけるオペレーションの指揮を集中化する。そのために USCYBERCOM が設立された。

第四に、他の機関や政府との提携を促進する。サイバースペースにおけるオペレーションの自由を確保し、ネットワークを防衛しなくてはならないが、ネットワーク・インフラストラクチャのかなりの部分を民間に依存している現状では、国防総省だけで完結する話ではなく、民間企業も含めて外部との提携が欠かせない。

QDR に関連して何が一番心配かと聞かれたウイリアム・J・リン（William J. Lynn III）国防副長官は、「一番はサイバー脅威だ。攻撃に際してわれわれのネットワークを守る能力を維持しなければ、わが軍、われわれの安全保障全体にとっての帰結は恐ろしいことになる」と述べた[13]。

2010 年 6 月、USCYBERCOM 司令官のアレクサンダーはワシントン D.C.の CSIS で講演し、国防総省のネットワークは敵国や犯罪組織から毎日約 600 万回もの攻撃を受けていると述べた[14]。実際には、正規のアクセスと不正アクセスを区別するのは難しく、概算の数字だと見る方が適切だろう。例えば、システムへの進入路となる「ポート」と呼ばれるネットワークのソフトウェア上の通信経路を探す「ポート・スキャニング」という手法は日常的になめるように行われている。そういったアクセスも含めれば毎日約 600 万回という数字も誇張ではないかもしれない。国土安全保障省によれば、政府および民間企業への不正侵入などの件数は 2005 年の 4095 件から 2008 年には 7 万 2065 件に増えていると明らかにしている[15]。

リン国防副長官は 2010 年秋に『フォーリン・アフェアーズ』誌で発表した論文の中で、2008 年のある日、マルウェアと呼ばれる悪意あるコードが書き込まれたフラッシュ・ドライブ（USB メモリ）が米軍のラップトップ・コンピュータに差し込まれ、ネットワークを通じてマルウェアの感染が拡大し、大きな被害が出たことを明らかにした[16]。

（２）米国議会の対応の遅れ

サイバー攻撃の脅威を指摘する米軍と行政府側からの声を受けて、米国連邦議会では数多くの法案が提出されることになった。第 112 議会（2011ー12 年）を見ると、少なくとも 76 本のサイバーセキュリティ関連法案・決議案が提出された（表 1）。

しかし、そのうち成立したのは、予算関連の法案 3 本（H.R.1540、H.R.2055、H.R.4310）、予算関連の決議案 1 本（H.J.RES.117）、イスラエルとの協力に関する法案 1 本（S.2165）のみであり、サイバーセキュリティ政策を前進させるための法案はまったく成立しなかったといってよい[17]。イスラエルとの防衛協力をうたった S.2165（United States-Israel Enhanced Security Cooperation Act of 2012）は、法案成立後 180 日以内に議会にサイバーセキュリティに関する協力がある場合には報告せよと一言入っているだけである[18]。

サイバーセキュリティに関連して特に注目された法案はいずれも成立しなかった。上院のリーバーマン法案（S.2105：Cybersecurity Act of 2012）、同じく上院のファインスタイン法案（S.2102：Cybersecurity Information Sharing Act of 2012）、下院のロジャース議員提出による CISPA（H.R.3523：Cyber Intelligence Sharing and Protection Act）などである。

これらの法案にはいくつかのポイントがあったが、そのうち、情報共有に関する条項は合意された。しかし、金融、運輸、通信、水道、電力、ガスなどの重要インフラストラクチャ保護で合意できなかったといわれている。リーバーマン法案では、政府が重要インフラストラクチャの規制に乗り出すことになっていたが、共和党議員たちは民間事業への政府の関与に強く反対し、折り合いが付かなかった。そこで、重要インフラストラクチャの事業者たちが自発的な基準を設定すべきかどうかが焦点となっていた。

議会が有効な法案を成立させることができない中、議会はオバマ大統領に対し、どのような法案の成立を求めているか意見を求め、オバマ大統領はそれに応じて見解を公表したこともあった。しかし、それでも法案が成立しなかったことを受け、オバマ大統領に大統領命令（executive order）の発出を求める声が、2012 年秋頃から出てきた。リーバーマン法案の起案者であるジョセフ・リーバーマン（Joseph Lieberman）上院議員も、法案が成立しない以上、大統領が大統領命令で補完せざるを得ないという見解を出している[19]。

ところが、リーバーマン上院議員が共和党寄りの独立議員であるのに対し、共和党の議員たちは、オバマ大統領による大統領命令の発出に反対した[20]。ホワイトハウスの一方的な行動は、議員たちの溝を悪化させるだけだというのである。

しかし、2012 年末までに決着が付かなかったため、オバマ大統領は、2013 年 2 月 12 日、一般教書演説の直前に大統領命令に署名し[21]、一般教書演説の中でもサイバーセキュリティに触れ、この問題が重要であることをアピールした。大統領命令は恒久的な解決策ではなく、議会が法案を成立させるべきであるとオバマ大統領は議員たちに求めた[22]。

この数日後の 2 月 18 日、ニューヨーク・タイムズ紙（オンライン版）は、同紙をはじめとする米国メディアへのサイバー攻撃が行われていたことと関連し、中国の人民解放軍による執拗な APT が行われていたとする民間コンサルタント会社マンディアント（Mandiant）の報告書について報じた[23]。その報告書によれば、数多くの APT が中国の上海にあるビルまでたどることができ、そこで人民解放軍の部隊 61398 が活動していることが分かったという。そして、この報告書の内容について米国政府のインテリジェンス機関も同意していると同紙は報じている。

米国のレオン・E・パネッタ（Leon E. Panetta）国防長官と中国の梁光烈国防部長と 2012 年 5 月に会談した際、両国はサイバーセキュリティでの協力を検討していくことで合意し

ていた[24]。それにもかかわらず、人民解放軍からの執拗な APT が行われていることに米国がいらだちを強めていることを一連の動きは示しているといえるだろう。

表 1　第 112 議会におけるサイバーセキュリティ関連法案

法案番号	法案名	法案成立の可否
H.R.12	American Jobs Act of 2011	×
H.R.76	Cybersecurity Education Enhancement Act of 2011	×
H.J.RES.117	Continuing Appropriations Resolution, 2013	○
H.R.154	National Defense Authorization Act for Fiscal Year 2012	×
H.R.174	Homeland Security Cyber and Physical Infrastructure Protection Act of 2011	×
H.R.209	Cybersecurity Enhancement Act of 2012	×
H.RES.446	Supporting the goals and ideals of National Cyber Security Awareness Month and raising awareness and enhancing the state of cyber security in the United States.	×
H.R.516	Bring Jobs Back to America Act	×
H.R.607	Broadband for First Responders Act of 2011	×
H.RES.631	Providing for consideration of the bill (H.R. 3523) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cyber security entities, and for other purposes; providing for consideration of motions to suspend the rules; providing for consideration of the bill (H.R. 4628) to extend student loan interest rates for undergraduate Federal Direct Stafford Loans; and for other purposes.	×
H.R.1136	Executive Cyberspace Coordination Act of 2011	×
H.R.1261	Chief Technology Officer Act	×
H.R.1540	National Defense Authorization Act for Fiscal Year 2012	○
H.R.2017	Department of Homeland Security Appropriations Act, 2012	×
H.R.2055	Consolidated Appropriations Act, 2012	○
H.R.2096	Cybersecurity Enhancement Act of 2011	×
H.R.2112	Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act, 2012	×
H.R.2258	National Hurricane Research Initiative Act of 2011	×
H.R.2314	Interagency Personnel Rotation Act of 2011	×
H.R.2356	WMD Prevention and Preparedness Act of 2011	×
H.R.2976	HEROES Act of 2011	×
H.R.3070	Making appropriations for the Departments of Labor, Health and Human Services, and Education, and related agencies for the fiscal year ending September 30, 2012, and for other purposes.	×
H.R.3116	Department of Homeland Security Authorization Act for Fiscal Year 2012	×
H.R.3509	Wireless Innovation and Public Safety Act of 2011	×
H.R.3523	Cyber Intelligence Sharing and Protection Act（ロジャース法案）	×
H.R.3630	Middle Class Tax Relief and Job Creation Act of 2011	×

法案番号	法案名	法案成立の可否
H.R.3671	Consolidated Appropriations Act, 2012	×
H.R.3674	PRECISE Act of 2012	×
H.R.4133	United States-Israel Enhanced Security Cooperation Act of 2012	×
H.R.4257	Federal Information Security Amendments Act of 2012	×
H.R.4263	SECURE IT Act of 2012	×
H.R.4310	National Defense Authorization Act for Fiscal Year 2013	○
H.R.4485	Credible Military Option to Counter Iran Act	×
H.R.5743	Intelligence Authorization Act for Fiscal Year 2013	×
H.R.5855	Department of Homeland Security Appropriations Act, 2013	×
H.R.5972	Transportation, Housing and Urban Development, and Related Agencies Appropriations Act, 2013	×
H.R.6018	Foreign Relations Authorization Act, Fiscal Year 2013	×
H.R.6020	Financial Services and General Government Appropriations Act, 2013	×
H.R.6221	Identifying Cybersecurity Risks to Critical Infrastructure Act of 2012	×
S.8	Tough and Smart National Security Act	×
S.21	Cyber Security and American Cyber Competitiveness Act of 2011	×
S.68	Secure Chemical Facilities Act	×
S.RES.306	A resolution supporting the goals and ideals of National Cybersecurity Awareness Month and raising awareness and enhancing the state of cybersecurity in the United States.	×
S.372	Cybersecurity and Internet Safety Standards Act	×
S.413	Cybersecurity and Internet Freedom Act of 2011	×
S.709	Secure Chemical Facilities Act	×
S.813	Cyber Security Public Awareness Act of 2011	×
S.911	SPECTRUM Act	×
S.1011	Electronic Communications Privacy Act Amendments Act of 2011	×
S.1040	Broadband for First Responders Act of 2011	×
S.1151	Personal Data Privacy and Security Act of 2011	×
S.1152	Cybersecurity Enhancement Act of 2011	×
S.1159	Cyberspace Warriors Act of 2011	×
S.1253	National Defense Authorization Act for Fiscal Year 2012	×
S.1254	Department of Defense Authorization Act for Fiscal Year 2012	×
S.1268	Interagency Personnel Rotation Act of 2011	×
S.1342	Grid Cyber Security Act	×
S.1426	Foreign Relations Authorization Act, Fiscal Years 2012 and 2013	×
S.1469	International Cybercrime Reporting and Cooperation Act	×

法案番号	法案名	法案成立の可否
S.1535	Personal Data Protection and Breach Accountability Act of 2011	×
S.1546	Department of Homeland Security Authorization Act of 2011	×
S.1549	American Jobs Act of 2011	×
S.1596	Transportation, Housing and Urban Development, and Related Agencies Appropriations Act, 2012	×
S.1599	Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2012	×
S.1660	American Jobs Act of 2011	×
S.1867	National Defense Authorization Act for Fiscal Year 2012	×
S.2102	Cybersecurity Information Sharing Act of 2012（ファインスタイン法案）	×
S.2105	Cybersecurity Act of 2012（リーバーマン法案）	×
S.2151	SECURE IT	×
S.2165	United States-Israel Enhanced Security Cooperation Act of 2012	○
S.2322	Transportation, Housing and Urban Development, and Related Agencies Appropriations Act, 2013	×
S.3216	Department of Homeland Security Appropriations Act, 2013	×
S.3254	National Defense Authorization Act for Fiscal Year 2013	×
S.3295	Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2013	×
S.3342	SECURE IT	×
S.3414	CSA2012	×

注：米国連邦議会のウェブページ（http://thomas.loc.gov/）にて「cyber security」または「cybersecurity」で検索した結果を整理した。実際の検索では同じ法案の違うバージョンが複数ヒットする。「H.R.」は下院の法案、「S.」は上院の法案、「RES」と付くものは決議案である。

おわりに

2012 年後半、さまざまな国際会議においてサイバーセキュリティの問題が取り上げられた。第一に、ハンガリーのブダペストにおいて、2012 年 10 月に「サイバースペース会議（Conference on Cyberspace）」が開かれた。これは、前年に英国のウィリアム・ヘイグ（William Hague）外相が呼びかけて開催されたロンドン会議に続くもので、さまざまな議題が議論されたが、中心はサイバーセキュリティであった。また、国連総会第一委員会の政府専門家会合（GGE）でもサイバーセキュリティが議論されている。さらに、2012 年 12 月にドバイで開かれた国際電気通信連合（ITU）の世界電気通信会議（WCIT）では、インターネットを国家が管理すべきという中国を中心とする発展途上国の提案に対し、日米などが反対して決裂するという事態になった。サイバーセキュリティは国際政治上の課題として重要性を増してきている。

こうした国際会議での中心軸は、米国対中国になっている。インターネットへの国家の関与を強め、国際交渉の議題に中国はしようとしている。一見すると、こうした国際交渉で手足を縛ってしまえば、サイバー攻撃を行っている中国にとっても不利になるかと思えるが、中国の公式見解は、中国は何も悪いことはしていないという立場である。したがって、こうした交渉がまとまれば、中国は、自分たちは従来の主張を繰り返しながら、中国に対する攻撃を止めるために米国その他の国々に注文を付けられると踏んでいるようである。

本章の目的は、米国のオバマ政権になってなぜサイバーセキュリティに対する積極的な取り組みが行われてきたのかを分析することであった。それに対する答えは、第一に、国防総省のネットワークをはじめとして米国政府あるいは民間のシステムが日常的に攻撃対象となっており、実際に 2009 年 7 月の大規模攻撃のような被害が見られるようになってきていることが挙げられる。第二に、2007 年のエストニアやシリアなど、深刻な被害が米国外でも起こるようになり、グローバル・コモンズとしてのインターネットその他の情報通信システムへの脅威が増してきている点も重要である。そして第三に、こうした攻撃の主体が、これまでの安全保障政策で想定してきたような対称的な存在ではなく、非対称的で匿名性の高い存在であり、いち早く新しい安全保障システムを作り出す必要をオバマ政権が認識したということもあるだろう。

こうした米国政府の変化は、オバマ政権だからこそ始まったというよりは、インターネットや携帯電話など新しいデジタル情報通信技術が急速に発展したことによる必然的な変化と考える方が適切である。無論、オバマ大統領は 2008 年の大統領選挙でインターネットを駆使し、その威力に敏感であったという点も無視できない。社会システムがますますネットワーク技術に依存するようになることを考えれば、それが安全保障上の脆弱点とならないよう手を打つことは、政策担当者の重要な課題となるだろう。

しかしながら、内政という視点から見ると、米国連邦議会は、オバマ政権の意向をくみ取った形で法案を可決することができず、民主・共和両党の政策方針の違いに妥協を見出すことができないでいる。

－注－

[1] 詳しくは記事を書いたサンガー記者の著書を参照。David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), chapter 8.

[2] 近年のサイバーセキュリティに関する関心の高まりに注目したものとしては、以下が挙げられる。Richard A. Clarke, and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do*

about It (New York: ECCO, 2010). 邦訳は以下の通り。リチャード・クラーク、ロバート・ネイク『世界サイバー戦争―核を超える脅威　見えない軍拡が始まった―』北川知子、峯村利哉訳（徳間書店、2011 年）。西本逸郎、三好尊信『国・企業・メディアが決して語らないサイバー戦争の真実』（中経出版、2012 年）。伊東寛『「第５の戦場」サイバー戦の脅威』（祥伝社、2012 年）。土屋大洋『サイバー・テロ　日米 vs.中国』（文藝春秋、2012 年）。

[3] Richard L. Armitage and Joseph S. Nye, *The U.S.-Japan Alliance: Anchoring Stability in Asia* (Washington, D.C.: Center for Strategic and International Studies, August 2012), p. 13.

[4] Joseph S. Nye, Jr., "Cyber Power," Harvard Kennedy School Belfer Center for Science and International Affairs, (May 2010).

[5] Clarke and Knake, *Cyber War*, pp. 11-16.

[6] Tim Reid, “China’s Cyber Army is Preparing to March on America, says Pentagon,” Times Online (September 8, 2007). <http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece>, accessed on May 9, 2010.

[7] CSIS, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C., CSIS, December 2008).

[8] United States Government, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>, accessed on May 31, 2009.

[9] ibid., p. iii.

[10] シュミットはブッシュ政権でも似たようなポジションに就いていたが、返り咲いたことになる。そのシュミットも 2012 年 5 月末で辞任し、後任には行政管理予算局（OMB）の経歴が長いマイケル・ダニエル（Michael Daniel）が着任した。ダニエルは必ずしも IT に強い専門家というわけではなく、このポジションの弱さがうかがえる。

[11] United States Department of Defense, *Quadrennial Defense Review* <http://www.defense.gov/qdr/>, accessed on February 28, 2010.

[12] エア・シー・バトルの実現には、米国の各軍の統合運用だけでなく、同盟国との協力も重要になる。したがって、国際的なサイバーセキュリティもまた重要になるという側面がある。

[13] John J. Kruzel, “Cybersecurity Seizes More Attention, Budget Dollars,” <http://www.defense.gov/news/newsarticle.aspx?id=57871>, accessed on May 3, 2010.

[14] Gautham Nagash, “Alexander Says U.S. Networks under Constant Attack,” *The Hill*, (June 3, 2010).

[15] 「『サイバー安保』で調整官ポストの創設発表、オバマ氏」CNN.co.jp（2009 年 5 月 30 日アクセス）。

[16] William J. Lynn, III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, vol. 89, no. 5 (September/October 2010), pp. 97-108.

[17] 2012 年 12 月にワシントン D.C.で行ったヒアリングでも同様の見解が得られた。

[18] ただし、いわゆる「スタックスネット」が米国とイスラエルの協力によって行われたとする報道があることから、この法案の一文は興味深い。

[19] Josh Peterson, “Lieberman pushes Obama to Issue Cybersecurity Executive Order,” The Daily Caller <http://dailycaller.com/2012/09/26/lieberman-pushes-obama-to-issue-cybersecurity-executive-order/>, accessed on September 26, 2012. Dara Kerr, “Senator urges Obama to Issue 'Cybersecurity' Executive Order,” CNET <http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/>, accessed on September 24, 2012.

[20] Eric Chabrow, “GOP Senators Warn Obama on Executive Order,” Bank Info Security <http://www.bankinfosecurity.com/gop-senators-warn-obama-against-issuing-executive-order-a-5162>, accessed on October 2, 2012.

[21] The White House, “Executive Order – Improving Critical Infrastructure Cybersecurity,” White House Office of the Press Secretary <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>, accessed on February 23, 2013.

[22] The White House, “Remarks by the President in the State of the Union Address,” White House Office of the Press Secretary <http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address>, accessed on February 23, 2013.

[23] David E. Sanger, David Barboza and Nicole Perlroth, “Chinese Army Unit is Seen as Tied to Hacking Against U.S.,” New York Times (February 18, 2013) <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>, accessed on February 23, 2013.

[24] Cheryl Pellerin, “U.S., China Must Work Together on Cyber, Panetta Says,” U.S. Department of Defense (May 7, 2012) <http://www.defense.gov/News/NewsArticle.aspx?ID=116235>, accessed on February 23, 2013.