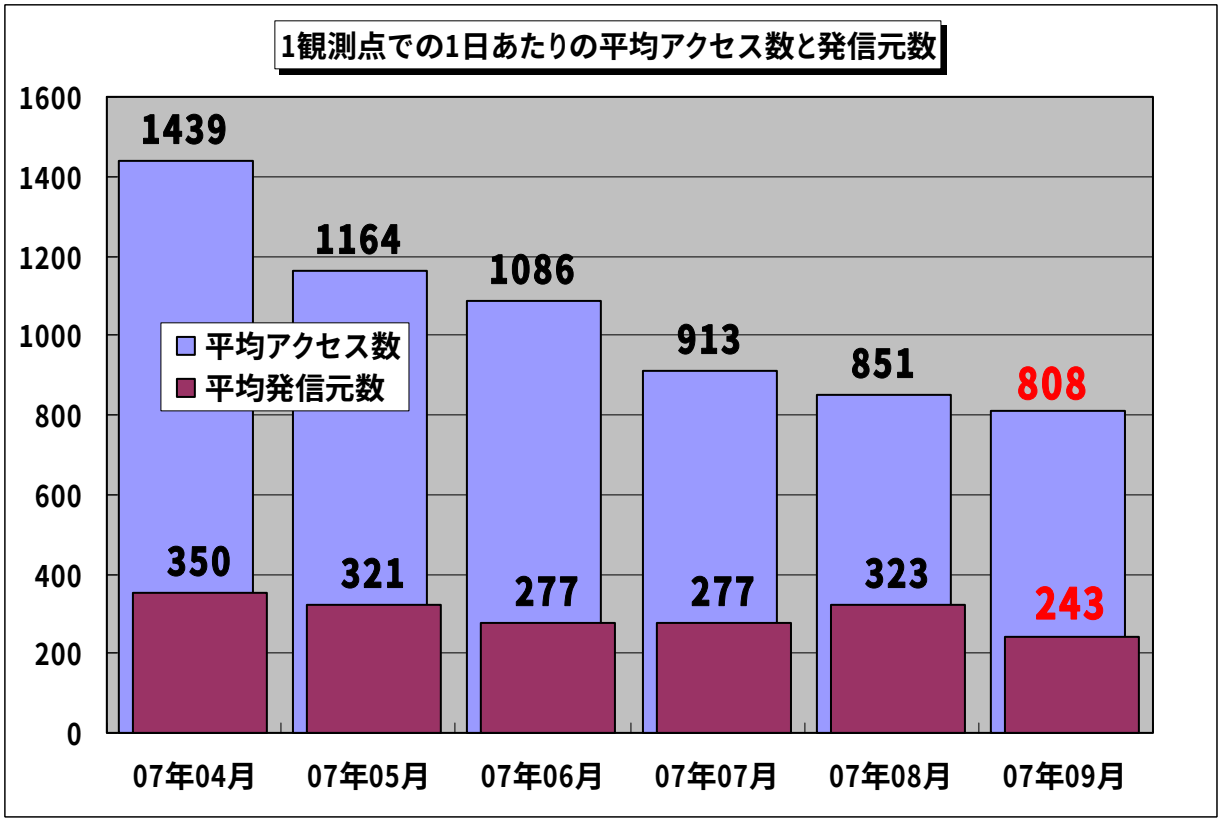
別紙 3

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、2007 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 **242,378 件**ありました。1 観測点で 1 日あたり **243** の発信元から **808 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、243 人の見知らぬ人(発信元)から、発信元一人当たり約 3 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　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】

2007 年 4 月～2007 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 1.1 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、3 ヶ月連続で 1000 を切り、緩やかな減少傾向にあります。

