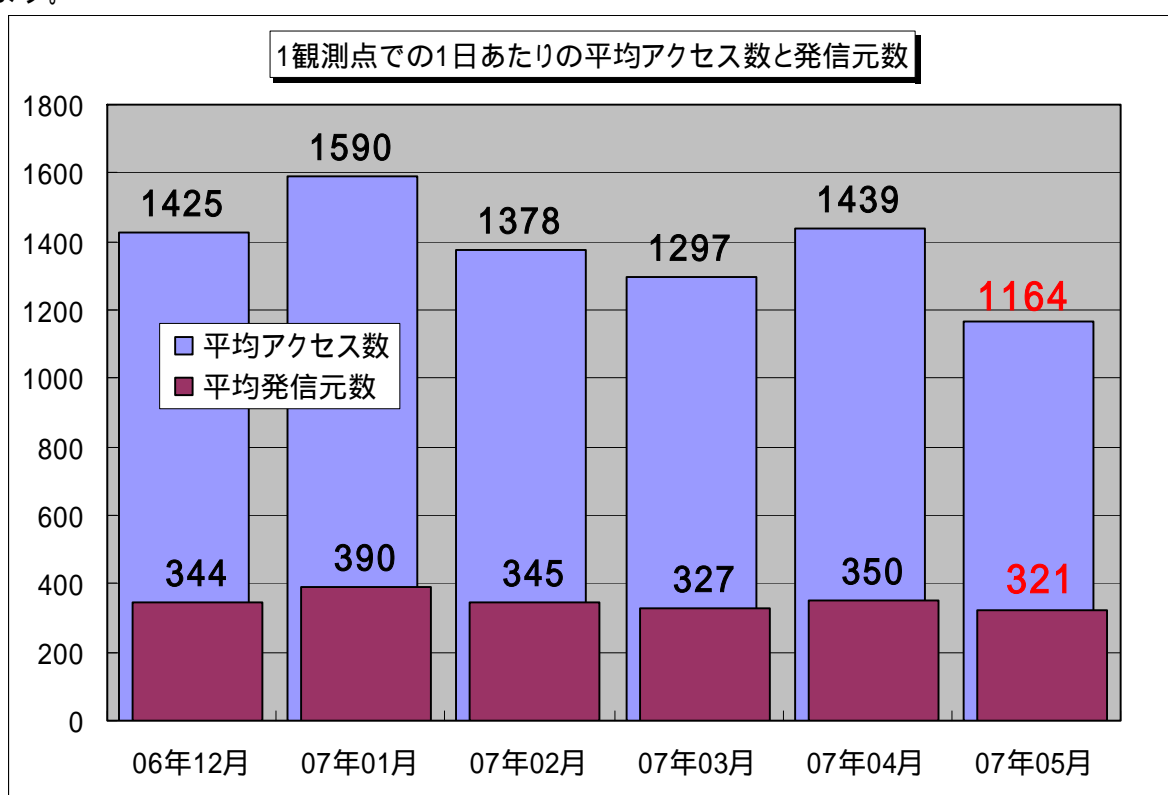


インターネット定点観測(TALOT2)での観測状況について

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、2007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209,499件ありました。1観測点で1日あたり321の発信元から1,164件のアクセスがあったこととなります。

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向的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、321人の見知らぬ人(発信元)から、発信元一人当たり4件の不正と思われるアクセスを受けている**ということになります。



【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】

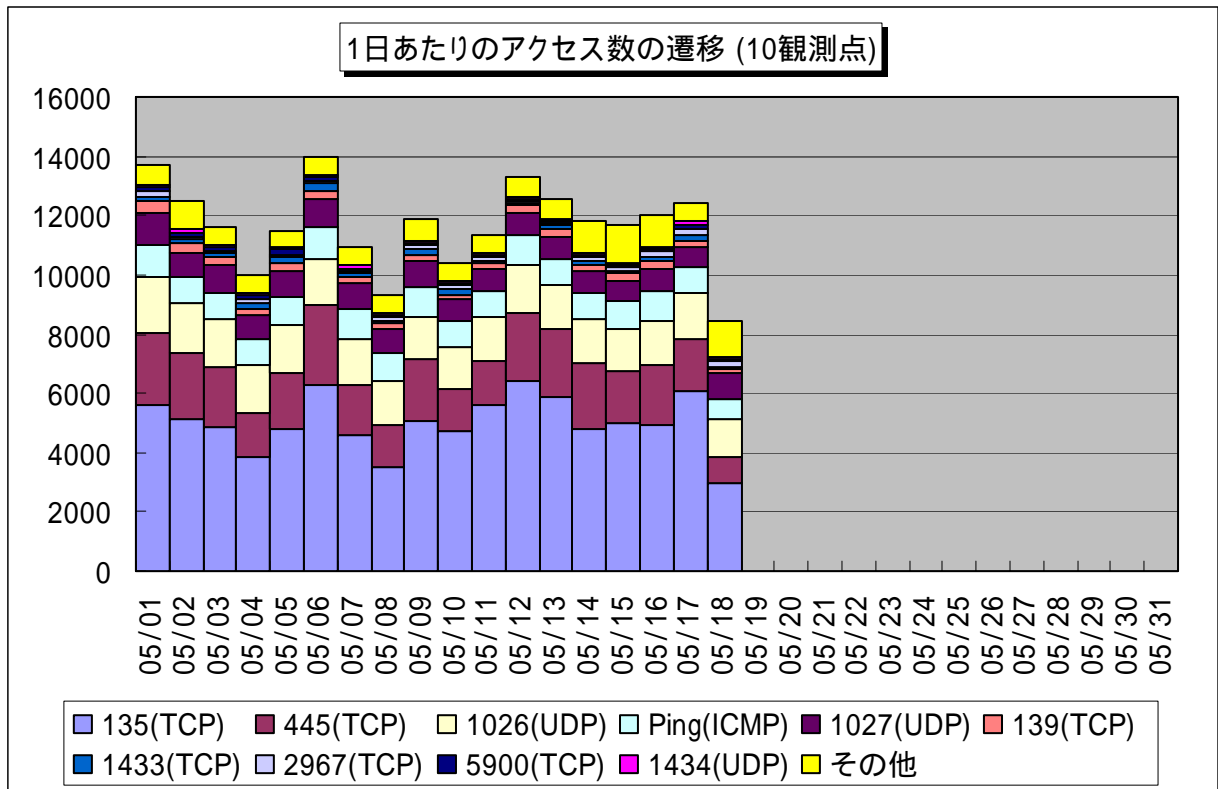
2006年12月～2007年5月までの各月の1観測点での1日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図1.1に示します。

注意)

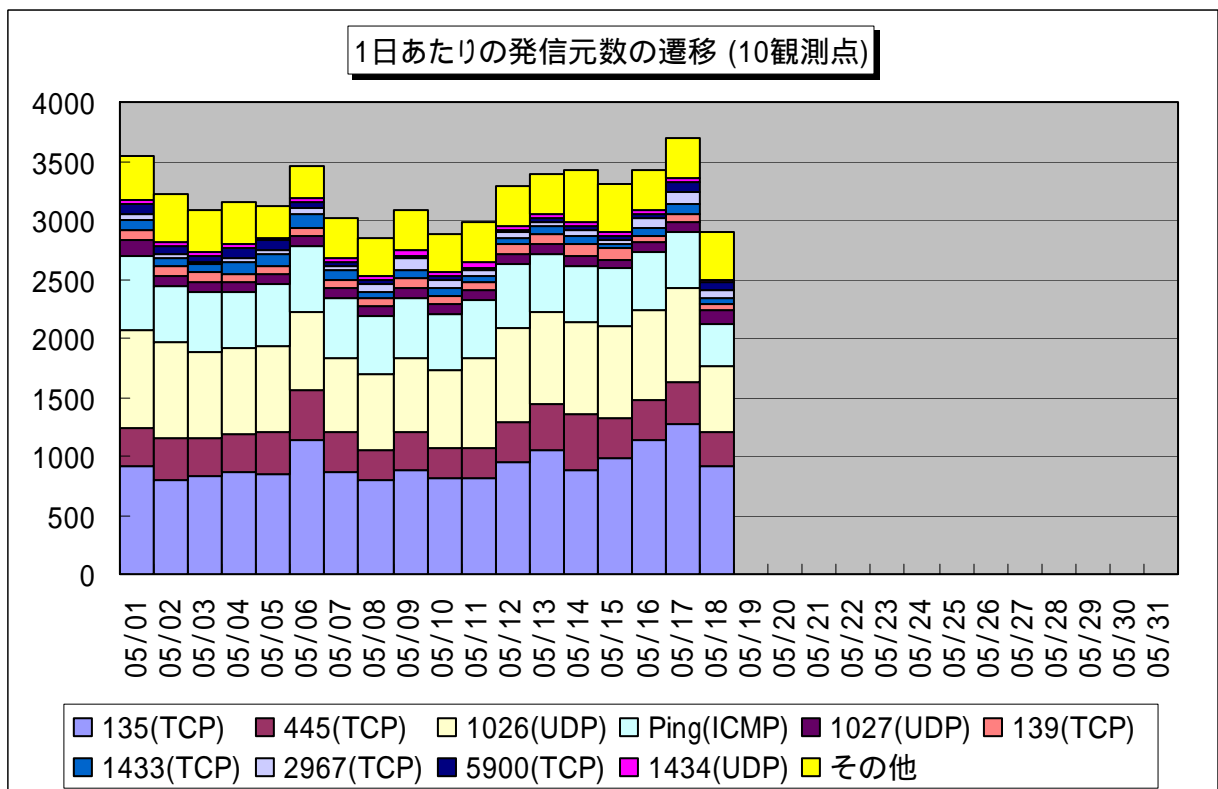
5月はTALOT2システム保守の為、5月1日から5月18日までの観測データで発表しておりますことをご了承下さい。

