別紙 3

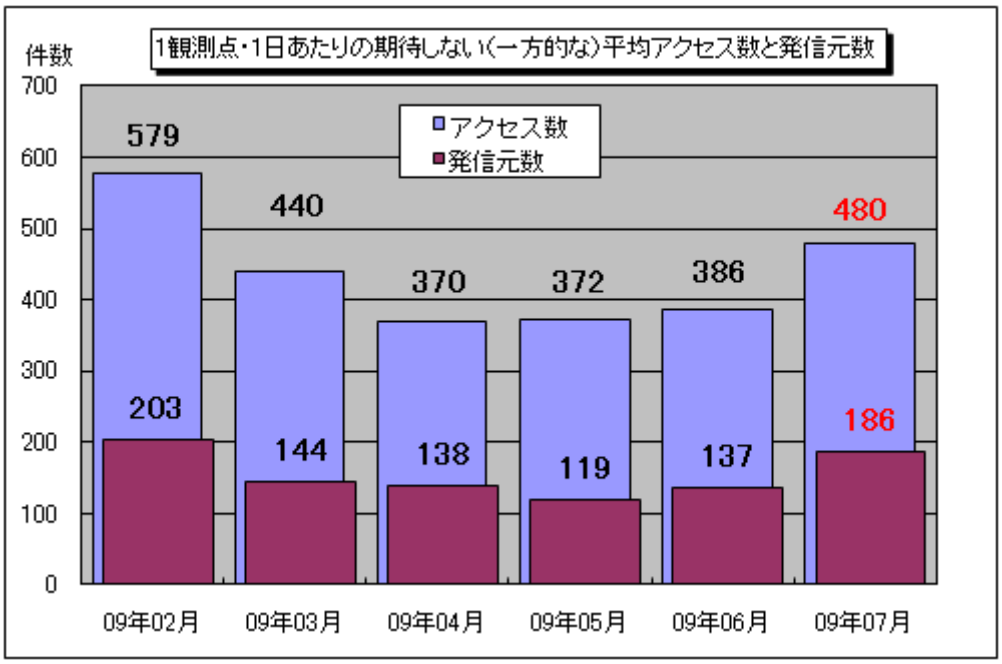
インターネット定点観測（TALOT2）での観測状況について

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 7 月の期待しない（一方的な）アクセスの総数は 10 観測点で **148,935 件**、総発信元（※）は **57,687 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 186 の発信元から 480 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。



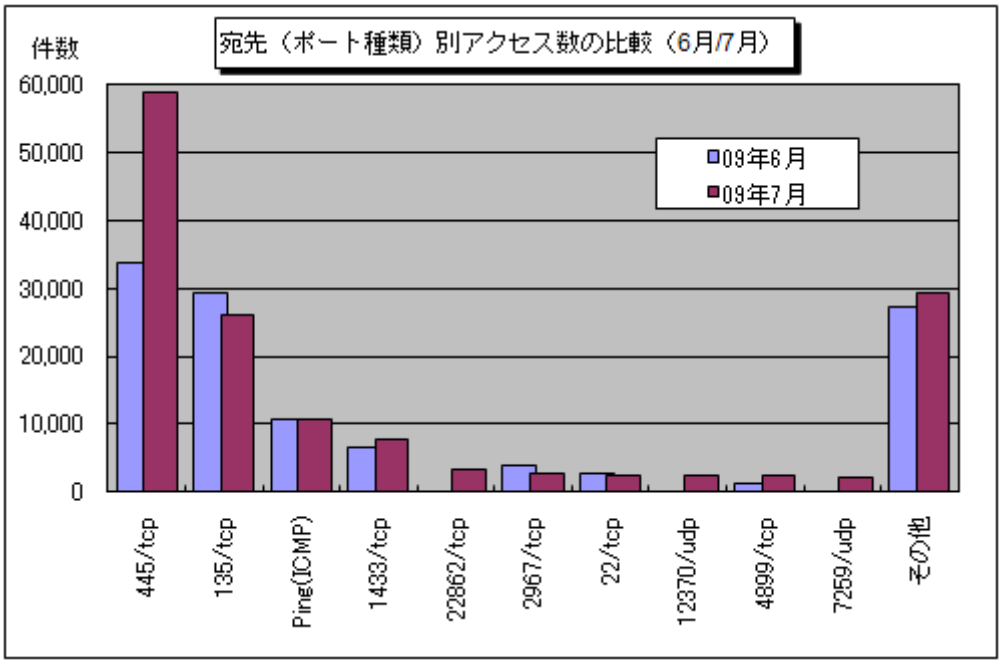
【図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009 年 2 月～2009 年 7 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。7 月の期待しない（一方的な）アクセスは、6 月と比べて増加しました。

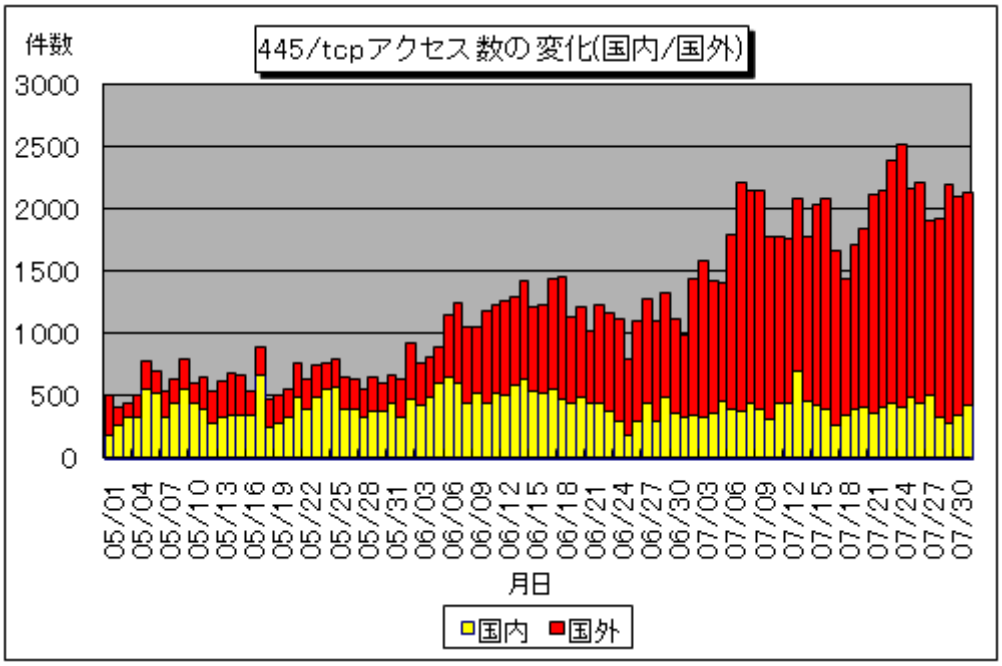
6 月と 7 月の宛先（ポート種類）別アクセス数の比較を図 1-2 に示します。

7 月は 6 月に増加した 445/tcp へのアクセスがさらに増加していました。6 月にアクセス数が増加したのは、国外からのアクセスが増加したためでしたが、7 月も継続して国外からのアクセスが増加していました（図 1-3 参照）。その原因については特定できておりませんが、6 月同様、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さらに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、6 月は全く観測されなかったポートへのアクセスが、複数のポート（22862/tcp、12370/udp、7259/udp など）で観測されました。これらのポートへ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、いずれも特定の 1 観測点のみで観測されたアクセスでした。



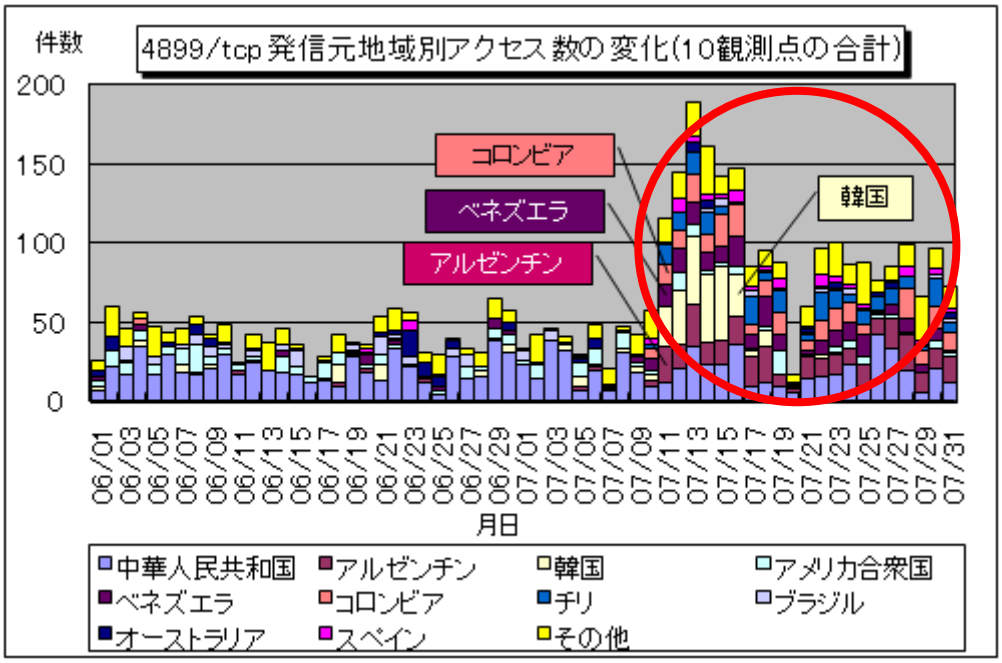
【図 1-2：宛先（ポート種類）別アクセス数の比較（6 月/7 月）】



【図 1-3：445/tcp のアクセス数の変化（国内/国外）】

2. 4899/tcp へのアクセス

7 月の中頃に、一時的に 4899/tcp へのアクセスが増加した期間がありました。これは、韓国の 1 つの発信元からのアクセスと、アルゼンチン、ベネズエラ、コロンビアなどの南米地域の多数の発信元からのアクセスが増加したためです（図 2-1 参照）。



【図 2-1：4899/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】

南米地域の発信元からの 4899/tcp へのアクセスの増加は、定点観測を行っている他の組織でも観測されており、広い範囲で同様の事象が発生している可能性があります。

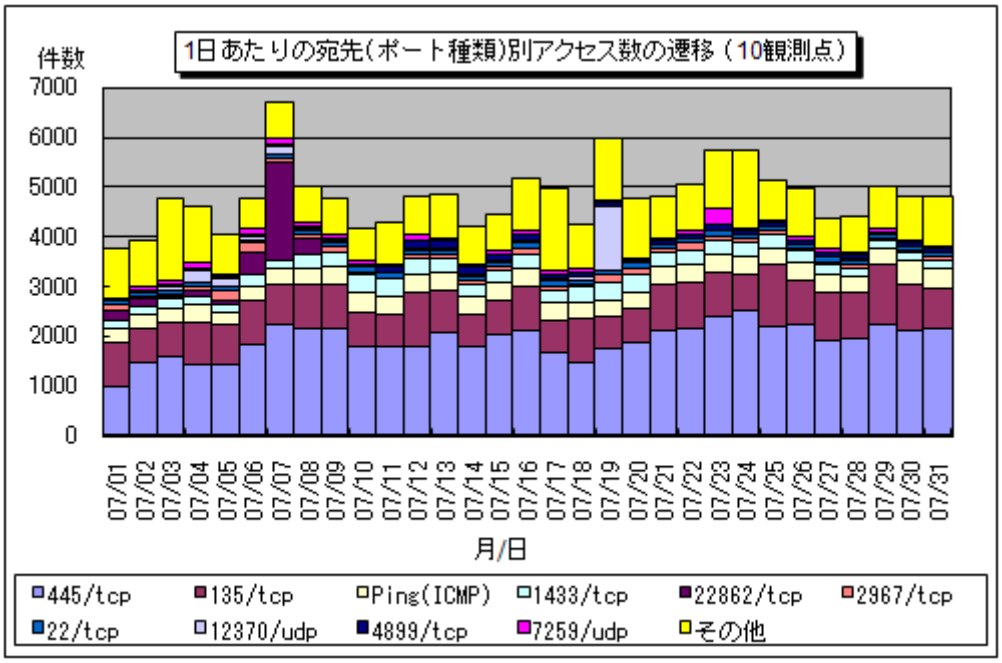
4899/tcp は、Famatech 社のリモートコントロールソフトウェア Radmin が使用するポートとして知られています。

Radmin の利用者は、4899/tcp に対して、接続を許可していない発信元からのアクセスが来ていないかを確認し、状況に応じてアクセス制限（接続を許可する IP アドレスの範囲を絞るなど）や、接続認証の強化を行ってください。

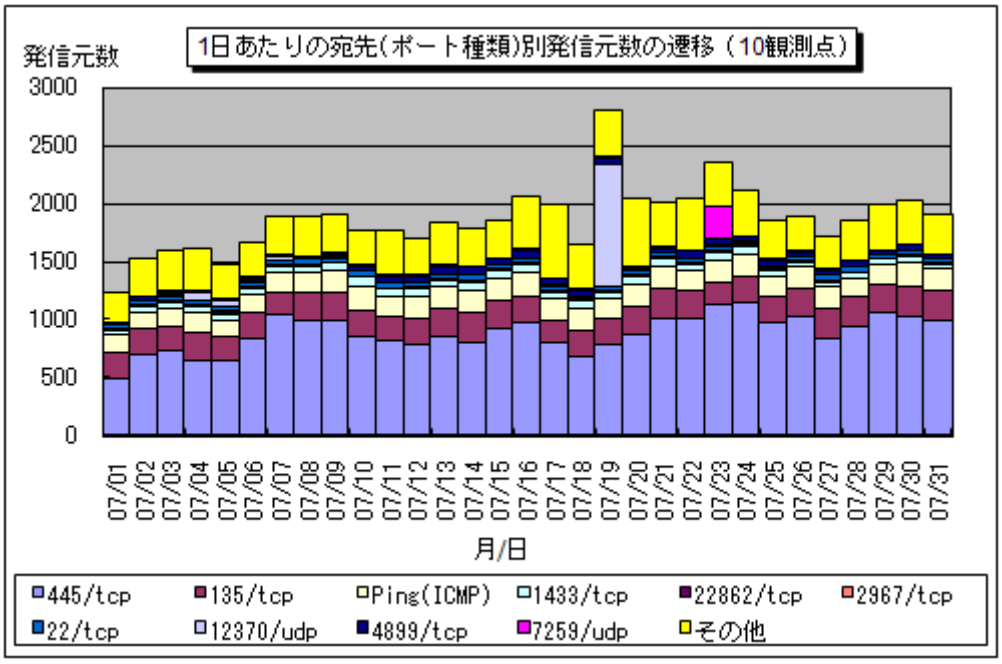
3. 2009 年 7 月の一方的なアクセス状況

（1） 宛先（ポート種類）別のアクセス状況

2009 年 7 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。



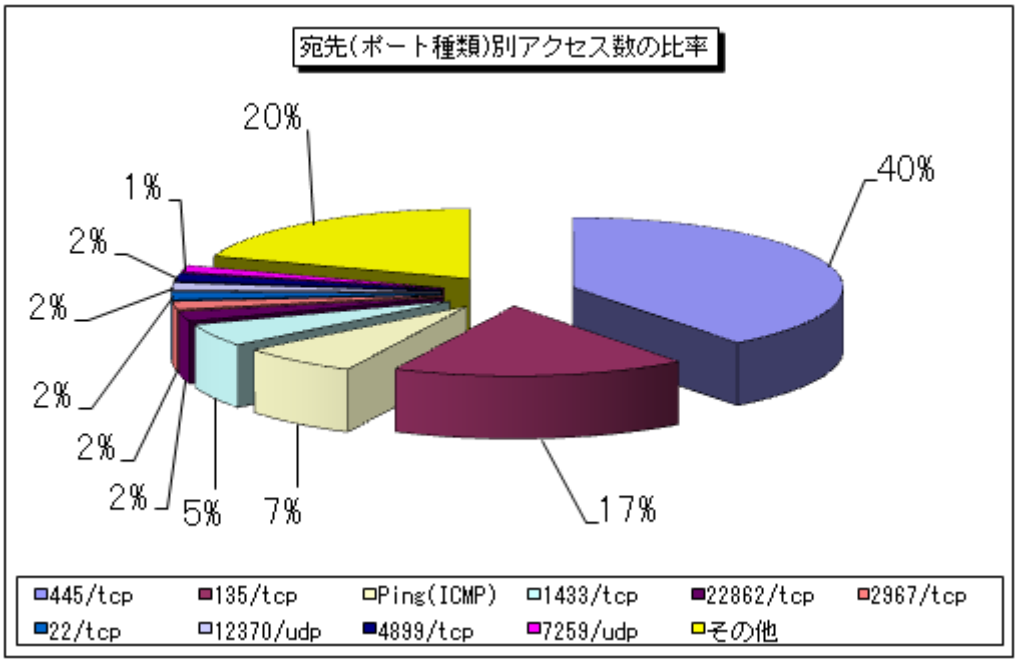
【図 3-1：2009 年 7 月の 1 日あたりの宛先（ポート種類）別アクセス数の遷移】



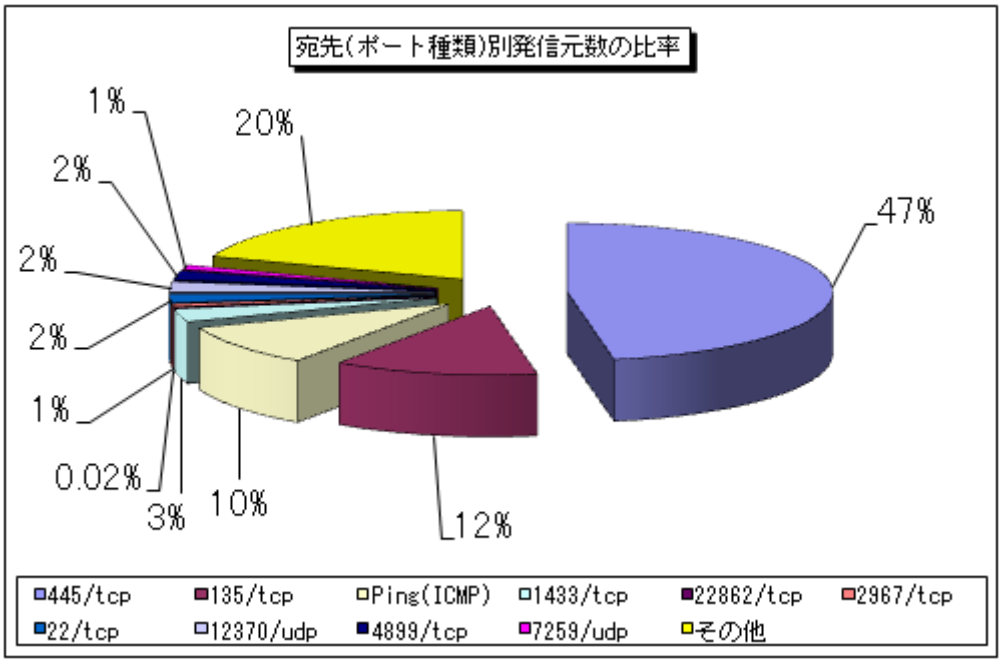
【図 3-2：2009 年 7 月の 1 日あたりの宛先（ポート種類）別発信元数の遷移】

（2）宛先（ポート種類）別の比率

2009 年 7 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。



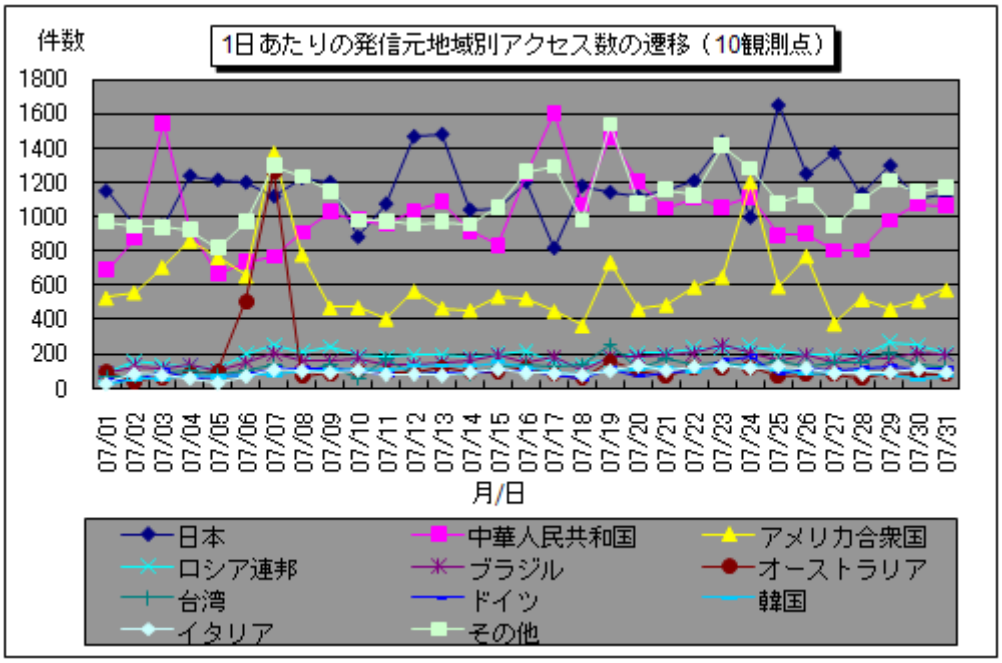
【図 3-3：2009 年 7 月の宛先（ポート種類）別アクセス数の比率】



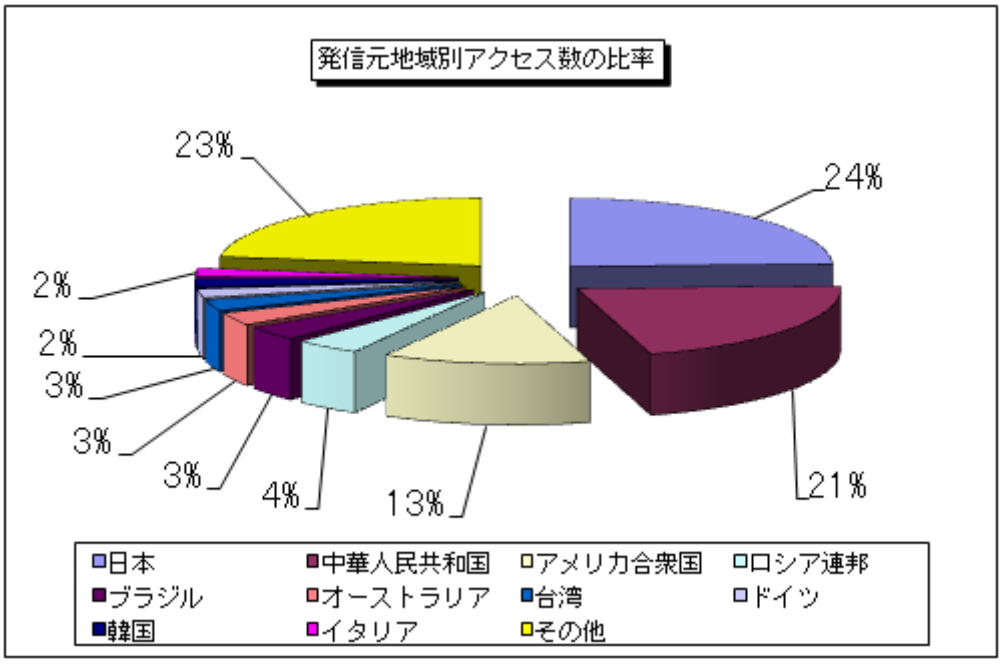
【図 3-4：2009 年 7 月の宛先（ポート種類）別発信元数の比率】

（3）発信元地域別のアクセス状況

2009 年 7 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。

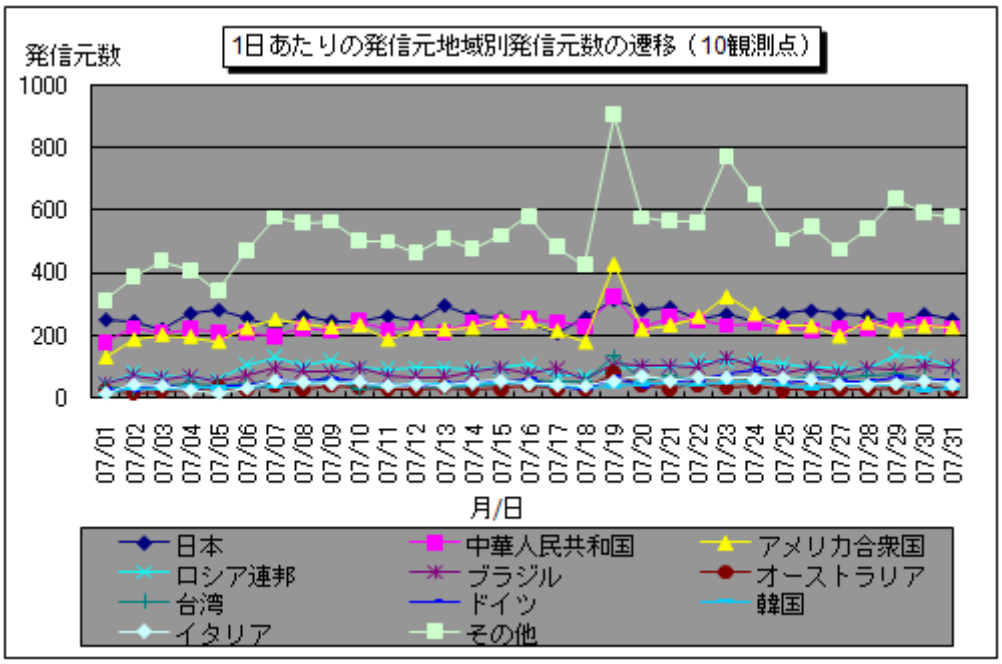


【図 3-5：2009 年 7 月の 1 日あたりの発信元地域別アクセス数の遷移】

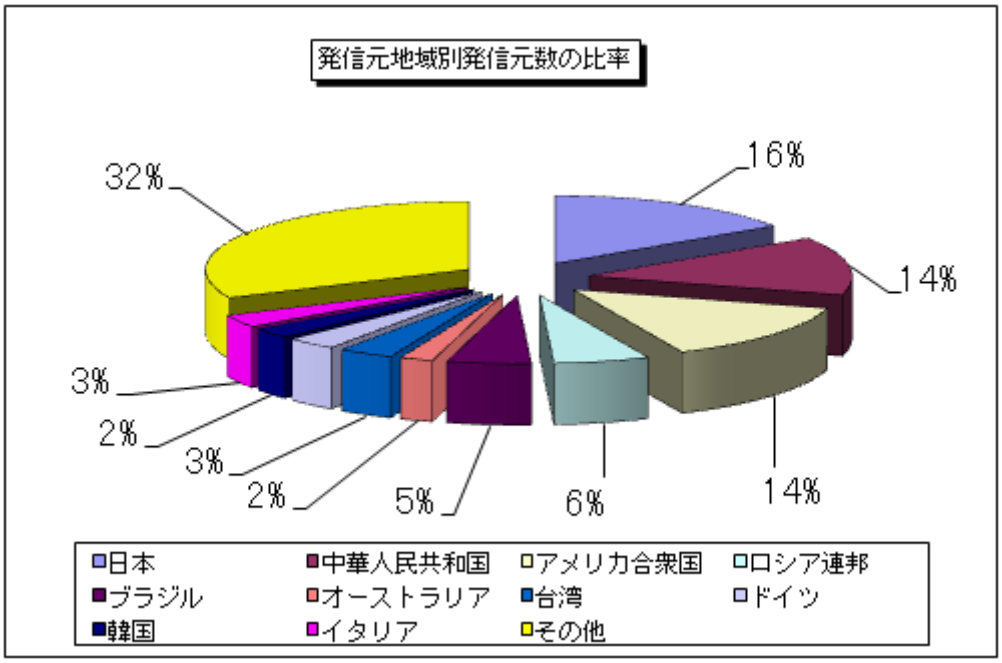


【図 3-6：2009 年 7 月の発信元地域別アクセス数の比率】

2009 年 7 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 7 月の 1 日あたりの発信元地域別発信元数の遷移】

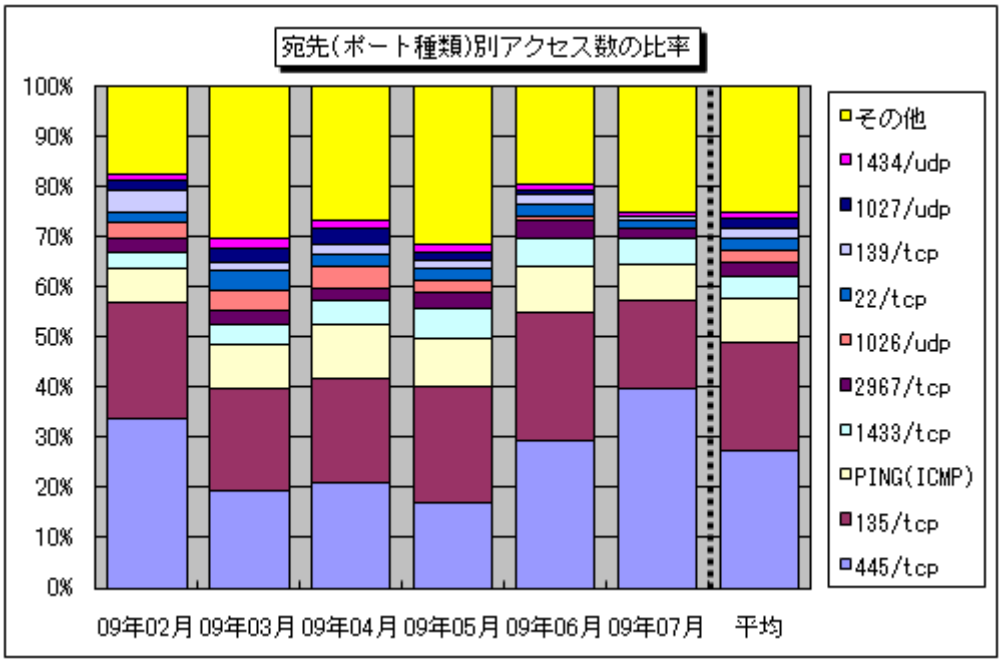


【図 3-8：2009 年 7 月の発信元地域別発信元数の比率】

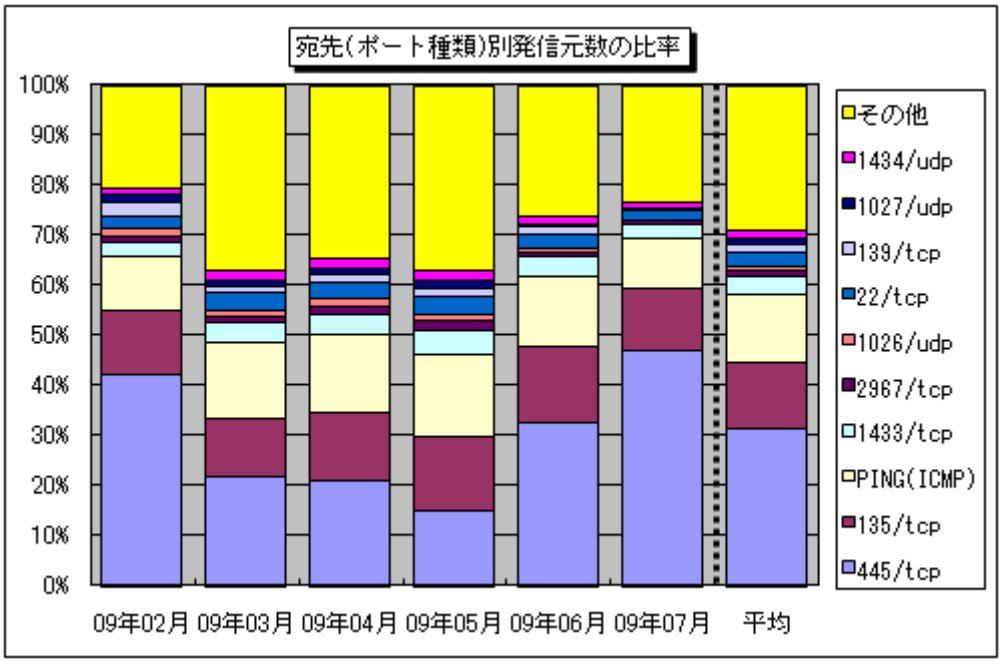
4. 統計情報

（1）宛先（ポート種類）別の比率

2009 年 2 月～2009 年 7 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。



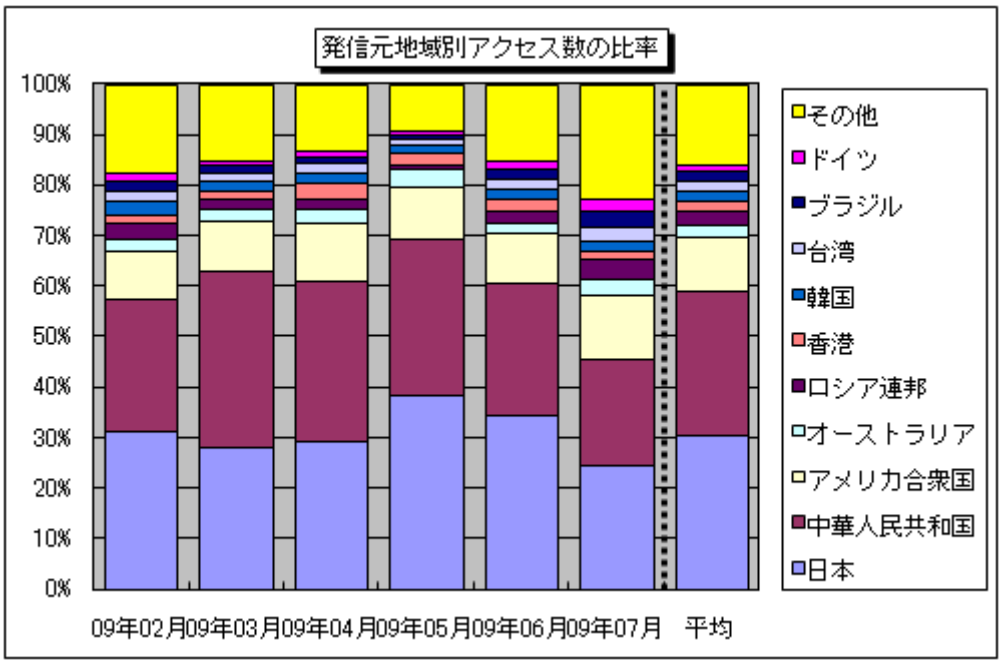
【図 4-1：2009 年 2 月～2009 年 7 月の宛先（ポート種類）別アクセス数の比率】



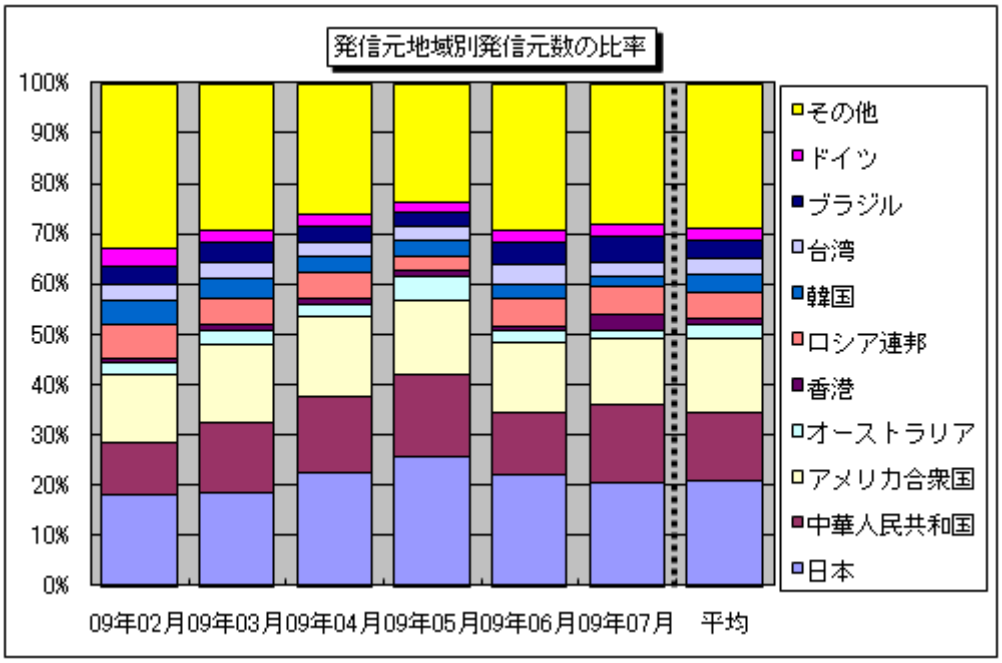
【図 4-2：2009 年 2 月～2009 年 7 月の宛先（ポート種類）別発信元数の比率】

（2）発信元地域別の比率

2009 年 2 月～2009 年 7 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 4-3：2009 年 2 月～2009 年 7 月の発信元地域別アクセス数の比率】



【図 4-4：2009 年 2 月～2009 年 7 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 7 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。
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）。
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。
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）。
7259/udp	多数の発信元から 1 観測点のみに観測された、原因不明のアクセス。
12370/udp	多数の発信元から 1 観測点のみに観測された、原因不明のアクセス。
22862/tcp	特定の少数の発信元から 1 観測点のみに観測された、原因不明のアクセス。

■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