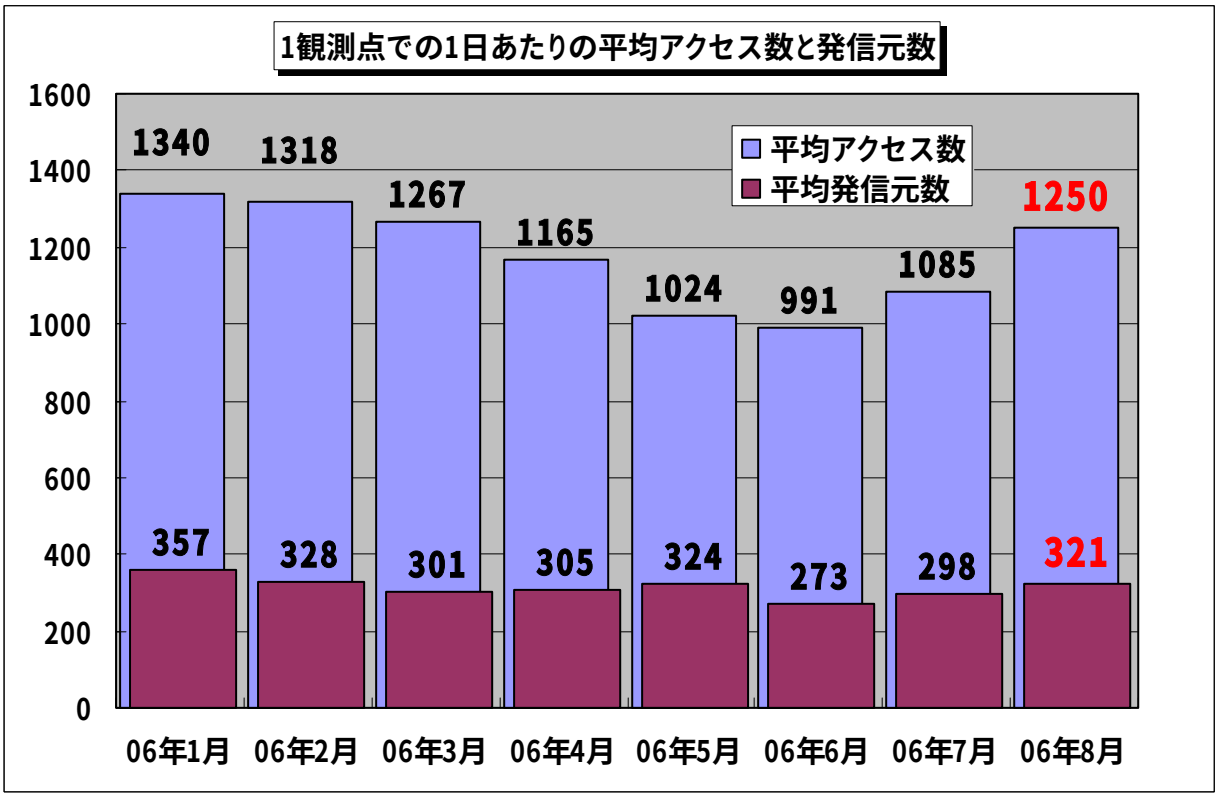
別紙 3

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、2006 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 **387,534 件**ありました。1 観測点で 1 日あたり **321** の発信元から **1,250 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、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**と言うことになります。



【図 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 1 月～2006 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 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、先月より増加しました**。全体的なアクセス内容については、定常化していると言えますが、新しい Windows のぜい弱性を狙ったと思われるアクセスが発生しています。ご注意下さい。

2．8 月のアクセス状況

8 月のアクセス状況は、全体的には 7 月とほぼ同じ状況ですが、**新しい Windows のぜい弱性を狙ったと思われる 139(TCP)ポートへのアクセスが発生しています**。既存の Windows のぜい弱性を狙っていると思われる不正なアクセスもあいかわらず多いようで、これらのアクセスの多く

は、ボットに感染したコンピュータから送信されていると思われます。さらに、先月末からのアクセス(数)の増加傾向が続いており、パスワードクラッキングによるコンピュータへの侵入を狙う22(TCP)ポートへのアクセスも増加しています。

2.1 2006 年 8 月の 139(TCP)ポートへのアクセス状況

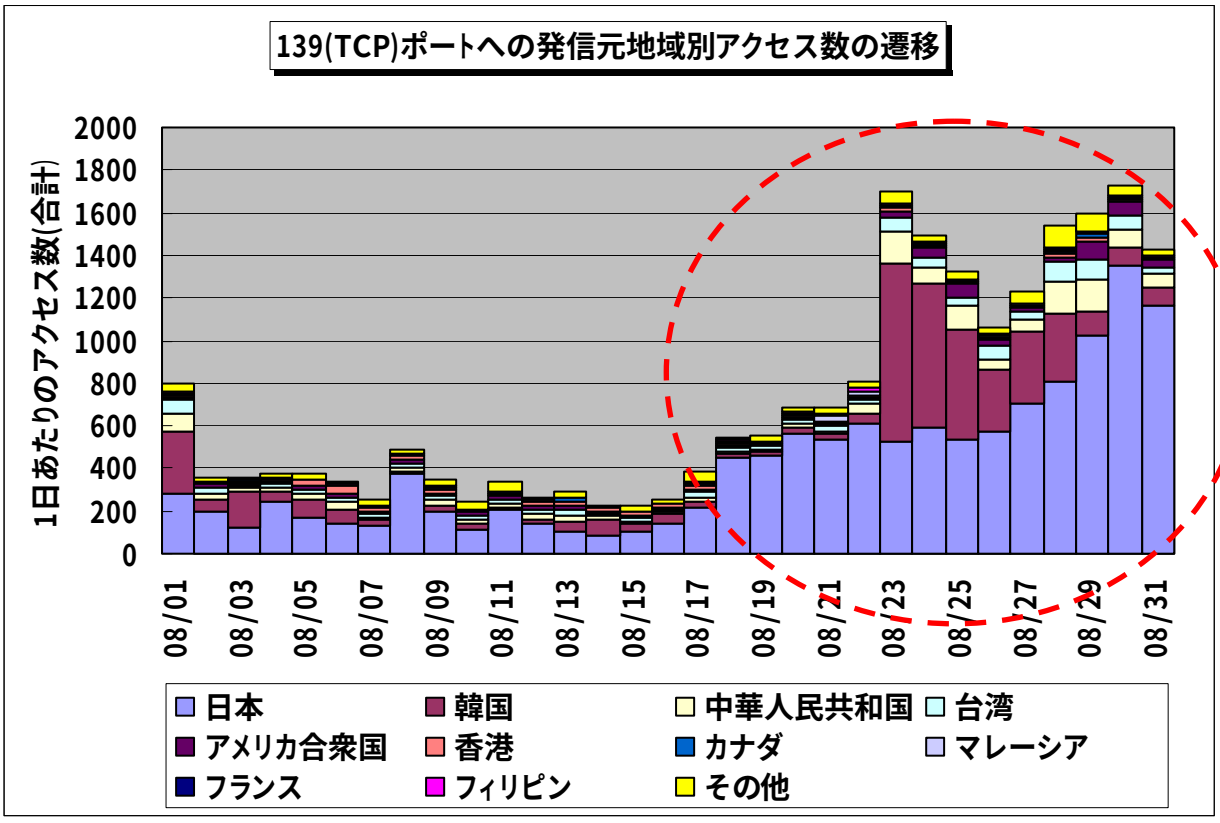
139 (TCP) ポートへのアクセスについては、新しい Windows のぜい弱性(MS06-040)を狙ったものと考えられます。このぜい弱性に対する攻撃(検証)コードが公開されており、ぜい弱性を狙った新しいワームや、攻撃コードが仕込まれたボットが広がっている可能性があります。

図 2.1.1、図 2.1.2 および図 2.1.3 に、139(TCP)ポートへの発信元地域別アクセス数と発信元数の遷移を示します。これらの図を見ると、8 月 18 日前後から発信元を国内とするアクセスが増加し、8 月 23 日から韓国方面を発信元とするアクセスが急増しています。実際には、国内からは被害報告や問い合わせがないため、国内での被害状況については分かりませんが、発信元となっている国内のコンピュータにはワームあるいはボットが感染しているものと思われます。国内のアクセス数が増加傾向にあることが危惧されます。韓国方面からのアクセスについては、発信元数から見ると、終息方向にあるようです。アクセスのパターン (同一の観測点に対するアクセス回数) によると、国内からのアクセスと韓国方面からのアクセスは、少し違う様子なので、種類の違う攻撃コード (ワームあるいはボット) と思われます。

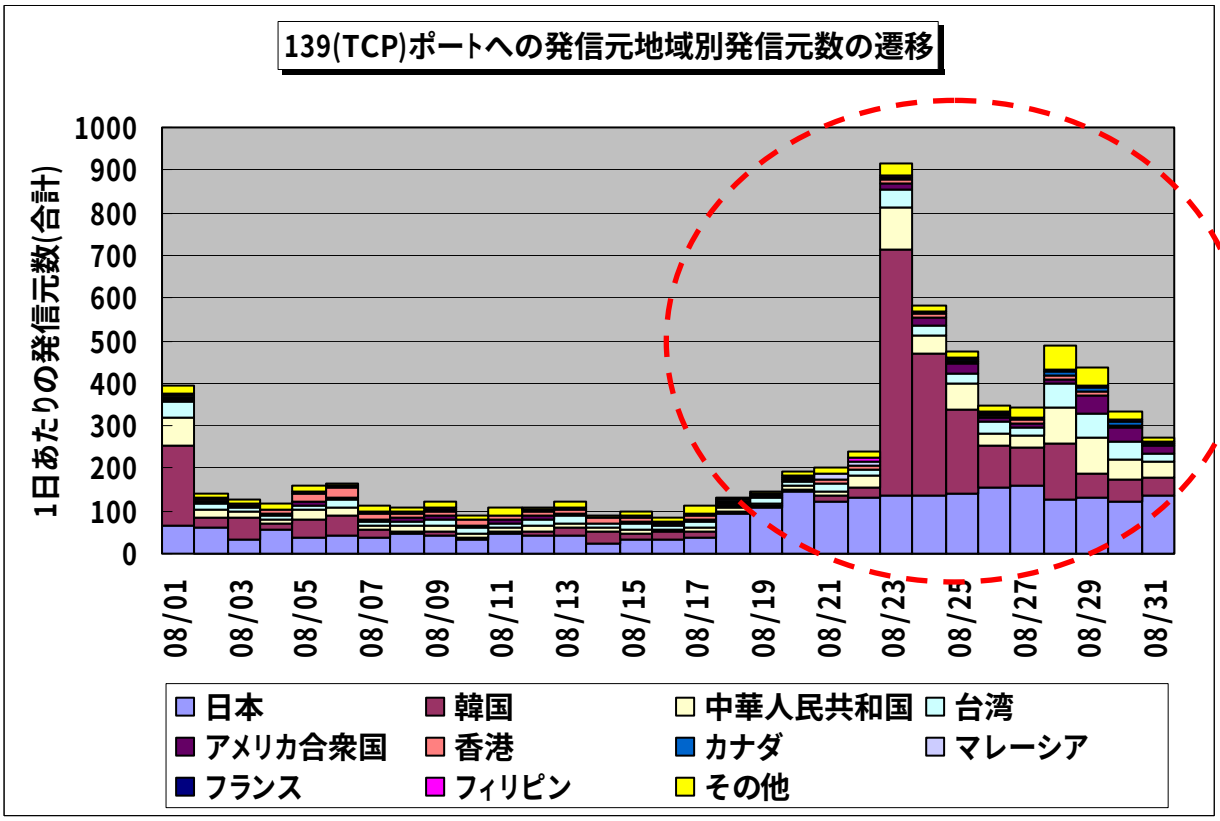
外部からの不正なアクセスを明確に防御している企業(組織)の場合は、特に問題にはなりませんが、インターネットにモデムなどで直接接続する形態の Windows コンピュータを利用されている方は、8 月 10 日に Microsoft から発信されている Windows のぜい弱性を解消するパッチを適用し、さらにファイアウォール機能の利用など、被害に遭わないように心掛けて下さい。

コンピュータの個人利用者は、以下の資料を参考にして、不正アクセス対策を実施して下さい。

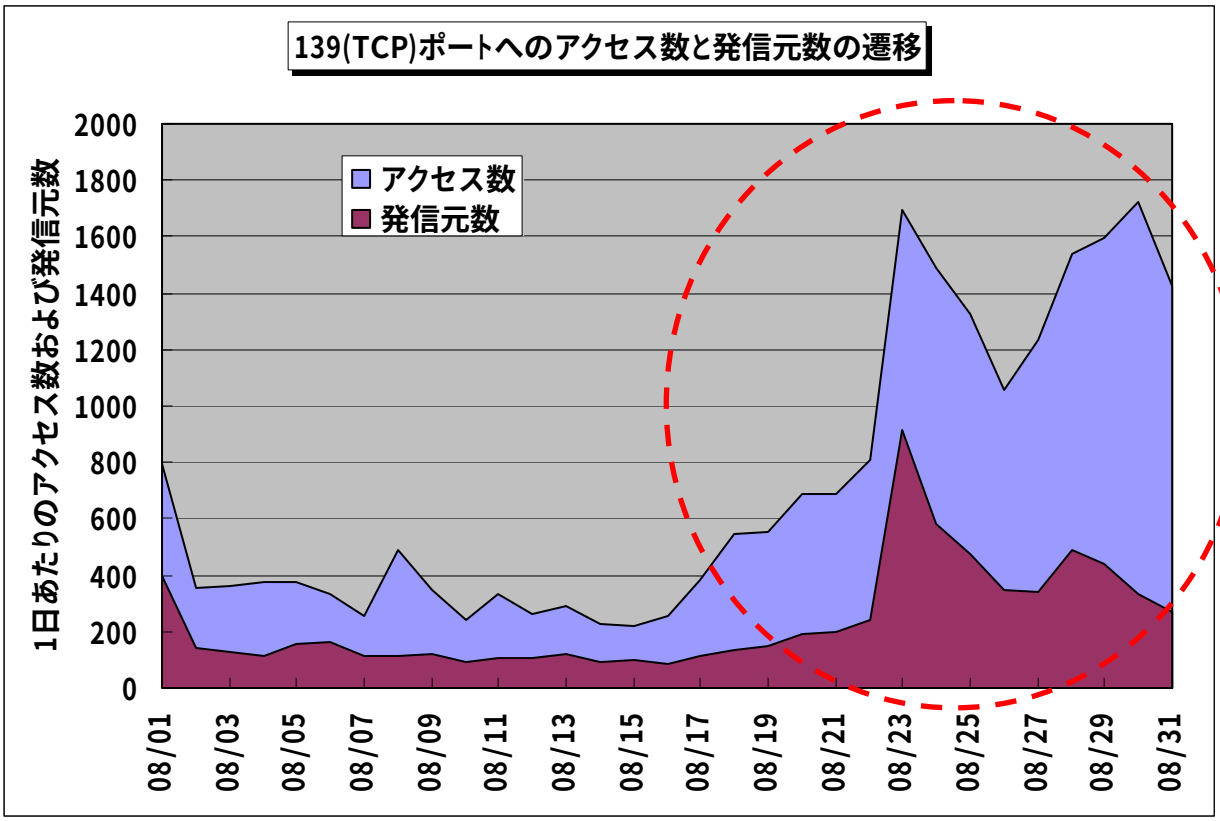
■ 不正アクセス対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html



【図 2.1.1 2006 年 8 月の 139(TCP)ポートへの発信元地域別アクセス数の遷移】



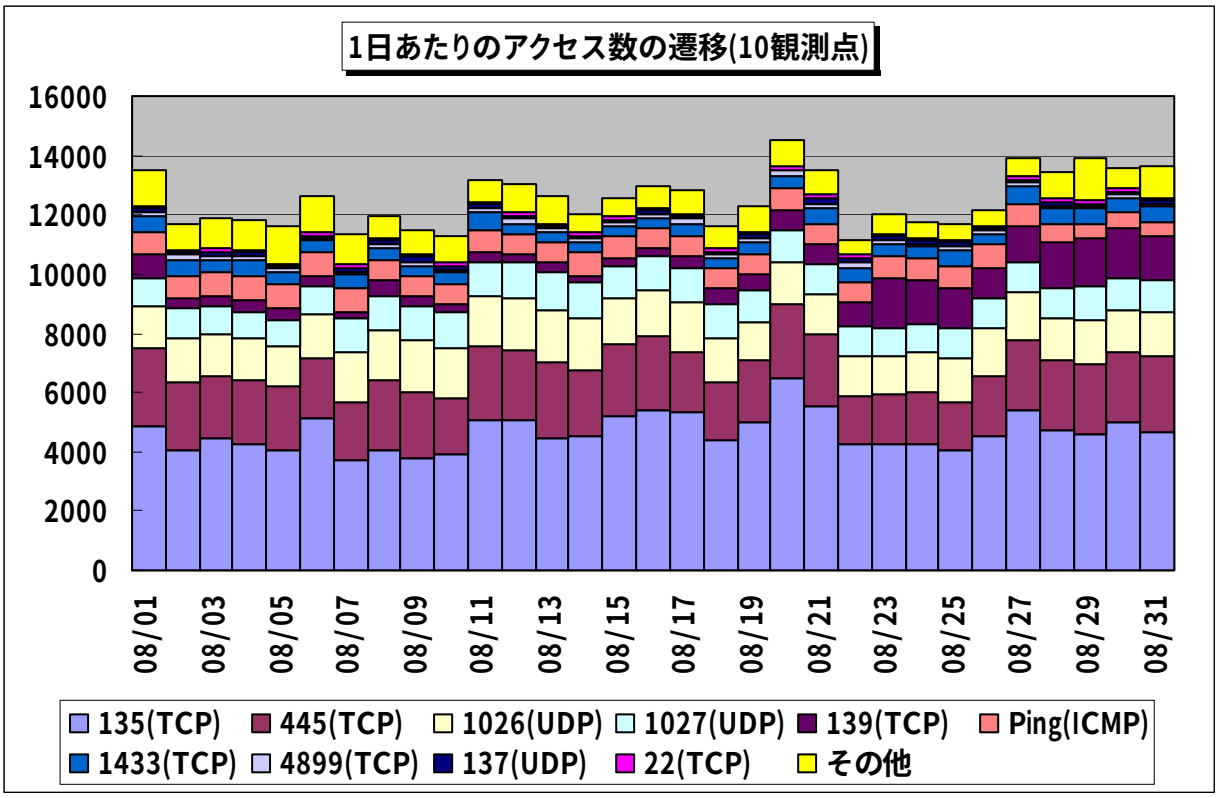
【図 2.1.2 2006 年 8 月の 139(TCP)ポートへの発信元地域別発信元数の遷移】



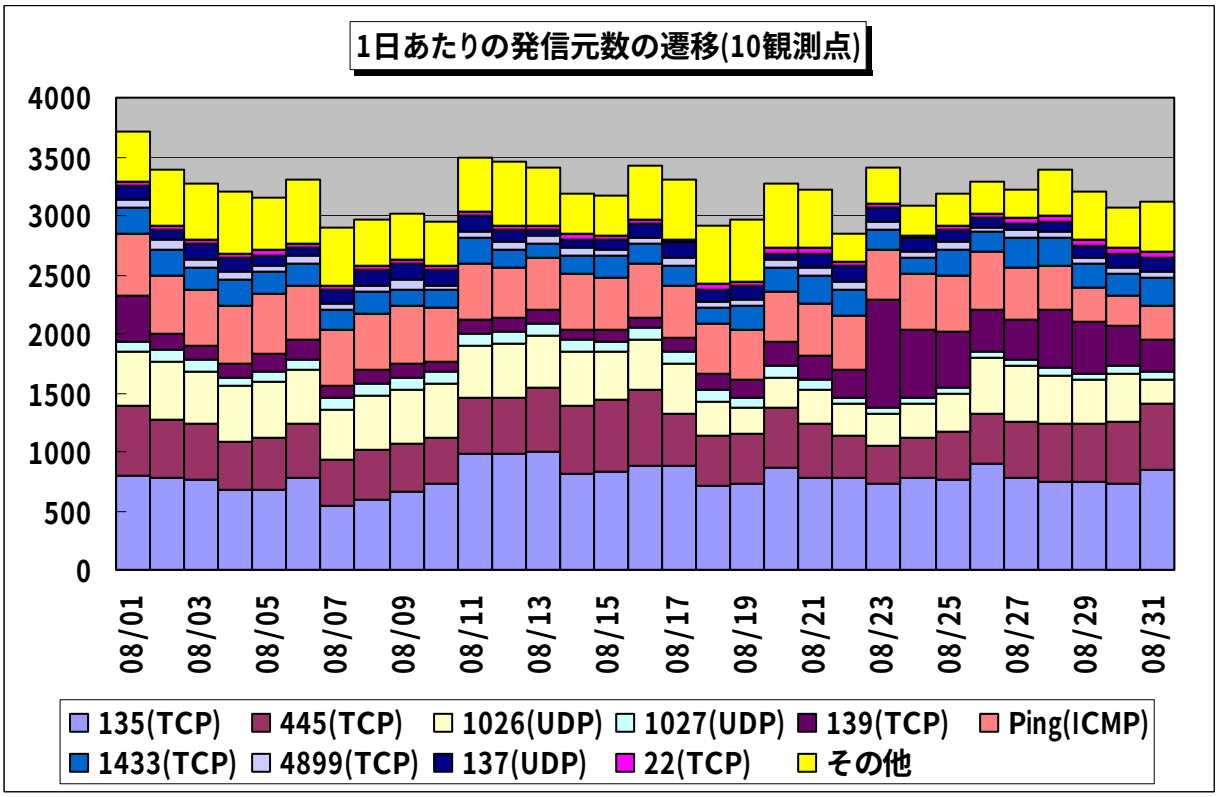
【図 2.1.3 2006 年 8 月の 139(TCP)ポートへのアクセス数と発信元数の遷移】

2.2 2006 年 8 月の一方的なアクセス状況

2006 年 8 月の一方的なアクセス状況（アクセス数）の遷移を図 2.2.1 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。



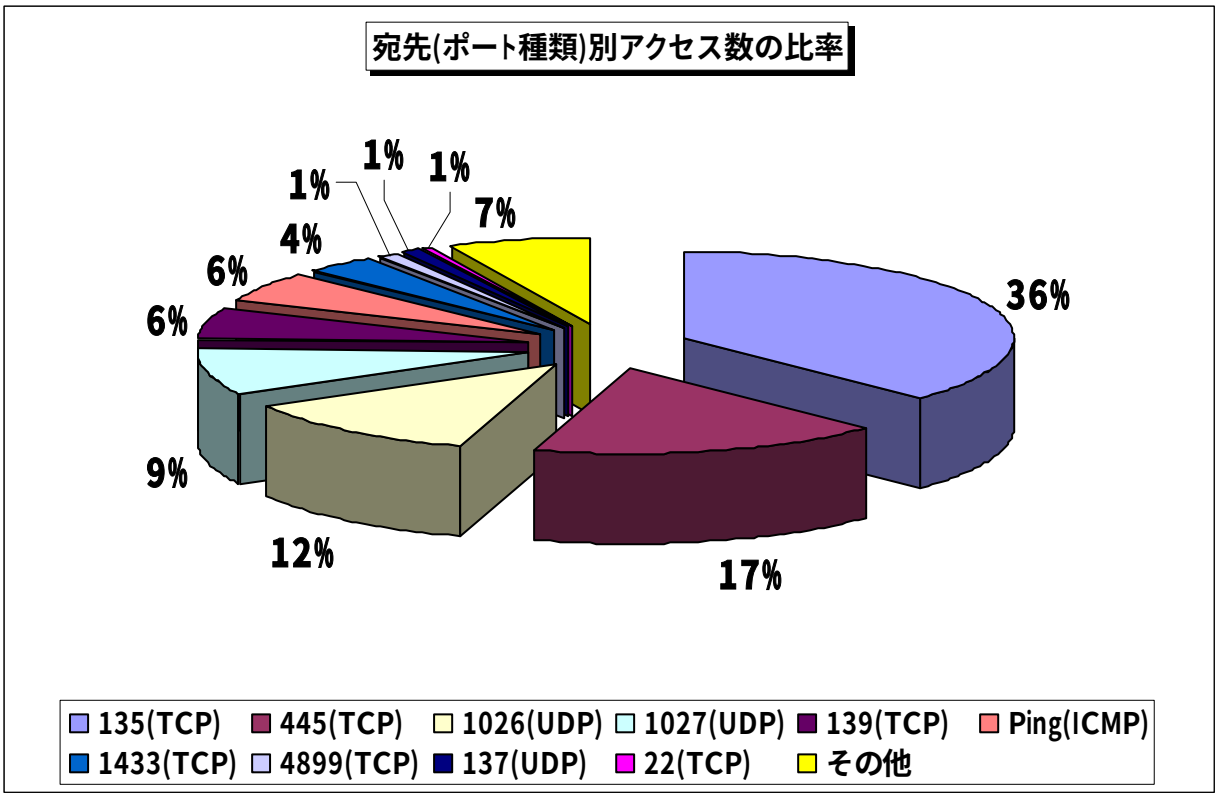
【図 2.2.1 2006 年 8 月の一方的なアクセス状況(アクセス数)】



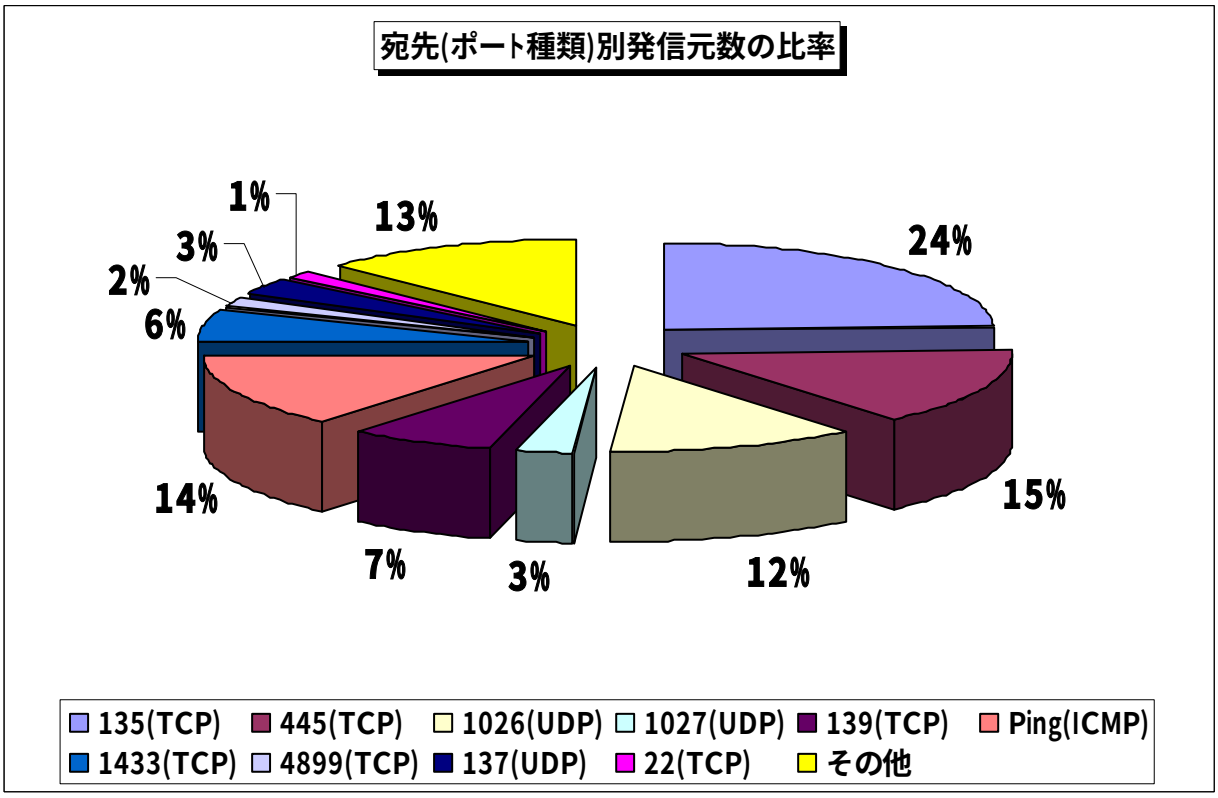
【図 2.2.2 2006 年 8 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 8 月の宛先(ポート種類)別の比率

2006 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 2.3.1 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。



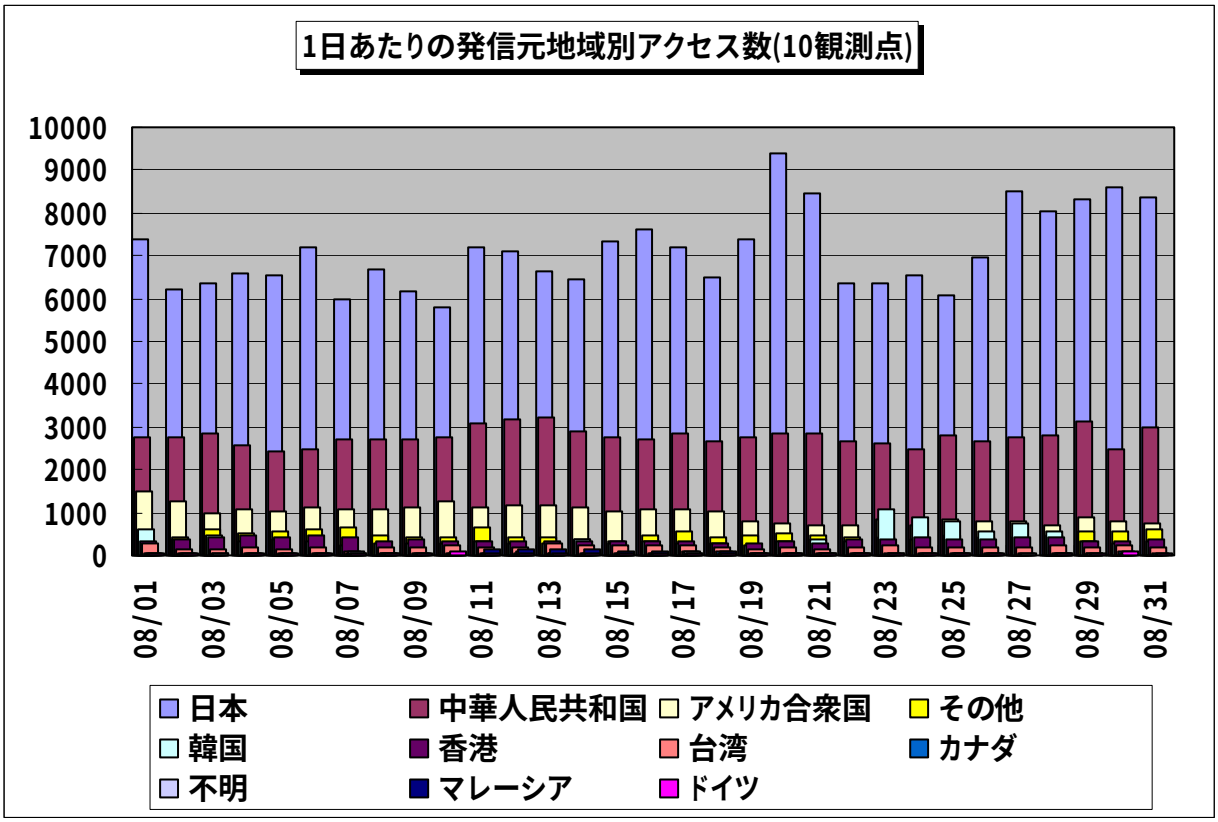
【図 2.3.1 2006 年 8 月の宛先(ポート種類)別アクセス数の比率】



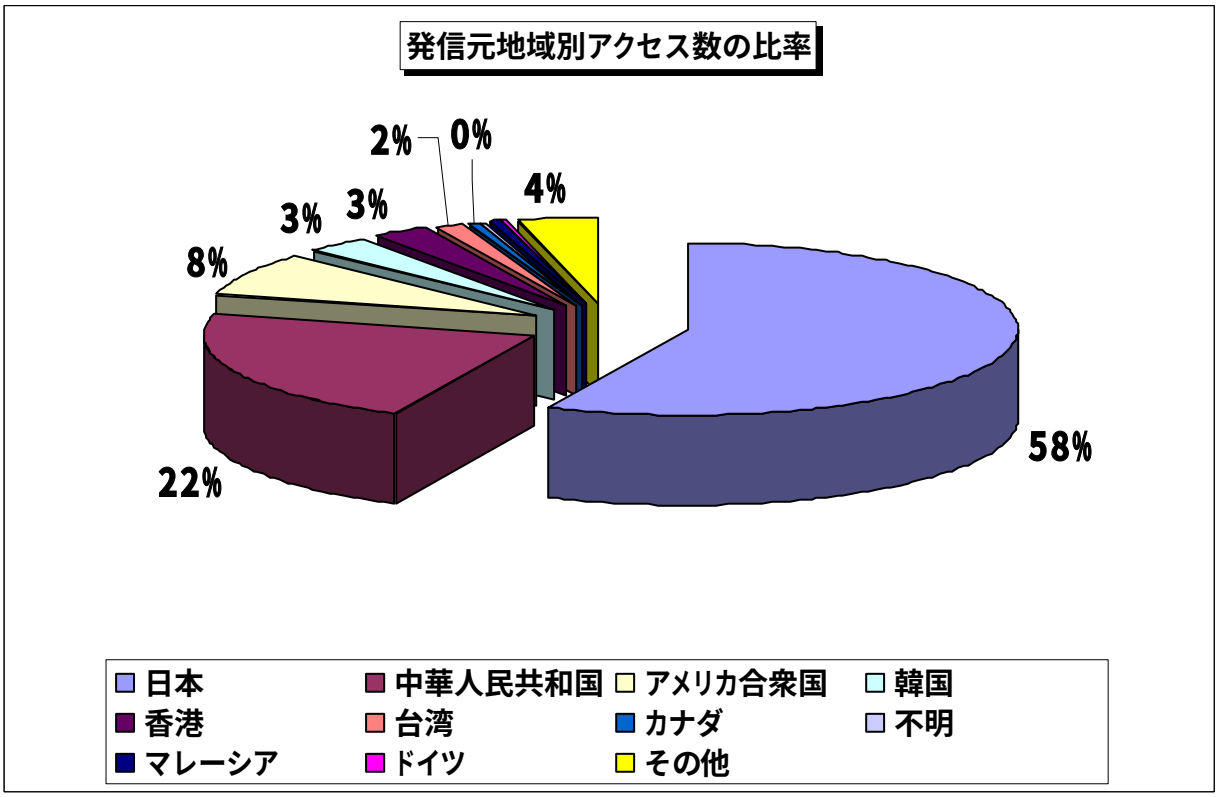
【図 2.3.2 2006 年 8 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 8 月の発信元地域別アクセス状況

2006 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 2.4.1 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。

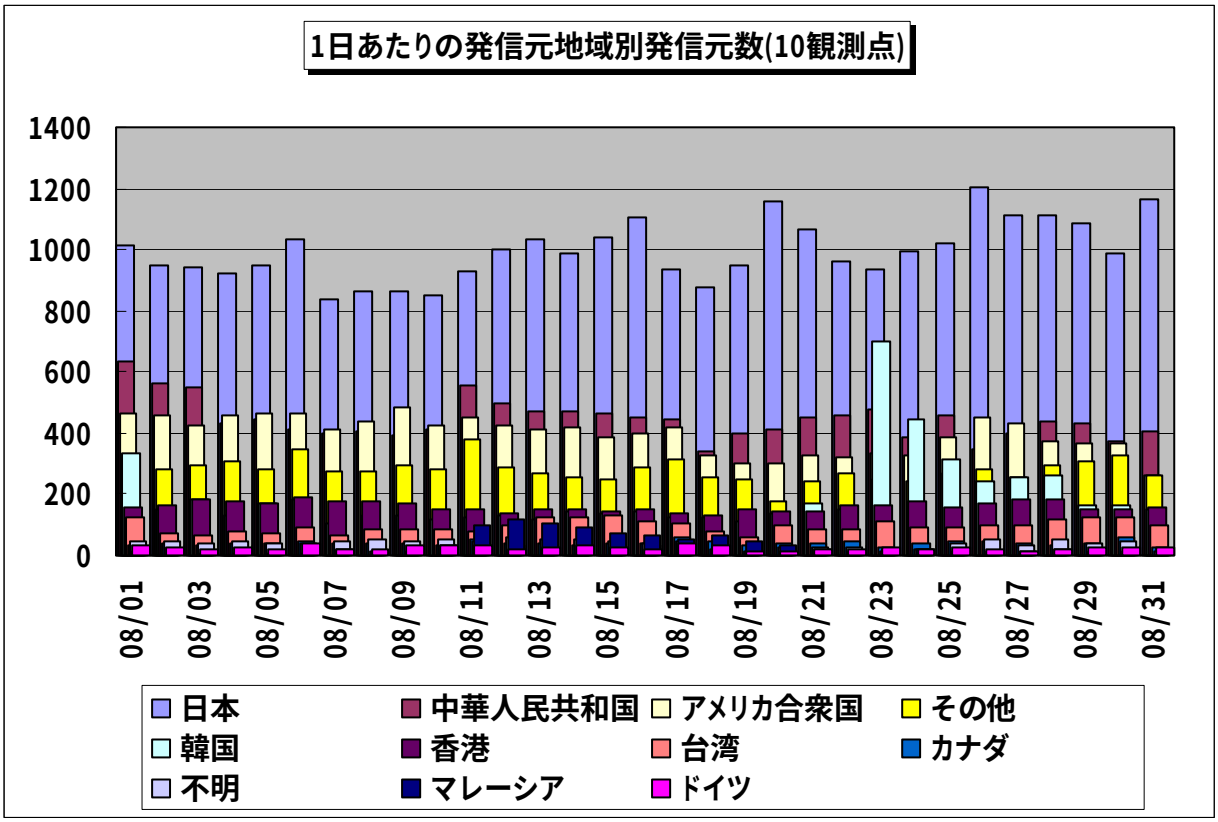


【図 2.4.1 2006 年 8 月の発信元地域別アクセス数の変化】

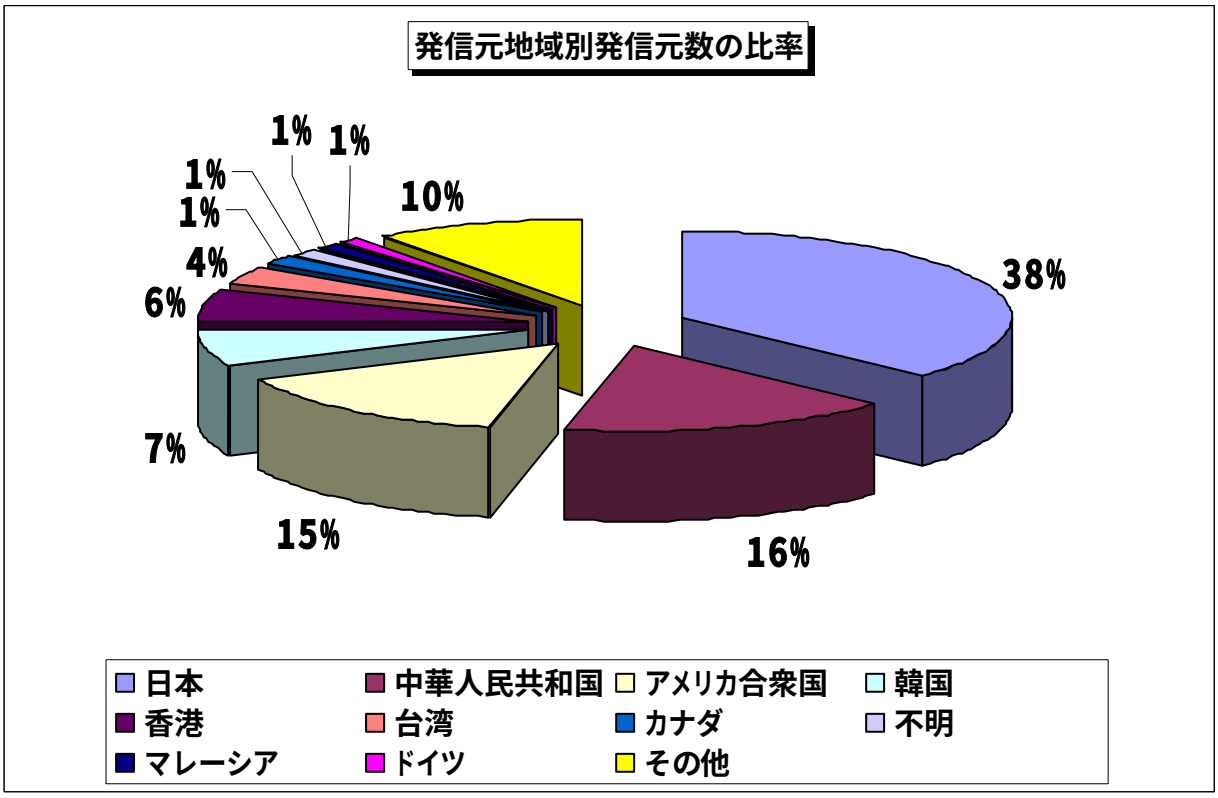


【図 2.4.2 2006 年 8 月の発信元地域別アクセス数の比率】

2006 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 2.4.3 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 2006 年 8 月の発信元地域別発信元数の変化】

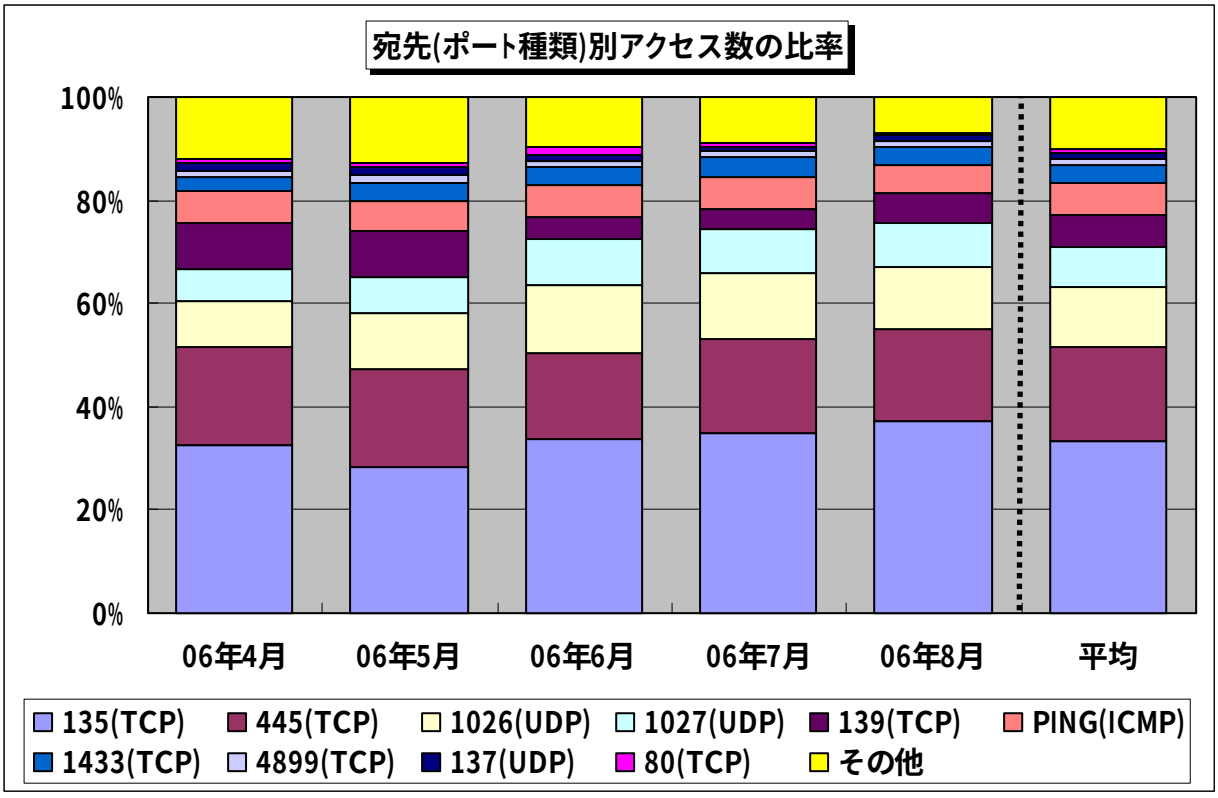


【図 2.4.4 2006 年 8 月の発信元地域別発信元数の比率】

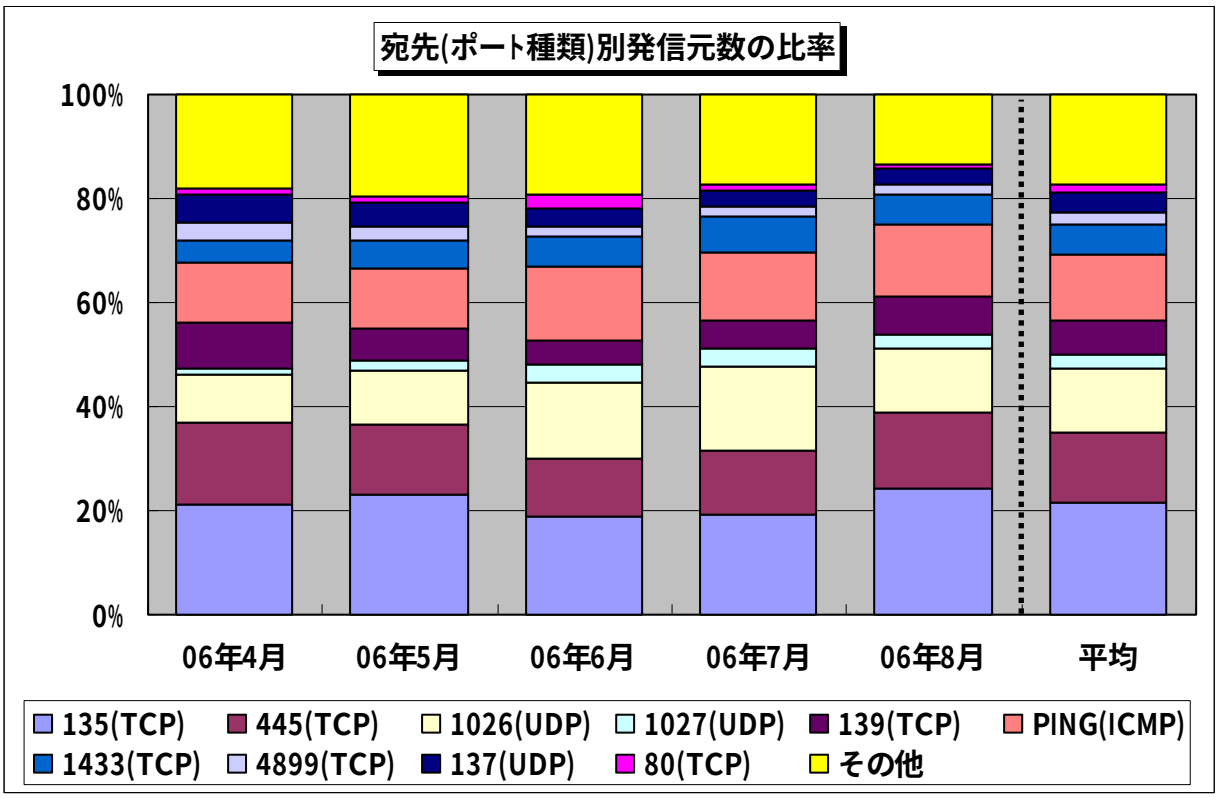
3．統計情報

3.1 2006 年 4 月～2006 年 8 月の宛先(ポート種類)別の比率

2006 年 4 月～2006 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。



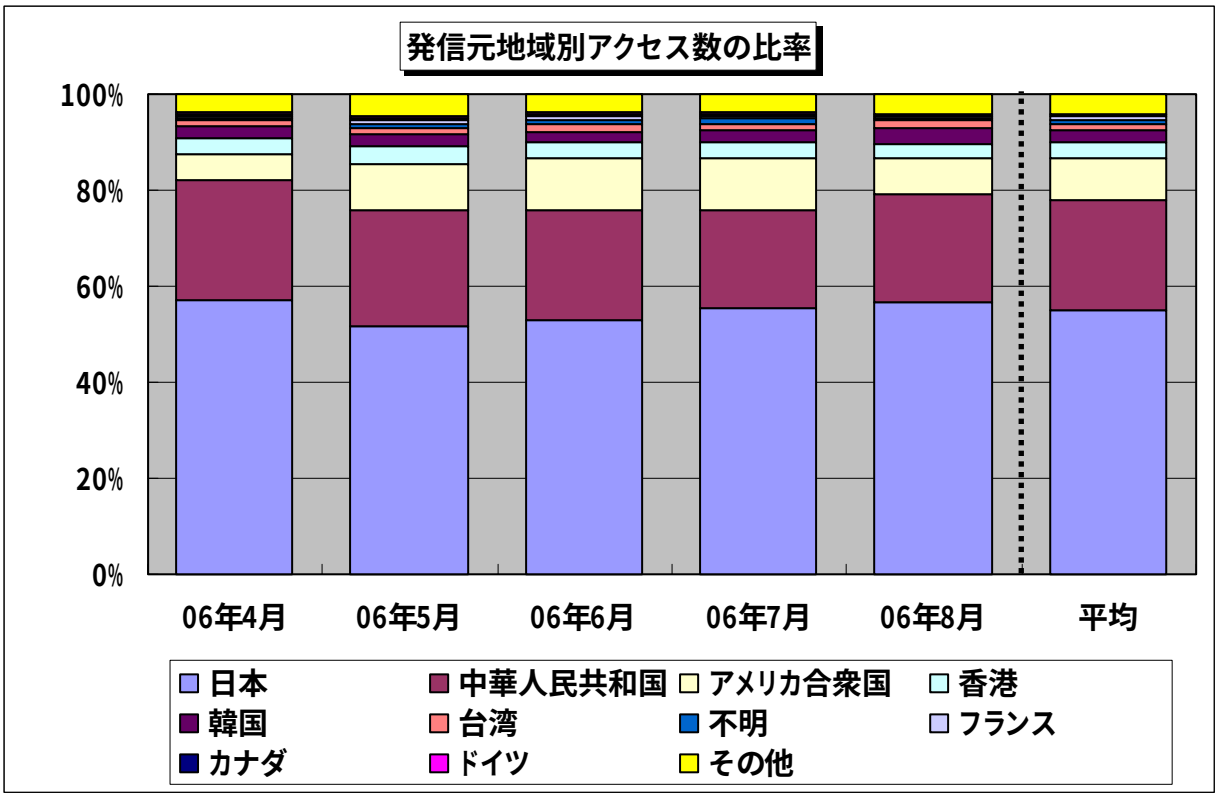
【図 3.1.1 2006 年 4 月～2006 年 8 月の宛先(ポート種類)別アクセス数の比率】



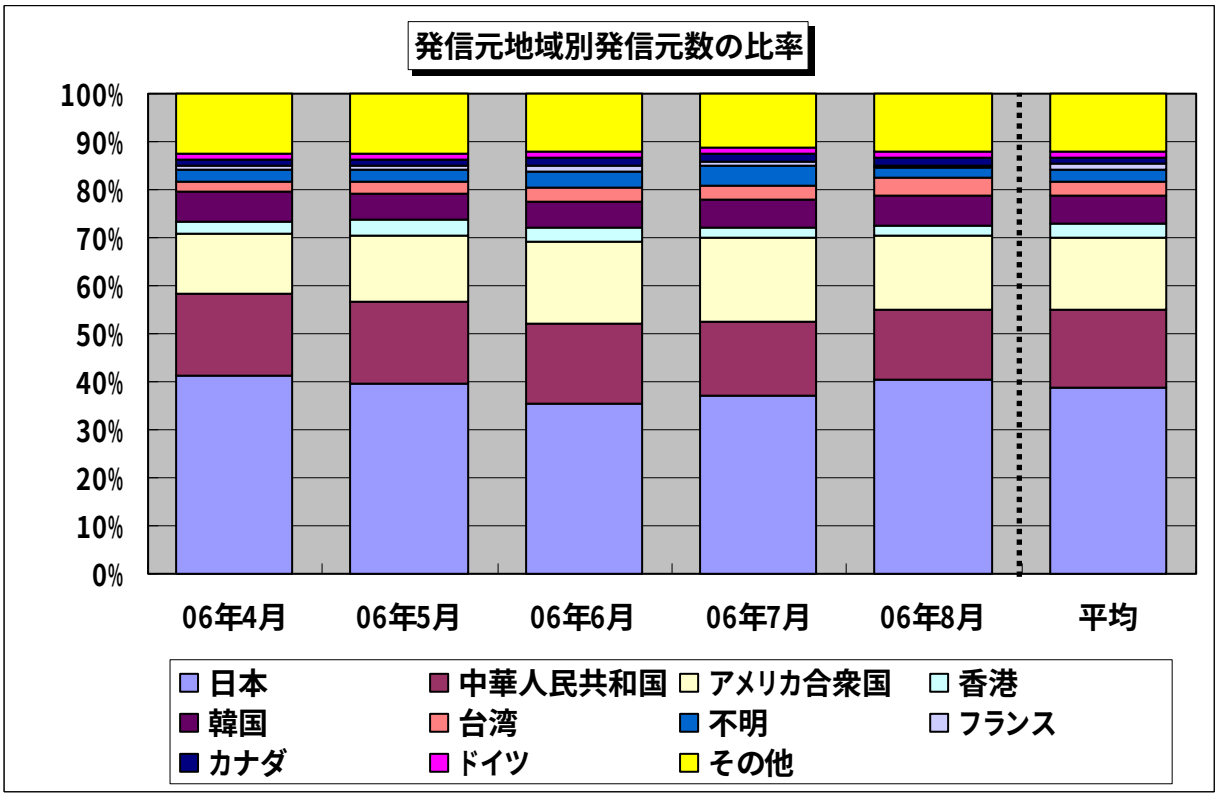
【図 3.1.2 2006 年 4 月～2006 年 8 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 4 月～2006 年 8 月の発信元地域別の比率

2006 年 4 月～2006 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 2006 年 4 月～2006 年 8 月の発信元地域別アクセス数の比率】



【図 3.2.2 2006 年 4 月～2006 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、2006 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)
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
4899(TCP)	リモート操作を行うための RAdmin のぜい弱性を狙った不正アクセスが有名(RAdmin は複数のコンピュータを遠隔操作するためのアプリケーション)
137(UDP)	NETBIOS のポートであり、NETBIOS 経由でのコンピュータへの接続(侵入)などの目的で使用されます
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

■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／内山
Tel:03-5978-7527 Fax:03-5978-7518
E-mail:isec-info@ipa.go.jp