

インターネット情報インフラ防護のための技術調査

Report on the Vulnerability of the Internet Infrastructure

太田 耕平¹⁾, 阿部 勝久¹⁾, グレン マンスフィールド キニ¹⁾, 藤井 章博²⁾

KEENI Glenn MANSFIELD, Akihiro FUJII, Kohei OHTA, Katsuhisa ABE

1) 株式会社サイバー・ソリューションズ (〒989-3204 仙台市青葉区南吉成 6-6-3ICR ビル)

2) 宮城県立宮城大学 (〒981-3298 宮城県黒川郡大和町学苑 1 番)

ABSTRACT. In this paper, we examined the current security status of Internet infrastructure with special focus on wide-area routing, domain name service and directory service. These services form the base of the Internet infrastructure and their trustworthiness is implicitly taken for granted by users, applications, and network administrators. But this trust is misplaced in the absence of secure protocols and practices. We have pointed out this lack of awareness in the protocol designs and their implementations. We have discussed the areas that need urgent attention to make the Internet secure and reliable.

1. 背景

近年、インターネット基盤システムの重要構成要素に対して、そのセキュリティ脆弱性を攻略した攻撃や DoS 攻撃（サービス妨害攻撃）が行われ、社会的な問題となりつつある。これらの脅威の増大は、いわゆるサイバーテロの可能性および潜在的な影響範囲拡大を意味している。

最近では、2002 年 10 月 22 日早朝に、世界に 13 ヶ所存在するルートネームサーバに対するサービス妨害攻撃が発生した。ルートネームサーバのひとつは、日本の WIDE プロジェクトが管理しており、影響が大きかった 7 台のうちの 1 台であるが、一般ユーザに影響が出るほどの性能低下は発生しなかったという。

このような脅威による社会的なリスクを低減させるためには、インターネット基盤システムに関するセキュリティの現状を、技術的な観点から把握し、問題箇所および防衛手段の方向性を明確に認識する必要がある。

2. 目的

情報通信の要となる情報集合点のセキュリティを分析し、それらの利用状況、脅威に対する影響範囲を技術的根拠に基づいて把握するとともに、講じられるべき運用の改善策および技術開発を要する分野を明らかにする。

3. 通信セキュリティの現状

情報通信におけるセキュリティリスクの要素は多岐にわたる。これまでに多くのインシデントが報告されているが、実際にはソフトウェアやシステムの脆弱性等を個別に検討するだけでは、十分ではない。実際には、当事者のセキュリティ意識と運用が最も重要であることが指摘される。それらをセキュリティポリシーとして策定し、

確実に実施することが必要である。本章においては、情報通信にともなう危険性と現状におけるセキュリティ対策状況を調査分析する。

(1) バックボーンにおける通信状況調査

現在のインターネット利用者のセキュリティ意識およびトラフィックの現状を調査するため、バックボーンネットワークにおける通信プロトコルの利用状況を調査した。

現在の通信の現状を理解するために、国内の大規模ネットワークである WIDE のトラフィックデータ[1]を対象とした分析を実施した。対象データは一日あたり約 10 分間のサンプルである。分析対象は以下の通り。

観測対象ネットワーク Trans-Pacific line (18Mbps CAR on 100Mbps link)

a) 管理者等の比較的技能のあるユーザ

本調査において、最も広く普及し、各種 OS に標準で装備されている telnet とセキュアな通信環境を実現する SSH の利用率を比較した。比較は telnet と SSH の標準通信 port である 23 と 22 に関連するパケット数を計測することで実施した。

両期間を通して、常に一定以上の port 23 を使った通信があることがわかる。これら全てがインセキュアな通信とは断定できないが、ユーザ名、パスワードを含む全ての通信内容が平文でネットワークに流れる通信が一定量以上あることを示唆しているといえる。本比較によって、一般的なセキュア通信の利用状況とすることはできないが、このようなアプリケーションが主に管理者および比較的高スキルのネットワーク利用者によって多く利用されることを踏まえると、一般利用者ではさらにこの比率

が大きくなることが予想できる。

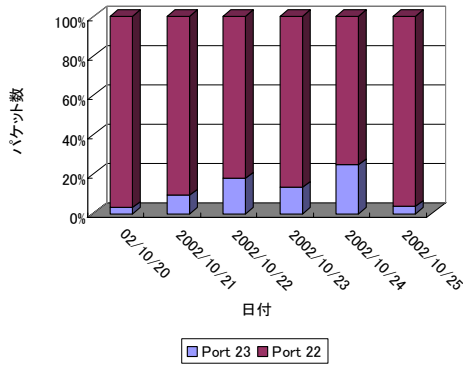


図 3-1 2002 年 10 月下旬の Port 23 (telnet)と Port 22 (SSH)トラフィック量

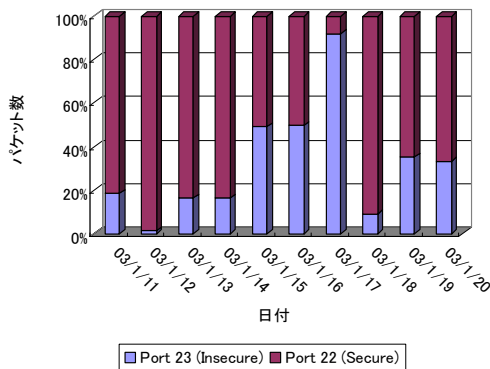


図 3-2 2003 年 1 月中旬の Port 23 (telnet)と Port 22 (SSH)トラフィック量

b) アプリケーション利用主体の一般利用者

一方で、代表的なメール取得プロトコルである POP[2]の利用状況について、同じくセキュアな通信の利用状況を調査する。セキュアな通信は通信路が保護される Secure な POP[3]とした。両期間を通して、保護されていない通信が非常に多くの割合を占めていることがわかる。このことだけで利用者意識を判断することはできないが、広く利用されており、ユーザ名、パスワード、さらにはプライバシー情報も含むメールに関する通信の相当量が平文でネットワークに流れていることを示しており、一般利用者のセキュリティ意識は大きく立ち遅れていることがうかがえる。

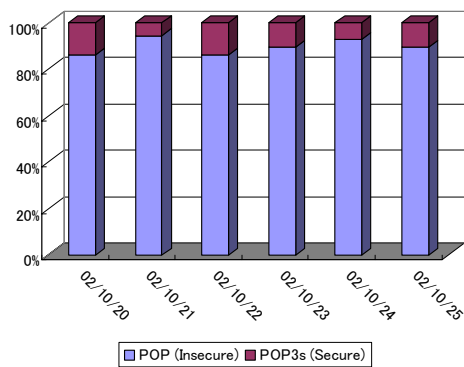


図 3-3 2002 年 10 月下旬 POP 通信トラフィック量比率

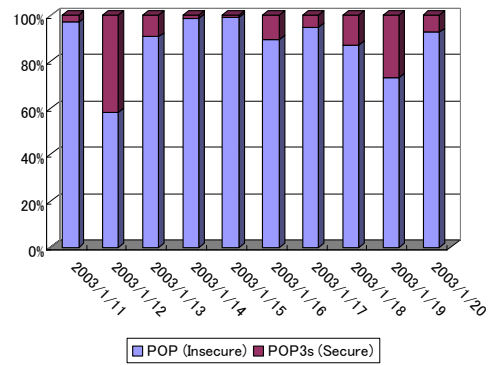


図 3-4 2003 年 1 月中旬の POP 通信トラフィック量比率

c) IPsec の利用状況

さらにインフラとしての通信のセキュリティ状況を検討するために IPsec[4][5]の通信量についても調査した。IPsec は IP レベルにおける通信を保護するための基盤技術として標準化されており、インターネットに基本的なセキュリティをもたらすことが期待されている。

図 3-5に量を示す。グラフは縦軸が対数軸となっており、IPsec による通信は事実上ないも同然であることを示している。観測対象が海外との接続であることを考慮しても、ほとんど普及していないと言っても過言ではない。

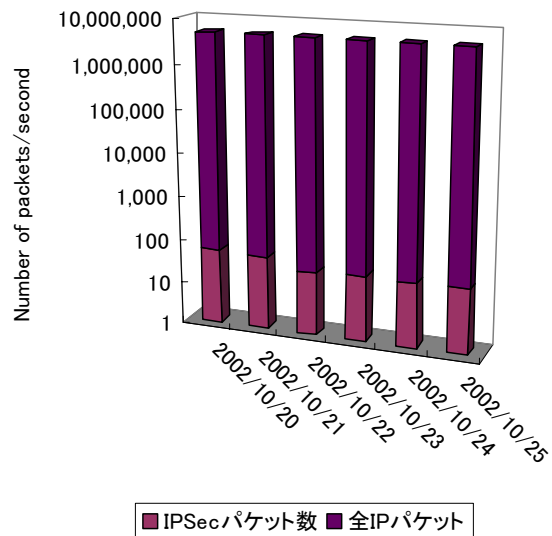


図 3-5 2002 年 10 月下旬の IPsec のトラフィック量比率

(2) より巧妙な DoS 攻撃

目標に壊滅的な打撃を与える DoS は規模が大きくなると得ざるを得ず、攻撃者にとっても検知、追跡のリスクが大きくなる。

しかし、攻撃トラフィックを巧妙に制御することによって、それらのリスクを大幅に抑制しつつ、なおかつ効果のある攻撃が可能になる場合がある。それらは文献[6][7]等によって「DeS(Degradation of Service)攻撃」として存在が指摘されている。

また、分散型 DoS 攻撃である DDoS についても、これまでに知られていた多数の攻略したノードに設置したゾンビ (Zombie) を利用する DDoS 攻撃[8]以外に、通常のノ

一の機能を利用した攻撃も登場しており、攻撃手法がより巧妙になってきている。

ここでは、攻撃トラフィックを巧妙に生成する Pulsing DoS と一般ノードを使った反射型攻撃の例を述べる。

a) Pulsing DoS

通常の DoS 攻撃が大容量のトラフィックを連続的に送信するのに対して、Pulsing DoS では非常に短い時間で比較的少数の packets を断続的に送信する。攻撃トラフィックが従来の DoS と比べかなり少ないため検知・追跡が困難になる。この手法は、TCP の輻輳制御アルゴリズムの影響で、帯域を埋め尽くすことなく通常通信の TCP の性能を引き下げることができる。

図 3-6 に FTP による転送性能に対する Pulsing DoS による影響を示す。図の Normal FTP として示された線は攻撃がない状態における FTP によるファイル転送性能を示している。Pulsing DoS は TCP 通信に対する効果的な攻撃であることがわかる。このことは DoS 攻撃対策としてもより高度な技術が必要となることを示唆している。

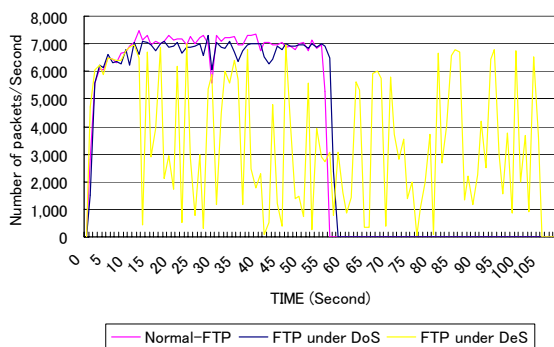


図 3-6 DeS 攻撃のインパクト

b) Distributed Reflection DoS (DRDoS) 攻撃

DRDoS 攻撃は、様々なシステムおよびアプリケーションが生成する応答パケットを利用して DoS トラフィックを生成する反射型の DoS 攻撃である。攻撃者は、Reflector となるノードに向けて Source IP を攻撃目標となるように改竄した何らかの要求パケットを送信し、Reflector にそれに対する応答パケットを目標（改竄された Source IP）に対して送信（返信）させることで成立する[9][10][11]。

また通信プロトコルとしての基本的な機能を利用したものであるため、インターネット上の多くのノードが Reflector になりえる。このことは多くのノードを使った大規模な DDoS トラフィックを容易に生成し得ることを示しており、今後大きな脅威となり得る。

図 3-7 にトラフィックが Reflector によって増幅される様子を示す。グラフは 10 秒間のパケット数の推移を示しており、オリジナルとして示したものが攻撃者 A によって生成された Reflector R への TCP SYN パケットであり、反射として示したものが R によって生成された応答パケットで被攻撃者 V に対して攻撃となる TCP SYN-ACK パケットである。

グラフから明らかなように、Reflector によってほぼ 2 倍の量にパケットが増幅されている。これは TCP が SYN/ACK の再送を試みることによるものである。この

ことから攻撃に使うパケットを効率よく選ぶことで、攻撃者はその能力以上のパケット数を被攻撃者に送ることが可能になる。

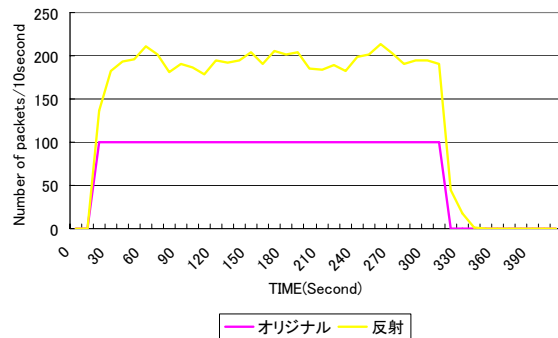


図 3-7 反射攻撃によるパケットの増幅

以上の事実から反射型の分散 DoS は非常に広範囲のノードを Reflector として利用し、攻撃パケットの出所を広く分散可能とするとともに、パケットの増幅も可能な攻撃であり、防御、および攻撃者の特定の双方とも困難な DoS 攻撃であるといえる。

4. インターネット情報集合点に関するセキュリティリスクの調査・分析

本調査・分析はネットワークを介した通信について「End Point Authentication」の考え方をベースとし、認証という視点をキーに通信を分析する。

(1) End Point Authentication

通信を、

- 対面しての直接通信
- 通信システムを経由しての間接通信

に分類し、それぞれの認証モデルを検討する。

a) Face to face communication

対面しての直接通信では、通信者は前節で挙げた情報を直接交換することができるため、原則として情報交換に際してのセキュリティ上の脅威は存在しない。

b) Network communication

それに対して、通信システムを経由しての間接通信では、通信者はいかなる情報も第三者である通信システムを経由することになるため、交換するすべての情報が本人から発せられたかどうか確認できない。このことは、通信者間に存在するものは、原則として一切信頼できないことを意味しており、それが一見安全のように見えていても通信者はそれを期待してはならないことを示している。

(2) 通信モデル

通信システムを経由しての間接通信を利用する際のセキュリティリスク分析の基本モデルを検討する。ここで重要な要素となるのは、通信者が通信路を利用する際に共通に必要なサービス基盤である。通信相手を検索し呼び出すサービスと適切な経路を選択する経路制御サービス等がこれにあたる。このようなサービスは、通信者と通信路の間に入り込み得る信頼できない第三者とな

る上、通信路の利用に不可欠であることから、非常に重大なセキュリティリスクを含んでいるといえる。

a) 情報インフラモデル

現在、情報・通信インフラとして急速に成長しているインターネット技術においては、End-to-end のコンセプトに基づいて、基本技術が原則としてオープンスタンダードとなっており仕様が公開されている。また分散システムとしてのアーキテクチャに基づいていることから、集中的な管理ポイントを持たない。

このことはインターネット技術が低コストで急速に普及する原動力となったものの、同じ仕様のシステムが広く普及することで、一度問題が起こればその影響が広範囲におよぶことにつながるとともに、運用管理の責任が分散することにもつながり、リスク管理を困難にしている。

インターネットのインフラとしてのサービスとしては、

- 認証基盤、宛先検索の LDAP
- 名前解決のための DNS
- 大規模経路制御のための IRR

に注目する。これらはインターネットを利用するためのインフラ情報システムであり、通信に不可欠な要素（図 4-1）であるとともに、信頼できない第三者となり得る重要なサービスである。

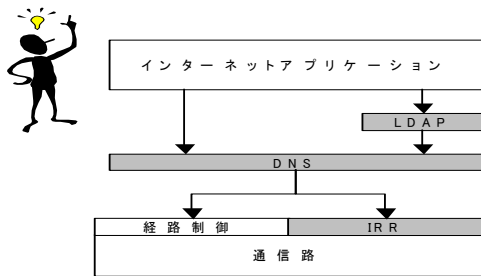


図 4-1 インターネット情報インフラ

特に DNS はあらゆるアプリケーションが利用する基盤サービスであるとともに、全世界にわたって広く連携する分散データベースでもあることから、その重要度は数あるインターネット技術の中でも最も高いものの一つとなる。

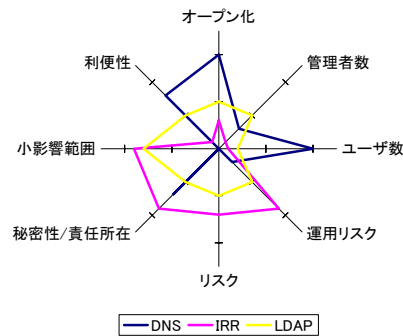
b) インターネット技術の現状

これまでの議論を踏まえ、現状のインターネットの情報インフラにおけるセキュリティを検討する。オープン化、管理体制、利用者数、利便性の観点からその影響を検討する。

- オープン化が進むことによって、急速な普及が可能になったが、単一の技術が広く利用されるようになり、何らかの脆弱性があった場合リスクが高くなる。
- ユーザ数が増大することによって、多くのユーザがサービスの恩恵を受けることが可能になったが、何

らかの問題が発生したときの影響範囲も広がる。

- 管理者の多い管理体制によって、管理コストの集中が避けられるが、責任の所在が曖昧になるとともに管理パスワードなど秘密情報の維持が困難になる。
- 利便性が向上し誰でも使える技術が浸透することによって、多くの利用者がサービスを利用可能になるが、スキルの低下等による運用ミスが増加する。



図からわかることは、インターネット技術は相反する多くの要素から成り立っていることであり、上記のレーダーチャートがバランスよくなることは本質的に不可能なことである。

5. ケーススタディ

本章においては、情報インフラのセキュリティについて、その最も重要な要素である DNS に注目して、その危険性、配備体制、監視体制、およびあるべき体制について検討する。

(1) Events of 21-Oct-2002

2002年10月21日 20:45UTC～22:00UTC に、階層的に構成されている DNS サービス群のルートにあたる DNS サーバー、ルートネームサーバが大規模な DoS 攻撃を受けた[12]。

- 攻撃は複数の攻撃ノードが連携する DDoS 攻撃であり、13 ある DNS サーバーが同時に狙われた。
- 攻撃の規模は一つのルートサーバあたり 50～100Mbps の規模であり、全体的には約 900Mbps におよんだ。
- 攻撃に使われたパケットは、ICMP、TCP SYN、Fragmented TCP および UDP であった。
- 攻撃に使われたパケットのソースアドレスは、ランダムに改竄されていた。

この攻撃の結果、いくつかのルートネームサーバが攻撃期間中不到達となったが、すべてのルートサーバが不到達になるケースはほとんどなかったとされている。

しかし、ルートネームサーバが情報通信基盤であるインターネットの、さらに基盤となる情報インフラであることを考えると、このようなケースにより適切に対応できるようにするために更なる検討が必要であることは明らかである。

a) Root name server の運用状況

現在は 13 ノードが Root DNS Server として運用されている[13]。DNS は、全てのサーバーへの到達性がなくとも機能するように設計されており、これらのサーバーをバランスよく配備、運用することで、全システムがダウンするリスクを避ける必要がある。

b) 攻撃の可能性

問題の攻撃時周辺について、トラフィック状況のうち特徴的な部分を図 5-1 に示す。

データは折れ線で表した部分は観測された全トラフィック量を表しており、期間を通じて一定で特に変化がないことがわかる。しかし、DNS によって利用されるポートである 53 番に注目すると、突出した量となっている。

これは、攻撃が海外とのリンクに影響を与えていたことを示しているとともに、単純なトラフィック量監視では、この現象が検知できないことを示している。

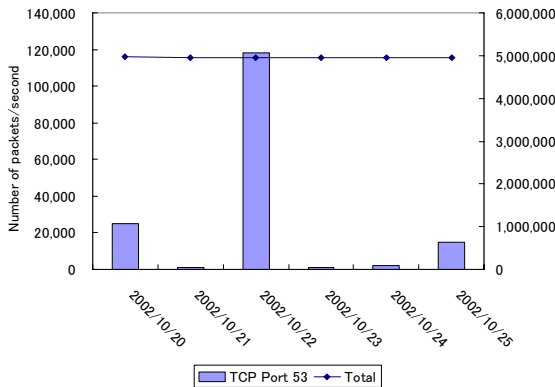


図 5-1 ルートネームサーバ攻撃時のトラフィック状況

さらに 10/22 の 53/TCP の部分だけに注目し、通信しているノード（ソースポートが 53/TCP であるもの）について分析した。結果を図 5-2 に示す。

特定のノードが非常に多くのパケットを生成していることがわかる。これらは攻撃を受けたルートネームサーバからの応答パケットの可能性もあるが、一部のノード間の通信が多数を占めている特徴的なトラフィック特性となっていることから、このような観測も定常的な観測として有効であるといえる。

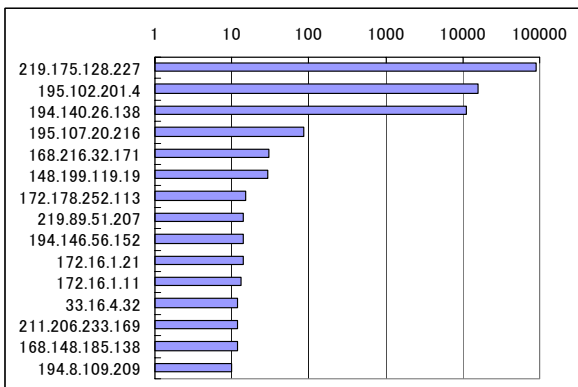


図 5-2 多くのパケットを送出しているノードランク

(2) 地理的配備状況

現在のルートネームサーバの地理的配備状況は CAIDA(Cooperative Association for Internet Data Analysis) における研究による NetGeo - The Internet Geographic Database [14]によると以下の図 5-3 ようになる。



図 5-3 ルートネームサーバの地理的配備状況

基本的に北半球、特に北米に集中していることがわかる。このことは全世界のインターネットを支える重要なインフラが特定に国と地域の安定に大きく依存していることを示している。

DNS は、すべてのルートネームサーバに対する到達性がなくとも機能するように設計されているが、地理的に偏った構成は、災害等による物理的なインシデント時への備えの点で問題がある。インシデント時はその配下の名前空間すべてのネームサービスが利用不可能になり、アプリケーションからみると事実上その名前をもつノードへの通信が不到達になる。

(3) トポロジ的配備状況

地理的な配備状況だけではなく、ネットワーク的な論理構成についても検討する。本分析は、情報処理振興事業協会：平成 9 年度独創的先進的情報技術に係わる研究開発テーマの公募において研究開発された「インターネットオリエンテーリング可能な地図構成法に関する研究」の成果物を用いたネットワーク地図を活用する。

ネットワーク地図は、IRR の情報に基づいて生成されるものである。現在の IRR 情報は非常に多くサーバーが独自に保持しており、情報全体へのアクセスが困難な状況となっている。現在の IRR サーバのリストは文献[15]から得られる。本ネットワーク地図の情報は最も多くの IRR 情報が集約されている <http://www.radb.net/> から得られる情報に基づいている。

図 5-4 に IRR に登録されている AS のルートネームサーバのある AS からのホップ数のヒストグラムを示す。例えば多くの AS が AS5459 から 2 またはホップの距離にあることを表しており、AS5459 にあるルートネームサーバ k.root-servers.org は広範囲にわたる到達性が見込めることを意味している。

各ルートネームサーバのある AS ごとに異なった特性を示しており、AS2149 では比較的 AS 距離が遠くなりがちであることがわかる。

これらの分析から、現在のルートネームサーバの配置はネットワークトポロジ的にも偏っている傾向があることがわかる。理想的には小さなホップ数で多くがつながることが望ましい。

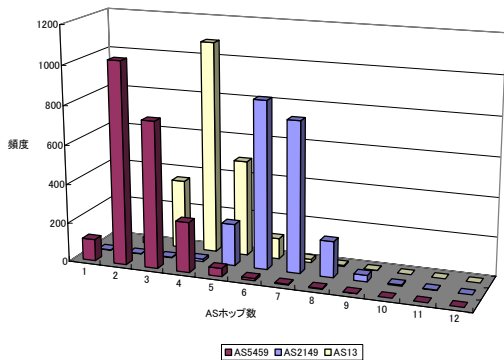


図 5-4 主なルートサーバからの AS ホップ数

図 5-5には、AS2500 からみた世界の AS 地図を示している。図のハイライトした部分はルートネームサーバのある AS を表している。4つしかないのは、AS2500 からみえる IRR に登録されている AS のみしか表示されていないためである。

図 5-6には AS5459 からみた世界の AS への到達性を表している。図中の異なる色で表している○が、ルートネームサーバが所属している AS であり、IRR に登録されている情報から分析する限りは、ルートネームサーバ毎に世界への到達性が大きく異なることがわかる。

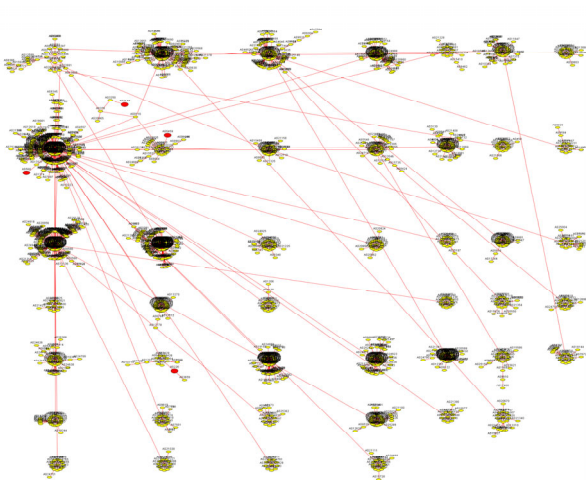


図 5-5 AS2500 からみた世界の AS 地図

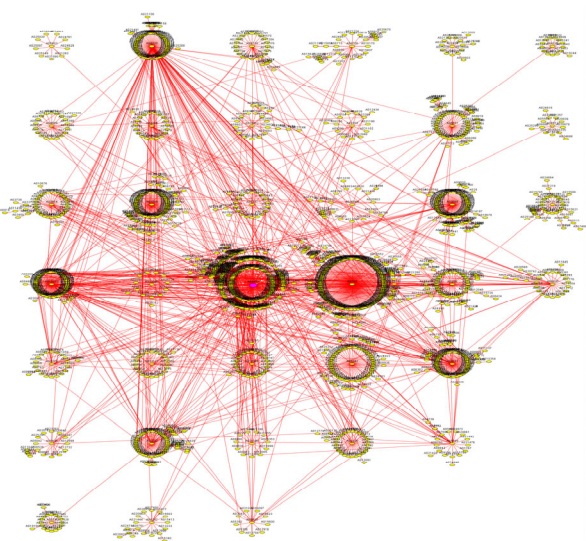


図 5-6 AS5459 からみた世界の AS

(4) Root DNS Service の監視体制

いくつかのルートネームサーバでは、監視情報を公開している。

- Root DNS Server 中で D, E, F, H, K, M では何らかの形で運用情報が公開されている。
- D と F については、Paul Vixie らによる 2002 年 10 月 21 日に発生した大規模な Root DNS への攻撃についての資料が公開されている。
- E, F, K, M では、トラフィックの統計情報が公開されている。
- K, M では、継続的にトラフィック統計情報を公開している。
- K では DNS の Query 毎の統計情報を公開している。

しかし、これまでに考察してきたようなトラフィック分析、地理的位置関係、トポロジ的位置関係、およびインシデントを関連付けるような情報は少なくとも公開されていない。

(5) ケーススタディのまとめ

定常的な適切な監視体制

問題を早期に発見し、その後の対策に利用するために定常的な監視体制が重要である。現在の監視体制は必要最小限のものであり、公共のインフラとして、さらに十分な監視体制が必要である。

バランスのよい配備戦略

インシデント発生時にもその影響を可能な限り局所化するために地理的、トポロジ的に検討された配置が必要である。現状ではそれらが考慮されておらず、自然災害、地域紛争、大規模なサイバーテロ等に対して十分分散されているかどうか検証も困難である。

追跡技術

ソースアドレスを改竄された攻撃にも対応できるようにするために追跡技術が必要である。攻撃を根絶するために、攻撃者を特定する技術が重要である。連携のための通信を行い、広く情報共有する必要がある。

6. 提言

インターネットの設計思想は、分散型の管理である。このことが、脅威に対して特に脆弱性を勘案すべき点である。そこで、安全性の確保には、運用機関が安全性に関する一定の技術的要件、組織的要件を満足しており、それらの機関が的確なルールによって連携する必要がある。

(1) ネットワーク運用機関の連携における公的機関

a) 公的機関の必要性

ネットワークを運用する機関では、例えば DNS の設定などの情報インフラに対する一定の制御機能をつかさどる場合は、実施する組織・機関において、満たすべき要件を定める必要がある。その要件とは、運用ポリシーの表明、運用規範の徹底、安全性に関する規範の徹底、運用担当者の技能確保と教育の充実などがあげられる。そのような機関は、これらの項目に照らして、基準を満たしていることに関する認定を受ける必要がある。ネットワークの運用に携わる機関は、そのような認定証を保持してい

るという前提のもとで、何らかの公的機関の承認のもとで、ネットワークの運営に参画することになる。

b) 公的機関の役割

現状のネットワーク運用の状況を把握し、関係機関で共通の認識とするために、「運用マップ」の作成が必要である。運用マップは、「運用組織」「接続関係」「帯域」「ルーティングプロトコルの種別」「ルーティングに関する制御関係」「DNSによる名前解決の関係」等の情報インフラとしての「公共の情報」が記述される。このマップは、本報告書で問題としているネットワーク安全性への脅威に重要な意味を持つ情報であるため、何らかの公的機関が一元管理する必要がある。

c) インシデント時における連携の必要性

ネットワーク運用機関の連携、セキュリティ情報の共有、情報交換の必要性を端的にしめす文献として、カーネギーメロン大学ソフトウェア工学研究所の論文[16]では、DoS攻撃の対象ISPの対処方を簡便にまとめている。また文献[17]でもDDoSに対するISP間の連携が必要であることが議論されている。また、情報共有を推進するためには、組織的なもの、技術的なものを含めた情報共有のためのプロトコルの標準化が重要となる。

d) RFC3013

これまでの議論により、ネットワーク環境の安全性を高めるためには、標準化すべき課題が多く存在することが理解される。しかしながら、現段階ではISPが実施すべき要件に関しての標準化が十分達成されていない。この問題はRFC3013で取り扱われているが、この文書は、Best Current Practice（現段階における最善の実装）カテゴリのRFCに過ぎず、標準ではない。このため、現行のISPは厳密な意味で安全であるとはいえない。そこで、以下では、RFC3013の内容に関する問題点を指摘する。

本書は、ISP間の通信回線を安全に保つという観点から十分な注意が喚起されていないと考える。本書では、インシデント発生時における「安全な回線の確保」が重要であることを主張するとどまっている。しかし、注意を喚起すべきはインシデント時だけではなく、「ISPが取り扱う、インターネットのインフラを維持するために利用されるすべての回線」に対して安全性の確保された通信を実施することを強く提言する。

さらに、「安全性の確保された通信回線」という用語の厳密な規定が必要であろう。文書ではこの点についての言及がされていない。「安全な回線」とは、①通信の当事者間で疑う余地無く双方が認証されていること、②通信に際して情報の完全性(integrity)が保証されていること、③必要に応じて秘匿性(privacy)が保証されていること、が必要である。

1. RFC3013の7ページ、セクション4.2では、誤ったルーティング情報によりネットワークに「ブラックホール(パケットを吸い込んで他に転送しない地点)」や「ハイジャック(回線ののっとり)」を作る可能性を指摘している。本書では、この問題に対処するための方策としてBGPルーティング情報の取り扱いに関して安全性が確保されていれば良いとする内容が述べられているが、これは誤った認識をISPに与える可能性があることを指摘したい。すな

わち、ISP間の通信で利用される「すべてのルーティング情報」について安全性が確保されることがMUSTであるべきである。

2. RFC3013の9ページ、セクション5では、電子メールアプリケーションに関して言及されている。しかし、DNS、LDAP、WEB、NTP等のアプリケーションの運用に関する安全性に関しては、言及されていない。これらのアプリケーションはインターネット自身とその利用者に直接影響を与える。すなわち、これらに関連する情報が改竄されて攻撃された場合にネットワークに対して悲惨な影響を与えかねない。
 3. 本書は、利用者のログを保持することの重要性を見落としていると考えられる。悪意のある利用者は、ダイヤルアップ回線を利用して侵入することが想定される。このような行為の捜査を行うためには、ログ情報が不可欠である。
 4. 攻撃に対する捜査を行うためには、異なるISPに所属する担当者間によるネットワーク上または直接の連絡網の充実が不可欠である。本書では、このような機構を導入することの重要性に関して十分言及されていない。この重要性を語る例をあげれば、ウイルスが投入されたような場合やネットワークへの攻撃がなされた場合に、その源を特定することである。
 5. ISPは、IDSを装備することが、強く求められていると考えられる。
- #### e) 情報インフラの防護と広域配備戦略

情報インフラを防護するためには、それらのセキュリティメカニズムを十分に活用することと同時に、広域サービスとして全世界的なサーバー配置等を考慮することが重要である。提言としては、ネットワーク地図を構成する技術に基づいて、ネットワーク運用サービスおよびサーバーを配備することである。その際、地理的条件、地政学的条件、ネットワークトポロジ、トラフィック量、などの条件を十分考慮しなければならない。このような施策を実施する主体とそれによる早急な対応が求められる。

(2) 今後必要な研究開発

a) 監視・計測技術の研究開発

大容量の通信を効率よく監視するための情報収集技術、広域なネットワークを効率よく監視するための技術、高速ネットワークを監視するための技術、さらには不正アクセスを監視できる技術が必要である。例えば、文献[18]では、Pulsing DoS等の巧妙なDoS攻撃への対応として、高精度な監視の必要性を指摘している。トポロジの監視や最適化への自動対応等多くの情報から必要な情報を効率よく監視する技術が必要である。

b) 追跡手法の確立

現在不正アクセスの追跡技術は大きな注目を集めており、標準化の場でも議論されている。標準化が議論されている二つの方式itrace、ipptが特に注目を集めているが、これらは現在実用化に近づいているものも多い。これらの技術には国内でも多くの取り組みがあり、世界的に見ても先進的である。広域ネットワークにおける実証実験等で実用化のための試験を行える段階といえる。

c) 障害シナリオの蓄積および分析サービスの充実

本節では、カーネギーメロン大学の文献を参考に、攻撃パターンを形式的に記述する有効な方法の概要と関連する研究・開発の可能性を述べる。文献では、1~4の攻撃のシナリオについて攻撃木を用いたモデル化がされている。このように、木構造をより詳細に分析することで、攻撃のシナリオを記述することになる。脅威への対処は、このような木構造のデータベースを元に、脅威の場合分けを網羅することが必要となる。

