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、サイ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。

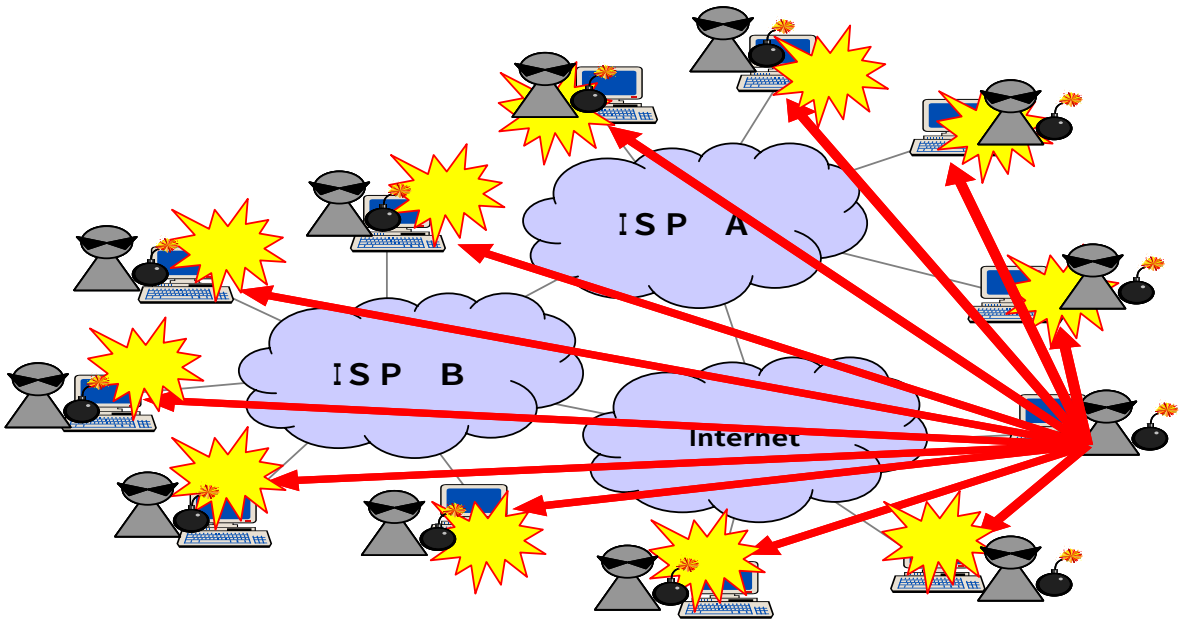
また、同一のボットプログラムの指揮命令下にあるコンピュータ群を「ボットネット」という。

（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。

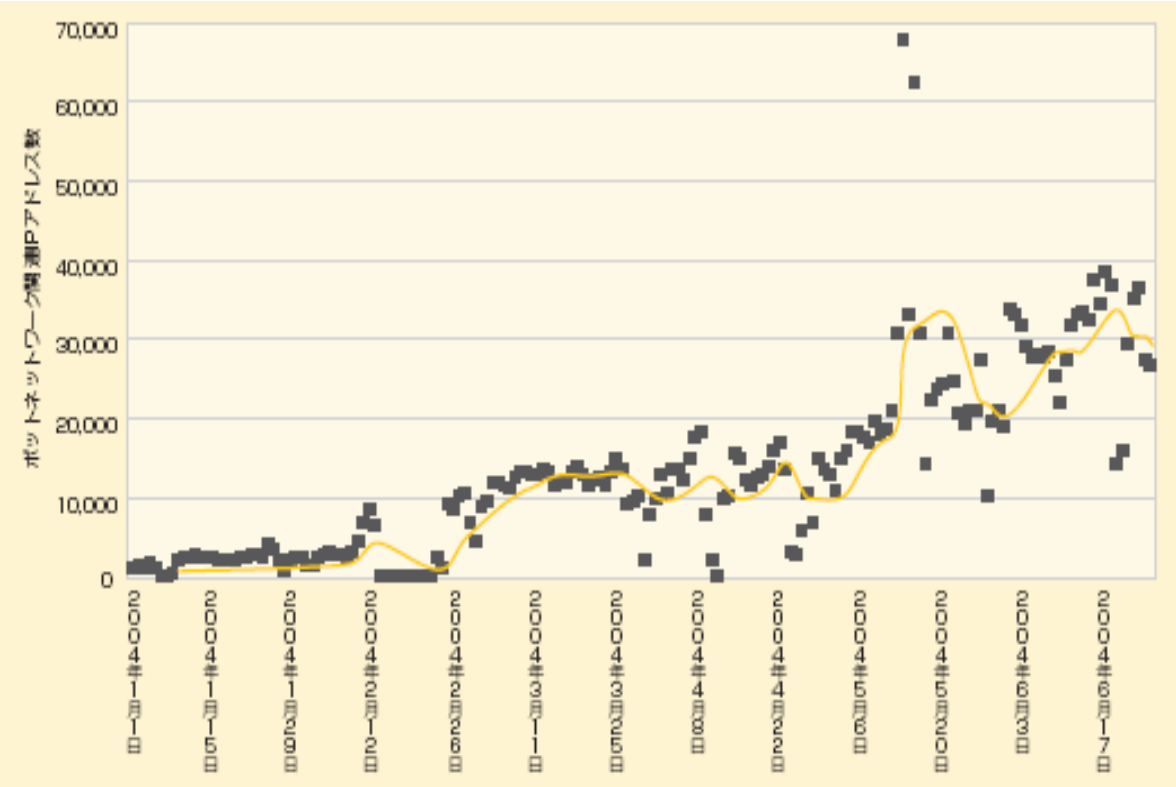
また、一斉に同一の攻撃を行うゾンビの一群をゾンビクラスターと呼ぶ。ボットネットはゾンビクラスターの一種である。

▽　ボットネットのイメージ図



<u>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。</u>

▽　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ＤｏＳ攻撃機能等、他者を攻撃するのに使用する機能の 1 つ又は複数を有する。

（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ＩＲＣ（Internet Relay Chat）が利用されている場合が多い。

ＩＲＣ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、ＩＲＣ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。

ＩＲＣ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、ＩＲＣ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）。

ＩＲＣ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ＩＲＣ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、統制の取れたサイバー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（ダウンローダー機能、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(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、手動か自動的か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・ベンダーは、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・ベンダーが「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。

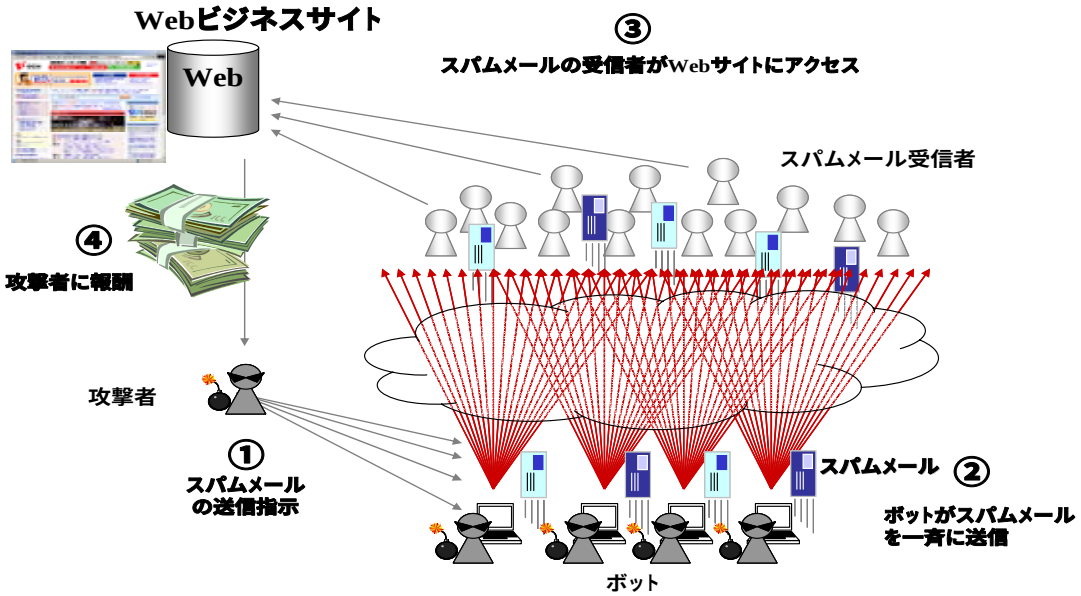
１．４．２　ボットネットがもたらす脅威

ボットネットがもたらす脅威は、次のものが挙げられる。

（1）スパムメール等の送信・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。

▽　ボットを活用したスパムメールビジネス

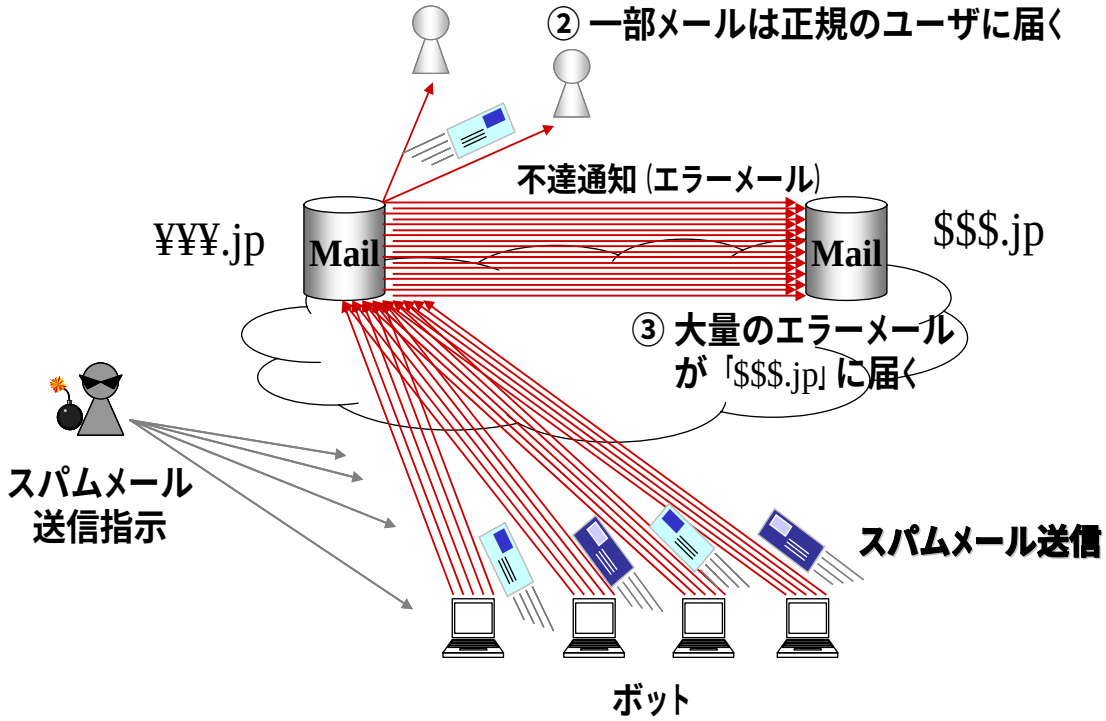


送信の宛先については、あらかじめリストアップされたメールアドレスや自動生成されたメールアドレスを利用する。

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ヒックが膨大になる。

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



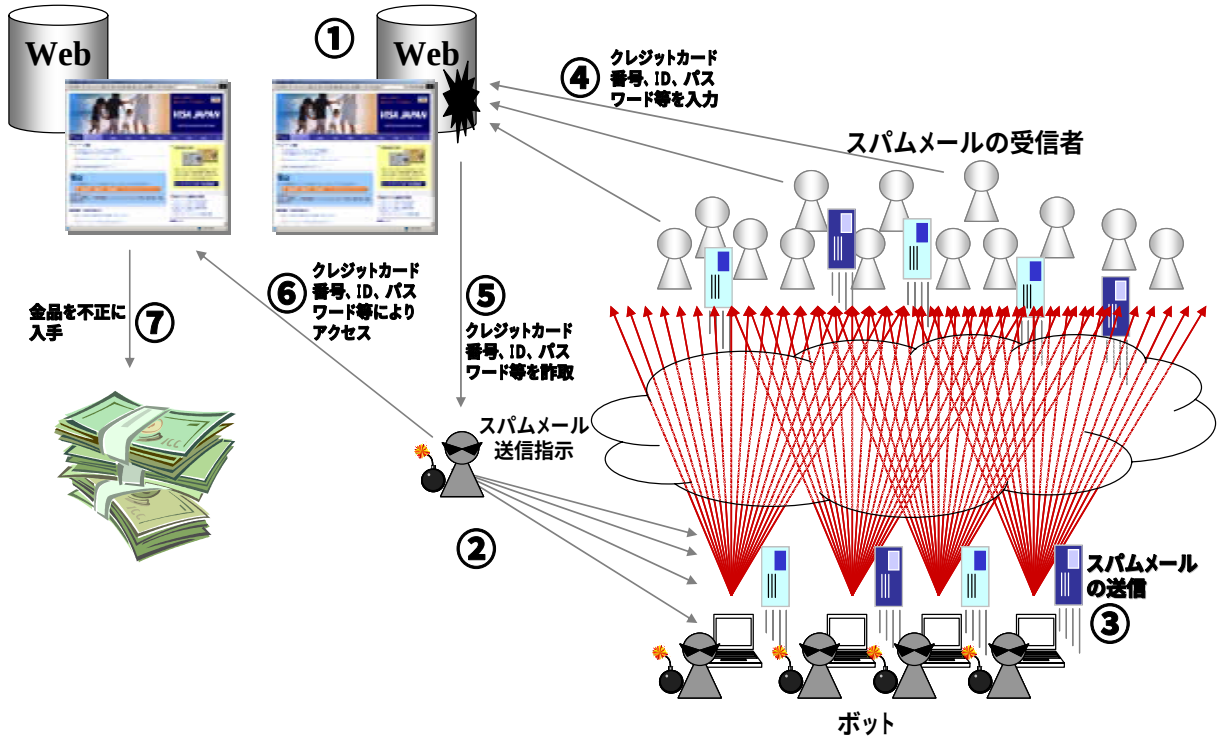
① 送信元を「$$$.jp」ユーザと詐称したスパムメールを「¥¥¥.jp」ユーザに送信

（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。

このとき、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



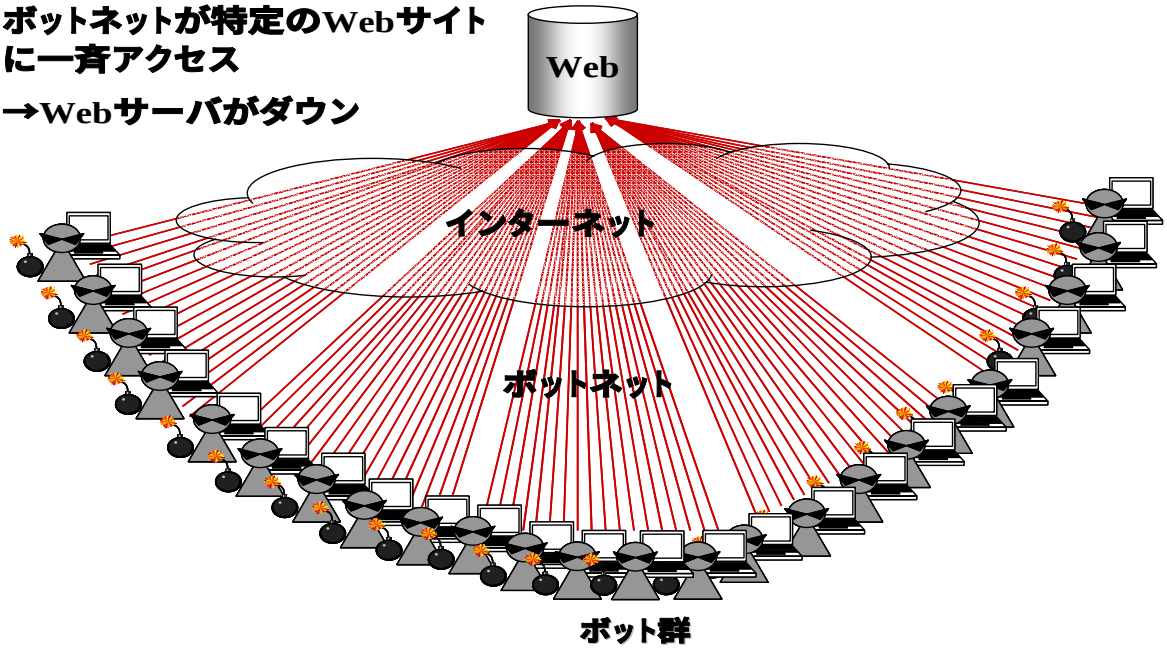
（３）ＤｏＳ攻撃

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ＤｏＳ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ＤｏＳ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、上述した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、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ＤｏＳ攻撃



（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（ブローカー）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ッグ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ことが必要である。

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。

これまでのサイバー攻撃では、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」ことと、「ボットネットの攻撃から守る」という２点について対策を採る必要がある。

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・ベンダーにおいては、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、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いるユーザへの警告、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、関連業界と政府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・ベンダー、通信機器メーカ、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・ベンダー、通信機器メーカ、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ず、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くことが必要と考えられる。

具体的には、セキュリティ・ベンダー、システム・インテグレータ、ＩＳＰ、通信機器メーカ等が連携して、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することが重要である。

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、ユーザのコンピュータが次のような弊害をもたらしている場合には、スパムメールと同様、当該ユーザへの警告、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よう。

① ＩＳＰの電気通信設備を損傷し、又はその機能に障害を与えている場合。

② ＩＳＰの電気通信設備を利用する他の利用者に迷惑を及ぼしている場合。

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にあっては、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、明確な指針を従業員に対して示されなければならない。

また、セキュリティポリシーの目的と動機付けについて、従業員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、従業員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員に示すことも重要である。

これにより、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、従業員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

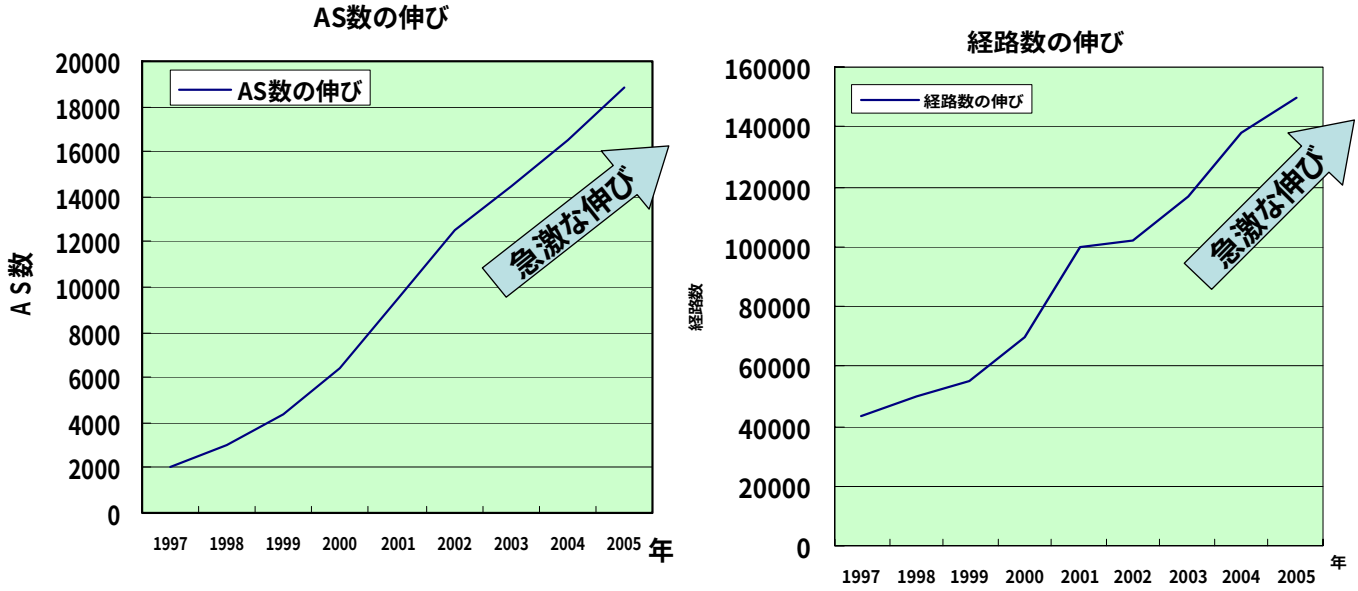
これまでは不正アクセスやウイルス、ワーム等、意図的要因によるインシデントについて検討してきたが、以下では、経路情報の誤りによるＩＣＴ障害について検討する。

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開始以来、現在まで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



http://www.cidr-report.org/　より作成

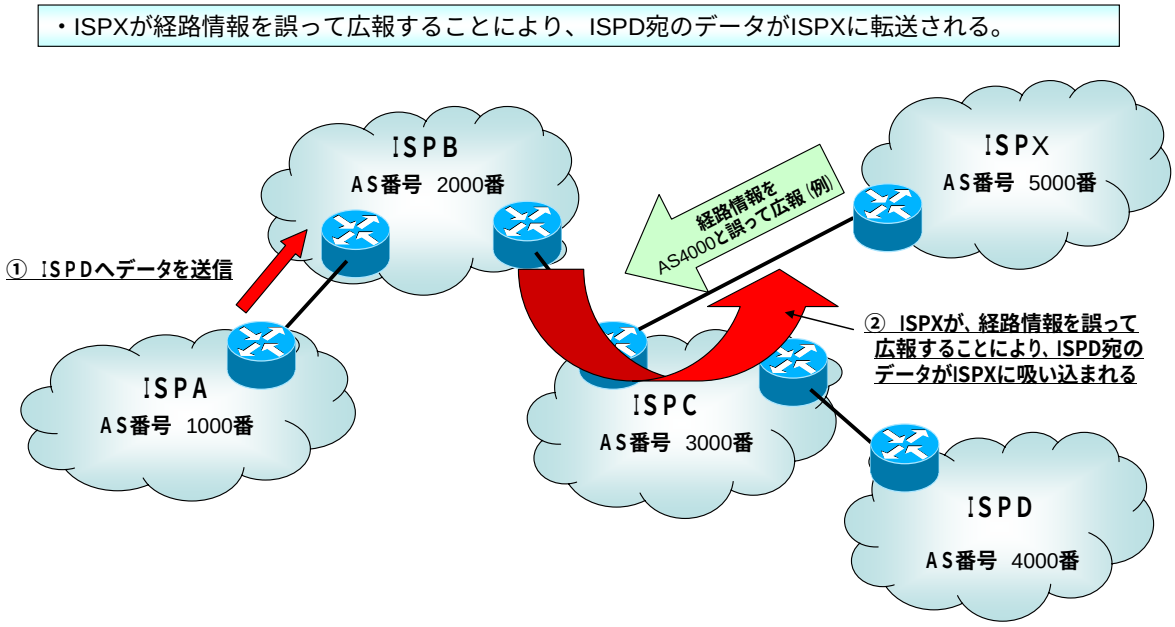
１．６．２　経路情報の誤りによるＩＣＴ障害

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のトラヒックを“吸い込む”（適切なＩＳＰにトラヒックを受信させず、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）



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が引き起こす経路障害の誤りや、海外のＩＳＰによるトラヒックの吸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つと言える。

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憑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、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、予防を行うことが求められる。

この点については、経路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、経路障害の回復、経路障害の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。