



次世代IPインフラ研究会 第二次報告書（案）の概要

「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

セキュリティWGの開催状況

平成16年12月13日 第1回WG

WGの進め方について

インシデント情報の共有・分析について

平成17年1月20日 第2回WG

セキュリティ水準の向上について

平成17年2月17日 第3回WG

情報家電等のインターネット接続に伴うセキュリティの確保について

平成17年3月17日 第4回WG

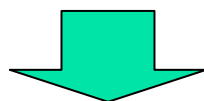
セキュリティ人材の育成について

平成17年4月27日 第5回WG

報告書(骨子)の審議

平成17年5月20日 第6回WG

報告書(案)の審議



パブコメ(5月25日~6月15日)

平成17年6月30日 第6回 次世代IPインフラ研究会 親会

セキュリティWG構成員

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

第1章 インシデント対応の現状と課題

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 -

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

第4章 セキュリティ人材育成

第5章 総括



第1章 インシデント対応の現状と課題

-Our security depends on your security-

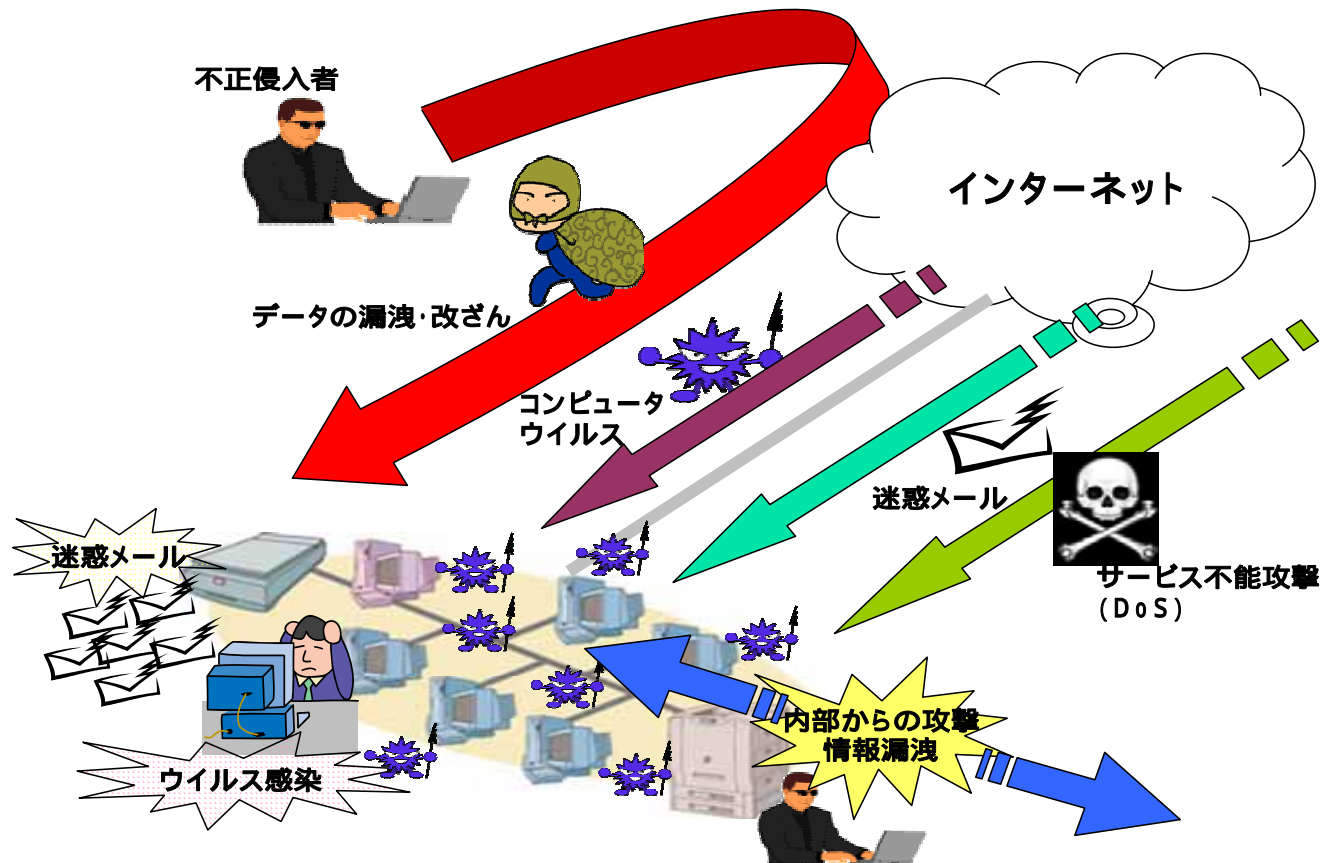
1.1 ICT障害

情報通信技術（ICT）の機能不全による障害（ICT障害）を次の3つに分類

- 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）
- 経路情報の誤りによるICT障害
- 自然災害によるICT障害

本報告書で取り上げるICT障害

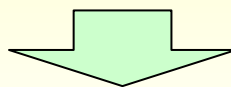
インシデントのイメージ図



1.2 インシデントの最近の傾向

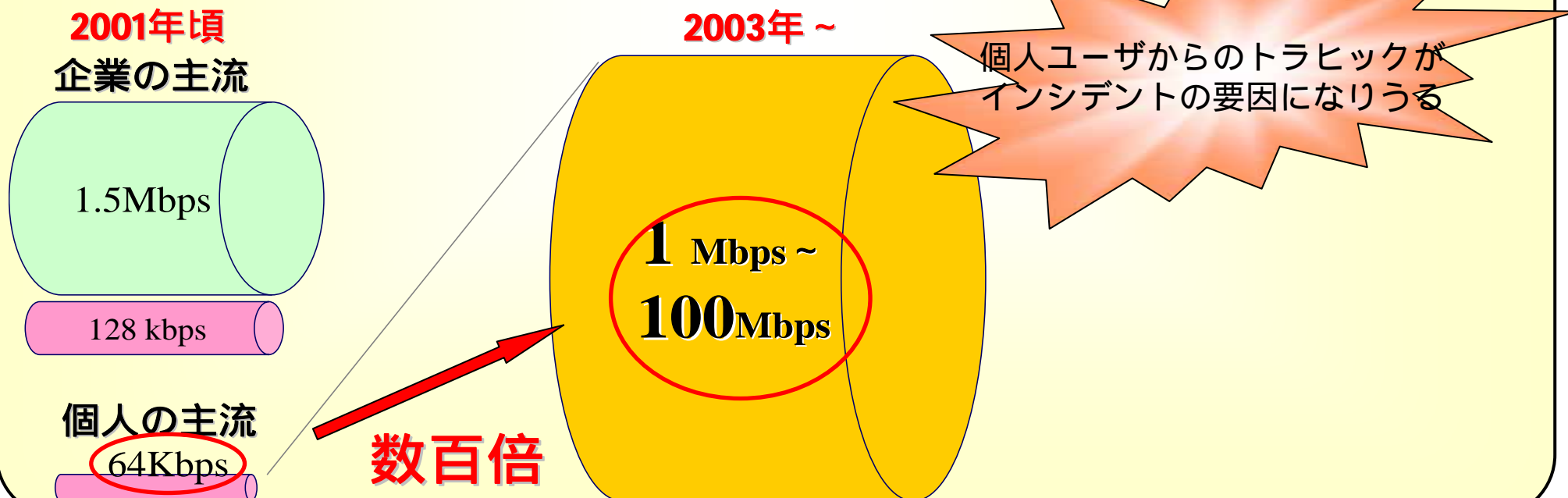
個人ユーザの影響力の増大

常時接続・定額料金のプロードバンドの普及により、従量課金・ナローバンドによるインターネット接続が主流であった頃と比べると、ユーザが数百倍のトラヒックの受発信能力を有する



自己増殖したワームからのトラヒックによるネットワークへの過負荷

個人ユーザの影響力の増大



1.3 インシデントに対するISPの対応事例

2003年
ネットワーク感染型ワームへの対応
ブラスター
ソービッグF

教訓

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。

攻撃の回避策は、攻撃を受けないようにすることはできても、従来利用していたサービスの回復にはならず、本質的な解決策にはならない。

今後の課題

1社のみへの対応には限界

広域モニタリングシステムの構築・強化

ブロードバンド環境で伝送される大容量データをどのようにすれば技術的に解析できるのか

「通信の秘密」の保護や個人情報保護に抵触しないよう、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

Telecom-ISAC等の関係機関に政府もオブザーバとして参加する形で研究開発に取り組んでいくことが必要。

2004年
DoS攻撃(Antinny)対応

「ボットネット」とは

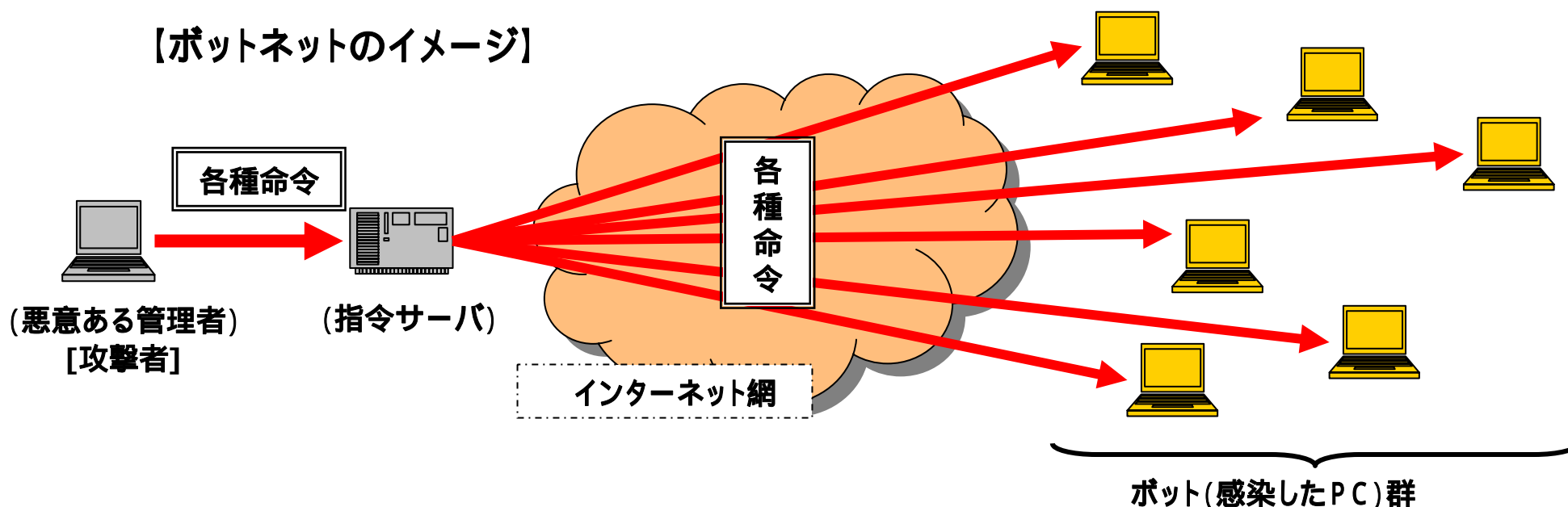
「ボット」とは、悪意のある攻撃者（管理者）の指揮命令下に置かれたコンピュータネットワーク経由の遠隔操作により、コンピュータを攻撃等に悪用することを可能とするプログラムを「ボットプログラム」といい、ボットプログラムに感染したコンピュータがボット

