別紙 3

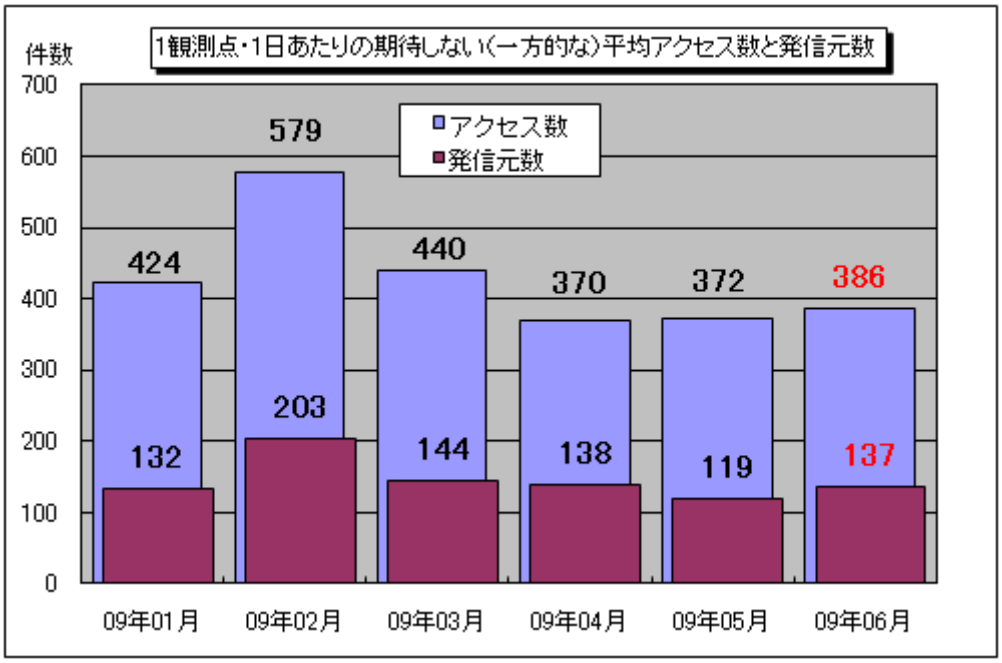
インターネット定点観測(TALOT2)での観測状況について

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 6 月の期待しない(一方的な)アクセスの総数は 10 観測点で **115,860 件**、総発信元(※)は **41,065 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 137 の発信元から 386 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】

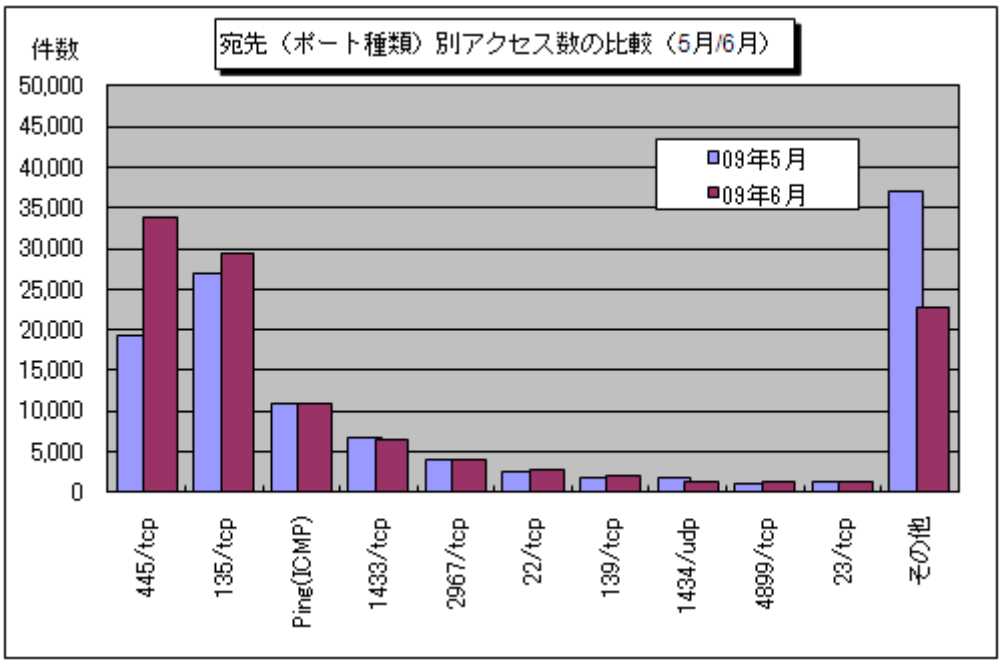
2009 年 1 月～2009 年 6 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 1-1 に示します。6 月の期待しない(一方的な)アクセスは、5 月と比べて若干ですが増加しました。

