別紙 3

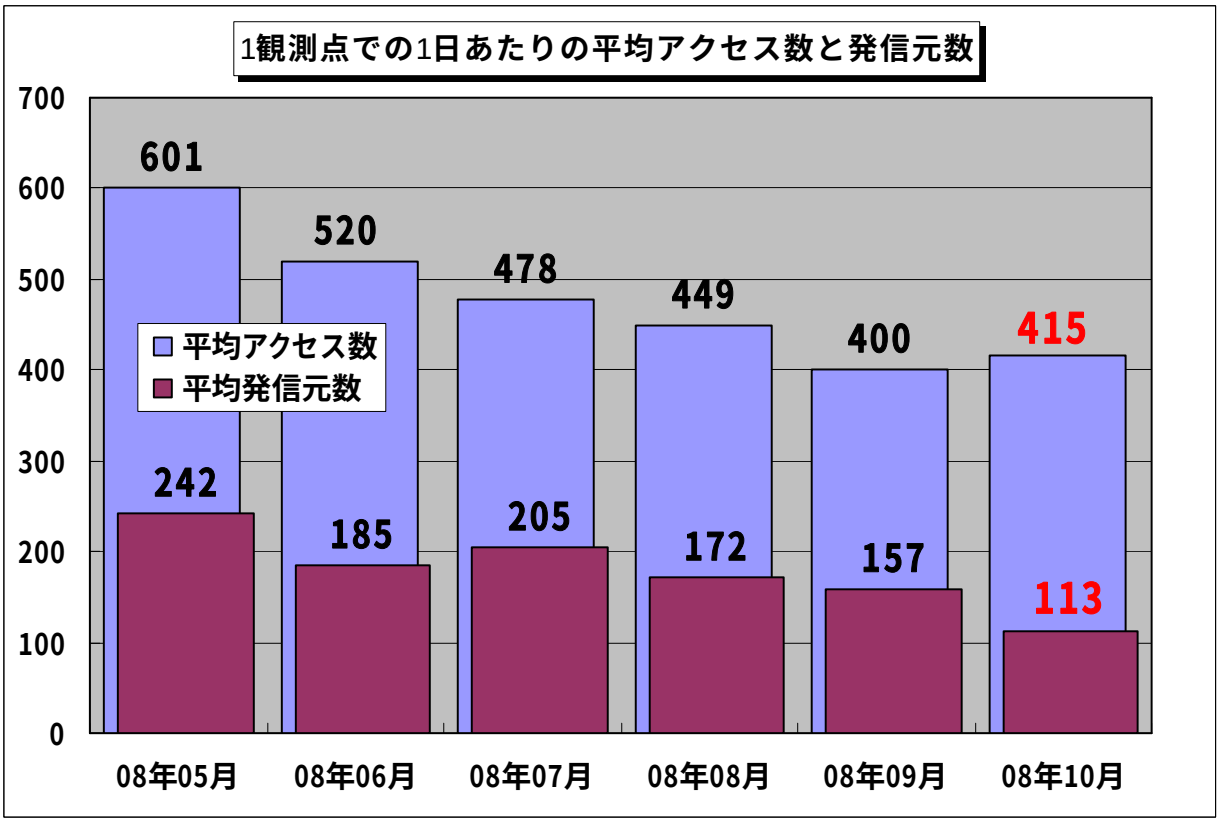
インターネット定点観測(TALOT2)での観測状況について

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 10 月の期待しない(一方的な)アクセスの総数は 10 観測点で 128,667 件、総発信元(※)は 34,926 箇所ありました。1 観測点で見ると、1 日あたり 113 の発信元から 415 件のアクセスがあったことになります。

総発信元(※)：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。



【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】

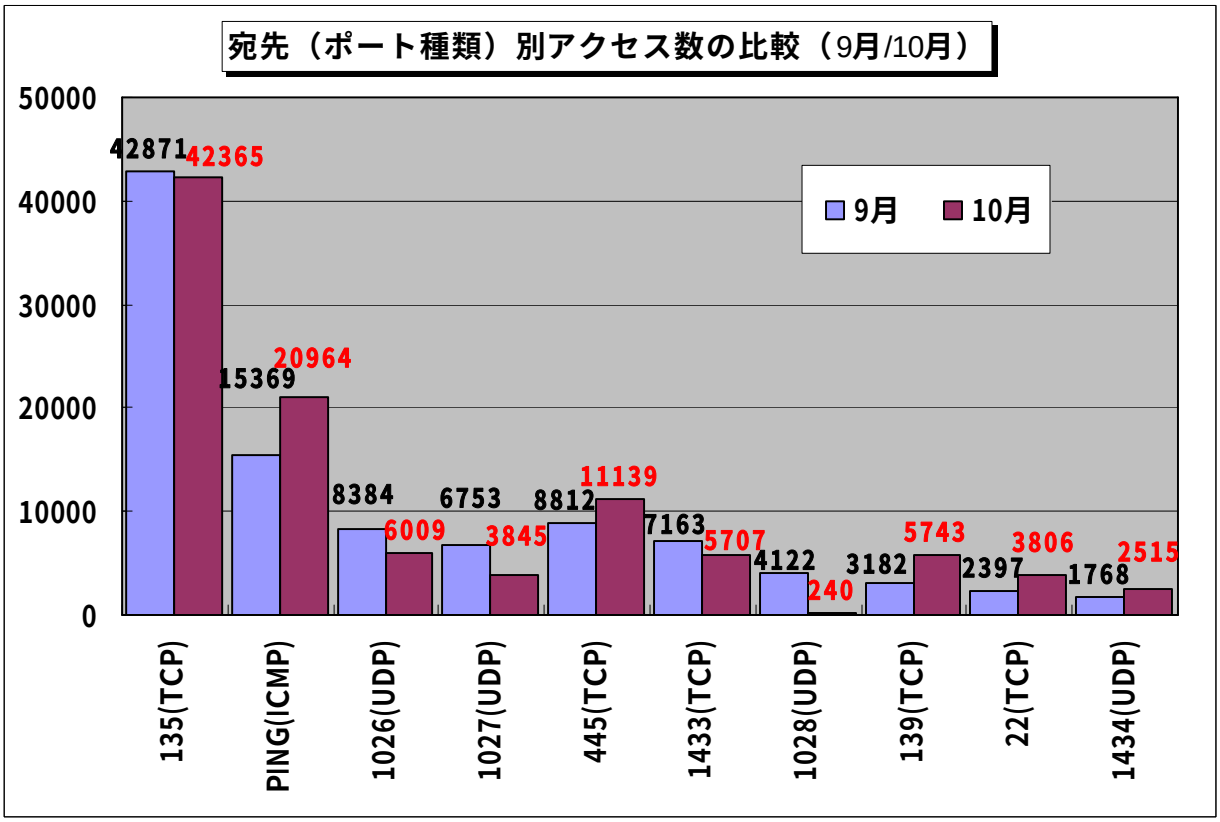
2008 年 5 月～2008 年 10 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、10 月の期待しない(一方的な)アクセスは 9 月と比べて若干増加しました。過去 6 ヶ月を通してみると、これまでの減少傾向が一段落した格好です。

2．10 月のアクセスの状況

2008 年 9 月と 10 月の宛先(ポート種類)別アクセス数の比較結果について図 2.1.1 に示します。

9 月よりアクセス数が増加したのは、Ping、445/tcp、139/tcp 及び 22/tcp へのアクセスでした。

また、アクセス数が減少したのは 1026/udp、1027/udp、及び 1028/udp へのアクセスでした。これらのアクセスは、Windows のメッセンジャサービス機能を利用して、悪意あるメッセージを送りつけるのに使われていると思われます。つまり、10 月はこれらの悪意あるメッセージの流通が総じて減少していると思われます。

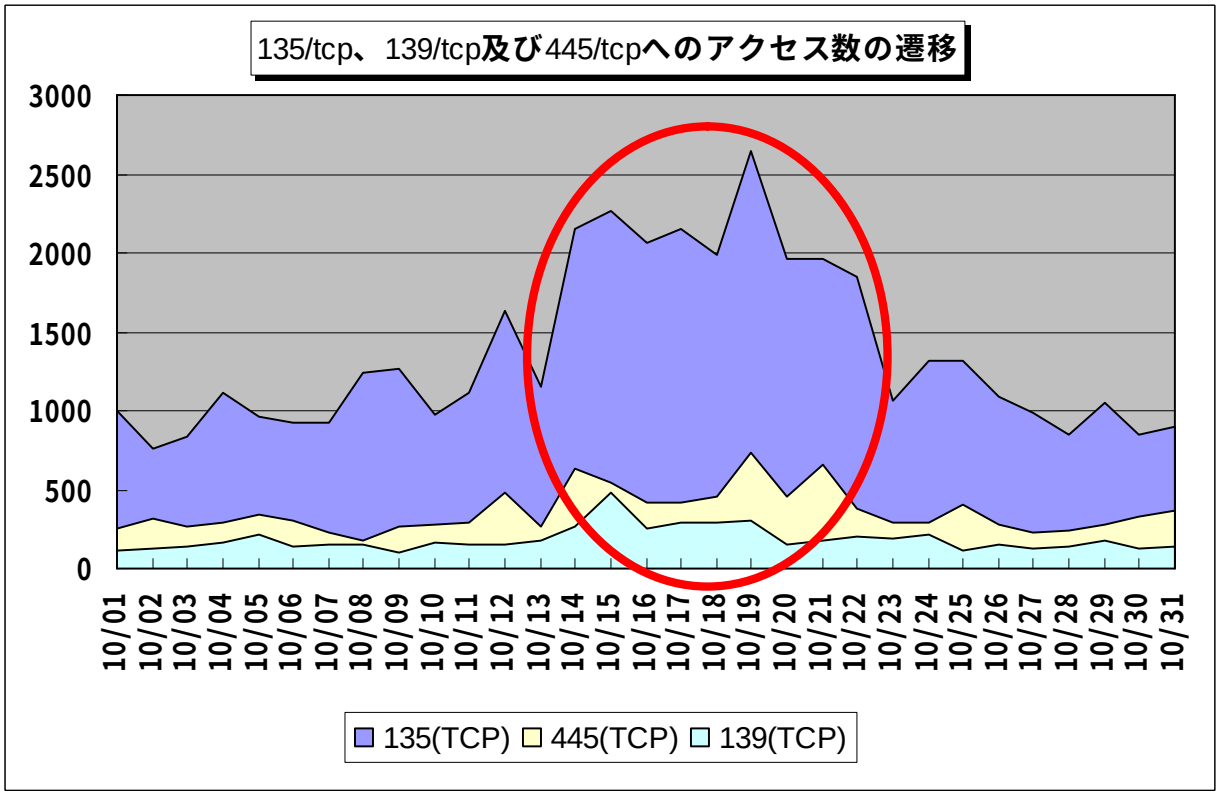


【図 2.1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2.1 135/tcp、139/tcp 及び 445/tcp へのアクセス

10 月 14 日から 22 日にかけて全体的にアクセス数が増加しました。このうち 135/tcp、139/tcp 及び 445/tcp へのアクセスに関しては、10 月 15 日に発表されたマイクロソフトの脆弱性（ぜいじゃくせい）情報の中の、Windows の脆弱性を狙った攻撃が含まれていた可能性があります。

図 2.1.2 に 135/tcp、139/tcp 及び 445/tcp へのアクセス数の遷移を示します。



【図 2.1.2　135/tcp、139/tcp 及び 445/tcp へのアクセス数の遷移】

OS やアプリケーションの脆弱性を解消し、常に最新の状態で使うことは、セキュリティ対策の基本です。

Windows には、更新情報を通知させる設定(自動更新機能)があります。この機能を利用している方は、更新情報が通知されたら、すぐに更新作業を行うように心掛けてください。

この機能を利用していない方は、以下のマイクロソフトのホームページを参考にして、利用するようにしてください。

また、業務サーバなどのように停止が困難なサーバであっても、メンテナンスのための時間を確保するなどして、確実に脆弱性を修正するようにしてください。

＜参考情報＞

■「自動更新機能で常に最新の Windows XP を使おう」(マイクロソフト社)
http://www.microsoft.com/japan/windowsxp/security/au.mspx

■ Windows Vista の自動更新機能の解説（マイクロソフト社の Windows Vista まるわかりガイドの情報）
http://www.microsoft.com/japan/windows/using/windowsvista/guide/security/update.mspx

また、更新情報の通知が行われないアプリケーションなどについても、専用サイトなどで脆弱性情報をこまめに確認し、更新作業が手遅れにならないように十分注意ください。

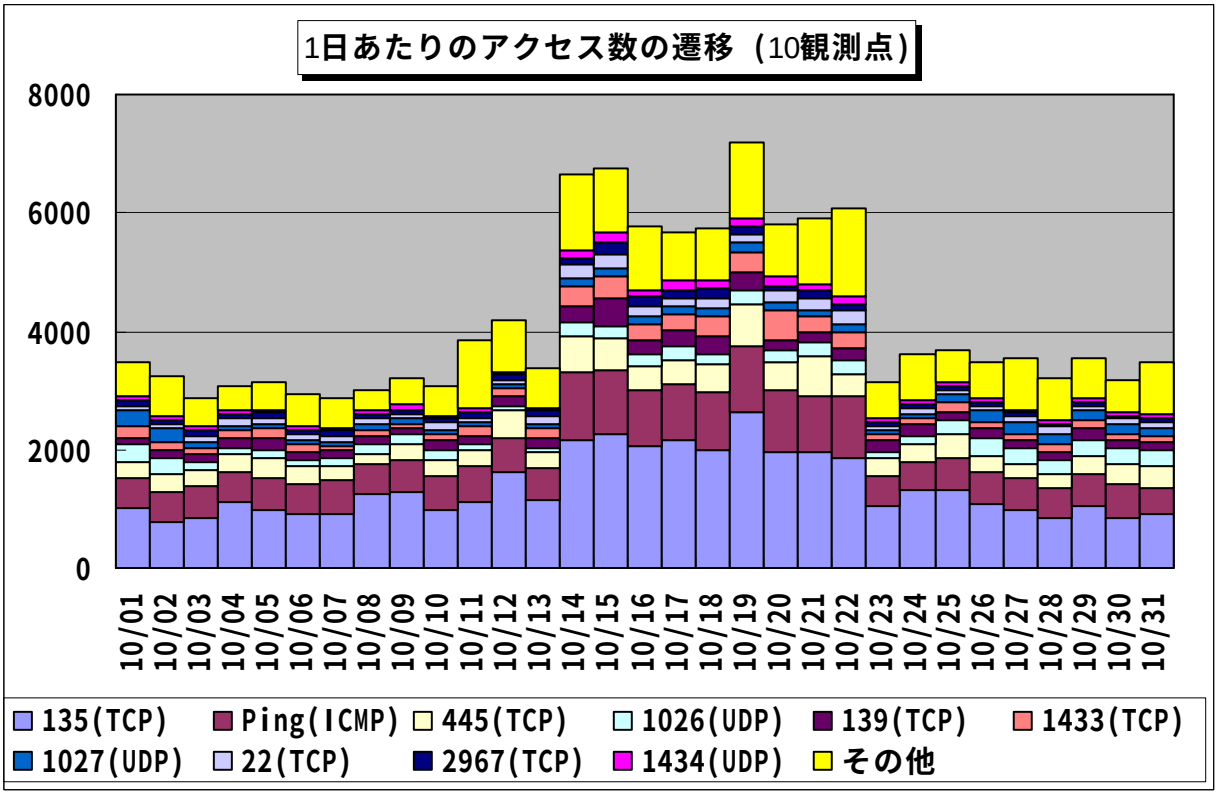
＜参考情報＞

■「Microsoft Update と Windows Update の利用の手順」(マイクロソフト社)
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx

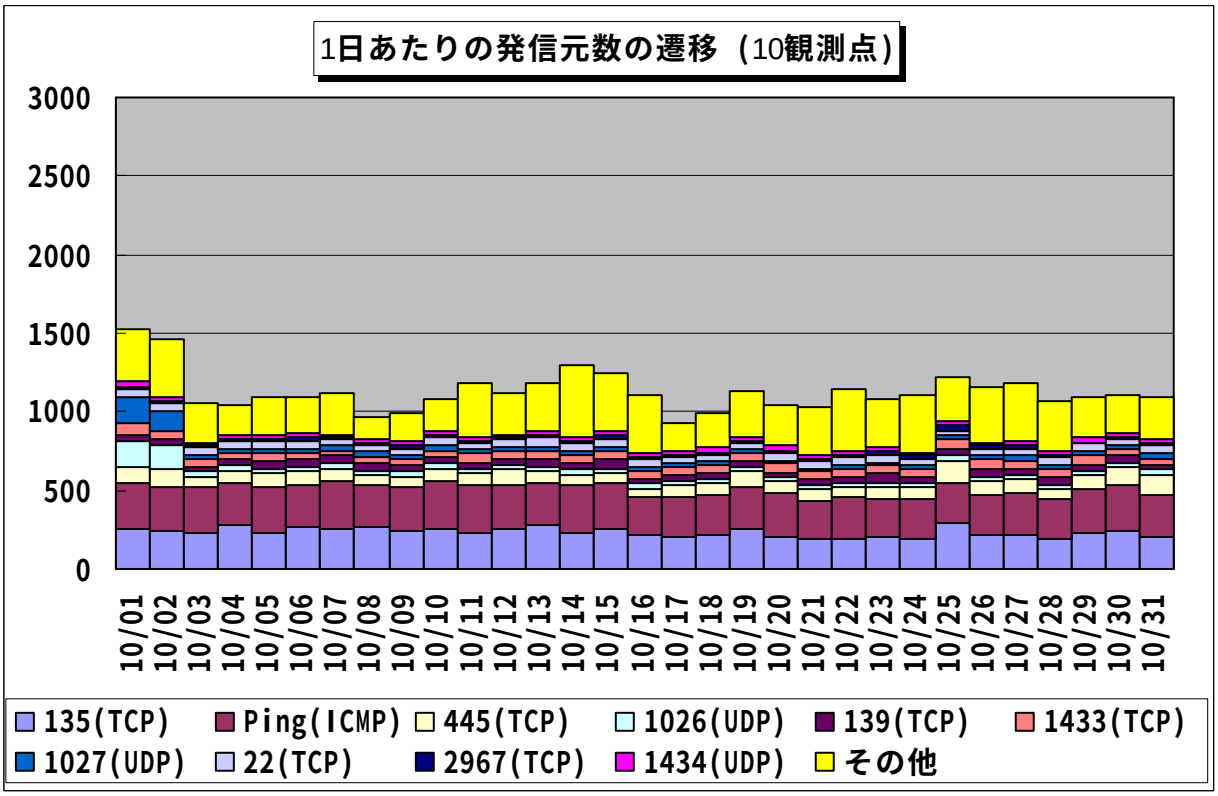
■「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

2.2 2008 年 10 月の一方的なアクセス状況

2008 年 10 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。



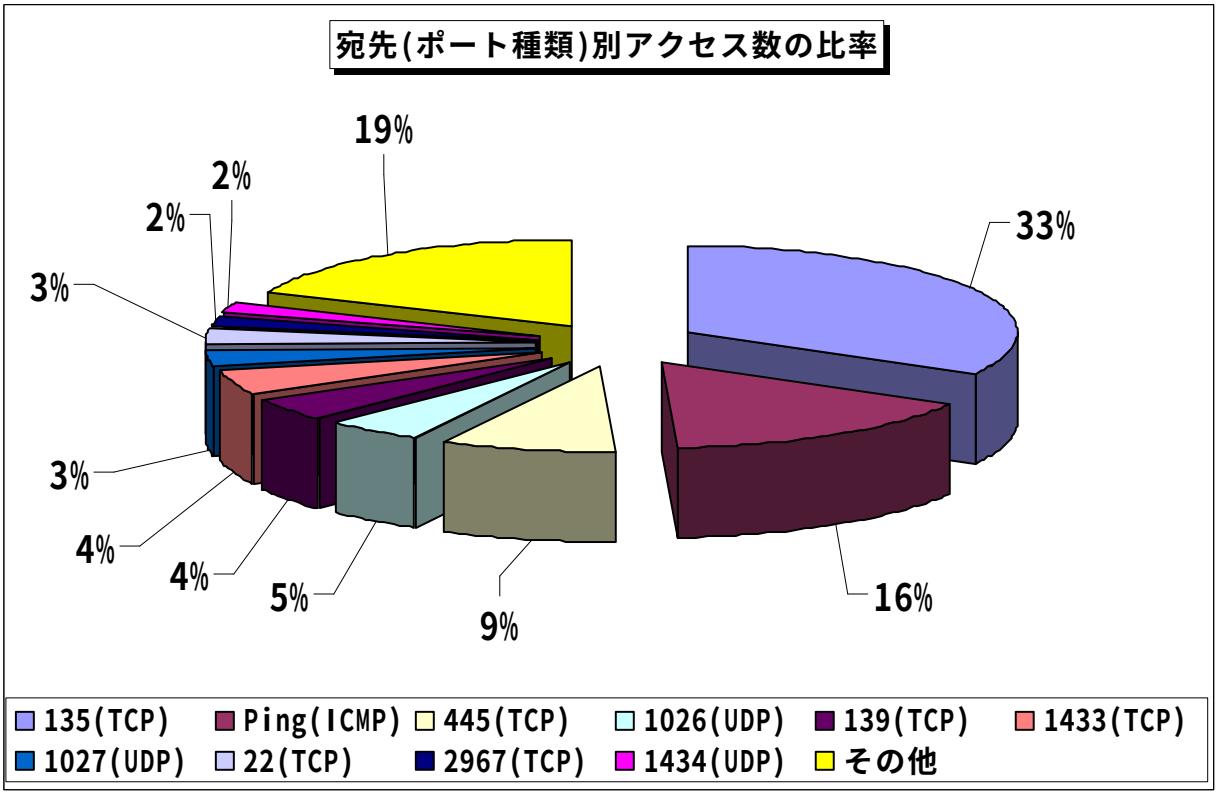
【図 2.2.1 2008 年 10 月の一方的なアクセス状況(アクセス数)】



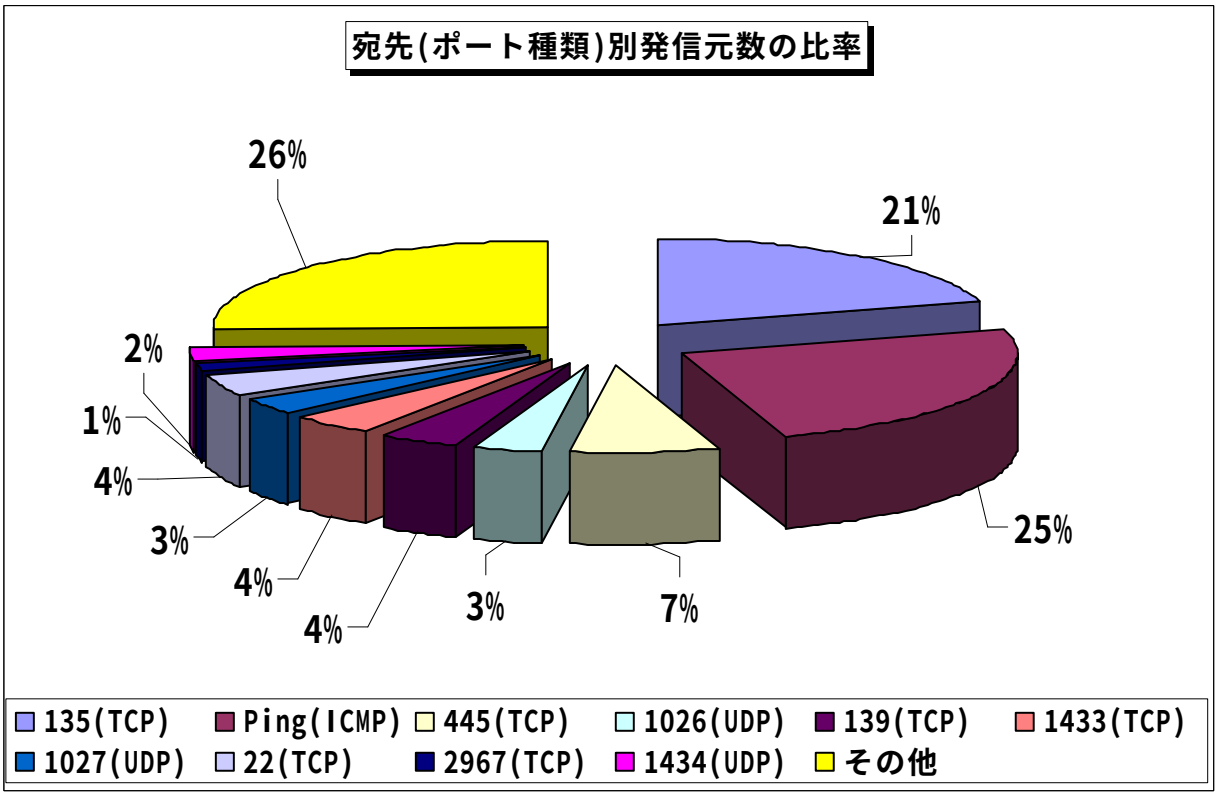
【図 2.2.2 2008 年 10 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 10 月の宛先(ポート種類)別の比率

2008 年 10 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。



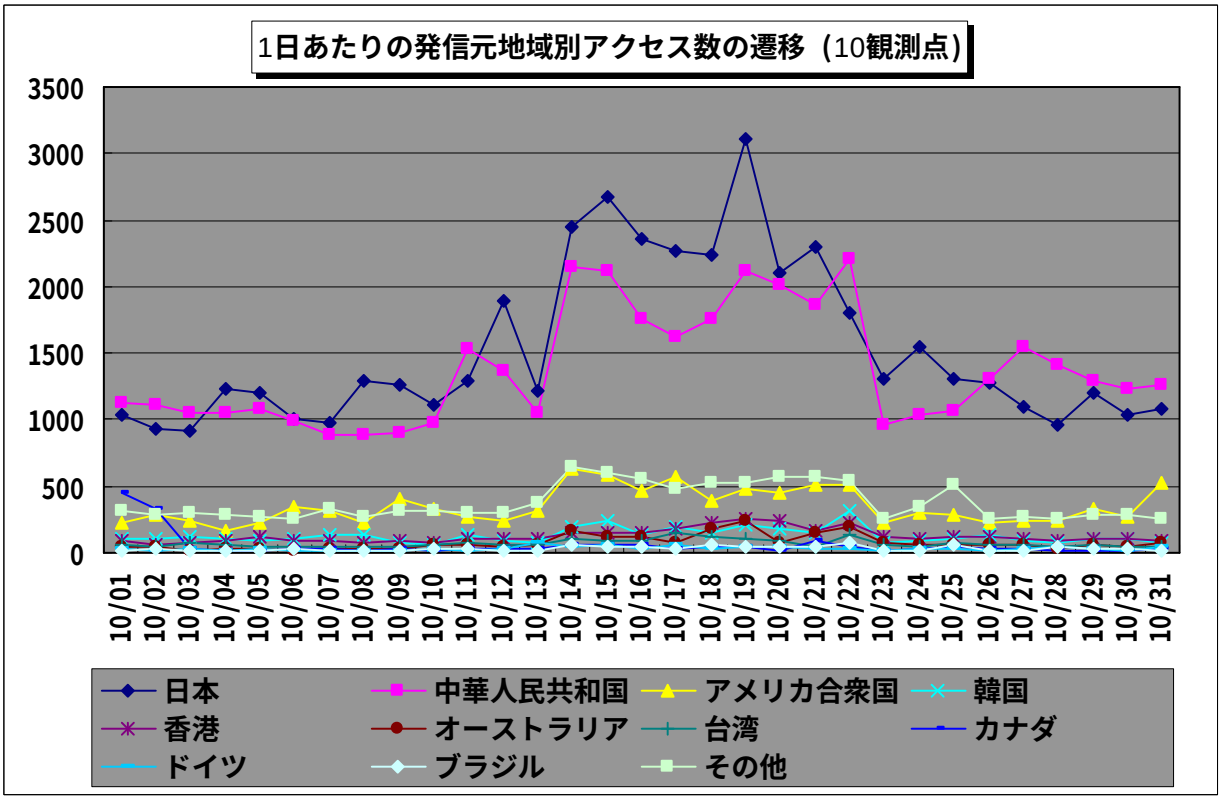
【図 2.3.1 2008 年 10 月の宛先(ポート種類)別アクセス数の比率】



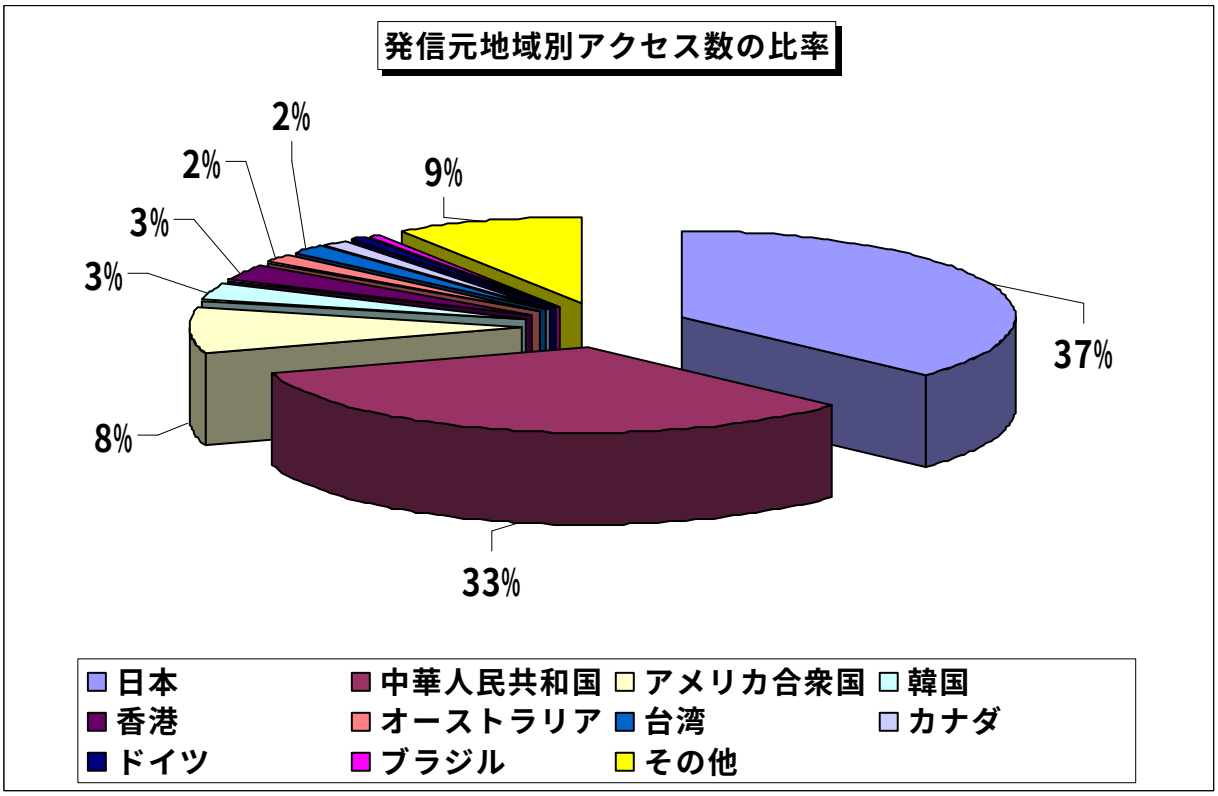
【図 2.3.2 2008 年 10 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 10 月の発信元地域別アクセス状況

2008 年 10 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。

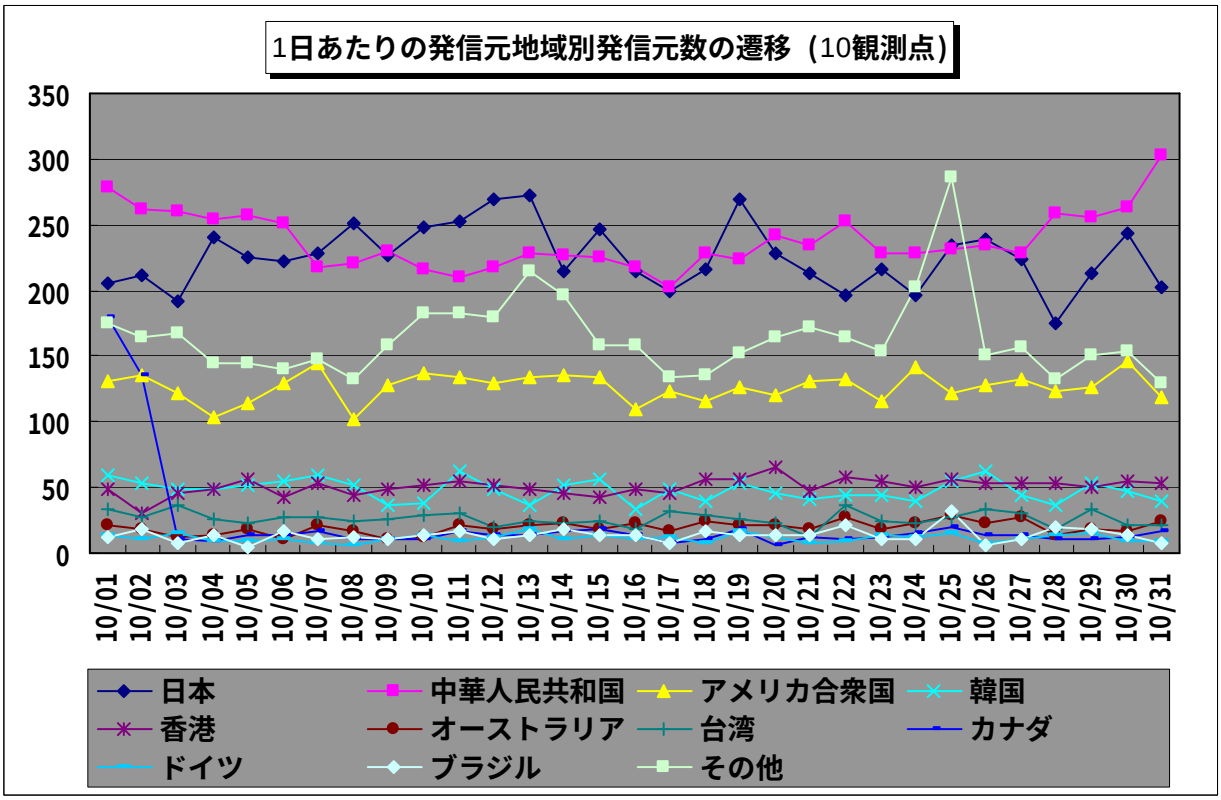


【図 2.4.1 2008 年 10 月の発信元地域別アクセス数の変化】

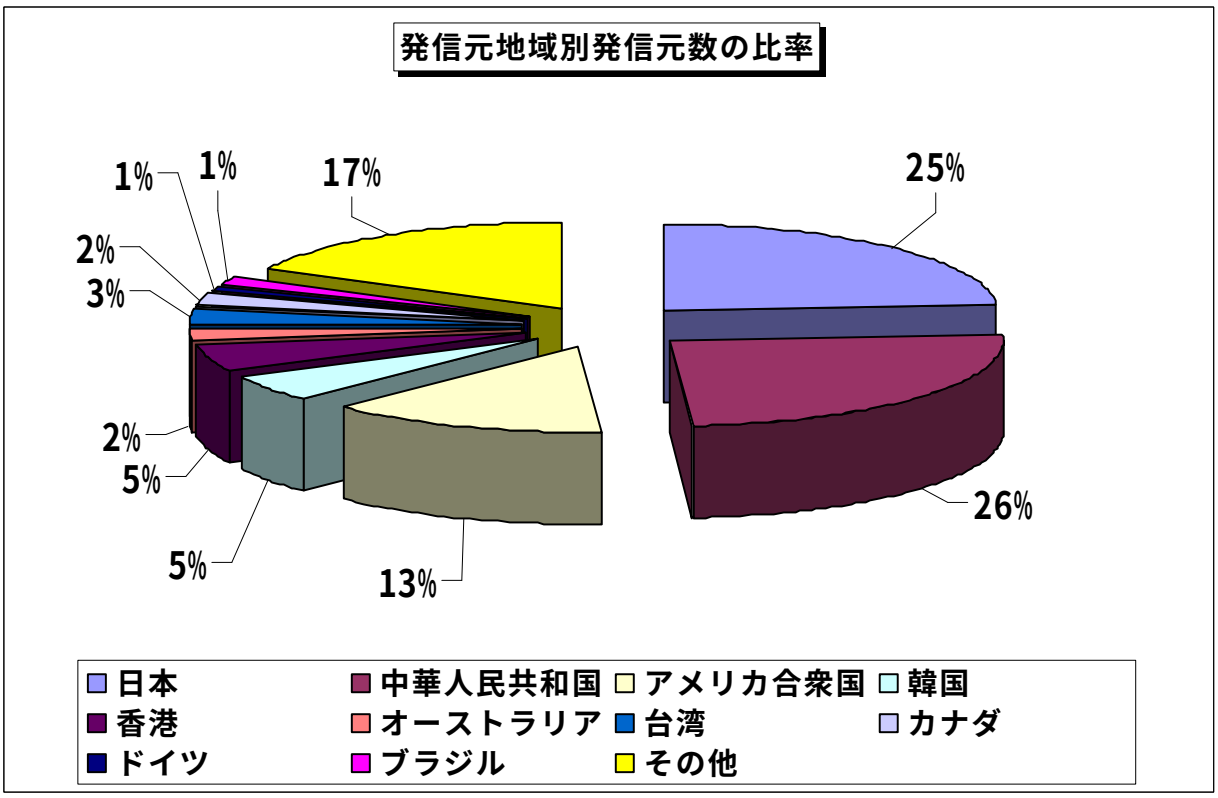


【図 2.4.2 2008 年 10 月の発信元地域別アクセス数の比率】

2008 年 10 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 10 月の発信元地域別発信元数の変化】

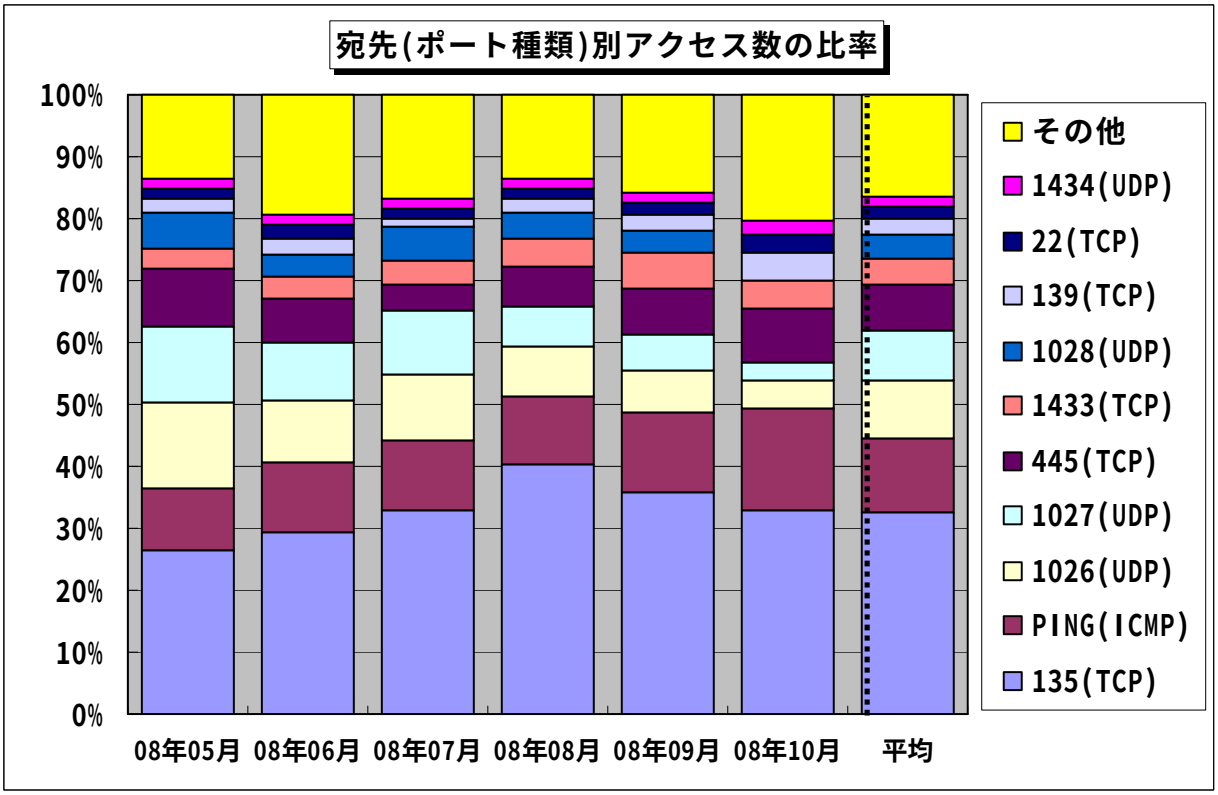


【図 2.4.4 2008 年 10 月の発信元地域別発信元数の比率】

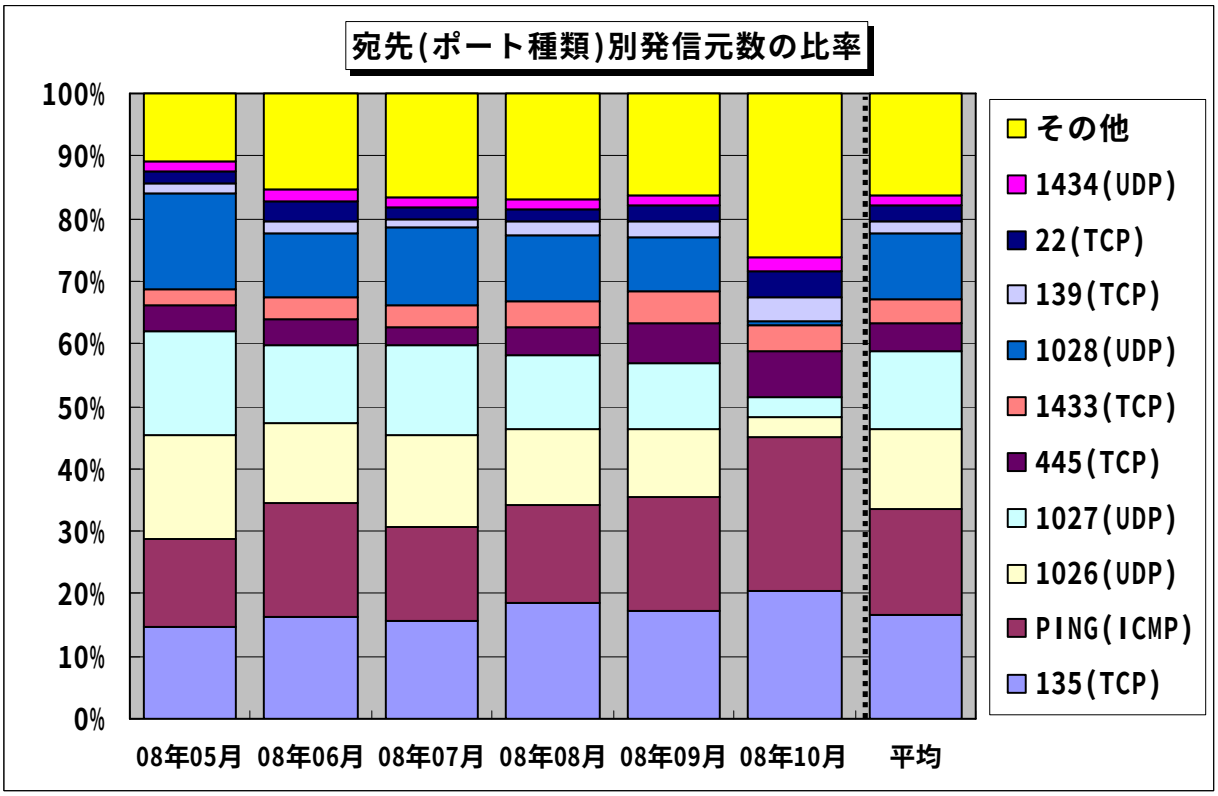
3．統計情報

3.1 2008 年 5 月～2008 年 10 月の宛先(ポート種類)別の比率

2008 年 5 月～2008 年 10 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。



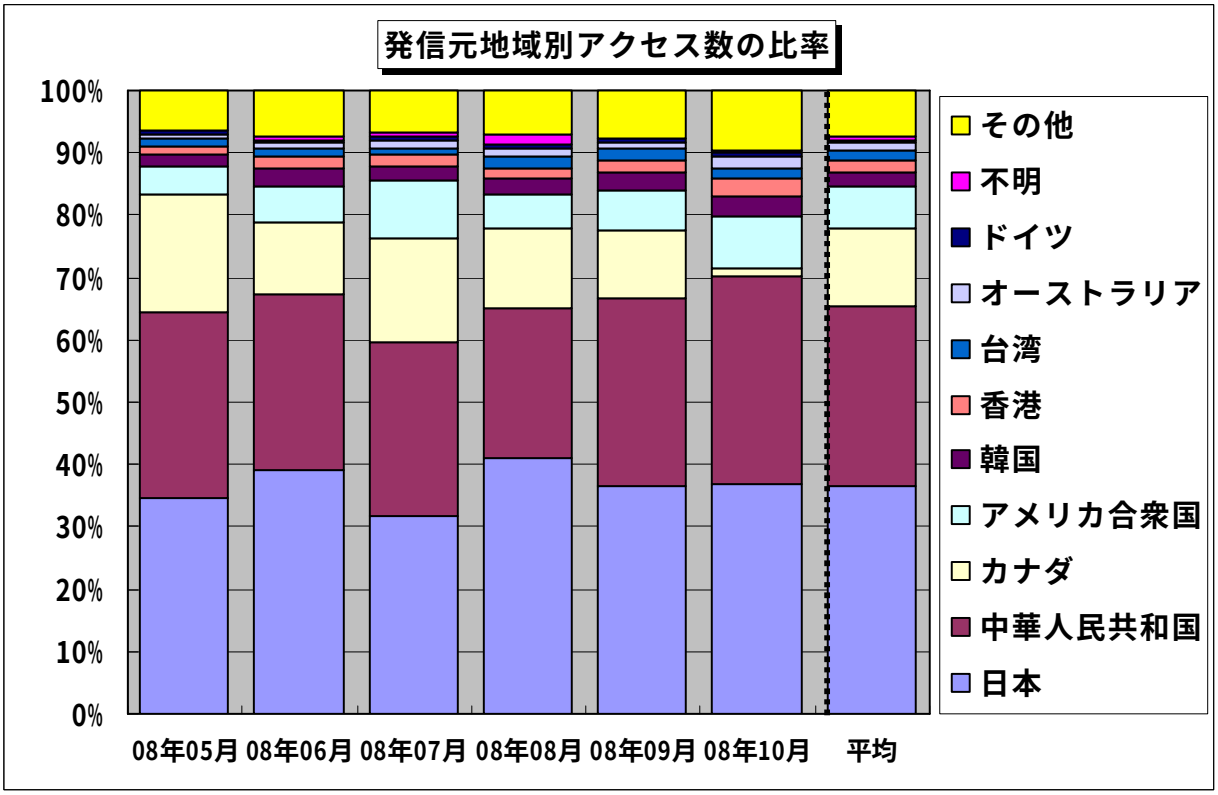
【図 3.1.1 2008 年 5 月～2008 年 10 月の宛先(ポート種類)別アクセス数の比率】



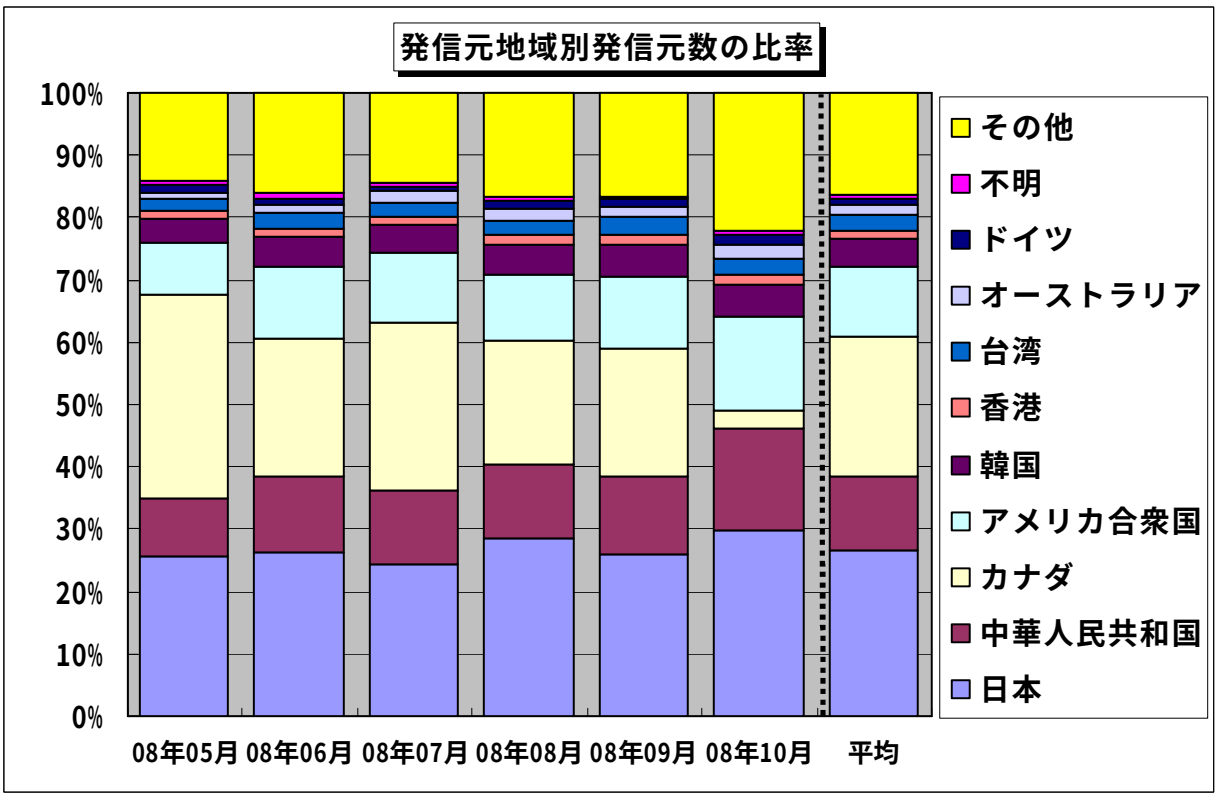
【図 3.1.2 2008 年 5 月～2008 年 10 月の宛先(ポート種類)別発信元数の比率】

3.2 2008 年 5 月～2008 年 10 月の発信元地域別の比率

2008 年 5 月～2008 年 10 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 5 月～2008 年 10 月の発信元地域別アクセス数の比率】



【図 3.2.2 2008 年 5 月～2008 年 10 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 10 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)
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脆弱性を狙ったものと考えられます

■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