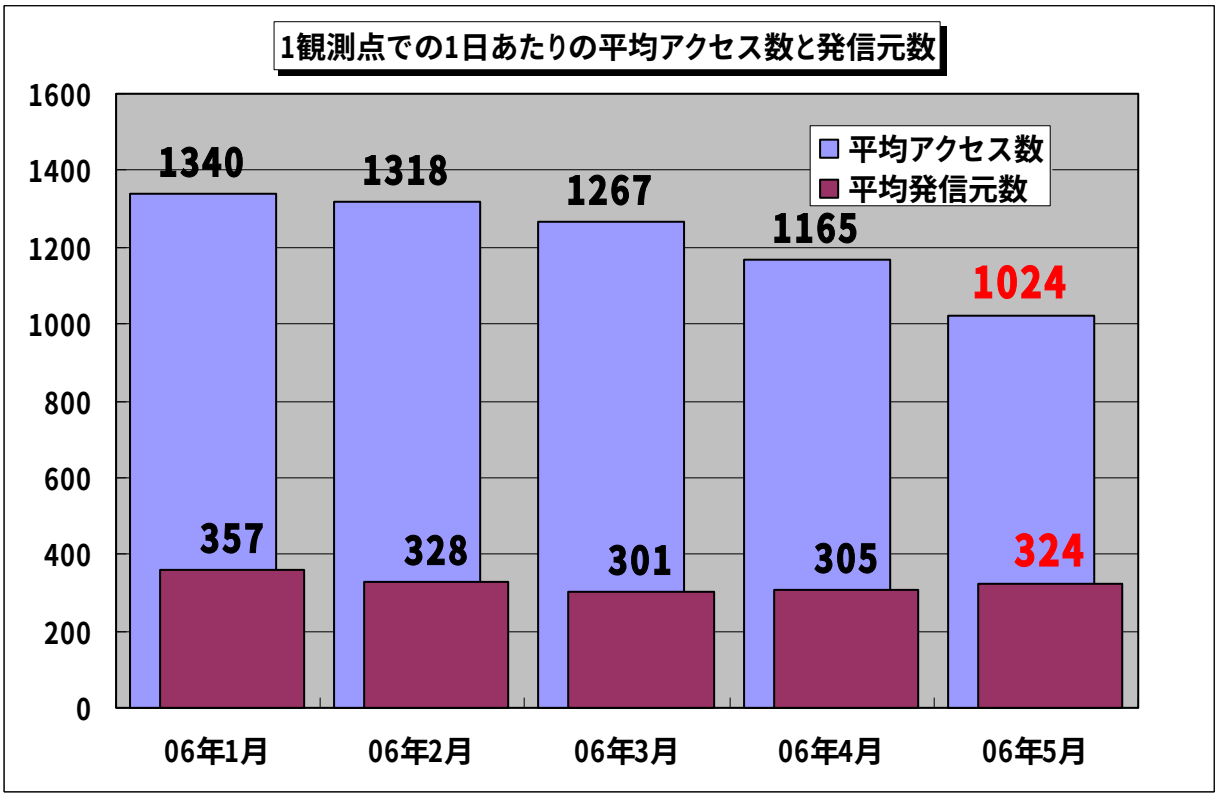
別紙 3

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 5 月の期待しない（一方的な）アクセスの総数は、10 観測点で **317,490 件**ありました。1 観測点で 1 日あたり **324** の発信元から **1024 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、324 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 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 5 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、緩やかに減少傾向にあるようです**。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。

2．5月のアクセス状況

5月のアクセス状況は、4月とほぼ同じ状況です。Windowsの脆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。

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 の脆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。

2.1 2006年5月の特記事項

今月、特徴的であったアクセスは以下の通りです。

・ 5900(TCP)ポートへのアクセス

2.1.1 5900(TCP)ポートへのアクセス

5900(TCP)ポートへのアクセスは、TALOT2 への全体のアクセスからすると、目立たない程度のものですが、脆弱性を狙ったアクセスである可能性があると言うことで、特徴的なアクセスであると思われます。

5900(TCP)ポートは、RealVNCクライアントがRealVNCサーバへ接続するときに使用するデフォルトのポートですが、RealVNC には以下に示す脆弱性が公表されています。

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

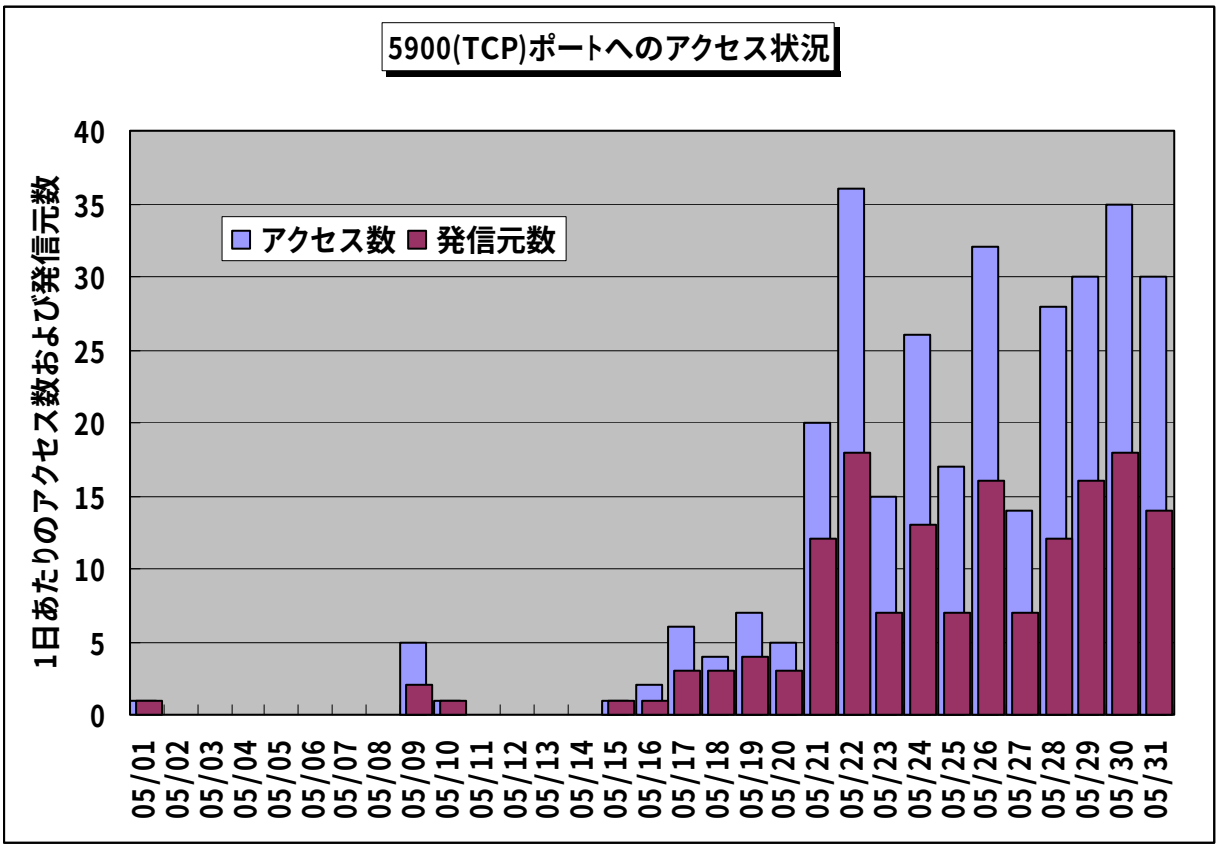
■ RealVNC サーバの認証が回避される脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060005.txt

資料にあるように、5 月 17 日の時点で、脆弱性を攻撃することが可能なコードが確認されており、今回のアクセスの増加は、この影響と予測されます。

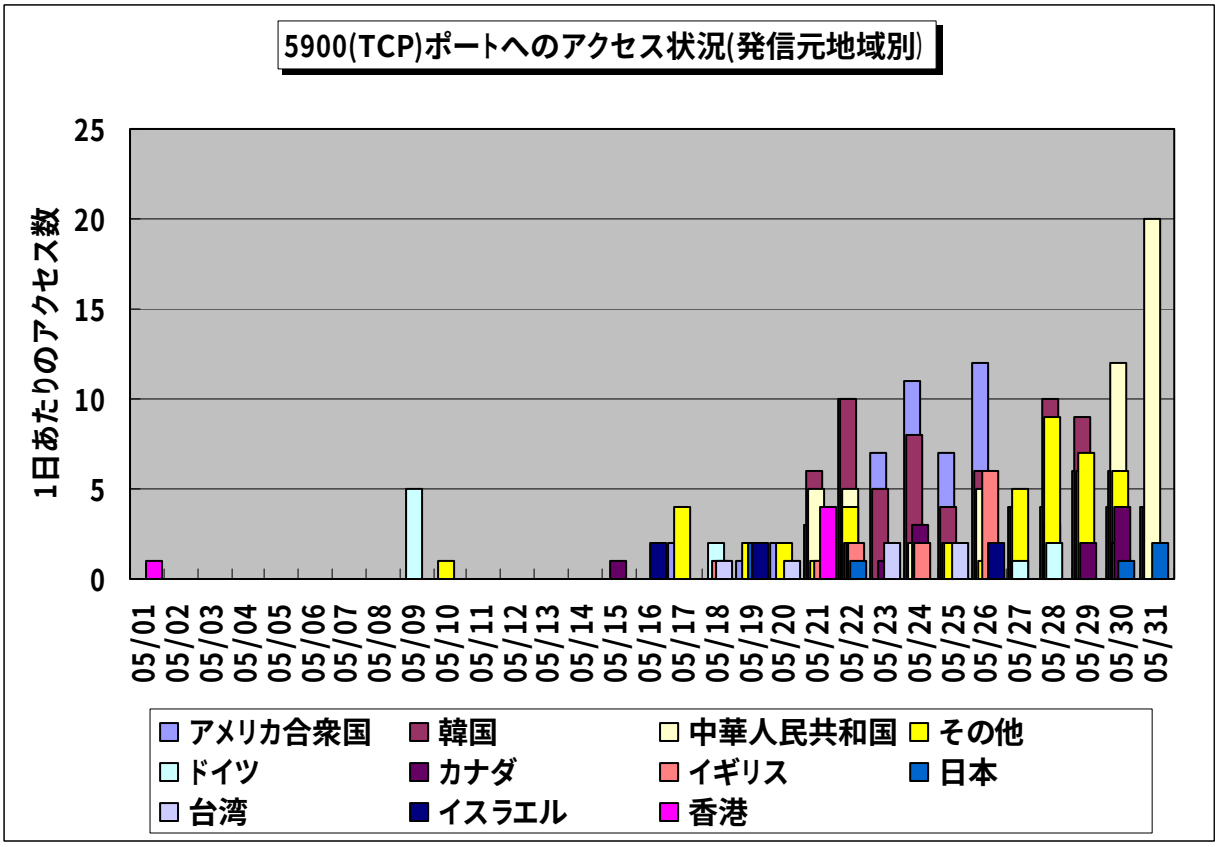
TALOT2では、各ポートへのアクセスに対して応答することはありません。したがって、これらのアクセス（ポートスキャン）が、実際の攻撃につながるものかは確認していません。

アクセスの増加は、5 月 17 日前後から増加しましたが、現在は一定のレベルで安定しています。発信元地域に関しては、アメリカ、韓国、中国方面が比較的多いようですが、5月9日のドイツ方面からのアクセスが少し気になるところです。

RealVNCでの運用を行っているシステムの管理者は、上記の情報を参考にし、早急に、脆弱性に対する対応を実施して下さい。



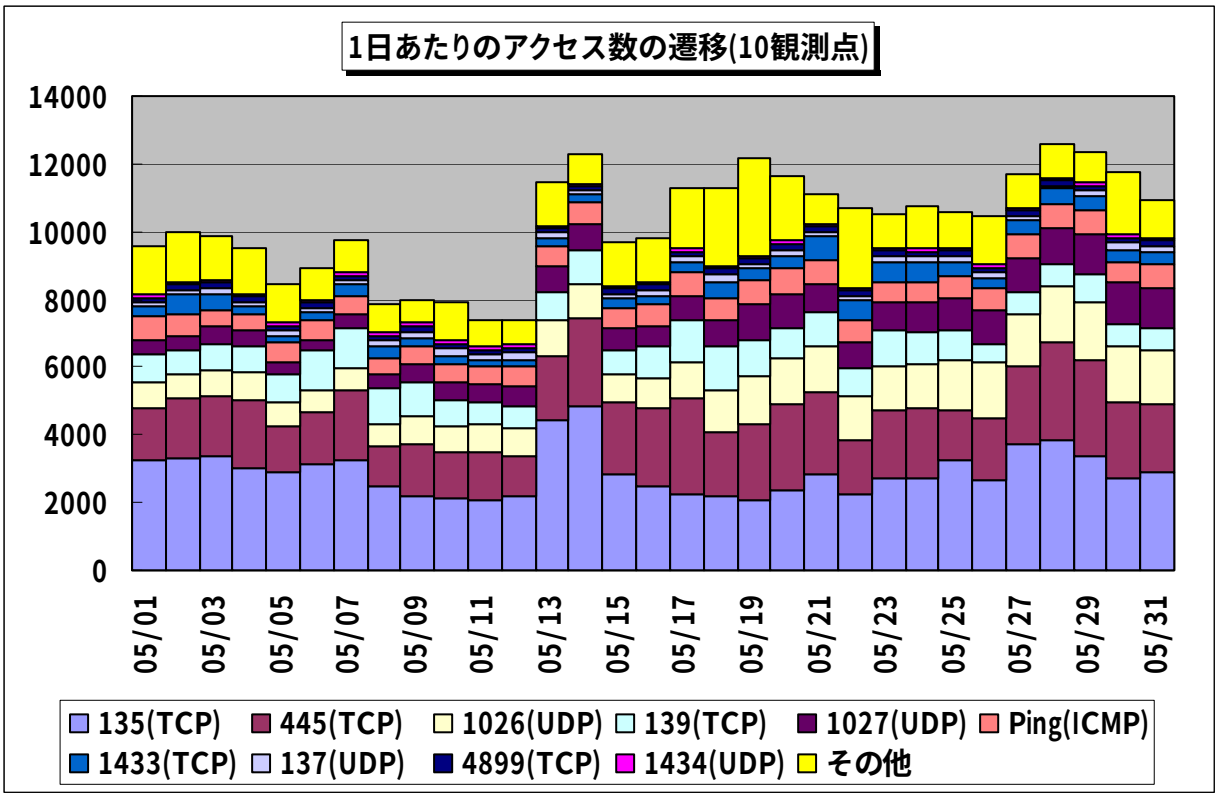
【図 2.1.1.1 2006 年 5 月の 5900(TCP)ポートへのアクセスの状況】



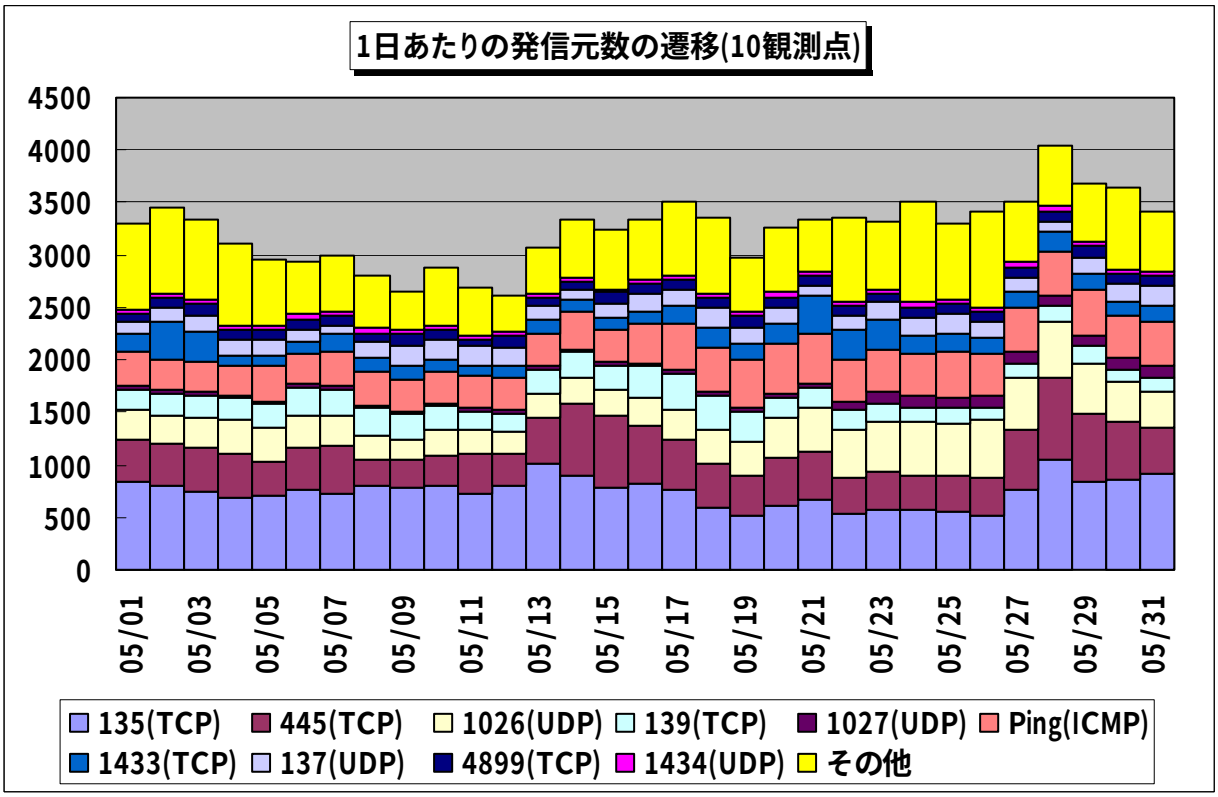
【図 2.1.1.2 2006 年 5 月の 5900(TCP)ポートへの発信元地域別アクセスの状況】

2.2 2006 年 5 月の一方的なアクセス状況

2006 年 5 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。



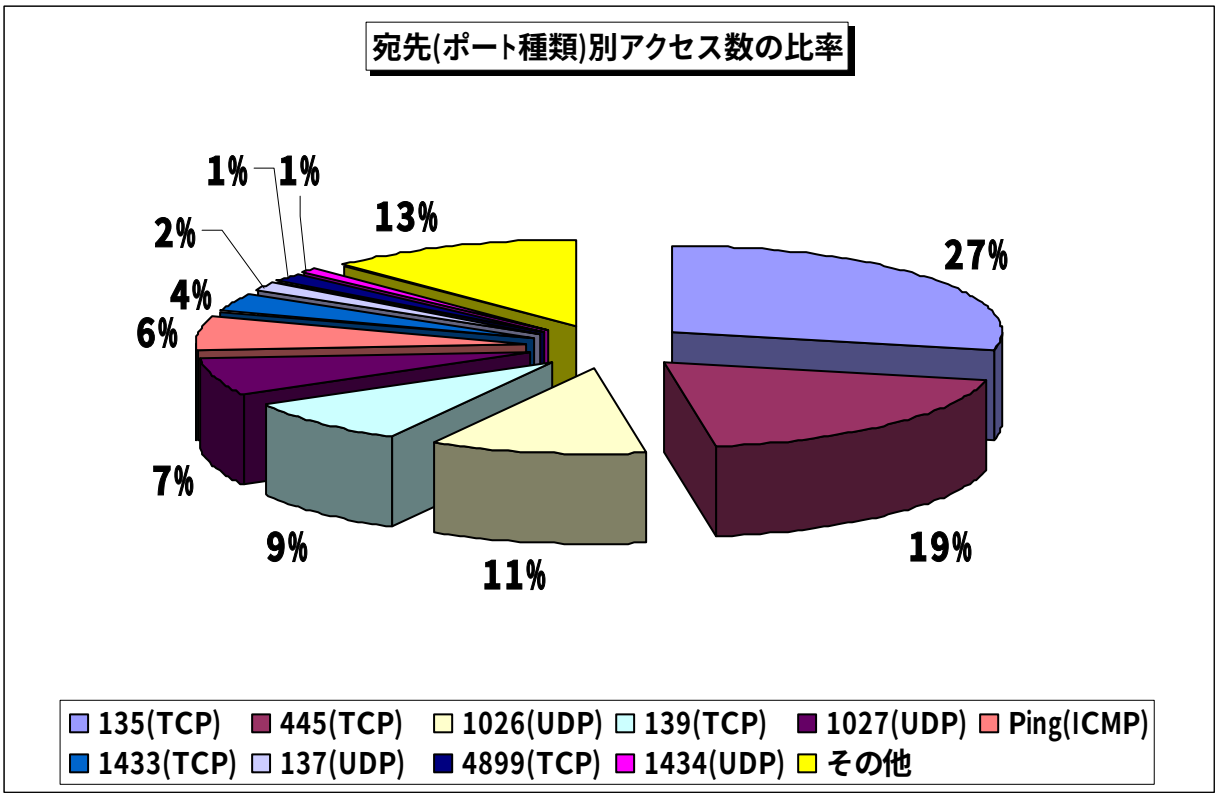
【図 2.2.1 2006 年 5 月の一方的なアクセス状況(アクセス数)】



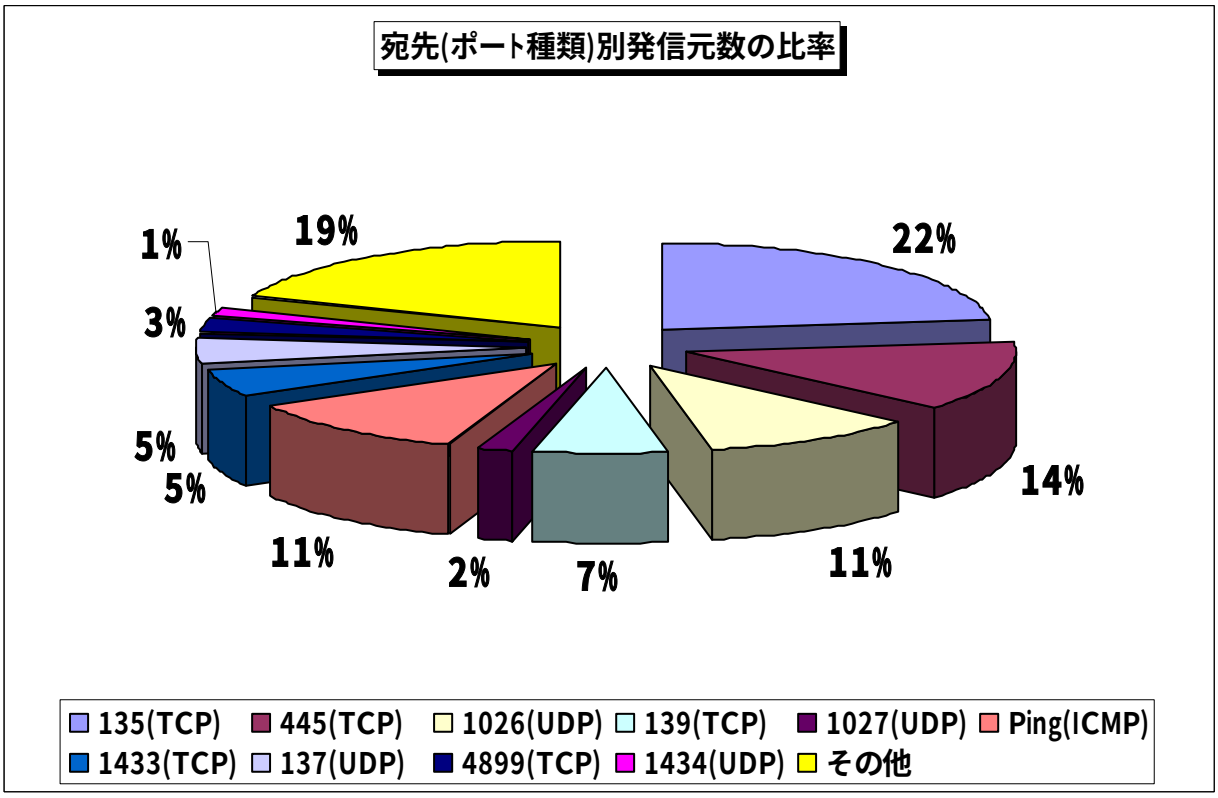
【図 2.2.2 2006 年 5 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 5 月の宛先(ポート種類)別の比率

2006 年 5 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。



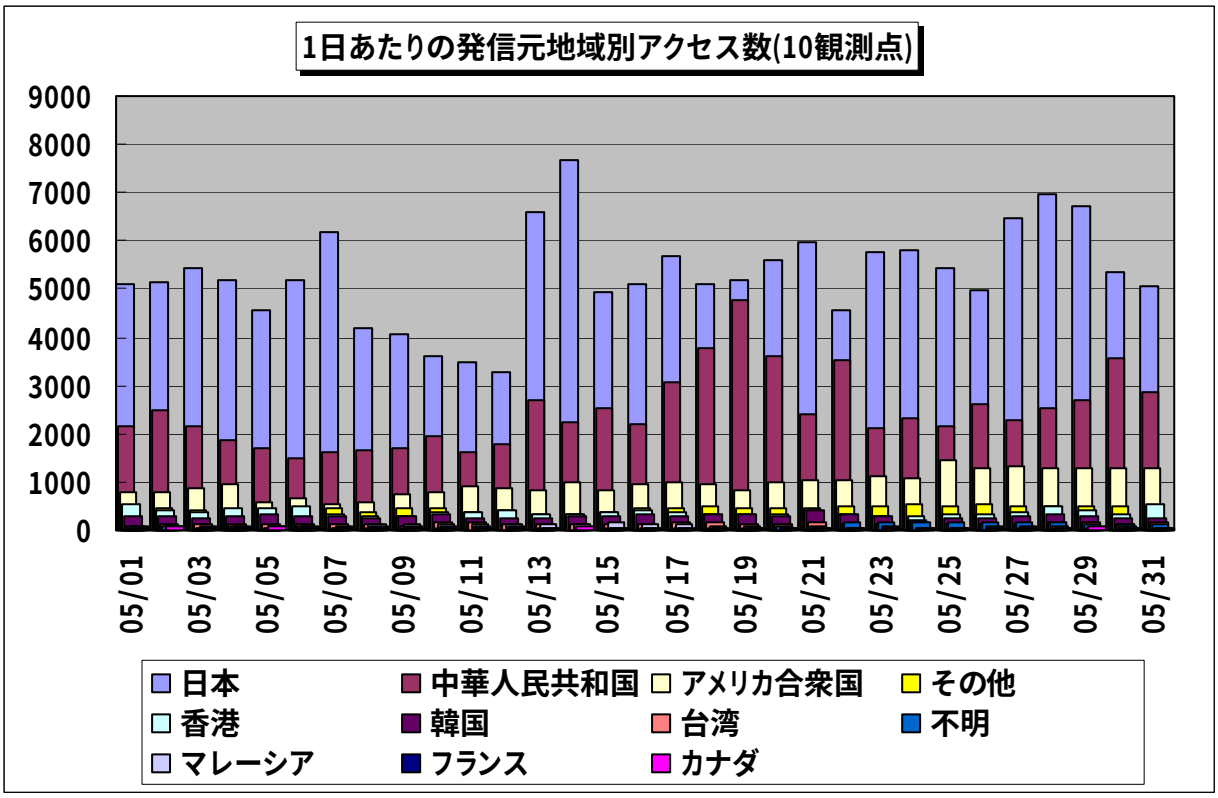
【図 2.3.1 2006 年 5 月の宛先(ポート種類)別アクセス数の比率】



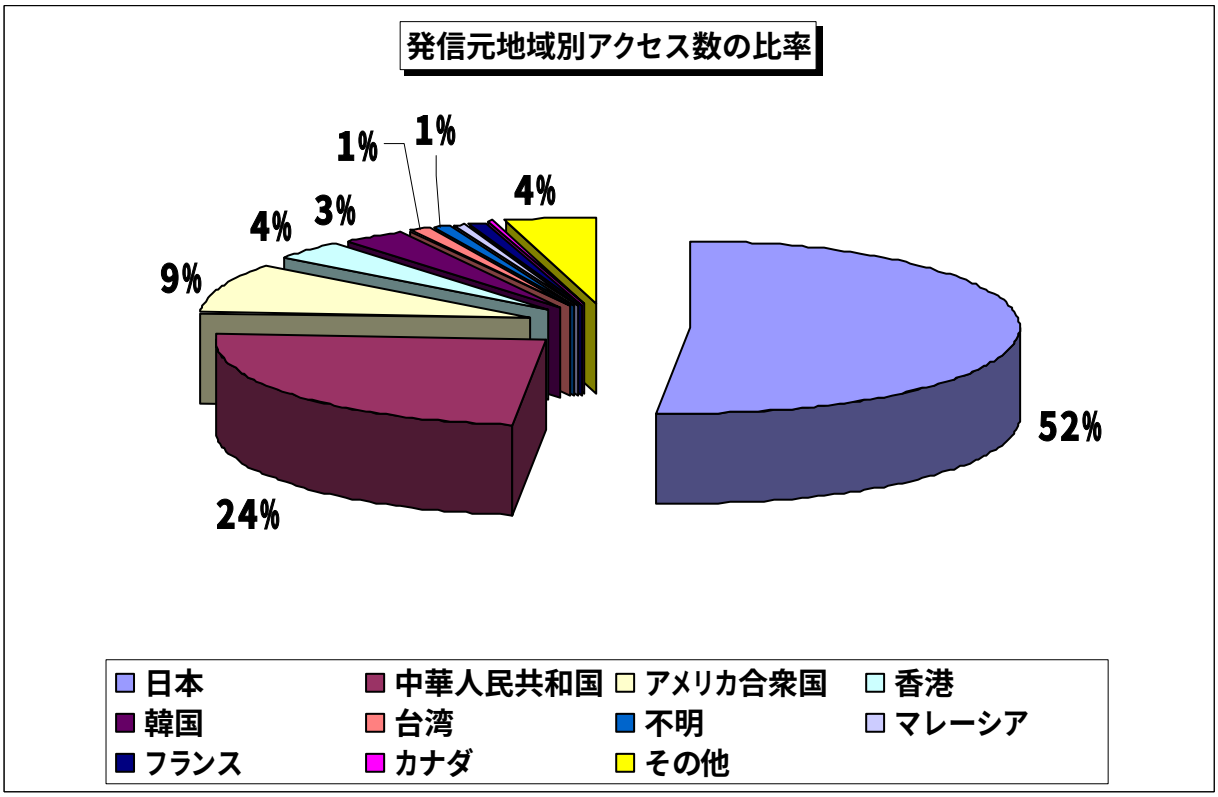
【図 2.3.2 2006 年 5 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 5 月の発信元地域別アクセス状況

2006 年 5 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。

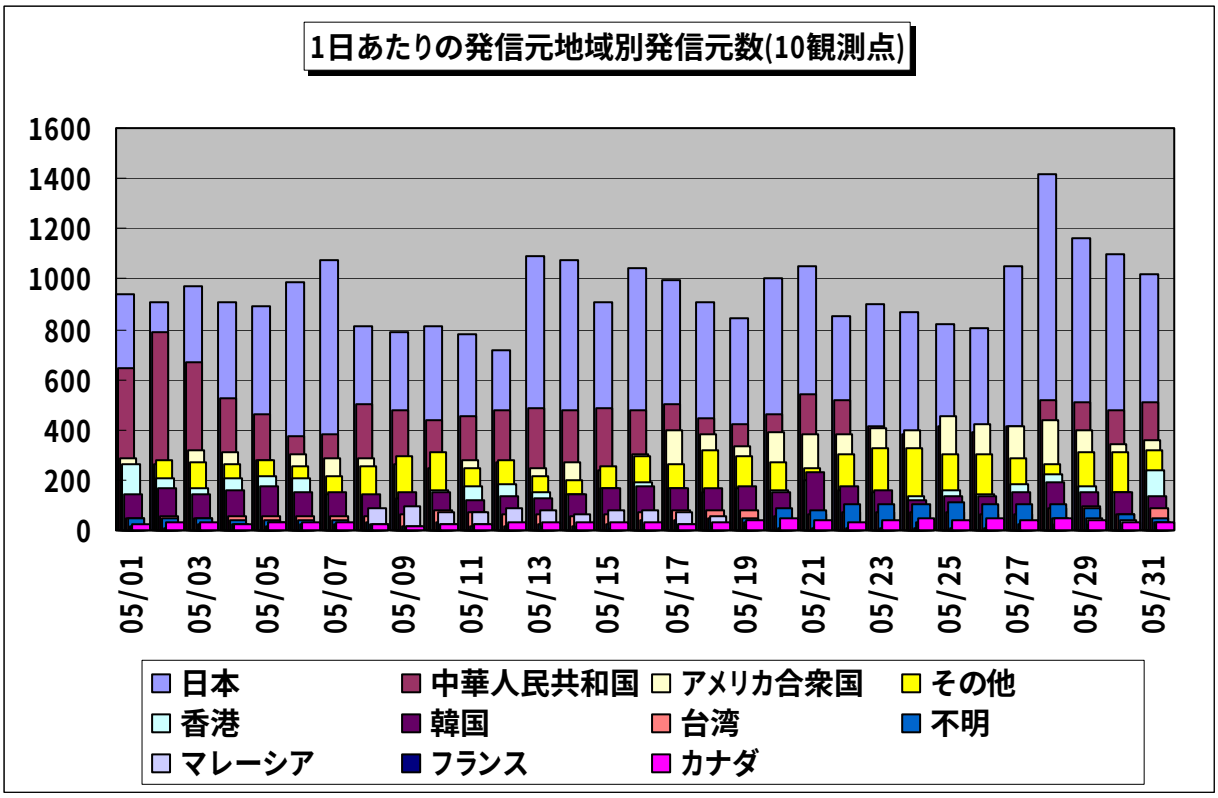


【図 2.4.1 2006 年 5 月の発信元地域別アクセス数の変化】

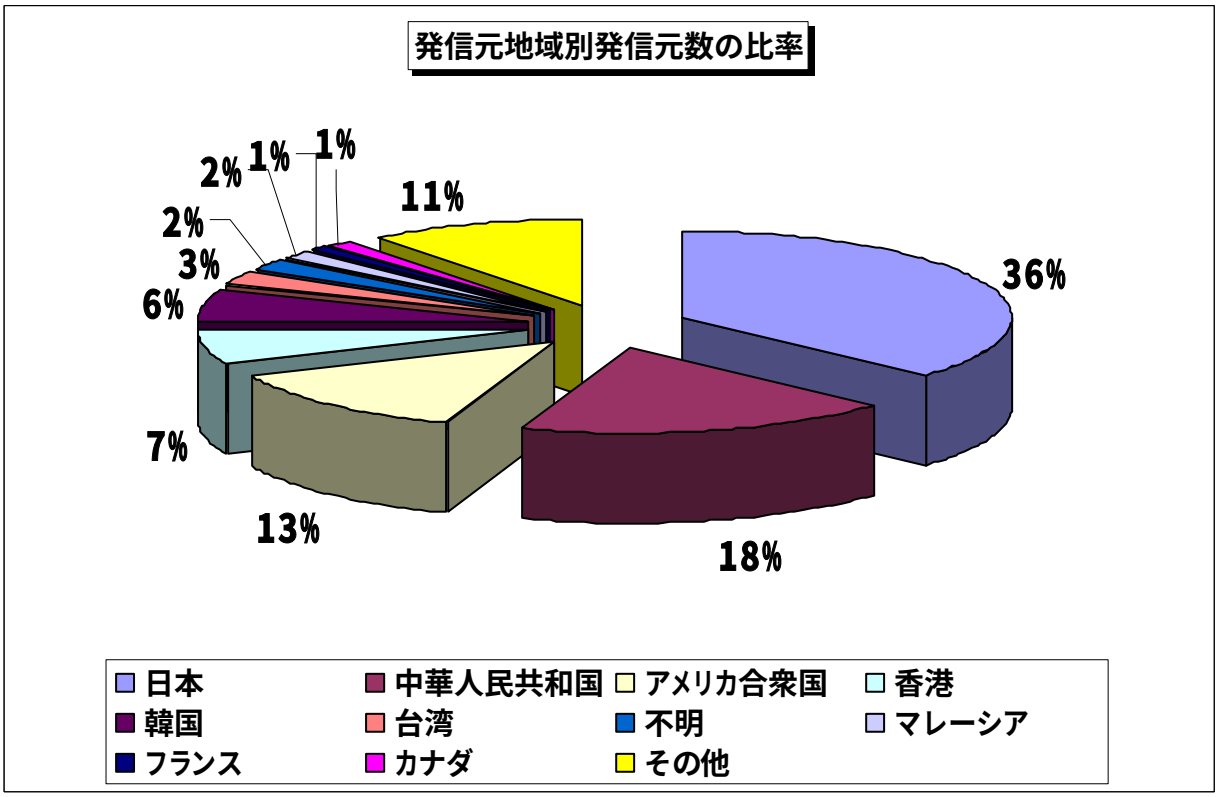


【図 2.4.2 2006 年 5 月の発信元地域別アクセス数の比率】

2006 年 5 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 2006 年 5 月の発信元地域別発信元数の変化】

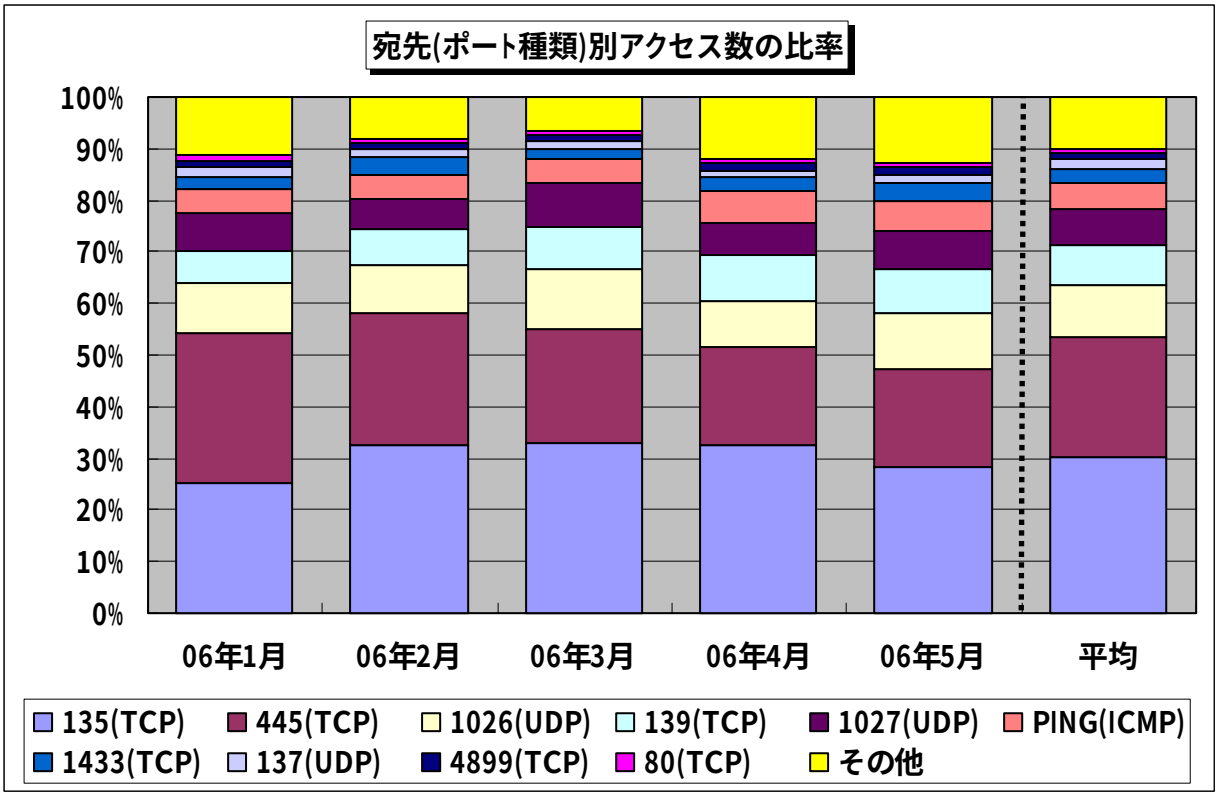


【図 2.4.4 2006 年 5 月の発信元地域別発信元数の比率】

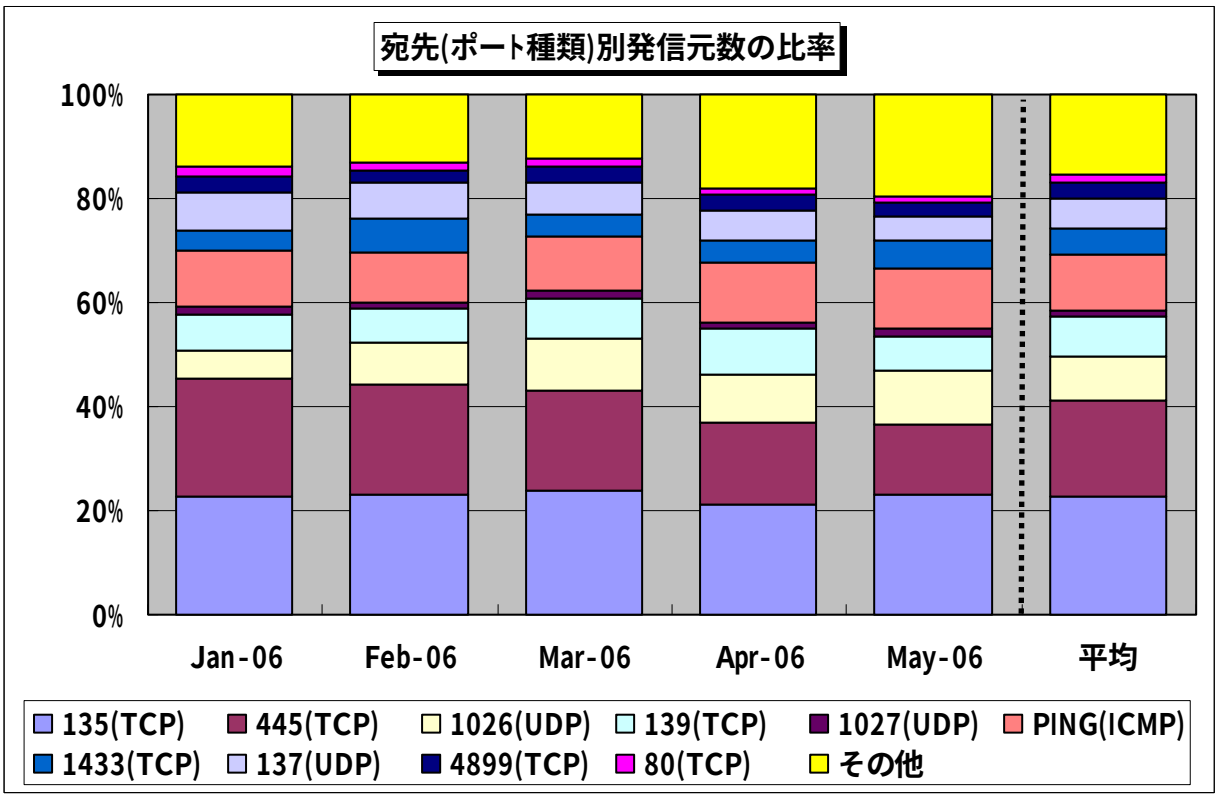
3．統計情報

3.1 2006 年 1 月～2006 年 5 月の宛先(ポート種類)別の比率

2006 年 1 月～2006 年 5 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。



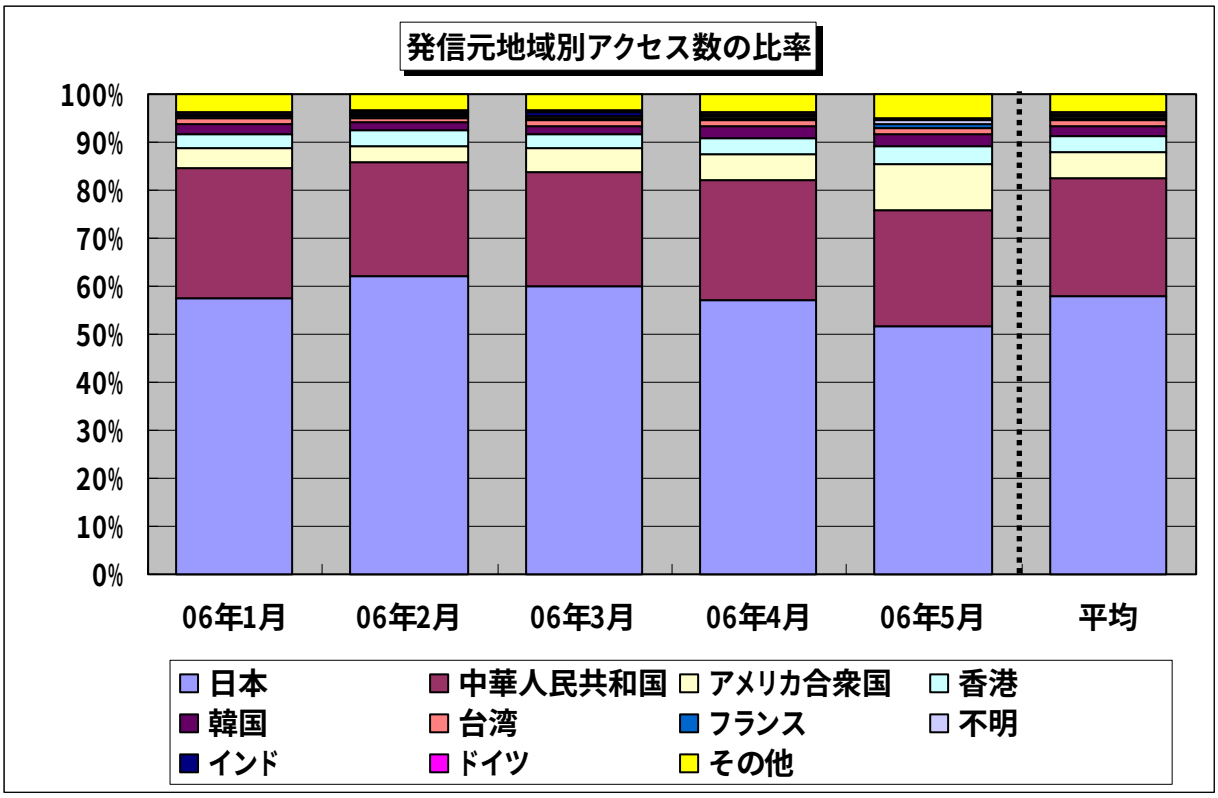
【図 3.1.1 2006 年 1 月～2006 年 5 月の宛先(ポート種類)別アクセス数の比率】



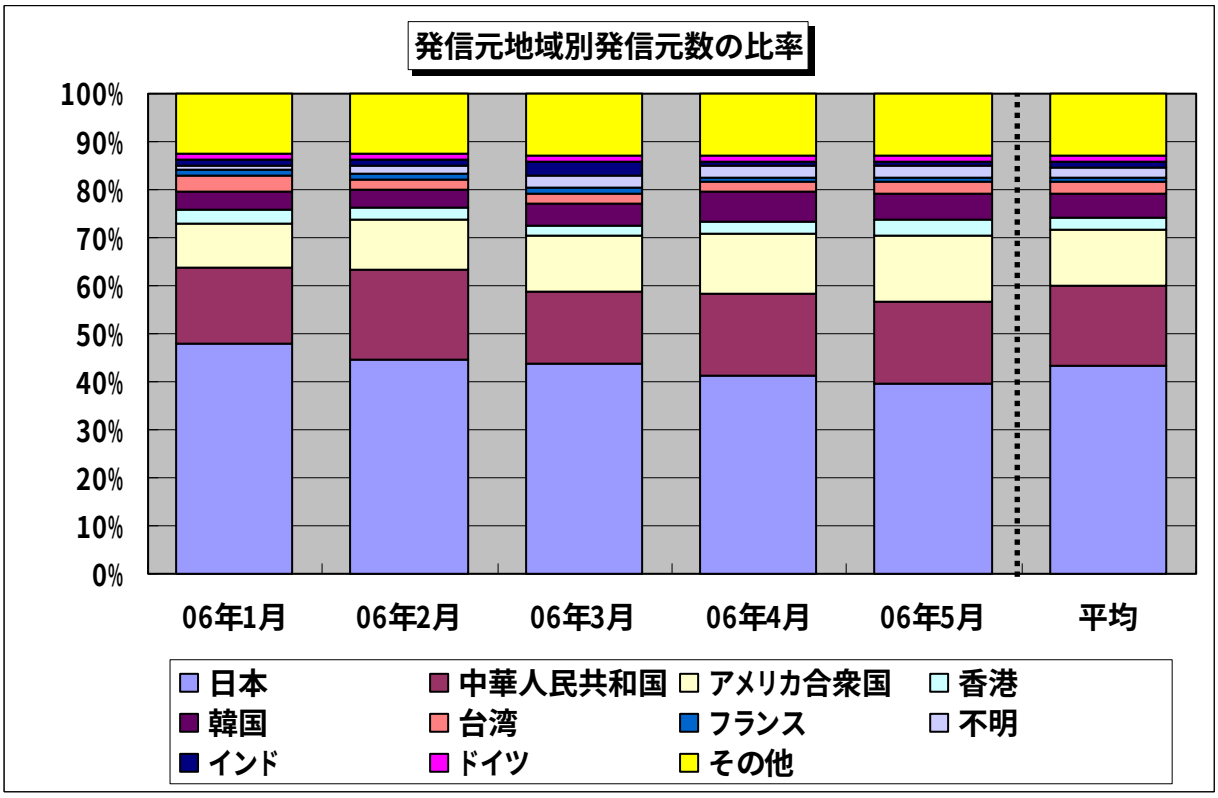
【図 3.1.2 2006 年 1 月～2006 年 5 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 1 月～2006 年 5 月の発信元地域別の比率

2006 年 1 月～2006 年 5 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 5 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 5 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 5 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 に関する脆弱性(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 特有の脆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
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
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 の脆弱性を狙った不正アクセスなど
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
4899(TCP)	リモート操作を行うための RAdmin の脆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)
1025(TCP)	135(TCP)と同じように Microsoft Windows Remote Procedure Call (RPC)で利用されるポートであり、Windows の脆弱性(MS05-051)を狙った不正アクセスに利用されている

■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