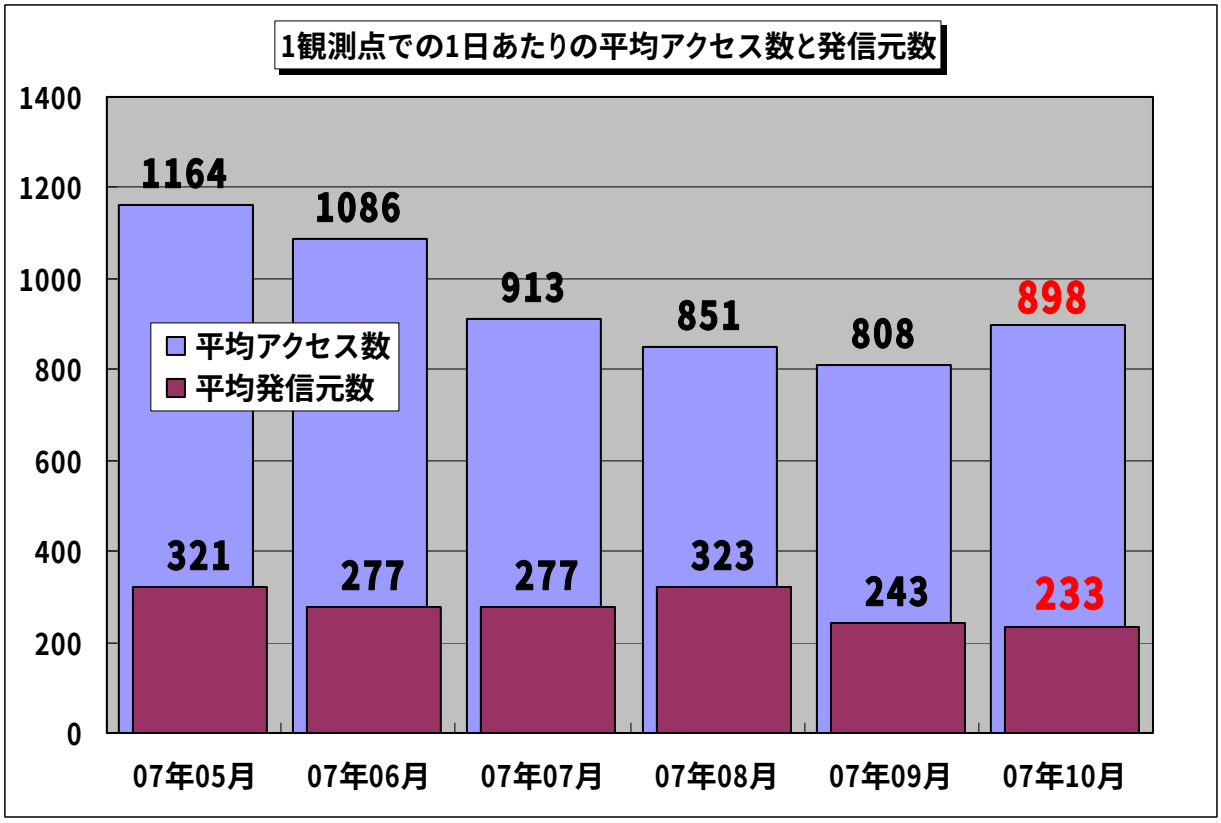
別紙 3

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 10 月の期待しない（一方的な）アクセスの総数は、10 観測点で **278,497 件**ありました。1 観測点で 1 日あたり **233** の発信元から **898 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、233 人の見知らぬ人(発信元)から、発信元一人当たり約 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】

2007 年 5 月～2007 年 10 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、9 月より若干ですが増加傾向にあります。

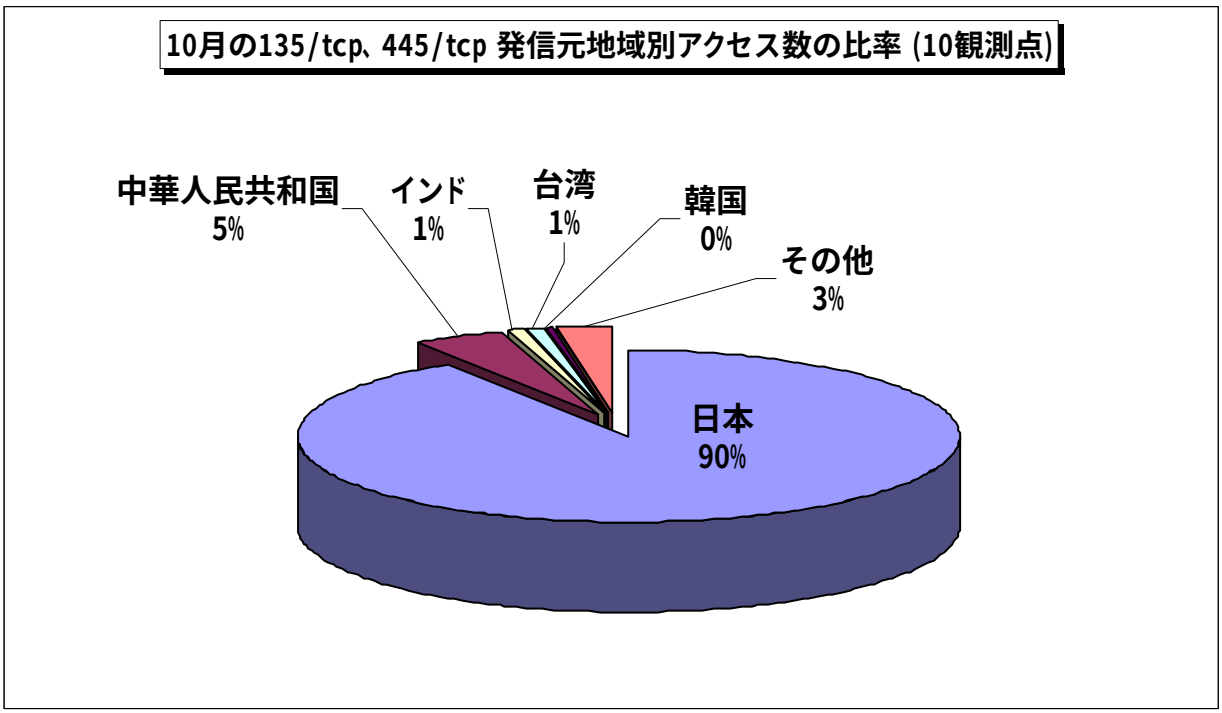
2．10 月のアクセス状況

2007 年 10 月のアクセス状況は、8 月、9 月に比べると若干ですが増加しました。これは、Windows の脆弱性を狙っていると思われる、135/tcp、445/tcp のアクセスが増加したのが原因です。

