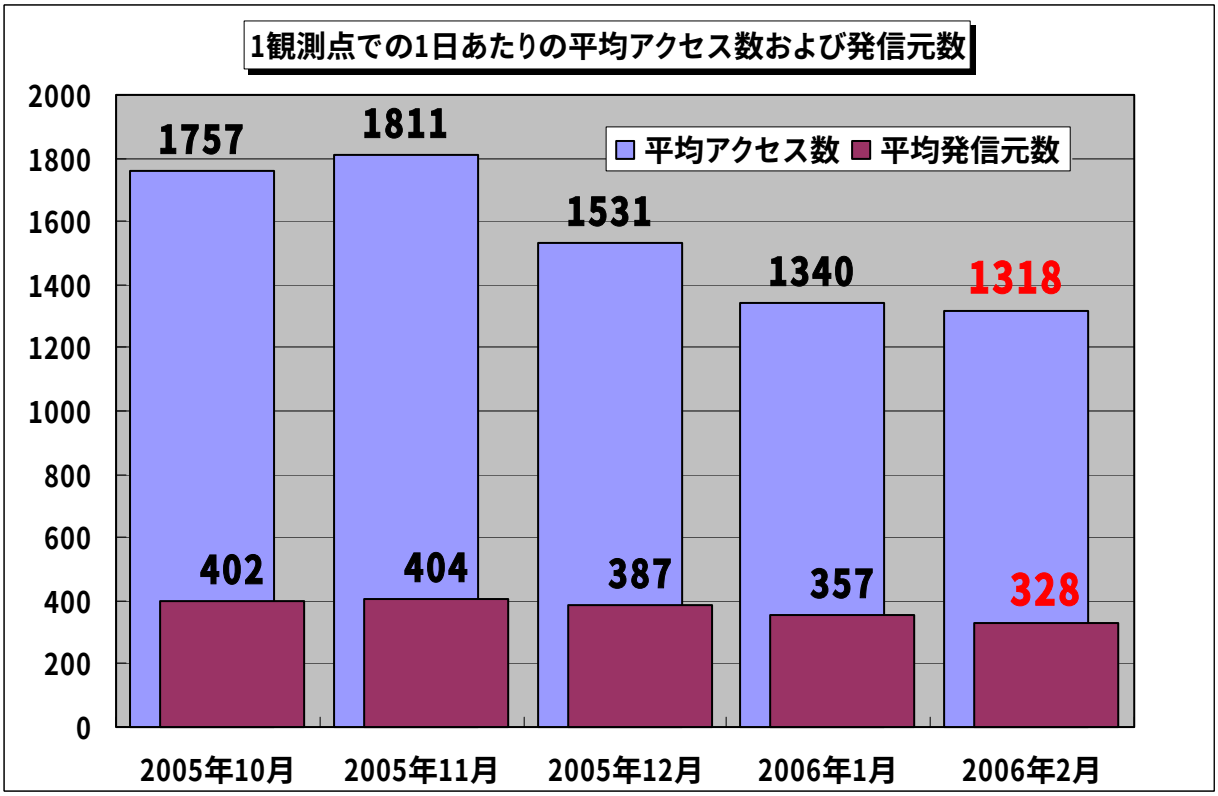
別紙 3

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 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 **316,533 件**ありました。1 観測点で 1 日あたり **328** の発信元から **1,318 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、328 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】

2005 年 10 月～2006 年 2 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。

2006 年 2 月 3 日 18 時 30 分から 2 月 6 日 13 時 30 分の間、TALOT2 のシステムメンテナンスを実行したため、観測が行われていません。今回の報告においては、2 月 3 日から 6 日までの 4 日分の観測データを除外して統計情報等を作成してあります。ご注意下さい。

2．2月のアクセス状況

2月のアクセス状況は、1月とほぼ同じ状況です。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、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。

また、一時的ではありますが、Microsoft SQL Server[注1]の稼動するサーバを狙ったアクセス[1433(TCP)ポートへのアクセス]も増加しました。

さらに、統計情報等には出ていませんが、パスワードクラッキングでのシステムへの侵入を目的とした、MySQL[注2]の稼動するサーバを狙ったものと思われるアクセス[3306(TCP)ポートへのアクセス[注3]]や SSH（Secure Shell：通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール）を狙ったアクセス[22(TCP)ポートへのアクセス[注4]]も見受けられます。

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、さらに利用するアプリケーションのパスワード強化や接続認証の強化を実施して下さい。

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。

注1） Microsoft SQL Server
マイクロソフト社のSQLデータベース

注2） MySQL
オープンソースのＳＱＬデータベース

注3) 3306(TCP)ポートへのアクセス
3306(TCP)ポートは、MySQL(オープンソースＳＱＬデータベース)が使用するデフォルトのポートです。このポートが開いているコンピュータは、MySQLを使用しているとみなし、これらのコンピュータを探す目的で、いわゆるポートスキャンを行っていると思われます。一般的には、安易なパスワード設定の場合、パスワードクラッキングの手口で、コンピュータに侵入される可能性が高いので、注意が必要です。
インターネット(外部)から接続する必要がないならば、ルータやファイアウォールにて、このポートへの通信を遮断することをお勧めします。

注 4) 22(TCP)ポートへのアクセス

ソーシャルエンジニアリング対策として、グラフ等は掲載しませんが、TALOT2 のシステムメンテナンス用に SSH(Secure Shell：:通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール)を利用している観測点には、2006 年 2 月、1 発信元から 1 日当たり 10,000 回以上のアクセス（パスワードクラッキングによるシステムへの侵入が狙いと思われる）をしてくるケースが 9 回(日)もありました。アクセス数最大のケースでは、1 発信元から 1 日当たり 50,000 回以上でした。これらのアクセスは、特定観測点に対するものなので、統計情報にそぐわないため除外してあります。

特記事項)

2006 年 2 月の実際の観測データのうち、特定の観測点に集中して発生したアクセスがあります。この観測データについては、報告の統計情報にそぐわないため、除外してあります。

除外した観測データは、いわゆる P2P ファイル交換ソフトが使用するアクセスでした。

TALOT2 ではインターネットの一般利用者と同様の環境で観測するために、不定期に観測点の IP アドレスを変更します。これらのIPアドレスの、以前の利用者が、P2P ファイル交換ソフトを使用していたようで、これらのIPアドレス宛てに他の利用者から接続要求が、観測点に送られてきたようです。

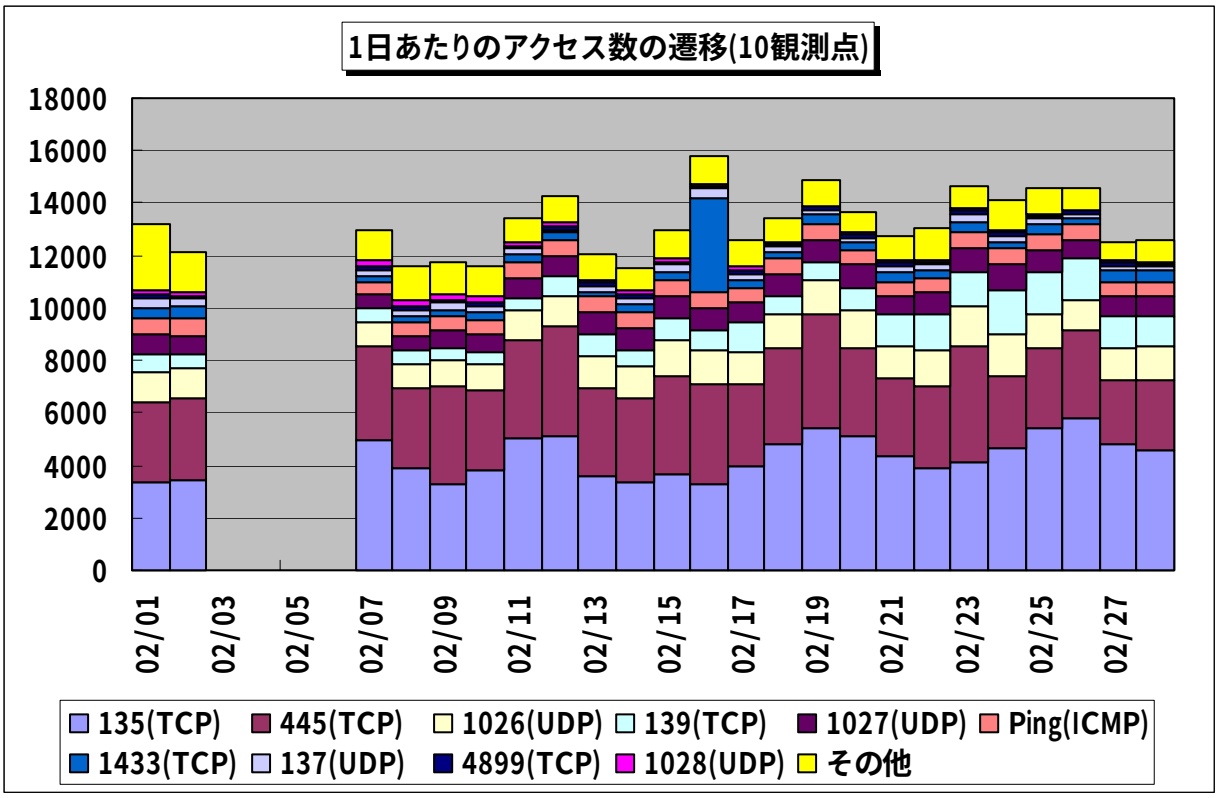
今回 TALOT2 で観測された上述のアクセスのうち特に目立ったものは、1 箇所の発信元から、特定観測点のIPアドレスに対して、30 秒間隔で 3 回ずつのアクセスが繰り返し行われ、そのアクセスが 4 日間も継続したことです。これは、P2P ファイル交換ソフトを自動的に動作させ、アクセスを続けていたものと思われます。

このような状況が発生する可能性は、以前に比べて多くなっているようで、P2P ファイル交換ソフトのものと思われるアクセスが多く見受けられます。P2P ファイル交換ソフトの利用者が増加していることを示しているようです。

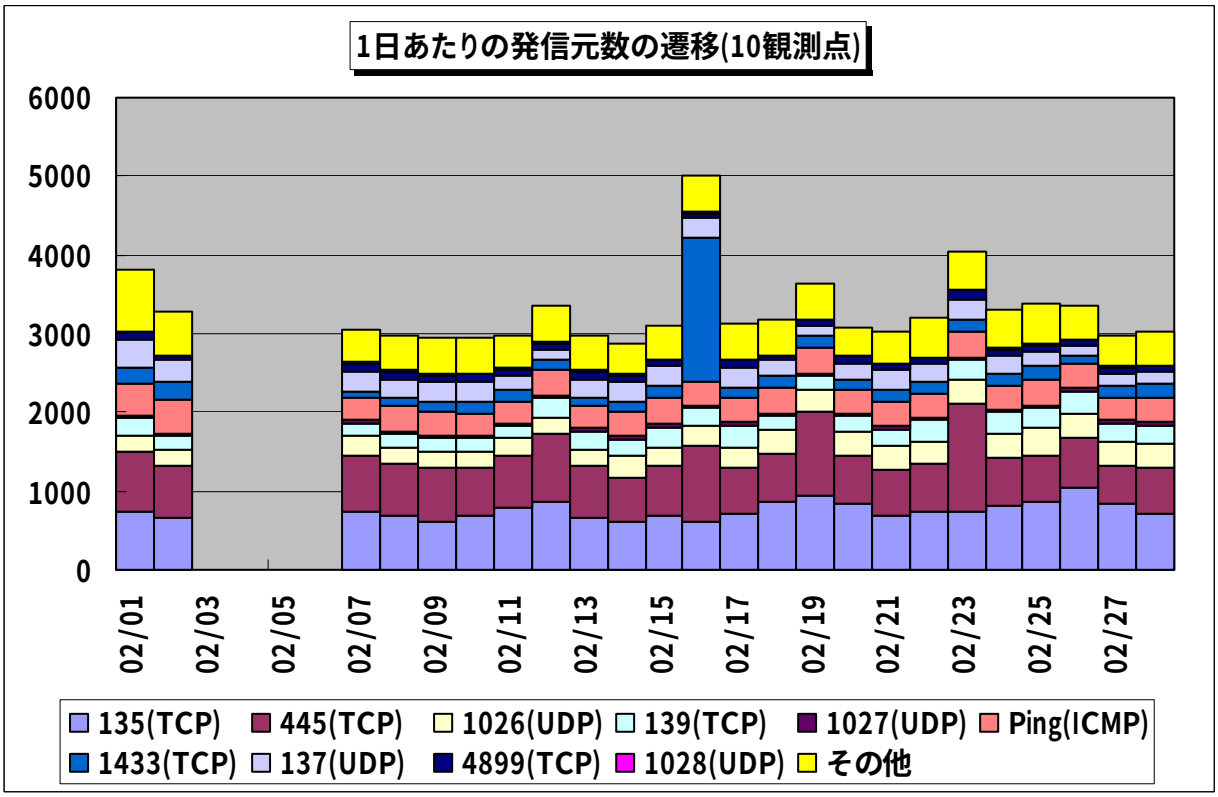
P2P ファイル交換ソフトを利用する方は、このような状況が発生することを認識し、ソフトの利用の際は、通信の相手が正しいことを確認していただきたいと思います。場合によっては、DoS 攻撃とみなされる可能性もあります。十分注意して下さい。

2.1 2006 年 2 月の一方的なアクセス状況

2006 年 2 月の一方的なアクセス状況（アクセス数）の遷移を図 2.1.1 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。



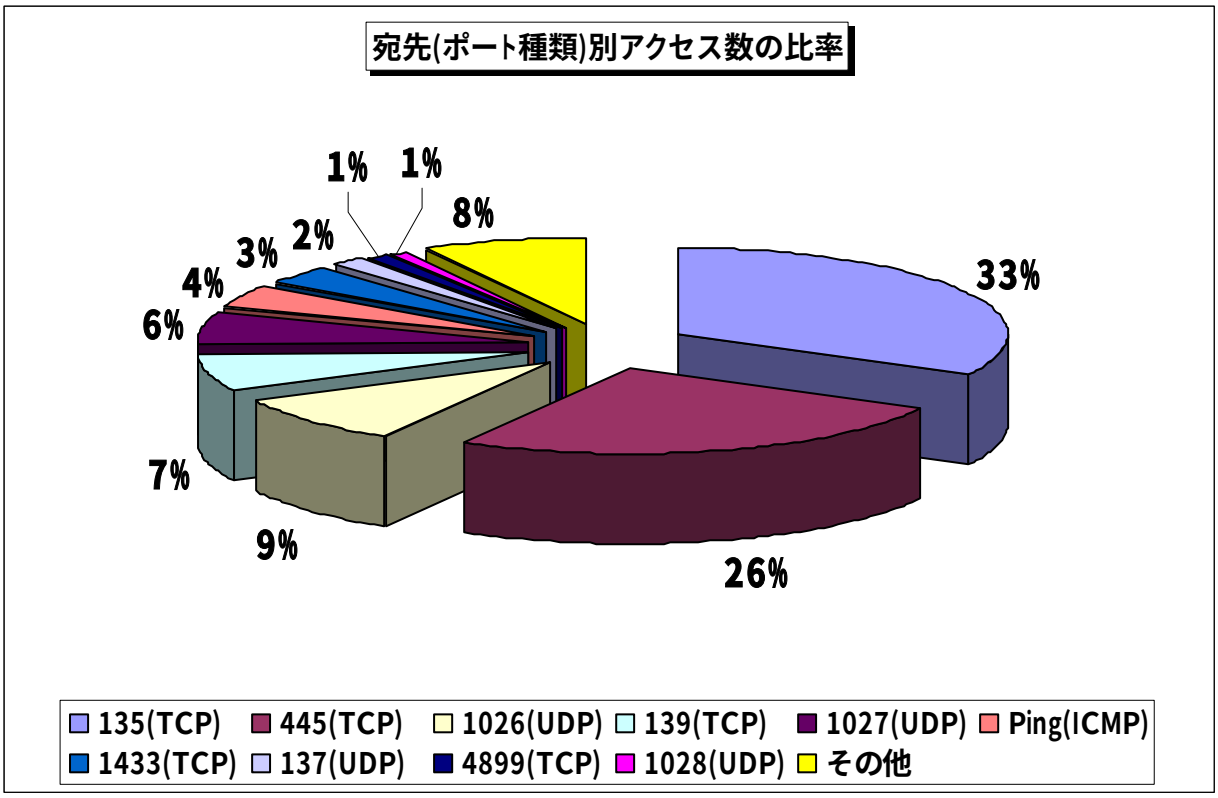
【図 2.1.1 2006 年 2 月の一方的なアクセス状況(アクセス数)】



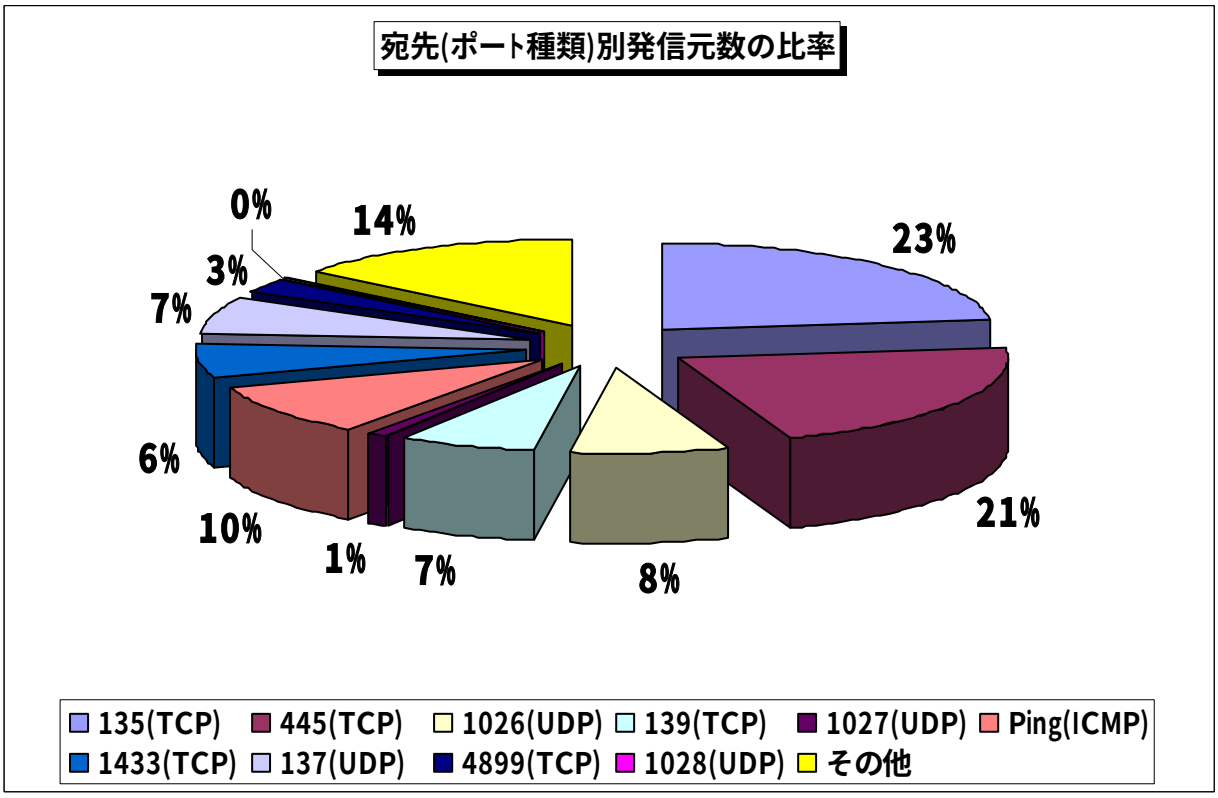
【図 2.1.2 2006 年 2 月の一方的なアクセス状況(発信元数)】

2.2 2006 年 2 月の宛先(ポート種類)別の比率

2006 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 2.2.1 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。



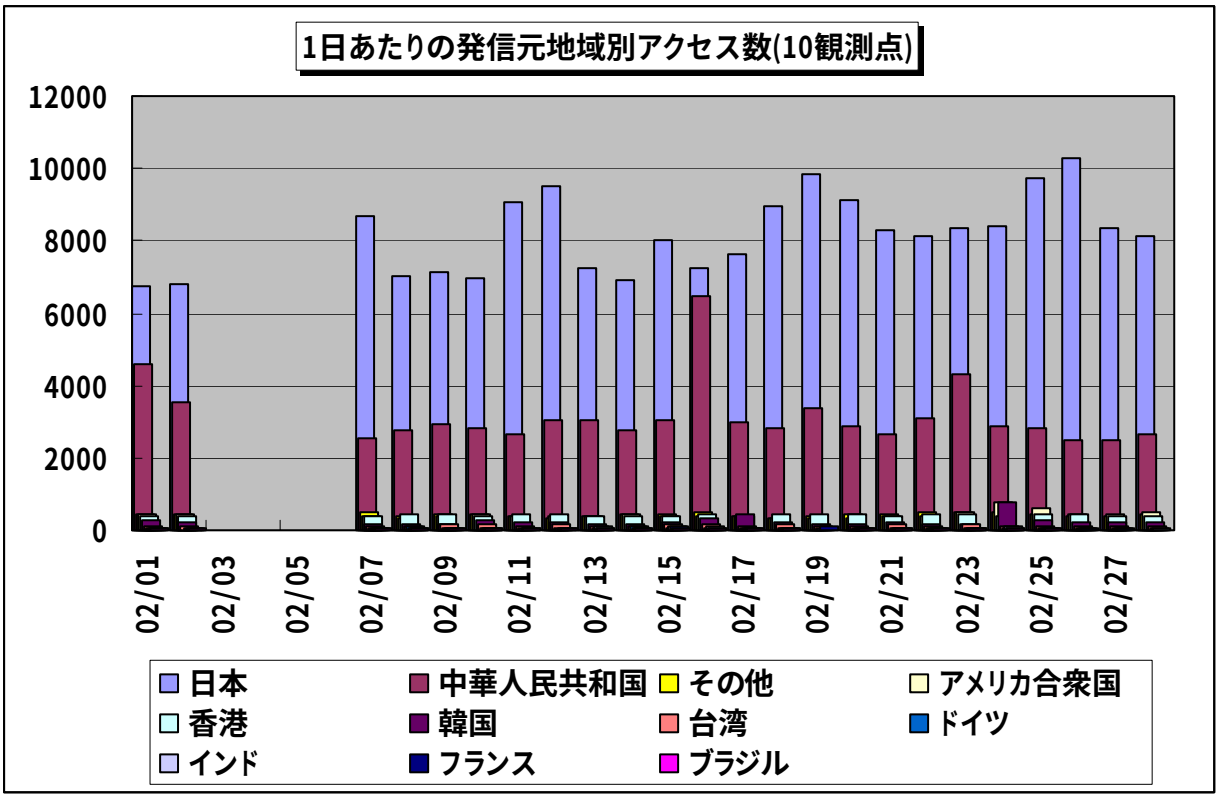
【図 2.2.1 2006 年 2 月の宛先(ポート種類)別アクセス数の比率】



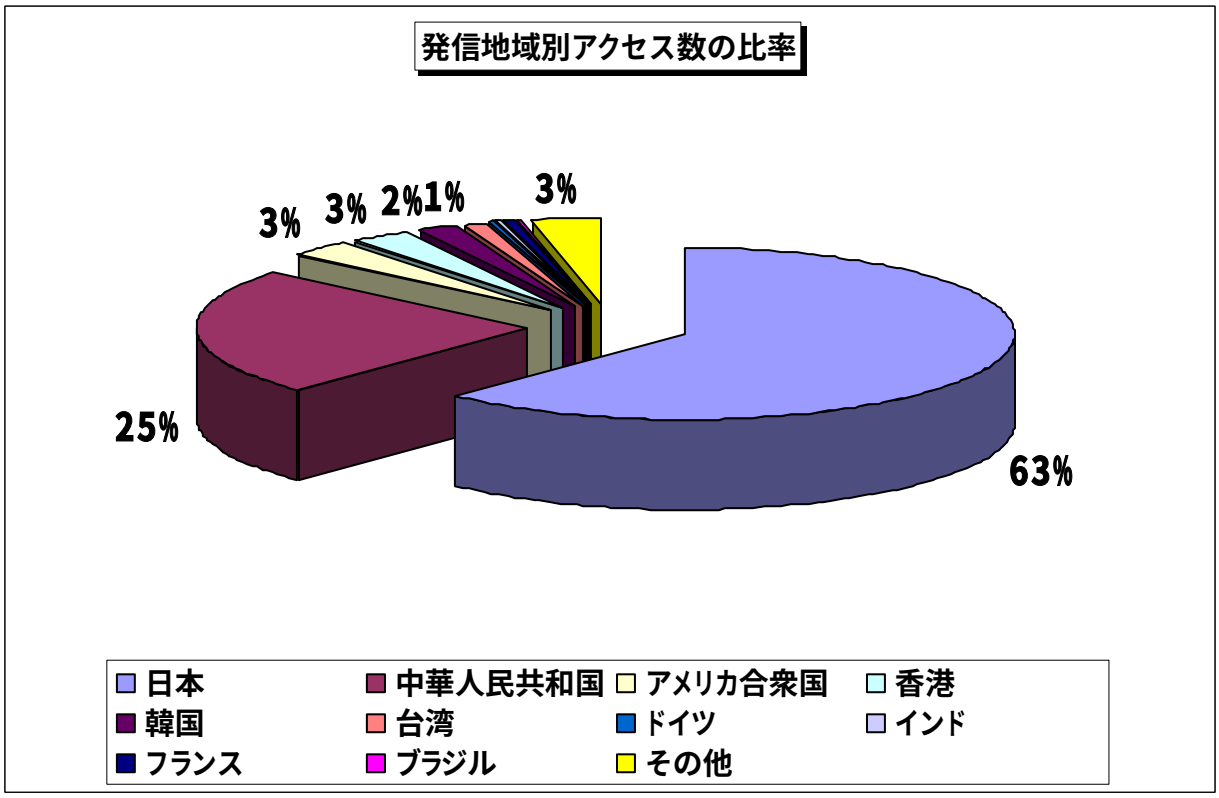
【図 2.2.2 2006 年 2 月の宛先(ポート種類)別発信元数の比率】

2.3 2006 年 2 月の発信元地域別アクセス状況

2006 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 2.3.1 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。

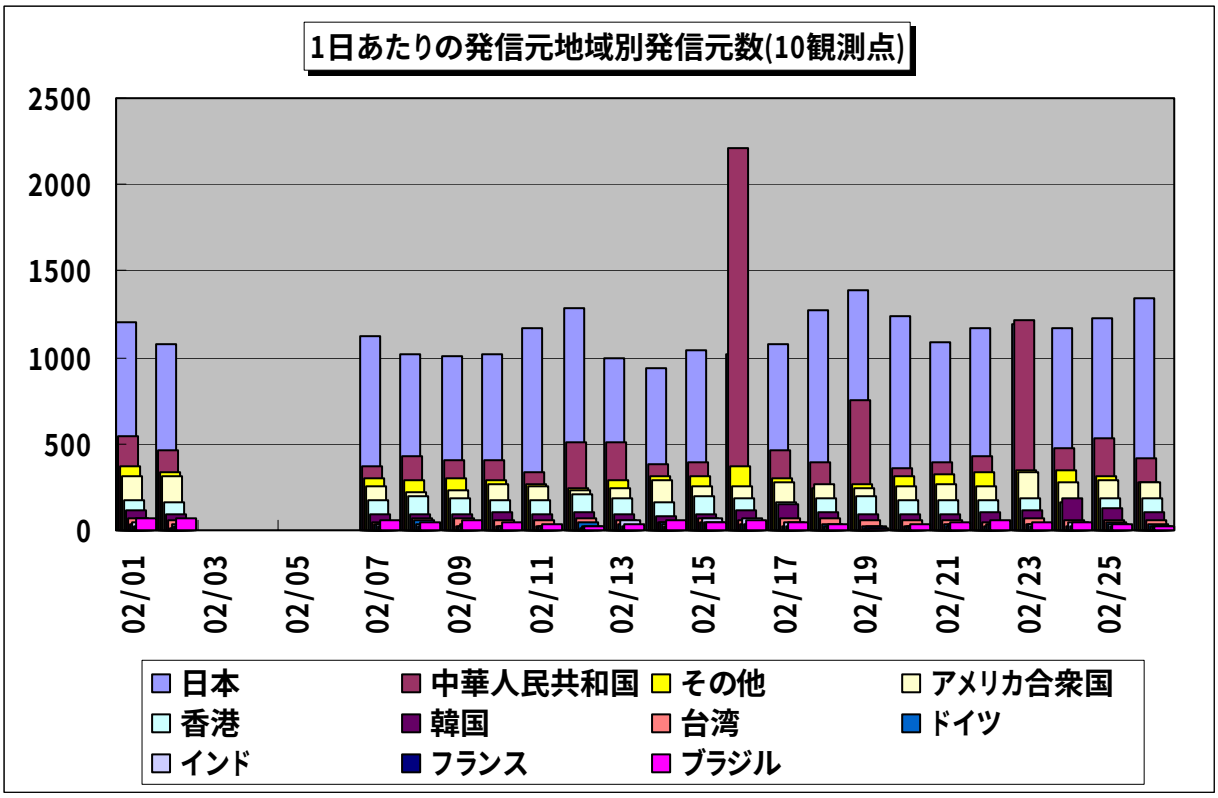


【図 2.3.1 2006 年 2 月の発信元地域別アクセス数の変化】

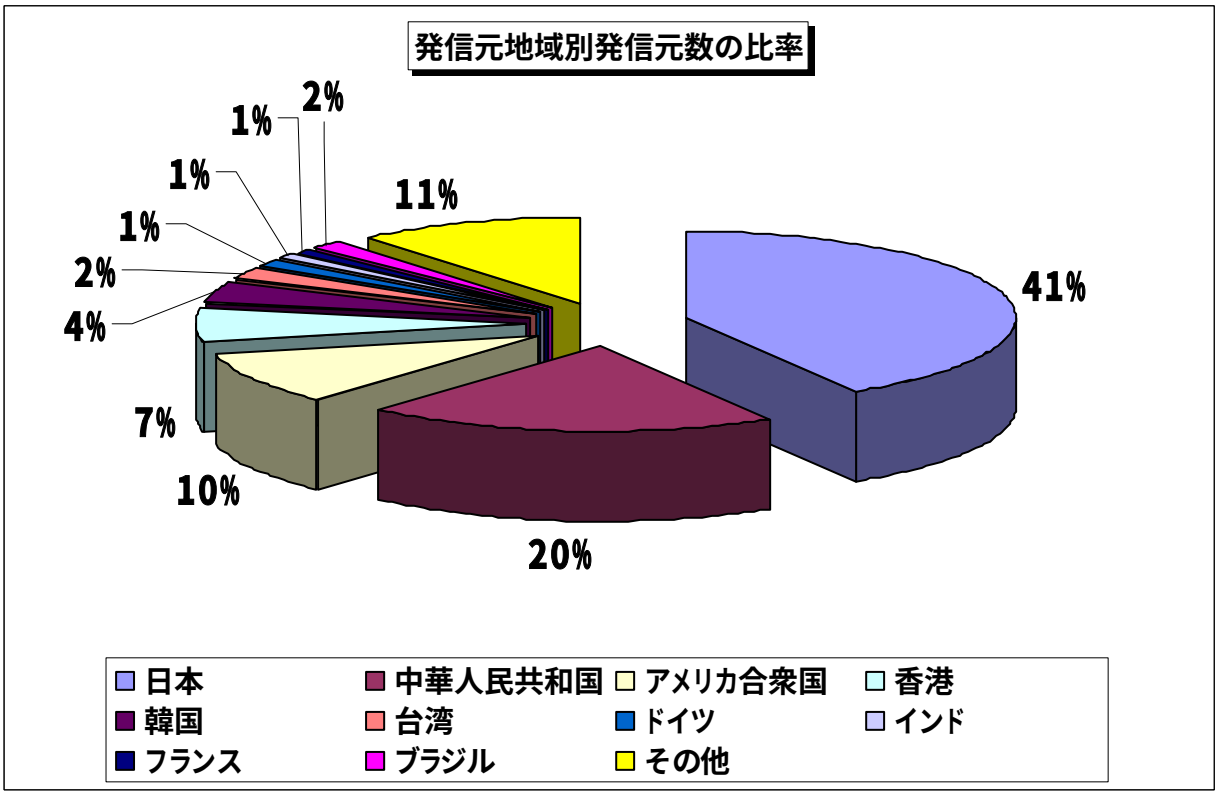


【図 2.3.2 2006 年 2 月の発信元地域別アクセス数の比率】

2006 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 2.3.3 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 2 月の発信元地域別発信元数の変化】

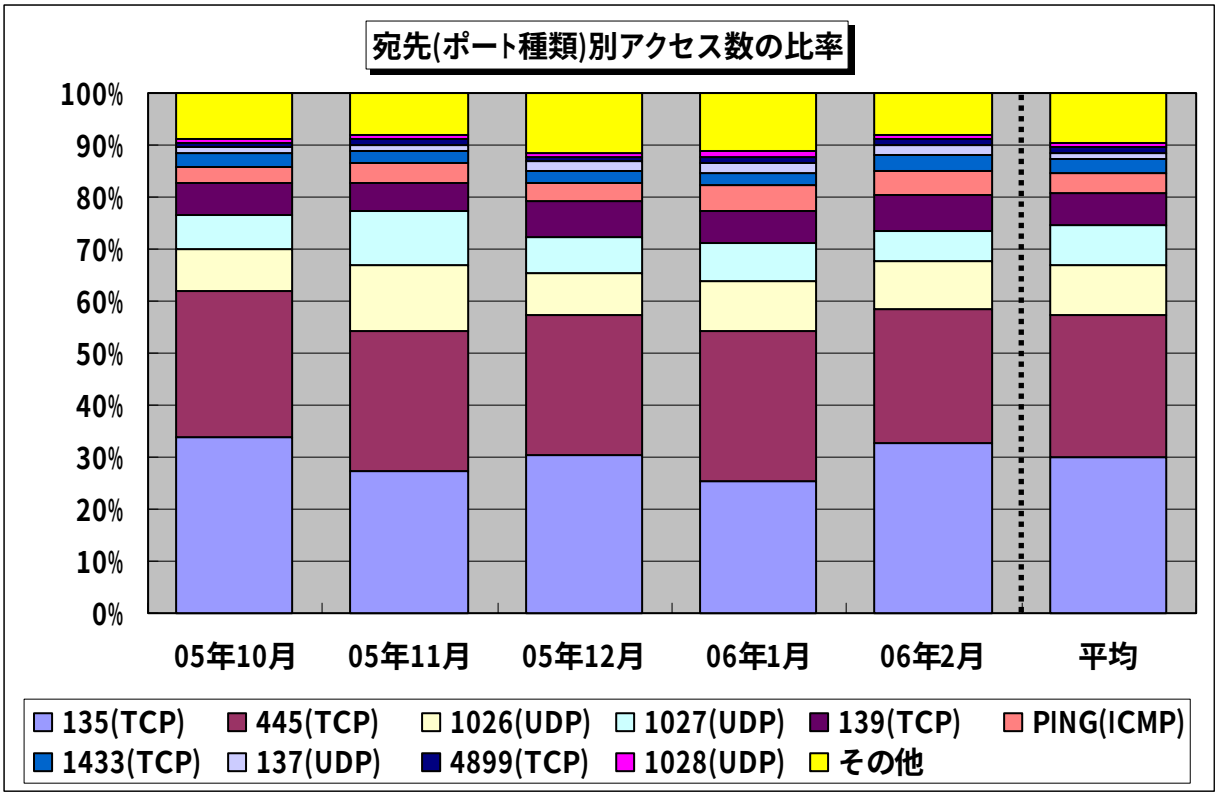


【図 2.3.4 2006 年 2 月の発信元地域別発信元数の比率】

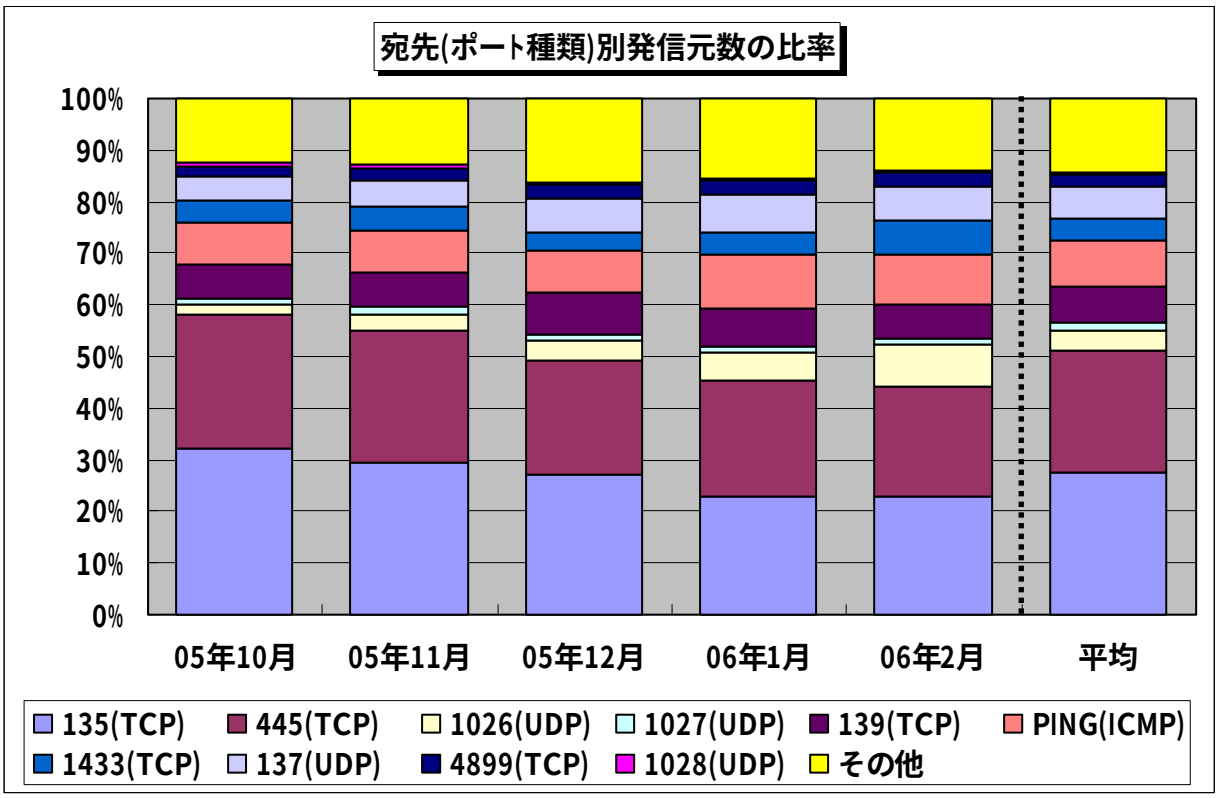
3．統計情報

3.1 2005 年 10 月～2006 年 2 月の宛先(ポート種類)別の比率

2005 年 10 月～2006 年 2 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。



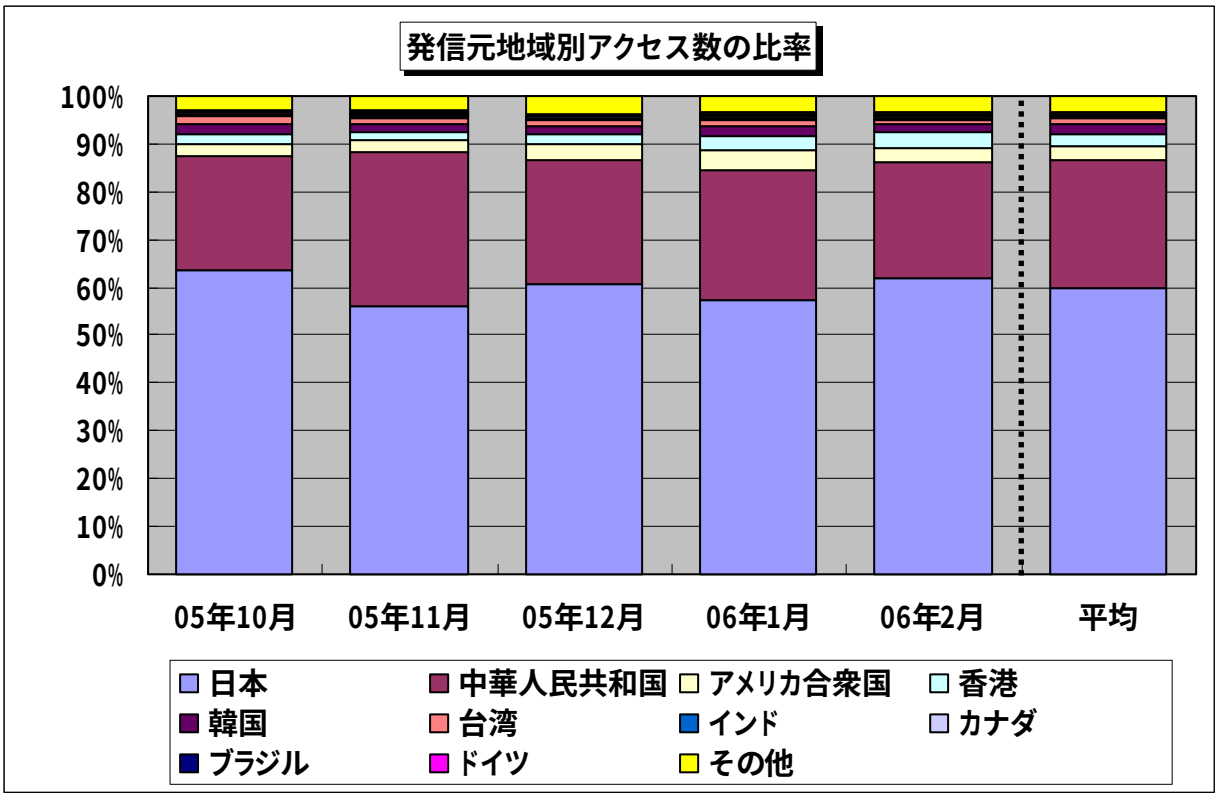
【図 3.1.1 2005 年 10 月～2006 年 2 月の宛先(ポート種類)別アクセス数の比率】



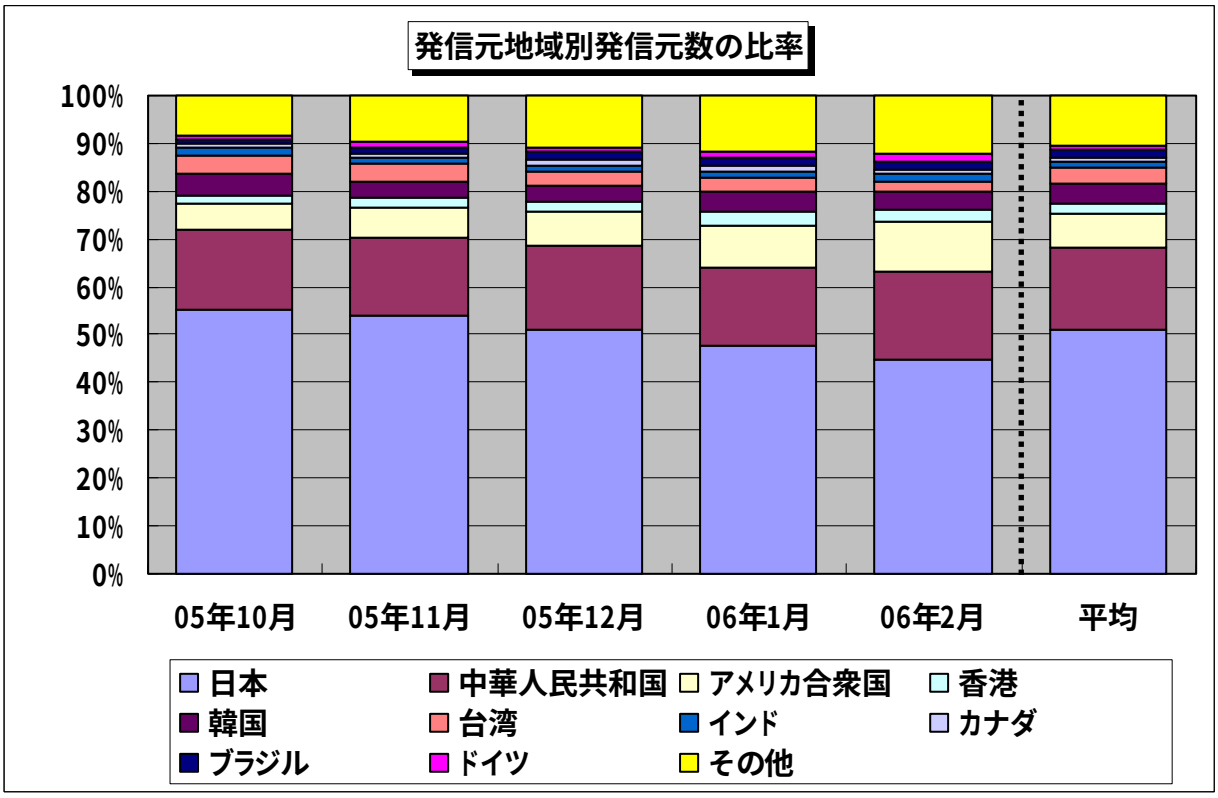
【図 3.1.2 2005 年 10 月～2006 年 2 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 10 月～2006 年 2 月の発信元地域別の比率

2005 年 10 月～2006 年 2 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 2 月の発信元地域別アクセス数の比率】

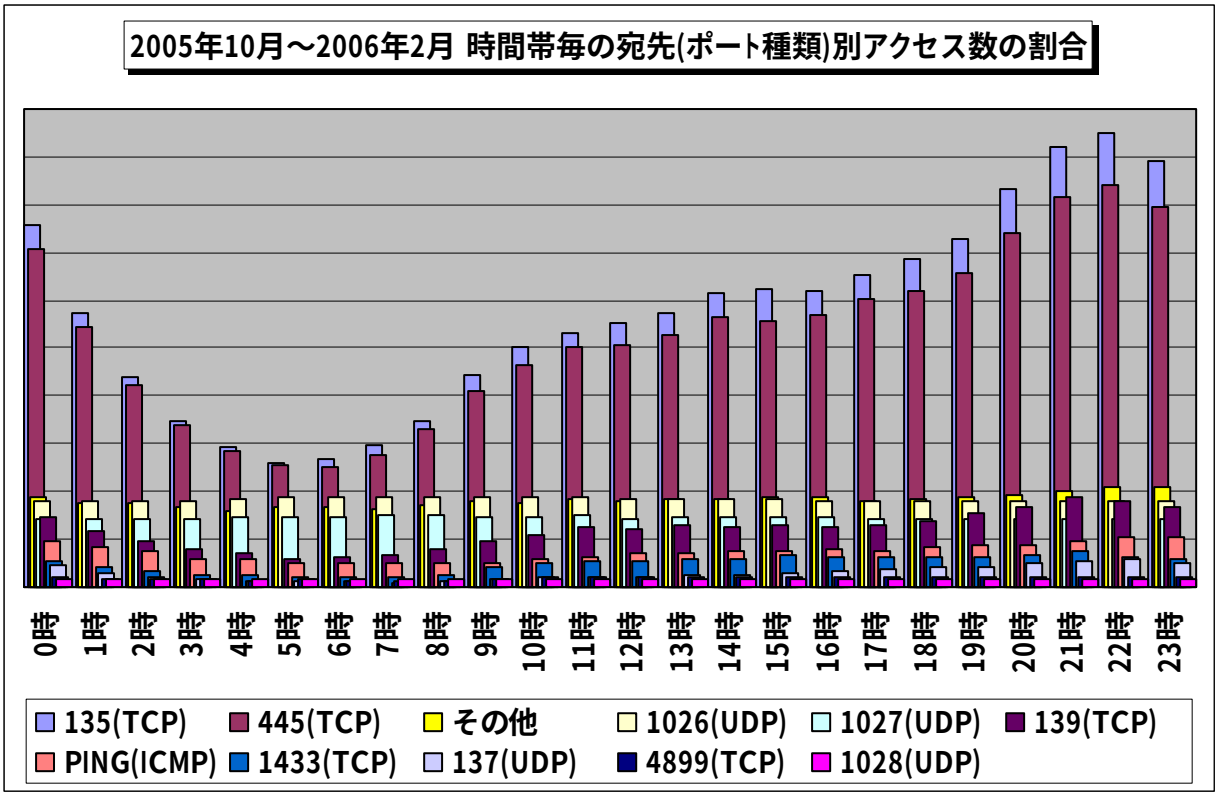


【図 3.2.2 2005 年 10 月～2006 年 2 月の発信元地域別発信元数の比率】

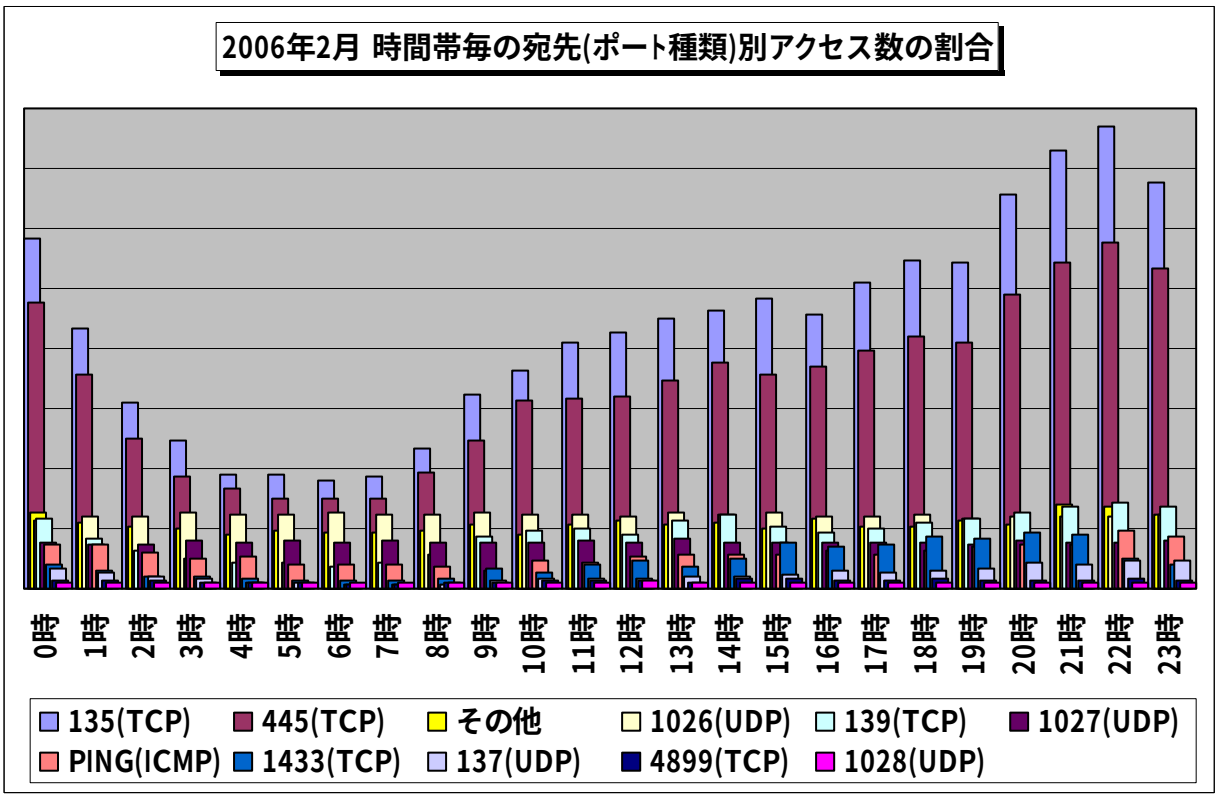
4．その他の統計情報

4.1 2005 年 10 月～2006 年 2 月の時間帯統計

2005 年 10 月～2006 年 2 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 2 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 2 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 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
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)
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)
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
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)
1028(UDP)	1026(UDP)/1027(UDP)と同じアクセス

■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