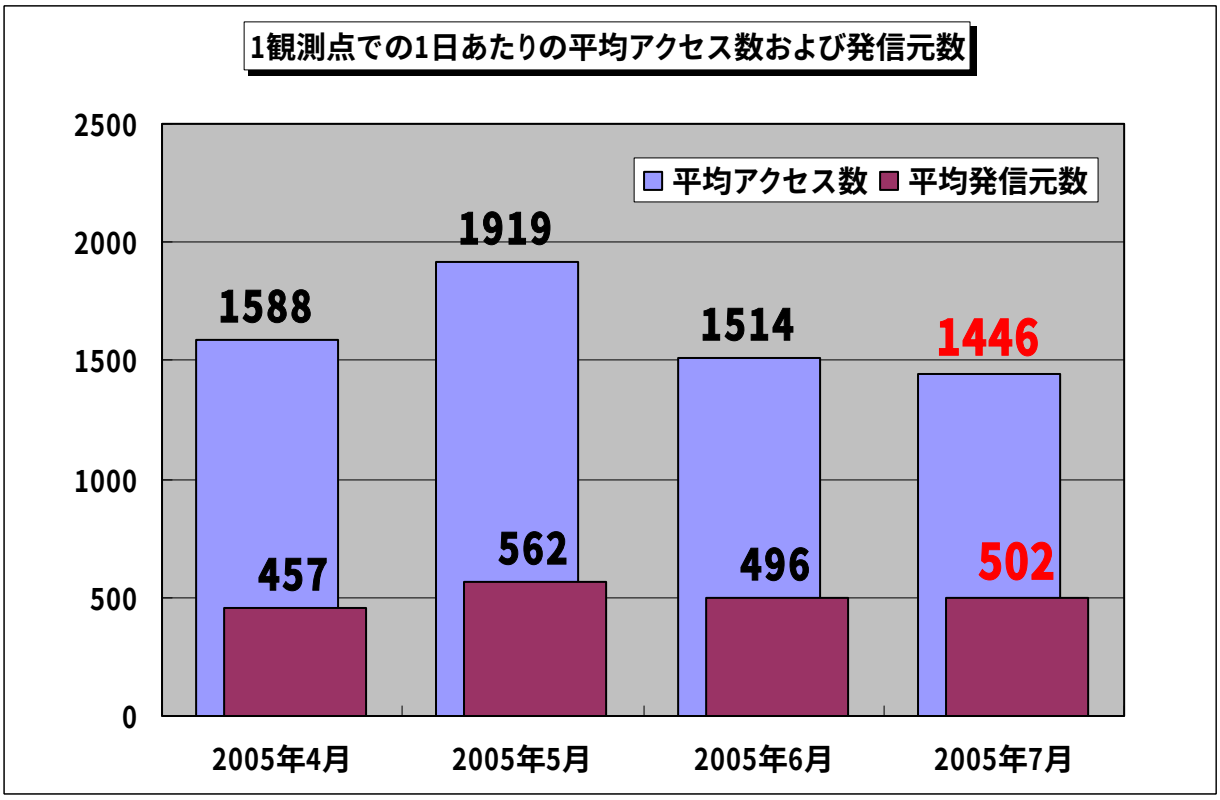
別紙 3

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7月の期待しない（一方的な）アクセスの総数は、10観測点で**448,232件**ありました。1観測点で1日あたり**約500**の発信元から**約1,450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、500 人の見知らぬ人から、3 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～7 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。

2．7月のアクセス状況

2005 年7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が多いようです。7月の特筆すべきアクセスは、1433(TCP)、1026(UDP)/1027(UDP)へのアクセスと先月から引き続きの 139(TCP)へのアクセスでした。これらのアクセスについては後述します。

次に、図 2.1.2 に宛先(ポート種類)別アクセス数ではなく、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。

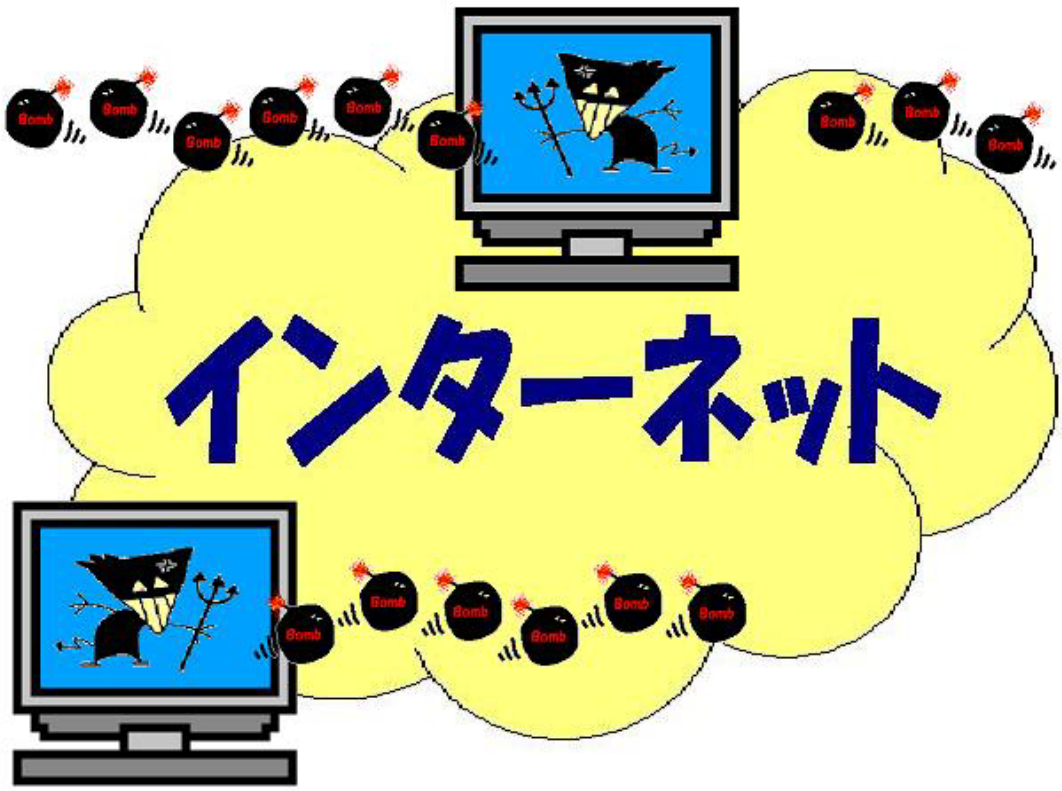
135(TCP),445(TCP)ポートへのアクセスについては、アクセス数の場合と同様に発信元数も多いことが分かります。

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。

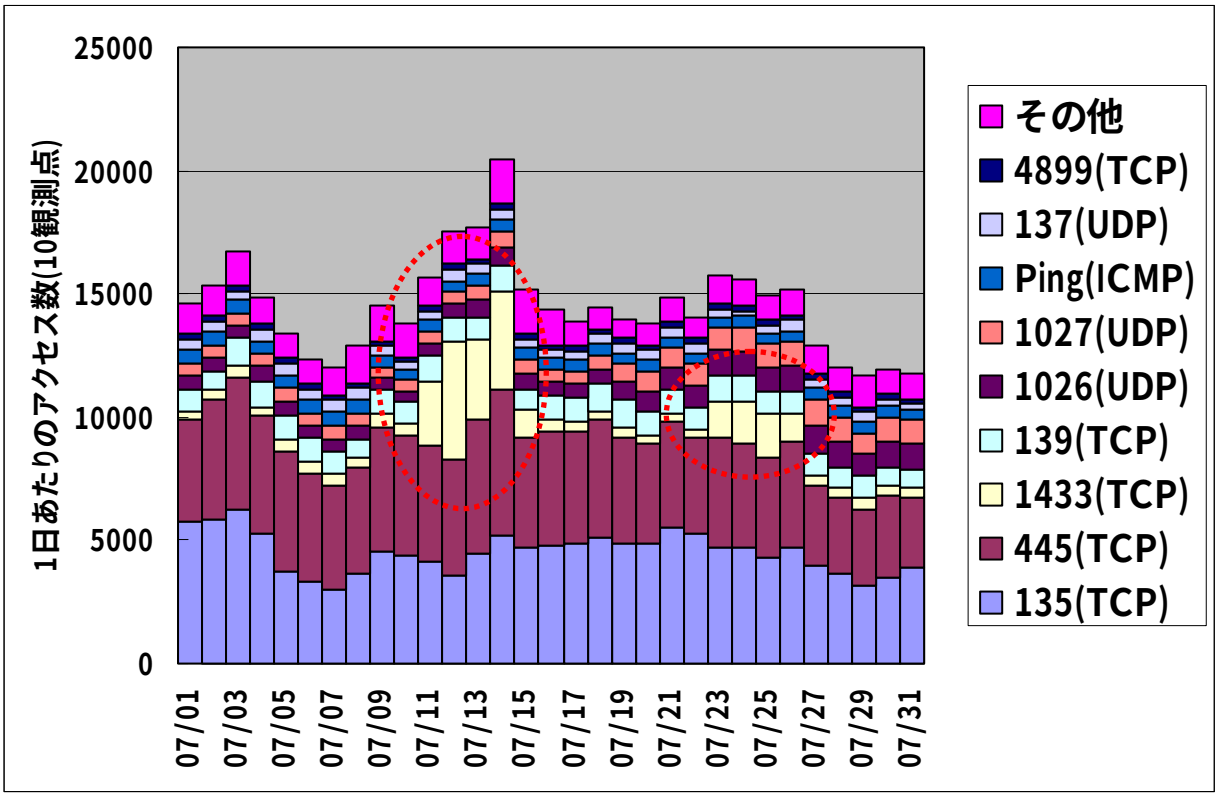
図 2.1.1 と図 2.1.2 の違いは、ちょうどウイルス発見届出での検知件数と届出件数の違いと、同じ理屈になっており、図 2.1.1 のアクセス数でのアクセス状況は実際のアクセスの脅威を示し、図 2.1.2 の発信元数でのアクセス状況からはアクセスの原因となるコンピュータ(発信元)の感染状況を示すと考えられます。

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。

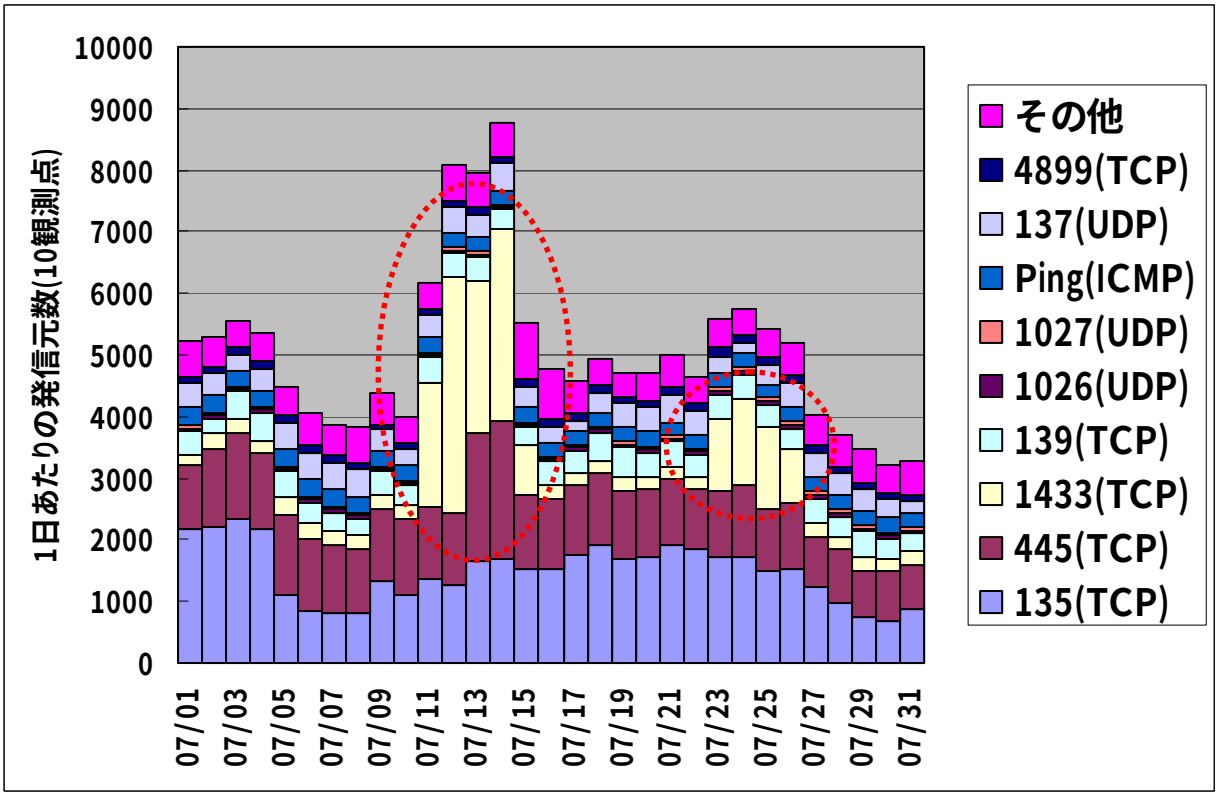
図 2.3.1 および図 2.3.2 には、発信元地域別アクセス数の変化および発信元地域別発信元数の変化を 1 日単位で示しています。



2.1 2005 年 7 月の一方的なアクセス状況



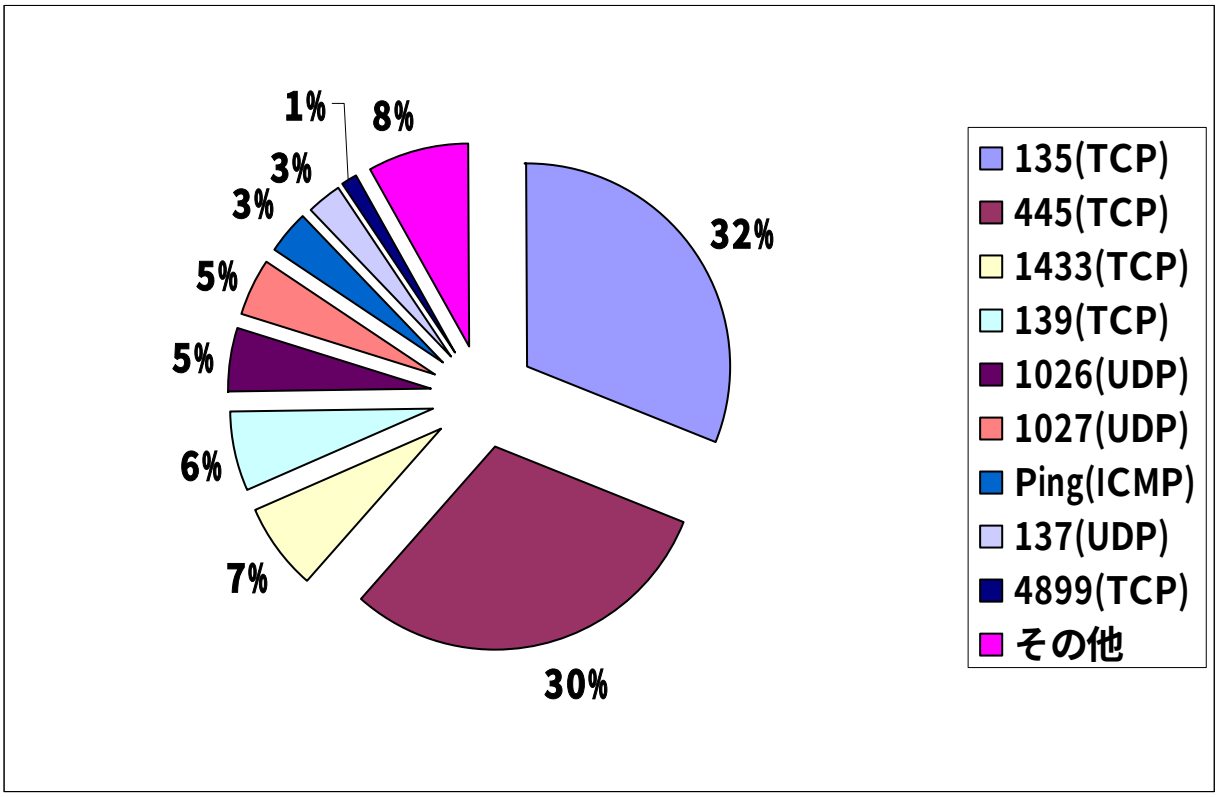
【図 2.1.1 2005 年7月の一方的なアクセス状況(アクセス数)】



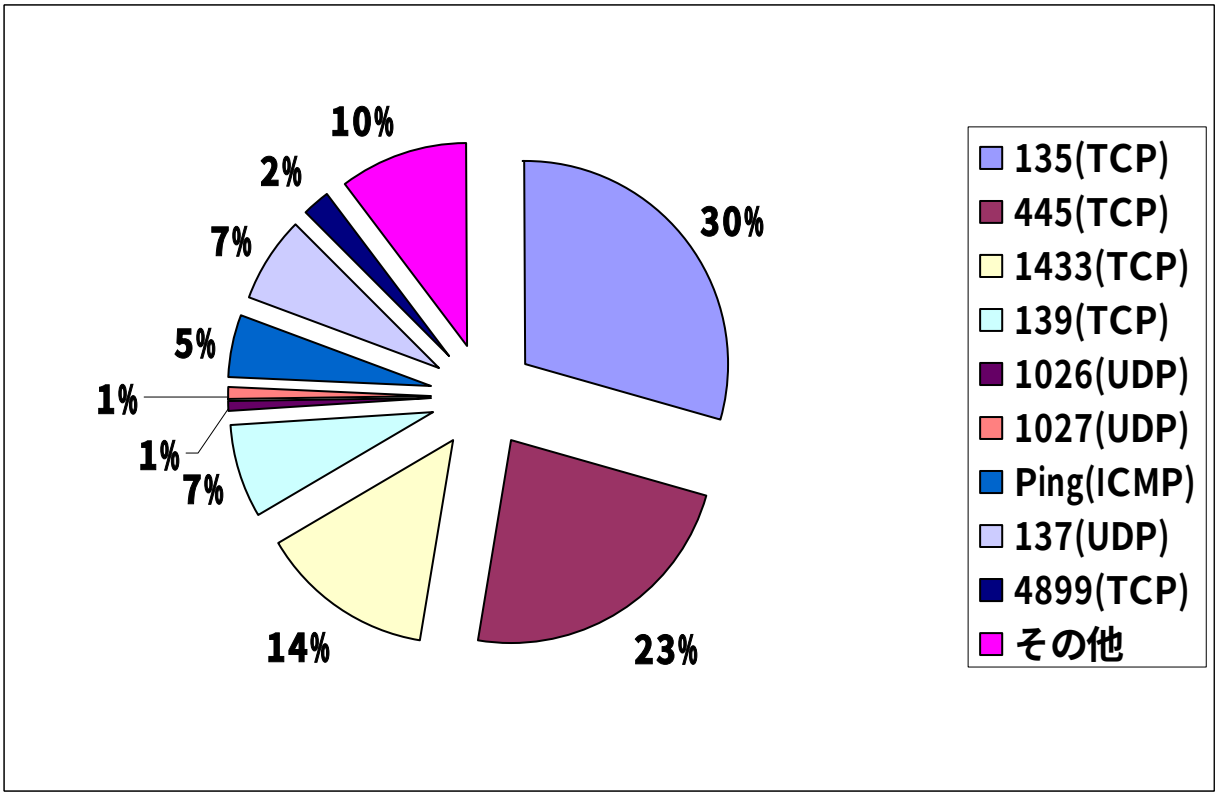
【図 2.1.2 2005 年7月の一方的なアクセス状況(発信元数)】

- 2005 年7月は図 2.1.1 や図 2.1.2 を見ても分かるとおり、1433(TCP)へのアクセスが特徴的でした(図中の赤点線)。さらに、1026(UDP)/1027(UDP)へのアクセス数も月の半ば過ぎから増加傾向でした(詳細は後述)。

2.2 2005 年 7 月の宛先(ポート種類)別の比率



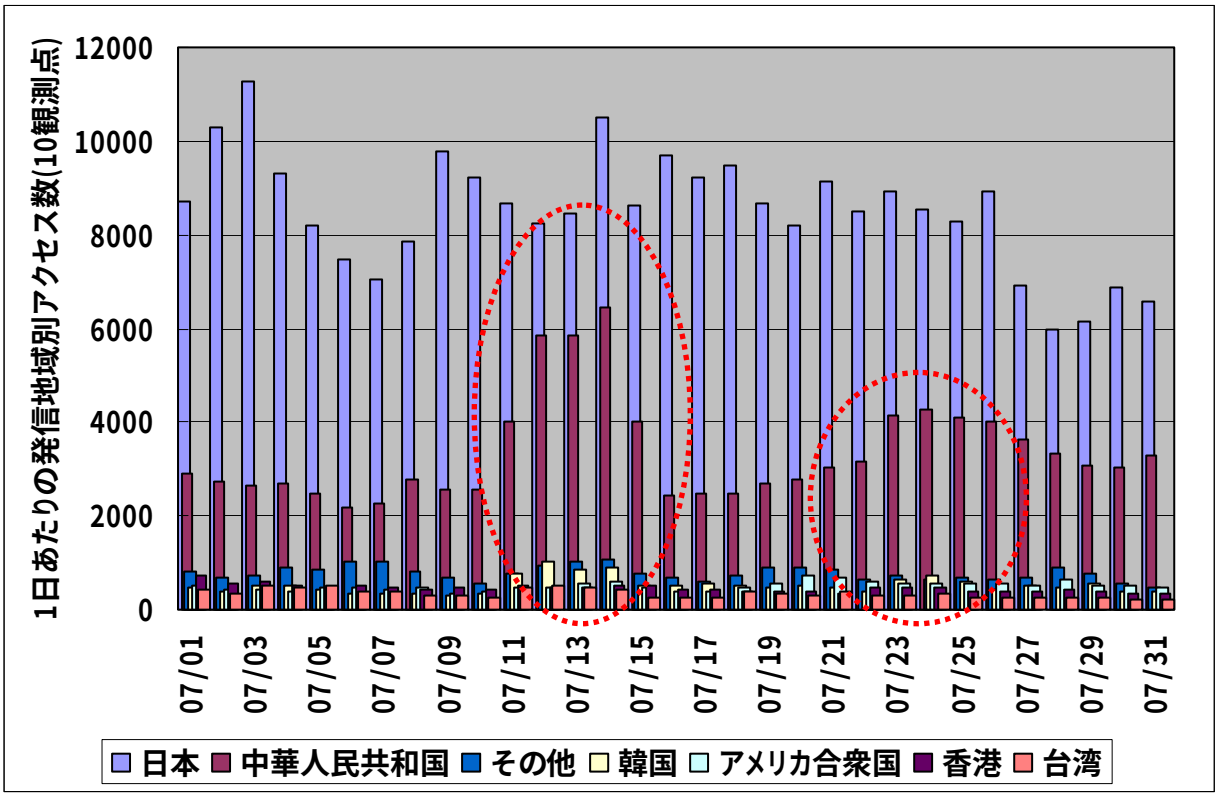
【図 2.2.1 2005 年7月の宛先(ポート種類)別アクセス数の比率】



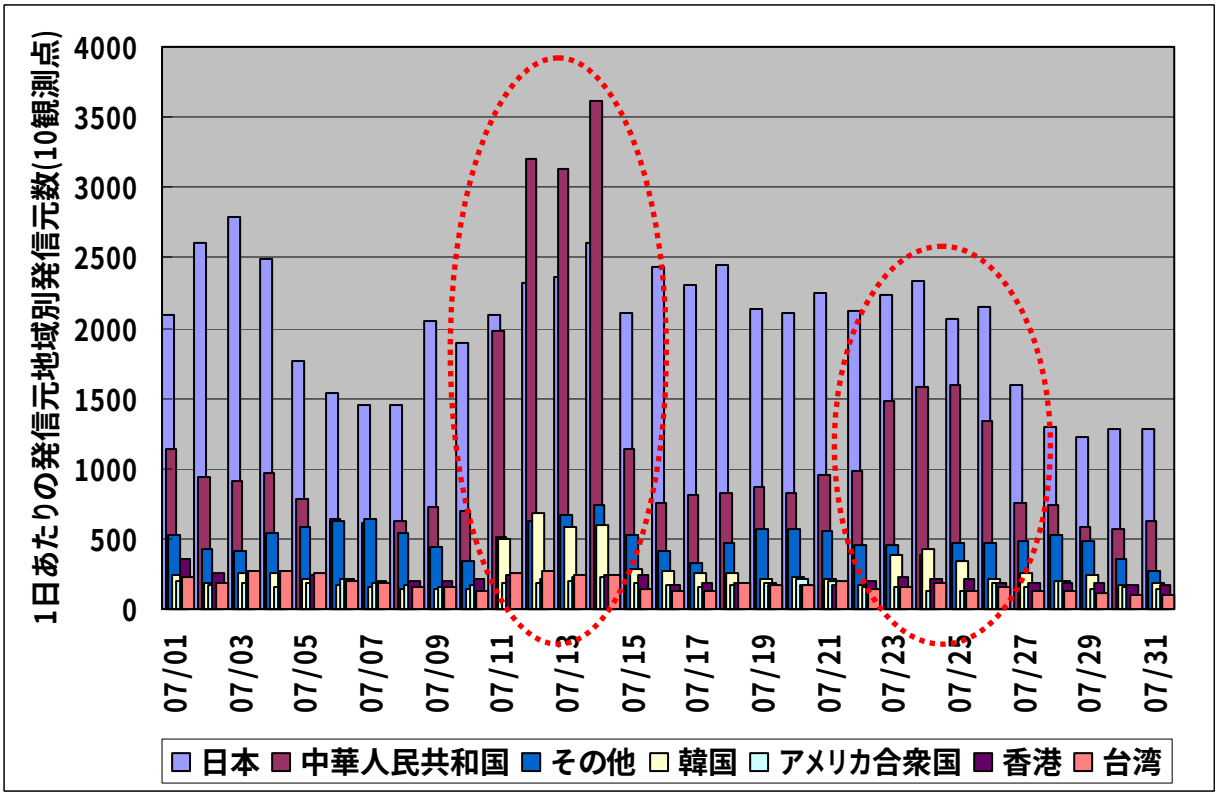
【図 2.2.2 2005 年7月の宛先(ポート種類)別発信元数の比率】

- 1026(UDP)/1027(UDP)へのアクセスについて(「**2.5 1026(UDP)/1027(UDP)ポートへのアクセスについて**」を参照下さい)、アクセス数に比べて発信元数の比率が少ないことがうかがえます。

2.3 2005 年 7 月の発信元地域別アクセス状況



【図 2.3.1 2005 年 7 月の発信元地域別アクセス数の変化】



【図 2.3.2 2005 年 7 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、1433(TCP)へのアクセス増加による中国、韓国方面からのアクセスの増加が見受けられました(図中の赤点線)。

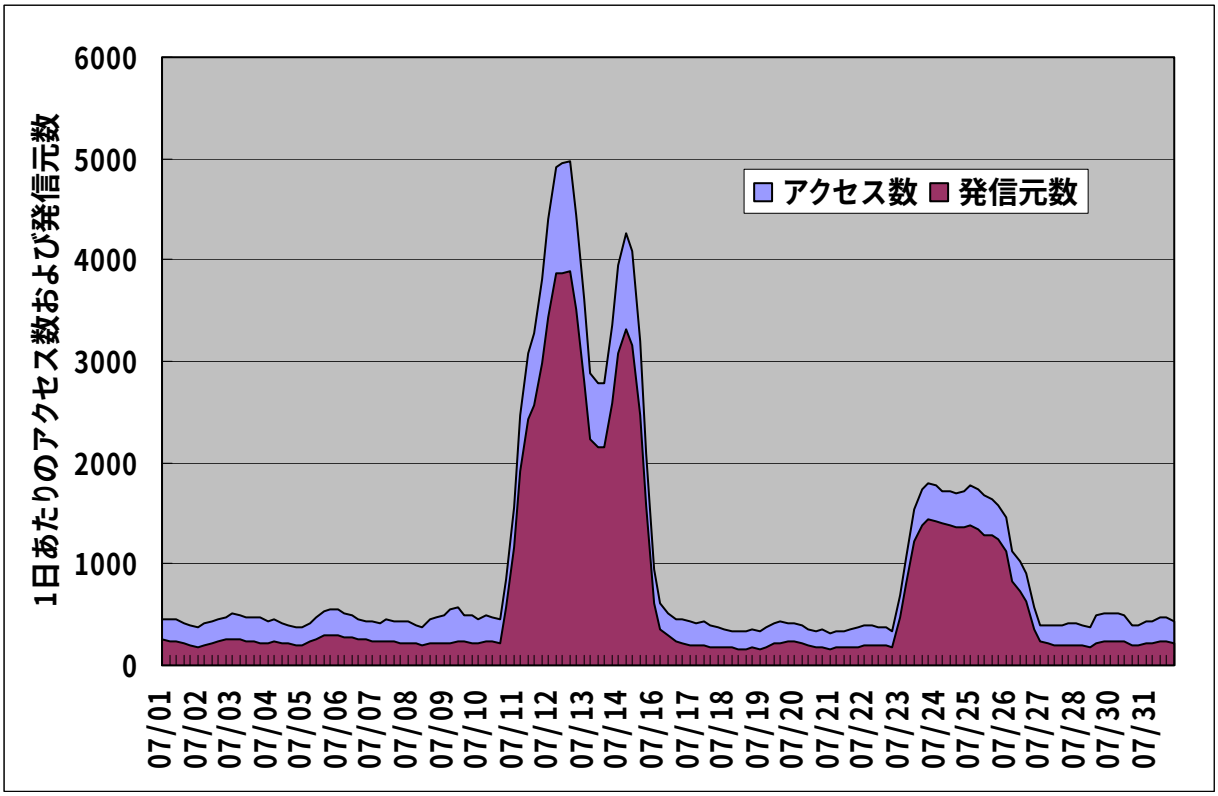
2.4 1433(TCP)ポートへのアクセスについて

2005 年 7 月 11 日～15 日までと、23 日～27 日ごろまで、1433(TCP)ポートへのアクセスが増加しました(図 2.4.1 を参照下さい)。発信元の多くは、中国、韓国方面でした(図 2.4.2 および図 2.4.3 を参照下さい)。

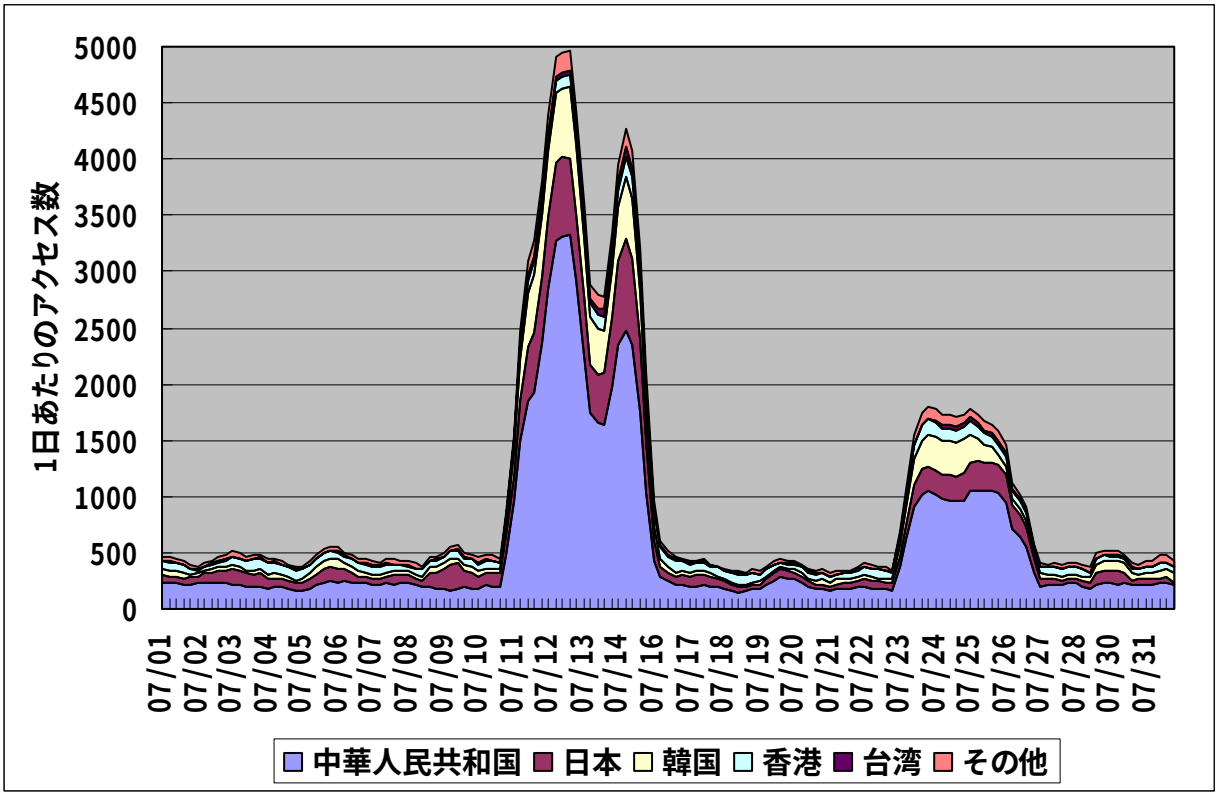
もう 1 つのインターネット定点観測システムである TALOT において、観測点に仕掛けた簡単なハニーポットでのパケットダンプ分析結果によると、Microsoft SQL サーバの何らかの脆弱性(バッファオーバーフローあるいはバッファオーバーランと呼ばれる脆弱性)を狙ったものではないかと考えられます。

国内においては、SQL サーバ絡みの攻撃が広がる気配はない(システム管理者が真面目に対応していると言うことです)ので、特に大きな問題は発生しなかったようです。この攻撃が新しい脆弱性を狙ったものであれば、当然新しいワームの発生であった可能性もあります。

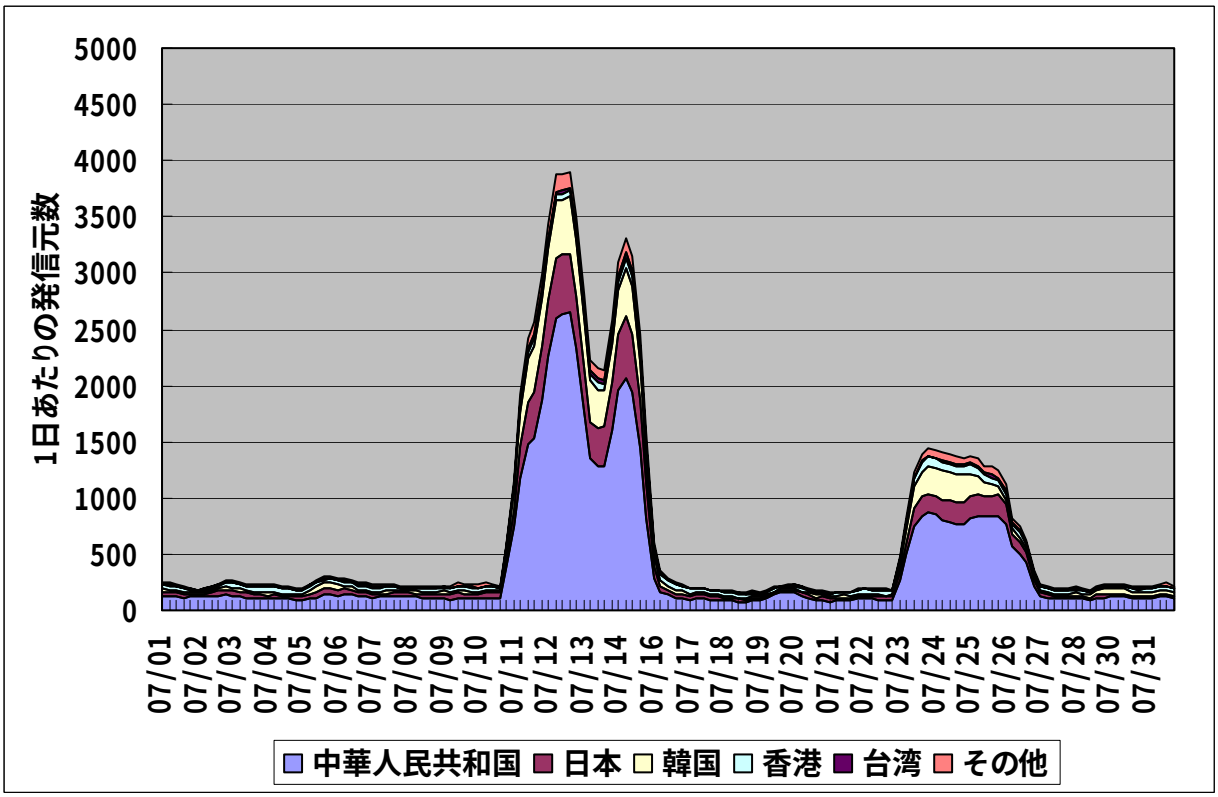
一般的に 1433(TCP)ポートが開いている状況というのは、無対策な Windows サーバをインターネットにさらした状態であり、特に中国方面で多く見受けられるという噂もあります。実際に SQL サーバが動作していなくても、関連アプリケーションがインストールされているだけで、デフォルトでポートを開いている状況が、Windows サーバにはあるようです。『サーバはデフォルト状態で利用しない』が鉄則と言うことになります。



【図 2.4.1 1433(TCP)ポートへのアクセス数と発信元数の変化】



【図 2.4.2 1433(TCP)ポートへの発信地域別アクセス数の変化】



【図 2.4.3 1433(TCP)ポートへの発信地域別発信元数の変化】

2.5 1026(UDP)/1027(UDP)ポートへのアクセスについて

2005 年 7 月半ば過ぎから、1026(UDP)および 1027(UDP)ポートへのアクセスが緩やかな増加傾向にあります。

これらのアクセスは、1026(UDP)や 1027(UDP)経由で、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。

以下の情報は、観測データ(パケットダンプ)から抽出したものです。

例 1) 中国方面からのメッセージ(1027(UDP)経由:DCE RPC)

以下、単語等は原文のまま(一部省略)

```
SECURITY ALERT

IMPORTANT NEW VIRUS OUTBREAK ALERT
YOUR COMPUTER MAY BE INFECTED BY THIS NEW VIRUS!
Name:     Korgo.BA-1
Aliases: Trojan.Korgo.BA-1
Type:      Win32 Trojan
Desc:      Key Recording Trojan
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
```

例 2) アメリカ方面からのメッセージ(1027(UDP)経由:Microsoft Messenger Service)

以下、原文のまま SYSTEM → ALERT

```
Windows has encounted an Internal Error
Your registry is corrupted.
http://*****.com
To repair your system ASAP!!
```

例 3) アメリカ方面からのメッセージ(1027(UDP)経由:Microsoft Messenger Service)

以下、原文のまま SECURITY → ALERT

```
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. Ru ...
```

例 4) 中国方面からのメッセージ(1026(UDP)経由:Microsoft Messenger Service)

以下、原文のまま SYSTEM → ALERT

```
Windows has encountered an Internal Error
Your Windows registry is corrupted.
An Immediate system scan is recommended.
visit
http://www.**********.com
to repair.
```

画面表示サンプル

2005 年 3 月下旬から徐々にアクセス数を増加させてきた 1026(UDP)および 1027(UDP)へのアクセスは、5 月初旬に倍増のステップを踏んだ後、定常的にアクセスが行われていました。
2005 年 7 月に入って、20 日頃から、アクセス数が増加しています（図 2.5.1 の赤点線部分を参照下さい）。発信元数の変化のグラフ(図 2.5.2 の赤点線部分を参照下さい)からは、発信元が直線的に増加しているのが分かります。

ここで示す全ての 1026(UDP)および 1027(UDP)へのアクセスが、上に示したポップアップメッセージを送信しているものであるかは、全てを検証したわけではないので明言できませんが。ほとんどは、そうであると思われます。

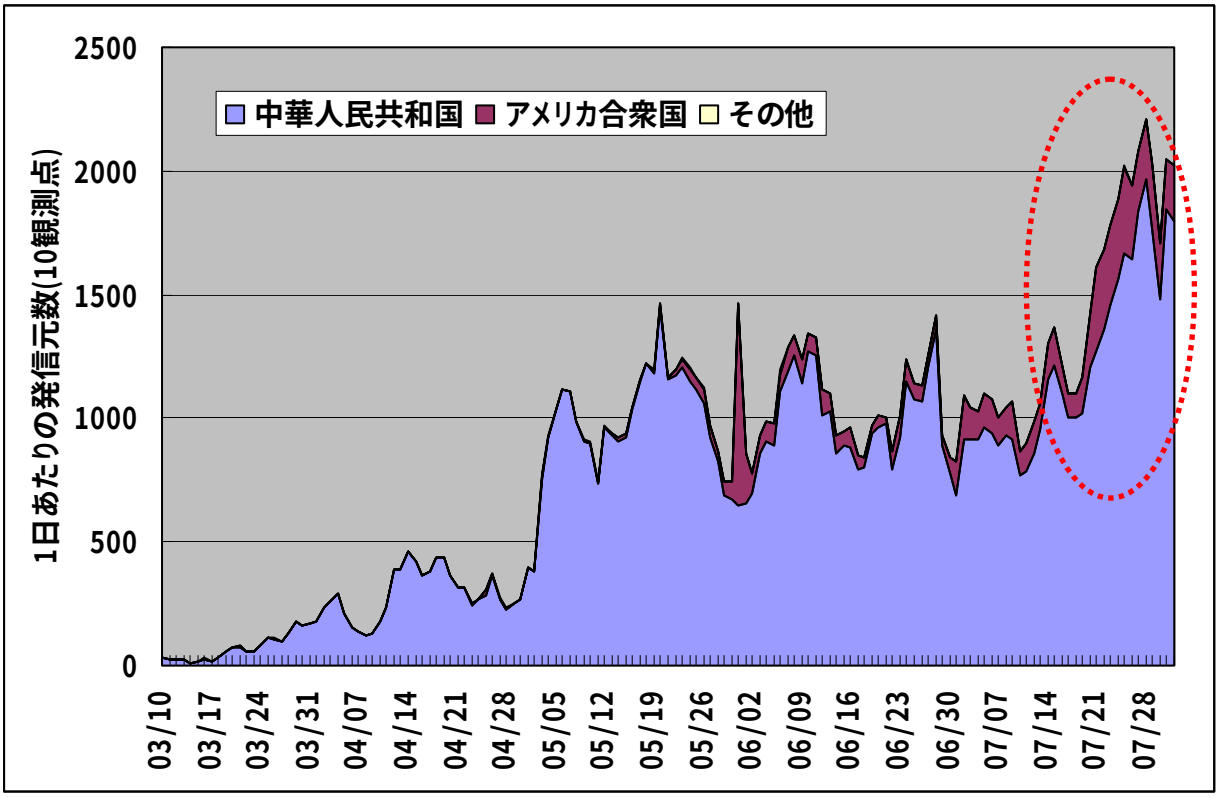
これらのポップメッセージがコンピュータの画面に表示される原因は、そのコンピュータがグローバルアドレスでインターネットに接続されている場合です。さらに、Messenger サービスが動作している場合となります。

一般的に、上記の 2～4 の例の Windows Messenger Service は、閉じた LAN の中で、サーバとクライアント間でのメッセージ表示に使われるサービスであり、システム管理者がサーバの状況をクライアントに伝える場合に使われます（net send コマンドの使用）。

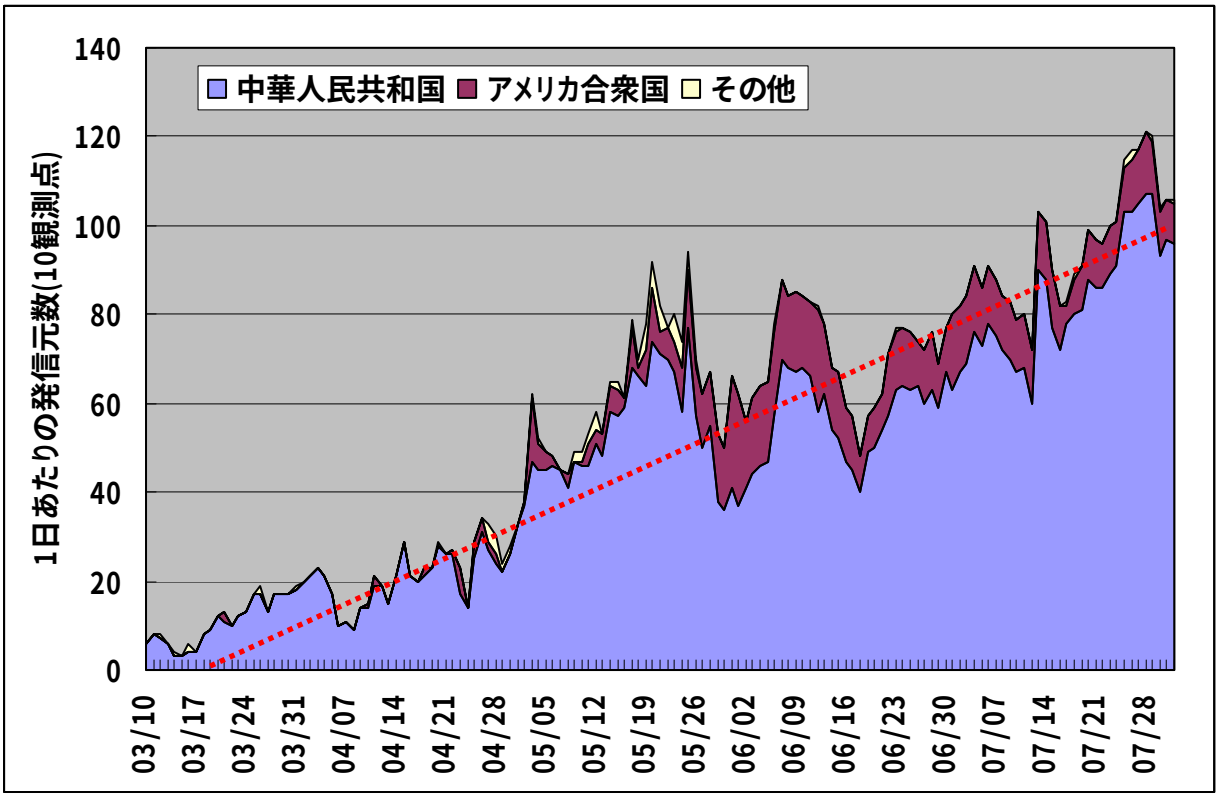
一方的にインターネットから送られてきたメッセージ(スパムメッセージのようなもの)なので、無視すれば問題はありませんが、不正なアクセスであることにかわりがありません。メッセージ中には具体的な操作指示が書かれていますが、従わないで下さい。表示された画面やダイアログ(プロンプト)ボックスは、×ボタンで終了して下さい。

表示させたくなければ、インターネット側(WAN 側)からの 1026 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。



【図 2.5.1 1026(UDP)+1027(UDP)ポートへの発信元地域別アクセス数の変化】



【図 2.5.2　1026(UDP)+1027(UDP)ポートへの発信元地域別発信元数の変化】

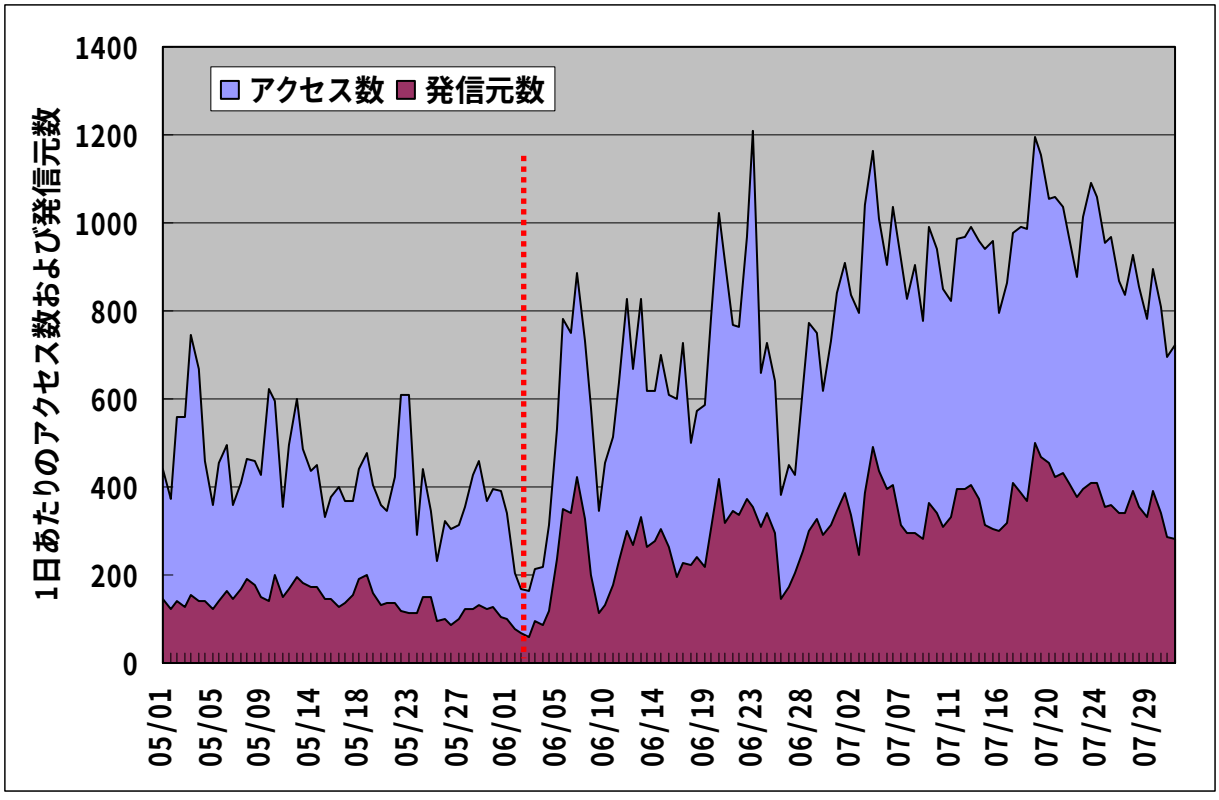
　これらのアクセスの発信元は、ほとんどが中国方面およびアメリカ方面のものであり、メッセージの中には、悪意のあるサイトへの誘いがあるものも予想されます。ご注意下さい。

2.6 139(TCP)ポートへのアクセスについて

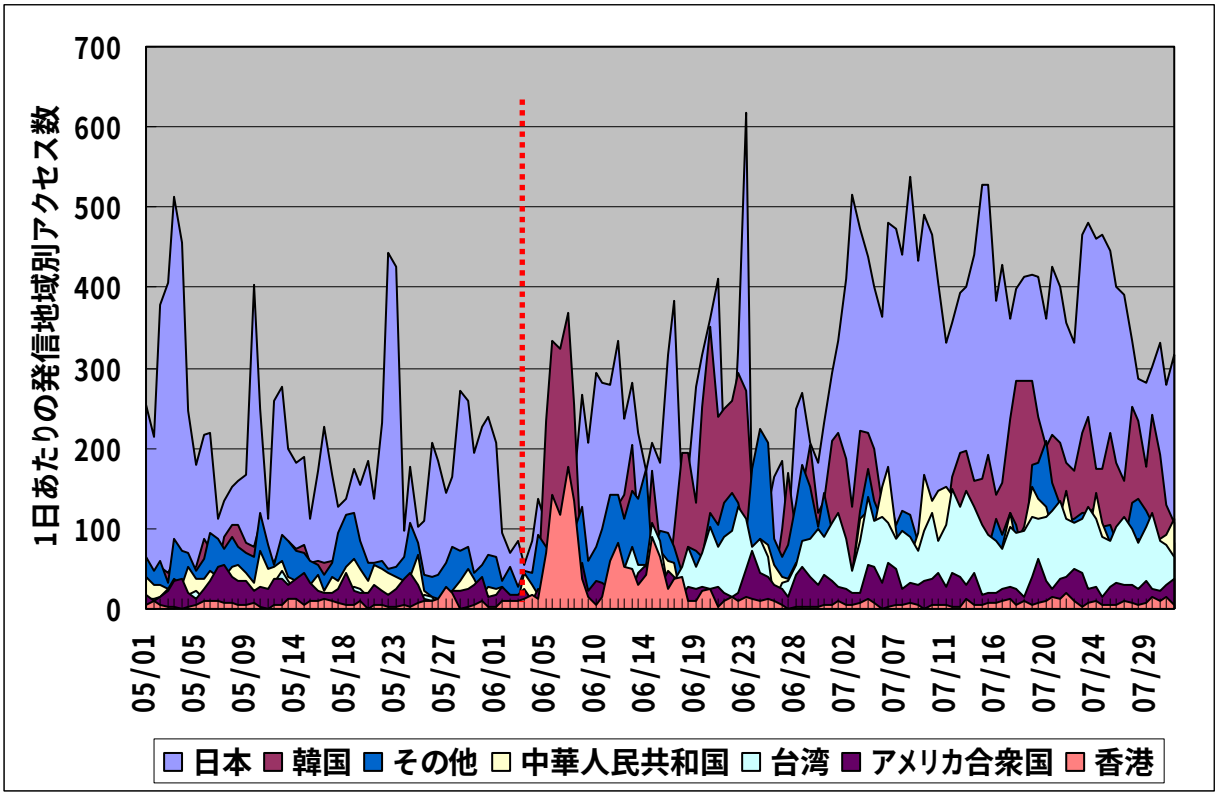
2005 年 6 月 5 日頃から、韓国、香港、台湾方面からの 139(TCP)ポートへのアクセスが増加しています。図 2.6.1 に 2005 年 5 月から 7 月にかけての 139(TCP)ポートへのアクセス数と発信元ＩＰ数を、図 2.6.2 に同期間の発信地域別のアクセス数の変化を、図 2.6.3 に同期間の発信地域別の発信元数の変化を示していますが、5 月の状況と 6 月～7 月の状況の変化(赤点線が境界)が良く見て取れます。

このアクセスは、Windows 系のファイル共有への不正アクセスと思われます。一般的には、139(TCP)ポートをインターネット側（WAN 側）には開いていないと考えられますが、万が一このポートを WAN 側に開いている場合は注意が必要です。ファイル共有のためのアクセス制御(特にパスワード設定等)があまいと、管理者権限を奪取され、コンピュータへ侵入される可能性があります。

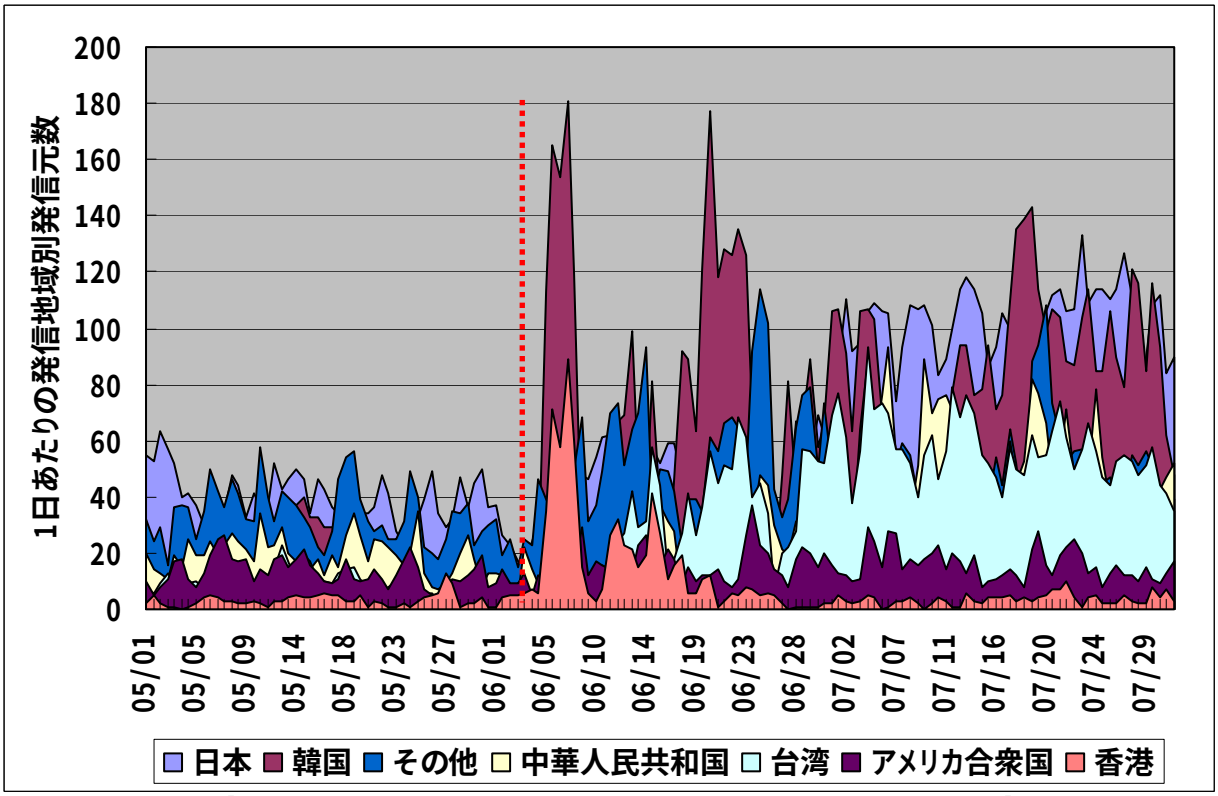
極端なアクセス数の増加ではありませんが、連続するＩＰアドレスを持つＴＡＬＯＴの観測では、連続する観測点に、アドレスを総ナメするようにアクセスが観測されていますので、システム管理者は、今一度 WAN 側のポートの開閉状況あるいはファイアウォールの設定を確認する必要があると思われます。



【図 2.6.1 139(TCP)ポートへのアクセス数と発信元数の変化】



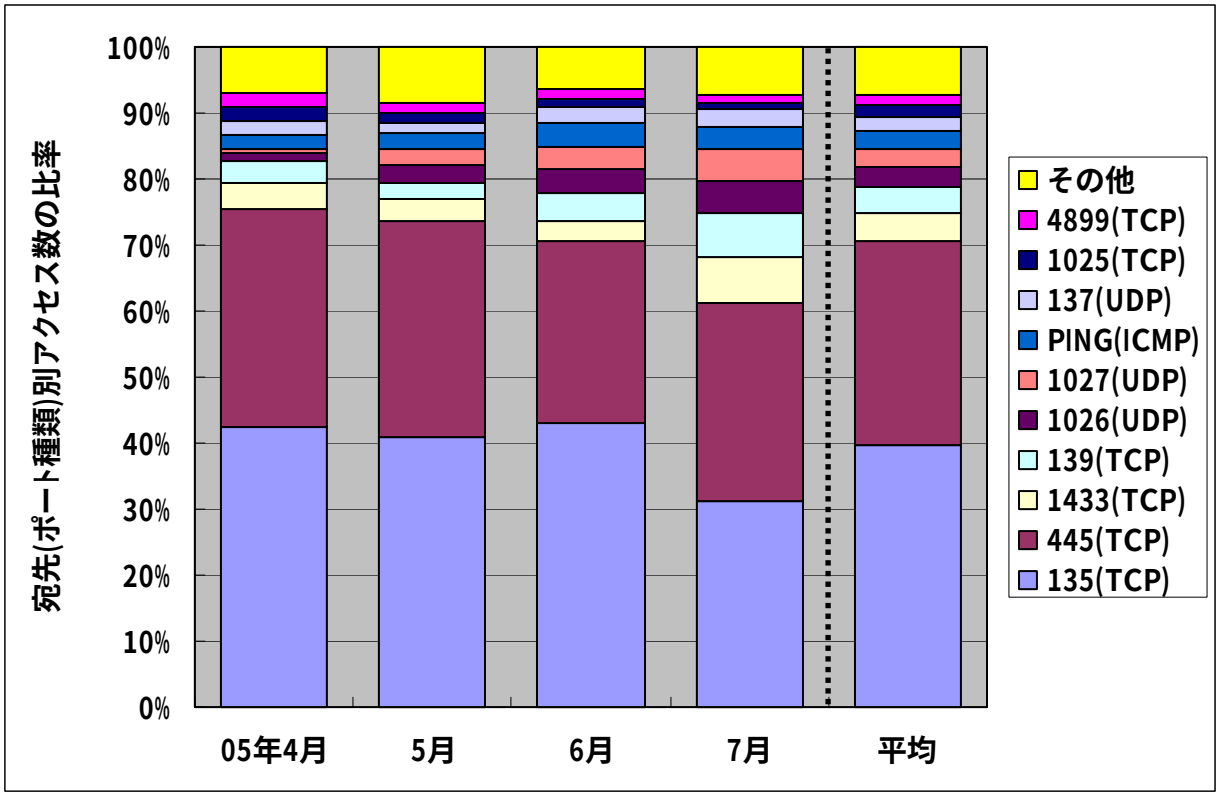
【図 2.4.2 139(TCP)ポートへの発信地域別アクセス数の変化】



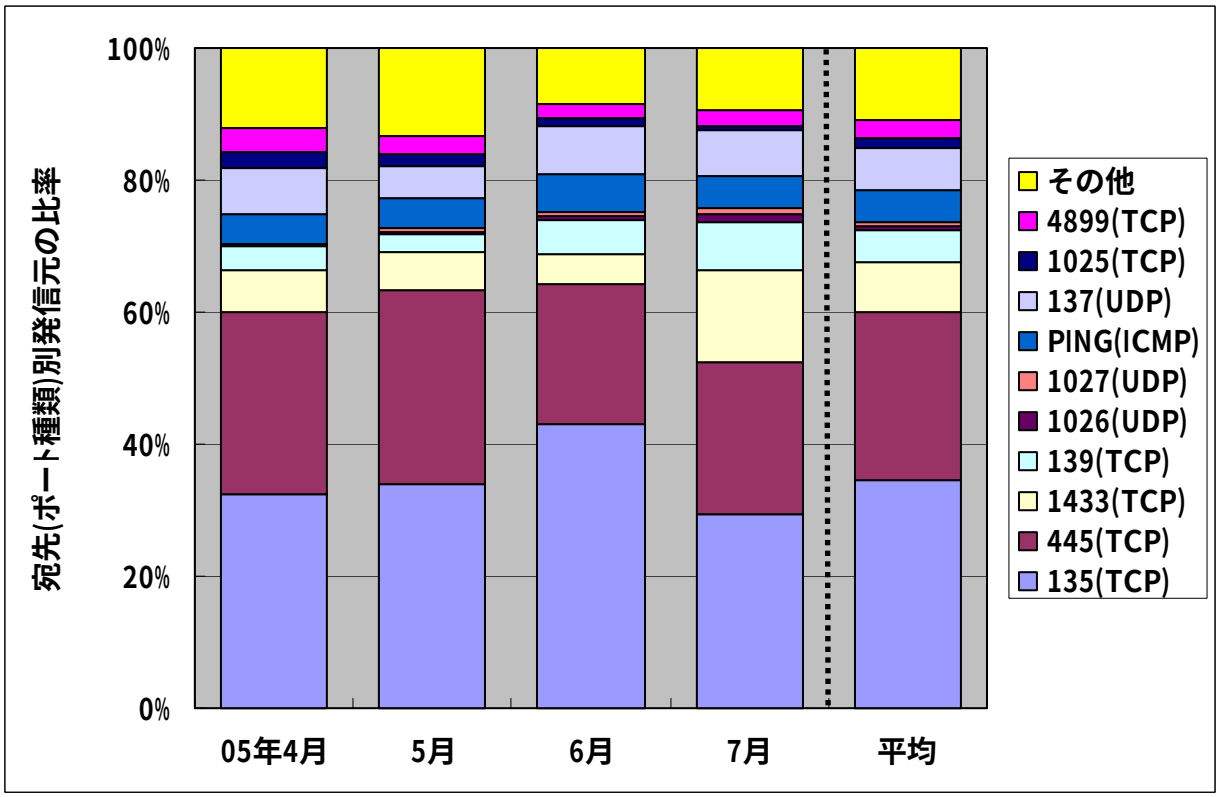
【図 2.4.3 139(TCP)ポートへの発信地域別発信元数の変化】

3．統計情報

3.1 2005 年 4 月～7 月の宛先(ポート種類)別の比率

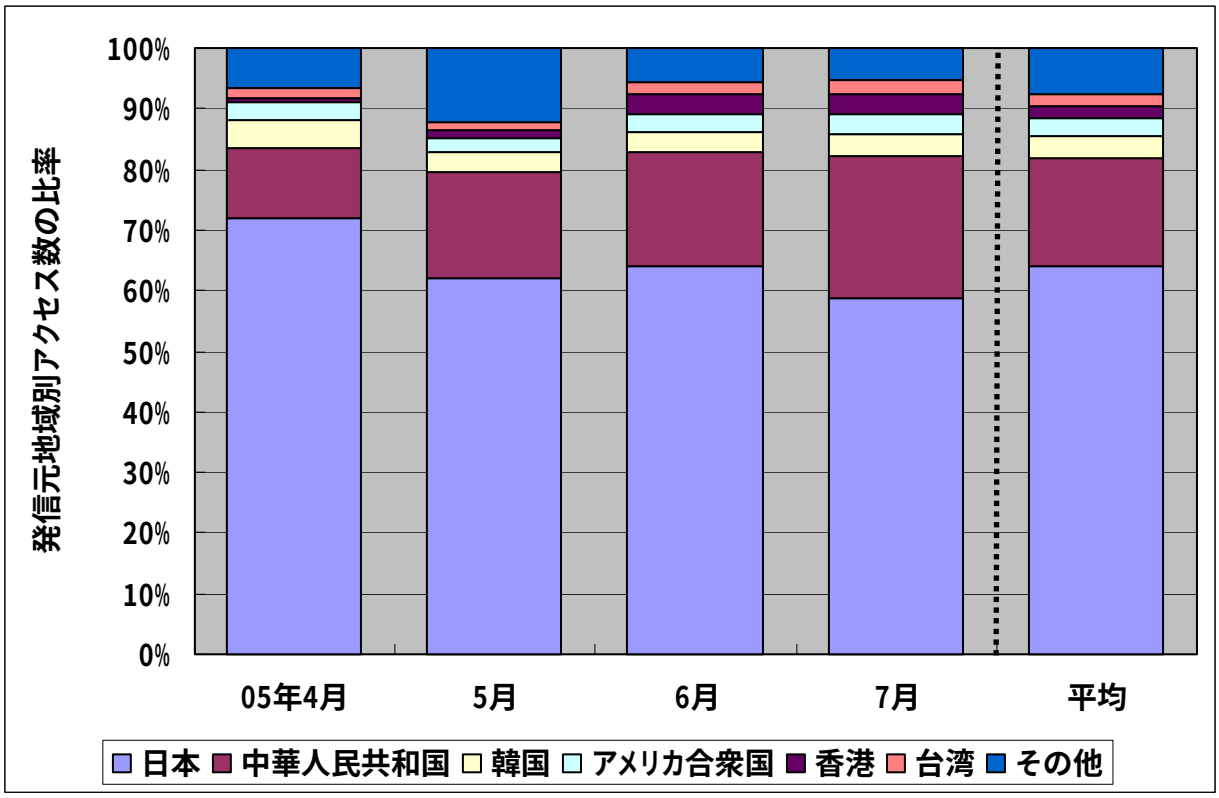


【図 3.1.1 2005 年 4 月～7 月の宛先(ポート種類)別アクセス数の比率】

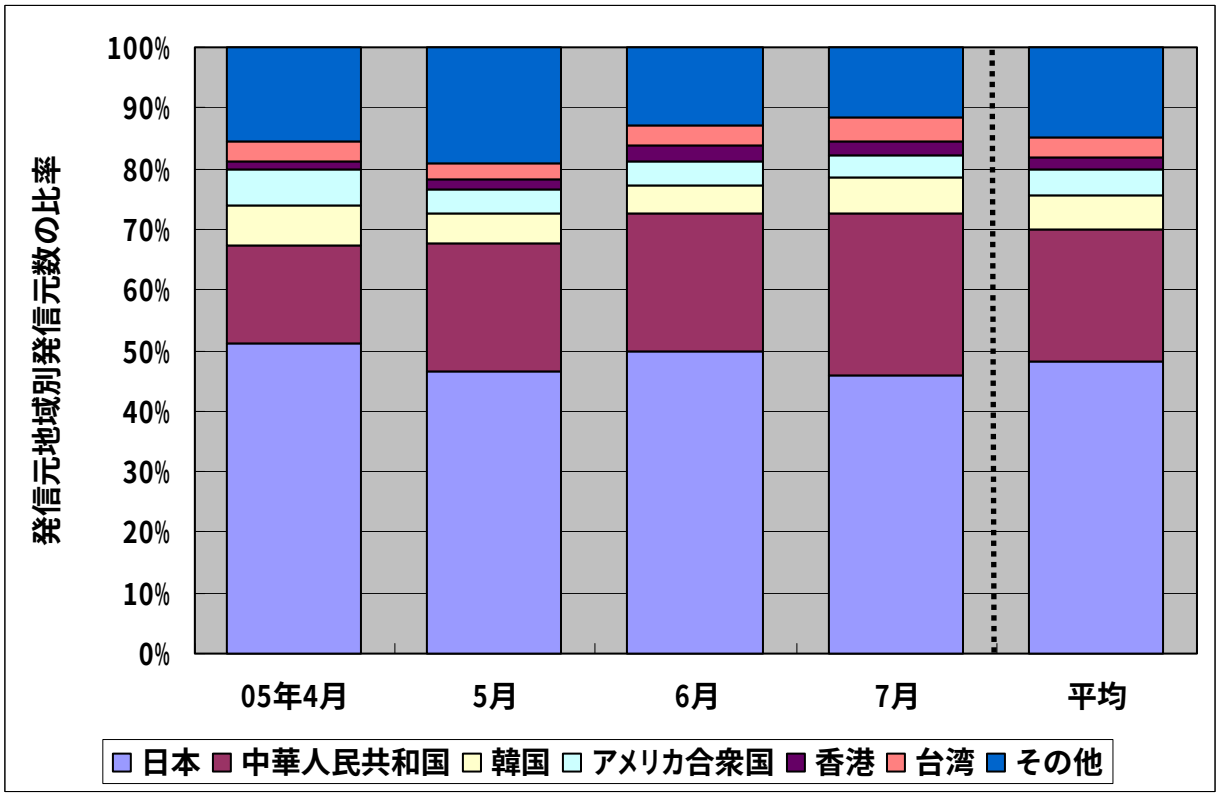


【図 3.1.2 2005 年 4 月～7 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 4 月～7 月の発信元地域別の比率



【図 3.2.1 2005 年 4 月～7 月の発信元地域別アクセス数の比率】



【図 3.2.2 2005 年 4 月～7 月の発信元地域別発信元数の比率】

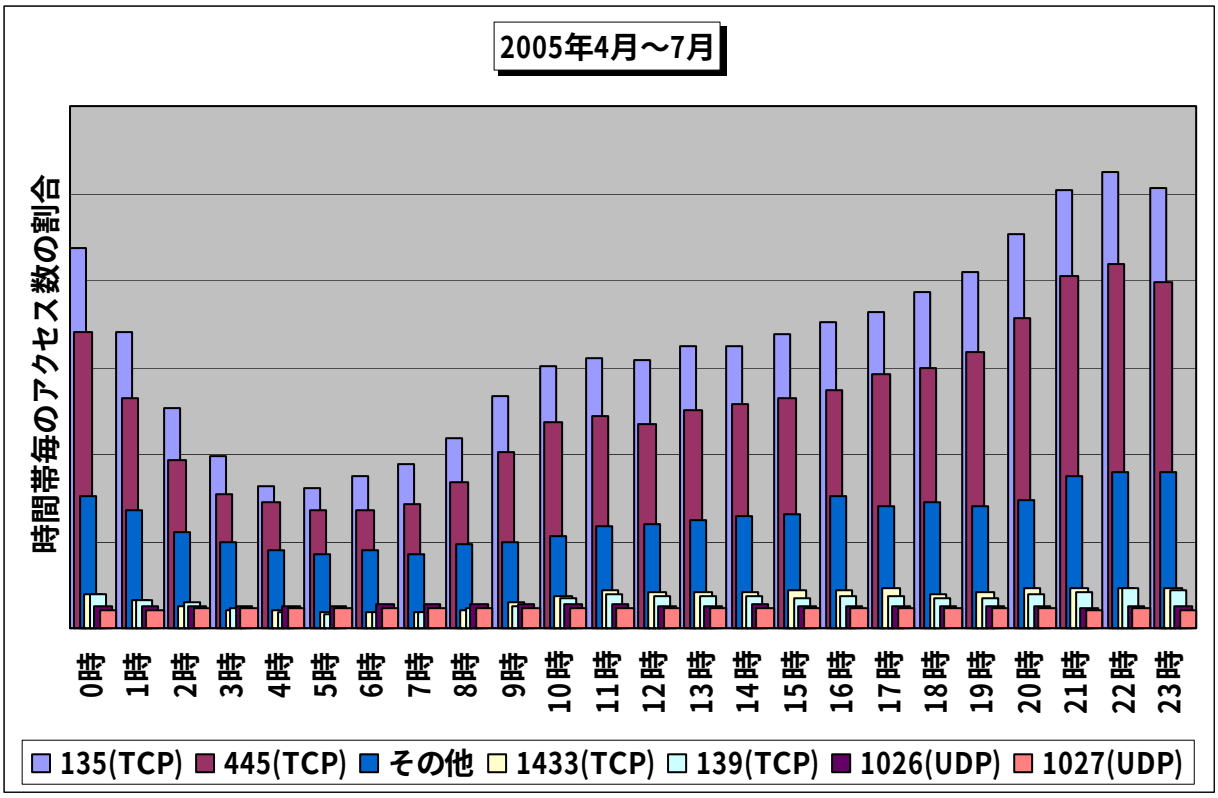
4．その他の統計情報

4.1 2005 年 4 月～7 月の時間帯統計

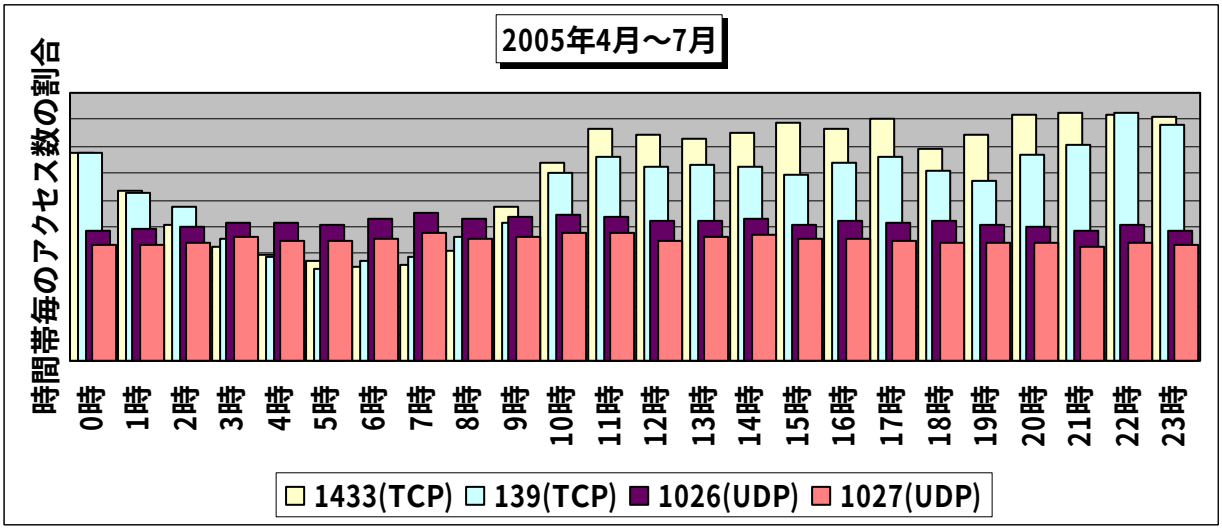
2005 年 4 月～7 月の宛先(ポート種類)別アクセス数の時間帯統計を図 4.1.1 に示します。

「2.5　1026(UDP)/1027(UDP)ポートへのアクセスについて」に記述した 1026(UDP)および 1027(UDP)へのアクセスは、図 4.1.1 あるいは図 4.1.2 を見る限り、時間帯による変動はありません。これらのアクセスの発信元は、常に動作しており、不正なメッセージを放出し続けていると言うことになります。

135(TCP)や 445(TCP)へのアクセスについては、時間帯による変動があり、コンピュータ利用者の生活リズムにあっているような雰囲気です。午前中よりも夕方から夜中にかけてアクセス数が増加するのは、これらのアクセスを行っているコンピュータのユーザは、企業ユーザではなく、一般ユーザを示しているのかも知れません。



【図 4.1.1 2005 年 4 月～7 月の宛先(ポート種類)別アクセス数の時間帯統計】

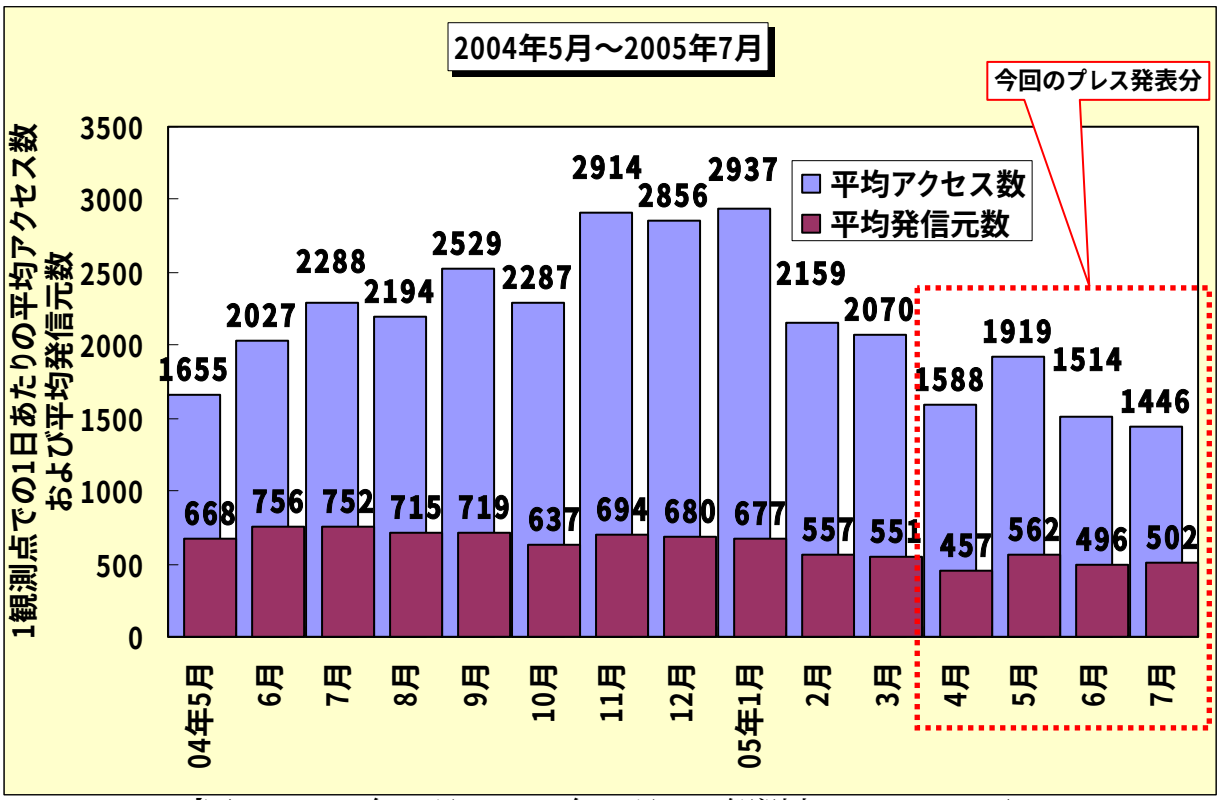


【図 4.1.2 2005 年 4 月～7 月の宛先(ポート種類)別アクセス数の時間帯統計(抜粋)】

4.2 参考情報

現在の、期待しない（一方的な）アクセスの状況を補足するために、TALOT2 での観測が始まった 2004 年 5 月から現在までの、1 観測点での 1 日あたりの平均アクセス数と平均発信元数を図 4.2 に示します。

2005 年 1 月がアクセス数のピークで、現在は、観測開始以来の最小値を示しています。少なくとも、年初に比べると状況が好転していると考えられますが、アクセスの種類(内容)は時々で変化しており、安心できる状況に向かっているかは明言できません。



【図 4.2 2004 年 5 月～2005 年 7 月の 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】

インターネットを利用される際は、ご自身の接続環境を理解し、それぞれの接続に適したコンピュータや接続機器の設定、ならびにコンピュータを常に最新の状態に保つ処置を、継続的に実施することをお勧めします。

最も危険な接続は、インターネットにグローバル IP アドレスで、コンピュータを直接接続した状態であり、一般的には、モデムによる接続形態であると言われています。同じように、不特定多数の利用者のいる無線 LAN スポットでの接続も、注意が必要です。

また、企業内で利用されているコンピュータを、企業から持ち出して使用する場合も注意が必要です。特に、ファイル共有を利用されている場合は、持ち出しの際に設定変更を行うことをお勧めします。

■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