別紙 3

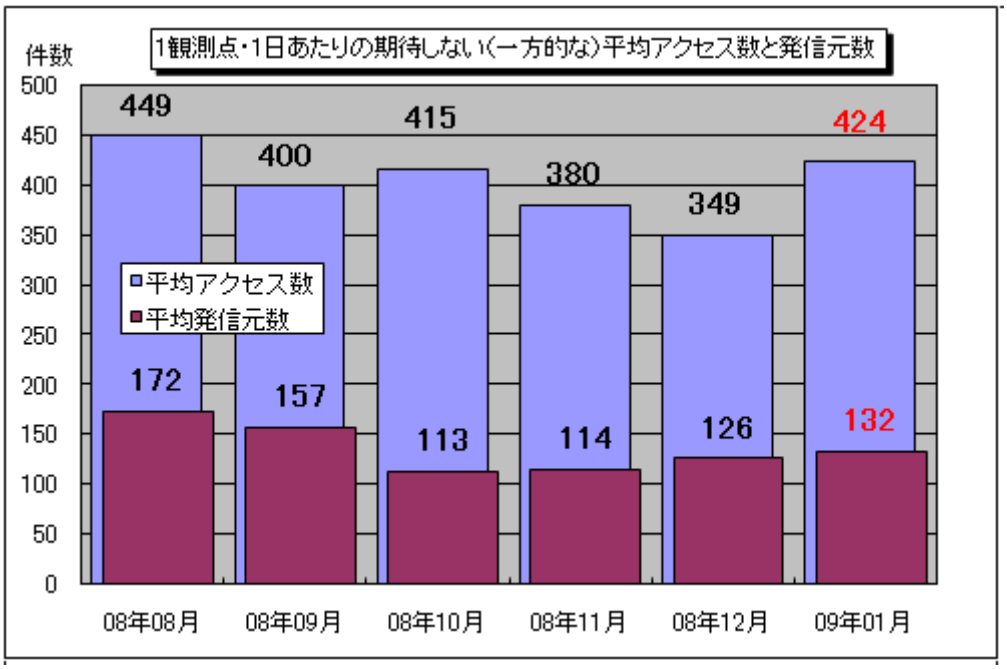
インターネット定点観測(TALOT2)での観測状況について

1．一般のインターネット利用者の皆さんへ

インターネット定点観測(TALOT2)によると、2009 年 1 月の期待しない(一方的な)アクセスの総数は 10 観測点で 131,296 件、総発信元(※)は 41,171 箇所ありました。平均すると、1 観測点につき 1 日あたり 132 の発信元から 424 件のアクセスがあったことになります(図 1-1 参照)。

総発信元(※)：TALOT2 にアクセスしてきた発信元の総数。同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合でも、発信元数は 1 としてカウント。

TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。



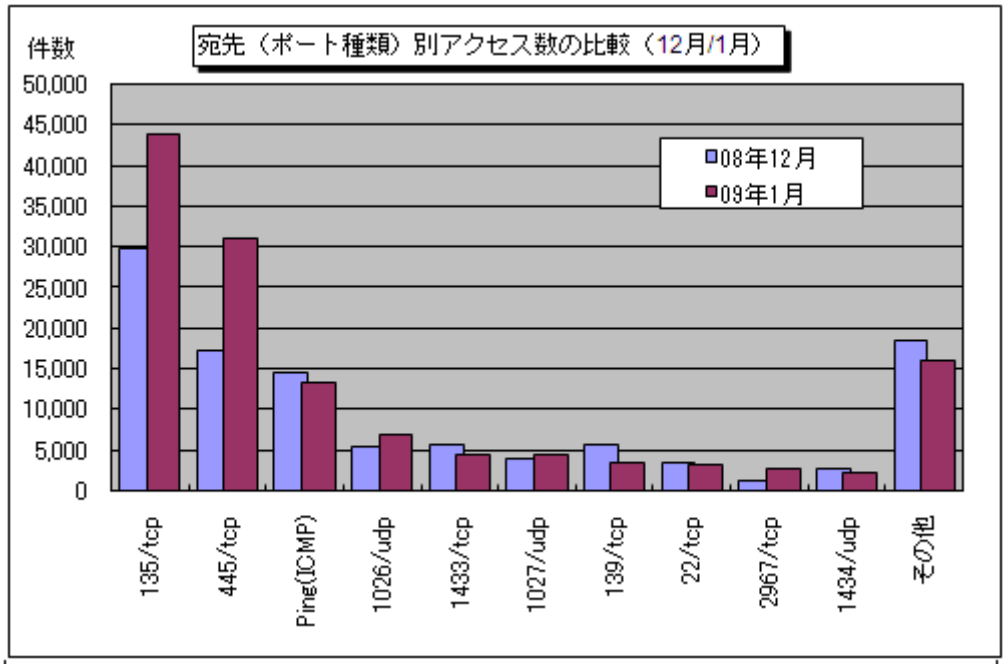
【図 1-1　1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 8 月～2009 年 1 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 1-1 に示します。1 月の期待しない(一方的な)アクセスは 12 月と比べて増加しました。

2008 年 12 月と 2009 年 1 月の宛先(ポート種類)別アクセス数の比較を図 1-2 に示します。

12 月よりアクセス数が大幅に増加したのは、445/tcp、135/tcp でした。これらのポートは Windows の脆弱性(ぜいじゃくせい)を狙った攻撃を行う際に狙われる可能性が高いポートです。445/tcp へのアクセスの増加については、以降で説明します。

なお、135/tcp へのアクセスの増加については詳細の原因は不明ですが、今後も引き続き注意が必要です。



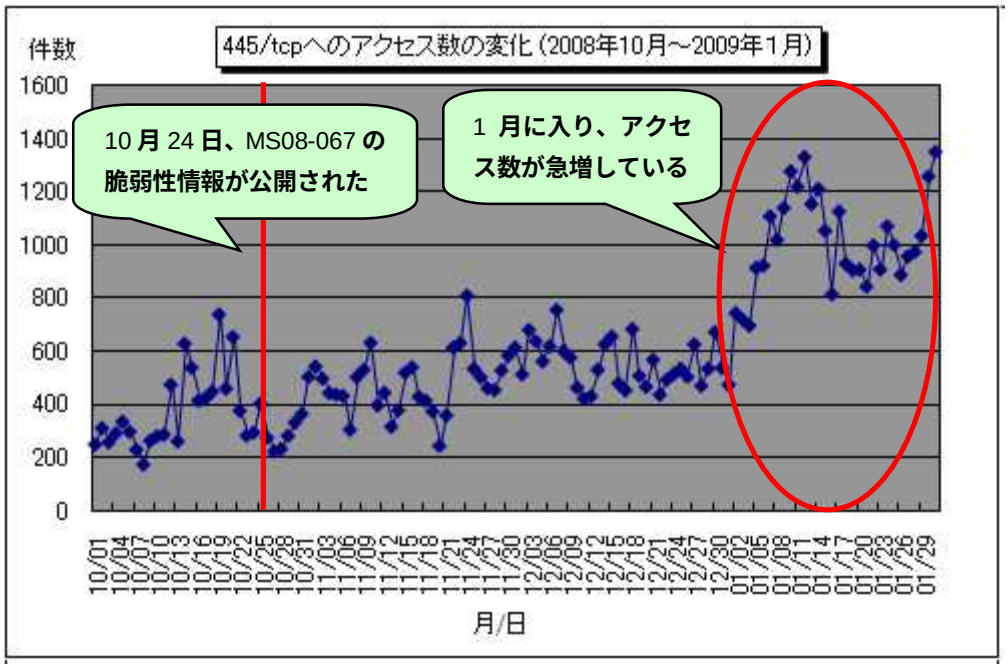
【図 1-2　宛先（ポート種類）別アクセス数の比較（12 月/1 月）】

2.　2009 年 1 月の特異なアクセス

(1) 445/tcp へのアクセス

2008 年 10 月～2009 年 1 月までの 445/tcp へのアクセス数の変化について図 2-1 に示します。

2008 年 12 月の報告で、445/tcp へのアクセスの増加について取り上げましたが、2009 年 1 月に入り、さらにその傾向が顕著になっています。



【図 2-1　445/tcp アクセス数の変化（10 観測点の合計）】

これは、2008 年 10 月 24 日(日本時間)にマイクロソフトから緊急に発表された、Windows の脆弱性（ぜいじゃくせい）MS08-067 を狙ったアクセスであった可能性があります。マイクロソフトによると、この情報が公開される 2 週間ほど前から、この脆弱性を突いた攻撃が確認されていたとのことです。Windows 系のサーバや、一般の方がお使いの Windows パソコンが狙われていたということです。

この脆弱性は、特別な細工がされたパケット(通信データ)が、攻撃対象のパソコンに送りつけられた場合に、Windows でファイルやプリンタの共有などを行うために利用されるサービス(Server サービス)において、意図せずに任意の命令が実行されてしまう可能性がある、というものです。

(ご参考)
「マイクロソフトセキュリティ情報 MS08-067 - 緊急」
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx
「Windows の Server サービスの脆弱性(MS08-067)について」(IPA)
http://www.ipa.go.jp/security/ciadr/vul/20081024-ms08-067.html

この脆弱性を悪用した攻撃を行うウイルスの一つに、Downadup と呼ばれる種類のウイルスが確認されています。このウイルスは 2008 年 11 月下旬に発見され、12 月末にはその亜種である Downadup.B が発見されています。このウイルスは、脆弱性が解消されていないパソコンにネットワーク経由で感染したのち、そのパソコンを起点に、さらに多くのパソコンへ感染活動を試みます。このため、多数のパソコンが接続されている LAN の中で 1 台でもウイルス感染すると、その組織(企業、学校など)の LAN の中で感染が拡大する恐れがあります。

なお、亜種である Downadup.B の特徴として、USB メモリなど外部記憶媒体への感染機能が新たに追加されたことが挙げられます。1 月に入り 445/tcp へのアクセスが急増したのは、自宅などで Downadup.B ウイルスに感染してしまった USB メモリを組織の LAN 内のパソコンで利用した結果、組織内のパソコンがウイルス感染し、組織の LAN の中で感染が拡大したことが原因ではないかと考えられます。ウイルスの亜種発生をきっかけとしてウイルス感染パソコンが増加し、それに伴い他のパソコンを攻撃するアクセス総数も増加したのではないか、ということです。

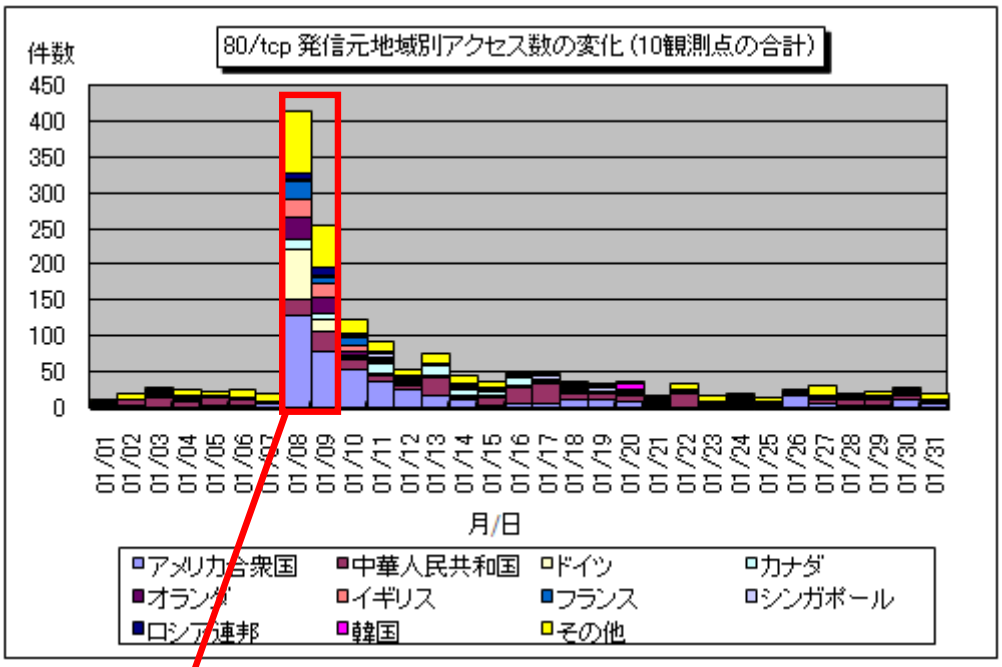
被害に遭わないための基本的な対策は、この脆弱性を解消しておくことですので、お使いのパソコンにこの脆弱性が解消されているか、今一度確認してください。解消されていない場合は直ちにセキュリティパッチを適用して、脆弱性を解消してください。

