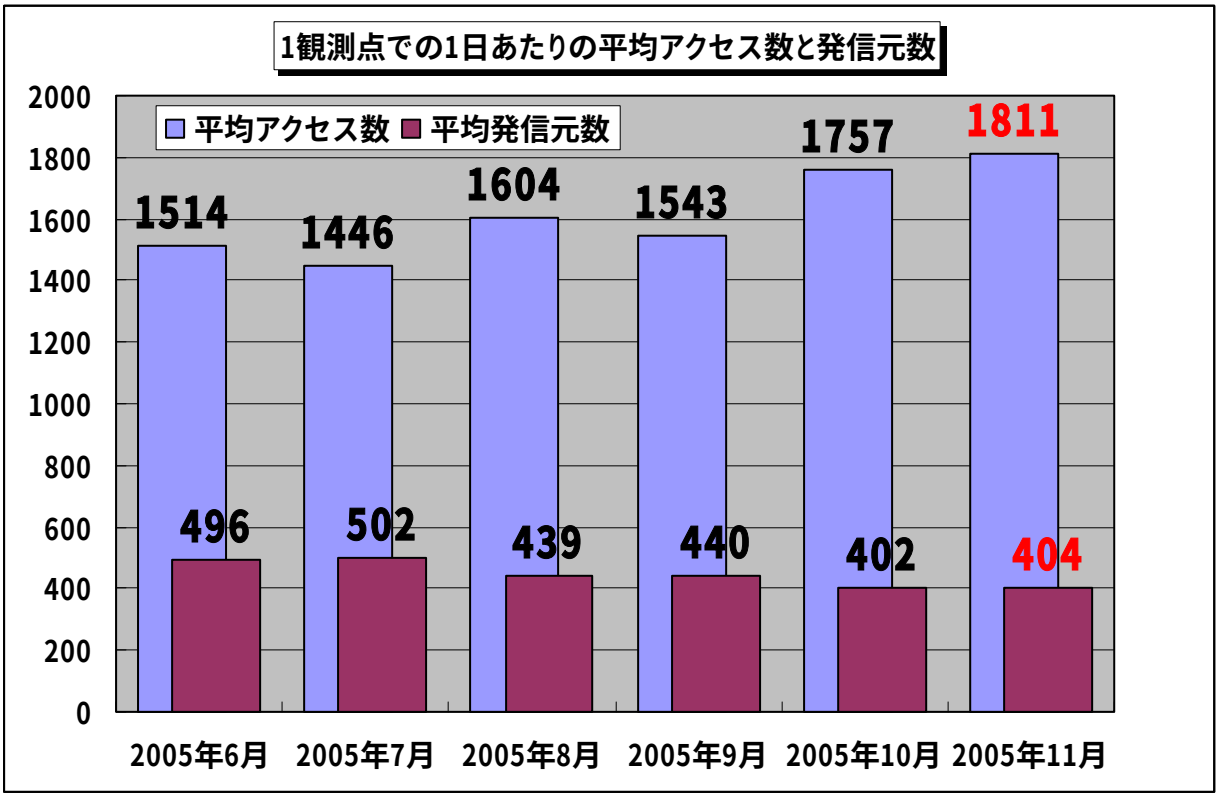
別紙 3

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 11 月の期待しない（一方的な）アクセスの総数は、10 観測点で **543,415 件**ありました。1 観測点で 1 日あたり **404** の発信元から **1,811 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、404 人の見知らぬ人(発信元)から、発信元一人当たり 4～5 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 6 月～11 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、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。10 月以降の増加については、102x(UDP)/103x(UDP)ポートへのアクセス数の増加によるものです。

2．11 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等を有効利用することをお勧めします。

11 月の特徴的なアクセスは 10 月から引き続き発生している 102x(UDP)/103x(UDP)ポートへのアクセスです。11 月のアクセス数と発信元数の関係を図 1 でみると、ここ数ヶ月と比べて、発信元数が減少している割にはアクセス数が多い状況です。この理由として挙げられるのが、これらの 102x(UDP)/103x(UDP)ポートへのアクセスの増加です。

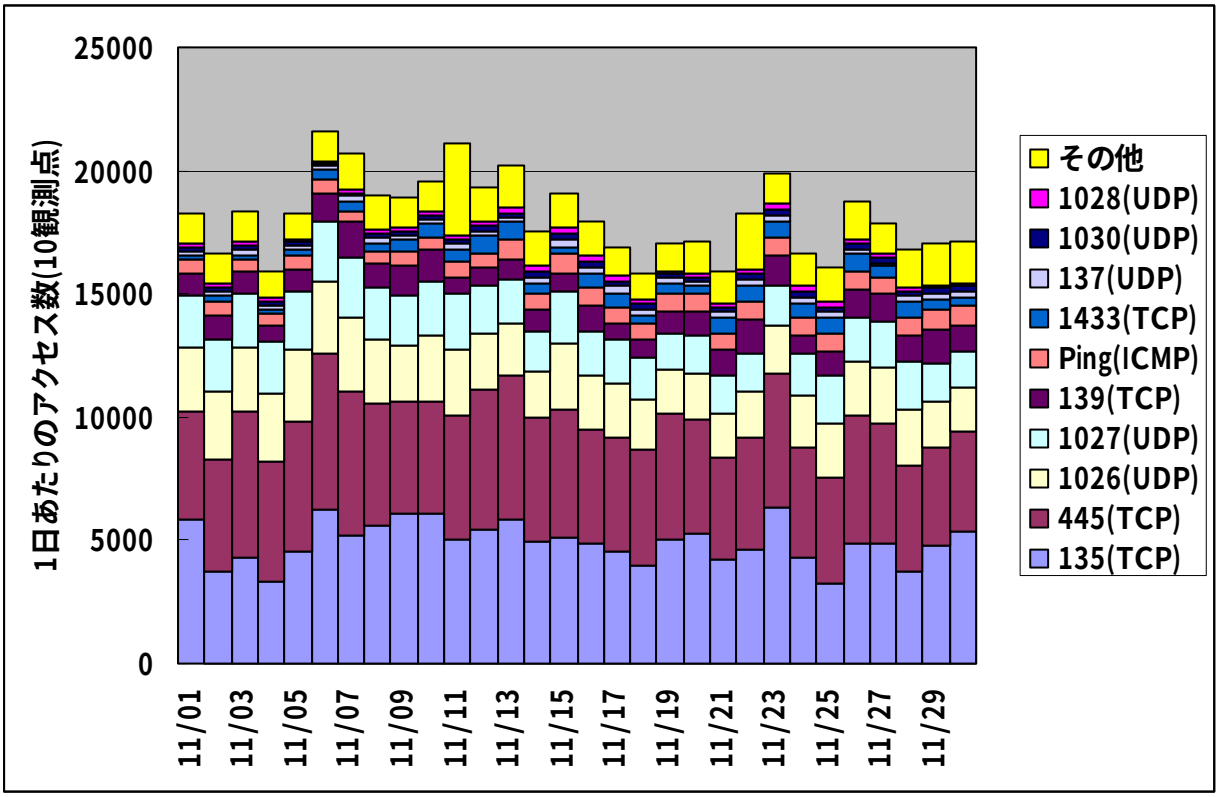
10 月のレポートでは 1026(UDP)/1027(UDP)ポートへのアクセスが、Windows Messenger 機能を利用したポップアップメッセージを送りつけるものと報告しましたが、その後の調査で、他の 102x(UDP)/103x(UDP)ポートへのアクセスも同じ内容であることが分かりました。メッセージが表示されるだけであれば、パソコンを操作する上では邪魔な存在ということで、特に害のあるアクセスではありませんが、『メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043) 』のパッチが適用されていない場合は、リモートからコードが実行される危険性があります。これらのアクセスについては、「**2.4 102x(UDP)/103x(UDP)ポートへのアクセスについて**」に詳細を記述します。

(参考情報)

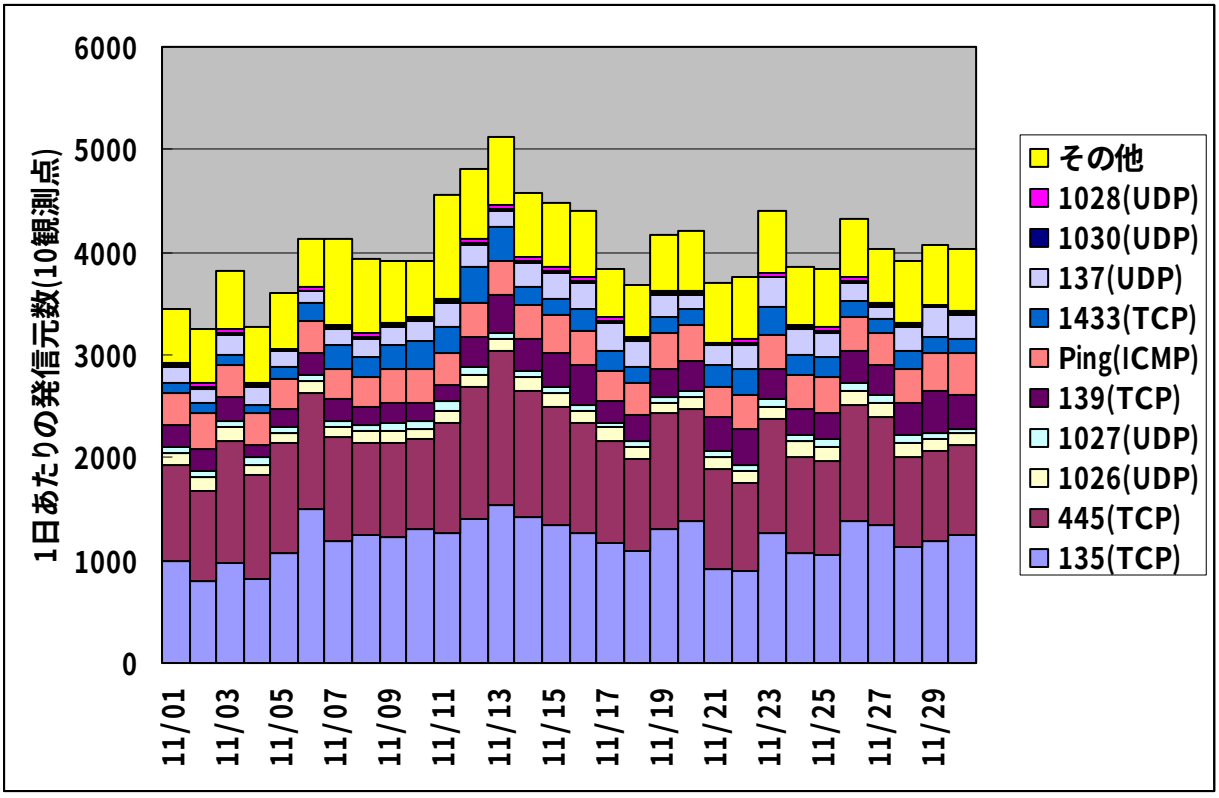
■メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043)

http://www.microsoft.com/japan/technet/security/bulletin/MS03-043.mspx

2.1 2005 年 11 月の一方的なアクセス状況

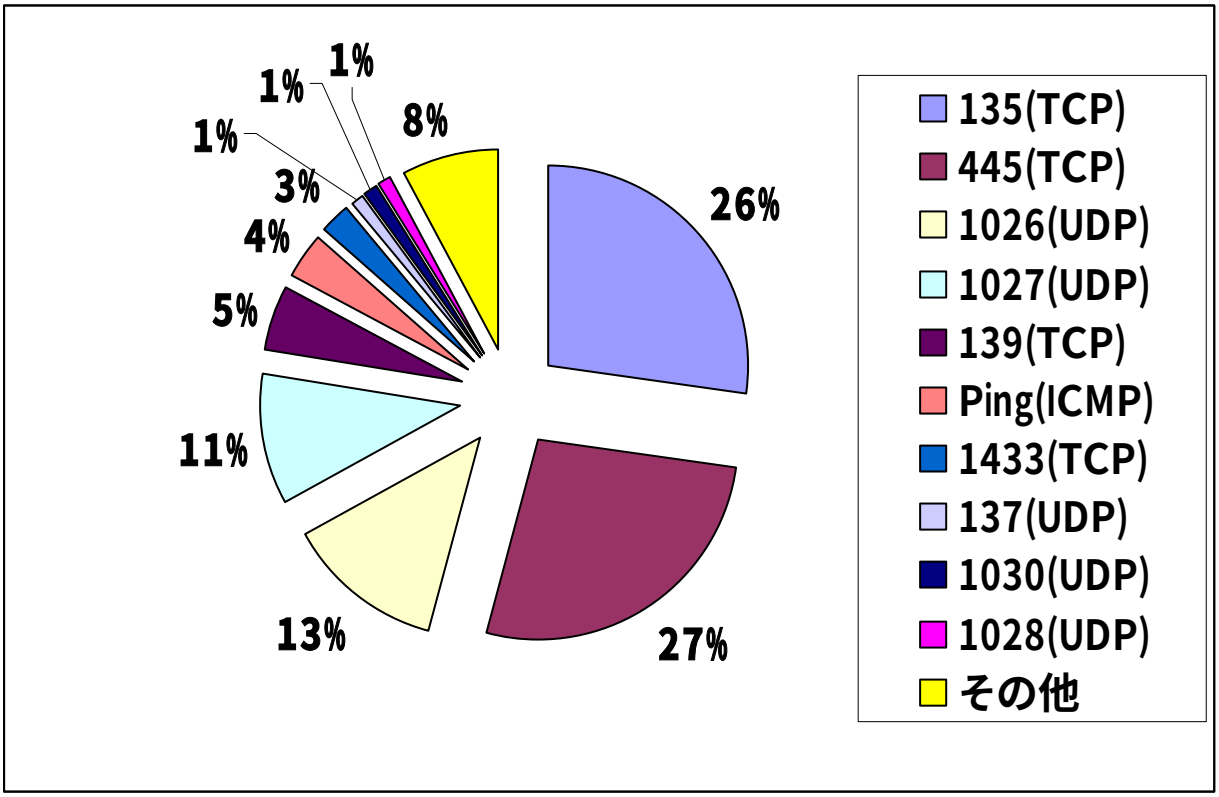


【図 2.1.1 2005 年 11 月の一方的なアクセス状況(アクセス数)】

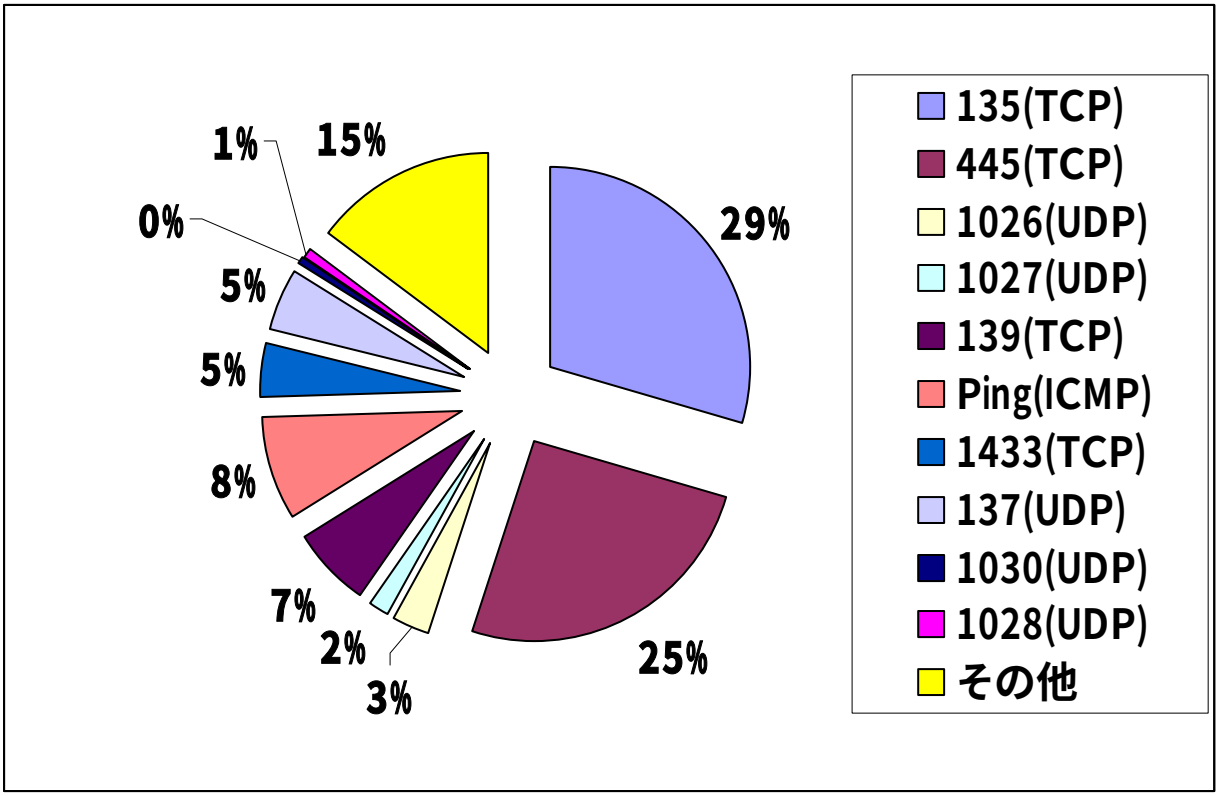


【図 2.1.2 2005 年 11 月の一方的なアクセス状況(発信元数)】

2.2 2005 年 11 月の宛先(ポート種類)別の比率

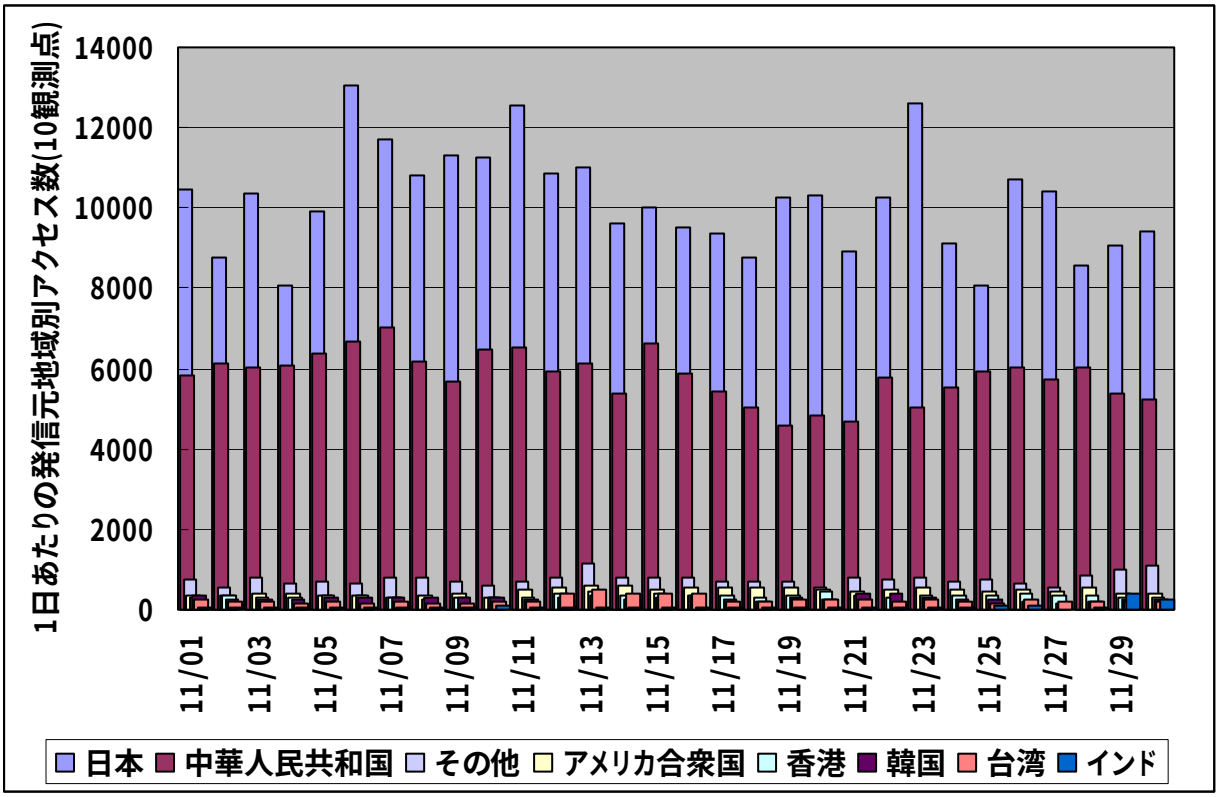


【図 2.2.1 2005 年 11 月の宛先(ポート種類)別アクセス数の比率】

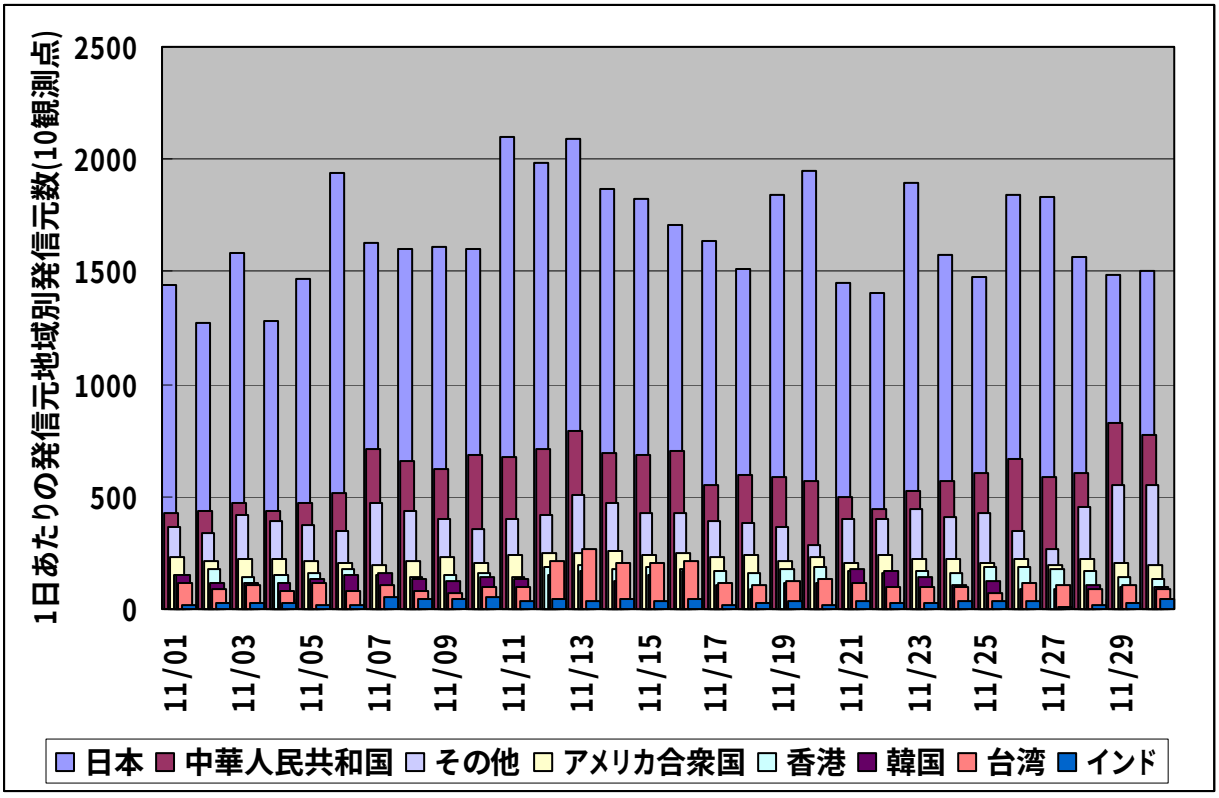


【図 2.2.2 2005 年 11 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 11 月の発信元地域別アクセス状況

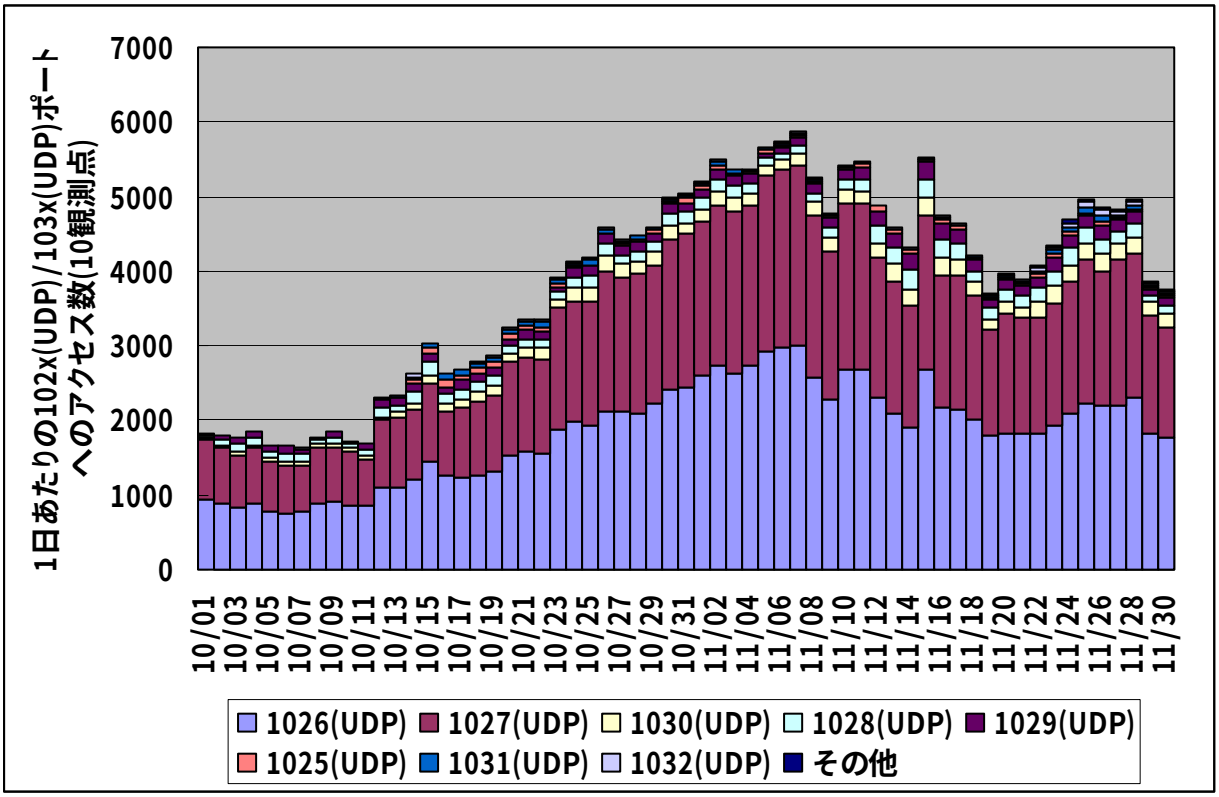


【図 2.3.1 2005 年 11 月の発信元地域別アクセス数の変化】



【図 2.3.2 2005 年 11 月の発信元地域別発信元数の変化】

2.4 102x(UDP)/103x(UDP)ポートへのアクセスについて



【図 2.4.1 102x(UDP)/103x(UDP)ポートへのアクセス状況】

- 102x(UDP)/103x(UDP)ポートへのアクセスが 10 月に入ってから増加傾向を示しています。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。
- これらのアクセスは、102x(UDP)ポートや 103x(UDP)ポート経由で、Windows の Messenger 機能を利用したポップアップメッセージを送りつけるケースであり、以前から定常化していました。TALOT2 の観測では、各観測点へ同一の発信元から送られてくる場合もあり、かなり広い範囲へ一方的に送られていることが分かります。

最近のメッセージ本文例(綴りは原文のままですが、一部伏せ字にしています)

```
Critical Error
The Microsoft Windows system contains invalid registry
entries and your computer will crash. Please download
the Windows registry application from:
www.********.com
To fix your system immediately.
```

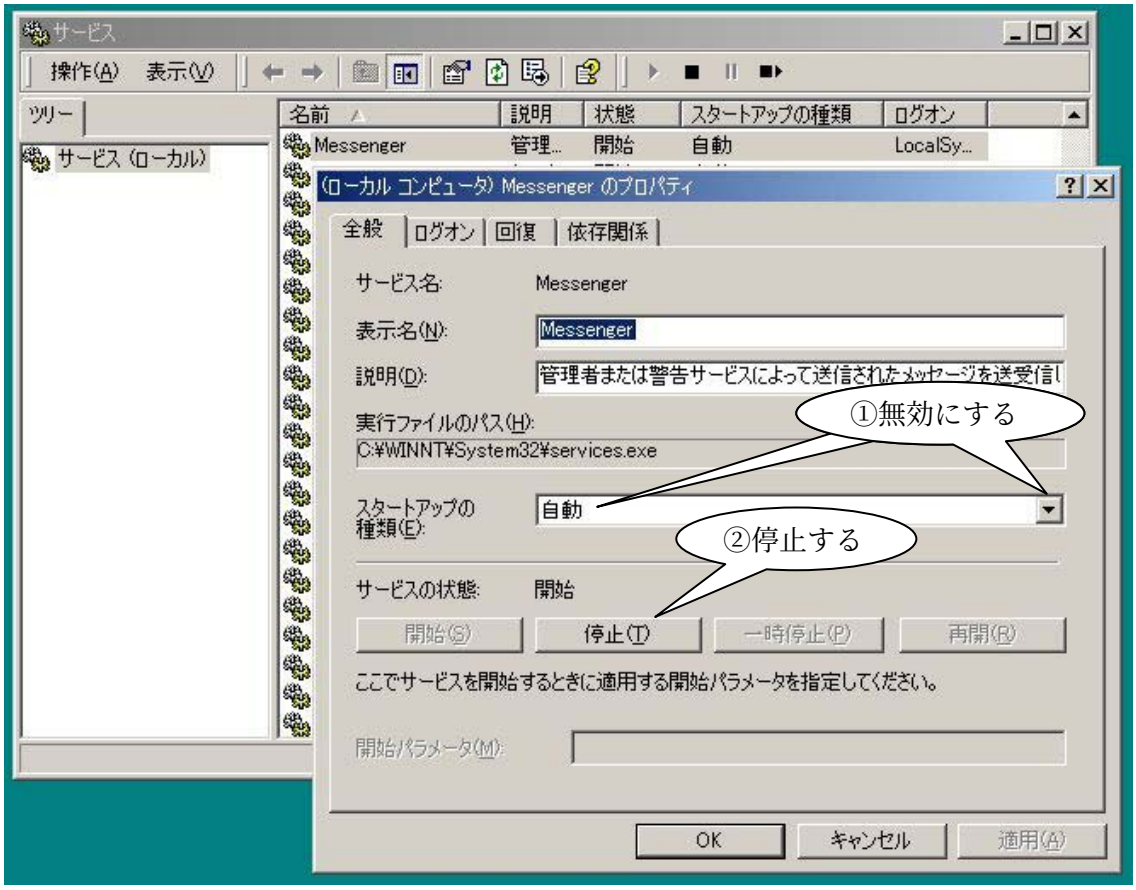
```
STOP! System has encountered an Internal Error
Your registry is corrupted.
We recommend a complete system scan.
Visit
www.********.com
To repair now
FAILURE TO ACT NOW MAY LEAD TO SYSTEM FAILURE!
```

STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
Windows has found CRITICAL SYSTEM ERRORS.
To fix the errors please do the following:
1. Download Registry Repair from: http://www.********.com
2. Install Registry Repair
3. Run Registry Repair
4. Reboot your computer
FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
Windows has found 55 Critical System Errors.
To fix the errors please do the following:
1. Download Repair Registry Pro from: www.********.com
2. Install Repair Registry Pro
3. Run Repair Registry Pro
4. Reboot your computer
FAILURE TO ACT NOW MAY LEAD TO SYSTEM FAILURE!

- これらのメッセージがコンピュータの画面上に表示される条件(AND 条件)があり、全てのコンピュータに表示されるわけではありません。
  - Windows OS(NT 以降)を使用したコンピュータ
  - インターネットにグローバル IP アドレスで接続
  - Messenger サービスが動作している (Default で自動的に動作しています)
  - Windows XP でファイアウォール機能を使用していない
- 一方的にインターネットから送られてきたメッセージ(スパムメッセージのようなもの)なので、無視すれば問題はありませんが、『メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043) 』のパッチが適用されていない場合は、リモートからコードが実行される危険性があります。
- メッセージ中には具体的な操作指示が書かれていますが、従わないで下さい。表示された画面やダイアログ(プロンプト)ボックスは、画面右上の×ボタンあるいは ALT+F4 キーで終了するようにしましょう。
- Messenger サービスは、一般的には企業内のクライアント-サーバ環境で利用される機能であり、例えば、プリントサーバから印刷完了のメッセージを通知する場合に使われます。しかしながら、一般的な家庭ユーザの場合は、このサービスが動作している必要はないと考えられます。

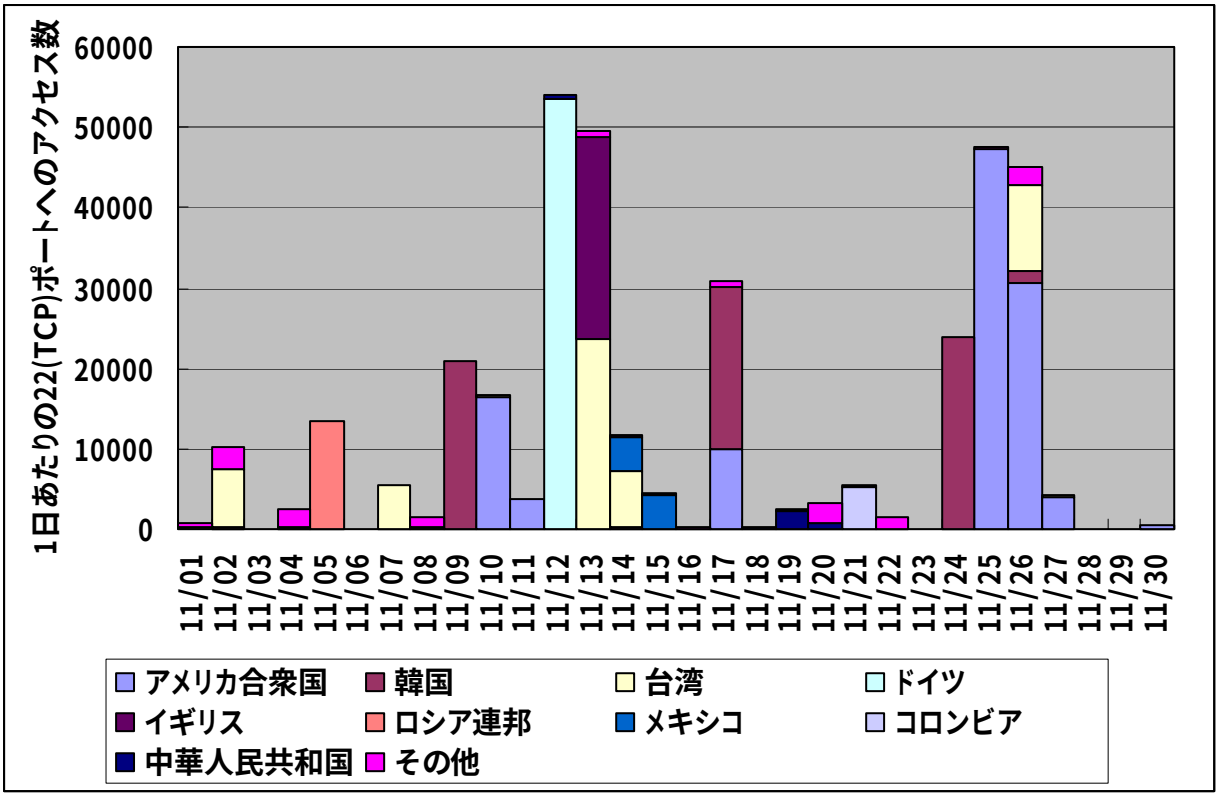
- メッセージが頻繁に表示されるようであれば、表示を抑止することができます。
  - Windows XP の場合は、「スタート」の「コントロールパネル」から「パフォーマンスとメンテナンス」を選択し、「管理ツール」の「サービス」を起動する。
  - Windows 2000 の場合は、「スタート」の「設定」から「コントロールパネル」を選択し、「管理ツール」の「サービス」を起動する。
  - サービスの画面で Messenger の項目を見つけ、状態が「開始」であれば、この項目を選択し、マウスの右ボタンクリックにより、プロパティを表示する(図 2.4.2 を参照下さい)。
  - Messenger はデフォルトの状態で、「スタートアップの種類」が「自動」で「サービスの状態」は「開始」となっています。
  - 「(ローカル コンピュータ)Messenger のプロパティ」画面の「スタートアップの種類」を「無効」に変更する(右端の▼で選択できます)。
  - 「サービスの状態」にある「停止」ボタンを押す。
  - Windows XP の場合は、ファイアウォール機能も有効にして下さい。
  - ただし、企業内 LAN 等で使用しているコンピュータの場合は、システム管理者の指示に従って下さい。



【図 2.4.2 Messenger サービスの停止方法】

2.5 22(TCP)ポートへのアクセスについて

TALOT2 での観測点の 1 つで、メンテナンス用に SSH(Secure Shell)サーバを動作させています。この観測点での 22(TCP)へのアクセスについては、特定コンピュータへの攻撃と言うことで、観測データから除外しています。しかしながら、11 月も SSH サーバへの侵入を試みる攻撃が多かったため、ここで、報告することにしました。

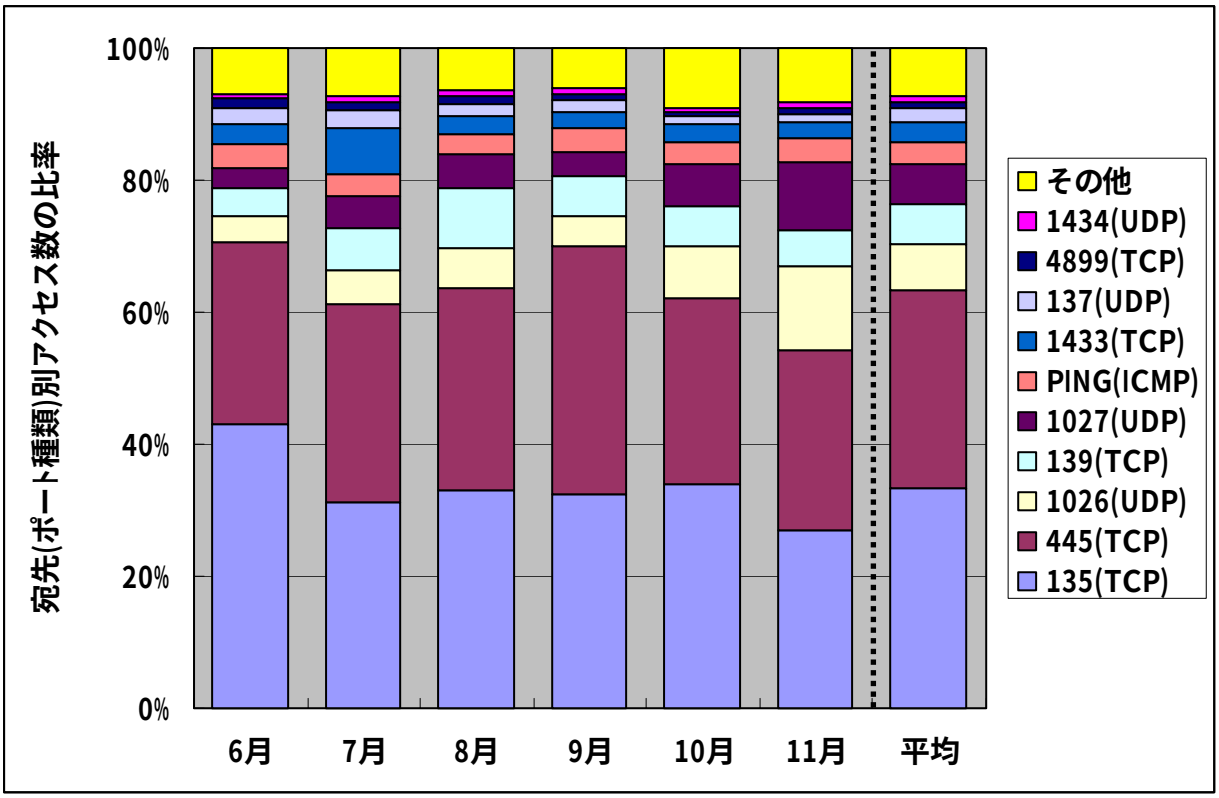


【図 2.5.1 22(TCP)ポートへのアクセス状況(アクセス数)】

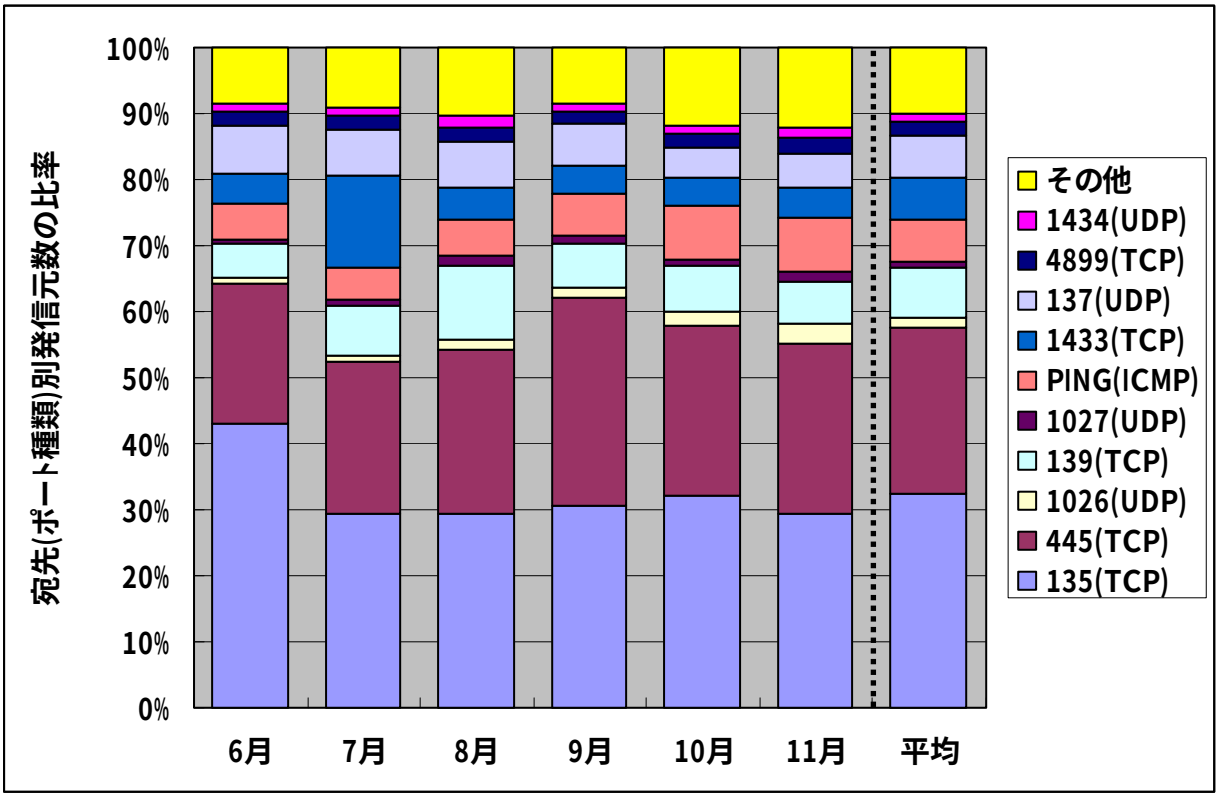
- 上図のアクセスは、ほとんどがこのサーバ(コンピュータ) に侵入しようとするアクセスです。
- パスワードクラッキング (辞書攻撃) と呼ばれる方法で、ログイン ID やパスワードを変化させながら、数千～数万回続けてアクセスすることで、サーバへログインしようとしています。
- これらのアクセスは世界中から行われています。
- 一般的には、インターネットに接続されたコンピュータに対して、22(TCP)ポートのポートスキャンを行い、反応するコンピュータに対して侵入を試みるようです。実際には、これらの操作を自動的に行う攻撃ツールもあるようです。少なくとも、人の操作で数万回のアクセスを連続的に行うのは不可能でしょう。
- ログイン ID やパスワードが安易に設定されていると、コンピュータへの侵入を許すことになります。SSH サーバを運用しているならば、利用者認証の方法を強化して下さい。

3．統計情報

3.1 2005 年 6 月～11 月の宛先(ポート種類)別の比率

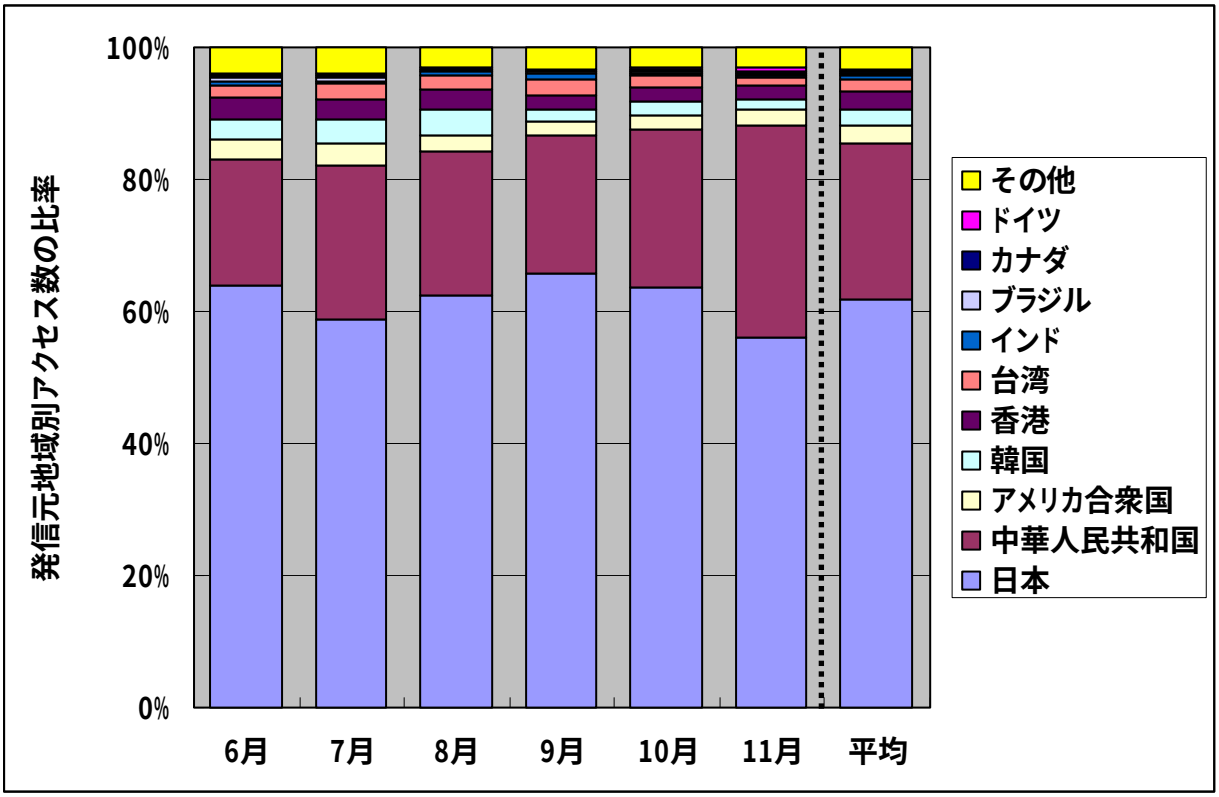


【図 3.1.1 2005 年 6 月～11 月の宛先(ポート種類)別アクセス数の比率】

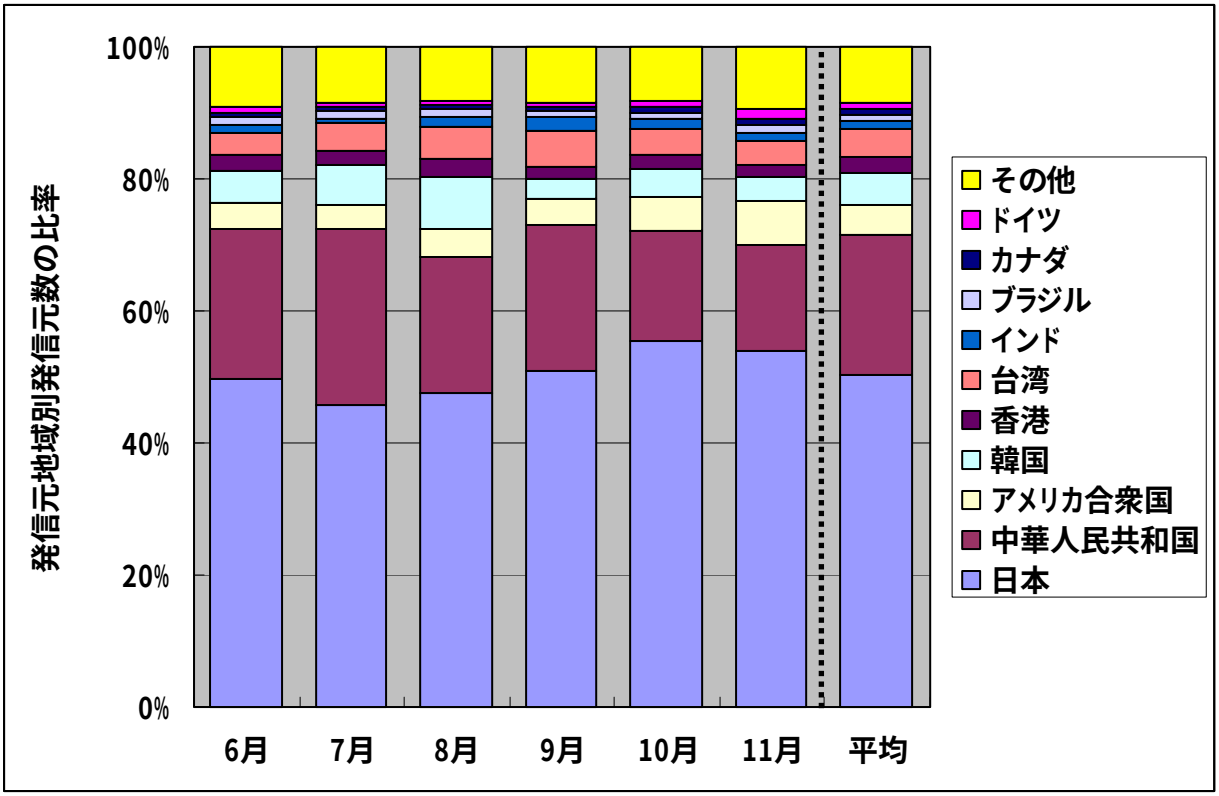


【図 3.1.2 2005 年 6 月～11 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 6 月～11 月の発信元地域別の比率



【図 3.2.1 2005 年 6 月～11 月の発信元地域別アクセス数の比率】

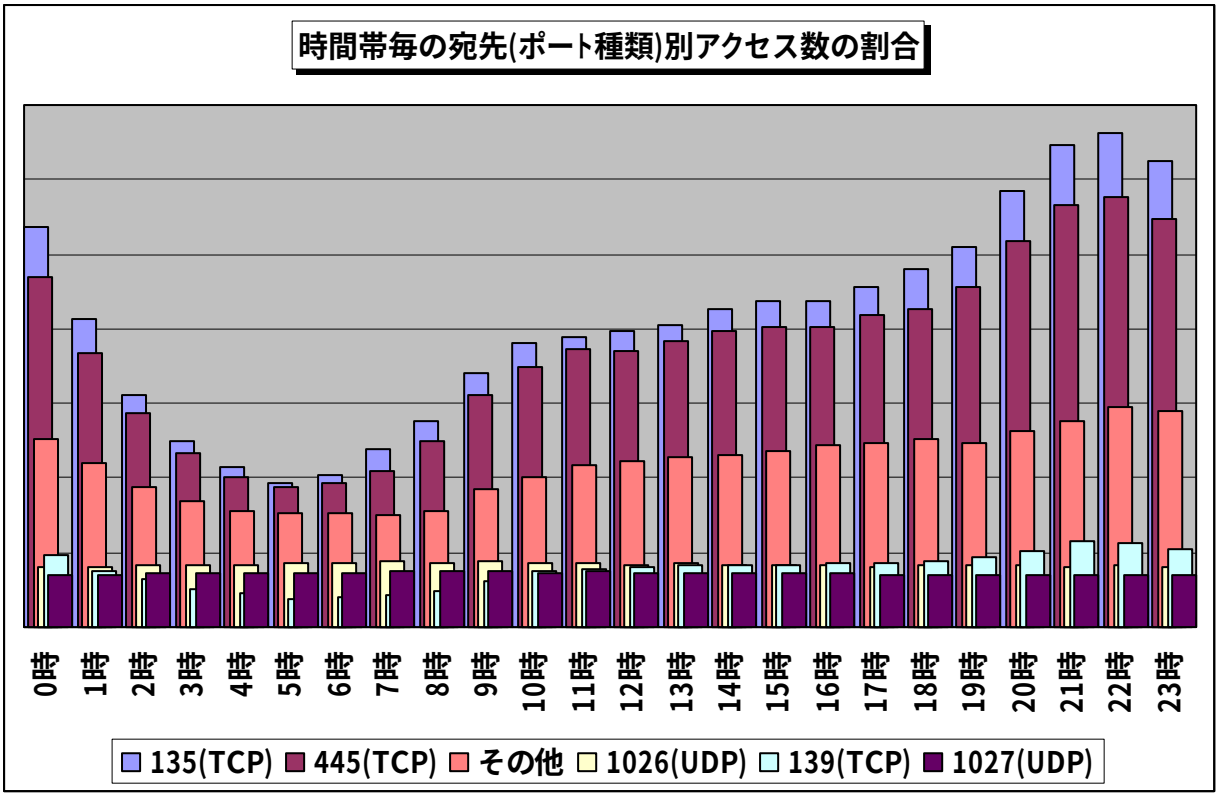


【図 3.2.2 2005 年 6 月～11 月の発信元地域別発信元数の比率】

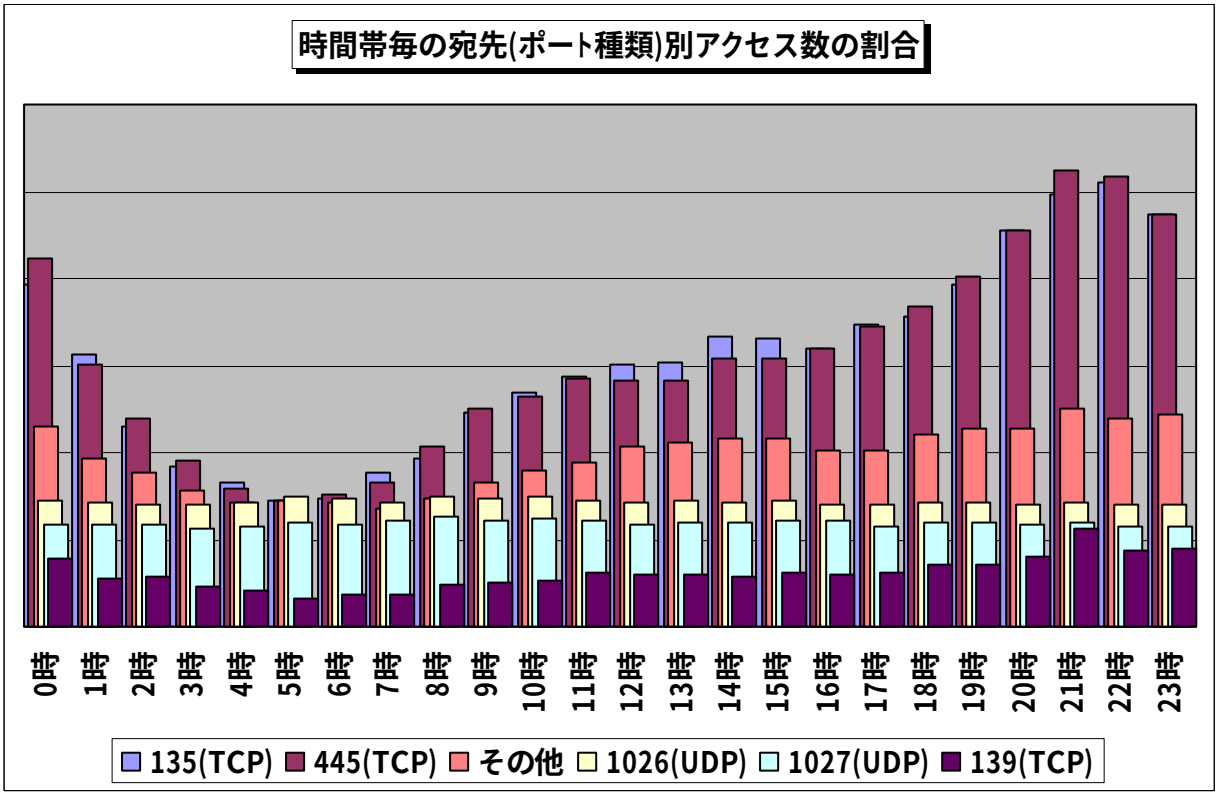
4．その他の統計情報

4.1 2005 年 6 月～11 月の時間帯統計

2005 年 6 月～11 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 11 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。



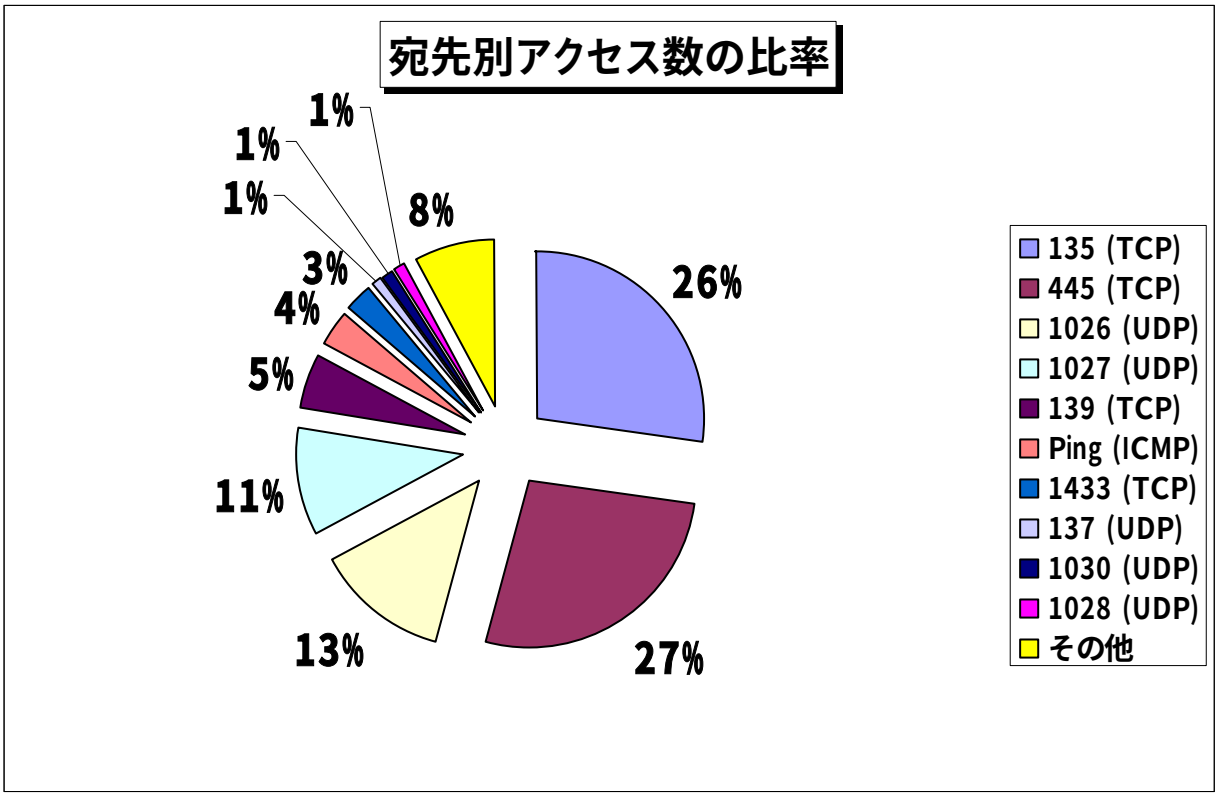
【図 4.1.1 2005 年 6 月～11 月の宛先(ポート種類)別アクセス数の時間帯統計】



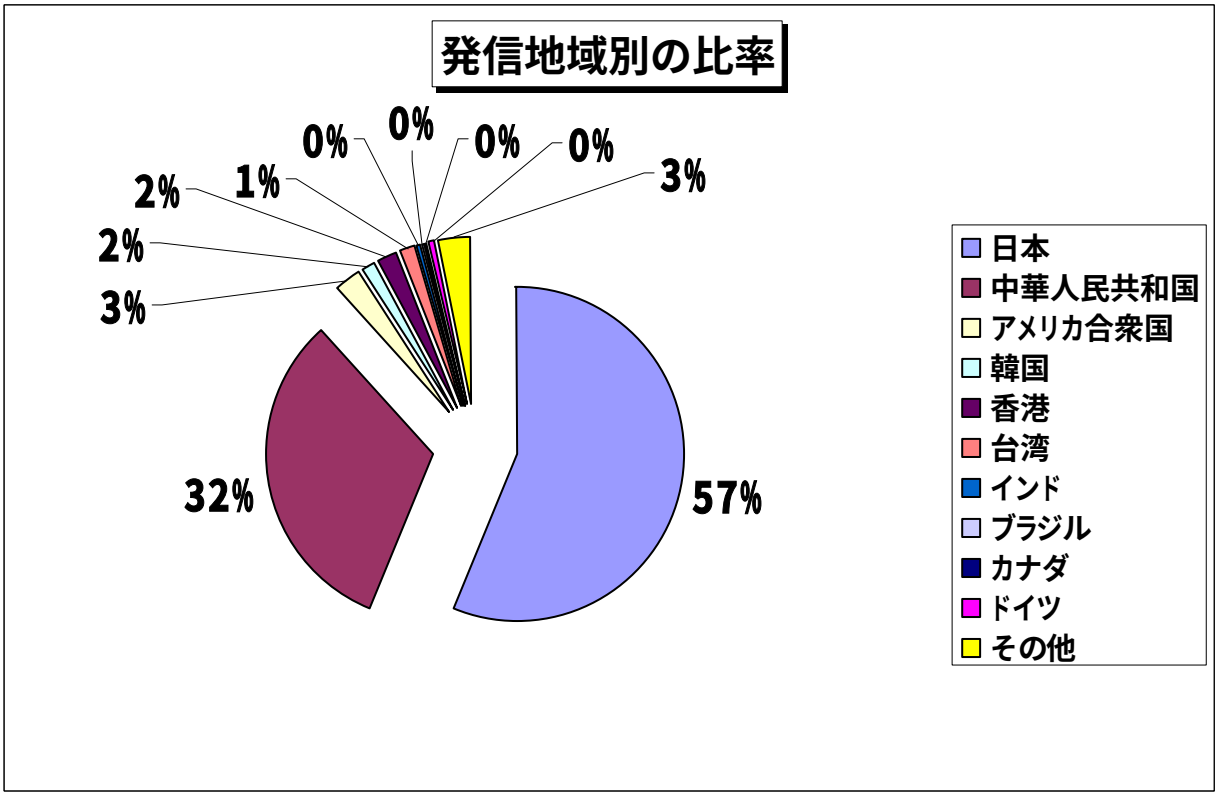
【図 4.1.2 2005 年 11 月の宛先(ポート種類)別アクセス数の時間帯統計】

4.2 2005 年 11 月の発信元地域別統計

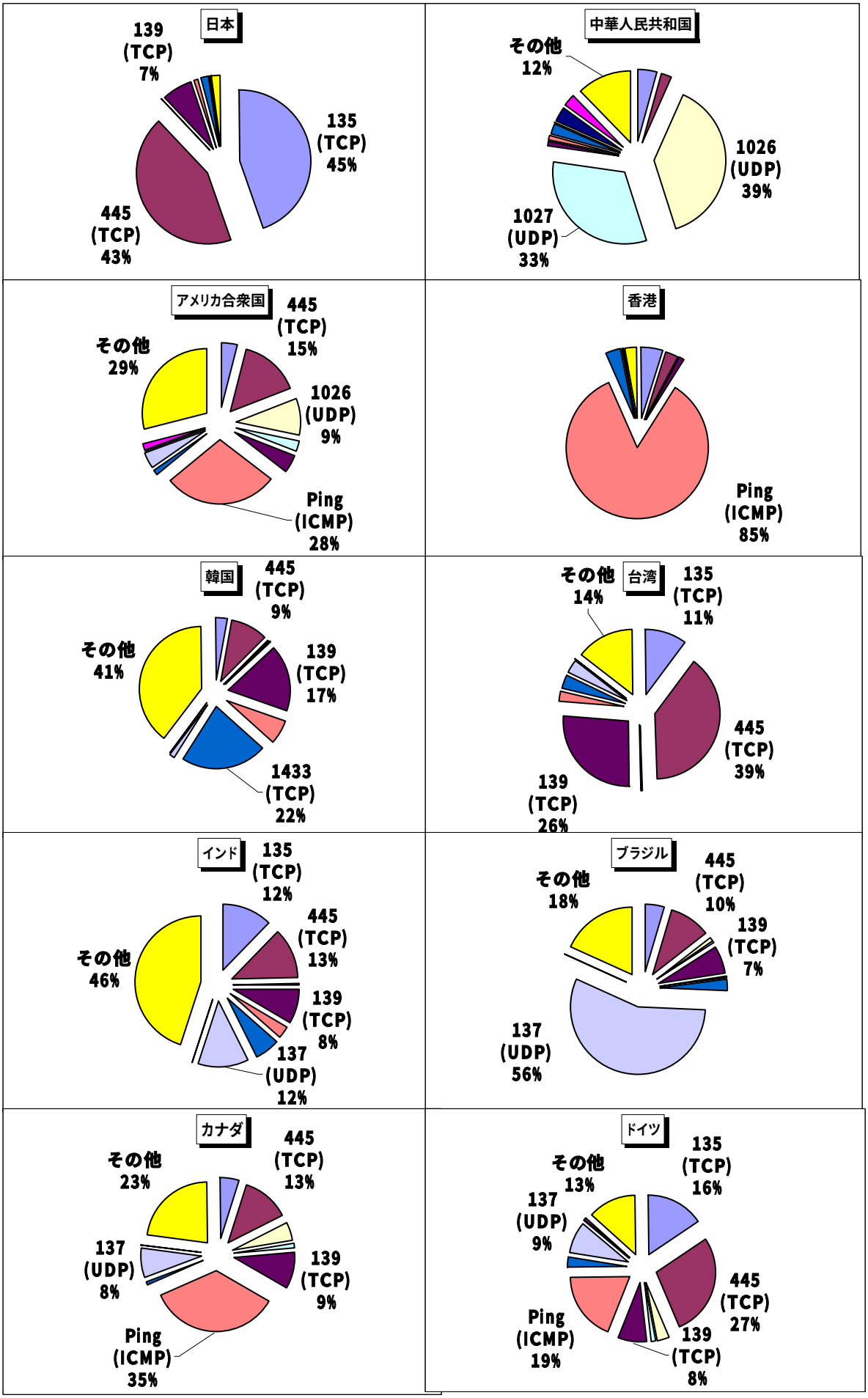
2005 年 11 月の発信地域別の宛先(ポート種類)別アクセス数の比率を以下に示します。



【図 4.2.1 2005 年 11 月の宛先(ポート種類)別アクセス数の比率】



【図 4.2.2 2005 年 11 月の発信元地域別アクセス数の比率】



【図 4.2.3 2005 年 11 月の発信元地域毎の宛先(ポート種類)別アクセス数の比率】

5．補足説明

以下に、当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である
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
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
1028(UDP)/1030(UDP)	1026(UDP)/1027(UDP)と同じく 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す

■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