別紙 3

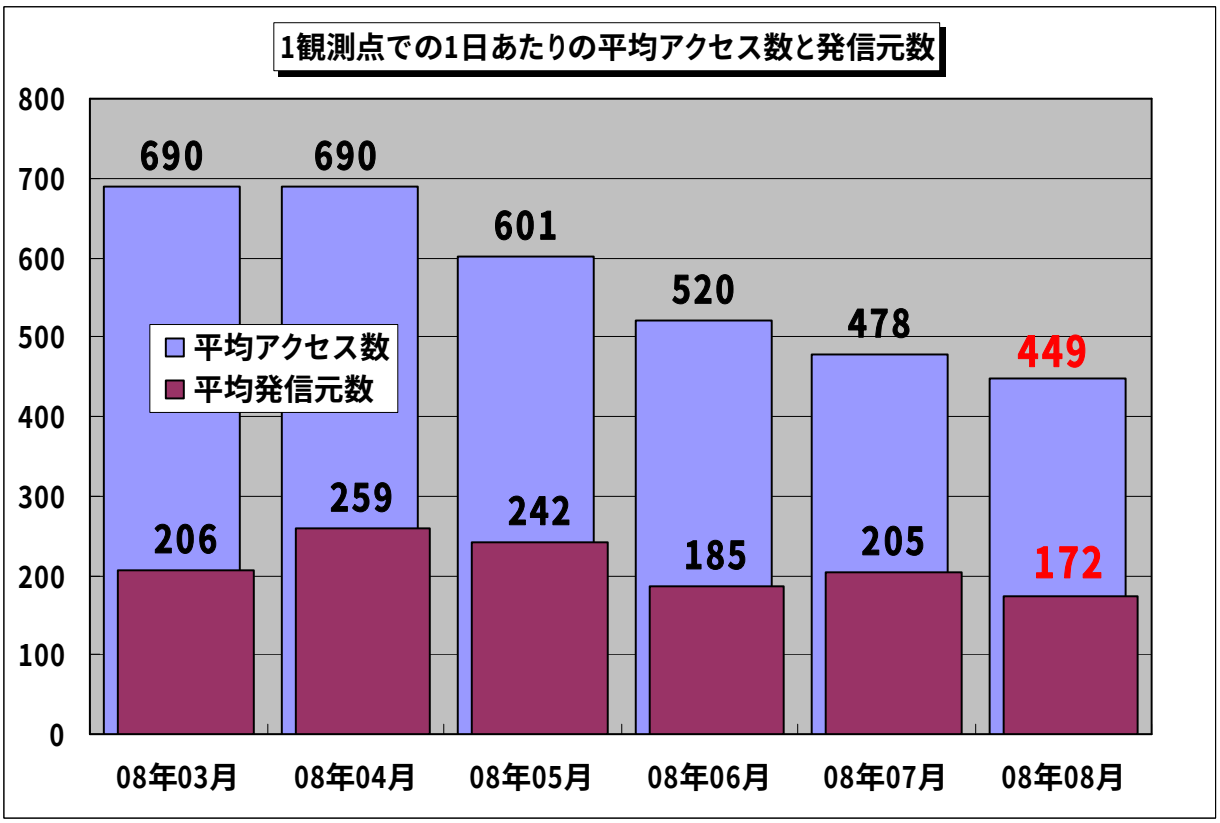
# インターネット定点観測(TALOT2)での観測状況について

## 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 8 月の期待しない（一方的な）アクセスの総数は 10 観測点で **139,174 件**、総発信元数(※)は **53,451 箇所**ありました。1 観測点で見ると、1 日あたり **172** の発信元から **449 件**のアクセスがあったことになります。

**総発信元数**（※）：TALOT2 にアクセスしてきた発信元の総数。なお、同一発信元から同一観測日・観測点・ポートにアクセスがあった場合は 1 つの発信元としてカウント。

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、172 人の見知らぬ人(発信元)から、それぞれ約 3 件ずつ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】

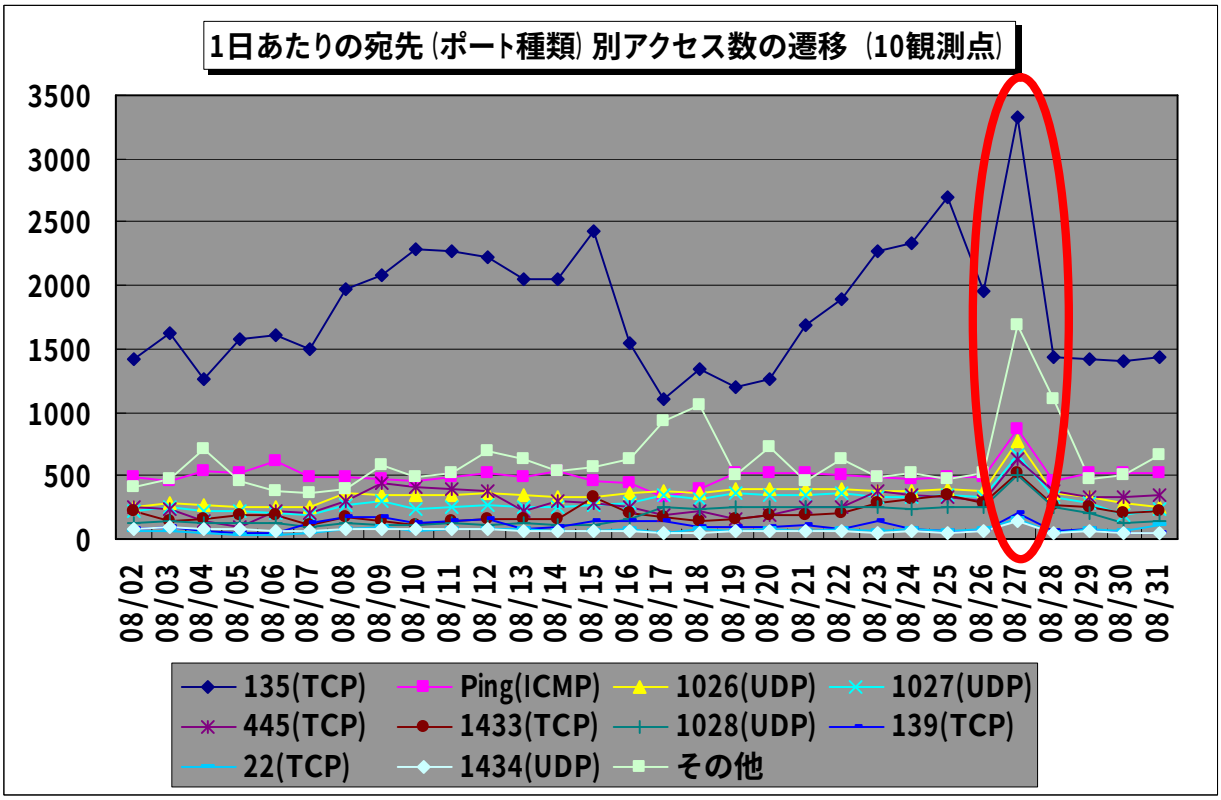
2008 年 3 月～2008 年 8 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、8 月の期待しない（一方的な）アクセスは 7 月と比べて若干減少しており、過去 6 ヶ月間を通してみても、減少傾向を示していると言えます。

## 2．8 月のアクセスの状況

2008 年 8 月のアクセス状況は、7 月と比べて若干減少しました。これは、主に Windows Messenger サービスを利用したポップアップ(スパム)メッセージを送信するアクセスである 1026/udp および 1027/udp へのアクセスが全体的に減少したためです。逆に先月よりアクセスが増加しているものは、Windows の脆弱性（ぜいじゃくせい）を狙っていると考えられている 135/tcp へのアクセスでした。その他のポートへのアクセス数については大きな変化はありませんでした。

## 2.1 135/tcp へのアクセス

8 月 27 日に一時的にアクセスの増加を観測しました。これは、Windows の脆弱性を狙った 135/tcp へのアクセスが増加したためです。この日の 135/tcp へのアクセスの発信元数の約 6 割が日本、約 3 割が中華人民共和国でした。この日は、135/tcp 以外のポートへのアクセスも 8 月の他の日に比べ若干増加していました。これらのアクセスが一時的に増加した原因は不明です。（図 2.1.1 参照）



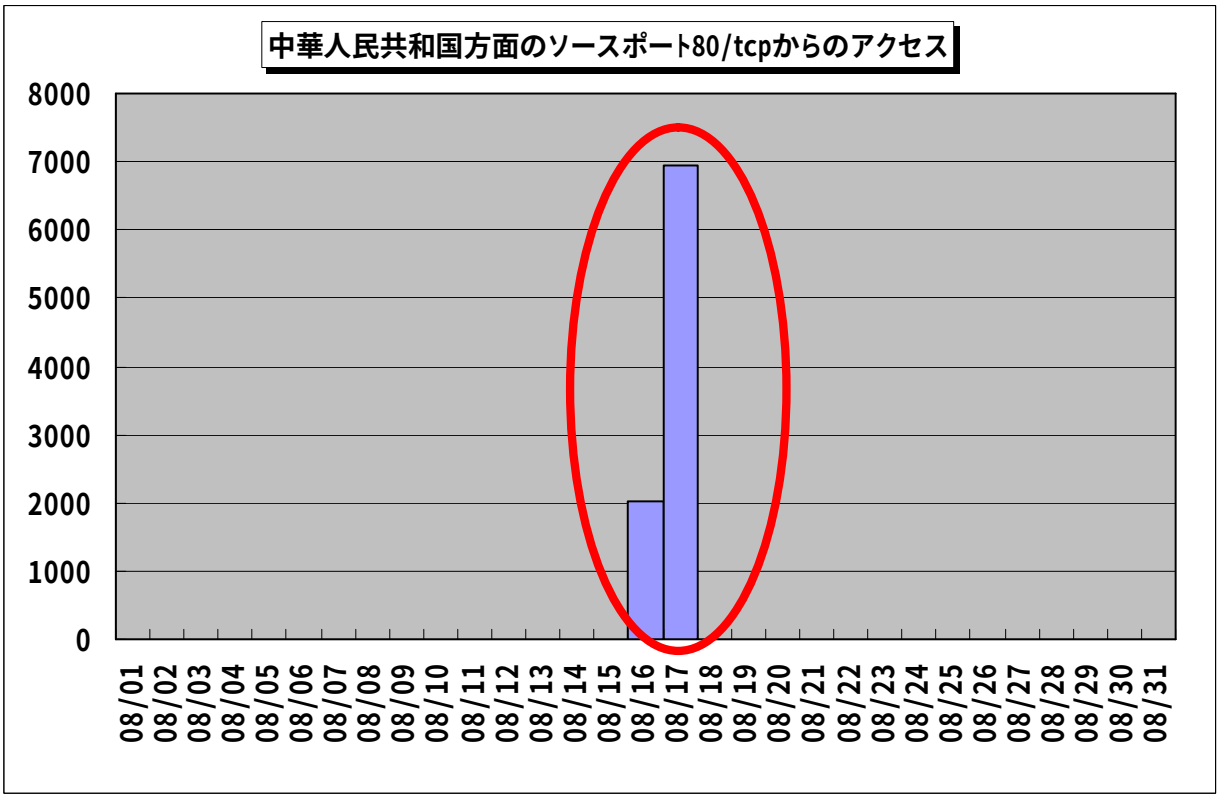

【図 2.1.1 2008 年 8 月のポート別アクセス状況】

また、8 月 16 日、17 日に中華人民共和国の特定の通信事業者を狙った DoS 攻撃（SYN Flood 攻撃）[*1] の影響と思われるアクセスが観測されました。これらのアクセスは全て同一発信元の 80/tcp ポートからの SYN＋ACK パケットでした。

TALOT2で使用しているアドレスが、攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN+ACK パケットが大量に届いたということです。

この攻撃が行われたのが、北京オリンピック期間中であったことから、何らかの北京オリンピックに便乗した攻撃であった可能性が高いと思われます。（図 2.1.2 参照）

注：このアクセスは TALOT2 への直接的な攻撃（アクセス）ではない為、集計からは除外しています。




【図 2.1.2 中華人民共和国方面への SYN Flood 攻撃のバックスキャッタ(*3)】

今回は 8 月中に観測された DoS 攻撃 (SYN Flood 攻撃) の影響と思われるアクセスのうち、最も規模の大きいものを取り上げましたが、これ以外にも数箇所で観測しています。このような攻撃は、攻撃先のみならず、発信元 IP アドレスとして詐称された利用者にとっても、迷惑なアクセスです。いかなる理由があるにせよ、このような行為は行うべきではありません。

(*1):DoS 攻撃 (SYN Flood 攻撃)

「サービス妨害攻撃」Denial of Service の略からＤｏＳ攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。このＤｏＳ攻撃の1つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット(3 ウェイ・ハンドシェーク(*2)での接続確立の最初に送られるパケット)を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下に A と B の通信確立の手順を示します。

①A から B へ SYN パケットの送信

②B から A へ ACK+SYN パケットの送信

③A から B へ ACK パケットの送信

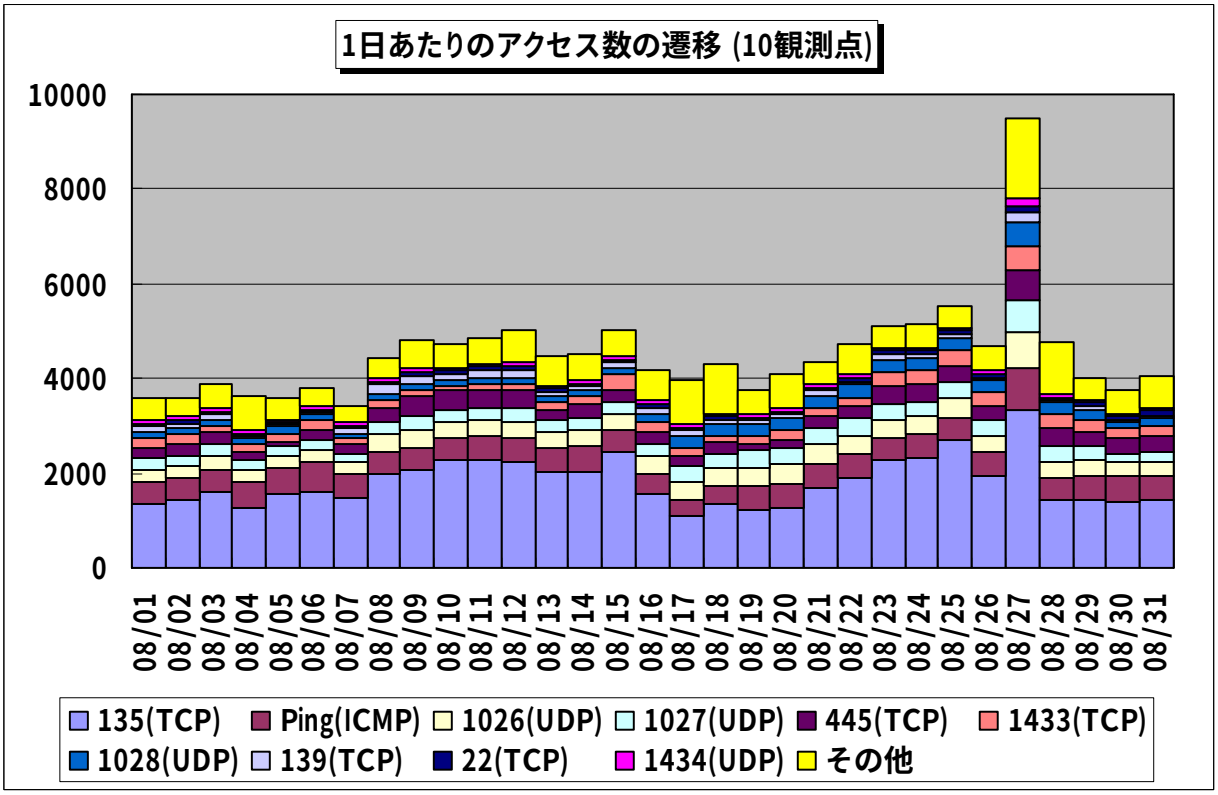
これで、AB 双方の通信が確立されます。

(*3):バックスキャッタ

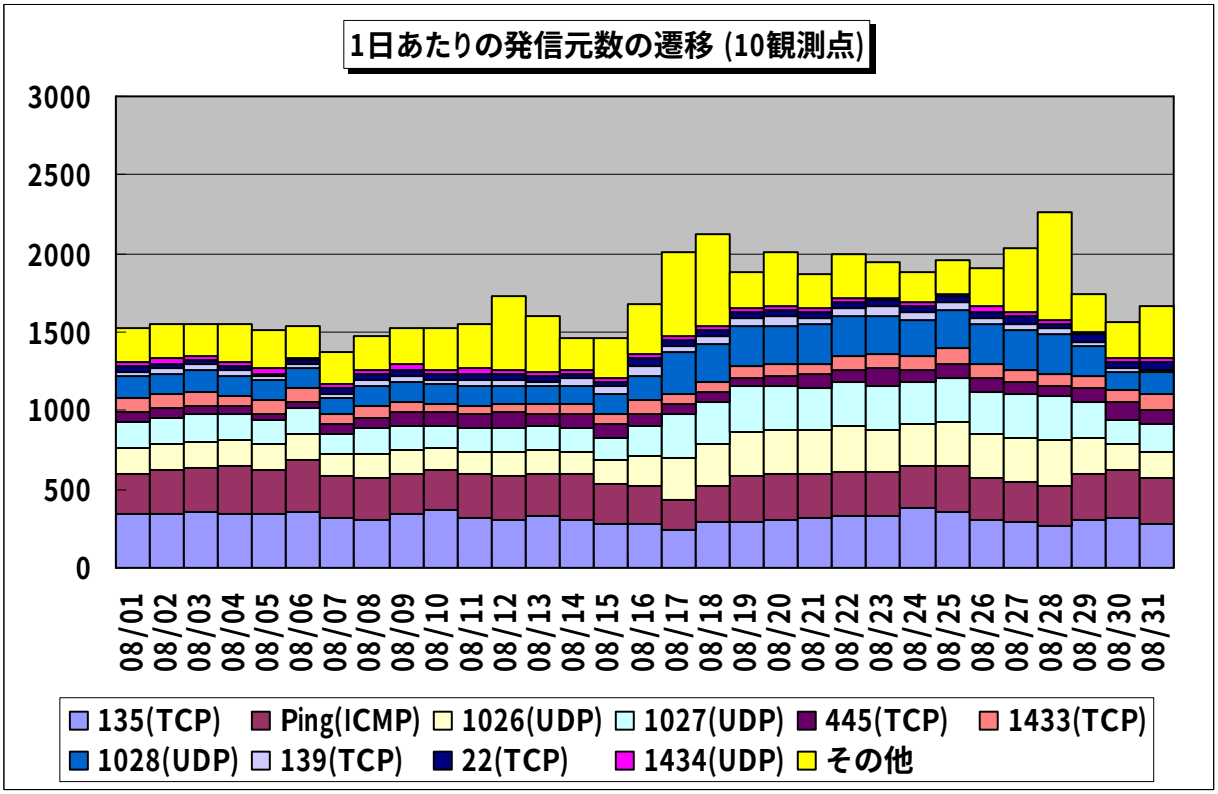
DoS 攻撃 (SYN Flood 攻撃) において攻撃者が詐称した発信元アドレスに、標的マシンから大量の SYN+ACK パケットが返信されてくることです。

## 2.2 2008 年 8 月の一方的なアクセス状況

2008 年 8 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 2.1.2 に示します。



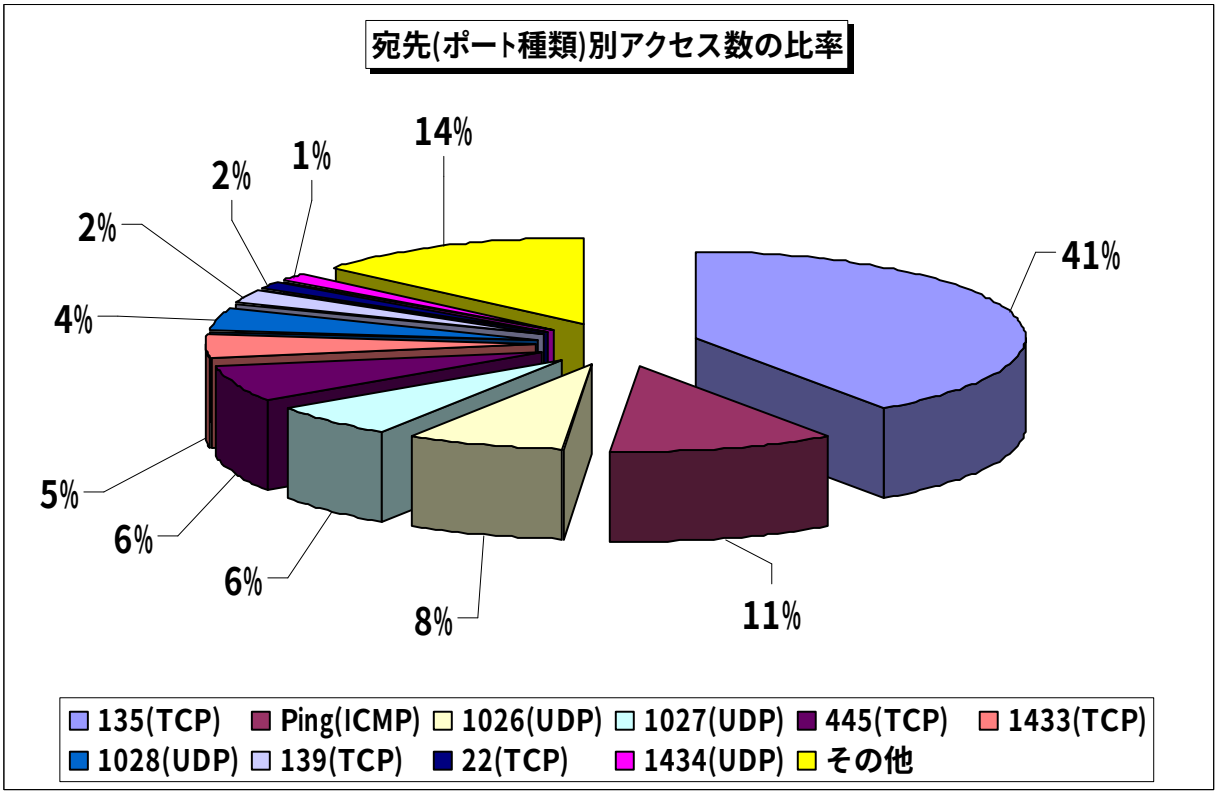

【図 2.2.1 2008 年 8 月の一方的なアクセス状況(アクセス数)】



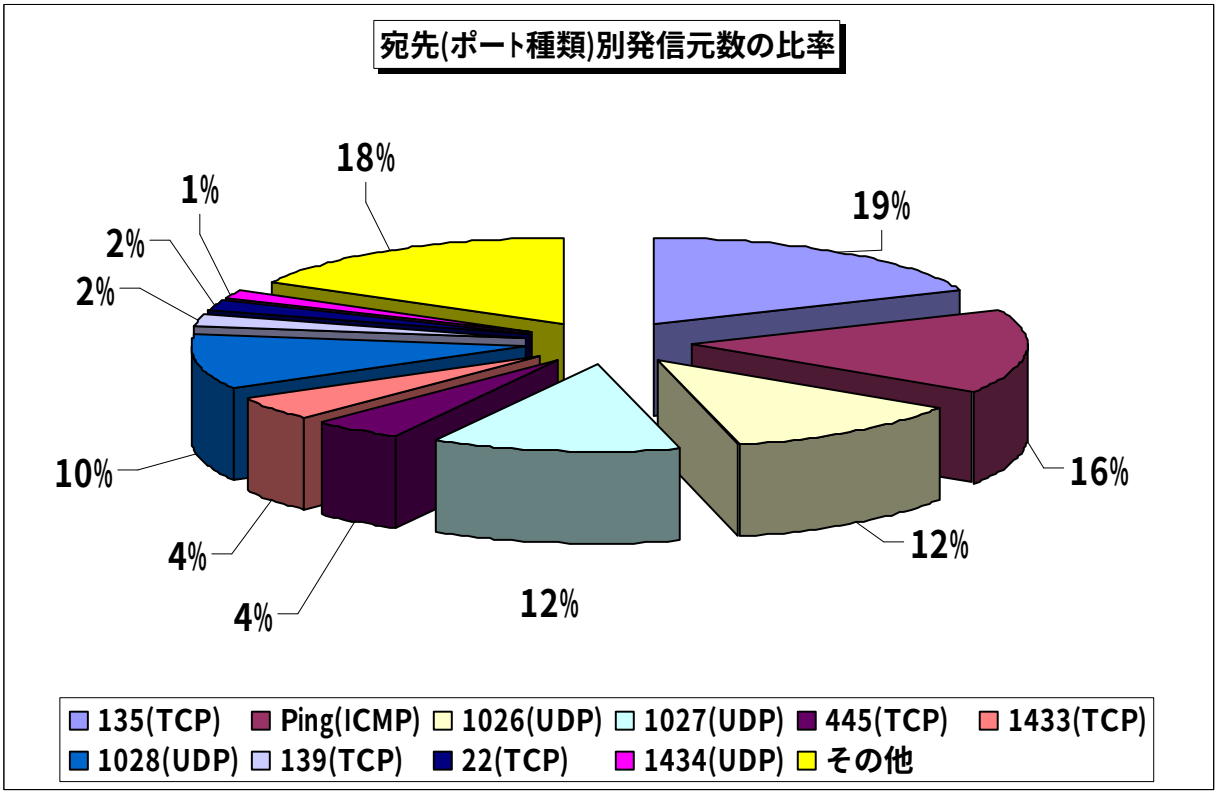

【図 2.2.2 2008 年 8 月の一方的なアクセス状況(発信元数)】

## 2.3 2008 年 8 月の宛先(ポート種類)別の比率

2008 年 8 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。



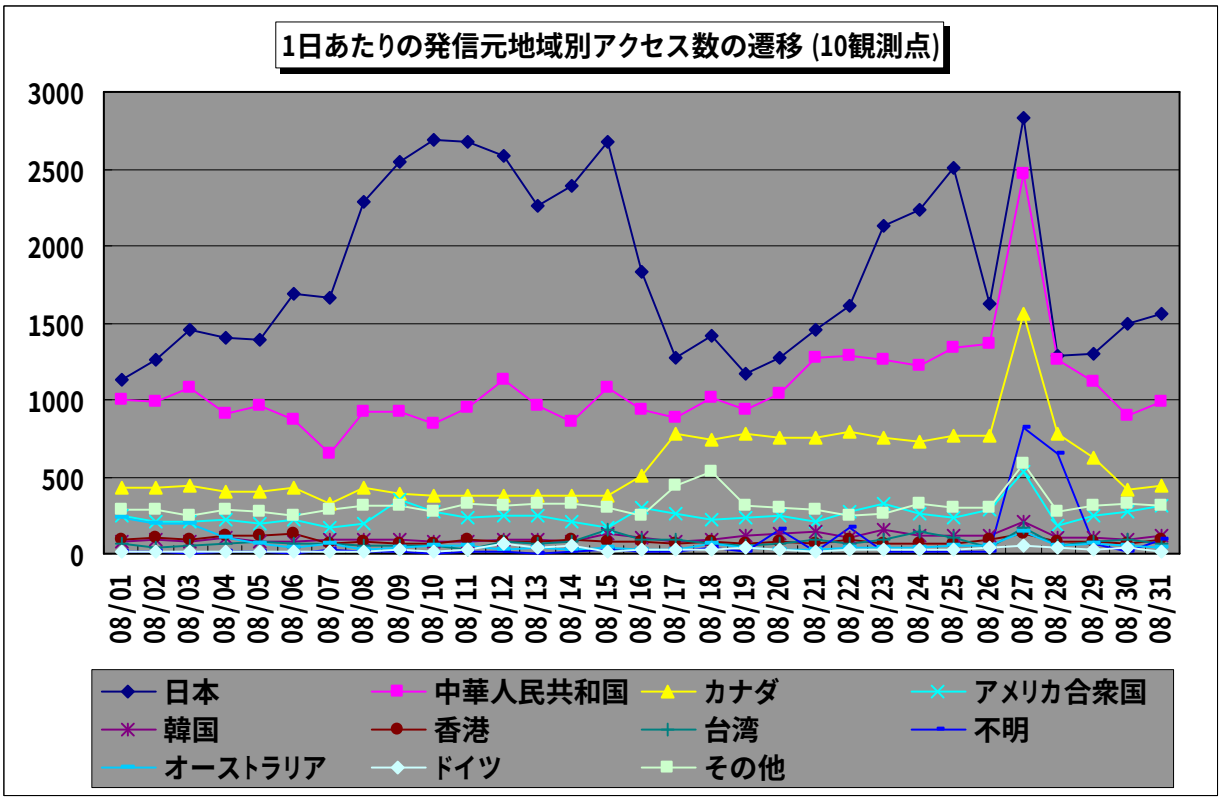

【図 2.3.1 2008 年 8 月の宛先(ポート種類)別アクセス数の比率】



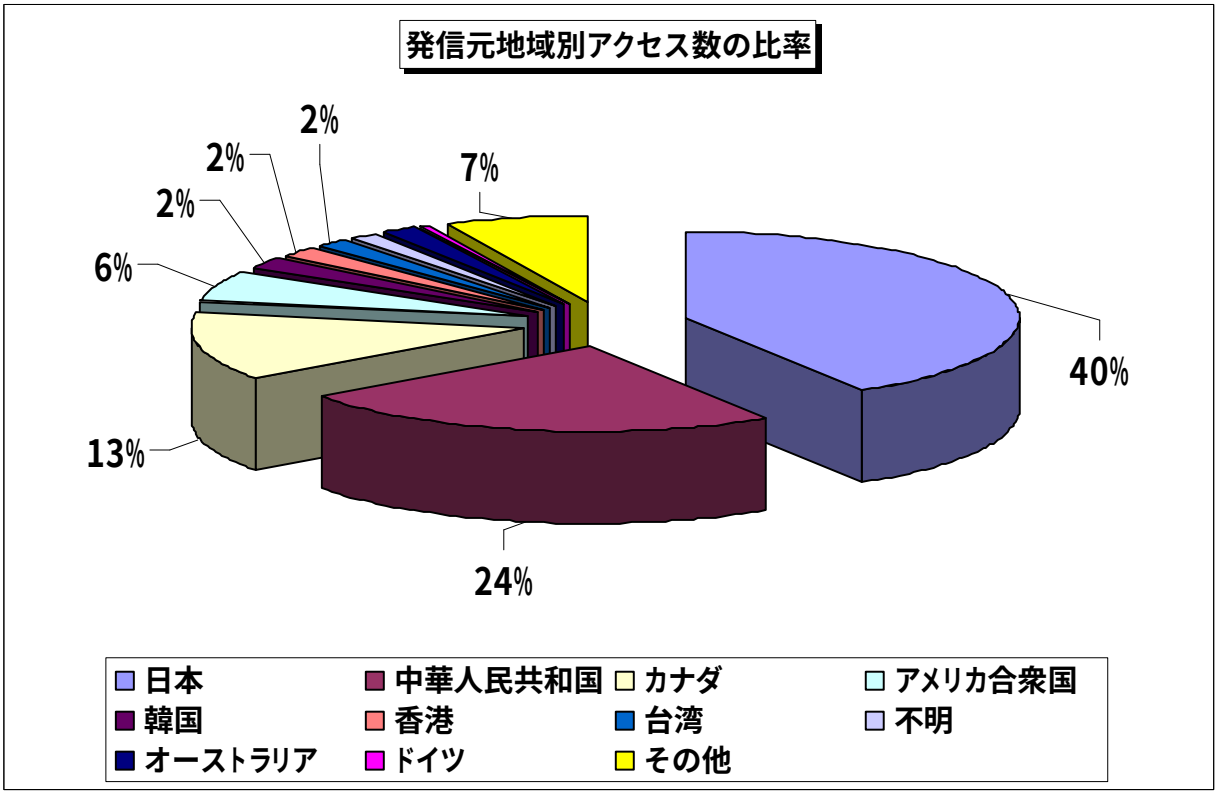

【図 2.3.2 2008 年 8 月の宛先(ポート種類)別発信元数の比率】

## 2.4 2008 年 8 月の発信元地域別アクセス状況

2008 年 8 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。

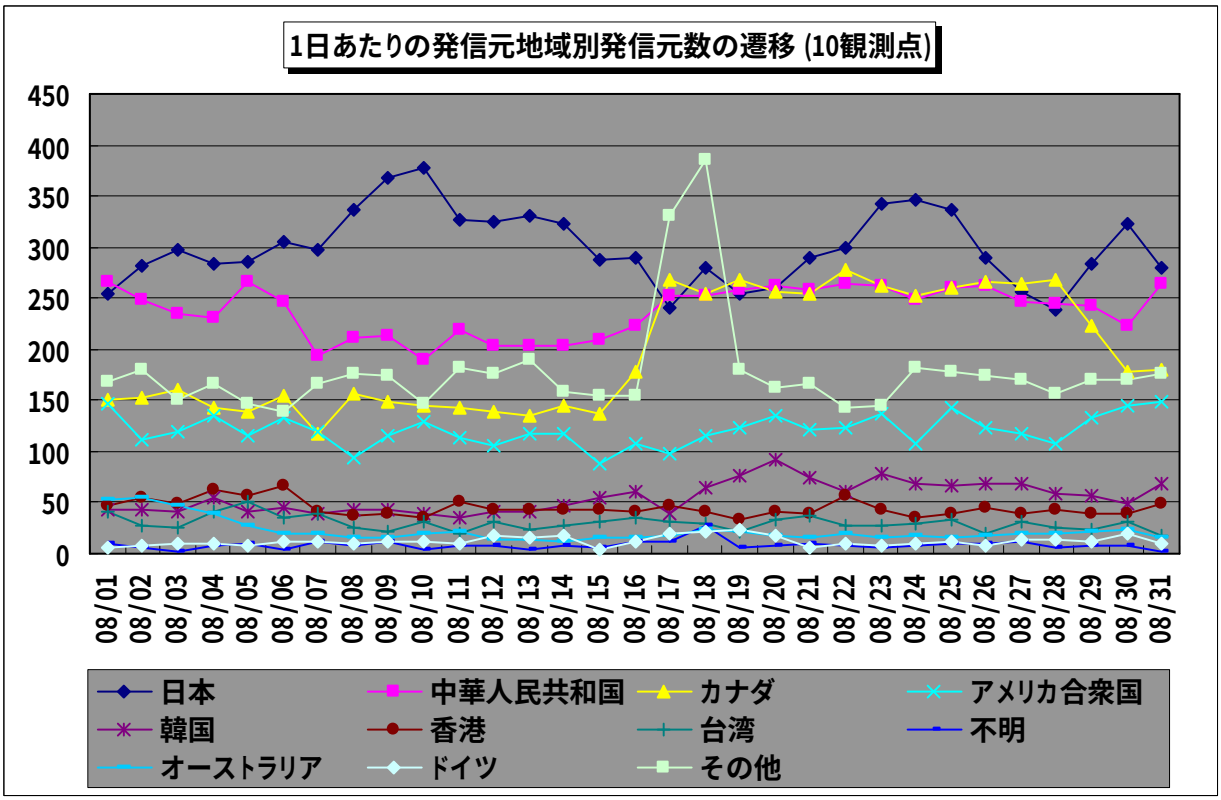



【図 2.4.1 2008 年 8 月の発信元地域別アクセス数の変化】

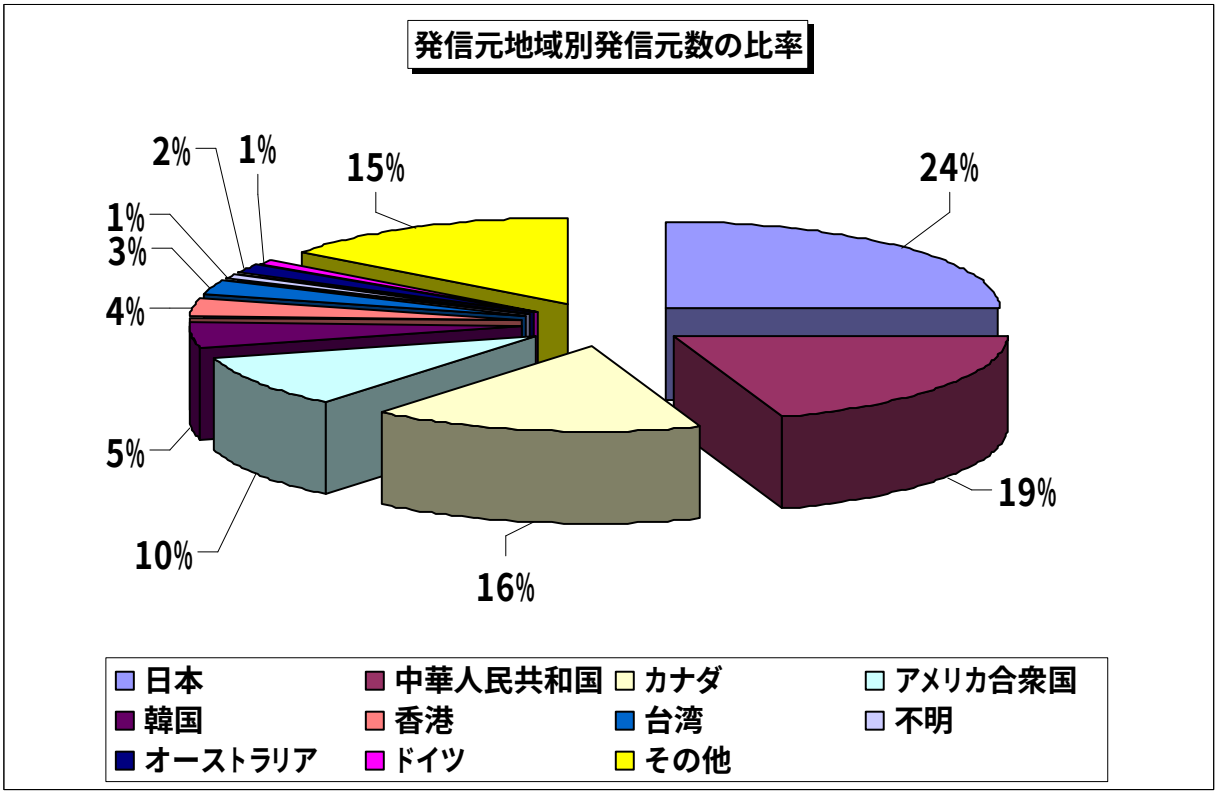



【図 2.4.2 2008 年 8 月の発信元地域別アクセス数の比率】

2008 年 8 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 8 月の発信元地域別発信元数の変化】

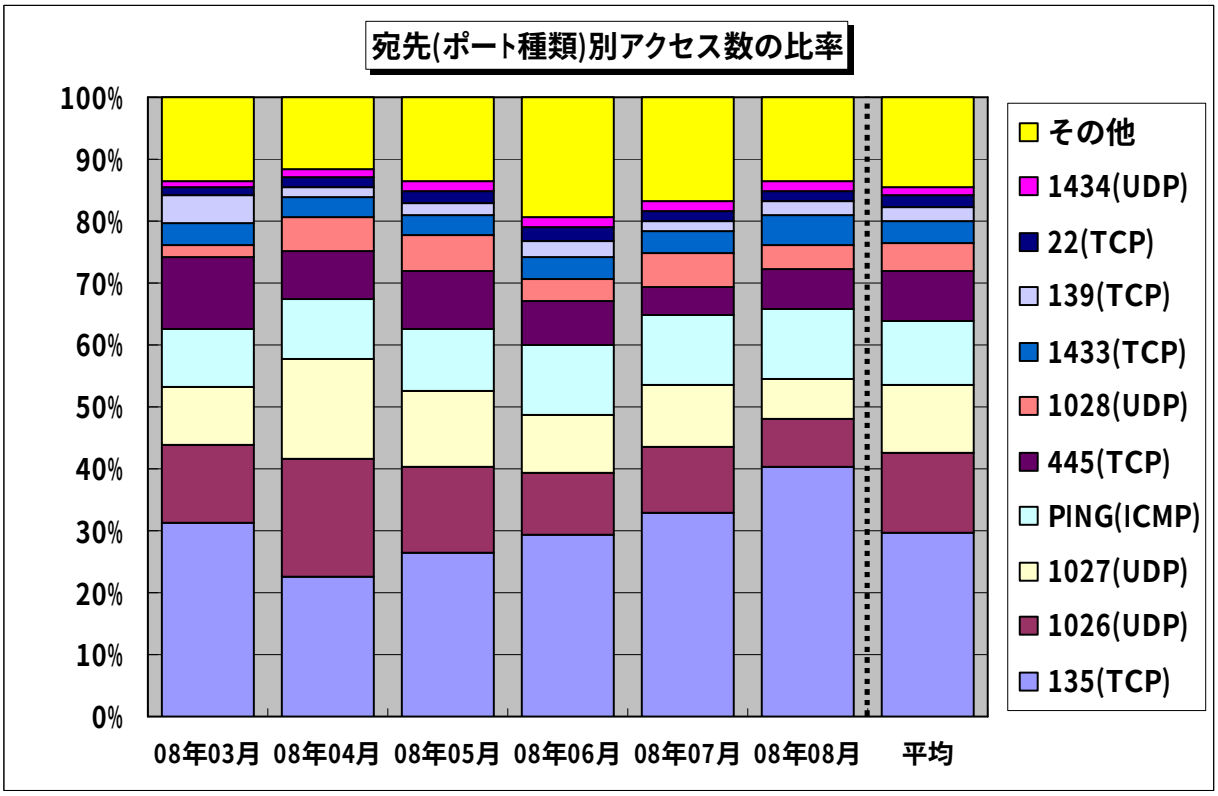



【図 2.4.4 2008 年 8 月の発信元地域別発信元数の比率】

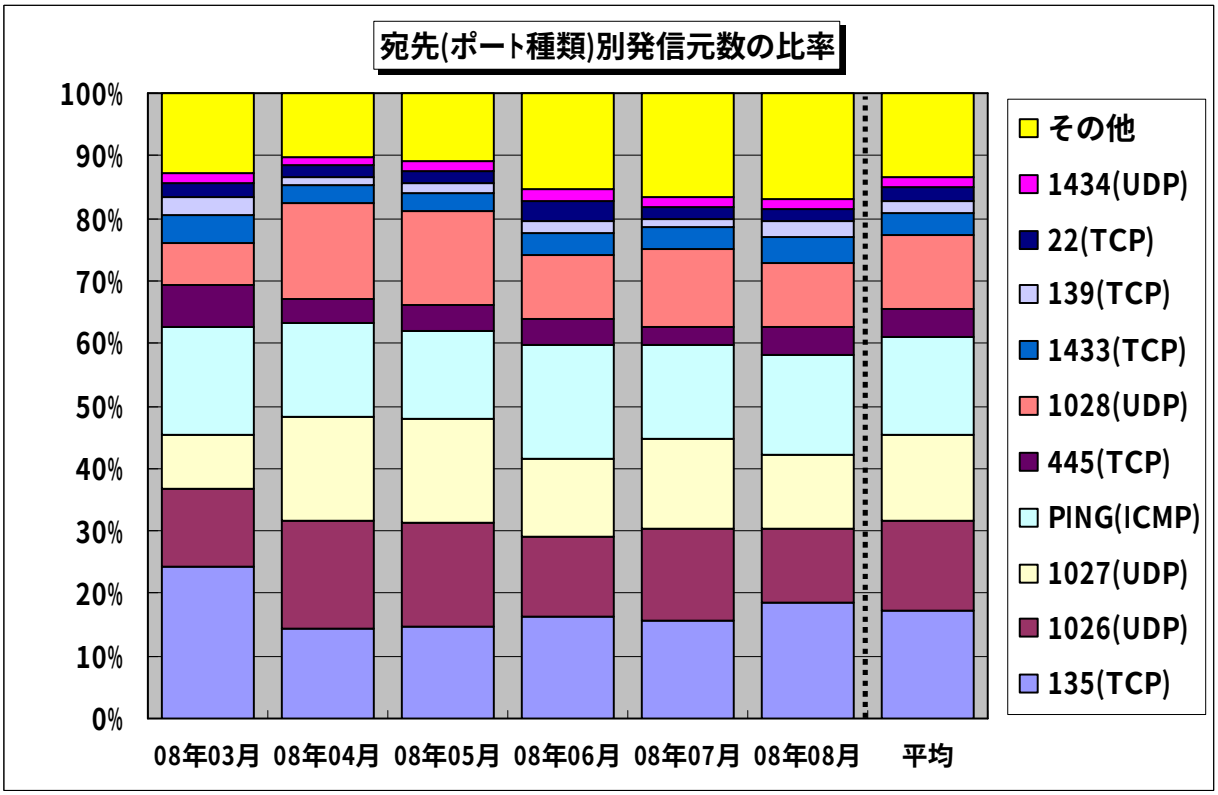
# 3．統計情報

## 3.1 2008 年 3 月～2008 年 8 月の宛先(ポート種類)別の比率

2008 年 3 月～2008 年 8 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。



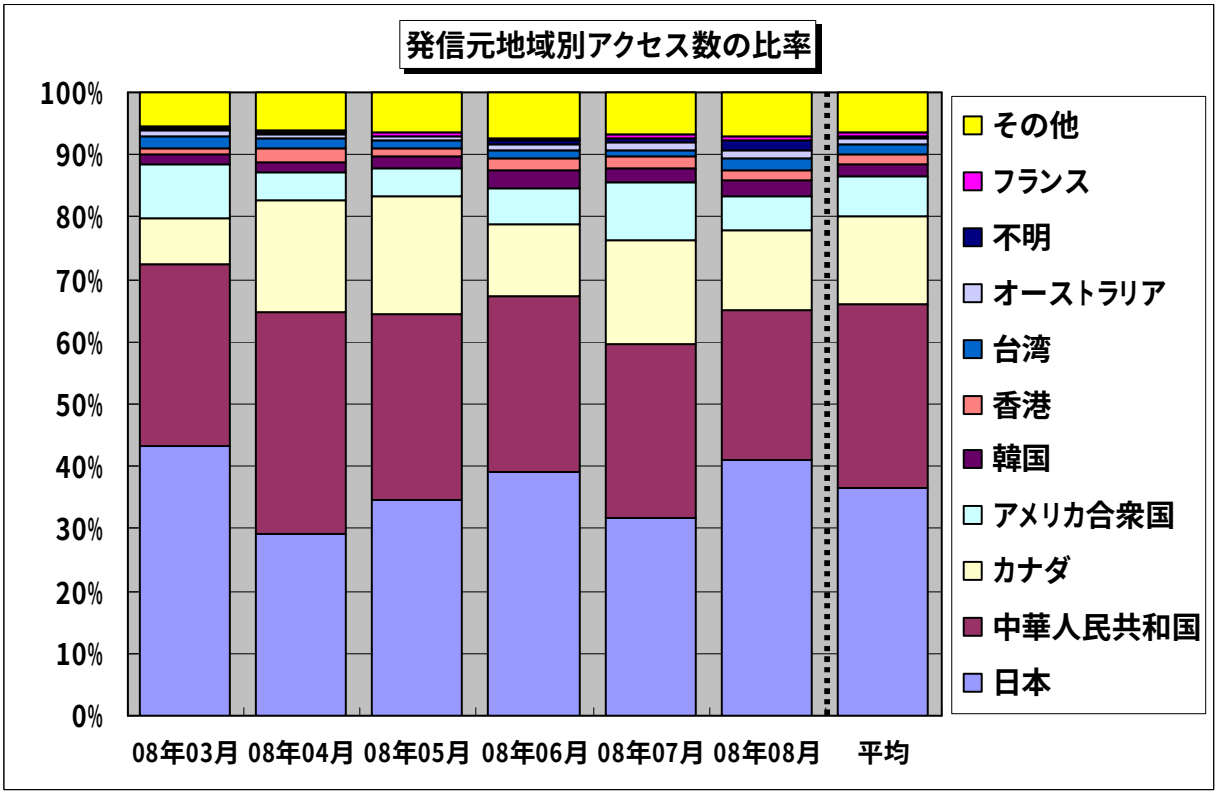

【図 3.1.1 2008 年 3 月～2008 年 8 月の宛先(ポート種類)別アクセス数の比率】



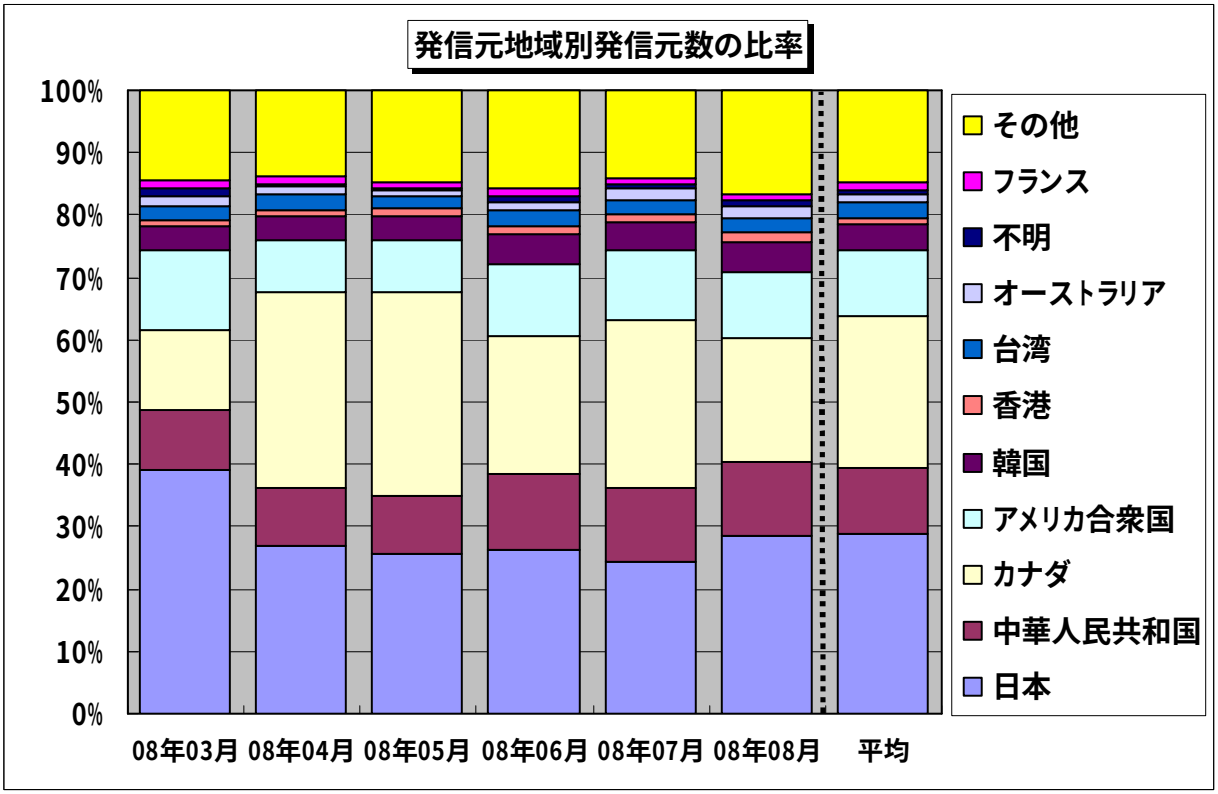

【図 3.1.2 2008 年 3 月～2008 年 8 月の宛先(ポート種類)別発信元数の比率】

## 3.2 2008 年 3 月～2008 年 8 月の発信元地域別の比率

2008 年 3 月～2008 年 8 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 2008 年 3 月～2008 年　8 月の発信元地域別アクセス数の比率】




【図 3.2.2 2008 年 3 月～2008 年 8 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 8 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 |
|---|---|
| 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 |
| 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）を狙ったアクセスです |
| 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) |
| 139（TCP） | 保護の甘いファイル（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 Window の脆弱性を狙ったアクセスである可能性が高いです |
| 445(TCP) | 保護の甘いファイル（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） |
| 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 |
| 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 |
| 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
大浦／望月／加賀谷
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp