論題 Title	米国における重要インフラのサイバーセキュリティ強化策
他言語論題 Title in other language	Cybersecurity Enhancement Measures for Critical Infrastructure in the United States
著者 / 所属 Author(s)	山﨑　治（Yamazaki, Osamu） / 国立国会図書館調査及び立法考査局専門調査員　外交防衛調査室主任
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	828
刊行日 Issue Date	2020-01-20
ページ Pages	29-56
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	サイバー攻撃による重要インフラの障害発生を防ぎ、発生した場合でも素早く復旧できるようにすることは、安全保障上の重要課題になっている。その課題に早くから取り組む米国の施策をまとめた。

米国における重要インフラのサイバーセキュリティ強化策

国立国会図書館　調査及び立法考査局
専門調査員　外交防衛調査室主任　山﨑　治

目　　次

キーワード：重要インフラ、サイバー攻撃、サイバーセキュリティ、安全保障

要　旨

① 閉鎖的なネットワークで運用され、独自技術、独自システムで構成された重要インフラの制御システムは、サイバー攻撃を受けにくいと考えられてきた。しかし、近年、重要インフラにおける制御システムの標準化等の進展、制御システムの他の情報システムとの連携の要求、重要インフラの制御システムを攻撃する手法に関する情報の拡散が行われるようになったことで、重要インフラの制御システムに対するサイバー攻撃が可能になったと考えられている。

② サイバー攻撃により重要インフラに重大な障害が発生した事例としては、2010年に行われたイランの核燃料濃縮施設に対する攻撃（遠心分離機を稼働不能にした）、2015年と2016年に行われたウクライナの電力網に対する攻撃（制御システムに侵入し、2015年は最大6時間、2016年は最大1時間15分の停電を引き起こした）が挙げられる。

③ 米国において、クリントン政権は、重要インフラ保護の必要性に対する認識の高まりとともに、物理的及びサイバー上のセキュリティを高める施策を進め、情報通信ネットワークの安全性及び信頼性の向上を図るためのプログラムを発表した。ブッシュ政権は、重要インフラを国土安全保障戦略の重要分野の1つとして位置付け、重要インフラ保護の国家戦略、保護計画を充実させた。オバマ政権は、サイバーセキュリティを向上させるために実施すべき計画を具体化し、サイバーインシデントへの対応システムの運用レベルの平準化を図った。また、障害発生からの復旧力の強化とサイバーセキュリティ情報の共有化に取り組んだ。トランプ政権は、リスク管理アプローチのレベルを高め、サイバー空間の脅威から米国を守るための安全保障政策を整理した。電力に関しては、壊滅的な停電も念頭に置いた対策を講じている。

④ 近年の日本は、自然災害による大規模停電を経験しており、多くの国民が電力の重要性を認識している。他の重要インフラに障害が発生した場合も社会的・経済的損失は大きく、サイバー攻撃により重要インフラ障害が引き起こされることを未然に防ぎ、引き起こされた場合でも素早く復旧可能な環境を整えておくことは、安全保障上の優先順位が高い課題になっている。日本では、平成30年策定の「サイバーセキュリティ戦略」、「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づいた施策が進められている。しかし、サイバーセキュリティに関しては、技術の進歩が速く、これだけの対策を講じれば十分と言い切ることが難しい。今後も迅速に関連情報の入手を図り、対策を充実させていくことが望まれる。

はじめに

2019年9月6日、エネルギー関連のニュースサイト「E&E News」は、同年3月5日に米国西部の電力網に対してサイバー攻撃(1)が行われ、停電が起こることはなかったが、電力管理センター等に低レベルの影響を及ぼしたことを報じた(2)。北米電力信頼度協会（North American Electric Reliability Corporation: NERC）(3)は、サイバー攻撃により発電所内の装置間の通信及び発電所と電力管理センター間の通信が短時間（5分未満）停止させられることを防ぐための対策として、ファイアウォール(4)のファームウェア(5)の迅速な更新、インターネットに接続する機器の可能な限りの削減、ファイアウォールで処理する前に受信トラフィック(6)をフィルタリング(7)するためのアクセス制御リストの使用等が考えられることを明らかにしていた(8)。

電力網に対するサイバー攻撃としては、東欧のウクライナにおいて2015年12月と2016年12月に停電を引き起こした攻撃（詳しくは後述）がよく知られているが、インフラ施設に対するサイバー攻撃は電力網以外にも行われており、社会の安定を揺るがす脅威とみなされている。例えば、米国における重要インフラ(9)を対象としたサイバー攻撃の「産業用制御システム・サイバー緊急対応チーム」（Industrial Control Systems Cyber Emergency Response Team: ICS-CERT）(10)への報告件数は、2009会計年度は9件にすぎなかったが、2013会計年度には257件まで増加し、2016会計年度は290件に達しており、サイバー攻撃によって重大インフラの大規模障害が引き

＊　本稿における肩書は全て当時のもので、インターネット資料の最終アクセス日は2019（令和元）年12月6日である。

(1)「サイバー」は「インターネットが形成する情報空間（サイバースペース）に関連した」の意。コンピュータ・ネットワークに不正に侵入する行為を指す言葉は、正確には「クラッキング（Cracking）」であるが、一般的には「ハッキング（Hacking）」が使われることが多い。本稿もその慣例に倣う。

(2) Blake Sobczak, “Report reveals play-by-play of first U.S. grid cyberattack,” 2019.9.6. E&E News HP <https://www.eenews.net/stories/1061111289>

(3) NERCは、北米市場の電力システムの信頼性やセキュリティを向上させる目的で1968年に設立され、電力業界と連邦政府の間で重要インフラ問題に関する情報の交換を調整する役割を担っている。NERCは、全米10の地域信頼性評議会（regional reliability council）で構成され、各地域信頼性評議会には、民間公益機関、連邦電力機関、地方の電力協同組合、州・地方公共団体の公益機関、独立系発電所、総合エネルギー会社、エンド・ユーザー企業などが加盟しており、事実上米国とカナダで供給・利用される電力会社・機関のほとんどを占めている（渡辺弘美「米国における重要インフラ保護対策の状況」『ニューヨークだより』2005.11, p.19. 情報処理推進機構 HP <https://www.ipa.go.jp/files/000006015.pdf>）。

(4) コンピュータ・ネットワークの結節点となる場所に設けられ、セキュリティ上、通過させてはいけない通信を阻止するシステム。

(5) コンピュータ・システム（ハードウェア）を制御するため、電子機器に組み込まれたソフトウェア。

(6) コンピュータ・ネットワークを流れる情報。

(7) 指定した条件により、情報の流通を許可するか遮断するか判断する機能。

(8) North American Electric Reliability Corporation, “Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities,” 2019.9.4. E&E News HP <https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf>

(9) 米国において、重要インフラ（Critical Infrastructure）とは「物理的、仮想的を問わず、その無能力化又は破壊が国家の安全、経済安全保障、公衆衛生、環境又はそれら複数の弱体化につながる米国にとって極めて重要なシステム及び資産」（42 U.S.C. 5195c(e)）と定義され、2013年に出された大統領政策指令21号（“Presidential Policy Directive - Critical Infrastructure Security and Resilience,” 2013.2.12. White House President Barack Obama HP <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>）において、該当する部門として、化学、商業施設、通信、重要機器製造業、ダム、防衛産業基盤、救急サービス、エネルギー、金融サービス、食糧・農業、政府施設、医療・公衆衛生、情報技術、原子炉及び核燃料・核廃棄物施設、運輸システム、上下水道システムの16部門が指定されている。

(10) 国土安全保障省（DHS）のサイバーセキュリティ・インフラ・セキュリティ庁（CISA）（詳しくは後述）の組織で、制御システムの脆弱性報告の受付や攻撃への対応支援を行っている。

起こされる事態を未然に防ぐ必要性が高まっている。

本稿では、重要インフラに対する代表的なサイバーインシデント(11)を紹介した上で、早くから重要インフラのサイバーセキュリティ強化を図ってきた米国の施策について、障害が発生したときの影響が特に大きいと考えられる電力(12)の例とともに解説する。

Ⅰ　重要インフラに対するサイバー攻撃の事例

1　重要インフラに対するサイバー攻撃が可能となった背景

従来、重要インフラの制御システムは、インターネット等から隔離された閉鎖的なネットワークで運用され、一般の情報システムと異なり、多くの独自技術、独自システムで構成されているため、サイバー攻撃を受けにくいと考えられてきた(13)。しかし、近年、①重要インフラにおける制御システムの標準化、汎用化、一般商品化の進展、②重要インフラの制御システムの他の情報システムとの連携の要求（スマートな社会の実現に向けた動き）、③重要インフラの制御システムを攻撃する手法に関する情報の拡散、が行われるようになったことで、重要インフラの制御システムに対するサイバー攻撃が可能になったと考えられている。

サイバー攻撃の主体は、個人、犯罪集団に限らず、国家の関与が疑われるケースも現れている(14)。国境を越えどこからでも攻撃を仕掛けることができる攻撃者は、常に優位に立ち、新しいソフトウェアの脆弱性をいち早く発見してシステムへの侵入を試みたり、マルウェア（悪意のあるソフトウェア）を開発して攻撃に活用したりするなど、防御側の一歩先の手を打つことができる。サイバー攻撃の手法は日々進化を遂げ、国家の関与が疑われるケースでは、高度な技術が使われ、多大な手間とコストをかけて執拗な攻撃が行われる傾向にある。

サイバー攻撃により重要インフラの制御システムが被害を受けたインシデントの例としては、2010 年にイランの核燃料濃縮施設の遠心分離機が稼働不能になった例と、2015 年と 2016 年にウクライナで停電が引き起こされた例が挙げられることが多い。本稿でも、最初に、それらのインシデントの要点を簡単に紹介する。

2　イランの核燃料濃縮施設に対する攻撃

2010 年 11 月 30 日、イランのアハマディネジャド（Mahmoud Ahmadinejad）大統領が、ナタンズ

(11)　サイバースペースにおけるインシデントとは、情報及び制御システムの運用におけるセキュリティ上の問題として捉えられる事象で、情報流出、不正侵入、マルウェア（悪意のあるソフトウェア）感染、Web サイト改ざん、DoS／DDoS 攻撃（単数（DoS 攻撃）又は複数（DDoS 攻撃）のコンピュータから標的となるサーバーに対しネットワークを介して大量の処理要求を送ることによりサービスを停止させてしまう攻撃）等の事象がある（「インシデントとは」JPCERT コーディネーションセンター HP <https://www.jpcert.or.jp/aboutincident.html> 等）。

(12)　例えば、Scott Kelly et al., *Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy*, Cambridge: University of Cambridge, 2016, pp.22, 36. University of Cambridge Judge Business School HP <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf> は、英国の南部及び東部の電力網に対しサイバー攻撃が行われたと仮定し、3 つのシナリオを想定して経済的損失額を試算している。攻撃を受けてから 5 年間にわたり継続する経済的損失額は、S1 シナリオ（65 発電所が被害、停電 10.5 日）で 490 億ポンド、S2 シナリオ（95 発電所が被害、停電 21 日）で 1290 億ポンド、X1 シナリオ（125 発電所が被害、停電 42 日）で 4420 億ポンドである（平成 31 年 4 月 1 日適用の省令レートは、1 ポンド＝ 148 円）。

(13)　以下の本段落の記述については、松本泰「重要インフラ事業者が理解するべきサイバーセキュリティの動向」『SE』183 号, 2016.6, pp.21-22. 総合安全工学研究所 HP <http://www.i-s-l.org/shupan/pdf/SE183_4_open.pdf> を参照した。

