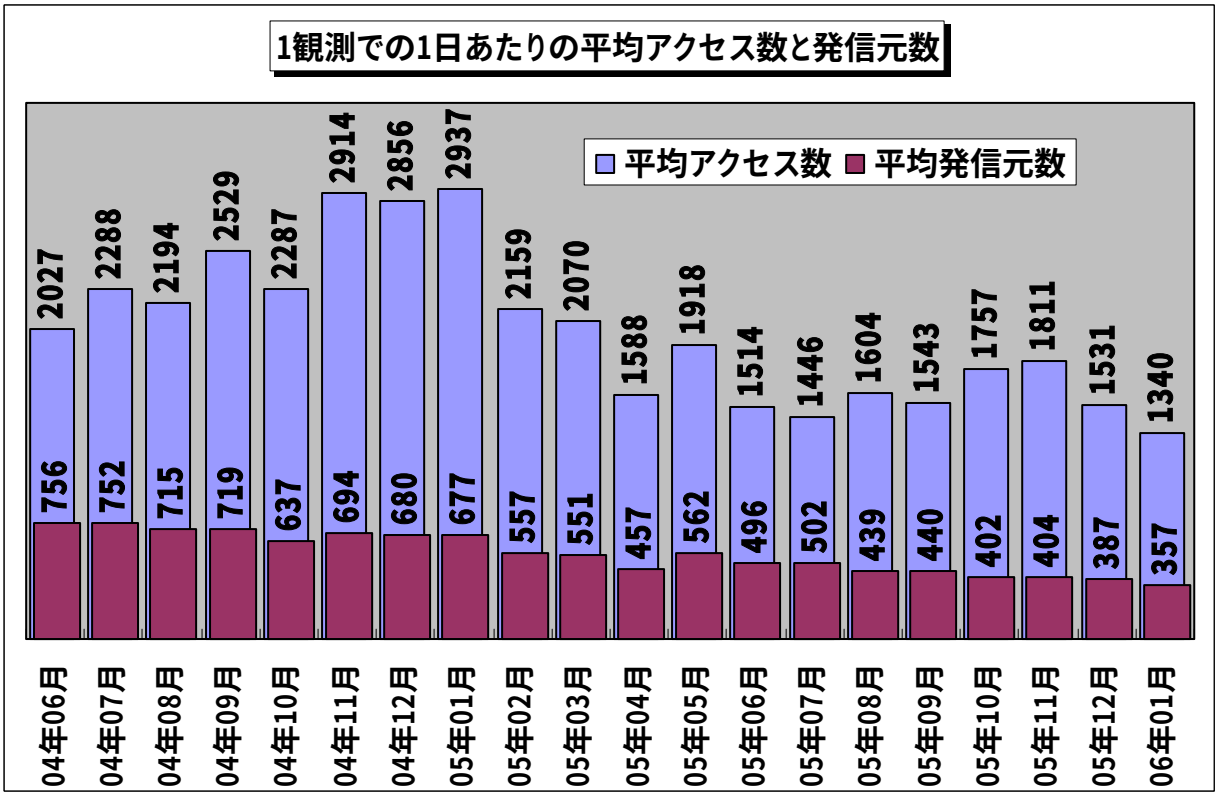
別紙 3

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、2006 年 1 月の期待しない（一方的な）アクセスの総数は、10 観測点で **415,438 件**ありました。1 観測点で 1 日あたり **357** の発信元から **1,340 件**のアクセスがあったことになります。

TALOT2 での1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。言い換えれば、**あなたのコンピュータは、毎日、平均して、357 人の見知らぬ人(発信元)から、発信元一人当たり 4 件の不正と思われるアクセスを受けている**と言うことになります。



【図 1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2004 年 6 月～2006 年 1 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1 に示しています。この図を見ると、期待しない（一方的な）アクセスは、発信元数も含めて、緩やかに減少傾向にあるようです。さらに、アクセス内容についても定常化(後述の統計情報を参照下さい)していると言えます。

2．1月のアクセス状況

あいかわらず、Windows の脆弱性を狙っていると思われる不正なアクセスが多いようです。これらのアクセスの多くは、ボットに感染したコンピュータから送信されていると思われます。

特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。

システムの管理者は、サーバに脆弱性がないか確認し、常に最新の状態に保つことを心掛けて下さい。

一般のコンピュータ利用者は、これらの不正なアクセスによる感染を予防するために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフトやパーソナルファイアウォール等の有効利用をお勧めします。

また、10 月に発生した Windows Messenger サービスを悪用したポップアップスパムメッセージの 102x(UDP)/103x(UDP)ポートへのアクセスも、10 月や 11 月に比べると減少したものの、あいかわらず継続しています。

最近は、ウイルス対策や不正アクセス対策を勧めるポップアップメッセージやネットサーフィン時のアドウェアによるポップアップ広告等も多いので、これらの内容に騙されないように注意して下さい。

102x(UDP)や 103x(UDP)ポートへのアクセスの対策としては、管理された LAN(企業内 LAN 等)以外では、**Windows Messenger サービスを止めること**をお勧めします。

さらに、ウイルス対策や不正アクセス対策に利用する各種の対策ソフト(最近では、ウイルス対策ソフトだけでなくパーソナルファイアウォール機能や個人情報流出を防止する機能などを組み合わせた製品が増えているようです)については、信頼のおけるベンダーのものを利用することをお勧めします。

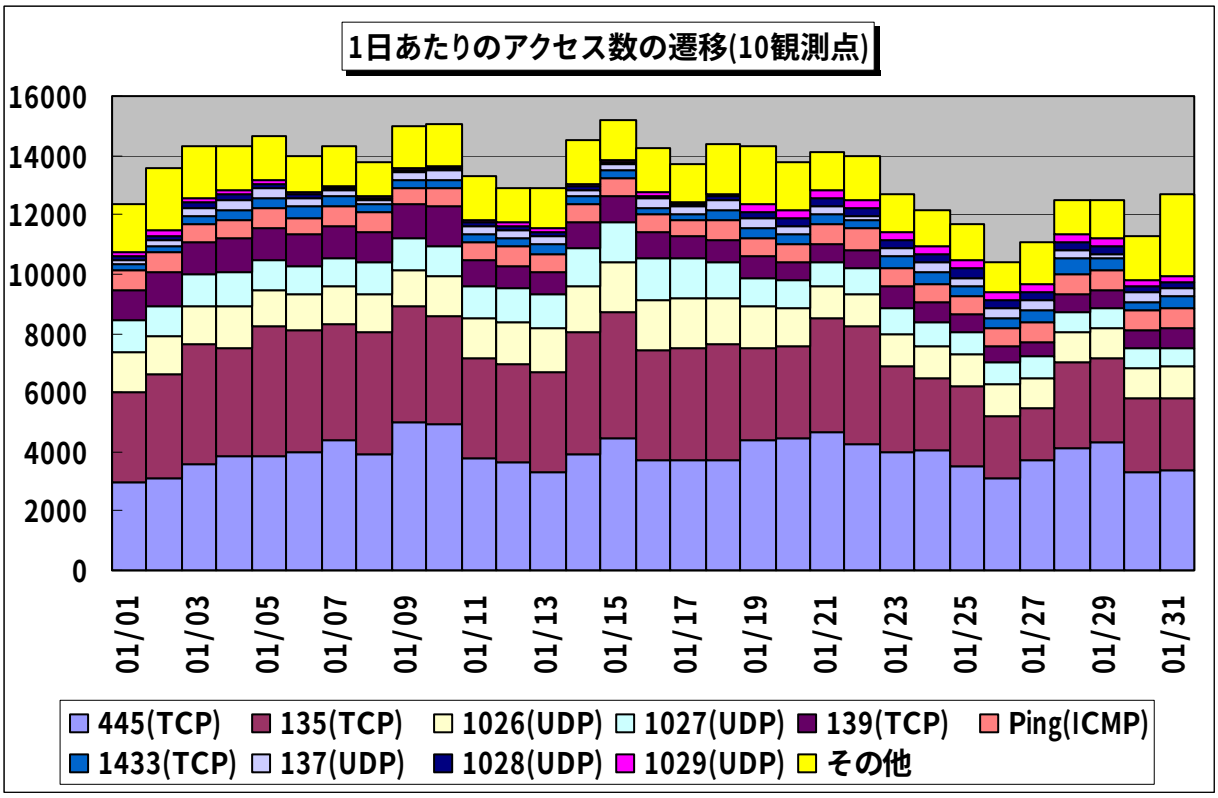
参考情報 (IPA 対策のしおりシリーズ)

(1) ウイルス対策のしおり
(2) スパイウェア対策のしおり
(3) ボット対策のしおり

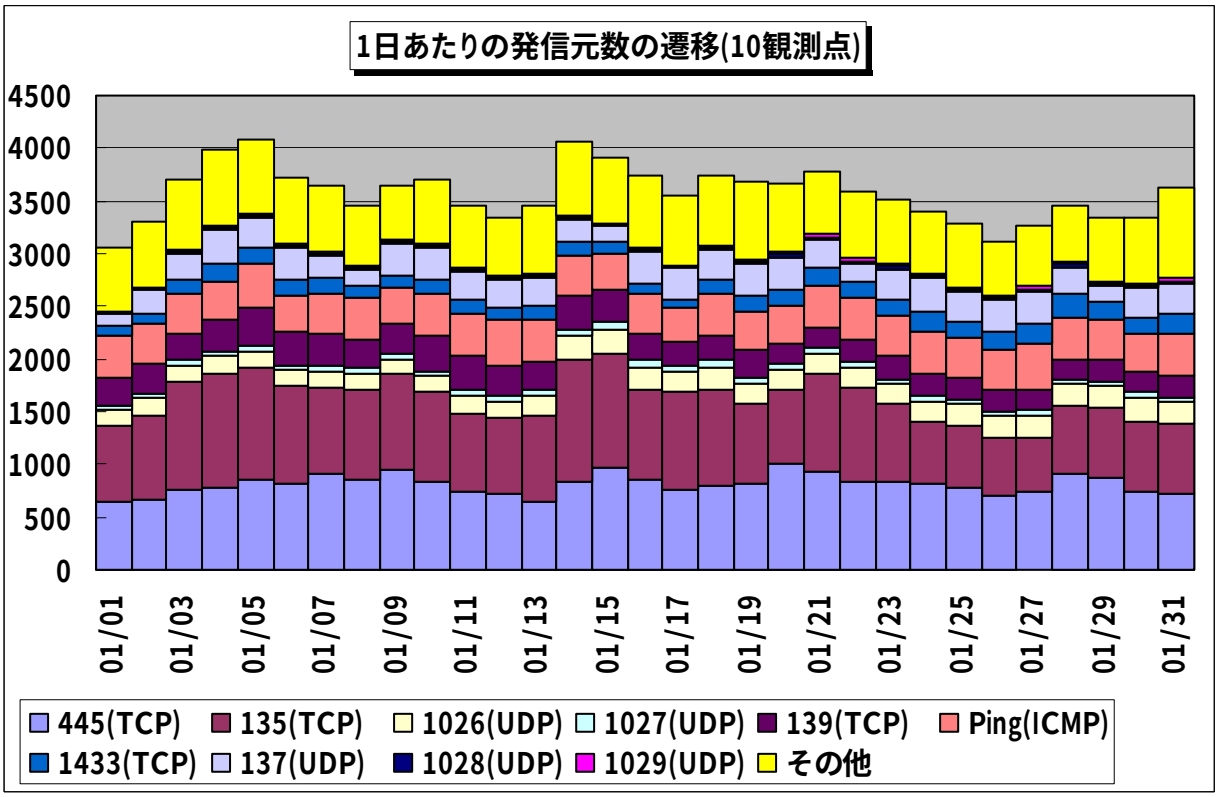
http://www.ipa.go.jp/security/antivirus/shiori.html

2.1 2006 年 1 月の一方的なアクセス状況

2006 年 1 月の一方的なアクセス状況（アクセス数）の遷移を図 2.1.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.1.2 に示します。



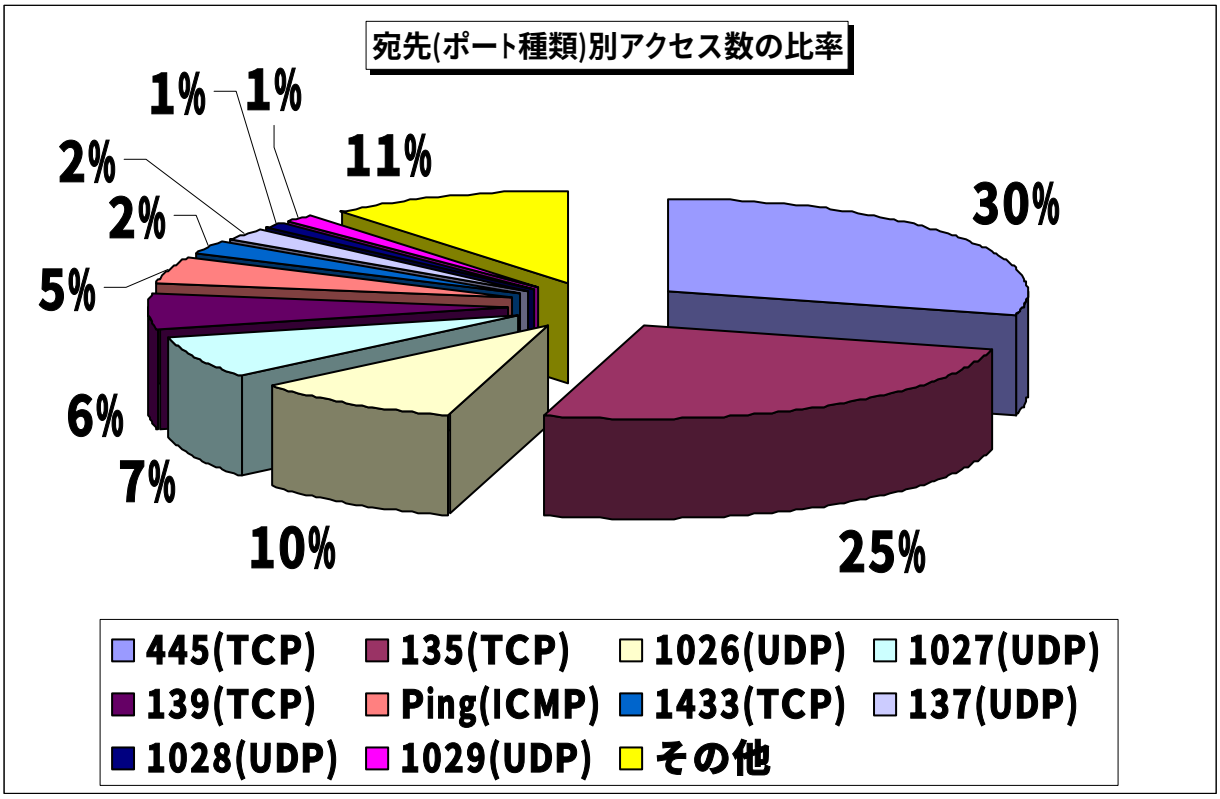
【図 2.1.1 2006 年 1 月の一方的なアクセス状況(アクセス数)】



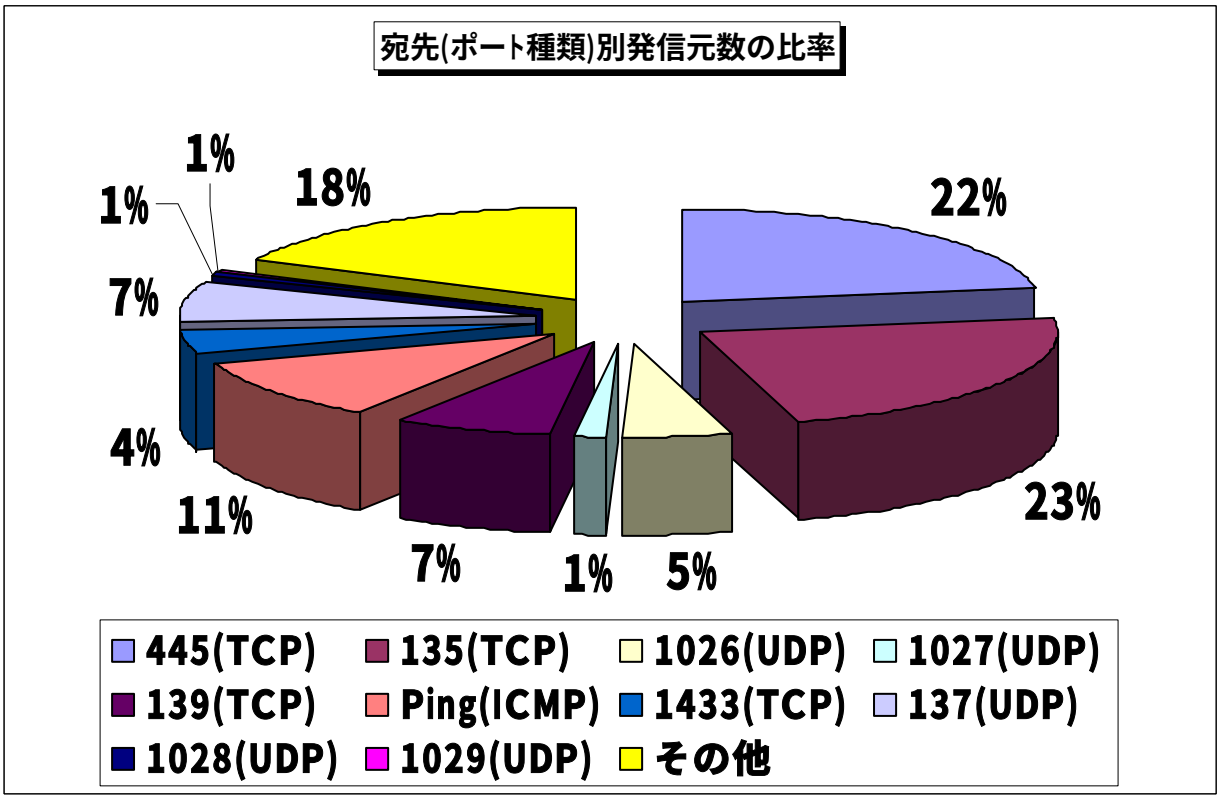
【図 2.1.2 2006 年 1 月の一方的なアクセス状況(発信元数)】

2.2 2006 年 1 月の宛先(ポート種類)別の比率

2006 年 1 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 2.2.1 に、宛先(ポート種類)別発信元数の比率を図 2.2.2 に示します。



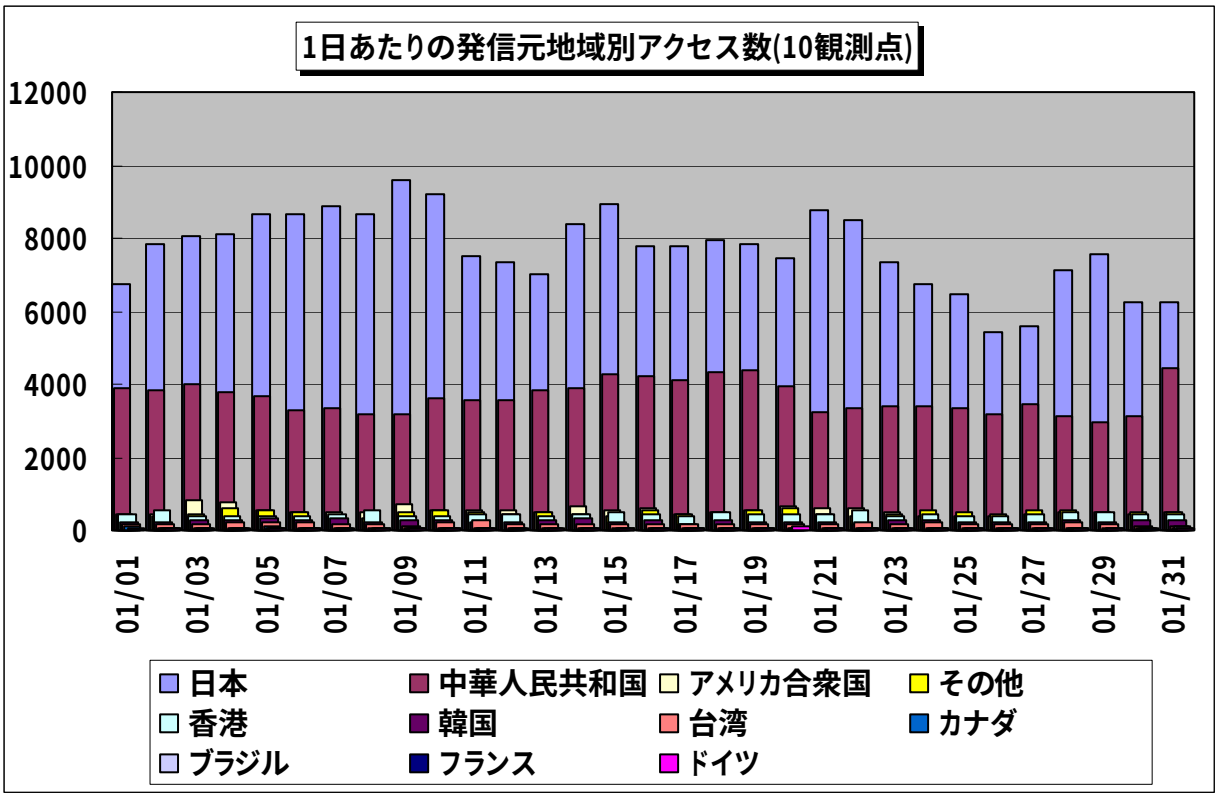
【図 2.2.1 2006 年 1 月の宛先(ポート種類)別アクセス数の比率】



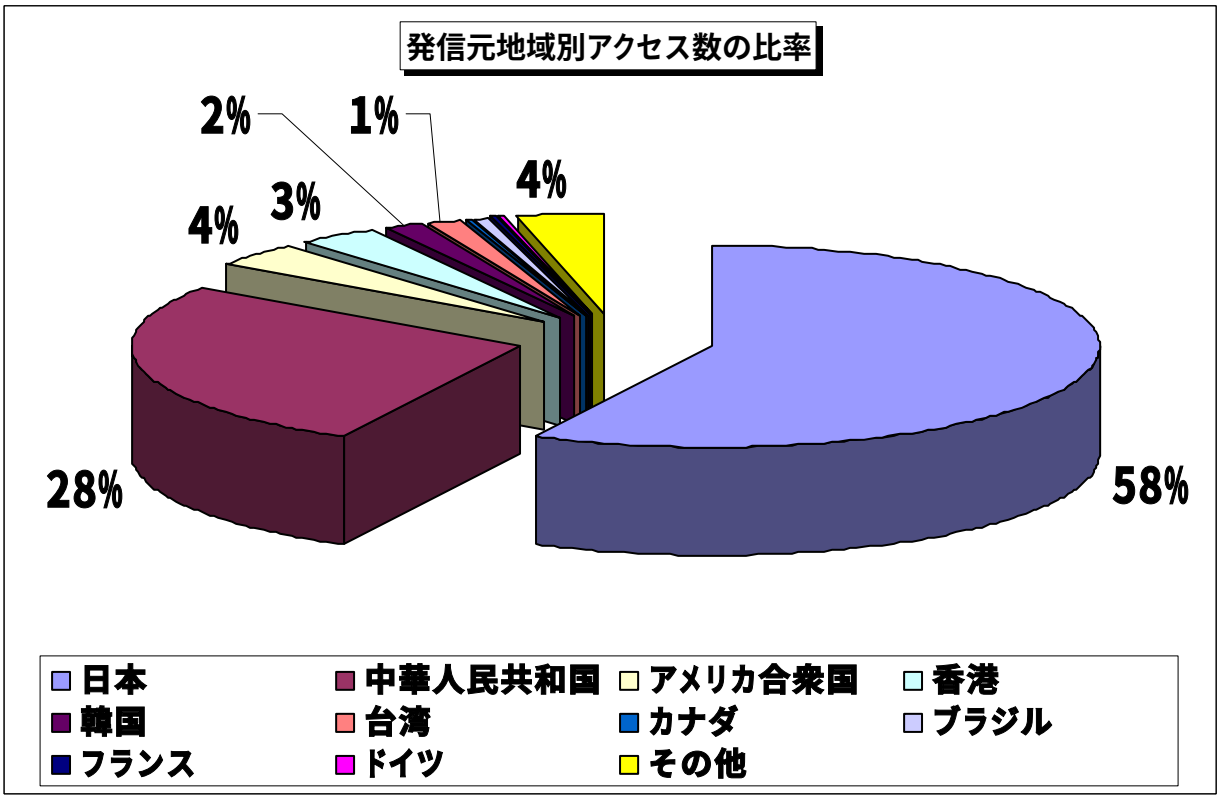
【図 2.2.2 2006 年 1 月の宛先(ポート種類)別発信元数の比率】

2.3 2006 年 1 月の発信元地域別アクセス状況

2006 年 1 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 2.3.1 に、発信元地域別アクセス数の比率を図 2.3.2 に示します。

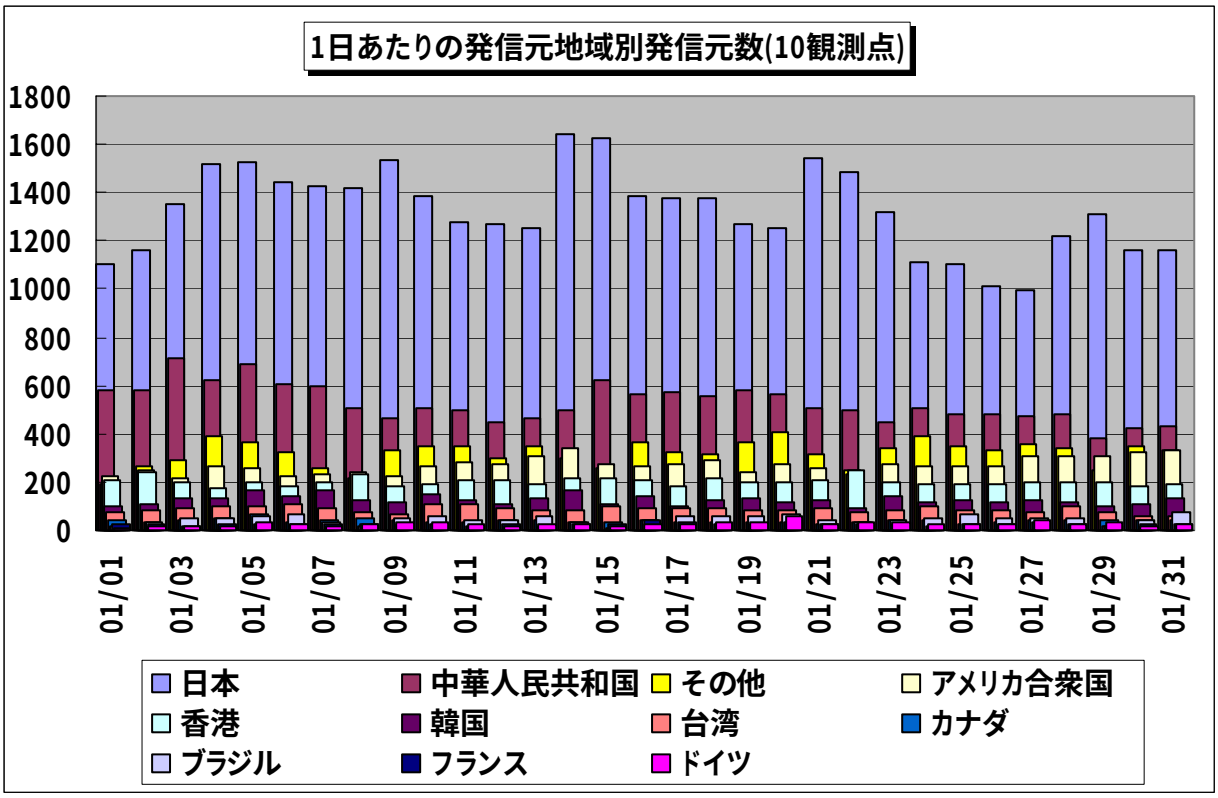


【図 2.3.1 2006 年 1 月の発信元地域別アクセス数の変化】

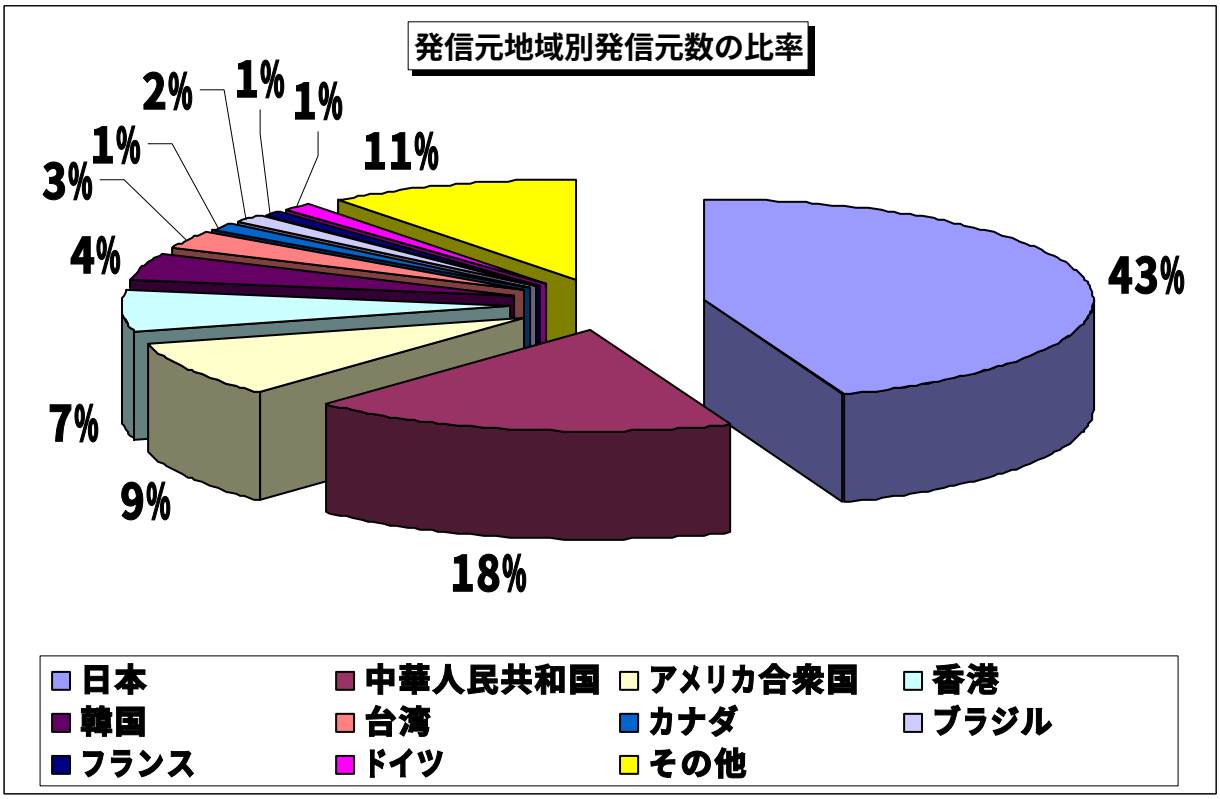


【図 2.3.2 2006 年 1 月の発信元地域別アクセス数の比率】

2006 年 1 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 2.3.3 に、発信元地域別発信元数の比率を図 2.3.4 に示します。



【図 2.3.3 2006 年 1 月の発信元地域別発信元数の変化】

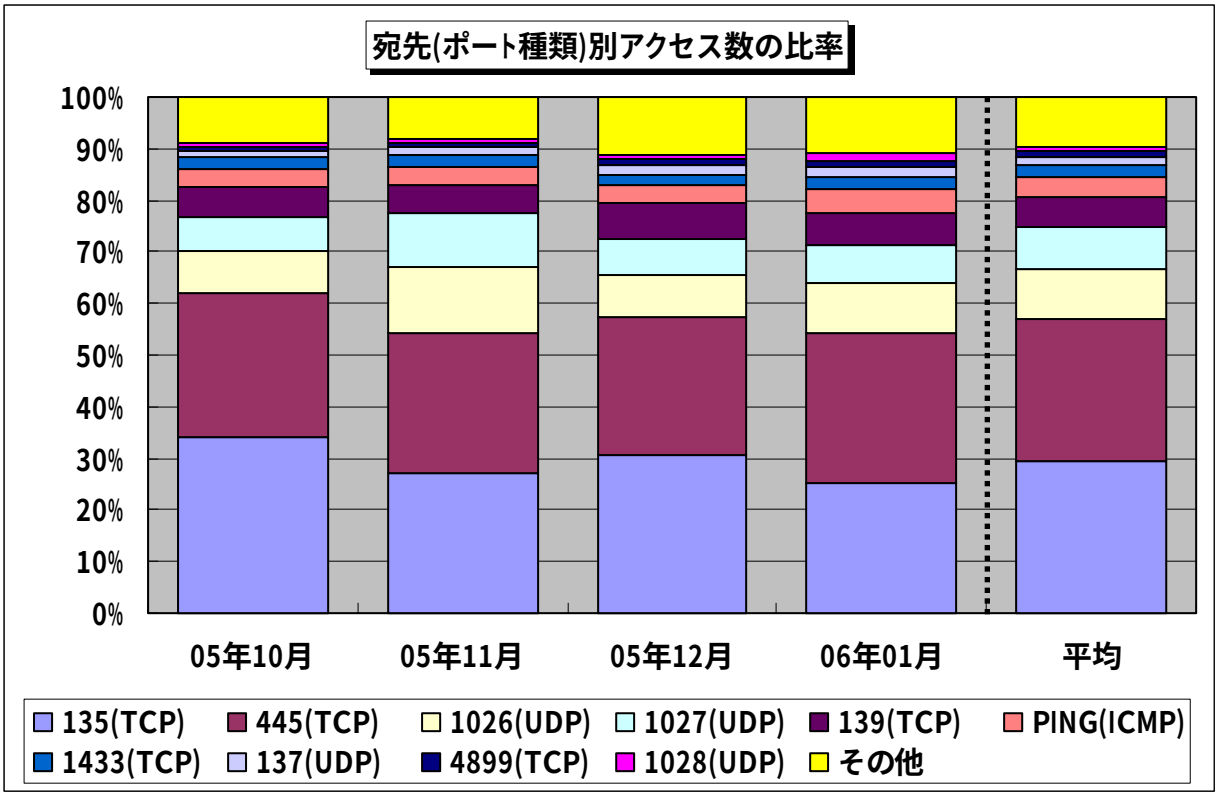


【図 2.3.4 2006 年 1 月の発信元地域別発信元数の比率】

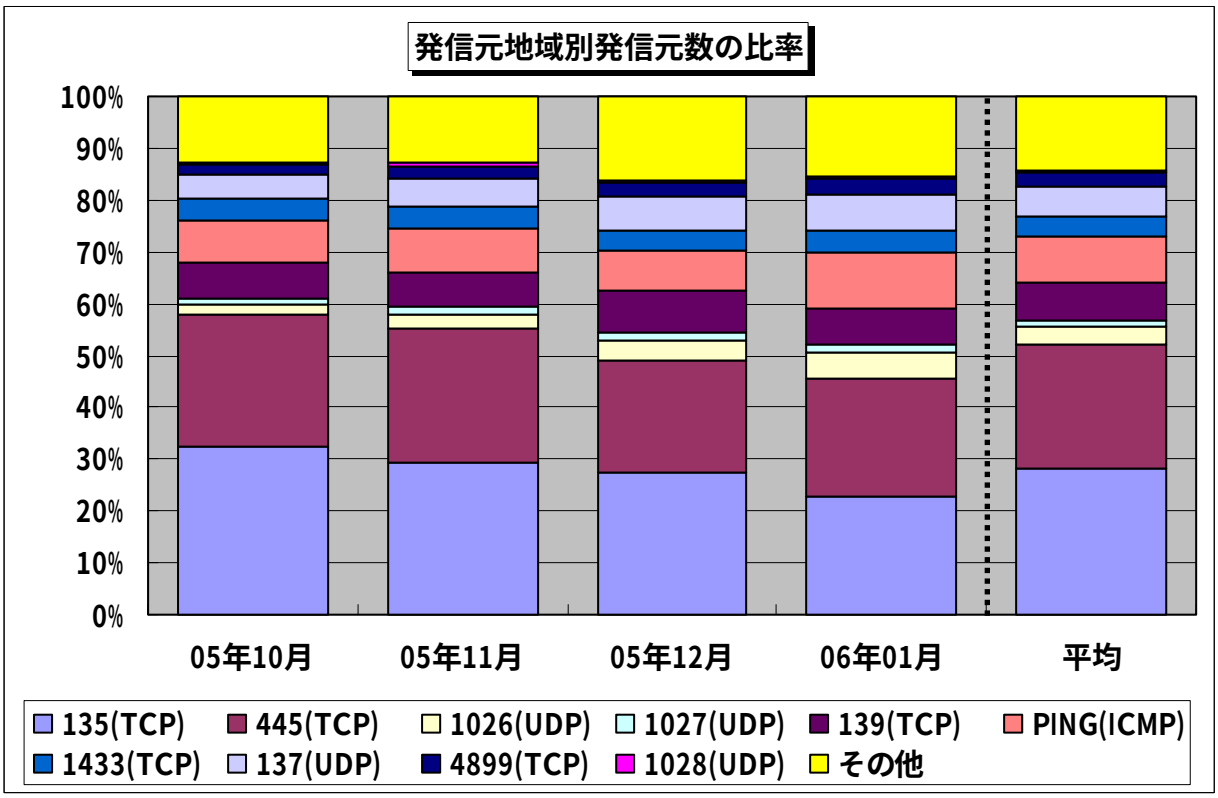
3．統計情報

3.1 2005 年 10 月～2006 年 1 月の宛先(ポート種類)別の比率

2005 年 10 月～2006 年 1 月の宛先(ポート種類)別アクセス数の比率を図 3.1.1 に、宛先(ポート種類)別発信元数の比率を図 3.1.2 に示します。



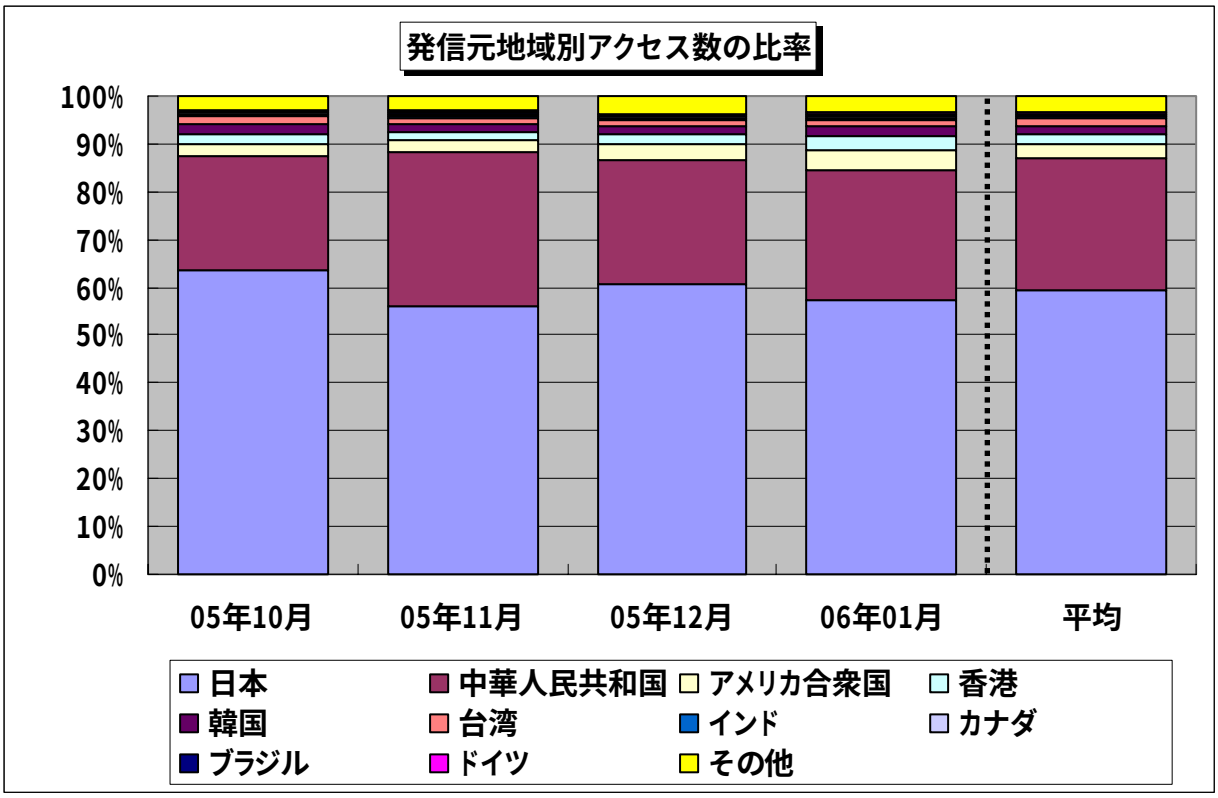
【図 3.1.1 2005 年 10 月～2006 年 1 月の宛先(ポート種類)別アクセス数の比率】



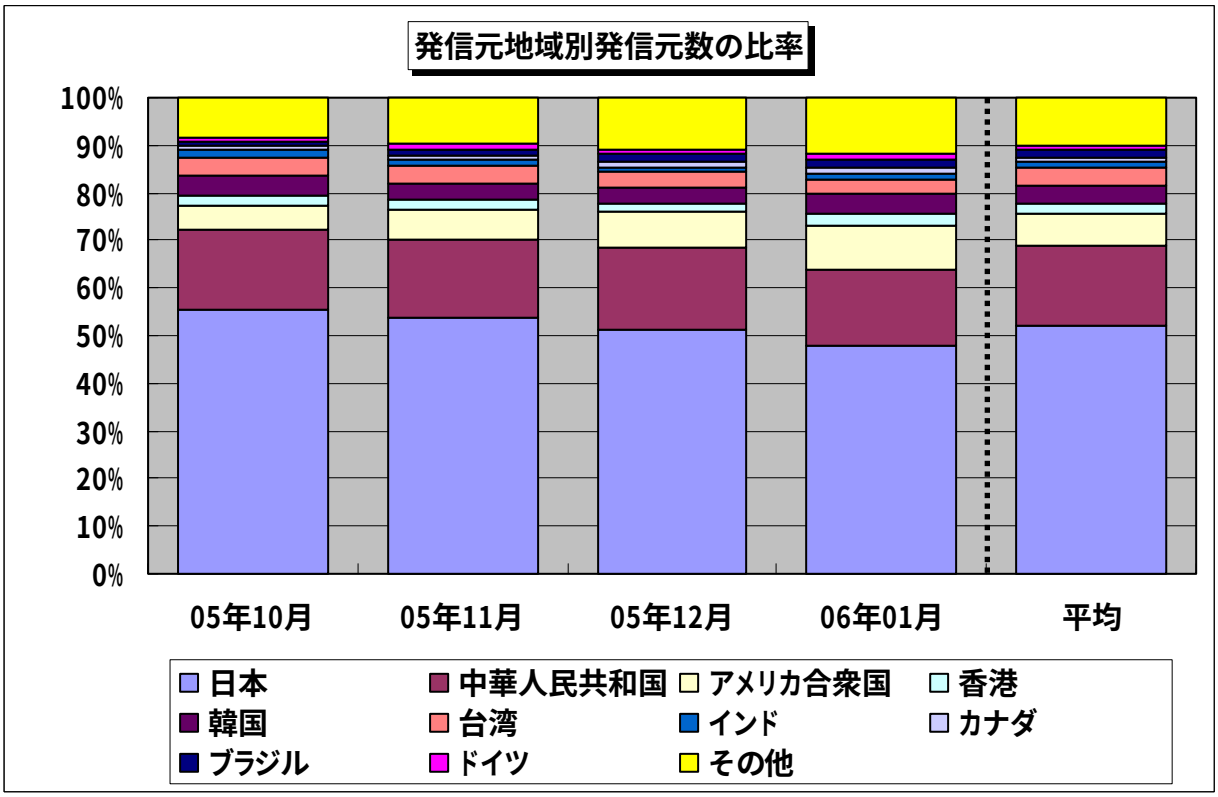
【図 3.1.2 2005 年 10 月～2006 年 1 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 10 月～2006 年 1 月の発信元地域別の比率

2005 年 10 月～2006 年 1 月の発信元地域別アクセス数の比率を図 3.2.1 に、発信元地域別発信元数の比率を図 3.2.2 に示します。



【図 3.2.1 2005 年 10 月～2006 年 1 月の発信元地域別アクセス数の比率】

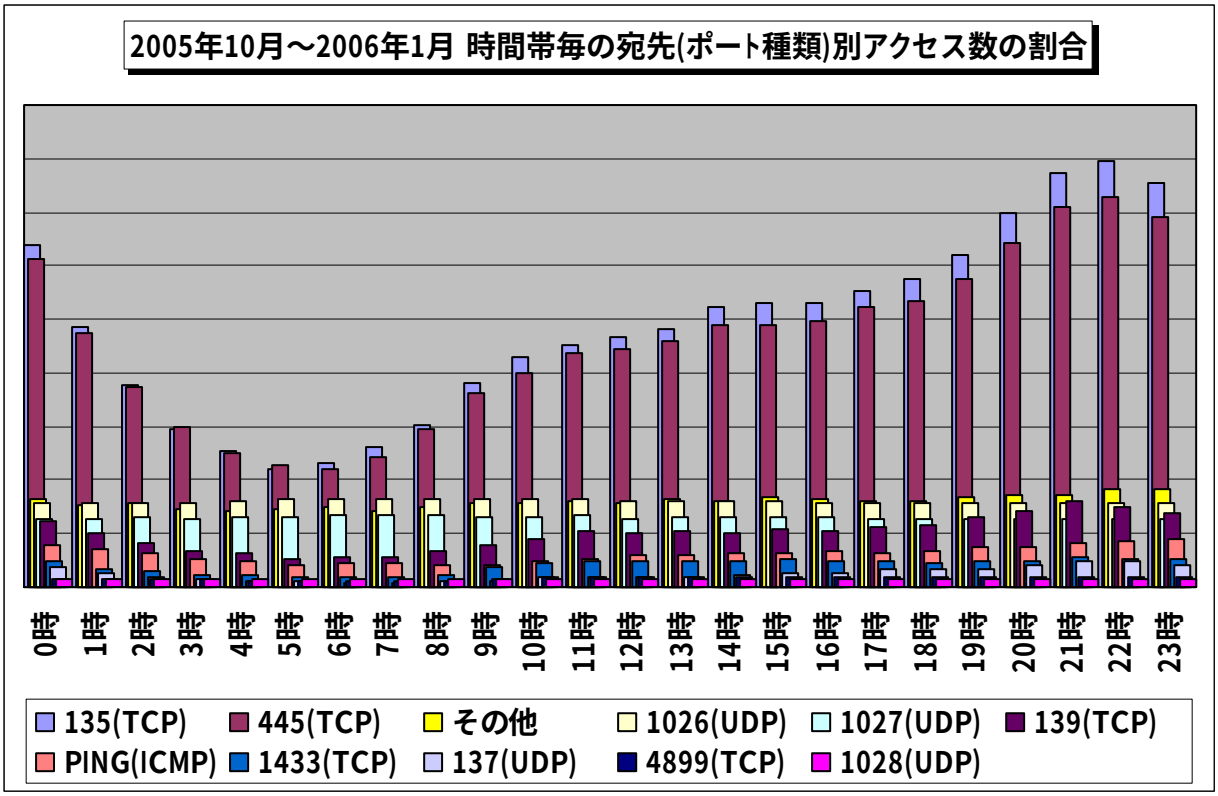


【図 3.2.2 2005 年 10 月～2006 年 1 月の発信元地域別発信元数の比率】

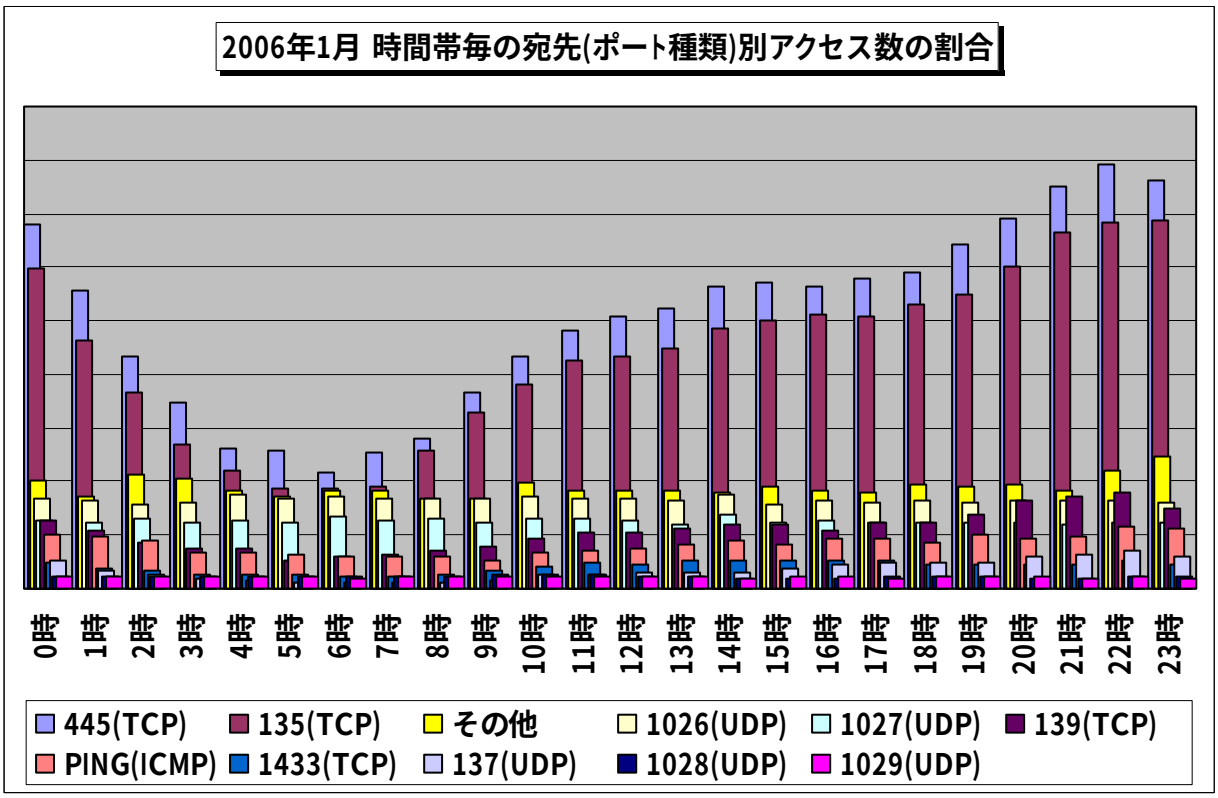
4．その他の統計情報

4.1 2005 年 10 月～2006 年 1 月の時間帯統計

2005 年 10 月～2006 年 1 月の宛先(ポート種類)別アクセス数の時間帯統計を図 4.1.1 に、2006 年 1 月の宛先(ポート種類)別アクセス数の時間帯統計を図 4.1.2 に示します。



【図 4.1.1 2005 年 10 月～2006 年 1 月の宛先(ポート種類)別アクセス数の時間帯統計】



【図 4.1.2 2006 年 1 月の宛先(ポート種類)別アクセス数の時間帯統計】

5．補足説明

以下に、2006 年 1 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)	保護のあまいファイル（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)
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)
1026(UDP)/1027(UDP)	Microsoft Windows Messenger service（MSN Messenger とは別物）を利用したポップアップ(スパム)メッセージの送信で有名
139(TCP)	保護のあまいファイル(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
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
137(UDP)	NETBIOS のポートであり、NETBIOS 経由でのコンピュータへの接続(侵入)などの目的で使用されます
1028(UDP)	1026(UDP)/1027(UDP)と同じアクセス
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
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加賀谷／内山
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp