

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

2001年3月

情報処理振興事業協会

目次

総論	1
米国のコンピュータ・ウイルス対策関連組織.....	4
NIPC	5
CERT/CC.....	12
FEDCIRC	18
CIAC.....	22
NASIRC.....	25
AFCERT	28
COMPUTER SECURITY DIVISION OF NIST.....	31
CSI.....	35
FIRST	39
NU-CERT	43
PCERT	46
SUNSET.....	49
その他コンピュータ・セキュリティー関連組織.....	52
CIAO	53
NCCS.....	54
IPCIS	55
NSA	56
NACIC.....	57
CCIPS	58
IATAC.....	59
CSSPAB.....	60

[米国ウイルス対策関連組織の相互関係図](#)

総論

政府セキュリティ関連組織におけるウイルス対策の位置付け

米国において、コンピュータ・セキュリティ対策に関連する公的機関は数多く存在する。しかし、その中でウイルス対策だけに活動を絞った政府組織、機関は存在しない。米国のコンピュータ関連組織は、通常、コンピュータ・セキュリティや情報セキュリティに関する対策全般、クリティカル・インフラ保護を目的にしており、それらの活動の一環としてウイルス対策に取り組んでいるケースが多い。本調査報告書ではセキュリティに関わる代表的な政府系組織を2つのグループに分け、それらのプロフィールおよび活動内容を分析した。グループ1は、直接ウイルス対策の活動を手がけている組織であり、グループ2は、間接的に関わっている組織である。具体的には、グループ1は、コンピュータ・セキュリティに関する啓蒙活動やトレーニング、ハッキング技術分析などの事前防止対策に加え、攻撃の検知、警告発信、事件後対応などの活動を行っており、グループ2は、セキュリティ関連政策の設定などを行っている。

省庁間でのセキュリティ政策の一元化への動き

米国の政府機関は、従来は各省庁が独自に情報システム開発を手がけ、セキュリティ対策を講じてきたという歴史があり、各省庁間の活動が調整されておらず、政府全体としてのセキュリティ政策やセキュリティ確保の手順が確立されてこなかった。しかし、1998年になって、このような状態に歯止めをかけるべく、米国連邦政府内で首尾一貫したセキュリティ方針の確立に向けた対応がとられた。1998年5月にクリントン大統領が発したPDD(Presidential Decision Directive) 63によってNIPC(National Infrastructure Protection Center)が設立されるとともにCIAO(Critical Infrastructure Assurance Office)が設立され、国としてのセキュリティ政策の一元化が図られることとなったのである。NIPCは、国家全体のセキュリティ(実際の施設およびサイバーネットワーク上の両方)を保護し、米国司法省およびFBIによる取締活動の支援を行う。CIAOは、セキュリティ・ポリシーの統一を図っている。しかし、政府間の調整は必ずしもうまくいっておらず、近年激化の一途をたどるウイルス攻撃などに対する各政府機関の対応のばらつきや、情報の独占などが各方面から継続して指摘されており、今後の進展に期待が寄せられている。

民間セクターにおける主導権

米国においては、セキュリティ対策分野において、民間セクターおよび大学が主導権を握

っているといえる。米国政府は、国家運営に支障がないよう、安全保障の観点からセキュリティー対策に関する国家レベルでのポリシーは確立しているものの、セキュリティー対策を実際に手がけているのは民間セクターである。例えば、近年のウイルス感染事件においても、最初にウイルス拡散の警報を発し、対応策を配信したのは、民間企業であったように、インフォーマルな形で、ウイルス対策やセキュリティー対策は民間主導で実施されている。政府機関は、民間から発信される情報を受け取った後、その後の対応や官民学の共同活動促進、取締機関強化などを行っている。

セキュリティー関連企業の役割

米国において、ウイルス対策において中心的な役割を果たしているのはウイルス対策（anti-virus）ソフト会社である。代表的なウイルス対策ソフト企業としては、マカフィー（McAfee）、シマンテック（Symantec）、ネットワークアソシエイツ（Network Associates）、ドクター・ソロモンズ（Dr. Solomon's）などが挙げられる。このような企業はセキュリティー・アプリケーション・サービス・プロバイダーと呼ばれ、一般消費者から大規模機関までを対象に、多岐にわたるウイルス保護・防止・処理関連製品を提供している。さらに、ウイルス最新情報や、時には修復ツールの無償提供などを行ったりしている。民間企業によるウイルス情報は、政府機関によるサイトに比べてもより詳細でユーザー・フレンドリーである場合が多く、ユーザーからのフィードバックも行いやすいようになっている。米国のコンピュータ・セキュリティー市場は年々大きく成長しており、今まではセキュリティー分野に関わってこなかったITベンダーも同市場の成長を見込んで、活発に参入している。例えば、マイクロソフト社は、2000年12月7日「SafeNet 2000」と呼ばれる同社初のセキュリティーサミットをワシントン州レッドモンドで開催したが、本大会にはIT業界全体が参加し、活況を呈した。米国のセキュリティー産業はダイナミックに発展を遂げており、今後のウイルス対策活動も、民間主導で展開されることが見込まれる。

官民の協力体制

近年、米国連邦政府においてコンピュータ・セキュリティー対策の重要性が高まっており、この分野において公的セクターと民間セクターとの協力関係を強化しようとする動きが目立っている。例えば、NIPCによる新しいプログラムであるInfraGardや、CIAC（Computer Incident Advisory Capability）とCERT/CC（Computer Emergency Response Team Coordination Center）によるIT-ISAC（Information Sharing and Analysis Center for Information Technology）などは、官民相互支援を今までよりも踏み込んだ形で実現するものと見られている。しかし、ウイルス対策を含むコンピュータ・セキュリティー分野での官民協力体制を構築するのは難しい側面も大きい。

従来から、民間企業は、企業の名声や、取引先との関係、株価や資金調達能力に大きくひびくことを恐れて、ウイルス感染や不正アクセスなどの被害に関する情報を提供することに極めて消極的であった。官民の情報共有の場を設ける InfraGard にしても、「セキュリティー・ホール（穴）をいちいち FBI に知らせる」ことに躊躇する参加企業も多い。ジョージタウン大学のセキュリティー・エキスパートであるドロシー・デニング（Dorothy Denning）氏は、「多くの場合、コンピュータ・セキュリティー問題は、民間レベルで解決されている」と述べている。しかし、技術力・財力を持つ大企業の場合、自社内で対策を講じることができるが、中小企業は政府に頼らざるを得ないという声もあり、今後の官民協力を寄せられる期待は大きい。

国際協調の進展

米国におけるコンピュータ・セキュリティー対策は、コンピュータ・ネットワークへの依存度が急速に高まった米国の国家安全保障に関わる問題として、これまで主に国内問題としての視点に重点を置いて検討が進められてきた。しかし、欧州や日本を含むアジア諸国におけるコンピュータ・ネットワークの発展と、特に金融分野等において見られる国際的なサイバーネットワーク間の相互依存関係の進展を背景にして、コンピュータ・セキュリティー対策を国際協調の下に進めることの重要性に対する認識が高まっている。今後、米国内のみならず、コンピュータ・ウイルス対策を始めとするコンピュータ・セキュリティー対策の国際的な調整・連携のための取り組みが加速されることとなろう。

米国のコンピュータ・ウイルス対策関連組織

1. NIPC (National Infrastructure Protection Center) [DOJ, FBI]
<http://www.nipc.gov/>
2. CERT (Computer Emergency Response Team) [DARPA, Carnegie Mellon Univ.]
<http://www.cert.org/>
3. FedCIRC (Federal Computer Incident Response Capability) [CIO Council]
<http://www.fedcirc.gov/>
4. CIAC (Computer Incident Advisory Capability) [DOE]
<http://ciac.llnl.gov/>
5. NASIRC (NASA Incident Response Center) [NASA]
<http://www-nasirc.nasa.gov/>
6. AFCERT (Air Force Computer Emergency Response Team) [DOD]
<http://afcert.csap.af.mil/>
7. Computer Security Division of NIST [NIST]
<http://www.itl.nist.gov/div893/>
8. CSI (Computer Security Institute) [Association]
<http://www.gocsi.com/>
9. FIRST (Forum of Incident Response and Security Teams) [Association]
<http://first.org/>
10. NU-CERT (Northwestern University - Computer Emergency Response Team)
<http://grumpy.nsg.northwestern.edu/nu-cert/nu-cert.html>
11. PCERT (Purdue Computer Emergency Response Team)
<http://www.cerias.purdue.edu/pcert/pcert.html>
12. SUNSeT (Stanford University Network Security Team)
<http://www.stanford.edu/group/itss-ccs/security/index.html>

(略称) 名称	NIPC National Infrastructure Protection Center
所在地	J. Edgar Hoover Building 935 Pennsylvania Avenue, NW Washington, D.C. 20535-0001 Voice: (202) 323-3205 Fax: (202) 323-2079 電子メール : nipc.watch@fbi.gov ウェブサイト : http://www.nipc.gov
設立年月	1998年2月
組織規模(人員)	125人(FBIから85人、その他の政府機関および民間セクターから40人)
組織の目的	1)クリティカル・インフラの保護 2)政府と民間の情報共有 3)事件発生後の捜査・取締
組織の位置付け	組織分類 : 政府・NGO・大学・その他() 上位組織 : 司法省、FBI 傘下組織 : なし その他関連組織 : FedCIRC
ウイルス対策活動内容	調査 : ウイルス被害状況の把握 研究 : 脆弱性分析 開発 : 警察に対するトレーニング・プログラム 実施範囲 : 政府及び民間 普及・啓発 : InfraGard、IAW プログラム、トレーニング、ニュースレターなど サポート : Incident Report 取締り : FBI などの取締当局への支援を行う その他 : 具体的な活動例(トピック) W32 などのウイルス警告
その他	NIPC は FBI 本部の中に設置されたセキュリティー犯罪防止・取締支援機関である。

概要

NIPC (National Infrastructure Protection Center) の使命は「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(”to detect warn of, respond to, and investigate unlawful acts involving computer intrusions and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures”)」ことである。

1998年5月、クリントン大統領は、テロなどによる攻撃から国家を保護するための新しい構想を打ち立てた。これによってサイバー・テロや生物兵器など、新しい形の脅威にどの様に対処すべきかがまとめられた。この一環としてNIPCは、クリントン大統領率いるクリティカル・インフラ保護委員会(Commission of Critical Infrastructure Protection)によって提唱され、司法省とFBIによって設立された。

NIPCは、ワシントンDCにあるFBI本部建物の中に設置されており、連邦、州、地方政府の担当官と民間セクターからの代表者が、共同で国家のクリティカル・インフラを保護するための中央機関(National Focal Point)としての機能を遂行している。NIPCは、物理的なインフラ攻撃に対する対策も行っており、ウイルス対策を含めたサイバー攻撃のみを活動目的としているわけではない。しかし、公益事業者による事業のコンピュータ化が急速に進む米国において、ハッキングといったコンピュータ・システムの直接攻撃により国家の機能が麻痺してしまうような事態にも陥りかねないことから、NIPCはサイバー攻撃に対応するための機能を確実に拡大しつつある。

米国では、国家クリティカル・インフラの90%以上が民間によって運営されており、事件発生時には民間セクターとの協調なしには政府は事故状況の把握さえ難しいと考えられている。そのため、NIPCは、政府と民間企業との情報共有体制を確立するために尽力している。すなわち、NIPCは情報収集の場を提供し、民間はハッキング事件などの脆弱要素などの情報を提供するという補完関係を構築している。

情報共有の場を提供すると同時にNIPCは、国家クリティカル・インフラに対する脅威度分析、警告発信、捜査、攻撃の対処法の伝授など、啓蒙活動と取締の支援を行っている。情報の収集(諜報機関などからの機密情報から民間オープンソースまで)を行いそれを分析して関連ユーザーに警告を発することをNIPCは第一の目標としている。第二の目標としては、不正侵入などの犯罪が起きた場合に、NIPCは連邦政府代表としてその対応と捜査を行う。

クリティカル・インフラとは、以下のような社会の基盤となるインフラを指す。

- 電気通信 (Telecommunications)
- 銀行、金融 (Banking and Finance)
- 水道 (Water Supply Systems)
- 交通 (Transportation)
- 政府機能 (Government Operations)
- 緊急事態対処 (Emergency Services)
- 電気 (Electrical Power)
- ガス、石油の貯蔵と配布 (Gas and Oil Storage and Delivery)

組織構成

上部組織は司法省と FBI である。FedCIRC (詳細は 13 ページを参照) とインフラ保護の共同活動を行っている。

NIPC は以下の 3 つのセクションで成り立っており、3 セクションとも何らかの形でウイルス対策を行っている。

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。

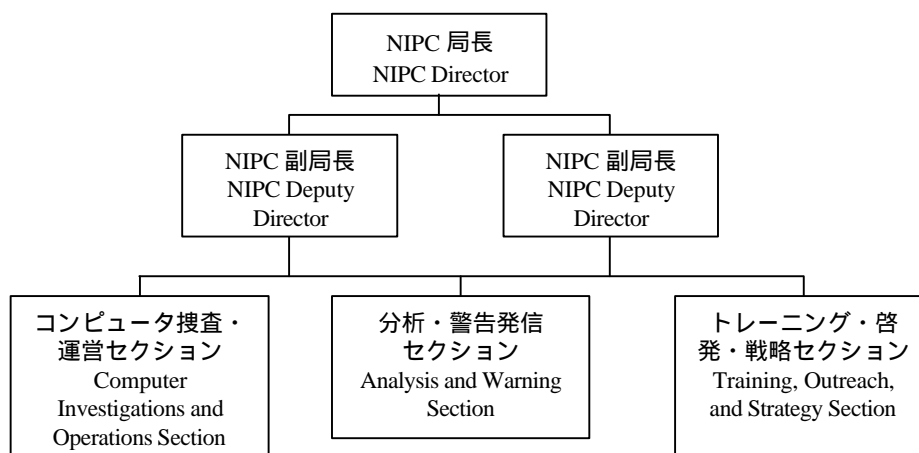
分析・警告発信セクション (Analysis and Warning Section)

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。

< 内部機構 >



出典：NIPC のウェブサイトを用いてワシントン・コアが作成

主な活動内容

官民学間の情報シェアを推進するために NIPC が行っている活動には以下のようなものが含まれる。

インフラガード・プログラム (InfraGard)

CITAC*の官民学相互協力の流れを受け、FBI は、2001 年 1 月に、ハッカー及び電子不正侵入に関する官民学間の情報共有を目的とした InfraGard を発足させた。InfraGard に参加するメンバー機関には、事件発生の際に関連情報を暗号化したものが送信され、FBI と NIPC には暗号化された事件内容が送信される。InfraGard への参加機関は、米国連邦準備銀行、オハイオ州立大学、IBM、Condor Ssystems、National City Bank、Secure Interiors、Alcatel Americas、などが挙げられる。

* CITAC (Computer Investigations and Infrastructure Threat Assessment Center) は、1996 年 7 月に FBI の傘下機関として、米国のクリティカル・インフラに対するサイバー・テロなど、国家セキュリティに関わるコンピュータ犯罪に関する捜査を行うために創設された。1998 年、CITAC は NIPC に吸収された。CITAC によって、FBI は、政府と民間セクターとの間におけるアライアンスの形成を図り、セキュリティ情報の自由な流れを促進すると共に、事件対応の協調体制の実現に向けて活動を展開した。

IAW プログラム

NIPC は、電力会社と共同で、電力会社に対するサイバーおよび物理的な脅威に関する情報をリアル・タイムで共有するための「指示・分析・警告プログラム (IAW:

Indications, Analysis, and Warning Program)」を実施している。現在、公益事業社は、事業の様々な側面で IT を導入している。多くの会社はオンラインのコール・センターでありとあらゆる業務をオンライン処理しており、従業員は一つのプラットフォームから顧客データを検索でき、顧客はインターネットを通して請求書の受取から料金支払、支払履歴の検索などを行っている。このような電子インフラは今日、社会が機能するための重要な位置を占めており、これら電子インフラに対するサイバー攻撃を回避するのが IAW プログラムの使命である。

メンバーとなった電気会社には、サイバーアタックに際して最も迅速な警告と実用的な指示が与えられる。メンバー会社がサイバー攻撃の被害に遭った場合、攻撃が発見されてから 60 分以内に NIPC に被害届を出す。

インフラ警告 (Infrastructure Warning)

NIPC は、FBI の国家脅威警告システム (National Threat Warning System) で開発されたインフラ警告を発信している。インフラ警告には、「評価 (Assessments)」「助言 (Advisories)」「警告 (Alerts)」の 3 段階があり、「評価」段階では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し、「助言」段階では即座の対応が必要な脅威や攻撃に関する情報を提供し、「警告」段階では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する。

2000 年に行われた「評価」段階における情報提供では、11 月と 12 月に発見された「W32 navidad@M Worm」と「W32/ProLin@MM” Internet Worm」というウイルスの情報がある。幸いどちらも米国において致命的な被害は出なかったが、感染したらどのような症状が出るのかといった説明、またウイルスの除去方法が記載されているサイトなどが紹介された。

トレーニング (Training and Continuing Education Unit)

トレーニングと継続教育課 (Training and Continuing Education Unit) は、警察など取締に関わる人材がネットワーク侵入捜査に必要な知識と技術を会得するためのコースを提供している。コースには「ネットワーク侵入の基本的な技術」「捜査ツールとしてのインターネット」「UNIX 侵入技術」などがある。

また NIPC は、「CyberNotes」という 2 週間に 1 度のニュースレターを発行しており、最新の

ソフトウェア脆弱性情報をニューズレターグループに配信している。

(略称) 名称	CERT/CC Computer Emergency Response Team Coordination Center
所在地	CERT® Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890 U.S.A. 電話 : +1 412-268-7090 Fax : +1 412-268-6989 電子メール: cert@cert.org ウェブサイト : www.cert.org
設立年月	1988年11月
組織規模(人員)	非公開
組織の目的	1)インシデント・リスポンス 2)他組織のコーディネート 3)脆弱性分析、情報配信、啓蒙活動
組織の位置付け	組織分類 : 政府・ NGO ・ 大学 ・その他() 上位組織 : カーネギーメロン大学 Software Engineering Institute、国防総省、FBI 傘下組織 : なし その他関連組織 : FedCIRC、FIRST
ウイルス対策活動内容	調査 : ネットワーク不正侵入被害状況 研究 : 脆弱性分析 開発 : ナレッジ・データベース、事件対応体制 実施範囲 : 国防総省、大学、民間 普及・啓発 : トレーニング、メーリングリスト サポート : 24時間ホットライン、電子メール、ウェブサイト 取締り : 警察と連携 その他 : 具体的な活動例(トピック) トロイの木馬、メリッサ、チェルノブイリ、Happy99、ExploreZip などのウイルス報告を受け、直ちに対処法を配信した。
その他	CERT は、DARPA によって創設され、カーネギーメロン大学内に設置されており、官民学の共同活動体制を敷いている。

概要

モリス虫 (Morris Worm) と呼ばれるウイルスがインターネットに接続されているコンピュータの約 10% を汚染するという事件が起こった直後の 1988 年 12 月に、DARPA (Defense Advanced Research Projects Agency) (国防総省の一部) によって CERT (Computer Emergency Response Team) は設立された。その後 CERT は、CERT コーディネーション・センター (CERT/CC) へと拡大し、カーネギーメロン大学ソフトウェア・エンジニアリング・インスティテュート (Software Engineering Institute) におけるネットワーク・システム強化プログラム (Networked Systems Survivability Program) の一部となっている。このプログラムは国防総省のために創設され、ネットワーク・システム上の攻撃を防止するための最新技術の開発、および攻撃の際に被害を最小限に抑え、主要サービスの継続を可能とすることを目的としている。

国防総省の高等研究計画局 (ARPA: Advanced Research Projects Agency) がスポンサーとなって開発された全国規模のコンピュータ・ネットワークで現在のインターネットの母体である ARPANET が、1980 年代の後半、実用段階に入った。1988 年 11 月、「インターネット虫 (Internet worm)」と呼ばれるウイルスによって ARPANET が汚染され、完全に破壊されてしまった。この事件に対する対処は、機関ごとにばらばらで統一性に欠け、異なる機関が全く同じ研究を同時に行うなど無駄が多かった。この事件をきっかけとして「コンピュータ・セキュリティーに関する中央機関が必要だ」という声が各方面から上がり、その結果、CERT コーディネーション・センターが設立された。

創設以来、CERT/CC は他の多くのインシデント・リスポンス・チームの開設を支援し、世界で 85 以上のインシデント・リスポンス・チームが CERT/CC の緊急事態対応活動を踏襲している。当初の使命はコンピュータ不正行為に対する対処であったが、現在では、不正行為に対する対応を行う他のチーム設立の援助、複数のチームのコーディネート、専門家に対するトレーニングの提供、セキュリティー脆弱性の原因追及、脆弱性改善策の提供、システム・セキュリティーの改善、大規模ネットワークの点検、などを行っている。サービス対象はコンピュータ・セキュリティーに関わる全セクターの組織および個人である。

2000 年 4 月にカーネギーメロン大学が CMISS (Carnegie Mellon Institute for Survivable Systems) を設立した。CERT は、CMISS のメンバーとして、ネットワーク・セキュリティーおよび強化の問題を解決すべく他のメンバー組織と共に活動を展開している。CMISS は、カーネギーメロン大学内の各学部及び研究所による共同研究により開発され、民間からの出資を受けており、カーネギーメロン学内の情報システム・セキュリティーの改善に努めることをその使命としている。

組織構成

CERT コーディネーションセンターは、DARPA によって創設され、現在、カーネギーメロン大学のソフトウェア・エンジニアリング・インスティテュート (Software Engineering Institute) におけるネットワーク・システム強化プログラム (Networked Systems Survivability Program) の一部である。CERT/CC は、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。

CERT は FIRST (詳細は 34 ページを参照) に属しており、スレット (脅威) 情報源としての役割を果たしている。

主な活動内容

CERT コーディネーション・センターの主な活動は以下のようなものが挙げられる。

- ネットワーク強化管理 (Survivable Network Management)
- ネットワーク強化技術 (Survivable Network Technology)
- 不正侵入に対する対処 (Incident Response)
- 不正侵入および脆弱性の分析 (Incident and Vulnerability Analysis)
- ナレッジベース開発 (Knowledgebase Development)
- 教育とトレーニング (Education and Training)
- 啓蒙活動 (Information Dissemination)
- 出版 (Publications)

ネットワーク強化管理 (Survivable Network Management)

ネットワーク・コンピューティング・システムのセキュリティを改善するためのメソッドを提供する。同メソッドは「自発型セキュリティ評価法 (self-directed security evaluation method)」と呼ばれ、ネットワーク・システムにおける危険度を定期的に測定する。

ネットワーク強化技術 (Survivable Network Technology)

セキュリティの不備を発見し、ネットワーク・システムが侵入を受けた場合の技術的な対処法を提供する。

不正侵入に対する対処 (Incident Response)

システム・アドミニストレーターからセキュリティ上の問題が報告された場合、支援を提供する。また、要望に応じて警察との連携も行う。1999 年の 1 月から 12 月の間に 32,967 通の電子メール、2,099 本のホットライン電話によってコンピュータ不正使用の報告及び情報請求が

行われ、419 件の脆弱性発覚の報告が行われ、8,268 件のセキュリティー関連の事件対応を行った。また、年々増加の一途をたどるコンピュータ不正操作に対する対処は、チームで行う必要があるため、他のインシデント・リスポンス・チームとのコーディネートも行っている。

不正侵入および脆弱性の分析 (Incident and Vulnerability Analysis)

CERT/CC の各メンバー組織から提出される脆弱性レポートを「脆弱性分析エキスパート」が分析し、それに対する対応をトラックする。また、脆弱性を引き起こす原因となっているソフトウェアのエンジニアリングおよびシステム・アドミニストレーターの作業形態を追跡する。分析において得られた情報は、消費者や事業者、インストラクターなどに分配される。

ナレッジベース開発 (Knowledgebase Development)

ネットワーク強化 (network survivability) やセキュリティーに関連した情報をより効率的に利用するためのナレッジベースを他機関と共同で開発している。

教育とトレーニング (Education and Training)

各メンバー組織の Computer Security Incident Response Team のテクニカル・スタッフやマネージャー、およびシステム・アドミニストレーターなどネットワーク・セキュリティーに携わる一般の技術者に向けてトレーニング・コースを提供している。また、CERT/CC のスタッフ・メンバーで、カーネギーメロン大学で情報セキュリティー管理を教えている者もいる。

啓蒙活動 (Information Dissemination)

ホットライン、電子メール、メールグループ (majordomo@cert.org)、USENET ニュースグループ、ホームページなどを通じて情報の交換を頻繁に行っている。現在までに 340 件のセキュリティー・アラートを発している。

出版 (Publications)

CERT サマリー : CERT に報告されるサイバー・アタックに関する情報やそれに対する対処法などで、年に 4 回から 6 回、出版される。サマリーは、メーリングリスト、USENET ニュースグループ、ホームページに掲載される。

インシデント・ノート、脆弱性ノート : インシデント・ノートは、CERT インシデント・リスポンス・チームに報告された最新のイントルーダー (侵入者) の動向を紹介する。脆弱性ノートは、インターネット関連のシステムにおける脆弱性を説明する。

セキュリティ改善基準: CERT のウェブサイト <http://www.cert.org/security-improvement/> において、ネットワーク・システムのセキュリティを改善するための実際のガイドであるセキュリティ改善基準 (Security Improvement Module) が提供されている。

(略称) 名称	FedCIRC Federal Computer Incident Response Capability
所在地	FedCIRC 7th and "D" Streets S.W. Washington, DC 20407 電話：888.282.0870 電子メール： fedcirc@fedcirc.gov
設立年月	1996年10月
組織規模(人員)	非公開
組織の目的	1)連邦政府に対するコンピュータ・セキュリティ取締支援 2)政府機関への情報提供 3)官民学の橋渡し
組織の位置付け	組織分類：政府・NGO・大学・その他() 上位組織：CIO Council 傘下組織：なし その他関連組織：NIST、CERT/CC、CIAC、NIPC
ウイルス対策活動内容	調査：サイバー攻撃被害状況 研究：脆弱性分析 開発：トレーニング・プログラム 実施範囲：文官政府機関 普及・啓発：特になし サポート：24時間ホットライン、料金制オンライン・ヘルプ 取締り：国防総省、警察に取締の支援を提供する その他： 具体的な活動例(トピック) ホットライン・サービスなど
その他	FedCIRC は、軍事を除くその他の連邦省庁に対しセキュリティー・サービスを提供する。

概要

FedCIRC (Federal Computer Incident Response Capability) は、コンピュータ・セキュリティーの専門家と警察との協力関係を強化し、連邦政府に対してコンピュータ・セキュリティー取締支援サービスを提供することを目的として設立された。FedCIRC は、文官政府機関及び連邦政府機関に影響を及ぼし得るコンピュータ・セキュリティー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。FedCIRC の事件対応 (incident response) と顧問活動 (advisory activities) は、国防総省および警察、諜報機関、学際機関、連邦政府機関のコンピュータ・セキュリティー専門員など、官民学を横断した優秀な人員を集結することにより、強力なセキュリティー・チームの結成を可能にしている。

1996 年、GITS (Government Information Technology Services) が NIST (National Institute of Standards and Technology) に対し 279 万 6 千ドルの予算を提供して FedCIRC が設立された。FedCIRC は、現在、連邦 CIO 評議会¹ (Federal Government's Chief Information Officers Council) によって資金提供を受けている。FedCIRC は、“バーチャル・リスpons・チーム”として、専用のリスpons・チームを機関内に持たない文官政府機関に対し支援サービスを提供する。

政府の情報リソースに対する攻撃からの防御および攻撃からの回復を効果的に行うため、FedCIRC は、連邦政府機関のセキュリティー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。また、クリティカル・インフラへの脅威となり得る犯罪行為を取締るため、NIPC (National Infrastructure Protection Center) と共同活動を行っている。

FedCIRC は、連邦政府機関、コンピュータ・インシデント・リスpons・チーム、ベンダー、学際機関、セキュリティー機関、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。FedCIRC は、パートナーである顧問 (Advisories) 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、などを提供し、顧問は、スレット、ウイルスの影響力、問題解決法、などの分析を行う。FedCIRC はまた、政府のコンピュータ・システムに対する不正侵入の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。

組織構成

FedCIRC は GITS の資金を受けた NIST によって 1996 年に創設され、現在、連邦 CIO 評議会が上部組織となって資金提供を行っている。

¹ CIO Council は、連邦政府機関の情報リソース管理を改善するために、大統領令によって 1996 年に設立された。

主な活動内容

FedCIRC のサービスは、大きく分けると「基本サービス (Baseline Service)」と「料金制サービス (Fee Based Services)」の 2 つに分けられる。基本サービスでは、コンピュータ・セキュリティ脅威に対する対処法を継続的に提供するもので、料金制サービスでは、その場その場に合った対応が連邦政府機関に対して提供される。

基本サービス (Baseline Service)

- 事件対応 (Incidnet Response)
 - 事件報告 (Incident Reporting)
 - 24 時間ホットライン (1-888-282-0870)
 - 電子メール fedcirc@fedcirc.gov
 - Fax (1-412-268-6989)
 - 事件後対応 (Incident Handling)
 - 事件発生後の対策指示を講じる政府機関の中心となる。
 - 回復手段を講じる。
 - 文官機関と警察機関との橋渡しを行い適切な情報発信を行う。
 - 民間と政府のコーディネーションを行うことにより互いの能力を融合させ、機能を促進させる。
- 事件発生防止と問題認識 (Incidnet Prevention and Recognition)
 - セキュリティ掲示板、顧問、セキュリティ関連ツールへのリンク提供 (Security Bulletins, Advisories and Links to Security and Analysis Tools)
 - 事件分析
 - セキュリティ・ツールへのリンク
 - 脆弱性の改善
 - データ収集
 - データ・ウェアハウスとデータ配信
 - 能力開発 (Competency Development)
 - ウェブ・ベースの情報発信
 - トレーニング・コース開発
 - 最新情報提供
 - トレーニング教材の開発

料金制サービス (Fee Based Services)

- オンサイト事件拡大防止と回復 (On-site containment and recovery)
- オンサイト事件回復支援とコンサルティング (On-site computer incident recovery assistance and consultation)
- オンサイトログ分析 (On-site audit trail analysis)
- リスク分析 (Risk Analysis)
- ネットワーク・セキュリティー・プロファイリング (Network Security Profiling) など

(略称) 名称	CIAC Computer Incident Advisory Capability
所在地	Computer Security Technology Center (CSTC) University of California Lawrence Livermore National Laboratory (LLNL) 7000 East Avenue Livermore, CA 94550 電話 : +1 925 422-8193 Fax : +1 925 423-8002 電子メール : ciac@llnl.gov ウェブサイト : http://ciac.llnl.gov
設立年月	1989 年
組織規模 (人員)	非公開
組織の目的	1) エネルギー省に対する緊急事態の技術・情報提供 2) エネルギー省に対する啓蒙・トレーニング提供 3) 官民の情報シェア
組織の位置付け	組織分類 : 政府・NGO・大学・その他 () 上位組織 : エネルギー省 (DOE)、Computer Security Technology Center (CSTC)、Lawrence Livermore National Laboratory (LLNL) 傘下組織 : なし その他関連組織 : FIRST、CERT
ウイルス対策活動内容	調査 : 脅威傾向 研究 : 脆弱性分析、技術トレンド 開発 : オンサイト・ワークショップなど 実施範囲 : エネルギー省コミュニティーおよび民間企業 普及・啓発 : ニュースレター、ウェブサイト サポート : エネルギー省に対する緊急サポート 取締り : 当局への情報提供 その他 : 具体的な活動例 (トピック) http://HoaxBusters.ciac.org においてにせ物ウイルス情報の提供 など
その他	エネルギー省に対する緊急時対応 米国で最も古いコンピュータ・セキュリティー機関のひとつ

概要

1989年、増加の一途をたどるコンピュータ・セキュリティー関連犯罪に対応するため、エネルギー省がCIAC (Computer Incident Advisory Capability) を設立した。CIACは、ローレンス・リバモア国立研究所² (LLNL: Lawrence Livermore National Laboratory) 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。創設以来、米国で最初のリスポンス・チームの1つとして米国内外でその活躍が認識されている。

CIACは、エネルギー省管轄のサイトが何らかのセキュリティー問題に直面した際に、エネルギー省に対して直ちに技術支援と情報提供を行う。エネルギー省コミュニティー (エネルギー省役員、スタッフおよび請負業者) に対しては、緊急事態対応だけでなく、啓蒙、トレーニング、傾向・脅威・脆弱性データ収集と分析、技術トレンド・ウォッチ、などのサービスが提供される。

CIACは、米国の原子力発電所のモニターリングも含め、エネルギー省が運営する各サイトのうち、サイバーアタックの対象となる可能性のあるものに対し技術的サポートおよび情報提供を行っている。CIACは、セキュリティー情報およびツールに加え、情報掲示板やウイルス・データベース、インターネット捏造情報ページ、グループ・ニュースレター、OSページ、他のコンピュータ・リサーチ・センターへのリンクなど、広範囲にわたるセキュリティー情報の提供を行っており、同種の政府機関としては、まず最初に閲覧すべきサイト³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、最新スレッドおよびその対処法などの情報が提供される。

最新動向としては、2001年1月に、マイクロソフトやオラクル、IBMなどトップレベルの企業19社が、連邦機関であるCIAC及びCERTとチームを組んで情報シェアに取り組むとした発表を行った。民間の企業は競合する企業同士ということもあり、製品脆弱性やハッカー攻撃傾向などの情報はこれまで機密情報として取り扱われていた。しかしそのような情報を共有し、共同対策を打ち立てることにより消費者からの信頼を取り戻し、インターネットを介した事業収入を確保することを狙いとしている。

この情報共有プログラムは、IT-ISAC (Information Sharing and Analysis Center for Information

² ローレンス・リバモア国立研究所は、エネルギー省の傘下機関であり、カリフォルニア大学によって管理されている。

³ Information Today, July 1, 1999

Technology) と呼ばれる非営利機関として機能する。これら企業機密に関わる情報の共有は企業同士の信頼関係の上に成り立っており、また同時に政府機関からは最新のスレット情報が提供される、という相互支援が同プログラムの前提となっている。IT-ISAC 発足当時のノーマン・ミネタ商務長官は「共同戦線を張ることにより、サイバーアタッカーに対して威嚇を行っていく」と語っている。

組織構成

CIAC は、CSTC (Computer Security Technology Center) の一部分であり、ローレンス・リバモア国立研究所 (Lawrence Livermore National Laboratory) によって支援を受けている。CIAC は FIRST (詳細は 34 ページを参照) の創設メンバーの 1 つであり、全世界のコンピュータ・セキュリティ・チームの相互協力体制の構築に努めている。

主な活動内容

- 事件処理コンサルティング (Incident Handling Consulting)
- コンピュータ・セキュリティ情報提供 (Computer Security Information)
- オンサイト・ワークショップ (On-site Workshop)
- 政府監査 (White-hat Audit)

エネルギー省の各種サイト運営母体は、重要度が高いと思われるサイバー・セキュリティ事件の全てを CIAC に報告する。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、傾向・パターンの判断、などを直ちに行う。エネルギー省の各機関は、毎日 24 時間のインシデント・レポートやコンピュータ不正使用報告提出や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。

特にウイルスに関しては、CIAC は定期的にウェブサイト掲示板に特定のウイルスに関する最新情報を掲載している。同種の情報提供量では、業界では最大と言われている。また、定期的に「The CIAC Computer Virus Informatin Update」を出版し、ウェブサイトに掲載している。同レポートでは、拡散度の高いウイルスの MS-DOS、ウィンドウズ、マッキントッシュのプラットフォームに対する影響を分析している。

その他にも、CIAC は<http://HoaxBusters.ciac.org>において hoax (にせ物) ウイルス情報の提供も行っている。

(略称) 名称	NASIRC NASA Automated Systems Incident Response Capability
所在地	Goddard Space Flight Center Code 630.2 Greenbelt, MD 20771 USA 電話：1-800-7NASIRC (+1-800-762-7472) 国際：+1-301-286-7777 Fax：+1-301-286-7483 ウェブサイト： http://www-nasirc.nasa.gov/
設立年月	1987年
組織規模(人員)	非公開
組織の目的	1)NASA に対する緊急事態対応 2)NASA 内のセキュリティー・コーディネーション 3)セキュリティー情報・ツールの配信
組織の位置付け	組織分類：政府・NGO・大学・その他() 上位組織：NASA 傘下組織：なし その他関連組織：FIRST、FedCIRC
ウイルス対策活動内容	調査：NASA のセキュリティー状況 研究：脅威・脆弱性分析、製品分析 開発：NASA 情報セキュリティー・ツール 実施範囲：NASA および国際リスpons・チーム 普及・啓発：ニュースレター、トレーニングコース サポート：NASA の緊急事態対応 取締り：当局へ情報提供 その他： 具体的な活動例(トピック) 不正侵入のトラッキングなど
その他	NASA の緊急事態対応

概要

1987年のコンピュータ・セキュリティー法（Computer Security Act of 1987）を基にNASIRC（NASA Automated Systems Incident Response Capability）が創設された。NASIRC創設の根拠法としてはこの他に、NASAを対象とした機密・非機密の政府情報に関連するその他の連邦法および規制などがある。

NASA内で検知された全てのコンピュータ事件がNASIRCに通報されるようになっており、ネットワーク攻撃など重要度の高い犯罪はNASAの監察長官に報告される。NASIRCは、攻撃警報の配信、攻撃パターンの分析、脆弱性情報及びパッチの配布、などを行う。また、攻撃例の収集を行うことにより、攻撃の性質及び頻度、対応パターンなどを分析する。

その他にもNASIRCは、ウェブサイト上でセキュリティー・ツールの無料提供を行うなど、NASAだけでなく、民間機関にもアクセスを提供している。

組織構成

NASA内のコンピュータ・セキュリティーを管理する目的でNASA内に設置されており、NASAが上部組織である。NASIRCとFedCIRCは、カーネギーメロン大学のコンピュータ緊急対応チーム（Computer Emergency Response Team）やその他の国際リスポンス・チームと共同の警告発信サービスや、ベンダーのモニター、ニュース・グループなど、様々な共同活動も行っている。

主な活動内容

NASIRCは、NASAに対し、セキュリティー管理・分析および技術サポート、コンピュータ及びネットワークのセキュリティー関連事件の防止対策、事件が起こった場合のソリューション、などを提供する。

セキュリティー関連事件は以下のように定義されている。

- (1) 機密情報の盗難、盗難の企て、
- (2) 政府情報の不正使用、改竄、無断破棄、
- (3) 基幹システムの妨害、
- (4) NASAシステムに影響を及ぼすと思われる脆弱性の指摘、

NASIRC の使命は以下のように定義されている。

- 1) 国内外のシステムから不正侵入するハッカーおよびウイルス、ベンダーによるハードウェア/ソフトウェア不正使用、産業スパイなど、コンピュータ犯罪や脅威に対応するため、事前分析を行い防止策を設定する。
- 2) NASA コミュニティーに配布される新しい情報セキュリティ・ツールの開発を行う。
- 3) NASA コンピュータ・システムの管理プロセスやガイドラインなどの質を向上させるための情報交換を行う。
- 4) 製品分析やニュースレター・パンフレットの配布、トレーニングコースの提供などを通して啓蒙活動に努める。

NASIRC が行うインシデント・リスポンスには以下のようなものがある。

- 中央集中型インシデント・トラッキング (Centralized Incident tracking)
- NASA センター間のコーディネーション (Inter-Center coordination)
- トレンド分析 (Trend Analysis)
- 事前準備および対応見直し活動 (Proactive and responsive corrective action)

(略称) 名称	AFCERT Air Force Computer Emergency Response Team
所在地	250 Hall Blvd Ste 139 San Antonio TX 78243 電話：210-977-3157 電子メール：afcert@afcert.kelly.af.mil ウェブサイト： http://afcert.csap.af.mil
設立年月	1992年10月
組織規模(人員)	非公開
組織の目的	1)米国空軍に対する情報保護対策の提供 2)空軍関連政府機関に対する政策決定サポート 3)
組織の位置付け	組織分類：政府・NGO・大学・その他() 上位組織：国防総省、空軍 傘下組織：なし その他関連組織：CERT
ウイルス対策活動内容	調査：空軍情報システムのセキュリティー状況 研究：脆弱性分析 開発：情報保護データベース、パッチ、その他 実施範囲：米国空軍 普及・啓発：特になし サポート：ASIMS 取組み：空軍特殊捜査局と連携 その他： 具体的な活動例(トピック) IloveYou ウイルス対策など
その他	米国空軍の CERT

概要

AFCERT (Air Force Computer Emergency Response Team) の使命は、米国空軍に対し、情報保護(Information Protection)の支援を行うことである。空軍情報システムにおける不正侵入探知、事件対応、セキュリティー情報提供、脆弱性分析などを行う。また、航空幕僚、防衛情報システム局 (Defense Information Systems Agency)、空軍特殊捜査局 (Air Force Office of Special Investigations)、その他の政府機関に対し、政策決定サポートを提供している。

AFCERT は、米国空軍の IT ホットラインと位置付けられており、軍のインターネット NIPRNET を通って空軍基地を通過する全てのデータをモニターするシステムである ASIMS (Atomated Secure Instrument Measuring Systems) を介して、全世界に点在する 100 以上の米国空軍基地同士をリンクしている。ASIMS は、コンピュータ・ネットワークへの不正侵入を検知すると 30 秒以内に AFCERT へ警告を発する。

組織構成

AFCERT は米国空軍の傘下機関である。

主な活動内容

AFCERT の使命は以下のようなものがある。

- 1) 不正侵入やロジック爆弾のようなウイルスなど、電子メールを介して空軍システム・ユーザーから報告された事件に対応する。
- 2) 防止対策の開発および報告された脆弱性に対する対応
- 3) 情報保護データベースの構築及び管理
- 4) 攻撃被害の対応および回復手段の提供
- 5) AFCERT Advisories、AFCERT IP Bulletins、ASSIST Buleltins、CERT/CC Alert、ベンダー主導の掲示板、などの情報の配信

AFCERT の活動の流れとしては、ウイルス検知、脅威分析、データベース作成などの防止対策と共に、AFCERT 内のインシデント・リスポンス・チームが、ウイルス攻撃によりどのような損害が与えられ、システムを回復するにはどのような手順を踏むべきか、という分析を行う。脆弱性の改善とその後の攻撃に対する防衛としてパッチの開発・設定を行う。リスポンス・チームは、事件の通報直後に世界中のどの場所にも派遣できるよう 24 時間体制で待機しており、パッチも AFCERT によって定期的に検査がなされ、有効に機能しているかどうかを確認されるようになっている。また、AFCERT は、空軍特殊捜査局に対し、法律に準拠した上で犯人を処

罰するためのサポートを提供する。

「ILOVEYOU」ウイルス対応

2000年5月4日に「ILOVEYOU」ウイルスが欧州の米国空軍を攻撃したとの警告を AFCERT が受け取った。AFCERT は直ちにウイルスの複製を入手し、ウイルスの拡散を防ぐ対策を講じた。警告発信の3時間以内に、全ての米国空軍ネットワークは保護対策を講じた。

名称	Computer Security Division of NIST
所在地	National Institute of Standards and Technology Information Technology Laboratory 100 Bureau Drive, Stop 8900 Gaithersburg, MD 20899-8900 電話：301-975-2144 Fax：301-840-1357 電子メール： itlab@nist.gov
設立年月	1996 年
組織規模（人員）	55 人
組織の目的	1)コンピュータ・セキュリティー関連情報の啓蒙 2)セキュリティー基準の設定 3)
組織の位置付け	組織分類： <input type="checkbox"/> 政府・NGO・大学・その他（ <input type="checkbox"/> ） 上位組織：NIST、商務省 Technology Administration 傘下組織：CSRC (Computer Security Resource Center) その他関連組織：NSA (National Security Agency)
ウイルス対策活動内容	調査：サイバー攻撃状況 研究：脆弱性分析 開発：セキュリティー標準、暗号化技術、データベース 実施範囲：連邦システム 普及・啓発：政府・一般消費者向けウェブ情報 サポート：データベースなど情報提供 取組み：特になし その他： 具体的な活動例（トピック） ウイルス情報提供など
その他	連邦政府システムの標準設定およびセキュリティー啓蒙活動

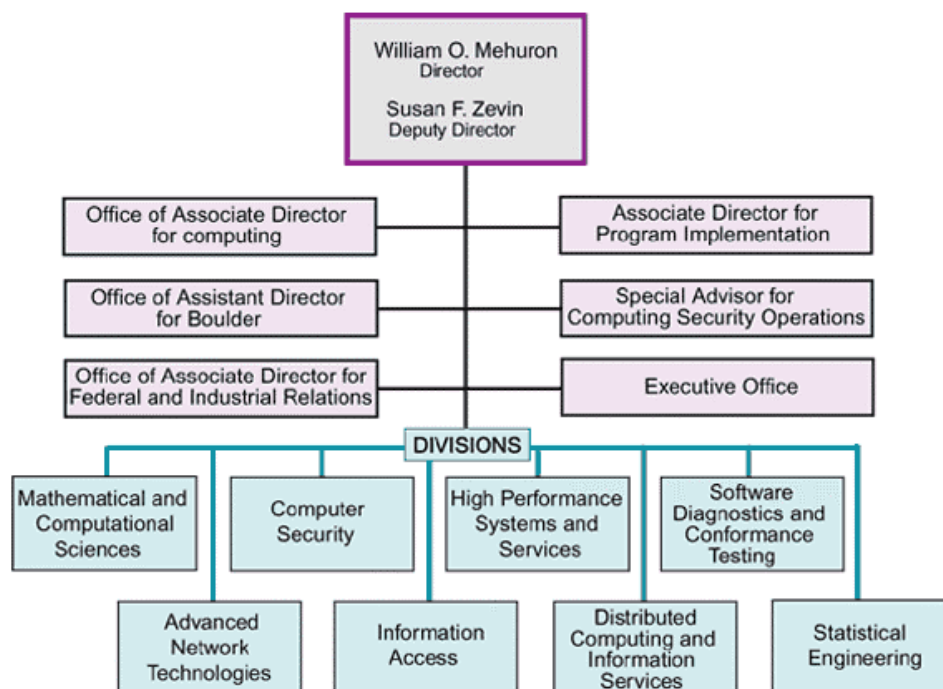
概要

NIST(National Institute for Standards and Technology)の ITL(Information Technology Laboratory)は、年々その需要を増すコンピュータの標準設定および試験技術の開発を行っている。情報インフラの整備やグローバル情報市場の拡大と共に ITL の活動の幅も広がりつつある。NIST は、コンピュータ攻撃などに関する詳細な情報が含まれたデータベースを構築することにより、セキュリティー・コミュニティにおける情報共有を促進するための活動も行っている。

組織構成

Computer Security Division は、NIST の ITL 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その目的としている。

NIST IT Labo の組織図



出典：NIST のウェブサイトより

主な活動内容

- IT リスク、脆弱性、侵入防止策などに関する政府機関およ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。

現在進行中のプロジェクトには以下のようなものが含まれる。

- 高度暗号標準 (Advanced Encryption Standard)
- 認証管理と高度アクセス・コントロール・モデル (Authorization Management and Advanced Access Control Models)
- 暗号ツールキット標準 (Cryptographic Toolkit Standard)
- 情報セキュリティー全国パートナーシップ (National Information Assurance Partnership)
- PKI (Public Key Infrastructure)

また CSD (Computer Security Division) 内に CSRC (Computer Security Resource Center) (<http://csrc.nist.gov>) が設置されている。NIST の CSD は、CSRC のウェブサイトの管理を行っている。CSRC は、コンピュータ・セキュリティ関連情報の収集および配信を行うことにより、ユーザー、システム・アドミニストレーター、システム管理者、セキュリティー専門員などを支援する。CSRC の活動目標は、コンピュータ・システム・ユーザーのセキュリティーに関する知識を高めることである。

CSRC がウェブサイト上で提供する情報には以下のようなものがある。

1) ICAT 脆弱性データベース (ICAT Vulnerability Database)

ICAT は、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であり、パッチなどの情報へのリンクをユーザーに提供する。

2) ウイルス情報 (Virus Information)

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。

3) 事件処理情報 (Incident Handling Information)

1989 年以来、NIST Computer Security Division は、事件処理コミュニティーと密接に関わってきており、今までに蓄積された情報を提供する。

4) コンピュータ・セキュリティ・パッチ (Computer Security Patches)

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する。

5) 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。

また、NIST 内には Computer Security Resource Clearinghouse (CSRC 注 : Computer Security Resource Center の略称と同じ) (<http://csrc.nist.gov/welcome.html>) が設置されている。同機関は、clearinghouse (情報センター) の名の通り、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ーであり、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ある。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が対象ユーザーとなっているものの、CSRC の最終的な目標は、米国の全てのコンピュータ・ユーザーのセキュリティ意識を高めることである。

ディレクトリーで提供される情報は以下のようなものがある。

イベント - セキュリティ関連のセミナーやコンファレンス

組織 - セキュリティ関連の組織・団体

政策 - 米国政府による最新のコンピュータ・セキュリティ関連政策文書

出版 - 情報セキュリティ問題関連の最新の出版物

トレーニング - コンピュータ・セキュリティ専門家及びインストラクターのためのリソース

(略称) 名称	CSI Computer Security Institute
所在地	600 Harrison Street, San Francisco, CA 94107 電話：415-905-2626 Fax：415-905-2218 電子メール： csi@mfi.com ウェブサイト： http://www.gocsicom
設立年月	1974年
組織規模(人員)	非公開
組織の目的	1)メンバーである情報セキュリティ機関に対するサービス提供 2)セキュリティ・セミナーの開催 3)
組織の位置付け	組織分類：政府・ <input type="checkbox"/> NGO・大学・その他() 上位組織：なし 傘下組織：なし その他関連組織：サンフランシスコ FBI
ウイルス対策活動内容	調査：サイバー攻撃被害状況 研究：脆弱性分析 開発：トレーニング・プログラム 実施範囲：官民学セクターからのメンバー機関 普及・啓発：出版物、ニュースレター、セミナー サポート：24時間ホットライン 取締り：特になし その他： 具体的な活動例(トピック) NetSec 国際会議など
その他	米国内外の情報セキュリティ専門機関の協会

概要

CSI (Computer Security Institute) は、企業及び政府機関のネットワーク・セキュリティ専門員のトレーニングを提供する、世界でも最新の情報セキュリティ専門機関のアソシエーション(協会)である。サンフランシスコをベースに、世界中に何千と点在するメンバー機関を擁し、広範囲に渡る情報及び教育プログラムを提供している。メンバー機関は、政府系、民間セクターのどちらも含まれている。1974年に創設されて以来、様々な教育プログラム、トレーニング、出版物を提供している。

CSIは、6月に「NetSec(ネット・セキュリティの略)」会議、11月に「CSI Annual」と、年に2度の国際会議を開催すると共に、暗号技術、侵入対策、インターネット、ファイヤーウォール、啓蒙活動、ウィンドウズ、など幅広いトピックにおけるセミナーを開講している。また、「Alert」というニュースレターや、「Computer Security Journal」という季刊誌、セキュリティ商品の年刊ガイドである「Buyers Guide」などの出版も行っている。これに加え、コンピュータ犯罪やファイヤーウォール製品など広範囲におけるトピックに関するデータや報告書の出版も行っている。

組織構成

CSIは、メンバーである世界中のコンピュータ・セキュリティ機関によって構成されている。会費は以下の通りである。

会員料金

期間	米国内および カナダの会員	米国およびカナダ 外の会員
1年	197ドル	237ドル
2年	349ドル	423ドル
3年	469ドル	567ドル

出典：CSIのホームページより

CSIのメンバーになると、以下のようなサービスが受けられる。

会員特典

1. The Computer Security Alert

CSIの会員のみを送付されるニュースレターによってセキュリティ関連の最新情報が提供される。

2. The Computer Security Journal

四半期に一度、送付される雑誌には、ケーススタディー、調査結果、エキスパートによる解説など重要な技術情報が掲載してある。

3. Educational Discount

CSI の NetSec およびコンピュータ・セキュリティー会議、情報セキュリティー・トレーニング・セミナーの参加費が割引される。

4. Hotline

緊急事態の発生時にメンバーはホットラインを通じてアドバイスを受けることができる。

5. Networking

メンバー同士のネットワーキングができる。

6. Career opportunity

セキュリティー専門家を目指す人へのキャリアに関するアドバイスが受けられる。

7. Computer Security Products and Services Buyer's Guide

セキュリティー製品・サービスの完全ガイドが得られる。

8. Issues & Trends

最新情報と傾向を常にアップデートできる。

9. Publications Discounts

出版物の割引サービスが利用できる。

主な活動内容

上記にあるようなメンバーを対象とした情報提供活動の他にも、CSI は、サンフランシスコ FBI コンピュータ侵入対策班 (Computer Intrusion Squad) の支援を受け、「コンピュータ犯罪とセキュリティー調査 (Computer Crime and Security Survey)」を毎年、行っている。結果は報告書としてまとめられ、電話及び電子メール、ウェブサイトより申し込むと CSI より無料で一般提供される。第 5 回目の「Computer Crime and Security Survey 2000」によると、以下のような結果が出ている。

- 90%のアンケート回答機関（大規模企業及び政府機関）が、12ヶ月以内に何らかのコンピュータ不正行為を検知した。
- 85%がコンピュータ・ウイルスを検知した。
- 60%が DOS (Denial-of-Service サービス停止) 攻撃を報告した。

また、CSI は定期的にセミナーを開催し、一般の参加者に対しても幅広い情報提供・教育を行っている。公認情報システム・セキュリティー専門員 CISSP (Certified Information Systems Security Professional) を目指す受講者のための授業も提供されている。クラス内容を明記した

カタログは電話および電子メール、ウェブサイトで郵送の申し込みができる。

2000年6月に行われた「NetSec2000」Network Security Conferenceにおいては、85を超えるワークショップが開催され、セキュリティー・エキスパートやウイルス・エキスパートによる最新犯罪傾向や取締状況など、様々な項目がカバーされた。NetSec会議は、ネットワーク・セキュリティーに焦点を絞った会議で、ポリシー設定や啓蒙活動などの非技術面における対策と、侵入検知などの技術サイドの対策と、2つのテーマに分かれてワークショップが行われる。2000年はNetSec会議の10年目にあたり、インターネットとイントラネット、安全な電子商取引、コンピュータ犯罪、科学調査（forensic investigation）、リスポンス・チーム、暗号、侵入検知、プライバシー問題、遠隔アクセス、など内容も年々拡大、充実している。

CSIはまた、セキュリティー・セミナーを米国各地の都市で開催しており、ここではセキュリティー入門から専門技術まで、セキュリティー一般に関するワークショップが開催される。2000年に行われた「Information Security Seminars 2000」は、多数の都市で開催された。CSI情報セキュリティー・セミナー2000スケジュールを一部、以下に紹介する。

2月	<u>メリーランド州ゲイサースバーグ</u> 「暗号化及び認証専門員のための実用ガイド」 (A Practical Guide to Encryption and Certificate Authorities)
3月	<u>ミズーリ州セントルイス</u> 「ファイアーウォールとインターネット・セキュリティー」 (Firewalls and Internet Security) <u>ニューヨーク</u> 「科学捜査：ツールと技術」 (Forensic Investigation: Tools and Techniques)
4月	<u>ルイジアナ州ニューオリンズ</u> 「侵入手口とその対策」 (Intrusion Techniques and Countermeasures) <u>オハイオ州シンシナチ</u> 「コンピュータ・インシデント・リスポンス・チームに必要な技術」 (Essential Skills for the Computer Incident Response Team)
5月	<u>カナダ オタワ</u> 「勝つセキュリティー・アーキテクチャの構築」 (How to Develop a Winning Security Architecture)
6月	<u>カリフォルニア州サンフランシスコ</u> 「ネットワーク脆弱性の評価方法」 (How to Conduct a Network Vulnerability Assessment) 「情報セキュリティー・ポリシーの構築方法」 (How to Develop Information Security Policies and Procedures)

出典：CSIのホームページを元にワシントン・コアが作成

(略称) 名称	FIRST Forum of Incident Response and Security Teams
所在地	現在、FIRSTのスタッフは、世界中に点在する機関に勤務する専門家のボランティアによって成り立っており、特定の住所はない。緊急時の連絡はFirst秘書室(Secretariat)である下記の電子メール・アドレスに連絡することになっている。 電子メール： first-sec@first.org ウェブサイト： http://first.org
設立年月	1990年
組織規模(人員)	非公開
組織の目的	1)メンバー機関の情報交換 2)セキュリティー事件処理会議、セミナー、ディスカッション・フォーラムの開催 3)
組織の位置付け	組織分類：政府・ NGO ・大学・その他() 上位組織：なし 傘下組織：なし その他関連組織：メンバー機関
ウイルス対策活動内容	調査：セキュリティー被害状況 研究：脆弱性分析 開発：特になし 実施範囲：米国内外、全セクターからのメンバー機関 普及・啓発：セキュリティー事件処理会議、セミナー サポート：協力体制強化 取締り：当局へ情報提供 その他： 具体的な活動例(トピック) ワークショップの開催など
その他	世界中のCERTを統合する国際相互協力機関

概要

FIRST (Forum of Incident Response and Security Teams) は、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 : computer security incident response teams) を統合する、国際相互協力機関である。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しており、メンバー間の情報交換促進および事件後対応の協力体制の強化を目指している。1990年の設立当時は11であったメンバー機関も1997年には60機関を超え、現在では約70機関に成長している。

FIRST が設立された背景には、世界各国における CERT (緊急事態対応チーム) の急増が挙げられる。米国では、1988年11月、国防総省の ARPANET がウイルスに汚染された事件をきっかけに、CERT/CC が設立され、その翌年、エネルギー省が CIAC (Computer Incident Advisory Capability) を設立した。その後2年間で無数の CERT が世界各国で創設され、それぞれに異なった目的、財源、報告義務などを持って活動を開始した。これら世界中の CERT 間の意思伝達は、言語、時間差、標準などの違いから、ますます困難なものとなっていった。

このような CERT 乱立状態の整備を行い、CERT 間の意思伝達を促進して相互支援体制を確立するために、1990年に FIRST が設立された。現在、FIRST を介して、学際機関、民間産業、ベンダー、政府、軍などあらゆるセクターから参加するメンバーが共同活動を行っている。

組織構成

米国内外の、官民学すべてのセクターから参加するメンバー機関によって構成される。

<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全ての機関がメンバー参加できる。メンバー参加するには、参加申請書を提出し、FIRST 運営委員会が審査を行い、運営委員会の3分の2が承認すると参加が許可される。

メンバーには以下の3種類がある。

- FIRST メンバー：セキュリティ関連の情報技術を提供する機関
- リエゾン：セキュリティには直接関係ないが FIRST にとって有益な機関および個人
- SC メンバー：メンバーより選出され2年間、運営委員会 (Steering committee) として参加し、運営ポリシー、運営方法など全般的な業務を担当する機関

主なメンバーには以下のような機関が含まれる。

民間

アップル・コンピュータ、AT&T、CERT/CC、BCERT (Boeing CERT) など。

米国連邦

NASIRC (NASA)、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 (British Telecommunications CERT Co-ordination Centre)、CERT-IT (CERT Italiano)、JPCERT/CC (Japan CERT 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) など。

<FIRST メンバーの特典>

- メンバー同士によるセキュリティー情報の交換、顧問サービスなどが得られ、問題解決に役立てる。
- FIRST は、コンピュータ・セキュリティー関連事件処理会議 (Computer Security Incident Handling conference) を毎年開催しており、世界中からセキュリティー関連の専門家が参加する。会議は会員、非会員ともに開かれている。
- FIRST 技術セミナー (FIRST Technical Colloquia) は、FIRST メンバー・チームが、脆弱性やコンピュータ犯罪、セキュリティー・ツールなどに関する情報をシェアするためのディスカッション・フォーラムを提供する。フォーラムはメンバー自らの主催で年に2、3回、開催される。フォーラムはFIRST メンバーのみ参加できる。

主な活動内容

<FIRST の活動目標>

1. コンピュータ・セキュリティ犯罪の防止・探知および事件後の対応をより効果的なものにするために情報技術専門家の間の共同活動を促進する。
2. 警告発信および支援情報の伝達手段を提供する。
3. FIRST のメンバー機関のコーディネートを行う。
4. セキュリティ関連情報およびツール、技術の共有を促進する。

(略称) 名称	NU-CERT Northwestern University Computer Emergency Response Team
所在地	Northwestern University Academic Computing and Network Services (ACNS) 2129 N. Campus Drive Evanston, Illinois 60208-2850 電話：(847) 491-4058 電子メール： nu-cert@nwu.edu ウェブサイト： http://grumpy.nsg.northwestern.edu/nu-cert/nu-cert.html
設立年月	1994 年
組織規模（人員）	非公開
組織の目的	1) ノースウェスタン大学内のコンピュータ・セキュリティー改善 2) 大学内の各機関同士の相互支援を促進 3) 警察などの機関へのコンタクトポイント提供
組織の位置付け	組織分類：政府・NGO・大学・その他（ ） 上位組織：Northwestern University – ACNS, UCC and UMS 傘下組織：なし その他関連組織：CERT
ウイルス対策活動内容	調査：大学内のセキュリティー状況の把握 研究：対応の標準化 開発：対応標準化 実施範囲：ノースウェスタン大学 普及・啓発：ニュースグループ サポート：フォーラム開催など 取締り：警察などのコンタクトポイントとなる その他： 具体的な活動例（トピック） ニュースグループへ情報提供など
その他	ノースウェスタン大学の CERT

概要

NU-CERT (Northwestern University Computer Emergency Response Team) は、1994 年、ノースウェスタン大学内のコンピュータ・セキュリティの改善を目的に設立された。NU-CERT は、カーネギーメロン大学に設置されている全国版 CERT の、ノースウェスタン大学版として、その名称を継承している。CERT は、セキュリティの脆弱性や、脆弱性改善のための情報共有を目的に設立され、NU-CERT もその機能を同じくし、ノースウェスタン大学キャンパス内におけるコンピュータ・セキュリティ対応の発信地として活動を行っている。ノースウェスタン大学の教授、スタッフ、生徒に対し、基本的なコンピュータ・セキュリティ知識を提供することを第一の目的としている。

NU-CERT の活動は、UNIX サーバーとワークステーションにおけるセキュリティ管理の重要性をキャンパス内に広めることから始まった。セキュリティ対策はウイルスだけでなく、不正侵入、データ改ざん・窃盗、テロ活動、学術研究不正利用などありとあらゆる不正行為を対象としている。

組織構成

機能、目的は CERT と共通しているが、NU-CERT はノースウェスタン大学内のみで活動を行う独立機関である。

主な活動内容

NU-CERT の活動内容は以下の通りである。

- キャンパス内のネットワーク・セキュリティ改善のためにフォーラムを提供する。
- セキュリティに関する問い合わせを受け付けるコンタクト・ポイントを設置する。
- コンフィギュレーション、管理、バグ修理などを含むコンピュータ・セキュリティ一般に関する情報を収集、配信する。
- セキュリティを向上するためにノースウェスタン大学キャンパス内の相互支援を推進する。
- 何らかの問題が起こった際の部課間の意思疎通を促進するために対応の標準化を行う。
- Darpa CERT、DOE CIAC、警察などに対するコンタクト・ポイントを提供する。
- セキュリティ対応に利用できるキャンパス内のリソースを有効利用できるようにコーディネートする。

NU-CERT の目的は、セキュリティ規制を設定することでも取締の権限を持つことでもな

く、大学内の部課がそれぞれ独自のセキュリティー・ポリシーを設定することを支援することである。

NU-CERT による連絡事項や情報は、ノースウェスタン大学のメールアドレス保持者にのみ有効なニュースグループ (nwu.comp.security) に常時、掲載される。

(略称) 名称	PCERT Purdue Computer Emergency Response Team
所在地	Purdue University West Lafayette, Indiana 電話：765-494-4600 電子メール： pcert-request@cs.purdue.edu ウェブサイト： http://www.cerias.purdue.edu/pcert/pcert.html
設立年月	1990年
組織規模(人員)	非公開
組織の目的	1)パーデュー大学内の機関の意思疎通促進 2)情報提供 3)アーカイブ管理
組織の位置付け	組織分類：政府・NGO・ 大学 ・その他() 上位組織：Purdue University 傘下組織：情報セキュリティ教育センター(CERIAS: Center for Education and Research in Information Assurance and Security) その他関連組織：FIRST、CERT
ウイルス対策活動内容	調査：セキュリティ状況 研究：脆弱性分析 開発：対応標準化 実施範囲：パーデュー大学 普及・啓発：データベース公開 サポート：ウェブサイト情報、電子メールなど 取締り：警察などのコンタクトポイントとなる その他： 具体的な活動例(トピック) モリス虫の分析など
その他	パーデュー大学内のCERT

概要

PCERT (Purdue Computer Emergency Response Team) は、パーデュー大学キャンパス内のコンピュータ・セキュリティの向上を目指し、コンピュータに関する何らかの事件が起こった場合の対応をコーディネートする目的で、パーデュー大学の教授とその他のスタッフとで構成されたチームである。パーデュー大学キャンパス内の、コンピュータ・サイエンス部 (CS: Computer Science Department)、エンジニアリング・コンピュータ・ネットワーク (ECN: Engineering Computer Network)、コンピューティング・センター (PUCC: Computing Center)、総務データ・プロセッシング・センター (ADPC: Administrative Data Processing Center) の専門員が、自主参加型の共同チームとして PCERT を発足させた。

PCERT の活動目標は、コンピュータ・ウイルス、不正侵入、データ盗難、実験妨害、学術用不正使用、詐欺行為、テロリズムなど、パーデュー大学キャンパス内におけるコンピュータ犯罪行為を防止すべく、啓蒙活動を行い、またリスポンス・チームなどの事件対応活動を向上させることである。

PCERT の名称は、DARPA (Defense Advanced Research Project Agency) の CERT (Computer Emergency Response Team) に由来しており、CERT の機能を継承するために PCERT は設立された。

組織構成

PCERT はパーデュー大学の機関であり、パーデュー大学の傘下機関である。PCERT は、FIRST (Forum of Incident Response Teams) メンバーとして参加した最初の大学チームであり、CERT の機能を踏襲している。また、PCERT の設立者の一人が局長を務める CERIAS (Center for Education and Research in Information Assurance and Security) (詳細は次ページを参照) と共同で活動にあっている。PCERT と CERIAS は共同でセキュリティ関連のツール及び資料の情報をまとめたアーカイブを管理しており、情報は <http://www.cerias.purdue.edu/coast/hotlist/> においてパーデュー大学のユーザーおよびその他が閲覧できるようになっている。

主な活動内容

PCERT の活動は以下のようなものが含まれる。

- ・パーデュー大学内のコンピュータ・セキュリティに関する相互支援を促進させる。

- 何らかの問題が起こった際の部課間の意思疎通を促進するために対応の標準化を行う。
- Darpa CERT、DOE CIAC、警察などに対するコンタクト・ポイントを提供する。
- パーデュー大学のセキュリティーに関するセントラル・ポイントとなり情報を提供する。
- コンフィギュレーション、管理、バグ修理などを含むコンピュータ・セキュリティー一般に関する情報を収集、配信する。
- セキュリティー対応に利用できるキャンパス内のリソースを有効利用できるようにコーディネートする。

< CERIAS について >

CERIAS は、インフォメーション・セキュリティーの分野における学際調査および教育を行う世界でも最新の大学センターである。1999 年、CERIAS は、パーデュー大学のコンピュータ・サイエンス部が運営していた COAST (Computer Operations, Audit, and Security Technology) を吸収し、その活動を拡大した。COAST は一学部内の活動に限られていたが、CERIAS はどの学部からも独立しており、リソースとスタッフを全学部から集めているため、その活動がキャンパス全体に及んでいる。CERIAS はパーデュー大学の傘下組織として大学理事会に報告を行う義務を負っている。CERIAS は、2001 年の前半に NIST と共同で IT におけるセキュリティー基準の開発のための官民共同 IT セキュリティー会議を開催する計画を立てており、今後も官民学を横断したセキュリティー対策活動が進められる。

CERIAS の創設者であり PCERT の立役者であるパーデュー大学コンピュータ・サイエンス・インスティテュートのユージーン・スパフォード (Eugene Spafford) 博士は、2000 年 11 月に NIST および NCSC (National Computer Security Center) より「第 23 回 National Computer Systems Security Award」を受賞している。スパフォード博士は、この他にも「モリス虫 (Morris Worm)」の分析や数々のコンピュータ・セキュリティーに関する著作物の出版、パーデュー大学における卓越したリーダーシップ、官民学を取り込んだ地域貢献など、その業績が高く評価されている。

(略称) 名称	SUNSeT Stanford University Network Security Team
所在地	Stanford University Sweet Hall, 3 rd Floor 590 Escondido Mall Stanford, California 94305-3090 電話：1.650.723.2911 Fax：1.650.725.9121 電子メール： security@stanford.edu ウェブサイト： http://www.stanford.edu/group/itss-ccs/security/index.html
設立年月	1995年6月
組織規模(人員)	非公開
組織の目的	1)セキュリティ情報収集 2)セキュリティ対策情報提供 3)事件対応
組織の位置付け	組織分類：政府・NGO・ <u>大学</u> ・その他() 上位組織：スタンフォード大学 傘下組織：スパム対策チーム Stanford University Anti-Spam Team (SUAST) その他関連組織：FIRST
ウイルス対策活動内容	調査：セキュリティ状況 研究：脆弱性分析 開発：対応標準化 実施範囲：スタンフォード大学 普及・啓発：ウェブサイト サポート：ニュースグループ 取締り：スパムメール、電子ハラスメントなどの対応を行う その他： 具体的な活動例(トピック) ニュースグループにウイルス警報など
その他	スタンフォード大学の CERT

概要

SUNSeT は、スタンフォード大学の CERT であり、スタンフォード大学の情報技術システム/サービス部 (ITSS : Information Technology Systems and Services) 内のコンピューティング配信グループ (DCG : Distributing Computing Group) の後援を受けて活動を行っている。スタンフォード大学内のコンピュータ・セキュリティを改善するため、各種のポリシー形成、啓蒙活動、警告発信、セキュリティ・ソフトウェアなどの情報提供を行うと同時に、事件発生時の対策提供を行う。

組織構成

SUNSeT は、スタンフォード大学内の機関であり、同大学が上部組織である。

SUNSeT 内には、スパム問題を専門に取り扱う SUAST (Stanford University Anti-Spam Team) が設置されている。

SUNSeT は FIRST のメンバーである。

主な活動内容

オンラインで以下のような情報が提供される。

セキュリティ・ポリシー設定

- 認証の重要性
- ID パスワードおよび PIN の重要性

セキュリティ・サポート

SUNSeT は、オンライン・ハラスメント、システム不正侵入、ネットワーク不正使用、セキュリティ・ポリシー、法律問題などを取り扱う他、ジャンクメールやスパムなどの問題解決も行っている。スパムなどの嫌がらせなどが送信された場合、[junkmeil@stanford.edu]へ転送し、また誹謗中傷などのメールが送信された場合は[security@standord.edu]に送信するなど、ネットワーク上の一般的な管理を行っている。

ID パスワード基準

- 6 桁から 16 桁の長さであること
- 推測できるような言葉ではないこと

セキュリティ・ソフトウェア

ウイルス対策ソフトウェア情報

以下に SUNSeT による電子メールでの警告連絡内容の一部を紹介する。

1999年6月27日	
対象	Solaris2.x 使用者
日時	1999年6月26日22:00に最初の侵入が検知された。
被害	不明
今後の影響	侵入者は学内コンピュータへのフル・アクセスを持っているため、ファイルを抹消したり、個人メールを読んだり、助成金申請書をコピーしたり、他人のホストを利用して他のコンピュータへの攻撃を行う可能性がある。
SUNSeTによる処置	影響のあったホストのネットワーク・インターフェースをシャットダウンし、被害がこれ以上広まるのを阻止した。
1999年2月25日	
内容	スタンフォード校内の学生寮にて「トロイの木馬」ウイルス・プログラムである Netbus と Back Orifice が発見された。
感染方法	電子メールの添付として「トロイの木馬」プログラムが送信され、送信者は「クリックすれば良いことが起こる」というような内容が書き込まれている。ファイルを開けてプログラムが開始されるとコンピュータのオペレーティング・システムに感染する。
対象	Back Orifice は全てのウィンドウズ 95/98 システムに影響を及ぼす。Netbus は全てのウィンドウズ 95/98 と NT システムに影響を及ぼす。マックは影響されない。
今後の影響	ウイルス・プログラムがコンピュータのオペレーティング・システムに入ると、ウイルス送信者はそのコンピュータをインターネットを介して遠隔操作することができるようになる。
削除方法	トロイの木馬は最新のウイルス対策ソフトウェアで削除できる。スタンフォード・ユーザーは、マカフィーのソフトウェアを無料でダウンロードすることができる。
1999年2月23日	
内容	新しいウィンドウズ・ベースのメール・ウイルス Happy99.exe
感染方法	電子メールの添付として「HAPPY99.EXE」プログラムが送信され、クリックしてファイルを開くと花火のディスプレイが現れ、ウイルスがシステムに感染する。自動的に他の人にも同じ感染メールが送信される。
対象	電子メールにウィンドウズ 95/98 と NT システムを使用している全ての人。マックは影響されない。
防止策	添付ファイルを開かないこと。ファイルを開かなければ感染しない。
削除方法	スタンフォード・ユーザーは、マカフィーのソフトウェアを無料でダウンロードすることができる。

出典：SUNSeT ホームページを元にワシントン・コアが作成

その他コンピュータ・セキュリティー関連組織

1. CIAO (Critical Infrastructure Assurance Office)
<http://www.ciao.gov/default.htm>
2. NCCS (National Computer Crime Squad) [FBI]
<http://www.emergency.com/fbi-nccs.htm>
3. IPCIS (Infrastructure Protection and Computer Intrusion Squad) [FBI]
<http://www.fbi.gov/programs/ipcis/index.htm>
4. NSA (National Security Agency) [NSC, DOD, DOJ, IOB, Congress]
<http://www.nsa.gov/>
5. NCIC (National Counterintelligence Center) [NSC]
<http://www.nacic.gov/>
6. CCIPS (Computer Crime and Intellectual Property Section) [DOJ]
<http://www.cybercrime.gov/>
7. IATAC (Information Assurance Technology Analysis Center) [DISA, DOD]
<http://iac.dtic.mil/iatac/>
8. CSSPAB (Computer System Security and Privacy Advisory Board) [NIST]
<http://csrc.nist.gov/csspab/>

Critical Infrastructure Assurance Office

CIAO

U.S. Department of Commerce
Bureau of Export Administration
Critical Infrastructure Assurance Office
1401 Constitution Avenue, N.W.
Basement Mezzanine 024
Washington, D.C. 20230

電話：202-482-7450
Fax：202-482-7498
電子メール：media@ciao.gov
ウェブサイト：
<http://www.ciao.gov/default.htm>

-
- | | |
|------|---|
| 概要 | CIAO の創設目的は、様々な組織・機関によるクリティカル・インフラ保護計画の国家プランとしての統一、政府のクリティカル・インフラへの依存度分析、国家レベルでの啓蒙プログラム開発、などである。また、政府内で実際に使用されるコンピュータ・ネットワークの強化を支援するために、CIAO は、CIO 評議会（Chief Information Officers Council）など連邦政府コンピュータ・セキュリティ・プログラムの開発・設置に携わる専門員と共同で活動にあっている。 |
| 背景 | クリントン大統領は、1998年5月、クリティカルインフラ保護ポリシーとしてPDD（Presidential Decision Directive）63を発し、それに基づいてCIAOが設立された。 |
| 活動内容 | 啓蒙活動および情報セキュリティに対する投資を増加することによりクリティカル・インフラ・アシュアランス（確保）を促進する。米国においては、州および地方政府、民間セクターによる国家クリティカル・インフラの管理率が高いため、CIAO は、情報システムへ依存することの危険度を明確にするために、官民学セクターにおける情報技術専門家に対する情報提供も行っている。 |
| 上位組織 | 商務省 |

National Computer Crime Squad

NCCS

Federal Bureau of Investigation
Washington Metropolitan Field Office
601 4th Street, N.W.
Washington, D.C. 20535-0002

電話 : (202) 324 - 9164
電子メール : nccs@fbi.gov
ウェブサイト :
<http://www.emergency.com/fbi-nccs.htm>

概要 政府および金融、医療関係のコンピュータへの不正侵入など、連邦犯罪の取締を行う。「連邦レベルのコンピュータ犯罪ケース (Federal interest computers)」は、連邦法によって「多数の州を横断して行われた 2 つ以上のコンピュータに対する犯罪 (two or more computers involved in a criminal offense, which are located in different states)」と定義されており、他州からの侵入を受けた商用コンピュータも「連邦レベルのコンピュータ犯罪ケース」として捜査の対象となる。

背景 NCCS は、「1986 年のコンピュータ不正使用および悪用に関する連邦法 (Federal Computer Fraud and Abuse Act of 1986)」に違反したコンピュータ犯罪を調査するために設置された。FBI のワシントン DC 地区フィールドオフィス内に設置されており、連邦司法権を有する。また海外における犯罪ケースに関して FBI と共同で調査を行う。

活動内容 「1996 年の経済スパイ対策法 (Economic Espionage Act of 1996)」などに基づき、ワシントン DC 地区におけるコンピュータ・スパイ犯罪やその他のコンピュータ関連法律違反を取り締まる。

NCCS の調査対象犯罪ケース

- 電話会社など公益ネットワークへの侵入
- コンピュータ・ネットワークへの大規模な侵入
- ネットワーク不正侵入、データ改ざん
- プライバシーの侵害
- 産業スパイ
- 海賊版ソフトウェア、など

上位組織 FBI

Infrastructure Protection and Computer Intrusion Squad
IPCIS

Federal Bureau of Investigation
National Infrastructure Protection Center
935 Pennsylvania Avenue N.W.
Washington, D.C. 20535-0001

電話 : (202) 323-3205
FAX:(202) 323-2079
電子メール : nipc@fbi.gov
ウェブサイト :
<http://www.fbi.gov/programs/ipcis/index.htm>

- 概要** IPCIS は、FBI のワシントン・フィールドオフィス内に設置されており、NIPC の一部として、コンピュータ犯罪の取締、捜査を行う。対象は、電話会社や民間企業、米国政府機関、官民の教育機関に属するコンピュータ・ネットワークへの不正侵入などである。また、ケーブルや衛星の信号の不法傍受、ソフトウェアの著作権侵害などの捜査も行う。特にワシントン DC 地区の電気通信インフラに被害があった場合、どのような影響が及ぼされ得るのか分析するために、産業セクターと共同で捜査活動を進める。
- 背景** 1998 年、NIPC の設立時に、NIPC のコンピュータ犯罪捜査班として設立された。
- 活動内容** ウェブ上に「不正侵入報告フォーム (Intrusion Report Form)」が設置されており、不正侵入の被害を受けた組織がすぐさま IPCIS に連絡できるようになっている。また、一般にコンピュータ不正侵入に関する情報を持っている人に対して情報提供を呼びかけており、民間からの情報収集にも努めている。
- 被害を受けた組織に対する対応は、専門技術のアドバイス、事件の全国レベルでの通知、地域警察と国家安全対策レベルの情報交換、その他政府機関と合同調査、宣伝を利用した抑止効果、などがある。しかし、被害を受けたシステムの修復や、犯人の情報公開、被害再発の防御、などは行わない。
- 上位組織** FBI、NIPC

National Security Agency
NSA

National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000

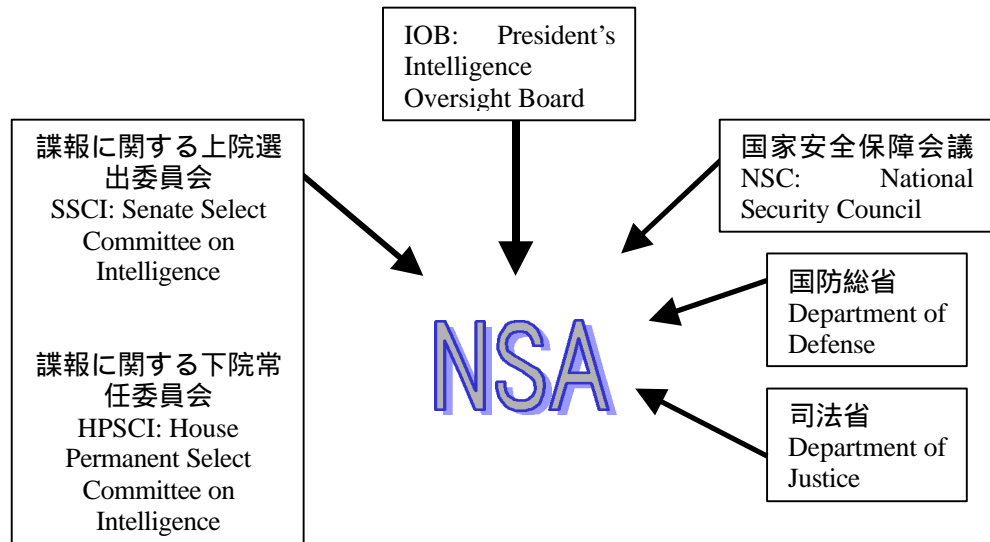
電話 : (301) 688-6524
ウェブサイト : <http://www.nsa.gov/>

概要 NSA/CSS (National Security Agency/ Central Security Service) は、米国の公式な機密暗号組織であり、米国政府の情報システムの保護および機密情報信号の作成を主な使命として国防総省をサポートしている。

背景 1952 年に国防総省内に設立され、朝鮮戦争などにおいて諜報活動および政府の秘密通信活動を行い、現在に至っている。CSS (Central Security Service) が、軍と NSA の暗号技術を一つに統合するために 1972 年に設立され、現在では総称して NSA/CSS と呼ばれることもある。

活動内容 サービス提供機関は、大統領府、CIA や国務省など各政府機関、軍など、米国の保安、防衛に携わる政府組織である。傍受、不正アクセスなどの国家セキュリティ・システムに対する脅威から政府組織を保護する。政府の機密情報を扱うため、人員数および予算、施設などは一般には公開されない。

上位組織 NSA の監督を行う上位組織



出典 : NSA のホームページを元にワシントン・コアが作成

National Counterintelligence Center
NACIC

National Counterintelligence Center
Room 3W01, NHB
Washington, DC 20505

電話 : (703) 874-4123
ウェブサイト : <http://www.nacic.gov/>

-
- 概要** NACIC は、諜報に関連した報告書をウェブサイトにて定期的に出版しており、一般市民の啓蒙活動も行っている。コンピュータ・セキュリティーに関しては、「Networked Information Systems: Protecting Against the Threat 2000」という10ページの報告書を掲載しており、コンピュータ・ネットワークに対する外国の諜報活動やハッカーによる犯罪に関する基本的な情報を提供している。
- 背景** NACIC は、1994年に設立された諜報活動機関であり、米国政府および民間セクターに対し、国家レベルの諜報活動関連製品・サービスを提供する。NACIC は、NSC (National Security Council) の下部組織として、セキュリティー専門人員をFBI、CIA、NSA、軍などから配置している。
- 活動内容** NACIC は、「Program Integration Office」「Threat Assessment Office」「Executive Secretariat」の3つの事務局に分かれており、それぞれサービス提供を行っている。
- Program Integration Office : (703) 874-4122
- 諜報運用プログラムに関する国家戦略
 - 民間セクターに対する諜報支援
 - コミュニティー・トレーニング、など
- Threat Assessment Office : (703) 874-4119
- 国家により義務付けられている研究、報告書作成
 - 外国からの諜報脅威の分析、など
- Executive Secretariat : (703) 874-4121
- 政策の見直し
 - リソースの確保、など
- 上位組織** NSC (National Security Council)

Computer Crime and Intellectual Property Section
CCIPS

Department of Justice
Computer Crime and Intellectual Property
Section
P.O. Box 887
Ben Franklin Station
Washington, D.C. 20044-0887

電話 : (202) 514-1026
Fax : (202) 514-6113
ウェブサイト : www.cybercrime.gov/

-
- 概要** CCIPS は、コンピュータ知的所有権に係わる犯罪を専門とした弁護士、約 50 人を擁している。CCIPS 弁護士は、連邦政府検察官や警察などに対する助言の提供、関連法の提案、コンピュータ犯罪対策の国際的なコーディネートなどを行う。CCIPS 弁護士は、コンピュータ科学者、コンピュータ・エンジニア、連邦政府検察官などの専門職を経ている者が多い。知的所有権以外の分野における専門は、電子プライバシー権に係わる法律、電子商取引、ハッカー捜査などがある。
- 背景** CCIPS は、司法省 刑事犯罪セクション (Criminal Section) 内の、General Litigation and Legal Advice Section (現在は存在しない) 内のコンピュータ犯罪班 (Computer Crime Unit) として 1991 年に発足し、1996 年に司法省の刑事犯罪部 (Criminal Division) の一セクションに拡大された。
- 活動内容** 訴訟 : コンピュータ犯罪捜査において、訴訟に関する役割を担う。オンライン環境において持ち上がる法律上、司法上、政策上の問題に関し、警察と検察側に対して法律上のガイドラインを作成する。最近では、メリッサ・ウィルスの作成者デービッド・スミスにコンピュータ不正取締法違反で約 8 千万ドルの過失を出したことを認めさせるために検察、警察側の支援を行った。他にも、ロサンジェルスにおけるケビン・ミットニック (世界最大規模のハッキングを行った) ダラスにおけるハッカー・グループ “グローバル・ヘル”、バージニア州アレキサンドリアにおけるエリック・バーンズ (ホワイトハウスのウェブ・ページをハッキングした) などの起訴に成功した。
- トレーニング : CCIPS は、NCTP (National Cybercrime Training Partnership) と呼ばれる、連邦、州、地方政府のコンピュータ犯罪対策トレーニングのコンソーシアムを主催しており、コンピュータ犯罪に係わる政府関係者の教育を行っている。
- 国際活動 : CCIPS は、ハイテク犯罪に関する G-8 Subgroup の議長を務め、コンピュータ犯罪に関するメンバー 15 カ国の相互支援をコーディネートしている。
- インフラ保護 : CCIPS は、国防総省、国家安全保障局 (NSA)、CIA などの機関に対し、情報戦争、インフラ保護などに関する法律上、技術上の助言を与える。
- 上位組織** 司法省
-

Information Assurance Technology Analysis Center
IATAC

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

電話 : (703) 289-5454
Fax : (703) 289-5467
電子メール : iatac@dtic.mil
ウェブサイト : <http://iac.dtic.mil/iatac/>

概要 情報戦争による敵からの攻撃(Information Warfare attacks)などの緊急事態に備え、国防総省に対して情報確保に必要なシステムへのアクセス・ポイントを提供する。ネットワーク及びシステムの防衛に関する的確な判断を国防総省が下せるよう十分な情報を提供する。

背景 1983 年に国防総省の科学技術情報プログラム (STIP: Scientific and Technical Information Program) の一部として発足

活動内容 調査サービス

基本調査 - 情報確保 (Information Assurance) に関する情報を提供する。

拡大調査 - 情報検索、分析を行う。

調査・要約 - 関連書物を検索し、重要箇所を要約する。

概説・分析 - 関連書物とラボにおける調査との詳細な分析を行う。

その他のサービス

技術関連 - 調査や分析などの基となる技術的な土台を提供する。

トレーニング・コース - コンピュータ科学捜査など情報セキュリティ関連の教育コースを提供する。

会議・イベント - 公開、非公開の会議を主催する。

データベース : IATAC のデータベースは以下のような情報を提供する。

情報セキュリティ・ツール・データベース - 不正侵入探知、ファイヤーウォール、脆弱性分析などを提供する。

内容別専門データベース - 様々な分野のエキスパートによるポイント・オブ・コンタクト情報を提供する。

文献目録データベース - ポリシー、報告書、レポートなどが含まれる。

インフラ・データベース - 国防総省のインフラ関連文書を提供する。

科学技術情報 : 国防総省に向け、以下のような科学技術情報を提供する。

情報セキュリティ・ニュースレター : 技術の最新情報を紹介する。

情報セキュリティ・ツール・レポート : データベース上のツールを説明する。

評価 : R&D の結果や技術評価を掲載する。

上位組織 国防総省 DISA

運営は民間 IT コンサルティング会社の Booz Allen & Hamilton が行っている。

Computer System Security and Privacy Advisory Board

CSSPAB

Computer System Security and Privacy Advisory Board
Executive Secretariat
National Computer Systems Laboratory
Technology Building, Room B-154
National Institute of Standards and Technology
Gaithersburg, MD 20899

電子メール : elaine.frye@nist.gov.
ウェブサイト : <http://csrc.nist.gov/csspab/>

-
- 概要** CSSPAB は、委員長と 12 人の評議員で成り立っている。NIST ディレクターと商務長官が、委員長を含めたメンバーを任命し、任期は 4 年間となっている。メンバーは通常、コンピュータ技術、システム・セキュリティー、電気通信などの分野における専門家から選出される。
- CSSPAB の使命は、連邦政府のコンピュータシステム・セキュリティーとプライバシーに係わる、管理上、技術上、行政上、の問題を明確にし、商務省と NIST に対して助言を行うことである。また CSSPAB は、調査の結果を、商務省、行政管理予算局 (OMB : Office of Management and Budget)、国家安全保行局 (NSA)、その他関連の議会委員会に報告する。
- 背景** 「1987 年のコンピュータ・セキュリティー法 (Computer Security Act of 1987)」の顧問評議会として米国議会が CSSPAB を設立した。
- 活動内容** CSSPAB は、連邦政府のコンピュータや電気通信システムにおける機密情報に係わる問題を調査する。民間セクターのシステムはサービスの対象とならない。CSSPAB は、基本的に年に 2 回、2 日間の会議を開催し、商務省長官と NIST ディレクターに提出する報告書を編纂する。それ以外は委員長の要請により随時、会議が開かれる。
- 上位組織** NIST