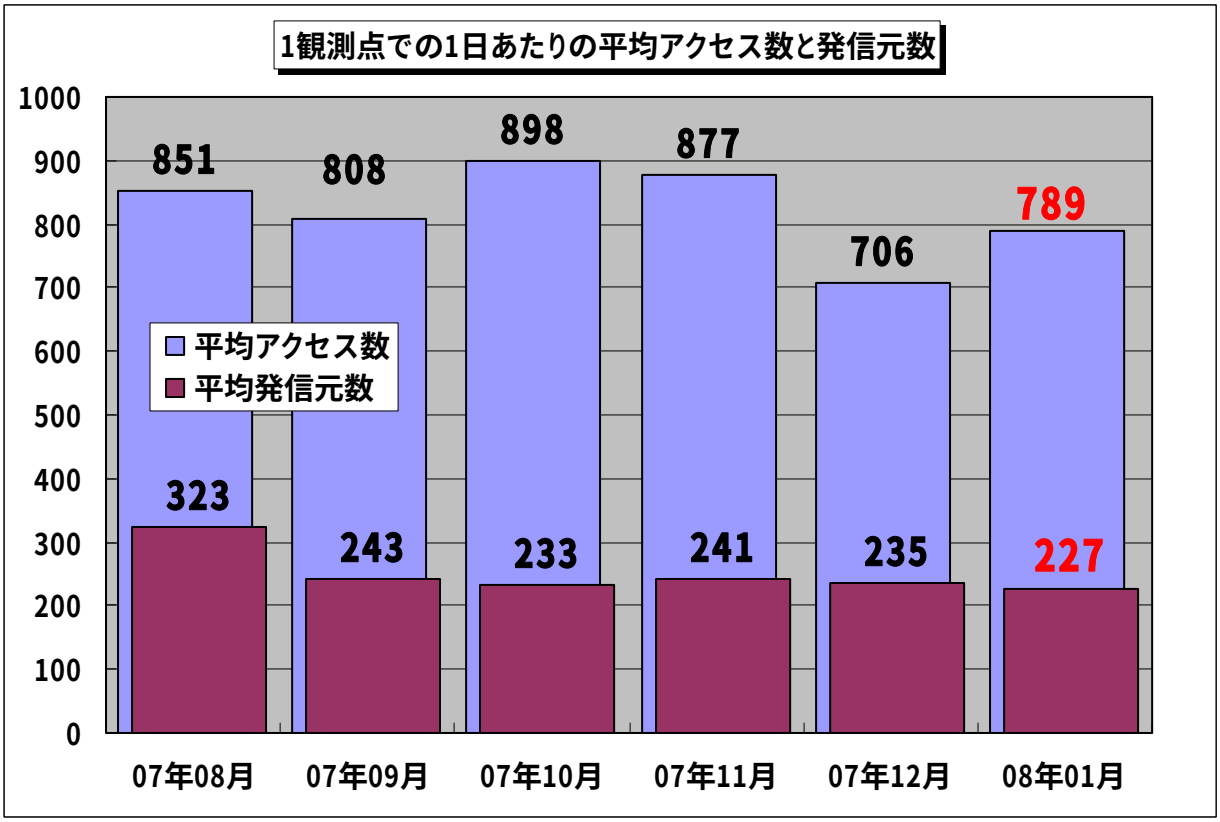
別紙 3

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 1 月の期待しない（一方的な）アクセスの総数は、10 観測点で **244,657 件**ありました。1 観測点で 1 日あたり **227** の発信元から **789 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、227 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 8 月～2008 年 1 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、1 月の期待しない（一方的な）アクセスは昨年 12 月よりも若干ですが増加しましたが、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。

2．1 月のアクセスの状況

2008 年 1 月のアクセス状況は、昨年 12 月よりも、若干ですが増加しました。これは、Windows のぜい弱性を狙っていると思われる、135/tcp のアクセスが増加したのが原因です。また、昨年 12 月にアクセスが多かった、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アクセスの内、1028/udp のアクセス（主な発信元地域はカナダ）が減少しました。

2.1. 135/tcp を狙ったアクセス

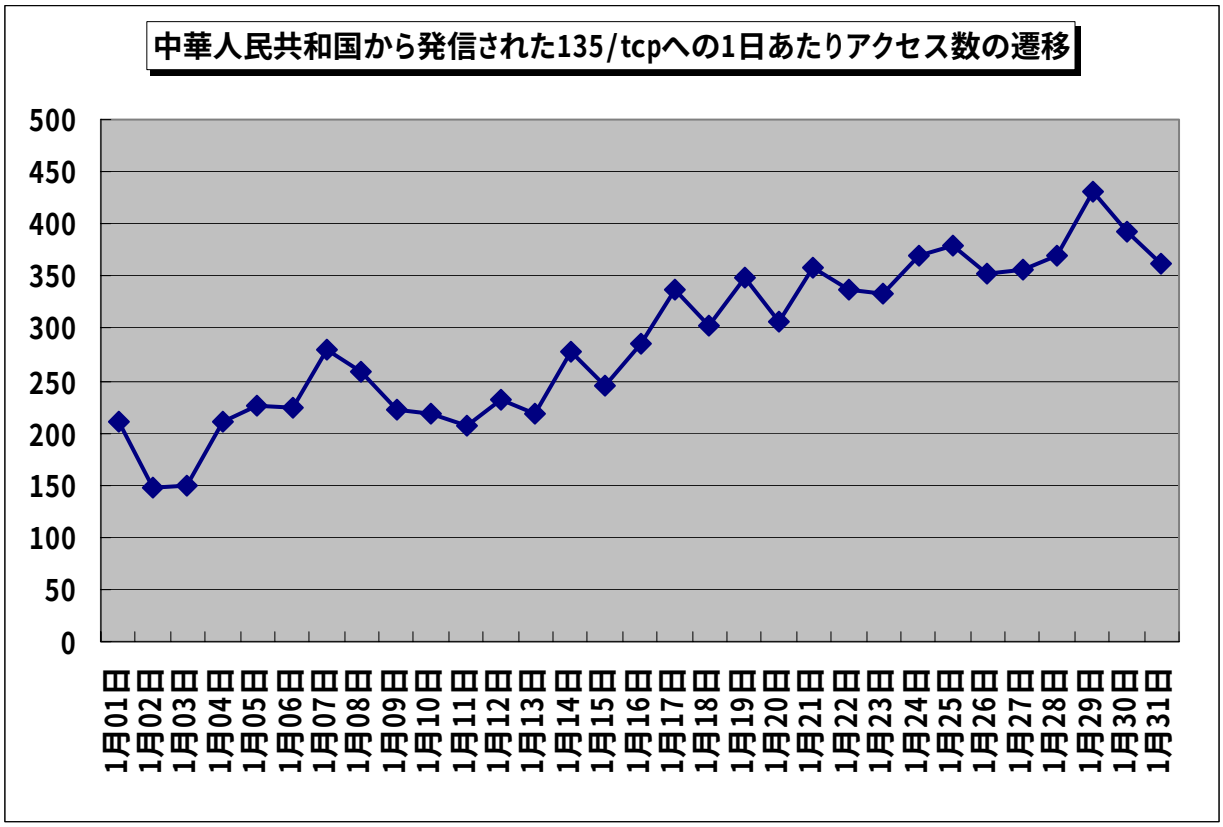
1 月は 135/tcp へのアクセスが増加しました。これは、Windows のぜい弱性を狙っていると思われるアクセスで、最近では、2007 年 10 月に Microsoft 社から MS07-058 のセキュリティ情報が公開されてから、主に日本を発信元地域とした、135/tcp へのアクセスが増加傾向にありました。

