別紙 3

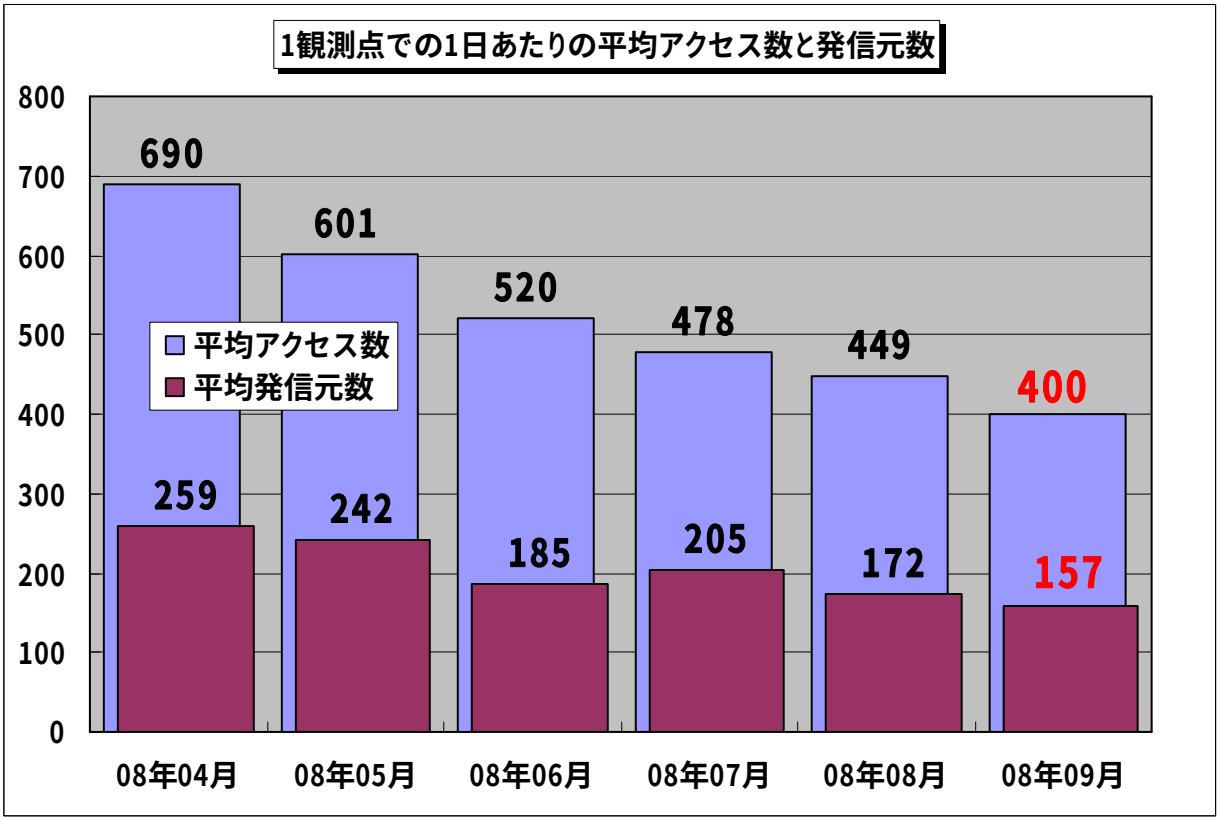
インターネット定点観測(TALOT2)での観測状況について

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 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 **119,926 件**、総発信元数(※)は **47,248 箇所**ありました。1 観測点で見ると、1 日あたり **157** の発信元から **400 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、157 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。



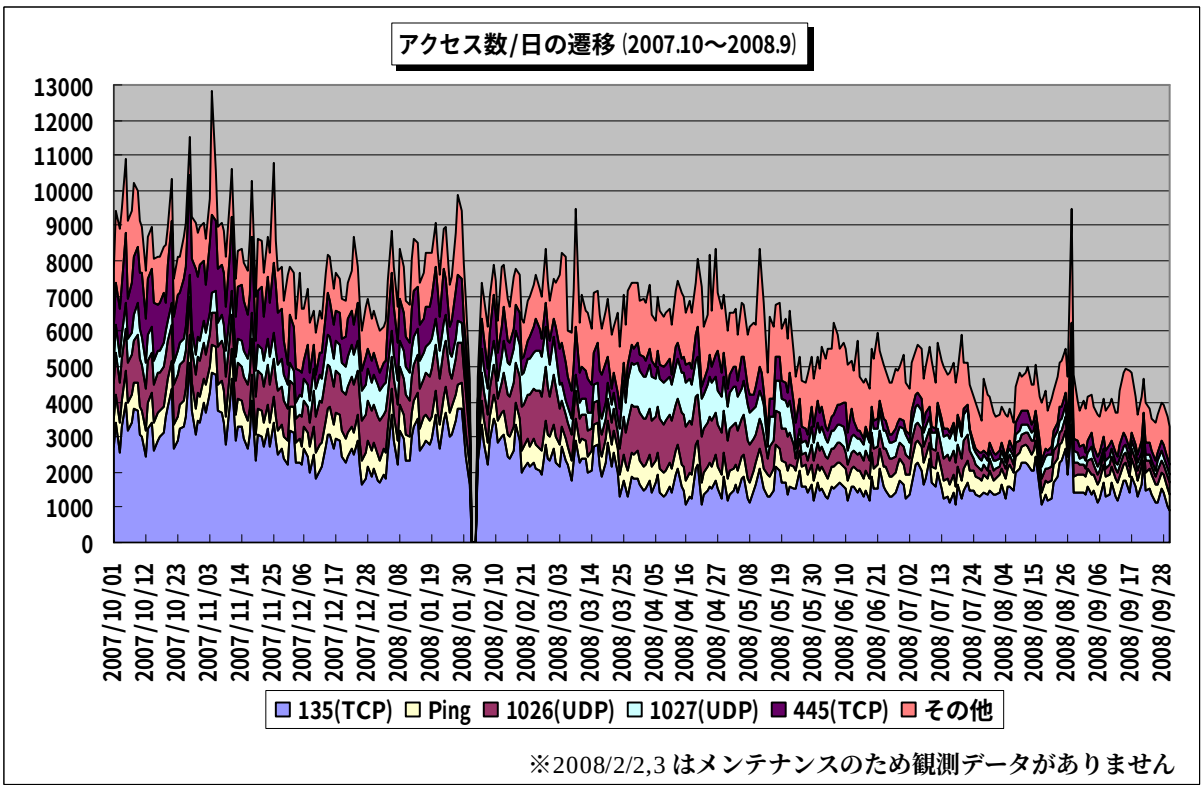
【図 1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2008 年 4 月～2008 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、9 月の期待しない（一方的な）アクセスは 8 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。

2．9 月のアクセスの状況

2008 年 9 月のアクセス状況は、8 月と比べて若干減少しました。これは、主に 8 月にアクセスが増加していた Windows の脆弱性（ぜいじゃくせい）を狙っていると思われる 135/tcp へのアクセスと、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 へのアクセスが減少したためです。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。

前述したように TALOT2 への期待しない（一方的な）アクセス数は毎月減少傾向を示しています。図 2.1.1 に過去 1 年間の一日毎の種類別アクセス数の遷移を示します。

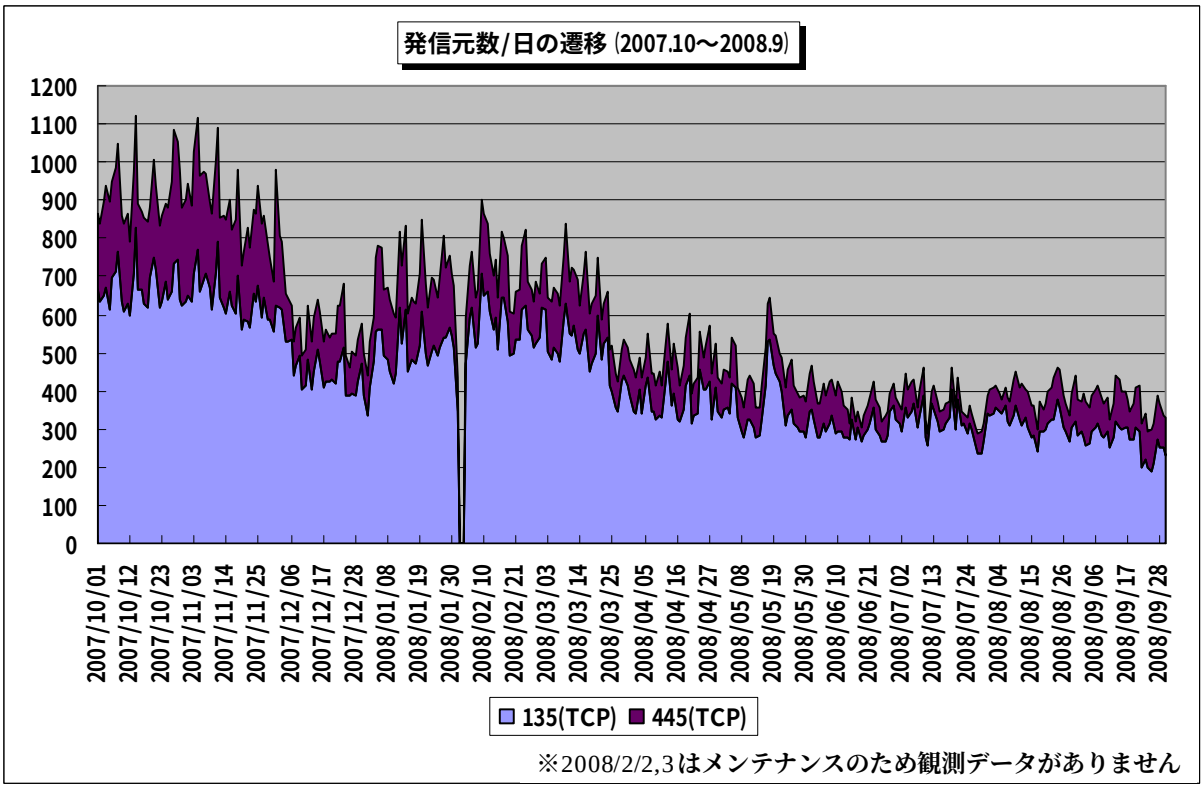


【図 2.1.1 2007 年 10 月から 2008 年 9 月までの種類別アクセス数/日の遷移】

全体のアクセス数の推移において、支配的と言える 135/tcp や 445/tcp へのアクセスが一年を通して明らかに減少傾向を示していることが、全体のアクセス数の推移に影響していることが見て取れます。

これらの種類のアクセスが減少している要因として、これらのポートの脆弱性を狙った（2003 年 8 月に流行した MSBlaster や 2004 年 5 月に流行した Sasser あるいはそれらの攻撃手法を取り込んだボットと呼ばれるような）何らかのウイルスの感染活動が減少していると言えます。

