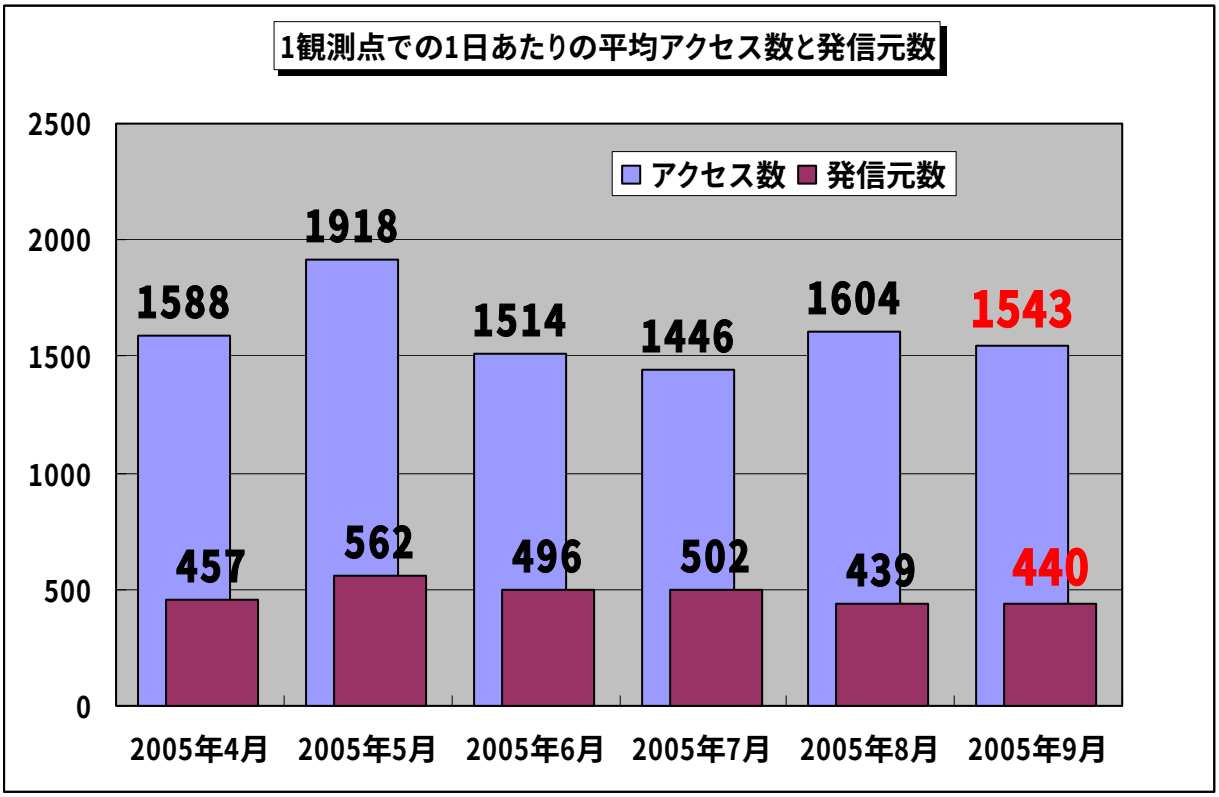
別紙 3

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 9 月の期待しない（一方的な）アクセスの総数は、10 観測点で **462,928 件**ありました。1 観測点で 1 日あたり **440** の発信元から **1,543 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 3.5 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。これは、2005 年 8 月とほぼ同じ状況です。



【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 4 月～9 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。

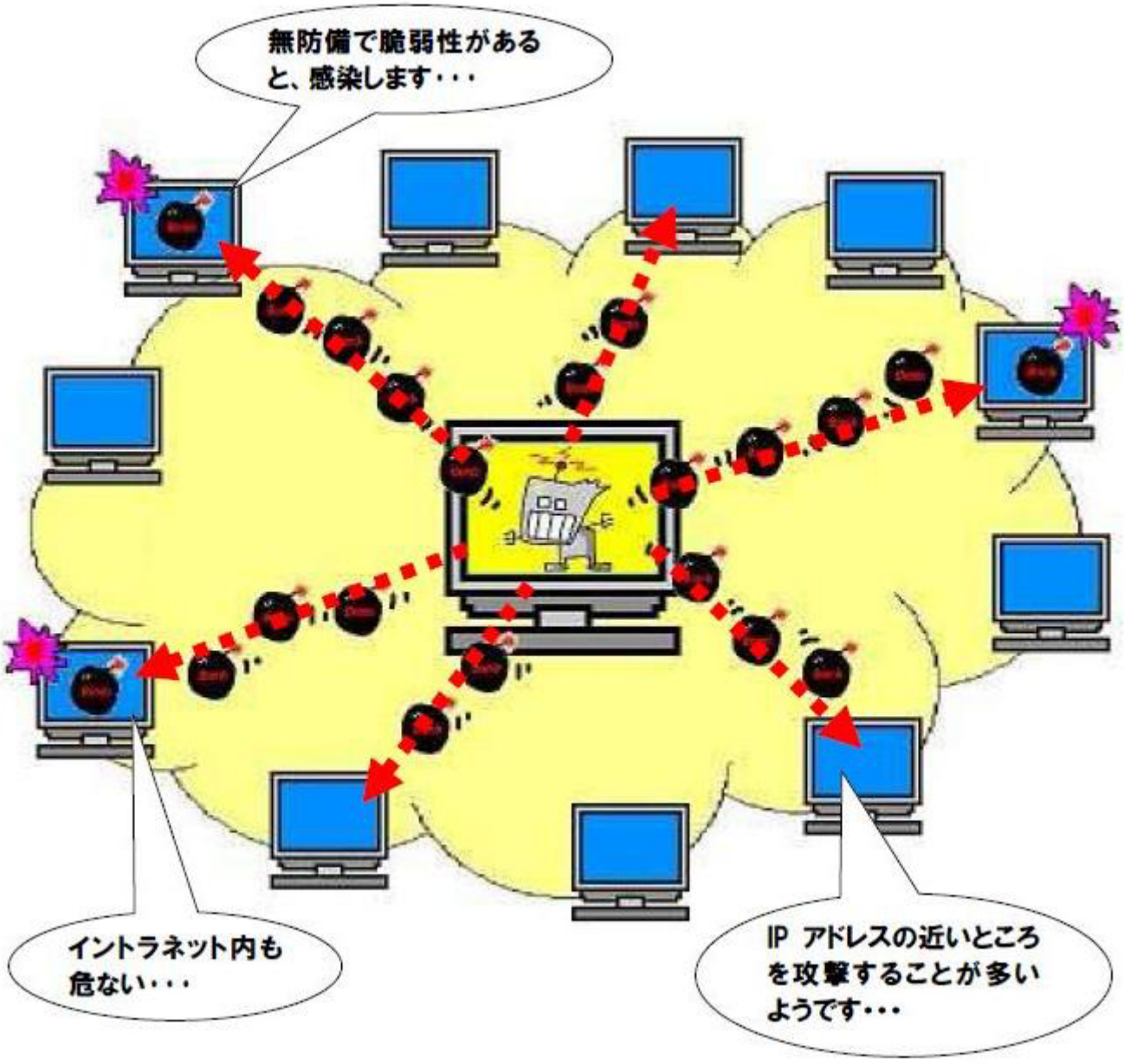
2．9月のアクセス状況

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。

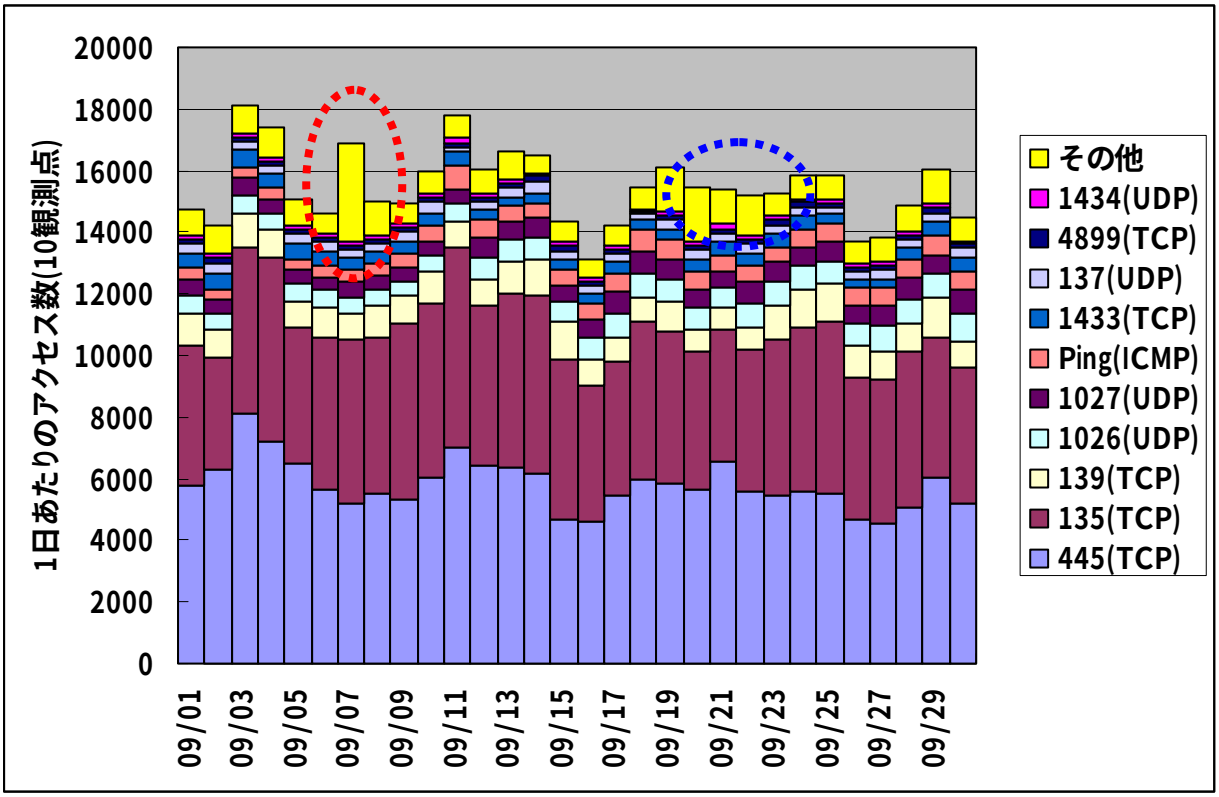
最近ボットと呼ばれるワームが流行していることから、これらのアクセスを行っているワームもボットである可能性が高いと思われます。特にアクセス数の多い 135(TCP),445(TCP)へのアクセスは、Windows の古いタイプの脆弱性を狙っていると思われ、これらのアクセスの多くが国内発信であることから、国内でのボットの感染が広がっていることが予測されます。

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。

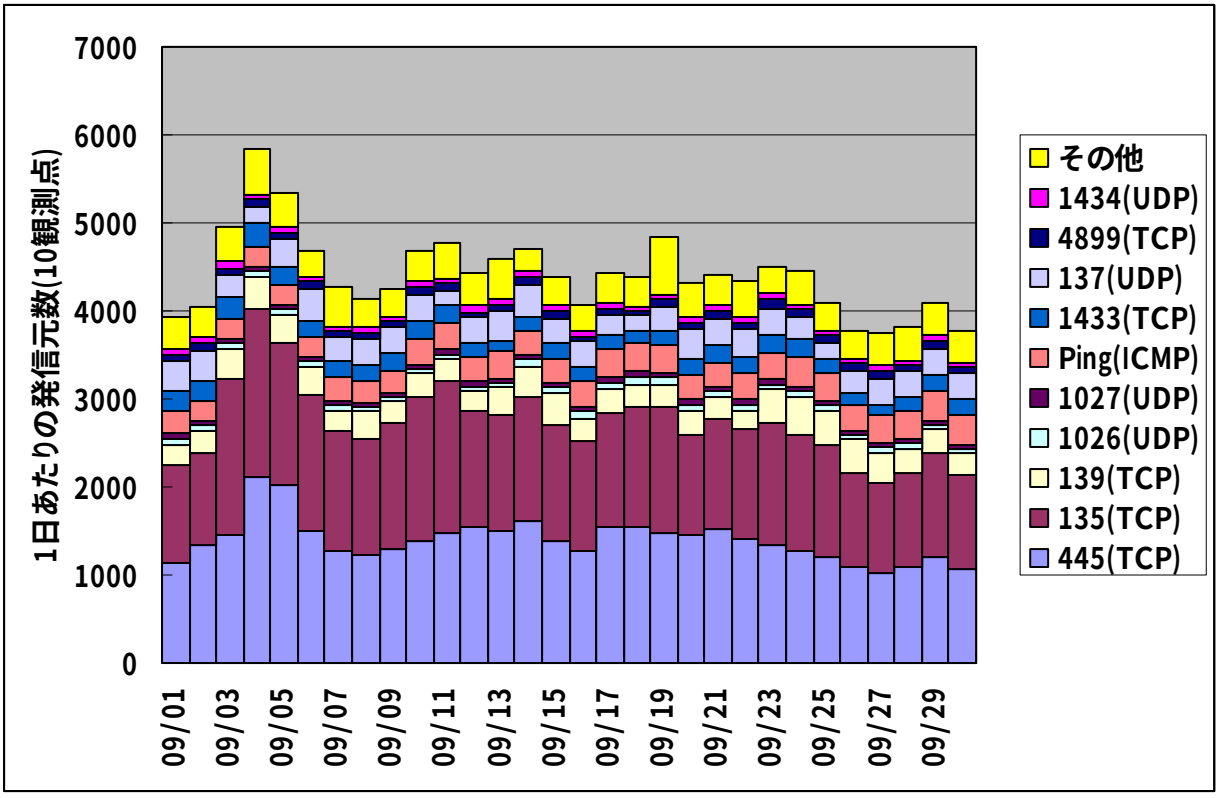
一般のコンピュータ利用者は、これらのボットに感染しないために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフト等を有効利用することをお勧めします。



2.1 2005 年 9 月の一方的なアクセス状況

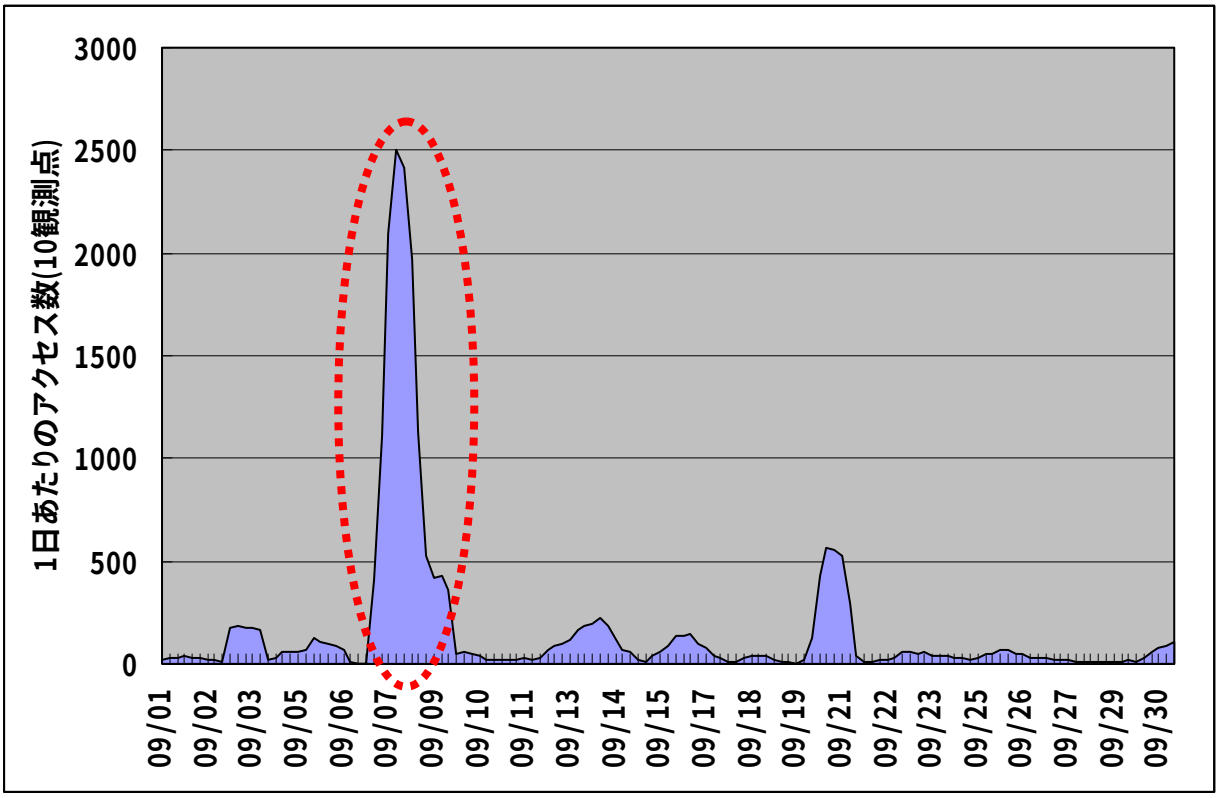


【図 2.1.1 2005 年 9 月の一方的なアクセス状況(アクセス数)】



【図 2.1.2 2005 年 9 月の一方的なアクセス状況(発信元数)】

- 2005 年 9 月の特徴的なアクセスは 9 月 7 日前後の ポート種類＝その他 のアクセスの増加です(図 2.1.1 中の赤丸部分)。このアクセスは、複数の受信ポートにアクセスしていますが、実際には、発信元が同一で、発信元ポートも同一のアクセスです。図 2.1.3 に、これらのアクセスの状況を示します。



【図 2.1.3 発信元ポート 7000(TCP)からのアクセス状況】

- これらのアクセスの発信元は、すべて中国方面であり、それらの多くがゲーム関連のサイトのようでした。発信元ポートは 7000(TCP)であり、解析の結果、これらのアクセスは、これらのサイトを狙った **DoS 攻撃(SYN Flood 攻撃)**(*1)の跳ね返りパケットのようです。ポート 7000(TCP)は、ファイルサーバでも使われるポートで、オンラインゲームでも利用されるようです。このポートに対して、何者かが、発信元アドレスを詐称したＳＹＮパケットを大量に送りつけている結果ということになります。
- これらのアクセスが確認された TALOT2 の観測点は複数であり、攻撃者は、かなり広い範囲でアドレス詐称を行っている可能性があります。
- 攻撃の目的は分かりませんが、このような攻撃は、標的になったサイトだけでなく、アドレスを詐称された利用者にとっても、好ましくないものです。
- 当月には、20 日～23 日にかけて、同様の攻撃が 80(TCP)ポートを利用して行われているのも観測されています(図 2.1.1 中の青丸部分および図 2.1.4 の青丸部分)。
- ただし、7000(TCP)からのアクセスについては、2005 年 9 月の特別なアクセスではなく、以前から多く見受けられるアクセスで、そのほとんどが、中国方面のゲーム関連サイトへの DoS 攻撃(SYN Flood 攻撃)と思われます。
- 図 2.1.4 に過去 6 ヶ月間の状況を示しますが、中国方面以外からのアクセスはグラフ上で確認することが出来ないほど少ないです。

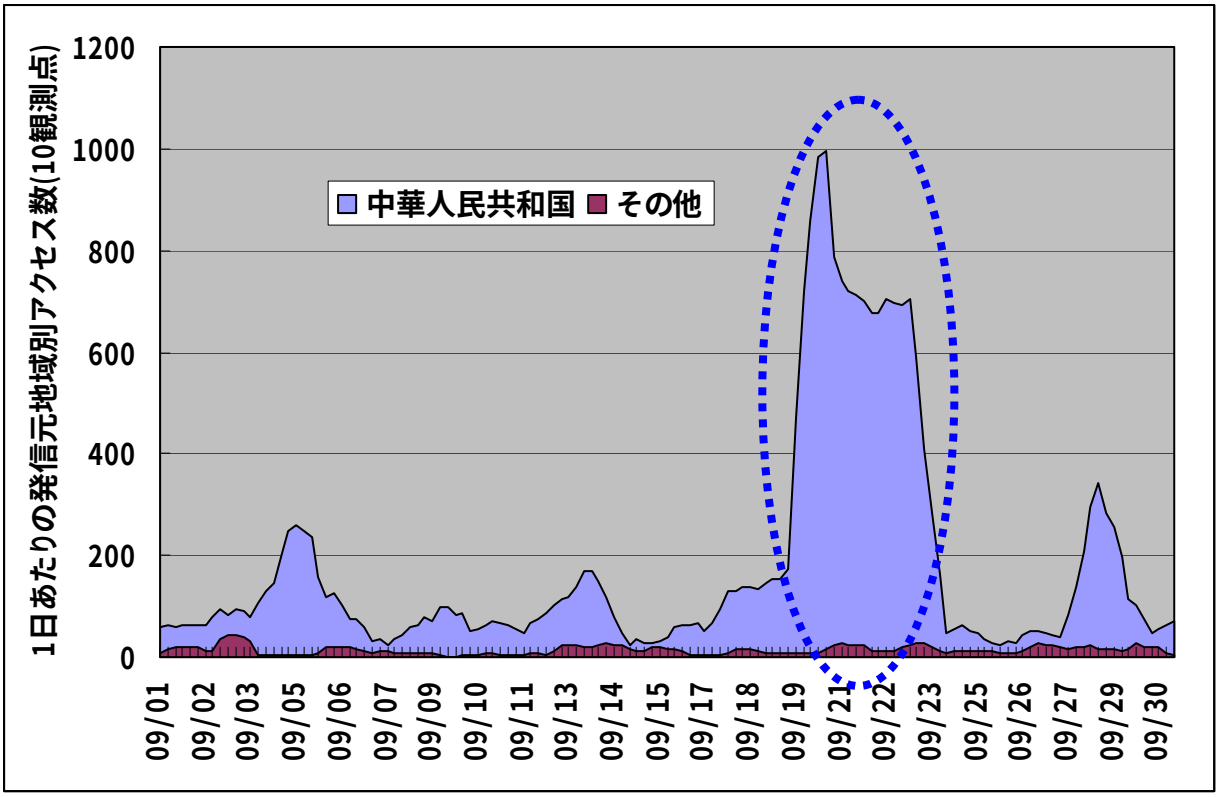
(*1)ＤｏＳ攻撃(SYN Flood 攻撃)

「サービス妨害攻撃」Denial of Service の略からＤｏＳ攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。このＤｏＳ攻撃の 1 つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称したSYNパケット(3ウェイ・ハンドシェーク(*2)での接続確立の最初に送られるパケット)を大量に送りつけ、確立途中状態の接続を大量作成するものです。

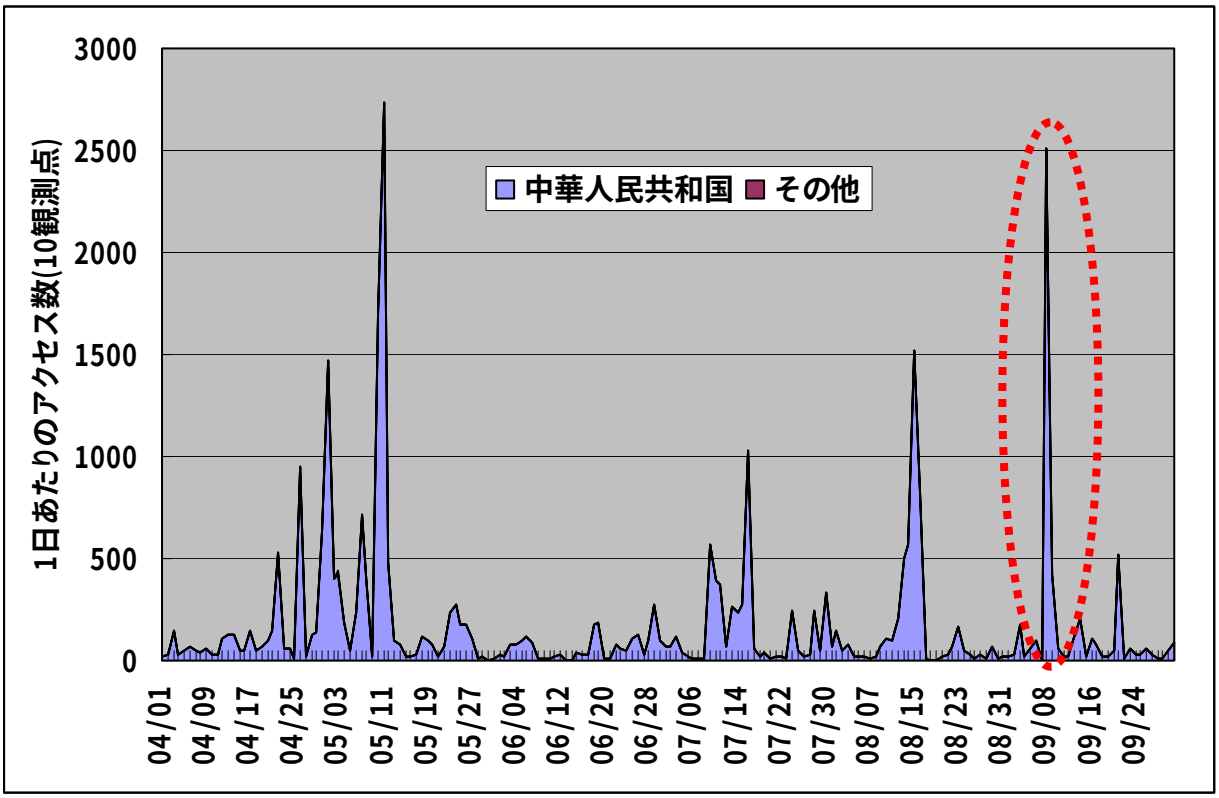
(*2) 3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認で

きるわけです。
以下に A と B の通信確立の手順を示します
①A から B へ SYN パケットの送信
②B から A へ ACK+SYN パケットの送信
③A から B へ ACK パケットの送信
これで、AB 双方の通信が確立されます。

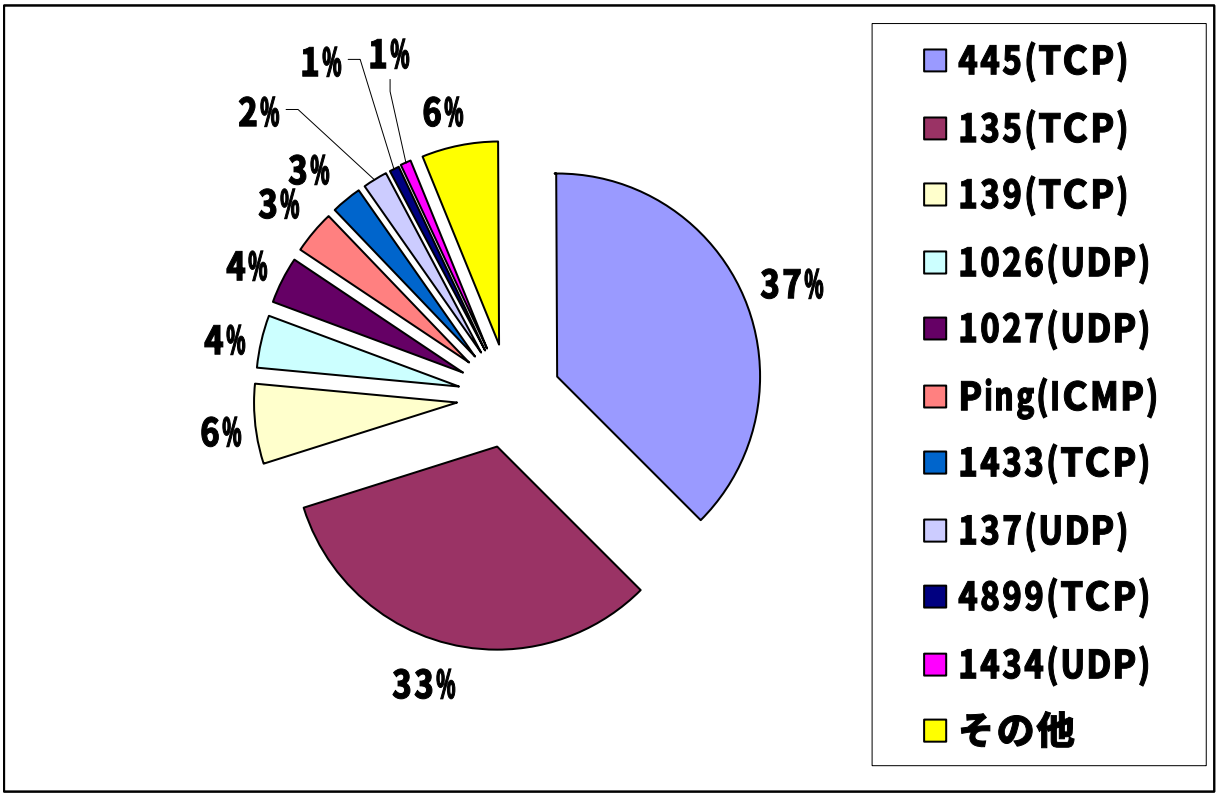


【図 2.1.4 発信元ポート 80(TCP)からのアクセス状況】

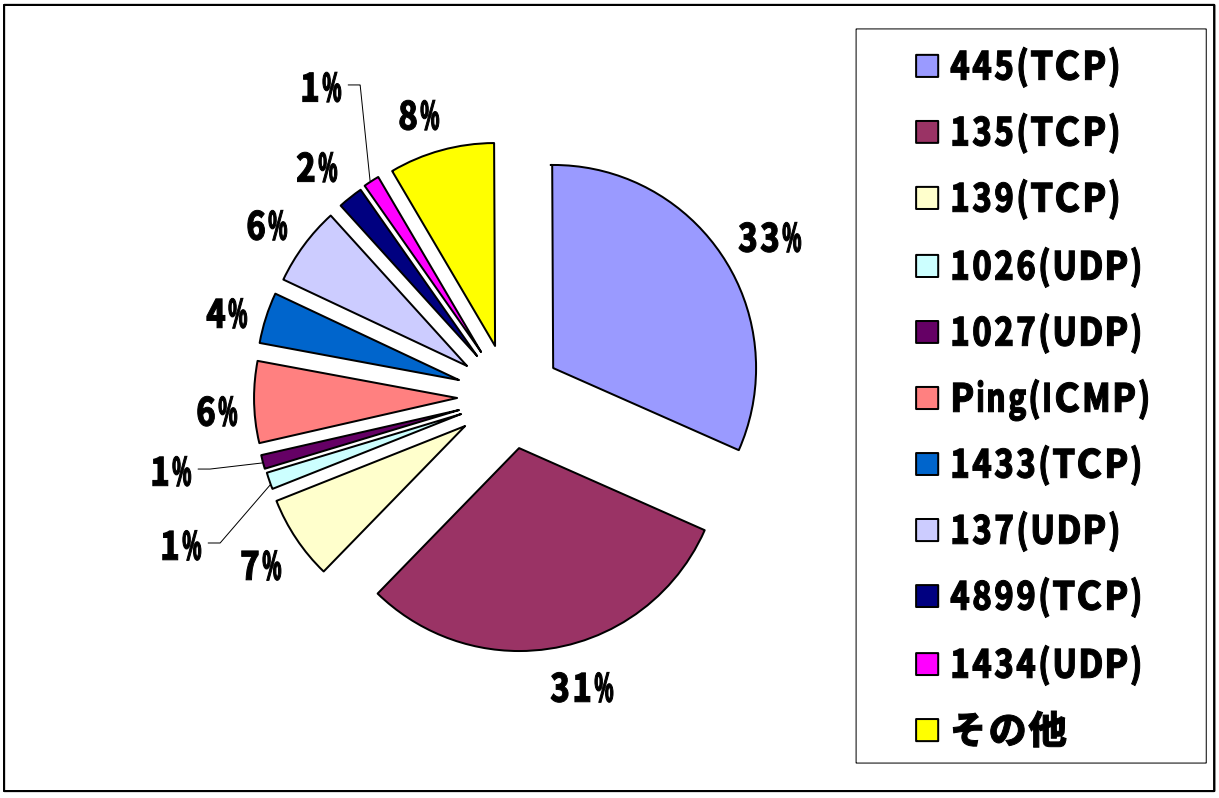


【図 2.1.5 発信元ポート 7000(TCP)からのアクセス状況(6 ヶ月)】

2.2 2005 年 9 月の宛先(ポート種類)別の比率

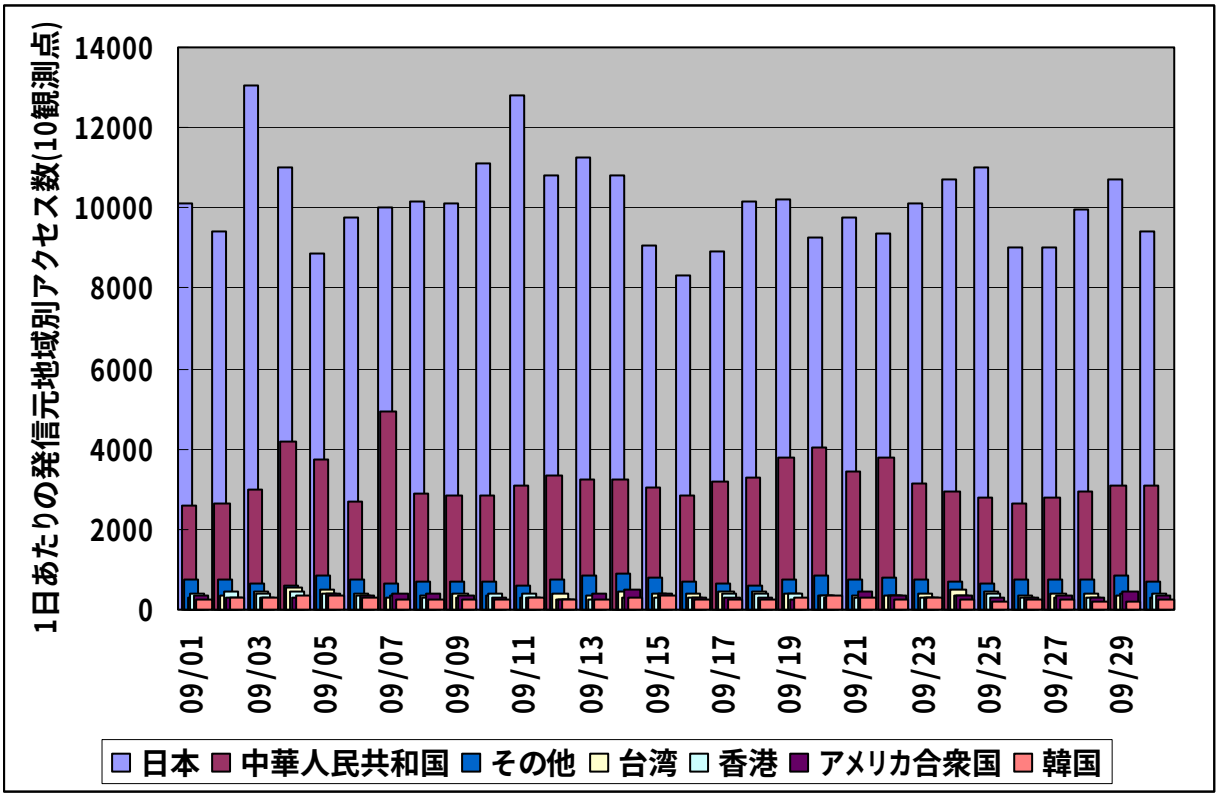


【図 2.2.1 2005 年 9 月の宛先(ポート種類)別アクセス数の比率】

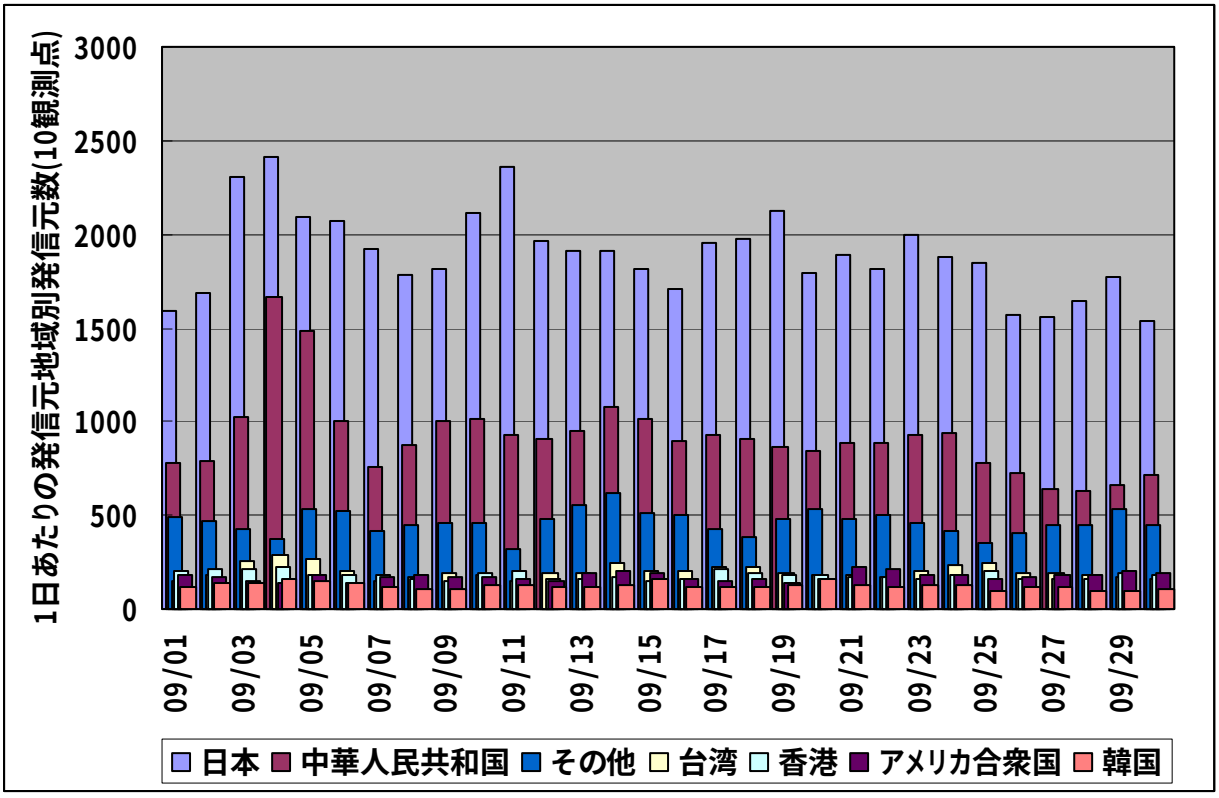


【図 2.2.2 2005 年 9 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 9 月の発信元地域別アクセス状況



【図 2.3.1 2005 年 9 月の発信元地域別アクセス数の変化】



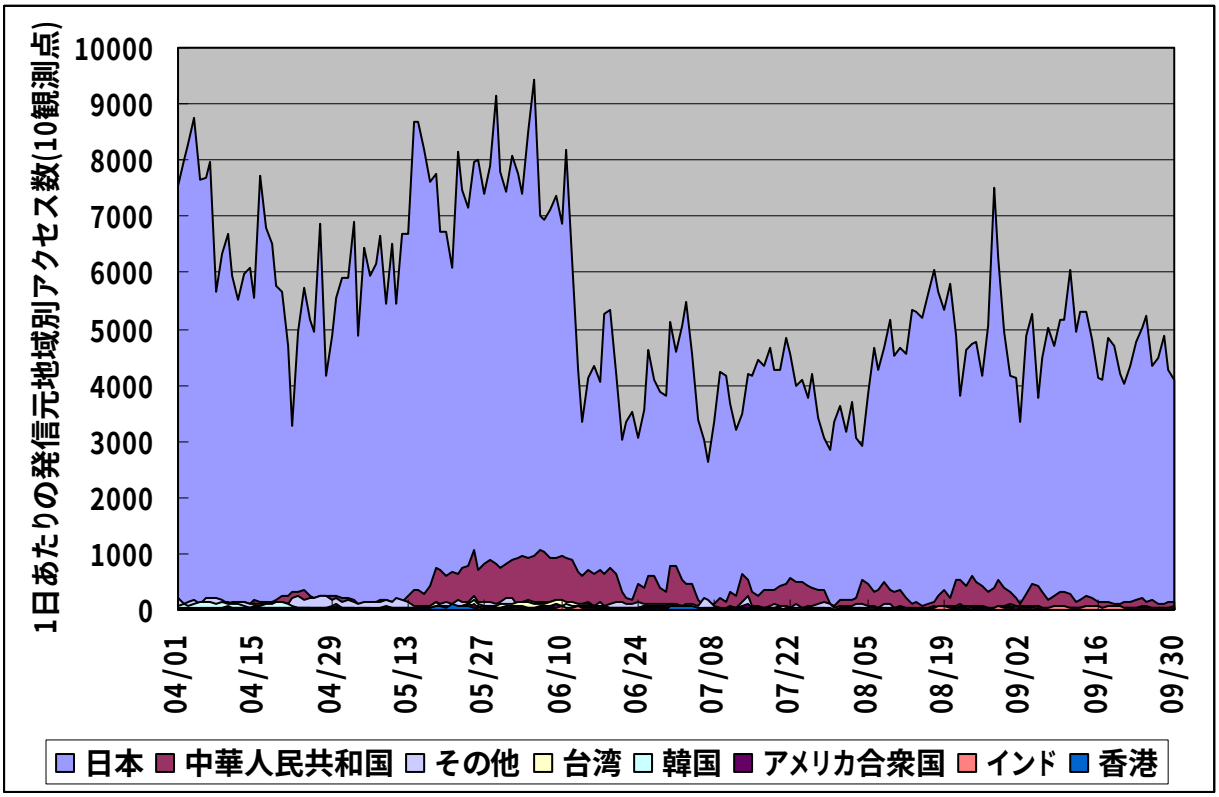
【図 2.3.2 2005 年 9 月の発信元地域別発信元数の変化】

2.4 4月～9月のアクセスの発信元地域別変化について

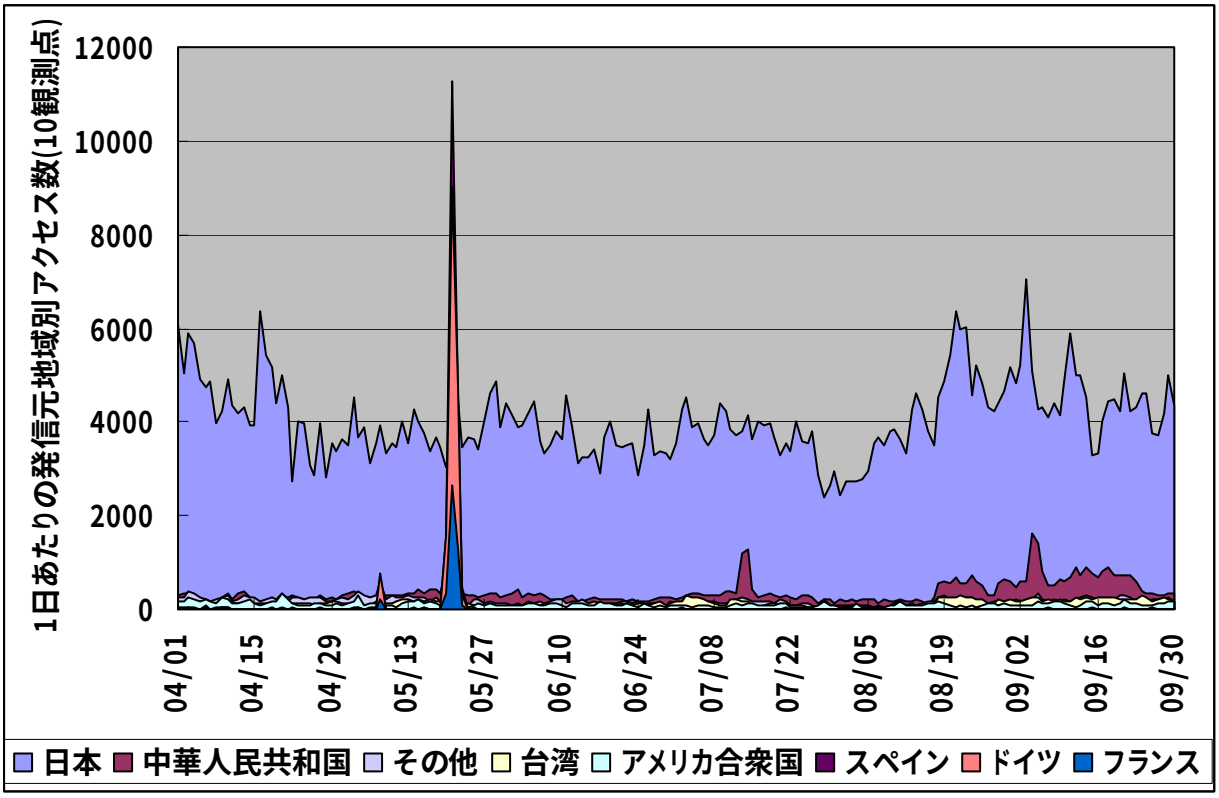
2005年4月～9月の、アクセス数が多いアクセスについて着目し、それらの発信元地域別変化について以下に示します。

対象となるアクセスは、宛先が135,445,139,1026/1027のものです。

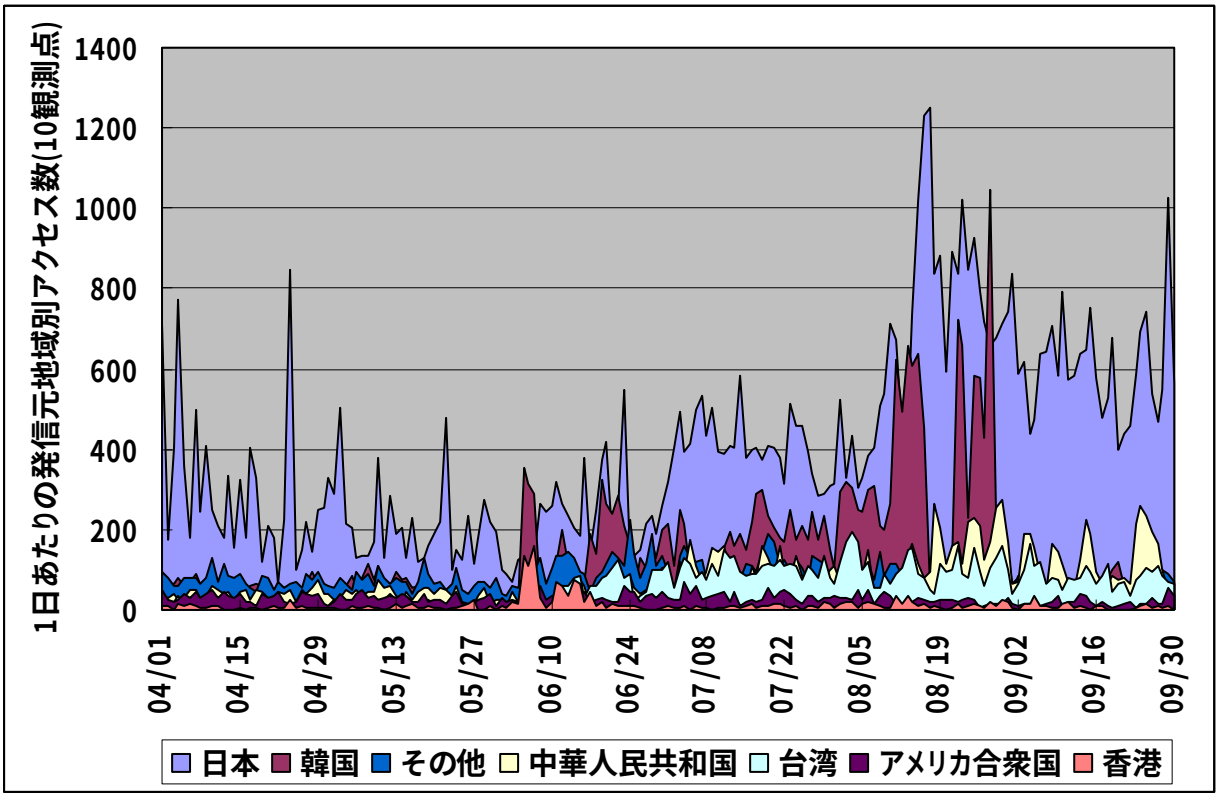
これらのアクセスは、ほとんどがWindows系コンピュータの脆弱性を狙ったアクセスと思われ、ボット系のワームによるものと考えられます(1026/1027へのアクセスはスパムメッセージ表示)。



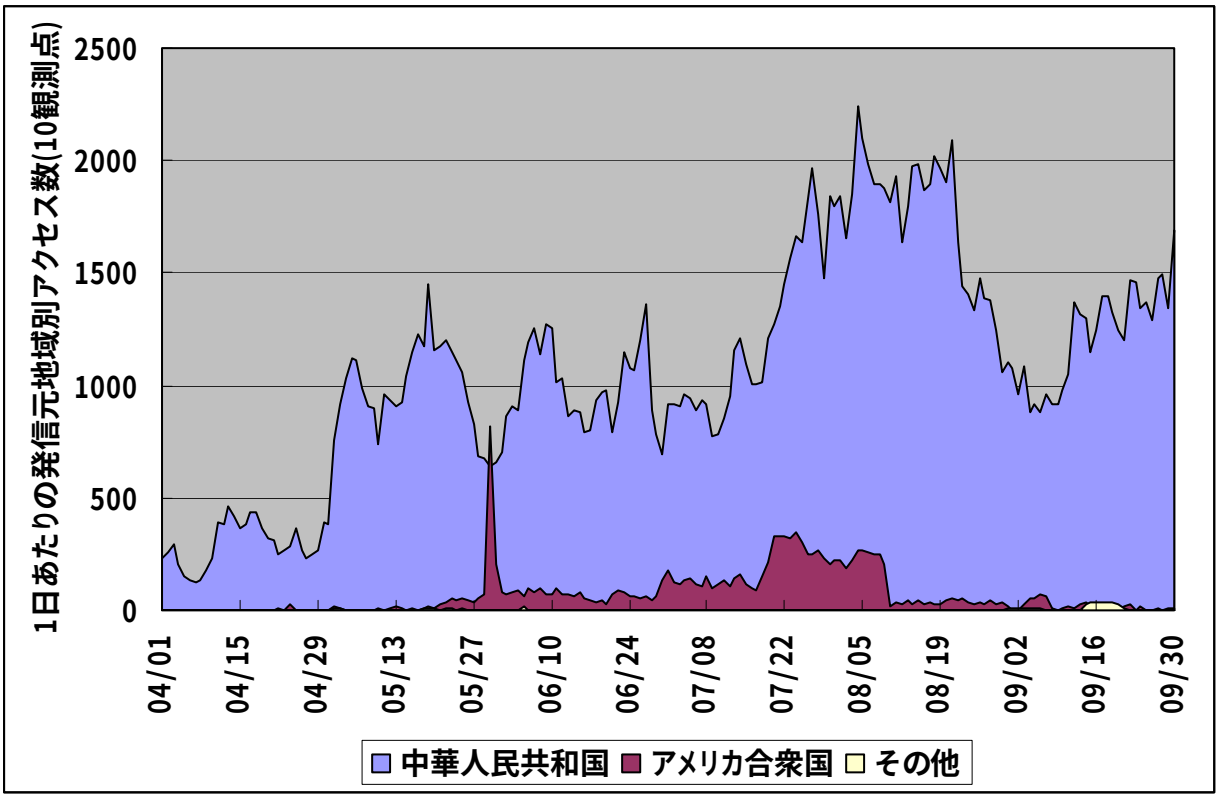
【図 2.4.1 135 ポートへの発信元地域別アクセス数の変化】



【図 2.4.2 445 ポートへの発信元地域別アクセス数の変化】



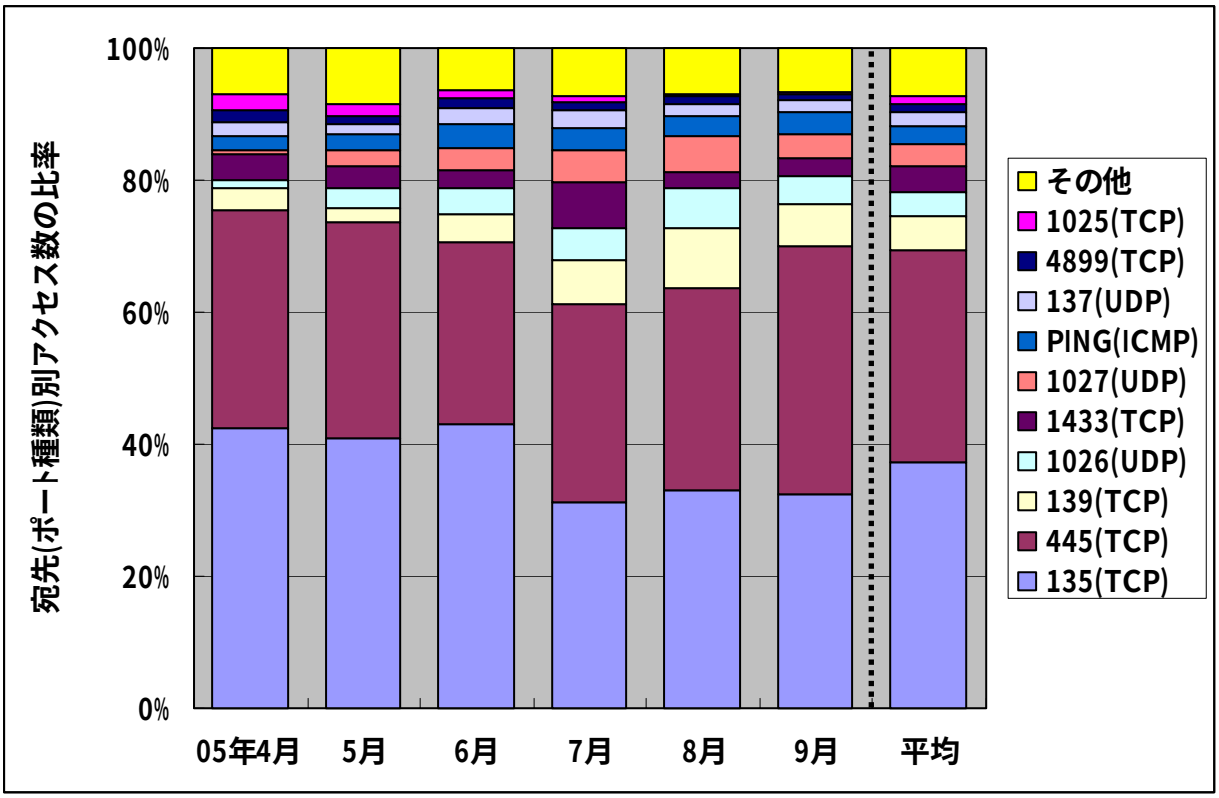
【図 2.4.3 139 ポートへの発信元地域別アクセス数の変化】



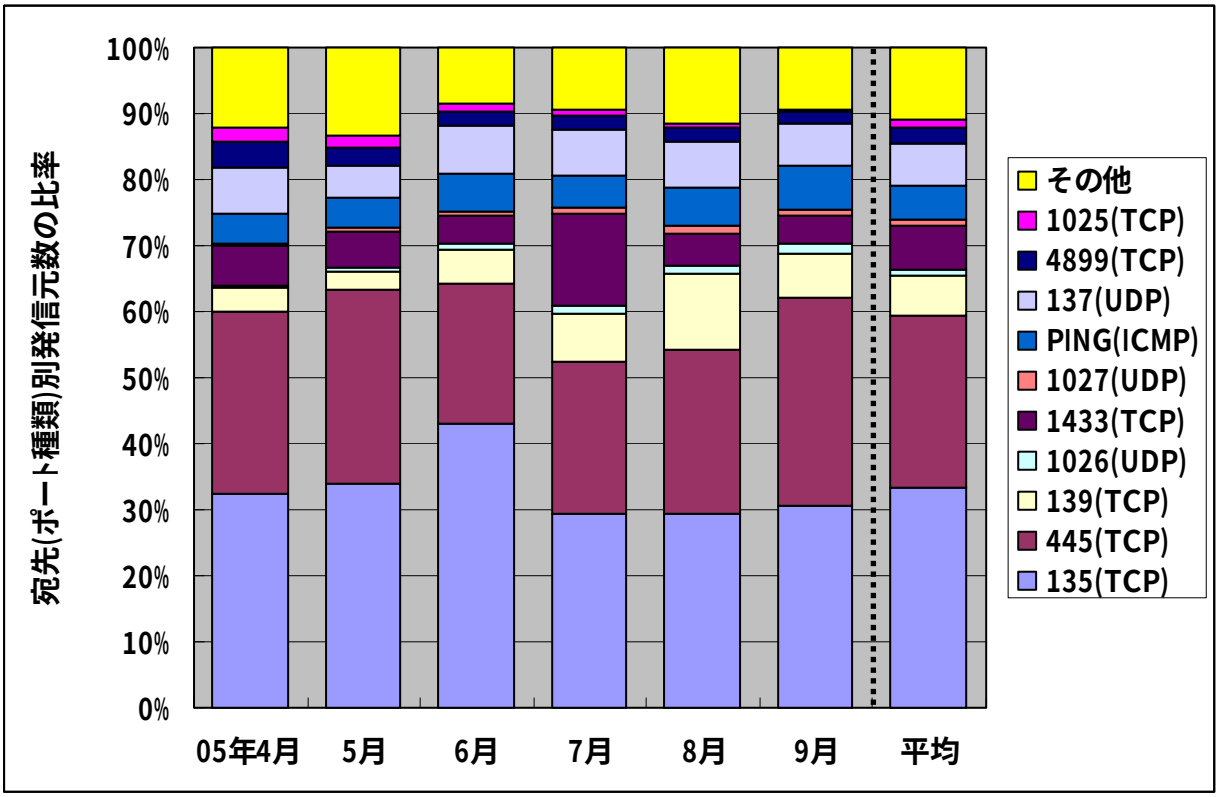
【図 2.4.4 1026/1027 ポートへの発信元地域別アクセス数の変化】

3．統計情報

3.1 2005 年 4 月～9 月の宛先(ポート種類)別の比率

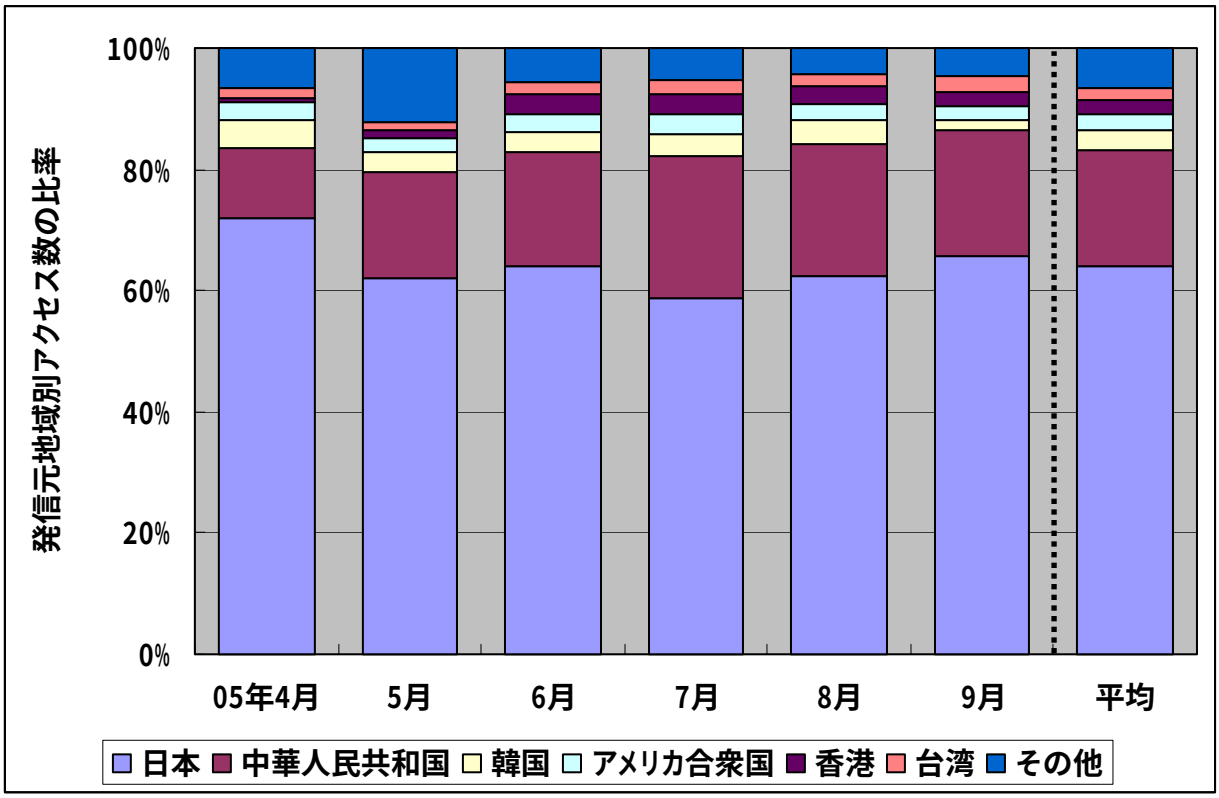


【図 3.1.1 2005 年 4 月～9 月の宛先(ポート種類)別アクセス数の比率】

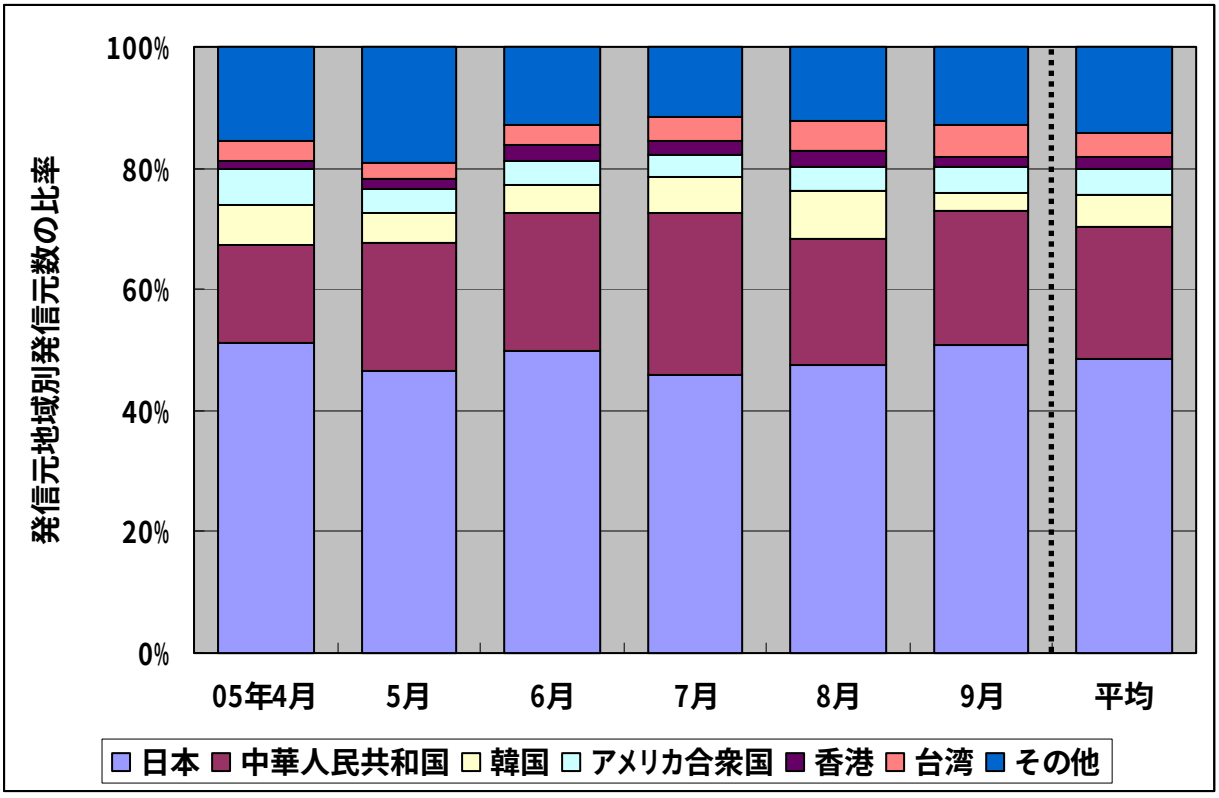


【図 3.1.2 2005 年 4 月～9 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 4 月～9 月の発信元地域別の比率



【図 3.2.1 2005 年 4 月～9 月の発信元地域別アクセス数の比率】

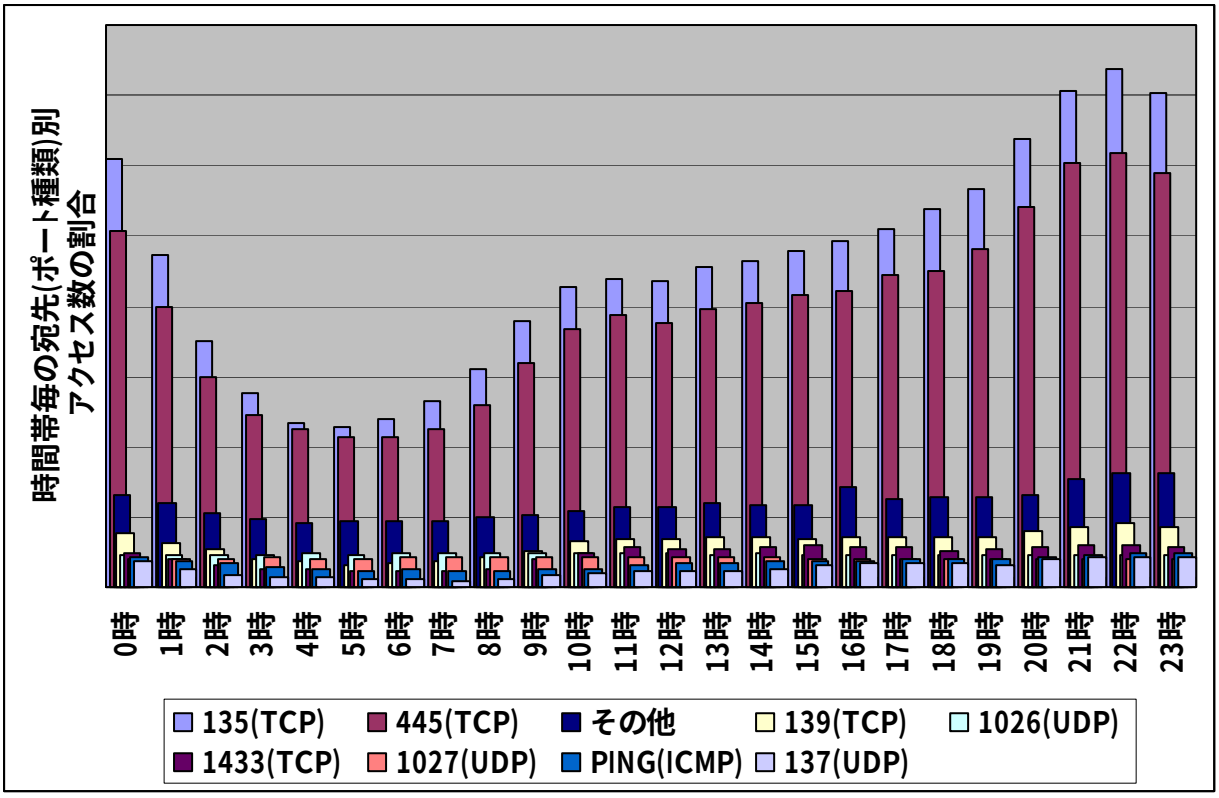


【図 3.2.2 2005 年 4 月～9 月の発信元地域別発信元数の比率】

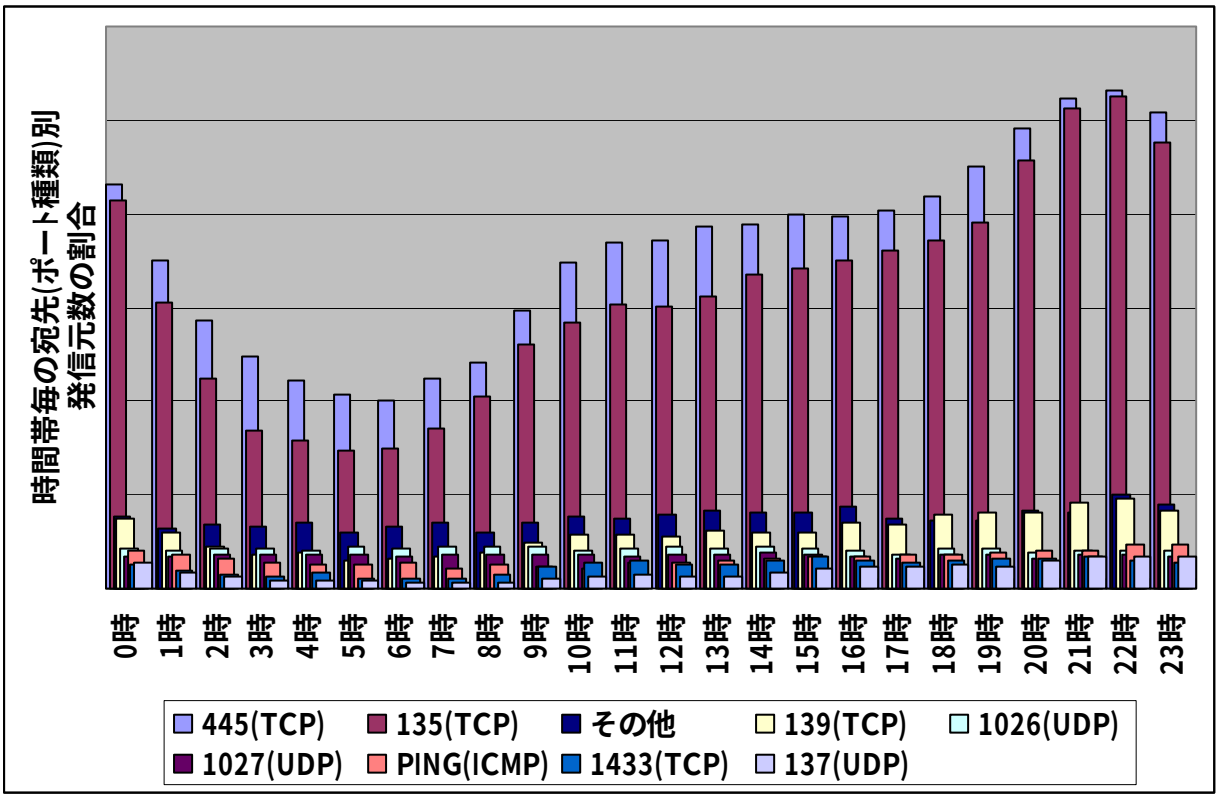
4．その他の統計情報

4.1 2005 年 4 月～9 月の時間帯統計

2005 年 4 月～9 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 9 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～9 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 9 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
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)

■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