８．障害連鎖防止

（１）通信障害連鎖の事例

２．で述べたとおり、「e-Japan 戦略Ⅱ」に盛り込まれたＩＴの利活用を進めていくためには、将来的なトラヒック増加に対応するだけでは十分ではない。

多数のネットワークが多様に接続することによって成り立っているインターネットにおいては、一つのネットワークにおける通信障害が全体に波及するおそれがあり、インターネット全体の安定した運用を確保する観点から、障害連鎖を防止するためにどのような方策（ＩＳＰ間の連携、技術開発等）が必要かつ有効か、という点も検討しておかなければならない課題である。

インターネットは、発展を続けるオープンなネットワークであり、様々なサービスやコンテンツが生まれるワークベンチであるというメリットを有する一方、「隣人が信じている隣人（第三者）を信用する」ということを前提として成り立っているネットワークであり、適切な対策を講じなければ障害や攻撃に対して無防備であるというデメリットを有している。

実際、インターネット上では、様々な通信障害が起こっており、各ＩＳＰでは、いわゆる「モグラ叩き」のように対策を講じてきているのが実状である。

通信障害連鎖の事例

原因	内容
経路情報の誤り（海外）	1997 年 4 月、ある米国 ISP(AS 番号 7007)から大量の経路情報が逆流。これにより、インターネットは 12 時間以上にわたり経路が混乱。
	1997 年 10 月、UUNET(AS701)が誤った経路情報を大量に広報。
	2003 年 2 月、海外の ISP から日本のある ISP の誤った経路情報が広報されたため、 当該 ISP のネットワークオペレーションに支障を来した。
経路情報の誤り（日本）	1994～95 年、NSPIXP における誤った国際経路情報の広報により、ルータに過負荷。
	2000 年 9 月、ある ISP から IX を含む経路情報を誤って広報。１つの誤った経路情報で IX におけるパブリック・ピアリングがダウン。
	2002 年 1 月、ISP から誤った国際経路情報が大量に広報。
DDoS 攻撃(分散拠点からのサービス拒否攻撃)	1997 年、Cisco 社のルータの工場出荷時設定の不備をついた攻撃
	2001 年、Yahoo!、Microsoft 等、特定の有名サイトを狙った DoS 攻撃
	2002 年 10 月、インターネットのドメイン・ネームを管理する 13 台のルートサーバを狙った攻撃
	2003 年、メールやセキュリティ・ホールをついたワーム (*) が流行。韓国では、インターネットの大規模な停止が発生。

（＊）通常のコンピュータウイルスは感染の対象となるファイルといっしょになってパソコン間を移動するが、そのようなファイルを必要とせずに、自力で多くのパソコンに感染するウイルスのことを「ワーム」という。

（２）通信障害の定義と種類

通信障害とは、ＩＳＰの電気通信設備の故障やネットワーク運用時のオペレーションミス等により通信に支障が生じることをいい、障害により、①通信ができなくなる、②回線容量に対して過度のトラヒックが集中し輻輳が発生する、といった事態を招く場合が多い。

通信障害には、障害の範囲が１つのＩＳＰ内にとどまり他のＩＳＰに影響が波及しないものと、他のＩＳＰに障害が連鎖して被害が拡大するものとがあるが、本WGでは、後者の通信障害への対応策について検討した。

（３）連鎖する通信障害の種別と原因

通信障害の原因には、ＩＳＰ側で不適切な経路情報を広報してしまう場合と、端末設備からのDoS攻撃やウイルスによる場合とがある。

連鎖する通信障害の種別をその原因ごとに整理すると、下表のとおりである。

▽　通信障害の種別と原因

種別	内容	原因
経路障害	・不適切な経路情報が広報され、通信ができなくなる。 ・経路の確立・切断が頻繁に行われる等により、ルータ間の接続が不安定になる。	・通信装置の故障やバグ ・ＩＳＰの運用ミス ・不正アクセス、不正制御
パケット転送障害	・異常なトラヒックが発生することにより、回線が輻輳する。	・利用者の端末設備がウイルス等に感染し、不正なトラヒックを送出 ・DoS攻撃　　等
アプリケーション障害	・ドメインネーム・サーバの障害により、名前解決ができなくなる（実際には希少）。	・ＩＳＰの運用ミスや不正アクセス、不正制御

（４）通信障害が発生した場合における対処の実状

それでは次に、通信障害が発生した場合に、実際にどのような対処がとられているかを見ておくこととする。

通信障害が発生した場合には、何よりもまず障害の状況を把握しなければならない。

障害状況把握の手段としては、接続しているＩＳＰ同士での情報交換、ＩＸ事業者

やＪＡＮＯＧ（JApan Network Operators' Group）で運営しているメーリング・リストの活用等があるが、実際には、各ＩＳＰのシステム担当者同士が携帯電話等で直接連絡し合うことにより、緊急対応している場合が多い。

障害が実際に発生した場合に、各ＩＳＰが講じている主な対処方法を挙げると、次のとおりである。

（ア）経路情報の誤り

経路情報の誤りには、電気通信設備の障害とは異なり、①アラームが出ないことから監視が困難である、②「経路が不安定」という点に関する定義や認識がＩＳＰごとに異なる、③障害の認識とその対策について人間の判断が介在するため迅速な対応が困難である、という課題を抱えている。

こうした中で、各ＩＳＰにおいては、次のように対処している。

▽　経路情報の誤りへのＩＳＰの対処

（ａ）他のＩＳＰのネットワークとの責任分界点に設置されるゲートウェイにおいて、不適切な経路情報を分別（フィルタリング）して廃棄する。
（ｂ）経路の確立・切断が頻繁に行われる等により、ルータ間の接続が不安定になった場合には当該ＢＧＰでのプライベート・ピアリングそのものを一時停止する。

しかしながら、この方法を採用するためには、正常なトラヒックまで止めてしまわないようにするため、バックアップとして他のＩＳＰへの通信経路を複数確保しておく必要があり、ＩＳＰにとっては費用が嵩む１つの要因となっている。

また、正常か異常かの判断自体が困難な場合が多いことに加え、約款上接続を一時停止できる旨の規定があったとしてもＩＳＰには営業上の配慮も働くことから、上記のうち、（ａ）のフィルタリングはまだしも、（ｂ）のプライベート・ピアリングの一時停止については実施しにくいとの指摘が、一部のＩＳＰからなされている。

（イ）ＤｏＳ攻撃やウイルス

ＤｏＳ攻撃において、攻撃先がＩＳＰのネットワーク内にある場合は、攻撃先である特定アドレス向けのパケットを一時的に破棄するという対処がなされている。

また、攻撃元が特定でき、かつＩＳＰのネットワーク内にある場合には、攻撃元の端末の管理者に対応を依頼するとともに、攻撃元の特定アドレスからのパケットをＩＳＰ側で破棄するという対処がなされている。

（５）障害連鎖の予防

上記（４）では、通信障害が発生した場合の「対処の実状」を見た訳であるが、それだけではなく、障害連鎖をどのように「予防」するかという点も重要である。

現在、各ＩＳＰに採用されている主な予防策は、以下のとおりである。

（ア）フィルタリングの活用

連鎖する通信障害のうち、予防の対策を講じることが可能なものとしては、不適切な経路情報の受信の予防がある。

実際には、ＢＧＰに一定のフィルタリング機能を設定することにより、予防策を講じているＩＳＰが多い。

フィルタリングの種類とその内容

種類	内容
AS-path フィルタリング	AS-path情報を交換し、AS(Autonomous System)(*)間の責任分界点に置かれるルータの設定において、AS-path情報にあった経路のみを受け取るようフィルタリング。
Prefix フィルタリング	Prefix(**)情報を交換し、AS間の責任分界点に置かれるルータの設定において、Prefix情報にあった経路のみを受け取るようフィルタリング。
Maximum prefix フィルタリング	受信する Prefix 数の上限を設定し、それを超える経路を受け取った場合に、アラーム発出または接続停止を行うようフィルタリング。
不適切情報のフィルタアウト	デフォルトルート、プライベートアドレス、マルチキャストアドレス、ループバックアドレス等インターネット上へ流すべきでない経路をフィルタリングして破棄。

（＊）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み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。

（＊＊）Prefix 情報とは、ISP 間で経路情報の交換を行う場合、アドレス空間を指定するための情報。アドレス空間の開始位置とアドレス空間の大きさの２つを組み合わせて指定される。

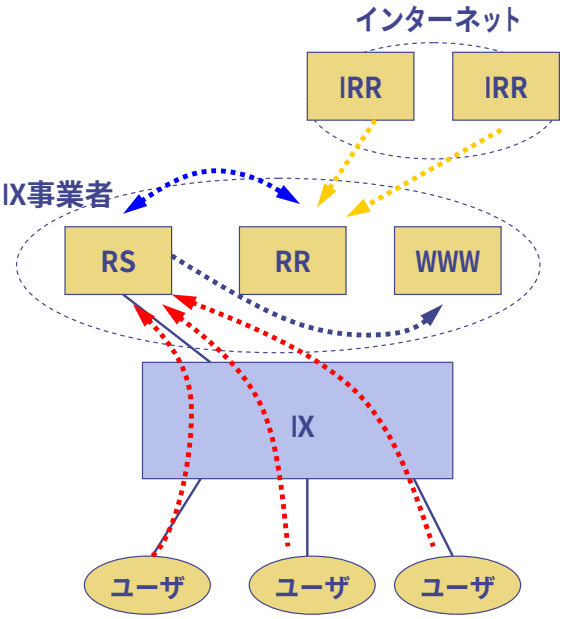
（イ）ＩＲＲ (Internet Routing Registry)の活用

ＩＲＲ（Internet Routing Registry）とは、インターネット上でのデータの経路情報、どの接続からどのようなデータをどのように優先的に流すかについての情報、また、その経路が誰に管理されているかについての情報を蓄積したデータベースのことをいい、既に多くのＩＲＲが存在している。

ＩＳＰにとってＩＲＲは、他のネットワークから受信した経路情報をＩＲＲに登録されているものと比較して経路情報を確認する場合や、ＩＳＰ間でフィルタリングを行う場合等に活用されている。

IRRを活用した経路情報の確認の仕組み（JPIXにおける事例）

- IRRに登録されている正しい(と思われる)経路情報をIXのRouting Registry (RR)にコピー
- IXのRoute Serer (RS) は、ISPから経路情報を受信
- RSで受信した経路とRR上の経路情報とを比較
- 比較した結果をWebサイトにてISPに提供



http://www.nic.ad.jp/ja/materials/irr/20030724/04_jpix.pdf

（ウ）ＩＳＰ間の協調

障害の連鎖を予防するためには、ＩＳＰ間の情報共有や連携が不可欠である。

現在では、ＮＡＮＯＧ（North American Network Operators' Group）、ＪＡＮＯＧ（JApan Network Operators' Group ）等の任意団体で情報交換が行われているほか、ＩＸ事業者が主催するメーリング・リストやミーティングなどにおいて、障害情報や障害連鎖防止のためのノウハウに関する技術交流等が行われている。

（６）障害連鎖防止に向けての課題

（ア）不適切な経路情報による障害連鎖に対する予防

第１に、各ＩＳＰにおいて経路情報の設定ミスや運用ミスにより、障害連鎖が発生しないようにすることが求められる。

このためには、Prefix フィルタリングを導入することが望ましいと考えられるが、その導入にはコストがかかる等、ＩＳＰ側に運用面で負担がある。

第２に、我が国においては、ＩＸを経由した経路情報の広報による障害連鎖が多いことから、相互接続における運用や接続方針を明確化することも求められる。

第３に、ＩＲＲの活用も有効であると考えられているが、全てのＩＳＰが登録している訳ではないので、その適用範囲が限定されている状況にあることから、多くのＩＳＰがＩＲＲに登録するよう、インターネットの安定運用のためにＩＲＲがどれほど有効かという点についての普及・啓蒙活動を行うこと等により、未登録ＩＳ

ＰにＩＲＲ登録へのインセンティブを与えていくことを検討すべきであると考えられる。

また、ＩＲＲの情報が適切に更新されていないため、ＩＲＲのデータベースの信憑性の向上自体が課題であるとの指摘もある。

この点については、ＩＲＲのデータベースの維持・更新・管理を随時行うこと等により、その信頼性を高めていくことが必要である。

この点については、我が国でＩＰアドレスの管理を行っているＪＰＮＩＣ（JaPan Network Information Center）において、ＩＲＲ企画策定専門家チームが設立され、ＩＲＲの活用促進策が検討されているが、今後とも、こうした活動が充実・強化されていくことが期待される。

第４に、ＩＳＰとして最低限守るべき運用方針やネットワーク品質の明確化を図ることも有効であると考えられる。

この点については、例えば、現在ＪＡＮＯＧ（JApan Network Operators' Group ）等の任意団体において情報交換や技術交流が行われているが、事業を開始したばかりのＩＳＰやこれから事業を開始しようとするＩＳＰに対して、障害連鎖防止のための運用のノウハウを普及・啓蒙させていくための施策も必要と考えられる。

インターネットの安定運用は、各ＩＳＰやＩＸ事業者の技術者がＪＡＮＯＧ等の民間団体における活動等を通じて情報交換や技術交流を行うことにより支えられてきているのが実情であり、こうした活動を肯定的に認知し支援することは、インターネットの信頼性を向上させていく上で重要である。

また、障害発生時には、自社の情報を他社と共有することが必要となるが、他方で、インターネット全体の安定運用を確保する観点から、自社の情報をどこまで出して良いか、また出すべきかについての基準は明確ではなく、各ＩＳＰやＩＸ事業者の技術者はジレンマに陥る場合も多い。

このため、障害発生時に自社情報をどこまで出して良いかについて、各ＩＳＰやＩＸ事業者において経営者レベルまで話を上げて、一定の考え方を整理しておく必要があるのではないかと考えられる。

いずれにしても、ＪＰＮＩＣやＪＡＮＯＧ等の活動は、費用がかかる一方で収益には直結せず、にもかかわらずインターネット全体の安定運用に資するものであることから、政府による政策支援の在り方を検討すべきであると考えられる。

第５に、インターネットにおける障害連鎖は、国境を越えて広がり得るものであり、国内のみならず、国際的な連携も必要である。

この点については、例えば、我が国で行われているＩＳＰ間の協調を国際間でも行い、国際レベルでのＩＲＲのデータベースの信憑性の確保や、障害連鎖防止のた

めの運用ノウハウの途上国ＩＳＰへの提供等を推進していくこと等を検討すべきである。

（イ）DoS攻撃やウイルスへの対応

DoS攻撃への対応としては、まず攻撃元の検出方法を確立することが有効であると考えられる。

しかしながら、攻撃元がアドレスを偽れば、技術的な対処をとりようがないのが実情であり、DoS攻撃やウイルスへの対応できるシステムの導入について、研究開発・実証実験の推進をするとともに、DoS攻撃やウイルスが発生した際のＩＳＰ間の協力体制についても検討すべきである。

また、端末設備側のセキュリティの向上も重要であり、端末設備やアプリケーション・ソフトそれ自体のセキュリティを高めるとともに、ＩＳＰ、通信機器メーカ、システムインテグレータ等において、利用者のセキュリティ意識を高め、セキュリティ対策が適切に実行されるための方策を見出す必要がある。