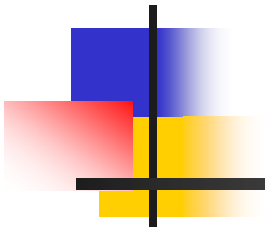
WG５－３

セキュリティＷＧ　検討報告骨子（素案）

平成１７年４月２７日

目　次



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

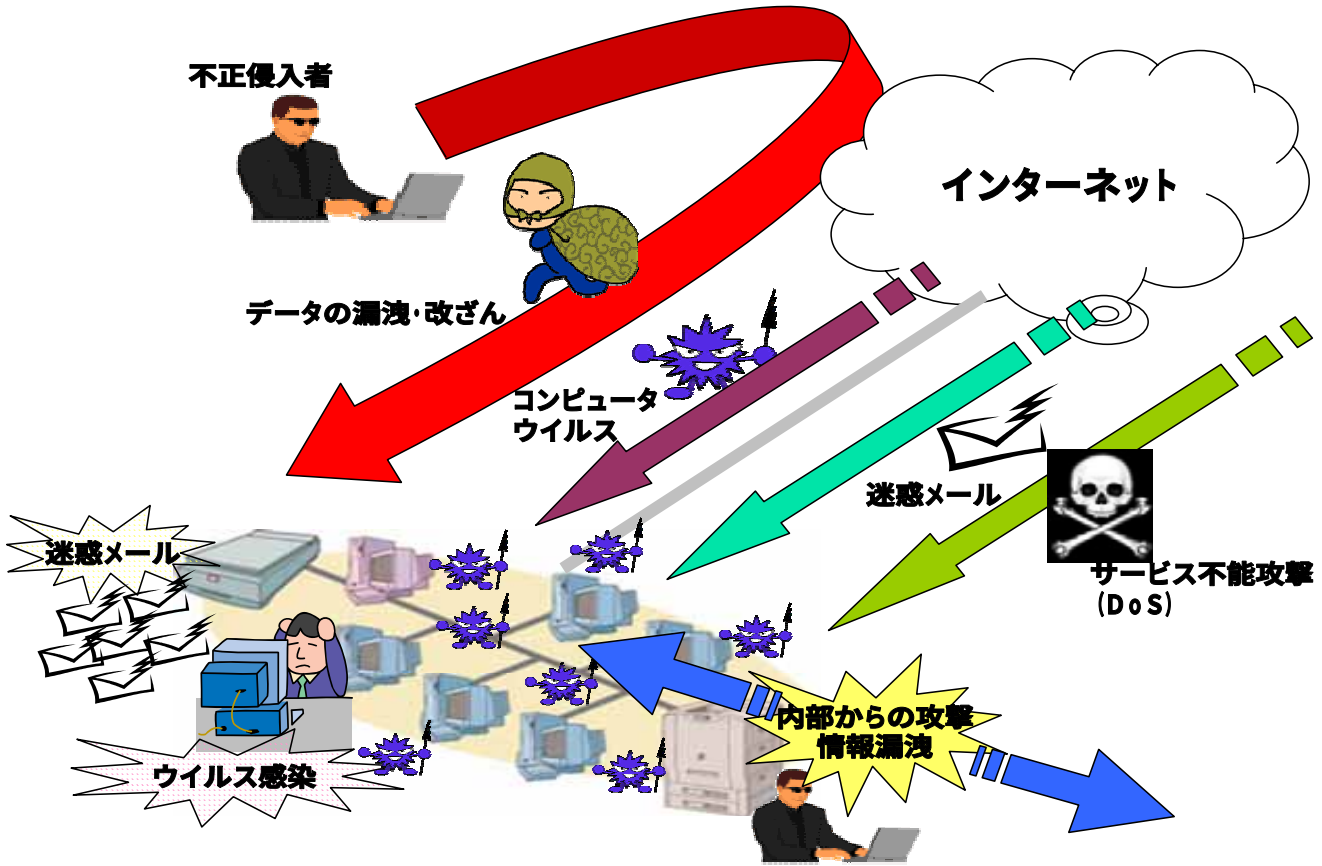
① 不正アクセスやウイルス、ワーム等によるICT障害（以下、「インシデント」という）

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

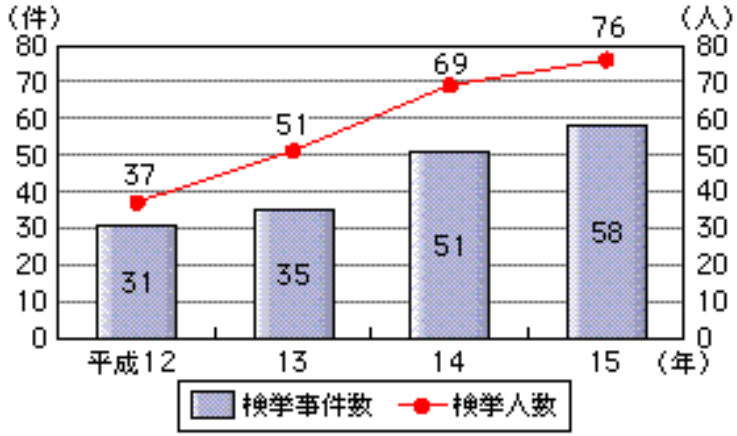
} 本報告で取り上げるICT障害

▽　インシデントのイメージ図



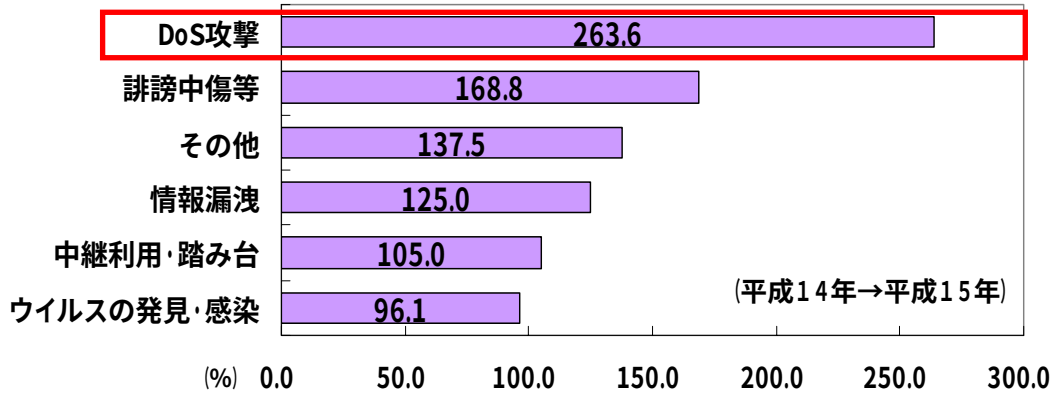
１．２　インシデントの最近の傾向（１）

不正アクセス禁止法違反事件の検挙状況の推移



ＤｏＳ攻撃の増加率が高い

▽　企業情報通信ネットワークにおける被害内容とその増加率



ウイルス／ワームの悪質化

～　昔　～

○ フロッピディスク等の記憶媒体を介した感染

悪質化

～　現在　～

○　電子メールやWebサイトにアクセスするだけで感染
○　ネットワークに接続しているだけで感染

▽　ウイルス／ワームの悪質化

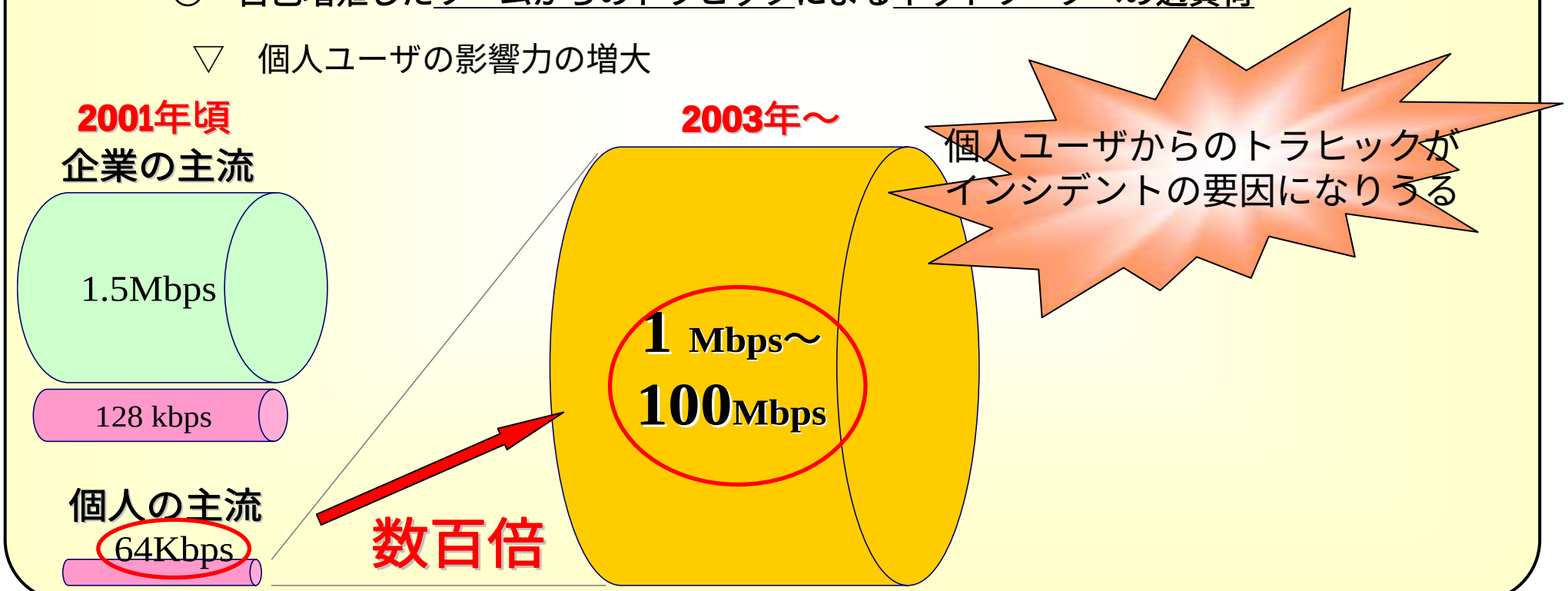
	感染方法	対　策
昔	媒体(フロッピ等)により感染	①ウイルス対策ソフトによる検知・駆除 ②不審なフロッピを使わない
最近	メールやWWWアクセスにより感染	①OSアップデート、②ウイルス対策ソフトで駆除 ③不審なメールの添付ファイルを開かない
2003年以降	**ネットに接続するだけで感染**	①OSアップデート ②ファイウォールやルータで不審なパケットを遮断

個人ユーザの影響力の増大

○　常時接続・定額料金のブロードバンドの普及により、従量課金の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
１．３．１　2003年　～ネットワーク感染型ワームへの対応（１）～

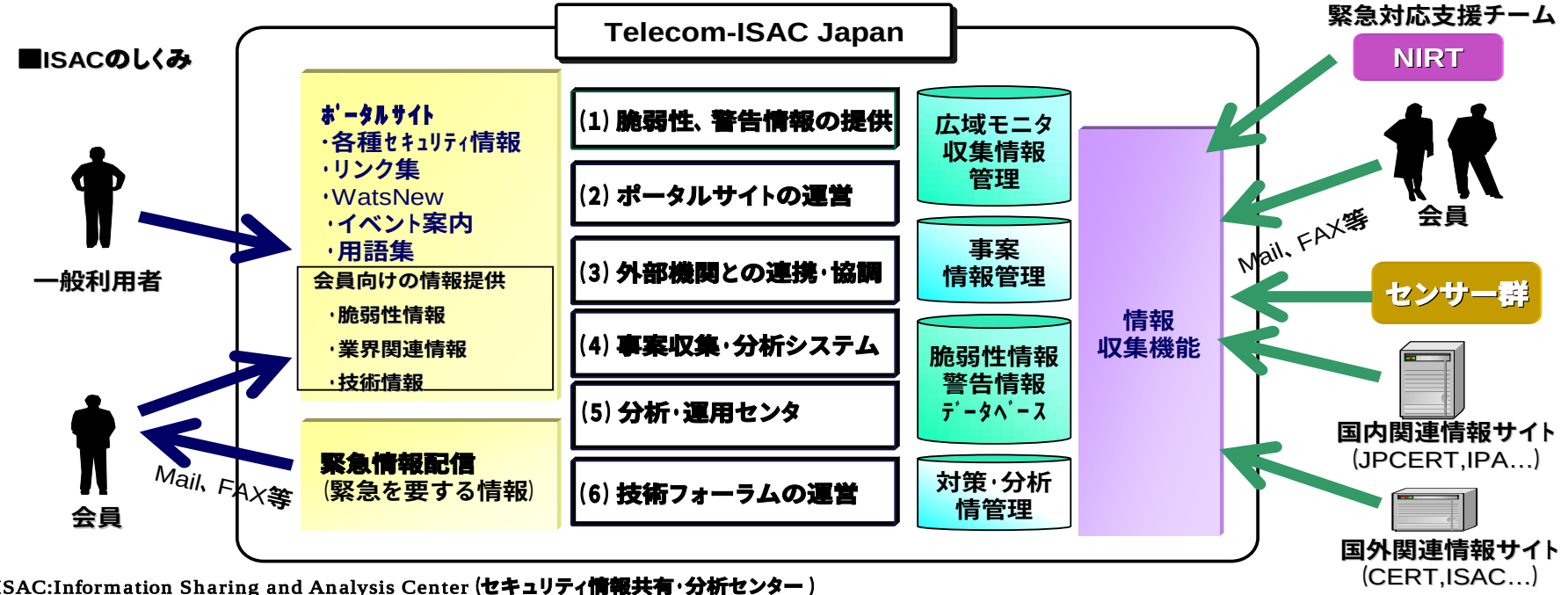
○ 大量メール送信型ワームは、ネットワーク全体に与える影響が無視できないことから、ISP側における対応も必要になる。

○ インシデント情報の収集･分析･共有を目的として、ＩＳＰ等で構成されるTelecomーISACの対応事例を紹介

▽　Telecomー ISAC Japanの概要

■Telecom-ISAC Japanの目的
通信業界に属する企業のサービス基盤において発生したインシデントに関する情報を収集･分析し、その結果を業界内で共有すること。

■Telecom-ISAC Japanの役割
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サイバー攻撃、コンピュータ犯罪等の脅威及び被害情報の提供



ISAC:Information Sharing and Analysis Center（セキュリティ情報共有･分析センター）
設立：2002年7月　メンバー：NTTコミュニケーションズ、KDDI、日本テレコム、パワードコム、 NEC、 IIJ、ニフティ、ヤフー、松下電器、日立製作所、横河電機、沖電気

▽　ブラスターの蔓延とTelecom-ISAC Japanの対応

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

▽　ソービッグＦの蔓延とTelecom-ISAC Japanの対応

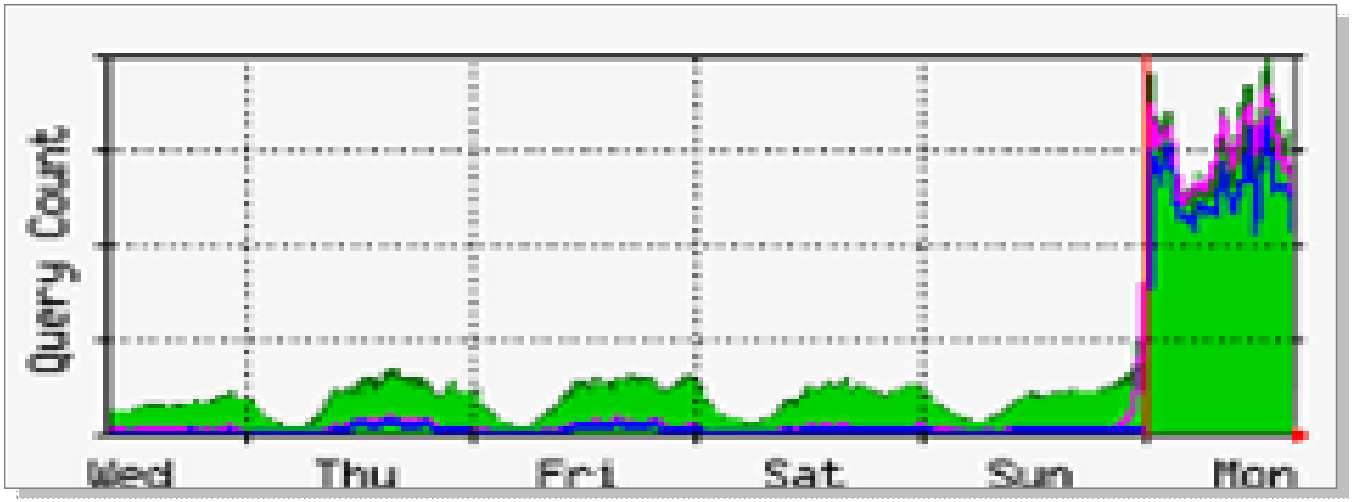
日時	内容
8/19	ソービッグＦの出現 欧米で感染が拡大との情報
8/19夜	日本でもAVシステムで急速な感染を確認
8/20	ＩＳＰによるユーザ周知（各社対応）
8/22	ソービッグＦの解析情報入手 トロイの木馬機能の活性化が23日早朝にプログラムされているとの情報
8/23	緊急対応 トロイの木馬がダウンロードするサーバIPアドレス20を遮断 （攻撃は不発のため後日対策解除）

１．３．２　2004年～ＤｏＳ攻撃（Antinny）対応事例（１）～

Antinny（アンチニー）

- ○ Winnyユーザに感染、特定日に特定のWebに個人情報をアップロードする機能を持つワーム
- ○ アップロード先のDNSの名前解決ができるまで、ISPのDNSサーバに対して、無限に名前解決要求を行う。
- ○ 攻撃を受けていたユーザ側では、攻撃回避のためDNSサーバの設定を変更。
- ○ 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サービスからのエラー処理により、ISPのDNSサーバに高負荷
- ○ 各ISPにおいて「ブラックホールIPアドレス」を設定し、多量のトラヒックを“疑似サイト”で破棄することにより、Antinnyに対応。

▽　ＯＣＮ提供　DNSサーバへのアクセスの急増



2004.4.5 Mon

※Antinny（アンチニー）：P2P（Peer to Peer）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

１．３．２　2004年～ＤｏＳ攻撃（Antinny）対応事例（２）～

○　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

○　DoS攻撃からの回避策は、DoS攻撃を受けないようにすることはできても、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

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　～

インシデントへの対応は、ＩＳＰ１社だけでは限界。

○　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、トラヒ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**

等

○　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取り組んでいくことが適当

１．４　２００４年　～ボットネット対策の黎明期～

「ボットネット」とは

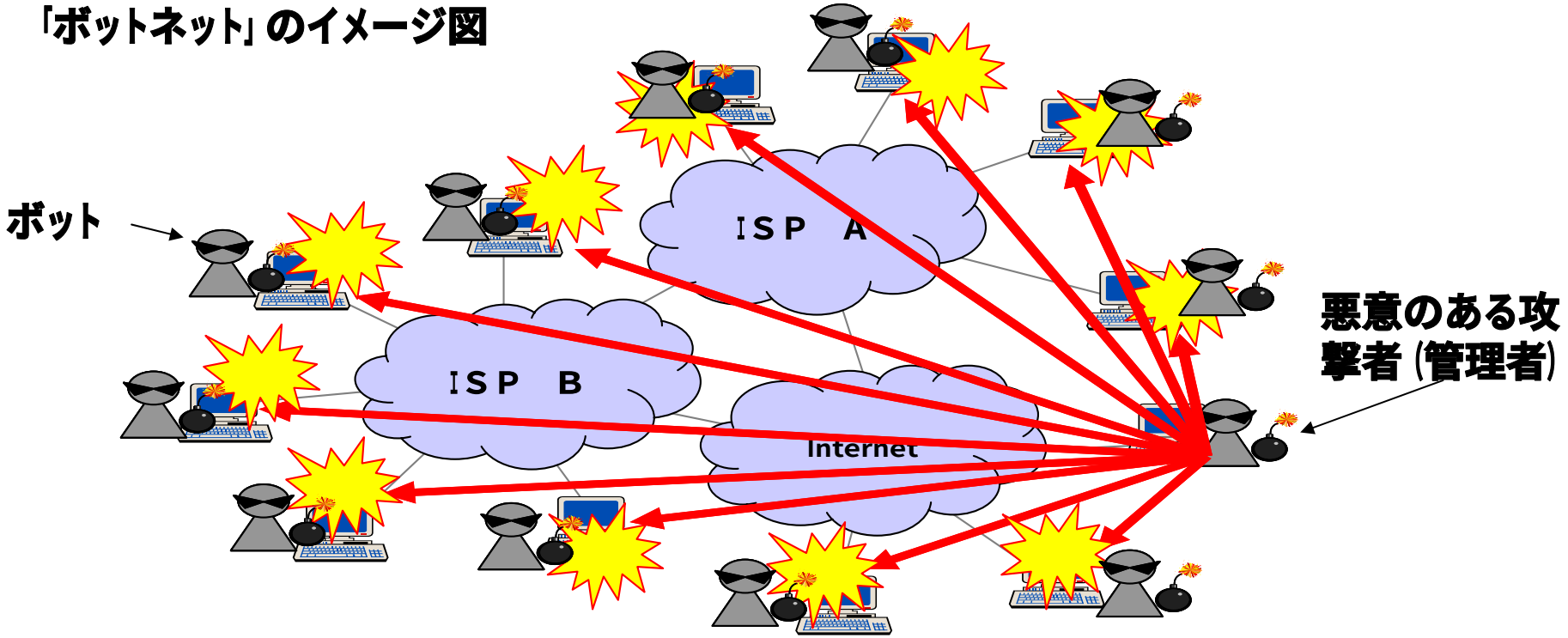
○ 「ボット」とは、悪意のある攻撃者（管理者）の指揮命令下に置かれたコンピュータ

○ ネットワーク経由の連携動作により、サーバー攻撃等にコンピュータを悪用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ＤｏＳ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。

「ボットネット」のイメージ図



１．４．１　ボットの特徴

(1) 他者を攻撃しうる機能　スパムメール送信機能、DoS攻撃機能等を有する。

(2) スパイウェア機能　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により統率の取れたサイバー攻撃を行うことができる。

(4) ネットワーク化

ボットプログラムの種類、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、攻撃の発信元を分散させ、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

任意のWebサイトからファイルをダウンロード又はインストールし、当初のボットとは全く異なるボットに変わったり、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から、ユーザは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

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けたバックドアを介して感染する。

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。

１．４．２　ボットのもたらす脅威

(1) スパムメール等の送信･中継

スパムメールを送信し、中継することができる。

実在しないアドレスに対する送信が大量に行われる場合、エラーメールメッセージの送信によるトラヒックが膨大となり、一種のＤｏＳ攻撃と化すこともある。

(2) フィッシング (Phishing) 詐欺

ボットを使ってフィッシングWebサイトのURLを記載したスパムメールを送信し、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ることで、個人情報を不正に入手することができる。

(3) ＤｏＳ攻撃

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ＤｏＳ攻撃を行うことができる。

(4) スパイウェア機能

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。

以上のように、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と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きている。

１．４．３　ボットプログラムの蔓延の背景
１．４．４　対策の現状

蔓延の背景

○ **２００３年に猛威を振るったネットワーク感染型のワームが媒介したことにより、短期間に広く拡散した可能性**

○ **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蔓延の背景**

対策の現状

○ **セキュリティ意識の高くないユーザが多い。**

・**最新のセキュリティパッチ、ウイルス対策ソフト、ファイアーウォール等の導入が不十分**

○ **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。**

・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**。

○ 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

今後の課題

(1) 技術上の課題

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

(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。

(3) 体制に上の課題

○ 感染防止と早期駆除に関しては、検体の収集・分析・解析のために、セキュリティ・ベンダー、機器ベンダー、ＩＳＰからなる協力体制を構築することが必要。また、これら各業界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。

○ 攻撃の予防と防御に関しては、ＩＳＰ相互の連携体制が不可欠。

１．５　ユーザのセキュリティ対策

ユーザのセキュリティ対策の実態

○ ＯＳの脆弱性が発見されるたびに、最新のセキュリティパッチを適用するようISP等から呼掛け

○ しかし、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

○ 特に、ボットについては、次の事情もあり、これまで以上にユーザへの啓発を図る必要

① ユーザ側にボットプラグラムに感染しているという自覚がない

② こうしたボットが既に大量に存在

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、他のユーザのコンピュータに攻撃を加える可能性

１．５　ユーザのセキュリティ対策

セキュリティ対策実装の役割分担

○　常時接続の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、ユーザは大きなパワー

○　インターネットが広く国民一般に普及するに伴い、セキュリティ等に関する専門知識を有しないユーザが増大

○　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、ユーザ等の関係者間での役割分担が必要である、という考え方を社会一般に醸成し、関係者が協力して社会全体のセキュリティ水準の向上に努めていくことが必要

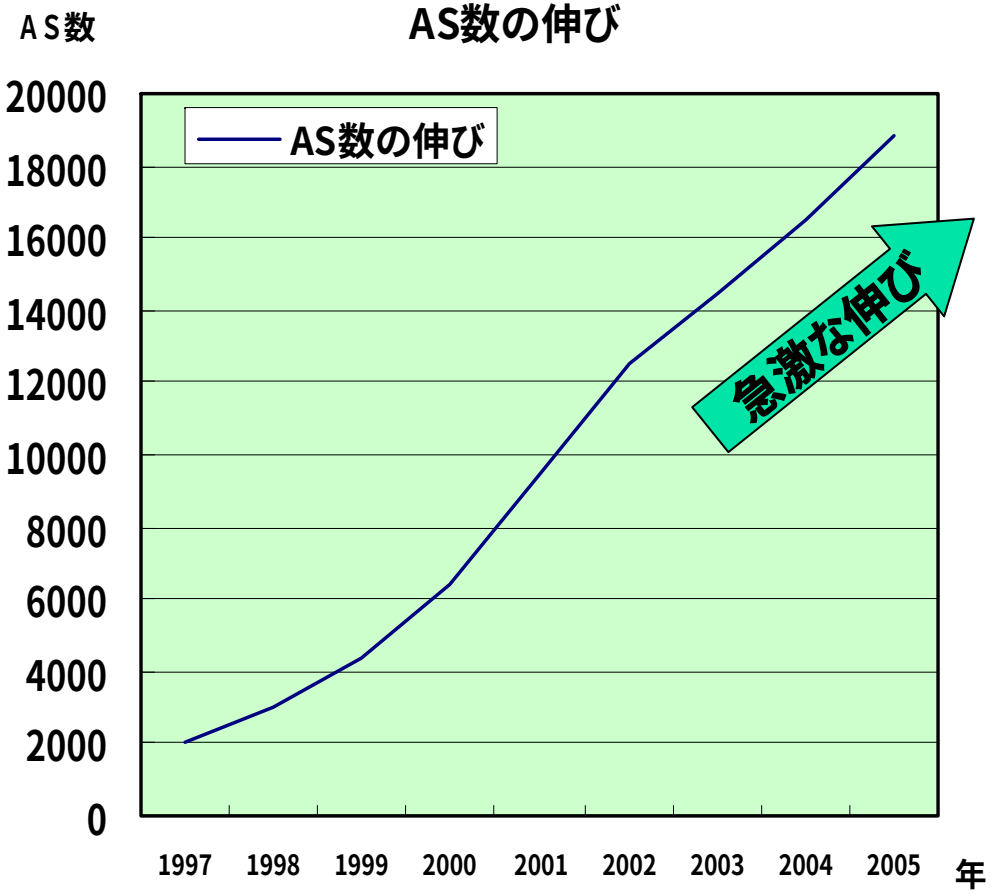
○特に、ユーザのコンピュータがボット化していることが判明した場合には、当該ユーザへ個別の注意喚起や駆除の方法に係る情報提供を行う等、これまでよりも踏み込んだユーザ啓発が必要

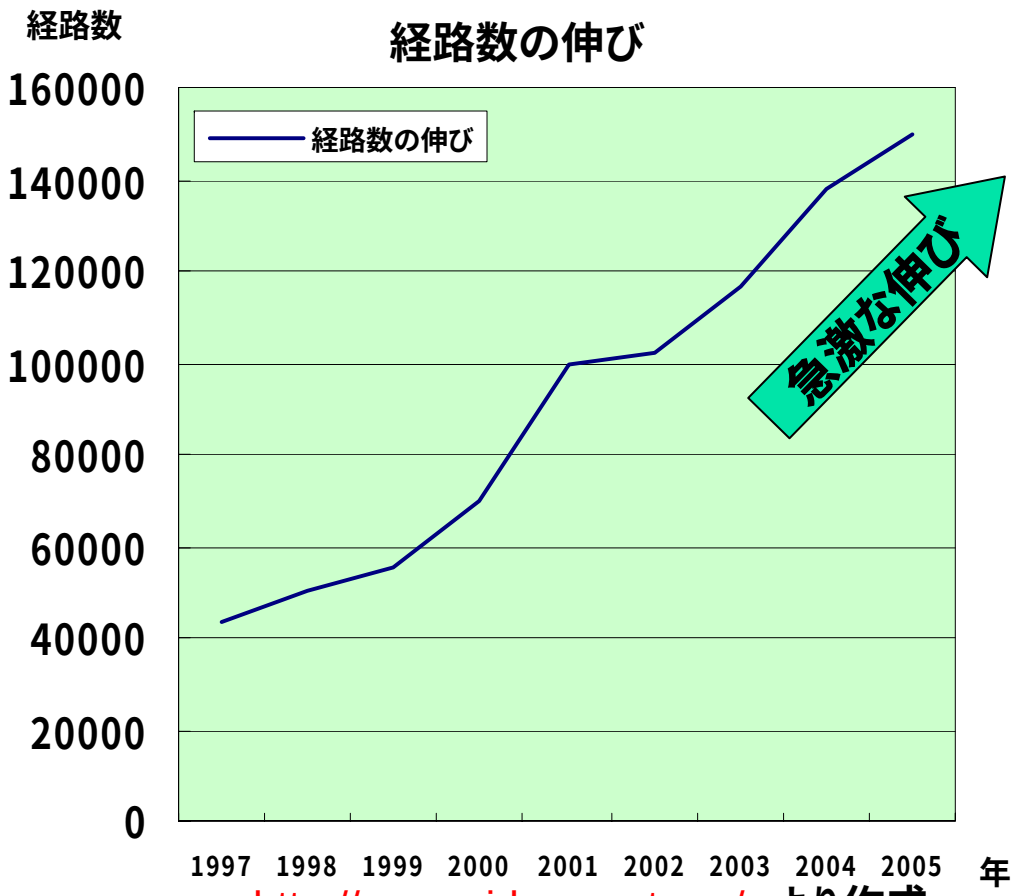
○　また、ISPの電気通信サービスに支障を来たしている場合等において、警告、利用の一時停止、更には契約解除といった措置をとることができる旨を、約款又は契約で予め明確化しておくことも求められる。

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

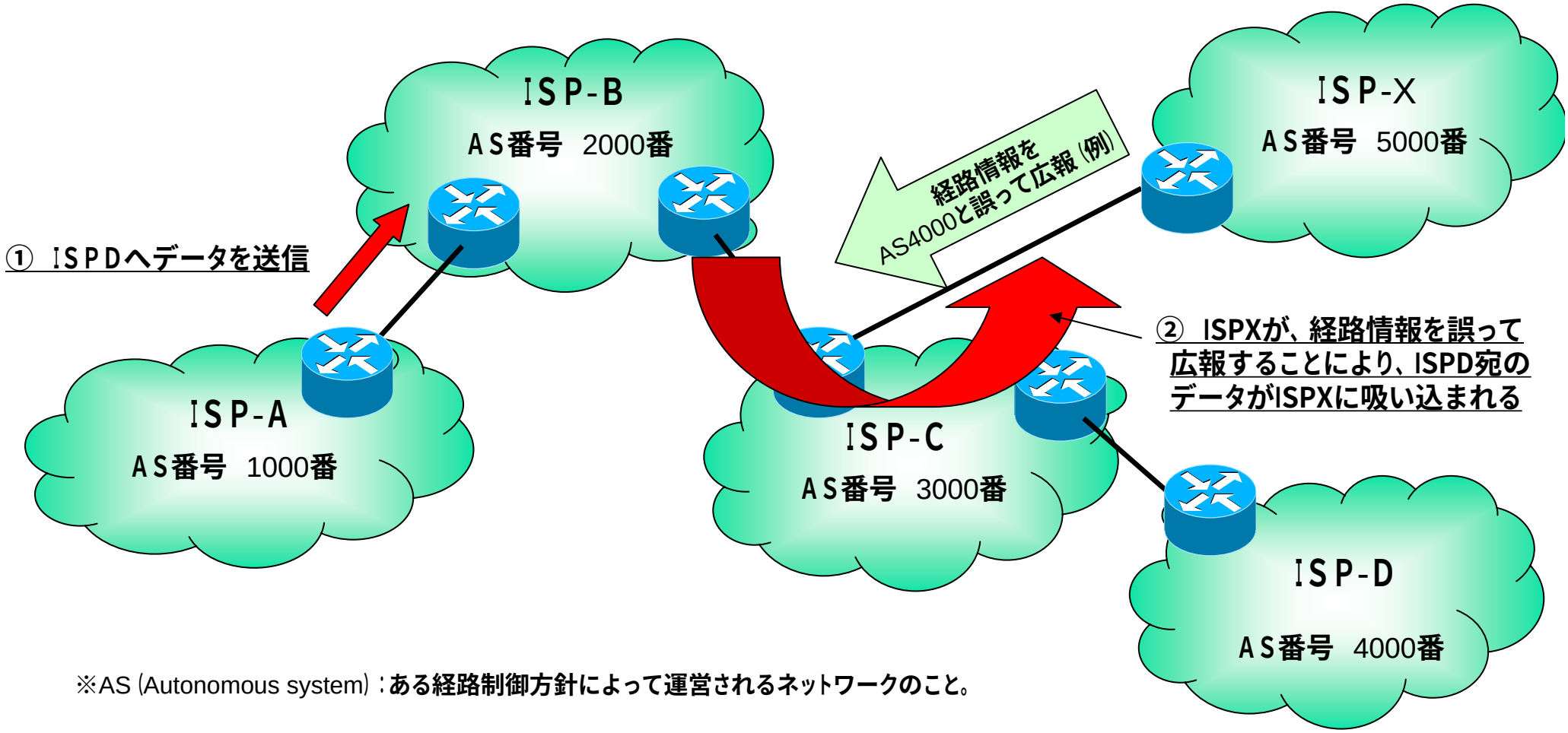




http://www.cidr-report.org/ より作成

１．６．２　経路情報の誤りによるICT障害

・ISPX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。**

１．６．３　経路情報の誤りによるICT障害への対応策

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

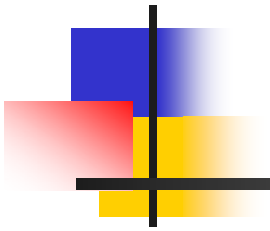
○特に、海外のＩＳＰがひき起こした経路情報の誤りに際しては、ネットワーク運用に対する考え方の違いや言語の違い等から、その対応には相当の時間を要する。

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。

(3) こうした技術開発を進めるとともに、誤った経路情報を意図的に広報することによる組織的な攻撃が発生する場合に備え、普段からＩＳＰ同士が連携することも重要。



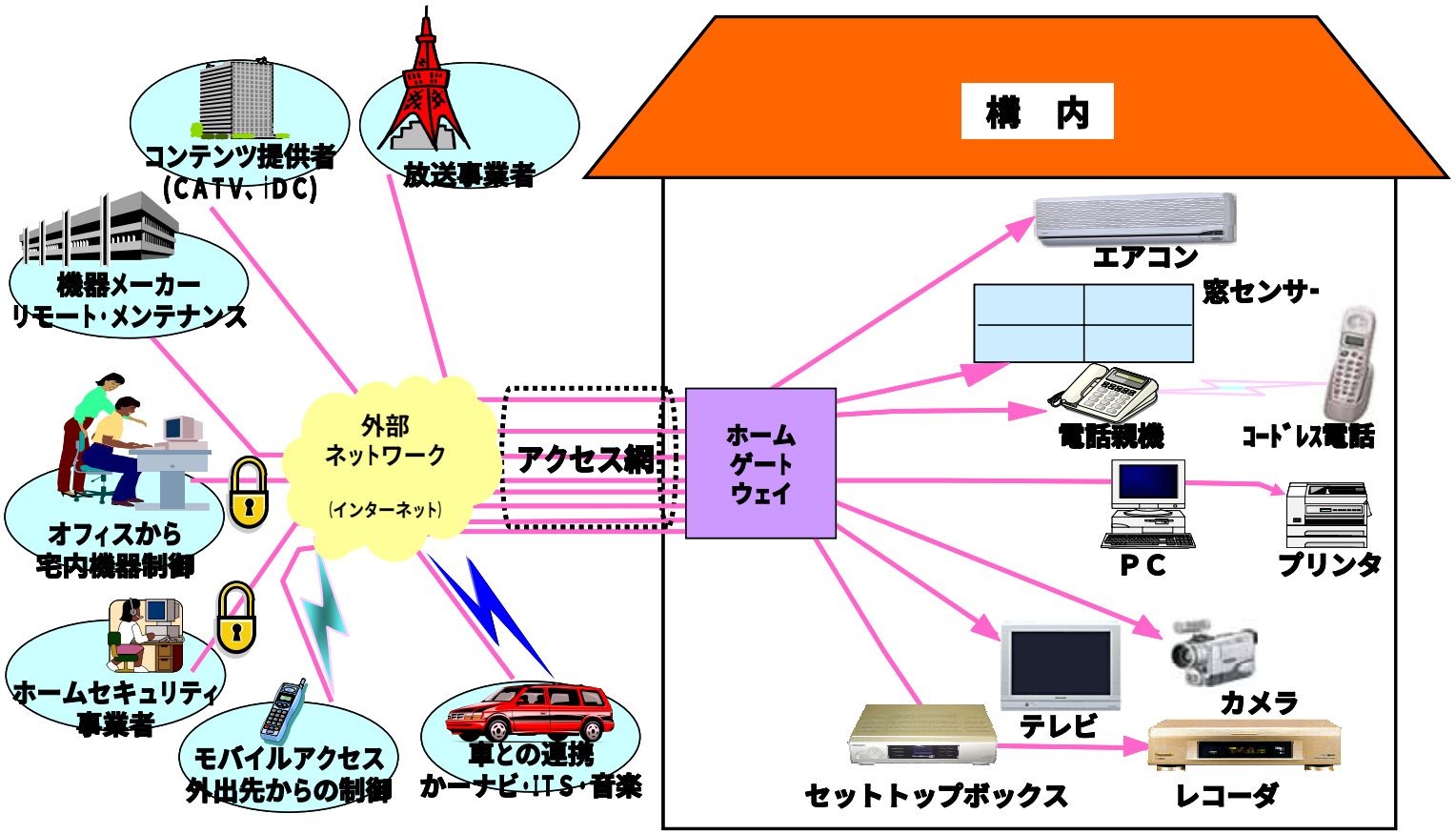
第２章　情報家電のセキュリティ確保

２．１　情報家電に対する期待と課題（１）

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、「ユビキタスネットワーク社会」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



２．１　情報家電に対する期待と課題（２）

▽　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

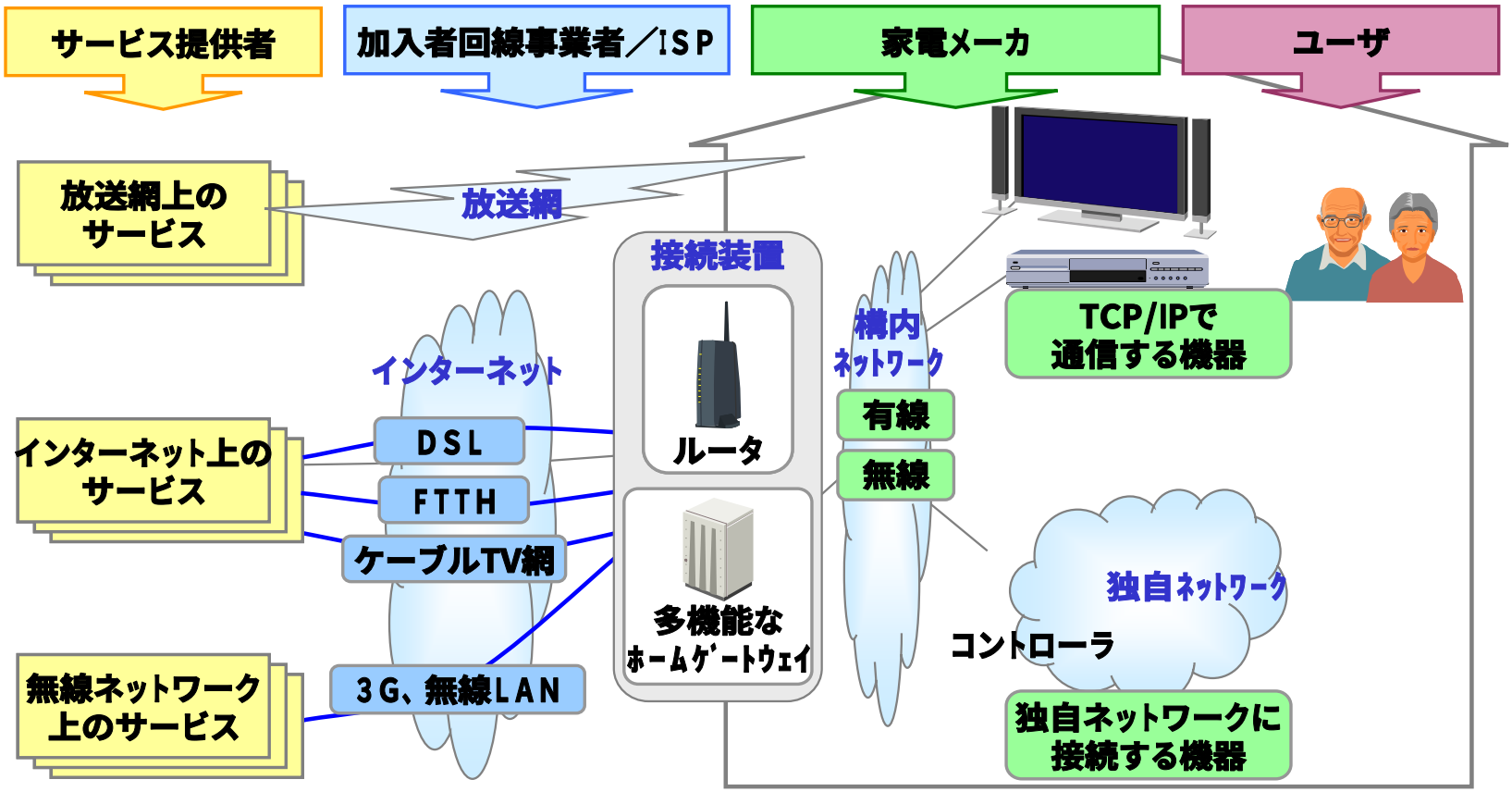
機器の連携	宅外リモコン(機器遠隔制御)	①エアコン ②VTR/DVD機器 ③風呂	６９.９％	簡単・快適
機器の連携	蓄積番組の視聴	好きなときに好きな番組が見られる(ｷｰﾜｰﾄﾞ自動番組録画・リモート視聴)	５４.６％	感動
機器の連携	くらし安心	①ｶﾞｽ/火災 ②不審 ③部屋 ④照明 ⑤施錠	５１.３％	安全・安心
サービス・機器の更新	TVによる情報提供 映像・情報配信	①ＢＢサービス　②TV電話等	４５.７％	感動
サービス・機器の更新	TVによる情報提供 地域情報や電子チラシの配信		３９.７％	簡単・快適
サービス・機器の更新	TVによる情報提供 定点観測監視モニタ	①行楽地や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

２．１　情報家電に対する期待と課題（３）

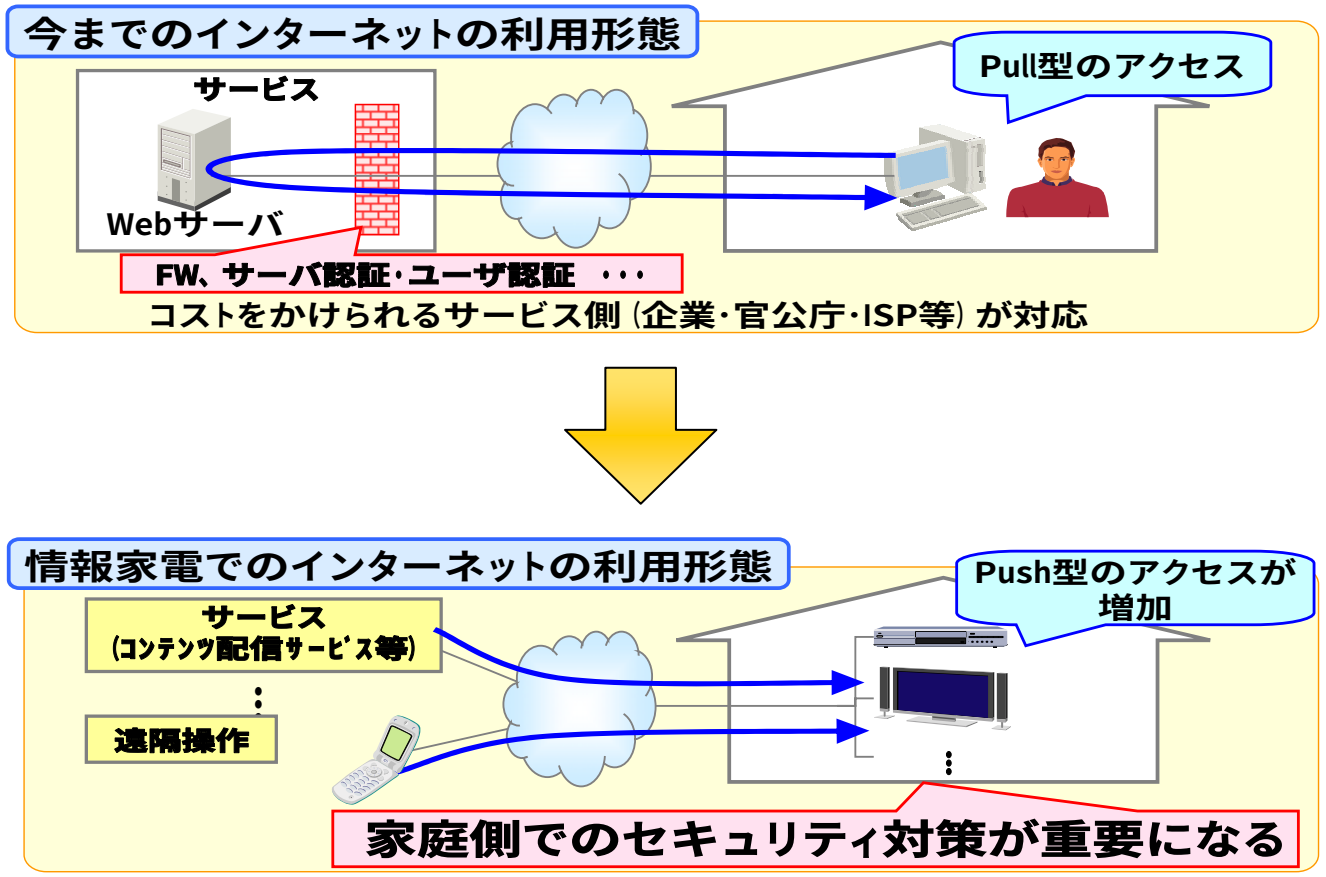
▽　情報家電によるサービスに関わる様々な業種

情報家電によるサービスには、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。



２．１　情報家電に対する期待と課題（４）

▽　アクセス形態の変化



○　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。

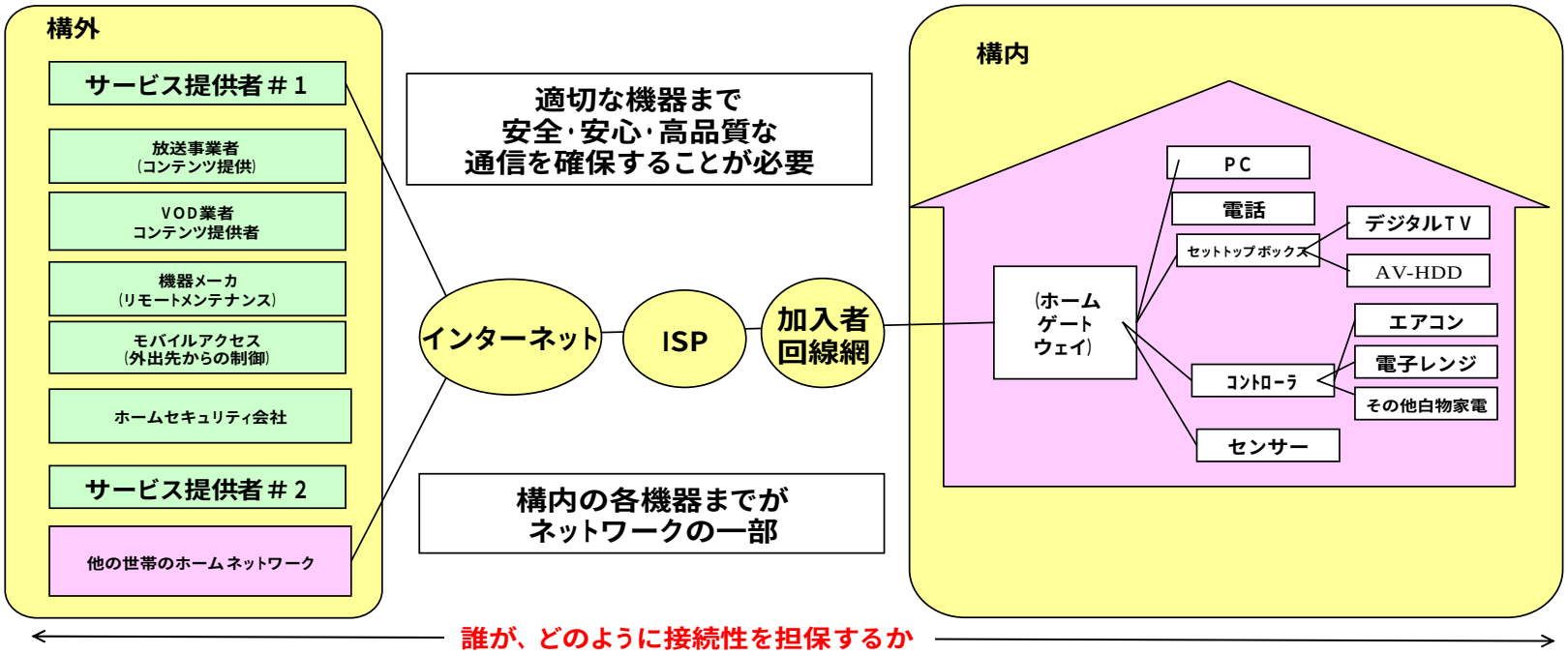
２．２　情報家電のセキュリティ確保に関する課題
２．２．１　接続検証

○ 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。

○ 各社ごと接続検証を行うのでは、件数も無限大となり、非効率。業界の枠を超えて接続検証を行うことが適当。

○ 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。

接続検証件数＝N（サービス提供者）× N（ISP）× N（加入者回線事業者）× N（ｹﾞｰﾄｳｪｲ）× N（宅内ﾈｯﾄ）× N（IP情報家電）× N（非IP情報家電）＝∞



２．２．２　情報家電がボット化した場合の対応

ＩＳＰからすれば、情報家電機器は、コンピュータと同様、ワームやボットプログラムに感染する恐れのある端末機器であり、情報家電機器がボット化して、

①当該情報家電機器との接続がＩＳＰの電気通信設備を損傷し又はその機能に障害を与える場合、

②当該情報家電機器との接続が他のユーザに迷惑を及ぼす場合、

等においては、接続の停止やサービスの停止を行うことがあり得る旨を、予め約款又は契約で明確化し、ユーザに周知しておくことが必要と考えられる。

２．２．３　コンピュータとの比較

▽ セキュリティ確保におけるコンピュータと情報家電の異同

同じ点	違う点
①　コンピュータのOSはWindowsに集約されているが、情報家電のOSはLinux、TRON等に集約されつつある、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。 ②　接続環境が千差万別で、接続検証に手間がかかる。	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。 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。 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。 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応が必要になると、結果としてセキュリティの水準が低い製品に揃ってしまう可能性がある。

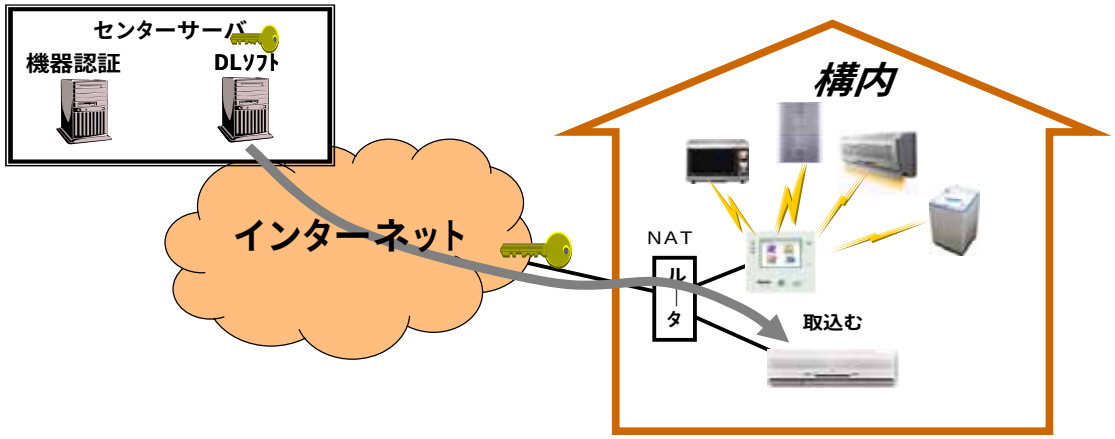
２．２．４　リモートメンテナンスと機器認証

リモート･メンテナンス

○　情報家電のＯＳやソフトウェアへの脆弱が発見された場合、修正プログラムを構外から配信するリモート･メンテナンスが必要となってくる可能性大。

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、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。

２．２．５　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、元のユーザが情報家電を通じて利用するサービス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

○　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。

２．３　家電業界とＩＳＰ業界との情報交換・情報共有の必要性

○　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、家電メーカとISPとの間で、連絡窓口も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求められている。

２．４　政府による支援の必要性

このまま何も対策を打たないと・・・

① 情報家電を攻撃対象とするインシデントが発生した場合には、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につながりかねない

② 情報家電を踏み台としたインシデントが発生した場合には、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

③ 情報家電について、現段階で対策を打たないまま、脆弱な機器が大量に市場に出回った場合は、回収等が困難。

政府による支援の必要性

○ 情報家電に関する脆弱性を検証。

○ 情報家電からの大容量のトラヒックがインターネット全体に与える負荷を抑制。

○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。

⇨ これらの検証作業を、政府として早急に支援していくことが必要。