5 月と 6 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。

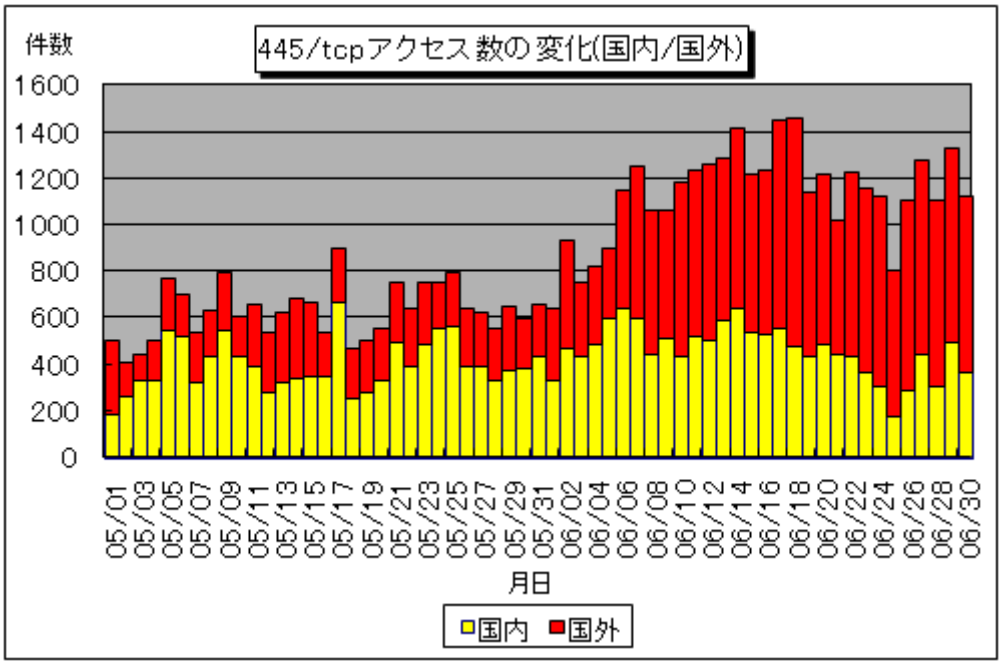
6 月は 5 月に比べ、445/tcp へのアクセスが大幅に増加していました。これは 5 月に比べ、国外からのアクセスが増加したためです(図 1-3 参照)。国外からのアクセスが増加した原因については特定できておりませんが、特定の発信元からのアクセス回数が増加したわけではなく、国外からの発信元数自体が増加したことでアクセス数の増加につながっていました。

また、定点観測を行っている他の組織においても、445/tcp へのアクセスにおいて、国外の発信元数が増加してきているという情報があります。

それ以外のポートへのアクセスについて、大きく変化のあったポートはありませんでしたが、アクセス数の多い上位 10 ポート以外のポートへのアクセスが大幅に減少していました。



【図 1-2　宛先(ポート種類)別アクセス数の比較(5 月/6 月)】

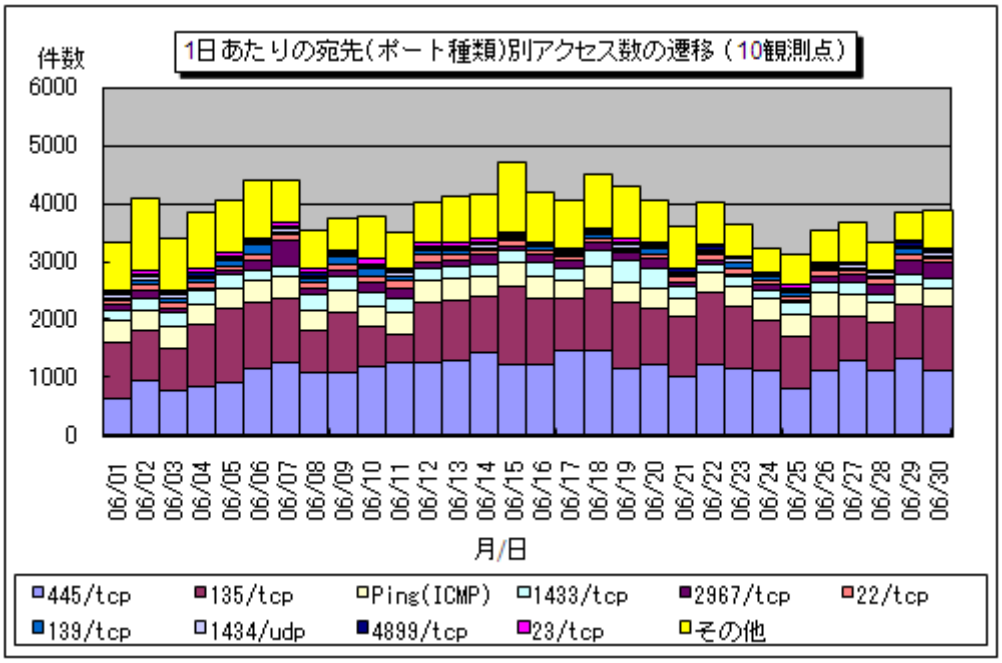


【図 1-3　445/tcp アクセス数の変化(国内/国外)】

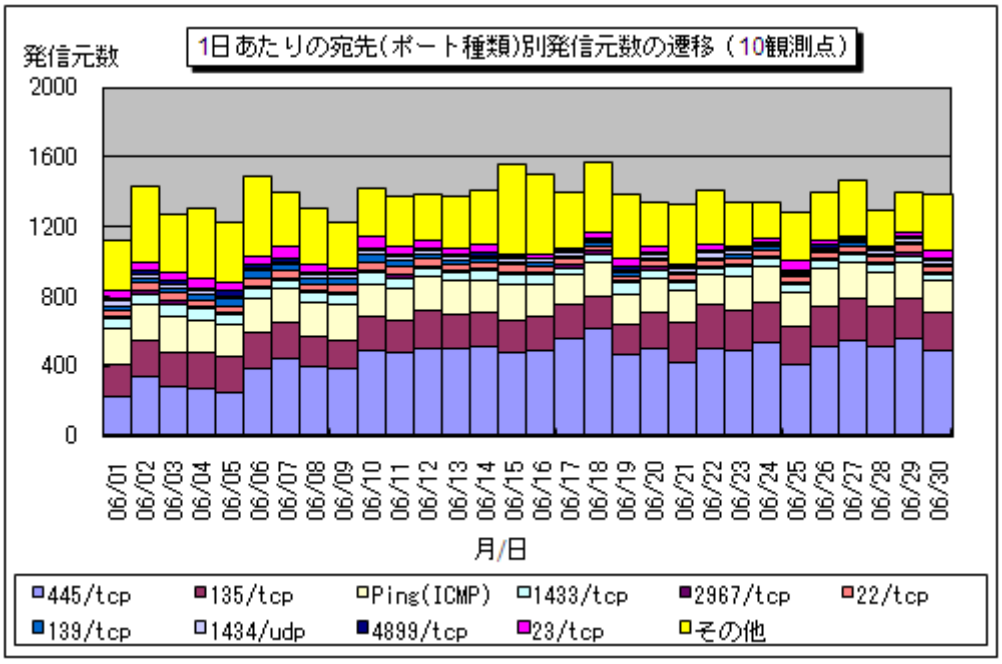
2. 2009 年 6 月の一方的なアクセス状況

(1) 宛先(ポート種類)別のアクセス状況

2009 年 6 月の一方的なアクセス状況(アクセス数)の遷移を図 2-1 に、一方的なアクセス状況(発信元数)の遷移を図 2-2 に示します。



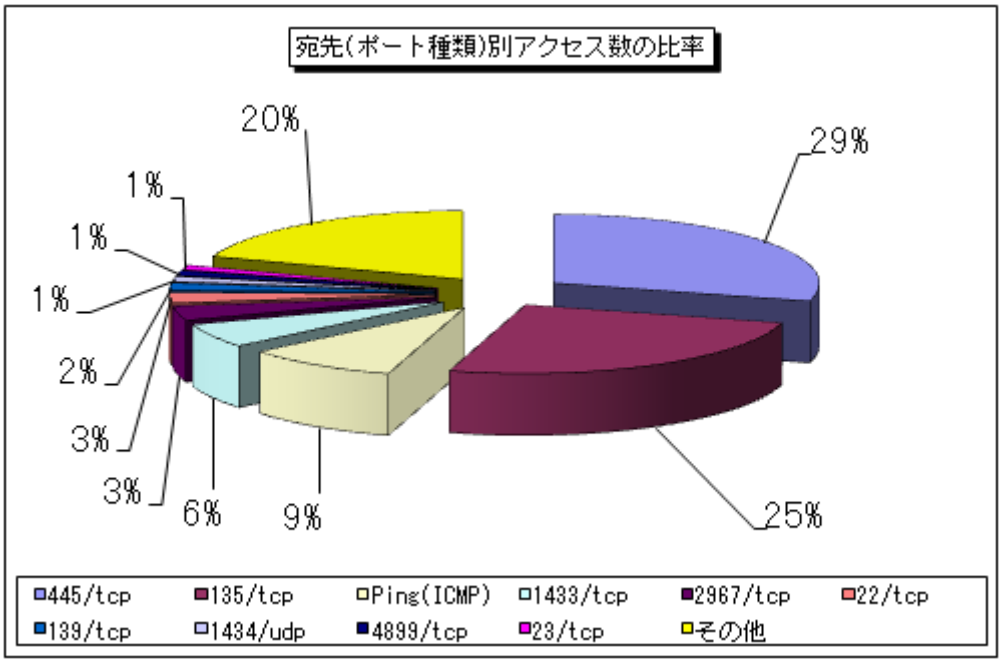
【図 2-1　2009 年 6 月の 1 日あたりのアクセス数の遷移(10 観測点)】



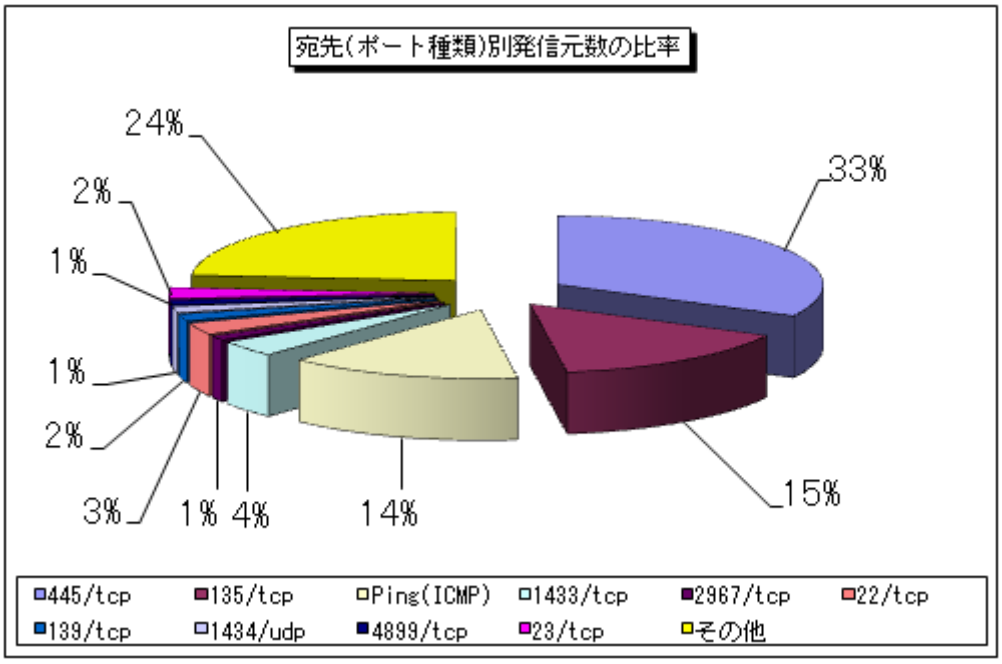
【図 2-2　2009 年 6 月の 1 日あたりの発信元数の遷移(10 観測点)】

(2)宛先(ポート種類)別の比率

2009 年 6 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 2-3 に、宛先(ポート種類)別発信元数の比率を図 2-4 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。



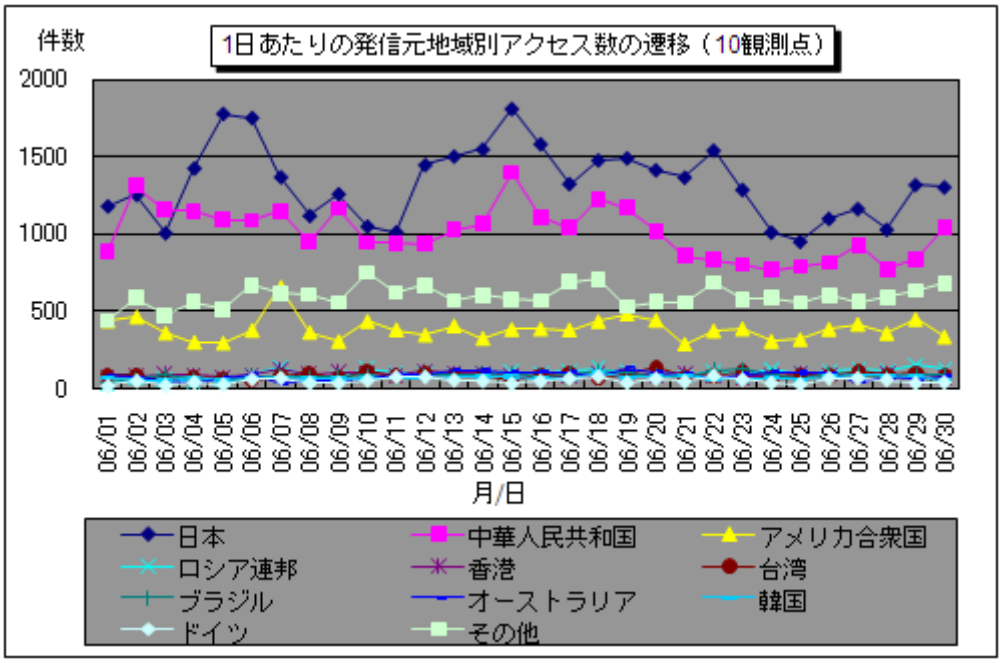
【図 2-3　2009 年 6 月の宛先(ポート種類)別アクセス数の比率】



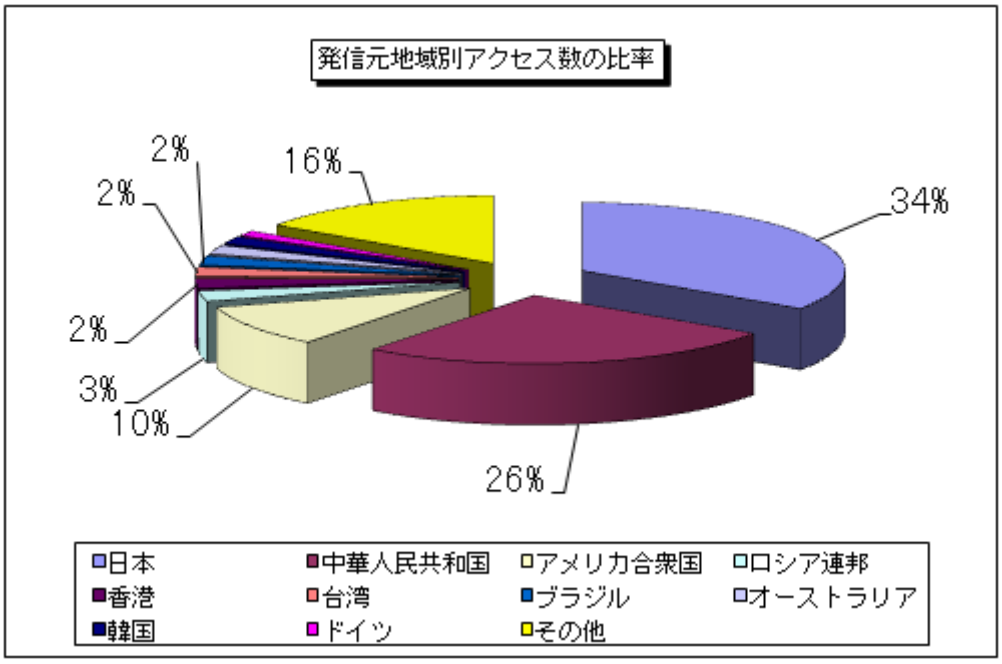
【図 2-4　2009 年 6 月の宛先(ポート種類)別発信元数の比率】

(3)発信元地域別のアクセス状況

2009 年 6 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 2-5 に、発信元地域別アクセス数の比率を図 2-6 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。

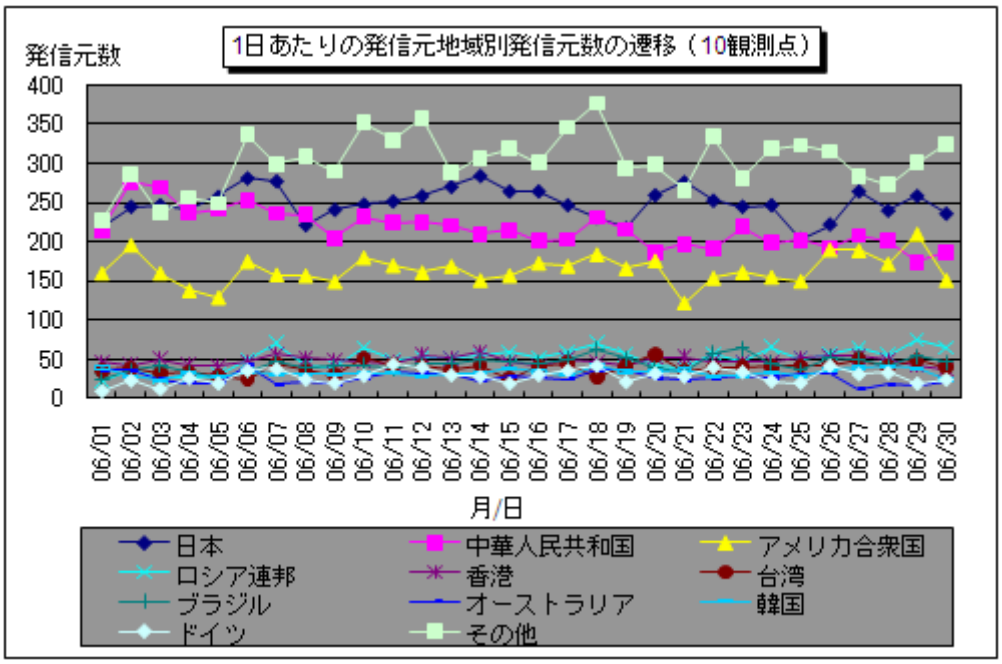


【図 2-5　2009 年 6 月の 1 日あたりの発信元地域別アクセス数の遷移(10 観測点)】

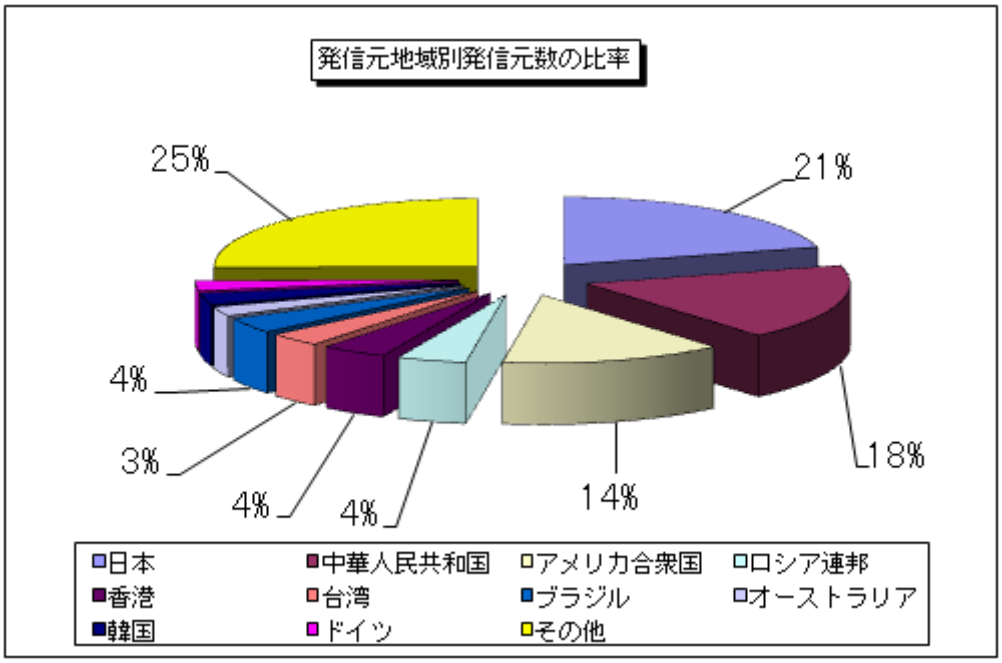


【図 2-6　2009 年 6 月の発信元地域別アクセス数の比率】

2009 年 6 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 2-7 に、発信元地域別発信元数の比率を図 2-8 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 2-7　2009 年 6 月の 1 日あたりの発信元地域別発信元数の遷移(10 観測点)】

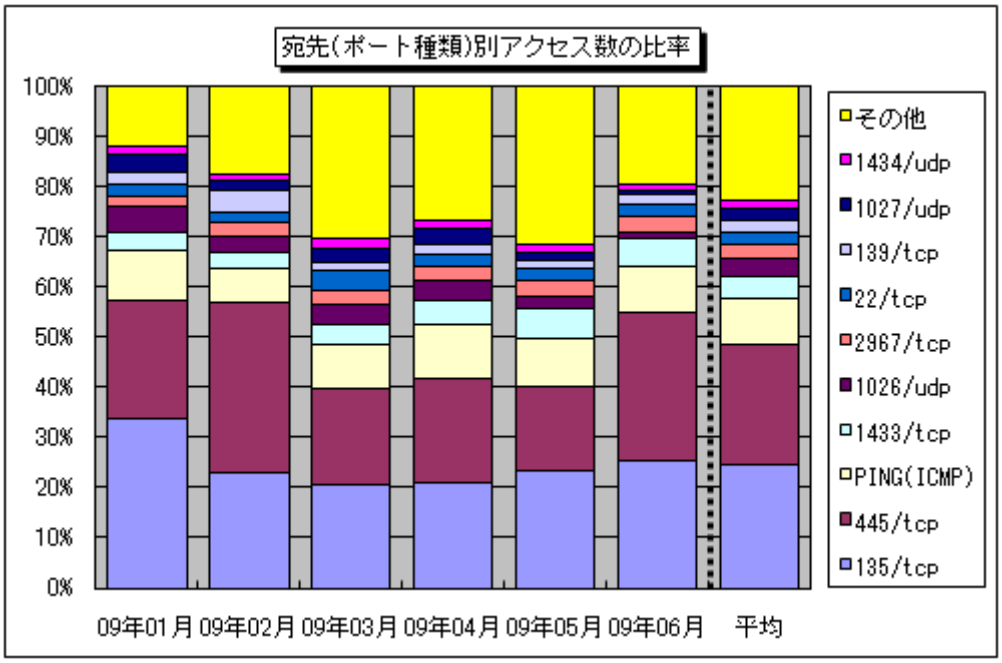


【図 2-8　2009 年 6 月の発信元地域別発信元数の比率】

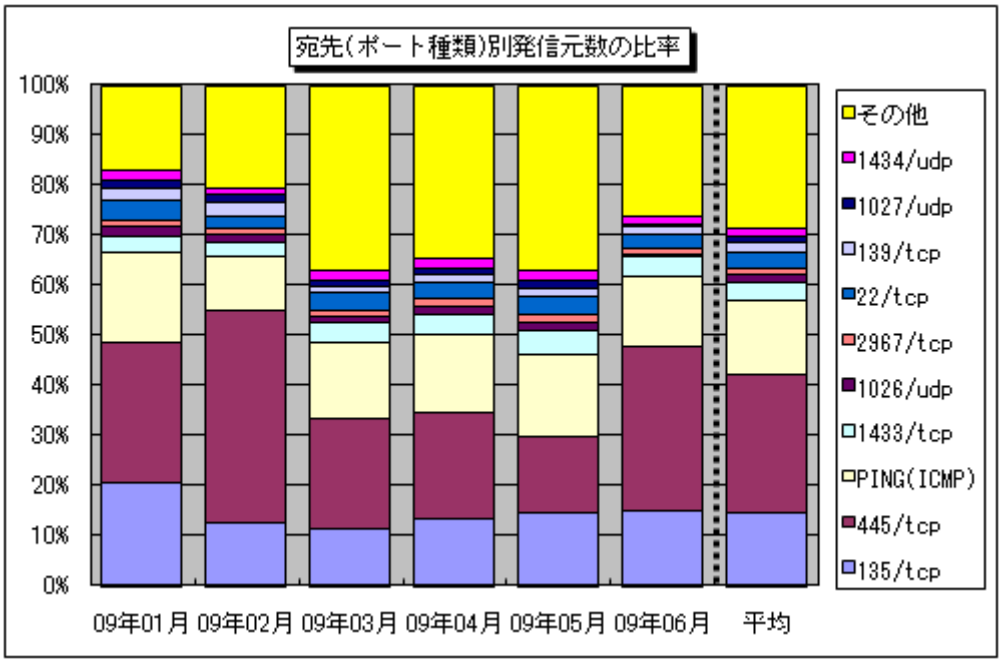
3. 統計情報

(1)宛先(ポート種類)別の比率

2009 年 1 月～2009 年 6 月の宛先(ポート種類)別アクセス数の比率を図 3-1 に、宛先(ポート種類)別発信元数の比率を図 3-2 に示します。



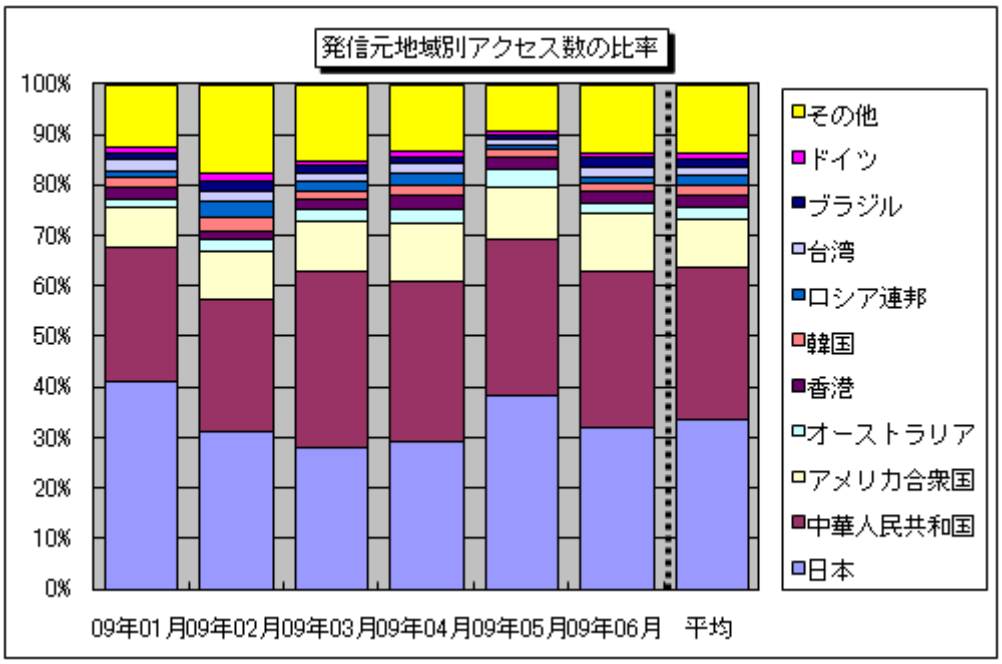
【図 3-1　2009 年 1 月～2009 年 6 月の宛先(ポート種類)別アクセス数の比率】



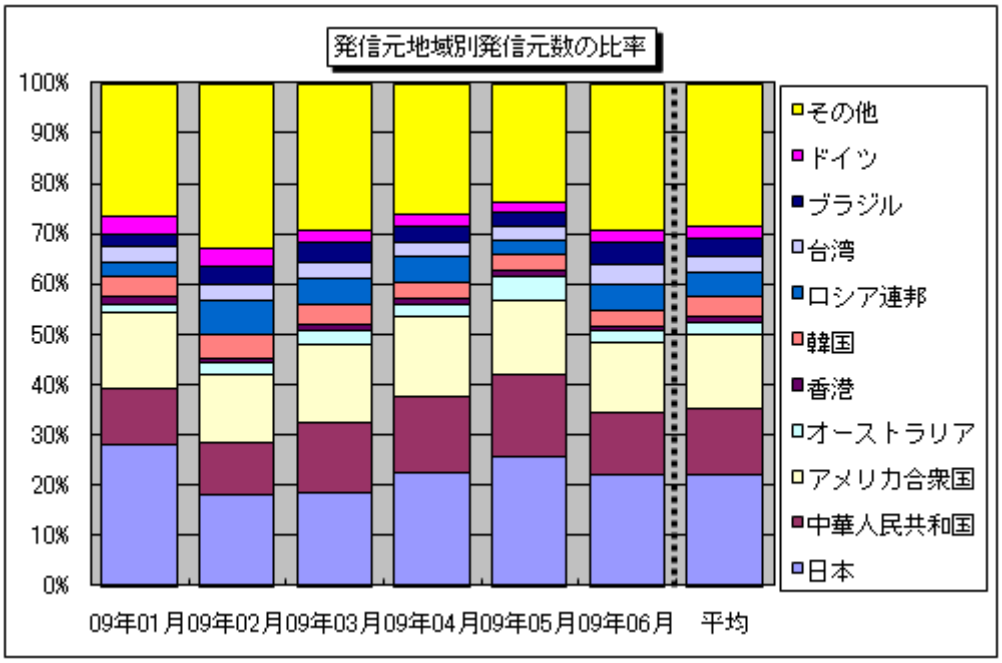
【図 3-2　2009 年 1 月～2009 年 6 月の宛先(ポート種類)別発信元数の比率】

(2)発信元地域別の比率

2009 年 1 月～2009 年 6 月の発信元地域別アクセス数の比率を図 3-3 に、発信元地域別発信元数の比率を図 3-4 に示します。



【図 3-3　2009 年 1 月～2009 年 6 月の発信元地域別アクセス数の比率】



【図 3-4　2009 年 1 月～2009 年 6 月の発信元地域別発信元数の比率】

4. 補足説明

以下に、2009 年 6 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)を狙ったアクセスである可能性が高い。
23/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、telnet を狙ったアクセスである可能性が高い。
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。
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)。また、Windows の脆弱性(MS08-067)を悪用するワームが狙う可能性の高いポートでもある(W32/Downad など)。
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。
4899/tcp	リモート操作を行うための RAdmin の脆弱性を狙った不正アクセスが有名(RAdmin は複数のコンピュータを遠隔操作するためのアプリケーション)。

■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