別紙 3

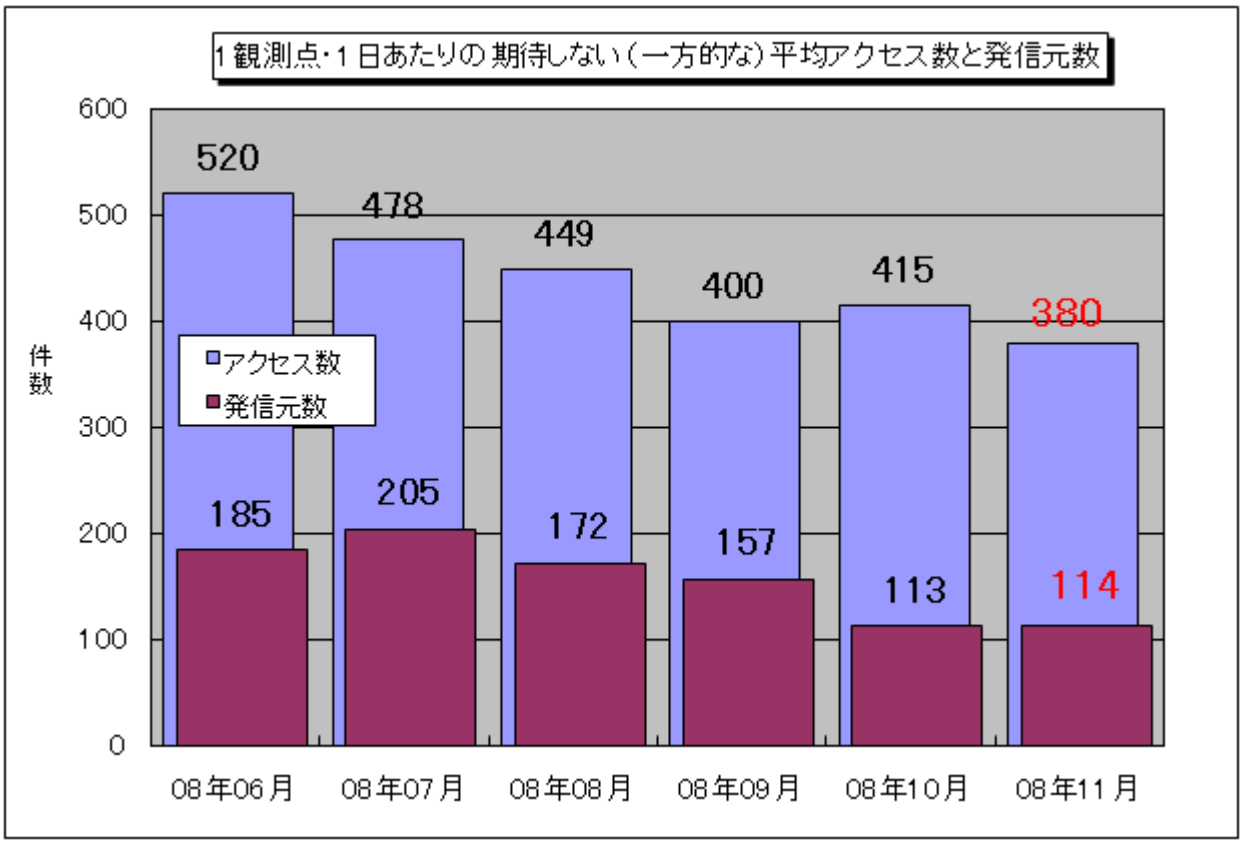
インターネット定点観測(TALOT2)での観測状況について

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 11 月の期待しない(一方的な)アクセスの総数は 10 観測点で 113,906 件、総発信元(※)は 34,179 箇所ありました。平均すると、1 観測点につき 1 日あたり 114 の発信元から 380 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。同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合でも、発信元数は 1 としてカウント。

TALOT2 における各観測点の環境は、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・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

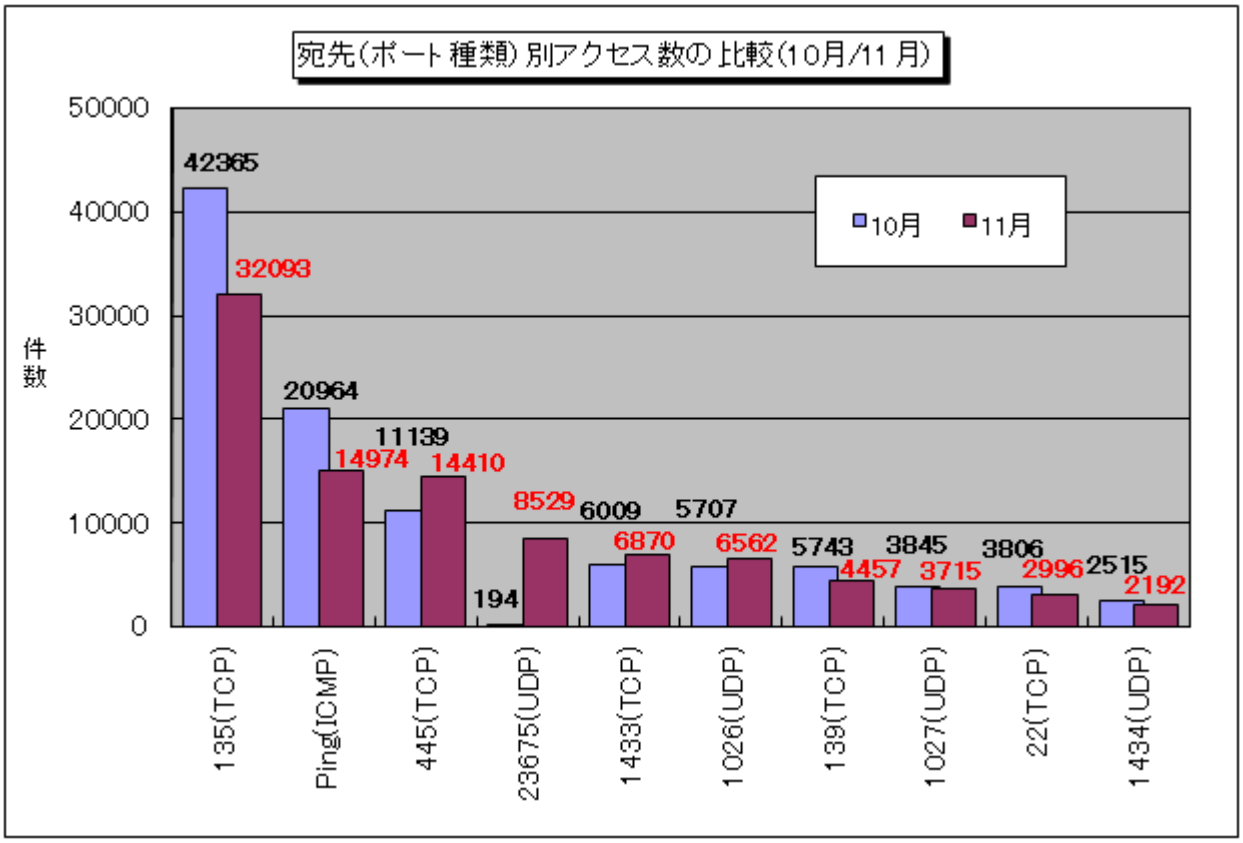
2008 年 6 月～2008 年 11 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、11 月の期待しない(一方的な)アクセスは 10 月と比べて若干減少しました。過去 6 ヶ月を通してみると、減少傾向にあると言えます。

2．11 月のアクセスの状況

2008 年 10 月と 11 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。

10 月よりアクセス数が特に減少したのは、135/tcp および Ping でした。

また、10 月はあまり多くのアクセスがなかった 23675/udp へのアクセスが、多く観測されました。このアクセスが何を目的としたものだったかは不明ですが、アクセス数の約 97%はアメリカ合衆国の 2 か所の発信元からのものだったということは判明しています。



【図 2.1.1　宛先（ポート種類）別アクセス数の比較（10 月/11 月)】

2.1 22/tcp へのアクセス

TALOT2 には、管理上、SSH(*1)を利用している観測点があります。その観測点の 22/tcp (SSH で利用されるポート)に対してアクセス(*2)を行う発信元数が、11 月 20 日に急増したのち、緩やかに減少していきました。

TALOT2 では攻撃の内容を解析していないため、断定はできませんが、このアクセスは日本時間の 11 月 15 日に公開された SSH の脆弱性を突く、攻撃を行うための探索行為であった可能性があります。

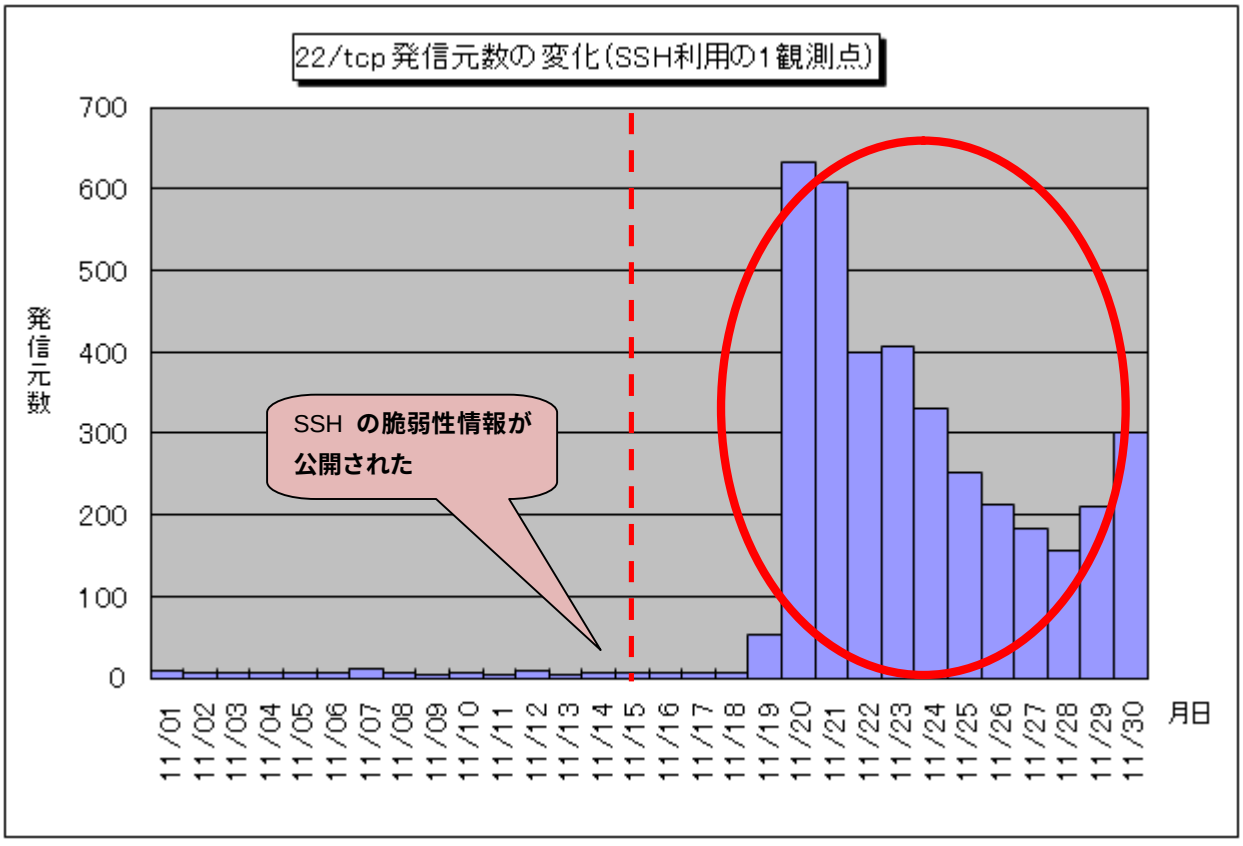
＜参考情報＞

■「SSH 通信において一部データが漏えいする可能性」(JVN)
http://jvn.jp/niscc/CPNI-957037/

TALOT2 で管理上、SSH を利用している観測点の 22/tcp へのアクセスの発信元数の変化を図 2.1.2 に示します。

(*1)SSH (Secure SHell) … ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。

(*2)SSH を利用している観測点に対する 22/tcp への観測データは、アクセスに対する応答を行わない他の観測データとは異なるため、統計情報からは除外してあります。



【図 2.1.2　22/tcp への発信元数の変化（SSH 利用の 1 観測点)】

脆弱性情報が公開されると、短期間でその脆弱性に関連したアクセスが増えることがあります。サーバ管理者の方は、日頃から JVN などの脆弱性対策情報ポータルサイトを確認して、お使いのシステムの脆弱性対策を迅速に行えるようにしてください。

