「米国における重要インフラ保護対策の状況」

渡辺弘美@JETRO/IPA NY

1. 重要インフラ保護に向けた米国政府の取り組み

2001 年 9 月の同時多発テロ事件以来、米国内では重要インフラの保護に対する関心が高まっている。重要インフラとは、国家安全保障、経済力及び国民の暮らしにとって極めて重要な資産やシステム、機能を指す。これらの重要インフラは、食品、水、緊急時のサービス、エネルギー、輸送、情報技術、通信、銀行・金融、郵便、船舶などさまざまな分野に関わっている。そしてこれらの重要インフラの運営は、コンピュータやネットワークに依存しており、その依存度は年々高まる一方である。現在、こうしたネットワークの多くは、インターネットにもつながっている。インターネットは政府機関や民間セクターに多大な貢献をもたらした一方、重要インフラに対するサイバー攻撃のリスクも高めている。

重要インフラの約 85%は民間セクターが所有しているため米国連邦政府だけでこれを保護することは不可能であるが、連邦政府として重要インフラ保護強化を効果的に支援できる策はあるとして、ホワイトハウス及び国土安全保障省（Department of Homeland Security: DHS）が中心となり取り組みを進めてきている。また、こうした重要インフラ保護に関する取り組みの中で、サイバーセキュリティ対策については非常に重要な位置を占めている。

(1) ブッシュ政権による重要インフラ保護に向けた大統領令

ブッシュ政権は 2003 年 12 月 17 日、国家安全保障に関わる大統領令：Homeland Security Presidential Directive（HSPD-7）を発表した。これは、国家の重要インフラ及び主要リソース（CI/KR = Critical Infrastructure and Key Resource）をテロリストの攻撃から守るため、連邦政府機関が CI/KR について特定し、保護のプライオリティを定めることを目的としたものである。

なお、ここで、CI とは、USA Patriot Act of 2001 の Section 1016(e)において、「物理的、バーチャルに関係なく、米国にとって極めて重要なシステムもしくは資産で、これらが利用不能な状態もしくは破壊されてしまった場合、安全保障（security）、国家経済セキュリティ（national economic security）、国家公衆衛生・安全（national public health or safety）が弱体化してしまうほどのインパクトを与えるもの」と位置付けられている。一方、KR とは Homeland Security Act of 2002

の Section 2 (9) において「公的及び民間に管理されており、経済及び国家運営にあたって最小限必要とされるリソース」と定義されている。

HSPD-7 は、国家重要インフラの脆弱性を排除することを目的として、1998 年 5 月 22 日にクリントン政権が署名した Presidential Decision Directive-63 (PDD-63) の改訂版である。PDD-63 は特にサイバーセキュリティに対する取り組みを明確に打ち出したことで知られる。例えば、重要インフラに対する国際的サイバー攻撃に対抗するための防衛手段を 2003 年までに設立するという目標を設定し、連邦捜査局（FBI）に National Infrastructure Protection Center （NIPC、現在は DHS の一部に組み込まれている）を設置した。その後、ブッシュ政権成立後に起こった同時多発テロをきっかけに、国家安全保障政策の中心として 2003 年 1 月より DHS が発足。これにあわせ、ブッシュ政権は PDD-63 から、ポスト 9/11 時代の DHS を中心とした国家重要インフラ保護ポリシーに置き換えることとなった。

こうした背景から HSPD-7 は、Homeland Security Act of 2002 を根拠とし、あらゆる重要インフラ保護に関する国家政策の中心に DHS を据える内容となっている。例えば、DHS 長官が米国 CI/KR 保護強化の先頭に立って活動し、国家として目指すべきポリシー、ガイドライン、メソドロジーなどを示すこととしている。また DHS は、自ら IT、電気通信、化学、交通システムなどに関する重要インフラの保護の取り組みを実施するとともに、他の連邦政府機関に対しても関連分野の重要インフラ保護を行うよう促し、複数の機関が関係するインフラについては、DHS が調整役となることを求めている。さらに、サイバーセキュリティに関しては、DHS 長官が重要インフラ・サイバーセキュリティの中核的存在となることを明言した。

この大統領令をより具体化し、実行に移すための目標設定を行うために、連邦政府機関は各機関が所有・管理する重要インフラ保護計画をまとめ、2004 年 7 月までに行政管理予算局（OMB=Office of Management and Budget）に提出、これを DHS が中心となってレビューを実施し、最終的に DHS がまとめる National Infrastructure Protection Plan に反映することとされた。

HSPD-7 に定められた各連邦政府機関が対象とするセクター

連邦政府機関	対象セクター
Department of Agriculture	Agriculture, food (meat, poultry, egg products)
Department of Health and Human Services	Public health and healthcare; Food (other than meat, poultry, egg products)
Environmental Protection Agency	Drinking water and wastewater treatment systems
Department of Energy	Energy, including the productions, refining, storage, and distribution of oil and gas, and electronic power (except for commercial nuclear power facilities)
Department of the Treasury	Banking and finance
Department of the Interior	National monuments and icons
Department of Defense	Defense industrial base
Department of Homeland Security	Information technology; telecommunications; chemical; transportation systems; postal and shipping; dams; government facilities; commercial facilities; Nuclear reactors; materials, and waste.

(2) DHS による重要インフラ・セキュリティ方針

① 重要インフラ・セキュリティ方針

DHS は HSPD-7 や各政府機関の計画などを受けて、2005 年 2 月、『暫定版　国家インフラストラクチャー保護計画（Interim National Infrastructure Protection Plan: Interim NIPP）』を発表した（270 日以内に発表される予定）。本計画書は、重要インフラ保護の取り組みを国家プログラムとして統一性を持たせるために、連邦・州・地方政府機関および民間セクターが一体となって取り組む枠組みを示したものである。

Interim NIPP は、重要インフラ保護における国家としての 5 つの目標と、それを達成するための具体的な目的、および官民が協力して行うべき活動（コア・アクション）を示している。

