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、2010 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 **81,226 件**、延べ発信元数※は **37,550 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 134 の発信元から 290 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。

※12 月 22 日～24 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 3 日間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。

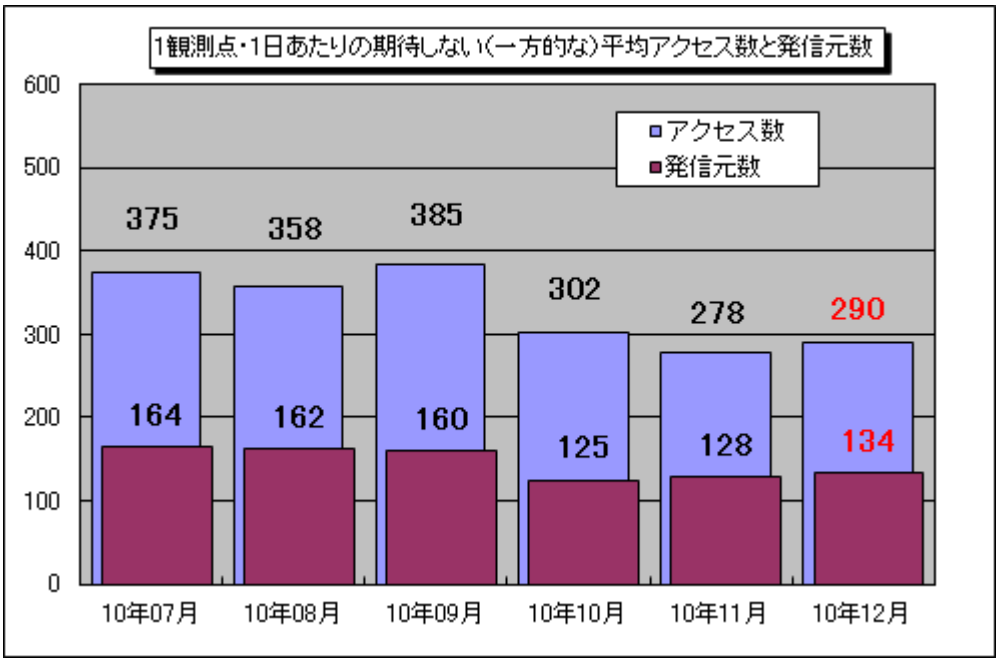

図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 7 月～2010 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 1-1 に示します。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。11 月に比べ、特に増加が観測されたのは 445/tcp へのアクセスでした。

445/tcp は、先月に引き続き増加していましたが、これは主にアメリカと日本からのアクセスが増えたことによるものでした（図 1-3 参照） 。

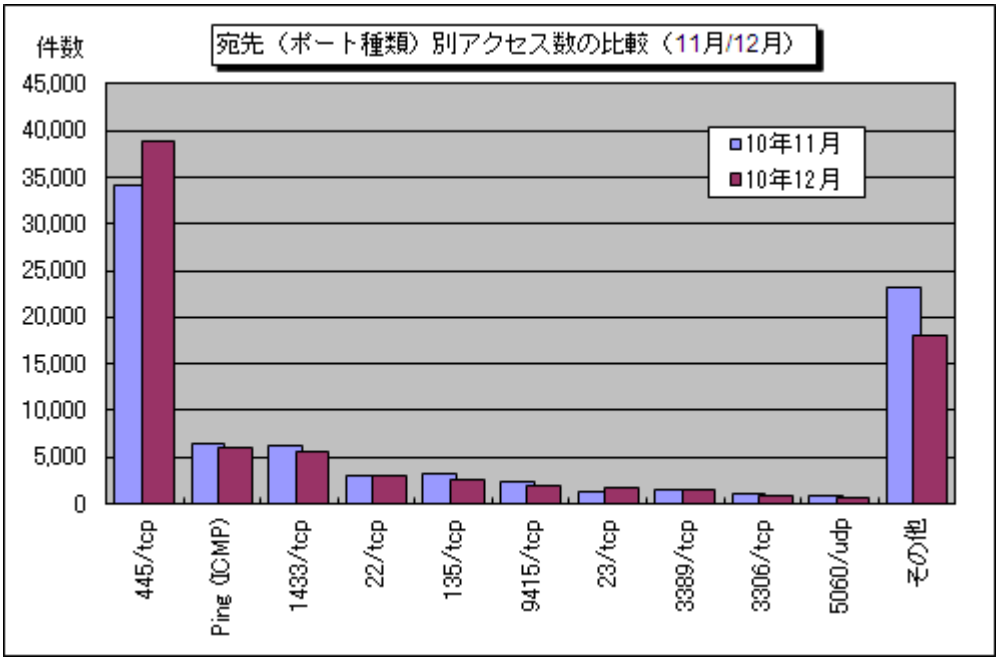

図 1-2：宛先（ポート種類）別アクセス数の比較（11 月/12 月）

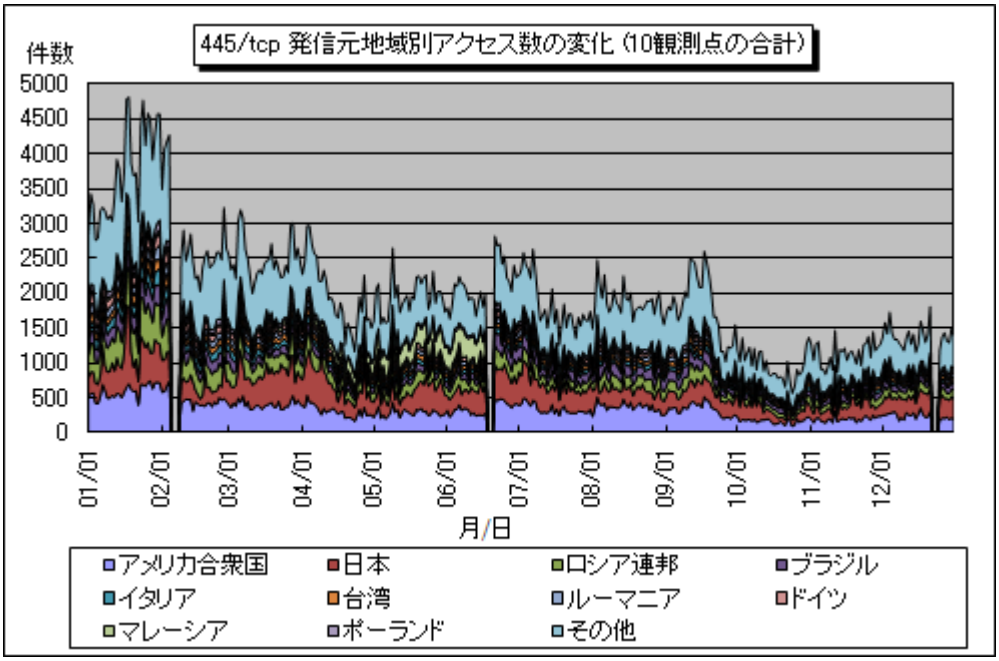

図 1-3：445/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

（1）2010 年のアクセス状況

2010 年 1 月～2010 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 1-4 に示します。アクセス数について年間を通してみると、アクセス数の多かった 1 月から減少傾向にあり、4 月、6 月、9 月に増加が見られましたが、最終的に 1 月の約半分の水準まで減少しました。

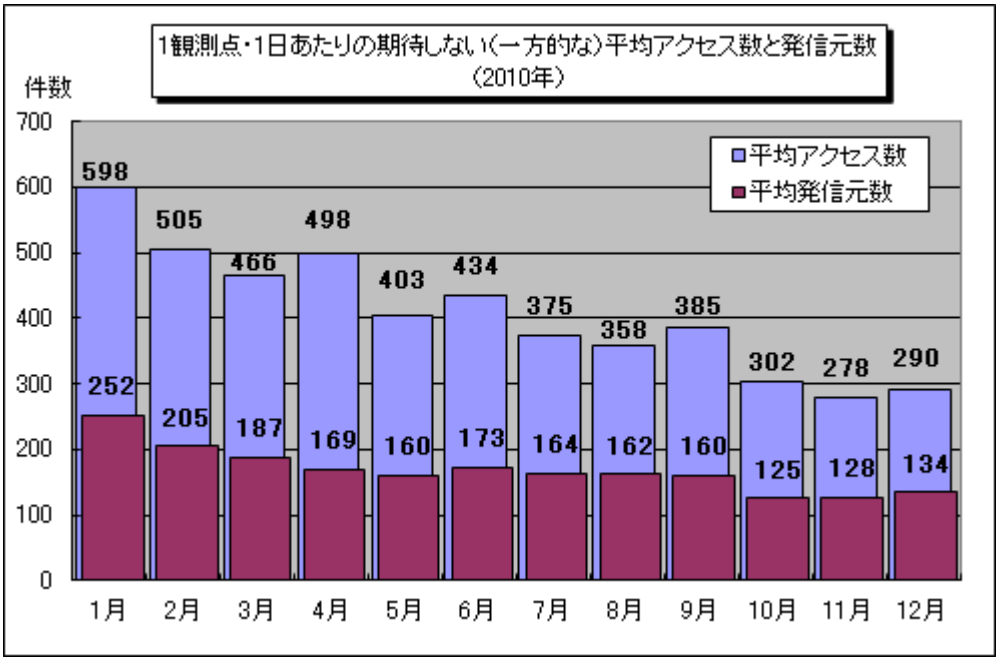

図 1-4：1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数

図 1-4 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 1-5 に示します。この図をみると、当初全体のアクセス数に対して支配的だった 445/tcp へのアクセスは減少が顕著で、最終的に全体の半数までに減少する形となりました。

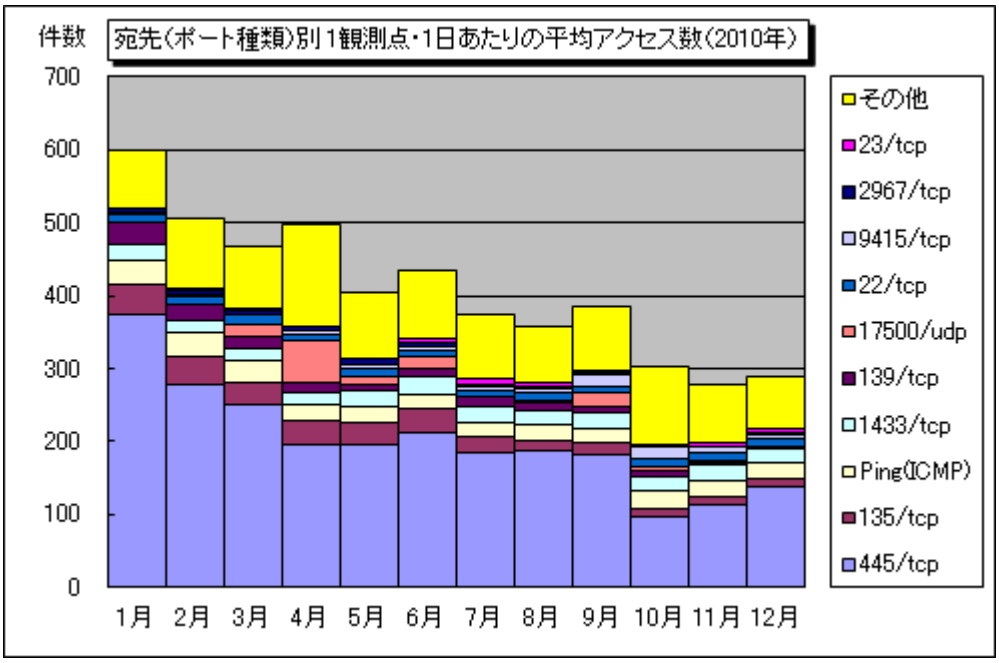

図 1-5：宛先（ポート種類）別 1 観測点・1 日あたりの平均アクセス数

次に、2009 年と 2010 年の宛先（ポート種類）別アクセス数の比較を図 1-6 に示します。2009 年からアクセス数が増加したのは 445/tcp、17500/udp、9415/tcp であり、445/tcp は約 3 万件の増加、17500/udp は約 4 万件の増加、9415/tcp は、約 2 万件の増加でした。逆に減少したのは 135/tcp、Ping（ICMP）、2967/tcp であり、135/tcp は約 21 万件の大幅な減少、Ping（ICMP）は約 6 万件の減少、2967/tcp は約 3 万件の減少でした。

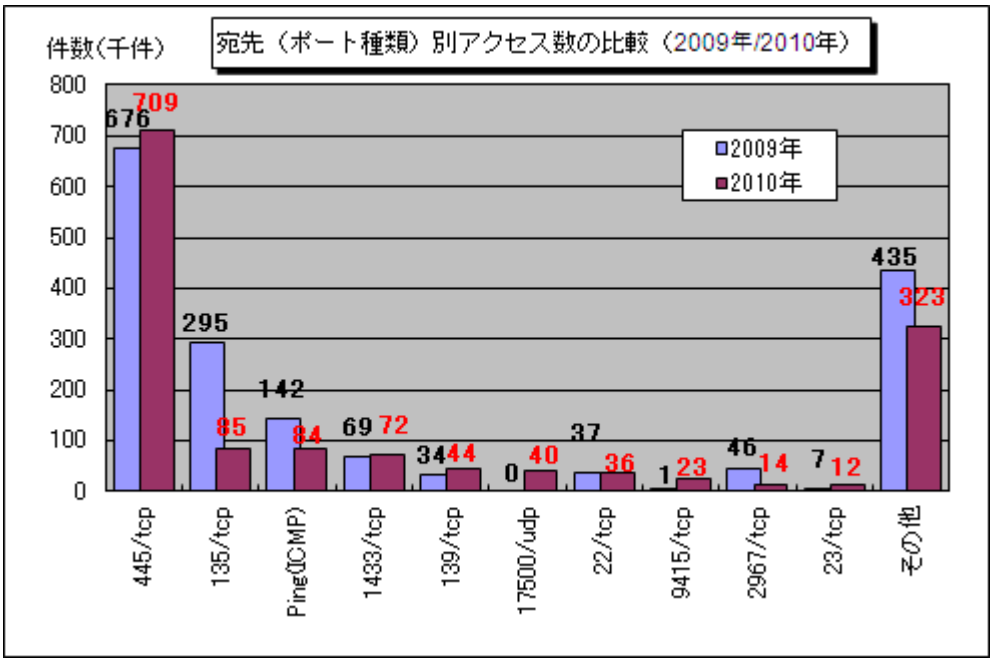

図 1-6：宛先（ポート種類）別アクセス数の比較（2009 年/2010 年）

2010 年の TALOT2 のアクセス状況において、特徴的なのは 17500/udp と 9415/tcp へのアクセスの大幅な増加と言えます。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ったため、これが原因の一つと考えられます。複数と思われていた発信元 IP アドレスは、実はパソコンを立ち上げる度に変化していた 1 箇所のパソコンで、その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。

また、9415/tcp については、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このポートで待ち受けを行うことが確認されており、可能性として、悪意ある者がこのソフトウェアを踏み台としてウェブサーバ等への攻撃に使うために、このソフトウェアがインストールされたパソコンを探索していたものだったと考えられます。

2010 年 1 月からの 17500/udp へのアクセス数の変化を図 1-7 に示します。

2010 年 1 月からの 9415/tcp へのアクセス数の変化を図 1-8 に示します。

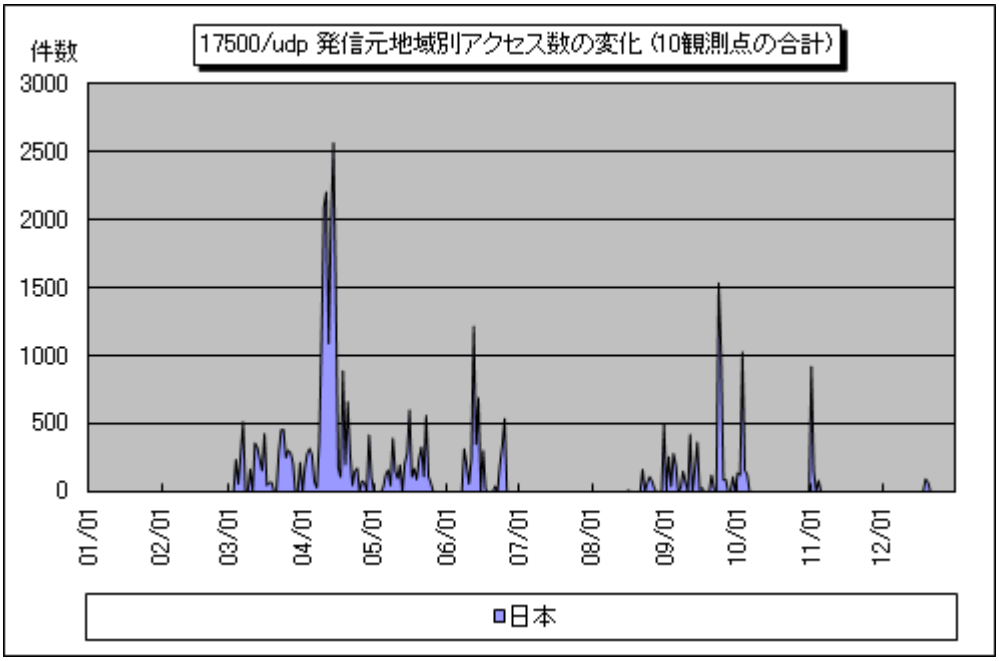

図 1-7：17500/udp 発信元地域別アクセス数の変化

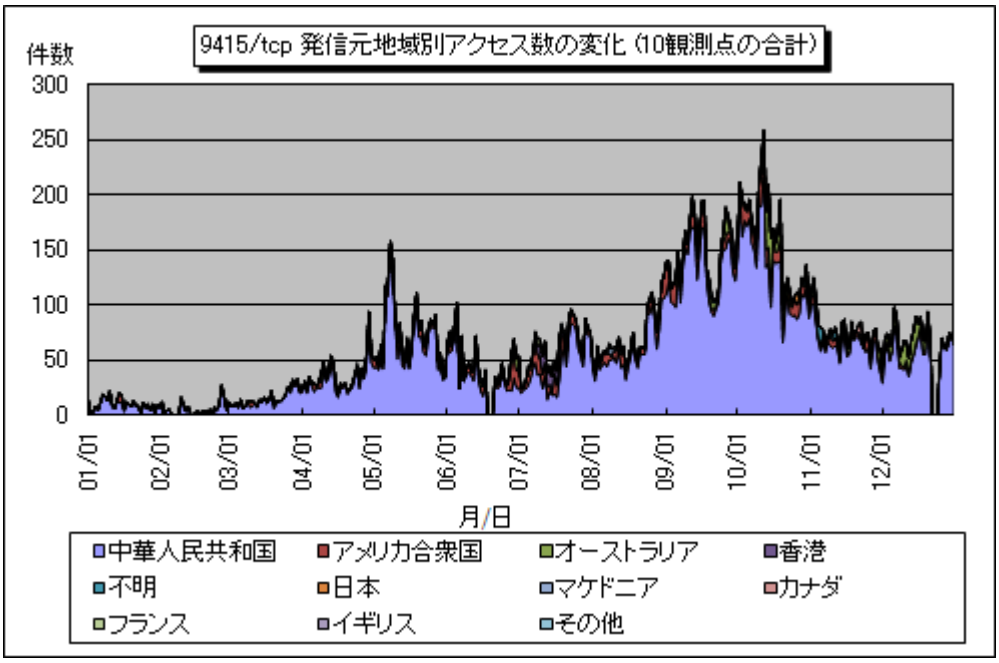

図 1-8：9415/tcp 発信元地域別アクセス数の変化

2. 2010 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

2010 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。

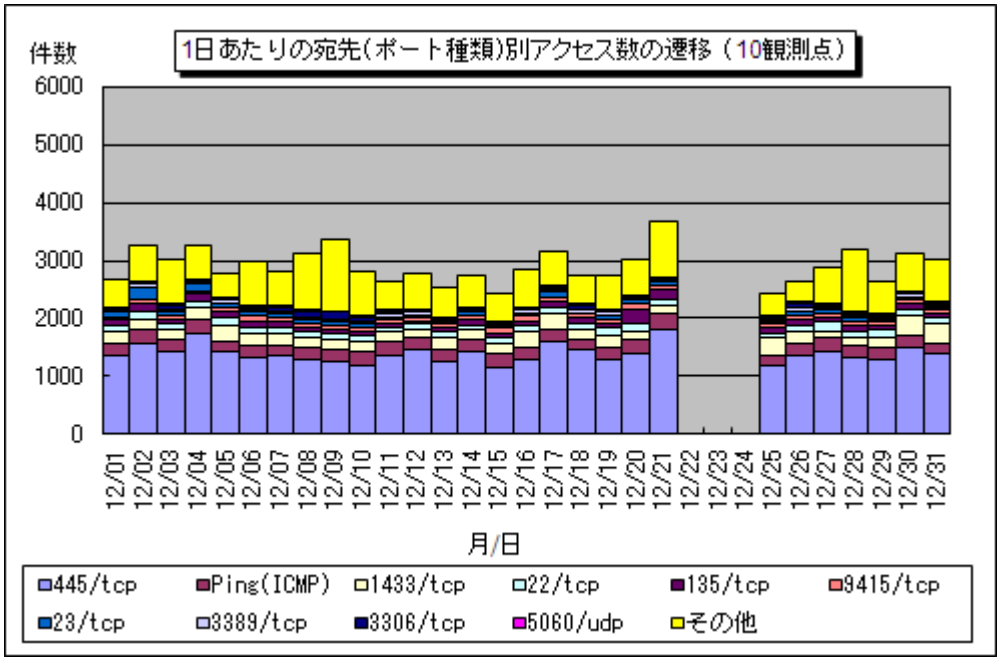

図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移（10 観測点）

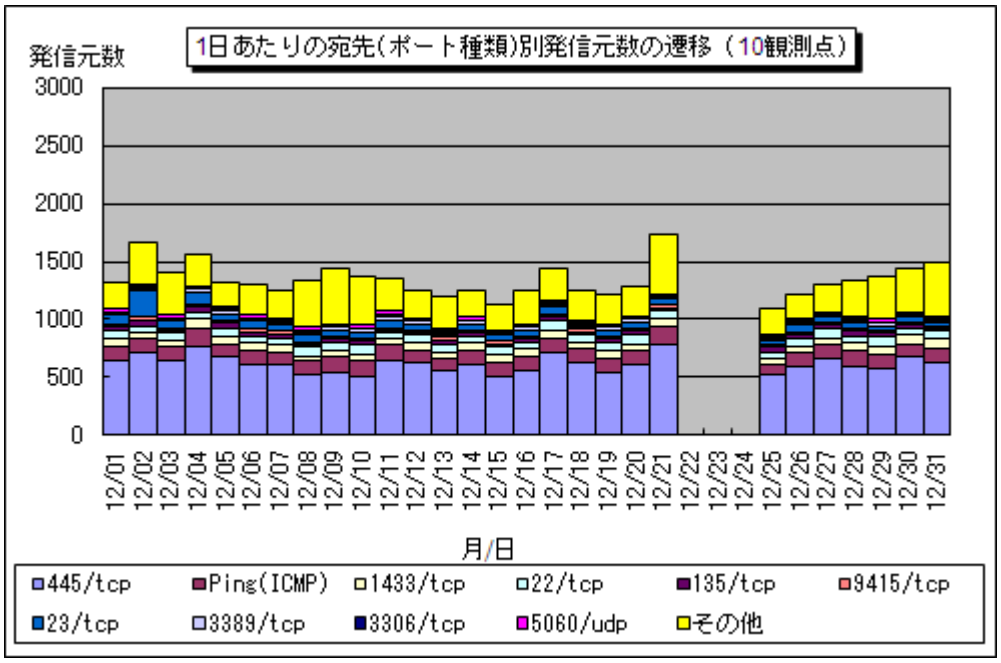

図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）

（2）宛先（ポート種類）別の比率

2010 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。

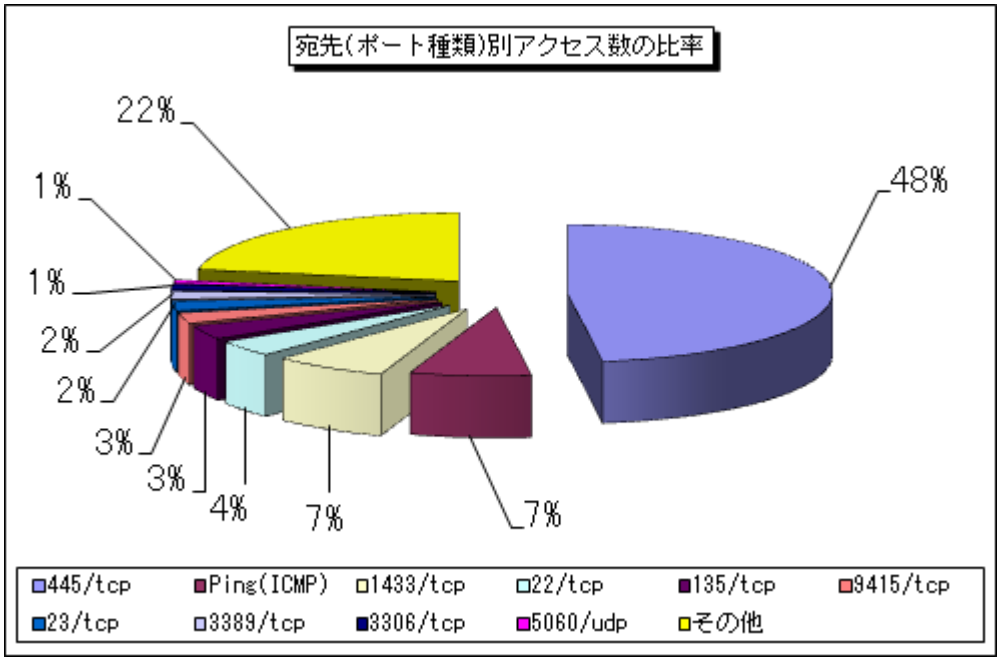

図 2-3：宛先（ポート種類）別アクセス数の比率

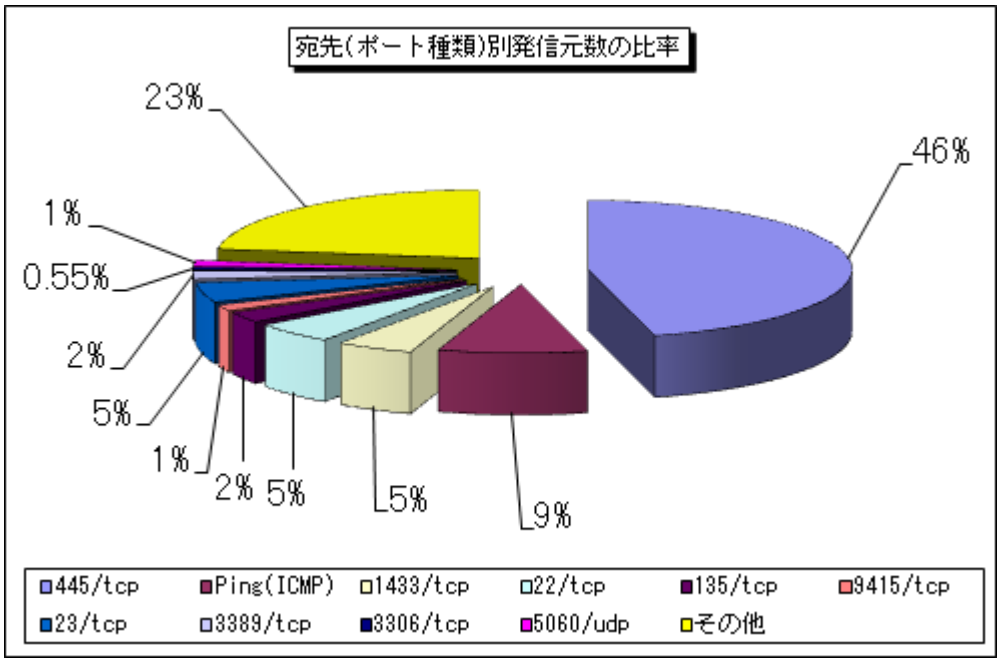

図 2-4：宛先（ポート種類）別発信元数の比率

（3）発信元地域別のアクセス状況

2010 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。

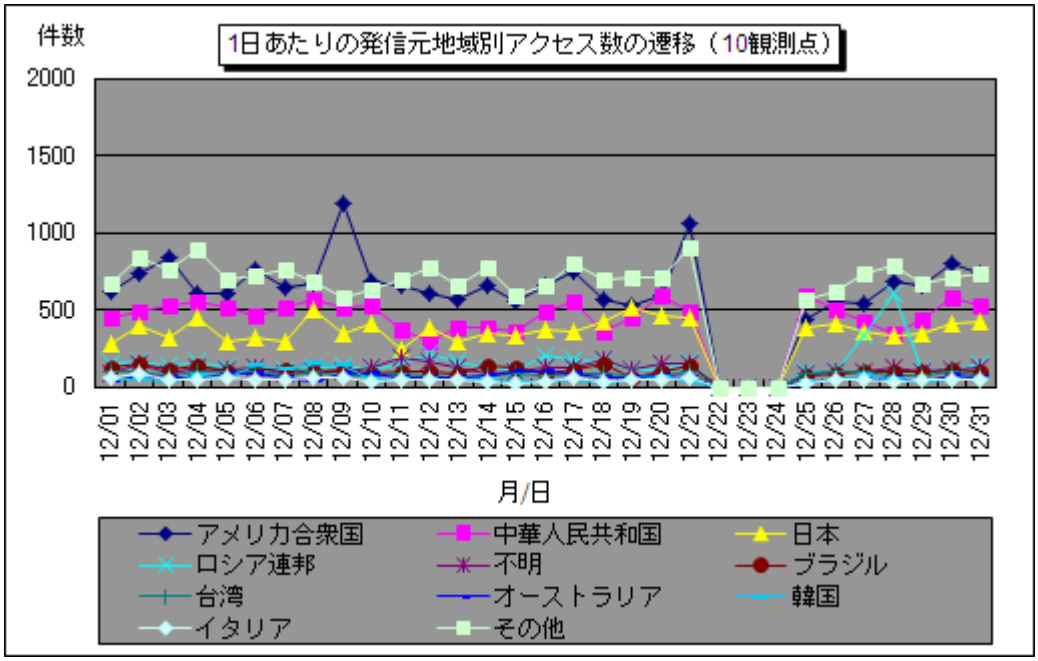

図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）

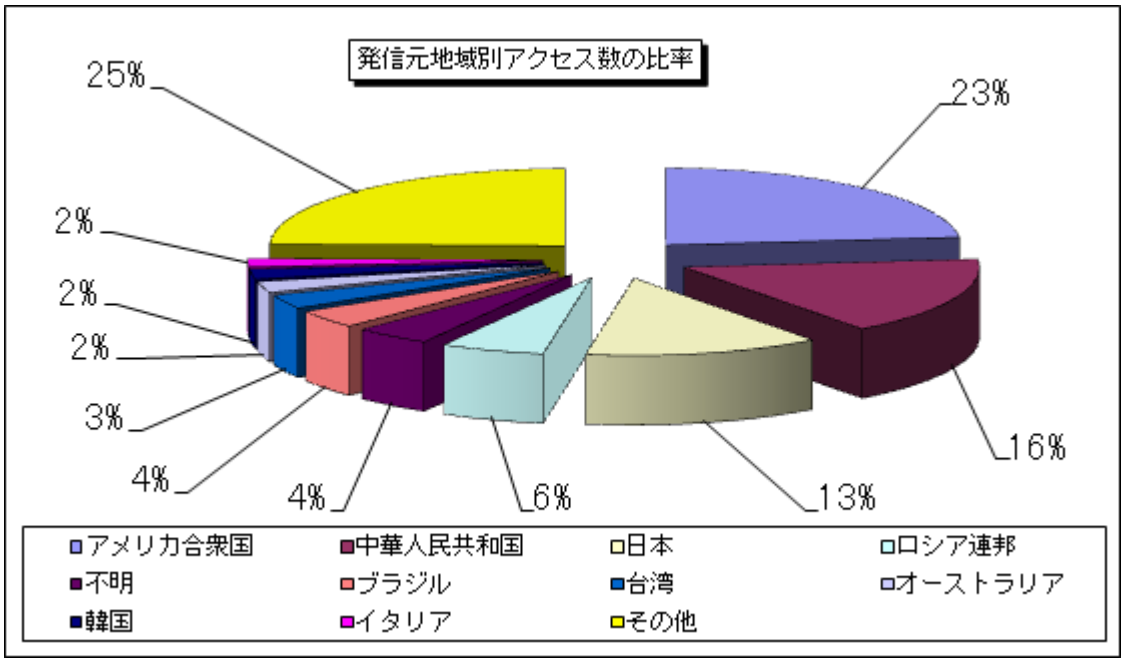

図 2-6：発信元地域別アクセス数の比率

2010 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。

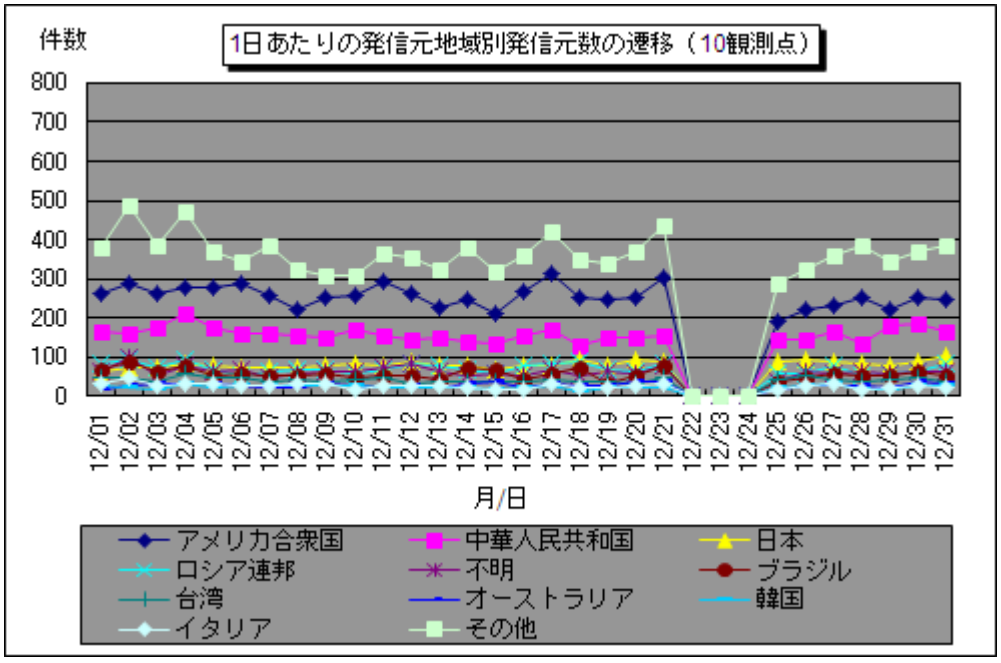

図 2-7： 1 日あたりの発信元地域別発信元数の遷移（10 観測点）

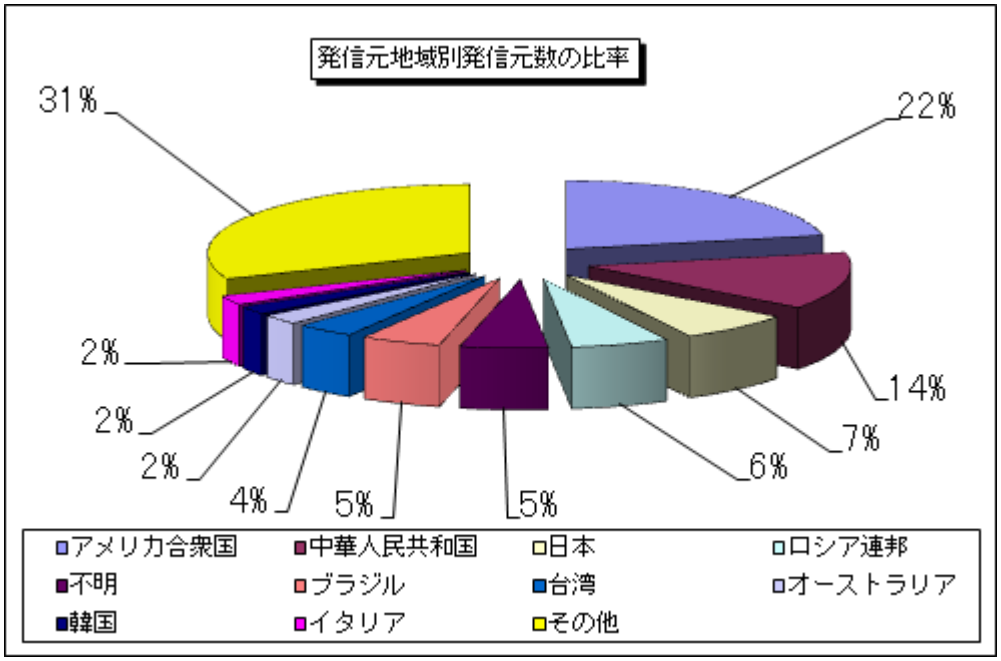

図 2-8：発信元地域別発信元数の比率

3. 統計情報

（1）宛先（ポート種類）別の比率

2010 年 7 月～2010 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。

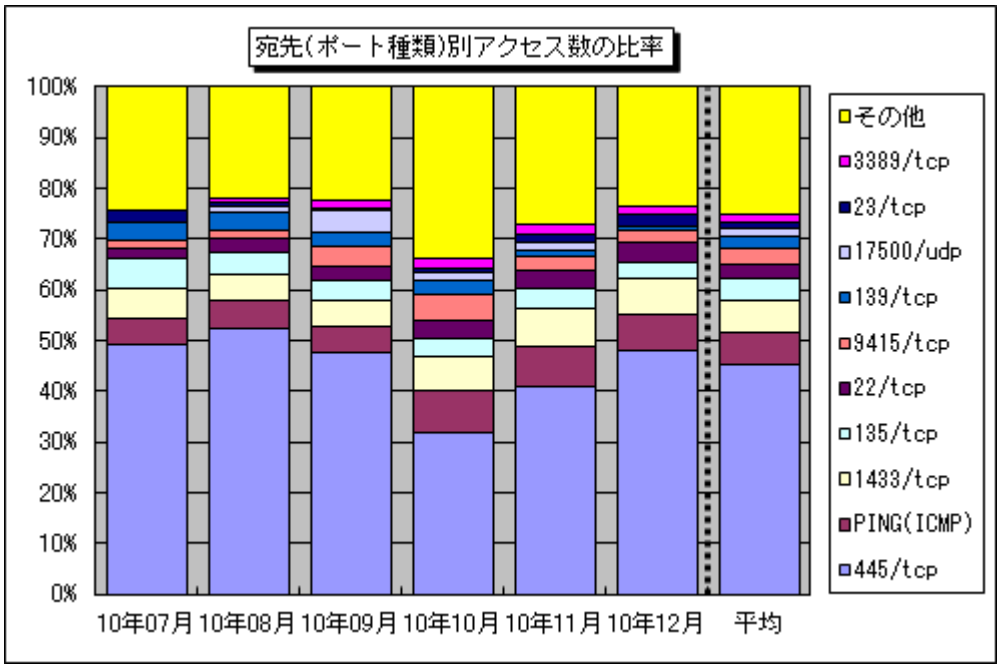

図 3-1：宛先（ポート種類）別アクセス数の比率

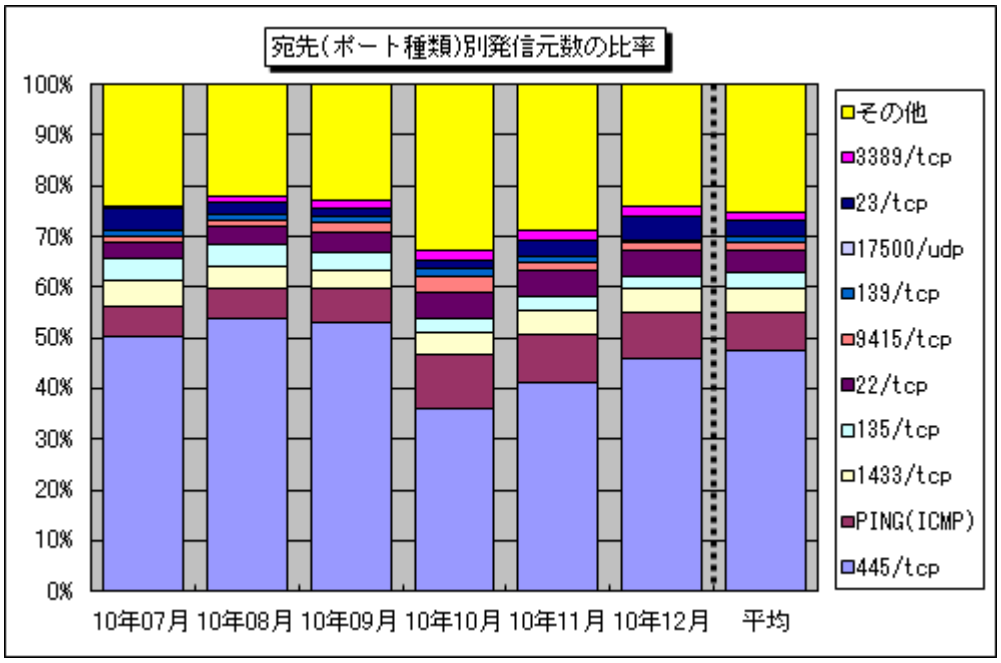

図 3-2：宛先（ポート種類）別発信元数の比率

（2）発信元地域別の比率

2010 年 7 月～2010 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。

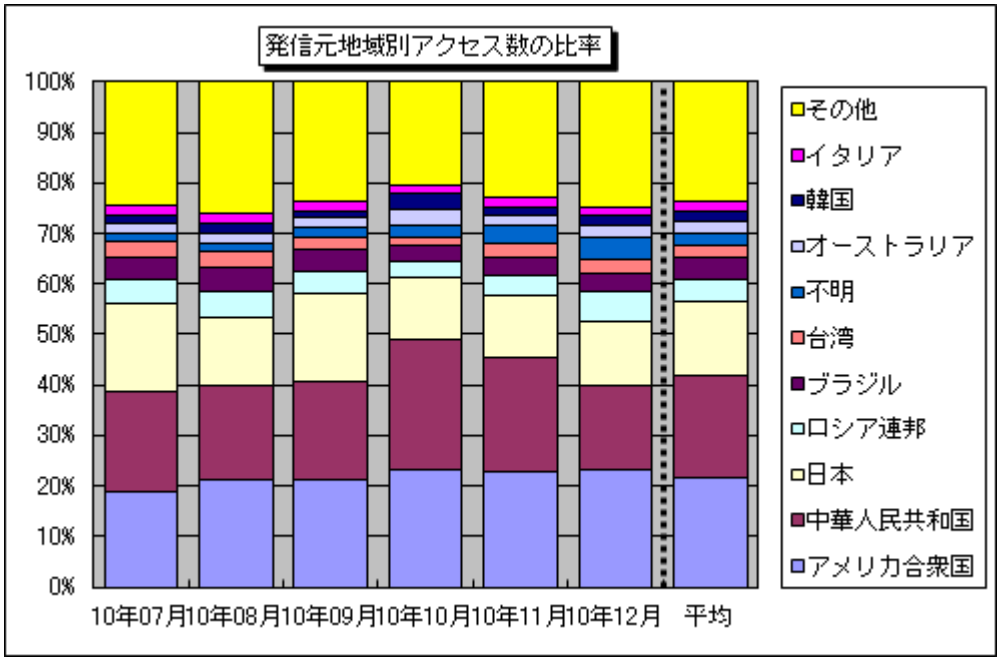

図 3-3：発信元地域別アクセス数の比率

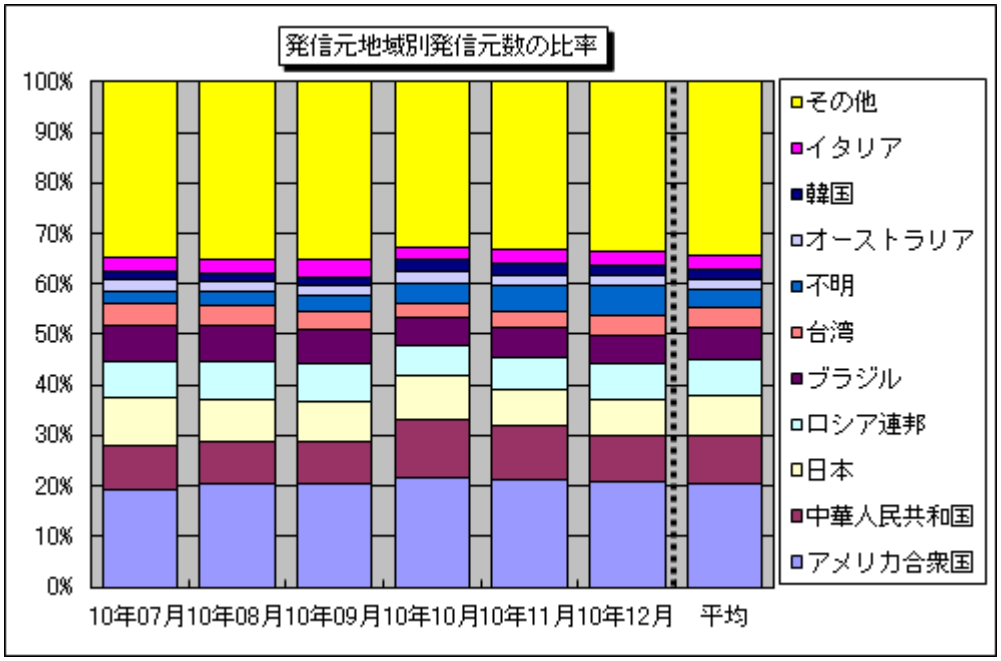

図 3-4：発信元地域別発信元数の比率

4. 補足説明

以下に、2010 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）。
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。
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。
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。
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。
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）。
23/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、Telnet 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。
3306/tcp	MySQL Sever 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。
5060/udp	7 月 9 日から TALOT2 の複数の観測点で多く観測され始めた、海外の複数の発信元からのアクセス。SIP サーバ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 セキュリティセンター　加賀谷／古川
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp