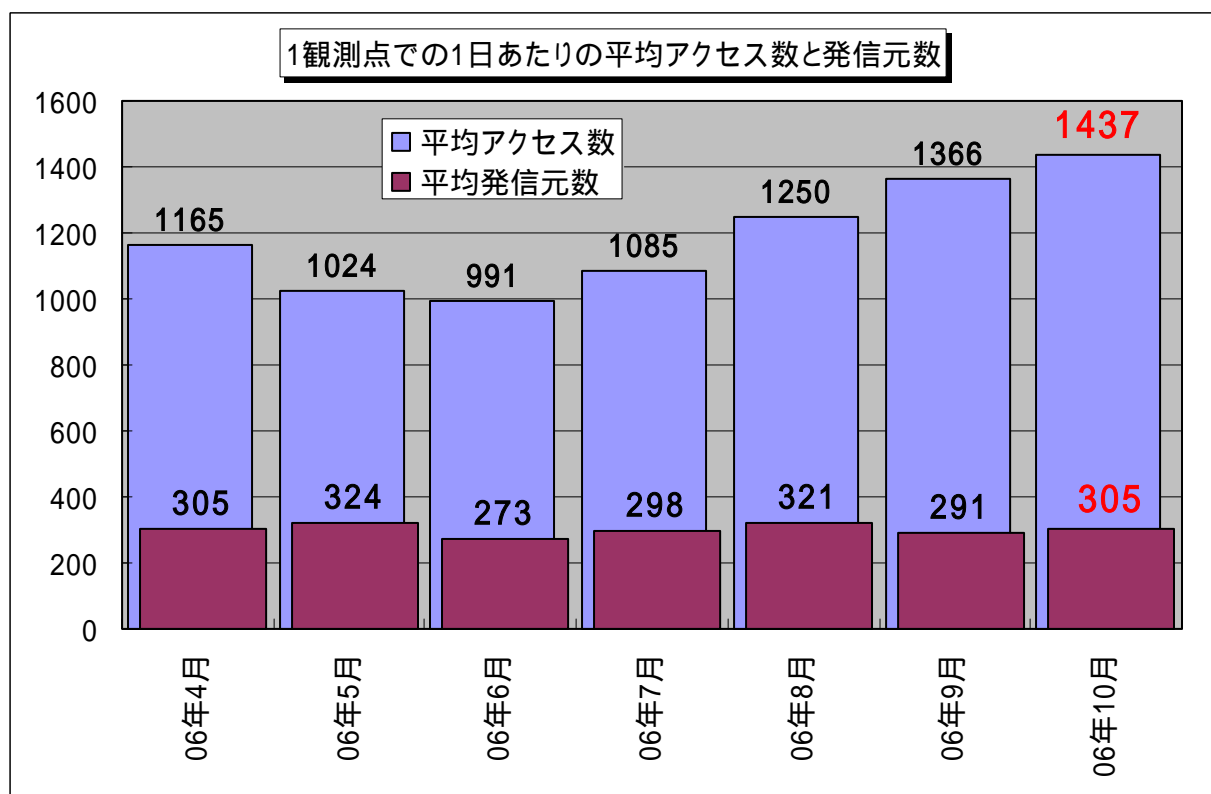


## インターネット定点観測(TALOT2)での観測状況について

### 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416,676件ありました。1観測点で1日あたり305の発信元から1,437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、305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4月～2006年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。

注意)

10月9日と10日は、定点観測システムのメンテナンスのため、観測データの一部が保存されていません。そのため、9日および10日の観測データは統計情報から除外してあります。以降に示す統計情報の図を見ると、9日および10日のデータが欠損していますが、ご了承下さい。

## 2. 10月のアクセス状況

10月のアクセス状況は、全体的には9月とほぼ同じ状況ですが、ファイル交換関連と思われるポートへのアクセスが多い月でした。図2.1.1と図2.2.1を比較すると、これらのアクセスの多さが分かります。これらのファイル交換関連と思われるポートへのアクセスについては、統計情報から除外していますが、今月のトピックとして、これらのアクセスについて状況を説明します。

### 2.1 2006年10月のファイル交換関連と思われるポートへのアクセス状況

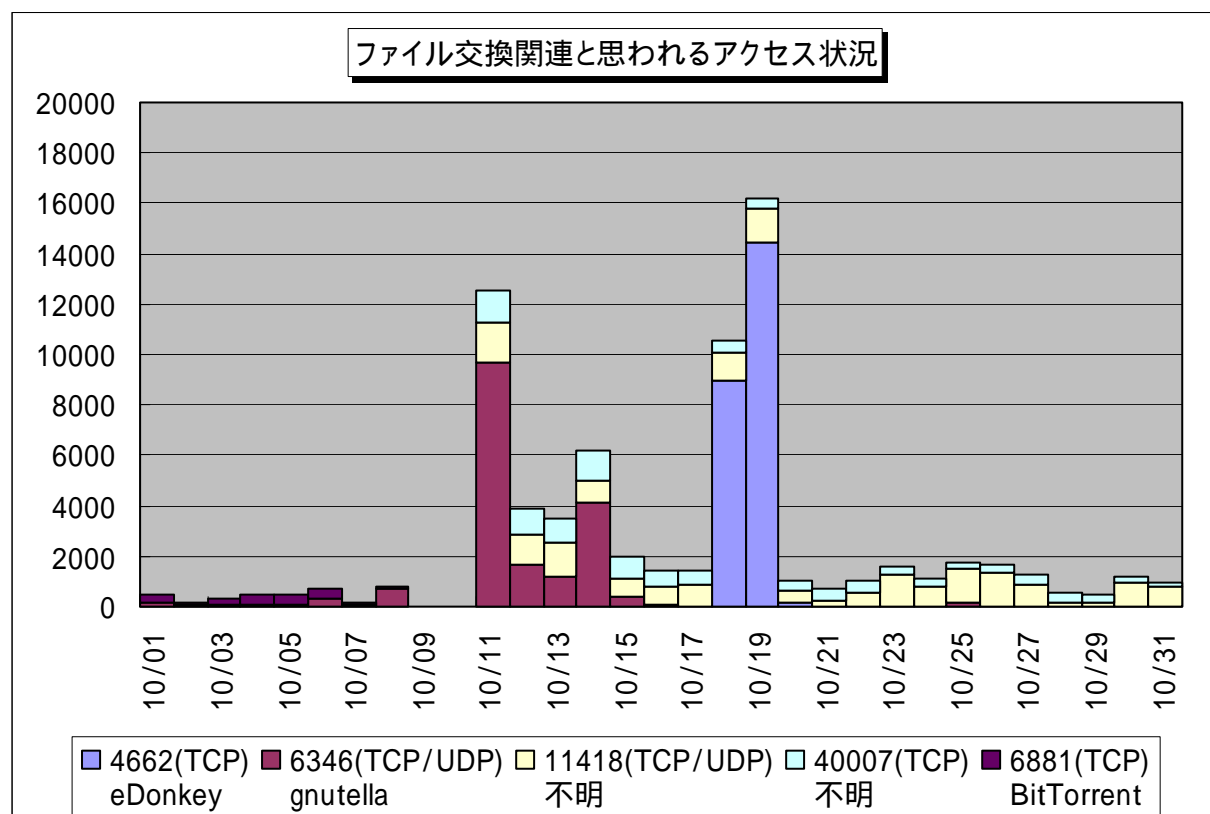
はじめにファイル交換について説明します。ファイル交換とは、ファイル交換ソフトを利用して特定のコンピュータどうして直接ファイル(データ)を交換することです。

ファイル交換の方法にはいろいろありますが、ファイル交換を行うための情報を管理するサーバを中心としたファイル交換ネットワークを組む方式と、ファイル交換ソフトを介して数多くのコンピュータがファイル交換ネットワークを組む方式がほとんどです。

ファイル交換を行うコンピュータは、一般的に、そのコンピュータが使っているIPアドレスによって特定されます。交換できるファイルの情報と、このIPアドレスの情報等がファイル交換ネットワーク上を流れることになります。

ところで、一般的なインターネットの利用者のコンピュータは、利用するプロバイダを介してネットワーク上の空いているIPアドレスを動的に割り当てられるのが普通です。そのため、ファイル交換を利用するコンピュータのIPアドレスも、ネットワークとの接続を行うたびに、違うIPアドレスになります。このため、ファイル交換を行っていたコンピュータがネットワークから切断されても、ファイル交換ネットワーク上には、以前使っていたIPアドレスの情報が残ってしまう場合があります。この残ってしまったIPアドレスが、同じプロバイダ内の違う利用者のコンピュータに割り当てられ、このコンピュータに対して、同じファイル交換を利用する別のコンピュータからファイル交換の接続要求(アクセス)がくることになります。

以下に示すアクセスのほとんどが、このような状況で発生したアクセスと考えられます。



【図 2.1.1 2006年10月のファイル交換関連と思われるアクセス数の遷移】

これらのアクセスの発信元については、以下の通り

- ・ 4662(TCP)ポートへのアクセスの発信元はスペイン方面がほとんど(図 2.1.2 参照)
- ・ 6346(TCP/UDP)ポートへのアクセスの発信元は日本国内がほとんど
- ・ 11418(TCP/UDP)ポートへのアクセスの発信元は台湾方面がほとんど
- ・ 40007(TCP)ポートへのアクセスの発信元も日本国内がほとんど
- ・ 6881(TCP)ポートへのアクセスの発信元も日本国内がほとんど

でした。

著作権のあるデータ(ファイル)を非合法にファイル交換する人たちがいるため、最近ではサーバを中心に持つタイプのファイル交換では、サーバが閉鎖に追い込まれたり、違法なファイル交換を行った人が逮捕されたりという事件も起こっています。

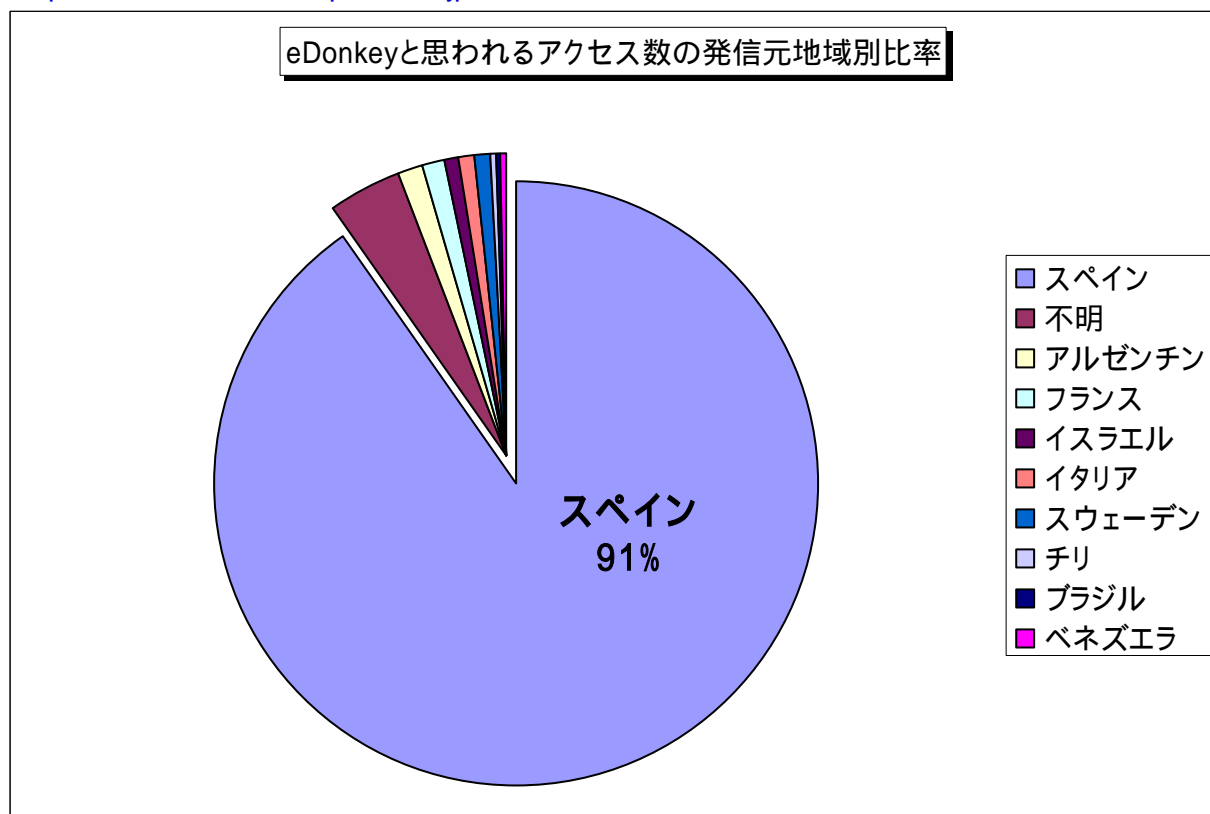
さらに、ファイル交換を介した情報漏えいの問題も多発しているため、ファイル交換を問題視する傾向もあるようです。

図 2.1.1 に示した、一番アクセス数の多かった 4662(TCP)は、eDonkey と呼ばれるファイル交換ソフトを利用したアクセスのようです。eDonkey については、欧州を中心に eDonkey のサーバの閉鎖やファイル交換ソフトの配布停止となったために、残ったサーバが閉鎖される前に、駆け込み的にファイルをダウンロードしようと、急激にアクセスが増加したものと考えられます。

#### 参考情報

国際レコード産業連盟、違法ファイル交換に対し 17 カ国で 8,000 件の訴訟 (2006/10/18)

<http://internet.watch.impress.co.jp/cda/news/2006/10/18/13661.html>



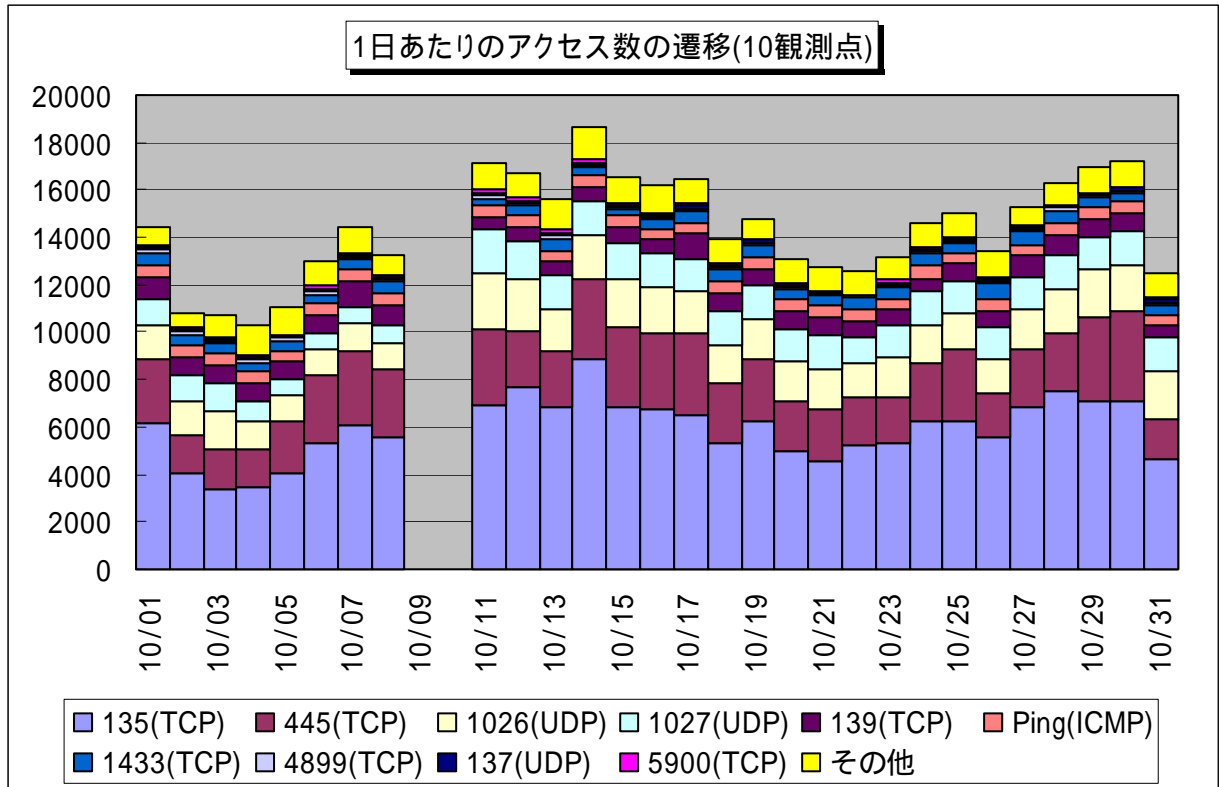
【図 2.1.2 eDonkey とと思われるアクセス数の発信元地域別比率】

特定のIPアドレスに、このようなアクセスが集中すると、ほとんどDoS攻撃を受けている状況となります。このようなアクセスは、ほとんどがファイル交換を自動化した場合に発生するものであり、ファイル交換の利用者の方には、このような状況を理解いただき、ファイル交換の接続先の確認をあらかじめ行ってから、アクセスするように心掛けていただきたいものです。

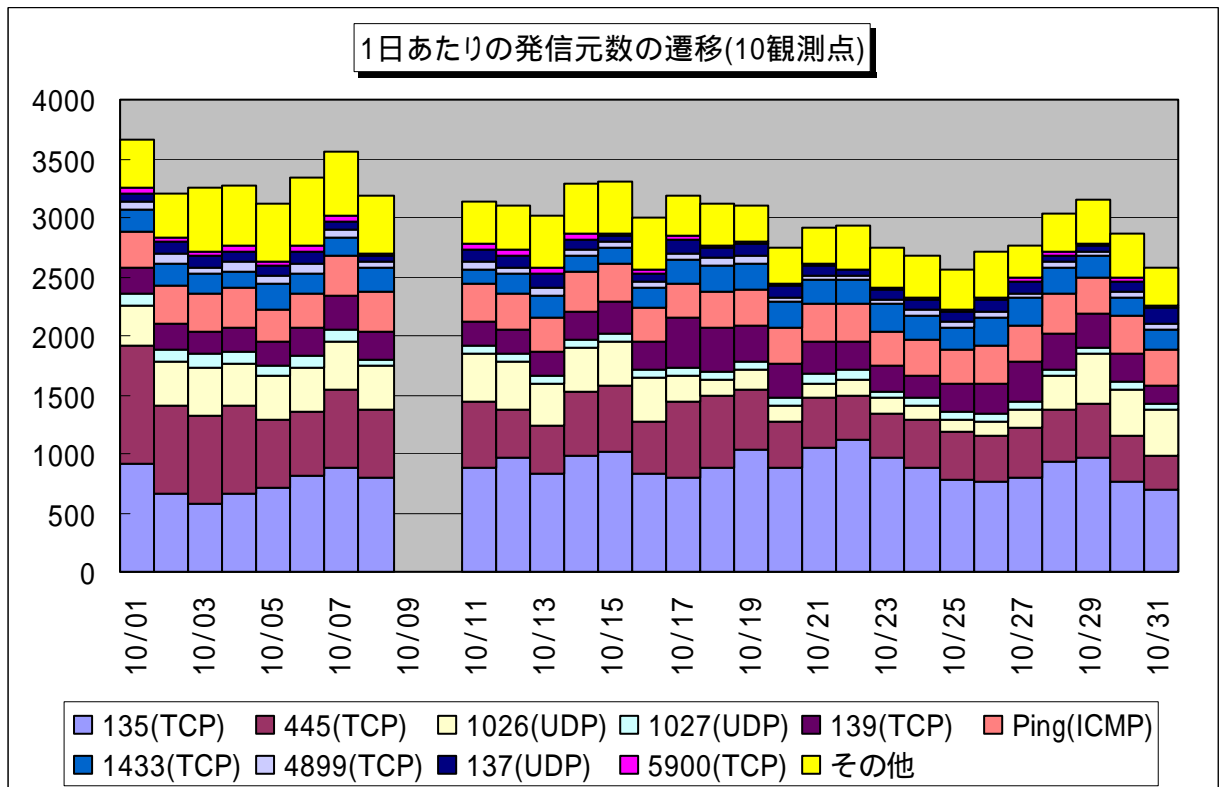
さらに、ファイル交換を介した情報漏えい問題も多発していますので、利用者には、ファイル交換の仕組みをご理解いただき、さらなる注意を払っていただきたいものです。

## 2.2 2006年10月の一方的なアクセス状況

2006年10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。



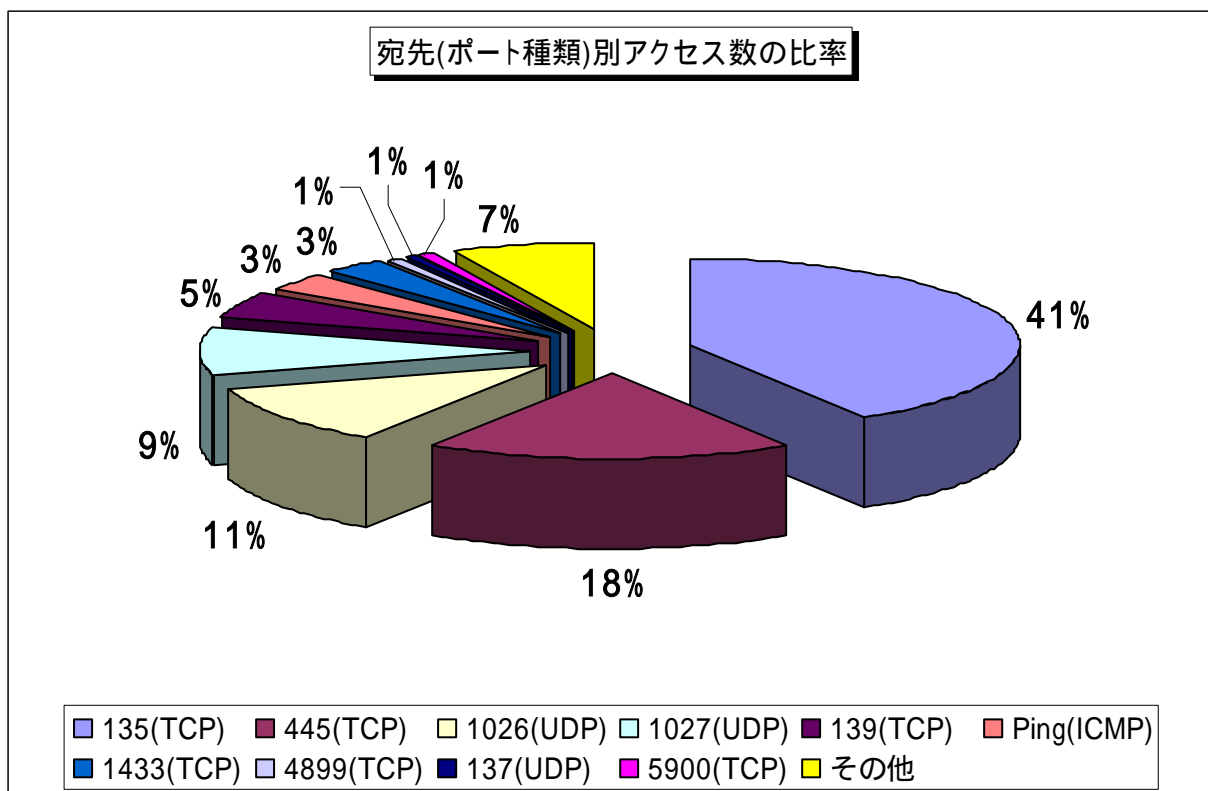
【図 2.2.1 2006年10月の一方的なアクセス状況(アクセス数)】



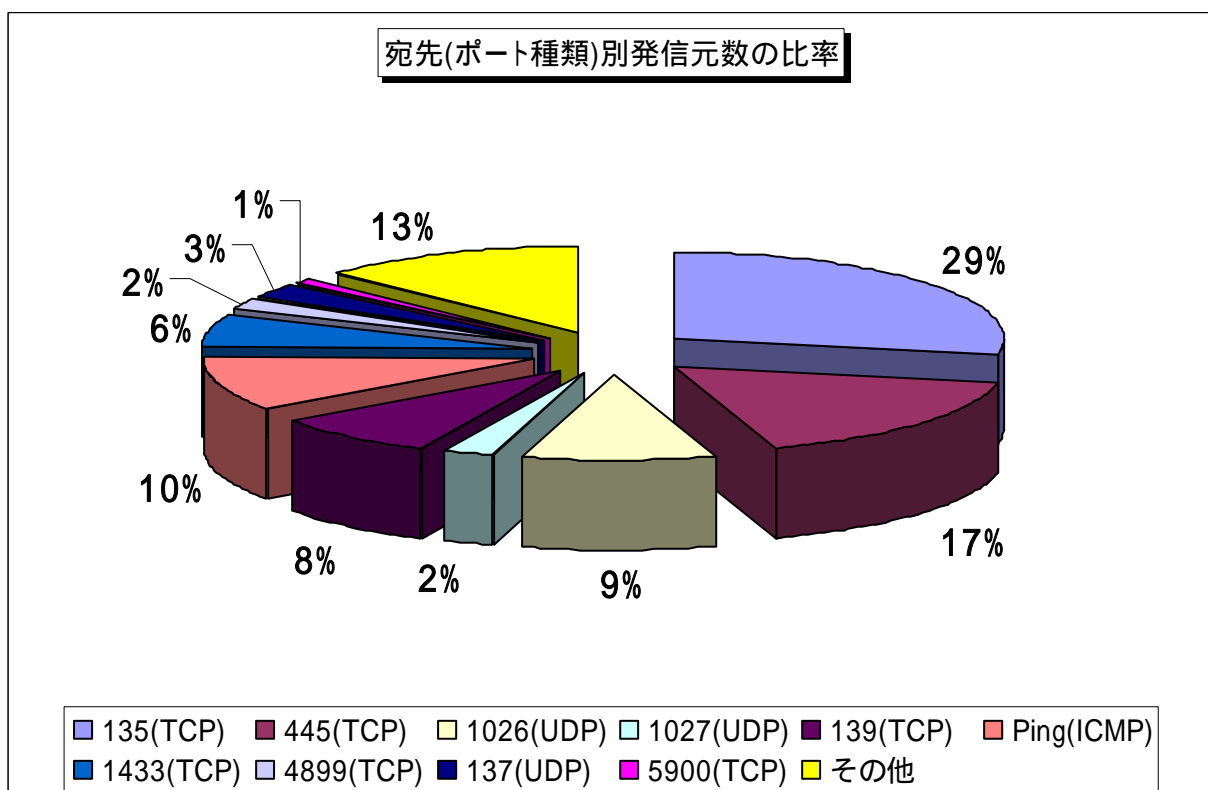
【図 2.2.2 2006年10月の一方的なアクセス状況(発信元数)】

### 2.3 2006年10月の宛先(ポート種類)別の比率

2006年10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。



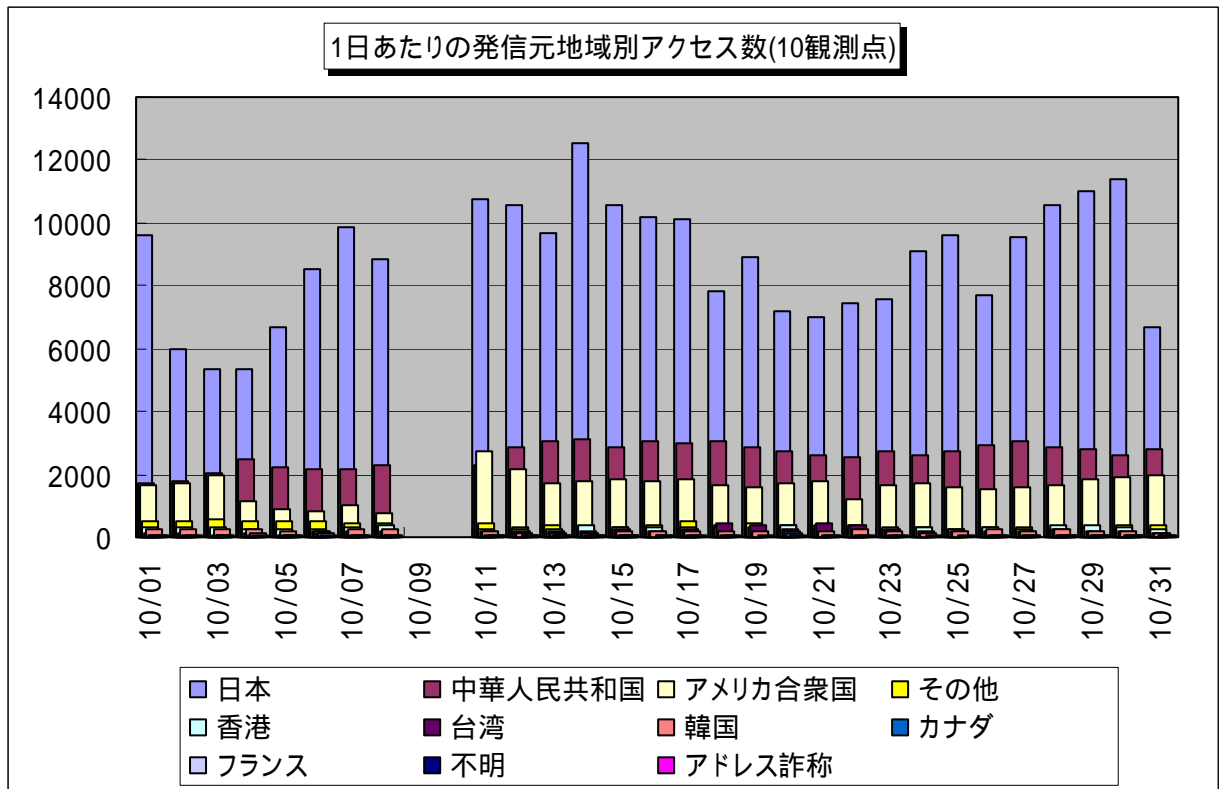
【図 2.3.1 2006年10月の宛先(ポート種類)別アクセス数の比率】



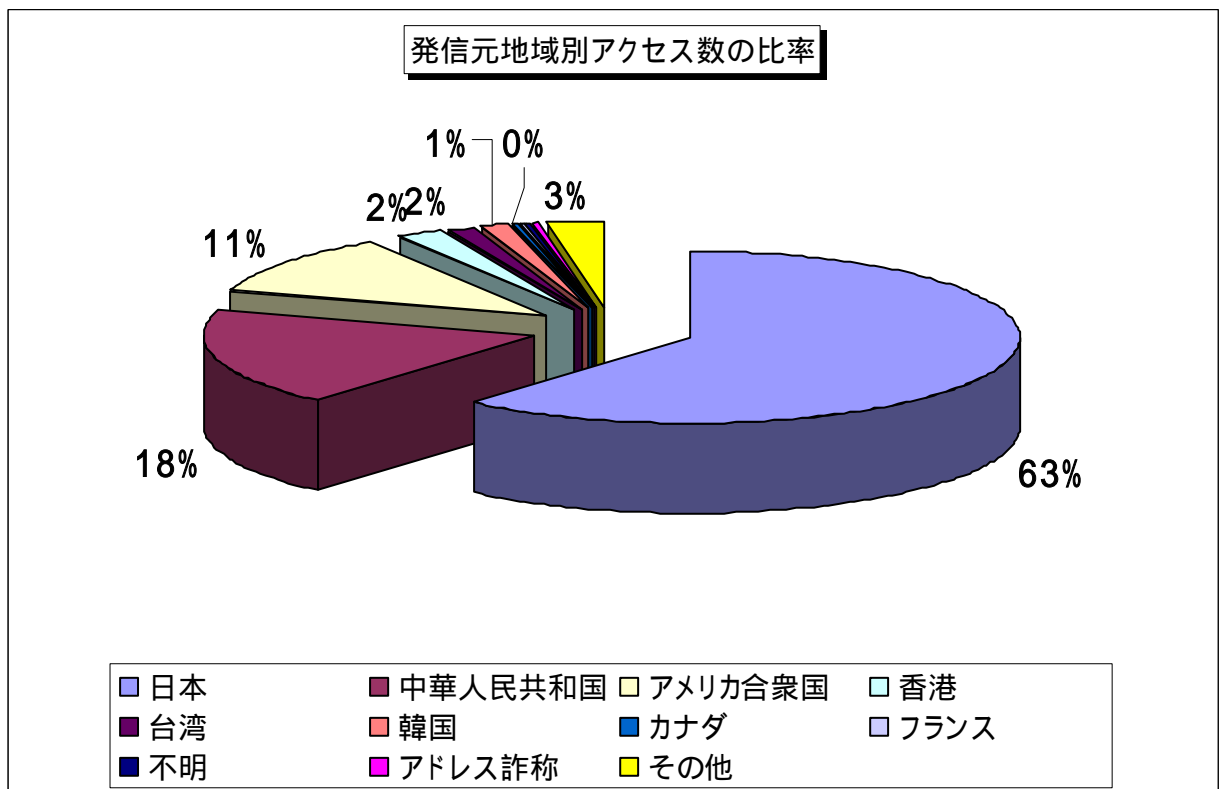
【図 2.3.2 2006年10月の宛先(ポート種類)別発信元数の比率】

## 2.4 2006年10月の発信元地域別アクセス状況

2006年10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。

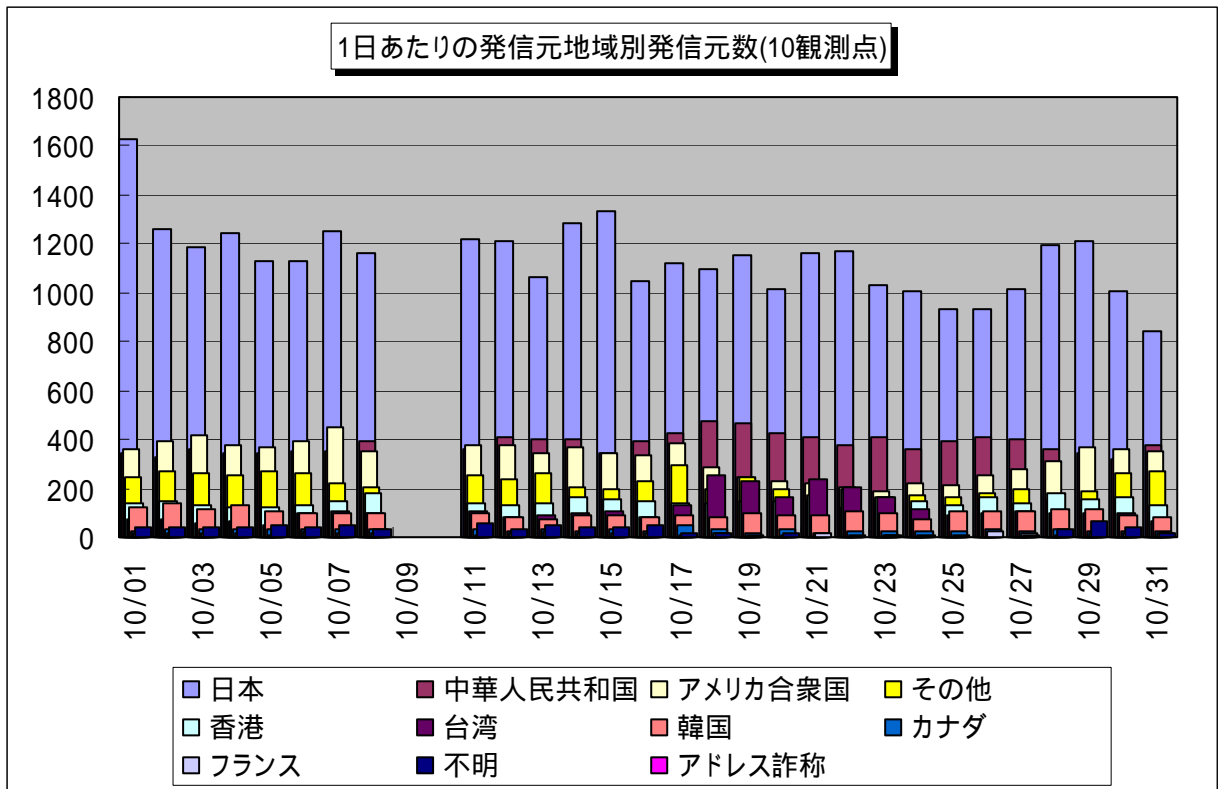


【図 2.4.1 2006年10月の発信元地域別アクセス数の変化】

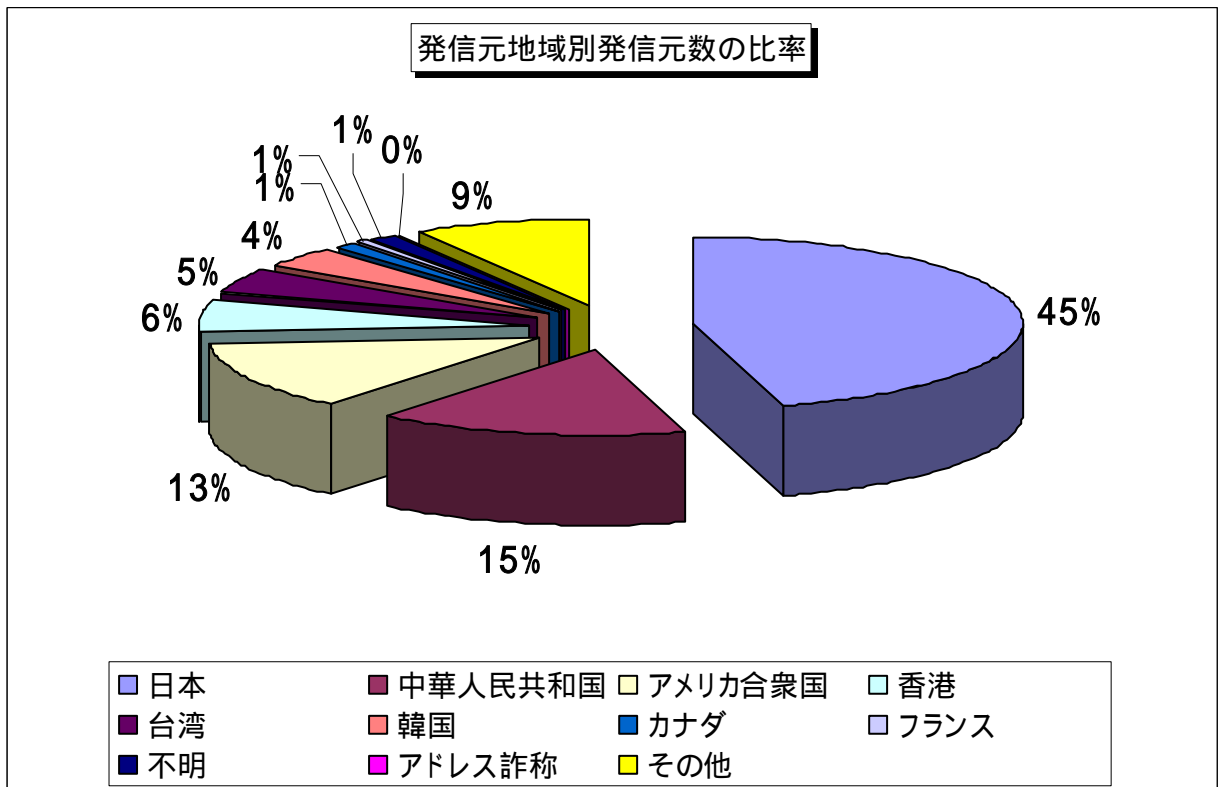


【図 2.4.2 2006年10月の発信元地域別アクセス数の比率】

2006年10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2.4.4に示します。



【図 2.4.3 2006年10月の発信元地域別発信元数の変化】

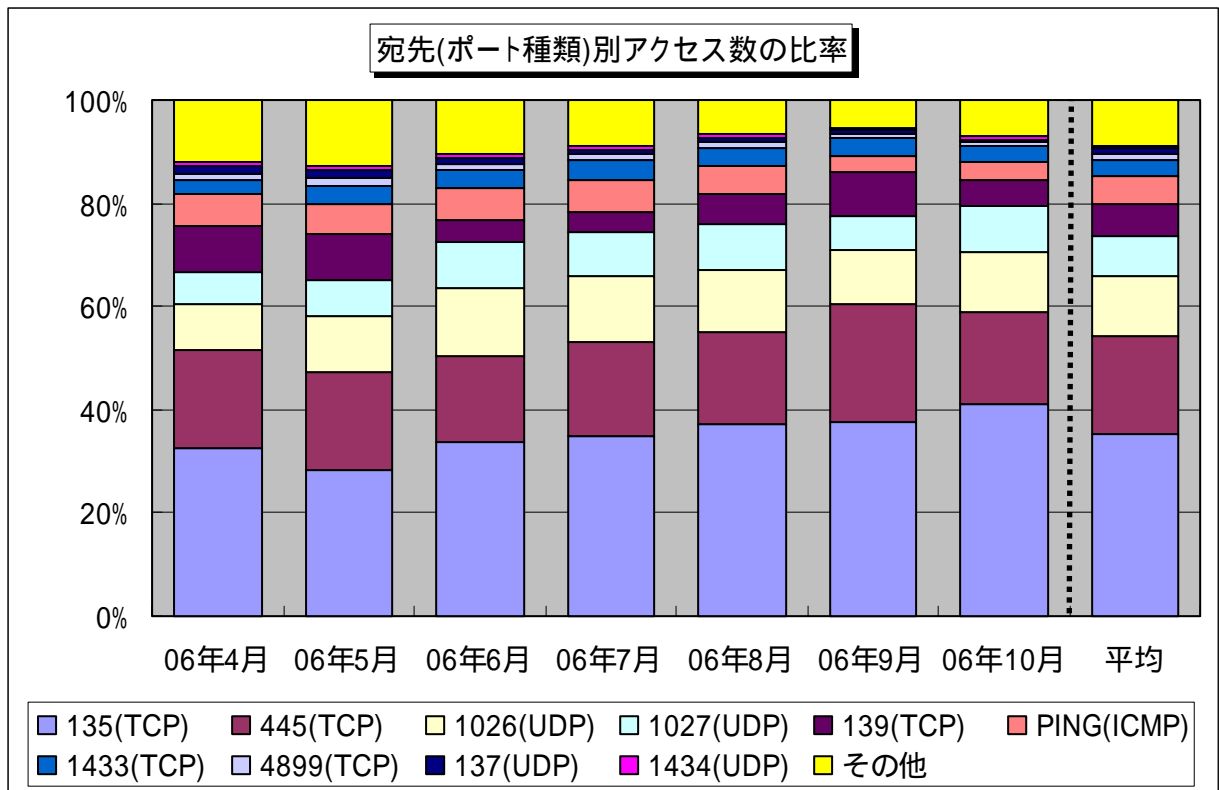


【図 2.4.4 2006年10月の発信元地域別発信元数の比率】

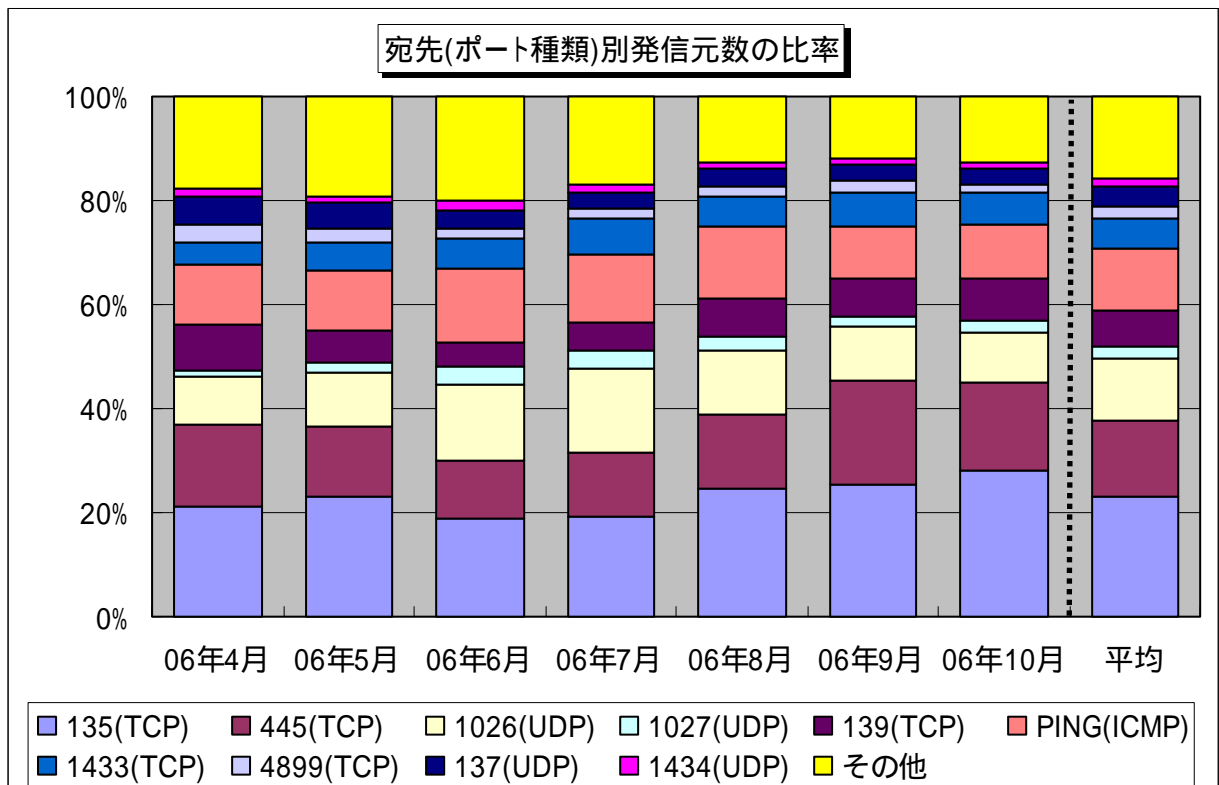
### 3. 統計情報

#### 3.1 2006年4月～2006年10月の宛先(ポート種類)別の比率

2006年4月～2006年10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10月の宛先(ポート種類)別アクセス数の比率】

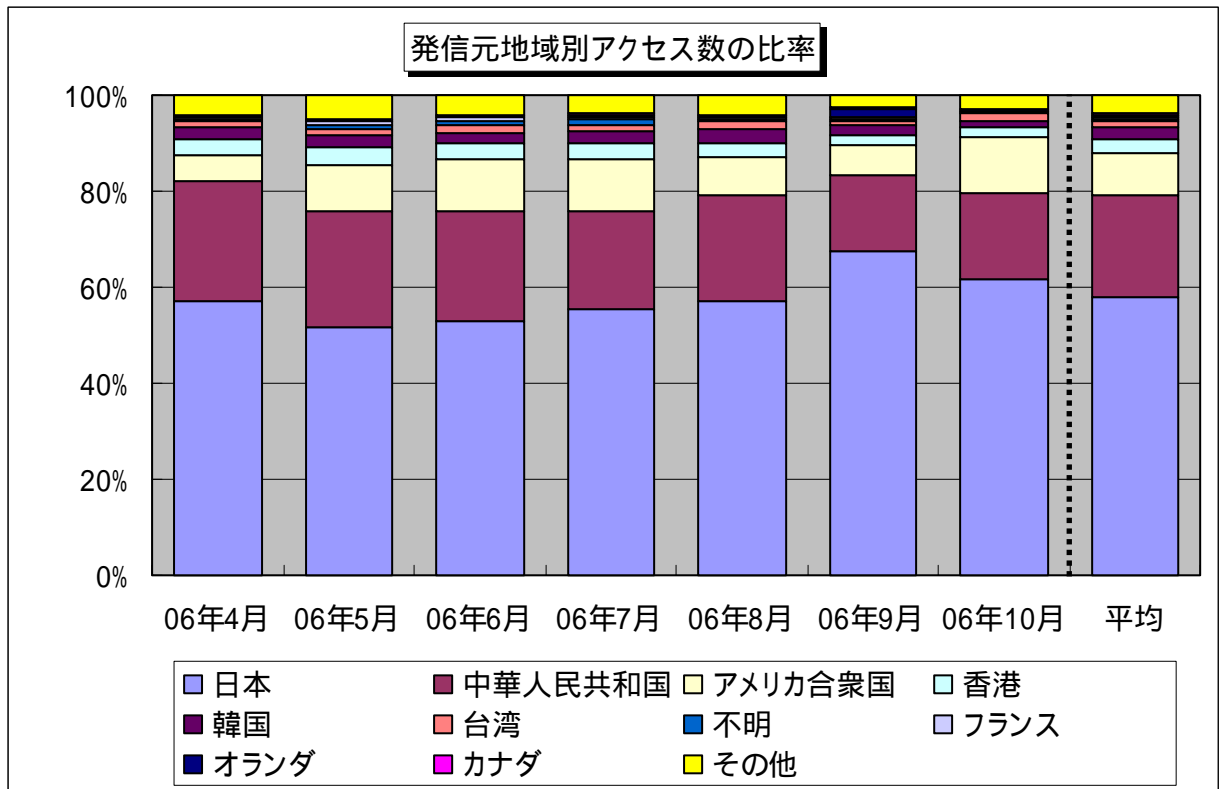


【図 3.1.2 2006年4月～2006年10月の宛先(ポート種類)別発信元数の比率】

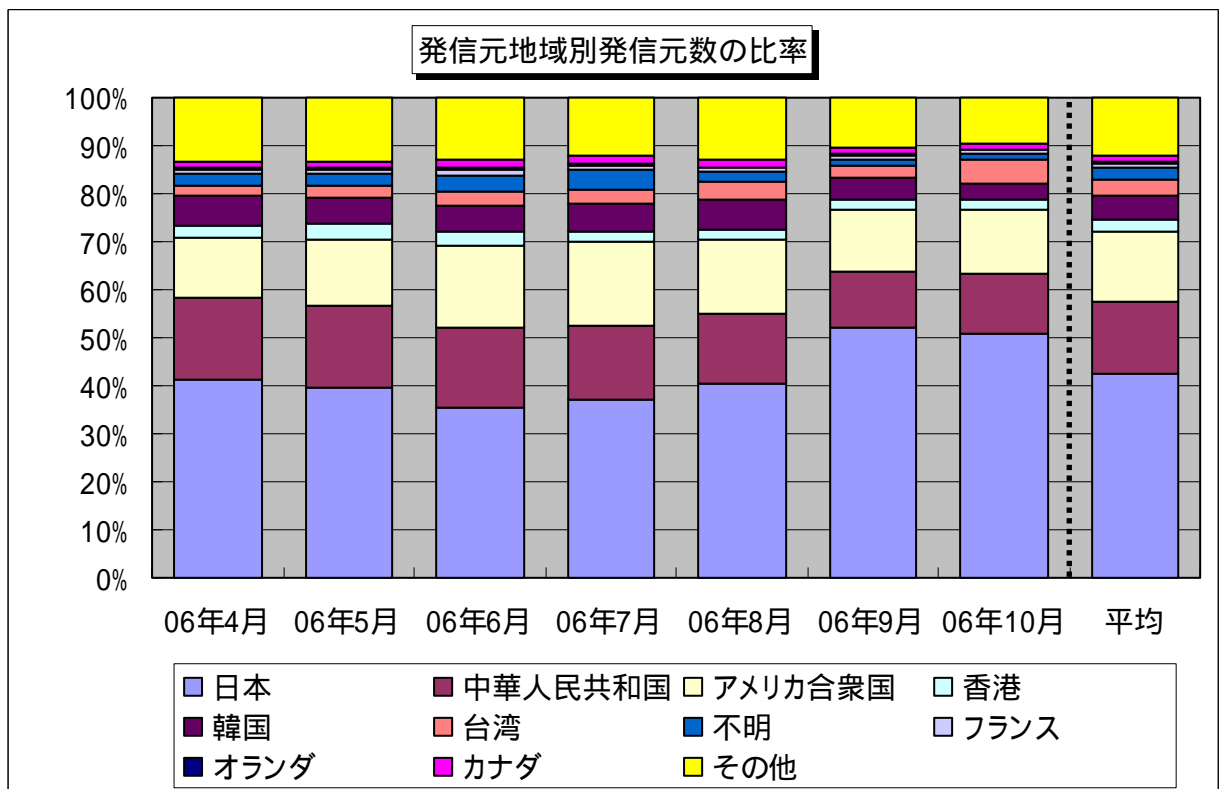


### 3.2 2006年4月～2006年10月の発信元地域別の比率

2006年4月～2006年10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10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10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
5900(TCP)	リモートアクセスツール RealVNC のぜい弱性を狙っていると思われるアクセスです

### 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