(参考情報)

■ 2007 年 10 月のインターネット定点観測 (TALOT2) での観測状況について
http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0711.pdf

■ Microsoft セキュリティ情報 (MS07-058) RPC の脆弱性により、サービス拒否が起こる (933729)
http://www.microsoft.com/japan/technet/security/bulletin/MS07-058.mspx

11 月、12 月は、135/tcp のアクセスは減少していましたが、1 月に入り、中華人民共和国を発信元地域としたアクセスが、少しずつですが増加しています (図 2.1.1 参照)。



【図 2.1.1 中華人民共和国から発信された 135/tcp への 1 日あたりアクセス数の遷移】

この様なアクセスは、主にボットウイルスからと思われます。今後増える可能性は十分ありますので、以下の資料を参考にしてもらい、ボット対策および不正アクセス対策を実施して下さい。

(参考情報)

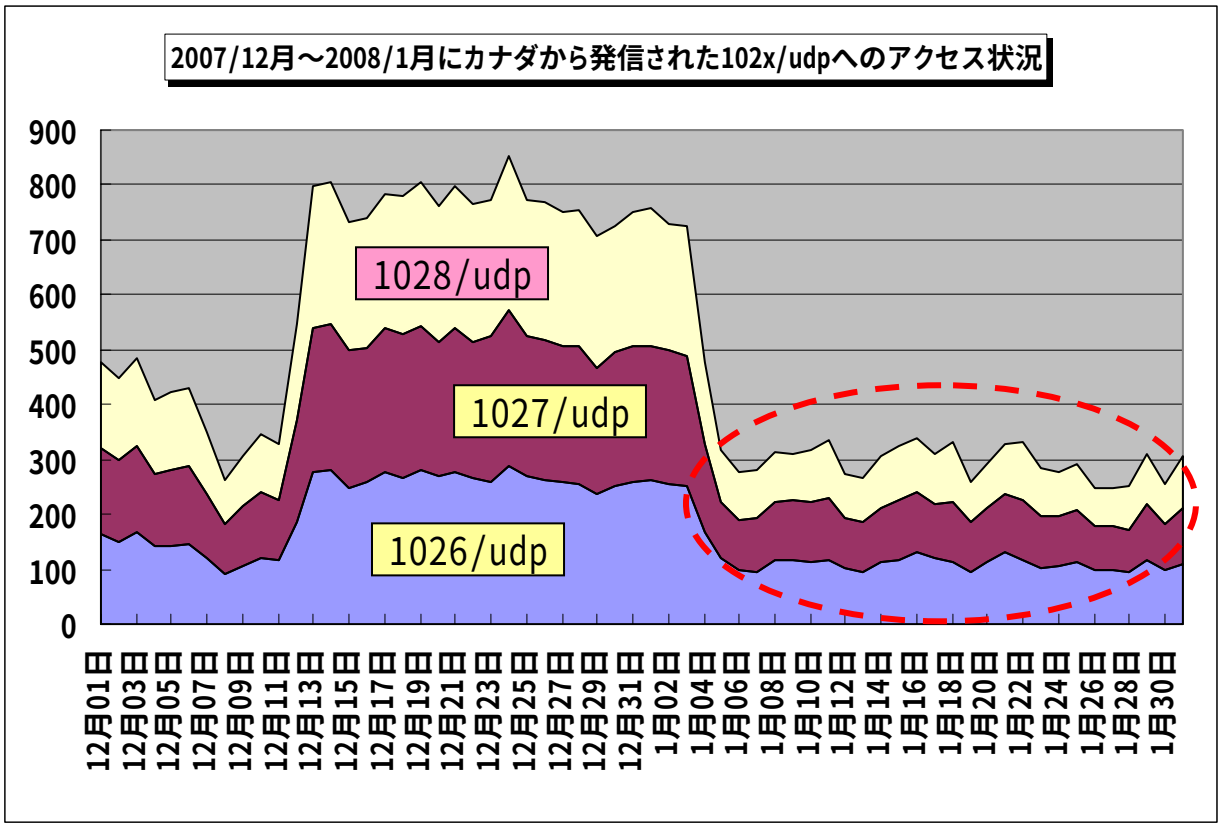
■ ボット対策のしおり／不正アクセス対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

■ 総務省･経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/

■ 感染防止のための知識 (サイバークリーンセンター)
https://www.ccc.go.jp/knowledge/

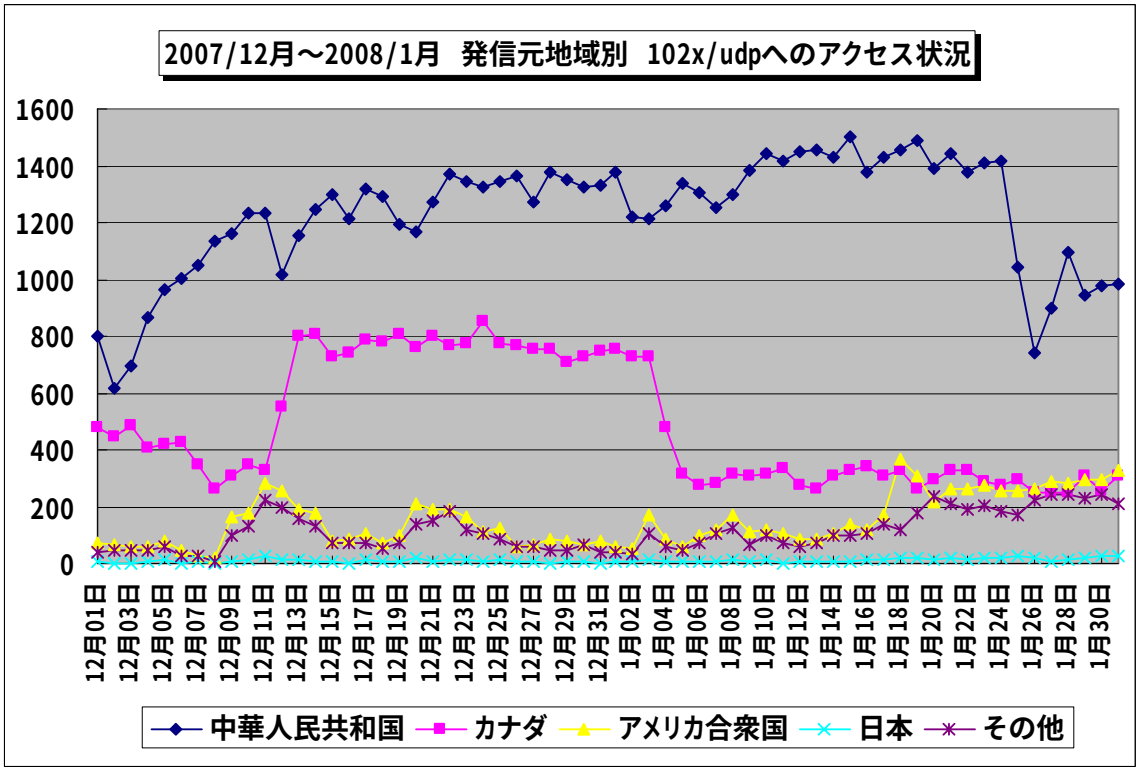
2.2. 1028/udp を狙ったアクセス

発信元地域がカナダからの、1028/udp へのアクセスが、1 月は昨年 12 月から比べて減少しました。併せて、発信元地域がカナダからの 1026/udp、1027/udp へのアクセスも減少しました。



【図 2.2.1　2007 年 12 月～2008 年 1 月にカナダから発信された 102x/udp へのアクセス状況】

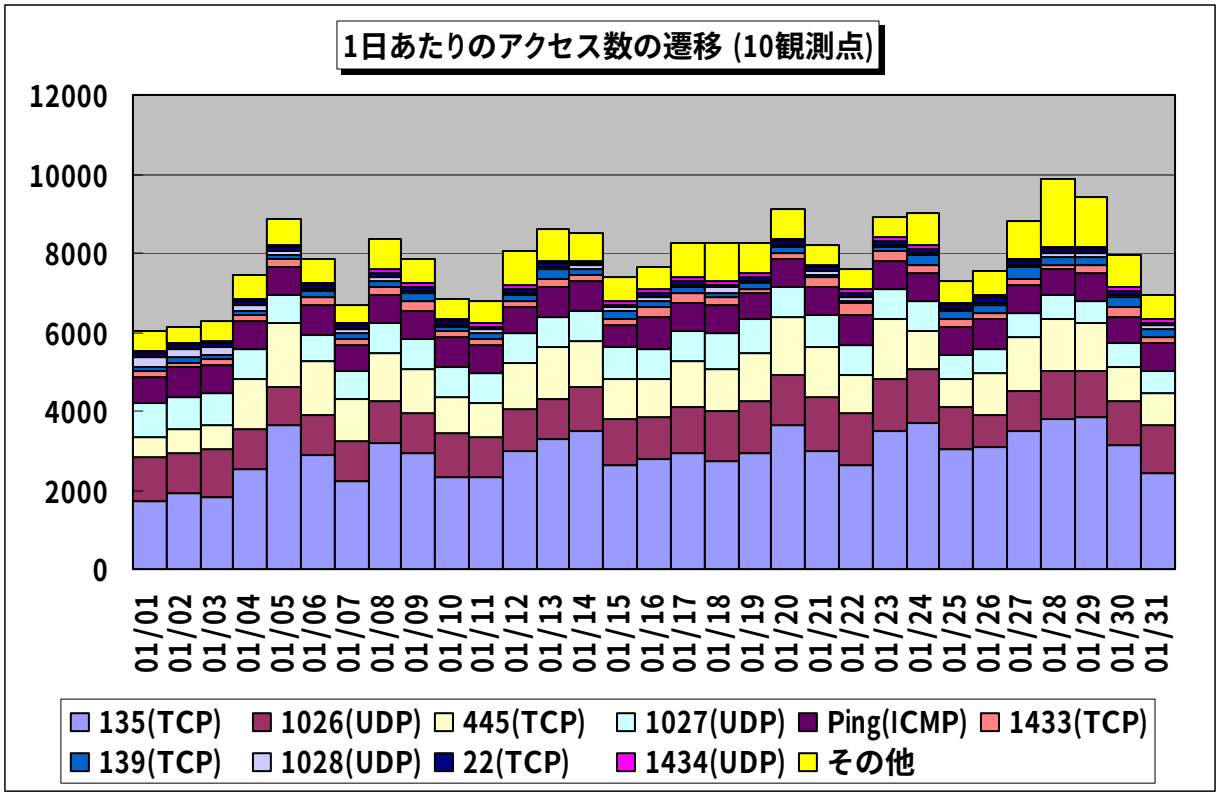
減少の理由は不明ですが 1 月の 102x/udp のアクセスは、発信元地域が中華人民共和国からのアクセスが増えましたので、102x/udp のアクセス数全体としては昨年 12 月と同水準でした。



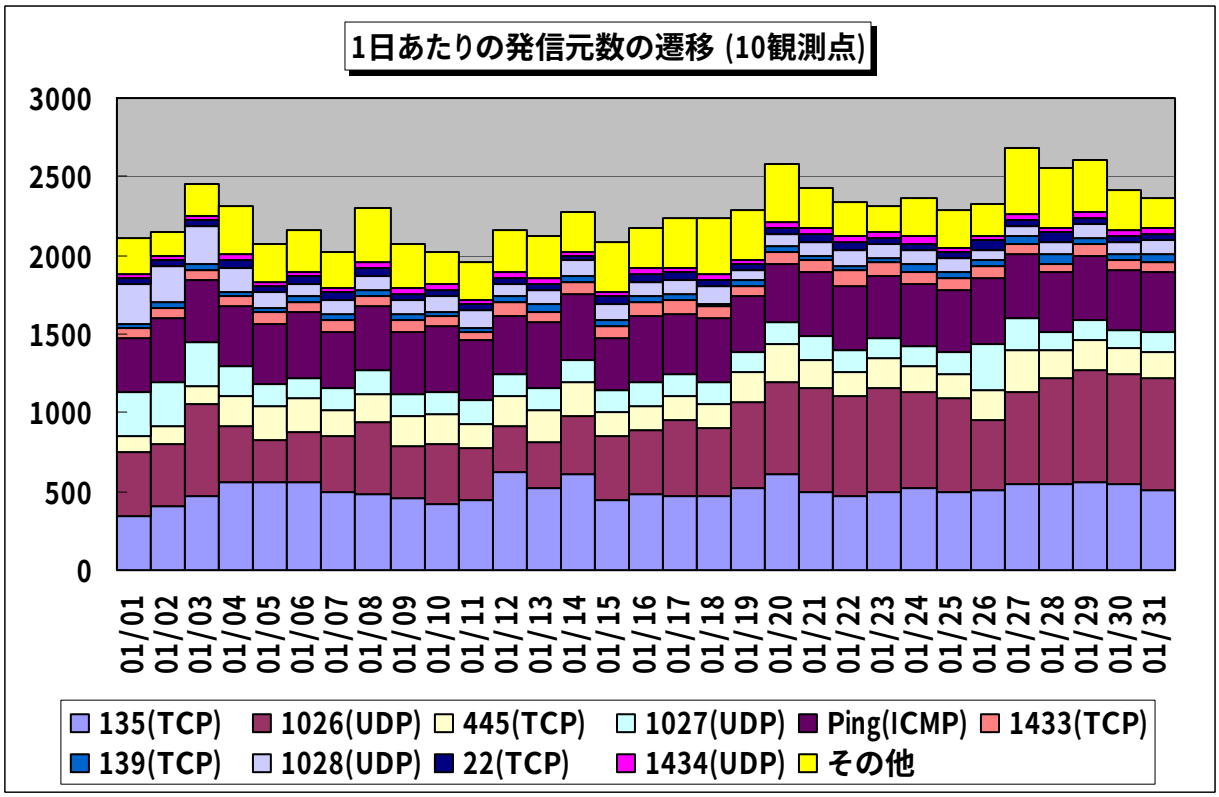
【図 2.2.2　2007 年 12 月～2008 年 1 月　発信元地域別 102x/udp へのアクセス状況】

2.3 2008 年 1 月の一方的なアクセス状況

2008 年 1 月の一方的なアクセス状況（アクセス数）の遷移を図 2.3.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.3.2 に示します。



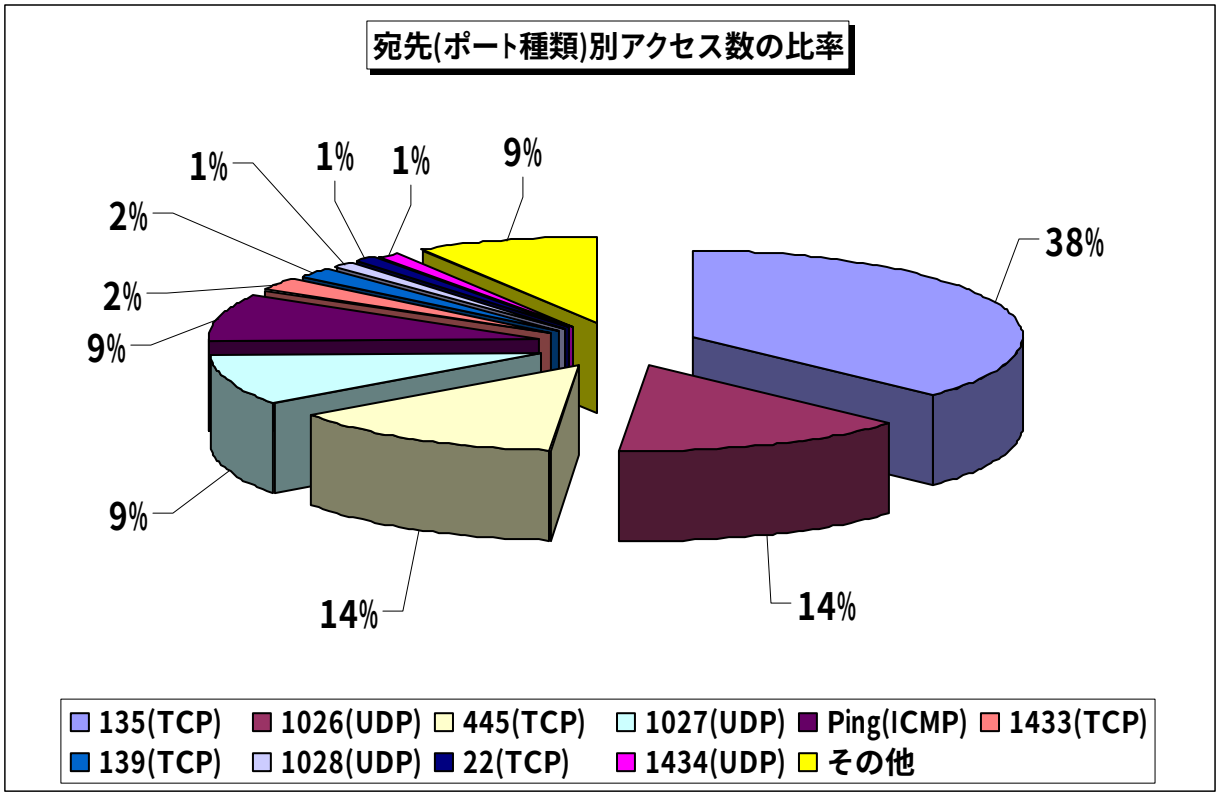
【図 2.3.1 2008 年 1 月の一方的なアクセス状況(アクセス数)】



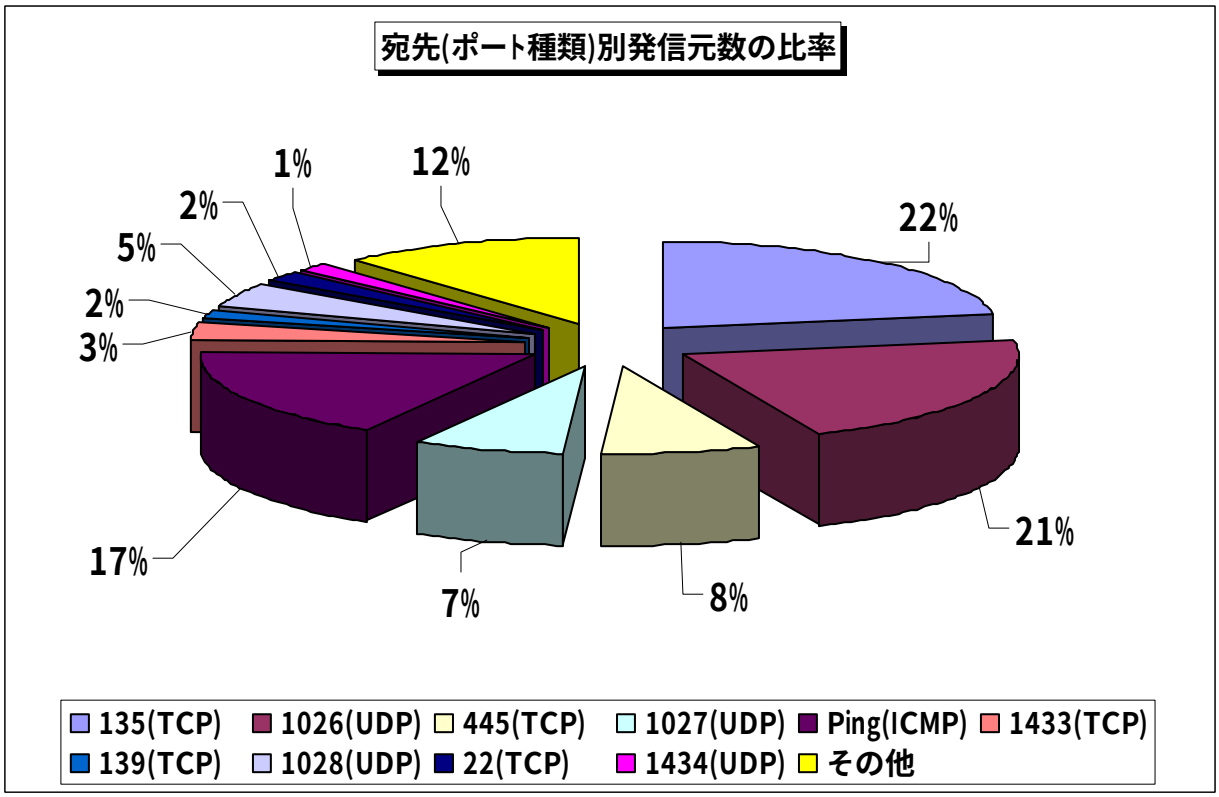
【図 2.3.2 2008 年 1 月の一方的なアクセス状況(発信元数)】

2.4 2008 年 1 月の宛先(ポート種類)別の比率

2008 年 1 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 2.4.1 に、宛先(ポート種類)別発信元数の比率を図 2.4.2 に示します。



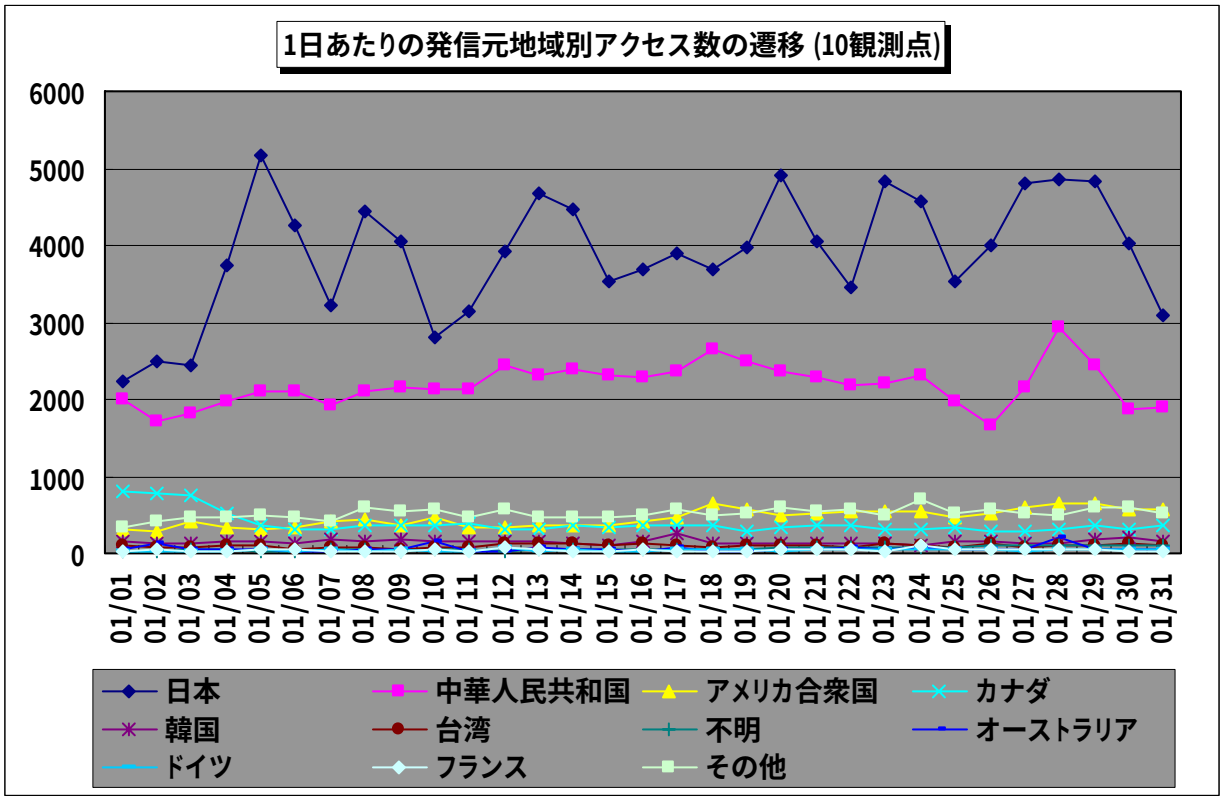
【図 2.4.1 2008 年 1 月の宛先(ポート種類)別アクセス数の比率】



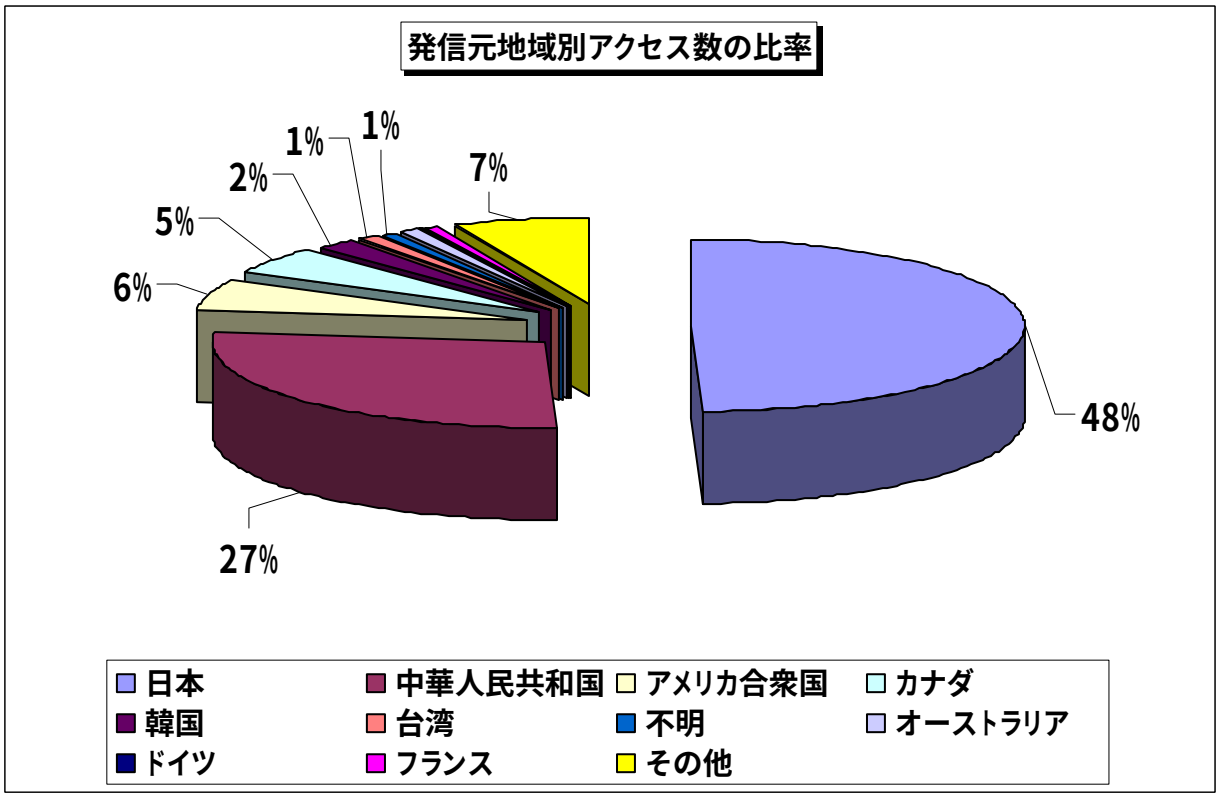
【図 2.4.2 2008 年 1 月の宛先(ポート種類)別発信元数の比率】

2.5 2008 年 1 月の発信元地域別アクセス状況

2008 年 1 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 2.5.1 に、発信元地域別アクセス数の比率を図 2.5.2 に示します。

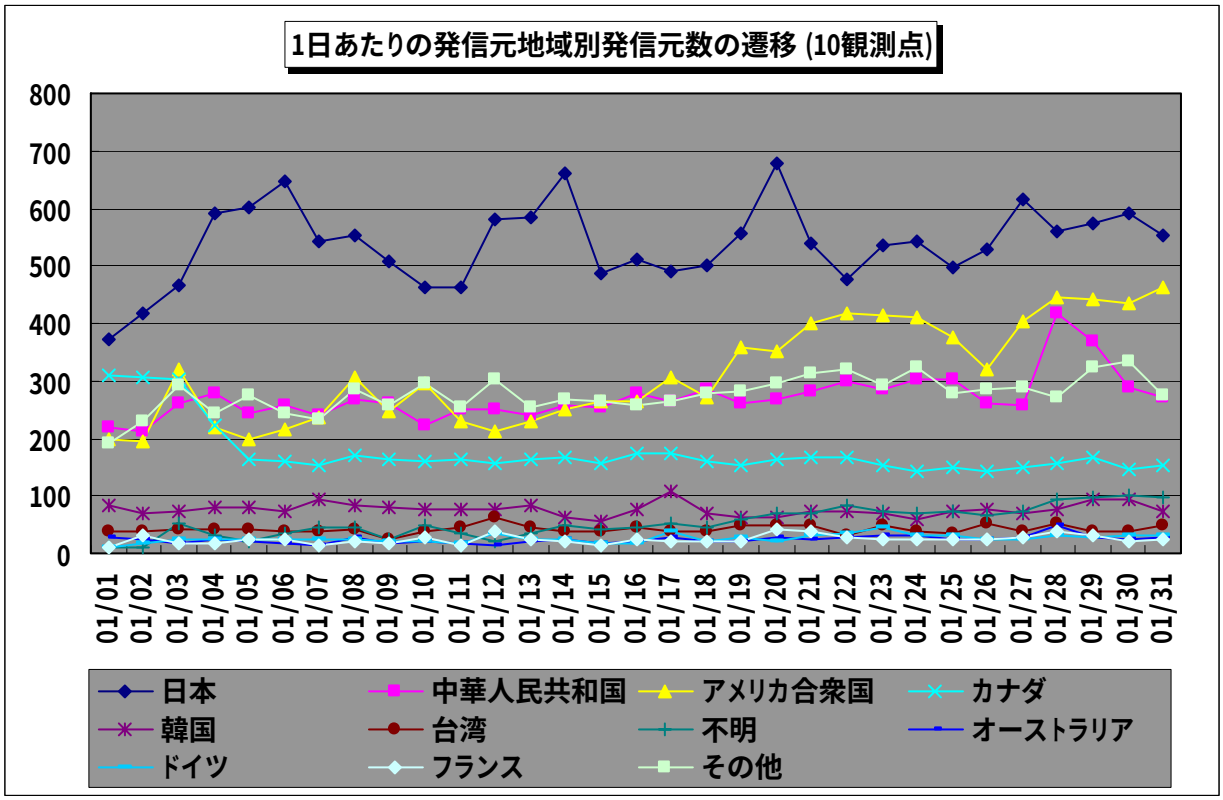


【図 2.5.1 2008 年 1 月の発信元地域別アクセス数の変化】

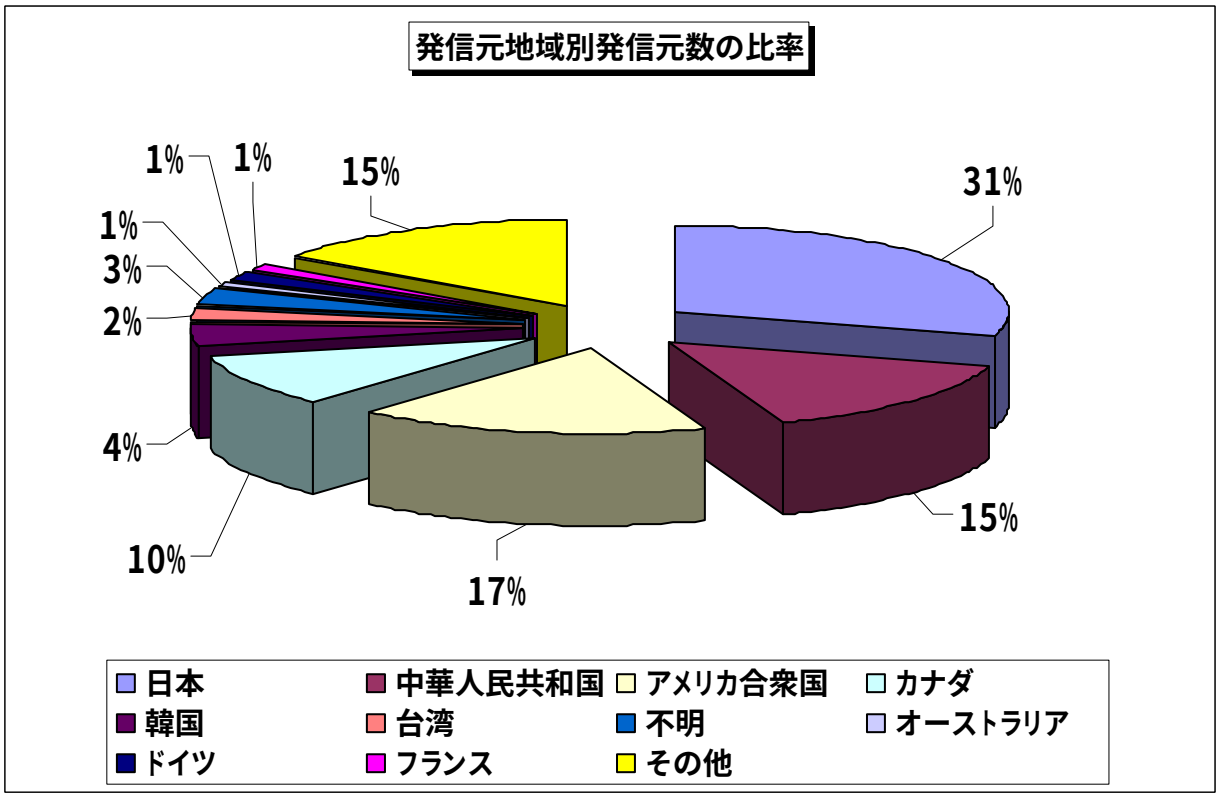


【図 2.5.2 2008 年 1 月の発信元地域別アクセス数の比率】

2008 年 1 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 2.5.3 に、発信元地域別発信元数の比率を図 2.5.4 に示します。



【図 2.5.3 2008 年 1 月の発信元地域別発信元数の変化】

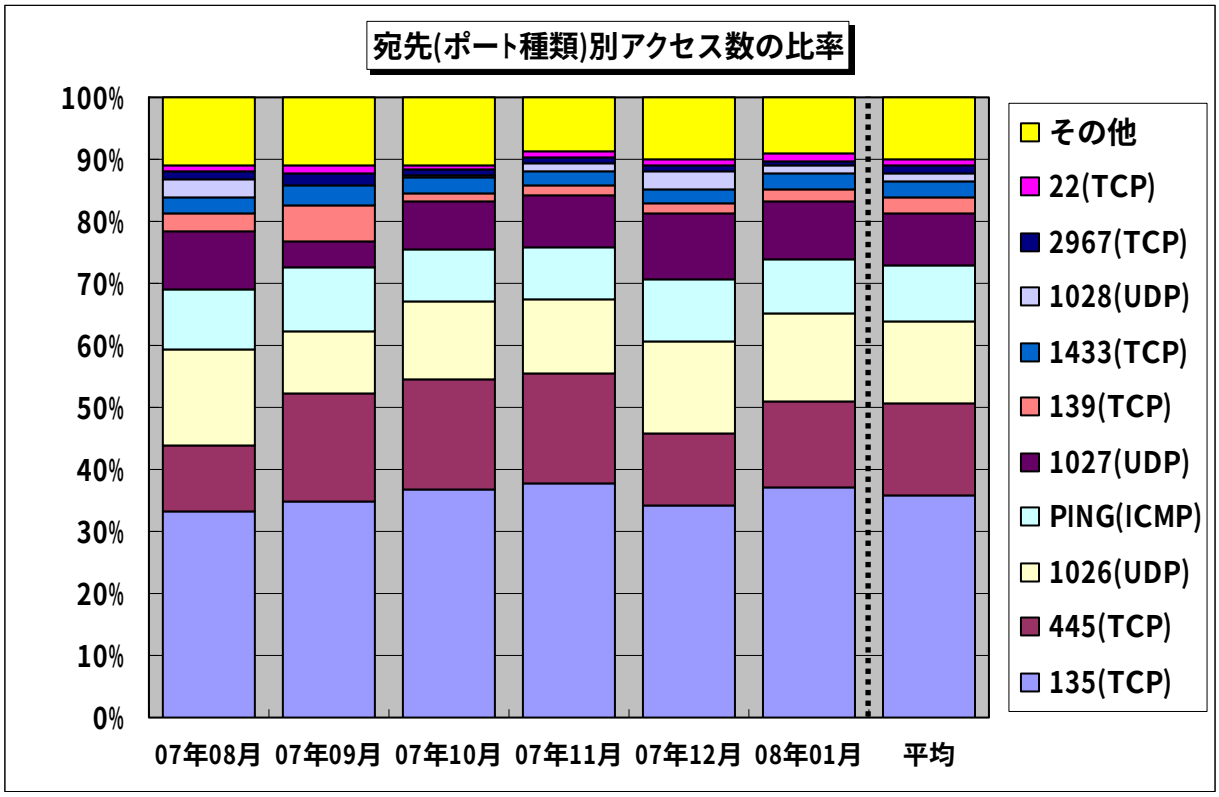


【図 2.5.4 2008 年 1 月の発信元地域別発信元数の比率】

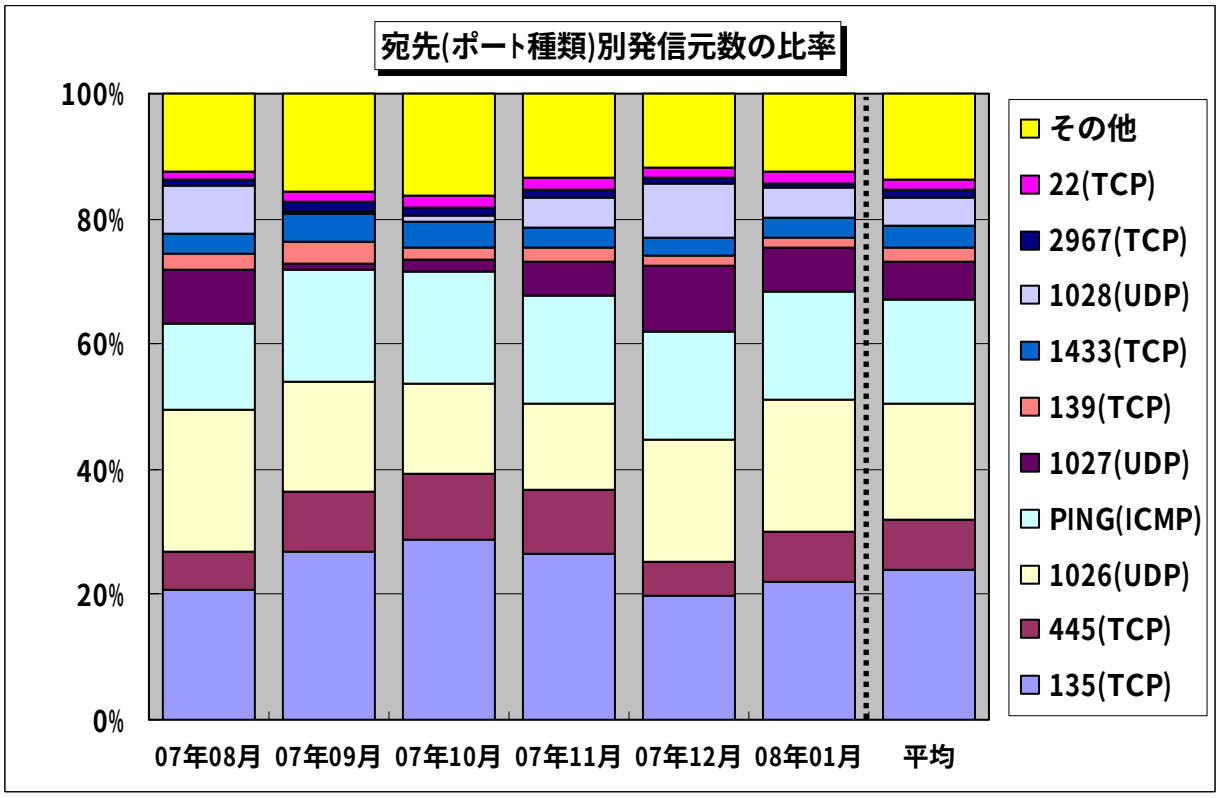
3．統計情報

3.1 2007 年 8 月～2008 年 1 月の宛先(ポート種類)別の比率

2007 年 8 月～2008 年 1 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。



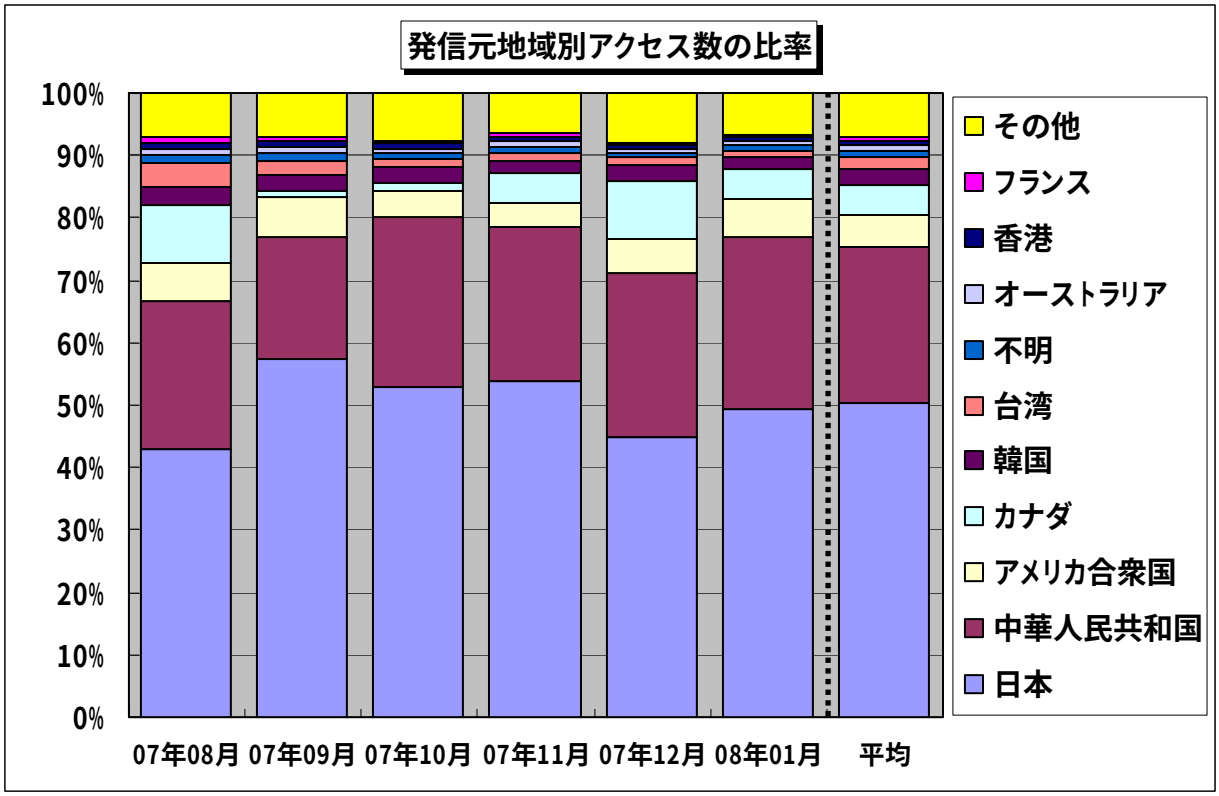
【図 3.1.1 2007 年 8 月～2008 年 1 月の宛先(ポート種類)別アクセス数の比率】



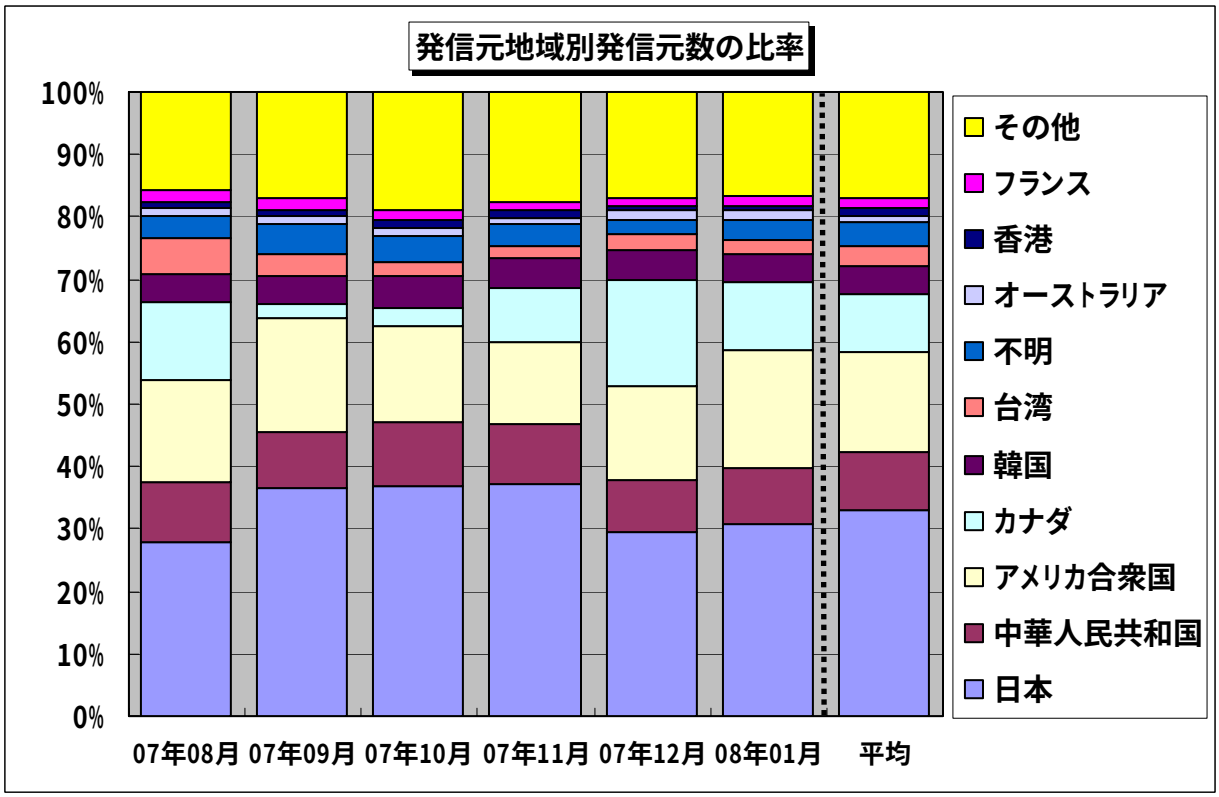
【図 3.1.2 2007 年 8 月～2008 年 1 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 8 月～2008 年 1 月の発信元地域別の比率

2007 年 8 月～2008 年 1 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 8 月～2008 年 1 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 8 月～2008 年 1 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 1 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)/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
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
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)

■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