次世代ＩＰインフラ研究会
報告書（案）
(version.4)

「情報セキュリティ政策２００５」

２００５年5月２０日

セキュリティWG

本報告書で取り上げる事項

(Agenda)

1. インシデント対応の現状と課題

- Our security depends on your security -

2. ユビキタスネット社会におけるセキュリティ確保

- 情報家電のネットワーク接続に伴う課題 -

3. 電気通信事業における情報セキュリティマネジメント

4. セキュリティ人材育成

目次

序章　はじめに

インターネットが「有用」であることに異論を差し挟むユーザは、もはや少ないであろう。

それどころか、内外の社会経済活動は、インターネットへの依存度をますます高めていると言える。

金融、航空、鉄道、電力、ガス、政府・行政サービス等他の重要インフラも、インターネットを活用するに至っており、インターネットは、今や社会インフラとして定着してきていると言えよう。

他方で、我が国のインターネットは、２１世紀以降、急速にブロードバンド化が進み、「速さ」と「安さ」において世界 1 との評価を受けるに至っており、常時接続のブロードバンド・ユーザは、ダイヤルアップがインターネット接続の主流であった２０世紀中に比べ、トラヒックの受発信において数１００倍のパワーを有していることも認識しておかなければならない。

このため、インターネット接続サービス提供事業者（ＩＳＰ；Internet Service Provider）にとって予想もつかないようなインターネットの使い方をするユーザも存在し、そのユーザが発生させるトラヒックがＩＳＰのネットワークに過剰な負荷を与えてしまう、といった事案も発生しているのが実情である。

更に、ブロードバンドの普及によって、情報通信技術（ＩＣＴ）の機能不全による障害（インシデント）も広域化・多様化が進んでおり、こうしたインシデント事案に対し、ＩＳＰは、時としてアクロバティックな運用により、対処しているのが実態である。

しかるに、果たして何人のユーザが上記のような実態を認識しているであろうか？

また、自らの通信機器がウイルスに感染していることに気付かず、無意識のうちに感染を更に拡大させ、他のユーザやＩＳＰの通信機器に攻撃を加えてしまう場合があり得ることを、どれ程のユーザが自覚しているであろうか？

加えて、インターネットの分野は、”dog year”あるいは”mouse year”と言われるほど技術革新が著しく、こうした技術革新の速さが、ブロードバンド・ユーザがどのようなインターネットの使い方をしてくるか予想できないという事情とも相俟って、「次世代」のＩＰ（Internet Protocol）インフラに必要な要件は何か、についての像を描きにくくしている。

実際のところ、１０年先、５年先はおろか、２～３年先、１年先の像さえ描きにくいというのが、多くのＩＳＰの実感であろう。

ただ、情報家電を始めとするさまざまなモノがインターネットに接続される「ユビキタスネット社会」が到来するであろうことは、現時点でも、通信業界・家電業界の双方から想定され、期待されているところである。

しかるに、家電がインターネットに接続され、通信機器として機能すると、情報セキュリティ上の問題も発生し得ることを、どれ程の消費者が承知しているであろうか？

「次世代」のＩＰインフラを論ずる際には、不正アクセス、ウイルス、ワーム等々の情報セキュリティをめぐる問題は、インターネットを利用するからこそ発生するという認識から出発する必要がある。

すなわち、通信インフラ側から通信サービスの提供条件を規定してきた「電話の時代」には、不正アクセスやウイルス感染、ワーム等は大きな社会問題とはならなかった。

通信インフラの種別を問わず、また、様々な通信アプリケーションを伝送することができるという特徴を有するＩＰインフラの利用が拡大するに伴い、不正アクセス、ウイルス、ワーム等によるインシデントが大きな問題になってきた、という歴史的認識を持つ必要がある。

換言すれば、インシデントへの対応、家電のネットワーク接続に伴う情報セキュリティの確保といった課題を検討することで、「次世代」のＩＰインフラの像を（少なくともその一部なりとも）描くことができ、更に、これらの課題を克服することで「次世代」のＩＰインフラの実現に寄与していくことができるものと考えられる。

今や社会経済活動のインフラとなっているＩＰインフラの、「次世代」に向けての課題の１つが、情報セキュリティの確保である、ということである。

一般ユーザのセキュリティ意識の低さ、組織内従業員の無知・無警戒、経営陣による情報セキュリティマネジメントの未実施、ＩＳＰ等電気通信事業者におけるセキュリティ人材の不足、等といった人材面の脆弱性を克服していくことも、「次世代」のＩＰインフラの実現に寄与するものと言えよう。

そこで、この「次世代 IP インフラ研究会」では「セキュリティWG」を設置して、検討を行った。

まず、第１章において、不正アクセスやウイルス、ワームからボットネットに至るまで、最近のネットワーク運用においてＩＳＰがどのようなインシデント事案に直面しているかについて、実情をレビューするとともに、今後の課題を整理している。

また、第２章においては、今後あらゆるモノがネットワークにつながる「ユビキタスネット社会」において、日本が世界のフロントランナーを目指す観点から、情報家電を含む様々なモノが接続されるに伴い、より多様化・高度化するインターネットにおいて、情報セキュリティをどのように確保すべきかについて検討している。

第３章においては、ＩＳＰを含む電気通信事業者において、経営陣が情報セキュリティマネジメントをどのように行っていくべきかについて、国際電気通信連合（ＩＴＵ）におけるＩＳＭＳ－Ｔ（Requirements for telecommunications of information security management system）の策定に係る動きも踏まえながら、今後の課題を整理している。

更に、第４章では、あらゆるセキュリティ対策を講じる上での基盤となる人材の育成について、電気通信事業者における取組みの現状を踏まえつつ、今後の政策支援の在り方について、諸外国の取組事例も踏まえて、検討を加えている。

情報セキュリティ対策に完璧なものはあり得ない。

計画し（Plan）、実行し（Do）、点検し（Check）、処置する（Act）という P-D-C-A のサイクルを繰り返すことにより、セキュリティ水準の向上を図っていくことが必要である。

このことは、インターネットがいま現在も急速に進化・発展を続けるオープンなネットワークであることを考慮すれば尚更である。

本報告書は、２００５年時点での我が国のインターネットの現状を踏まえ、情報セキュリティに係る課題を整理し、「情報セキュリティ政策　２００５」という政策提言を取りまとめたものであり、ＩＰインフラにおける情報セキュリティの確保に取り組まなければならないあらゆる関係者の「永続的な」取組みの一助となれば幸いである。

第１章　インシデント対応の現状と課題

- Our security depends on your security -

１．１　ＩＣＴ障害

情報通信技術（ＩＣＴ）の機能不全による障害（以下「ＩＣＴ障害」という。）については、

①　不正アクセスやウイルス、ワーム等によるＩＣＴ障害（以下「インシデント」という。）

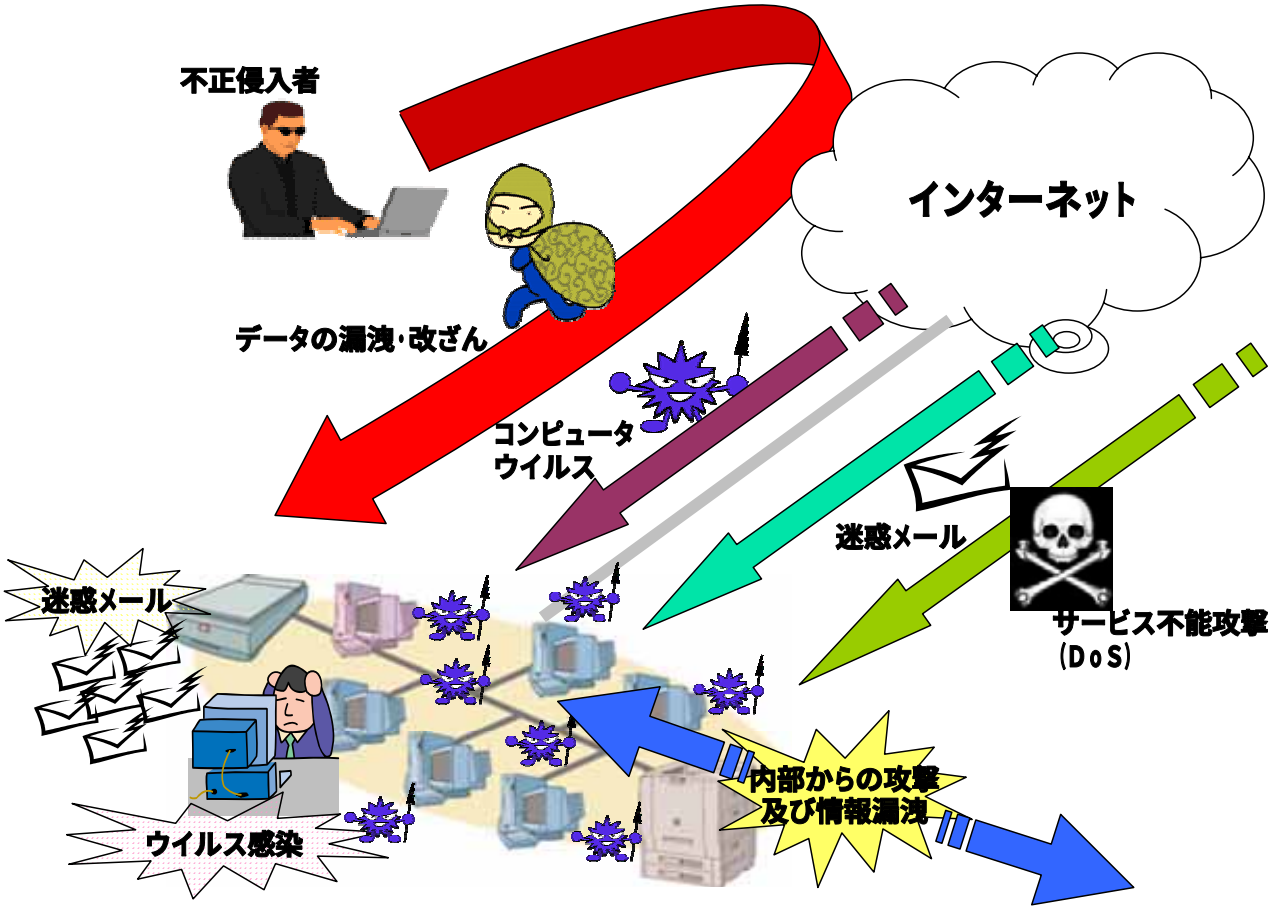
②　経路情報の誤りによるＩＣＴ障害

③　自然災害によるＩＣＴ障害

という３つのタイプに分けて考えることができるが、ここでは、インターネットの進化・発展に伴い障害事案が大きく変化してきている①と②について検討する。

特に①については、障害を発生させる者に対し、「電子計算機損壊等業務妨害罪」（刑法第２３４条の２）や「不正アクセス行為の禁止等に関する法律」、「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」に盛り込まれている「不正指令電磁的記録作成罪」（いわゆるウイルス製造罪）等によって、制裁措置がきちんと担保されているか、制裁措置の対象に漏れはないか等について法制上の精査を行うことが求められるが、この研究会では、障害の発生による影響を受ける側にとって、障害の検知・回復・予防をどうするかという観点から検討を加えた。

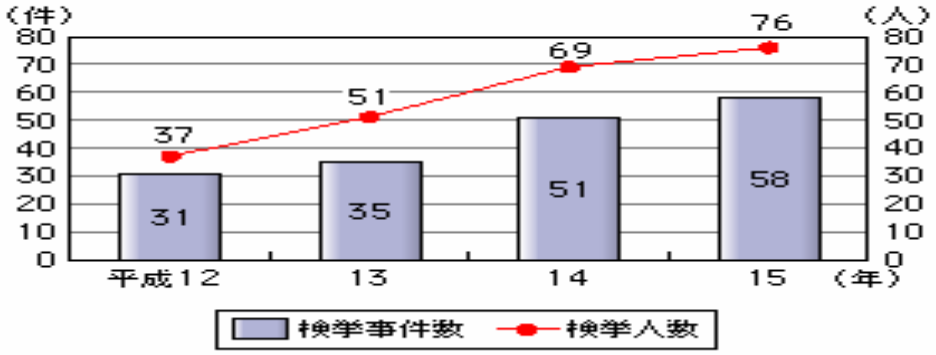
▽　インシデントのイメージ図



１．２　インシデントの最近の傾向

情報通信ネットワークへの不正アクセスは、物理的な侵入を伴うものから、ネットワークを介してリモートでアクセスするものへと拡大してきた。

▽　不正アクセス禁止法違反事件の検挙状況の推移



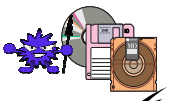
国家公安委員会、総務大臣、経済産業大臣
「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」より作成

ウイルス(注１)やワーム(注２)の感染についても、フロッピーディスク等の記録媒体を介した感染から、電子メールや Web サイトへのアクセスを介して感染するものや、情報通信ネットワークに常時接続しているだけで感染するものへと拡大してきている。

（注１）ウイルス（virus）とは、他の電子ファイルに寄生する形で感染し、他のプログラムの破壊や削除、ハード・ディスクの初期化等の障害をもたらすプログラムをいう。

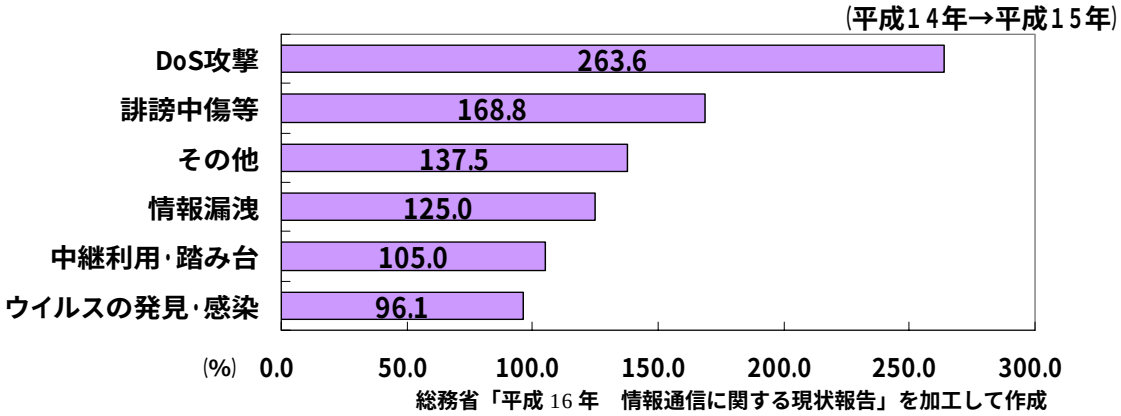
（注２）ワーム（worm）とは、他の電子ファイルに寄生せず、ネットワークを介して自分自身をコピーして単体で自己増殖を繰り返しながら、感染を拡大していくプログラムをいう。ただし、最近では、厳密にはワームであるものも含め、広義の「ウイルス」と呼ぶことがある。

▽　ウイルス／ワームの悪質化

	感染方法	対　策
昔	**媒体(フロッピ等)により感染** 	**①ウイルス対策ソフトによる検知・駆除** **②不審なフロッピを使わない**
最近	**メールやWWWアクセスにより感染** 	**①OSアップデート、②ウイルス対策ソフトで駆除** **③不審なメールの添付ファイルを開かない**
2003年以降	**ネットに接続するだけで感染** 	**①OSアップデート** **②ファイアウォールやルータで不審なパケットを遮断**

また、電子商取引等のサービスを提供している Web サイトに対して、その処理能力を超える多量のデータを送信したり、バグ（ソフトウェアの不具合）を突くことなどにより、サービス提供機能を停止させる「サービス不能化（ＤｏＳ；Denial of Service）攻撃」による被害が、平成１４年から平成１５年にかけて、最も増加している状況にある。

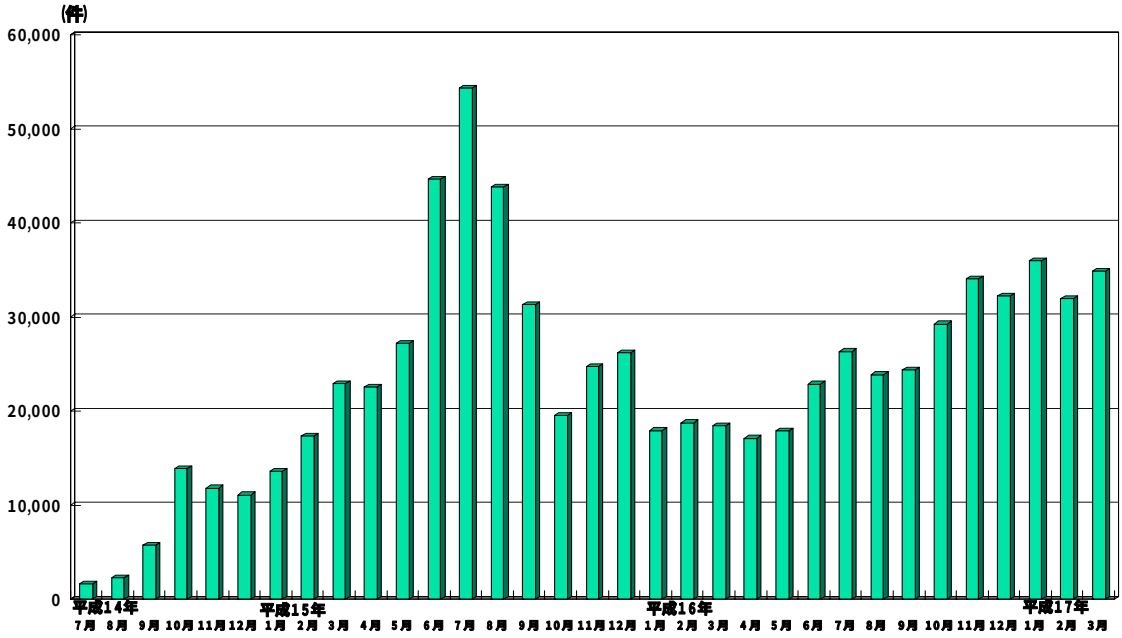
▽　企業の情報通信ネットワークにおける被害内容とその増加率



総務省「平成 16 年　情報通信に関する現状報告」を加工して作成

最近では、受信者の意思に関係なく一方的に送信されるスパムメールにより、大量に広告宣伝メールが送信されたり、スパムメールを利用したフィッシング(注3)やスパイウェア(注4)等による個人情報の不正な収集という新たな脅威が発生している。

▽「迷惑メール相談センター」に寄せられた違法な広告宣伝メールの申告件数の推移



注:「迷惑メール相談センター」とは、平成14年7月10日に、特定電子メール法第13条に基づく指定法人である「(財) 日本データ通信協会」内に設置された組織。

（注３）フィッシング（Phishing）とは、銀行等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ＩＤ、パスワード等）を入力させるなどして個人情報を不正に入手する詐欺的な行為をいう。Sophisticate された手法により個人情報を釣り上げる（fishing）ことから作られた造語と言われている。

（注４）スパイウェア（Spyware）とは、特定の Web サイトを閲覧した際や、他のソフトウェアをインストールした際等に、ユーザが気付かないうちにインストールされ、ユーザの端末機器から個人情報等を収集し、スパイウェアの配布元等、外部に向けて送信するソフトウェアをいう。

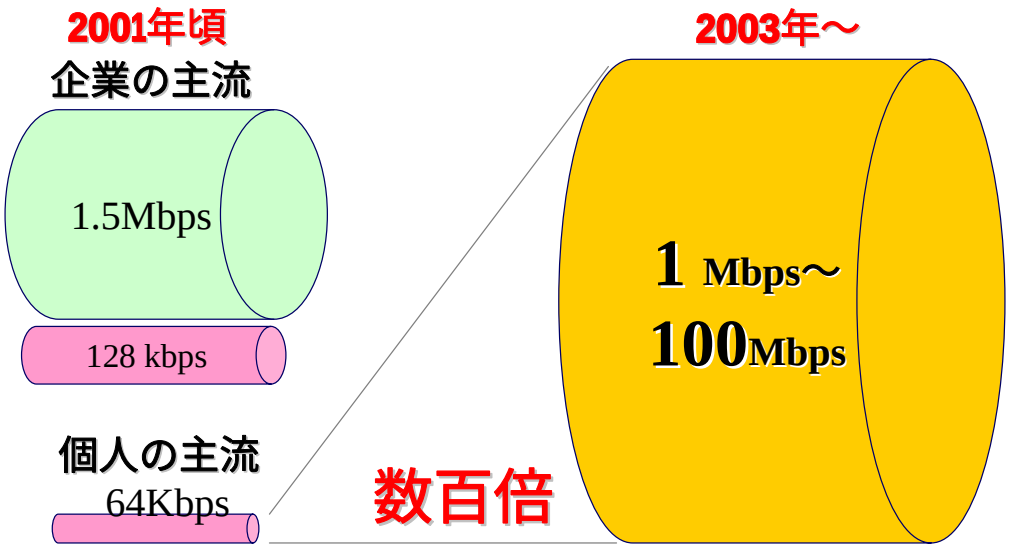
ダイヤルアップ接続等ナローバンド（狭帯域網）によるインターネット接続が主流であった２００１年までは、ユーザの端末機器がウイルスやワームに感染したとしても、ネットワークが被害を受けることは少なかった。

しかし、ブロードバンド（広帯域網）による「常時接続」が急速に普及した２００３年以降は、インターネットに接続しているだけでウイルスやワームに感染してしまい、かつ最新のセキュリティパッチ（ソフトウェアの不具合を修正するためのデータやプログラム）を適用していないユーザが多いことも相俟って、インターネット上にワームが蔓延し、そのワーム自体が大容量のトラヒックを発生させ、ＩＳＰのネットワークに大きな負荷をかけるという事態も発生している。

実際、多くのユーザがキロビット毎秒クラスの速度で、従量課金によりインターネットに接続していた２００１年以前に比べ、メガビット毎秒クラスの速度で、常時接続・定額料金によりインターネットに接続可能な現在のブロードバンド・ユーザは、トラヒックの受発信に関して数１００倍のパワーを有していることになる。

今後、セキュリティに関するユーザの意識を啓発し、ＩＳＰ、システム・インテグレータ及びユーザという３者間で、セキュリティ対策の実装について役割分担を図る必要が出てきていると考えられる。

▽　個人ユーザの影響力の増大



以下では、２００３年及び２００４年に発生したワームに対し、ＩＳＰがどのように対処したかを見ておくとともに、これらの事例から汲み取ることのできる教訓を整理しておくこととする。

１．３　インシデントに対するＩＳＰの対応事例

１．３．１　２００３年　～ネットワーク感染型ワームへの対応～

（1）２００３年に発生した主なワーム

２００３年は、ネットワークを介して自己複製したプログラムを、他の通信機器に送信することにより増殖するワーム（以下「ネットワーク感染型ワーム」という。）が発生し、ＩＳＰがその対応に追われた年であった。２００３年に発生した主なワームは次のとおりである。

▽　２００３年に発生した主なワーム

ワームの名称	概要
１．ソービッグ (Sobig) 2003 年 1 月発見	電子メールや共有フォルダを媒介にして感染する。電子メールを開かなくてもプレビューするだけで感染する。感染するとアドレス帳に登録された者にメールを送信する。また、差出人をアドレス帳に登録されているユーザに設定して送信するため、感染元の特定が難しくなる。2003 年 8 月には、亜種である電子メール添付型のソービッグ F の感染が広がった。
２．SQL スラマー (SQL.Slammer) 2003 年 1 月発見	データベースサーバのソフトウェアである「SQL 2000 Server」のセキュリティ・ホールを媒介にして感染する。感染した機器は、ウイルスの複製を更に他の機器に向け大量に送信するため、ネットワークの伝送速度が下がるおそれがある。これにより、韓国では、全土のインターネットが約９時間にわたり麻痺した（注５）。
３．ブラスター (Blaster) 2003 年 8 月発見	Windows のセキュリティ・ホールを媒介にして msblast.exe というファイルがダウンロードされることにより感染する。感染するとユーザの端末機器が自動的に再起動を繰り返す。2003 年 8 月には、ウェルチア(Welchia)という亜種も発見された

総務省「平成 16 年　情報通信に関する現状報告」より

（注５）SQL スラマーへの感染数が最も多かったのはアメリカであったが、韓国での被害が大きくなったのは、時差による攻撃開始時間と現地時間のズレや、韓国における高速インターネットの急速な普及やそれに反してユーザのセキュリティ意識が低かったこと等が指摘されている。

（２）　ワームの蔓延パターンと一般的な対策

時系列でみると、次のようなパターンで感染が蔓延している場合が多い。

イベント	内容
１．脆弱性情報の公開	**ソフトウェアのセキュリティ・ホール等、脆弱性情報がセキュリティ関連の Web サイトに公開される。ソフトウェアのベンダーがセキュリティパッチと共に公開したり、セキュリティ・ベンダーが任意に公開することが多いが、検索エンジンで到達しにくいアンダーグラウンドなＷｅｂサイトで公開されることもある。前者の場合は、その情報だけでは悪用できない程度の情報が公開されるが、後者の場合は、より詳細で、場合によっては Exploit Code（後述）と共に公開される。**
２．Exploit Code 公開	**脆弱性情報が公開されてから、早ければ数日から１０日後に、このセキュリティ・ホールをつく Exploit Code (注６) が公開される。**
３．ワームの出現	**Exploit Code の公開から、早ければ数日程度でワームが出現する。**
４．大規模な蔓延	**未対策のユーザが多く、ワームの設計が巧妙であれば、被害の蔓延は必至である。**

（注６）Exploit Code とは、セキュリティ・ホールを突いたり、誤動作を引き起こす方法をコード化（プログラム化）したもの。Exploit Code を用いて、実際に被害をもたらすワーム等が作成される。

こうしたワームが出現した場合には、

①　バグを修正するセキュリティパッチを適用する、

②　ワームの感染を検査し、感染している場合にはこれを取り除くワクチン・ソフトを導入する、

といった対応をとることが考えられる。

しかし、セキュリティパッチやワクチン・ソフトが開発されるまでの期間に、ユーザの端末機器はワームに感染する危険にさらされ、また、セキュリティパッチやワクチン・ソフトが仮に開発されていたとしても、ユーザがそれを使用しなければ効果はない。

対応をとろうとしない一般ユーザが多いことも問題であるが、特に業務上の基本的なソフトウェアとなっているＯＳ（Operating System）へのセキュリティパッチの適用に関しては、企業ユーザや Web でサービス提供している事業者においては、早急に対策を取れない事態が発生している。

というのも、基本的なソフトウェアへのパッチの適用が、その上で動作する他のソフトウェアに影響を及ぼすため、実稼動環境と同様のテスト環境で動作検証を行う必要があるからである。

仮に検証結果に問題がなくても、その検証に要する時間は致命的な遅延になり得る。

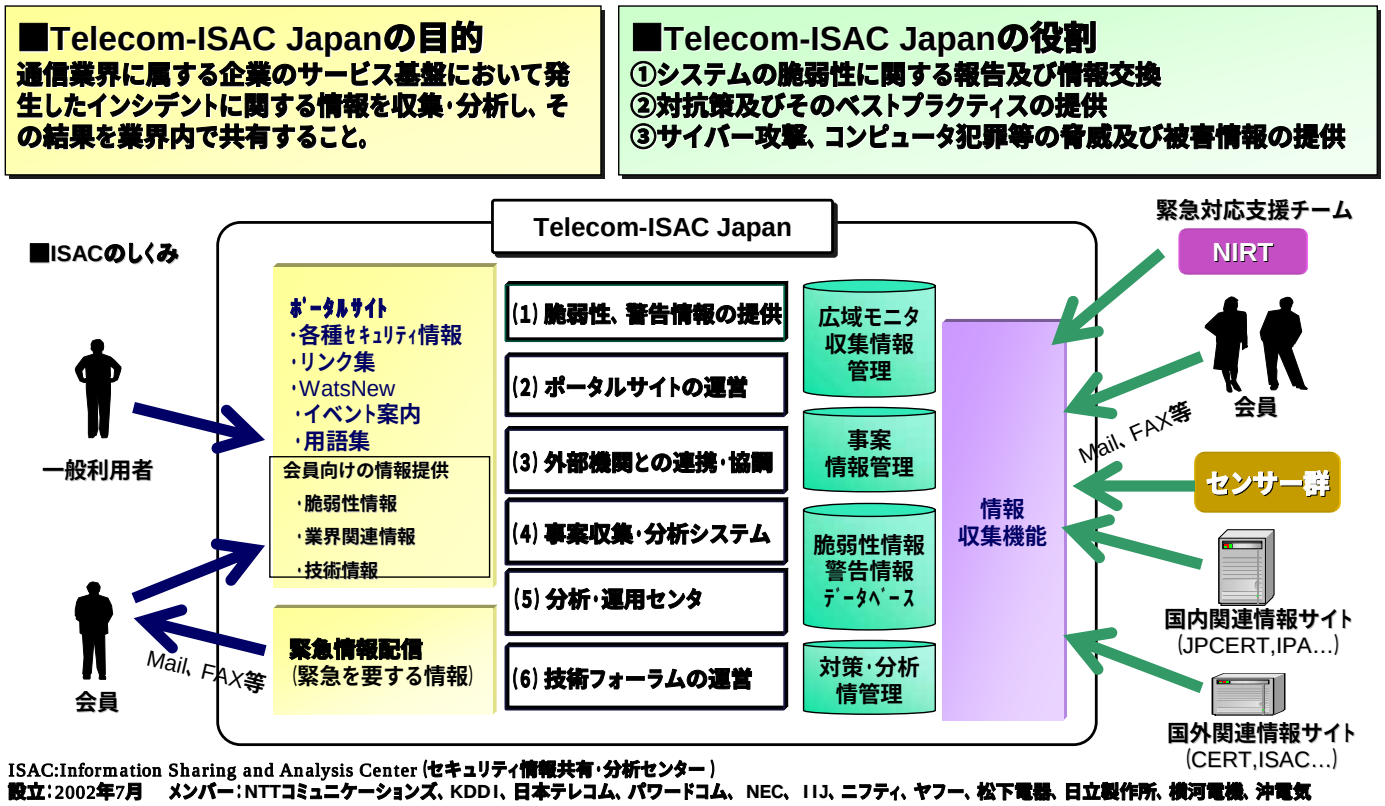
現に、後述するブラスター騒動では、検証期間中に感染して被害を受けた事例が我が国においても存在する。

（３）　ＩＳＰにおける対応事例

一方、ネットワーク感染型ワームは、ネットワークを介して自己複製したワームを他の通信機器に大量に送信する等、ネットワーク全体に与える影響も無視できないレベルにあることから、ＩＳＰ側における対応も必要になる。

ここでは、インシデント情報の収集・分析・共有を目的として、ＩＳＰ等で構成されている組織である Telecom-ISAC Japan における対応事例を紹介しておく。

▽　Telecom-ISAC Japan の概要



１）ブラスターへの対応事例

まず、２００３年８月に出現したネットワーク感染型ワーム、ブラスター（Blaster）に対して、Telecom-ISAC Japan がどのような対応をとったのかを概観しておくこととする。

ブラスターは、Windows のセキュリティ・ホールを利用して msblast.exe というファイルがダウンロードされることにより感染し、感染するとユーザの端末機器が自動的に再起動を繰り返すものである。

ブラスター蔓延とこれに対する Telecom-ISAC Japan の対応は、次のとおりである。

▽　ブラスターの蔓延と Telecom-ISAC Japan の対応

日時	内容
7/17	**セキュリティ・ホールに係る脆弱性情報の公開** **Telecom-ISAC Japan における情報共有開始**
7/27	**Exploit Code 公開**
8/05	**セキュリティ・ホールを狙うトロイの木馬（注7）発見**
8/11	**セキュリティ・ホールを狙う Blaster 発見**
8/12	**Telecom-ISAC Japan と NIRT（注8）との情報連絡体制構築**
8/14	**大規模な蔓延、Telecom-ISAC Japan における緊急対応体制へ** **通信事業者のネットワークへの影響度合いの分析と、対応策の検討（技術的検討）**
8/15　01:00	**全ユーザへの注意喚起メール発出（ＯＣＮの事例）**
8/15　09:00	**監視及びユーザ対応体制強化（ＯＣＮの事例）**
8/15　17:00	**対応策決定、対策実施**
8/15　23:00	**事案の収束に伴い、重点監視体制にシフト**

（注７）トロイの木馬：正体を偽ってコンピュータへ侵入し、データ消去やファイルの外部流出、他のコンピュータの攻撃などの破壊活動を行なうプログラム。トロイの木馬はウイルスのように他のファイルに寄生したりはせず、自分自身での増殖活動も行わない。

（注８）NIRT とは、政府や重要インフラ事業者の情報システムへのサイバーテロ等、国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案について、各省庁における情報セキュリティ対策の立案に必要な調査・助言等を行うために内閣官房に設置された緊急対応支援チーム(National Incident Response Team)をいう。

2）ソービッグＦへの対応事例

次に、同じく２００３年８月に出現したソービッグＦ（Sobig-F）に対して、Telecom-ISAC Japan がどのような対応をとったのかを概観しておくこととする。

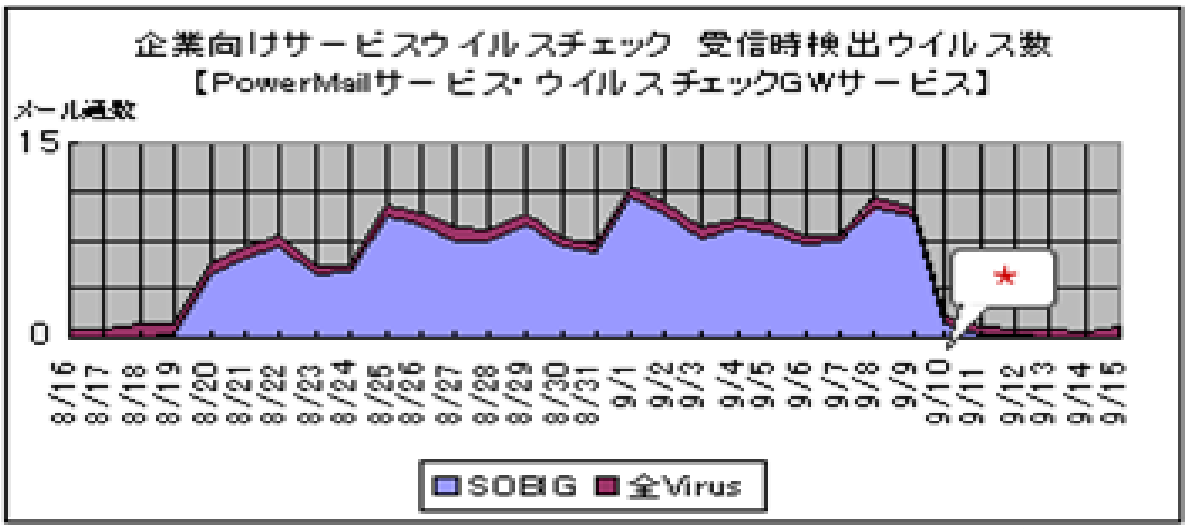
ソービッグＦは、約１．８メガバイトの容量をもつ巨大ワームで、世界中のホスト・コンピュータ２０台からプログラムをダウンロードし、第三者の指令で何らかの動作を行う仕様になっており、スパムメールやＤｏＳ攻撃の発射の基盤として活用されていた可能性がある。

ソービッグＦの蔓延とこれに対する Telecom-ISAC Japan の対応は、次のとおりである。

▽　ソービッグＦの蔓延と Telecom-ISAC Japan の対応

日時	内容
8/19	**ソービッグＦの出現** **欧米で感染が拡大との情報**
8/19 **夜**	**日本でも** AV **システムで急速な感染を確認**
8/20	**ＩＳＰによるユーザ周知（各社対応）**
8/22	**ソービッグＦの解析情報入手** **トロイの木馬機能の活性化が** 23 **日早朝にプログラムされているとの情報**
8/23	**緊急対応** **トロイの木馬がダウンロードするサーバ** IP **アドレス** 20 **を遮断** **（攻撃は不発のため後日対策解除）**

▽　ソービッグＦが添付されたメール通数の変化（ＯＣＮの事例）



※ 通常を１とした相対的なグラフ　　★ **Sobig-F**は**9/10**で終息

１．３．２　２００４年　～ＤｏＳ攻撃（Ａｎｔｉｎｎｙ）対応事例～

ＤｏＳ攻撃は、その対象となったユーザのほか、そのユーザと接続しているＩＳＰにとっても、ネットワークの安定運用上の大きな脅威となる。

現状では、ＩＳＰが、攻撃を受けているユーザからの要請に基づいて、攻撃パケットを遮断するパケットフィルタリング等の対策を実施する場合がある。

他方、ＤｏＳ攻撃から逃れるためにユーザが採った措置が、インターネット全体に負の影響を与えた例がある。

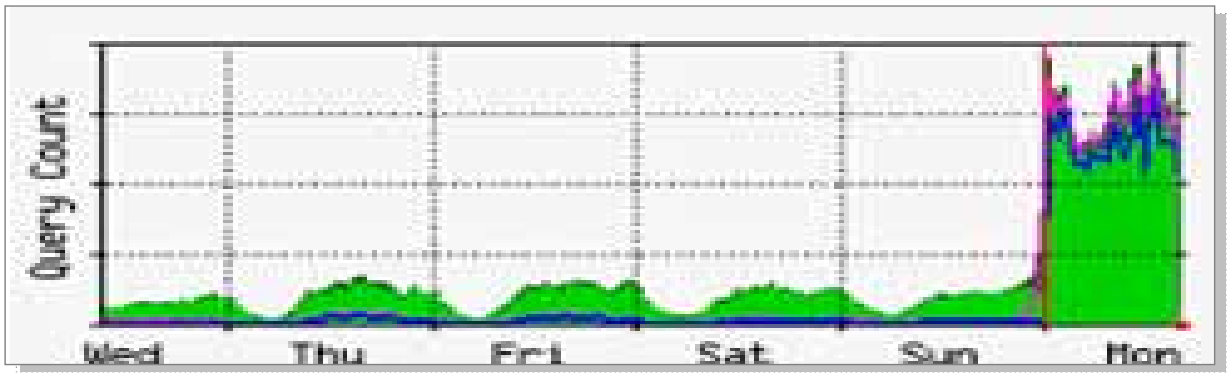
Ｐ２Ｐ（Peer to Peer**）型通信**[注9]**のアプリケーション・ソフトの１つであるＷｉｎｎｙが媒介し感染するＡｎｔｉｎｎｙ（アンチニー）と呼ばれるワーム型ウイルスがその事例である。**

（注９）Ｐ２Ｐ型通信とは、クライアント・サーバ型の通信とは異なり、ユーザ同士が直接１対１で行う対等型通信をいう。Ｗｉｎｎｙは、Ｐ２Ｐで行われるファイル転送アプリケーションであり、サーバを介在せず、一定の検索条件の下でユーザのコンピュータから他のユーザのコンピュータにファイルが転送され、共有される。

（１）　Ａｎｔｉｎｎｙの影響

２００４年４月５日、複数のＩＳＰが運用するＤＮＳ（Domain Name System）サーバの負荷が突然急上昇し、あるＩＳＰのＤＮＳサーバにおいては、名前解決要求（query）が平常時の６倍以上に跳ね上がる異常事態が発生した。

▽　ＯＣＮのＤＮＳサーバへのアクセスの急増



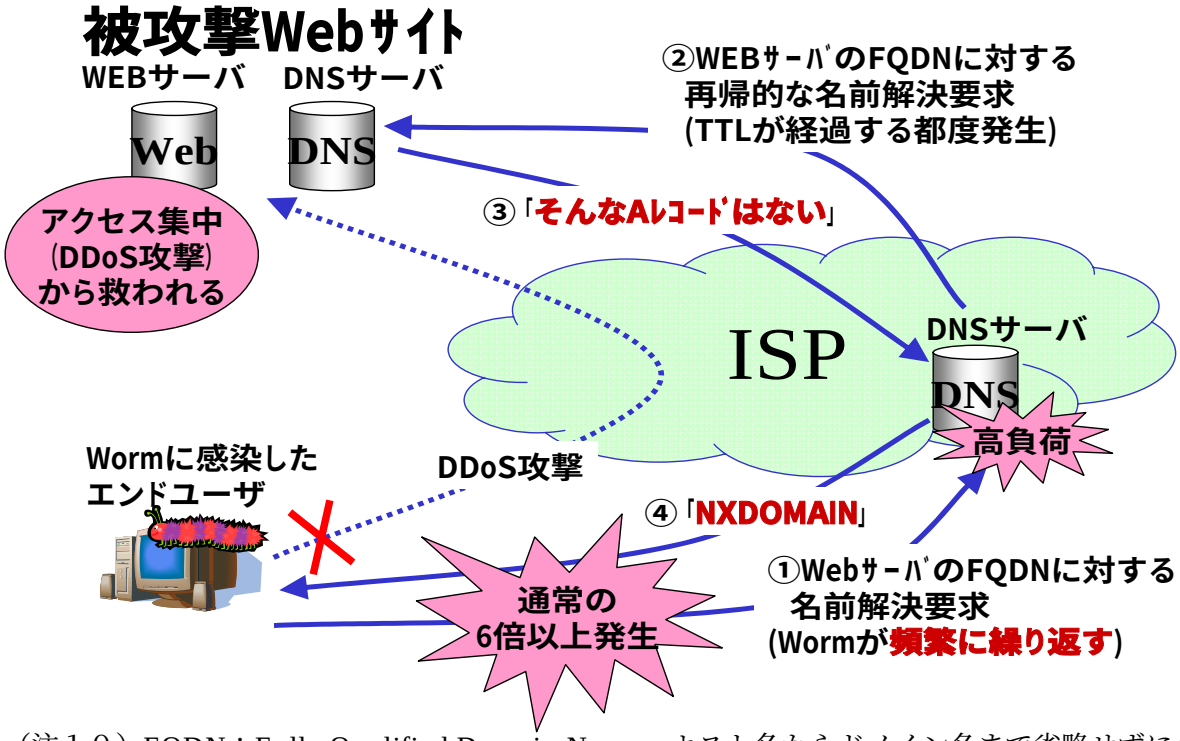
2004.4.5 Mon

これは、ＡｎｔｉｎｎｙによるＤｏＳ攻撃に対処するために、攻撃を受けているユーザ側で、Web サイトに係るＤＮＳの設定を変更したことに由来するものである。

Ａｎｔｉｎｎｙは、Ｗｉｎｎｙユーザに感染し、特定日に特定の Web サイトに個人情報をアップロードする機能を持ったワームであり、Telecom-ISAC Japan による観測や他の関係機関の情報から、アップロード先のＤＮＳの名前解決ができるまで、ＩＳＰのＤＮＳサーバに対し、無限に名前解決要求（query）を行うことが判明した。

攻撃を受けていたユーザ側では、攻撃が予想される時間に合わせて、当該 Web サイトの名前解決を行わないように自らのＤＮＳの設定を変更することで、ＤｏＳ攻撃の影響を受けないようにしたところ、ＡｎｔｉｎｎｙがＩＳＰのＤＳＮサーバに対し名前解決要求を繰り返したことから、複数のＩＳＰのＤＮＳサーバにおいて、Ａｎｔｉｎｎｙからの名前解決要求と、攻撃を受けているユーザ側のＤＮＳサーバからのエラー処理により、高負荷の状態に陥ったものである。

▽　ＤＮＳサーバに対し名前解決要求が大量に発生した背景



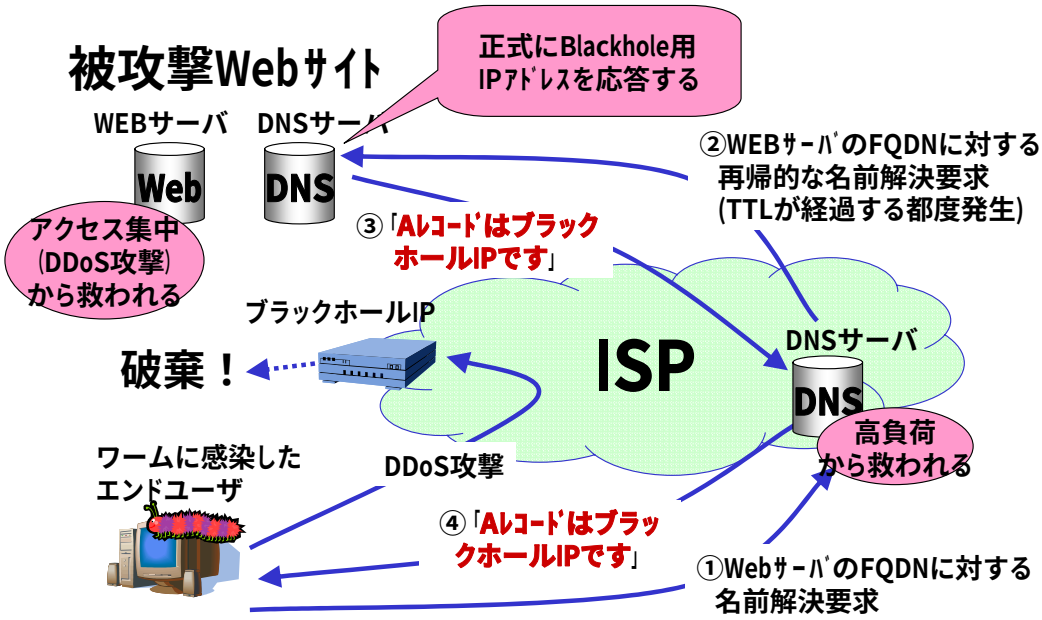
（注１０）FQDN：Fully Qualified Domain Name、ホスト名からドメイン名まで省略せずに全て表記すること。www.soumu.go.jp などを指す。

NXDOMAIN：存在しないドメインに対する問い合わせを行った際に設定されるレスポンスコードのひとつ。

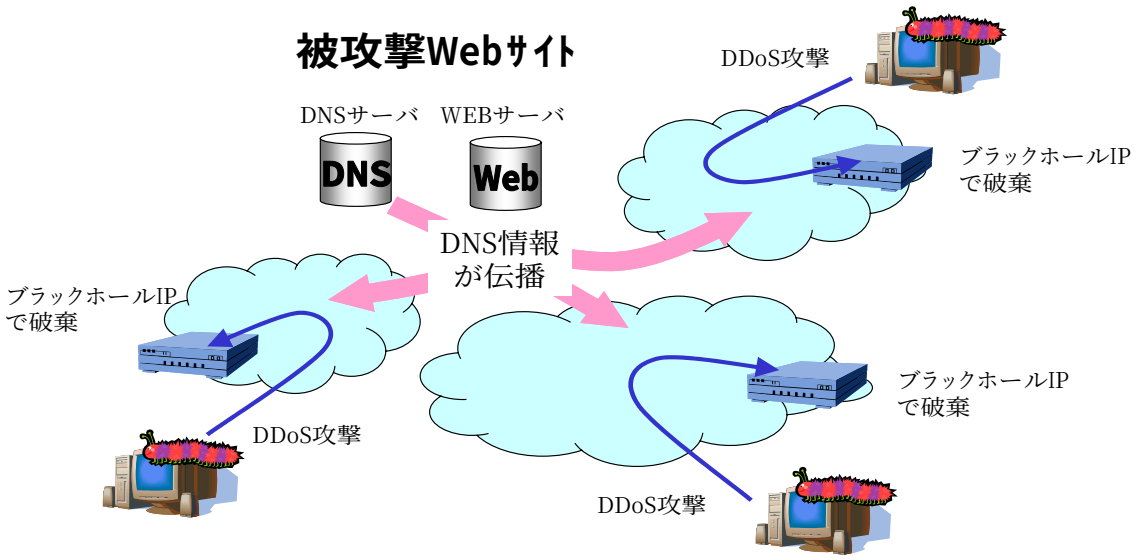
（２）　Ａｎｔｉｎｎｙへの対策

こうした事態に直面したＩＳＰでは、Telecom-ISAC Japan を通じて攻撃を受けているユーザ側と対策を協議し、ユーザ側のＤＮＳサーバが名前解決要求を受けた場合には、「おとり」のＩＰアドレス（ブラックホールＩＰアドレス）を返すように設定し、ブラックホールＩＰアドレスへの攻撃トラヒックを、複数のＩＳＰが共同で破棄するという対策を実施した。

▽　ブラックホールＩＰアドレスによる攻撃回避策



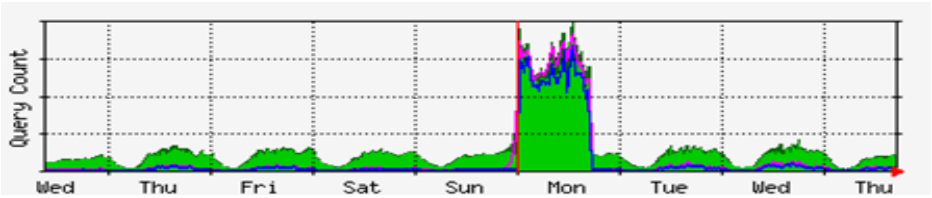
▽　攻撃トラヒックの破棄は複数のＩＳＰで設定



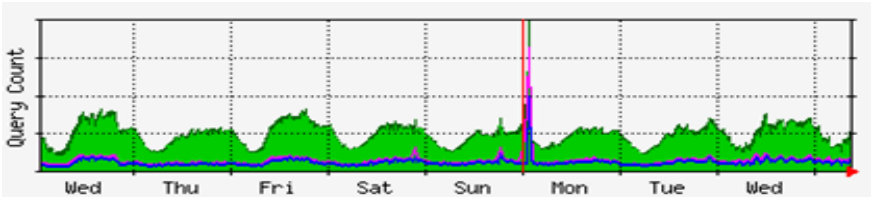
Telecom-ISAC Japanが中心となり大手ISPが連携

こうした対策の結果、ＤＮＳサーバは救われ、ブラックホールＩＰアドレス利用による攻撃トラヒックの破棄により、ネットワークも安定的に運用されるようになった。

▽　ブラックホールＩＰアドレス設定による攻撃回避策の効果



2004/04のあるDNSサーバの状況



2004/06のあるDNSサーバの状況

（3）　Ａｎｔｉｎｎｙの教訓

Ａｎｔｉｎｎｙへの対応は、ＤｏＳ攻撃対策の難しさを改めて示すものとなった。

すなわち、

①　攻撃を受けているユーザ側で行う対策は、インターネット全体への影響を十分に考慮すべきであり、そのためにＩＳＰ等と情報共有や対策協議が必要なこと、

②　ブラックホールＩＰによる攻撃回避策は、ＤｏＳ攻撃を受けないようにすることはできても、ＤＮＳの設定を変更している間は、攻撃の対象となっている Web サイトにはアクセスできないため、本質的な解決策にはならないこと、

といった課題が明らかになった。

その後、Telecom-ISAC Japan では、攻撃を受けているユーザ側の要請を受けて、ネットワーク環境を元に戻し、大容量の回線、大容量のデータの蓄積が可能なストレージ・サーバ、個人情報の含まれる通信を含む可能性を排除した Web サーバのコピー等で構成される観測システムを一時的に構築して、攻撃の予兆の分析を行っている。

しかし、このような観測システムは、費用面においても、個々のＩＳＰが永続的に運用できるものではない。

Ａｎｔｉｎｎｙへの対応は、ＤｏＳ攻撃対策の技術面、運用面、そして費用面での課題を同時に浮き彫りにしたものと言える。

１．３．３　これまでに得られた教訓 － インシデント情報の共有及び分析の重要性

上述のような対応を通じ、様々な課題は残っているものの、インシデント情報の共有及び分析の重要性が改めて認識された。

インシデントへの対応は、ＩＳＰ１社だけでは限界がある。

脆弱性情報の影響度合いの分析、セキュリティパッチの有効性の確認、Exploit Code に関する情報収集、ワームの挙動分析、特定のホスト・コンピュータとの通信の遮断等において、複数のＩＳＰが相互に連携して対応しなければ、奏功しない場合が多いのが実情である。

この点に関して、Telecom-ISAC Japan では、

①　システムの脆弱性に関する報告及び情報交換、

②　対抗策及びそのベストプラクティスの提供、

③　インシデントの脅威及び被害情報の提供、

を行っているほか、２００４年度からは、独立行政法人「情報通信研究機構」（NiCT）とも連携して「広域モニタリングシステム」を構築し、

④　国内の主要ＩＳＰから、トラヒック情報やセキュリティ関連のログ情報を収集して、ネットワーク全体の傾向を把握するとともに、

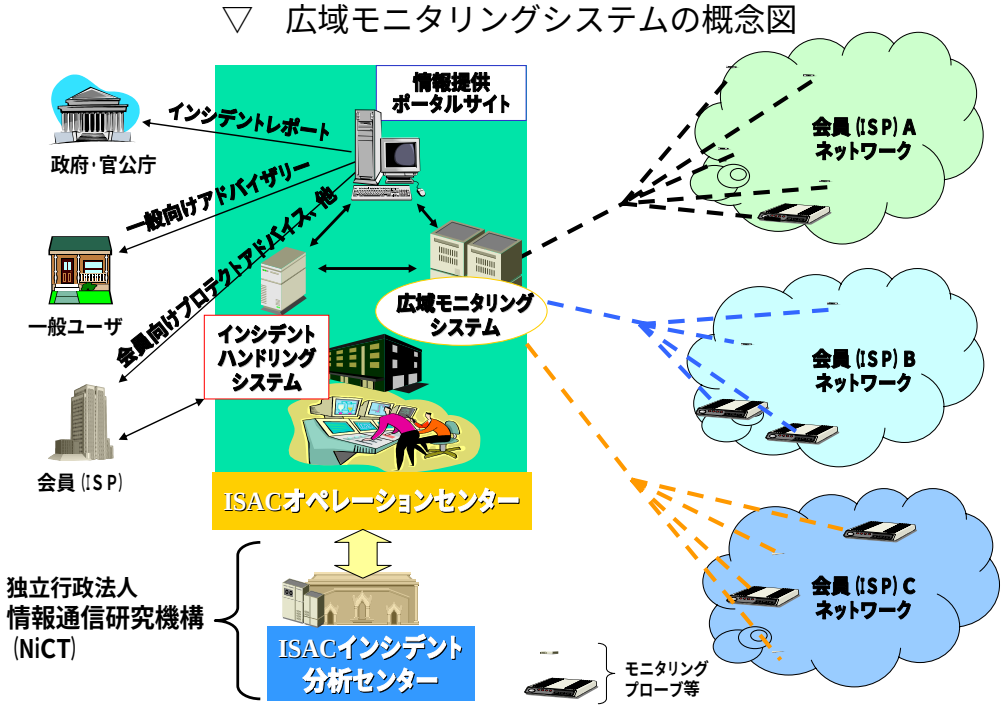
⑤　収集された情報からトラヒックの異常を観測し、

⑥　不正アクセス、ウイルス、ワーム等の挙動を分析し、

⑦　インシデントの予兆がある場合にはＩＳＰに連絡して警戒強化を促す、

等といった対応を始めており、今後とも、こうした活動を継続・強化していくことが必要である。

▽　広域モニタリングシステムの概念図



実際に、今後、広域モニタリングを継続・強化していくに当たっては、

① ブロードバンド環境で伝送される大容量のデータを、どうすれば技術的に解析できるのか、

② 「通信の秘密」の保護や個人情報保護法に抵触しないよう、トラヒック情報やログ情報をどの程度、またどのように仮装（masking）し、抽象化して把握すべきか、

等の技術上又は制度上の課題を克服することが必要である。

こうした課題については、民間事業者だけでは克服し得ないものであり、Telecom-ISAC Japan 等の関係機関に政府もオブザーバとして参加する形で取り組んでいくことが適当と考えられる。

また、これまでのインシデントから得られた分析結果と実際にとった措置の効果について、Telecom-ISAC Japan と政府とが連携して整理しておくことは、今後、類似のインシデントが発生した場合に迅速な対応措置をとる上で極めて有効と考えられる。