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、2011 年 8 月の期待しない（一方的な）アクセスの総数は 10 観測点で **106,910 件**、延べ発信元数※は **46,101 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 149 の発信元から 345 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。

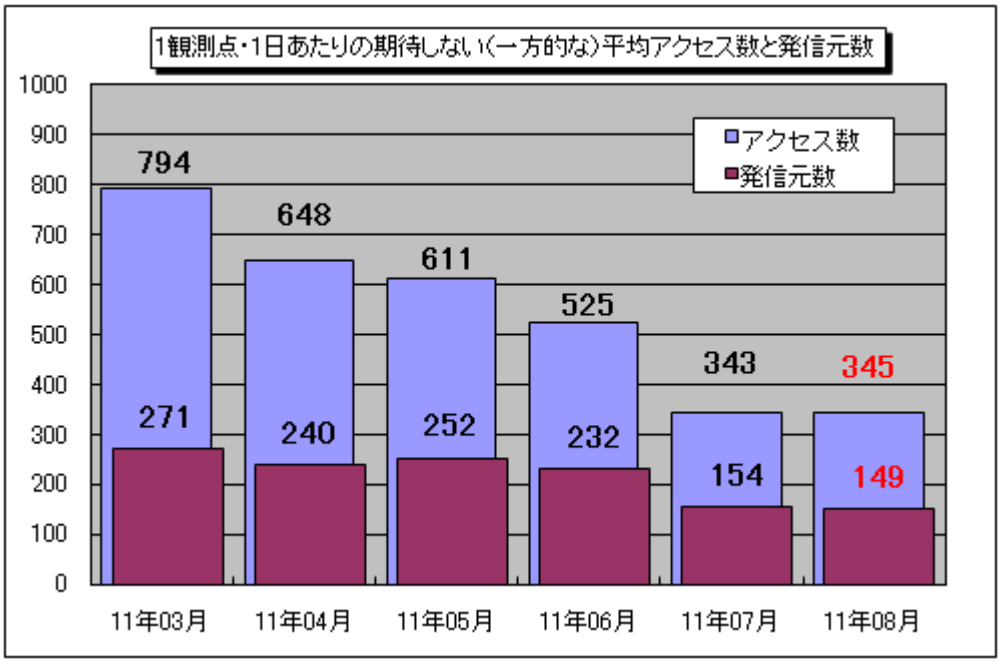

図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは 2011 年 3 月～2011 年 8 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。8 月の期待しない（一方的な）アクセスは、7 月と比べてほぼ同程度でした。

7 月と 8 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 月に比べ、増加が観測されたのは、22936/udp、10394/udp、および 3389/tcp へのアクセスでした。

22936/udp、および 10394/udp 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く、これら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、どちらも特定の 1 観測点のみで観測されていました。

3389/tcp は、8 月の後半に増加が観測されており（図 1-3 参照）、国内で定点観測を行っている他の組織でもほぼ同様の傾向が観測されていたとのことです。このポートは、主に RDP※1 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※2」と呼ばれるウイルスが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。

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ってください。

※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索し、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。

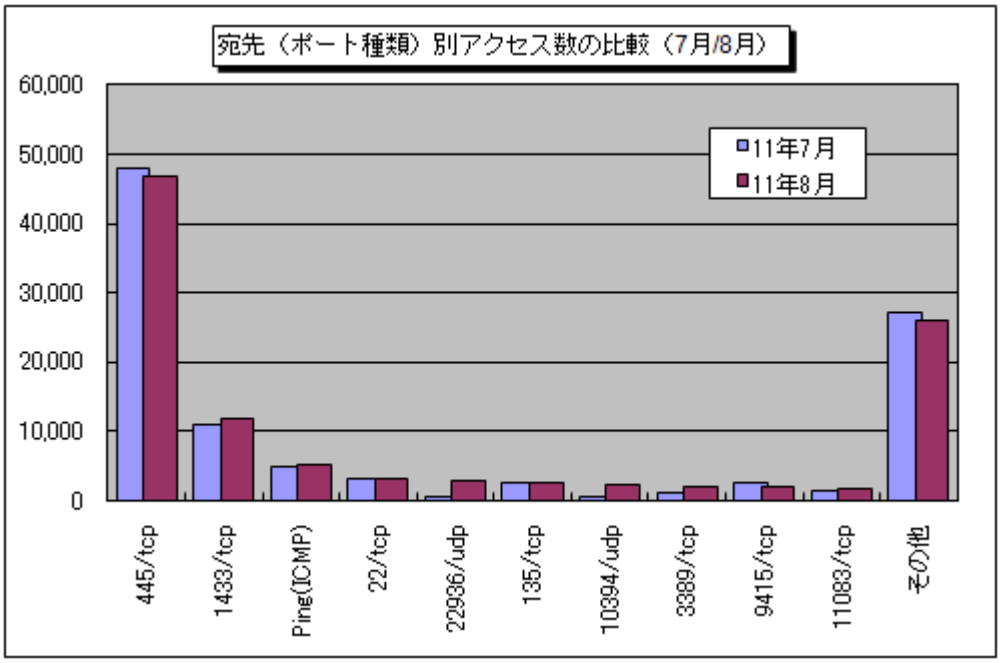

図 1-2：宛先（ポート種類）別アクセス数の比較（7 月/8 月）

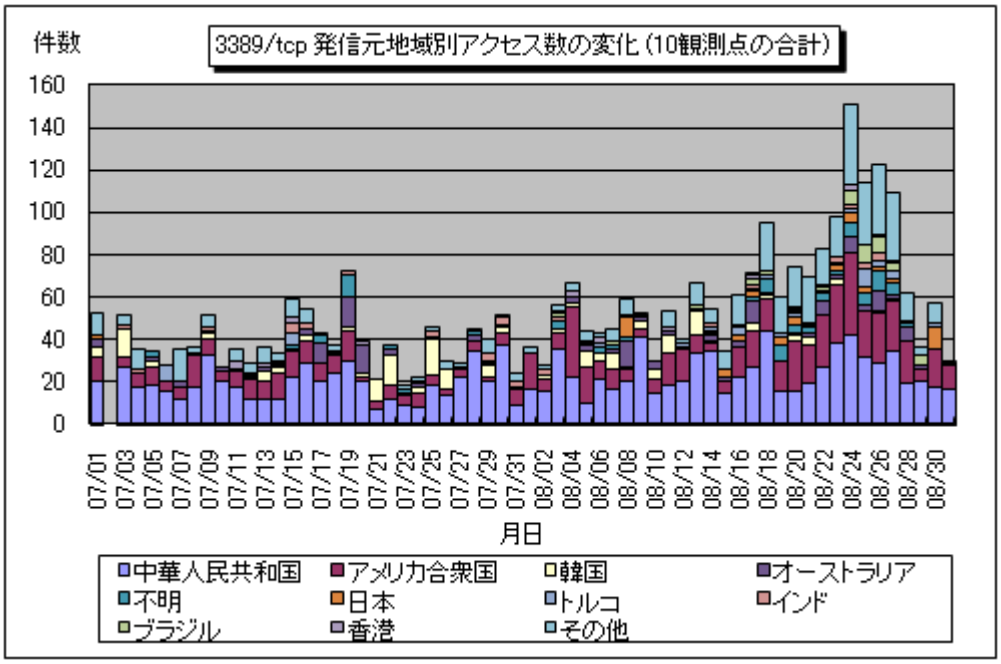

図 1-3：3389/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

※7/2 は保守作業のため、システムを停止しています。

2. 2011年8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 8 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。

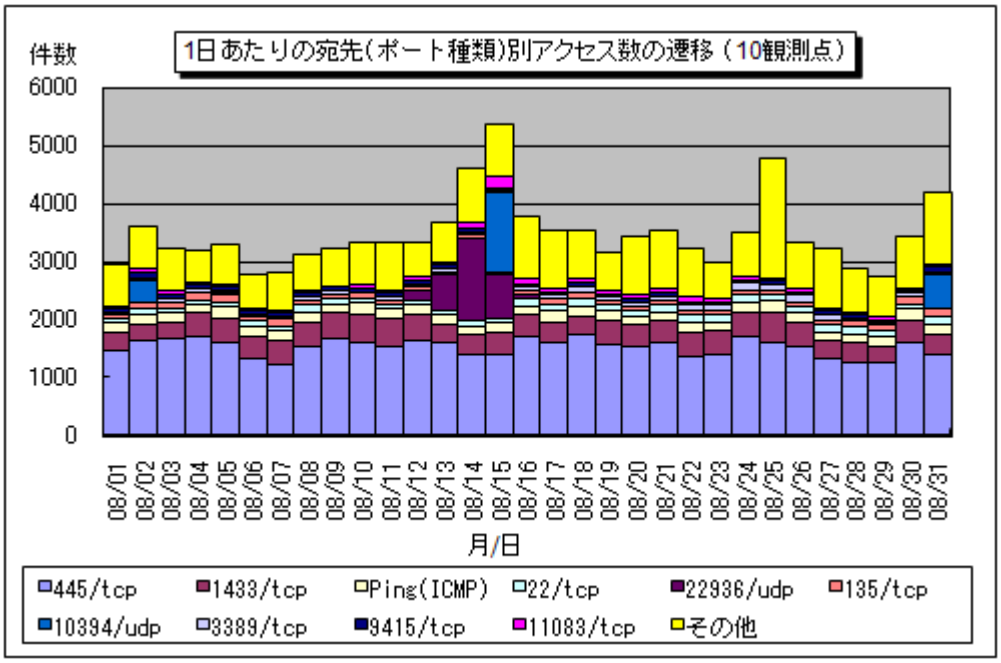

図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移（10 観測点）

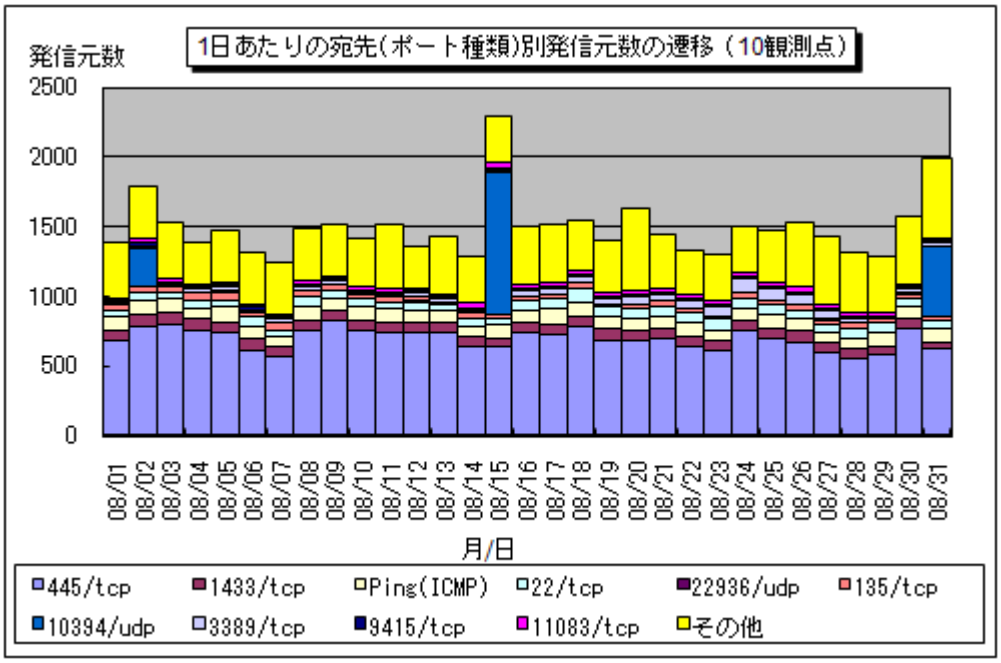

図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）

（2）宛先（ポート種類）別の比率

2011 年 8 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。

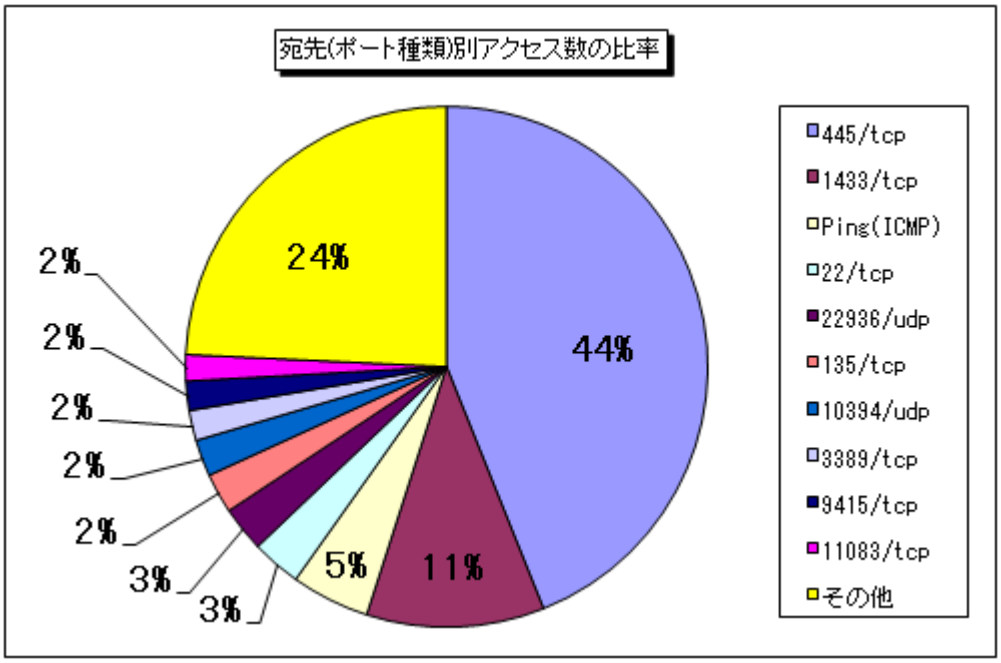

