別紙 3

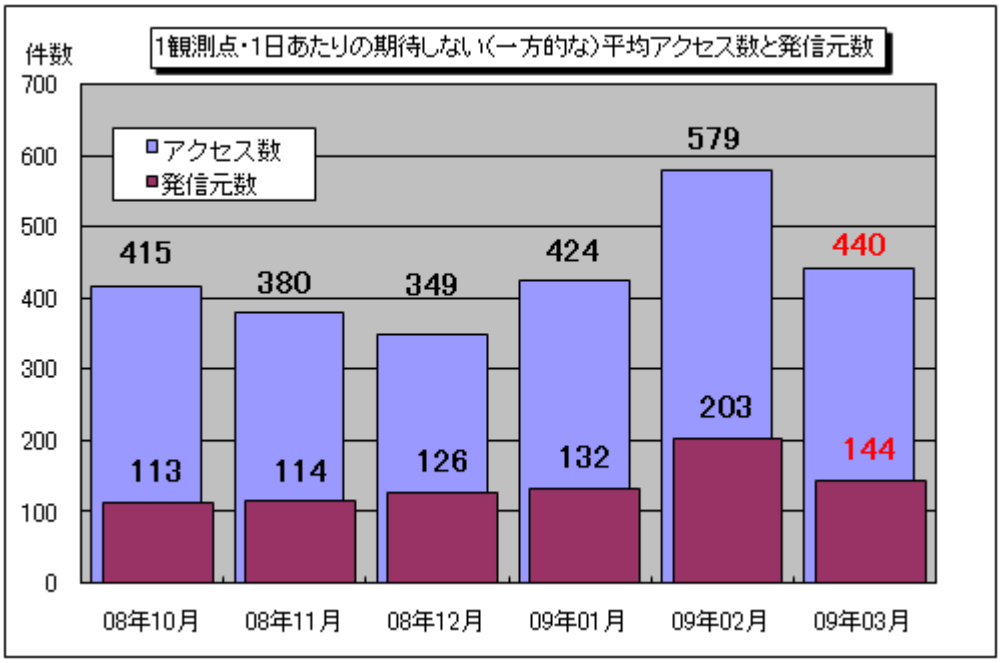
インターネット定点観測(TALOT2)での観測状況について

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 3 月の期待しない(一方的な)アクセスの総数は 10 観測点で 136,473 件、総発信元(※)は 44,646 箇所ありました。平均すると、1 観測点につき 1 日あたり 144 の発信元から 440 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。

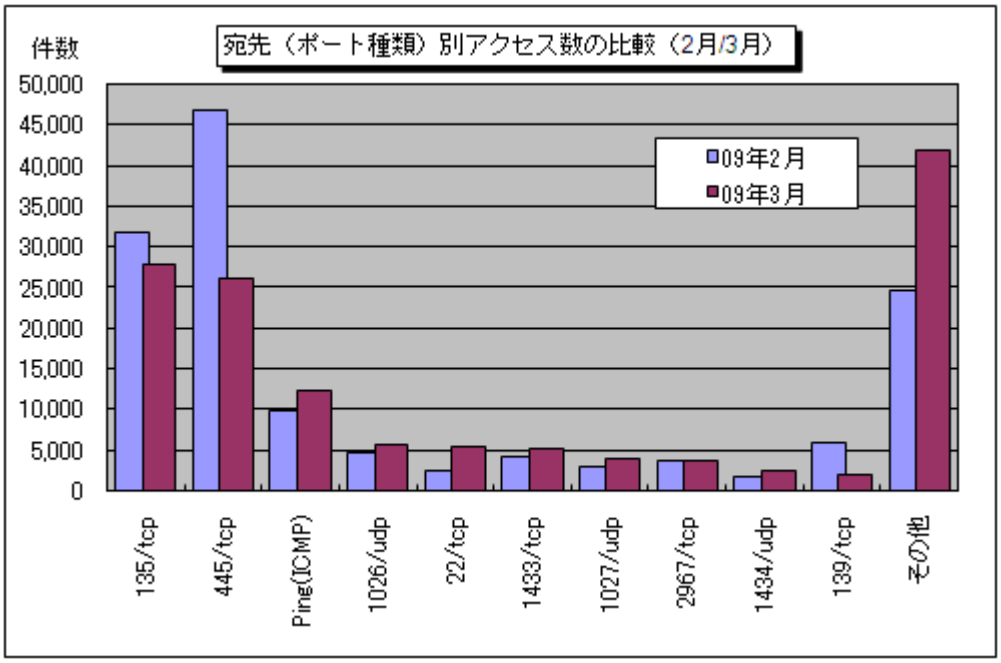


【図 1-1　1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 10 月～2009 年 3 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。3 月の期待しない(一方的な)アクセスは 2 月と比べて大幅に減少しました。

2 月と 3 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。

2 月より大幅に減少したのは 445/tcp へのアクセスであり、約 2 万件の減少(2 月比で約 56%)でした。詳細は 2 項(1)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。



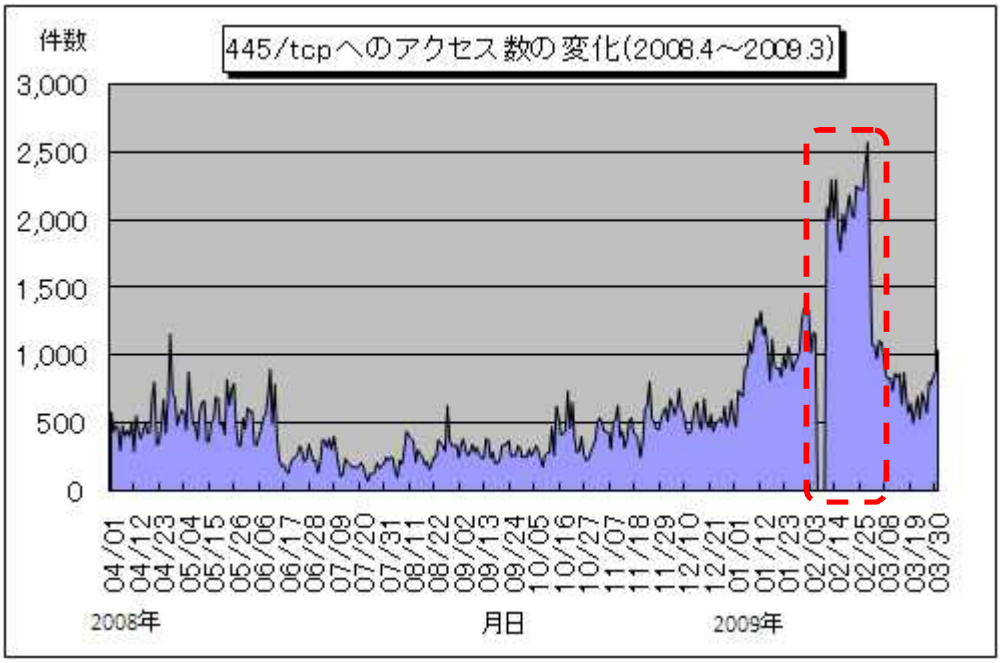
【図 1-2　宛先（ポート種類）別アクセス数の比較（2 月/3 月）】

2.　2009 年 3 月の特異なアクセス

(1) 445/tcp へのアクセス

2 月と比較して 3 月は 445/tcp へのアクセスが大幅に減少しましたが、過去 1 年間を通してみると、2 月はアクセス数が特別多かったに過ぎず、3 月は 2 月より前の水準に戻ったと言えます(図 2-1 参照)。

445/tcp へのアクセスが 2 月に増加したタイミングはメンテナンスによるシステムの停止がきっかけでしたが、3 月に減少したタイミングも不定期に行っている TALOT2 の観測点の変更がきっかけでした。それぞれのタイミングで 445/tcp へのアクセス数が大きく変化したことについて、本質的な要因は特定できておりません。

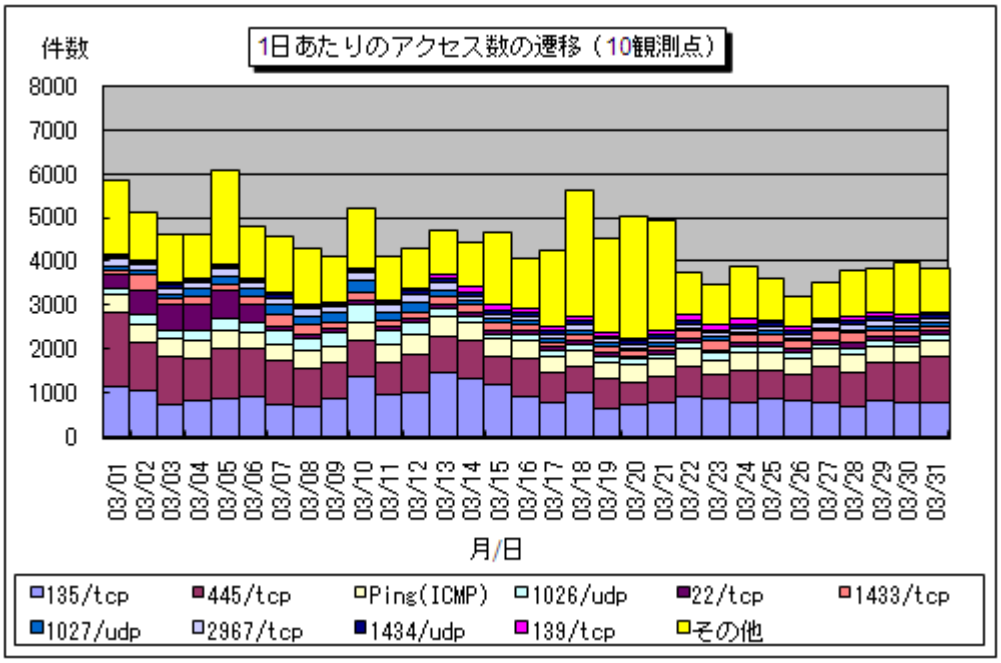


【図 2-1　445/tcp 発信元地域別アクセス数の変化】

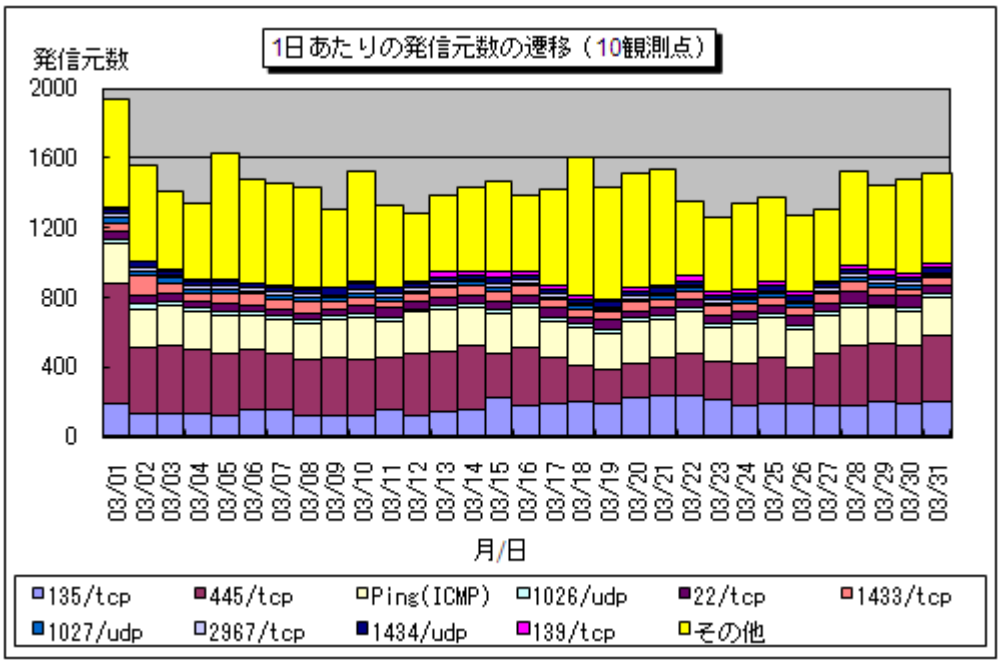
3. 2009 年 3 月の一方的なアクセス状況

(1) 宛先(ポート種類)別のアクセス状況

2009 年 3 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。



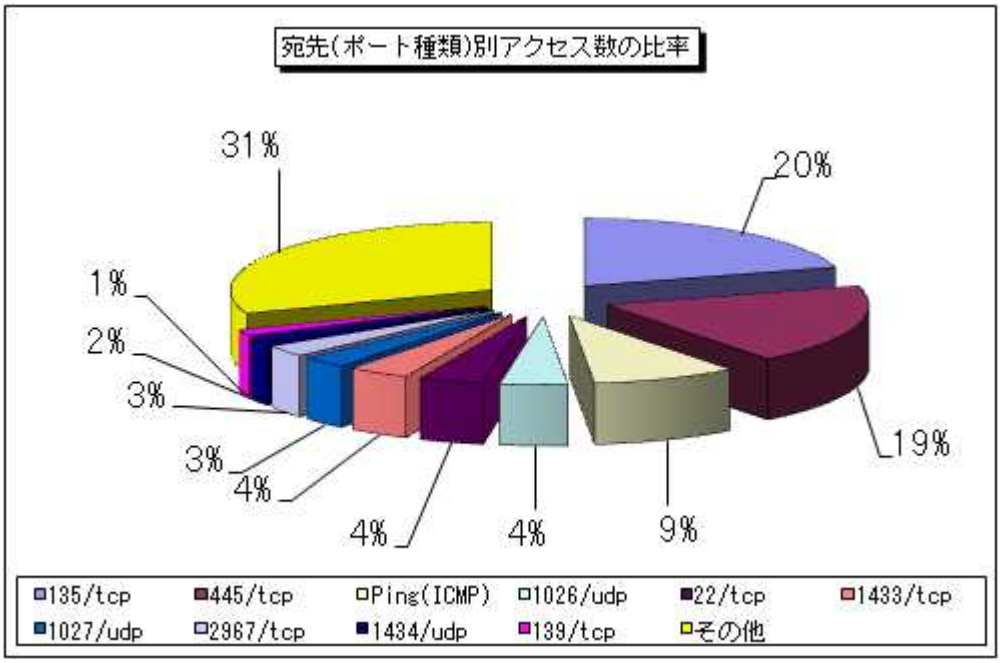
【図 3-1　2009 年 3 月の 1 日あたりのアクセス数の遷移】



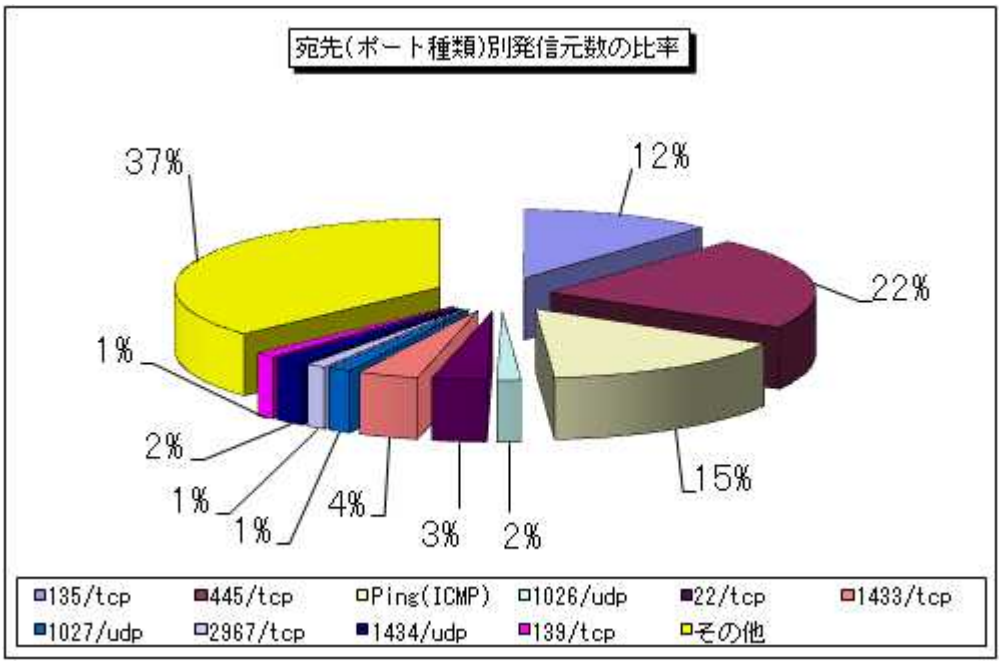
【図 3-2　2009 年 3 月の 1 日あたりの発信元数の遷移】

(2)宛先(ポート種類)別の比率

2009 年 3 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。



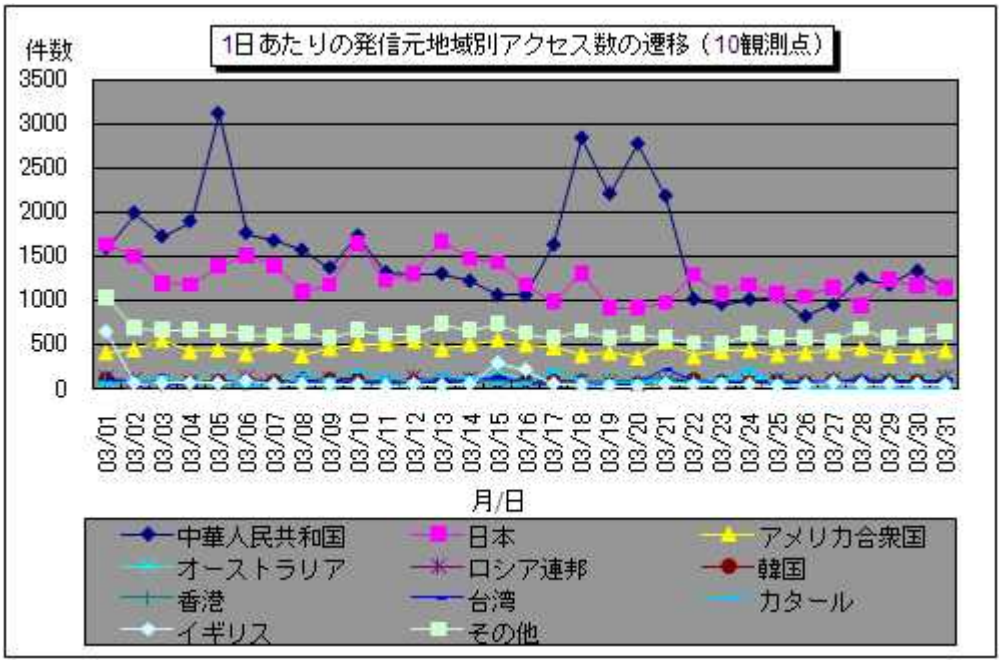
【図 3-3　2009 年 3 月の宛先(ポート種類)別アクセス数の比率】



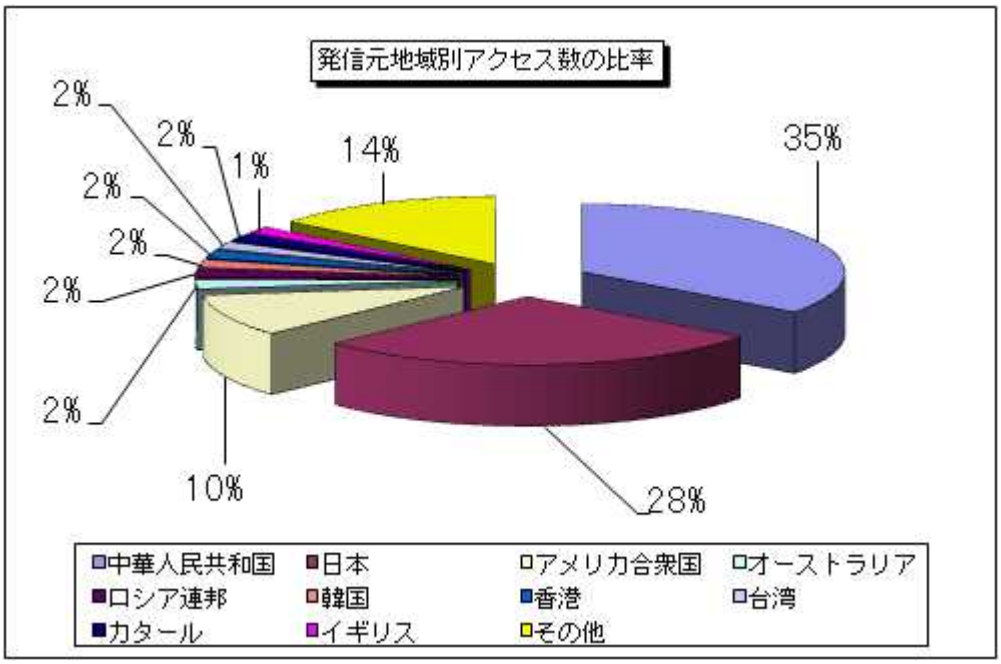
【図 3-4　2009 年 3 月の宛先(ポート種類)別発信元数の比率】

(3)発信元地域別のアクセス状況

2009 年 3 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。

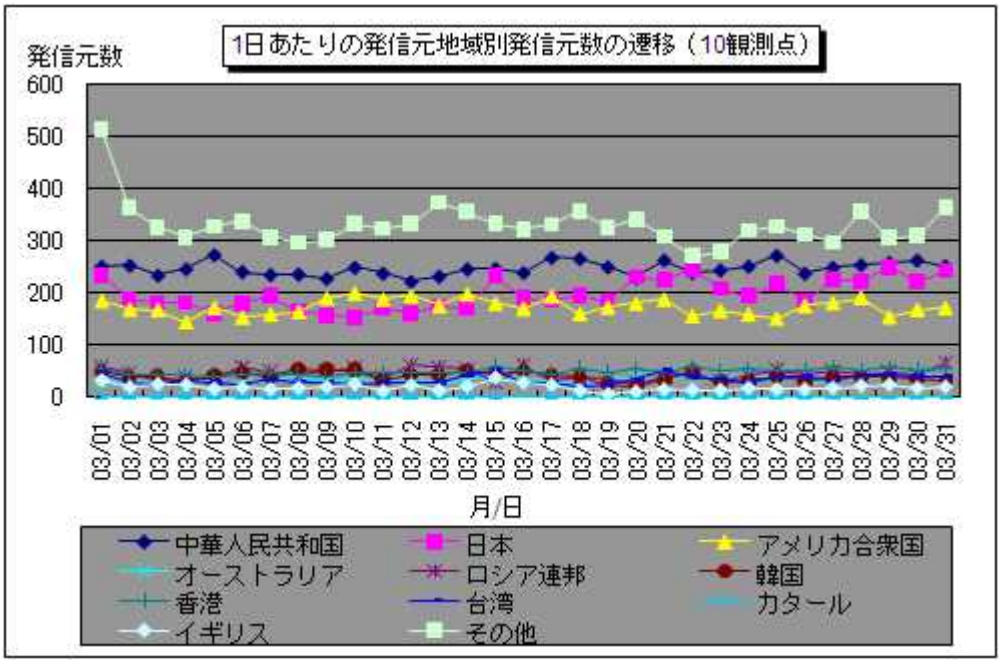


【図 3-5　2009 年 3 月の 1 日あたりの発信元地域別アクセス数の遷移】

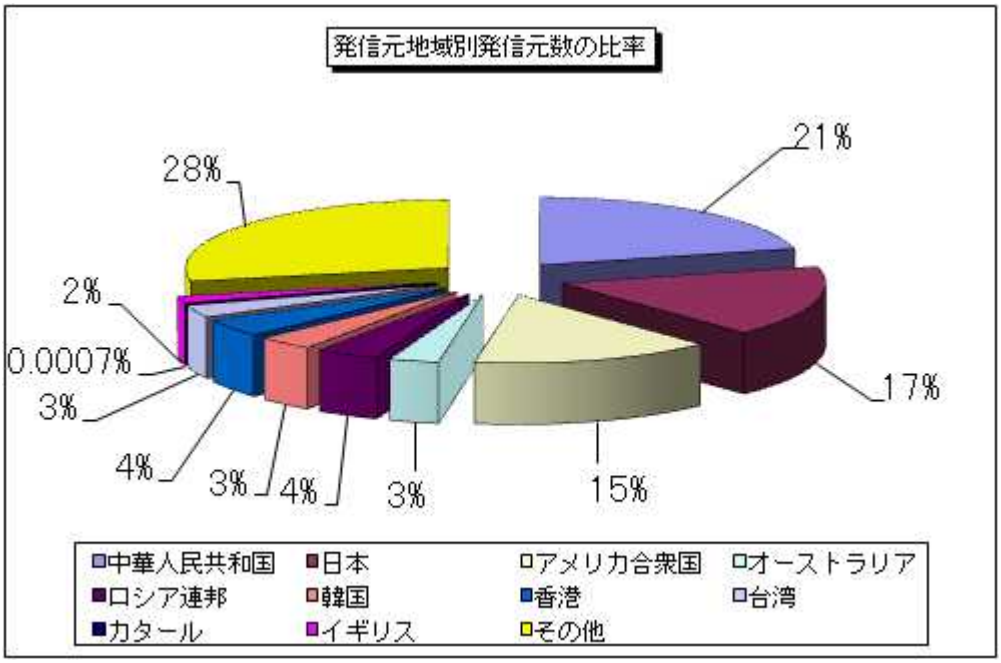


【図 3-6　2009 年 3 月の発信元地域別アクセス数の比率】

2009 年 3 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 3 月の 1 日あたりの発信元地域別発信元数の遷移】

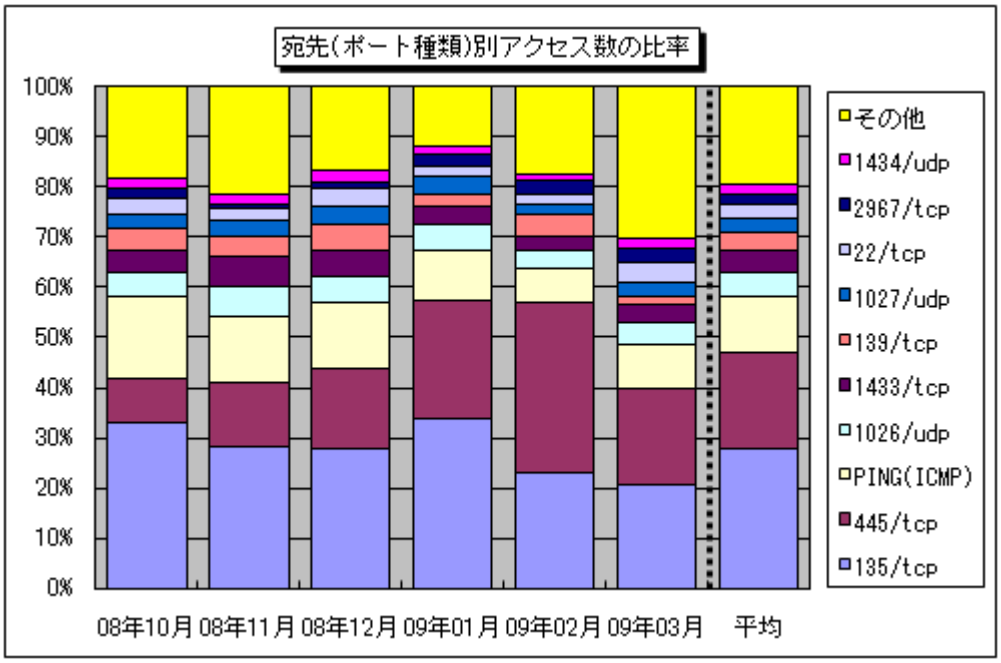


【図 3-8　2009 年 3 月の発信元地域別発信元数の比率】

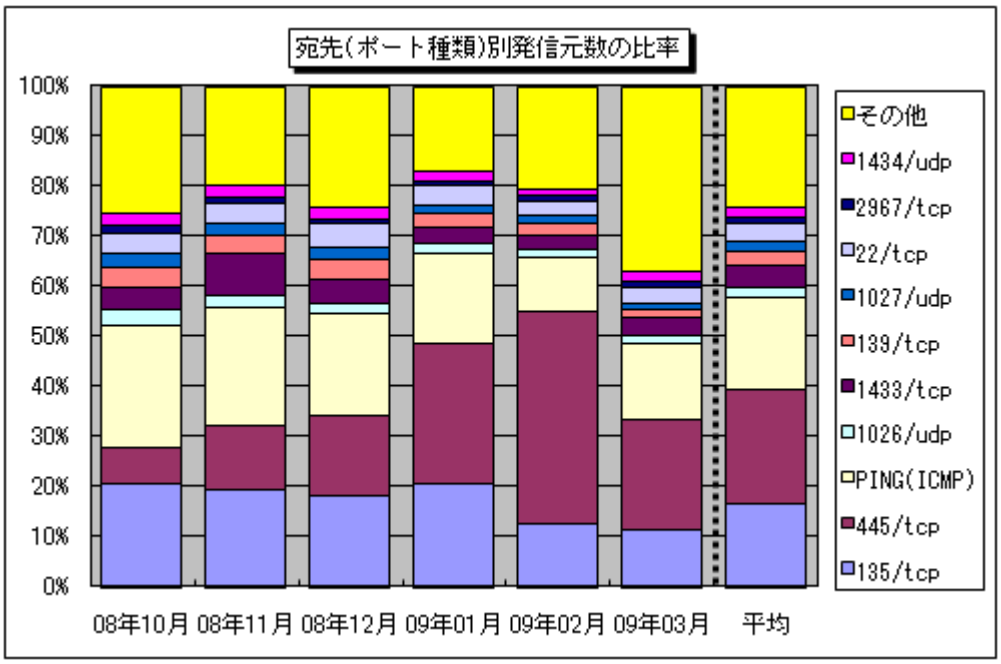
4．統計情報

(1)宛先(ポート種類)別の比率

2008 年 10 月～2009 年 3 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。



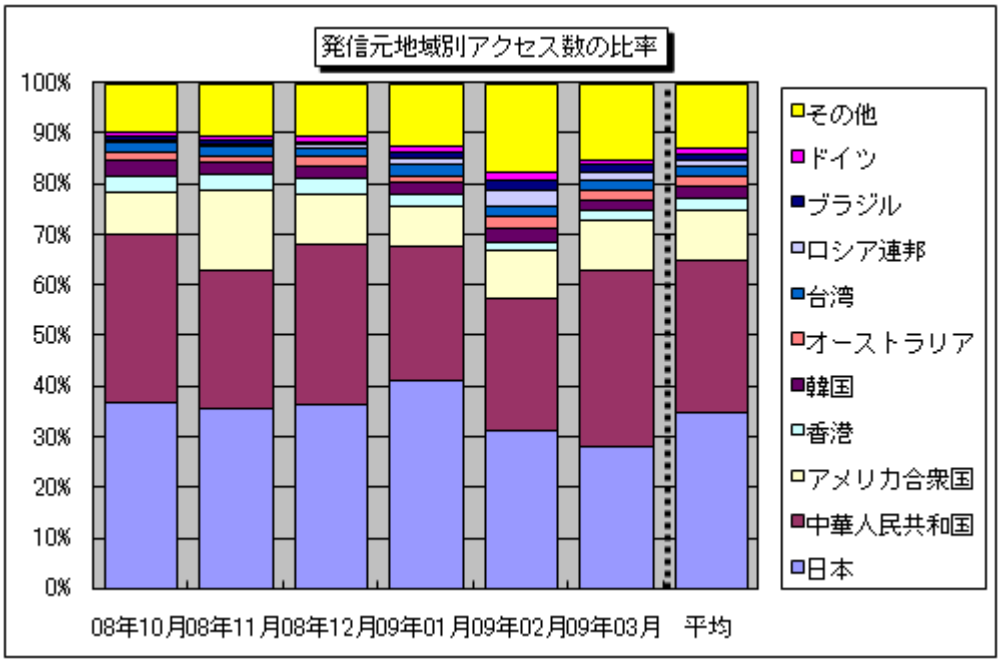
【図 4-1　2008 年 10 月～2009 年 3 月の宛先(ポート種類)別アクセス数の比率】



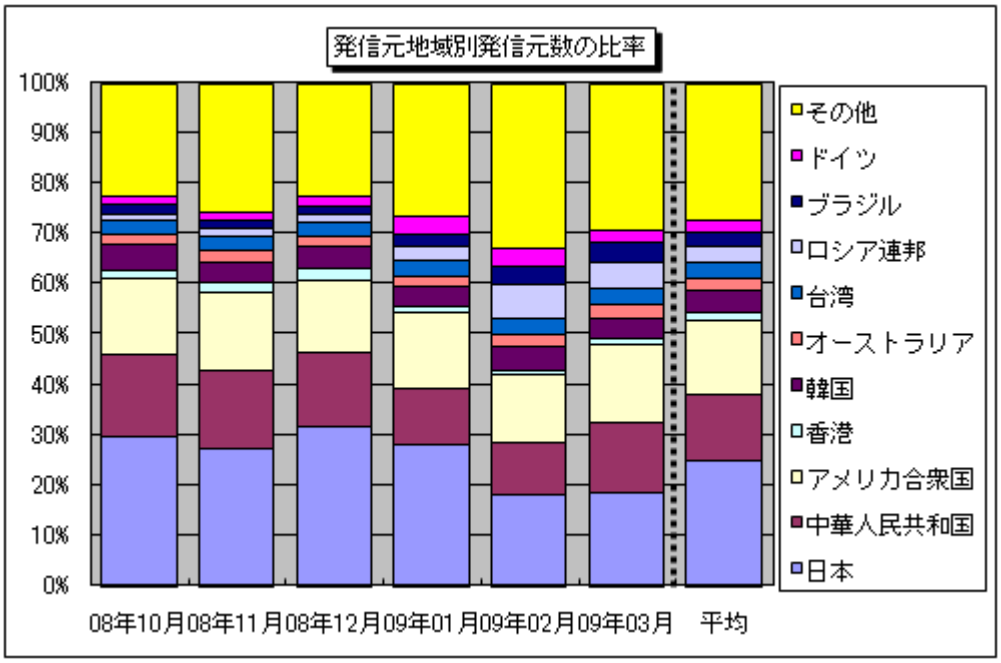
【図 4-2　2008 年 10 月～2009 年 3 月の宛先(ポート種類)別発信元数の比率】

(2)発信元地域別の比率

2008 年 10 月～2009 年 3 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 10 月～2009 年 3 月の発信元地域別アクセス数の比率】



【図 4-4　2008 年 10 月～2009 年 3 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 3 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。

■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