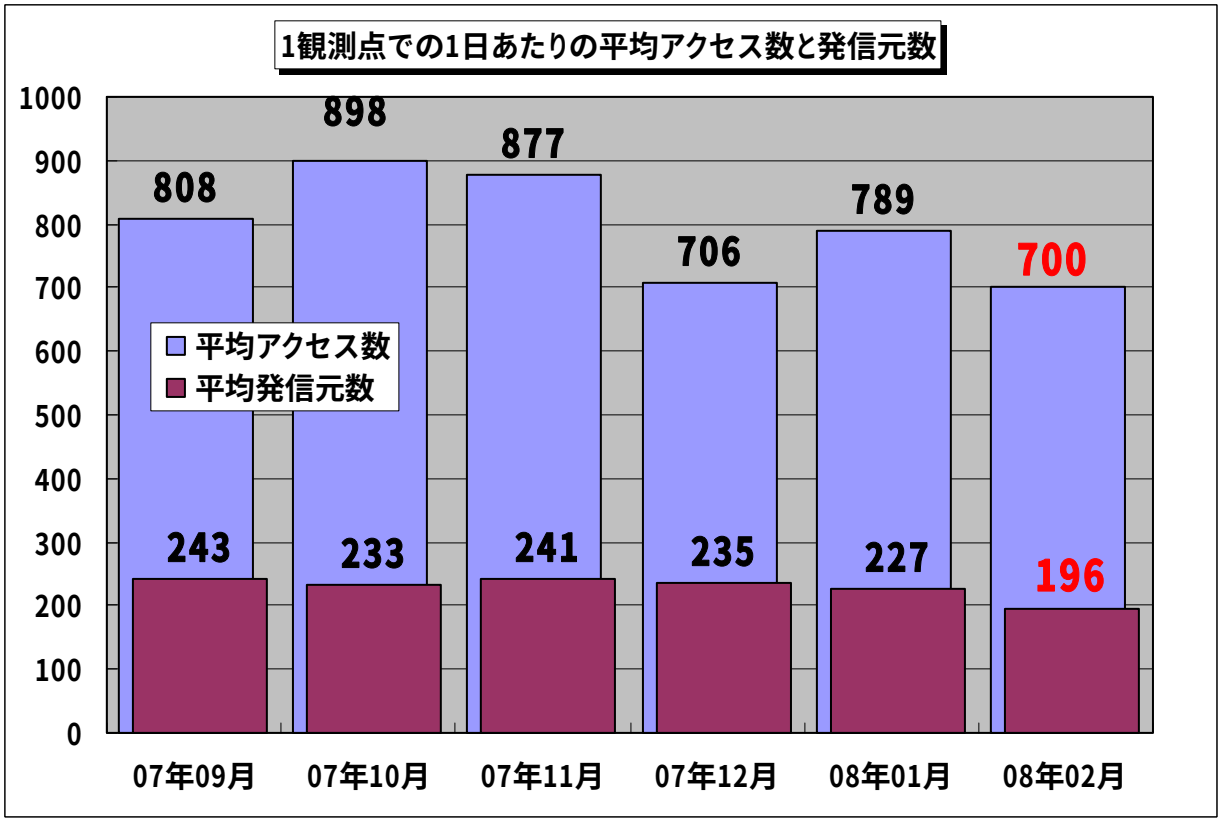
別紙 3

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、2008 年 2 月の期待しない（一方的な）アクセスの総数は、10 観測点で **189,006 件**ありました。1 観測点で 1 日あたり **196** の発信元から **700 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、196 人の見知らぬ人(発信元)から、発信元一人当たり約 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 9 月～2008 年 2 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、2 月の期待しない（一方的な）アクセスは 1 月よりも減少しましたが、全体的なアクセスの内容としては、定常化していると言えます。

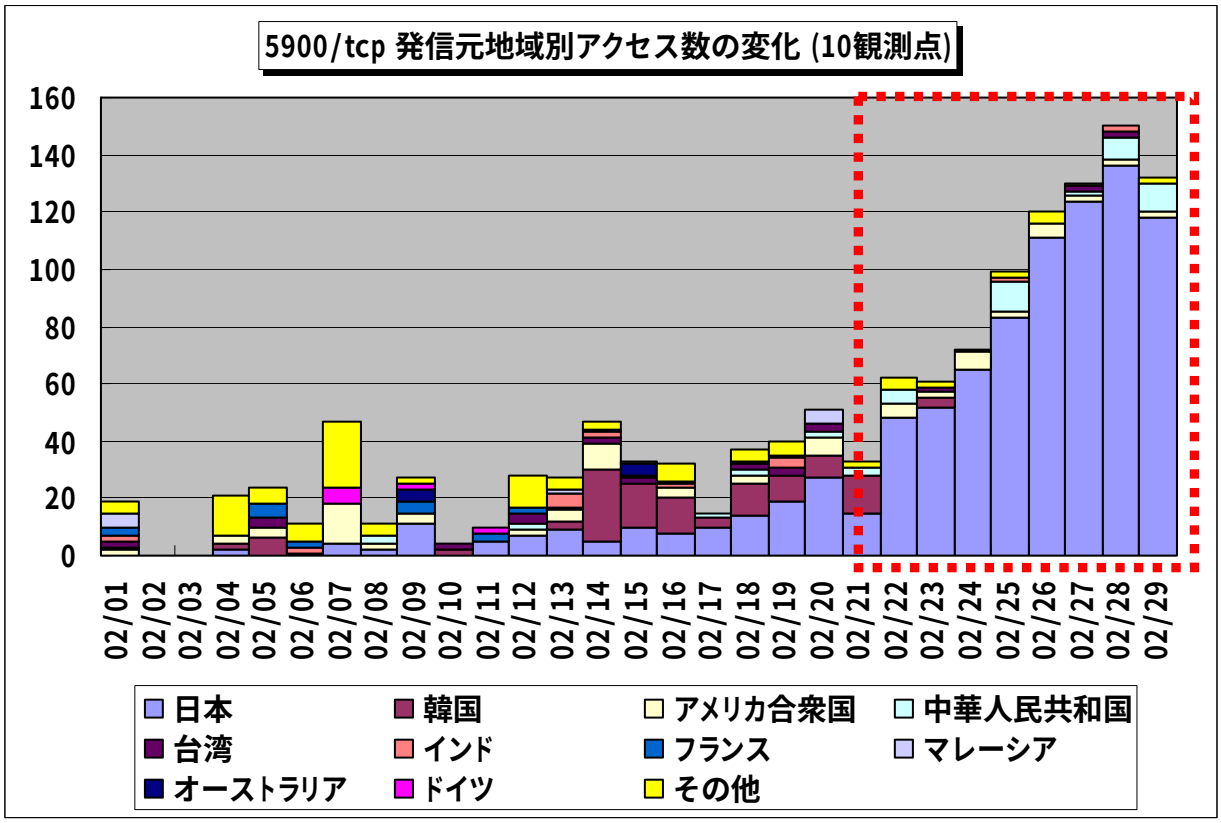
2．2 月のアクセスの状況

2008 年 2 月のアクセス状況は、1 月よりも減少しました。これは、全体のアクセス数そのものが減少したためです。ただ、Windows の脆弱性（ぜいじゃくせい）を狙った、135/tcp、445/tcp へのアクセスや、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 へのアクセスは 1 月と同じ水準で観測されました。

※ 2 月 2 日～3 日は、TALOT2 のシステムメンテナンスのため、観測データがありません。今月の報告書は、この 2 日間を除外して統計情報を作成している事をご了承下さい。

2.1. 5900/tcp を狙ったアクセス

2 月の後半には、5900/tcp へのアクセスが増加しました。これは、RealVNC クライアントが RealVNC サーバへ接続するときに使用するデフォルトのポートです。発信元地域のほとんどは、日本からでした。(図 2.1.1 参照)



【図 2.1.1 5900/tcp ポートへの発信元地域別アクセス数の変化】

RealVNC は、リモートのコンピュータを遠隔操作するためのソフトウェアですが、2006 年 5 月に、”認証なしに端末にリモートアクセスできてしまう脆弱性”が公開されています。対策は、バージョンアップです。

(参考情報)

■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/

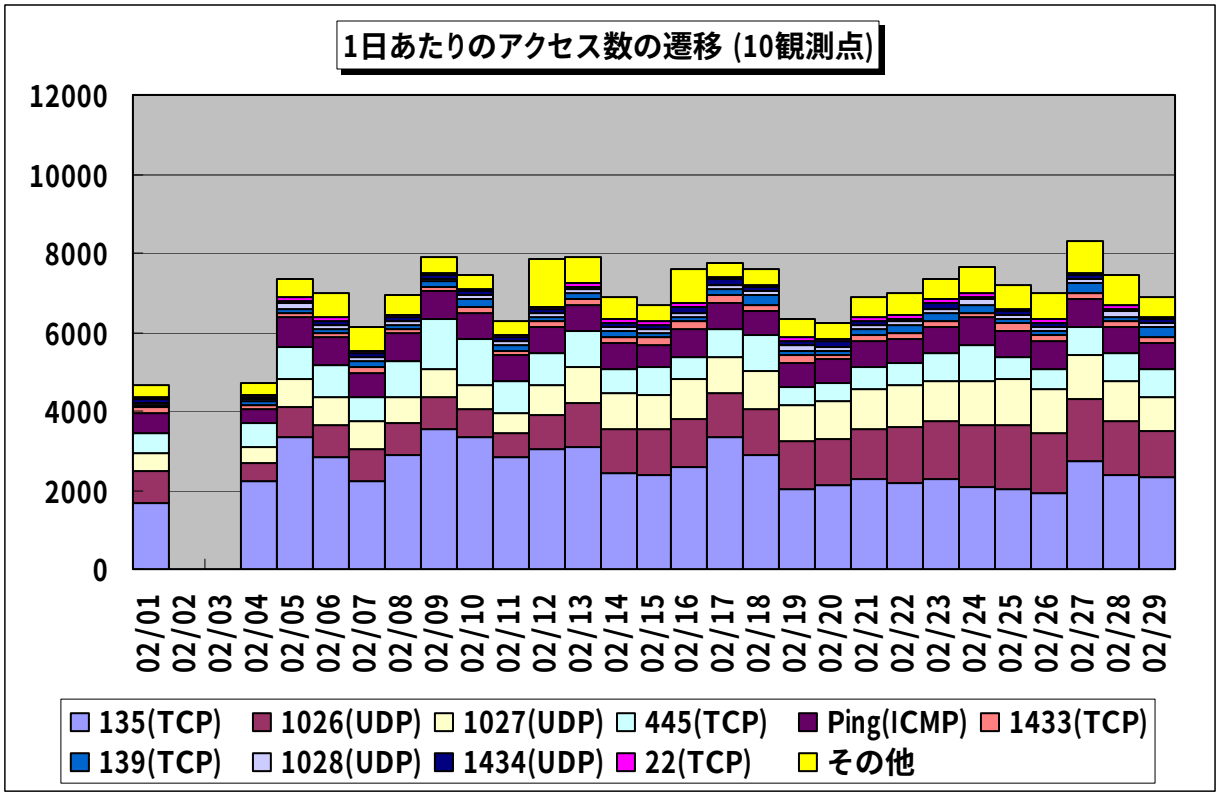
この脆弱性情報の公開の後、RealVNC に関する新しい脆弱性情報は特に公開されていませんが、攻撃者からみれば、リモートアクセスサービスは不正アクセスの足がかりとして有効なものです。

観測では、5900/tcp へのアクセスと同時に Windows の脆弱性を狙った 135/tcp、445/tcp も同時にアクセスするものも多く見受けられます。このことから、これらの不正アクセスは、ツールによって攻撃されている可能性が高く、広範囲に攻撃を行う可能性も考えられます。

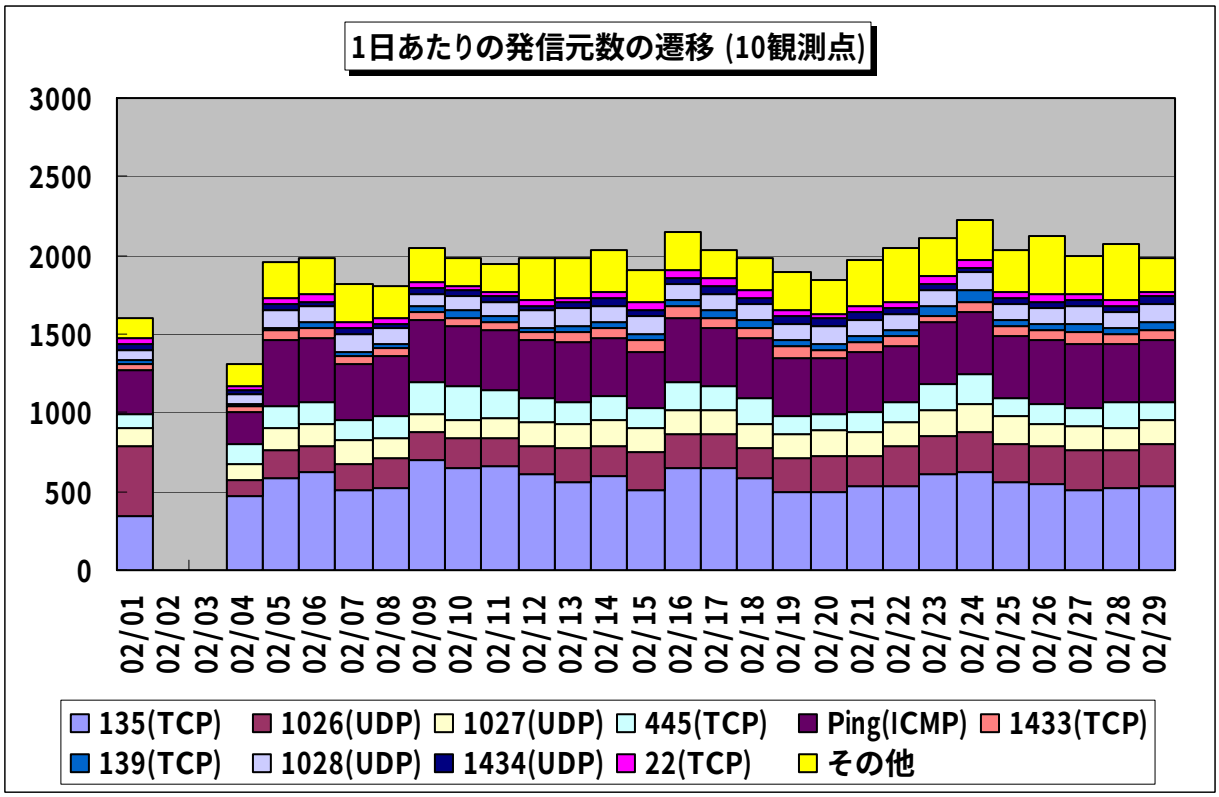
RealVNC などのリモートアクセスツールをお使いの方は、配布元などの情報を確認し、お使いのツールが最新のものであるか確認することをお勧めします。

2.2 2008 年 2 月の一方的なアクセス状況

2008 年 2 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。



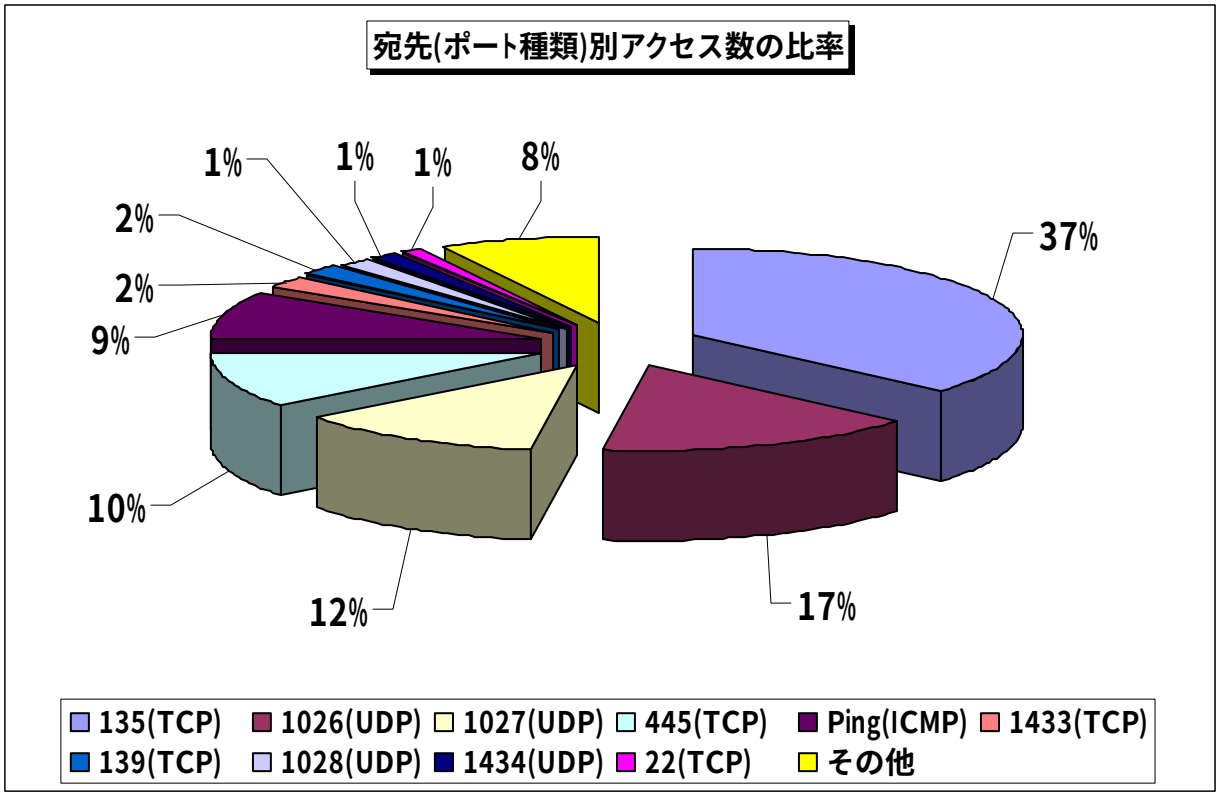
【図 2.2.1 2008 年 2 月の一方的なアクセス状況(アクセス数)】



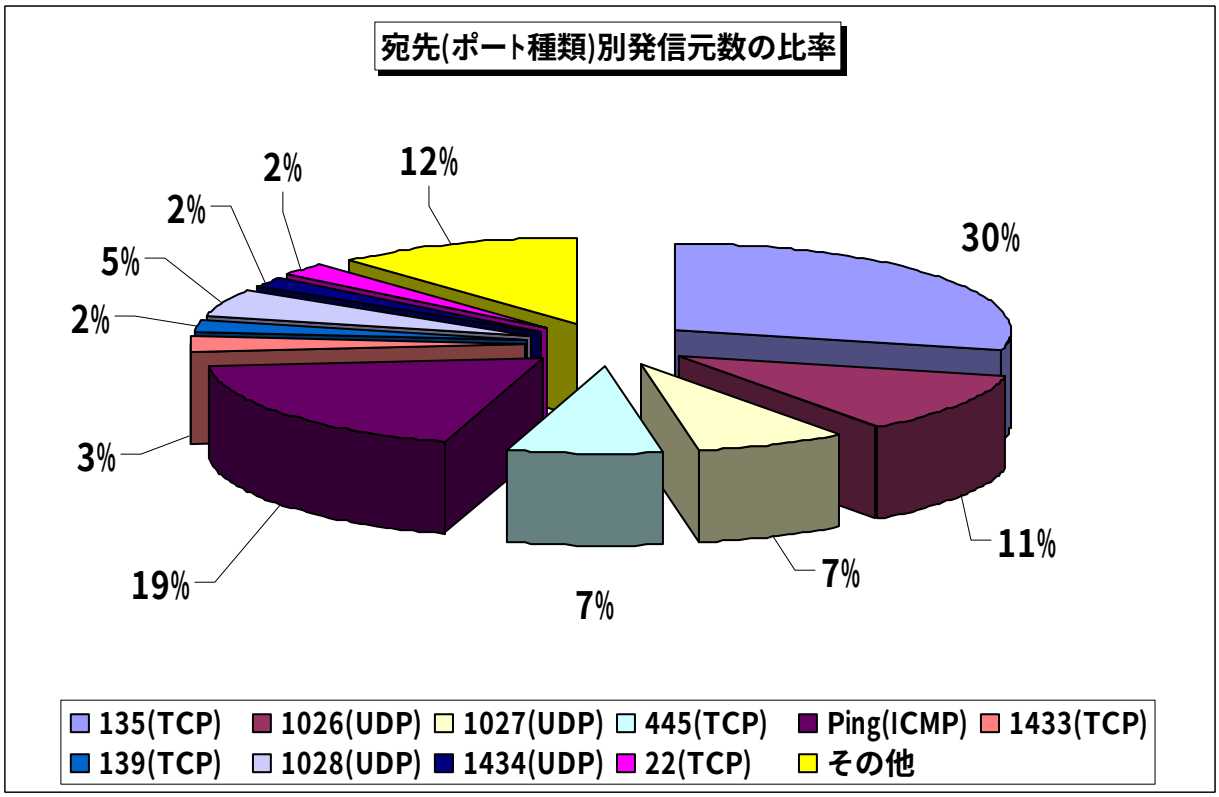
【図 2.2.2 2008 年 2 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 2 月の宛先(ポート種類)別の比率