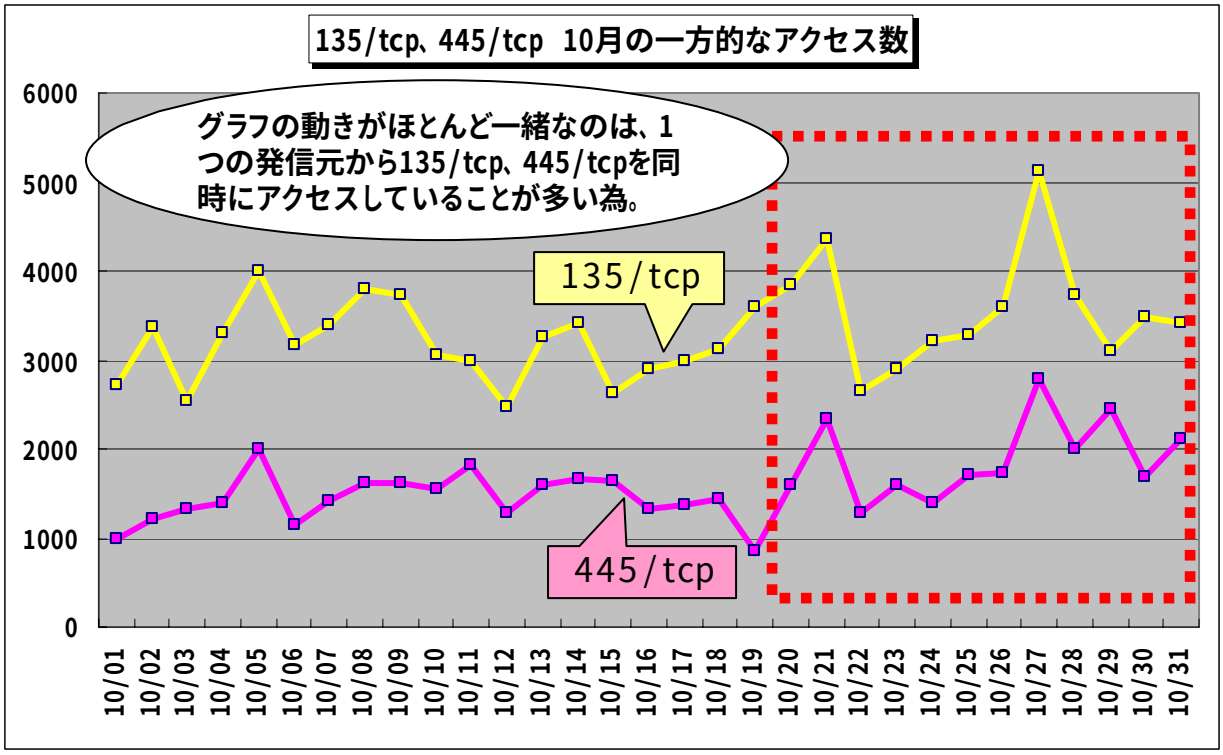
2.1. Windows の脆弱性を狙ったアクセス

135/tcp や、445/tcp へのアクセスは、Windows の古い脆弱性（MS03-026、MS04-011）を狙ったアクセスと思われますが、今でも頻繁にアクセスがあるポートでもあります。最近では、ボットに感染したコンピュータが、さらにボットの感染を広げようとするアクセスが主流と思われます。

発信元地域は、ほとんどが日本からのアクセスです（図 2.1.1 参照）。また、1 つの発信元から 135/tcp と 445/tcp に対して、数回～数百回のアクセスを同時に行なっていることもわかっています（図 2.1.2 参照）。これを見る限り、ボットに感染しているコンピュータが、日本にもまだまだ多いと言えます。



