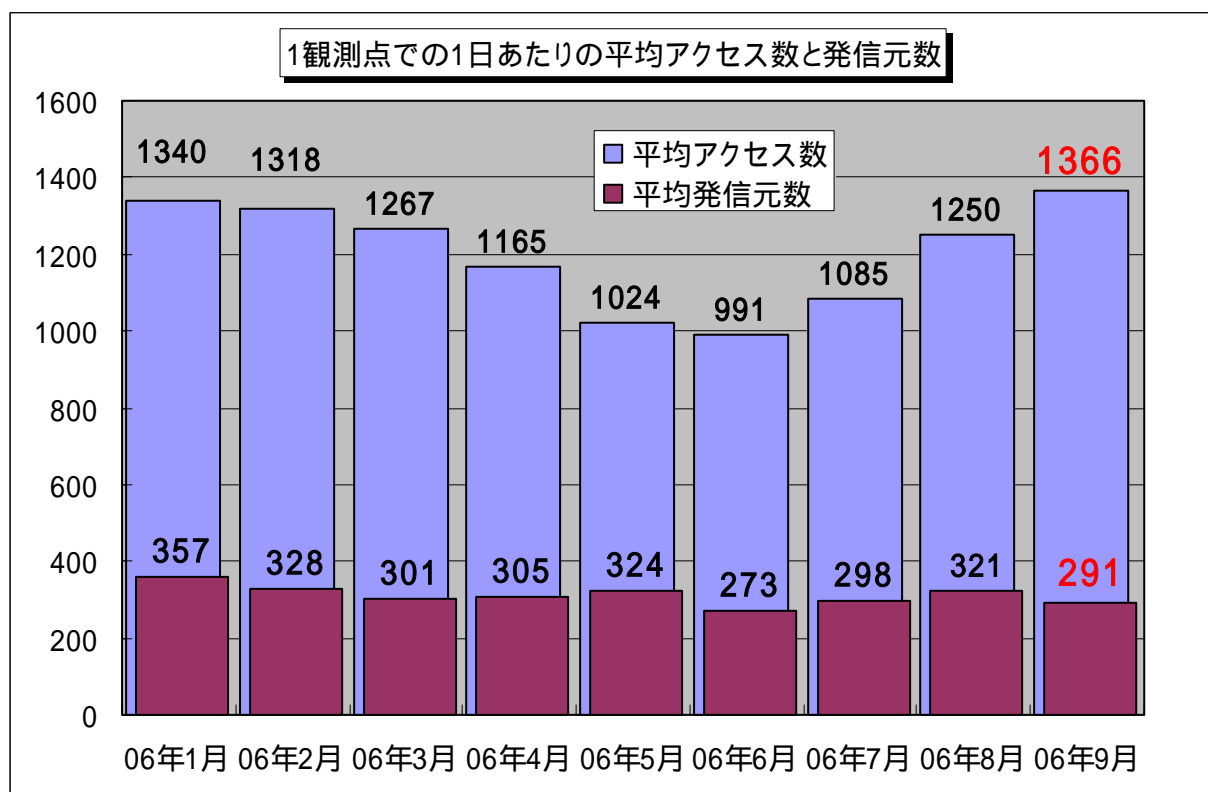


## インターネット定点観測(TALOT2)での観測状況について

### 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、2006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409,772件ありました。1観測点で1日あたり291の発信元から1,366件のアクセスがあったこととなります。

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、291人の見知らぬ人(発信元)から、発信元一人当たり5件の不正と思われるアクセスを受けている**ということになります。



【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】

2006年1月～2006年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に示します。この図を見ると、**期待しない(一方的な)アクセスは、7月以降増加傾向です**。全体的なアクセス内容については、定常化していると言えます。

### 2. 9月のアクセス状況

9月のアクセス状況は、全体的には8月とほぼ同じ状況ですが、**Windowsのぜい弱性を狙ったと思われる139(TCP)ポートへのアクセスが継続しています**。既存のWindowsのぜい弱性を狙っていると思われる不正なアクセスもあいかわらず多いようで、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。

## 2.1 2006年9月の139(TCP)ポートへのアクセス状況

139(TCP)ポートへのアクセスについては、Windows のぜい弱性(MS06-040)を狙ったものと考えられます。このぜい弱性に対する攻撃(検証)コードが公開されており、ぜい弱性を狙った新しいワームや、攻撃コードが仕込まれたボットが広がっている可能性があります。

図 2.1.1、図 2.1.2 および図 2.1.3 に、139(TCP)ポートへの発信元地域別アクセス数と発信元数の遷移を示します。これらの図を見ると、8月18日前後から発信元を国内とするアクセスが増加し、8月23日から韓国方面を発信元とするアクセスが急増しています。実際には、国内からは被害報告や問い合わせがないため、国内での被害状況については分かりませんが、発信元となっている国内のコンピュータにはワームあるいはボットが感染しているものと思われます。韓国方面からのアクセスについては、発信元数から見ると、短期間で終息したようです。アクセスのパターン(同一の観測点に対するアクセス回数)によると、国内からのアクセスと韓国方面からのアクセスは、少し違う様子なので、種類の違う攻撃コード(ワームあるいはボット)と思われる。

9月に入ってから、国内を発信元とするアクセスが多く見受けられますが、国内の発信元数を見ると一定の水準で安定していました。そして、9月15日を境にアクセス数ならびに発信元数が減少しています。今回の攻撃は終息したと考えられます。

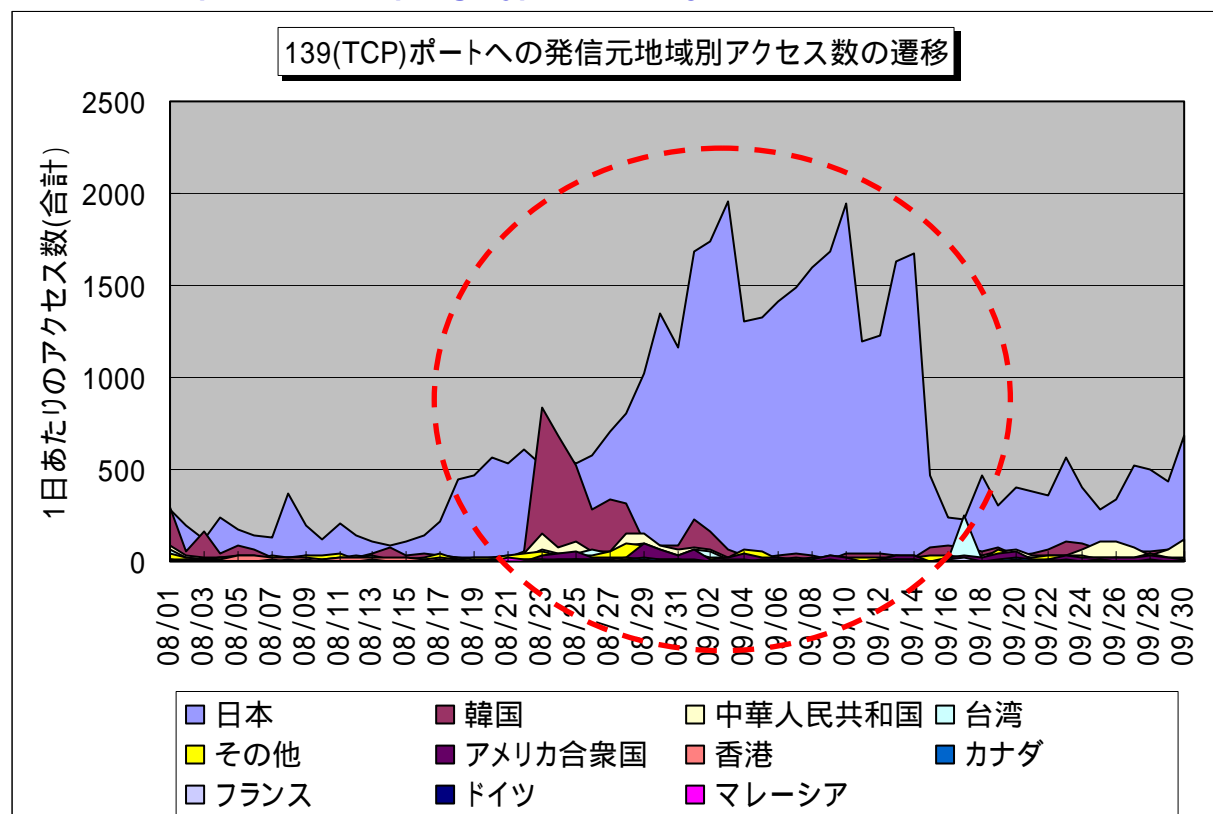
外部からの不正なアクセスを明確に防御している企業(組織)の場合は、特に問題にはなりませんが、インターネットにモデムなどで直接接続する形態のWindows コンピュータを利用されている方は、コンピュータのぜい弱性を解消し、ファイアウォール機能の利用など、被害に遭わないように心掛けて下さい。

コンピュータの個人利用者は、以下の資料を参考にして、ボット対策および不正アクセス対策を実施して下さい。

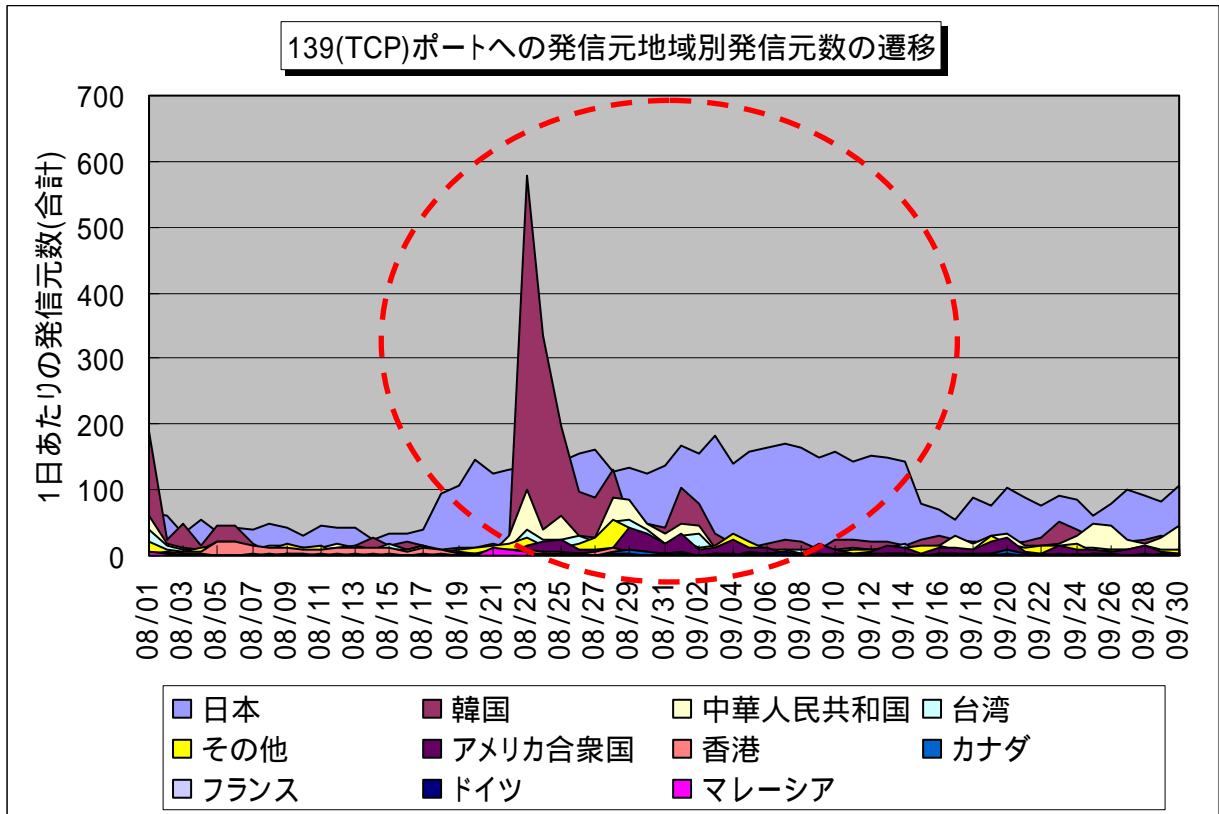
ボット対策のしおり

不正アクセス対策のしおり

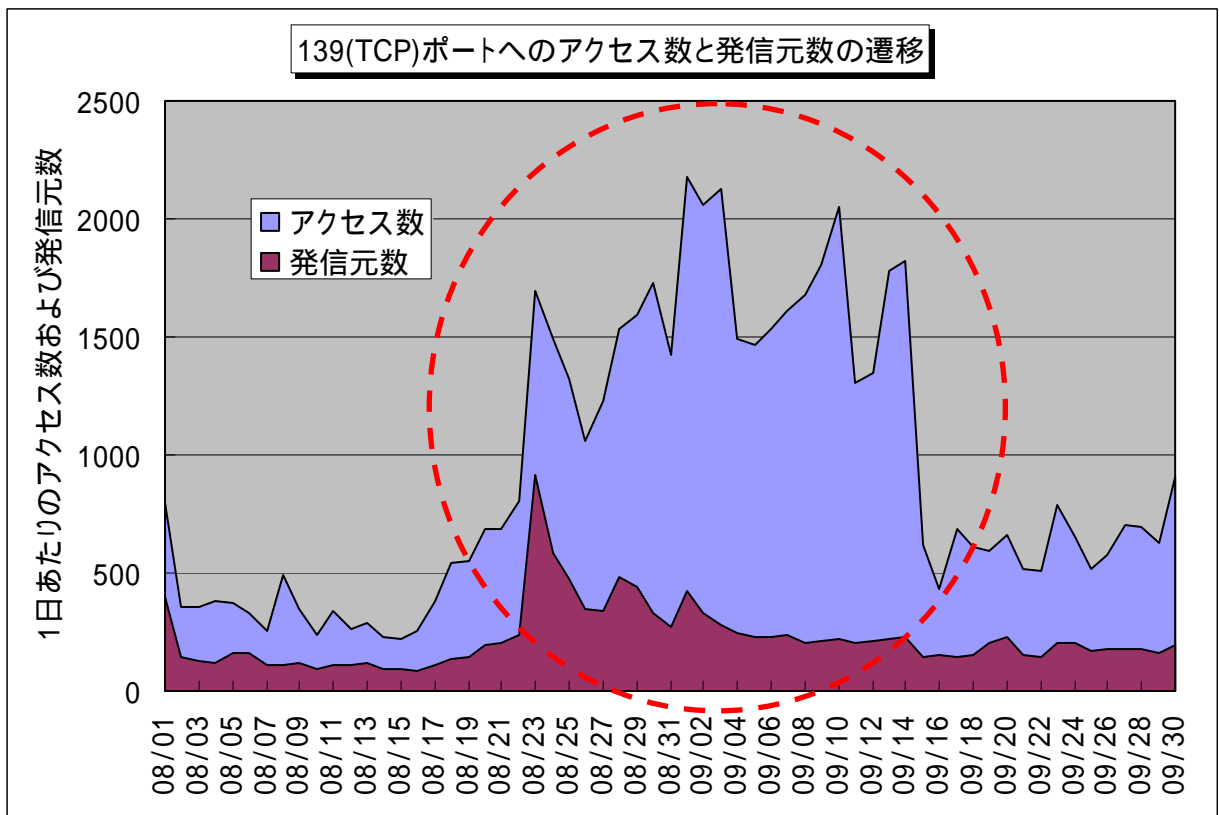
<http://www.ipa.go.jp/security/antivirus/shiori.html>



【図 2.1.1 2006年8月～9月の139(TCP)ポートへの発信元地域別アクセス数の遷移】



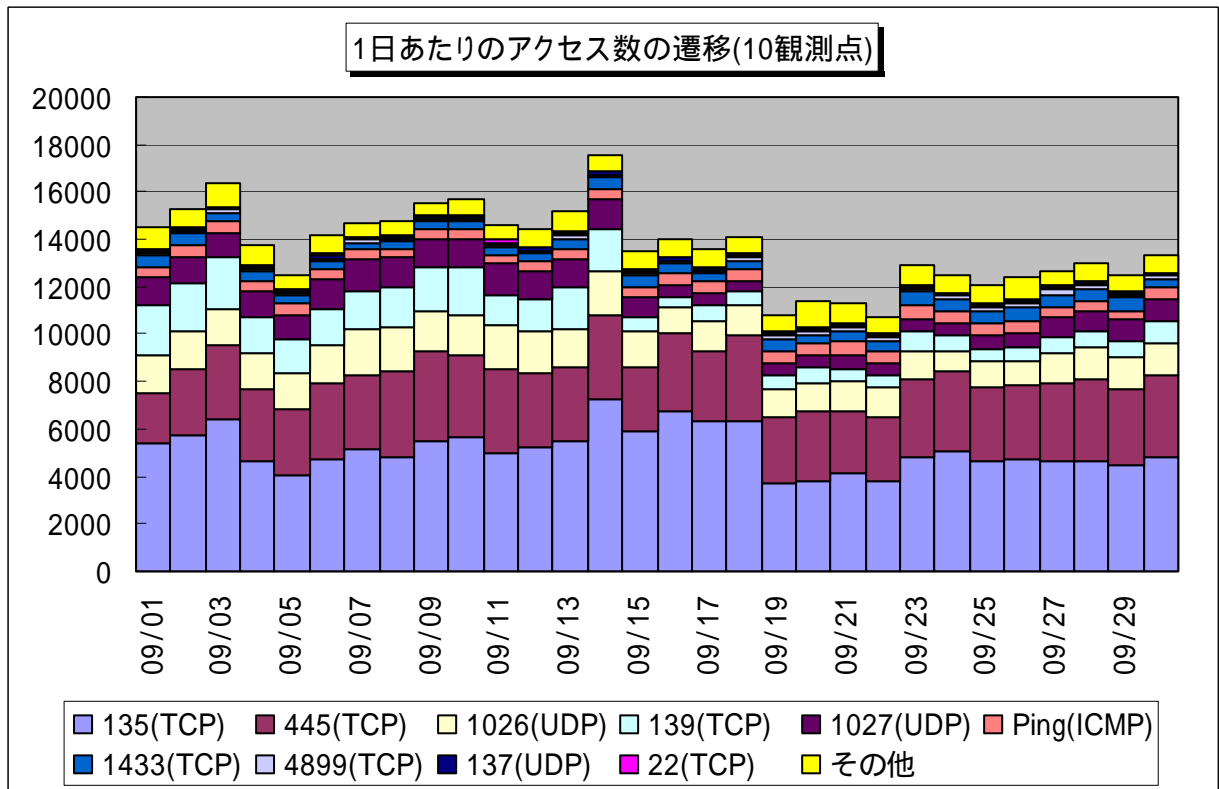
【図 2.1.2 2006 年 8 月～9 月の 139(TCP)ポートへの発信元地域別発信元数の遷移】



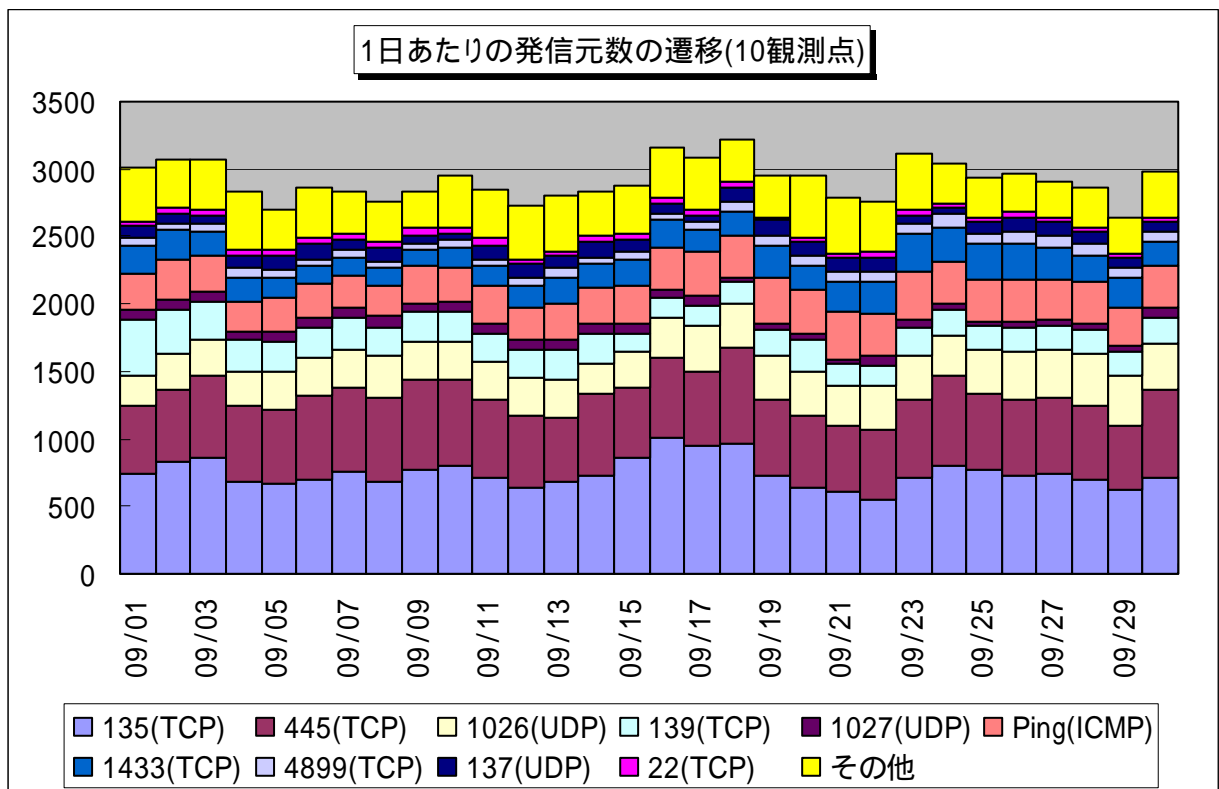
【図 2.1.3 2006 年 8 月～9 月の 139(TCP)ポートへのアクセス数と発信元数の遷移】

## 2.2 2006年9月の一方的なアクセス状況

2006年9月の一方的なアクセス状況(アクセス数)の遷移を図2.2.1に、一方的なアクセス状況(発信元数)の遷移を図2.2.2に示します。



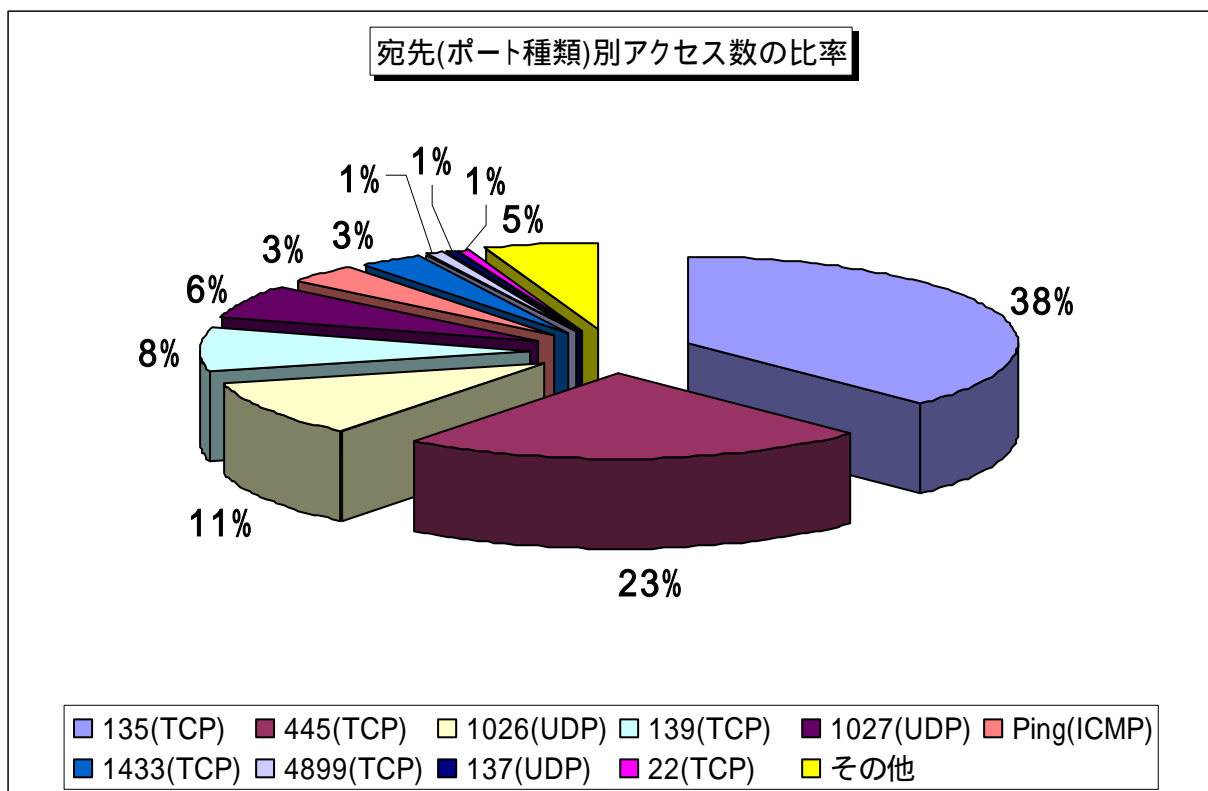
【図 2.2.1 2006年9月の一方的なアクセス状況(アクセス数)】



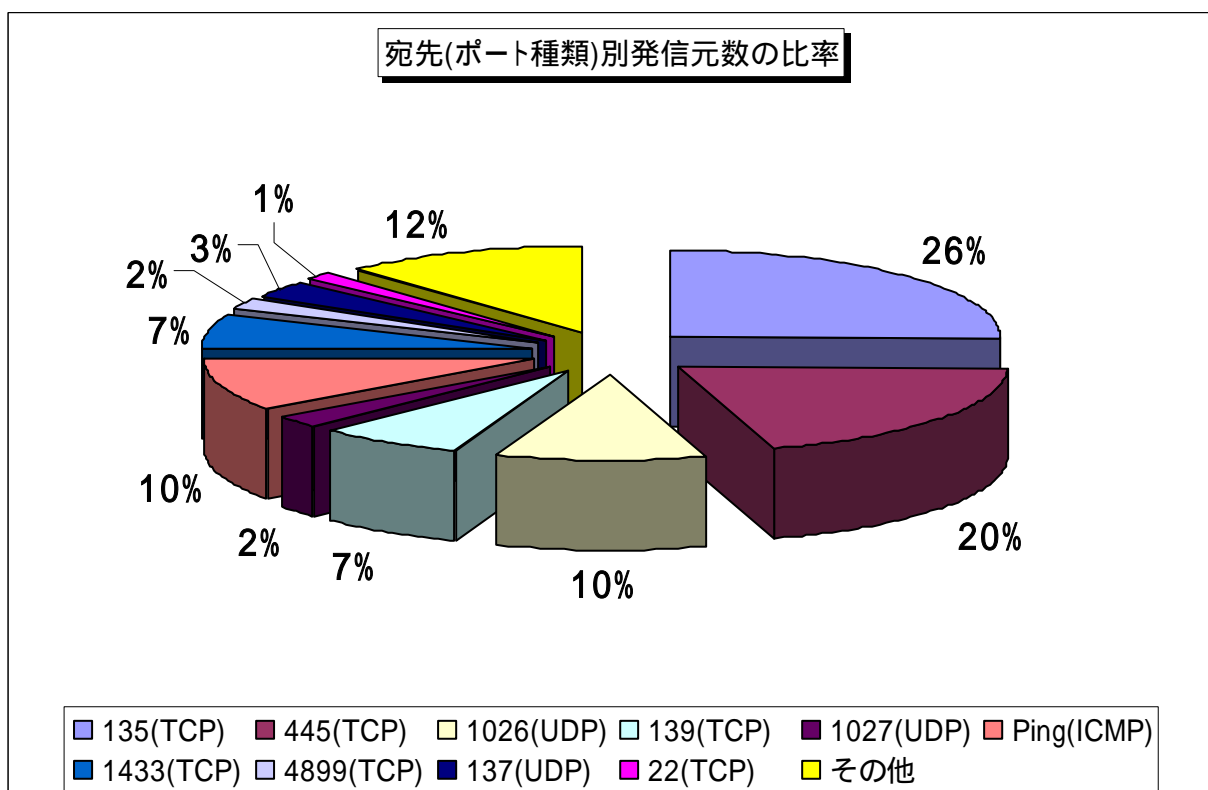
【図 2.2.2 2006年9月の一方的なアクセス状況(発信元数)】

### 2.3 2006年9月の宛先(ポート種類)別の比率

2006年9月の一方的なアクセスの宛先(ポート種類)別アクセス数の比率を図2.3.1に、宛先(ポート種類)別発信元数の比率を図2.3.2に示します。



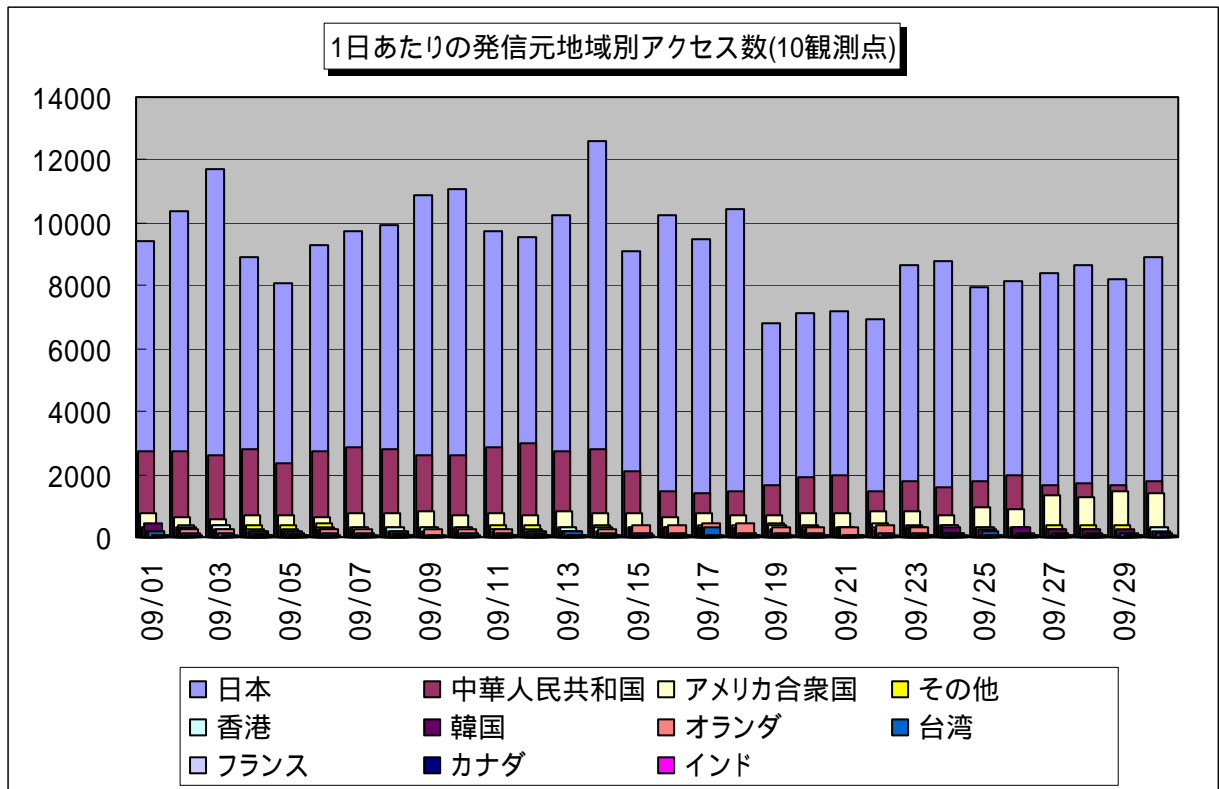
【図 2.3.1 2006年9月の宛先(ポート種類)別アクセス数の比率】



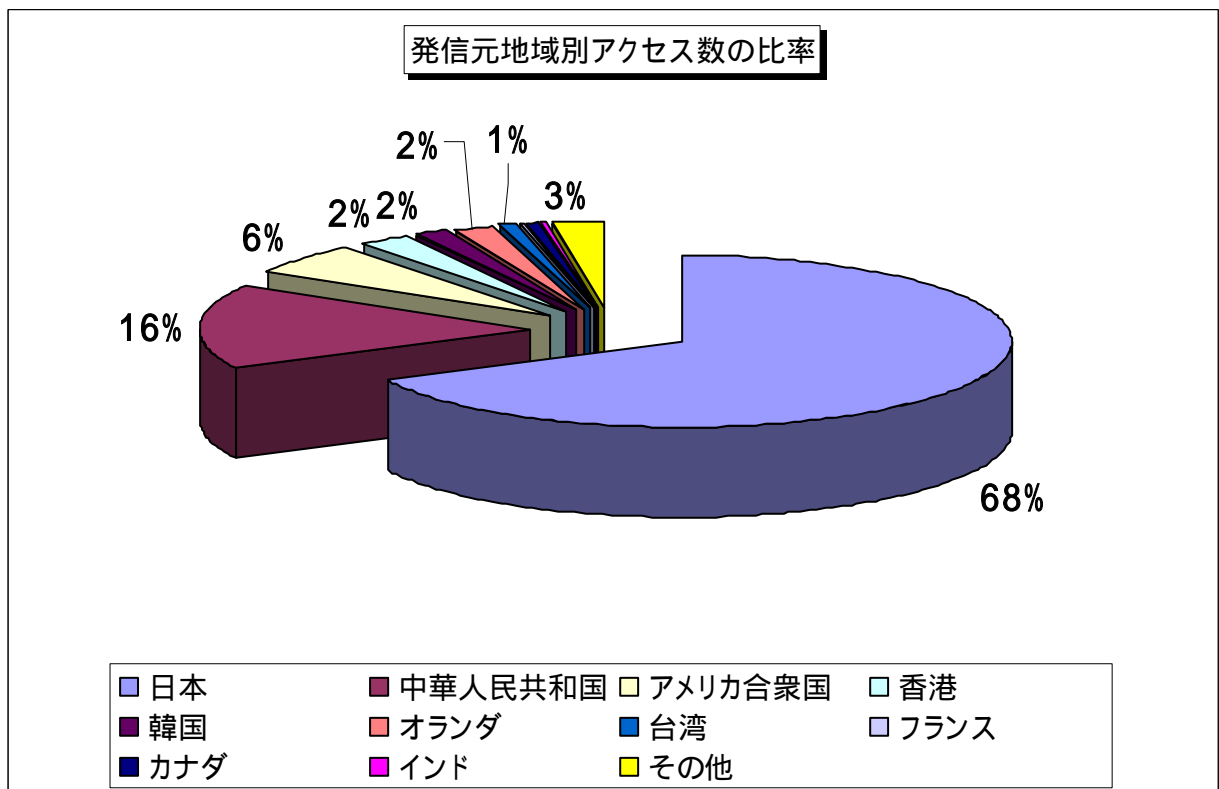
【図 2.3.2 2006年9月の宛先(ポート種類)別発信元数の比率】

## 2.4 2006年9月の発信元地域別アクセス状況

2006年9月の一方的なアクセスの発信元地域別アクセス数の変化を図2.4.1に、発信元地域別アクセス数の比率を図2.4.2に示します。

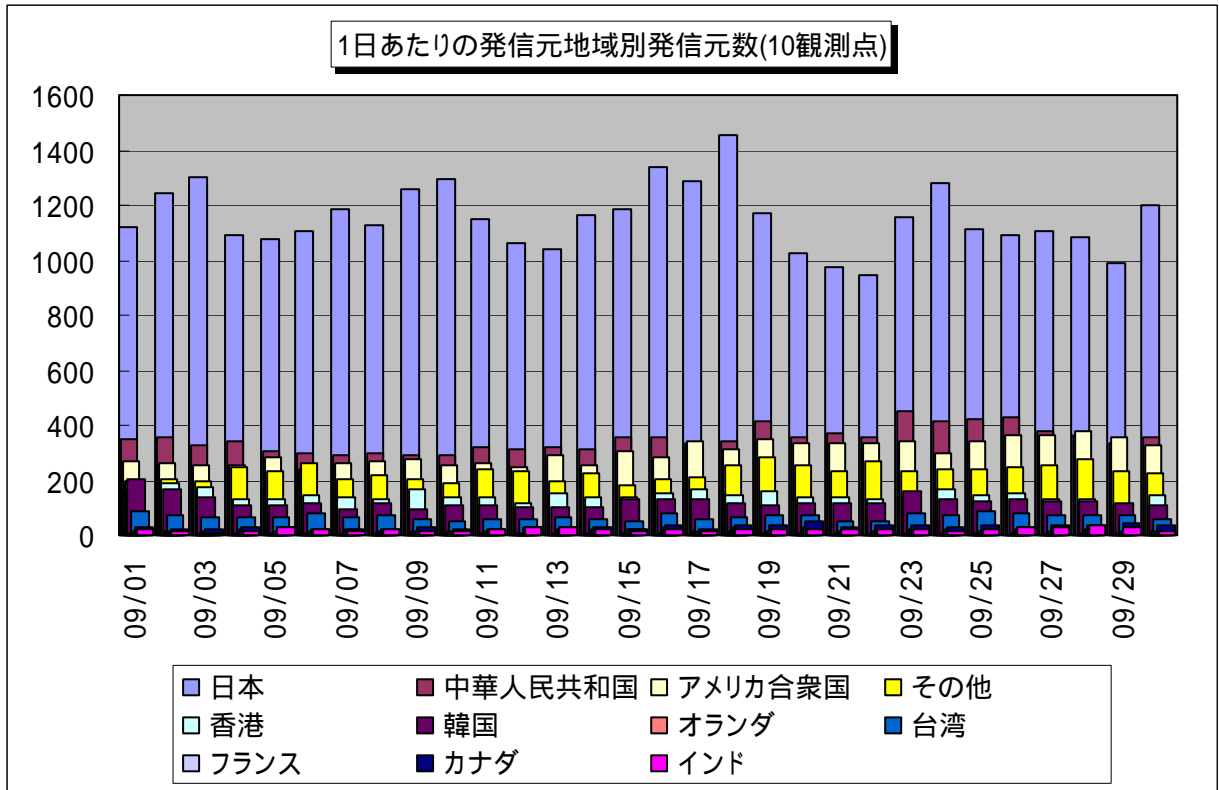


【図 2.4.1 2006年9月の発信元地域別アクセス数の変化】

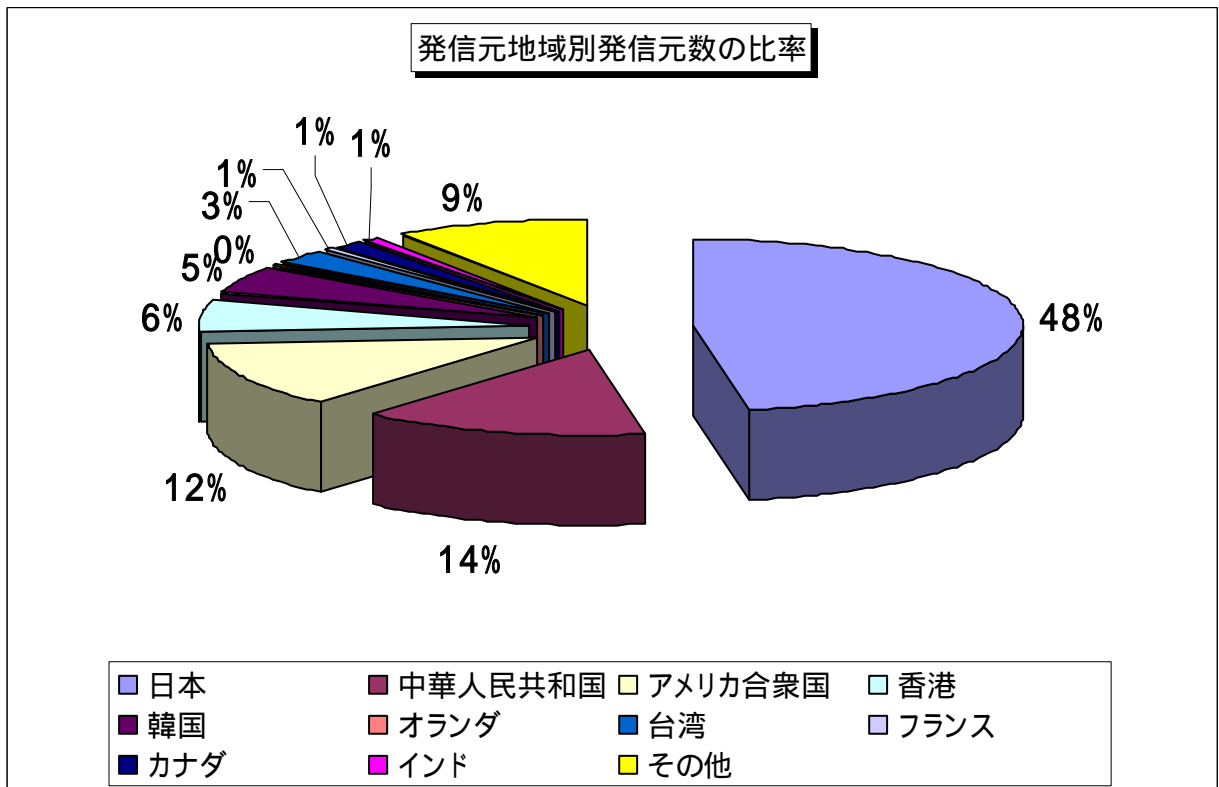


【図 2.4.2 2006年9月の発信元地域別アクセス数の比率】

2006年9月の一方的なアクセスの発信元地域別発信元数の変化を図2.4.3に、発信元地域別発信元数の比率を図2.3.4に示します。



【図 2.4.3 2006年9月の発信元地域別発信元数の変化】

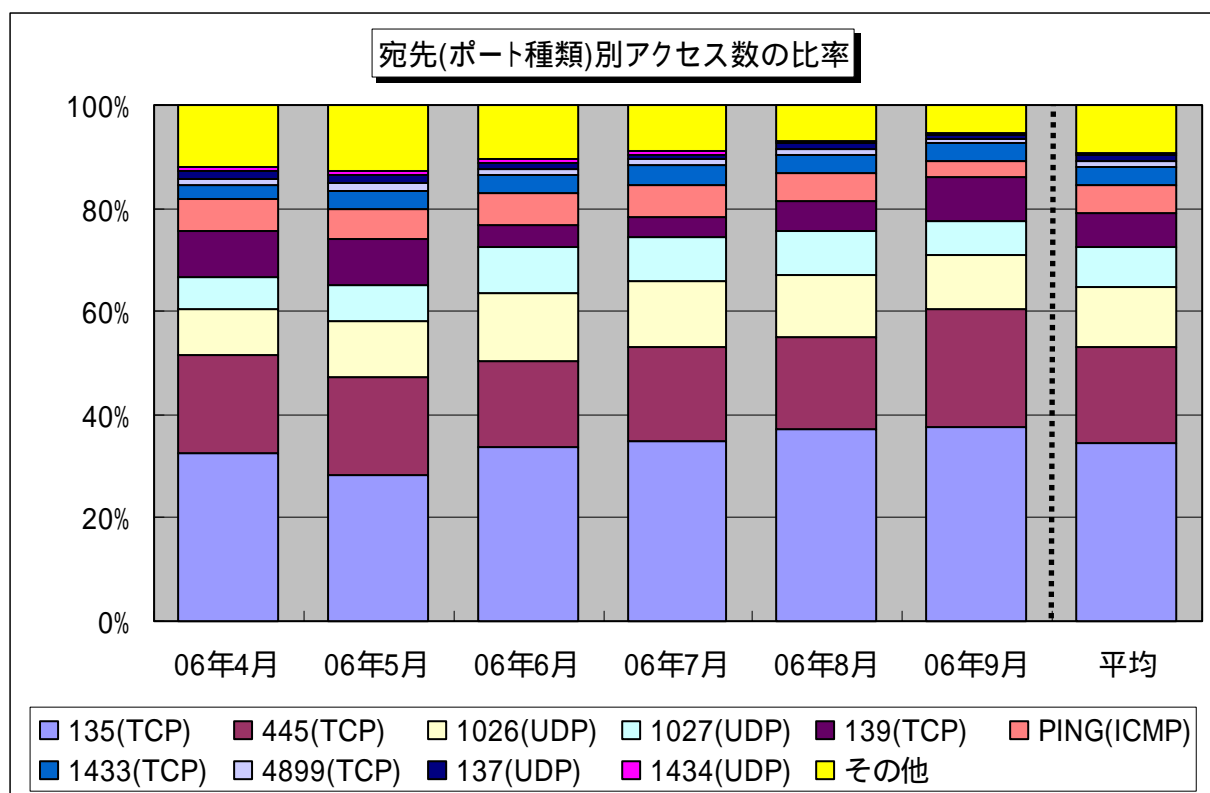


【図 2.4.4 2006年9月の発信元地域別発信元数の比率】

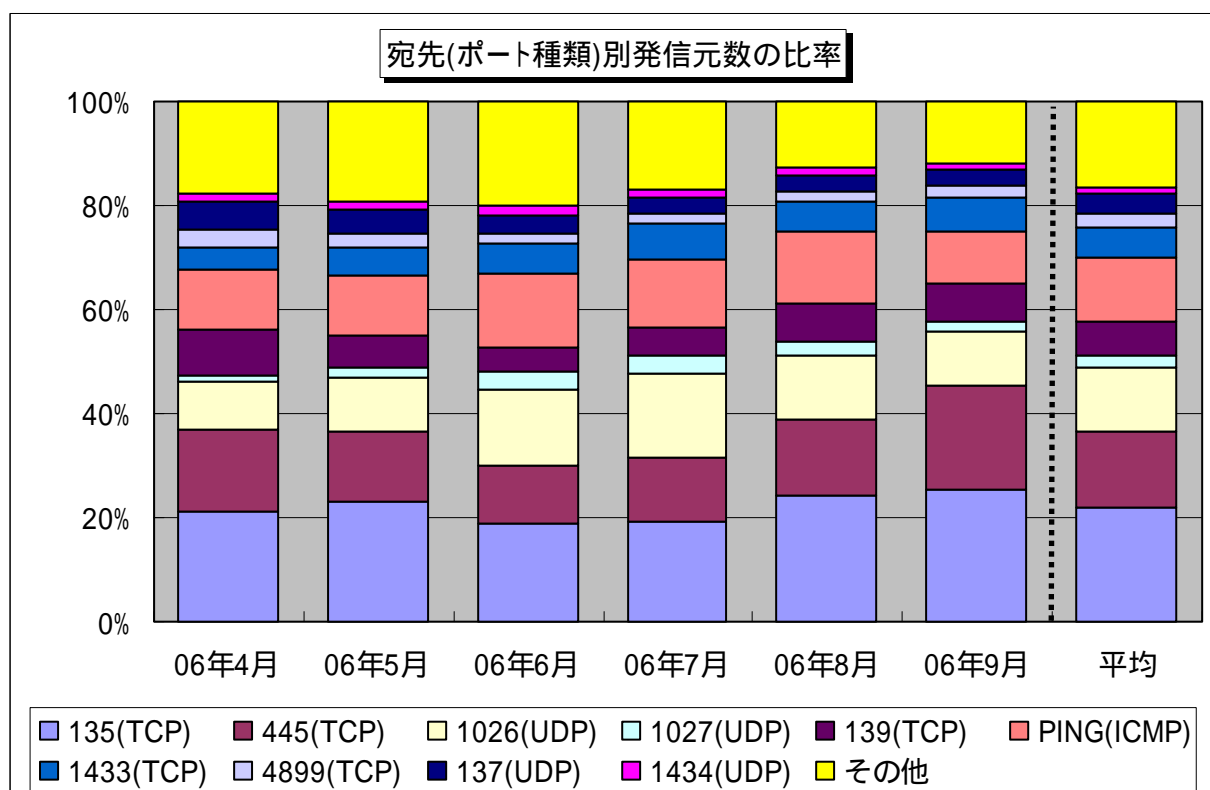
### 3. 統計情報

#### 3.1 2006年4月～2006年9月の宛先(ポート種類)別の比率

2006年4月～2006年9月の宛先(ポート種類)別アクセス数の比率を図3.1.1に、宛先(ポート種類)別発信元数の比率を図3.1.2に示します。



【図 3.1.1 2006年4月～2006年9月の宛先(ポート種類)別アクセス数の比率】

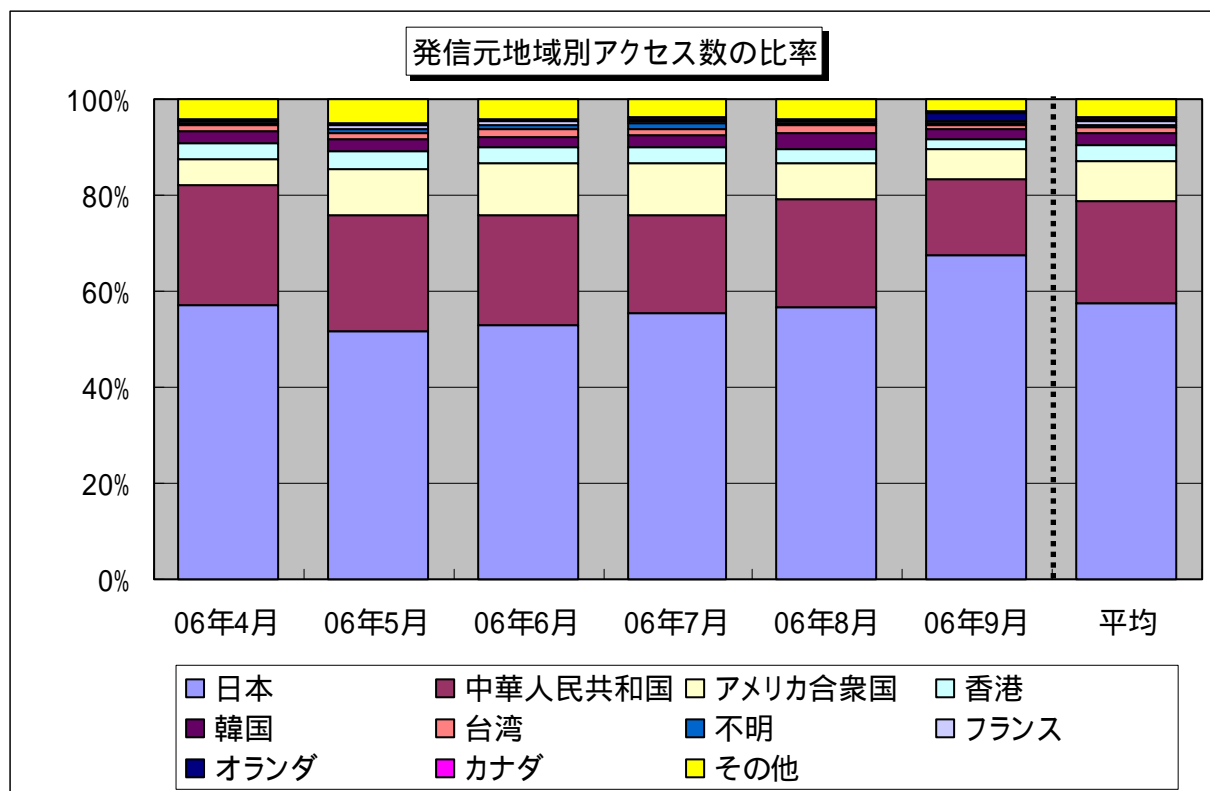


【図 3.1.2 2006年4月～2006年9月の宛先(ポート種類)別発信元数の比率】

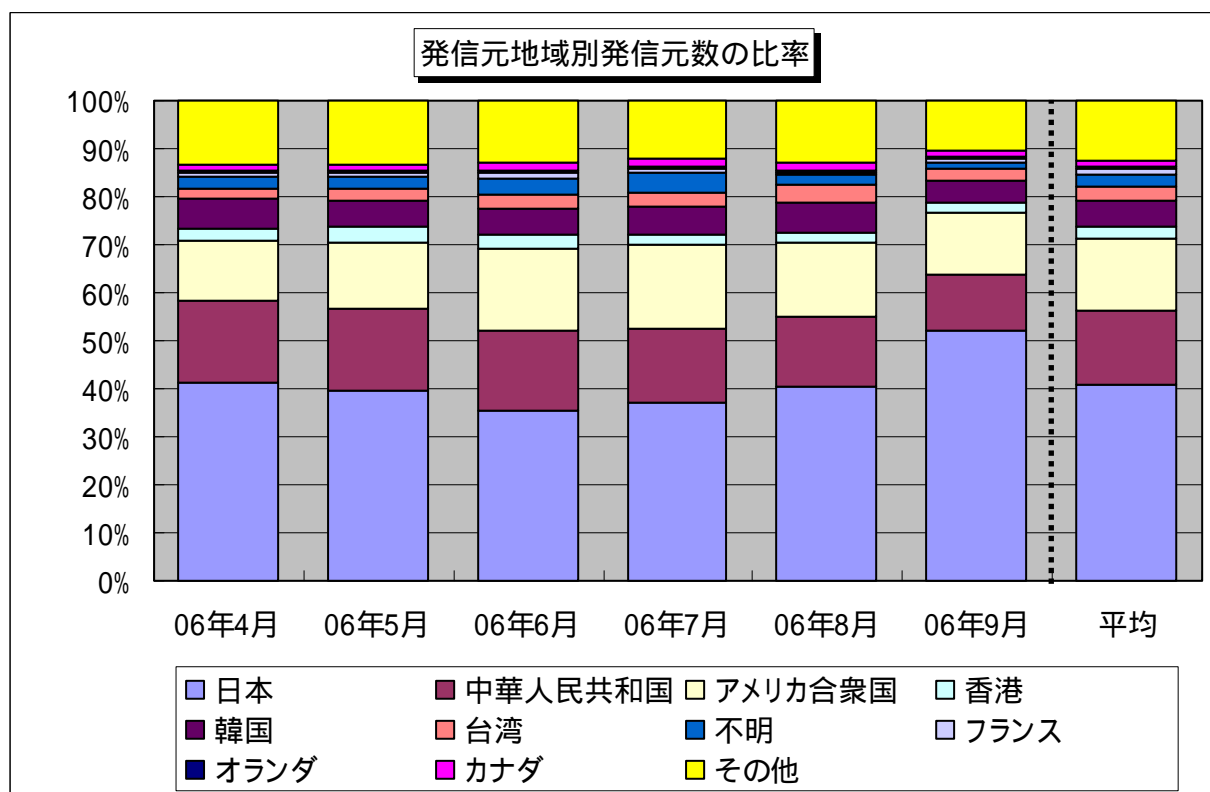


### 3.2 2006年4月～2006年9月の発信元地域別の比率

2006年4月～2006年9月の発信元地域別アクセス数の比率を図3.2.1に、発信元地域別発信元数の比率を図3.2.2に示します。



【図 3.2.1 2006年4月～2006年9月の発信元地域別アクセス数の比率】



【図 3.2.2 2006年4月～2006年9月の発信元地域別発信元数の比率】

## 4. 補足説明

以下に、2006年9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
135(TCP)	Microsoft Windows Remote Procedure Call(RPC)のデフォルトポートであり、RPCに関するぜい弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster など)
445(TCP)	保護のあまいファイル(ネットワーク)共有や Windows2000 特有のぜい弱性を狙った不正アクセスが有名 (W32/Sasser 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
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 のぜい弱性を狙ったアクセスである可能性が高いです
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 のぜい弱性を狙った不正アクセスなど
4899(TCP)	リモート操作を行うための RAdmin のぜい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)
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ます
22(TCP)	パスワードクラッキング攻撃によるシステムへの侵入を目的とした、SSH(Secure Shell: 通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール)を狙ったアクセス

### 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