2008 年 2 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。



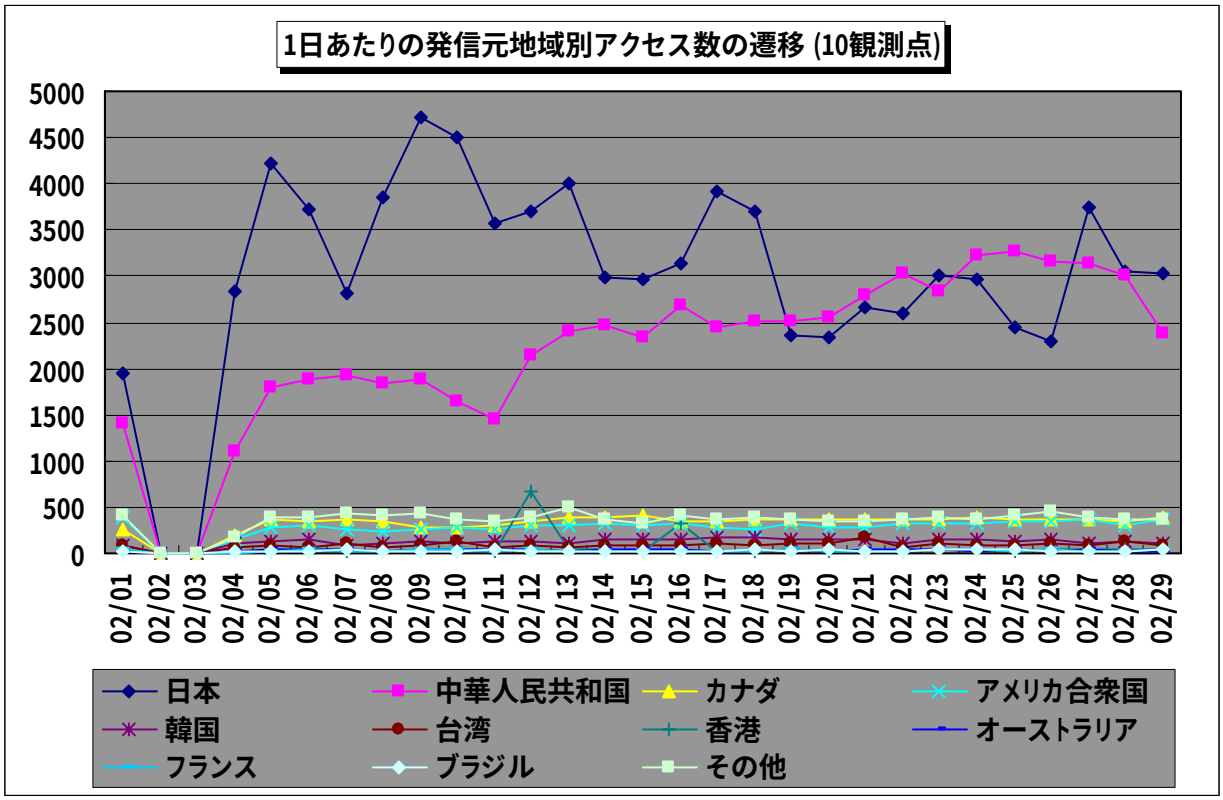
【図 2.3.1 2008 年 2 月の宛先(ポート種類)別アクセス数の比率】



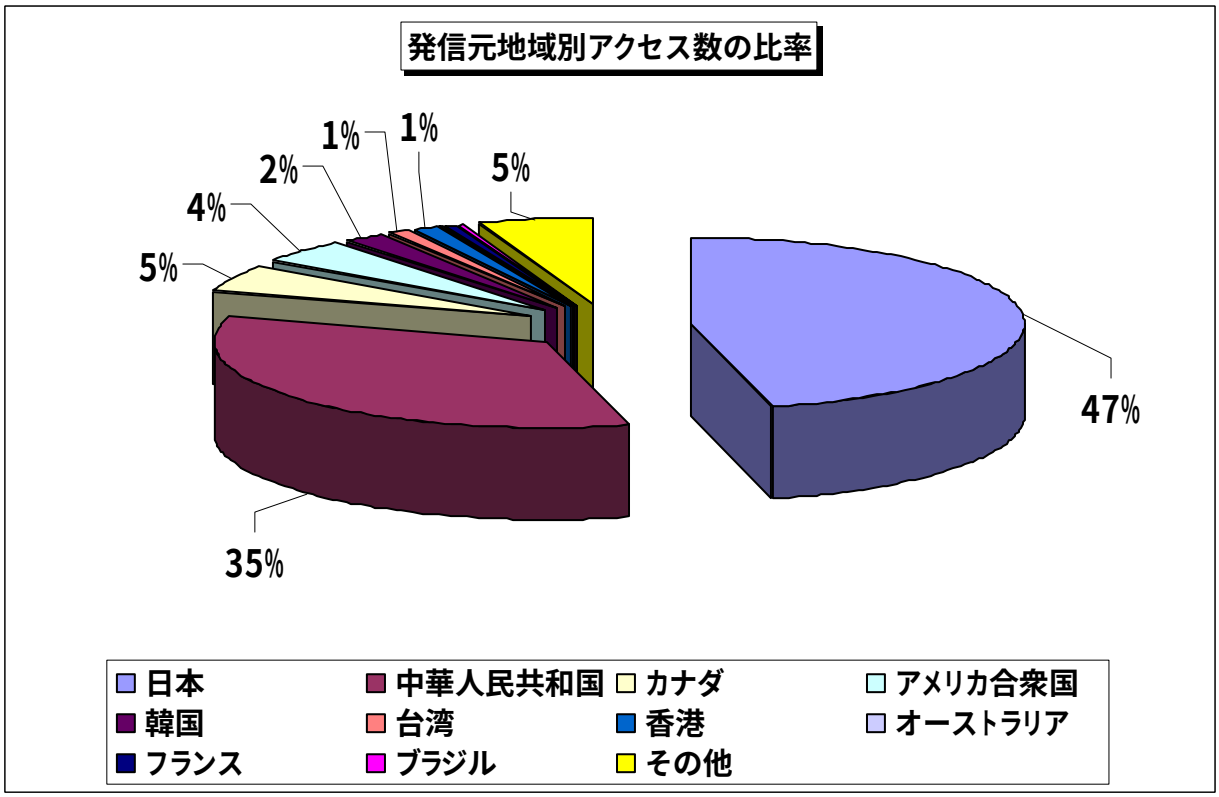
【図 2.3.2 2008 年 2 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 2 月の発信元地域別アクセス状況

2008 年 2 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。

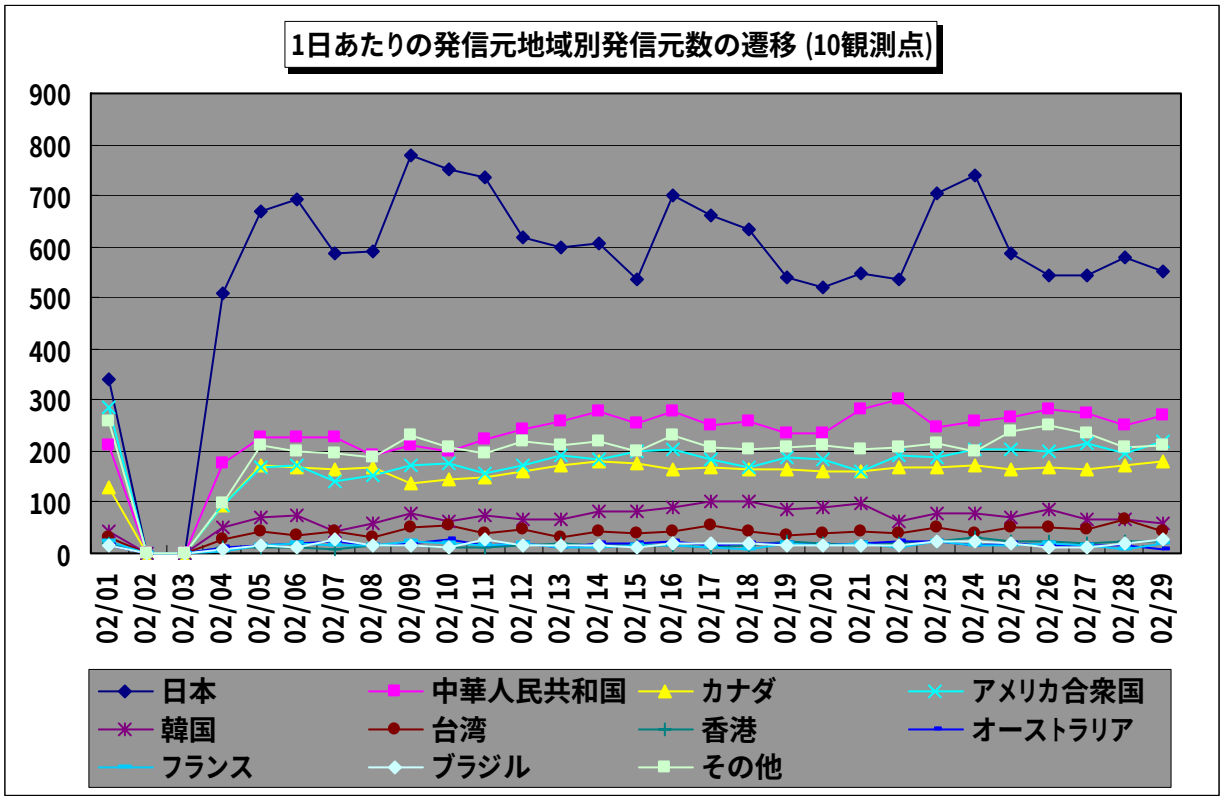


【図 2.4.1 2008 年 2 月の発信元地域別アクセス数の変化】

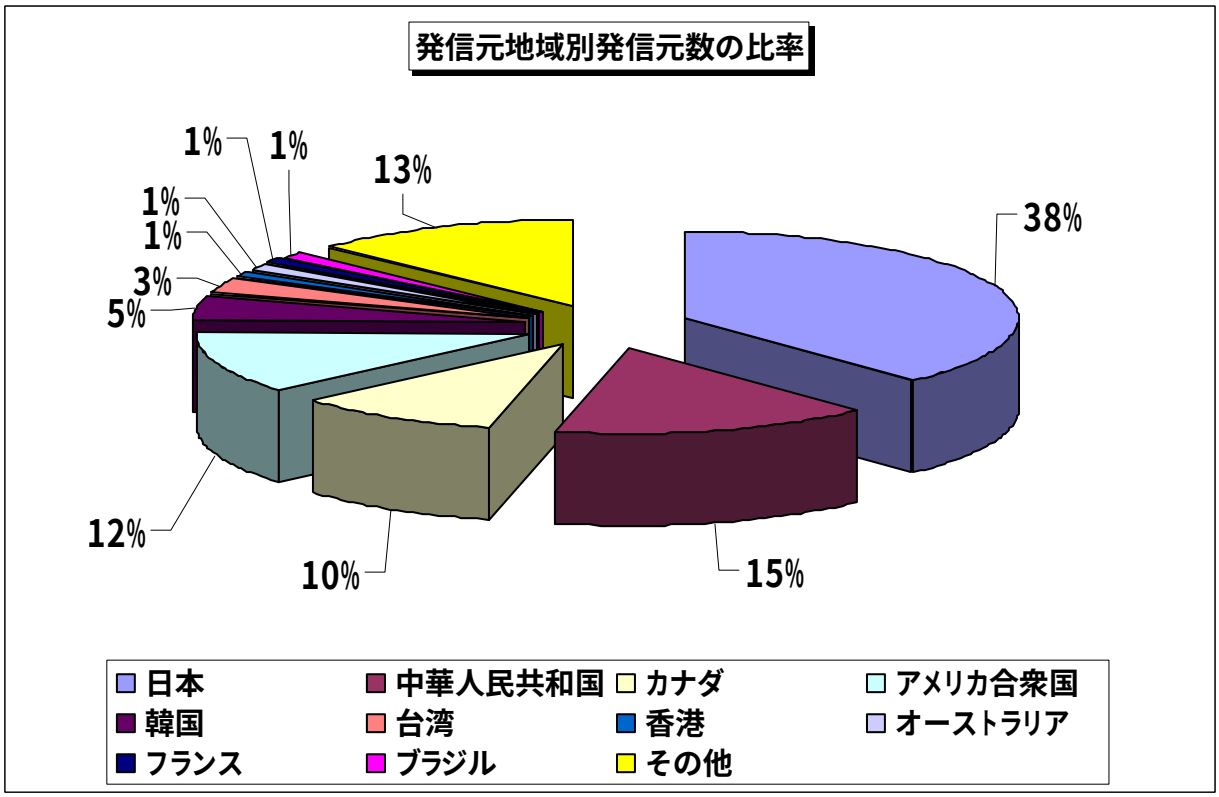


【図 2.4.2 2008 年 2 月の発信元地域別アクセス数の比率】

2008 年 2 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 2008 年 2 月の発信元地域別発信元数の変化】

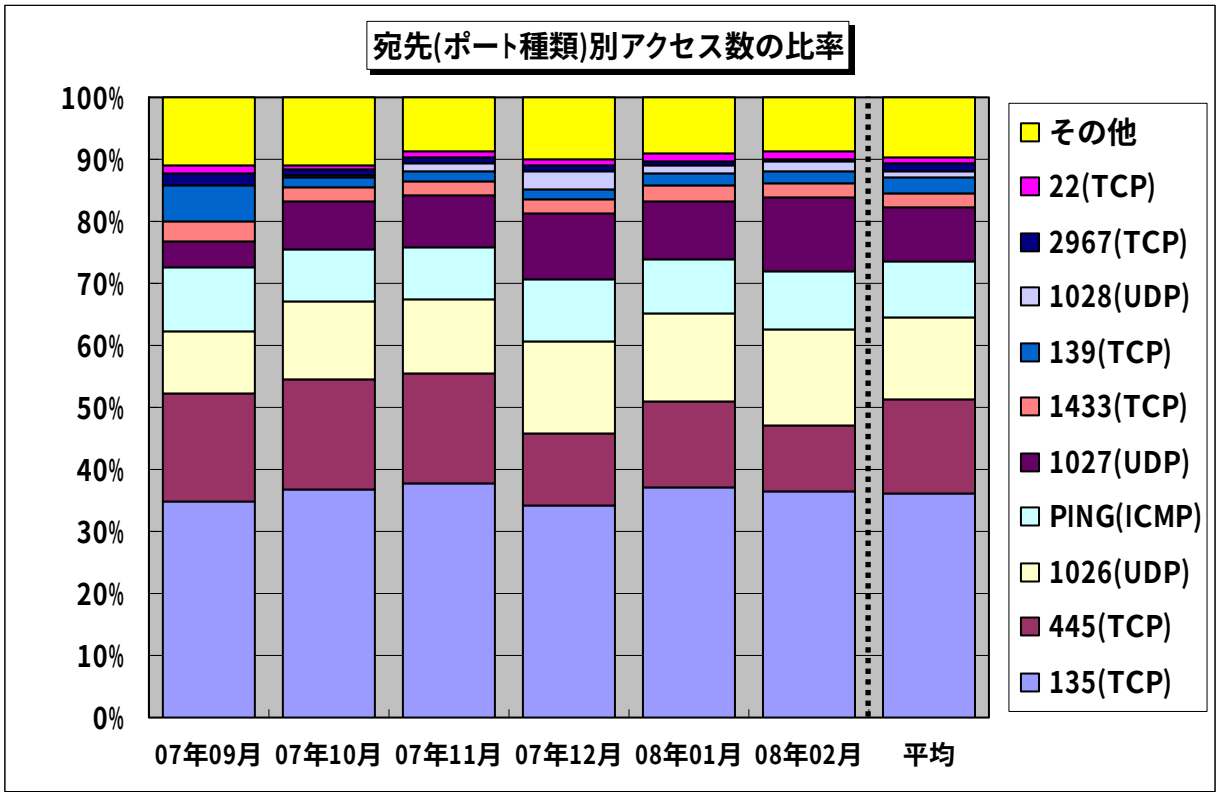


【図 2.4.4 2008 年 2 月の発信元地域別発信元数の比率】

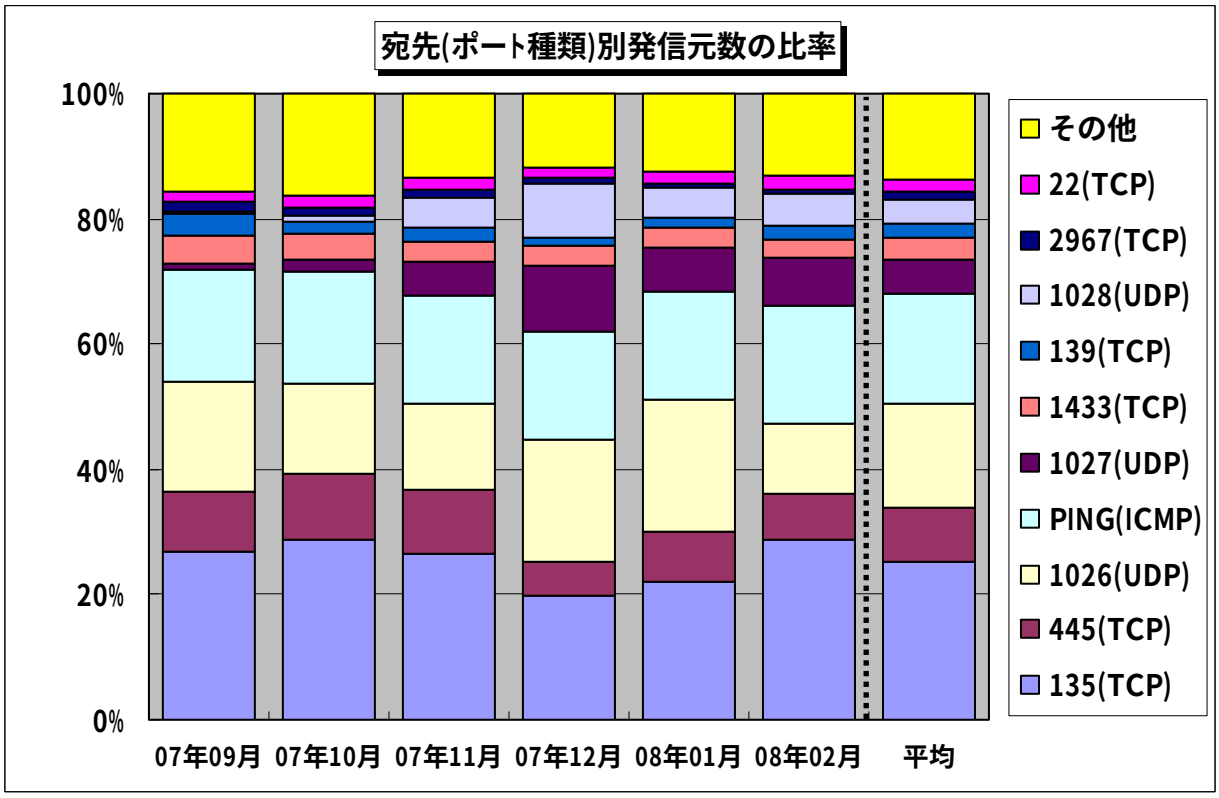
3．統計情報

3.1 2007 年 9 月～2008 年 2 月の宛先(ポート種類)別の比率

2007 年 9 月～2008 年 2 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。



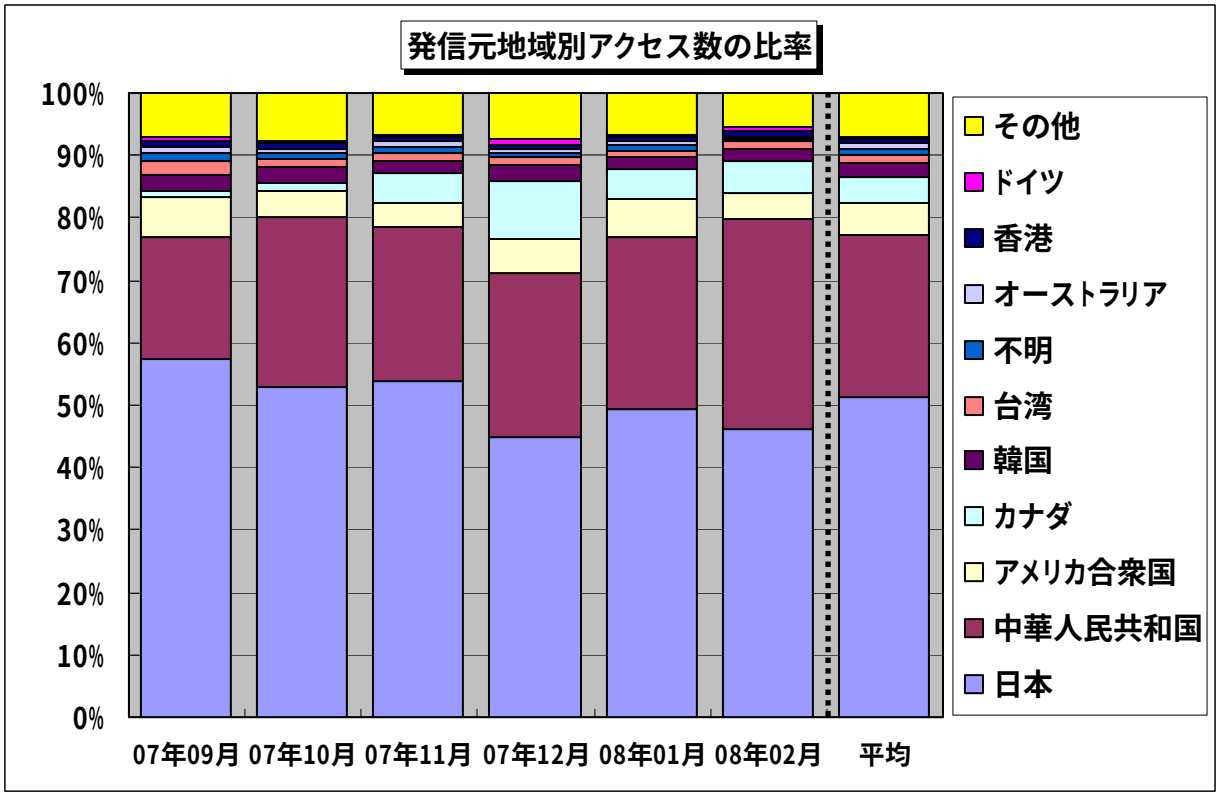
【図 3.1.1 2007 年 9 月～2008 年 2 月の宛先(ポート種類)別アクセス数の比率】



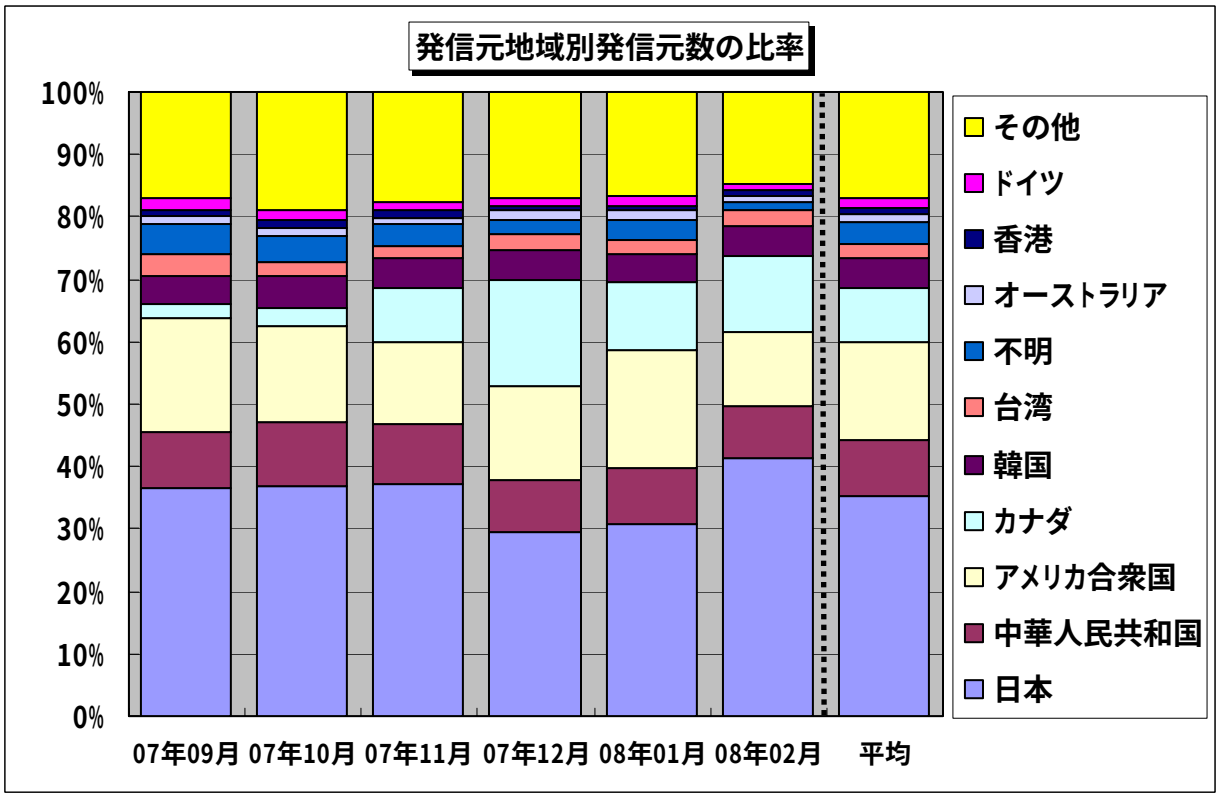
【図 3.1.2 2007 年 9 月～2008 年 2 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 9 月～2008 年 2 月の発信元地域別の比率

2007 年 9 月～2008 年 2 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 9 月～2008 年 2 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 9 月～2008 年 2 月の発信元地域別発信元数の比率】

4．補足説明

以下に、2008 年 2 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 に関する脆弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster など)
1026(UDP)/1027(UDP)/1028(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 特有の脆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 の脆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 の脆弱性を狙ったアクセスである可能性が高いです
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)
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