(ご参考)
「Microsoft Update と Windows Update の利用の手順」(マイクロソフト社)
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx

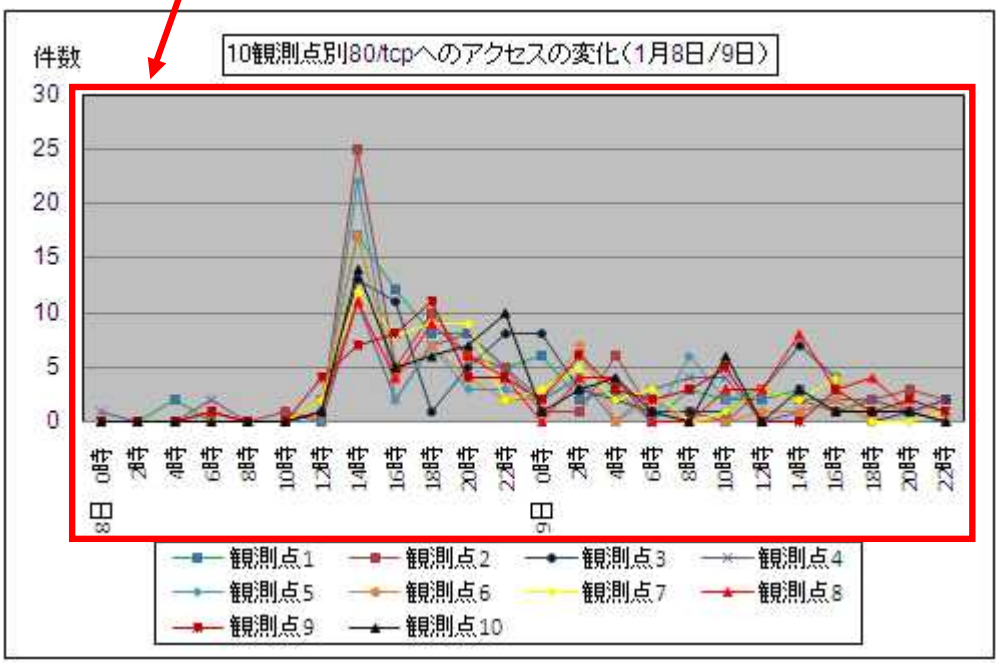
(2) 80/tcp へのアクセス

80/tcp へのアクセスは、1 月の宛先(ポート種類)別アクセス数の TOP10 には入っていませんが、短期間で急増していた期間がありました(1/8 より前の 1 週間の平均 22 件/日→ピーク 414 件/日)。1 月 8 日に 80/tcp へのアクセスが急増した後、数日で減少しました(図 2-2 参照)。

この現象は TALOT2 の 10 観測点すべてにほぼ同時期に発生しており(図 2-3 参照)、定点観測を行っている他の組織でも同様の事象が観測されていることから、かなり広範囲に同時に発生していたことが予想されます。



【図 2-2　80/tcp 発信元地域別アクセス数の変化(10 観測点の合計)】



【図 2-3　10 観測点別 80/tcp へのアクセス数の変化(1 月 8 日/9 日)】

また、IPA にあるもう一つの定点観測システムである MUSTAN(※)においても、同様のアクセスが観測されており、アクセスのログに以下の文字列が含まれていることが確認されています。

/nonexistenshit
/mail/bin/msgimport
/bin/msgimport
/rc/bin/msgimport
/roundcube/bin/msgimport
/webmail/bin/msgimport

上記にある「msgimport」というファイルは「Roundcube Webmail」と呼ばれるウェブメールソフトに関係するものと思われます。2008 年 12 月中旬にこのソフトのセキュリティパッチがリリースされているため、この脆弱性が解消されていないサーバを探索していた可能性があります。

(ご参考)

「RoundCube Webmail」の脆弱性情報（SOURCEFORGE.NET）
http://sourceforge.net/forum/forum.php?forum_id=898542
「RoundCube Webmail」のリリース情報（SOURCEFORGE.NET）
http://sourceforge.net/forum/forum.php?forum_id=902703

「Roundcube Webmail」のようなメールシステムに侵入された場合、プライバシーが侵害されたり機密情報が漏れたりするなどの被害が発生する可能性があります。「Roundcube Webmail」を利用しているシステム管理者は、上記のサイトを参考にして、最新の安定版バージョンにアップグレードしてください。

脆弱性が公開されると、短期間でその脆弱性に関連したアクセスが増加することがあります。日頃から JVN などの脆弱性対策情報ポータルサイトを確認して、お使いのソフトの脆弱性対策を迅速に行えるようにしてください。

MUSTAN(※)：MUSTAN(MUlti Sensor Traffic ANalysis)とは、複数の観測点に配置されたセンサによってインターネット上を流れるトラフィックを観測・分析し、攻撃的なトラフィックに関する情報を提供しているシステムのことです。

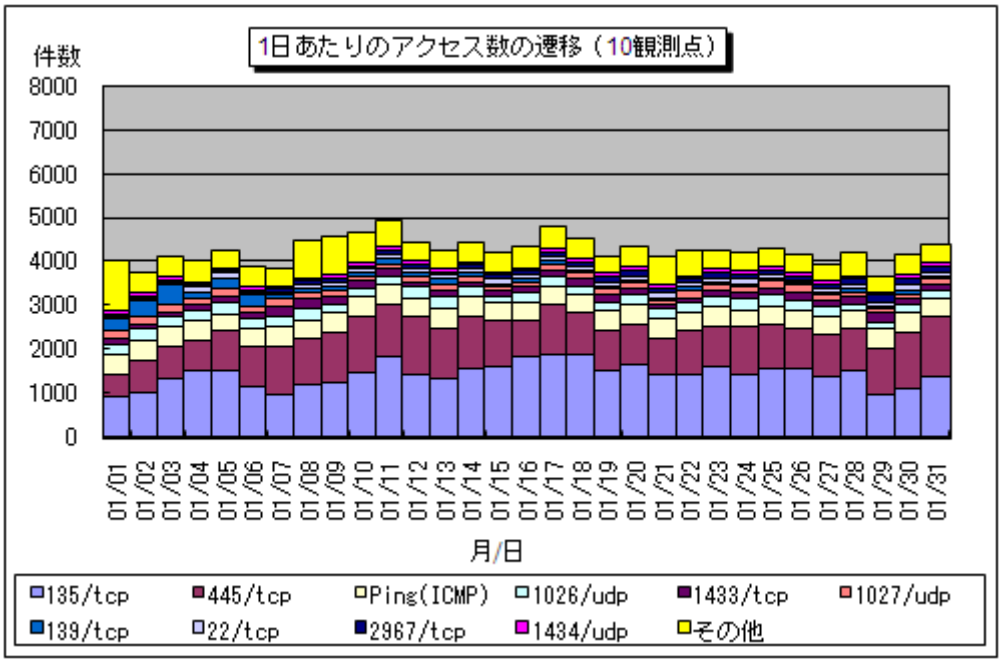
(ご参考)

「MUSTAN インターネットレポート」
http://mustan.ipa.go.jp/mustan_web/
「JVN (Japan Vulnerability Notes)」（脆弱性対策情報ポータルサイト）
http://jvn.jp/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

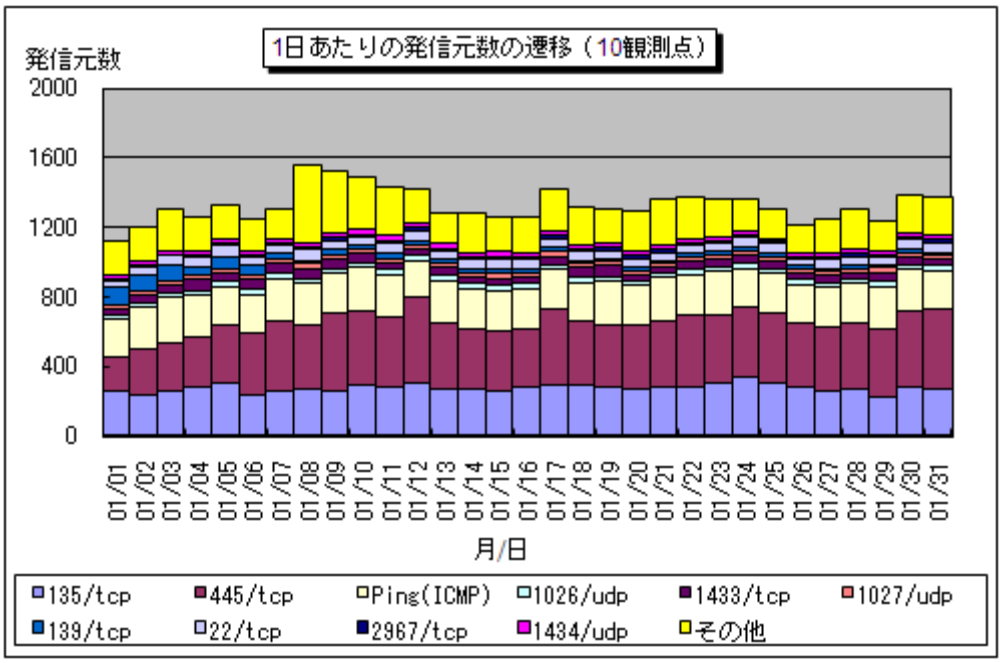
3. 2009 年 1 月の一方的なアクセス状況

(1) 宛先(ポート種類)別のアクセス状況

2009 年 1 月の一方的なアクセス状況(アクセス数)の遷移を図 3-1 に、一方的なアクセス状況(発信元数)の遷移を図 3-2 に示します。



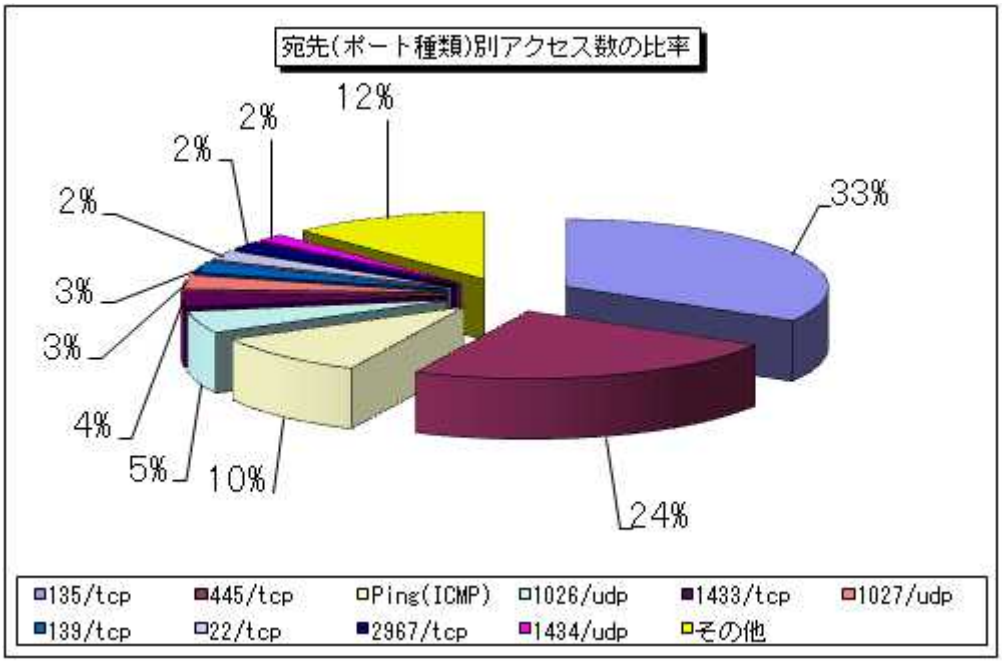
【図 3-1　2009 年 1 月の 1 日あたりのアクセス数の遷移】



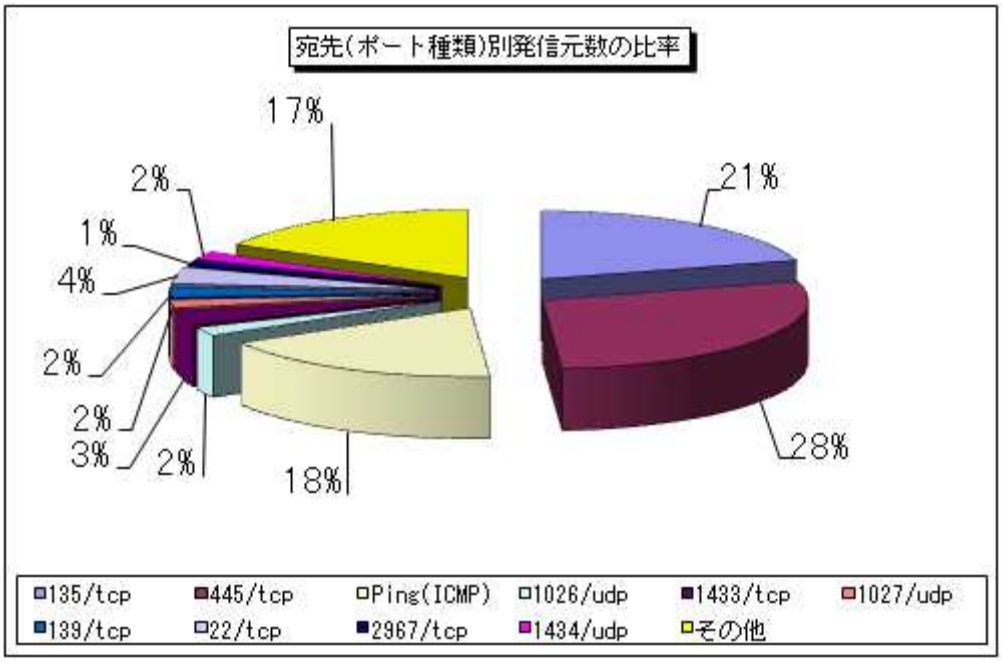
【図 3-2　2009 年 1 月の 1 日あたりの発信元数の遷移】

(2)宛先(ポート種類)別の比率

2009 年 1 月の一方的なアクセスの宛先(ポート種類)別アクセス数の比率を図 3-3 に、宛先(ポート種類)別発信元数の比率を図 3-4 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



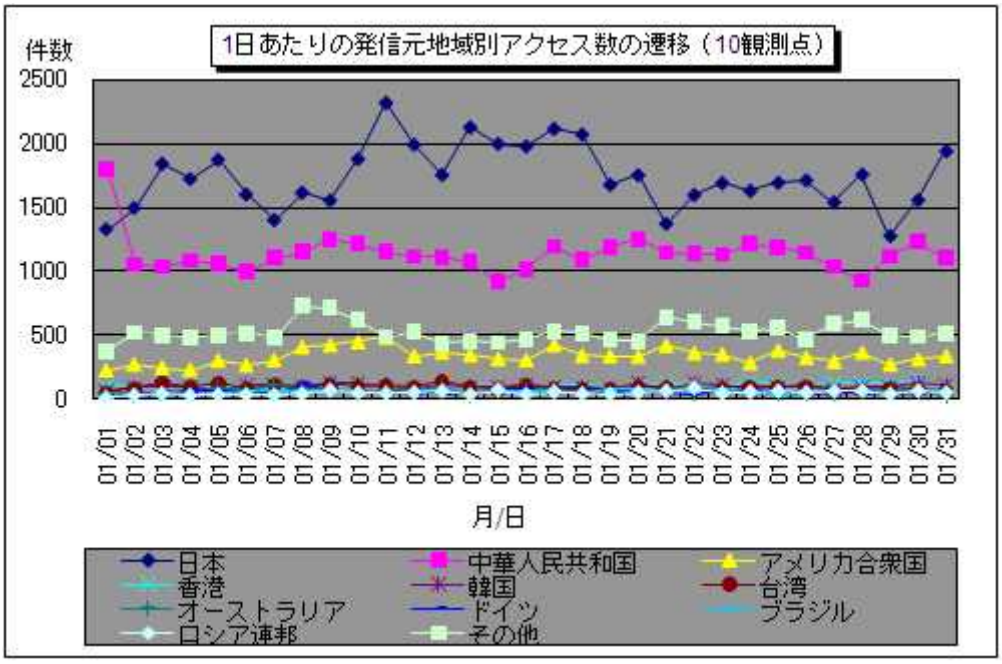
【図 3-3　2009 年 1 月の宛先(ポート種類)別アクセス数の比率】



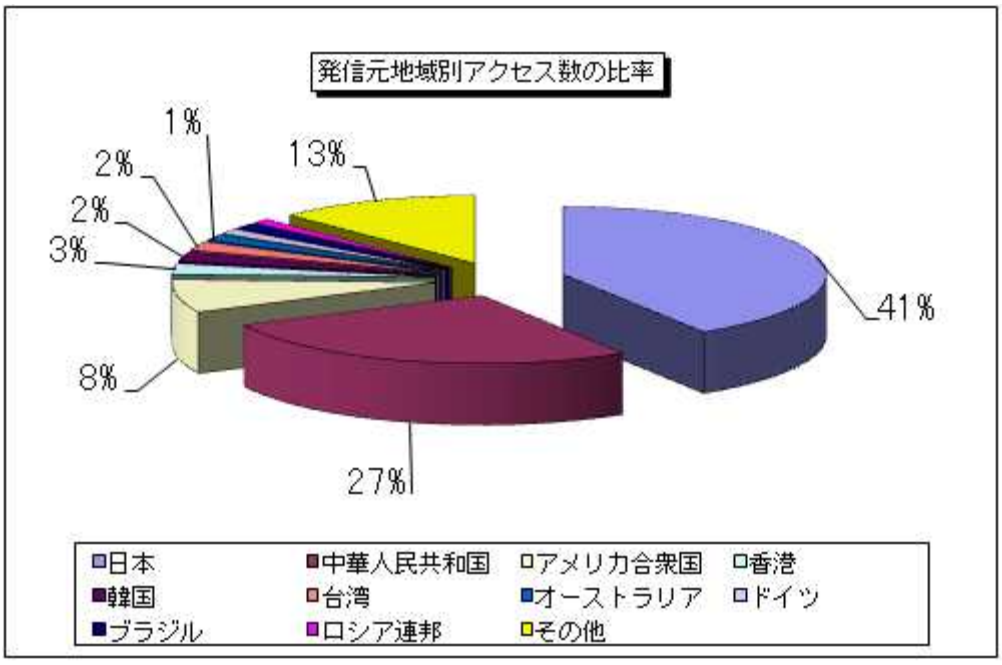
【図 3-4　2009 年 1 月の宛先(ポート種類)別発信元数の比率】

(3)発信元地域別のアクセス状況

2009 年 1 月の一方的なアクセスの発信元地域別アクセス数の変化を図 3-5 に、発信元地域別アクセス数の比率を図 3-6 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。

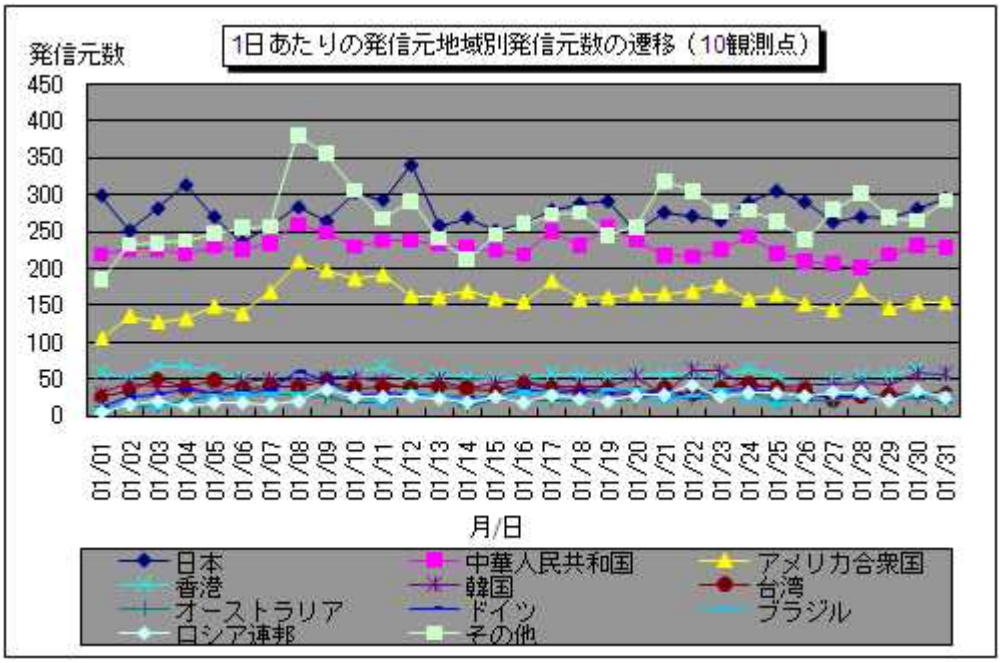


【図 3-5　2009 年 1 月の 1 日あたりの発信元地域別アクセス数の遷移】

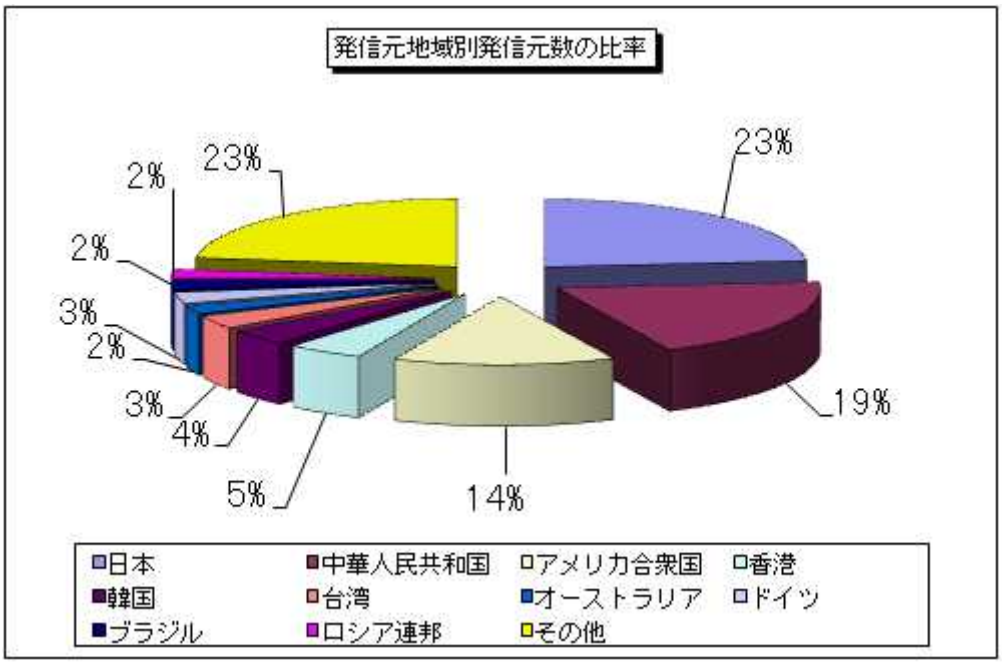


【図 3-6　2009 年 1 月の発信元地域別アクセス数の比率】

2009 年 1 月の一方的なアクセスの発信元地域別発信元数の変化を図 3-7 に、発信元地域別発信元数の比率を図 3-8 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



【図 3-7　2009 年 1 月の 1 日あたりの発信元地域別発信元数の遷移】

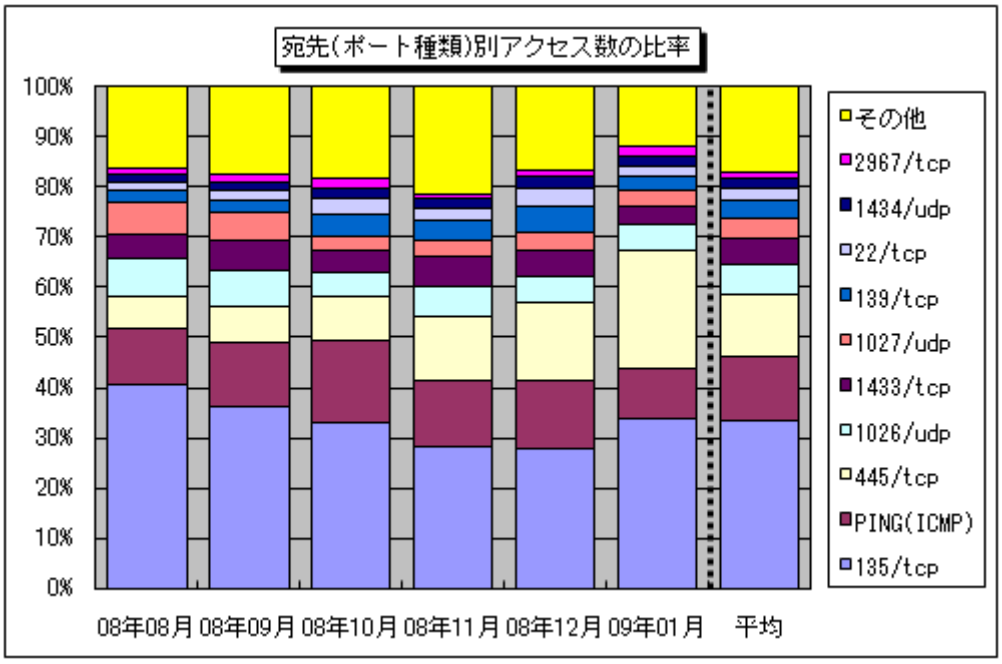


【図 3-8　2009 年 1 月の発信元地域別発信元数の比率】

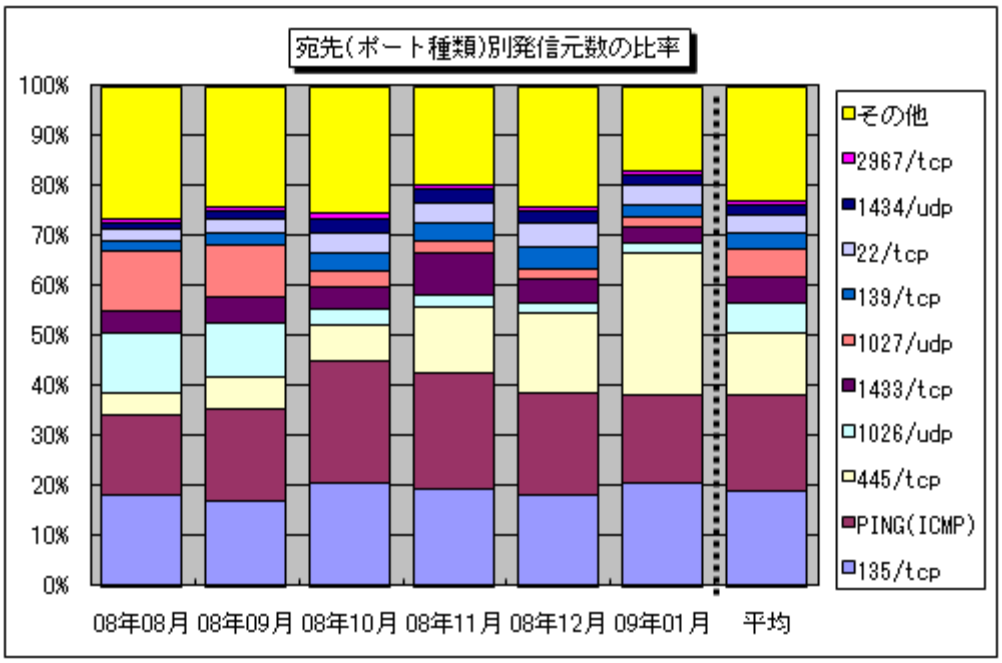
4．統計情報

(1)宛先(ポート種類)別の比率

2008 年 8 月～2009 年 1 月の宛先(ポート種類)別アクセス数の比率を図 4-1 に、宛先(ポート種類)別発信元数の比率を図 4-2 に示します。



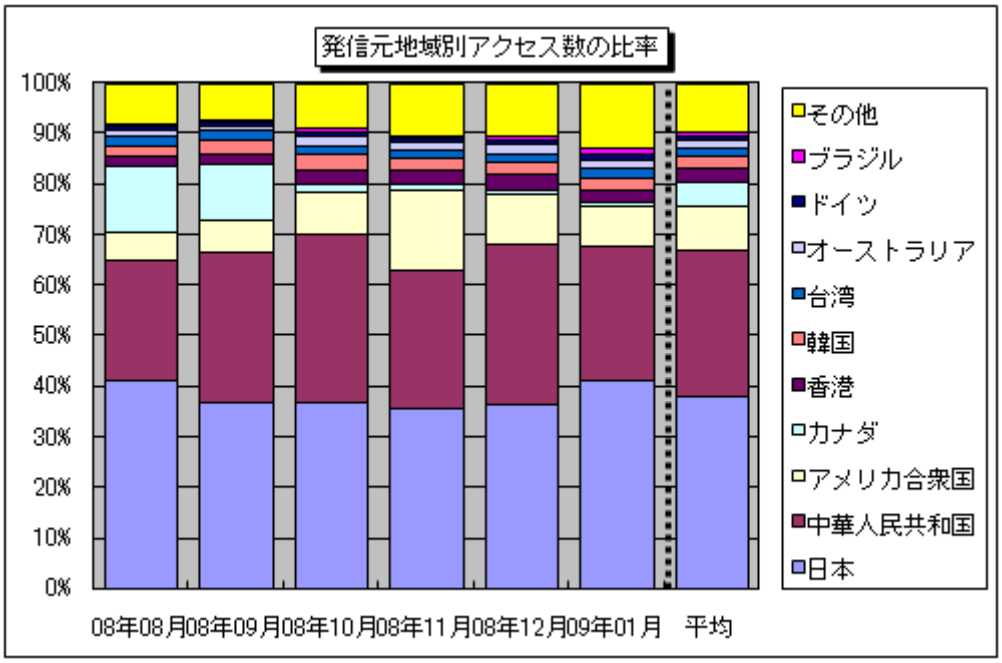
【図 4-1　2008 年 8 月～2009 年 1 月の宛先(ポート種類)別アクセス数の比率】



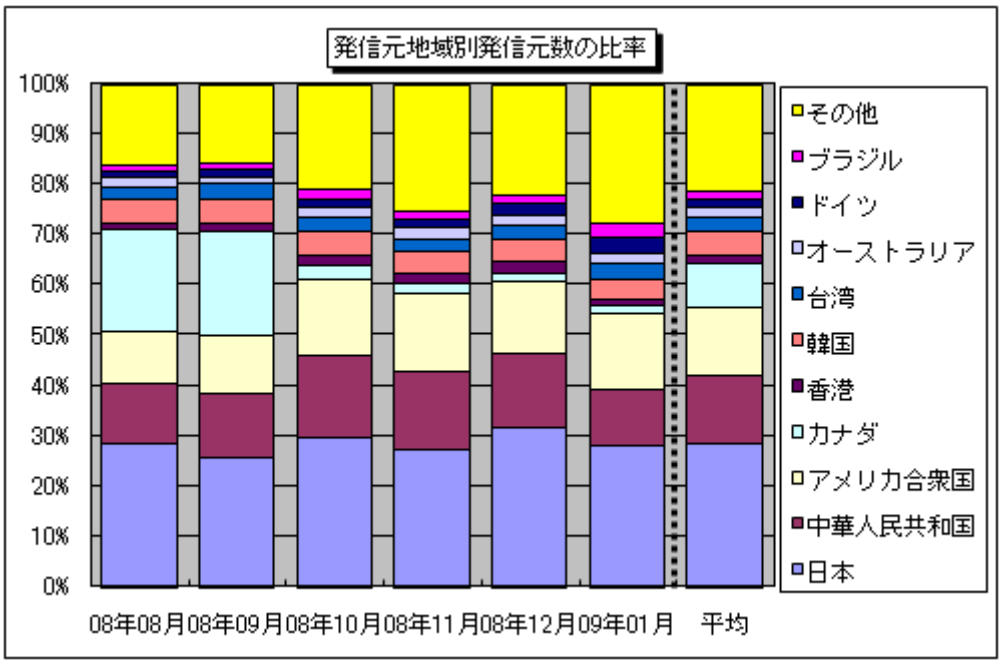
【図 4-2　2008 年 8 月～2009 年 1 月の宛先(ポート種類)別発信元数の比率】

(2)発信元地域別の比率

2008 年 8 月～2009 年 1 月の発信元地域別アクセス数の比率を図 4-3 に、発信元地域別発信元数の比率を図 4-4 に示します。



【図 4-3　2008 年 8 月～2009 年 1 月の発信元地域別アクセス数の比率】



【図 4-4　2008 年 8 月～2009 年 1 月の発信元地域別発信元数の比率】

5．補足説明

以下に、2009 年 1 月にアクセス数の多かった宛先(ポート種類)の解説を行います。

ポート種類	解説
Ping(ICMP)	相手のコンピュータが動作中か調べる目的で使用されるが、不正アクセスの対象コンピュータを探す目的で、W32/Welchia などに利用されたことで有名
22(TCP)	パスワードクラッキング攻撃によるシステムへの侵入を目的とした、SSH(Secure SHell … ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ)を狙ったアクセスです
135(TCP)	Microsoft Windows Remote Procedure Call(RPC)のデフォルトポートであり、RPC に関する脆弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster など)
139(TCP)	保護の甘いファイル(ネットワーク)共有を狙った不正アクセスが有名ですが、一般的に Window の脆弱性を狙ったアクセスである可能性が高いです
445(TCP)	保護の甘いファイル(ネットワーク)共有や Windows2000 特有の脆弱性を狙った不正アクセスが有名(W32/Sasser など)
1026(UDP)/1027(UDP)/1028(UDP)	Microsoft Windows Messenger service(MSN Messenger とは別物)を利用したポップアップ(スパム)メッセージの送信で有名
1433(TCP)	Microsoft SQL Sever の既定ポートであり、SQL Server が動作中のコンピュータを探す目的や、SQL Server の脆弱性を狙った不正アクセスなど
1434(UDP)	Microsoft SQL Sever の脆弱性を狙った不正アクセスなどが有名(W32/SQLSlammer など)
2967(TCP)	Symantec 製品の脆弱性を狙ったアクセスである可能性が高い

■お問い合わせ先
IPA セキュリティセンター　大浦／花村／加賀谷
Tel:03-5978-7527　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp