

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12月の期待しない（一方的な）アクセスの総数は10観測点で81,017件、延べ発信元数※は30,870箇所ありました。平均すると、1観測点につき1日あたり144の発信元から324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。

※12月26日～31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、12月の観測データは、この6日を除外して統計情報を作成しています。

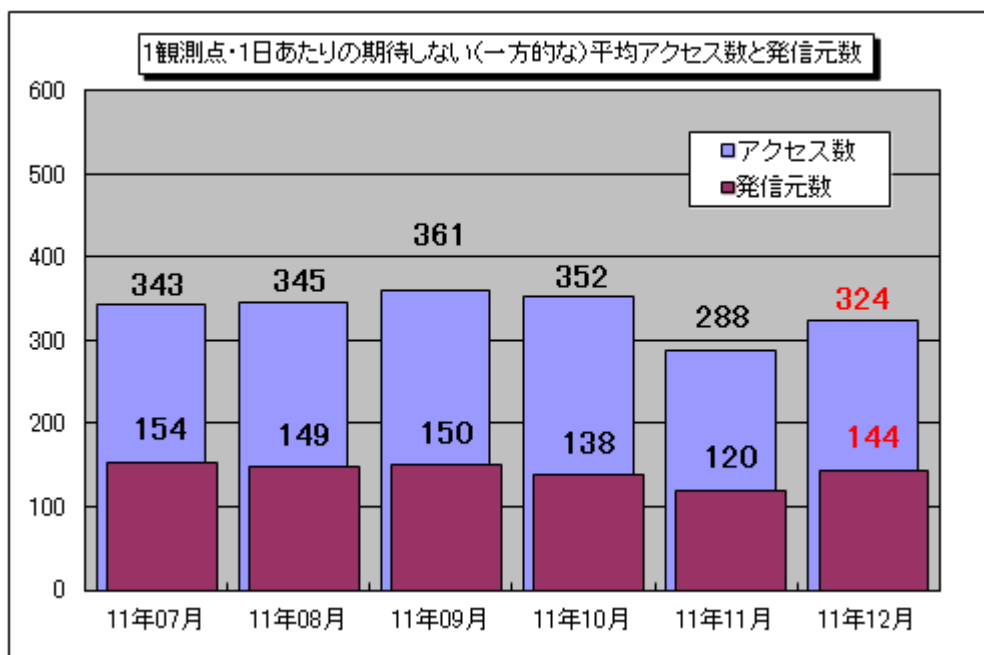


図1-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは2011年7月～2011年12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。12月の期待しない（一方的な）アクセスは、11月と比べて増加しました。

11月と12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、11月は少なかった24529/tcpや8612/tcpへのアクセスが、12月は増加していました。

24529/udp、および8612/udpについては、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が、ともに特定の1観測点のみで観測されていました。

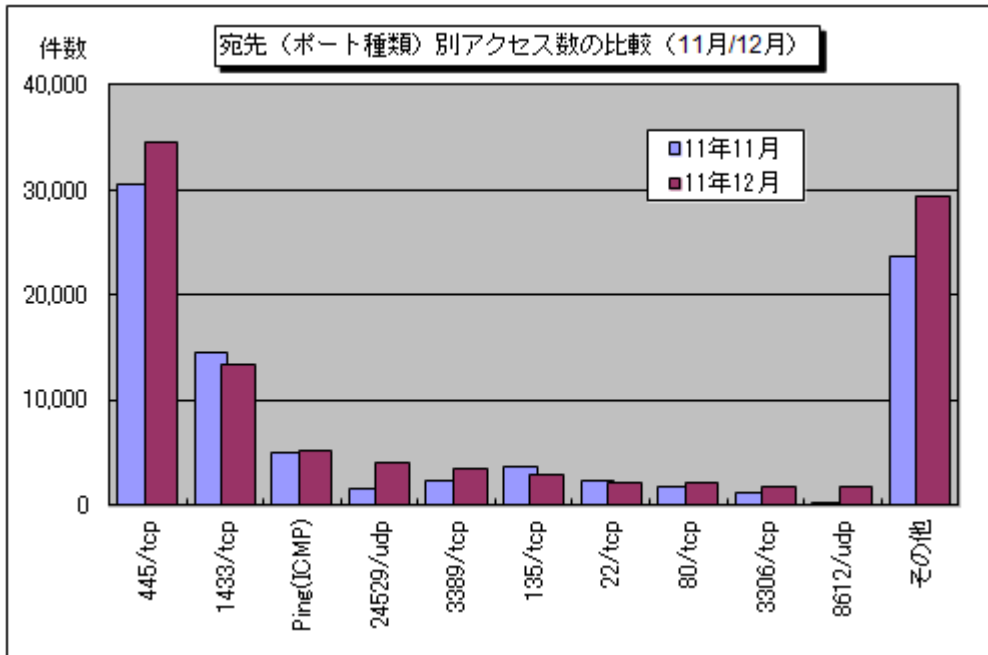


図 1-2：宛先（ポート種類）別アクセス数の比較（11月/12月）

(1) 2011年のアクセス状況

2011年1月～2011年12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1-3に示します。アクセス数について年間を通してみると、1月から3月にかけて大幅に増加したのち減少し、7月以降はそれほど大きな変化もなく推移していました。

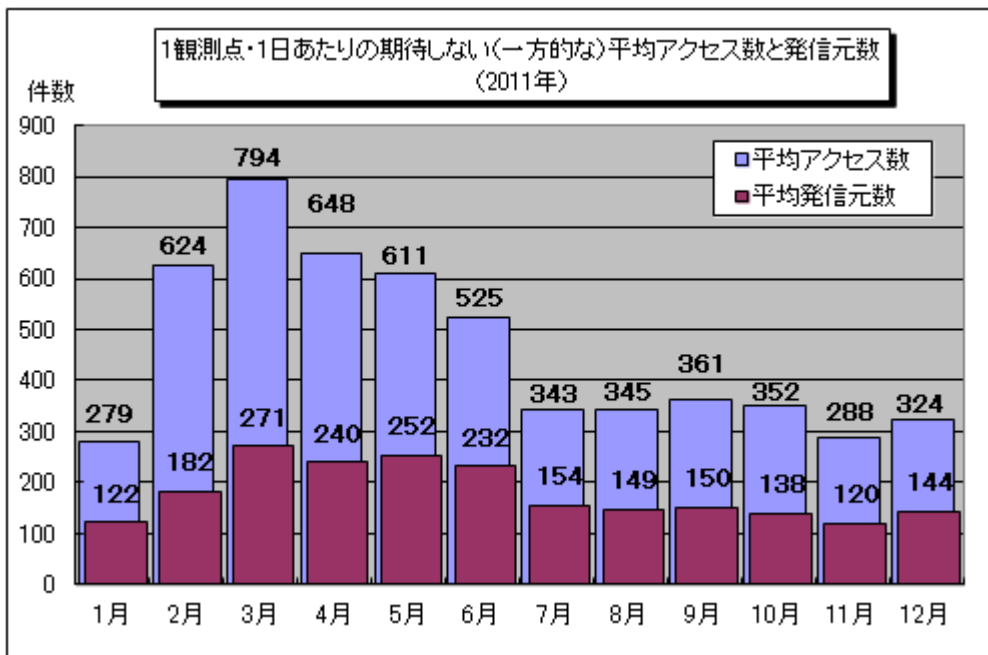


図1-3：1観測点・1日あたりの期待しない(一方的な)平均アクセス数と発信元数（2011年）

図1-3の平均アクセス数を宛先（ポート種類）別で表したものを図1-4に示します。これをみると、2011年は445/tcpへのアクセスが年間を通して支配的でした。また、2011年の上半期に全体のアクセス数が増加していたのは、2月～6月にかけて445/tcpへのアクセスが増加していたことと、2月～4月に17500/udpへのアクセスが増加していたことと、2月と3月に80/tcp、443/tcpへのアクセスが増加していたことが主な要因と言えます。

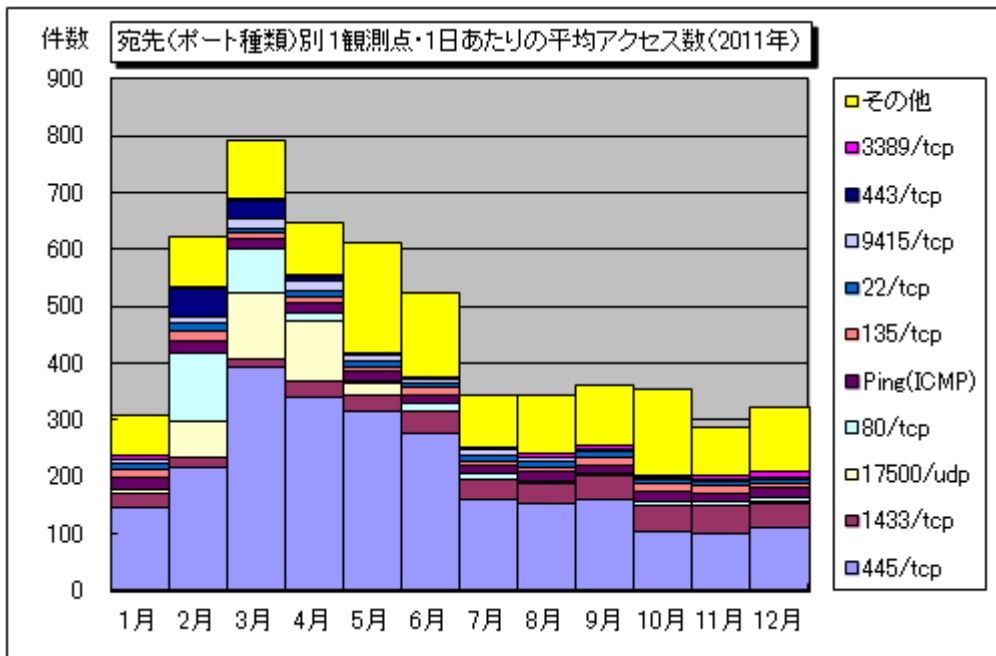


図1-4：宛先（ポート種類）別 1観測点・1日あたりの平均アクセス数（2011年）

次に、2010年と2011年の宛先（ポート種類）別アクセス数の比較を図1-5に示します。2010年からアクセス数が増加したのは445/tcp、1433/tcp、17500/udp、80/tcp、443/tcpなどであり、445/tcpは約26千件の増加、1433/tcpは約47千件の増加、17500/udpは約49千件の増加、80/tcpは約64千件の増加、443/tcpは約24千件の増加でした。

逆に減少したのはPing（ICMP）、135/tcpなどであり、Ping（ICMP）は約23千件の減少、135/tcpは44千件の減少でした。

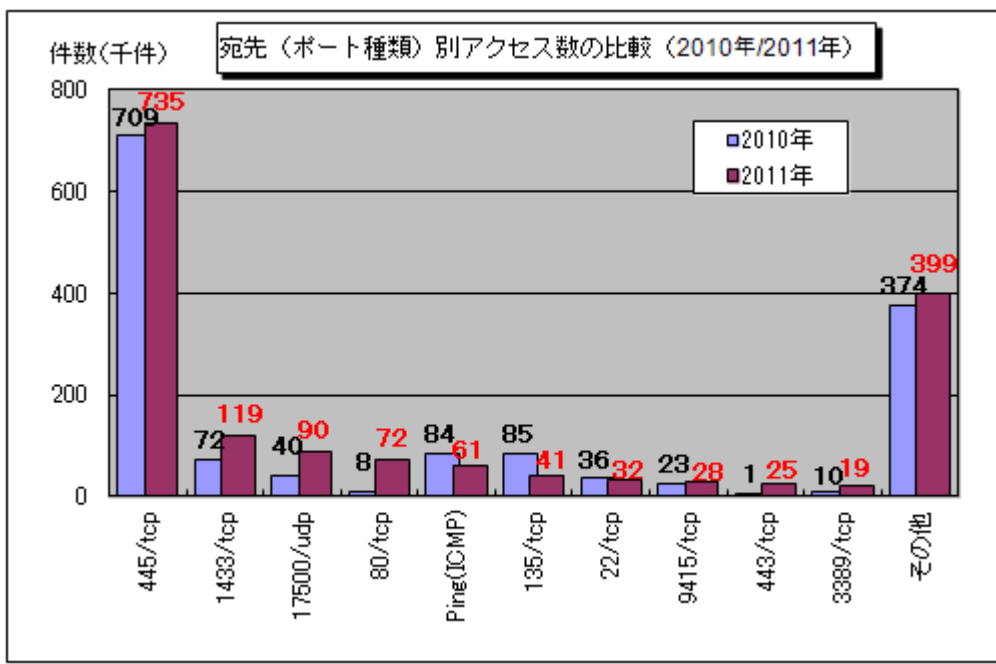


図1-5：宛先（ポート種類）別アクセス数の比較（2010年/2011年）

2011年のTALOT2のアクセス状況において特徴的だったのは、2011年の上半期の445/tcp、17500/udp、80/tcpなどへのアクセスの増加でした。

2011年1月～7月の445/tcp発信元地域別アクセス数の変化を図1-6に示します。

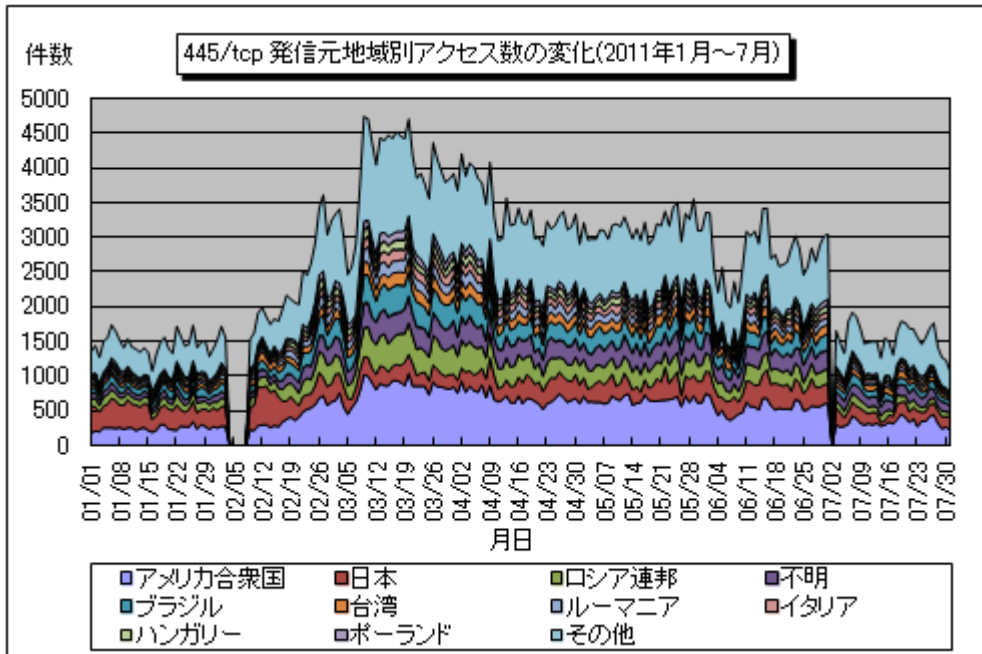


図 1-6 : 445/tcp への発信元地域別アクセス数の変化 (2011 年 1 月~7 月)

17500/udp へのアクセスの特徴としては、TALOT2 の特定の 1 観測点に対して、同一セグメント内の複数の IP アドレスから規則的な間隔で送られていたという点が挙げられます。このアクセスについて調査したところ、17500/udp に対してブロードキャストを送信するアプリケーションが存在することが分かりました。そのアプリケーションを使っているパソコンからのブロードキャストが TALOT2 の観測点に届いていた可能性があります。なお、他の観測点はブロードキャストが端末に到達しない仕様のようなので、当該アクセスは観測されませんでした。2011 年 1 月~5 月の 17500/tcp 発信元地域別アクセス数の変化を図 1-7 に示します。

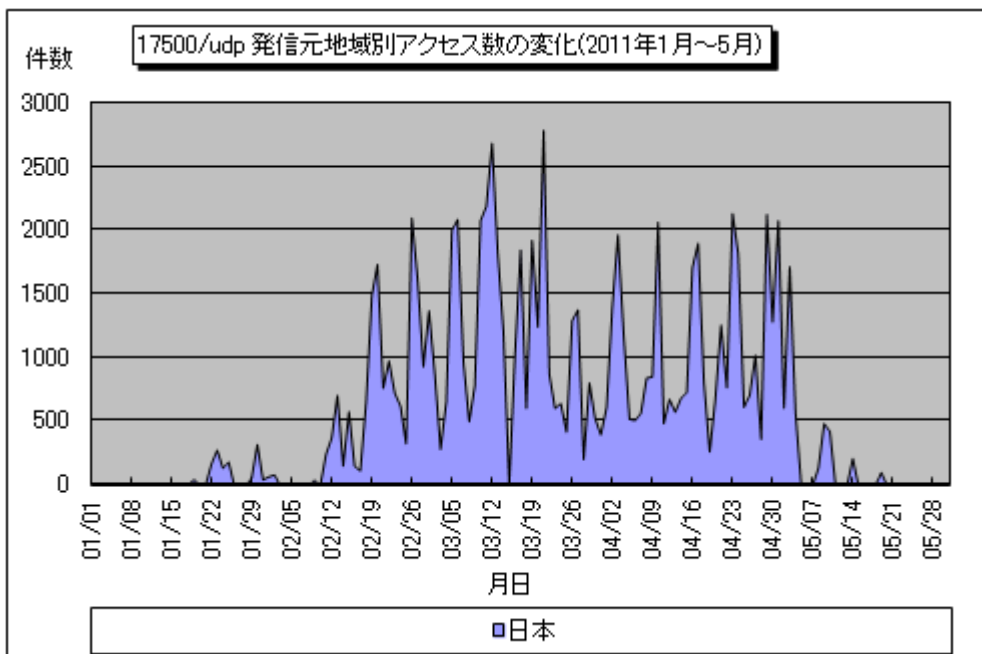


図 1-7 : 17500/udp への発信元地域別アクセス数の変化 (2011 年 1 月~5 月)

80/tcp と 443/tcp へのアクセスについては、2 月から 3 月にかけて、ミャンマーの IP アドレスから TALOT2 の複数の観測点にアクセスの増加を観測しました。この現象は定点観測を行っている他の組織でも観測されていたため、比較的広範囲に発生していた可能性があります。これらのアクセスがこの時期に増加した原因は不明ですが、80/tcp に関しては、CMS*の脆弱性を悪用した攻撃に使われる可能性があるため、脆弱性が解消されていないウェブサイトの探索を目的としたアクセスだった可

能性があります。

2011年2月～4月のミャンマーのIPアドレスからの80/tcp、443/tcpへのアクセス数の変化を図1-8に示します。

※CMS（Contents Management System）：ウェブコンテンツを構成するデータを一元的に保存・管理するシステムのこと。

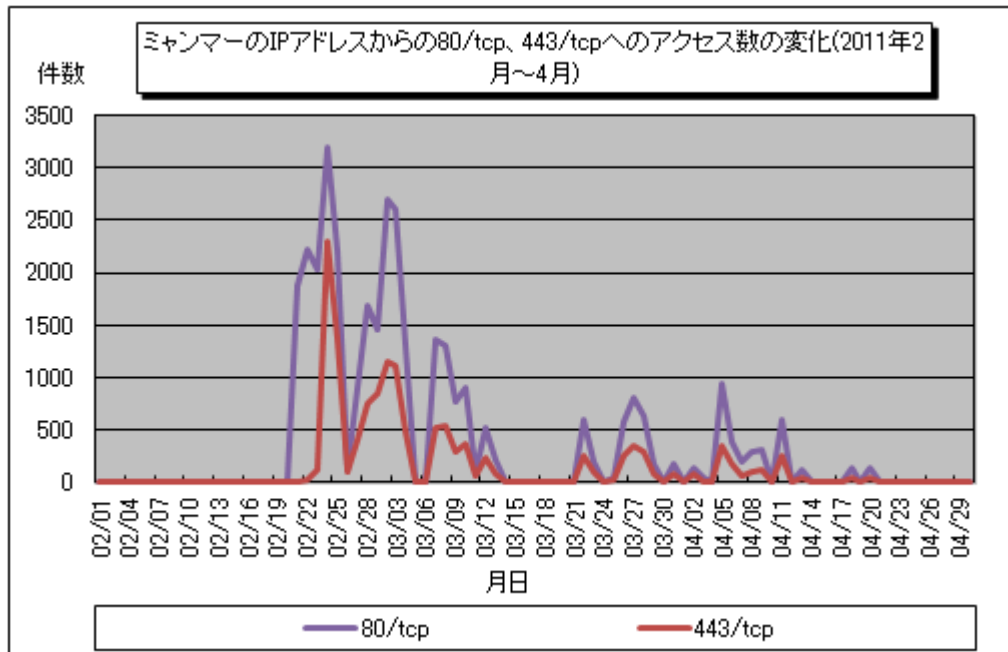


図 1-8 : ミャンマーの IP アドレスからの 80/tcp、443/tcp へのアクセス数の変化 (2011 年 1 月～4 月)

2. 2011年12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12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。

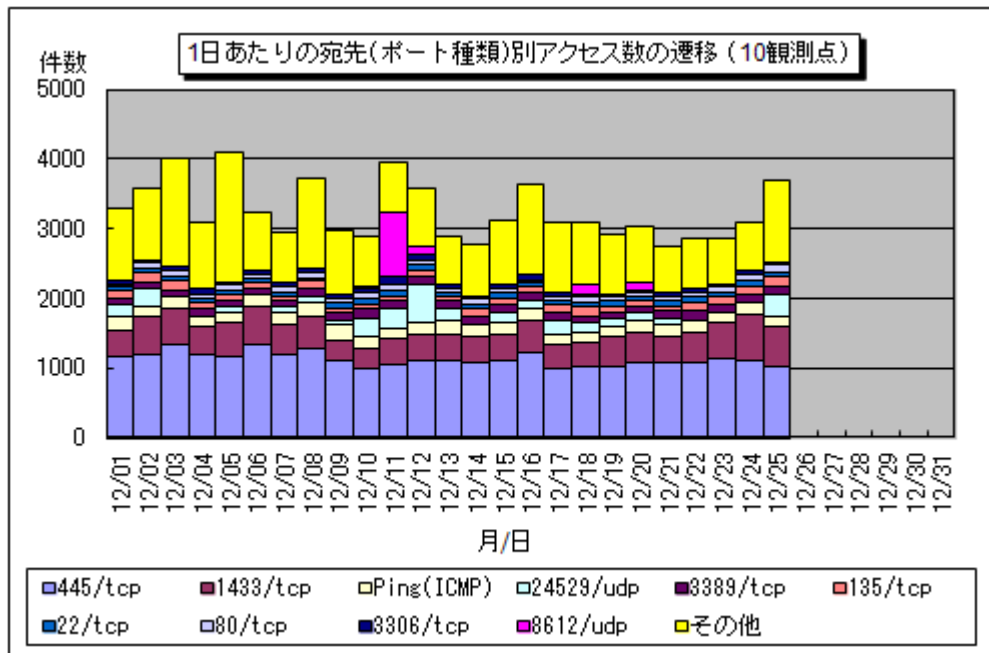


図 2-1 : 1日あたりの宛先（ポート種類）別アクセス数の遷移（10観測点）

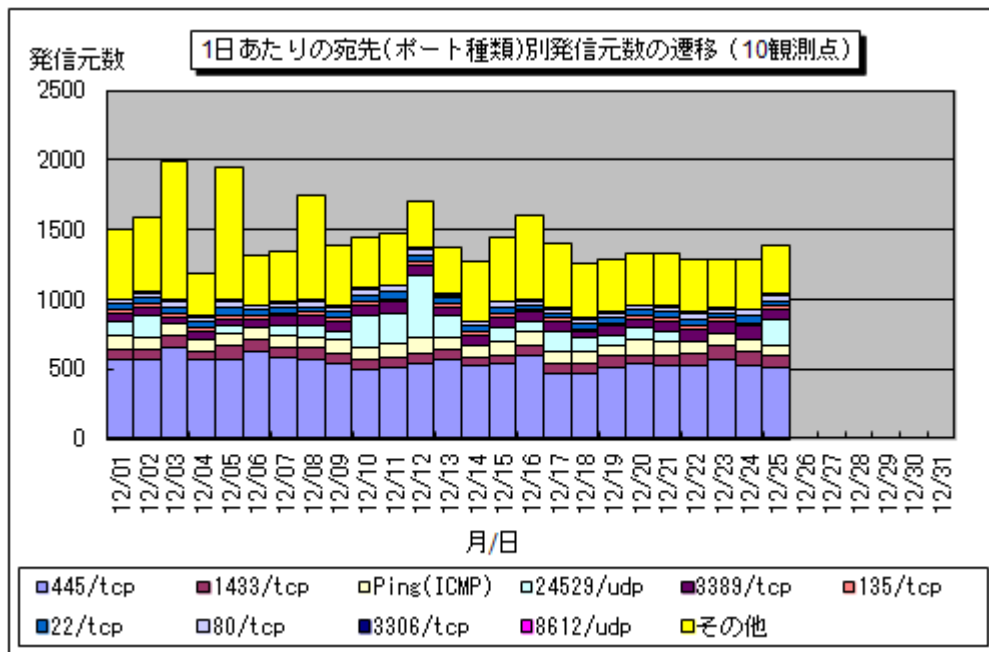


図 2-2 : 1日あたりの宛先（ポート種類）別発信元数の遷移（10観測点）

(2) 宛先（ポート種類）別の比率

2011年12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。

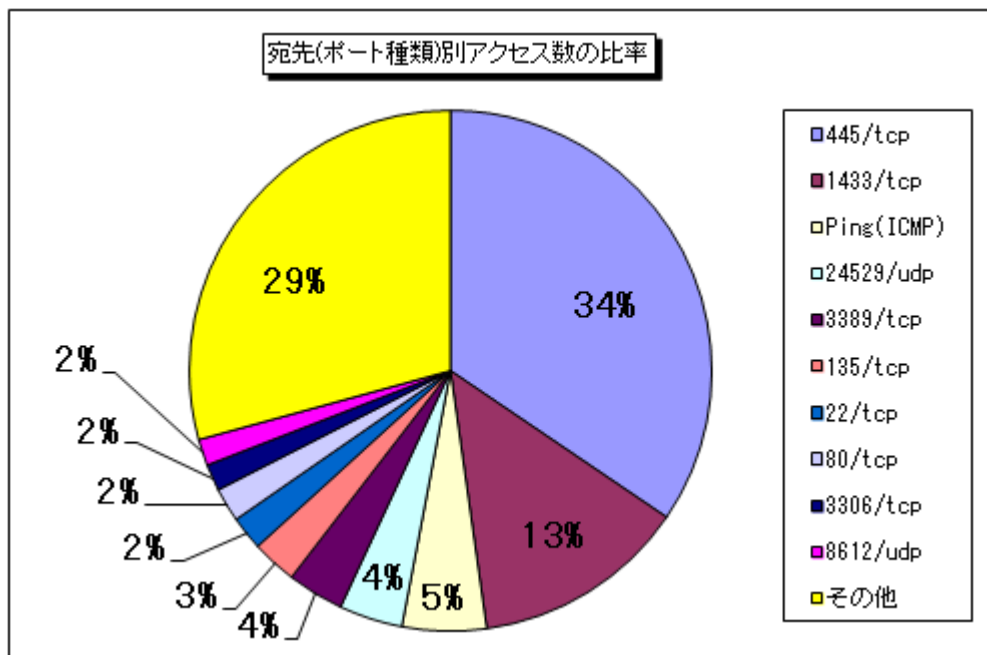


図 2-3：宛先（ポート種類）別アクセス数の比率

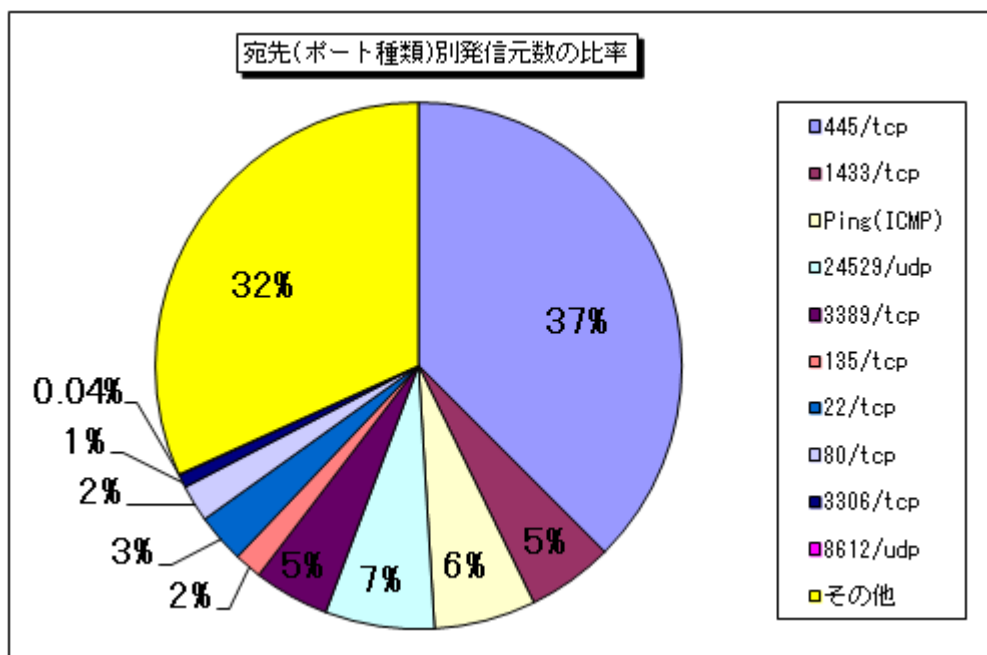


図 2-4：宛先（ポート種類）別発信元数の比率

(3) 発信元地域別のアクセス状況

2011年12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。

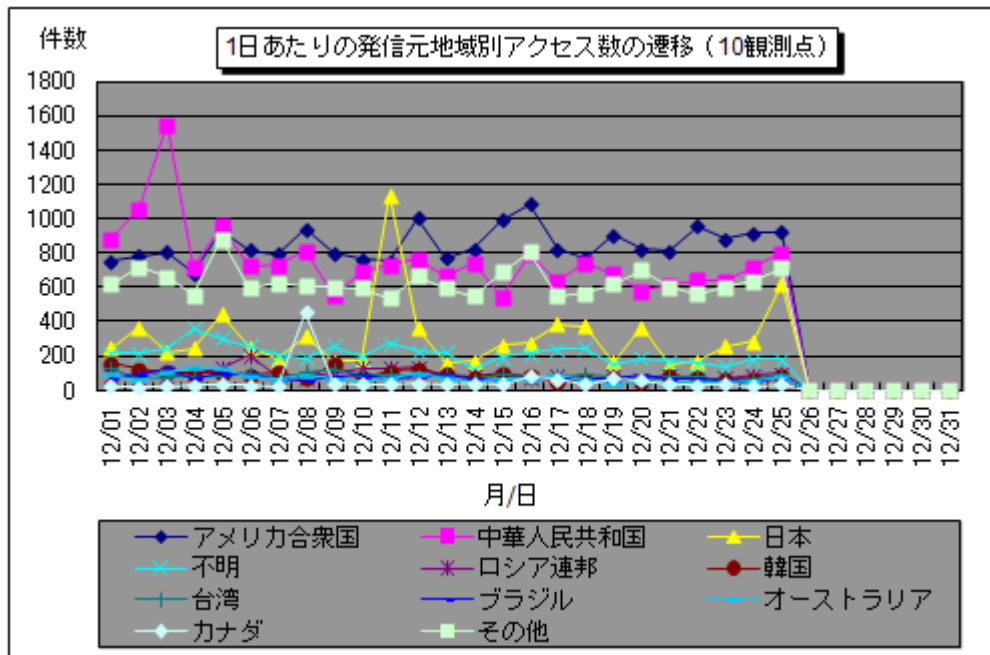


図 2-5 : 1日あたりの発信元地域別アクセス数の遷移 (10観測点)

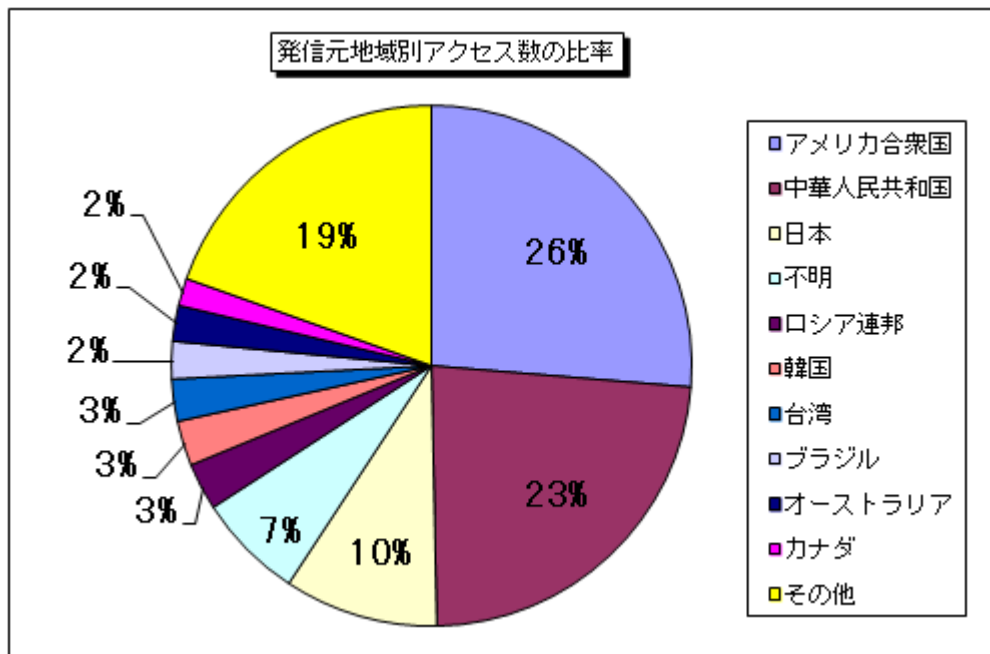


図 2-6 : 発信元地域別アクセス数の比率

2011年12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。

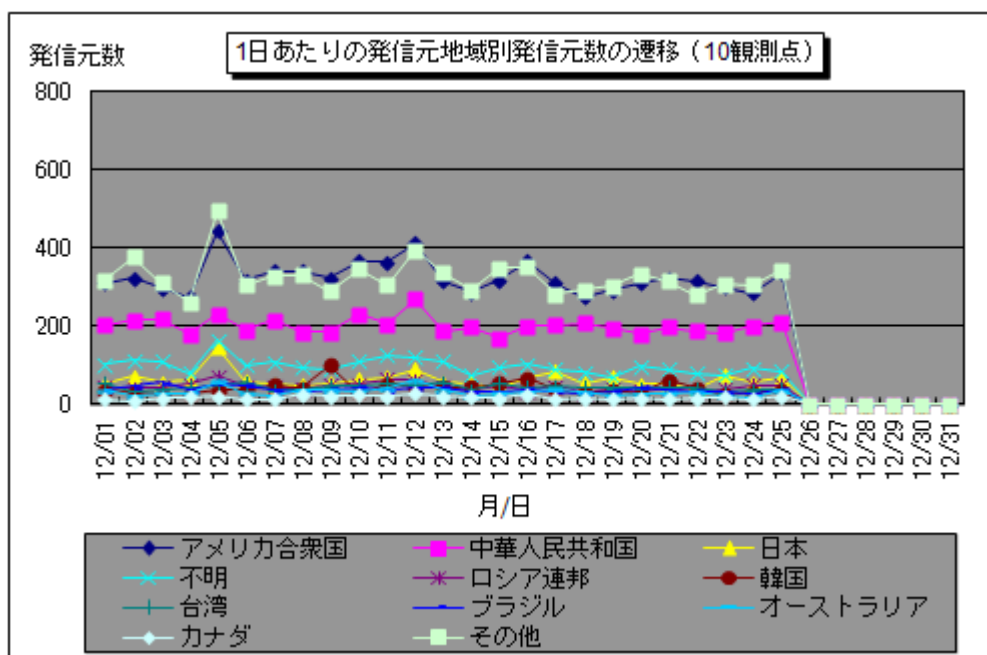


図 2-7： 1日あたりの発信元地域別発信元数の遷移（10観測点）

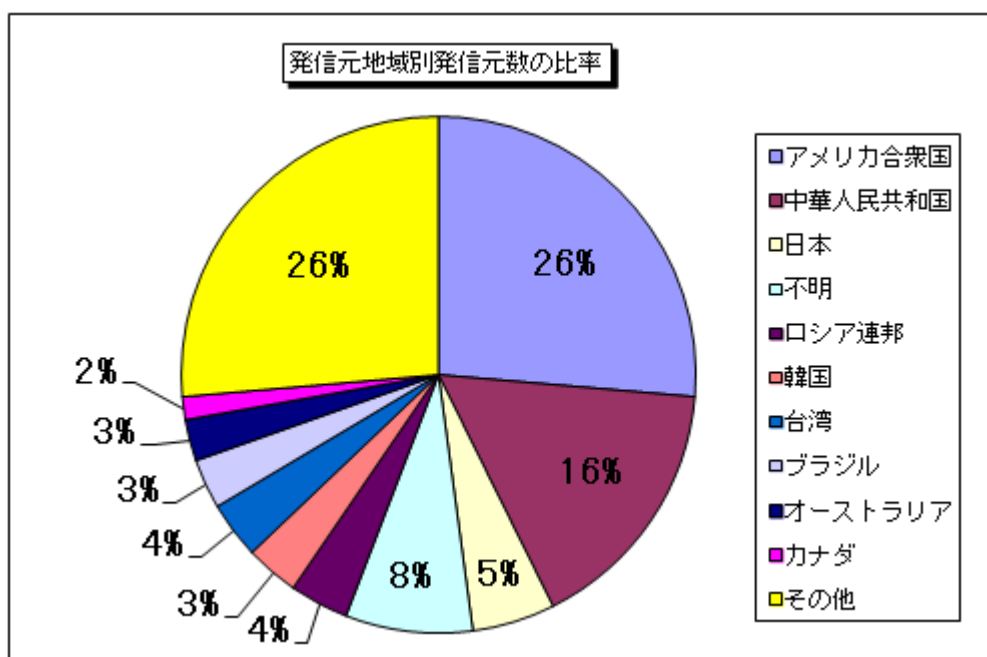


図 2-8： 発信元地域別発信元数の比率

3. 統計情報

(1) 宛先（ポート種類）別の比率

2011年7月～2011年12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。

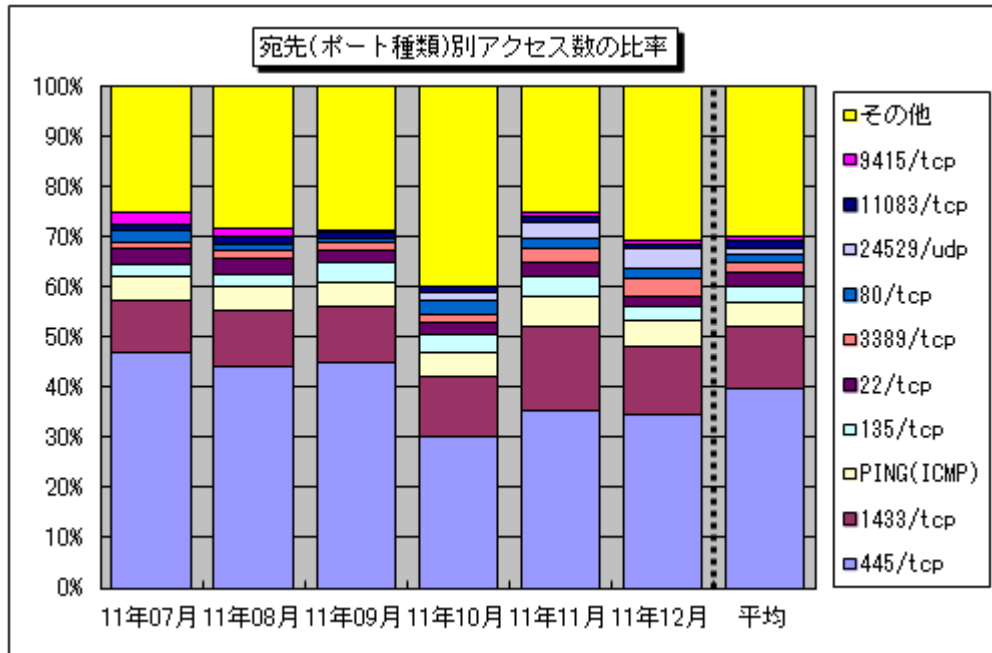


図 3-1：宛先（ポート種類）別アクセス数の比率

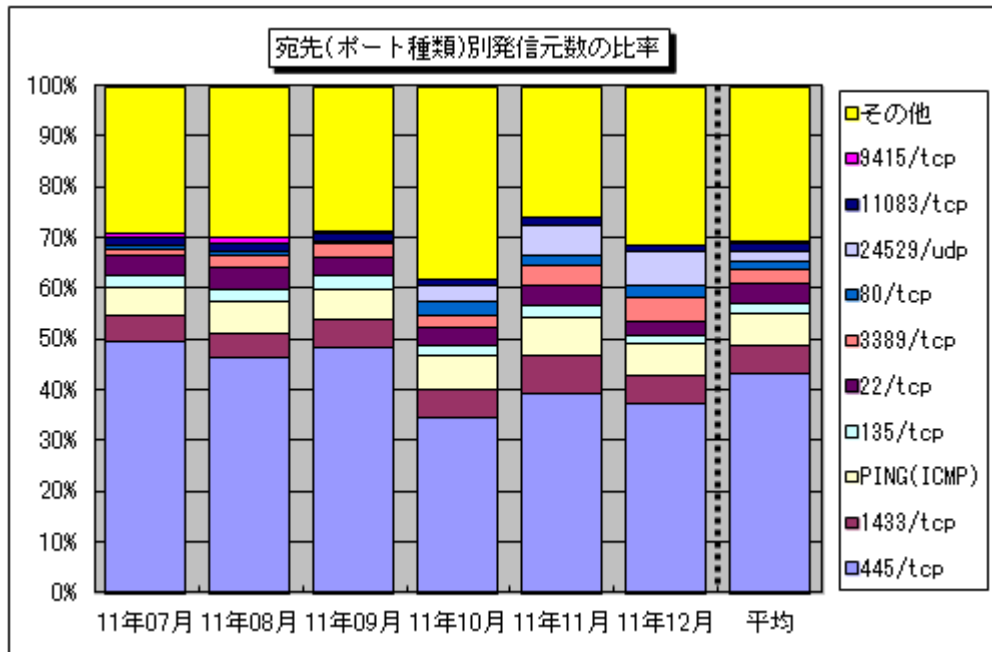


図 3-2：宛先（ポート種類）別発信元数の比率

(2) 発信元地域別の比率

2011年7月～2011年12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。

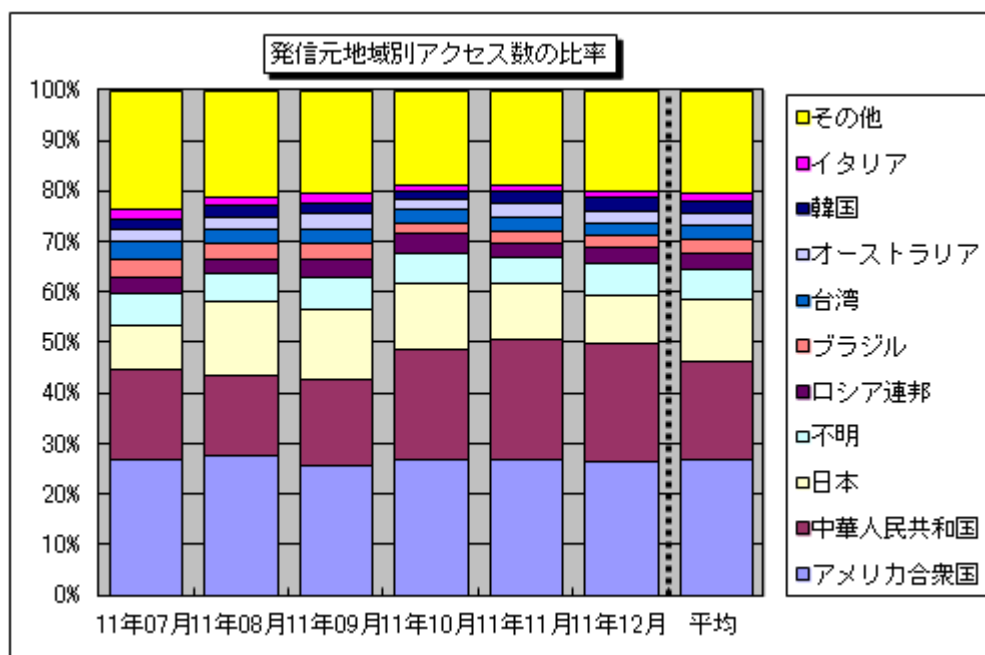
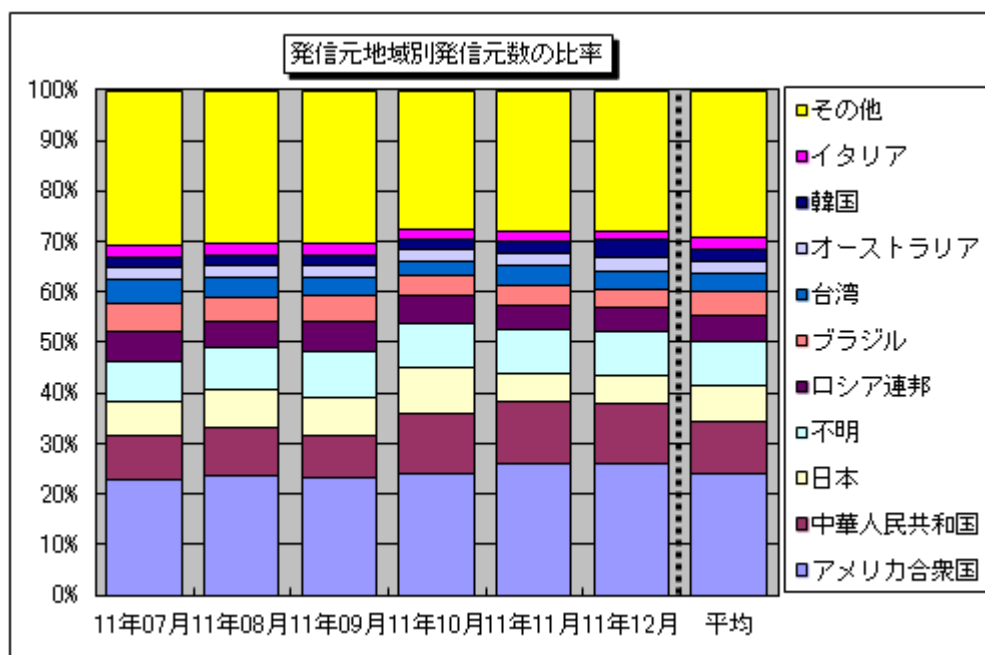


図 3-3：発信元地域別アクセス数の比率

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12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。
24529/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。
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。
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。
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。
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