トピックス

通信・電力・行政などの重要インフラに対する サイバー攻撃への米国の防衛

沖縄総合通信事務所長　　大寺　廣幸

1　はじめに

７月31日（火）の新聞夕刊に「新種のコンピュータウイルス猛威の恐れ　FBIが警告」という見出しの記事が載った。このコンピュータウイルスは名前は「コードレッド」。マイクロソフトの「ウィンドウズNT」や「ウィンドウズ2000」をサーバで使っている場合に感染し、世界標準時の８月１日午前０時から一斉に特定のウェブサイトへのアクセスを繰り返し、コンピュータの処理速度を極端に低下させるウイルスだ。この警告を発したのが、米国連邦政府機関の一つ、インフラ防衛センター（National Infrastructure Protection Center: NIPC）である。実質的にFBI（米連邦捜査局）の下にある。

IT革命とかインターネットの爆発的普及とか情報通信が社会に大きな変革をもたらしてきている。その裏面として情報通信ネットワーク・システムへのハッカーの侵入やサイバーテロなどのサイバー攻撃が社会を大きく混乱させるのではないか、との危惧がますます高まっている。

米国では、通信、電力、金融や行政といった国民生活や社会・ビジネス活動を支える基盤（インフラ）への攻撃、特にサイバー攻撃に対して、早期警戒、被害の最小化など国を挙げての対策が90年代からスタートしている。

この小稿は、NIPCを中心とする米国の取り組みの鳥瞰図である。

2　重要インフラへのサイバー攻撃のリスク

相互に接続したコンピュータシステムのリスクはますます深刻になり多様化している。攻撃は、インターネットやその他のネットワーク、さらにダイヤルアップの電話回線を通じて世界のどこからでも仕掛けられる危険がある。攻撃する側は、身元や場所、意図を巧妙に隠す。相手を見つけ出すことは難しく時間もかかる。攻撃によって、コンピュータ依存が大きい業務・事業はきわめて大きなダメージを受け、秘密にすべき情報の信頼度が落ち、重要データの無謬性が損なわれる。米国の国家完全保障局（National Security Agency）によれば、コンピュータ攻撃能力を開発した外国政府もあり、米国のシステムを研究し攻撃方法を開発中、という米国に潜在的に敵対する勢力もあるとのことである。サイバー攻撃は、幸いシステムを壊滅させるほど深刻なものはまだないが、その数は増加している。Carnegie-Mellon大学のCERT調整センターが集計した公表攻撃件数は、1993年１,300件が、1999年９,800件、2000年21,000件と急増している。同じく、FBIの報告によれば、

FBIのコンピュータ侵入関連の捜査は1998年に比して2000年は倍増しているそうである。

FBIが分類する攻撃の主体は次のとおりである。まず、サイバーシステムへの脅威は大きく４つに分けられる。

１）　インサイダー

なんらかの不満をもつ従業員や元従業員（インサイダー）が、企業、団体を対象とするコンピュータ犯罪の犯人であることが多い。インサイダーは、当然のことながら勤務先のコンピュータシステムについて知識をもち操作方法に慣れている。本来なら許可されないアクセスを行って、システムに損害を与え重要データを窃取するケースも出てきている。1999年のComputer Security Institute/FBIの報告では、アンケート回答の55%が、インサイダーによる不当行為をあげた。

２）　ハッカー

ハッカー（あるいはクラッカー）の中には、侵入できないよう防御されているものに挑んでみるスリルを単純に味わいたいとか、ハッカー仲間の社会で侵入できたという勲章を得たいとかいった動機からシステムに攻撃をしかける人たちもいる。ところが、最近では、不当な経済的利益を得るなど不正な動機をもって攻撃を仕掛ける事例が多くなってきている。過去においては、閉ざされたコンピュータシステムに、はるか離れた場所からクラッキングするには、コンピュータシステムに関する相当の知識・技能が必要であった。ところが、今では、インターネットのWorld Wide Webを通じ、攻撃を仕掛けるためのスクリプトやプロトコールなどの情報を容易にダウンロードできるようになった。防御側がますます障壁を高くする一方で、ますます巧妙・洗練された攻撃ノウハウがインターネット上に出回ってきているのだ。

さらに、ウェブページや電子メール・サーバーに対し、政治的意図をもって仕掛ける攻撃が出てきている。これはHacktivismと称されている。彼らは、特定の電子メール・サーバーを負荷過剰に追い込んでダウンさせたり、また、ウェブサイトの管理機能を奪い政治的メッセージをもつ電子メールを発信させたり、といった行動に出ている。これらの攻撃は、Operating Systems（OS）やネットワークそのものを換えるものではないが、サービスを混乱させ経済的損失を与え、大切な情報をもつウェブサイトへの多くの人のアクセスを妨害するものである。

３）　ウイルス送信マニア・パラノイア

コンピュータ・ウイルスの伝搬は、世界中のネットワークやシステムにとってますます深刻な問題になってきている。この数年、幾つものコンピュータ・ウイルス、ウァーム（虫）が増殖し破壊的なダメージを与えた。Melissa Macro VirusやExplore.Zip worm、CIH（Chernobyl）Virusなどがそうだ。NIPCは、これらのウイルスに関し、たびたび警報や、特に危険性の高いものについては、予防措置・事後対策など被害の最小化に資する情報を流してきている。

Melissa Macro VirusについてNIPCの活動をみてみよう。NIPCは、ウイルスとその影響につき確実な情報を得るや直ちに警報を出した。警報はコンピュータネットの利用者に広く伝わり、被害の拡大、深化をふせぐことができた。他方でNIPCは、犯罪捜査に関しては、FBI各支部や地元警察との連絡窓口となった。アメリカ・オンライン（AOL）からニュージャージー州警察へもたらされた情報とその後のFBIニューアーク支部の捜査によって、1999年４月１日、David L.Smithが逮捕された。彼の自供によれば、約百万のコンピュータシステムに攻撃を企て、約８千万ドルの損害を与えようとしたとのことである。

４）　犯罪グループ

資金詐取などのためサイバーシステムへ侵入す

る犯罪が増加している。1999年９月、「Phonemasters」と称する犯罪グループの二人のメンバーに有罪判決がくだった。保有が許されないアクセス機器を盗み、これを保有・使用して連邦政府機関のコンピュータにアクセスしたためだ。Phonemastersは、国際的な広がりをもつ犯罪グループで、MCIやSprint、AT＆Tなどの民間企業のみならず、国家刑事情報センター（National Crime Information Center）などにも侵入を繰り返してきた。裁判所からの電子監視令状のもと、FBIのダラス支部は、通話行動と被疑者のモデムパルスの監視を行った。被疑者の一人Calvin Cantrellは、Sprintの幾千もの加入者のコーリングカード番号をダウンロードし、そのデータは、カナダ人に売られ、その後、オハイオ在住の米国人、スイス人と転々売買され、最後にイタリアの犯罪グループの手にわたった。Cantrellは有罪を認め二年の懲役刑となった。Phonemastersの手口は、「dumpster diving」の一種で、まず古くなった電話帳とシステムの技術マニュアルを集める。この情報を使ってターゲットの企業等の従業員に電話をかけ、いろいろ甘言を使いログオンとパスワードの情報を聞き出す。そして、システムに侵入するのである。

このようなサイバーシステムへの４つの脅威に加え、米国社会に広く影響を与え安全保障の観点から注意すべき３つの脅威があるとFBIは指摘している。

１）　テロリスト

テロリストグループは、テロ計画の策定、資金の調達、プロパガンダの頒布、仲間どうしの連絡に、ITやインターネットをますます活用している。CIA長官George Tenetは、「2000年の世界的な脅威」に関する議会証言の中で次のように述べている。「HizbollahやHAMAS、Abu Nidal、Bin LadenのalQa'idaなどのテロリストグループは、その活動を支援するためコンピュータ化したファイル、電子メール、暗号技術を使っている。」たとえば、世界貿易センター爆破事件の首謀者、Ramzi Yousefは、米国の航空会社の襲撃破壊計画をそのラップトップパソコンに暗号ファイルのかたちで入力していた。また、Tamil Tigersの関連団体と報道されているInternet Black Tigersなどのテロリストグループは、幾つもの国の政府機関のウェブサイトや電子メール・サーバーに攻撃を仕掛けたと報道されている。これらのグループが、行政や市民生活・経済を混乱に陥れるため、電力、運輸、政府機能などの重要インフラに対し大規模なサイバー攻撃を加えた事例はまだ見つかっていない。しかし、かれらもコンピュータ活用ノウハウを蓄積しIT依存を強めている傾向からみて、サイバー攻撃の危険は高まっていると考えるのが自然だろう。

２）　情報機関

情報機関は、情報収集、防諜などのため、情報通信ツールを使ってきている。たとえば、「カッコウの卵」事件として知られる有名な事例だが、まだインターネットが一般に普及する前、1986年にKGBは、西ドイツのハッカーを雇い国防総省の情報通信ネットワークに侵入した。

３）　情報戦争

戦争の一形態として、他国の重要インフラに対する軍組織を使う組織的・包括的なサイバー攻撃は、「情報戦争」ということができよう。国家安全保障確保のためもっとも脅威になるものであろう。情報機関の報告では、幾つかの国が米国その他の外国を対象に情報戦争の戦略、作戦計画をたて、サイバー攻撃の能力を向上させているとのことである。これらの国では、従来型の「リアルな」武器では米国に対抗できないと認識し、政府、ビジネス諸活動のIT依存傾向の高まりとともに、「アキレス腱」となりつつある重要インフラの情報通信ネットワークへのサイバー攻撃を念頭において、戦略・戦術を組み立てているとのことであ

る。

3　1990年代の取り組み

1998年５月22日、クリントン大統領は、重要インフラ防衛政策に関する大統領決定指令63（Presidential Decision Directive（PDD）63）を発表した。現在の米国のサイバー攻撃に対する対策は、このPDD 63に源泉があるといってよいだろう。このPDD 63に至るまでの情報通信ネットワークの脆弱性に関する取り組みについて、主要なものを概観してみよう。

3.1　国家研究会議（National Research Council）の報告

1991年、「Computers at Risk: Safe Computing in the Information Age」という報告が公表された。報告書は、「コンピュータシステムは、一層発展し複雑化し物理的なプロセスに組み込まれ、相互に連結していく。そのため、コンピュータシステムの設計が貧弱であったり、システムを機能不全においこむ事故が発生したり、システムへの攻撃が起きたりすると、社会は、ますます脆弱化していく。」と指摘した。この報告書は、官民双方から注目があつまり、技術に依存しすぎることのもろさ、危険を警告した。

3.2　重要インフラ作業グループ（Critical Infrastructure Working Group）の報告

1995年６月、司法長官のもとに作業グループができた。この作業グループは、次の事項についてレポートをとりまとめた。

１）重要インフラを特定しそれらに及ぶ脅威の範囲と性質を評価。

２）これらの脅威に対処する現在の政府のメカニズムを調査。

３）重要インフラへの脅威に対する長期的な政府の対策を検討する常設的な組織について選択肢を提示。

3.3　国家防衛承認法（National Defense Authorization Act）の制定

1996年２月、連邦政府は、国家防衛承認法によって、国家情報インフラ（National Information Infrastructure: NII）に対する戦略的攻撃への警報能力の開発など、政府として取り組むべき政策や計画を、議会に報告する義務を負うことになった。この年、上院の政府関係事項委員会（Committee on Governmental Affairs）の調査小委員会がサイバースペースに関する公聴会をスタートさせた。

3.4　重要インフラ防衛委員会（Commission on Critical Infrastructure Protection）の設置

1996年７月、クリントン大統領の諮問に答える委員会が設けられ、サイバー攻撃、物理的攻撃の脅威に対する国家レベルの脆弱性について検討がはじまった。

3.5　議会への報告（High-Risk Series: Information Management and Technology）

1997年から２年に一度、わが国の会計検査院にあたるUnited States General Accounting Office（GAO）が、情報セキュリティ・リスクの高い政府分野に関する現状報告をとりまとめ連邦議会に報告するようになっている。

3.6　重要インフラ防衛委員会の報告

1997年10月、上記３．４の委員会が報告書を発表した。国家的なレベルにおいて、情報セキュリティの脆弱さを放置すればいかに悲惨な結果をもたらすか、について詳細な記述が報告書にまとめられている。

１）「今後想定されるサイバーベースの脅威、被

害を抑えるため、調査、分析評価、早期警報、復旧メカニズムの仕組みを確立すること」など、総合的な取り組みの必要性を強調。

2）さらに、FBIがすでに取り組みだした警報・脅威分析機能を拡充すべきであると指摘。

3）FBIは、インフラへの攻撃に対する全国的な早期警報センターとして有用であり、このサイバー攻撃に関する情報収集・分析、捜査、取り締まりなどで中心的な役割を果たすべきだと指摘。

4　重要インフラ防衛政策に関する大統領決定指令63（Presidential Decision Directive（PDD）63）

1998年５月22日、クリントン大統領は、PDD 63を発表した。米国の重要インフラ防衛に関する考え方が端的に示されている。このPDD 63本文を紹介してみよう。

4．1　増大する潜在的脆弱性

米国は世界最強の軍事力、最大の経済力をもっている。この二つのパワーは相互に依存し強めあう関係にある。また、重要インフラとその上に構築される情報システムに米国社会はますます依存するようになってきている。

重要インフラは、物理的かつ仮想的なシステムであり、経済や政府が最小限機能するため不可欠なものである。重要インフラに含まれるものは、通信、エネルギー、金融、運輸、水道、緊急サービスで、公私を問わない。歴史的に見て、重要インフラの多くは、各々独立し相互関係はほとんどなかった。ところが、情報技術（IT）の発展と効率性の追求のため、これらのインフラは、ますます自動化され関連が強まった。それとともに物的損壊、人為ミス、自然災害、物理的・仮想的攻撃に対する脆弱度合いが高くなってきた。これらの脆弱性に対しては、公私両セクターがいっしょになり、さらに国内のみならず国際的にも協力し合って、柔軟で革新的な対応が求められるようになってきている。

わが国の軍事力を考えると、国家であろうとグループ・個人であろうと、米国への加害行為はこれまでにない方法で行われる可能性がある。わが国の経済はますます相互依存的で仮想的なインフラに依存するようになってきており、これらのインフラや情報システムへの新たなタイプの攻撃はわが国の軍事力と経済に対し相当程度損害を与える可能性がない、とは言えない。

4．2　大統領の方針

重要インフラの機能を途切れることなく有効に維持、確保していくことは米国の長年の政策である。クリントン大統領は、重要インフラへの物理的・仮想的な攻撃に対する弱みをすみやかになくすため、米国は必要とみなすあらゆる手段をつかう方針である。

4．3　国家目標

2000年までに米国は、第一次的な対応力をもつ。PDD 63への大統領署名から５年以内に、３つの部門の機能を著しく低下させる意図的攻撃から国家的な重要インフラを防衛する能力をもつ。

1）基本的な国家安全保障のミッションを果たし国民の健康と安全を確保する連邦政府部門

2）秩序を維持し最低限の基本的な公共サービスを提供する州等の地方政府部門

3）経済の正常な運営と基本的な通信、エネルギー、金融、運輸のサービスの提供を担当する民間部門

これらの重要機能が妨害を受け正常に働かなくなったとしても、米国の繁栄をたもつため、その障害は、短期間で修復され、まれにしか起こらず、管理可能で、地理的に限られ、また、被害は最小

にすべきである。

4.4　脆弱性を減らすための官民のパートナーシップ

わが国の重要インフラへの攻撃の対象に、民間経済機構と政府の両方の施設が含まれていると考えられるので、想定される脆弱性をなくすには、官民双方の緊密な連携が必要である。このパートナーシップは、利害をこえ相互理解のもと互助的なものでなければならない。わが国の重要インフラの脆弱性をなくすという国家目標を達成するため、連邦政府は、可能な限り、政府規制の増加をおさえ、財政的裏付けのない民間セクターへの強制を避けるべきである。

インフラへの攻撃に弱いわが国経済の主要部門に対しては、連邦政府は、それらの民間部門との共同作業のため、適当な主管連邦機関（Lead Agency）の幹部職員をその部門の連絡調整官（Sector Liaison Official）として指名する。連絡調整官は、その部門の関係機関と討議・調整を行い、民間サイドを代表する人を部門調整者（Sector Coordinator）に指名する。かれら二人の代表と関係の省庁、業界団体は、部門ごとの国家インフラ安全プラン（National Infrastructure Assurance Plan）の策定に寄与する。その策定に当たっては、次の事項を盛り込む。

1）サイバー・物理的攻撃に対する当該部門の脆弱性を分析評価する
2）甚大な影響を与える脆弱性についてそれをなくすための方策を勧告する
3）想定される大きな攻撃を識別しこれを回避するシステムを提案する
4）攻撃に対し警告・抑止・制止するためのプランや、攻撃を受けた後、場合のよっては連邦緊急管理庁（FEMA）の協力を得て、最小限であっても主要な機能の早期回復をはかるためのプランを構築する

部門別プランが策定されるまでの間、国家調整官（National Coordinator）は、主管連邦機関の部門連絡調整官や国家経済諮問委員会（National Economic Council）の代表と連携し、全体調整と部門別プランの相互調整を行う。

4.5　ガイドライン

この潜在的な脆弱性をなくすため、クリントン大統領は、次の一般的な原則を踏まえるべきであると考えている。

1）この指令に定める目的達成のため取り組むべき政策については議会と協議し議会の意見を取り入れるべきである。
2）わが国の重要インフラの防衛にあたっては、インフラの所有者、運用者そして政府が共同責任を負いパートナーシップを組むべきである。さらに、連邦政府は、この問題が世界的な広がりをもつものである点にかんがみ、国際的な協力を促進すべきである。
3）わが国の重要インフラに関する安全性、脆弱性、脅威については、頻繁に分析評価すべきである。なぜなら、技術革新や重要インフラへの脅威は急速に変容を遂げており、防衛方法もこの状況変化に応じるように変えていく必要があるからだ。
4）市場が生み出すインセンティブが重要インフラ防衛の課題を解決するためまず考慮されるべきである。規制は、市場が米国国民の健康、安全、福祉を守れないときに限り発動されるべきである。このような場合、望ましい対応をうながす経済的なインテンティブの提供や民間セクターによる解決策に関する情報の提供など、直接的な規制に代わる対応策について、関係行政機関は検討すべきである。これらのインセンティブやその他の措置をとるに

際しては、最新技術の活用を念頭におき、国際的課題へは世界的なレベルの解決策の採用に努め、また、民間セクターの関係者が最大限、セキュリティ確保に柔軟な対策がとれるよう配慮すべきである。

5）連邦政府のすべての機関が、取締り、規制、情報収集、国防に関する能力・資源を使って重要インフラ防衛にあたるべきである。

6）プライバシーにかかる権利の尊重への配慮が必要である。情報は、正確で秘密が守られ安心して取り扱われるとの信頼を、消費者や民間企業がもつことができるようにすべきである。

7）連邦政府は、研究開発や調達を通じ、インフラ防衛に有効な手段を関係機関が導入できるよう促すべきである。

8）連邦政府は、民間セクターのモデルとなって、インフラ防衛のためどのような対策がベストかを実証し、可能な限りその成果を広く民間セクターに示すべきである。

9）私たちは、予防措置とともに脅威・危機管理に焦点をあてるべきである。民間セクターは、自ら管理するインフラのセキュリティ確保について可能な対策は最大限講じ、また、その対策実施のため必要な情報を政府に提供すべきである。ただし、民間が自ら進んで対策を講じるようにするためには、全米的なインフラ防衛システムへの民間関係機関の参加は任意としたほうがよい。

10）州やその他の地方政府、さらに重要インフラへの攻撃に真っ先に対処しなくてはならない機関（第一次対応機関）との間の緊密な協力、調整は、インフラ防衛プランを確固かつ現実妥当なものにするため不可欠である。すべての重要インフラ防衛プランやこれに基づくアクションは、州やその他の地方政府、第一次対応機関の任務、活動を念頭におくべきである。

4.6　構造と組織

連邦政府は、その果たすべき機能から４つの部門に体系づけて組織される。

１）部門ごとの主管連邦機関

サイバー・物理的攻撃の標的になるインフラ部門ごとに、連絡調整にあたる連邦機関を一つずつ決める。各機関は、次官補以上のランクの幹部職員を連絡調整官に指名する。連絡調整官は、民間サイドを代表する部門調整者の協力をえて、重要インフラ防衛のための問題解決にあたる。特に、国家インフラ安全プランの当該部門に関する部分の策定に寄与する。主管連邦機関とそのカウンターパートとなる民間セクターは、当該部門の脆弱性認識・教育プログラムの開発・実施を担当する。

２）特別の機能に関する主管連邦機関

さらに、連邦政府が主に担当する重要インフラに関する機能がある。（国防、外交、情報活動、取締り）このため、連邦政府機関のすべての活動を調整する責務を有する主管機関をおく。各々の機関は、連邦政府の当該機能の調整官（Functional Coordinator）に、次官補以上のランクの幹部職員を指名する。

３）省庁間調整

各主管連邦機関の部門連絡調整官と機能別調整官は、セキュリティ・インフラ防衛・テロ対策担当の国家調整官（National Coordinator）が主宰する重要インフラ調整グループ（CICG）のもとで、国家経済諮問委員会など関係する省庁の代表とともに、この指令の具体化のため調整会議を開く。大統領が指名する国家調整官は、国家安全保障担当補佐官を通じて大統領にレポートを提出する。CICGは、次官補以上の上級政策担当者で構成さ

れる。

4） 国家インフラ安全諮問委員会（National Infrastructure Assurance Council）

主管連邦機関、国家経済諮問委員会、国家調整官の勧告により、大統領は、国家インフラ安全諮問委員会のメンバーとして、主要インフラ関係民間企業や州その他の地方政府の代表を指名する。大統領は、この諮問委員会の委員長を指名する。国家調整官は、この委員会の事務局長となる。この委員会は定期的に会議を開き、官民の各部門が重要インフラ防衛のため協力を強める方策を話し合い、必要があれば大統領にレポートをだす。連邦機関の幹部スタッフも必要に応じこの会議に加わる。

4.7　連邦政府の重要インフラ防衛

すべての連邦政府機関は、自ら所管する重要インフラ、特にサイバーベースのシステムを防衛する責任を有する。各連邦機関の最高情報責任者（Chief Information Officer: CIO）は、情報の安全確保に責任を負う。また、各連邦機関は、最高情報安全責任者（Chief Information Assurance Officer: CIAO）を指名する。CIAOは、CIOが担当する責務を除きその他の当該機関の重要インフラに関する事項にすべて責任をもつ。場合によっては、CIOとCIAOは兼任することも可能だ。これらの者は、コンピュータシステムなどを対象とする脆弱性の分析評価の実施につき、実施許可の有効・明確な手続きを定めなくてはいけない。司法省は、この許可手続きの法的ガイドラインを定める。

この指令発効後180日以内に、すべての省庁は、サイバーベース・システムを含むその所管する重要インフラの防衛プランを策定する。国家調整官は、省庁をまたがるインフラにつき調整を行う。CICGは、これらのプランの専門家レビューを監理する。２年以内にこれらのプランは実行され二年ごとに更新される。このスケジュールを担保するため、連邦政府は、民間セクターに対し重要インフラ防衛方法につきモデルを提示する。

4.8　作業

策定される国家インフラ安全プランに盛り込まれる事項は次のようなものが想定される。

1）脆弱性分析

攻撃に対する脆弱性を分析評価しなければならない。この分析評価は定期的に見直す。この評価には、最低限、維持存続させるべきインフラは何かを明らかにすることも場合によっては必要である。

2）復旧プラン

脆弱性評価をもとに、復旧プランを勧告する。プランには、復旧スケジュール、担当機関、所要経費を盛り込む。

3）警報

大きなインフラ攻撃に対し全米レベルで警報をだすセンターを早急にたちあげる。その後ただちに民間セクターからの可能な限りの参加を得て、攻撃を探知、分析する高度なシステムをそのセンターにおく。

4）緊急対応

相当規模のインフラへの攻撃に緊急対応するシステムが構築中である。この緊急対応では、ダメージを拡大させず一部に抑え最小化することが目標だ。

5）復旧

仮に攻撃が成功してもその被害の拡大をふせぐため、最小限必要となるシステムの早期復旧をはかるシステムを構築する。

6）教育・啓蒙

人々にセキュリティの重要性を認識してもらい、攻撃をうけたとき、特にサイバーシステムへの攻

撃を受けたときの緊急・復旧訓練に役立ててもらうため、官民双方で脆弱性認識・教育プログラムが必要だ。

7）研究開発

インフラ防衛の支援のため連邦政府が資金援助する研究開発のプランの策定が求められる。このプランは、計画期間を数年とし、民間セクターの研究を考慮し、早期かつ達成可能なスケジュールで脆弱性の最小限化をめざし、適切に資金配分されたものであければならない。

8）情報活動

情報関係機関は、わが国のインフラに対する海外からの脅威につき情報収集、分析を強化するプランを策定し実行する。この中には、外国のサイバー・情報戦争の脅威に対するものも含まれる。

9）国際協力

重要インフラ防衛に関し、友好国、国際機関、多国籍企業との協力を拡大するプランを作るべきである。

10）法的措置・予算措置

重要インフラに関する行政手続き、法的措置、予算措置の優先順位を明確にすべきである。必要があれば大統領に勧告を行う。この評価、勧告は行政管理予算局（Office of Management and Budget）（OMB）長官との調整を行う。

4.9　実施状況のモニター

180日レポートとともに、国家調整官は、国家経済諮問委員会と共同で、大統領と各省庁長官に対し、国家安全保障担当補佐官を通じ毎年、この指令の実施状況についてレポートを提出する。レポートには、最新の脅威の評価、国家プランやそのほかの政策で定めた目標への達成度合い、法的・予算措置の勧告を盛り込むべきである。この評価・勧告は、OMB長官と調整すべきである。さらに、2000年に第一次的な対応力を確立した後、国家調整官は、ゼロベースでレビューを行う。

5　連邦政府の取り組み

ここで、PDD 63を受け現在とられている連邦政府の取り組みを鳥瞰してみよう。

5.1　セキュリティ・インフラ防衛・テロ対策担当の国家調整官（National Coordinator）

ホワイトハウスの国家安全保障会議スタッフの国家調整官は、サイバーセキュリティ問題の対外窓口責任者でPDD 63と国家プランの実施全体を見ている。

5.2　重要インフラ安全局（Critical Infrastructure Assurance Office: CIAO）

商務省内におかれた省庁横断機関で、連邦政府の重要インフラ防衛に関する政策、取り組みの調整を支援する。

この組織は3つの使命をもつ。まず、情報セキュリティ防衛に関する国家プランの成文化につき調整する。このプランの第一版は、2000年1月、クリントン大統領により公表された。第二に、重要インフラの相互連関性などに関する連邦機関の分析を支援する。CIAOは、プロジェクトマトリックスを作成しているが、これによって連邦機関が、安全保障や経済安定化、公衆衛生サービス・セキュリティを確保していく上で中核となる資源・資産を特定することが容易になる。第三に、民間セクター等への周知、啓蒙、教育を調整する。CIAOは、重要インフラ防衛の官民パートナーシップ醸成の媒介役である。CIAOは、個別産業部門をまたぐ問題や連邦機関の既存権限では対応しきれない問題に焦点をあて対処する。このように、CIAOは、重要インフラ防衛に対し首尾一貫し集中的に対処する要となるところである。

5．3　インフラ防衛センター（National Infrastructure Protection Center: NIPC）

FBI内におかれた省庁横断機関で、脅威に対する警報を出し、脆弱性を減らすための政策をとりまとめるほか、取締りにもあたる。センターは、FBI職員と他の連邦機関から出向の職員の混成部隊で、さらに、州の取締まり組織から出向のスタッフや英国、カナダからの代表もセンターに席をおいている。センターは、連邦機関、州などの自治体、重要インフラを所有・運営する民間企業などさまざまな関係機関とのあいだで関連情報を収集、分析し配布する結節点の役目をになっている。FBIの56の支部等にはインフラ防衛を担当する職員がいて、コンピュータ侵入、サービス拒否、ウイルスなどの事案を扱うほか、民間との連携、州等の取締まり機関と間でコンピュータ犯罪タスクフォースの結成、コンピュータ犯罪捜査官の養成、データベースの構築、コンピュータ捜査専門家の必要な事件への応援などを行っている。

5．4　主管連邦機関

サイバー・物理的攻撃の標的になるインフラ部門ごとに、一の連邦の省庁が連絡調整にあたる。該当の省庁は、連絡調整官をその職員のなかから選ぶ。連絡調整官は、重要インフラ調整グループ（CICG）の国家調整官といっしょになって作業を行う。

主管連邦機関とその担当部門

商務省	情報、通信
財務省	銀行その他の金融機関
環境保護庁（EPA）	水道
運輸省	航空、ハイウエイ、大量輸送、パイプライン、鉄道、海上輸送
司法省（FBI）	緊急法執行サービス
連邦緊急管理庁（FEMA）	消防、政府一般サービス
健康・福祉サービス省（HHS）	公衆衛生サービス（予防・検査・研究サービスや個人健康サービスを含む）
エネルギー省	電力、石油・ガス生産備蓄

5．5　特別の機能に関する主管連邦機関

民間部門にカウンターパートがいない、連邦政府が担当する重要インフラに関する機能がある。（国防、外交、情報活動、法執行、研究開発）このため、連邦政府機関のすべての活動を調整する責務を有する主管機関をおく。各々の機関には、連邦政府の当該機能の調整官がおかれる。

主管連邦機関とその担当機能

司法省（FBI）	法執行、国内治安
CIA	対外情報活動
国務省	外交
国防総省	国防
大統領府科学・技術政策局（OSTP）	研究開発

5．6　重要インフラ調整グループ（Critical Infrastructure Coordination Group: CICG）

CICGは、省庁横断委員会で重要インフラに関する政策課題を分析し閣僚レベルの親委員会に政策提言を行う。このCICGの下に、サイバー事件監理グループ（Cyber Incident Steering Group:

CISG）とサイバー事件作業グループ（Cyber Incident Working Group: CIWG）がおかれる。国家調整官が主宰するCISGはCIWGに政策指針を示し、国家安全保障会議に勧告をおこなう。NIPC所長が主宰するCIWGは、サイバー攻撃等の事態がおきたときに関連連邦機関間での対策の実施や取締りなどの調整をおこなう。

5．7　最高情報責任者会議（Chief Information Officers Council: CIO Council）

連邦の各機関のCIOをメンバーとするこの会議は、連邦の情報システムのデータに関するプライバシー保護と利用確保のため設けられている。この下部組織であるセキュリティ・プライバシー・重要インフラ小委員会（Subcommittee on Security, Privacy and Critical Infrastructure）は、政府サービスの途絶をふせぎ、プライバシーを保護し、また、慎重な取り扱いを要する国家安全保障にかかる情報を守秘するため、連邦政府内のセキュリティ確保の具体的措置を検討する。

5．8　合同電気通信リソース委員会（Joint Telecommunications Resources Board: JTRB）

JTRBは、平時の緊急事態に対応する国家通信システム（National Communications System: NCS）に関する権限の行使につき、大統領府科学・技術政策局（OSTP）長官を補佐する。NCSの構成要素である国家通信センター（National Communications Center: NCC）は、民間セクターの企業を構成メンバーとし、OSTPとJTRBから支援を受ける。NCCは、連邦機関の電気通信インフラの主要エレメントで、官民協調の有力なモデルともなっている。

5．9　国家セキュリティ電気通信・情報システムセキュリティ委員会（National Security Telecommunications and Information Systems Security Committee: NSTISSCC）

1990年設けられたこの委員会は、政策課題を議論するフォーラムを提供し、また、国家セキュリティシステム防衛の運用ガイドラインを策定する役割をになっている。委員会メンバーは民間企業代表や軍関係者など広い範囲から選ばれている。

5．10　国家情報安全パートナーシップ（National Information Assurance Partnership: NIAP）

これは、情報技術（IT）の供給・需要の両サイドが等しくもつセキュリティ・テストを実施したいというニーズを満たすため、連邦政府が音頭をとって作った仕組みである。NIAPは、国家標準・技術機構（National Institute of Standards and Technology: NIST）と国家安全保障局（National Security Agency: NSA）の連携プロジェクトで、両機関のITセキュリティの経験が活かされている。ITセキュリティ関連技術・機器の品質評価の手法や試験方法などの調査研究をおこなうとともに、供給・需要両サイドのニーズをみたす試験評価をおこなう民間の試験研究機関の育成もめざしている。

5．11　連邦コンピュータ事件対応機構（Federal Computer Incident Response Capability: FedCIRC）

連邦政府の各省庁に影響を与えるコンピュータセキュリティ問題を扱う中心的な調整・分析組織である。事件発生となると、FedCIRCは、緊急対策の企画立案実施やアドバイスのため、国防総省、取締り機関、情報機関、学会、各省庁のコンピュータセキュリティ専門家とチームを組んで共同して事に当たる。

5.12 連邦サイバーサービス（Federal Cyber Services: FCS）

国家プランで定められた教育訓練施策で、高度な知識技能をもつ連邦情報システムのセキュリティ専門家を養成するものである。

6 省庁間の連携

ハッキングから情報戦争までサイバー世界の脅威は多種多様で幅広い。単に捜査するサイドに探知・予防・復旧のための新技術・技能を導入するだけでは十分ではない。さまざまな組織が協力する体制が必要である。サイバー攻撃では普通、攻撃は誰がどこから何のために、といったことは即座にわからない。ターゲットはただ一つなのか多方面に向けられたものかといった攻撃の範囲もつかめない。攻撃当初は、それが単なる悪戯なのか、組織犯罪なのか、それともテロか、スパイ活動か、戦略的な軍事行動の一環なのか、判然としない。その発信源、攻撃の性質、攻撃の広がりを知るには、ターゲットとして犠牲になったサイトやインターネットサービスプロバイダーや通信会社のサイトからの情報にたよるしかない。米国の憲法下では、このような情報は犯罪捜査当局しか集めることができない。NIPCがFBIに属する理由はまさにここにある。しかしまた、サイバー攻撃の脅威の広がりと多様さから、単にFBIなどの捜査機関にまかせるだけでは不十分で、国防総省やCIA等の情報機関、エネルギー省や運輸省などの民間のインフラを担当する省庁もいっしょになって対処しなくてはいけない。さらに州やその他の地方政府の捜査機関も関係しなくてはいけない。このため、NIPCは、省庁を横断的にまたがる機関となり、さまざまな組織の出向者がメンバーになっているのである。たとえば、国防総省からNIPCへの出向の状況は次のとおりである。

NIPCのポスト	出向元の機関
NIPC副所長	国防総省長官官房
コンピュータ捜査・運用部長	空軍特別捜査局
監視・警戒課長	陸軍
軍連絡官	海軍
計画マネジャー・監視官・捜査官・分析官	国家安全保障局、国防刑事情報サービス、空軍情報局、海軍刑事情報サービスなど

NIPCは、特に国防総省との関係を重視している。国防関係のシステムがサイバー攻撃の標的に頻繁になっているからだ。さらに現実問題として、サイバー攻撃関係の情報収集はFBIやNIPCより国防総省のほうが、質量とも格段にすぐれている。公開情報や産業界からの情報、さらにFBIなどの捜査機関からの情報では不十分で、国防総省からの情報を得てはじめてサイバー攻撃の全体像が見えてくることが多い。NIPCは、国防総省と共同タスクフォースー情報通信ネットワーク防衛（Joint Task Force-Computer Network Defense: JTF-CND）を通じ密接な連携をとっている。

省庁間の連携、特に国防総省との協調のケースを紹介してみよう。

Solar Sunrise事件。この事件は、1998年、イラクの武器監査が緊張に達していたとき、米軍のコンピュータシステムに侵入したものである。ハッカーは、Sun Solaris運用システムの脆弱性をさぐった。幾度かの侵入は、中近東からであった。ハッカーのタイミング、性質、標的などからペンタゴンは、イラクが米軍部隊の展開を妨害する意図で行っているのではないかと疑った。NIPCは、FBI、空軍特別捜査局、NASA、司法省、国防情報システム局、国家安全保障局、CIAなど多数の省庁と協力して捜査にあたった。数日して、このハッカーはイラクが起こしたものではなく米国とイスラエルの十代の青少年のしわざだと判明。こ

の事例は、攻撃を仕掛けてくる者の特定や報復措置をとる前に、関係機関が協力し合って標的となったサイトのみならず他のサイトについても広く情報をとることの重要性を示すものであった。一昨年発生したMoonlight Maze事件は、国防総省などの連邦機関のみならず民間企業のコンピュータシステムに対してロシア国内から攻撃がしかけられたもので、国防関係の研究技術情報など大量の機密データが盗まれた。このおりも事件解明のため、FBIの各支部、国防総省、関係情報機関がNIPCに協力した。

7　民間部門との協力

サイバー犯罪を防止するには、民間企業との密接な協力が不可欠である。サイバー攻撃で最も多くの犠牲がでているのは民間企業だ。サイバー犯罪を捜査しうまく起訴にもちこむには、民間企業からの情報提供と捜査への協力がキーである。民間企業のなかには、今でも、社員の行為ゆえ信用失墜になると危惧し、また、セキュリティに弱いとの風評をおそれ、サイバー攻撃の事実を内密にし捜査当局に情報提供しないところがある。しかし、大半の企業は、サイバー攻撃撃退のため捜査機関と連携するは重要だと認識し、今では進んで情報を提供し捜査に協力している。

登録会員数2,970万人、オンラインオークションなど電子商取引ビジネスを世界規模で展開しているeBayのRobert Chesnutは、昨年２月16日の上院歳出委員会で次のように証言した。

「先週の攻撃よりずっと前、eBayは、FBIの北カルフォルニア支部のコンピュータ犯罪捜査チームと共同作業する体制をととのえた。詐欺やハッキングなどのサイバー犯罪と戦う最善の方法は捜査当局と協力して事にあたることだと当社は考えている。そこで、昨年、当社のウェブサイトへの攻撃のような事態になったときにFBIに通報する手続きを定めた。この結果、今回の攻撃に際してもFBIのコンピュータ侵入捜査チームと常時連絡をとることができ、捜査を助ける情報をFBIに提供することができた。」

攻撃の標的となった企業やインターネットサービスプロバイダー（ISP）のネットワーク管理者は、捜査がうまくいくか否かの鍵となる存在だ。管理者はそのシステム特有の仕様を知っており、捜査官といっしょになって犯罪行為の証拠となる重要な取引データをチェックすることができる。

民間セクターには、事件解決に重要な決め手となる技術スタッフがいる。捜査機関があらゆるOSやネットワーク構成に精通したスタッフをもつことは無理だ。捜査には、民間の技術専門家の力を借りることが必要である。

民間セクターの協力を得るため、NIPCは、日常的に民間企業に役立つ活動をしている。たとえば、攻撃の脅威がある場合にはその関連情報を提供し、分析結果を公表し、警報を出し、また、さまざまな業界の集まりの機会をとらえては話をするようにしている。

8　終わりに

これまでNIPCを中心に米国の状況を概観してきた。昨年、このNIPCの活動とその課題について、上院司法委員会の技術・テロリズム・政府情報小委員会が、GAOに監査するよう依頼した。今年４月、GAOは、この小委員会に報告書を提出した。報告書の表題は、「重要インフラの保護：国家機能向上のための重大な挑戦（Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities）」。米国の社会、経済、行政の中枢神経系、基幹情報通信ネットワークが機能不全におちいらないよう、扇の要の役割をはたすNIPCに対して、GAOが８か月にわたって行った辛口の監査の報告である。

報告は、サイバー攻撃に対しタイミングよく警報を出していないのではないか、と指摘。また、民間セクターとの連携はまだら模様で、電力のように上手くいっているところもあれば、金融、通信のような部門では必ずしも連携が密ではないと述べている。警報を出す仕組みがなお十分でないのは、１）スタッフのコンピュータ・セキュリティやITマネッジメントに関する専門知識・経験の不足、２）幹部スタッフの未補充と、３）事件・事故のデータをすみやかに集め分析する全国的な仕組みができていないためであると指摘している。さらに、もっと基本的な問題は、NIPCの役割について連邦政府の関係機関でコンセンサスができていない点であるとコメント。NIPCは、FBIのコンピュータ犯罪捜査への支援では有効に機能しているが、サイバー攻撃の脅威への対抗手段に懸念をもつ民間セクターや他の政府機関への支援が不十分ではないか、と論評した。

GAOの指摘は厳しいものがある。しかし、冒頭にあげたように、コンピュータ・ウイルスの発生警報を迅速に出すなど、NIPCは、着実に実績を積み重ねている。

わが国も、情報通信ネットワーク・システムへの依存度合いは米国に負けない。サイバー攻撃に対する脆弱性がますます増大していることは誰もが感じるところである。ネットワークのグローバル化が進んでいる状況では、サイバー攻撃に対し日本だけが独力で防衛することは不可能であるし、また、日本だけに攻撃をとどめることもきわめて困難である。米国をはじめとし各国の取り組みを参照し早急な対策が官民協力し講じるべきである。