別紙 3

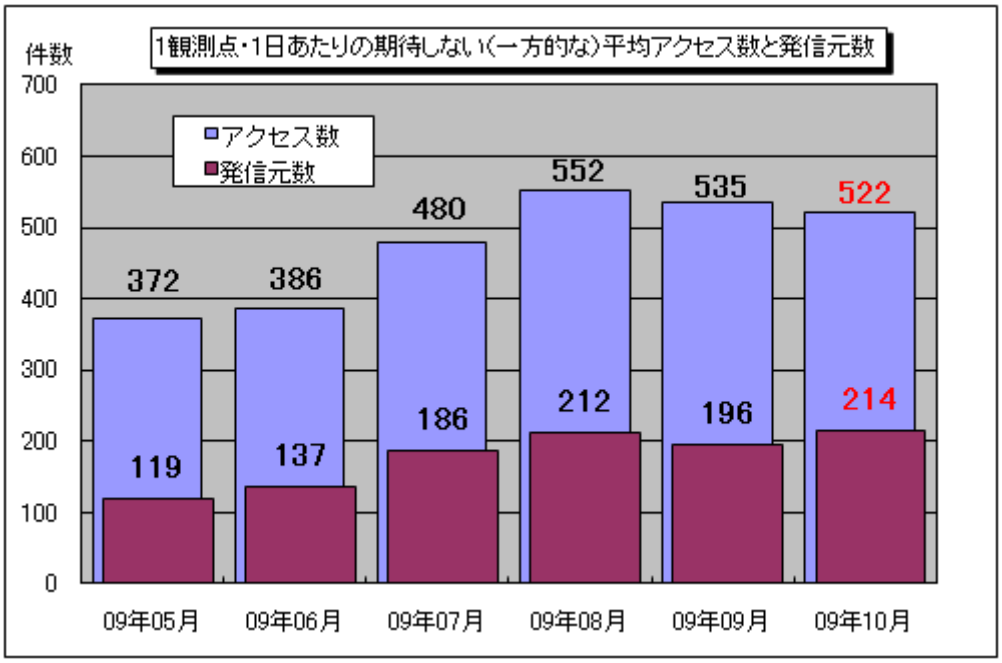
インターネット定点観測（TALOT2）での観測状況について

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、2009 年 10 月の期待しない（一方的な）アクセスの総数は 10 観測点で **161,716 件**、延べ発信元数 (※) は **66,430 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 214 の発信元から 522 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 5 月～2009 年 10 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。10 月の期待しない（一方的な）アクセスは、9 月と比べて若干減少しました。

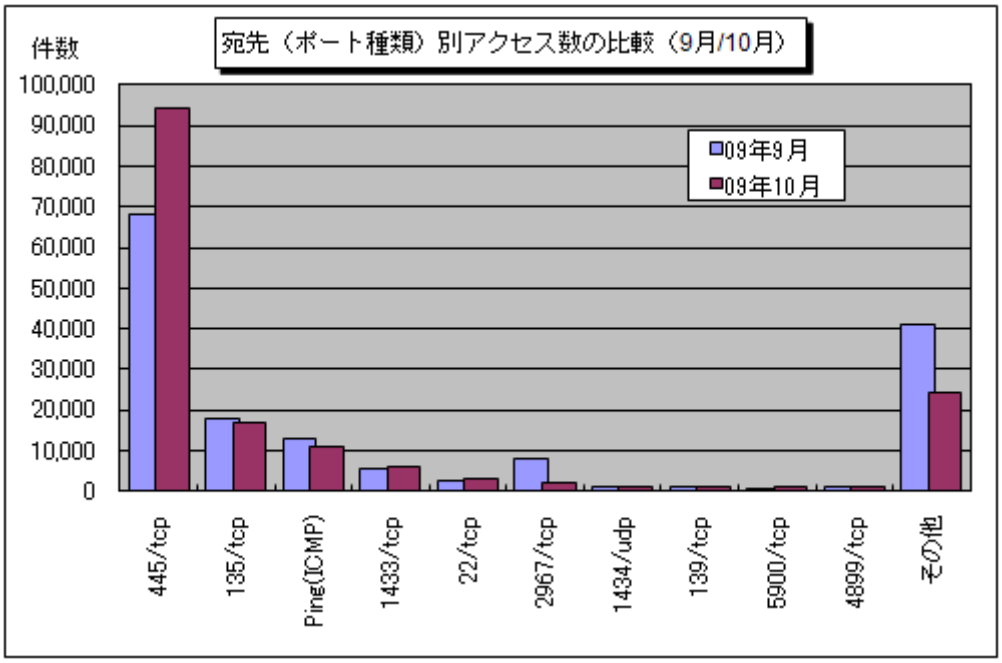
9 月と 10 月の宛先（ポート種類）別アクセス数の比較を図 1-2 に示します。

9 月と 10 月のアクセス数を比較したところ、445/tcp へのアクセスが 9 月に比べて約 1.4 倍に増加していました。

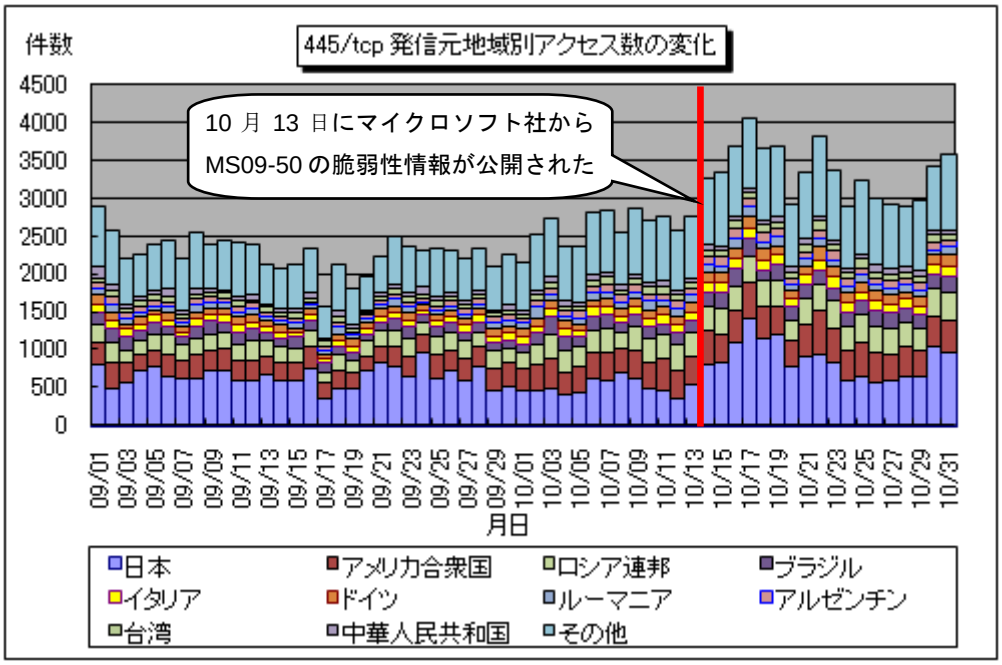
445/tcp は Windows の脆弱性（MS08-067）を悪用するワームなど、ウイルスによって狙われる可能性の高いポートとして有名です。2009 年 10 月 13 日（米国時間）にマイクロソフト社から公開された「Windows における SMBv2 (※) の脆弱性（MS09-050）」も 445/tcp を悪用するものでした。

TALOT2 では、脆弱性情報が公開されたあたりから 445/tcp へのアクセスの若干の増加が観測されていたことから、この脆弱性を悪用しようとするなんらかの動きがあった可能性があります（図 1-3 参照）。この脆弱性は、脆弱性情報の公開と同時に提供された修正プログラムを適用することで恒久的な処置が可能ですので、まだ適用されてない場合はただちに実施してください。

SMBv2（※）：SMB（Server Message Block）とは、既定で Windows ベースのコンピュータ上で使用されるファイル共有プロトコルです。 SMBv2 (SMB Version 2.0) とはこのプロトコルに対する更新で、Windows Server 2008、Windows 7 および Windows Vista を実行しているコンピュータでのみサポートされています。



【図 1-2：宛先（ポート種類）別アクセス数の比較（9 月/10 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）】

＜参考情報＞

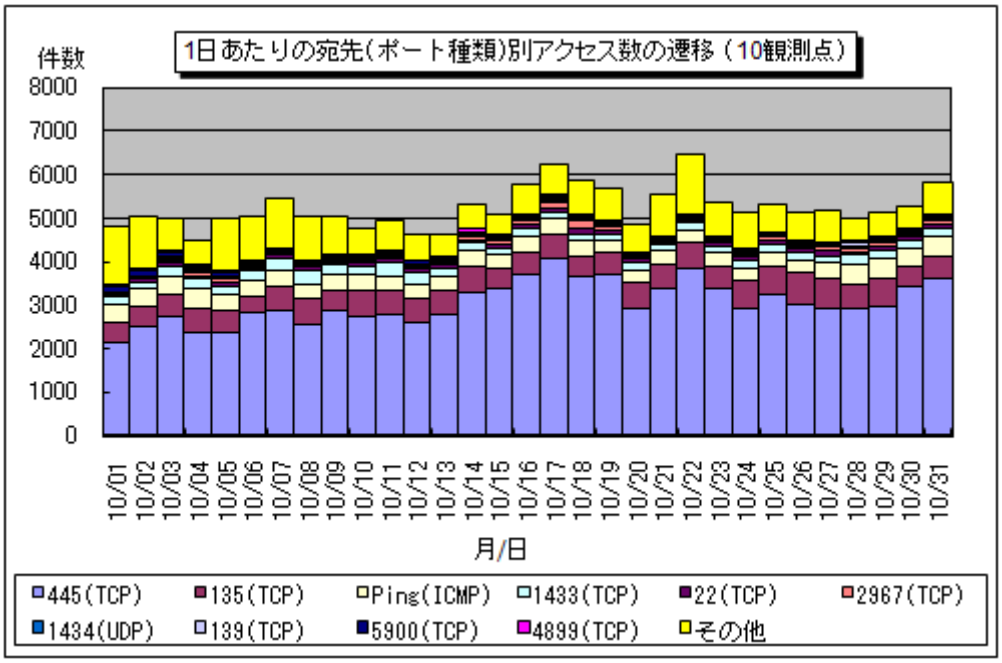
■「SMBv2 の脆弱性により、リモートでコードが実行される」(マイクロソフト社)
http://www.microsoft.com/japan/technet/security/bulletin/MS09-050.mspx

■「Microsoft Windows における SMBv2 の脆弱性（MS09-050）について」（IPA）
http://www.ipa.go.jp/security/ciadr/vul/20091014-ms09-050.html

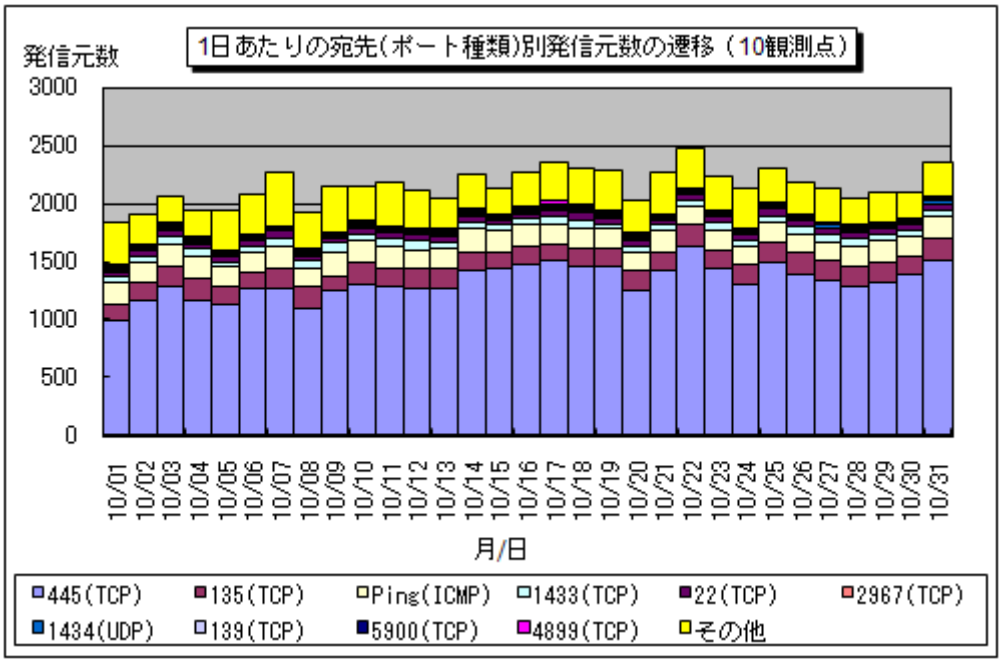
2. 2009 年 10 月の一方的なアクセス状況

（1） 宛先（ポート種類）別のアクセス状況

2009 年 10 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。



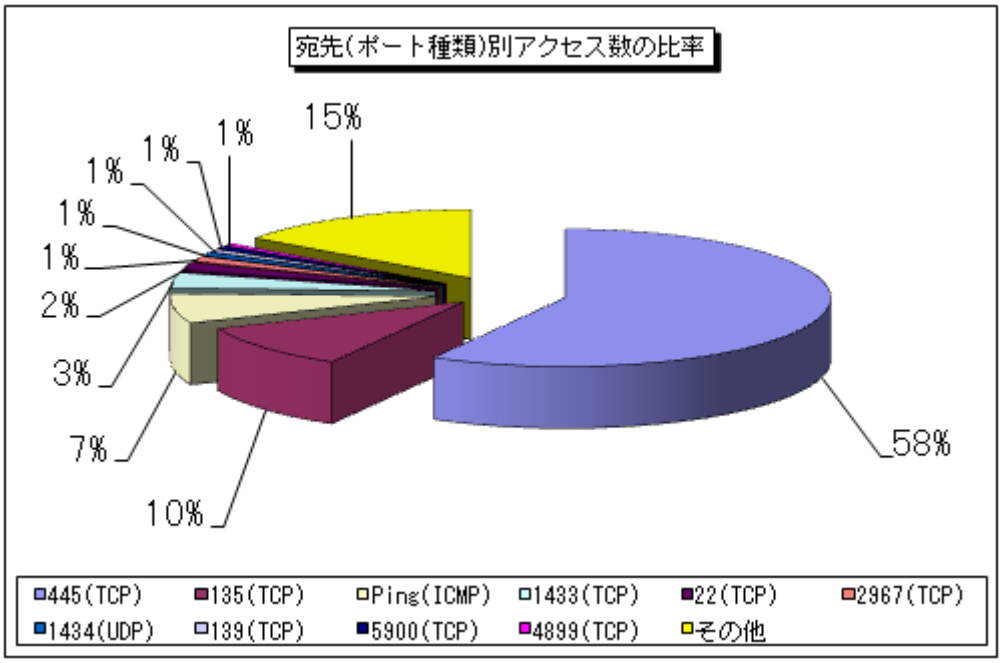
【図 2-1：2009 年 10 月の 1 日あたりの宛先（ポート種類）別アクセス数の遷移】



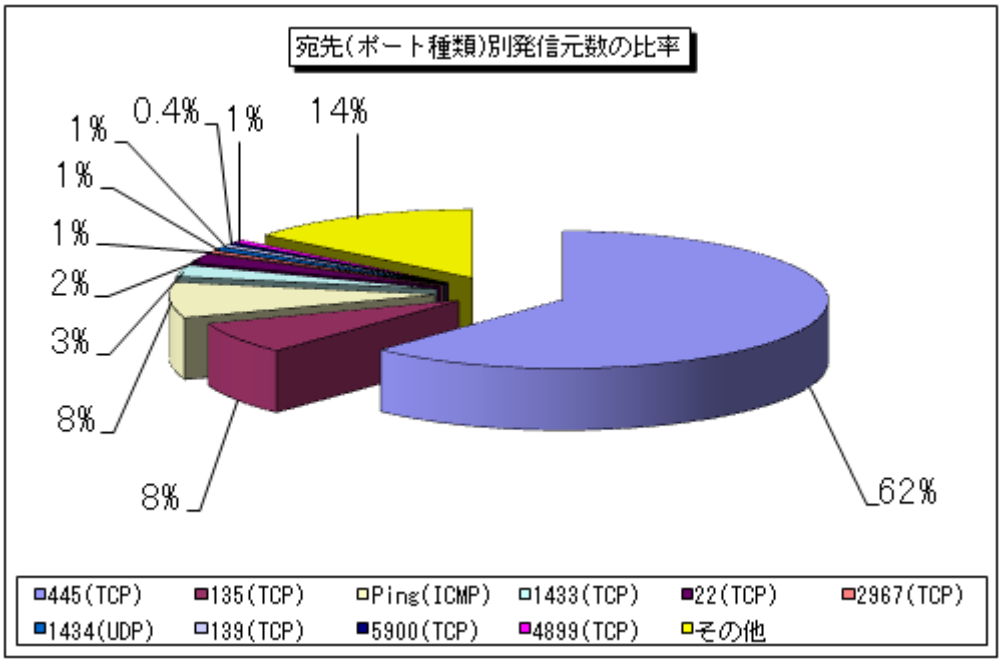
【図 2-2：2009 年 10 月の 1 日あたりの宛先（ポート種類）別発信元数の遷移】

（2）宛先（ポート種類）別の比率

2009 年 10 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。



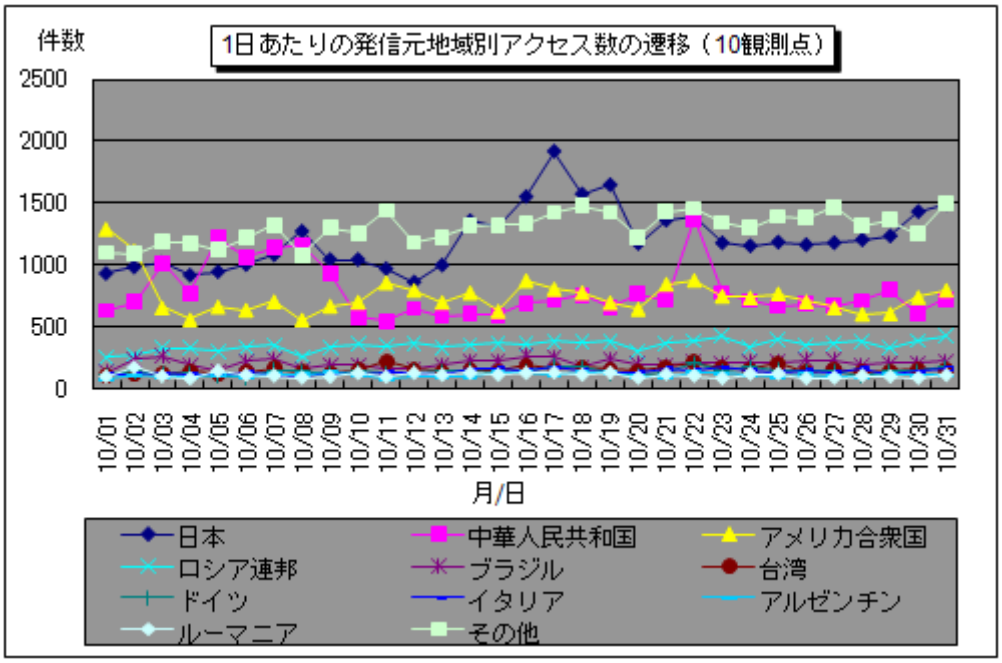
【図 2-3：2009 年 10 月の宛先（ポート種類）別アクセス数の比率】



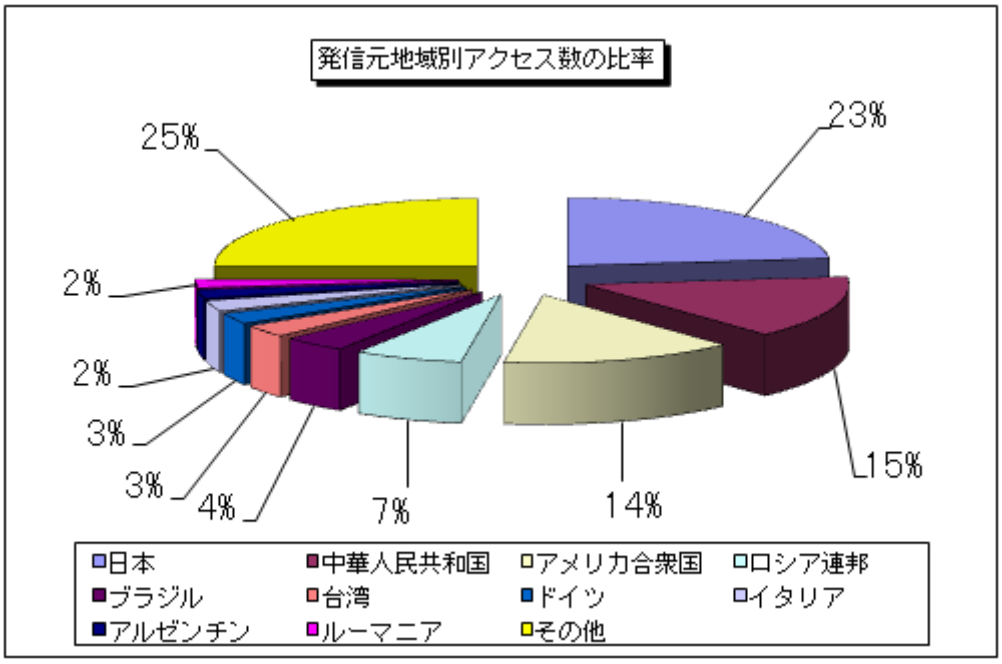
【図 2-4：2009 年 10 月の宛先（ポート種類）別発信元数の比率】

（3）発信元地域別のアクセス状況

2009 年 10 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。

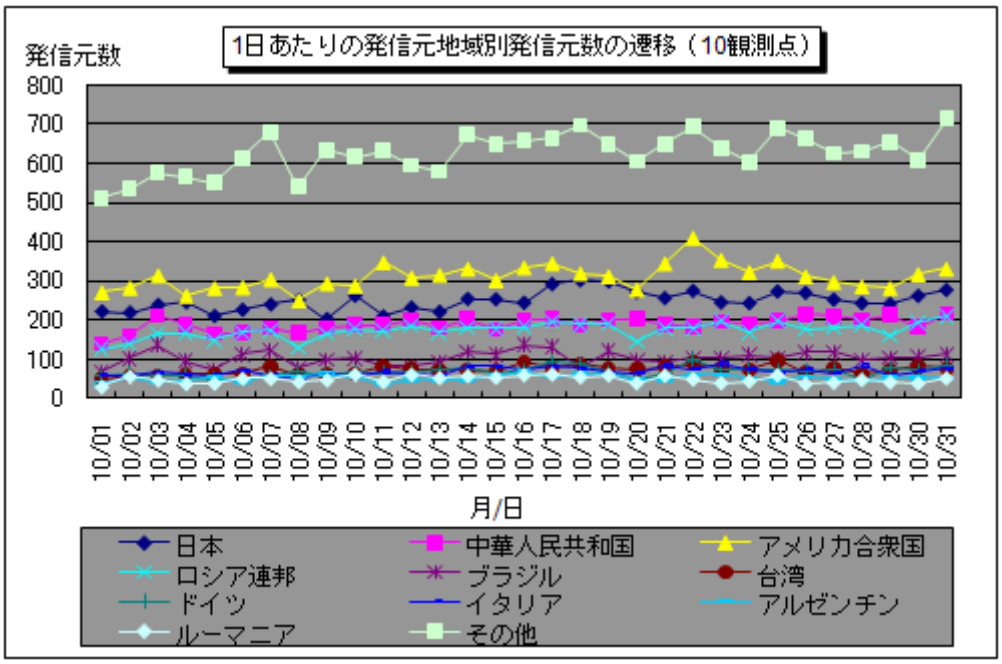


【図 2-5：2009 年 10 月の 1 日あたりの発信元地域別アクセス数の遷移】

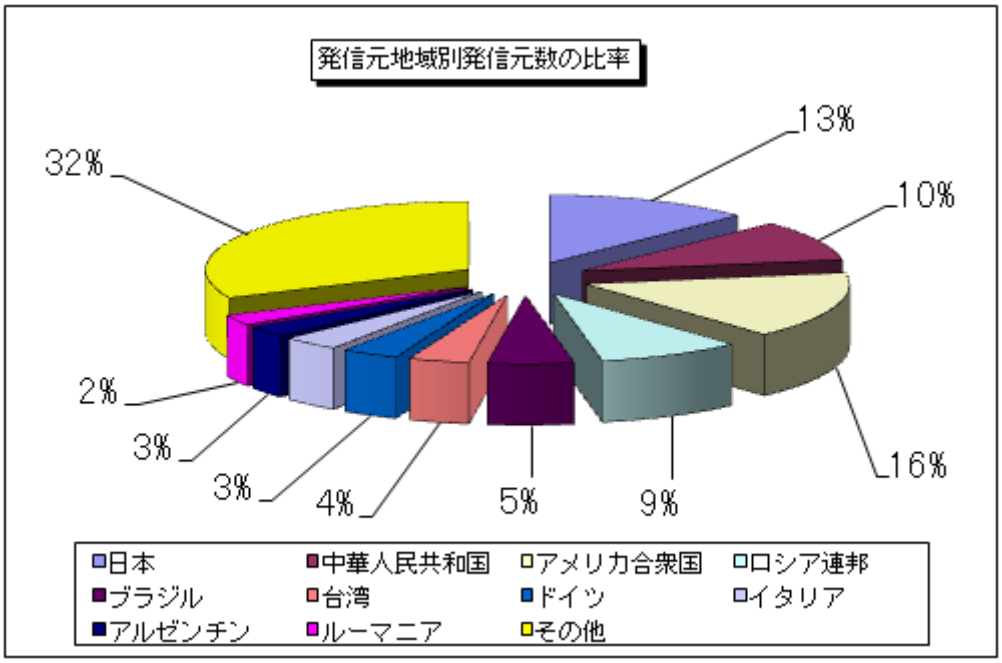


【図 2-6：2009 年 10 月の発信元地域別アクセス数の比率】

2009 年 10 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 2-7：2009 年 10 月の 1 日あたりの発信元地域別発信元数の遷移】

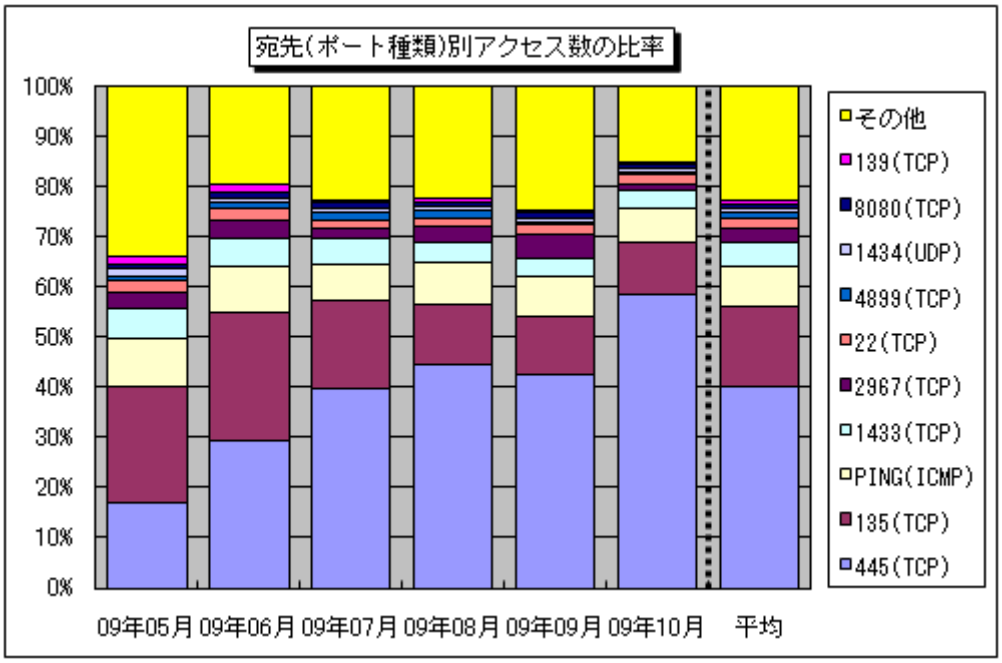


【図 2-8：2009 年 10 月の発信元地域別発信元数の比率】

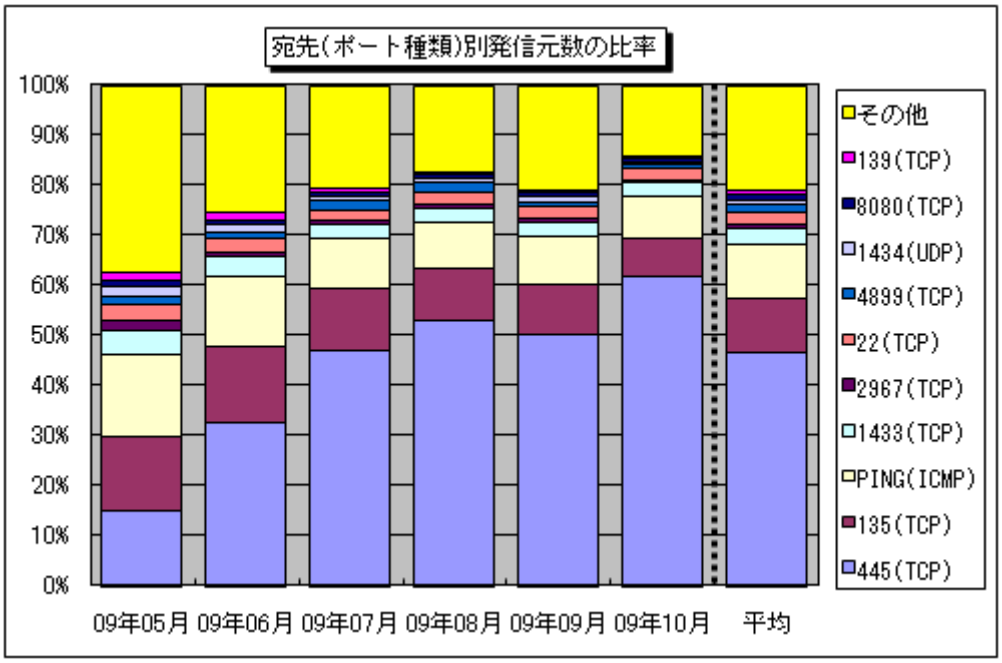
3. 統計情報

（1）宛先（ポート種類）別の比率

2009 年 5 月～2009 年 10 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。



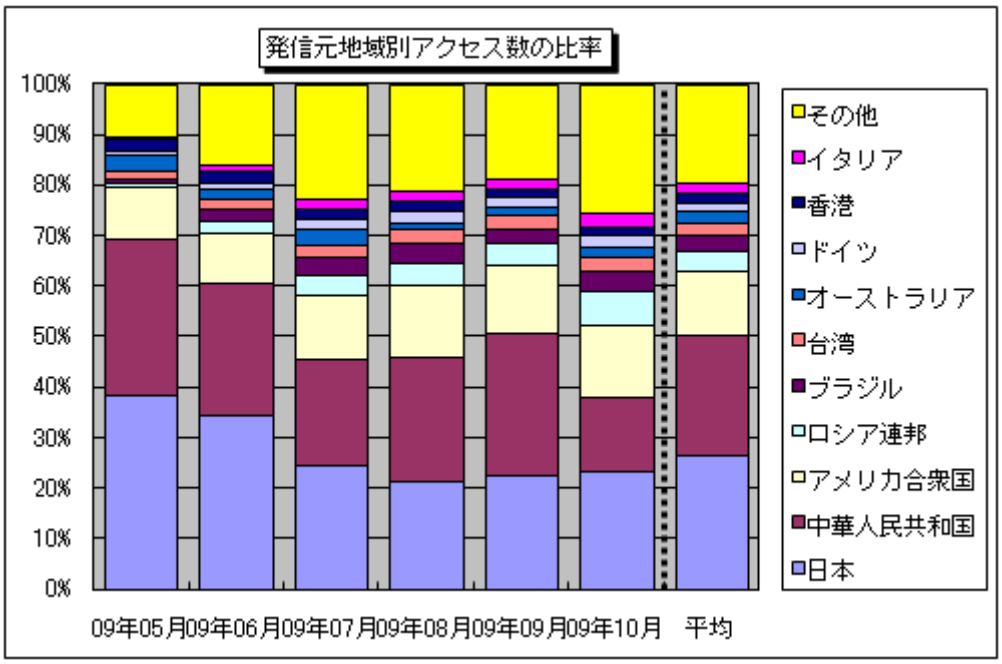
【図 3-1：2009 年 5 月～2009 年 10 月の宛先（ポート種類）別アクセス数の比率】



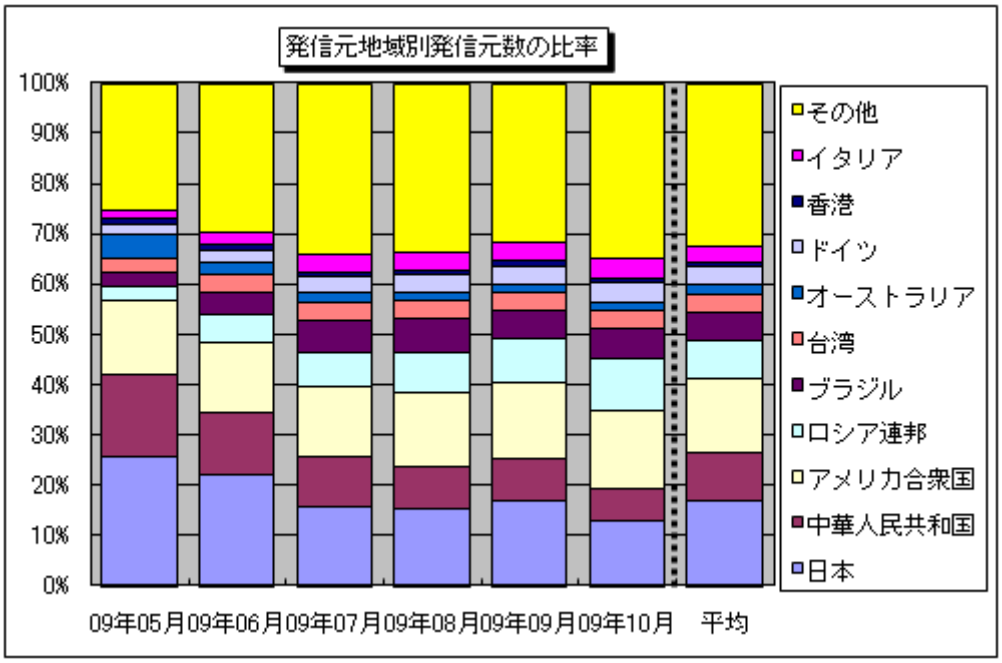
【図 3-2：2009 年 5 月～2009 年 10 月の宛先（ポート種類）別発信元数の比率】

（2）発信元地域別の比率

2009 年 5 月～2009 年 10 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 3-3：2009 年 5 月～2009 年 10 月の発信元地域別アクセス数の比率】



【図 3-4：2009 年 5 月～2009 年 10 月の発信元地域別発信元数の比率】

4. 補足説明

以下に、2009 年 10 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）。
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、SQL Server が動作中のコンピュータを探す目的や、SQL Server の脆弱性を狙った不正アクセスなど。
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。
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。
1434/udp	Microsoft SQL Sever の脆弱性を狙った不正アクセスなどが有名(W32/SQLSlammer)など。
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です。
5900/tcp	リモートアクセスツール RealVNC のぜい弱性を狙っていると思われるアクセスです。
4899/tcp	リモート操作を行うための RAdmin の脆弱性を狙った不正アクセスが有名（RAdmin は複数のコンピュータを遠隔操作するためのアプリケーション）。

■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