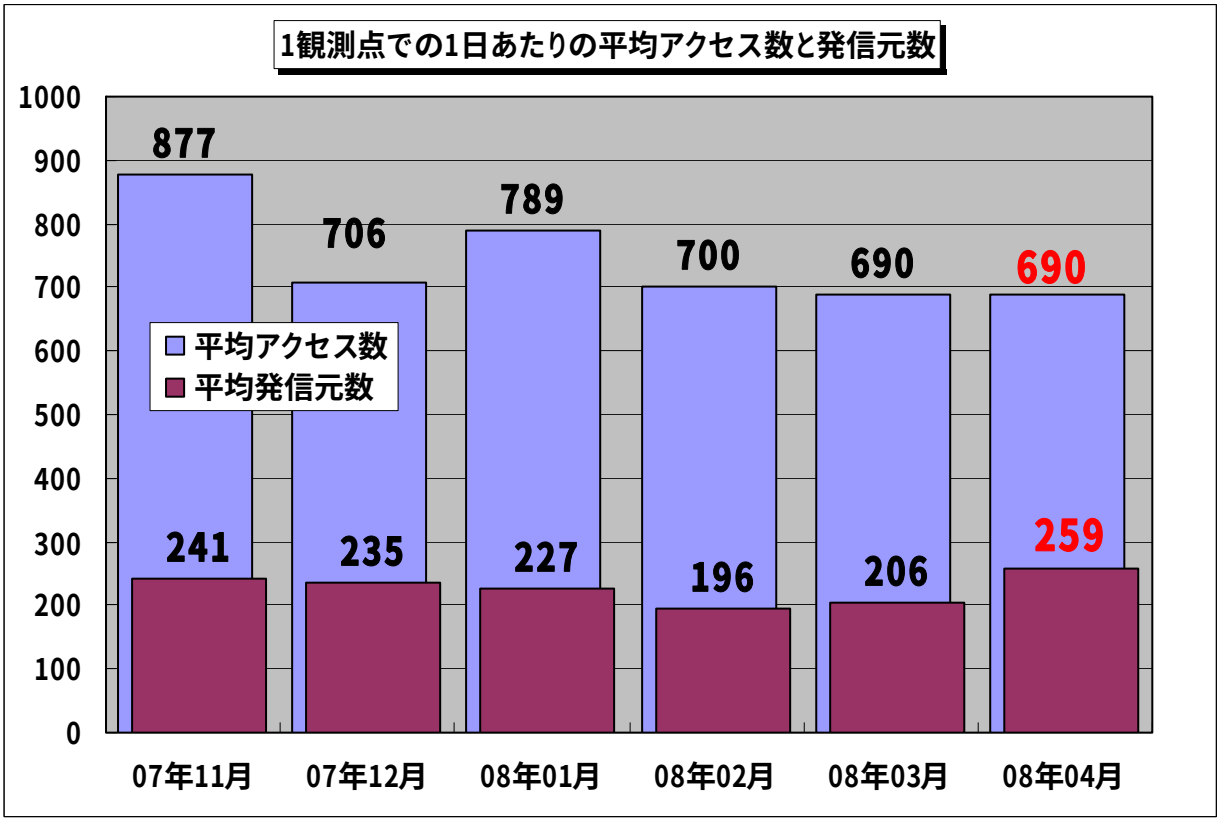
別紙 3

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 4 月の期待しない（一方的な）アクセスの総数は、10 観測点で **206,970 件**あり、且つ発信元の総数は 10 観測点で **77,804** ありました。1 観測点で 1 日あたり **259** の発信元から **690 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、259 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。

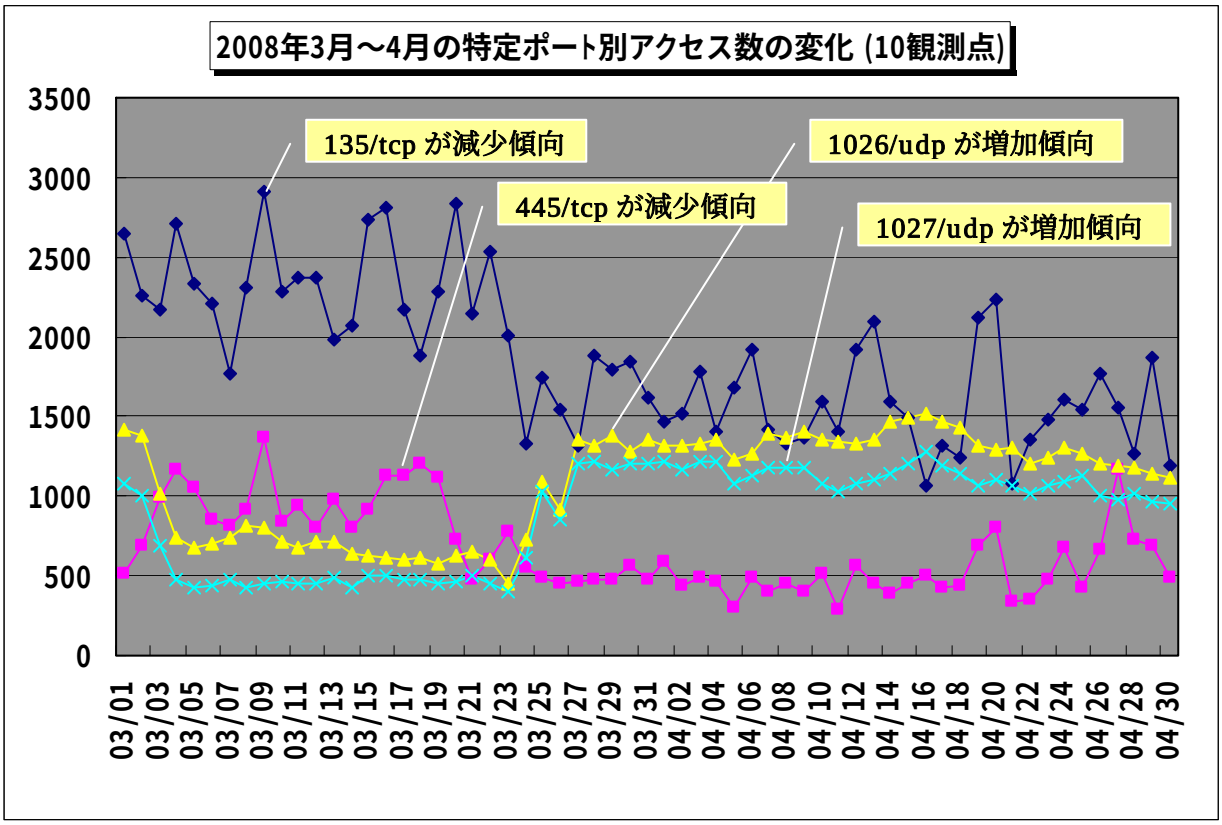


【図 1.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2007 年 11 月～2008 年 4 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、4 月の期待しない（一方的な）アクセスは 3 月とほぼ同水準であり、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。

2．4月のアクセスの状況

2008年4月のアクセス状況は、3月とほぼ同水準でした。増減の内訳としてはWindowsの脆弱性をねらったアクセスである 135/tcp、445/tcp が減少傾向を示し、Windows Messenger service を利用したポップアップ（スパム）メッセージを送信するアクセスである 1026/udp、1027/udp が増加傾向を示していました。（図2.1参照）



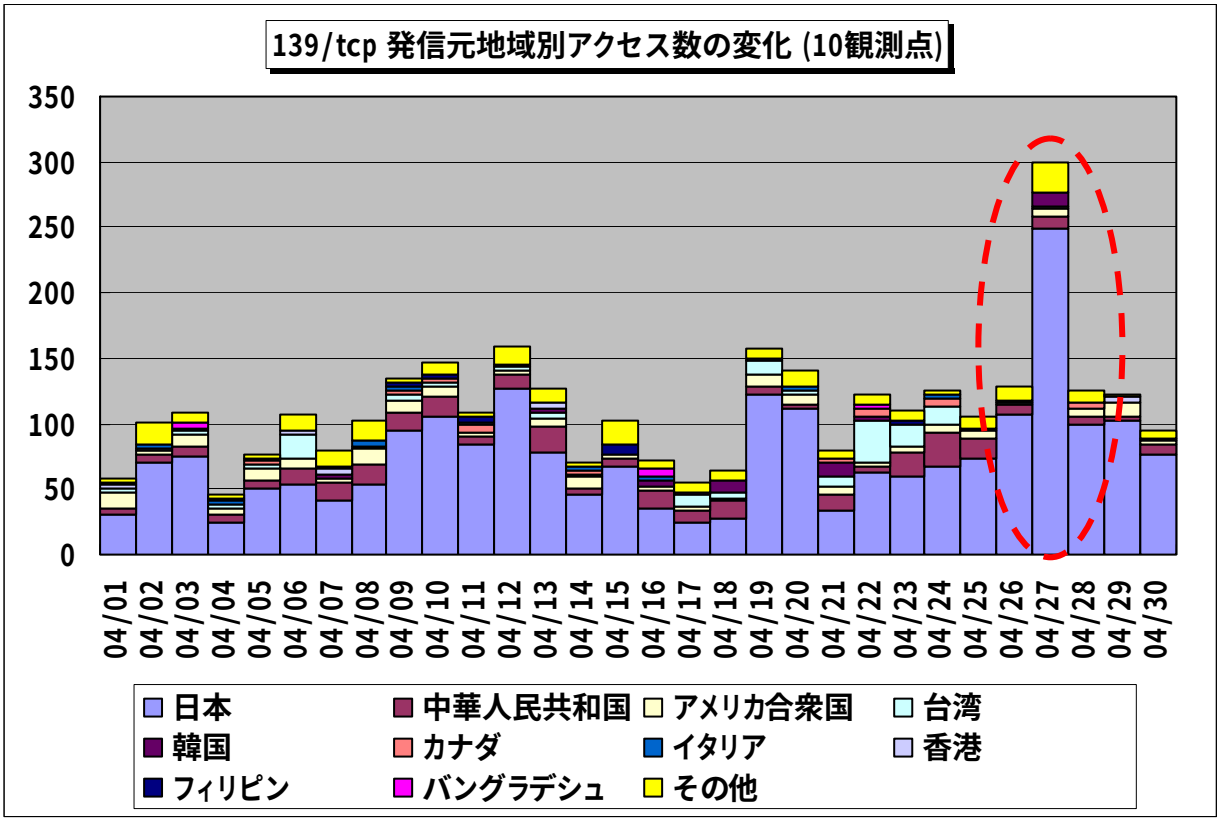
【図2.1　2008年3月～4月　特定ポート別のアクセス数の変化】

2.1．139/tcp、445/tcp ポートを狙ったアクセス

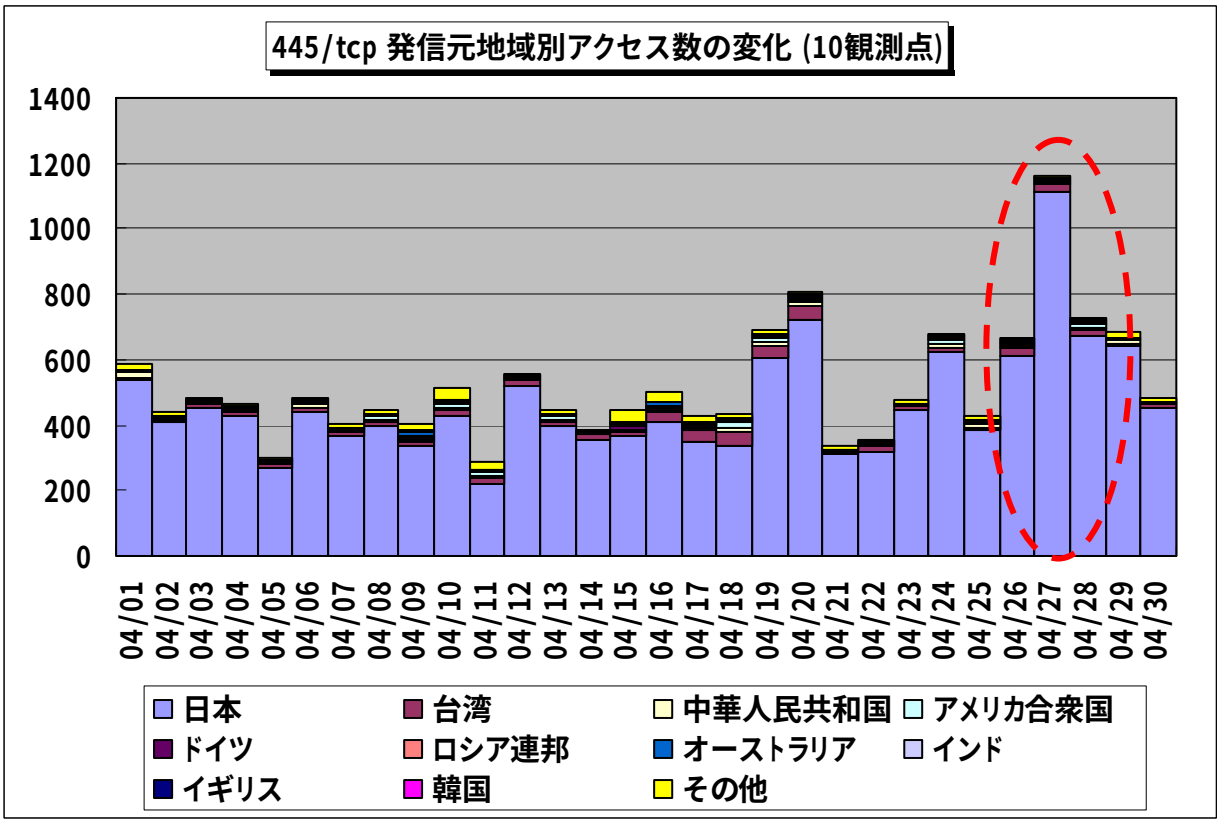
4月の後半辺りに139/tcpポートや、445/tcpポートへのアクセスが一時的に多く見受けられました。これはゴールデンウィークに入り、自宅でパソコンを利用する人が増え、そのパソコンがボットに感染していた為にそこからのアクセスが一時的に増加した可能性が考えられます。

これらのポートは保護の甘いファイル（ネットワーク）共有や Windows の脆弱性を突いて狙われる可能性が高いポートです。

図2.1.1、図2.1.2に2008年4月の139/tcp、445/tcpポートへの発信元地域別アクセス数の変化を示します。



【図 2.1.1　139/tcp ポートへの発信元地域別アクセス数の変化】



【図 2.1.2　445/tcp ポートへの発信元地域別アクセス数の変化】

ボットによる感染は利用者に気づかれることなく行われることが多く、知らないうちにボットネットワークに組み込まれている場合が多く見られます。

残りのゴールデンウィーク中もこのような傾向が続くことが予想されますので、今一度ご自分のパソコンがボットに感染していないか以下を参考に確認してください。

(参考資料)

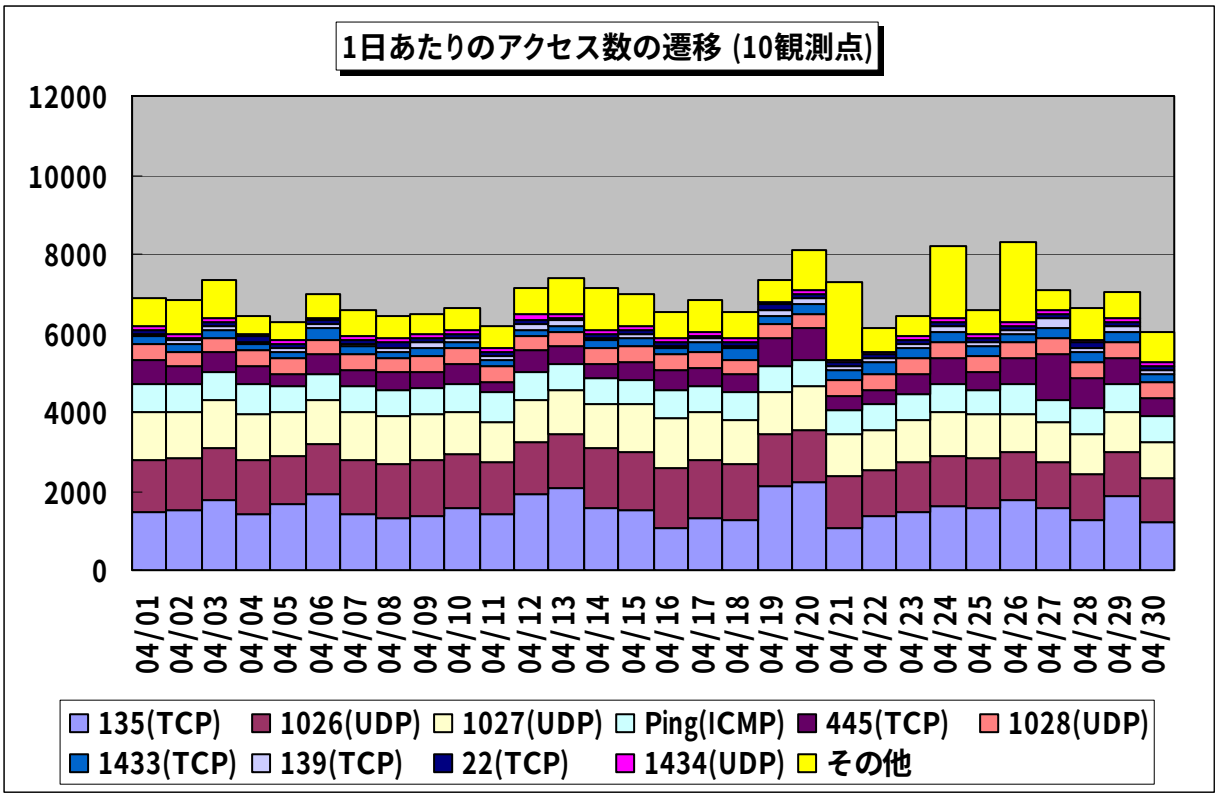
■ ボット対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/3_bot_v5.pdf

■ 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/

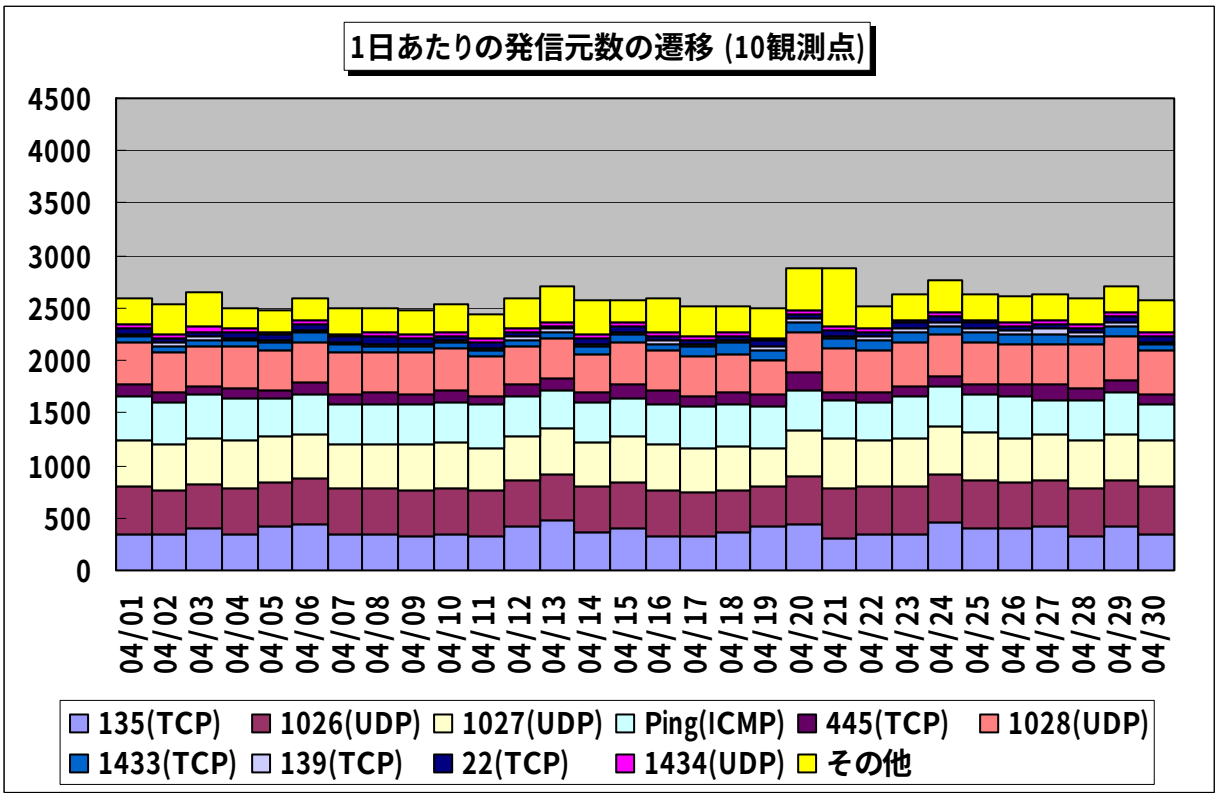
■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html

2.2 2008 年 4 月の一方的なアクセス状況

2008 年 4 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。



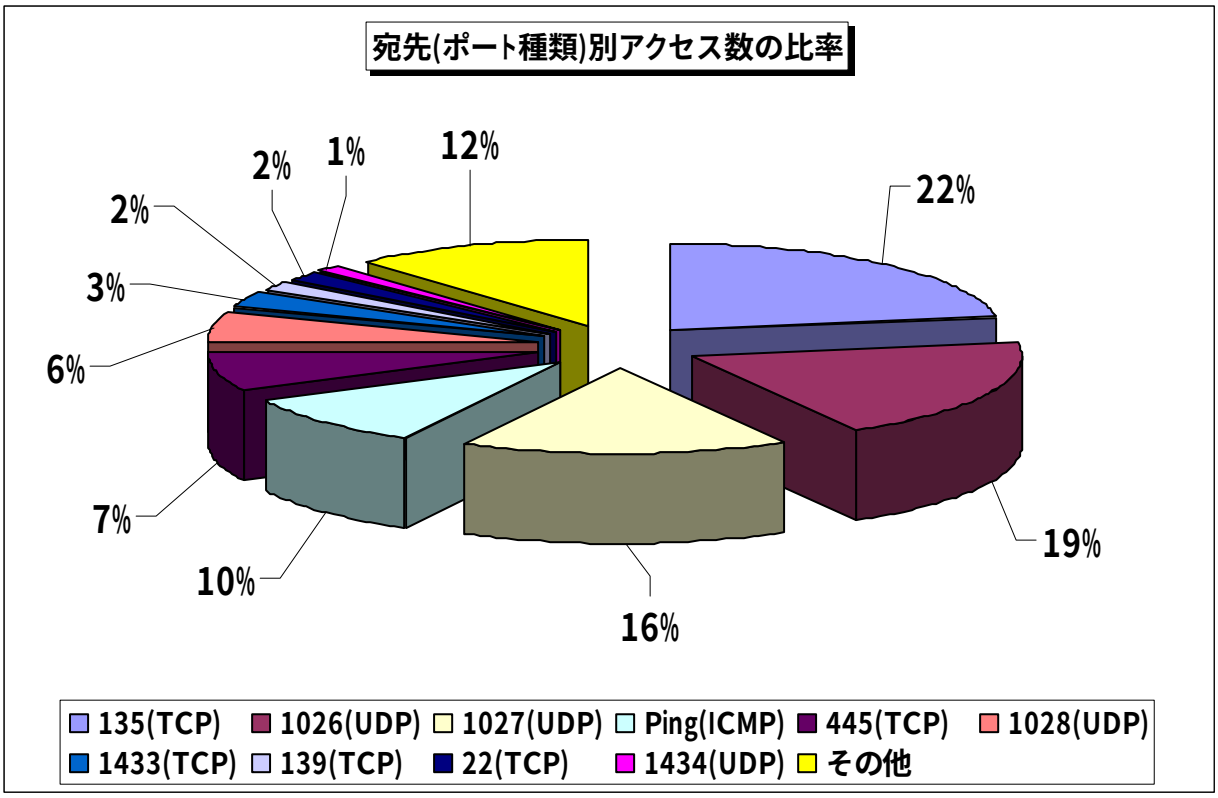
【図 2.2.1 2008 年 4 月の一方的なアクセス状況(アクセス数)】



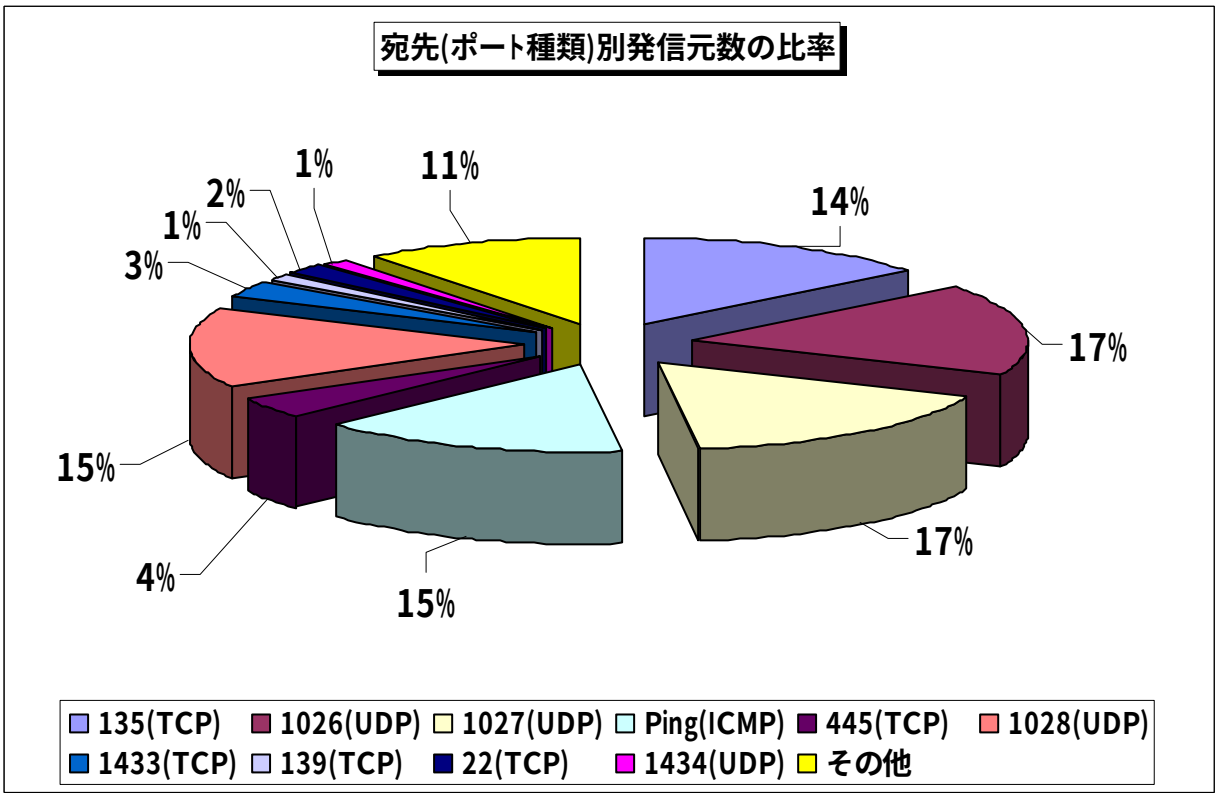
【図 2.2.2 2008 年 4 月の一方的なアクセス状況(発信元数)】

2.3 2008 年 4 月の宛先(ポート種類)別の比率

2008 年 4 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。



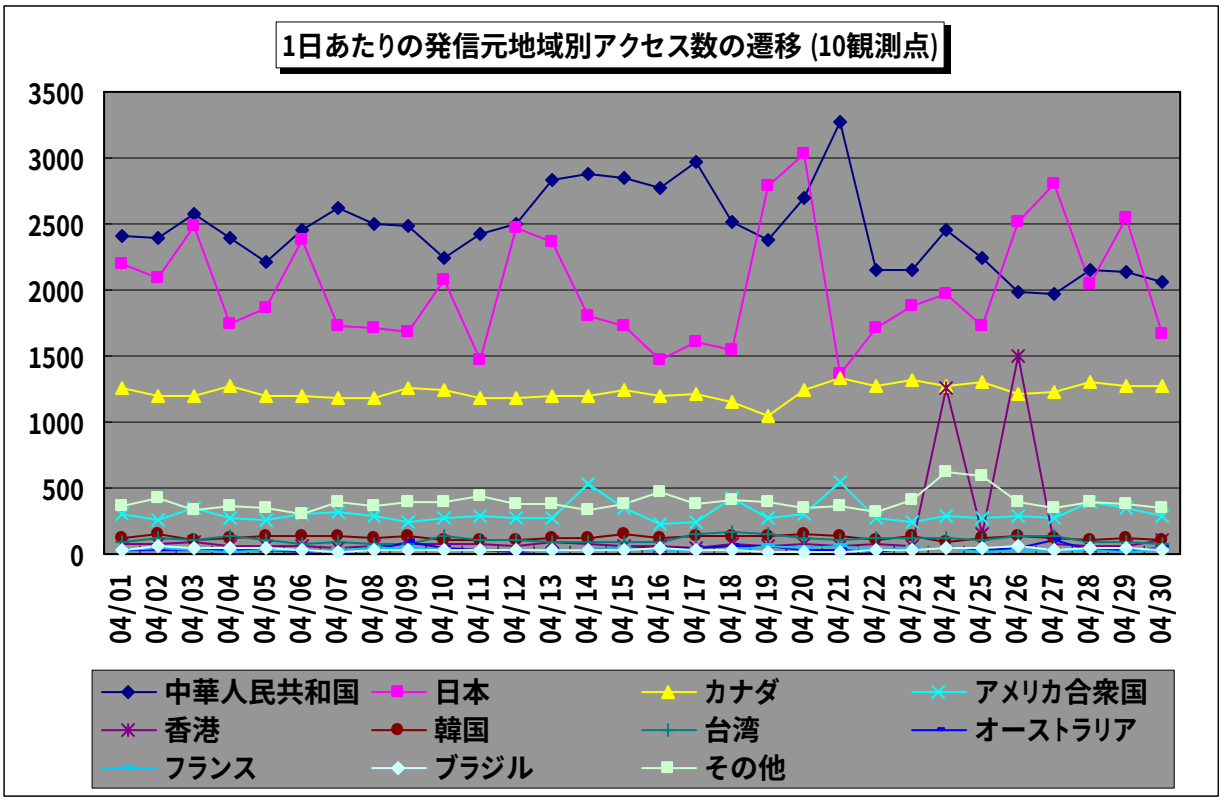
【図 2.3.1 2008 年 4 月の宛先(ポート種類)別アクセス数の比率】



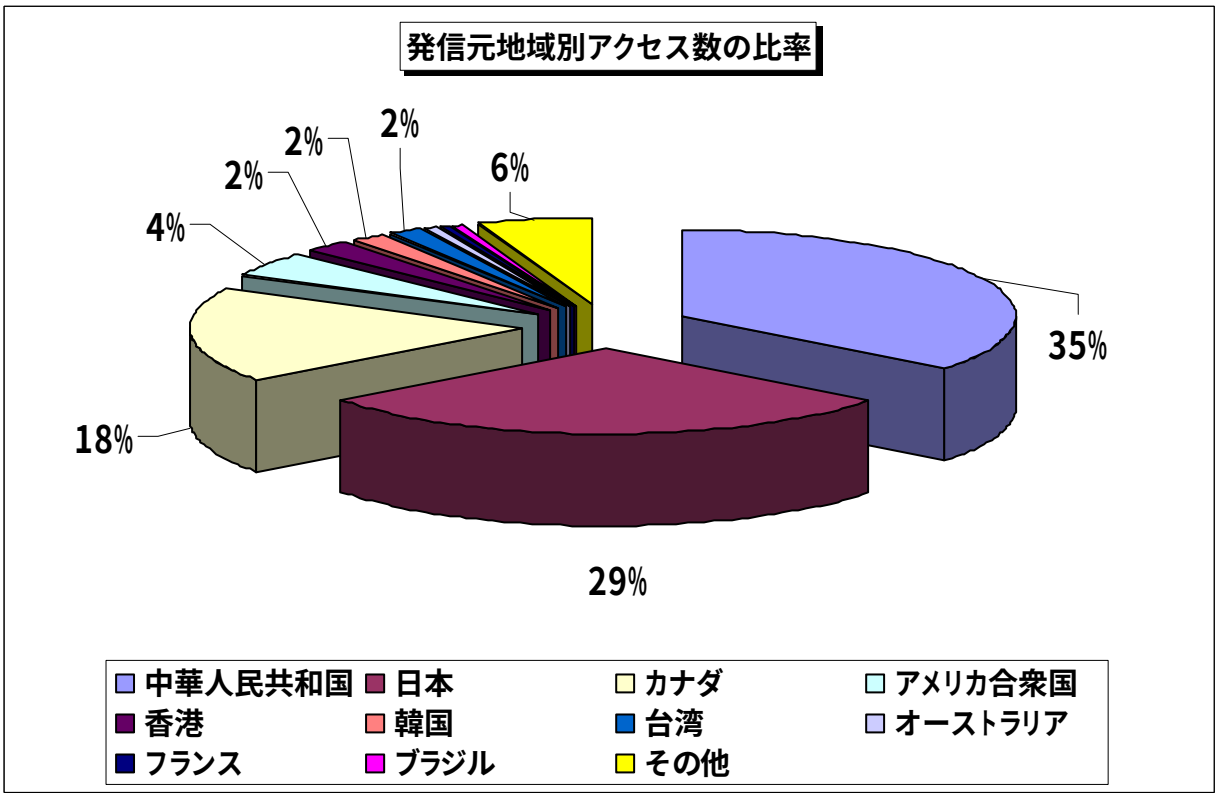
【図 2.3.2 2008 年 4 月の宛先(ポート種類)別発信元数の比率】

2.4 2008 年 4 月の発信元地域別アクセス状況

2008 年 4 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。

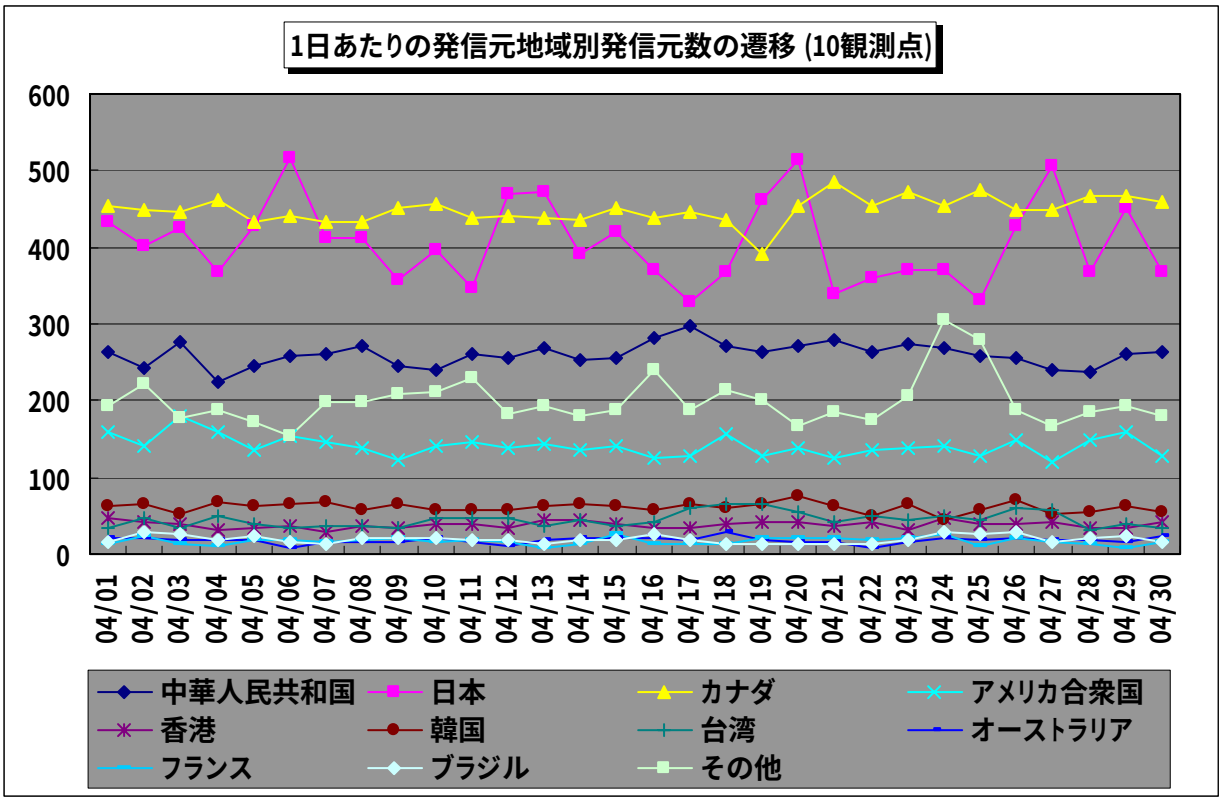


【図 2.4.1 2008 年 4 月の発信元地域別アクセス数の変化】

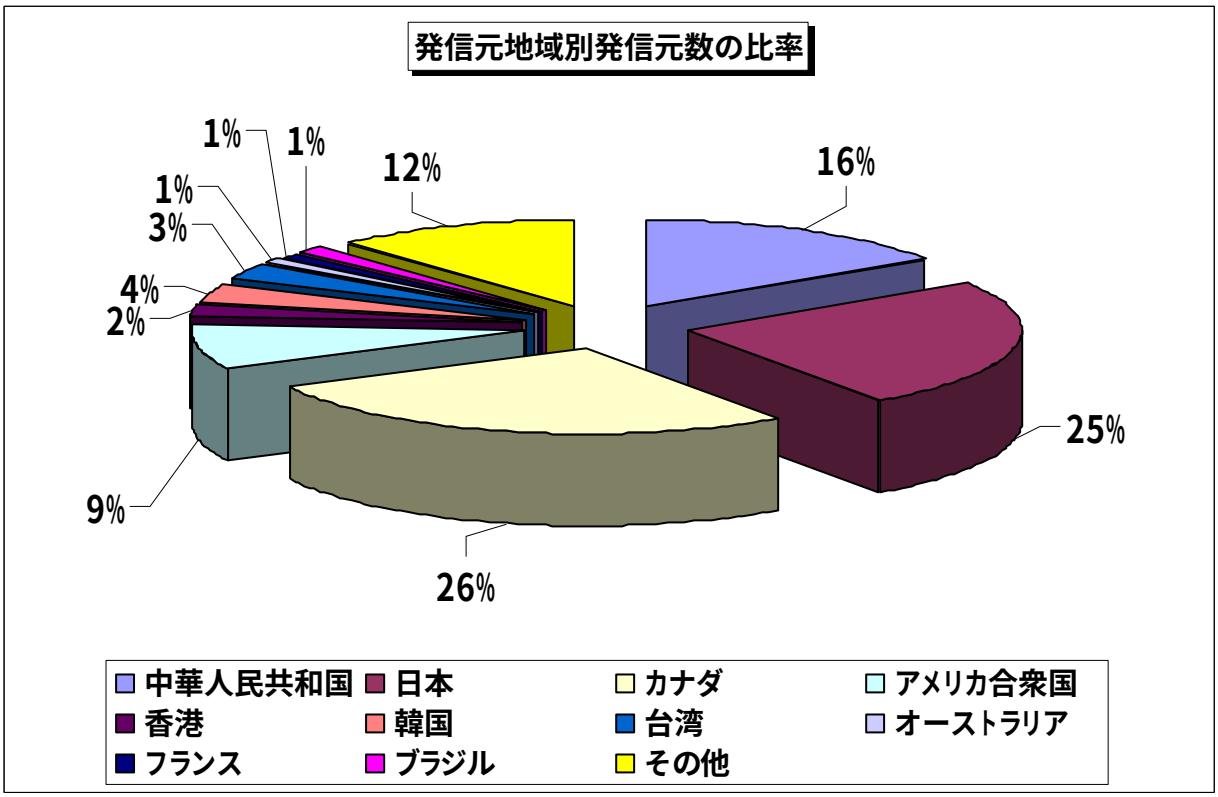


【図 2.4.2 2008 年 4 月の発信元地域別アクセス数の比率】

2008 年 4 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 4 月の発信元地域別発信元数の変化】

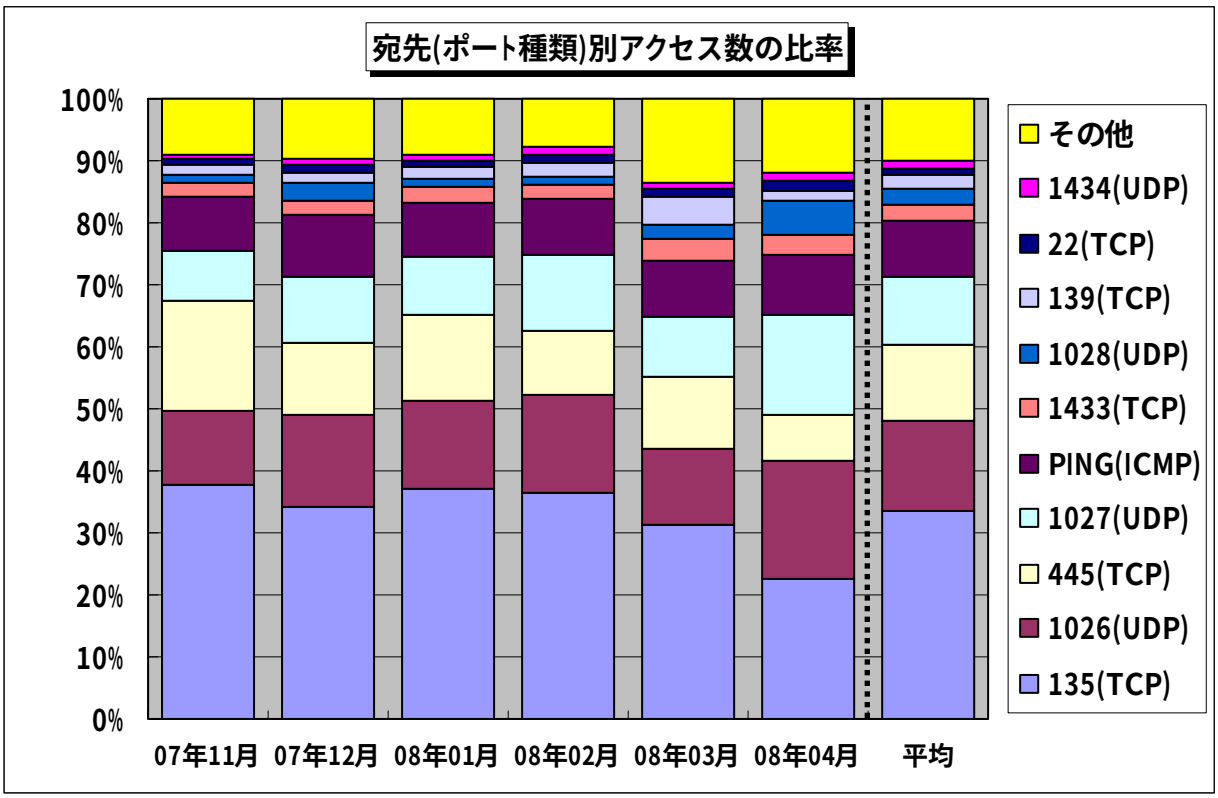


【図 2.4.4 2008 年 4 月の発信元地域別発信元数の比率】

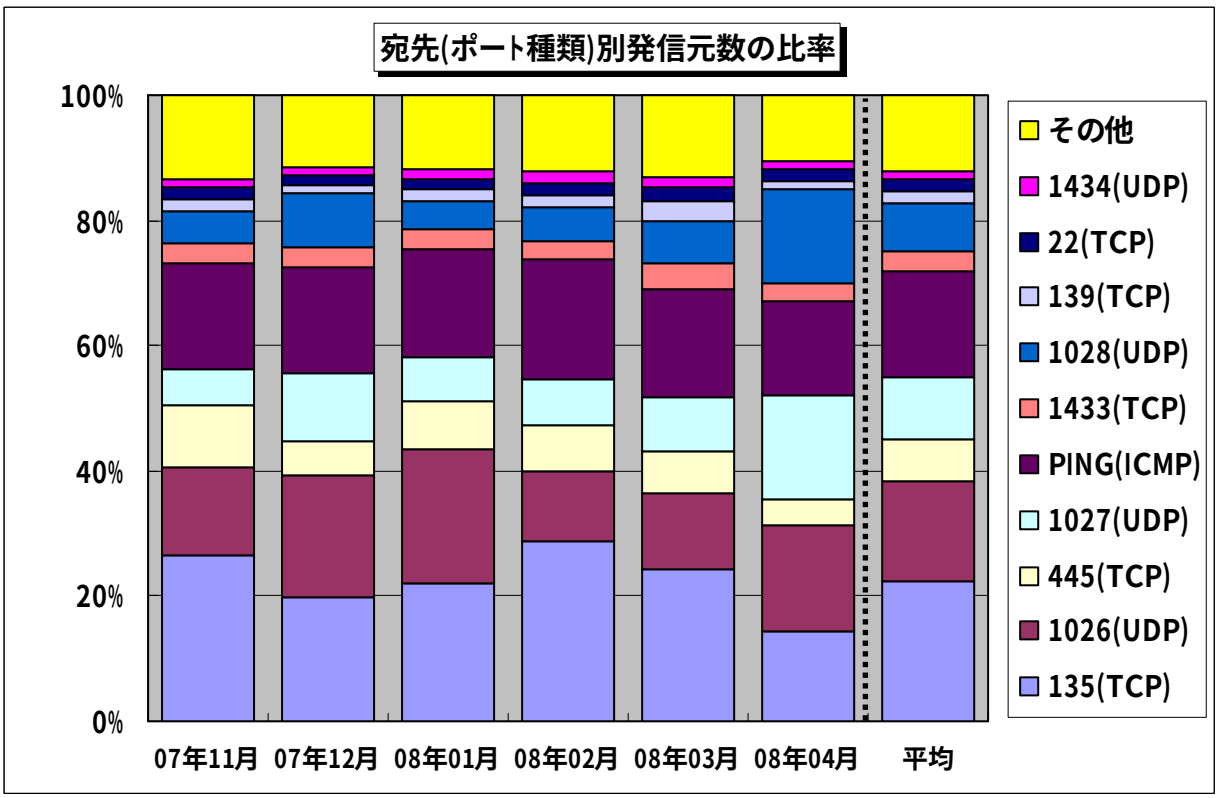
3．統計情報

3.1 2007 年 11 月～2008 年 4 月の宛先(ポート種類)別の比率

2007 年 11 月～2008 年 4 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。



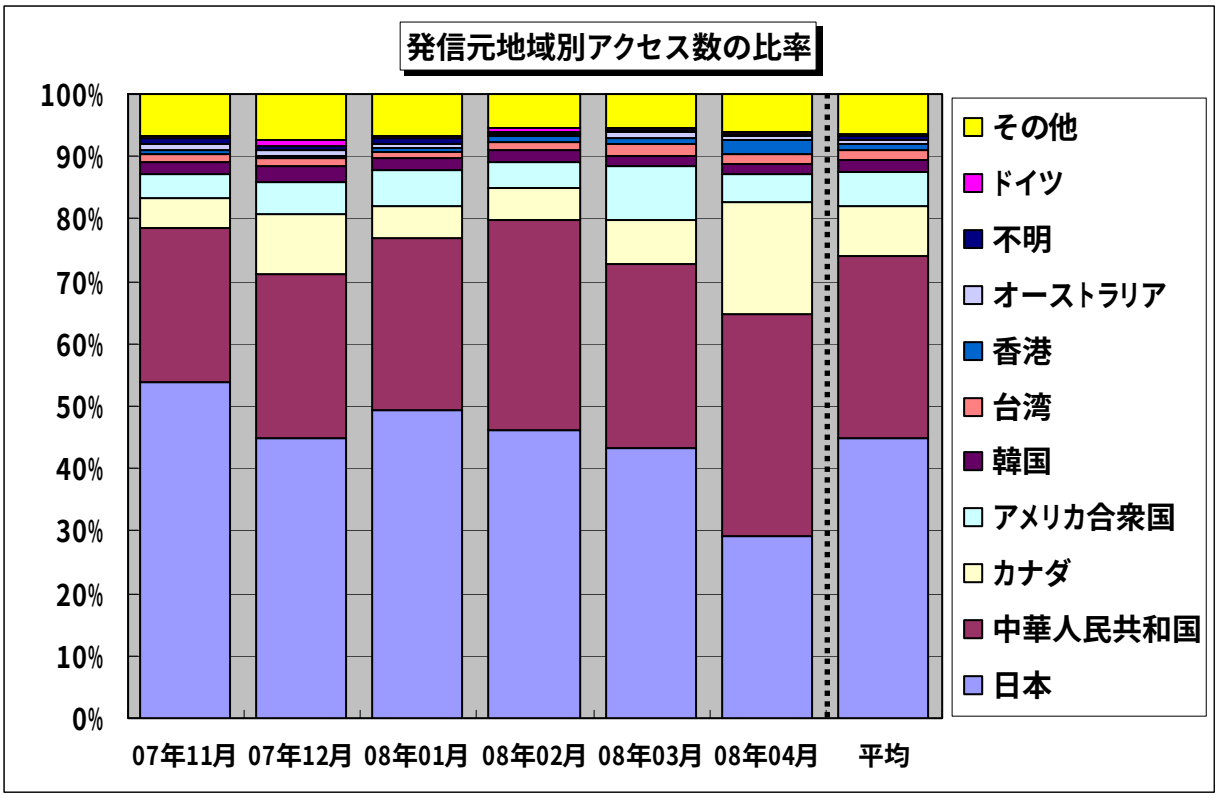
【図 3.1.1 2007 年 11 月～2008 年 4 月の宛先(ポート種類)別アクセス数の比率】



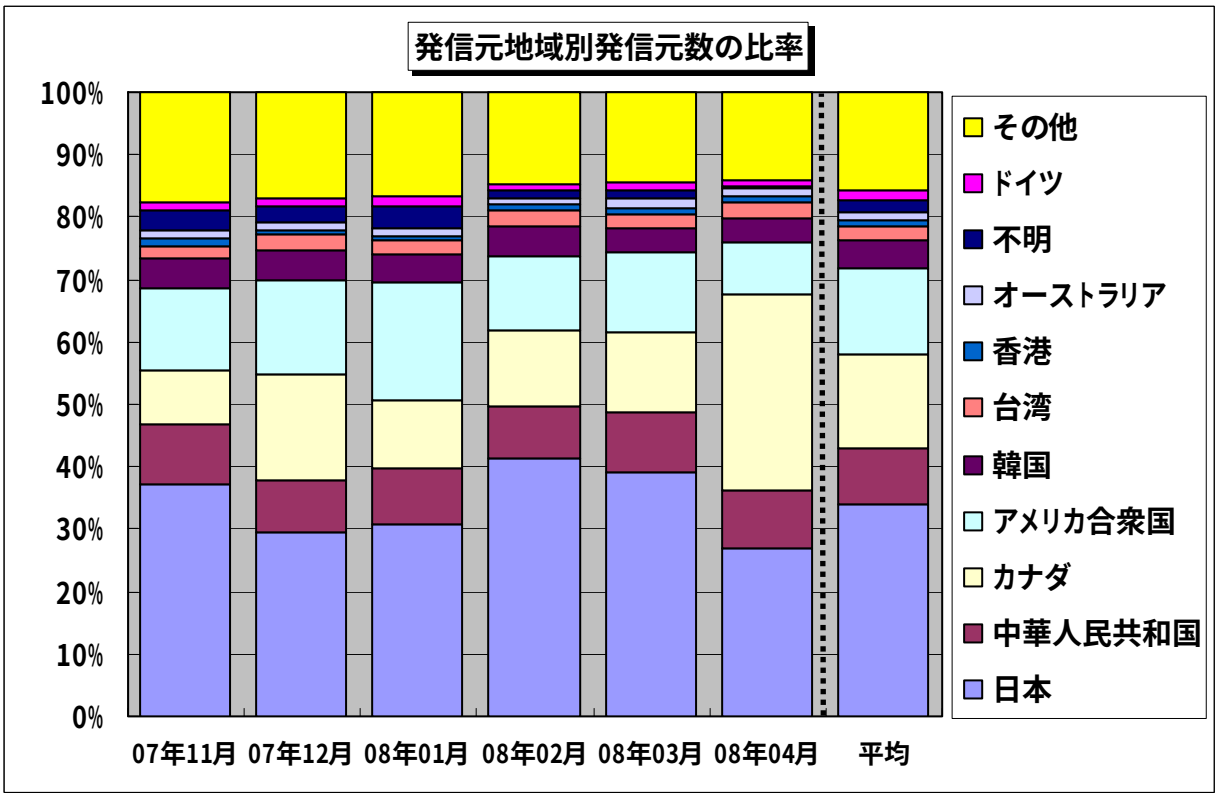
【図 3.1.2 2007 年 11 月～2008 年 4 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 11 月～2008 年 4 月の発信元地域別の比率

2007 年 11 月～2008 年 4 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 11 月～2008 年 4 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 11 月～2008 年 4 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 4 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