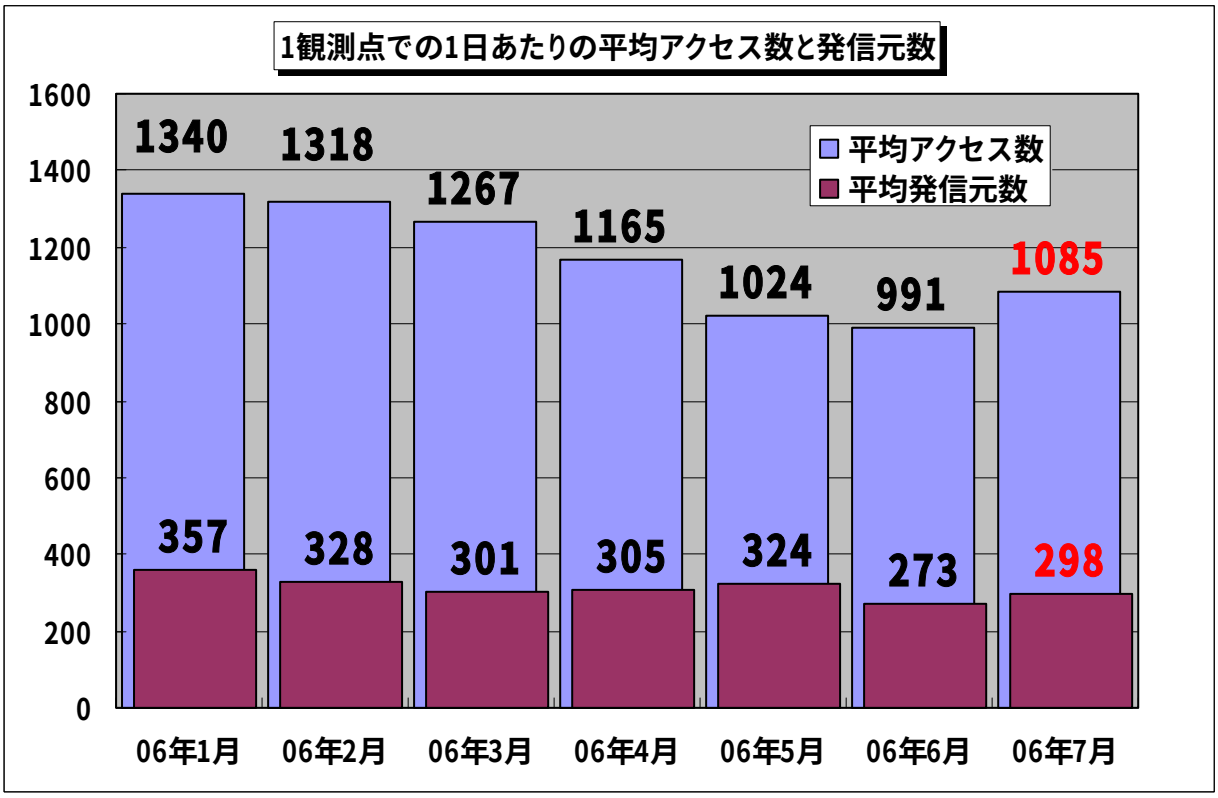
別紙 3

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 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 **336,361 件**ありました。1 観測点で 1 日あたり **298** の発信元から **1,085 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、298 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 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 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、先月より微増しました**。アクセス内容については、定常化(後述の統計情報を参照下さい)していると言えます。

2．7 月のアクセス状況

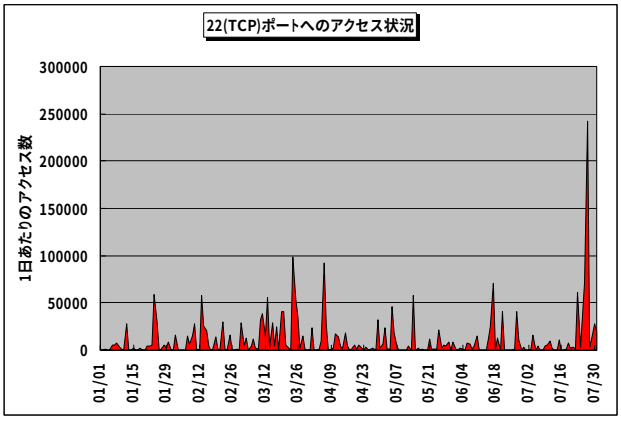
7月のアクセス状況は、6 月とほぼ同じ状況です。Windows のぜい弱性を狙っていると思われる不正なアクセスが多いようで、これらのアクセスの多くは、ボットに感染したコンピュータから送信されていると思われます。また、月末にかけて、これらのアクセス(数)が増加傾向なので、注意が必要です。

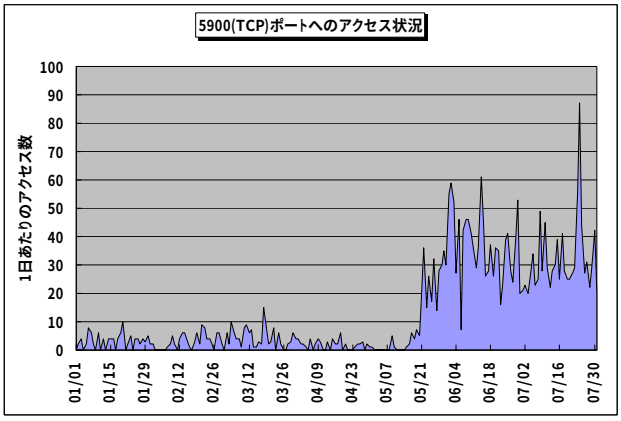
特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows のぜい弱性を狙っています。また、Windows Messenger サービスを悪用したポップアップスパムメッセージの 1026(UDP)/1027(UDP)ポートへのアクセスは、継続しています。

また、6 月分の詳細資料で特集を行った、ネットワークからの 22(TCP)ポートを狙ったパスワードクラッキング攻撃(*1)や、リモートアクセスツール RealVNC のぜい弱性(*2)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、継続的に発生しています。どちらのアクセスも、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。

特に、7 月の 22(TCP)ポートを狙ったパスワードクラッキング攻撃は、TALOT2 観測での記録的な数値を示しました。月後半の 3 日間に以下に示すアクセスがあり、ほとんど DoS 攻撃を受けているような状況でした。

- 発信元がアメリカ方面、10 時間のあいだに 242,511 回のアクセス→ 6.7 回/秒
- 発信元が韓国方面、4 時間半のあいだに 63,098 回のアクセス→ 3.9 回/秒
- 発信元がアメリカ方面、1 時間 45 分のあいだに 33,959 回のアクセス→ 5.4 回/秒





(*1) 22(TCP)ポートを狙ったパスワードクラッキング攻撃

ログイン ID やパスワードを変更させながらログインを繰り返すことで、システムへの侵入を試みる、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 22(TCP)ポートへのアクセス。

TALOT2 では、SSH への攻撃の実情を調べるために、SSH を利用しています。この SSH の利用する 22(TCP)ポートに対するポートスキャンおよび実際のパスワードクラッキング攻撃が、他の不正なアクセスとともに観測することができます。

攻撃者は、開いている(応答のある)22(TCP)ポートを見つけると、ID やパスワードを変更させながら、ログイン操作を繰り返し実行します。

SSH を利用する観測点で観測されたパスワードクラッキング目的のアクセスについては、特定観測点への攻撃であることから、本レポート内の観測データから除外してありますので、ご注意下さい。

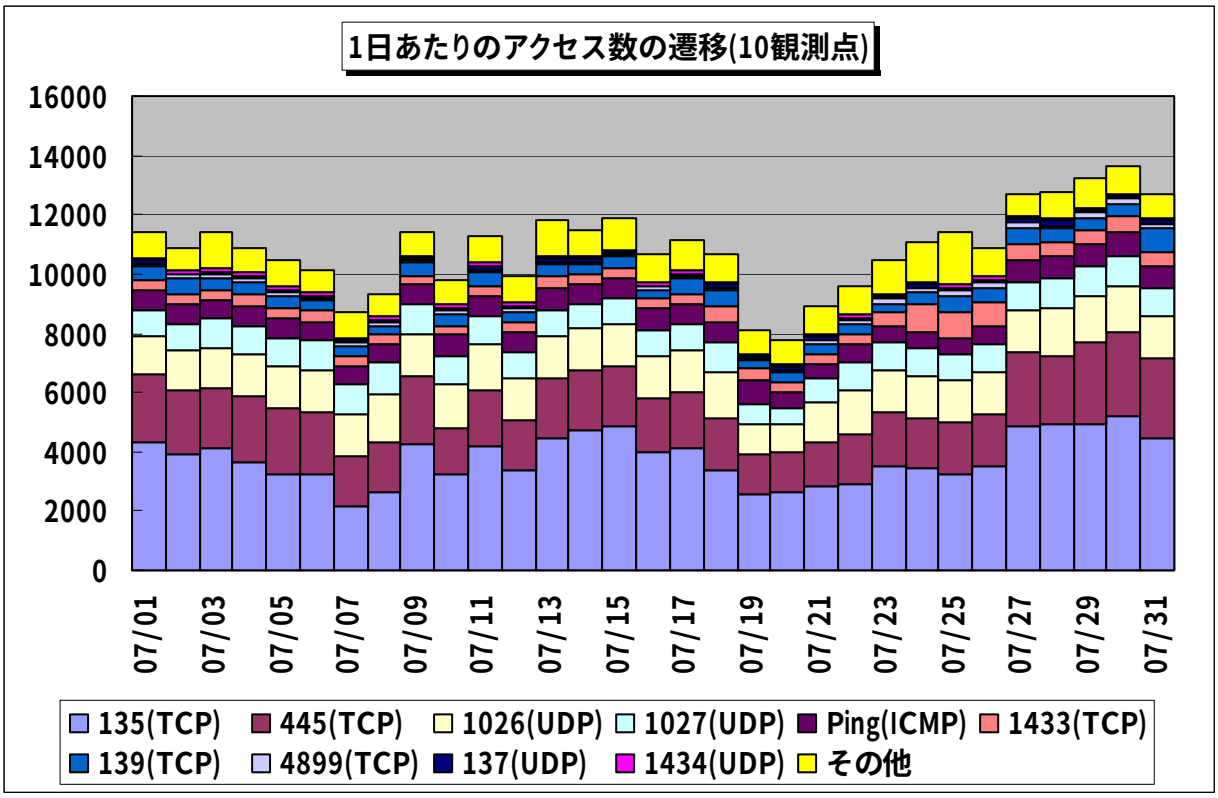
(*2) RealVNC のぜい弱性

遠隔操作ソフトである RealVNC Server には、クライアント認証の回避が可能な脆弱性が存在します。以下のサイトを参照下さい。

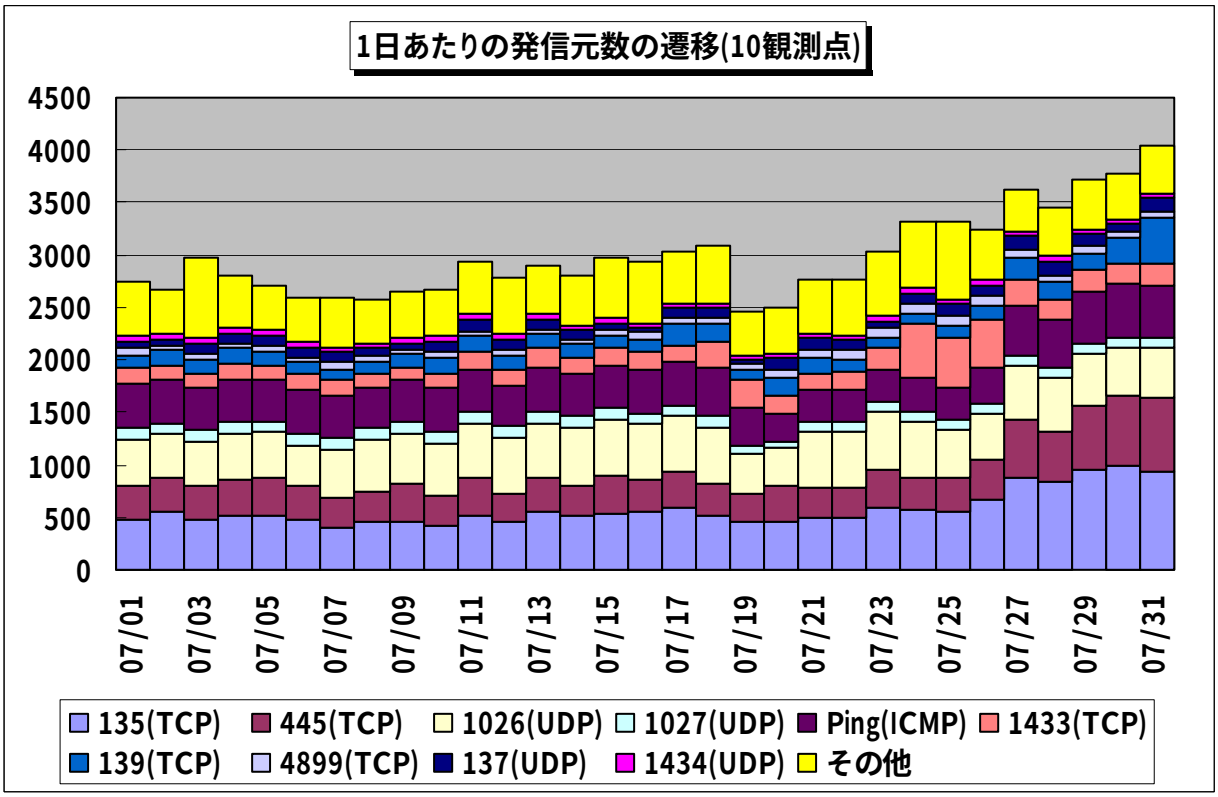
■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/index.html

2.1 2006 年 7 月の一方的なアクセス状況

2006 年 7 月の一方的なアクセス状況（アクセス数）の遷移を図 2.1.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.1.2 に示します。



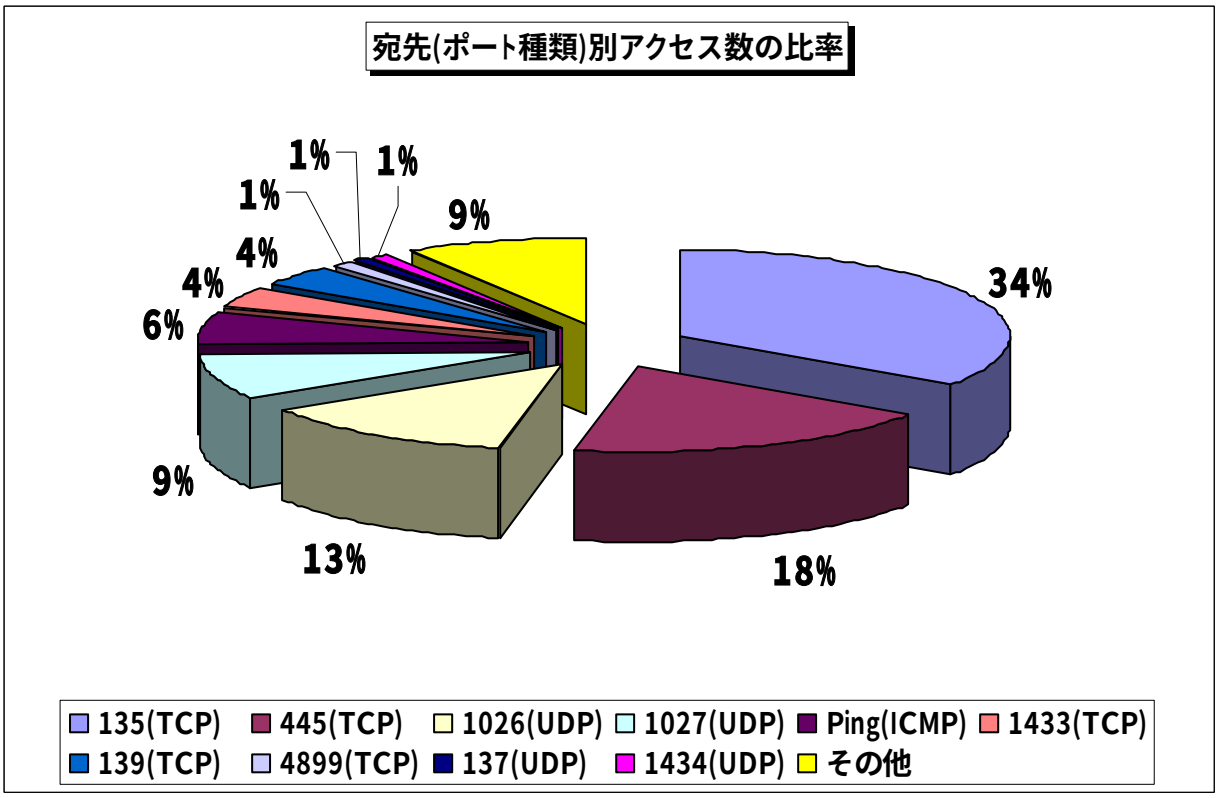
【図 2.1.1 2006 年 7 月の一方的なアクセス状況(アクセス数)】



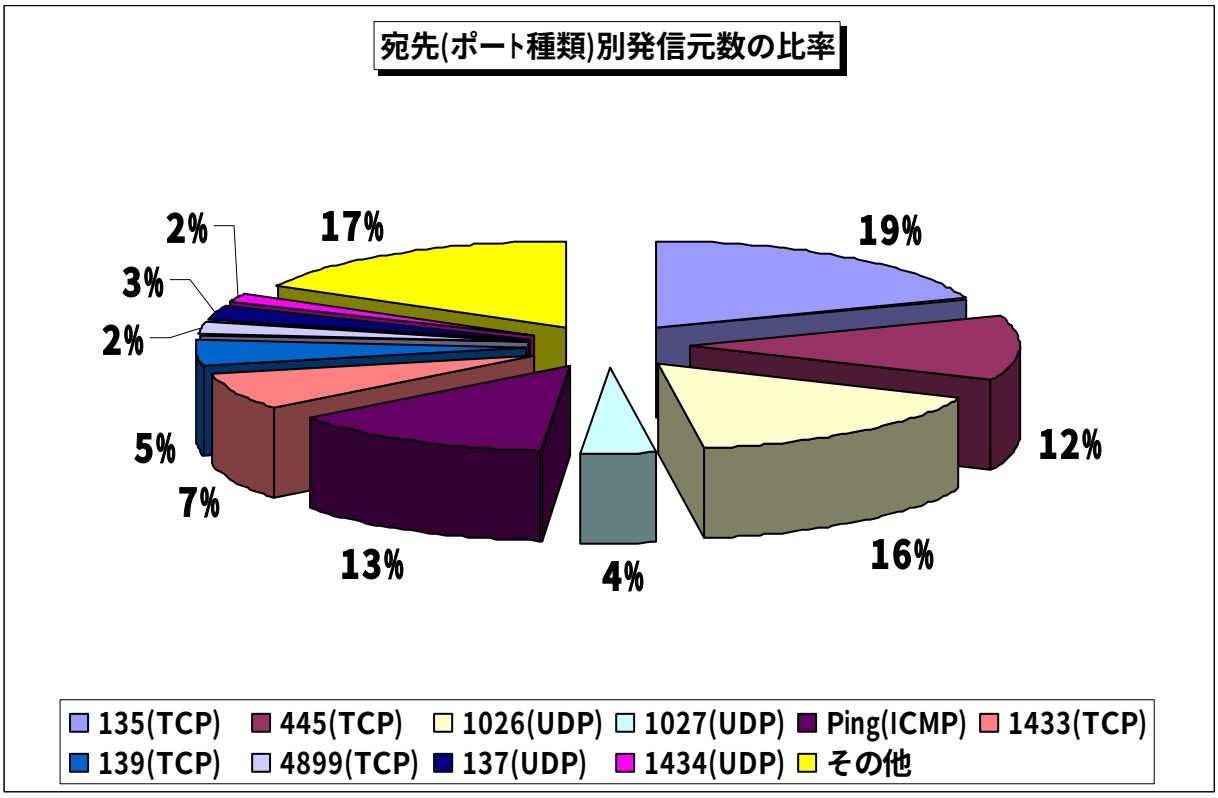
【図 2.1.2 2006 年 7 月の一方的なアクセス状況(発信元数)】

2.2 2006 年 7 月の宛先(ポート種類)別の比率

2006 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 2.2.1 に、宛先(ポート種類)別発信元数の比率を図 2.2.2 に示します。



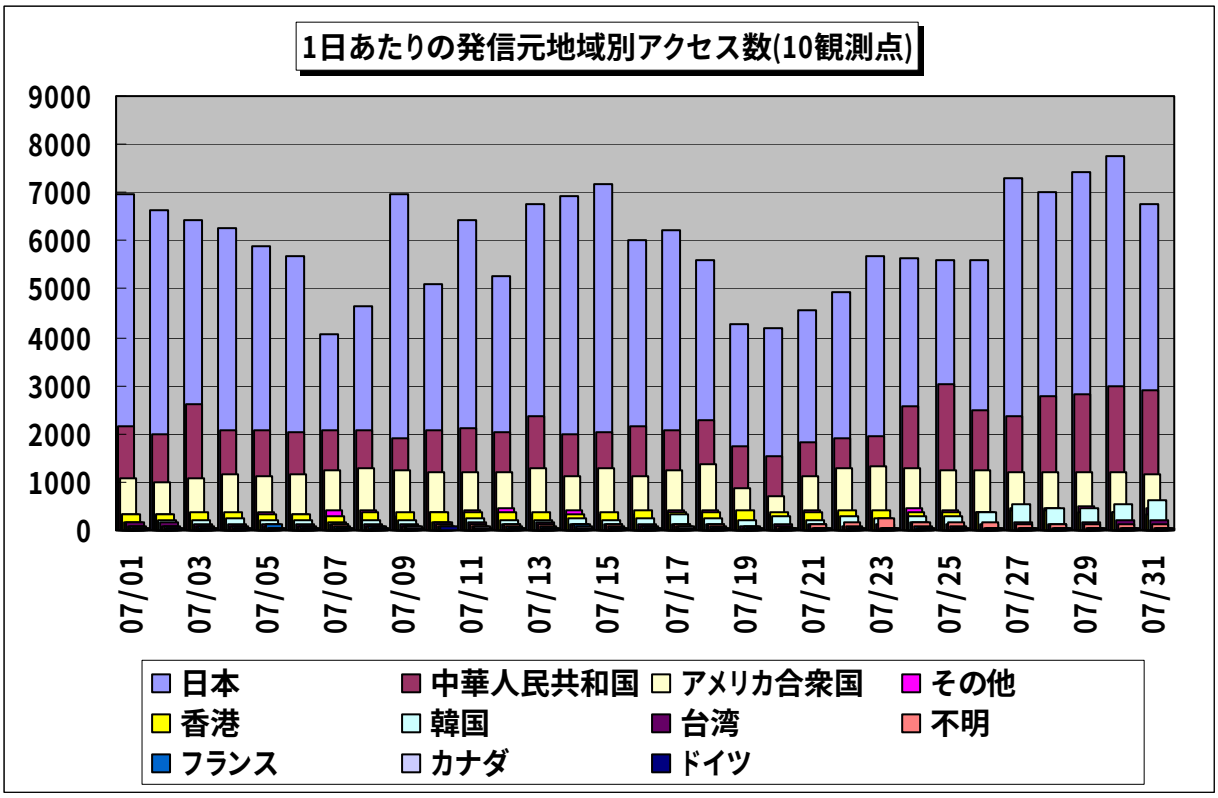
【図 2.2.1 2006 年 7 月の宛先(ポート種類)別アクセス数の比率】



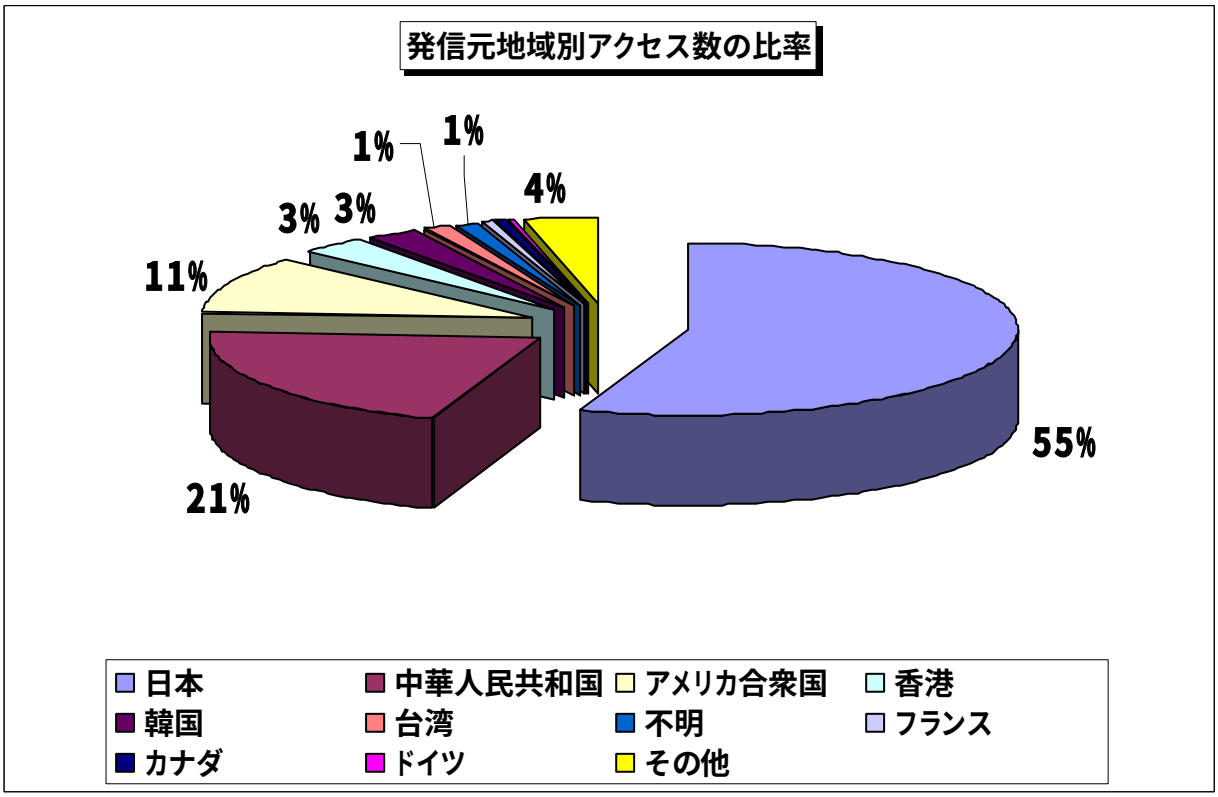
【図 2.2.2 2006 年 7 月の宛先(ポート種類)別発信元数の比率】

2.3 2006 年 7 月の発信元地域別アクセス状況

2006 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 2.3.1 に、発信元地域別アクセス数の比率を図 2.3.2 に示します。

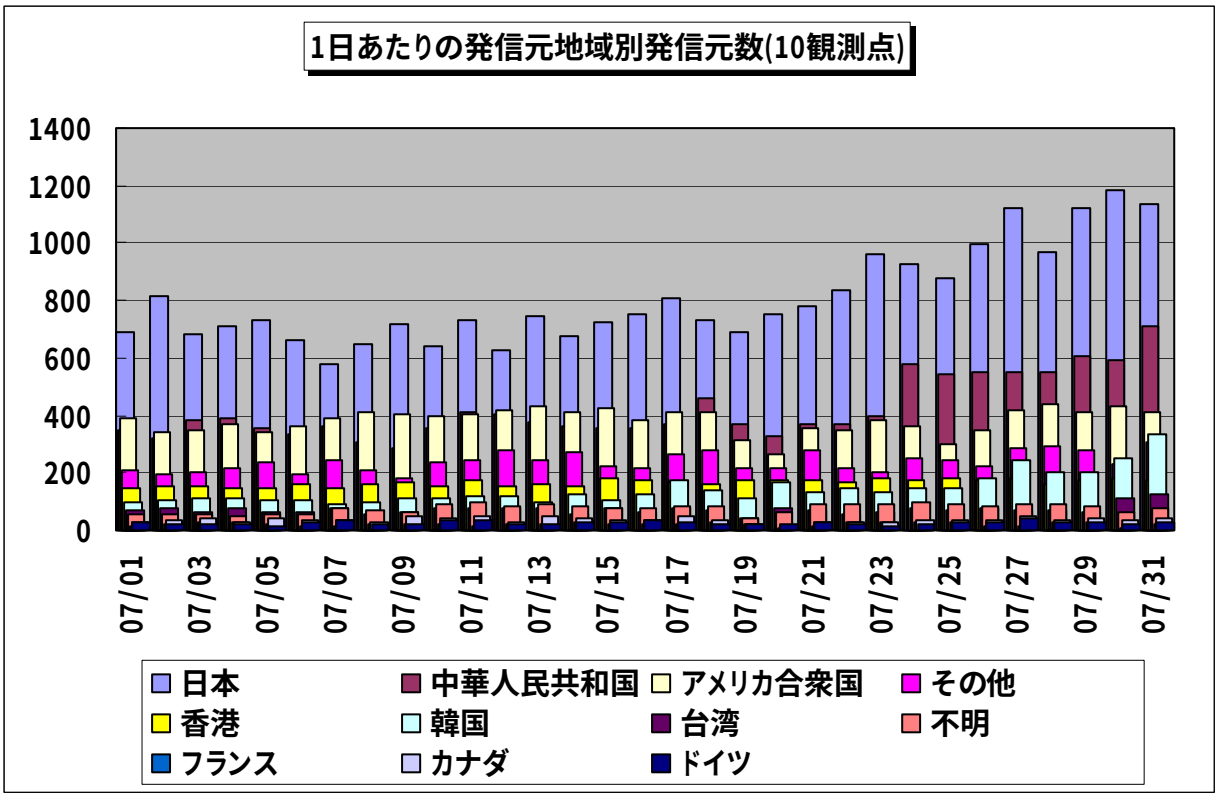


【図 2.3.1 2006 年 7 月の発信元地域別アクセス数の変化】

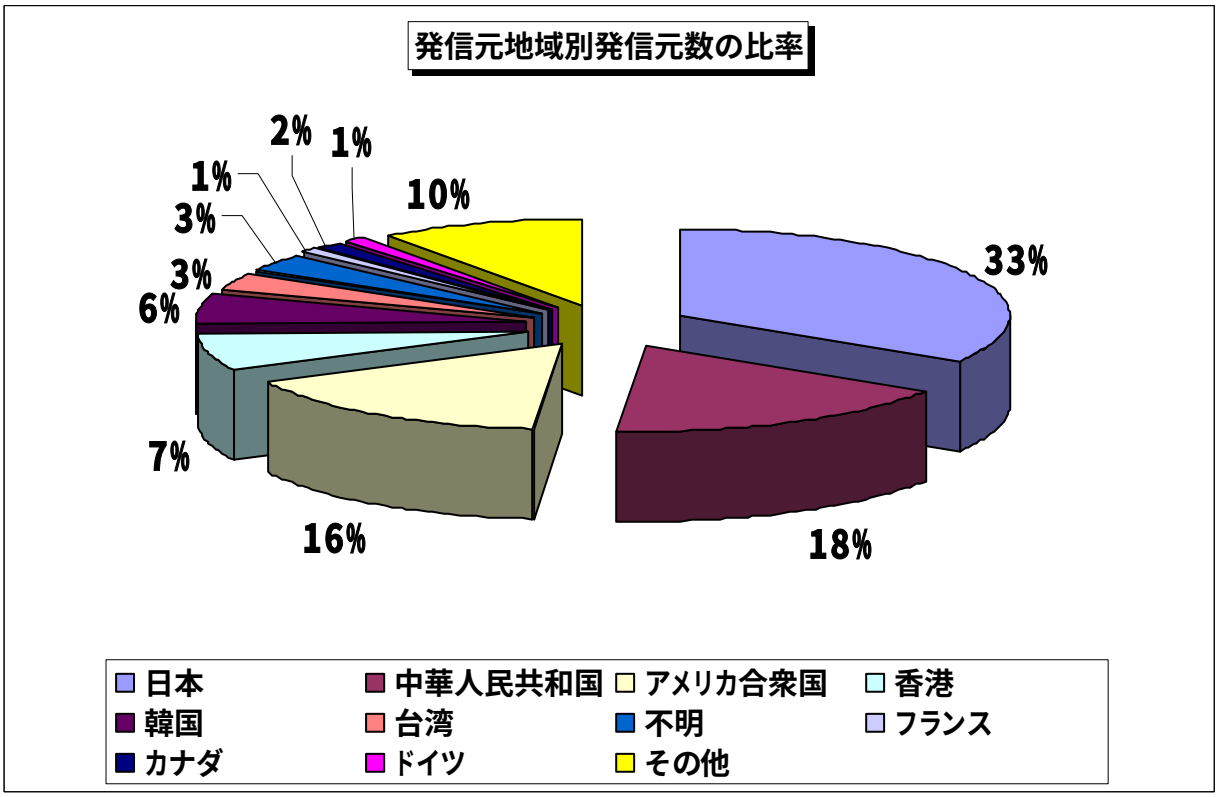


【図 2.3.2 2006 年 7 月の発信元地域別アクセス数の比率】

2006 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 2.3.3 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 2.3.3 2006 年 7 月の発信元地域別発信元数の変化】

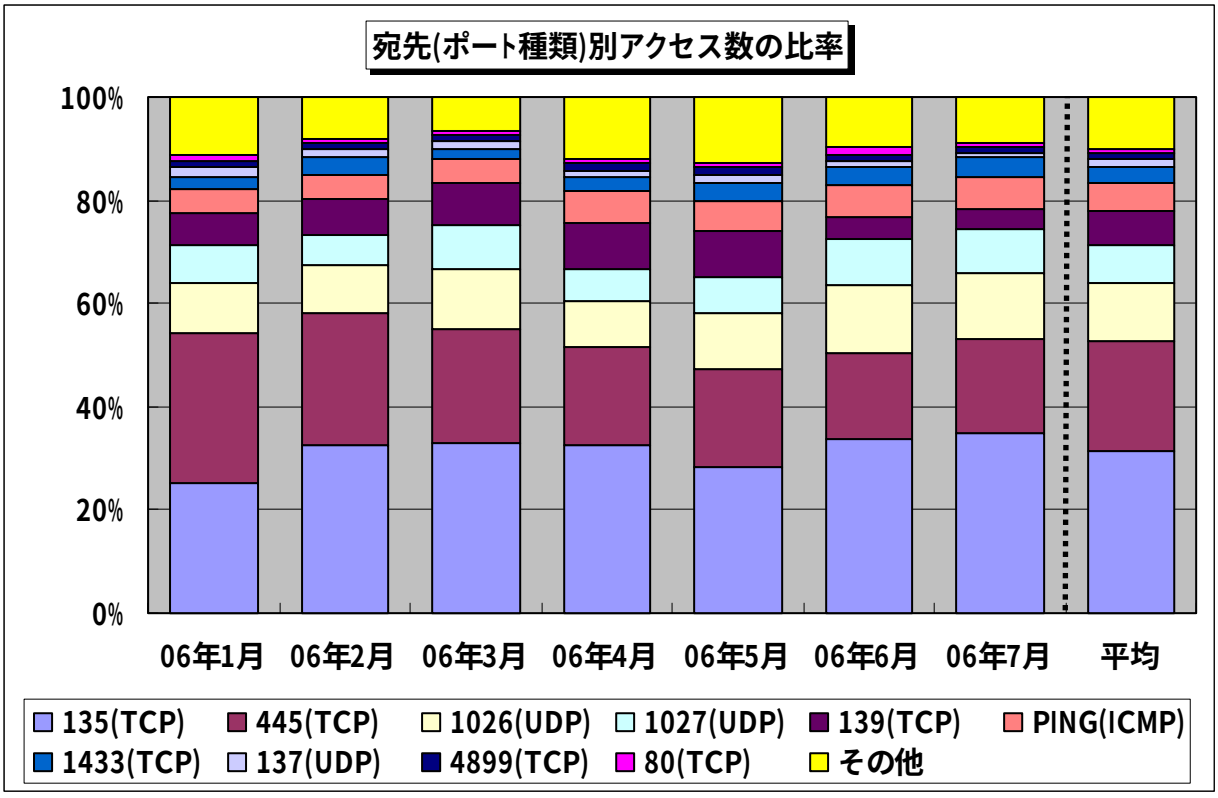


【図 2.3.4 2006 年 7 月の発信元地域別発信元数の比率】

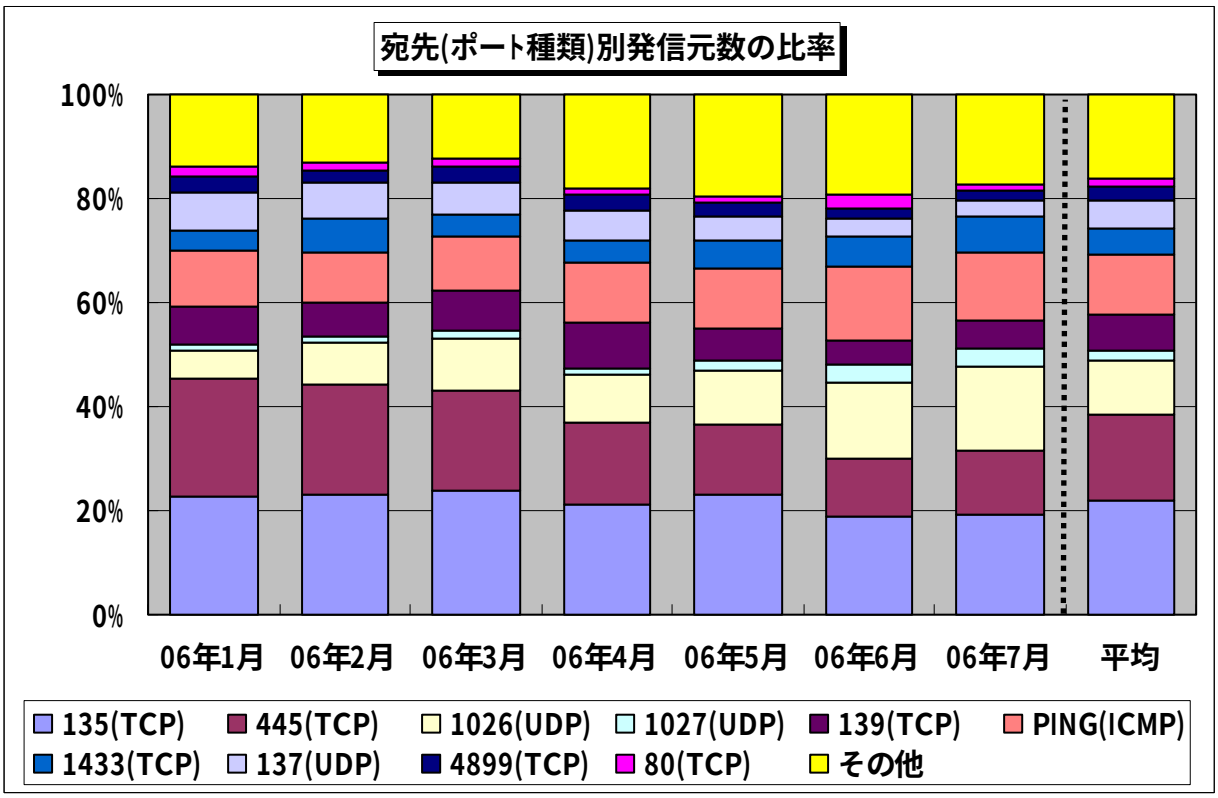
3．統計情報

3.1 2006 年 1 月～2006 年 7 月の宛先(ポート種類)別の比率

2006 年 1 月～2006 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。



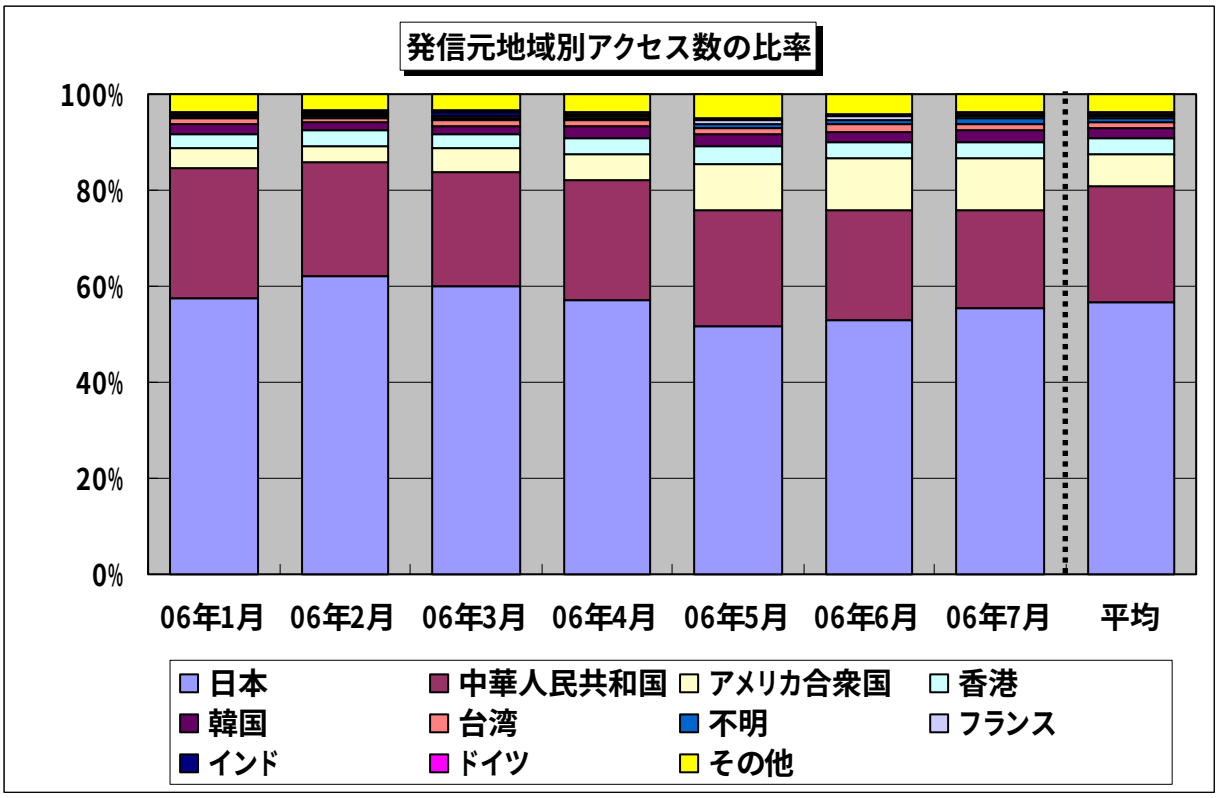
【図 3.1.1 2006 年 1 月～2006 年 7 月の宛先(ポート種類)別アクセス数の比率】



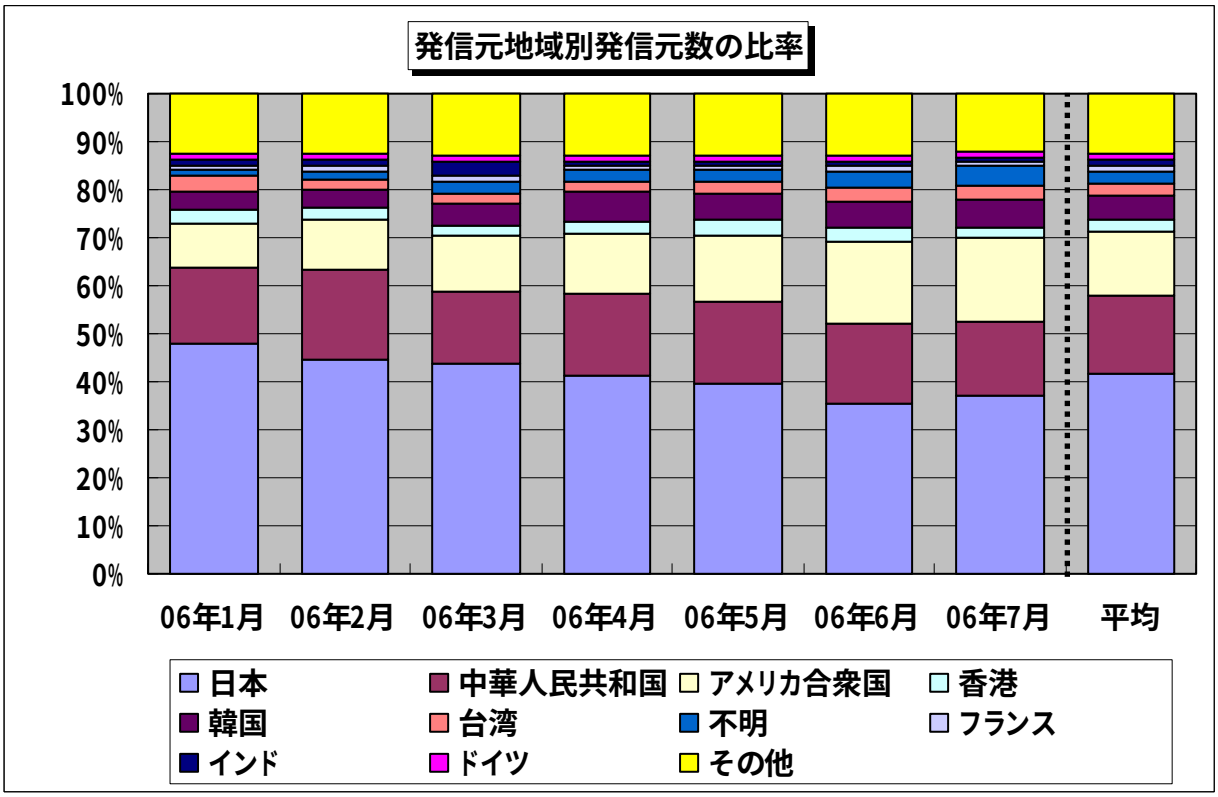
【図 3.1.2 2006 年 1 月～2006 年 7 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 1 月～2006 年 7 月の発信元地域別の比率

2006 年 1 月～2006 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 2006 年 1 月～2006 年 7 月の発信元地域別アクセス数の比率】



【図 3.2.2 2006 年 1 月～2006 年 7 月の発信元地域別発信元数の比率】

5．補足説明

以下に、2006 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
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)
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)
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

■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