

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**102,888件**、延べ発信元数[※]は**46,222箇所**ありました。平均すると、**1観測点につき1日あたり154の発信元から343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向的アクセスがあると考えられます。

※7月2日は保守作業のため、システムを停止しています。そのため、7月の観測データは、この1日を除外して統計情報を作成しています。なお、通常は常時稼働しています。

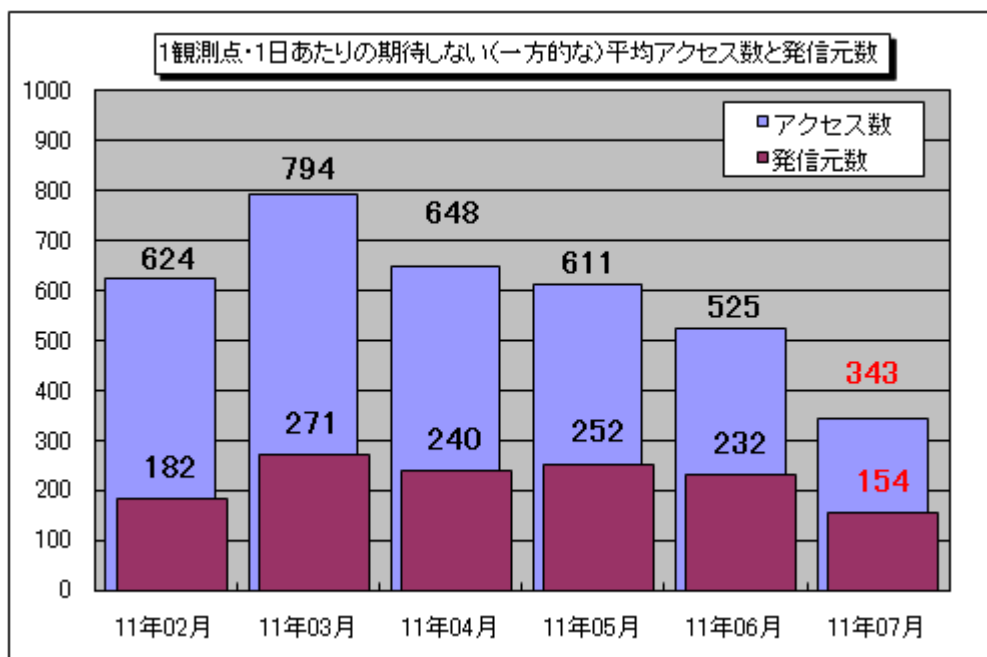


図1-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数

2011年2月～2011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月と比べて大きく減少しました。

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。445/tcpが大きく減少したにもかかわらず、増加が観測されたのは11083/tcpからのアクセスでした。

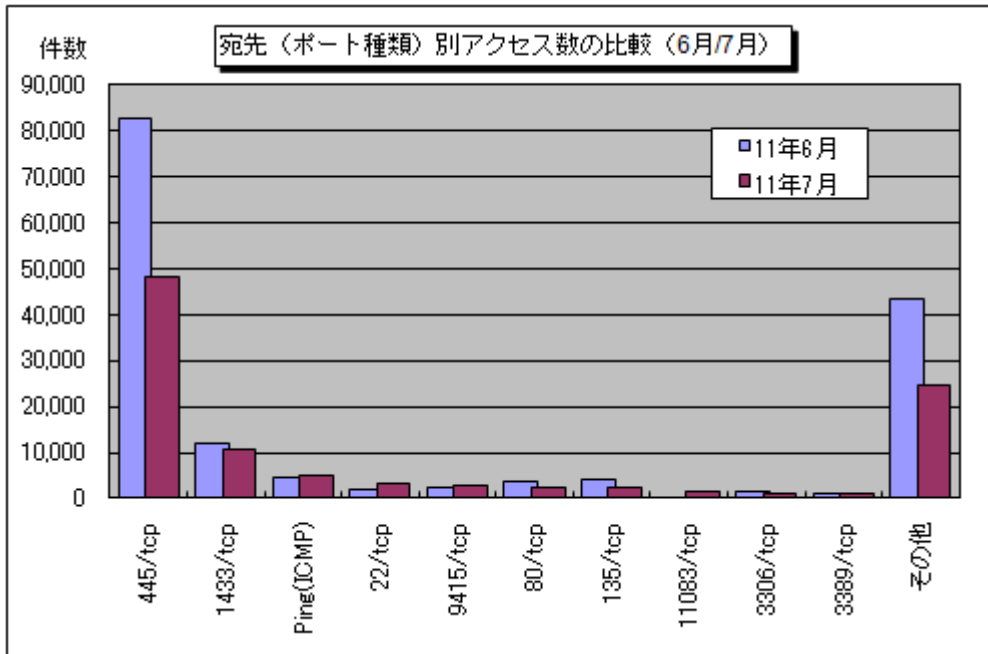


図 1-2 : 宛先 (ポート種類) 別アクセス数の比較 (6月/7月)

11083/tcp は、7月3日以降に TALOT2 の特定の1観測点で観測され始めたアクセスであり、発信元地域はアメリカと中国が大部分を占めていました (図 1-3 参照)。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。

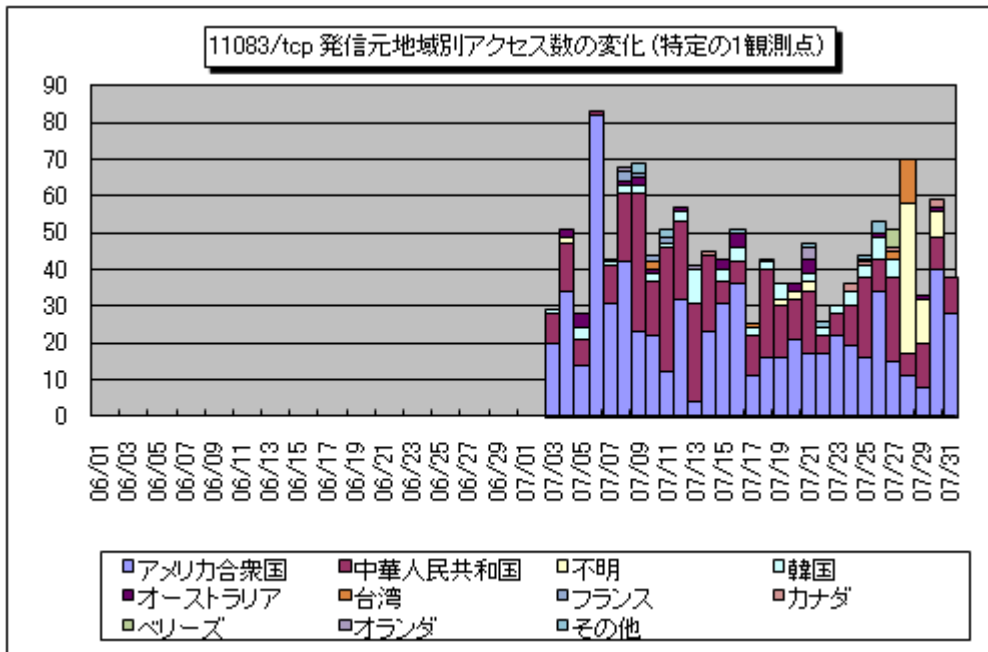


図 1-3 : 11083/tcp 発信元地域別アクセス数の変化 (特定の1観測点)

2. 2011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

2011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。

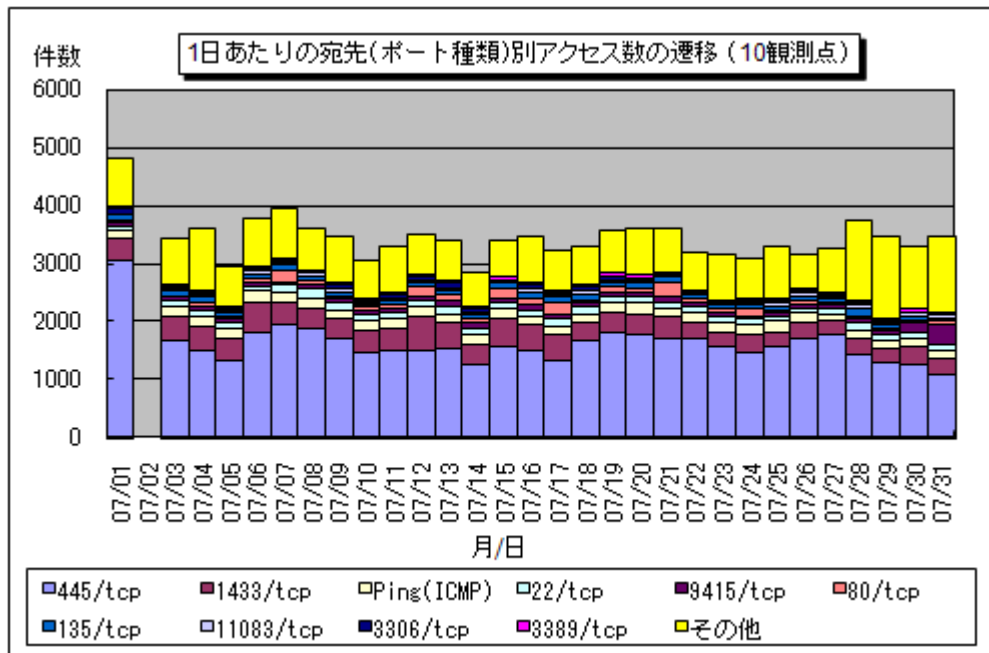


図 2-1：1日あたりの宛先（ポート種類）別アクセス数の遷移（10観測点）

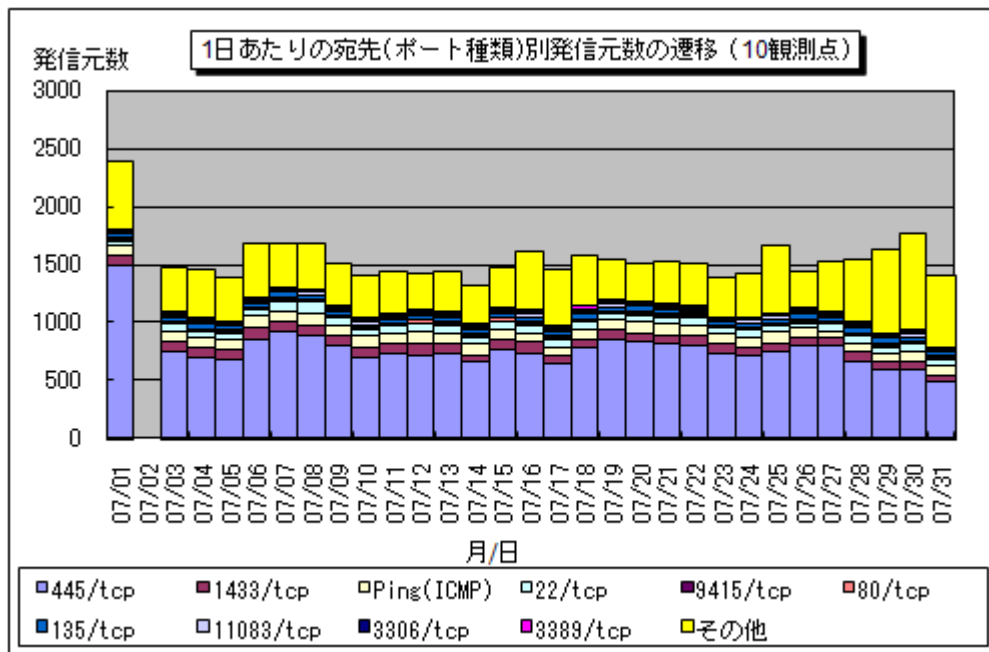


図 2-2：1日あたりの宛先（ポート種類）別発信元数の遷移（10観測点）

(2) 宛先（ポート種類）別の比率

2011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。

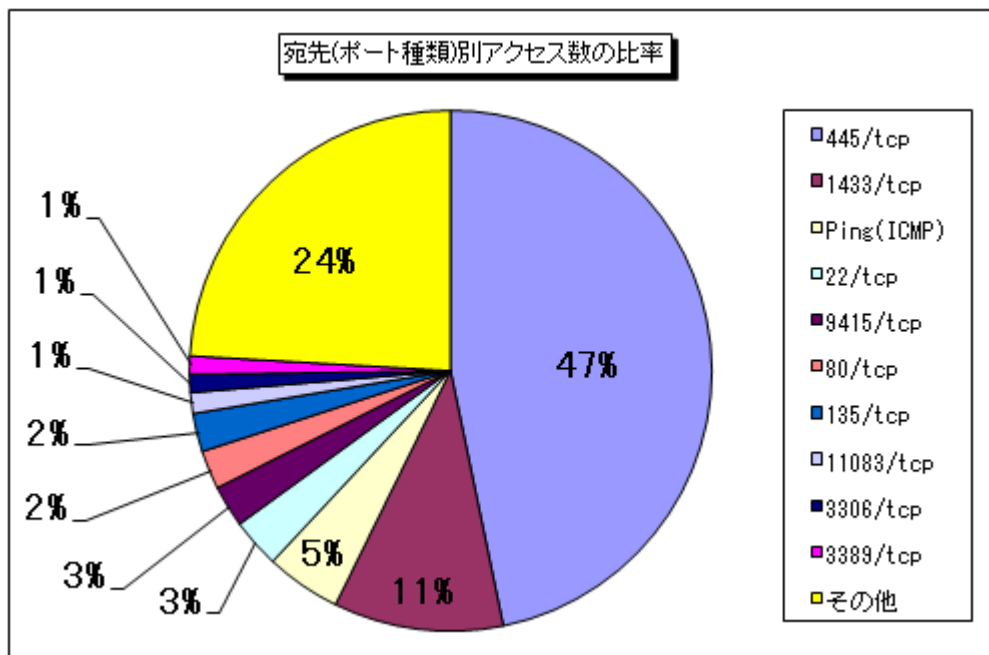


図 2-3：宛先（ポート種類）別アクセス数の比率

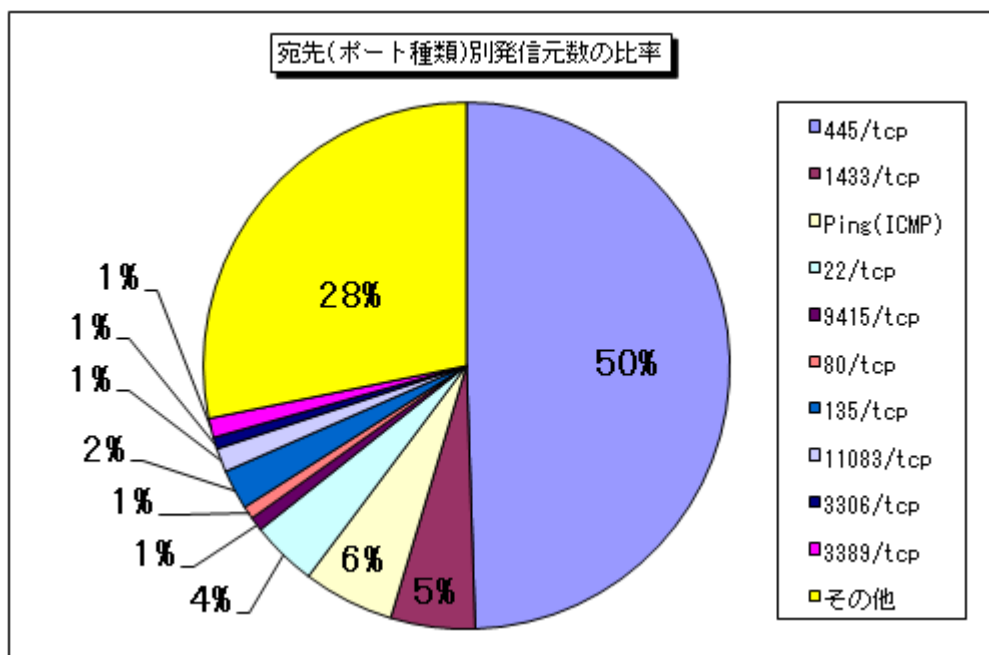


図 2-4：宛先（ポート種類）別発信元数の比率

(3) 発信元地域別のアクセス状況

2011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。

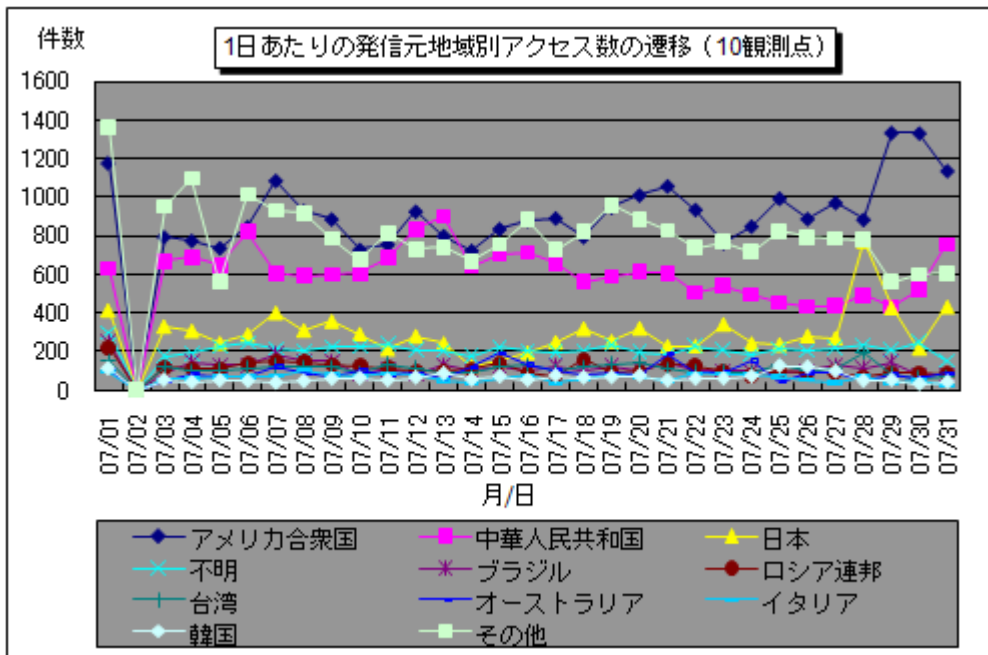


図 2-5 : 1日あたりの発信元地域別アクセス数の遷移 (10 観測点)

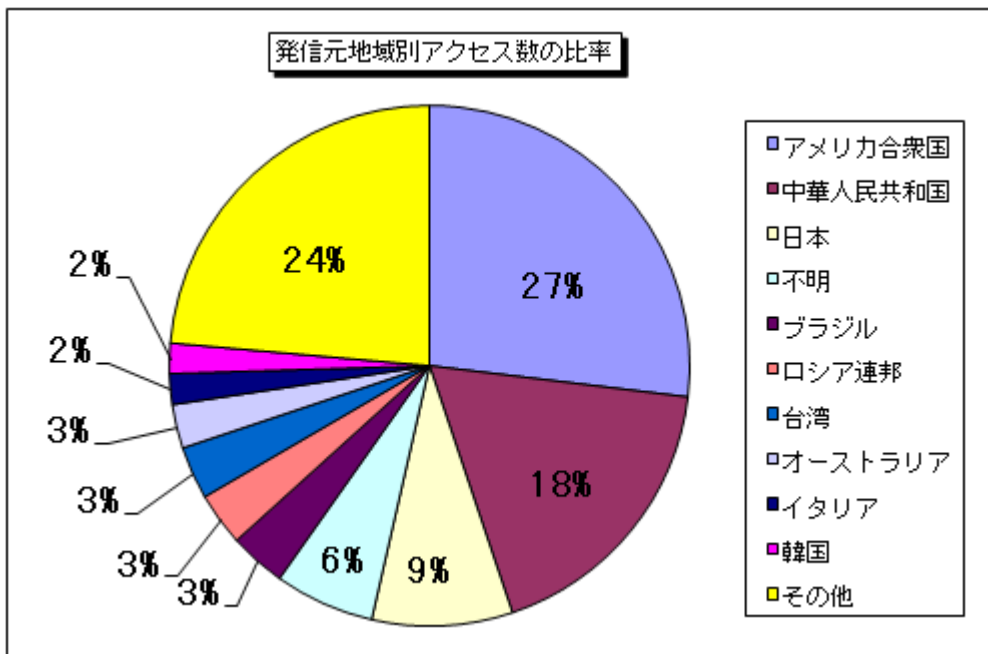


図 2-6 : 発信元地域別アクセス数の比率

2011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。

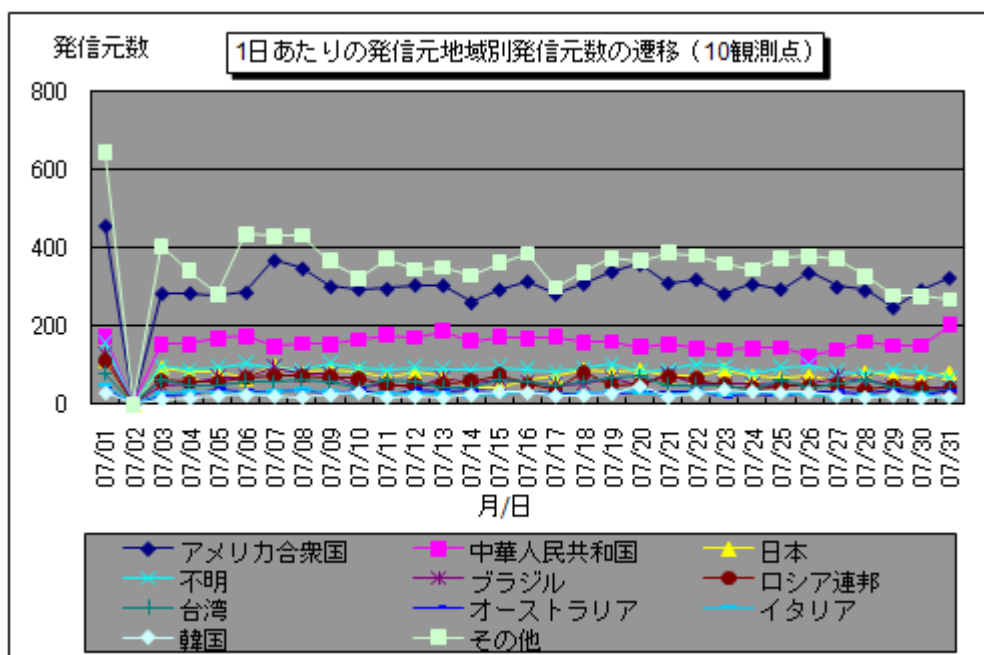


図 2-7： 1日あたりの発信元地域別発信元数の遷移 (10 観測点)

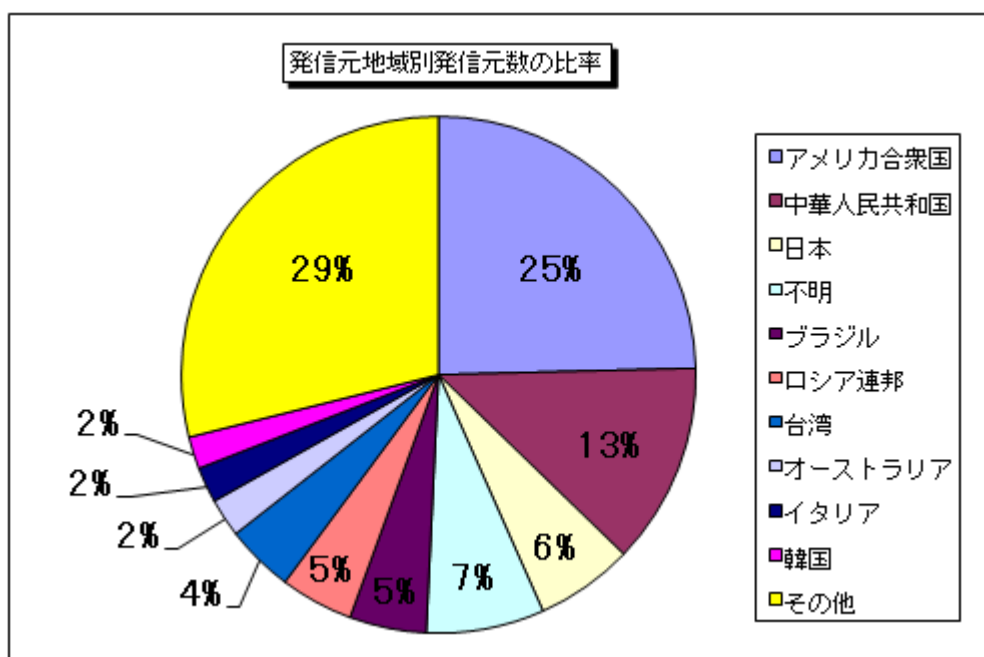


図 2-8： 発信元地域別発信元数の比率

3. 統計情報

(1) 宛先（ポート種類）別の比率

2011年2月～2011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。

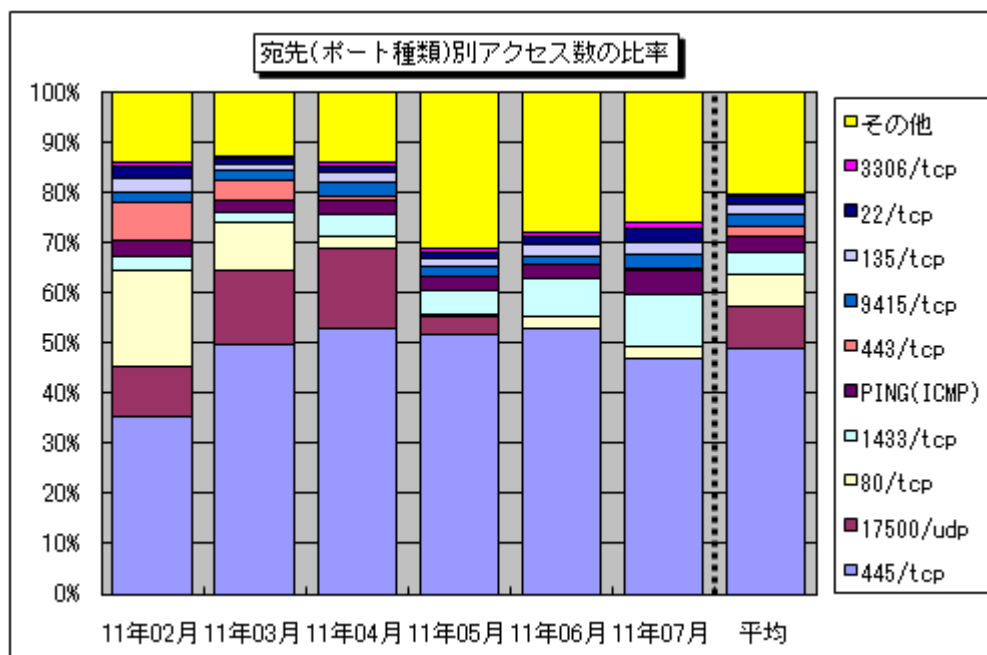


図 3-1：宛先（ポート種類）別アクセス数の比率

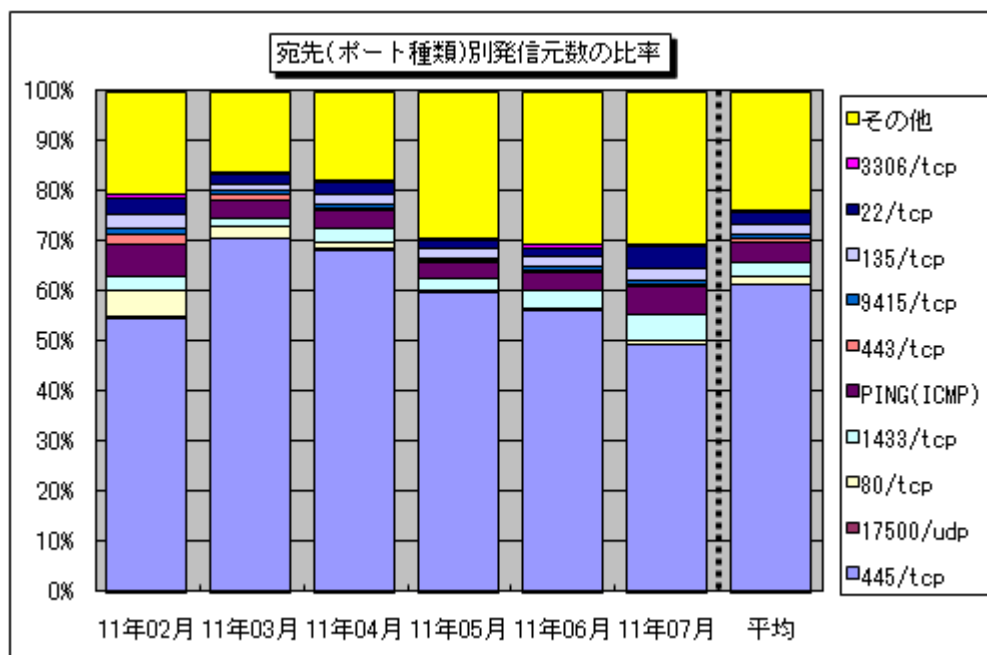


図 3-2：宛先（ポート種類）別発信元数の比率

(2) 発信元地域別の比率

2011年2月～2011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。

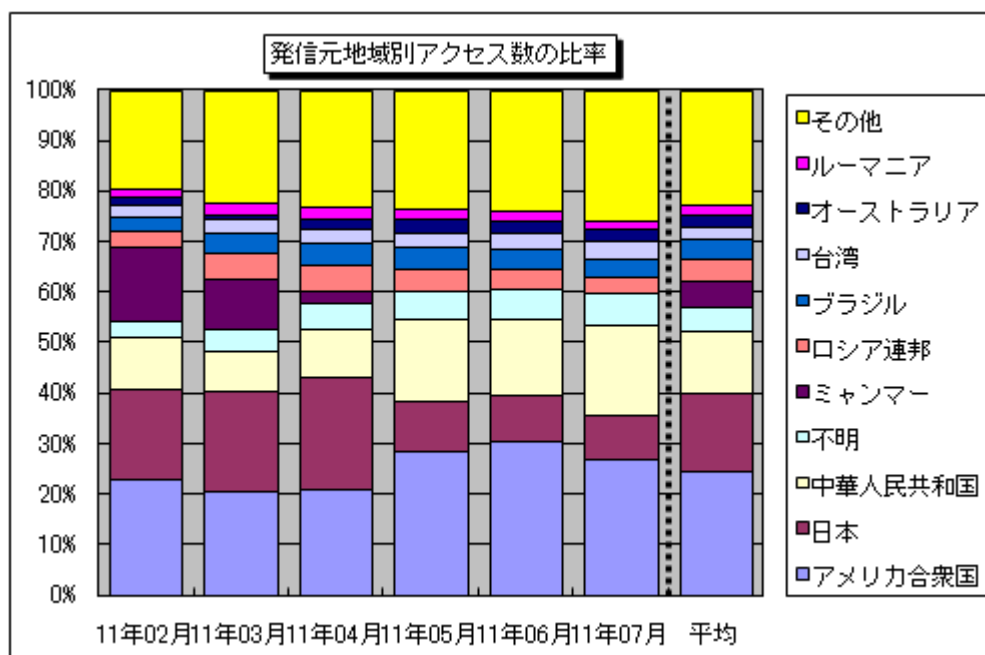


図 3-3：発信元地域別アクセス数の比率

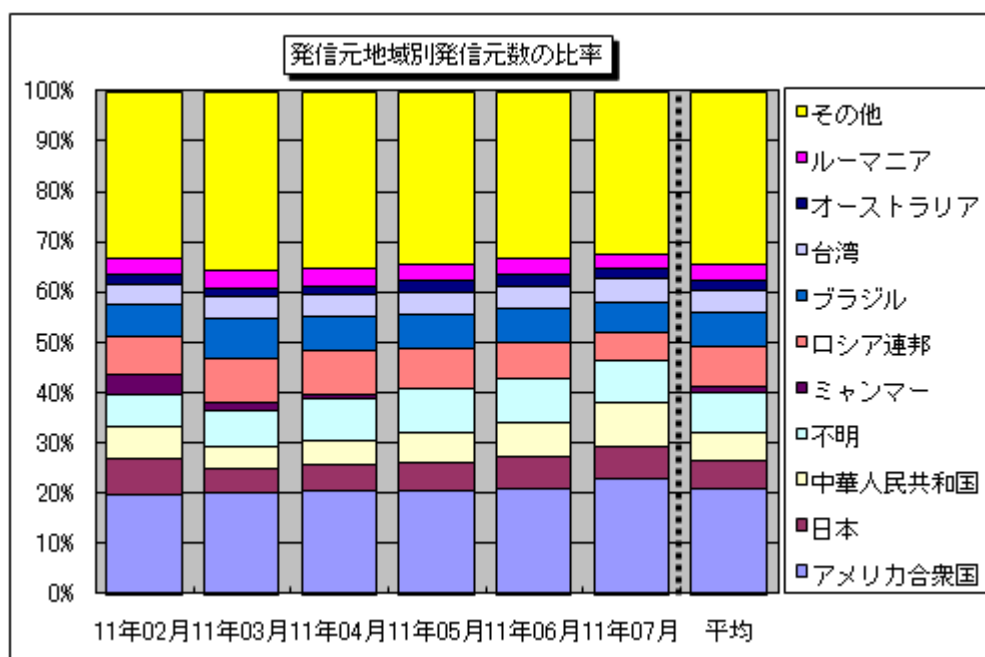


図 3-4：発信元地域別発信元数の比率

4. 補足説明

以下に、2011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 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。
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。
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。
80/tcp	ウェブアクセスのプロトコルであるHTTPが使うポートであり、ウェブアプリケーションの脆弱性を狙ったアクセスやDoS攻撃に用いられる可能性が高い。
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）。
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。
3306/tcp	MySQL Serverの既定ポートであり、このポートへのアクセスは、MySQL Serverが動作中のコンピュータを探す目的や、MySQL Serverの脆弱性を狙ったアクセスである可能性が高い。
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、この機能を狙った何らかのアクセスである可能性がある。

■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