

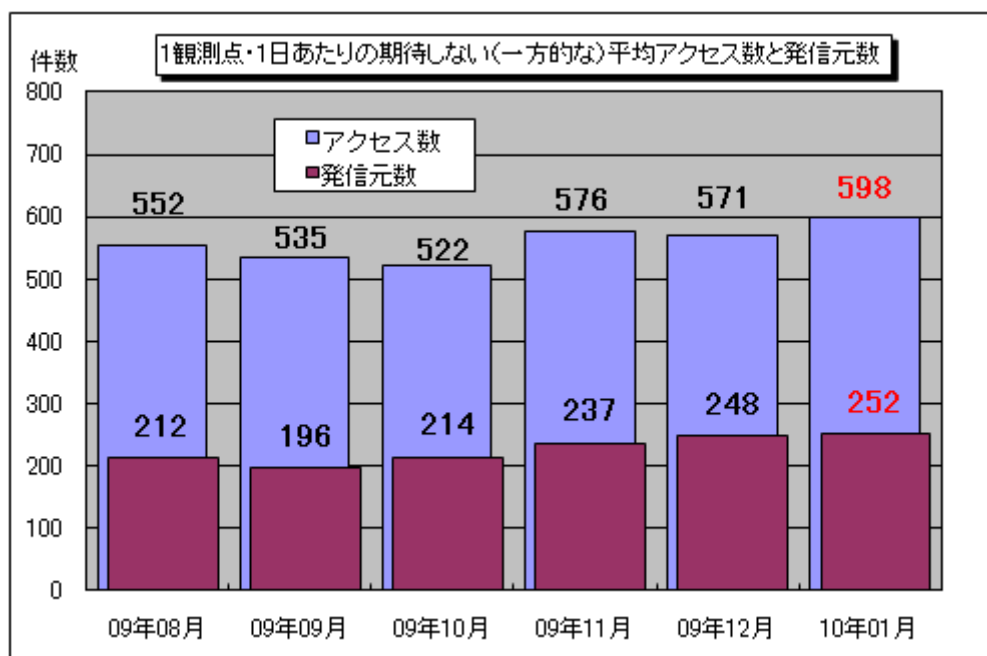
## インターネット定点観測（TALOT2）での観測状況について

### 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1月の期待しない（一方的な）アクセスの総数は10観測点で185,488件、延べ発信元数<sup>(※)</sup>は78,209箇所ありました。平均すると、1観測点につき1日あたり252の発信元から598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<sup>(※)</sup>：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。

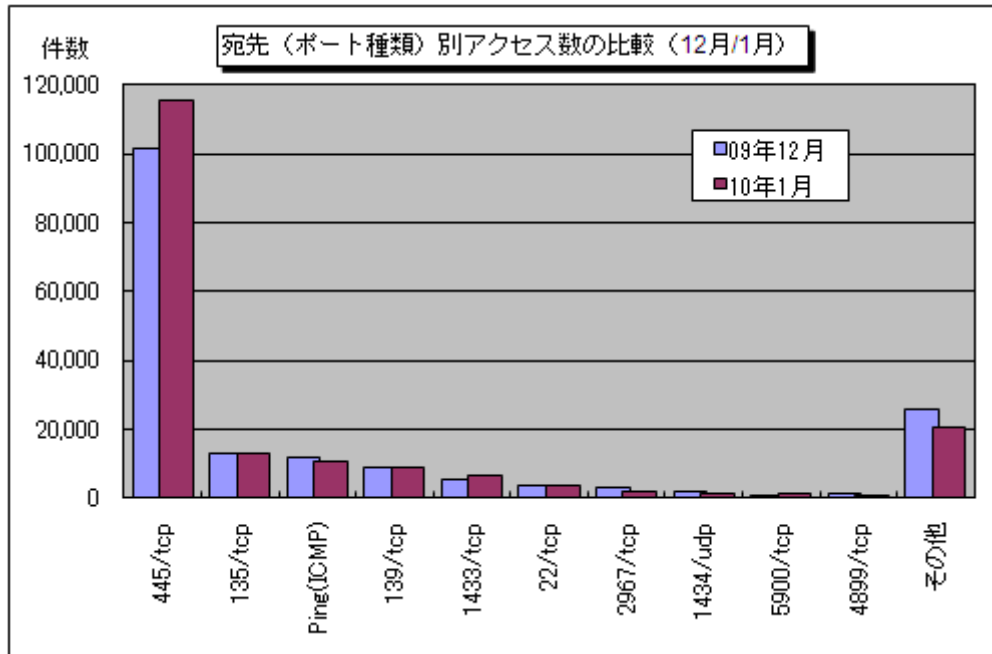


【図1-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009年8月～2010年1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。1月の期待しない（一方的な）アクセスは、2009年12月と比べて増加しました。