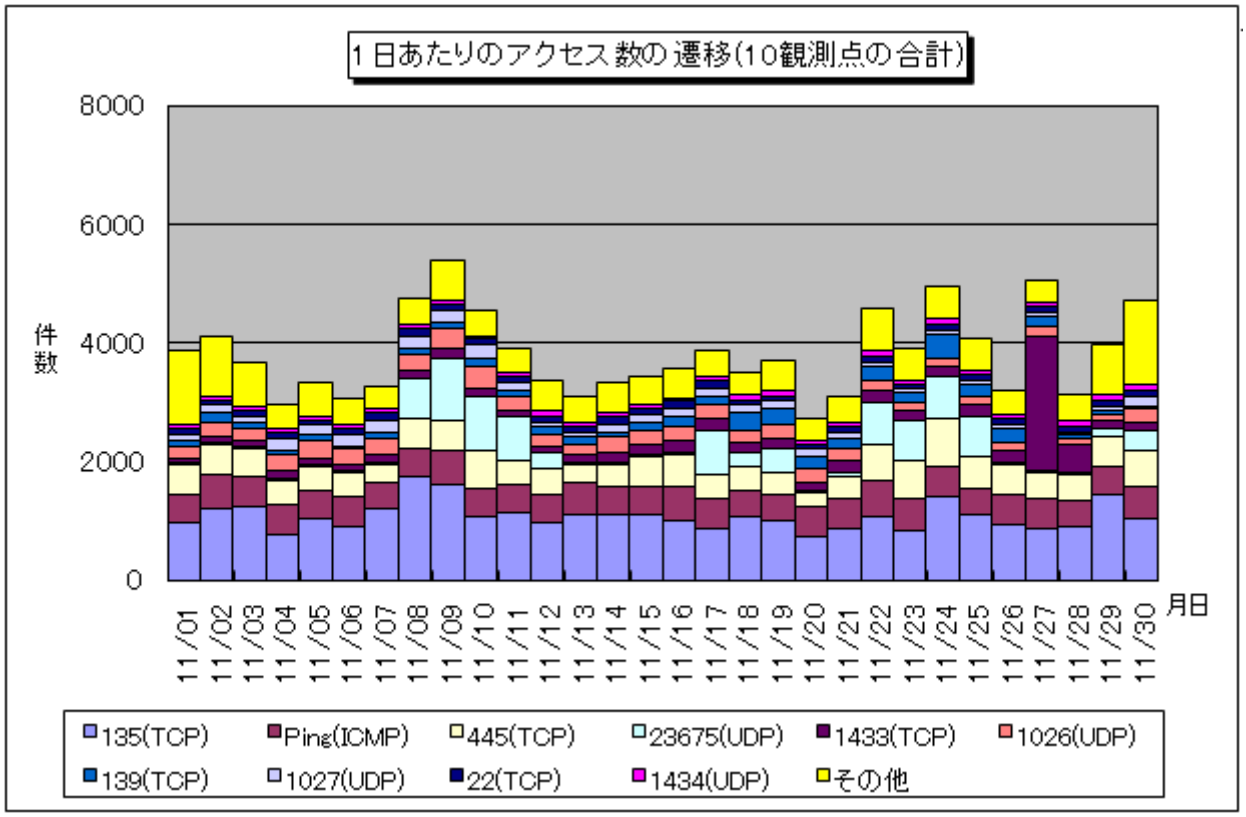
＜参考情報＞

■「JVN (Japan Vulnerability Notes)」（脆弱性対策情報ポータルサイト）
http://jvn.jp/

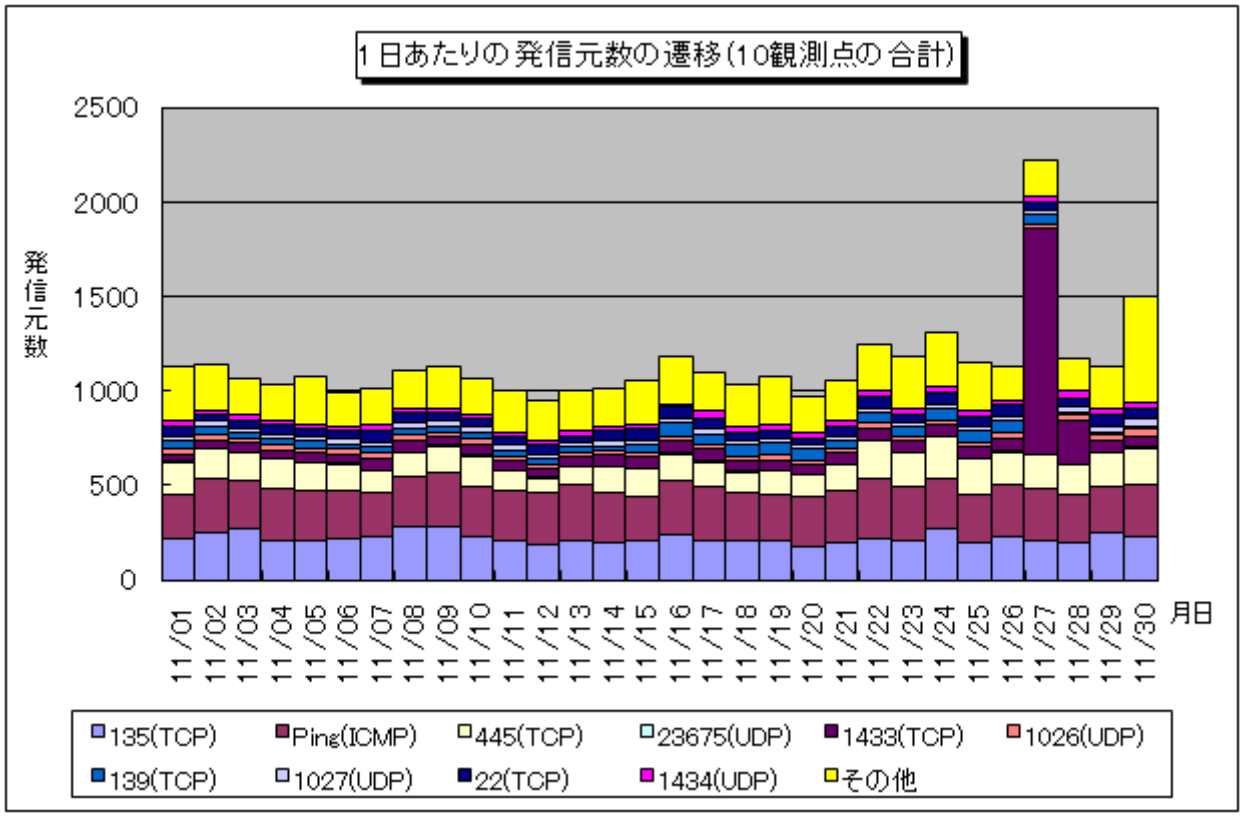
■「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

2.2 2008 年 11 月の一方的なアクセス状況

2008 年 11 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。



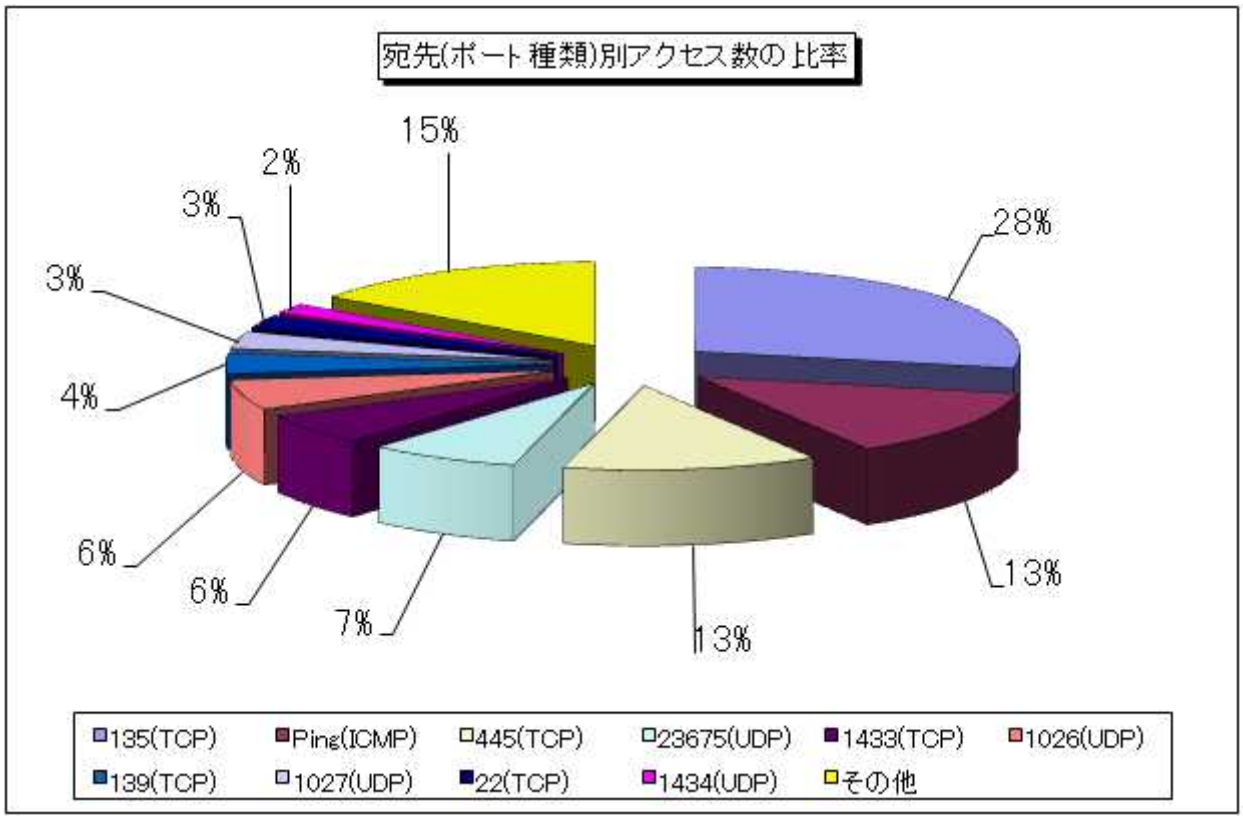
【図 2.2.1 2008 年 11 月の 1 日あたりのアクセス数の遷移】



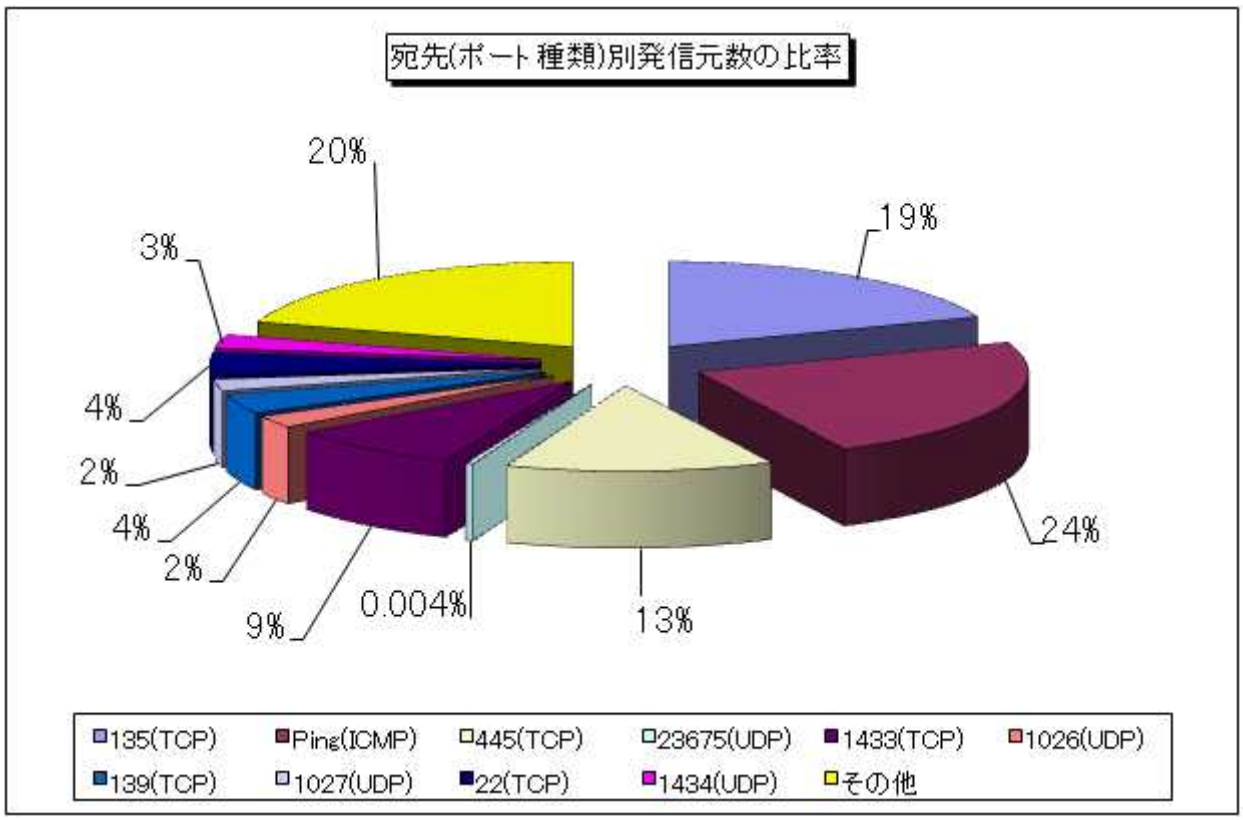
【図 2.2.2 2008 年 11 月の 1 日あたりの発信元数の遷移】

2.3 2008 年 11 月の宛先(ポート種類)別の比率

2008 年 11 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。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



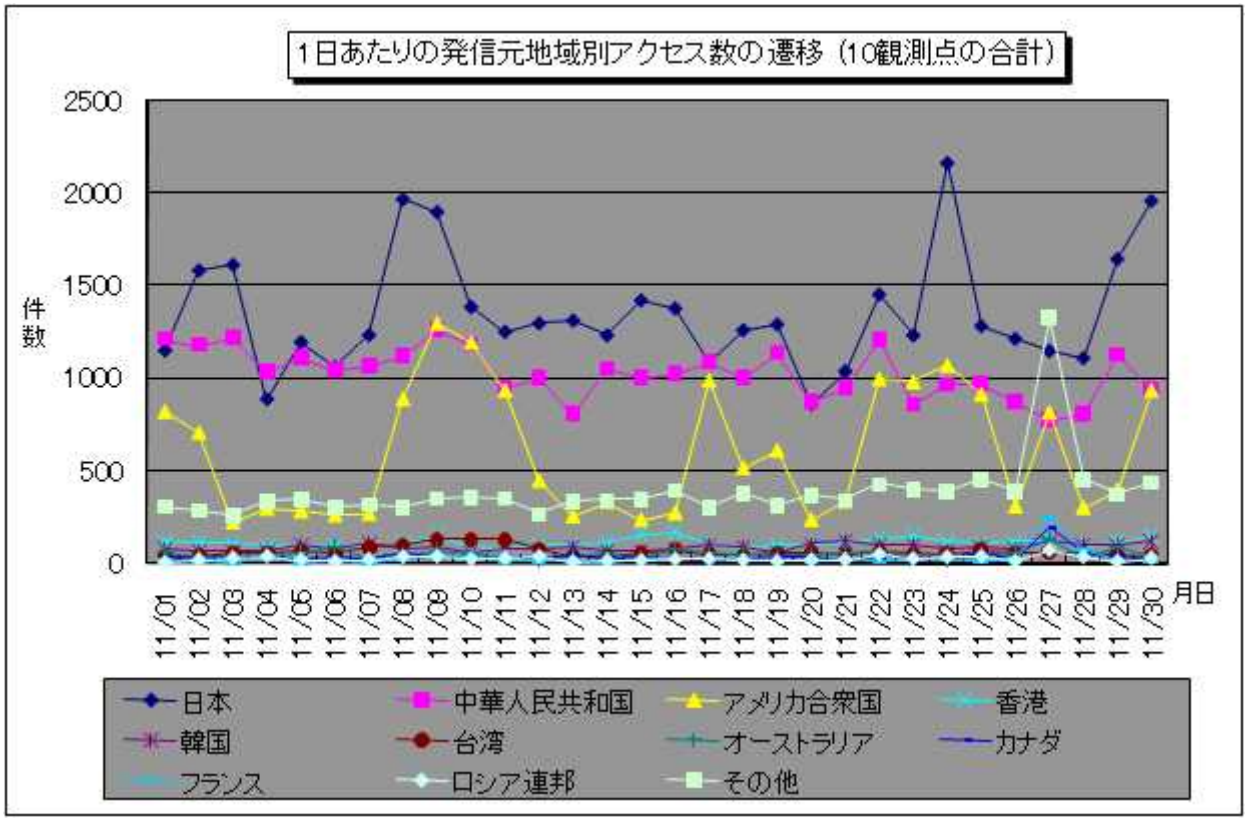
【図 2.3.1 2008 年 11 月の宛先(ポート種類)別アクセス数の比率】



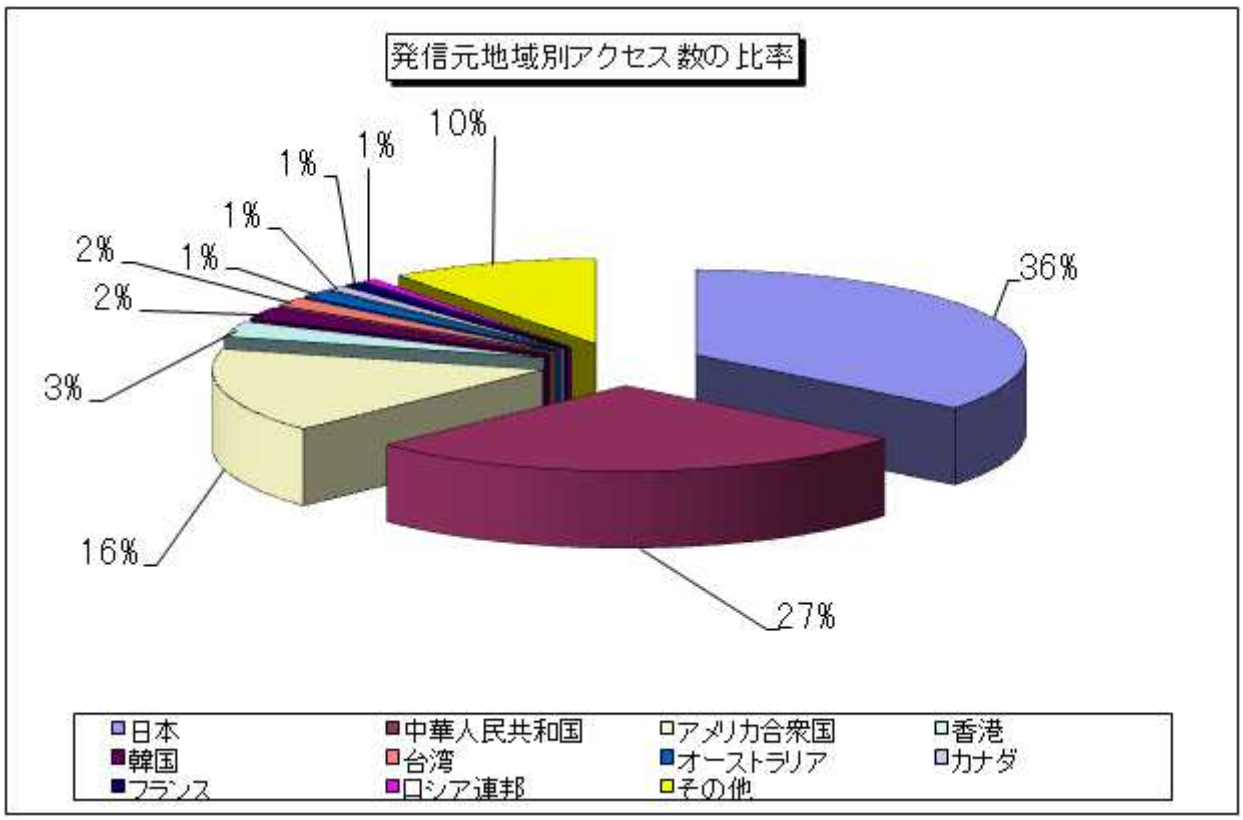
【図 2.3.2 2008 年 11 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 11 月の発信元地域別アクセス状況

2008 年 11 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。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。

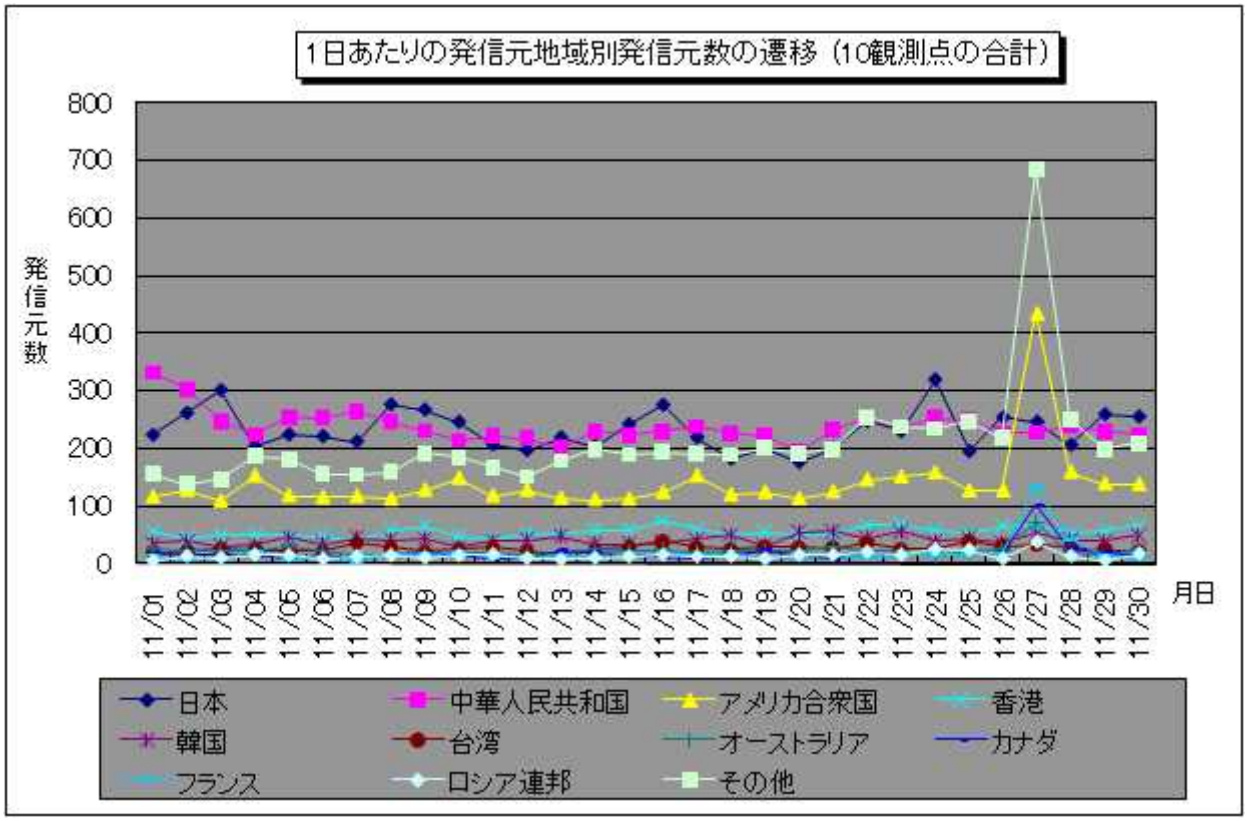


【図 2.4.1 2008 年 11 月の 1 日あたりの発信元地域別アクセス数の遷移】

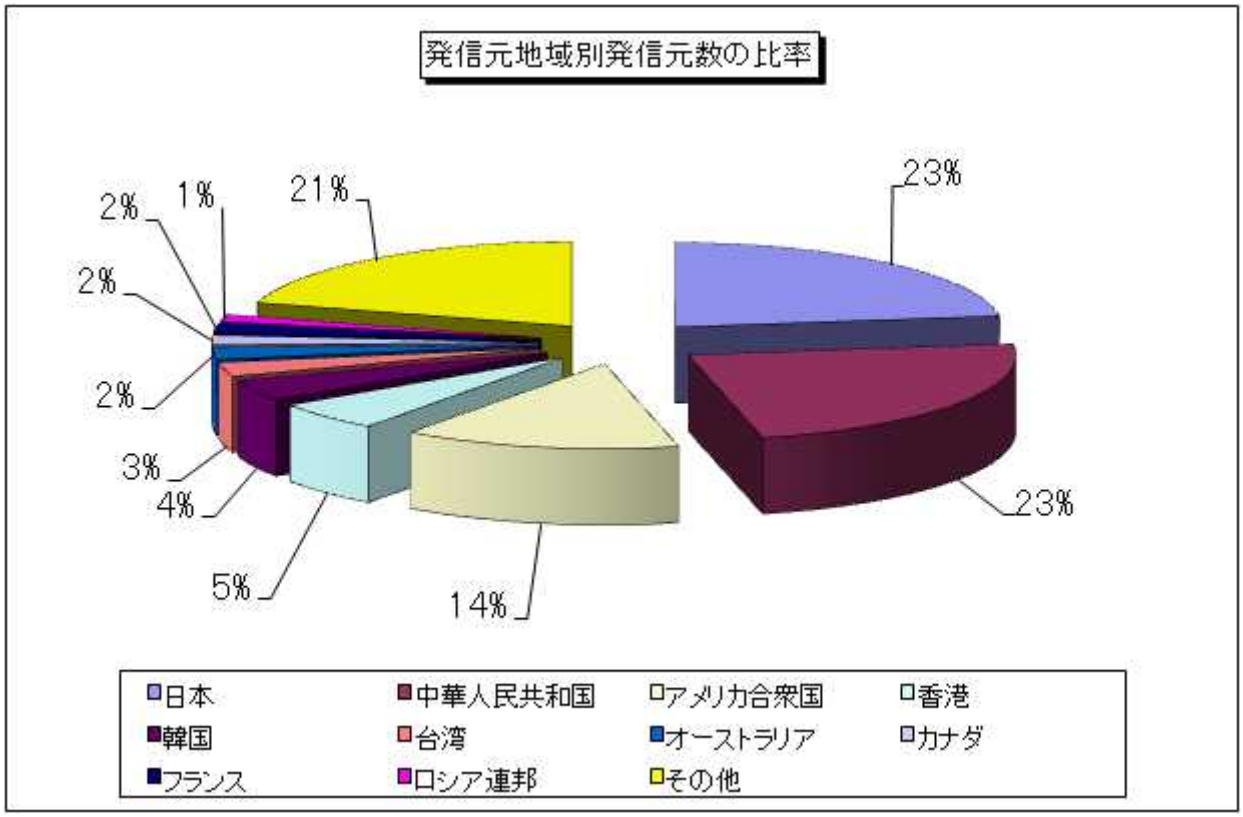


【図 2.4.2 2008 年 11 月の発信元地域別アクセス数の比率】

2008 年 11 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。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



【図 2.4.3 2008 年 11 月の 1 日あたりの発信元地域別発信元数の遷移】

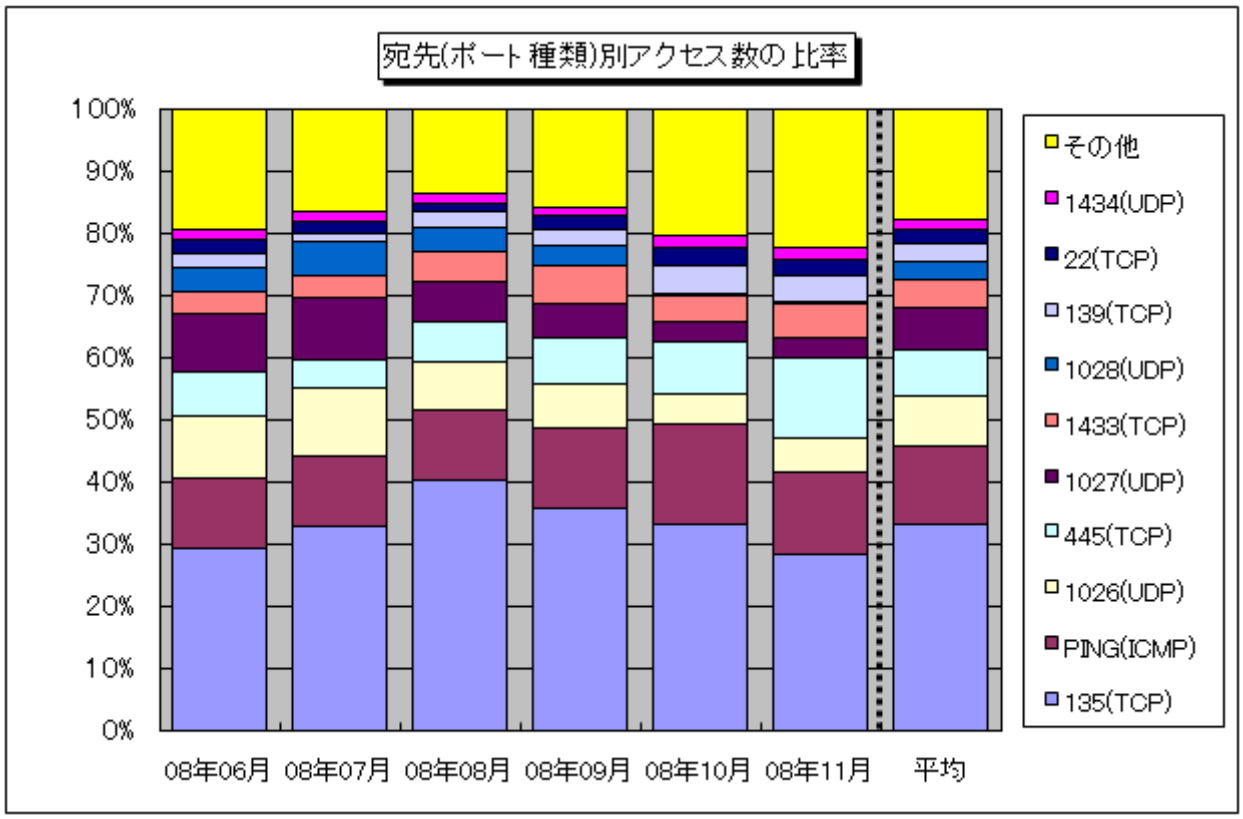


【図 2.4.4 2008 年 11 月の発信元地域別発信元数の比率】

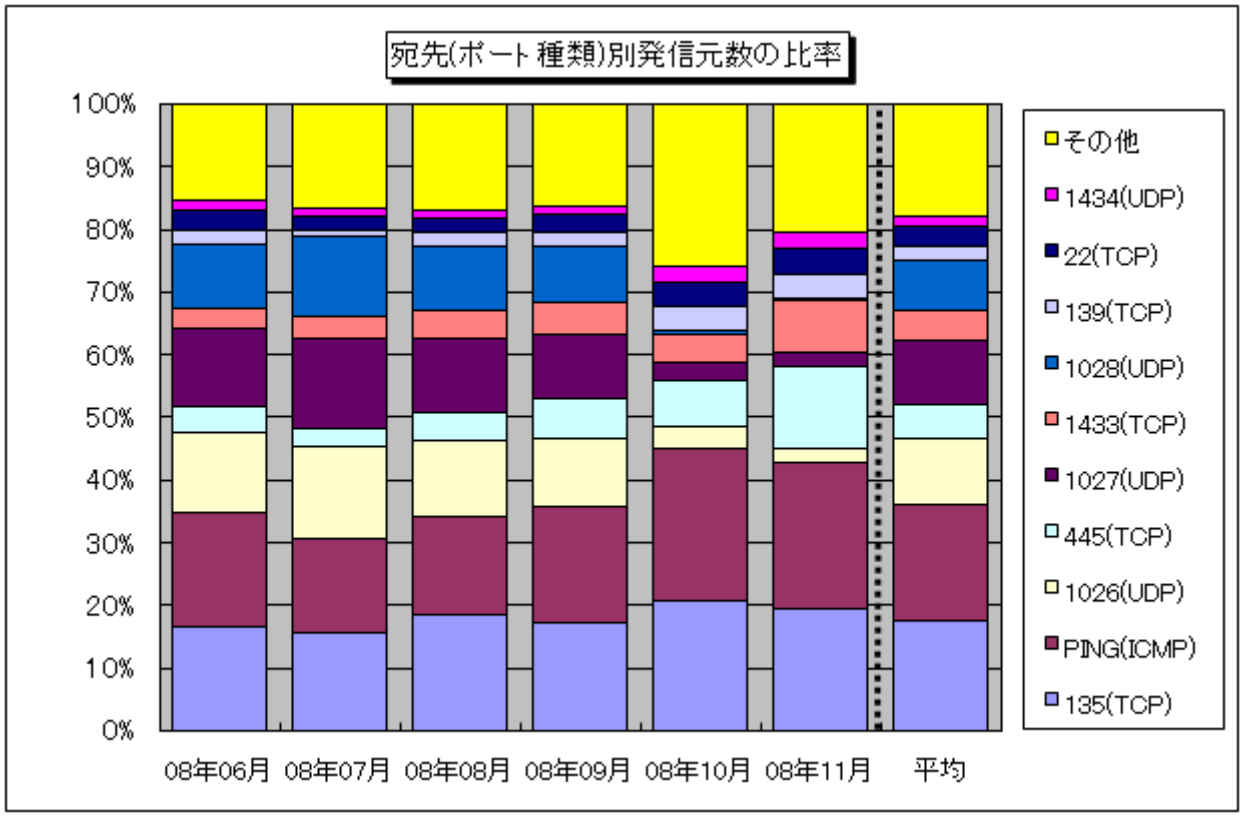
3．統計情報

3.1 2008 年 6 月～2008 年 11 月の宛先(ポート種類)別の比率

2008 年 6 月～2008 年 11 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。



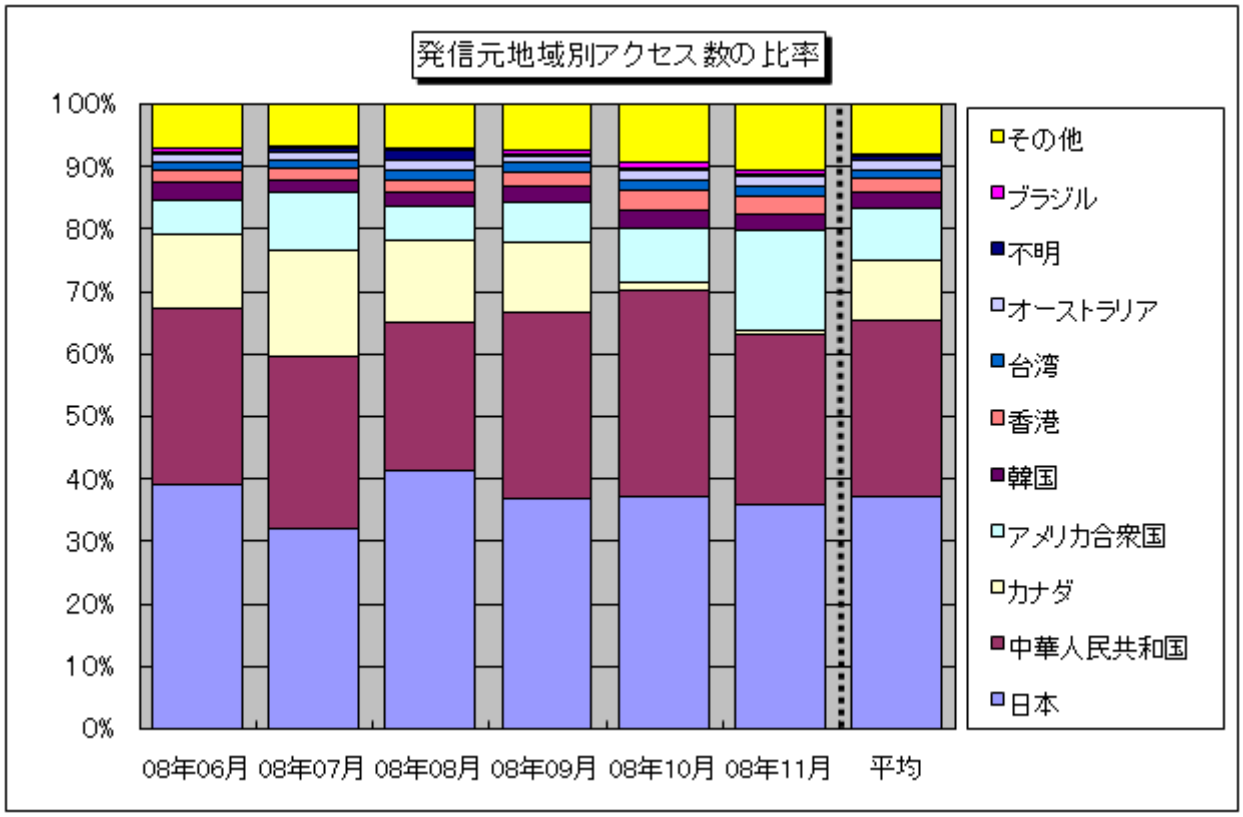
【図 3.1.1 2008 年 6 月～2008 年 11 月の宛先(ポート種類)別アクセス数の比率】



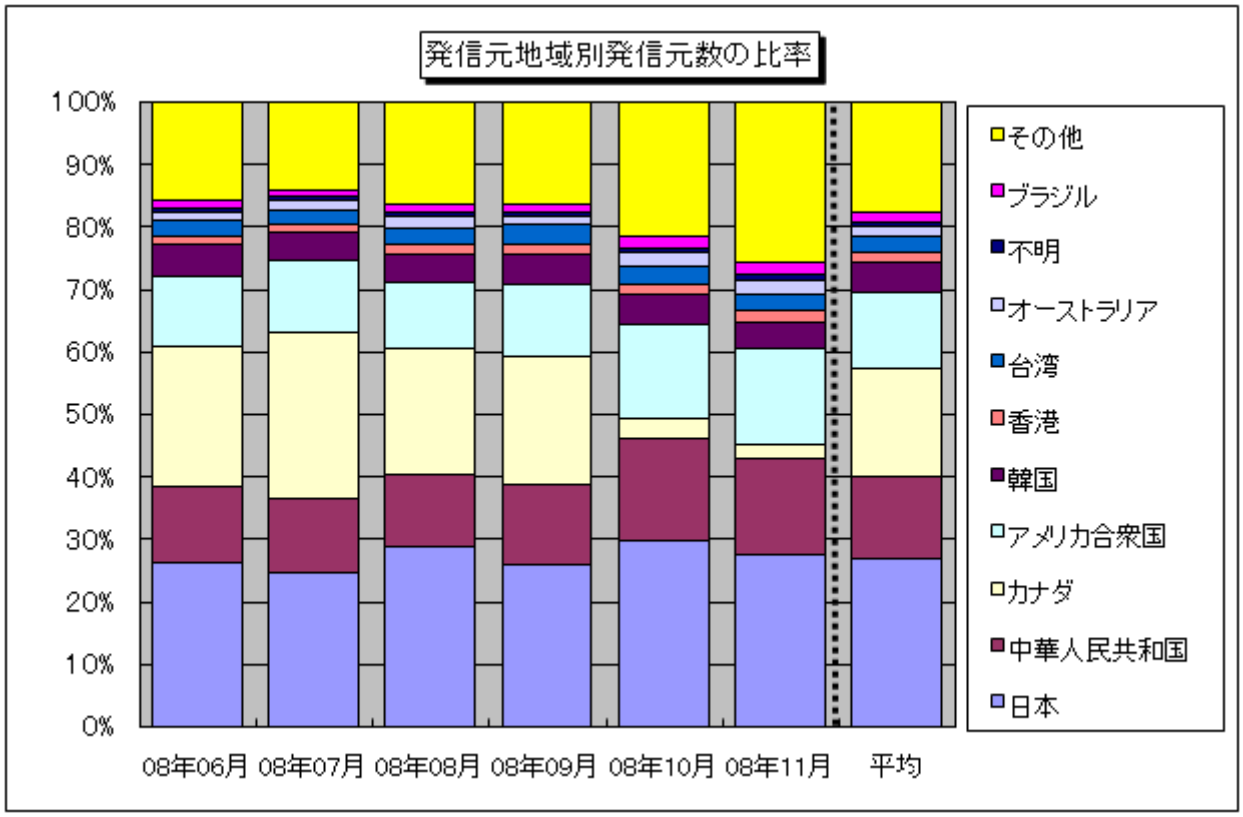
【図 3.1.2 2008 年 6 月～2008 年 11 月の宛先(ポート種類)別発信元数の比率】

3.2 2008 年 6 月～2008 年 11 月の発信元地域別の比率

2008 年 6 月～2008 年 11 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 6 月～2008 年 11 月の発信元地域別アクセス数の比率】



【図 3.2.2 2008 年 6 月～2008 年 11 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 11 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 … ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ)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)
23675（UDP）	目的不明のアクセスです

■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