別紙 3

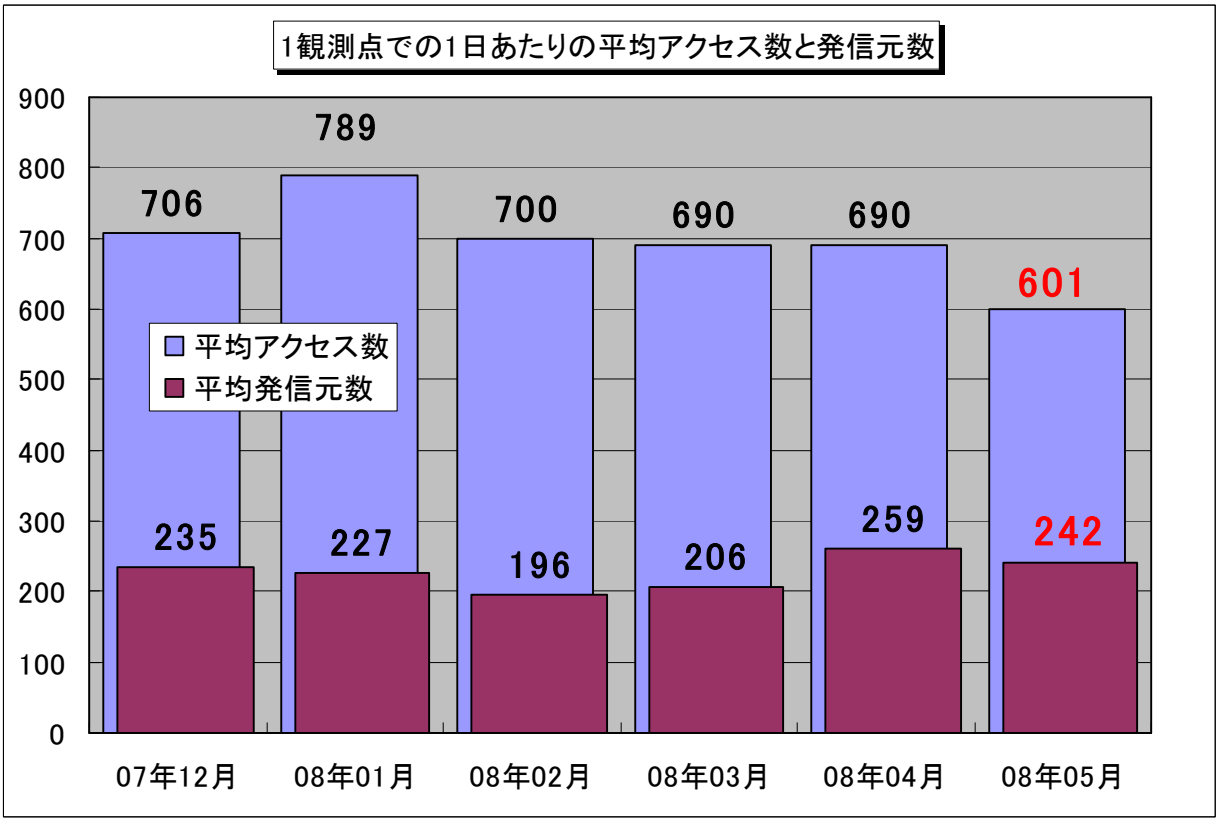
インターネット定点観測(TALOT2)での観測状況について

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 5 月の期待しない(一方的な)アクセスの総数は 10 観測点で **186,435 件**、総発信元数(※)は **74,936 箇所**ありました。1 観測点で見ると、1 日あたり **242** の発信元から **601 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、242 人の見知らぬ人(発信元)から、発信元一人当たり約 2 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 12 月～2008 年 5 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、5 月の期待しない(一方的な)アクセスは 4 月と比べて若干減少しており、全体的なアクセスの内容としても、徐々に減少傾向を示していると言えます。

2. 5 月のアクセスの状況

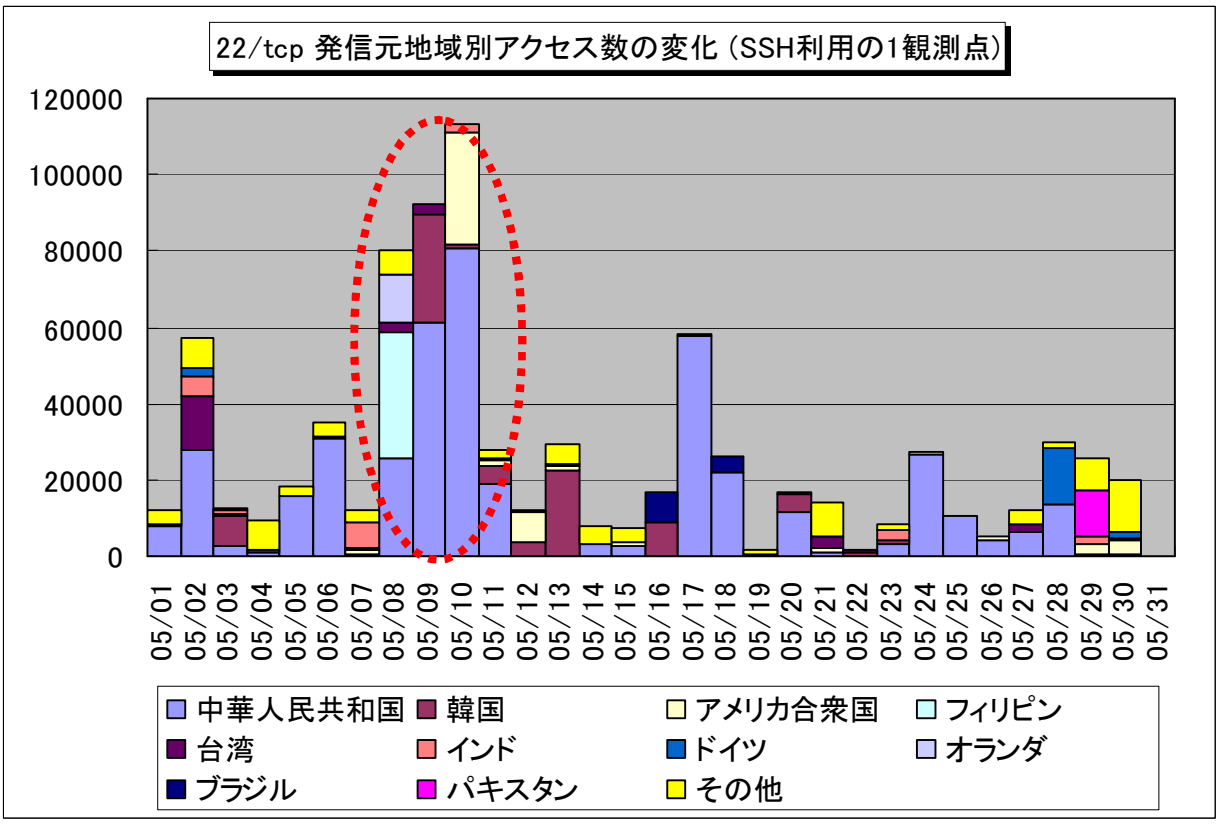
2008 年 5 月のアクセス状況は、4 月と比べて若干減少しました。これは主に Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスである 1026/udp、1027/udp および 1028/udp などへのアクセスが減少したためです。その他のポートへのアクセスについては特に大きな変化はありませんでした。

2.1. 22/tcp ポートを狙ったアクセス

22/tcp へのアクセスは 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）Server を探し出し脆弱なパスワード認証を破ることを目的としたアクセスであると考えられます。

TALOT2 でメンテナンス用に SSH を利用している観測点(※)の 22/tcp ポートへのアクセスについて 5 月にアクセスが急増している時期がありました。（図 2.1.1）

(※)：これらのアクセスは特定観測点に対するものであり、統計情報にそぐわない為、集計からは除外してあります。



【図 2.1.1 22/tcp（SSH 利用の 1 観測点）発信元地域別アクセス数の変化】

また、5 月の中旬に SSH に関連する脆弱性が見つかっています。この脆弱性は OpenSSL(※1)に予測可能な乱数が生成されるというもので、さらに OpenSSH(※2)にも間接的に影響します。この不具合のある Open SSL パッケージで生成された鍵を使用するアプリケーションにおいて影響があり、影響のあるシステムに対してブルートフォース攻撃(※3)を受けることで鍵情報が推測される可能性があります。

影響を受けるシステムを使用しているサーバ管理者は、ベンダより公開されている最新バージョンへのアップデートと、鍵の再生成をして下さい。

(※1) : OpenSSL グループによる SSL v2/v3 と TLS v1 を実装するオープンソースなツールキットです。

(※2) : OpenBSD グループによる SSH (Secure Shell) プロトコルを実装したクライアント／サーバプログラムです。

(※3) : ブルートフォース攻撃とは、総当り攻撃とも呼ばれ、パスワードを破るためにありとあらゆる解読方法を使用して攻撃する手法です。

(参考資料)

■ JVNVU#925211Debian および Ubuntu の OpenSSL パッケージに予測可能な乱数が生成される脆弱性

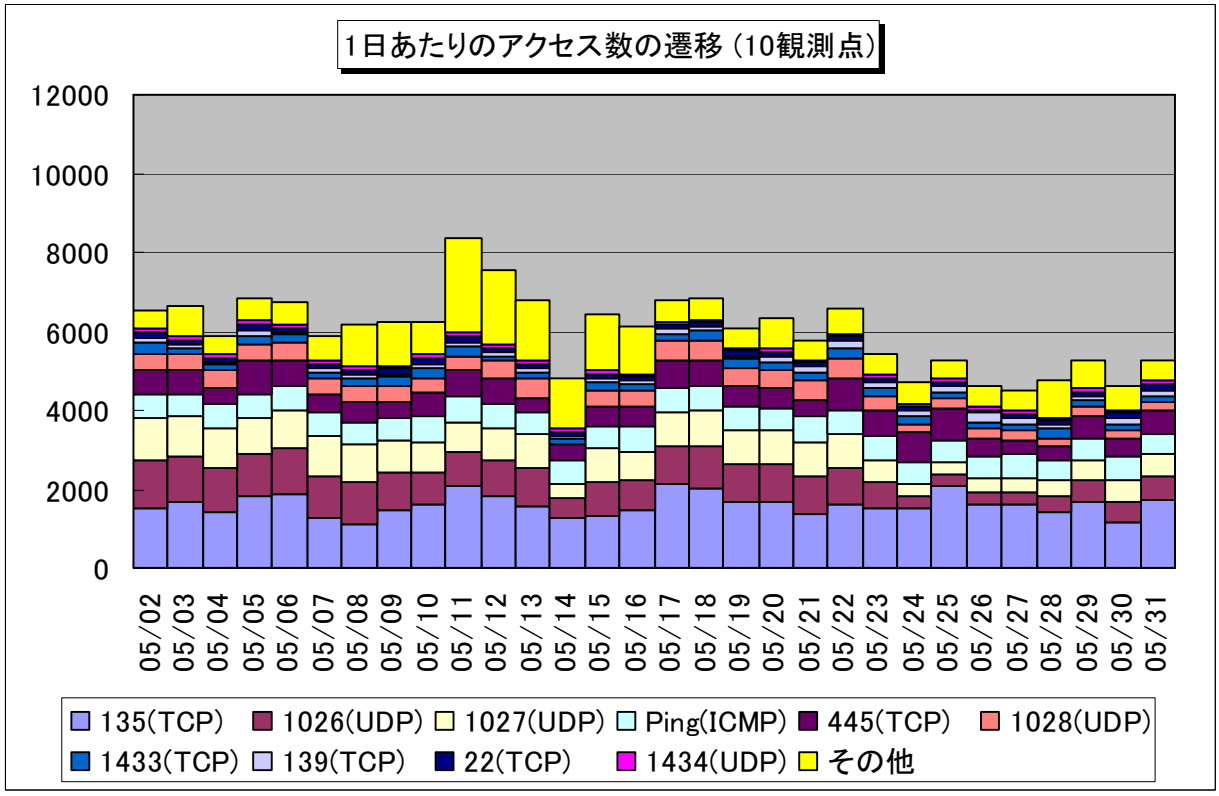
http://jvn.jp/cert/JVNVU925211/

■IPA-情報セキュリティ白書 2007 年版

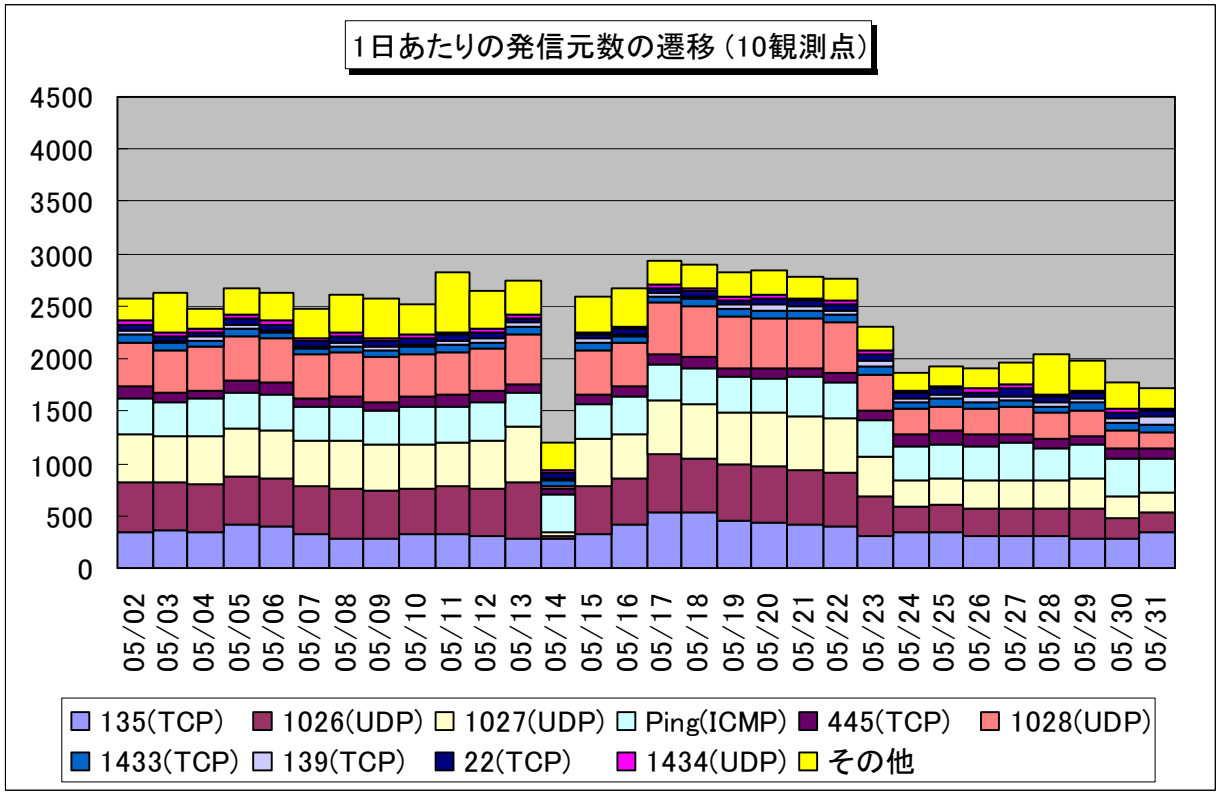
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

2.2 2008 年 5 月の一方的なアクセス状況

2008 年 5 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。



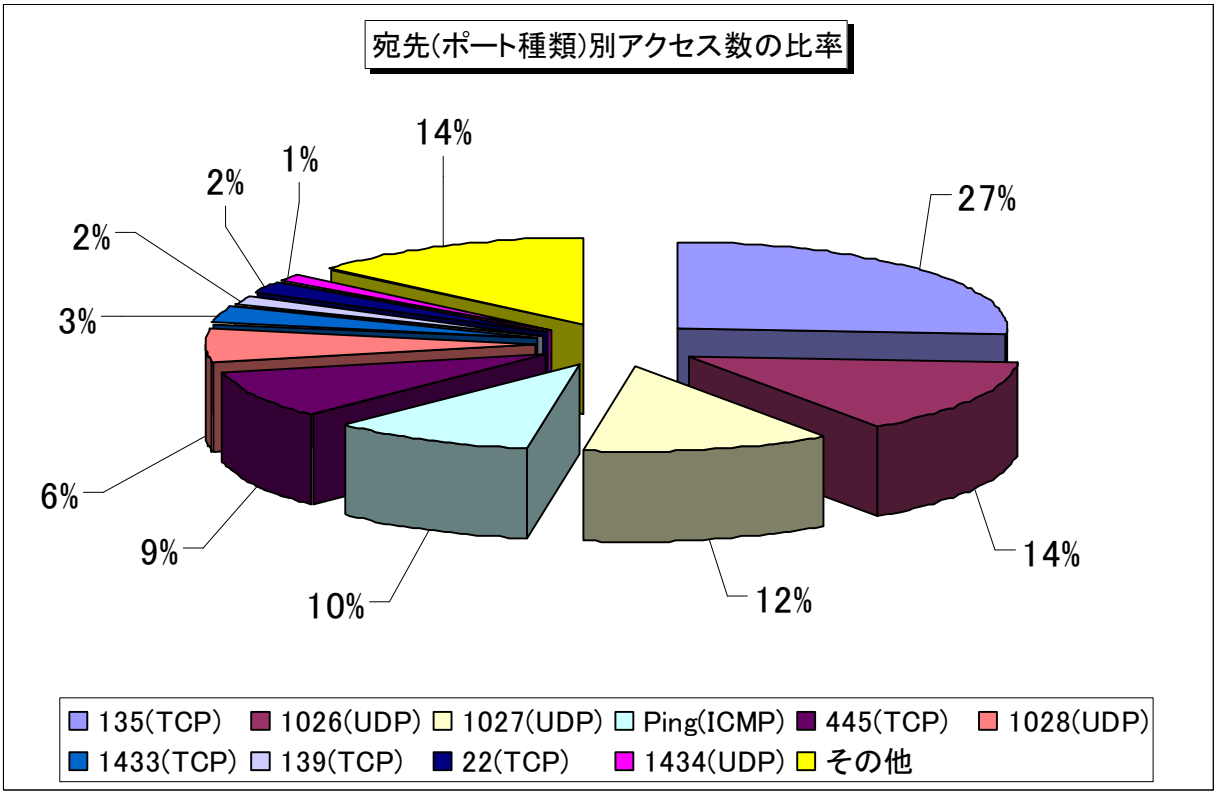
【図 2.2.1 2008 年 5 月の一方的なアクセス状況(アクセス数)】



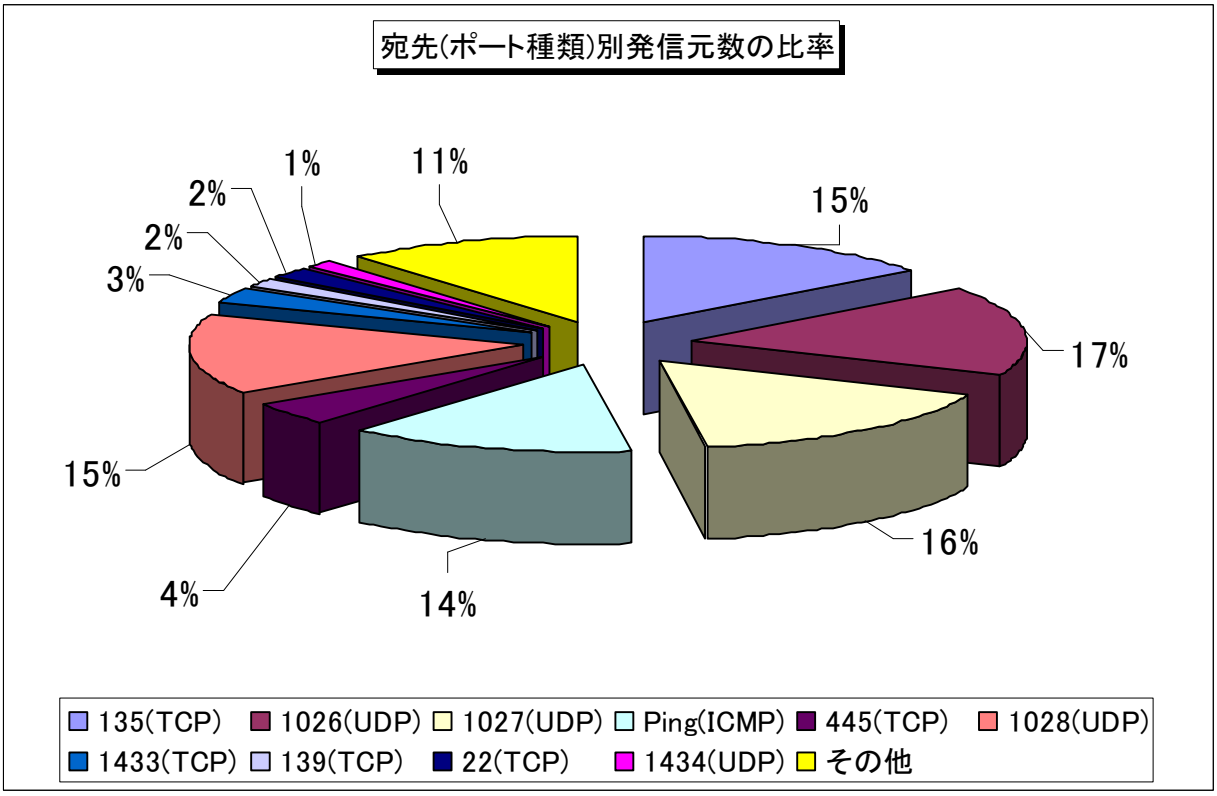
【図 2.2.2 2008 年 5 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 5 月の宛先(ポート種類)別の比率

2008 年 5 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。



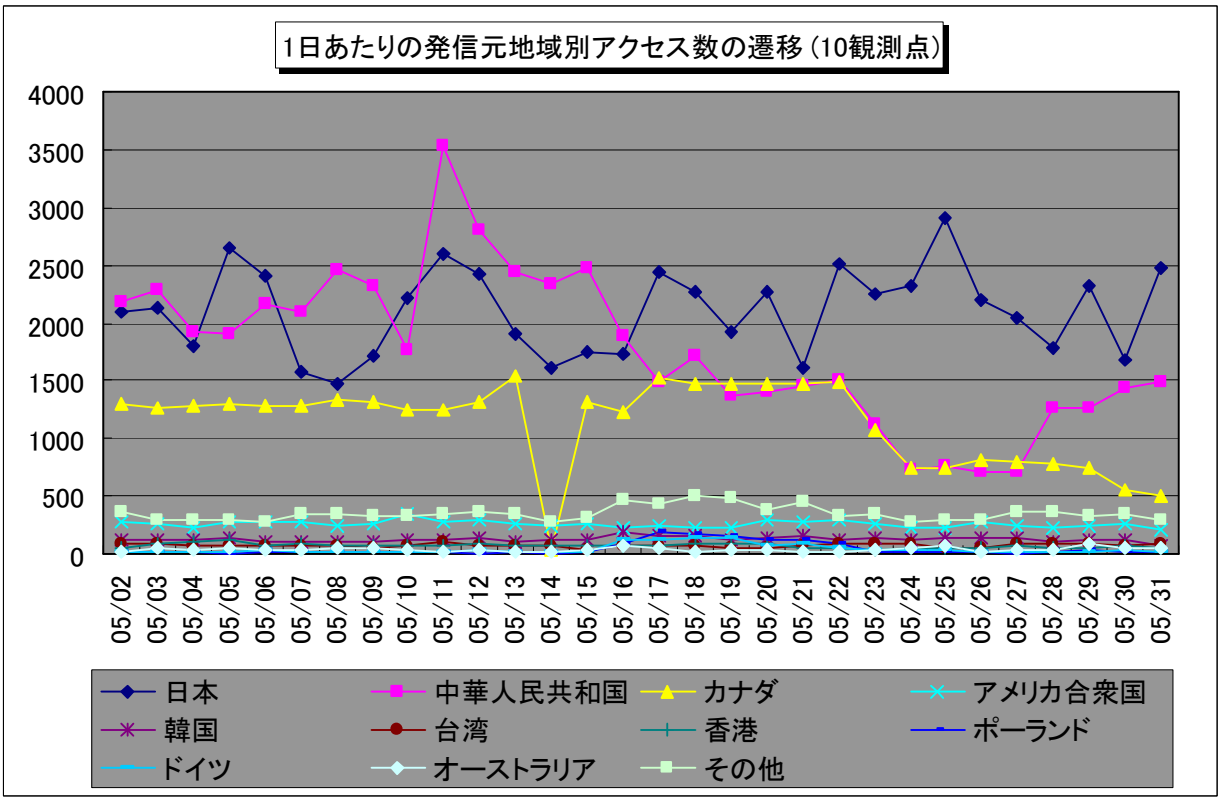
【図 2.3.1 2008 年 5 月の宛先(ポート種類)別アクセス数の比率】



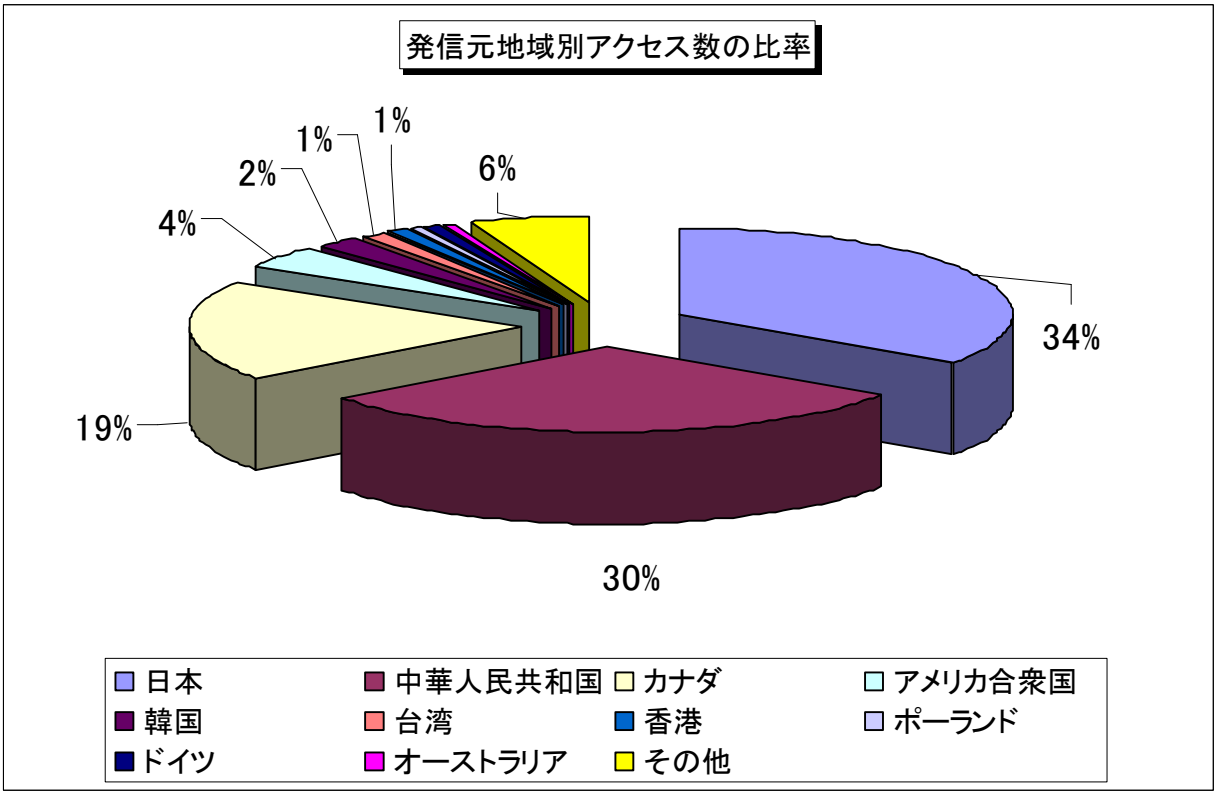
【図 2.3.2 2008 年 5 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 5 月の発信元地域別アクセス状況

2008 年 5 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。

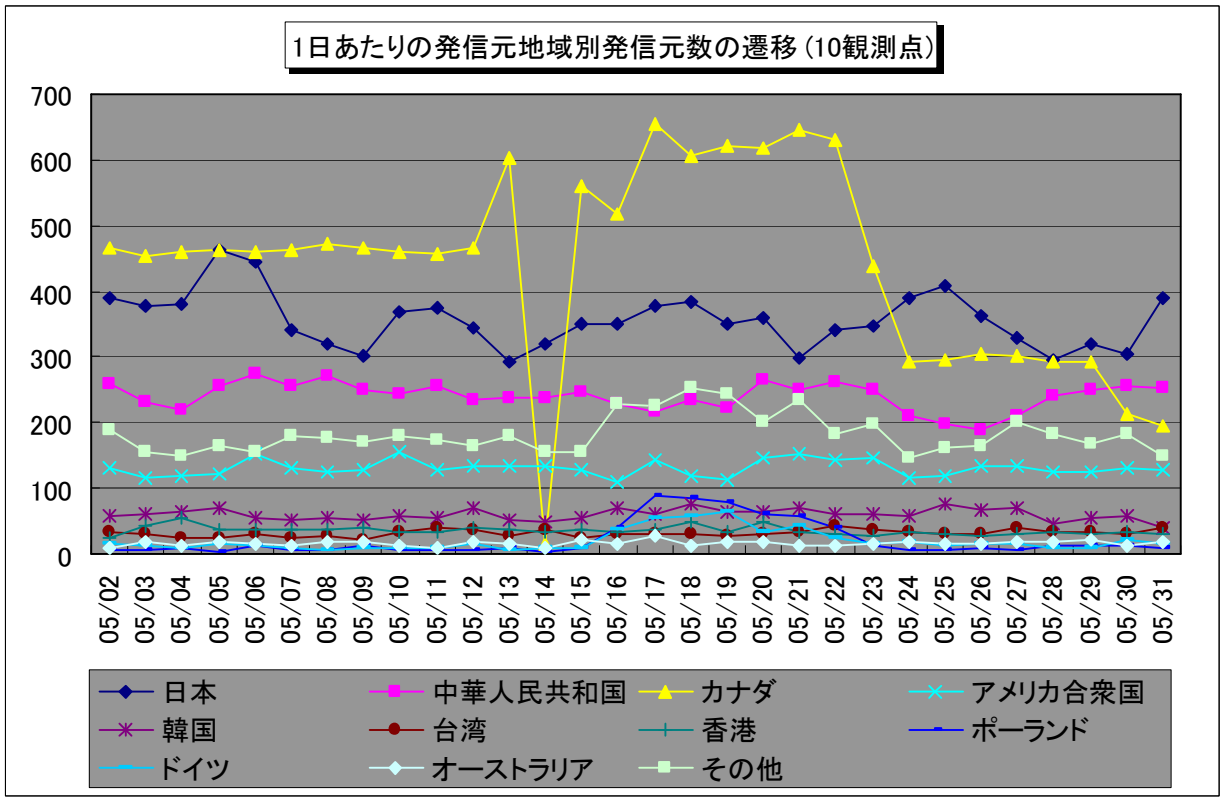


【図 2.4.1 2008 年 5 月の発信元地域別アクセス数の変化】

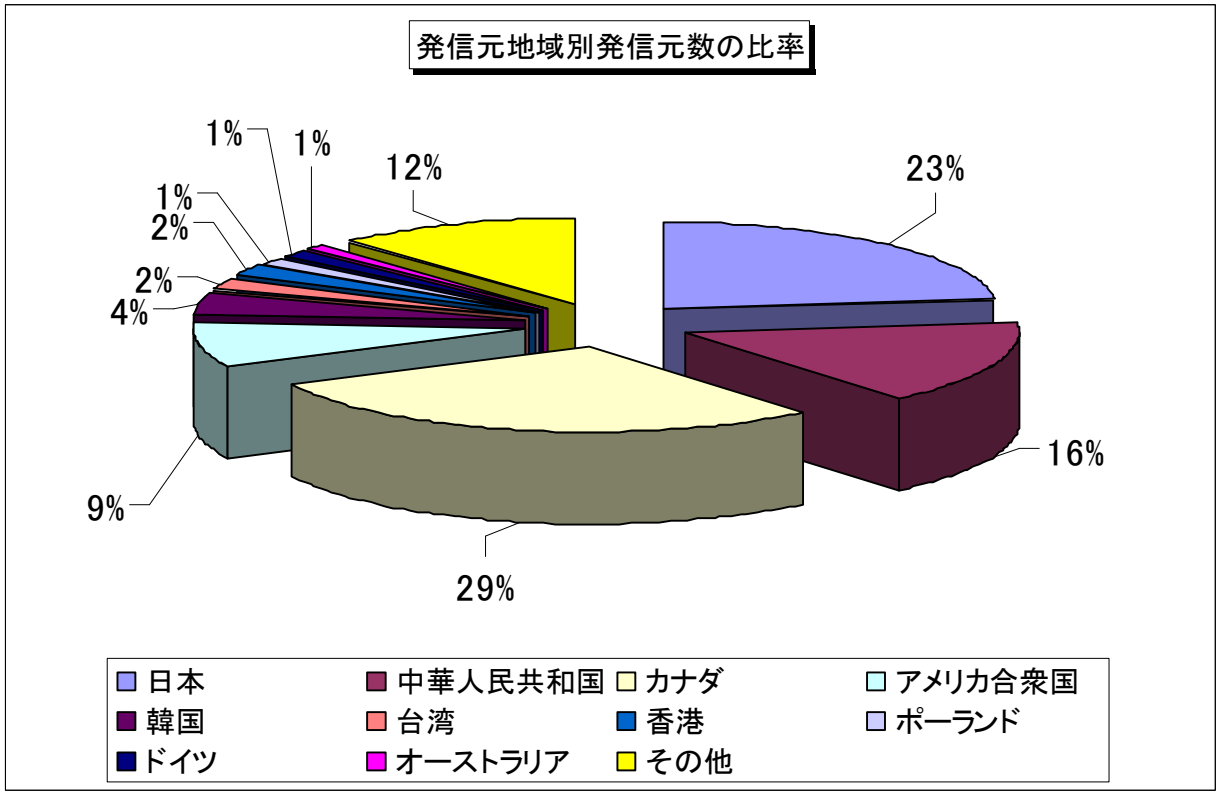


【図 2.4.2 2008 年 5 月の発信元地域別アクセス数の比率】

2008 年 5 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 5 月の発信元地域別発信元数の変化】

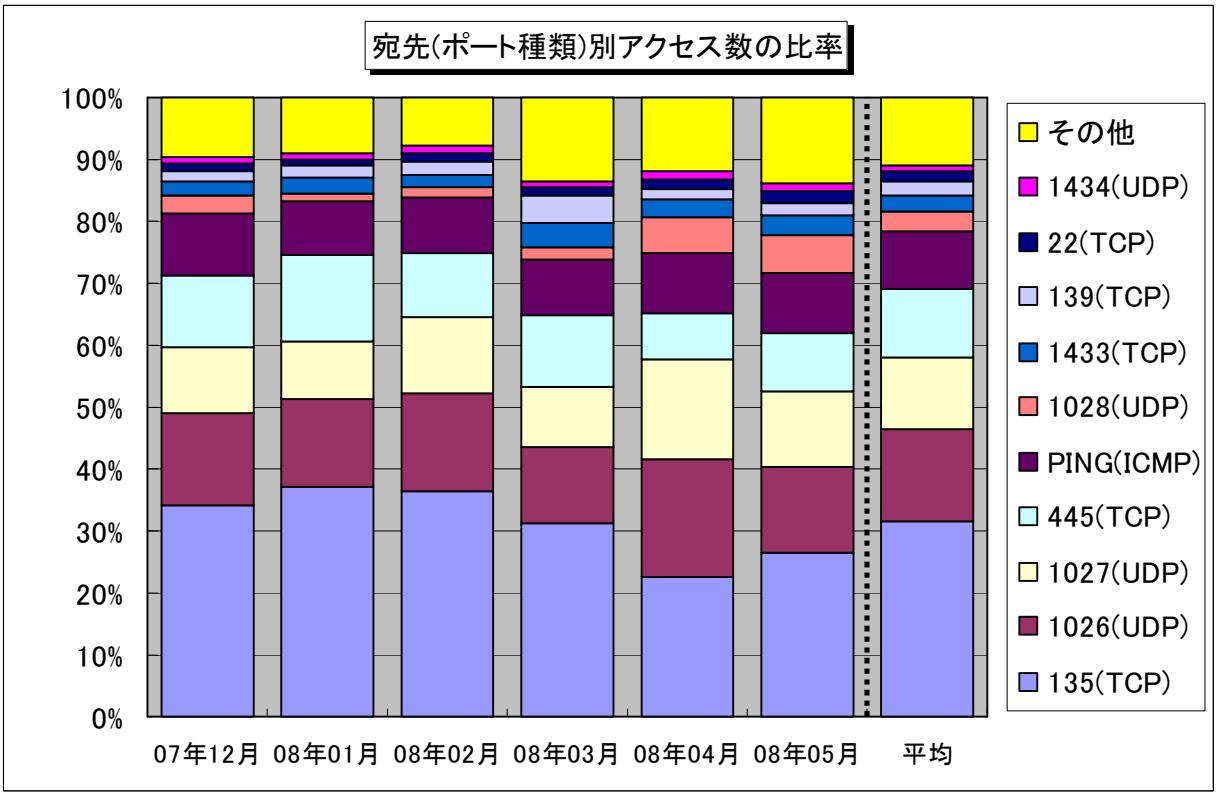


【図 2.4.4 2008 年 5 月の発信元地域別発信元数の比率】

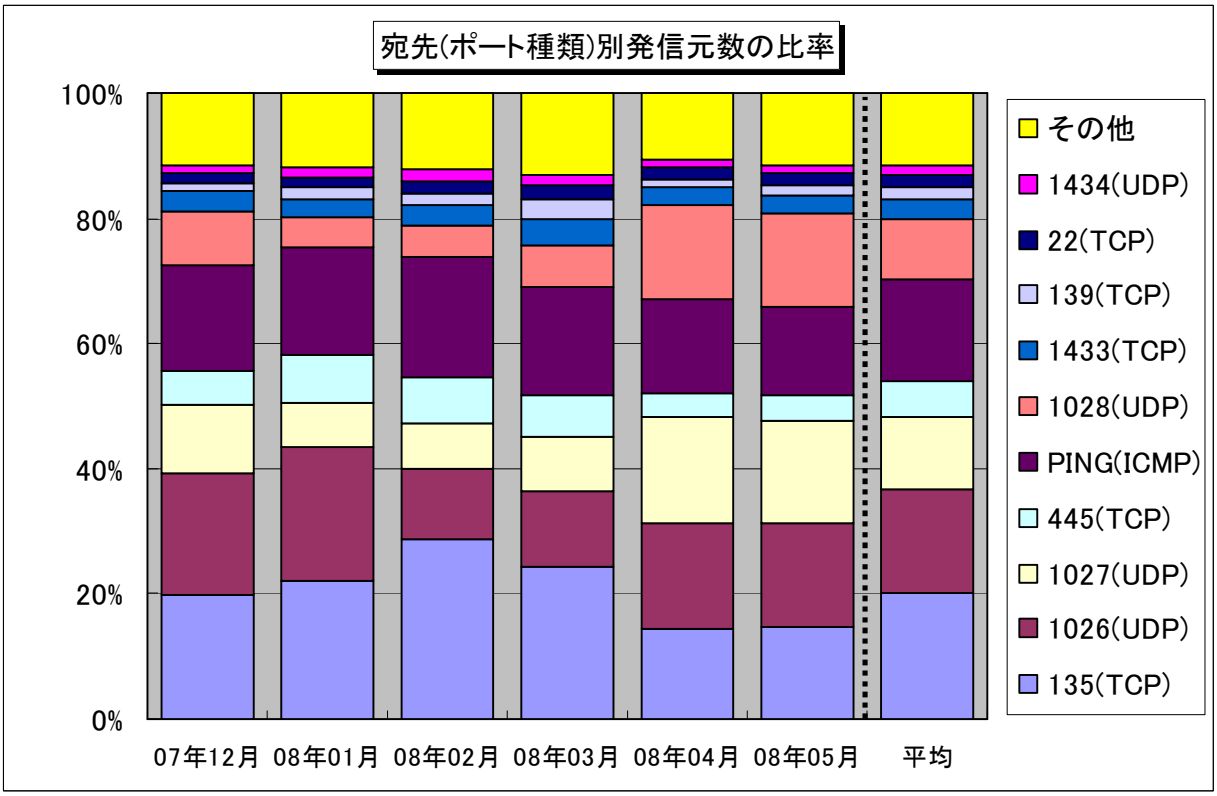
3. 統計情報

3.1 2007 年 12 月～2008 年 5 月の宛先(ポート種類)別の比率

2007 年 12 月～2008 年 5 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。



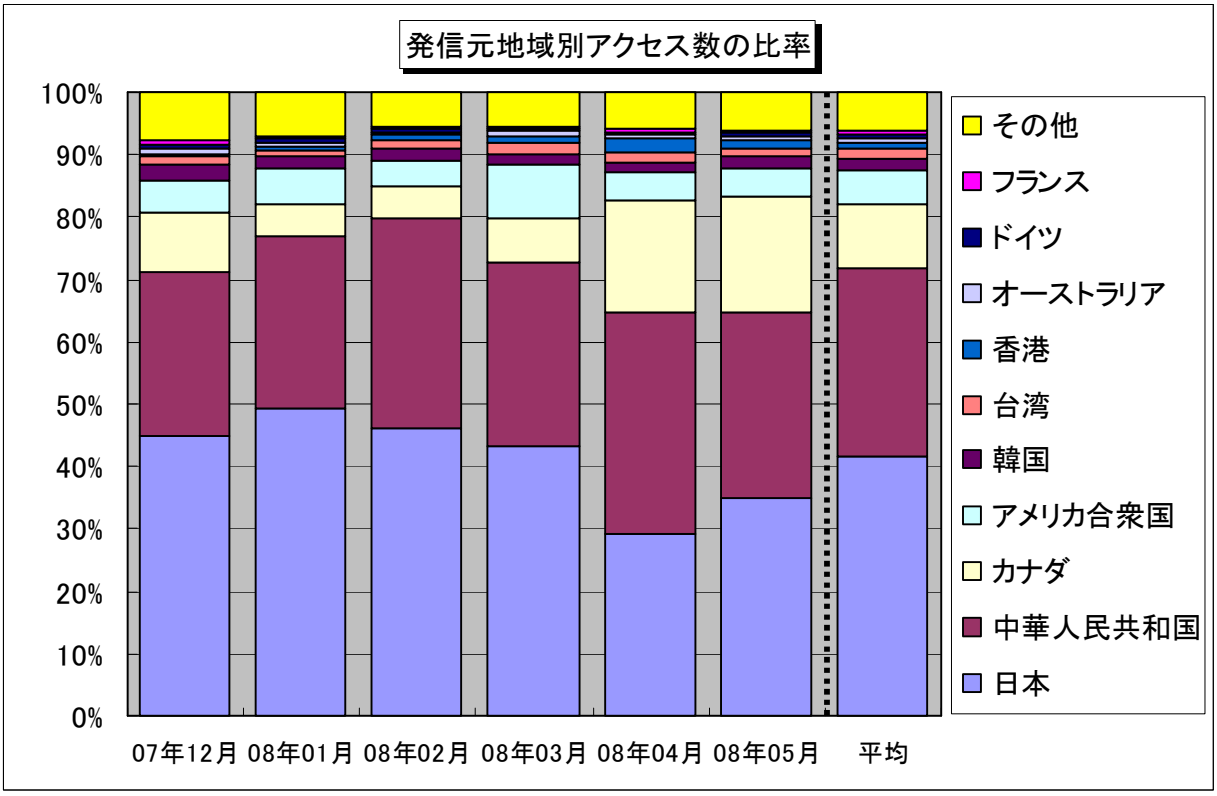
【図 3.1.1 2007 年 12 月～2008 年 5 月の宛先(ポート種類)別アクセス数の比率】



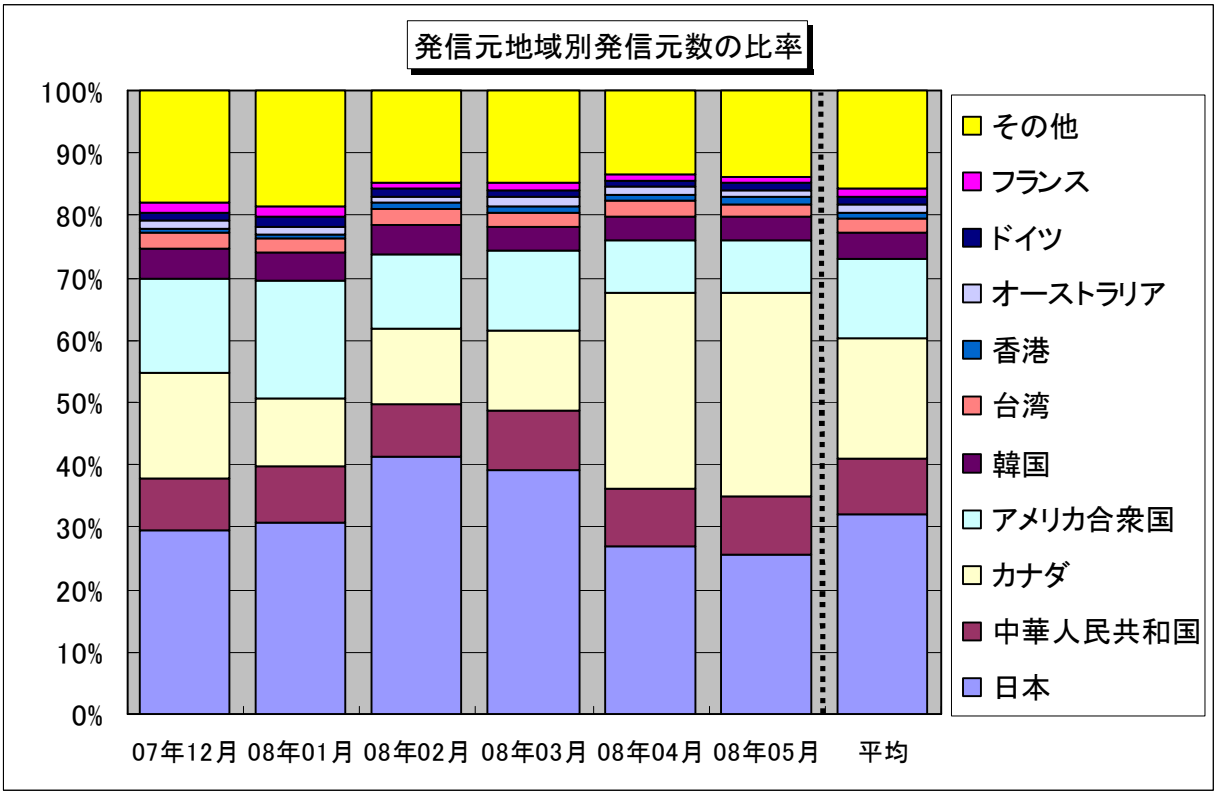
【図 3.1.2 2007 年 12 月～2008 年 5 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 12 月～2008 年 5 月の発信元地域別の比率

2007 年 12 月～2008 年 5 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 12 月～2008 年 5 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 12 月～2008 年 5 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 5 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
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)
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
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

■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