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

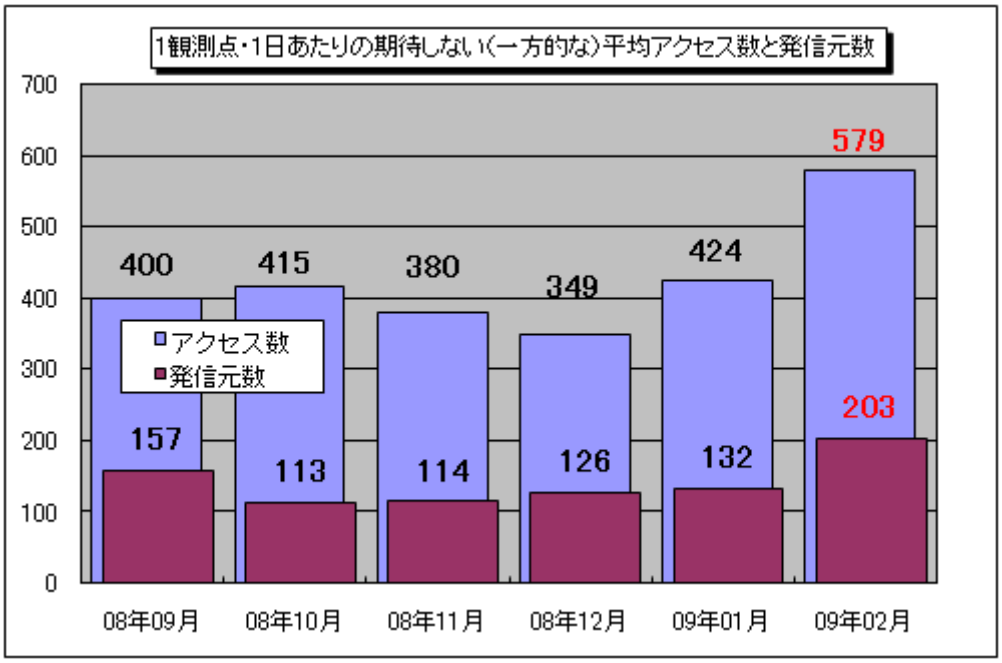
1．一般のインターネット利用者の皆さんへ

インターネット定点観測(TALOT2)によると、2009 年 2 月の期待しない(一方的な)アクセスの総数は 10 観測点で 138,944 件、総発信元(※)は 48,671 箇所ありました。平均すると、1 観測点につき 1 日あたり 203 の発信元から 579 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。

※2 月 6 日～9 日は、TALOT2 のメンテナンスのため、システムを停止しています。そのため、2 月の観測データは、この 4 日間を除外して統計情報を作成しています。



【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】

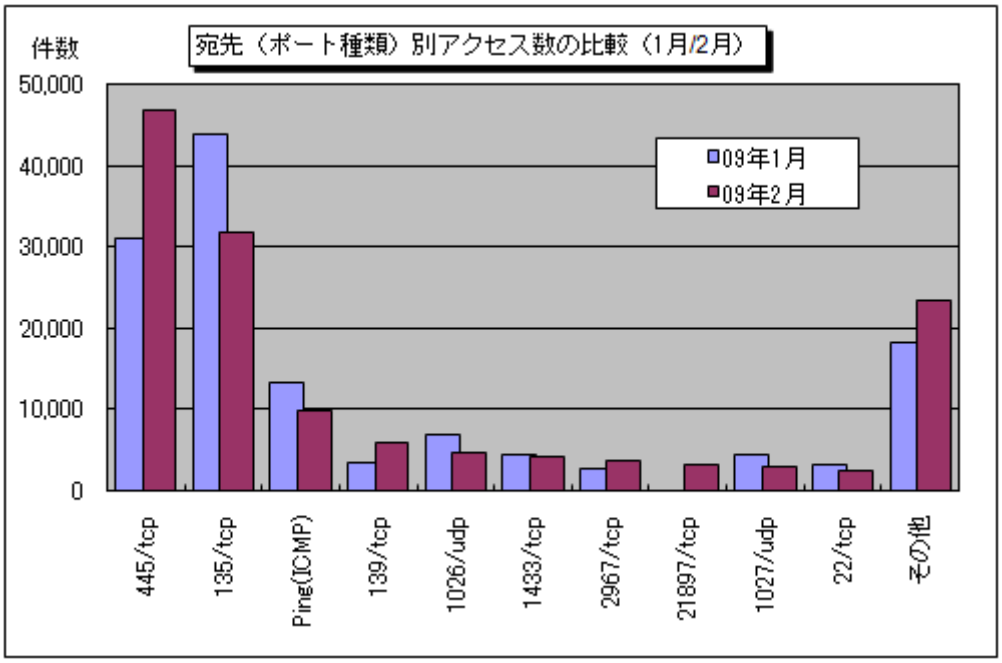
2008 年 9 月～2009 年 2 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 1-1 に示します。2 月の期待しない(一方的な)アクセスは 1 月と比べて大幅に増加しました。

1 月と 2 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。

1 月よりアクセス数が大幅に増加したのは、445/tcp でした。445/tcp へのアクセスは、2 月 6 日～9 日のシステム停止期間の後に大幅に増加していました。詳しくは 2 項(2)で説明しておりますので、そちらを参照ください。このポートは 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。

また、1 月はまったくアクセスがなかった 21897/tcp へのアクセスが多く観測されました。このアクセスが何を目的としたものだったかは不明ですが、特定の日に 1 観測点のみ観測されたアクセスだったことから、ファイル共有ソフトで利用されていた IP アドレスへの再接続動作であった可能性が

あります。以前、他のパソコンのファイル共有ソフトで利用されていた IP アドレスが、今回のシステム停止で、たまたま TALOT2 の観測点の一つに割り当てられた可能性があるということです。

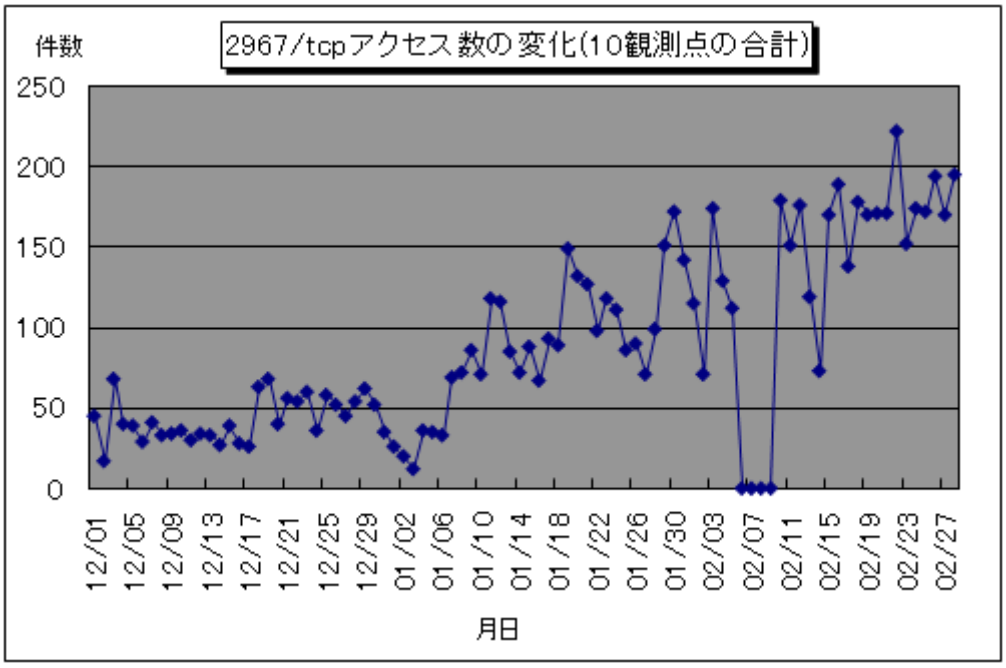


【図 1-2　宛先（ポート種類）別アクセス数の比較（1 月/2 月）】

2.　2009 年 2 月の特異なアクセス

(1) 2967/tcp へのアクセス

2967/tcp へのアクセスが 1 月に入ったあたりから増加し、2 月に入りさらに増加していました(図 2-1 参照)。



【図 2-1　2967/tcp アクセス数の変化（10 観測点の合計）】

2967/tcp は Symantec 製品がデフォルトで使用するポートです。過去に『Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性(SYM06-010)』が公開されています。

この脆弱性は、影響を受ける製品（Symantec Client Security や Symantec AntiVirus など）において、攻撃者によってファイルの取得または削除が可能となり、システムが破壊される可能性がある、というものです。

（ご参考）

「Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性(SYM06-010)」
2006 年 5 月 25 日発表
http://www.symantec.com/region/jp/avcenter/security/content/2006.05.25.html

今でもこの脆弱性を狙った攻撃が行われている可能性があります。Symantec Client Security や Symantec AntiVirus の利用者は、Live Update によりプログラムを最新にすることで脆弱性を解消することができます。利用者は、利用しているプログラムが最新であるか確認してください。特に、利用期限が終了していて最新のプログラムに更新できない方は、最新版を購入して使用してください。
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、お使いの製品の脆弱性対策を迅速に行えるようにしてください。

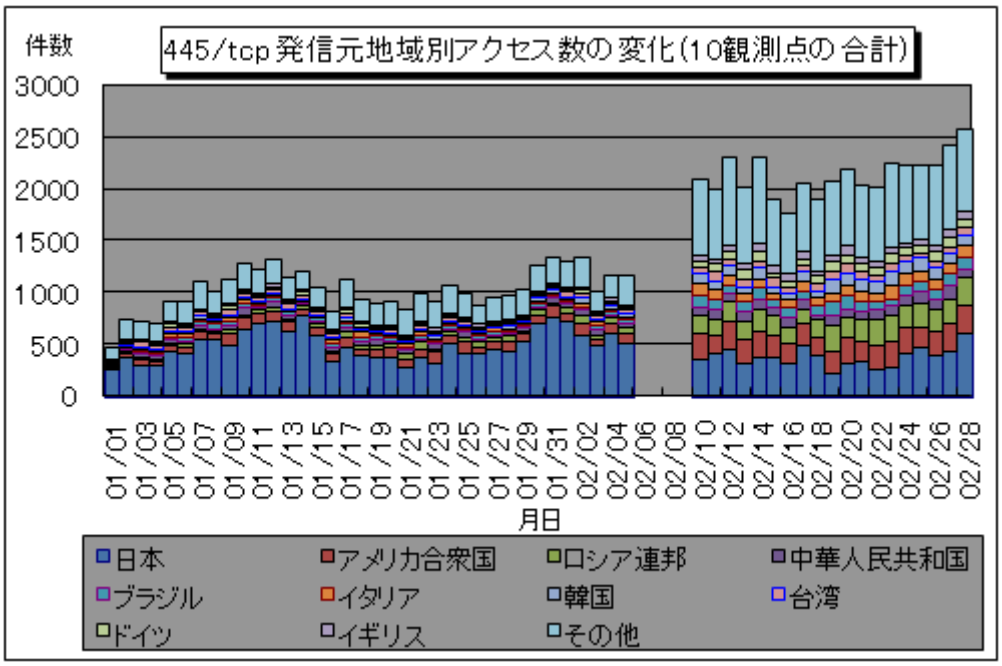
(ご参考)
「JVN (Japan Vulnerability Notes)」(脆弱性対策情報ポータルサイト)
http://jvn.jp/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