2009年12月と2010年1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、445/tcpへのアクセスは12月より増加しているものの、それ以外のポートではアクセス数に大きな変化は見られませんでした。

TALOT2の観測状況では、445/tcpへのアクセスが他のポートに比べて突出して多く、依然としてこのポートが悪意ある者に狙われやすい状況であることに変わりはありませんので、引き続き注意する必要があります。

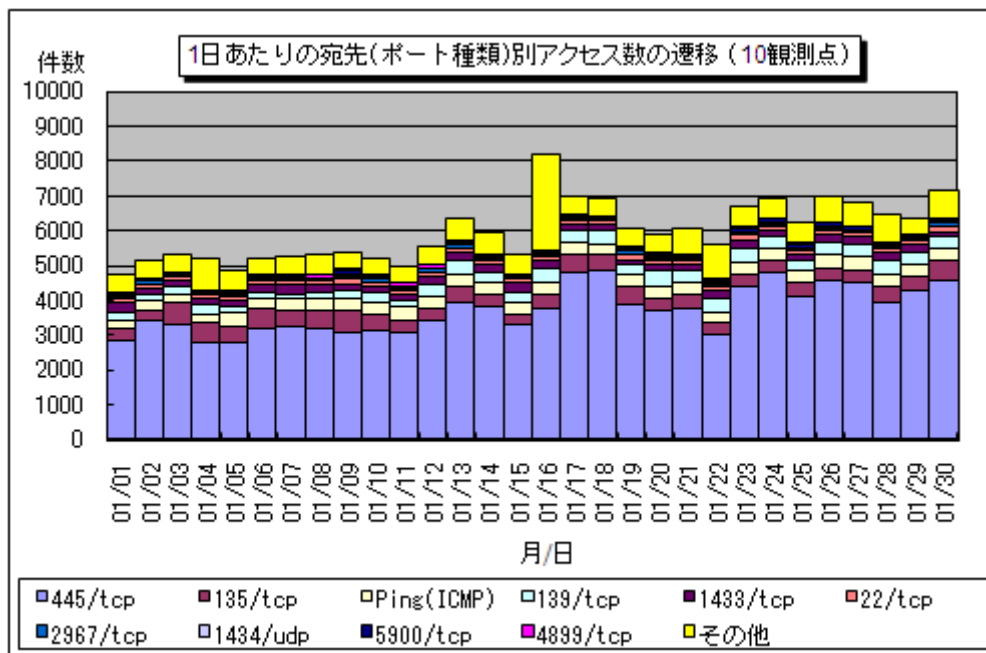


【図 1-2 : 宛先 (ポート種類) 別アクセス数の比較 (12月/1月)】

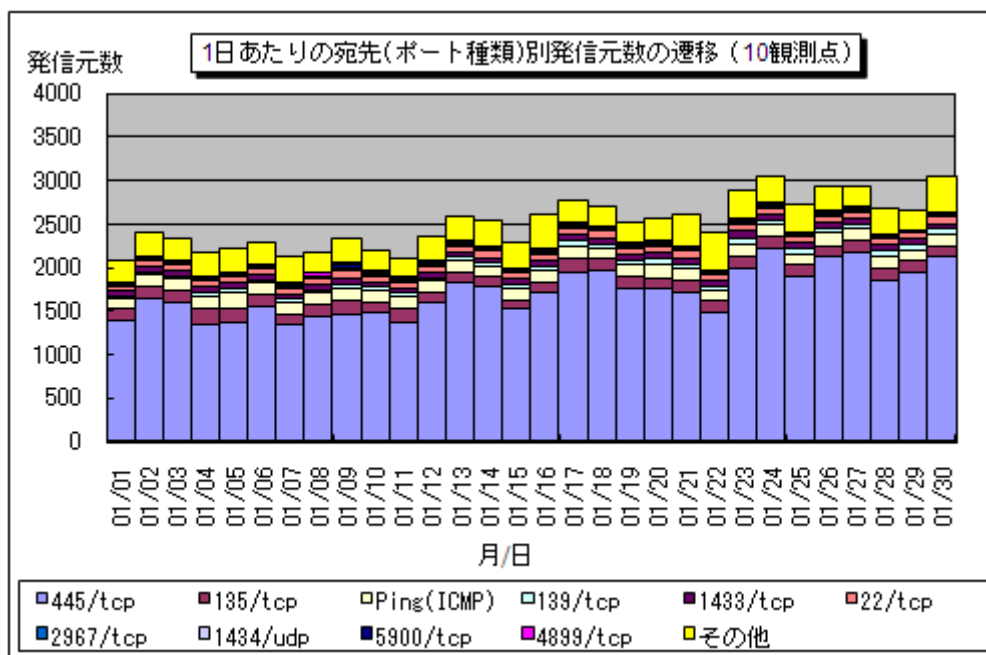
## 2. 2010年1月の一方的なアクセス状況

### (1) 宛先（ポート種類）別のアクセス状況

2010年1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。



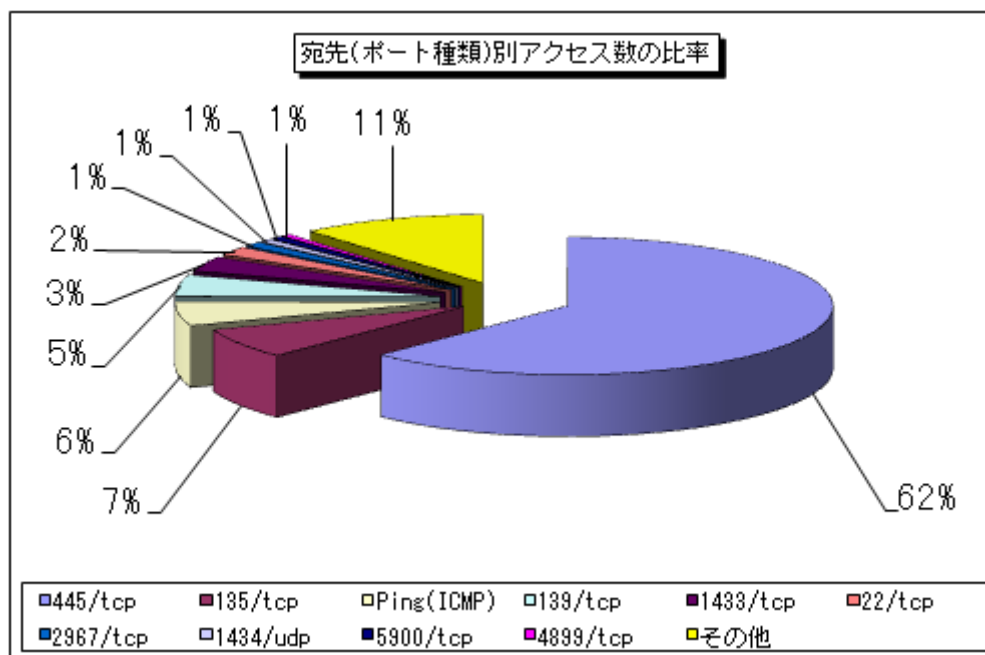
【図 2-1：2010年1月の1日あたりの宛先（ポート種類）別アクセス数の遷移】



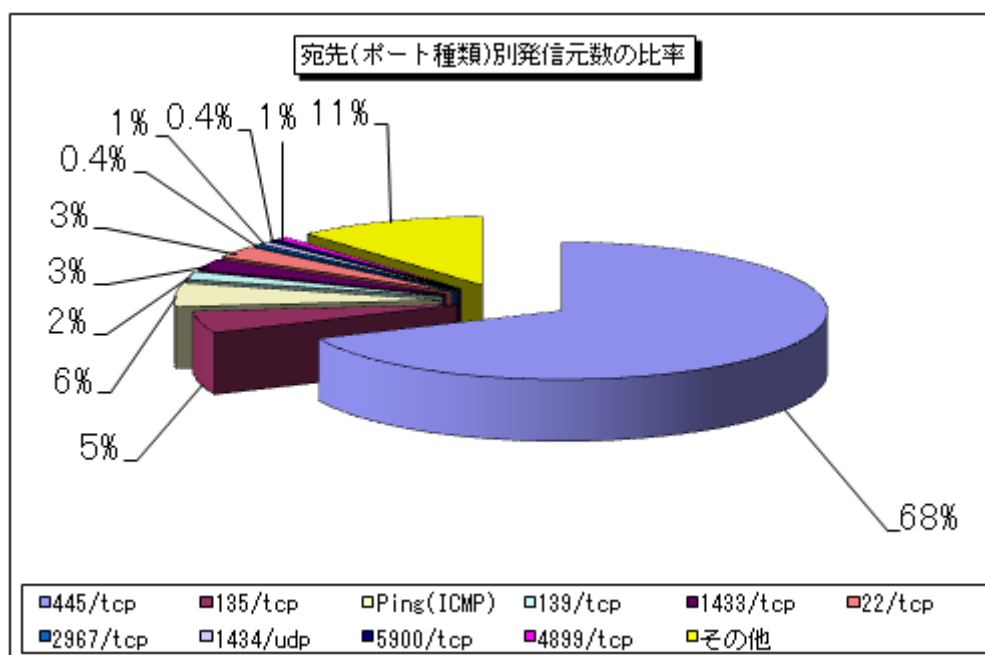
【図 2-2：2010年1月の1日あたりの宛先（ポート種類）別発信元数の遷移】

## (2) 宛先（ポート種類）別の比率

2010年1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。



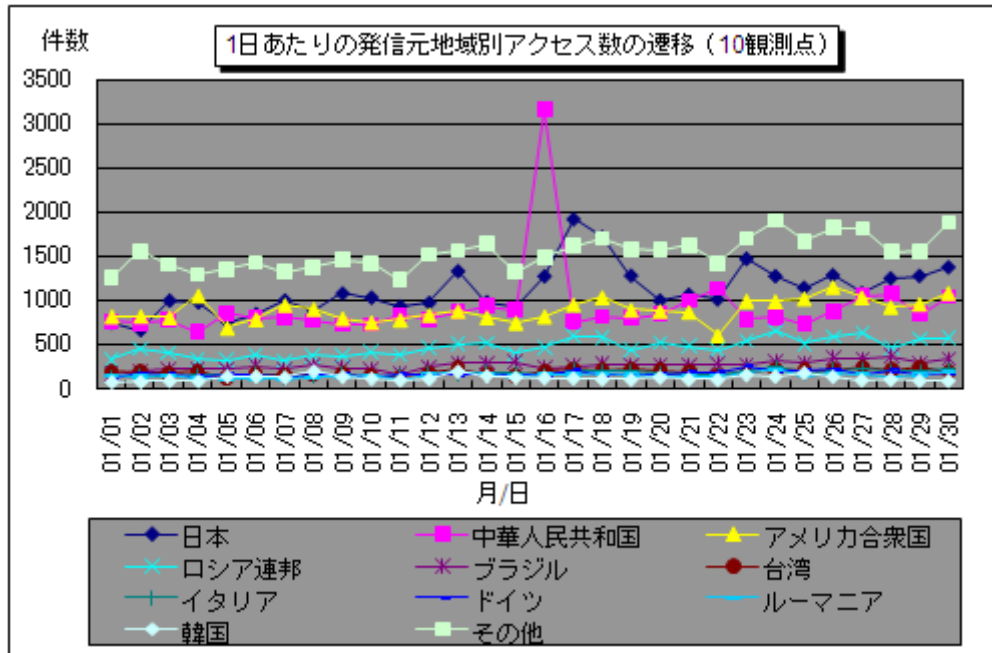
