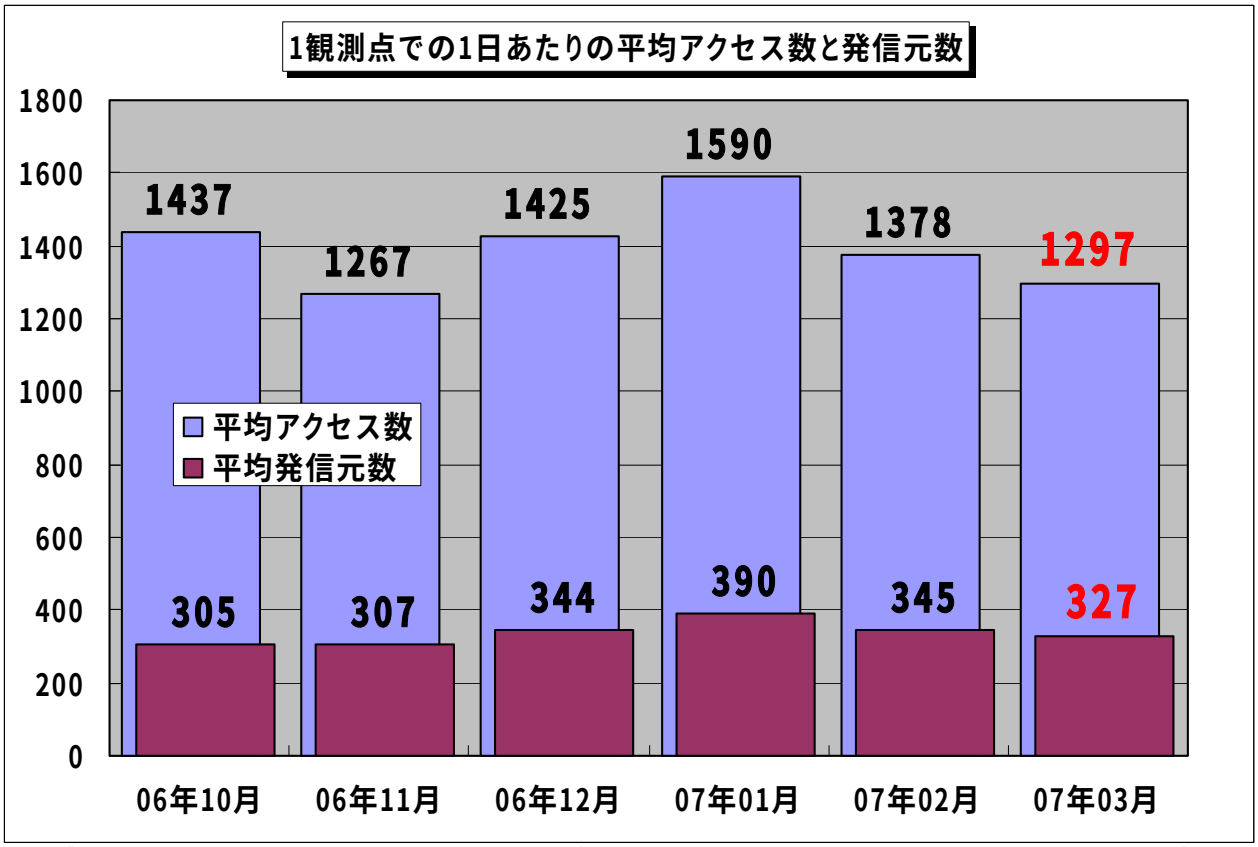
別紙 3

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、2007 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 **402,140 件**ありました。1 観測点で 1 日あたり **327** の発信元から **1,297 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、327 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　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 10 月～2007 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 1.1 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、2007 年 2 月に比べて多少の減少傾向で、ほぼ 2006 年 11 月の状況に戻りました。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。

2．3 月のアクセス状況

2007 年 3 月のアクセス状況は、全体的には 2007 年 2 月とほぼ同じ状況です。ただし、リモートアクセスで操作されるパソコンの脆弱性を突いて攻撃するアクセスは、インシデント事例の報道もあり、さらなる注意が必要です。

2.1 3月の特徴的なアクセス

2.1.1 22/tcp ポートへのアクセス

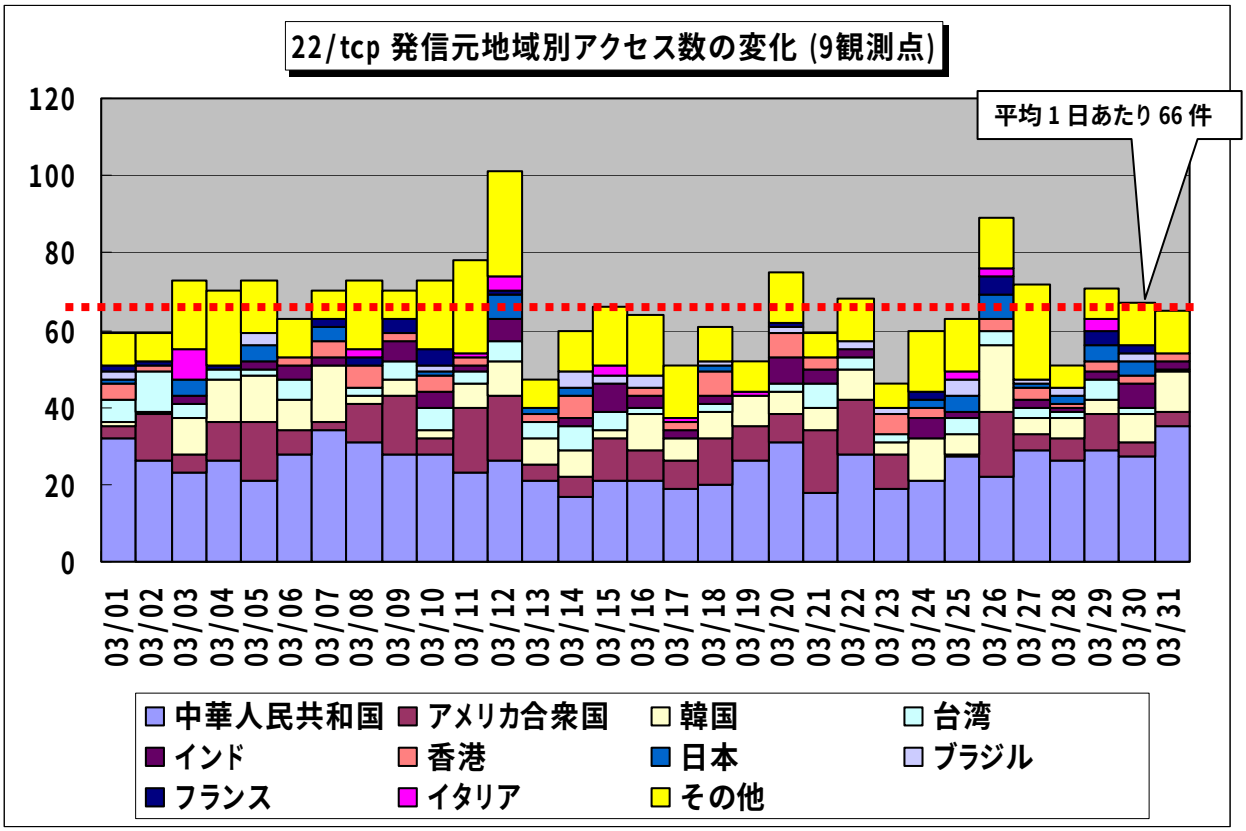
22/tcp へのアクセスは、SSH (Secure Shell) Server を探し出し、脆弱なパスワード認証を破ることを目的としたアクセスであると考えられます。このアクセスに応答するコンピュータに対しては、パスワードを破るためにブルートフォース攻撃や辞書攻撃を仕掛けます。

ブルートフォース攻撃とは、総当り攻撃とも呼ばれ、パスワードを破るためにありとあらゆる解読方法を使用して攻撃する手法です。辞書攻撃とは、パスワードにしやすい単語を登録した辞書を利用した攻撃のことで、辞書攻撃もブルートフォース攻撃の一種である言え、どちらも脆弱な(安易な)パスワード設定の場合は、破られる可能性が高くなります。

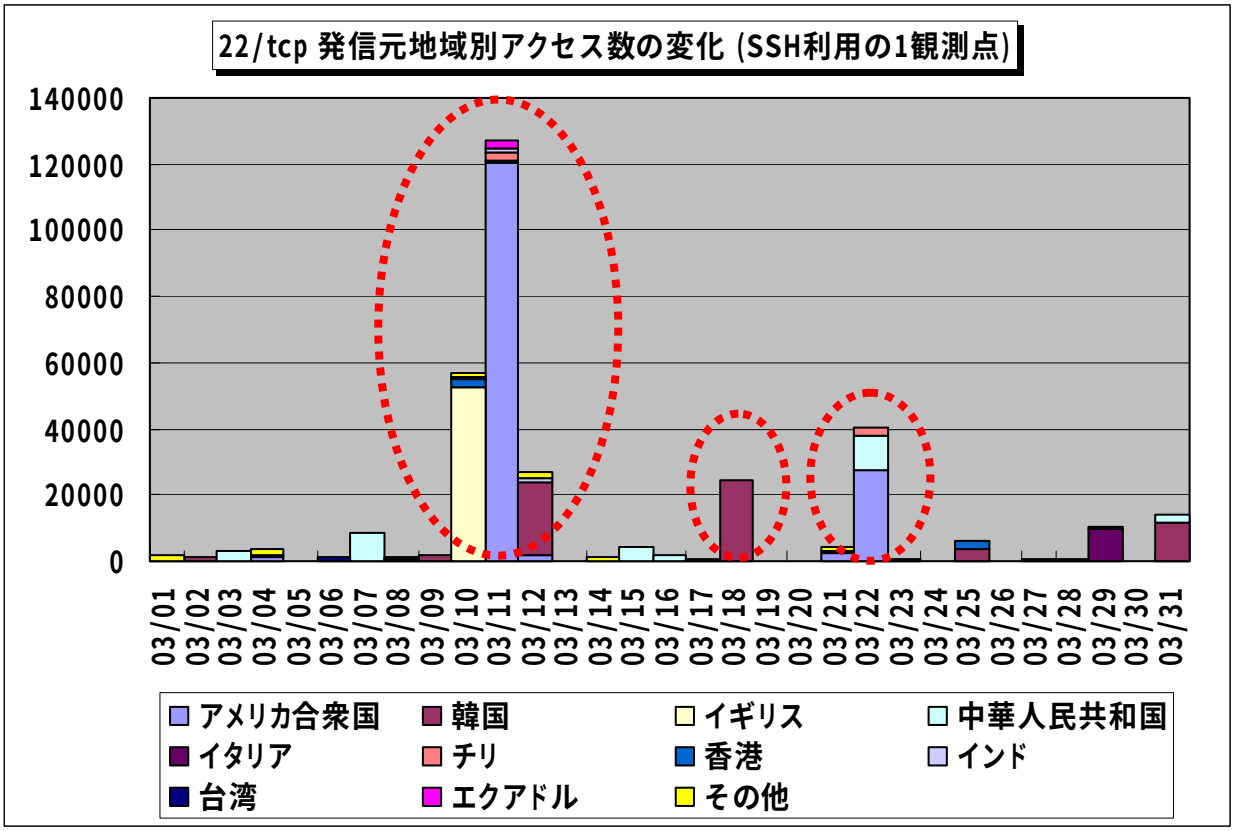
SSH (Secure Shell) を使用している企業では、サーバ等の管理体制とセキュリティポリシーの見直し、監視体制の強化をお願いします。

<参考情報>

■ IPA - セキュアな Web サーバの構築と運用 ～ ユーザ認証
http://www.ipa.go.jp/security/awareness/administrator/secure-web/chap6/6_userauth-1.html



【図 2.1.1.1 22/tcp 発信元地域別アクセス数の変化(9 観測点)】

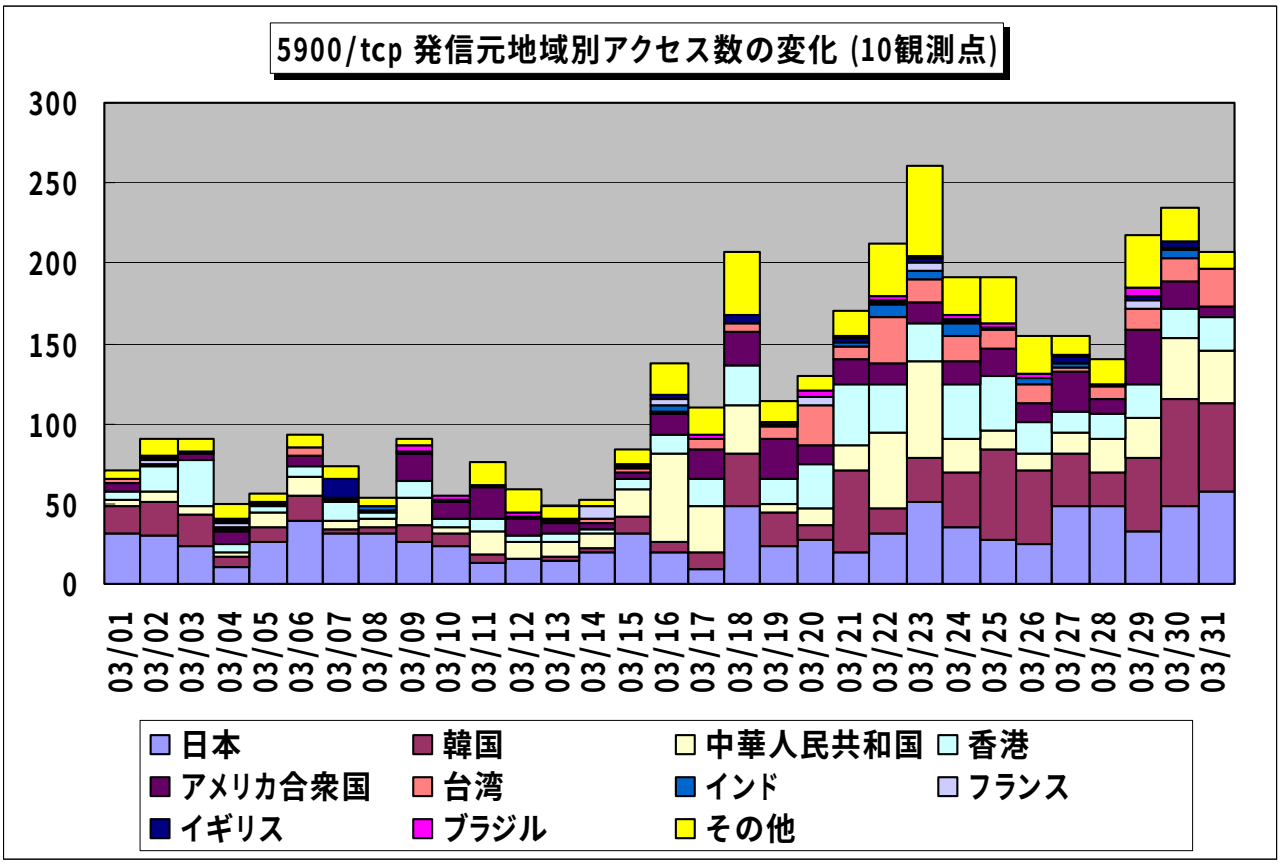


【図 2.1.1.2　22/tcp　発信元地域別アクセス数の変化(SSH 利用の 1 観測点)】

2.1.2 RealVNC のパスワード認証迂回のぜい弱性を狙ったアクセス

22/tcp へのアクセスと同様に、やはりリモートアクセスがらみの攻撃として、5900/tcp へのアクセスが観測されています。5900/tcp ポートは RealVNC サーバへのアクセス用のデフォルトポートであり、これらのアクセスが RealVNC のパスワード認証迂回のぜい弱性を狙ったものであると考えられます。(VNC は Virtual Network Computer の略)

月の中旬から増加傾向のアクセスでありますが、このぜい弱性狙いのアクセスも 2006 年 5 月の攻撃コードの公開から続くなじみのもので、やはりボットに組み込まれたぜい弱性狙いの感染活動コードによるものと考えられます。



【図 2.1.2　RealVNC のパスワード認証迂回のぜい弱性を狙ったアクセス】

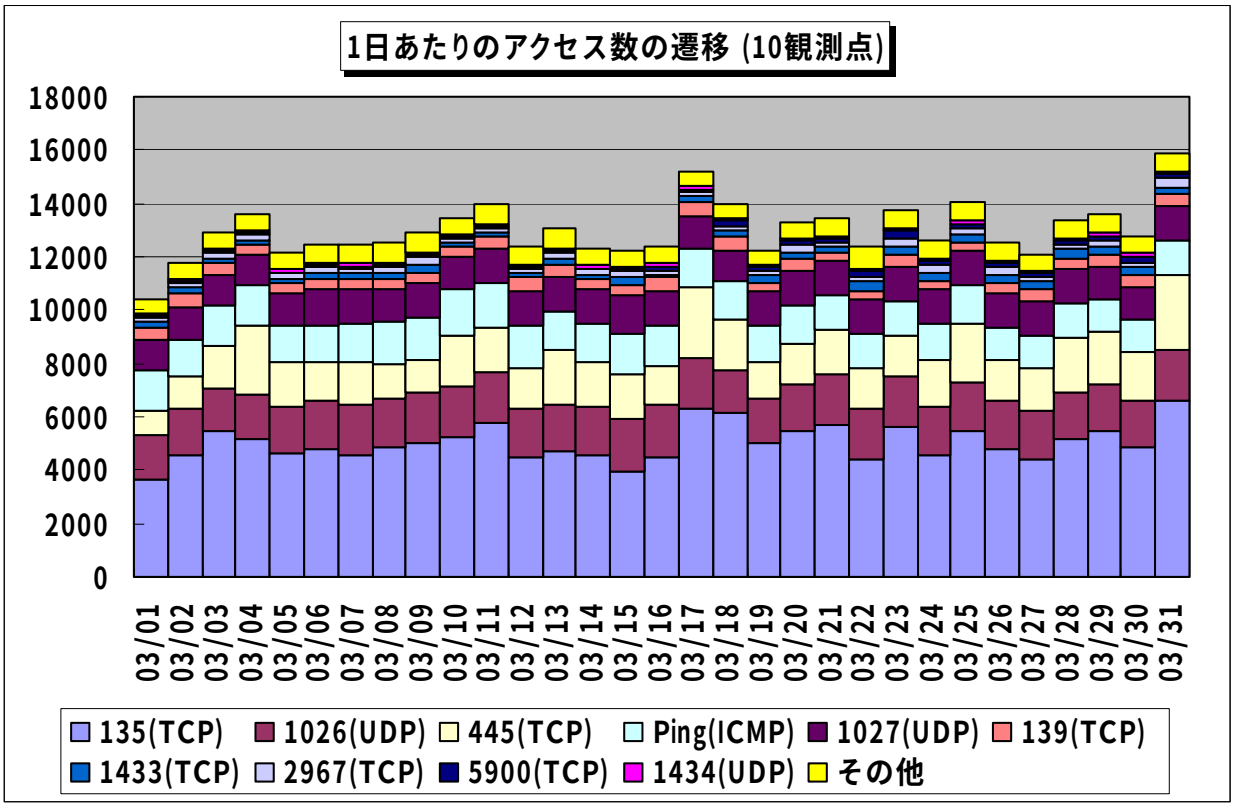
<参考情報>

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

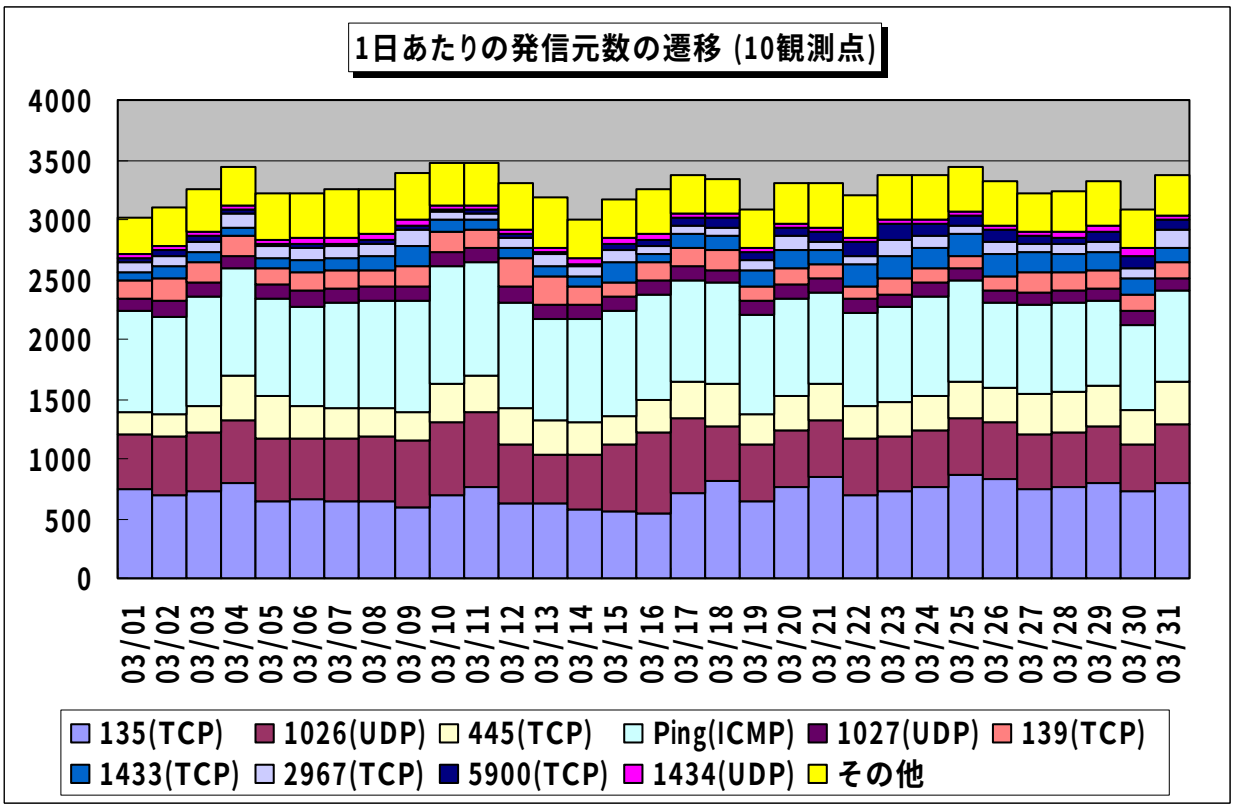
■ RealVNC サーバの認証が回避される脆弱性に関する注意喚起
http://www.jpcert.or.jp/at/2006/at060005.txt

2.2 2007 年 3 月の一方的なアクセス状況

2007 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。



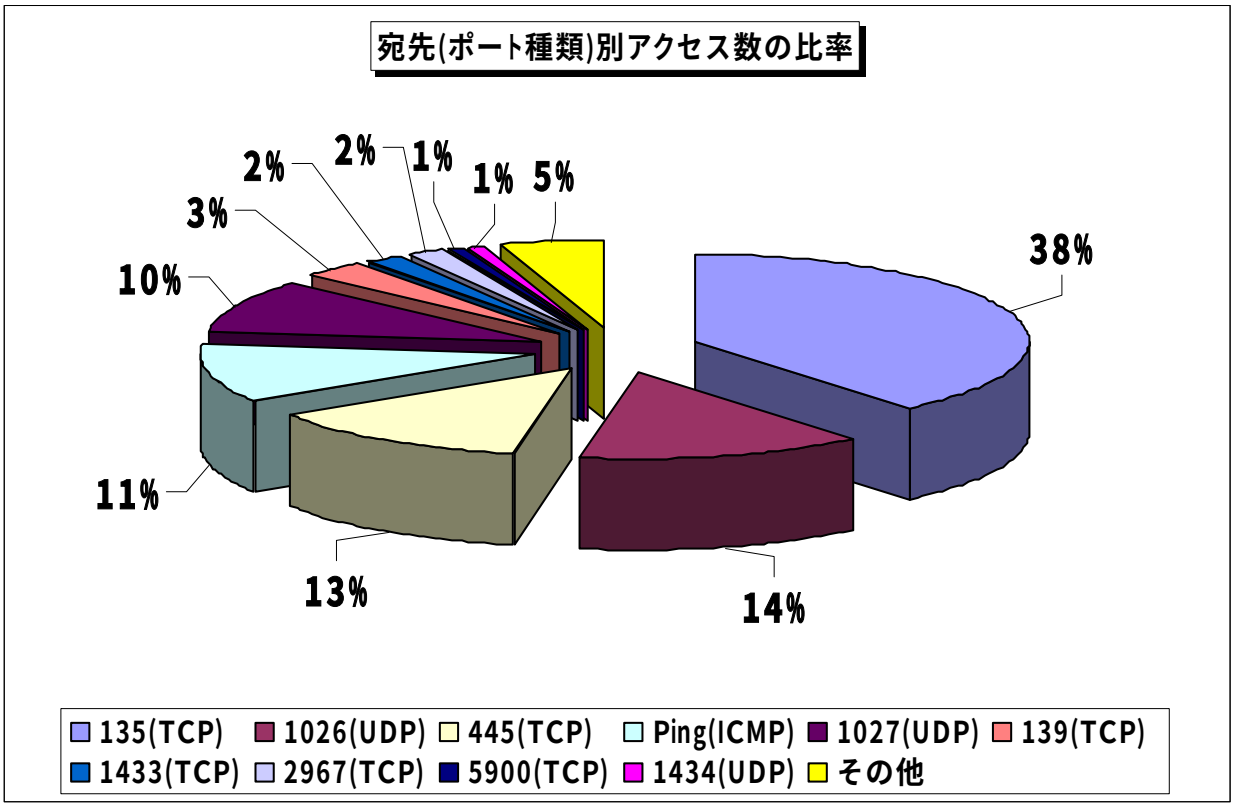
【図 2.2.1 2007 年 3 月の一方的なアクセス状況(アクセス数)】



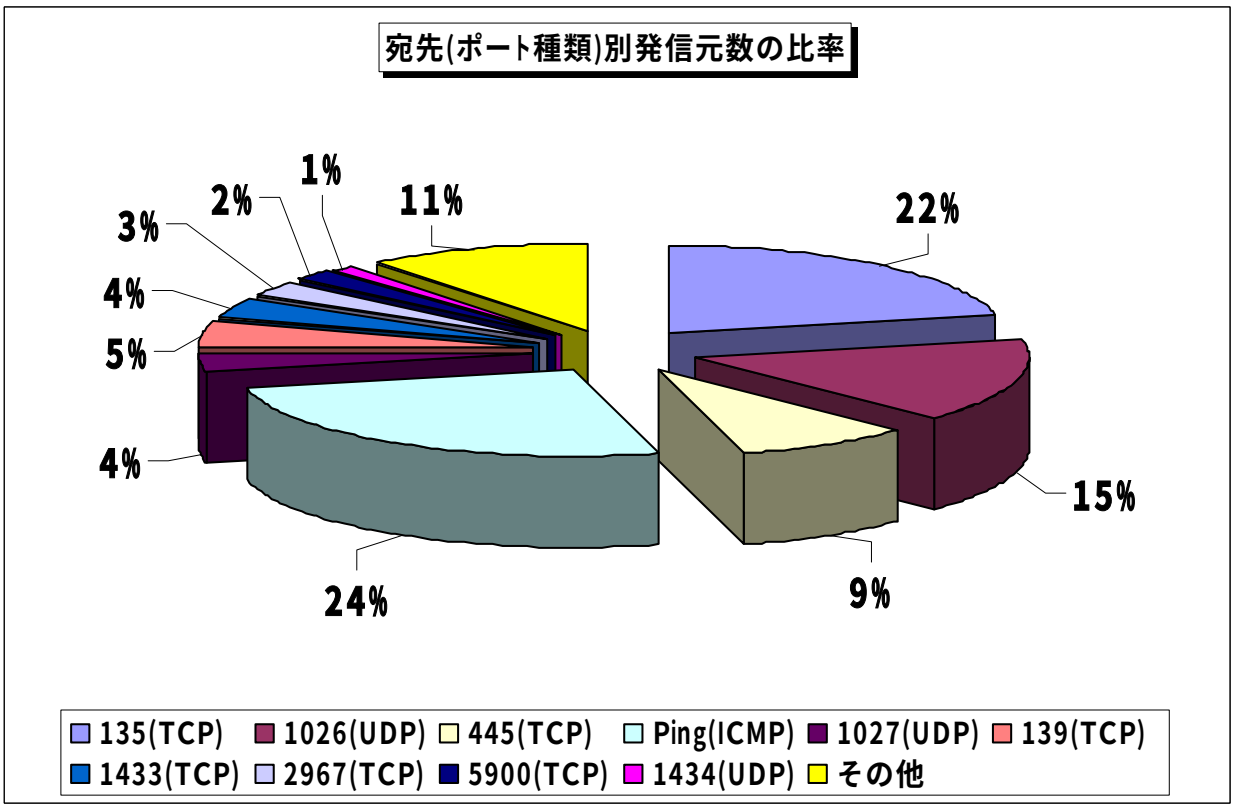
【図 2.2.2 2007 年 3 月の一方的なアクセス状況(発信元数)】

2.3 2007 年 3 月の宛先(ポート種類)別の比率

2007 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。



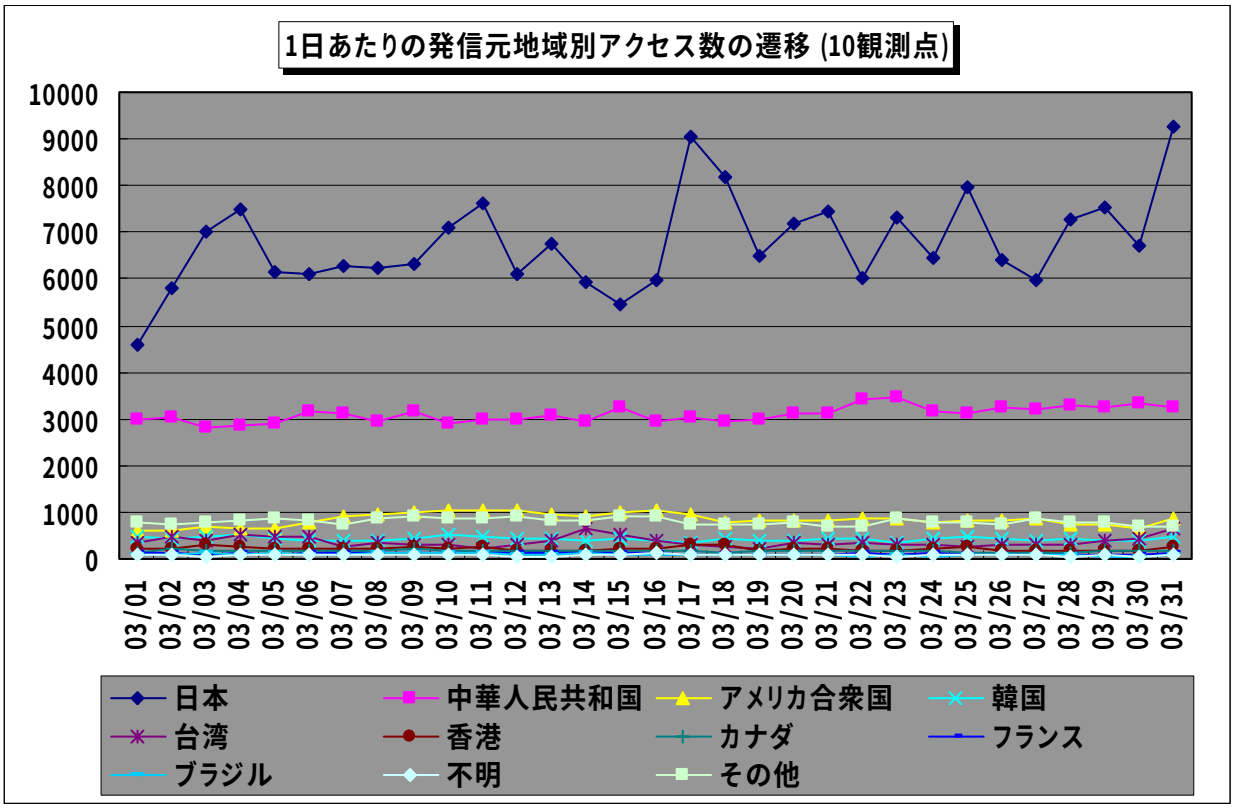
【図 2.3.1 2007 年 3 月の宛先(ポート種類)別アクセス数の比率】



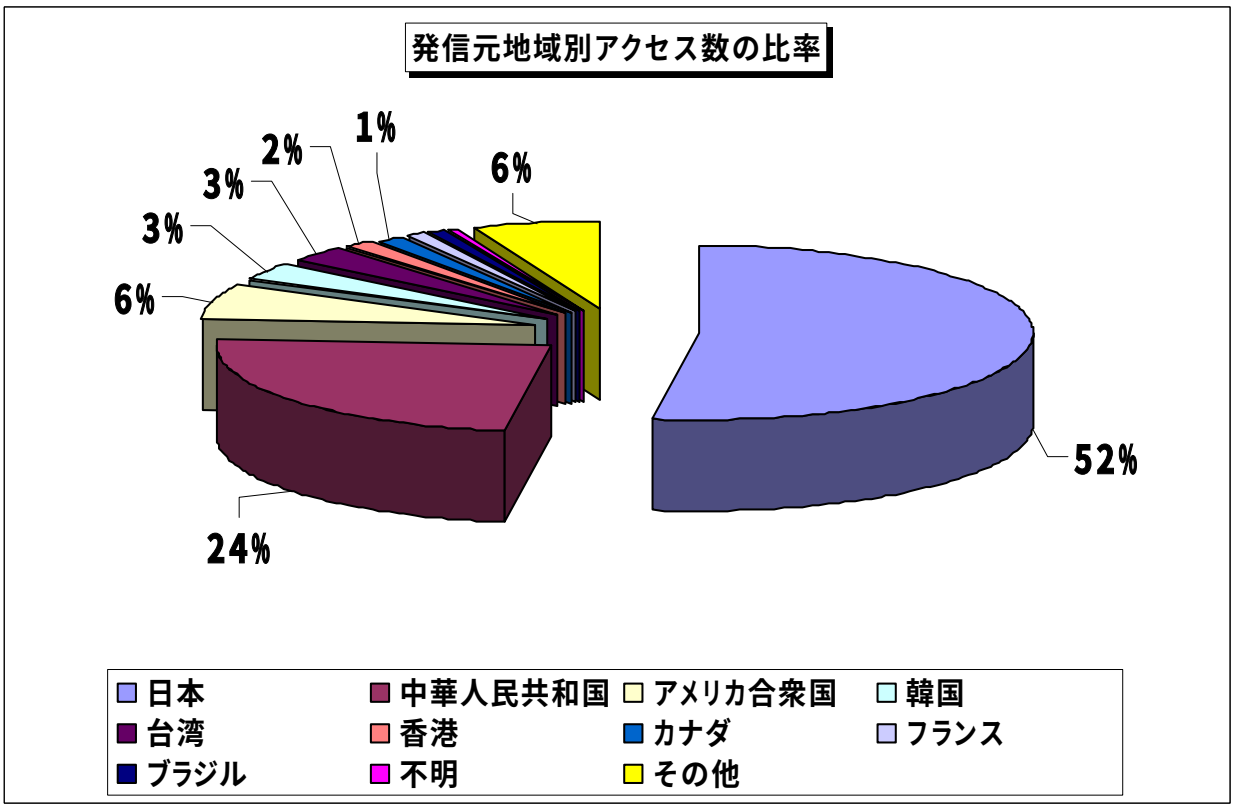
【図 2.3.2 2007 年 3 月の宛先(ポート種類)別発信元数の比率】

2.4 2007 年 3 月の発信元地域別アクセス状況

2007 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。

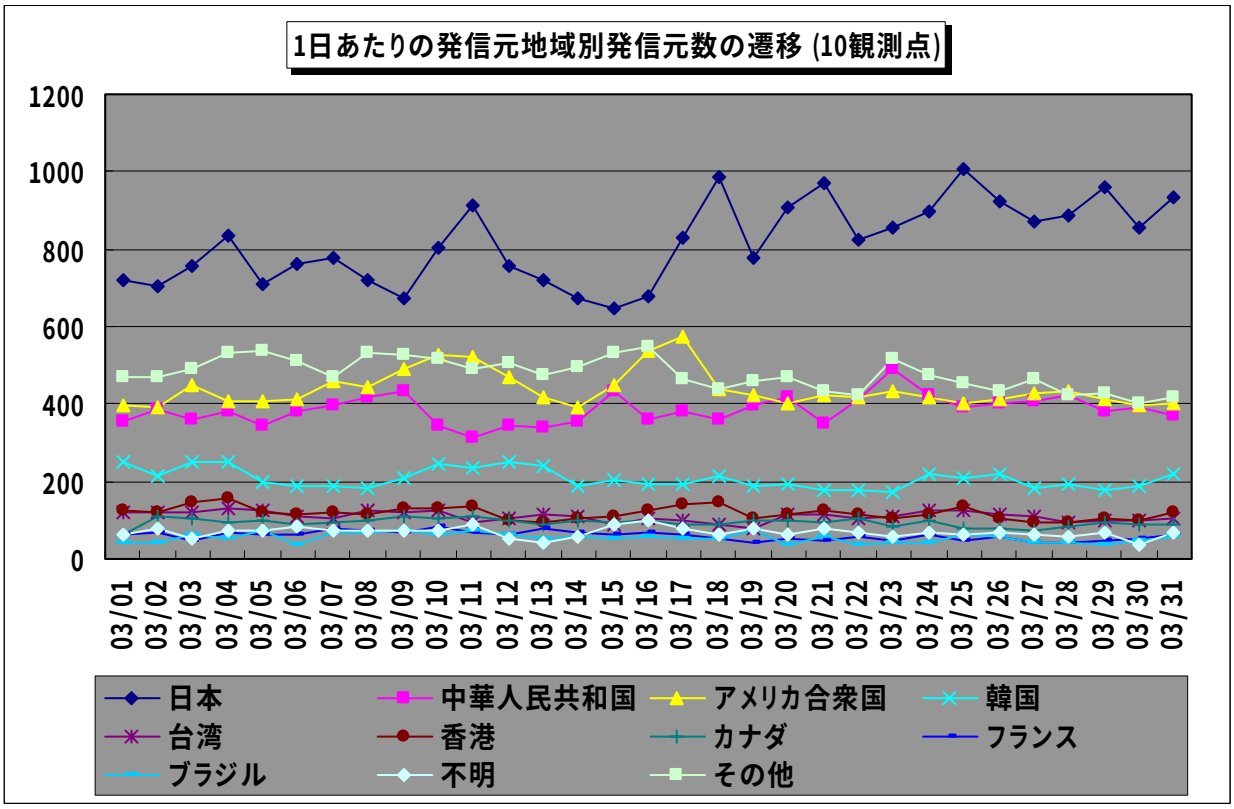


【図 2.4.1 2007 年 3 月の発信元地域別アクセス数の変化】

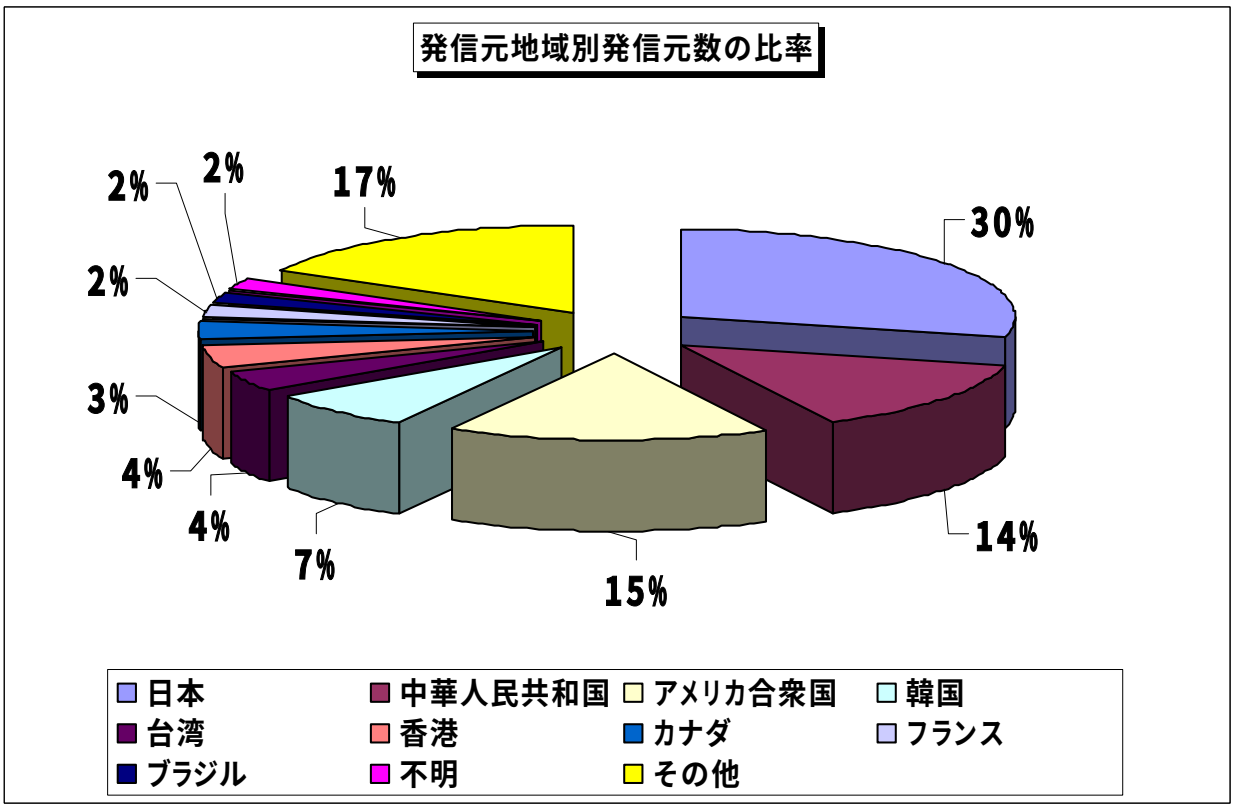


【図 2.4.2 2007 年 3 月の発信元地域別アクセス数の比率】

2007 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 2.3.4 に示します。



【図 2.4.3 2007 年 3 月の発信元地域別発信元数の変化】

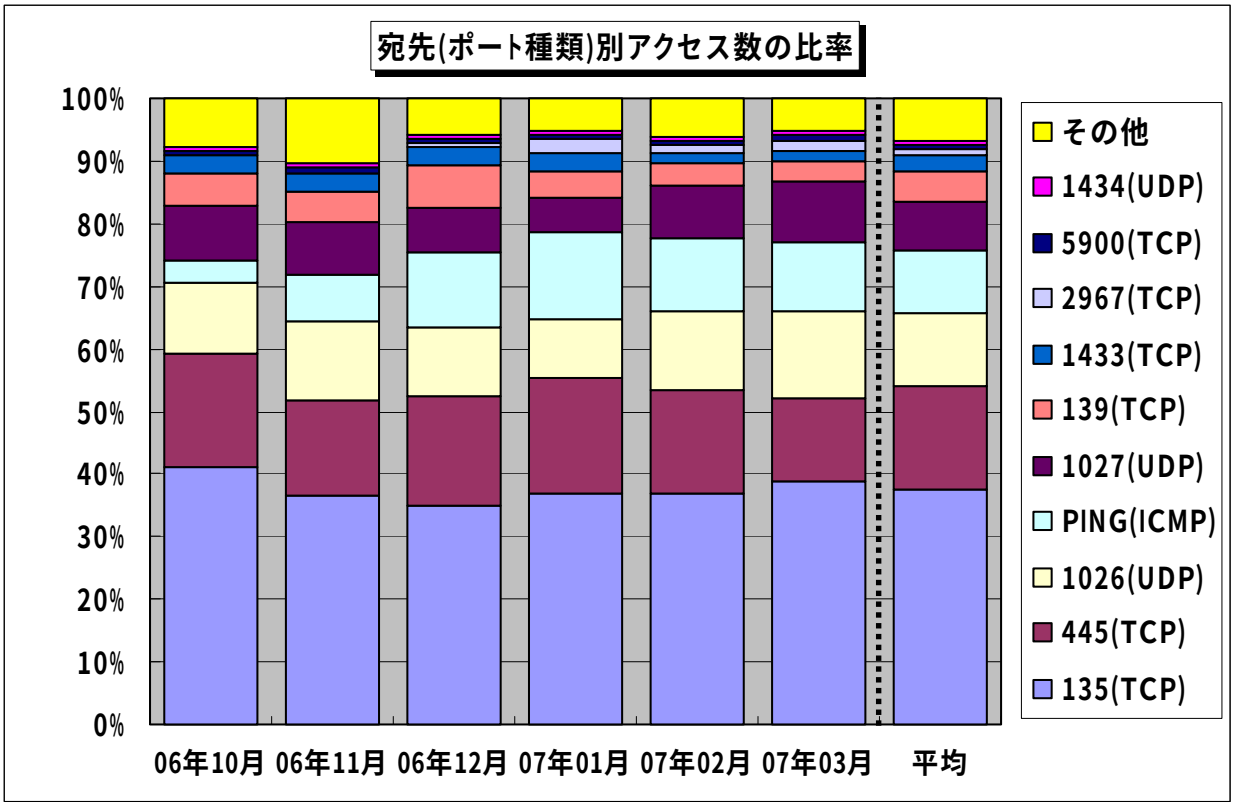


【図 2.4.4 2007 年 3 月の発信元地域別発信元数の比率】

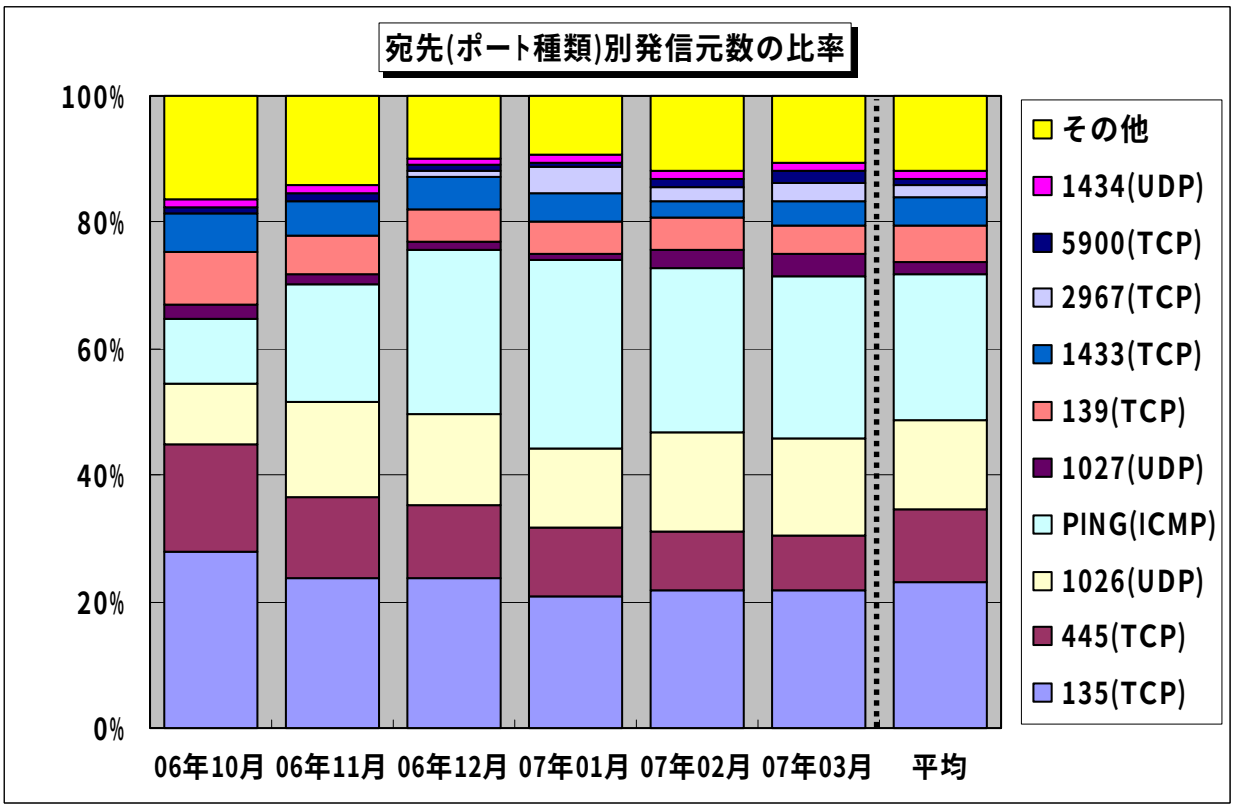
3．統計情報

3.1 2006 年 10 月～2007 年 3 月の宛先(ポート種類)別の比率

2006 年 10 月～2007 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。



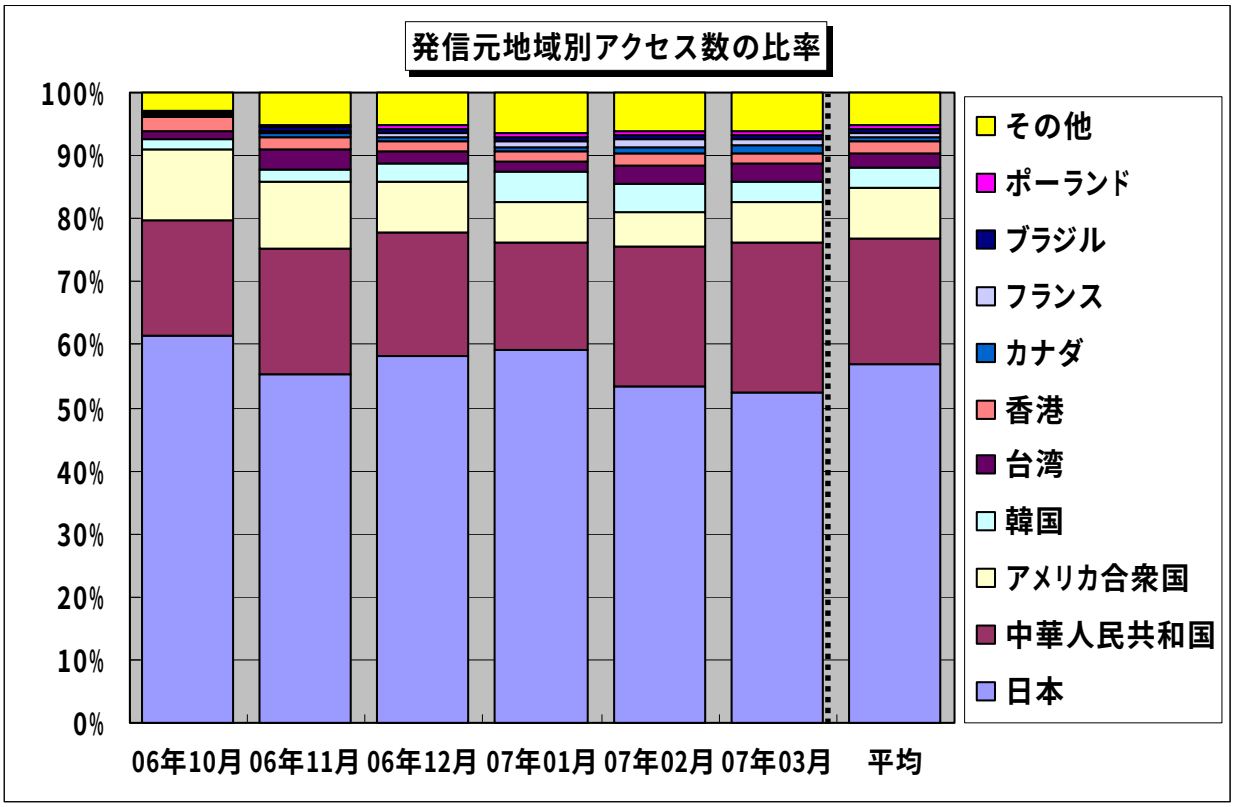
【図 3.1.1 2006 年 10 月～2007 年 3 月の宛先(ポート種類)別アクセス数の比率】



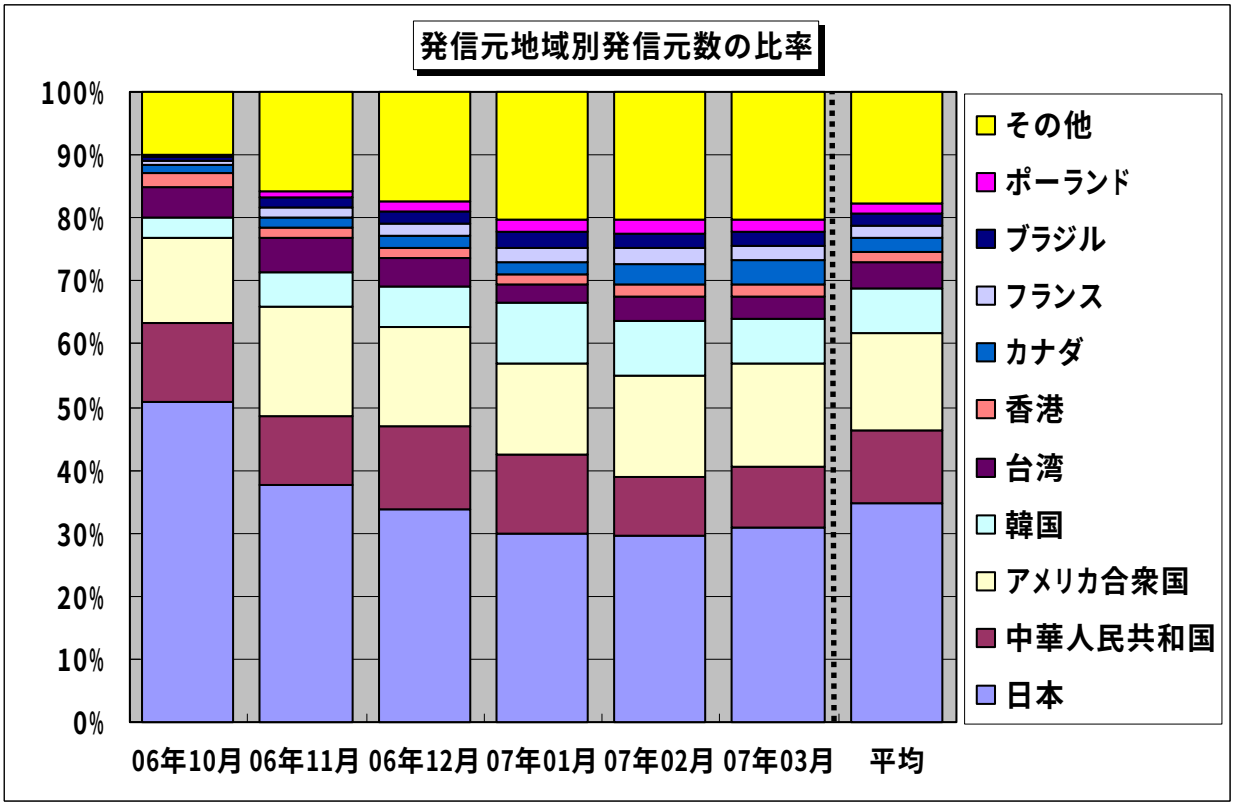
【図 3.1.2 2006 年 10 月～2007 年 3 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 10 月～2007 年 3 月の発信元地域別の比率

2006 年 10 月～2007 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 2006 年 10 月～2007 年 3 月の発信元地域別アクセス数の比率】



【図 3.2.2 2006 年 10 月～2007 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、2007 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 に関するぜい弱性(MS03-026)を狙った不正アクセスが有名(W32/MSBlaster 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
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)
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
2967(TCP)	Symantec Client Security や Symantec AntiVirus がデフォルトで使用するポートで、今回のアクセスはこれらの製品のぜい弱性を狙ったものと考えられます
5900(TCP)	リモートアクセスツール RealVNC のぜい弱性を狙っていると思われるアクセスです
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／宮本
Tel:03-5978-7527 Fax:03-5978-7518
E-mail:isec-info@ipa.go.jp