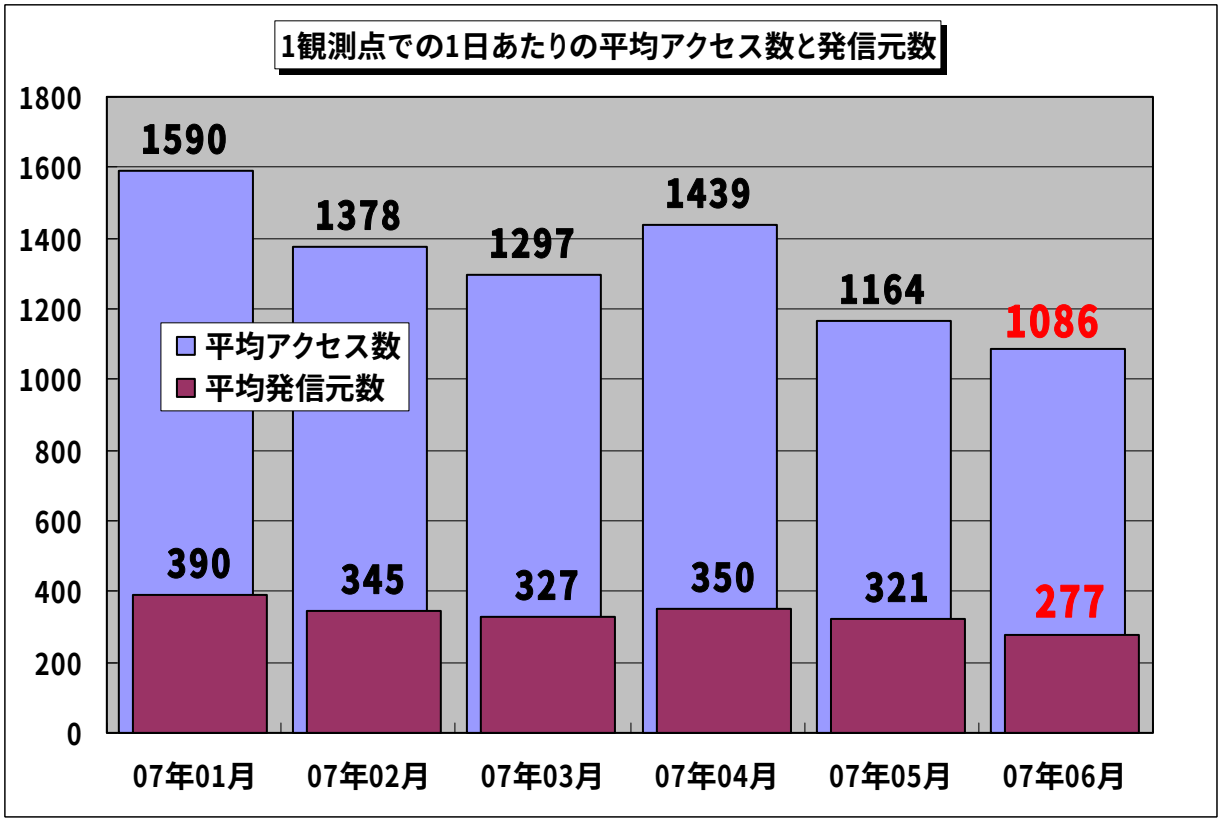
別紙 3

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 6 月の期待しない（一方的な）アクセスの総数は、10 観測点で **293,252 件**ありました。1 観測点で 1 日あたり **277** の発信元から **1,086 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、277 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　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 1 月～2007 年 6 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、緩やかですが減少傾向にあるようです。

注意）

6 月 1 日から 3 日までは TALOT2 システム保守の為、6 月 4 日から 6 月 30 日までの観測データで発表しておりますことをご了承下さい。

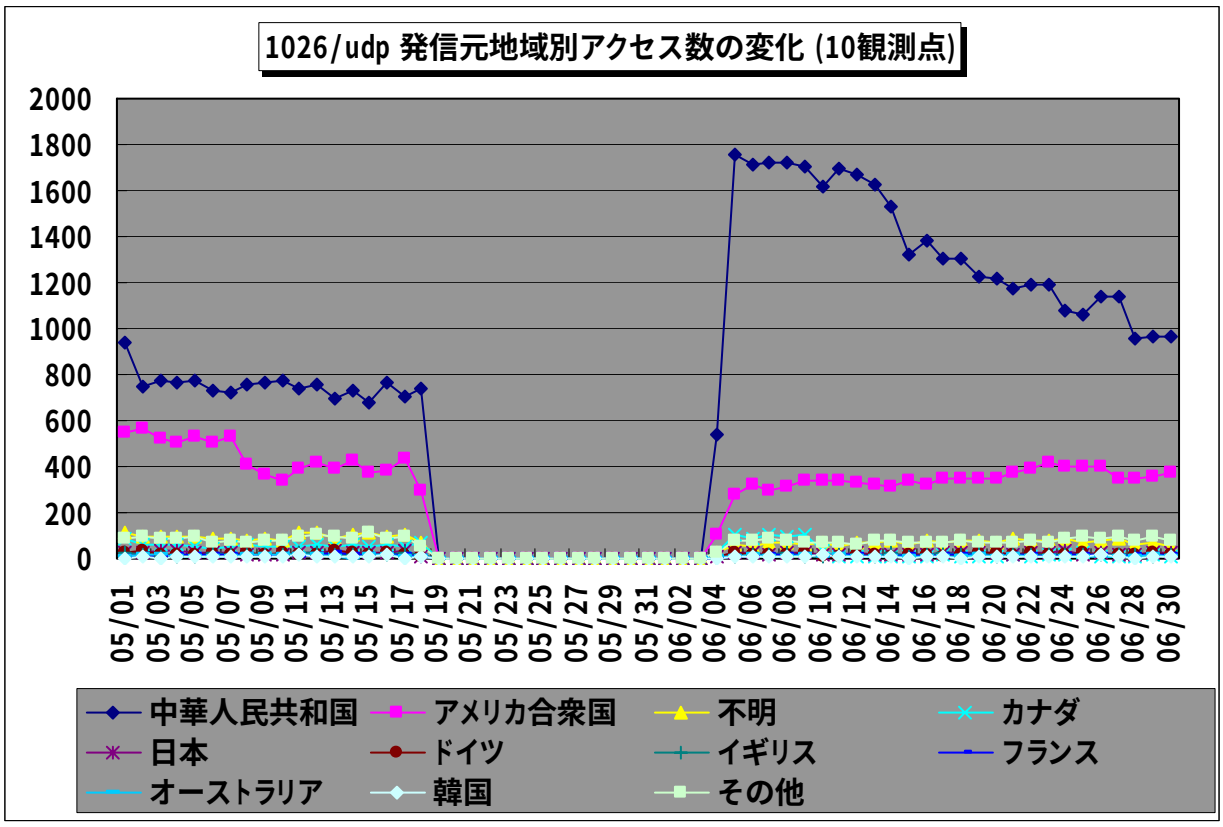
2．6 月のアクセス状況

2007 年 6 月のアクセス状況は、全体的に 5 月と同じで定常化していると言えます。Windows のぜい弱性を狙った、135/tcp、445/tcp のアクセスは相変わらず多い状況の中、Windows Messenger サービスを悪用してポップアップメッセージを送信する、1026/udp、1027/udp のアクセスが増加しました。

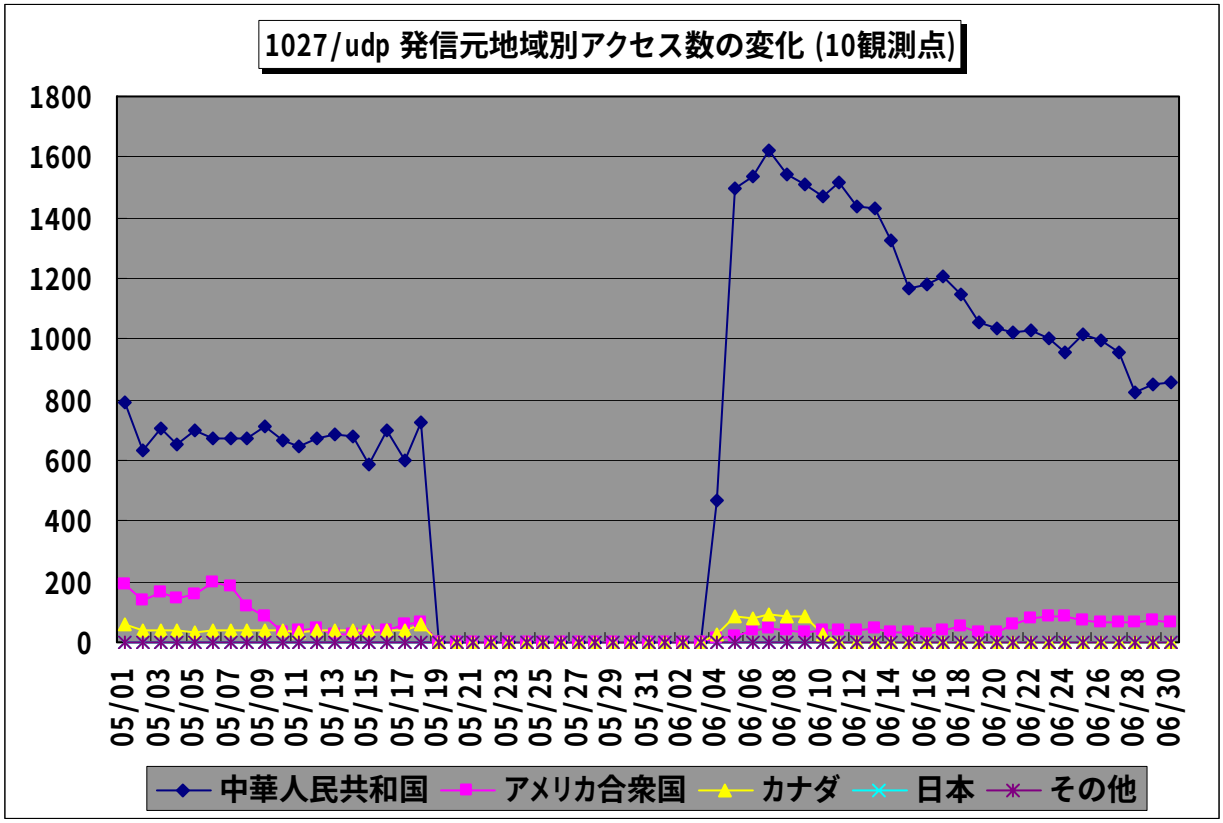
2.1. 1026/udp、1027/udp ポートを狙ったアクセス

2007 年 6 月の、1026/udp、1027/udp ポートのアクセスは、2007 年 5 月と比べると、約 2 倍近くのアクセス数がありました。これらのほとんどが中国からのアクセスです。

図 2.1.1、図 2.1.2 に、2007 年 5 月から 2 ヶ月間の、1026/udp、1027/udp ポートへの発信元地域別アクセス数の変化を示します。



【図 2.1.1　2007 年 5 月～6 月の 1026/udp ポートへの発信元地域別アクセス数の変化】



【図 2.1.1　2007 年 5 月～6 月の 1027/udp ポートへの発信元地域別アクセス数の変化】

これらのアクセスは、Windows Messenger サービスを悪用して、ポップアップメッセージを送りつけてくるものです。ただ、メッセージが表示されるには、いくつかの条件がある為、全てのコンピュータに表示されるわけではありません。

このように送られてくるポップアップメッセージは、スパムメッセージのようなものが多いので、無視をしていれば問題はありませんが、Windows Messenger サービスの脆弱性のセキュリティパッチが適用されていないと、リモートからコードを実行される危険性があります。セキュリティパッチが適用されているか確認を行ってください。

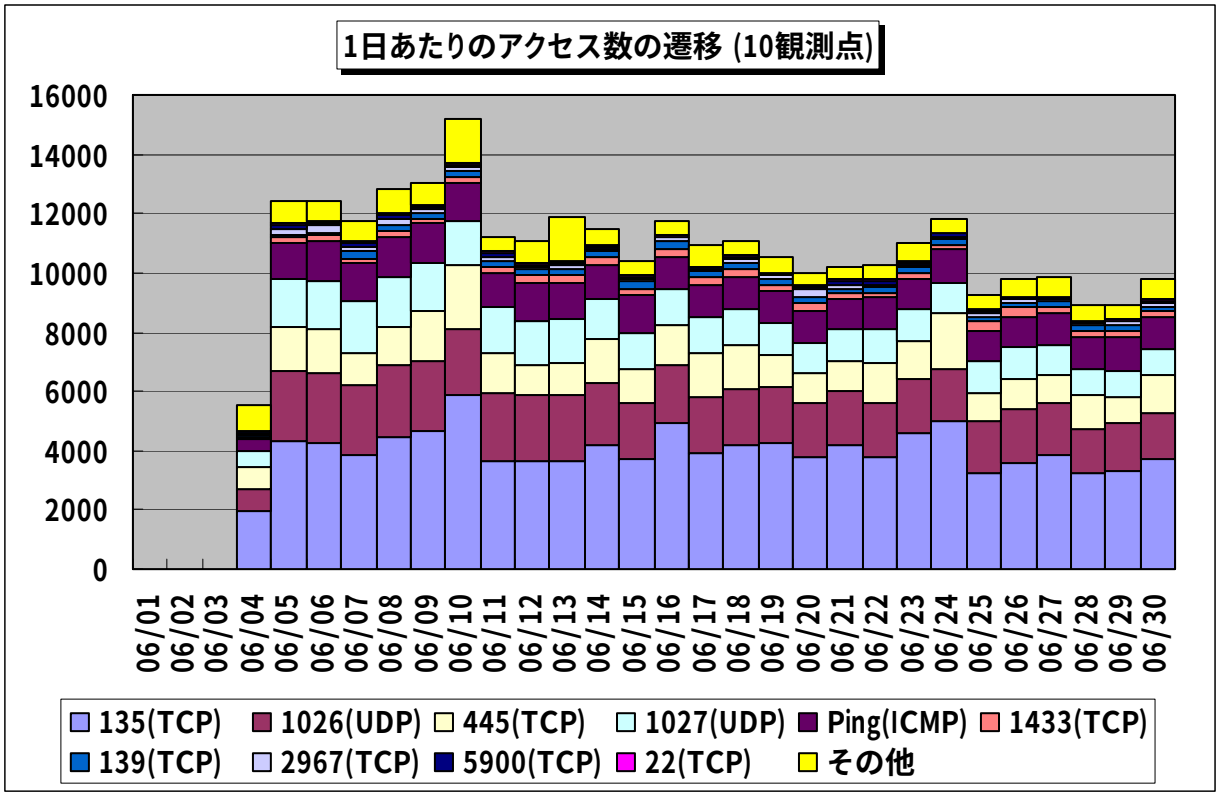
<参考情報>

■ メッセンジャ サービスのバッファオーバーランにより、コードが実行される。(MS03-043)
http://www.microsoft.com/japan/technet/security/Bulletin/MS03-043.mspx

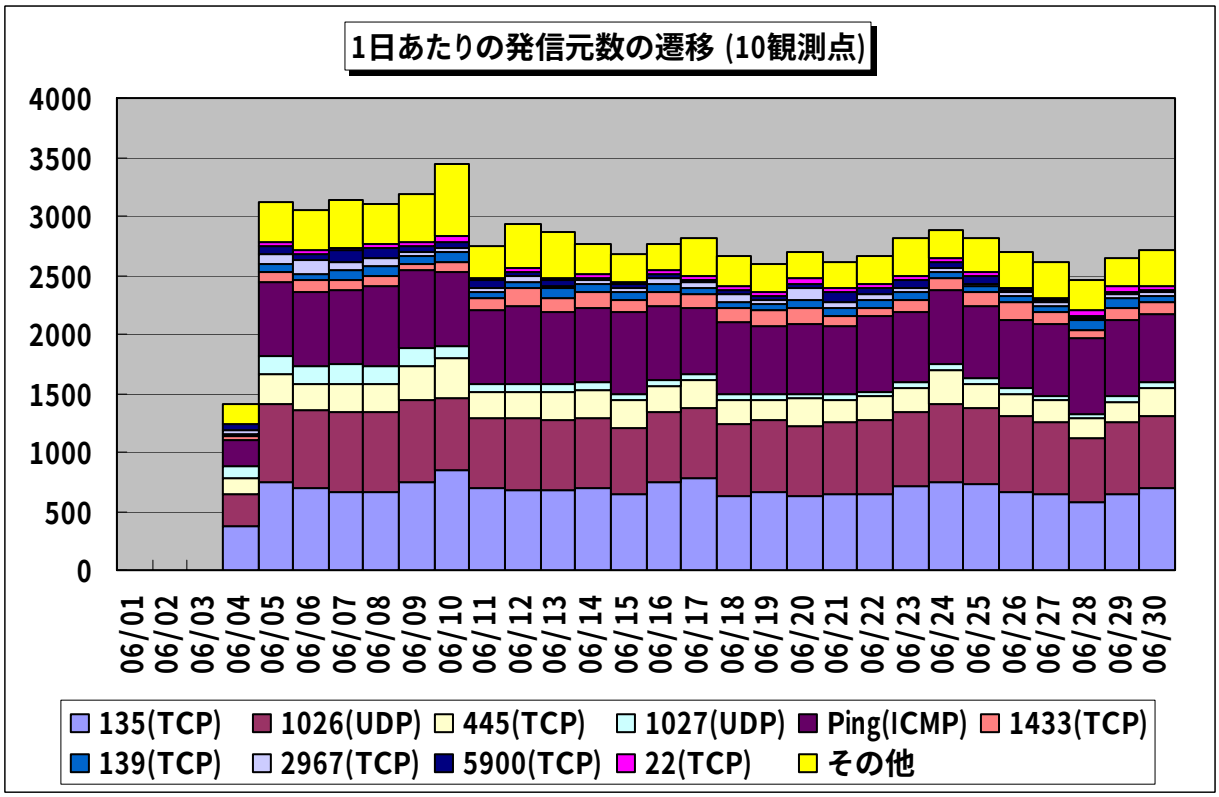
最近では、この様な Messenger サービスを使って、ウイルスが送られてきたり、フィッシングサイトに誘導するものもあります。Messenger サービスを使用しているコンピュータのセキュリティ対策を、再確認されることをお勧めします。

