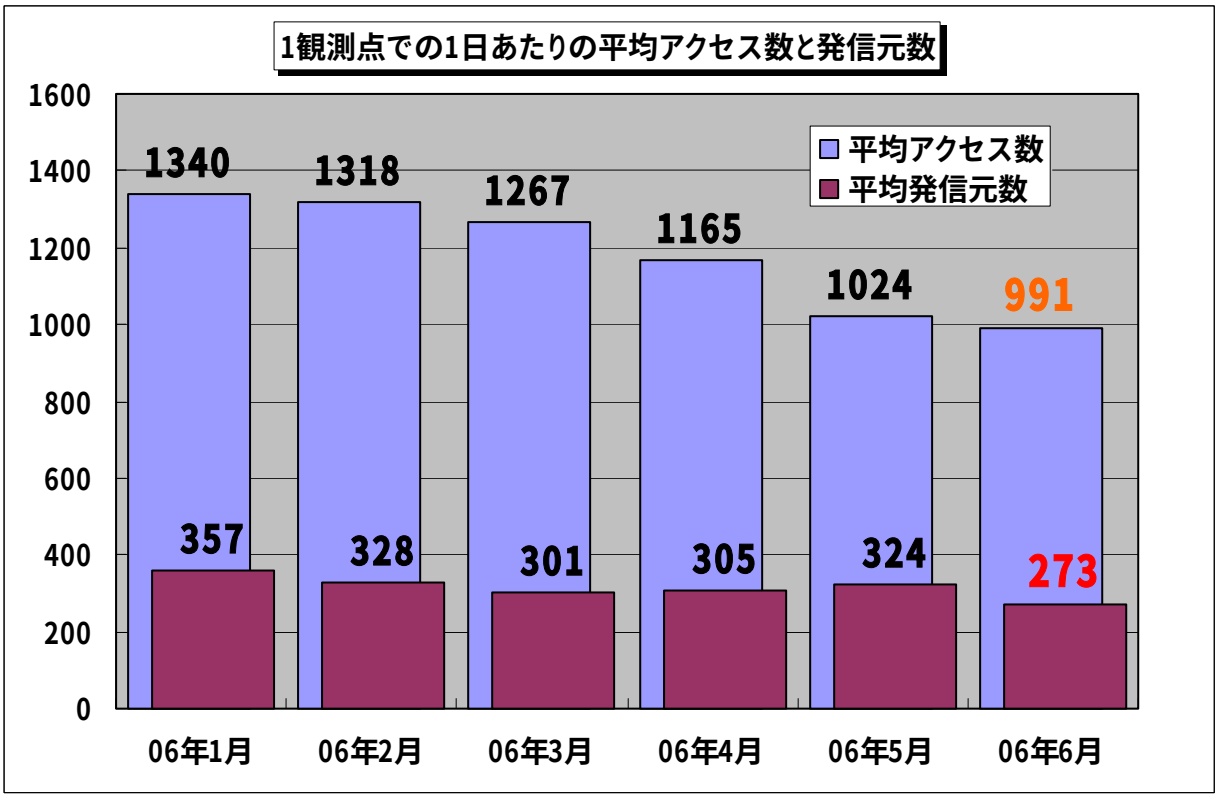
別紙 3

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 6 月の期待しない（一方的な）アクセスの総数は、10 観測点で **297,445 件**ありました。1 観測点で 1 日あたり **273** の発信元から **991 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、273 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 6 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。

2．6 月のアクセス状況

6 月のアクセス状況は、5 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。

さらに、80(TCP)ポートへのアクセス数が増加傾向にあるようです。ディレクトリトラバーサル(*1)をはじめとする Web アプリケーションの脆弱性が騒がれていますので、Web サイトの運用管理者のかたは、あらためて注意が必要と思われます。

(*1) ディレクトリトラバーサル
相対パス指定を悪用し、Web サイトの管理者が意図しないサーバ上のディレクトリを覗かれる脆弱性を狙った攻撃手法。管理者の意図しない情報漏えいを起こす可能性があります。

2.1 2006 年 6 月の特集

今月の『コンピュータウイルス・不正アクセスの届出状況[2006 年 6 月]について』の呼びかけキーワードとなっているパスワードについて、インターネット定点観測でも特集を組みました。

- ネットワークからのパスワードクラッキング攻撃
- 5900(TCP)ポートへのアクセスの経過報告

2.1.1 ネットワークからのパスワードクラッキング攻撃

以前から、時々話題にしていた SSH（Secure Shell）を狙った攻撃について 2006 年 1 月～6 月の TALOT2 での状況を示します。

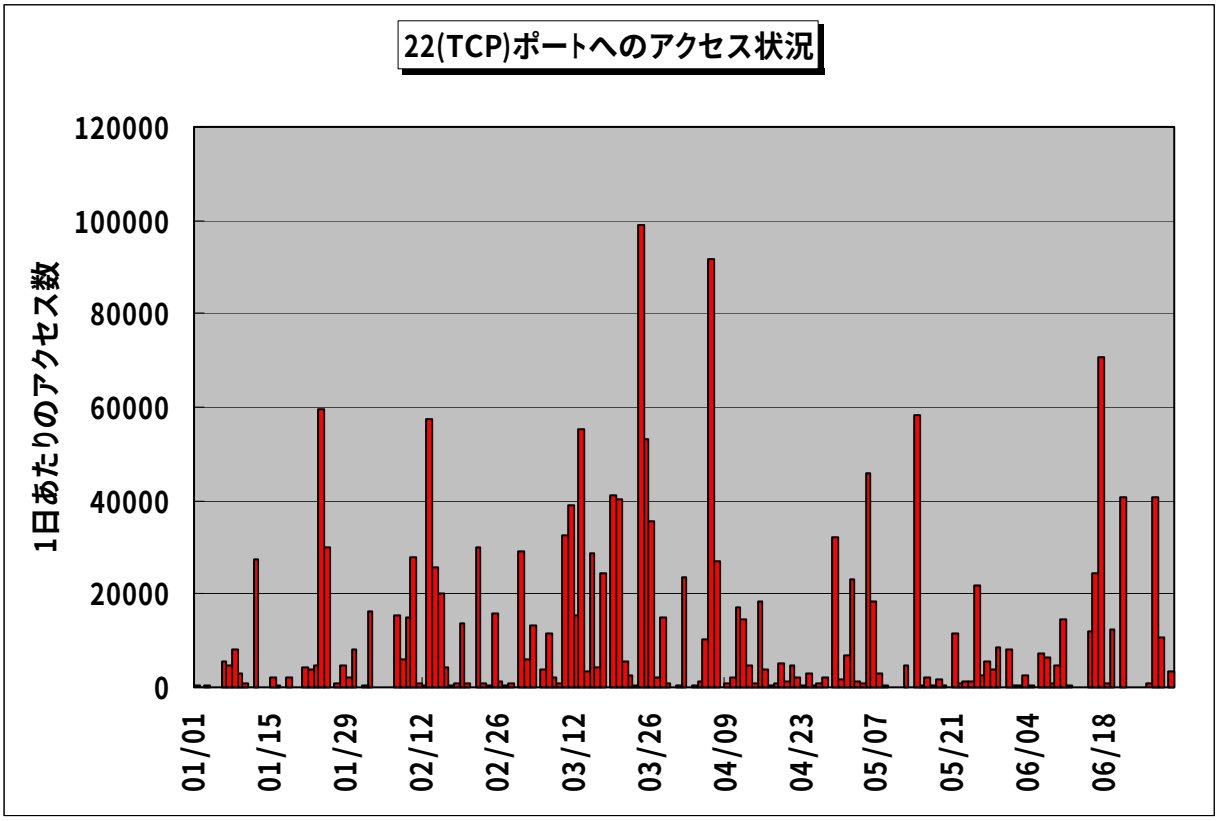
(注意)
これらのパスワードクラッキング攻撃と思われるアクセスについては、通常の観測データからは除外しています。

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す。

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。

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1月～6 月の 22(TCP)ポートへのアクセス状況(アクセス数)】

(解説)

図2.1.1を見ても分かる通り、攻撃者は何らかの攻撃ツールを使い、数万回のログインの試行を繰り返しています。最大値は 10 万回に手が届きそうな状況でした。これらの攻撃の観測を実施している観測点は、常に固定観測点ではなく、不定期に IP アドレスを変更しています。しかし、攻撃は続いています。攻撃者は、22(TCP)ポートが開いていることをポートスキャンで探し出し、ターゲットを見つけると、このような攻撃を仕掛けます。ログインに必要な ID やパスワードが単純である場合は、攻略される危険性が高くなります。いわゆる総当り攻撃（ブルートフォース攻撃）(*1)や辞書攻撃(*2)を行われると、たちどころに侵入されることになります。

これらの攻撃を回避する方法としては、ログインに必要な ID とパスワードの組み合わせのみによる認証だけでなく、別の認証方法もサポートすることが有効です。

不特定多数の利用者を想定している場合は、公開鍵認証方式が有効です。特定の利用者に限定できる場合は、ファイアウォールによる接続先の限定方式などが有効となります。

(*1) 総当り攻撃（ブルートフォース攻撃）

何らかの規則にしたがって、文字の組み合わせを総当りで試行する攻撃方法。いわゆる力ずくの攻撃方法のことです。

(*2) 辞書攻撃

辞書に載っているような文字列を、片端から試行する攻撃方法。英語の辞書のある単語をはじから試す方法などがありますが、最近ではパスワード等に使われやすい単語が登録された攻撃用の辞書も出回っているようです。さらに、それらの辞書が日本語対応になっているものがあると言われています。

2.1.2 5900(TCP)ポートへのアクセスの経過報告

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。

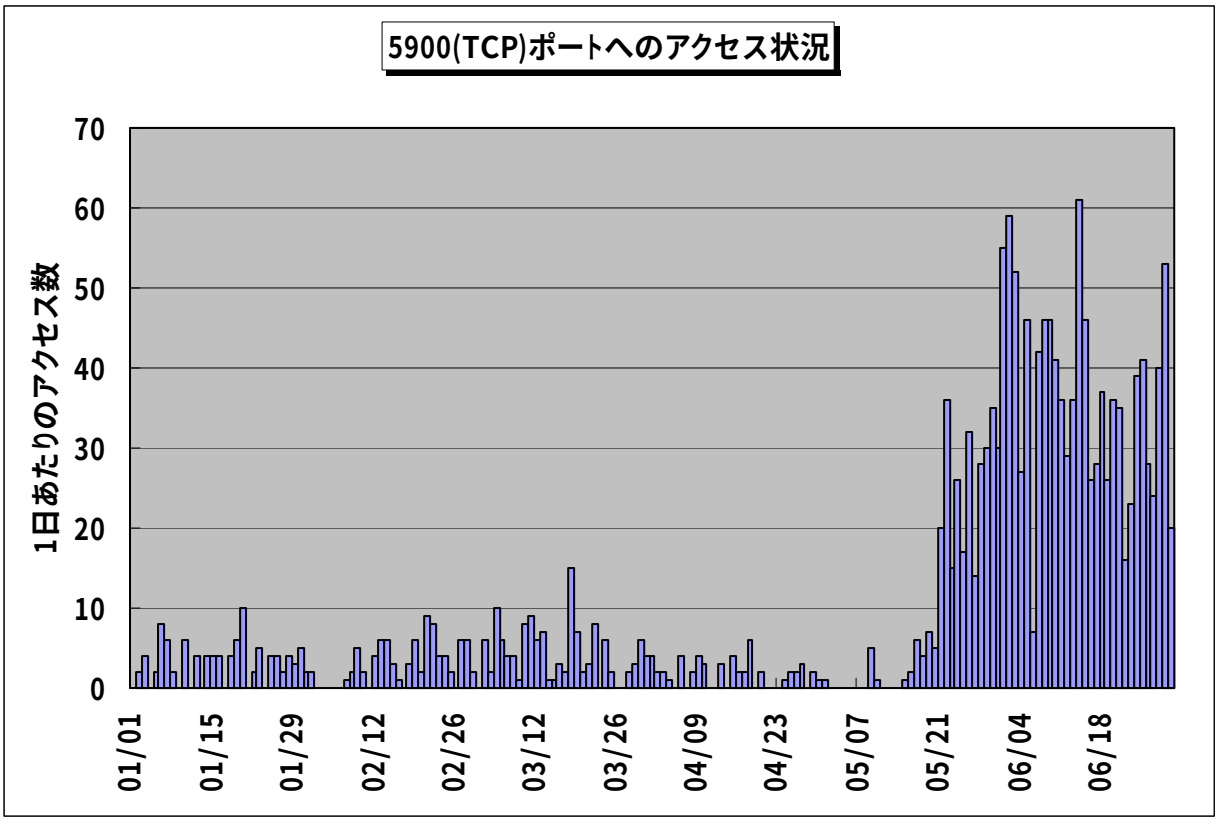
■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/index.html

■ 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。

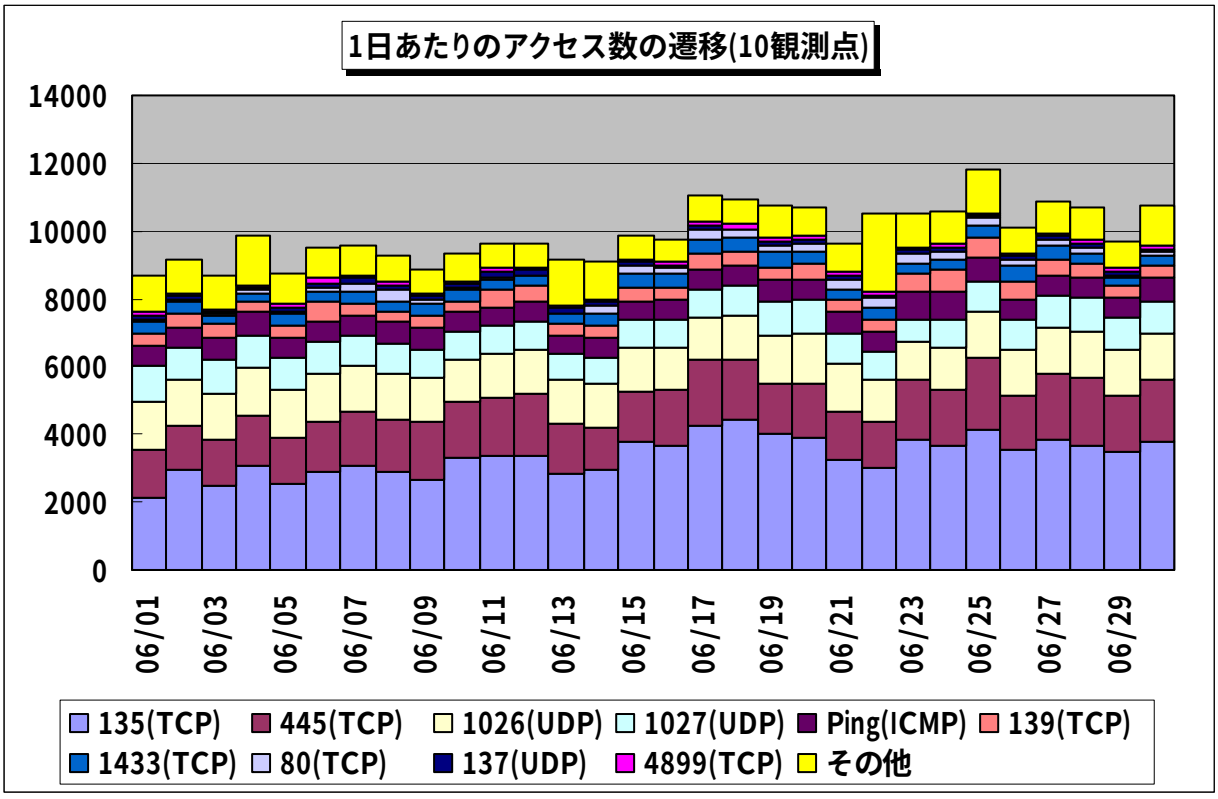
アクセスの増加は、5 月 17 日前後から増加しましたが、現在は、増加したまま一定のレベルで安定しています。RealVNCでの運用を行っているシステムの管理者は、上記の情報を参考にし、早急に、脆弱性に対する対応を実施して下さい。



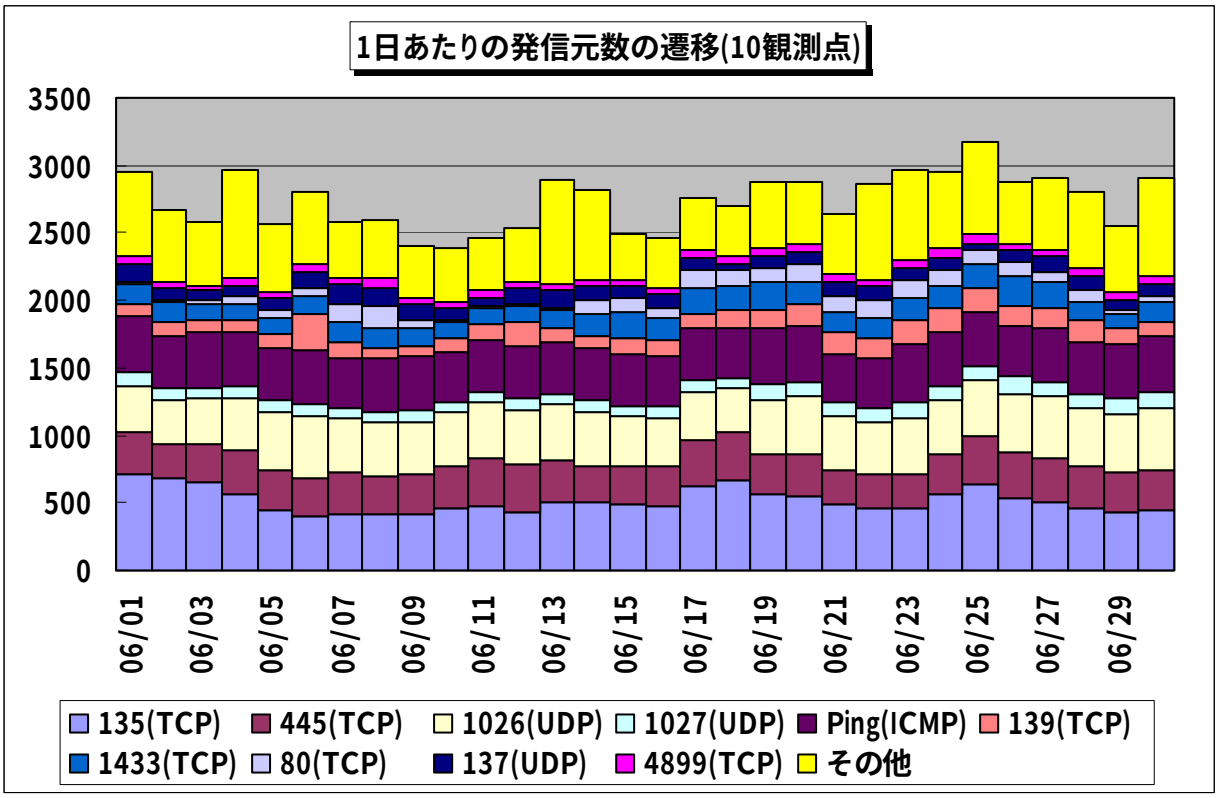
【図 2.1.2 2006 年1月～6 月の 5900(TCP)ポートへのアクセス状況(アクセス数)】

2.2 2006 年 6 月の一方的なアクセス状況

2006 年 6 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。



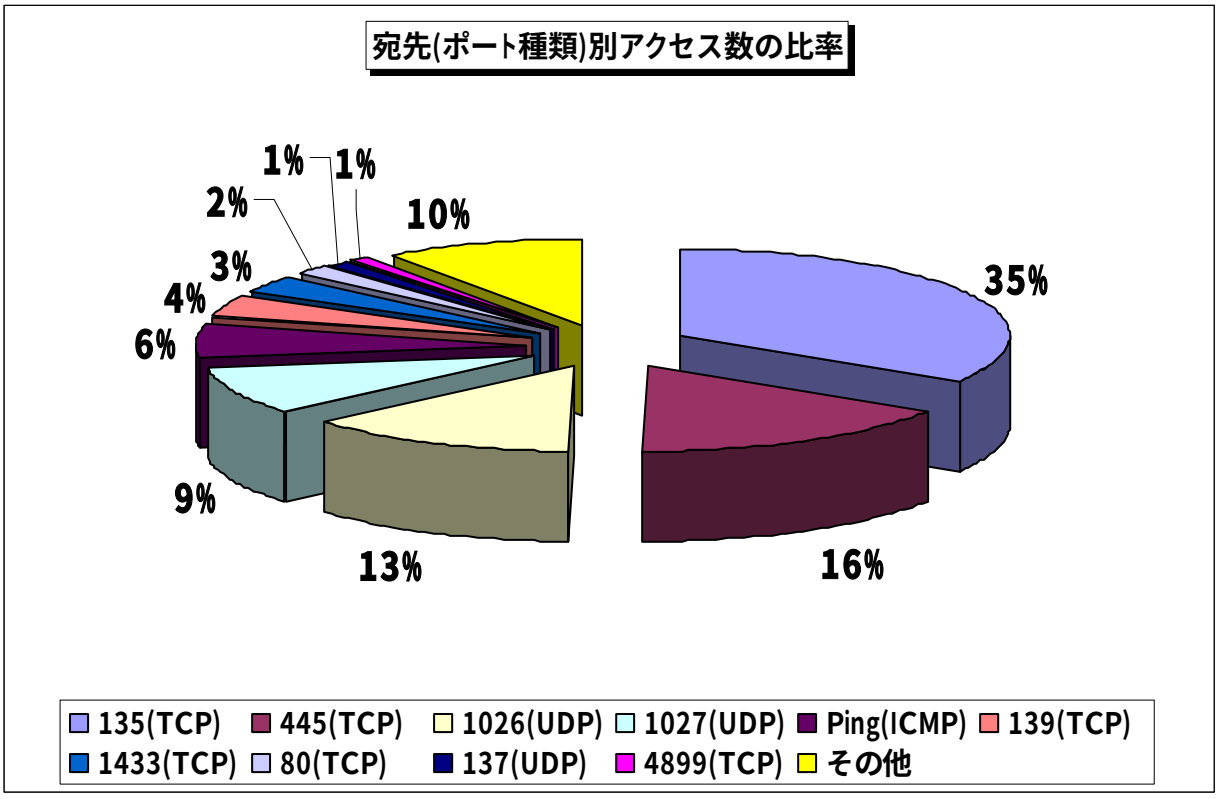
【図 2.2.1 2006 年 6 月の一方的なアクセス状況(アクセス数)】



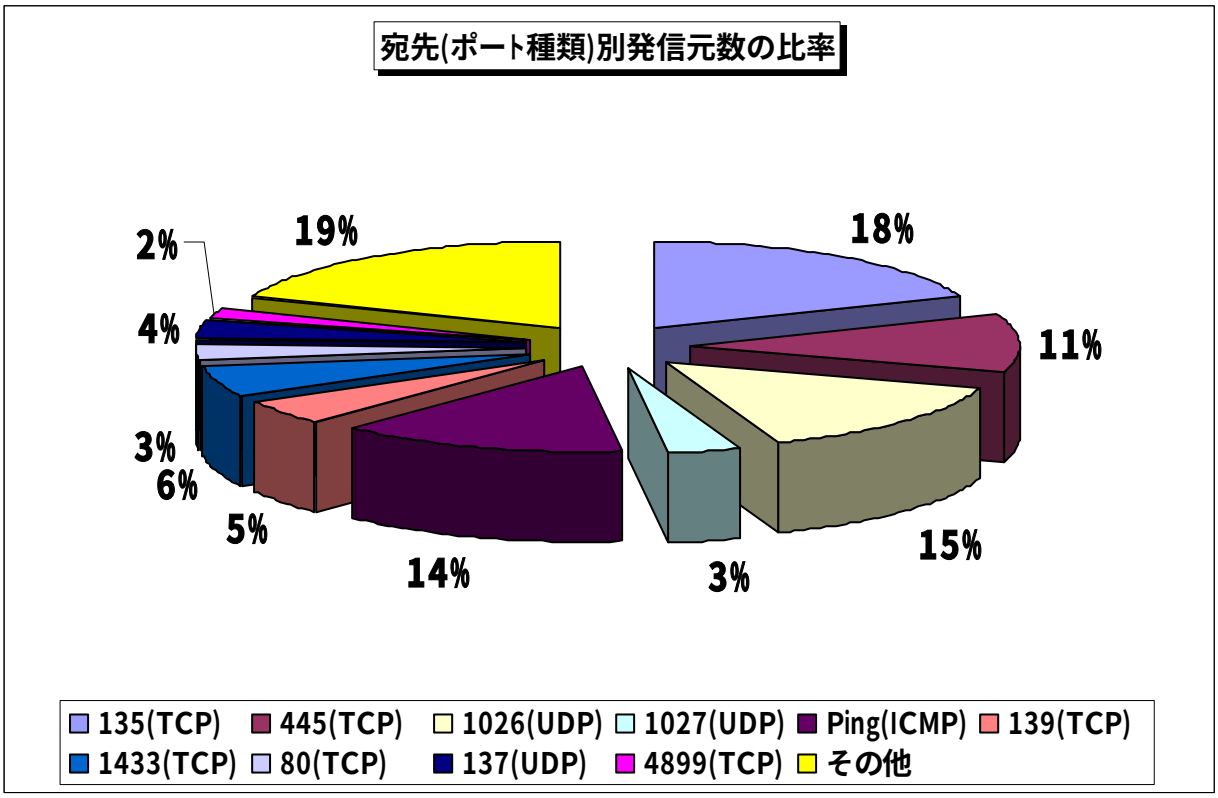
【図 2.2.2 2006 年 6 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 6 月の宛先(ポート種類)別の比率

2006 年 6 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。



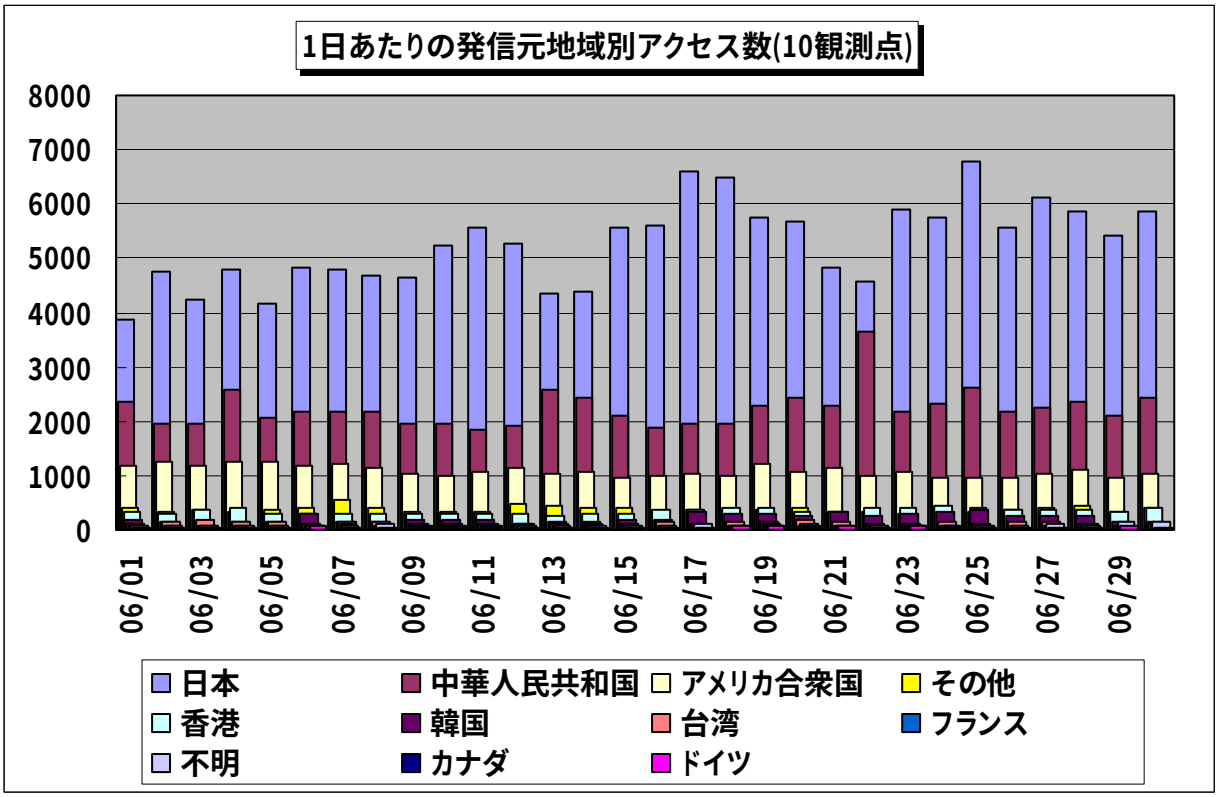
【図 2.3.1 2006 年 6 月の宛先(ポート種類)別アクセス数の比率】



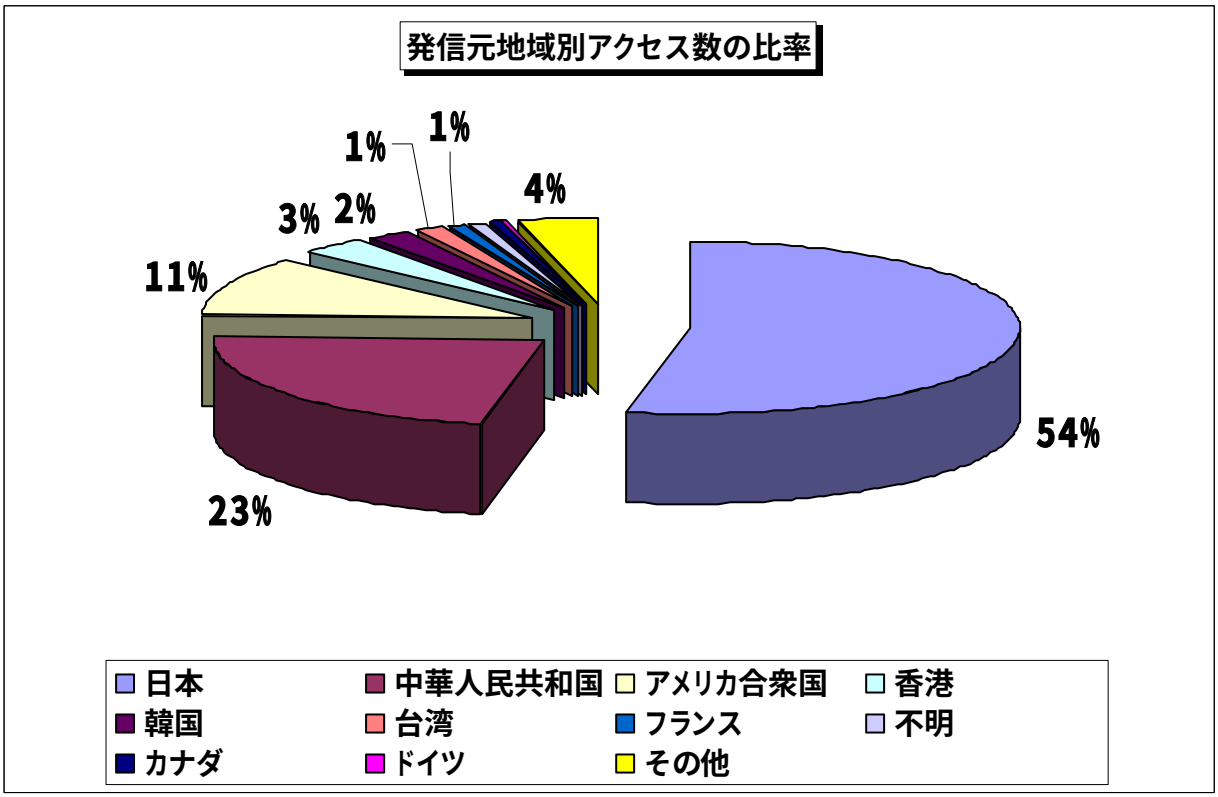
【図 2.3.2 2006 年 6 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 6 月の発信元地域別アクセス状況

2006 年 6 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。

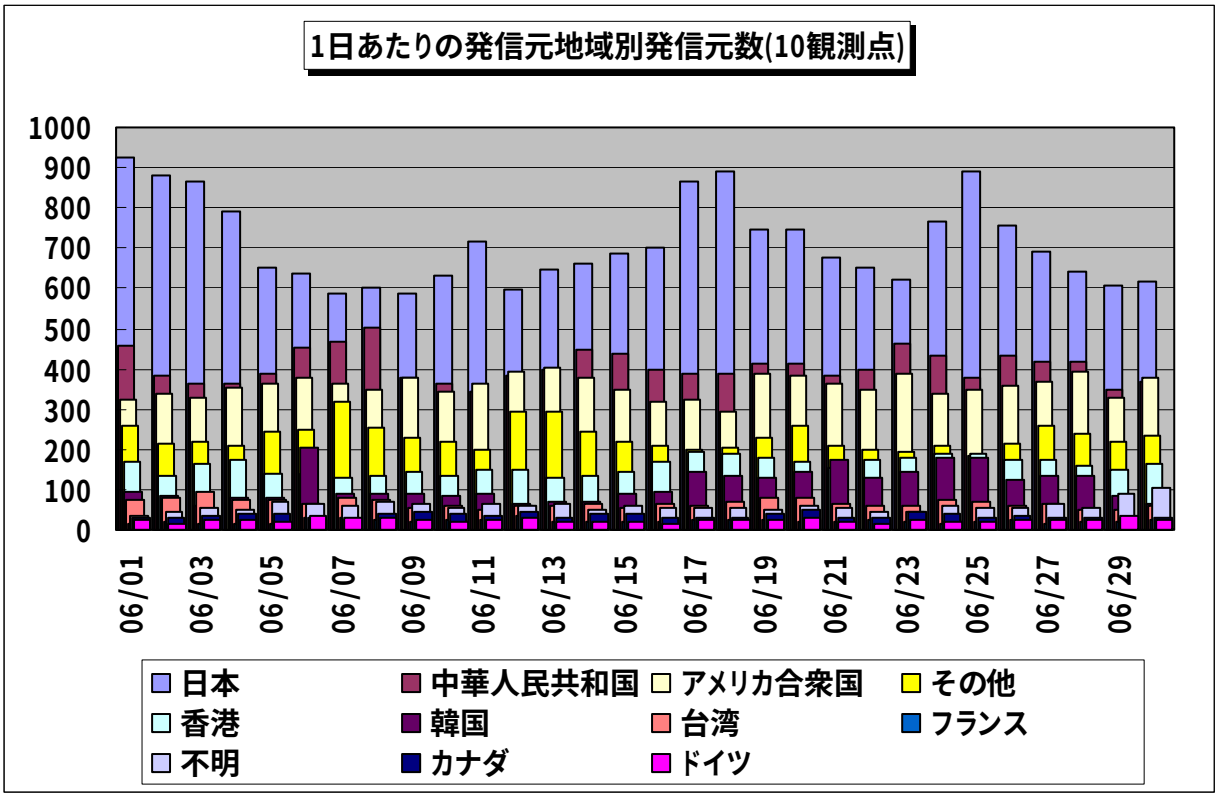


【図 2.4.1 2006 年 6 月の発信元地域別アクセス数の変化】

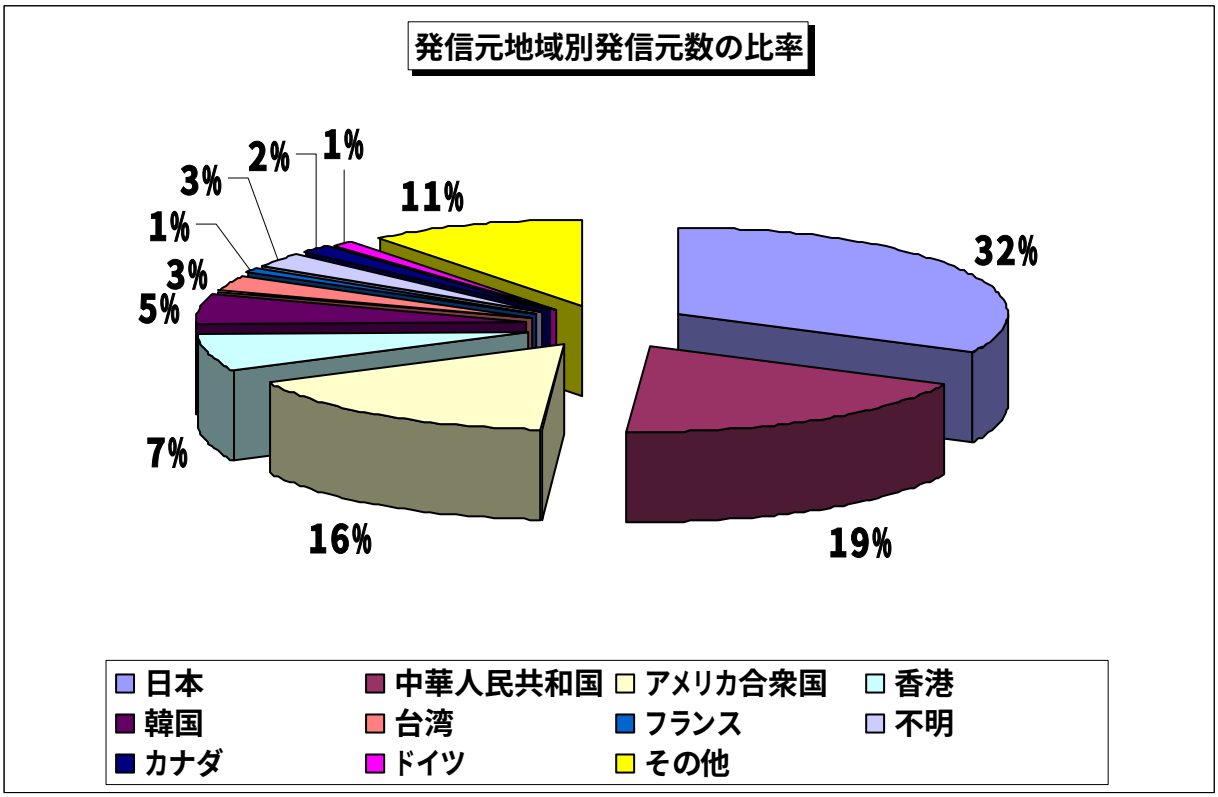


【図 2.4.2 2006 年 6 月の発信元地域別アクセス数の比率】

2006 年 6 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 6 月の発信元地域別発信元数の変化】

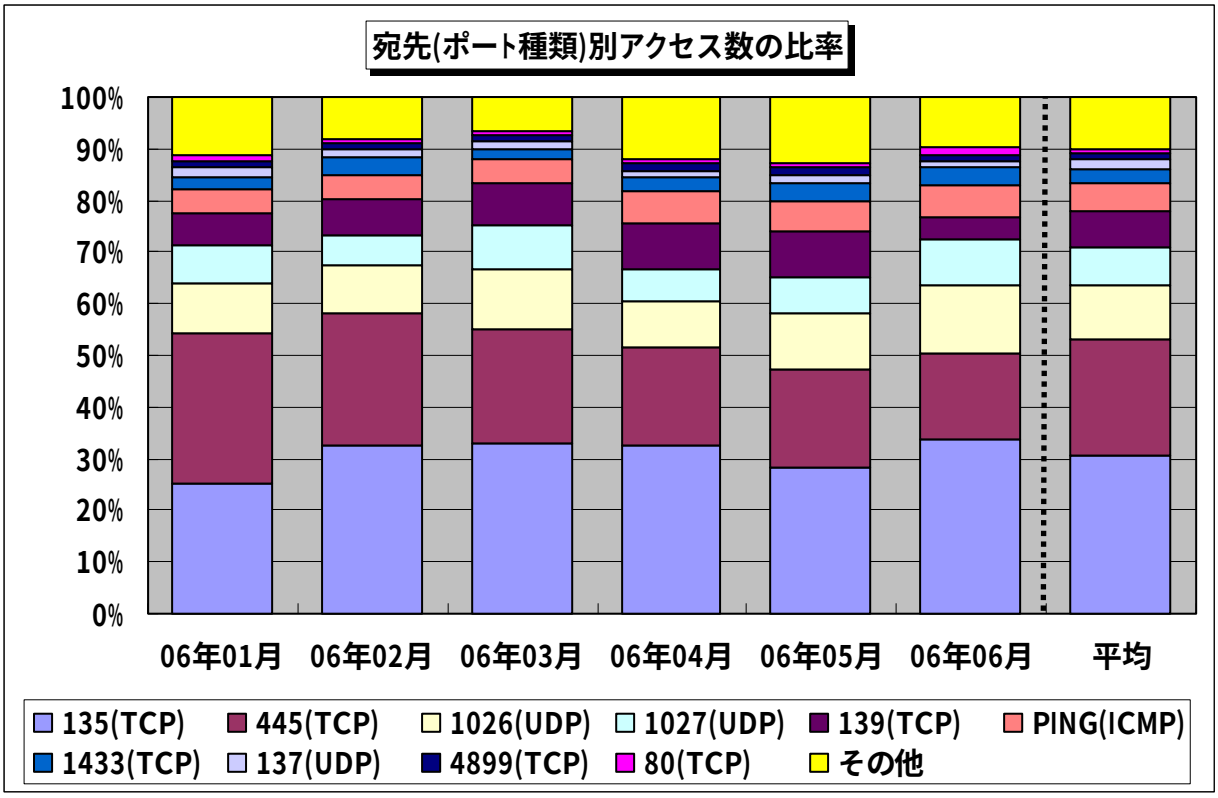


【図 2.4.4 2006 年 6 月の発信元地域別発信元数の比率】

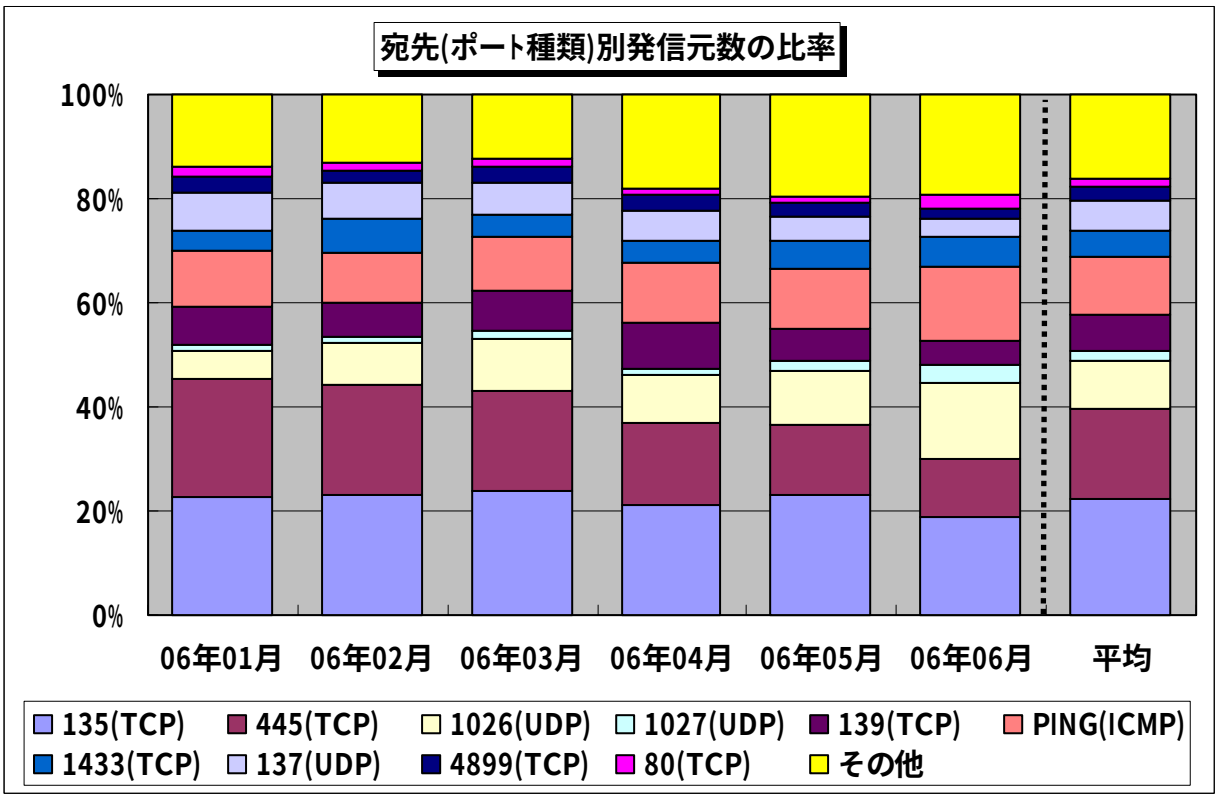
3．統計情報

3.1 2006 年 1 月～2006 年 6 月の宛先(ポート種類)別の比率

2006 年 1 月～2006 年 6 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。



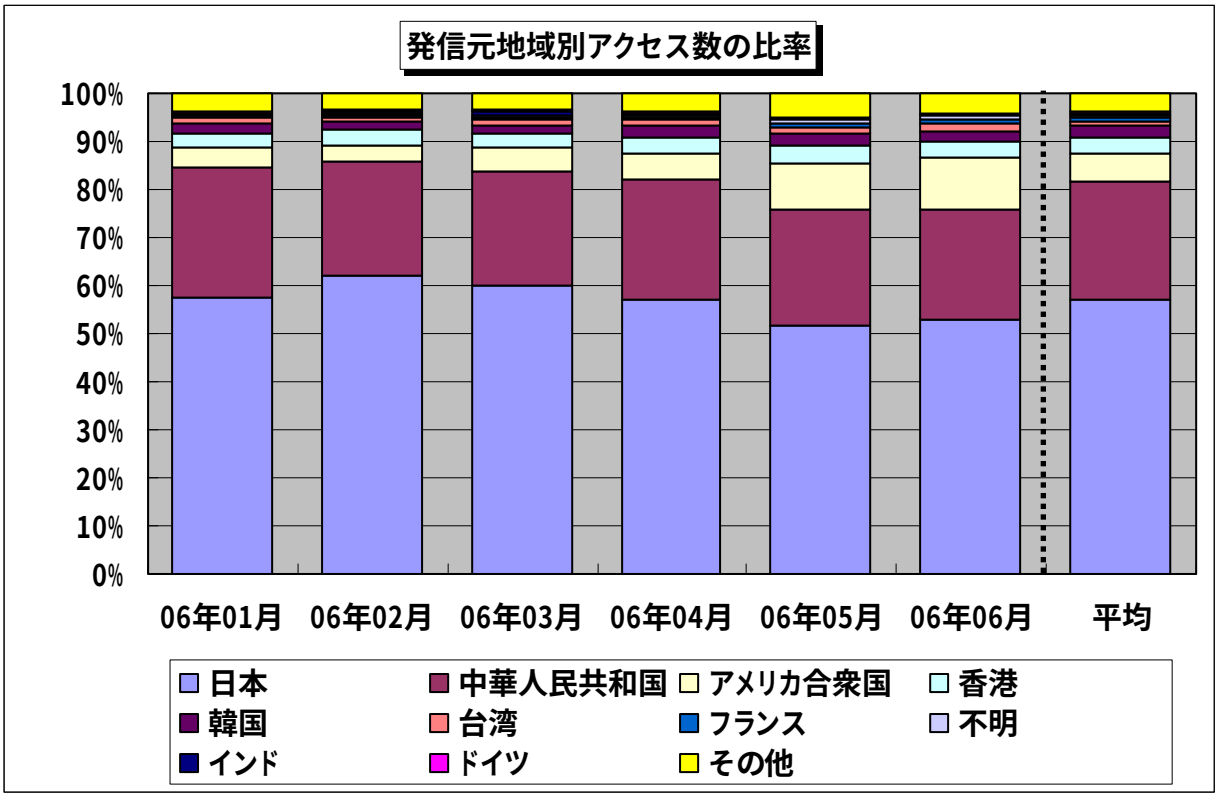
【図 3.1.1 2006 年 1 月～2006 年 6 月の宛先(ポート種類)別アクセス数の比率】



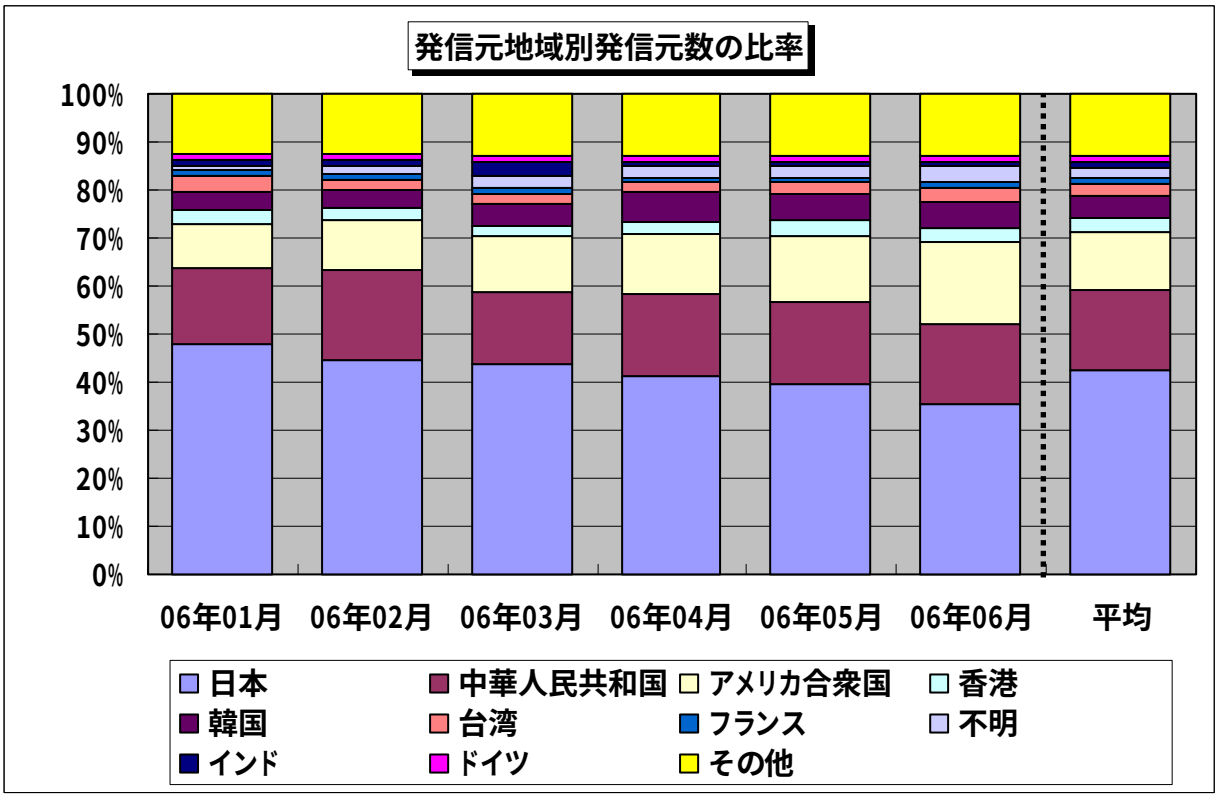
【図 3.1.2 2006 年 1 月～2006 年 6 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 1 月～2006 年 6 月の発信元地域別の比率

2006 年 1 月～2006 年 6 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 6 月の発信元地域別アクセス数の比率】

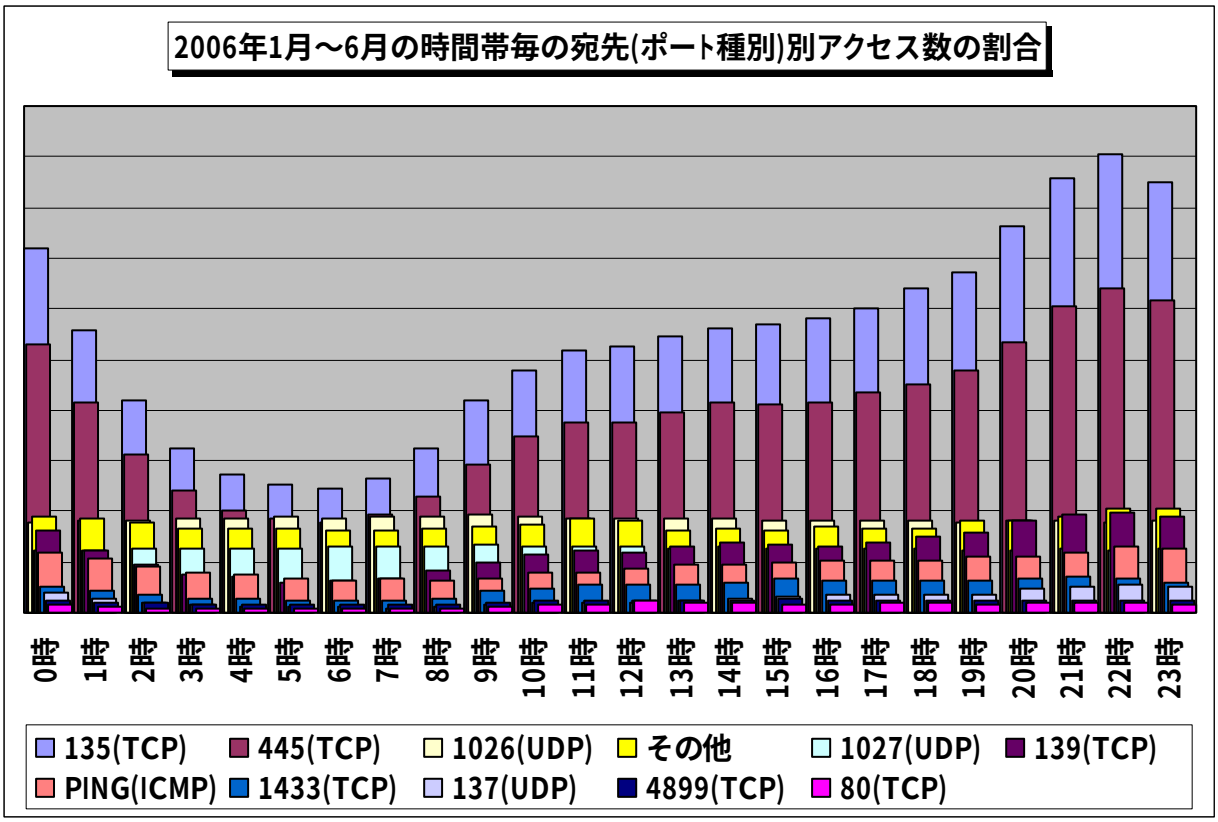


【図 3.2.2 2006 年 1 月～2006 年 6 月の発信元地域別発信元数の比率】

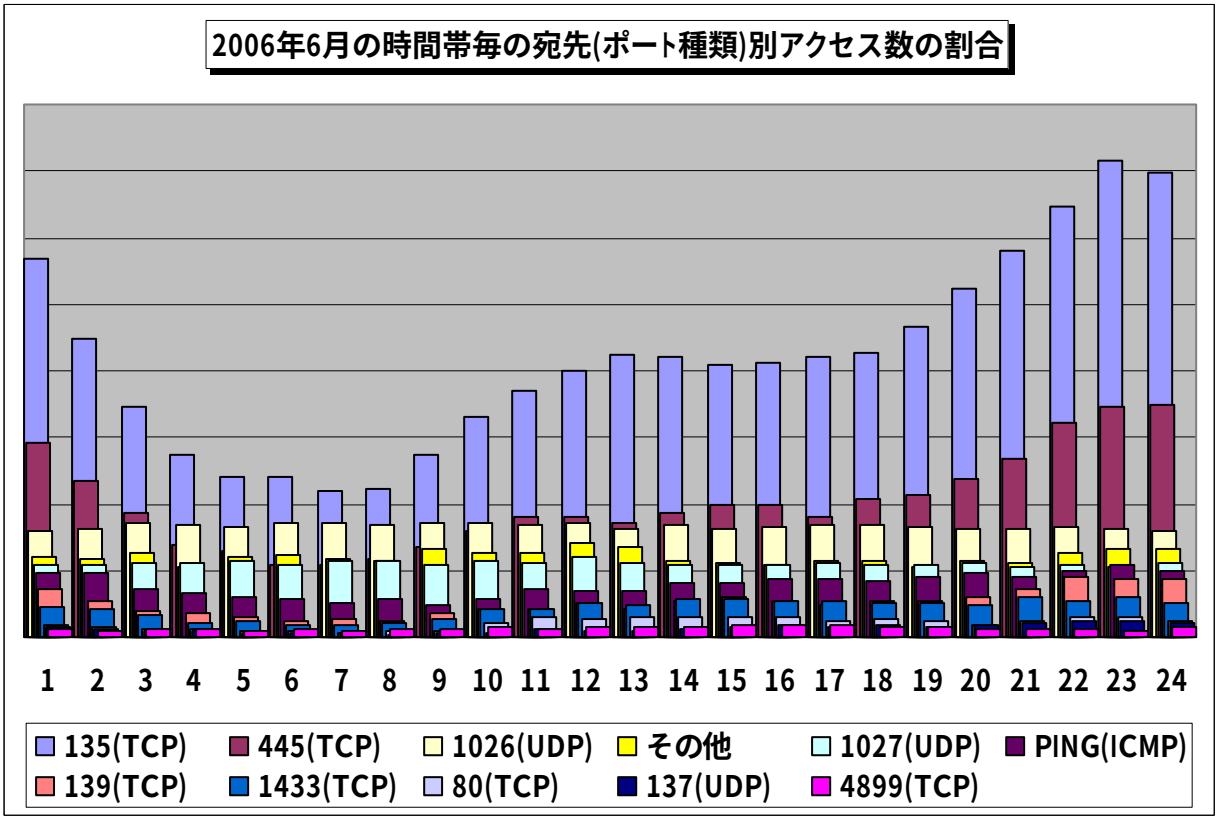
4．その他の統計情報

4.1 2006 年 1 月～6 月の時間帯統計

2006 年 1 月～6 月の宛先(ポート種類)別アクセス数の時間帯統計を図 4.1.1 に、2006 年 6 月の宛先(ポート種類)別アクセス数の時間帯統計を図 4.1.2 に示します。



【図 4.1.1 2006 年 1 月～6 月の宛先(ポート種類)別アクセス数の時間帯統計】



【図 4.1.2 2005 年 6 月の宛先(ポート種類)別アクセス数の時間帯統計】

5．補足説明

以下に、2006 年 6 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
80(TCP)	一般的に Web サイトを閲覧する際に利用されるポートですが、以前からセキュリティ上の脆弱性が多く、CodeRed や Nimda 等による不正アクセスが有名です。最近では、ディレクトリトラバーサル等の Web アプリケーションの脆弱性を狙うものも報告されています。
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)

■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