Interim NIPP による重要インフラ保護の国家レベルの目標

目標１：具体的かつ可能性のある脅威から重要インフラ／キー・リソース
＜具体的な目的＞ **●CI/KR セクター全体で、脅威の環境に対する認識を高める。** **●脅威や脆弱性に関する情報を、脆弱性削減活動の優先順位付けをする要素として利用する。** **●ある特定の脅威に対応する際、脆弱性評価に関する情報を利用する。** **●ある特定の脅威に対する保護措置を判別、導入する。**
＜コア・アクション＞ **■セクターごとおよびセクター横断型の保護計画を開発、導入する。** **■セクターごとのデータを基にして、セクターどうしの相互依存性分析を行う。** **■情報関連の重要インフラが未承認のまま公開されることがないよう保護する。**
目標 2：長期的に、包括的および統合的な手法で CI/KR の脆弱性を削減する
＜具体的な目的＞ **●CI/KR の資産（有形・無形）および脆弱性に関する包括的な国家目録を作成、管理する。** **●互いの資産どうし、および異なる CI/KR セクター間の相互依存性に関するマッピングを行う。** **●国家レベルの CI/KR の脆弱性評価を行う。** **●国家レベルの活動で重要インフラ保護活動とその他の活動が重複しないよう統合する。** **●必要な場合は、セクター内および複数のセクター間に存在する一般的な脆弱性を削減する。**
＜コア・アクション＞ **■CI/KR の資産を把握し、その情報を定期的に更新する。** **■セクター内、複数のセクター間、資産レベルでそれぞれ脆弱性評価を行い、定期的に更新する。** **■脆弱性評価のデータ分析を行い、法的に可能な範囲で関連機関と情報を共有する。** **■CI/KR を保護するための新技術を開発、導入する。**
目標 3：インフラ保護のためのリソースを最大限に利用する
＜具体的な目的＞ **●新たな保護措置の優先順位を決定する際は、特有の脆弱性や既存の保護措置、適用後の脅威に関する情報に照らし合わせた投資効果を考慮する。** **●HSPD-7 で指定されたセクターごとの管轄連邦政府機関（Sector-Specific Agency: SSA）がそれぞれの専門性を活用できるよう支援、奨励する。**

●重要インフラの所有者や運営管理者の自発的取り組みを促すような市場ベース型のインセンティブを見つける ●セクターごとの取り組みで教訓やベストプラクティスを確実に活かす。
＜コア・アクション＞ ■自己評価ツールを開発、管理、普及させる。 ■セクター内および複数のセクター間で資産の標準化や優先順位付けを行なう。 ■組織的な境界を越えた専門性の活用を促進する。 ■努力の重複を防ぐため、教訓を共有する。
目標４：CP プログラムの導入に連邦、州、地方政府、他国政府、民間セクターが協力して取り組む
＜具体的な目的＞ ●それぞれの役割や責任を明確に描写する。 ●責務を遂行するために必要な組織やスタッフ体制の確立、研修などを行う。 ●活動を実施するための予算や資金提供を当局に要請する。 ●パートナー間の情報交流や協調を促すメカニズムを確立する。 ●それぞれの関与や進展具合を把握するメカニズムを確立する。
＜コア・アクション＞ ■SSA 内で重要インフラ保護プログラムを実施するため組織を編成する。 ■ステークホルダーの間でパートナーシップを確立する。 ■DHS および SSA の間でパートナーシップを確立する。
目標５：継続的なトラッキングおよび国家的取り組みの向上
＜具体的な目的＞ ●国家レベルおよびセクター・レベルで、脆弱性および脆弱性削減努力の進展具合をトラッキングする メカニズムを確立する。 ●重要インフラ保護のイニシアチブや活動の重要性を強調するため、インフラ保護に関する活動や指標を組織全体の戦略上の活動や指標と位置付ける。 ●国家レベルのリスク・プロフィール（全てのセクターにおけるリスクや保護に関する要点）を作成し、戦略意思決定の際に役立てる。 ●教訓を迅速に広めるための情報共有システムを開発する。
＜コア・アクション＞ ■保護的策の成果を測定する指標を開発する。 ■CI/KR の保護的策の成果をトラッキングする。 ■必要に応じて NIPP を改訂する。 ■イニシアチブが目標や具体的な目的を支援していることを確実にする。

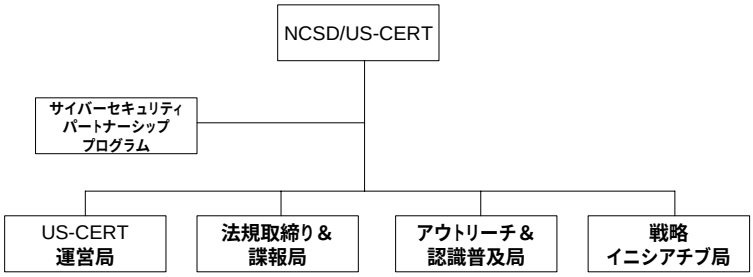
このほか、Interim NIPP **では、重要インフラを保護するために、**DHS **が中心となり、**SSA**、その他の連邦政府機関、州・地方政府、民間セクターの役割や責務などを包括的にまとめている。**

② DHS **の重要インフラ・サイバーセキュリティ対策不備を指摘する** GAO

この Interim NIPP **を含め、**DHS **による重要インフラ保護の取り組みに対して、**GAO（The Government Accountability Office : **政府説明責任局）は、『重要インフラ保護　サイバーセキュリティ上の責務を果たす** DHS **の課題（**Critical infrastructure protection. Department of Homeland Security faces challenges in fulfilling cybersecurity responsibilities）』と題する報告書を** 2005 **年** 5 **月に発表した。**

これは、重要インフラ保護の中でも、特にサイバーセキュリティに対するものであり、DHS **でサイバーセキュリティを専門とする組織として** 2003 **年** 6 **月に設置された「国家サイバーセキュリティ部門（**National Cyber Security Division: NCSD）」**の取り組みが不十分であるとの警鐘を鳴らすものとなった。**

NCSD **の組織図**



- **サイバーセキュリティパートナーシップ・プログラム（**Cyber Security Partnership Program）**：業界、政府、学界の間で効果的な官民パートナーシップの育成を目的としたプログラム。**
- US-CERT（Computer Emergency Readiness Team）**運営局（**US-CERT Operations Branch）**：**24 **時間体制でサイバー上の脅威の監視、警告、対応に取り組む** US-CERT **の運営部門。**
- **法規取締り＆諜報局（**Law Enforcement and Intelligence Branch）**：全米サイバー対応調整グループ（**National Cyber Response Coordinating Group）**の管理。法規取締り、諜報、民間セクターによる情報共有の促進。**
- **アウトリーチ＆認識普及局（**Outreach and Awareness Branch）**：国民のサイバーセキュリティに対する認識の強化。**
- **戦略イニシアチブ局（**Strategic Initiatives Branch）**：重要インフラ保護のサイバーセキュリティ強化、コントロールシステム・セキュリティ、ソフトウェア開発、研修および教育、（サイバー事故への）対応強化、標準およびベストプラクティスに関するイニシアチブを推進。**

また、GAO の同報告書によれば、この Interim NIPP は、国家レベルの目標やコア・アクションなどは明確に示しているものの、サイバーセキュリティに関連する問題を中心に、現時点では以下の問題が欠けているとし、次回発表される報告書ではこれらの点を盛り込む必要性を指摘した。

- **Interim NIPP には、セクターごとの具体的なサイバーセキュリティ計画が盛り込まれていない。**
- **Interim NIPP は最終計画ではない。NIPP は現在進行中の計画であり、これがさらに発展するためには、関係する連邦、州、地方政府機関や民間セクター、外国政府、国際機関などの関与が必要である。**
- **Interim NIPP には、それぞれの取り組みの達成具合を測るためのマイルストーンが盛り込まれていない。**

さらに、GAO は、DHS による重要インフラのサイバーセキュリティの取り組みには、鍵となる責務が 13 件あるとしている。

重要インフラ保護のサイバーセキュリティにおける DHS の責務

1）	サイバーセキュリティを含めた重要インフラ保護のための包括的な国家計画を開発すること。
2）	その他の連邦政府機関や州、地方政府、民間セクターとのパートナーシップを確立すること。DHS は、サイバーセキュリティのフォーカルポイントとして機能すること。
3）	パートナーシップやコラボレーションを通じて、サイバー攻撃や脅威、脆弱性に関する官民の情報共有を強化すること。
4）	米国のサイバー分析や警告システムに関する能力を開発および強化すること。
5）	インシデント対応や回復計画の策定に努力すること。サイバー関連の緊急時における回復計画で、関係機関のコーディネイトを行うこと。
6）	サイバー上の脅威や脆弱性の判定および評価を行うこと。
7）	サイバー上の脅威や脆弱性を削減する努力を支援すること。
8）	サイバースペースのセキュリティを強化するための研究開発を推進、支援すること。
9）	サイバーセキュリティに関する認識の普及やアウトリーチ活動を行うこと。
１０）	サイバーセキュリティ関連の研修や認定制度を奨励すること。
１１）	連邦、州、地方政府とパートナーシップを組み、国家の重要な情報インフラのサイバーセキュリティを強化すること。

１２）	他国の政府機関や国際機関、業界団体などを協力して、世界的なサイバーセキュリティの強化に取り組むこと。
１３）	国家インフラストラクチャー保護計画など、その他の国家セキュリティ計画と重要インフラのサイバーセキュリティを統合すること。

さらに GAO 報告書は、DHS による取り組みに一定の評価を示しているものの、上述した 13 の責務を十分に果たしているとはいえないとして、重要インフラのサイバーセキュリティ強化に関する DHS の能力を強化するため、DHS 長官に対して以下の 3 点を勧告した。

- 適切なステークホルダーを集め、サイバーセキュリティにおいて鍵となる責務の優先順位付けを行うこと。そうすることで、最も重要な活動から実施していくことができる。
- NCSD に対し、責務を遂行する上で障害となっている課題を克服するための活動に優先順位を付けさせること。
- 上記のことで優先順位付けされた活動の成果やマイルストーンを測定するための方法を特定すること。

一方、上記の GAO 報告書に関連して、7 月 19 日に上院国土安全保障・政府問題委員会（Committee on Homeland Security and Governmental Affairs）の連邦財政管理・政府情報・国際セキュリティ小委員会（Subcommittee on Federal Financial Management, Government Information, and International Security）が、「サイバーセキュリティ：国家の情報インフラを保護する努力は引き続き課題に直面している（Secure Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges）」と題する公聴会を実施した。

同公聴会で、トム・コバーン（Tom Coburn）委員長は、「HSPD-7、全米サイバースペース保護戦略（2003 年 2 月発表）、国土安全保障法（Homeland Security Act of 2002）によって、DHS はサイバーセキュリティの責務を負うことが明確に示されている。米国がサイバー攻撃の被害を受けないようにするには、計画、計画に伴う予算、計画を実施するための議会のコミットメントが必要である」と述べた上で、①NIPP の正式版の完成、②NIPP におけるマイルストーン（具体的な担当省庁が指定されること）の成果測定方法の決定、③マイルストーンに伴う予算アイテムの決定、に米国がコミットするよう望む、との見解を示した。

また、公聴会の証言者の一人である GAO のデイビッド・ポウナー（David Powner）氏は、「DHS は、自らに課せられた責務に対応するため、努力を開始し

たがまだ多くの業務が残っている」、「DHS は、サイバーセキュリティのフォーカルポイントとして自らを確立することができずにいる」といった見解を示した。

これに対して NCSD のドナルド・パーディ（Donald Purdy）ディレクター代理（Acting Director）は、「我々は、GAO 報告書は、現在までの進展に適正な評価を示していると考えている。と同時に、これまでに多くの取り組みがなされてきた一方、変化の激しいこの分野においてさらなる取り組みが必要であるという GAO の見解にも同意している」と述べている。そして、GAO が指摘した懸念の一つであるリーダーシップと組織上の問題に関して、7 月に新設が発表された「サイバー・通信セキュリティ担当次官補（Assistant Secretary for Cyber and Telecommunications Security）」は、こうした懸念に対処するものとなるであろうと、述べている。この新たな次官補ポストについては、チャートフ国土安全保障長官が 7 月 13 日に発表した国土安全保障省の組織再編計画の柱の一つである。同再編計画では、これまでの情報分析・インフラ保護局を「準備局（Directorate for Preparedness）」と名称変更するとともに、同局内に、重要な通信インフラおよび資産の脆弱性の発見・評価、脅威情報のタイムリーな提供、サイバーおよび通信への攻撃に対する国家的対応の先導の責任者として、サイバー・通信セキュリティ担当次官補を新設すると発表したものである。ただし、11 月 1 日現在、同担当次官補は任命されておらず、サイバーセキュリティ対策は従来どおり、NCSD が行っている。

2. 各連邦政府機関の取り組み

各連邦政府機関は、重要インフラ保護に関する国家プランを作成したり、官民の間で重要インフラのサイバーセキュリティに関する情報の共有を促進するなどの取り組みを行っている。以下は、こうした取り組みの一部をまとめたものである。

こうした具体例の中から、『財務省による金融サービス ISAC 支援』、『NIST による FISMA 導入プロジェクト』について説明する。

また、上記以外に、公的機関及び民間セクターにおける重要インフラ保護サイバーセキュリティ強化を目的とした GAO のフレームワークについても紹介する。

重要インフラのサイバーセキュリティ強化のための政策とその具体例

政策	概要や目的	具体例
「国家重要インフラ保護プラン」の作成	連邦政府による重要インフラ保護の活動の枠組みを示す。	2004 年 12 月の国土安全保障大統領指令（HSPD）7 に基づき、DHS は包括的な国家重要インフラ保護プランを作成することになっている（前述）。
リスク評価支援	セクターによるリスク評価に資金を提供するなどして脆弱性や脅威、およびこれらを削減する戦略の特定を支援する。	環境保護庁（EPA）はユーティリティ機関による飲料水の脆弱性評価活動に資金を提供。運輸省は、Global Positioning System を使った輸送セクターの脆弱性評価を実施。
重要インフラへの脅威・脆弱情報の提供	重要インフラに対する脅威や脆弱性を判断する政府の能力を強化し、それを民間に広めることで民間セクターのサイバー脅威に対する意識やサイバーセキュリティの必要性を強化する。	DHS は重要インフラに対する脅威情報を収集し、周知している。
重要インフラに関する情報共有の強化	連邦政府機関内および官民パートナーシップの情報共有システムを強化し、サイバー脅威に対する公的・民間セクターの意識を向上させる。	財務省による金融サービス ISAC 支援（後述）。EPA は、Association of Metropolitan Water Agencies による、諜報セクターと水セクターの間で最新の脅威・事故情報を共有するシステムへ 200 万ドルを提供。
標準およびガイドラインの開発	サイバーセキュリティ技術向けのプロトコルや製品標準、サイバーセキュリティを選択、導入、運営管理するためのガイドラインを開発する。	米国標準技術局（NIST）による標準およびガイドラインの開発（後述）。
外国政府との協力によるサイバー攻撃対策。	サイバー攻撃の発信地が米国内とは限らないため、外国政府と協力することはサイバー攻撃の追跡および犯人逮捕に重要である。	「サイバーセキュリティ国家戦略」（2003 年 2 月発表）では、米国がサイバー犯罪の捜査や起訴において国際協調を図るよう指示。HSPD-7 ではその責務を国務省に与えている。

(1) 財務省による金融サービス ISAC 支援

連邦政府機関が民間セクターとサイバー上の脅威に関する情報の共有を強化するために行っている取り組みの一つとして、財務省は、金融機関の業界団体、金融サービス ISAC（Financial Services/Information Sharing and Analysis Center: FS/ISAC）の活動を支援している。

1998 年に、米国の重要インフラを保護するために物理的およびサイバー上の脅威や脆弱性に関する情報を官民セクターが共有するよう指示した大統領決定指令（Presidential Decision Directive-63）PDD-63 が発令され、これに応える形で金融サービス機関による FS/ISAC が発足した。FS/ISAC は、金融サービス機関や商業セキュリティ機関、連邦・州・地方政府機関から、信頼性がありタイムリーなセキュリティ情報を常時収集し、加盟機関へ配信している。また、加盟機関から脅威や脆弱性に関する情報が送られてきた場合は、専門家が検証、分析するとともに推奨ソリューションを特定し、加盟機関へ警告を配信をしている。財務省および DHS は、金融サービス機関に対して FS/ISAC に加盟するよう奨励しており、現在、加盟機関は 1500 社を超えるという。

また財務省は、2003 年 12 月に、FS/ISAC に対して、米国内の金融サービス機関における物理的およびサイバー上のセキュリティ意識を強化する策を実施するよう求めるとともに、200 万ドルの資金を提供している。これを受けて FS/ISAC は、重要な警告情報をより速く、ほぼ同時に配信でき、ユーザ認証および受信確認機能を備えた「重要インフラストラクチャー通知システム（Critical Infrastructure Notification System）」を開発した。

(2) NIST による FISMA 導入プロジェクト

2002 年 12 月に制定された「電子政府法（E-Government Act）」のタイトル III、「連邦情報セキュリティ管理法（Federal Information Security Management Act: FISMA）」では、各連邦政府機関に対して、各機関の業務や資産を支える情報および情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践するよう求めている。これを受けて、米国標準技術局（National Institute of Standards and Technology: NIST）は、「FISMA 導入プロジェクト（FISMA Implementation Project）」を開始し、情報システム・セキュリティの標準やガイドラインの開発を進めている。

FISMA 導入プロジェクトは、以下の 3 つのフェーズで構成されている。

- フェーズ I（2004～2005 年）：セキュリティの標準およびガイドラインの開発
- フェーズ II（2006 年度予定）：認定プログラムの開発

- **フェーズ** III**（**2006 **年度予定）：セキュリティ・ツール検証プログラムの開発**

現在はフェーズ I **で、これまでに以下の** 9 **種理の標準やガイドラインが発表されている。**

- **連邦政府の情報および情報システムのセキュリティ分類に関する標準**
- **セキュリティ分類のための情報および情報システムのマッピングに関するガイドライン**
- **連邦情報システムに関する推奨セキュリティ・コントロール**
- **連邦情報システムにおけるセキュリティ・コントロール評価に関するガイド**
- **連邦情報システムのセキュリティ証明および認証に関するガイド**
- **国家セキュリティ・システムとしての情報システムの判別に関するガイド**
- **連邦情報システムのセキュリティ・コントロール**
- **情報システムおよびセキュリティ・プログラムの評価ガイド**
- **情報システムのためのセキュリティ計画策定に関するガイド**

フェーズ II **の認定プログラムの開発では、連邦政府機関向けにセキュリティ証明サービスを提供する公的・民間機関を認定するプログラムの開発に取り組む。セキュリティ証明サービスとは、情報システムに関する管理、運営、技術面のセキュリティ・コントロールを包括的に評価し、これらのコントロールが正しく導入されているか、目的どおりに運営されているか、必要とされるセキュリティ条件を満たす成果をもたらしているかを判断するサービスである。セキュリティ証明サービス機関は、認定プログラムに参加することで、**NIST **が開発したセキュリティの標準やガイドラインを活用する能力を有していることを示すことができる。認定を受けたセキュリティ証明サービス機関のネットワークが拡大すれば、サービスを利用する連邦機関からの信頼性も向上するであろう。**

フェーズ III **では、商業向けおよび政府向けに市販されているセキュリティ・ツールを検証するためのプログラムの開発に取り組む。フェーズ** III **では、**NIST **の承認を受けた民間研究所で、セキュリティ・ツールの評価が行われる。フェーズ** III **の開始にあたり、製造側および利用者側からの意見を集め、**NIST **の承認研究所としてセキュリティ・ツールの評価を行う民間研究所を募るため、ワークショップが開催される予定である。**

(3) GAO **による重要インフラ保護のためのフレームワーク**

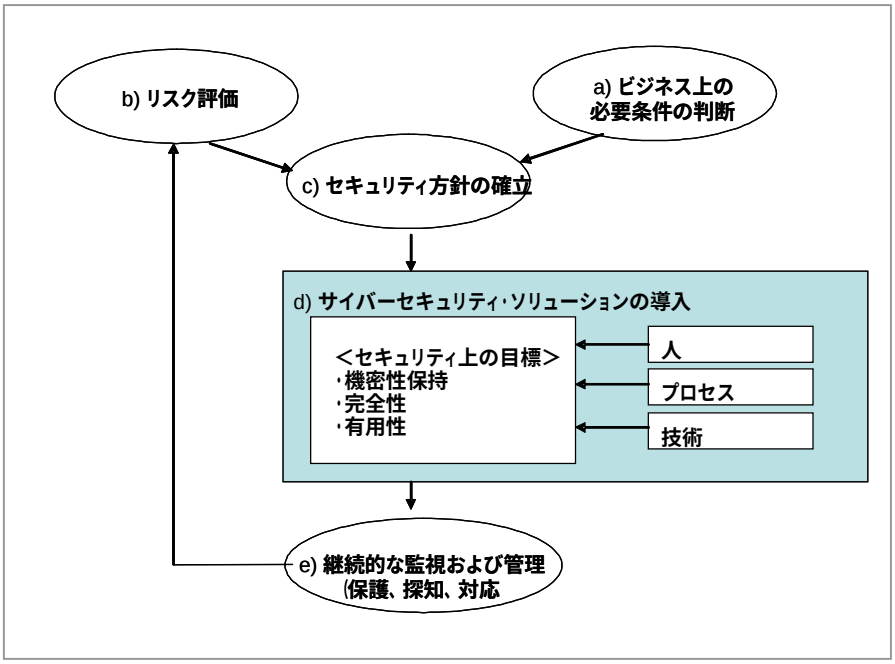
GAO **は、**2004 **年** 5 **月、『技術評価　重要インフラ保護のためのサイバーセキュリティについて（**Technology Assessment: Cybersecurity for critical infrastructure

protection）』と題する報告書を発表した。この中で、重要インフラ保護におけるサイバーセキュリティ上の脅威及びその対策技術についての現状を分析し、これをベースとして政府機関だけでなく民間セクターでの適用可能なセキュリティ技術導入のためのフレームワークを提示した。また、産官学が将来に向けてさらなる研究開発を進めるべき分野についても指摘している。

①　サイバーセキュリティ導入のためのフレームワーク

GAO は a) ビジネス上の必要条件の判断、b) リスク評価をベースとして、それを基に c) セキュリティ方針の確立、d) サイバーセキュリティ・ソリューションの導入を行い、その後も e) 継続的な監視及び管理を行うというフレームワークを提示した。

重要インフラのサイバーセキュリティ導入のフレームワーク



a) 重要インフラにおけるサイバーセキュリティ技術導入の第一歩として、組織としてのニーズや、保護すべきコンピュータ・リソースや情報（プライバシー保護などに関する法規の遵守も含め）を特定、判断する。
b) ビジネス上の必要条件の判断及びリスク評価に基づき、セキュリティ方針を確立する。
c) セキュリティ方針の詳細は各機関の業務や機能によって異なるが、セキュリティ方針の目標の基本的な共通項として、機密性、完全性、有用性を確実にすることが挙げられる。これらのセキュリティ上の目標は、人、プロセス、技術を

駆使したサイバーセキュリティ・ソリューションを導入することによって達成される。

d) さらに、サイバーセキュリティ・ソリューションを導入した後も、コンピュータ・リソースや情報を保護するために、サイバー関連の事故の探知や対応を継続的に行う。

また、同フレームワークは一度行えば十分というものではなく、サイバーセキュリティ・ソリューションの導入後も、継続的な監視および管理を行い、リスク評価の見直しを図り、必要に応じてセキュリティ方針を改善することが重要であるとしている。

② さらなる研究が必要とされる分野

重要インフラを保護するために有効なサイバーセキュリティ技術はいくつかあるものの、新たな脆弱性は頻繁に発見されており、これらに対応する新技術のニーズは常に高い。現在、連邦政府や学界、民間セクターなどがさまざまな新技術の研究開発に取り組んでいる。GAO 報告書『技術評価　重要インフラ保護のためのサイバーセキュリティについて（Technology Assessment: Cybersecurity for critical infrastructure protection）』は、その中から重要なサイバーセキュリティ研究分野として、以下の 6 項目を挙げている。

