情報セキュリティに関わる諸機関

下記の機関の詳細なデータ、取り組み等は、「米国政府関連のコンピュータウイルス対策等組織調査報告書」情報処理振興事業協会 2001 年 3 月参照。

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。
- サイバーセキュリティ問題の対外窓口責任者であり、PDD63 と国家プランの実施全体を監督。

国家インフラ保障審議会

(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。
- 審議会は、インフラ保護の分野での官民の協力を促進するために、定期的に開かれる。また、必要に応じて、大統領に報告書を提出する。
- National Coordinatorは、審議会のエグゼクティブディレクターとして、参加。

最高情報責任者会議

Chief Information Officers Council: CIO Council

- 連邦各機関の CIO をメンバーとする。
- 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。

重要インフラ調整グループ

(CICG:Critical Infrastructure Coordination Group)

- 省庁横断の委員会。
- 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。
- 各重要インフラ部門担当省庁の連絡調整官と共に、CICG は、インフラとの連絡調整にあたる。
- CICG の下にはサイバー事件監理グループ(CISG:Cyber Incident Steering

Group)とサイバー事件作業グループ(CIWG:Cyber Incident Working Group)が置かれる。

- National Coordinatorが主宰するCISGはCIWGに政策指針を示し、国家安全保障会議（NSC）に勧告を行う。
- CIWGは、サイバー攻撃等の事態が起きたときに関連連邦諸機関での対策の実施や取締りの調整を行う。

国家科学技術委員会

NSTC：National Science and Technology Council

- OSTP大統領府下科学技術政策局の下部組織。
- 連邦政府として科学技術への投資についての明確な目標を立てるために、閣僚レベルで科学、宇宙、技術政策を連邦政府として横断的にコーディネートする。

技術委員会

CT ： Committee on Technology

IT研究開発における省際ワーキンググループ

IWG on IT R&D:The Interagency Working Group on IT R&D

大統領情報技術諮問委員会

PITAC：President's Information Technology Advisory Committee

IT研究開発における国家調整委員会

NCO for IT R&D：National Coordination Office for IT R&D

司法省

DOJ: Department of Justice

連邦捜査局

FBI：Federal Bureau of Investigation

- 56 の FBI 地域オフィスを設置し、捜査にあたる。（InfraGard）
- 地域オフィス管轄内の Key Asset を決定し、リストを作成。（KAI）

全米インフラ保護センター

NIPC:National Infrastructure Protection Center

- 主な使命：

  「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。

- NIPC に参加している機関

  国防省、諜報機関、陸海空軍、Air Force Office of Specialinvestigations, 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 などの多数の機関から代表を募った interagency なものである。

  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。

- 民間セクターから Center へ人材登用も進めている。
- Emergency Law Enforcement Sector(ELES)と共に法の整備を進めている。州、地方の当局に NIPC のサイバーテロ警告が届くようになっている。
- NIPC が発令する警報には 3 段階ある。
  - ・assessments：緊急で対策を講じる必要のないような一般的な情報や分析を提供。
  - ・advisories：即座の対応が必要な脅威や攻撃に関する情報を提供。
  - ・alerts：国家レベルのネットワーク及びクリティカル・インフラを目標と

した脅威や攻撃に関する情報を提供。

- FedCIRC と NIPC の関係

  ある機関が事件報告をしてきたら、FedCIRC はその機関と共に、事件のタイプを判定し、機関のシステムの復旧ガイドラインを示す。

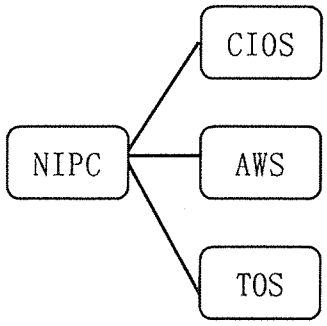
  NIPC は alerts、advisories, assessments のドラフトを作成し、各機関へのリリース前に FedCIRC に意見を聞く。

- NIPC は CERT は相互の利益のための契約関係にある。
  - NIPC は CERT の分析情報を手に入れ、警告発令機能を強める。
  - NIPC は、定期的に CERT/CC、アンチウイルスコミュニティと電話連絡をし、脆弱性、スレットの情報を交換する。
  - NIPC が警報内容を作成中のときには、CERT/CC の情報が求めれらる。
  - NIPC は調査結果等を CERT に提供、CERT を用いて産業界のセキュリティ専門家、公的機関に配信することもある。
  - NIPC Daily Report は e-mail で CERT/CC に流される。
  - NIPC は CERT/CC にスレットに関する新しい情報を流し、CERT/CC と協力して情報提供することも多い。

- NIPC はすべてのコンピュータ侵入の際の捜査において、マネージャの役割。

  コンピュータ犯罪関連の情報は、FBI 地域オフィス、米国の Intelligence Community、Department of Justice Criminal Division's Computer Crime and Intellectual Property Section, Office of Intelligence Policy and Review, U.S. Attorney's Offices その他の政府機関、民間セクター、メディア、その他のオープンソース、諸外国の法執行機関との接触によって得ることができる。NIPC はこれらの情報を調整、収集、分析しそれを多くに配信することに役割がある。

- NIPC は３つのセクションで構成される。



コンピュータ捜査・運営セクション(Computer Investigations and Operations Section)

コンピュータ捜査・運営セクションは、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。

分析・警告発信セクション (Analysis and Warning Section)

分析・警告発信セクションは、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。

トレーニング・啓発・戦略セクション (Training, Outreach, and Strategy Section)

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

1. InfraGard：
   - 「FBI地域オフィス（全米で56箇所）管轄内の地方InfraGard支部を通して、政府と民間セクターのメンバーの情報交換を促進させる」プログラムであり、InfraGard 支部の仕事は、サイバーテロ情報（“sanitized”（簡略版） and “detailed”（詳細版） format）をセキュアなネットワークで、NIPC及びFBIの地域オフィスに提供することである。
   - 全米1800機関とセキュリティ情報を共有。
     例：米国連邦準備銀行、オハイオ州立大学、IBM, Condor Systems, National Ciy Bank, Secure Interore, Anacatel Americas等
   - InfraGard支部のメンバーは、FBI、民間企業、その他の連邦、州、地方の政府機関、法執行機関、大学等が参加。
   - 対応の流れ：

InfraGard が情報入手

→該当する FBI 地域オフィスが detailed version を用いて調査開始。NIPC が当局、諜報機関、産業界の情報とあわせて分析し、侵入が多数のサイトへアタックしているうちの 1 つかどうか、決定する。

→NIPC 本部が sanitized version、使われているテクニックをその他のメンバーに機関に連絡。InfraGard のメンバーには、無償で情報提供をしている。メンバーになる際に、秘密保持契約が必要。

2. 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。
   - 非常時に備えた Key asset との 24 時間の連絡体制。
   - 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する役割を担う。
   - 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、リストをまとめ、national database をメンテ。

3. 物理的、サイバー上のアタックに対する "Indication and Warning program"
   - North American Electrical Reliability Council(NERC)と共に進行中の pilot program
   - プログラムの流れ:

     electric utility company and other power entitirs が NIPC に報告。

     →NIPC がその報告を分析し、Alert, Adivisory, Assessment のどれを電気関連コミュニティに発令したらよいかを決定し、その後発令。

     →民間との情報共有にも役立つ。

     その他のインフラセクターとの pilot program も検討中。

     現在、通信セクターとの Indication and Warning program を検討中。

コンピュータ犯罪と知的所有権セクション

Computer Crime and Intellectual Protect Section

- サイバー犯罪の他、コンピュータが使用された犯罪の取り締まり、犯人検挙。
- 電子メールモニターシステム「カーニボー」:
  - 一般の ISP ネットワークに取り付けることができ、一般ユーザの電子メールをモニターすることにより、サイバー犯罪の容疑者を探し出すようプログラミングされている。
  - 一般コンピュータユーザに対するプライバシーの侵害との批判。