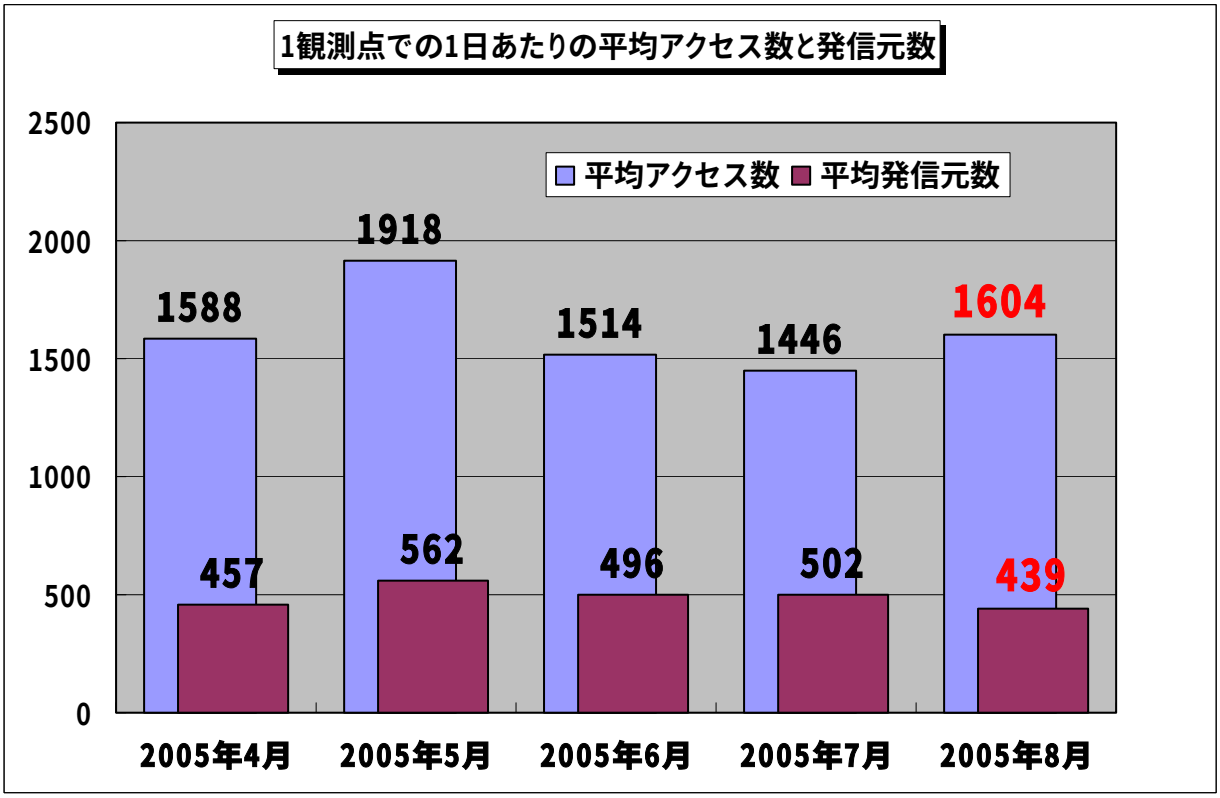
別紙 3

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 8 月の期待しない（一方的な）アクセスの総数は、10 観測点で **497,340 件**ありました。1 観測点で 1 日あたり **439** の発信元から **1,604 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、440 人の見知らぬ人から、発信元一人当たり 3～4 件ずつ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 4 月～8 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 5 月以外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。

2．8 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、ワーム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。昨今の状況から考えて、最近ボットと呼ばれるワームが流行していることから、これらのアクセスを行っているワームもボットである可能性が高いと思われます。

特にアクセス数の多い 135(TCP),445(TCP)へのアクセスは、Windows の古いタイプの脆弱性を狙っていると思われ、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に心掛けて下さい。

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等を有効利用することをお勧めします。

2005 年 8 月の一方的なアクセスの変化<宛先(ポート種類)別アクセス数の変化>を、図 2.1.1 に示します。あいかわらず、135(TCP),445(TCP)ポートへのアクセスおよび 139(TCP)ポートへのアクセスが多いことが確認できます。

次に、図 2.1.2 に宛先(ポート種類)別発信元数の状況を示します。宛先(ポート種類)別発信元数とは、特定の宛先(ポート種類)へアクセスしている発信元(発信 IP アドレス)の数のことです。

135(TCP),445(TCP)ポートへのアクセスについては、アクセス数の場合と同様に発信元数も多いことが分かります。

ただし、複数の宛先へ同一の発信元からアクセスされる場合もあるので、図2.1.2の縦軸に示された発信元数が、実際の発信元数ではないことに注意して下さい。

図 2.1.1 と図 2.1.2 の違いは、ちょうどウイルス発見届出での検知件数と届出件数の違いと、同じ理屈になっており、図 2.1.1 のアクセス数でのアクセス状況は実際のアクセスの脅威を示し、図 2.1.2 の発信元数でのアクセス状況からはアクセスの原因となるコンピュータ(発信元)の感染状況を示すと考えられます。

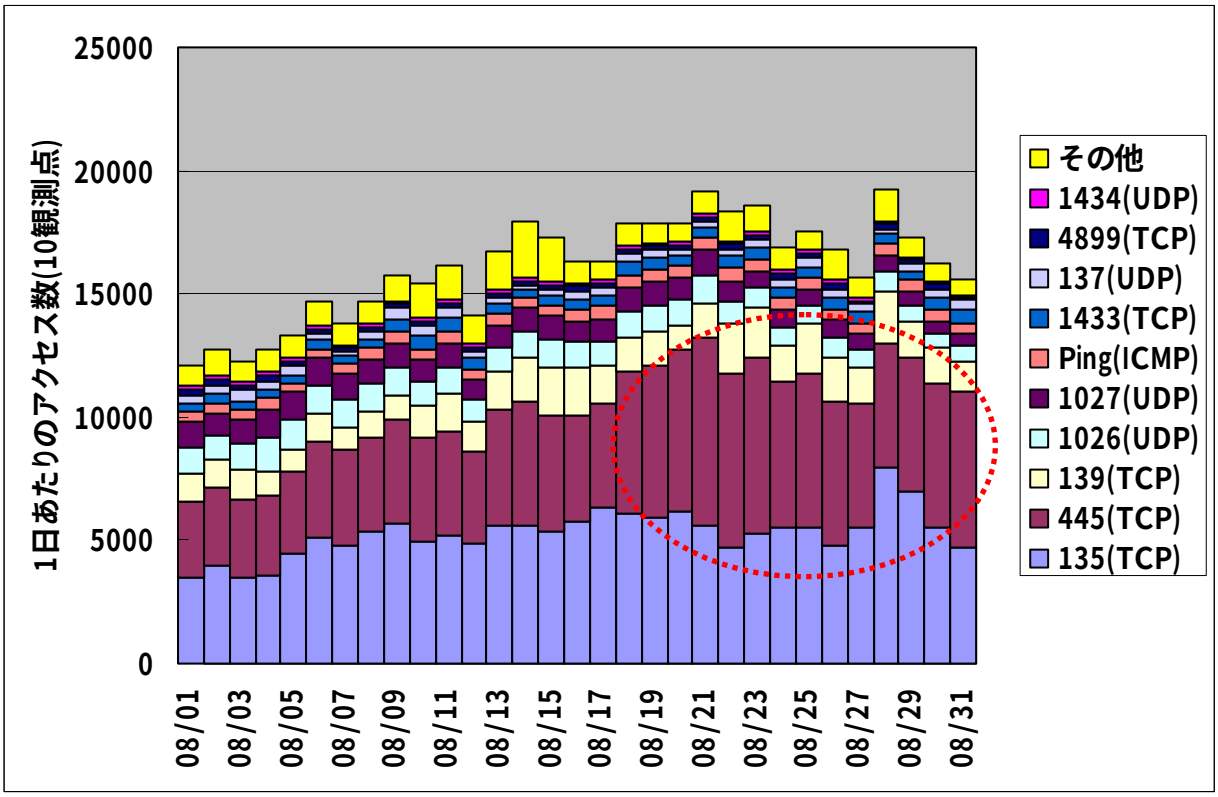
図 2.2.1 および図 2.2.2 には、宛先(ポート種類)別アクセス数の比率および宛先(ポート種類)別発信元数の比率を示します。

図 2.3.1 および図 2.3.2 には、発信元地域別アクセス数の変化および発信元地域別発信元数の変化を 1 日単位で示しています。

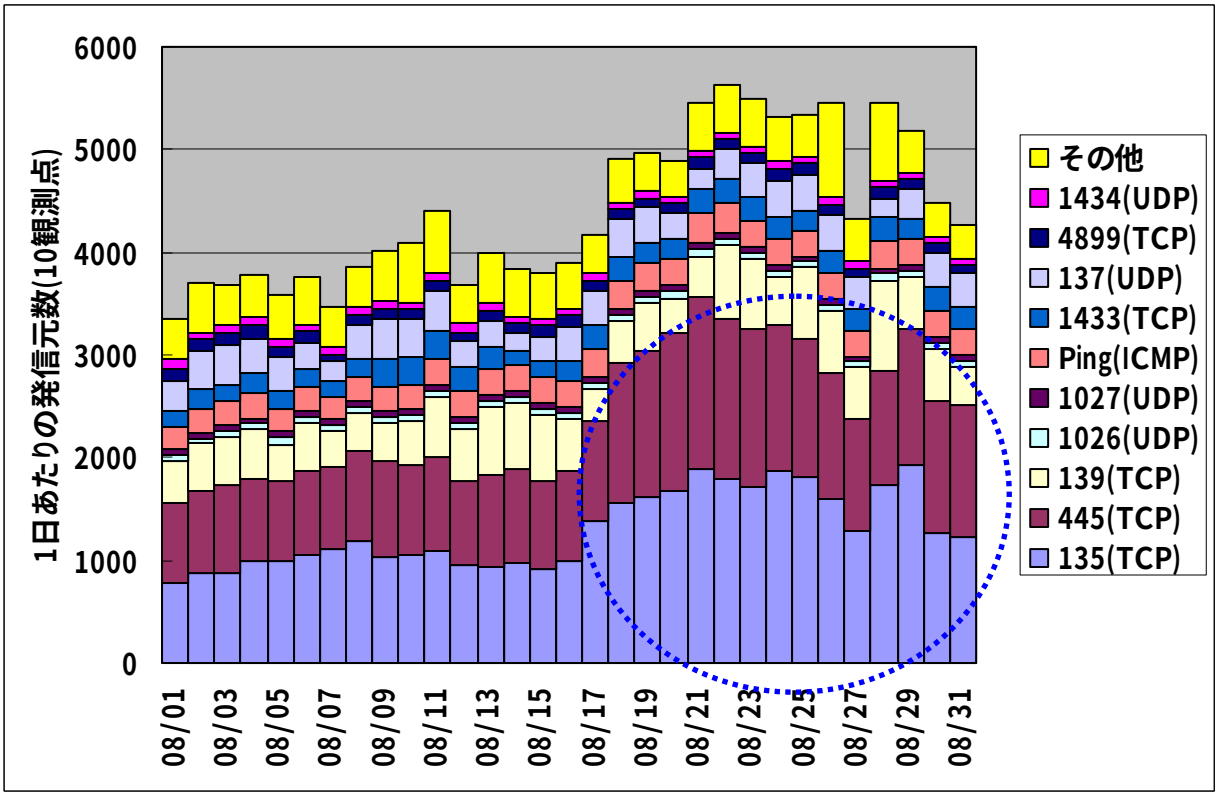
今回のプレスリリースでは、『**4.2 どこからどんなアクセスが発生しているか**』にも、発信元地域別の宛先(ポート種類)毎のアクセス数比率について情報がありますので、参考にして下さい。

図 2.4.1～図 2.4.4 には、2005 年 4 月～8 月の、アクセス数が多いアクセスについて着目し、それらの発信元地域別変化について示しています。

2.1 2005 年 8 月の一方的なアクセス状況



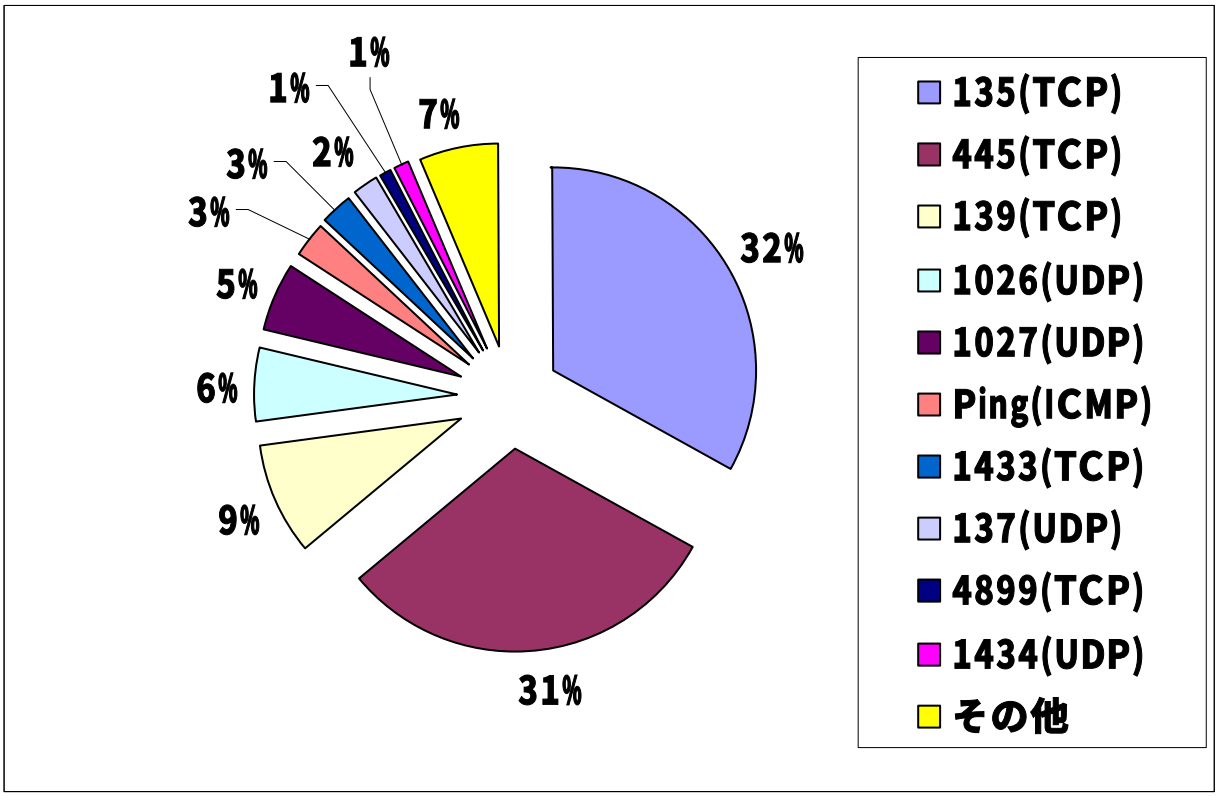
【図 2.1.1 2005 年 8 月の一方的なアクセス状況(アクセス数)】



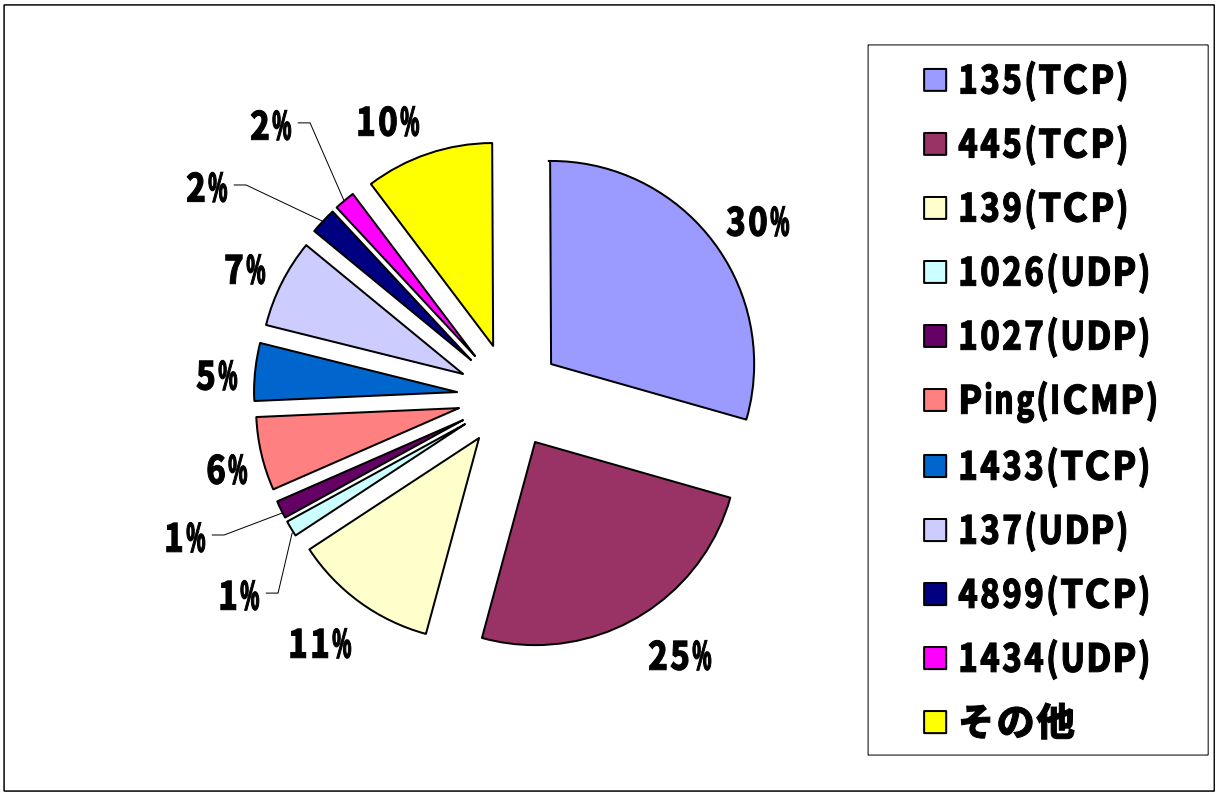
【図 2.1.2 2005 年 8 月の一方的なアクセス状況(発信元数)】

- 2005 年 8 月は図 2.1.1 や図 2.1.2 を見ても分かるとおり、445(TCP)へのアクセスが月の後半から増加傾向にあることでした(図中の赤丸部分)。あわせて、135(TCP)および 445(TCP)へのアクセスの発信元数も同じように増加傾向でした(図中の青丸部分)。

2.2 2005 年 8 月の宛先(ポート種類)別の比率

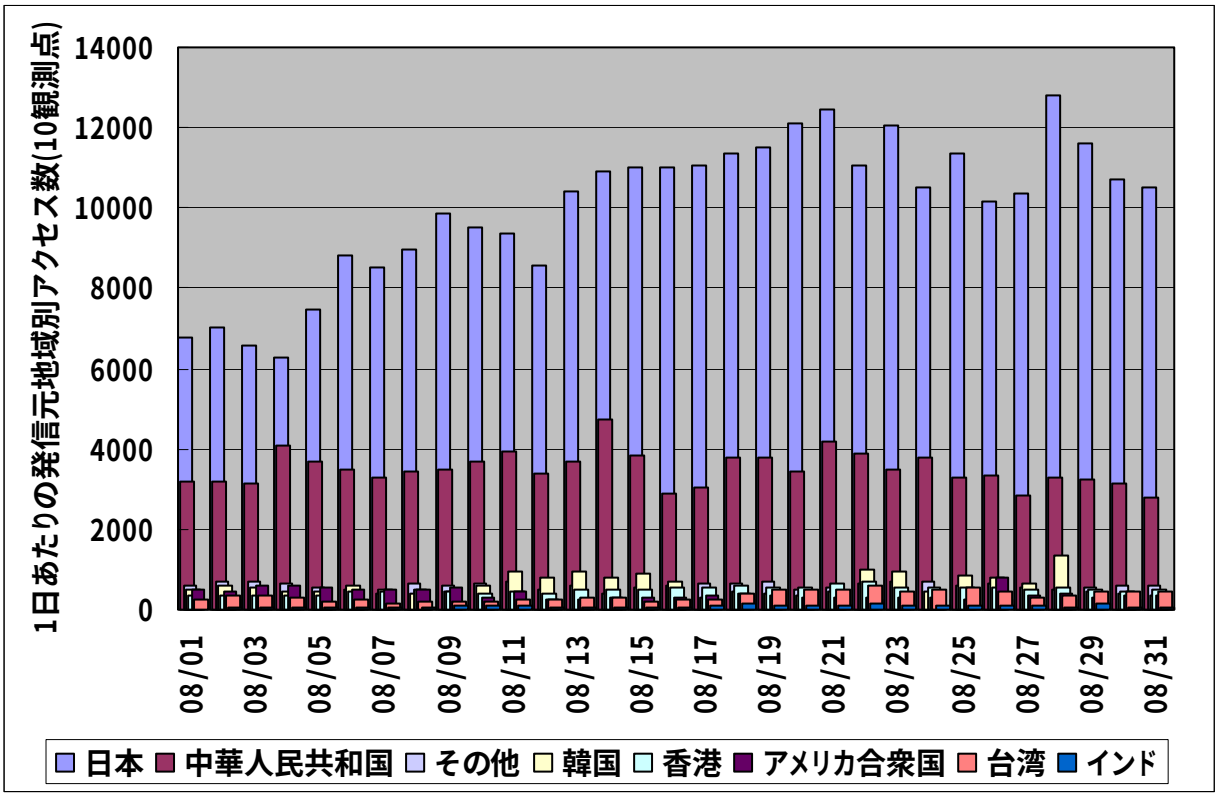


【図 2.2.1 2005 年 8 月の宛先(ポート種類)別アクセス数の比率】

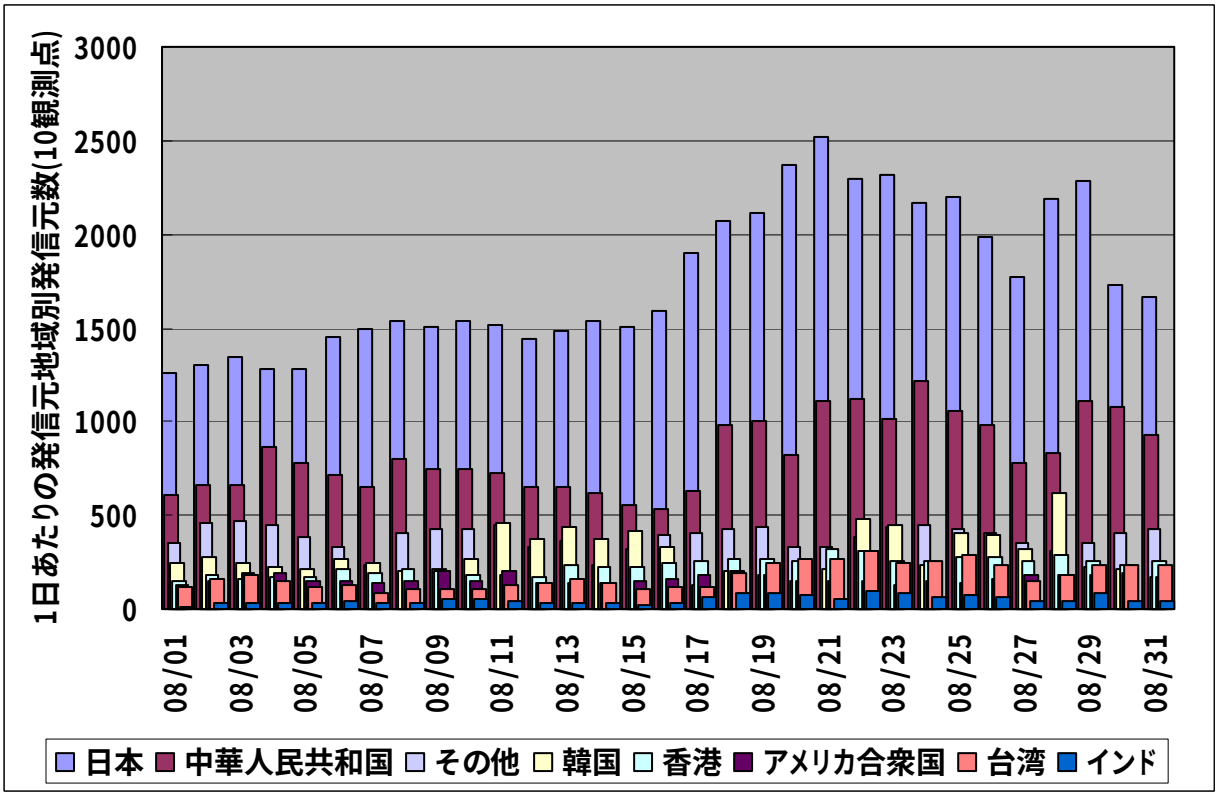


【図 2.2.2 2005 年 8 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 8 月の発信元地域別アクセス状況



【図 2.3.1 2005 年 8 月の発信元地域別アクセス数の変化】



【図 2.3.2 2005 年 8 月の発信元地域別発信元数の変化】

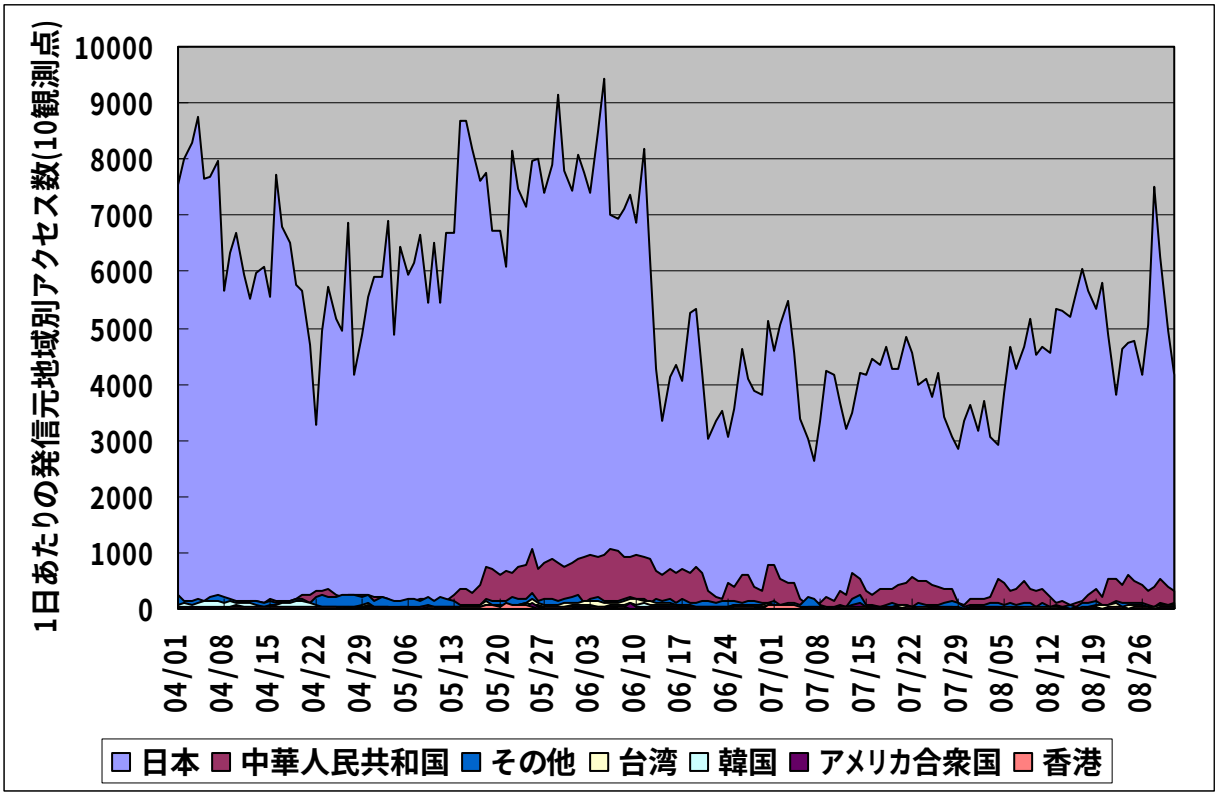
- 2.1 のアクセス状況にも示しましたが、135(TCP)へのアクセス増加は、ほぼ国内からのアクセス増加が原因のようです。また、445(TCP)へのアクセス増加は、国内および中国方面からのアクセス増加が原因のようです。

2.4 4月～8月のアクセスの発信元地域別変化について

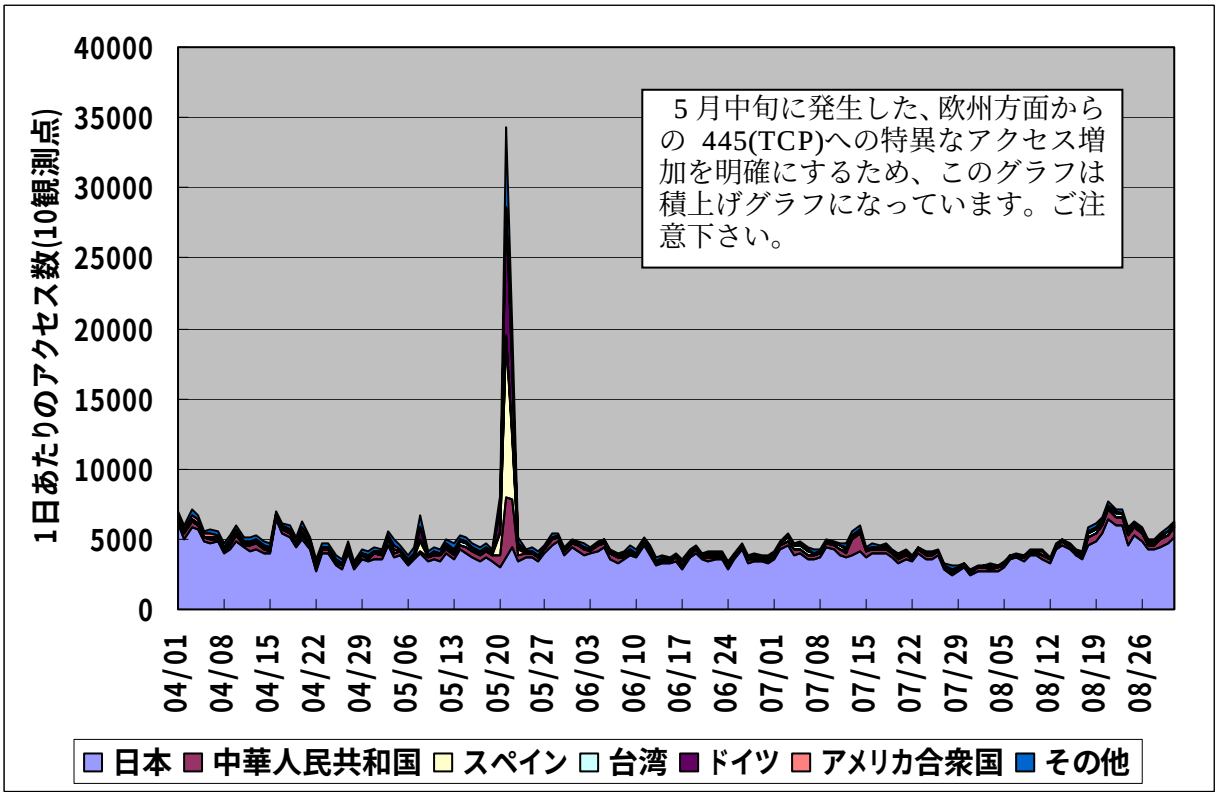
2005年4月～8月の、アクセス数が多いアクセスについて着目し、それらの発信元地域別変化について以下に示します。

対象となるアクセスは、宛先が135(TCP),445(TCP),139(TCP),1433(TCP)のものです。

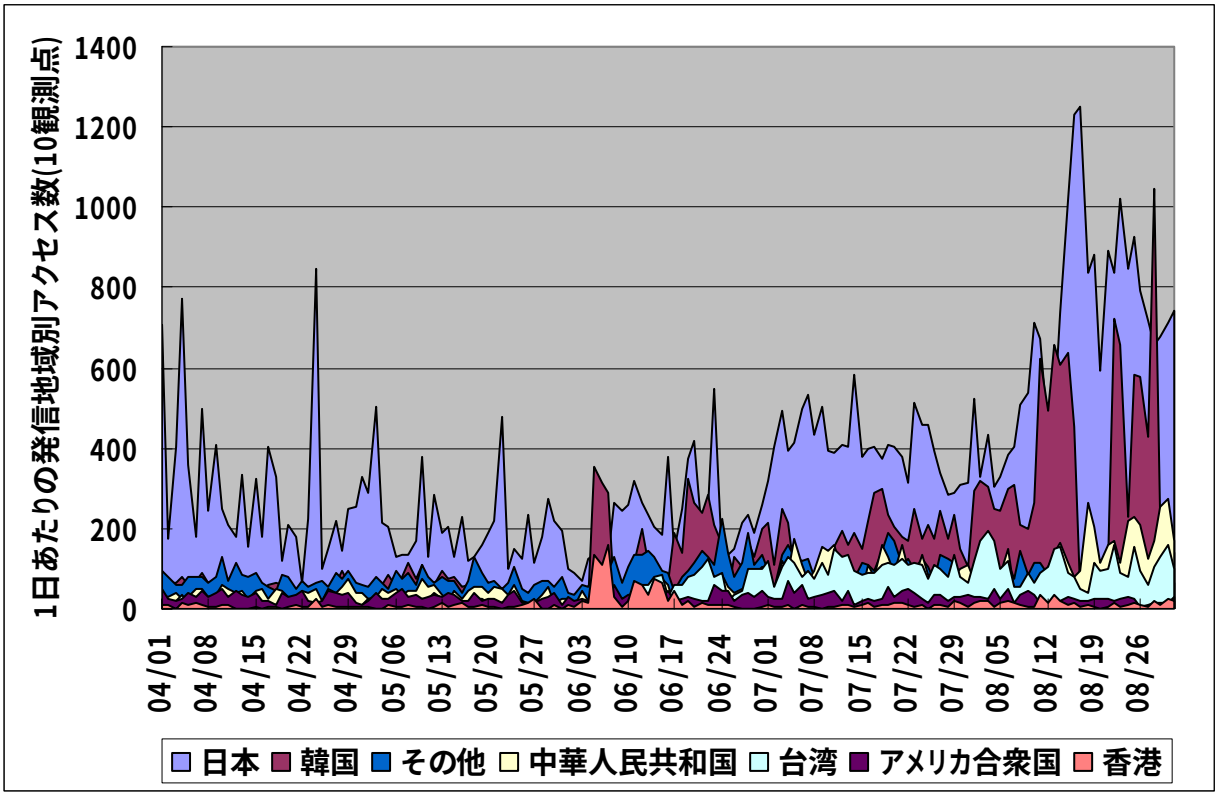
これらのアクセスは、ほとんどがWindows系コンピュータの脆弱性を狙ったアクセスと思われ、ボット系のワームによるものと考えられます。



【図 2.4.1 135(TCP)ポートへの発信元地域別アクセス数の変化】

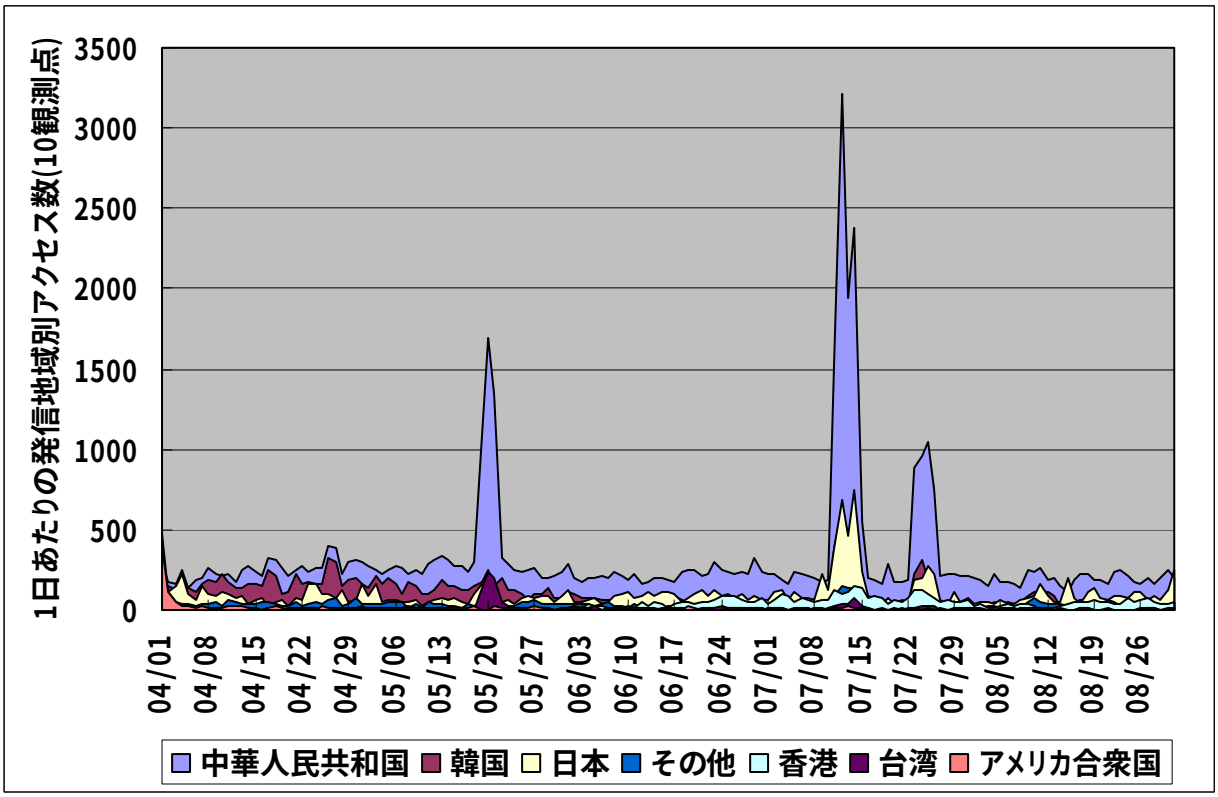


【図 2.4.2 445(TCP)ポートへの発信元地域別アクセス数の変化】



【図 2.4.3 139(TCP)ポートへの発信元地域別アクセス数の変化】

- 2005 年 6 月 5 日頃から、韓国、香港、台湾方面からの 139(TCP)ポートへのアクセスが増加していますが、この傾向は 8 月も継続しています。

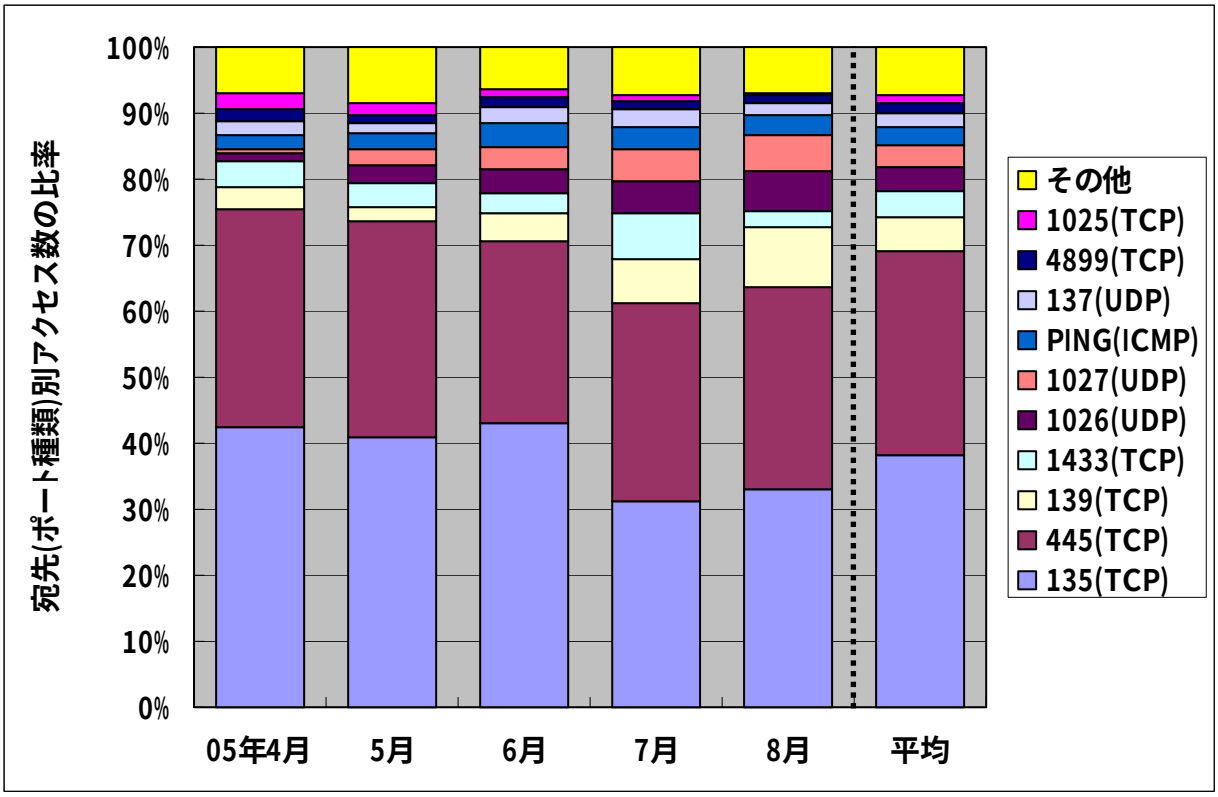


【図 2.4.4 1433(TCP)ポートへの発信元地域別アクセス数の変化】

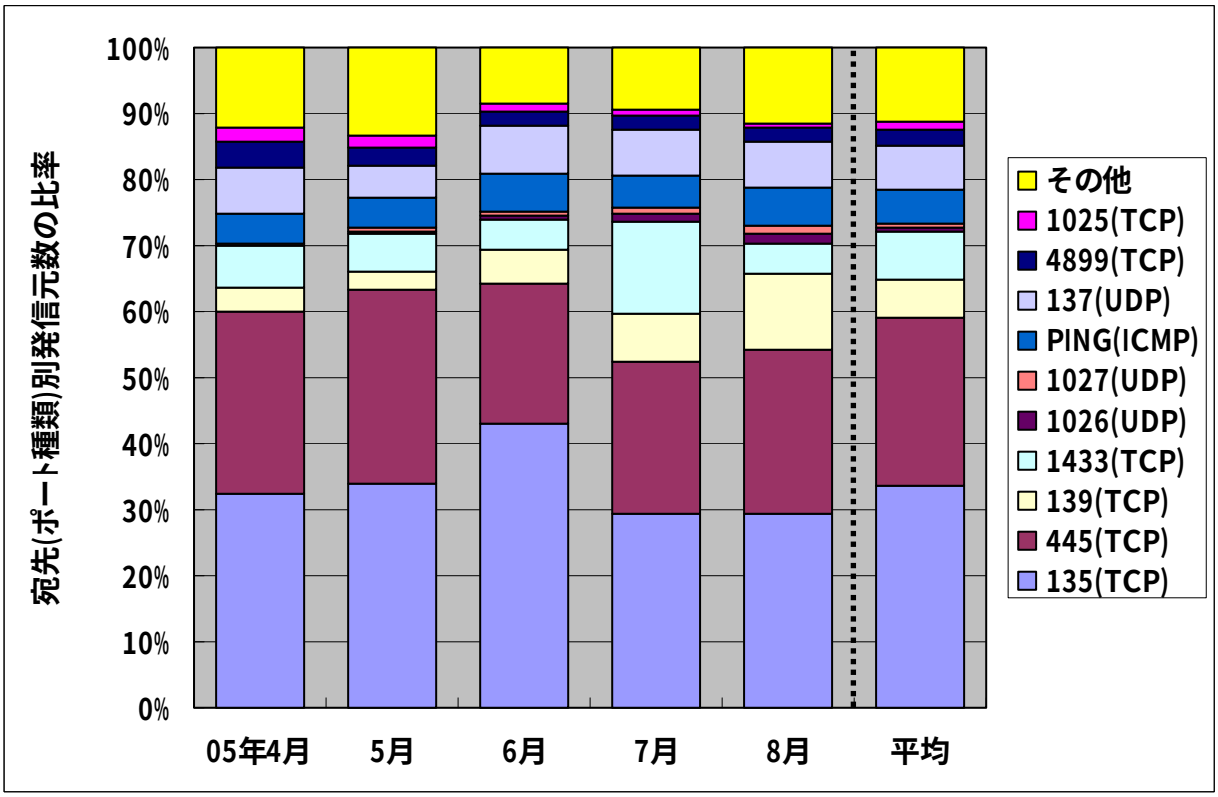
- 1433(TCP)へのアクセスについては、8 月は安定(定常化)していました。

3．統計情報

3.1 2005 年 4 月～8 月の宛先(ポート種類)別の比率

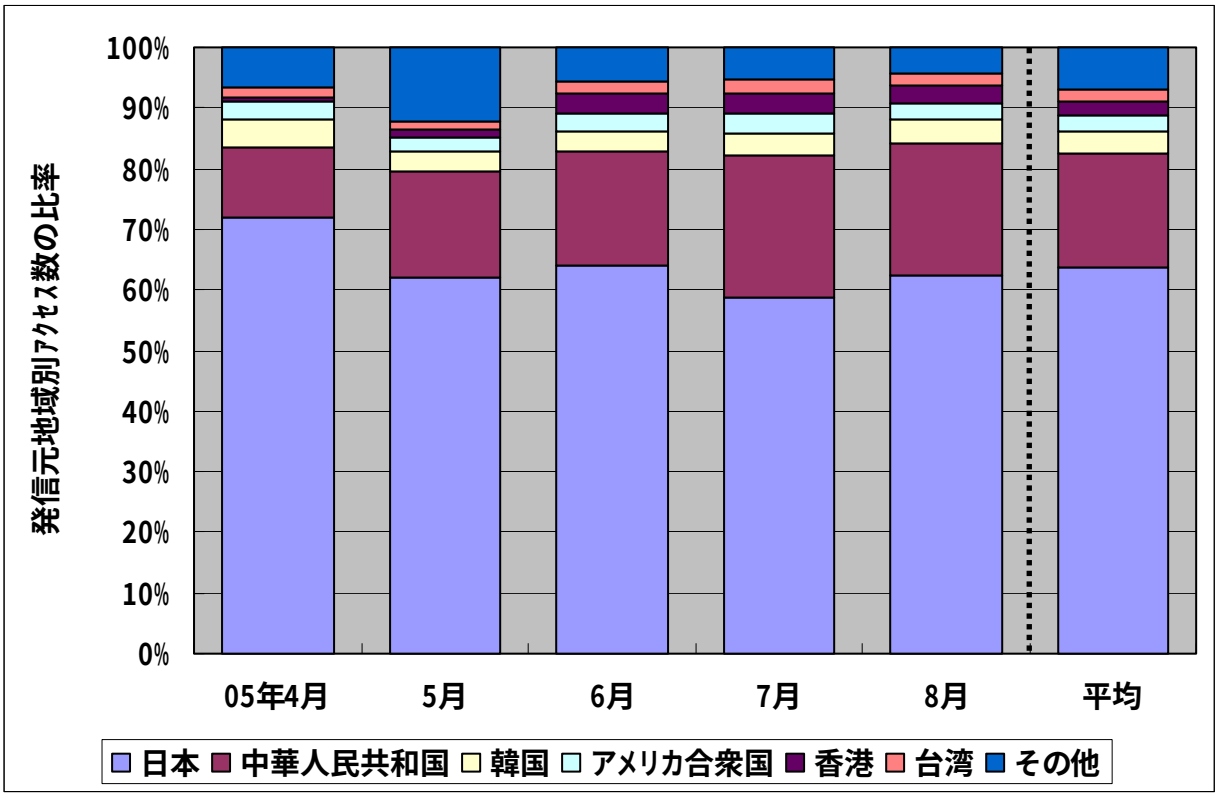


【図 3.1.1 2005 年 4 月～8 月の宛先(ポート種類)別アクセス数の比率】

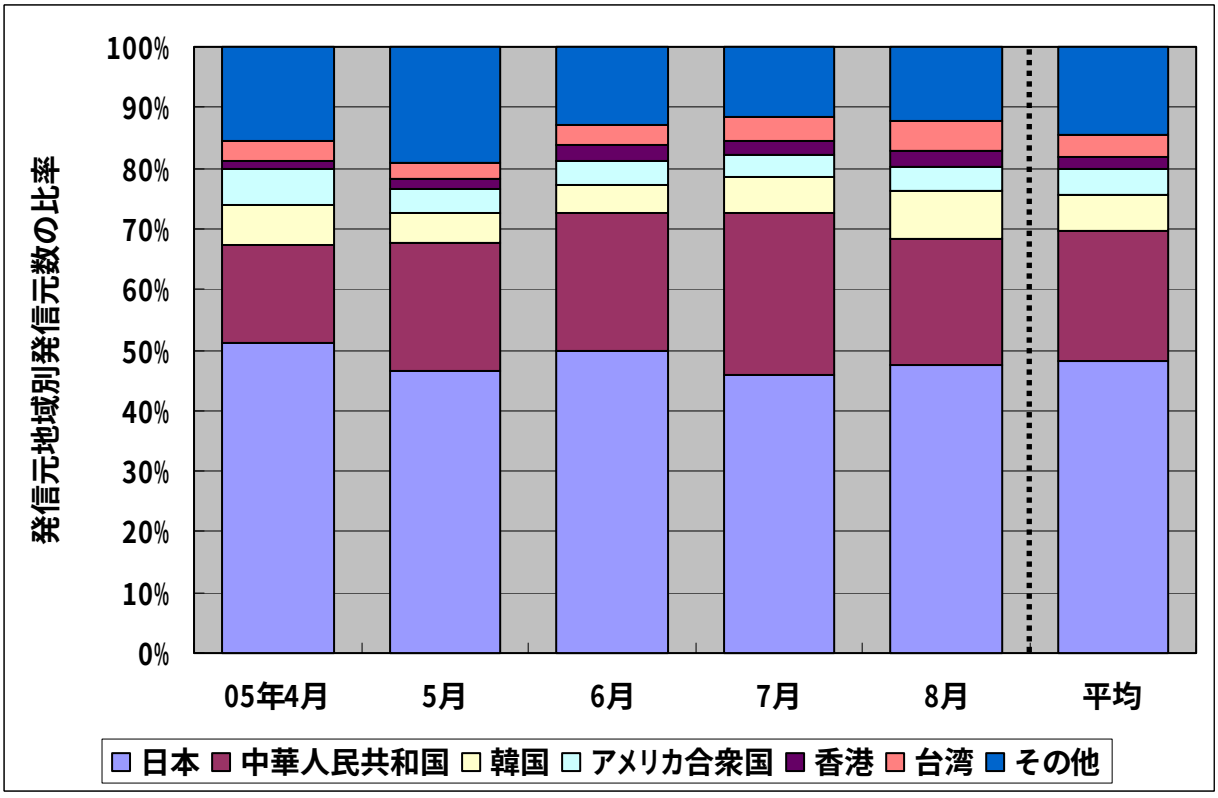


【図 3.1.2 2005 年 4 月～8 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 4 月～8 月の発信元地域別の比率



【図 3.2.1 2005 年 4 月～8 月の発信元地域別アクセス数の比率】

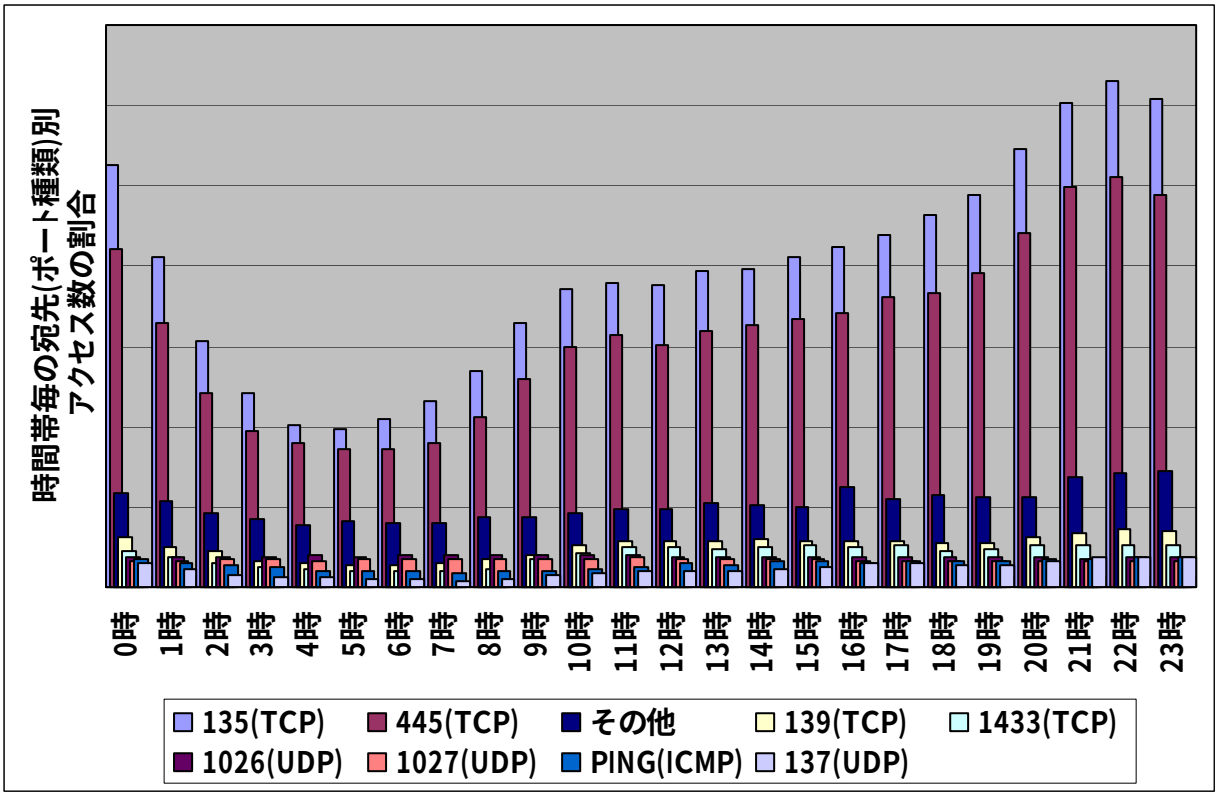


【図 3.2.2 2005 年 4 月～8 月の発信元地域別発信元数の比率】

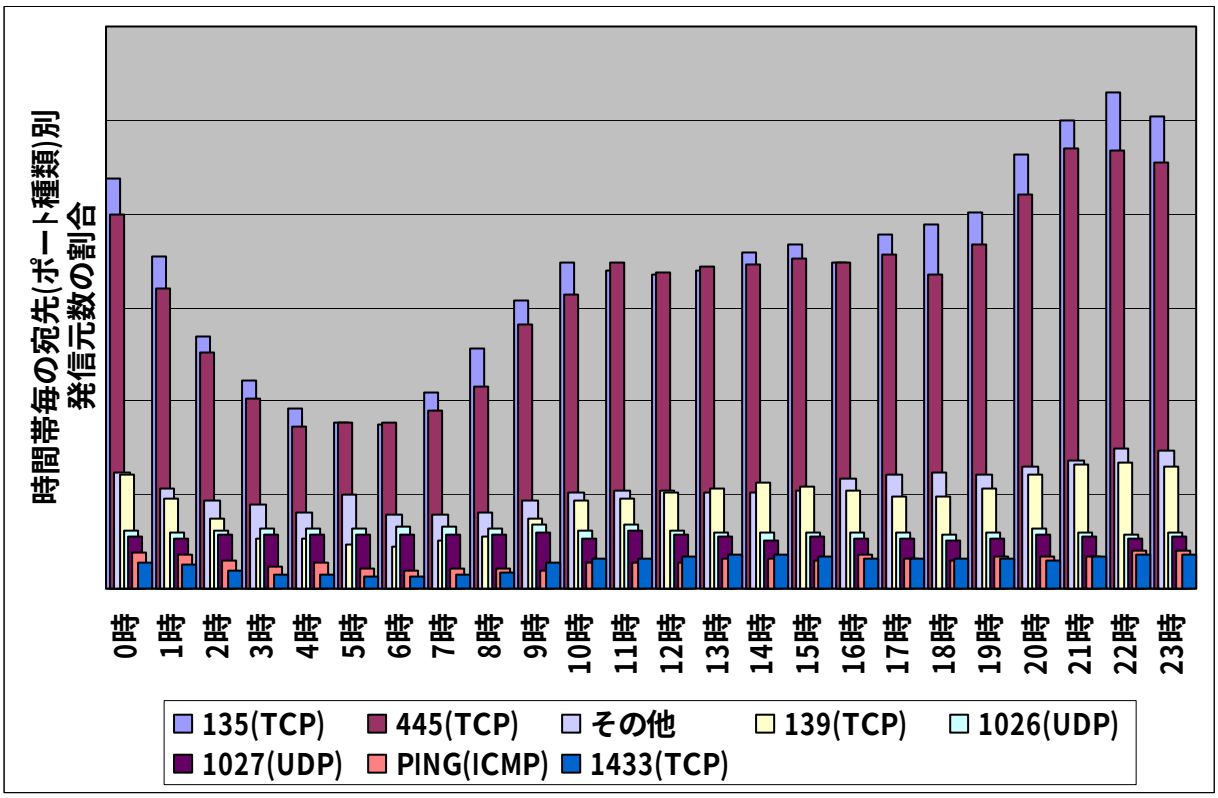
4．その他の統計情報

4.1 2005 年 4 月～8 月の時間帯統計

2005 年 4 月～8 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 8 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 4 月～8 月の宛先(ポート種類)別アクセス数の時間帯統計】

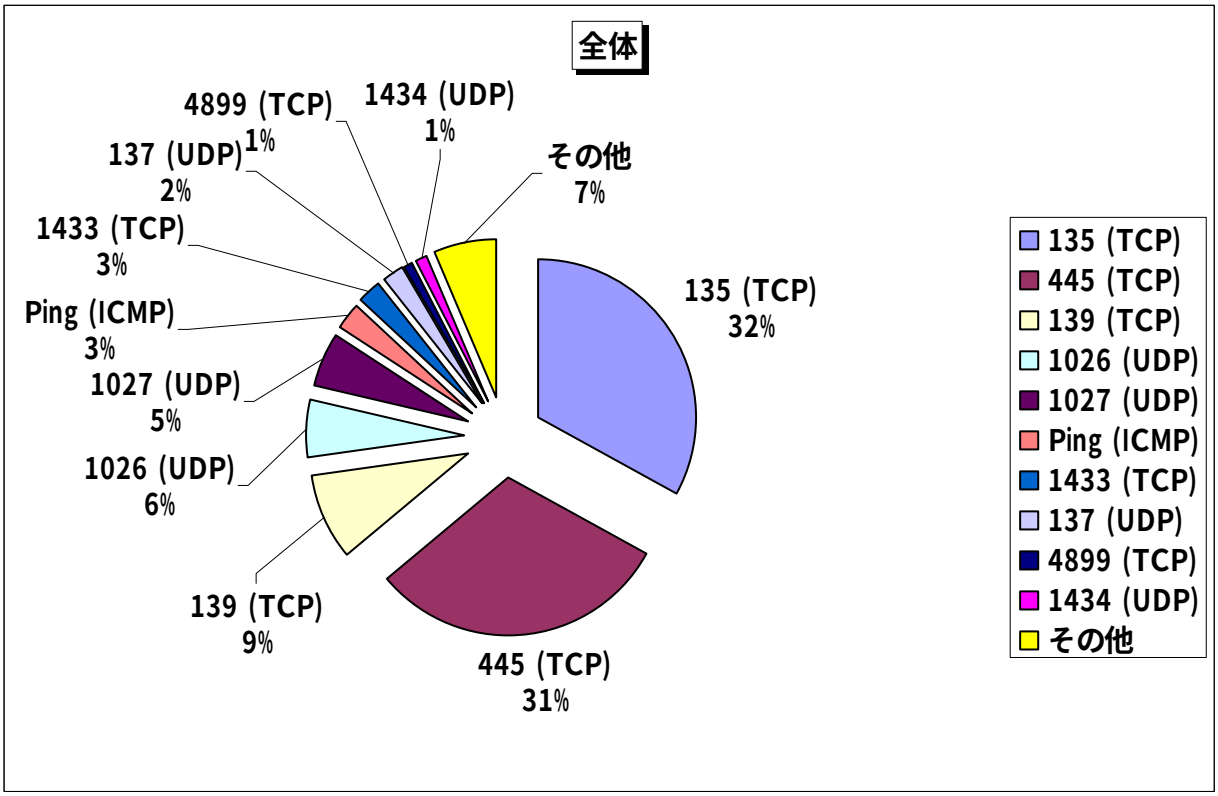


【図 4.1.2 2005 年 8 月の宛先(ポート種類)別アクセス数の時間帯統計】

4.2 どこからどんなアクセスが発生しているか

2005 年 8 月の発信元地域別の宛先(ポート種類)毎のアクセス数比率について、図 4.2.1 から図 4.2.11 に示します。特定の発信元地域毎の、アクセスの宛先（ポート種類）の違いが分かります。図 4.2.2 から図 4.2.11 に示すグラフはすべて、図 4.2.1 の全体グラフで示す宛先(ポート種類)順に表示しているため、発信元地域によっては、アクセス数が 0 の宛先（ポート種類）もあります。これらの宛先（ポート種類）については、図中の宛先（ポート種類）に×をつけてありますので、ご注意下さい。

これらのグラフに表された、アクセスの宛先(ポート種類)が、それぞれの発信元地域での状況を示しているかどうかは明確ではありませんが、発信元地域からの違いを見ると、特定の宛先へのアクセス数が多いなど特徴的なものも多く、地域毎のパターンが見受けられます。



【図 4.2.1 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】

以下に、宛先(ポート種類)の意味を記述します。

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

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

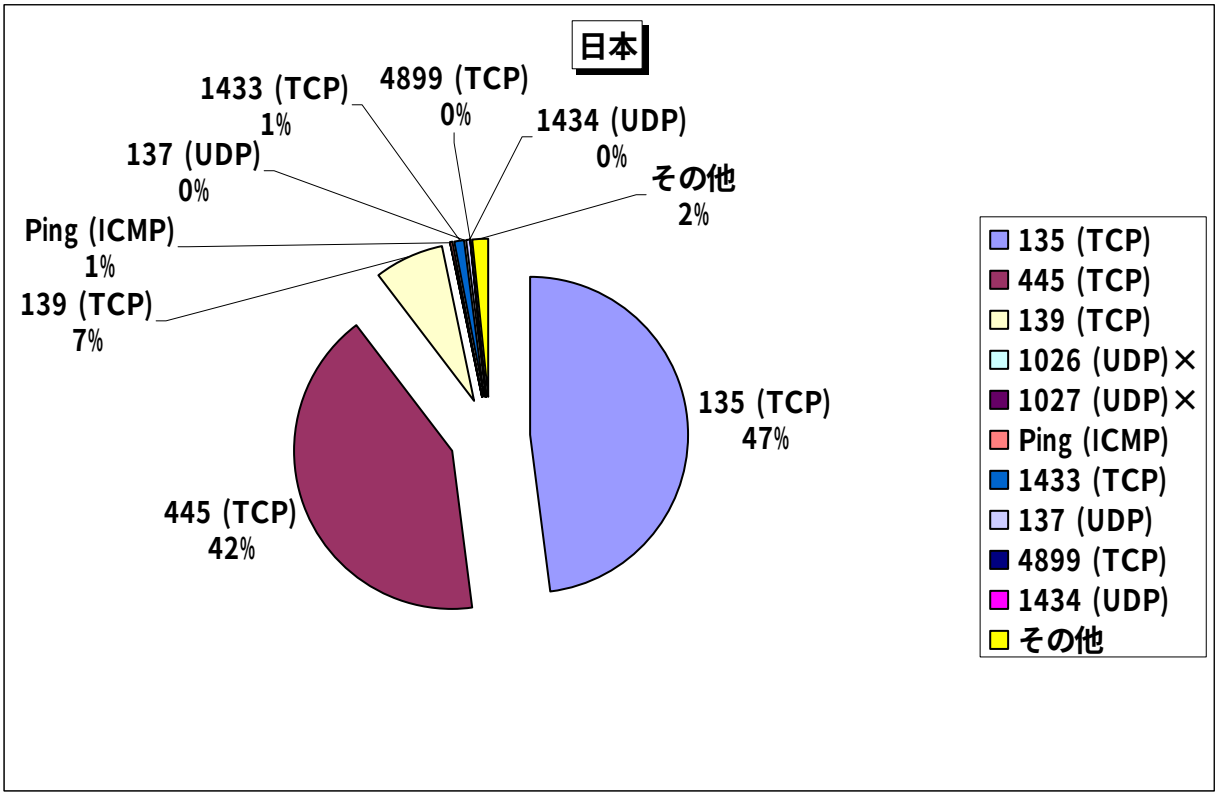
Ping(ICMP)： 相手のコンピュータが動作中か調べる目的で使用されるが、不正アクセスの対象コンピュータを探す目的で、W32/Welchia などに利用されたことで有名

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がある

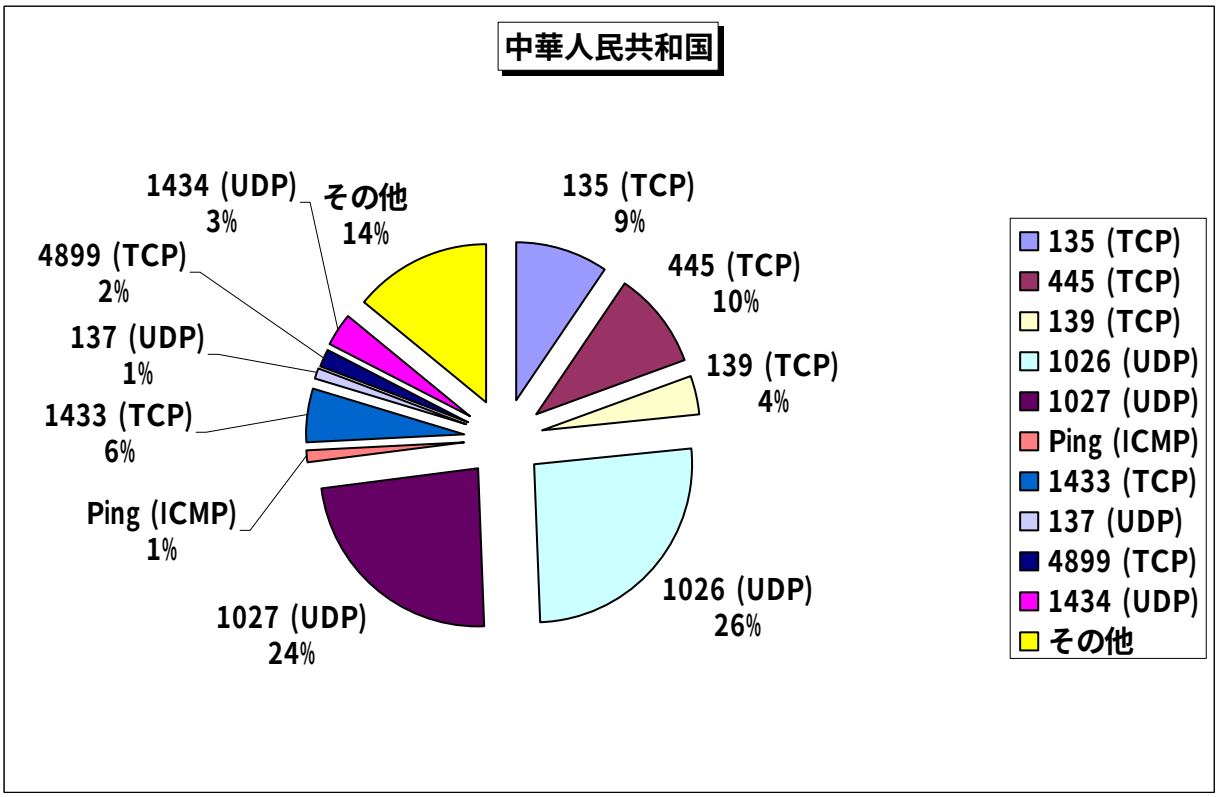
137(UDP)： NETBIOS のポートであり、NETBIOS 経由でのコンピュータへの接続(侵入)などの目的で使用される

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

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)

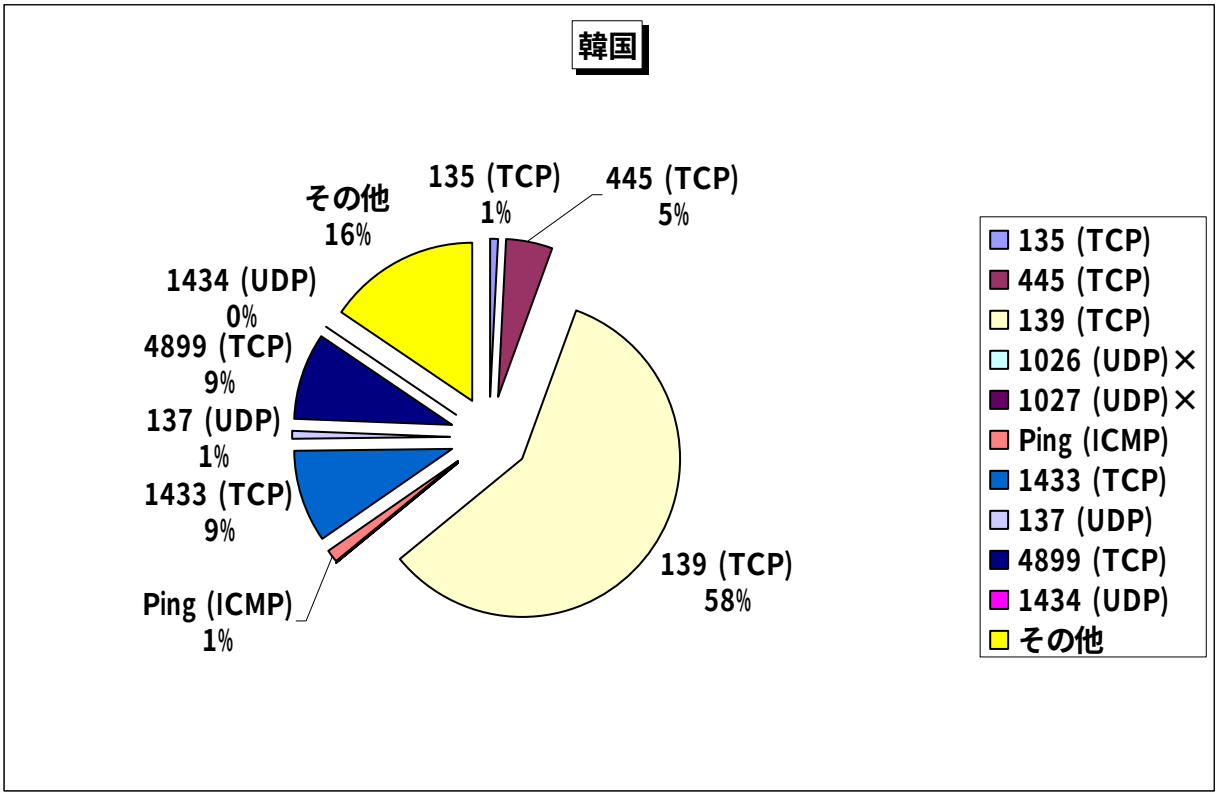


【図 4.2.2 国内からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】

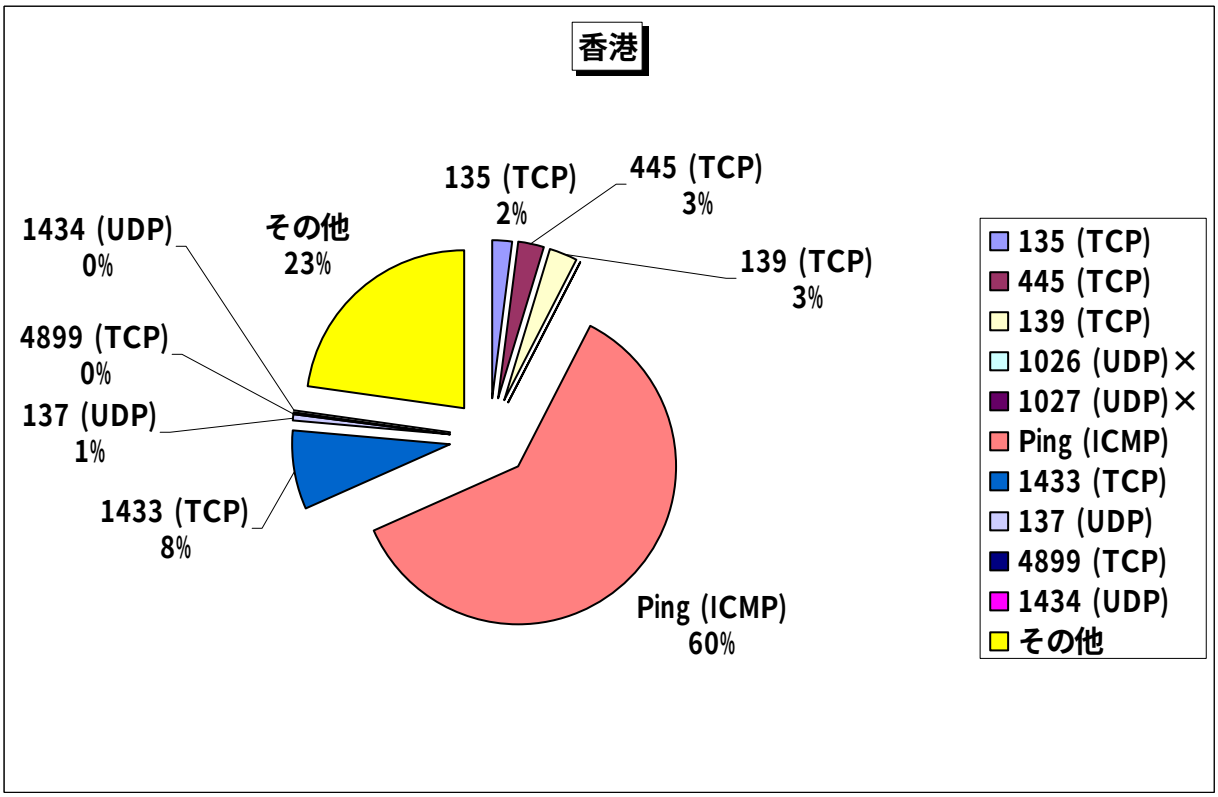


【図 4.2.3 中国方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】

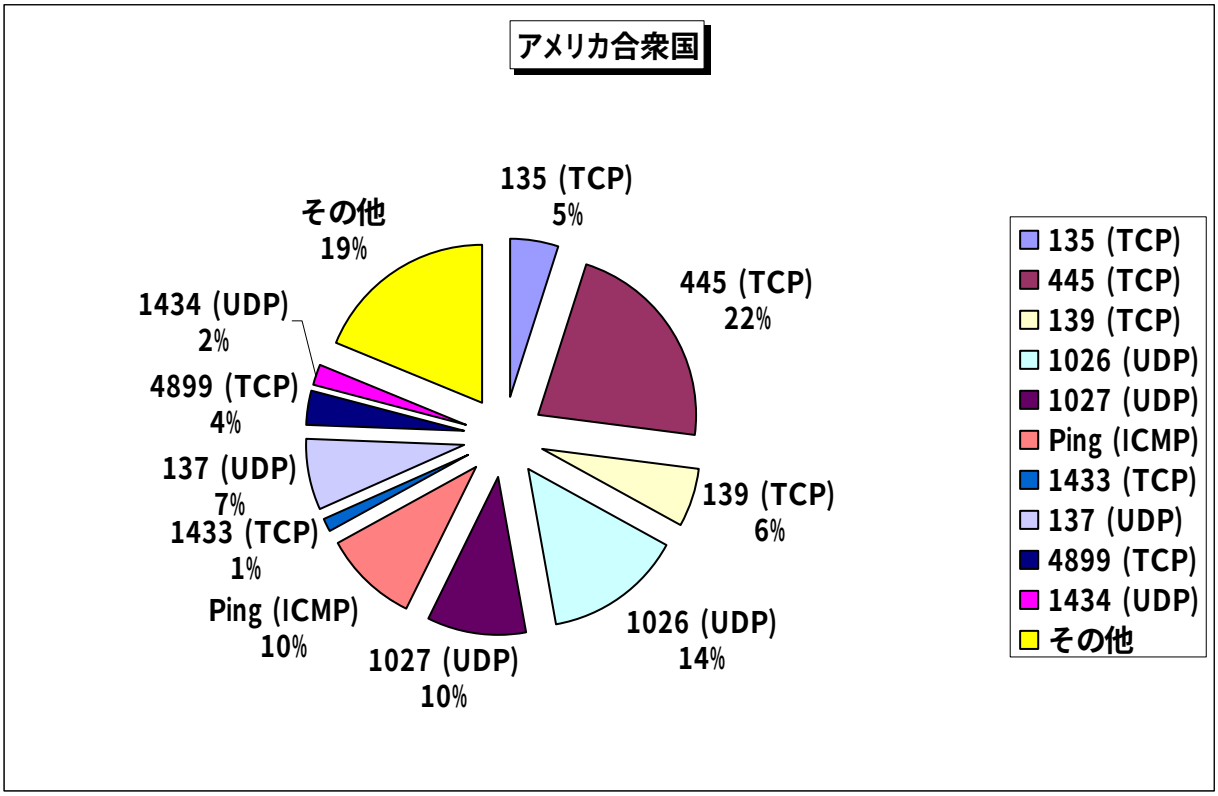
- 中国方面からの 1026(UDP)および 1027(UDP)のアクセスは、発信元数は非常に少なく、特定の発信元が、大量のアクセスを行っています。このアクセスの詳細については、先月のプレスﾘﾘｰｽを参照下さい。
  http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0508.pdf



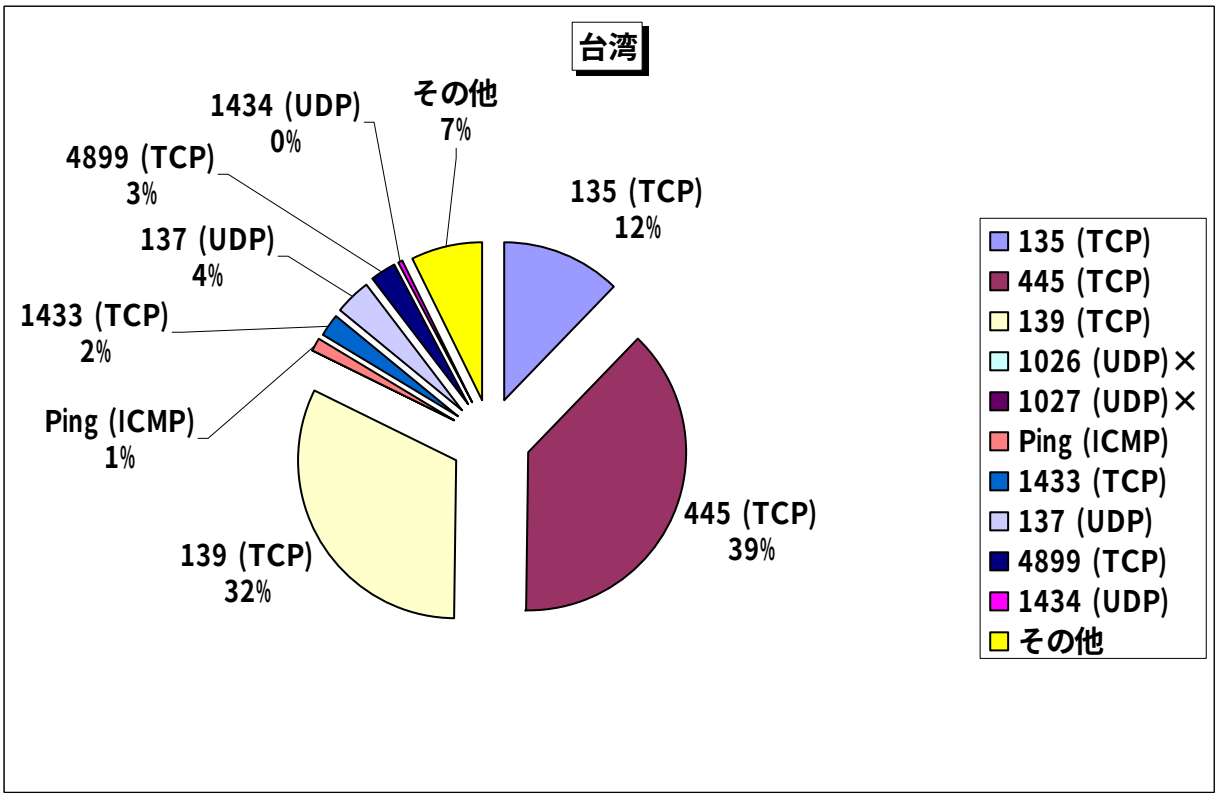
【図 4.2.4 韓国方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



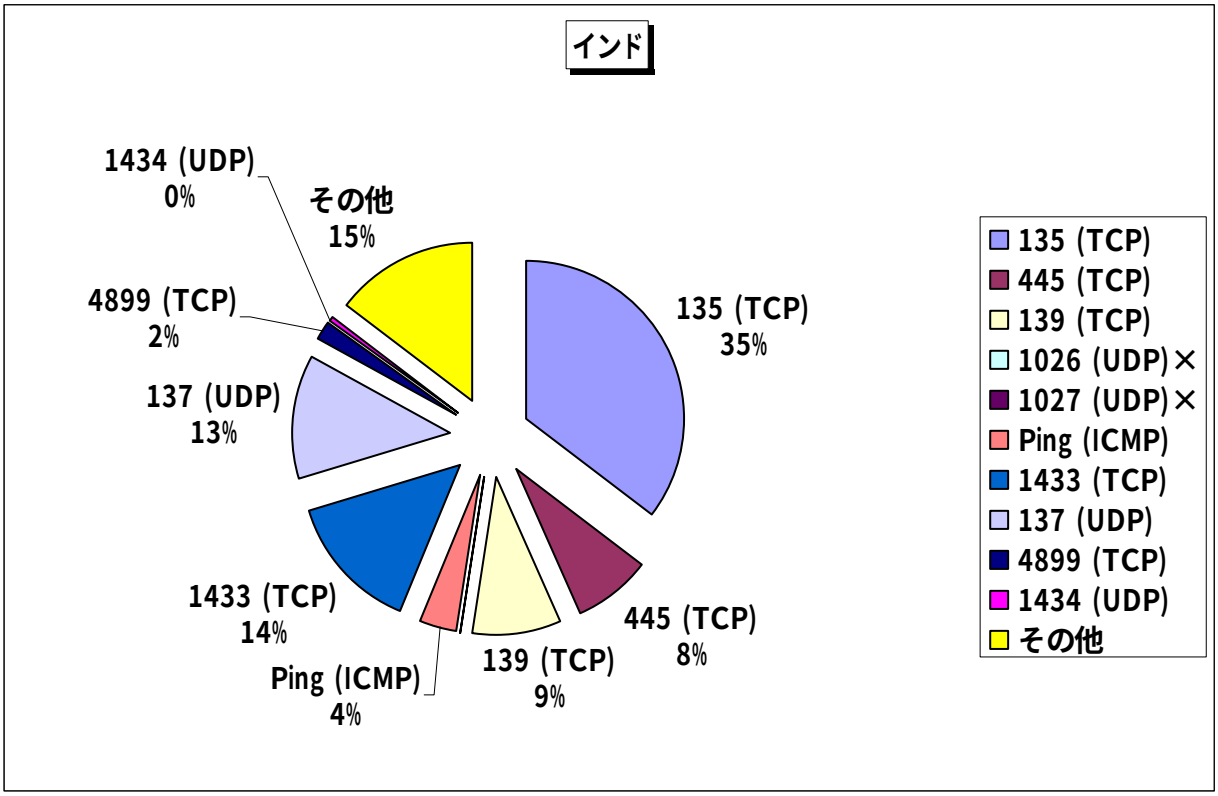
【図 4.2.5 香港方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



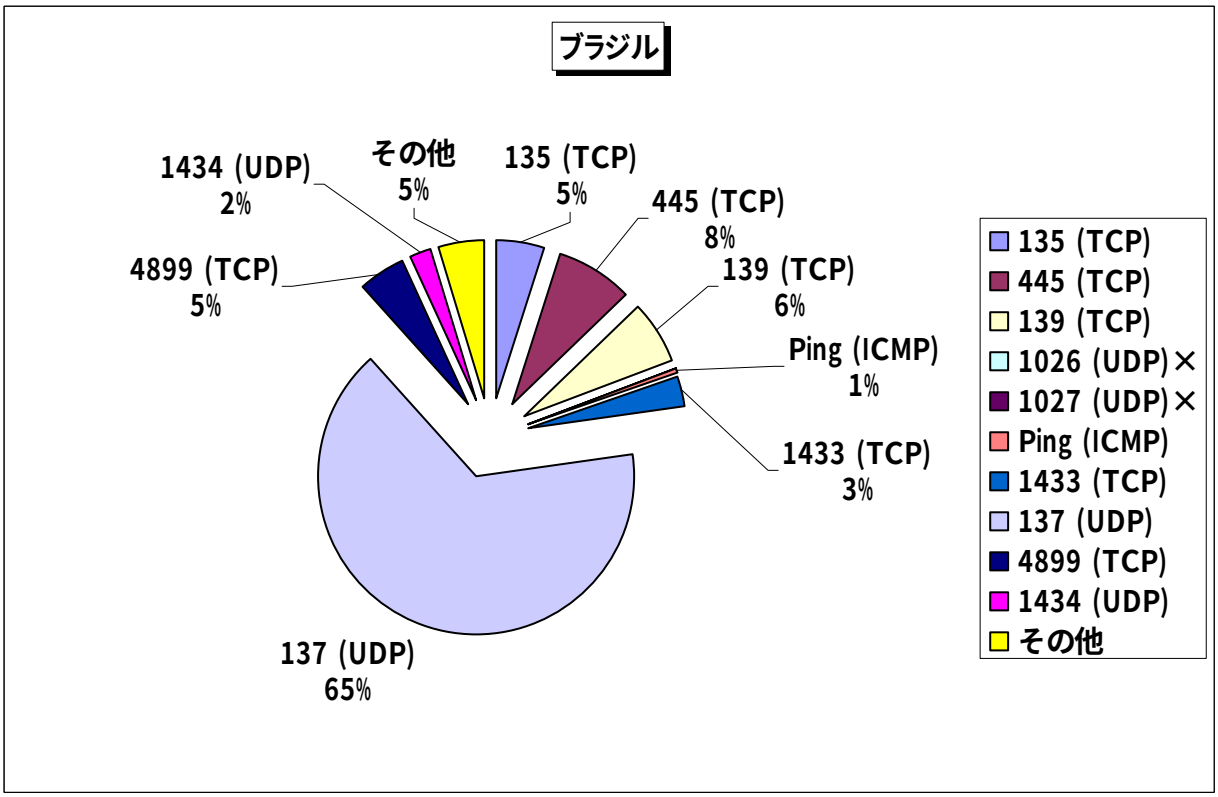
【図 4.2.6 アメリカ方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



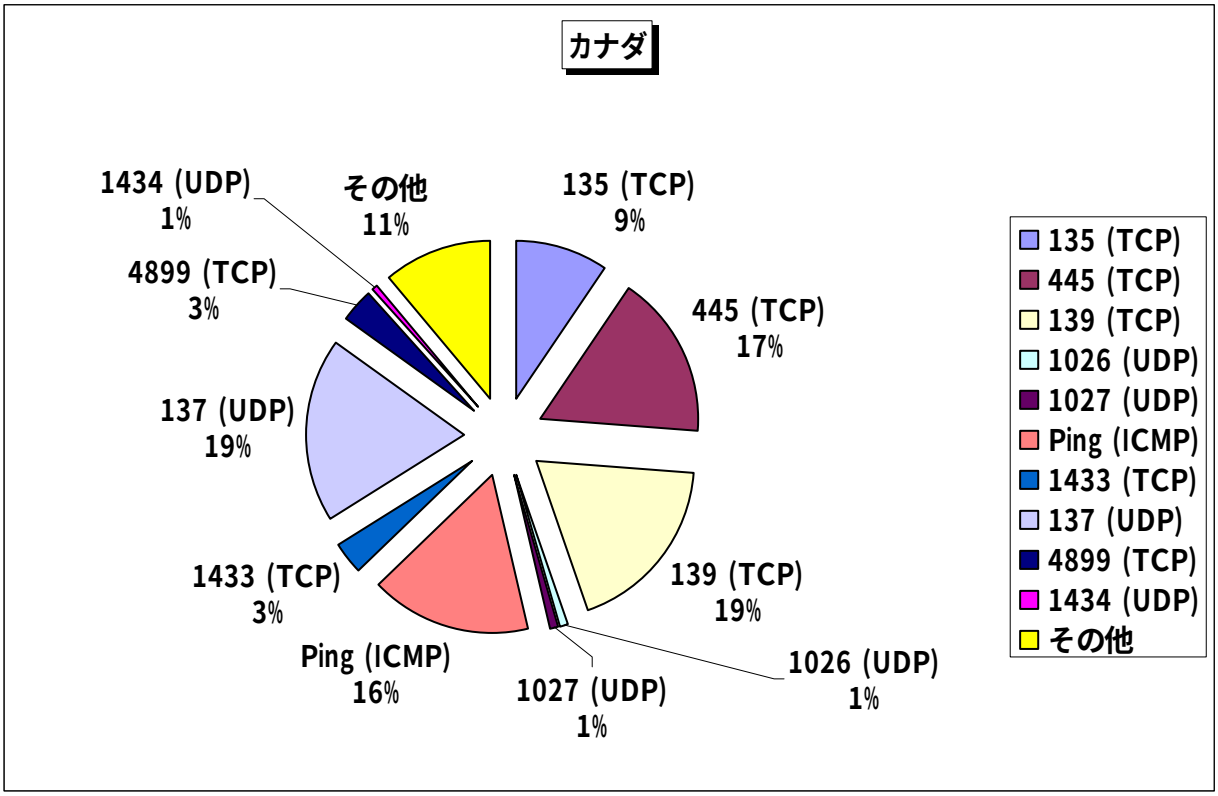
【図 4.2.7 台湾方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



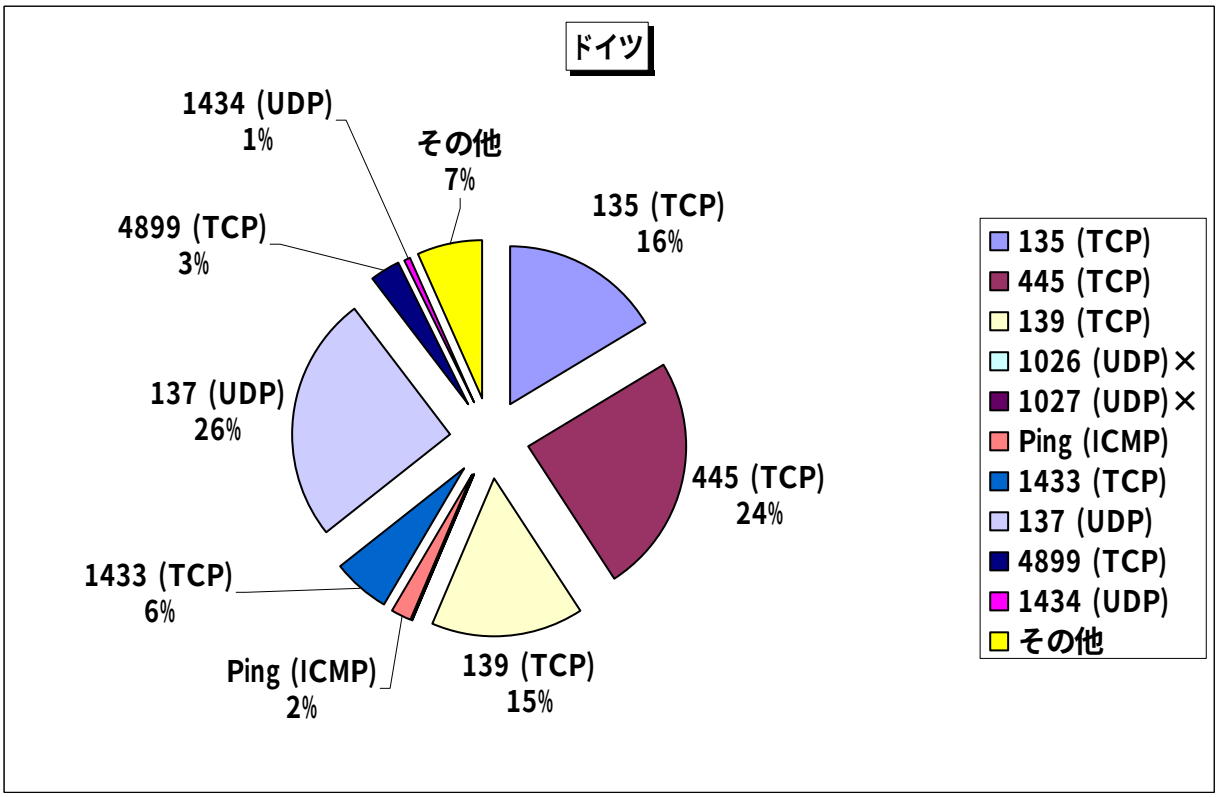
【図 4.2.8 インド方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



【図 4.2.9 ブラジル方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



【図 4.2.10 カナダ方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】



【図 4.2.11 ドイツ方面からの 2005 年 8 月の宛先(ポート種類)毎のアクセス数比率】

■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