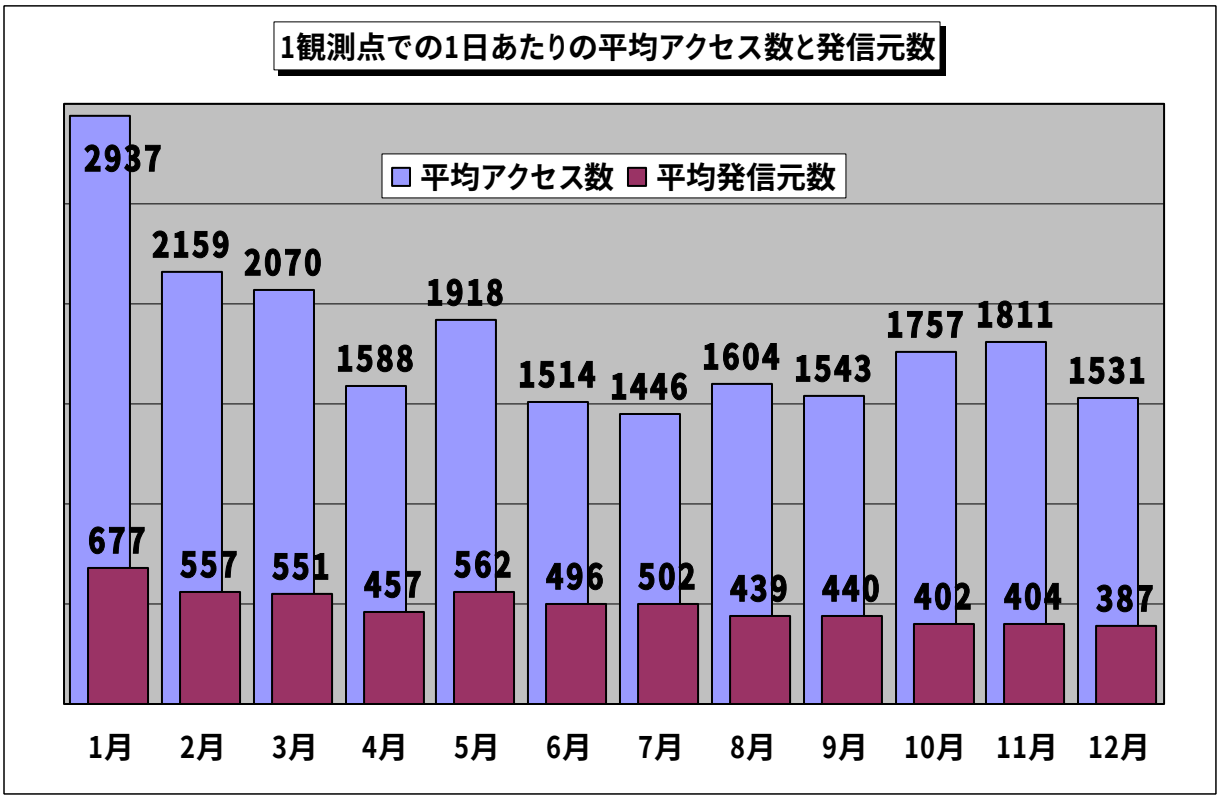
別紙 3

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、2005 年 12 月の期待しない（一方的な）アクセスの総数は、10 観測点で **474,526 件**ありました。1 観測点で 1 日あたり **387** の発信元から **1,531 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、387 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 1 月～12 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、2005 年の後半は、アクセス数および発信元数が同じ水準であるようです。状況は定常化していると言えます。

2．12 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。これらのアクセスの多くが国内発信であることから、国内でのボットの感染が広がっていることが予測されます。

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て下さい。

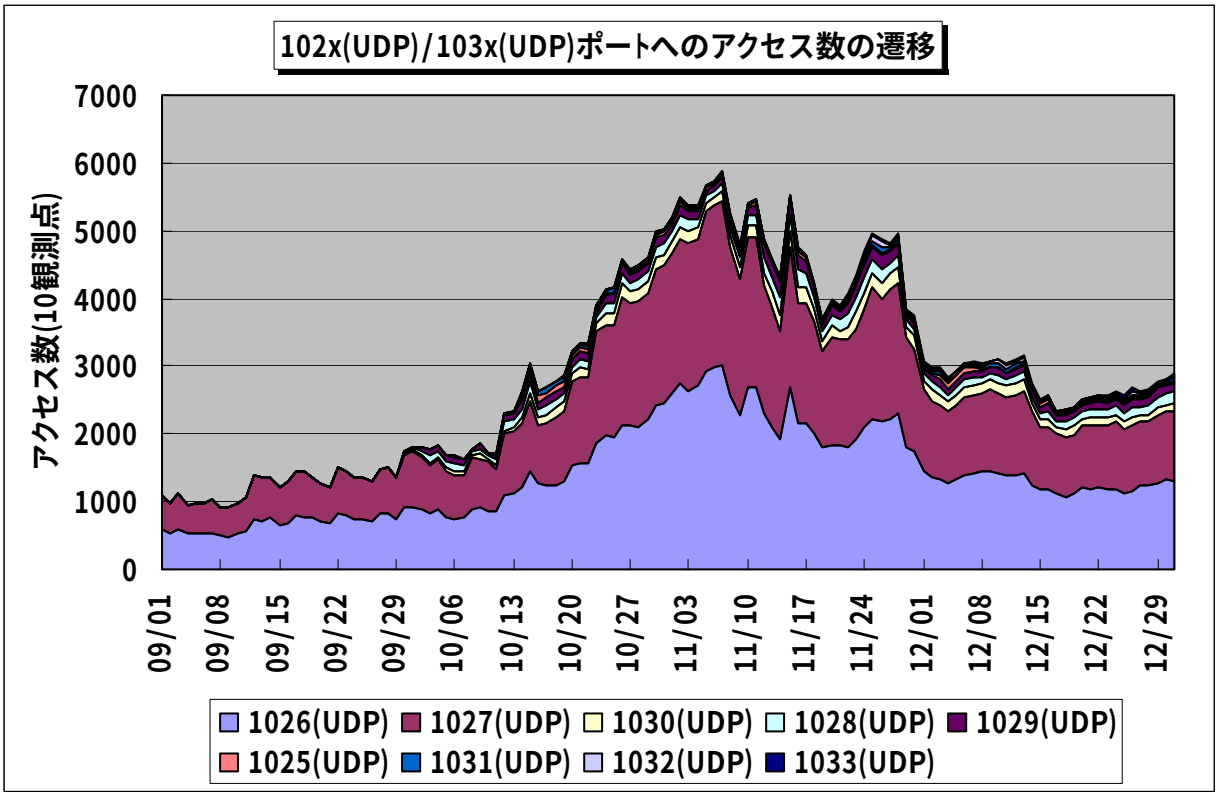
一般のコンピュータ利用者は、これらのボットに感染しないために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフトやパーソナルファイアウォール等を有効利用することをお勧めします。

12 月の特徴的なアクセスは、**Dasher** と呼ばれるワームによる発信元 6000 ポートからの 1025(TCP)ポートへのアクセスです。このアクセスは、Windows の脆弱性(MS05-051)を狙ったもので、該当脆弱性のパッチが適用されていない状態で、インターネットに直接接続（グローバル IP で接続）されたコンピュータの場合は、感染する可能性があります。実際には、月末に向けてアクセス数は減少傾向にあるようです。これらのアクセスについては、「**2.4 発信元 6000 ポートからの 1025(TCP)ポートへのアクセスについて**」に詳細を記述します。

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(下図を参照下さい)。

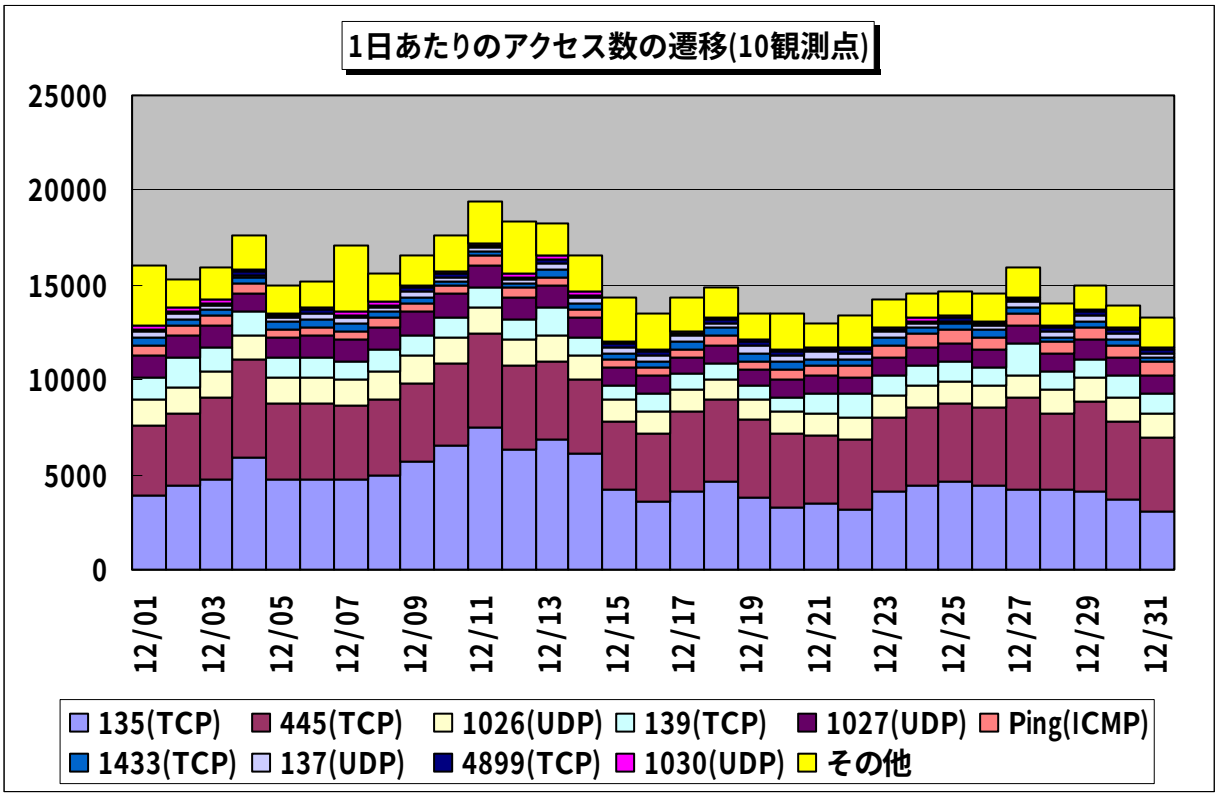
最近は、ウイルス対策や不正アクセス対策を勧めるポップアップメッセージやネットサーフィン時のアドウェアによるポップアップ広告等も多いので、これらの内容に騙されないように注意して下さい。

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。

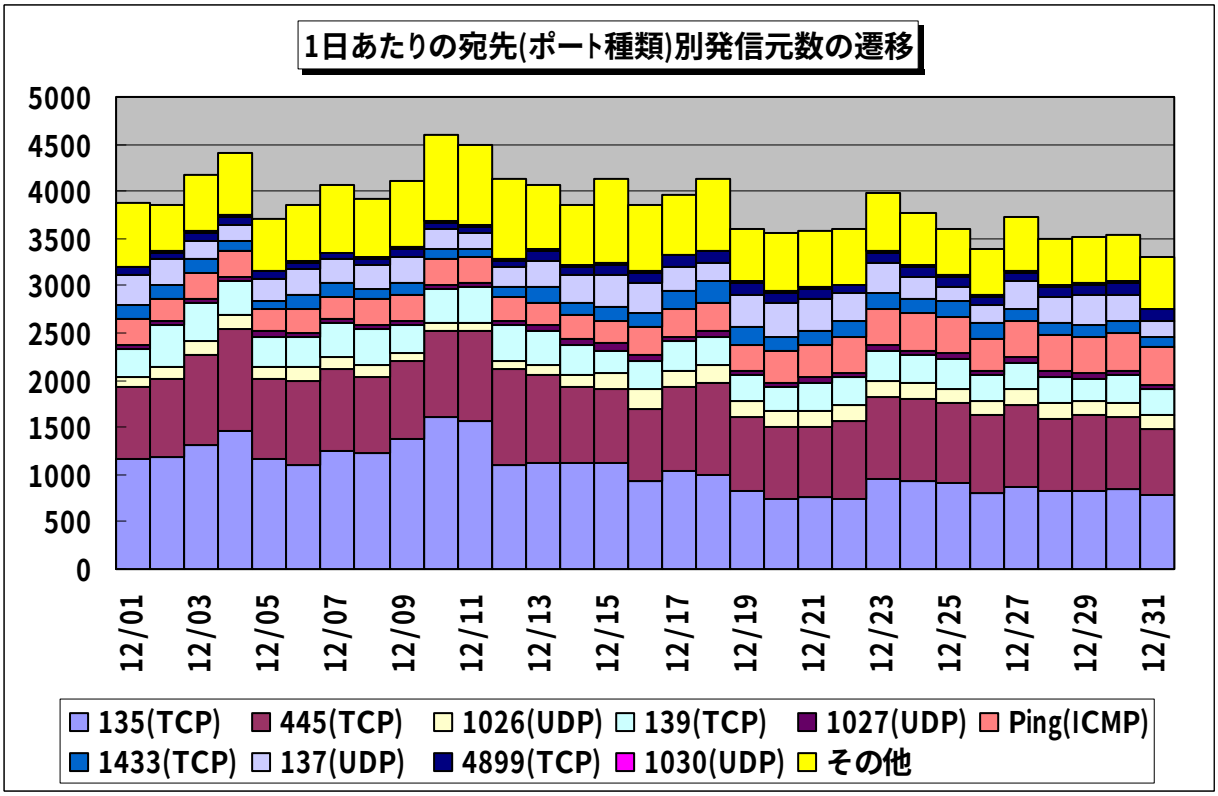


【図 2 102x(UDP)/103x(UDP)ポートへのアクセス数の遷移】

2.1 2005 年 12 月の一方的なアクセス状況

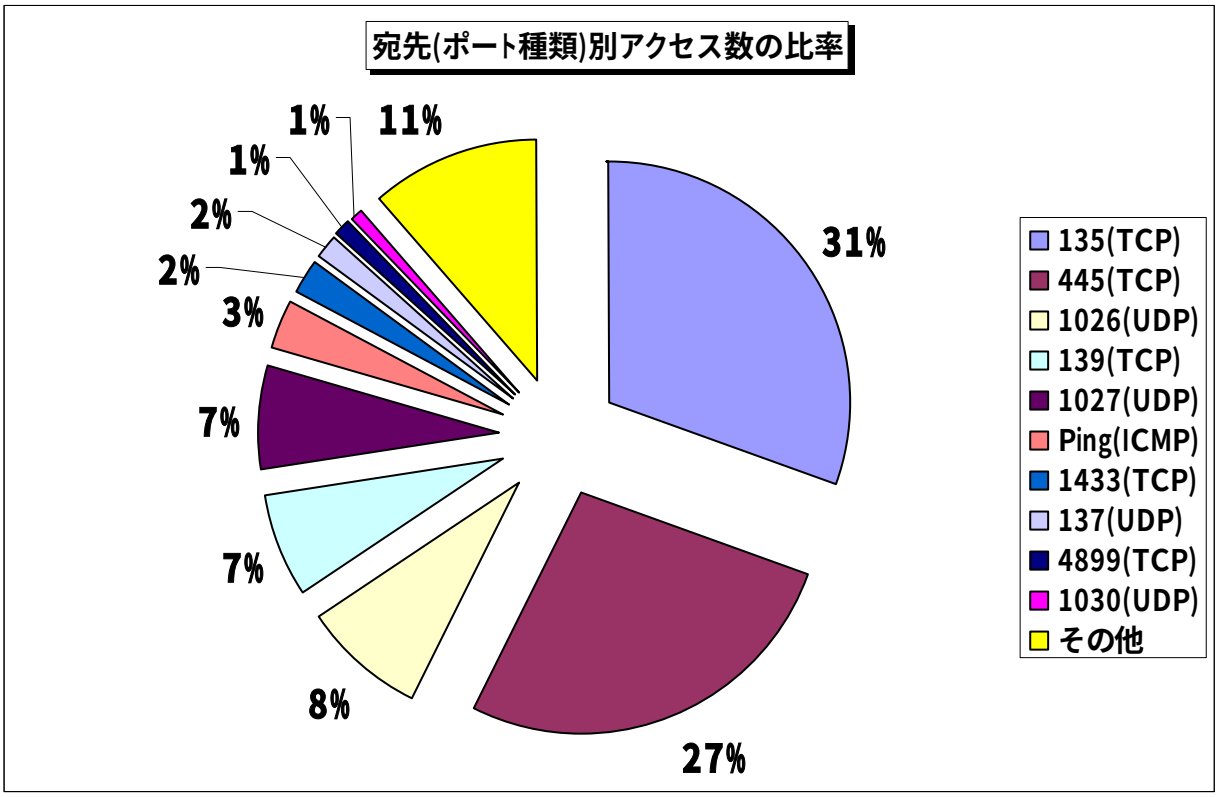


【図 2.1.1 2005 年 12 月の一方的なアクセス状況(アクセス数)】

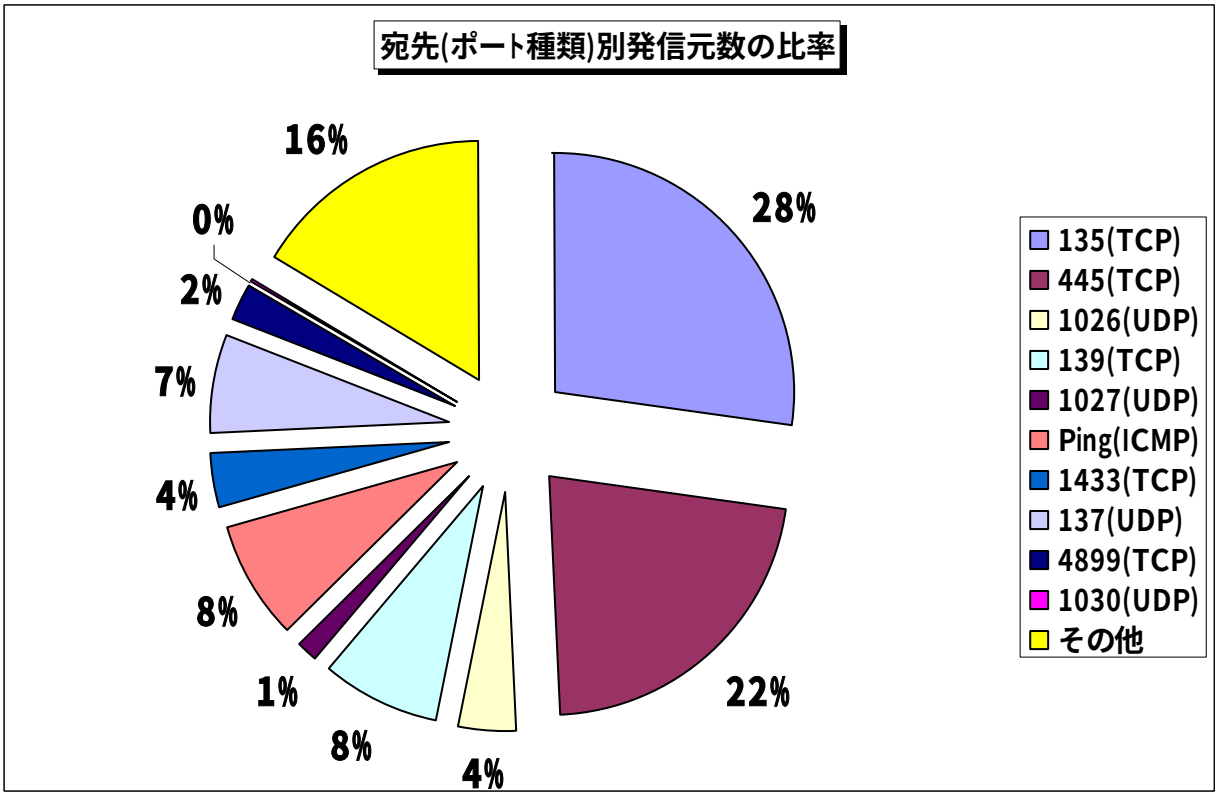


【図 2.1.2 2005 年 12 月の一方的なアクセス状況(発信元数)】

2.2 2005 年 12 月の宛先(ポート種類)別の比率

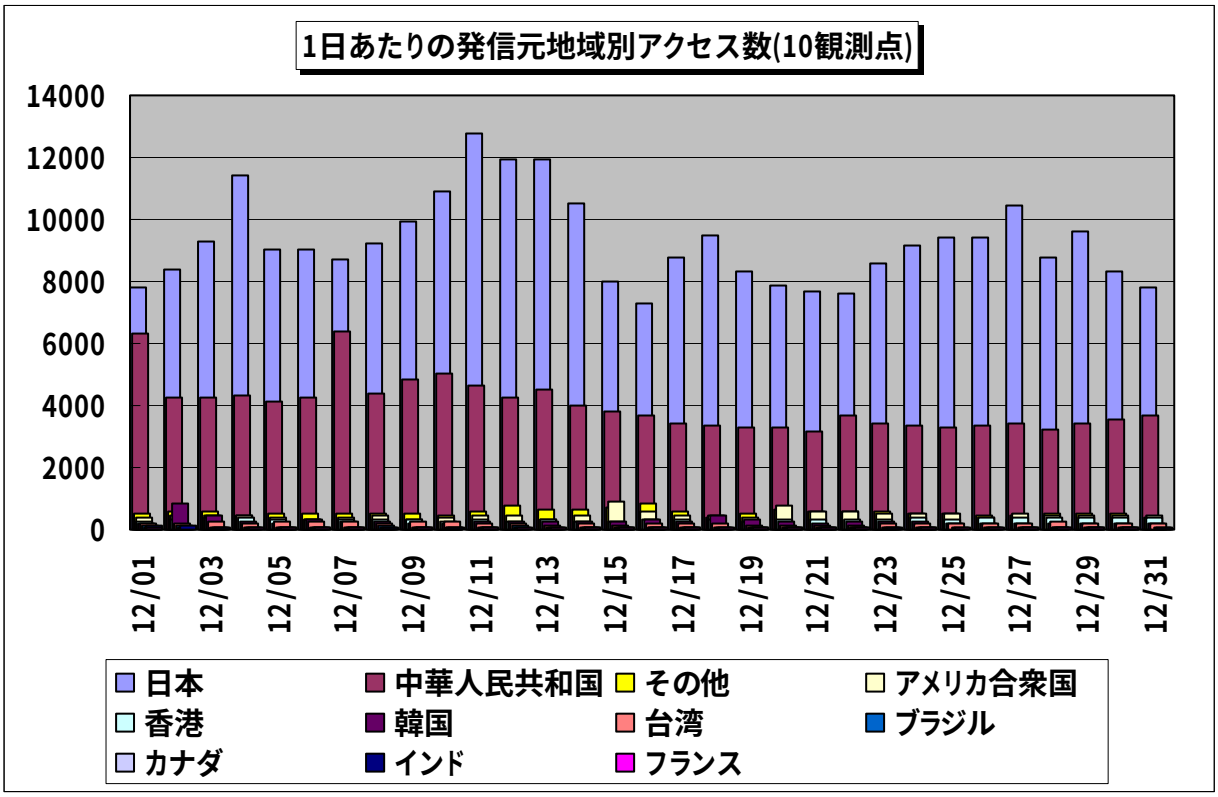


【図 2.2.1 2005 年 12 月の宛先(ポート種類)別アクセス数の比率】

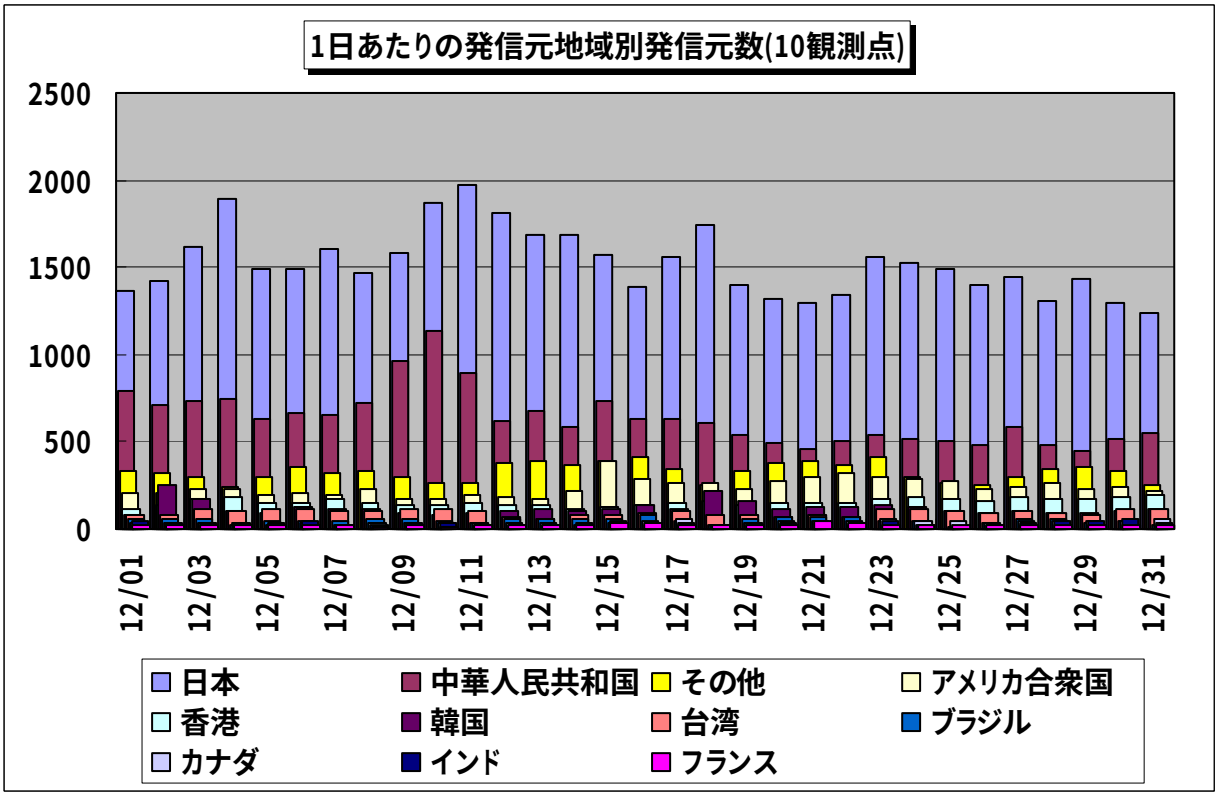


【図 2.2.2 2005 年 12 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 12 月の発信元地域別アクセス状況

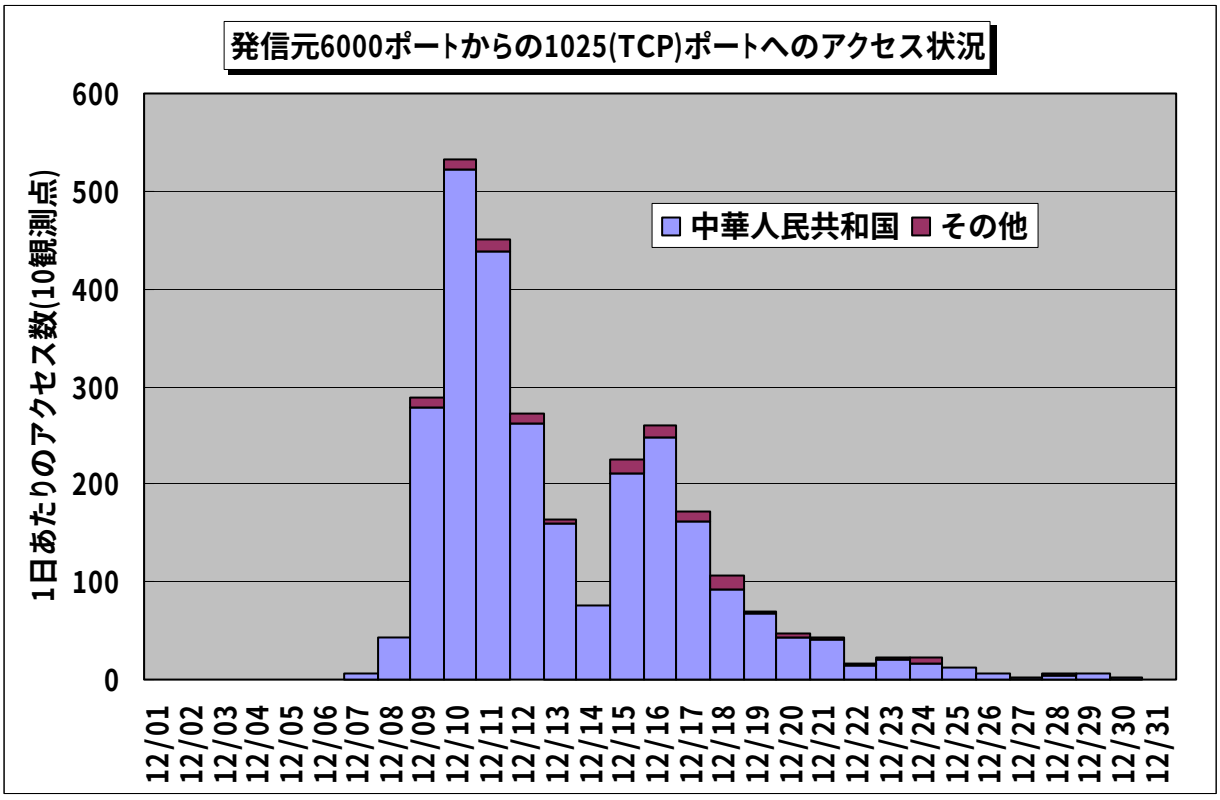


【図 2.3.1 2005 年 12 月の発信元地域別アクセス数の変化】

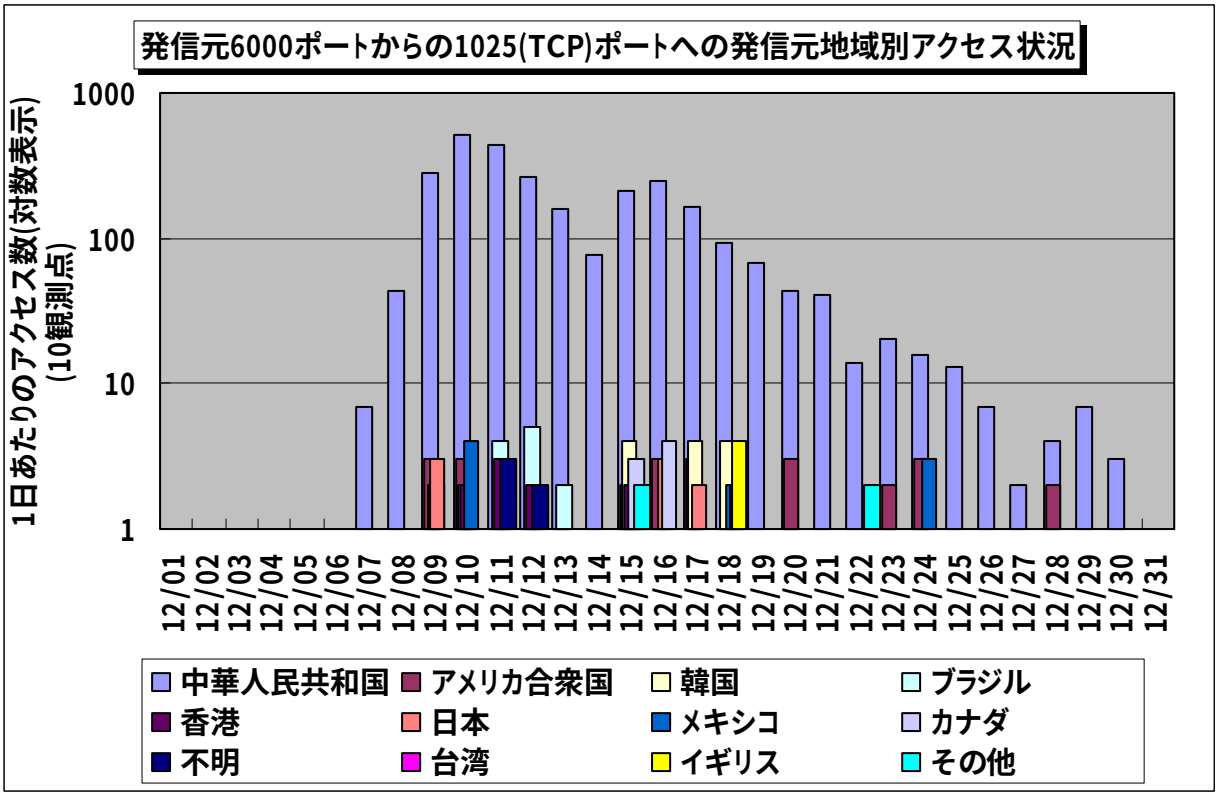


【図 2.3.2 2005 年 12 月の発信元地域別発信元数の変化】

2.4 発信元 6000 ポートからの 1025(TCP)ポートへのアクセスについて



【図 2.4.1 発信元 6000 ポートからの 1025(TCP)ポートへのアクセス状況】



【図 2.4.2 発信元 6000 ポートからの 1025(TCP)ポートへの発信元地域別アクセス状況】

- 発信元 6000 ポートからの 1025(TCP)ポートへのアクセスが 12 月 7 日から観測されています。これらのアクセスは、ほとんどが中国方面からのものです(図 2.4.2 は縦軸が対数表示になっているので、ご注意下さい)。

- これらのアクセスは、**Dasher** と呼ばれるワームによると考えられます。
- 月末に向けて、アクセス数は減少傾向にあるようですが、注意が必要です。
- 1025(TCP)ポートへのアクセスは、Microsoft Windows の脆弱性(MS05-051)を攻略するためのポートスキャンであり、パッチが適用されていない状態で、インターネットに直接接続（グローバル IP で接続）されたコンピュータの場合は、この脆弱性が攻略される可能性があります。
- 被害にあわないための対策は以下の通り
  - **Windows Update (Microsoft Update) により Windows の脆弱性を解消する**
  - **インターネットと直結接続している場合は、ルータ等の機器を導入する**
  - **Windows XP の場合は、ファイアウォール設定を有効にする**
  - **パーソナルファイアウォールを導入する**

(参考情報)

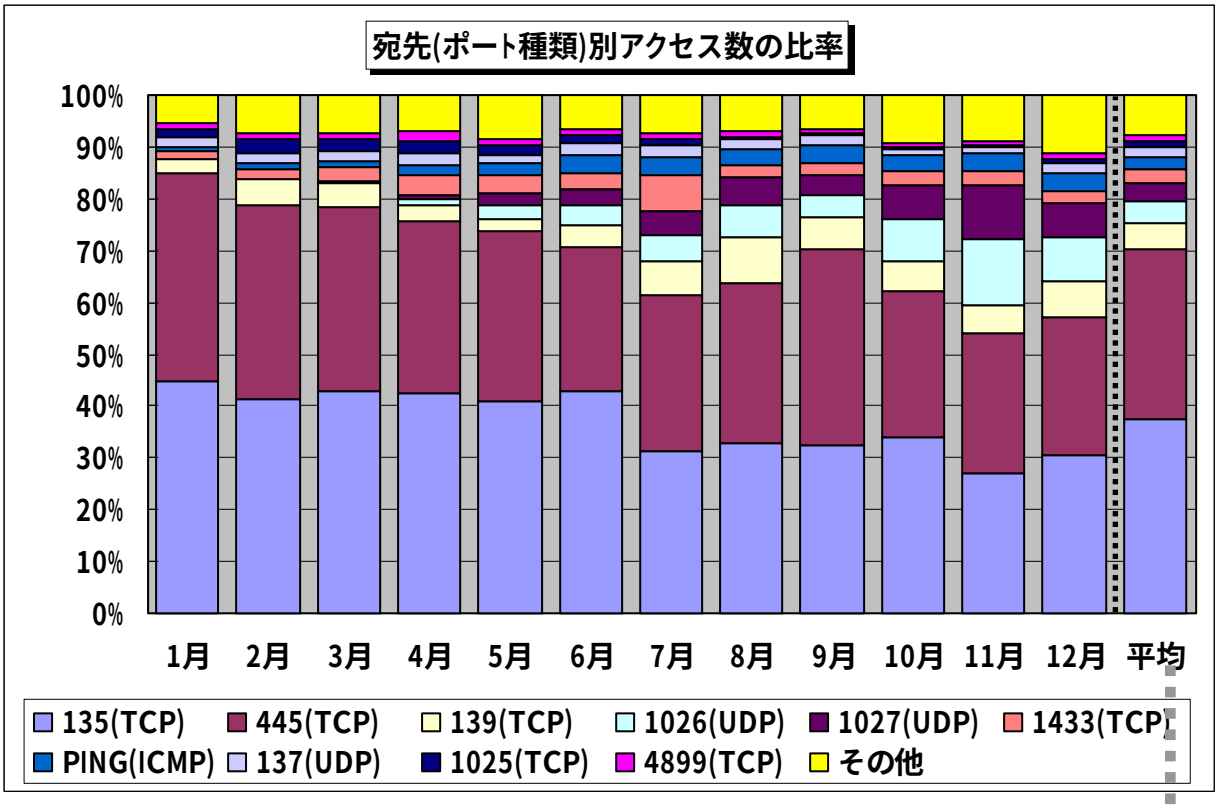
■Microsoft 社 Windows の脆弱性 (MS05-051) について
http://www.ipa.go.jp/security/ciadr/vul/20051216-ms05-051.html
■MSDTC および COM+ の脆弱性により、リモートでコードが実行される (902400) (MS05-051)
http://www.microsoft.com/japan/technet/security/bulletin/ms05-051.mspx
■US-CERT
http://www.kb.cert.org/vuls/id/180868
http://www.kb.cert.org/vuls/id/950516
■CIAC
http://www.ciac.org/ciac/bulletins/q-009.shtml

(ウイルス情報)

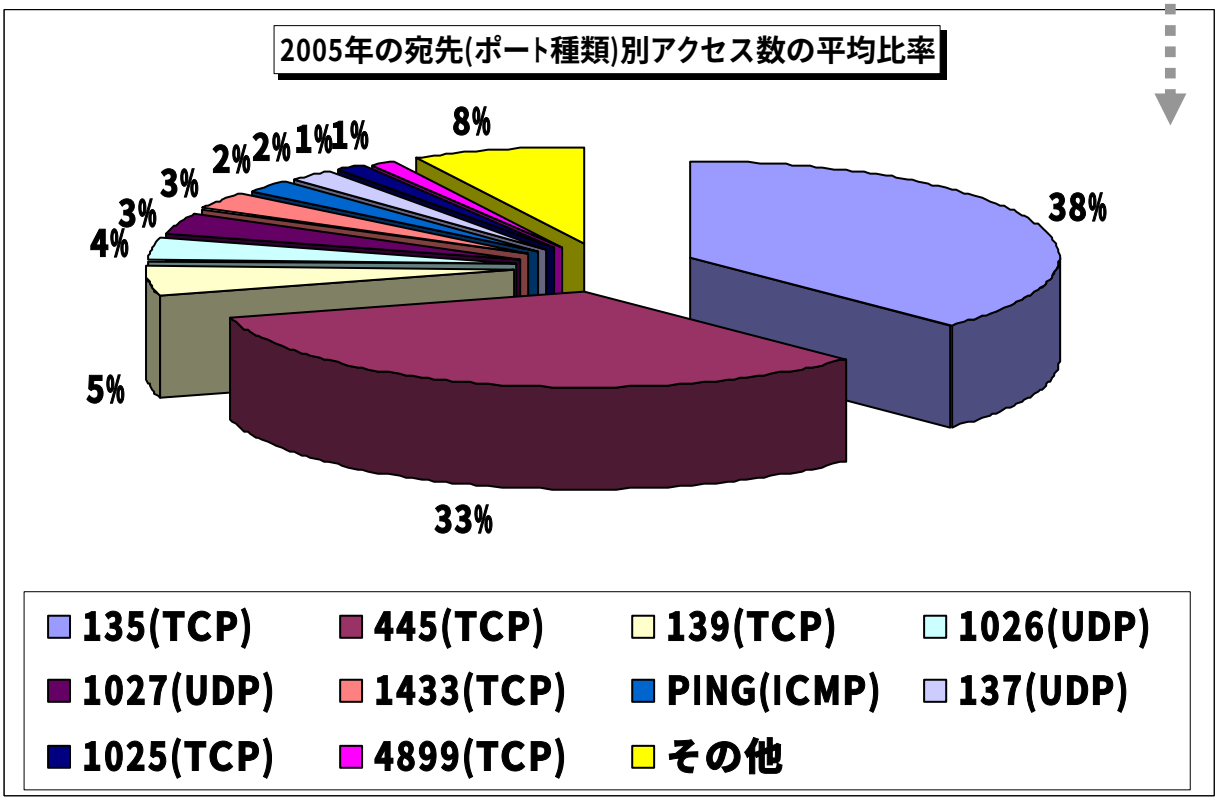
□F-SECURE
http://www.f-secure.co.jp/v-descs/v-descs3/Dasher.B-jp.htm
http://www.f-secure.co.jp/v-descs/v-descs3/Dasher.A-jp.htm
□Symantec
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.dasher.d.html
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.dasher.c.html
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.dasher.b.html
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.dasher.a.html
□McAfee
http://www.mcafee.com/japan/security/virD.asp?v=W32/Dasher.worm
□SOPHOS
http://www.sophos.co.jp/virusinfo/analyses/w32dasherc.html
□TRENDMICRO
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_DASHER.C
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_DASHER.B
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_DASHER.A

3．統計情報

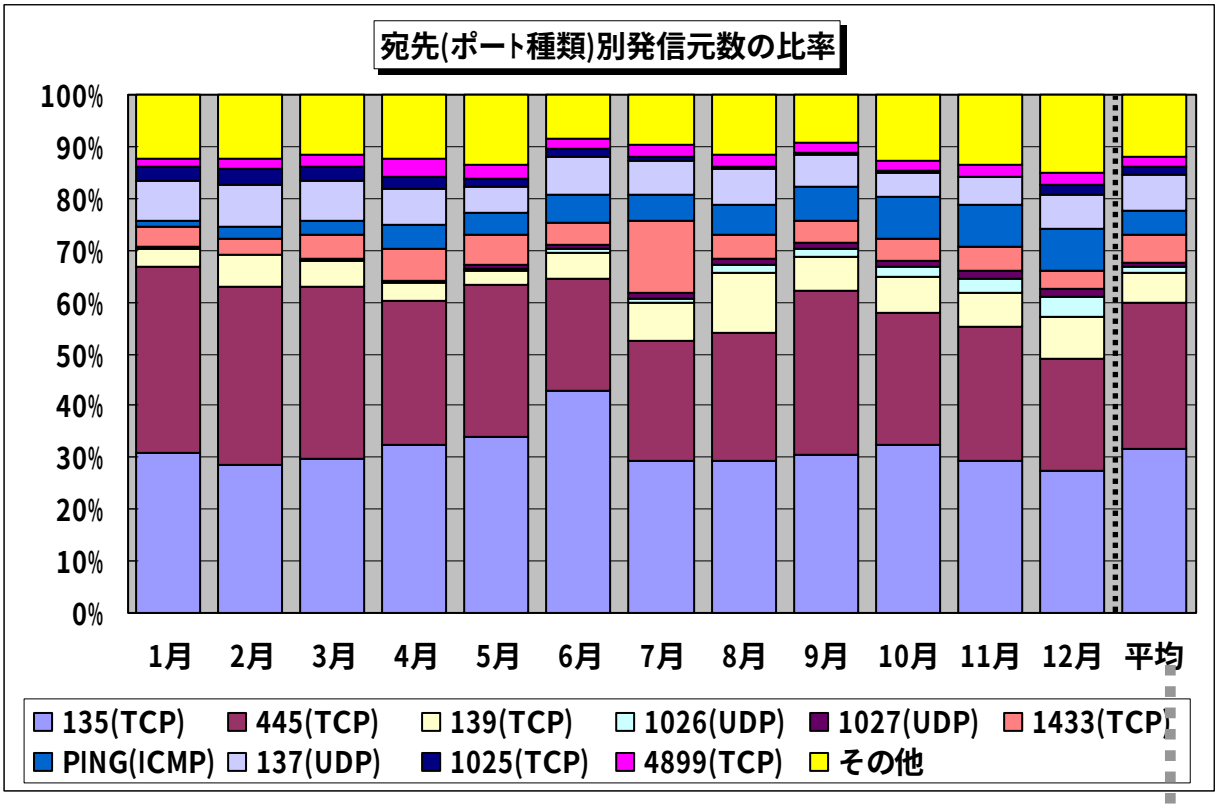
3.1 2005 年 1 月～12 月の宛先(ポート種類)別の比率



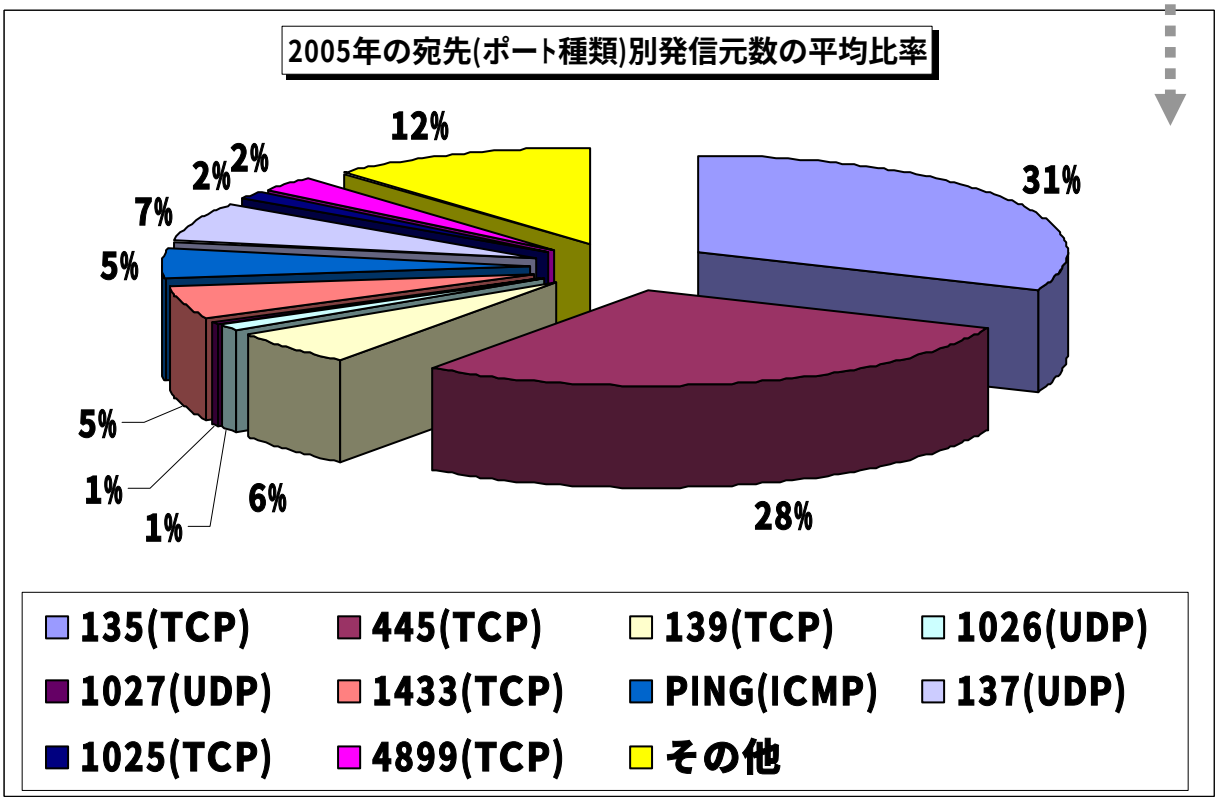
【図 3.1.1 2005 年 1 月～12 月の宛先(ポート種類)別アクセス数の比率】



【図 3.1.2 2005 年の宛先(ポート種類)別アクセス数の平均比率】

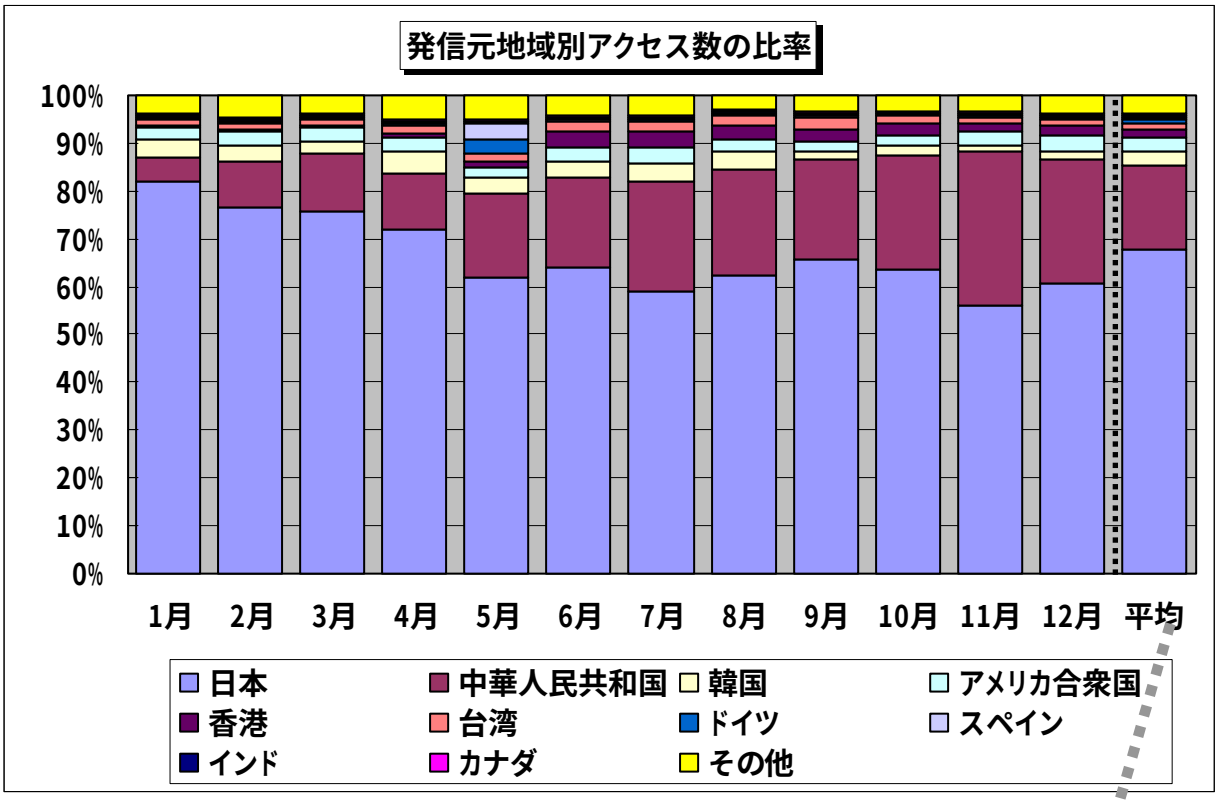


【図 3.1.3 2005 年 1 月～12 月の宛先(ポート種類)別発信元数の比率】

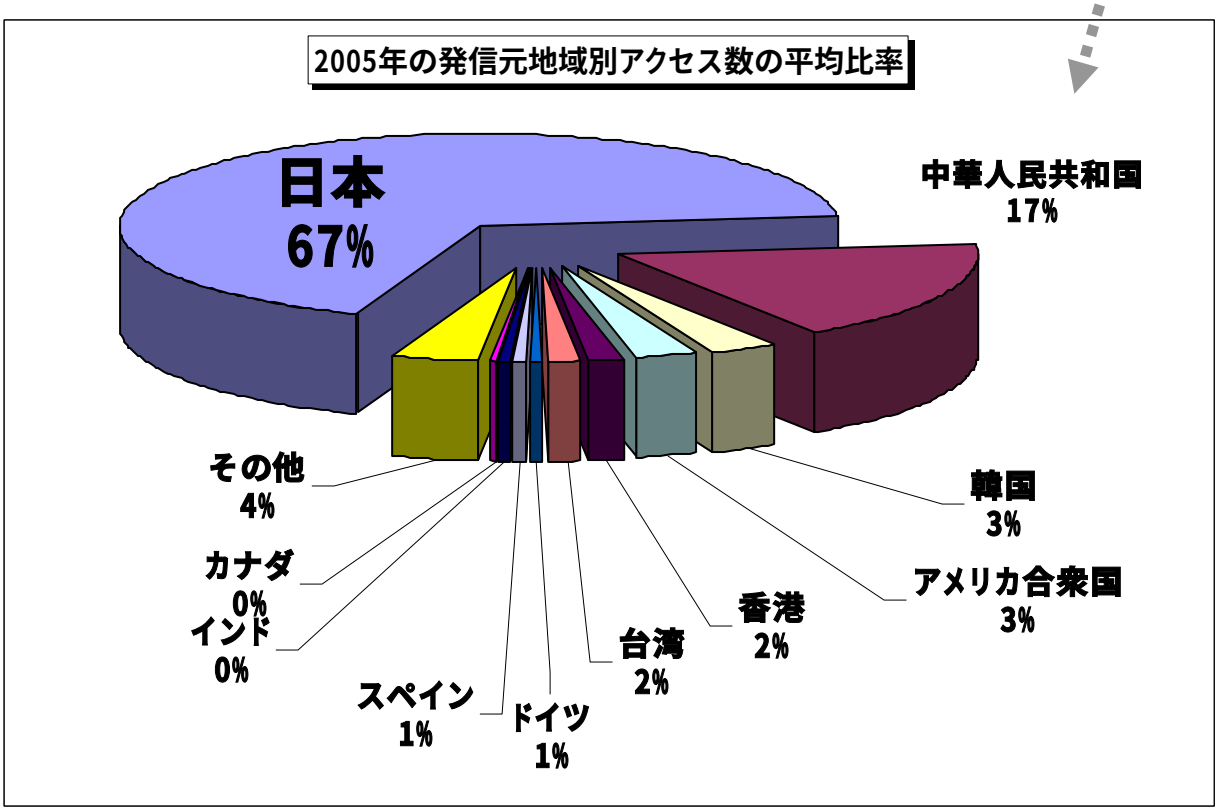


【図 3.1.4 2005 年の宛先(ポート種類)別発信元数の平均比率】

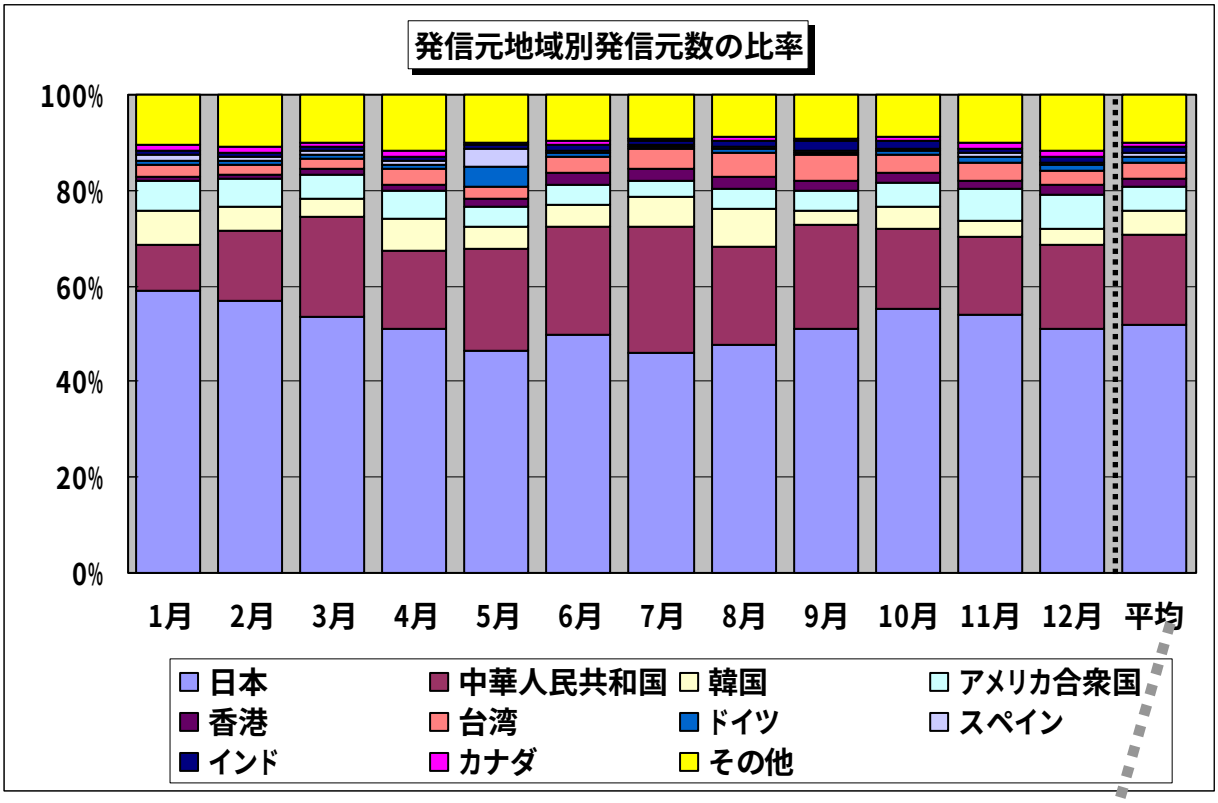
3.2 2005 年 1 月～12 月の発信元地域別の比率



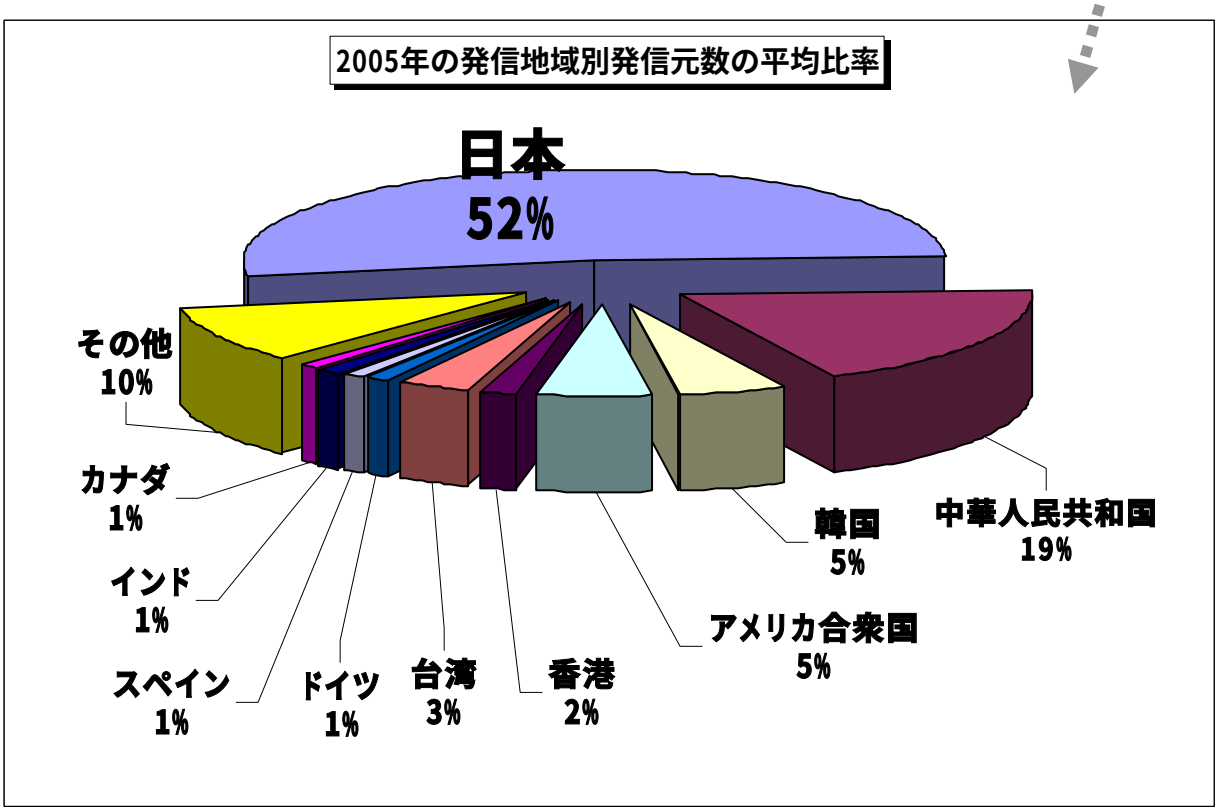
【図 3.2.1 2005 年 1 月～12 月の発信元地域別アクセス数の比率】



【図 3.2.2 2005 年の発信元地域別アクセス数の平均比率】



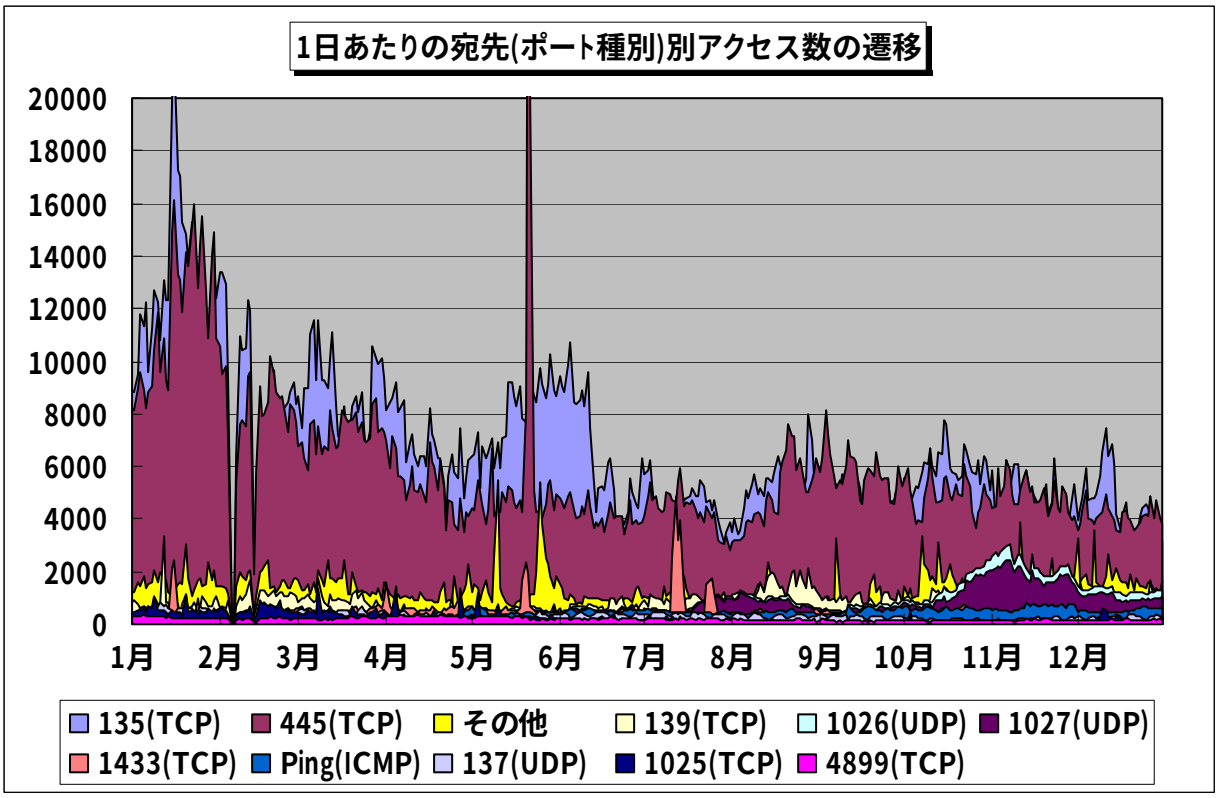
【図 3.2.3 2005 年 1 月～12 月の発信元地域別発信元数の比率】



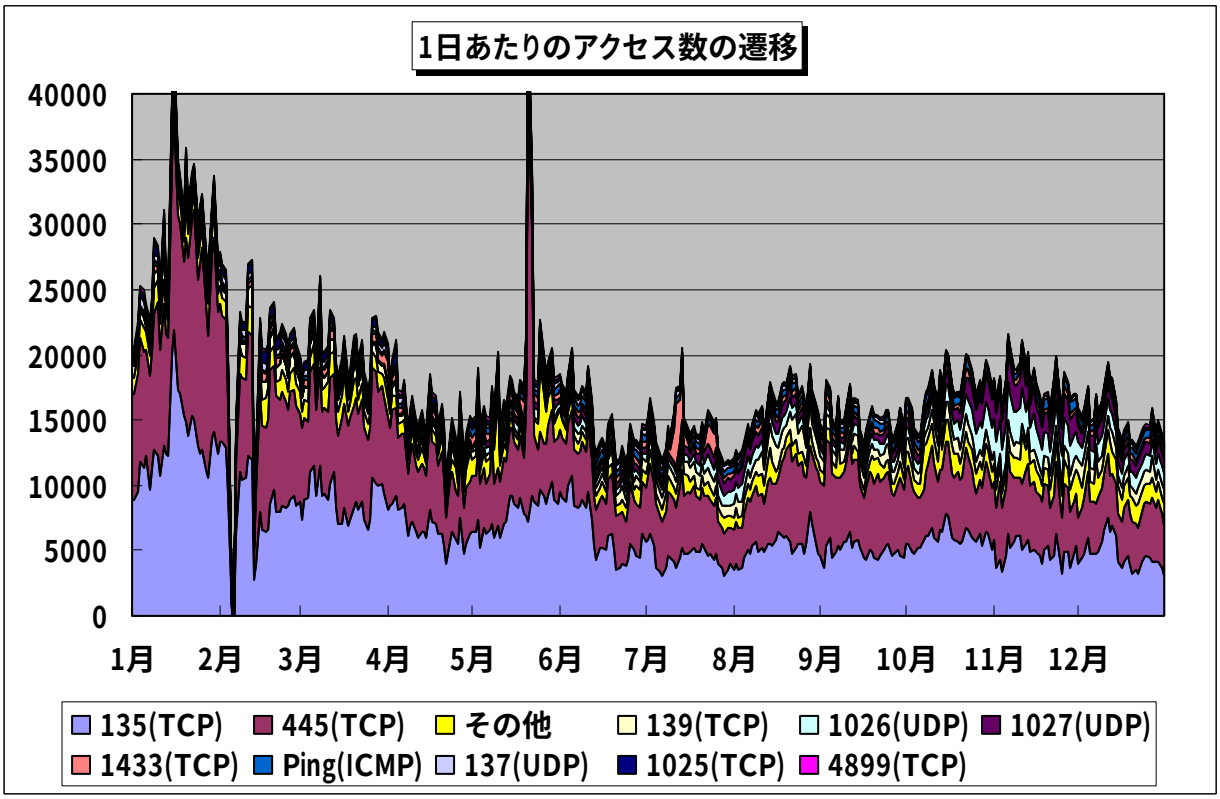
【図 3.2.4 2005 年の発信元地域別発信元数の平均比率】

3.3 2005 年 1 月～12 月のアクセス数および発信元数の変化

2005 年 1 月～12 月の宛先(ポート種類)別アクセス数の変化を図 3.3.1 および図 3.3.2 に示します。

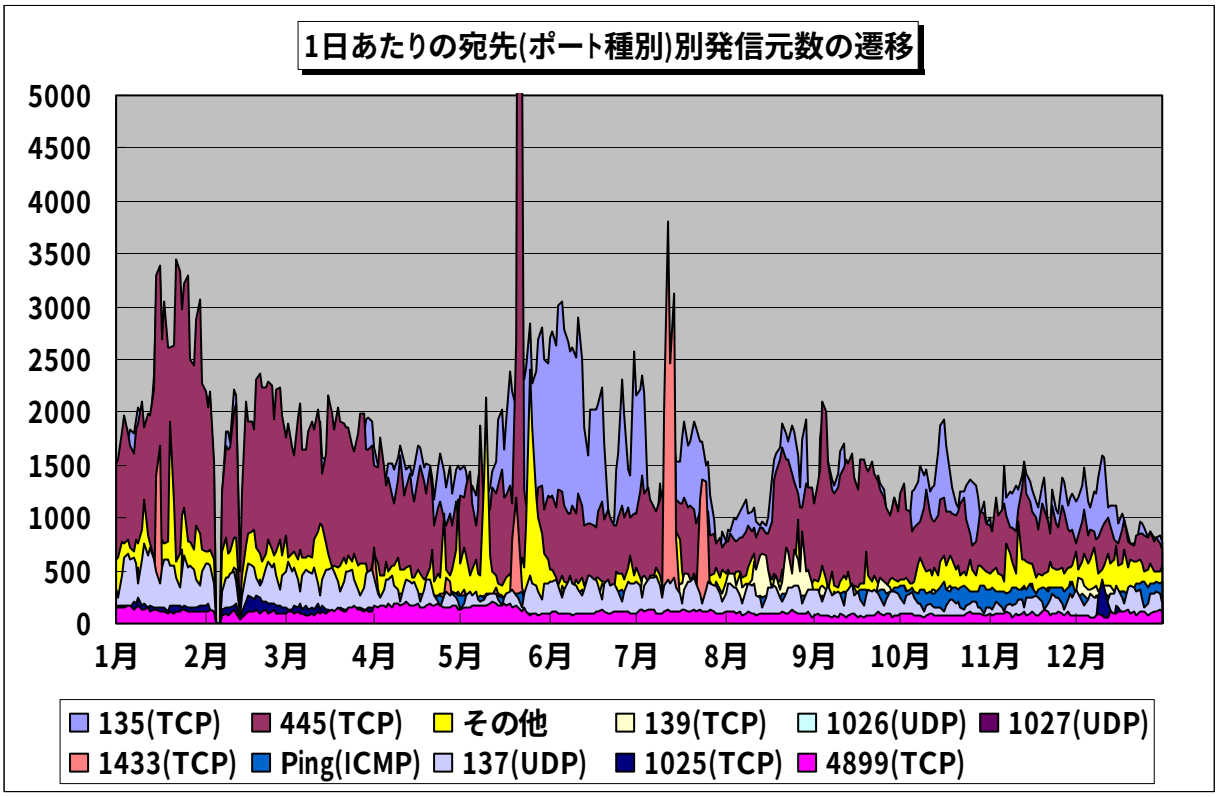


【図 3.3.1 2005 年の宛先(ポート種類)別アクセス数の変化】

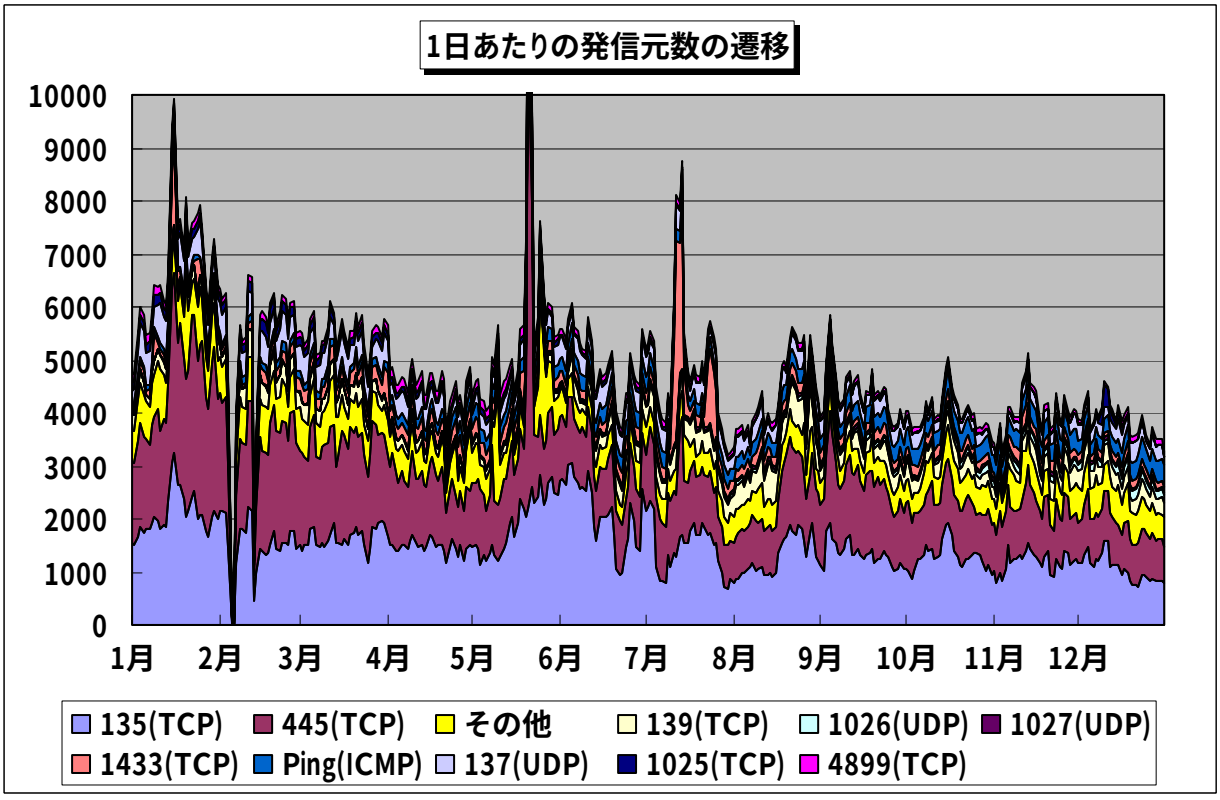


【図 3.3.2 2005 年のアクセス数の変化(1)】

2005 年 1 月～12 月の宛先(ポート種類)別発信元数の変化を図 3.3.3 および図 3.3.4 に示します。

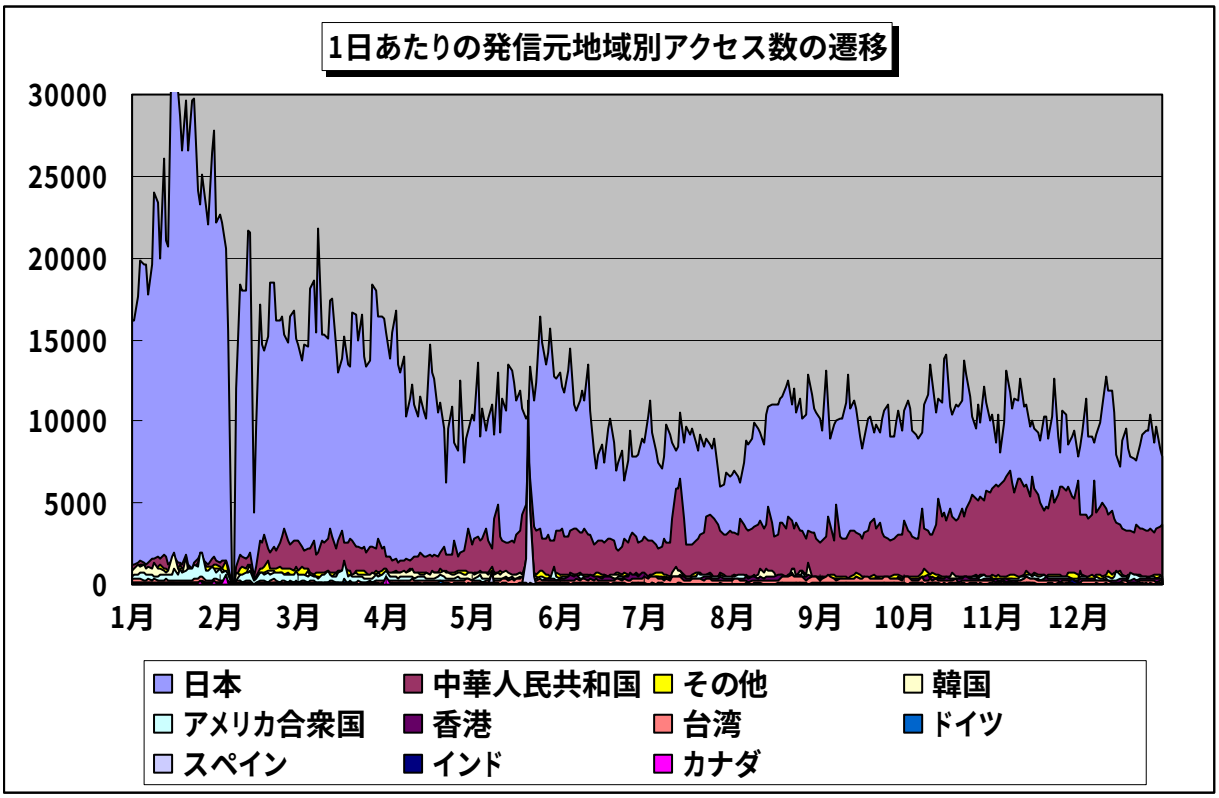


【図 3.3.3 2005 年の宛先(ポート種類)別発信元数の変化】

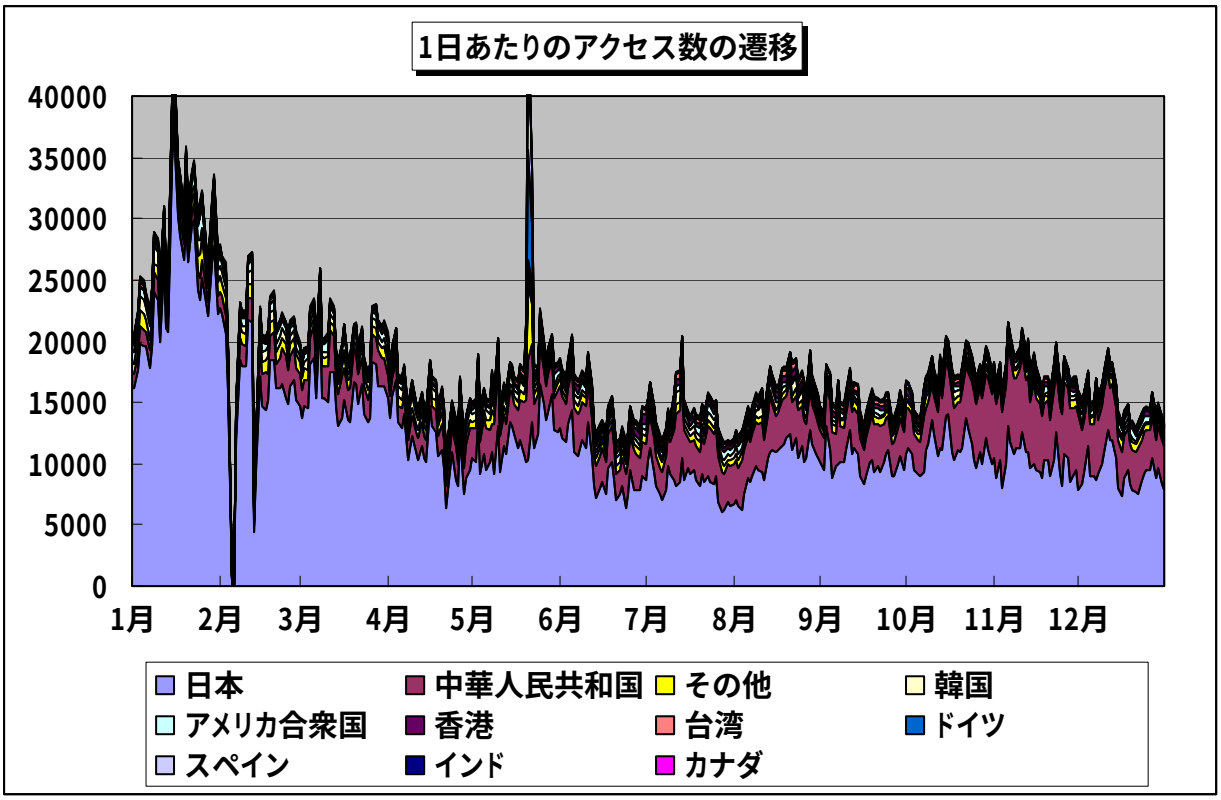


【図 3.3.4 2005 年の発信元数の変化(1)】

2005年1月～12月の発信元地域別アクセス数の変化を図3.3.5および図3.3.6に示します。

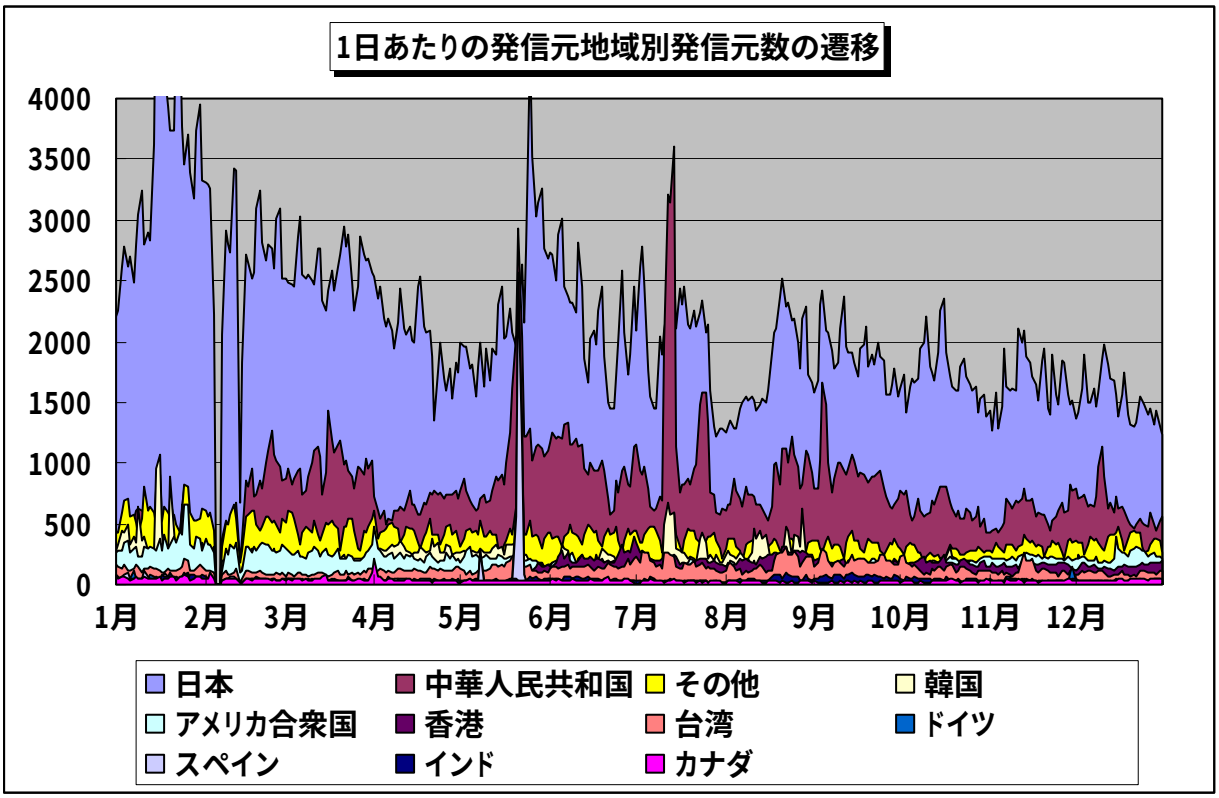


【図 3.3.5 2005 年の発信元地域別アクセス数の変化】

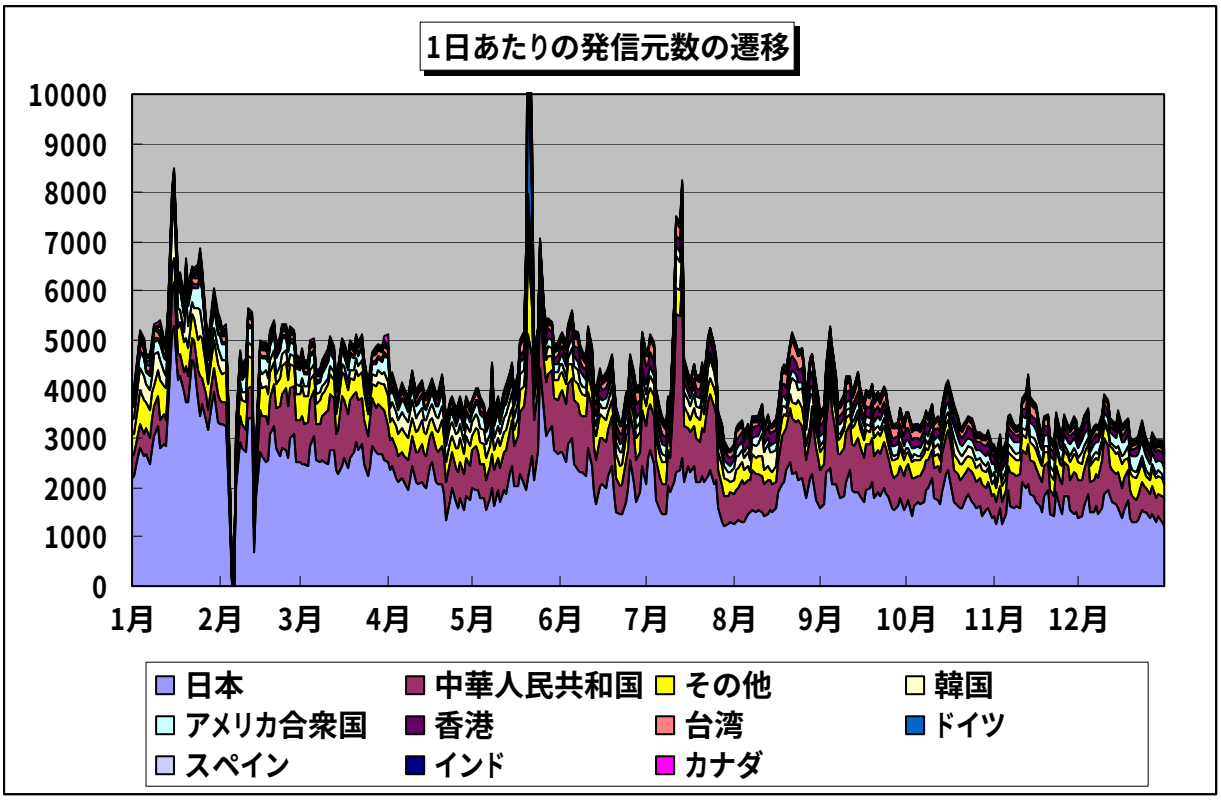


【図 3.3.6 2005 年のアクセス数の変化(2)】

2005 年 1 月～12 月の発信元地域別発信元数の変化を図 3.3.7 および図 3.3.8 に示します。



【図 3.3.7 2005 年の発信元地域別発信元数の変化】

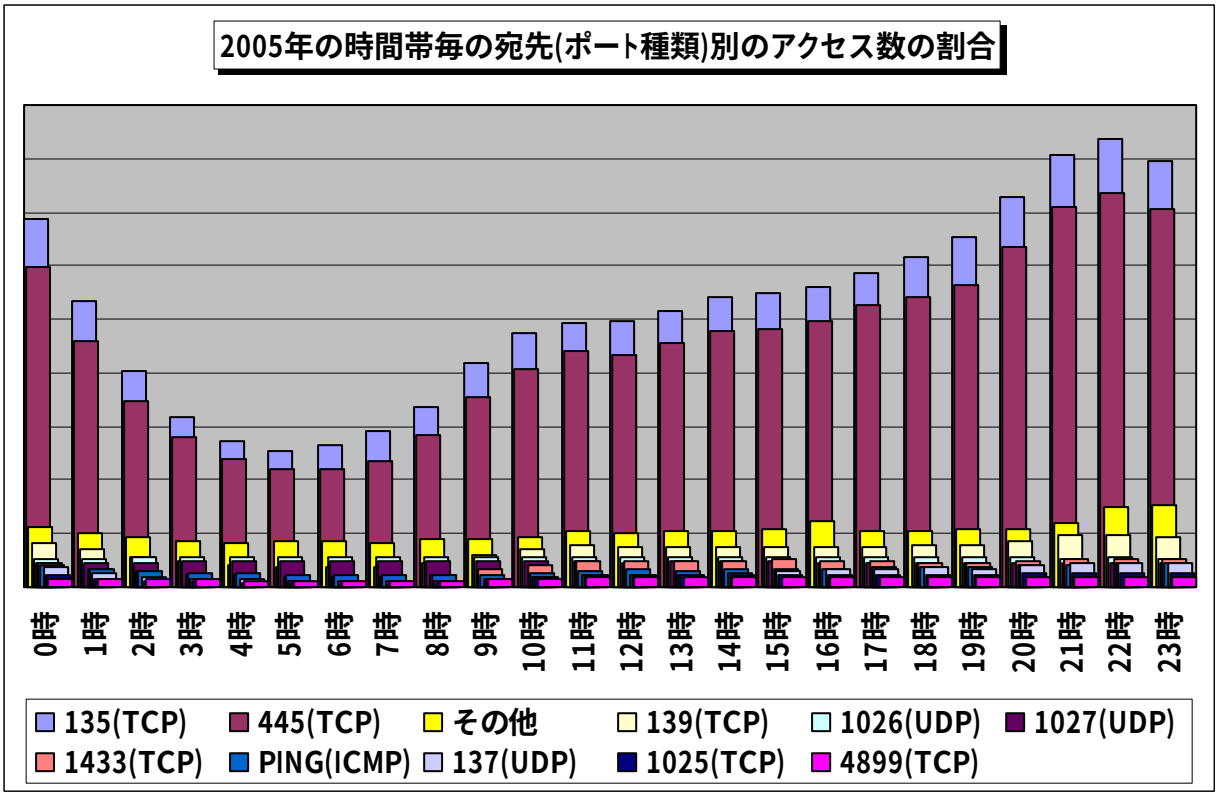


【図 3.3.8 2005 年の発信元数の変化(2)】

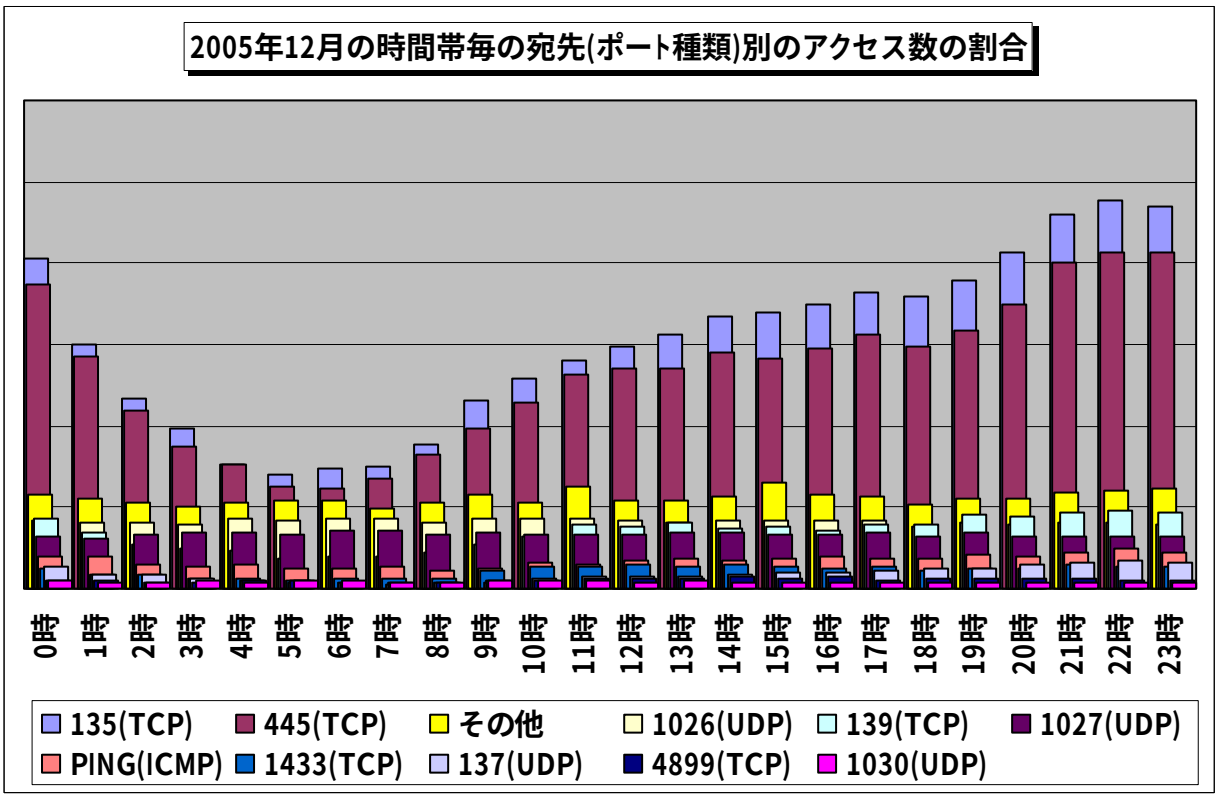
4．その他の統計情報

4.1 2005 年 1 月～12 月の時間帯統計

2005 年 1 月～12 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、2005 年 12 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 1 月～12 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 2005 年 12 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、2005 年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)
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ようです
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である
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がある
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
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る
1025(TCP)	135(TCP)と同じように Microsoft Windows Remote Procedure Call (RPC)で利用されるポートであり、12 月には Windows の脆弱性(MS05-051)を狙った不正アクセスに利用されている
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である

■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