

次世代 I P インフラ研究会
第二次報告書（案）

「情報セキュリティ政策2005」の提言

2005年6月30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	・・・ 1
第1章	インシデント対応の現状と課題	・・・ 5
1. 1	ICT障害	・・・ 7
1. 2	インシデントの最近の傾向	・・・ 8
1. 3	インシデントに対するISPの対応事例	・・・ 11
1. 3. 1	2003年～ネットワーク感染型ワームへの対応～	・・・ 11
(1)	2003年に発生した主なワーム	・・・ 11
(2)	ワームの蔓延パターンと一般的な対策	・・・ 12
(3)	ISPにおける対応事例	・・・ 13
1)	ブラスターへの対応事例	・・・ 13
2)	ソービッグFへの対応事例	・・・ 14
1. 3. 2	2004年～DoS攻撃(Antinny)対応事例～	・・・ 15
(1)	Antinnyの影響	・・・ 16
(2)	Antinnyへの対策	・・・ 17
(3)	Antinnyの教訓	・・・ 18
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	・・・ 19
1. 4	2004年～ボットネット対策の黎明期～	・・・ 21
1. 4. 1	ボットの特徴	・・・ 22
(1)	他者を攻撃し得る機能	・・・ 22
(2)	スパイウェア機能	・・・ 23
(3)	第三者からの指揮命令に従った活動	・・・ 23
(4)	ネットワーク化	・・・ 23
(5)	変態機能(ダウンロード機能、インストーラ機能)	・・・ 23
(6)	無自覚症状	・・・ 24
(7)	「静かな感染」活動	・・・ 24
1. 4. 2	ボットネットがもたらす脅威	・・・ 25
(1)	スパムメール等の送信・中継	・・・ 25
(2)	フィッシング(Phishing)詐欺	・・・ 26
(3)	DoS攻撃	・・・ 27
(4)	スパイウェア機能	・・・ 28
(5)	他のボットプログラムやウイルス等の拡散	・・・ 28
1. 4. 3	ボットプログラムの蔓延の背景	・・・ 28
1. 4. 4	ボットネット対策の現状	・・・ 29

1. 4. 5	今後の課題	・・・ 30
(1)	技術上の課題	・・・ 30
1)	感染防止と早期駆除	・・・ 30
①	検体収集	・・・ 30
②	ボットネットの行動特性の把握	・・・ 31
2)	攻撃の予防と防御	・・・ 31
①	テストベットにおける実証結果を踏まえた広域モニタリング（定点観測）	・・・ 31
②	攻撃元となっているボット（ボットネット）の把握	・・・ 32
③	攻撃のフィルタリング	・・・ 32
(2)	制度上の課題	・・・ 33
(3)	体制上の課題	・・・ 33
1)	感染防止と早期駆除	・・・ 33
2)	攻撃防御・予防	・・・ 34
(4)	ユーザへの啓発	・・・ 34
1. 5	ソーシャルエンジニアリングへの対処	・・・ 36
1. 6	経路情報の誤りによる I C T 障害	・・・ 38
1. 6. 1	経路数の拡大	・・・ 38
1. 6. 2	経路情報の誤りによる I C T 障害	・・・ 38
1. 6. 3	経路情報の誤りによる I C T 障害への対応策	・・・ 39

第2章	ユビキタスネット社会におけるセキュリティ確保	・・・41
2. 1	ユビキタスネット社会におけるセキュリティ確保の必要性	・・・43
2. 2	情報家電に対する期待と課題	・・・45
2. 3	情報家電のネットワーク接続に伴うセキュリティ上の課題	・・・49
2. 3. 1	接続検証と規格化	・・・49
2. 3. 2	情報家電がボット化した場合の対応	・・・49
2. 3. 3	リモートメンテナンスと機器認証	・・・50
2. 3. 4	情報家電を破棄・転売した場合の課題	・・・52
(1)	サービス利用者と課金対象者が異なる可能性	・・・52
(2)	個人情報保護	・・・52
2. 4	家電業界とISP業界との情報交換・情報共有の必要性	・・・53

第3章	電気通信事業における情報セキュリティマネジメント	・・・55
3. 1	電気通信事業における情報セキュリティマネジメントの必要性	・・・57
3. 2	ISMSの概要と最近の改訂作業の動向	・・・59
3. 2. 1	ISMSの概要	・・・59
3. 2. 2	ISMS適合性評価	・・・60
3. 2. 3	ISMSの改訂作業の動向	・・・62
3. 2. 4	ISMSの今後の課題	・・・63
(1)	産業分野別のISMSの策定	・・・63
(2)	ISMSの確立・運用に対する支援	・・・63
(3)	国際的なクロスボーダー認証の実現	・・・64
3. 3	ISMS-Tの概要と今後の改訂の方向性	・・・65
3. 3. 1	ISMS-Tの概要	・・・65
3. 3. 2	ISMS-Tの今後の改訂の方向性	・・・66
(1)	改訂ISMSを参照する必要性	・・・66
(2)	現行ISMS-Tへの追加項目の検討	・・・66
3. 4	我が国における今後の活動の方向性	・・・68
3. 4. 1	ISMS-Tの国内における展開	・・・68
3. 4. 2	国内における普及促進	・・・68
3. 4. 3	国際貢献	・・・68

第4章	セキュリティ人材育成	・・・71
4. 1	我が国におけるセキュリティ人材の現状	・・・73
4. 1. 1	労働市場における情報処理技術者の「供給」面	・・・73
4. 1. 2	労働市場における情報処理技術者の「需要」面	・・・74
4. 1. 3	我が国電気通信事業者におけるセキュリティ人材の現状	・・・75
(1)	セキュリティ人材の充足感	・・・76
(2)	セキュリティ人材育成の現状	・・・76
4. 2	他のICT先進国におけるセキュリティ人材の現状と育成策	・・・79
4. 2. 1	米国におけるICT人材数	・・・79
4. 2. 2	米国におけるセキュリティ人材の育成策	・・・79
4. 2. 3	シンガポールにおけるセキュリティ人材の育成策	・・・80
4. 3	我が国におけるセキュリティ人材育成	・・・81
4. 3. 1	セキュリティ人材に関する我が国電気通信事業者の要望	・・・81
4. 3. 2	既存のセキュリティ講習等に対する評価の基準	・・・82
(1)	資格や認定の効果が有効期限付きのものか	・・・82
(2)	実機を使った演習があるか	・・・82
(3)	技術だけでなく、管理・運用、法制度についても講習があるか	・・・83
4. 3. 3	既存のセキュリティ講習等の例－NISM	・・・83
4. 3. 4	大学におけるセキュリティ人材教育	・・・85
4. 4	事業者をまたがる総合的な演習の必要性	・・・86

第5章 総括	．．． 89
5. 1 今後、集中的に取り組むべき3つの課題	．．． 91
(1) ICT障害の広域化への対応	．．． 91
(2) ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）	91
(3) 人材面の脆弱性の克服	．．． 91
5. 2 「情報セキュリティ政策2005」の提言	．．． 93
(1) ICT障害の広域化への対応	．．． 93
1) 広域モニタリングシステムの構築・強化	．．． 93
2) ボットネット対策に関する研究開発	．．． 93
3) 経路情報の誤りによるICT障害の検知・回復・予防に関する研究開発	．．． 94
(2) ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）	94
1) 接続検証と規格化	．．． 94
2) 機器認証	．．． 94
3) インターネット全体に与える負荷軽減（情報家電がボット化した場合の対応）	．．． 94
4) 業界をまたがる障害対応の迅速化	．．． 95
(3) 人材面の脆弱性の克服	．．． 95
1) 一般ユーザへの啓発	．．． 95
2) ソーシャルエンジニアリングの研究と対応策の提示	．．． 96
3) ISMS-Tの国内における普及促進と国際貢献	．．． 96
4) 事業者をまたがる総合的な演習の必要性	．．． 96
用語集	．．． 99
参考資料	．．． 109
1. 次世代IPインフラ研究会 構成員	．．． 111
2. セキュリティWG 構成員	．．． 112

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、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も広域化・多様化が進んでおり、こうした障害事案に対し、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様々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ません。

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

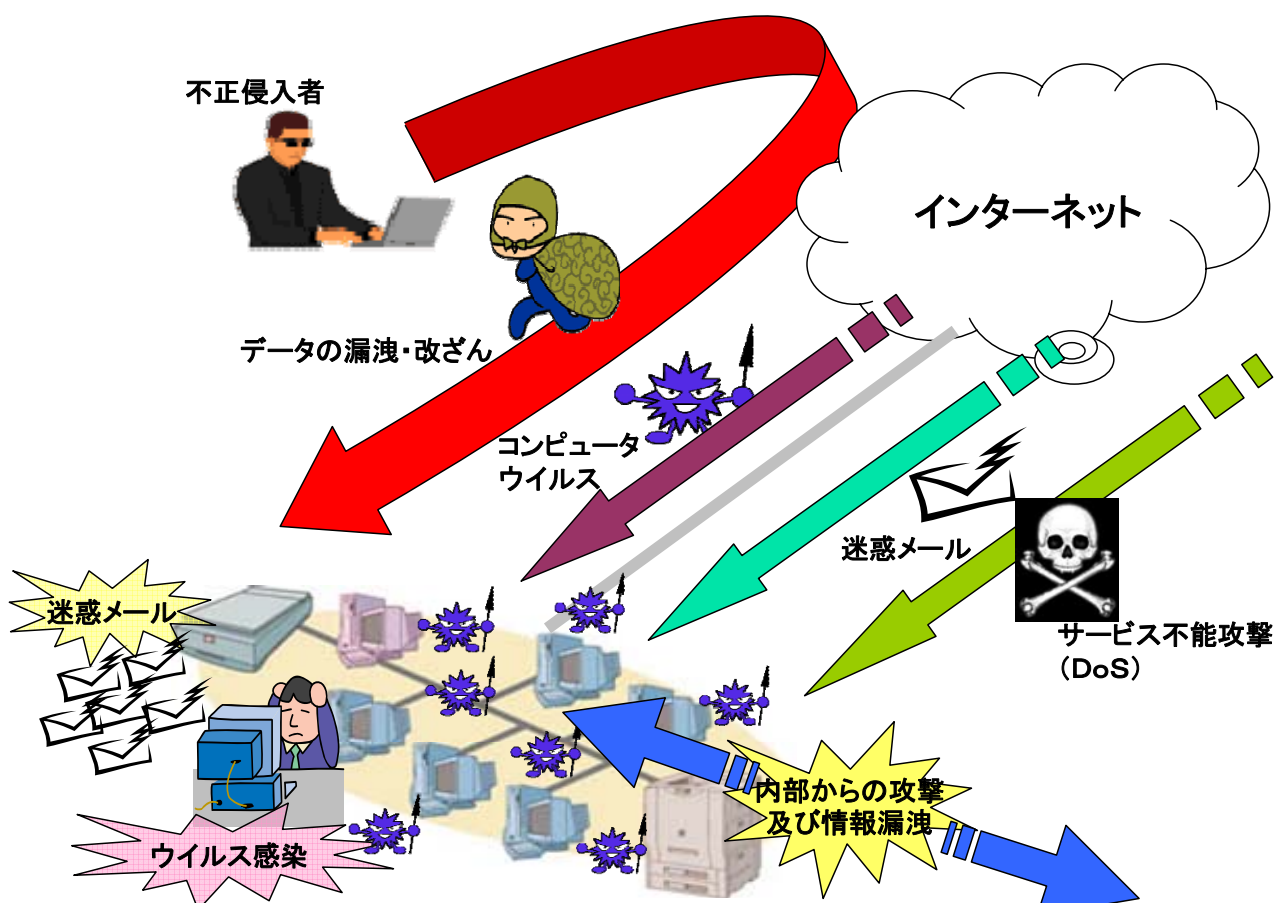
情報通信技術（ICT）の機能不全による障害（以下「ICT障害」という。）については、

- 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。

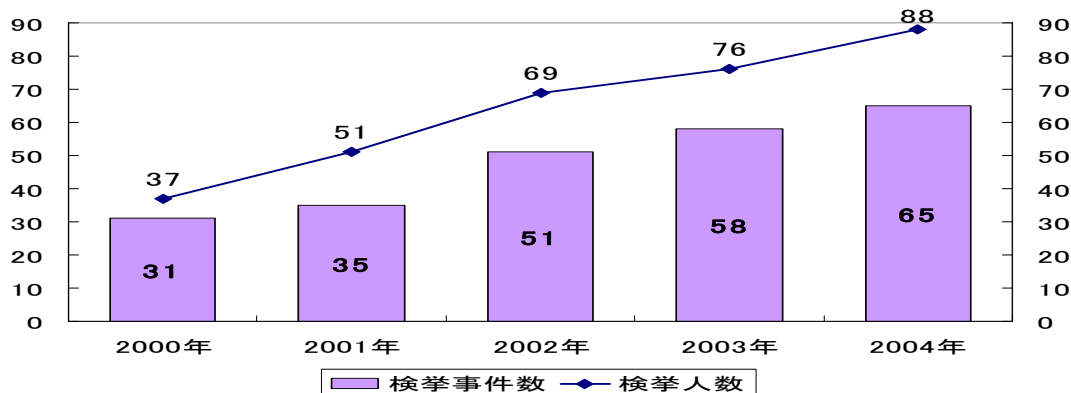
▽ インシデントのイメージ図



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



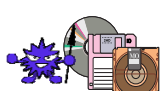

国家公安委員会、総務大臣、経済産業大臣
「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」より作成

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。

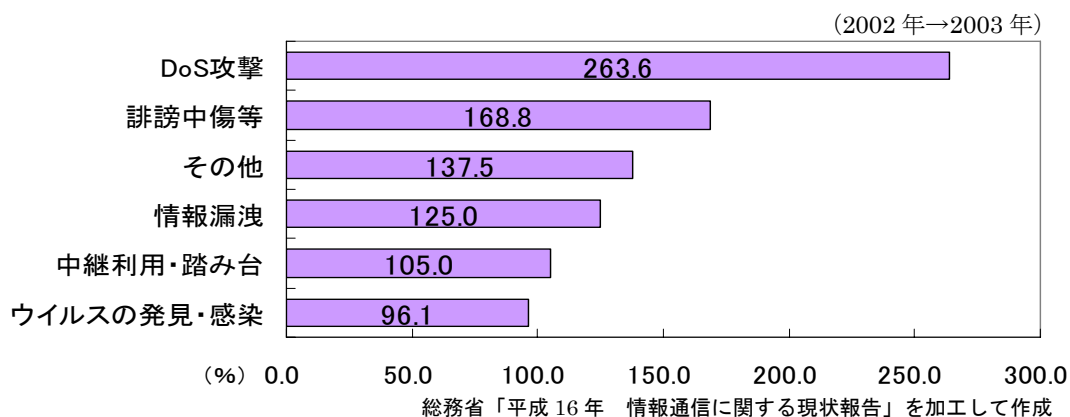
(注2) ワーム (worm) とは、他の電子ファイルに寄生せず、ネットワークを介して自分自身をコピーして単体で自己増殖を繰り返しながら、感染を拡大していくプログラムをいう。ただし、最近では、厳密にはワームであるものも含め、広義の「ウイルス」と呼ぶことがある。

▽ ウイルス/ワームの悪質化

	感染方法	対策
昔	媒体(フロッピー等)により感染 	①ウイルス対策ソフトによる検知・駆除 ②不審なフロッピーを使わない
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

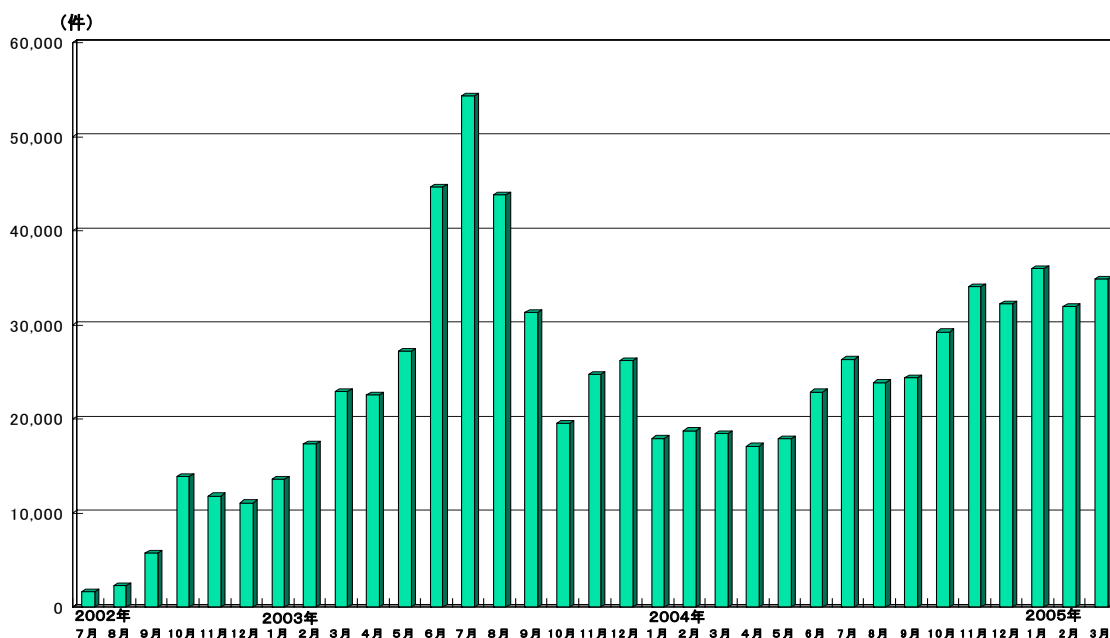
また、電子商取引等のサービスを提供しているWebサイトに対して、その処理能力を超える多量のデータを送信したり、バグ(ソフトウェアの不具合)を突くことなどにより、サービス提供機能を停止させる「サービス不能化(DoS; Denial of Service)攻撃」による被害が、2002年から2003年にかけて、最も増加している状況にある。

▽ 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



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。

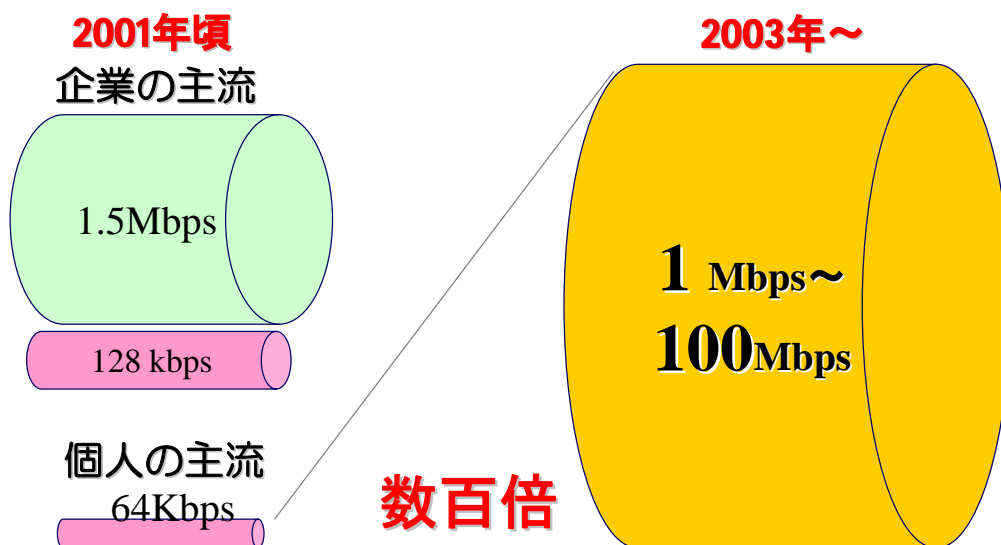
ダイヤルアップ接続等ナローバンド（狭帯域網）によるインターネット接続が主流であった2001年までは、ユーザの端末機器がウイルスやワームに感染したとしても、ネットワークが被害を受けることは少なかった。

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フィックを発生させ、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、キロビット毎秒クラスで、従量課金によりインターネットに接続していた2001年以前の多くのユーザに比べ、メガビット毎秒クラスで、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、トラフィ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。

このため、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とともに、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。

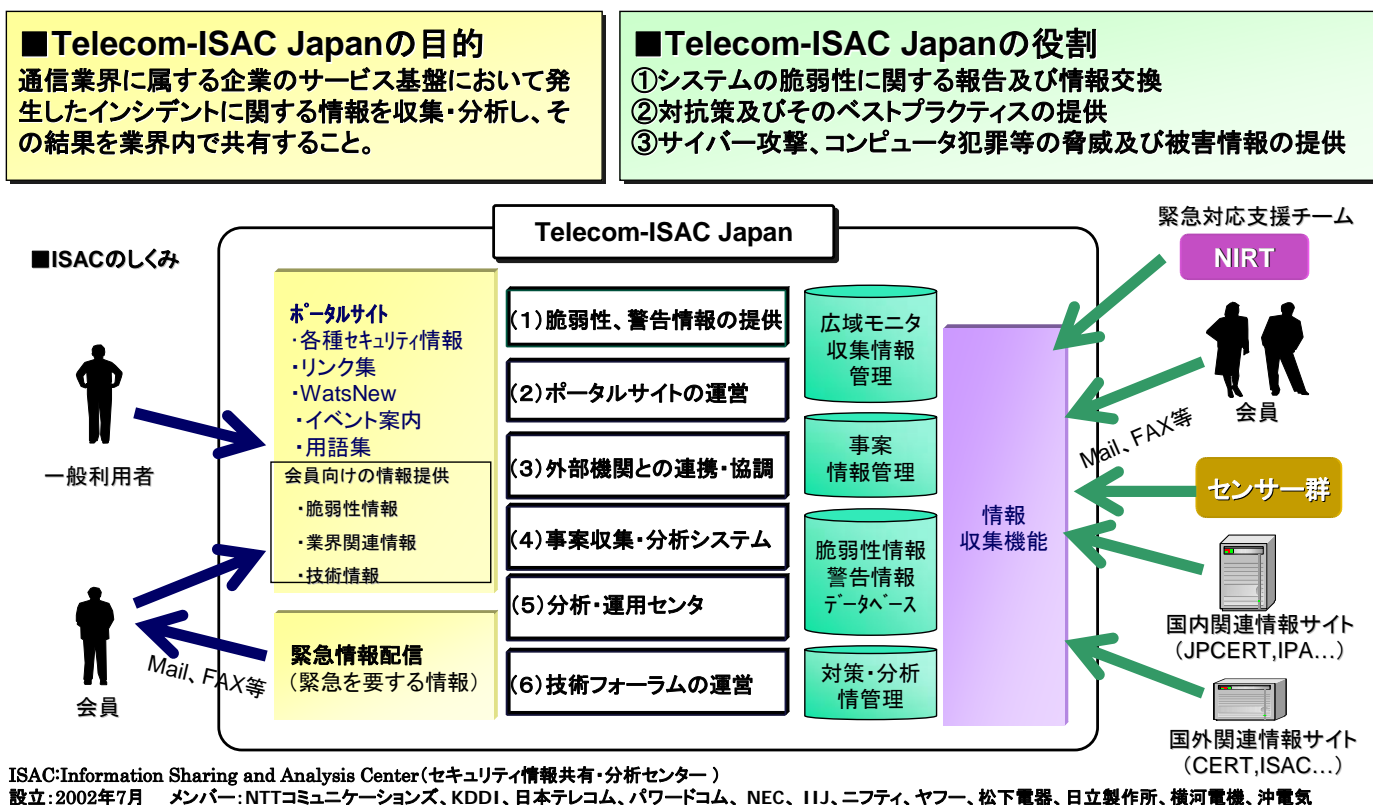
現に、後述するブラスター騒動では、検証期間中に感染して被害を受けた事例が我が国においても存在する。

(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 電気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。

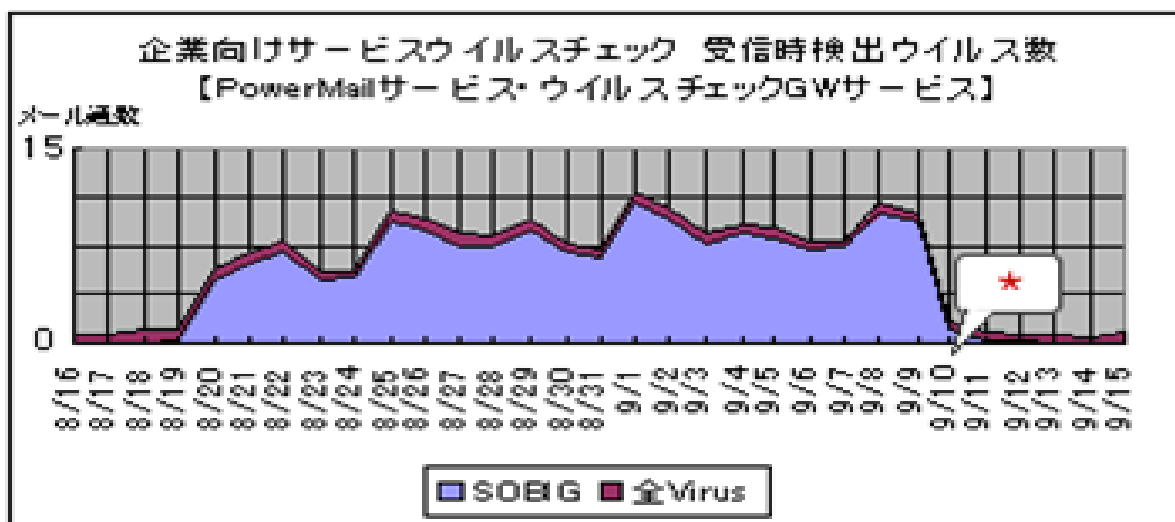
ソービッグFは、約1.8メガバイトの容量をもつ巨大ワームで、世界中のホストコンピュータ20万台からプログラムをダウンロードし、第三者の指令で何らかの動作を行う仕様になっており、スパムメールやDOS攻撃の発射の基盤として活用されていた可能性がある。

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	I S P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）



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。

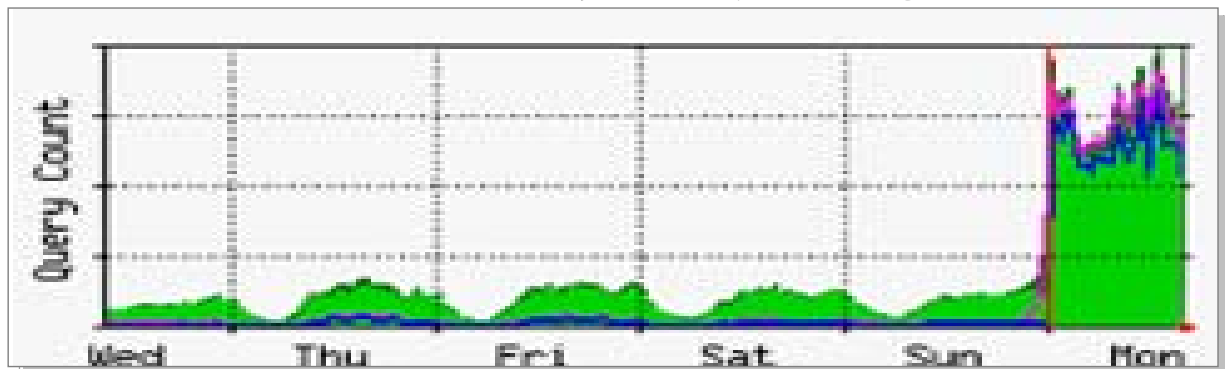
P2P (Peer to Peer) 型通信^(注9)のアプリケーションソフトの1つであるWinnyが媒介し感染するAntinny (アンチニー) と呼ばれるワーム型ウイルスがその事例である。

(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



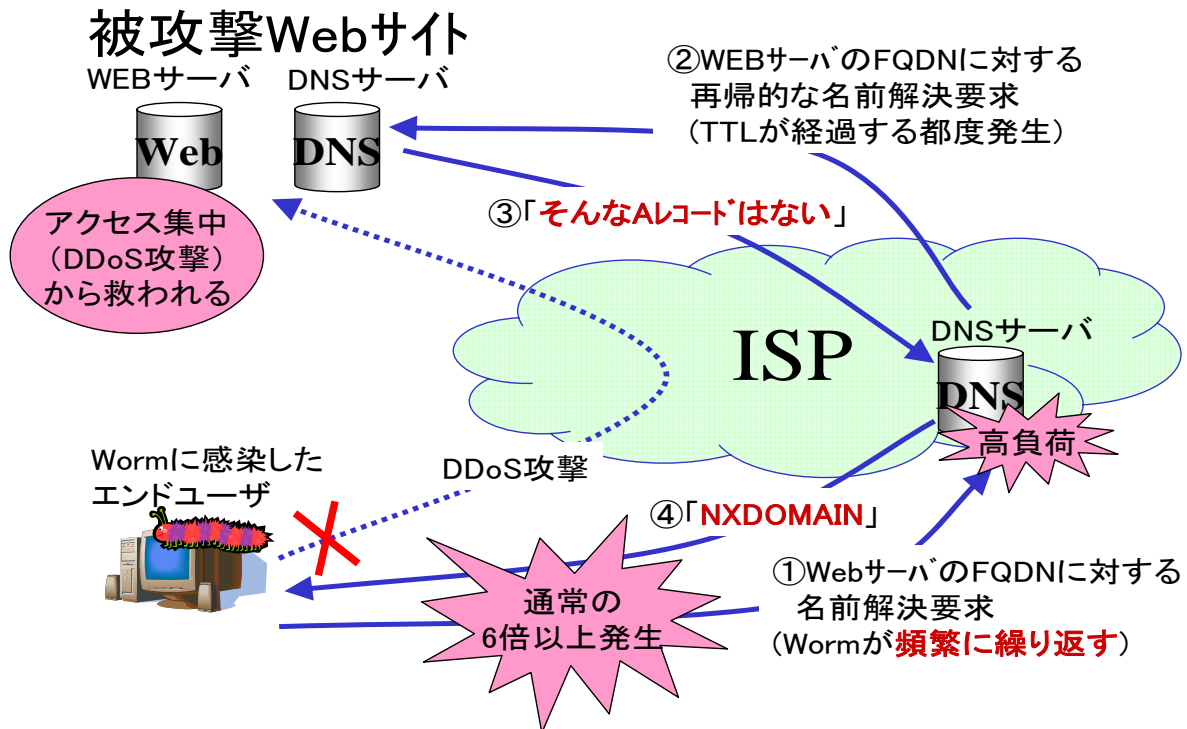
2004.4.5 Mon

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DNS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



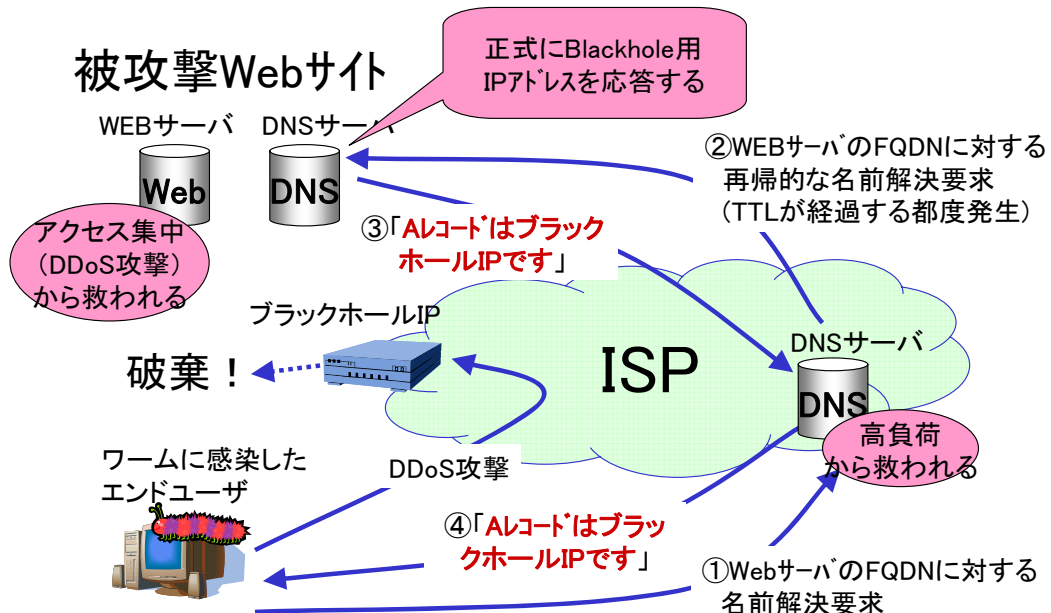
(注10) FQDN : Fully Qualified Domain Name、ホスト名からドメイン名まで省略せずに全て表記すること。www.soumu.go.jpなどを指す。

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。

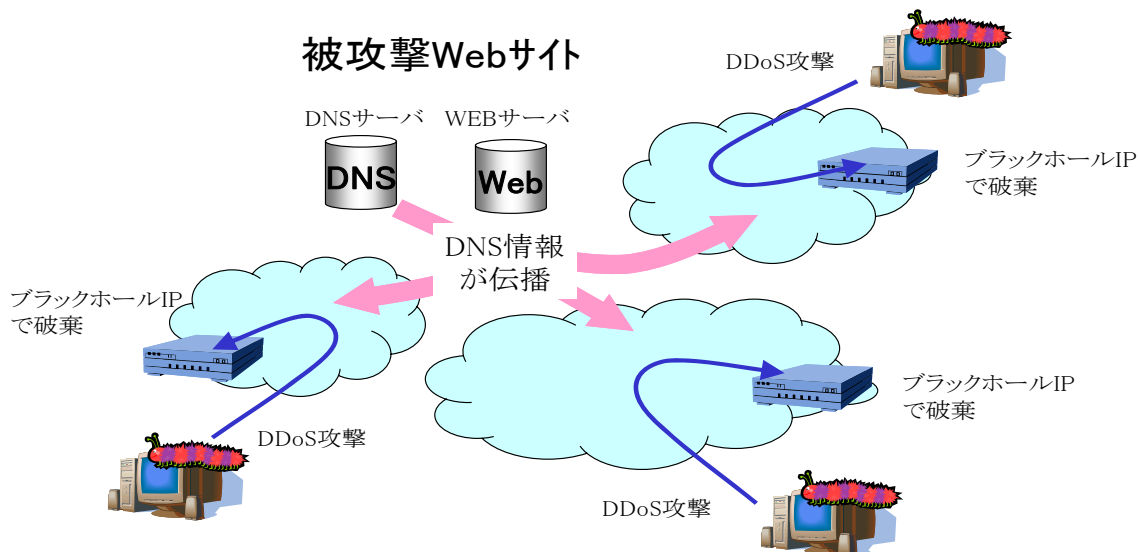
(2) Antinnyへの対策

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フィックを、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



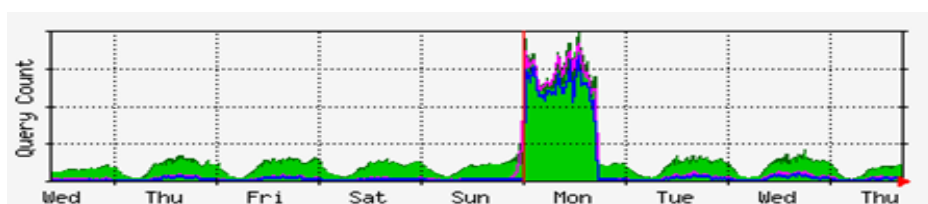
▽ 攻撃トラヒックの破棄は複数のISPで設定



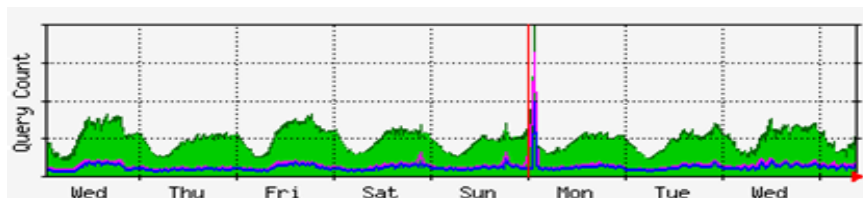
Telecom-ISAC Japanが中心となり大手ISPが連携

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 I S P が永続的に運用できるものではない。

A n t i n n y への対応は、D o S 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、I S P 1 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 I S P 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、

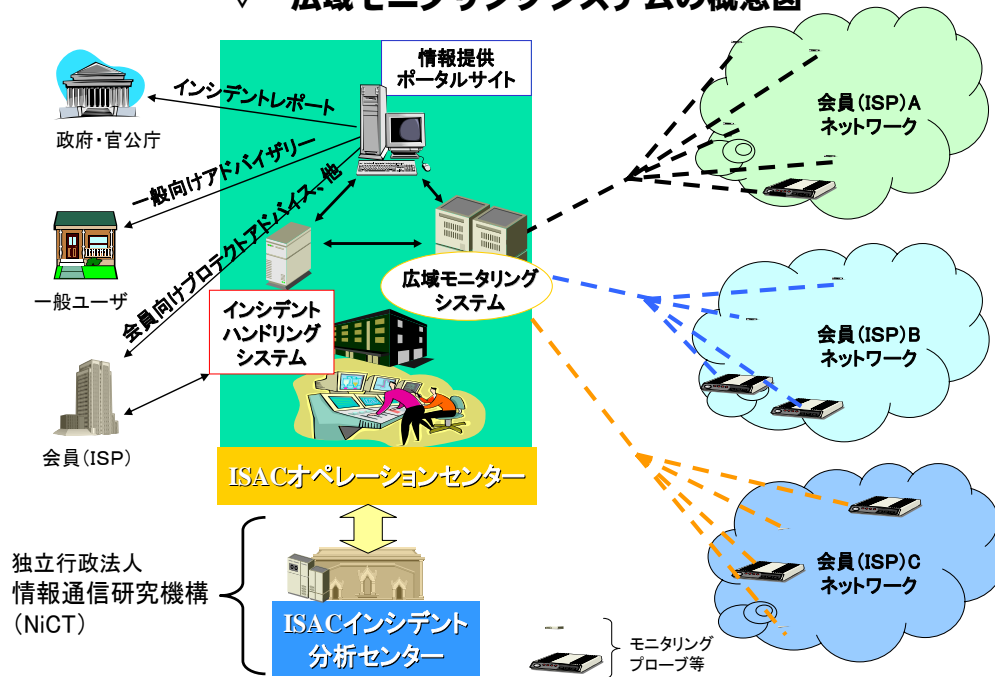
- ① システムの脆弱性に関する報告及び情報交換、
- ② 対抗策及びそのベストプラクティスの提供、
- ③ インシデントの脅威及び被害情報の提供、

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 I S P から、トラフィ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フィ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 I S P 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、トラフィ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 等の関係機関に行政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 と行政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。

1.4 2004年 ～ボットネット対策の黎明期～

2004年は、ボットネットの存在が認知された年であった。

「ボット」^(注11)とは、悪意のある攻撃者（管理者）の指揮命令下に置かれたコンピュータのことである。

ネットワーク経由の遠隔操作により、コンピュータを攻撃等のために悪用することを可能とするプログラムを「ボットプログラム」といい、ボットプログラムに感染したコンピュータがボットである。

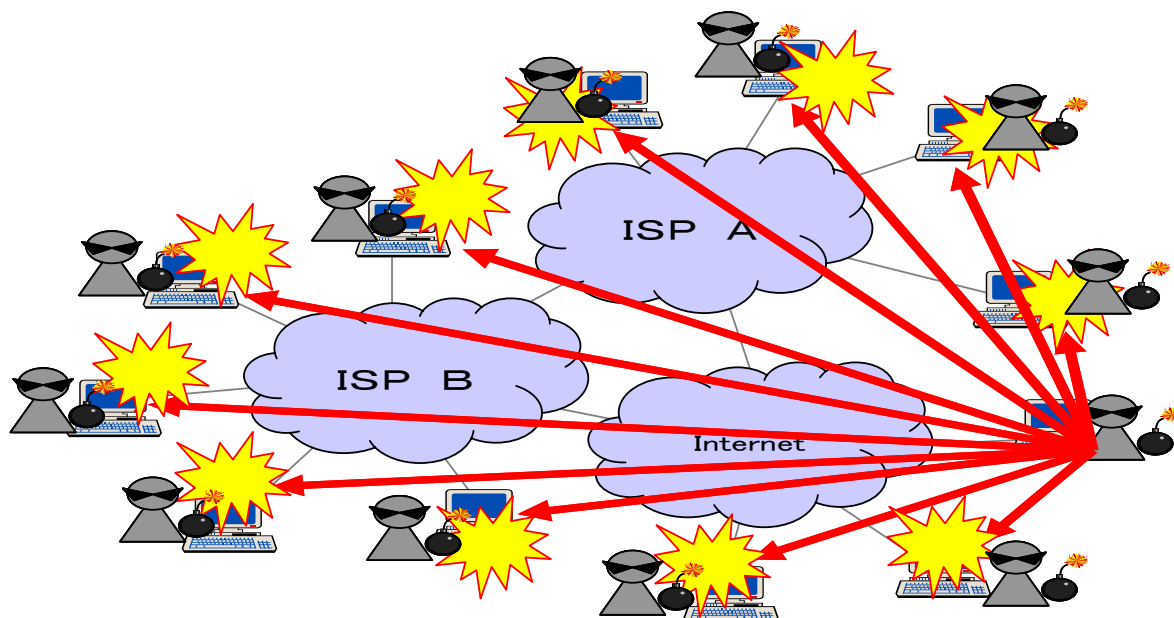
また、同一のボットプログラムの指揮命令下にあるコンピュータ群を「ボットネット」という。

(注11) ボットに類似の言葉として「ゾンビ」があるが、これはボットよりも広い概念で、ボット以外にも、攻撃者の指令を受けるのではなく、事前に一定の動作をするように仕組まれたウイルスに感染したコンピュータや、人手を掛けて乗っ取られたコンピュータが含まれる。

例えば、2003年8月に大流行したブラスターや、2004年2月から現在に至るまで拡散しているネッスカイ及びその亜種のように、決められた時間に特定のサイトをDoS攻撃する機能がプログラムされたワームに感染したコンピュータはゾンビである。

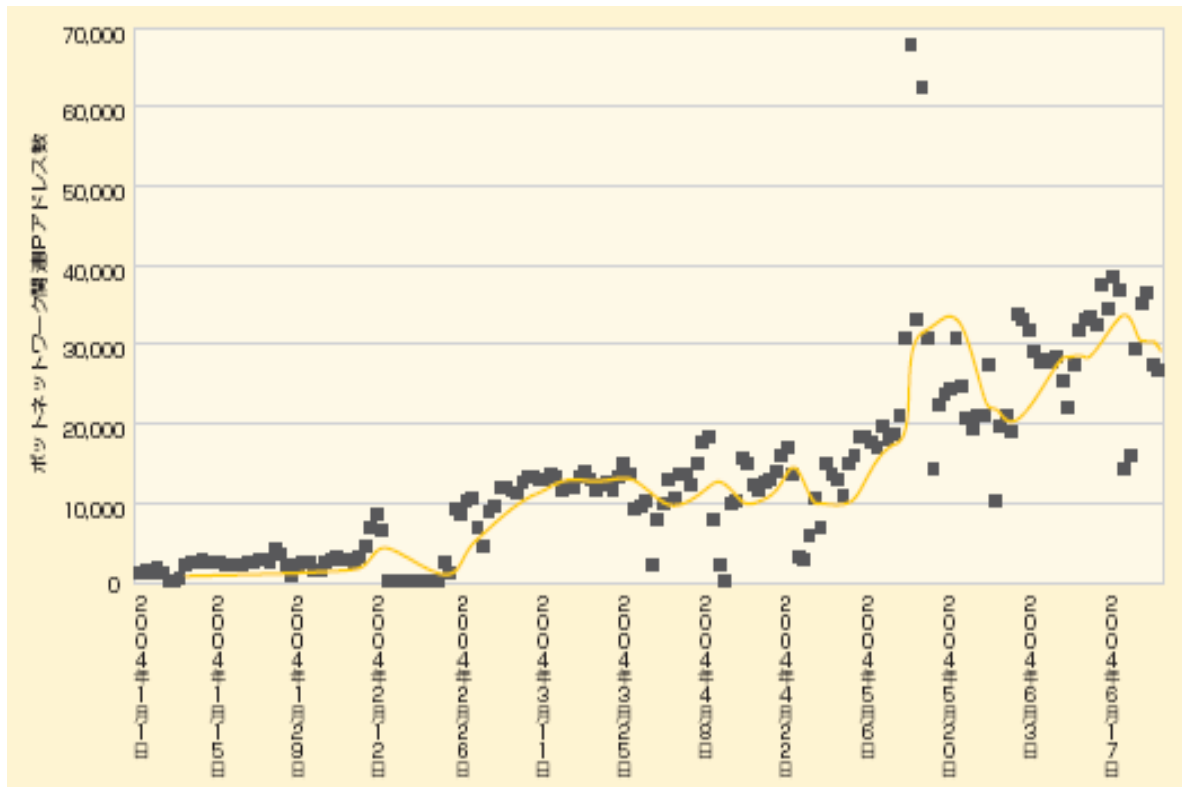
また、一斉に同一の攻撃を行うゾンビの一群をゾンビクラスターと呼ぶ。ボットネットは、ゾンビクラスター的一种である。

▽ ボットネットのイメージ図



シマンテックの調査によれば、2004年1月から同年6月の間で特定されたボットの数は2,000台から30,000台以上へと大幅に増加したことが確認されている。

▽ 一日当たりのボット数の推移



2004年9月シマンテック「インターネット脅威レポート」より

ボットには、スパムメール送信やD・S攻撃、フィッシング、スパイウェアといった攻撃機能が組み込まれており、攻撃者はボットネットに属するボットを制御することができる。

ボットプログラムは、脆弱なコンピュータが感染しやすいという点ではウイルスと同様の側面を持っているが、感染による自覚症状がなく、一旦感染すると変態を繰り返す等、ウイルスには見られないボット特有の性質も持ち合わせていることから、従来のウイルス対策とは異なる対策が必要である。

1.4.1 ボットの特徴

現在確認されているボットの主な特徴は次の通りである。

(1) 他者を攻撃しうる機能

ボットは、スパムメール等を送信／中継するメールサーバ機能、フィッシングや各種ダウンロードに利用するWebサーバ機能やFTPサーバ機能、及び各種D・S攻撃機能等、他者を攻撃するのに使用する機能の1つ又は複数を持つ。

(2) スパイウェア機能

ボットは、自らのコンピュータ内の個人情報等を攻撃者に送信する機能を有する。

(3) 第三者からの指揮命令に従った活動

攻撃者との通信については独自のプロトコルを持っているものもあるが、一般的にはテキストベースのチャットシステムである I R C (Internet Relay Chat) が利用されている場合が多い。

I R Cはサーバを介してクライアント同士が対話をするチャットシステムで、I R Cサーバはチャンネルと呼ばれるグループを管理しており、同一のチャンネルに属するクライアント同士がチャットを行う。

I R Cを利用するボットの場合、攻撃用に開設されたチャンネルには、I R Cクライアントであるボット及び攻撃者が属している。

攻撃者はこのチャンネルを介してボットにテキスト形式のコマンド（指令）を送出し、ボットはそのコマンドを解釈して行動する。

(4) ネットワーク化

ボットは、それ自身（元々のボットプログラム）の種類や持ち合わせている攻撃機能等に応じて、他のコンピュータとともに群を成し、同一の指揮命令系統に入っている（ボットネット）。

I R Cを利用している場合、同一のチャンネルに属している攻撃者以外の I R Cクライアント（ボット）が、一つのボットネットを成している。

攻撃者は、ボットネットに属しているボットに対して攻撃指令を出すことで、統制の取れた攻撃を行うことができる。また、ボットのネットワーク化は、攻撃の発信元を分散させる効果がある。

これにより、攻撃時に1台のボット（攻撃元）にかかる負荷を軽減するとともに、ボットの近隣のネットワーク環境におけるトラヒックを通常の誤差範囲内に抑えることができ、攻撃の発信元の把握を困難にすることができる。

(5) 変態機能（ダウンロード機能、インストーラ機能）

ボットは、任意の Web サイトからファイルをダウンロードし、インストールする機能を有する。

この機能により、コンピュータが一旦ボットプログラムに感染すると、別のボットプログラムをもインストールしてしまい、当初のボットとは全く異なるボットに変わり、また、複数のボット機能を併せ持つ場合がある。

(6) 無自覚症状

ウイルスと異なり、システムの破壊等ユーザにすぐそれと分かるような活動を行わない上、1台のボットにかかる負荷が小さいこと(上記(4))から、ユーザは自身のコンピュータがボットプログラムに感染したことについて自覚症状がない場合が多い。

(7) 「静かな感染」活動

変態機能(上記(5))により、手動か自動的に関わらず他のボットプログラムをダウンロードしてインストールすることにより感染するほか、ファイル共有機能やP2Pファイル交換ソフト、又は、ウイルス等が開いたバックドア^(注12)を介して感染する。

(注12) バックドアとは、通常のネットワーク経路とは異なる場所に設けられたアクセスの受け口のことをいう。

一般的には、大量メール送信型ウイルスのような派手な感染活動は行わない。

上記の特徴のうち、特に(5)～(7)は、ボット対策を困難にしている特徴と言える。

セキュリティベンダは、通常、ユーザからのウイルス感染報告や検体提供を受け、又は自らが設置した「おとり」となる機器(通称「ハニーポット」)に侵入したウイルスを検体として、当該ウイルスを分析し、ウイルスの特徴等を記述した定義ファイルを作成・公表する。

ユーザは、その定義ファイルをダウンロードしてウイルス対策ソフトに反映する訳である。

ボットについても、仮に検体が収集できればウイルスと同様の措置が可能であるが、ユーザが感染に気づかず(上記(6))、また感染活動が静か(上記(7))であることから、そもそも検体の収集がままならないのが実情である。

セキュリティベンダが「ハニーポット」等の機器を拡充して、自らの検体収集能力を増強することも考えられるが、機器の調達・運用コストが嵩むことに加え、自ら感染して検体を収集しようとしても、そのためには多くの経路(IPアドレス)を確保する必要があり、十分な検体収集能力を準備することができないのが実情である。

また、検体が収集できたとしても、ボットの変態機能(上記(5))から、全てのボットプログラムを収集することは非常に難しい。

ボットプログラムの中でも、アゴボット等、幾つかのボットプログラム及びその亜種についてはウイルス対策ソフトでの検出・駆除が可能であるが、それは数1000種類ともいわれるボットプログラムの中の氷山の一角に過ぎない。

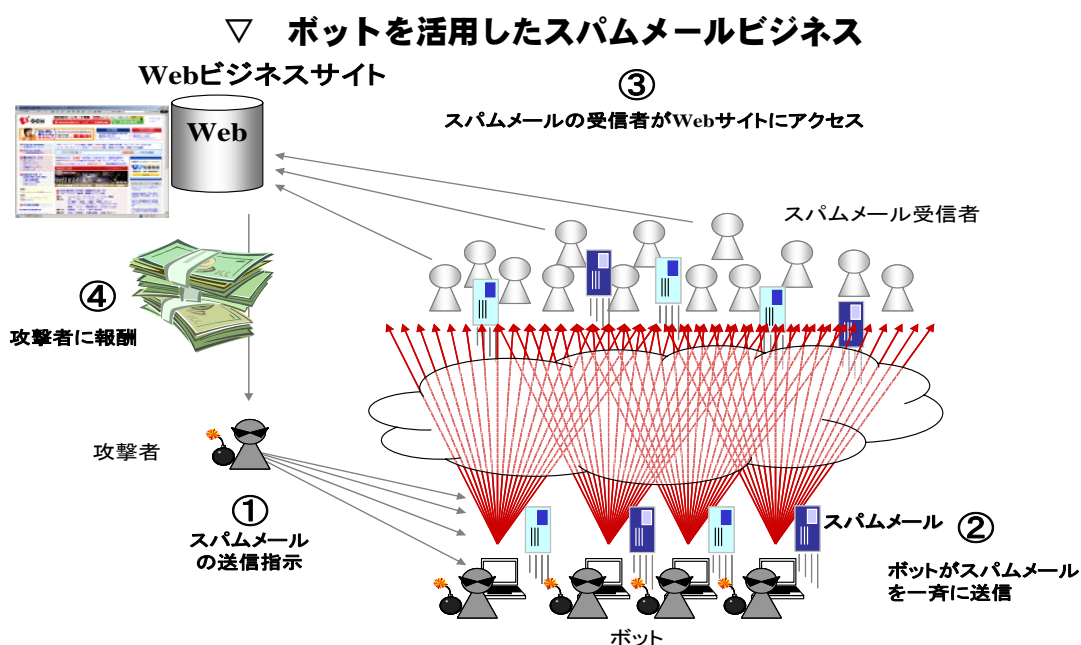
このため、上述した7つの特徴以外の特徴を持つボットが存在する可能性も十分にある。

1.4.2 ボットネットがもたらす脅威

ボットネットがもたらす脅威としては、次のものが挙げられる。

(1) スпамメール等の送信・中継

ボットプログラムは、スパムメールを送信し、また攻撃者から送信されたスパムメールを中継することができる。

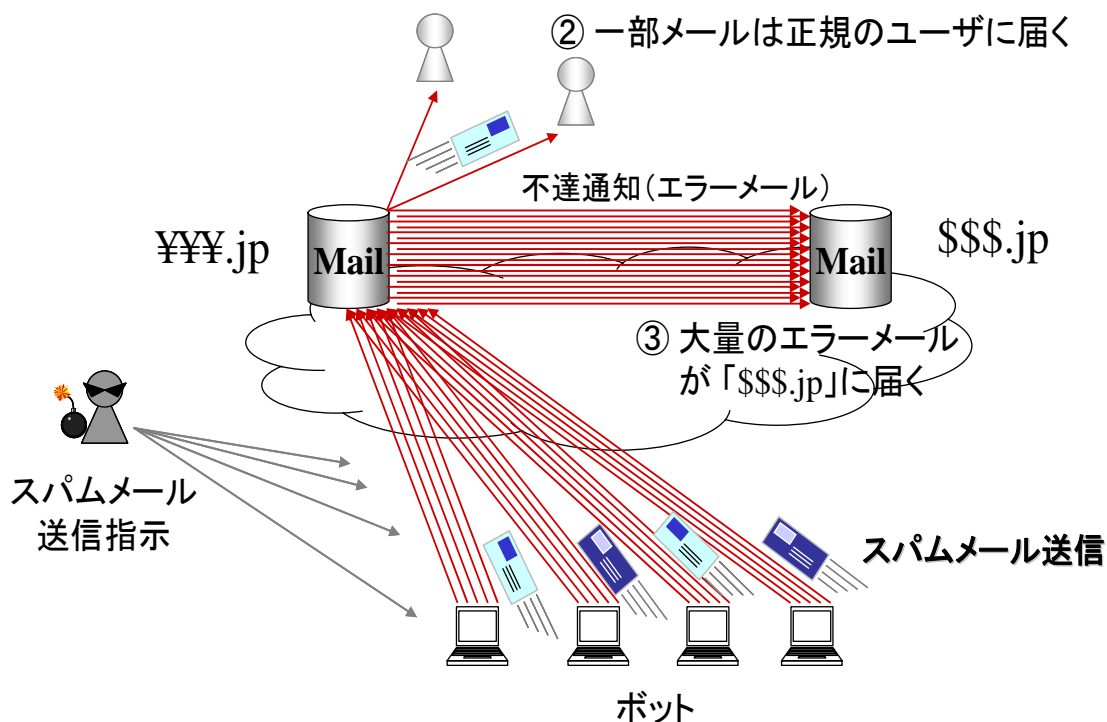


送信の宛先については、あらかじめリストアップされたメールアドレスや自動生成されたメールアドレスを利用する。

自動生成されたメールアドレスを使用する場合、実際には存在しないアドレスに対する送信が大量に行われることから、ISPのメールサーバにおけるエラーメールの処理とエラーメールメッセージの送信によるトラフィックが膨大になる。

送信元のメールアドレスを詐称している場合も多いため、エラーメールメッセージの転送が一種のDOS攻撃と化すこともある。

▽ ボットのスパムメールによるISPのメールサーバへの過負荷



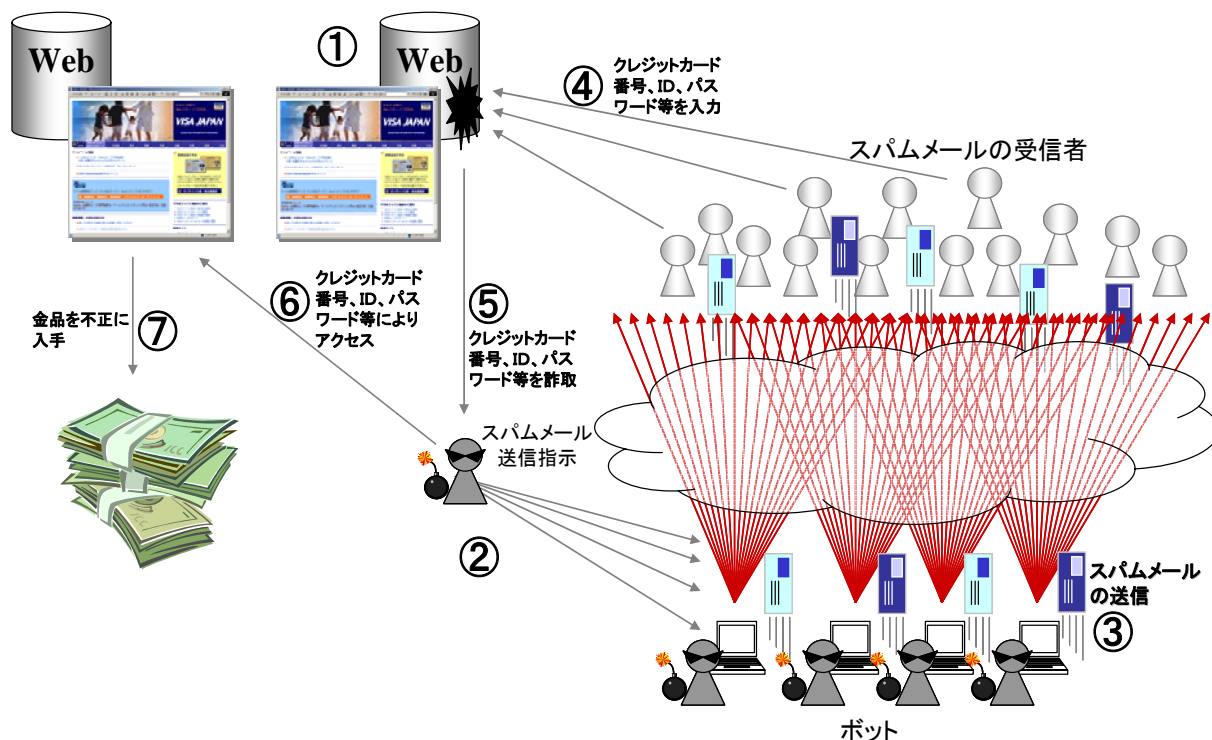
① 送信元を「\$\$\$\$.jp」ユーザと詐称したスパムメールを「¥¥¥.jp」ユーザに送信

(2) フィッシング (Phishing) 詐欺

フィッシング詐欺を企てる者は、ボットにフィッシング用スパムメールの送信を指令し、このスパムメールの受信者にフィッシング Web サイトにアクセスさせ、クレジットカード番号、ID、パスワード等を入力させること等により、個人情報を不正に入手することができる。

また、ボットがフィッシング Web サイトとして利用されている場合もある。

▽ ボットによるフィッシング詐欺の手口



(3) D o S 攻撃

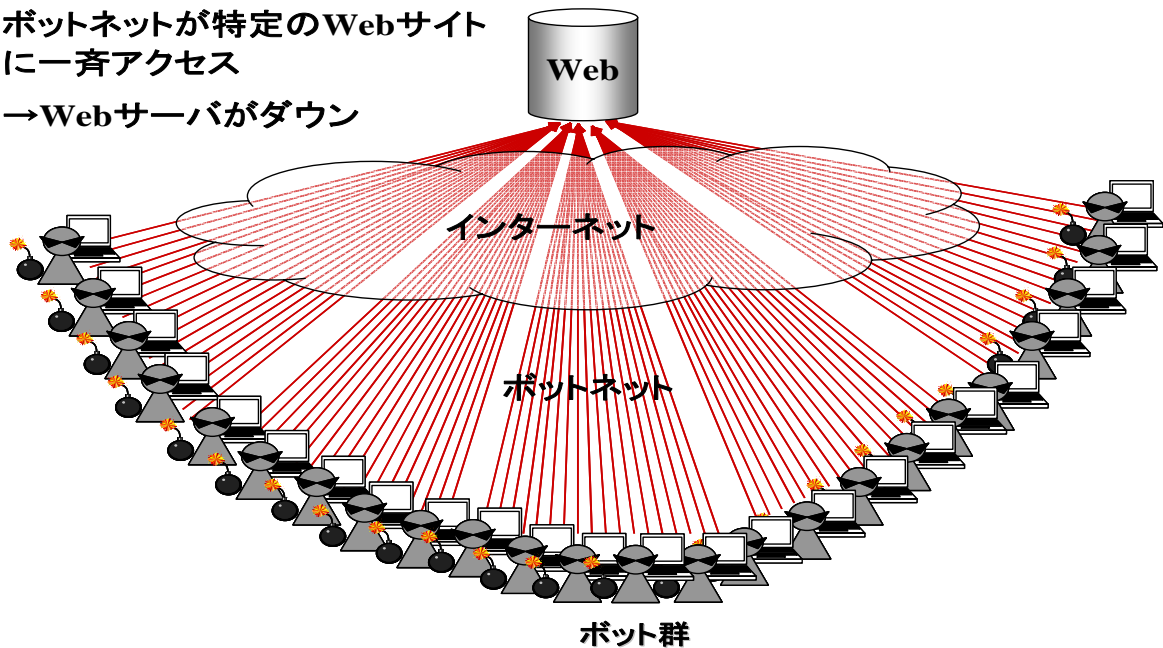
ボットプログラムは、攻撃者の指令により、ボットネットに属するボットから特定の Web サイトに対して、一斉に D o S 攻撃を行うことができる。

2004年6月には、米国のコンテンツデリバリーネットワーク事業者である Akamai Technologies 社の DNS サーバに D o S 攻撃があり、一時、Yahoo、Google、Microsoft、Apple 等の Web サイトにアクセスできない状態となったが、同社ではこの攻撃をボットネットによるものだとしている。

また、Antinnyの感染範囲は日本国内に限られていたが、仮に Antinny による攻撃が1つのボットネットからのものであり、今後、複数のボットネットが Antinny と同様の攻撃を同時に開始することがあり得るとすれば、インターネット全体の問題となる可能性がある。

▽ ボットを利用したD o S 攻撃

ボットネットが特定のWebサイトに
一斉アクセス
→Webサーバがダウン



(4) スパイウェア機能

ボットプログラムは、ユーザによるキーボードへのタイプ履歴や、コンピュータ内の個人情報などを攻撃者に送信することができる。

(5) 他のボットプログラムやウイルス等の拡散

他のボットプログラムやウイルス等を、ボットが有するメールサーバやダウンロードの機能等を利用して拡散させることができる。

また、ボットネットには、販売業者（ブローカ）がいると言われ、スパムメールの送信業者やフィッシングを企てる者に対して、有償でボットネットを貸すビジネスを展開しているとの指摘もある。

以上に見たように、ボットネットは、インターネットで現在問題となっている主な脅威の元凶になっているところであり、ボットネットへの対策は、安全・安心なインターネットの利用環境を整備する上で重要な課題となっている。

1. 4. 3 ボットプログラムの蔓延の背景

「静かな感染」活動を行うはずのボットが短期間に蔓延した理由は定かではない。

ただ、2003年に猛威を振るったネットワーク感染型ワームが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したこと等により、短期間に広く拡散した可能性がある。

例えば、2003年夏に流行したソービグFは、自らが保持しているサーバリストから自らの更新ファイルをダウンロードする機能を持っており、これにより自らをスパムメールやDOS攻撃の送信元に変化させることができるとの指摘があった。

また、現在確認されているボットプログラムの一つであるアゴボットは、マイドゥーム等のウイルスが開けたバックドア等を利用して感染することが確認されている。

換言すれば、これらのウイルスは、ボットプログラムを蔓延させるのが主な目的であり、多くの亜種が作られたのも、ボットプログラムを蔓延させるためのものだったとも考えられる。

いずれにしても、脆弱なままのコンピュータの存在、すなわち、セキュリティ意識の低いユーザがブロードバンドで常時接続していることが、ボットプログラムの蔓延の背景にあると考えられる。

最近では、ISPやセキュリティベンダ等によるユーザに対するセキュリティ啓発活動が盛んに行われるようになっているが、それでも、脆弱なコンピュータは減少していない。

今後、ユーザのセキュリティ対策について、より効果的な啓発活動を官民を挙げて検討し、継続的に推進していく必要があるものと考えられる。

1. 4. 4 ボットネット対策の現状

ボットプログラムは、脆弱なコンピュータをターゲットに感染することから、まず、ユーザ側において利用しているOSに最新かつ適切なセキュリティパッチを当てる必要がある。

また、既に存在が知られているボットプログラムもあることから、通常のウイルス対策の延長として、ウイルス対策ソフトの定義ファイルを常に最新のものに保ち、定期的にコンピュータのスキャンを実施することも必要である。

更に、ファイアウォール（パーソナルファイアウォールを含む。）を導入すれば、なお効果的である。

しかし、セキュリティ意識の高くないユーザが多いのが実情であり、また、既にボットプログラムに感染しているコンピュータについては、これらの対策を講じても、ボットプログラム自体が変態することから駆除できない場合も多く、ボットの絶対数を減らすことは難しい状況にある。

ISP側においても、最近になってボットネットの性質と対策の難しさが認識されてきたところであり、効果的な対策はまだ見出されている訳ではない。

1. 4. 5. 今後の課題

ボットネット対策において留意しなければならないことは、ボットは被害者であり、かつ加害者でもあるという点である。

これまでの攻撃では、主に攻撃を受ける者が被害者であったが、ボットの場合、ボットプログラムに感染してしまっているという点では、被害者であるが、攻撃源となっている点では加害者である。

このため、「ボットプログラムの感染から守る」とこと、「ボットネットの攻撃から守る」という2点について対策をとる必要がある。

これらについては、①ボットの特徴を考慮した技術上の課題、②期せずして攻撃に加担してしまったボットの取扱い等に係る制度上の課題、③対策を進める上で必要な体制上の課題について検討することが必要である。

そこで、以下では、技術上の課題、制度上の課題、体制上の課題及びユーザへの啓発について詳述する。

(1) 技術上の課題

技術上の課題としては、次の2点が挙げられる。

- 1) ボットを今以上に増やさないようにする感染防止と感染した場合の早期駆除
- 2) 既に存在しているボットネットからの攻撃の予防と防御

1) 感染防止と早期駆除

① 検体収集

ボットプログラムは、その検体を捕捉できれば、ウイルス対策ソフト等による駆除が可能である。

しかし、ボットプログラムは、ユーザが感染に気付きにくいという特徴を持っていることから、ユーザからの感染報告や検体提供に多くの期待を寄せることはできない。

また、ボットプログラムは、通常のリバースエンジニアリングの手法（プログラム解析）では検体の解析に時間がかかることが課題となっている。

すなわち、セキュリティベンダにおいては、パターンファイル作成を主要な業務としており、ボットを解析するのではなく、ボットの種類を判別するだけなので、ボットによる被害を防止するために必要となる情報を解析することが求められている。

このため、おとりとなる機器（「ハニーポット」）を用いた検体収集システムを今まで以上に増強する必要がある。

増強に当たっては、第1に、ボットプログラムの「静かな感染」に対応して検体を収集するために、多くのIPアドレスを取得し、今まで以上におとりの感染経路を広域に張り巡らすとともに、第2に、システム構成やシステムリソースを増強することが必要である。

ボットは、攻撃者からの指令を待ち、かつ変態機能を有するという特徴を持っていることから、いったんボットプログラムに感染したハニーポットについては、ハニーポット自体が他のコンピュータに攻撃を加えないようにしつつ、攻撃者からの指令や変態の状況を観測しうるシステムになっている必要がある。

そのためには、外部との通信やそれに伴うシステム内部の状態の変化等を長期間にわたり、つぶさに記録し得るだけの記録領域を持つとともに、その記録の中からボットに関連するものを取捨選択し得る機能を持ち合わせている必要がある。

② ボットネットの行動特性の把握

ボット及びボットネットの活動・行動については、まだあまり知られていない。

攻撃者の指令の下で行動をするボットネットの特性を知るとともに、ボットネットからの攻撃がインターネット全体に与える影響や、攻撃経路に与える影響等を推測・推定するために、実際のインターネットに近いテストベッド環境において、ボットネットからの攻撃を実証する動的な分析も必要である。

2) 攻撃の予防と防御

① テストベッドにおける実証結果を踏まえた広域モニタリング（定点観測）

既に存在しているボットネットからの攻撃を予防し防御するためには、トラヒックの全般的な動向から、攻撃をできるだけ早期に把握し、大きな障害にならないうちに対策をとる必要がある。

現状においても、ISPは自らのネットワークのトラヒックを監視しており、また、Telecom-ISAC Japanでは、国内主要ISPをまたがってトラヒックの動向等を監視する広域モニタリングシステムによる定点観測を実施している。

しかし、ボットネットによる攻撃は、ボットの近隣においてトラヒックの劇的な増加がなく、通常トラヒックの誤差程度でしかないため、これまでの定点観測システムでは、ボットネットによる攻撃を早期に検知することは困難である。

そこで、上記1) ②のテストベッドでの実証結果から得られたボットネットの行動特性を加味して、広域モニタリングシステムを構築する必要がある。

また、検体収集システムとリアルタイムに連携することも検討すべきである。

すなわち、仮想的にボット化したハニーポットに対し、攻撃指令や攻撃につながる活動、あるいはこれらを想起させる指令や活動が起きた場合に、アラームが出るようにすることができれば、攻撃開始前又は攻撃開始後早期に、対策を実施することができるようになると考えられる。

② 攻撃元となっているボット（ボットネット）の把握

次に、ボットネットからの攻撃への対策の1つとして、攻撃元又は攻撃元に近い中継器で、攻撃を遮断することが考えられる。

しかしながら、攻撃の多くは、送信元のアドレスを詐称しているため、攻撃元を把握することは難しいのが実情である。

こうした技術上の課題について、攻撃を受けている側から経路の追跡を可能にしようとする「トレースバック技術」が提案されている。

トレースバック技術の開発については、レイヤの低いデータリンク層から、IP(ネットワーク層)、更にはアプリケーション層に至るまで、複数のレイヤで幾つかの方式が提案されており、複数のレイヤを跨って連携する方式も提案されている。

しかしながら、これまでに提案された方式は、閉じたネットワーク内での方式に留まっており、実際のインターネットに近い環境下での活用を目指したものはない。

ボットネットによる攻撃が顕在化してきている中で、仮に裁判所の令状をとったとしても、技術的には攻撃元を把握することができないとすれば、攻撃を抑止することはできない。

そこで、技術的には攻撃元を把握することができるよう、トレースバック技術の研究開発を進めることが必要である。

③ 攻撃のフィルタリング

攻撃を遮断するためには、攻撃の対象となっている受信者側の機器において、攻撃データのみをフィルタリングすることが考えられる。

しかしながら、ブロードバンドの普及に伴い、伝送速度に対し、フィルタリングの処理能力が追いつかなくなっている。

上記②のトレースバック技術により、攻撃元となっているボットを把握することができれば、そのボットに近い中継器における高速のフィルタリングは必要ないと考えられるが、大規模な攻撃が起きている状況において、全てのボットを短時間にトレースバックすることは困難である。

このため、攻撃の対象となっている受信者側の機器において、高速かつ確実に攻撃をフィルタリングできる技術の研究開発に取り組むことが必要である。

(2) 制度上の課題

感染防止と早期駆除にしても、攻撃の防御・予防にしても、トラヒック情報やログ情報を収集することが不可欠であるが、「通信の秘密」の保護や個人情報保護法に抵触しないよう、これらの情報をどの程度、またどのように仮装（masking）し、抽象化して把握すべきかが課題になる。

また、トレースバック技術の研究開発等により、攻撃元となっているボットが技術上把握できるようになった場合には、どのような場合にその技術を利用することができるかについての制度上の検討に加え、当該ボットとなったコンピュータを利用してユーザーへの警告、サービスの一時停止等について、約款又は契約の在り方を検討することも求められる。

(3) 体制上の課題

(2) から明らかなように、技術上の課題が解決できたとしても、制度上の課題を解決しなければ、開発及び構築した技術を実際に適用し運用していくことはできない。こうした課題については、関連業界と行政が密に連携して取り組んでいく必要がある。

また、技術上の課題を解決し、インターネットの実運用環境に実装するためには、以下のような体制上の課題を解決する必要がある。

1) 感染防止と早期駆除

(1) で述べたとおり、ボットプログラムの感染防止・早期駆除を行うためには、検体の収集が必要である。

ボットの場合、ユーザーがボットプログラムへの感染に気がつかない場合が多いことから、相当規模の検体収集システムを構築しなければ、十分な検体収集体制はできない。

また、ボットプログラムの「静かな感染」活動に対応すべく、多くの感染経路を用意しておくことも、検体の収集能力を高める上で必要である。

更に、収集した検体を効率的に分析・解析するための人材の確保も重要である。

以上から、セキュリティベンダ、通信機器メーカー、ISPからなる協力体制を構築することが必要である。

実際の協力体制構築に当たっては、個々の業界の特性や、ボットネットに対する業界間での立場の違い、及び個々の業界内での利害関係が存在することから、それらを調整する機能が必要となる。

そのためには、セキュリティベンダ、通信機器メーカー、ISPなど各業界における専門家のほかに、これらの専門家による協力体制を促進することのできる調整力のある人材を育成し、専従的に確保することが求められる。

2) 攻撃防御・予防

攻撃防御に関してはISP相互の連携体制が不可欠である。

既に、Telecom-ISAC Japanでは、ISP間でインシデント情報を共有し、広域モニタリングシステムを運用しているが、それをボットネットの攻撃特性に対応させ、攻撃の予兆がある場合に、速やかに防御体制をとることができるよう、連携体制を整備することが求められる。

トレースバック技術の研究開発については、(2)で述べたように、制度面の検討と平行して行うことが必要である。

また、研究開発成果については、複数ISPをまたがるシステムとして実装して運用されなければならない、こうした課題についてTelecom-ISAC Japanを中心に整理・検討しておくことが必要である。

また、海外のボットからの攻撃や、国内のボットから海外への攻撃に対処するために、政府レベル、業界団体レベル等、各層における国際協力体制を構築することも求められよう。

(4) ユーザへの啓発

ボットネットの問題の根底には、次のような事情がある。

- ① ユーザ側にボットプログラムに感染しているという自覚がない場合が多いこと
- ② こうしたボットが既に大量に存在していること
- ③ ボットプログラムに感染しているユーザは、自らは気付かないうちに、攻撃者からの指令を受けて他のユーザのコンピュータに攻撃を加える可能性があること

常時接続のブロードバンドの普及により、ダイヤルアップで接続していた頃と比べ、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にもかかわらず、最新のセキュリティパッチのダウンロードの仕方が分からないというユーザも存在するのが実態であり、ユーザへの啓発が一層重要な課題となっている。

ブロードバンドの普及により、トラヒックの受発信に関してユーザが大きなパワーを有している状況にかんがみると、インターネットにおいてセキュリティ対策を講ずるべき主体はISPのみではなく、ISP、システムインテグレータ、ユーザ等の関係者による取組みがどれ一つ欠けても十全なセキュリティ対策を講じることができない、という考え方を社会一般に醸成しなくては必要と考えられる。

具体的には、セキュリティベンダ、システムインテグレータ、ISP、通信機器メーカー等が連携して、ボットネットのメカニズムやこれに対する対策をわかりやすく、迅速かつ確実に一般ユーザに提供していくことが重要である。

特に、大容量のデータ送信や他のユーザからの苦情申告等により、あるユーザのコンピュータがボット化していることが判明した場合には、当該ユーザに対する個別の注意喚起や駆除の方法に係る情報提供を行う等、これまでよりも一層踏み込んだ形でセキュリティ対策に関するユーザ啓発を行うことが必要である。

更に、接続しているユーザのコンピュータが次のような弊害を実際にもたらす場合には、スパムメールと同様、当該ユーザへの警告、電気通信サービスの一時停止、更には契約解除等の措置をとることがあり得る旨を、ISPにおいて約款又は契約で予め明確化しておくことも求められよう。

- ① 当該ISPの電気通信設備の機能に障害を与える場合。
- ② 当該ISPとの間に電気通信サービスの提供を受ける契約を締結している他のユーザの電気通信設備の機能に障害を与える場合。

また、どのようなコンピュータがボット化し易いかについて調査を進めることも有益である。

常時接続のブロードバンドサービスが普及している中であっては、電源をつけたままの家庭内のコンピュータや企業ネットワーク内で管理されずに放置されているコンピュータがボットプログラムに感染しやすいものと考えられることから、ボット化するコンピュータが減少するように社会的に啓発を進めていくことが重要である。

1. 5 ソーシャルエンジニアリングへの対処

インシデントの最近の傾向をみると、攻撃を行う側の方が、攻撃を受ける側よりも、情報把握の面においても技能（skill）の面においても有利な立場にある。

また、攻撃を行う側は、技能だけでなく、攻撃を受ける側の無知や無警戒、更には心理を逆手にとって不正に情報を収集している場合が多い。

一般のユーザを対象とするフィッシング詐欺は、その最たる事例と言える。

情報セキュリティにおいて最も脆弱なのは、ハードウェアやソフトウェアよりも、むしろ人間であり、ハードウェアやソフトウェアについて厳重なセキュリティ対策を施したとしても、人間が騙されてしまえば、攻撃者は簡単に組織のシステム内部に侵入することが可能である。

人間の無知や無警戒、あるいは心理や行動様式につけ込んで組織のセキュリティを侵害する手法は、「ソーシャルエンジニアリング（social engineering）」と呼ばれ、米国等では既に研究が進んでいる。

▽ソーシャルエンジニアリングの事例

(1) なりすまし

- ① 攻撃者が内部の者であると装って企業のコンピュータヘルプデスクに電話を掛け、システムへのアクセスに障害が発生したので、これまでのパスワードをリセットさせて、新しいパスワードを設定できるようにすることが考えられる。他の手法により内部情報を入手している場合、ヘルプデスク担当者を更に信頼させることができる。
- ② 攻撃者が企業のコンピュータヘルプデスクであると装って、問題を解決するためにパスワードやID等を企業内ユーザから聞き出すことも考えられる。

(2) のぞき見

ユーザのIDやパスワードを、コンピュータを操作する指の動きから読み取り、又は書き残したメモを見ること等により入手することが考えられる。

(3) トラッシング（ゴミ）の渉猟

たとえ断片であっても、ゴミから個人情報、企業内の組織図、カレンダーに記入された会議や休暇の予定を入手すること等により、内部者としてなりすますことを容易にすることが考えられる。

我が国においても、ソーシャルエンジニアリングについて早急に研究を進め、攻撃を受ける側にとって有益な情報提供と対応策の提示を行っていくことが必要である。

これについては、組織においてセキュリティポリシーを策定し（Plan）、それに沿った従業員教育やセキュリティ対策を実施・運用し（Do）、監査し（Check）、改善する（Act）という情報セキュリティマネジメントに関するP-D-C-Aサイクルを実行することが有用と考えられる（これについては、第3章で再度取り上げる。）。

セキュリティポリシーは、どのような行為が許され、どのような行為が制限されるのかに関し、明確な指針に従業者に対して示さなければならない。

また、セキュリティポリシーの目的と動機付けについて、従業者に対し十分な教育が行われることも必要である。

更に、ソーシャルエンジニアリングであると疑われる手法が発見された場合において、従業者からの報告が速やかに行われ、これを受けて経営陣が対処しているということを従業者に示すことも重要である。

これにより、従業者のモチベーションを維持し、ソーシャルエンジニアリングへの対処に、従業者を組み込んでいくことが容易になる。

以上に加え、ソーシャルエンジニアリングへの対処は、従業者のみを対象とするのではなく、経営陣による組織に対する背信行為があり得ることも考慮に入れるべきである。

これについては、経営陣の中で相互に監視し合うとともに、株主による監視や、所管官庁による業務監査又はシステム監査等の方法により対処することも考えられる。

1.6 経路情報の誤りによるICT障害

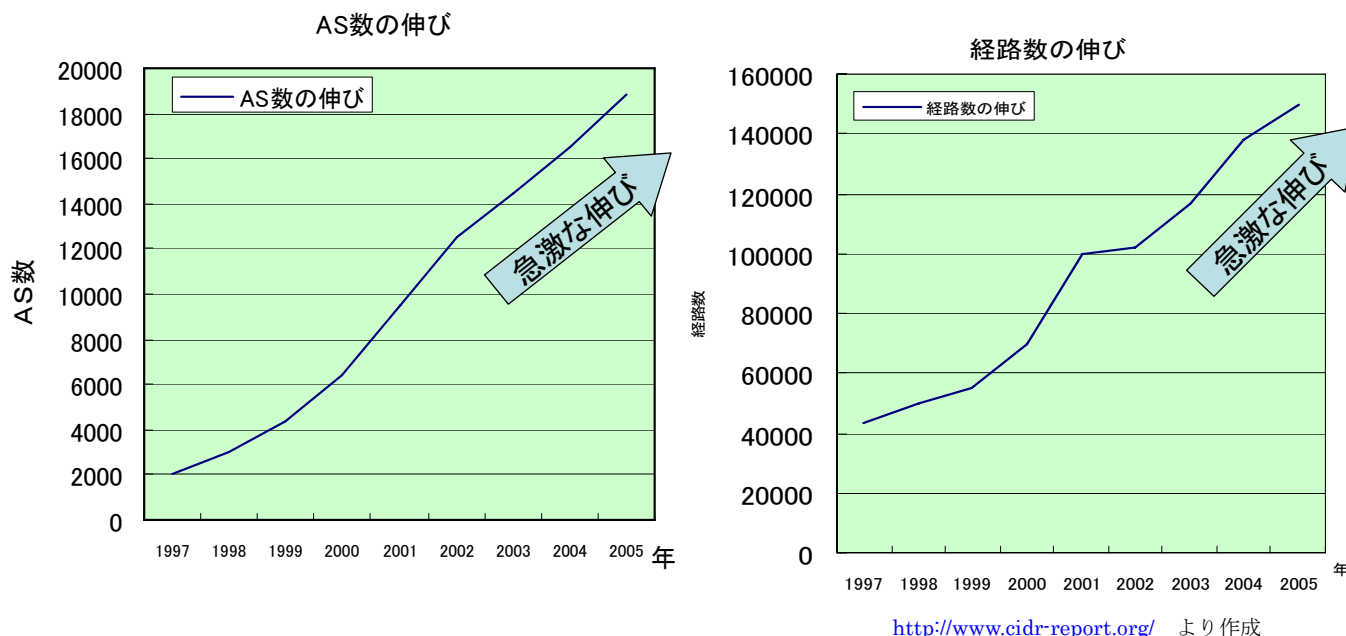
これまでは不正アクセスやウイルス、ワーム等、意図的要因によるインシデントについて検討してきたが、以下では、経路情報の誤りによるICT障害について検討する。

1.6.1 経路数の拡大

インターネットは、1990年代に米国で商用サービスが開始されて以来、一貫して拡大を続けており、現在では、ISP等によって管理されているネットワーク（AS^(注13)；Autonomous System）の数は1万8千を超え、AS間を結ぶ経路数は15万に達している。

（注13）AS（Autonomous system）とは、ある経路制御方針によって運営されているネットワークのことを言う。

図 経路数の拡大



1.6.2 経路情報の誤りによるICT障害

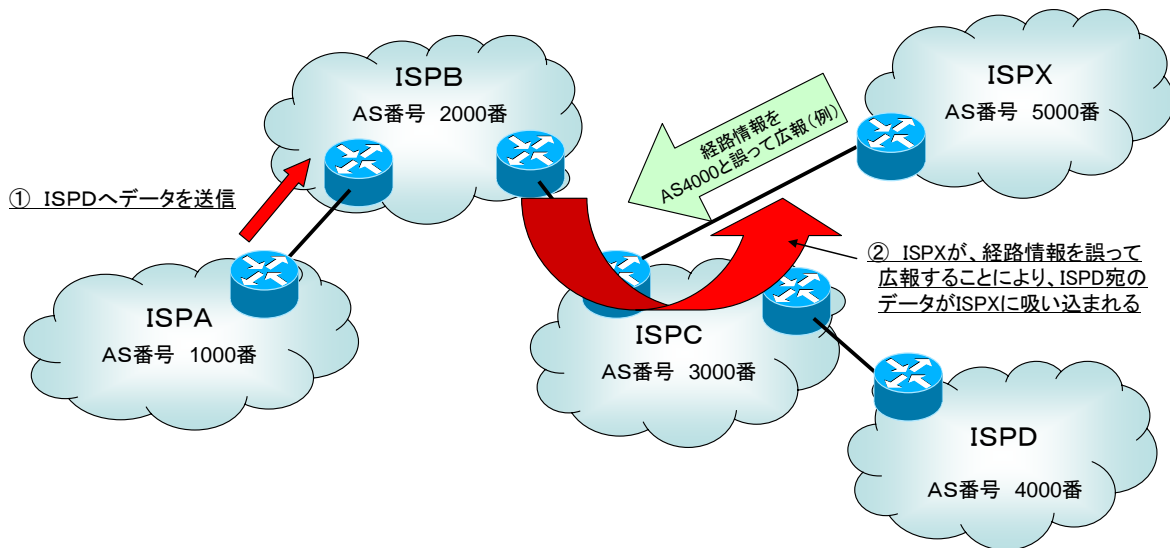
インターネットは、「ネットワークのネットワーク」と言われるとおり、複数のネットワークが相互に接続したネットワークであり、あるISPから見れば、直接の接続相手より先は、どこに接続しているのかが分からないネットワークである。

このため、障害が発生した場合の対応や協調運用が困難となっている面があるのが実情である。

その原因の1つである経路情報の誤りは、①非意図的に誤った経路情報を広報してしまう場合や、②意図的に誤った経路情報を広報し、他のISPのトラフィックを“吸い込む”（適切なISPにトラフィックを受信させず、誤った経路情報を広報したISPが受信してしまう）事例が見られる。

図 経路情報の誤りによるトラヒックの吸い込み（例）

・ISPXが経路情報を誤って広報することにより、ISPD宛のデータがISPXに転送される。



経路情報の誤りによる障害は、他のISPによる経路情報を信頼してデータを転送するという現在のインターネットの仕組みでは発見が難しく、データが届かないことに気づいたユーザによって障害が発見される場合が多い。

ISPでは、経路情報の誤りによる障害が発生した場合、何処に問題があるのかを解析・特定し、経路設定を誤ったISPに電話等で直接コンタクトをとることにより対応を図っており、障害の回復に時間を要しているのが実情である。

特に、海外のISPが引き起こす経路情報の誤りや、海外のISPによるトラヒックの吸い込みがあった場合には、ネットワーク運用に対する考え方の違いや言語の違い等から、その対応には相当の時間を要しており、こうした経路情報の誤りは、インターネットの信頼性を損なう大きな要因の1つとなっている。

1.6.3 経路情報の誤りによるICT障害への対応策

経路情報の誤りによる障害に対応するためには、まず、ISPにおいて経路情報の信頼性を確保するための取組みが不可欠であるが、各ISPにおける取組みには差異がある（特に、海外のISPの取組みも含めて考えると差異は大きい）ことから、経路情報の誤りを全く無くすことはできない。

このため、情報の誤りによる障害が発生し得ることを前提に、障害の広域にわたる検知、回復、予防を行うことが求められる。

この点については、障害を広域に検知するためのモニタリングシステムの構築、障害の回復、予防を迅速かつ効率的に行うために必要な技術開発・実証実験を行うことが有効と考えられるところであり、ISPが連携して取り組むことが適当である。

第2章 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—

2. 1 ユビキタスネット社会におけるセキュリティ確保の必要性

第1章では、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た。

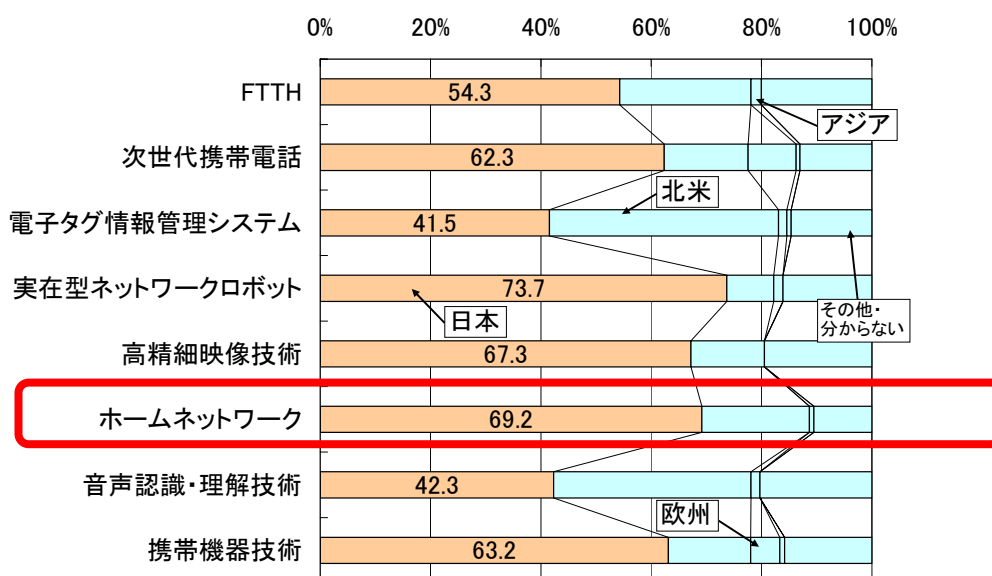
他方、我が国はブロードバンド通信の「安さ」と「速さ」において既に世界1の環境を実現し、2004年12月に総務省が取りまとめた「u-Japan政策」では、2001年1月のe-Japan戦略におけるキャッチアップ的な発想から脱却し、2010年には世界最先端（フロントランナー）のICT国家として世界を先導することが目標とされている。

このu-Japan（ユビキタスネットジャパン）政策においては、「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながる「ユビキタスネット社会」を実現することが必要不可欠な事項とされており、このユビキタスネット社会を支えるためにも、情報セキュリティの確保は重要な政策課題と言える。

すなわち、情報家電を含むあらゆる端末がネットワークにつながる「ユビキタスネット社会」を想定してセキュリティ確保に取り組んでいくことは、我が国がフロントランナーとして世界を先導していく上で不可欠であり、こうしたフロントランナーとしての取組みは、セキュリティを含め、我が国のICT産業の国際競争力を維持・強化する上でも重要と考えられる。

実際、情報家電を含むホームネットワークは、我が国が国際的に技術優位性を有すると考えられている分野であり、そのセキュリティ確保に向けた取組みは、ホームネットワークに関する我が国の国際競争力の維持・強化に寄与するものである。

▽ 情報通信技術の優位性に関する国際比較



※各技術の優位性について、情報通信技術者へのアンケート調査

(出典)ユビキタス社会の動向に関する調査

また、情報家電を始めネットワークにつながる端末が多種多様になることは、それによってサービスを提供するアプリケーションサービスプロバイダ（ASP）、家電メーカー、ISP等にとって新たなビジネス機会の創出につながるものと言える。

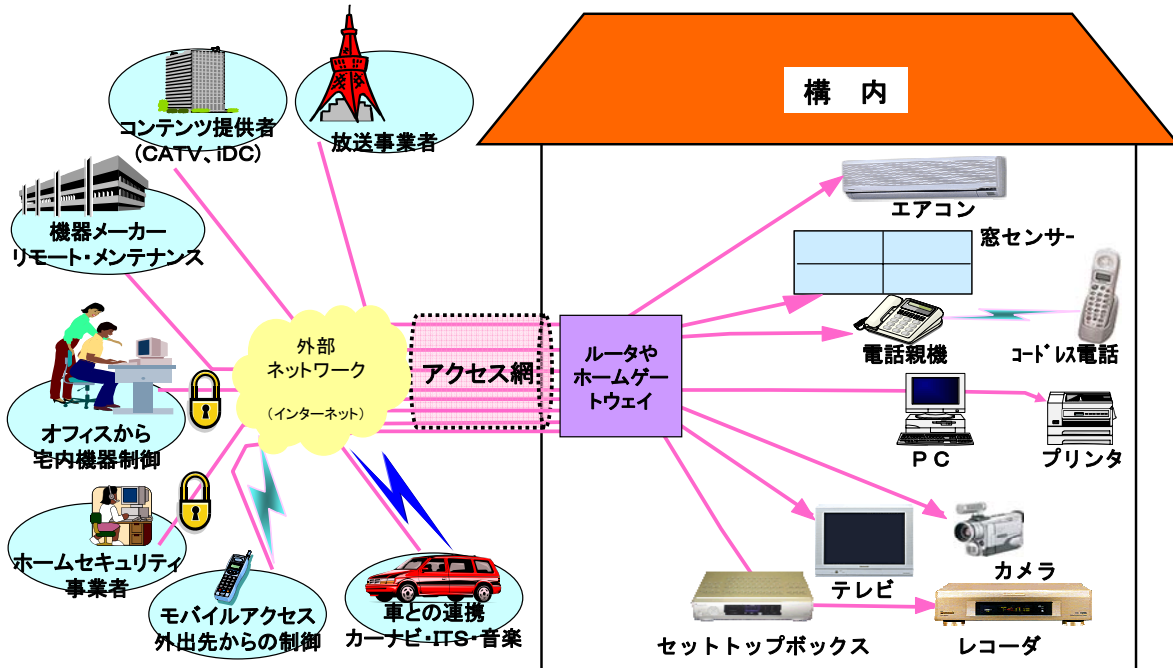
他方、家電業界やISP業界の視点からではなく、消費者の視点からみると、家電がインターネットに接続され、通信機器として機能すると、情報セキュリティ上の問題も発生し得るということを認識していない消費者も多いと考えられるところであり、「誰でも、簡単かつ安全に」家電を利用できるようにするためのセキュリティ基盤を確立することが求められていると言える。

そこで以下では、情報家電に焦点を当てて、そのネットワーク接続に伴うセキュリティ確保について検討する。

2. 2 情報家電に対する期待と課題

「情報家電」とは、通信機能をもつ家電機器であり、ネットワークと接続することで、構内又は構外にある他の機器との通信を行い、構外からのサービスの利用や構内の機器の相互連携を可能にするものであり、「ユビキタスネット社会」の実現に寄与するものとして期待されている。

▽ 情報家電の利用イメージ



▽ 情報家電への期待

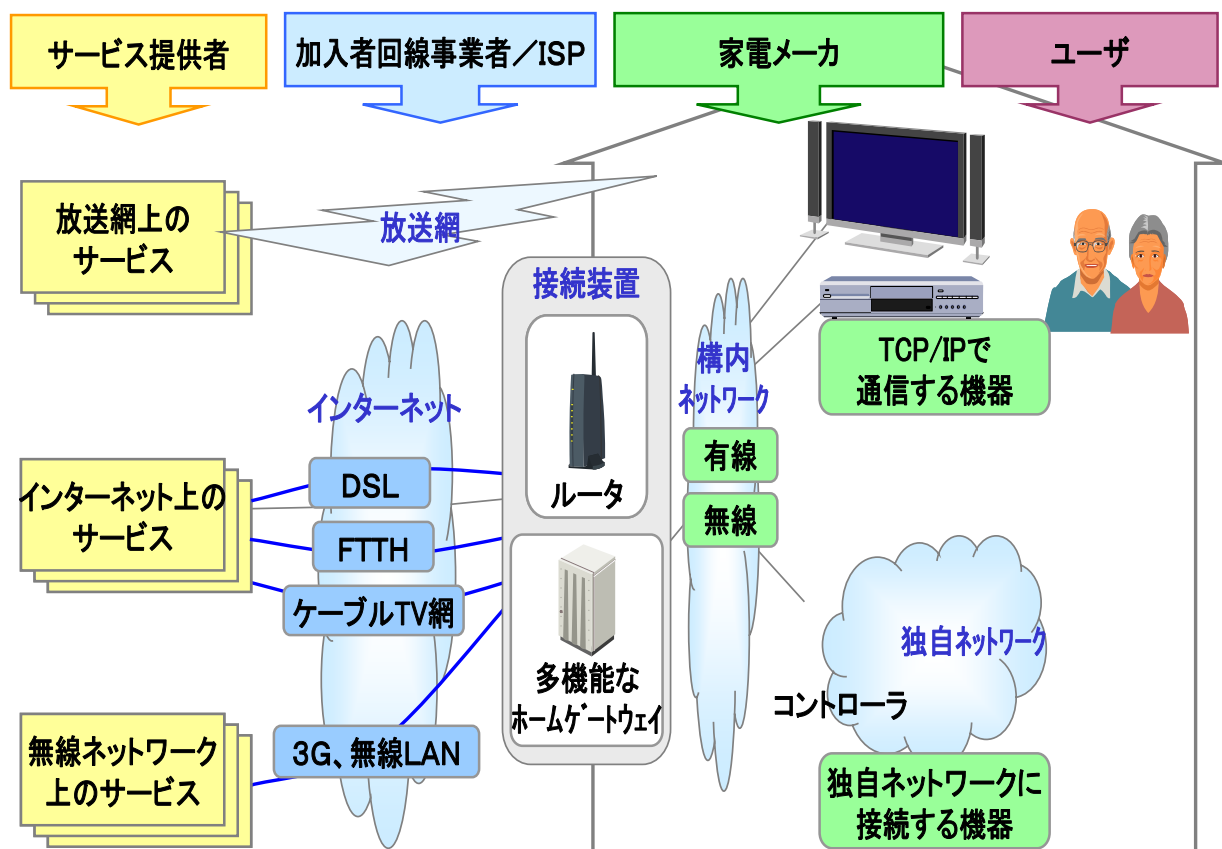
- ・約1万人の調査→73%がネットワーク情報家電を使ってみたい
- ・利用者の不安 ①機器の価格②セキュリティ③サービス料金④使いこなせるか
- ・機器価格は3千円～1万円アップ、サービス料金は300円/月ぐらいだと許容できる

機器の連携	宅外リモコン (機器遠隔制御)	①エアコン ②VTR/DVD機器 ③風呂	69.9%	簡単・快適	
	蓄積番組の視聴	好きなときに好きな番組が見られる (キーワード自動番組録画・リモート視聴)	54.6%	感動	
	くらし安心	①ガス/火災 ②不審 ③部屋 ④照明 ⑤施錠	51.3%	安全・安心	
サービス・機器の更新	TVによる情報提供	映像・情報配信	①BBサービス ②TV電話等	45.7%	感動
		地域情報や電子チラシの配信		39.7%	簡単・快適
		定点観測 監視モニタ	①行楽地や道路/病院混雑状況 ②幼稚園	37.3%	安全・安心
		出かける前の 情報確認	①天気 ②時刻表 ③乗換 ④地図等	34.8%	簡単・快適

2002年8月 松下電器調査

また、情報家電によるサービスには、家電メーカーのほか、構内ルータ／ゲートウェイのメーカー、加入者回線（アクセス）網提供事業者、I S P等、様々な事業者が関わるものであり、業種をまたがった連携や調整が、情報家電を定着させていく上で必要不可欠である。

▽ 情報家電によるサービスに関わる様々な業種

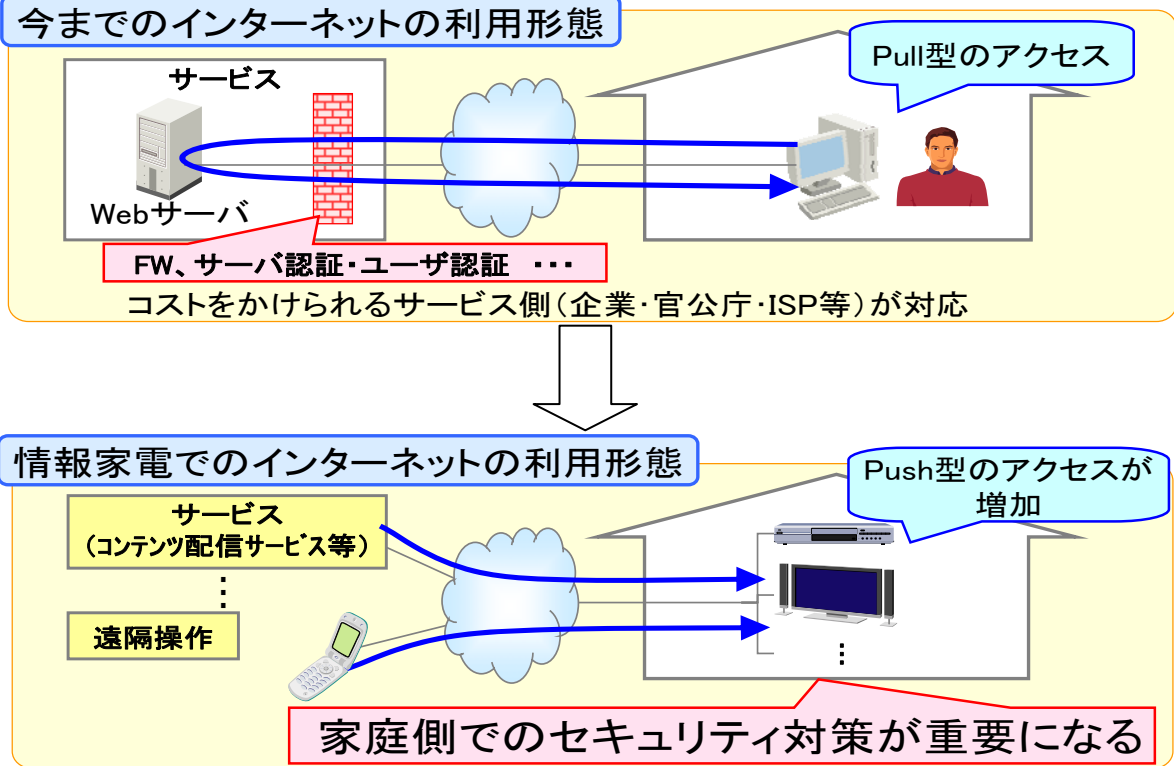


更に、情報家電によるインターネットの利用形態は、従来のインターネットの利用形態とは大きく異なる可能性がある点にも、留意しておくことが適当である。

すなわち、従来のクライアントサーバ型のインターネットの利用形態においては、構内に居るユーザから構外のサーバにアクセスして情報を引き出してくる「Pull 型のアクセス」が主流であったが、情報家電によるインターネットの利用形態は、構外にいるユーザから構内の情報家電をコントロールし、また、サービス提供者が構内の情報家電に直接コンテンツを配信するなどの「Push 型のアクセス」が多くなると考えられるからである。

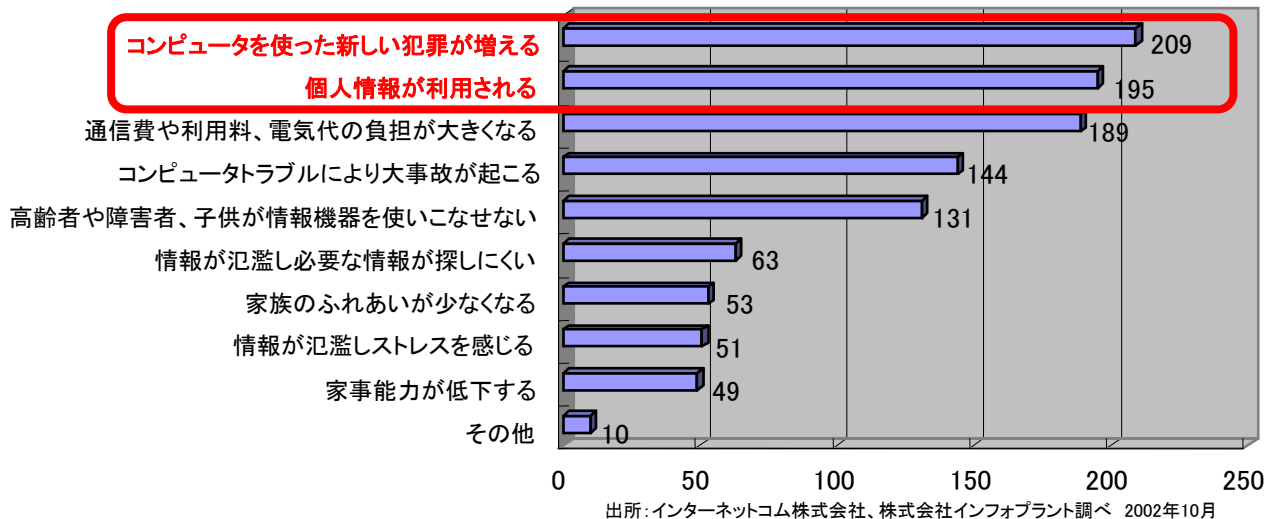
「Pull 型のアクセス」の場合は、アクセスを受ける企業、官公庁、I S P等において費用をかけてファイアウォールや認証機器を整備すれば良かったが、「Push 型」の場合にアクセスを受けるのは、構内にある情報家電であり、構内の情報家電側、すなわちユーザ側でセキュリティ対策を講じることが極めて重要になる。

▽ アクセス形態の変化とセキュリティ対策のリバランス



情報家電に関するユーザの意識を見ても、セキュリティの確保が課題の上位に挙げられており、情報家電が普及する条件としてセキュリティ確保を図ることが重要となっている。

▽ 情報家電とユーザの意識



実際、2004年10月には、

- ① 外部からユーザ名やパスワードの入力不要でアクセスできていたDVDレコーダが出荷され、外部からの不正アクセスにより、このDVDレコーダを踏み台にして大量のスパム（無意味な電子データ）が送信されてしまう危険性が出荷メーカー自身から警告された事例や、

② 専用の接続装置でしか解除できない筈のケーブルテレビのスクランブル（視聴制限処理）を解除することのできる機器が出回った事例、

など、情報家電のセキュリティ事案が相次いで報道された。

そこで、次に情報家電のセキュリティ確保に関する課題を整理してみることにする。

2. 3 情報家電のネットワーク接続に伴うセキュリティ上の課題

2. 3. 1 接続検証と規格化

そもそも、情報家電によるサービスの実現に当たっては、情報家電、構内ネットワーク、ゲートウェイ、加入者回線（アクセス）網、ISP、アプリケーションサービス提供事業者（ASP）というように、多段階にわたる接続検証を重ねる必要がある。

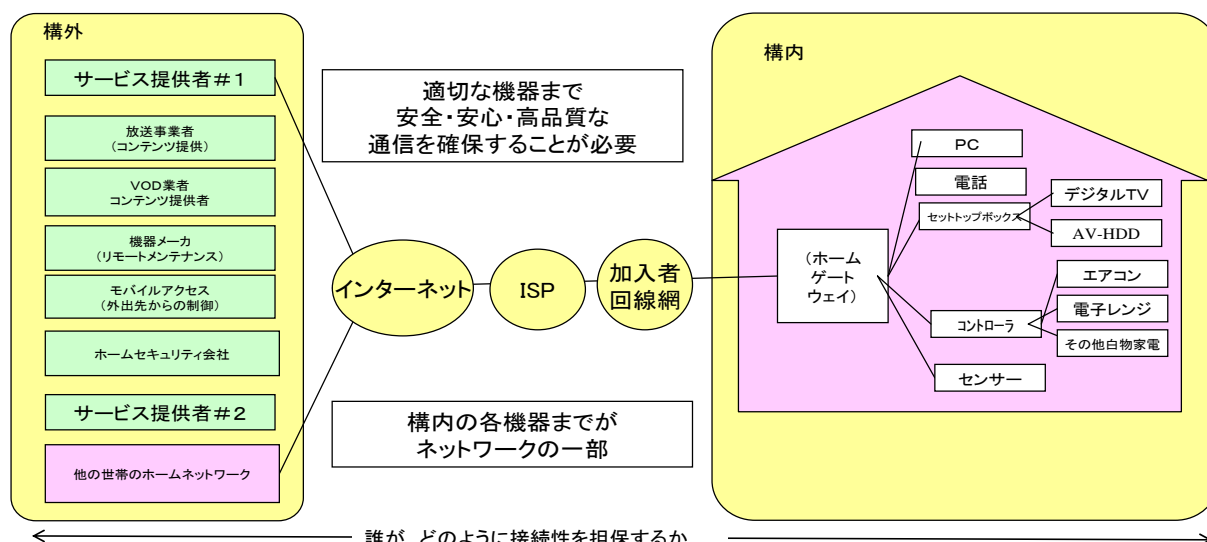
こうした接続検証を各社ごとに行うのでは、件数も無限大となり、非効率と考えられることから、業界の枠を超えて接続検証と相互利用可能な規格化を行うことが適当と考えられる。

その際、品質保証等の機能の提供方式のモデル化、接続に関する責任分界点の明確化、接続管理方式の策定等の作業も併せて行うことが望ましいと考えられる。

▽ 接続検証

$$\text{接続検証件数} = N \times N \times N \times N \times N \times N \times N \times N = \infty$$

(サービス提供者) (ISP) (加入者回線事業者) (ゲートウェイ) (宅内ネット) (IP情報家電) (非IP情報家電)



2. 3. 2 情報家電がボット化した場合の対応

ISPからすれば、情報家電機器もワームやボットプログラムに感染する可能性のある通信機器であり、接続しているユーザの情報家電機器がボット化し、次のような弊害を実際にもたらす場合には、当該ユーザへの警告、接続の停止、電気通信サービスの一時停止等の措置をとることがあり得る旨を、約款又は契約で予め明確化し、ユーザに周知しておくことも求められよう。

- ① 当該ISPの電気通信設備の機能に障害を与える場合。
- ② 当該ISPとの間に電気通信サービスの提供を受ける契約を締結している他のユーザの電気通信設備の機能に障害を与える場合。

2.3.3 リモートメンテナンスと機器認証

情報家電のセキュリティ確保を検討する際には、コンピュータについて講じられている以上のセキュリティ確保が情報家電には必要なのか否か、という観点から考察を加えてみるのが有効である。

セキュリティ確保に関する課題について、コンピュータと情報家電の異同点を挙げてみると、下表のとおりである。

▽ セキュリティ確保におけるコンピュータと情報家電との異同

同じ点	違う点
<p>① コンピュータでは、Windows 等の汎用的なOSが多く利用されているが、情報家電においても機器固有のソフトウェアだけでなく Linux や TRON 等の汎用的なOSを利用するケースが増えつつある。そのため、ひとたび脅威が発生すると、全体が機能不全に陥る恐れがあり、情報家電についてもコンピュータと同様の脆弱性対策が必要である。</p> <p>② 接続環境が千差万別で、接続検証に手間がかかる。</p>	<p>① 表示画面が小さくキーボードがない等、ユーザインターフェースに難がある。</p> <p>② バグの修正、仕様変更をユーザ側に適用することがしにくく、バグを内在した機器がコンピュータ以上に拡散してしまう可能性が大きい。</p> <p>③ プログラムの命令を実行する装置であるCPU(Central Processing Unit;)の能力が低く、搭載メモリ容量が小さい。</p> <p>④ 色々な情報家電製品が出荷され、それぞれのセキュリティ対策水準が異なると、結果としてセキュリティ対策の水準が低い製品に揃ってしまう可能性がある。</p>

情報家電のOSやソフトウェアに脆弱性が発見された場合、コンピュータと同様、修正プログラムを適用する必要があるが、ほとんどの情報家電においてはコンピュータと異なり、表示画面が小さく、表示画面すら無い場合がある。

加えて、キーボードのような多機能な入力装置はなく、リモコンがあるものもあれば、制御用の入力装置すらないものまである。

更に、情報家電は、CPU能力が低い、メモリが少ない等の特徴があることから、セキュリティ確保のために必要な作業を、端末側でこなすことは困難が伴う。

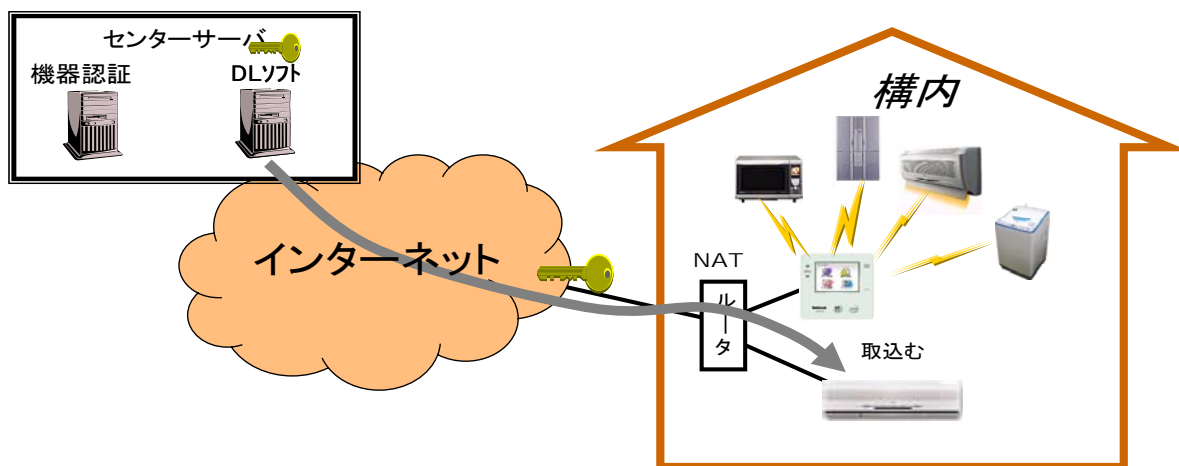
また、ユーザの多くは、自ら機器のメンテナンスができない層であると考えられる。

更に、情報家電は生活に密着しており、子供から高齢者まで様々な人々が利用すると想定されること、情報家電は通信機器でもあるという認識に欠ける消費者も多いと考えられること等から、情報家電のユーザに対し、コンピュータのユーザと同様に修正プログラムを適用してもらうよう期待するのは、現実的ではない。

以上から、構外の機器側から構内の情報家電に対して、能動的に修正プログラムを配信し、ユーザ側の操作を簡易にすることを検討する必要があると考えられる(いわゆる「リモートメンテナンス」)。

こうしたリモートメンテナンスに限らず、構内の情報家電に対して構外から接続するに当たっては、構外から不正なアクセスが行われたり、不正なプログラムが適用されたりすることのないよう、構内の情報家電側から構外の機器を認証するとともに、逆に、構内にある情報家電が適切なものであるかどうかについて、構外の機器から構内の情報家電を認証することが求められる。

▽ リモートメンテナンスのイメージ図



こうした機器認証の機能を

- 家電機器メーカーが担うのか、ISPや携帯電話事業者が担うのか、それともサービス提供者が担うのか
- 各社ごとの認証で良いのか、業界を挙げた又は業界横断的な認証の仕組みが必要ではないのか、

という点については、関係各社のビジネスモデルとも絡む調整の難しい問題であるが、一定の規格化を図ることで、

- ① 家電機器メーカー、ISPや携帯電話事業者、セキュリティベンダのいずれにとっても、体制の構築、作業の統一等の面で費用削減を図ることができること、
- ② ユーザにとっても、家電機器メーカーごとの独自の規格や操作方法等に対応する必要がなくなり、利便性の向上につながること、

から、どこまで規格化することが適切かについて、関係業界で十分に検証し、調整することが必要であると考えられる。

2. 3. 4 情報家電を破棄・転売した場合の課題

(1) サービス利用者と課金対象者が異なる可能性

情報家電を破棄・転売した場合において、当該情報家電を通じて利用することのできるアプリケーションサービス（以下、この章で単に「サービス」という。）の契約を元のユーザが解約しないと、当該情報家電を入手した別の人間がそのサービスを利用した場合、サービス料金を破棄・転売した元のユーザが支払ってしまう可能性がある。

クレジットカードによる支払いや月払い会費制等で支払額が僅少にとどまる場合は、破棄・転売後もサービス料金を支払っていることに気付かない恐れがある。

このため、情報家電の破棄・転売時には、当該情報家電を利用して受けていたサービスの解約を行うようユーザに周知徹底を図るほか、サービスの利用履歴をユーザに対し適時通知する等の措置を検討することが必要である。

(2) 個人情報保護

また、破棄・転売した情報家電にサービスの利用に係る個人情報が残っていると、個人情報が漏洩し、悪用される恐れがあることから、破棄・転売の際には、サービスの利用に係る個人情報を消去するようユーザを啓発することも求められる。

▽ 情報家電に残っている可能性のあるサービス利用に係る個人情報

情報家電	残っている可能性のある個人情報
テレビ電話	アドレス帳、通信料引落し口座等
コンテンツ配信用レコーダ	サービス契約情報、コンテンツ復号用秘密情報等
エアコン、照明	利用者の帰宅時間
冷蔵庫	冷蔵庫にあった食料品履歴

2. 4 家電業界とISP業界との情報交換・情報共有の必要性

情報家電も、インターネットと同様、社会的に見て「有用」であるからこそ、その普及が期待されている訳であるが、これまでに見たように、セキュリティリスクを伴うものであることもまた事実であり、家電業界、ISP業界、行政とが連携して、こうしたセキュリティリスクに迅速に対処していくための体制を構築していくことが求められる。

特に、情報家電のセキュリティ確保に関する課題の根底には、家電業界の技術者は、インターネットの技術を十分に知らず、逆に、インターネットの技術者は、家電側の要求をよく知らないという事情がある。

また、家電に関するユーザのセキュリティ意識は、コンピュータに関するユーザのセキュリティ意識に比べて低いという人的・社会的要素に起因する脆弱性も、情報家電におけるセキュリティ確保をコンピュータにおけるセキュリティ確保以上に難しくしている。

このため、全ての利用者がセキュリティに関する知識を十分持ち合わせていないということを前提に、情報家電を含む利用者端末が自律的に安全性を確保し得る技術を開発すること等により、家電業界と通信業界とが連携して、こうした脆弱性を補完する仕組みを構築していくことも重要である。

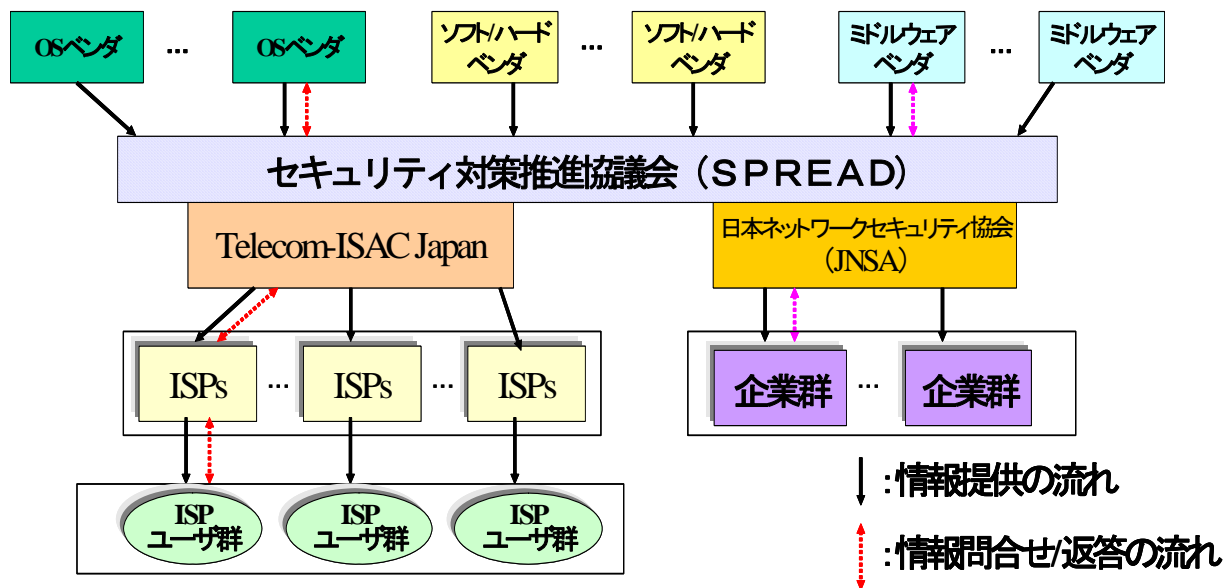
更に、情報家電を攻撃対象とするインシデントや、情報家電を踏み台とするインシデントが実際に発生した場合に、家電メーカーとISPとの間で、どの部署の誰を窓口として連絡を取り合えば良いのか、明確に決まっていない状況にある。

業界を越えた連携状況がこうした実態にある中では、ユーザは、どこに何を頼めば希望するサービスを利用することができるのか、情報家電を通じたサービスに苦情がある場合に、どこに申告すれば良いかも分からず、混乱するだけであろう。

こうした状況を克服し、情報家電の普及を促すためには、家電業界とISP業界との間で業界横断的なセキュリティ情報の共有・分析・提供・公開やユーザの啓発に関する連携の枠組みを構築することが有効であると考えられる。

2004年6月には、メーカー等で構成される非営利組織である「日本ネットワークセキュリティ協会」(JNSA)とTelecom-ISAC Japanとの間で、安全で快適なインターネット利用環境の普及とユーザ環境のセキュリティの確保・維持を推進することを目的として、「セキュリティ対策推進協議会(SPREAD)」が設立されており、行政としては、こうした民間団体による取組みを支援していくことが望ましいと考えられる。

▽ セキュリティ対策推進協議会（SPREAD）



SPREAD : Security Promotion Realizing sEcurity meAsures Distribution

特に、

- ① 情報家電を攻撃対象とするインシデントは、情報家電の操作ができなくなるだけでなく、場合によっては人命に関わる事態（情報家電の操作により、風呂を沸騰させる、部屋を冷却する等）につながりかねないこと、
- ② 情報家電を踏み台としたインシデントは、情報家電の機器の総数が多いだけに、インターネット全体に過剰な負荷を与えかねないこと、
- ③ 情報家電は、これからサービスの本格的な多様化や利用の急拡大が見込まれており、現段階でセキュリティ対策を講じないまま、脆弱な機器が大量に市場に回収った場合は、回収等が困難なこと

等から、情報家電からの大容量のトラフィックがインターネット全体に与える負荷を軽減するとともに、人命に関わる事態につながらないよう情報家電の作動範囲を規定することが求められる。

第3章 電気通信事業における 情報セキュリティマネジメント

3. 1 電気通信事業における情報セキュリティマネジメントの必要性

ISPによるインシデント対応の現状と課題については第1章で、ユビキタスネット社会におけるセキュリティ確保策については情報家電に焦点を当てて第2章で、それぞれ検討を加えた。

ここでは、サービスの継続性とユーザ（法人ユーザ及び個人ユーザ）のデータ保護を確保する観点から、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講じていくべきかについて、検討することとする。

情報そのものや情報システムは、その重要性の割には、我が国経営陣の評価が低いと言わざるを得ない。

金銭であれば、経営者や財務部門の一定のランク以上の従業者が管理するのに対し、情報や情報システムの管理については、社内の若いセキュリティ技術者や社外のセキュリティベンダに任せたまま、自らは管理に関わらない経営者も存在するのが実情である。

しかしながら、情報システムが破られ、情報セキュリティが侵害された場合の被害は計り知れない。

このため、まず、情報セキュリティマネジメントやセキュリティ人材の重要性に関し、経営陣が、これまでの認識を改めるとともに、セキュリティポリシーを策定し、これに従って従業者教育やセキュリティ対策を実施していくことが必要不可欠である。

特に、自らの電気通信設備をユーザの通信の用に供する電気通信事業者は、「通信の秘密」に属する情報を始めとして多くのユーザ情報を取り扱うものであり、情報資産をより適切に管理することが求められること等から、関係法令をも踏まえ、セキュリティポリシーを策定し、セキュリティ対策を実施していくことが求められる。

この点に関しては、国際標準化機構（ISO）と国際電気標準会議（IEC）が2000年12月に策定した国際規格（ISO/IEC 17799）があり、これを基に、一般の企業を対象とした汎用的な情報セキュリティマネジメントシステム（ISMS）とその適合性評価制度の整備・展開が、各国で進んでいる。

また、国際電気通信連合（ITU）では、我が国が中心となって検討を進め、電気通信事業分野を対象としたISMS（ISMS-T）を2004年7月に勧告している。

一般の企業を対象とする汎用的なISMSについては、2005年6月に改訂版が発行されたところであり、これを踏まえ、ISMS-Tについても、今後、改訂が必要となろう。

更に、ISMSは国際規格であり、今後、ある国でISMSに適合していると評価された組織が、他国においてもISMSに適合しているものと評価されるよう、国際

的な認証の枠組みを構築していくことも展望される。

このため、ISMS-Tの改訂作業に積極的に取り組むことは、大きな意義を有するものと考えられる。

そこで以下では、ISMSとISMS-Tの概要をみた上で、我が国における今後の活動の方向性について検討することとする。

3. 2 ISMSの概要と最近の改訂作業の動向

3. 2. 1 ISMSの概要

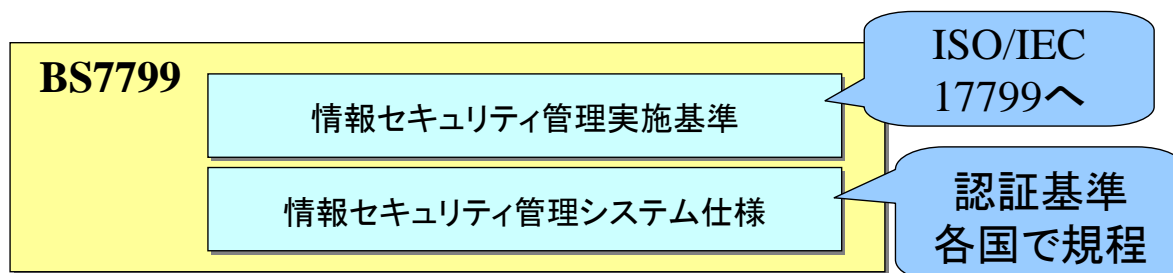
ISOとIECが2000年12月に国際規格として策定したISMSであるISO/IEC17799は、1995年に英国で国内規格として策定されたBS7799を国際規格化したものであり、この国際規格では、情報セキュリティマネジメントに影響のある127の管理策（Control）を次の10のマネジメント領域に分類している。

▽ ISMS (ISO/IEC17799) のマネジメント領域

1. セキュリティ方針 (Security policy)
2. セキュリティ組織 (Security organization)
3. 資産の分類及び管理 (Asset classification and control)
4. 人的セキュリティ (Personnel security)
5. 物理的及び環境的セキュリティ (Physical and environmental security)
6. 通信及び運用管理 (Communications and operations management)
7. アクセス制御 (Access control)
8. システムの開発及び保守 (Systems development and maintenance)
9. 事業継続管理 (Business continuity management)
10. 適合性 (Compliance)

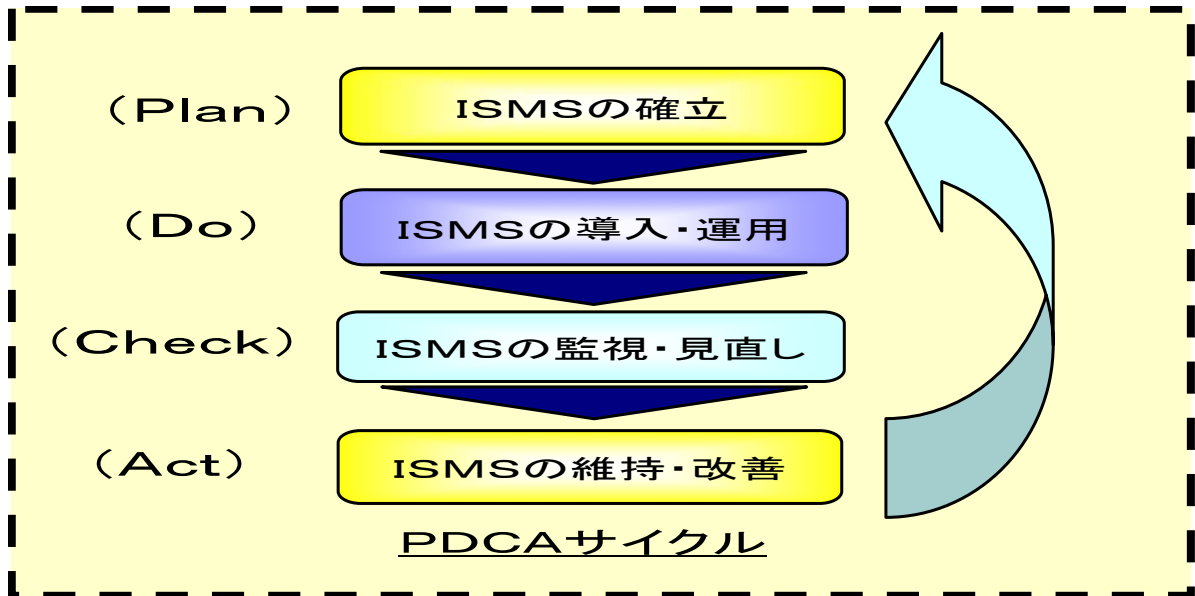
このISO/IEC17799では、BS7799の「管理規格」のみが国際規格化され、ISMSに適合しているか否かを評価する際の基準となる「認証規格」については、各国がその国情に適した形で策定することとされている。

▽ BS7799とISO/IEC17799



各国で実施されているISMS適合性評価は、評価を希望する組織が、ISMSを確立し（Plan）、導入・運用し（Do）、監視・見直しを行い（Check）、維持・改善を行う（Act）というP-D-C-Aサイクルを実施していることを、第三者（審査機関）が評価する、という形で実施されており、評価は企業単位ではなく、組織（事業所）単位で行われている。

▽ PDCAサイクル

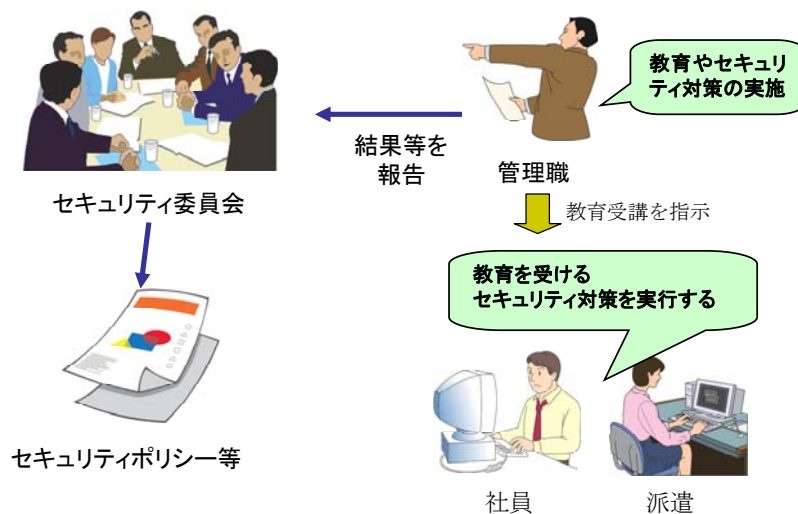


3. 2. 2 ISMS適合性評価

実際のISMS適合性評価に当たっては、まずは組織自身の中で次の①から④のPDCAサイクルを実行し、当該組織のISMSを確立することになる。

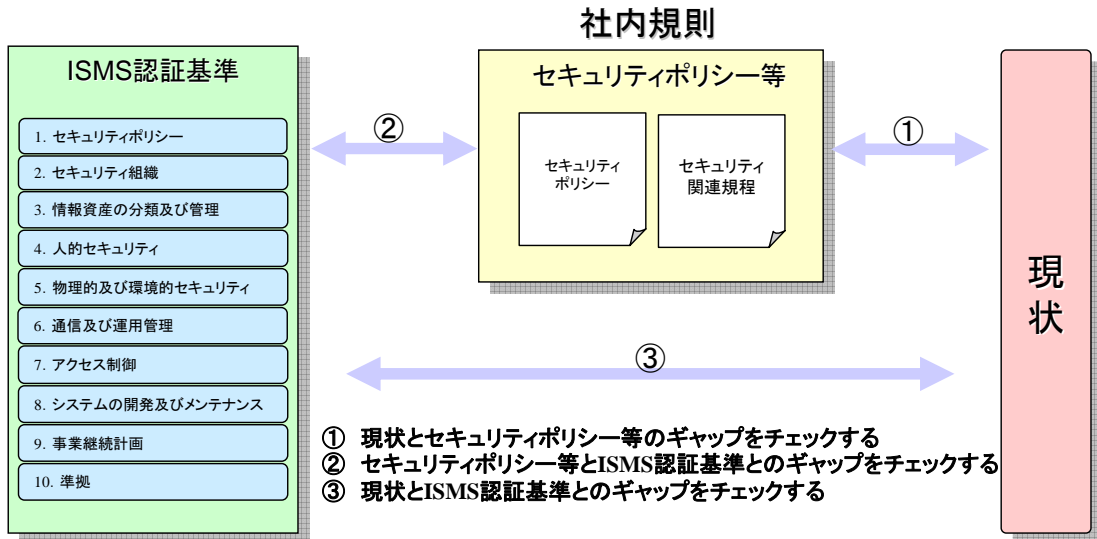
- ① 情報セキュリティ関連ルール（セキュリティポリシー及び実施手順）（以下、「セキュリティポリシー等」という。）を策定する。（Plan）
- ② セキュリティポリシー等に沿った社員教育やセキュリティ対策等を実施・運用する。（Do）

▽ ISMS適合性評価－第2段階（Do）



- ③ セキュリティポリシー等がISMS認証基準と整合しているか、また、セキュリティポリシー等に沿って社員教育やセキュリティ対策が実施されているか等を監査する。（Check）

▽ ISMS 適合性評価—第3段階 (Check)



- ④ 監査等の結果を基に、セキュリティポリシー等や実施・運用を見直し、改善する。(Act)

次に、ある組織が自ら確立した ISMS に適合しているか否かを評価するに当たっては、審査の申請を受けた第三者（審査機関）において、

- ① ISMS 認証基準と文書の整合性
- ② セキュリティポリシー等と現状との整合性

について審査を行い、当該組織における ISMS が適切と判断できれば、認証を与えることになる。

ここでは、審査を希望する組織（事業所）、その組織における ISMS 認証基準とその適用範囲を確認の上、当該組織の責任者による承認が適正になされているか否か、という点のみを審査することになる。

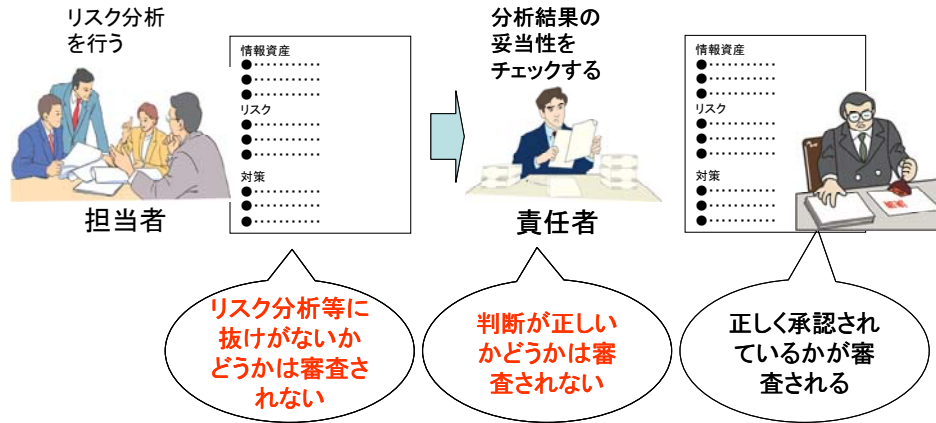
換言すれば、第三者による審査においては、

- ① 審査対象となる組織自身が実施するリスク分析等に抜けがないかどうか、
- ② 責任者による判断が正しいかどうか、

という点は、審査対象とならないものである。

すなわち、第三者の審査は、組織の中で P-D-C-A サイクルが適正に実施されているか否かを評価するものであり、組織内において一定水準以上のセキュリティ対策が実施されていることを保証しているものではない点に、留意する必要がある。

▽ I S M S 適合性評価—第三者による審査



3. 2. 3 I S M S の改訂作業の動向

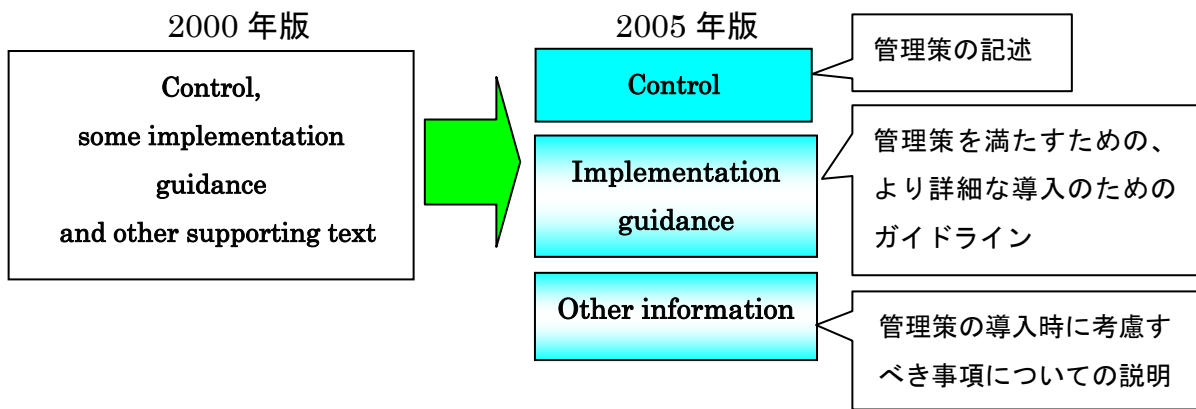
2000年12月に策定されたISO/IEC17799（以下「2000年版」という。）は、2001年から改訂作業が開始され、23カ国から2,500以上の意見が提出された。

これを受けて改訂作業が進められたISMS（以下「2005年版」という。）では、管理策（Control）が127から135に増え、「情報セキュリティに係るインシデントのマネジメント」（Information security incident management）というマネジメント領域が新たに括り出されている。

また、2005年版では、規定の仕方においても、管理策（Control）、導入のためのガイドライン（Implementation guidance）、関連情報（Other information）という3つの層に分けて規定されており、ISMSを確立し、運用しようとする組織にとって導入しやすいものにする工夫が施されている。

▽ 2000年版と2005年版の規定の比較

2000年版	2005年版
セキュリティ方針	Security policy
セキュリティ組織	Organising information security
資産の分類及び管理	Asset management
人的セキュリティ	Human resources security
物理的及び環境的セキュリティ	Physical & environmental security
通信及び運用管理	Communications & operations management
アクセス制御	Access control
システムの開発及び保守	Information systems acquisition, development and maintenance
	Information security incident management
事業継続管理	Business continuity management
適合性	Compliance



3. 2. 4 ISMSの今後の課題

2005年版は、2005年の6月に発行されているが、今後のISMSの課題を整理してみると、次のとおりである。

(1) 産業分野別のISMSの策定

守るべき情報やマネジメントの対象となる資産は、産業分野ごとに異なるものであり、各業界の特性によっては、その業界に固有のISMSが示されることが望ましいと考えられる。

実際、医療分野についてはISO/IEC 27799が、金融分野についてはISO/TC 68が、電気通信事業分野についてはITUにおいてISMS-Tが、それぞれ策定されている。

ISMS-Tについては、3.3で検討する。

(2) ISMSの確立・運用に対する支援

ISMSを確立し運用しようとする組織が直面しがちな次の課題について、情報を共有し、課題解決に向けたガイドライン作り等の支援活動を行っていくことも必要になるものと考えられる。

- ① 組織内部の情報セキュリティのための体制
- ② 社員の教育訓練
- ③ 内部監査
- ④ 個人情報保護等、法令上の要求事項への対応
- ⑤ 技術上の対策との連携や技術上の対策の適用方法

こうした支援活動も、業界の特性に応じて、業界別に行うことが適当であろう。

(3) 国際的なクロスボーダー認証の実現

I S M S は国際規格であることから、ある国で I S M S に適合していると評価された組織は、本来、他国においても同様に評価されるべきものであり、こうした国際間の認証の枠組みを構築することも、今後の課題になるものと考えられる。

3.3 ISMS-Tの概要と今後の改訂の方向性

3.3.1 ISMS-Tの概要

ITUでは、2001年以来、我が国が中心となって検討を進め、2004年7月に電気通信事業分野を対象としたISMS（ISMS-T<X.1051>）を勧告した。

これは、電気通信システム及び電気通信サービスを対象として、ISMSを実装していくに当たっての要求条件を規定しているものである。

一般の企業を対象とする汎用的なISMS（ISO/IEC17799）と比べると、次の5つのマネジメント領域について、電気通信事業分野に固有の管理策（Control）の充実が図られている。

▽ ISMS-Tで管理策の充実が図られているマネジメント領域

3. 資産の分類及び管理（Asset classification and control）
5. 物理的及び環境的セキュリティ（Physical and environmental security）
6. 通信及び運用管理（Communications and operations management）
7. アクセス制御（Access control）
8. システムの開発及び保守（Systems development and maintenance）

また、汎用的なISMSと比べて変更を加えていない管理策（Control）についても、電気通信事業分野に固有の実装要件をImplementation Requirementsとして追加している。

▽ 電気通信事業分野における実装要件の例

資産の分類及び管理（Asset classification and control） 管理策（Control） それぞれの資産を明確に識別しなければならない。また、全ての重要な資産について目録を作成し、維持しなければならない。	ISMS-TとISMSとで変更無し
電気通信分野における実装要件（Implementation requirements for Telecom） 各電気通信事業者に関する重要な資産について目録を作成し、維持すること。電気通信事業者に関する資産には多くの種類があり、それには以下のものが含まれる。 a) 交換設備資産 b) 伝送設備資産 c) 運用設備資産 d) 電気通信サービス資産 e) 人々とその資格と能力 f) 組織の評判やイメージといった無形資産	

3.3.2 ISMS-Tの今後の改訂の方向性

(1) 改訂ISMSを参照する必要性

現行のISMS-Tは、2000年版のISMSを踏まえてITUで勧告化されたものであるが、今後は、2005年版を踏まえ、改訂作業が進められることが想定される。

▽ ISMS（2000年版・2005年版）とISMS-Tの管理策の比較

2000年版 ISMS	2005年版 ISMS	ISMS-T
セキュリティ方針	Security Policy	
セキュリティの組織	Organizing information security	Organizing Information security
資産の分類及び管理	Asset management	Asset management
人的セキュリティ	Human resources security	Human resources security
物理的及び 環境的セキュリティ	Physical & environmental security	Physical & environmental security
通信及び運用管理	Communications & operations management	Communications & operations management
アクセス管理	Access control	Access control
システム開発及び保 守	Information systems acquisition, development and maintenance	Information systems acquisition, development and maintenance
	Information security incident management	
事業継続計画	Business continuity management	
適合性	Compliance	

(2) 現行ISMS-Tへの追加項目の検討

また、現行のISMS-Tについては、例えば、「適合性」(Compliance)について、電気通信事業分野に固有の管理策は規定されていない。

2000年版の「適合性」の領域には、「知的所有権」、「組織の記録の保護」、「データの保護及び個人情報の保護」、「情報処理施設の誤用の防止」、「暗号による管理策の規制」等が規定されているが、電気通信事業者に対しては、これら以外にも次のような法令上の要求事項があることから、今後、ISMS-Tにこれらの要素を追加すべきか否かを検討する必要がある。

- ① 取扱中に係る通信の秘密は、侵してはならないこと。取扱中に係る通信に関して知り得た他人の秘密を守らなければならないこと。（電気通信事業法第4条）
- ② 電気通信役務の提供について、不当な差別的取扱いをしてはならないこと。（電気通信事業法第6条）
- ③ 災害の予防若しくは救援、交通、通信若しくは電力の供給の確保又は秩序の維持のために必要な事項を内容とする通信等を優先的に取り扱わなければならないこと。（電気通信事業法第8条）
- ④ 他の電気通信事業者から接続請求を受けたときは、原則として、これに応じなければならないこと。（電気通信事業法第32条）
- ⑤ 利用者又は他の電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること。他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること。（電気通信事業法第41条）
- ⑥ 利用者の端末設備との接続によって、電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること。電気通信設備を利用する他の利用者に迷惑を及ぼさないようにすること。利用者の端末設備との責任の分界が明確であるようにすること。（電気通信事業法第52条）
- ⑦ 個人情報保護法及び電気通信事業における個人情報保護に関するガイドライン（平成16年8月31日総務省告示第695号）を遵守すべきこと 等。

以上のような法令上の要求事項は、「適合性」の領域だけでなく、「資産の分類及び管理」、「物理的及び環境的セキュリティ」、「通信及び運用管理」、「アクセス管理」、「システム開発及び保守」、「インシデントのマネジメント」、ひいては「セキュリティ方針」の領域にまで影響を及ぼす可能性があることから、現行のISMS-Tをこうした観点から見直し、充実させていくことが求められる。

3. 4 我が国における今後の活動の方向性

3. 4. 1 I S M S - T の国内における展開

前述したように、I S M S - T は、I T U において我が国が中心になって検討を進め、我が国の提案が採用されて国際的に勧告されているものであり、今後は、こうした国際勧告を国内で展開していくことが適当であると考えられる。

その際には、2005年版のI S M S が2005年6月に発行されていることから、その内容を踏まえることを始め、電気通信事業分野に固有の法令上の要求事項を充たすことのできるよう、検討を加えていくことが必要である。

3. 4. 2 国内における普及促進

I S M S - T を国内で普及促進させていくためには、これに従って情報セキュリティマネジメントを行おうとする電気通信事業者が直面しがちな次の課題について、情報の共有や課題解決に向けたガイドライン作り等の支援活動を行っていくことが適当である。

- ① 組織内の情報セキュリティのための体制
- ② 社員の教育訓練
- ③ 内部監査
- ④ 法令上の要求事項への対応
- ⑤ 技術上の対策の適用方法

特に、中小規模の電気通信事業者や地方で事業を展開している電気通信事業者にとっては、派遣社員を含めた人的セキュリティの確保、アクセス制御の厳重化等において、大規模事業者や都市部の事業者に比べ困難を伴う面もあることから、行政においては、既存及び新規の施策を組み合わせ、これらの事業者に対し、より大きなインセンティブを付与することを検討するべきである。

3. 4. 3 国際貢献

I S M S と同様、I S M S - T についても、今後、ある国でI S M S - T に適合していると評価された電気通信事業者（又はその中の一組織）が、他国においてもI S M S - T に適合しているものと評価されるよう、国際間の認証の枠組みを構築していくことが展望される。

このため、I S M S - T については、国内における普及促進を図るだけでなく、国際機関に積極的に提案を行うことができれば、大きな意義を有するものと考えられる。

換言すれば、国際的にも評価されるよう、ISMS-Tの国内における普及促進を図るとともに、国際機関への提案を準備することが求められるところであり、官民の知見を結集して、ISMS-Tの充実を図っていくことが重要であると考えられる。

2005年秋のITUの会合では、ISMS-Tの修正勧告の検討が開始される可能性があり、我が国としても、ITUにおける検討に積極的に参画し、貢献していくことが期待される。

第4章 セキュリティ人材育成

4. 1 我が国におけるセキュリティ人材の現状

あらゆるセキュリティ対策を講じる上で基盤となるのは、人材である。

2003年のITU調査によれば、ブロードバンド通信の「安さ」と「速さ」において、我が国は世界1との評価を受けているが、こうしたブロードバンドの進展状況に比べ、ブロードバンドを支えるセキュリティや、セキュリティ対策を講じる上で不可欠な人材が十分かどうかについては、疑問無しとしない。

そこで以下では、まず、我が国のセキュリティ人材の現状を見ておくこととする。

4. 1. 1 労働市場における情報処理技術者の「供給」面

電気通信業界に限定せず、我が国の労働市場全体で見ると、就業人口が高齢化し、かつ減少する中で、情報処理技術者については30代以下が約8割を占めているのが実態であり、若年就業者の減少が情報処理技術者の絶対的な不足をもたらす恐れが指摘されている。

▽ 就業人口の減少

- ▶ 総人口は2006年以降長期的減少へ（生産年齢人口（15～64歳）は1996年から減少）
- ▶ 高齢者人口（65歳以上）は2014年には総人口の4分の1超へ
- ▶ 就業人口は団塊世代が60歳になり始める2年後以降急速に減少へ

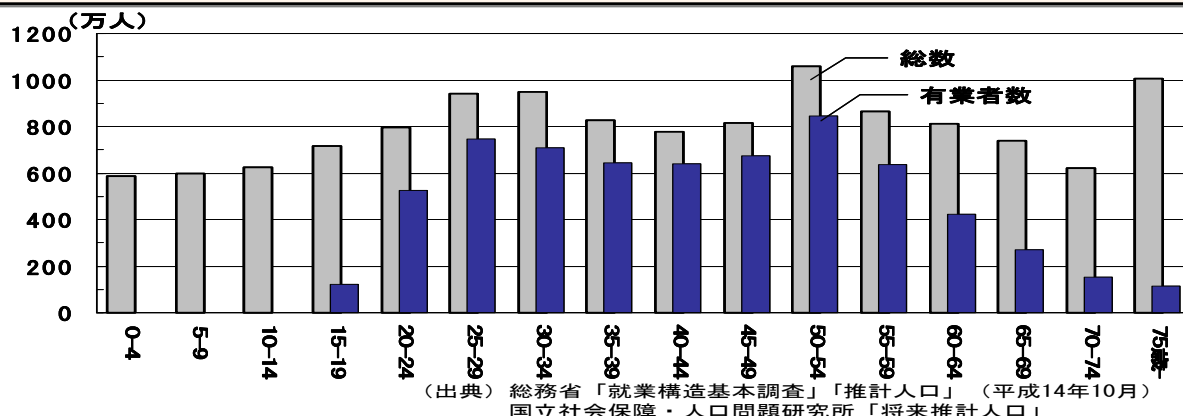
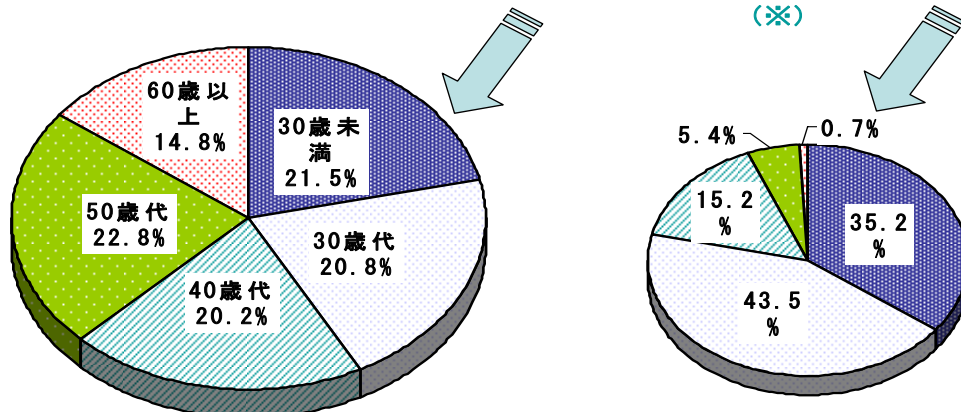


図 情報処理技術者の年齢構成

総人口 12,744万人 > 有業者 6,501万人 > 情報処理技術者 92万人 (※)

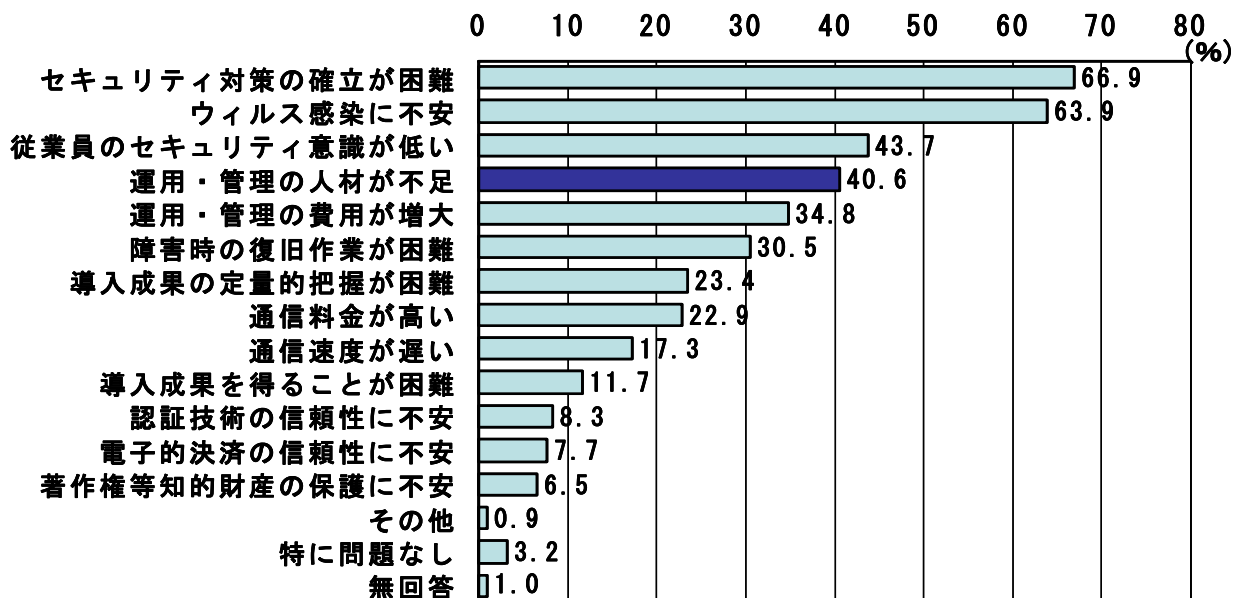


※ 情報処理技術者：情報処理技術に関する高度の専門的知識・経験をもって、システムの分析、設計の仕事に従事するもの及びプログラムの設計、作成についての技術的な仕事に従事するもの
(出典) 総務省「就業構造基本調査」及び「推計人口」より加工 (平成14年10月)

4. 1. 2 労働市場における情報処理技術者の「需要」面

他方、企業側から見ると、情報通信ネットワークの利用において、セキュリティ対策、ウイルス感染に続いて、従業員のセキュリティ意識の低さや人材不足が、懸念事項として挙げられている。

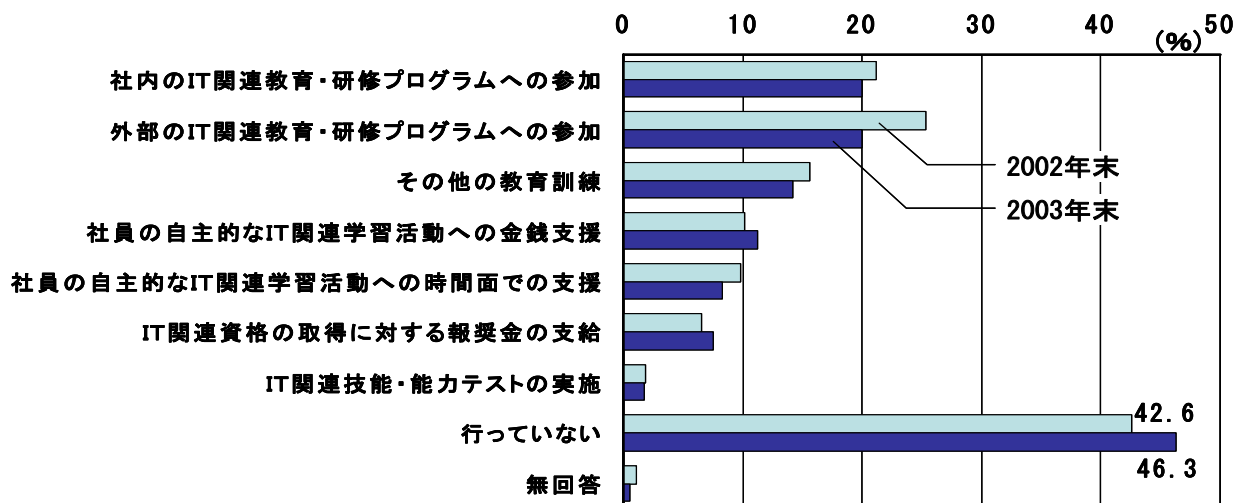
▽ 企業における情報通信ネットワーク利用上の問題点



(出典) 総務省「通信利用動向調査」(平成15年)

それにもかかわらず、企業における人材育成の状況をみると、人材育成を「行っていない」とする企業が4割以上を占めているのが実情である。

▽ 企業における人材育成



(出典) 総務省「通信利用動向調査」(平成15年)

2003年に開催された総務省の「情報通信ソフト懇談会」では、企業における専門的ICT人材は42万人、そのうちセキュリティ人材は12万人不足していると推計されている。

▽ 企業における専門的ICT人材の不足数

	所要数	現存数	不足数
上級人材	36万人	10万人	<u>26万人</u>
中級人材	92万人	76万人	<u>16万人</u>
セキュリティ人材 (上級・中級の中に含まれる)	25万人	13万人	<u>12万人</u>
プロジェクトマネージャー・ITアーキテクト・CIO (上級の中に含まれる)	10万人	1万人	<u>9万人</u>

※ ICT人材（上級人材、中級人材、セキュリティ人材）の現状について、平成15年に総務省で開催された「情報通信ソフト懇談会」の人材育成WGにおいて推計。また、プロジェクトマネージャー、ITアーキテクト、CIOの3類型の人材の現状についても同WGの主要メンバーの意見を踏まえ、同様の手法により推計。

※ 上級人材：専門的な知識、技能を一通り備える。複雑なシステム等の設計及び運用が可能。
中級人材：特定分野の基本的な知識、技能を備える。比較的容易なシステム等の設計及び運用が可能。

また、「日経ITプロフェッショナル」の2004年6月調査によれば、2万人を超えるIT技術者の46%が、「人の助けを借りながら業務を遂行できる」水準との指摘もある。

4. 1. 3 我が国電気通信事業者におけるセキュリティ人材の現状

次に、我が国の電気通信事業者において、実際にセキュリティ人材が充足しているか否かについて見ておくこととする。

インターネットは、ISP等のネットワークが相互に接続したネットワークであり、あるISPにおけるICT障害が他のISPにも影響を及ぼす可能性がある。

インターネットが社会経済活動を支えるインフラとなっている現状にかんがみると、ISP等の電気通信事業者において、セキュリティ人材が十分に確保されているか否かは、国民の社会経済生活を支える上で非常に重要である。

そこで、総務省では2005年4月に、(社)電気通信事業者協会、(社)テレコムサービス協会、(社)日本インターネットプロバイダー協会、及び(社)日本ケーブルテレビ連盟の加盟事業者に対し、セキュリティ人材^(注14)についてアンケートを行った。

(注14) このアンケートにおける「セキュリティ人材」としては、ウィルスチェック、コンテンツフィルタリング、不正アクセス監視、セキュリティ診断、リモートアクセス環境検査等のセキュリティサービスをユーザに対し提供できる従業者のほか、自社のネットワーク運用の障害予防、当該障害の監視・検出・制御、障害の再発防止等を講じることのできる従業者を想定している。

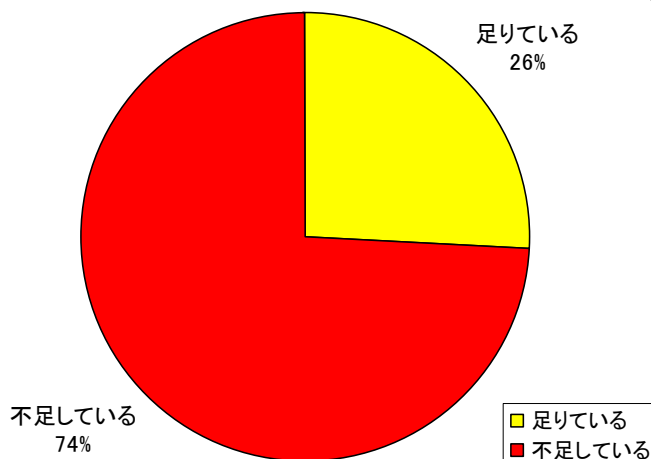
その結果は次のとおりである。

(1) セキュリティ人材の充足感

まず、セキュリティ人材の不足感についてアンケートをとったところ、約4分の3の事業者において、セキュリティ人材の不足している状況にある。

▽ セキュリティ人材の不足感

<有効回答数197社>



また、有効回答を寄せた197社が現在雇用しているセキュリティ人材は4306人であり、今後追加したいセキュリティ人材の数は全体で1324人と、現在雇用しているセキュリティ人材を31%増加させたいという結果になっている。

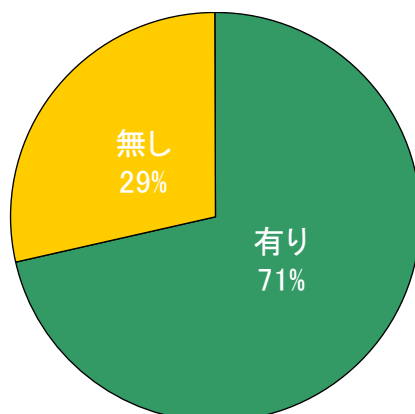
(2) セキュリティ人材育成の現状

次に、電気通信事業者において、セキュリティ人材をどのように育成しているかについてアンケートをとったところ、7割の事業者が社員のセキュリティ教育に取り組んでいる状況にある。

逆に言えば、3割にのぼる事業者は社員のセキュリティ教育を実施していない状況にあり、行政においては、セキュリティに係る人材育成の重要性について、事業者の意識を喚起すべきであると考えられる。

▽ 電気通信事業者のセキュリティ教育の実施状況

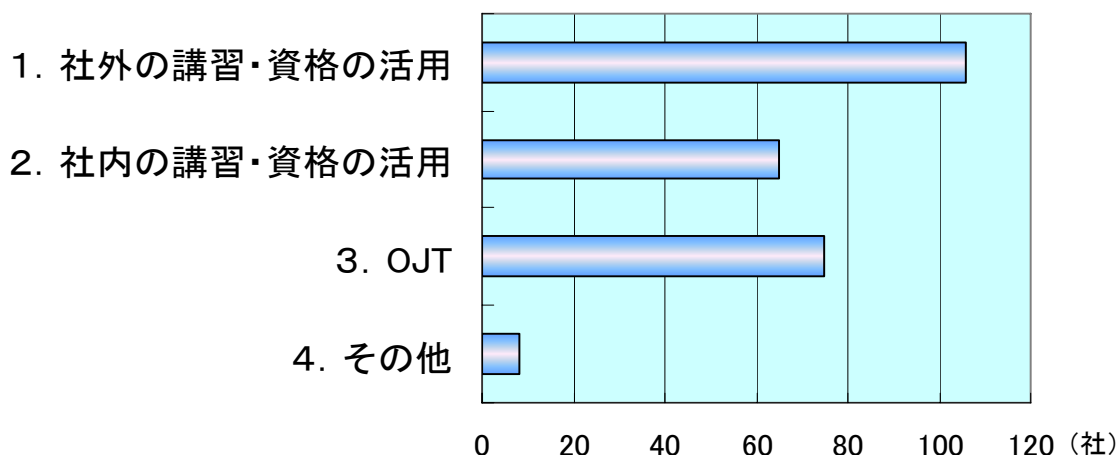
<有効回答数197社>



セキュリティ教育を実施している事業者について、セキュリティ教育の実施方法を見ると、社外の講習・資格の活用やOJTによる教育の割合が高くなっている。

▽ セキュリティ教育の実施方法

<有効回答数197社>



電気通信事業者における人材育成の実態をより詳細に見ると、中核となるセキュリティ人材を社外の研修事業者による講習等に派遣して技能・知識を習得させ、その中核となる人材が、通常の業務運用の中で、他の従業員に対し、講習等で得られた技能・知識を伝えていく、といった形で人材育成を行っており、特に系統立てた育成システムを行っていない場合が多い。

特に、中小規模の電気通信事業者においては、セキュリティのためだけに専任者を配置するというよりも、通常のネットワーク運用業務やシステム構築の一環として、事業者内部のセキュリティ確保や、ユーザに対するセキュリティサービスの提供を行っている場合が多いのが実情である。

これは、実際のネットワーク運用やシステム構築に従事していないと、「生きた」技術の修得が見込めず、結果として、セキュリティ人材の育成もできないという事情によるものである。

他方で、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激しく、それに応じてセキュリティ事案も多様化しており、社外の講習等に人材を派遣してみても、講習等で修得した技術だけでは対応できないインシデントが発生するケースが多く、結局は、現実に追われる「たちごっこ」ではないのか、という悩みを抱えている事業者も存在する。

現実の「後追い」ではなく、セキュリティ業務により積極的に取り組むためにセキュリティ人材を育成しようとする場合においても、セキュリティ人材は、以下のように技術から法令まで多くの技能・知識を習得することが必要であり、その育成には多くの時間と高額な費用を要するのが実情である。

▽ セキュリティ人材が修得すべき技術・知識の例

情報処理技術、ネットワーク技術、インシデント対応技術、監視技術、侵入検知システム（IDS）、ファイアウォール技術、トラヒック状況解析、ISMS、リスクマネジメント技術、国際規格、国内規格、国内法令、外国法令、等

実際、外部業者によるセキュリティ講習等は、期間が4～5日、費用が1回1人当たり40～50万円、高価なものでは80～100万円かかる場合がある。

このため、一定規模以上の電気通信事業者では、年間計画を組んだ上で、半強制的に従業者を社外の講習等に参加させることができているが、中小規模の電気通信事業者の中には、派遣期間及び費用の面で、自社のネットワーク運用において中核を担う従業者を社外の講習等にはとても参加させられないという事情も散見される。

加えて、地方においては、受講者が集まらないことから外部業者によるセキュリティ講習等がそもそも開催されず、地方で事業を展開している電気通信事業者にとっては、従業者を社外のセキュリティ講習等に参加させようと思えば、東京か大阪まで従業者を出張させなければならないことから、余計に費用がかかるという側面もある。

また、そもそもインターネットの分野は、技術革新の進展が急激であることから、人材育成も継続的な取り組みが必要である一方、社外の講習等に自社の従業者を派遣してみても、それによって得られるセキュリティ水準がどれ程かについての判定が難しく、結果として、電気通信事業者によるセキュリティ人材の育成を鈍らせる要因の1つとなっている。

このため、電気通信事業者の中には、特に地方において従業者にセキュリティ技術を習得させるための「場」を用意して欲しいとの要望があるほか、修得したセキュリティ技術の水準を評価できる仕組みを構築して欲しいとの要望もある。

このように、我が国電気通信事業者のセキュリティ人材の育成については、様々な課題を抱えているのが実情である。

4. 2 他のICT先進国におけるセキュリティ人材の現状と育成策

4. 2. 1 米国におけるICT人材数

上記において、我が国におけるセキュリティ人材の現状を見た訳であるが、これとの対比で米国の状況を見ておきたい。

この点については、1999年に米国商務省がICT人材について公表した資料があり、次の点が伺われる。

- ① ICT人材は、1996年から2006年までの10年間で、150万人から260万人まで増加させることが必要であるとしていること。
- ② 他の業界への転職者数を差し引くと、1996年から2006年までの10年間で、110万人を超えるICT人材の増加が必要であるとしていること。
- ③ ICT人材のうち、セキュリティ人材はComputer Scientistsに分類されており、1996年から2006年までの10年間で、25万人弱のComputer Scientistsの増加が必要であるとしていること。

▽ 米国のICT人材数

米国商務省発表資料(1999年)

単位: 千人

	1996年	2006年	Change, 1996-2006		
			Net Replacements	New Jobs	Total Growth
Computer Scientists	212	461	19	249	268
Computer Engineers	216	451	15	235	250
Systems Analysts	506	1,025	34	520	554
Computer Programmers	568	697	177	129	306
Total	1,501	2,634	244	1,134	1,378

<http://www.technology.gov/Reports/TechPolicy/digital.pdf>

4. 2. 2 米国におけるセキュリティ人材の育成策

以上のように、米国では、既に1999年の時点で、110万人を超えるICT人材の増加が必要とされていた点には、我が国としても注目する必要があると考えられる。

実際、米国では、1998年5月の大統領指令63号（「PDD63」^(注15)という。）を受けて、国家インフラ防護センター（NIPC）^(注16)や情報共有分析センター（ISAC）^(注17)等を創設したほか、国家の情報インフラの脆弱性を低減するためのセキュリティ人材育成策として、国家安全保障局（NSA）^(注18)においてCAEIAE^(注19)と呼ばれる人材育成プログラムを実施している。

(注15) PDD63: Presidential Decision Directive 63

(注16) NIPC: National Infrastructure Protection Center

(注17) ISAC: Information Sharing and Analysis Center

(注18) NSA: National Security Agency

(注19) CAEIAE: The National Centers of Academic Excellence in Information Assurance Education

これらのプログラムには、4年生の大学生と大学院生が応募することができ、国防総省の情報保証奨学金^(注20)やSFS^(注21)の奨学金制度への申請権が与えられている。

▽ CAEIAEプログラム (SFSの奨学金を受けた場合)

対象	4年生の大学生と大学院生
対象期間	最大2年間
奨学金	必要な全ての経費、書籍、授業料、部屋代など
給付金	大学生：年間最大 8,000 ドル 大学院生：年間最大 12,000 ドル
条件	奨学金受給期間又は1年のいずれか長い期間、連邦機関に勤務

(注20) 国防総省情報保証奨学金： Department of Defense Information Assurance Scholarship Program

(注21) SFS： Federal Cyber Service Scholarship for Service Program

4. 2. 3 シンガポールにおけるセキュリティ人材の育成策

シンガポールにおいても、情報通信開発庁 (IDA) において、「重要な情報通信技術資産プログラム」(CITREP^(注22)) と呼ばれる ICT 人材育成のプログラムを推進している。

(注22) CITREP： Critical Infocomm Technology Resource Program

このプログラムは、電気通信事業者や情報通信ネットワークを活用する組織が必要とする情報システム (情報セキュリティを含む。) に関する教育訓練又は資格取得の費用について、一定の助成を行うものである。

助成対象と助成上限額は次のとおりである。

▽ CITREPの助成対象と助成上限額

助成対象	教育訓練を受け、又は資格を取得しようとする個人等
助成上限額	教育訓練に係る費用の最大70% (S\$3,500：約23万円) まで 資格試験に係る費用の最大70% (S\$1,000：約6.5万円) まで

▽ CITREPの対象資格試験例 (情報セキュリティ関係：一部分)

CISSP CBK Review Seminar	Security Certified Network Professional (SCNP)
Check Point Certified Security Administrator & Certified Nokia Security Administrator - ECS (VPN-04)	Security Technology and Management Course (eSTEEM)
Computer Hacking Forensic Investigator	Sun Certified Security Systems Administrator - IM
CSPFA CISCO Secure PIX Firewall Advanced	Sun Certified Security Administrator for the Solaris Operating Environment - ECS (SC-300)
Developing Secure Internet Applications	Sun Network Intrusion & Detection - ECS (SC-345)
eXtreme Hacking	Ultimate Hacking
Linux Network Administration and Security	Web Application Security Training
Securing Cisco IOS Networks	

4.3 我が国におけるセキュリティ人材育成

4.3.1 セキュリティ人材に関する我が国電気通信事業者の要望

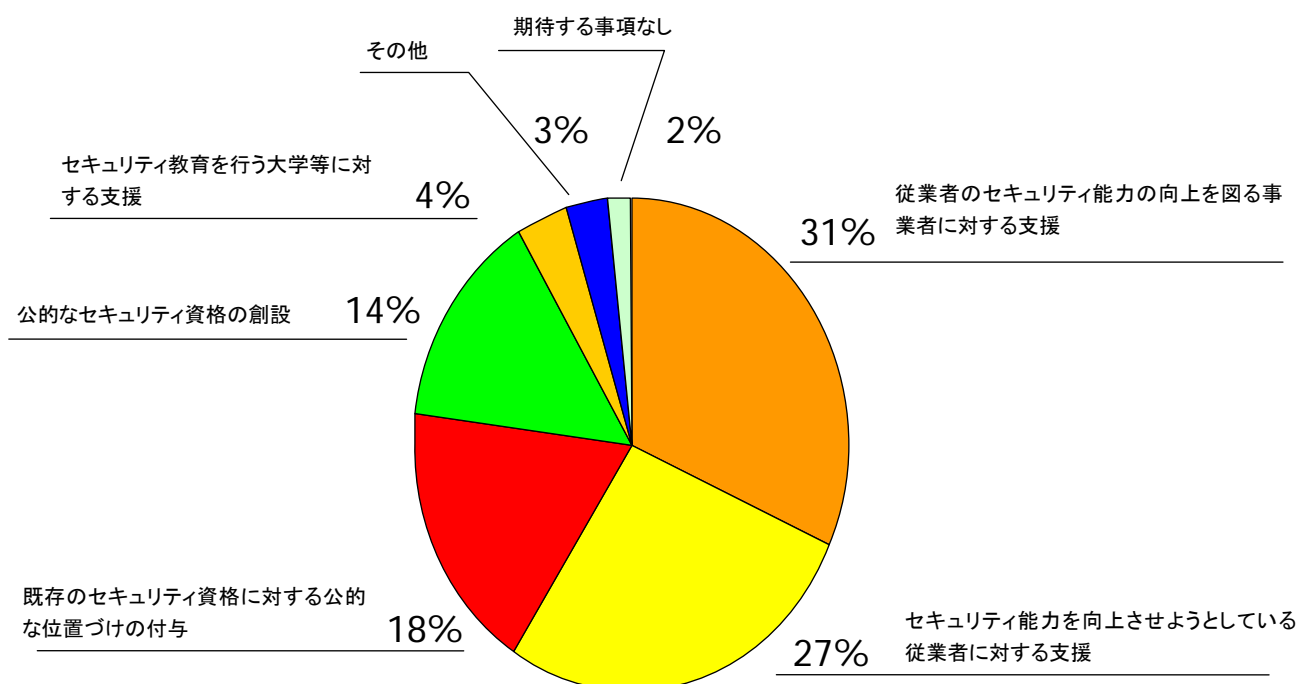
上述のように、米国やシンガポールでは、セキュリティに関する講習を受講しようとする個人又はセキュリティ資格を取得しようとする個人に対し、一定額を助成する形で行政による人材育成が進められている。

これに関しては、我が国電気通信事業者に対するアンケートの回答をみても、セキュリティに関する講習や資格（以下「セキュリティ講習等」という。）について、費用面で助成や公的な位置付けを求めるものが多くなっている。

- ① 従業者のセキュリティ能力の向上を図る電気通信事業者に対する支援
- ② セキュリティ能力を向上させようとする従業者に対する支援
- ③ 既存のセキュリティ資格に対する公的な位置付けの付与
- ④ 公的なセキュリティ資格の創設

▽ セキュリティ人材に関する電気通信事業者の要望

<有効回答数197社>



セキュリティ資格については、下表のとおり、民間企業によるものと公的なものとを問わず、既に多くのものが存在しており、これらのうち、インターネットの分野においては、どれが有用かを評価する際の基準を示すことの方が有益と考えられる。

▽ セキュリティ資格の例

略称、通称	正式名称	主催者	発足	期限	取得形態、教育時間	取得費用
NISM	Network Information Security Manager ネットワーク情報セキュリティマネージャー	NISM推進協議会 (CIAJ、テラ協、TCA、ARIB、JAIPA、テ協、NS協、TTCで構成)	2001	2年	「講習+認定試験」のみ (講習は2日間と3日間 (コースによる))	<ul style="list-style-type: none"> ■ ネットワークセキュリティ基礎 (69,300円/63,000円) ■ ネットワークセキュリティ実践 (173,250円/157,500円) ■ サーバセキュリティ実践 (184,800円/168,000円) ■ セキュリティ監視実践 (184,800円/168,000円) ■ セキュリティポリシー実践 (80,850円/73,500円) ■ セキュリティ監査実践 (80,850円/73,500円) ※ 金額は一般価格/会員価格
SS	情報セキュリティアドミ ンストラータ試験	(財)日本情報処理開 発協会 (~2003/12) (独)情報処理推進機 構 (2004/1~)	2001	なし	「認定試験」のみ	5,100円 (受験料)
CISSP	Certified Information System Security Professional	International Information Systems Security Certification Consortium, (ISC)2	1989	約120時間/ 3年間の教育 単位取得が 必要	「講習+認定試験」「認定 試験」のいずれも可。 講習は8時間×5日	630,000円 (受講料 (受験費用込み)) 68,500円 (試験のみの場合)
Security+	Security+	The Computing Technology Industry Association, CompTIA	2003	なし (試験内容は 2年で改訂)	「講習+認定試験」のみ 講習は6日間	504,000円 (受講料 (受験費用込み)) 28,665円 (試験のみの場合)
CISM	Certified Information Security Manager 公認情報セキュリティマ ネージャー	Information Systems Audit and Control Association, ISACA (情報システム コントロール協会)	2002	5年	「認定試験」のみ ただし、 更新時に、年間20CPE 時間以上、3年間で 120CPE時間以上が必要。 (1CPE時間は50分)	505ドル
CSBM、 CSPM (Technical, Managem ent)	Certified Security Basic Master (情報セキュリティ 技術認定 [基礎コース]) Certified Security Professional Master (情 報セキュリティ技術認定 [応用コース・テクニカル 編/マネジメント編])	Security Education Alliance / Japan, SEA/J	2000	なし	「講習+認定試験」「認 定試験」のいずれも可。	<ul style="list-style-type: none"> ■ 基礎コース (受講+受験料99,750円/受験のみ15,750円) ■ 応用コース・テクニカル編 (受講+受験料204,750円/受験のみ15,750円) ■ 応用コース・マネジメント編 (受講+受験料141,750円/受験のみ15,750円)
GIAC	Global Information Assurance Certification	SANS Institute	2002	2~4年 (受講 分野による)	「講習+認定試験」「認 定試験」のいずれも可。 講習は各6日間	受験費用63,000円 (トレーニングとの同時申込みの場合は、受験費用は 31,500円。別途受講料が必要。)

※HP等を参考に作成

4. 3. 2 既存のセキュリティ講習等に対する評価の基準

(1) 資格や認定の効果が有効期限付きのものか

まず、インターネットは、“dog year”あるいは“mouse year”で技術革新を続けており、セキュリティ技術についても日々刻々変化していることから、有効期限付きのセキュリティ資格や認定であることが適当である。

すなわち、セキュリティに関する資格や認定は、自動車免許のように有効期限付きのものであり、定期的に講習を受けることを求めるものが適当と考えられる。

有効期限付きのセキュリティ資格や認定は、更新を行うための組織が必要であること、新たな技術への対応ができること、教育体制が確立されている場合が多いこと等の特徴があり、これらの点からも望ましいと言える。

(2) 実機を使った演習があるか

セキュリティ人材は、机上の知識だけでなく、実際の通信機器を用いて「生きた」技術・技能を修得することが不可欠であり、実機を使った演習があることも重要である。

(3) 技術だけでなく、管理・運用、法制度についても講習があるか

セキュリティ人材の育成に当たっては、「技術」のみならず、「管理・運用」や「法制度」についても“三位一体”で知識を習得させることが重要である。

4.3.3 既存のセキュリティ講習等の例－NISM

期限付きで、かつ実機を使った演習があり、技術だけでなく管理・運用、法制度についても講習等があるものとして、例えば「ネットワーク情報セキュリティマネジャー」(NISM)がある。

NISMは、2000年に郵政省で開催された「電気通信事業におけるサイバーテロ対策検討会」の報告書を受けて、2001年に創設されたものであり、ハッカーや不正アクセス、コンピュータウイルスなどから情報通信ネットワークとそのユーザを防御するための専門知識を持つ技術者の育成を目的として、NISM推進協議会^(注23)によって実施されている人材育成プログラムである。

▽ NISMの概要

受講資格	① 「NISM推進協議会」を構成する団体に加盟する事業者に所属し当該事業者が推薦する者。 ② 加盟はしていないが、上司または管理する者が推薦する者であって、かつ「NISM推進協議会」が承認した者。
資格取得方法	「講習の受講」＋「講習最終日に実施される認定試験に合格」

(注23) NISM推進協議会は、(社)電気通信事業者協会、情報通信ネットワーク産業協会、(社)テレコムサービス協会、(社)電波産業会、(社)日本インターネットプロバイダー協会、(財)日本データ通信協会、(社)情報通信技術委員会から構成される。

このNISMでは、講習を受講して、講習最終日に実施される試験に合格した者に、NISM推進協議会より「認定」が与えられることとなっている。

また、NISMの特徴としては、次のような事項が挙げられる。

- ① 2年間の有効期限があり、更新試験により、資格を更新する。
- ② 実機を用いた実践的な演習がある。
- ③ 技術のみならず、管理・運用、法制度についても講習を実施する。
- ④ ベンダフリーの講習・資格のため、特定のセキュリティベンダの技術に縛られることなく、最新の必要な技術について学ぶことができる。
- ⑤ ISMSの取得時においても、「セキュリティに関する有スキル者（有資格者数）」として計上することができる。
- ⑥ 入札資格の一例としている地方公共団体も存在する。

▽ N I S M資格体系



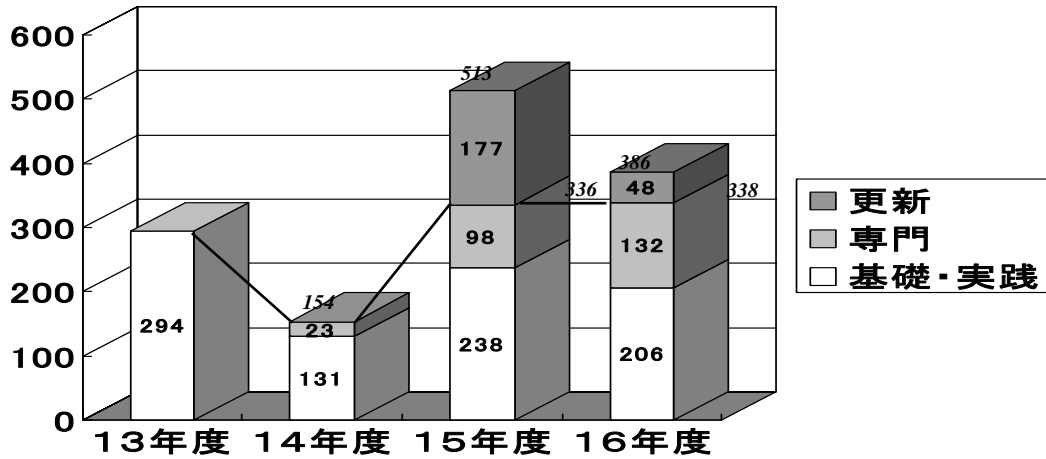
※ 価格は税込。 ※ 日程・講習会場等詳細はNISMホームページを参照。【URL】 <http://www.nism.jp>

NISMについては、2001年の創設以来、1,300名を超える認定取得者がいるが、電気通信業界におけるセキュリティ人材の需要の大きさからすると、依然として十分ではない。

今後とも、インターネットのセキュリティに関する技術革新の動向や電気通信事業者のニーズを踏まえ、講習をより良い内容にするとともに、電気通信事業者にとって広く利用されるよう、周知・啓発を図ることが適当と考えられる。

また、NISMに限らず、セキュリティ講習等に一般的に該当する傾向として、特に、従業者を参加させるに当たって負担の大きい中小規模の電気通信事業者や、地元で講習会が開催される機会の少ない地方の電気通信事業者にとって、利用しにくい側面があり、中小又は地方の電気通信事業者がセキュリティ講習等に参加し易い環境を整備するよう、行政においても支援策を講じていくことが求められる。

▽ NISMの認定取得者数の推移



年度	受講者数					資格取得者数					年度末有効ID数(概数)
	新規	基礎・実践	専門	更新	計	新規	基礎・実践	専門	更新	計	
H13	295	295	—	—	295	294	294	—	—	294	294
H14	154	131	23	—	154	154	131	23	—	154	448
H15	339	240	99	177	516	336	238	98	177	513	667
H16	340	206	134	48	388	338	206	132	48	386	899
合計	1,128	872	256	225	1,353	1,122	869	253	225	1,347	—

4.3.4 大学におけるセキュリティ人材育成

e-Japan 戦略等の国家戦略においても、セキュリティ人材の育成は喫緊の課題となっている。セキュリティ人材育成のため、一部の大学での取組みが始まっている。

表 大学におけるセキュリティ人材教育

大阪大学	セキュアネットワーク構築のための人材育成
早稲田大学	セキュリティ技術者養成センター
中央大学	21世紀COE 電子社会の信頼性向上と情報セキュリティ 情報セキュリティ・情報保証 人材育成拠点
工学院大学	セキュアシステム設計技術者の育成
情報セキュリティ大学院大学	修士課程 2004年4月開校
カーネギーメロン大学 情報大学院	修士課程 2005年9月開校

電気通信事業者から大学等の教育機関に対しては、基礎的かつ系統だったセキュリティ教育を施して欲しいという意見もあるところであり、こうした産業界からの意見を踏まえ、教育機関が自らの教育カリキュラムを見直し、充実させるとともに、行政において教育機関の取組みに対する支援策を講じていくことが求められる。

4. 4 事業者をまたがる総合的な演習の必要性

セキュリティ人材の育成は、個々の電気通信事業者で対応すれば済むものではない。

また、近年、インシデントは広域にわたって同時に発生するケースがあり、ポットネットに代表されるような組織的攻撃も増加している。

このように、インシデント事案の広域化や組織的攻撃の増加という最近の傾向にかんがみると、電気通信事業者間及び電気通信事業者と行政との間で連携して、セキュリティ対策を講じることのできる人材が求められる。

IT戦略本部の情報セキュリティ基本問題委員会が2005年4月に取りまとめた第2次提言においても、「演習・訓練及びセミナー等を通じて、重要インフラ^(注24)所管省庁及び重要インフラ事業者を中心に、高度なITスキルを有する人材を育成」すべきこととされ、更に「想定脅威の拡がりに対応した具体的脅威シナリオの類型を元に毎年度ごとにテーマを設定し、各重要インフラ事業者、各重要インフラ分野内情報共有機構等の協力を得ながら、重要インフラ横断的な総合的演習を企画・実施」することとされている。

(注24) 上記第2次提言では、「重要インフラ」として、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）の7分野のほか、医療、水道、物流等を含める方向性が示されている。

更に、大規模なインシデント事案に際しては、「高度なITスキルを有する人材」のほかに、これら「高度なITスキルを有する人材」の協力体制を促進することのできる調整力のある人材を、プロジェクトリーダーとして育成し、専従的に確保することも必要であると考えられる。

実際、既に米国では、攻撃を想定した総合的な演習が、数次にわたり実施されている。

我が国においても、米国における演習の事例を参考に、

- ① (セキュリティの専門家による) 実行可能な攻撃方法と攻撃による損害の程度
- ② 攻撃発生後の緊急対応体制が実際に機能するか否か

について演習を通じて検証しておくことは、有益なことと考えられる。

①については、ソーシャルエンジニアリングや、内部の従業者による意図的な経路の誤設定又はシステムへの脆弱性の埋込み等を視野に入れて検証することが有用である。

また、②についても、設備管理面やネットワーク運用面で各ISPの言葉遣いが統一されておらず、緊急時に意思疎通に齟齬を来すことが懸念されていることから、ネットワークの状況を定量的に伝えるための運用評価尺度に係る共通認識の醸成や言葉遣いの統一を、演習を通じて進めることが有益である。

▽ 米国における演習の事例

演習名称	実施時期	実施主体	演習の概要
The Day After	1996年3月 (約半日)	国防総省 (DARPA)	行政、大学、情報インフラ関係者による机上演習。攻撃の発生を想定して複数のシナリオを用意し、以下の演習プロセスを実施。 The Day of 攻撃の発生 The Day After 対策 The Day Before 被害を最小化するための予防策の改善 【シナリオの例】 ○ 複数の州のネットワークにトロイの木馬が仕掛けられ、通信障害が発生。
Eligible Recover	1997年6月 (2週間)	国家安全保障局 (NSA)	NSAのスタッフが「実際に」攻撃を実施し、電力や電話のシステムを切断する方法等を模索し、システムの脆弱性を検証。 【攻撃の結果例】 ○ 米国の複数市の送電網に侵入し、スイッチを切るサインを残せた。 ○ 国防省のネットワークへの侵入に成功した。
Digital Pearl Harbor	2002年7月 (3日間)	Gartner、米海軍大学	セキュリティ専門家が電力、通信インフラ、インターネット、金融サービスについて実行可能な攻撃方法と攻撃による損害を検証。 【シナリオの例】 ○ 重要インフラを運営する民間事業者に対し、攻撃の実質的な脅威を体験させるため、演習の参加者がそれぞれ攻撃者の役になり、公開情報とソーシャルエンジニアリングから得られる情報をもとに重要インフラを攻撃する効果的な戦術を模索し、社会的な信頼が損なわれるか否かを検証。
Livewire	2003年10月 (5日間)	国土安全保障省 (DHS)	通信、エネルギー、金融、地方自治の分野について、攻撃発生後の緊急対応体制が実際に機能するかを検証。 【シナリオの例】 ○ 攻撃への対応策を検証し、課題を抽出するため、演習に参加する組織の名称を非公開とする中で攻撃を実施し、攻撃を受けた組織が攻撃を認知したのは何時か、対策をとったのは何時か、行政の対応はどうか等について、連絡体制や意思決定過程も含めて検証。

更に、こうした演習には、セキュリティ講習等に参画できる機会が相対的に少ない中小又は地方のISPの参画を順次確保していくとともに、セキュリティに関する考え方や運用評価尺度が異なる場合のある情報家電機器メーカーや大学等の学術ネットワークの参画を得ていくことが望ましいと考えられる。

加えて、電気通信事業におけるICT障害が、金融、航空、鉄道、電力、ガス、政府・行政サービス、水道等の他の重要インフラに及ぼす影響についてもシミュレーションしておくことが有用であろう。

第5章 総括

以上、これまでの検討を総括すると、次のとおりである。

5. 1 今後、集中的に取り組むべき3つの課題

IPインフラにおいてセキュリティを確保していく上で、今後、集中的に取り組んでいく必要があるのは、次の3つの課題であると考えられる。

(1) ICT障害の広域化への対応

ブラスターやソービッグF等のネットワーク感染型ワーム、Antinny等のDOS攻撃、さらにはボットネットの脅威というように、2003年以降のICT障害を特徴付けるのは、障害が広域に及ぶという点である。

経路障害の誤りによるICT障害も、広域にわたって影響が及ぶ可能性があり、社会インフラとしてのインターネットを機能不全にする恐れがある。

そこで、まず、こうしたICT障害の広域化に、どう対応していくかが今後の重要な課題であると言える。

(2) ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）

次に、ユビキタスネット社会の到来に伴い、情報家電に代表される様々なモノがネットワークに接続され、IPインフラ自体が多様化・高度化する中であって、接続性の確保や機器認証、インターネット全体に与える負荷軽減、業界をまたがる障害対応の迅速化を確保していくことが課題となる。

消費者の視点からみると、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ということを認識していない者も多いと考えられるところであり、「誰でも、簡単かつ安全に」家電を利用できるようにするためのセキュリティ基盤を確立することが求められていると言える。

(3) 人材面の脆弱性の克服

あらゆるセキュリティ対策を講じる上で基盤となるのは人材であるが、情報セキュリティにおいて最も脆弱なのは人間である。

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など、人材面の脆弱性は多層にわたっており、これを克服する取組みを早急に実施していくことが求められる。

▽ 今後、集中的に取り組むべき3つの課題

ICT障害の広域化への対応

- ネットワーク感染型ワーム
- DDoS攻撃
- ボットネット
- 経路情報の誤りによる障害 等

ユビキタスネット社会への対応

- 接続性の確保
- 機器認証
- インターネット全体に与える負荷軽減
- 業界をまたがる障害対応の迅速化

IPインフラ

人材面の脆弱性の克服

一般ユーザーのセキュリティ意識の低さ

組織内従業員の無知や無警戒

経営陣による情報セキュリティマネジメント未実施

電気通信事業者におけるセキュリティ人材の不足

5. 2 「情報セキュリティ政策2005」の提言

これら集中的に取り組むべき3つの課題に対し、誰が、何時から、どのように取り組むべきかについてまとめてみると次のとおりであり、行政においては、これらの取り組みをパッケージ化し、「情報セキュリティ政策2005」として包括的かつ精力的に推進していくことが望まれる。

(1) ICT障害の広域化への対応

1) 広域モニタリングシステムの構築・強化

まず、ICT障害の広域化への対応については、ISP1社のみでの対応では限界があり、ISP等が連携して、広域モニタリングシステムを構築すること等により、インシデント情報を共有し分析することが有効である。

この点に関し、Telecom-ISAC Japan では、2004年度から広域モニタリングシステムを構築しているが、

- ① ブロードバンド環境下で伝送される大容量データをどのようにすれば解析できるのか、
- 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フィック情報やログ情報の把握をどの程度、またどのように仮装(masking)し抽象化して把握すべきか、

といった技術上・制度上の事項があることから、今後、Telecom-ISAC Japan 等の関係機関に行政もオブザーバとして参加する形で、事業者と行政とが協力して取り組んでいくことが適当である。

2) ボットネット対策に関する研究開発

2004年は、ボットネットの存在が認知され、その性質と対策の難しさが認識された年であり、効果的な対策はまだ見出されていない。

このため、ボットプログラムの感染防止と早期駆除、ボットネットによる攻撃の予防と防御について、セキュリティベンダ、通信機器メーカー、ISPとが協力して早急に研究開発に着手すべきである。

行政においても、こうした研究開発に対し、2006年度以降の支援策を検討するとともに、研究開発の推進に当たって必要となるトラフィック情報やログ情報の収集が「通信の秘密」や個人情報保護法に抵触しないよう適宜助言することが求められる。

3) 経路情報の誤りによるICT障害の検知・回復・予防に関する研究開発

経路情報の誤りによるICT障害についても、障害の回復に相当の時間を要していることから、障害の広域にわたる検知、回復、予防を可能とする研究開発に、ISPが連携して早急に取り組むことが有効であり、行政としてもこうしたISPの取り組みを支援していくことが求められる。

(2) ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）

1) 接続検証と規格化

そもそも、情報家電によるサービスの実現に当たっては、情報家電、構内ネットワーク、ゲートウェイ、加入者回線網、ISP、ASPと多段階にわたる接続検証を重ねる必要があり、業界の枠を超えて接続検証と相互利用可能な規格化を行うことが適当である。

その際には、責任分界の明確化、接続管理方式の策定等の作業も併せて行うことが望ましい。

2) 機器認証

構内の情報家電により構外からのサービスを利用するに当たっては、構内の情報家電側から構外の機器を認証することが必要であるとともに、構内にある情報家電が適切なものであるかどうかについて構外の機器から構内の情報家電を認証することも必要であることから、情報家電の普及を図っていくためには、機器認証が重要な課題となる。

この機器認証について一定の規格化を図ることで、提供側にとっては費用削減、ユーザ側にとっては利便性の向上につながることから、どこまで規格化することが適当かについて、関係業界で十分に検証し、調整することが必要である。

3) インターネット全体に与える負荷軽減（情報家電がボット化した場合の対応）

ISPからすれば、情報家電機器もワームやボットプログラムに感染する可能性のある通信機器であり、例えば、接続しているユーザの情報家電機器がボット化し、ISPの電気通信設備の機能に障害を与える等の弊害を実際にもたらすような場合には、当該ユーザへの警告、接続の停止、電気通信サービスの一時停止等の措置をとることがあり得る旨を、約款又は契約で予め明確化し、ユーザに周知しておくことも求められよう。

4) 業界をまたがる障害対応の迅速化

情報家電のセキュリティ確保に関する課題の根底には、家電業界の技術者は、インターネットの技術を十分に知らず、逆に、インターネットの技術者は、家電側の要求をよく知らないという事情があること等から、家電業界とISP業界との間で業界横断的なセキュリティ情報の共有・分析を行うとともに、障害発生後の対応の迅速化に向けた取組みを推進していくべきであり、行政においても、こうした業界横断的な取組みを支援していくことが望まれる。

特に、①情報家電を攻撃対象とするインシデントは、例えば風呂を沸騰させ又は部屋を冷却すること等により、場合によっては人命に関わる事態につながりかねないこと、②情報家電を踏み台としたインシデントは、情報家電の総数が多いだけにインターネット全体に過剰な負荷を与えかねないこと、③現段階でセキュリティ対策を講じないまま脆弱な機器が出回ると回収が困難なこと等の事情があることから、インターネット全体に与える負荷を軽減するとともに、人命に関わる事態につながらないよう家電の作動範囲を規定することが求められる。

(3) 人材面の脆弱性の克服

1) 一般ユーザへの啓発

一般ユーザへの啓発は、今すぐに取り組まなければならない事項であり、セキュリティベンダ、システムインテグレータ、ISP、通信機器メーカー、行政等が連携して、セキュリティに関する情報を分かりやすく、迅速かつ確実に一般ユーザに提供することが重要である。

その際、ブロードバンドの普及により、トラヒックの受発信に関してユーザが大きなパワーを有している状況にかんがみると、インターネットにおいてセキュリティ対策を講ずるべき主体はISPのみではなく、ISP、システムインテグレータ、ユーザ等の関係者による取組みがどれ一つ欠けても十全なセキュリティ対策を講じることができない、という考え方を社会一般に醸成していくことも求められる。

特に、大容量のデータ送信や他のユーザからの苦情申告等により、ユーザのコンピュータがボット化していることが判明した場合には、当該ユーザに対する個別の注意喚起や駆除の方法に係る情報提供を行う等、これまでよりも一層踏み込んだ形で啓発を行うことが必要である。

更に、例えば、接続しているユーザのコンピュータがボット化し、ISPの電気通信設備の機能に障害を与える等の弊害を実際にもたらすような場合には、当該ユーザへの警告、電気通信サービスの一時停止、更には契約解除等の措置をとることがあり得る旨を、ISPにおいて約款又は契約で予め明確化しておくことも求められよう。

2) ソーシャルエンジニアリングの研究と対応策の提示

組織内従業者等の無知や無警戒、あるいは心理や行動様式につけ込んで組織のセキュリティを侵害する手法は、「ソーシャルエンジニアリング (social engineering)」と呼ばれ、米国等では既に研究が進んでいるところであり、我が国においても早急に研究を進め、攻撃を受ける側にとって有益な情報提供と対応策の提示を行っていくことが必要である。

3) ISMS-Tの国内における普及促進と国際貢献

情報セキュリティマネジメントについては、経営陣においてセキュリティポリシーを確立し、これに従って従業者教育やセキュリティ対策を実施していくこと等が極めて重要である。

この点に関しては、ISO/IECが一般の企業を対象とした汎用的な情報セキュリティマネジメントシステム (ISMS) についての国際規格を2000年に策定しているほか、ITUが2004年に電気通信事業分野を対象としたISMS (ISMS-T) を勧告しており、今後、こうした国際規格や国際勧告を国内で普及促進していくため、電気通信事業者を対象としたISMS-Tの実施指針を2005年中にも提示すべきである。

その際、一般の企業を対象とする汎用的なISMSについては、改訂版が2005年6月に発行されていることから、ISMS-Tについても、この改訂版の内容を踏まえることが必要である。

また、現行のISMS-Tは、例えば「法適合性」(Compliance) について、通信の秘密の保護、重要通信の優先取扱い、接続、設備の責任分界等、電気通信事業分野に固有の内容は規定されていないことから、ISMS-Tの国内における普及促進を図るに当たっては、電気通信事業分野に固有の法令上の要求事項を踏まえることも求められる。

更に、2005年秋のITUの会合では、ISMS-Tの修正勧告の検討が開始される可能性があり、その時までには国際的にも評価される提案を我が国として準備しておくことが期待される。

4) 事業者をまたがる総合的な演習の必要性

あらゆるセキュリティ対策を講じる上で基盤となるのは人材であるが、当研究会が2005年4月に実施した我が国の電気通信事業者に対するアンケート調査では、約4分の3の事業者においてセキュリティ人材が不足している状況にある。

電気通信事業者の現状をみると、社外の研修事業者によるセキュリティ講習等を活用している事業者が相対的に多いが、従業者を参加させるに当たって負担の大きい中小規模の電気通信事業者や、地元で講習会が開催される機会の少ない地方の電気通信事業者にとって利用しにくい面があり、今後、中小又は地方の電気通信事業者への浸透を強化することが求められている。

また、セキュリティ人材の育成は、個々の電気通信事業者で対応すれば済むものではなく、インシデント事案の広域化やボットネット等による組織的攻撃の増加などの最近の傾向にかんがみると、電気通信事業者間及び電気通信事業者と行政との間で連携して、セキュリティ対策を講じることのできる人材が求められる。

特に、大規模なインシデント事案に際しては、「高度なITスキルを有する人材」のほかに、これら「高度なITスキルを有する人材」の協力体制を促進することのできる調整力のある人材を、プロジェクトリーダーとして育成し、専従的に確保することも必要であると考えられる。

米国でも攻撃を想定した総合的な演習が数次にわたり実施されていることから、我が国においても、①セキュリティの専門家により実行可能な攻撃方法と攻撃による損害を検証するとともに、②攻撃発生後の緊急対応体制が実際に機能するか否か等について演習を通じて検証するべきである。

また、こうした演習には、セキュリティ講習等に参画できる機会が相対的に少ない中小又は地方のISPや、セキュリティに関する考え方や言葉遣いが異なる場合のある情報家電機器メーカーの参画を得ていくことが望ましい。

▽ 「情報セキュリティ政策2005」

課題	小分類	政策の内容	何時	誰が				
				ISP	メーカ	セキュリティベンダ*	大学等	行政
ICT 障害の広域化	ネットワーク感染型ワーム	広域モニタリングシステムの構築・強化	04年～	◎	◎	◎	◎	○ (06年以降の支援策検討)
	ボットネット	ボットネット対策に関する研究開発	早急に	◎	◎	◎	◎	○ (06年以降の支援策検討)
	経路情報の誤り	障害の検知・回復・予防に関する研究開発	早急に	◎			◎	○ (06年以降の支援策検討)
ユビキタスネットワーク社会におけるセキュリティ確保	接続性の確保	業界横断的な接続検証と相互利用可能な規格化、責任分界の明確化	早急に	◎	◎			○ (06年以降の支援策検討)
	機器認証	規格化	早急に	◎	◎	◎		○ (06年以降の支援策検討)
	インターネットに与える負荷軽減	▽ ユーザへの啓発 ▽ 約款等の明確化	05年～	◎ ◎	○ ○			○ ○
	業界をまたがる障害対応の迅速化	▽ 業界をまたがる情報交換・情報交流、 ▽ 家電の作動範囲規定 ▽ 総合的な演習	早急に	◎ ◎	◎ ◎		◎ ◎	○ ◎ (06年以降の支援策検討)
人材面の脆弱性	一般ユーザ*	啓発	今すぐ	◎	◎	◎	◎	◎
	組織内従業員の無知、無警戒	ソーシャルエンジニアリングに関する研究と対応策の提示	早急に	◎	◎	◎	◎	○ (06年以降の支援策検討)
	経営陣による情報セキュリティマネジメント	ISMS-Tの普及促進 (実施要件の提示)	05年中	◎	○	○		◎
		ISMS-Tの充実に係る国際貢献	05年～	◎	○	○		◎
	セキュリティ人材の不足	▽ 社外の講習・資格の活用	引続き	◎	○	○	○	○
▽ 社内の従業者教育 ▽ 演習を通じた、インシデントに円滑に対応できる人材の育成		引続き 早急に	◎ ◎	○ ◎	○ ◎	○ ◎	○ ◎ (06年以降の支援策検討)	

◎は主体的に取り組むべき主体、○は◎の支援者又は政策の対象者。

用語集

名称	用語解説	掲載頁
重要インフラ	重要インフラとは、他に代替することが著しく困難なサービスを提供する事業者が形成する国民生活及び社会経済活動の基盤であり、その機能が著しく停止、低下、または利用不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるもの。IT 戦略本部の情報セキュリティ基本問題委員会が2005年4月に取りまとめた第2次提言では、「重要インフラ」として、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む)の7分野のほか、医療、水道、物流等を含める方向性が示されている。	1,14,86,87
ISP : Internet Service Provider	インターネットへの接続サービスを提供する電気通信事業者。	1,2,3,10,11,13,15,16,17,18,19,25,26,31,34,35,38,39,43,44,46,49,51,53,57,75,86,87,91,93,94,95,97,98
dog year	情報技術分野における革新のスピードを表す概念。(人間の7年が犬の1年に相当することから)	1,77,82
mouse year	情報技術分野における革新のスピードを表す概念。(人間の18年がマウスの1年に相当することから)	1,77,82
IP:Internet Protocol	インターネットを構成する通信機器が共通に使用する通信プロトコル。	1,2,3,15,17,18,24,31,32,91,92
情報家電	家庭用の電化製品でネットワークに接続されるもの。パソコン等の情報機器も含まれるが、むしろネットワークに接続される VTR / DVD 機器やエアコン、照明器具、冷蔵庫、風呂等、従来ネットワークに接続される機器とは考えられなかったものを指すことが多い。	2,41,43,44,45,46,47,48,49,59,51,52,53,54,57,87,91,94,95,97
ユビキタスネット社会	「いつでも」(昼でも夜でも24時間)、「どこでも」(職場でも家でも、都会でも地方でも、移動中でも)、「何でも」(家電も身の回り品も、車も食品も)、「誰でも」(大人も子供も、高齢者も障害者も)、ネットワークに簡単につながる社会。	2,41,43,45,57,91,92,94,98
不正アクセス	アクセス制御機能を有するネットワークに正当な権限なくアクセスをしてコンピュータを作動させ、利用する行為。	2,7,8,19,38,47,75,83

名称	用語解説	掲載頁
ウイルス	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。	2,7,8,10,11,14,15,19,21,22,24,25,28,29,30,38,75,83
ワーム	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。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。	2,7,8,10,11,12,13,14,15,16,19,21,28,38,49,91,92,94,98
インシデント	不正アクセスやウイルス、ワーム等に起因する情報通信技術の機能不全による障害。	2,5,7,8,11,13,19,20,34,36,38,43,53,54,57,62,67,77,78,86,93,95,97,98
ISMS (Information Security Management System)	企業などの組織が自身の情報試算を適切に保護し、事業継続を確実にし、事業損害を最小限にし、投資に対する見返り及び事業機会を最大限にすることを目的として、セキュリティポリシーを自ら策定し、これに基づいた管理策の選択・実施やリスクアセスメントの実施などを継続的に運用する枠組みのこと。	3,57,58,59,60,61,62,63,64,65,66,67,68,78,83,96,98
ISMS-T(x.1051)	2004年にITU(国際電気通信連合)が勧告した電気通信事業分野を対象としたISMS(情報セキュリティマネジメントシステム)。	3,57,78,63,65,66,67,68,69,96,98
国際電気通信連合 (ITU : International Telecommunication Union)	電気通信に関する国連の専門機関であり、多国間の円滑な通信を行うため、世界各国が独自の通信方式を採用することによる弊害の除去、有限な資源である電波の混信の防止、電気通信の設備が不十分な国に対する技術援助等を実施している。	3,57
経路情報	ルータや端末が保持するデータの伝送経路に関する情報。	7,38,39,92,94,98
サービス不能化 (DoS:Denial of Service)攻撃	標的となるコンピュータやルータに大量のデータを送りつけてシステムをダウンさせる攻撃。	8,14,15,16,18,19,21,22,25,27,28,29,91
スパムメール	受信者の意図に関係なく一方的に送信される広告宣伝メールや一時に多数の架空電子メールアドレスをその宛先とする電子メール。	9,14,22,25,26,28,29,35
フィッシング(Phishing)	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など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。	9,22,26,27,28,36

名称	用語解説	掲載頁
スパイウェア (Spyware)	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、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。	9,22,23,28
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。	10,12,19,29,35
ソービッグ (Sobig)	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。	11,14,15,29,91
SQL スラマー (SQL.Slammer)	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。	11
ブラスター(Blaster)	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	11,13,14,21,91
セキュリティ・ホール	アプリケーション等に存在する、情報セキュリティの不備。これを悪用することでネットワークへの不正アクセス等が可能となる。	11,12,13,14
Exploit Code	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。	12,14,19
OS (Opereating system)	システム全体を管理する基本的なソフトウェア。	12,50
Telecom-ISAC Japan	インシデント情報の収集・分析・共有を目的として、2002年に「インシデント情報共有・分析センター」として設立された団体。2005年2月に財団法人データ通信協会に編入。	13,14,15,16,17,19,29,31,34,53,93
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。	14,15,87

名称	用語解説	掲載頁
NIRT (National Incident Response Team)	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。	14
フィルタリング	特定の条件に合致するデータを通過させ又は破棄する行為や機能のこと。	15,32,33,75
P2P(Peer to Peer)型通信	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。	15,16,24
Antinny(アンチニー)	P2P 型通信のアプリケーションソフトの1つである Winny が媒介し感染するワーム型ウイルス。	15,16,17,18,19,27,91
DNS (Domain name system)	インターネット上のホスト名(ネットワークに接続されたコンピュータを人間が識別しやすいようにつける名前)と IP アドレスを対応させるシステム。全世界の DNS サーバが協調して動作する分散型データベースである。	16,17,18,27
A レコード	ホスト名と IP アドレスの対応関係	17
TTL (Time To Live)	パケットの有効期間を表す値。最大 255 までの整数値で表され、ルータなどを1回経由されるたびに値が1減少する。TTL が0になったパケットはその時点で廃棄され、廃棄通知がパケットの送信元に届くようになっている。	17
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。	17
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。	17
ブラックホール IP アドレス	DoS 攻撃等による攻撃パケットを破棄するために設定された「おとり」のIPアドレス。	17,18
トラヒック	ネットワークの特定の経路上を一定時間に流れる情報の量。	17,18,19,20,23,25,31,33,35,38,39,54,78,93,95
ベストプラクティス	最も効果的、効率的な実践の方法。または最優良の事例。	19

名称	用語解説	掲載頁
ボット	悪意のある攻撃者(管理者)の指揮命令下に置かれたコンピュータのことである。ネットワーク経由の遠隔操作により、コンピュータを攻撃等のために悪用することを可能とするプログラムをボットプログラムといい、ボットプログラムに感染したコンピュータをボットという。	21,22,23,25,26,27,28,29 30,31,32,33,34,35,49,8 6,91,93,94,95,97,98
ボットネット	同一のボットプログラムの指揮命令下にあるコンピュータ群。	21,22,23,25,27,28,29, 30,31,32,34,35,86,91, 93,97,98
ネットスカイ	電子メールを媒介にして感染する。感染すると、パソコン内で発見されたメールアドレスすべてに複製を添付した電子メールを送信する。2004年2月の、最初のネットスカイの発見後、亜種が次々と発見され、多くのパソコンを感染させた。	21
ゾンビ	ボットに類似の言葉として「ゾンビ」があるが、これはボットよりも広い概念で、ボット以外にも、攻撃者の指令を受けるのではなく、事前に一定の動作をするように仕組まれたウイルスに感染したコンピュータや、人手を掛けて乗っ取られたコンピュータが含まれる。例えば、2003年8月に大流行したブラスターや、2004年2月から現在に至るまで拡散しているネットスカイ及びその亜種のように、決められた時間に特定のサイトをDoS攻撃する機能がプログラムされたワームに感染したコンピュータはゾンビである。	21
ゾンビクラスター	一斉に同一の攻撃を行うゾンビの一群をゾンビクラスターと呼ぶ。ボットネットは、ゾンビクラスターの一つである。	21
メールサーバ	インターネット上に接続され、自ネットワーク内のユーザの電子メールの送信や受信を行なうコンピュータ。	22,25,26,28
FTPサーバ	FTPとはFile Transfer Protocol(ファイルトランスファープロトコル)の略で、ファイル転送するためのサーバ。	22
IRC (Internet Reley Chat)	インターネットやイントラネットなどのネットワーク上で、リアルタイムにテキストデータを交換するチャットシステム。	23
バックドア	通常のネットワーク経路とは異なる場所に設けられたアクセスの受け口のことをいう。	24,29
ハニーポット	不正アクセスの手法やウイルスの振舞い等を調査・研究するためにインターネット上に設置された、わざと侵入しやすいよう設定されたサーバやネットワーク機器のこと。「甘い蜜の入ったつぼ」の意味で、攻撃者やウイルスを「おびき寄せる」という意味からこのように呼ばれる。	24,31,32

名称	用語解説	掲載頁
アゴボット	トロイの木馬の亜種の不正プログラムで、ネットワークを通じて自身のコピーを頒布するワームの一種。	25,29
ファイアウォール	ネットワークの外部からのアクセスを制御するシステム。不正アクセスの防御壁としての役割を果たす。	29,46,78
リバースエンジニアリング	ソフトウェアやハードウェアなどを分解、あるいは解析し、その仕組みや仕様、目的、構成部品、要素技術などを明らかにすること。	30
パターンファイル	ウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイル。	30
ソーシャルエンジニアリング	人間の無知や無警戒、あるいは心理や行動様式につけ込んで組織のセキュリティを侵害する手法。	36,37,86,87,96,98
セキュリティポリシー	企業などの組織において、情報セキュリティを確保するための対策や体制等を定めた基本方針。	36,37,57,60,61
AS (Autonomous system)	ASとは、ある経路制御方針によって運営されるネットワークのことをいう。全国展開しているISPもインターネット全体から見ると一定の経路制御方針によって運営されている1つのネットワークであり、1つのASとして捉えられ、AS番号を割り当てられている。	38
アプリケーションサービスプロバイダ (ASP : Application Service Provider)	各種業務用ソフト等のアプリケーションソフトをデータセンター等において運用し、当該アプリケーションソフトをインターネット経由でユーザー(企業)に提供する事業者。	44,49,94
ゲートウェイ	ネットワーク上で、通信媒体やプロトコル(伝送手順)が異なるデータを相互に変換して通信を可能にする機器。通信媒体やプロトコルの違いを吸収して異機種間の接続を可能とする。	45,46,49,94
Push 型アクセス	サービス提供側からユーザ側に能動的に様々なサービスが提供される形態のアクセス方法。	46,47
Pull 型アクセス	ユーザ側からのリクエストにより、サーバが応答し、様々なサービスが提供される形態のアクセス方法。	46,47
CPU (Central Processing Unit)	中央演算処理装置。機器内の制御やデータの計算・加工を行なう中枢部分。	50

名称	用語解説	掲載頁
国際標準化機構 (ISO)	工業標準の策定を目的とする国際機関で、各国の標準化機関の連合体。1947年に設立され、現在では147カ国が参加している。本部はスイスのジュネーブ。	57
国際電気標準会議 (IEC)	「国際電気標準会議」の略。電気等の分野で各国の規格・標準の調整を行なう国際機関。1906年に設立され、1947年以降はISOの電気・電子部門を担当している。本部はスイスのジュネーブ。	57
BS7799	イギリス規格協会(BSI: British Standards Institution)が策定したセキュリティ管理・認証規格。	59
ISO/IEC27799	医療分野を対象としたISMS基準。	63
ISO/TC68	金融分野を対象としたISMS基準。	63
大統領指令63号 (PDD63: Presidential Decision Directive 63)	クリントン政権下における重要インフラ防護に関する重要な要素を示した大統領指令。	79

參考資料

次世代 IP インフラ研究会

構成員

(五十音順 敬称略)

- 安 念 彌 行 宇宙通信株式会社 代表取締役社長
- 磯 崎 澄 ジェイサット株式会社 代表取締役社長
- 伊 藤 泰 彦 KDDI株式会社 取締役執行役員専務 技術統轄本部長
- 江 崎 浩 東京大学大学院 情報理工学系研究科 教授
- 沖 松 哲 夫 日本インターネットエクスチェンジ株式会社 代表取締役社長
- 小 畑 至 弘 イー・アクセス株式会社 専務執行役員 チーフテクニカルオフィサー
- 後 藤 滋 樹 早稲田大学理工学部 教授
- ◎ 齊 藤 忠 夫 東京大学 名誉教授
- 佐々木 良一 東京電機大学 工学部情報メディア学科 教授
- 篠 田 陽 一 北陸先端科学技術大学院大学 情報科学研究科 教授
- 鈴 木 幸 一 株式会社インターネットイニシアティブ 代表取締役社長
- 田 邊 忠 夫 株式会社ケイ・オプティコム 代表取締役社長
- 所 眞理雄 ソニー株式会社 特別理事
- 中 根 滋 株式会社パワードコム 代表取締役社長兼CEO
- 中 村 隆 富士通株式会社 経営執行役
- 古 川 一 夫 株式会社日立製作所 執行役副社長 情報・通信グループ長&CEO 兼 輸出管理本部長
- 細 谷 僚 一 インターネットマルチフィード株式会社 代表取締役副社長
- 牧 園 啓 市 ソフトバンクBB株式会社 技術本部本部長
- 村 井 純 慶應義塾大学 環境情報学部 教授
- 矢 野 薫 日本電気株式会社 代表取締役副社長
- 山 田 隆 持 日本電信電話株式会社 代表取締役副社長

◎は座長 ○は座長代理

「セキュリティWG」

構成員

(五十音順 敬称略)

- | | | |
|---|---------|--|
| | 新 井 悠 | 株式会社ラック コンピュータセキュリティ研究所 グループリーダー |
| ○ | 飯 塚 久 夫 | NTTコミュニケーションズ株式会社 常務取締役 セキュリティマネジメント室長 |
| | 歌 代 和 正 | 株式会社インターネットイニシアティブ 取締役 フェロー |
| | 内 田 勝 也 | 情報セキュリティ大学院大学 助教授 |
| | 笠 原 裕 | 日本電気株式会社 ソリューション研究開発本部長 |
| | 加 藤 幹 之 | 富士通株式会社 経営執行役 法務・知的財産権本部長 |
| | 加 藤 佳 実 | 松下電器産業株式会社 eネット事業本部 ネットワークサービスエンジニアリングセンターGM |
| | 桑 子 博 行 | 社団法人テレコムサービス協会 サービス倫理委員会 委員長 |
| | 笹 木 一 義 | ソフトバンクBB株式会社 技術本部 技術企画部 担当部長 |
| ◎ | 佐々木 良 一 | 東京電機大学 工学部 情報メディア学科 教授 |
| | 篠 田 陽 一 | 北陸先端科学技術大学院大学 情報科学研究科 教授 |
| | 武 智 洋 | 横河電機株式会社 コーポレートマーケティング本部 セキュリティプロジェクト長 |
| | 手 塚 悟 | 株式会社日立製作所 システム開発研究所 第七部 部長 |
| | 中 尾 康 二 | KDDI株式会社 技術開発本部 情報セキュリティ部長 |
| | 永 瀬 正 敏 | 日本テレコム株式会社 情報セキュリティオフィス室長 |
| | 夏 井 高 人 | 明治大学 法学部 教授 |
| | 南 浮 泰 造 | 株式会社ケイ・オプティコム 企画室 経営戦略グループ 部長 |
| | 藤 谷 護 人 | 弁護士法人エルティ総合法律事務所 所長弁護士 |
| | 星 澤 裕 二 | 株式会社セキュアブレイン プリンシパル セキュリティアナリスト |
| | 松 島 裕 一 | 独立行政法人情報通信研究機構 情報セキュリティユニット ユニット長 |
| | 森 久 隆 | 株式会社パワードコム 専務執行役員 情報プライバシー担当 |

◎はグループリーダー ○はサブリーダー