## ２．米国におけるサイバー犯罪への対応

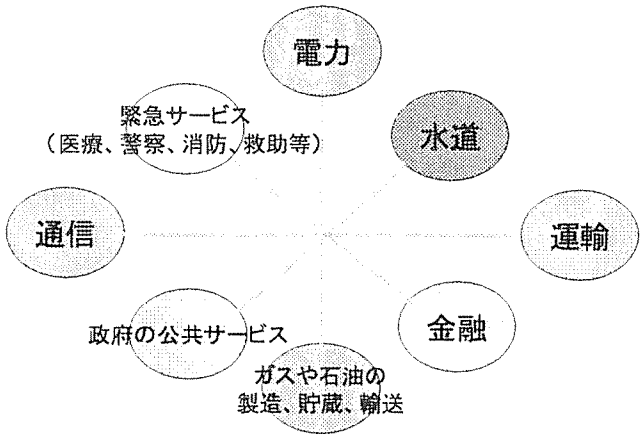
### （１）基本構造

米国におけるサイバー犯罪への対応は下記の２つの大統領命令により成り立っている。

・EO13010（1996）
PCCIP(The President's Commission on Critical Infrastructure Protection 重要インフラに関する大統領委員会）、Advisory Committee、インフラ防衛対策委員会（IPTF）を設立。これらは、米国の主なサービスに対する物理的な脅威とサイバーアタックの両方に対処するための必要性に応えるもの。

・PDD63（1998）
下記の 8 大重要インフラを保護するために、2003 年までに信頼性の高い相互接続された強固な情報システム・インフラを確立せよというもの。

図表３　EO13010 で指定された８つの重要インフラストラクチャ




図表４　８大インフラの担当官庁と計画策定状況（2001 年末現在）

| インフラ | 担当官庁 | ステータス |
|---|---|---|
| 電力 | エネルギー省 | 計画未策定 |
| 水道 | 商務省 | 計画未策定 |
| 運輸 | 運輸省 | 計画未策定 |
| 金融 | 財務省 | 計画策定済 |
| ガスや石油の製造、貯蔵、輸送 | エネルギー省 | 計画未策定 |
| 政府の公共サービス | CIAO | 計画未策定 |
| 通信 | FCC | 計画策定済 |
| 緊急サービス | FEMA | 計画未策定 |

CIAO：主要インフラ保証局

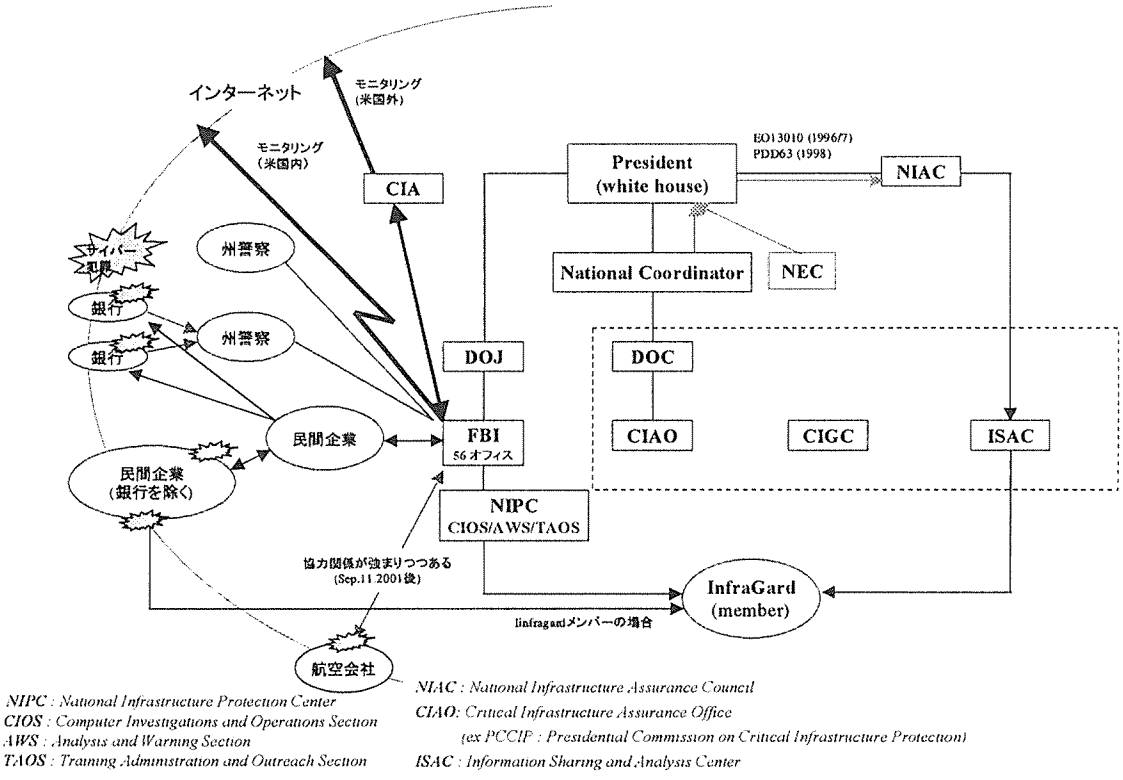
FCC：米国連邦通信委員会

FEMA：米国連邦緊急事態管理局

上記の担当官庁の最高情報担当責任者（CIO）が各担当インフラにおける情報関連の安全を確保する責任を負う。しかし、重要インフラの多くは民間企業によって運営されており、政府と民間が協力してインフラ保護を行うことが重要との認識から、PCCIP（The President's Commission on Critical Infrastructure Protection：重要インフラに関する大統領委員会）の結論として官民が協力してインフラ保護に関する情報交換を行う組織としてISAC（Information Sharing and Analysis Center：情報共有分析センター）を設置している。

さらに、PDD63においては、FBIの傘下に政府機関と民間部門からメンバーを参加させたNIPC（National Infrastructure Protection Center：全米インフラ保護センター）を設置している。

図表５　米国におけるサイバー犯罪への対応体制




## （２）主要機関

### ①ISAC

ISACは民間企業同士の「セキュリティ情報の共有」を目的とした非営利団体であり、重要インフラ毎にISACを設立しつつある。2001年末現在で、IT、金融、エネルギー（電力、石油）、通信で設立済みであり、運輸ISACが近々設立の見通しである。

【例：IT-ISAC】
・担当官庁：商務省
・参加企業：マイクロソフト、オラクル、HP など 19 社
・設立費用：総額 75 万ドル（年会費：5000 ドル）

ISAC と政府との連絡は CICG（Critical Infrastructure Coordination Group：重要インフラ調整グループ）を通して各担当官庁と行っている。

図表 6　代表的な ISAC の状況

| | 政府との関係 | | 運営状況 | |
|---|---|---|---|---|
| | 構成組織 | NIPCとの連携 | 緊急対応の実施体制 | 運営資金等 |
| IT-ISAC（IT業界） | 民間企業のみで構成<br>・IT関連企業<br>・ITAA（IT業界団体） | 情報提供は各会員企業の判断 | 民間企業(ISS) | 会員企業より調達<br>5000ドル／年 |
| Telecom ISAC（通信業界） | 官民の組織で構成<br>・政府機関<br>・NCC加盟企業 | NIPCとの情報共有の仕組み構築を検討中 | 政府機関（NCC） | 政府より調達 |
| FS/ISAC（金融業界） | 民間企業のみで構成<br>・金融関連企業 | NIPCとの情報共有の仕組み構築を検討中 | 民間企業(Global Integrity) | 会員企業及びGlobal Integrityより調達<br>7000ドル／年 |
| Electric Power ISAC（電力業界） | 官民の組織で構成<br>・業界団体のNERCに加盟する官民基幹 | ISAC／NIPC双方向の情報提供 | ・業界団体（NERC）<br>・政府機関（NIPC） | 値ＲＣを通じて調達 |

NCC：National Coordination Center for Telecommunication
ISS：Internet Security Systems
NERC：North American Electric Reliability Council

②NIPC
●使命
「コンピュータ侵入などに関わる不正行為、または米国のクリティカル・インフラを標的とした物理的およびサイバー上の不正行為に対し、それを検知し、警告を発し、対処し、捜査を行う」こと。

●参加機関
国防省、諜報機関、陸海空軍、Air Force Office of Special investigations, Defense Criminal Investigative Service, National Security Agency, United States Postal Service, Federal Aviation Administration, General Services Administration, Central Intelligence Agency(CIA), Critical Infrastructure Assurance Office, Sandia National Laboratory など。地方政府もローテーションで参加。これまでオレゴン州警察、アラバマ・タスカルーサ州の警察が参加。

●NIPC の構成

NIPC は下記の 3 つのセクションで構成されている。

| |
|---|
| ・CIOS (Computer Investigations and Operations Section：コンピュータ捜査・運営セクション) |
| ・AWS (Analysis and Warning Section：分析・警告発信セクション) |
| ・TOSS (Training, Outreach and Strategy Section：トレーニング・啓発・戦略セクション) |

・CIOS

同セクションは、コンピュータ不正侵入に関する捜査の支援を行う。被害に遭ったコンピュータを捜査する際の技術的サポートの提供、またはクリティカル・インフラへのサイバー攻撃に対処するために編成されたサイバー・イマージェンシー・サポート・チーム (Cyber Emergency Support Team) の運用などを行う。

・AWS

同セクションは、米国におけるクリティカル・インフラに対する国内外からの物理的およびサイバー・リスクを評価・分析し、その結果を発信する。情報センターとしての役割を担い、リアルタイムで警察、諜報、一般情報ソース、自発的に提供された民間データなどを収集し、政府と民間セクターに配信するため、官民をつなぐハブとしての役割を果たしている。双方のパートナーシップをより確実なものにするために、監視センター (Watch Operations Center) を1日24時間、毎日運営し、サイバー・アタックに関する情報発信を行っている。

・TOSS

連邦、州、地方警察機関と民間セクター、学際グループとの共同学習の場を提供し、情報交換を促進する。

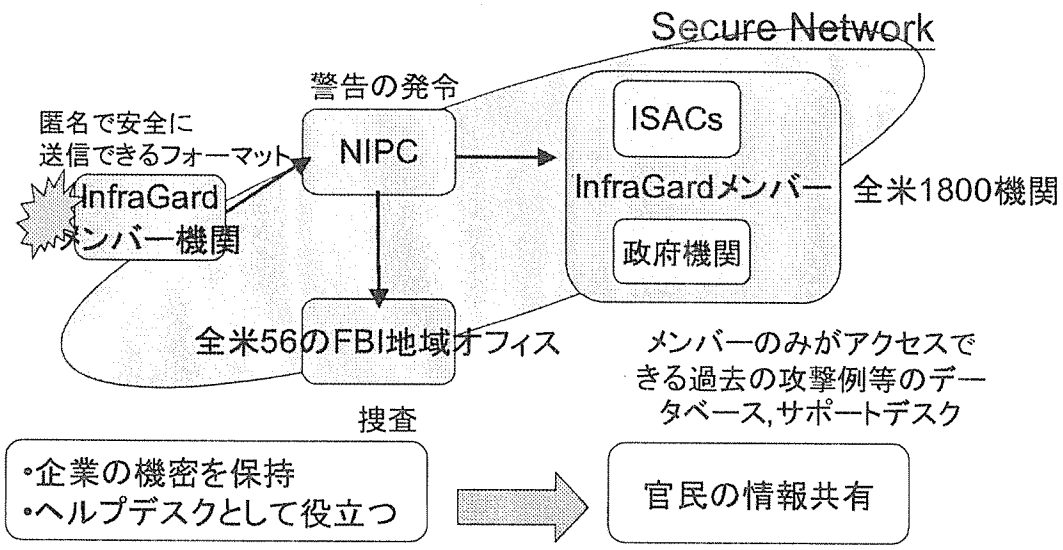
●NIPC が実施しているプログラム

・InfraGard

FBI をスポンサーとし、企業、研究機関、政府関係機関の約 1800 機関からなる組織である。法的に、及び財政的に政府のコントロール下から独立しており、その設立目的は基礎的インフラストラクチャの保護に関する情報の交換である。システムへの攻撃や情報漏洩に関して、問題点を共有し、自主的に他のメンバーや FBI に情報を提供するフォーラムを主催する。参加企業が共有したいと考えるシステムへの攻撃に関する情報のデータベースを構築・維持している。しかし、FOIA

（情報自由法）のために外部に公開されると言う潜在的な問題点が指摘されている。

図表７　InfraGard プログラムにおける情報の流れ




・the Key Asset Initiative (KAI)：民間―政府協力のため取り組み

FBI フィールドオフィス管轄内の重要資産(key asset)の決定をし、非常時に備えた Key asset との 24 時間の連絡体制を取っている。将来的にはそれぞれの Key asset へのアタックへの対応、対応演習、Key asset が攻撃されたときの被害のモデリングの役割を担う。FBI フィールドオフィスは、管轄内の Key asset のリスト作成、NIPC 本部はリストのまとめ、データベースのメンテナンスを担当。

③CIAO

商務省輸出行政局内に設置されている機関で NSC（国家安全保障会議）と共同で主要インフラ保護への意識を高める啓蒙活動を行っている。また、各連邦政府機関 CIO と共に、政府機関すべてが適切なセキュリティポリシーの導入、実行を行えるよう支援、監督を行っている。

具体的には、民間企業と共同で、リスク・アセスメント及び保険に関するガイドラインの作成や保険会社、監査機関、法律専門家、企業幹部と共同でセキュリティ・サミットを開催し、企業に対するサイバーセキュリティのガイドライン作成の支援などがある。

例：IIA（内部監査人協会：Institute of Internal Auditors）[1]は、CIAOと協力関係を結び、リスク管理に関するガイドを用意し、情報セキュリティにおける監査者の役割について対話を開始。

また、「国家情報システム保護計画」を作成し、情報セキュリティに関する教育や人材育成に努めようとしている。

**●国家情報システム保護計画**

下記に示すように「人材教育・資源」と「研究開発」の2つに大別される。

**「人的教育・資源」**

1.「連邦サイバーサービス」

- 2001年度：2,500ドルの予算
- 情報セキュリティに関する教育、トレーニングを行う。
- 人事管理庁（OPM）が中心に「情報技術卓越センター」、「サービス奨学金」、「高等・中等教育機関アウトリーチプログラム」、「連邦職員情報セキュリティ啓蒙プログラム」の4つを主に行う。

□ 「情報技術卓越センター（CITE）」プログラム
セキュリティに関する最先端の教育やトレーニングを連邦職員に行う。

□ 「サービス奨学金（SFS）」プログラム
情報セキュリティを専攻する大学3，4年生と大学院生に対して奨学金を与えるプログラム。

□ 「高等・中等教育機関アウトリーチプログラム」
中高生に対して、大学において情報セキュリティを専攻したくなるような、将来の連邦政府IT職員を目指したくなるような教育を行う。またコンピュータセキュリティについての個人の責任と倫理について教育を行うことを目指す。

---

[1] IIAは、70,000名の会員を有し、国際的な専門家によって構成される協会で、内部監査人やその組織に対して調査や教育、資格、標準化、その他の活動を提供するサービスを行っている。