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 2 月の期待しない（一方的な）アクセスの総数は 10 観測点で **143,494 件**、延べ発信元数※は **41,803 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 182 の発信元から 624 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。

※2 月 4 日～8 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、2 月の観測データは、この 5 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。

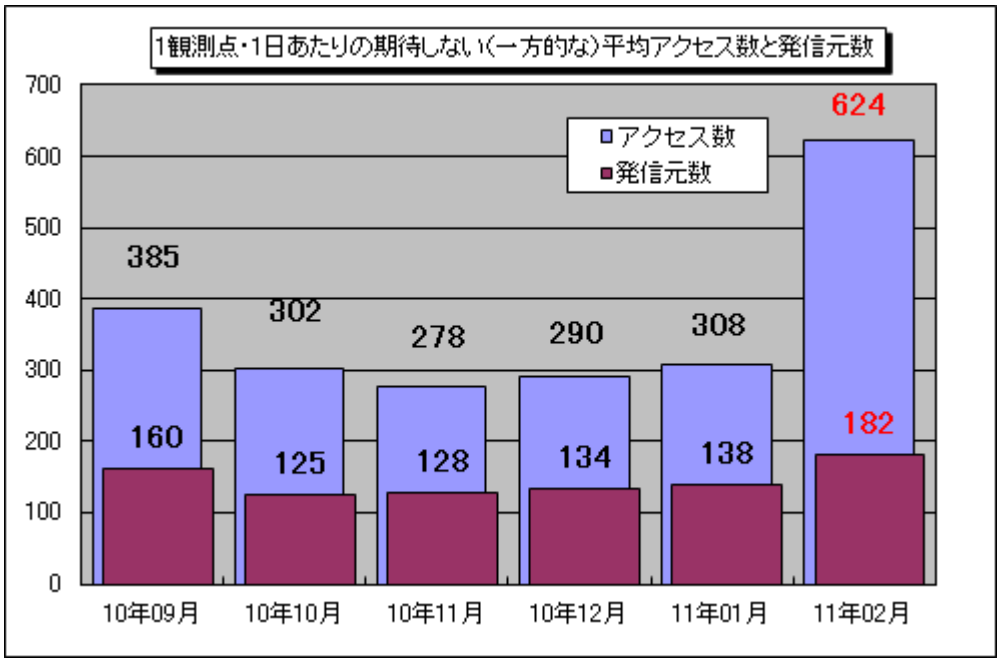

図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 9 月～2011 年 2 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。2 月の期待しない（一方的な）アクセスは、1 月と比べて大幅に増加しました。

1 月と 2 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。1 月に比べ、比較的増加が観測されたのは 80/tcp、17500/udp、443/tcp、25/tcp へのアクセスでした。

17500/udp については、2010 年 9 月頃にも一時期増加が観測されており、今回も以前と同様に 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特徴がありました（図 1-3 参照）。このポートに対してブロードキャストを送信する一般利用者向けのソフトウェアの存在が確認されていることから、このソフトウェアを使用しているパソコン利用者による通信であった可能性があります。複数の IP アドレスから送られていたのは、

当該パソコンがネットワークに接続する度に IP アドレスが変化していたためと思われます。なお、他の観測点ではブロードキャストが到達しない仕様のようなので、当該アクセスは観測されていません。

また、2 月は 80/tcp、443/tcp、25/tcp の増加が観測されていますが、これは 2 月 21 日以降にミャンマーの IP アドレスからのアクセスが TALOT2 の複数の観測点で増加したためです。上記のポートの他、21/tcp、22/tcp でも同様の IP アドレスからのアクセスの増加が観測されています（図 1-4 参照）。定点観測を行っている他の組織の中にも類似した傾向を観測しているところもあり、原因に関しては現在調査中ですが、何らかの攻撃が行われている可能性もありえるので、引き続きこれらのポートへのアクセスに注意していきます。

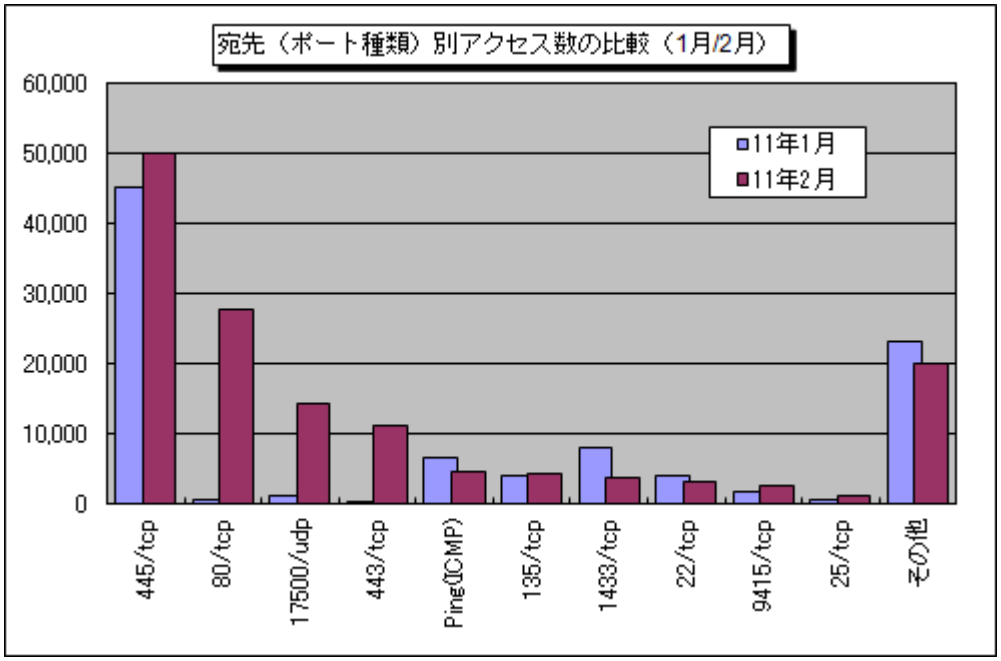

図 1-2：宛先（ポート種類）別アクセス数の比較（1 月/2 月）

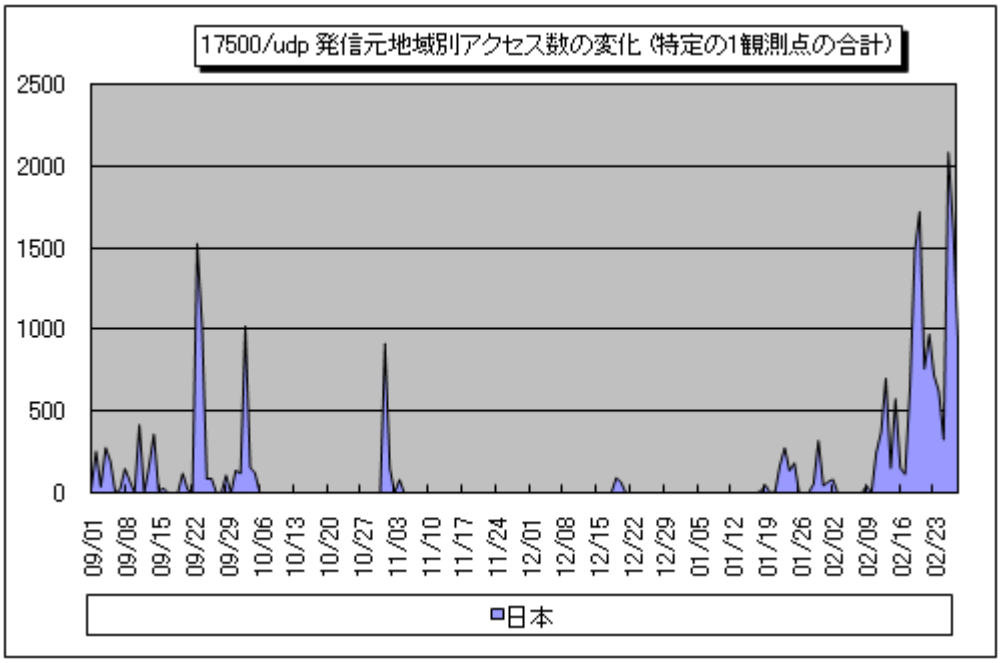

図 1-3：17500/udp 発信元地域別アクセス数の変化（特定の 1 観測点の合計）

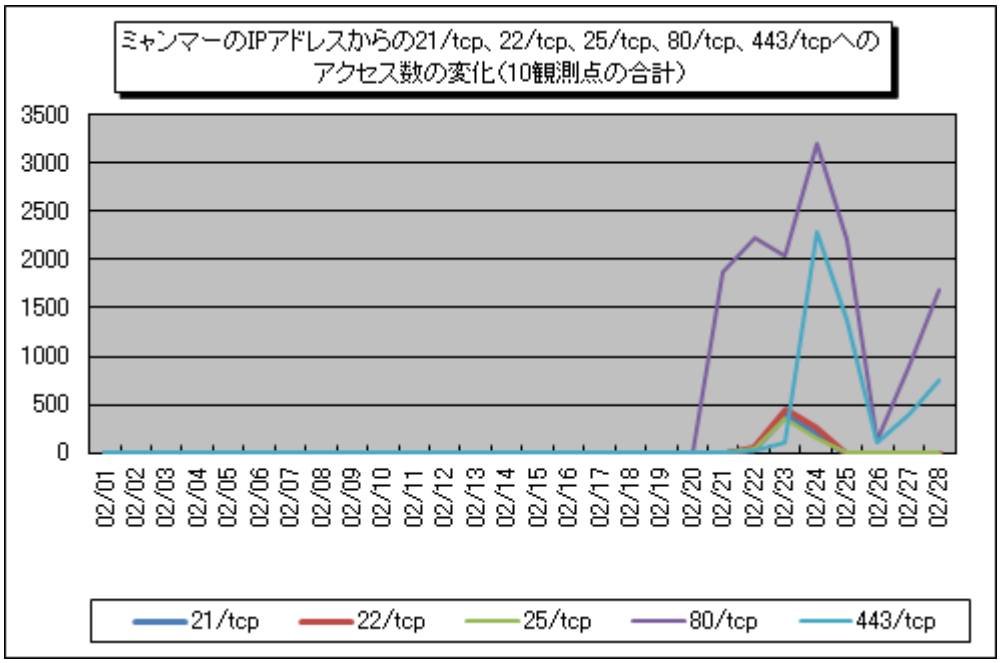

図 1-4：ミャンマーの IP アドレスからの 21/tcp、22/tcp、25/tcp、80/tcp、443/tcp へのアクセス数の変化

2. 2011 年 2 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 2 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。

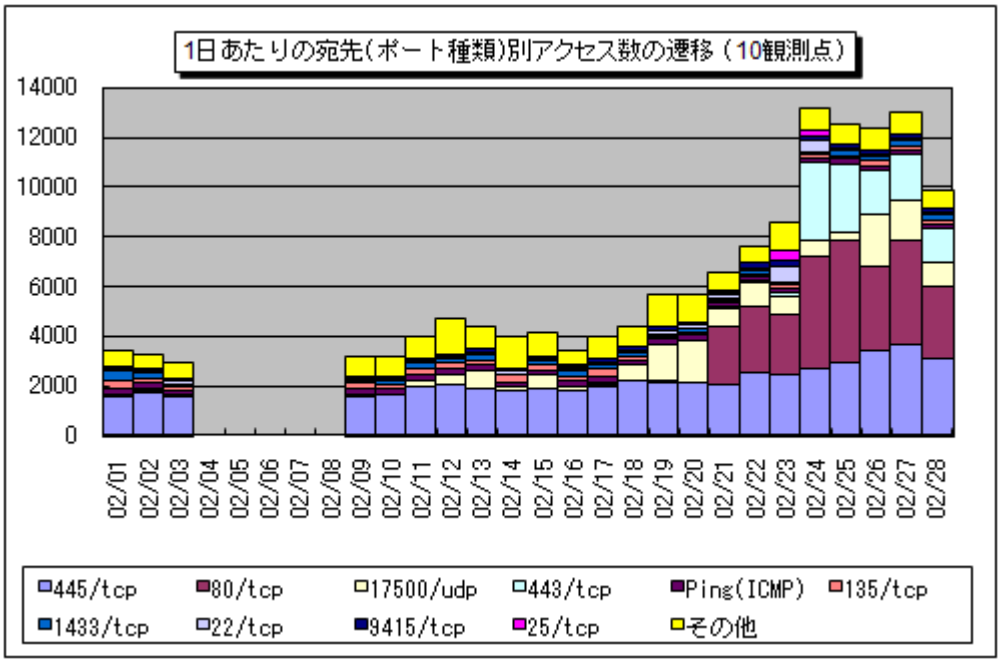

図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移（10 観測点）

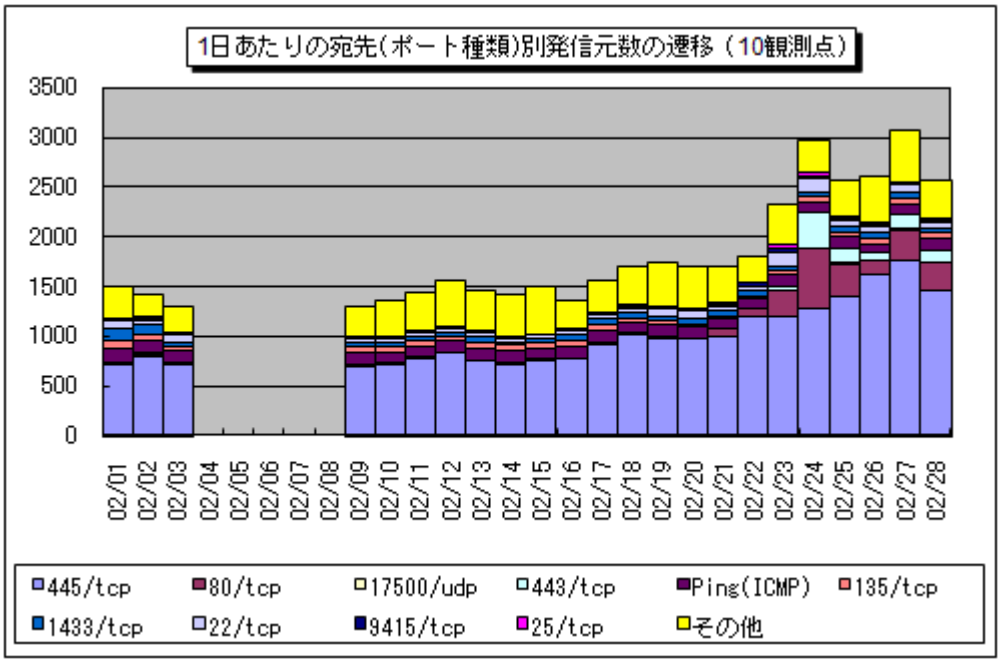

図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）

（2）宛先（ポート種類）別の比率

2011 年 2 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。

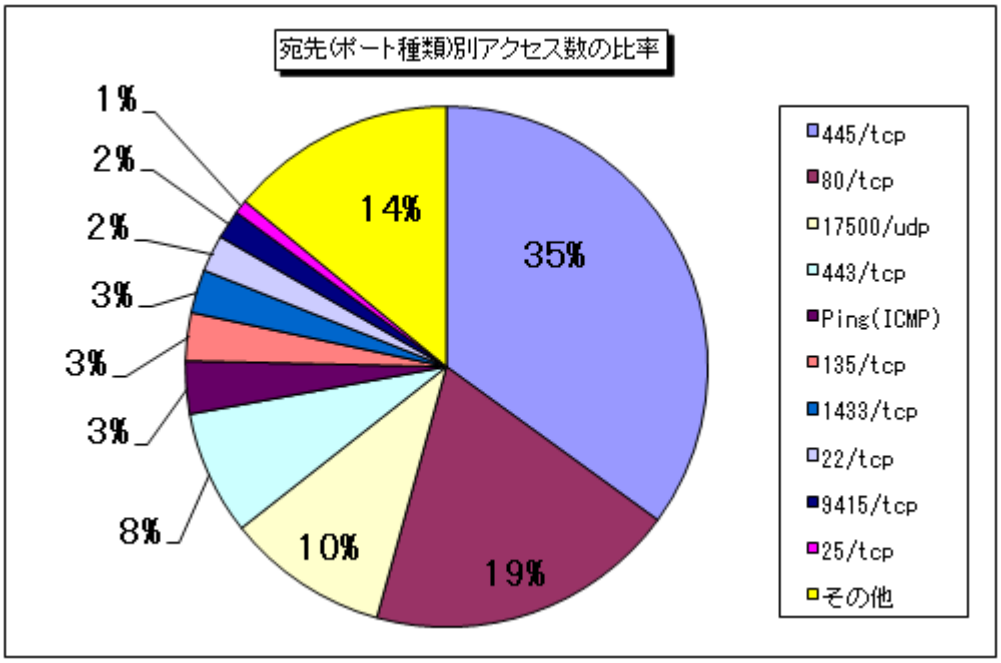

図 2-3：宛先（ポート種類）別アクセス数の比率

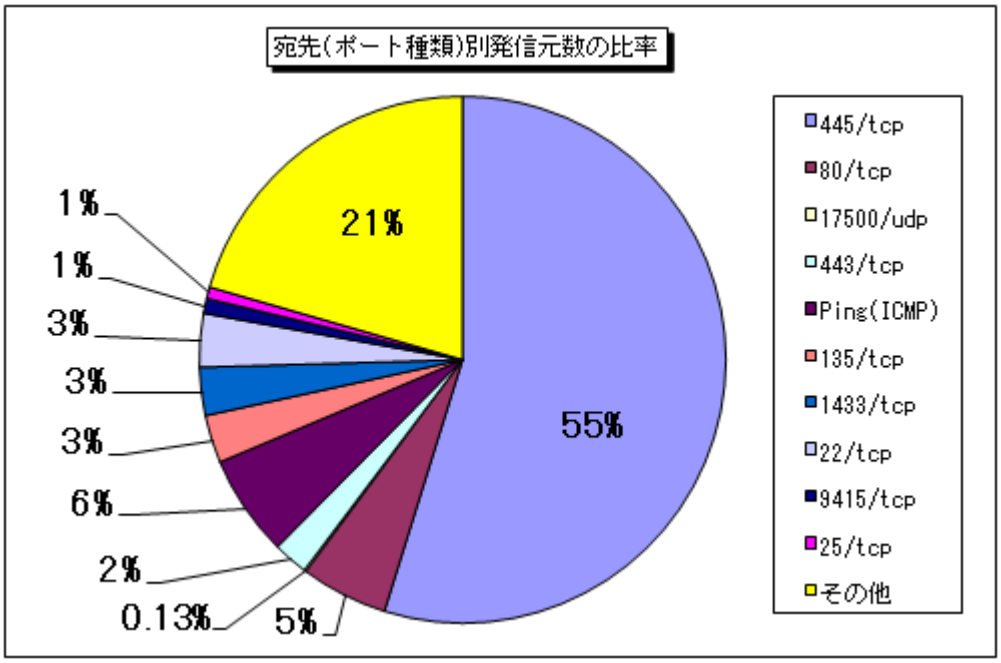

図 2-4：宛先（ポート種類）別発信元数の比率

（3）発信元地域別のアクセス状況

2011 年 2 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。

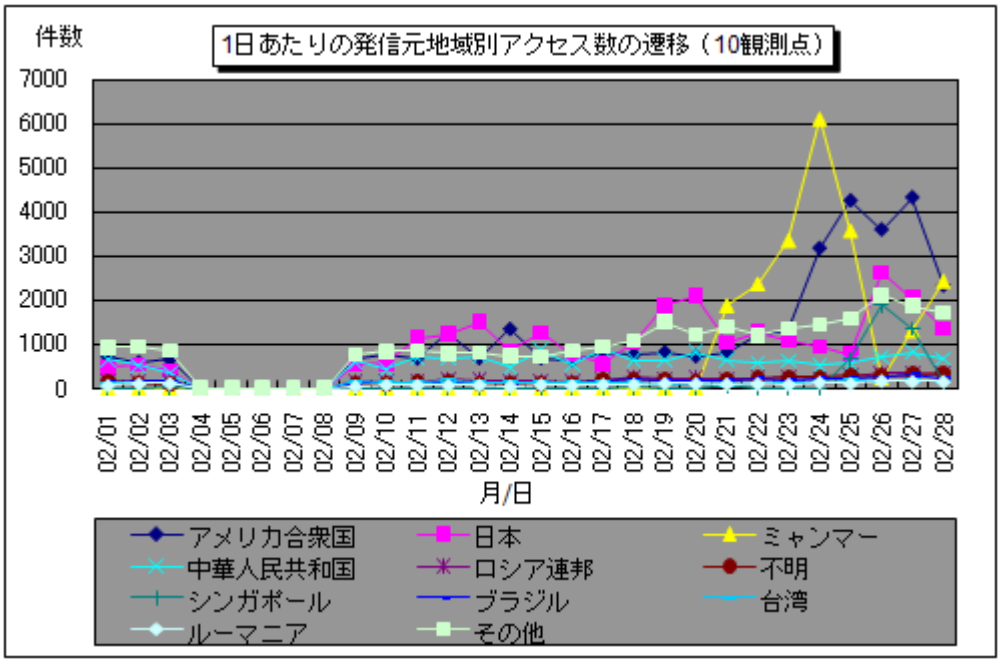

図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）

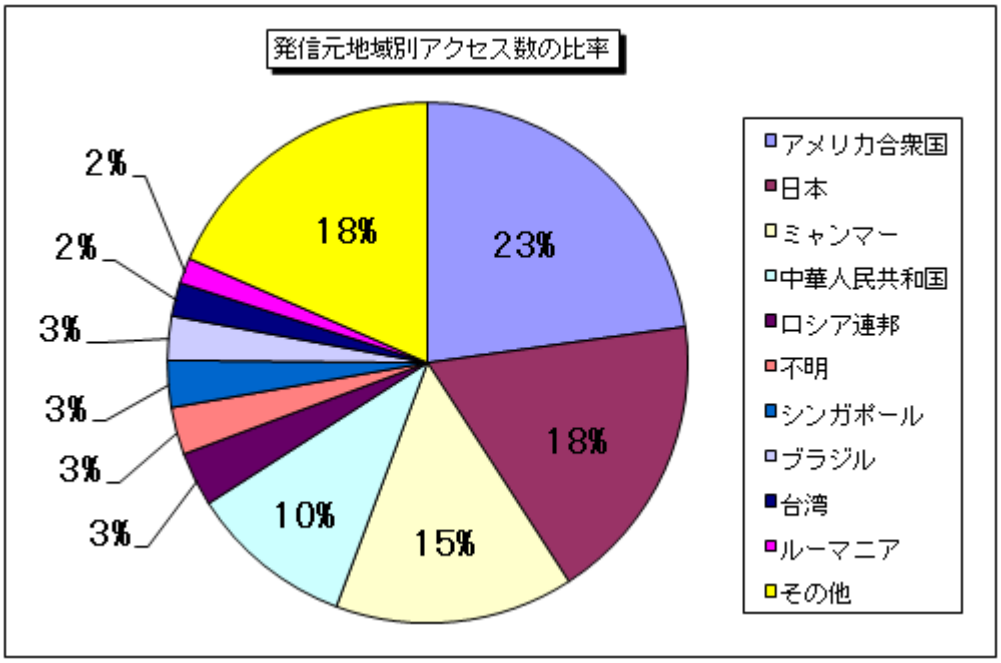

図 2-6：発信元地域別アクセス数の比率

2011 年 2 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。

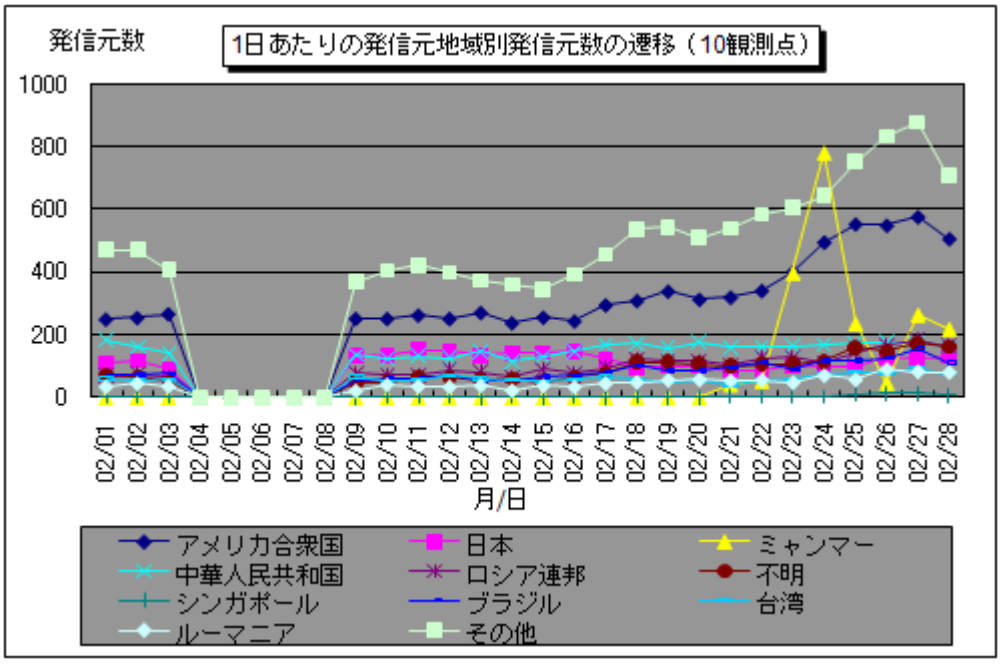

図 2-7： 1 日あたりの発信元地域別発信元数の遷移（10 観測点）

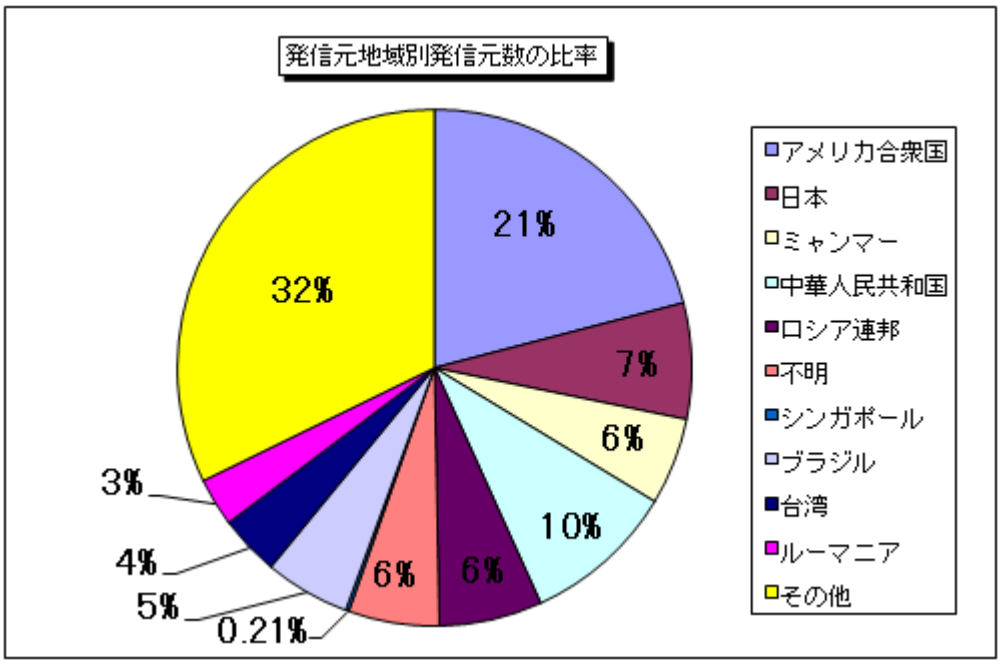

図 2-8：発信元地域別発信元数の比率

3. 統計情報

（1）宛先（ポート種類）別の比率

2010 年 9 月～2011 年 2 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。

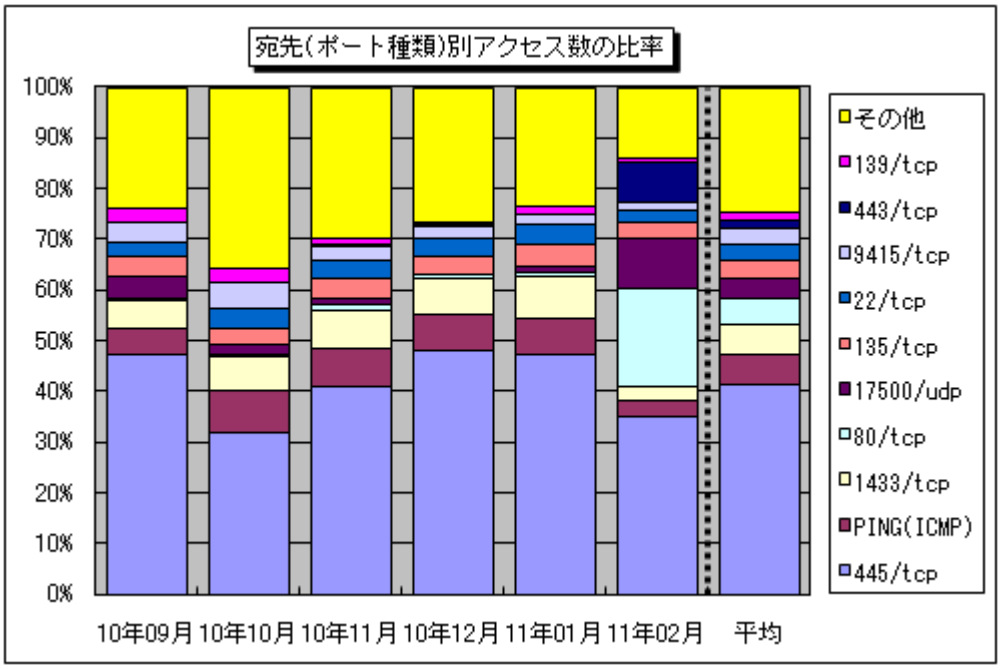

図 3-1：宛先（ポート種類）別アクセス数の比率

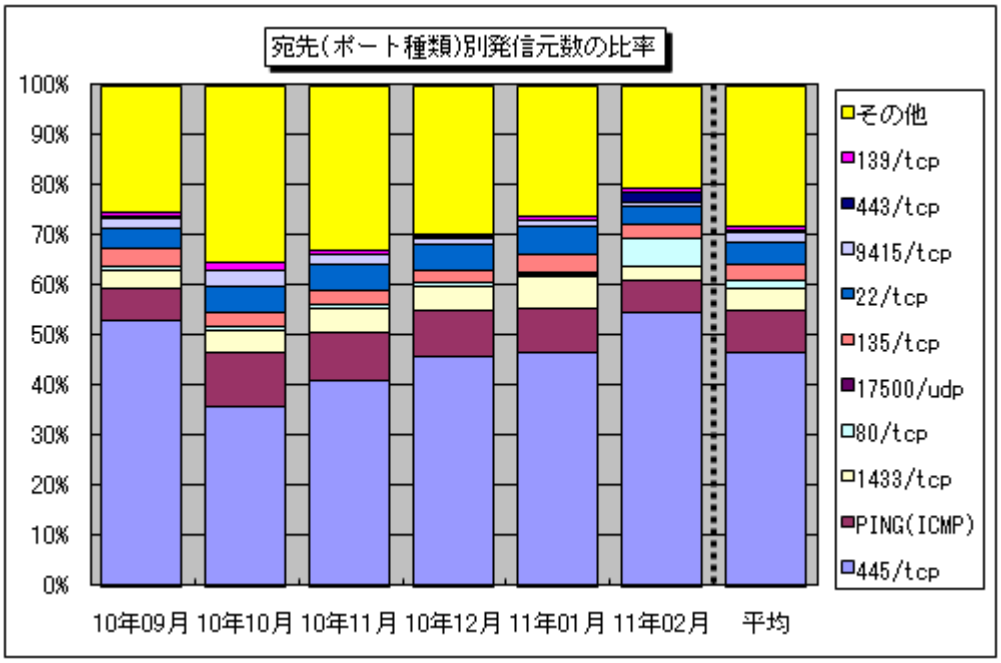

図 3-2：宛先（ポート種類）別発信元数の比率

（2）発信元地域別の比率

2010 年 9 月～2011 年 2 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。

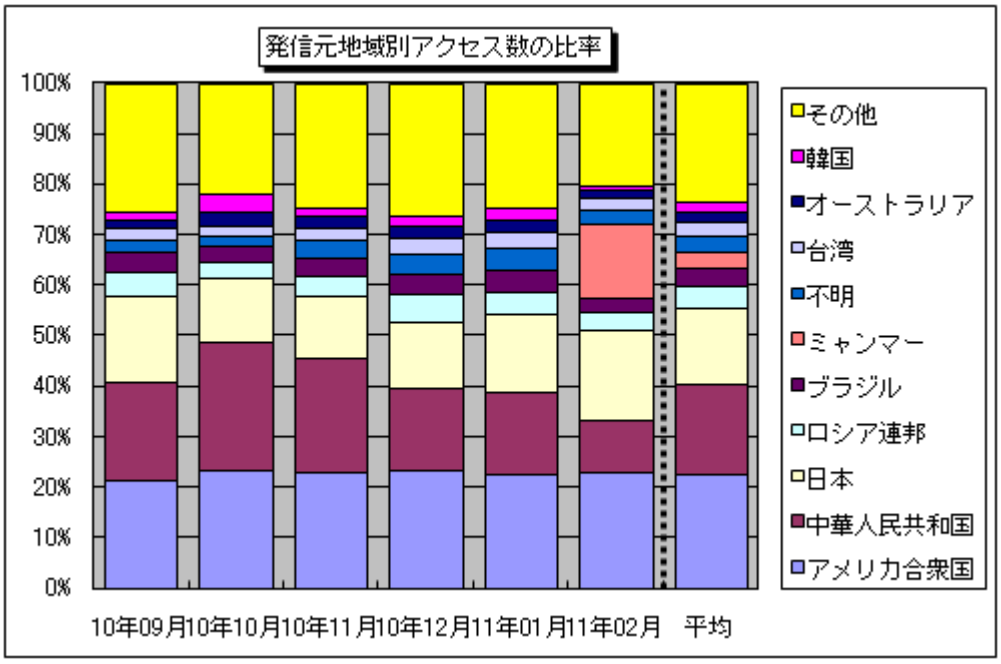

図 3-3：発信元地域別アクセス数の比率

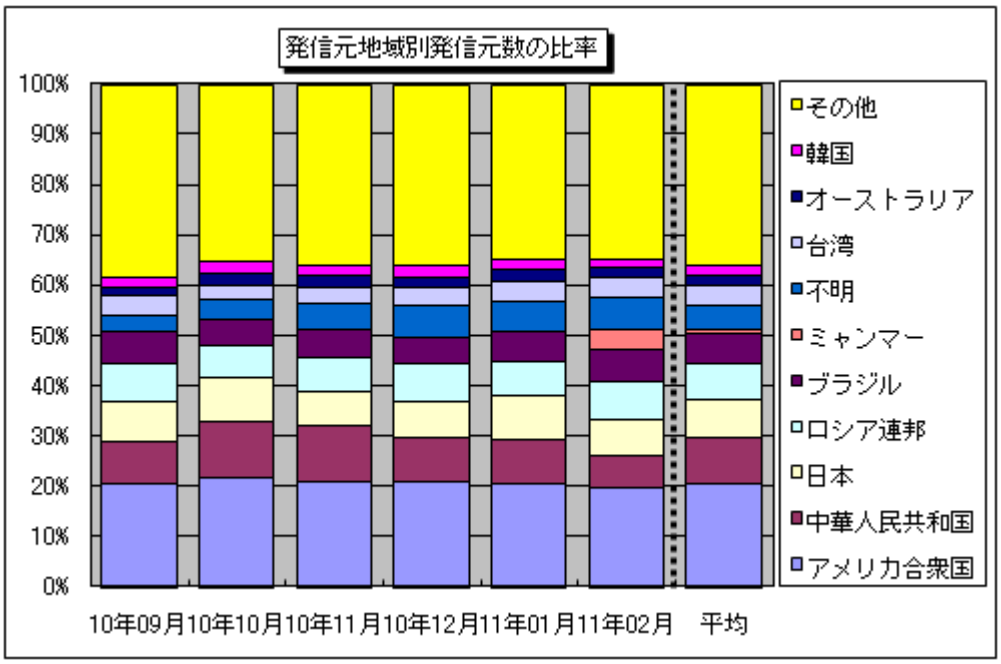

図 3-4：発信元地域別発信元数の比率

4. 補足説明

以下に、2011 年 2 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）。
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。
17500/udp	特定の観測点でのみ観測される、特定の発信元からのブロードキャストと思われるアクセス。
443/tcp	ウェブアクセスのプロトコルである HTTPS 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。
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）。
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。
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。
25/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。

■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