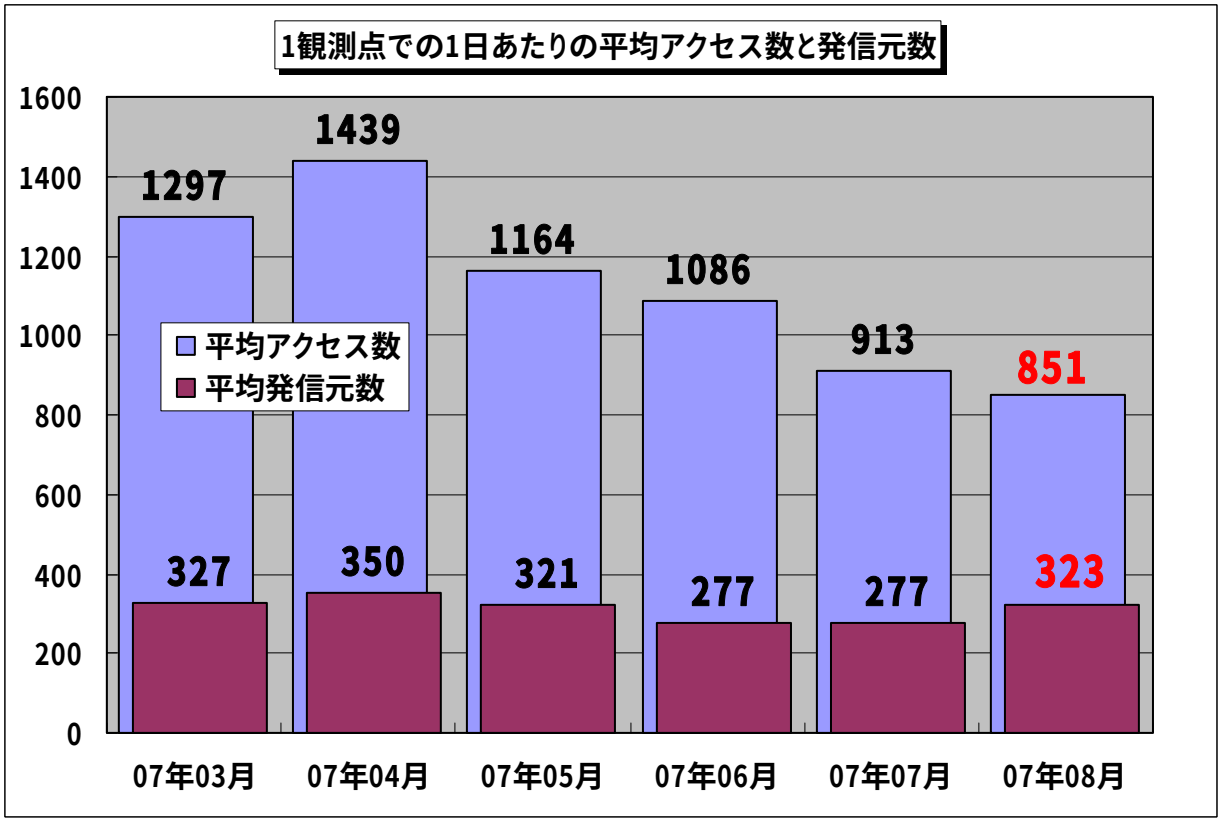
別紙 3

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 8 月の期待しない（一方的な）アクセスの総数は、10 観測点で **263,940 件**ありました。1 観測点で 1 日あたり **323** の発信元から **851 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、323 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】

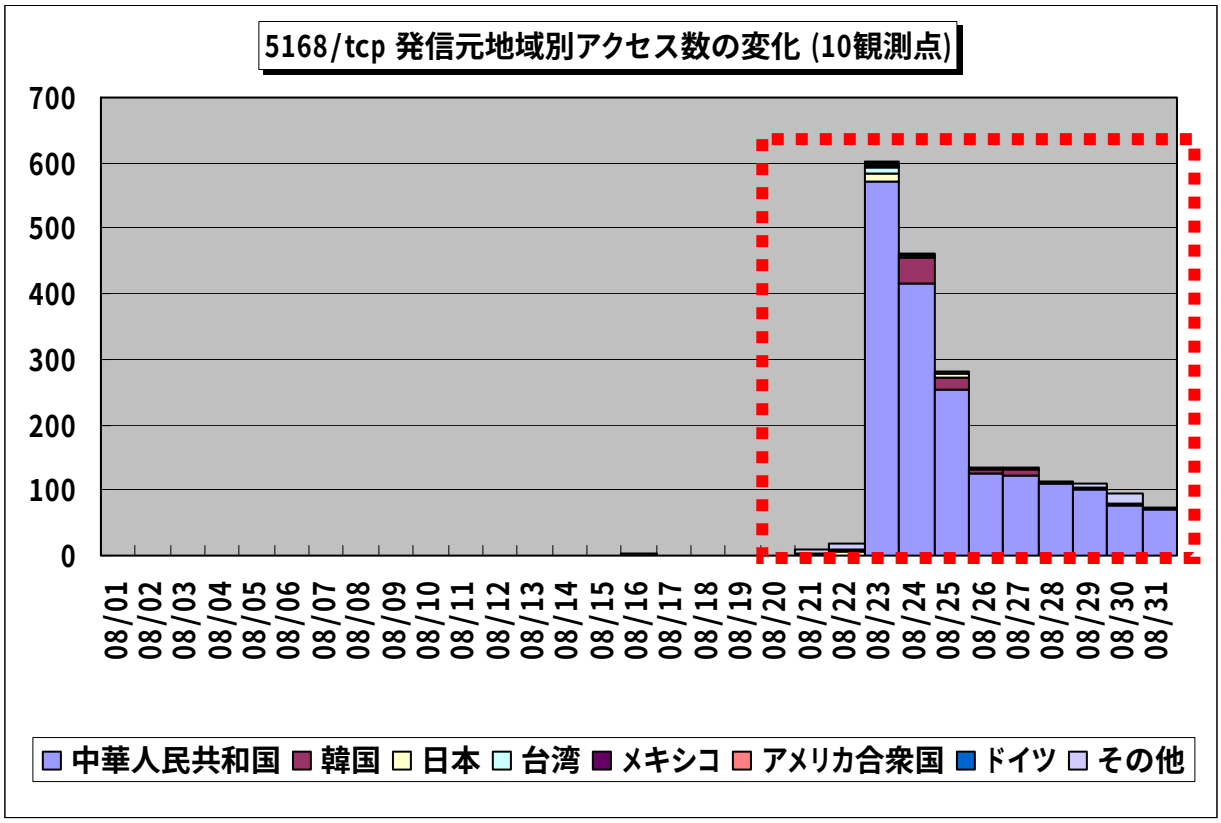
2007 年 3 月～2007 年 8 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、期待しない（一方的な）アクセスは、緩やかですが減少傾向にあります。

2．8 月のアクセス状況

2007 年 8 月のアクセス状況は、全体的に 7 月と同じで定常化していると言えます。その中において、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、1028/udp のアクセス合計数が、全体のアクセスの 4 分の 1 を占めました。また Trend Micro 社の、サーバ版ウイルス対策ソフトの脆弱性を狙ったと思われるアクセスが、一時的に多くありました。

2.1. トレンドマイクロ社サーバ版ウイルス対策ソフトのぜい弱性を狙ったアクセス

トレンドマイクロ社から、サーバ版ウイルス対策ソフトのセキュリティパッチが発表された辺りから、このソフトが管理用として使用する、5168/tcp ポートのアクセスが一時的に増加しました。



【図 2.1.1　2007 年 8 月の 5168/tcp ポートへの発信元地域別アクセス数の変化】

これは、トレンドマイクロ社のサーバ版ウイルス対策ソフトの脆弱性を狙ったアクセスと思われますが、現在は収まった感じに見受けられます。

ですが、この様な脆弱性情報が出されると、忘れた頃にまた同じ脆弱性を狙った攻撃が起こりますので、該当ソフトウェアをお使いの方は、以下の参考情報より早めの対応を行うことをお勧めします。

なお、該当ソフトウェアはサーバで使用するソフトウェアですので、対応にはシステム管理者の指示に従って下さい。

(参考情報)

■ ServerProtect for Windows/NetWare 5.58 用 Security Patch 2(Build_1185)適用のお願い (トレンドマイクロ社)
http://www.trendmicro.co.jp/support/news.asp?id=1003

■ TCP 5168 番ポートへのスキャン増加に関する注意喚起 (JPCERT/CC)
http://www.jpcert.or.jp/at/2007/at070019.txt

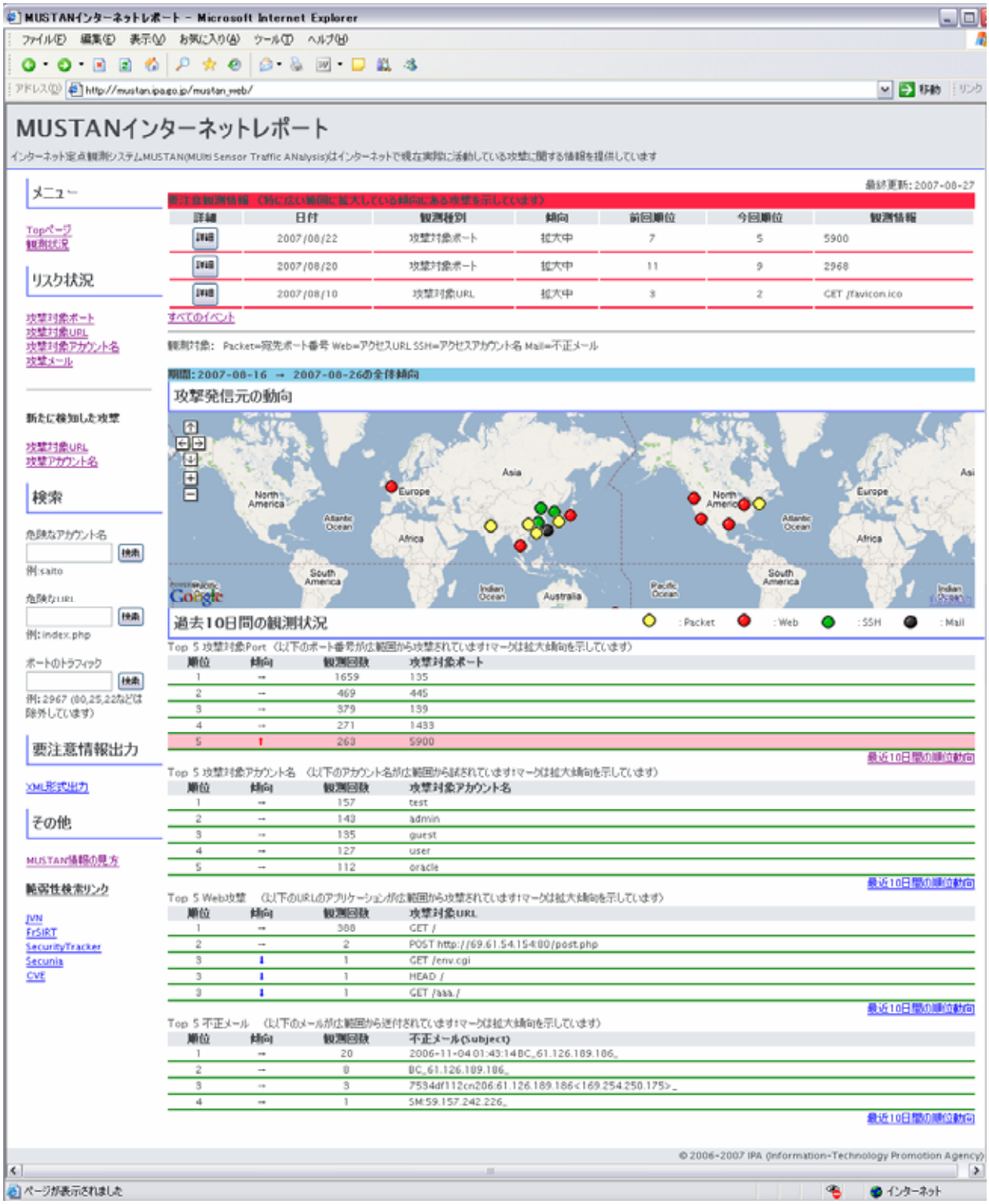
■ JVNTA07-235A Trend Micro ServerProtect に複数の脆弱性
http://jvn.jp/cert/JVNTA07-235A/

2.2 インターネット定点観測システム MUSTAN(Multi Sensor Traffic Analysis)について

MUSTAN は、インターネットで現在実際に活動している攻撃に関する情報を提供しています。実際に広範囲に流行しており、ネットワークユーザが特に注意すべき

- ◆ 新しい
- ◆ 活発な
- ◆ 活発化している

不正アクセスを自動的に検知･報告するシステムとして運用しています。



【図 2.2.1 MUSTAN TOP ページ】

2.2.1 機能概要

定点観測システム MUSTAN は、インターネット上に配置されたセンサによってインターネットに広がっている攻撃を監視しています。監視対象は以下の 4 つです。

- ポートへの不正なアクセス
- HTTP による不正なウェブアクセス
- SSH アカウントへの不正なログインの試み
- 不正なメール

観測された情報を分析し、発信元の数の増加をいち早く検知することで、流行の広がりを確認できます。
合わせて、過去 10 日間の攻撃発信元の動向や、各攻撃の状況が確認できます。

(1) 要注意観測状況

要注意情報では、観測対象不正アクセスの発信元を分析し、その数が特に**大きな増加傾向**を示しているものを抽出しています。ここに警告されている不正アクセスは、当該ポート、関連する URL について、**自サイトでの利用状況**を特に注意する必要があります。
[詳細]ボタンから、その不正アクセスの数、発信元の広がり状況を確認することができます。

(2) リスク状況

リスク状況は、要注意ほどの緊急度ではありませんが、上昇傾向にある不正アクセス、および新規に観測された不正アクセスを示しています [地図]ボタンから、発信元の広がり状況を確認することができます。

(3) 新しいウェブ攻撃

新規に観測されたウェブアクセスの状況を示しています。**ウェブアプリケーションに対する新たな攻撃のバリエーション**などを示しています。 この情報から自サイトで利用しているウェブアプリケーションの URL などを確認することで、関連するウェブアプリケーションの攻撃の有無を検索できます。

(4) 新しい攻撃アカウント

新規に観測された攻撃に利用された SSH アカウントを示しています。自サイトで利用している SSH 用アカウント名などを入力することで、関連の攻撃の有無を検索できます。

(5) 検索機能

MUSTAN が観測した攻撃に使用されている SSH アカウント名、ウェブアプリケーションの URL、ポート番号が検索出来ます。

(6) 要注意情報の XML 出力

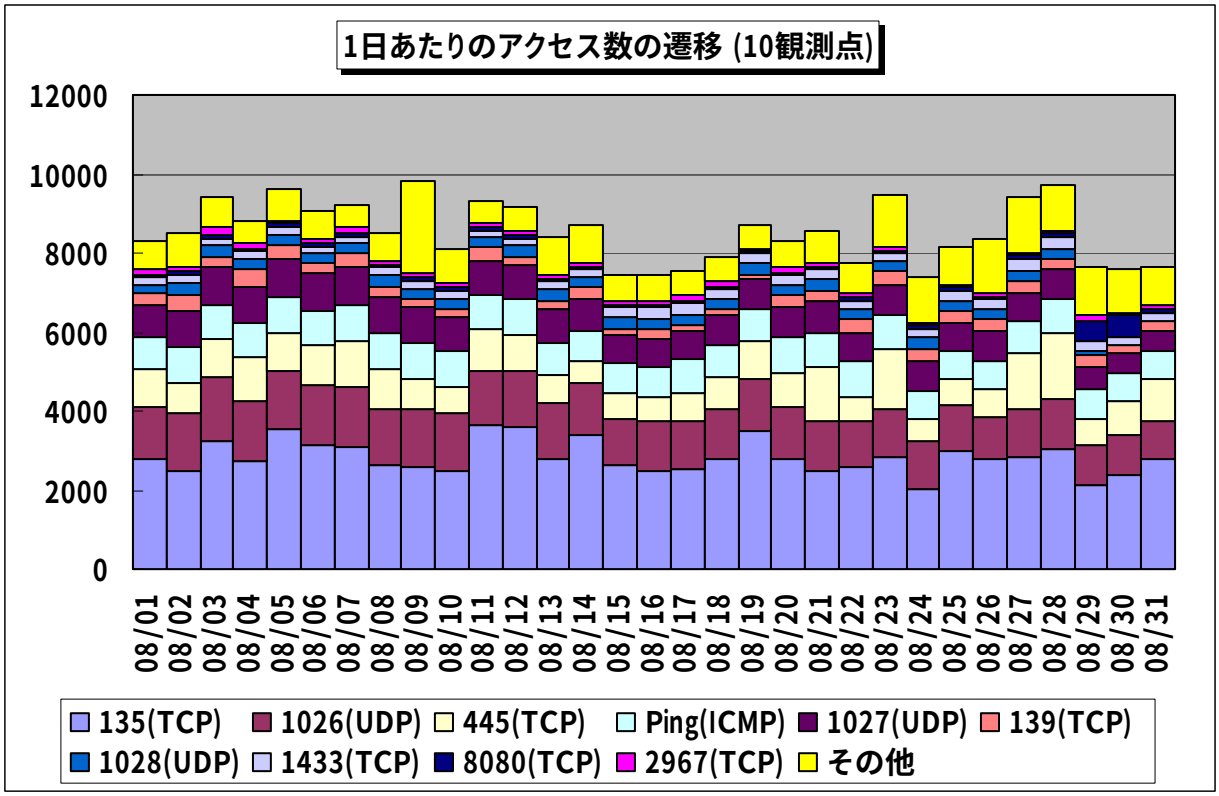
MUSTAN が観測、解析し、特に広い範囲に拡大している傾向にある攻撃の情報を XML ファイルとして取得できます。

IPA では、本システムを 6/29 より運用を開始しています。インターネット上で発生している不正アクセスの状況を把握するために、ご利用下さい。

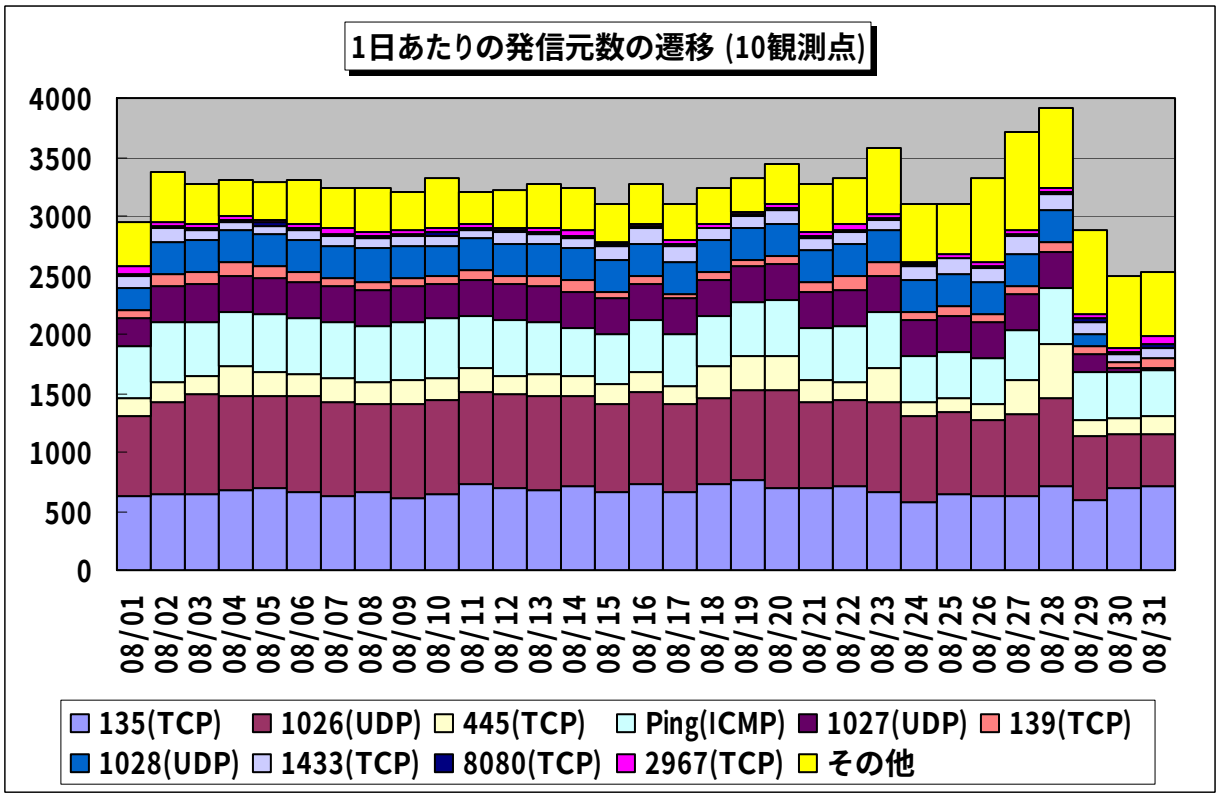
http://mustan.ipa.go.jp/mustan_web/

2.3 2007 年 8 月の一方的なアクセス状況

2007 年 8 月の一方的なアクセス状況（アクセス数）の遷移を図 2.3.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.3.2 に示します。



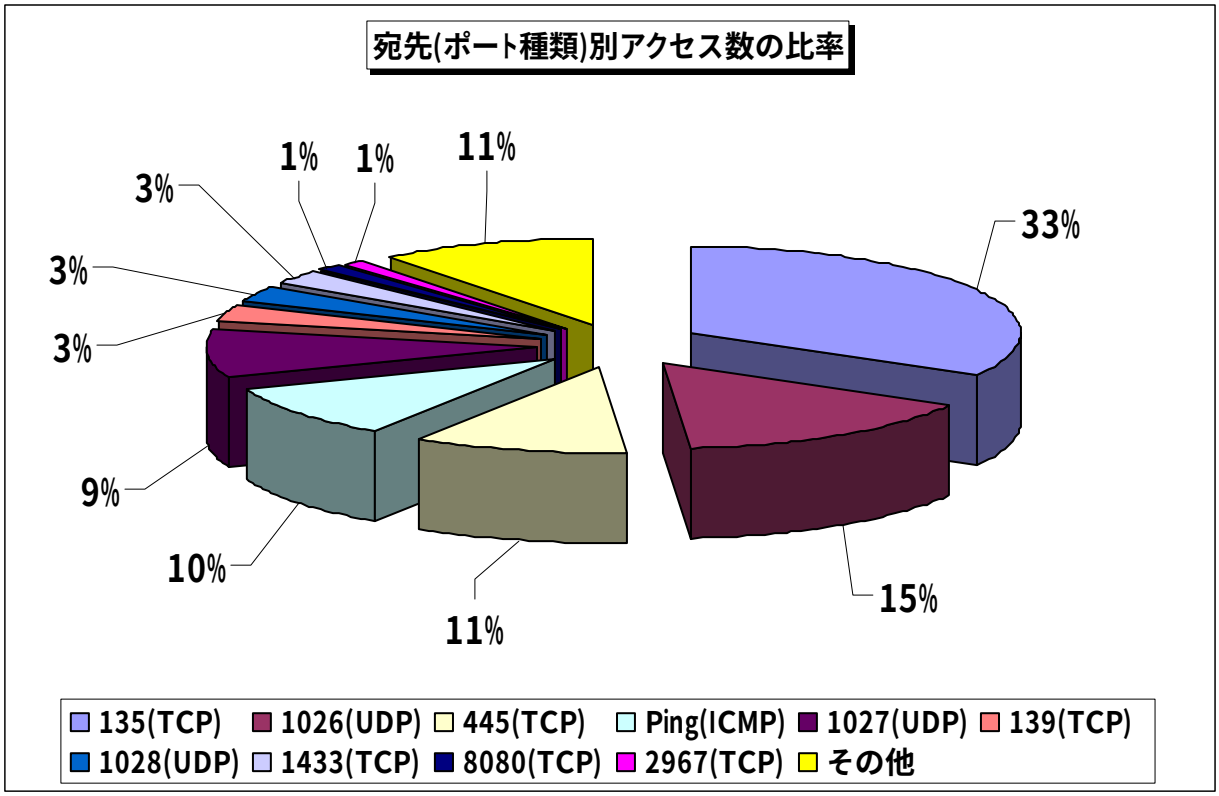
【図 2.3.1 2007 年 8 月の一方的なアクセス状況(アクセス数)】



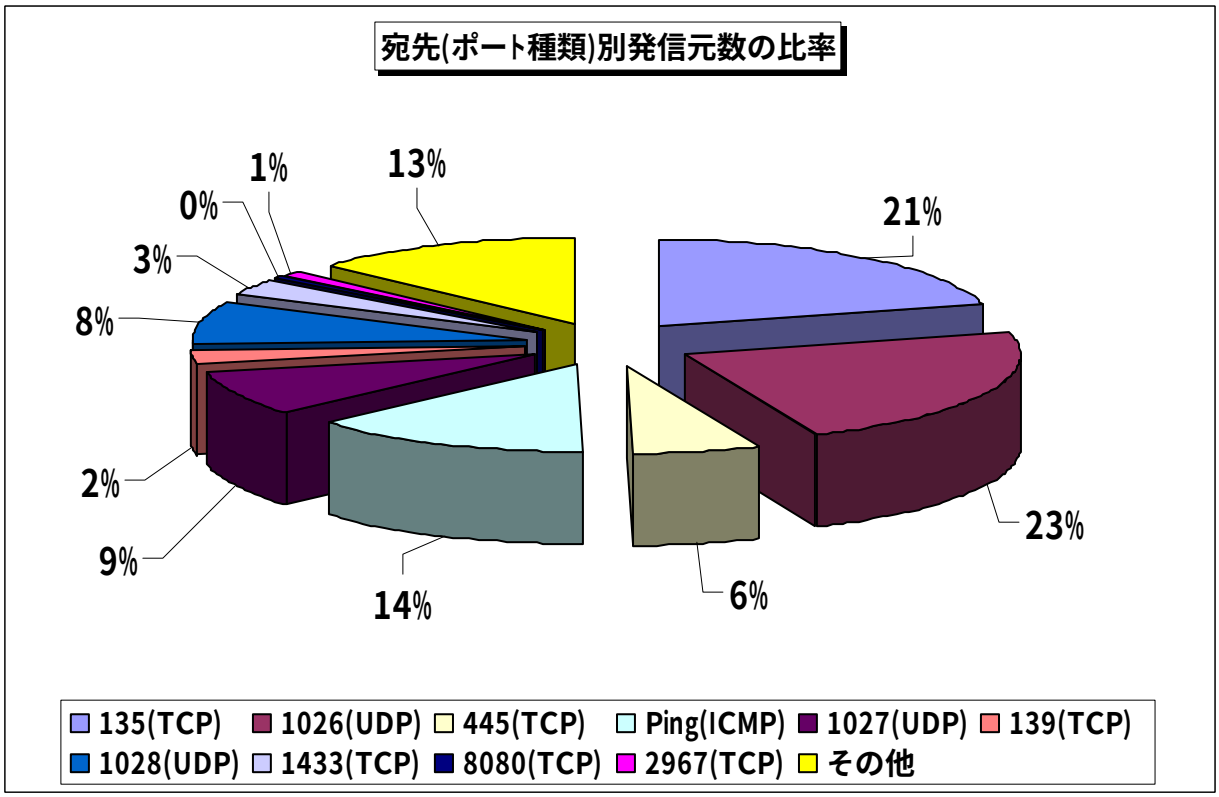
【図 2.3.2 2007 年 8 月の一方的なアクセス状況(発信元数)】

2.4 2007 年 8 月の宛先(ポート種類)別の比率

2007 年 8 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 2.4.1 に、宛先(ポート種類)別発信元数の比率を図 2.4.2 に示します。



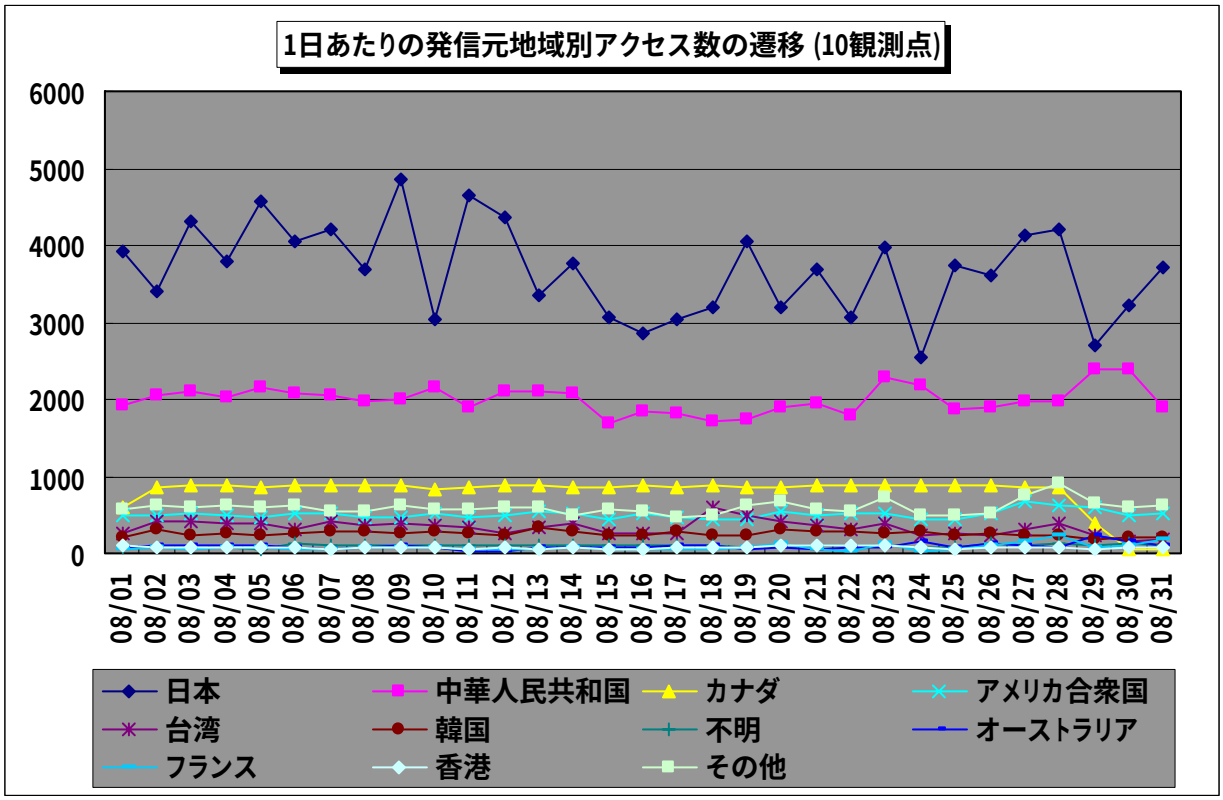
【図 2.4.1 2007 年 8 月の宛先(ポート種類)別アクセス数の比率】



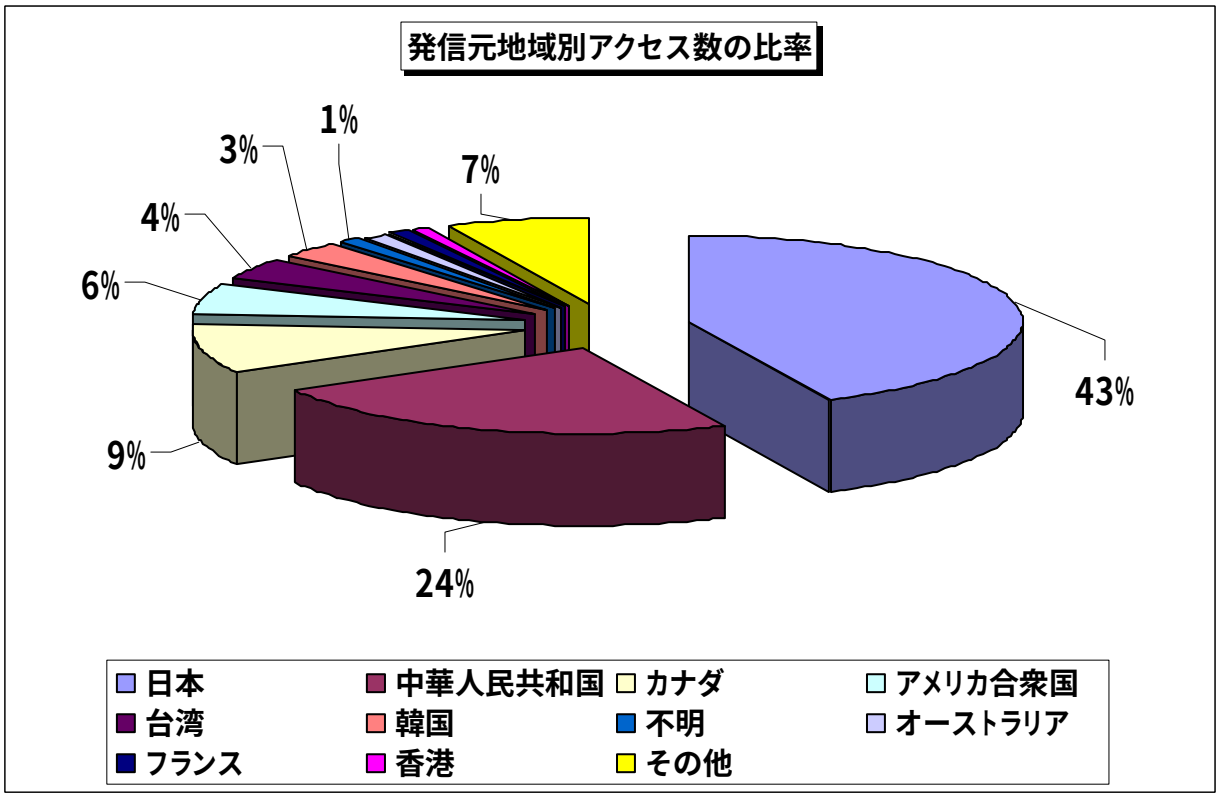
【図 2.4.2 2007 年 8 月の宛先(ポート種類)別発信元数の比率】

2.5 2007 年 8 月の発信元地域別アクセス状況

2007 年 8 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 2.5.1 に、発信元地域別アクセス数の比率を図 2.5.2 に示します。

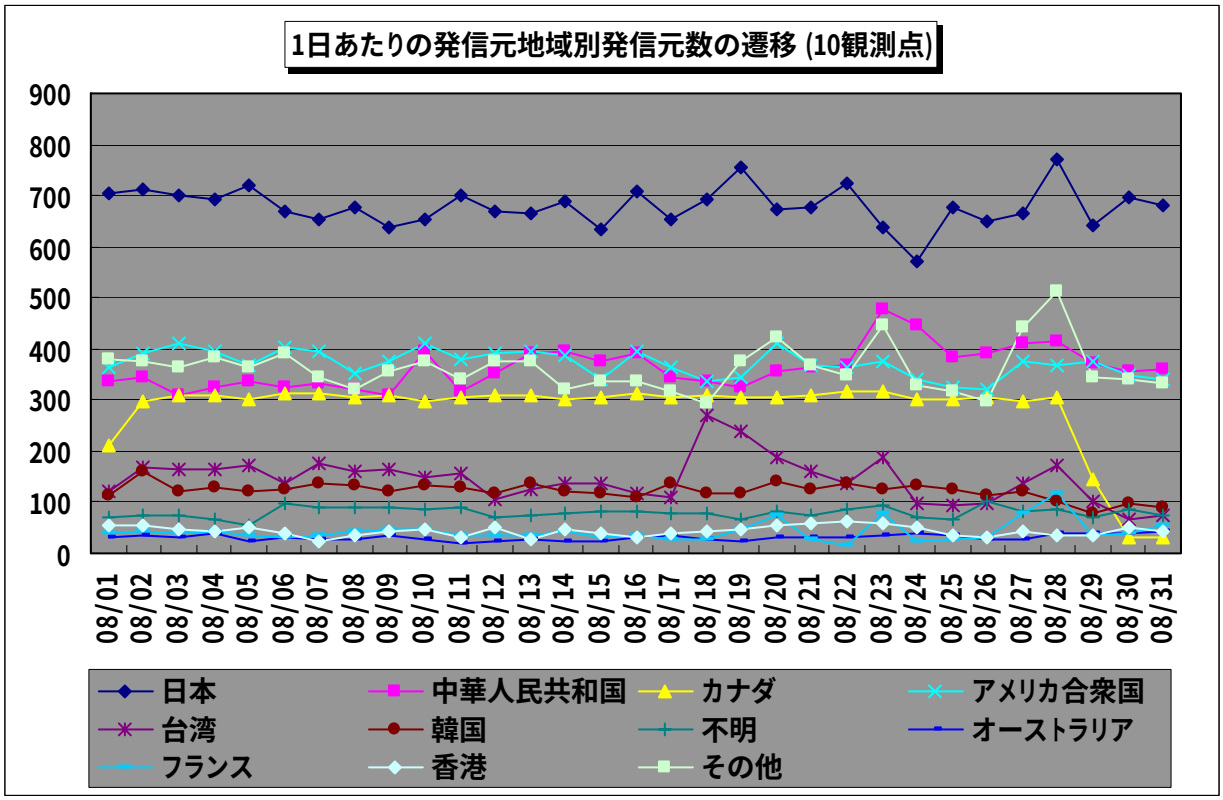


【図 2.5.1 2007 年 8 月の発信元地域別アクセス数の変化】

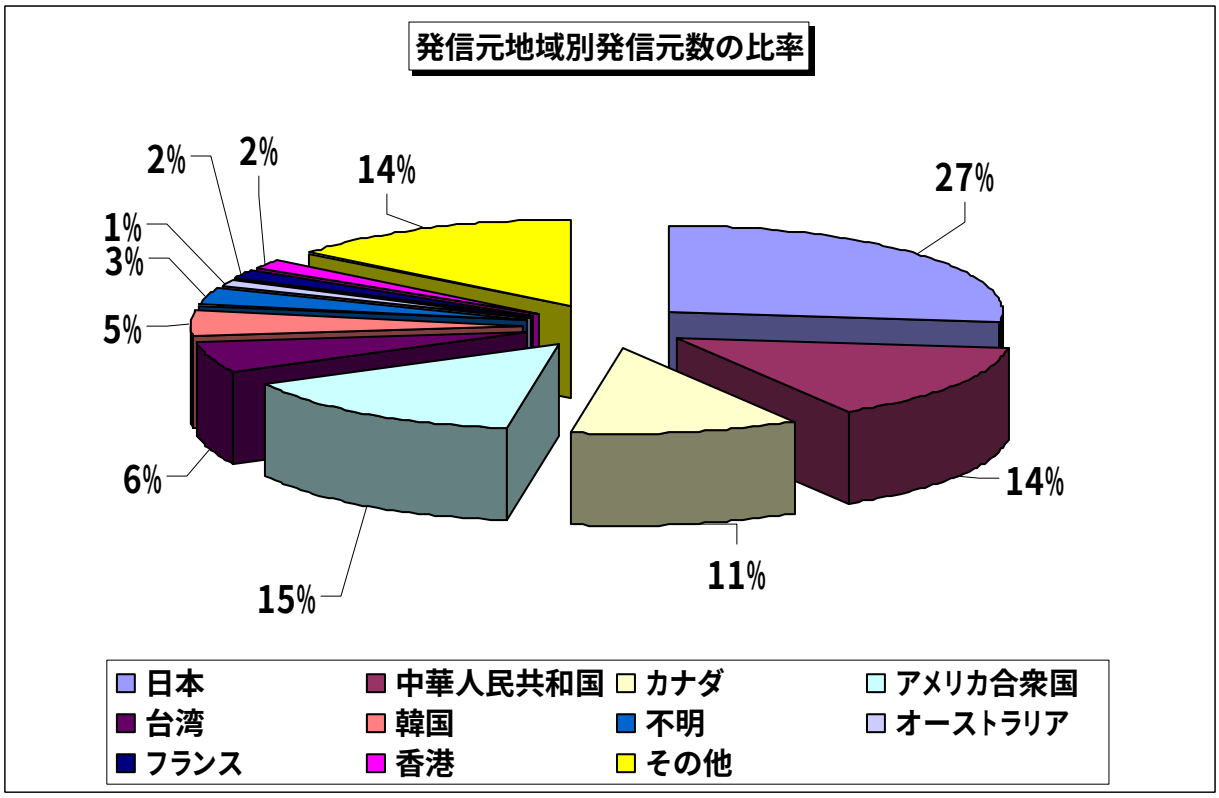


【図 2.5.2 2007 年 8 月の発信元地域別アクセス数の比率】

2007 年 8 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 2.5.3 に、発信元地域別発信元数の比率を図 2.5.4 に示します。



【図 2.5.3 2007 年 8 月の発信元地域別発信元数の変化】

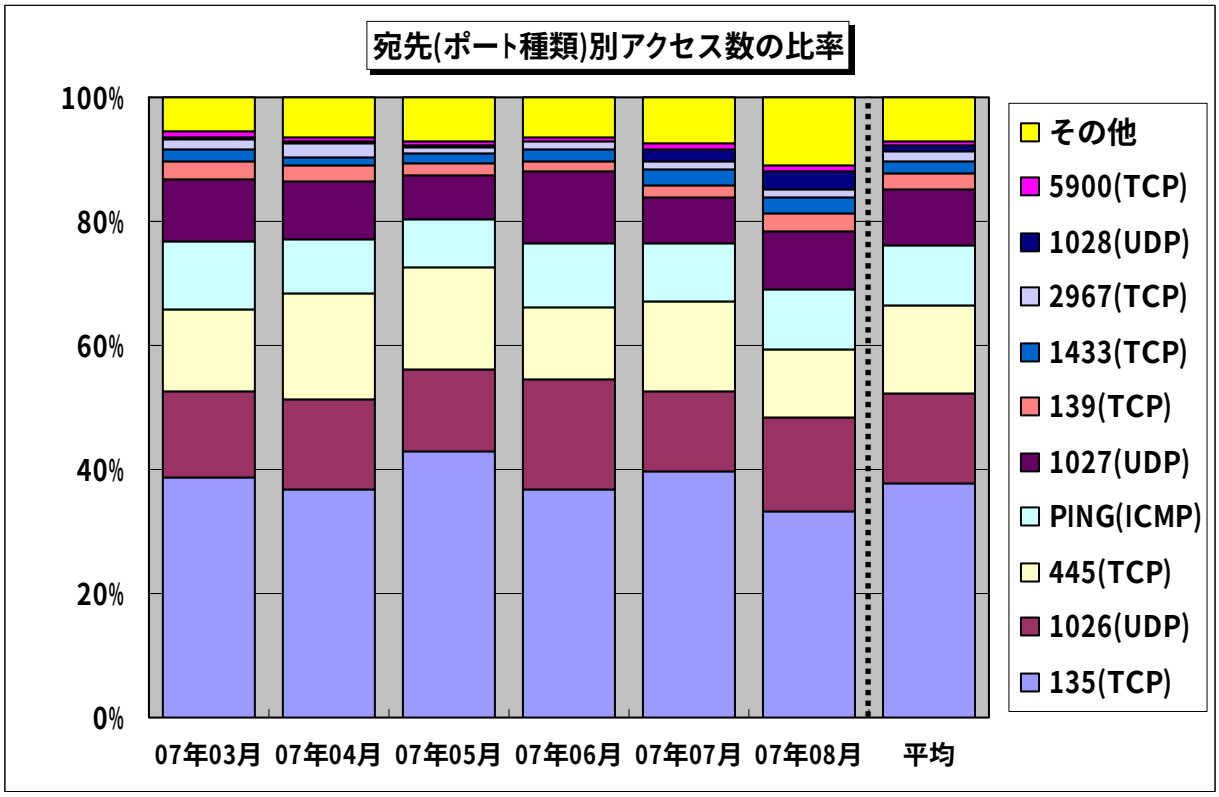


【図 2.5.4 2007 年 8 月の発信元地域別発信元数の比率】

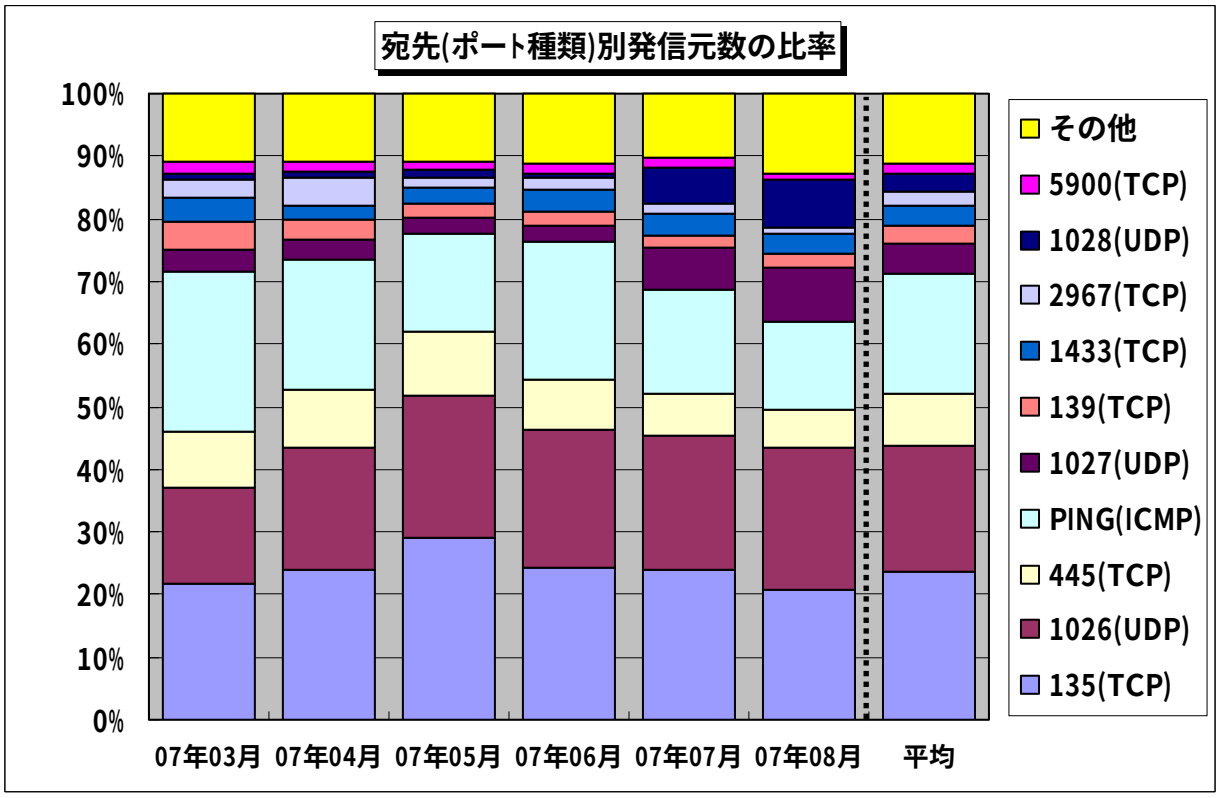
3．統計情報

3.1 2007 年 3 月～2007 年 8 月の宛先(ポート種類)別の比率

2007 年 3 月～2007 年 8 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。



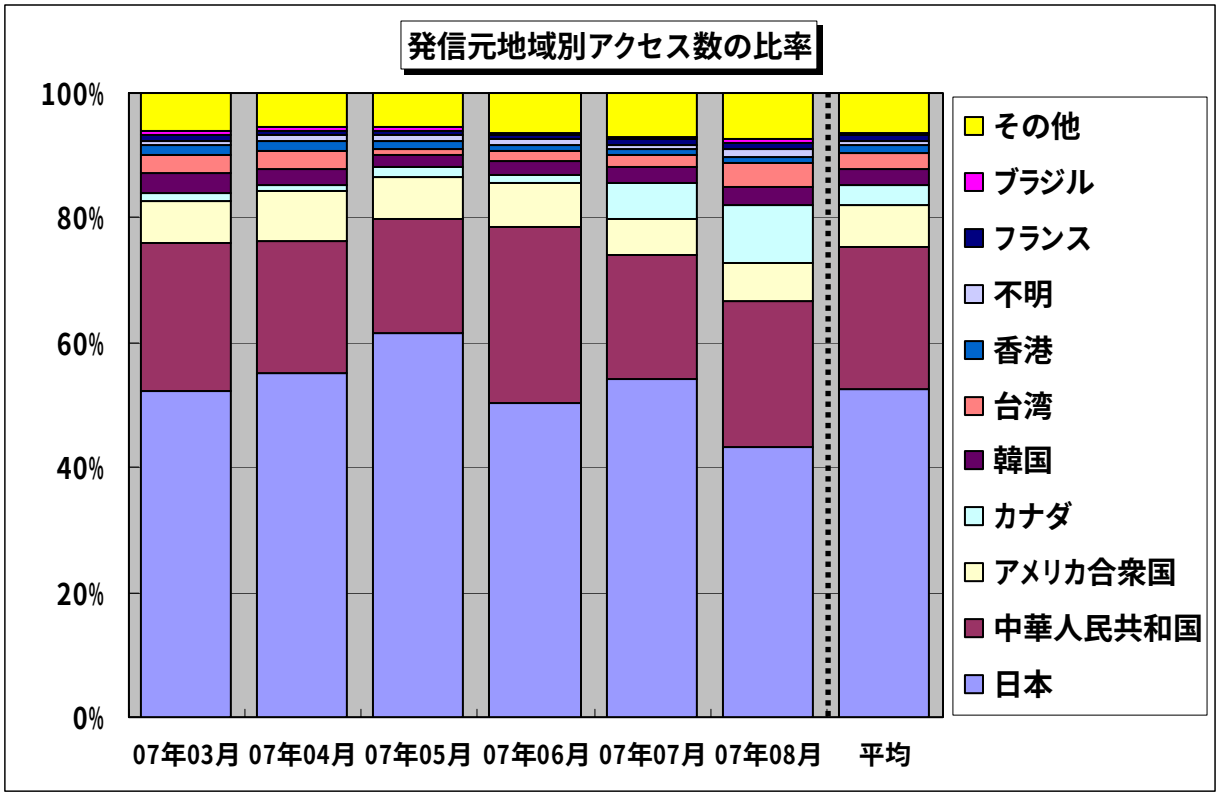
【図 3.1.1 2007 年 3 月～2007 年 8 月の宛先(ポート種類)別アクセス数の比率】



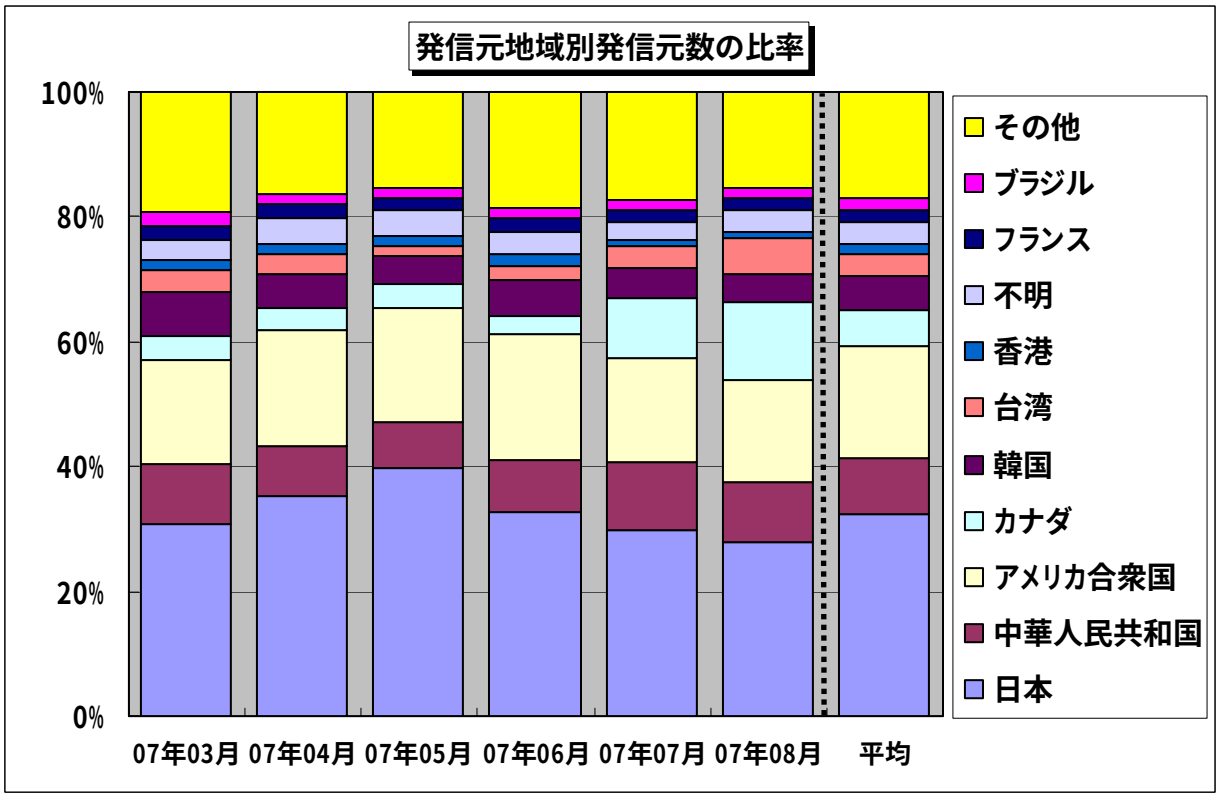
【図 3.1.2 2007 年 3 月～2007 年 8 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 3 月～2007 年 8 月の発信元地域別の比率

2007 年 3 月～2007 年 8 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 3 月～2007 年 8 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 3 月～2007 年 8 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 8 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)
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
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)
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
1028(UDP)	1026(UDP)/1027(UDP)と同じアクセス
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
8080(TCP)	80/tcp（ウェブサイトの閲覧に使用）の代替として使用される為、ウェブアプリケーションの脆弱性を狙ったアクセスと思われる。
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

■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