【図 2-3 : 2010 年 1 月の宛先（ポート種類）別アクセス数の比率】



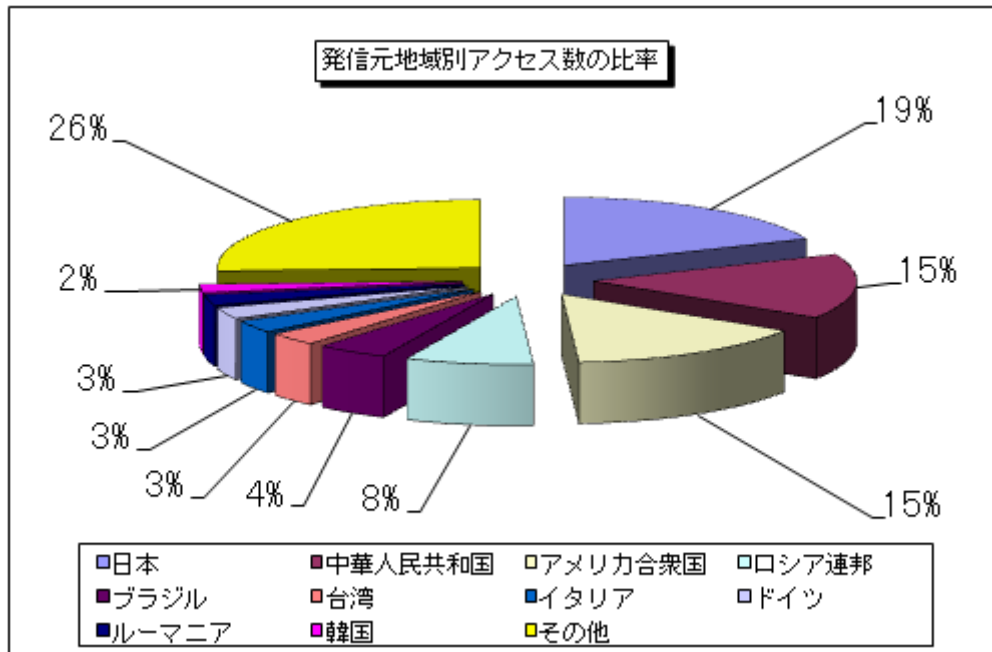
【図 2-4 : 2010 年 1 月の宛先（ポート種類）別発信元数の比率】

### (3) 発信元地域別のアクセス状況

2010年1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。

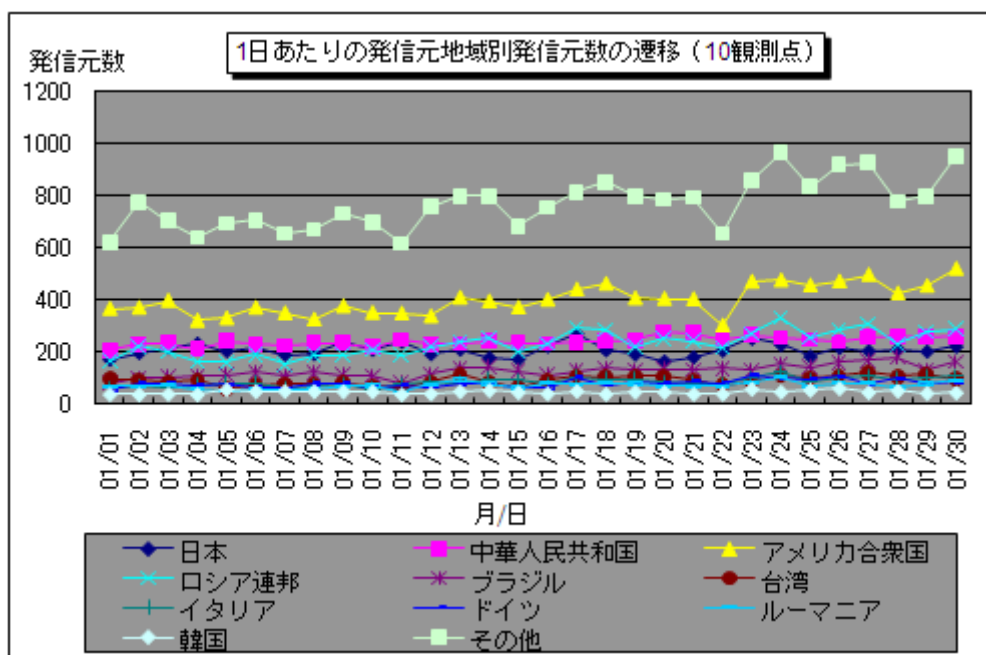


【図 2-5 : 2010年1月の1日あたりの発信元地域別アクセス数の遷移】

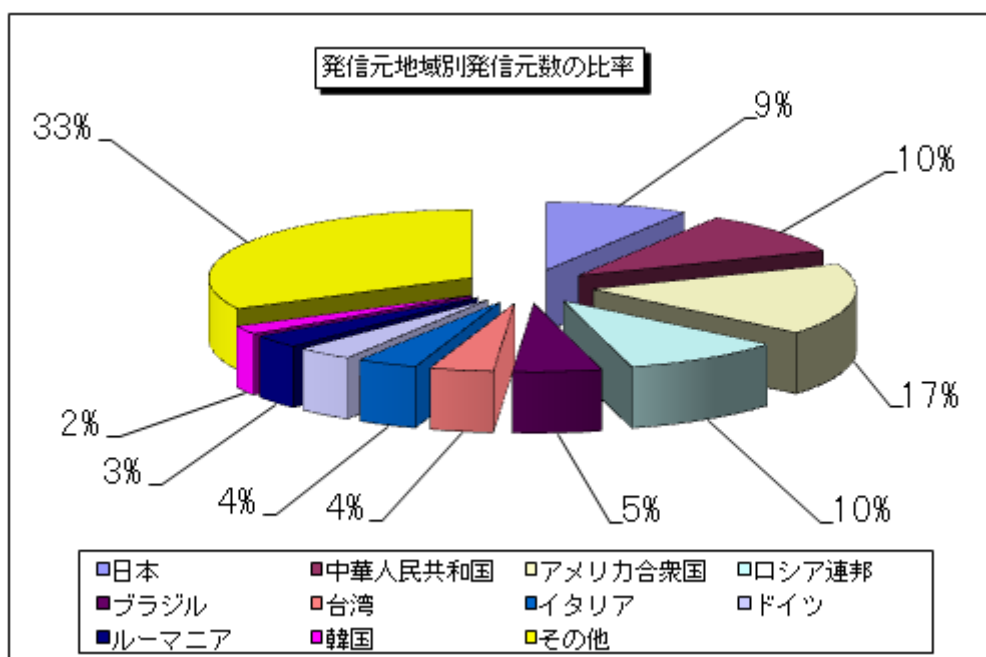


【図 2-6 : 2010年1月の発信元地域別アクセス数の比率】

2010年1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 : 2010 年 1 月の 1 日あたりの発信元地域別発信元数の遷移】

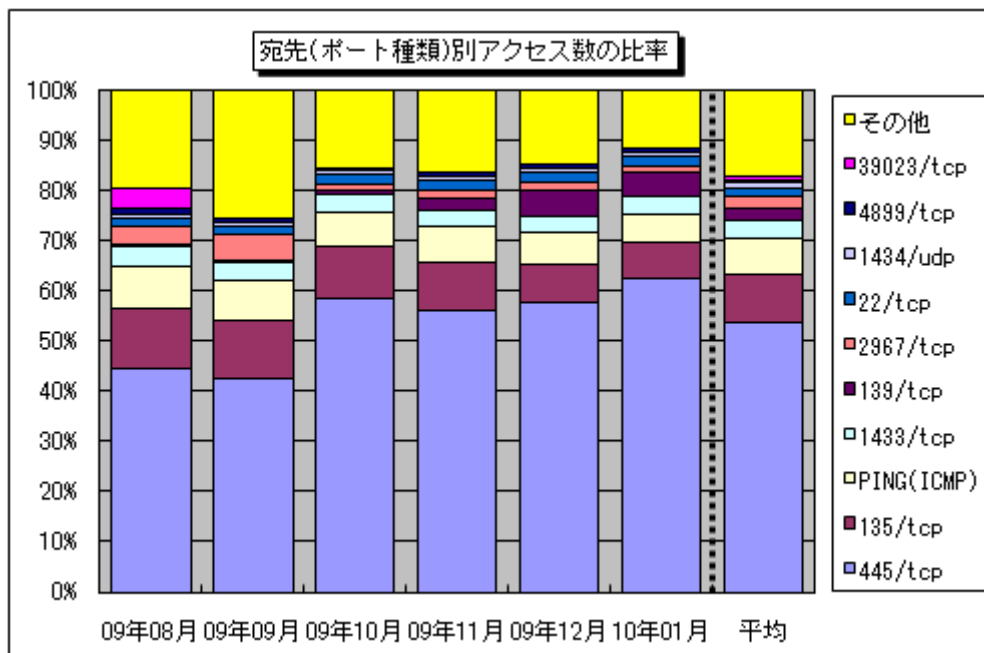


【図 2-8 : 2010 年 1 月の発信元地域別発信元数の比率】

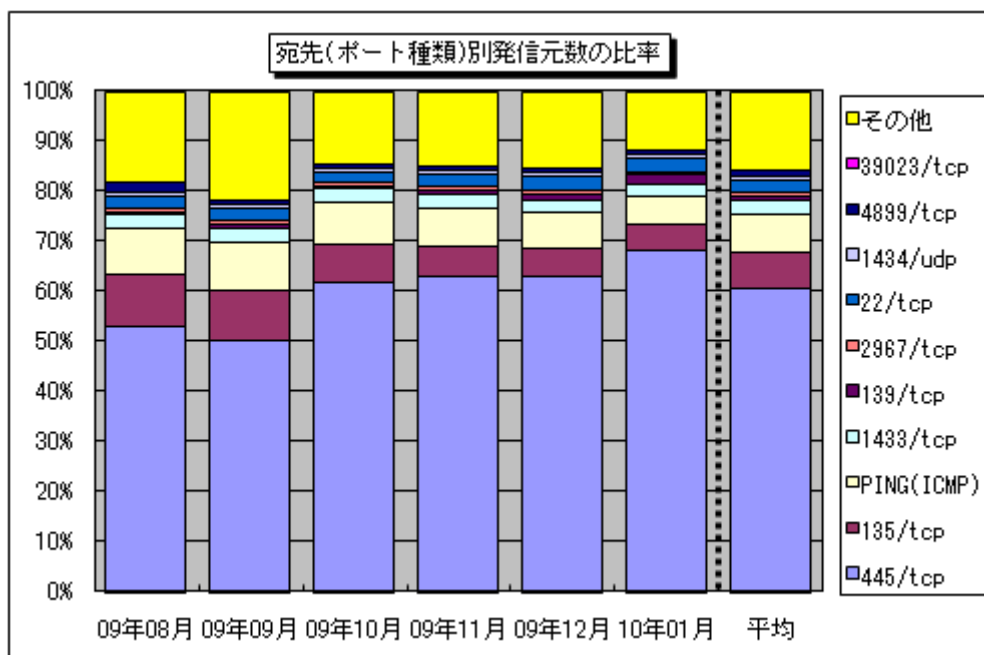
### 3. 統計情報

#### (1) 宛先（ポート種類）別の比率

2009年8月～2010年1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。



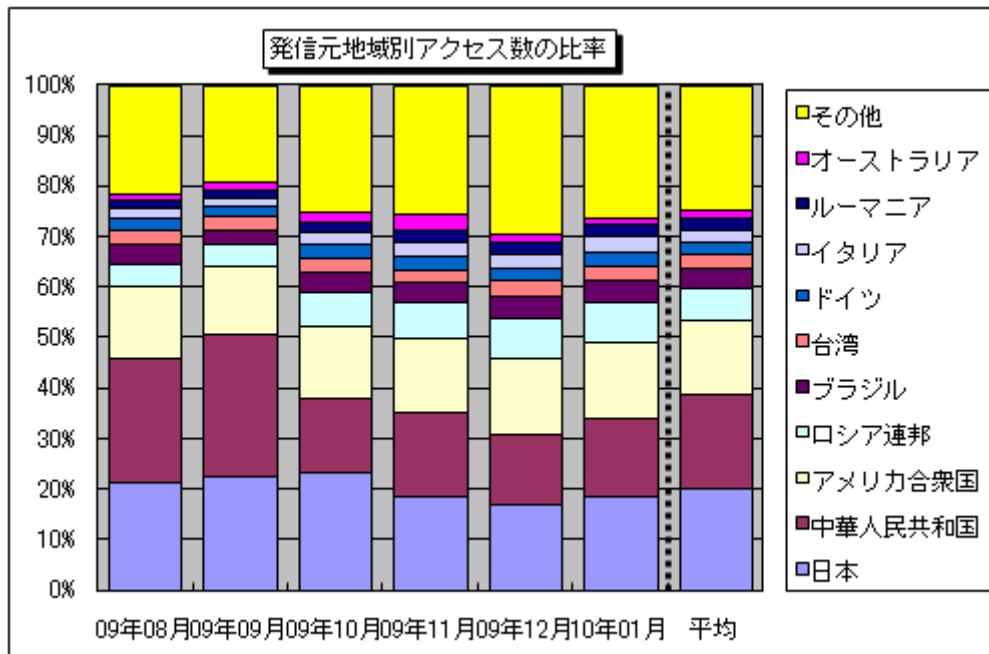
【図3-1：2009年8月～2010年1月の宛先（ポート種類）別アクセス数の比率】



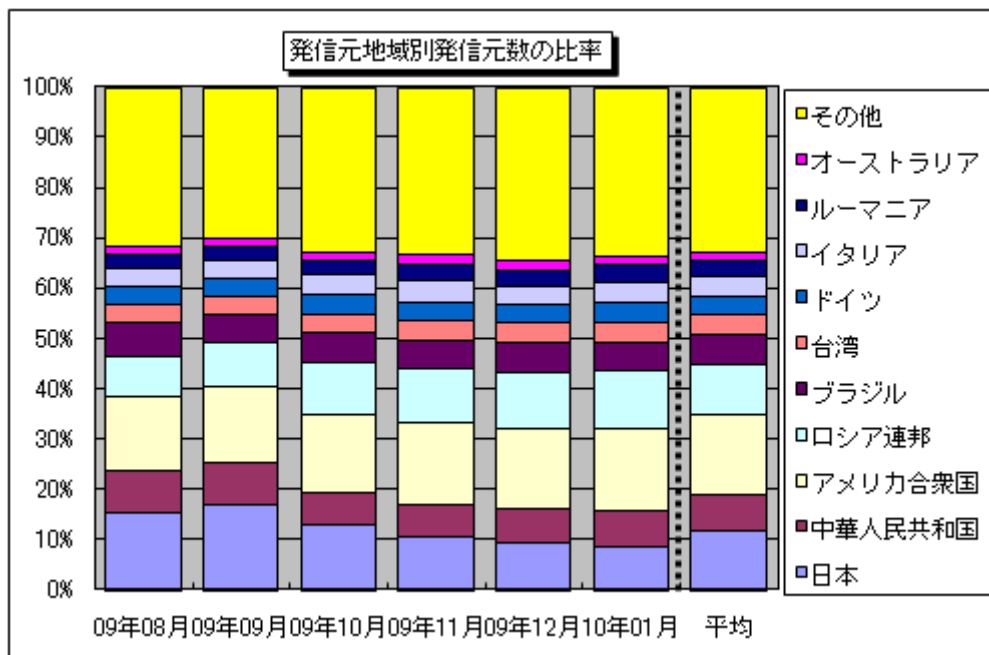
【図3-2：2009年8月～2010年1月の宛先（ポート種類）別発信元数の比率】

## (2) 発信元地域別の比率

2009年8月～2010年1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 8 月～2010 年 1 月の発信元地域別アクセス数の比率】



【図 3-4 : 2009 年 8 月～2010 年 1 月の発信元地域別発信元数の比率】



#### 4. 補足説明

以下に、2010年1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）。
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。
1433/tcp	Microsoft SQL Server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。
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。
1434/udp	Microsoft SQL Serverの脆弱性を狙った不正アクセスなどが有名（W32/SQLSlammerなど）。
5900/tcp	リモートアクセスツール RealVNCの脆弱性を狙ったアクセスである可能性が高い。
4899/tcp	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](mailto:isec-info@ipa.go.jp)