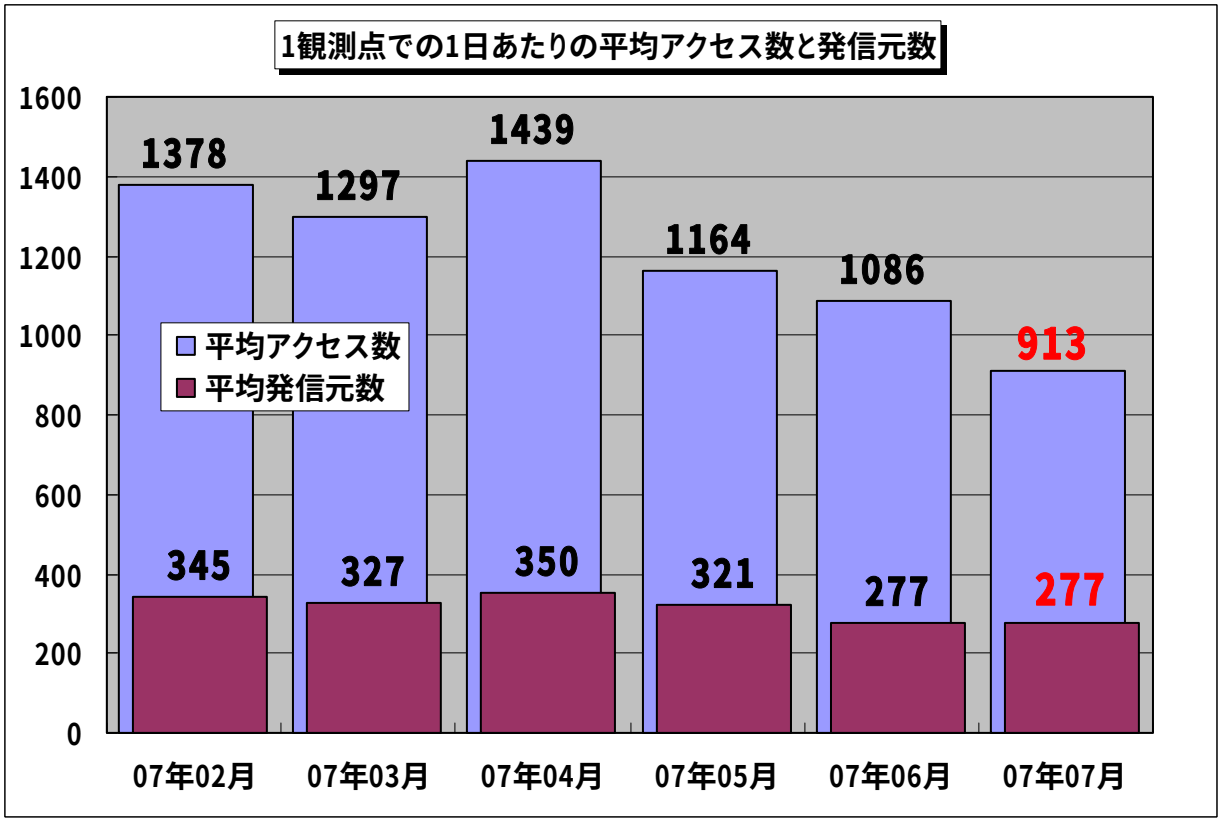
別紙 3

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、2007 年 7 月の期待しない（一方的な）アクセスの総数は、10 観測点で **282,889 件**ありました。1 観測点で 1 日あたり **277** の発信元から **913 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、277 人の見知らぬ人(発信元)から、発信元一人当たり 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】

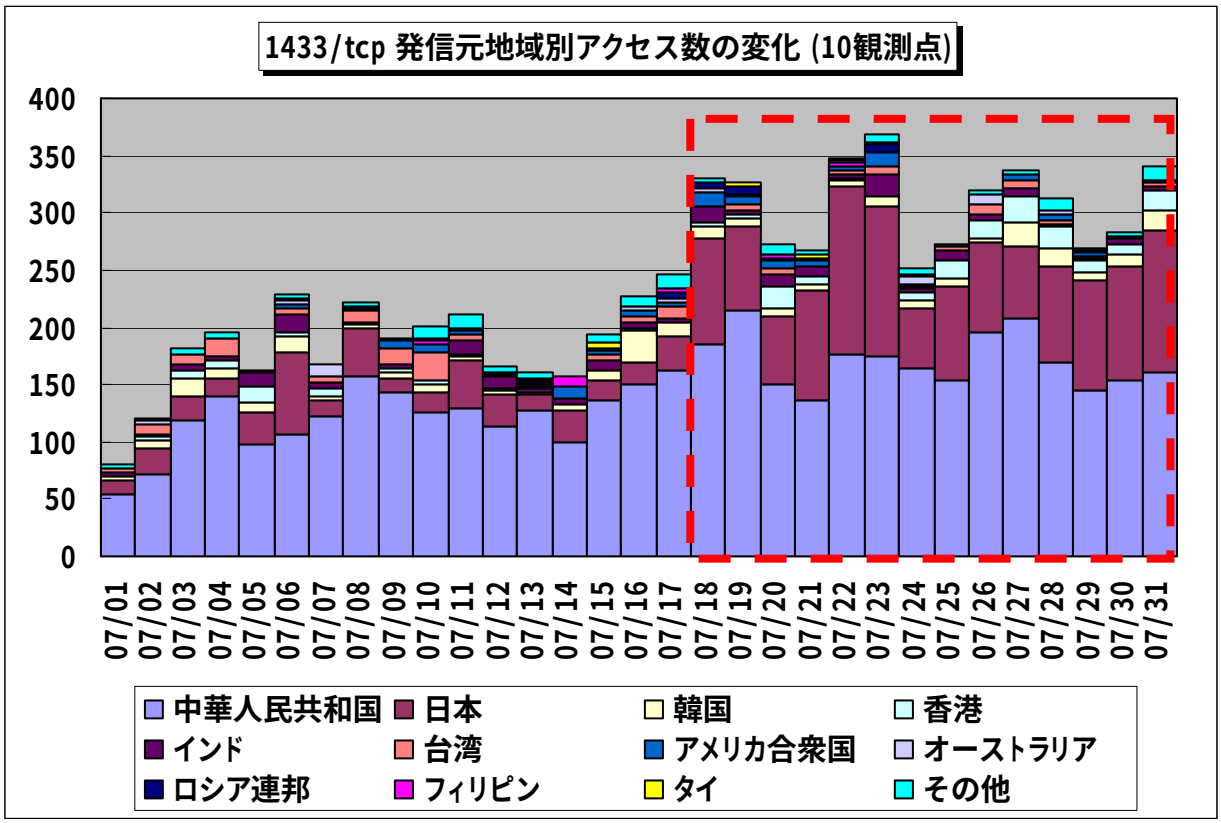
2007 年 2 月～2007 年 7 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、期待しない（一方的な）アクセスは、緩やかですが減少傾向にあるようです。

2．7 月のアクセス状況

2007 年 7 月のアクセス状況は、全体的に 6 月と同じで定常化していると言えます。その中において、Microsoft SQL Server のぜい弱性を狙った、1433/tcp のアクセスや、Symantec 社のセキュリティ対策ソフトのぜい弱性を狙った、2967/tcp のアクセスなど、アプリケーションソフトウェアのぜい弱性を狙ったアクセスが増加しました。

2.1. アプリケーションソフトウェアのぜい弱性を狙ったアクセス

2007 年 7 月の後半辺りから、1433/tcp ポートのアクセスが増加しました。これは、Microsoft SQL Server のぜい弱性を狙ったもので、主に中国や日本からのアクセスです。



【図 2.1.1 2007 年 7 月の 1433/tcp ポートへの発信元地域別アクセス数の変化】

日本からのアクセスの中には、Windows のぜい弱性を狙った、135/tcp、139/tcp、445/tcp を同時に狙ったアクセスも多いことから、ボットに感染したコンピュータからの感染活動（ボットの感染を広げようとしているアクセス）と思われます。

日本以外のアクセスを見てみると、中国、韓国、香港などからは、Symantec 社のセキュリティ対策ソフトのぜい弱性を狙った、2967/tcp や、MySQL（オープンソース SQL データベース）の稼動するサーバを狙った、3306/tcp を同時に狙ったアクセスもあります。（図 2.1.2、2.1.3 参照）

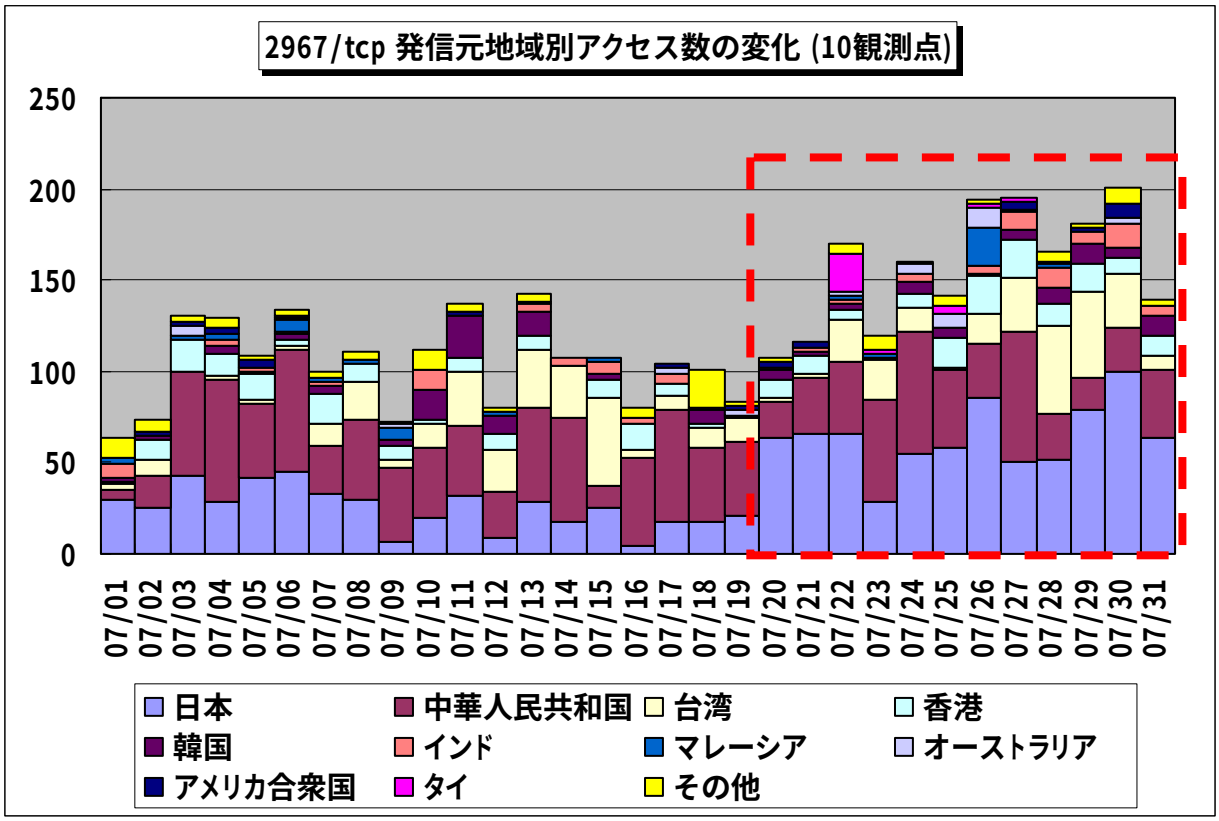
これらのアクセスは、日本で感染活動しているボットとは異なる種類のボットに感染したコンピュータからの感染活動と思われます。これにより、未だにボットに感染しているコンピュータが多いことが伺えます。

ボットは、感染していることに気づきにくいウイルスです。下記のサイトより、駆除ツールをダウンロードし、手順にしたがってボットの駆除を実行することをお勧めします。

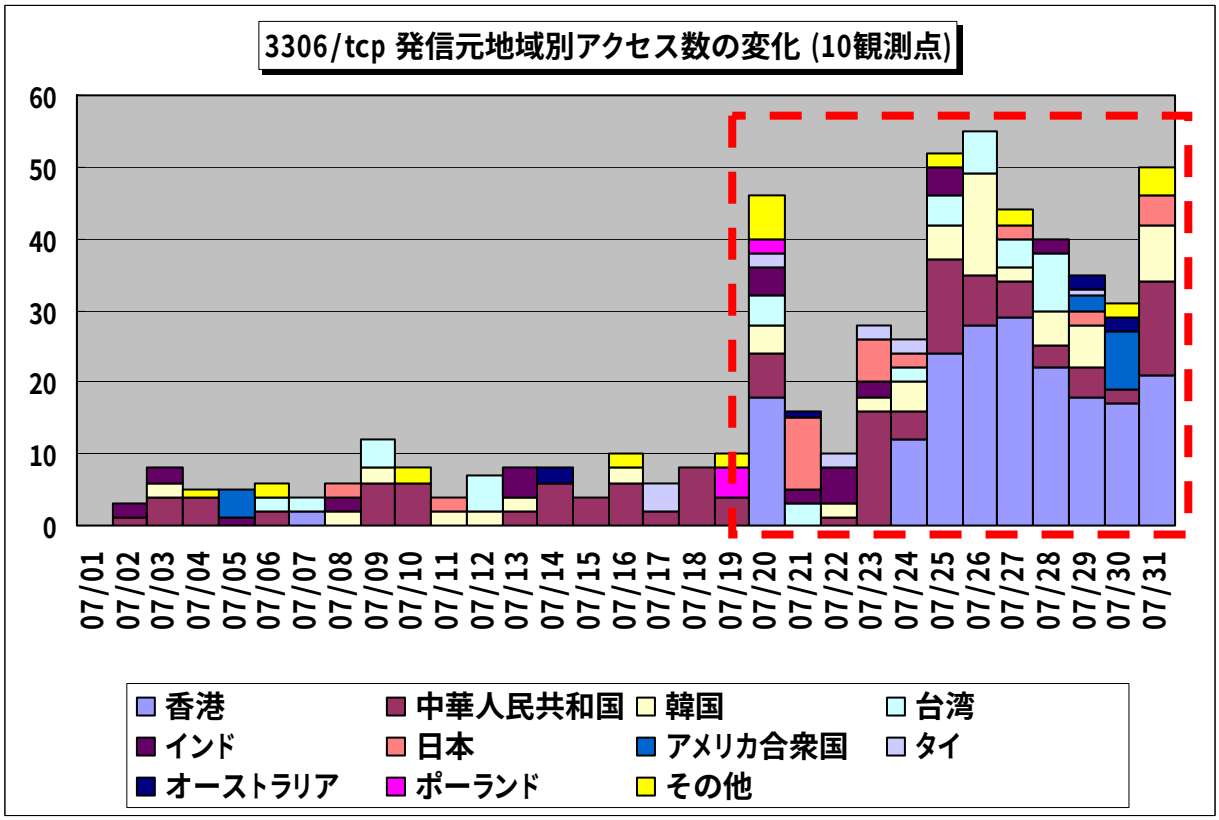
（参考情報）

■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html

■ 2007 年 6 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200706/0706monthly.html



【図 2.1.2　2007 年 7 月の 2967/tcp ポートへの発信元地域別アクセス数の変化】



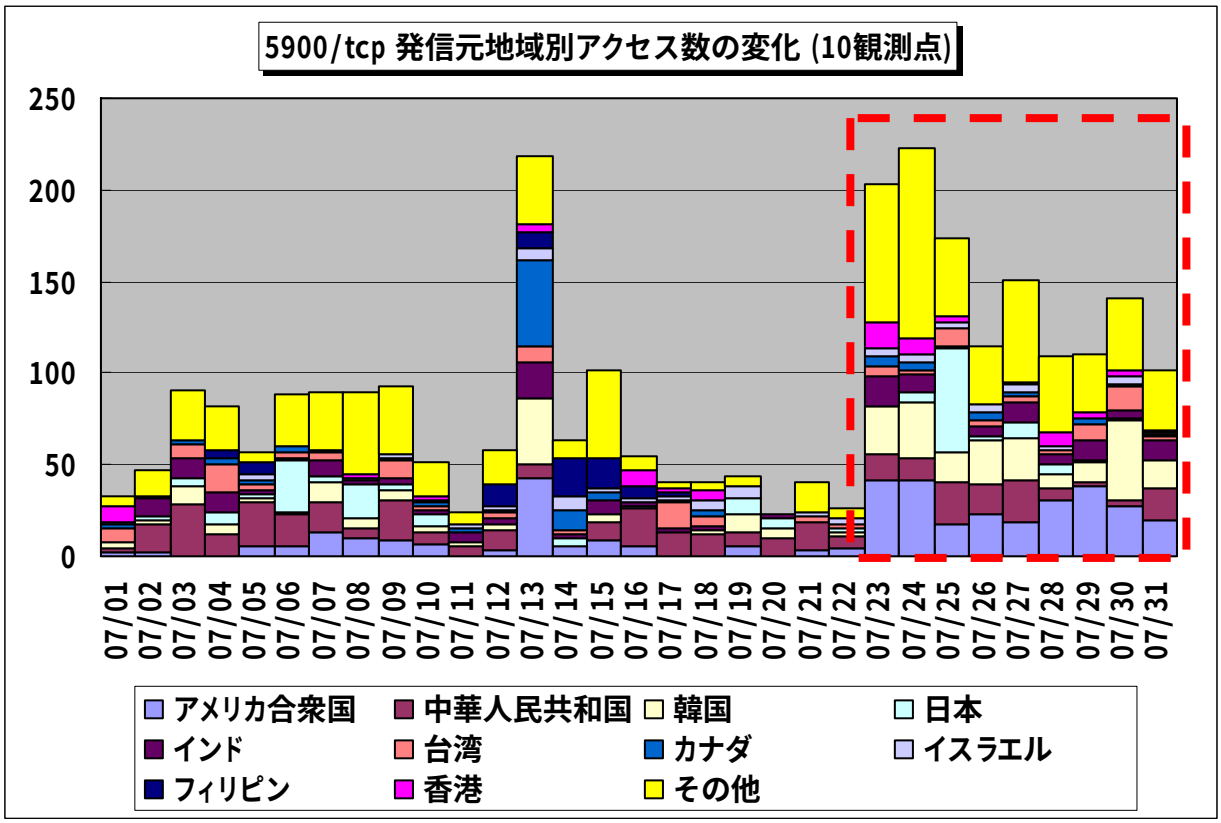
【図 2.1.3　2007 年 7 月の 3306/tcp ポートへの発信元地域別アクセス数の変化】

このほかに、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 5900/tcp ポートへのアクセスについても、同じタイミングで増加しました。(図 2.1.4 参照)

このアクセスは、リモートから攻撃先のコンピュータへ侵入を試みるものであり、このようなツールを利用して、サーバを運用しているシステムの管理者は、運用方法の再点検やぜい弱性の解消を怠らないようにして下さい。

(参考情報)

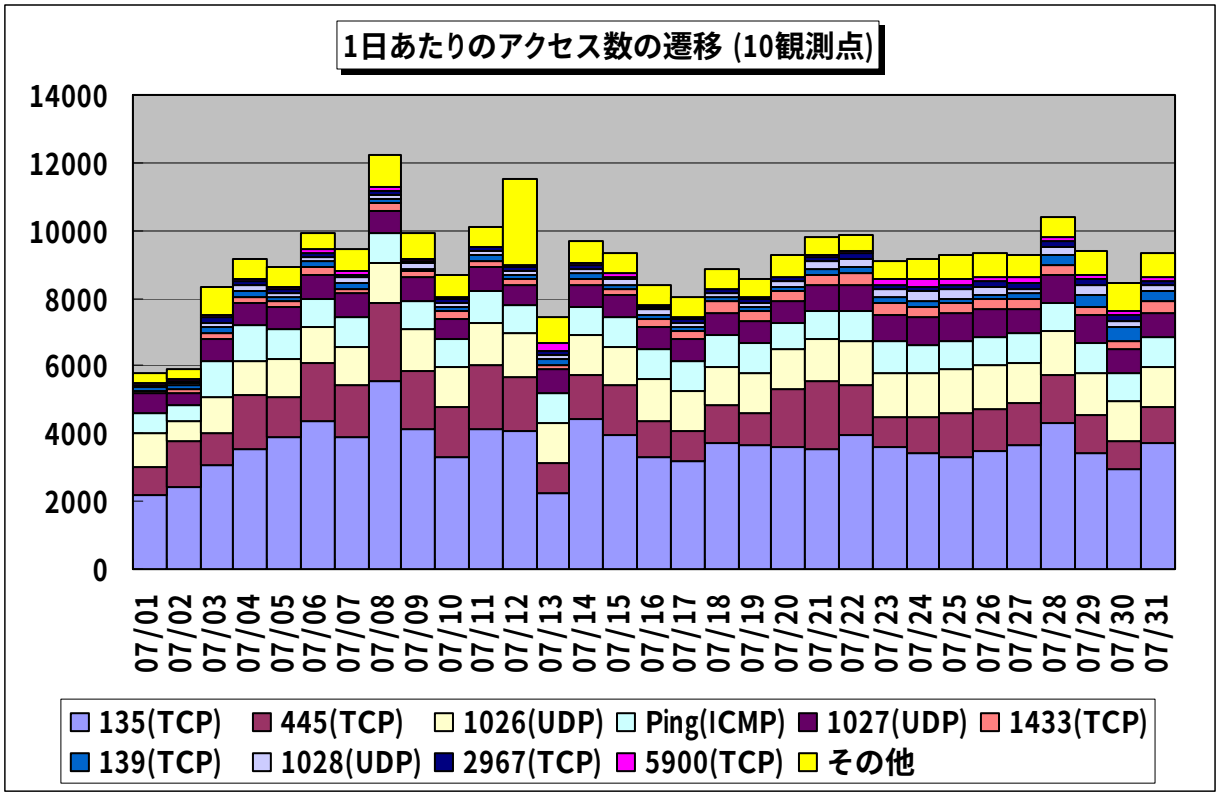
■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/index.html



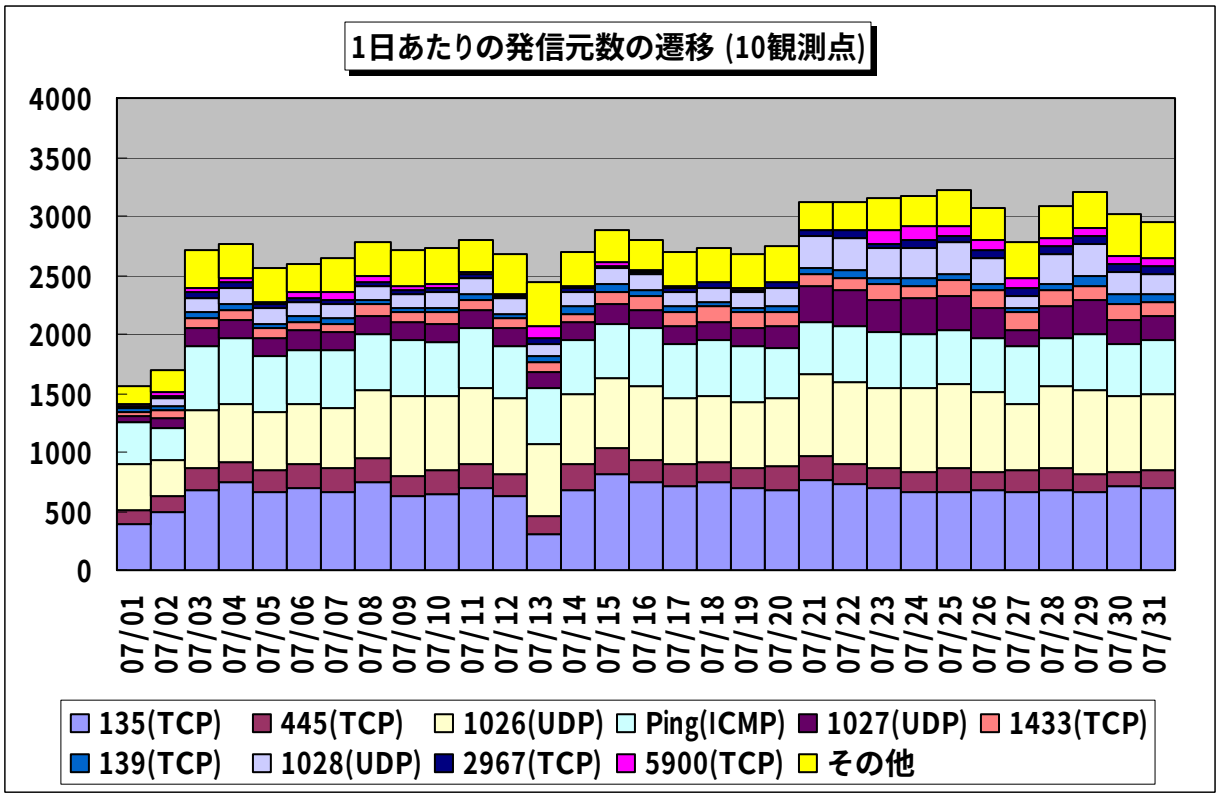
【図 2.1.4 2007 年 7 月の 5900/tcp ポートへの発信元地域別アクセス数の変化】

2.2 2007 年 7 月の一方的なアクセス状況

2007 年 7 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。



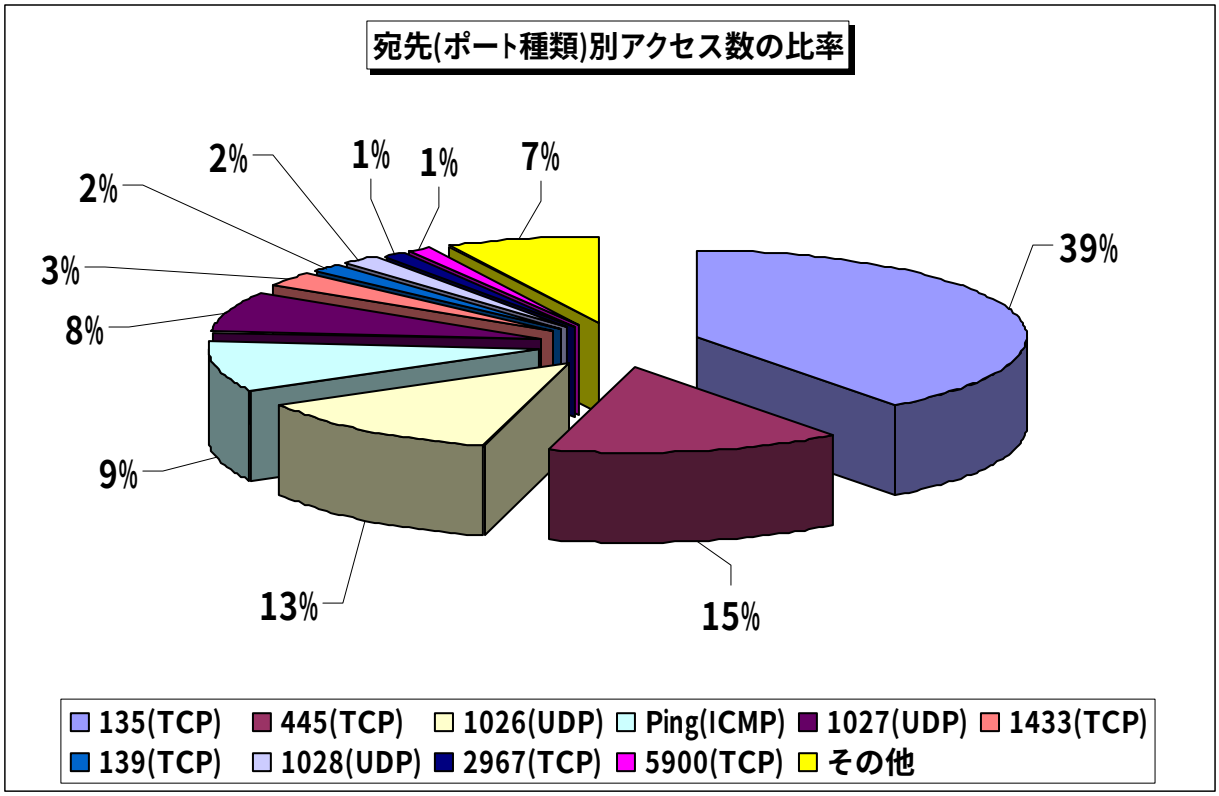
【図 2.2.1 2007 年 7 月の一方的なアクセス状況(アクセス数)】



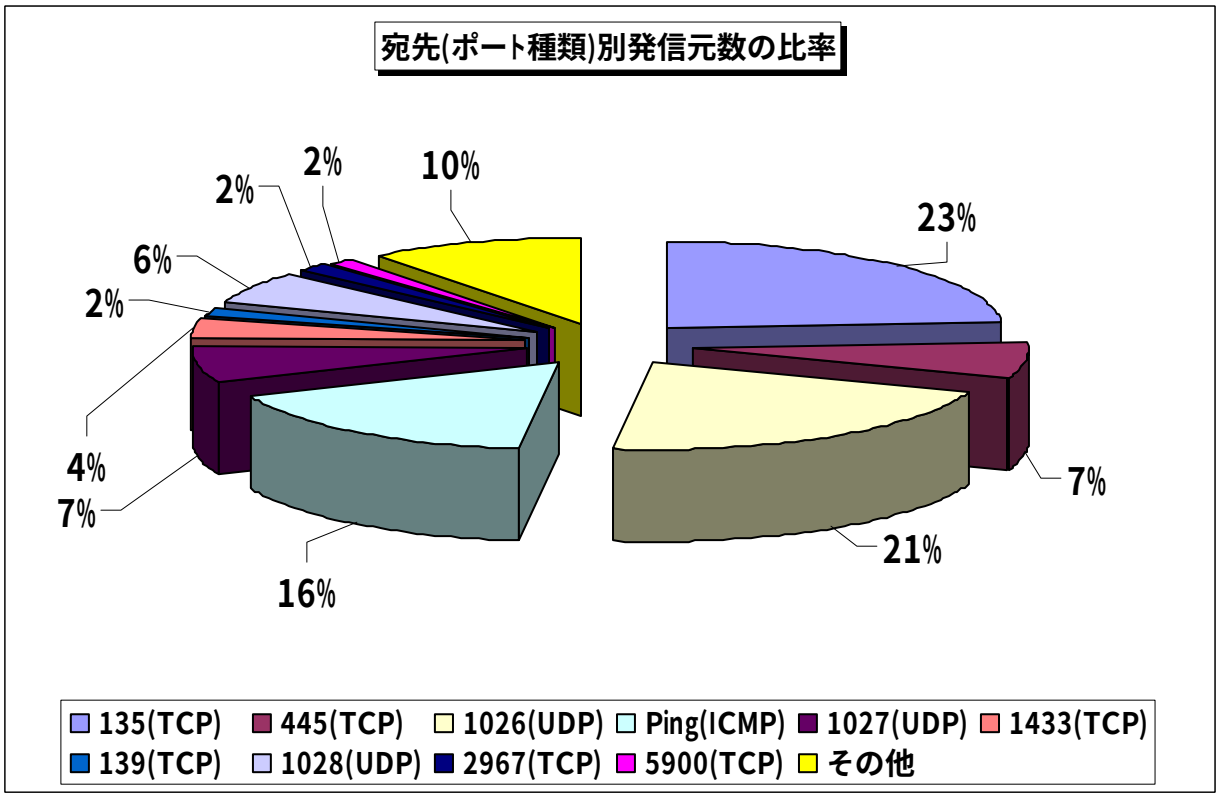
【図 2.2.2 2007 年 7 月の一方的なアクセス状況(発信元数)】

2.3 2007 年 7 月の宛先(ポート種類)別の比率

2007 年 7 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。



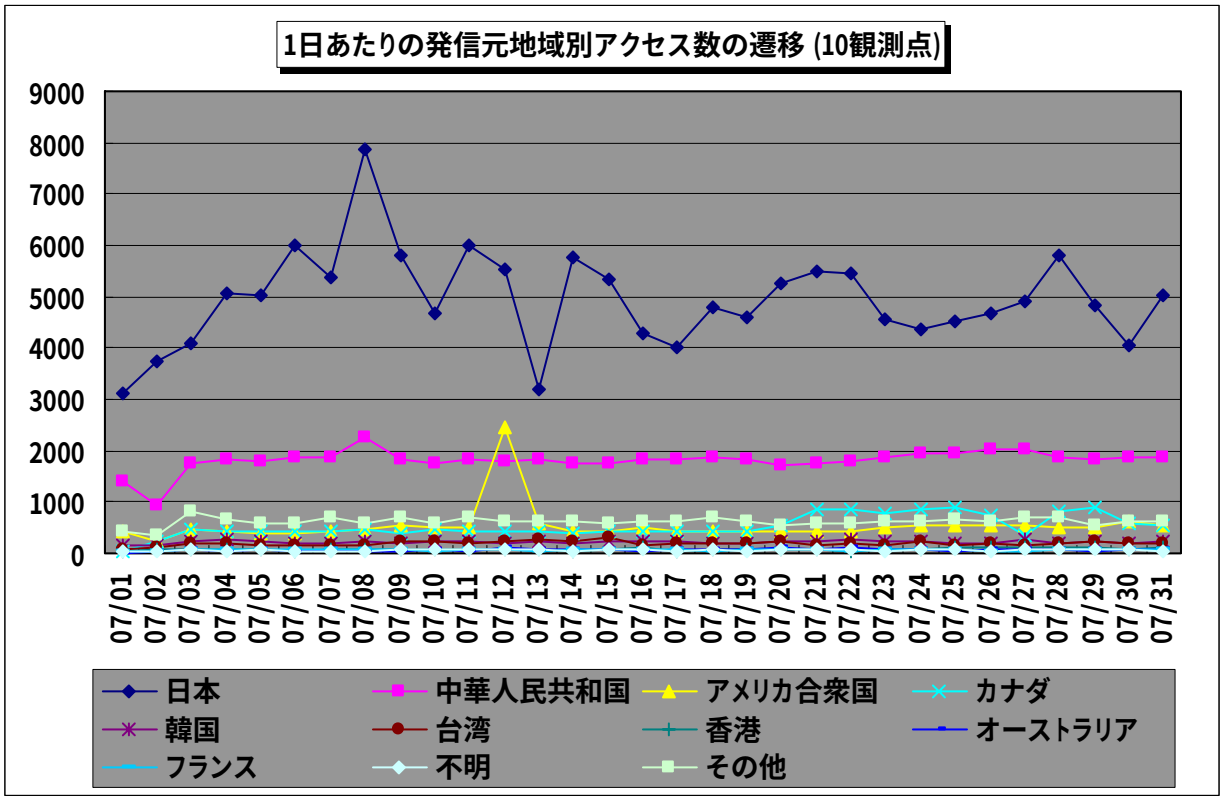
【図 2.3.1 2007 年 7 月の宛先(ポート種類)別アクセス数の比率】



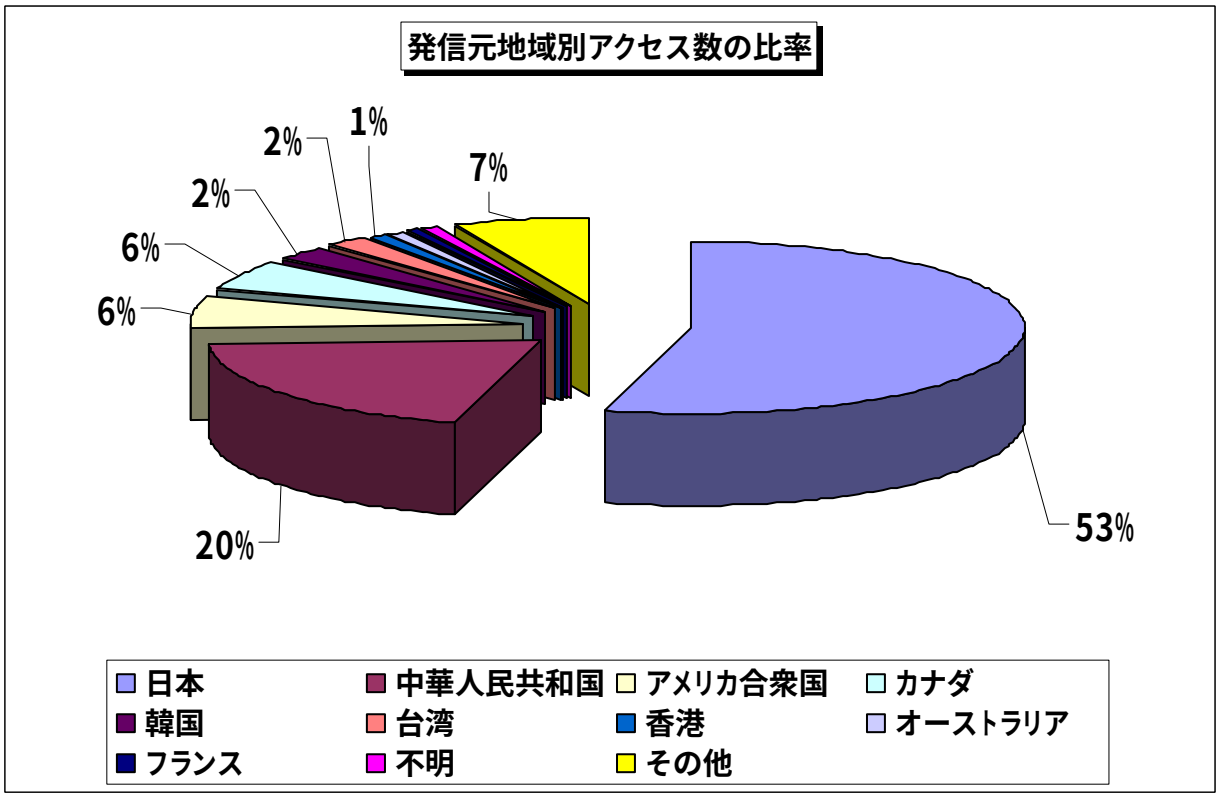
【図 2.3.2 2007 年 7 月の宛先(ポート種類)別発信元数の比率】

2.4 2007 年 7 月の発信元地域別アクセス状況

2007 年 7 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。

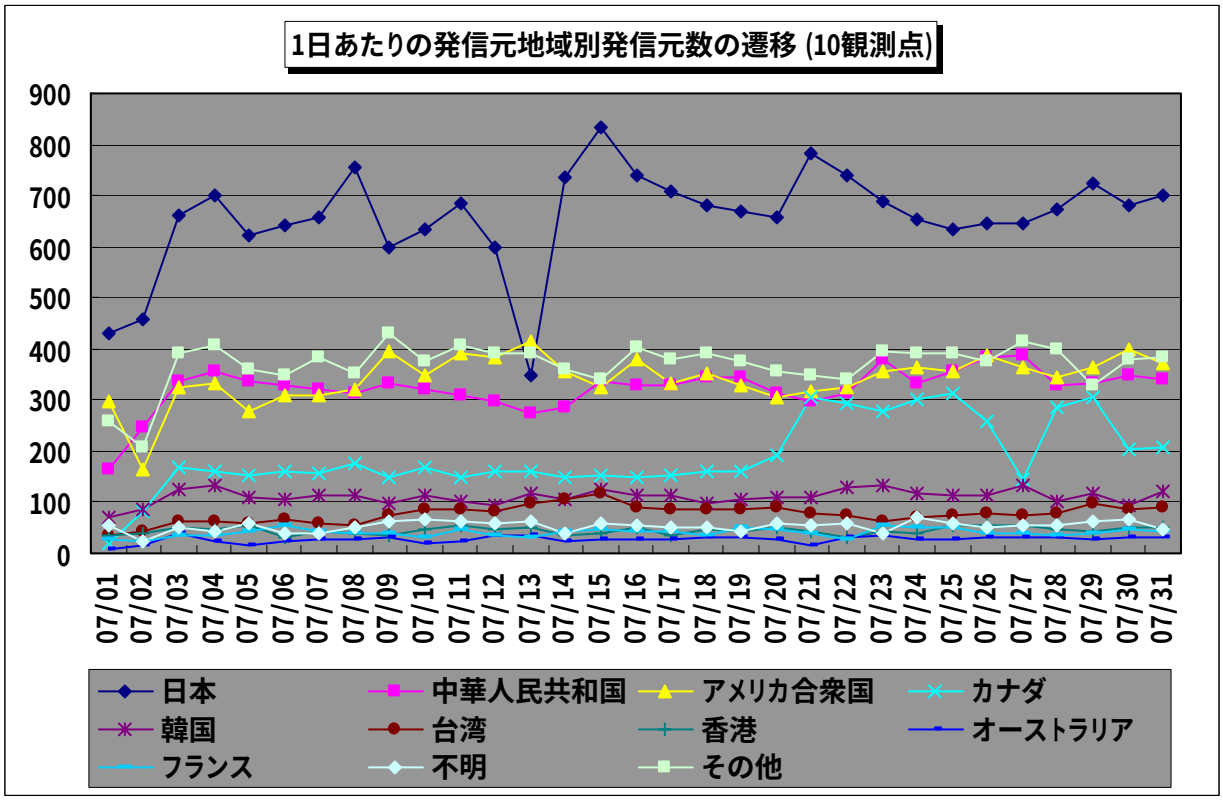


【図 2.4.1 2007 年 7 月の発信元地域別アクセス数の変化】

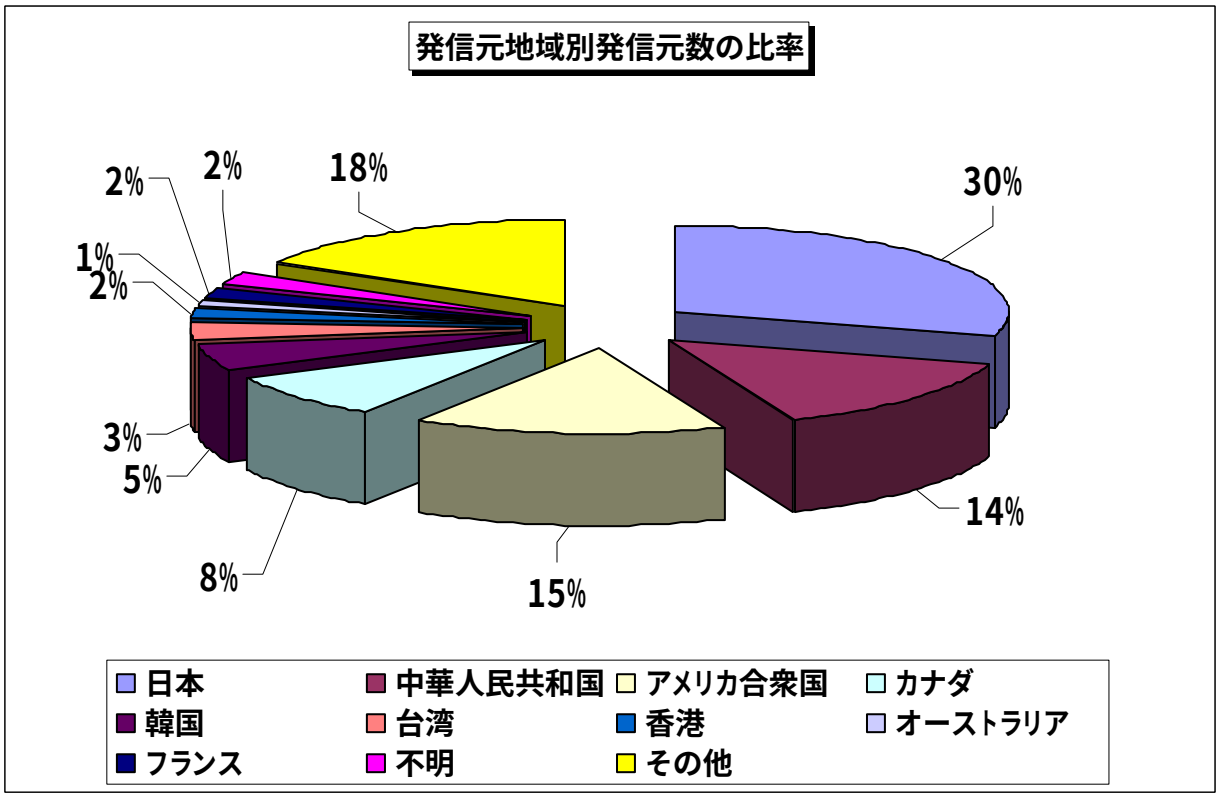


【図 2.4.2 2007 年 7 月の発信元地域別アクセス数の比率】

2007 年 7 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 2007 年 7 月の発信元地域別発信元数の変化】

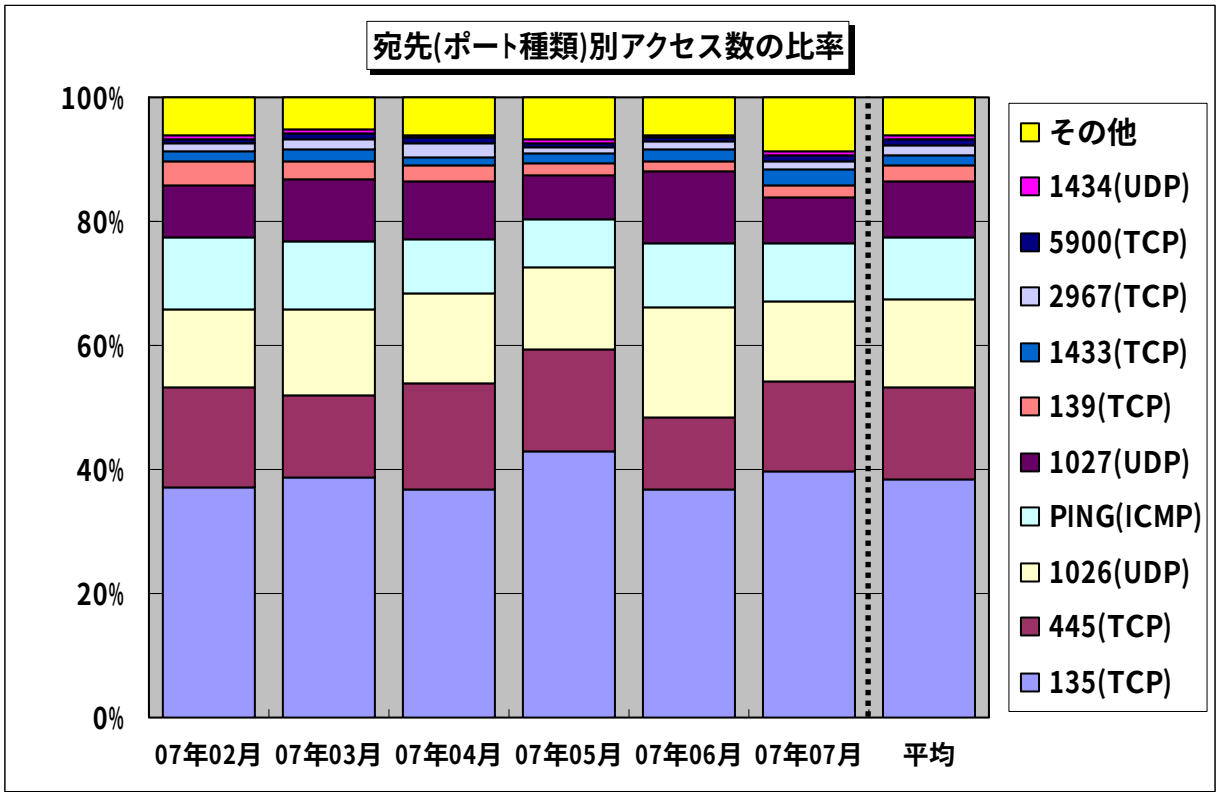


【図 2.4.4 2007 年 7 月の発信元地域別発信元数の比率】

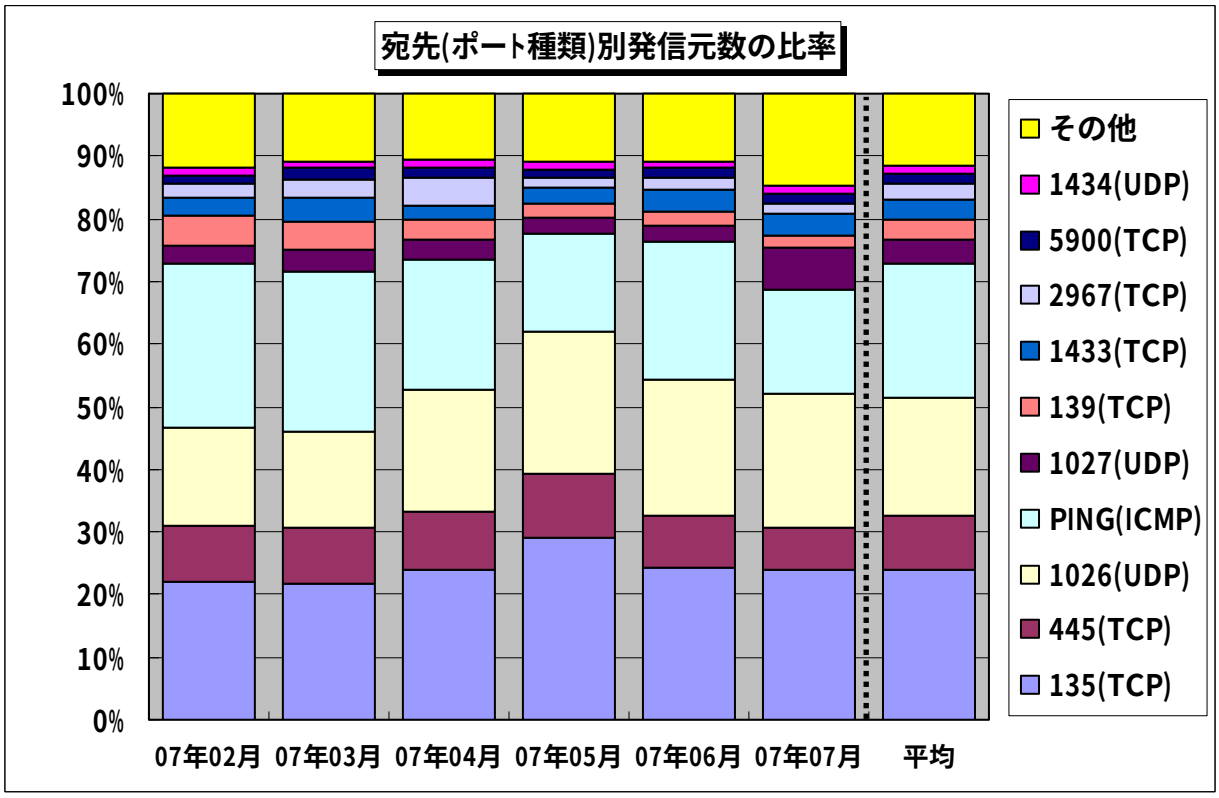
3．統計情報

3.1 2007 年 2 月～2007 年 7 月の宛先(ポート種類)別の比率

2007 年 2 月～2007 年 7 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。



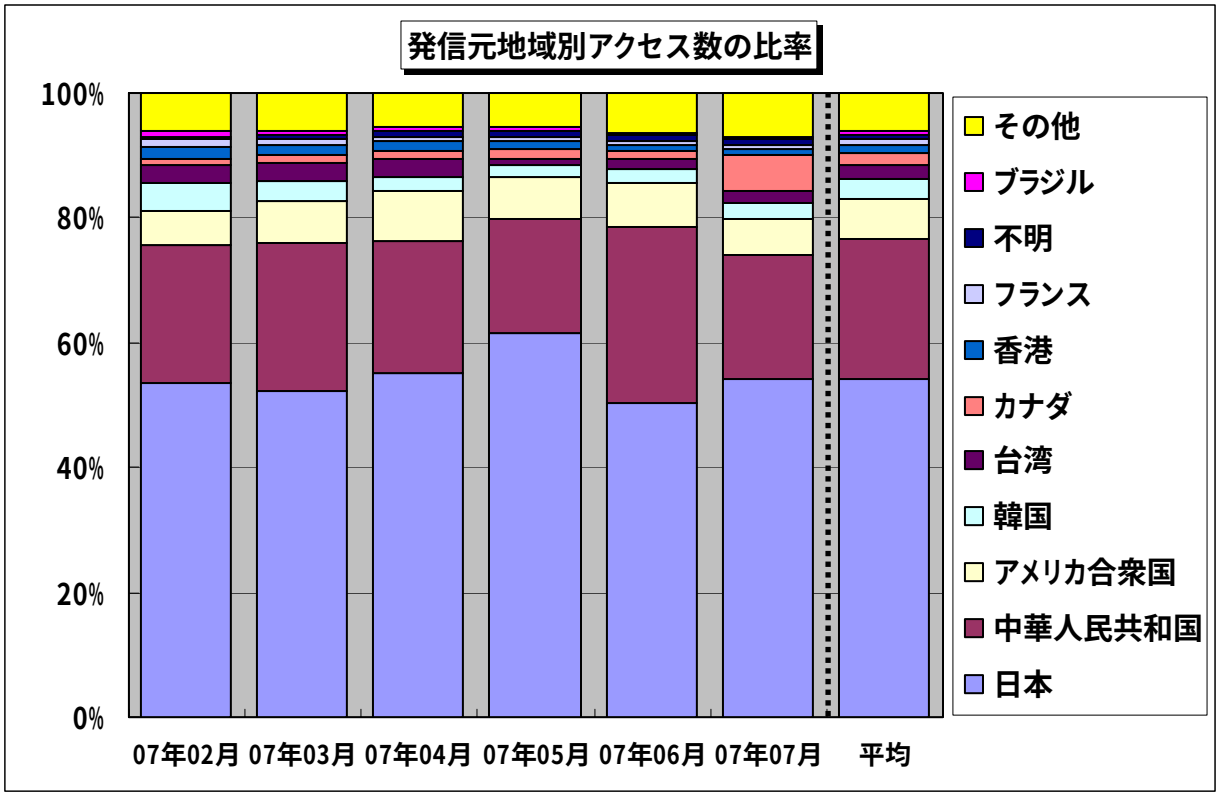
【図 3.1.1 2007 年 2 月～2007 年 7 月の宛先(ポート種類)別アクセス数の比率】



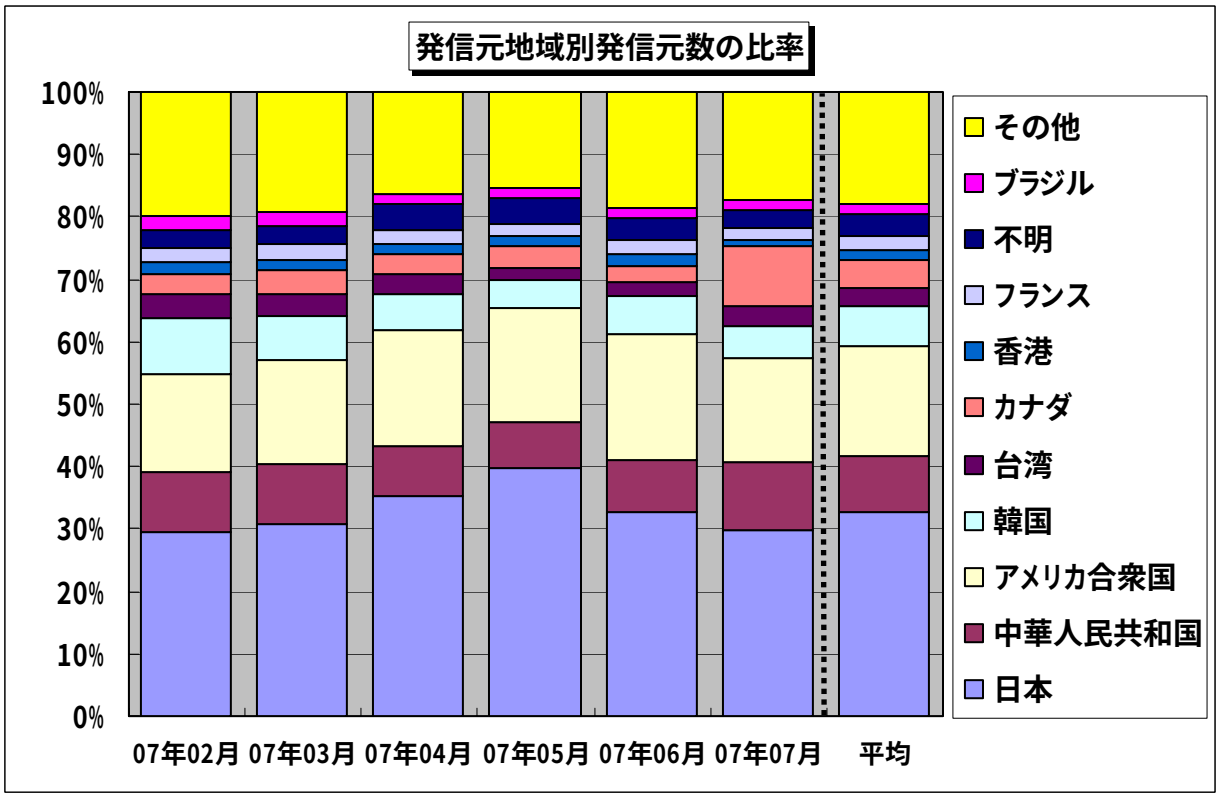
【図 3.1.2 2007 年 2 月～2007 年 7 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 2 月～2007 年 7 月の発信元地域別の比率

2007 年 2 月～2007 年 7 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 2 月～2007 年 7 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 2 月～2007 年 7 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 7 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
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
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
1028(UDP)	1026(UDP)/1027(UDP)と同じアクセス
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

■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