(14)　以下の本段落の記述については、谷脇康彦『サイバーセキュリティ』岩波書店, 2018, pp.8-13 を参照した。

にある核燃料濃縮施設のシステムがマルウェアに感染したことにより遠心分離機に問題が発生したことを認めたと報じられた(15)。同年9月に起こったこのインシデントにおいては「Stuxnet」と呼ばれる高度な技術を要するマルウェアが使われた(16)。攻撃者は、Stuxnetを仕込んだUSBメモリを施設内にばら撒き、それを拾った施設職員が施設内のコンピュータで使用したため、感染したと考えられている。Stuxnetは、USBメモリをパソコンに差し、ショートカットされたファイルを閲覧しただけで感染するようになっており、侵入後は、主にWindows(17)の脆弱性を利用し（利用された5件の脆弱性のうち4件は未知のものであった）、同一ネットワーク内にある特定のソフトウェア（シーメンス（Siemens）社が開発・販売した制御システム管理ソフトウェア「SIMATIC WinCC」）が搭載されたコンピュータに感染を広げた。この感染拡大は、ソフトウェア中に直接記述されていたパスワードを使用してSIMATIC WinCCが利用しているデータベースにログインし、データベース中にStuxnetをコピーして実行することにより行われた。そして、シーメンス社のツール「SIMATIC STEP 7」を利用してPLC（Programmable Logic Controller）(18)を不正に操作し、PLCにつながるインバータ機器（周波数変換装置）の周波数を変更したことで、約8,400台の遠心分離機が稼働不能になった。

3　ウクライナの電力網に対する攻撃

ウクライナの電力網は2回サイバー攻撃を受けている。2015年12月の攻撃については、インターネットとつながっているITシステムから制御システムへの通信を停止させただけで、制御システムを直接操作することはできていなかった（停電は、内通者が手動で引き起こした）とする見方もあるのに対し、2016年12月の攻撃は、ITシステムから制御システムに侵入して攻撃プログラムを作動させることにより、制御システムを外部から操作することに成功しており、人の手を介さず停電を引き起こしている(19)。2016年12月の攻撃に使われた「CrashOverride」（別名「Industroyer」）と呼ばれるマルウェアは、制御システムに関する深い知識と理解に基づいて作られたもので、電力システム向けに開発されたと見られているが、小プログラムを加えることにより、電力以外の重要インフラに被害をもたらすことが可能とする分析もある。

(1) 2015年12月に発生したインシデント

2015年12月23日、イバノフランコフスク、チェルノフツィ、キエフの3つの都市において

---

(15) Parisa Hafezi, “Iran admits cyber attack on nuclear plants,” 2010.11.30. Reuters HP <https://www.reuters.com/article/us-iran/iran-admits-cyber-attack-on-nuclear-plants-idUSTRE6AS4MU20101129>

(16) 以下の本段落の記述については、中島明日香『サイバー攻撃―ネット世界の裏側で起きていること―』講談社, 2018, pp.224-228を参照した。

(17) マイクロソフト（Microsoft）社が提供するOS（Operating System）で、コンピュータのシステム全体を管理する基本ソフトウェア。

(18) JIS規格において、PLCは、「ディジタル又はアナログ入出力を介し、種々の機械及びプロセスを制御するために、論理、順序、計時、計数及び算術演算のような特有機能を実行し、使用者が使う命令を内部に記憶するためにプログラマブルメモリを使用し、工業環境下で使用するために設計されたディジタル演算電子システム。（後略）」と定義されている（JISB3501「プログラマブルコントローラ―一般情報」p.2.「JIS検索」日本産業標準調査会HP <https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html> で、JIS番号「B3501」を入力すると閲覧することができる。）。

(19) 以下の本段落の記述については、経済産業省商務情報政策局「参考資料」（第1回産業サイバーセキュリティ研究会 参考資料）2017.12.27, p.8. <https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_s01_00.pdf> を参照した。

電力会社に対するサイバー攻撃が行われ、大規模停電が引き起こされた[20]。停電の復旧までには最大6時間を要し、22万5千人が被害を受けた。攻撃者は、サイバー攻撃の対象企業の情報（システム情報、組織情報、社員情報、取引先情報等）を6か月以上前から調査し、インターネット等で収集した社員情報などを基に標的型攻撃メール[21]を送付し、業務端末のマルウェア感染を誘った。その後、業務端末や各種サーバー（端末からの要求に対してサービスを提供するコンピュータ）へ感染を拡大させながら内部情報の探索・収集を行ったことにより、制御システムのリモート接続の正規認証情報やシステム構成情報を入手し、仮想専用線（Virtual Private Network: VPN）[22]経由で制御システムへの侵入を試み、制御端末からシステム環境の把握をして攻撃の準備を進めた。そして、攻撃に向けた準備が整った段階で、制御システム内の制御端末を不正に操作したと考えられている（前述のように、外部からの直接操作には成功していないとする見方もある）。また、攻撃者は、複数の手段を用いて同時にサイバー攻撃を実行していたとみられ、複合的な被害の発生を意図していた可能性も指摘されている。

(2) 2016年12月に発生したインシデント

2016年12月17日にキエフにおいて行われた電力会社へのサイバー攻撃は、最大1時間15分の停電を発生させ、数万人に被害を与えた[23]。当該インシデントが発生する数日前から、ウクライナのインフラ事業者へのサイバー攻撃が確認されていた。2015年と同様の攻撃手法により制御システムに侵入し、制御端末をCrashOverrideに感染させ、攻撃対象機器の情報を収集し、攻撃対象機器に合わせた攻撃プログラムを追加で開発した（CrashOverrideは攻撃実行日まで潜伏）。指定日に自動で行われた攻撃は、CrashOverrideから制御システムにブレーカーを開閉するコマンドを連続して送信することにより行われたと考えられている。CrashOverrideは、バックドア（正規の手続を経ずに内部に侵入すること）、データ消去機能、特定製品に対するDoS攻撃（コンピュータから標的となるサーバーに対しネットワークを介して大量の処理要求を送ることによりサービスを停止させてしまう攻撃）機能をモジュール化した（使いたい機能を選択して組み込むことを可能にした）もので、電力業界で使用されることが多いプロトコル[24]を実装していた。

---

⑳ 以下の本段落の記述については、情報処理推進機構セキュリティセンター「制御システムのセキュリティリスク分析ガイド補足資料　制御システム関連のサイバーインシデント事例1―2015年　ウクライナ　大規模停電―」2019.7, pp.4-8. <https://www.ipa.go.jp/files/000076755.pdf> を参照した。

㉑「標的型攻撃メールは、不特定多数に大量に送られるウイルスメールとは異なり、特定の組織や人にしか送られないため、セキュリティソフトの定義ファイルに登録される前に標的とするメール受信者まで届いてしまう。そのため、受信者がセキュリティソフトを利用していても、被害を防ぐことが難しい。また、メール受信者が不審をいだかないように様々な騙しのテクニックが駆使されているため、メール受信者は本物のメールと勘違いしてしまい、ウイルス感染の仕掛けが施された添付ファイルを開いたり、本文に記載されたウイルス感染の仕掛けが施されたサイトへのリンクをクリックしたりしてしまう可能性が高い。」（情報処理推進機構セキュリティセンター「IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」」2015.1.9, p.1. <https://www.ipa.go.jp/files/000043331.pdf>）

㉒ 企業等の拠点間を専用線でつなぐかわりに、複数のユーザーで共用する回線を仮想的な専用ネットワークとして利用する技術及びサービス。トンネリング（通信ネットワーク上の2点間を結ぶ閉じられた仮想的な直結回線を確立すること）やカプセル化（ある通信手順によるデータ表現の内部に、別のプロトコルによるデータ表現を埋め込んで伝送すること）、さらに暗号化や認証の技術を用いることで、共用の回線があたかも専用線のように安全に利用できるようになる。VPNは使用する回線によって、インターネット回線を用いる「インターネットVPN」と通信事業者の閉域ネットワークを用いる「IP-VPN（閉域VPN）」の2つに大別される（「VPN（Virtual Private Network）とは？」NTT東日本HP <https://business.ntt-east.co.jp/content/VPN-select/>）。

㉓ 以下の本段落の記述については、情報処理推進機構セキュリティセンター「制御システムのセキュリティリスク分析ガイド補足資料　制御システム関連のサイバーインシデント事例2―2016年　ウクライナ　マルウェアによる停電―」2019.7, pp.4-7. <https://www.ipa.go.jp/files/000076756.pdf> を参照した。

Ⅱ　米国における重要インフラのサイバーセキュリティ強化策

米国においては、1993年2月26日に発生した世界貿易センタービルの地下駐車場爆破事件[25]以降、テロの脅威への対応が重視されるようになり、重要インフラについても、物理的及びサイバー上の保護施策が講じられてきた。本章では、重要インフラ全般、電力分野、原子力発電に分け、主なサイバーセキュリティ強化策とサイバーインシデントの説明を行う。一部の動きを除き、本章で取り上げた動きを年ごとにまとめ直したのが本稿末尾の別表である。安全保障上の必要性の高まりとともに重要インフラのセキュリティ強化が進められ、サイバー上の施策が独立して策定されるようになったこと、重要インフラ保護の国家戦略と保護計画の充実化、重要インフラ事業者内における保護能力の平準化と情報の共有化が図られたこと等がわかる。

1　クリントン政権時（1993.1.20-2001.1.20）のサイバーセキュリティ強化策

1996年7月15日、クリントン（William J. Clinton）大統領は、行政命令13010号「重要インフラの保護」（EO-13010）[26]を発出した[27]。EO-13010では、通信、電力システム、ガス・石油の貯蔵・輸送、銀行・金融、運輸、水供給システム、医療・警察・消防等の救急サービス、政府サービスの8分野が重要インフラとされ、それらの重要インフラに対する脅威として、物理的攻撃だけでなくサイバー攻撃も念頭に置かれた。そして、重要インフラの保護戦略を策定するため、「重要インフラに関する大統領委員会」（President's Commission on Critical Infrastructure Protection: PCCIP）が設置された。

PCCIPは、1997年10月に、「重要基盤：米国のインフラの保護」と題する報告書[28]を大統領に提出した。同報告書において、PCCIPは、サイバー攻撃からのインフラ保護のために最も効果的なのは、インフラ所有者・運営者と政府機関の間のパートナーシップに基づく協力と情報共有の戦略であるとし、重要システム保護のための技術開発の促進等を政府に求めた。この報告書を受け、1998年8月に、大統領決定指令63号「重要インフラの保護：部門コーディネータ」（PDD-63）[29]が発出された。同指令により、重要インフラの所有者・運営者の利益を代表できるよう、部門コーディネータ（Sector Coordinators: SCs）という民間部門の代表者が置かれ、SCsの特別な役割の1つとして、重要な情報・コミュニケーションのインフラに関する国全体の保

⑵④　例えば、変電装置と制御システムとの間のデータのやりとりのために使われる手順を定めた「IEC 60870-5」（「産業制御システムに最大級の脅威をもたらすマルウェア「インダストロイヤー」」2017.6.20. キヤノンマーケティングジャパン株式会社HP <https://eset-info.canon-its.jp/malware_info/trend/detail/170620.html>）。

⑵⑤　1993年2月26日に、ニューヨークの世界貿易センタービルの地下駐車場で爆弾が爆発し、6人が死亡し、1,000人以上が負傷した事件（外務省領事局邦人テロ対策室「海外赴任者のための安全対策小読本」2014.1, p.36. <https://www.anzen.mofa.go.jp/pamph/pdf/pamph_08.pdf>）。

⑵⑥　"Executive Order 13010 of July 15, 1996, Critical Infrastructure Protection." govinfo HP <https://www.govinfo.gov/content/pkg/WCPD-1996-07-22/pdf/WCPD-1996-07-22-Pg1242-2.pdf>

⑵⑦　大統領が発出する命令の総称である「大統領令（presidential directive）」のうち「executive order」の訳として、本稿は「行政命令」を用いる。大統領令については、中村絢子「アメリカ大統領のユニラテラルな（単独での）政策実現手段―大統領令を中心に―」『21世紀のアメリカ―総合調査報告書―』（調査資料2018-3）国立国会図書館, 2019.3, pp.25-40. <http://dl.ndl.go.jp/view/download/digidepo_11254533_po_20180304.pdf?contentNo=1> を参照。

⑵⑧　President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," 1997.10. Federation of American Scientists HP <https://fas.org/sgp/library/pccip.pdf>

⑵⑨　"Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators," *Federal Register*, vol. 63 no.150, August 5, 1998, pp.41804-41806. <https://www.govinfo.gov/content/pkg/FR-1998-08-05/pdf/98-20865.pdf>

護計画の策定に関わることが挙げられた。

重要インフラの保護施策を進める一方で、情報通信ネットワークの安全性及び信頼性の向上を図る目的で、2000年に政府が発表したのが「情報システム保護のための国家計画―対話への招待」[30]である。同計画において提示されたプログラムは、①重要なインフラ資産及び相互依存関係を確認し、脆弱性に対処する、②攻撃及び不正侵入を検出する、③重要な情報システムを保護するために情報収集能力及び法執行能力を高める、④攻撃警告・情報をタイムリーな形で共有する、⑤攻撃に迅速に対応し、システムを素早く再構築、復旧できる機能を備える、⑥プログラム①～⑤をサポートする研究開発を強化する、⑦適切な人数の情報セキュリティ専門家を育成・雇用する、⑧国民にサイバーセキュリティ改善の必要性を認識させるための啓蒙活動を行う、⑨プログラム①～⑧をサポートする法律を整備し、予算を確保する、⑩計画の全ての場面において、国民の市民的自由、プライバシーに対する権利、所有データの保全に対する権利の完全な保護を確保する、であった。

2　ブッシュ政権時（2001.1.20-2009.1.20）のサイバーセキュリティ強化策

(1) 国土安全保障国家戦略等

政権交代後の2001年9月11日に米国で発生した同時多発テロ事件[31]により、米国民の間で安全、防衛の重要性に対する認識が更に高まると、重要インフラ保護が国土安全保障[32]戦略の重要分野の1つとして明確に位置付けられた。同時多発テロ事件以前から、政府関係者には、重要インフラとシステムがサイバー攻撃に対してもろいものだという認識があり、国家安全保障電気通信諮問委員会（National Security Telecommunications Advisory Committee: NSTAC）[33]の主要メンバーは、国家の情報システムが侵入や攻撃の危険に耐えられないものであることをクリントン大統領に伝えていた[34]。また、中央情報局（Central Intelligence Agency: CIA）は、特に電気通信インフラに対するテロの脅威が現実に起こり得ると考え、サイバーセキュリティとサイバーテロに対する問題対処の提案を繰り返し、脅威に関する評価を求めていた。

ブッシュ（George W. Bush）大統領は、2002年7月に「国土安全保障国家戦略」[35]を公表した。同戦略は、国土安全保障の戦略目的として、①米国内におけるテロ攻撃の防止、②テロに対する脆弱性の低減、③攻撃によるダメージの最小化と攻撃を受けた後の復旧、を挙げた。また、

⑶⓪ White House, “National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue,” 2000. Federation of American Scientists HP <https://fas.org/irp/offdocs/pdd/CIP-plan.pdf>

⑶① 民間航空機4機がハイジャックされ、そのうちの2機がニューヨークの世界貿易センタービルに衝突、1機がワシントンの国防省に突入、1機がピッツバーグ郊外に墜落し、約2,800人が死亡・行方不明となった事件（外務省領事局邦人テロ対策室　前掲注⑵⑸, p.35.）。

⑶② 米国独自の概念と考えられる「国土安全保障」（homeland security）は、後述する「国土安全保障国家戦略」において、「米国内のテロリストの攻撃を防止し、米国のテロへの脆弱性を低減させ、行われた攻撃からの損害を最小化して復旧させる協調的な国家努力」と定義されている（Office of Homeland Security, “National Strategy for Homeland Security,” 2002.7, p.2. Department of Homeland Security HP <https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf>）。

⑶③ 1982年に設立され、現在は後述する国土安全保障省（DHS）に所属する。信頼性が高く、安全で、復旧力のある通信を米国が維持できるよう、大統領に勧告を行う役割を持つ。メンバーは、最大30名で、IT業界、通信業界を代表する者として指名される（“President’s National Security Telecommunications Advisory Committee Charter.” *ibid*. <https://www.dhs.gov/sites/default/files/publications/NSTAC%20Charter%20Renewal%20CMOts_filed%2013NOV2017.pdf>）。

⑶④ 以下の本段落の記述については、情報処理推進機構「電力重要インフラ防護演習に関する調査　報告書」2004.8, p.18. <https://www.ipa.go.jp/security/fy15/reports/infra/documents/infra_2004.pdf> を参照。

⑶⑤ Office of Homeland Security, *op.cit*.⑶②

同戦略では、その目的達成における重要分野が明らかにされており、重要分野の 1 つとして「重要インフラと資産の保護」が挙げられた。同戦略については、2007 年 10 月に改訂版[36]が公表されているが、そこでは、①テロ攻撃を防止・妨害する、②米国民、重要インフラ、主要資源を保護する、③発生したインシデントに対応し、復旧を図る、④長期的な成功を確実にするための基盤を強化し続ける、という目標が掲げられた。

国土安全保障体制の再編を目的として 2002 年 11 月に成立した「2002 年国土安全保障法」[37]に基づき、2003 年 1 月 24 日に国土安全保障活動の統括組織である国土安全保障省（Department of Homeland Security: DHS）が発足した。また、2002 年国土安全保障法の Subtitle B に「2002 年重要インフラ情報法」（Critical Infrastructure Information Act of 2002: CIIA）の規定が設けられたことにより、政府と重要インフラの運営企業との間で情報セキュリティに関する情報が共有されるようになった。その際、重要インフラの運営企業が政府に情報を提供すると、当該情報が「情報自由法」（Freedom of Information Act）[38]における情報開示請求の対象となって開示されてしまう懸念が生じたため、CIIA においては、当該企業が政府に提出する情報が「重要インフラ情報」（critical infrastructure information）に指定された場合は、情報自由法における情報開示請求の適用除外とする規定（6 U.S.C. § 133 (a)(1)(A)）が置かれた[39]。

(2) 原子力発電所に対する 2003 年のサイバーインシデント等

2003 年 1 月 25 日、オハイオ州のデービス・ベッセ原子力発電所のシステムに、VPN 接続を介してワーム型不正プログラム[40]「WORM_SQLP1434」（通称「Slammer」）が侵入し、SCADA[41]システムが約 5 時間、炉心プロセス・コンピュータ[42]が約 6 時間停止するインシデントが発生した[43]。他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。Slammer は、マイクロソフト社のデータベース管理システム「SQL Server 2000」の脆弱性を利用して、サーバーのデータ一時記憶領域に侵入後、ネットワーク上に大量のパケット（データの集合体）を送信してネットワーク機器等をダウンさせた。発電所のサーバーは、ファイアウォールにより外部ネットワークと遮断されていたが、ファイアウォール内部のネットワークに接続されていた外部コンサルタント会社のパソコンが感染源となっていた。Slammer に対応するた

⑶6 Homeland Security Council, “National Strategy for Homeland Security,” 2007.10. Department of Homeland Security HP <https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf>

⑶7 Homeland Security Act of 2002, P.L.107-296. <https://www.congress.gov/107/plaws/publ296/PLAW-107publ296.pdf>

⑶8 1966 年に成立し、1967 年に施行された法律（P.L.89-487）で、行政機関の情報公開について規定している（行政管理研究センター「諸外国における情報公開制度に関する調査研究　報告書」2019.3, pp.3-54. 総務省 HP <http://www.soumu.go.jp/main_content/000628852.pdf>）。

⑶9 永野秀雄「米国の重要インフラに関するサイバーセキュリティとセキュリティ・クリアランス法制（上）」『人間環境論集』19 巻 1 号, 2018.12, p.19. 法政大学学術機関リポジトリ HP <https://hosei.repo.nii.ac.jp/?action=repository_uri&item_id=21926&file_id=22&file_no=1>

⑷0 自身を複製して他のシステムに拡散する性質を持ったマルウェア。感染対象（ファイル、他のプログラム）のない単体のプログラムとして動作する点でウイルスとは異なる。

⑷1 「Supervisory Control And Data Acquisition」の略称で、製造や産業の現場でプロセス制御と集中監視を行う。

⑷2 発電所において、運転中の原子炉の中性子束分布や水温、制御棒位置などを監視し運転データとして記憶装置に記録し、その記録された運転データを用いて、実測値に合うように計算値を補正する学習機能を備えたコンピュータ（吉岡研一「使用済燃料輸送および貯蔵機器の臨界安全設計方法」『特許公報』2011.3.9. <https://patents.google.com/patent/JP4649122B2/ja>）。

⑷3 以下の本段落の記述については、情報処理推進機構セキュリティセンター「重要インフラの制御システムセキュリティと IT サービス継続に関する調査」2009.3, pp.22-23. <https://www.ipa.go.jp/files/000025097.pdf> を参照した。

めの SQL Server 2000 のパッチ(44)は公開済みであったが、攻撃を受けた発電所のシステムには適用されていなかった。

このような状況の中で政府は、2003 年 2 月に、2002 年の国土安全保障国家戦略に基づく政策ペーパーとして、「重要インフラ及び主要資産の物理的保護のための国家戦略」(45)を公表した。同戦略において示された目標は、①国家レベルの公衆衛生・安全、ガバナンス、経済、国家安全保障等にとって最も重要なインフラと資産の保護を保証すること、②タイムリーな警告を行うことにより、差し迫った脅威に直面しているインフラと資産の保護を保証すること、③連邦政府、州・地方政府及び民間部門が管理するインフラと資産をより適切に保護する協力環境を整えることにより、テロリストのターゲットになる可能性のある他のインフラと資産の保護を保証すること、であった。

(3) 国土安全保障大統領令 7 号等

ブッシュ大統領は、2003 年 12 月 17 日に、国土安全保障大統領令 7 号「重要なインフラの識別、優先順位及び保護」(HSPD-7)(46)を発出した。HSPD-7 は、重要インフラ及び主要資産を特定して優先順位を付け、テロリストの攻撃から保護するための連邦政府機関の国家政策を確立するものである。HSPD-7 は、DHS 長官に米国の重要インフラ及び主要資産の保護を強化するための国家的施策全般の調整を行う責任を負わせ、DHS がサイバーセキュリティの中核的存在としての役割を果たし続けられるようにすることを求めた。また、連邦政府機関は、各々が所有・管理する重要インフラの保護計画をまとめ、行政管理予算局（Office of Management and Budget: OMB）長官に提出することとされた。

2006 年 6 月、DHS は、OMB 長官に提出された各連邦政府機関の重要インフラ保護計画を基に、重要インフラを保護するためのリスク管理の枠組みを定めた「国家インフラ保護計画」(National Infrastructure Protection Plan: NIPP)(47)を策定した。同計画は、2009 年 1 月、2013 年 12 月に改訂されており(48)、2006 年の計画は第 1 次計画ということになる。第 1 次計画は、米国経済と国家安全保障はグローバルなサイバーインフラに大きく依存しているとの認識の下、DHS、分野別担当政府機関（Sector Specific Agencies: SSAs）、民間のインフラ所有者・運営者の各々が関与する分野を連携させ、また、電気通信部門と情報技術部門のパートナーシップを進めることにより、サイバーリスクの低減とサイバーセキュリティの強化を図るとした。

(4) 包括的全米サイバーセキュリティ・イニシアティブ

2008 年 1 月 8 日には、サイバーセキュリティ戦略の枠組みとなる「包括的全米サイバーセ

---

(44) コンピュータにおいてプログラムの一部分を更新してバグ修正や機能変更を行うためのデータ。

(45) White House, “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,” 2003.2. Homeland Security Digital Library HP <https://www.hsdl.org/?view&did=1041>

(46) “Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,” 2003.12.17. Department of Homeland Security HP <https://www.dhs.gov/homeland-security-presidential-directive-7>

(47) U.S. Department of Homeland Security, “National Infrastructure Protection Plan,” 2006. <https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf>

(48) 2009 年の第 2 次計画については、U.S. Department of Homeland Security, “National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency,” 2009. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf> を、2013 年の第 3 次計画については、U.S. Department of Homeland Security, “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,” 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf> を参照。

キュリティ・イニシアティブ」（Comprehensive National Cybersecurity Initiative: CNCI）が、国家安全保障大統領令 54 号／国土安全保障大統領令 23 号（NSPD-54 / HSPD-23）として発出された。CNCI に関する情報は基本的に機密扱いで、2008 年には公開されなかったが(49)、政権交代後の 2010 年 3 月に、機密扱いが一部解除され、概要版(50)が公表された。概要版では、①今日の差し迫った脅威に対する最前線の防衛を確立する、②あらゆる種類の脅威から防御する、③将来のサイバーセキュリティ環境を強化する、という 3 つの目標と、12 のイニシアティブ（取組）が明らかにされている。12 のイニシアティブは、①連邦政府機関のネットワークを信頼できるインターネット接続を備えた単一のネットワークとして管理する、②全ての連邦政府機関に侵入検知システムを装備する、③全ての連邦政府機関への侵入防止システムの装備を促進する、④研究開発（R&D）の取組を調整・変更する、⑤状況認識を強化できるよう現在あるサイバー情報集約機関を結合する、⑥政府全体のサイバー防諜計画を策定・実行する、⑦機密情報を扱うネットワークのセキュリティを強化する、⑧サイバー教育を拡大する、⑨永続的な技術開発戦略及びプログラムを定め、展開する、⑩永続的な抑止戦略とプログラムを定め、展開する、⑪グローバルなサプライチェーン（製品やサービスの提供において事業者から消費者に至る一連の流れ）のリスク管理のための多面的なアプローチを展開する、⑫サイバーセキュリティを重要インフラの領域まで拡張するための連邦政府の役割を定める、である。

3　オバマ政権時（2009.1.20-2017.1.20）のサイバーセキュリティ強化策

(1) サイバー空間政策レビュー等

オバマ（Barack Obama）大統領は、2009 年 5 月に、自ら組み立て直したサイバーセキュリティ戦略を「サイバー空間政策レビュー」(51)の形で公表した。同レビューは、実施すべき行動計画を、短期（10 項目）（表 1 を参照）と中期（14 項目）（表 2 を参照）に分けて整理している。

短期行動計画で挙げられた項目については、2011 年 5 月 12 日に政府報告書「政府のサイバーセキュリティ政策の成果」(52)が公表され、全て実施済みと報告されている。例えば、短期行動計画の最初に挙げられていたサイバーセキュリティ政策担当官として、2009 年 12 月にサイバーセキュリティ調整官（Cybersecurity Coordinator）が設置され、初代調整官としてシュミット（Howard Schmidt）氏が就任した(53)。また、8 番目に挙げられた項目については、2010 年 9 月に「全米サイバーインシデント対応計画」（National Cyber Incident Response Plan: NCIRP）(54)が策定され

---

(49)　ワシントンポスト紙は、2008 年当時、国家情報長官府（Office of the Director of National Intelligence: ODNI）に設けられるタスクフォースが、政府のコンピュータ・システムに対するサイバー攻撃の原因を特定するための対応を調整し、その対応の一環として、DHS はシステム保護に取り組み、国防省は侵入者に対する反撃戦略を考案すると報じていた（Ellen Nakashima, “Bush Order Expands Network Monitoring,” *Washington Post*, 2008.1.26. <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html>）。

(50)　U.S. Executive Office of the President, “The Comprehensive National Cybersecurity Initiative,” 2010.3. Homeland Security Digital Library HP <https://www.hsdl.org/?view&did=28609>

(51)　“Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” [2009]. U.S. Department of Energy HP <https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf>

(52)　White House, Office of the Press Secretary, “FACT SHEET: The Administration’s Cybersecurity Accomplishments,” 2011.5.12. <https://obamawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments>

(53)　“Welcoming the New Cybersecurity Coordinator,” 2009.12.22. U.S. Department of Homeland Security HP <https://www.dhs.gov/blog/2009/12/22/welcoming-new-cybersecurity-coordinator>

(54)　U.S. Department of Homeland Security, “National Cyber Incident Response Plan: Interim Version,” 2010.9. <https://federalnewsnetwork.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf>

表１　「サイバー空間政策レビュー」において示された短期行動計画の主な内容

1	米国のサイバーセキュリティ政策・活動の調整を担当するサイバーセキュリティ政策担当官を指名する。国家安全保障会議（National Security Council: NSC）と国家経済会議（National Economic Council: NEC）のスタッフを兼務するサイバーセキュリティ政策担当官の指示の下で、サイバーセキュリティ関連の戦略・政策の省庁横断的な展開を調整するための強力な担当部門を NSC 内に設ける。
2	情報通信のインフラを保護するため、大統領の承認を得た最新の国家戦略を用意する。同戦略には、包括的全米サイバーセキュリティ・イニシアティブ（Comprehensive National Cybersecurity Initiative: CNCI）の活動の継続的な評価が含まれる。
3	サイバーセキュリティを大統領の重要な優先管理事項の 1 つとして位置付け、パフォーマンスの評価手法を確立する。
4	NSC のサイバーセキュリティ担当部門においてプライバシーと市民の自由を担当する者を指名する。
5	政策策定プロセスにおいて特定された優先度の高いサイバーセキュリティ関連の問題に関して省庁横断的な法的分析を実施するため、適切な省庁横断的仕組みを構築する。連邦政府全体のサイバーセキュリティ関連活動に対する省庁の役割、責任等を明確にする一貫した統一的な政策ガイダンスを策定する。
6	サイバーセキュリティを高めるため、全国的な啓発活動と教育キャンペーンを開始する。
7	国際的なサイバーセキュリティ政策の枠組みにおける米国政府の立場を高め、サイバーセキュリティに関連する幅広い活動、政策、機会に対処するイニシアティブを策定するため、国際的な協力関係を強化する。
8	サイバーセキュリティ・インシデント対応計画を準備する。また、最大限の成果を上げるための資源の合理化、調整、提供に向け、官民の協力関係を強化するための対話を開始する。
9	大統領府（Executive Office of the President: EOP）の組織同士で協力し、デジタル・インフラのセキュリティ、確実性、復元力、信頼性を強化する可能性のある革新的な技術に焦点を当てた研究開発戦略のための枠組みを構築する。また、ツールの開発、理論のテスト、実行可能な解決策の確認を促進するための情報に研究者のコミュニティがアクセスできるようにする。
10	プライバシーと市民の自由の利益に配慮したサイバーセキュリティ・ベースの管理ビジョン・戦略を構築し、国全体のプライバシー強化技術を高める。

（出典）“Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” [2009], p.37. U.S. Department of Energy HP <https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf> を基に筆者作成。

表２　「サイバー空間政策レビュー」において示された中期行動計画の主な内容

1	サイバー運用のための法律の解釈、政策・権限の適用に関する省庁間の不一致の解決プロセスを改善する。
2	サイバーセキュリティの目標追求に当たっては、行政管理予算局（Office of Management and Budget: OMB）のプログラム評価の仕組みを使用し、各省庁への予算配分が実績に基づいたものとなるようにする。
3	情報化時代の経済において国全体の競争力を維持するため、主要な教育プログラムと研究・開発に対する支援を拡大する。
4	連邦政府内のサイバーセキュリティの専門家について、勧誘及び保持を含めた雇用及び育成の強化を図る戦略を策定する。
5	戦略的警告を受け、状況を認識し、インシデント対応能力を通知するための最も効率的かつ効果的な仕組みを決定する。
6	リスク管理上の判断、復旧計画、研究・開発の優先順位決定に使える一連の脅威シナリオと指標を開発する。
7	サイバーインシデントの防止、検出、対応を支援するための政府と民間部門の間の手順を整える。
8	サイバーセキュリティ関連情報の共有方法を整え、プライバシーと情報の占有に関する懸念に対処するとともに、情報共有を双方にとって有益なものとする。
9	ネットワークの中立性を確保しながら、自然災害、危機又は紛争が起こったときに緊急通信機能を使用可能にするための解決法を考案する。
10	主要な同盟国とのネットワーク・インシデント及び脆弱性に関する情報共有を拡大し、市民の自由とプライバシーの権利を保護しながら、経済的利益と安全上の利益を改善する二国間・多国間協定を追求する。
11	研究・開発における革新の迅速な実現に向けた経路及び誘因を作るため、学術研究所と産業研究所の間の協力を奨励する。
12	国内及び国際的標準化団体の目標を定めるため、インフラの目的及び研究・開発の枠組みを使う。
13	価値の高い活動（例えば、電力の流れを供給側・需要側の両方から制御して最適化するスマートグリッド）のために管理システムを相互運用可能とする仕組みを構築し、相互オンライン取引のための信用体制を確立し、プライバシー保護を強化する。
14	政府調達戦略を刷新し、安全で復旧力のあるハードウェア及びソフトウェア製品、革新的なセキュリティ技術、安全に管理されたサービスの市場インセンティブを改善する。

（出典）“Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” [2009], p.38. U.S. Department of Energy HP <https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf> を基に筆者作成。

た。NCIRP は、日々発生するサイバーインシデントへの国の対応、事業者が対応システムを運用する能力を全国的に平準化するよう調整するための施策の戦略的方向性を定めた。

(2) 発電所に対する 2012 年のサイバーインシデント

2012 年には、米国の 2 つの発電所で USB メモリのマルウェア感染が確認されている。1 つは、発電所の従業員が、自らの USB メモリに不具合が生じたため、IT 担当者に USB メモリの検査を求めて発覚したものである(55)。この従業員は、管理システム設定のバックアップを取るため、普段から USB メモリを使っていた。IT 担当者がセキュリティソフトをアップデートして

(55)　以下、本段落における記述は、“Malware Infections in the Control Environment,” *ICS-CERT Monitor*, 2012.10-12, p.1. <https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf> を参照した。

検査したところ、3 件の問題が見つかり、うち 1 件は高度な機能を持った既知のマルウェアであった。発電所の求めに応じ、DHS の産業用制御システム・サイバー緊急対応チーム（ICS-CERT）が問題が発覚した USB メモリが使われていた機器を検査したところ、管理業務運用にとって重要なエンジニアリング・ワークステーション 2 台でマルウェア感染が見つかり、駆除が行われた。

10 月には、電力事業者から、タービン制御システムがマルウェアに感染し、ネットワーク上のコンピュータ約 10 台が影響を受けたインシデントが報告された(56)。調査・分析の結果、外部の技術者がソフトウェアのアップデートを行うために使った USB メモリが、マルウェア「Mariposa」に感染していたことが判明した。この感染により、システムをアップデートするために休止していた発電所の再稼働は 3 週間あまり遅れた。ICS-CERT は、重要インフラの所有者・運営者に対し、セキュリティソフトのウイルス定義（ウイルスの特徴を記録したデータで、ウイルスの検出に使われる）を常に最新のものにする、ウイルスに対するパッチを適正に管理システムに適用する、リムーバブルメディア（補助記憶装置の記録媒体について、その媒体が機器本体から容易に取り外すことのできるもの）の使用を制限するという基本的なセキュリティ・ポリシーを策定し、実施することを強く求めた。

(3) 重要インフラのサイバーセキュリティ向上のためのフレームワーク等

オバマ大統領は、二期目に入ると、重要インフラのセキュリティ保護に向けて官民の情報連携の強化を図ることを重視し、急速に増大するサイバー攻撃の脅威に対応するための法整備を議会に求める一般教書演説(57)を行った 2013 年 2 月 12 日に、重要インフラのサイバーセキュリティ強化に関する行政命令 13636 号（EO-13636）(58)及び重要インフラのセキュリティと復旧力に関する大統領政策指令 21 号（President Policy Directive / PPD-21）(59)を発出した。

EO-13636 は、行政機関に対し、①テクノロジーに依存しない自発的なサイバーセキュリティの枠組みを構築すること、②サイバーセキュリティ慣行の採用を促進し、奨励すること、③サイバー脅威情報の共有の量、適時性、質を向上させること、④重要インフラを保護するため、全てのイニシアティブにプライバシーと市民の自由の強力な保護を組み込むこと、⑤サイバーセキュリティを促進するため、使用可能な既存の規制の活用を検討することを指示した(60)。

PPD-21 は、重要インフラの予期せぬ事態からの復旧力(61)を高めるため、行政機関に対し、①インフラをほぼリアルタイムで機能させるため、物理的、サイバー上の両面から対処できるよう、状況把握能力を向上させること、②連鎖的なインフラ障害の発生を想定すること、③官民

---

(56) 以下、本段落における記述は、“Virus Infection at an Electric Utility,” *ICS-CERT Monitor*, 2012.10-12, p.2 を参照した。

(57) “Remarks by the President in the State of the Union Address,” 2013.2.12. White House President Barack Obama HP <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/remarks-president-state-union-address>

(58) “Executive Order 13636 of February 12, 2013, Improving Critical Infrastructure Cybersecurity.” govinfo HP <https://www.govinfo.gov/content/pkg/DCPD-201300091/pdf/DCPD-201300091.pdf>; ローラーミカ「【アメリカ】サイバーセキュリティに関する大統領令」『外国の立法』No.255-2, 2013.5, pp.2-3. <http://dl.ndl.go.jp/view/download/digidepo_8205972_po_02550201.pdf?contentNo=1>

(59) “Presidential Policy Directive/PPD–21 of February 12, 2013, Directive on Critical Infrastructure Security and Resilience.” govinfo HP <https://www.govinfo.gov/content/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf>

(60) U.S. Department of Homeland Security, “Executive Order of (EO) 13636 Improving Critical Infrastructure Cybersecurity, Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience,” 2013.3. <https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf>

(61) 復旧力（resilience）とは、変化する状況を想定して準備を行い、変化する状況に適応し、混乱状態に耐え、そこから素早く復旧する能力のことで、意図的な攻撃、事故、又は自然に発生する脅威・インシデントに耐え、そこから復旧する能力が含まれている（*ibid.*）。

パートナーシップを評価し、成熟させること、④国家インフラ保護計画（NIPP）を更新すること、⑤包括的な研究開発計画を策定することを指示した。

これらの指示を受け、国立標準技術研究所（National Institute of Standards and Technology: NIST）[62]が2014年2月12日に発表したのが「重要インフラのサイバーセキュリティ向上のためのフレームワーク　バージョン1.0」[63]である。このフレームワークは、サイバーセキュリティの取組を行わせるためにビジネス上の誘因を与え、サイバーセキュリティ・リスクを組織のリスク管理プロセスの一部として理解させることを重視している。フレームワークは、フレームワーク・コア、フレームワーク・プロファイル、フレームワーク実装レベルの3つの部分で構成されている。フレームワーク・コアは、重要インフラ全体に共通するサイバーセキュリティに関する活動、成果、参考情報をまとめたもので、個々の組織が自らのプロファイルを作成する際の詳細なガイダンスを提供する。フレームワーク・プロファイルは、コアが示した基準、ガイドライン、慣行を個別の実施シナリオに合わせて整理したものである。フレームワーク実装レベルは、その組織のサイバーセキュリティ管理慣行がどの程度厳密で高度なものか示すものである。レベル1は「部分的である」、レベル2は「リスク情報を活用している」、レベル3は「繰り返し適用可能である」で、レベル4の「適応している」は、リスクが把握され、対応プロセスが確定・実行され、リスクの変化に追随できる状態で、最も高い評価である。このフレームワークは、2018年4月16日にバージョン1.1[64]にアップデートされている。

(4) 民間部門におけるサイバーセキュリティ情報の共有促進

オバマ大統領は、2015年2月13日に、「民間部門におけるサイバーセキュリティ情報共有の促進に関する行政命令13691号」（EO-13691）[65]を発出した。EO-13691は、①特定の部門・地域、特定の脅威や脆弱性への対応等の共通点を基に組織される情報共有分析機関（Information Sharing and Analysis Organizations: ISAOs）を設置すること[66]、②2002年国土安全保障法に基づき設立された国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center: NCCIC）がサイバー面のリスク及びインシデントに関する情報の共有について、ISAOsと継続的、協調的、包括的調整を行うこと、③ISAOsの設置促進に当たり、DHS長官に対し、当該分野特有の機関、独立規制機関、国家安全保障及び法執行機関等のサイバーセキュリティ活動の実施に責任を持つ他の連邦機関と協議することを命じた。

62　商務省傘下の連邦研究機関で、通信技術、サイバーセキュリティ等、国家的に重要な分野において米国の競争力を強化する活動を行っている（“Performance Evaluation (Impacts Studies).” National Institute of Standards and Technology HP <https://www.nist.gov/industry-impacts/performance-evaluation-and-economic-impact>）。

63　National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0,” 2014.2.12. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf>

64　National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” 2018.4.16. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>; 情報処理推進機構「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1版　米国国立標準技術研究所　2018年4月16日」<https://www.ipa.go.jp/files/000071204.pdf>

65　“Executive Order 13691 of February 13, 2015, Promoting Private Sector Cybersecurity Information Sharing.” govinfo HP <https://www.govinfo.gov/content/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf>; 岩澤聡「【アメリカ】サイバーセキュリティ情報の共有を促す大統領令」『外国の立法』No.263-1, 2015.4, pp.2-3. <http://dl.ndl.go.jp/view/download/digidepo_9218613_po_02630101.pdf?contentNo=1>

66　米国では、それ以前から、重要インフラの業界ごとに脅威や脆弱性に関する情報の共有・分析を行うISAC（Information Sharing and Analysis Center）が設置されていた。ISAOとISACを合わせ、現在、72の情報共有組織（地域組織15、産業／分野組織42、特定分野組織7、その他組織8）が設置されている（“Information Sharing Groups.” ISAO Standards Organization HP <https://www.isao.org/information-sharing-groups/>）。

2015 年 12 月には、「2015 年サイバーセキュリティ情報共有法」（Cybersecurity Information Sharing Act of 2015）[67]が成立し、サイバーセキュリティの脅威又はセキュリティの脆弱性を検出、防止又は軽減するため、民間事業者が、書面による同意を得て、他の民間事業者又は政府機関の情報システムの防衛策に関する情報を共有することが可能になった。これにより、DHS は、サイバー攻撃に係る情報共有が自動で行われる「サイバー脅威情報共有システム」（Cybersecurity Automated Indicator Sharing: AIS）の運用を開始した。重要インフラ事業者は、このシステムを使うことが義務付けられているわけではないが、AIS に加入している事業者には、同システムへの報告義務が課せられている。AIS で共有された情報は、サイバー脅威情報統合センター（Cyber Threat Intelligence Integration Center: CTIIC）で分析され、DHS を通して民間部門と共有される仕組みになっている[68]。

オバマ大統領は、2016 年 2 月 9 日には、自らの政権の 7 年間の努力の「冠石」（capstone）である「サイバーセキュリティ国家行動計画」[69]を実施するよう行政機関に指示した。具体的に求めたのは、①今後 10 年にわたり取るべき行動に関する提言を行う「サイバーセキュリティ向上委員会」（Commission on Enhancing National Cybersecurity）の設立、② 31 億ドルの情報技術近代化基金による政府 IT の近代化、③セキュリティ強化において省庁横断的な変革を推進する「連邦主席情報セキュリティ担当官」（Federal Chief Information Security Officer）のポストの新設、④パスワードに加えた認証システムの採用によるオンライン・アカウントの保護、⑤ 2017 会計年度に 190 億ドル強の予算のサイバーセキュリティ強化費用への充当、等である。

（5）米国におけるサイバーインシデントの調整に関する大統領政策指令 41 号等

オバマ大統領は、2016 年 7 月 26 日に、「米国におけるサイバーインシデントの調整に関する大統領政策指令 41 号」（PPD-41）[70]を発出した。PPD-41 では、サイバーインシデント対応策として連邦政府機関が実施する取組として、①脅威レスポンス：サイバーインシデントが発生したサイトにおける適切な法執行と捜査活動の実施、②アセット・レスポンス：資産保護、脆弱性軽減、サイバーインシデントの影響軽減を目的とした被害事業者に対する技術支援の提供、③インテリジェンス支援及び関連活動：脅威状況に関する情報の収集と共有、脅威の傾向・事象の分析、脅威の力を低下させる能力の向上等、が挙げられた。そして、連邦政府機関が攻撃を受けた場合、連邦政府機関は、追加措置として、④業務の継続性の確保、財政上の悪影響への対処、プライバシーの保護、法的要件の順守、職員又は影響を受ける個人とのコミュニケーションの確保、メディアや議会からの問合せへの対応等も行うこととされた。

2016 年 12 月 30 日、バーモント州の電力会社、バーリントン・エレクトリック・デパートメント（Burlington Electric Department）社は、前日の 29 日に、自社の送電網システムに接続されていないパソコン内で、DHS から警告を受けていたマルウェアを発見したが、顧客情報の漏洩はな

⑹ 「2016 年連結歳出法」（Consolidated Appropriations Act, 2016, P.L.114-113. <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>）の Division N である「サイバーセキュリティ法（Cybersecurity Act of 2015）」の Title 1 に当たる法律。

⑹ 笹川平和財団安全保障事業グループ「サイバー空間の防衛力強化プロジェクト　政策提言　“日本にサイバーセキュリティ庁の創設を！”」2018.10, p.15. <https://www.spf.org/global-data/20181029155951896.pdf>

⑹ White House, Office of the Press Secretary, “FACT SHEET: Cybersecurity National Action Plan,” 2016.2.9. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

⑺ “Presidential Policy Directive/PPD-41 of July 26, 2016, Directive on United States Cyber Incident Coordination.” govinfo HP <https://www.govinfo.gov/content/pkg/DCPD-201600495/pdf/DCPD-201600495.pdf>

かったという発表を行っている(71)。

4　トランプ政権時（2017.1.20-）のサイバーセキュリティ強化策

(1) 連邦ネットワーク及び重要インフラのサイバーセキュリティの強化

民主党から共和党への政権移行後も、サイバーセキュリティを重視する政策は継続された。トランプ（Donald J. Trump）大統領は、2017年5月11日に、行政命令13800号「連邦ネットワーク及び重要インフラのサイバーセキュリティの強化」（EO-13800）(72)を発出した。EO-13800においては、①連邦政府のネットワークのサイバーセキュリティ、②重要インフラのサイバーセキュリティ、③国家・国民のためのサイバーセキュリティが取り上げられている(73)。このうち、②重要インフラのサイバーセキュリティについては、a) 国家の重要インフラの所有者・運営者のサイバーセキュリティのリスク管理の取組を支援するため、その権限と機能を使用することは行政機関のポリシーである、b) 大きなリスクを抱えた重要インフラを支援する、c) 重要インフラ事業者によるサイバーセキュリティのリスク管理慣行の透明性を促進するための連邦政府の政策が十分かどうか調査する、d) インターネット及び通信システムの復旧力を向上させ、システムを自動化したことに伴い発生する脅威を劇的に低減するという目標に向け、適切な利害関係者による行動を促すための透明なプロセスを確保する、e) 停電が発生した場合の対応能力の評価を行う、f) 連邦政府関係機関は、サイバーセキュリティのリスク軽減に関する報告書を大統領に提出する、等の対応が記されている。

f) に従い、例えば、OMBは、2018年5月に「連邦サイバーセキュリティ・リスク決定報告書及び行動計画」（Federal Cybersecurity Risk Determination Report and Action Plan）(74)を公表した。連邦政府機関のサイバーセキュリティ・リスク管理のNISTのフレームワークへの準拠状況を76の指標を用いてOMBが評価した結果、96の連邦政府機関のうち71が、リスクのある又はリスクの高いサイバーセキュリティ・プログラムを運用していることが判明した。そのような状況を改善するため、OMBは、①連邦政府機関内のサイバーセキュリティ・リスクに対する認識を高め、取組に優先順位を付け、サイバーセキュリティ・リスクを管理するサイバー脅威フレームワークを実装する、②コストをコントロールし、資産管理を改善するため、IT及びサイバーセキュリティの能力を標準化する、③インシデントの検出及び対応能力を向上させるため、政府機関の安全運営センター（Secure Operations Center: SOC）を統合する、④改善された統制プロセス、繰り返し行われるリスク評価、政府機関に対して指導力を有するOMBの関与を通し、政府機関全体の説明責任能力を向上させる、としている。

---

(71) Neale Lunderville, “No Indication that Electric Grid or Customer Information Compromised,” 2016.12.30. Burlington Electric Department HP <https://www.burlingtonelectric.com/news/46>

(72) “Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” govinfo HP <https://www.govinfo.gov/content/pkg/DCPD-201700327/pdf/DCPD-201700327.pdf>; 永野前掲注(39), pp.61-73.

(73) EO-13800の内容、有識者の評価、影響については、中沢潔「トランプ政権におけるサイバーセキュリティ政策の現状」『ニューヨークだより』2017.9, pp.1-12. 情報処理推進機構 HP <https://www.ipa.go.jp/files/000061964.pdf>に詳しく記されている。

(74) Office of Management and Budget, “Federal Cybersecurity Risk Determination Report and Action Plan,” 2018.5. White House HP <https: //www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf>

(2) DHS のサイバーセキュリティ戦略等

2017 年 7 月 6 日、ニューヨーク・タイムズ紙は、DHS と連邦捜査局（Federal Bureau of Investigation: FBI）が発表した緊急共同報告書によると、同年 5 月以降、原子力発電所等のエネルギー施設のコンピュータ・ネットワークを狙ったハッキング行為が増加しており、カンサス州にあるウルフ・クリーク原子力発電所運営会社（Wolf Creek Nuclear Operating Corporation）に対するものは脅威レベルが高いと推測されること等を報じた(75)。

それらの状況も踏まえ、DHS は、2018 年 5 月 15 日に「サイバーセキュリティ戦略」（Cybersecurity Strategy）(76)を発表した。同戦略では、リスク管理アプローチについて 5 つの柱が設けられ、7 つの目標を達成することが目指されている（表 3 を参照）。

表３ 「サイバーセキュリティ戦略」における目標

柱 1：リスクの特定	目標 1	進化したサイバーセキュリティ・リスクの評価：進化した国家のサイバーセキュリティ・リスクに対する姿勢を理解し、リスク管理活動への情報提供、優先順位付けを行う。
柱 2：脆弱性の低減	目標 2	連邦政府の情報システムの保護：連邦政府機関の脆弱性を減らし、適切なレベルのサイバーセキュリティを確保する。
	目標 3	重要インフラの保護：主要な利害関係者と提携し、国家のサイバーセキュリティ・リスクが適切に管理されるようにする。
柱 3：脅威の縮小	目標 4	サイバースペースの犯罪使用の防止：国境を越えた犯罪組織や高度なサイバー犯罪者に対抗することにより、サイバー脅威を減らす。
柱 4：被害の軽減	目標 5	サイバーインシデントへの効果的な対応：コミュニティ全体の協調的な取組により、潜在的に重大なサイバーインシデントからの影響を最小限に抑える。
柱 5：サイバーセキュリティの効果の発揮	目標 6	サイバーエコシステム（サイバー技術と人と社会の調和が取れたシステム）の安全性と信頼性の強化：グローバルなサイバーセキュリティ・リスク管理の改善を可能にする政策と活動を支援する。
	目標 7	DHS のサイバーセキュリティ活動の管理方法の改善：統合され優先順位が付けられた方法で、DHS のサイバーセキュリティに関する取組を実施する。

（出典）U.S. Department of Homeland Security, “Cybersecurity Strategy,” 2018.5.15, p.3. <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf> を基に筆者作成。

目標 3 の「重要インフラの保護」において更に細かく設定された目標は、①重要インフラに対する重大な国家的リスクに対処するため、サイバーセキュリティの取組を成熟させる、②サイバー脅威指標、防御手段、その他のサイバーセキュリティ情報の共有を拡大し、改善する、③その分野特有の政府機関、規制当局、政策立案者が利用可能なサイバーセキュリティの機能と資源を改善する、である。

---

(75) Nicole Perlroth, “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and FBI. Say,” *New York Times*, 2017.7.6. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?referer=http://www.kansas.com/news/local/article160030764.html>

(76) U.S. Department of Homeland Security, “Cybersecurity Strategy,” 2018.5.15. <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>

(3) 国家リスク管理センターの創設

DHS は、2018 年 7 月 31 日、官民共同でサイバー防衛戦略のビジョンを策定するために開催した「国家サイバーセキュリティ・サミット」において、重要インフラの保護を目的とした「国家リスク管理センター」（National Risk Management Center: NRMC）を創設することを明らかにした(77)。NRMC が官民の共同活動を調整することにより、例えば、重要インフラの相互依存性を評価することによってリスク及び重要な機能に与える影響を特定することが可能になると考えられている(78)。また、グローバルに展開された情報通信技術のサプライチェーン・リスクに関する課題を特定し、対処法を考案するため、同年 10 月に設置が公表された情報通信技術サプライチェーン・リスク管理タスクフォース（Information and Communications Technology （ICT） Supply Chain Risk Management Task Force）(79)は、NRMC の支援の下で、重要な官民パートナーシップとして機能することが期待されている(80)。

(4) 国家サイバー戦略等

2018 年 9 月、サイバー空間の脅威から米国を守るための安全保障政策を強化した「国家サイバー戦略」（National Cyber Strategy）が発表された。国家サイバー戦略は、2017 年 12 月に策定された「国家安全保障戦略」(81)に基づき策定された。国家サイバー戦略は、オバマ前政権の防御主体の政策を転換し、外国からのサイバー攻撃に対抗して積極的に「攻撃的手段」をとっていくことも辞さない方針を表明したもので、ロシア、中国、イラン、北朝鮮について、サイバー攻撃を行うソフトウェアを使用し、米国及び同盟国の経済、民主主義を損ない、知的財産を盗み、民主的プロセスを妨げる敵対国家とみなしている(82)。

国家サイバー戦略においては、①ネットワーク、システム及びデータを保護することにより、国家を守る方策、②安全で繁栄的なデジタル経済を育成し、国内における強力なイノベーションを促進することにより、米国の繁栄を推進する方策、③同盟国及びパートナーと協力することで、悪意ある目的でサイバーツールを使用する人々を阻止し、必要な場合は処罰する米国の能力を強化することにより、平和と安全を維持する方策、④開放的で相互運用性があり、信頼性が高く、安全であるというインターネットの重要な特性を更に活かすため、米国の海外における影響力を高める方策、が示されている(83)。そして、国家安全保障会議（National Security Council: NSC）の職員は、国家サイバー戦略を実施するための適切なリソース（人員、予算等）計画の策定について、各省庁及び OMB と調整を図ることになっている。

また、同年 11 月には、DHS にサイバーセキュリティ・インフラセキュリティ庁（Cybersecurity

---

(77) “DHS Hosts Successful First-Ever National Cybersecurity Summit,” 2018.8.1. U.S. Department of Homeland Security HP <https://www.dhs.gov/news/2018/08/01/dhs-hosts-successful-first-ever-national-cybersecurity-summit>

(78) “National Risk Management Center.” Cybersecurity and Infrastructure Security Agency HP <https://www.cisa.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%2020181115_CISA%20v2.pdf>

(79) NRMC に関する説明文書（*ibid.*）では「Information and Communication Technologies (ICT) Supply Chain Risk Management Task Force」と表記されていた。

(80) “ICT Supply Chain Risk Management Task Force.” Cybersecurity and Infrastructure Security Agency HP <https://www.cisa.gov/sites/default/files/publications/19_0305_cisa_ICT-supply-chain-risk-management-task-force-fact-sheet.pdf>

(81) White House, “National Security Strategy of the United States of America,” 2017.12. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

(82) White House, “National Cyber Strategy of the United States of America,” 2018.9, p.2. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

(83) *ibid*., p.3.

and Infrastructure Security Agency: CISA）が設置された(84)。CISAは、国家のリスク・アドバイザーとして、官民にまたがるパートナーと共に今日の脅威を防ぎ、将来のためにより安全で復旧力のあるインフラを構築するための組織である。CISAには、①サイバーセキュリティ部：重要ネットワークのセキュリティを強化するため、連邦政府の「.gov」ドメインを保護し、民間部門の「.com」ドメインと協力する取組を主導する、②インフラストラクチャー部：重要インフラの所有者・運営者等が重要インフラのリスクを理解して対処するのに役立つ脆弱性評価を行い、新たな脅威に関する情報を提供し、業界パートナー等が資産、システム、ネットワークのリスクを管理するのを支援するためのツール・訓練を提供する、③緊急コミュニケーション部：重要インフラにおける緊急対応者と米国の安全、復旧力確保を担当する政府職員が使用する通信をサポートする、に加え、④国家リスク管理センター：米国の重要インフラに対する最も重大なリスクを特定して対処するための計画策定、分析、協力を行う、が置かれている(85)。

5　電力分野におけるサイバーセキュリティ強化策

電力については、サイバー攻撃を阻止するための要件が早い時期に設定された。近年は、壊滅的な停電や送配電におけるサプライチェーン・リスクも念頭に置かれるようになっている。

(1) FERCの「重要インフラ保護に必須の信頼性基準」等

電力に関しては、北米電力信頼度協会（NERC）の前身である北米電気信頼性評議会（North American Electric Reliability Council）が、2002年6月に、電力部門の重要施設を物理的及びサイバー上の脅威から保護するためのベスト・プラクティスをまとめた「電力部門のためのセキュリティ・ガイドライン」のバージョン1.0(86)を作成した。同資料では、脆弱性及びリスク評価、脅威への対応、緊急時計画、事業継続、物理的セキュリティ、サイバーセキュリティ等の項目について、目的、適用対象、ガイドライン等が示されており、サイバーセキュリティの項目は、更に、リスク管理、アクセス・コントロール、ファイアウォール、侵入検出に分けられていた。

サイバー攻撃に起因するものではないが、2003年8月14日に米国北東部とカナダ南東部で大規模停電が発生したこと(87)もあり、連邦エネルギー規制委員会（Federal Energy Regulatory Commission: FERC）から電力部門のサイバーセキュリティの信頼性基準（以下「電力サイバーセキュ

---

(84)　2018年11月16日に成立した「2018年サイバーセキュリティ・インフラセキュリティ庁設置法」（Cybersecurity and Infrastructure Security Agency Act of 2018, P.L.115-278. <https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf>）に基づき、DHSの国家防護プログラム局（National Protection and Programs Directorate: NPPD）を大幅に改組・拡充する形で設置された（廣瀬淳子「【アメリカ】サイバーセキュリティー・インフラセキュリティー庁設置」『外国の立法』No.278-2, 2019.2, pp.6-7. <http://dl.ndl.go.jp/view/download/digidepo_11239706_po_02780203.pdf?contentNo=1>）。

(85)　"ABOUT CISA." Cybersecurity and Infrastructure Security Agency HP <https://www.cisa.gov/about-cisa>

(86)　North American Electric Reliability Council, "Security Guideline for the Electricity Sector Version 1.0," 2002.6.14. Information Warfare Site HP <http://www.iwar.org.uk/cip/resources/nerc/Security%20Guidelines%20for%20the%20Electricity%20Sector%20-%20Version%201.pdf>

(87)　停電が発生したのは米国とカナダのエリー湖、オンタリオ湖周辺地域であった。停電電力は約6180万kW、被害者は約5000万人に上り、完全復旧までに2日以上を要した。被害額は米国で40億～100億ドルと推定されている。原因としては、①事業者の電力系統についての不十分な理解（事故が起きた場合に電力系統が安定的かどうかの事前のチェックが不十分等）、②事業者の不適切な状況把握（系統監視装置の故障、バックアップ及び再起動後のチェックの問題）、③事業者の不十分な樹木管理（樹木接触による送電線の切断）、④信頼度コーディネータ（広範囲にわたる系統の信頼度監視者）の不適切な状況判断（不完全な状態推定装置、入り組んだ監視体制等）、が指摘された（電力中央研究所「大停電、日本は大丈夫か―北米大停電最終報告書を踏まえて―」2004.6.9. <https://criepi.denken.or.jp/koko/powerline/data/final.pdf>）。

リティ標準」）を承認する権限を委譲されたNERCは、2006年3月に電力サイバーセキュリティ標準を策定した。電力サイバーセキュリティ標準は、基幹電力系統（Bulk Electric System: BES）（電力システムの中心となる送電・配電設備）の運用及びサポートに必要な電子情報の交換における安全性を確保し、重要なサイバー資産（端末、サーバー等）への物理的及びサイバー上の不正アクセスを阻止するための要件を確立するものである[88]。NERC加盟機関には同標準の順守義務があり、違反した場合には罰金が科せられる。電力サイバーセキュリティ標準は、2008年1月18日にFERCによって採択され、「重要インフラ保護に必須の信頼性基準」（FERC Order No.706）[89]として公表された。

FERC Order No.706で取り上げられた項目は、① CIP-002―重要サイバー資産の特定：リスク・ベースの評価手法[90]を用いて重要資産と重要サイバー資産を特定することが必要、② CIP-003―セキュリティ管理・制御：CIP-002に従って特定された重要サイバー資産を保護するため、セキュリティ管理・制御策を確定・実施することが必要、③ CIP-004―職員及び訓練：重要サイバー資産にアクセスできる職員の本人確認及び犯罪チェック、訓練が必要、④ CIP-005―電子的セキュリティ境界：電子的なセキュリティ境界とアクセスポイントの識別及び保護が必要、⑤ CIP-006―重要サイバー資産の物理的セキュリティ：電子的セキュリティ境界内の全てのサイバー資産が特定された物理的セキュリティ境界内に保持されることを保証する物理的セキュリティ計画を作成し、維持することが必要、⑥ CIP-007―システムのセキュリティ管理：重要サイバー資産として識別されたシステム及び電子的セキュリティ境界内の重要でないサイバー資産を保護するための方法、プロセス、手順を定めることが必要、⑦ CIP-008―インシデントの報告及び対応計画：重要サイバー資産に関連するサイバーセキュリティ・インシデントを特定、分類、対応、報告することが必要、⑧ CIP-009―重要サイバー資産の復旧計画：既存の事業継続計画及び災害復旧計画の手法を用いて重要サイバー資産の復旧計画を策定することが必要、である[91]。

（2）NIAC報告書「大停電からの復興：国家の能力を強化する方法」

大統領の国家インフラ諮問会議（President's National Infrastructure Advisory Council: NIAC）[92]は、

88　JETRO「米国の電力セクターにおけるサイバーセキュリティについて」p.4. <https://www.jetro.go.jp/ext_images/jfile/report/07000733/us_security.pdf>

89　United States of America Federal Energy Regulatory Commission, "[Docket No. RM06-22-000; Order No. 706] Mandatory Reliability Standards for Critical Infrastructure Protection," 2008.1.18. <https://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf>

90　考え得る脅威シナリオを元に、対象システムに対してどのような被害が考えられるかを分析した上で、セキュリティ対策を検討する手法。

91　CIPは「Critical Infrastructure Protection」の略。なお、サイバーセキュリティとは関係が薄い等の理由から、同文書で取り上げられなかった項目は、「CIP-001―労働者による妨害（サボタージュ）の報告」、「CIP-010―設定変更管理及び脆弱性評価」、「CIP-011―情報保護」、「CIP-012―制御センター間のコミュニケーション」、「CIP-013―サプライチェーンのリスク管理」、「CIP-014―物理的セキュリティ」（North American Electric Reliability Corporation, "CIP Standards." <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>）。

92　2001年10月に発出された行政命令13231号「情報時代の重要インフラの保護」（EO-13231）（"Executive Order 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age." govinfo HP <https://www.govinfo.gov/content/pkg/WCPD-2001-10-22/pdf/WCPD-2001-10-22-Pg1485.pdf>）に基づき設置された。民間事業者と州・地方政府の幹部によって構成され、物理的及びサイバー上のリスクを軽減し、国家の重要インフラ部門のセキュリティと復旧力を向上させる方法についてホワイトハウスに助言を行う（"National Infrastructure Advisory Council." U.S. Department of Homeland Security HP <https://www.dhs.gov/national-infrastructure-advisory-council>）。

2018 年 12 月、「大停電からの復興：国家の能力を強化する方法」と題する報告書[93]を発表した。同報告書は、既存の国家計画、対応資源、相互協力戦略では「壊滅的な停電」に対処できず、新たな国家的対応が必要だという認識を明らかにした。同報告書で想定されている「壊滅的な停電」とは、①相互支援協力計画では対応不可能な近年の経験を超えた規模の被害をもたらす、②通告なしで攻撃されることが多く、サイバー攻撃と物理攻撃が同時に行われることによって複雑化する可能性がある、③インフラが物理的に損傷した場合、数週間から数か月の長期にわたって続く、④複数の州又は地域にわたる広範な地理的領域に影響を及ぼし、数千万人に被害を与える、⑤重要インフラ（上下水道システム、通信、輸送、医療、金融サービス等）の運用状況を悪化させる深刻な連鎖的障害を引き起こす、ものである。

同報告書は、このような壊滅的な停電に備え、迅速な復旧を可能にするには、特別な官民の行動が必要になると考え、①壊滅的な停電に備え、対応し、復旧するための国家的アプローチを策定し、政府、産業からコミュニティ、個人に至る全てのレベルにおいて取られる行動に必要な連邦のガイダンス、資源、インセンティブを提供する、②重要インフラ全体における連鎖的な障害発生が復旧と復興に与える影響に関する理解を深める、という 2 つの包括的方法で対応する方針を示した。その上で、同報告書は、7 つの提言を行っている（表 4 を参照）。

表４　「大停電からの復興：国家の能力を強化する方法」における提言

提言		リーダー	サポート機関
1	壊滅的な停電や電力系統の安全性を妨げる緊急事態が発生したときに行使される連邦政府機関の権限を明確化し、閣僚レベルのリーダーシップと意思決定プロセスを明確に定める。	DHS 長官	エネルギー省（主）、国防省等
2	壊滅的な停電の影響を軽減し、復旧を図るために、インフラ部門、都市、コミュニティ、農村地域が必要とする標準的施策を連邦政府が策定する。	DHS 長官	エネルギー省（主）、NRMC、NIST 復旧プログラム、経済諮問委員会等
3	コミュニティ・エンクレイブ（周辺の人口を確保し、健康と安全を維持し、居住者が所定の場所に避難できるようにするため、重要なサービス・資源を確保してあるエリア）を設定するため、州、準州、市等のために、ガイダンスを作成し、必要な資源を提供する。	DHS 長官	FEMA（主）、CISA（主）、エネルギー省、NIST 復旧プログラム
4	企業、非政府組織、州、地方政府等がこのレポートに書かれた提言を実施するのをサポートするため、財政的な支援を行うか、財政上・規制上の障壁を取り除く誘導策の策定・支援を行う。	財務長官	関連する省庁の長官（主）、連邦エネルギー規制委員会等
5	バックアップ資源と相互支援協力が尽きることにより、2 次的、3 次的な連鎖的障害を引き起こす一連の地域壊滅的停電に備えた演習を実施し、分野を超えたサプライチェーンと電力系統の復旧を遅らせるサイバーリスクの調査を行う。	エネルギー省長官	FEMA（主）、NERC（主）、DHS、連邦エネルギー規制委員会
6	全ての重要な天然ガス輸送パイプラインのインフラが、壊滅的な停電が発生してもサービスを継続し、ブラックスタート発電（外部電源によって発電された電気を受電することなく、停電解消のための発電を行うこと）を迅速に支援する能力を維持可能な形に設計され、それに備えた訓練を実施していることを保証する。	エネルギー省長官	運輸省（主）、運輸安全委員会、NERC、連邦エネルギー規制委員会
7	重要なサービスの復旧を支援し、インフラの所有者・運営者、緊急事態の対応者、政府機関のリーダーが連絡を取れるよう、全ての部門において相互運用可能で、自己給電式で、あらゆる危険から防護可能な柔軟で適応力のある緊急通信システムを開発又はサポートする。	DHS 長官	国防省（主）、エネルギー省、連邦通信委員会

（注）「サポート機関」欄の「（主）」は、主たるサポート機関という意味。
（出典）President’s National Infrastructure Advisory Council, “Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation,” 2018.12, pp.7-21. U.S. Department of Homeland Security HP <https://www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf> を基に筆者作成。

(3) NERC 報告書「BES のサプライチェーンにおけるサイバーセキュリティ・リスク」

NERC は、2019 年 5 月 17 日、基幹電力系統（BES）のサプライチェーン[94]のサイバーセキュリティ・リスクについて分析を行い、対応策を提言した報告書「BES のサプライチェーンにおけるサイバーセキュリティ・リスク」[95]を発表した。NERC の評議委員会は、2017 年 8 月にサプライチェーン標準（新規の CIP-013-1[96]等）を採択した際、NERC に対し、サプライチェーン標準の対象となっていない影響度が低い資産に関連するものを含むサプライチェーンのサイバーセキュリティ・リスクの性質と複雑性について調査し、判明した問題に対し最適な対応策を講じるよう指示していた。同報告書は、その指示に従い、対応策の提言を行ったものである。

主な提言は、①電子アクセス制御・監視システム及び物理的アクセス制御システムに係る潜在的なサプライチェーン・リスクを評価し、影響度が高・中レベルの BES サイバーシステムに関連するこれらの制御システムをサプライチェーン標準に含めるよう同標準を改定する、② NERC は、影響度が低い BES サイバーシステムに対するサプライチェーン・リスク管理計画を事業者が自発的に適用することを支援するガイドラインを策定する、③サイバー資産によりリスク・レベルは異なるため、NERC は、保護されたサイバー資産を事業者がケースバイケースで評価することを支援するガイドラインを作成する、④事業者がサプライチェーン・リスク管理計画を策定する際、北米送電フォーラム（North American Transmission Forum）、米国公共電力協会（American Public Power Association）、全米農村電気協同組合（National Rural Electric Cooperative Association）、北米発電フォーラム（North American Generator Forum）が採用している業界慣行やガイドラインを参照することを推奨する、である[97]。

6　原子力発電のためのサイバーセキュリティ規則

米国では、重要インフラとして、電力を含む「エネルギー」とは別建てで「原子炉及び核燃料・核廃棄物施設」が指定されている（大統領政策指令 21 号）。そこで、最後に、原子力発電におけるサイバーセキュリティ対策のベースとなっている規則について補足的説明を行う。

2001 年の同時多発テロ事件を受け、原子力規制委員会（Nuclear Regulatory Commission: NRC）が命令「原子力発電所の暫定保障措置及びセキュリティ補償対策」（Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants）（EA-02-026）[98]を発出する等のセキュリティ強化策

---

(93) President's National Infrastructure Advisory Council, "Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation," 2018.12. U.S. Department of Homeland Security HP <https://www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf>

(94) BES に係るサプライチェーンに含まれるのは、需給制御機関、配電会社、発電所の所有者・運用者、信頼度コーディネータ、送電網の所有者・運用者。

(95) North American Electric Reliability Corporation, "Cyber Security Supply Chain Risks: Staff Report and Recommended Actions," 2019.5.17. <https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf>

(96) "CIP-013-1 - Cyber Security - Supply Chain Risk Management." North American Electric Reliability Corporation HP <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf>

(97) North American Electric Reliability Corporation, *op.cit.*(95), pp.v-vi.

(98) 2002 年 2 月に発出された。文書自体は非公開であるが、原子力発電所に対しサイバーセキュリティの脆弱性に対処するよう指示する内容が含まれていることは明らかにされている（Nuclear Regulatory Commission, "Regulatory Guide 5.71 (New Regulatory Guide): Cyber Security Programs for Nuclear Facilities," 2010.1, p.4. <https://www.nrc.gov/docs/ML0903/ML090340159.pdf>）。

が打ち出された(99)。それらは、原子力発電事業者に自主的な対応を求めるものであったが、2009年3月に、罰則を伴う規則「デジタル・コンピュータ並びにコミュニケーション・システム及びネットワークの保護」(10 CFR 73.54)(100)(以下「サイバーセキュリティ規則」)が定められ、原子力発電事業者のサイバーセキュリティへの対応が義務化された。

サイバーセキュリティ規則は、原子力発電事業者に、設計基礎脅威(Design Basis Threat)(101)に該当する脅威から、①安全関連機能及び安全上重要な機能、②セキュリティ機能、③サイト外との情報交換を含む緊急事態対応機能、④侵害された場合に①～③の機能に悪影響を及ぼす支援システム・設備に関連したデジタル・コンピュータ及びネットワーク等を適切に保護することを義務化した。想定されたサイバー攻撃は、①データ及び／又はソフトウェアの整合性又は機密性に悪影響を与えるもの、②システム、サービス及び／又はデータへのアクセスを拒否するもの、③OS、ネットワーク、関連設備の運用に悪影響を及ぼすもの、である。

原子力発電事業者は、①デジタル・コンピュータ並びにコミュニケーション・システム及びネットワークを分析してサイバー攻撃から保護する必要がある資産を特定し、②特定した資産を保護するためのサイバーセキュリティ・プログラムを策定、実施、維持し、③サイバーセキュリティ・プログラムを物理的保護プログラムの一部として組み込まなければならない。また、原子力発電事業者は、①サイバー攻撃を迅速に検出し、対応する能力を有し、②サイバー攻撃の影響を緩和し、③悪用された脆弱性を修正し、④サイバー攻撃により悪影響を受けたシステム、ネットワーク及び／又は設備を復旧する施策を盛り込んだサイバーセキュリティ計画(Cyber Security plan: CSP)を策定、実施、維持することも義務付けられた。

NRCは、2010年1月、原子力発電事業者がサイバーセキュリティ規則に記された要件を実施するための手引として、「原子力施設のためのサイバーセキュリティ・プログラム(Cyber Security Programs for Nuclear Facilities)」(RG 5.71)(102)を公表した。RG 5.71においては、セキュリティレベルの低いデジタル資産から高いデジタル資産へのデータ送信の禁止等の対応が示されている。また、RG 5.71には、原子力発電事業者のCSP策定を助けるため、「汎用的なCSPのテンプレート」(Generic Cyber Security Plan Template)が付されている。

NRCは、2015年7月に、新たな規則「サイバーセキュリティ・イベントの通報」(Cyber

---

(99) EA-02-026以外では、EA-03-086「放射線妨害に対する設計基礎脅威」(Design Basis Threat for Radiological Sabotage)(2003年4月)、NEI 03-12「セキュリティ計画、訓練・資格計画及び緊急時防護計画のテンプレート」(Template for the Security Plan, Training & Qualification Plan, Safeguards Contingency Plan)(原子力エネルギー協会、2004年)、NUREG/CR-6847「米国の原子力発電所のためのサイバーセキュリティ自己評価手法」(Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants)(2004年10月)、NEI04-04「原子炉のためのサイバーセキュリティ・プログラム」(Cyber Security Program for Power Reactors)(原子力エネルギー協会、2005年12月)等(Mario R. Fernandez Jr., ""Ask SME and Learn" NRC Cyber Security Regulatory Program Development." Nuclear Regulatory Commission HP <https://www.nrc.gov/docs/ML1333/ML13336A556.pdf>)。

(100) "§ 73.54 Protection of digital computer and communication systems and networks." *ibid*. <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html>

(101) 国際原子力機関(International Atomic Energy Agency: IAEA)の「核物質及び原子力施設の物理的防護に関する核セキュリティ勧告(INFCIRC/225/Rev.5)」においては、「不法移転又は妨害破壊行為を企てる恐れのある潜在的内部脅威者及び／又は外部からの敵対者の属性及び性格でこれに対して物理的防護システムが設計され、評価される。」と説明されている(内閣府政策統括官(科学技術政策・イノベーション担当)原子力政策担当室(原文:国際原子力機関)「【仮訳】IAEA核セキュリティ・シリーズNo.13　勧告文書　核物質及び原子力施設の物理的防護に関する核セキュリティ勧告(INFCIRC/225/Rev.5)」2012.6, p.41. 原子力規制委員会HP <https://www.nsr.go.jp/data/000125920.pdf>)。

(102) Nuclear Regulatory Commission, *op.cit.*(98)

security event notifications）（10 CFR 73.77）(103)を定め、原子力発電事業者に対し、サイバー攻撃を発見した場合、緊急時通報システム（Emergency Notification System: ENS）を通じて NRC 本部オペレーション・センター（NRC Headquarters Operations Center）に通報することを義務付けた。また、その順守を促すためのガイダンス（RG 5.83）(104)を公表した。

NRC は、RG 5.71 の改訂に向け、2018 年 8 月に改訂版の草案(105)を公表している。同草案は、2010 年の初版公表以降の運用経験から学んだ教訓、具体的には、10 CFR 73.54 への適合レベルを確認するマイルストーン(106)に関する検査、セキュリティに関するよくある質問（Security Frequently Asked Questions: SFAQs）プロセスで得られた追加的洞察、記録されたサイバー攻撃等を踏まえて作成された。

おわりに

現代人の生活・経済活動は電力に大きく依存しているため、電力が使えなくなった時の影響は大きい。近年の日本でも、2018（平成 30）年 9 月に発生した北海道胆振東部地震や、2019（令和元）年 9 月に襲来した台風 15 号等の自然災害による大規模停電を経験しており、被災者だけでなく多くの国民が電力の重要性を認識している。大規模停電は例として分かりやすいが、他の重要インフラに障害が発生した場合も社会的・経済的損失は大きい。サイバー攻撃により重要インフラ障害が引き起こされることを未然に防ぎ、万が一引き起こされた場合でも素早く復旧可能な環境を整えておくことは、安全保障上の優先順位が高い課題だと考えられる。

早い時期から重要インフラのサイバーセキュリティ強化に取り組んできた米国は、サイバー攻撃から重要インフラを保護するため、官民連携、情報共有を着実に進めている。例えば、インシデント情報の共有については、ISAO によるインシデント情報の収集（事業者との情報共有）→インシデント情報の DHS との共有（NCCIC 経由）→ DHS と他省庁等が入手したインシデント情報の CTTIC への集約→海外情報等も含めた CTTIC による総合的な分析→国家安全保障に関するセキュリティ事故の大統領等への報告、というルートを確立させている(107)。近年は、壊滅的な停電も想定し、サイバー攻撃を受けて重要インフラに障害が発生した場合の復旧力の強化に力を入れている。

日本では、サイバーセキュリティ基本法（平成 26 年法律第 104 号）に基づき、2018（平成 30）

---

(103) “§ 73.77 Cyber security event notifications.” Nuclear Regulatory Commission HP <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0077.html>

(104) Nuclear Regulatory Commission, “Regulatory Guide 5.83: Cyber Security Event Notifications,” 2015.7. <https://www.nrc.gov/docs/ML1426/ML14269A388.pdf>

(105) Nuclear Regulatory Commission, “Draft Regulatory Guide (DG)-5061: Proposed Revision 1 to Regulatory Guide 5.71, Cyber Security Programs for Nuclear Power Reactors,” 2018.8. <https://www.nrc.gov/docs/ML1801/ML18016A129.pdf>

(106) NRC は、2012 年 12 月に、10 CFR 73.54 への適合レベルを確認するため、①サイバーセキュリティ評価チームの設立、②重要システム及び重要デジタル資産の特定・文書化、③セキュリティレベルが低い機器と高い機器の分離、④携帯メディア・機器のアクセス管理の実施、⑤サイバー攻撃の監視・検出、⑥重要デジタル資産のサイバーセキュリティ管理の実施、⑦監視・評価活動の実施・継続、⑧ 10 CFR 73.54 の完全実施、というマイルストーンを示した（“Appendix A: Description of Milestones 1-8 of 10 CFR 73.54 Implementation.” Nuclear Regulatory Commission HP <https://www.nrc.gov/docs/ML1635/ML16354A272.pdf>）。

(107) 日本サイバーセキュリティ・イノベーション委員会「諸外国におけるサイバーセキュリティの情報共有に関する調査」2018.3.9, p.5. <https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf>

年7月に、今後3年間の基本的な計画として、新たな「サイバーセキュリティ戦略」(108)が策定された。重要インフラについては、更に「重要インフラの情報セキュリティ対策に係る第4次行動計画」(109)に基づき、①安全基準等の整備及び浸透、②情報共有体制の強化、③障害対応体制の強化、④リスクマネジメント、⑤防護基盤の強化、の5つの施策が進められている。しかし、サイバーセキュリティに関しては、技術の進歩が速く、攻撃側の優位性が高いため、これだけの対策を講じれば十分と言い切ることが難しい。今後も迅速に関連情報の入手を図り、対策を充実させていくことが望まれる。

（やまざき　おさむ）

⑽8 「サイバーセキュリティ戦略」2018.7.27. 内閣サイバーセキュリティセンター HP <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf>

⑽9 「重要インフラの情報セキュリティ対策に係る第4次行動計画」（平成29年4月18日サイバーセキュリティ戦略本部決定、平成30年7月25日サイバーセキュリティ戦略本部改定）同上 <https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf> においては、重要インフラ分野として、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道、物流、化学、クレジット、石油の14分野が特定されている。

別表　米国の重要インフラにおける主なサイバーインシデント及びサイバーセキュリティ強化策

年	電力分野（原子力発電を含む。）における主なサイバーインシデント	重要インフラにおける主なサイバーセキュリティ強化策（一部、物理的な対策を含む。）	電力分野（原子力発電を含む。）における主なサイバーセキュリティ強化策
1997		・1996年に発出された行政命令により設置された重要インフラの保護戦略を策定する委員会の報告書「重要基盤：米国のインフラの保護」（10月）：官民の協力と情報共有、重要システム保護のための技術開発の促進等を要求	
1998		・大統領決定指令「重要インフラの保護：部門コーディネータ」（5月）：重要インフラの所有者・運営者の利益を代表する仕組みの導入	
2000		・「情報システム保護のための国家計画」：情報通信ネットワークの安全性及び信頼性の向上を図るため、10項目のプログラムを公表	
2002		・「国土安全保障国家戦略」（7月）：国土安全保障の戦略目的、重要分野（うち1つは「重要インフラと資産の保護」）を提示 ・「2002年重要インフラ情報法」（11月）：政府と重要インフラ事業者との間で情報セキュリティに関する情報の共有化を可能にする規定	・「電力部門のためのセキュリティ・ガイドライン」(6月)：電力部門の重要施設を物理的及びサイバー上の脅威から守るためのベスト・プラクティスを提示
2003	・オハイオ州の原子力発電所がサイバー攻撃を受け、システムが約5時間停止（1月）	・「重要インフラ及び主要資産の物理的保護のための国家戦略」（2月）：2002年7月の国土安全保障国家戦略に基づく政策を提示 ・「国土安全保障大統領令」（12月）：重要インフラ及び主要資産を特定し、優先順位を付与	
2006		・「国家インフラ保護計画」（6月）：重要インフラを保護するためのリスク管理の枠組み、関係者の役割・責務等を規定	
2008		・「包括的全米サイバーセキュリティ・イニシアティブ」（1月）：サイバーセキュリティ戦略の枠組みとして、3つの目標と12の取組を提示	・「重要インフラ保護に必須の信頼性基準」（1月）：基幹電力系統の運用等に必要な電子情報交換の安全性確保、重要サイバー資産への不正アクセス阻止等の要件を確立
2009		・「サイバー空間政策レビュー」（5月）：サイバーセキュリティを向上させるために実施すべき計画を短期（10項目）と中期（14項目）に分けて整理	・規則「デジタル・コンピュータ並びにコミュニケーション・システム及びネットワークの保護」（3月）：原子力発電事業者にサイバーセキュリティ強化を義務付け
2010		・「全米サイバーインシデント対応計画」（9月）：事業者が対応システムを運用する能力を全国的に平準化するよう調整等	・「原子力施設のためのサイバーセキュリティ・プログラム」（1月）：2009年の規則に記された要件を実施するための手引を提示

2012	・2つの発電所でUSBメモリがマルウェアに感染（10月のインシデントでは、休止していた発電所の再稼働が3週間遅延）		
2013		・「重要インフラのセキュリティと復旧力に関する大統領政策指令」（2月）：重要インフラの予期せぬ事態からの復旧力を強化	
2014		・「重要インフラのサイバーセキュリティ向上のためのフレームワーク」（2月）：重要インフラ事業者のサイバーリスクに対する認識促進	
2015		・「民間部門におけるサイバーセキュリティ情報共有の促進に関する行政命令」（2月） ・「2015年サイバーセキュリティ情報共有法」（12月）：サイバー脅威情報共有システムの運用開始	・規則「サイバーセキュリティ・イベントの通報」（7月）：サイバー攻撃を受けた原子力発電事業者に、NRCへの通報を義務付け
2016	・バーモント州の電力会社のパソコンからマルウェアを発見（12月）	・「サイバーセキュリティ国家行動計画」（2月）：サイバーセキュリティ向上委員会、連邦主席情報セキュリティ担当官の設置等 ・「米国におけるサイバーインシデントの調整に関する大統領政策指令」（7月）	
2017	・カンサス州の原子力発電所運営会社等のネットワークを狙ったハッキングが発覚	・行政命令「連邦ネットワーク及び重要インフラのサイバーセキュリティの強化」（5月）	
2018		・「サイバーセキュリティ戦略」（5月）：リスク管理アプローチについて5つの柱と7つの目標を設定 ・「国家サイバー戦略」（9月）：2017年策定の「国家安全保障戦略」に基づき、サイバー空間の脅威から米国を守るための安全保障政策を整理	・NIAC報告書「大停電からの復興：国家の能力を強化する方法」（12月）：既存の計画等では「壊滅的な停電」に対処できないという認識を示し、新たな国家的対応として7項目を提言
2019	・電力網がサイバー攻撃を受け、停電には至らなかったが、電力管理センター等に低レベルの影響（3月）		・NERC報告書「サプライチェーンにおけるサイバーセキュリティ・リスク」（5月）：サプライチェーンに係るサイバーセキュリティ強化のため、規制範囲を広げること等を提言

（出典）筆者作成。