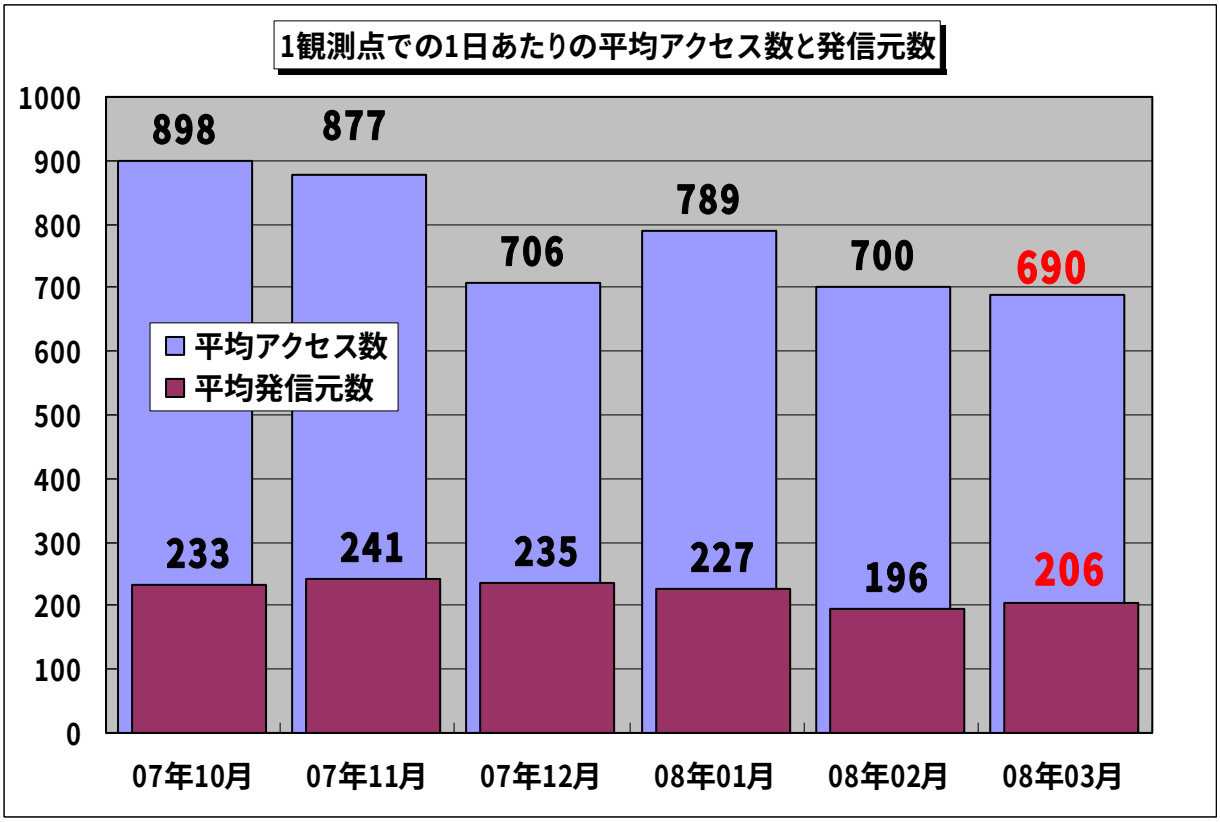
別紙 3

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 3 月の期待しない（一方的な）アクセスの総数は、10 観測点で **213,755 件**ありました。1 観測点で 1 日あたり **206** の発信元から **690 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、206 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。

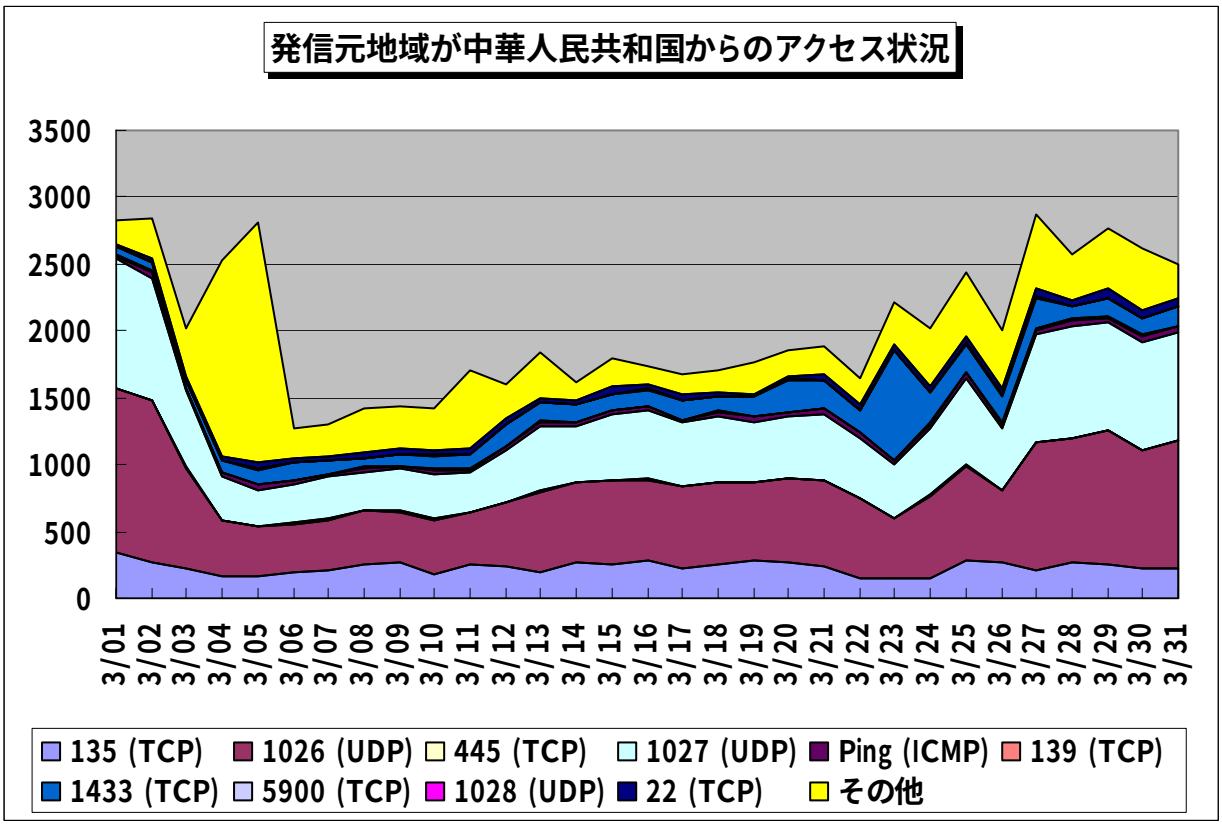


【図 1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

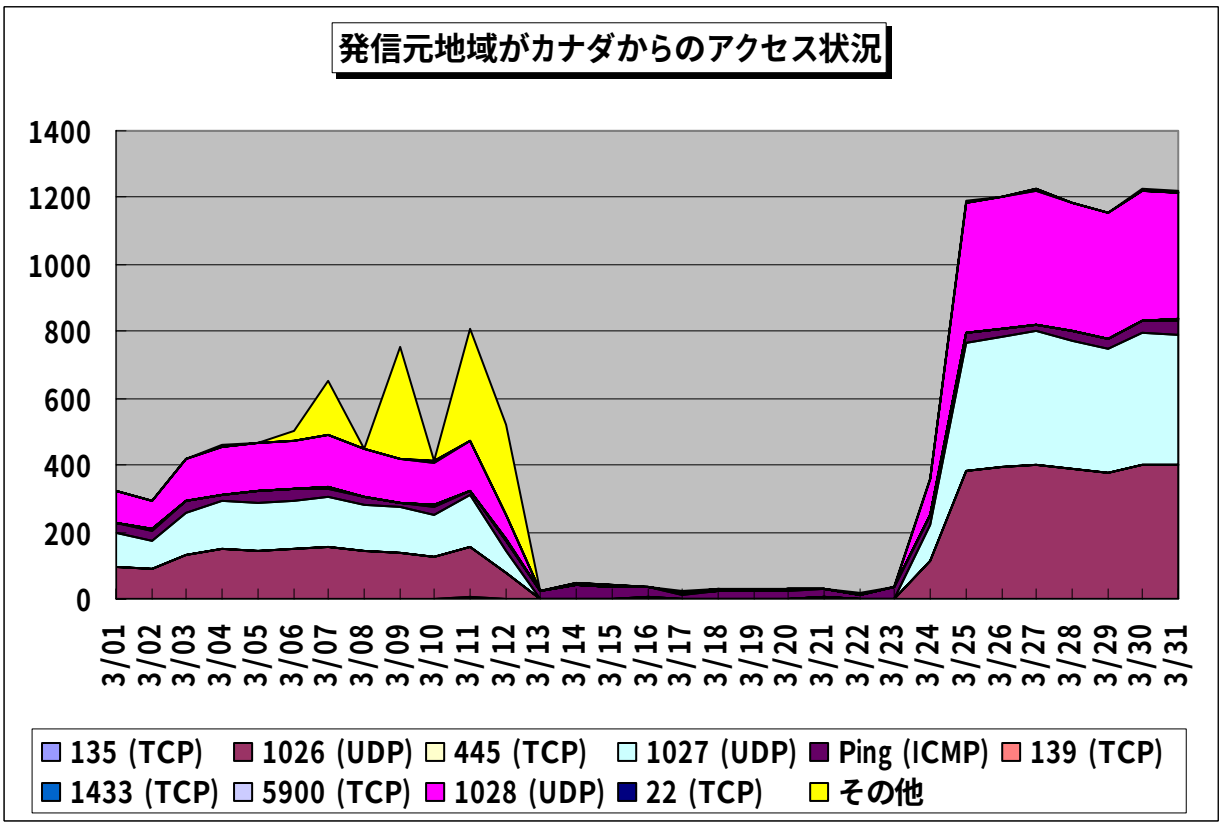
2007 年 10 月～2008 年 3 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、3 月の期待しない（一方的な）アクセスは 2 月よりも減少しましたが、全体的なアクセスの内容としては、定常化していると言えます。

2．3 月のアクセスの状況

2008 年 3 月のアクセス状況は、2 月よりも減少しました。これは、全体のアクセス数そのものが減少したためです。特に発信地域元が中華人民共和国からの、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、1026/udp、1027/udp へのアクセスや、発信元地域がカナダからの 1028/udp へのアクセスが、一定期間ですが減少しました。（図 2.1、2.2 参照）



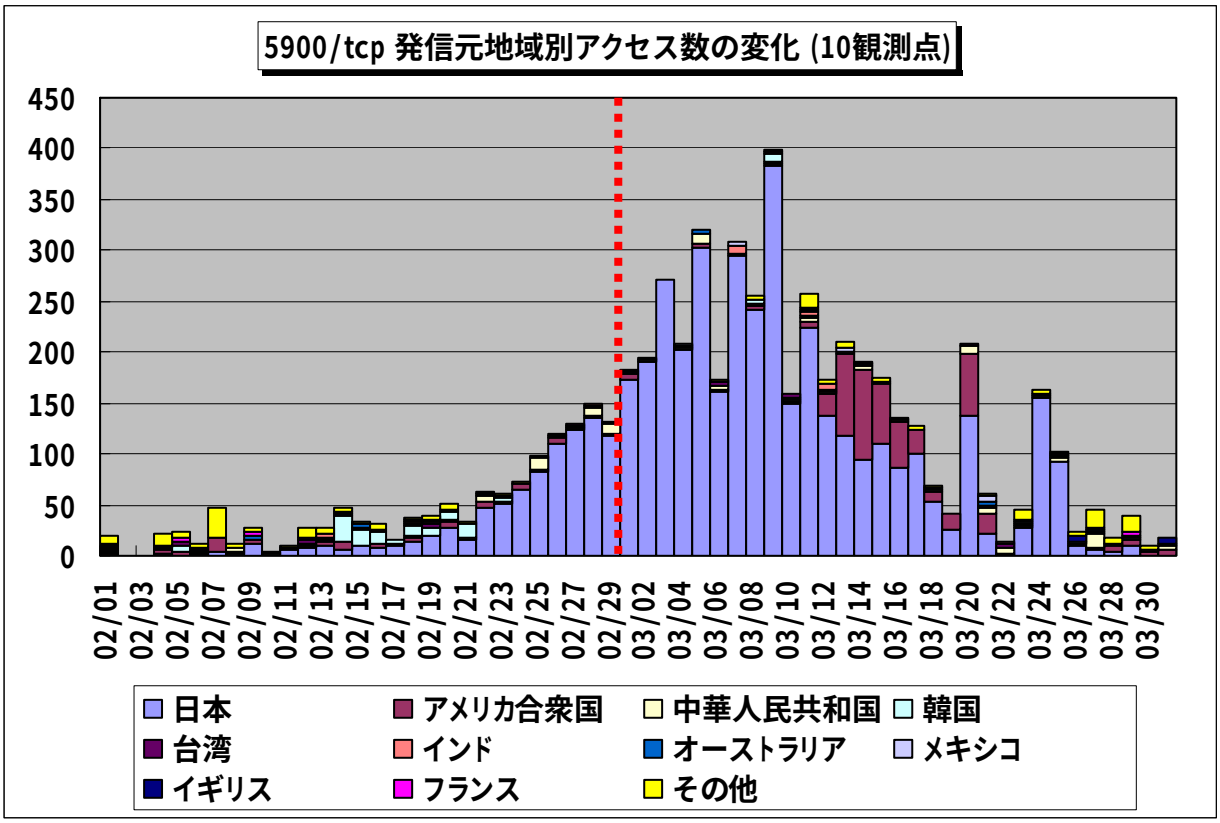
【図 2.1　2008 年 3 月　発信元地域が中華人民共和国からのアクセス状況】



【図 2.2　2008 年 3 月　発信元地域がカナダからのアクセス状況】

2 月の後半から増加していた、5900/tcp（コンピュータを遠隔操作するためのソフトウェア、RealVNCが使用するデフォルトのポート）へのアクセスは、3 月の始めまで増加しました（図 2.3 参照）。現在は落ち着いた感じには見えますが、引き続き注意が必要です。

（参考情報）
■ 2008 年 3 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/2008/documents/TALOT2-0803.pdf



【図 2.1　2008 年 2 月～3 月　5900/tcp ポートへの発信元地域別アクセス数の変化】

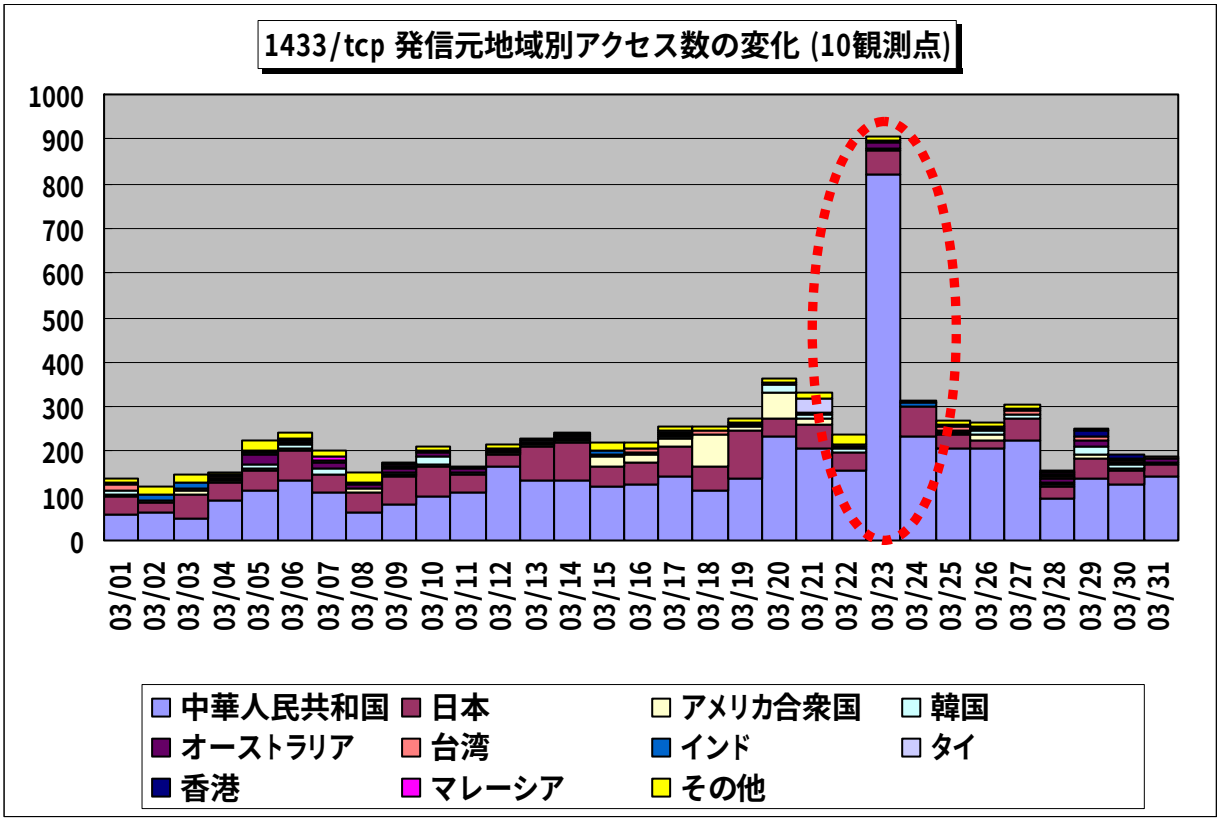
2.1. 1433/tcp へのアクセス

Microsoft SQL Server の脆弱性を狙っていると思われる、1433/tcp へのアクセスも一時的に増加しました。こちらは主に、発信元地域が中華人民共和国からのアクセスが多く観測されました。（図 2.1.1 参照）

こちらも、一時的に多く観測されているだけに見えますが、このアクセスの中には、Windows の脆弱性を狙った 135/tcp、139/tcp、445/tcp も同時にアクセスするものも見受けられることから、ツールによって攻撃されている可能性が高く、既知の脆弱性を狙って、広範囲に攻撃を行っている可能性も考えられます。

Windows も含め、使用されているアプリケーションソフトの脆弱性情報を今一度再確認し、コンピュータに脆弱性がないかを確認し、常に最新の状態に保つことを心掛けて下さい。

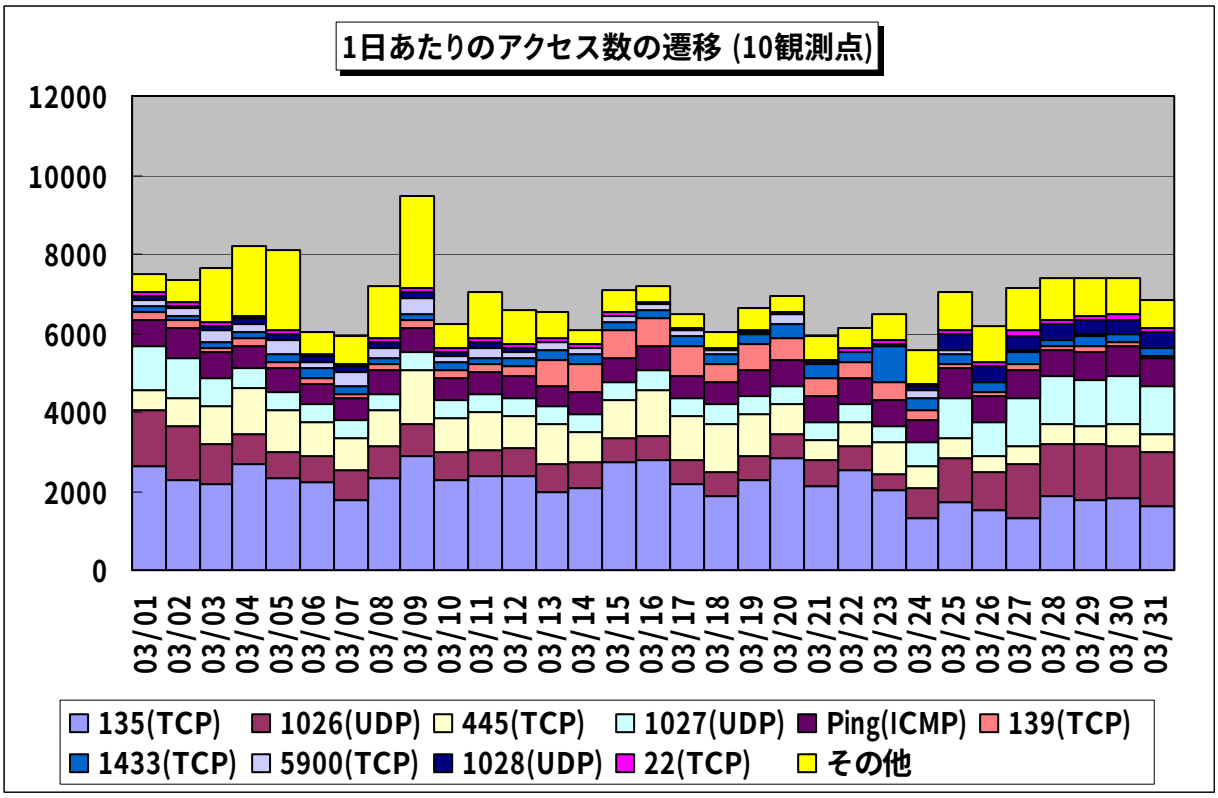
（参考情報）
■「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/



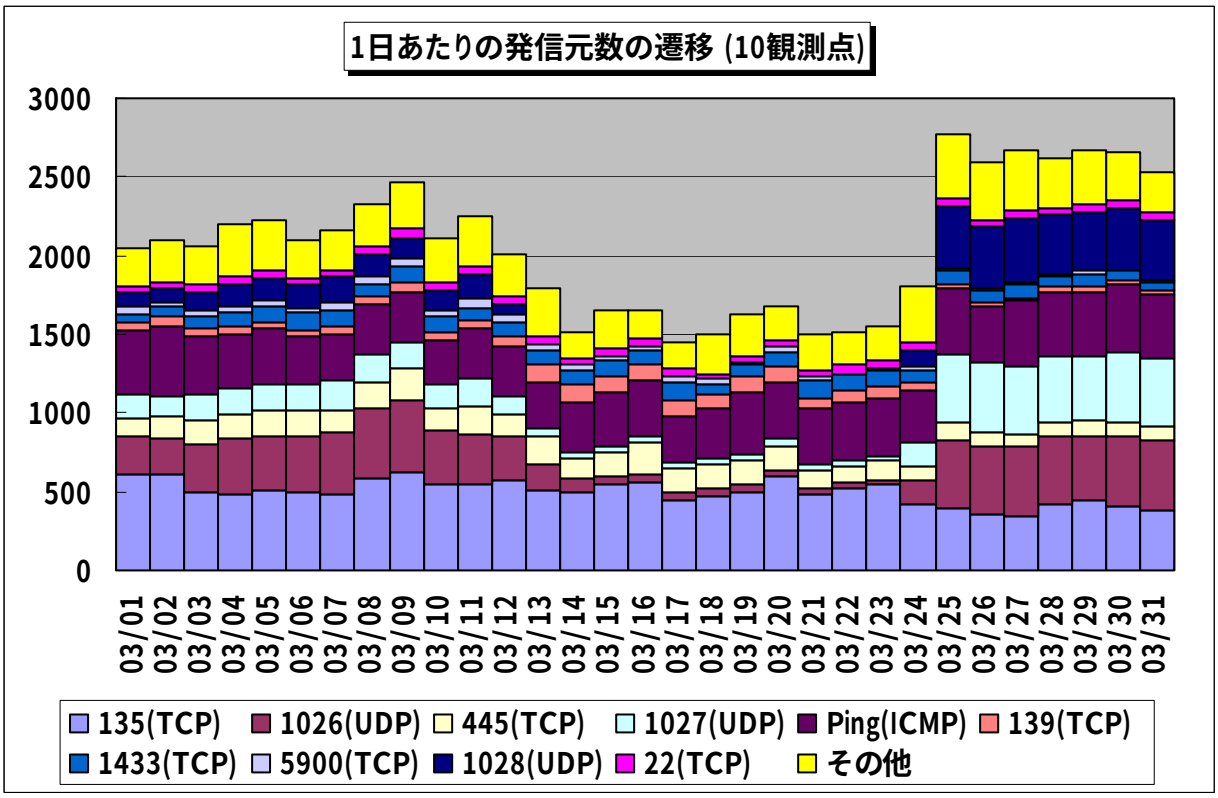
【図 2.1.1　1433/tcp ポートへの発信元地域別アクセス数の変化】

2.2 2008 年 3 月の一方的なアクセス状況

2008 年 3 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。



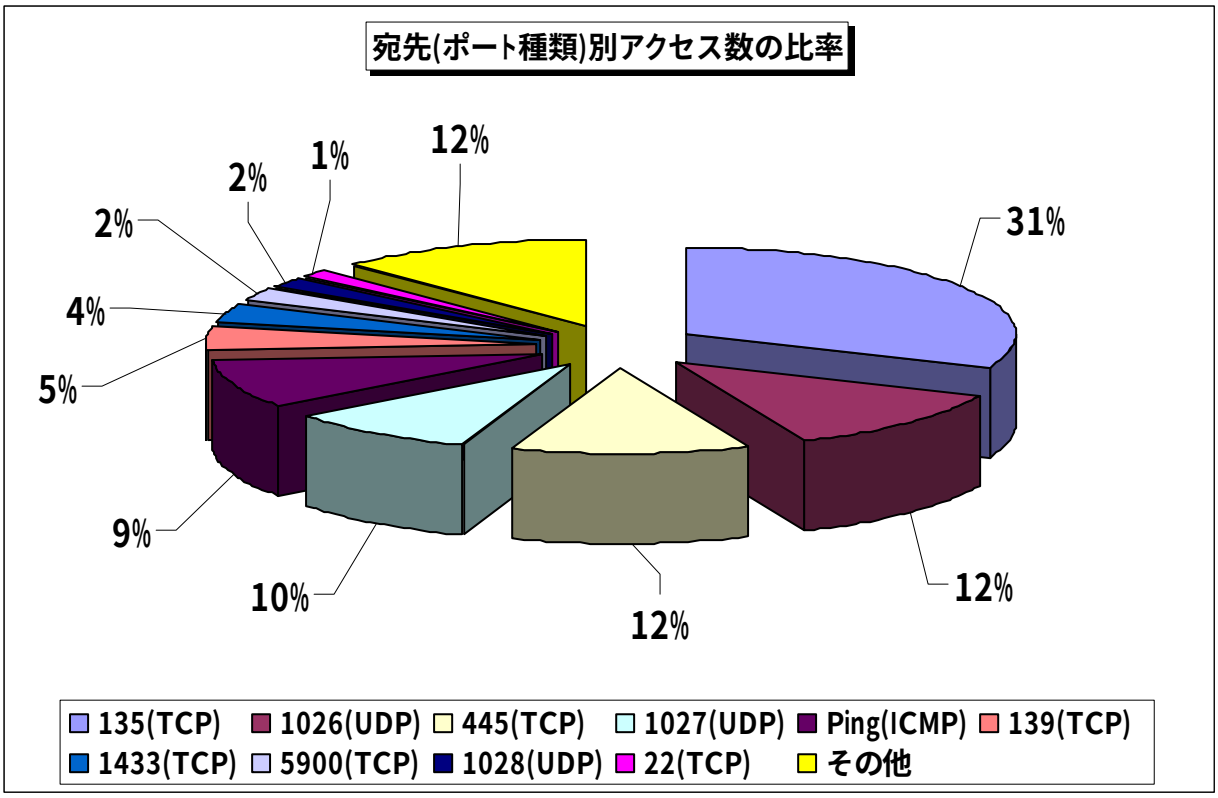
【図 2.2.1 2008 年 3 月の一方的なアクセス状況(アクセス数)】



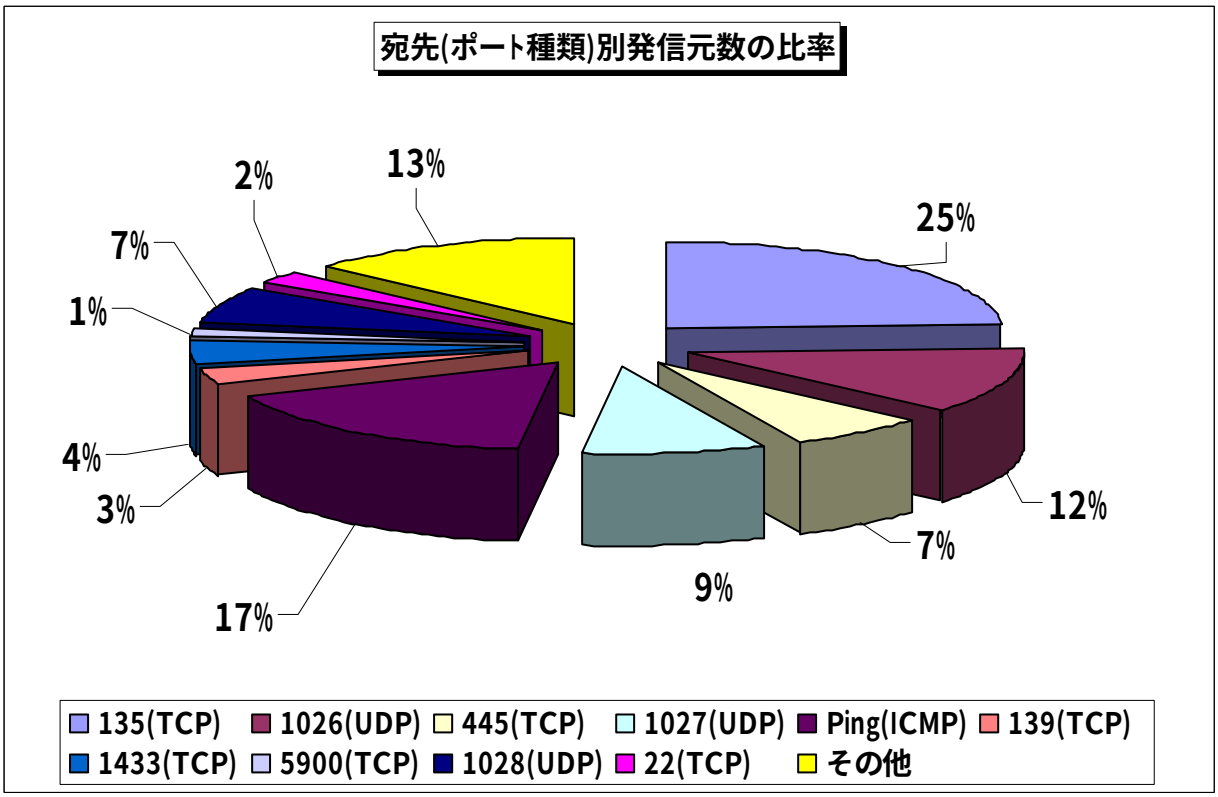
【図 2.2.2 2008 年 3 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 3 月の宛先(ポート種類)別の比率

2008 年 3 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。



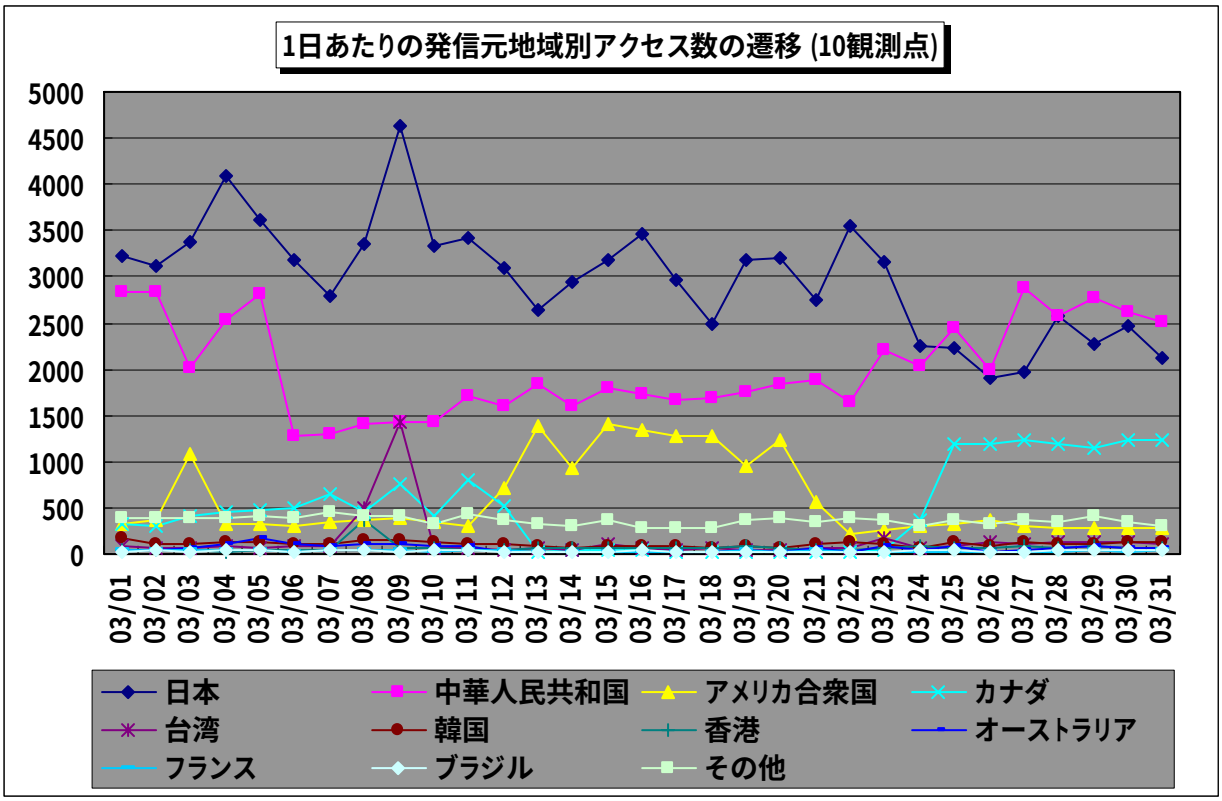
【図 2.3.1 2008 年 3 月の宛先(ポート種類)別アクセス数の比率】



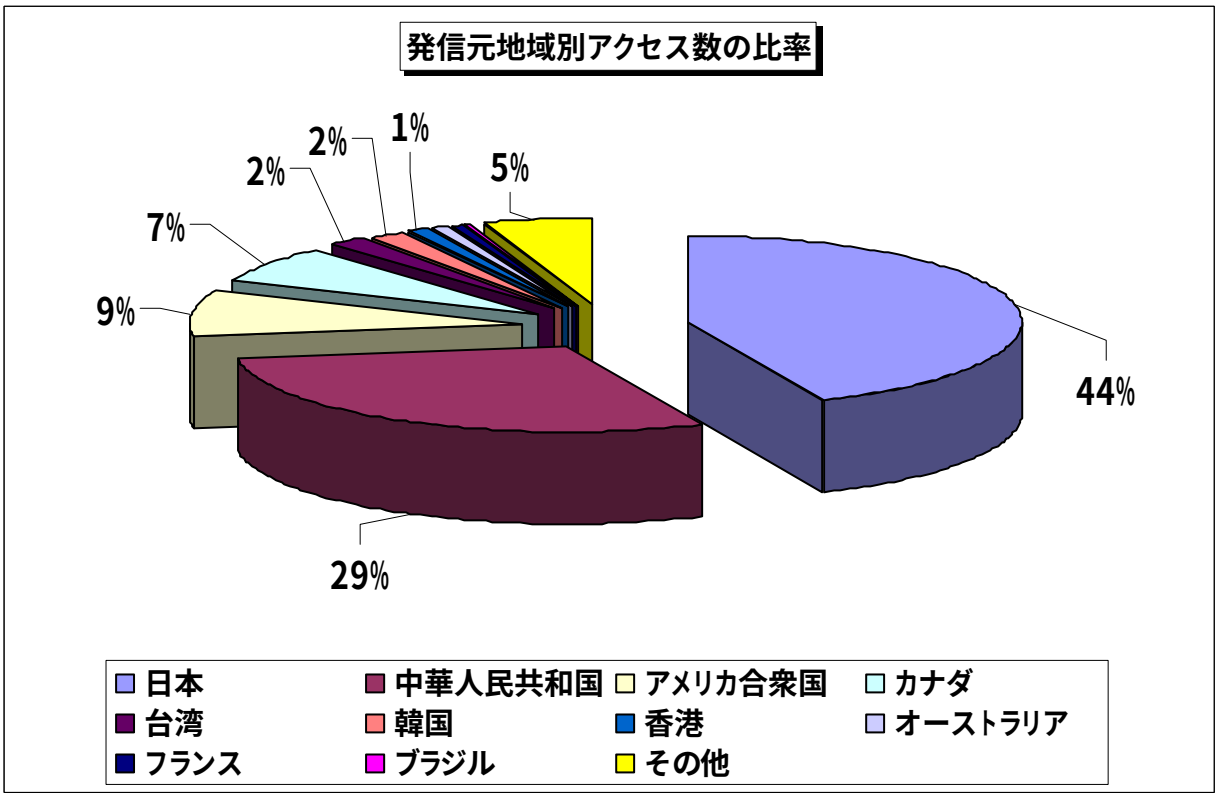
【図 2.3.2 2008 年 3 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 3 月の発信元地域別アクセス状況

2008 年 3 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。

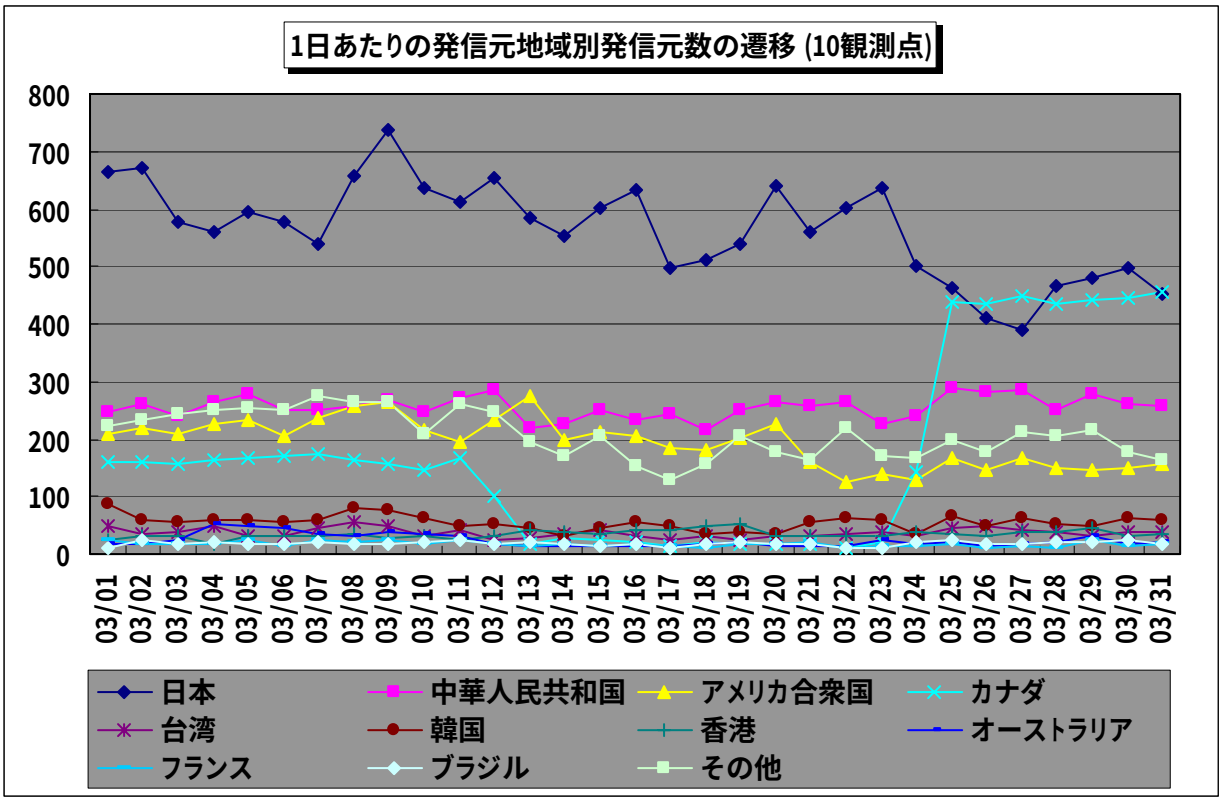


【図 2.4.1 2008 年 3 月の発信元地域別アクセス数の変化】

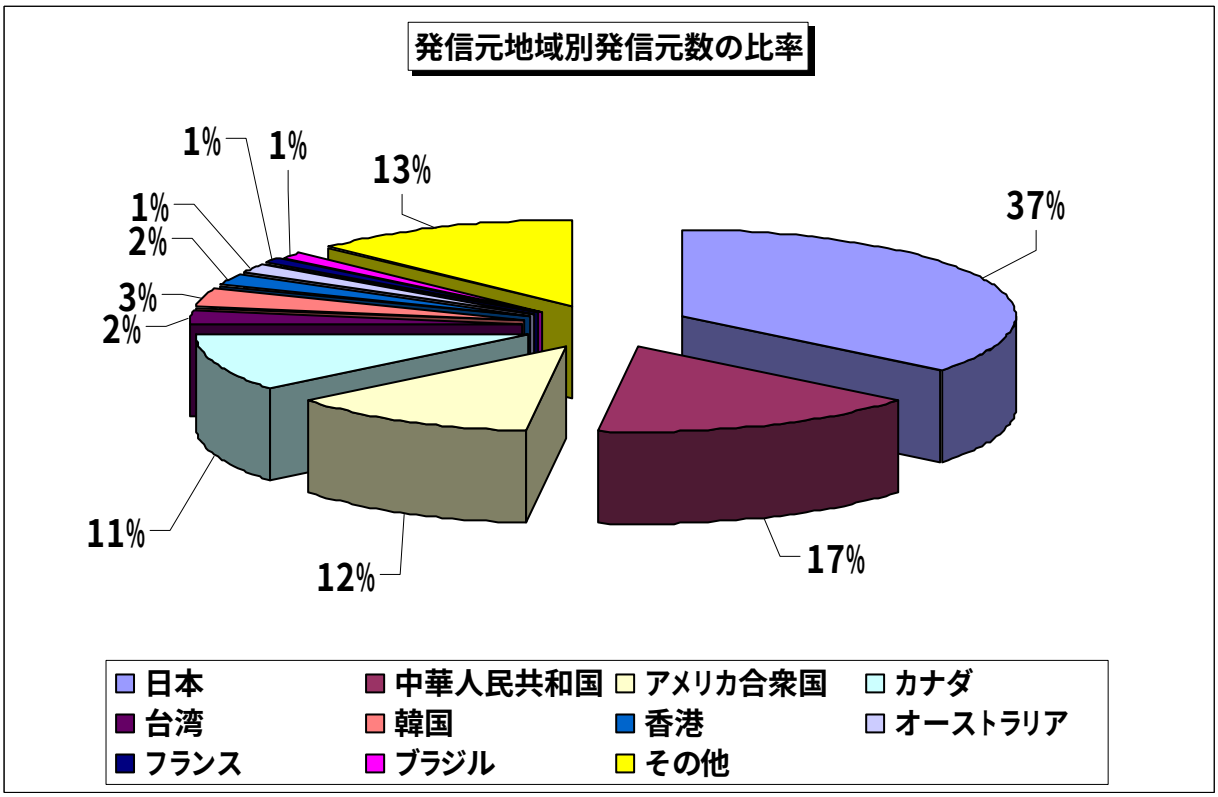


【図 2.4.2 2008 年 3 月の発信元地域別アクセス数の比率】

2008 年 3 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 3 月の発信元地域別発信元数の変化】

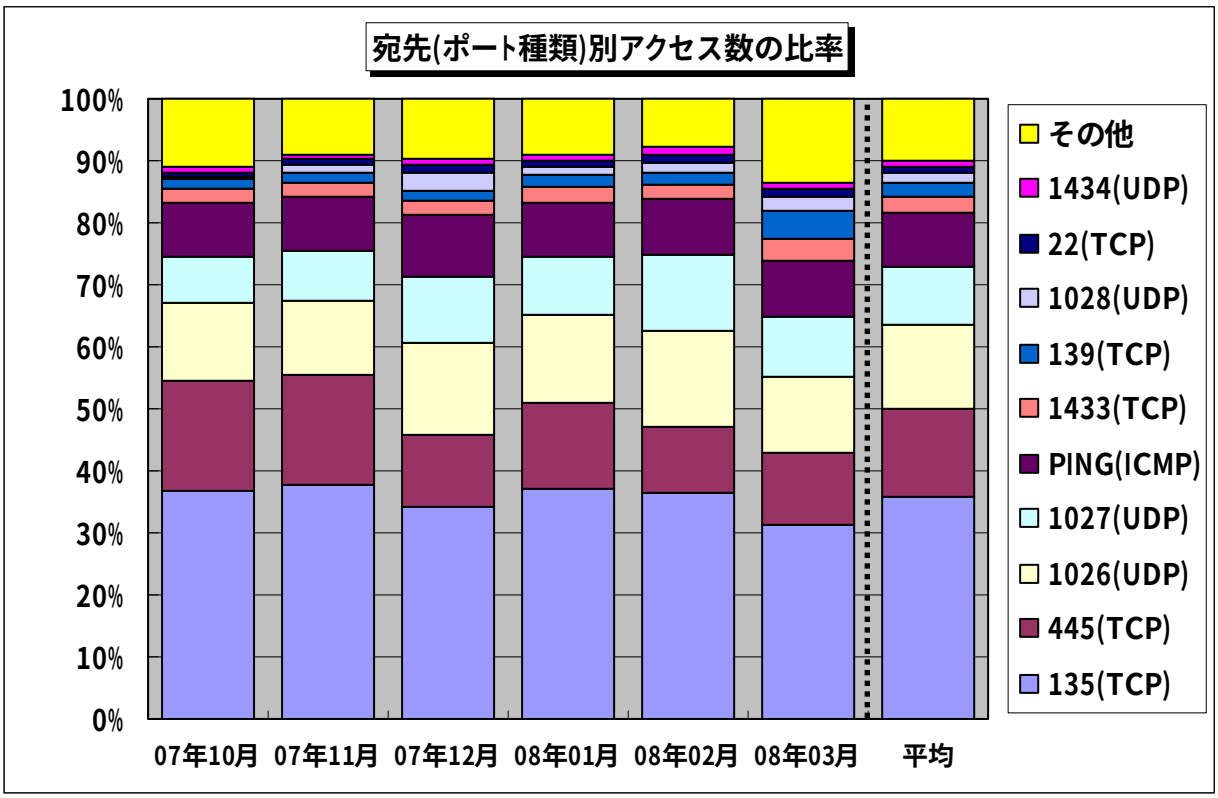


【図 2.4.4 2008 年 3 月の発信元地域別発信元数の比率】

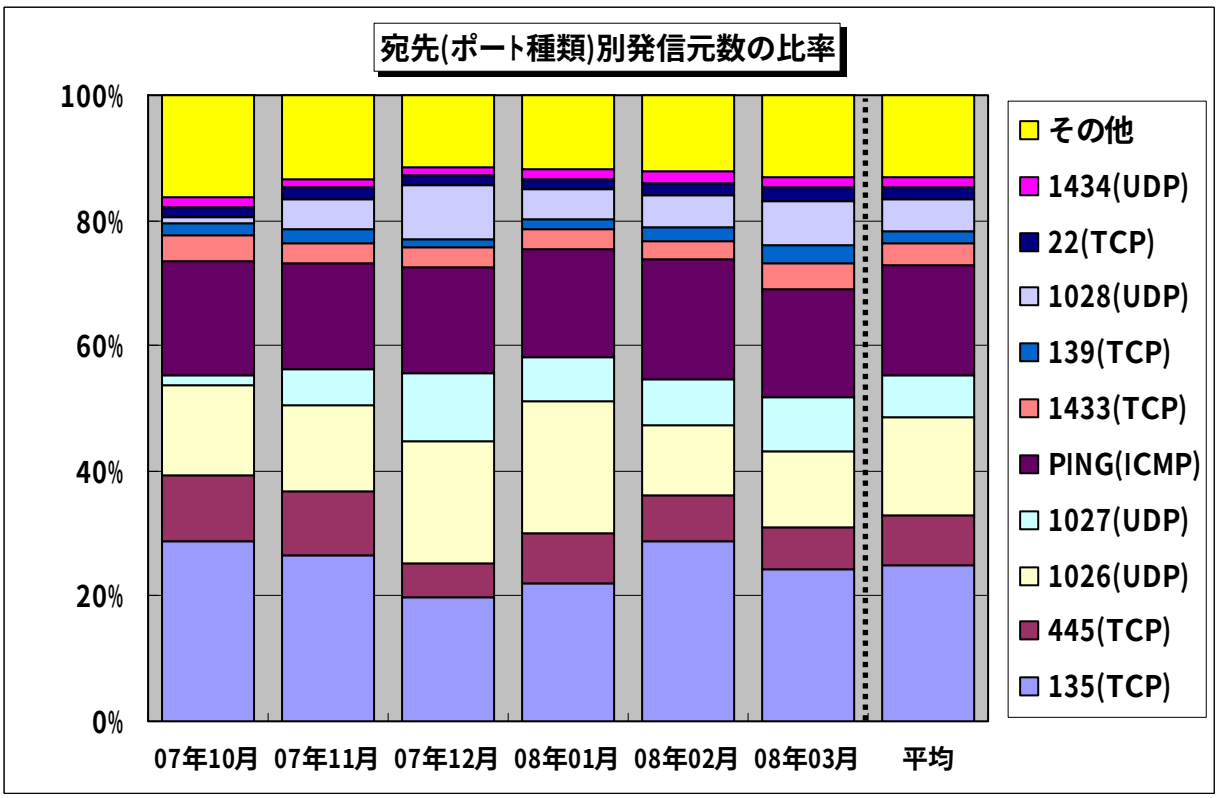
3．統計情報

3.1 2007 年 10 月～2008 年 3 月の宛先(ポート種類)別の比率

2007 年 10 月～2008 年 3 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。



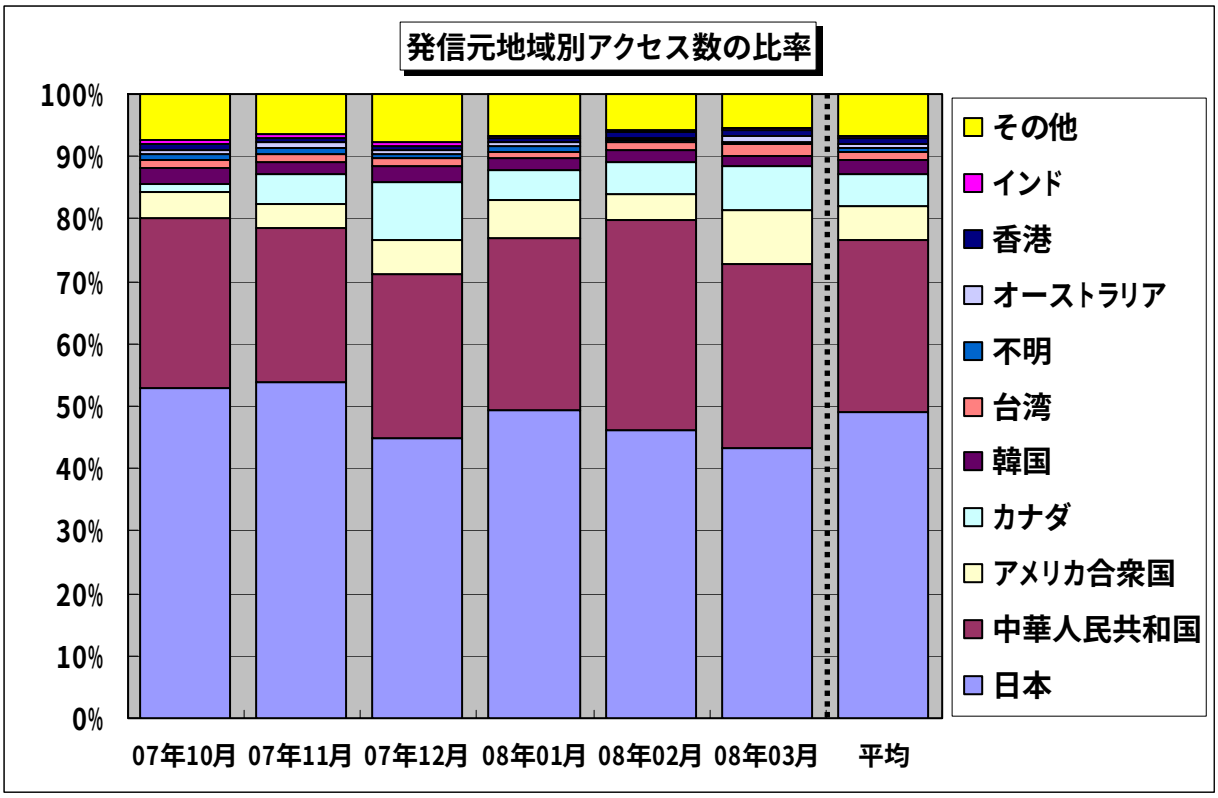
【図 3.1.1 2007 年 10 月～2008 年 3 月の宛先(ポート種類)別アクセス数の比率】



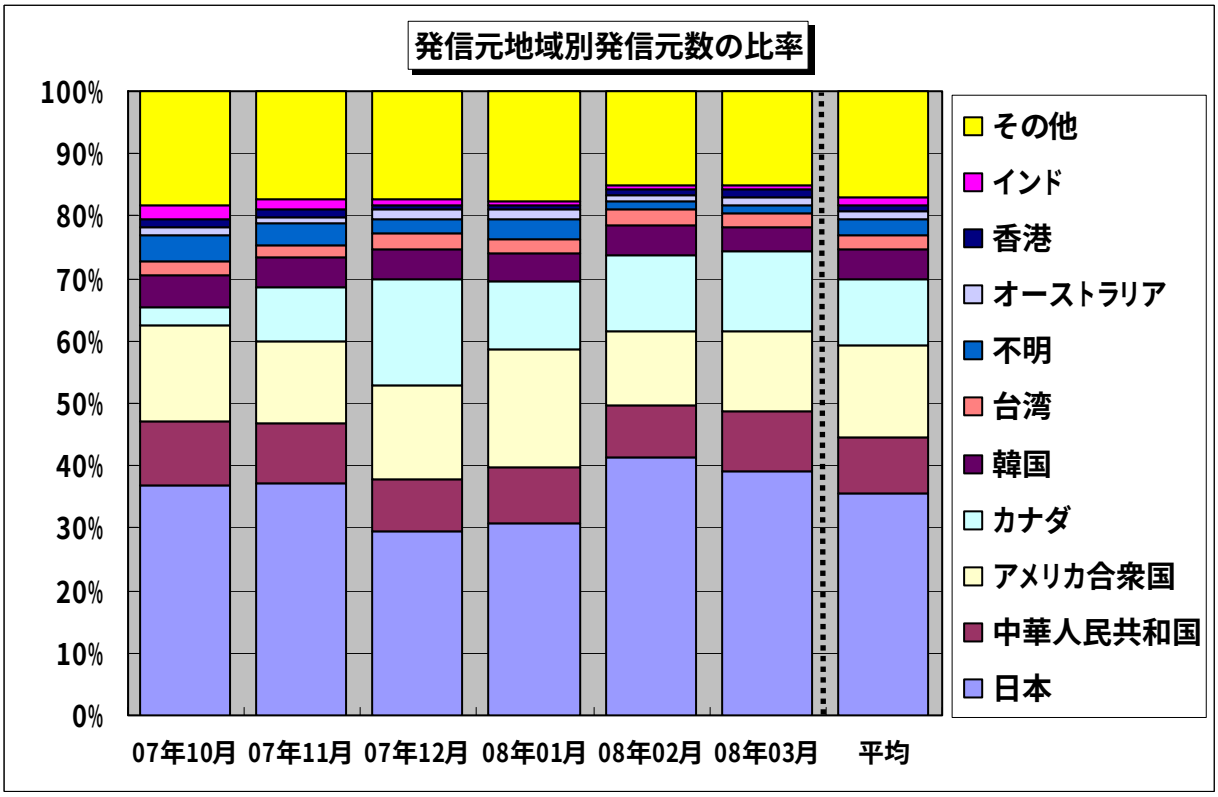
【図 3.1.2 2007 年 10 月～2008 年 3 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 10 月～2008 年 3 月の発信元地域別の比率

2007 年 10 月～2008 年 3 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 10 月～2008 年 3 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 10 月～2008 年 3 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 3 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 に関する脆弱性(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 特有の脆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
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 の脆弱性を狙ったアクセスである可能性が高いです
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
5900(TCP)	リモートアクセスツール RealVNC のぜい弱性を狙っていると思われるアクセスです
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