

## 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、2011年9月の期待しない（一方的な）アクセスの総数は10観測点で108,576件、延べ発信元数<sup>\*</sup>は45,285箇所ありました。平均すると、1観測点につき1日あたり150の発信元から361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。

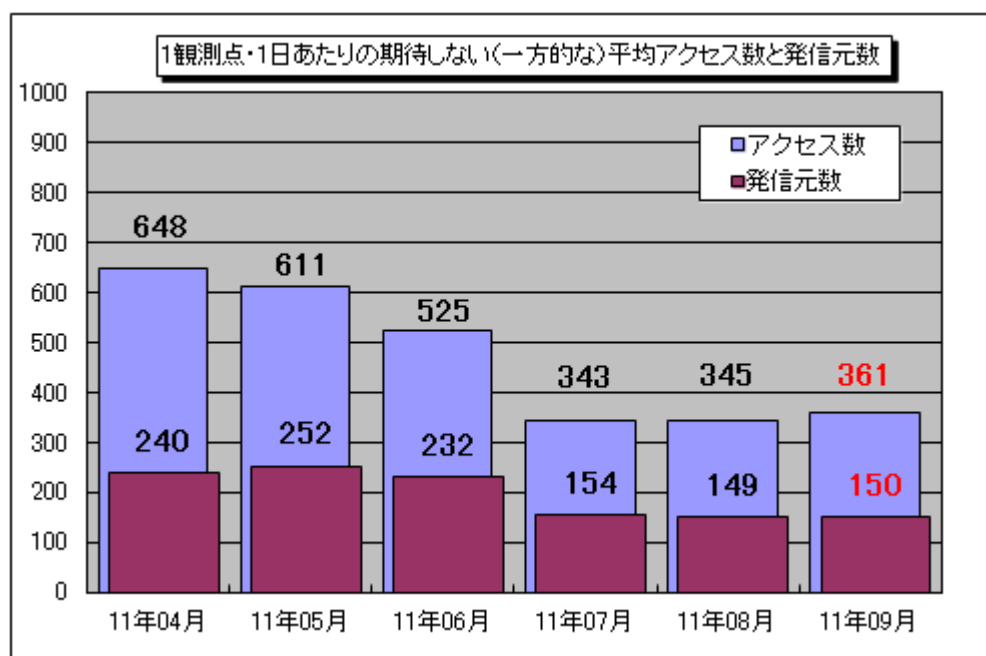


図1-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは2011年4月～2011年9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示しています。9月の期待しない（一方的な）アクセスは、8月と比べてやや増加しました。

8月と9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。これを見ると各ポートへのアクセス数において、8月と比べてそれほど目立った変化はありませんでしたが、2011年9月のレポートで8月の後半に増加が観測されたと報告しました3389/tcpへのアクセスは、その後一時的に減少したのち、再び増加傾向を示しました（図1-3参照）。

3389/tcpは、主にRDP<sup>\*1</sup>で使用されるポートであり、このポートを悪用してWindows端末に感染を広げる「Morto<sup>\*2</sup>」と呼ばれるウイルスが2011年8月に見つかっているため、このアクセスがウイルスの感染活動によるものだった可能性があります。

IPAへのウイルス届出状況において、現時点で「Morto」に関する届出はありませんが、Windows上でリモートデスクトップなどの機能を使用している方は、ウイルスの感染被害に遭わないために、ウイルス対策を再確認するとともに、ログインの際のパスワードを強化するなどの対策を行うことを

お勧めします。

※1 RDP (Remote Desktop Protocol) : 遠隔で Windows 端末の操作ができるリモートデスクトップ機能などで使われるプロトコルのこと。

※2 Morto : RDP を悪用して Windows 端末に感染するウイルスの一種。感染すると 3389/tcp にポートスキャンを行いリモートデスクトップ機能が有効な端末を探し、発見した端末に対してパスワードクラッキングを試みる。

(ご参考)

2011年8月のインターネット定点観測 (TALOT2) での観測状況について (IPA)

<http://www.ipa.go.jp/security/txt/2011/documents/TALOT2-1109.pdf>

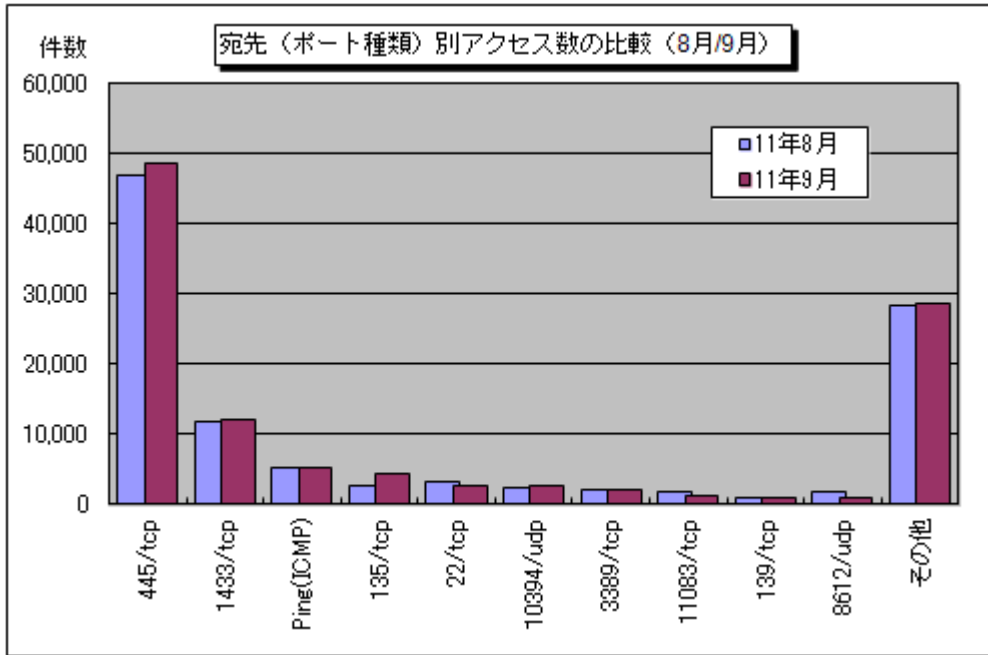


図 1-2 : 宛先 (ポート種類) 別アクセス数の比較 (8月/9月)

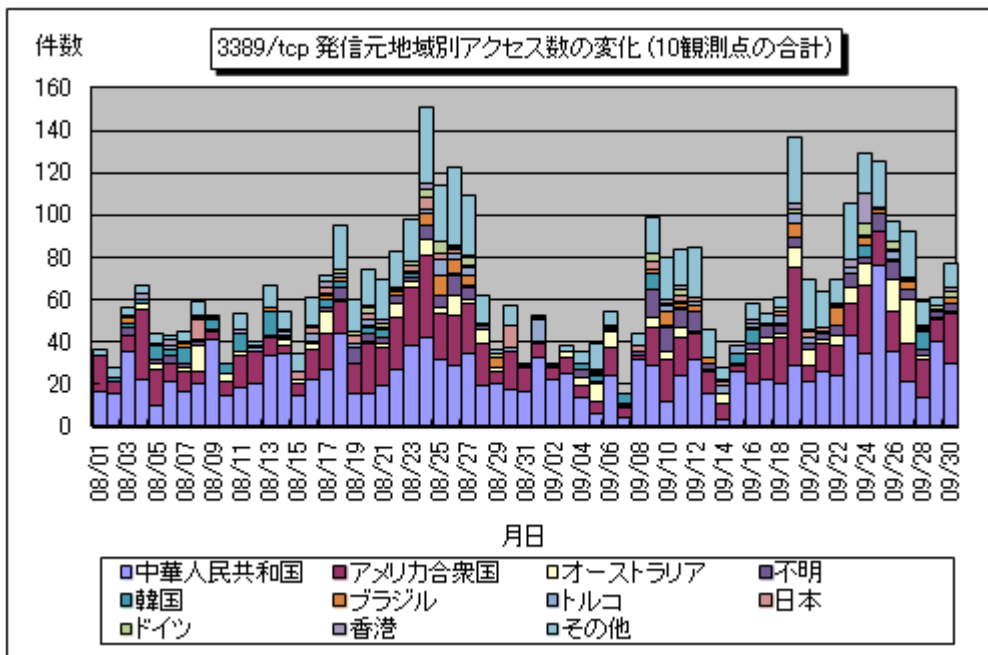


図 1-3 : 3389/tcp 発信元地域別アクセス数の変化 (10 観測点の合計)

## 2. 2011年9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

2011年9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。

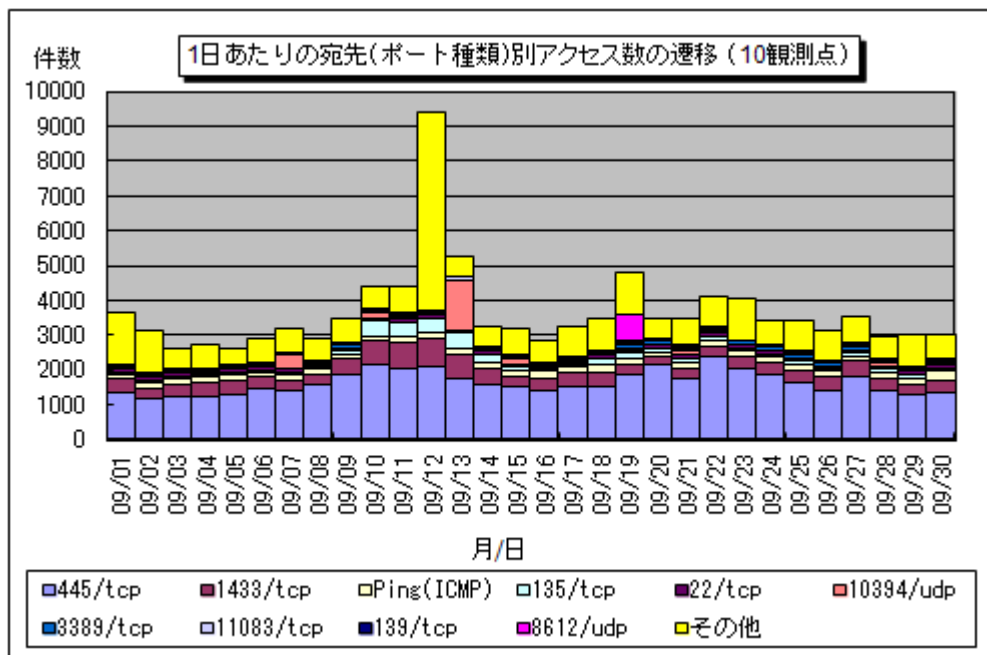


図 2-1：1日あたりの宛先（ポート種類）別アクセス数の遷移（10観測点）

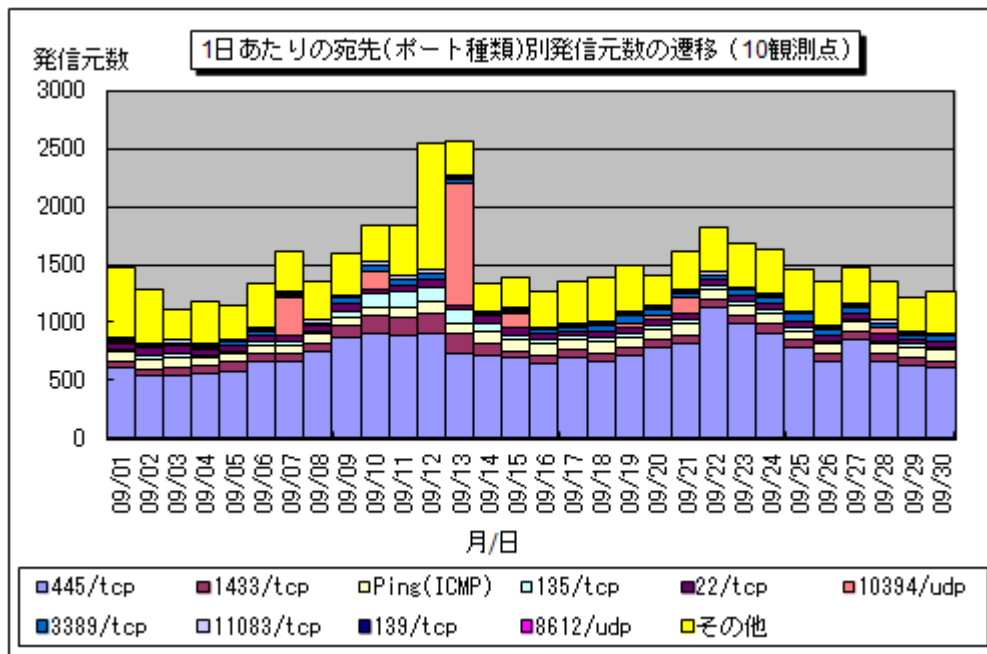


図 2-2：1日あたりの宛先（ポート種類）別発信元数の遷移（10観測点）

## (2) 宛先（ポート種類）別の比率

2011年9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。

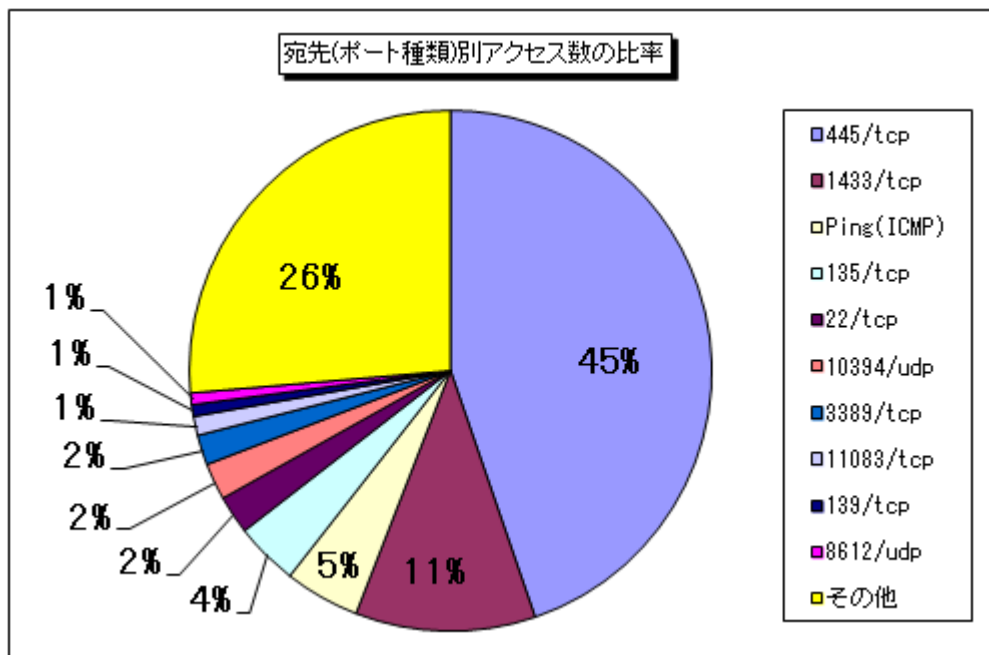


図 2-3：宛先（ポート種類）別アクセス数の比率

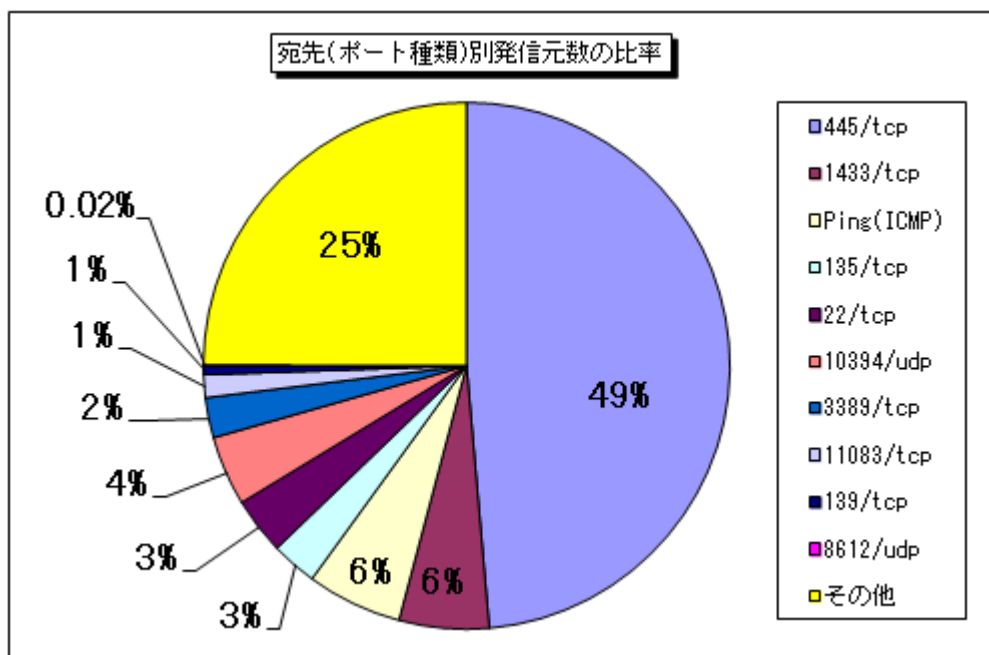


図 2-4：宛先（ポート種類）別発信元数の比率

### (3) 発信元地域別のアクセス状況

2011年9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。

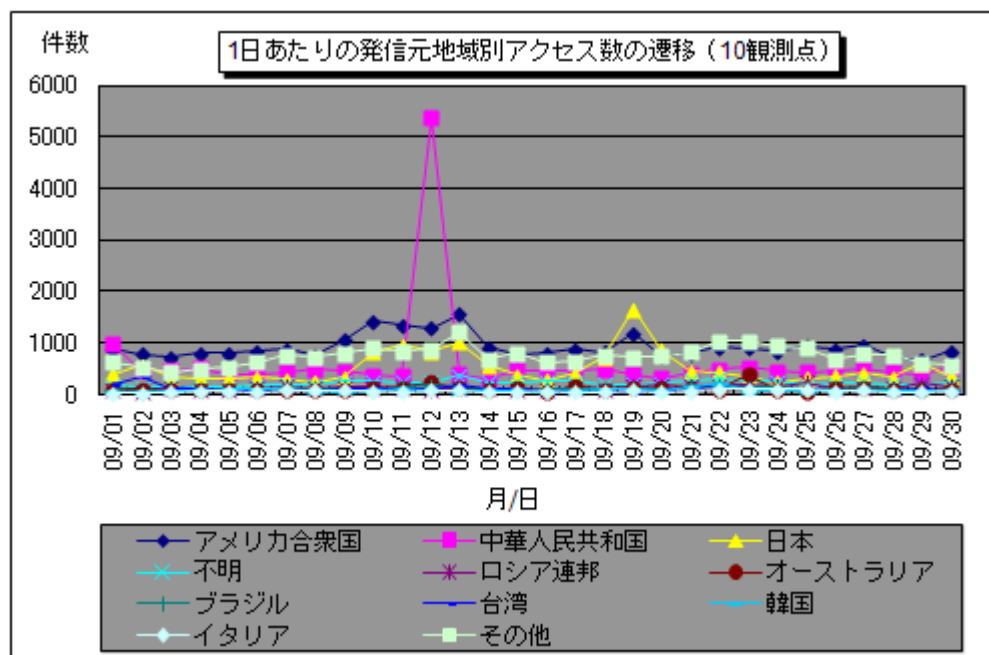


図 2-5 : 1日あたりの発信元地域別アクセス数の遷移 (10 観測点)

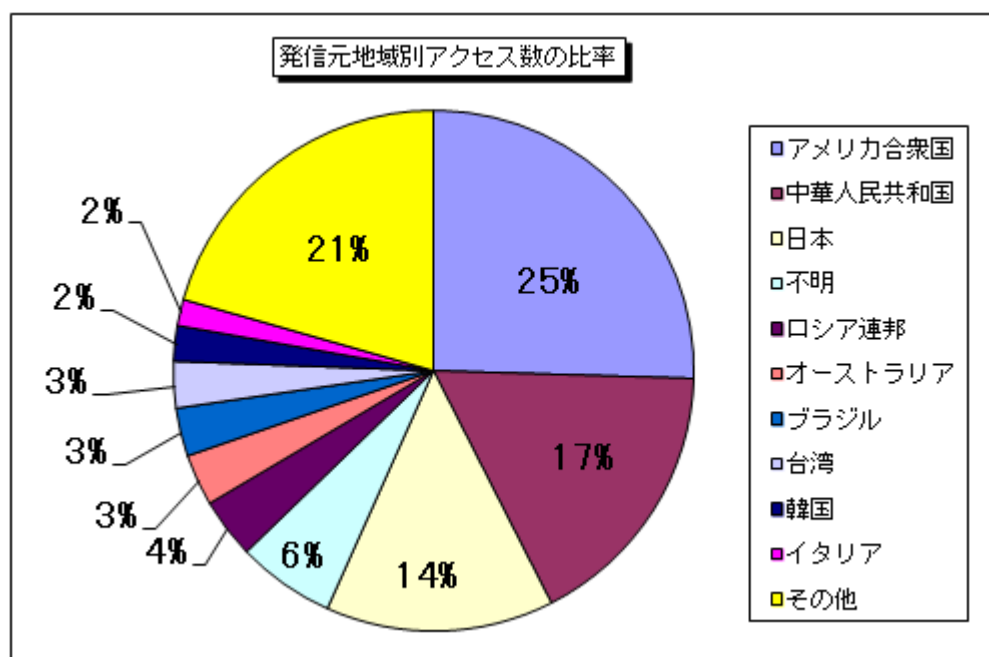


図 2-6 : 発信元地域別アクセス数の比率

2011年9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。

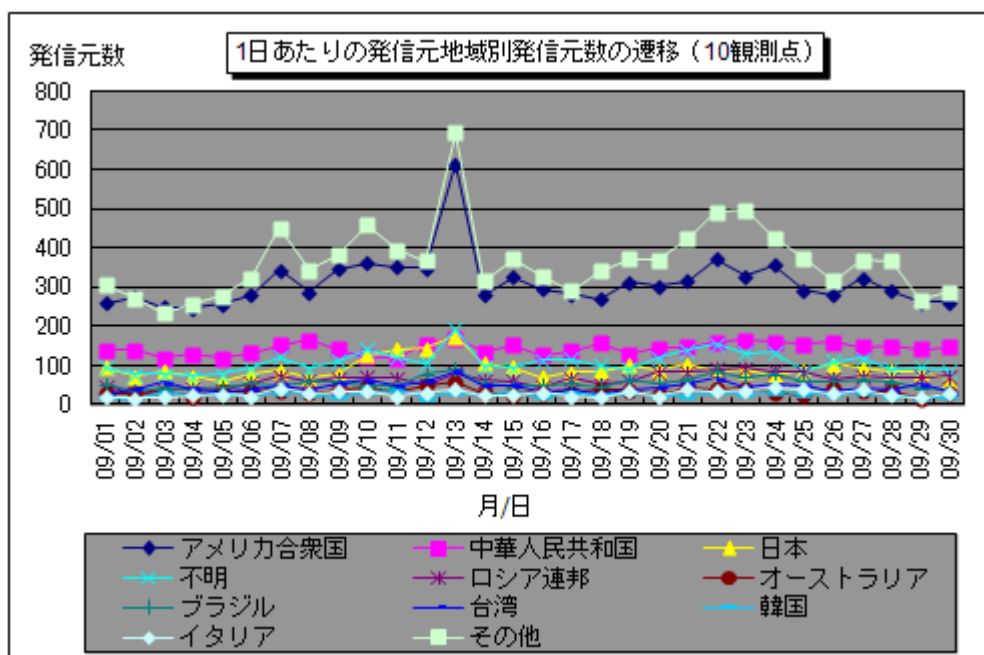


図 2-7： 1日あたりの発信元地域別発信元数の遷移（10観測点）

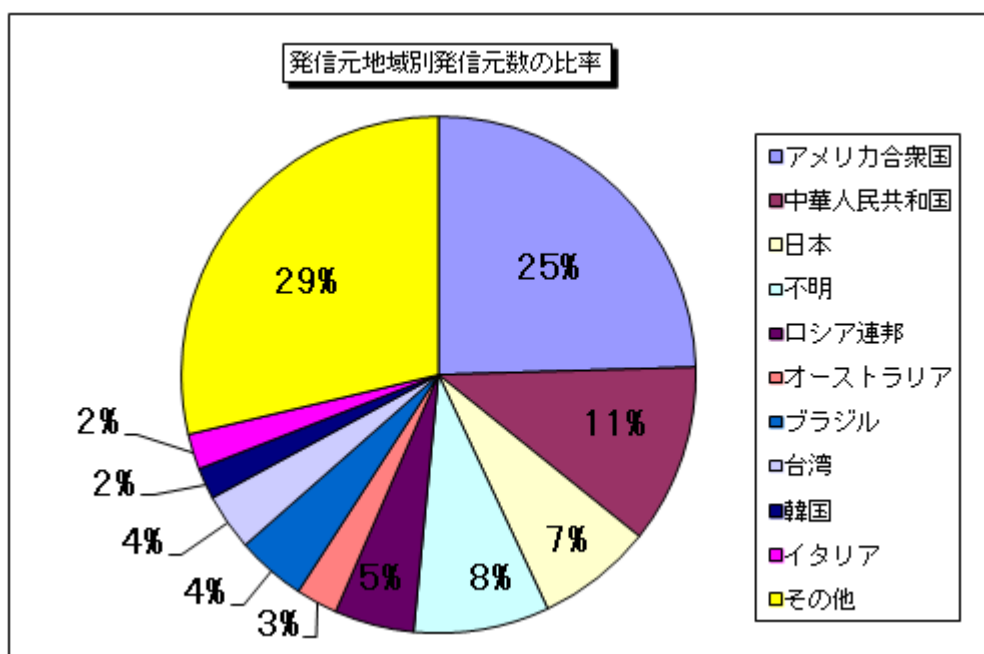


図 2-8： 発信元地域別発信元数の比率

### 3. 統計情報

#### (1) 宛先（ポート種類）別の比率

2011年4月～2011年9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。

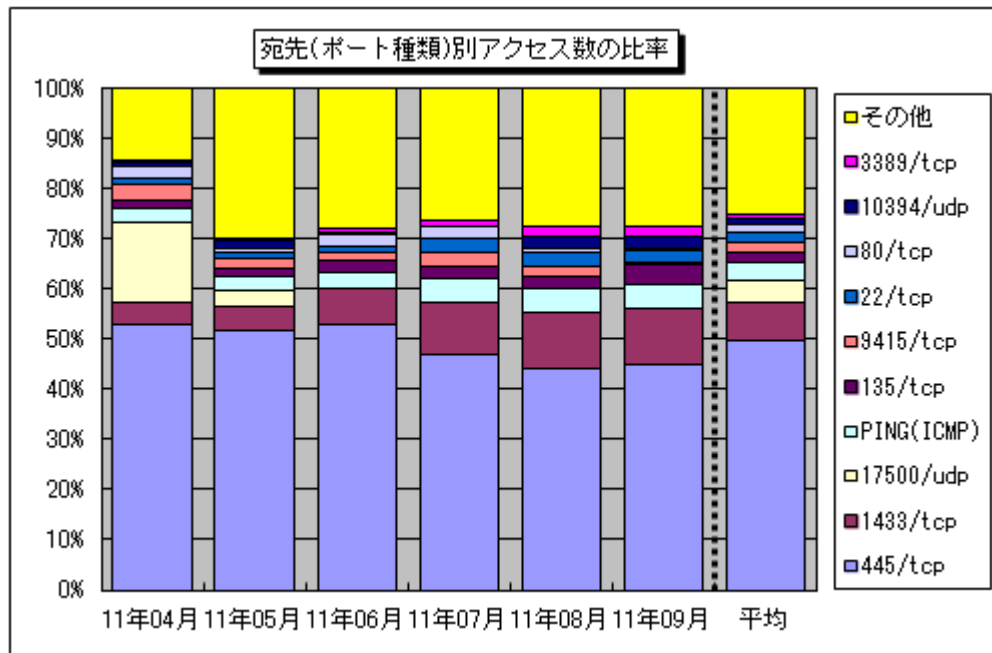


図 3-1：宛先（ポート種類）別アクセス数の比率

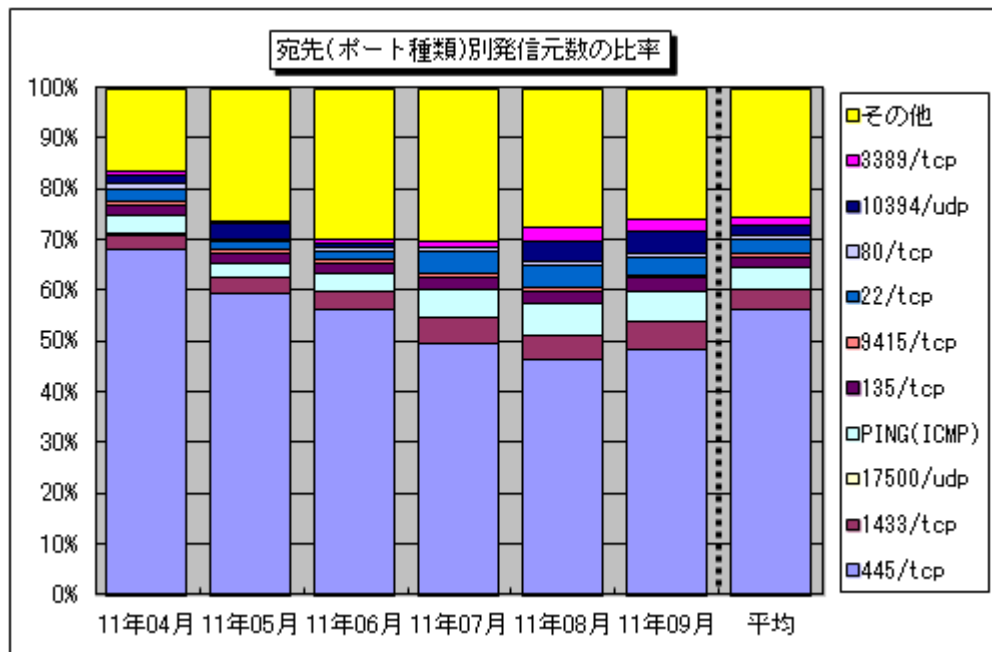


図 3-2：宛先（ポート種類）別発信元数の比率

## (2) 発信元地域別の比率

2011年4月～2011年9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。

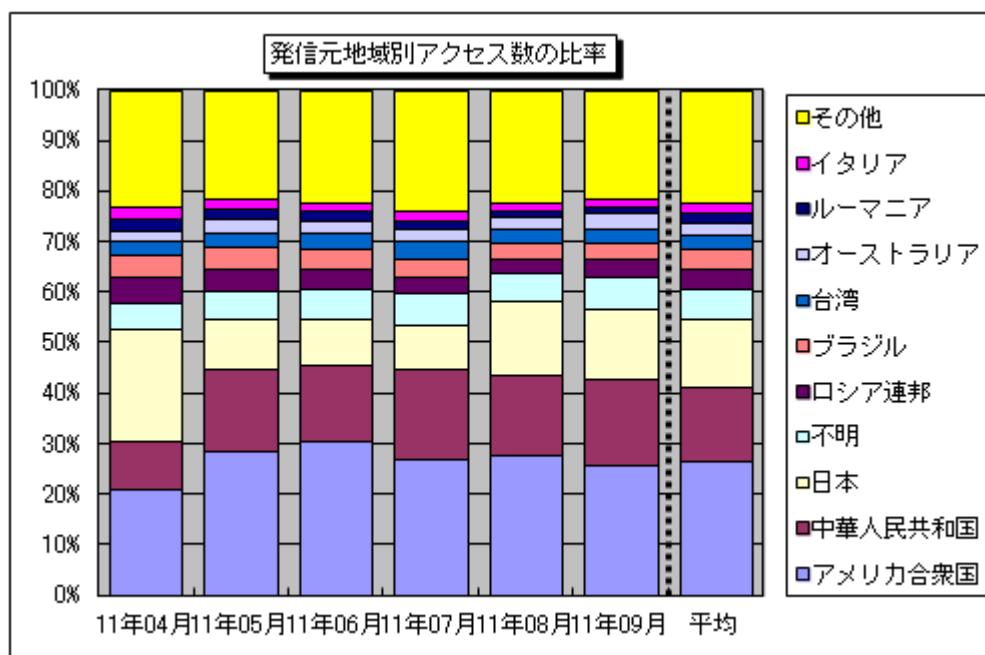


図 3-3：発信元地域別アクセス数の比率

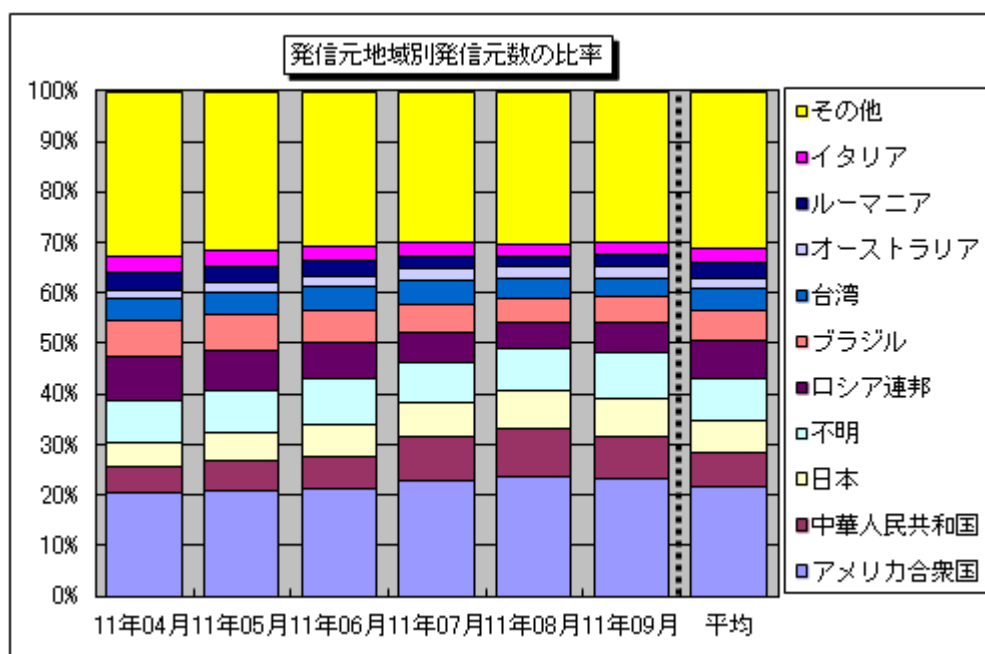


図 3-4：発信元地域別発信元数の比率



#### 4. 補足説明

以下に、2011年9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 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。
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）。
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。
10394/udp	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。 TALOT2の1観測点のみに観測された、原因不明のアクセス。
3389/tcp	MS WBT Server（MicroSoft Windows-Based Terminal Server）（ターミナルサービス/リモートデスクトップ）のデフォルトポートであり、この機能を悪用した何らかのアクセスである可能性がある。
11083/tcp	TALOT2の1観測点のみに観測された、原因不明のアクセス。
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。
8612/udp	TALOT2の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 技術本部 セキュリティセンター 加賀谷／大浦  
Tel:03-5978-7591 Fax:03-5978-7518  
E-mail: [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp)