別紙 3

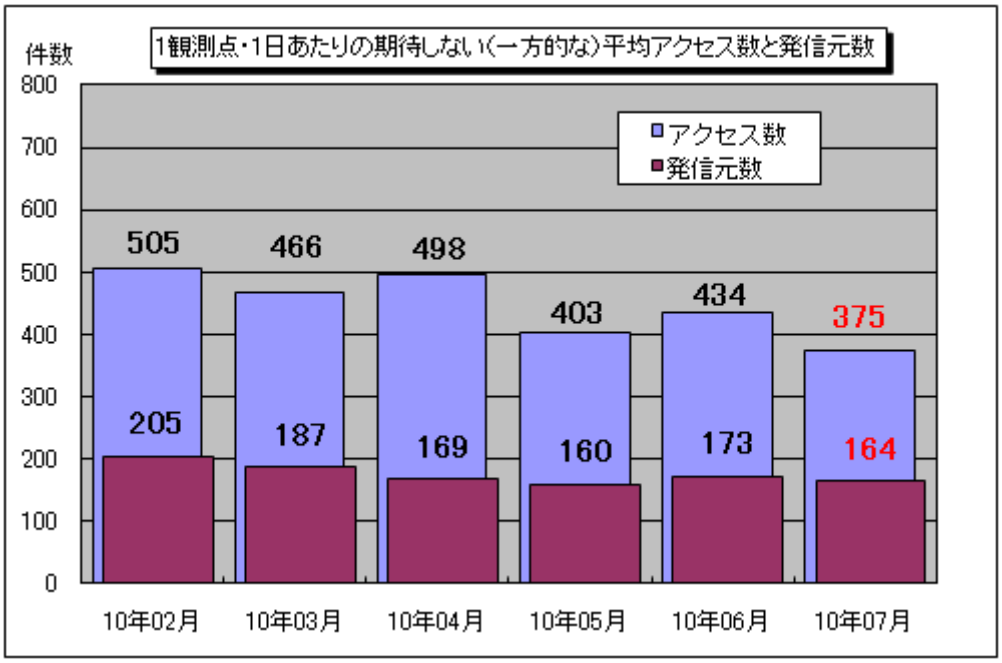
インターネット定点観測（TALOT2）での観測状況について

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、2010 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 **116,141 件**、延べ発信元数※は **50,845 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 164 の発信元から 375 件のアクセスがあった**ことになります（図 1-1 参照）。

※ 延べ発信元数：TALOT2 の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、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は、発信元数を 1 としてカウントする。

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】

2010 年 2 月～2010 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 月と比べて減少しました。

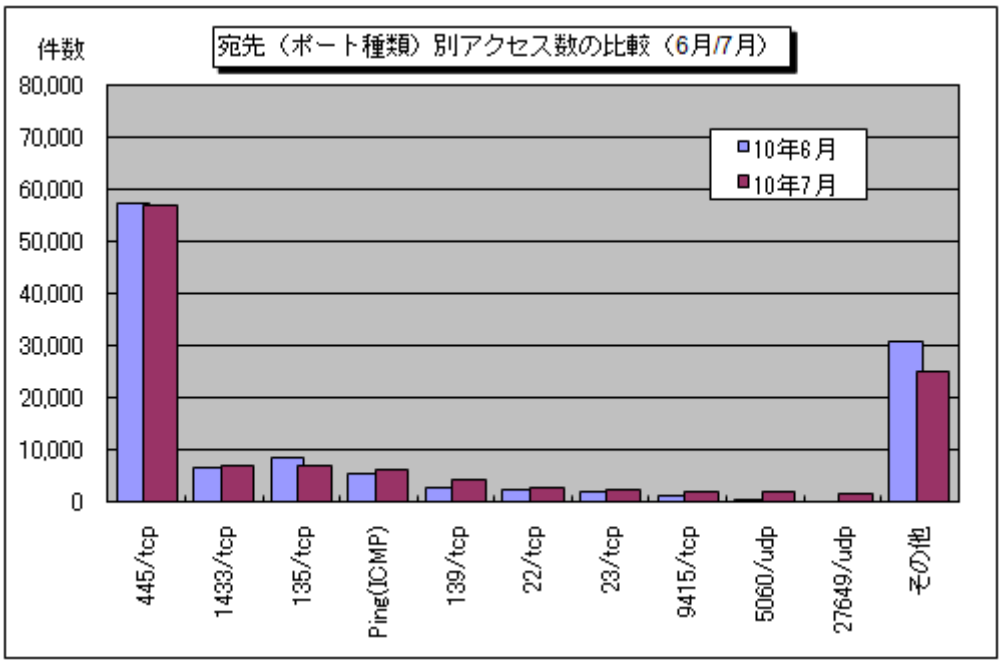
6 月と 7 月の宛先（ポート種類）別アクセス数の比較を図 1-2 に示します。これをみると、これまでは上位に挙がって来なかった 27649/udp や、5060/udp へのアクセスが上位にランクされました。

27649/udp に関しては、7 月上旬に TALOT2 の 1 つの観測点に海外の多数の発信元からのアクセスが観測されていました。このポートは特定のアプリケーションで使用されるポートというわけではなく、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。

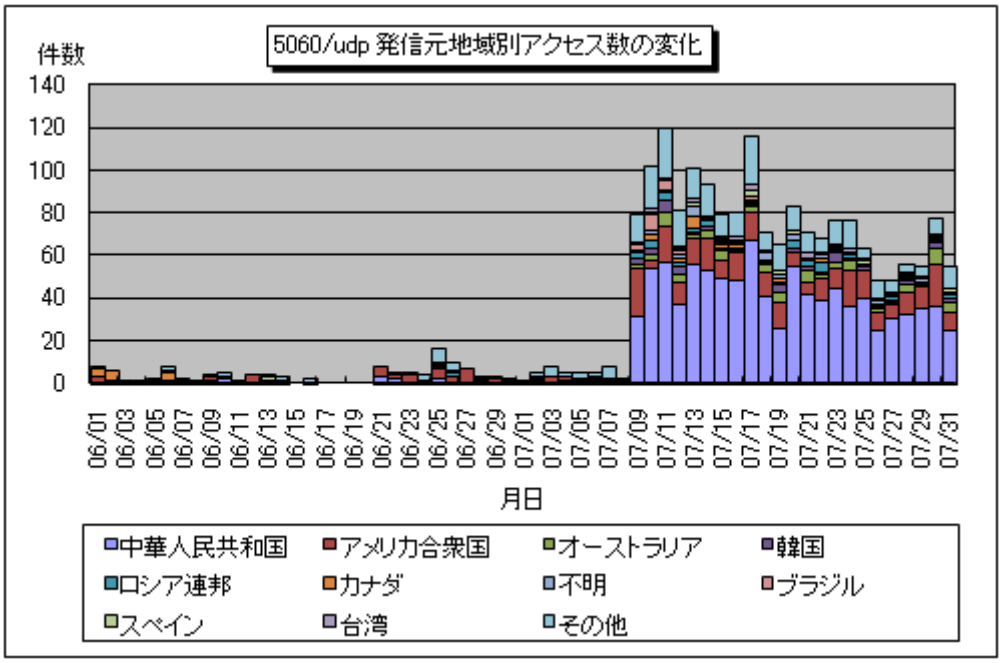
また、5060/udp に関しては、7 月 9 日から TALOT2 の複数の観測点で多く観測され始めました（図 1-3 参照）。この現象は他の定点観測を行っている組織でもほぼ同様に観測されており、広い範囲で発生していたと思われます。なお、5060/udp は一般的に SIP※サーバで利用されるポートであり、このアクセスが SIP サーバに対しての何らかの攻撃を目的としたものだった可能性があるため、SIP サーバを運用している場合は、何らかの影響を受けていないか確認してみることをお勧めします。

※SIP（Session Initiation Protocol）：IP 電話などに用いられる通信プロトコルのこと。

（ご参考）
5060/UDP に対するアクセスの増加について（警察庁）
http://www.npa.go.jp/cyberpolice/detect/pdf/20100714.pdf



【図 1-2：宛先（ポート種類）別アクセス数の比較（6 月/7 月）】

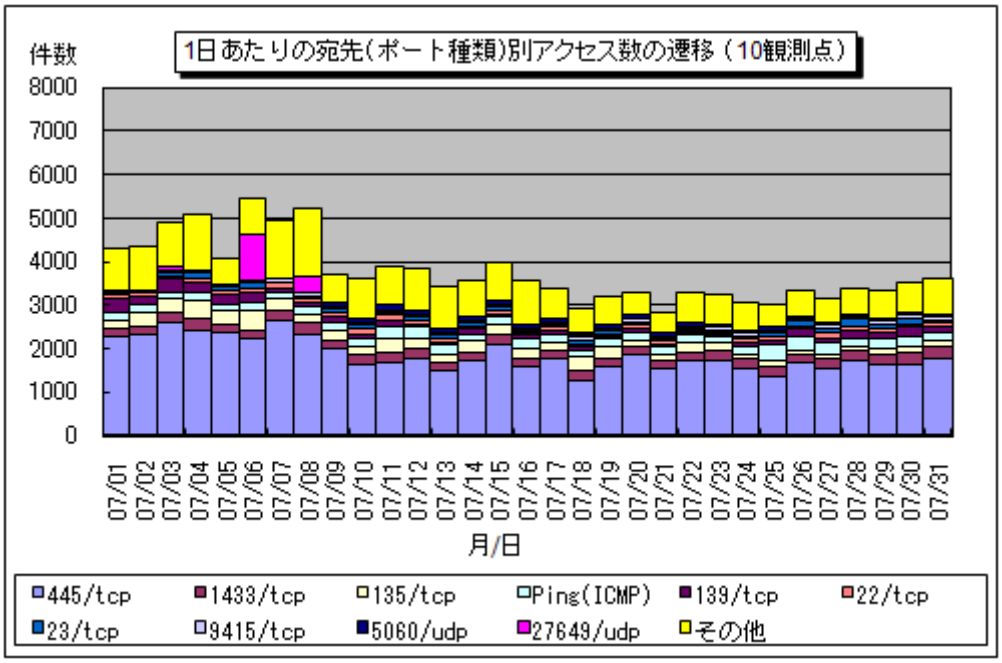


【図 1-3：5060/udp 発信元地域別アクセス数の変化】

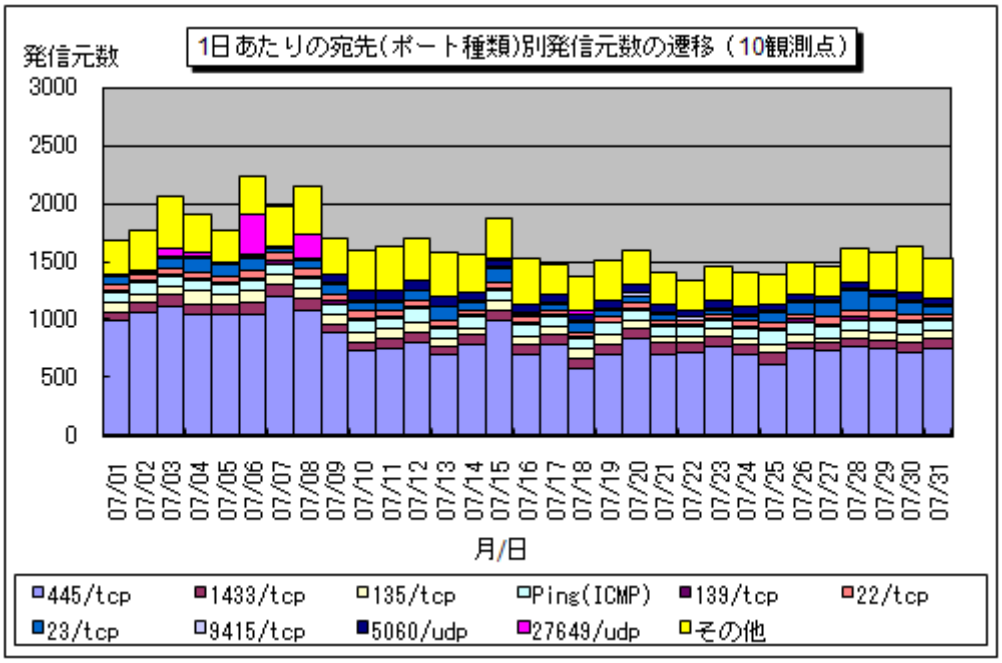
2. 2010 年 7 月の一方的なアクセス状況

（1）宛先（ポート種類）別のアクセス状況

2010 年 7 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。



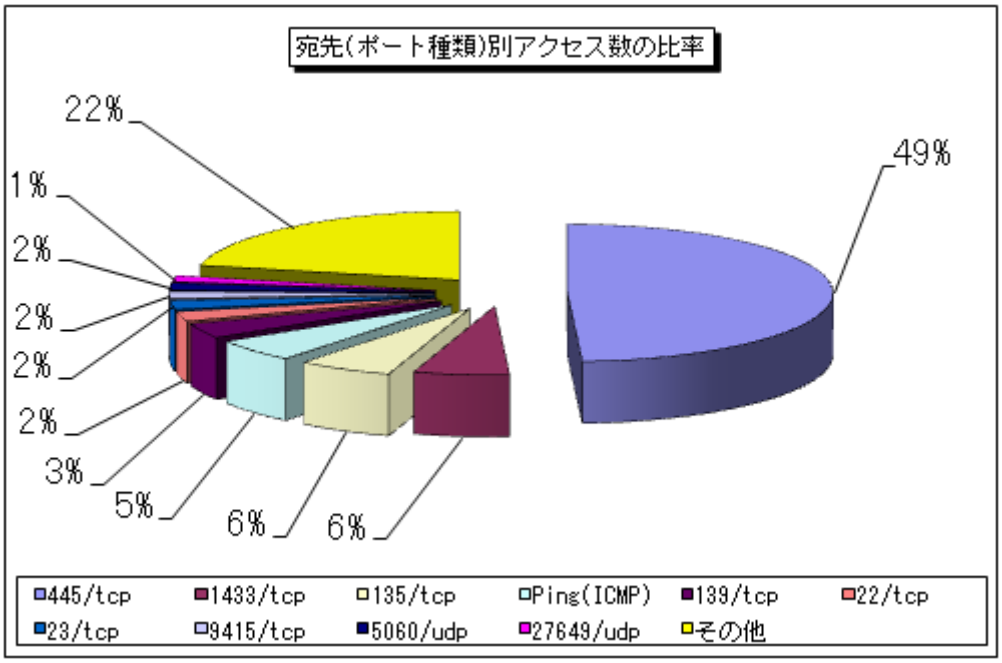
【図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移(10 観測点)】



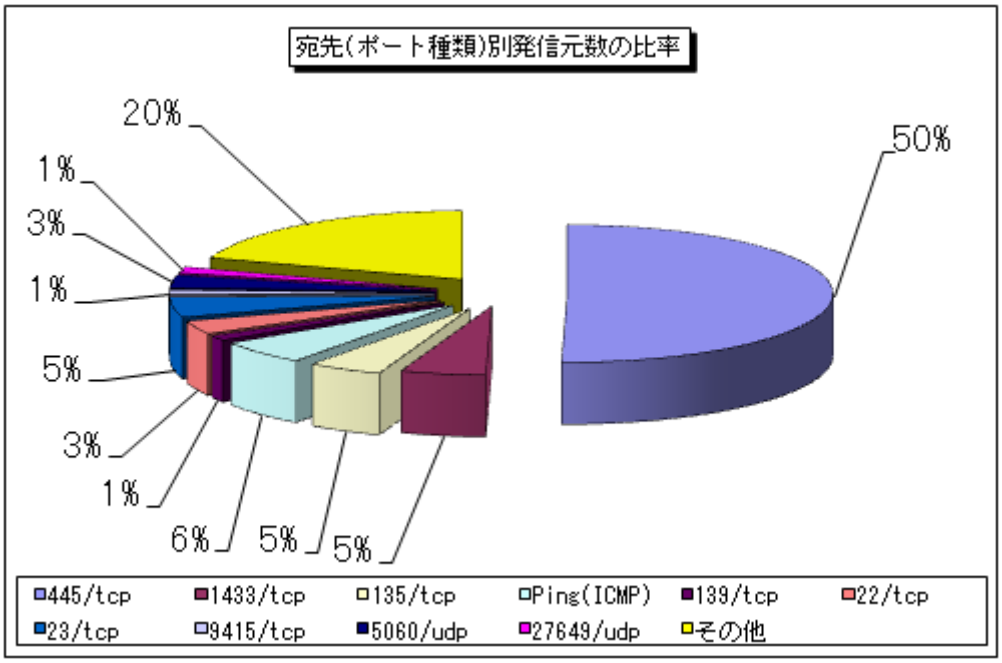
【図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）】

（2）宛先（ポート種類）別の比率

2010 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 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。



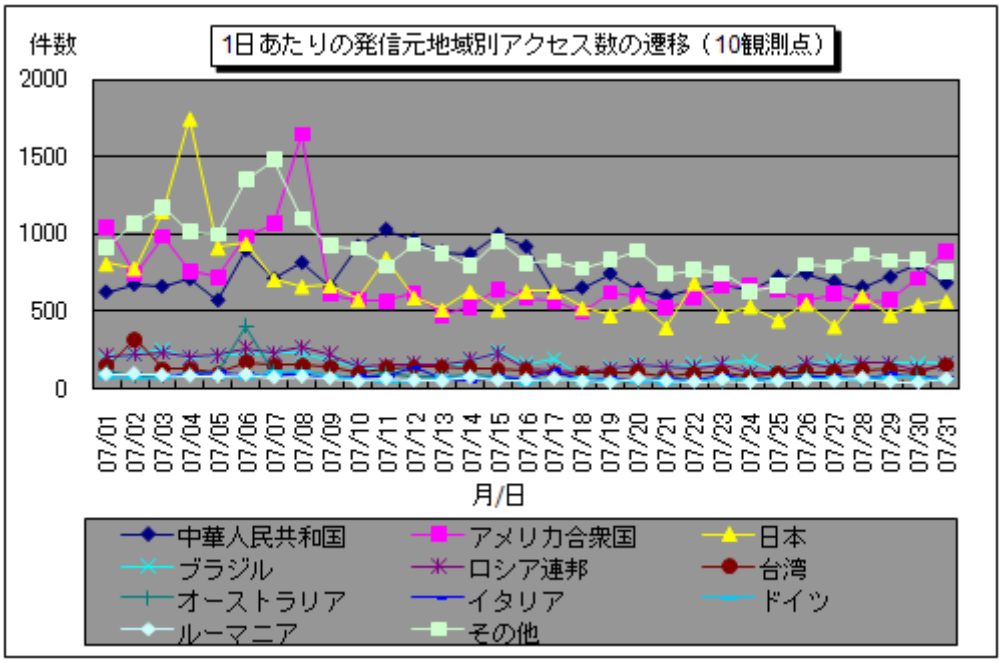
【図 2-3：宛先（ポート種類）別アクセス数の比率】



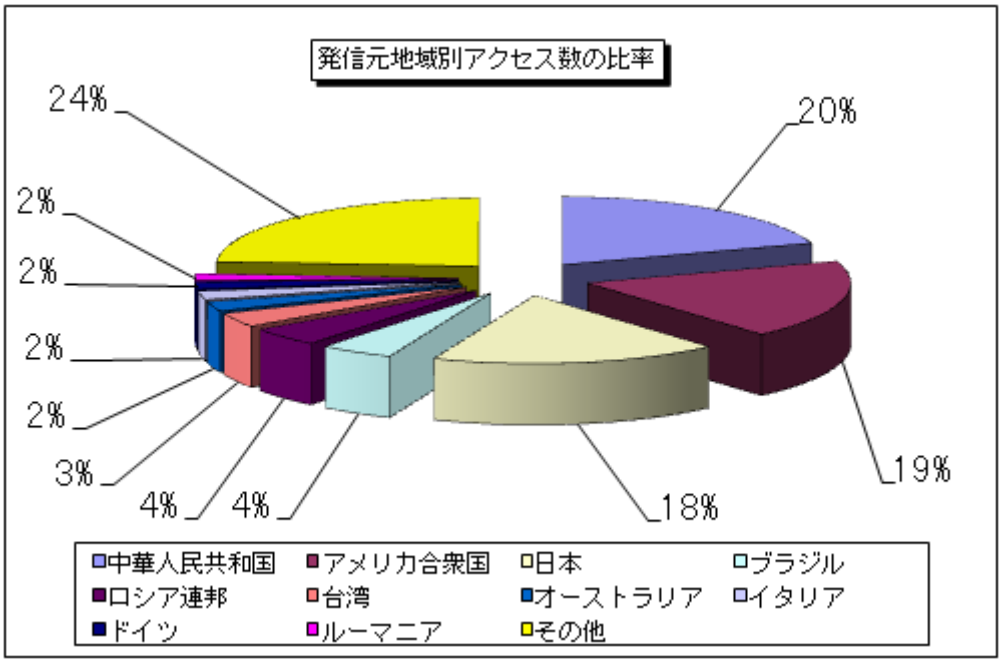
【図 2-4：宛先（ポート種類）別発信元数の比率】

（3）発信元地域別のアクセス状況

2010 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 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。

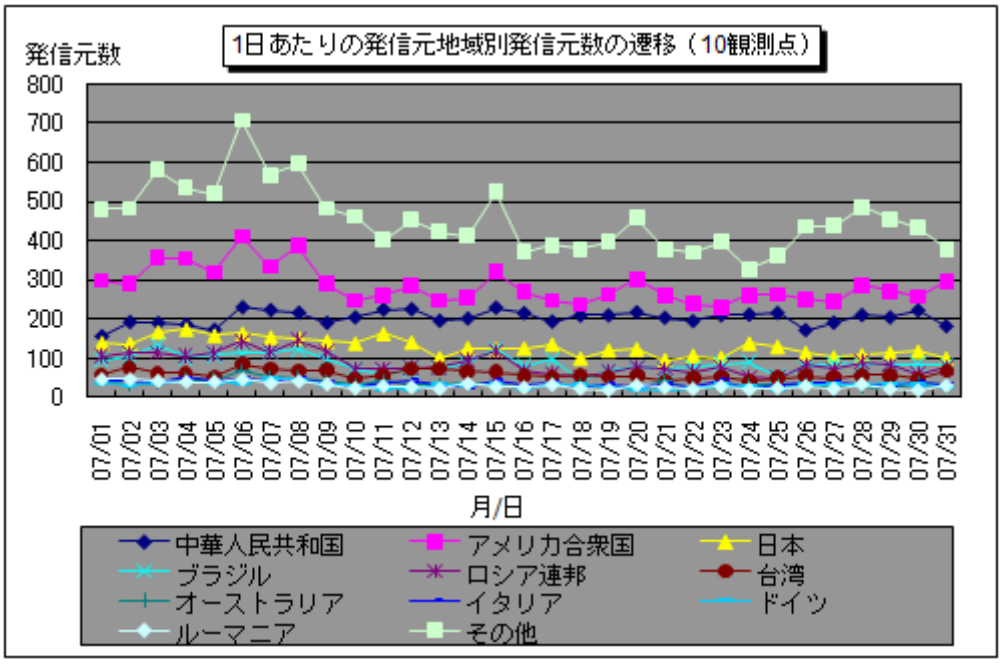


【図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）】

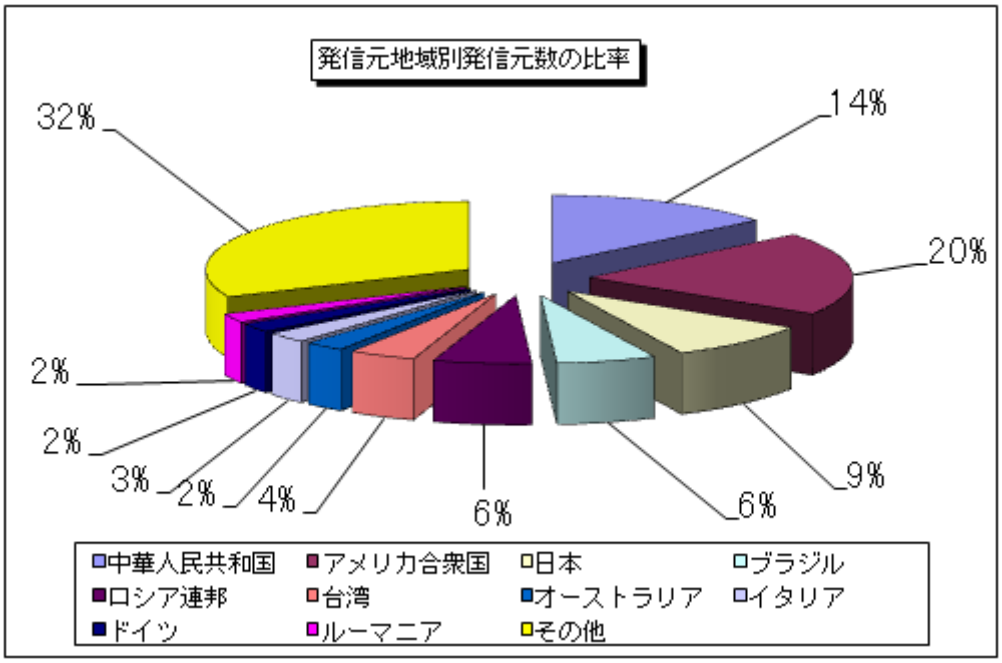


【図 2-6：発信元地域別アクセス数の比率】

2010 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 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： 1 日あたりの発信元地域別発信元数の遷移（10 観測点）】

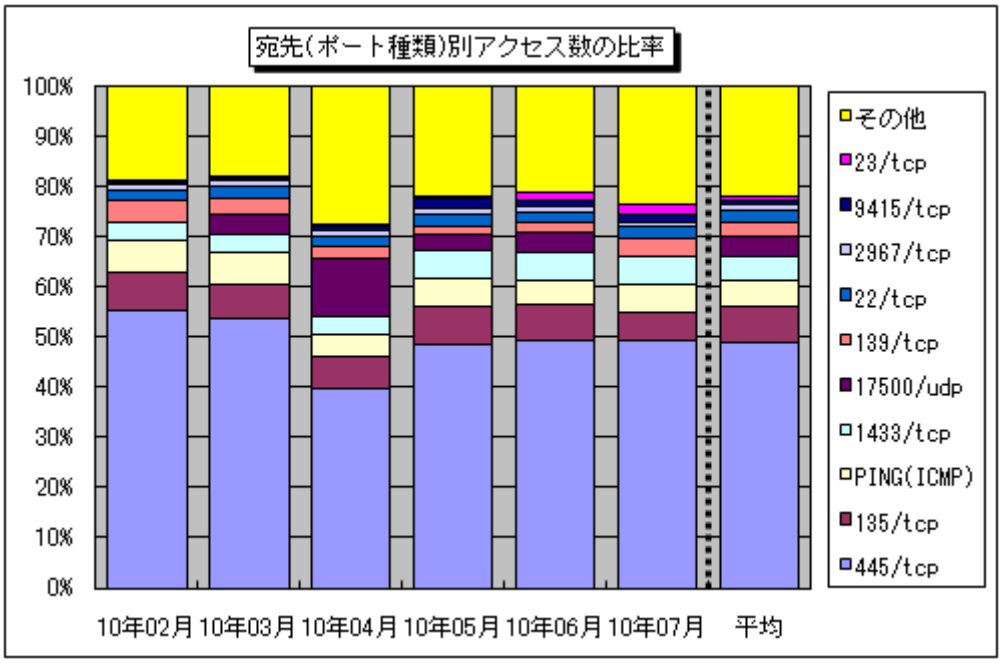


【図 2-8：発信元地域別発信元数の比率】

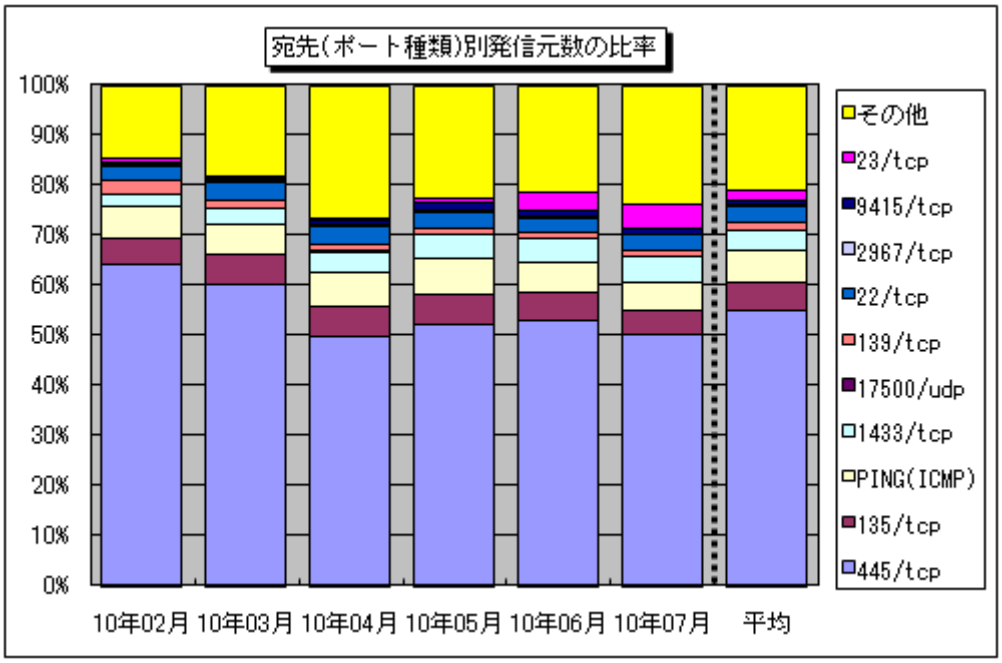
3. 統計情報

（1）宛先（ポート種類）別の比率

2010 年 2 月～2010 年 7 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。



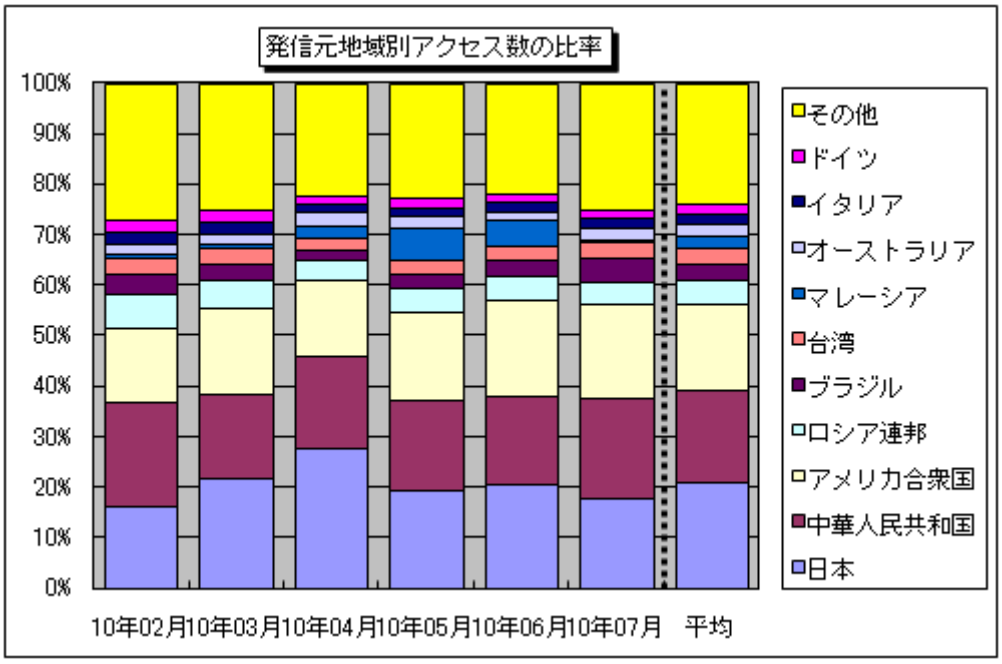
【図 3-1：宛先（ポート種類）別アクセス数の比率】



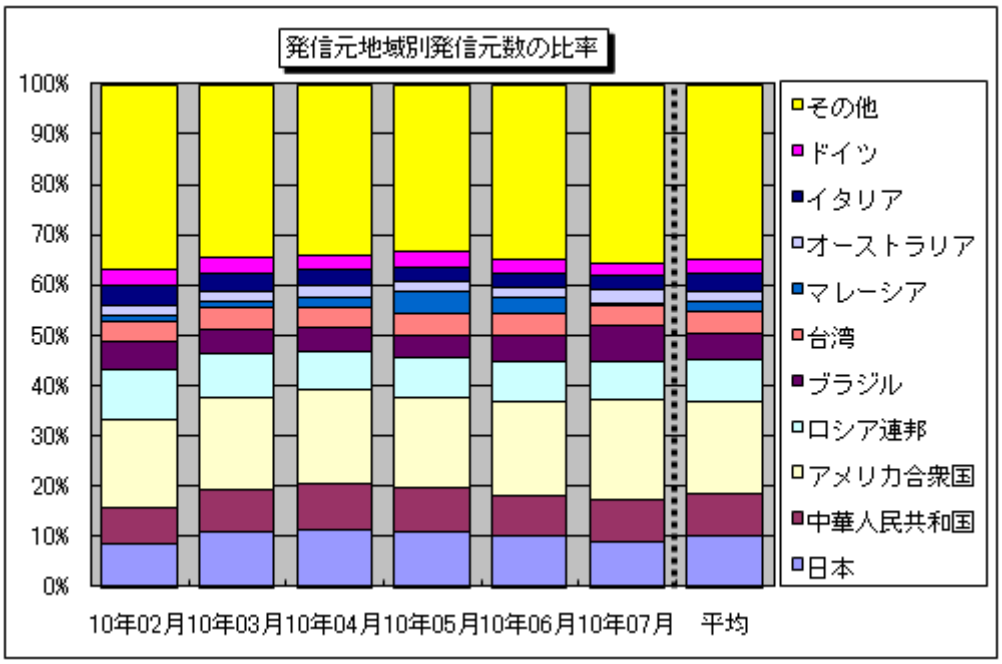
【図 3-2：宛先（ポート種類）別発信元数の比率】

（2）発信元地域別の比率

2010 年 2 月～2010 年 7 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：発信元地域別アクセス数の比率】



【図 3-4：発信元地域別発信元数の比率】

4. 補足説明

以下に、2010 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
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、このポートへのアクセスは、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）。
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。
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 Windows の脆弱性を狙ったアクセスである可能性が高い。
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。
9415/tcp	海外（主に中国）の複数の発信元から TALOT2 の複数の観測点で観測された目的不明のアクセス。
5060/udp	7 月 9 日から TALOT2 の複数の観測点で多く観測され始めた、海外の複数の発信元からのアクセス。SIP サーバを狙った何らかのアクセスである可能性がある。
27649/udp	7 月上旬に TALOT2 の 1 つの観測点に海外の多数の発信元からのアクセスの急増が観測された、目的不明のアクセス。

■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