7. まとめ

情報インフラの防護に関しては、技術面、運用面ともに十分であるとはいえない状況である。特に運用面におけるセキュリティ意識および組織的対応には不備が多く早急に対策をとる必要があると考えられる。特に既存のセキュリティ技術は有効に活用されているとは言えず、情報インフラに関するセキュリティ技術の普及が急務となっている。「システム中の最も弱い部分がシステム全体の強度を決める」という観点から考えると、全世界の公共サービスの一環である情報インフラ全体のセキュリティ強度を高めるためには、全世界規模の協調と対策が必須となる。

現在の課題は、セキュリティ意識の浸透と技術の普及である。本調査報告でも報告した通り、多くの有用なセキュリティ技術もその実装の脆弱性により無効化されることも多く、さらに大きな問題は利用者の意識の低さによって技術自体が利用されないケースが多々あることである。さらには確立した技術が使いやすいものであるかどうか、利用者のスキルが十分なものであるかどうかも大きな要素となる。

運用面の問題を解決するためには、運用組織のあり方も重要な問題となる。重要な情報インフラを扱う組織は、一定の水準のセキュリティ要件を満たし、高い意識を維

持することが必要となることから、常に監査をうけるような体制が必要といえる。

しかしそのような体制の形態には新しい概念も必要であるといえる、インターネットに代表される今日の情報ネットワークは、分散的な環境でそれぞれの部分が独自に運用されることから、従来の国家を中心とした中央集権的な組織はなじまないと考えられる。運用のための組織は官民を問わず、一定の水準を保証するような基準を設け、それらを満たす組織とすることが適切と思われる。

また、そのような分散的な組織が協調するために大きな課題となるのは情報共有である。変化しつづけるネットワークおよびセキュリティ技術に関する情報を一箇所ですべて管理するような組織構成は現実的ではない。上述したような運用組織が連携し、広く情報共有ができるような体制が必要である。情報共有と協調的セキュリティ対策についてはその必要性がクローズアップされたばかりであり、今後、さらなる施策が求められる。

インターネット技術には、その根幹に「End-to-Endの哲学」があり、それが現在の普及につながっている。本調査においても述べた通り、それはセキュリティの面では間に存在する全ての要素を信頼してはならないことを意味している。本調査において対象とした情報インフラを構成する技術についても同様である。異なる点は、他の多くの技術やアプリケーションがこれらの情報インフラを暗黙のうちに信頼している点である。現在標準化されている技術の早急な普及および運用組織の整備は、急務である。

8. 参加企業及び機関

- 宮城県立宮城大学
- 株式会社サイバー・ソリューションズ

9. 参考文献

- 1 Kenjiro Cho, Koushirou Mitsuya and Akira Kato. "Traffic Data Repository at the WIDE Project", USENIX 2000 FREENIX Track, San Diego, CA, June 2000.
- 2 J. Myers, M. Rose. "Post Office Protocol - Version 3", RFC1725, November, 1994
- 3 C. Newman, "Using TLS with IMAP, POP3 and ACAP.", RFC1730, December 1994
- 4 S. Kent, R. Atkinson., "Security Architecture for the Internet Protocol.", RFC2401, November 1998.
- 5 マスタリング IPsec, 馬場 達也, オライリー・ジャパン, Oct. 2001
- 6 Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial", IEEE Communication Magazine, October, 2002
- 7 Stefan Savage et.al at, "Estimating Global Denial-of-Service Activity" NANOG22, May 20-22, 2001 Scottsdale, AZ
- 8 Comp. Emergency Response Team, "Result of the Distributed-Systems Intruder Tools Workshop," http://www.cer.org/reports/dsit_workshop-final.html, Nov.1999.
- 9 Steve Gibson, "DRDoS", <http://grc.com/dos/drdoS.htm>
- 10 Vern Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", Computer Communication Review 31(3), July 2001
- 11 Rodney Denno "A Next-Generation DoS Attack: Distributed Reflection", <http://www.scmagazine.com/scmagazine/sc-online/2002/article/36/article.html>
- 12 Paul Vixie, Gerry Sneeringer, and Mark Schleifer, "Events of 21-Oct-2002", ISC/UMD/Cogent, OCTOBER21.TXT, November 24, 2002
- 13 Root Server Technical Operations Assn, <http://www.root-servers.org/>, February, 2003
- 14 David Moore, Ram Periakaruppan, Jim Donohoe, Kelly Claffy, "Where in the World is netgeo.caida.org?", http://www.caida.org/outreach/papers/2000/inet_netgeo/inet_netgeo.html
- 15 List of Routing Registries, <http://www.irr.net/docs/list.html>
- 16 Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Howard F. Lipson, Ph. D. CERT Coordination Center, November 2002, SPECIAL REPORT CMU/SEI-2002-SR-009
- 17 Comp. Emergency Response Team, "Result of the Distributed-Systems Intruder Tools Workshop," http://www.cer.org/reports/dsit_workshop-final.html, Nov.1999.
- 18 Glenn Mansfield, Sandeep Karakala, Takeo Saitoh, Norio Shiratori "High Resolution Traffic Measurement", PAM2001, Workshop on Passive And Active Measurements, Amsterdam, Netherlands, 22-24 April 2001.