図 2.1.2 に、過去 1 年間の一日毎の 135/tcp と 445/tcp へのアクセスの発信元数の遷移を示します。



【図 2.1.2 2007 年 10 月から 2008 年 9 月までの種類別発信元数/日の遷移】

135/tcp および 445/tcp へのアクセスの発信元数の遷移がアクセス数の遷移とほぼ比例しており、発信元数も減少傾向を示していることが見て取れます。

2.1 設定不備のプロキシサーバ(※1)を探索していると思われるアクセス

9月13日から17日にかけて、TALOT2の7観測点において、8080/tcpおよび6588/tcpへのアクセス急増が観測されました(図2.1.3参照)。

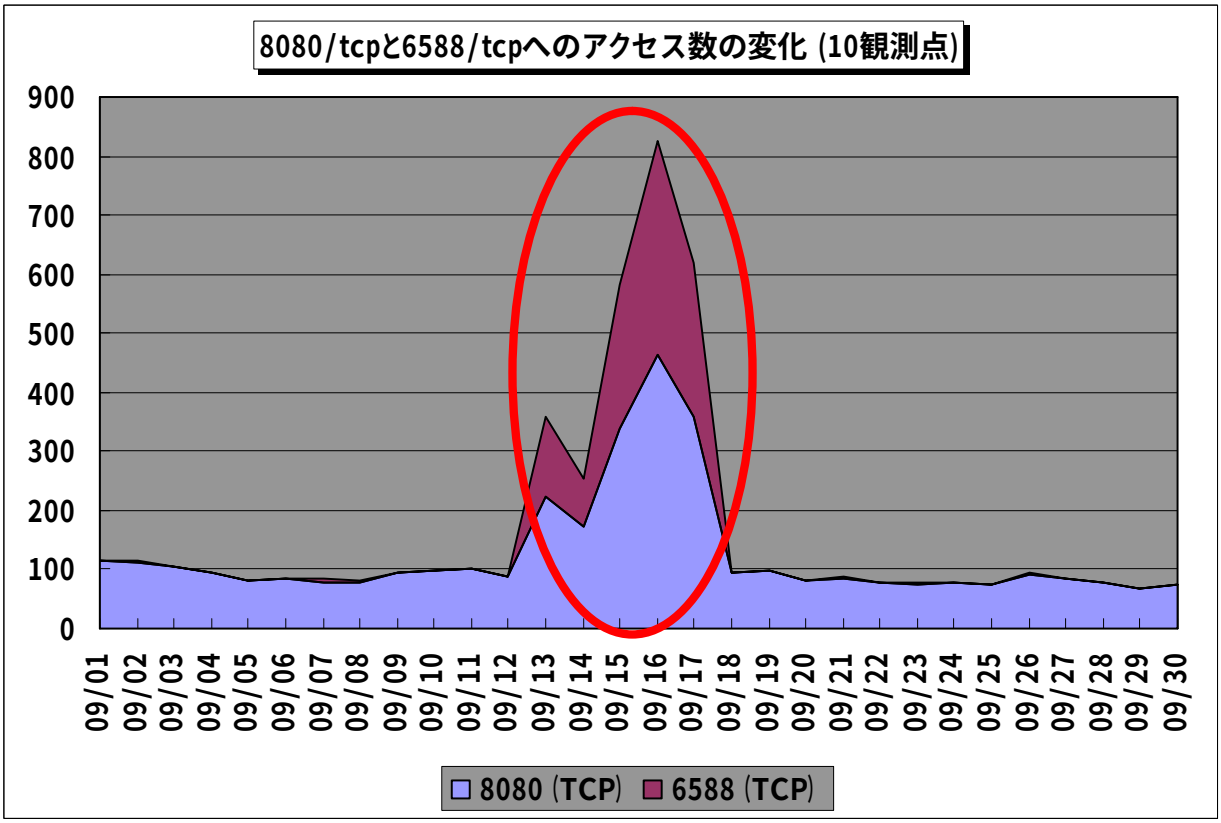
発信元は全て中華人民共和国の特定のIPアドレスでした。

8080/tcpおよび6588/tcpはプロキシサービスで利用されることの多いポートです。

これらのアクセスは、外部から迷惑メールの送信などに利用できるプロキシサーバ(オープンプロキシという)がないかを探索している可能性があります。また、短期間におなじ観測点に数百回もアクセスしているので、探索のためのツールをテストしている可能性もあります。

これらのアクセスにより、攻撃者にオープンプロキシであると判断されたプロキシサーバは、迷惑メールの送信などの踏み台として利用されることがあります。

プロキシサーバを運用しているシステム管理者は、お使いのプロキシサーバが外部から利用されないように、サーバ設定を再度確認して下さい。

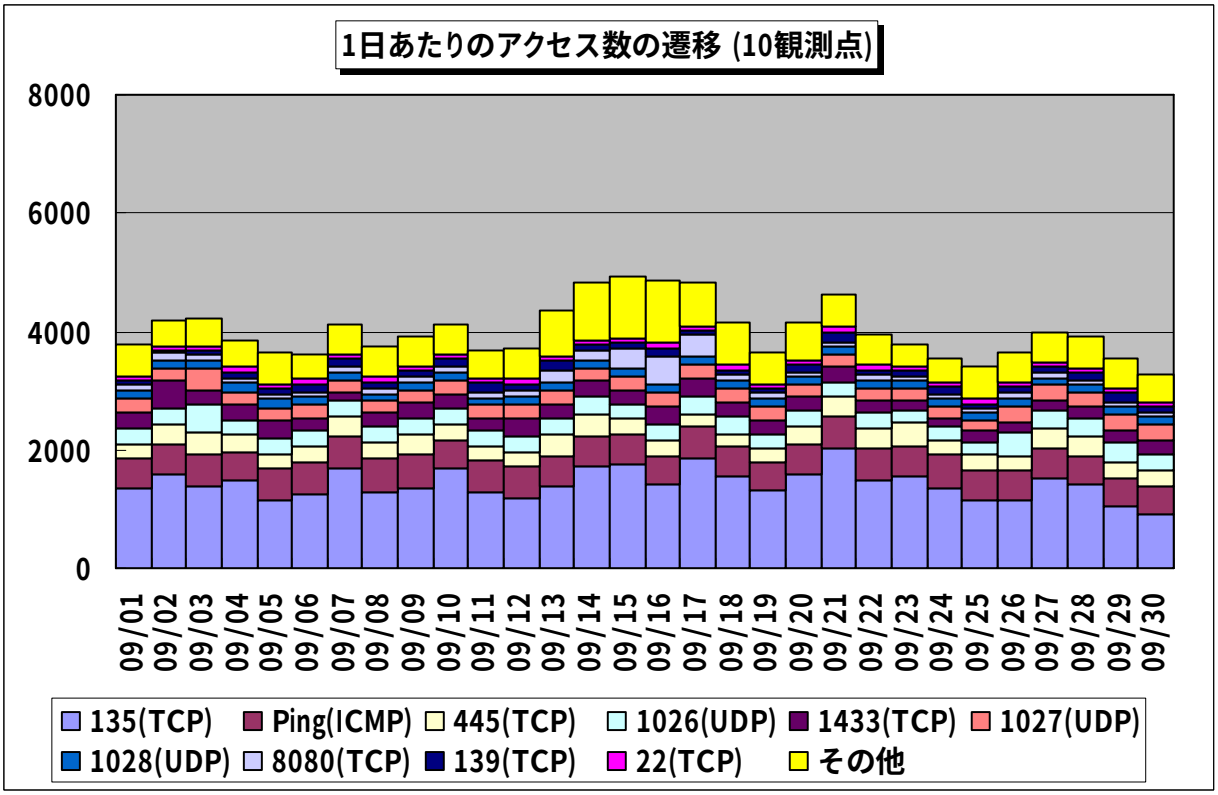


【図2.1.3 8080/tcpと6588/tcpへのアクセス数の変化】

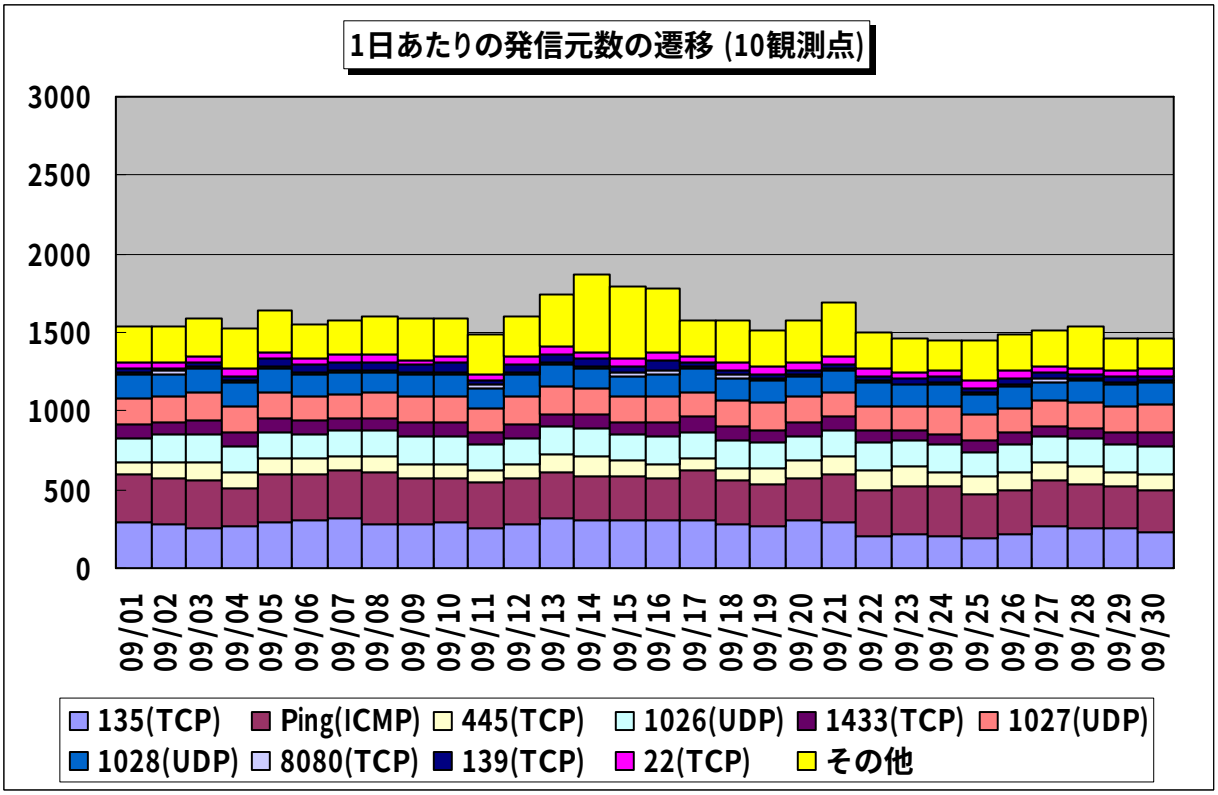
※1:プロキシサーバ:通信を代理で行うサーバのことを言います。主に企業などの組織で、内部ネットワークとインターネットの接続地点で、通信のセキュリティ確保と高速アクセスを実現させるために利用されることが多い。

2.2 2008 年 9 月の一方的なアクセス状況

2008 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 2.1.2 に示します。



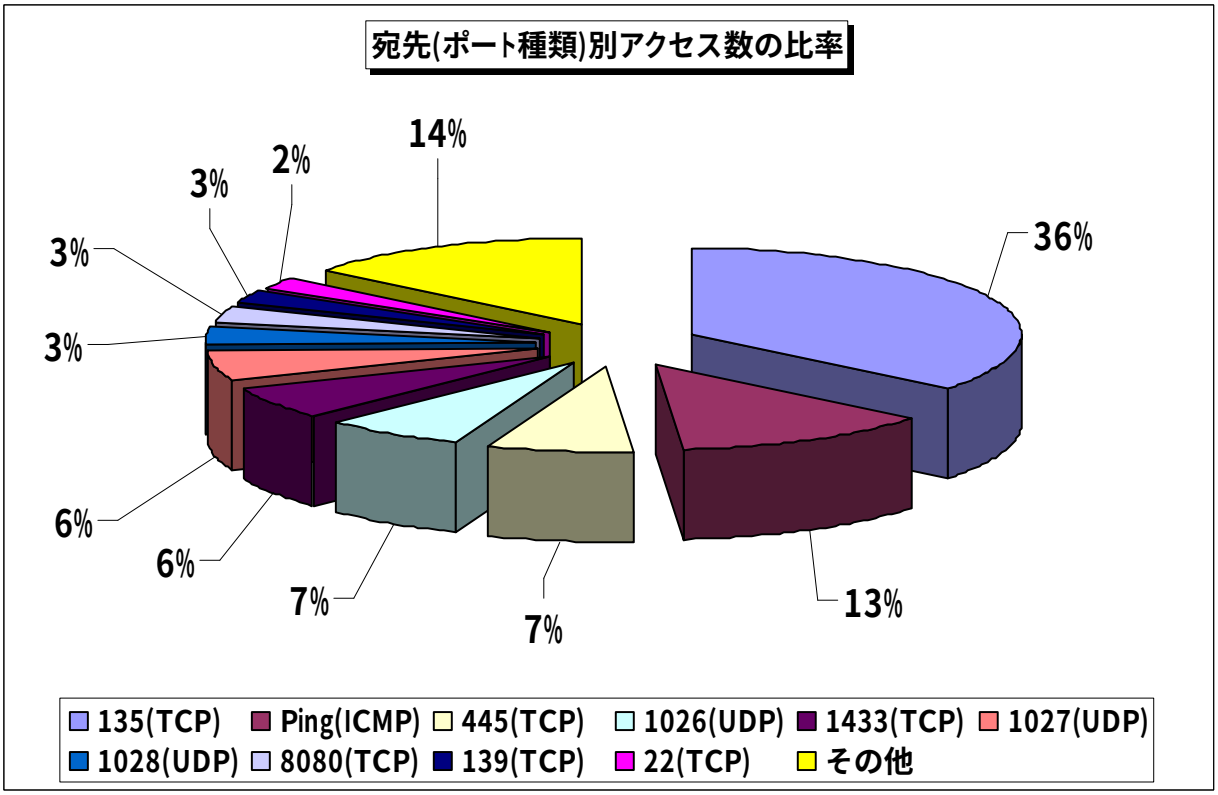
【図 2.2.1 2008 年 9 月の一方的なアクセス状況(アクセス数)】



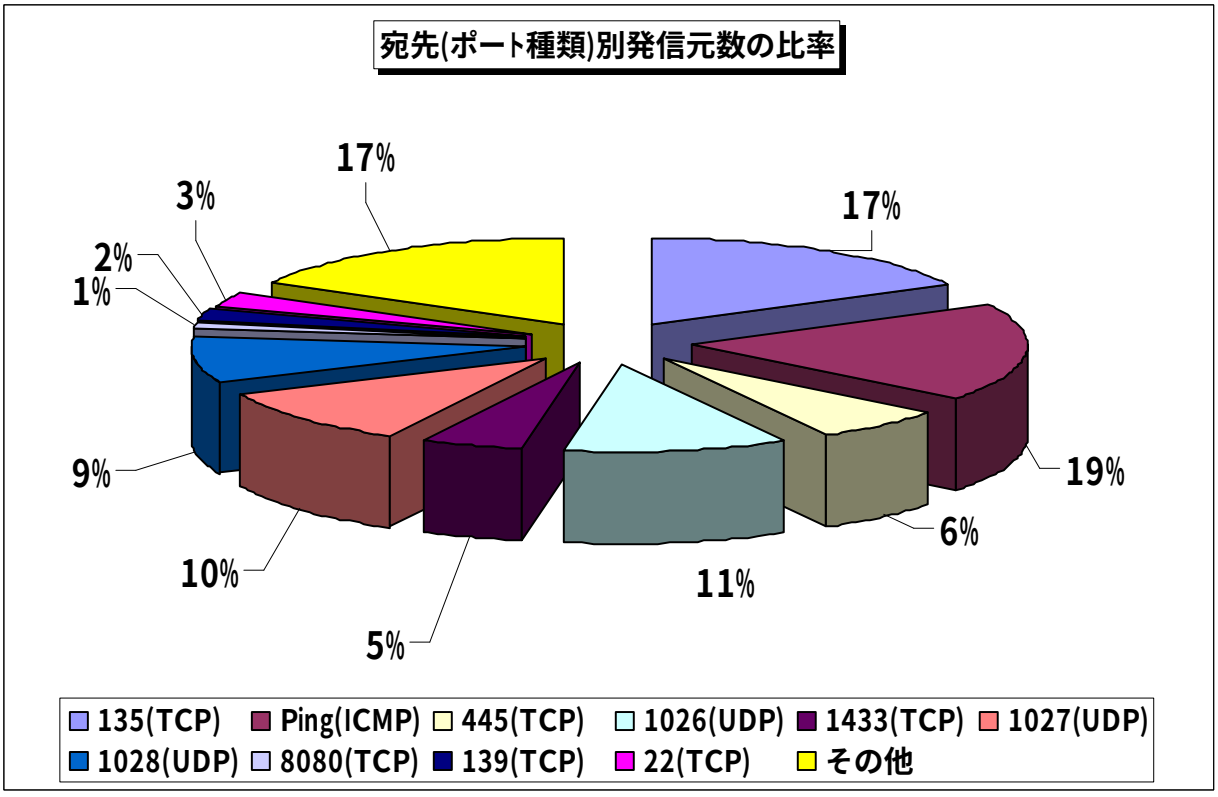
【図 2.2.2 2008 年 9 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 9 月の宛先(ポート種類)別の比率

2008 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。



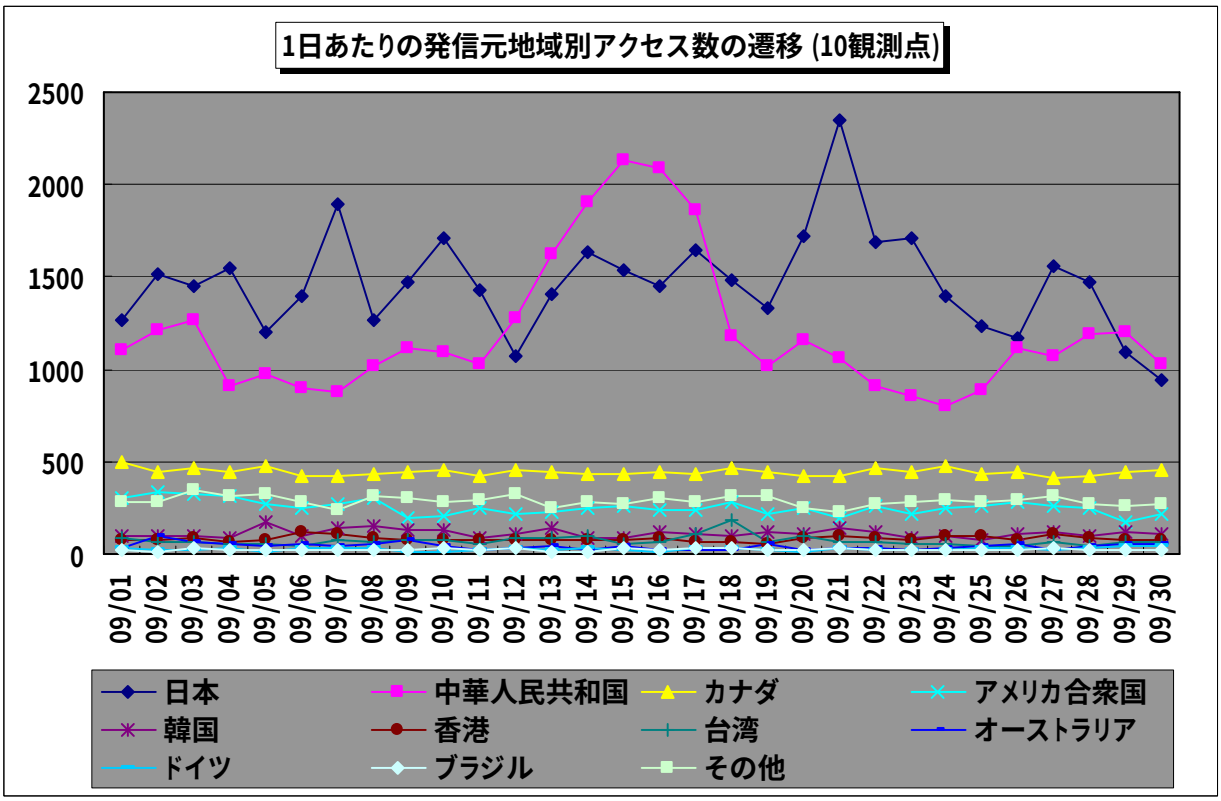
【図 2.3.1 2008 年 9 月の宛先(ポート種類)別アクセス数の比率】



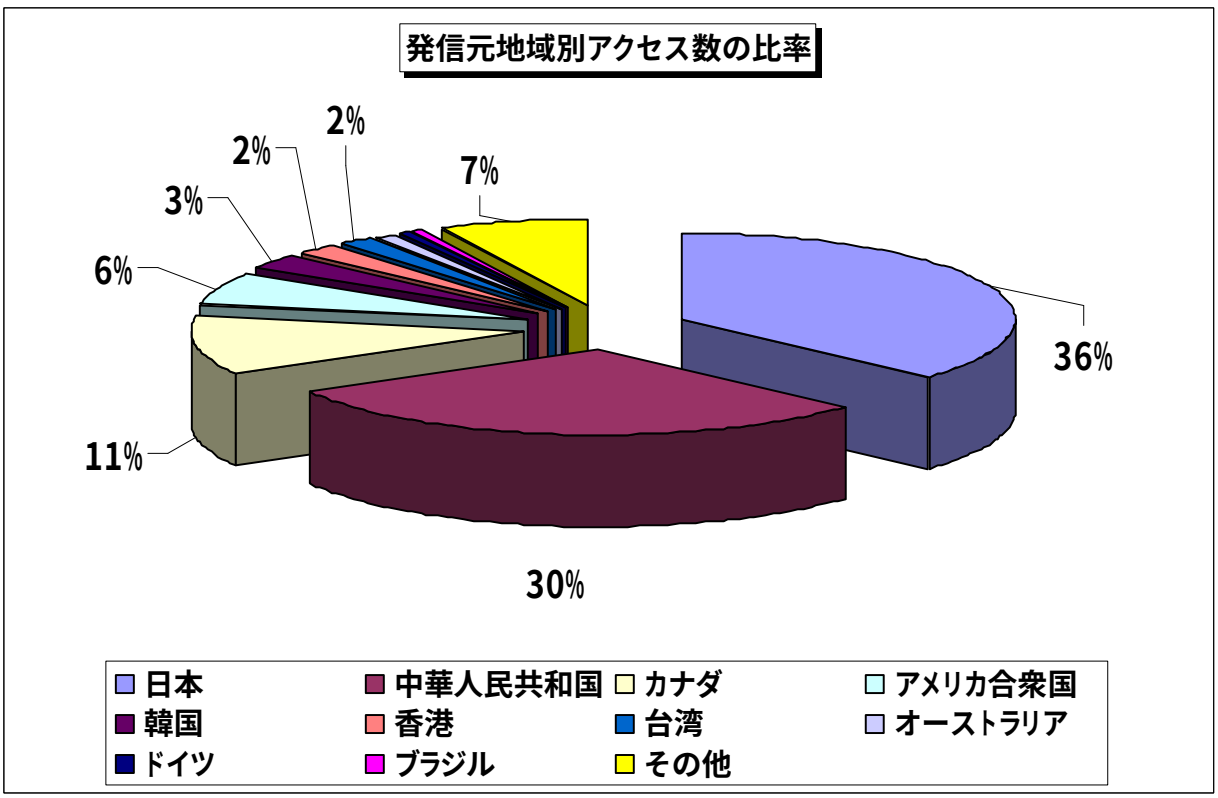
【図 2.3.2 2008 年 9 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 9 月の発信元地域別アクセス状況

2008 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。

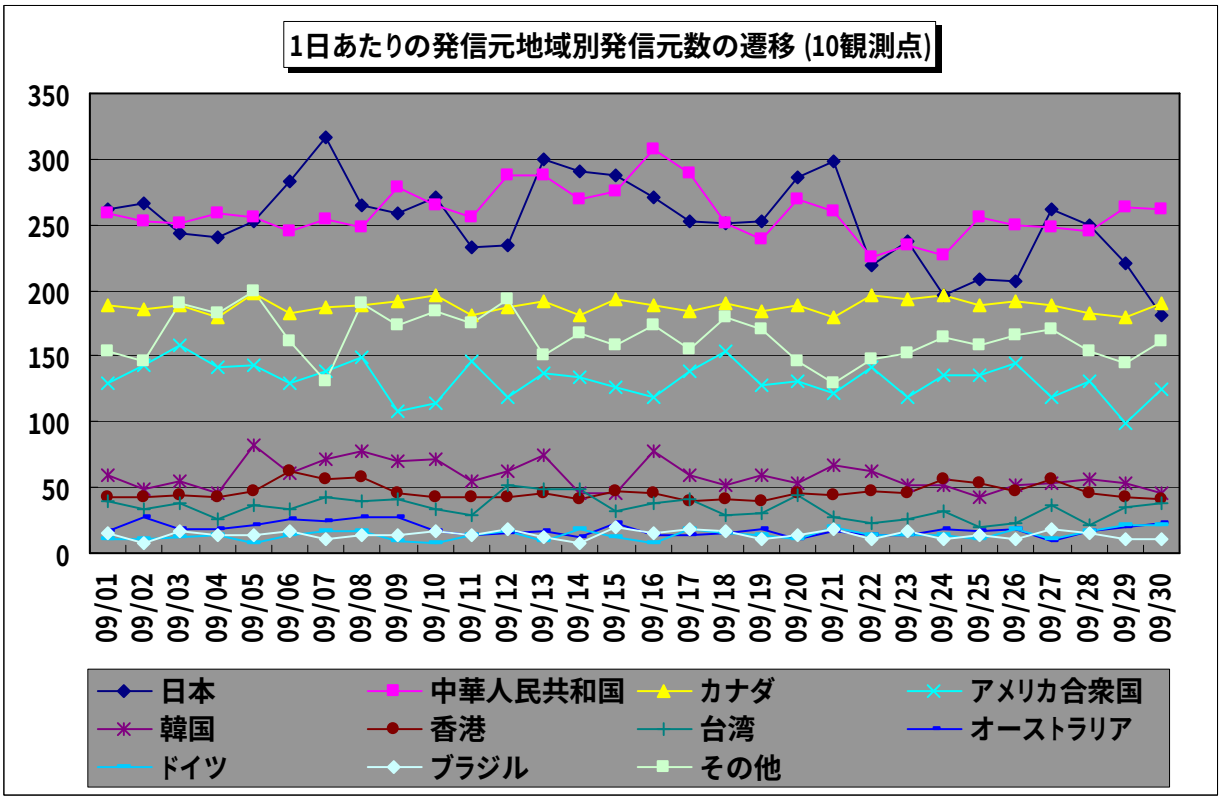


【図 2.4.1 2008 年 9 月の発信元地域別アクセス数の変化】

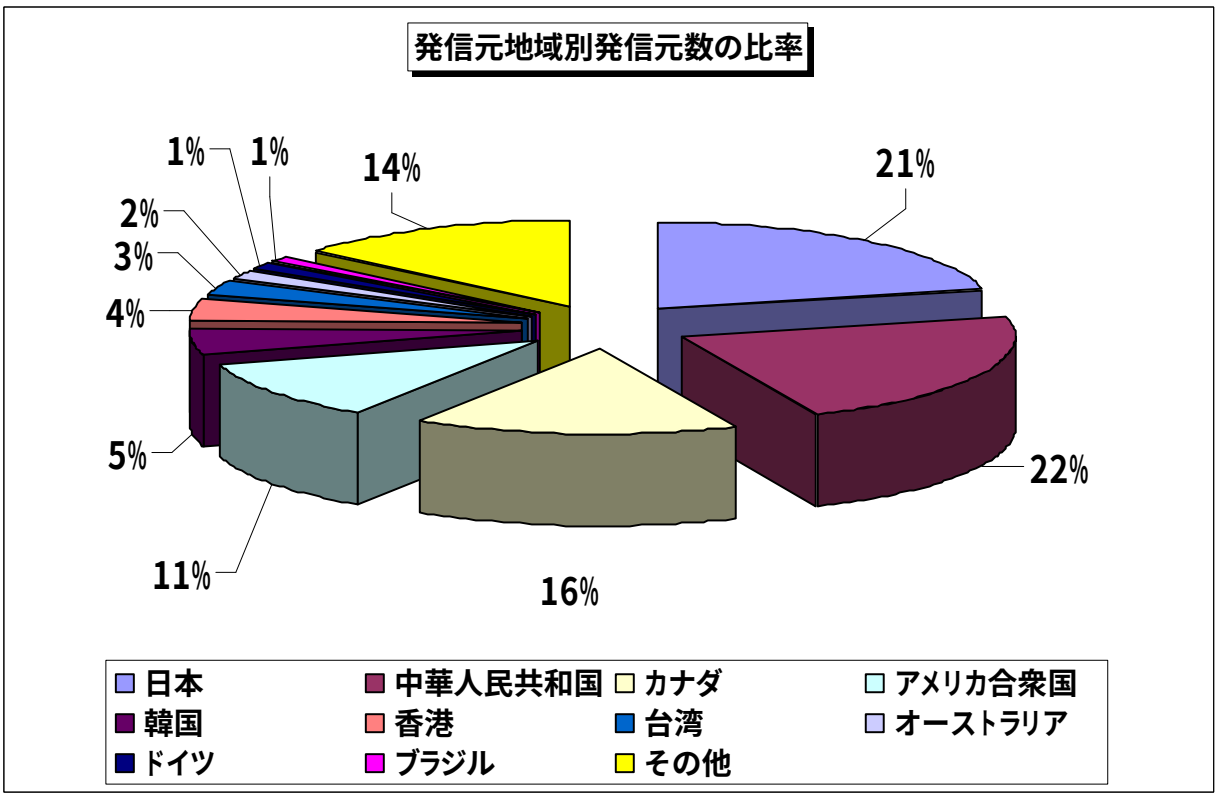


【図 2.4.2 2008 年 9 月の発信元地域別アクセス数の比率】

2008 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 2008 年 9 月の発信元地域別発信元数の変化】

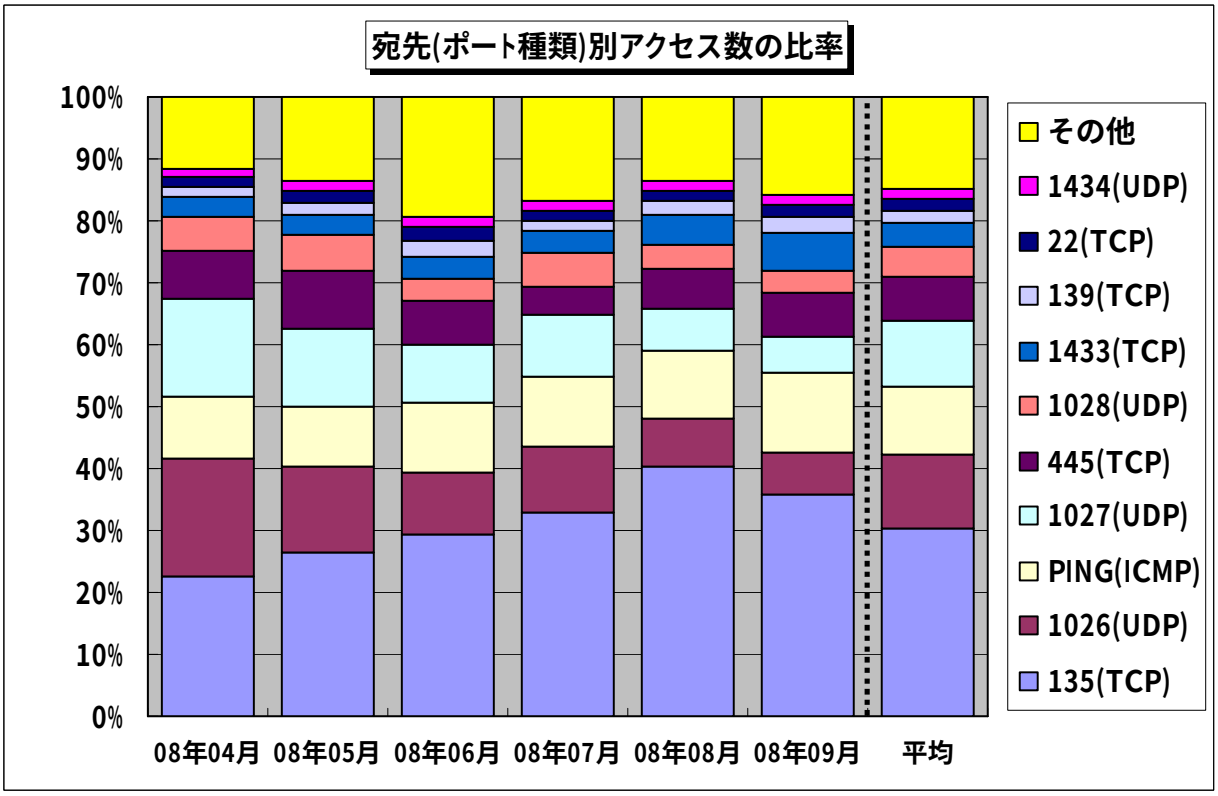


【図 2.4.4 2008 年 9 月の発信元地域別発信元数の比率】

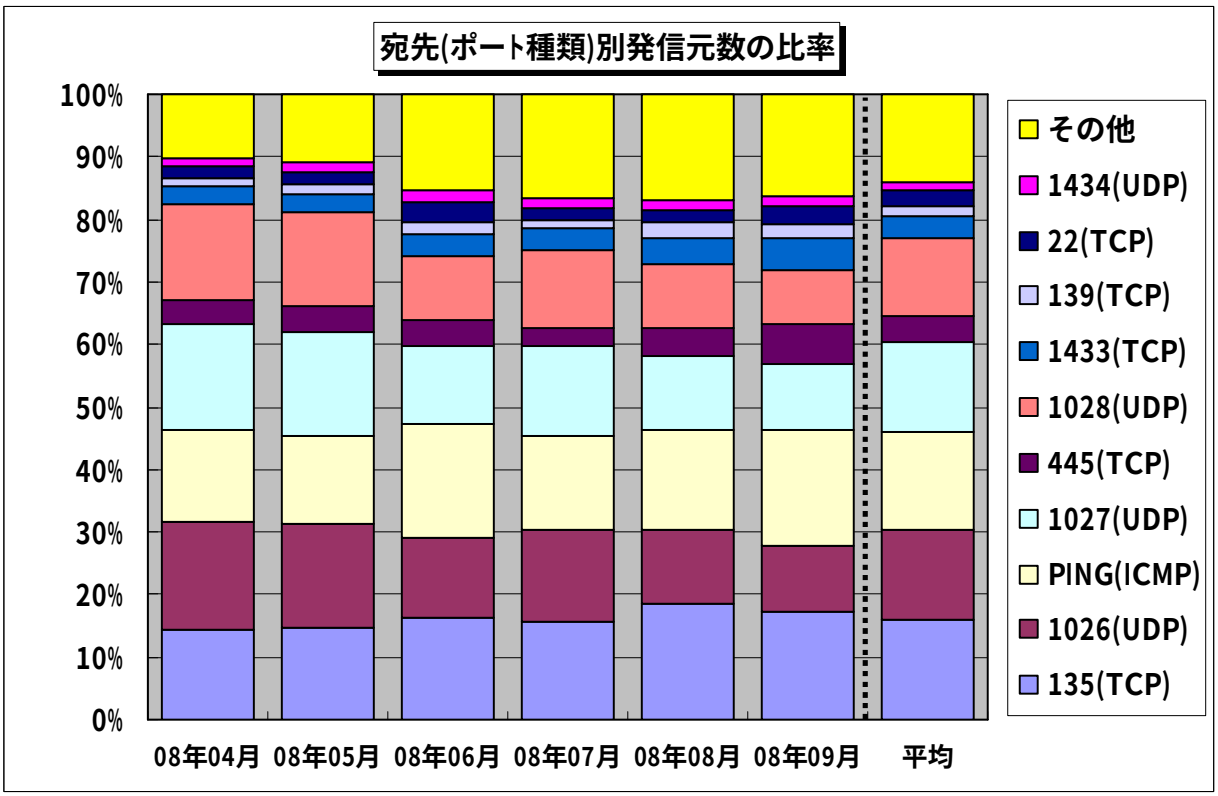
3．統計情報

3.1 2008 年 4 月～2008 年 9 月の宛先(ポート種類)別の比率

2008 年 4 月～2008 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。



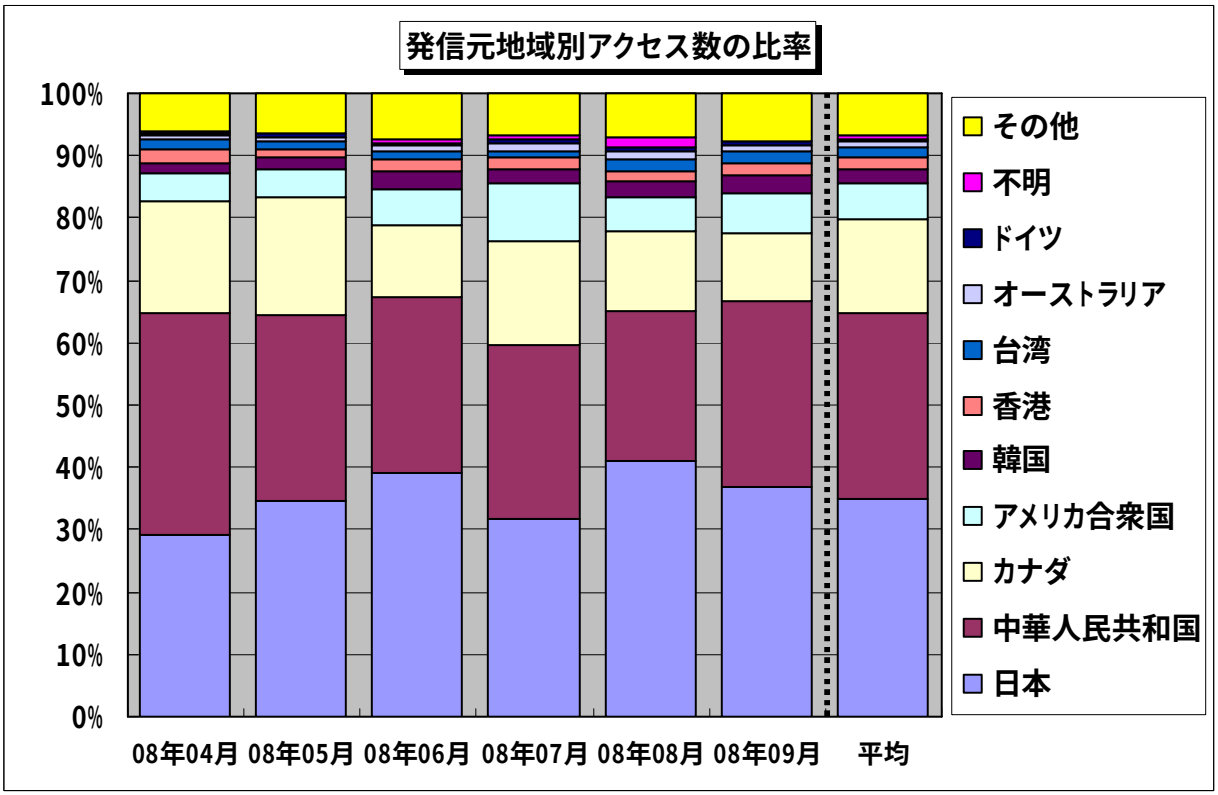
【図 3.1.1 2008 年 4 月～2008 年 9 月の宛先(ポート種類)別アクセス数の比率】



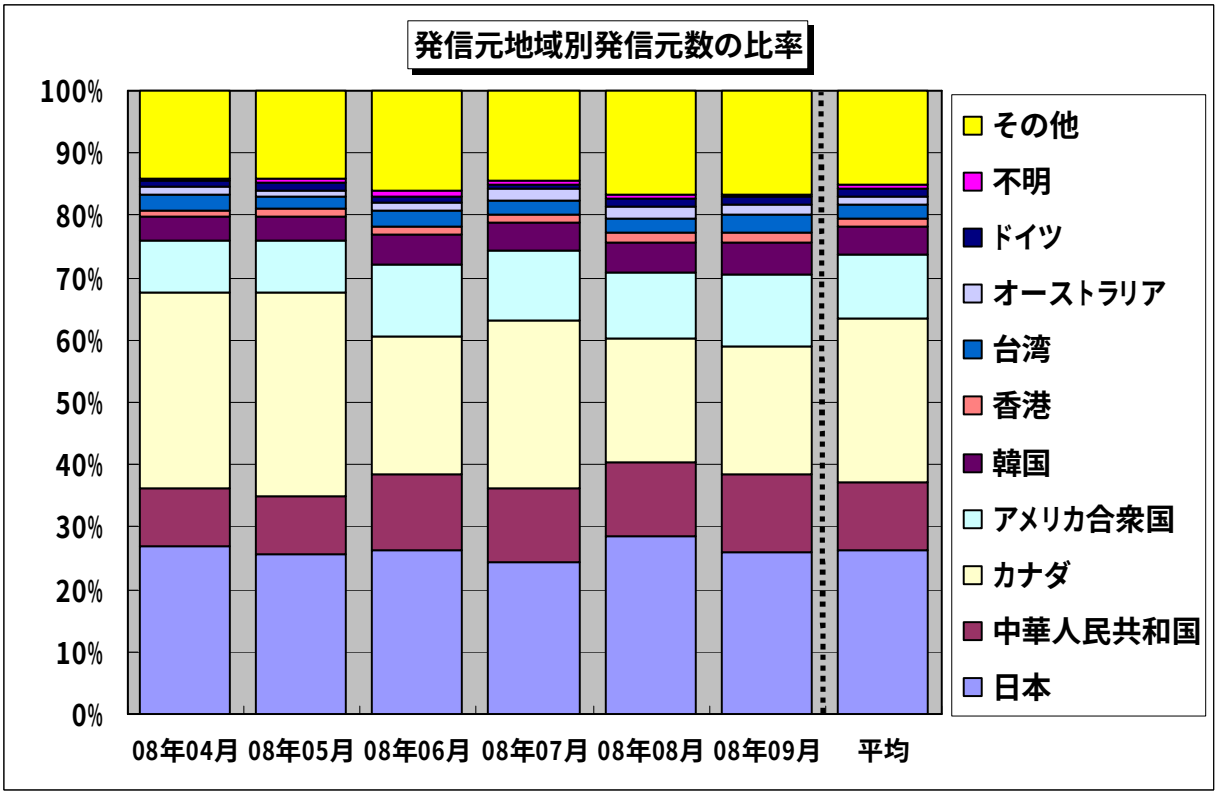
【図 3.1.2 2008 年 4 月～2008 年 9 月の宛先(ポート種類)別発信元数の比率】

3.2 2008 年 4 月～2008 年 9 月の発信元地域別の比率

2008 年 4 月～2008 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 2008 年 4 月～2008 年 9 月の発信元地域別アクセス数の比率】



【図 3.2.2 2008 年 4 月～2008 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、2008 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
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）
8080（TCP）	HTTP Proxy への接続にもっとも標準的に利用されるポートであり、悪意ある者が不正アクセスの踏み台として利用できるプロキシサーバを探索するためのアクセスである可能性が高い。

■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