2.2 2007年5月の一方的なアクセス状況

2007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。



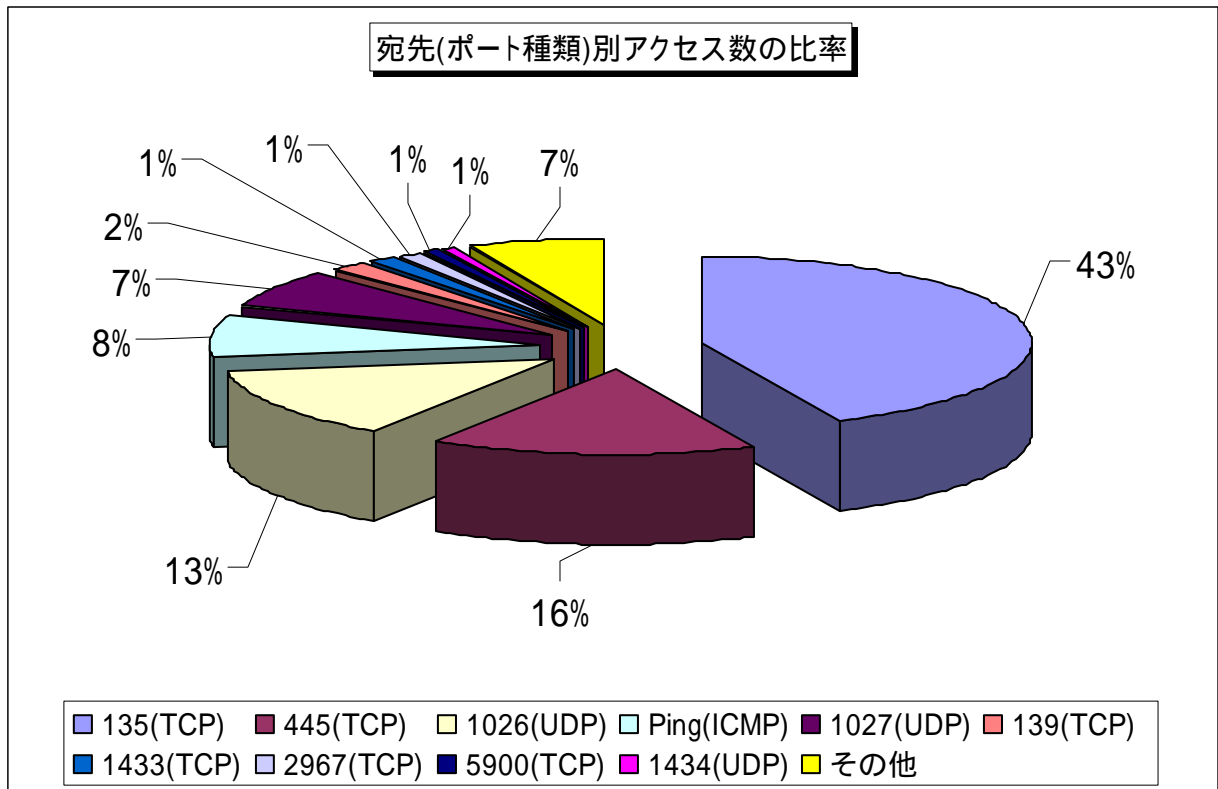
【図 2.2.1 2007年5月の一方的なアクセス状況(アクセス数)】



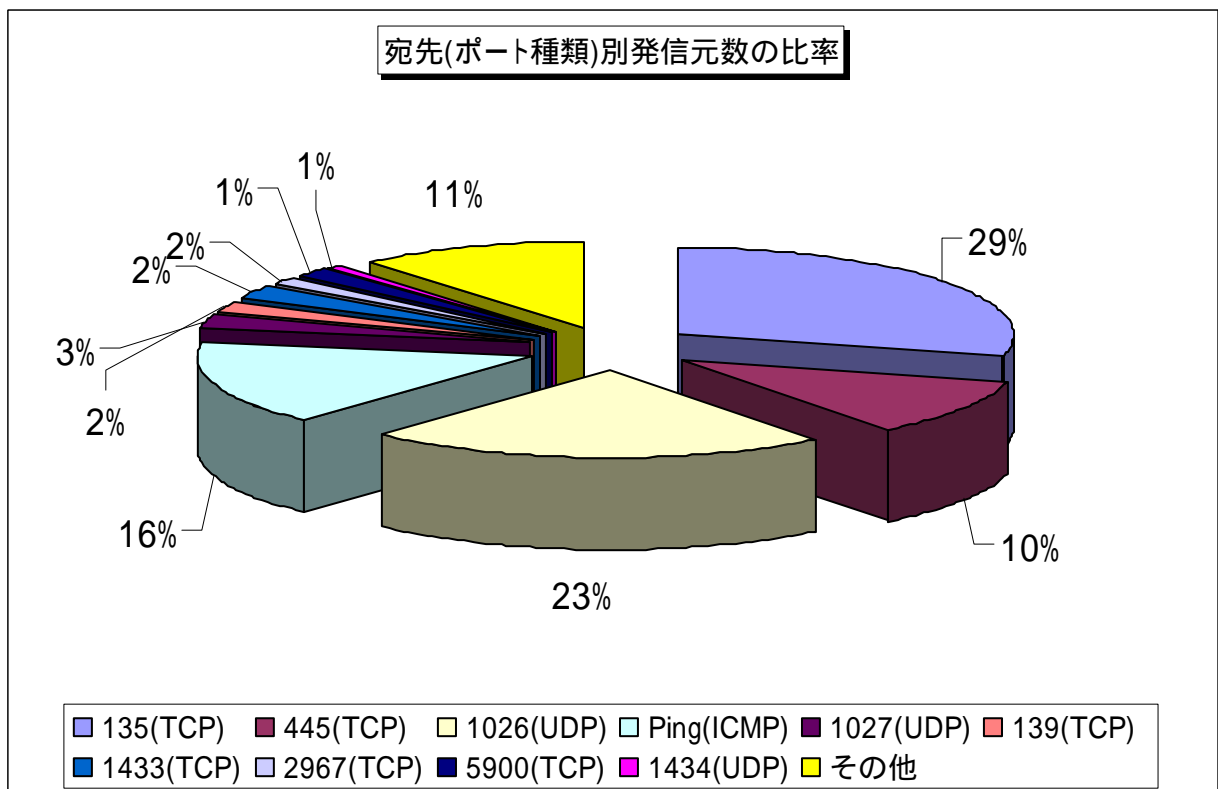
【図 2.2.2 2007年5月の一方的なアクセス状況(発信元数)】

2.3 2007年5月の宛先(ポート種類)別の比率

2007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。



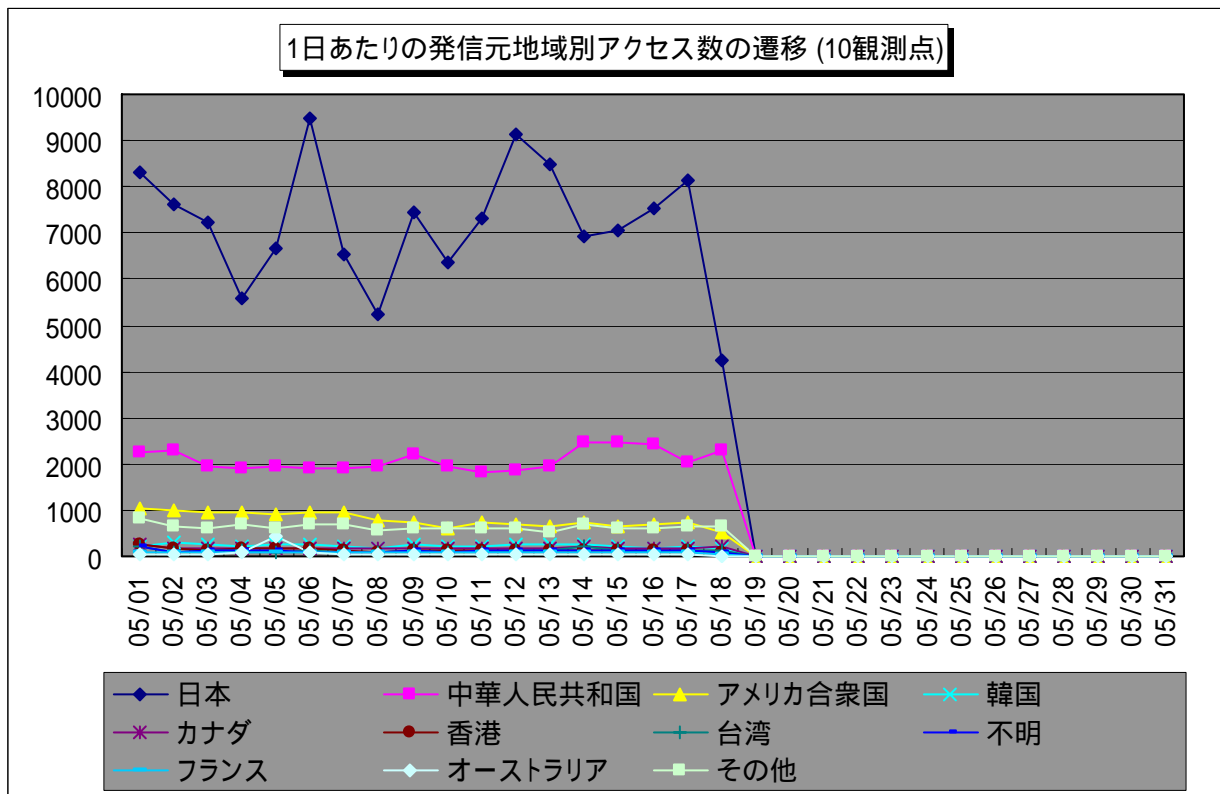
【図 2.3.1 2007年5月の宛先(ポート種類)別アクセス数の比率】



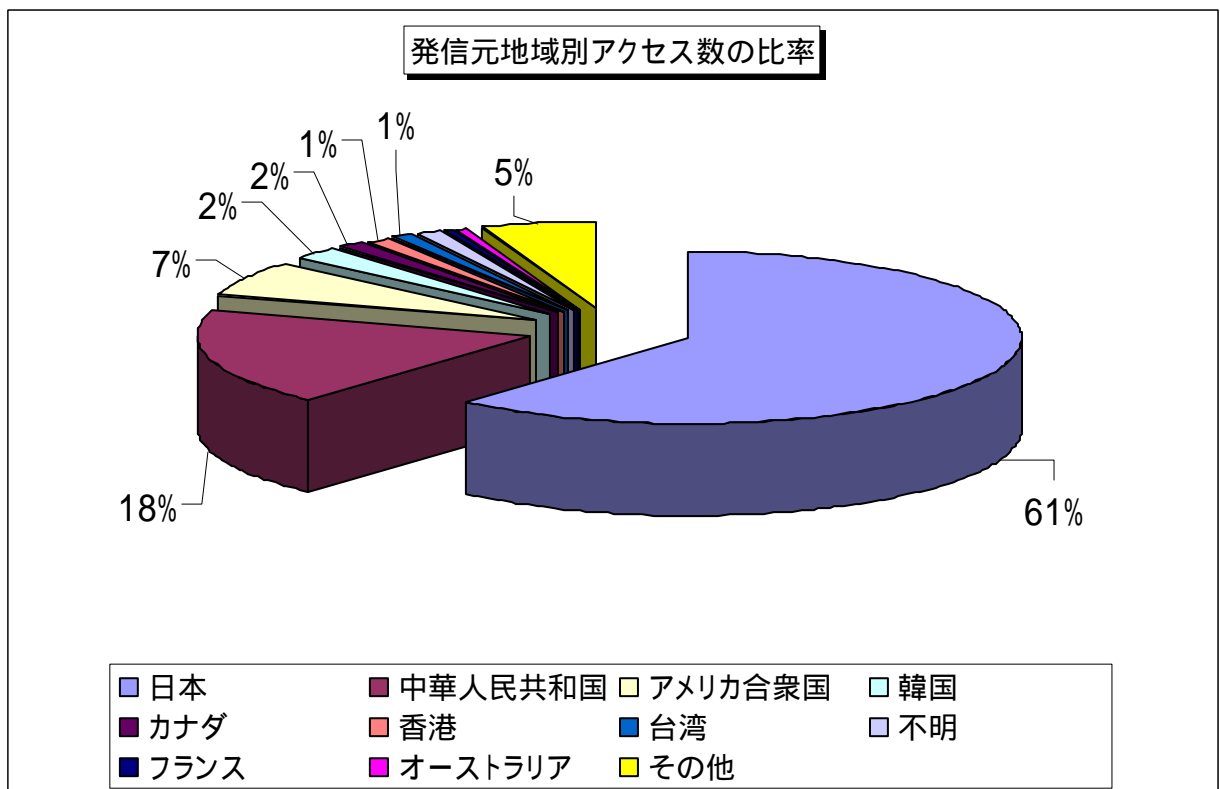
【図 2.3.2 2007年5月の宛先(ポート種類)別発信元数の比率】

2.4 2007年5月の発信元地域別アクセス状況

2007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。

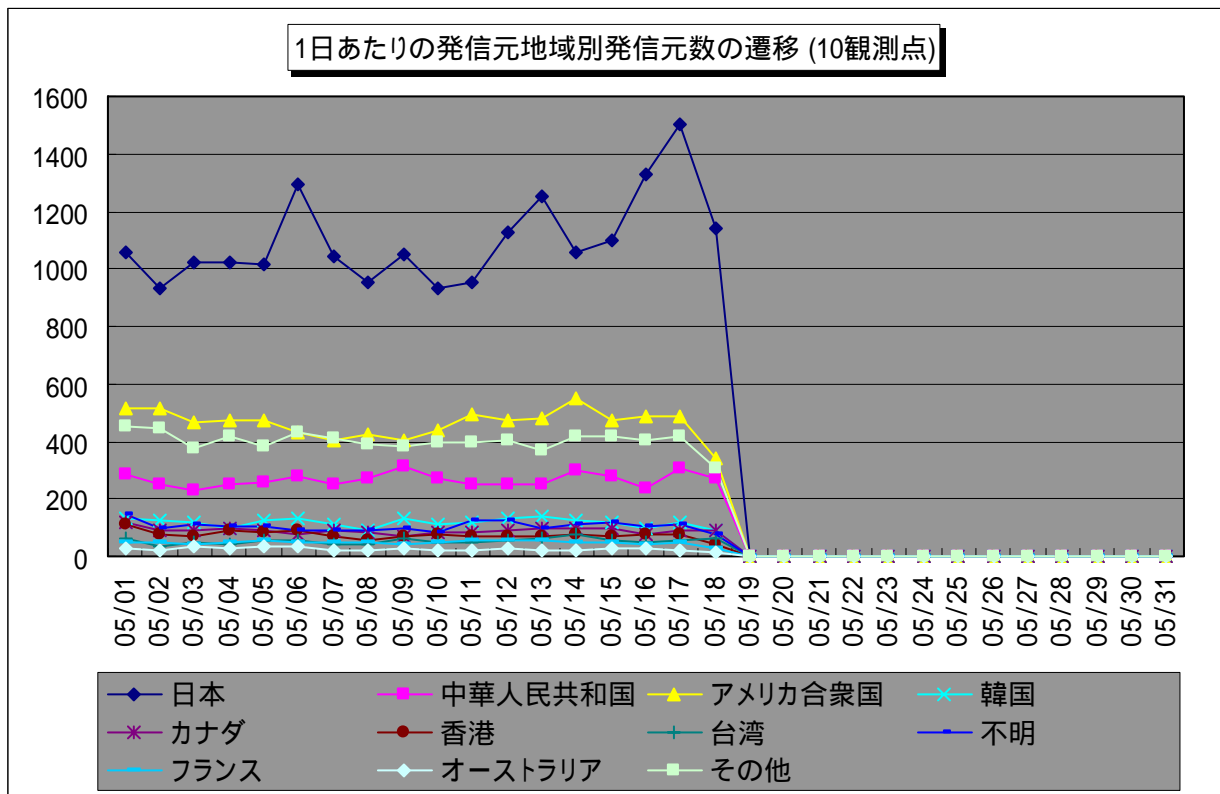


【図 2.4.1 2007年5月の発信元地域別アクセス数の変化】

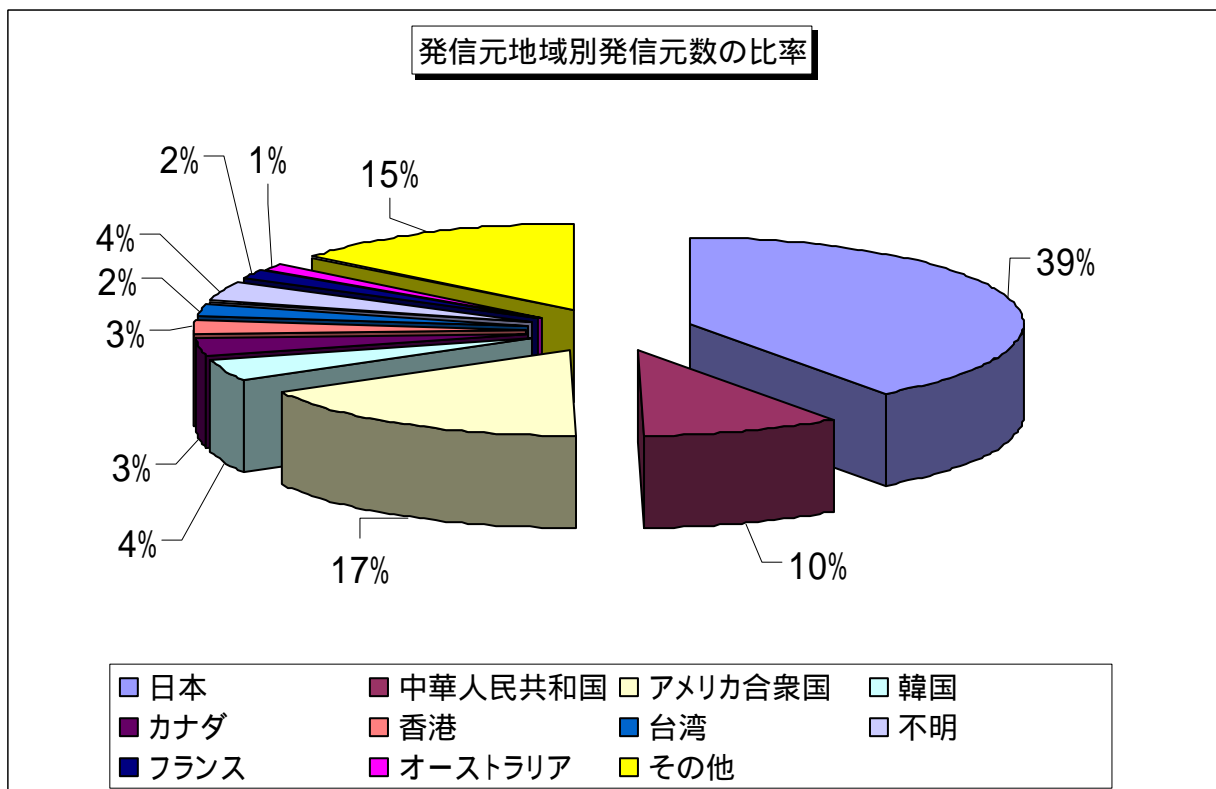


【図 2.4.2 2007年5月の発信元地域別アクセス数の比率】

2007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2.3.4に示します。



【図 2.4.3 2007 年 5 月の発信元地域別発信元数の変化】

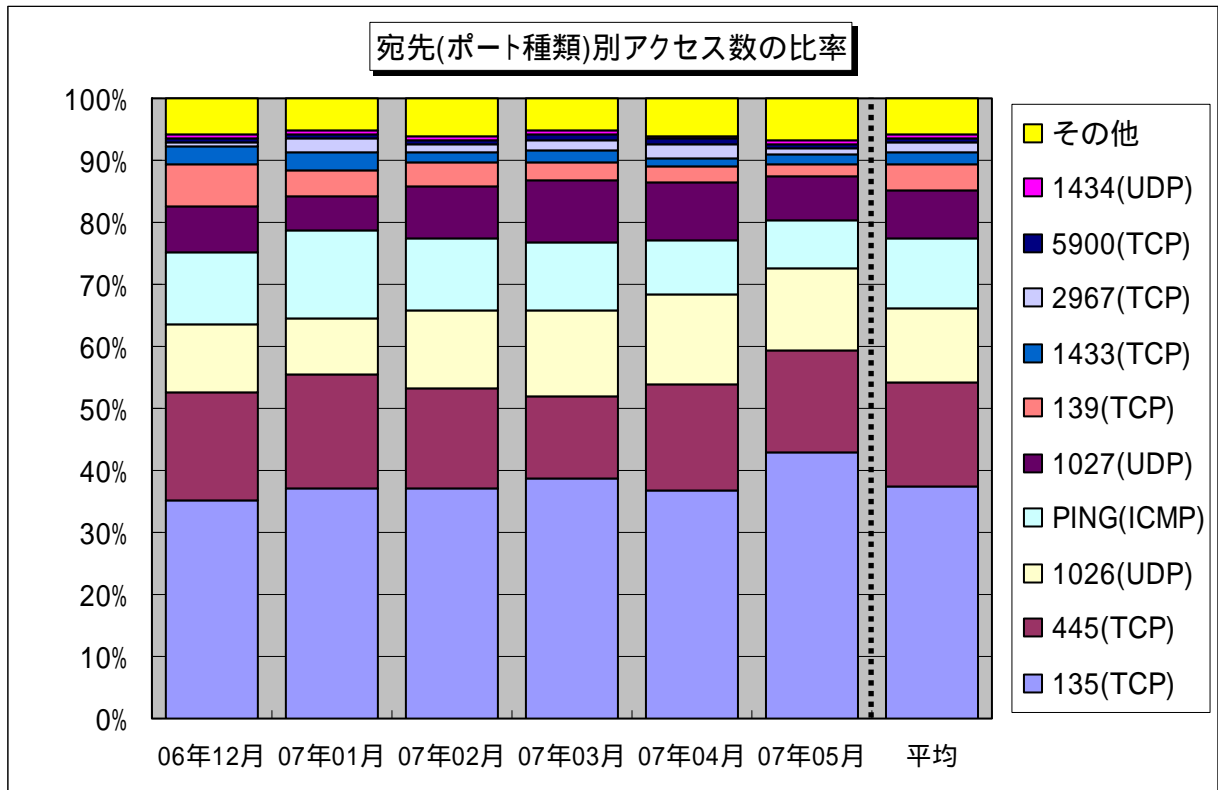


【図 2.4.4 2007 年 5 月の発信元地域別発信元数の比率】

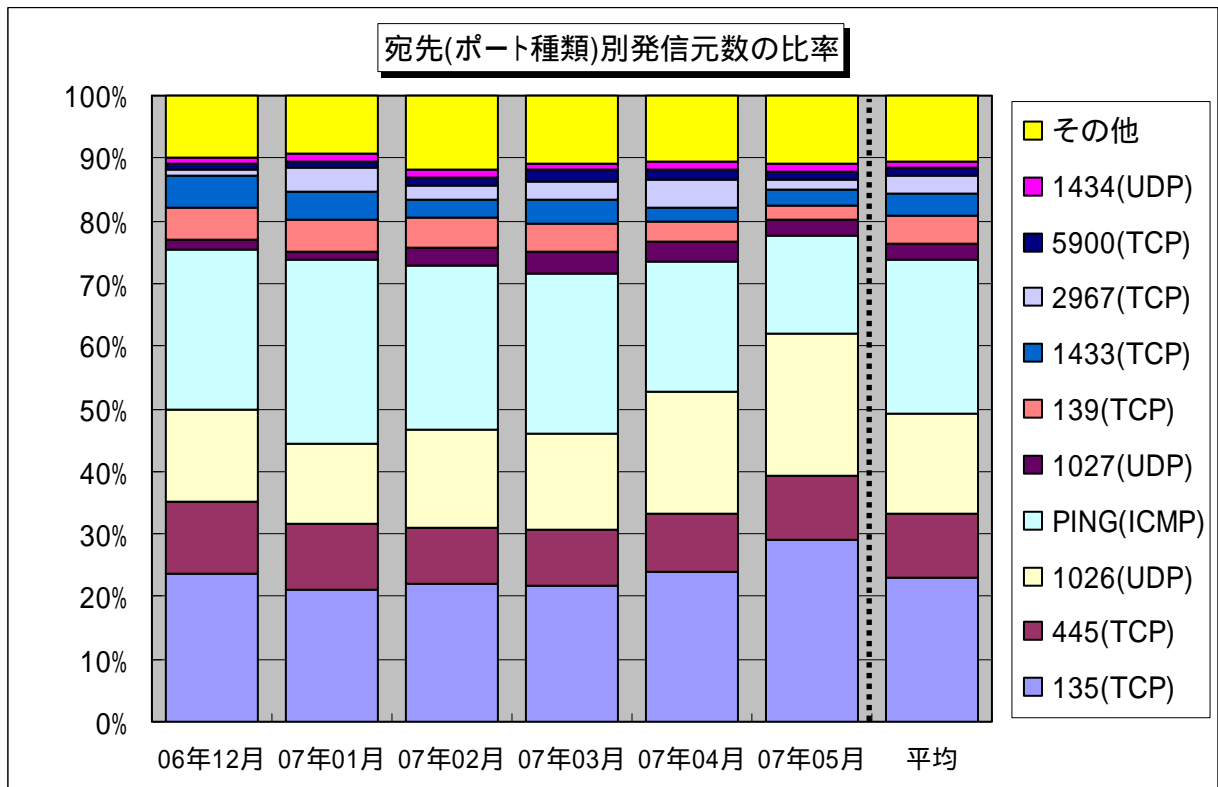
3. 統計情報

3.1 2006年12月～2007年5月の宛先(ポート種類)別の比率

2006年12月～2007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。



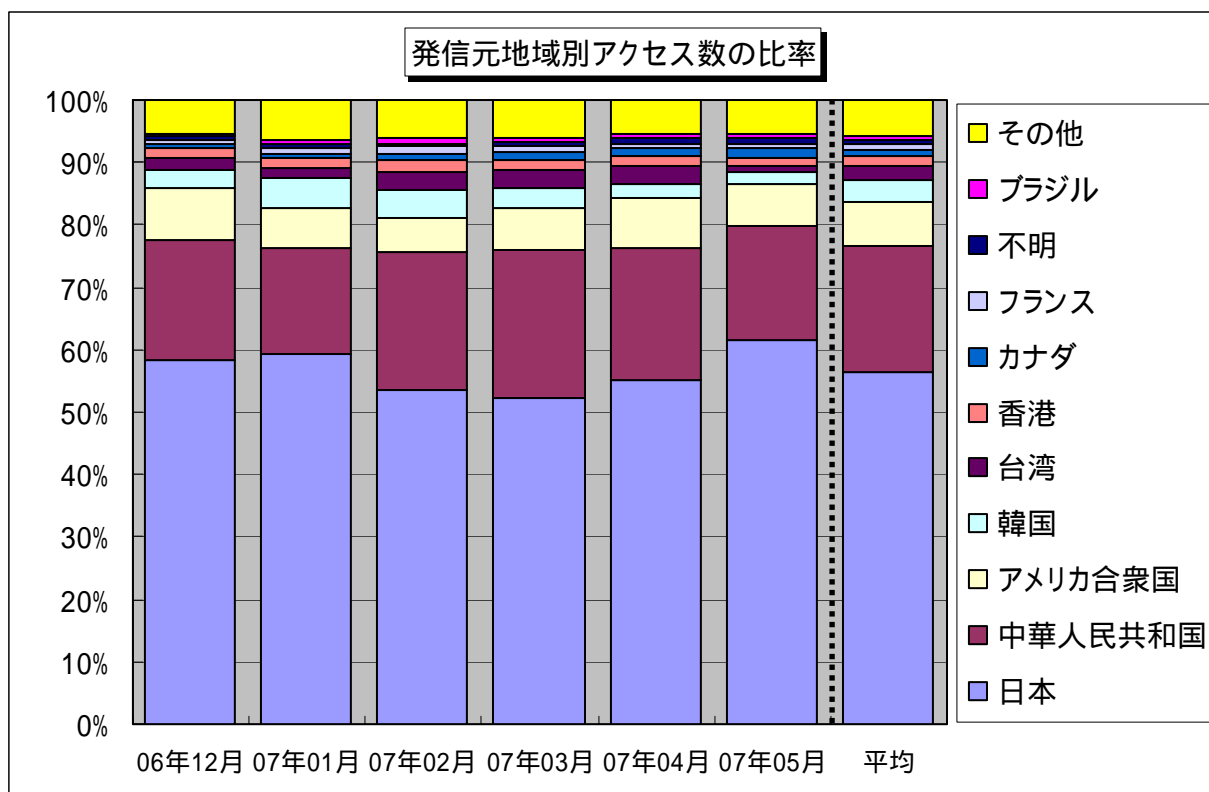
【図 3.1.1 2006年12月～2007年5月の宛先(ポート種類)別アクセス数の比率】



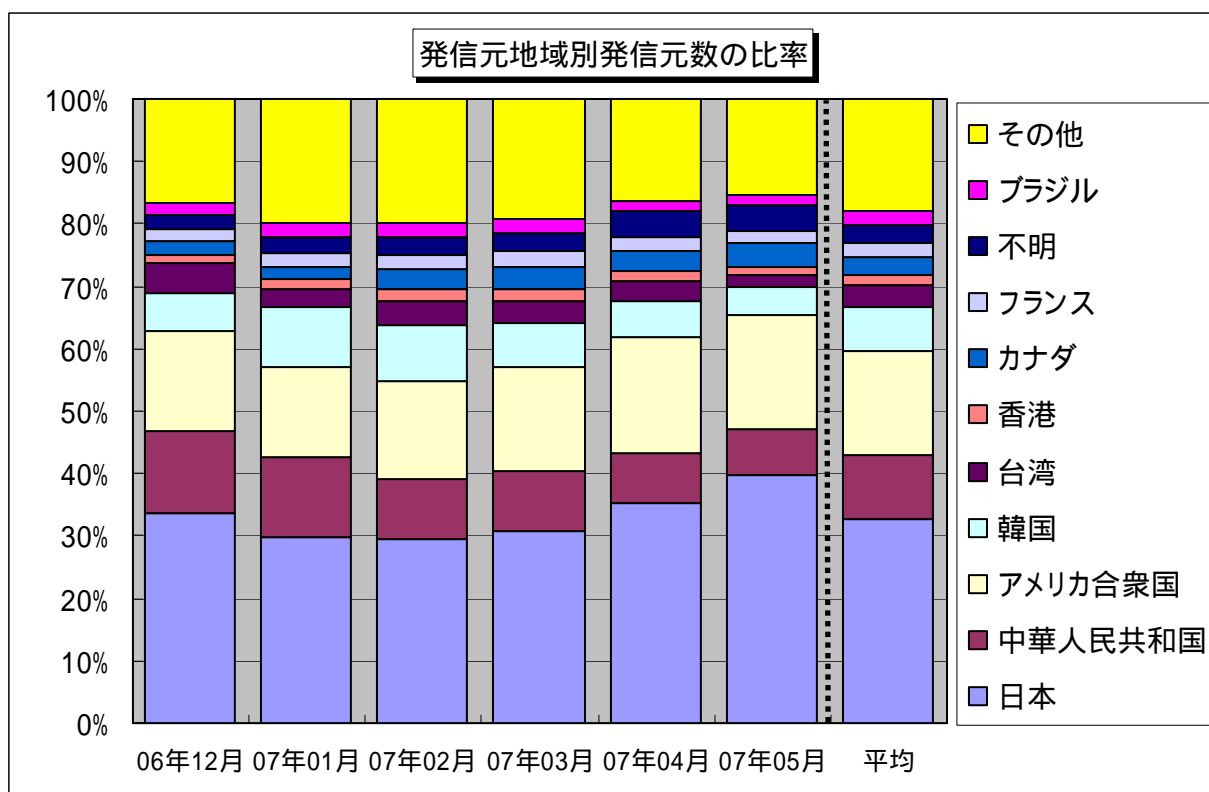
【図 3.1.2 2006年12月～2007年5月の宛先(ポート種類)別発信元数の比率】

3.2 2006年12月～2007年5月の発信元地域別の比率

2006年12月～2007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 2006年12月～2007年5月の発信元地域別アクセス数の比率】



【図 3.2.2 2006年12月～2007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、2007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
135(TCP)	Microsoft Windows Remote Procedure Call(RPC)のデフォルトポートであり、RPCに関するぜい弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster など)
445(TCP)	保護のあまいファイル(ネットワーク)共有や Windows2000 特有のぜい弱性を狙った不正アクセスが有名 (W32/Sasser など)
1026(UDP)/1027(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
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 のぜい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 のぜい弱性を狙った不正アクセスなど
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ぜい弱性を狙ったものと考えられます
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
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)

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
花村 / 加賀谷 / 宮本

Tel:03-5978-7527 Fax:03-5978-7518

E-mail:isec-info@ipa.go.jp