エネルギー省

DOE: Department of Energy

コンピューター事故調査顧問団

CIAC : Computer Incident Advisory Capability

- ローレンスリバモア国立研究所内に設置されており、その中のCSTC(Computer Security Technology Center)の一部となっている。
- ローレスンスリバモア研究所から支援を受けている。
- エネルギー省管轄のサイトに対する緊急事態の技術支援、情報提供。
  - ・エネルギー省の各種サイト運営母体は、重要と思われるサイバーセキュリティ事件のすべてをCIACに報告。
  - ・CIACは、エネルギー省の事件報告中央機関として、事件の報告を受け取ると、侵入元の追跡、事件内容の分析などを行う。
  - ・エネルギー省の各機関は、毎日24時間のインシデント・リポートやコンピュータ不正使用報告の提出、モニタリングを義務付けられており、CIACは各機関から寄せられる情報を分析する。
  - ・CIACは、必要に応じて、NIPC、エネルギー省諜報活動局（DOE Office of Counterintelligence）、FedCIRCにセキュリティ事件の情報を提供する。
  - ・CIACのWebは、同種の政府機関としては、まず最初に閲覧すべきサイトと業界ではみなされている。
  - ・情報掲示板は、電子メールで送信され、最新スレットおよびその対処法などの情報が提供される。

- IT-ISACとの連携
  - ・CIACは、CERT、IT-ISACとチームを組んで民間と情報を共有。
  - ・CIAC ウェブサイトのウイルス情報は、業界で最大の情報量といわれている。

- エネルギー省関連機関に対する啓蒙・トレーニング提供。

商務省

Department of Commerce

重要インフラ保証局

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（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う。
- 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、監督を行う。
- 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を作成。
- 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を支援。
  例：IIA（内部監査人協会：Institute of Internal Auditors）[4]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。
- 「国家情報システム保護計画」(National Information Systems Protection Plan)の第 2 版を 2001 年後半に発表する予定。
- 連邦サイバーセキュリティ部隊(Federal Cyber Corps)奨学金プログラムなどを通じて、CIO Council と共同で情報セキュリティ人材の育成に努めている。

全米規格技術院

NIST: National Infrastructure 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、セキュリティの新技術を公募。
  ex. DES 暗号方式に変わる新暗号議術の公募
- 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が進行中。

---

[4] 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。

- 「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。
- NIST 内には、Computer Security Resource Clearinghouse(CSRC-後述の Computer Security Resource Center の略称と同じ)が設置されている。
  CSRC は、
  ・NIST が提供するコンピュータセキュリティ情報のディレクトリで、官民学によるセキュリティ情報リソースが一箇所にまとめてリンクされている。
  ・対象は、一般ユーザー、システムアドミニストレーター、セキュリティ専門家など。

NIST 内コンピュータセキュリティ担当部

CSD: Computer Security Division

- CSD は、NIST の ITL (Information Technology Laboratory) の中にある 8 つの部局のうちの 1 つであり、情報システムのセキュリティー改善を目的としている。
- 主な活動内容は 2 つ
  ・IT リスク、脆弱性、侵入防止策などに関する政府機関及び一般消費者の知識を広める。
  ・消費者の啓蒙と連邦政府システムの標準設定のために必要な基準を設定する。
- CSD 内には CSRC(Computer Security Resource Center)が設置されており、CSD は、CSRC のウェブサイトの管理も行う。CSRC がウェブで提供する情報には以下のようなものがある。
  ・ICAT 脆弱性データベース
  コンピュータ脆弱性に関する情報を検索できるデータベース、パッチなどの情報へのリンクをユーザーに提供。
  ・ウイルス情報
  ウイルス対策ソフトウェアのベンダーや団体へのリンクを提供する。
  ・事件処理情報
  ・コンピュータセキュリティパッチ
  ベンダーによって提供されているソフトウェア・パッチに関する情報を掲載したサイトへのリンクを提供。
  ・FedCIRC
  文官政府機関と連邦政府機関に影響を及ぼすと考えられるコンピュータセキュリティ問題を取り扱う FedCIRC へのリンクを提供する。

国防総省

Department of Defense

Defense Computer Forensics Lab

- 軍部が巻き込まれるようなスパイ行為、殺人、その他の犯罪が発生した場合、電子的な証拠を解明する。[5]

JTF-CND

Joint Task Forces-Computer Network Defense

- ペンタゴンのコンピュータ、LAN、長距離ネットワークの防御を組織化すること。
- このシステムは、24時間、軍部のコンピュータ・ノードを監視している。[6]

サイバー戦センター

- アタックに対する戦術的な警告を提供すると共に、アタックの評価を行う。
- 連邦緊急事態管理局の支持のもとに、インフラの機能に対しての緊急対応演習を行うことができる。[7]

高度防衛調査局

(DARPA: Defense Advanced Research Projects Agency)

- 国防総省の中央研究開発機関であり、主に国防分野の研究および先端的開発を担当している。
- 現在、NSA(国家安全保障局)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 Opening System) を進めている。
- 重要インフラに対するサイバー攻撃演習「The Day After...」を 1996 年 3 月 23 日実施した。

---

[5] Bridis, Ted,"High-Tech Crime - Fighting Lab Unveiled", http://www.infowar.com/mil_c41/99/ mil_c41_092599a_j.shtml

[6] Brewin, Bob & Harreld, Heather, "U.S. sitting duck, DOD panel predicts," 11/11/96 Information Warfare

[7] Becker, Elizabeth, "Pentagon Sets up New Center for Waging Cyberwarfare", The New York Times News Service, 08/10/1999

連邦コンピュータ事故処理チーム

FedCIRC：Federal Computer Incident Response Capability

- 軍事を除く、連邦政府機関のコンピュータセキュリティ問題を解決するために、各政府機関のコーディネーションを行う中心的な組織。
- 連邦政府機関、インシデント・レスポンス・チーム（IRT）、ベンダー、学際機関、セキュリティ機関、警察などセクターを横断したパートナーシップで成り立っている。
- パートナーである顧問機関に対し、脆弱性や事件の報告、ウイルス対策サイトのリンクなどを提供。
- 顧問機関は、スレット、影響力、問題解決法などの分析を行う。
- 連邦政府機関のセキュリティ専門員が共同で活動を行い、情報を交換する場を提供する。
- 重要インフラへの脅威となりうる犯罪行為を取り締まるため、NIPC と共同活動を行っている。
- 政府のコンピュータシステムに対する不正侵入事例を配信しており、（情報そのものは CERT/CC から来る）、ベンダーやユーザーはそれらの情報をシステム保護に役立てることができる。

大学系の機関

コンピュータ事件緊急対応センター

CERT/CC：Computer Emergency Response Team Coordinating Center

- 1988年に国防総省によって創設。カーネギーメロン大に所属。半官半民。
- 国防総省、FBI、その他複数の連邦政府機関、民間セクターより資金を得ている。
- 連邦政府機関に対して、セキュリティの脆弱性の原因追求、改善策等のセキュリティ支援サービスを提供。
- 不正行為に対する対応を行う他のリスポンス・チーム設立の援助。複数のチームのコーディネート。
- 「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すること。

その他の大学系CERTは以下

NU-CERT（ノースウエスタン大のCERT）
PECERT（パーデュー大のCERT）
SUNSet（スタンフォード大のCERT）
BadgIRT（ウイスコンシン・マディソン大のCERT）

FIRST

Forum of Incident Response and Security Teams

- 世界中に多数存在するコンピュータセキュリティ対応チームCIRTを統合する国際相互協力機関。NGO。
- CERT間の意思伝達を促進し、相互支援体制を確立する。
- メンバーとして登録しているチームは、官民学すべてのセクターが参加。メンバー機関は約70機関。
- 主なFIRSTメンバー
  官民学セクターを限定せず、コンピュータセキュリティに関わるすべての機

関がメンバー参加できる。

民間

アップル・コンピュータ、AT&T、CERT/CC 、BCERT (Boeing CERT:ボーイング社のCERT) など。

米国連邦

NASIRC (NASAの情報関連の緊急対応センター) 、AFCERT (米国空軍CERT) 、CIAC (米国エネルギー省Computer Incident Advisory Capability) など。

国際機関

AUSCERT (Australian Computer emergency Response Team) 、BTCERTCC (BritishTelecommunications CERT Co-ordination Centre) 、CERT-IT (CERT Italiano) 、JPCERT/CC (JapanCERT Coordination Centre) 、DFN-CERT (ドイツ) 、RENATER (フランス) 、IRIS-CERT (スペイン) 、JANET-CERT (英国) 、MxCERT (メキシコ) など。

大学

BadgIRT (University of Wisconsin-Madison)
NU-CERT (ノースウエスタン大CERT)
PCERT (パーデュー大のCERT)
SUNSet (スタンフォード大のCERT)