2.2 2007 年 6 月の一方的なアクセス状況

2007 年 6 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。



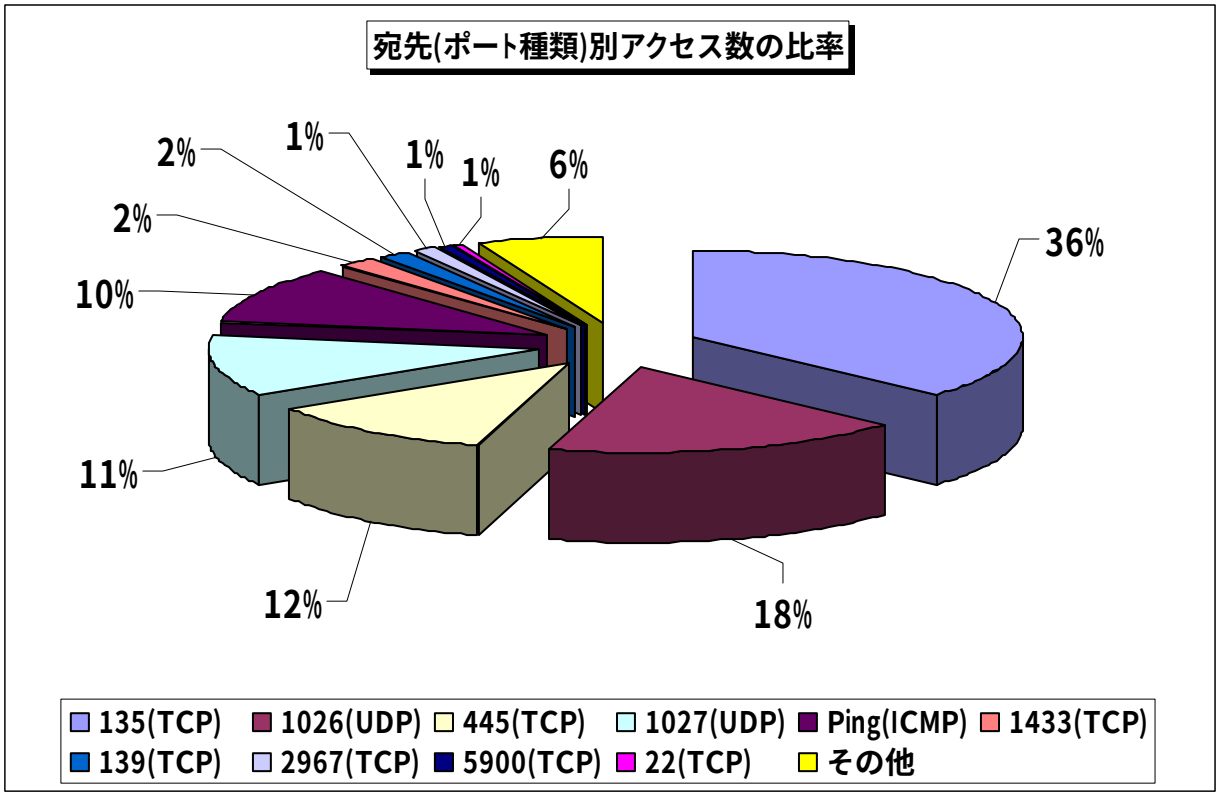
【図 2.2.1 2007 年 6 月の一方的なアクセス状況(アクセス数)】



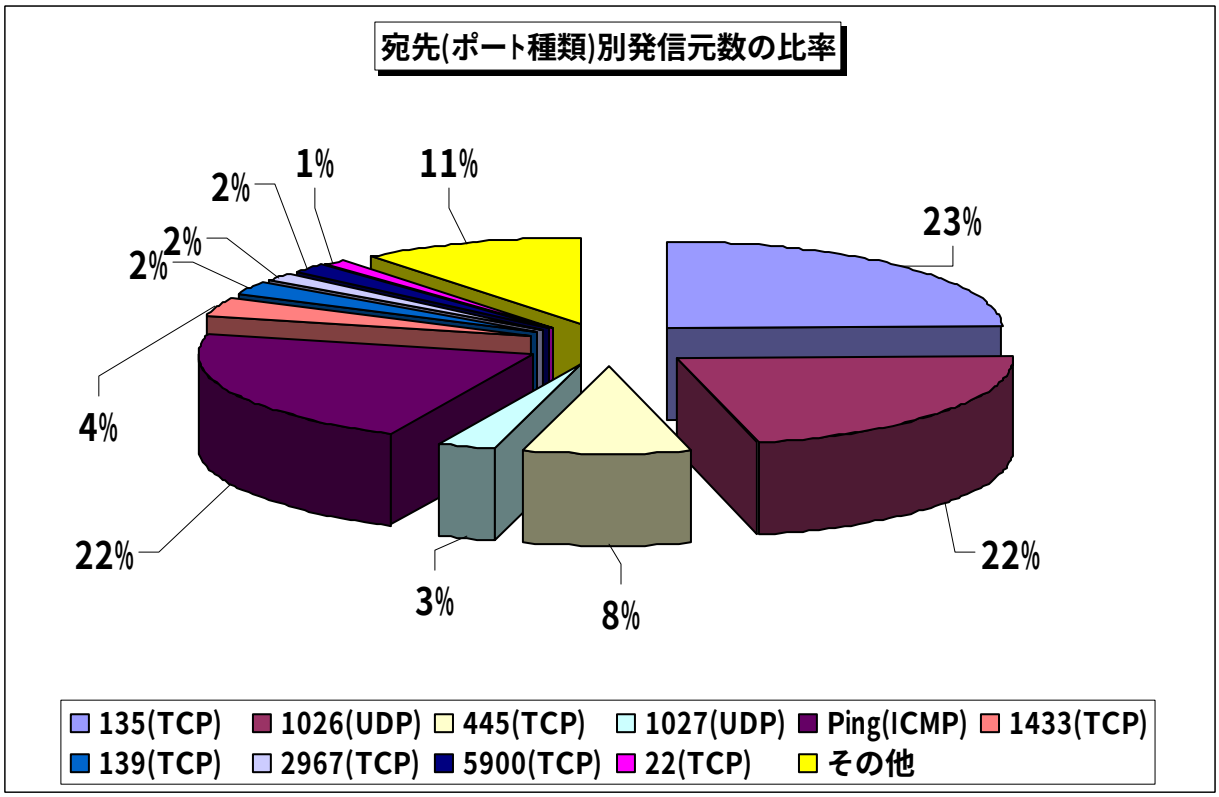
【図 2.2.2 2007 年 6 月の一方的なアクセス状況(発信元数)】

2.3 2007 年 6 月の宛先(ポート種類)別の比率

2007 年 6 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。



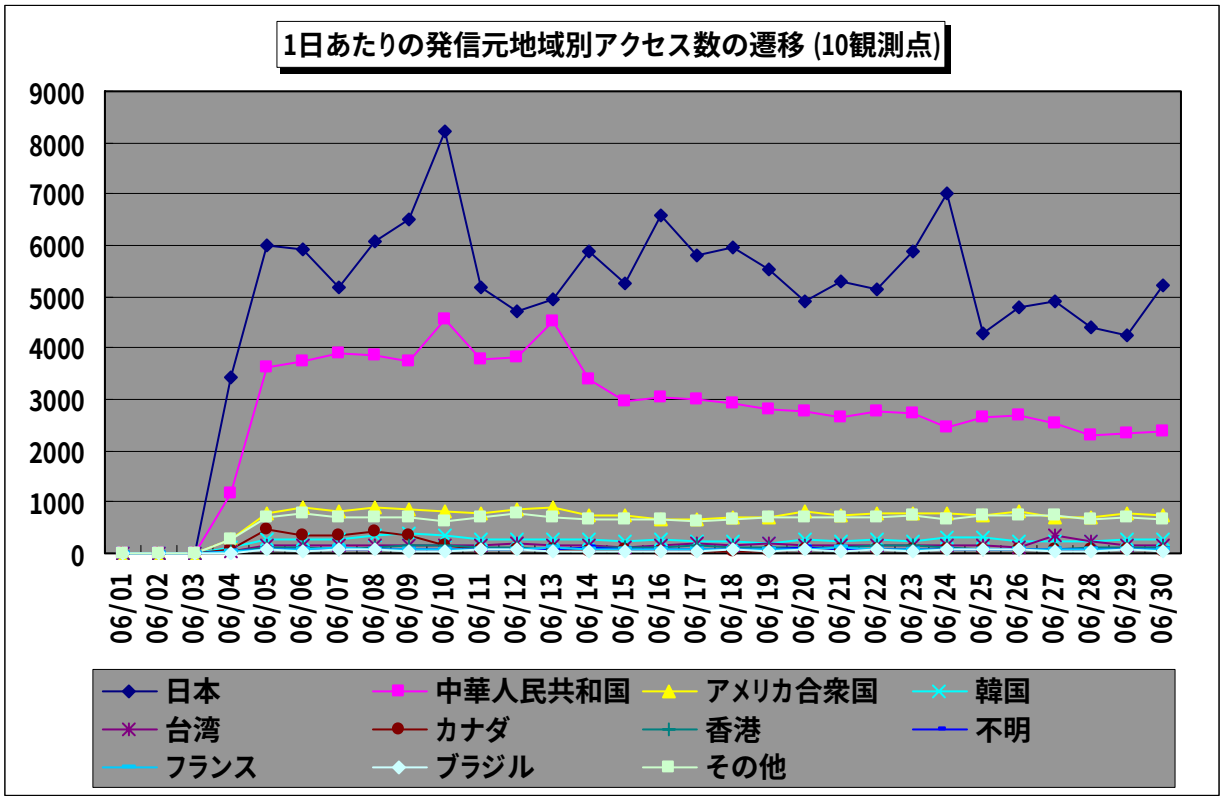
【図 2.3.1 2007 年 6 月の宛先(ポート種類)別アクセス数の比率】



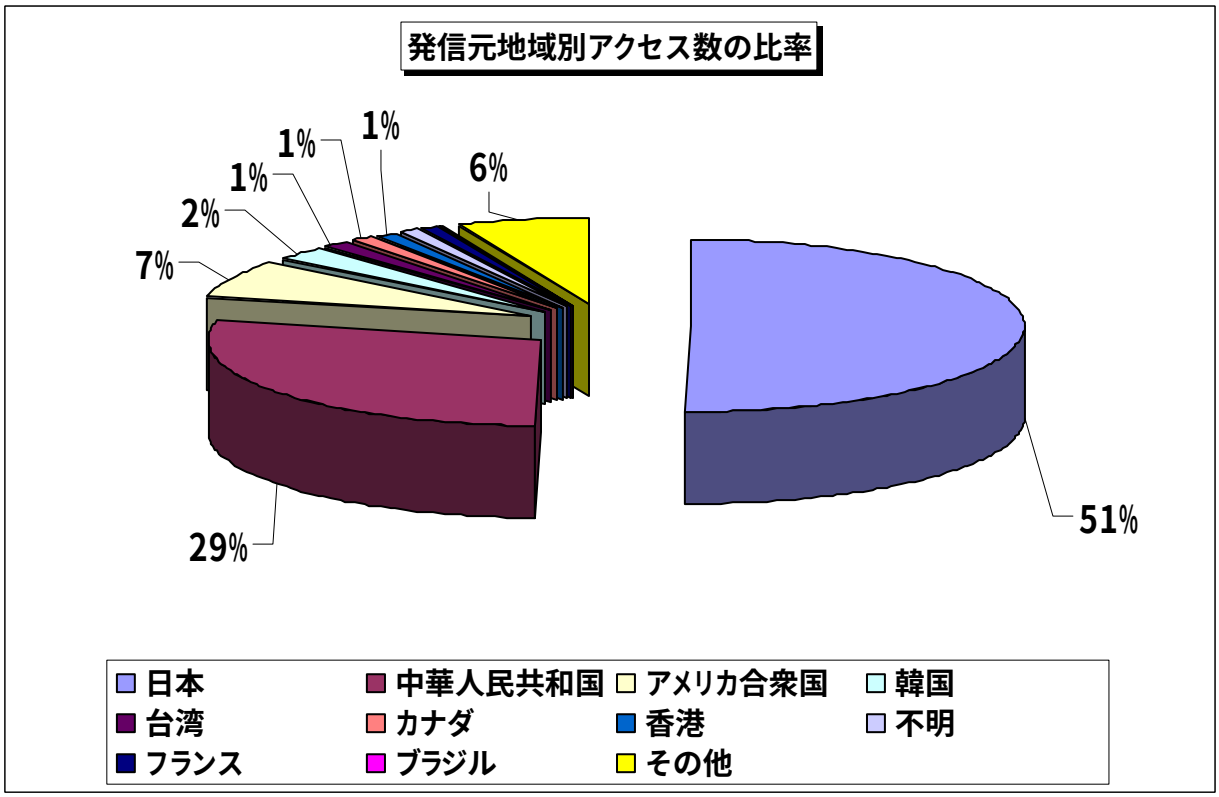
【図 2.3.2 2007 年 6 月の宛先(ポート種類)別発信元数の比率】

2.4 2007 年 6 月の発信元地域別アクセス状況

2007 年 6 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。

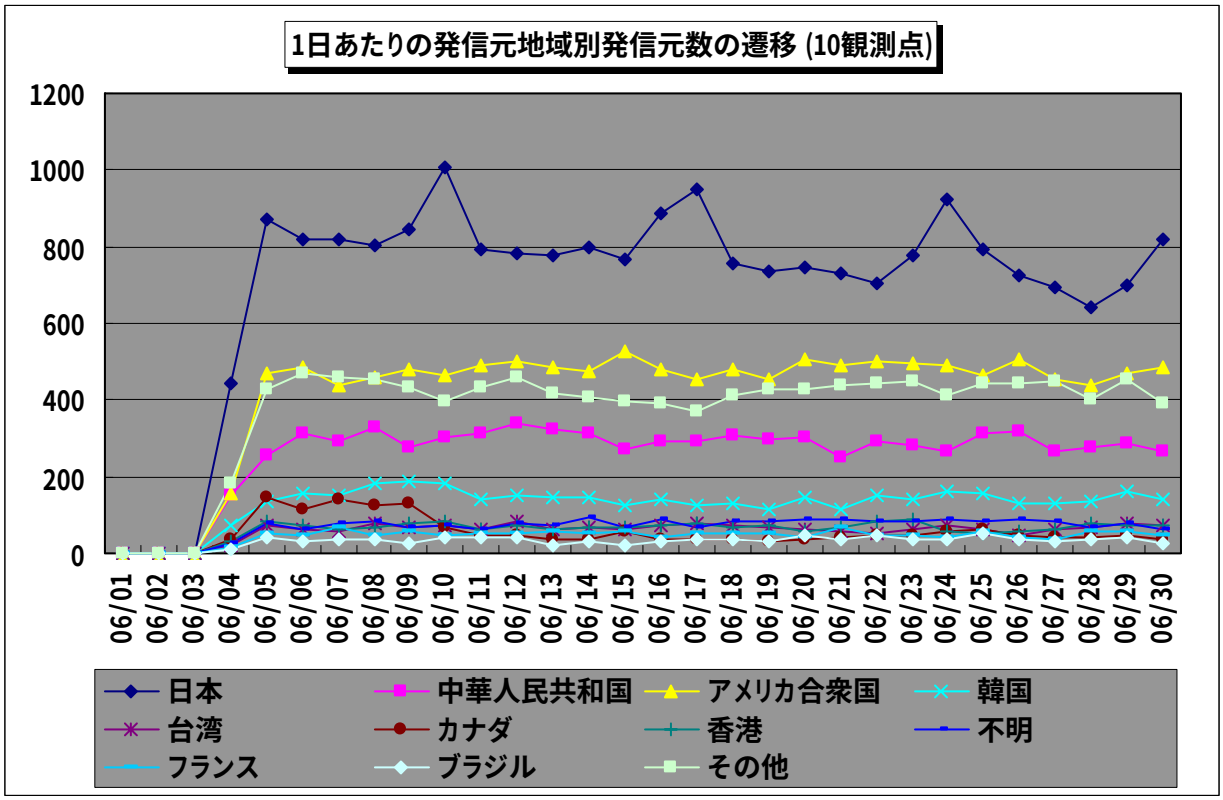


【図 2.4.1 2007 年 6 月の発信元地域別アクセス数の変化】

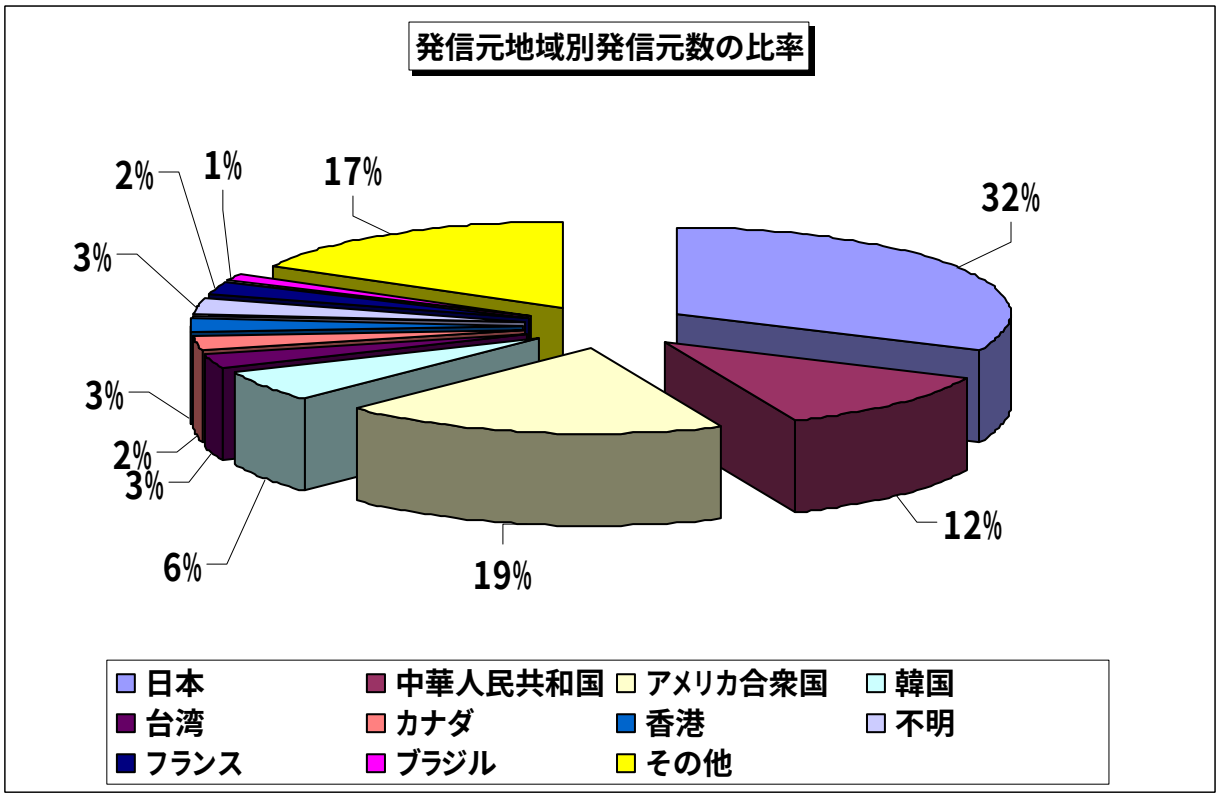


【図 2.4.2 2007 年 6 月の発信元地域別アクセス数の比率】

2007 年 6 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 2007 年 6 月の発信元地域別発信元数の変化】

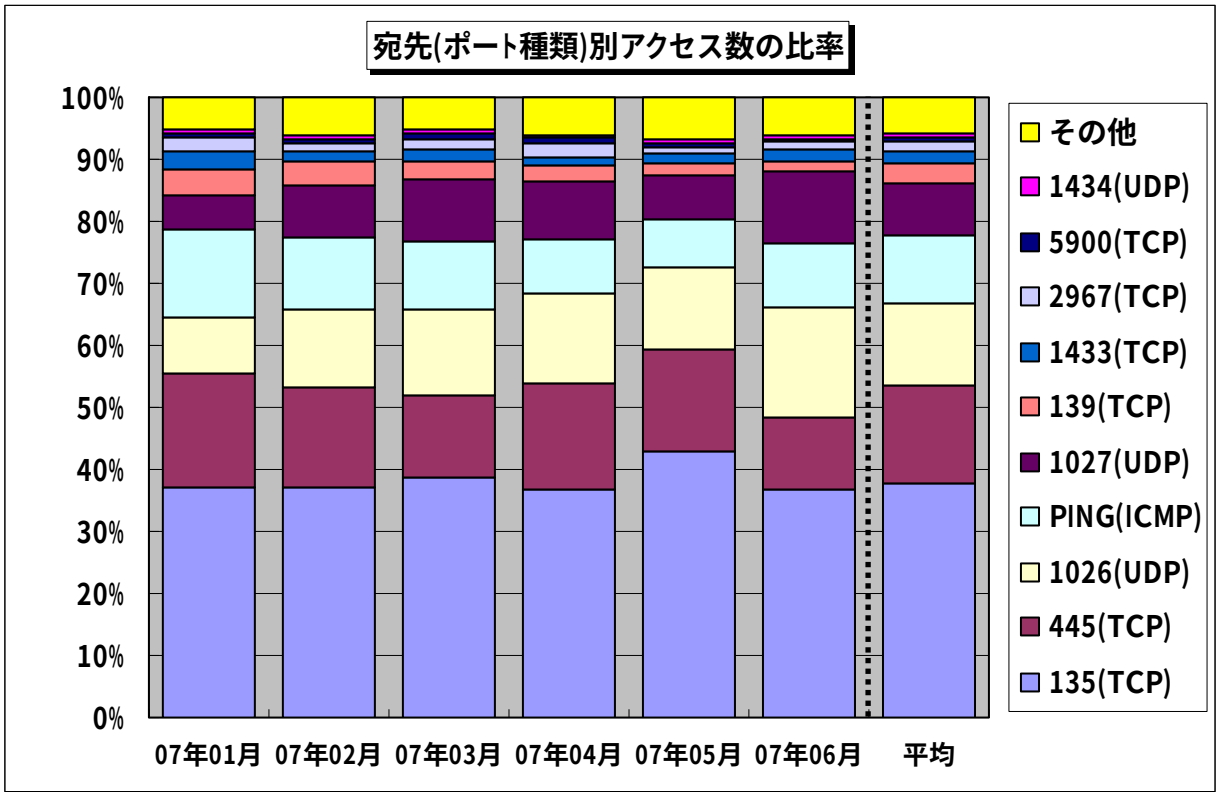


【図 2.4.4 2007 年 6 月の発信元地域別発信元数の比率】

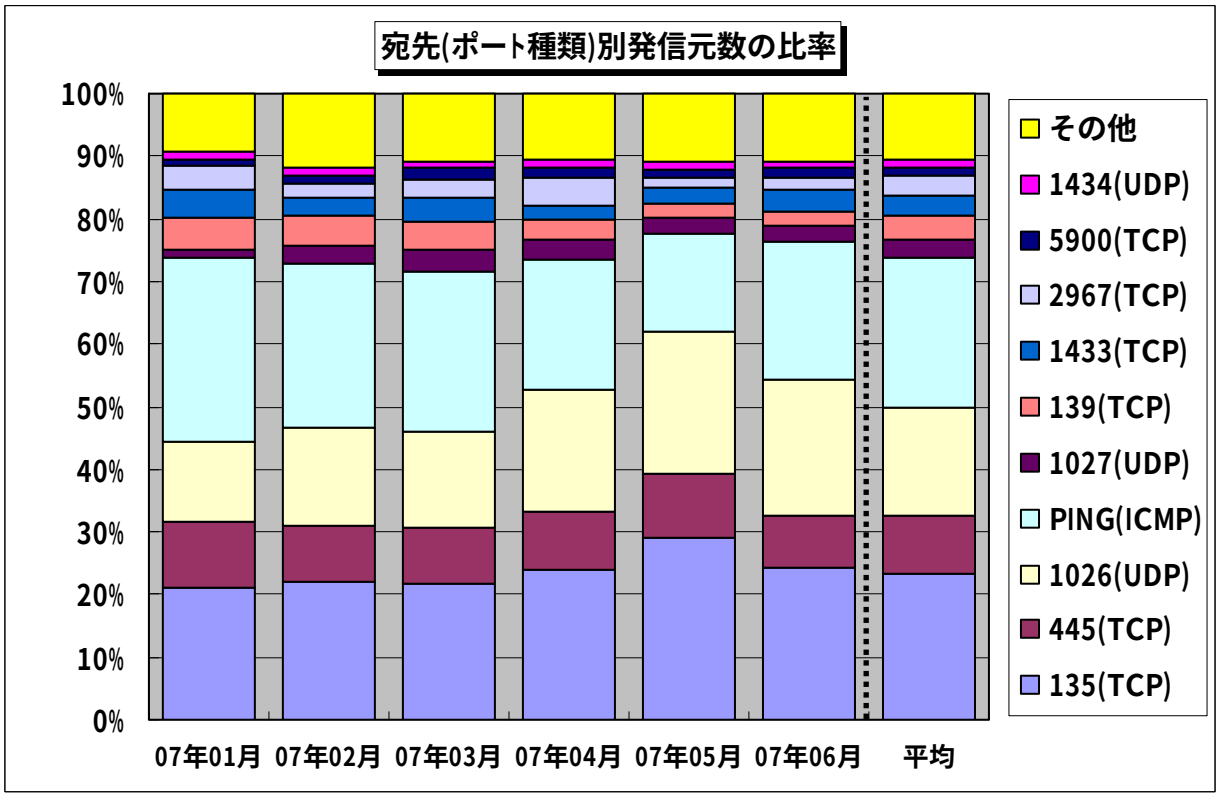
3．統計情報

3.1 2007 年 1 月～2007 年 6 月の宛先(ポート種類)別の比率

2007 年 1 月～2007 年 6 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。



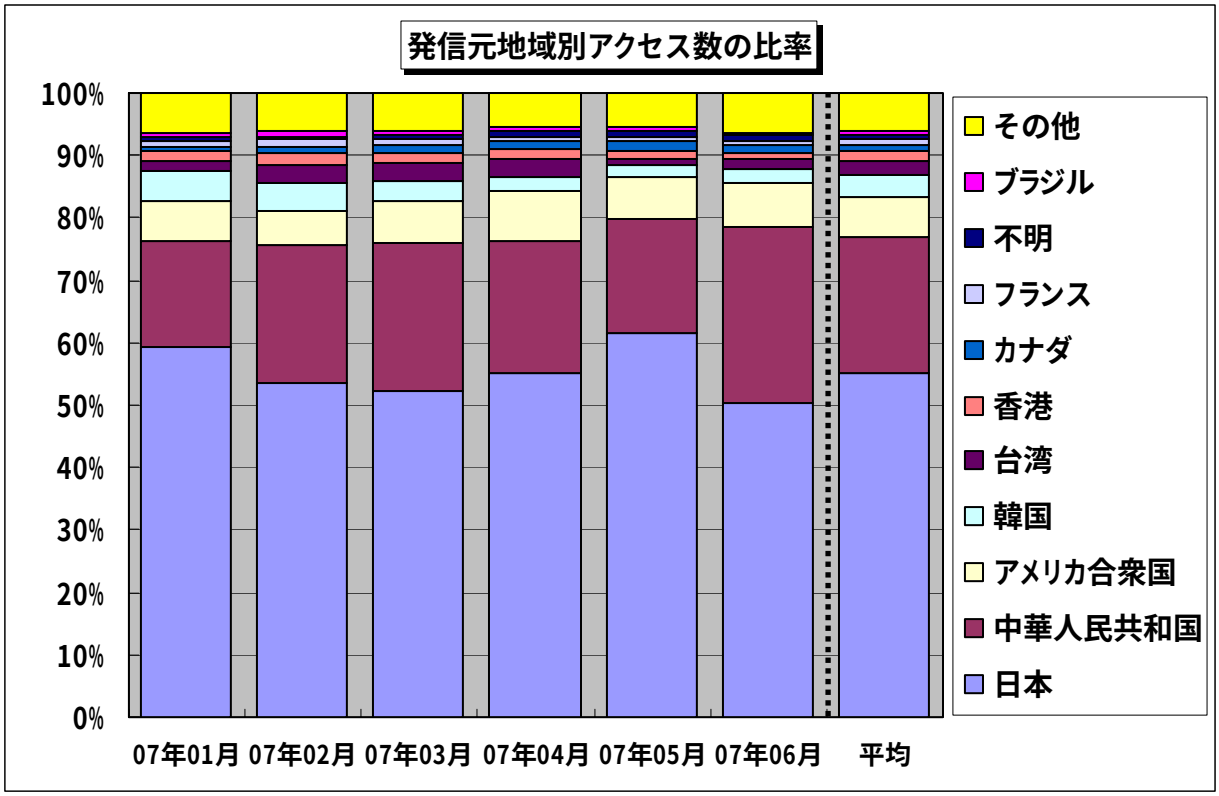
【図 3.1.1 2007 年 1 月～2007 年 6 月の宛先(ポート種類)別アクセス数の比率】



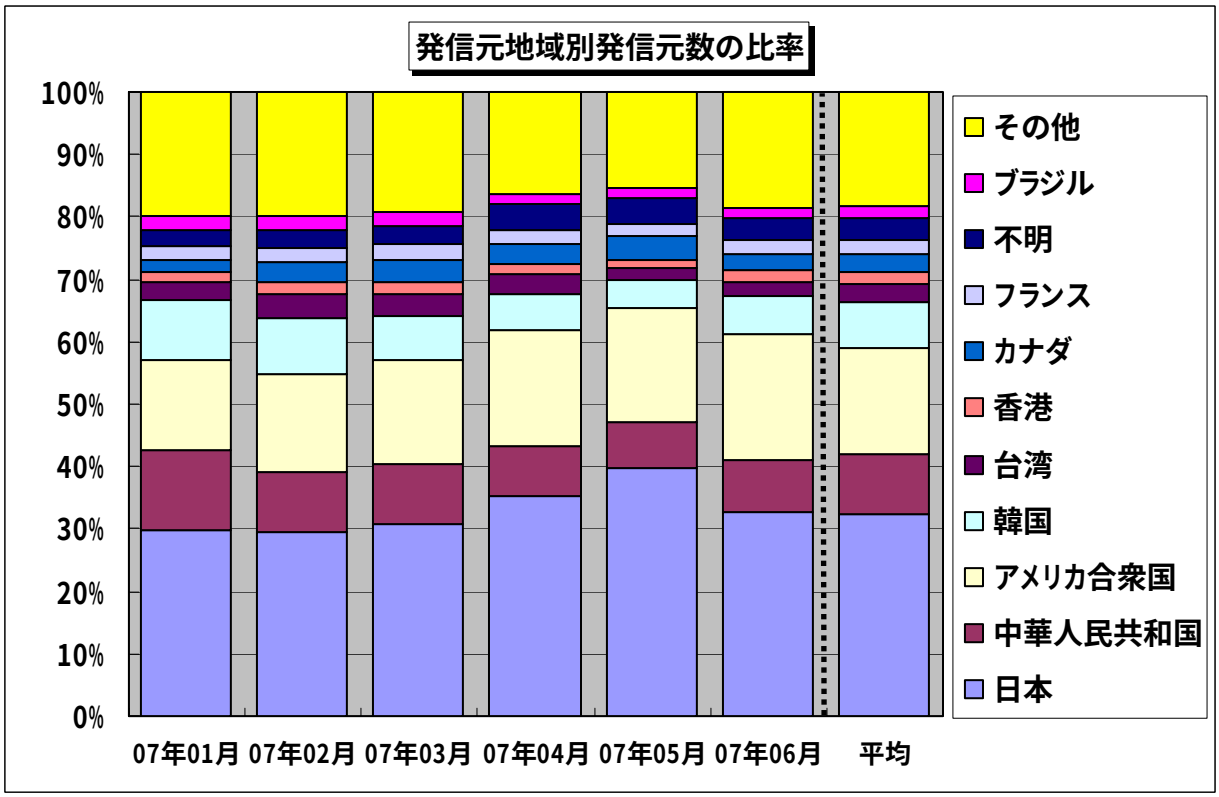
【図 3.1.2 2007 年 1 月～2007 年 6 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 1 月～2007 年 6 月の発信元地域別の比率

2007 年 1 月～2007 年 6 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 1 月～2007 年 6 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 1 月～2007 年 6 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 6 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)
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
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
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
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
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
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
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