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が「ボットネット」

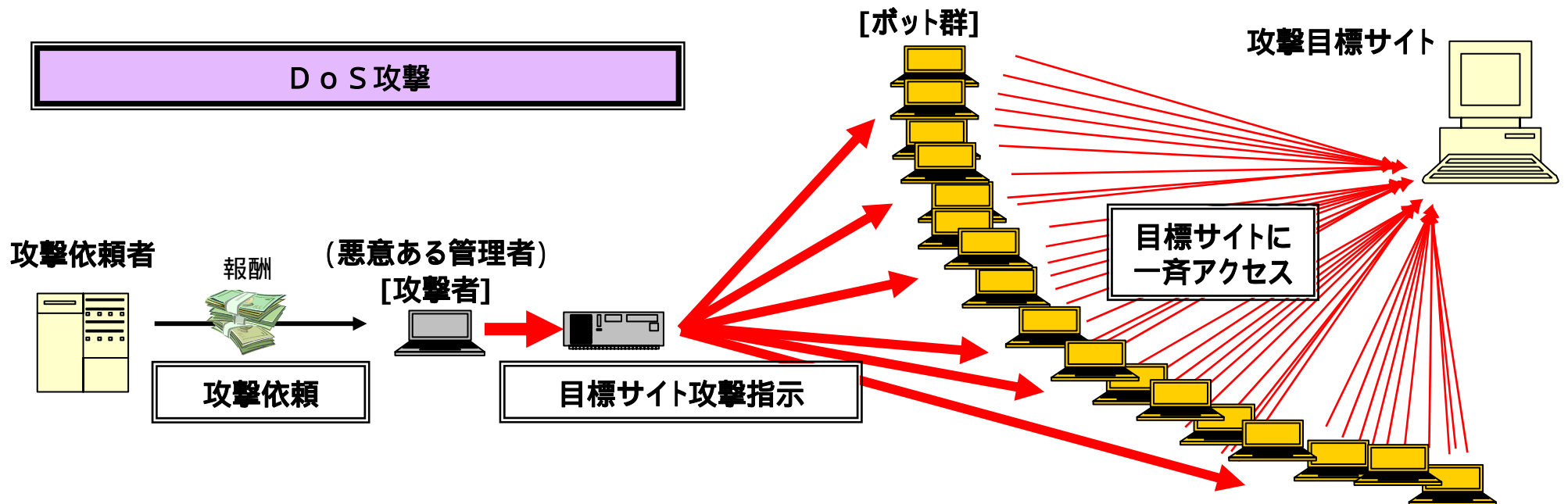
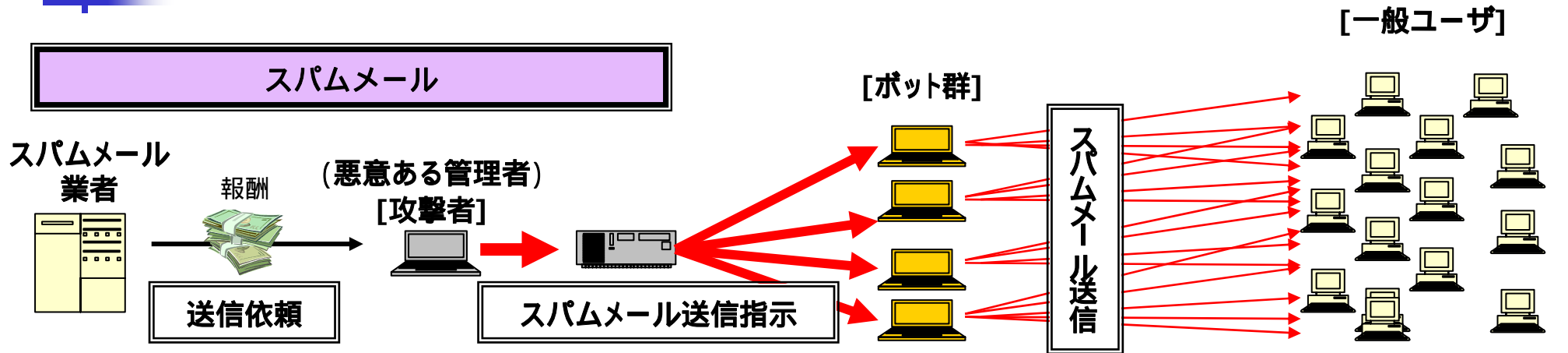
ボットには、スパムメール送信やD o S攻撃、フィッシング、スパイウェアといった攻撃機能がある。

ボットの保有者は、ボットプログラムに感染していること、及び他のコンピュータを攻撃していることを自覚していない場合が多い。

【ボットネットのイメージ】



ボットネットの悪用例



研究開発

1. 感染防止と早期駆除

- (1) 検体収集
- (2) ボットネットの行動特性の把握

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）
- (2) 攻撃元となっているボット(ボットネット)の把握
- (3) 攻撃のフィルタリング

こうした研究開発を進めるに当たっては、トラヒック情報やログ情報を収集することが不可欠。

「通信の秘密」の保護や個人情報保護に抵触しないよう、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。

セキュリティベンダ、通信機器メーカー、ISPから成る協力体制を構築することも必要。

ユーザへの啓発

ブロードバンドの普及により、トラヒックの受発信において、個人ユーザの影響力が増大。

特に、ボットについては、以下の事情から、これまで以上にユーザへの啓発を図る必要。

- (1) 感染しているという自覚がない。
- (2) 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という自覚もない。
- (3) こうしたボットが既に大量に存在。

大容量のデータ送信や他のユーザからの苦情等により、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、当該ユーザへの個別の注意喚起や駆除の方法に係る情報提供を行う等、これまでよりも踏み込んだ啓発が必要。

ボット化し易いコンピュータの調査や、ボット化するコンピュータが減少するよう、社会的に啓発を進めていくことが必要。

1.5 ソーシャルエンジニアリングへの対処

ソーシャルエンジニアリングとは

人間の無知や無警戒、心理や行動様式につけ込んで組織の情報セキュリティを侵害する手法。なりすまし、のぞき見、トラッシング（ゴミの狩猟）等の手法が利用される。

ソーシャルエンジニアリングへの対処

ソーシャルエンジニアリングについて研究を進め、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。

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、明確な指針を従業員に示す必要。

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、従業員からの報告が適切に行われ、これを受けて経営陣が対処しているということを従業員に示すことも、従業員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員を組み込んでいく上で重要。

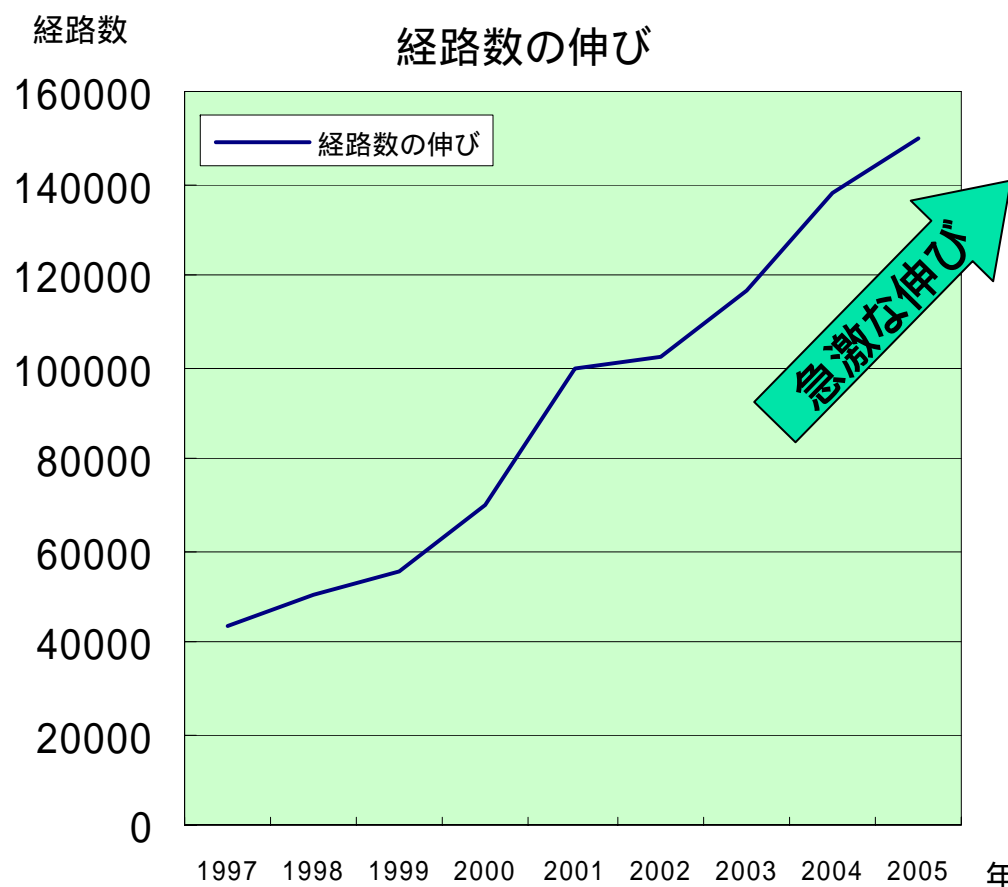
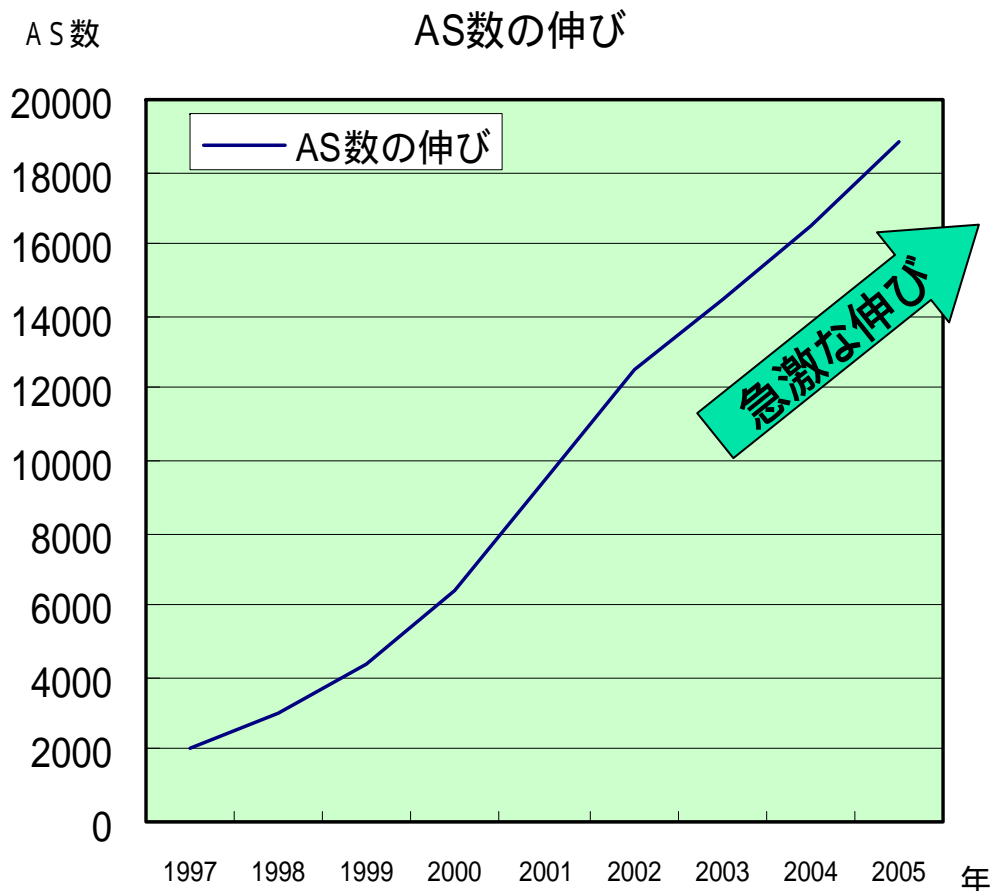
1.6 経路情報の誤りによるICT障害

1.6.1 経路数の拡大

インターネットの拡大

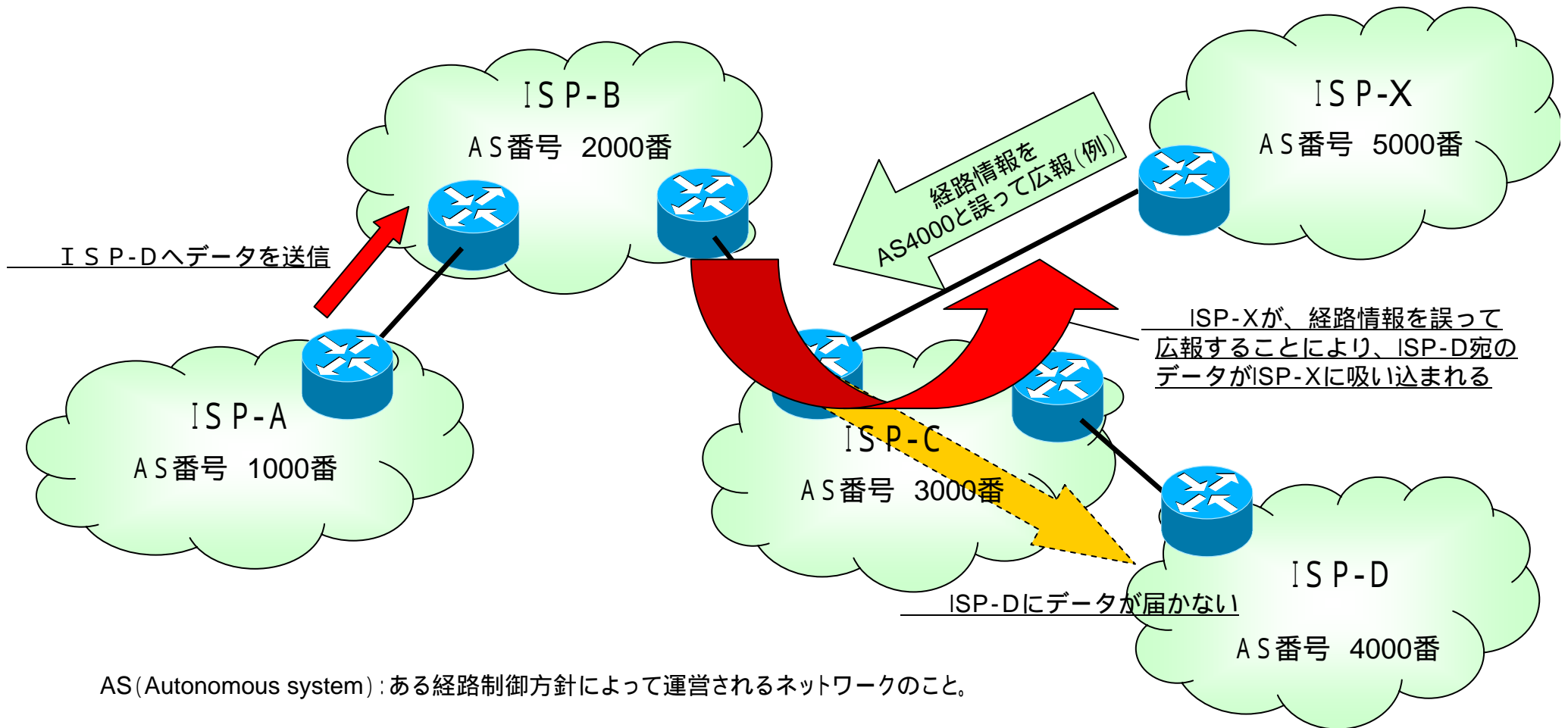
インターネットは、1990年代に米国で商用サービス開始以来、現在まで拡大の一途。

現在では、ISP等によって管理されるネットワーク (= AS (Autonomous System)) の数は1万8千を超え、AS間を結ぶ経路数は15万。



1.6.2 経路情報の誤りによるICT障害

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



AS (Autonomous system) : 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。

実情

インターネットは、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、直接の接続相手であるISPより先は、どこに接続しているか分からない。

➡ このため、障害が発生した場合の対応や協調運用が困難

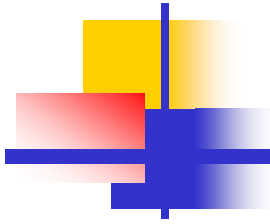
ISPでは、障害が発生した場合、どこに問題があるのかを解析・特定し、経路設定を誤ったISPに電話等で直接コンタクトをとることにより対応を図っており、障害の回復に時間を要している。

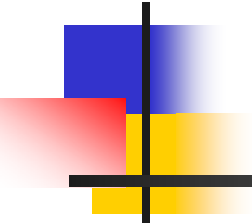
特に、海外のISPがひき起こす経路情報の誤りに際しては、ネットワーク運用に対する考え方の違いや言語の違い等から、その対応には相当の時間を要する。

対応策

(1) まず、ISPにおいて経路情報の信憑性を確保するための取組みが不可欠であるが、経路情報の誤りを全くなくすことはできない。

(2) 経路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、予防を可能とする技術開発・実証実験を行うことが有効。





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 -

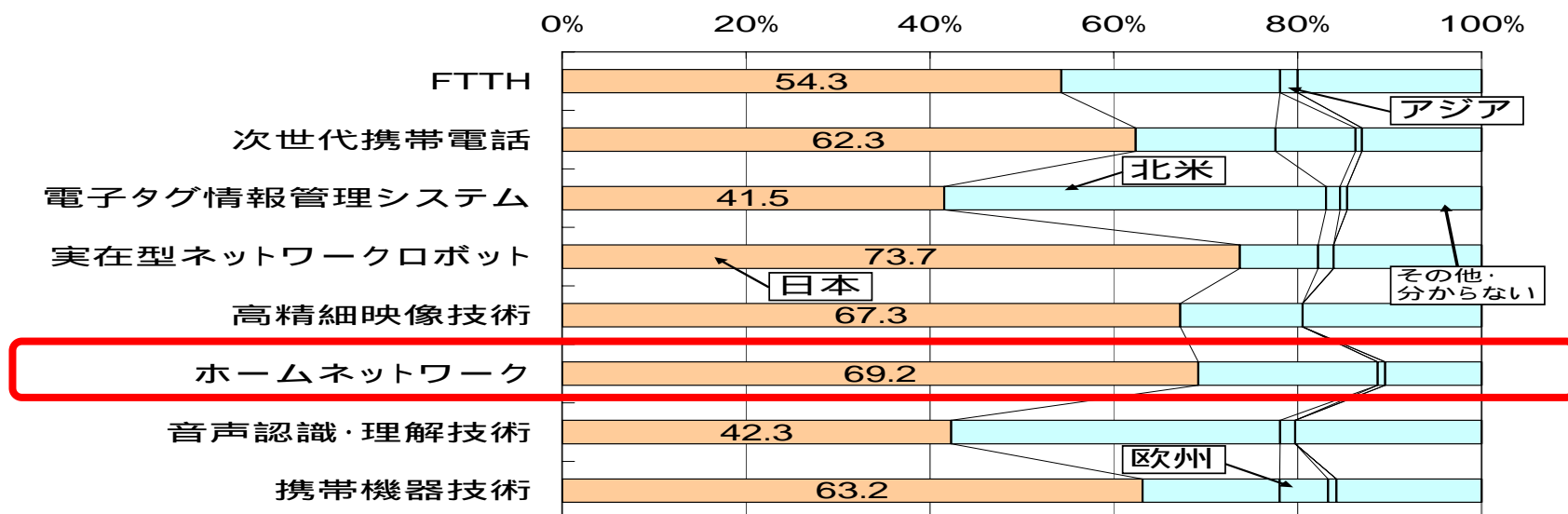
2.1 ユビキタスネット社会におけるセキュリティ確保の必要性

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。

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。

消費者の視点からみると、家電が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。

ICTの優位性に関する国際比較



2.2 情報家電に対する期待

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 機器の価格 セキュリティ サービス料金 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)	エアコン VTR/DVD機器 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	ガス/火災 不審 部屋 照明 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	BBサービス TV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	行楽地や道路/病院混雑状況 幼稚園	37.3%	安全・安心
		出かける前の 情報確認	天気 時刻表 乗換 地図等	34.8%	簡単・快適

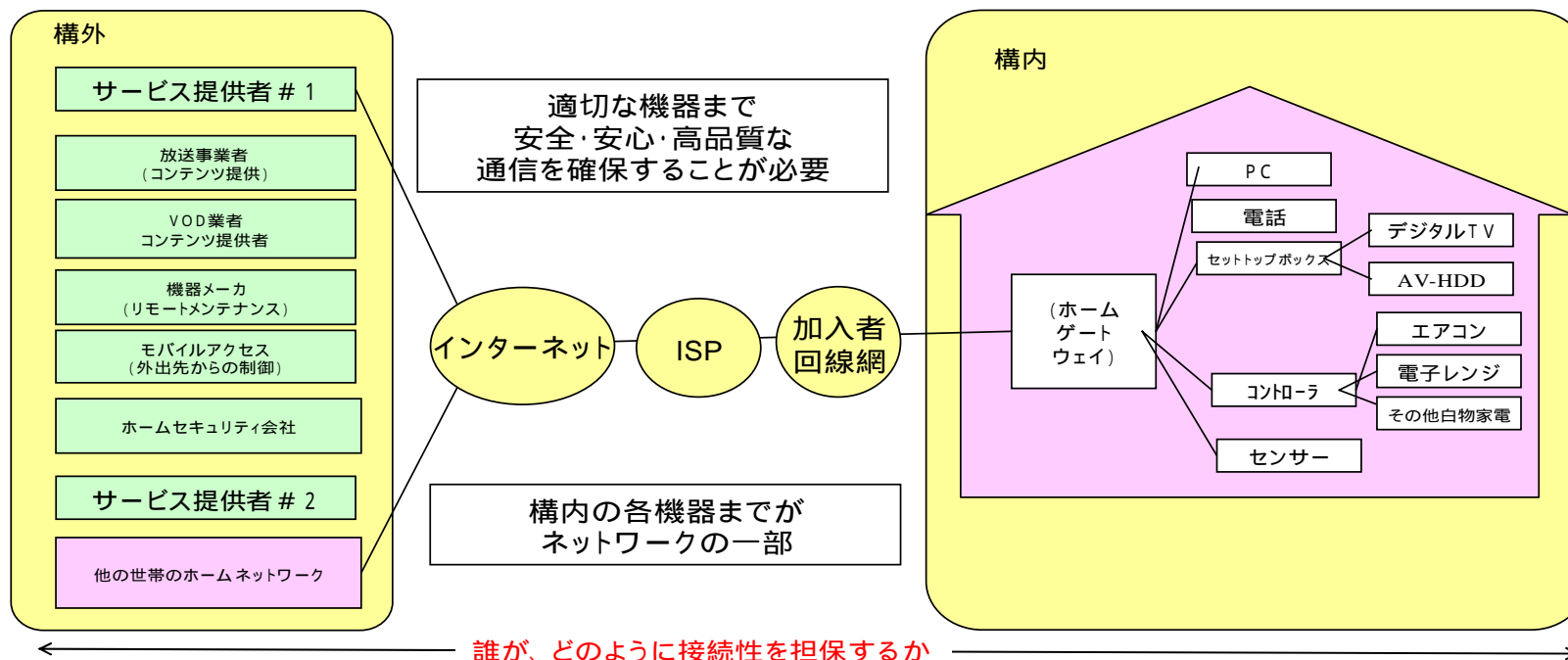
そもそも、情報家電によるサービスの実現に当たっては、情報家電、構内ネットワーク、ゲートウェイ、加入者回線（アクセス）網、ISP、ASPというように、他段階にわたる接続検証を重ねる必要。

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。

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。

接続検証件数 = N × N × N × N × N × N × N × N =

(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)



I S P 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恐れのある通信機器。

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。

当該 I S P の電気通信設備の機能に障害を与える場合。

当該 I S P 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。

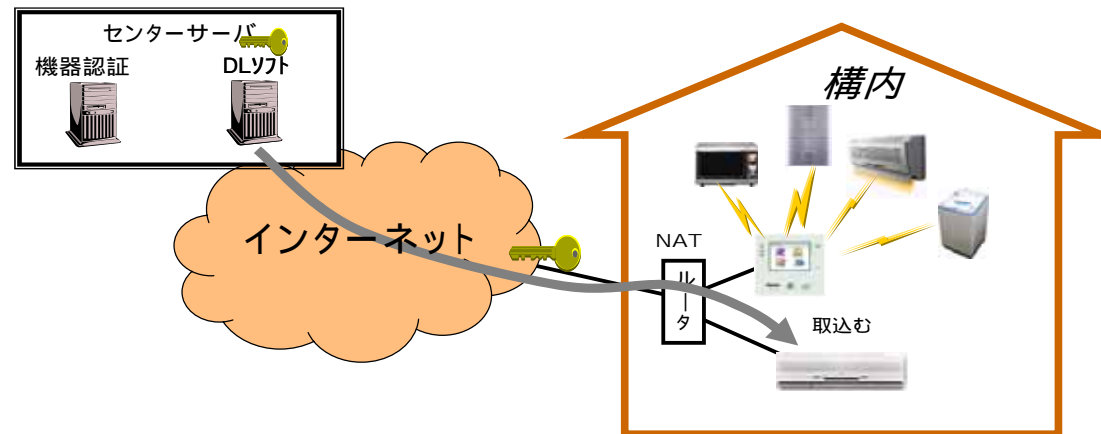
2.3.3 リモートメンテナンスと機器認証

リモートメンテナンス

情報家電は、表示画面が小さくキーボードがないなど、ユーザインターフェースに難があること等から、OSやソフトウェアに脆弱性が発見された場合、修正プログラムを構外から配信する、いわゆる「リモートメンテナンス」を検討する必要。

機器認証

リモート・メンテナンスに限らず、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が必要になる。



機器認証について一定の規格化を図ることで、家電機器メーカー、ISP等にとっては費用削減、ユーザにとっても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。

(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、元のユーザが情報家電を通じて利用するアプリケーションサービス（以下、本スライドで単に「サービス」という。）の契約を解約しないと、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、サービス料金を元のユーザが支払ってしまうことになる可能性がある。

このため、情報家電の破棄・転売時には、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。

(2) 個人情報保護

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	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、通信料引落とし口座等
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

家電業界の技術者は、インターネット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。

インシデントが発生した場合に、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。

ユーザは、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ない。



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、セキュリティに関するユーザの啓発等に関する連携の枠組みを構築することが有効。



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

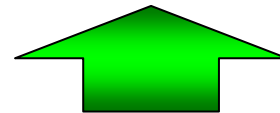
情報セキュリティマネジメントの重要性

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、情報セキュリティマネジメントの重要性を経営陣が適切に認識した上で、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。

電気通信事業分野では

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。



ISO / IECの国際規格やITUの勧告等を参照

3.2 ISMSの概要と最近の改訂作業の動向

2000年12月に策定されたISO/IEC 17799（以下「2000年版」）は、2001年から改訂作業が開始され、管理策が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」というマネジメント領域が新たに括り出された改訂ISMS（以下「2005年版」）が、2005年6月に発行されている。

ISMS：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

マネジメント
領域の追加

	概要
<p>(1) 産業分野別の ISMSの策定</p>	<p>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。</p> <p>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、<u>電気通信事業分野についてはITUにおいてISMS-T</u>がそれぞれ策定されている。</p>
<p>(2) ISMSの確立・ 運用に対する支援</p>	<p>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。</p> <ul style="list-style-type: none"> 組織内の情報セキュリティのための体制 社員の教育訓練 内部監査 個人情報保護等、法制上の要請への対応 技術上の対策との連携や技術上の対策の適用方法 <p>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。</p>
<p>(3) 国際的なクロス ボーダー認証</p>	<p>ISMSは国際規格であることから、ある国でISMS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仕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。</p>

3.3 ISMS - Tの概要と今後の改訂の方向性(1)

ISMS - Tは、2000年版のISMSを踏まえ、2004年にてITUで勧告されたもの。今後は、2005年版のISMS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	

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、電気通信分野に固有の管理策は盛り込まれていない。

現行のISMS - Tには規定されていないが、電気通信事業者に対しては、次のような法令上の要求事項があることから、今後、これらの要素を追加すべきか否かについて検討する必要がある。

通信の秘密の保護(電気通信事業法第4条)

不当な差別的取扱いの禁止(電気通信事業法第6条)

重要通信の優先取扱(電気通信事業法第8条)

接続義務(電気通信事業法第32条)

他人の電気通信設備の機能に障害を与えないこと等(電気通信事業法第41条及び52条)

個人情報保護法

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、その他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。

1. ISMS - Tの国内における展開

ISMS - Tは、ITUにおいて我が国が中心となって検討を進め、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。

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。

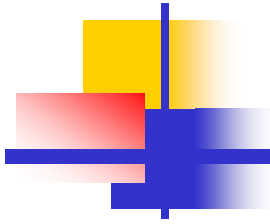
その際、2005年版のISMSが2005年6月に発行されていることから、その内容を踏まえることを始め、電気通信事業分野に固有の法令上の要求事項を充たすことのできるよう、検討を加えていくことが必要。

2. 国内における普及促進

ISMS - 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。

3. 国際貢献

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。

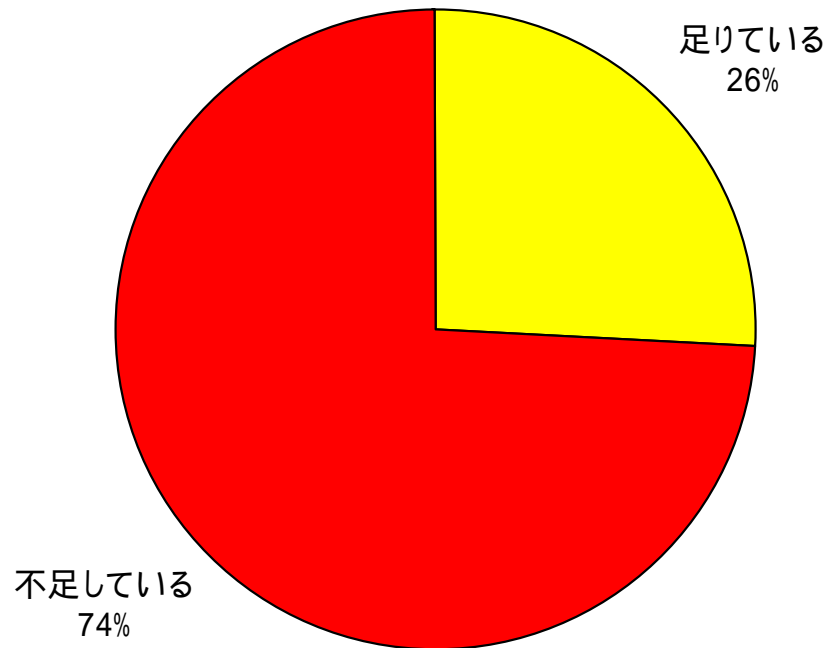




第4章 セキュリティ人材育成

4.1 我が国におけるセキュリティ人材の現状(1)

電気通信事業者に対するアンケート結果(注1)によれば、74%の事業者において、セキュリティ人材(注2)が不足



<有効回答197社>

(注1) 総務省が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て実施したアンケート

(注2) 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

セキュリティ技術・知識面の課題

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ない。

インターネットの分野は技術革新が激しく、それに応じて対応を要するセキュリティ事案も多様化しており、社外の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機会が多い。

セキュリティ人材は、技術から法令まで多くの技能・知識の習得が必要であり、その育成には多くの時間と高額な費用を要する。

ネットワーク運用・費用面の問題

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。

地方においてはセキュリティ講習が開催されていないことから、地方で事業を展開している電気通信事業者にとっては、従業者を社外の講習会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。

セキュリティ技術・知識の評価に係る問題

社外の講習等に自社の従業者を受講させたとしても、それによって得られるセキュリティ水準がどの程度か判定が難しい。

4.2 他のICT先進国におけるセキュリティ人材の育成策

米国の事例

米国では、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1）においてCAEIAE（注2）と呼ばれる人材育成プログラムを実施

このプログラムには、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3）やSFS（注4）の奨学金制度への申請権が与えられる。

シンガポールの事例

シンガポール情報通信開発庁（IDA）において、「重要な情報通信技術資産プログラム」（CITREP（注5））と呼ばれるICT人材育成のプログラムを推進

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

米国 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

シンガポール 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	<ul style="list-style-type: none"> 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

(注1) NSA: National Security Agency

(注2) CAEIAE: The National Centers of Academic Excellence in Information Assurance Education

(注3) 国防総省情報保証奨学金: Department of Defense Information Assurance Scholarship Program

(注4) SFS: Federal Cyber Service Scholarship for Service Program

(注5) CITREP: Critical Infocomm Technology Resource Program

セキュリティ資格については、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。

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効。

- (1) 資格や認定の効果が有効期限付きのもの
- (2) 実機を使った演習があるか
- (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

我が国におけ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、テレサ協、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))	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ニ ストレータ試験	(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, Management)	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。	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

4.4 事業者をまたがるサイバーテロ演習

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。

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・情報セキュリティ基本問題委員会の第2次提言（2005年4月）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

「想定脅威の広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。

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おり、我が国においても、

（セキュリティ専門家による）実行可能な攻撃方法と攻撃による損害の程度の検証、

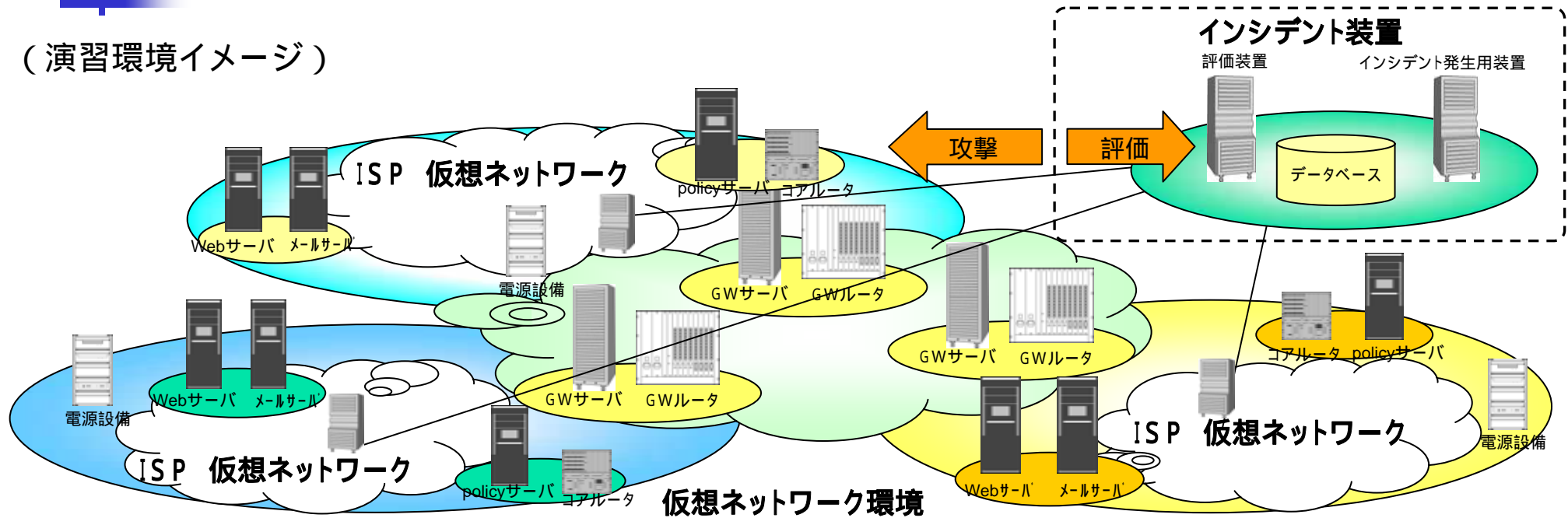
攻撃発生後の緊急対応体制が実際に機能するか否か

について、演習を通じて検証しておくことは有益。

こうした演習には、セキュリティ講習等に参加す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が異なる場合のある情報家電機器メーカー等の参画を得ることが望ましい。

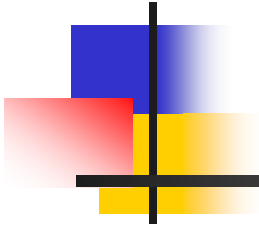
(参考) 攻撃を想定した総合的な演習 (イメージ)

(演習環境イメージ)



米国における攻撃を想定した演習

演習名称	実施時期	実施主体	演習の概要
The Day After	1996年3月	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。
Eligible Recover	1997年6月	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。
Digital Pearl Harbor	2002年7月	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。
Livewire	2003年10月	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。



第 5 章

総括

5.1 今後、集中的に取り組むべき3つの課題

「ネットワーク」、「モノ」、「人材」という3つの側面の脆弱性を克服する政策を推進することにより、社会インフラとしてのインターネットの「安心・安全」を実現

「ネットワーク」を通じた障害の広域化への対応

ネットワーク感染型ワーム
D o S 攻撃
ボットネット

経路情報の誤りによる障害

IPインフラ

ネットワークに繋がる 「モノ」の多様化への対応

情報家電について

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

「人材」面の脆弱性の克服

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

経営陣によるセキュリティマネジメントの未実施

電気通信事業者におけるセキュリティ人材の不足

「ネットワーク」を通じた障害の広域化への対応

ボットネット対策に関する研究開発

広域モニタリングシステムの構築・強化

経路情報の誤りによる障害

の検知・回復・予防に関する研究開発

IPインフラ

ネットワークに繋がる「モノ」の多様化への対応
(情報家電のネットワーク接続への対応)

接続検証と規格化

- ・業界をまたがる接続検証と相互利用可能な規格化の実施
- ・責任分界の明確化、接続管理方式の策定

機器認証の規格化

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等の対応)

- ・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の対応を約款/契約で明確化

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と総合的演習の必要性

「人材」面の脆弱性の克服

一般ユーザへの啓発

- ・自覚がないまま他のユーザに攻撃を加える可能性も。
- ・個別の注意喚起や情報提供等、踏み込んだ啓発が必要。

ソーシャルエンジニアリングの研究と対応策の提示

- ・従業者の無知・無警戒、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(ソーシャルエンジニアリング)を研究し、対応策を提示。

電気通信事業者におけるセキュリティマネジメント

- ・電気通信事業者向け指針を2005年中にも提示。
- ・2005年秋以降のITUにおける検討に我が国も積極的に貢献。

総合的な演習の必要性

- ・中小・地方のISP、情報家電機器メーカー等の参画を得て、実行可能な攻撃方法と攻撃による損害の程度、攻撃発生後の緊急対応体制の課題を検証。

「情報セキュリティ政策 2005」

課題		政策の内容	何時	誰が				
	小分類			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 社内の従業員教育 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 引続き 早急に					(06年以降の支援策検討)	