図 2-3：宛先（ポート種類）別アクセス数の比率

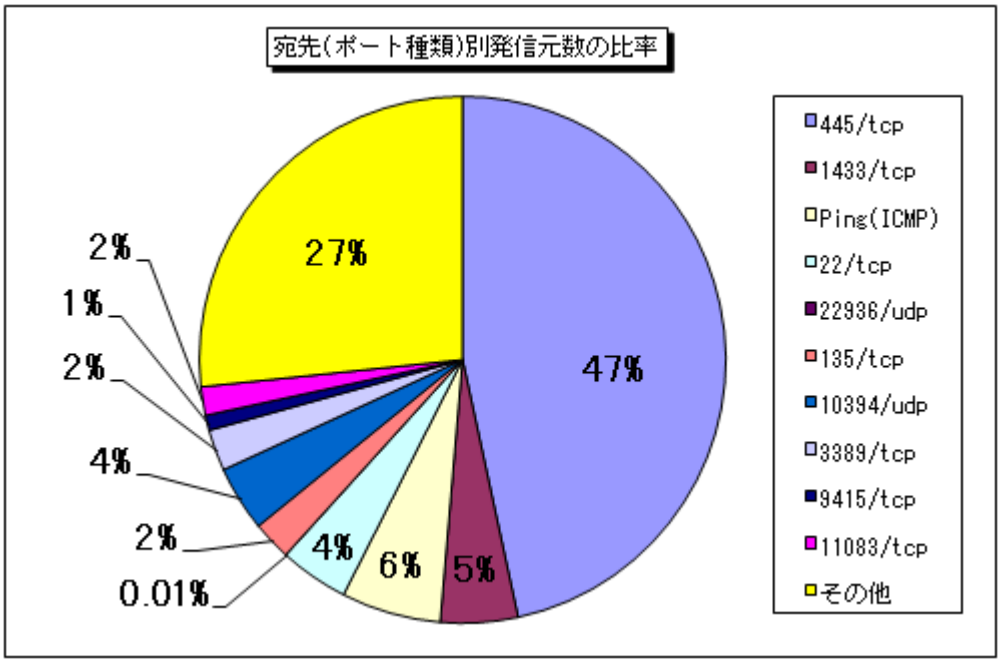

図 2-4：宛先（ポート種類）別発信元数の比率

（3）発信元地域別のアクセス状況

2011 年 8 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。

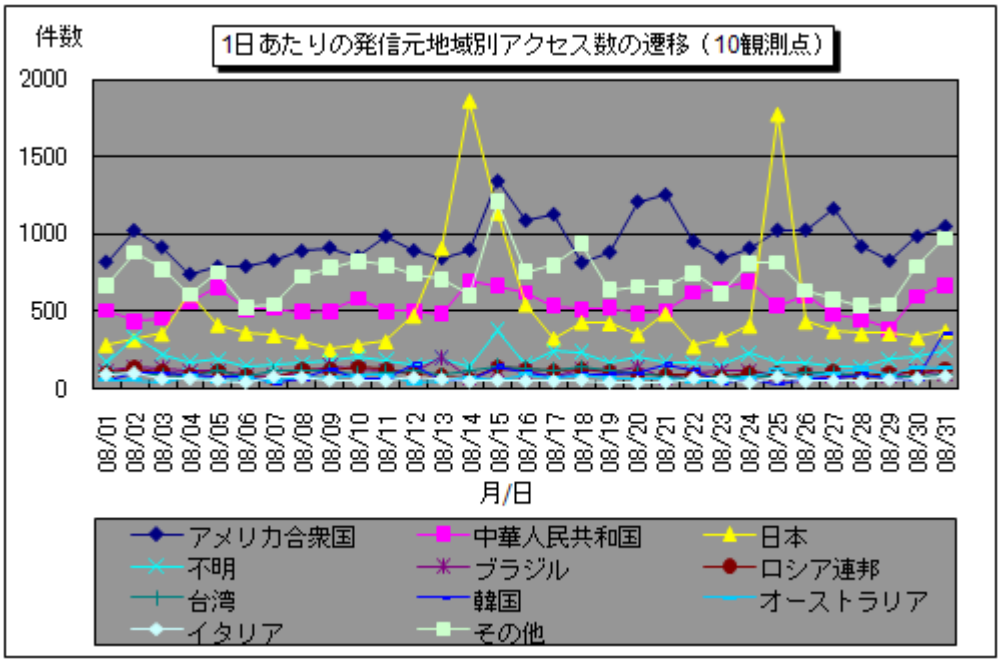

図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）

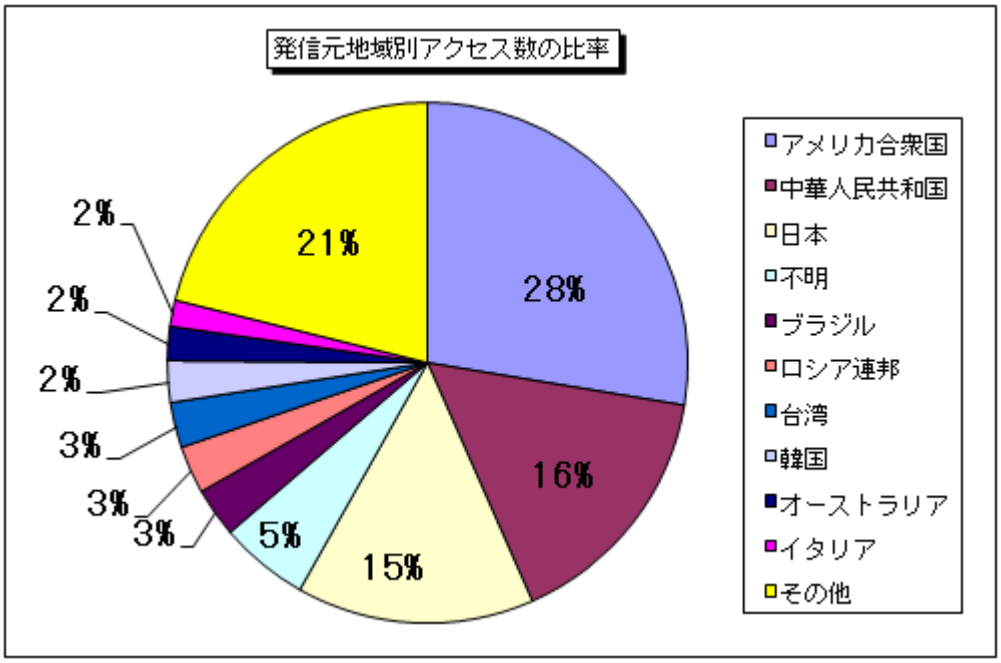

図 2-6：発信元地域別アクセス数の比率

2011 年 8 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。

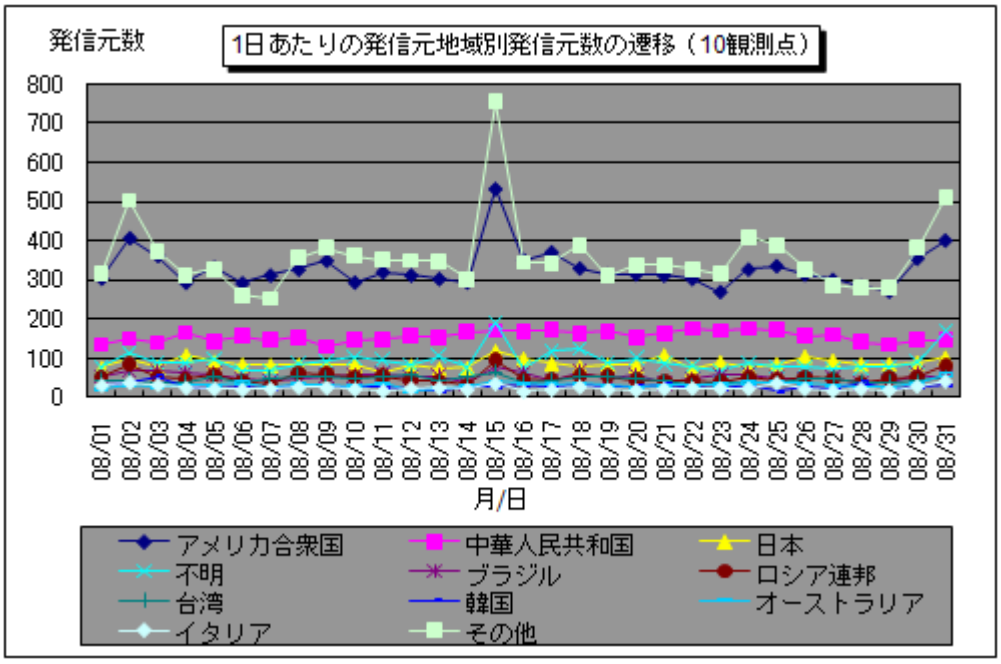

図 2-7： 1 日あたりの発信元地域別発信元数の遷移（10 観測点）

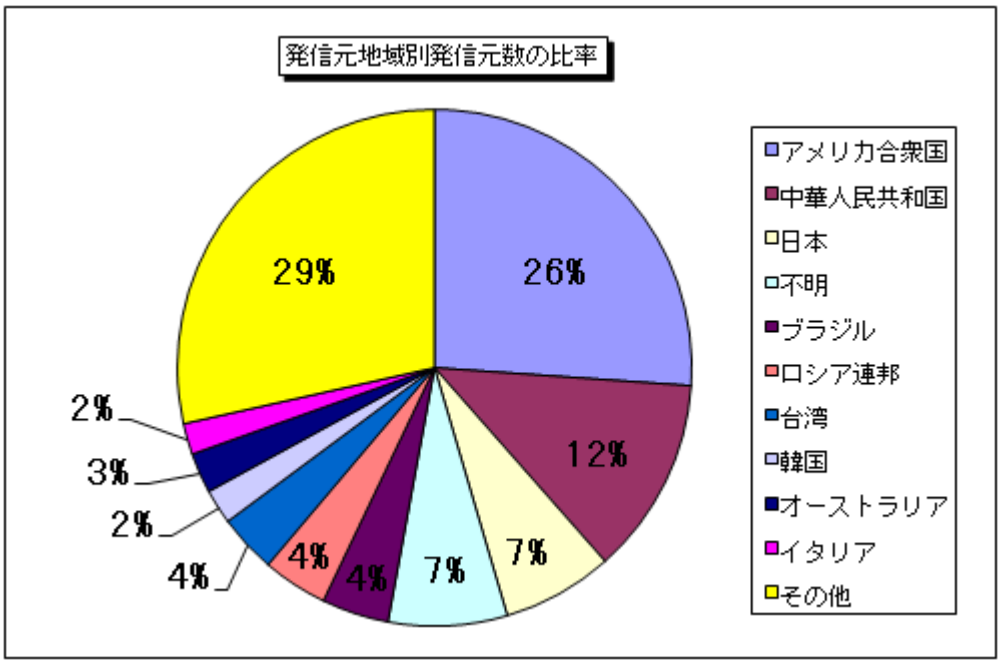

図 2-8：発信元地域別発信元数の比率

3. 統計情報

（1）宛先（ポート種類）別の比率

2011 年 3 月～2011 年 8 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。

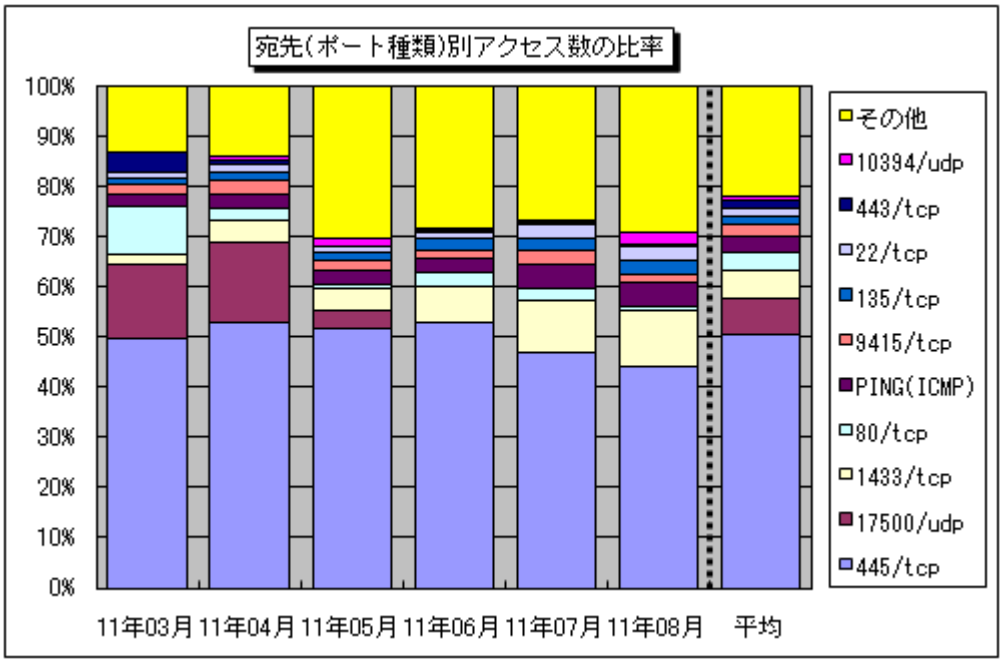

図 3-1：宛先（ポート種類）別アクセス数の比率

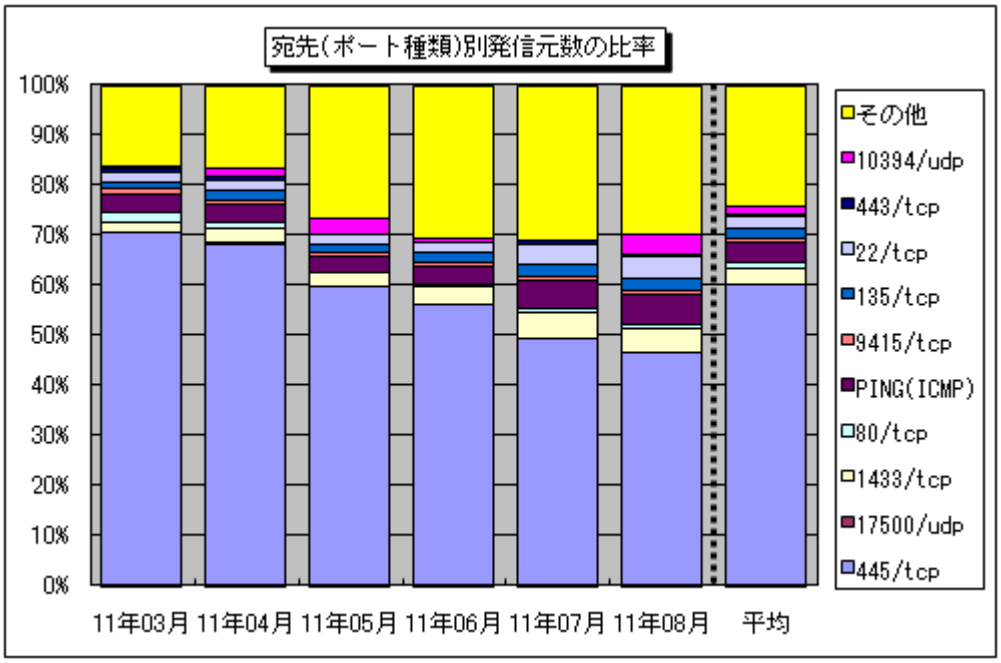

図 3-2：宛先（ポート種類）別発信元数の比率

（2）発信元地域別の比率

2011 年 3 月～2011 年 8 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。

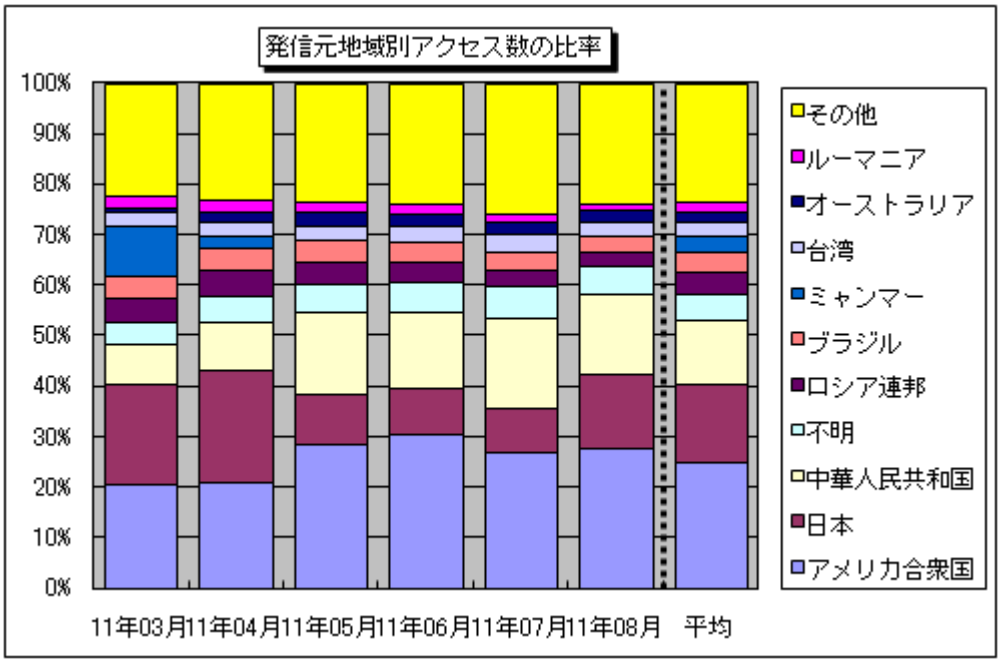

図 3-3：発信元地域別アクセス数の比率

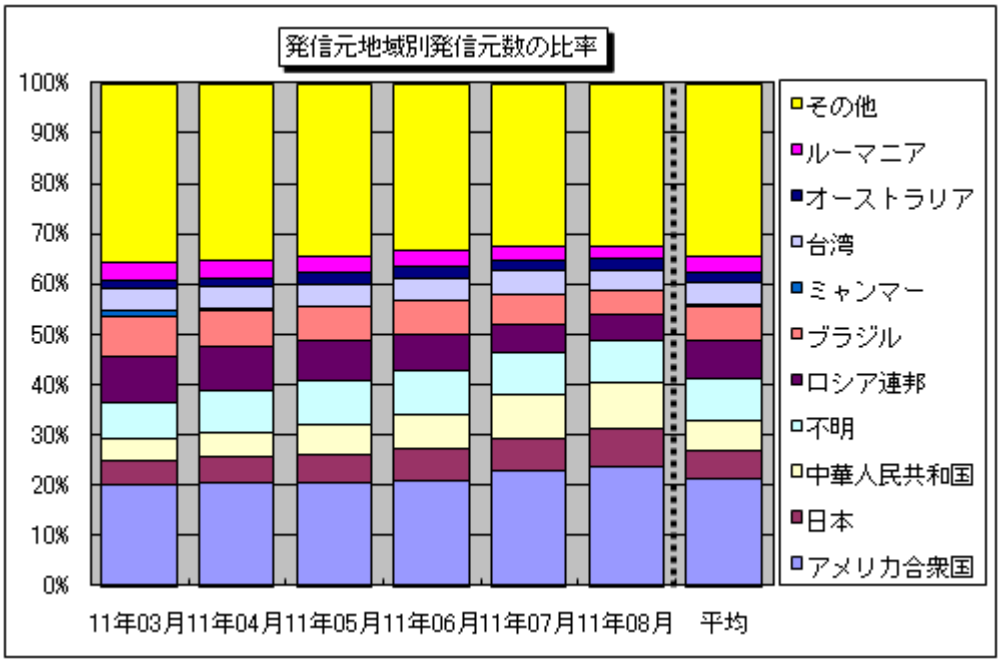

図 3-4：発信元地域別発信元数の比率

4. 補足説明

以下に、2011 年 8 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。
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）を狙ったアクセスである可能性が高い。
22936/udp	TALOT2の1観測点のみに観測された、原因不明のアクセス。
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）。
10394/udp	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。
9415/tcp	中国のあるサイトで公開されているプロキシ機能を持つソフトがインストールされているパソコンを、ウェブサーバ等への攻撃に使うために、探索している可能性のあるアクセス。
11083/tcp	主にアメリカと中国の発信元（IP アドレス）から、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 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