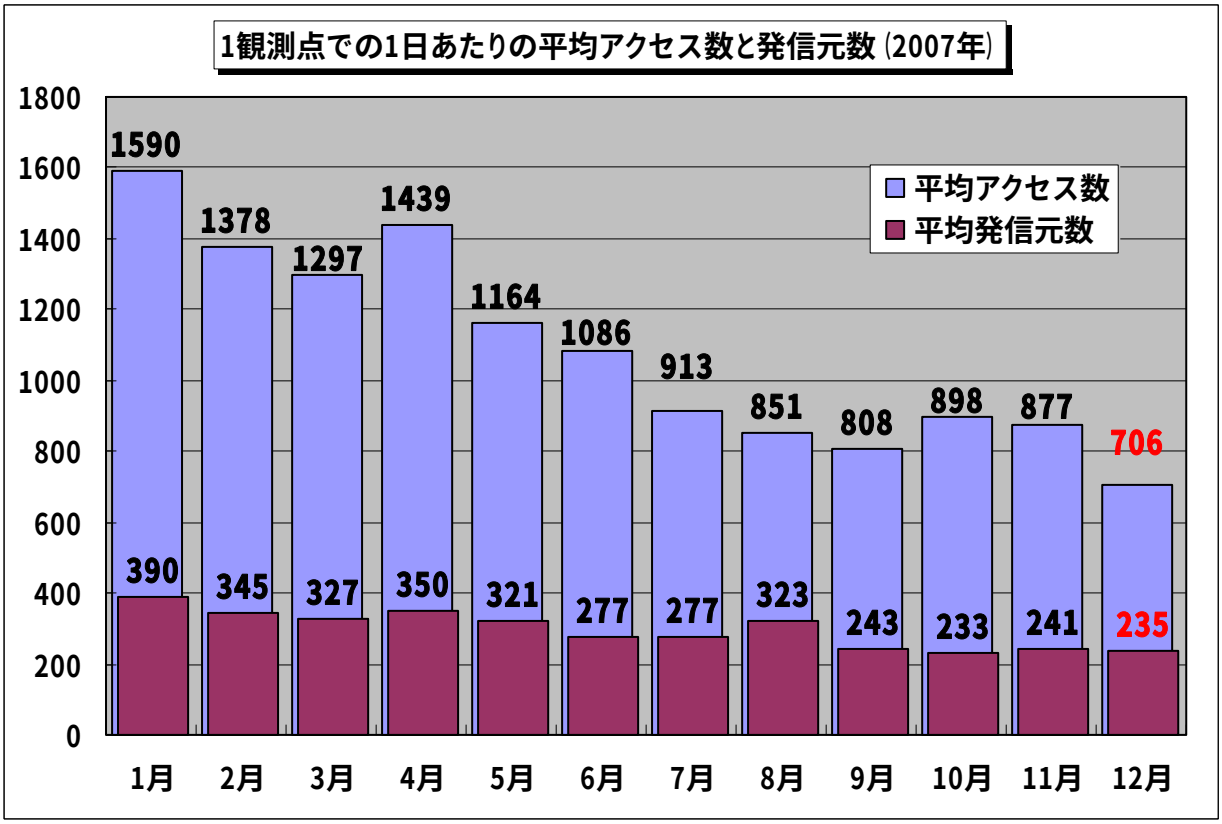
別紙 3

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 12 月の期待しない（一方的な）アクセスの総数は、10 観測点で **218,942 件**ありました。1 観測点で 1 日あたり **235** の発信元から **706 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、235 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。

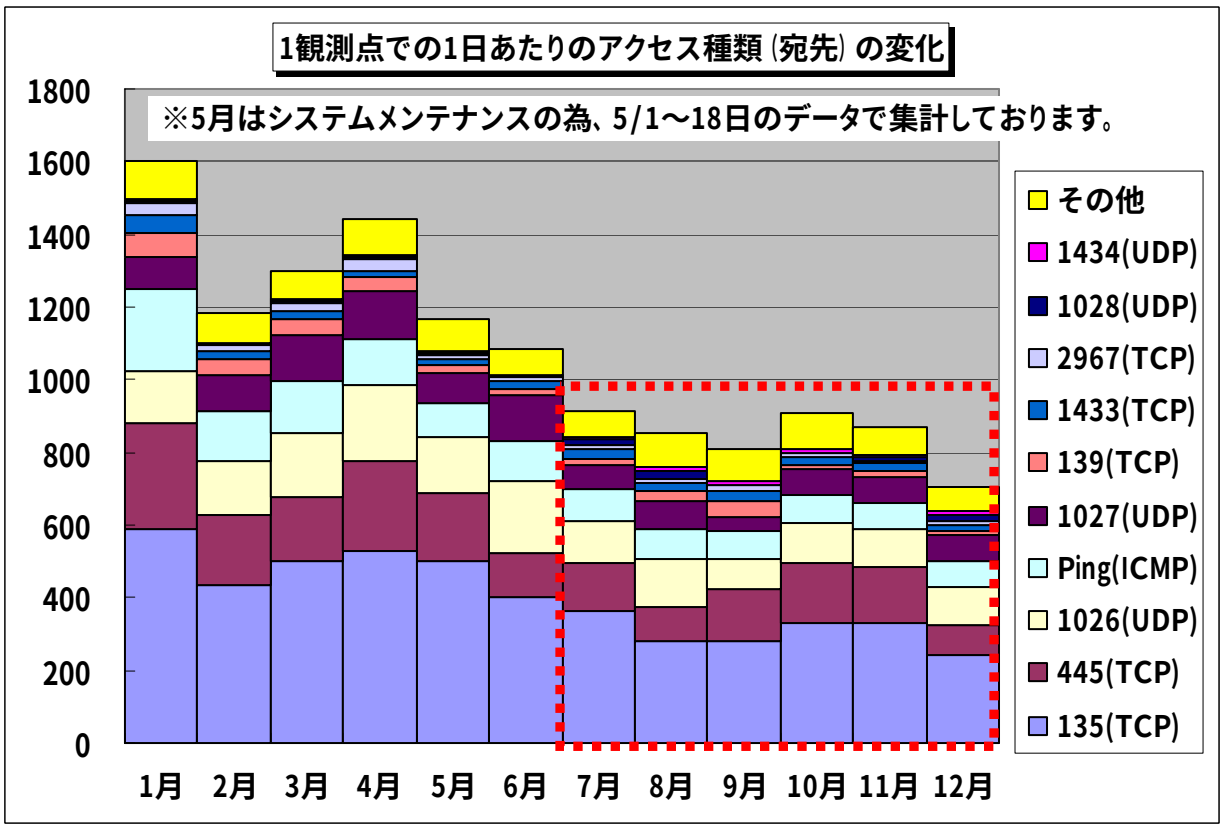


【図 1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2007 年 1 月～2007 年 12 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、12 月の期待しない(一方的な）アクセスは 11 月よりも減少し、2007 年における 1 日あたりのアクセス数として最低となりしまた。ただし、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。

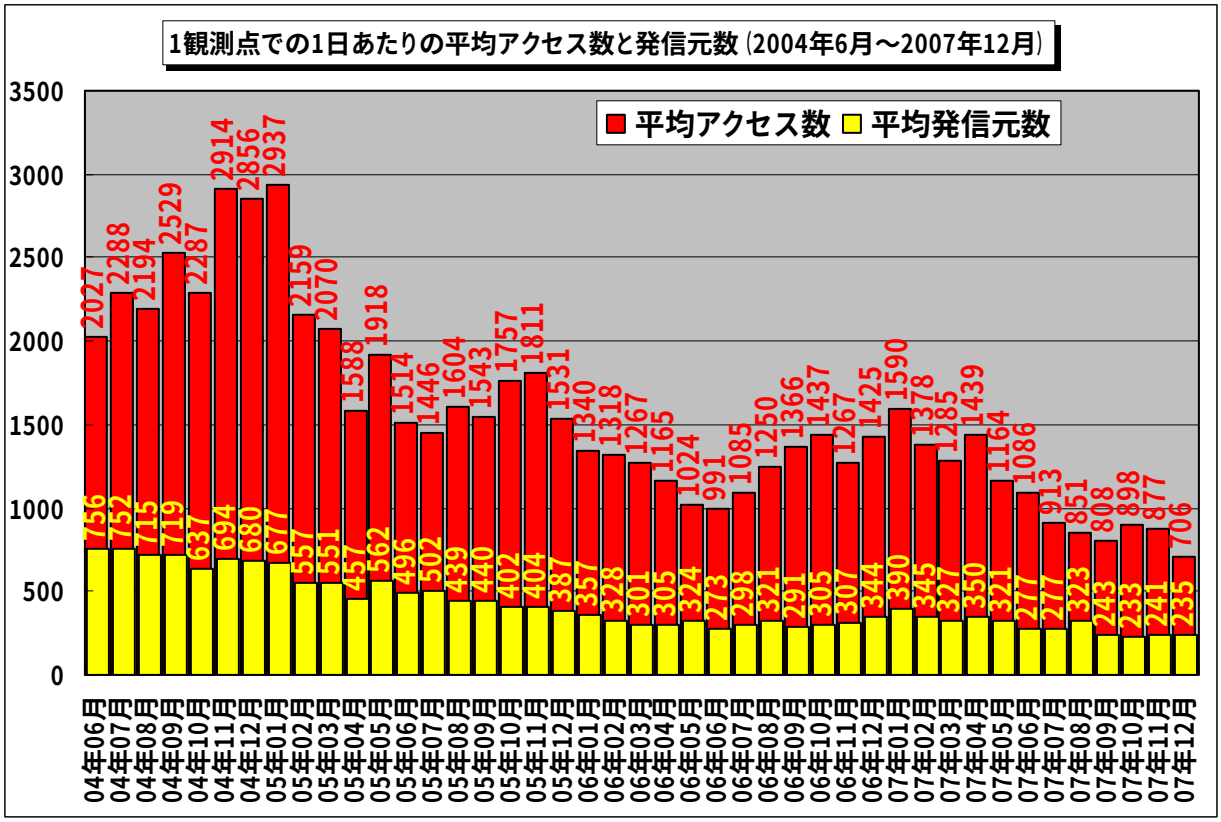
2．2007 年の期待しない（一歩的な）アクセスの状況

2007 年の、毎月の 1 日あたりの期待しない（一方的な）アクセス状況は、6 月を境にアクセスの種類に関わらず、全体的に少しずつ減少傾向でありました（図 2.1 参照）。



【図 2.1　1 観測点での 1 日あたりのアクセス種類（宛先）の変化】

また、定点観測を開始して以来、1 年を通した平均アクセス数でも過去最低となりました（図 2.2 参照）。



【図 2.2　2004 年 6 月～2007 年 12 月の 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】

なぜアクセス数が少なくなったのかは定かではありませんが、要因を挙げるとすれば、

(1) Windows の脆弱性を狙ったワームやウイルスによる、大量の感染被害が少なくなった
(2) 総務省･経済産業省連携プロジェクトである、サイバークリーンセンターが行なっているボット対策によるボットの駆除による効果
(3) 個人や企業の使用するコンピュータが、新しいマシンや新しい OS に入れ替わる事により、セキュリティ対策が向上する

などが考えられます。

(1)は、IPA に届けられる、コンピュータウイルス届出状況のウイルス届出数やウイルス検出数の減少からもうかがえますが、主に、各プロバイダで行なっている、迷惑メールやウイルスメールの対応も、感染被害の防止になっていると言えます。

(参考情報)
■ 2007 年コンピュータウイルスの届出状況について
http://www.ipa.go.jp/security/txt/2008/documents/2007all-vir.pdf

(2) は、ボットウイルスからのアクセスと思われるものに対して、効果を上げていると思われます。
サイバークリーンセンターでは、ボット駆除ツールの配布や、インターネットサービスプロバイダ(ISP)の協力の下、ボットに感染していると思われる顧客に対して、注意喚起メールの送信を行なったりしています。

(参考情報)
■ 総務省･経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/
■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html
■ 注意喚起活動について
https://www.ccc.go.jp/activity/index.html
■ ボット対策のしおり(PDF ファイル)
http://www.ipa.go.jp/security/antivirus/documents/3_bot_v5.pdf

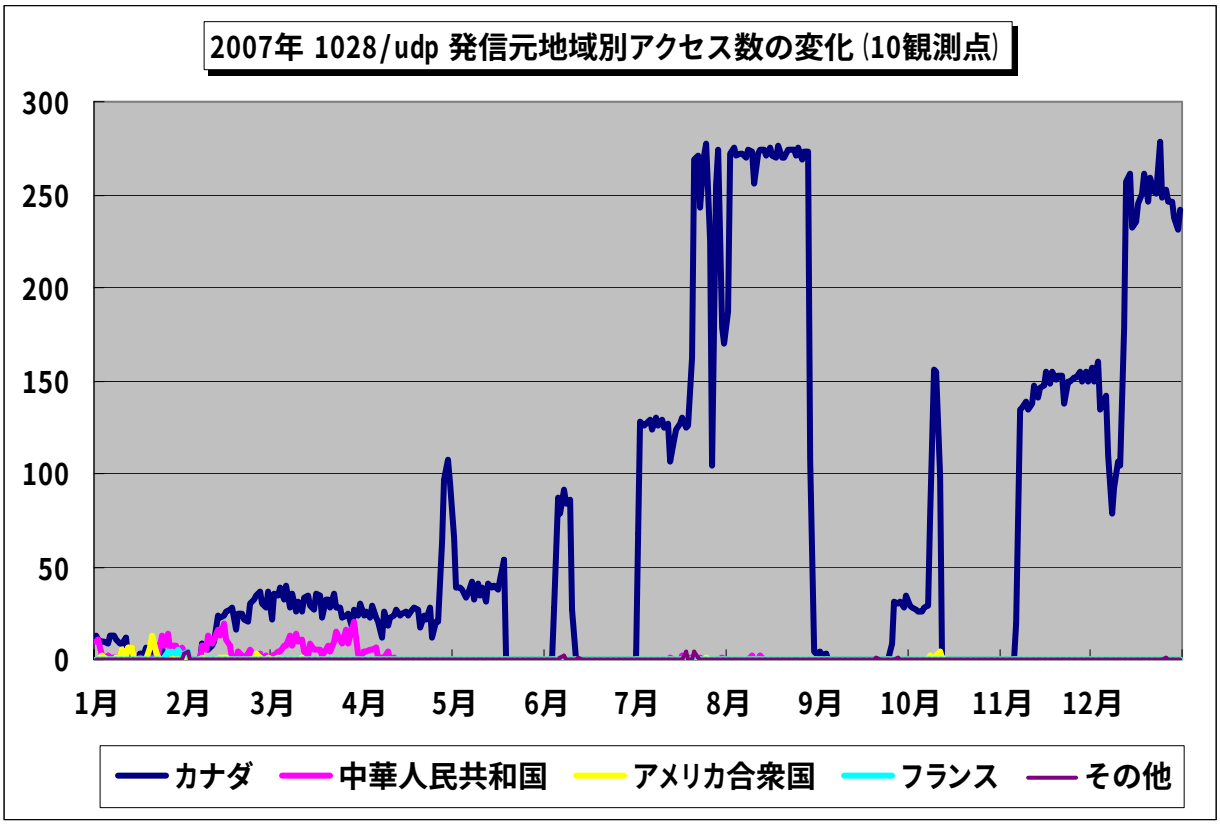
(3) については、あくまでも推測ですが、2007 年 1 月に Microsoft Windows の新しい OS (Windows Vista) が発売されました。これに伴い、個人や企業が新しい OS のコンピュータに替える事により、古いコンピュータにボットウイルスなどが感染していた場合には、知らない間にボットウイルスなども一緒に破棄されてしまう形になります。

また、新しい OS のコンピュータには、最初からインストールされているウイルス対策ソフトが、期間限定であるとしても、最新の状態で機能する事も見逃せないのではないでしょうか。

2.1. 2007 年に観測された主な期待しない（一方的な）アクセスの種類

2007 年に観測された、期待しない(一方的な)アクセスの種類を見てみると、特別目立ったものはありませんでした。ただその中において、12 月でも紹介した 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 1028/udp に対するアクセスが、2007 年の後半以

降に多く見受けられました（図 2.1.1 参照）。



【図 2.1.1　2007 年　1028/udp 発信元地域別アクセス数の変化（10 観測点）】

(参考情報)

■　2007 年 12 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/2007/documents/TALOT2-0712.pdf

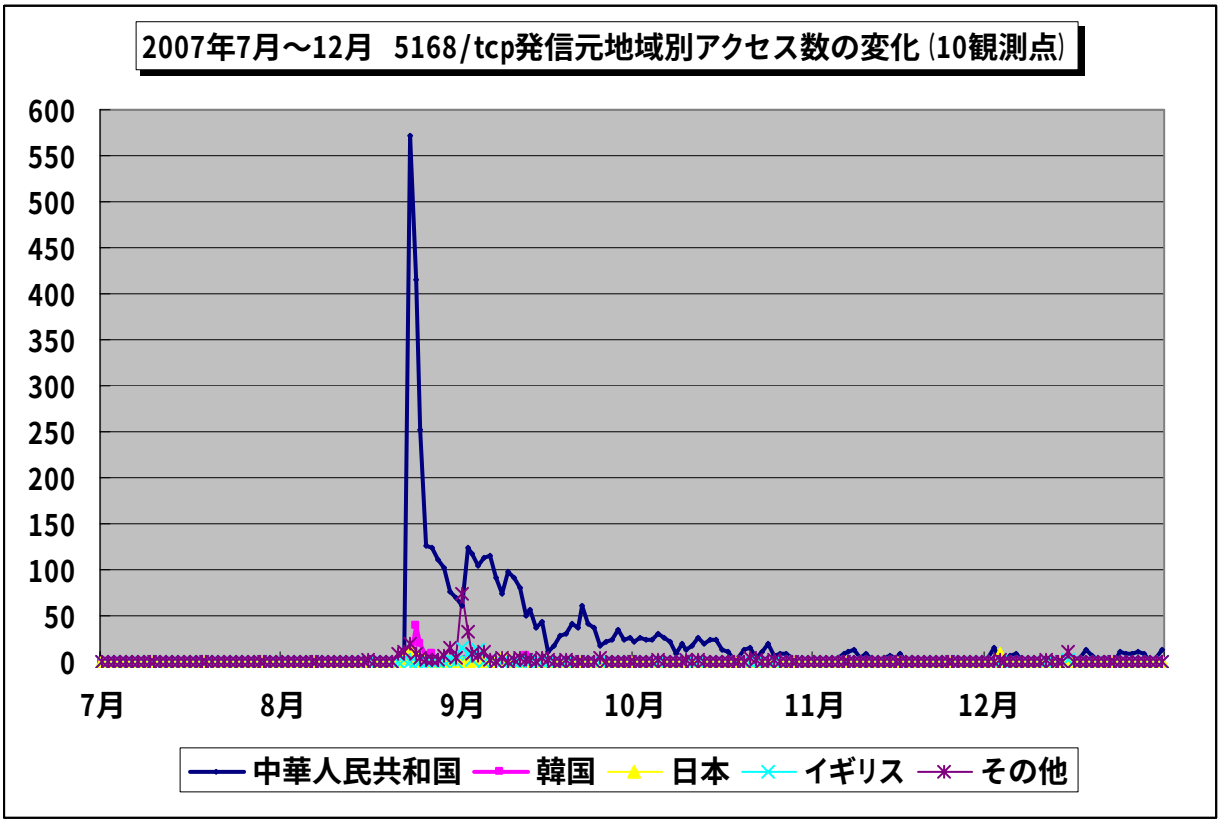
目新しいものでは、トレンドマイクロ社の、サーバ版ウイルス対策ソフトのぜい弱性を狙ったと思われる、5168/tcp へのアクセスが 8 月に一時的に多くありました（図 2.1.2 参照）。

このアクセスは、12 月現在ではもうほとんどありません。ただこの様に、ソフトウェアのぜい弱性を狙っているアクセスは継続的にありますので、お使いのソフトウェア製品のぜい弱性情報には、常に注意してください。

（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

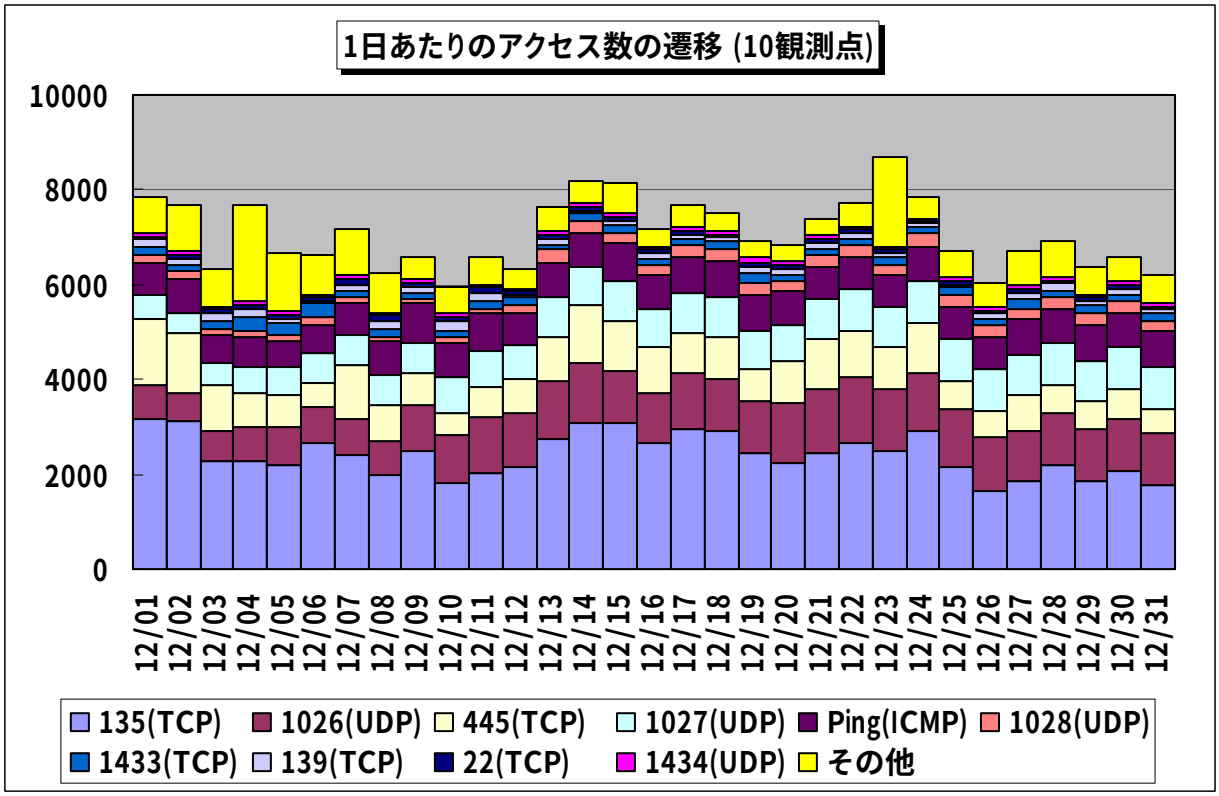
■　TCP 5168 番ポートへのスキャン増加に関する注意喚起　（JPCERT/CC）
http://www.jpcert.or.jp/at/2007/at070019.txt



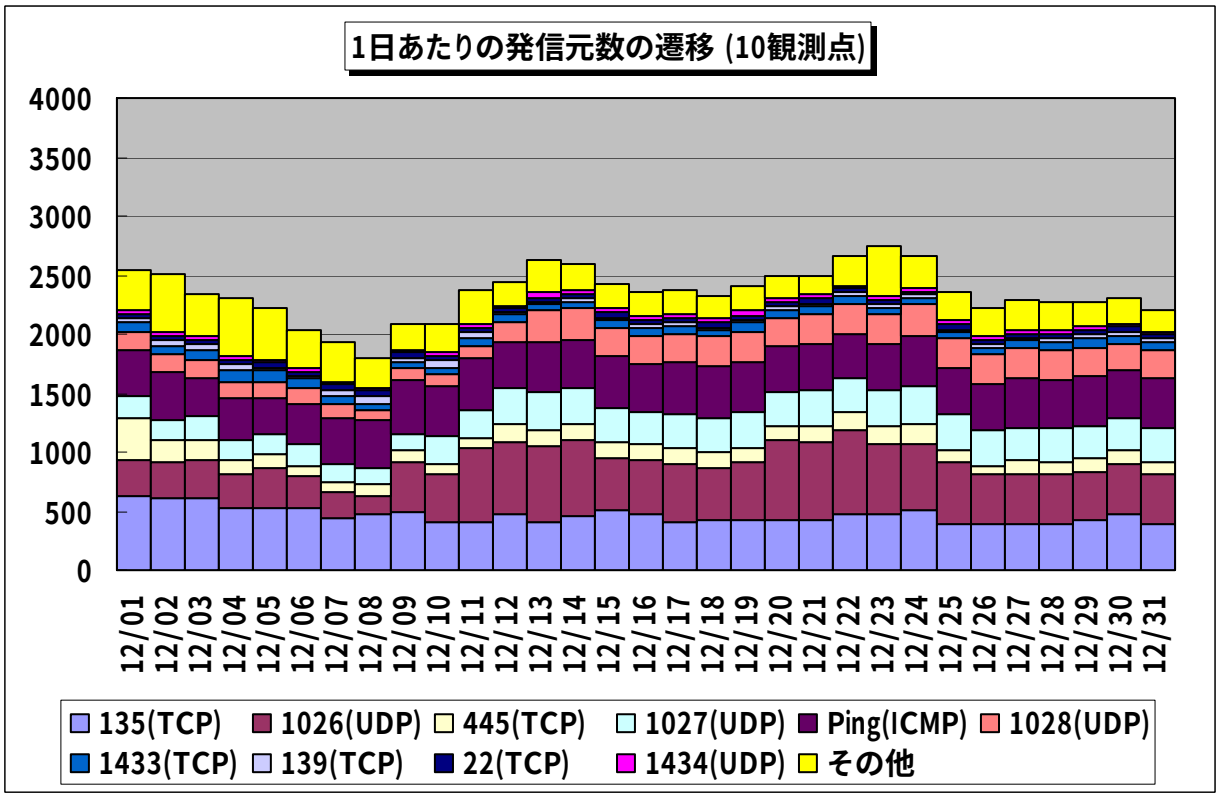
【図 2.1.2　2007 年 7 月～12 月　5168/tcp 発信元地域別アクセス数の変化（10 観測点）】

2.2 2007 年 12 月の一方的なアクセス状況

2007 年 12 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。



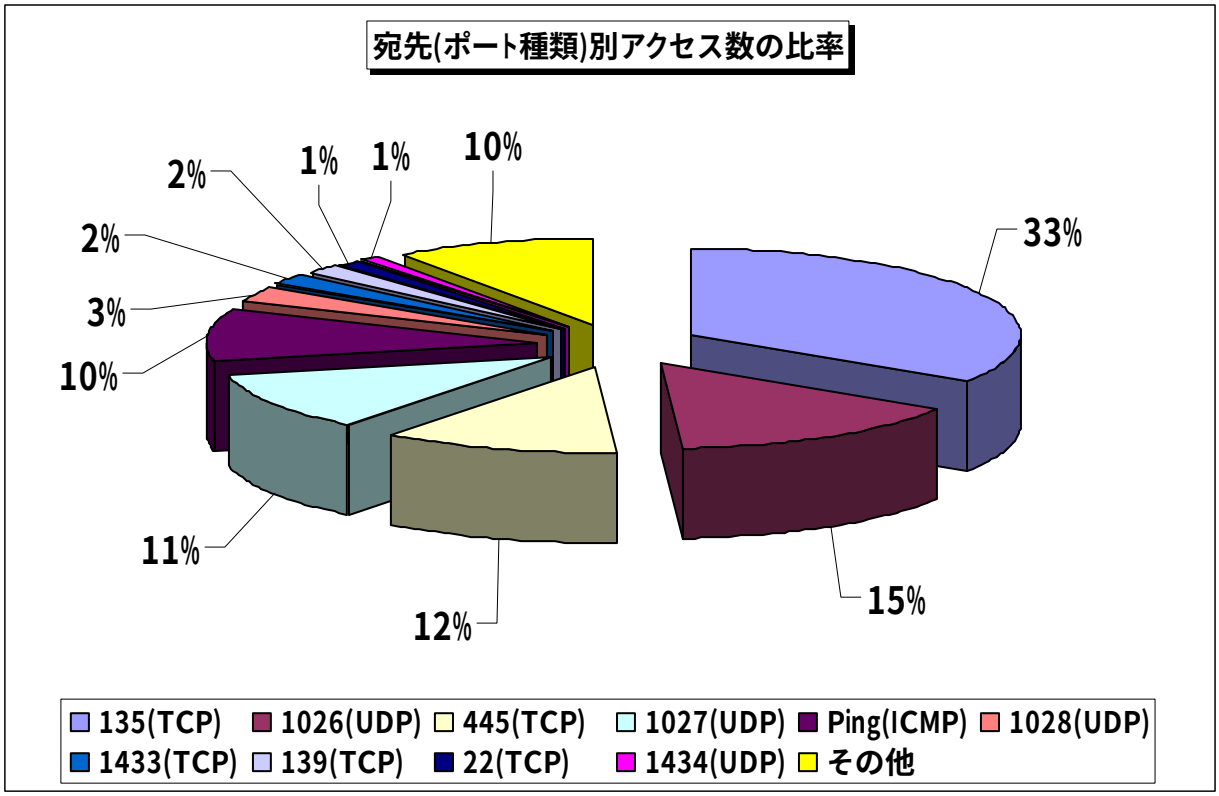
【図 2.2.1 2007 年 12 月の一方的なアクセス状況(アクセス数)】



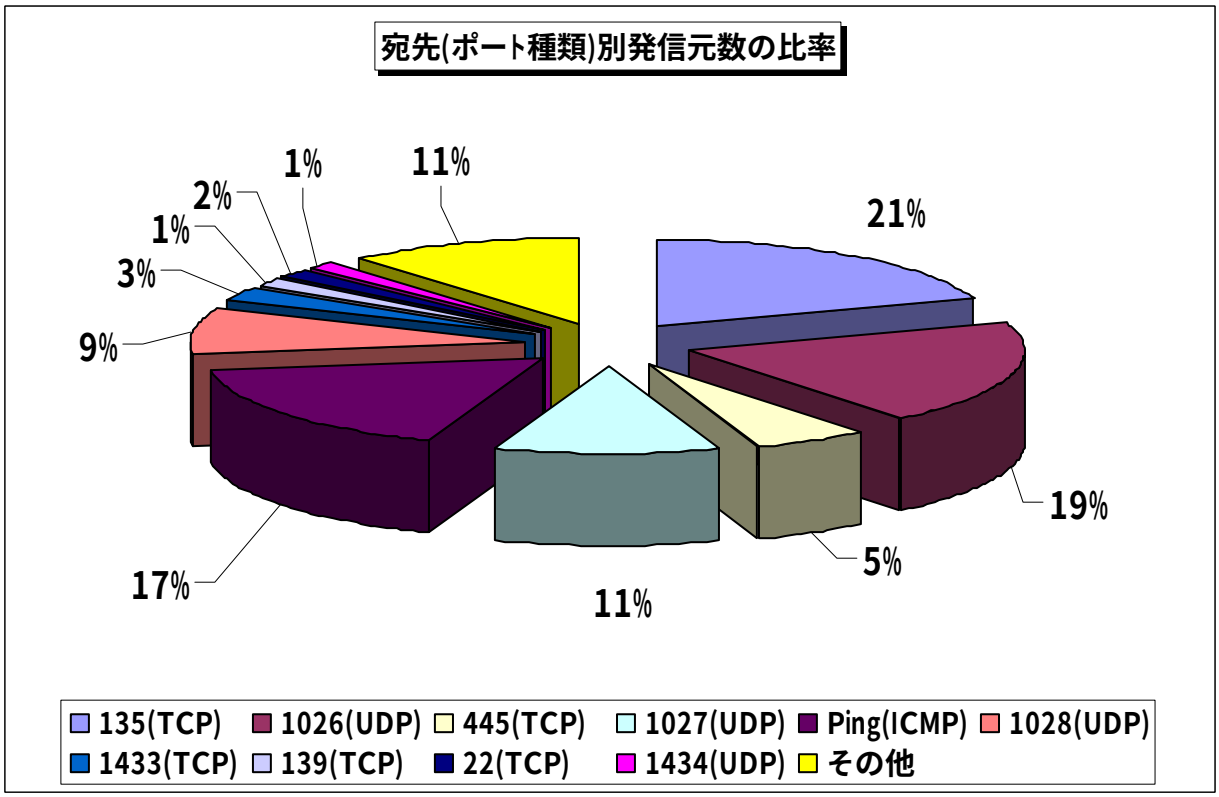
【図 2.2.2 2007 年 12 月の一方的なアクセス状況(発信元数)】

2.3 2007 年 12 月の宛先(ポート種類)別の比率

2007 年 12 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。



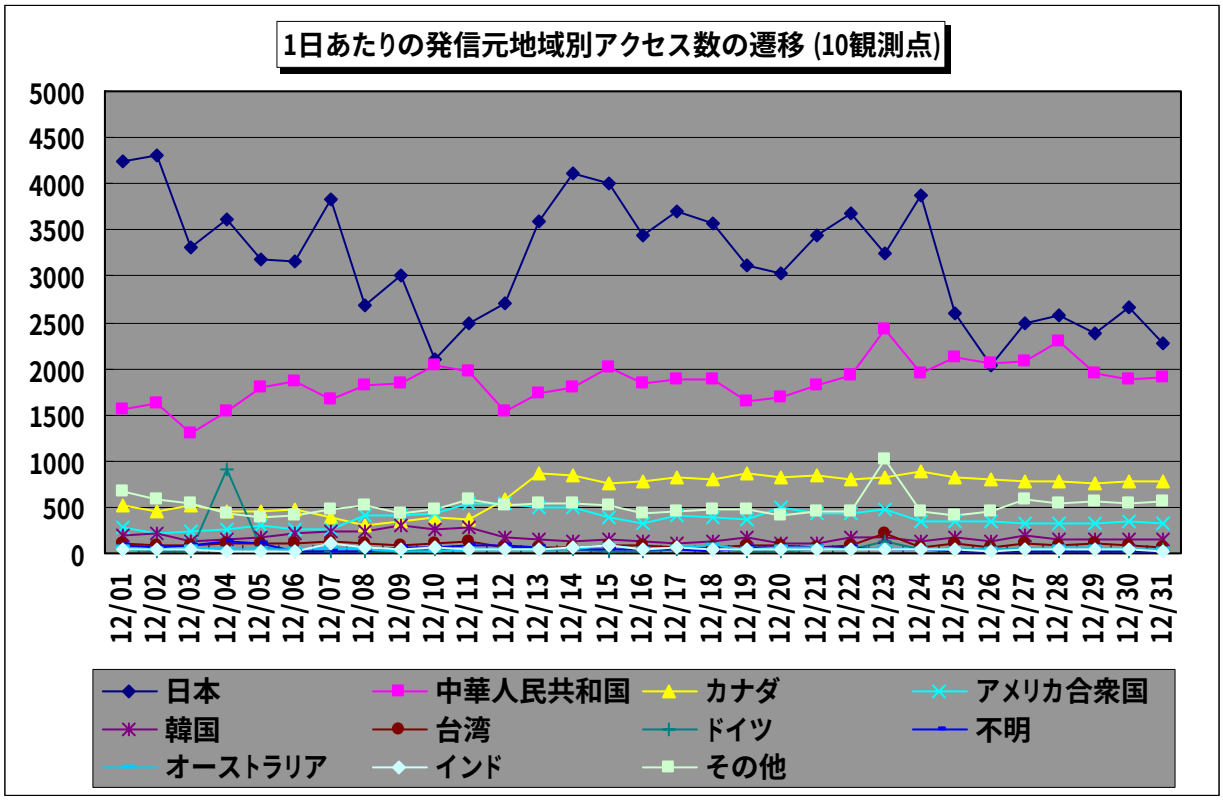
【図 2.3.1 2007 年 12 月の宛先(ポート種類)別アクセス数の比率】



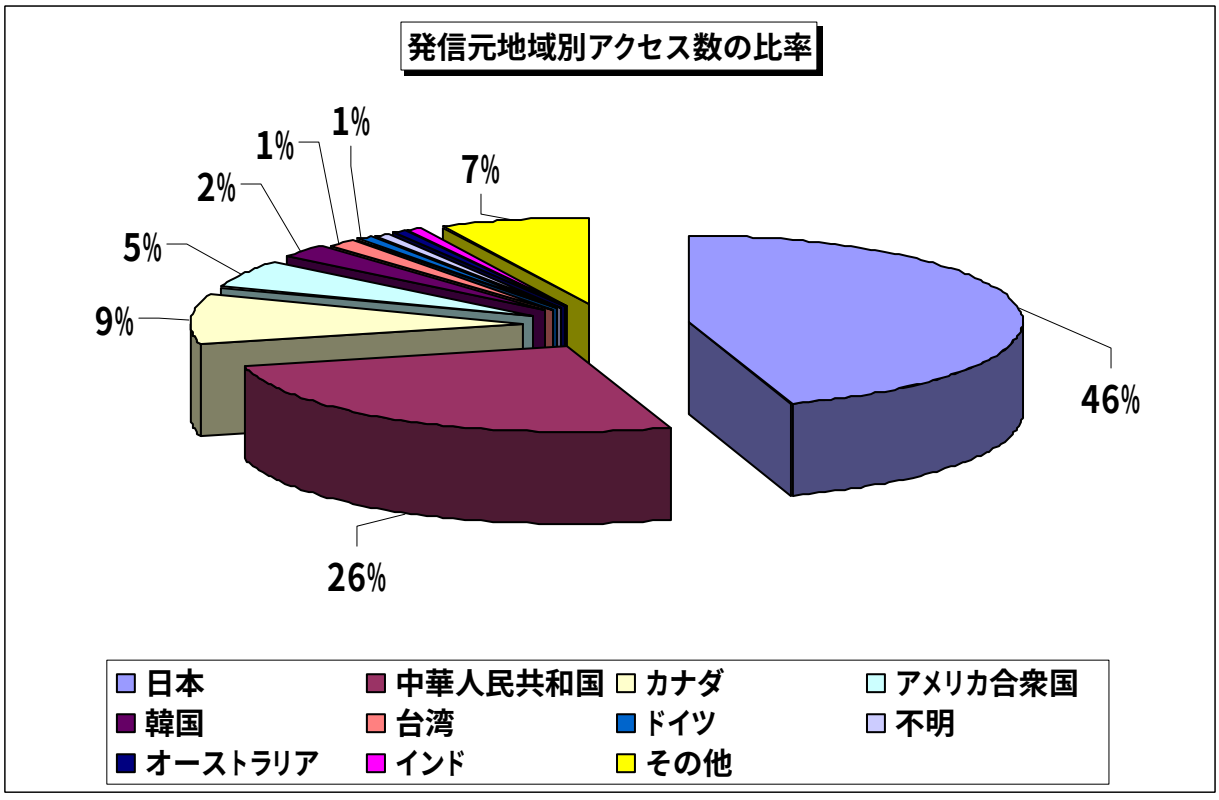
【図 2.3.2 2007 年 12 月の宛先(ポート種類)別発信元数の比率】

2.4 2007 年 12 月の発信元地域別アクセス状況

2007 年 12 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。

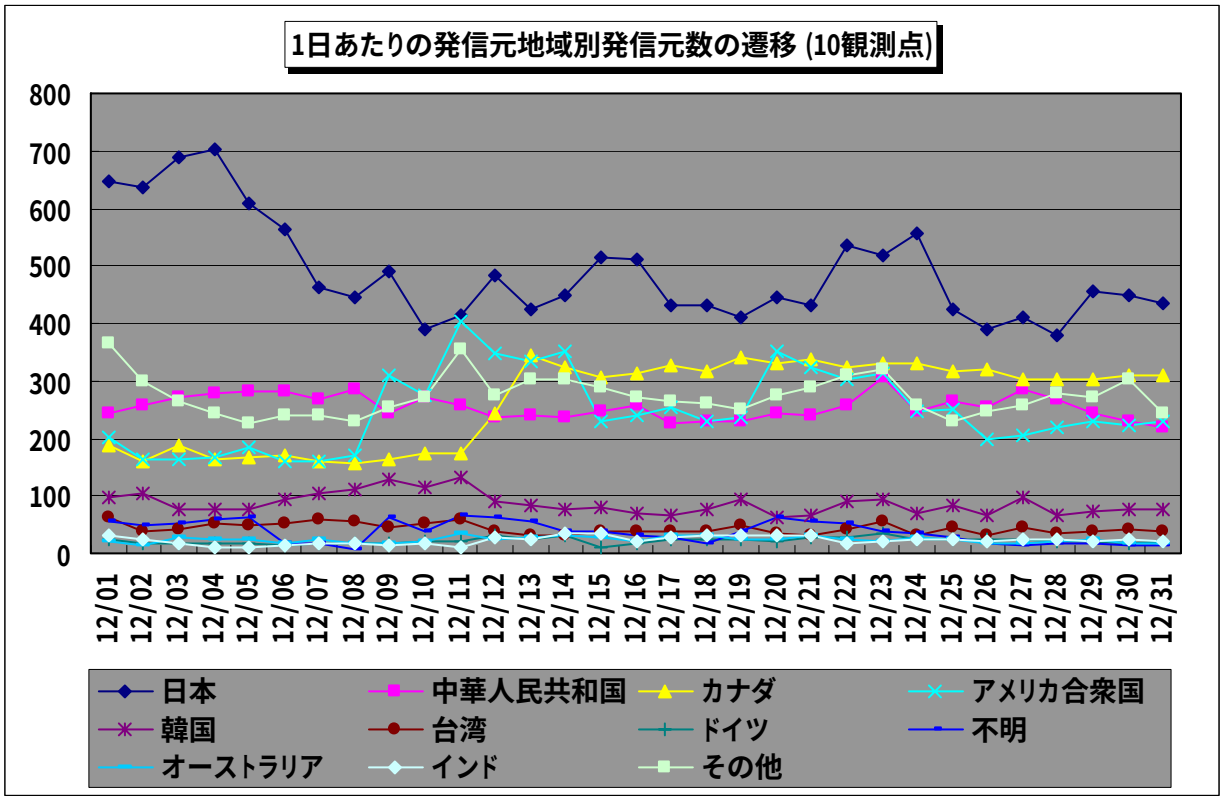


【図 2.4.1 2007 年 12 月の発信元地域別アクセス数の変化】

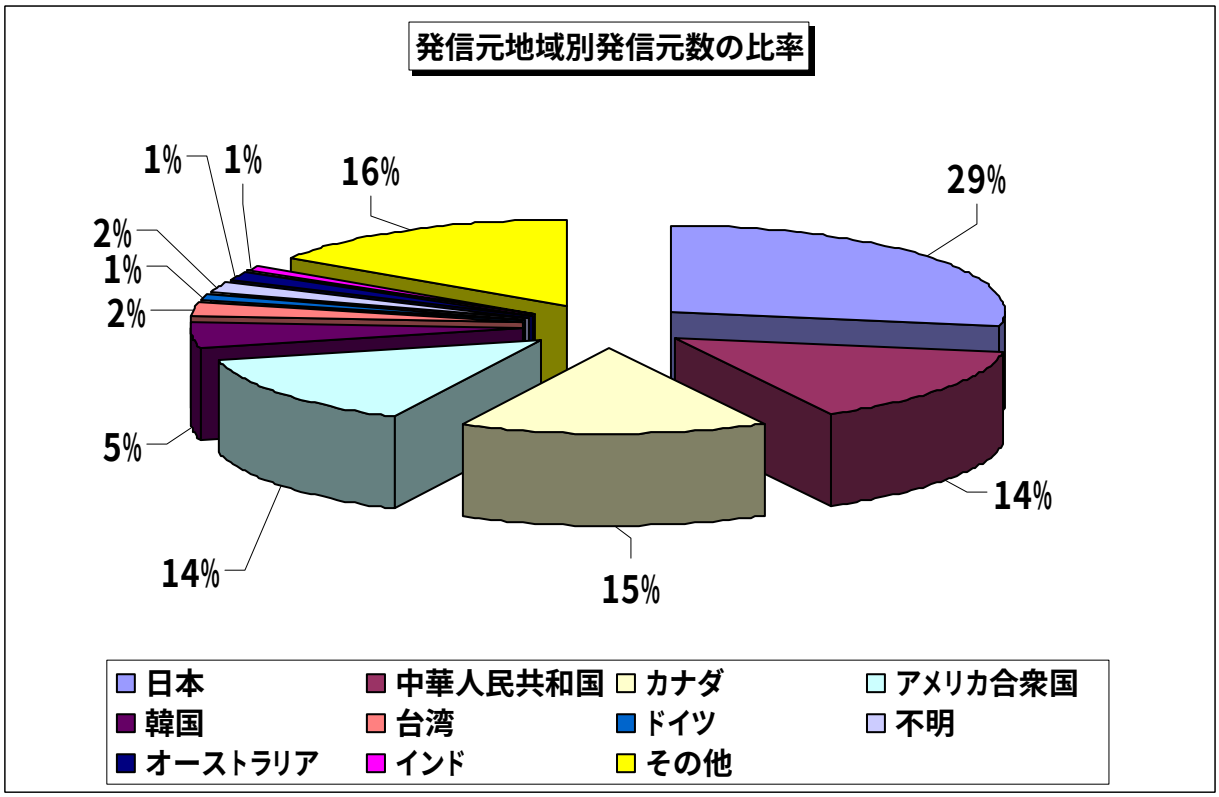


【図 2.4.2 2007 年 12 月の発信元地域別アクセス数の比率】

2007 年 12 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 12 月の発信元地域別発信元数の変化】

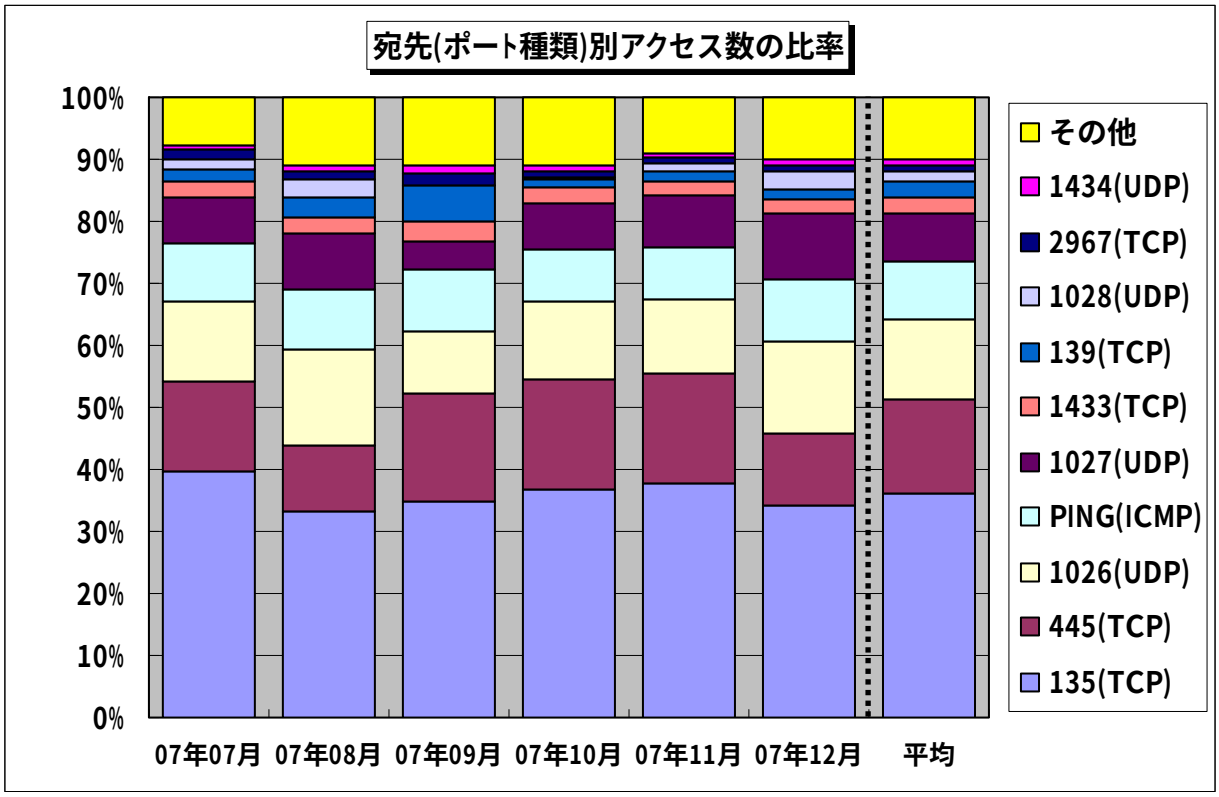


【図 2.4.4 2007 年 12 月の発信元地域別発信元数の比率】

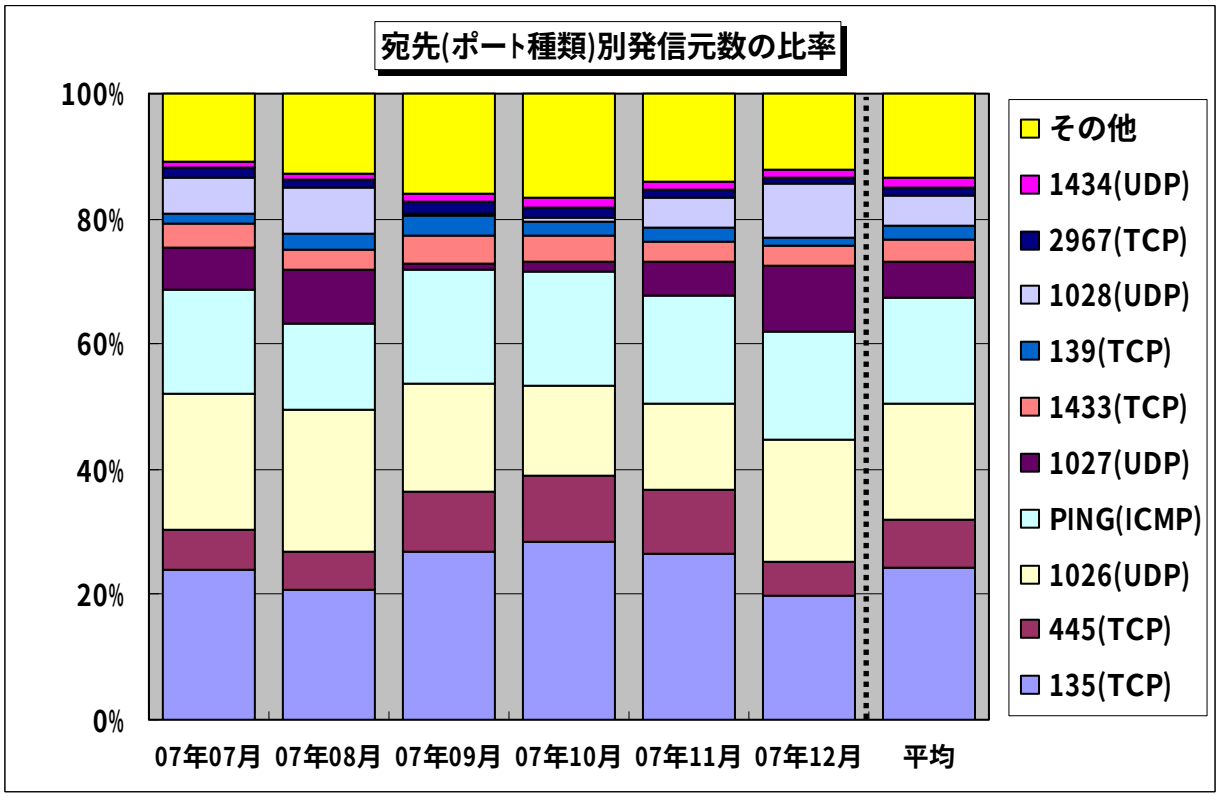
3．統計情報

3.1 2007 年 7 月～2007 年 12 月の宛先(ポート種類)別の比率

2007 年 7 月～2007 年 12 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。



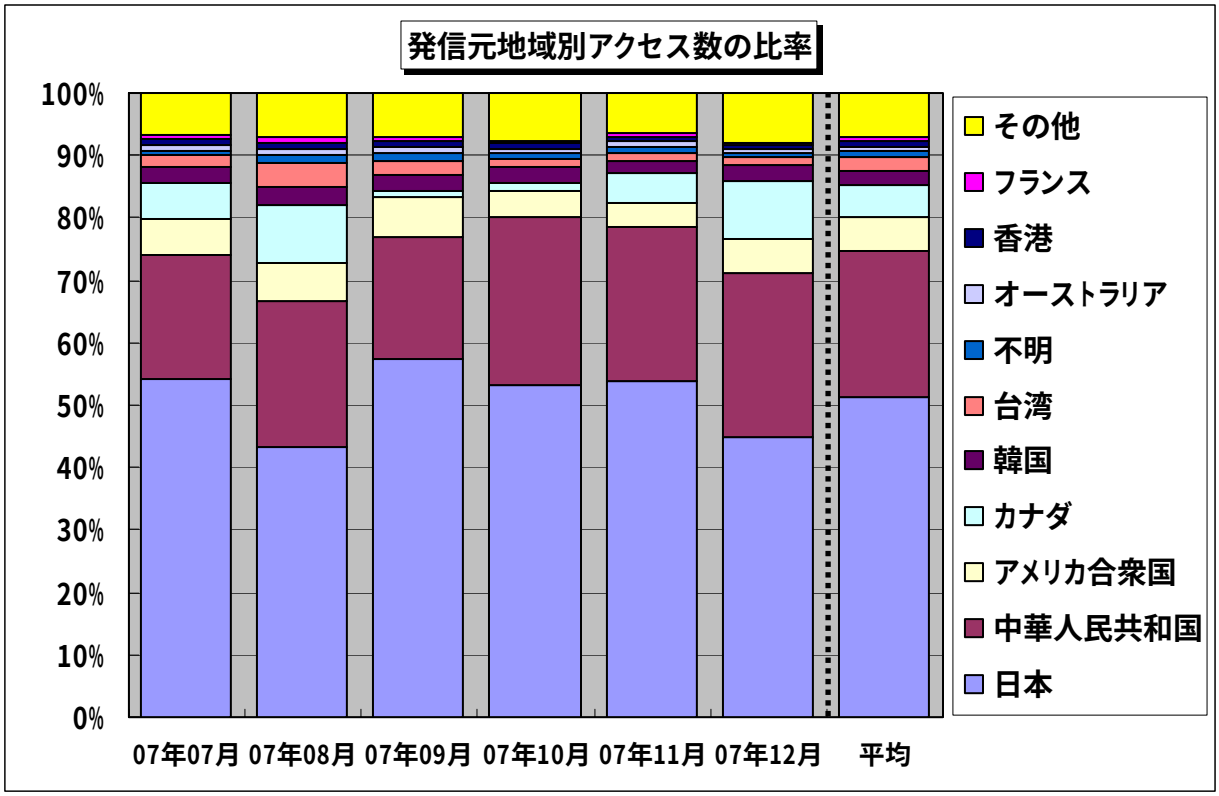
【図 3.1.1 2007 年 7 月～2007 年 12 月の宛先(ポート種類)別アクセス数の比率】



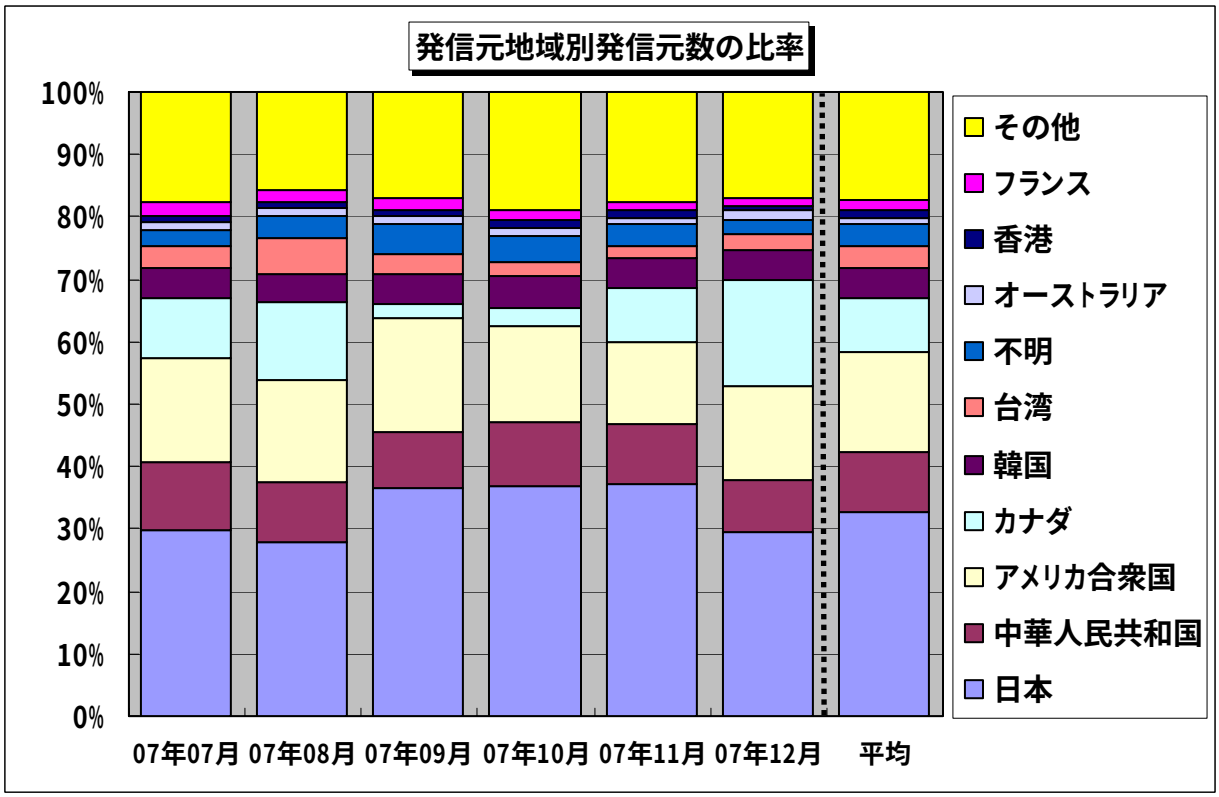
【図 3.1.2 2007 年 7 月～2007 年 12 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 7 月～2007 年 12 月の発信元地域別の比率

2007 年 7 月～2007 年 12 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 7 月～2007 年 12 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 7 月～2007 年 12 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 12 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)/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
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
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
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