(2) 445/tcp へのアクセス

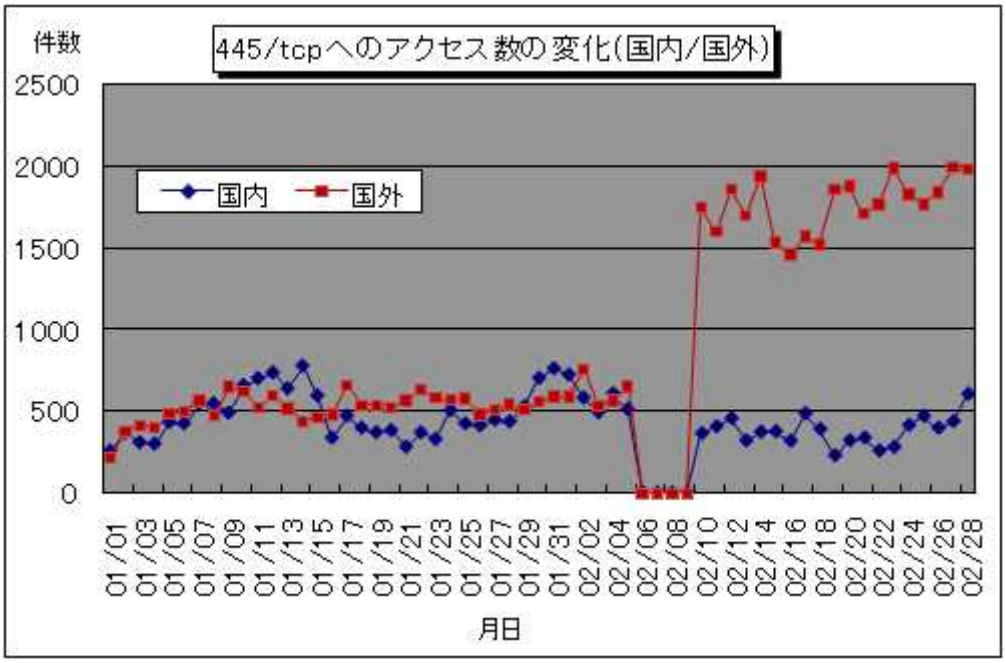
445/tcp へのアクセスは、1 月に既に多くのアクセスが観測されていましたが、2 月にはさらに多くのアクセスが観測されました(図 2-2 参照)。1 月の報告で解説した状況が続いているものと思われます。

(ご参考)
2009 年 1 月のインターネット定点観測(TALOT2)での観測状況について
http://www.ipa.go.jp/security/txt/2009/documents/TALOT2-0902.pdf

ところで、2 月 6 日～9 日のシステム停止期間の前後でこのポートへのアクセス状況を比較しところ、国内からのアクセスが減少していたにもかかわらず、国外からのアクセスが大幅に増加していたことが分かりました(図 2-3 参照)。
システム停止期間の前後で、IP アドレスのネットワークセグメントが変わっていたことも要因の一つとして考えられるでしょう。



【図 2-2　445/tcp 発信元地域別アクセス数の変化】

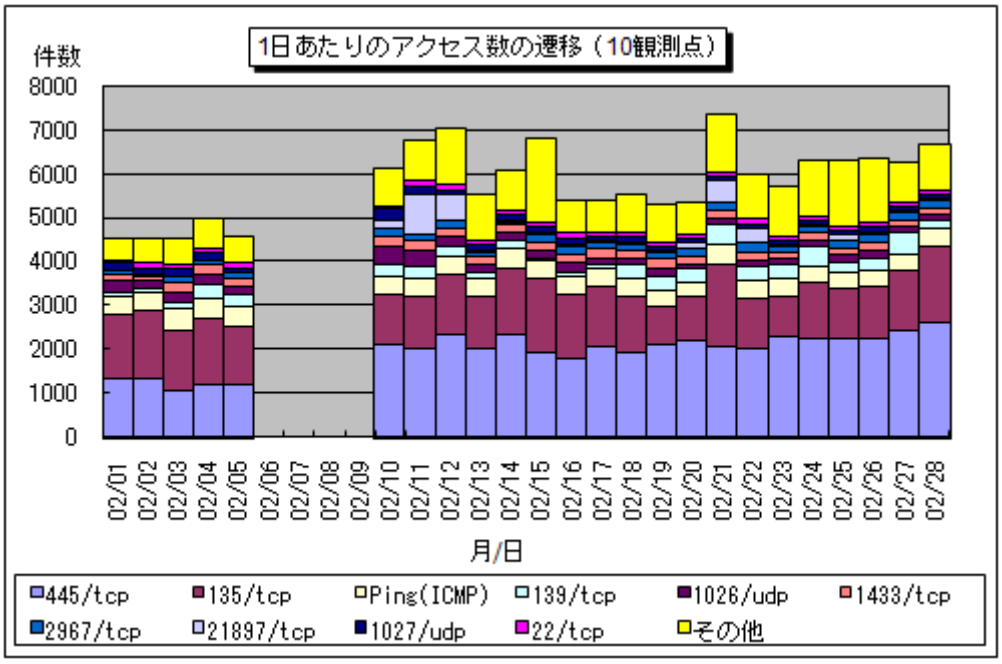


【図 2-3　445/tcp **へのアクセス数の変化（国内/国外)】**

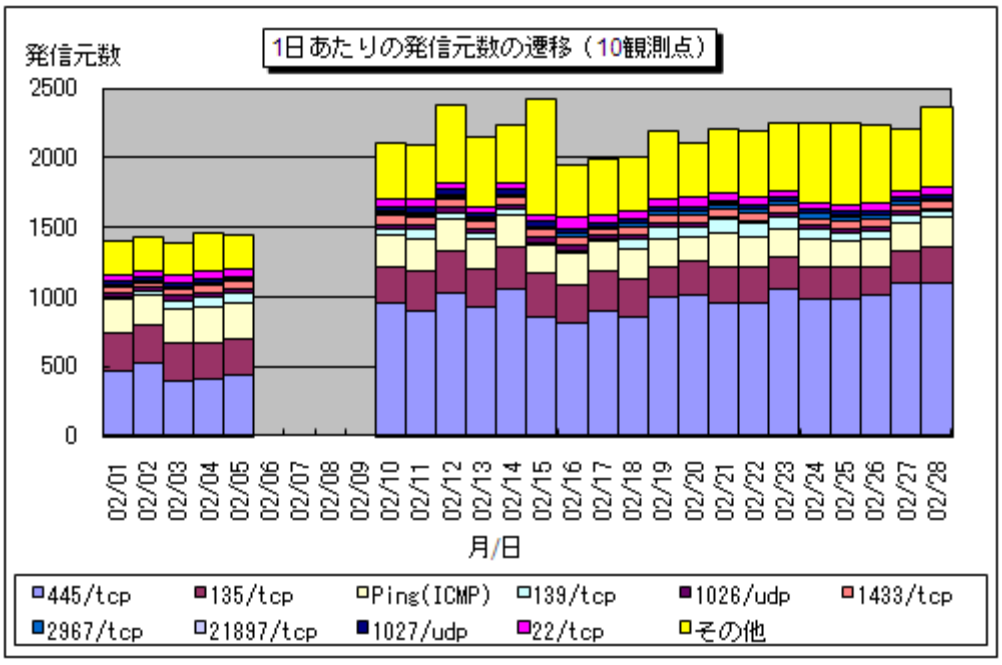
3. 2009 年 2 月の一方的なアクセス状況

(1) 宛先(ポート種類)別のアクセス状況

2009 年 2 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。



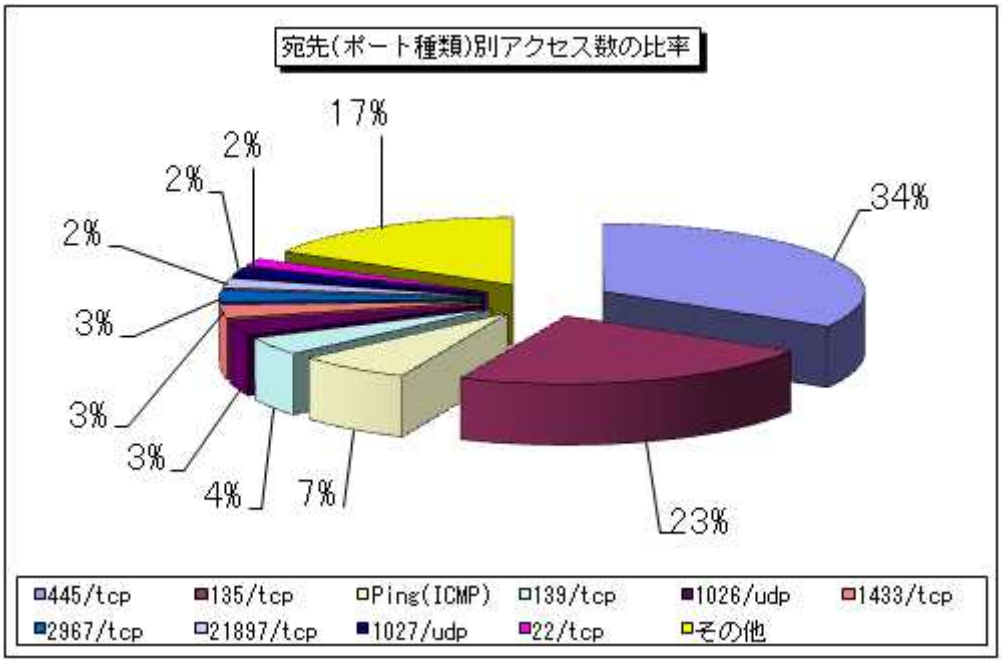
【図 3-1　2009 年 2 月の 1 日あたりのアクセス数の遷移】



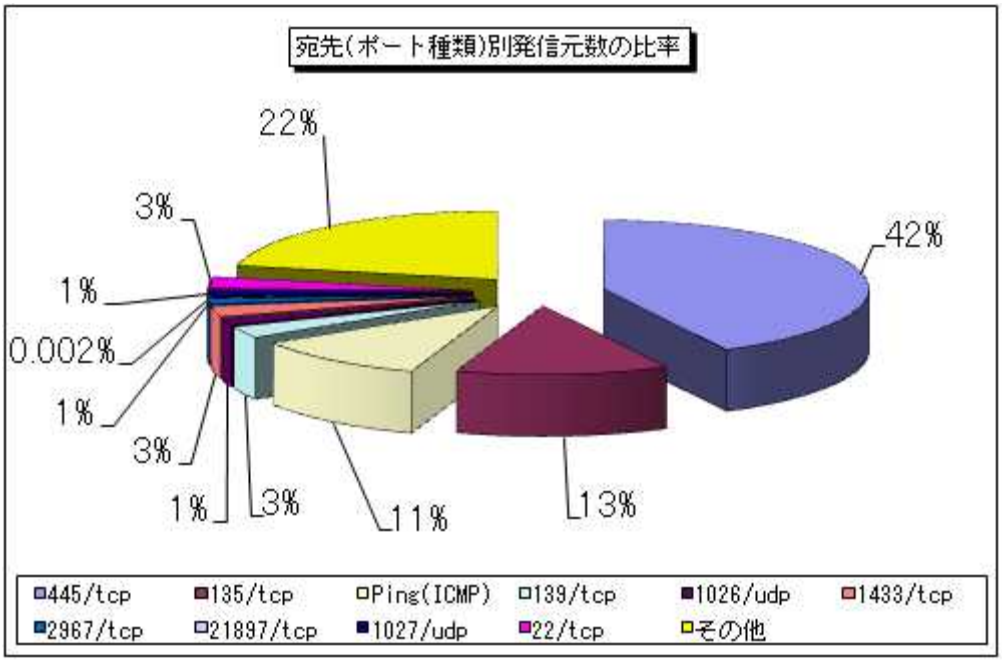
【図 3-2　2009 年 2 月の 1 日あたりの発信元数の遷移】

(2)宛先(ポート種類)別の比率

2009 年 2 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。



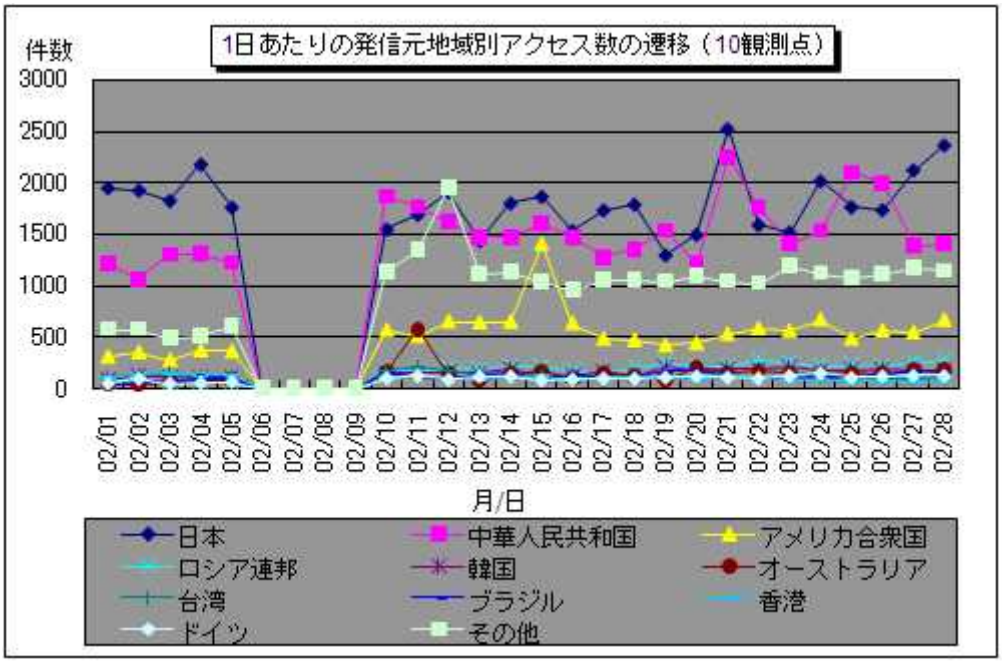
【図 3-3　2009 年 2 月の宛先(ポート種類)別アクセス数の比率】



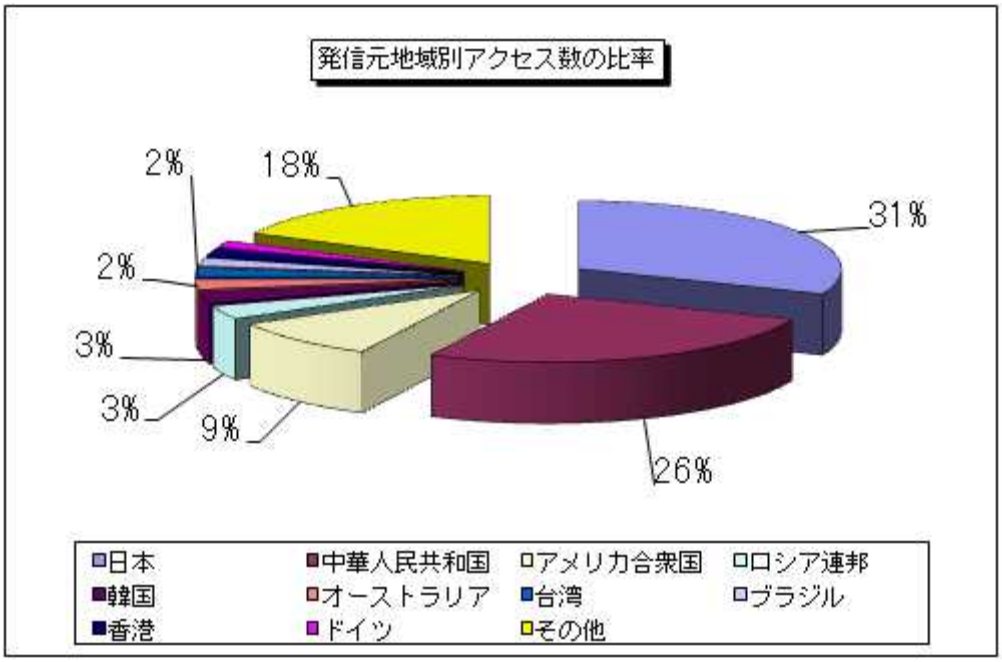
【図 3-4　2009 年 2 月の宛先(ポート種類)別発信元数の比率】

(3)発信元地域別のアクセス状況

2009 年 2 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。

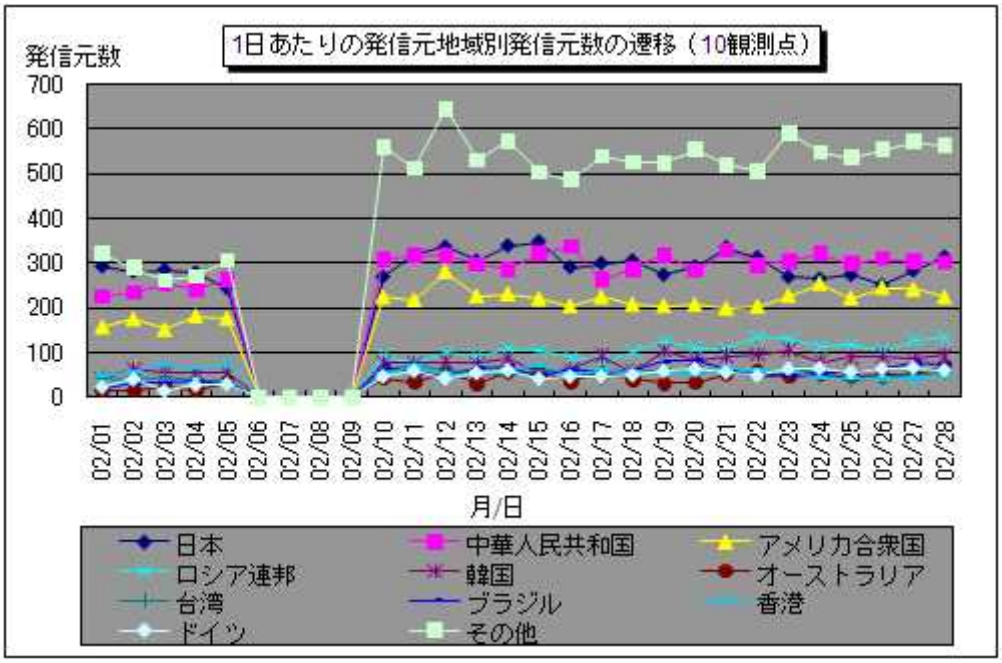


【図 3-5　2009 年 2 月の 1 日あたりの発信元地域別アクセス数の遷移】

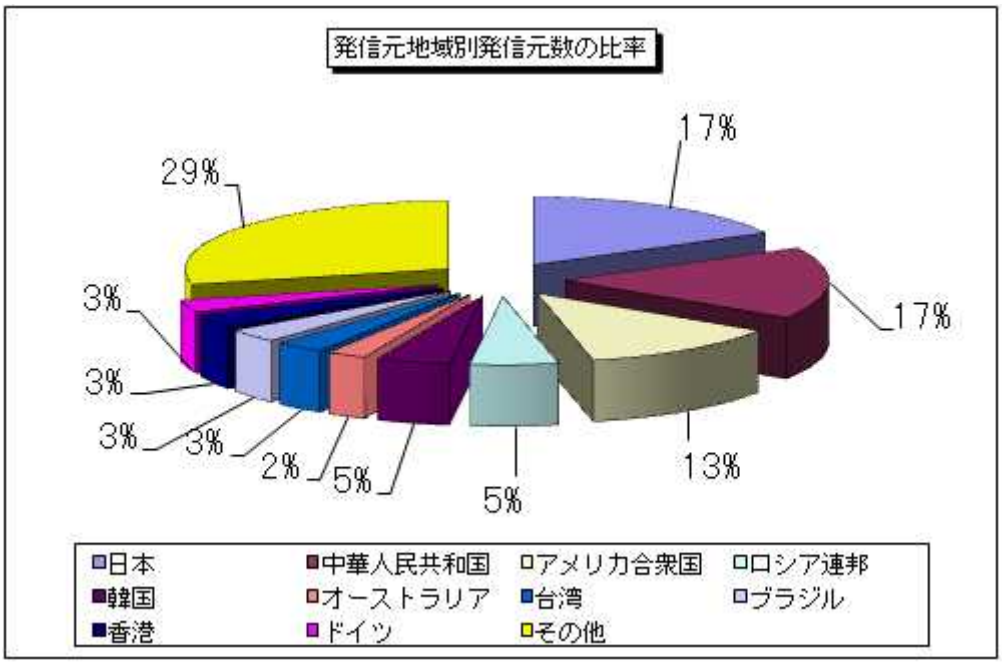


【図 3-6　2009 年 2 月の発信元地域別アクセス数の比率】

2009 年 2 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 2 月の 1 日あたりの発信元地域別発信元数の遷移】

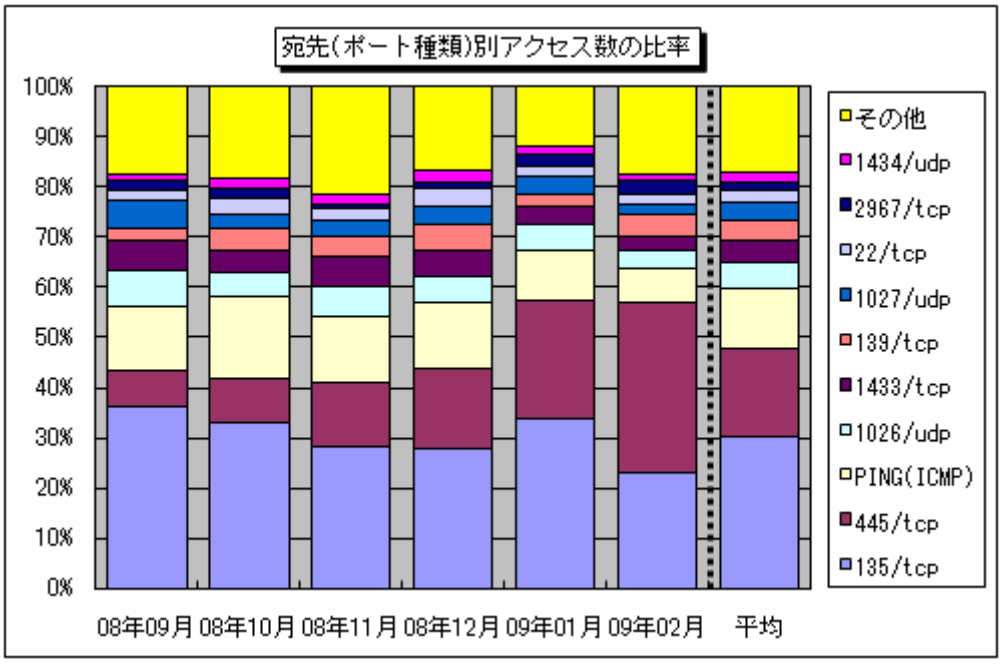


【図 3-8　2009 年 2 月の発信元地域別発信元数の比率】

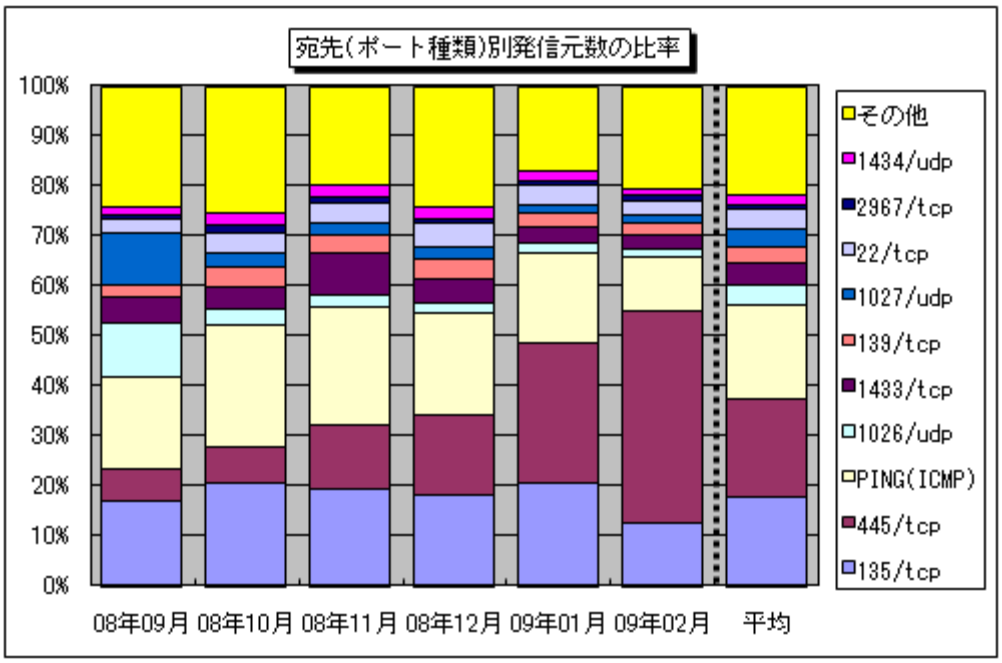
4．統計情報

(1)宛先(ポート種類)別の比率

2008 年 9 月～2009 年 2 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。



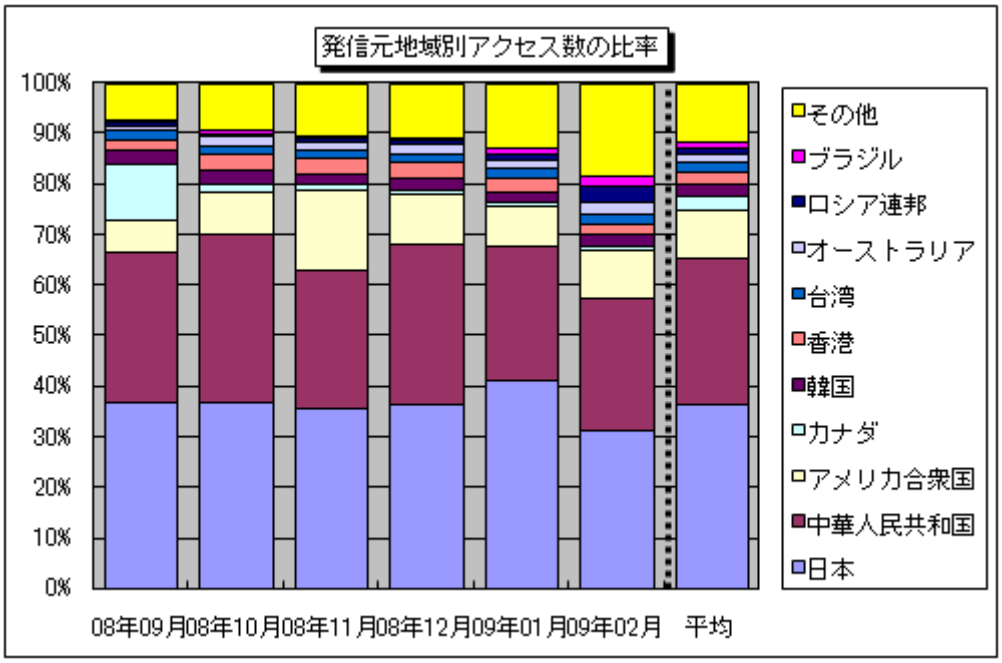
【図 4-1　2008 年 9 月～2009 年 2 月の宛先(ポート種類)別アクセス数の比率】



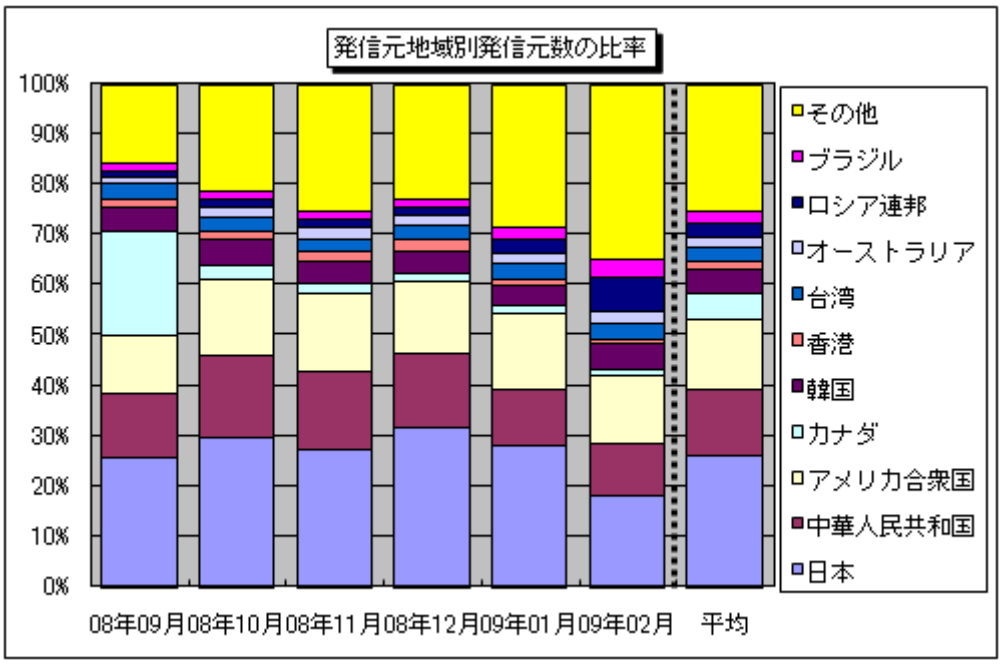
【図 4-2　2008 年 9 月～2009 年 2 月の宛先(ポート種類)別発信元数の比率】

(2)発信元地域別の比率

2008 年 9 月～2009 年 2 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 9 月～2009 年 2 月の発信元地域別アクセス数の比率】



【図 4-4　2008 年 9 月～2009 年 2 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 2 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	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(Symantec Client Security や Symantec AntiVirus など)の脆弱性を狙ったアクセスである可能性が高い。
21897/tcp	目的不明のアクセスですが、、以前ファイル共有ソフトで利用していた IP アドレスへの再接続動作であった可能性があります。

■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