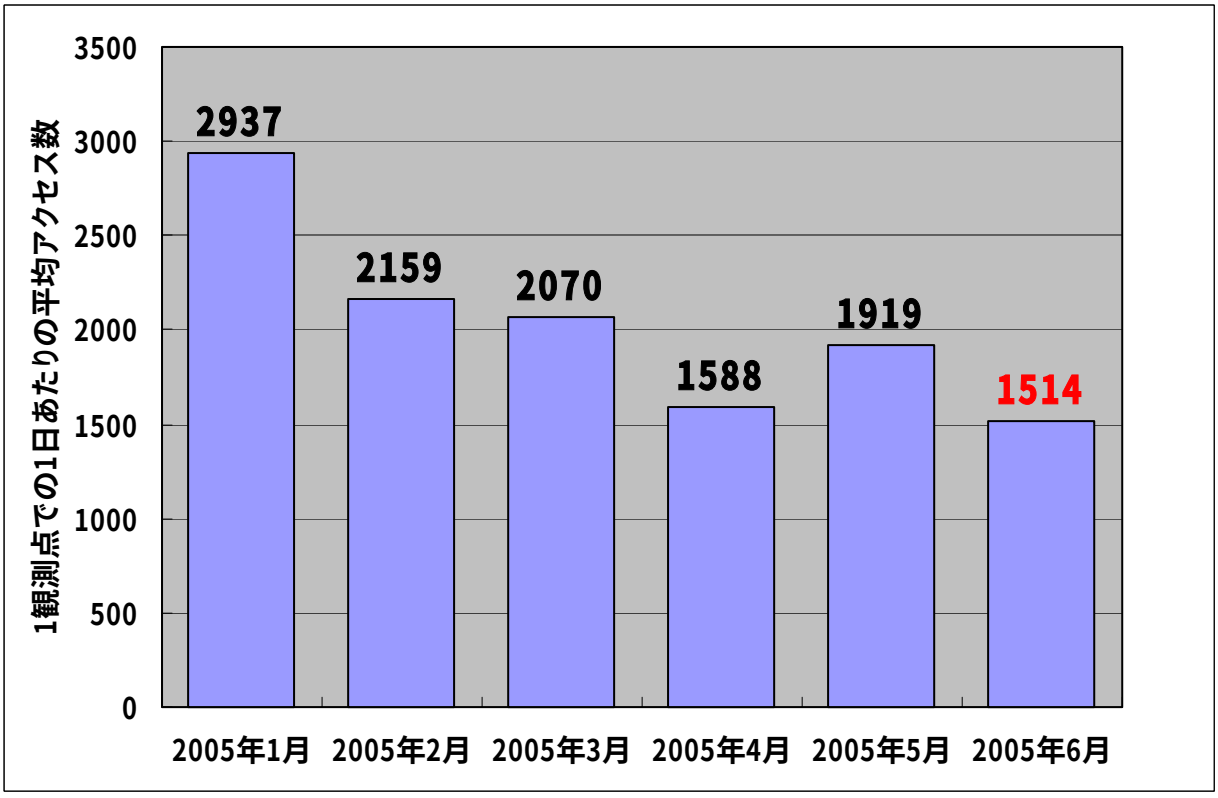
別紙 5

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 6 月の期待しない（一方的な）アクセスの総数は、10 観測点で **454,153 件**ありました。1 観測点で 1 日あたり**約 1,500 件**のアクセスがあったことになります。

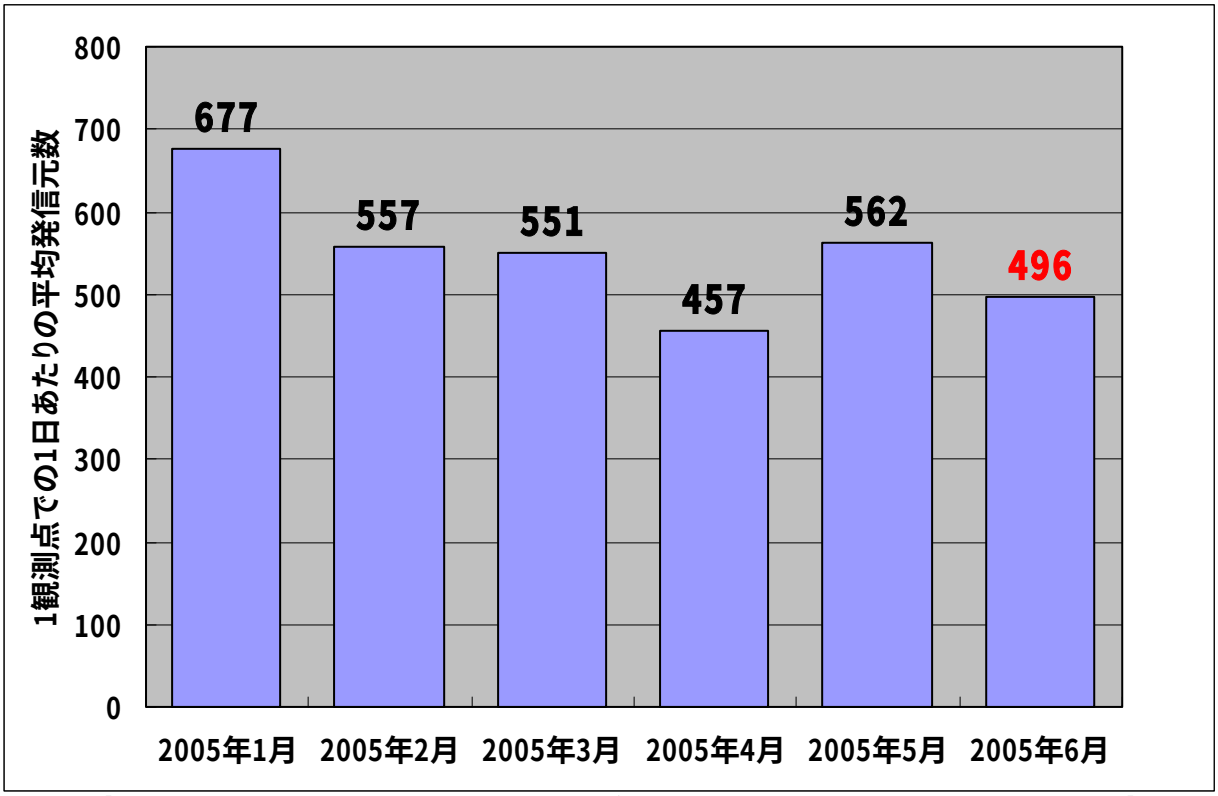
TALOT2 での1観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。



【図 1.1　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】

2005 年 3 月～6 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を図 1.1 に、それらのアクセスの平均発信元数を図 1.2 に示しています。これらの図を見ると、2005 年 5 月に比べて 2005 年 6 月はアクセス数および発信元数が減少し、2005 年 4 月の状況に戻ったようです。

5 月の 1433(TCP)へのアクセスや 445(TCP)へのアクセス増加がなければ、5 月のアクセス数や発信元数も 4 月や 6 月と同レベルであったと思われ、2005 年 1 月からの緩やかな減少傾向が下げ止まったような状況です。



【図 1.2　1 観測点での 1 日あたりの期待しない(一方的な)アクセスの発信元数】

これらの一方的なアクセスが最も脅威となるのは、コンピュータを無防備な状態（ルータ(*1)やファイアウォール機器で守られていない状態）でインターネットに直結した場合です。
止むを得ず直結する場合は、つなぐ前に、以下に示す対策を、必ず実施してください。

- **OS にファイアウォール機能が搭載されている場合は、その機能を正しく動作させる**
- **OS にファイアウォール機能が搭載されていない場合は、できる限り、パーソナルファイアウォール(*2)アプリケーションを導入し、正しく動作するように設定する**
- **コンピュータの OS やアプリケーションを最新の状態にする(例えば Windows Update の実施)**
- **不必要なファイル共有指定を外す**

同じように、不特定多数の利用者が使う無線 LAN ホットスポットやサービスで提供されるビジネスホテル等での LAN への接続の場合も、接続する LAN のセキュリティ設定が不明であったり、利用者の中に不心得者がいたりする可能性もあり、とても危険です。前述の対策は、このような場合も有効なので、必ず実施して下さい。

Microsoft Windows のユーザであれば、以下のサイトが参考になります。
■個人ユーザ向けセキュリティ：ウイルスとワーム

http://www.microsoft.com/japan/athome/security/viruses/default.mspx

---

(*1) ルータ(router)
ルータは、異なるネットワーク同士を相互接続するネットワーク機器です。一般利用者が、家庭等でインターネットを利用する場合、自身のパソコンを外部のネットワーク(プロバイダ)と繋ぐわけですが、この際にルータを使用すると、外部のネットワークと自身のコンピュータ(ネットワーク)を明確に区分けできるようになります。ルータについては、2005年3月のプレスリリースの以下の資料を参照下さい。
http://www.ipa.go.jp/security/txt/2005/documents/TALOT-0503.pdf

(*2) パーソナルファイアウォール(personal firewall)
エンドユーザが使用するパーソナルコンピュータ上で、インターネットからの不正なアクセスやワームによる攻撃を防ぐために導入するソフトウェアです。

2．6月のアクセス状況

2005 年 6 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。6 月の特筆すべきアクセスは、139(TCP)へのアクセスと 10000(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。

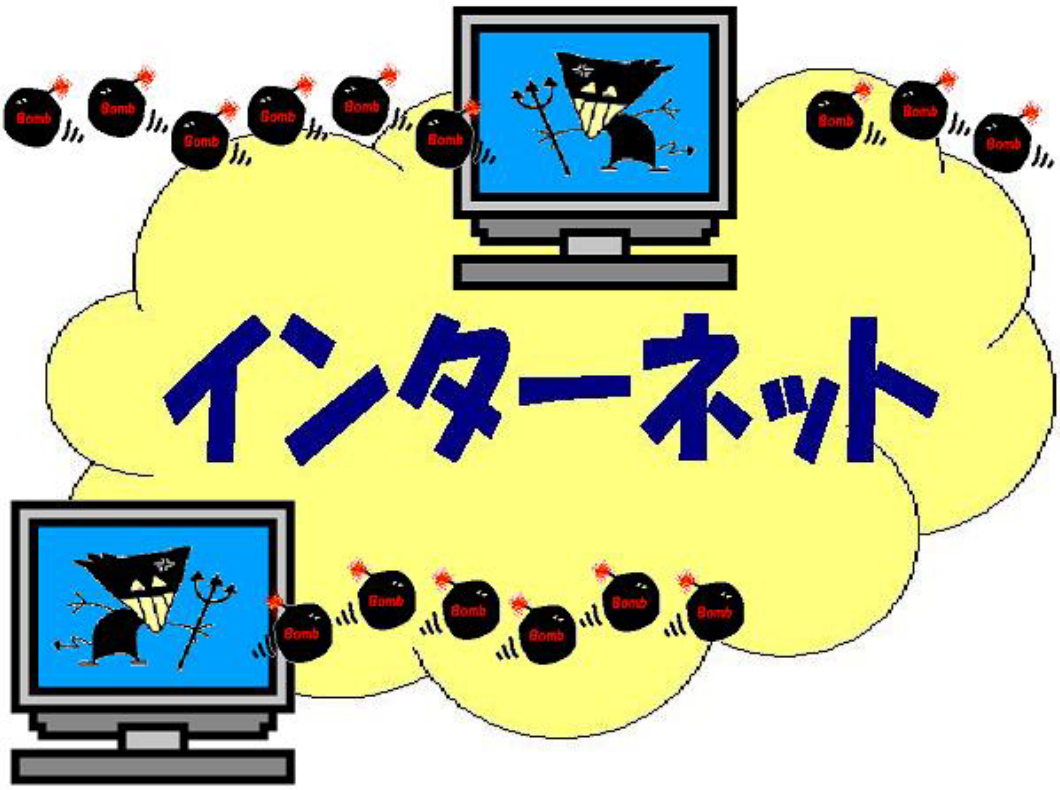
135(TCP),445(TCP)ポートへのアクセスについては、アクセス数の場合と同様に発信元数も多いことが分かります。

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。

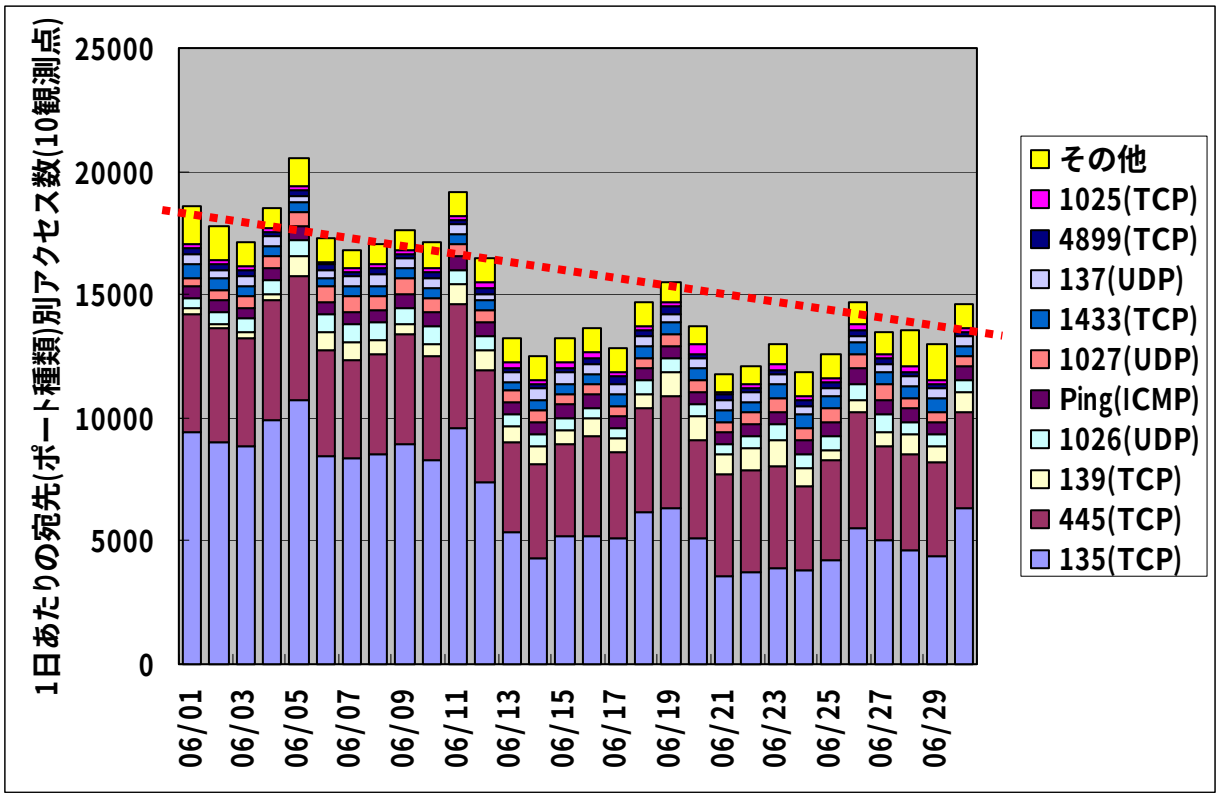
図 2.1.1 と図 2.1.2 の違いは、ちょうどウイルス発見届出での検知件数と届出件数の違いと、同じ理屈になっており、図 2.1.1 のアクセス数でのアクセス状況は実際のアクセスの脅威を示し、図 2.1.2 の発信元数でのアクセス状況からはアクセスの原因となるコンピュータ(発信元)の感染状況を示すと考えられます。

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。

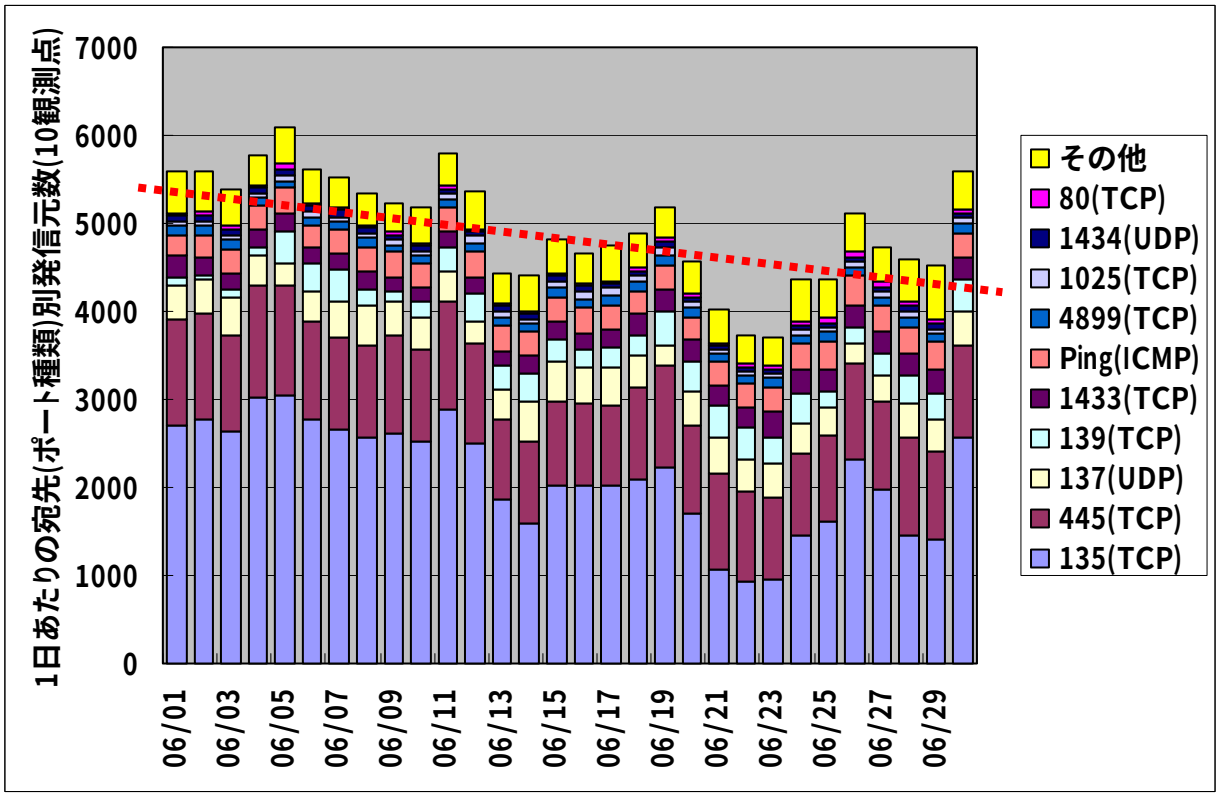
図 2.3.1 および図 2.3.2 には、発信元地域別アクセス数の変化および発信元地域別発信元数の変化を 1 日単位で示しています。



2.1 2005 年 6 月の一方的なアクセス状況



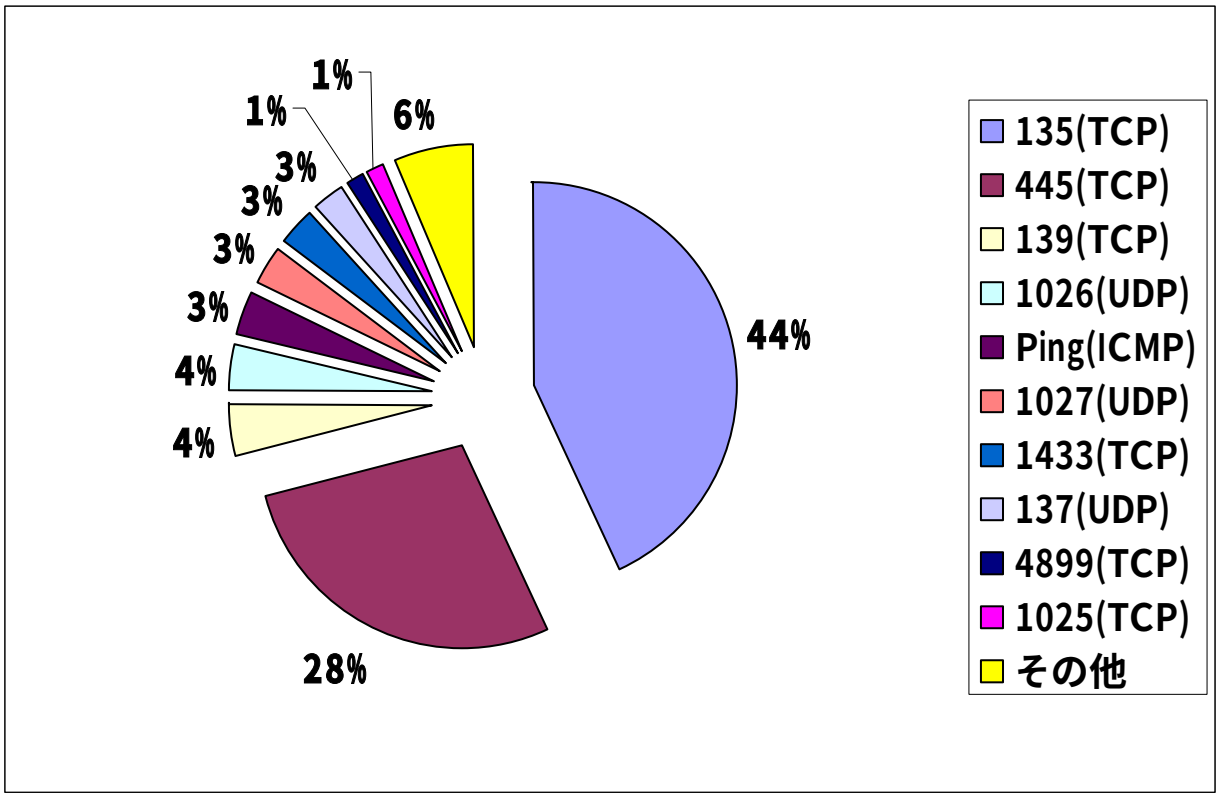
【図 2.1.1 2005 年 6 月の一方的なアクセス状況(アクセス数)】



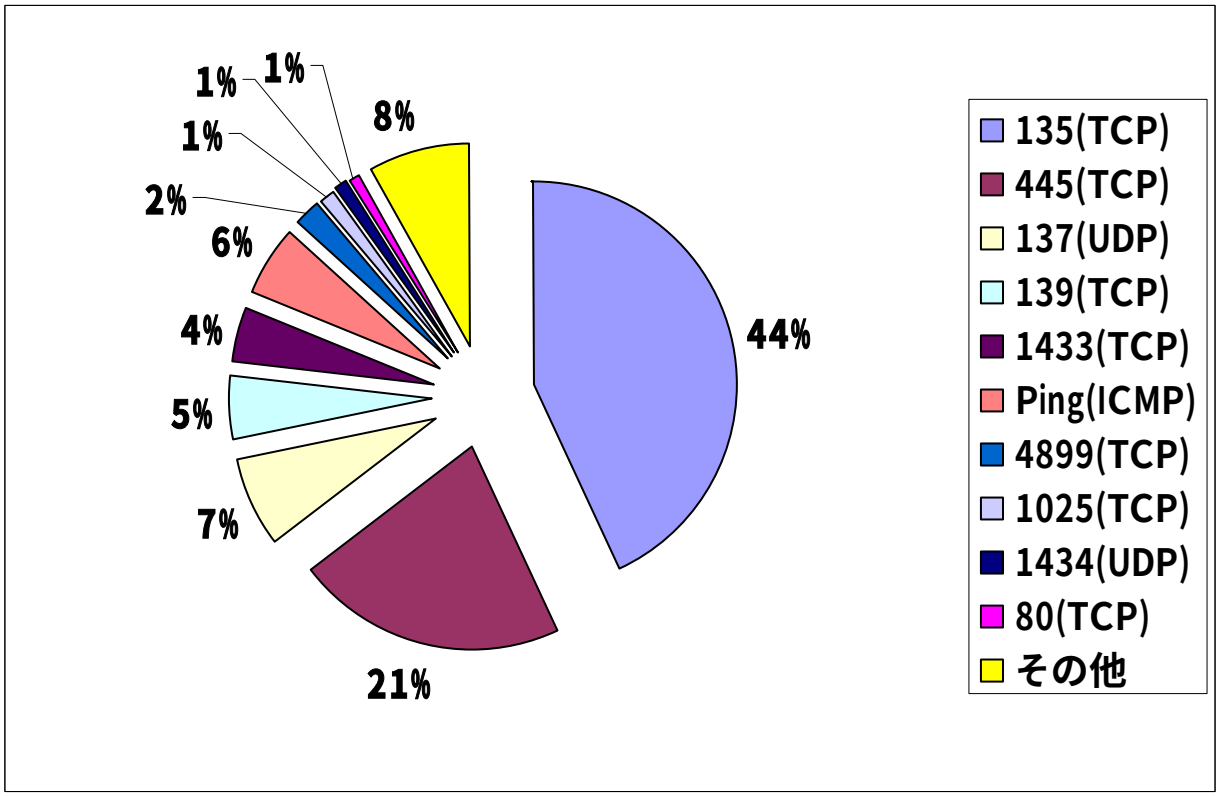
【図 2.1.2 2005 年 6 月の一方的なアクセス状況(発信元数)】

- 2005 年 6 月は全体的に特異な状況は出ていないようです。月内で見ると、総アクセス数および総発信元数について、緩やかな減少傾向(図中の赤点線)と言えます。

2.2 2005 年 6 月の宛先(ポート種類)別の比率



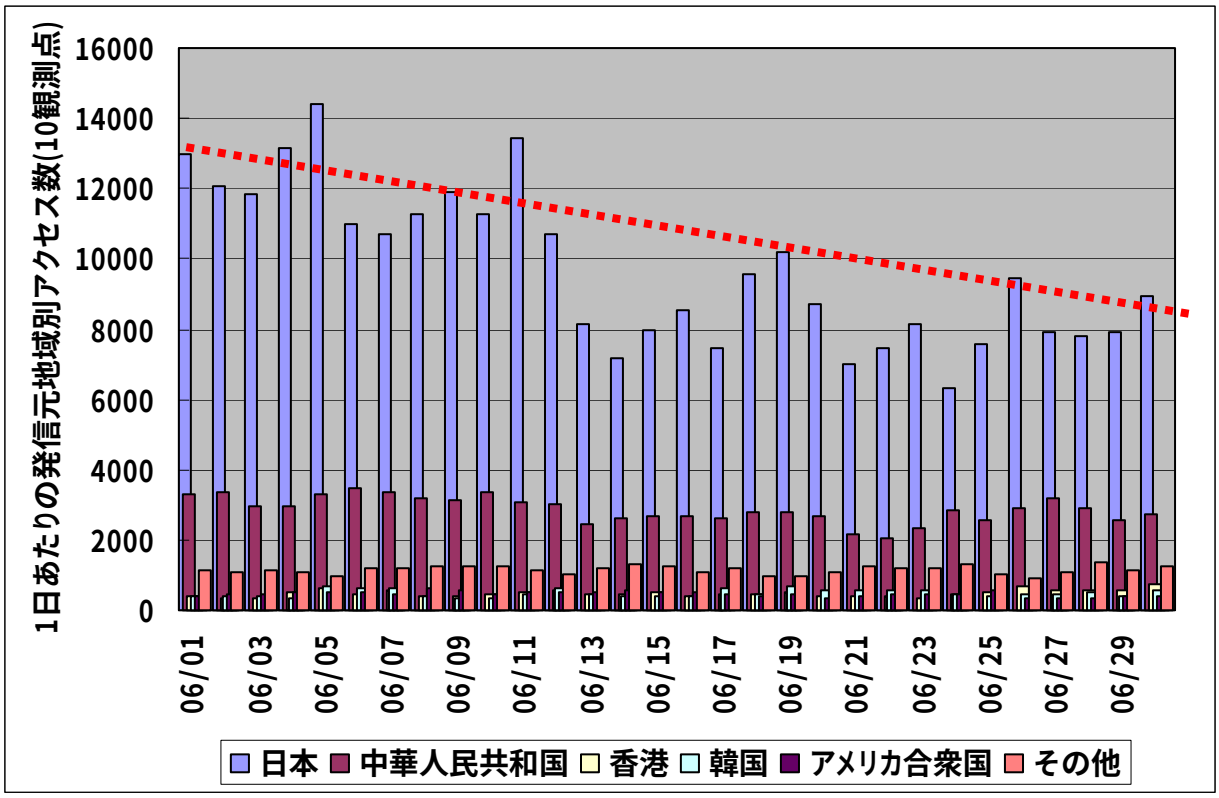
【図 2.2.1 2005 年 6 月の宛先(ポート種類)別アクセス数の比率】



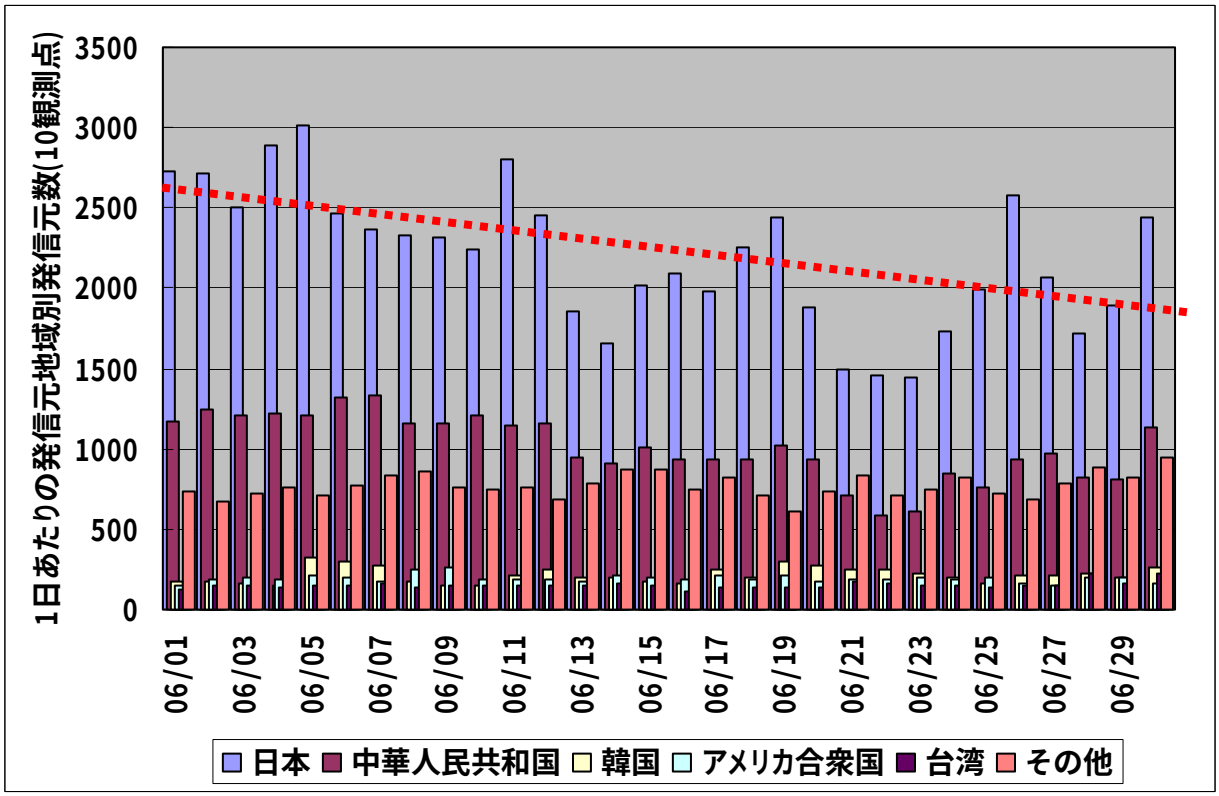
【図 2.2.2 2005 年 6 月の宛先(ポート種類)別発信元数の比率】

- 後述する 139(TCP)へのアクセスについて(「**2.4 139(TCP)ポートへのアクセスについて**」を参照下さい)、アクセス数にくらべて発信元数の比率が多いことがうかがえます。

2.3 2005 年 6 月の発信元地域別アクセス状況



【図 2.3.1 2005 年 6 月の発信元地域別アクセス数の変化】



【図 2.3.2 2005 年 6 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、月内でみるとアクセス数および発信元数が緩やかな減少傾向ですが、発信地域別の状況と比べると、国内からのアクセスが減少傾向(図中の赤点線)にあることが、その要因のようです。

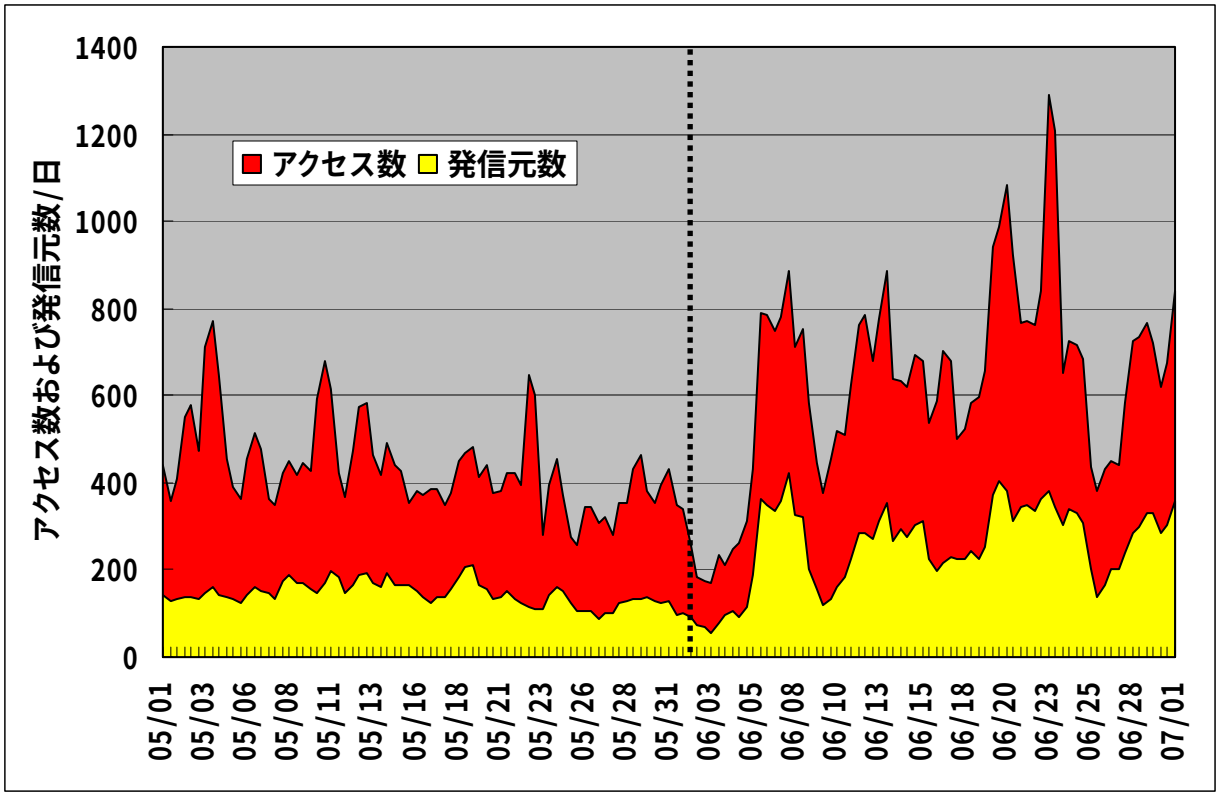
2.4 139(TCP)ポートへのアクセスについて

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 2.4.1 に 2005 年 5 月から 6 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 2.4.2 に同期間の発信地域別のアクセス数の変化を、図 2.4.3 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 月の状況の変化が良く見て取れます。

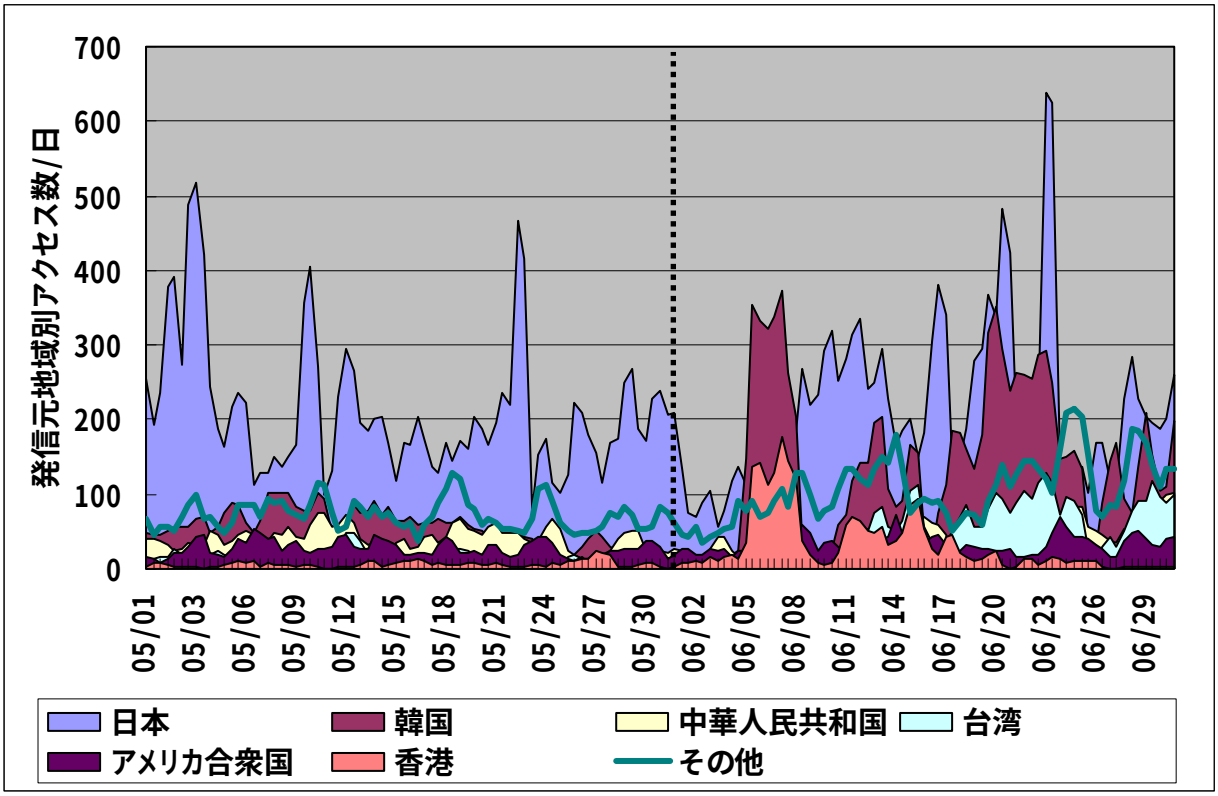
このアクセスは、Windows 系のファイル共有への不正アクセスと思われます。一般的には、139(TCP)ポートをインターネット側（WAN 側）には開いていないと考えられますが、万が一このポートを WAN 側に開いている場合は注意が必要です。ファイル共有のためのアクセス制御(特にパスワード設定等)があまいと、管理者権限を奪取され、コンピュータへ侵入される可能性があります。

これらのアクセスを行っているのは、ボット（ボットについては後述）系と呼ばれるウイルスと思われ、前述の韓国、香港、台湾方面で、これらのボット系のウイルスが流行り始めている可能性があります。

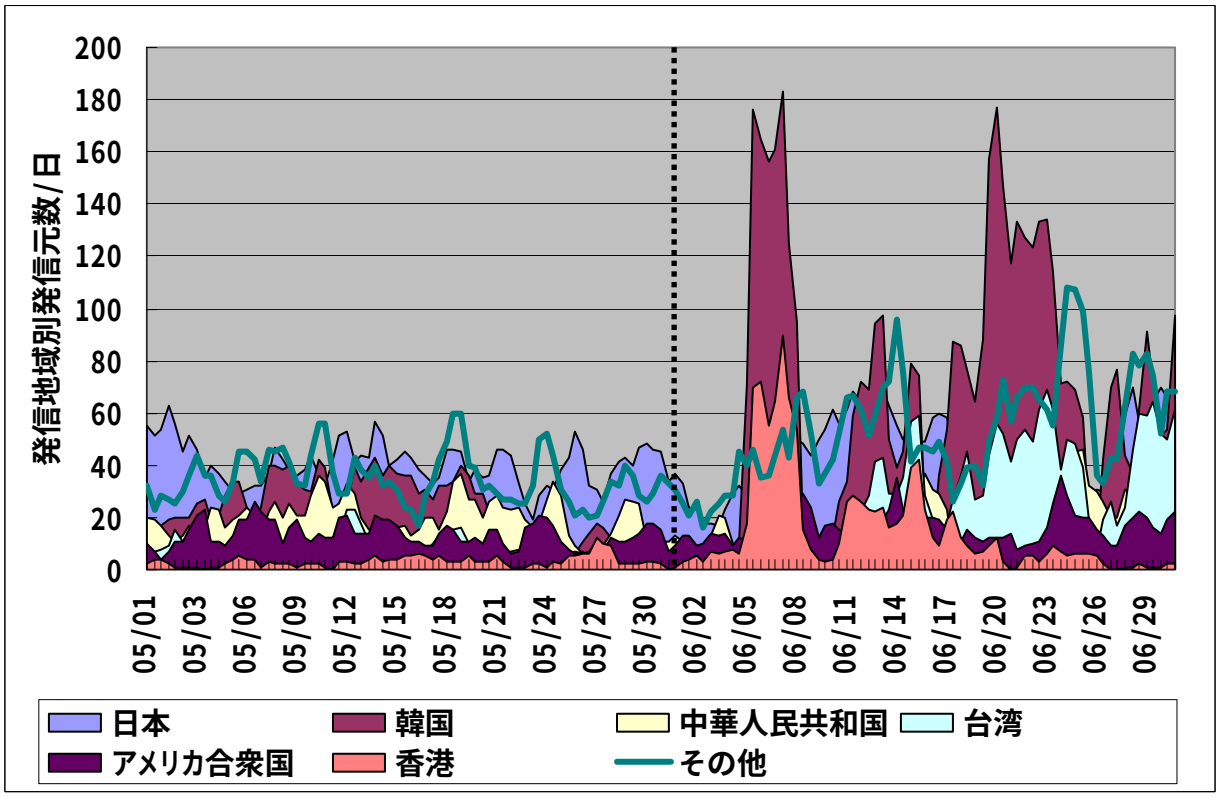
極端なアクセス数の増加ではありませんが、連続するＩＰアドレスを持つＴＡＬＯＴの観測では、連続する観測点に、アドレスを総ナメするようにアクセスが観測されていますので、システム管理者は、今一度 WAN 側のポートの開閉状況あるいはファイアウォールの設定を確認する必要があると思われます。



【図 2.4.1 139(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】

【ボットとは】

ボットとは、何らかの方法(後述)でコンピュータに感染(侵入)し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操るためのプログラムです。

ボットという名前は、ロボットに由来すると言われており、指示をひたすら待ち、指示があれば内蔵された処理を実行すると言うところから、こう呼ばれているようです。以前は、トロイの木馬型ウイルスに区分されていました。ボット以外には、ゾンビや不正(悪質)エージェントなどと呼ばれることもあります。

感染は、ウイルスメールの添付ファイルの実行、不正なWebページの参照(スパムメールに示されたリンク(URL)のクリックも含む)、コンピュータの脆弱性(パスワードの脆弱性も含む)を狙った不正アクセス、他のウイルス(Mydoomや Bagleなど)に感染した際に設定される**バックドア**(*1)を狙った不正アクセスなど、いろいろな方法で行われます。

感染すると、自らネットワークを通じて外部の指令サーバと通信(多くのボットは IRC(Internet Relay Chat)(*2)を使うようです)を行い、外部からの指示により指定された処理(攻撃活動・感染活動・**スキャン活動**(*3)など)を実行します。さらに、自分自身のバージョンアップさえ実行されます。ボット作成側からすれば、何でもできると言うことです。

同一の指令サーバの配下にある複数のボットは、指令サーバを中心とするネットワークを組むため、ボット(ゾンビ)ネットワークと呼ばれています。

これらのボットネットワークを利用することで、フィッシング目的のスパムメールの大量送信や、特定サイトへの **DDoS 攻撃**(*4)などに利用されることがあるため、大きな脅威になるわけです。

---

*1) IRC(Internet Relay Chat)

チャットシステムのこと。インターネット上のIRCサーバに、専用のソフトウェアを利用してアクセスすることで、複数のユーザとの間でメッセージの交換をすることができます。

*2) スキャン活動

ポートスキャンと言う手段を使い、対象のコンピュータの各ポートにおけるサービスの状態を調査すること。他のウイルスが仕掛けたバックドアなどが動作しているかも調査することができます。

*3) バックドア(裏口)

コンピュータへの不正侵入(アクセス)を目的に仕掛けられる仕組みで、特定のポートを開き、そのポートを利用するサービスとしてプログラムを起動させること。このサービスにより、外部からインターネットを通じて、コンピュータへ侵入することができます。

*4) DDoS 攻撃 (分散サービス妨害攻撃：Distributed Denial of Service attack)

サービス妨害攻撃（ＤｏＳ攻撃）には、インターネットプロトコルの特性を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供できなくするような攻撃があります。このようなＤｏＳ攻撃の攻撃元が複数で、標的とされたコンピュータがひとつであった場合、その標的とされるコンピュータにかけられる負荷は、より大きなものになります。このような攻撃を DDoS(Distributed Denial of Service：分散サービス妨害）攻撃と呼びます。

攻撃元は、攻撃者（人間）自身であるとは限らず、むしろ、攻撃者が事前に標的以外の複数サイトに攻撃プログラムを仕掛けておき、遠隔から一斉にＤｏＳ攻撃をしかける手法が広く知られています。

2.5 10000(TCP)ポートへのアクセスについて

2005 年 6 月 26 日から、10000(TCP)ポートへのアクセスが増加しました。

この 10000(TCP)ポートへのアクセスは、米 VERITAS のバックアップ・ソフト VERITAS Backup Exec のセキュリティ・ホールの攻略コードが公開されたことに起因するものと思われます。

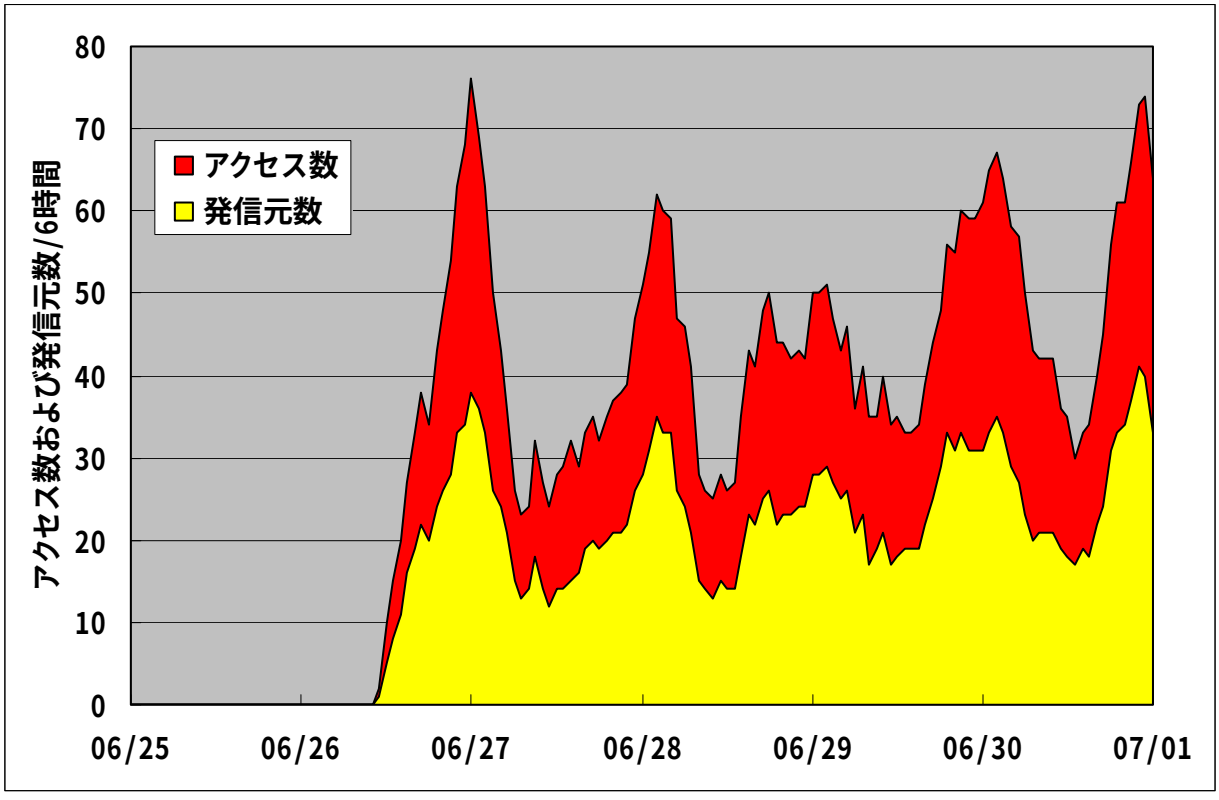
これらのアクセスについては、現状ではそれほどの量があるわけではありませんが、前述のアプリケーションを使用している利用者は、**早急に脆弱性を修正するために、アプリケーションへのパッチの適用**をお勧めします。

VERITAS 社の Backup Exec に複数の脆弱性

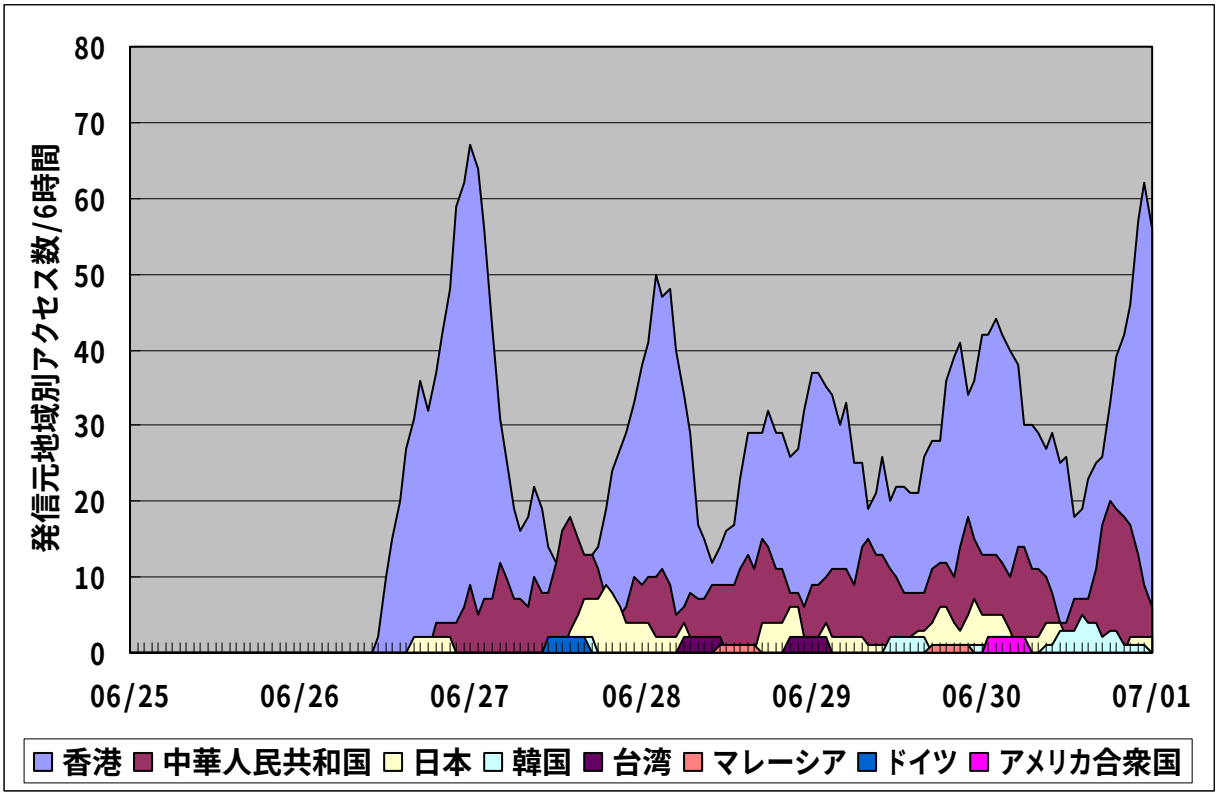
VERITAS 社の Backup Exec に複数の脆弱性が存在し、攻撃者にリモートから任意のコード（命令）を実行されたり、バックアップサーバの管理者権限を完全に奪われる可能性があります。

[関連情報]

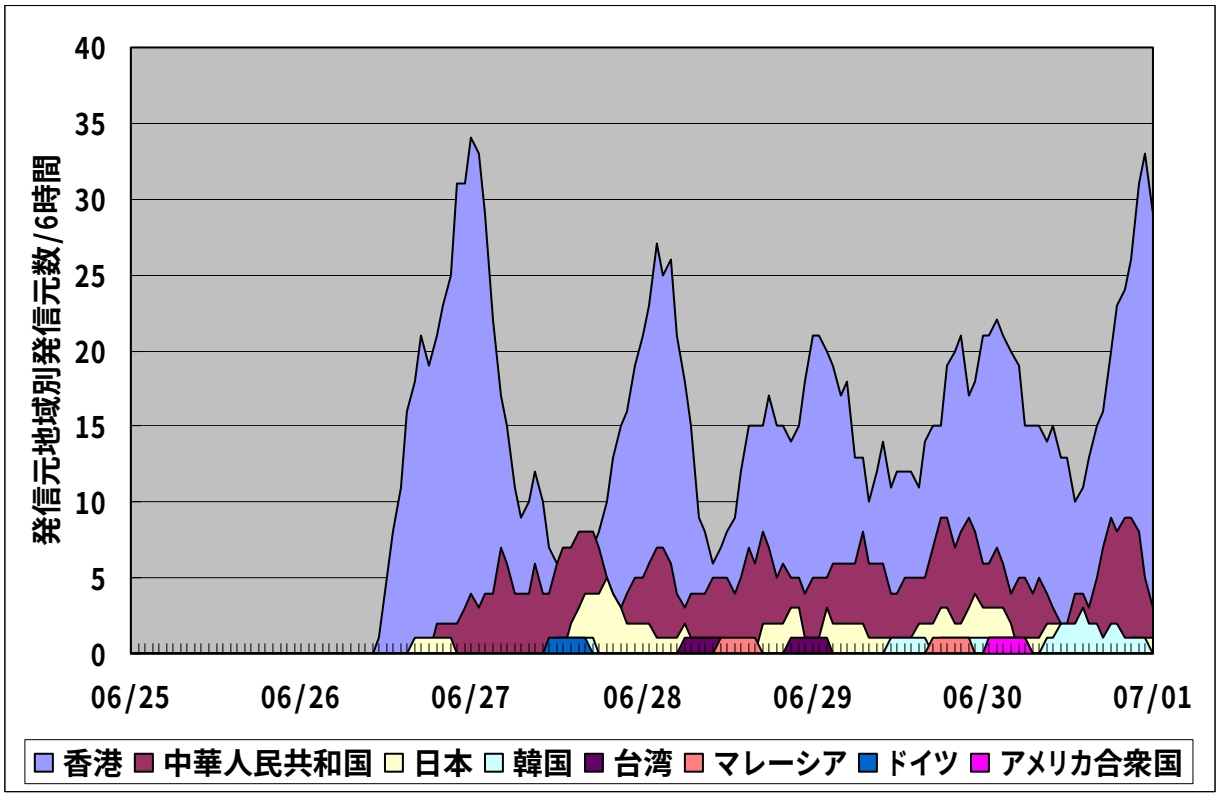
VERITAS	http://seer.support.veritas.com/docs/276608.htm
	http://seer.support.veritas.com/docs/276607.htm
	http://seer.support.veritas.com/docs/276606.htm
	http://seer.support.veritas.com/docs/276605.htm
	http://seer.support.veritas.com/docs/276604.htm
US-CERT	http://www.kb.cert.org/vuls/id/352625
	http://www.kb.cert.org/vuls/id/584505
	http://www.kb.cert.org/vuls/id/492105
CIAC	http://www.ciac.org/ciac/bulletins/p-232.shtml
CVE 番号	CAN-2005-0771 CAN- 2005-0773



【図 2.5.1 10000(TCP)ポートへの発信地域別アクセス数の変化】



【図 2.5.2 10000(TCP)ポートへの発信地域別アクセス数の変化】

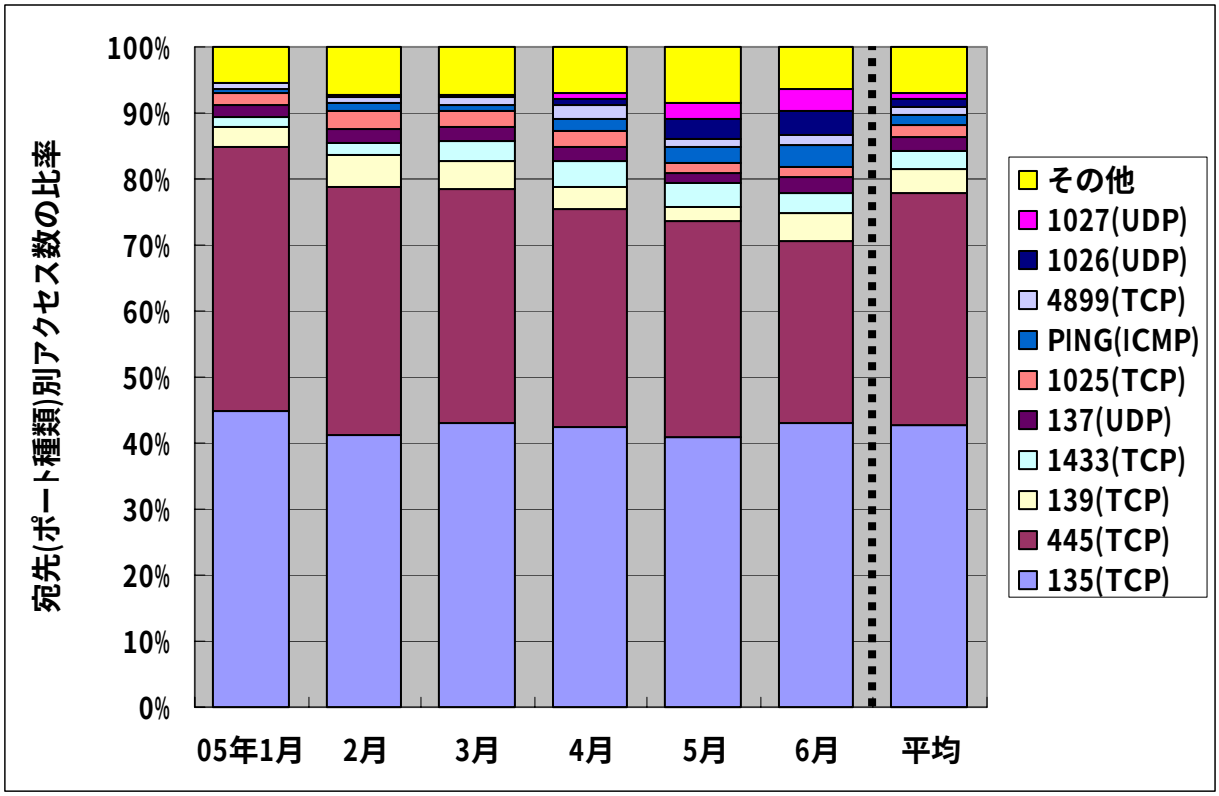


【図 2.5.3 10000(TCP)ポートへの発信地域別発信元数の変化】

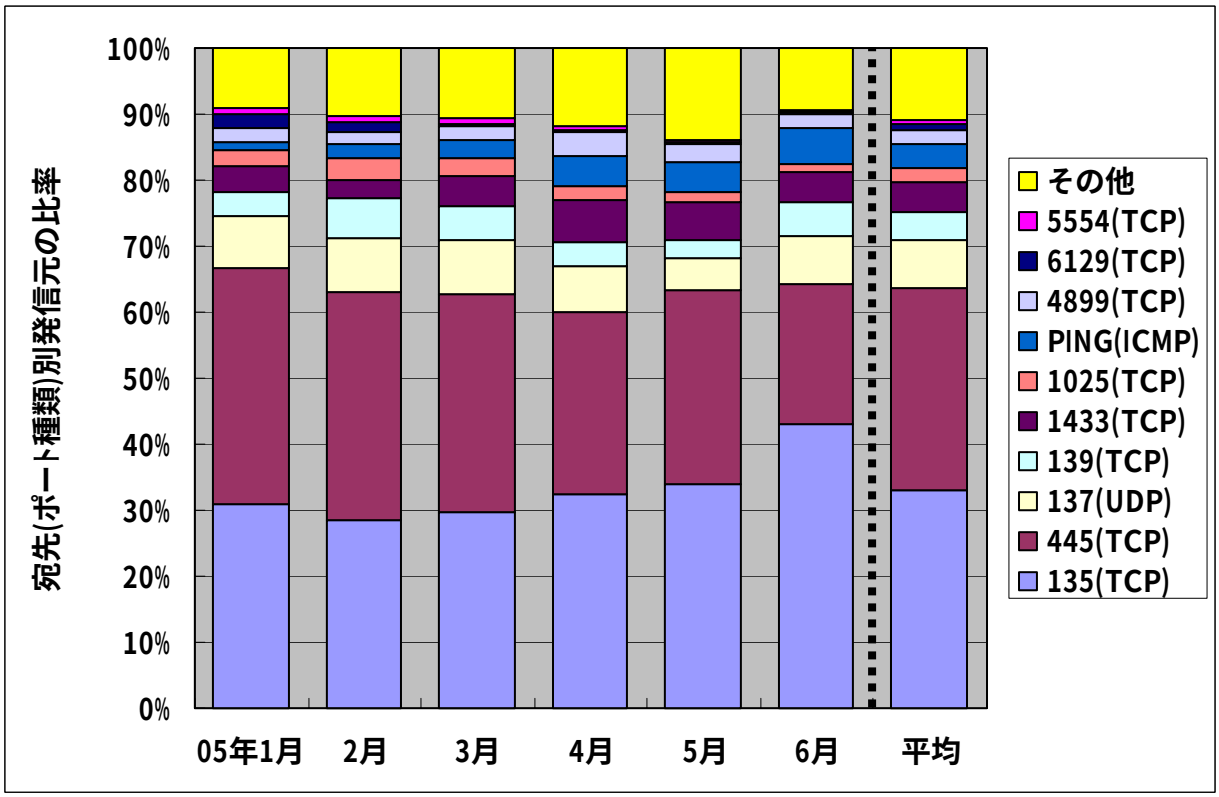
また、米 VERITAS のバックアップ・ソフト VERITAS Backup Exec のセキュリティ・ホールの攻略コードの公開以外にも、**Windows の SMB プロトコルの脆弱性(MS05-011、MS05-027)を狙った攻撃(445(TCP)ポートへのアクセス)が仕掛けられる恐れがある**ので、システム管理者は、あわせて注意が必要です。

3．統計情報

3.1 2005 年 1 月～6 月の宛先(ポート種類)別の比率

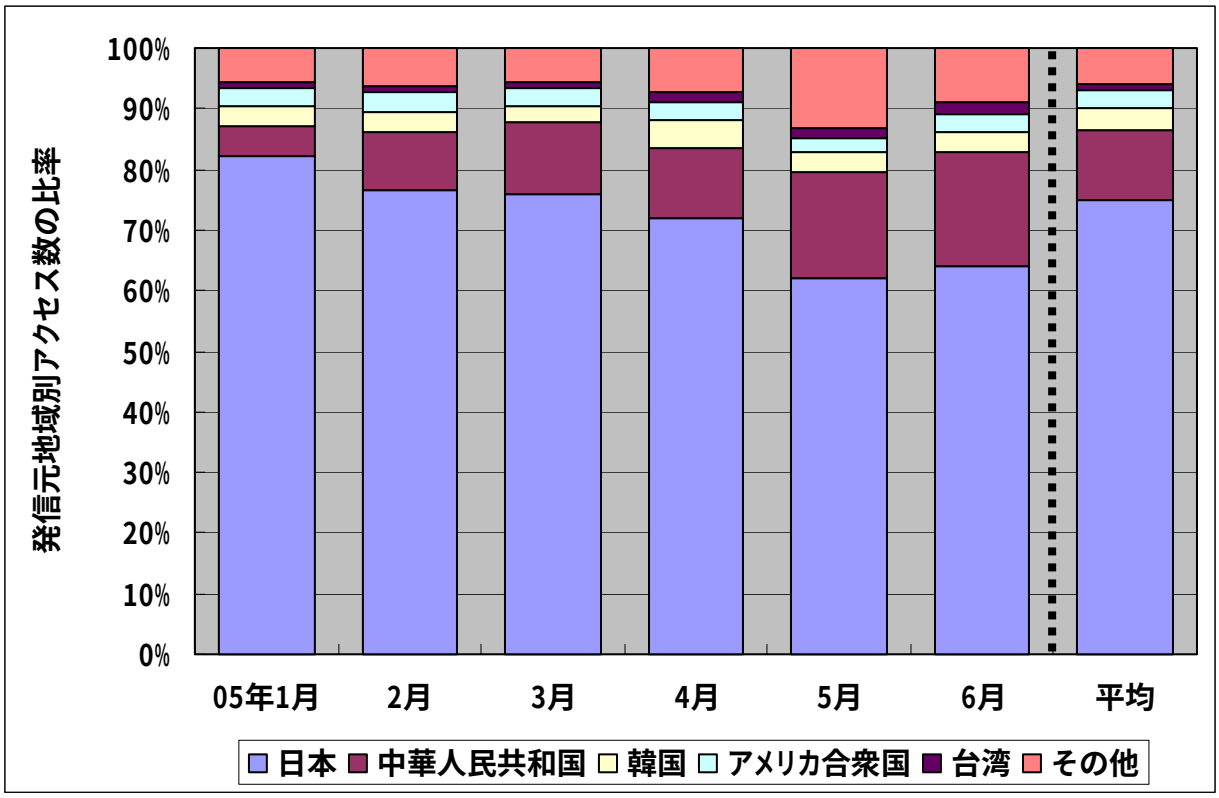


【図 3.1.1 2005 年 1 月～6 月の宛先(ポート種類)別アクセス数の比率】

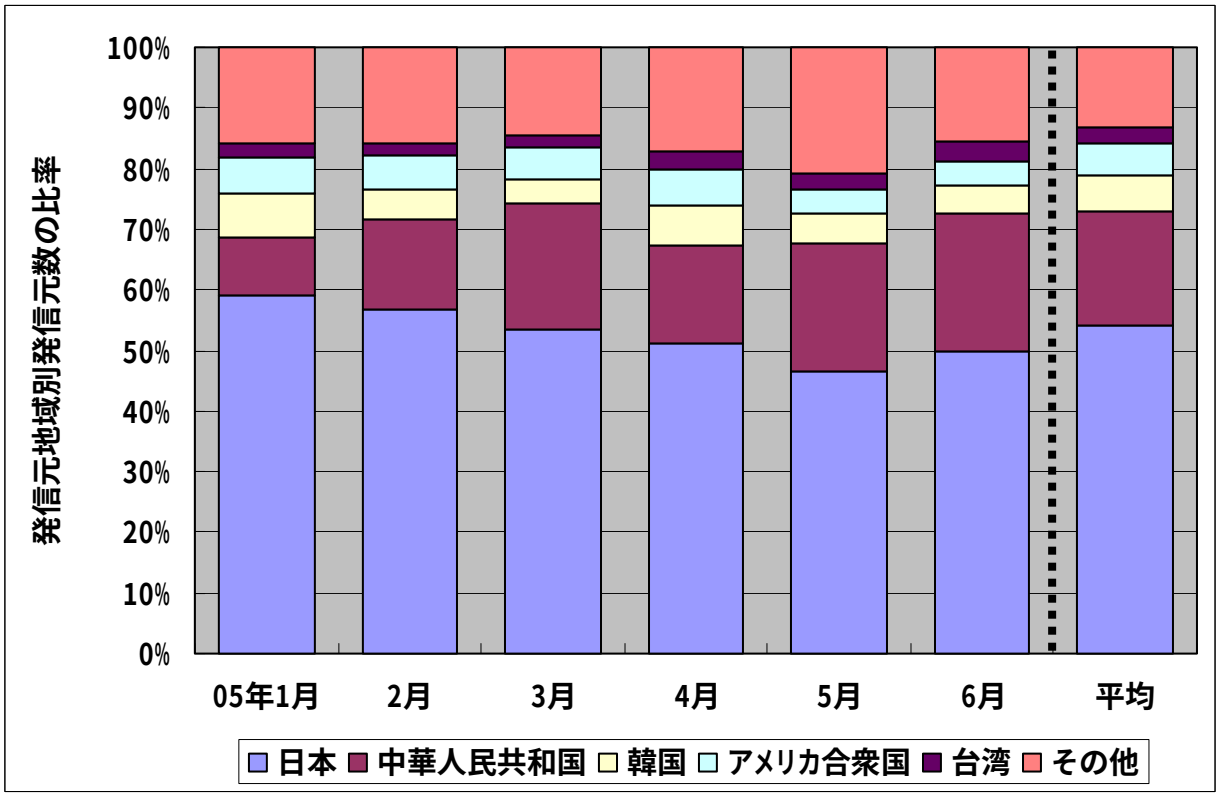


【図 3.1.2 2005 年 1 月～6 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 1 月～6 月の発信元地域別の比率



【図 3.2.1 2005 年 1 月～6 月の発信元地域別アクセス数の比率】



【図 3.2.2 2005 年 1 月～6 月の発信元地域別発信元数の比率】

■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