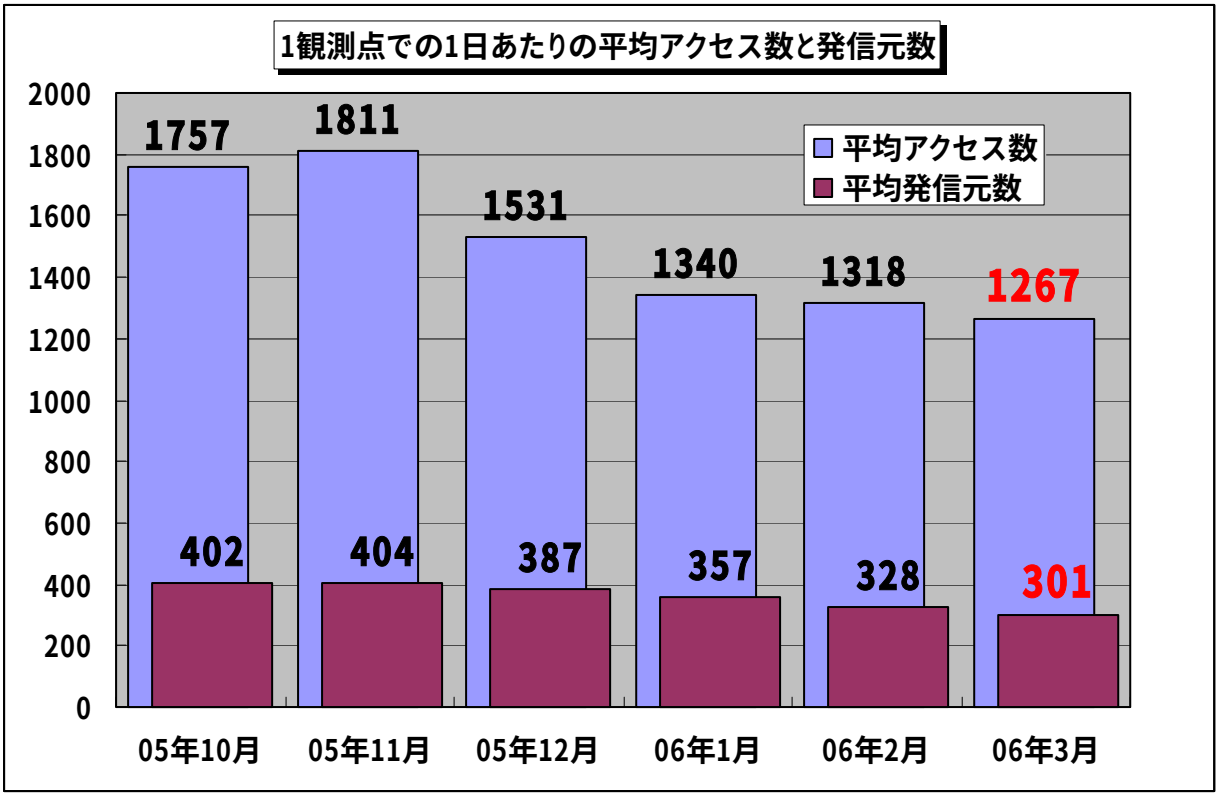
別紙 3

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 3 月の期待しない（一方的な）アクセスの総数は、10 観測点で **392,728 件**ありました。1 観測点で 1 日あたり **301** の発信元から **1,267 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、301 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】

2005 年 10 月～2006 年 3 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、発信元数も含めて、緩やかに減少傾向にあるようです。さらに、アクセス内容についても定常化(後述の統計情報を参照下さい)していると言えます。

2．3月のアクセス状況

3 月のアクセス状況は、2 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も、あいかわらず継続(緩やかな増加傾向)しています。最近は、ウイルス対策や不正アクセス対策を勧めるポップアップメッセージやネットサーフィン時のアドウェアによるポップアップ広告等も多いので、これらの内容に騙されないように注意して下さい。1026(UDP)/1027(UDP)ポートへのアクセスの対策としては、管理された LAN(企業内 LAN 等)以外では、Windows Messenger サービスを止めることをお勧めします。

一般のコンピュータ利用者は、これらの不正なアクセスによる感染を予防するために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフトやパーソナルファイアウォール等の有効利用をお勧めします。

さらに、ウイルス対策や不正アクセス対策に利用する各種の対策ソフト(最近では、ウイルス対策ソフトだけでなくパーソナルファイアウォール機能や個人情報流出を防止する機能などを組み合わせた製品が増えているようです)については、信頼のおけるベンダーのものを利用することをお勧めします。

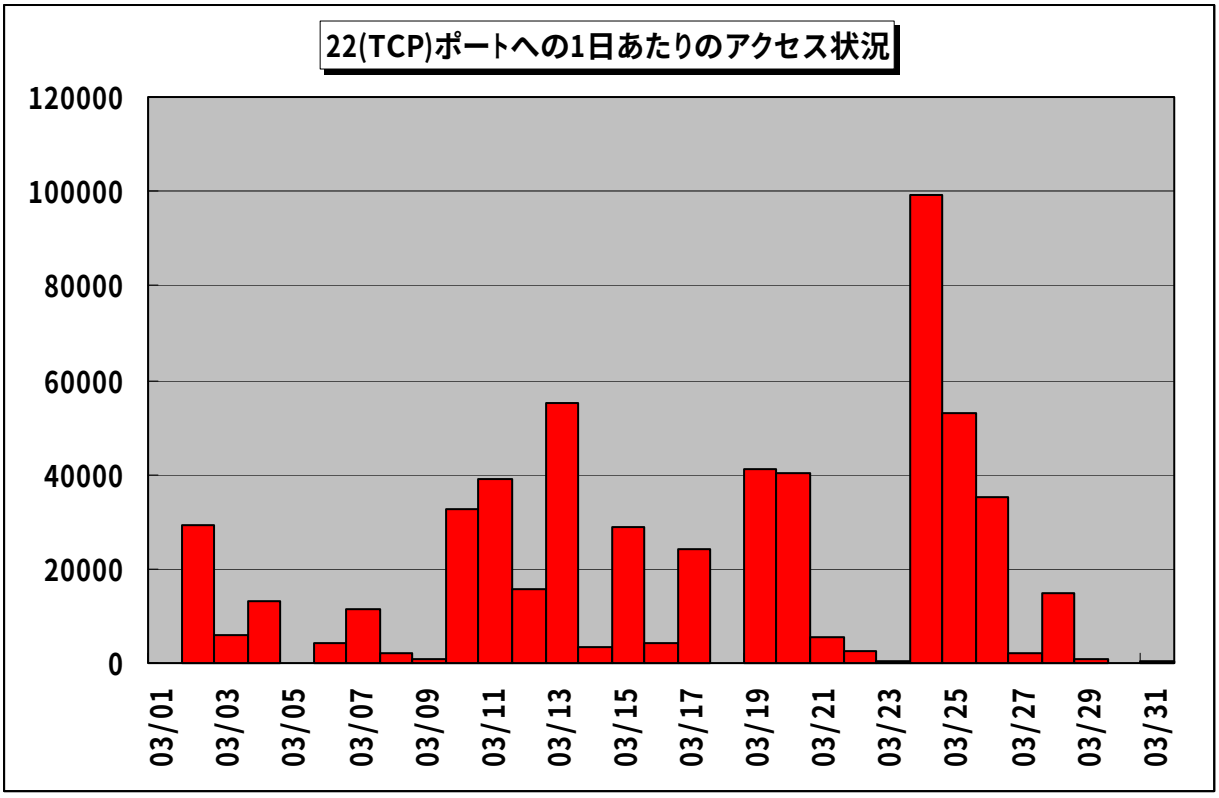
2.1 2006 年 3 月の特記事項

アクセスに特異性があるために統計情報から除外しているアクセスについて、今月の特記事項として以下に示します。

2.1.1 SSH を狙ったアクセス

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 22(TCP)ポートへのアクセスが、あいかわらず多く見受けられました。

IPA に届けられた不正アクセス届出にも、これらの攻撃により不正侵入されたものがあります。SSH を利用しているシステムの管理者は、サーバに脆弱性がないか確認し、常に最新の状態に保つことを心掛け、さらに利用するアプリケーションのパスワード強化や接続認証の強化を実施して下さい。



【図 2.1.1 2006 年 3 月の 22(TCP)ポートへのアクセス状況(アクセス数)】

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、一般的な不正なアクセスとともに観測することができます。SSH を使用していなければ、22(TCP)ポートへのポートスキャンのみ(1 日あたり数回から数十回がいいところです)で、図 2.1.1 に示すような状況にはなりえません。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。図 2.1.1 に示すピーク値では、1 日あたり 10 万回にせまるアクセス(発信元は 1 箇所)を繰り返されました。1 日当たり 2 万回～4 万回は当たり前の状況となっています。

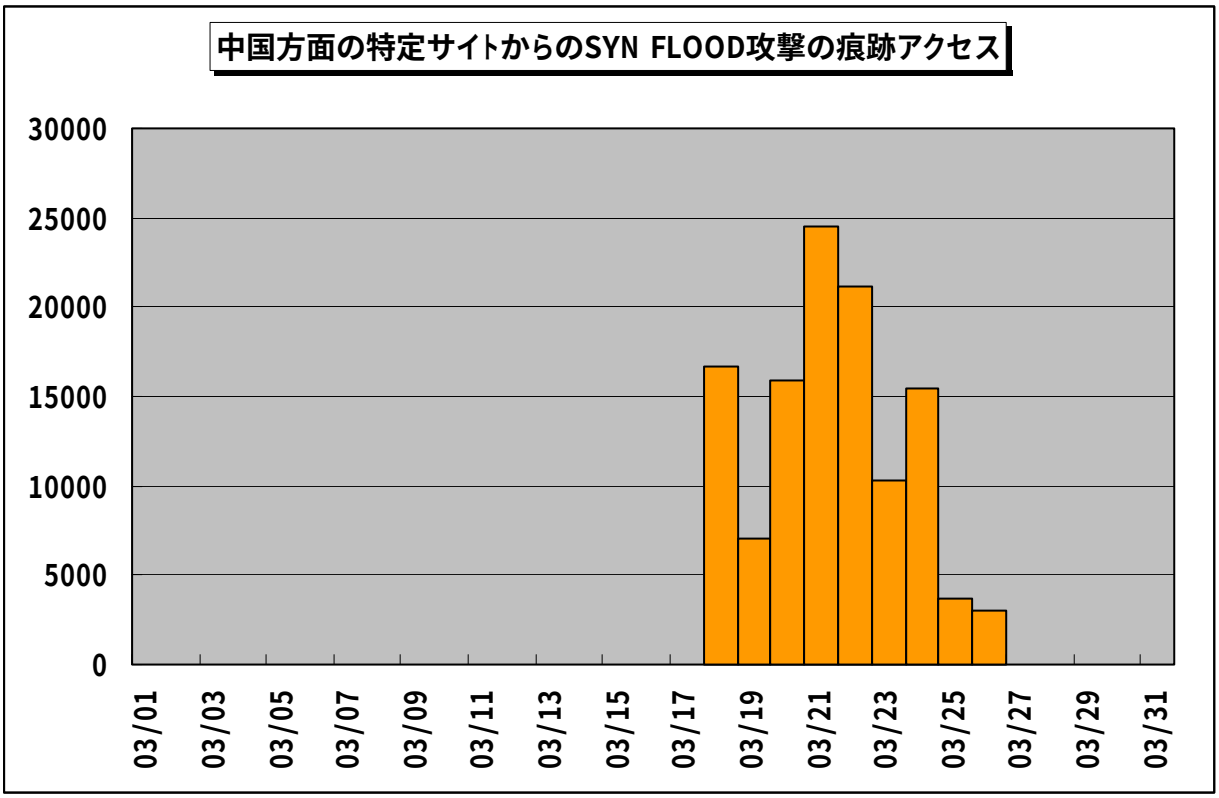
ID やパスワードの設定が安易であり、かつ接続認証が甘い場合は、これらのアクセスにより、システムに容易に侵入されることになります。でき得るならば、許可する接続先の限定や、公開鍵認証方式等の採用をお勧めします。SSH が使用するポートの変更も有効かも知れません。

2.1.2 DoS 攻撃の痕跡アクセス

攻撃者が、特定サイトへの SYN FLOOD 攻撃を仕掛けた際に、詐称した発信元 IP アドレスが、TALOT2 が使用していた観測点であったために観測されたアクセスについて以下に示します。

DoS(Denial of Service)攻撃の一種である SYN FLOOD 攻撃とは、インターネットのプロトコルの特性（スリーハンドシェイク）を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供することができなくする攻撃です。

TALOT2 が使用していた観測点の IP アドレスを、攻撃者がたまたま利用したために、図 2.1.2 に示すような DoS 攻撃の痕跡アクセスが観測されました。攻撃先は、中国方面の特定サイトでした。アクセスに使用されたポートが 80 ポートであることから、攻撃先は Web サイトと思われます。

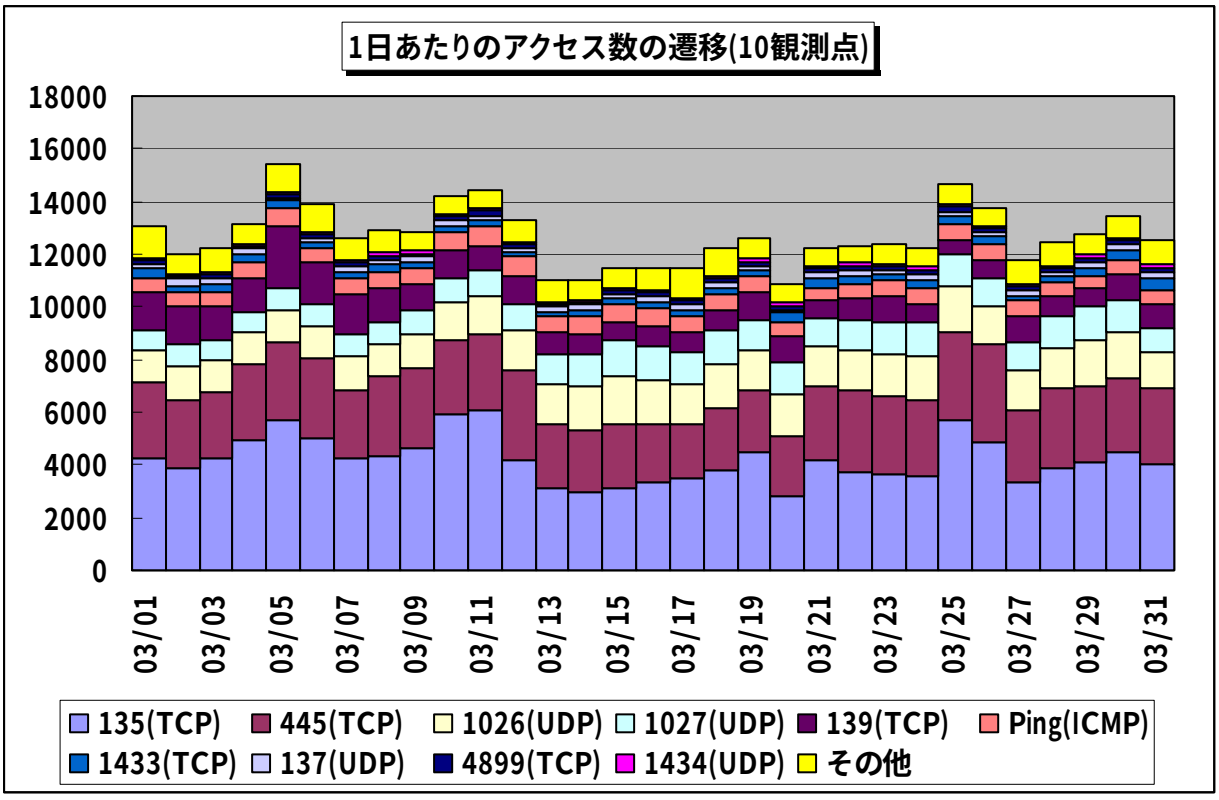


【図 2.1.2 2006 年 3 月の特定サイトからの 80(TCP) SYN+ACK アクセスの状況(アクセス数)】

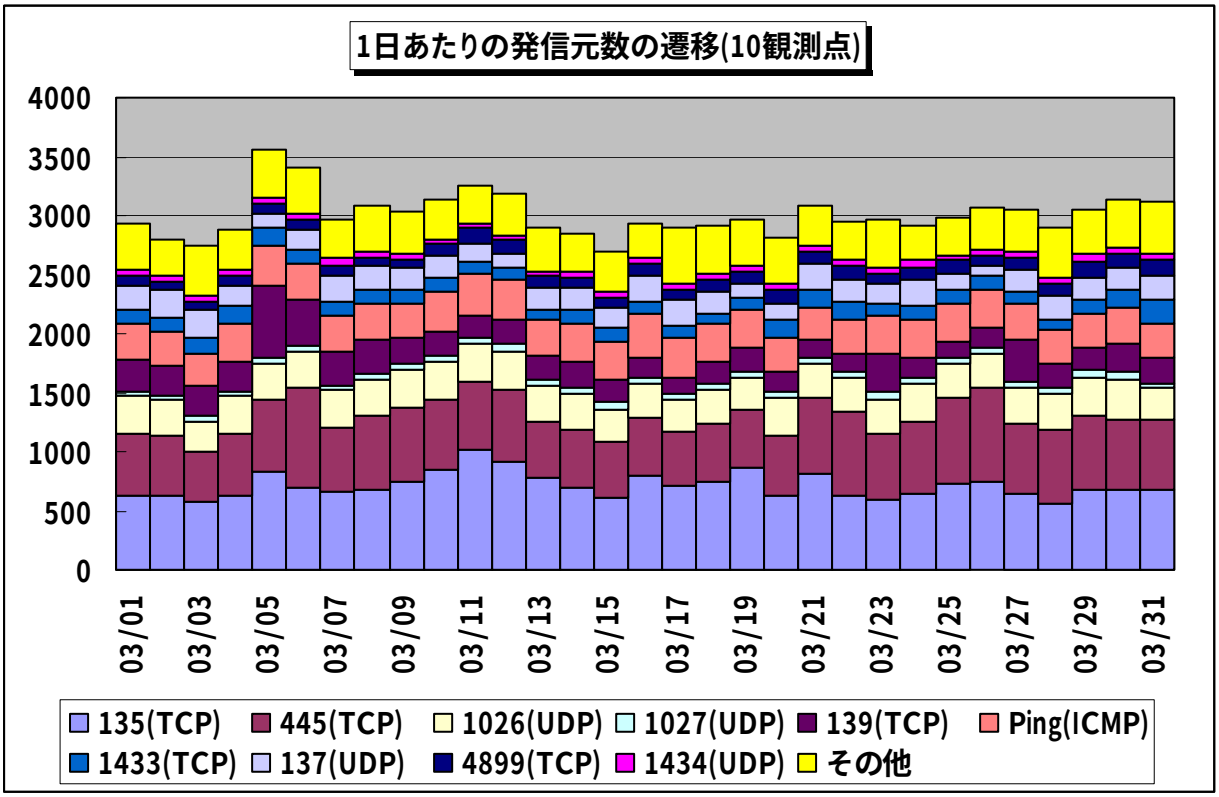
このような攻撃は、攻撃先のみならず、発信 IP アドレスとして詐称された、本来の IP アドレスの利用者にとっても、迷惑なアクセスです。いかなる理由があるのせよ、このような行為は行うべきではありません。

2.2 2006 年 3 月の一方的なアクセス状況

2006 年 3 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。



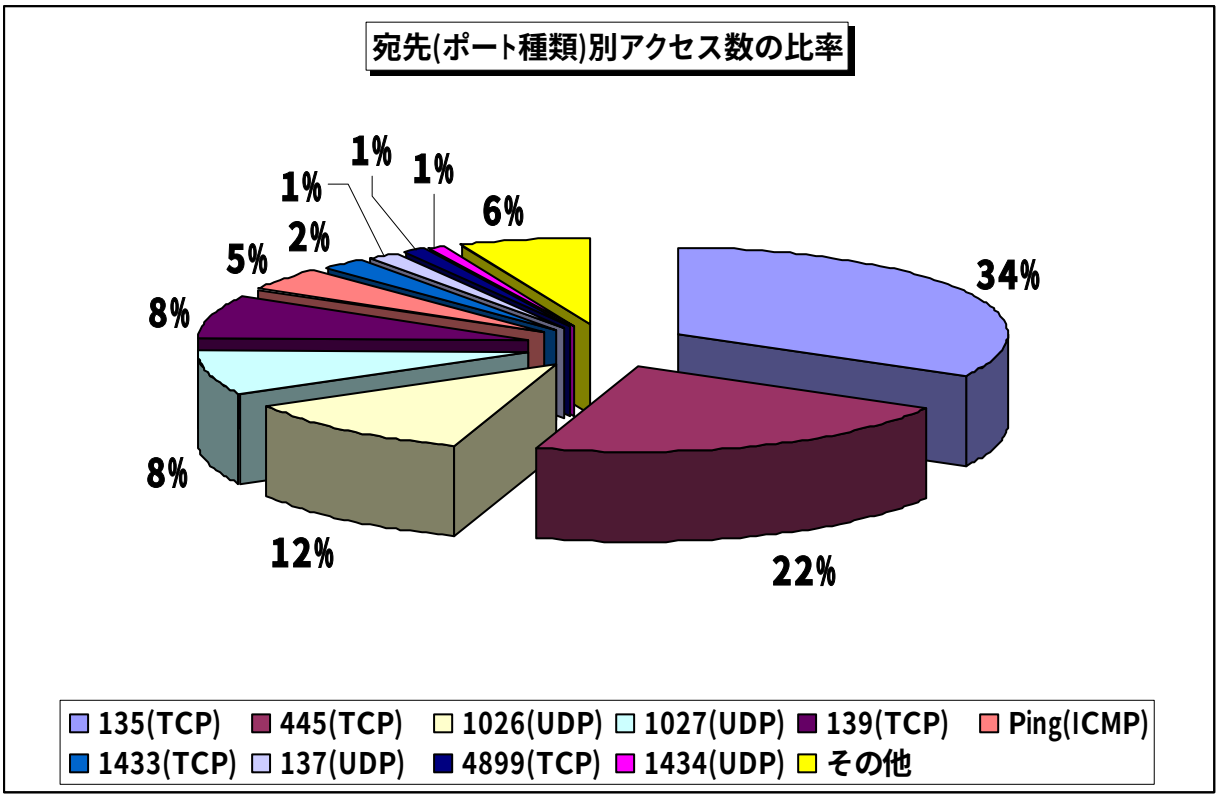
【図 2.2.1 2006 年 3 月の一方的なアクセス状況(アクセス数)】



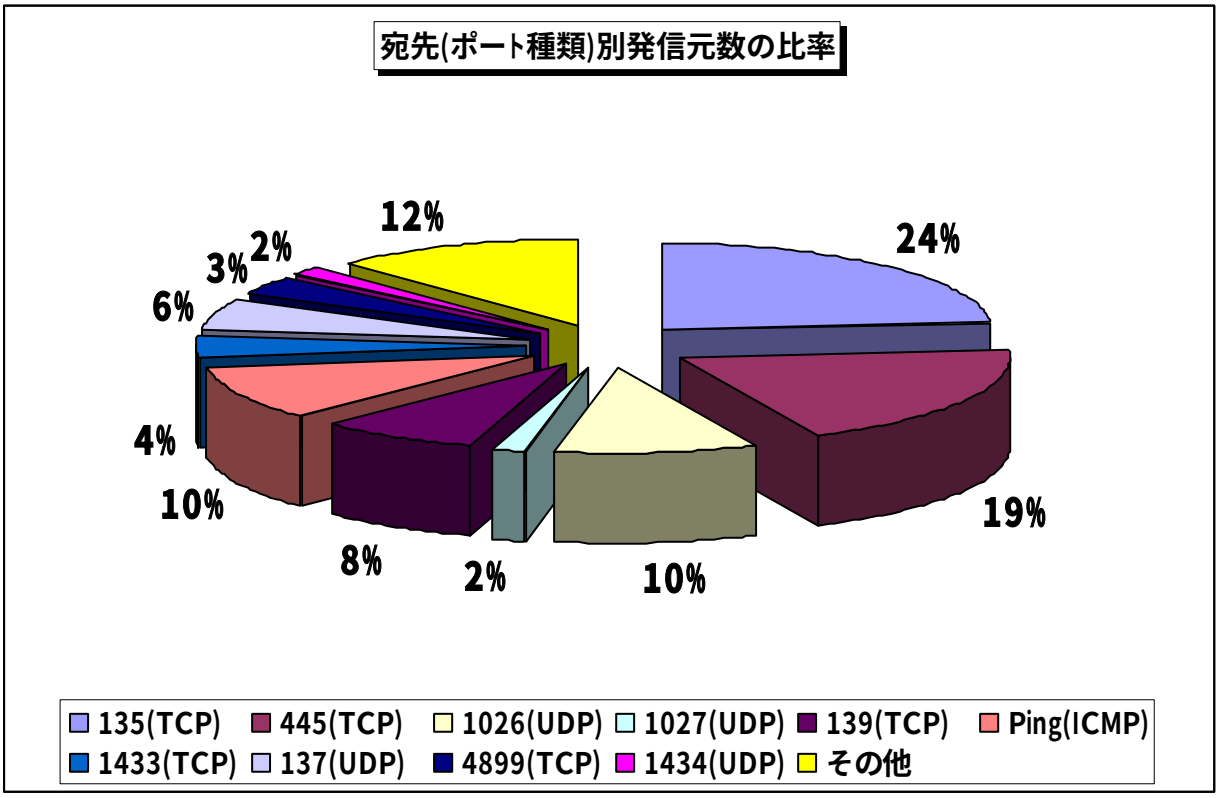
【図 2.2.2 2006 年 3 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 3 月の宛先(ポート種類)別の比率

2006 年 3 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。



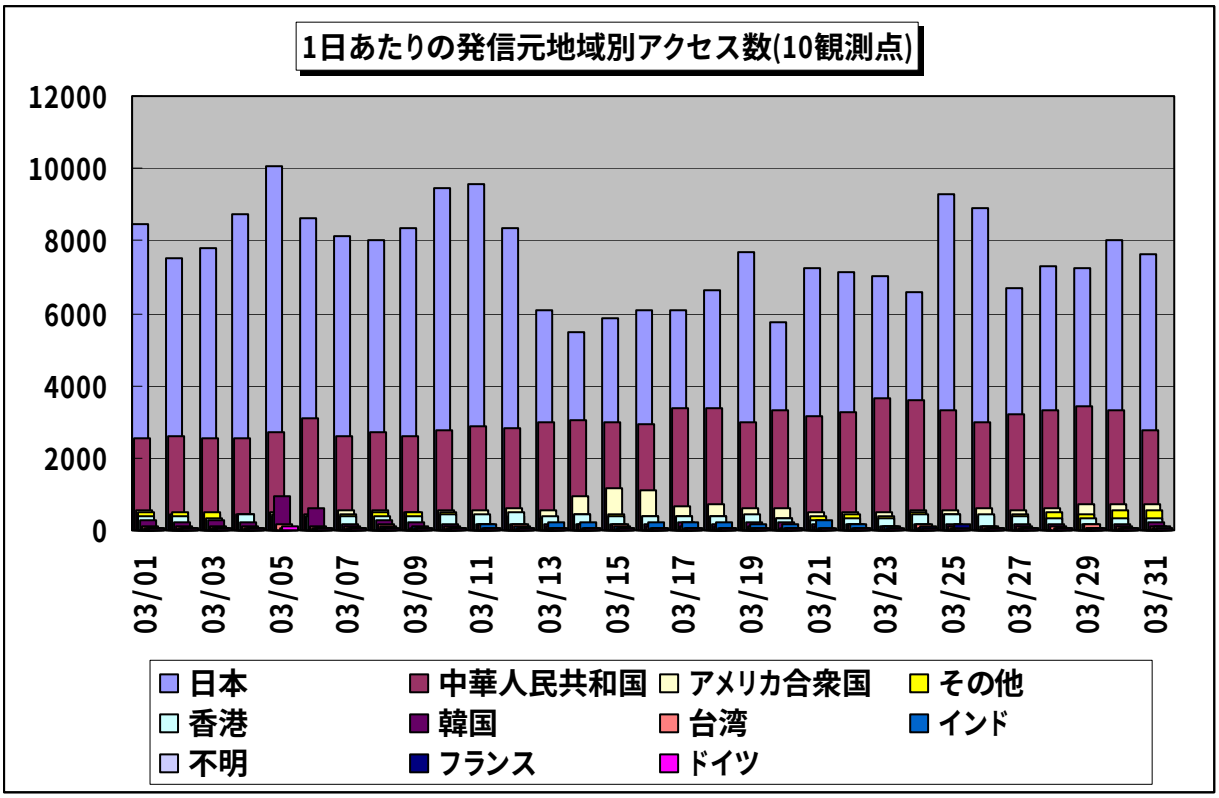
【図 2.3.1 2006 年 3 月の宛先(ポート種類)別アクセス数の比率】



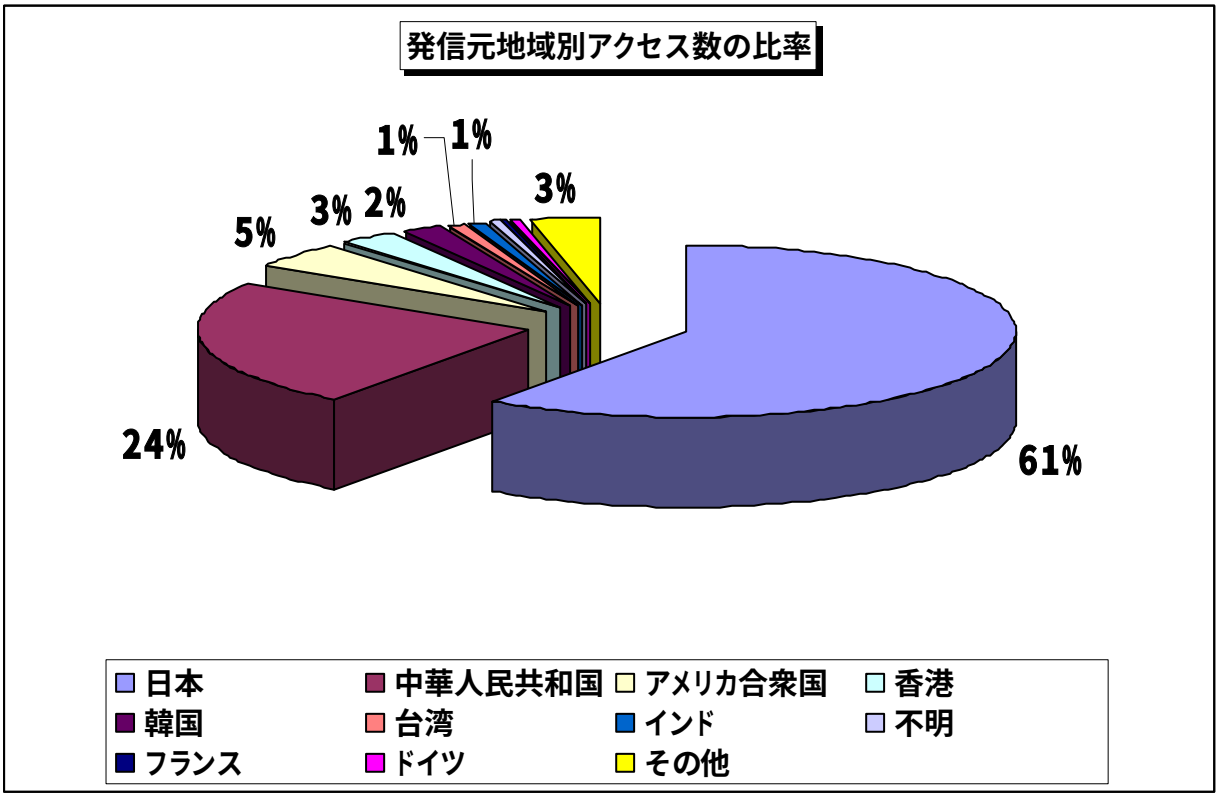
【図 2.3.2 2006 年 3 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 3 月の発信元地域別アクセス状況

2006 年 3 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。

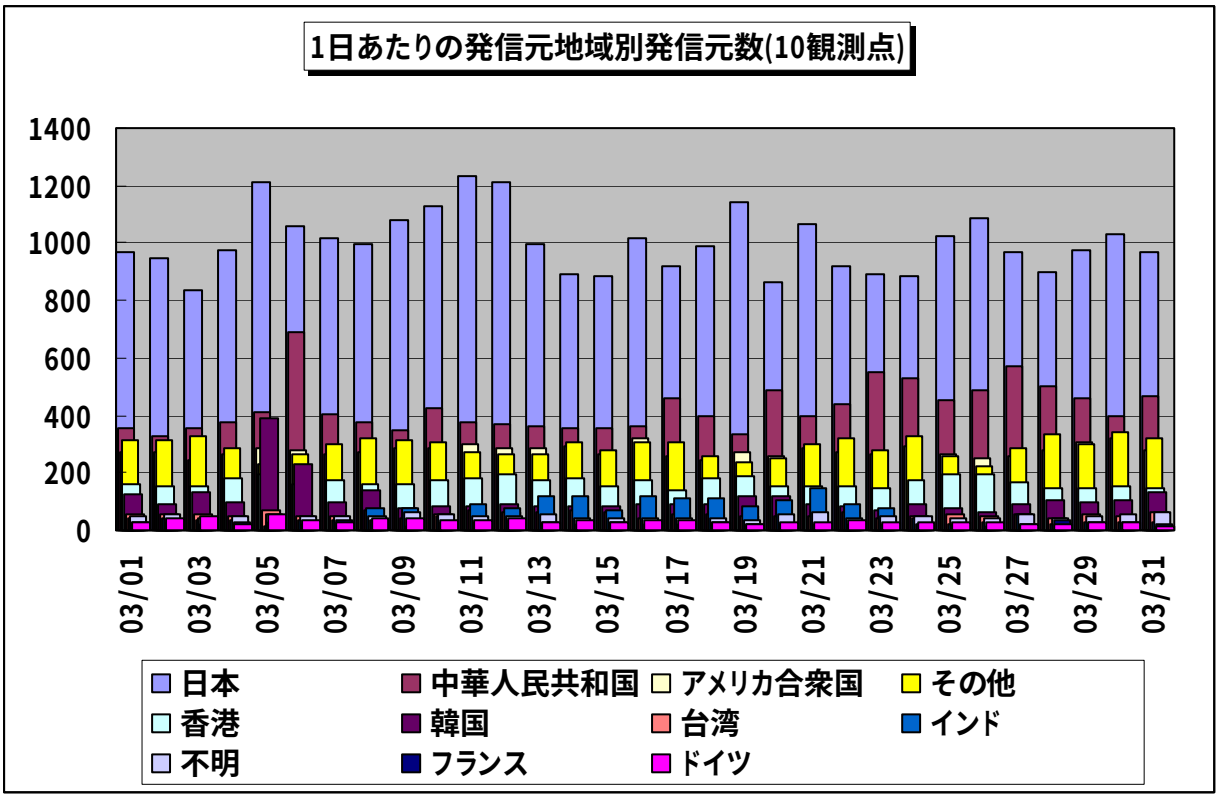


【図 2.4.1 2006 年 3 月の発信元地域別アクセス数の変化】

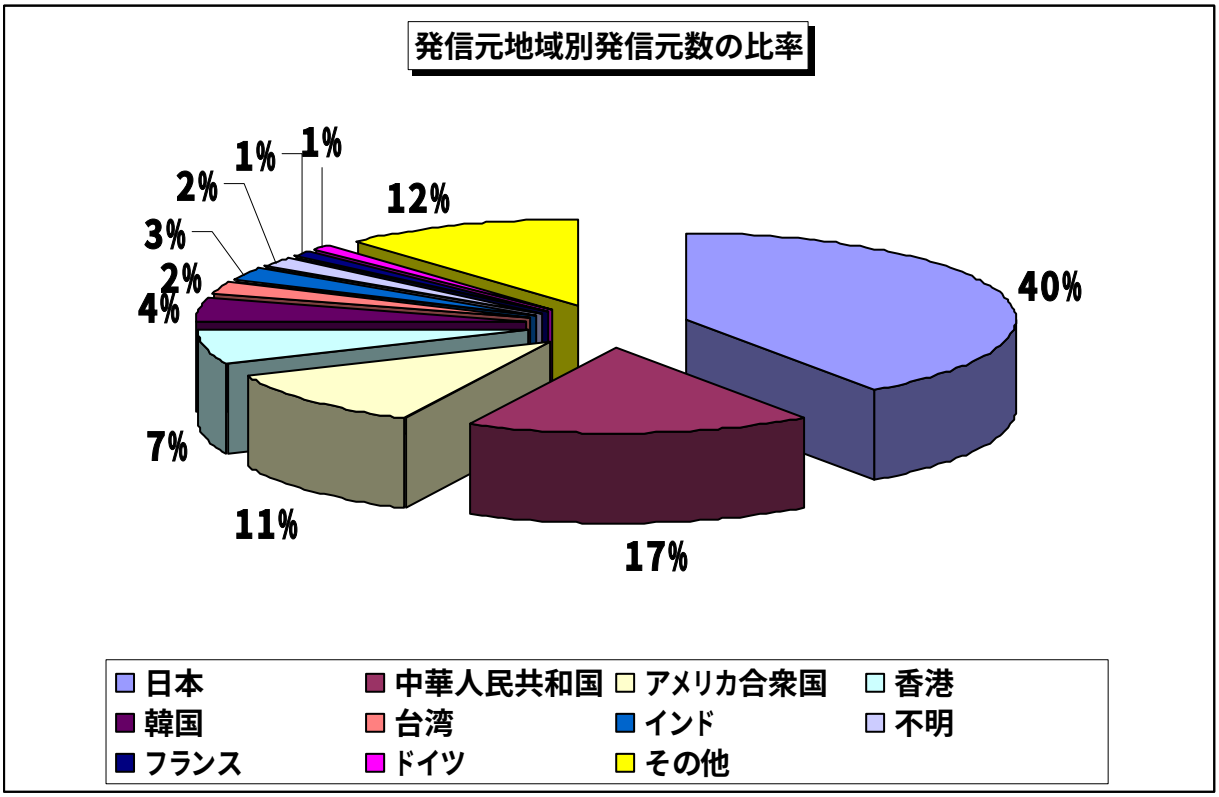


【図 2.4.2 2006 年 3 月の発信元地域別アクセス数の比率】

2006 年 3 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 3 月の発信元地域別発信元数の変化】

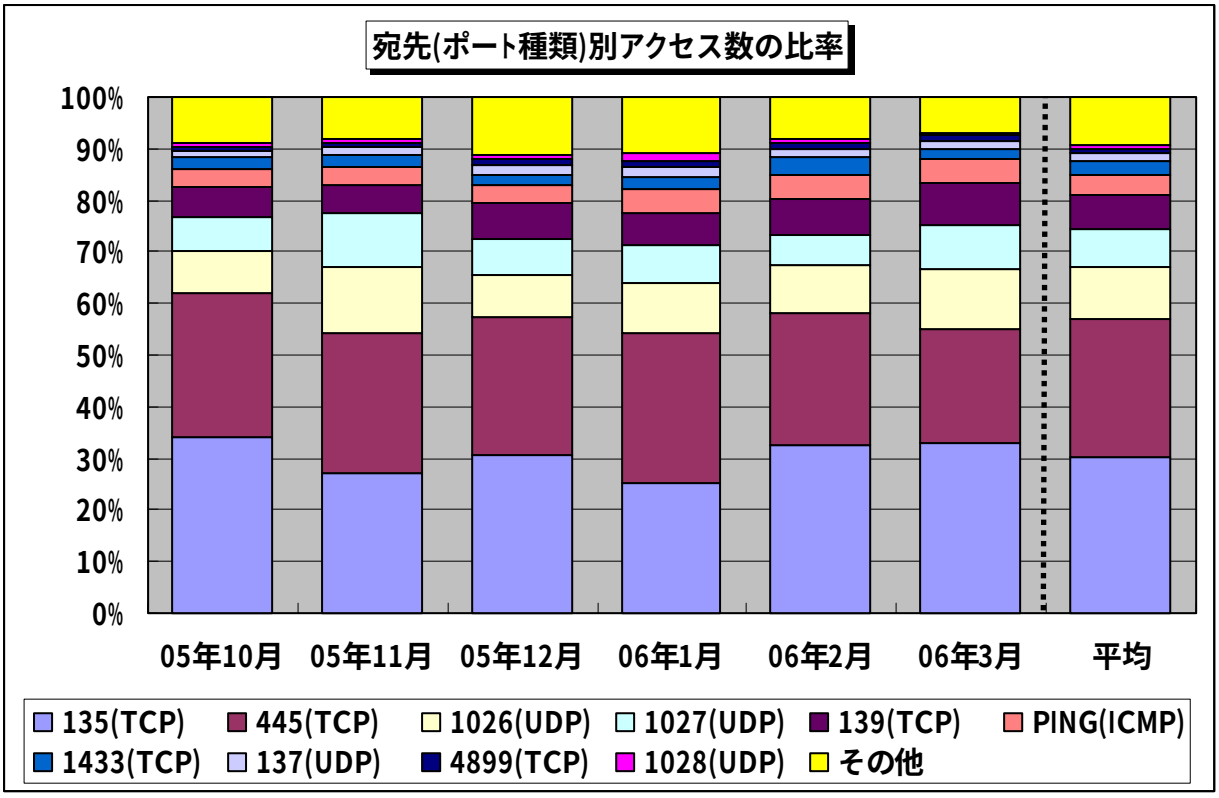


【図 2.4.4 2006 年 3 月の発信元地域別発信元数の比率】

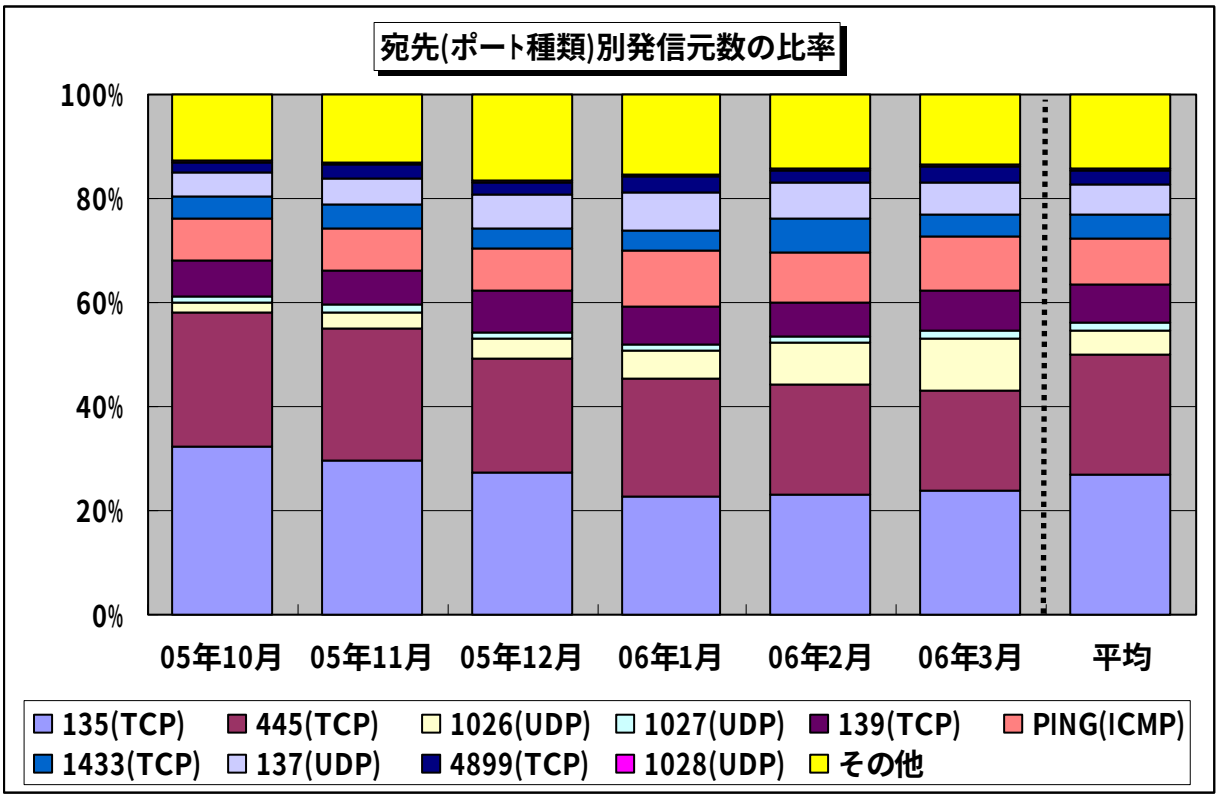
3．統計情報

3.1 2005 年 10 月～2006 年 3 月の宛先(ポート種類)別の比率

2005 年 10 月～2006 年 3 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。



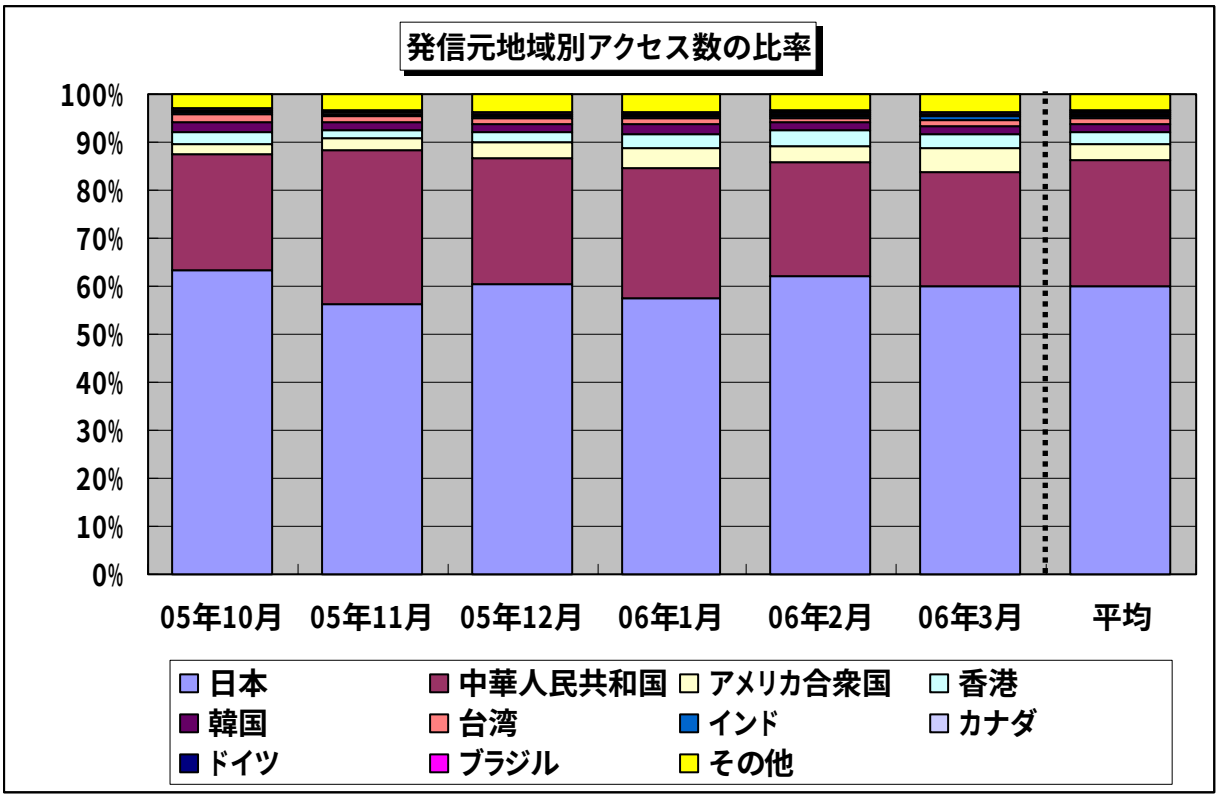
【図 3.1.1 2005 年 10 月～2006 年 3 月の宛先(ポート種類)別アクセス数の比率】



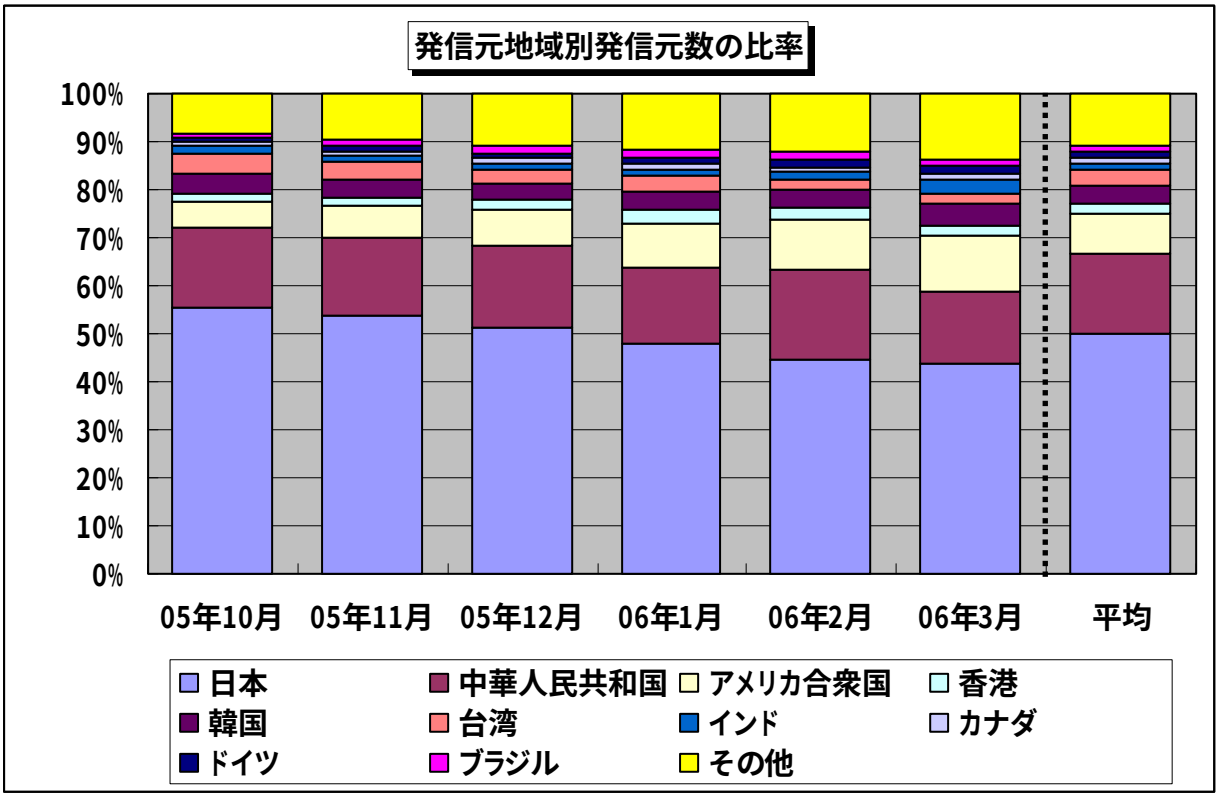
【図 3.1.2 2005 年 10 月～2006 年 3 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 10 月～2006 年 3 月の発信元地域別の比率

2005 年 10 月～2006 年 3 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 2005 年 10 月～2006 年 3 月の発信元地域別アクセス数の比率】



【図 3.2.2 2005 年 10 月～2006 年 3 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 3 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)
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／内山
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp