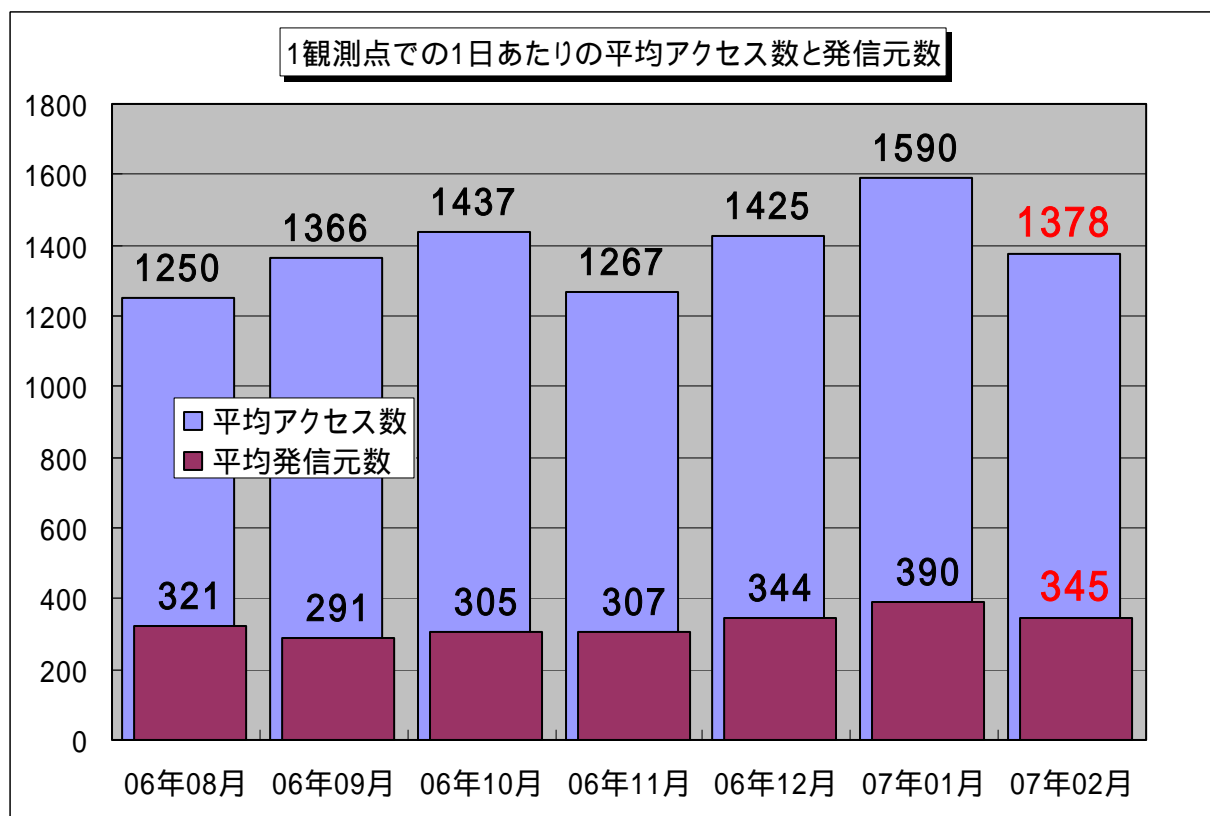


インターネット定点観測(TALOT2)での観測状況について

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2月の期待しない(一方的な)アクセスの総数は、10観測点で330,685件ありました。1観測点で1日あたり345の発信元から1,378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、345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**ということになります。



【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8月～2007年2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1月に比べて多少の減少傾向で、ほぼ2006年12月の状況に戻りました。この減少傾向は、Ping(ICMP)の安定化およびコンピュータの脆弱性を狙ったアクセスの安定化が原因と思われます。

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、ボットに感染したコンピュータからのボット感染活動(コンピュータのぜい弱性を狙い、ボットの感染を広げようとしているアクセス)のためのアクセスが主流であると考えられます。

Internet Control Message Protocol : 相手のコンピュータが動作中であるか、調べる為のプロトコル

2.2月のアクセス状況

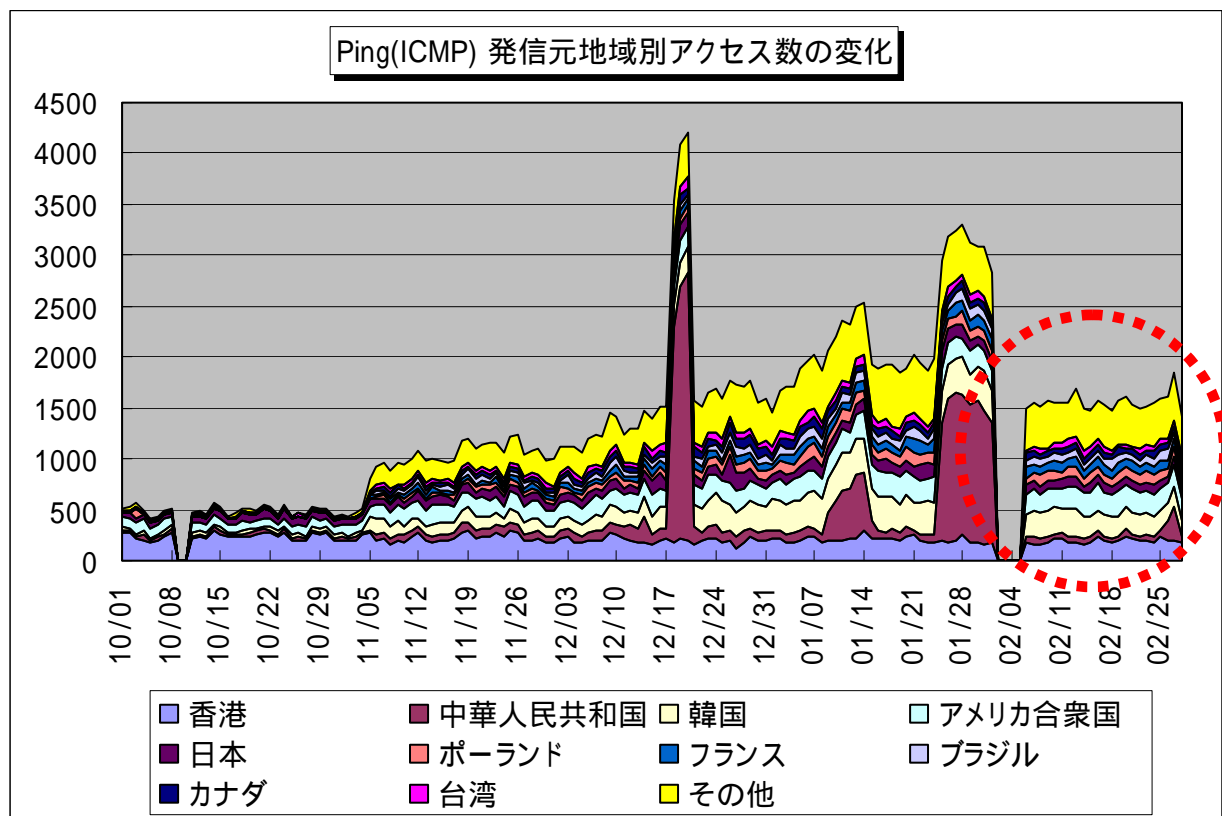
2007年2月のアクセス状況は、全体的には2007年1月とほぼ同じ状況ですが、前述したように Ping(ICMP)アクセスの安定化傾向、Symantec 社の Symantec Client Security および Symantec AntiVirus のぜい弱性を狙ったアクセス(2967/tcp ポートへのアクセス)の減少傾向が見られ、ボットの感染活動が頭打ちになってきたと考えられます。

2007年2月は、月初に TALOT2 システムのメンテナンスのため、2日～5日まで観測データがありませんが、この期間内にアクセスが安定化したようです。

2.1 2月の特徴的なアクセス

2.1.1 Ping(ICMP)アクセス

TALOT2 では、一方的なインターネットからアクセスを観測している関係上、Ping(ICMP)への応答は行っていません。そのため、これらの Ping(ICMP)に回答した場合の、それ以降のアクセスについて観測することができませんが、攻撃対象のコンピュータが動作しているか確認するためのアクセスと考えられます。



【図 2.1.1 2007年1月～2月の Ping(ICMP)アクセス】

図 2.1.1 は、Ping(ICMP)の発信元地域別アクセス数の変化を示していますが、2006年11月以降の増加傾向および中国方面からの一時的な増加を示していますが、2007年1月の中国方面からのアクセス増加が、2月6日以降は無くなりました。他の発信元地域からのアクセスを含めて、増加傾向は安定方向へ移行しつつあるようです。これらのアクセスの原因は不明ですが、脅威は依然として続いています。

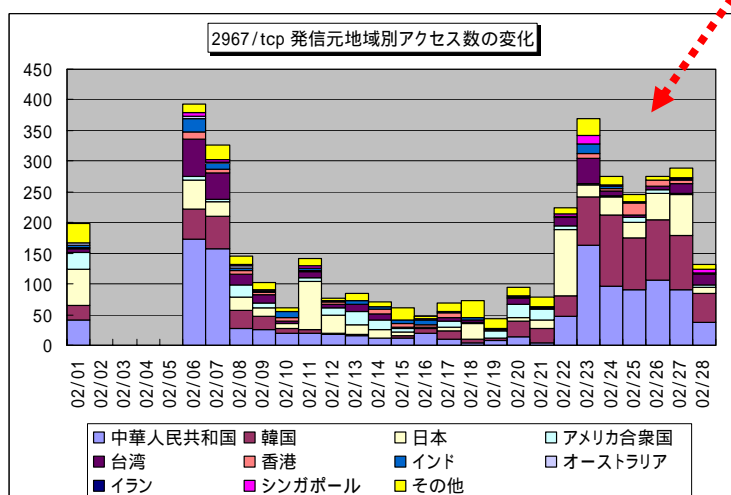
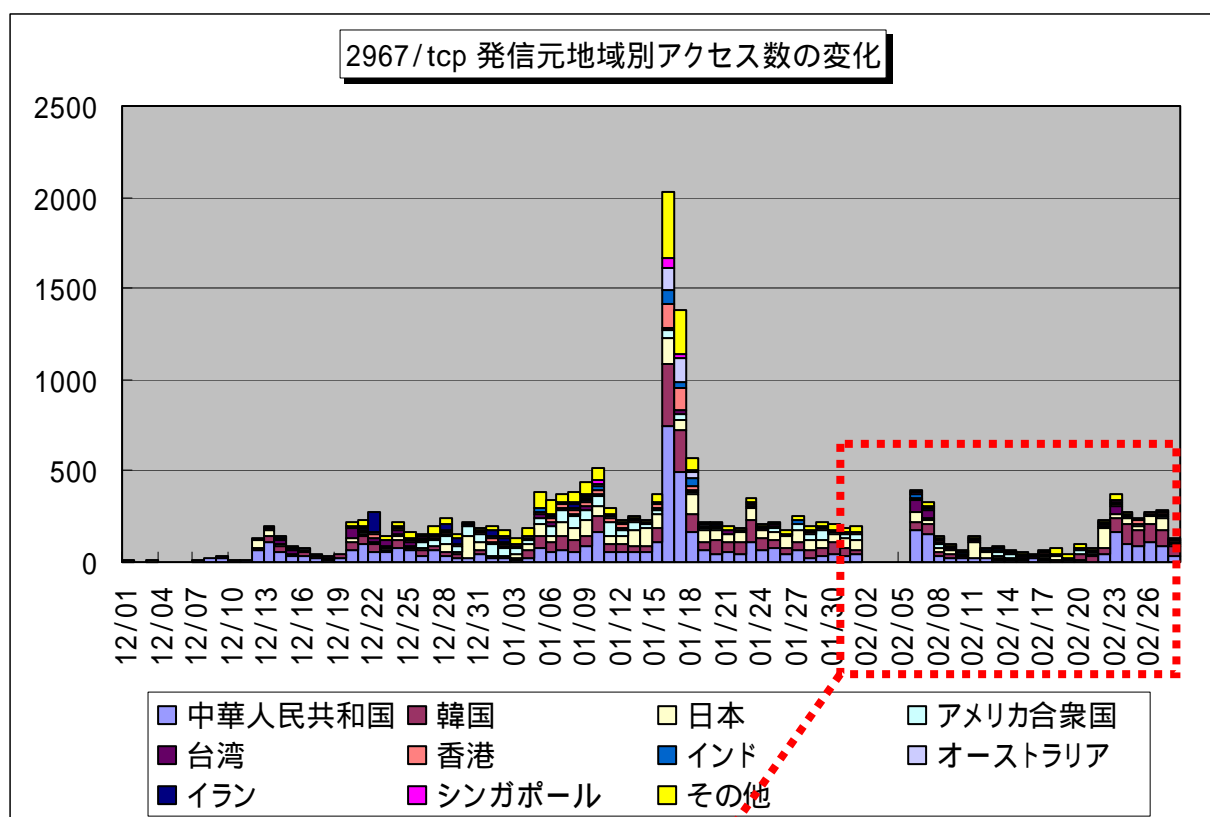
2.1.2 2967/tcp ポートへのアクセス

2967/tcp ポートは、Symantec Client Security や Symantec AntiVirus がデフォルトで使用するポートです。2006 年 5 月 25 日発表の『Symantec 社の Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性(SYM06-010)』が狙われている可能性が高いようです。実際にワームを捕らえて、解析しているセキュリティベンダもあるようです。

2967/tcp ポートへのアクセスは、2006 年 12 月初旬から目立つようになってきましたが、2 月 8 日前後から一定水準で安定してきたようでしたが、22 日頃から、また増加しています。このアクセスに関しても、ぜい弱性への対策が広く普及したことにより感染活動が頭打ちとなったと考えていましたが、脅威は依然として続いています。

Symantec 社の Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性(SYM06-010) 2006 年 5 月 25 日発表

<http://www.symantec.com/region/jp/avcenter/security/content/2006.05.25.html>



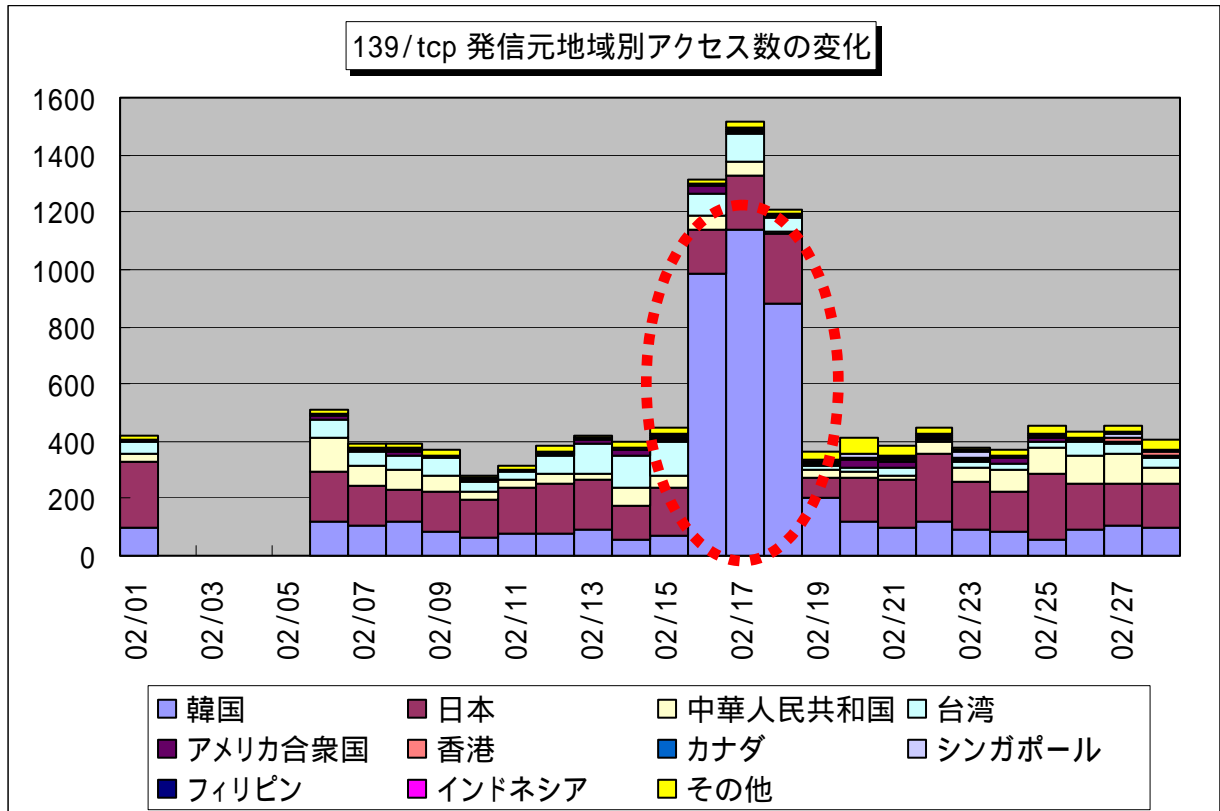
【図 2.1.2 Symantec 社製品のぜい弱性を狙っていると思われるアクセス】

2.1.3 139/tcp ポートへのアクセス

139/tcp ポートへのアクセスは、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、1月のような他のぜい弱性を狙ったアクセスと組み合わせられた攻撃でない、単一の攻撃が一時的に観測されました。

この一時的な増加は、ほとんどが韓国方面からのものであり、韓国方面に構築された特定のボットネットワークから発信されたものと考えられます。

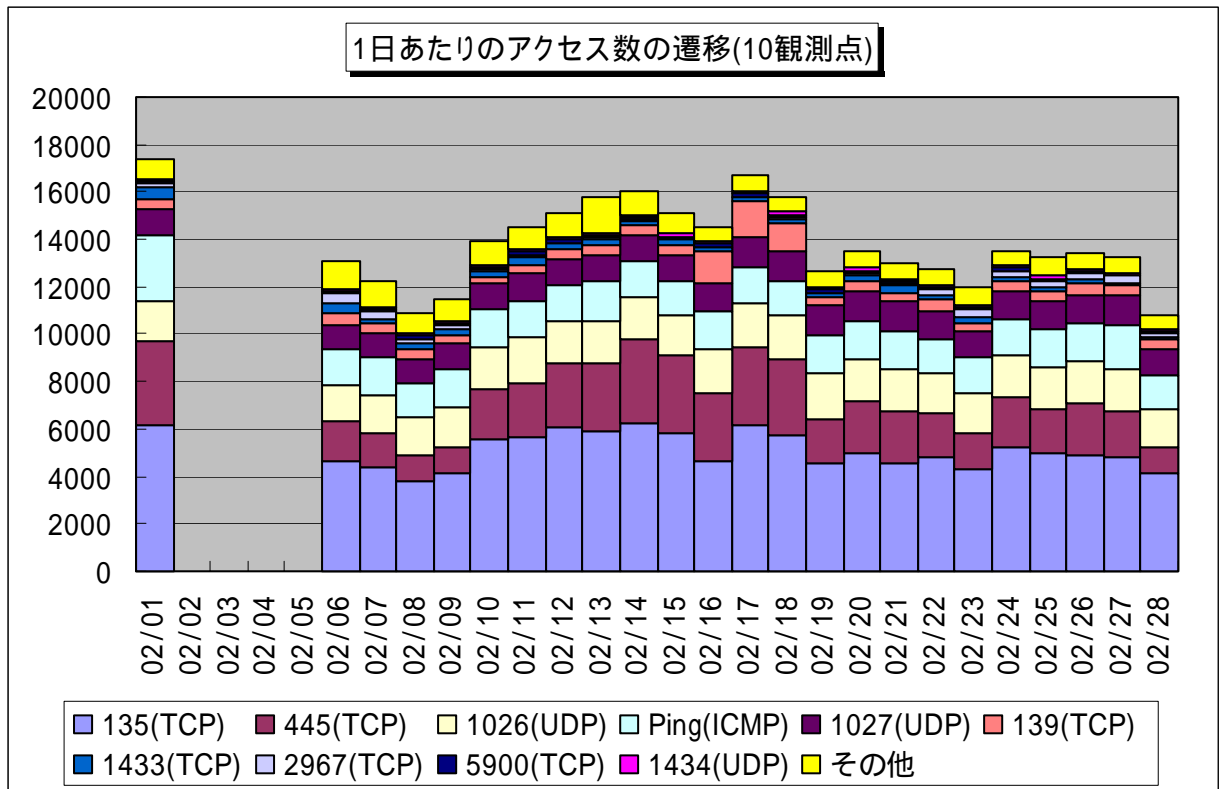
ただし、一時的なものであり、このポートが狙われるような新たなぜい弱性も発表されていないので、大きな脅威として考える必要はないと思われます。



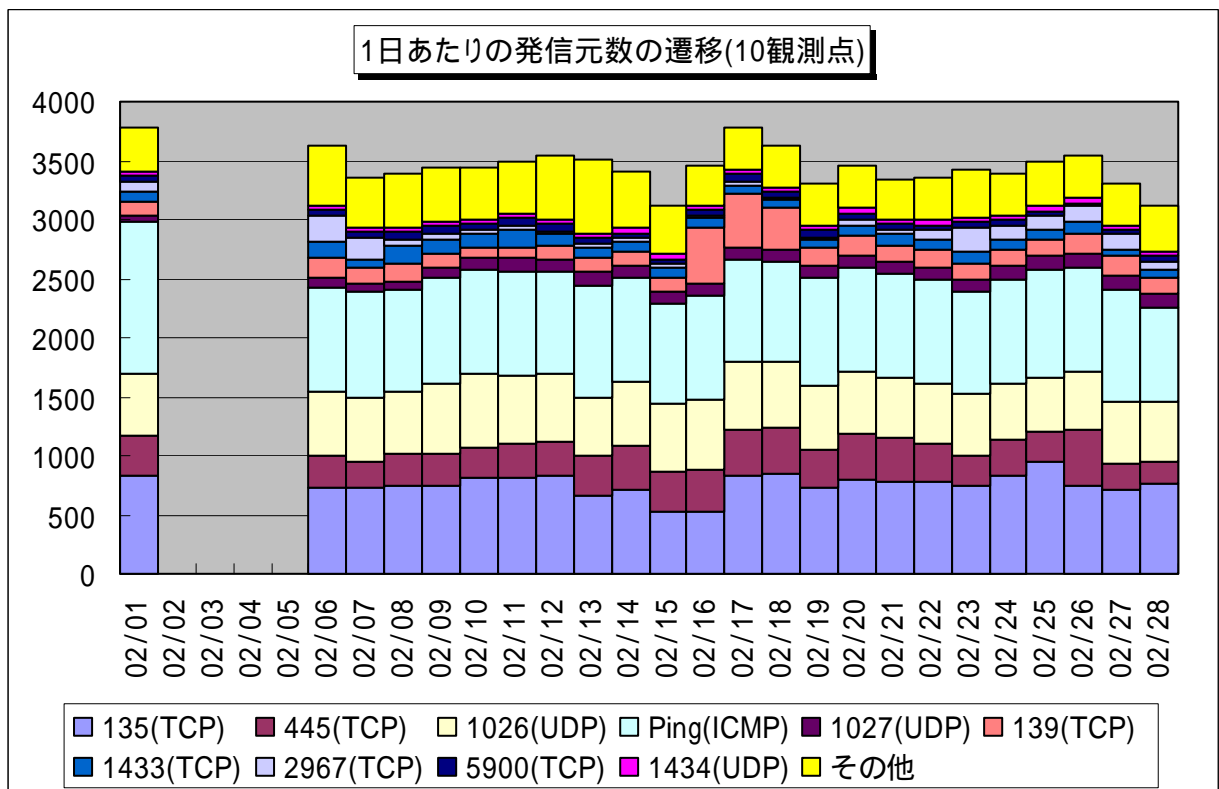
【図 2.1.3 139/tcp ポートへの発信元地域別アクセス数の変化】

2.2 2007年2月の一方的なアクセス状況

2007年2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。



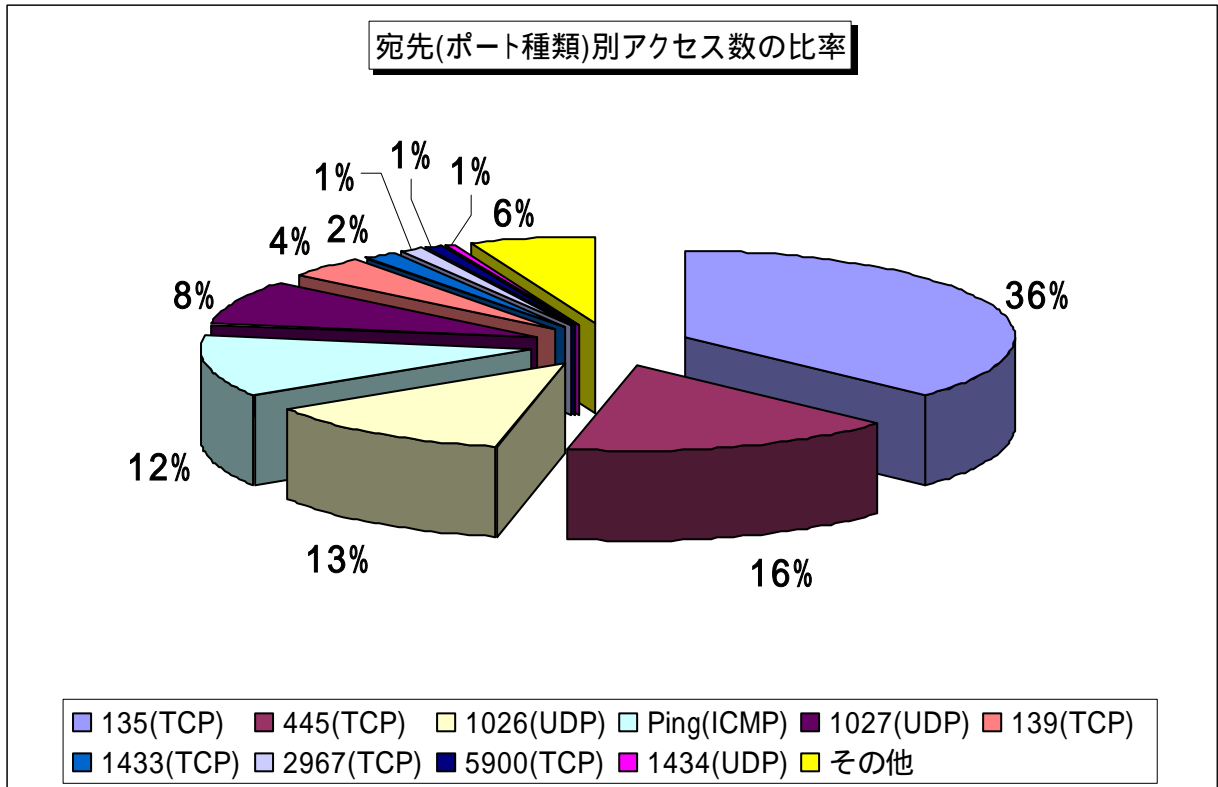
【図 2.2.1 2007年2月の一方的なアクセス状況(アクセス数)】



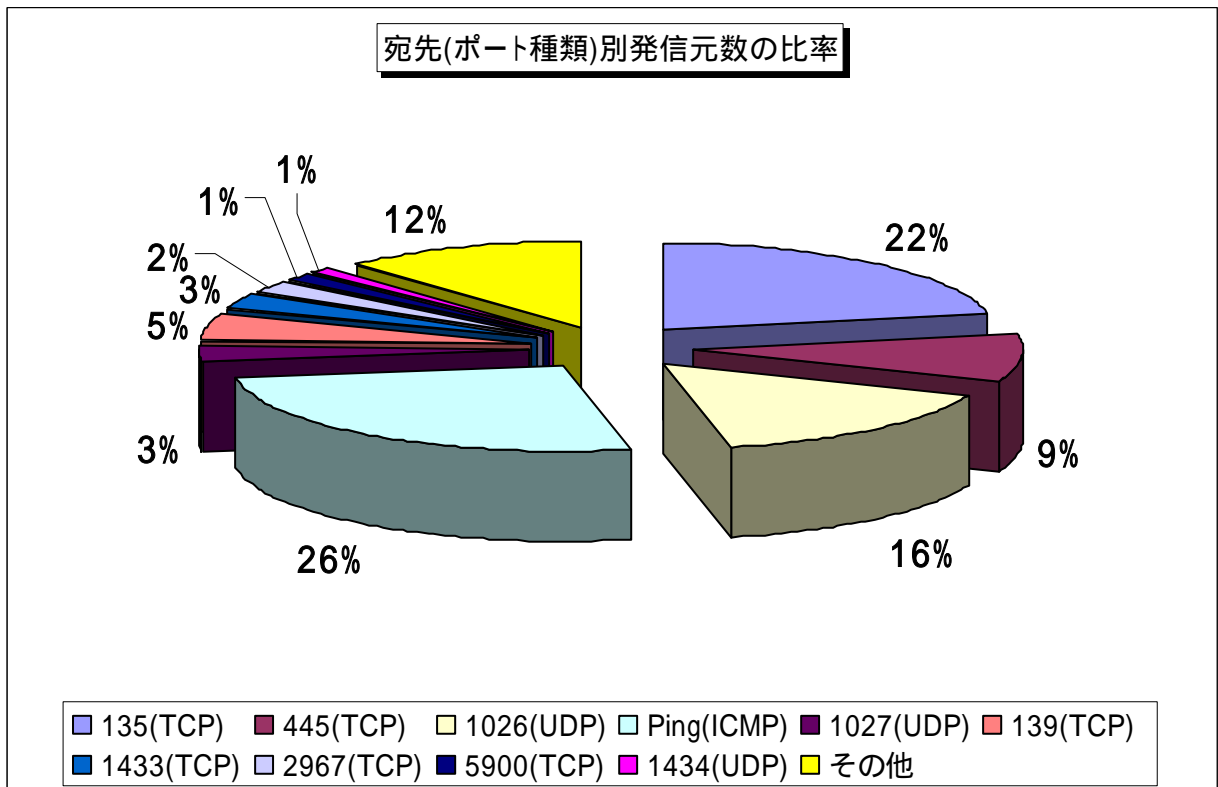
【図 2.2.2 2007年2月の一方的なアクセス状況(発信元数)】

2.3 2007年2月の宛先(ポート種類)別の比率

2007年2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。



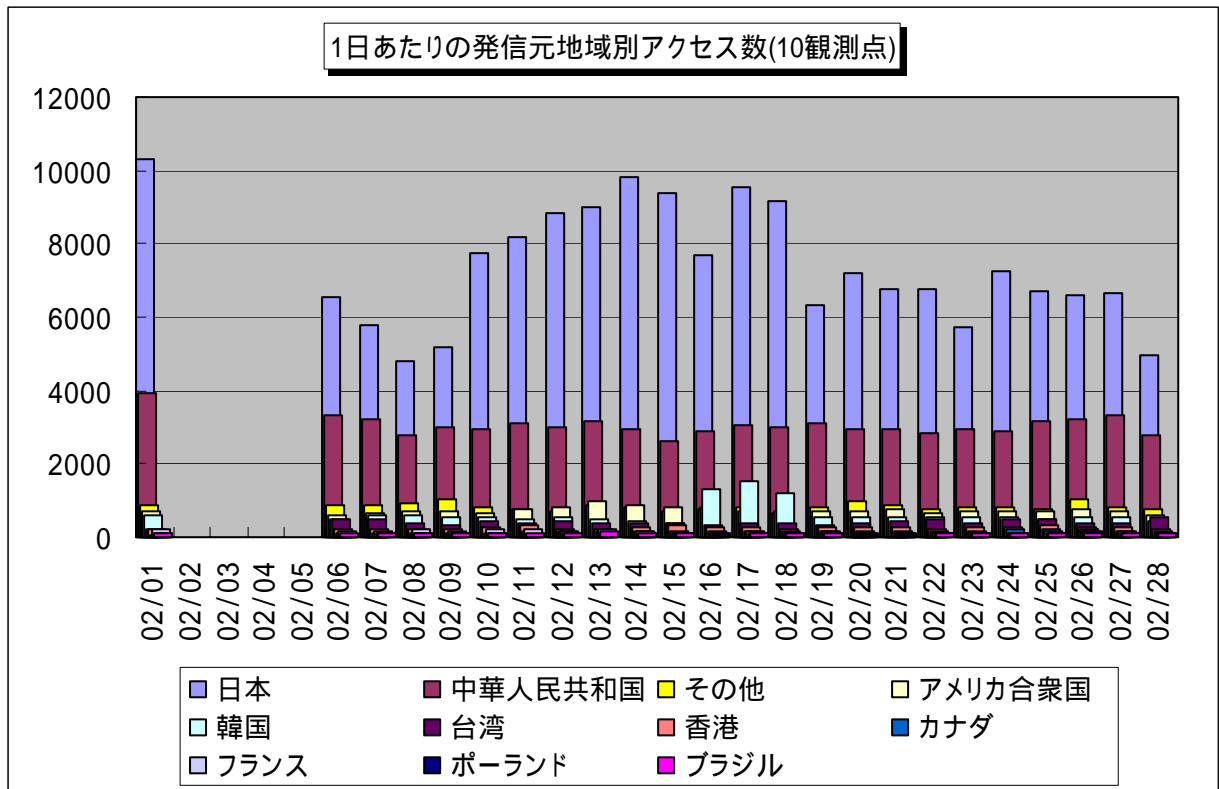
[図 2.3.1 2007年2月の宛先(ポート種類)別アクセス数の比率]



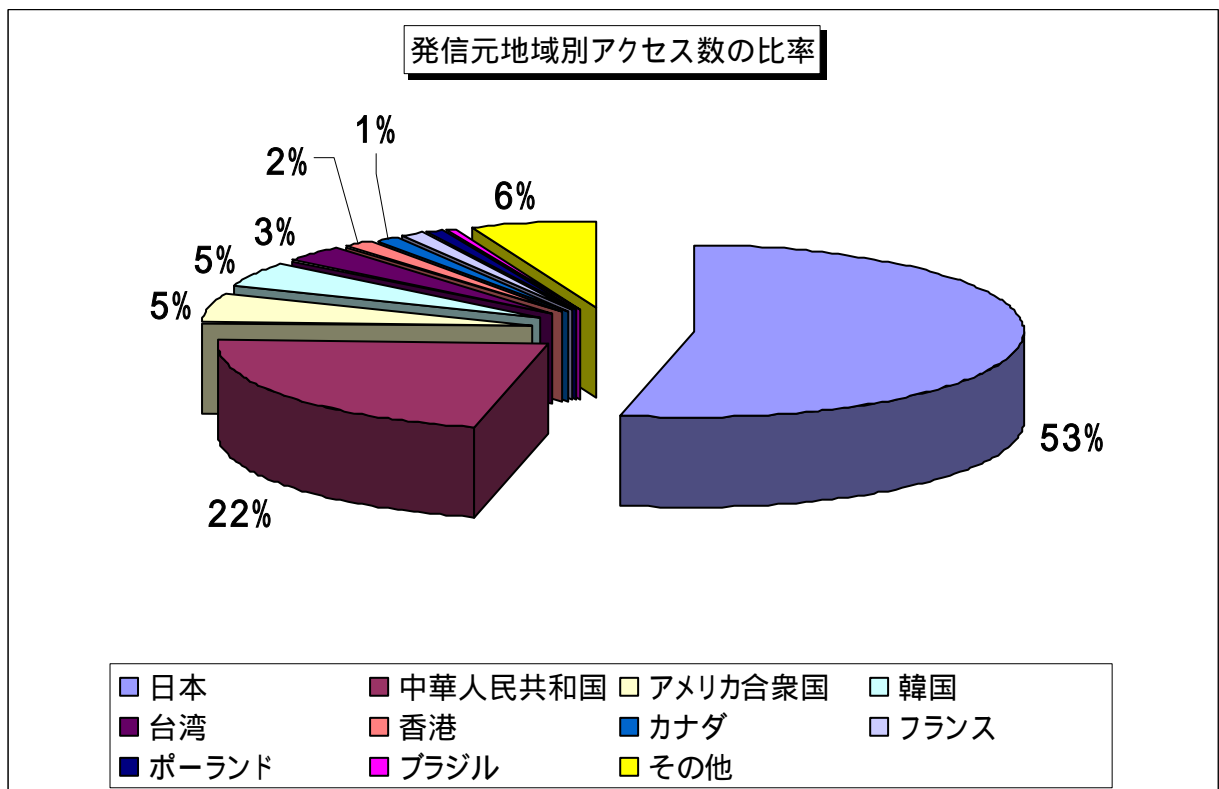
[図 2.3.2 2007年2月の宛先(ポート種類)別発信元数の比率]

2.4 2007年2月の発信元地域別アクセス状況

2007年2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。

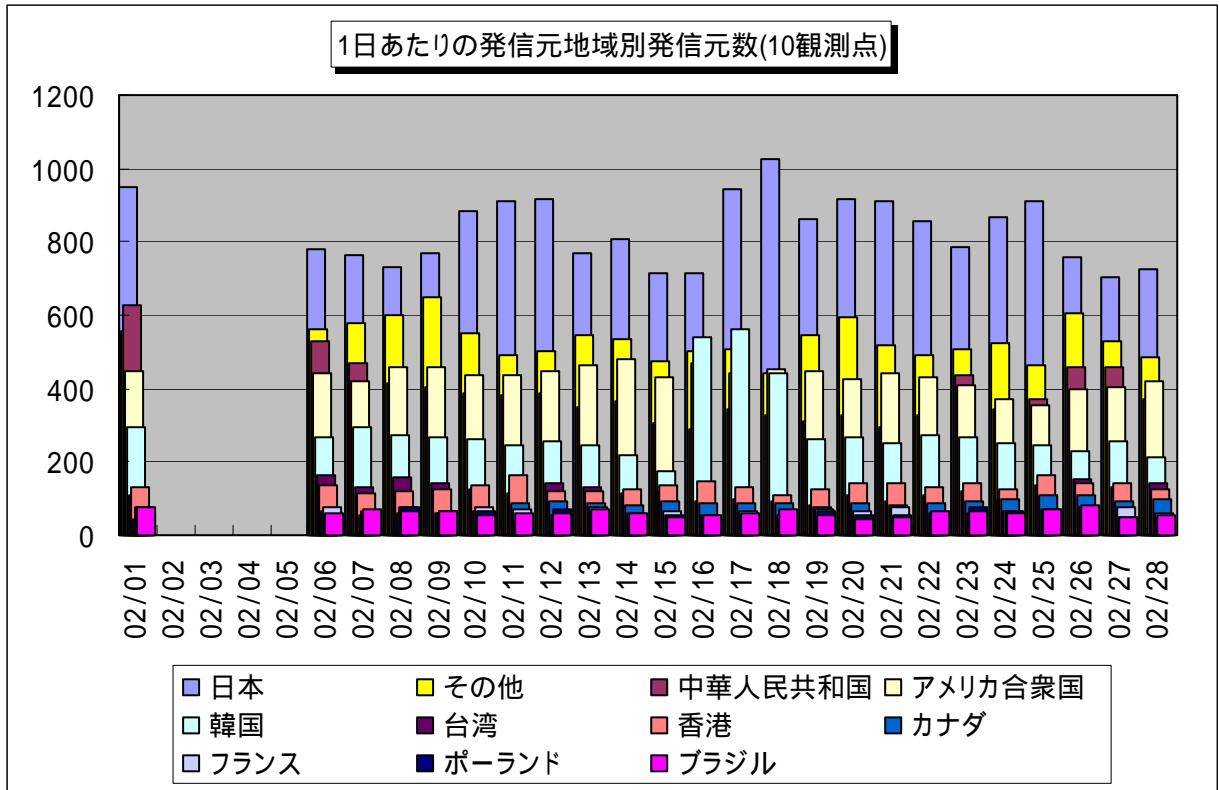


【図 2.4.1 2007年2月の発信元地域別アクセス数の変化】

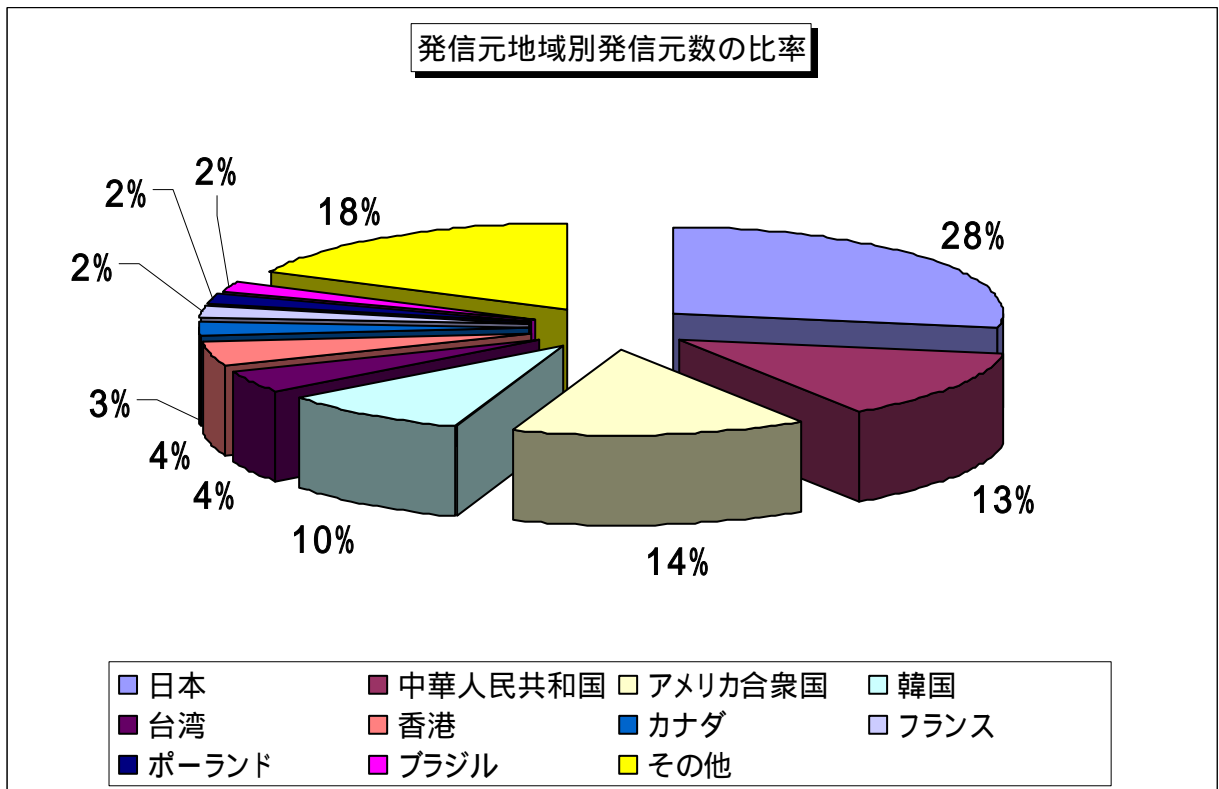


【図 2.4.2 2007年2月の発信元地域別アクセス数の比率】

2007年2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2月の発信元地域別発信元数の変化】

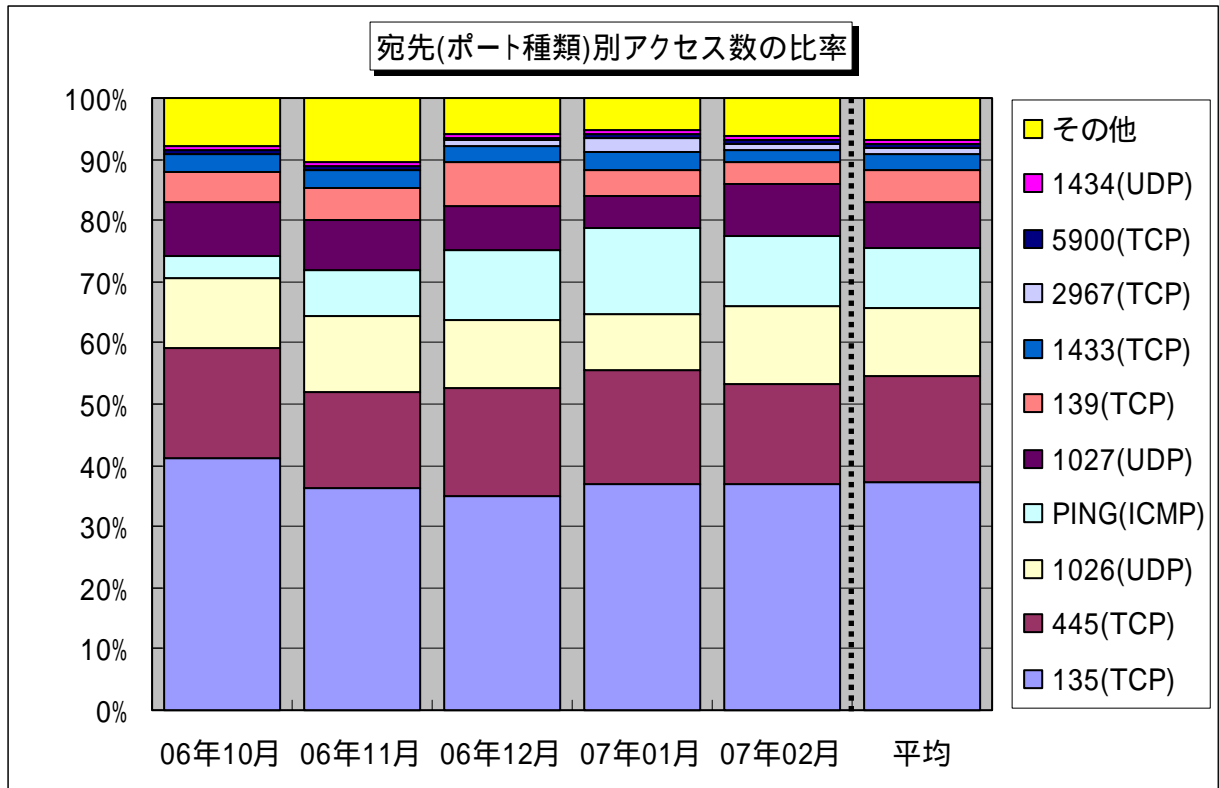


【図 2.4.4 2007年2月の発信元地域別発信元数の比率】

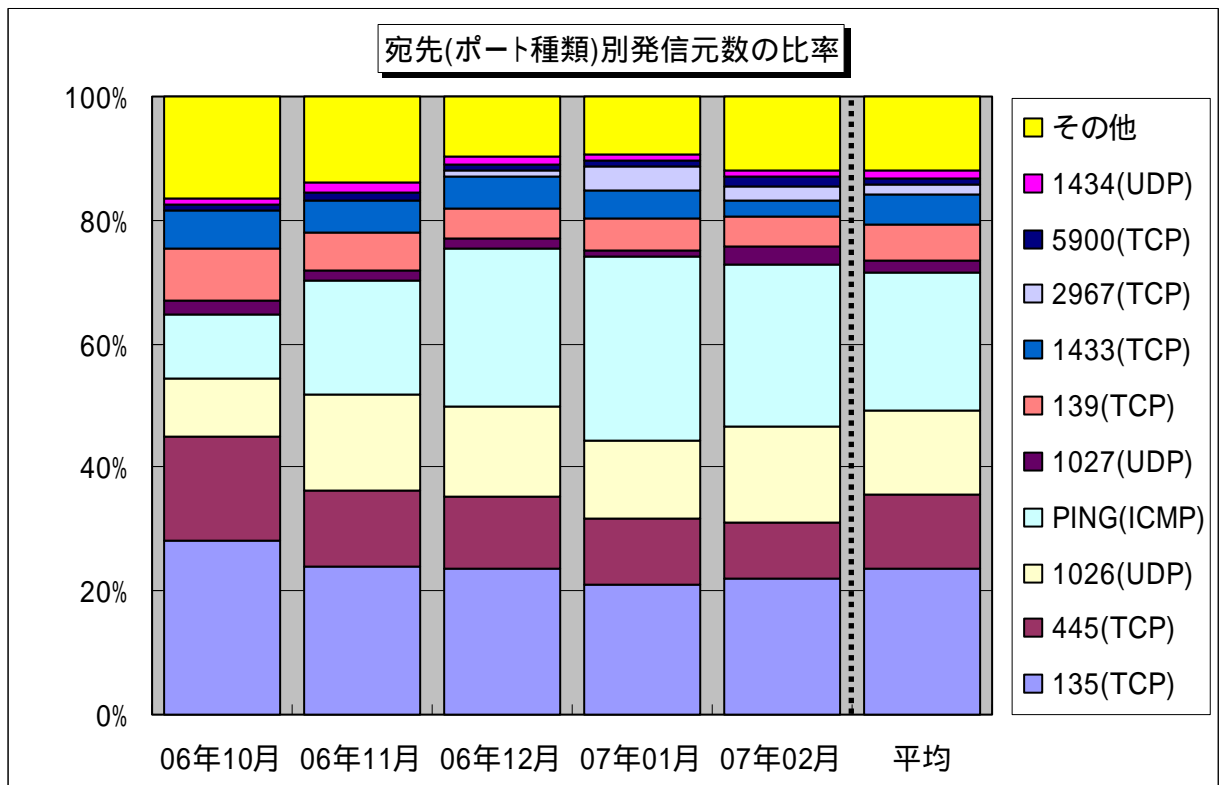
3. 統計情報

3.1 2006年10月～2007年2月の宛先(ポート種類)別の比率

2006年10月～2007年2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。



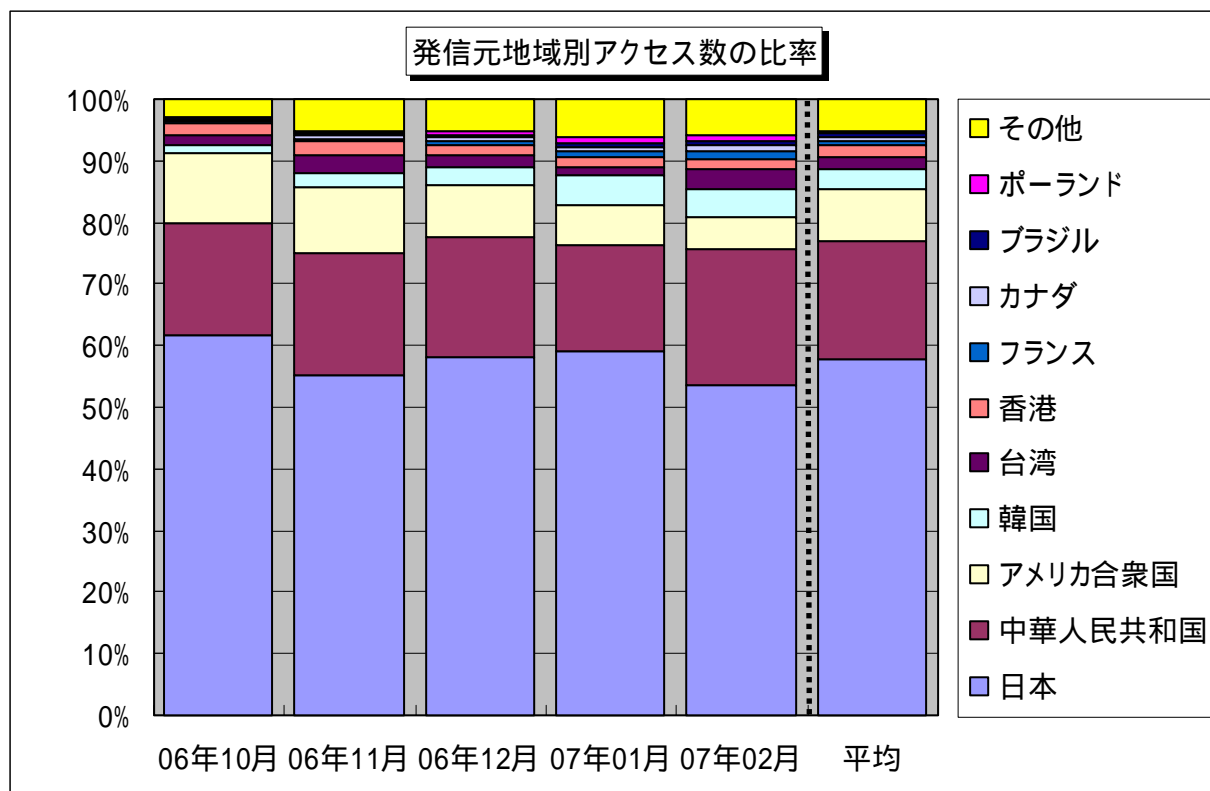
【図 3.1.1 2006年10月～2007年2月の宛先(ポート種類)別アクセス数の比率】



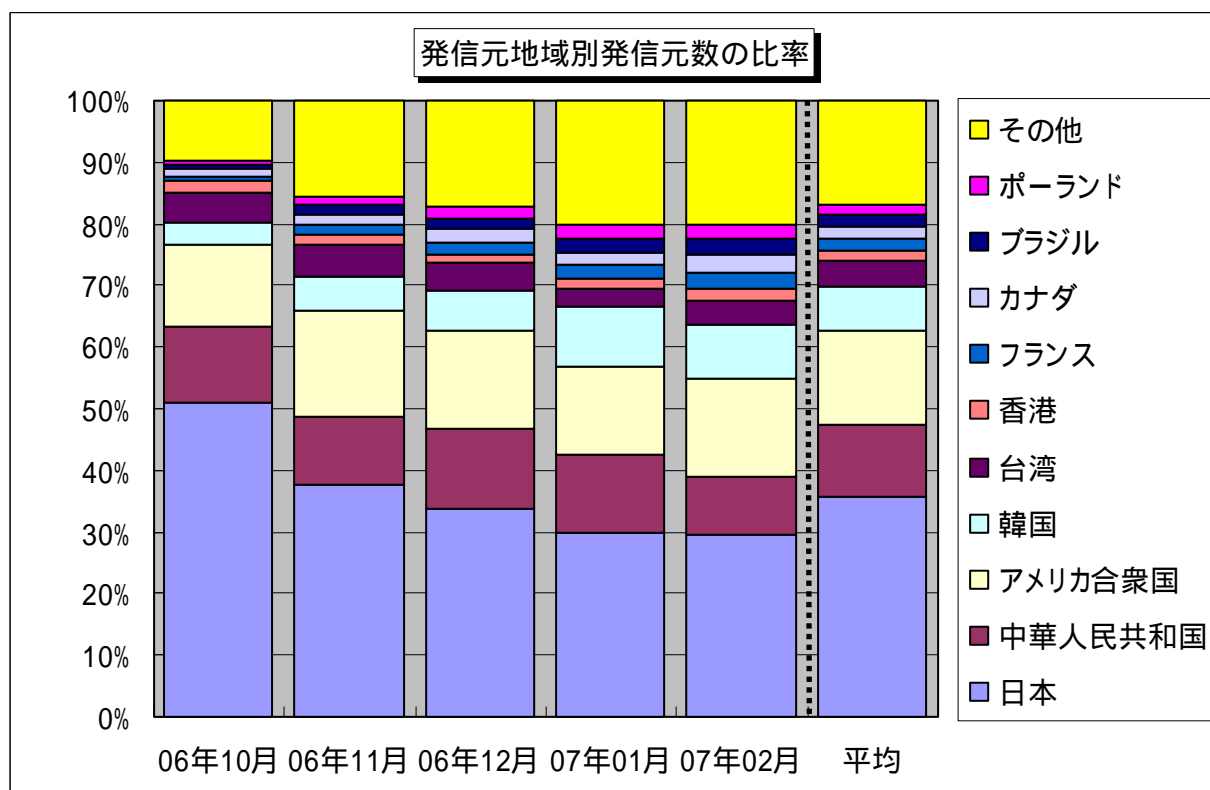
【図 3.1.2 2006年10月～2007年2月の宛先(ポート種類)別発信元数の比率】

3.2 2006年10月～2007年2月の発信元地域別の比率

2006年10月～2007年2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2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2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2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
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 / 内山

Tel:03-5978-7527 Fax:03-5978-7518

E-mail:isec-info@ipa.go.jp