別紙 3

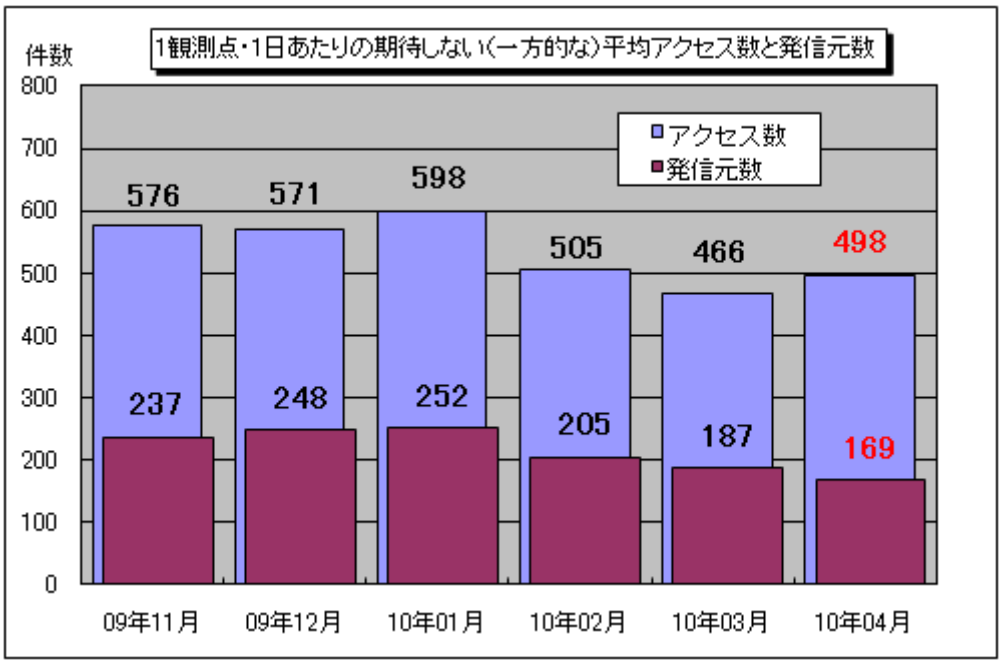
インターネット定点観測（TALOT2）での観測状況について

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 4 月の期待しない（一方的な）アクセスの総数は 10 観測点で **149,345 件**、延べ発信元数（※）は **50,563 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 169 の発信元から 498 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。



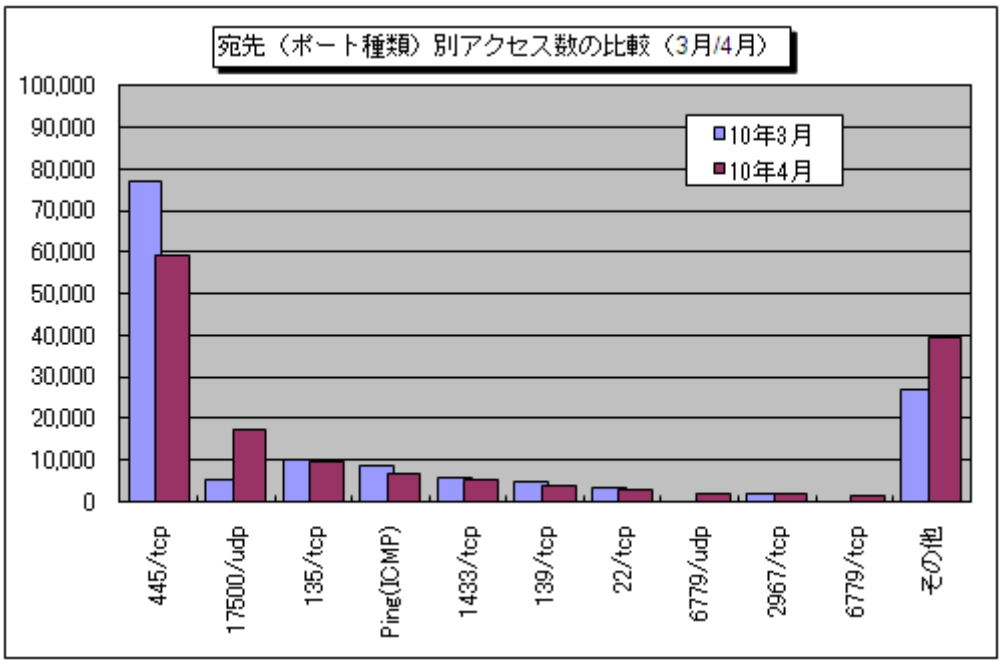
【図 1-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009 年 11 月～2010 年 4 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。4 月の期待しない（一方的な）アクセスは、3 月と比べて増加しました。

