各連邦政府機関の活動

大統領府

国際脅威対策局

(Office of Transnational Threats)

- 大統領府内、国家安全保障会議（National Security Council・NSC）の下部組織。
- 政府機関および民間セクターに対し、情報セキュリティ対策の重要性を訴える啓蒙活動。
- スピーチ等を各地で行う。

国家安全インフラ協議会

(NIAC : National Infrastructure Assurance Council)

- 1999年大統領令に基づき設立された機関。
- 民間セクターとの協力が必要とされるものについて、外部の高名な専門家を招聘し、ガイダンスを得る。
-

主要インフラ保証局

(CIAO :Critical Infrastructure Assurance Office)

- 商務省輸出行政局内に設置されている機関。
- NSCで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う。
- 民間企業と共同で、リスク・アセスメントおよび保険に関するガイドラインの作成。
- 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支援。
- 「国家情報システム保護計画」(National Information Systems Protection Plan)。

米国インフラ保護センター

(NIPC:National Infrastructure Protect Center)

- ウイルス攻撃や、セキュリティ攻撃ツールの登場等のセキュリティに関わる事件の早期発見、警告を主な使命（Daily Reportの作成）。
- FBIの関連機関としてセキュリティ事件の初期捜査を行う。
- 1999年3200万ドル、2000年2800万ドル。

指摘されているNIPCの問題点

- 他のセキュリティ機関と情報を共有しない。
- 政府と民間セクターとの間の技術上および認識度の大きなギャップ。
  例：オラクルの報告とNIPCの報告のズレ@Stanford Univ.

民間が提示した政府の問題点（民間と政府にギャップがある理由）

- 民間はセキュリティ情報を社外秘として扱いたい。しかし、政府取締り機関に連絡してしまうと公開捜査となり、機密情報が明らかになってしまう。
- 当局が容疑者を突き止めても、司法省にセキュリティに精通した弁護士の数が不足しており、解決に至らない。

NIPCの2つの改善策

- ISAC

  民間との情報共有のために、「情報共有と分析センター(ISAC:Information Sharing and Analysis Centers)」の設立を推進。

  ISACを通じて、政府と民間セクターとの連絡を緊密にする。

  ・ISACは、金融業、製造業など、各産業セクターが自発的に設立。各センターには、民間企業の代表者が常駐する。

  ・NIPCは、ISACにセキュリティ脅威に関する警告を発する。

  ・ISACでは、メンバーのみがアクセスできるセキュリティ情報データベースの公開、匿名で報告書を作成する機能などが提供されている。→企業は自らのセキュリティに関する機密を保ちつつ、活動に参加できる。

- InfraGardプログラム

  ・以下の4つの基本サービスを提供。

  ・暗号化された電子メールによる不正進入警告を行うネットワークの構築。

  ・不審活動や不正侵入に関する情報交換を行うための安全なウェブサイトの提供。

  ・地域グループ活動の推進（56のFBIフィールドオフィス）。

  ・ヘルプデスクの構築。

  InfraGardの優れている点：民間企業との連携がされやすい

  ・企業の機密性を保持

  民間企業がサイバー攻撃され、FBIのフィールドオフィスに報告を行う際、詳細な情報を記入できるフォーマットを利用し、匿名で安全に送信

することができる。

→FBIフィールドオフィス：提出された情報を元に操作を開始。

NIPC：報告された攻撃が「全国的なものか、地域的なものか」見極める。暗号化され情報源を匿名化した「警告メールを他の組織に送信する。

・ヘルプデスクとして役立つ

InfraGardに参加する企業コミュニティーに対して、安全対策の施されたウェブサイトを公開。分析ツールや警告ツールなどセキュリティ関連製品がダウンロードできる。

メンバー企業には、518の民間企業。IBMなどの大手企業も含まれている。

ブッシュ政権におけるNIPCの将来性

- 連邦CIO（Federal Chief Information Officer）を設置。（予定）

  連邦政府によるIT調達、投資の改善を図る。

  管理予算局（Office of Management and Budget）副局長が兼任。
- NIPCの役割変化の可能性

  ・NIPCが持つ犯罪捜査情報に、他のセキュリティ機関が容易にアクセスできるよう法改正を行う。

  ・NIPCを連邦CIOの下部機関とするか、国家情報セキュリティ問題を統合して処理する全く別の新しい組織を設立。

コンピュータ犯罪と知的所有権セクション

(Computer Crime and Intelectual Proctect Section)

- 司法省下の機関。
- サイバー犯罪の他、コンピュータが使用された犯罪の取締り、犯人検挙。

  ex.電子メールモニターシステム「Carnivore(カーニボー)」

全米規格技術院

(NIST: National Institute of Standards and Technology)

- 情報セキュリティ技術開発の連邦政府機関。
- 定期的にコンテストを開催し、新技術を公募 ex.DES に代わる新暗号技術の公募。
- 連邦政府機関における情報セキュリティレベルの測定方法を開発するプロジェクト（「コンピュータ・システム・セキュリティとプライバシー問題に関

する諮問委員会(Computer Systems Security and Privacy Advisory Board)」から資金提供を受けている）。

国家安全保障局

(NSA: National Security Agency)

「Secure Linux」プロジェクト（強固なセキュリティ機能を備えたリナックスを開発する）のスポンサー。

高度防衛調査局

(Defense Advanced Reserch Projects Agency)

NSA の協力を得ながら、独自でオープンソース OS 開発プロジェクト(Trusted Open Source Operating System)を進めている。

カーネギーメロン大学内 CERT/CC

(Computer Emergency Response Team Coordinating Center)

- 1988 年国防総省によって創設。
- 連邦政府機関に対してセキュリティ支援サービスを提供。
- 「灯台(Lighthouse)プロジェクト」（米国空軍から資金提供）。

  目標：システムアドミニストレータおよびネットワークアドミニストレータが、サイバー攻撃に対処するためにデータの定義、統合、抽出を行う際の、統一された専門用語コードを開発。

  専門用語コード：

  ・事件を検知、分析、対応 IDAR(Incident Detection, Analysis and Response)するためのガイドラインの基本フォーム。

  ・これらのコードを利用して、攻撃状況や対応状況などが記録される。
  IDAR データベースを構築。コードを利用して作成された攻撃、対応状況に関するデータが蓄積→より分析がしやすくなる。