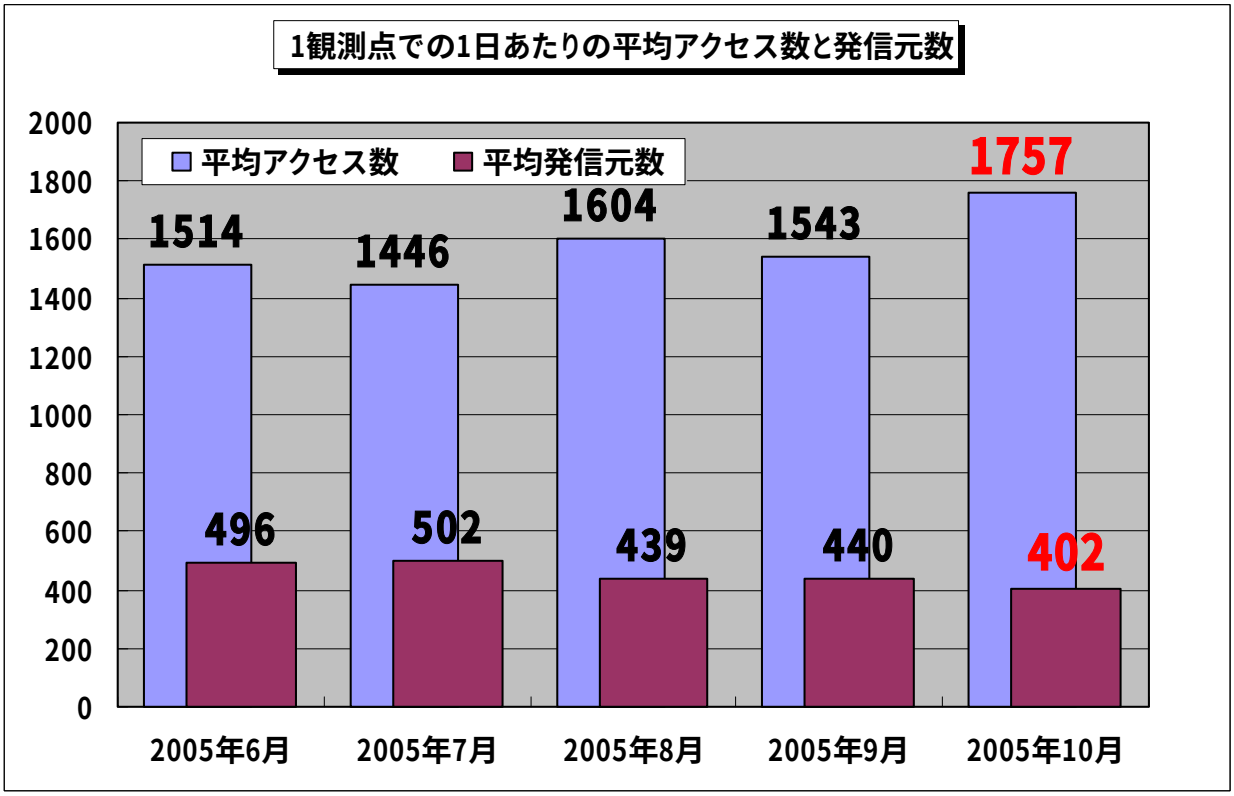
別紙 3

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 10 月の期待しない（一方的な）アクセスの総数は、10 観測点で **544,645 件**ありました。1 観測点で 1 日あたり **402** の発信元から **1,757 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、402 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。これは、2005 年9月に比べて、アクセス数で増加、発信元数で減少という状況です。



【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～10 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。

2．10 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。

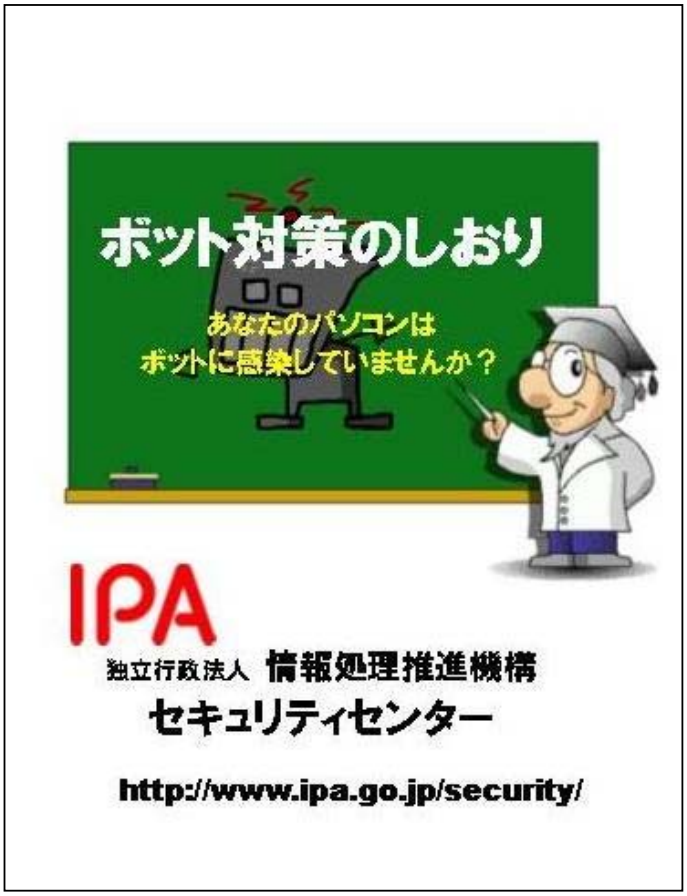
システムの管理者は、サーバに脆弱性がないか確認し、常に最新の状態に保つことに心掛けて下さい。

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。

■対策のしおり - ボット対策、スパイウェア対策 -
http://www.ipa.go.jp/security/antivirus/shiori.html

IPA は、情報セキュリティ対策のための「ボット対策のしおり」および「スパイウェア対策のしおり」を作成いたしました。

本しおりは、一般の家庭ユーザや社内でパソコンを利用する方を対象に、ボット対策やスパイウェア対策を分かりやすく説明したものです。気軽に読んでいただけるよう、挿絵を多用し、それぞれの脅威の概要、仕組み、対策を理解し、把握できるように工夫しております。これらの脅威への対策を実践するために、ぜひご活用ください。



10 月の特徴的なアクセスは 1026/1027(UDP)ポートへのアクセスおよび 20000(UDP)ポートへのアクセス数の増加です。

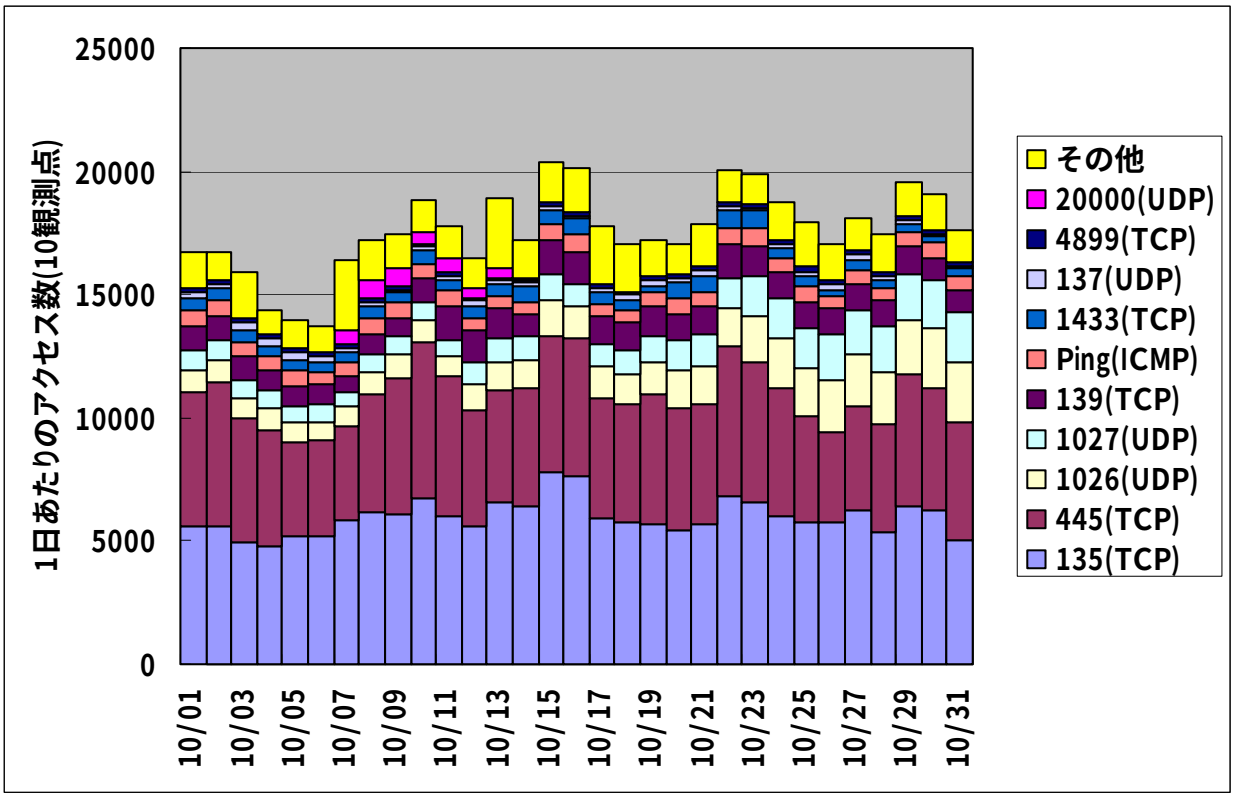
10月のアクセス数と発信元数の関係を図1でみると、ここ数ヶ月と比べて、発信元数が減少している割にはアクセス数が多い状況です。この理由として挙げられるのは、1026/1027(UDP)へのアクセスの増加です。これらのアクセスは、1026(UDP)ポートや 1027(UDP)ポート経由で、Windows Messenger 機能を利用したポップアップメッセージを送りつけるものです。

特に害のあるアクセスではありませんが、パソコンを操作する上では邪魔な存在です。これらのアクセスについては、「**2.4 1026/1027(UDP)ポートへのアクセスについて**」に詳細を記述します。

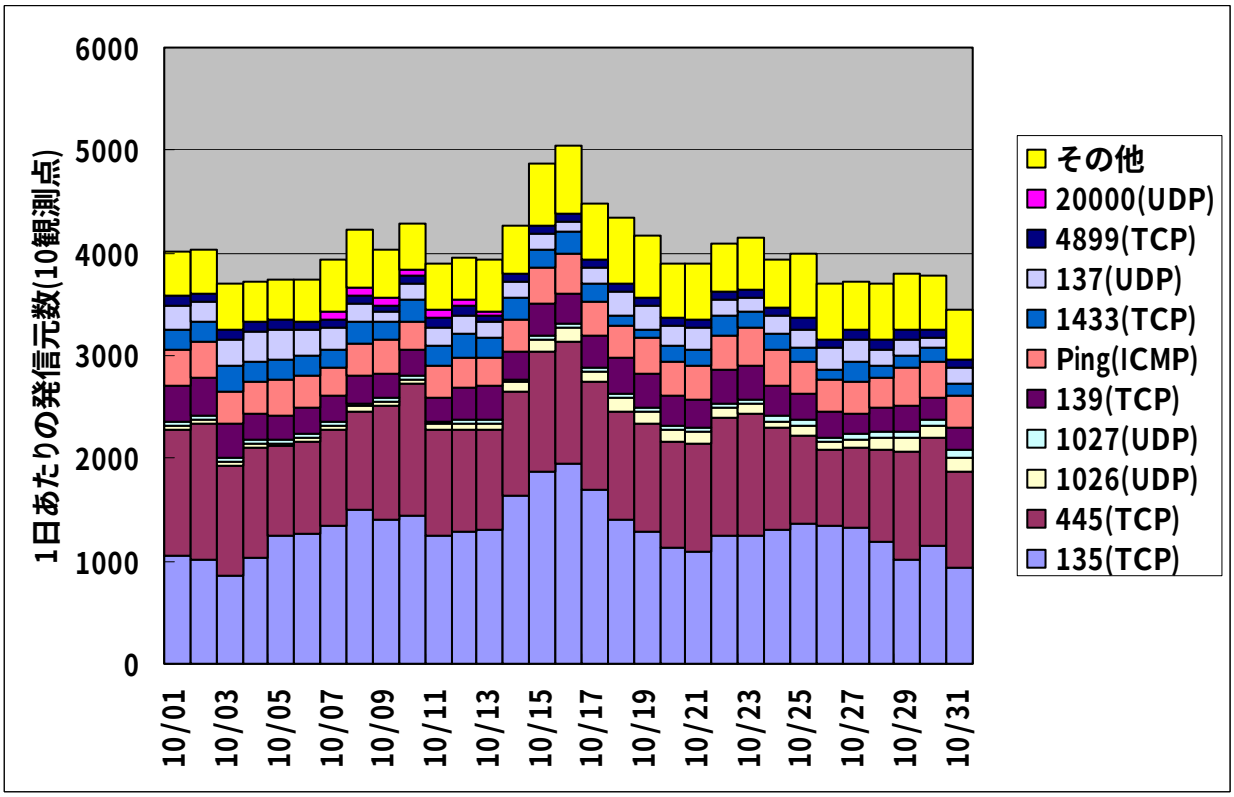
さらに、20000(TCP/UDP)へのアクセスが、観測点のＩＰアドレス変更と同時に観測されました。

このアクセスについても、「**2.5 20000(TCP/UDP)ポートへのアクセスについて**」に詳細を記述します。

2.1 2005 年 10 月の一方的なアクセス状況

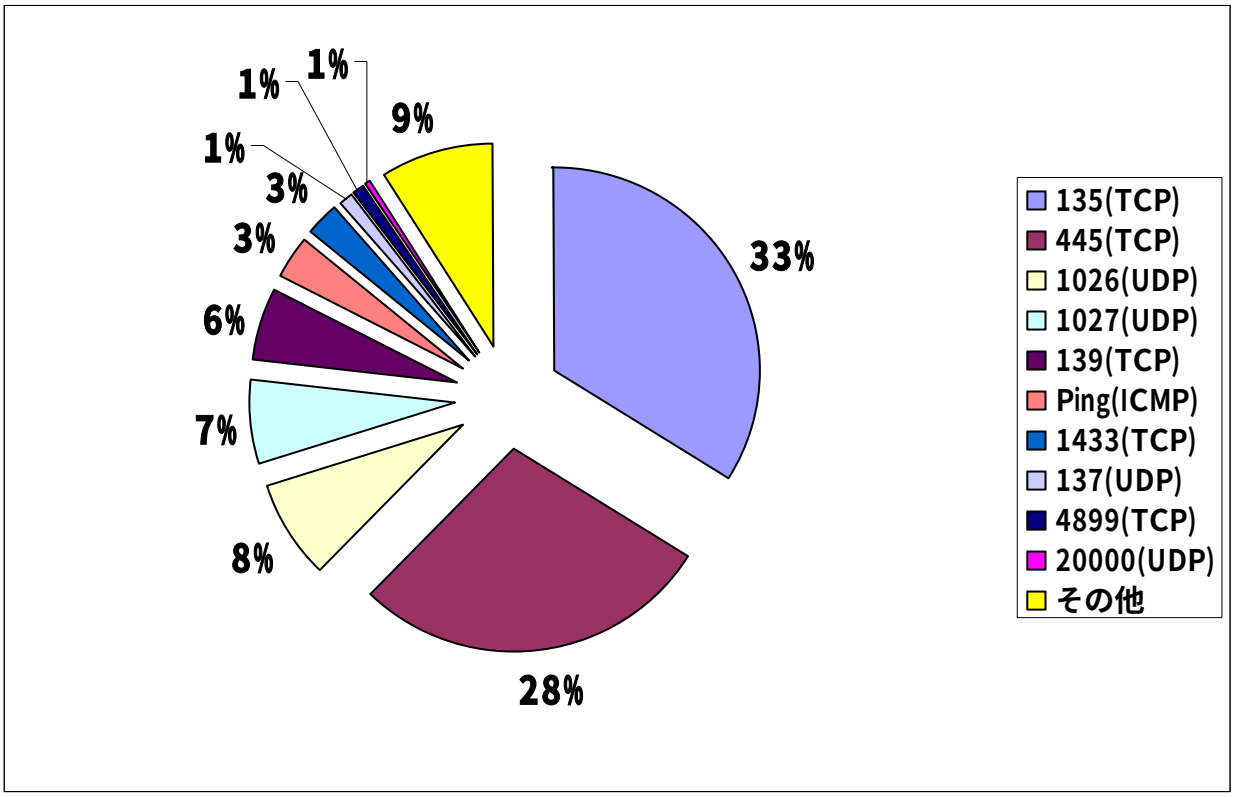


【図 2.1.1 2005 年 10 月の一方的なアクセス状況(アクセス数)】

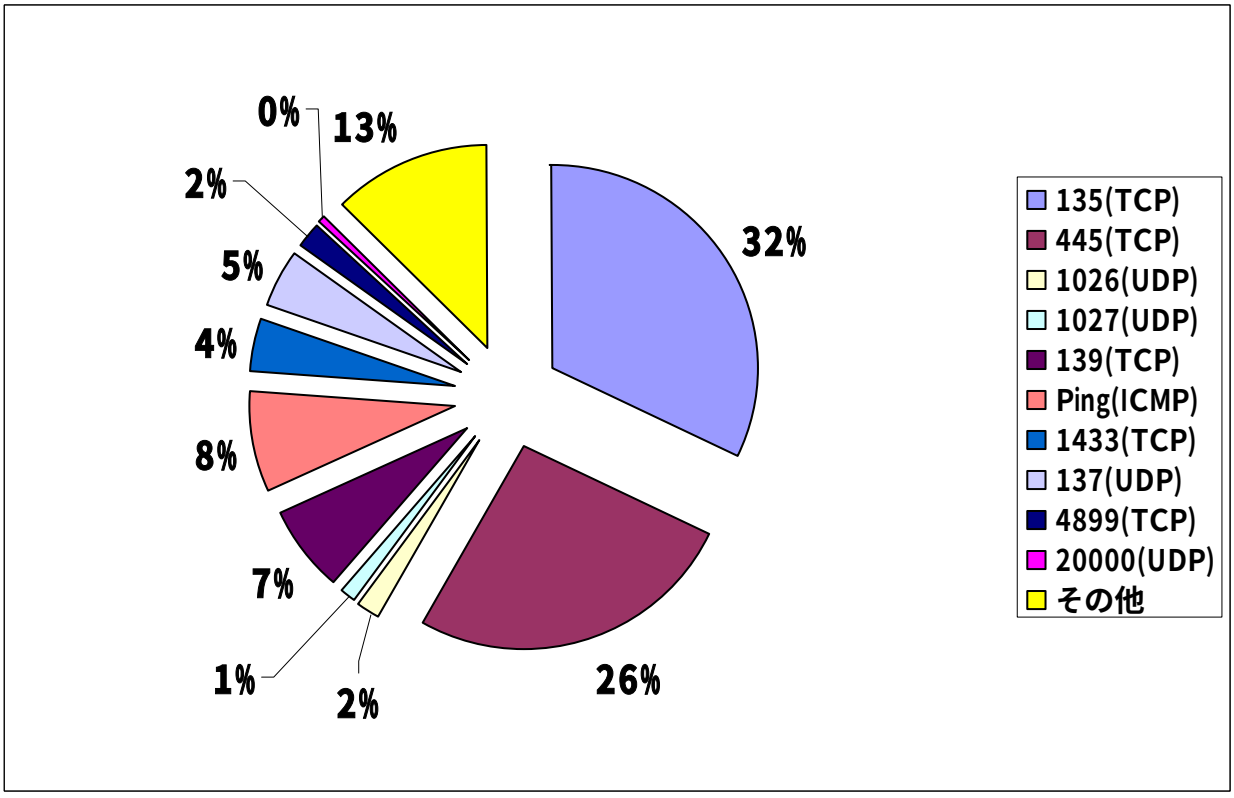


【図 2.1.2 2005 年 10 月の一方的なアクセス状況(発信元数)】

2.2 2005 年 10 月の宛先(ポート種類)別の比率

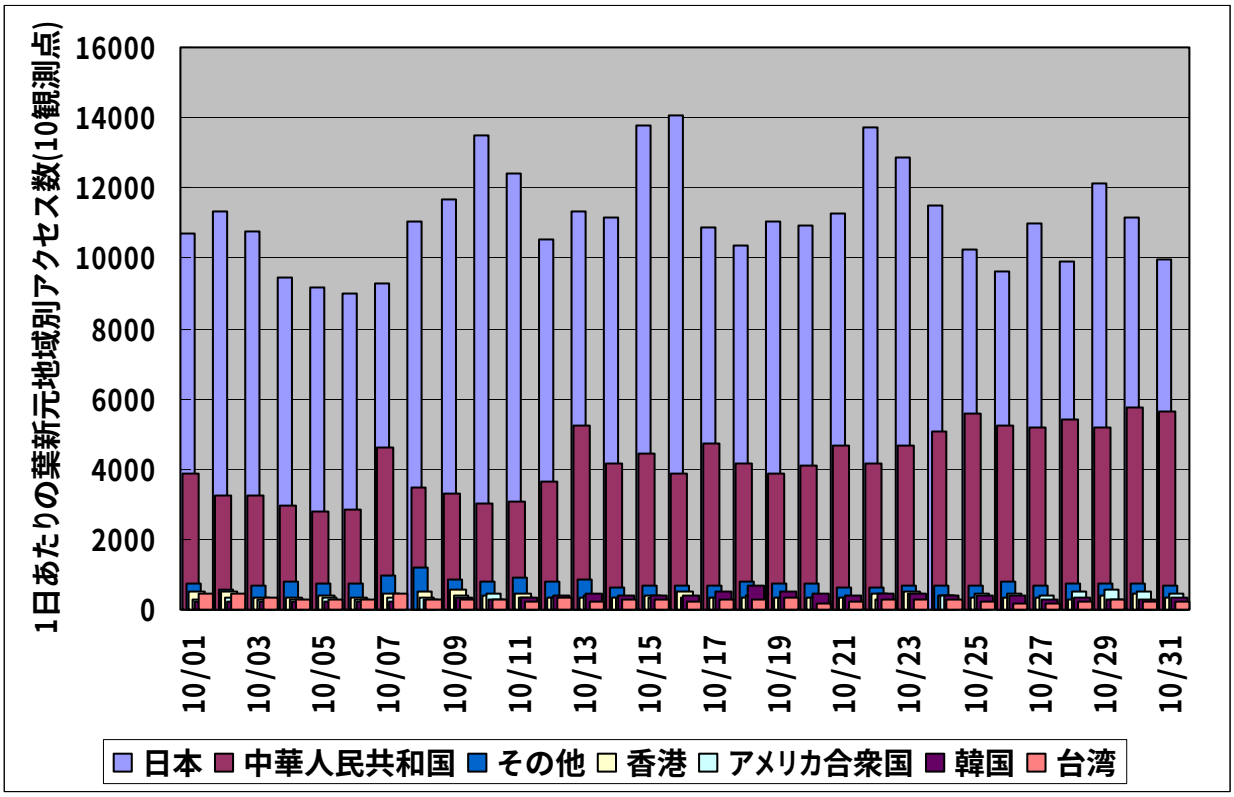


【図 2.2.1 2005 年 10 月の宛先(ポート種類)別アクセス数の比率】

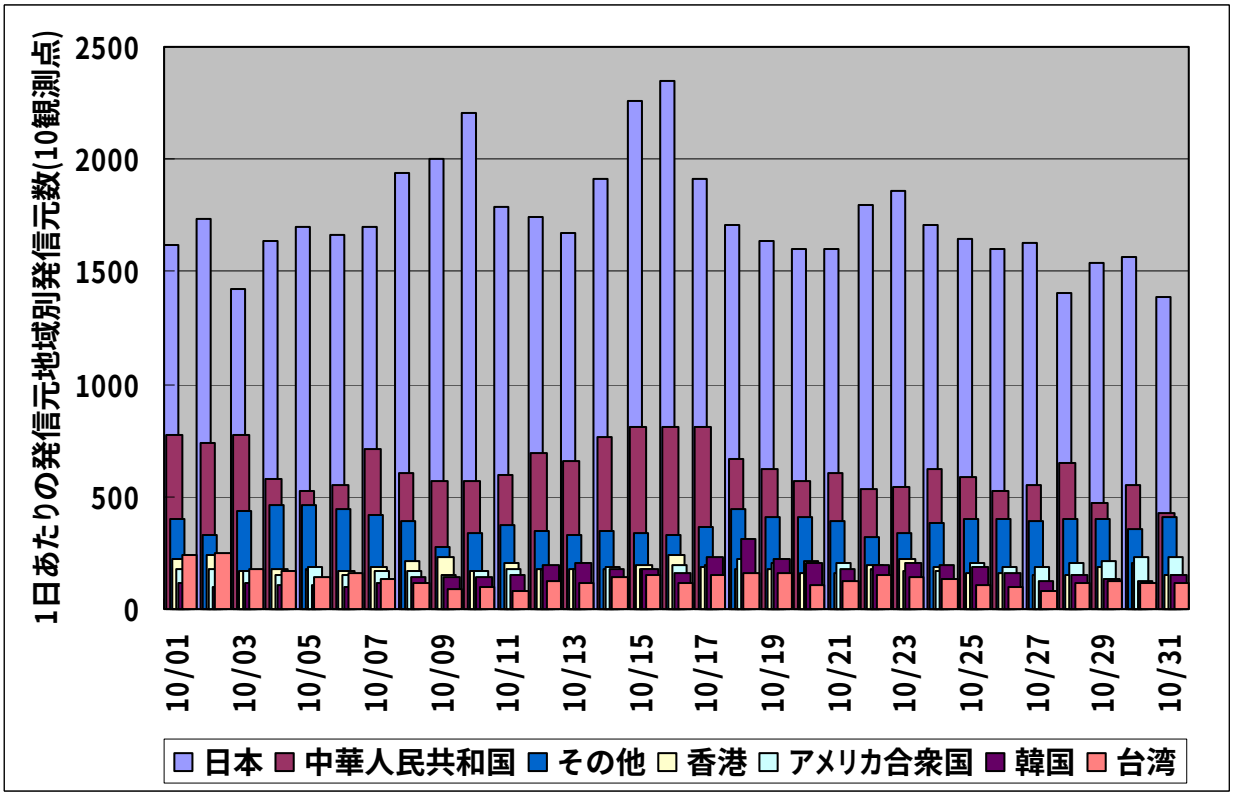


【図 2.2.2 2005 年 10 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 10 月の発信元地域別アクセス状況

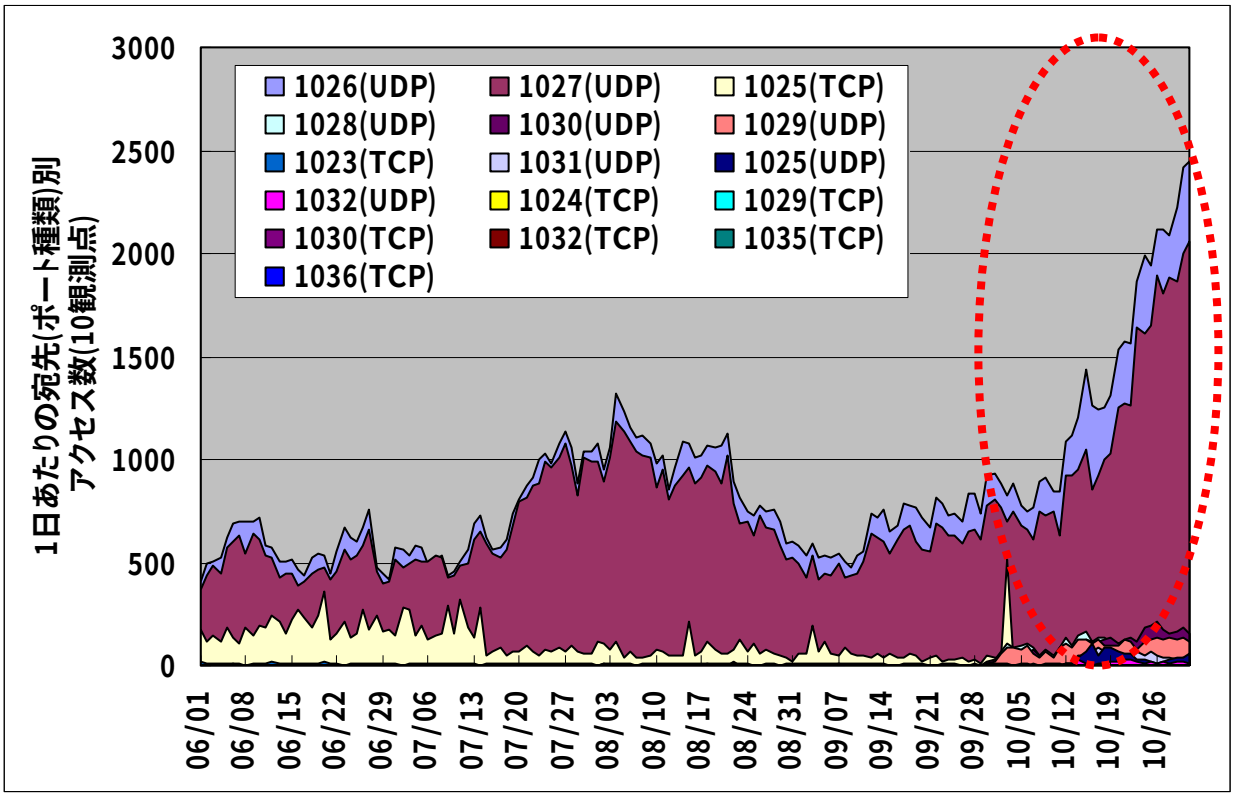


【図 2.3.1 2005 年 10 月の発信元地域別アクセス数の変化】



【図 2.3.2 2005 年 10 月の発信元地域別発信元数の変化】

2.4 1026/1027(UDP)ポートへのアクセスについて



【図 2.4.1 102x および 103x(TCP/UDP)ポート等へのアクセス状況】

- 1026/1027(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、1026(UDP)ポートや 1027(UDP)ポート経由で、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。

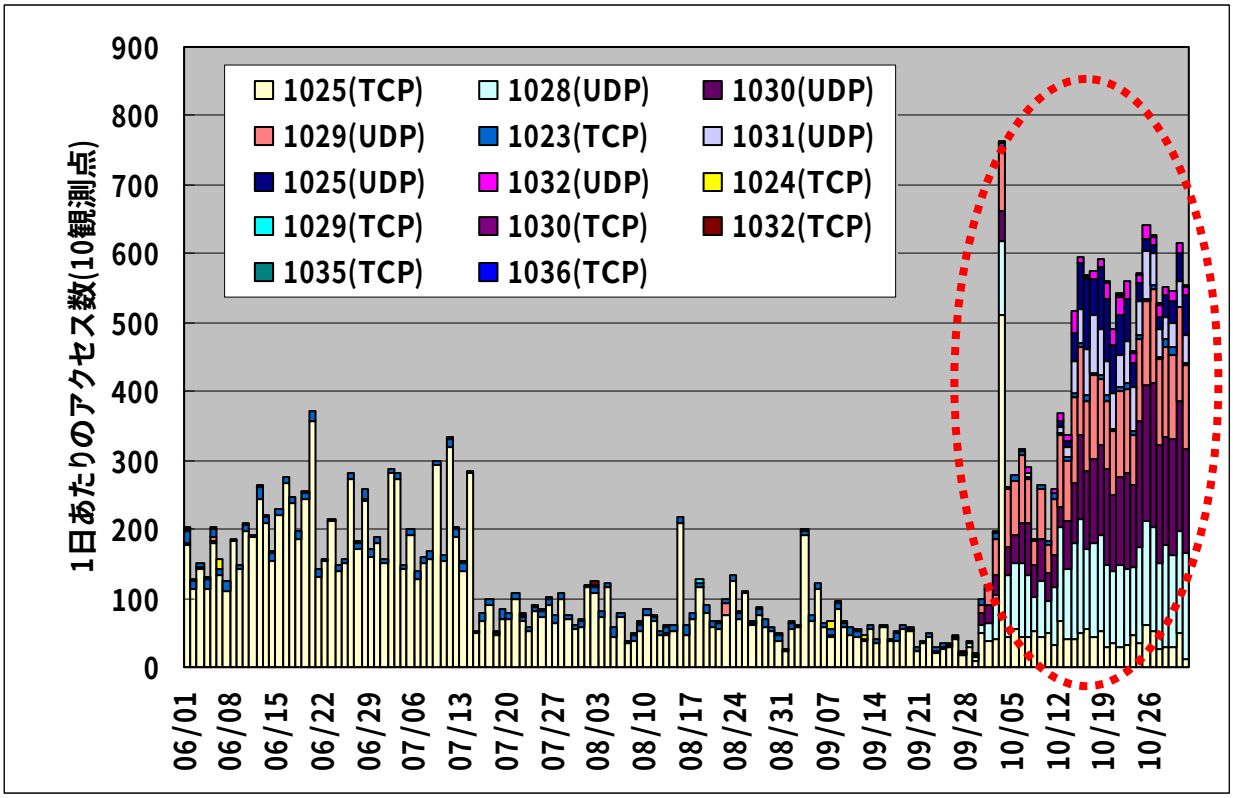
メッセージ本文例(綴りは原文のままですが、一部伏せ字になっています)

```
VIRUS OUTBREAK ALERT

Name:     Worm.SomeFool.AL
Aliases: Email-Worm.win32.NetSky.C
Type:     Win32 Worm
Desc:     Email Worm, Win32.HLLM.Netsky (Drweb), Win32.Netsky.C

If you already downloaded the Anti-Virus Pro, please update your virus
definition immediatly. Otherwise, please read the following instructions.
INSTRUCTIONS to Secure Your Computer:
1. Write down the web site address: http://**********.com
2. Open your Web Browser
3. Type the web site address: http://**********.com into the
  "Address" box at the top of your web browser and press the "Go" button
4. Click on "here" link to download and install the Anti-Virus program
DO NOT CLICK THE "OK" BUTTON BELOW UNTIL
YOU HAVE WRITTEN DOWN: http://**********.com
```

- 2005 年 8 月のプレスリリースでも、この件については報告しましたが、今回は増加傾向が大きいようです。

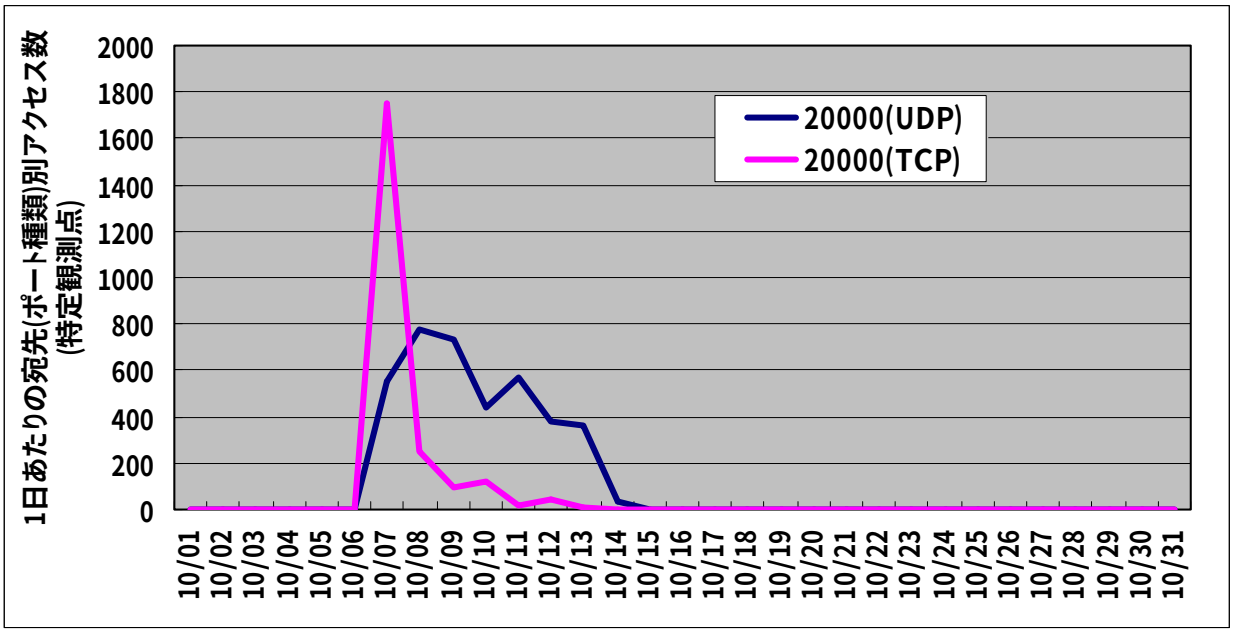
- 一方的にインターネットから送られてきたメッセージ(スパムメッセージのようなもの)なので、無視すれば問題はありませんが、不正なアクセスであることにかわりがありません。メッセージ中には具体的な操作指示が書かれていますが、従わないで下さい。表示された画面やダイアログ(プロンプト)ボックスは、×ボタンで終了して下さい。
- 表示させたくなければ、インターネット側(WAN 側)からの 1026 ポートおよび 1027 ポートをファイアウォールで閉じる(Windows XP の場合は、ファイアウォール機能を有効にすることでも同じです)か、Messenger サービスを無効にすることになります。ただし、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。

- さらに、この増加傾向に合わせたかのように、102x/103x(TCP/UDP)ポートへのアクセスが目立つようになりました(図 2.1.4 を参照下さい)。この中で、特に多いのが、1029(TCP/UDP)ポートへのアクセスと 1030(UDP)ポートへのアクセスです。これらのアクセスも、その多くが中国方面からのものですが、何らかの攻撃ツールによるものと思われますが、詳細については、現在調査中です。

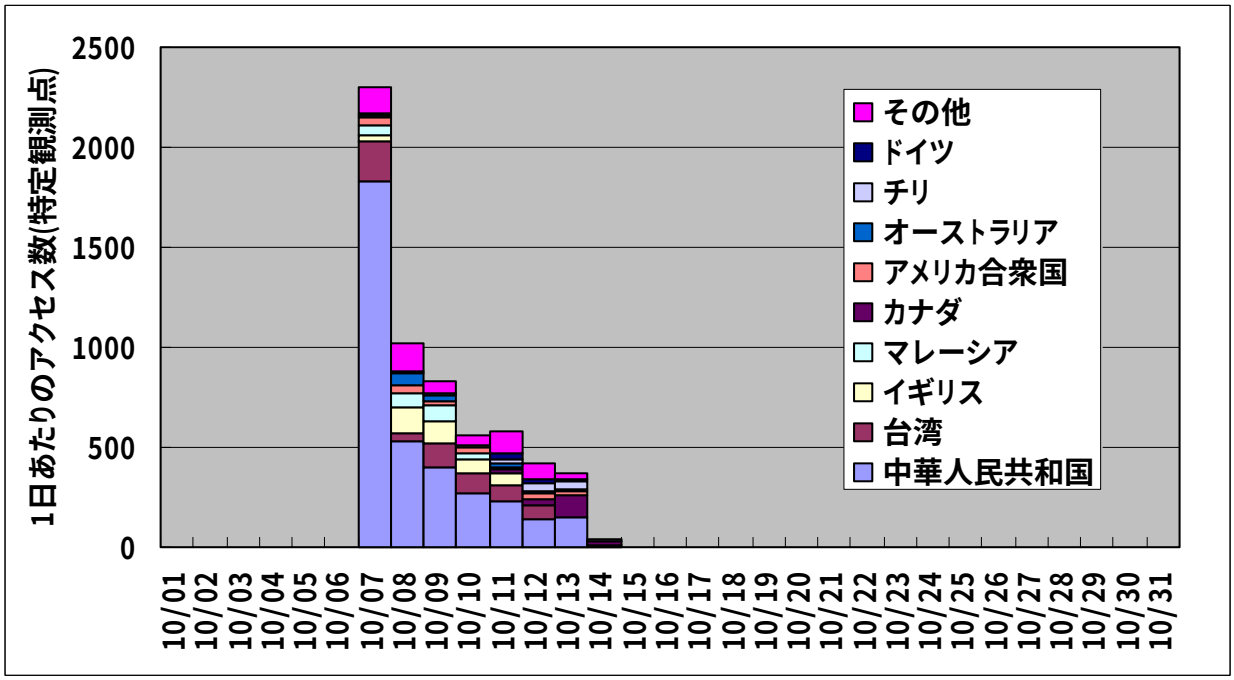


【図 2.4.2 1026/1027(UDP)を除く 102x および 103x(TCP/UDP)ポート等へのアクセス状況】

2.5 20000(TCP/UDP)ポートへのアクセスについて



【図 2.5.1 20000(TCP/UDP)ポートへのアクセス状況(アクセス数)】

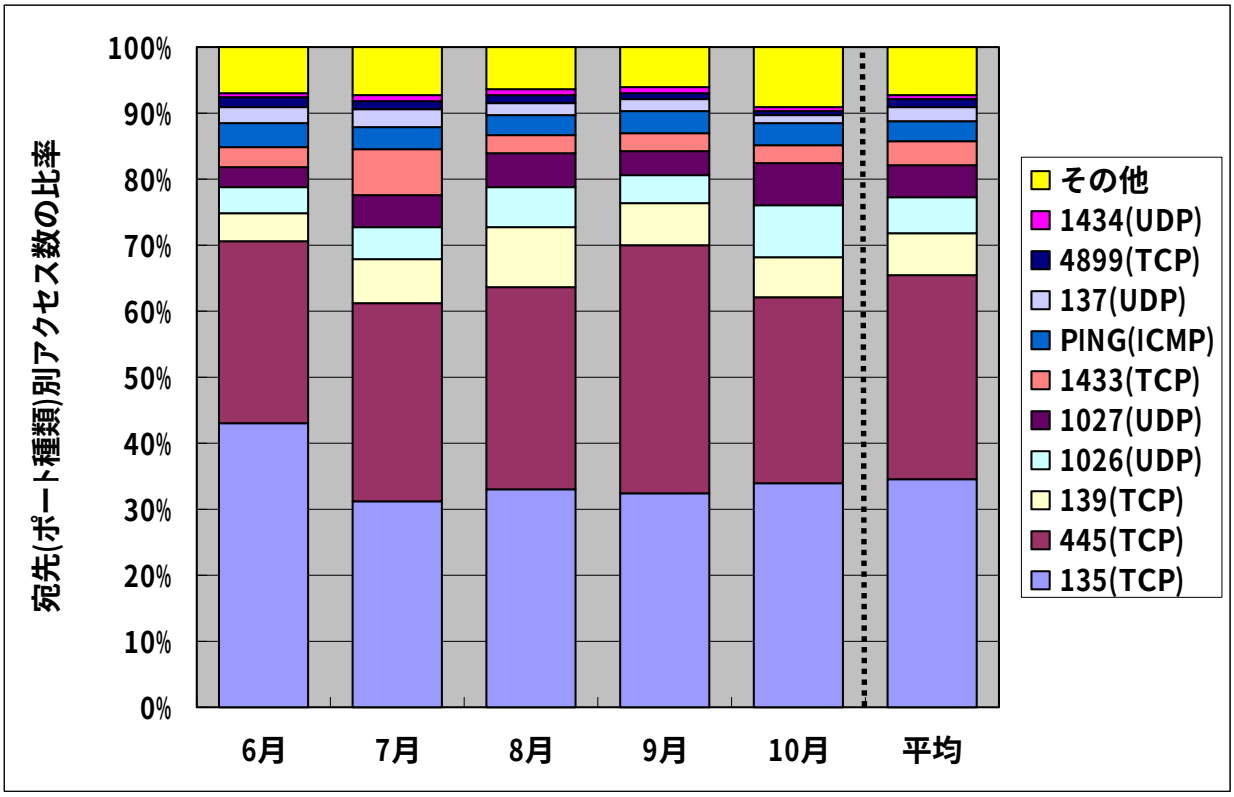


【図 2.5.2 20000(TCP/UDP)ポートへのアクセス状況(発信元地域)】

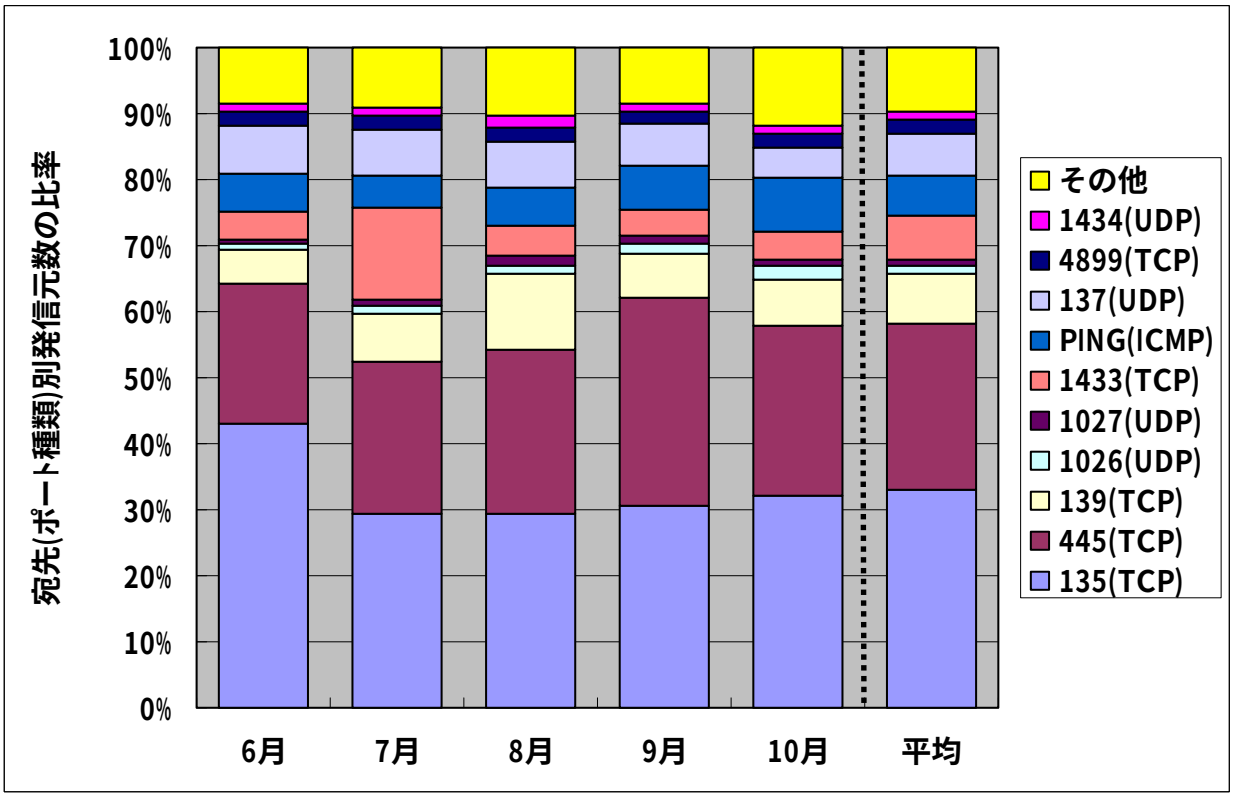
- TALOT2 での観測点の 1 つで、観測点 IP アドレスを更新したとたんに、20000(TCP/UDP)ポートへのアクセスが発生しました。
- このアクセスの詳細は不明ですが、P2P 関連のファイル交換あるいはオンラインゲーム関係のアクセスではないかと予測されます。世界中からアクセスと言うことでは、ファイル交換である可能性が高いと考えられます（詳細は不明）。
- 観測点の観測用 IP アドレスを変更した際に、新しく取得した IP アドレスが、以前ファイル交換あるいはオンラインゲームに利用していた可能性が高いと思われます。
- 実際には、1 週間程度で終息しましたが、このようなアクセスが、検出されるのも、一般利用者と同一の環境で観測している TALOT2 ならではのものと考えられます。
- この観測の結果、このようなアクセスは、一般の利用者の環境でも起こりうると言うことになります。

3．統計情報

3.1 2005 年 6 月～10 月の宛先(ポート種類)別の比率

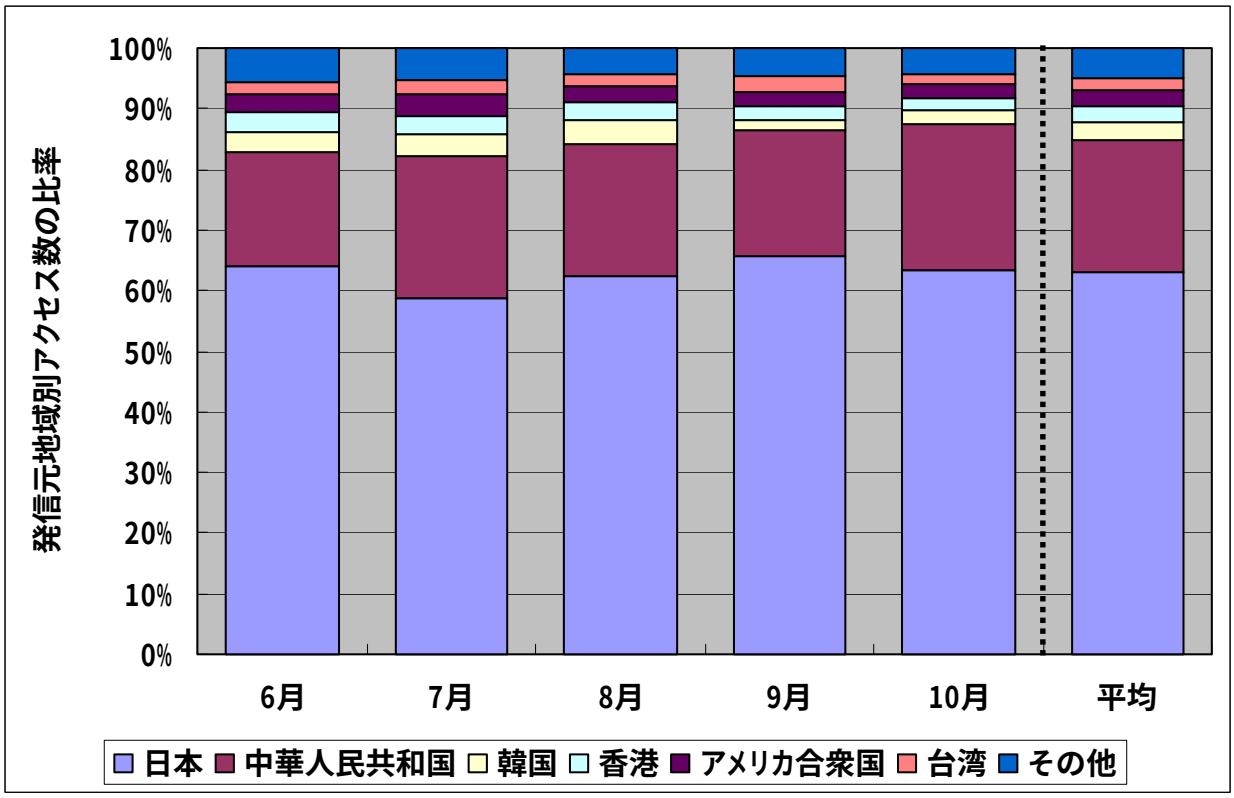


【図 3.1.1 2005 年 6 月～10 月の宛先(ポート種類)別アクセス数の比率】

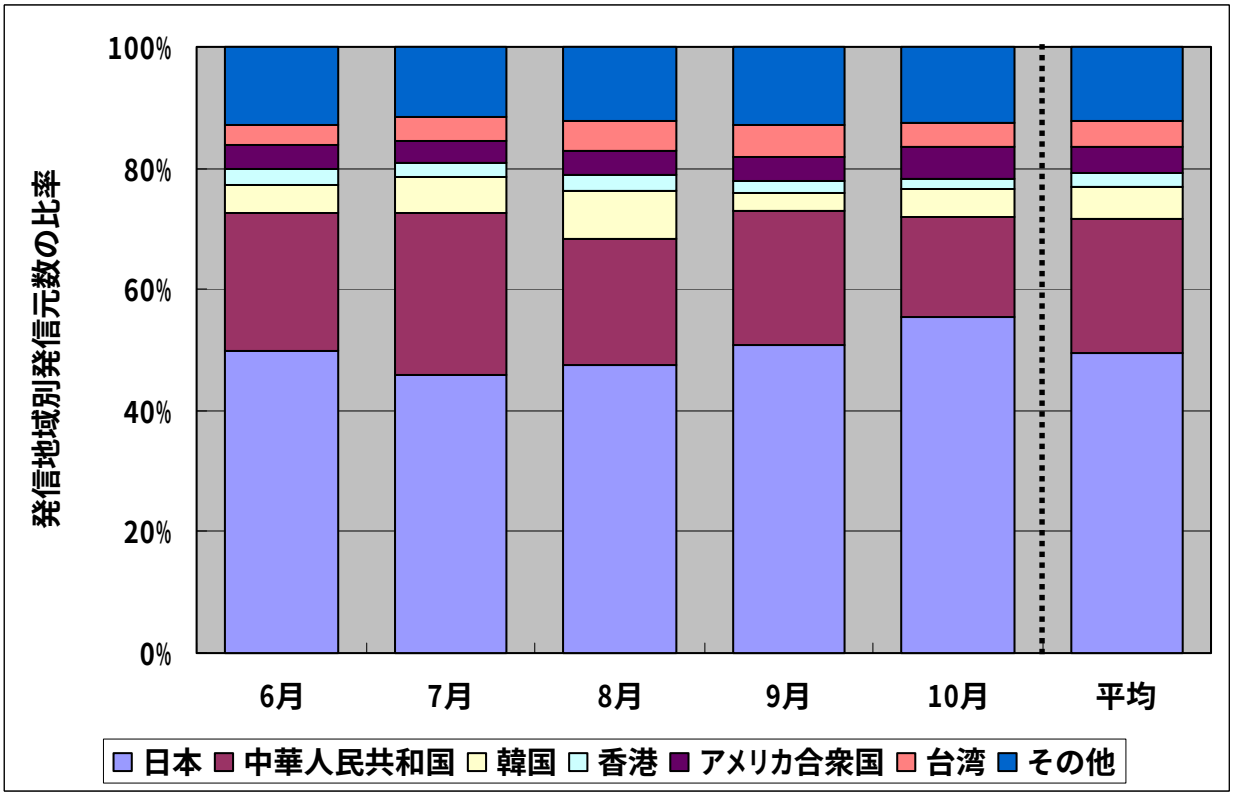


【図 3.1.2 2005 年 6 月～10 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 6 月～10 月の発信元地域別の比率



【図 3.2.1 2005 年 6 月～10 月の発信元地域別アクセス数の比率】

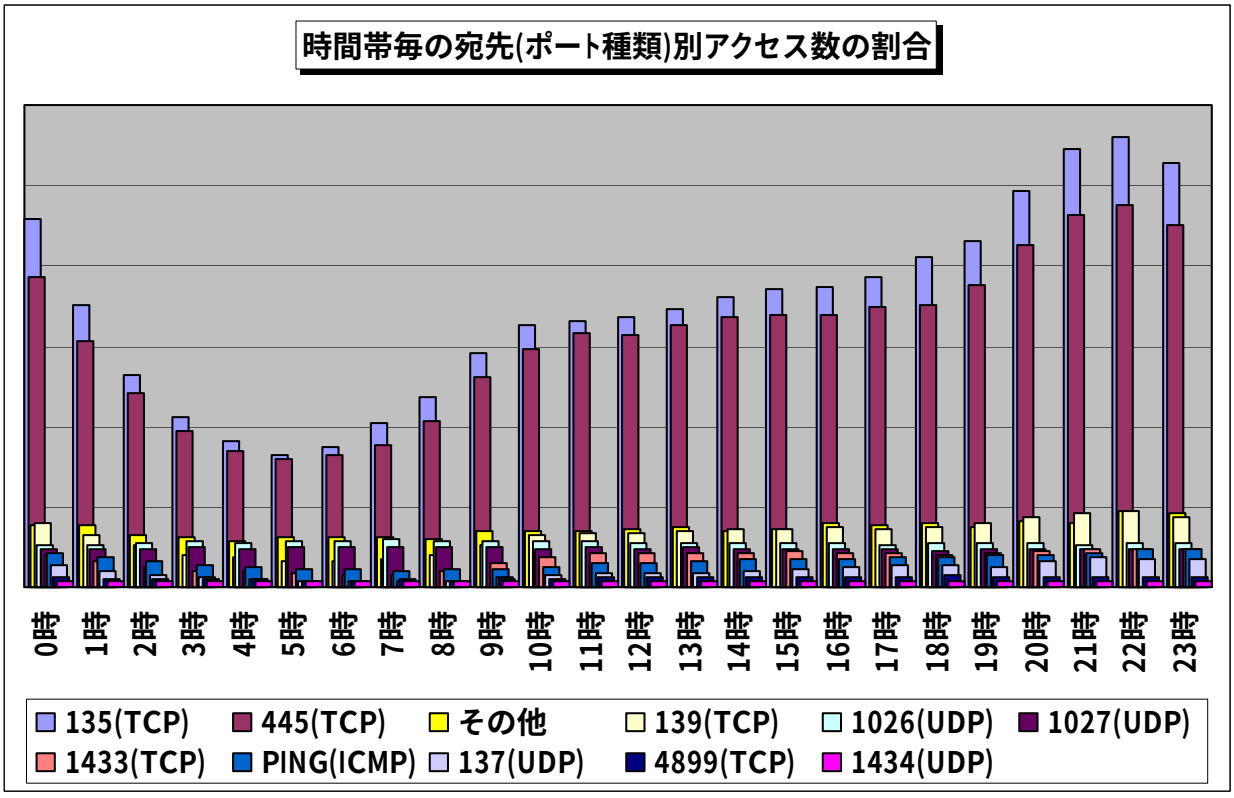


【図 3.2.2 2005 年 6 月～10 月の発信元地域別発信元数の比率】

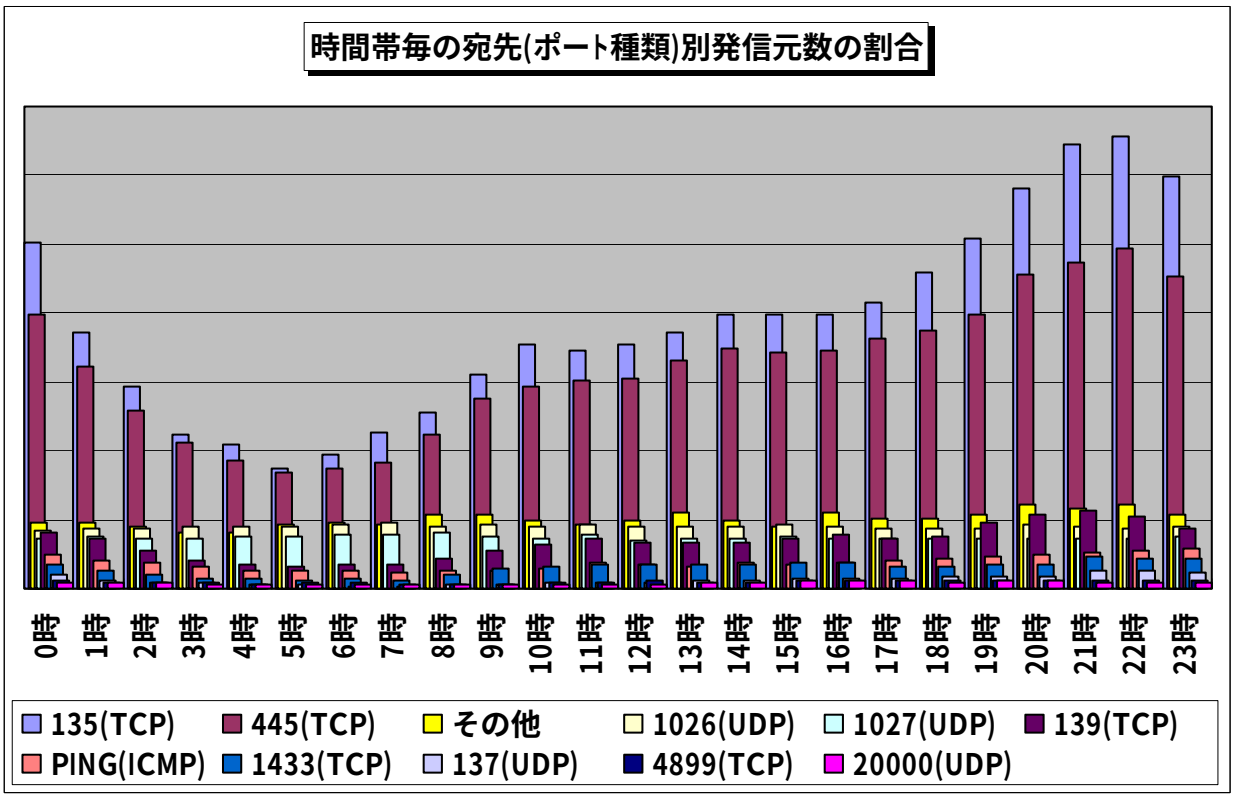
4．その他の統計情報

4.1 2005 年 6 月～10 月の時間帯統計

2005 年 6 月～10 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 10 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～10 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 10 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、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
20000(UDP)	20000 ポートを利用するトロイの木馬（Millenium）などがありますが、今回のアクセスについては、詳細は不明(本文を参照下さい)
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