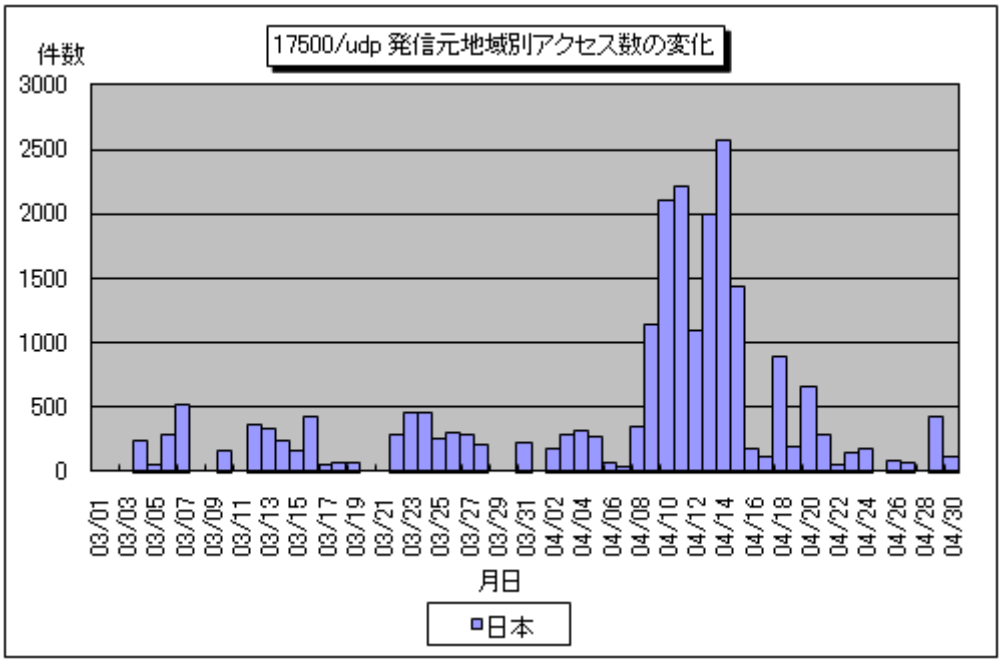
3 月と 4 月の宛先（ポート種類）別アクセス数の比較を図 1-2 に示します。これをみると 3 月に増加が観測されていた 17500/udp へのアクセスが、さらに大幅な増加を示していました（図 1-3 参照）。このアクセスの特徴としては、TALOT2 の特定の 1 観測点に対して、同一セグメント内の複数の IP アドレスから規則的な間隔で送られていたという点が挙げられます。このアクセスについて調査したところ、17500/udp に対してブロードキャストを送信するアプリケーションが存在することが分かったため、これが原因の一つと考えられます。複数と思われていた発信元 IP アドレスは、実はパソ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、3 月は全く観測されなかった 6779/tcp および 6779/udp へのアクセスが、多く観測されました。これらのポートは、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が、いずれも特定の 1 観測点でしか観測されていませんでした。



【図 1-2：宛先（ポート種類）別アクセス数の比較（3 月/4 月）】

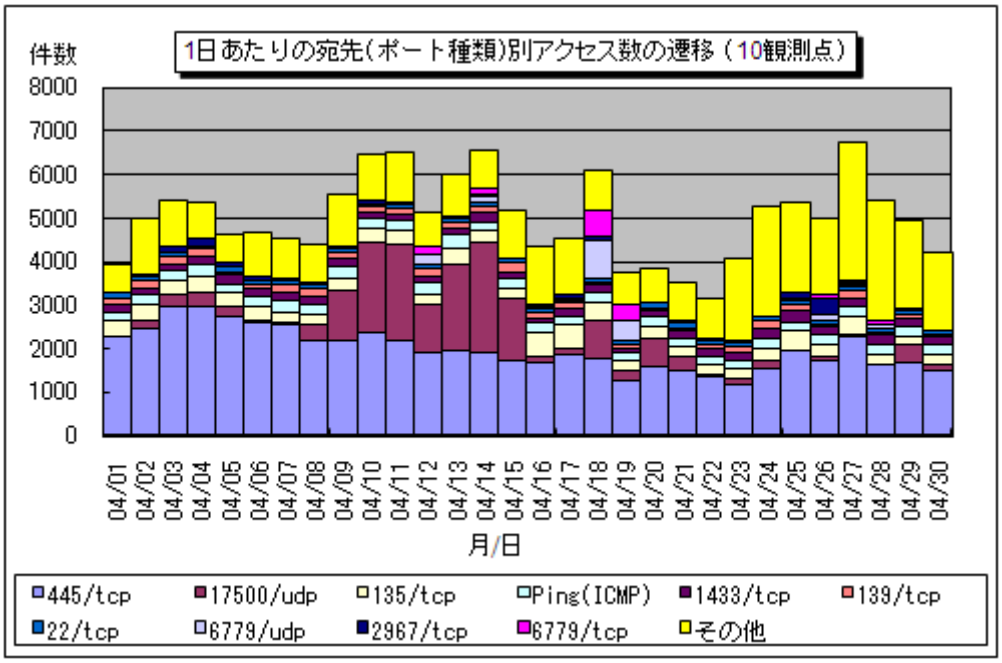


【図 1-3：17500/udp 発信元地域別アクセス数の変化】

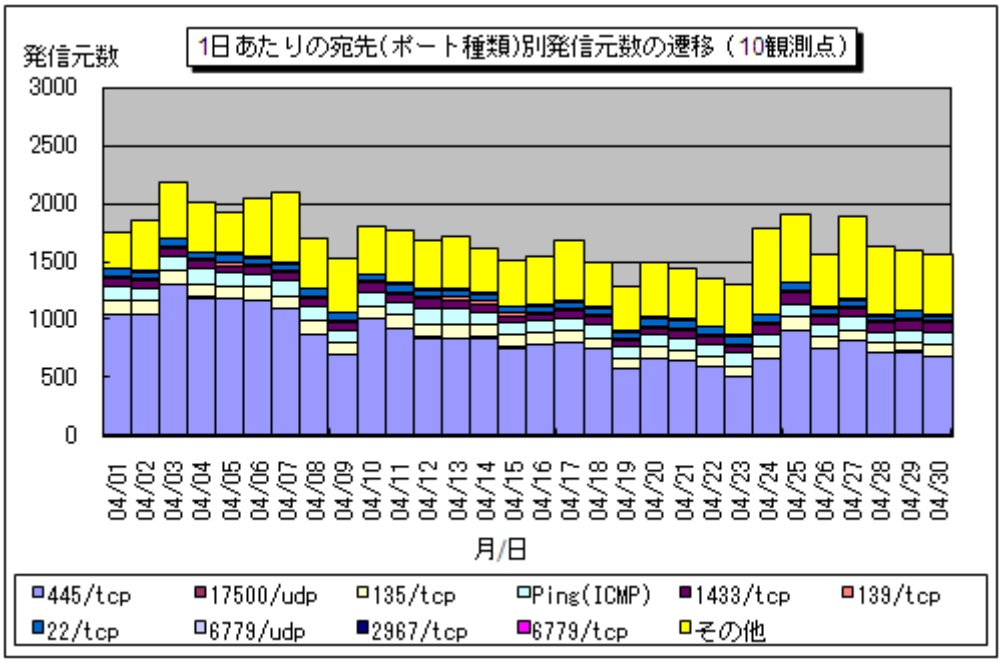
2. 2010 年 4 月の一方的なアクセス状況

（1） 宛先（ポート種類）別のアクセス状況

2010 年 4 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。



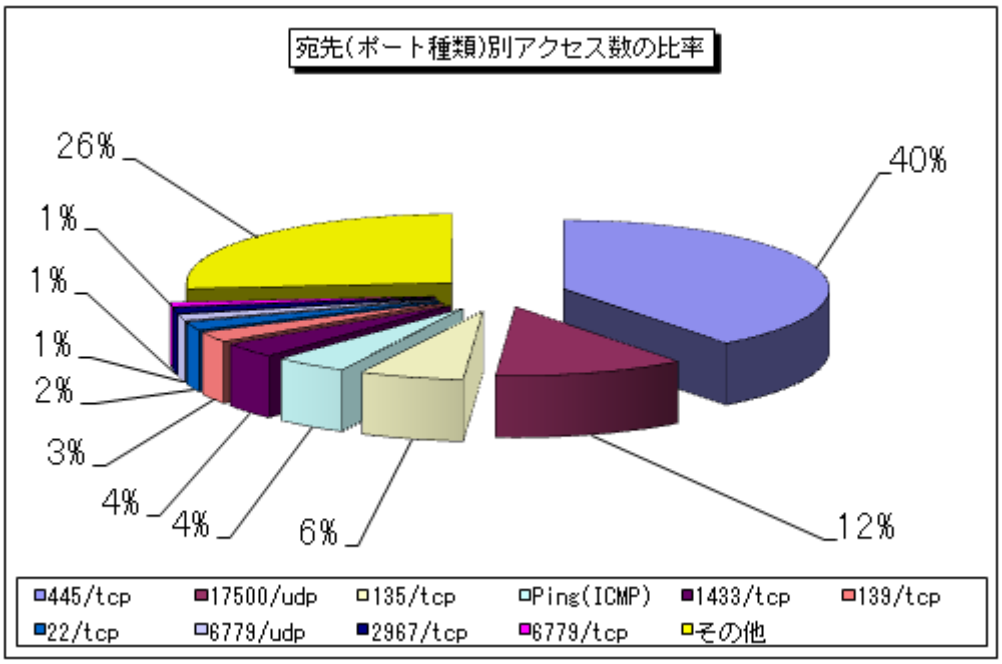
【図 2-1：1 日あたりの宛先（ポート種類）別アクセス数の遷移(10 観測点)】



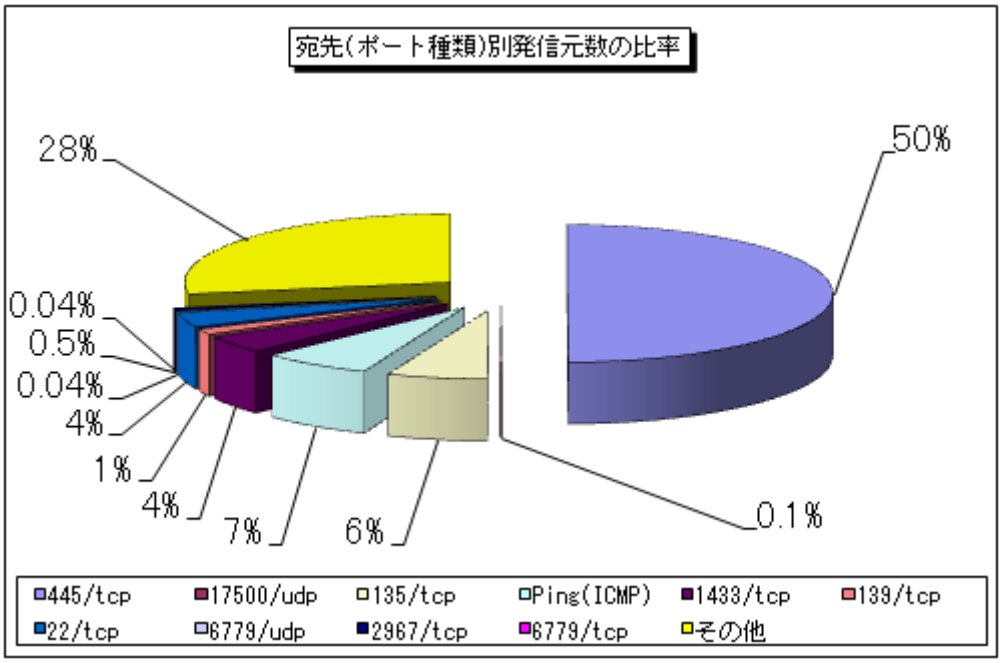
【図 2-2： 1 日あたりの宛先（ポート種類）別発信元数の遷移（10 観測点）】

（2）宛先（ポート種類）別の比率

2010 年 4 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。



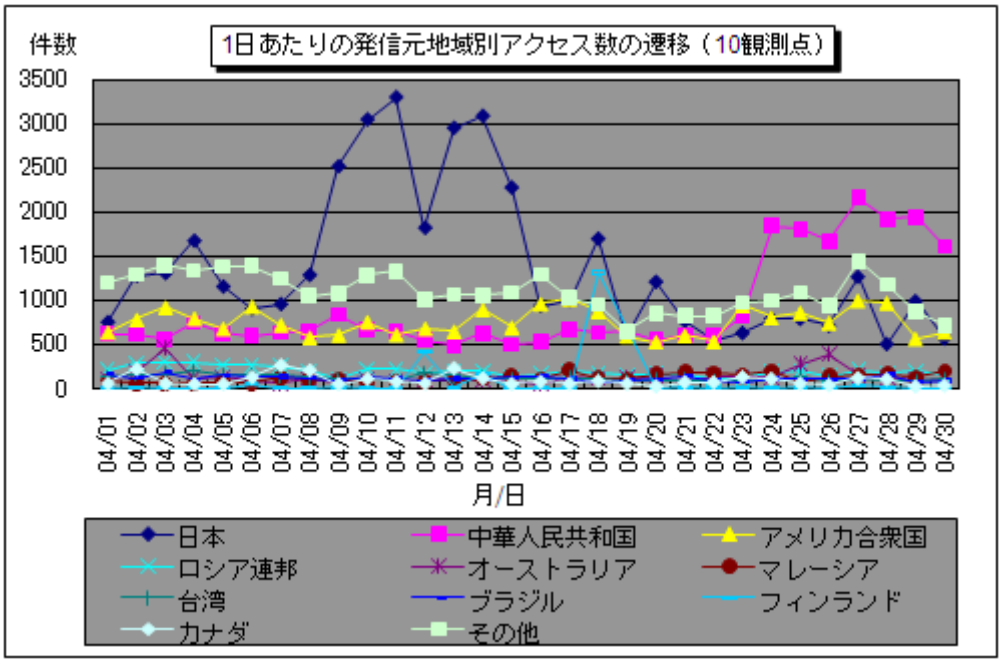
【図 2-3：宛先（ポート種類）別アクセス数の比率】



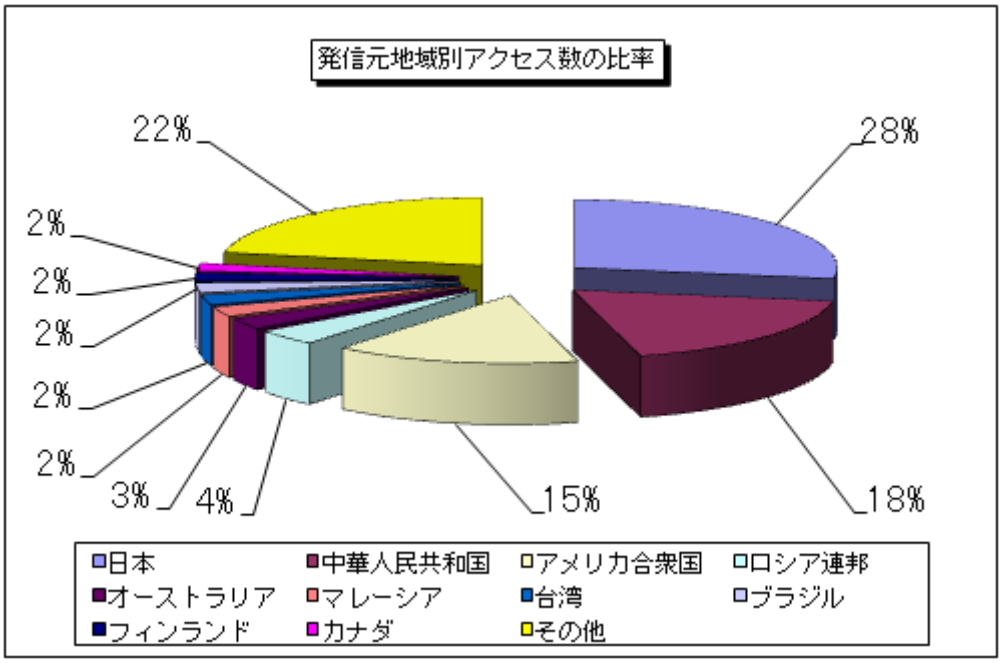
【図 2-4：宛先（ポート種類）別発信元数の比率】

（3）発信元地域別のアクセス状況

2010 年 4 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。

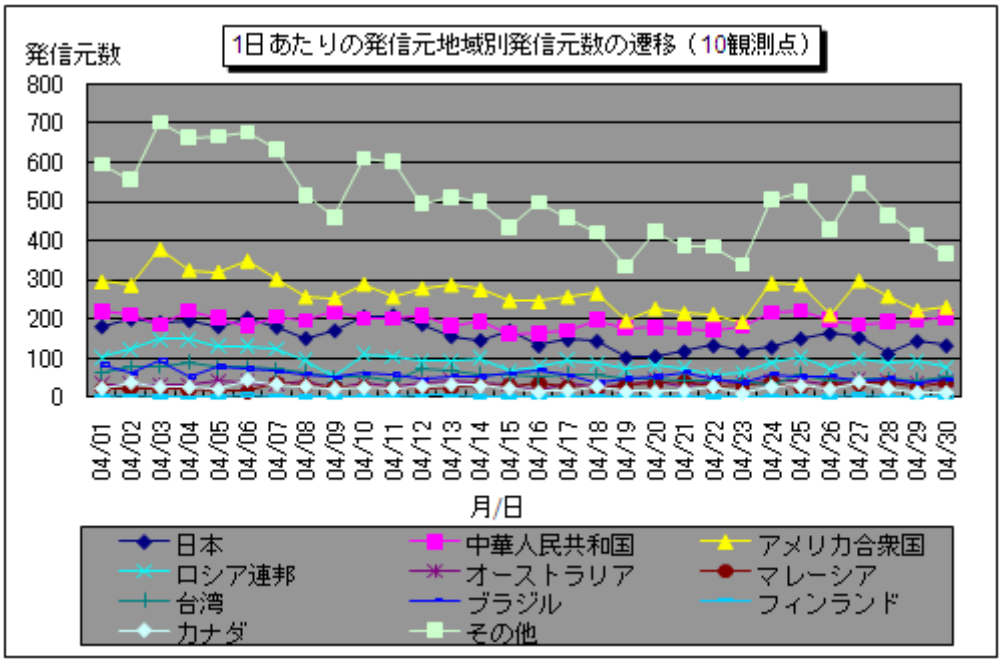


【図 2-5：1 日あたりの発信元地域別アクセス数の遷移（10 観測点）】

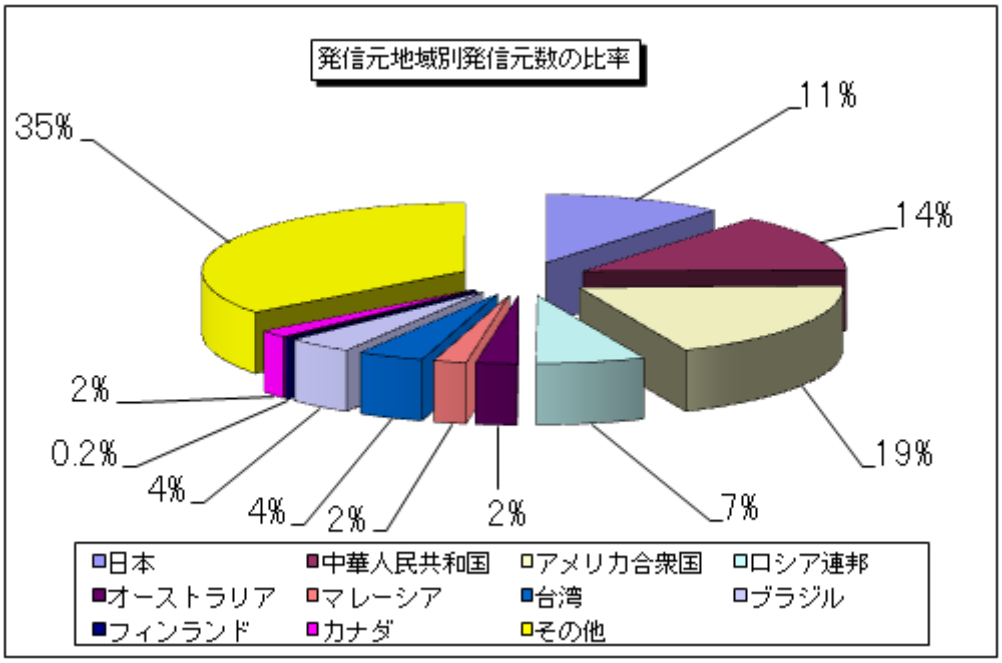


【図 2-6：発信元地域別アクセス数の比率】

2010 年 4 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）】

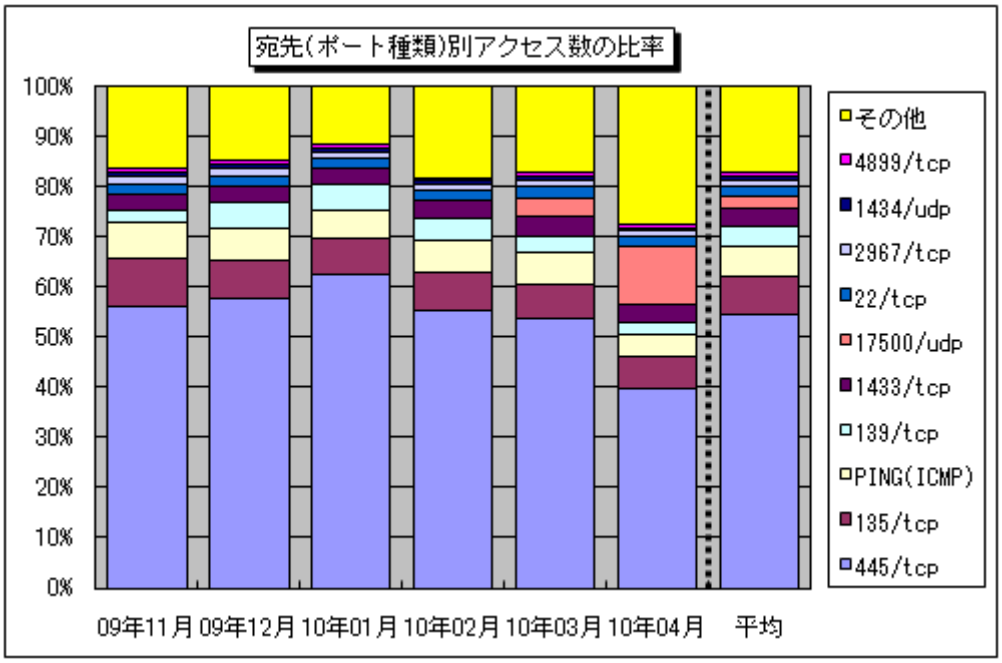


【図 2-8：発信元地域別発信元数の比率】

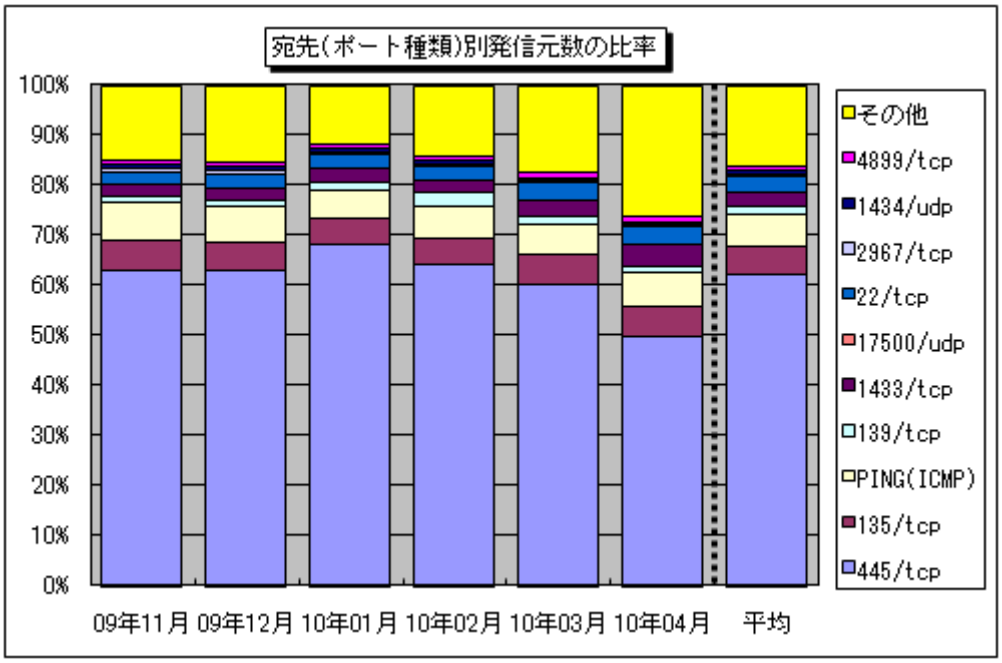
3. 統計情報

（1）宛先（ポート種類）別の比率

2009 年 11 月～2010 年 4 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。



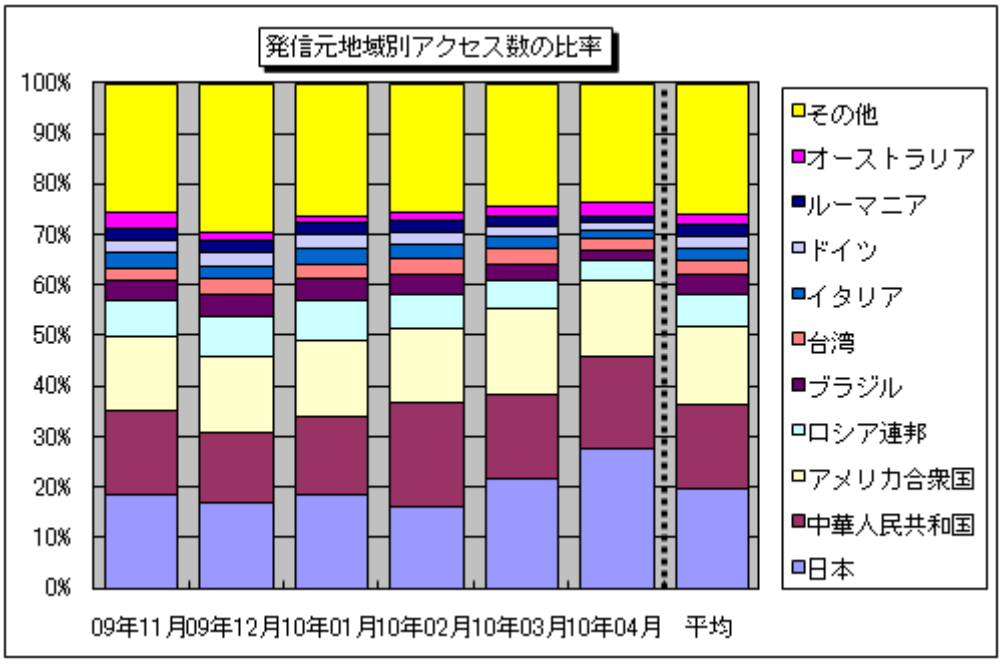
【図 3-1：宛先（ポート種類）別アクセス数の比率】



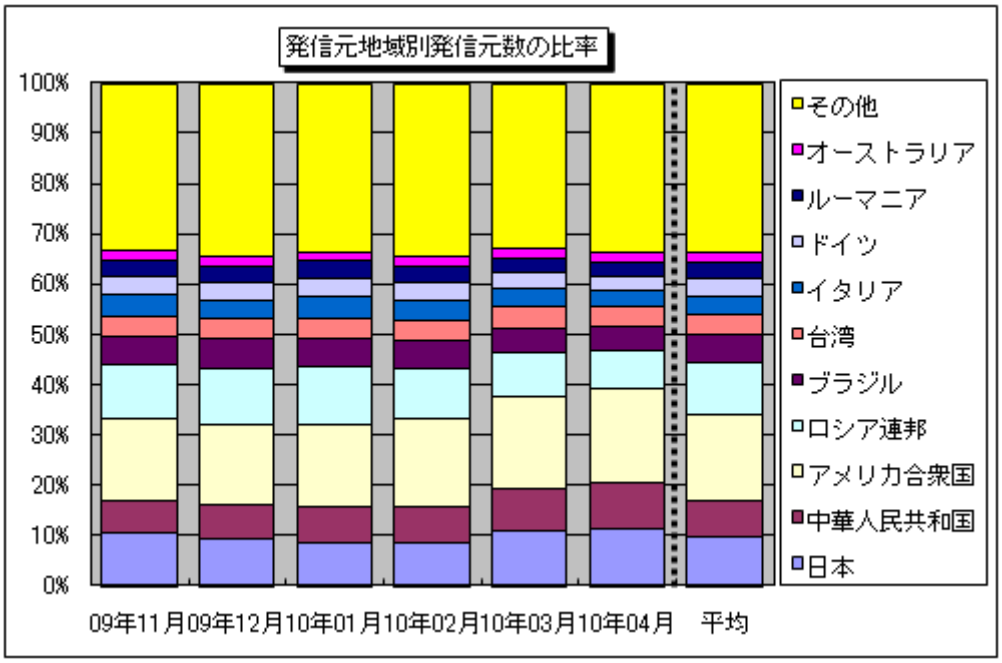
【図 3-2：宛先（ポート種類）別発信元数の比率】

（2）発信元地域別の比率

2009 年 11 月～2010 年 4 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 4 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）。
17500/udp	3 月から特定の観測点でのみ観測されはじめた、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。
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）。
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。
139/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。
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。
6779/udp	4 月の後半に特定の観測点のみで観測された、目的不明のアクセス。
2967/tcp	Symantec 製品（Symantec Client Security や Symantec AntiVirus など）の脆弱性を狙ったアクセスである可能性が高い。
6779/tcp	4 月の後半に特定の観測点のみで観測された、目的不明のアクセス。

■お問い合わせ先
IPA セキュリティセンター　大浦／花村／加賀谷
Tel:03-5978-7527　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp