過去の事例

FBI press room Congressional Statement 2001 August 29,2001 より

Leave Worm のケース

2001 年 6 月 23 日、NIPC は Leave Worm ウイルスに関して"Advisory 01-014"を発令。

7 月 23 日、24 歳の英国在住の男性を"Computer Misuse Act 1990"違反で逮捕。英国法のもとでは、このときこの男の身元確認を取れず（The individual who, under British Law, malicious code, known as the W32-Leave.worm, or Leaves worm, into Windows-based computer systems）、ウインドウズマシンが感染すると不正アクセスを可能にしてしまう W32-Leave.worm、Leaves Worm で知られるマリシャス・コードを作成し、広めたことに関わったとして逮捕された。
2001 年 9 月 24 日にこの男は、保護監察から解放され、New Scottland Yard に戻るよう命令された。

このマリシャス・コードは Systems Administration and Network Secutiy (SANS) Institute による分析によって、解明され、SANS によって、NIPC に報告された。

この逮捕は、FBI とスコットランドヤードの捜査協力によるものである。

Code Red のケース

Code Red はネットワークアドミニストレータによって、2001 年 7 月 13 日に発見された。

2001 年 6 月 19 日、NIPC と FedCIRC 共同で、マイクロソフト・ウインドウズ NT、2000 のシステムに脆弱性があると advisory を発令。

2001 年 7 月 19 日、NIPC は Code Red についての Advisory を発令。Code Red は、一番初めに eEye Digital Security という会社によって、マイクロソフト IIS Interet Server Application Program Interface (ISAPI) の脆弱性につけこむものと報告された。

2001 年 7 月 20 日、Code Red による Denial Of Service (DOS) が発生。
www.whitehouse.gov も感染。

NIPC は政府、民間セクターのパートナーとの協力の下、「Windows2000、NT の利用者はパッチファイルをインストールする必要がある」ことを知る。以下の機関からの担当官は、7 月 28-29 日の週末を通して、リスポンスに尽力した。

NIPC, CIAO, FedCIRC(of the General Services Administration), CERT/CC, SANS Institute, Microsoft, Internet Security Systems, Inc.(ISS), Cisco Systems, ITAA (Information Technology Association of America ITの業界団体,Digital Island ,Inc., IT-ISAC, Internet Security Alliance(ISA), UUNet, America Online, Partnership for Critical Infrastructure Security(PCIS)

2001年7月29日、NIPC、Microsoft, FedCIRC, ITAA, CERT/CC, SANS Institute, ISS, ISAは、共同でCode Redに対する警告メッセージを共同で発令。

NIPCは、InfraGardメンバーにInfraGardネットワークを通して警告発令。州、地方警察にNational Threat Warning System[2] を通して警告発令。FBIのAwareness National Security Issues and Response(ANSIR)[3]を通して、何万の民間企業に警告を発令。

マイクロソフトはパッチファイル作成。200 百万のファイルがダウンロードされた。

NIPCは8月16日、"Code Red Reminder and Clarification , Assessment 01-018"と言うassessmentを発令。Code Redに脆弱性のあるシステム、ソフトを明らかにした。

Lion Internet Wormの事例

2001年3月30日、NIPCの"Lion Internet Worm"に関するadvisory発令。

Unixを狙ったDDOS "Destributed Denial of Service" ツールをシステムから取り除く解決方法を、NIPCはシステムアドミニストレータ達に指示。この警告はFedCIRC、JTF-CNO、ISAC、その他のインフラのパートナーとの協議後に発令された。

---

[2] テロの際の連絡用にしかれたもので、政府機関、民間セクターへの連絡用のネットワーク。ANSIRはNational Threat Warning Systemの一部。

[3] ANSIR(Awareness of National Security Issue and Response)
FBIの国家安保認識プログラムとして、インフラの保護、スパイ、防諜、大規模テロなどに対する広報機能を担当する。このプログラムは未分類の国家保安上の脅威や警告をアメリカ国内安保関連機関に提供し、関連情報の提供についても電子メールとファックスを通じて受け付けている。

ヒューストンのある中小企業でのハッキング事例

2000年3月29日、ヒューストン中小企業に不正アクセスがあり、ハードディスクの内容が消された。

FBIヒューストンオフィスは、調査開始。翌日、ヒューストンオフィスがwormを作成したと思われる人物の居場所を捜査。

NIPCはNIPCのホームページ、SANS, InfraGardを通して公的機関に警告を発令。政府機関にテレタイプを打った。これにより、マリシャスコードが公的機関に放たれるのを防ぐことができた。

Melissa Marco Virusのケース

5月26日午後、ウイルスに関する第一報がNIPCのもとに届く。同日夕方、DOD等の政府機関からウイルスの発生を伝える電話がNIPCのもとに届く。

NIPCは速やかに調査を開始すると同時に、CERT/CCに電話をし、ウイルスが民間にも被害を与えているかを確認。alertを企業、政府機関、個人に発令することを決定し、さらにメリッサに関する警告を準備し、24時間警戒態勢に入る。

真夜中過ぎ、州、地方当局、連邦政府機関、そしてすべてのFBI地域オフィスに警告を発令。警告の内容は、ウイルスの特性と検知、駆除のためのサイトへのリンク。警告はInfraGardを通じて、民間セクターに発令された。また、FBIのAwareness of National Security and Response (ANSIR) プログラムで、10万の米国企業に向け発令された。NIPCは、その警告のコピーをCERT/CCに送り、ウェブにも警告を公開。

週明けの月曜日、5月29日にはオフィスに人が入るので、ウイルスが広まることが予想されたため、NIPCは日曜日にプレスに公開した。NIPCはウイルスの広がり、対応についてDOD、CERT/CCとの連絡を絶えず取る。

この捜査は、FBIのニューアークオフィスとニュージャージー州警察が協力して行った。

America Onlineからのニュージャージー州警察への捜査協力？(A tip received by the New Jersey State Police from America Online　この場合のtipは協力ということか？)、またＦＢＩのニューアークオフィスとの捜査協力により、1999年4月1日、犯人David L. Smithを逮捕。

犯罪グループによるコンピュータ侵入のケース

1999年9月、“Phonemasters”の異名をとるグループの2名がデバイスへの不正アクセス(18 USC, 1029)、連邦政府コンピュータへの不正アクセス(18 USC, 1030)で有罪判決を下された。

Phonemastersは国際的な犯罪グループでMCI, Sprint, AT&T, Equifax, FBIのNational Crime Information Centerにも侵入をした。

FBIダラスオフィスはCalvin Cantrellという容疑者の電話、モデムのパルスをモニタリングした。

Cantrellは Sprintの電話カードの番号を数千ダウンロードし、カナダ人にそれを売り、そのカナダ人はオハイオ州在住の人物にそれを渡していた。それらの番号は、スイス在住の者に渡り、最後にはイタリアの犯罪組織の手に渡っていた。

DDOSの例

1999年秋、新たなDDOS攻撃の脅威のレポートが何件かNIPCに届いていた。これらのケースには、Denial of Serviceを引き起こすことができる、Trinoo, Tribal Flood, TFN2K, Stacheldrahtなどのツールが使われた。

1999年12月に、NIPCはこれらのハッカーツールに関する脅威の警告を民間セクター、政府機関に発令。

NIPCの Special Technologies and Application Unit(STAU)は、システムアドミニストレータが DDOS ソフトがコンピュータにインストールされたことを検知できるパブリックソフトを作成し、リリースした。公的機関は、NIPCのウェブからそのソフトをダウンロードし、DDOSソフトがインストールされてしまったとき、侵入されたときにはFBIに報告した。

米国におけるサイバー・セキュリティ政策関連動向

1998年　クリントン政権　以下の四分野への対応強化

- 諸外国の法執行機関との国際協力
- 暗号政策の推進
- セキュリティ研究開発
- 重要インフラ保護

2000年1月「国家情報システム保護計画」第一版発表。

2月　ヤフー、アマゾンへのサービス妨害　(DDS) 事件。

クリントン大統領とＩＴ企業首脳が会談。

- 「Partnership for Critical Infrastructure Security」設立。
- 2000年度補正予算で900万ドルのセキュリティ予算確保。
- 2001年度予算で20億ドルセキュリティ予算要求の詳細発表。

1. 諸外国の法執行機関との国際協力

□ リヨングループ（国際組織犯罪上級専門家会合）のハイテク犯罪サブグループ

- 24時間体制のコンタクトポイント設置。
- ハイテク犯罪捜査促進のための法制度の検討。
- 操作共助要請に対する迅速な対応。
- 国境を越えたデータに対するアクセスのあり方等について議論。
  同グループと産業界の合同会合も開催。

□ 世界主要IT産業団体の集まり IITC (http:www.iiicongress.org)

- サイバー犯罪に関するコモンビュー・ペーパーについて議論。
- 人材、知識ベース、情報交換メカニズムなどのリソースの拡充。
- 刑法改正。
- 国境を越えた操作などに関わる国際協力。

□ GBDe(http:www.gbde.org)総会開催

- 産業界による自発的な情報共有メカニズムの確率に焦点。
- WITSによるGlobal InfoSecSummit (http:www.itaa.org/infosec/sumit.htm)
- ワシントンDCにInternational Information Security Coordinating Center

2. 暗号政策の推進

- 暗号製品の輸出緩和。
- DES 暗号に変わる次期暗号標準を選考中。
- 電子署名法を 2000 年 9 月に発効。

3. 重要インフラ保護

1998 年　クリントン大統領の通達　PDD63

- 2000 年までに「政府情報システムの安全性を著しく高める」
- 2003 年までに「信頼性が高く、相互接続された、安全な情報システム・インフラストラクチャを構築」を要求。
  - ・ホワイトハウスに行政府全体の調整を図る総責任者「National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism」を置く。
  - ・上記通達実行のため中心組織として、商務省内に「CIAO(http:www.ciao.gov)」を設立→「国家情報システム保護計画」の第一版を公表。

「国家情報システム保護計画」の内容は、ファイル「国家情報システム保護計画」を参照のこと。

「インターネット犯罪とエンフォースメント」

FBIの「カーニボー」（電子メールその他の電子的通信を盗聴するシステム）を例に。

プライバシーとカーニボー（ネット犯罪捜査）はtrade-off。

「米国市民自由連合（ACLU）」「電子プライバシー情報センター（EPIC）」から人権 問題を訴えるケースもある。

民間企業、特にISPからカーニボーに対する拒否反応も強い。

「サイバー犯罪とプライバシー保護」

「電子フロンティア：インターネットの利用による違法行為の挑戦」（司法省がサイバースペース上での不法行為を取り締まるための提言をまとめたもの）

→法執行機関は「匿名を使ったユーザの身元確認を行う能力」等の能力を身に付けなくてはならない。既存の連邦法を改正する必要も。

匿名性の保護については市民団体とプライバシーの観点でもめている。