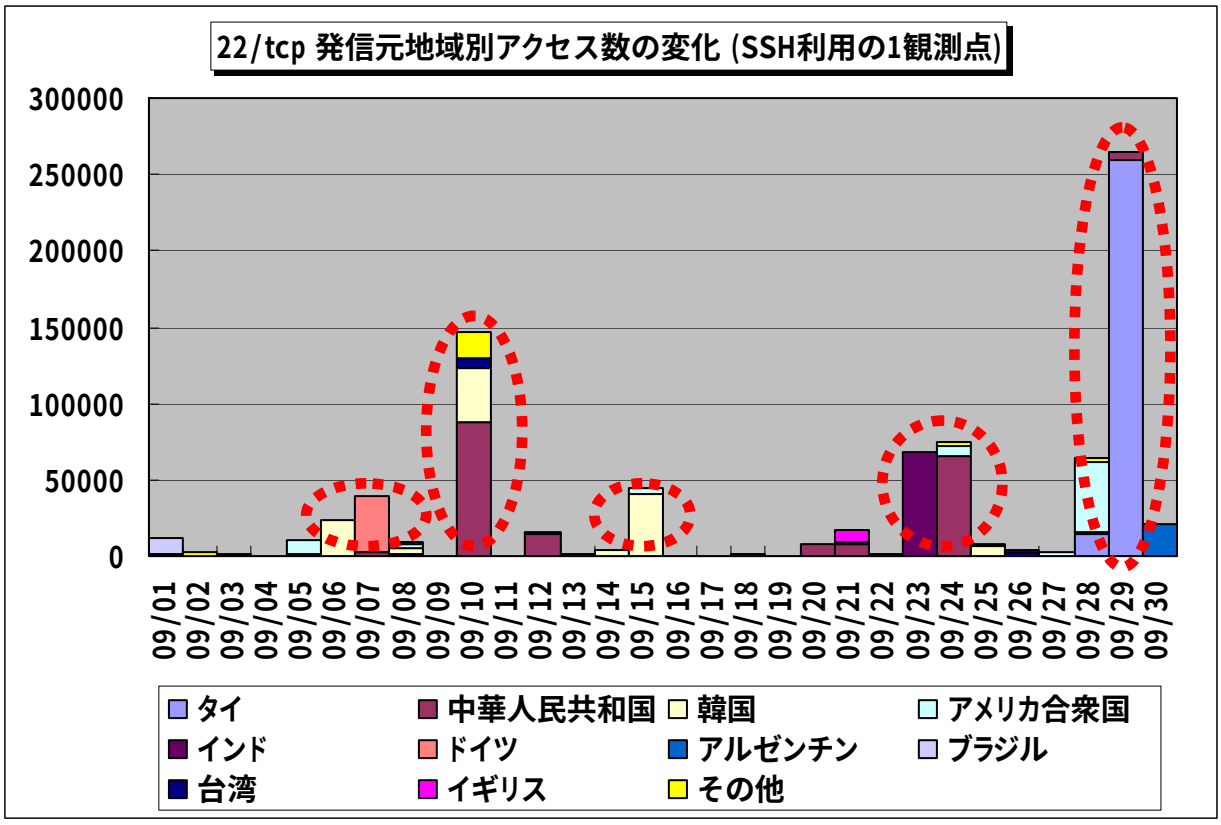
2．9 月のアクセス状況

2007 年 9 月のアクセス状況は、7 月、8 月と同じ様な感じで減少傾向にありますが、2007 年 1 月～9 月と、ほとんど変わらない状況です。そうした中において、リモートでアクセスするコンピュータを狙ったアクセスが多く見受けられました。

2.1. SSH を利用しているサーバを狙ったアクセス

SSH（Secure Shell：遠隔地にあるコンピュータに、リモートでアクセスする為に、通信路を暗号化することで安全性を高めたコマンド実行ツール）を利用しているコンピュータへのアクセスは、安易なパスワードで設定されているコンピュータを狙ったアクセスと思われます。

図 2.1.1 は、TALOT2 のメンテナンス用に SSH を利用している観測点の、22/tcp ポートへのアクセス数を示したものです。



【図 2.1.1　2007 年 9 月の 22/tcp ポートへの発信元地域別アクセス数の変化（SSH 利用の 1 観測点）】

この様に、1 日に数万～数十万回のアクセス※1 がくる場合があります。こうしたアクセスに応答するコンピュータに対しては、パスワードを破るための攻撃（ブルートフォース攻撃※2）を行なってきます。

※ 1　これらのアクセスは、特定観測点に対するものなので、統計情報にそぐわないため除外してあります。この他に、P2P ファイル交換ソフトが使用するアクセスも同様です。
全体的なアクセス数は減少していますが、この様な特定観測点のアクセスを含めて見てみると、決して期待しないアクセスが減少している訳ではありません。

※ 2　ブルートフォース攻撃とは、総当り攻撃とも呼ばれ、パスワードを破るためにありとあらゆる解読方法を使用して攻撃する手法です。

IPA に届けられた不正アクセスの情報では、ID やパスワードの不備が原因であった事例が年々増加しています。
システム管理者は、利用するアプリケーションの ID やパスワードの再確認や、接続認証の強化を実施して下さい。また、サーバに脆弱性がないかの確認も行って下さい。

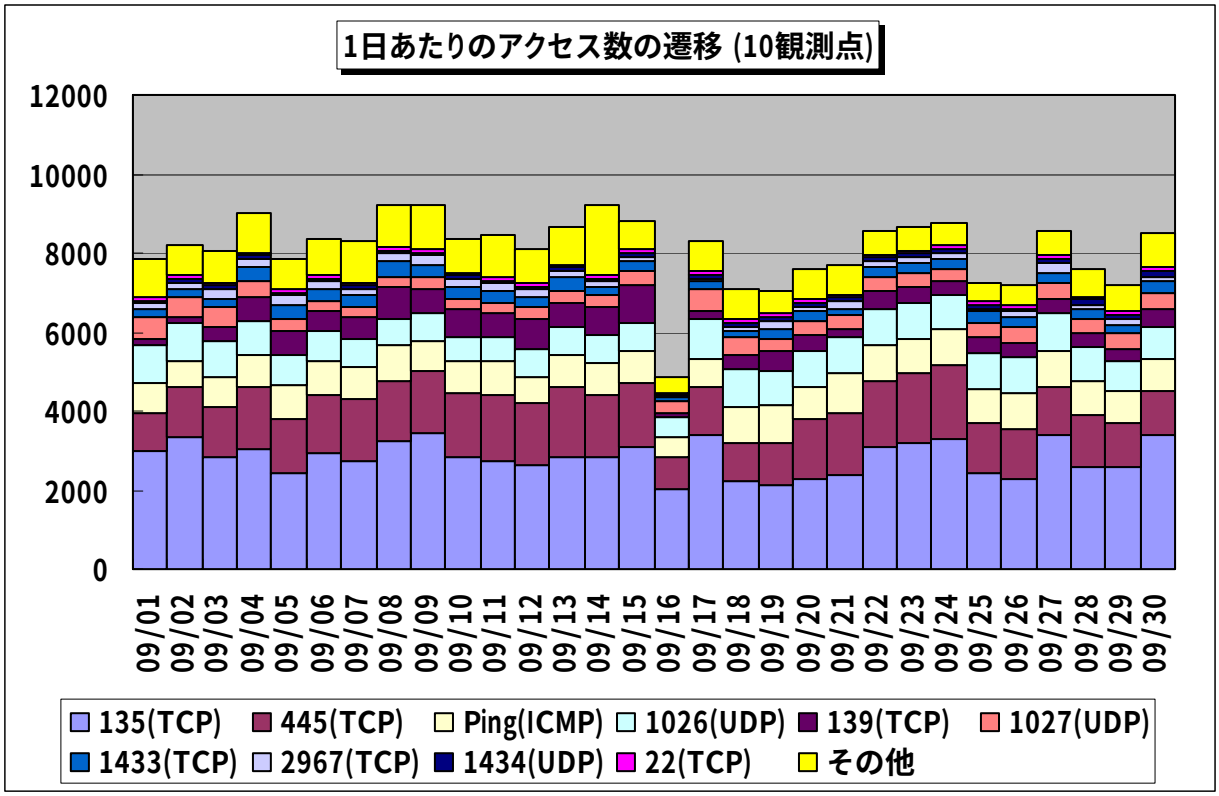
(参考情報)

■ IPA - セキュアな Web サーバの構築と運用 ～ ユーザ認証
http://www.ipa.go.jp/security/awareness/administrator/secure-web/chap6/6_userauth-1.html

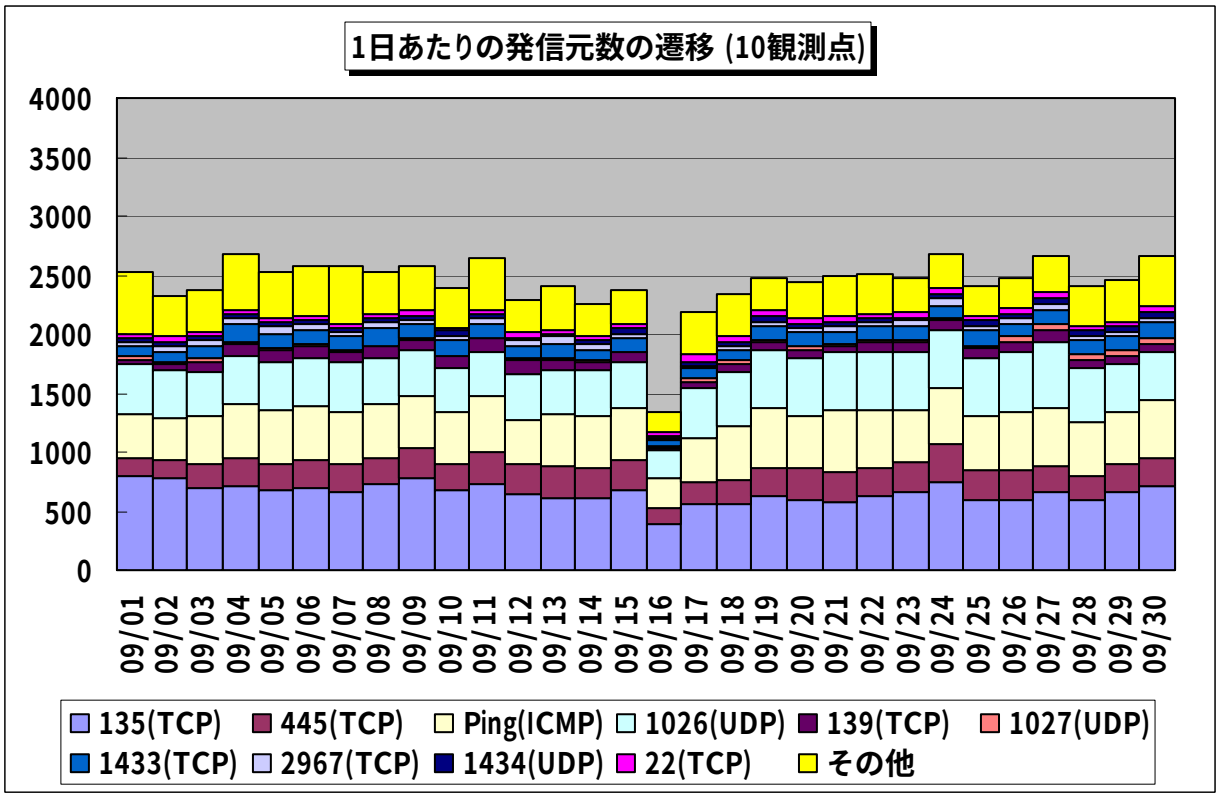
■ IPA - 情報セキュリティ白書 2007 年版
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

2.2 2007 年 9 月の一方的なアクセス状況

2007 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。



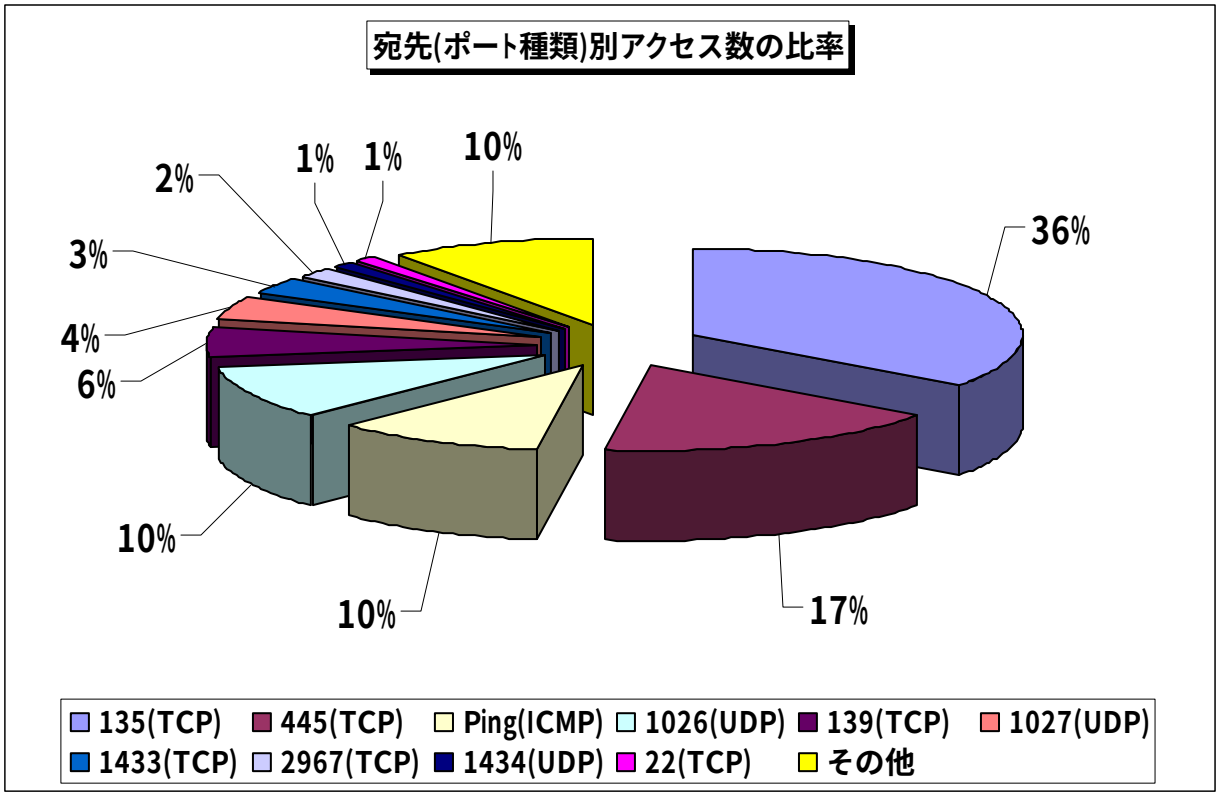
【図 2.2.1 2007 年 9 月の一方的なアクセス状況(アクセス数)】



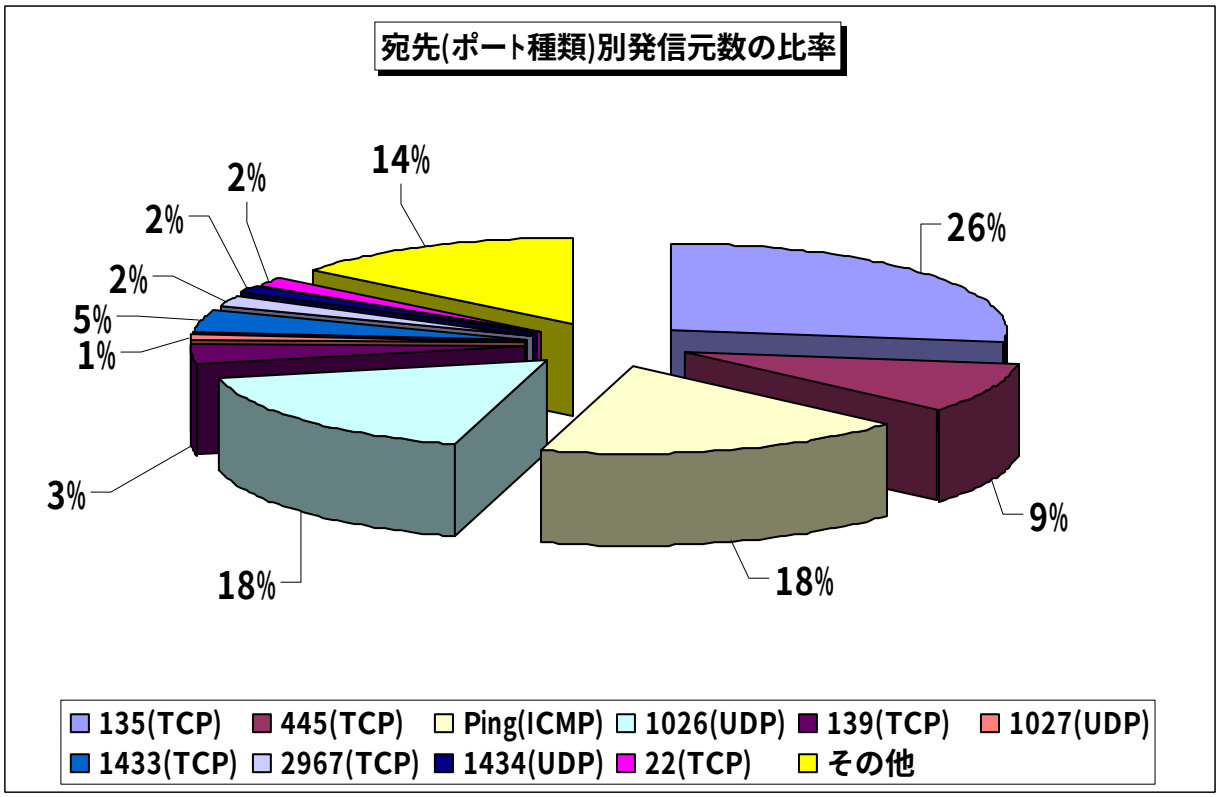
【図 2.2.2 2007 年 9 月の一方的なアクセス状況(発信元数)】

2.3 2007 年 9 月の宛先(ポート種類)別の比率

2007 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。



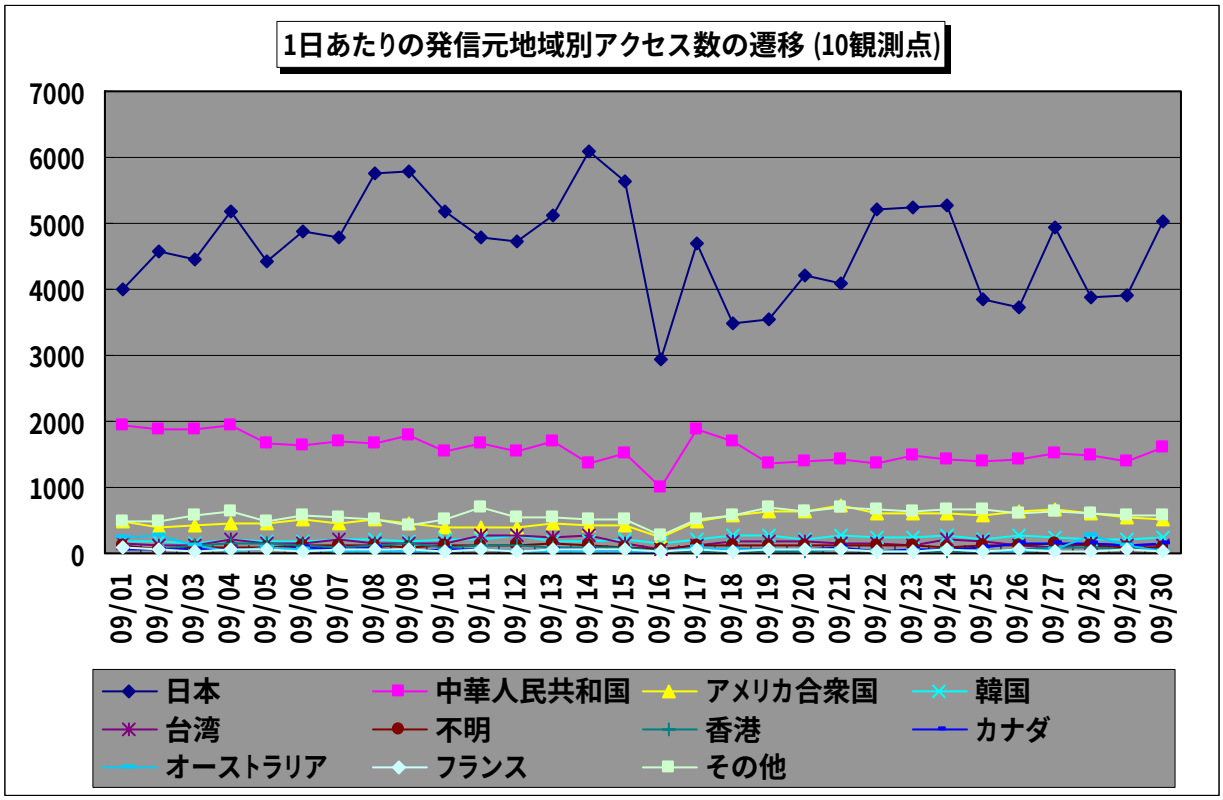
【図 2.3.1 2007 年 9 月の宛先(ポート種類)別アクセス数の比率】



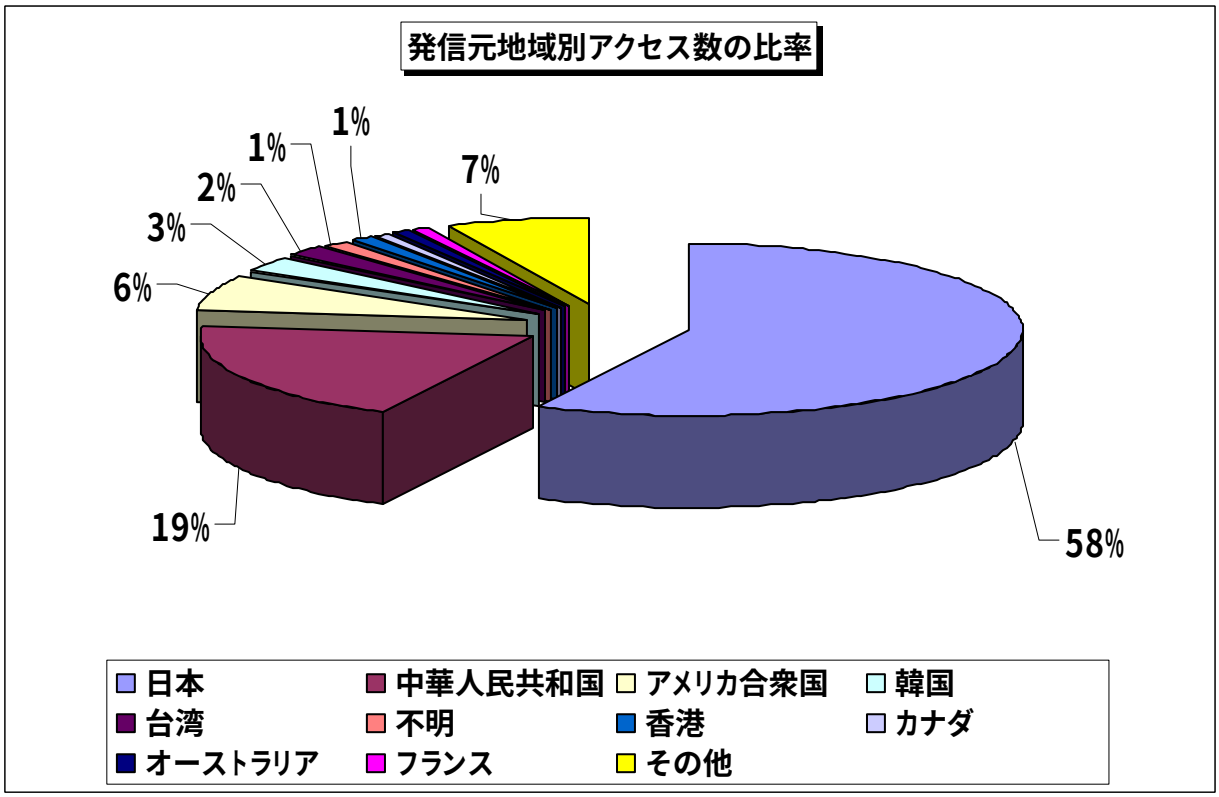
【図 2.3.2 2007 年 9 月の宛先(ポート種類)別発信元数の比率】

2.4 2007 年 9 月の発信元地域別アクセス状況

2007 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。

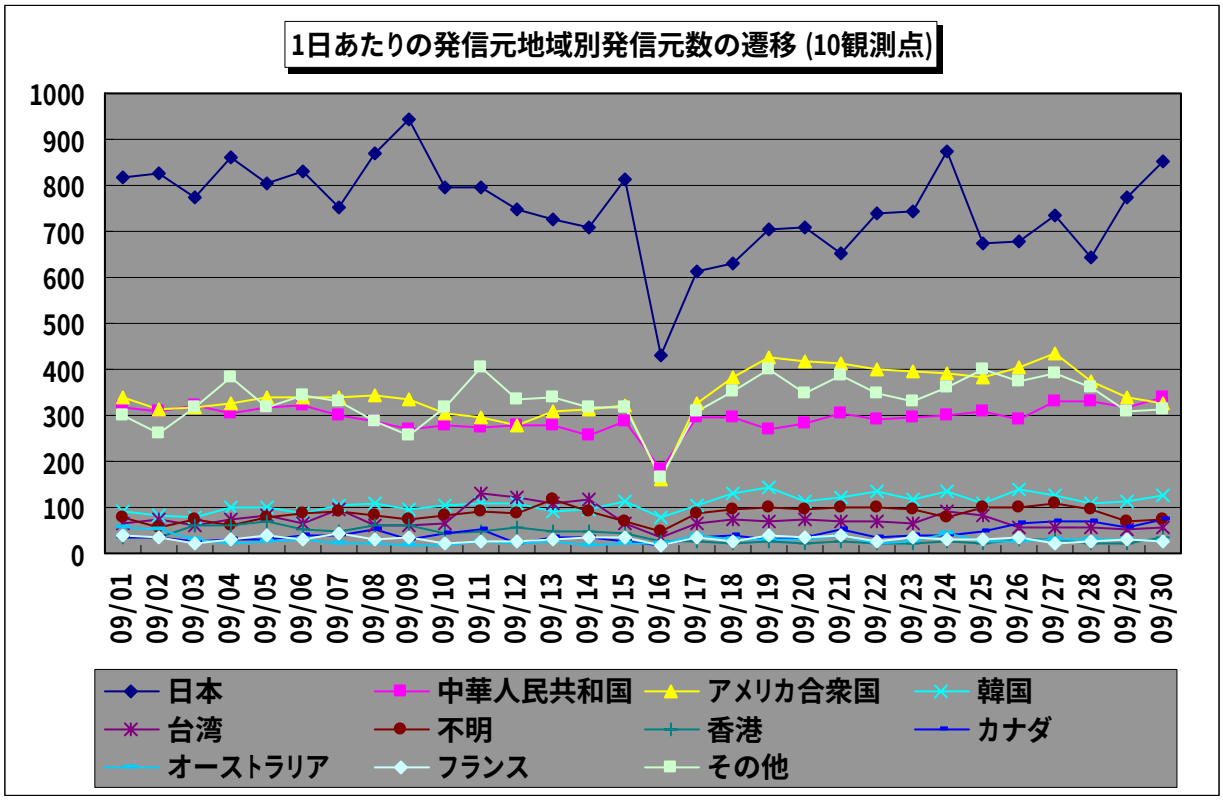


【図 2.4.1 2007 年 9 月の発信元地域別アクセス数の変化】

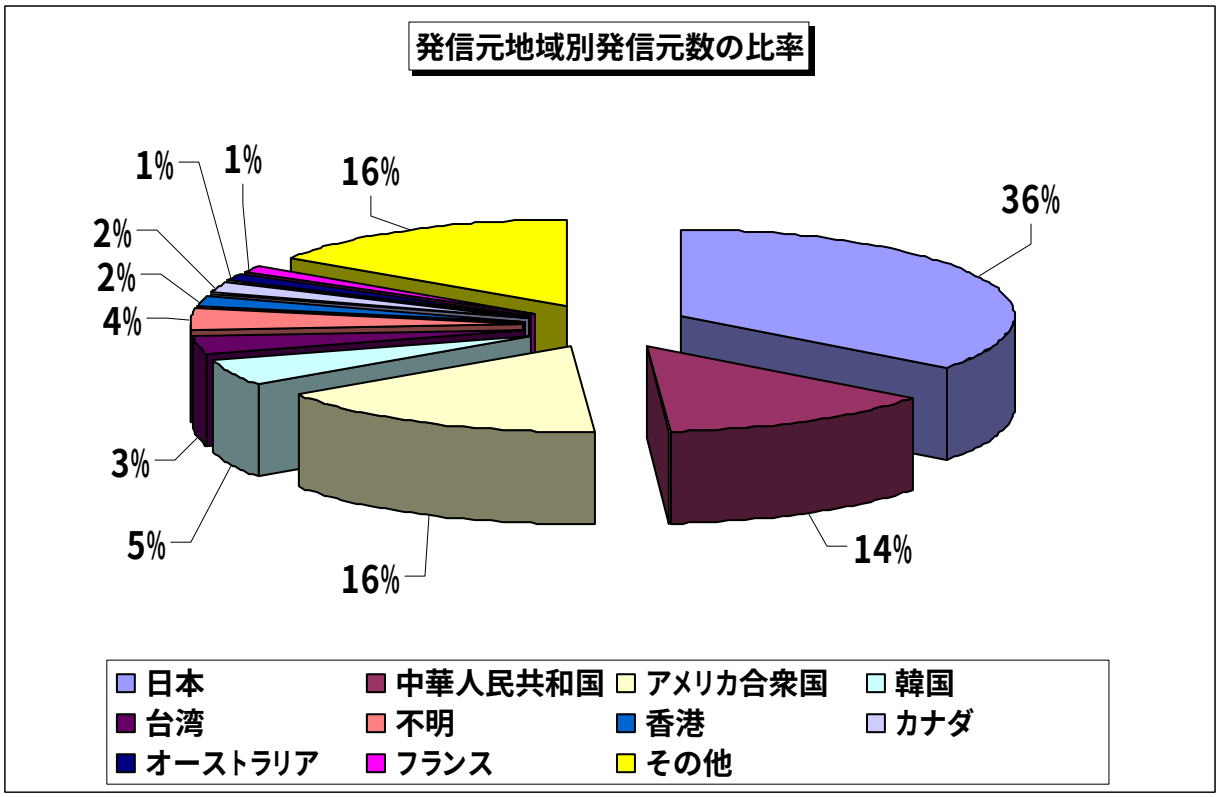


【図 2.4.2 2007 年 9 月の発信元地域別アクセス数の比率】

2007 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 2.4.4 に示します。



【図 2.4.3 2007 年 9 月の発信元地域別発信元数の変化】

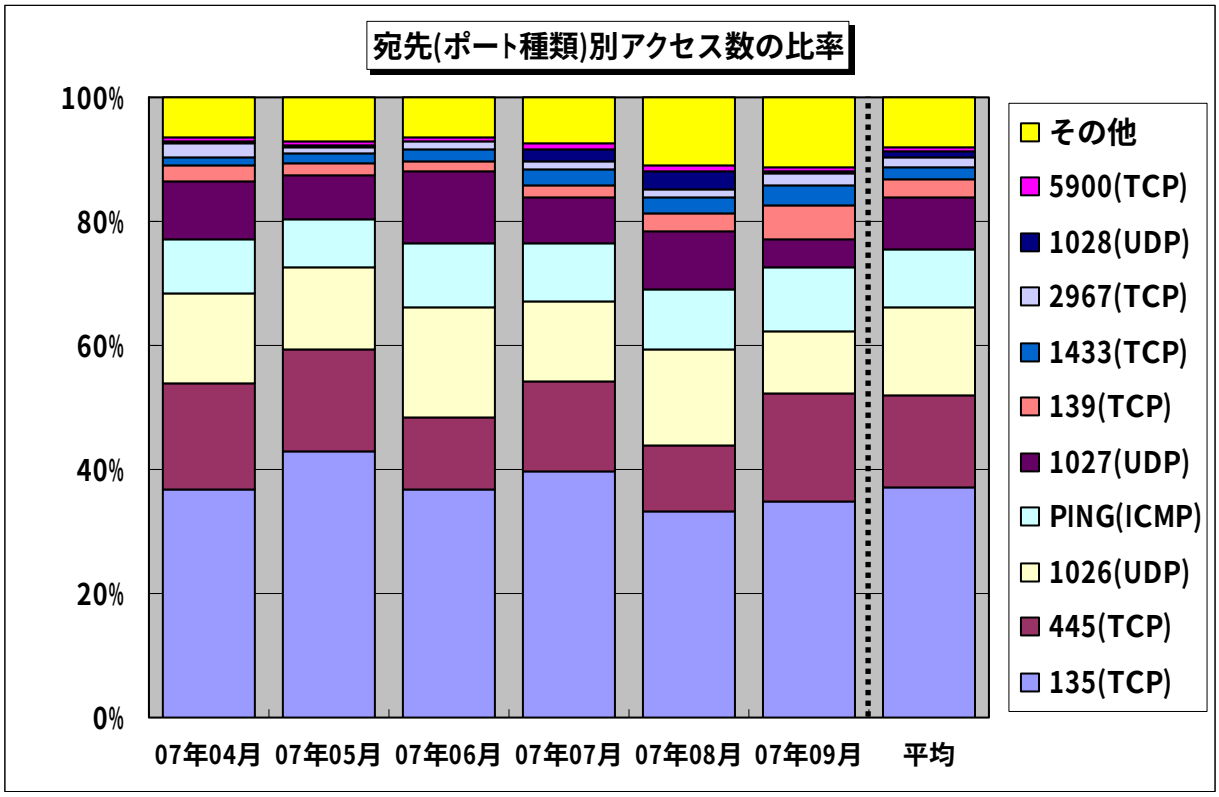


【図 2.4.4 2007 年 9 月の発信元地域別発信元数の比率】

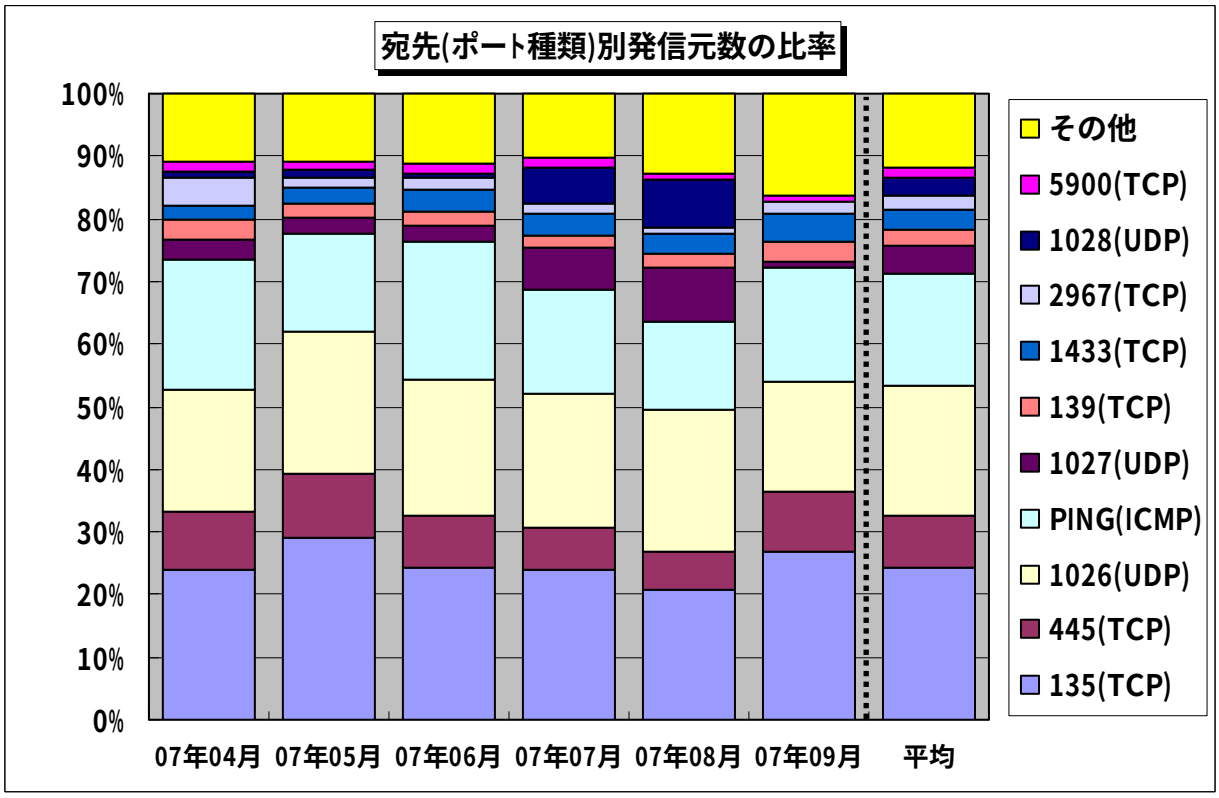
3．統計情報

3.1 2007 年 4 月～2007 年 9 月の宛先(ポート種類)別の比率

2007 年 4 月～2007 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。



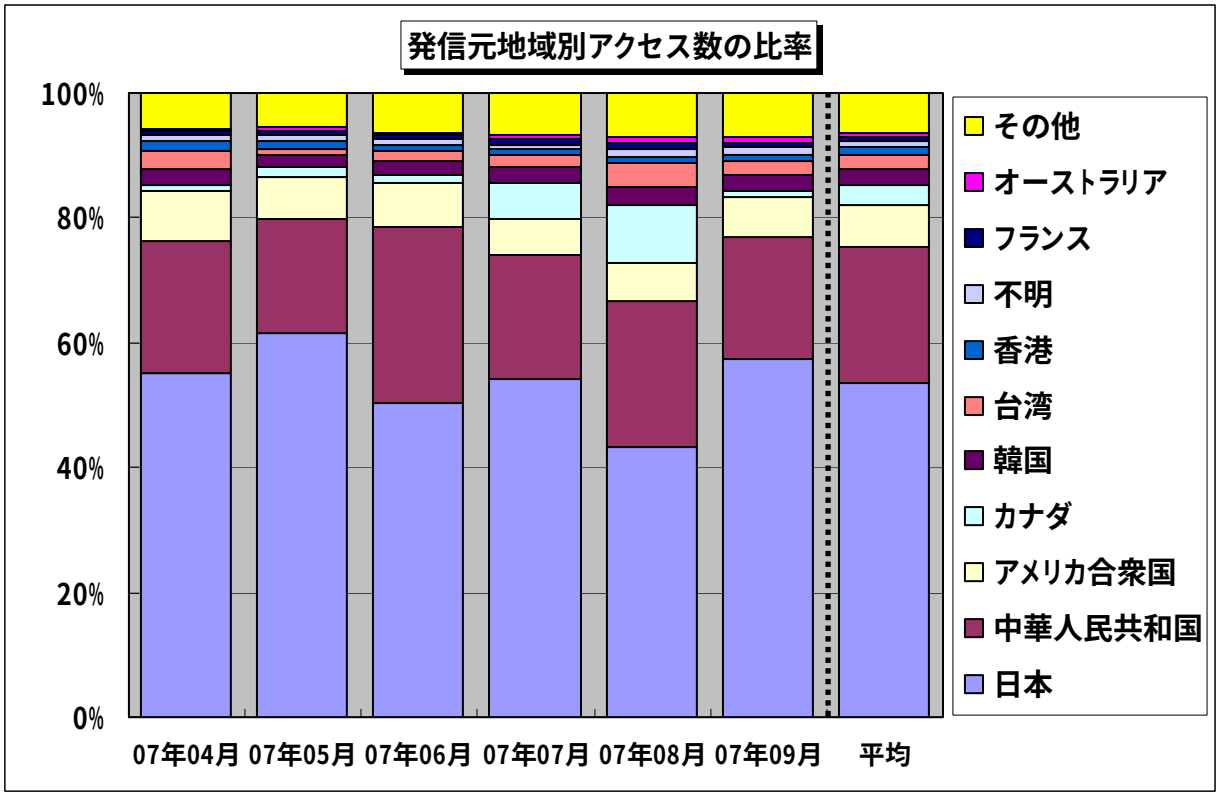
【図 3.1.1 2007 年 4 月～2007 年 9 月の宛先(ポート種類)別アクセス数の比率】



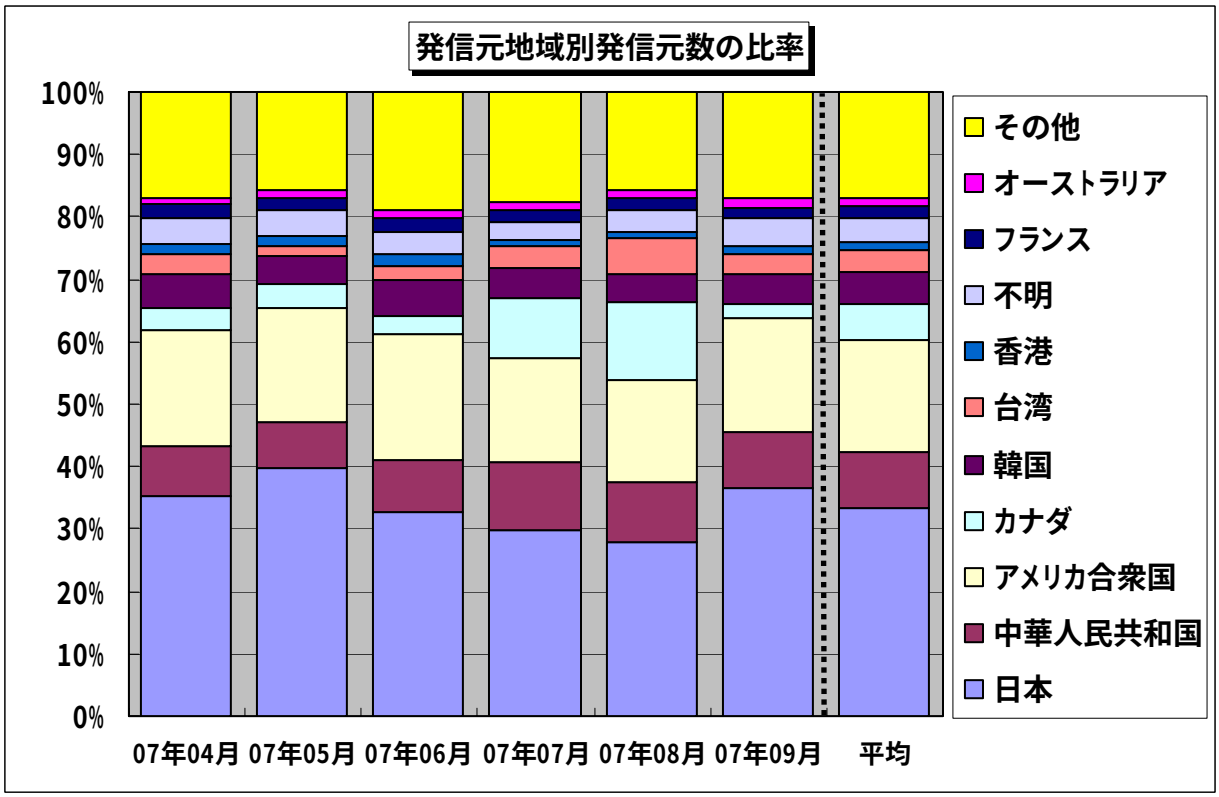
【図 3.1.2 2007 年 4 月～2007 年 9 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 4 月～2007 年 9 月の発信元地域別の比率

2007 年 4 月～2007 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 2007 年 4 月～2007 年 9 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 4 月～2007 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、2007 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)
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
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
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
2967(TCP)	Symantec Client Security や Symantec AntiVirus がデフォルトで使用するポートで、今回のアクセスはこれらの製品のぜい弱性を狙ったものと考えられます
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)
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／宮本
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp