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 5 月の期待しない（一方的な）アクセスの総数は 10 観測点で **189,497 件**、延べ発信元数※は **78,227 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 252 の発信元から 611 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。

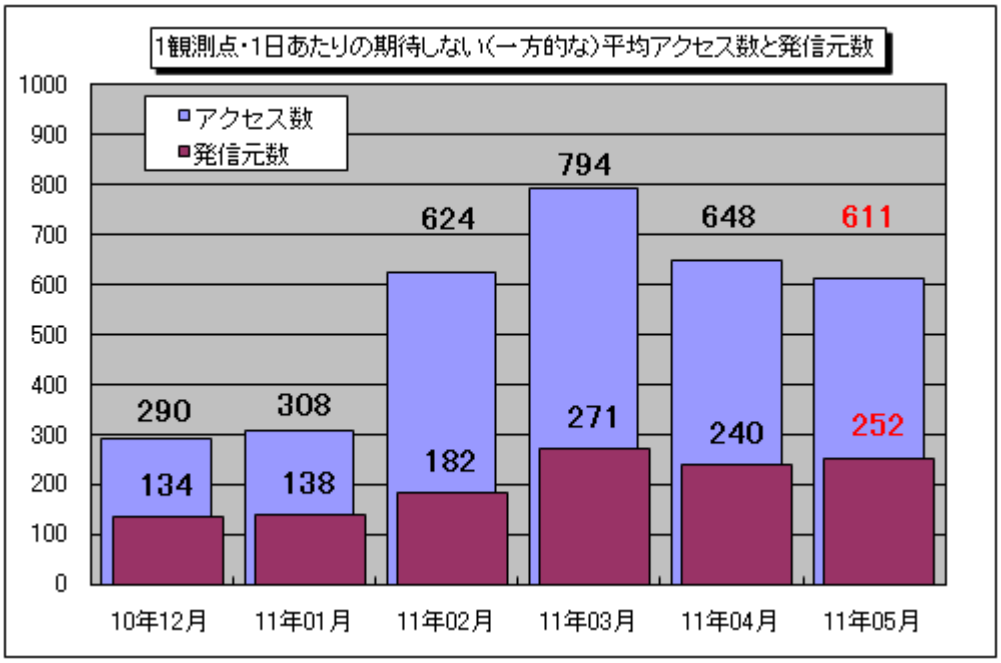

図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 12 月～2011 年 5 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。5 月の期待しない（一方的な）アクセスは、4 月と比べて減少しました。

4 月と 5 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。4 月に比べ、増加が観測されたのは 10394/udp 、10394/tcp、その他へのアクセスでした。

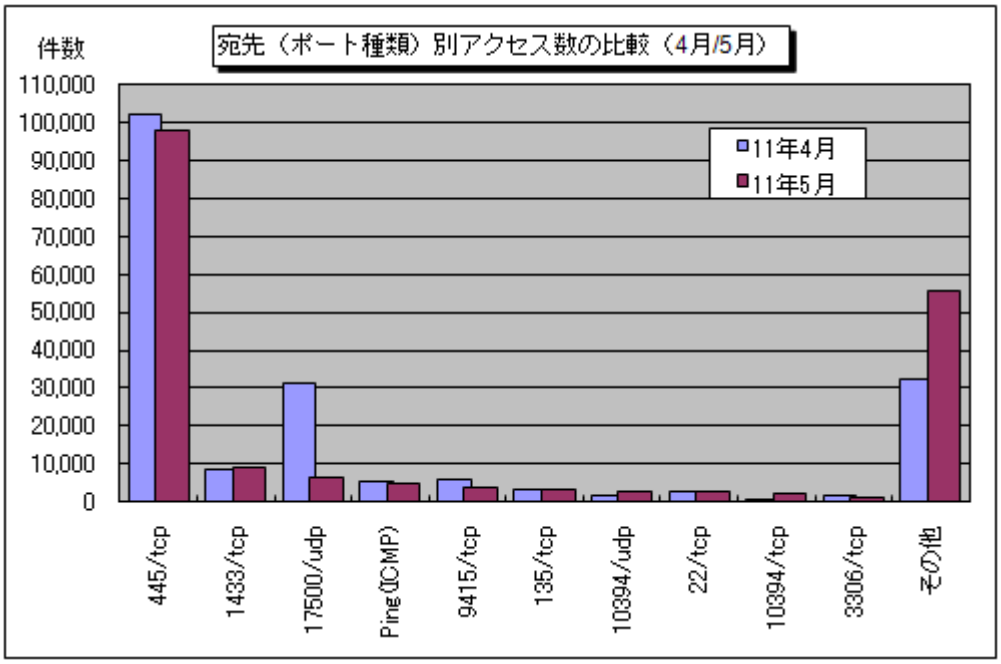

図 1-2：宛先（ポート種類）別アクセス数の比較（4 月/5 月）

10394/udp と 10394/tcp については、5 月 22 日の周辺に、増加が観測されていました（図 1-3 参照）。これらのポートはいずれも、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、このアクセスが何を目的としたものだったかは不明です。これらのアクセスは、特定の 1 観測点でしか観測されていませんでしたが、1 つの発信元からというわけではなく、複数の発信元からのアクセスが観測されていました。

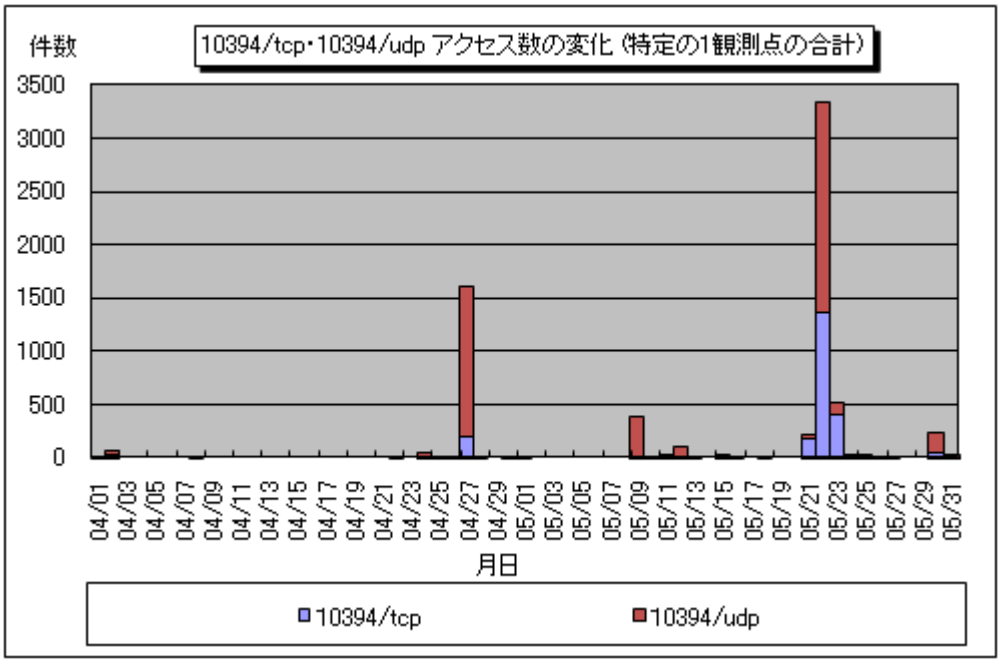

図 1-3：10394/tcp・10394/udp アクセス数の変化（特定の 1 観測点の合計）

その他へのアクセスの増加について、解析した結果、TALOT2 の特定の観測点に対し、5 月 20 日から 23 日の間に、アメリカ合衆国の特定の IP アドレスの 80/tcp からのアクセスが観測されました（図 1-4 参照）。これらのアクセスは、全て SYN/ACK パケットだったことから、TALOT2 で使用しているアドレスが、DoS 攻撃（SYN Flood 攻撃）(*1) の攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN/ACK パケット（跳ね返りパケット (*3)）が大量に届いていた可能性があるということです。

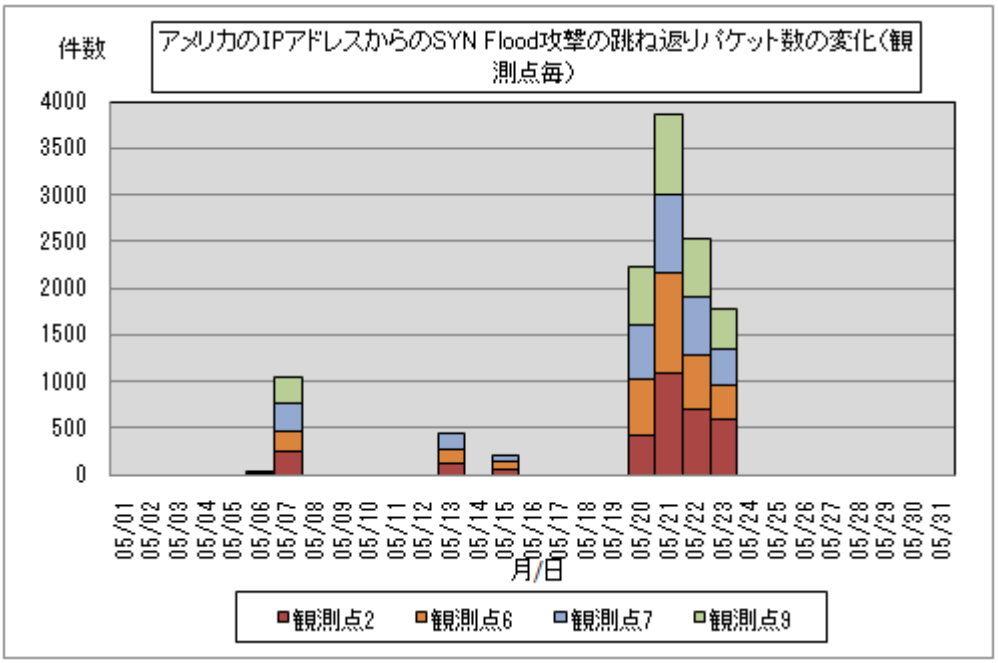

図 1-4：アメリカの IP アドレスからの SYN Flood 攻撃の跳ね返りパケット数の変化（観測点毎）

なお、5 月 26 日にも、中国の特定の IP アドレスの 7001/tcp からのアクセスが観測されていました（図 1-5 参照）。これらのアクセスも、全て SYN/ACK パケットだったことから、TALOT2 で使用しているアドレスが、攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN/ACK パケットが大量に届いていた可能性があるということです。

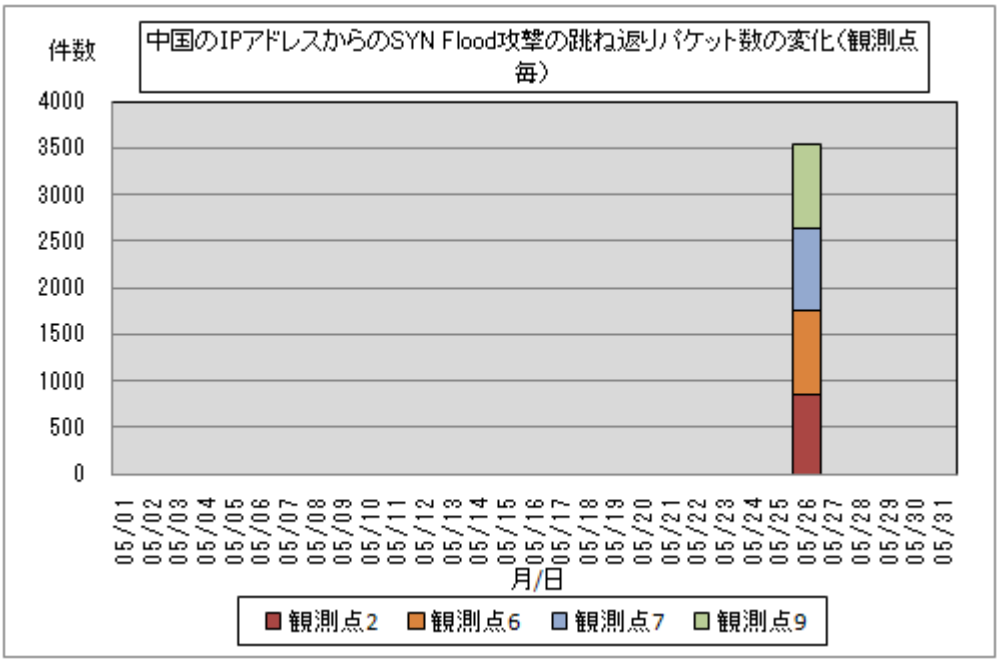

図 1-5：中国の IP アドレスからの SYN Flood 攻撃の跳ね返りパケット数の変化（観測点毎）

(*1):DoS 攻撃（SYN Flood 攻撃）

「サービス妨害攻撃」Denial of Service の略から DoS 攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。この DoS 攻撃の 1 つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット（3 ウェイ・ハンドシェーク (*2) での接続確立の最初に送られるパケット）を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、

通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下にA とB の通信確立の手順を示します。

①A からB へSYN パケットの送信

②B からA へACK+SYN パケットの送信

③A からB へACK パケットの送信

これで、AB 双方の通信が確立されます。

(*3):跳ね返りパケット

DoS 攻撃（SYN Flood 攻撃）において攻撃者が詐称した発信元アドレスに、標的マシンから大量のSYN+ACK パケットが返信されてくることです。

2. 2011年5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 5 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。

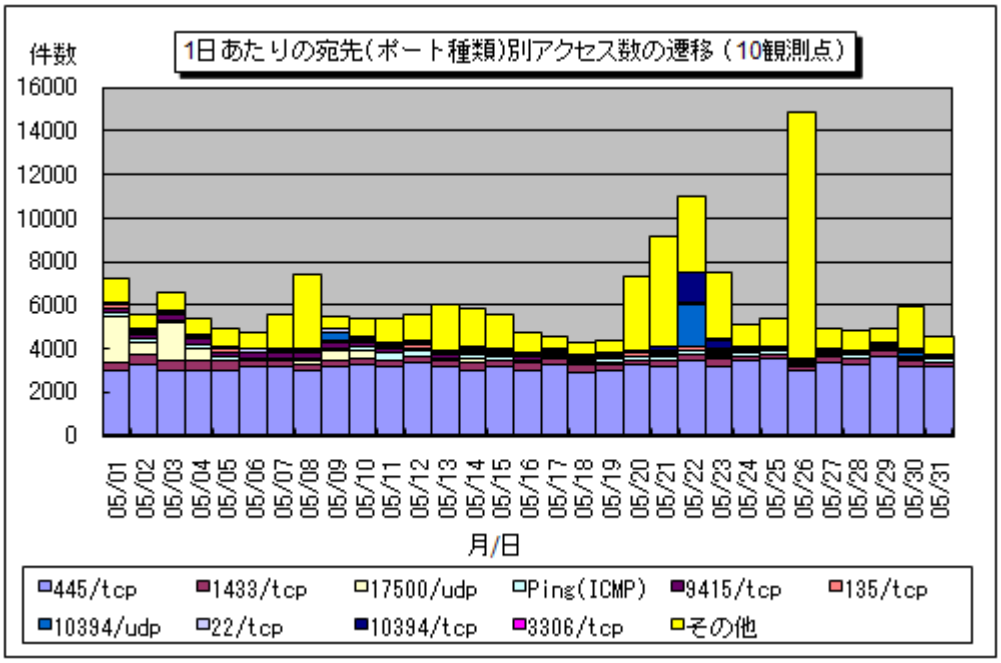

図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移（10 観測点）

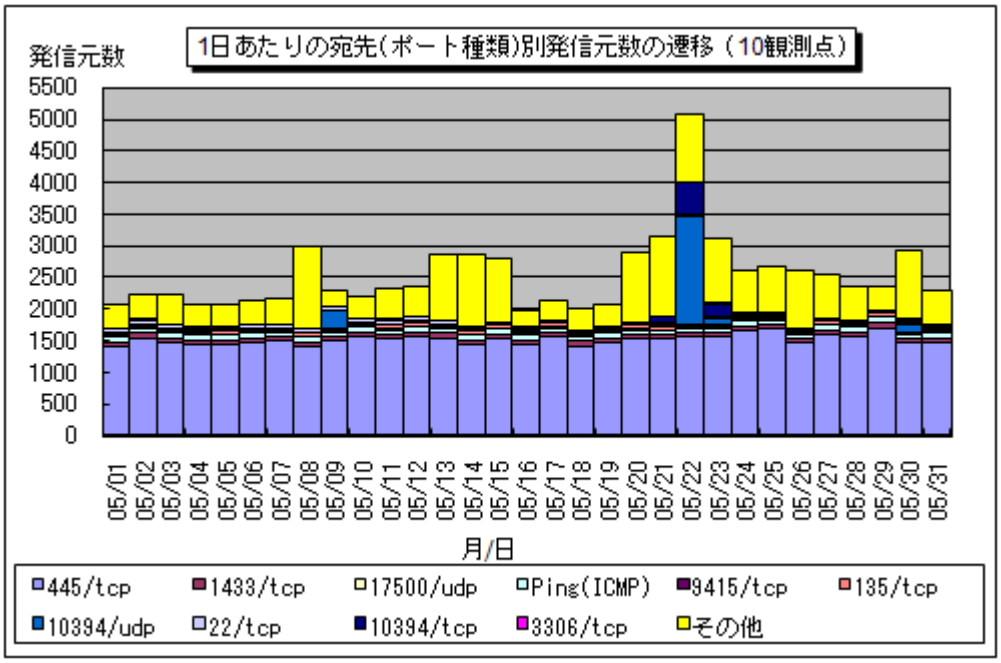

図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）

（2）宛先（ポート種類）別の比率

2011 年 5 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。

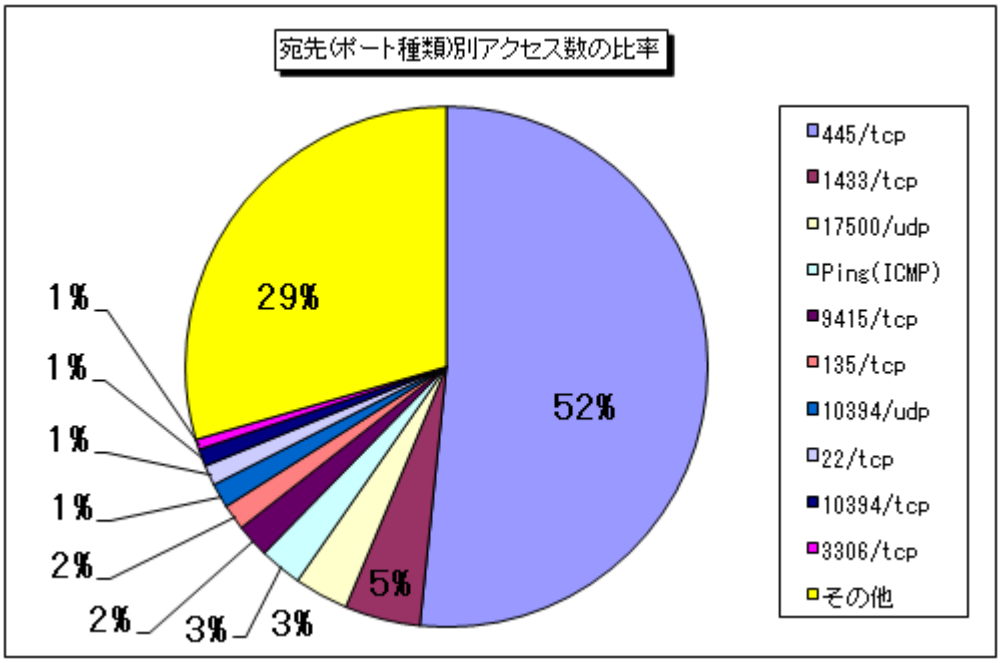

図 2-3：宛先（ポート種類）別アクセス数の比率

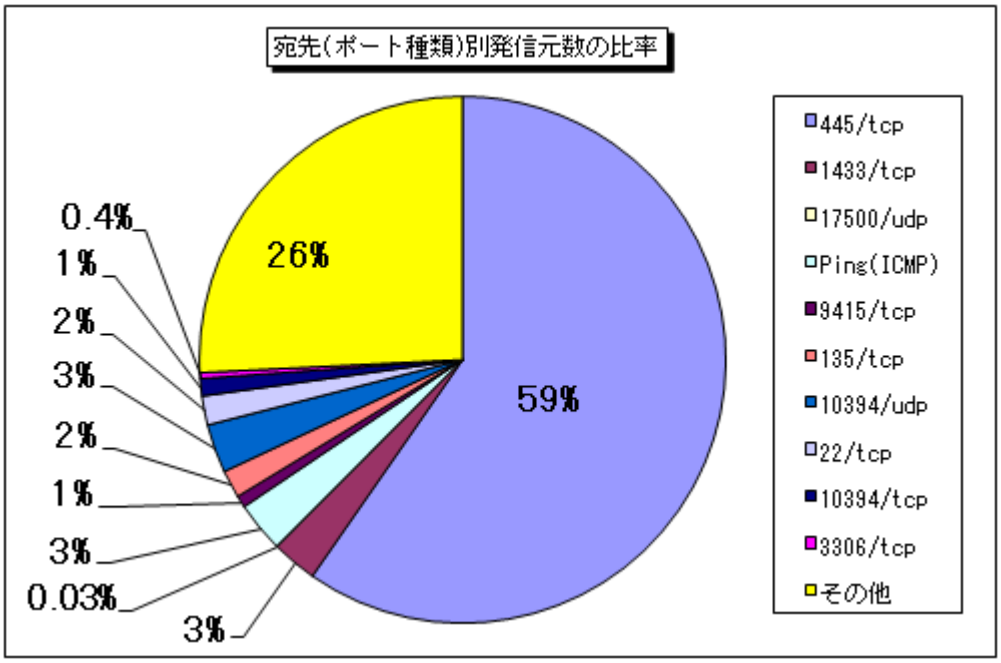

図 2-4：宛先（ポート種類）別発信元数の比率

（3）発信元地域別のアクセス状況

2011 年 5 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。

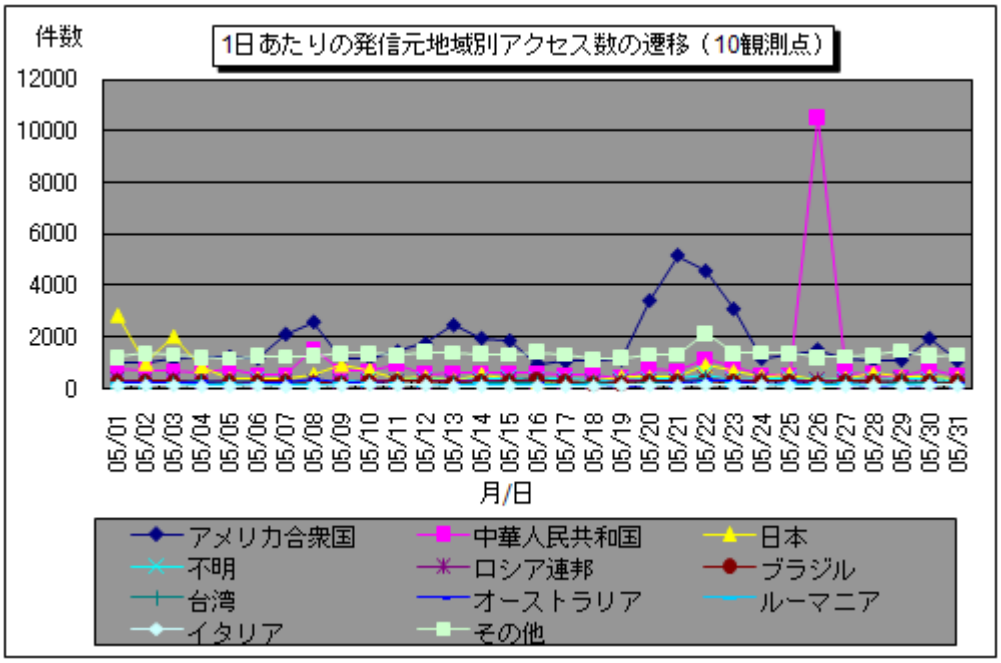

図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）

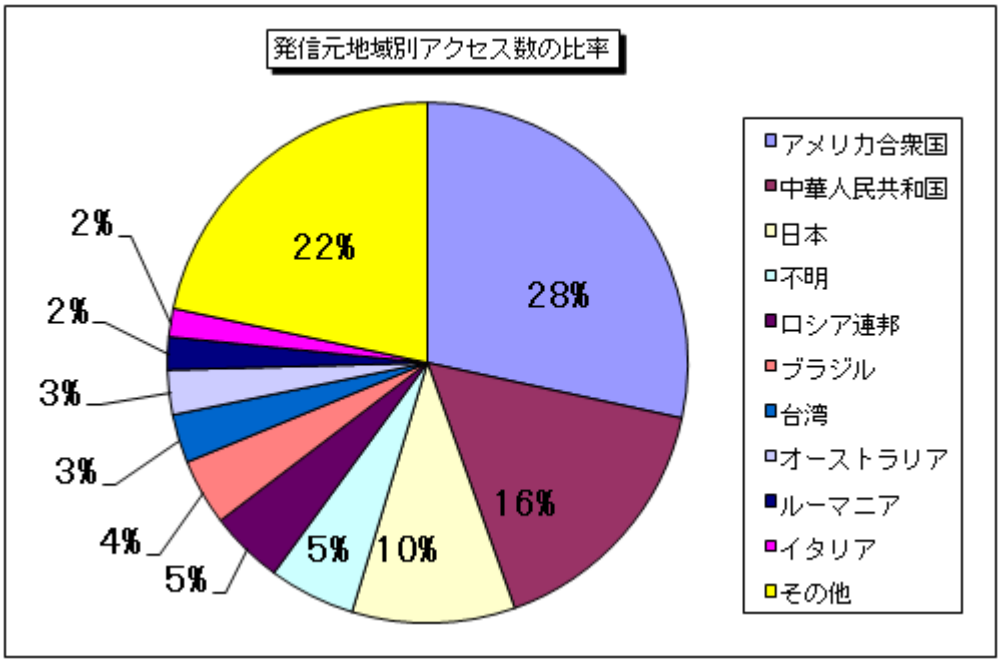

図 2-6：発信元地域別アクセス数の比率

2011 年 5 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。

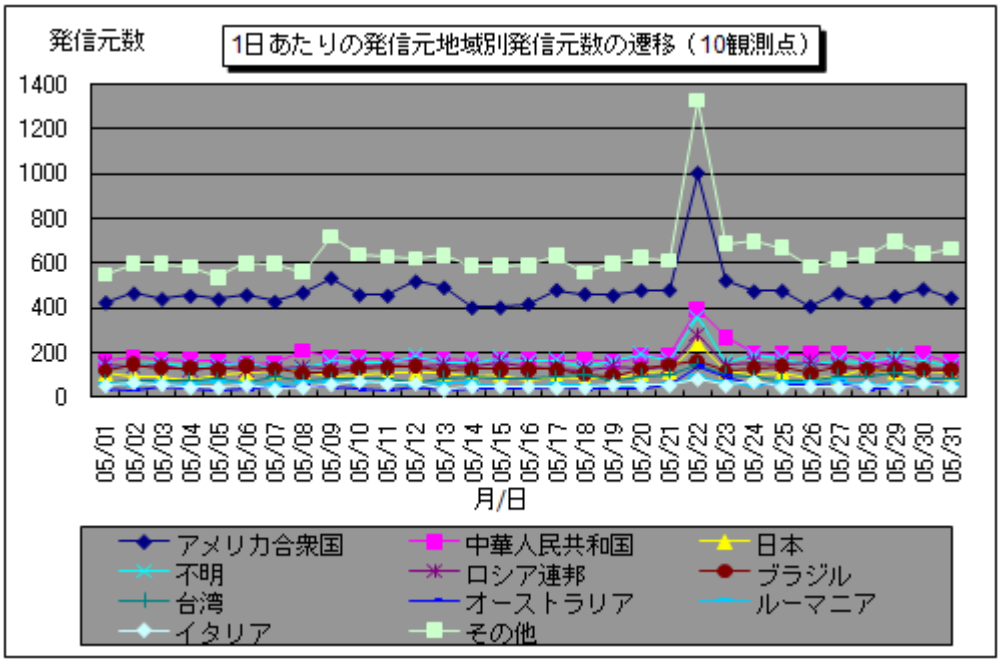

図 2-7： 1 日あたりの発信元地域別発信元数の遷移（10 観測点）

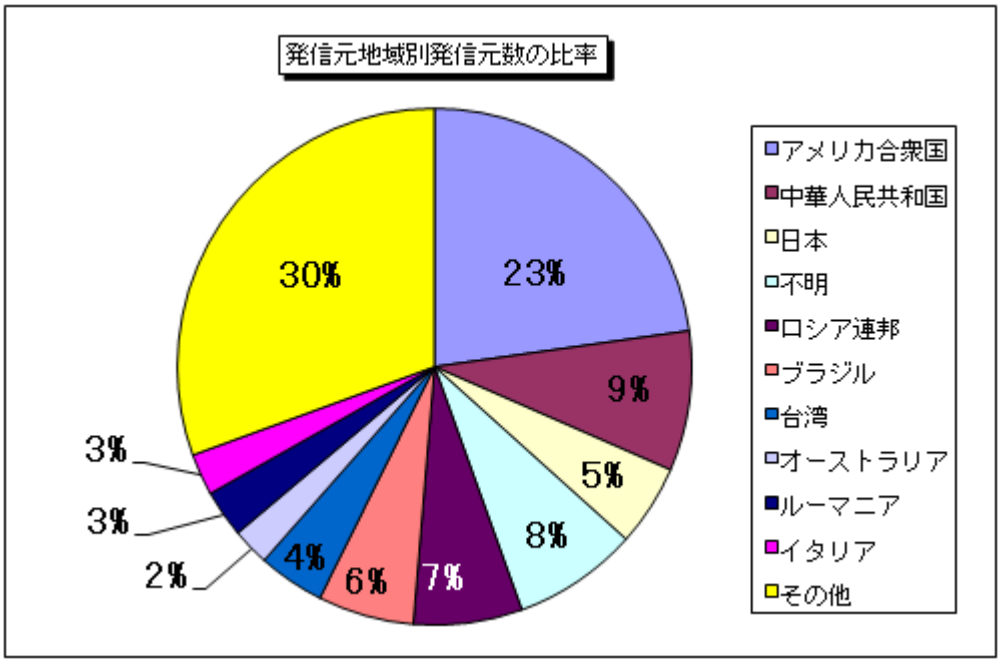

図 2-8：発信元地域別発信元数の比率

3. 統計情報

（1）宛先（ポート種類）別の比率

2010 年 12 月～2011 年 5 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。

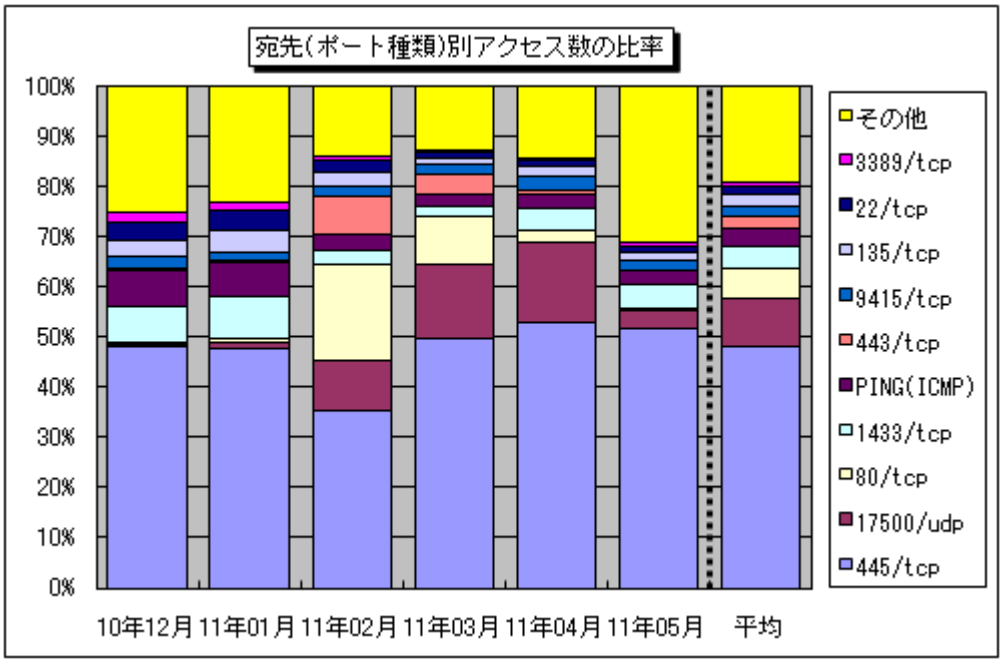

図 3-1：宛先（ポート種類）別アクセス数の比率

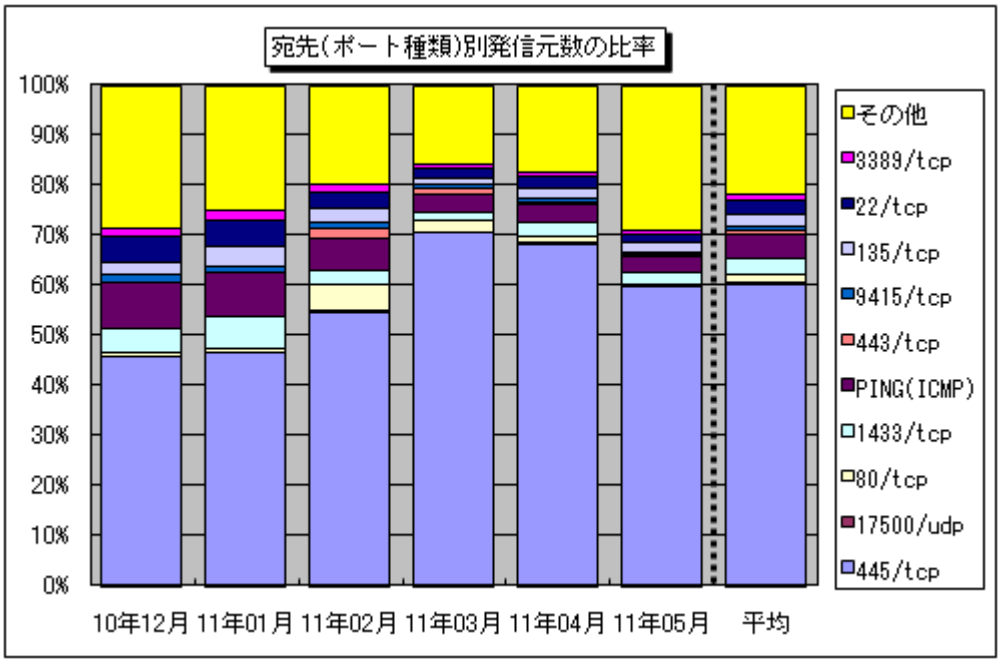

図 3-2：宛先（ポート種類）別発信元数の比率

（2）発信元地域別の比率

2010 年 12 月～2011 年 5 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。

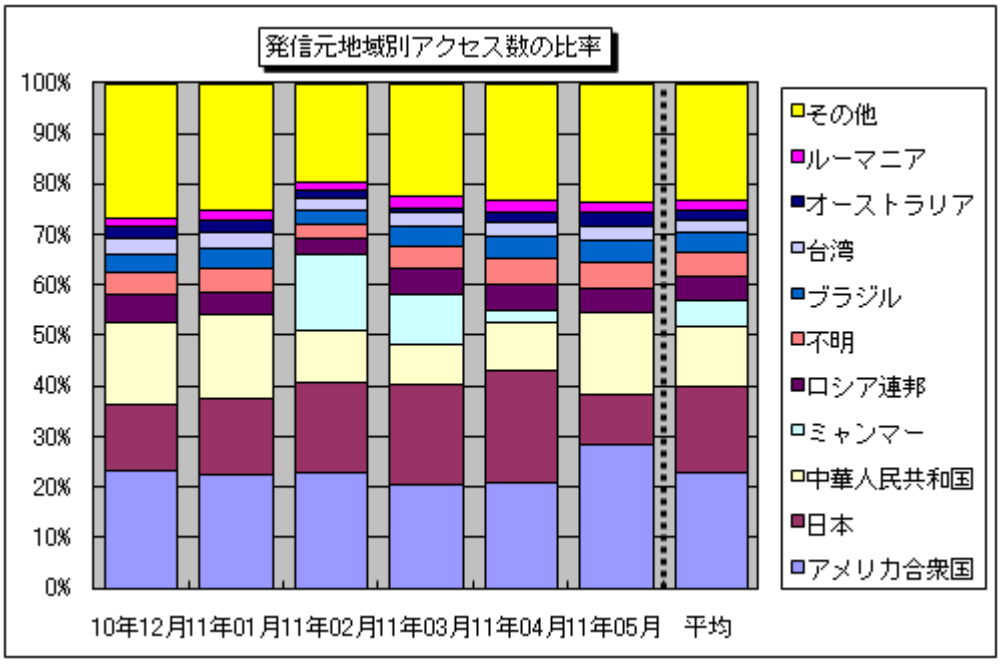

図 3-3：発信元地域別アクセス数の比率

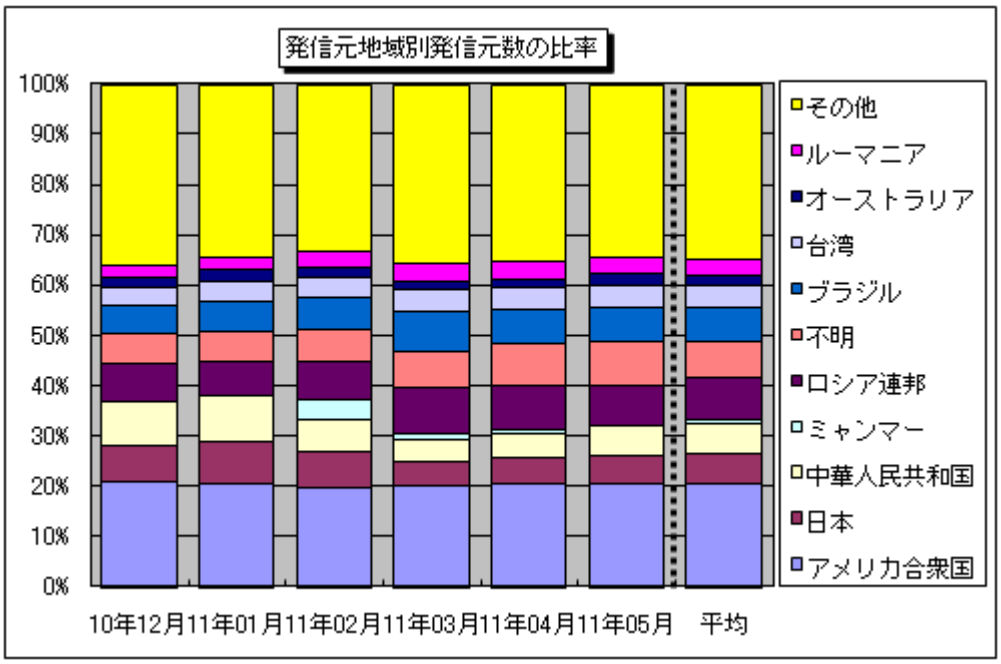

図 3-4：発信元地域別発信元数の比率

4. 補足説明

以下に、2011 年 5 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。
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。
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。
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。
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	複数の発信元から特定の 1 観測点のみに観測された、原因不明のアクセス。
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。
10394/tcp	複数の発信元から特定の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。

■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