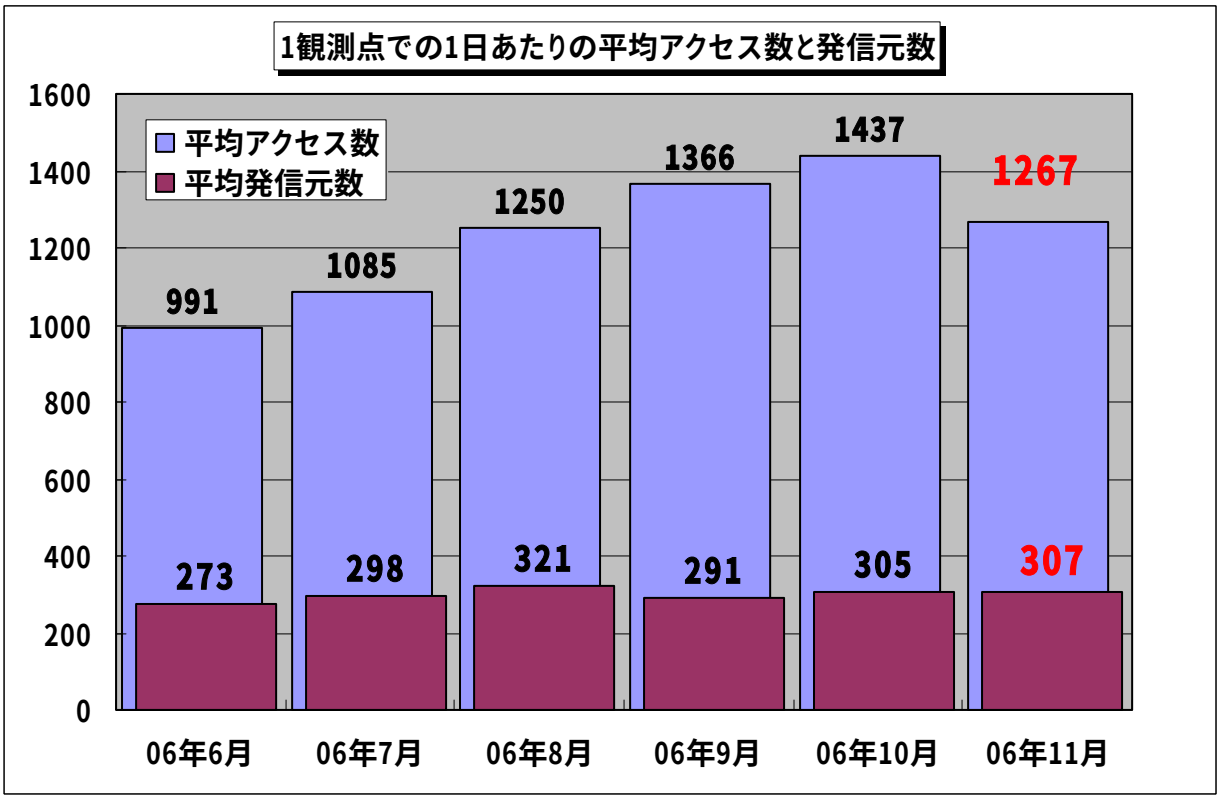
別紙 3

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、2006 年 11 月の期待しない（一方的な）アクセスの総数は、10 観測点で **380,054 件**ありました。1 観測点で 1 日あたり **307** の発信元から **1,267 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、307 人の見知らぬ人(発信元)から、発信元一人当たり 4 件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】

2006 年 6 月～2006 年 11 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 月以降増加傾向でしたが、11 月は 8 月と同レベルまで減少しました**。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。

2．11 月のアクセス状況

11 月のアクセス状況は、全体的には 10 月とほぼ同じ状況ですが、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は減少しました（図 2.1.1）。

2.1 2006 年 11 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で直接ファイル（データ）を交換することです。

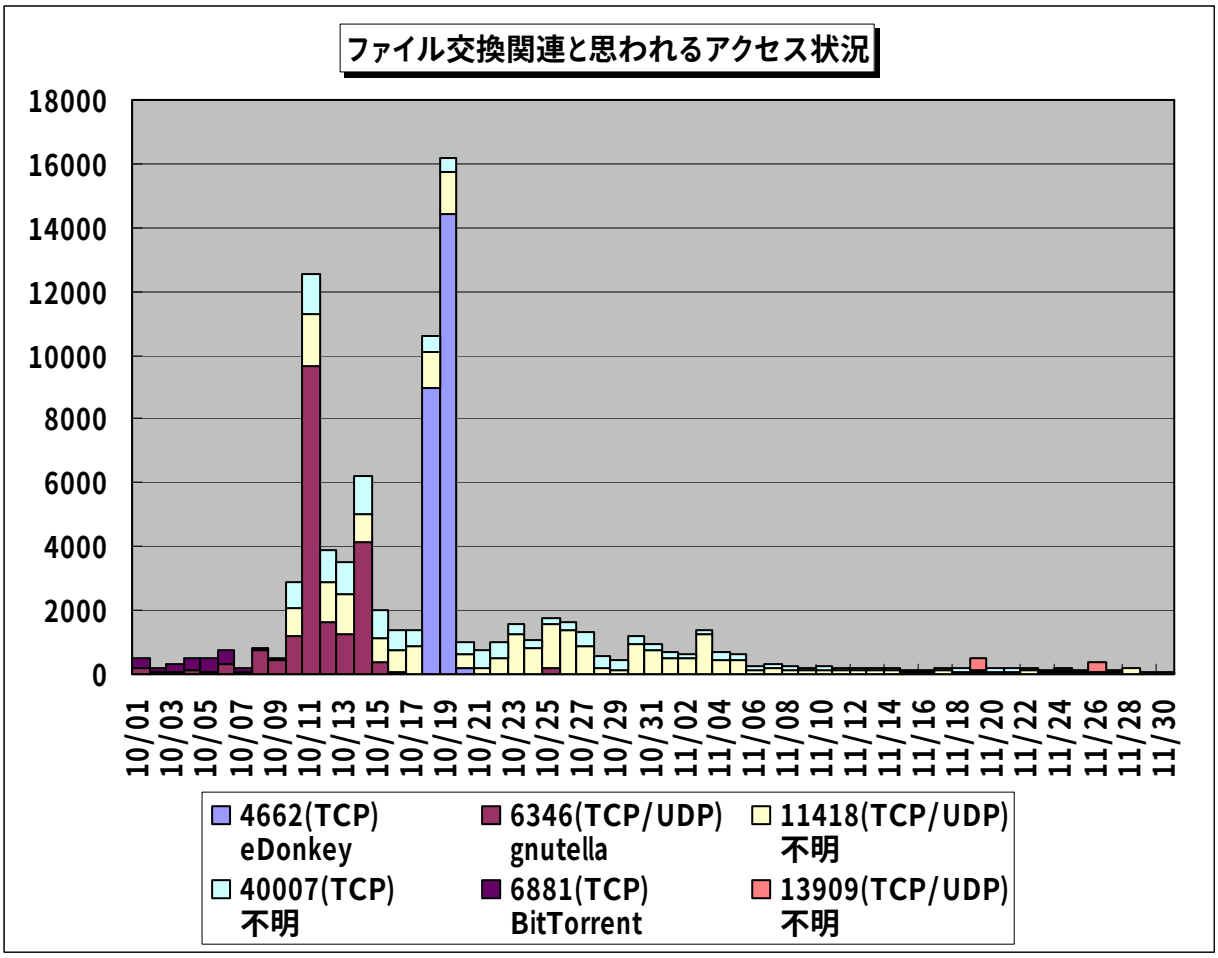
ファイル交換の方法にはいろいろありますが、ファイル交換を行うための情報を管理するサーバを中心としたファイル交換ネットワークを組む方式と、ファイル交換ソフトを介して数多くのコンピュータが直接ファイル交換ネットワークを組む方式がほとんどです。

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、同じファイル交換ソフト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。

図 2.1.1 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。

ただし、これらのアクセスについては、特定観測点における特異アクセスと言うことで、本資料の各種統計データからは除外しているので注意して下さい。



【図 2.1.1 2006 年 10 から 11 月のファイル交換関連と思われるアクセス数の遷移】

これらのアクセスを行っていると予測されるファイル交換ソフトと発信元については、以下の通りです。

- eDonkey と呼ばれるファイル交換ソフトのデフォルトポートである 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ですが、11 月には 1 件も観測されませんでした
- gnutella 系のファイル交換ソフトのデフォルトポートである 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でした
- ファイル交換ソフトの特定はできません(不明)が 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でした
- これもファイル交換ソフトの特定はできません(不明)が 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でした
- BitTorrent 系のファイル交換ソフトのデフォルトポートである 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
- これもファイル交換ソフトの特定はできません(不明)が 13909(TCP/UDP)ポートへのアクセスの発信元はオランダ方面がほとんどでしたが、このアクセスは 11 月から観測されました

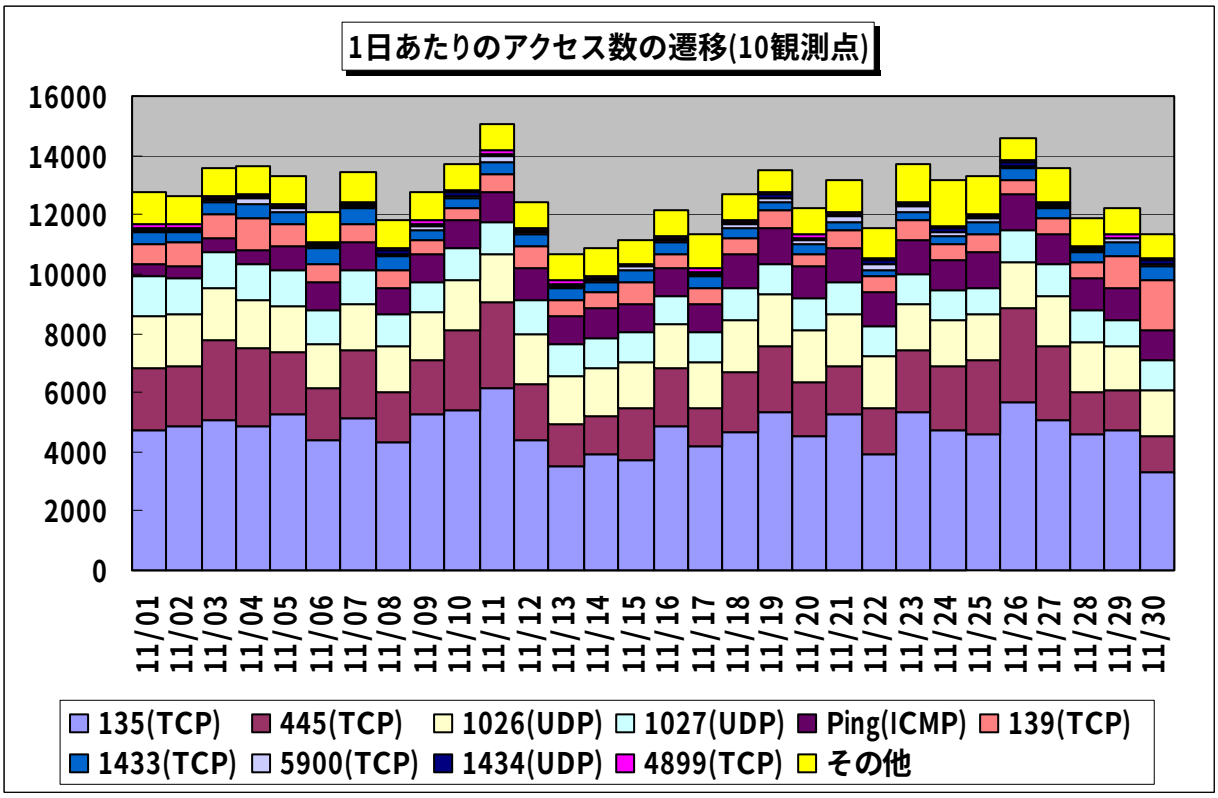
著作権のあるデータ（ファイル）を非合法にファイル交換する人たちがいるため、最近ではサーバを中心に持つタイプのファイル交換では、サーバが閉鎖に追い込まれたり、違法なファイル交換を行った人が逮捕されたりという事件も起こっています。

さらに、ファイル交換を介した情報漏えい事故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。最近では、航空自衛隊の内部情報がファイル交換ソフト Winny を介して漏洩した事故がテレビや新聞でも報道されていました。ファイル交換ソフトの利用者には、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ください。

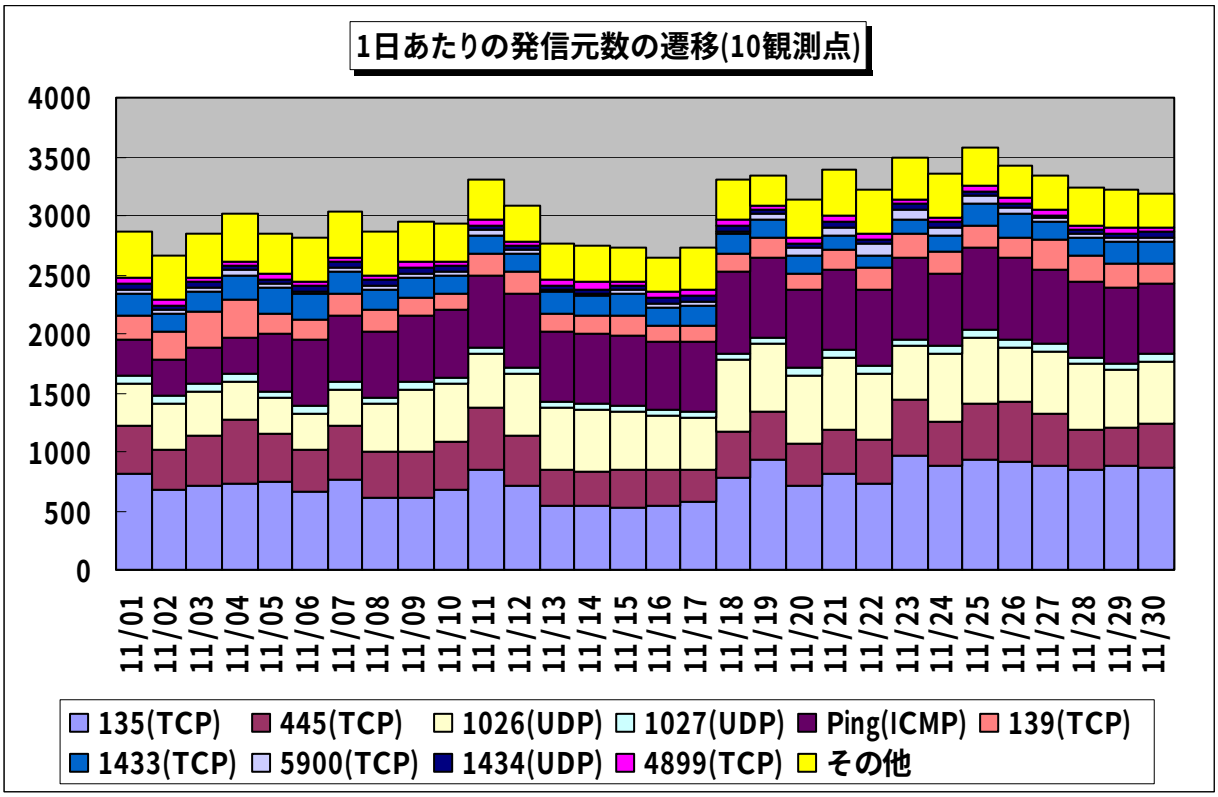
また、特定のＩＰアドレスに、前述のようなアクセスが集中すると、該当 IP アドレスを割り振られたコンピュータでは、あたかもＤｏＳ攻撃を受けているような状況となる場合もあります。このようなアクセスは、ほとんどがファイル交換を自動化して利用している場合に発生するものと考えられます。ファイル交換の利用者の方には、このような状況を理解いただき、ファイル交換の接続先の確認をあらかじめ行ってから、アクセスするように心掛けてください。

2.2 2006 年 11 月の一方的なアクセス状況

2006 年 11 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。



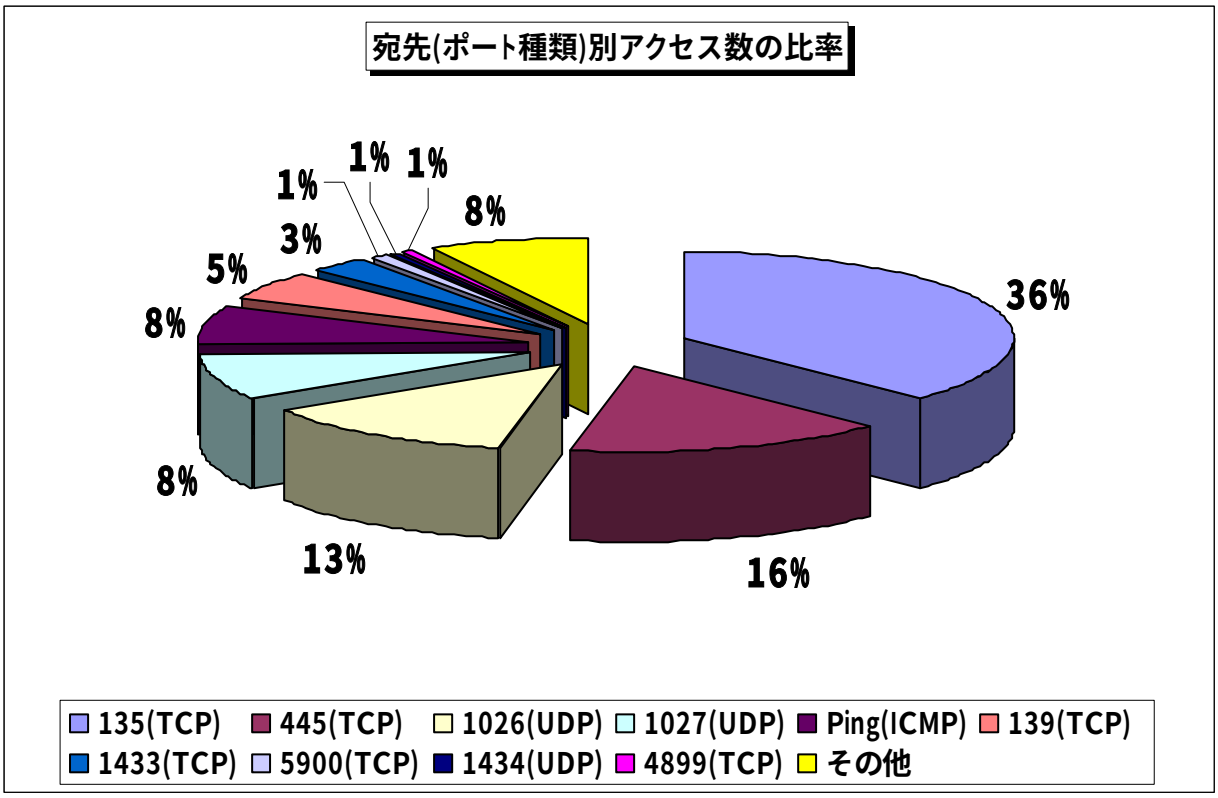
【図 2.2.1 2006 年 11 月の一方的なアクセス状況(アクセス数)】



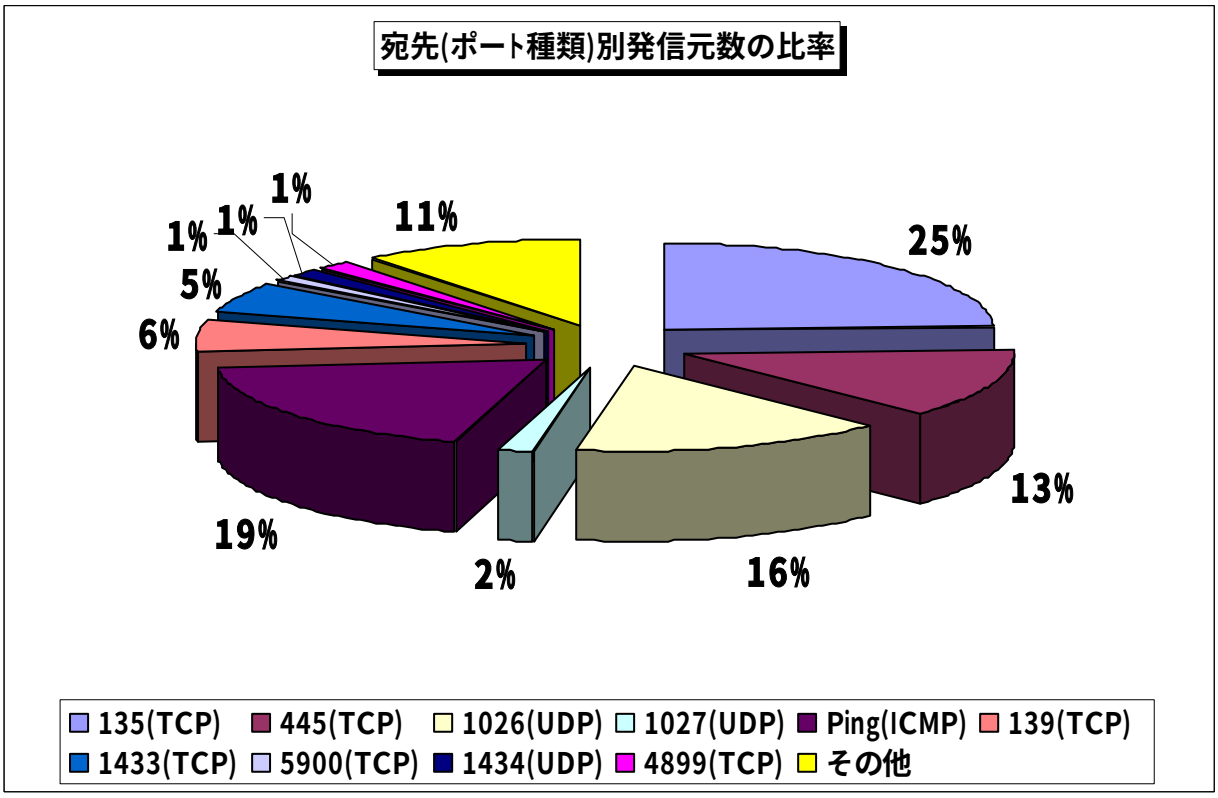
【図 2.2.2 2006 年 11 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 11 月の宛先(ポート種類)別の比率

2006 年 11 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。



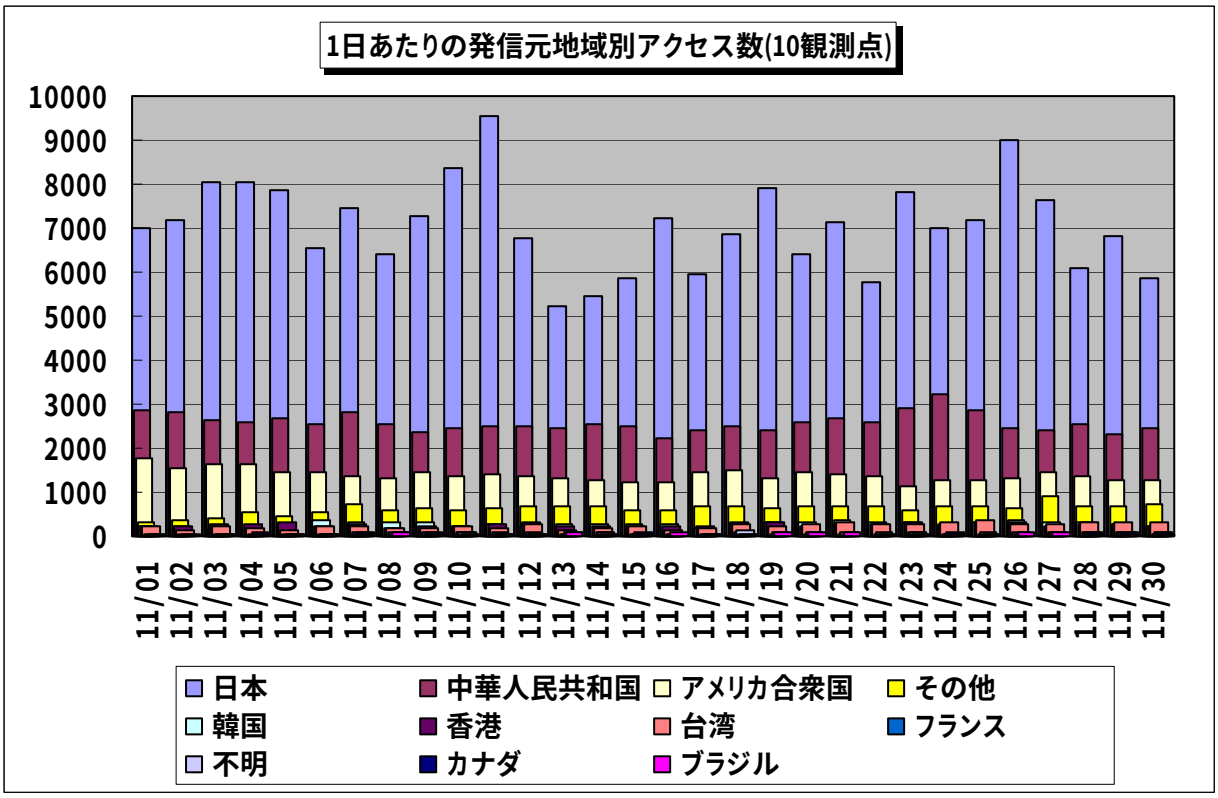
【図 2.3.1 2006 年 11 月の宛先(ポート種類)別アクセス数の比率】



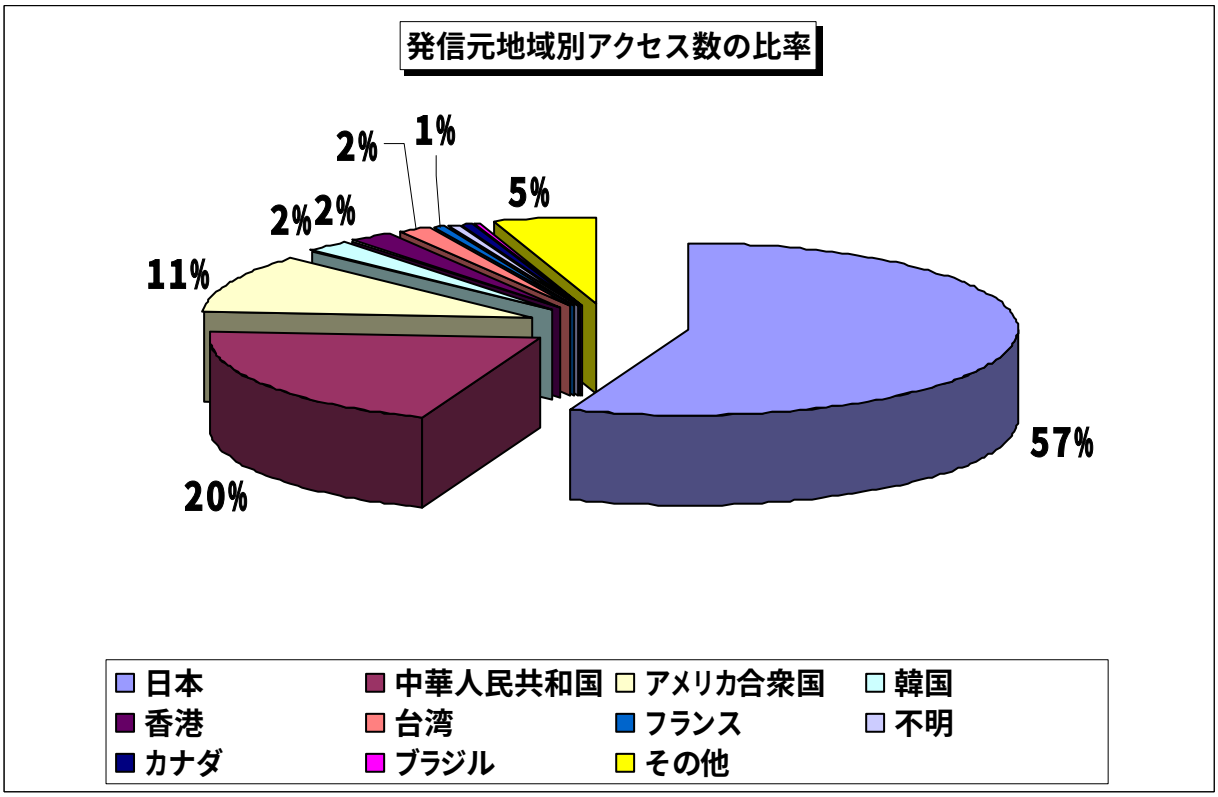
【図 2.3.2 2006 年 11 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 11 月の発信元地域別アクセス状況

2006 年 11 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。

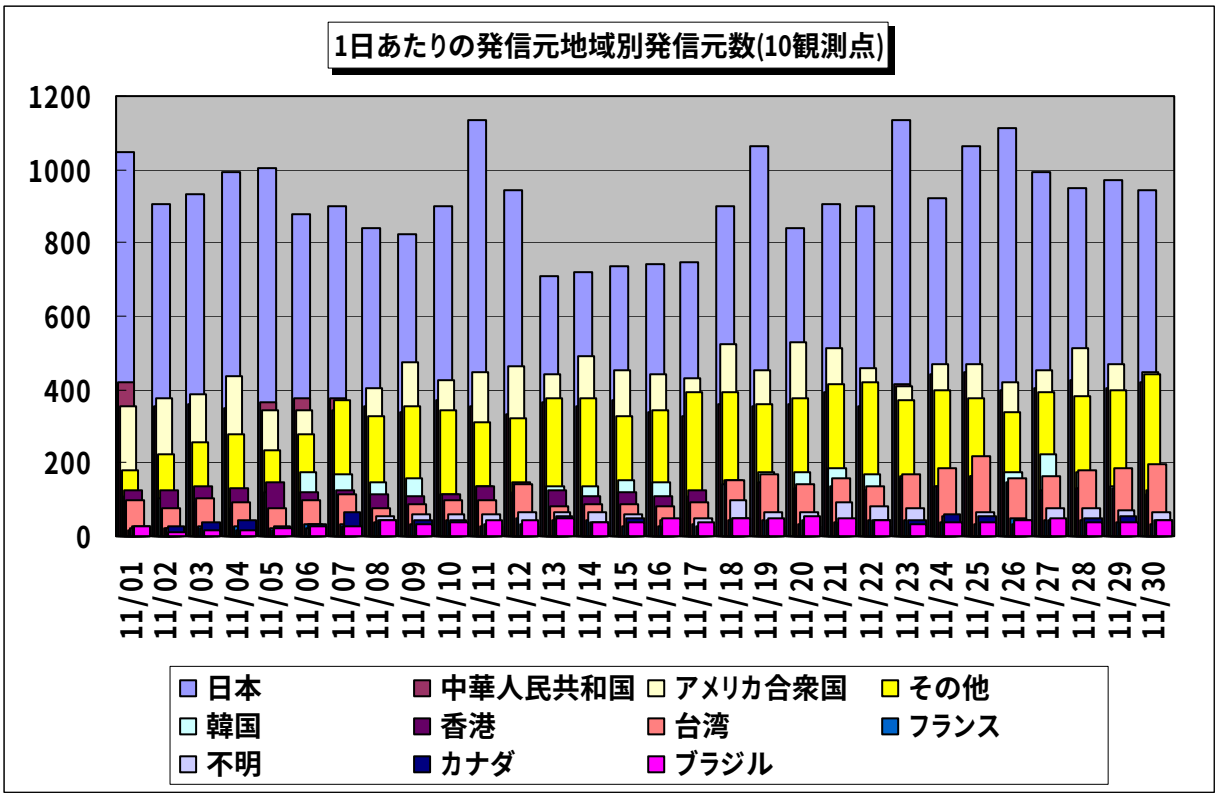


【図 2.4.1 2006 年 11 月の発信元地域別アクセス数の変化】

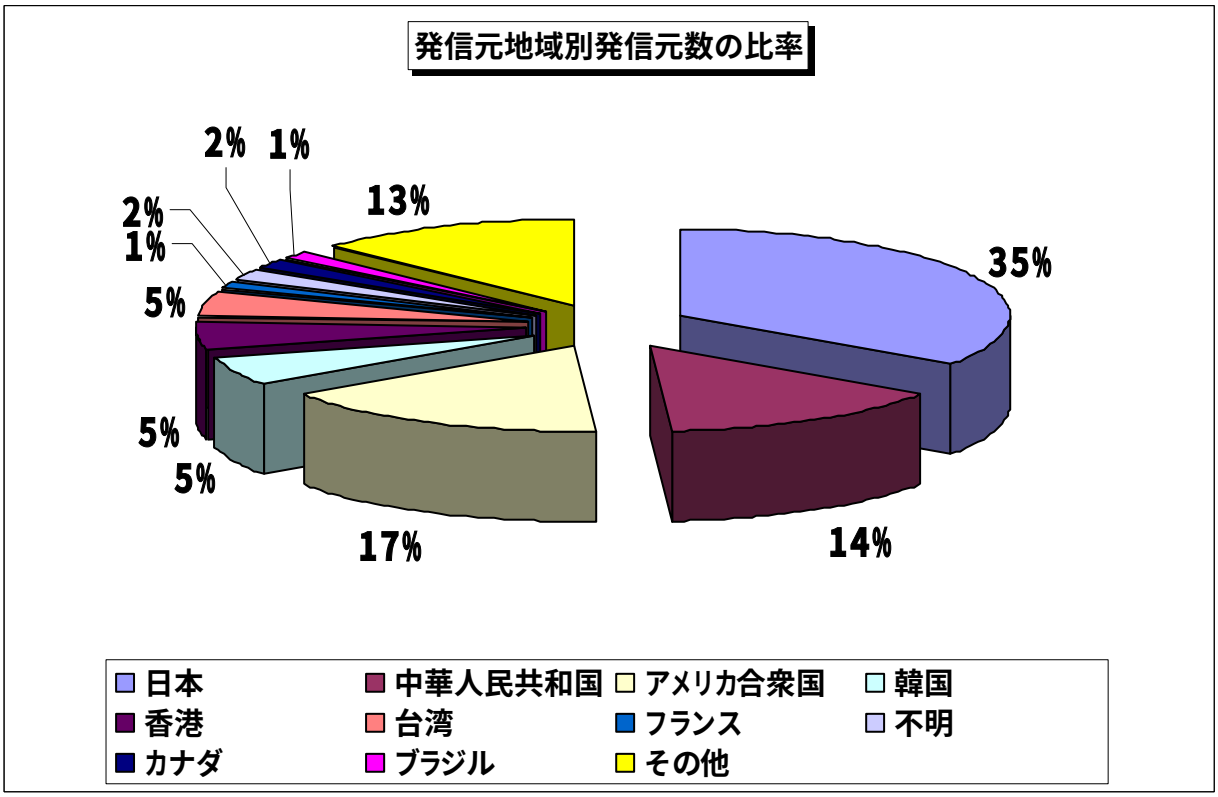


【図 2.4.2 2006 年 11 月の発信元地域別アクセス数の比率】

2006 年 11 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 11 月の発信元地域別発信元数の変化】

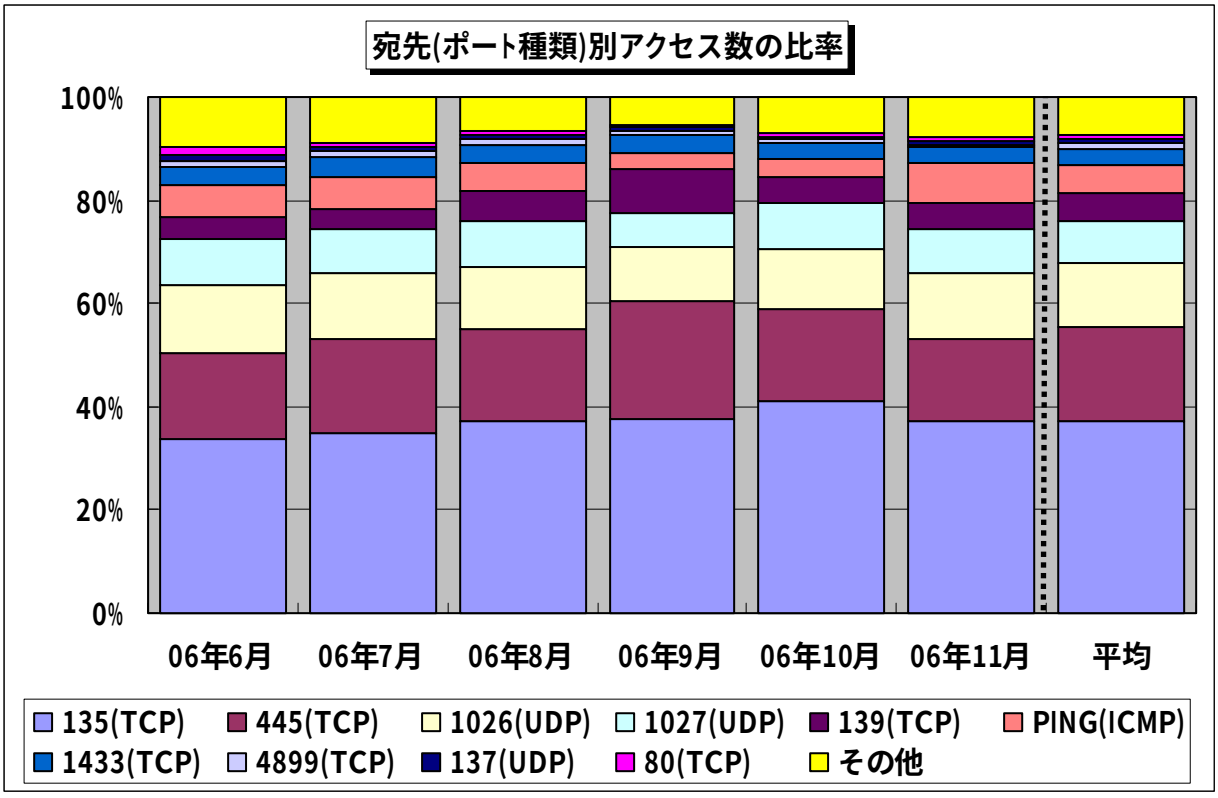


【図 2.4.4 2006 年 11 月の発信元地域別発信元数の比率】

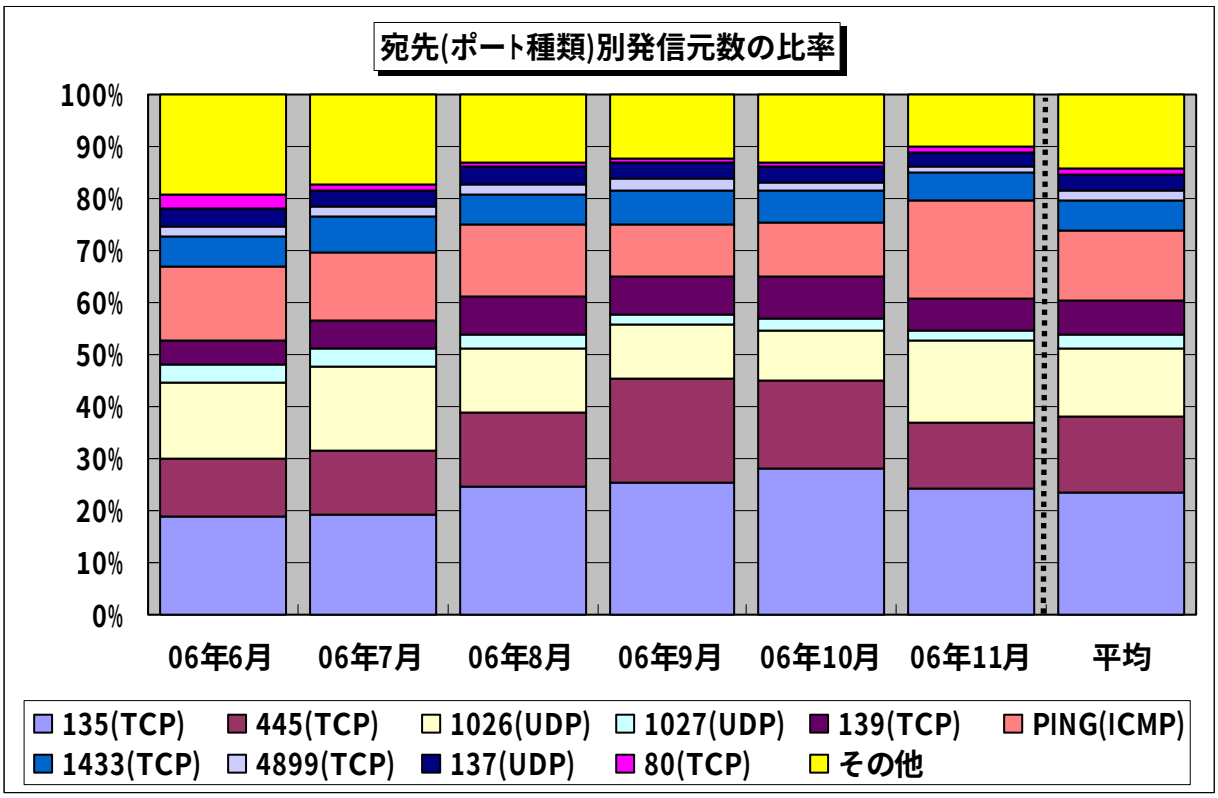
3．統計情報

3.1 2006 年 6 月～2006 年 11 月の宛先(ポート種類)別の比率

2006 年 6 月～2006 年 11 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。



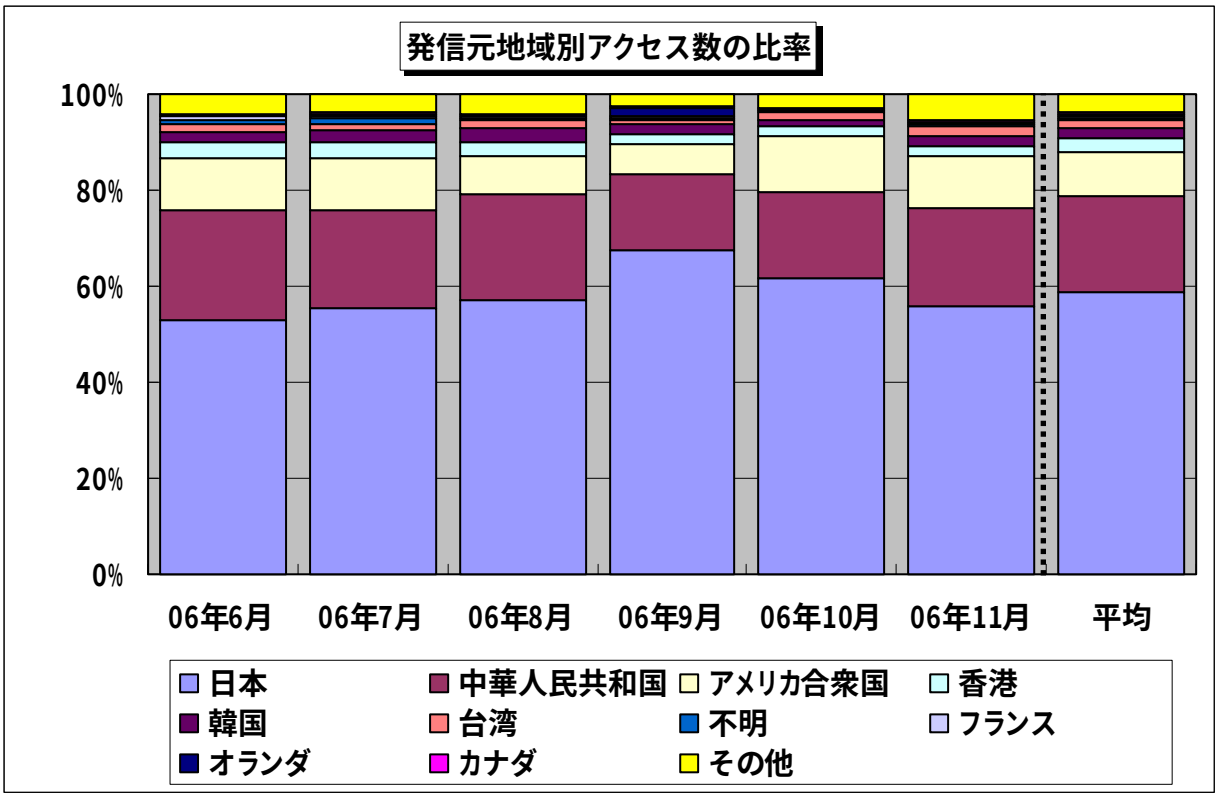
【図 3.1.1 2006 年 6 月～2006 年 11 月の宛先(ポート種類)別アクセス数の比率】



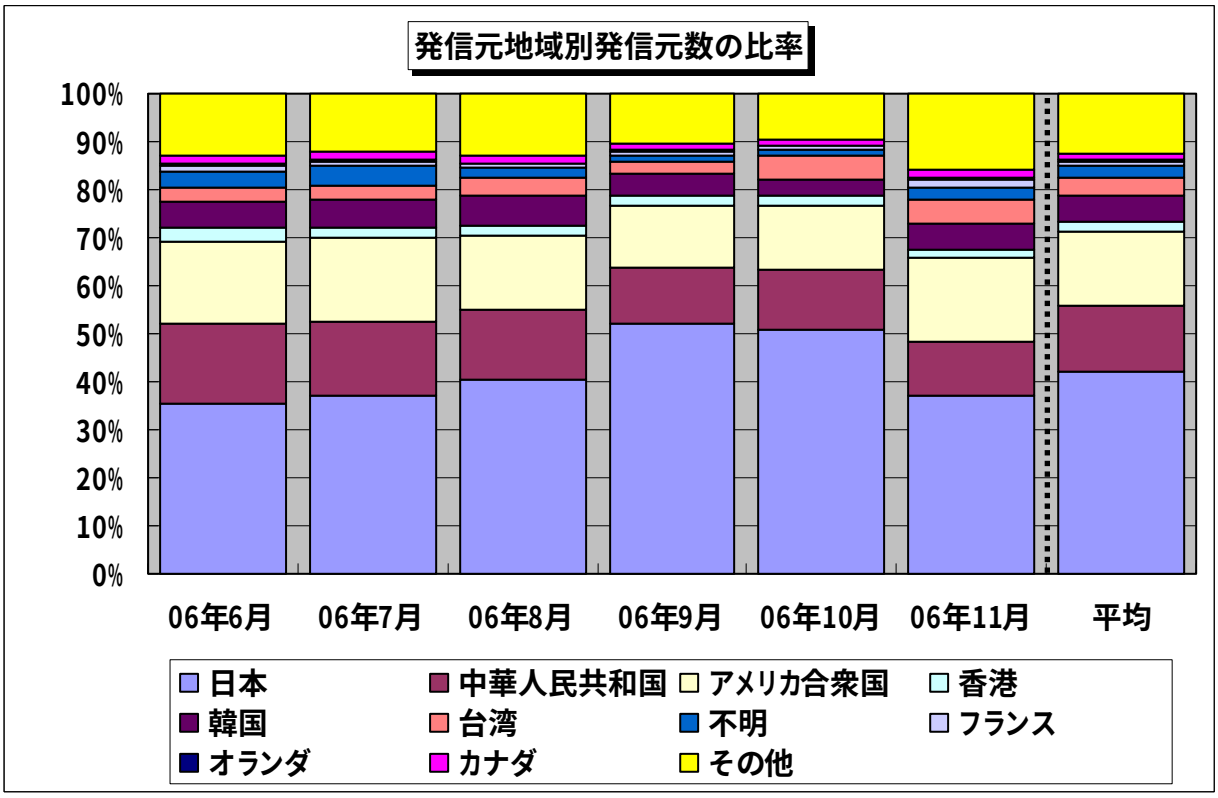
【図 3.1.2 2006 年 6 月～2006 年 11 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 6 月～2006 年 11 月の発信元地域別の比率

2006 年 6 月～2006 年 11 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 6 月～2006 年 11 月の発信元地域別アクセス数の比率】



【図 3.2.2 2006 年 6 月～2006 年 11 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 11 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
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
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
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
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
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)
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)

■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