

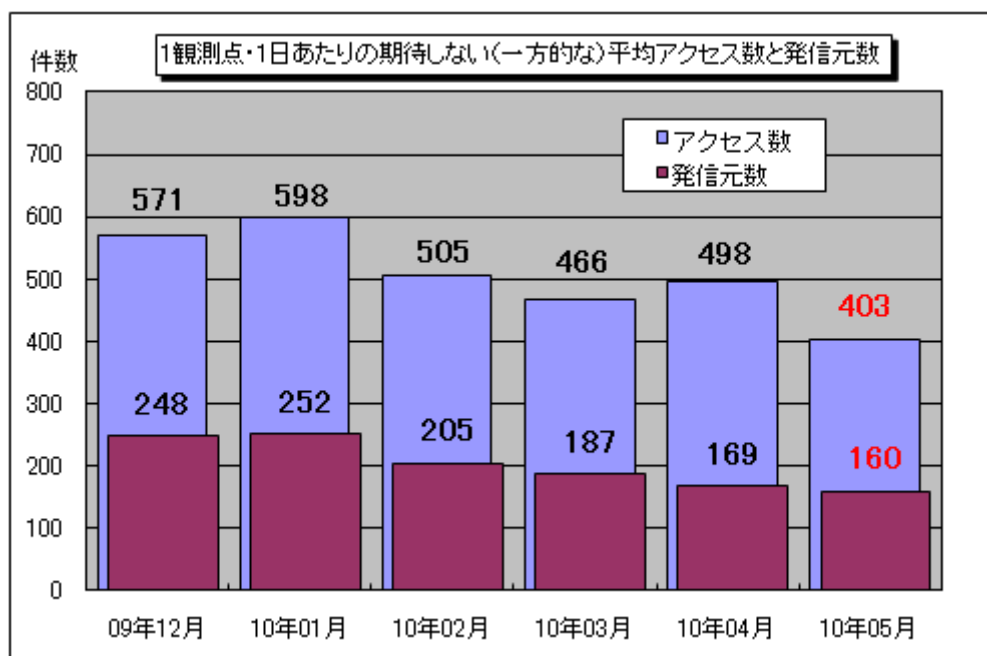
インターネット定点観測（TALOT2）での観測状況について

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5月の期待しない（一方的な）アクセスの総数は10観測点で125,020件、延べ発信元数^(※)は49,574箇所ありました。平均すると、1観測点につき1日あたり160の発信元から403件のアクセスがあったこととなります（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向的アクセスがあると考えられます。



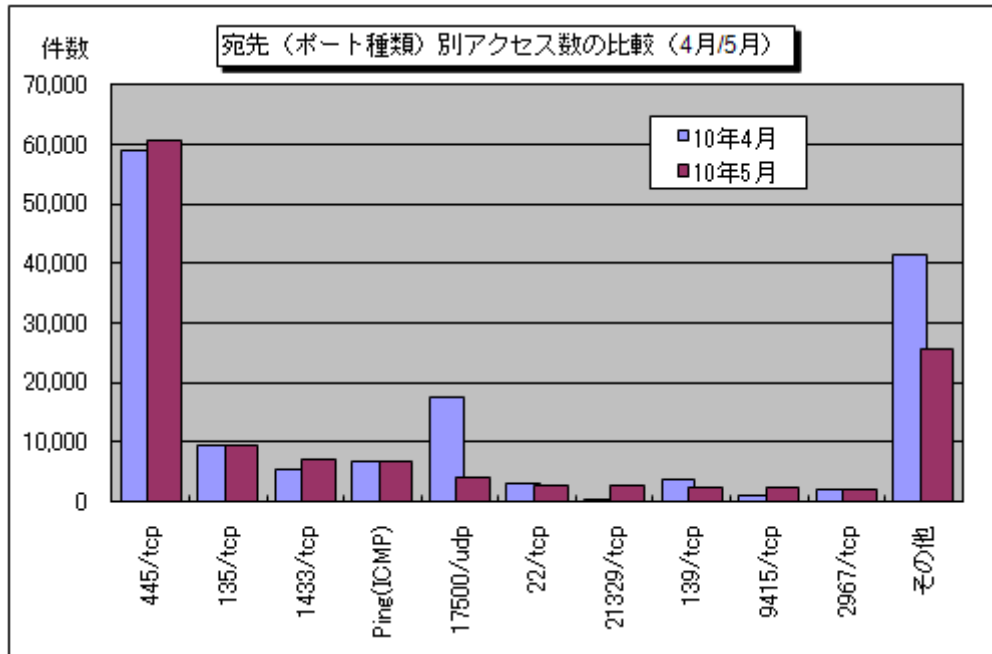
【図1-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009年12月～2010年5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。5月の期待しない（一方的な）アクセスは、4月と比べて減少しました。

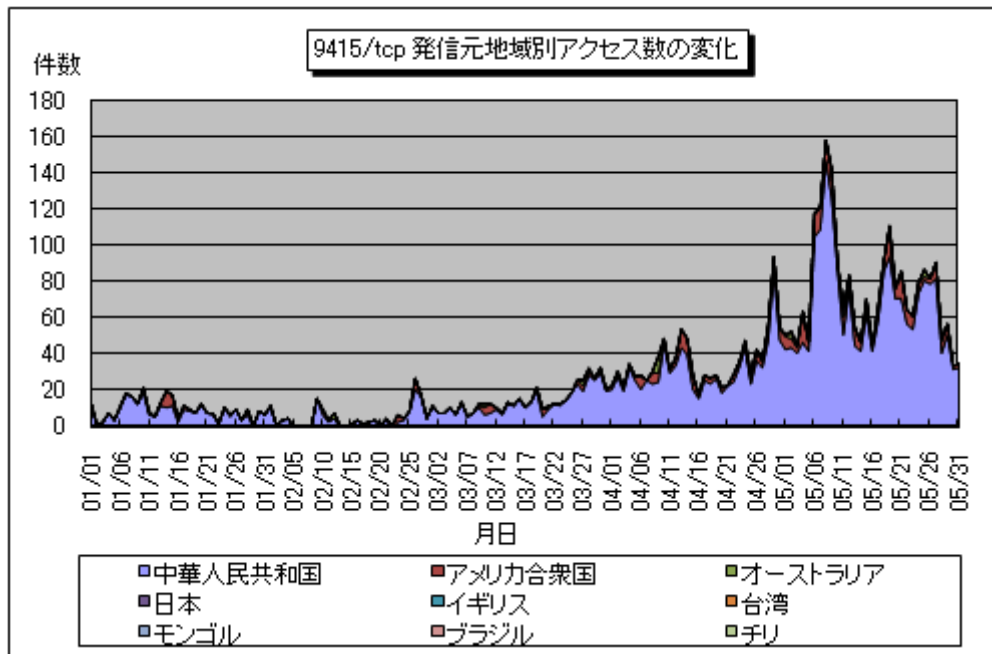
4月と5月の宛先（ポート種類）別アクセス数の比較を図1-2に示します。これをみると、5月はこれまであまり上位に挙がってこなかった9415/tcpや、21329/tcpといったポートへのアクセスが上位にランクされました。これらのポートはいずれも、特定のアプリケーションで使用されるポートというわけではないため、このアクセスが何を目的としたものだったかは不明です。

9415/tcpに関しては、TALOT2の複数の観測点に対して海外（主に中国）の複数の発信元からのアクセスの増加傾向が3月頃から継続していたといった特徴がありました（図1-3参照）。定点観測を行っている他の組織においても同様の増加傾向が観測されていたことから、広範囲に発生していたことが予想されるため、引き続き観測状況に注意する必要があります。

21329/tcpに関しては、5月の中旬にアメリカ合衆国の1か所の発信元からTALOT2の1つの観測点のみにアクセスの急増が観測されていました。



【図 1-2 : 宛先 (ポート種類) 別アクセス数の比較 (4月/5月)】

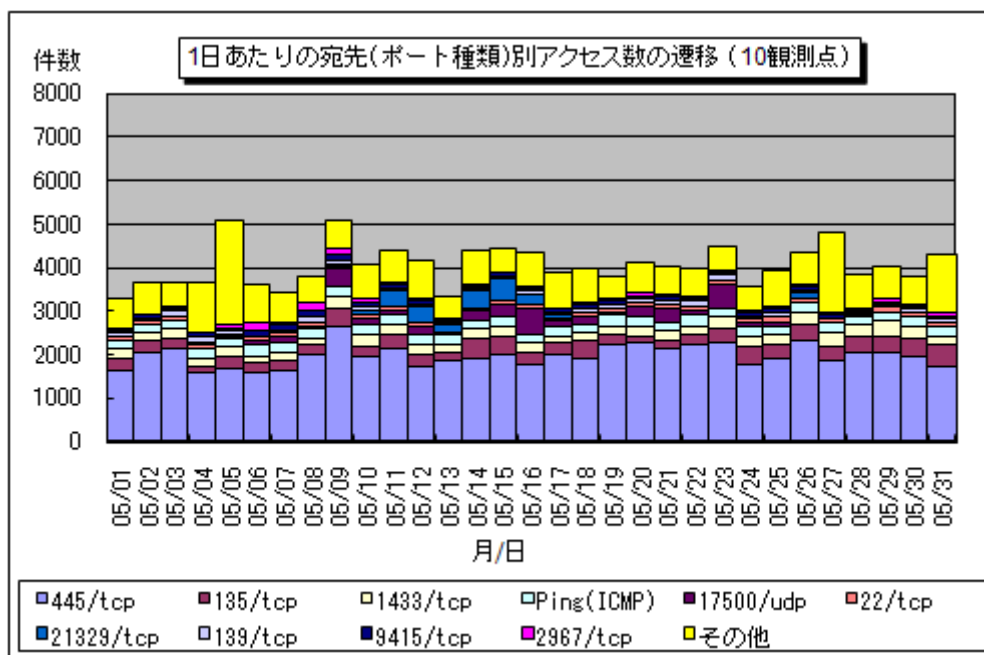


【図 1-3 : 9415/tcp 発信元地域別アクセス数の変化】

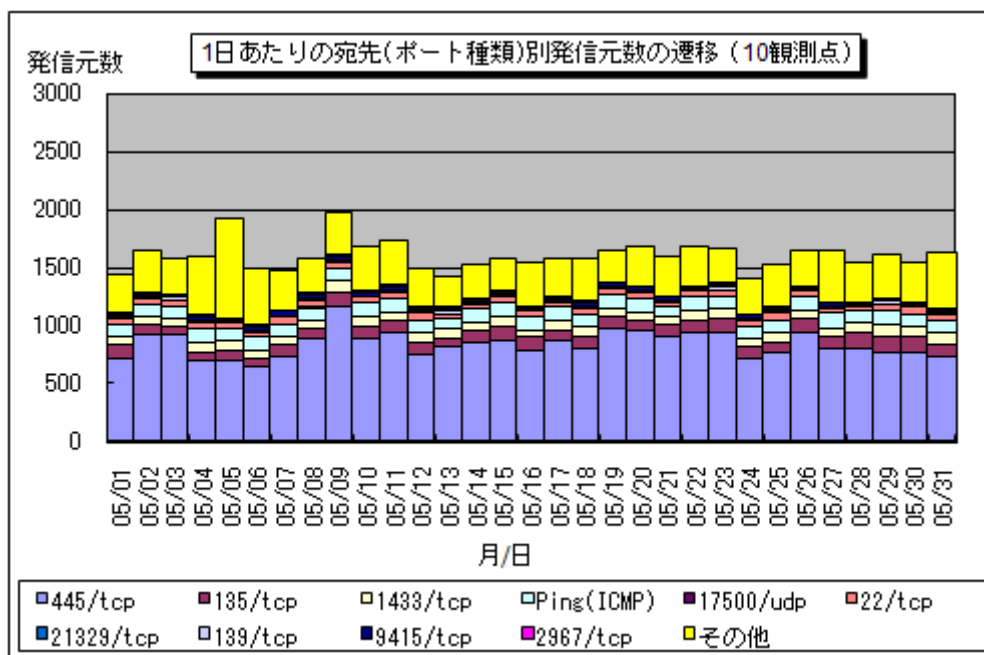
2. 2010年5月の一方的なアクセス状況

(1) 宛先（ポート種類）別のアクセス状況

2010年5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。



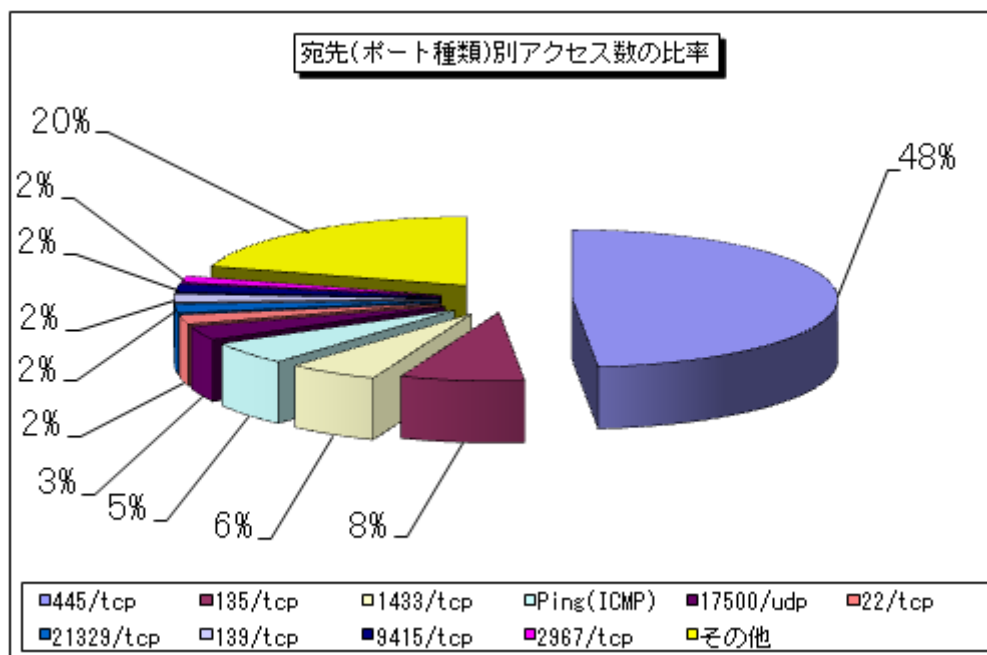
【図2-1：1日あたりの宛先（ポート種類）別アクセス数の遷移(10観測点)】



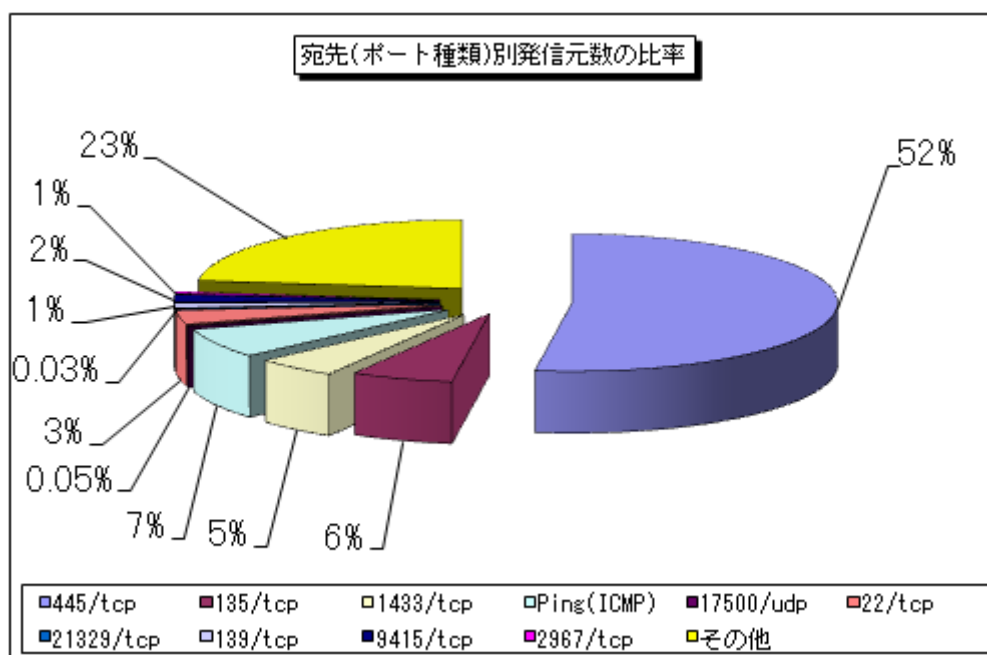
【図2-2：1日あたりの宛先（ポート種類）別発信元数の遷移(10観測点)】

(2) 宛先（ポート種類）別の比率

2010年5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。



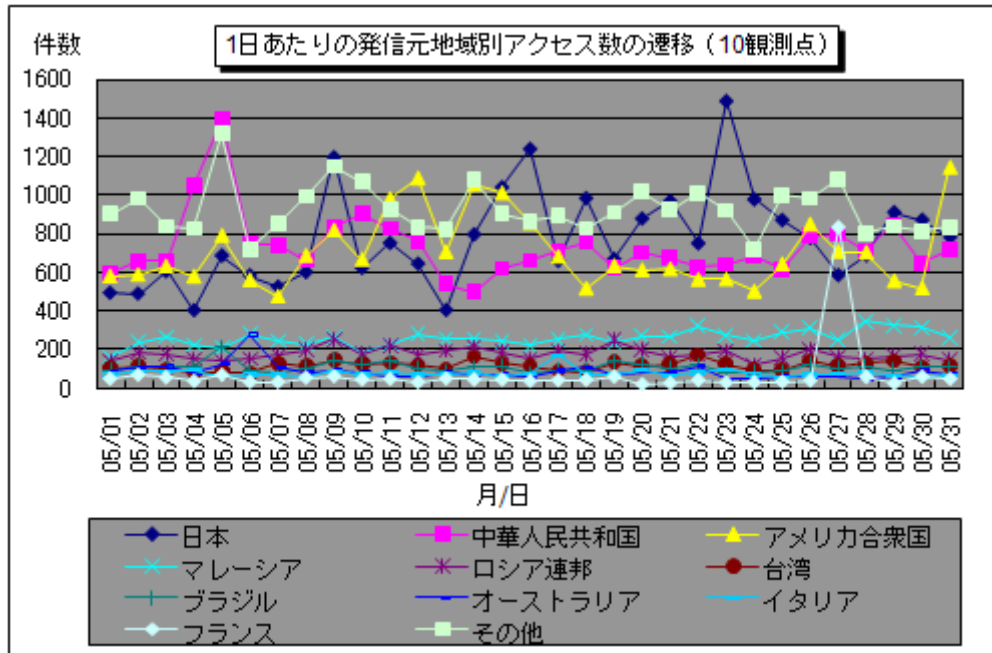
【図 2-3：宛先（ポート種類）別アクセス数の比率】



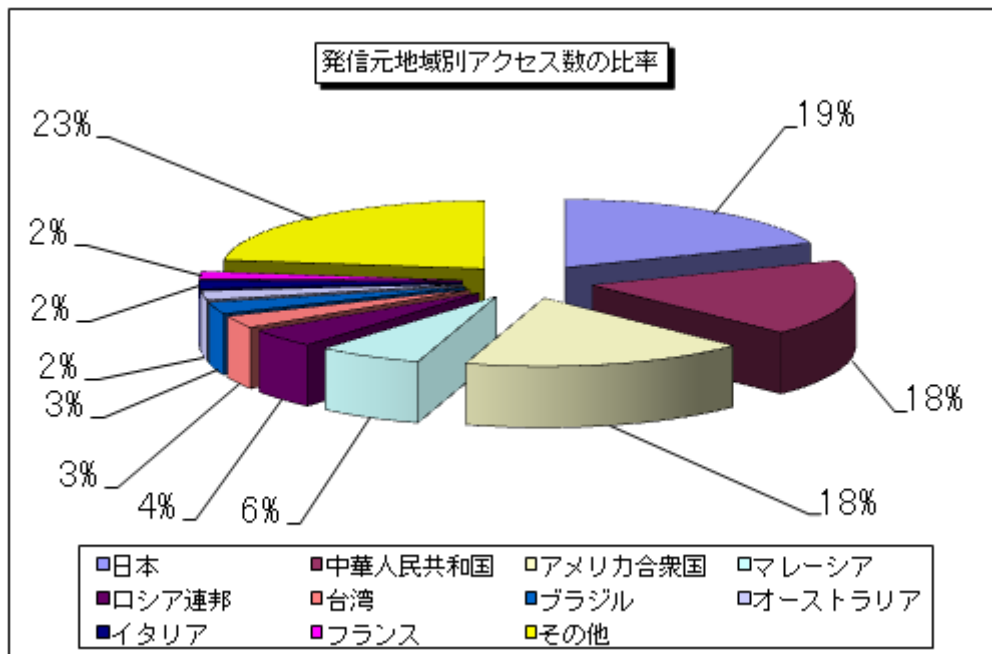
【図 2-4：宛先（ポート種類）別発信元数の比率】

(3) 発信元地域別のアクセス状況

2010年5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。

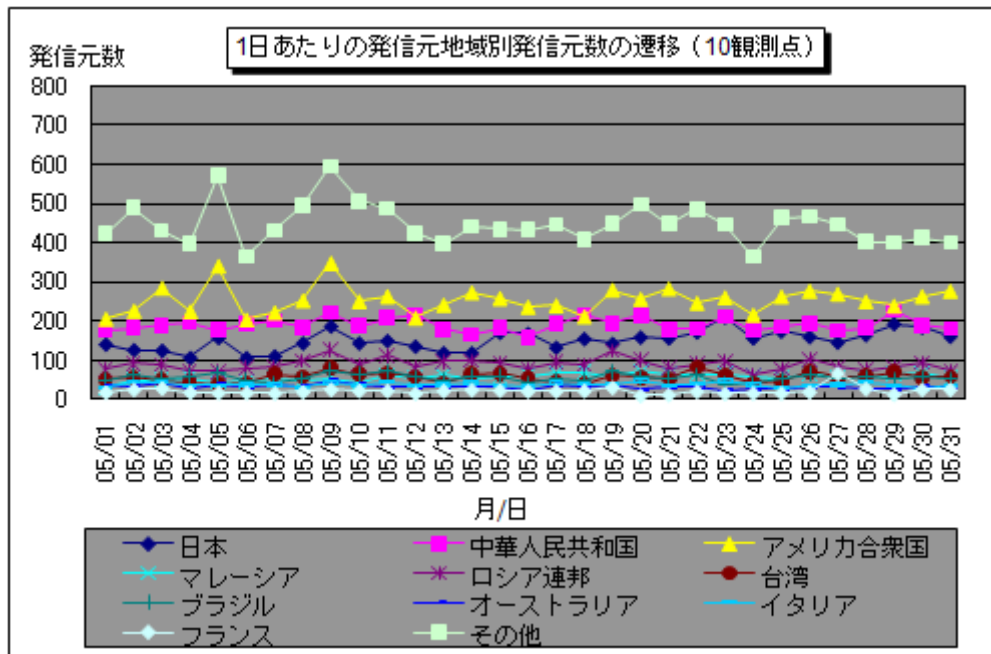


【図 2-5 : 1日あたりの発信元地域別アクセス数の遷移 (10観測点)】

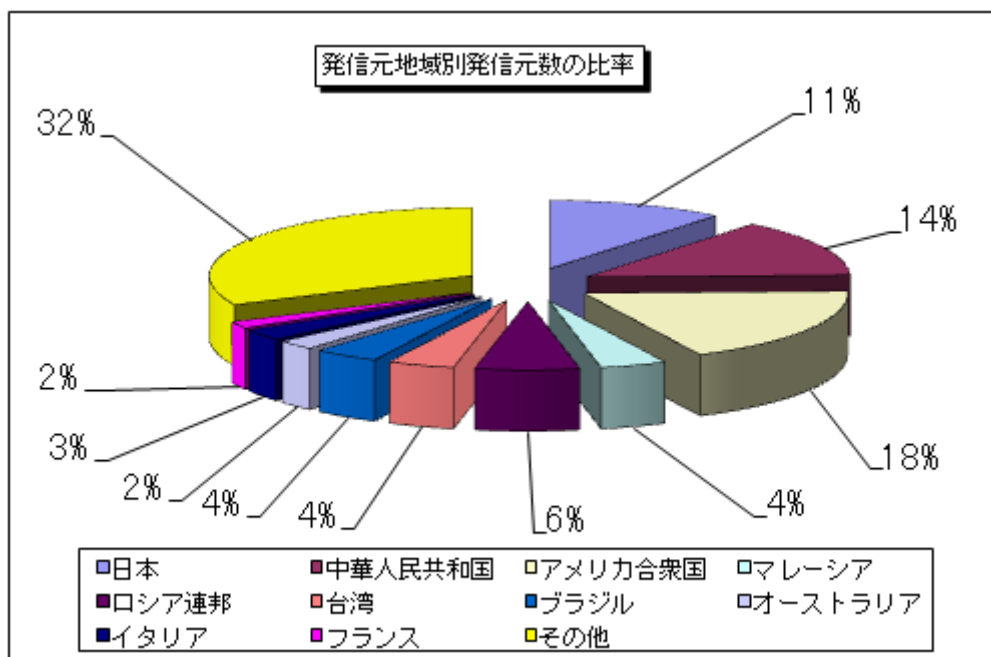


【図 2-6 : 発信元地域別アクセス数の比率】

2010年5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)】

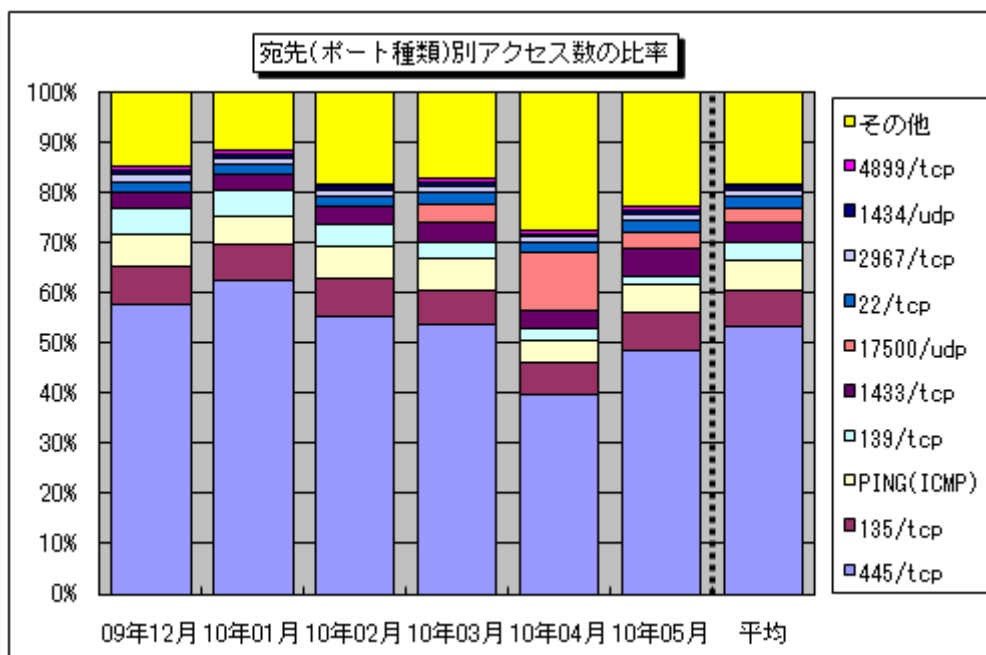


【図 2-8： 発信元地域別発信元数の比率】

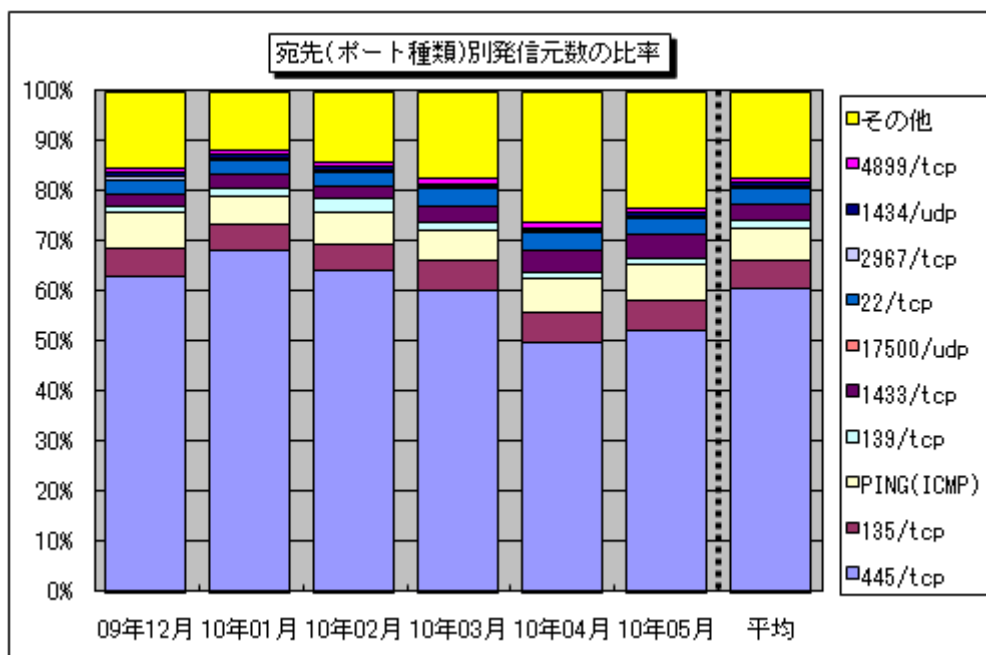
3. 統計情報

(1) 宛先（ポート種類）別の比率

2009年12月～2010年5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。



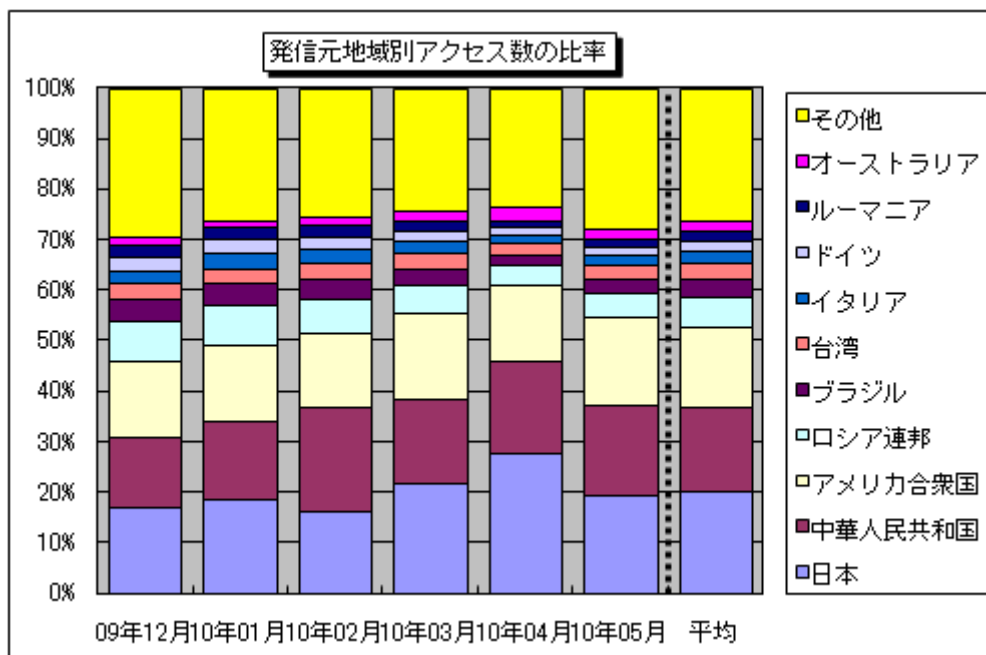
【図 3-1：宛先（ポート種類）別アクセス数の比率】



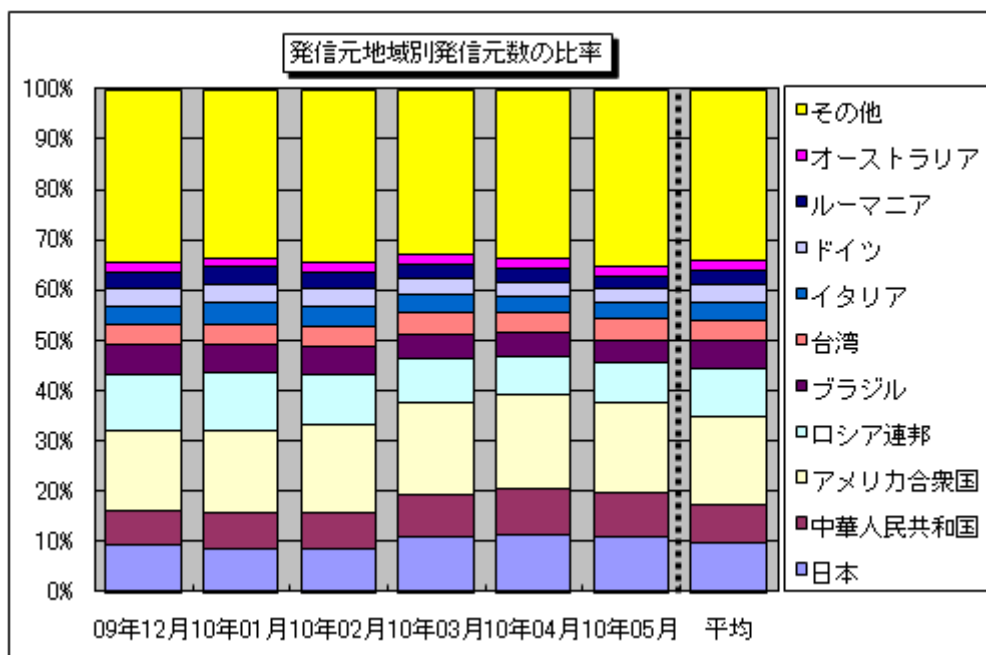
【図 3-2：宛先（ポート種類）別発信元数の比率】

(2) 発信元地域別の比率

2009年12月～2010年5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5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）。
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）。
1433/tcp	Microsoft SQL Server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。
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。
17500/udp	3月から特定の観測点でのみ観測されはじめた、特定の発信元からのブロードキャストと思われるアクセス。
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。
21329/tcp	5月の中旬にアメリカ合衆国の1つの発信元からTALOT2の1つの観測点のみに観測された目的不明のアクセス。
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。
9415/tcp	3月頃から徐々に増加してきた、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。
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