さらなる研究が必要とされるサイバーセキュリティ分野

１．脆弱性の判別および分析	製品やシステムのライフサイクルを通じて、ハッカーなどの攻撃に利用されそうな欠陥があるかどうか、セキュリティ上で予測外の問題が発生しているかどうかを判断するより良い手法が求められている。コードや機器、システムなどを総合的に分析する技術やツールが必要である。
２．不安定なコンポーネントから確実なシステムを構築する技術	障害から修復している間、セキュリティを維持しつつ、異機種による複雑なシステムを構築するための手法に関する研究が必要である。よりセキュアなシステムを構築するためには、生物学的手法やインテリジェント・マイクロシステムの利用などの新手法が検討されるであろう。
３．セキュリティ・メトリクスと評価	あらゆる方面（経済、組織、技術、リスク）からセキュリティ管理のコストや利点、影響を測定する指標の研究が必要である。これにより、セキュリティ上の決定の効果を測定することが容易になる。

４．ワイヤレス・セキュリティ	セキュリティをワイヤレス・ネットワークの基本的要素とすること、ワイヤレス・セキュリティの基礎科学の開発、ワイヤレス機器本体に組み込むセキュリティ・ソリューションの開発、既存のワイヤレス・プロトコルのセキュリティ面での調査などで研究が必要である。
５．セキュリティの社会経済的影響	サイバーセキュリティの規模や、インフラ保護に関係する法律や政策、技術への影響を判断するための研究が必要とされている。また、サイバーセキュリティ市場の構造や力学を把握するための研究、サイバーセキュリティ強化における標準やベストプラクティスの役割に関する研究、情報インフラに関するデータの収集や利用に関連した政策や法的意味合いの検討なども必要である。
６．ネットワーク・システムのセキュリティ	電力や石油、ガス、水といった分野のネットワーク・システムのセキュリティ評価に関する研究が必要である。ネットワーク・システムにセキュリティを組み込み、ネットワーク上の異常を探知し、それに対応する技術が求められている。

3. 連邦政府機関と協力する民間セクターの取り組み

政府以外に民間セクター、特に重要インフラを抱える業界では、連邦政府機関と協力し、業界独自の取り組みを進めている。たとえば、重要インフラを抱える業界と管轄の連邦政府機関の間で情報共有分析センター（Information Sharing and Analysis Center: ISAC）を確立している業界は少なくない。以下では、金融およびエネルギー業界における取り組みについて紹介する。

(1) 金融業界：FSSCC の取り組み

金融業界において重要インフラの保護を目的として活動する業界団体として、上述した FS/ISAC のほかに、2002 年に設立された金融サービス・セクター調整評議会（Financial Services Sector Coordinating Council: FSSCC）がある。FSSCC の加盟機関は、America’s Community Bankers や American Insurance Association などの業界団体が多く、FS/ISAC も FSSCC の加盟機関の一つとなっている。FSSCC も FS/ISAC 同様、財務省と協力しながら活動している（加盟機関は合計 31 団体・企業）。FSSCC は、さまざまな連邦政府機関や業界団体と協力しながら、米国金融セクターの安全保障強化に取り組んでいる。

FSSCC は 2004 年 5 月に、「金融サービス・セクターにおける重要インフラ保護のための国土安全保障戦略（Homeland Security Strategy for Critical Infrastructure

Protection in the Financial Services Sector）」と題する報告書を発表し、その中で金融セクターによる重要インフラ保護および国土安全保障強化のための戦略目標として、以下の 3 点を掲げた。

- 「金融サービス・セクターの脆弱性の認識およびその削減」：
  金融サービス・セクターのインフラストラクチャー上で、組織的攻撃や犯罪、違法行為、その他の破壊的な事件につながる可能性のある脆弱性を認識および削減すること。

- 「金融サービス・セクター・インフラの柔軟性強化」：
  金融サービス・セクターのインフラストラクチャーの柔軟性を確実にすることで、攻撃による損害を最小限にとどめ、回復を迅速に進めること。

- 「国民の信頼の強化」：
  金融サービス・セクターには攻撃に耐える能力、また攻撃から回復する能力があると国民が確信できるよう、米国の金融サービス・セクターに対する信頼を強化すること。

FSSCC は 2005 年 1 月に、これらの戦略目標に関して FSSCC および加盟機関による 2004 年の達成事項をまとめた報告書「米国金融セクターにおける重要インフラストラクチャーの保護　2004 年の成果（Protecting the U.S. Critical Financial Infrastructure: 2004 in Review）」を発表した。同報告書では、2004 年の達成事項として、以下のような点が挙げられている。

- 戦略目標 1：「金融サービス・セクターの脆弱性の認識およびその削減」

  - FS/ISAC の加盟機関拡大：
    戦略目標 1 における主要活動の一つは、金融機関による重要インフラ保護情報の共有を強化する方法として、FS/ISAC への加盟を奨励することである。FS/ISAC は加盟機関の拡大を図るため、メンバーシップのカテゴリーを拡大するなど努力した。こうした結果、当初 66 機関だった加盟機関は、メンバーシップ・カテゴリー拡大を経て、2004 年末には約 1000 機関に急増した。

  - フィッシング対策：
    金融機関になりすまして消費者へ電子メールを送り、消費者の口座番号やクレジットカード番号などの個人情報を盗み出す詐欺行為『フィッシング（phishing）』が増加しており、金融サービス・セクターはこれへの対策に迫られている。こうした詐欺行為の急増を受け、FSSCC は、金融・

銀行情報インフラストラクチャー委員会（Financial and Banking Information Infrastructure Committee: FBIIC）（注：FBIIC は、金融業界規制担当官どうしの調整やコミュニケーションの強化、金融セクターの柔軟性の強化、官民パートナーシップの推進を行なう連邦政府機関）とともに、フィッシング攻撃の見分け方や対策をまとめたガイダンス、「最近のフィッシング攻撃急増における消費者、金融セクター企業、政府機関の教訓（Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies during the Recent Rise of Phishing Attacks）」を共同発表した。

- 脆弱性の認識とその対策：
  FSSCC の加盟機関である BITS/Financial Services Roundtable は、金融サービス・セクターの企業が自社の情報技術インフラにおける脆弱性を認識し、その対策を行うための「ベストプラクティス」をまとめた報告書をいくつか発表した。

- インターネットの活用：
  FSSCC の加盟機関である証券業界協会（Securities Industry Association: SIA）が加盟機関向けに、緊急時にビジネスを続行するための戦略やプラクティス、関連規制やルールなどに関する情報を提供するウェブサイトを運営するなど、多くの団体が、重要インフラ保護や国土安全保障に関する情報を提供する手段としてインターネットを活用している。

- 戦略目標 2：「金融サービス・セクター・インフラの柔軟性強化」

  - 適切なプラクティスの推進：
    FSSCC は、2003 年 4 月に連邦準備制度理事会（Board of Governors of Federal Reserve System）や証券取引委員会（Securities and Exchange Commission）などが共同発表した「米国金融システムの柔軟性を強化するための適切なプラクティスに関する報告書（Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System）」の中で示された健全なプラクティスを加盟機関に奨励している。
    同報告書では、米国金融市場を支える重要機関および重要活動を対象に、①緊急事態に金融市場での取引を予定通りに完了するための方法を確立しておくこと、②緊急事態発生後、業務を回復するまでの目標時間を設定しておくこと、③地理的に十分に離れた所にバックアップ体制を整えておくこと、④業務回復計画を定期的に見直し検査すること、の 4 つを適切なプラクティスとして推奨している。

- **危機対応会議の拡大：**
  同時多発テロ事件後、各業界団体は危機発生時に対応策を検討するための会議を早急に実施できる体制作りに乗り出したが、2003 年に米国北東部州を襲った大停電後、こうした危機対応策会議は１業界のみならず、より大きなセクター全体で実施できるようにすべきであるとの認識が高まった（具体的には、証券業界や銀行業界といったそれぞれの業界団体で会議を行うのではなく、金融セクター全体で会議することにより他業界での動きも分かるようにするということ）。FSSCC は 2004 年に、緊急事態が発生した際、金融セクター全体で対応策会議を実施できるよう、危機管理対策会議リストを作成、発表した。加盟機関はこのリストを利用することで、金融セクター全体の情報共有や通知が可能になる。

- **戦略目標 3：「国民の信頼の強化」**

  - **従業員の安全確保：**
    金融サービス・セクターに対する国民の信頼を強化するには、緊急事態時にもビジネスを続行する能力を有していることが重要である。そのためには、金融サービス・セクターの従業員の安全を確保しなくてはならない。従業員の安全確保は基本的には各企業の責任であるが、FSSCC の加盟機関である証券業界協会（Securities Industry Association: SIA）では、ビジネス続行計画委員会の従業員準備対策小委員会が、従業員の安全性とビジネス続行計画に関する問題を扱い、それらの情報を加盟証券会社向けに提供している。

  - **アウトリーチ活動：**
    FSSCC は、連邦預金保険機構（Federal Deposit Insurance Corporation: FDIC）と共同で、インフラストラクチャー保護に関する問題を協議するアウトリーチ・プログラムを共同で実施した。アウトリーチ・プログラムは全米 28 都市で開催され、金融セクターの約 4100 社に、物理的およびサイバー上の脆弱性への対応策や FS/ISAC に関する情報、重要インフラ保護に関する話題を提供することができた。

  - **ビジネス続行とセキュリティに関する会議：**
    FSSCC の加盟団体の多くが、それぞれの加盟機関を対象に、ビジネス続行やセキュリティに関する会議を開催している。たとえば、米国コミュニティ銀行協会（America’s Community Bankers）は、加盟銀行向けに、物理的およびサイバー上のセキュリティ問題やビジネス続行、ネットワーク・セキュリティ管理などに関するセッション会議を実施したほか、連邦

信用組合協会（National Association of Federal Credit Unions）もセキュリティ問題に関して合計 37 回の会議を開催した。

(2) エネルギー業界：NERC

北米市場の電力システムの信頼性やセキュリティを確実にすることを目的とし、1968 年に設立された北米電力信頼性評議会（North American Electric Reliability Council: NERC）は、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フォーカルポイントとしての役割を担っている。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、民間ユーティリティ機関、連邦電力機関、地方の電力協同組合、州・地方公共団体のユーティリティ機関、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。

具体的には、エネルギー省が、電力業界における重要インフラ保護活動の調整機関として NERC を指定しているほか、NERC は、DHS やカナダ公共安全・緊急時準備対策（Public Safety ad Emergency Preparedness Canada）とも密接な協力関係にある。NERC による重要インフラ保護活動としては、以下のようなものが挙げられる。

① 電力セクター情報共有・分析センター（Electricity Sector Information Sharing and Analysis Center: ESISAC）としての機能

NERC は、電力セクターの情報共有・分析を担う機関として、業界および政府の間でセキュリティ関連の情報を収集、分析、拡散している。NERC が重要インフラ保護活動の一環として運営している ESISAC のウェブサイトでは、DHS やエネルギー省による脅威レベルおよび、電力セクター向けの脅威レベル（物理的、サイバー上）を表示しているほか、重要インフラ保護に関する勧告や警告などを発信している。

② 重要インフラ保護委員会（Critical Infrastructure Protection Committee: CIPC）設置

CIPC は、NERC によるセキュリティ関連のイニシアチブを調整している部門で、サイバーセキュリティ、物理的セキュリティ、セキュリティ運営管理などの分野の専門家によって構成されている。CIPC には、セキュリティ上の脅威や事故への対応強化を目的として、ESISAC の機能の強化に取り組む ESISAC 小委員会と、重要インフラストラクチャーを保護するための電力システムの強化に取り組むセキュリティ・プランニング小委員会がある。CIPC および両小委員会は、電力セクターの重要インフラの保護や、緊急事態の抑止、拡散防止、緊急事態からの迅速な回復などに関するワークショップやフォーラムなどを開催している。

③ **電力セクターのためのセキュリティ・ガイドライン**（Security Guidelines for the Electricity Sector）**作成**

NERC は、電力セクターの重要施設を物理的およ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「電力セクターのためのセキュリティ・ガイドライン」を作成した。本ガイドラインには、脆弱性やリスクの評価、ビジネス続行、物理的およびサイバー上のセキュリティ、重要な情報の保護、といった問題について、勧告や参考資料が盛り込まれている。サイバーセキュリティに関する項目としては、リスク評価、アクセス・コントロール、IT ファイアウォール、侵入探知などがある。

④ **サイバーセキュリティ標準**（Cyber Security Standard）**作成**

NERC は 2003 年 8 月、サイバーセキュリティ標準を採択した。これは、電力グリッドの信頼性強化や電力市場の円滑な運営に欠かせない電子情報のセキュリティを確実にするための最低限の必要条件をまとめたものである。また、このサイバーセキュリティ標準は、2006 年の正式版採択を目標とし、それまでの「緊急対策（Urgent Action）」版として 2003 年に採択したもので、その後、2004 年、2005 年と更新されている。上述③のセキュリティ・ガイドラインは自発的なガイドラインであるのに対し、このサイバーセキュリティ標準は加盟機関にコンプライアンスが義務付けられている。

現在、適用されているサイバーセキュリティ標準の項目と、その内容の一部は以下の通りである。

NERC によるサイバーセキュリティ標準の項目とその一部

●サイバーセキュリティ	●電子アクセスの監視
●重要なサイバー資産	●情報保護
●電子セキュリティ関連	●研修
●電子アクセス・コント	●システム管理
●物理的セキュリティ関	●検査手順
●物理的アクセス・コン	●電子事故対応
●人事	●物理的事故対応
●物理的アクセスの監視	●復旧計画

サイバーセキュリティ標準の内容（一部）

サイバーセキュリティ方針
＜要件＞ ●適用対象機関は、サイバーセキュリティ方針を確立、保持する必要がある。（注：NERC は現在、サイバーセキュリティ標準がどの機関に適用されるかについて検討中であり、暫定版においては、発電、配電、管理、運営などに関わるさまざまな機関に適用されるとしている。 ●適用対象機関は、上級管理職メンバーの中から、サイバーセキュリティ・プログラムを主導、管理する責任を負う者を任命する。本標準で求められている要件から逸脱または例外措置を設ける場合、この責任者によって承認されなくてはならない。また、逸脱・例外措置が実施される場合、その理由を文書にしなくてはならない。
＜方策＞ ●重要なサイバー資産を保護するコミットメントを表明したサイバーセキュリティ方針を文書化し、それを保持する。 ●サイバーセキュリティ方針を少なくとも年に 1 回見直す。 ●サイバーセキュリティ・プログラムの責任を負う上級管理職者の氏名、肩書き、電話番号、連絡先、任命日を明示する。 ●サイバーセキュリティ・プログラムの責任を負う上級管理職者が承認した逸脱・例外措置の理由を示した文書を保持する。
＜コンプライアンス監視プロセス＞ ●適用対象機関は NERC のコンプライアンス監視部門に自己証明（self-certification）を毎年提出する。コンプライアンス監視部門は 3 年ごとに現場視察を行い、異議申し立てがあれば調査を行う。 ●パフォーマンス評価の期間は 1 年間（暦年）とする。適用対象機関はデータを 3 年間、コンプライアンス監視部門は監査記録を 3 年間保持する。 ●コンプライアンス監視部門の要請があった場合、適用対象機関は、サイバーセキュリティ方針を示した文書、責任を負う上級管理職者の氏名・肩書き・連絡先・電話番号・任命日、逸脱・例外措置の理由を示した文書を提出すること。
＜非コンプライアンス・レベル＞ レベル 1：責任を負う上級管理職者が、暦年で 30 日未満任命されていない。またはサイバ

ーセキュリティ方針文書は存在するものの、昨年（暦年）1 度も見直しされていない。 レベル 2：責任を負う上級管理職者が、暦年で 30 日以上 60 日未満、任命されていない。 レベル 3：責任を負う上級管理職者が、暦年で 60 日以上 90 日未満、任命されていない。 レベル 4：責任を負う上級管理職者が、暦年で 90 日以上任命されていない。またはサイバーセキュリティ方針がない。
重要なサイバー資産
＜要件＞ ●適用対象機関は、重要なサイバー資産（インストールされたソフトウェアや電子データを含むコンピュータ、通信ネットワークなど）を把握する必要がある。
＜方策＞ ●重要なサイバー資産に関する情報を文書化し、管理する。 ●少なくとも年に 1 回、または重要なサイバー資産を拡充・廃棄してから 90 日以内に、重要なサイバー資産に関する文書を見直し・改訂する。
＜コンプライアンス監視プロセス＞ ●適用対象機関は NERC のコンプライアンス監視部門に自己証明（self-certification）を毎年提出する。コンプライアンス監視部門は 3 年ごとに現場視察を行い、異議申し立てがあれば調査を行う。 ●パフォーマンス評価の期間は 1 年間（暦年）とする。適用対象機関はデータを 3 年間、コンプライアンス監視部門は監査記録を 3 年間保持する。 ●コンプライアンス監視部門の要請があった場合、適用対象機関は、重要なサイバー資産のリスト、重要なサイバー資産の文書が正しく見直し・改訂されていることの証明を提出すること。
＜非コンプライアンス・レベル＞ レベル 1：文書は存在するが、重要なサイバー資産の拡充・廃棄から 90 日以内に改訂されていない。 レベル 2：文書は存在するが、過去 12 ヶ月間見直し・改訂されていない。 レベル 3：（とくに明文化されていない） レベル 4：文書が存在しない。

※いずれの項目においても、非コンプライアンス・レベルが認められた場合、まずは文書による制裁が実施される。制裁は、回数やレベルが増えるにつれて厳しくなり、罰金制裁（最高 1 万ドル）も発生する。

（参考資料）

http://www.fas.org/irp/offdocs/nspd/hspd-7.html
http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,86956,00.html
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
http://whitehouse.fed.us/omb/memoranda/fy04/m-04-15.pdf
http://www.deq.state.mi.us/documents/deq-wb-wws-interim-nipp.pdf
http://www.gao.gov/new.items/d05434.pdf
http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=261
http://hsgac.senate.gov/_files/071905Coburn.pdf
http://hsgac.senate.gov/_files/GAOstatement05827T.PDF
http://www.dhs.gov/dhspublic/display?theme=43&content=4598&print=true
http://www.fsisac.com/
http://www.fas.org/irp/offdocs/pdd-63.htm
http://csrc.nist.gov/sec-cert/
http://www.gao.gov/new.items/d04321.pdf
http://www.fsscc.org/annual.pdf
http://www.nerc.com/
http://www.esisac.com/
ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jp **までお願いします。**