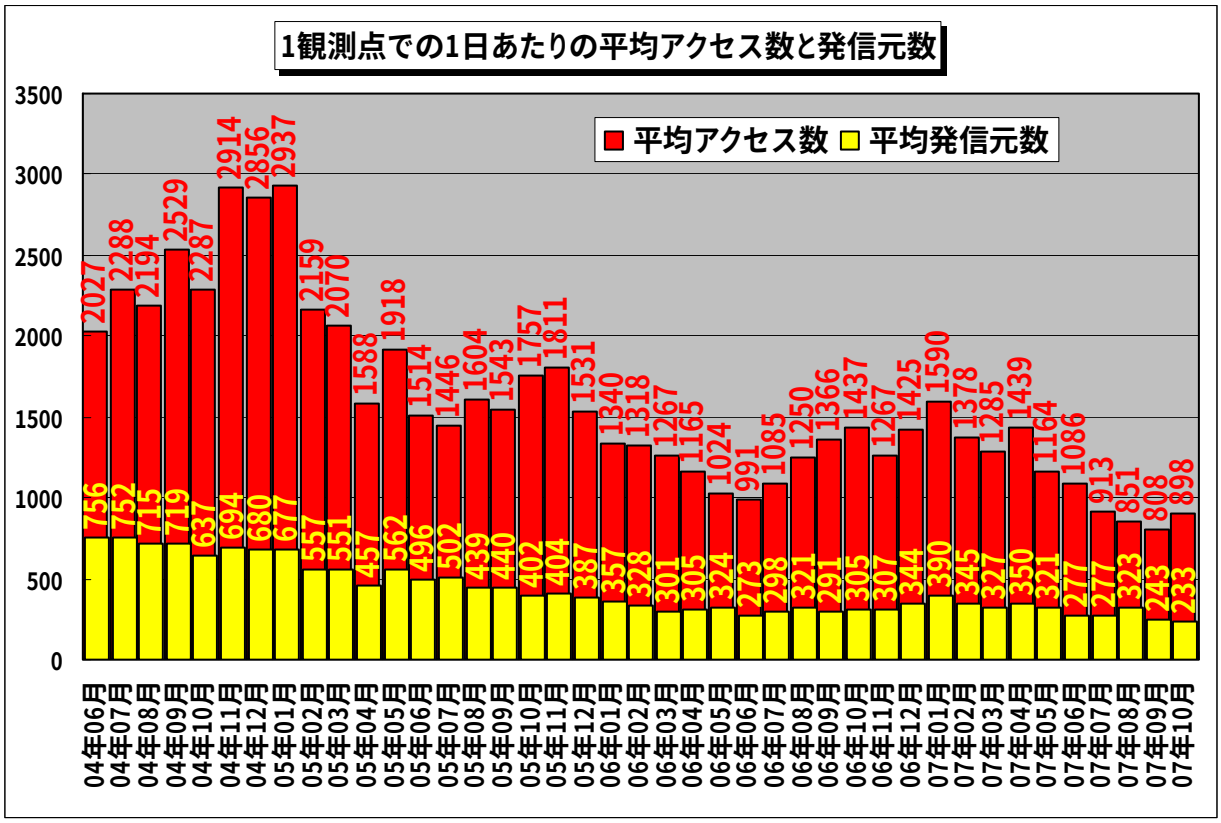
【図 2.1.1　2007 年 10 月の 135/tcp、445/tcp ポートへの発信元地域別アクセス数の比率】



【図 2.1.2　2007 年 10 月の 135/tcp、445/tcp ポートへの一方的なアクセス状況（アクセス数）】

2.2. 観測開始から現在までのアクセス状況

定点観測を開始してから 3 年 4 ヶ月になりますが、最近のアクセス数は、ゆるやかな減少の方向にあります。減少の原因は色々あると思いますが、一番の原因は、ワームウイルスの減少と思われます。これは、W32/SQLSlammer、W32/MSBlaster、W32/Welchia、W32/Sasser などに代表される、Windows の脆弱性を狙ったワームウイルスによる、大量の感染被害が少なくなったからと思われます。

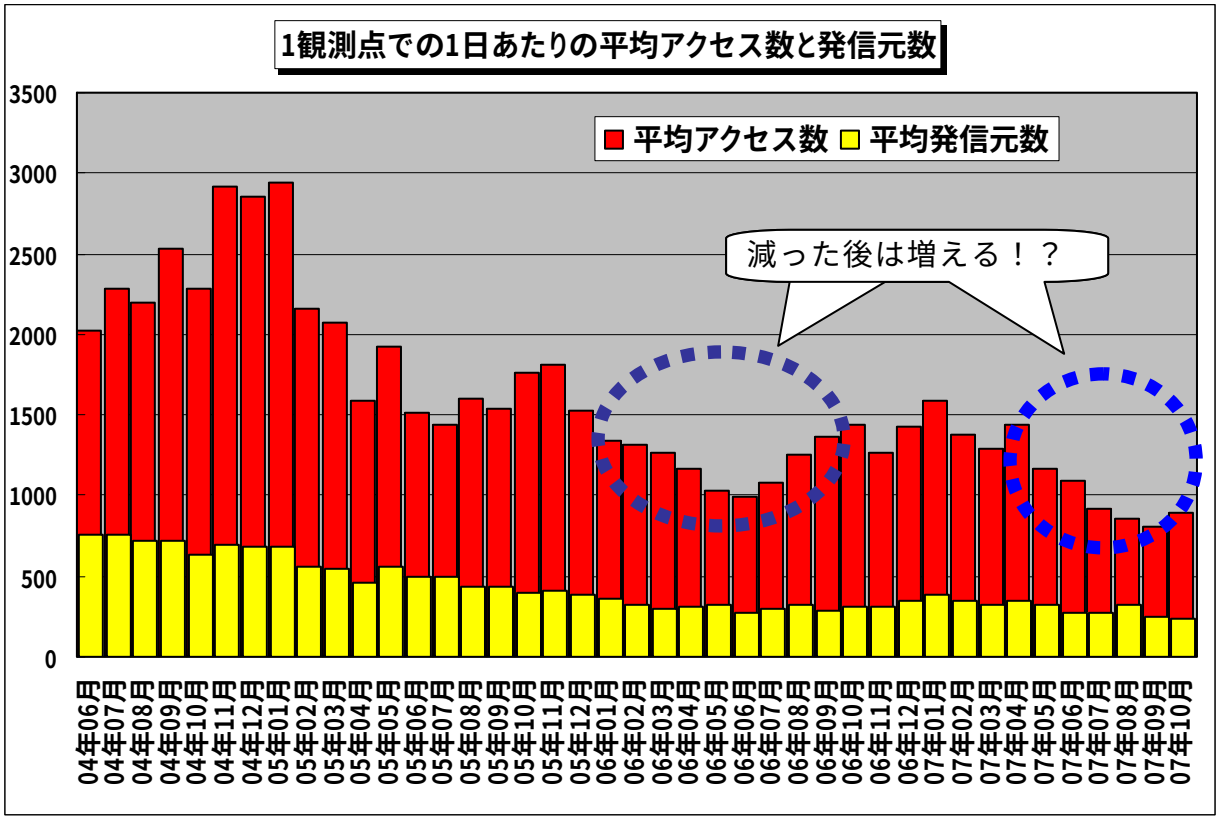


【図 2.2.1 2004 年 6 月～2007 年 10 月の 1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

感染被害が少なくなったのは、その様なウイルスが出回らなくなったことと、企業･個人を含めて、しっかりとしたセキュリティ対策（ウイルス対策ソフトの導入、セキュリティパッチの対応）が浸透してきたからと思われます。また、各プロバイダで行なっている、迷惑メールやウイルスメールの対応も、感染被害の防止になっていると言えます。これは、IPA に届けられる、コンピュータウイルス届出状況の、ウイルス届出数やウイルス検出数の減少からもうかがえます。

ただ、最近ではワームウイルスに代わり、ボットウイルスと思われるアクセスが多くなっています。2.1.で説明した通り、日本からのアクセスも多く、ボットウイルスが潜在的に多いことが考えられますので、Windows も含めたアプリケーションソフトの新しい脆弱性が公開されれば、アクセスが増えることが予想されます。

2007 年 5 月から 9 月まで、アクセス数は減っていますが、10 月は若干増加しました。図 2.2.2 を見る限りでも、一度減ってからまた増えていますので、今後同じ様に増加する可能性があります。



【図 2.2.2　2004 年 6 月～2007 年 10 月の 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】

Windows も含め、使用されているアプリケーションソフトの脆弱性情報を今一度再確認し、コンピュータに脆弱性がないかを確認し、常に最新の状態に保つことを心掛けて下さい。その際は、システム管理者の指示に従って下さい。

(参考情報)

■ 新種ワーム「W32/SQLSlammer ワーム」に関する情報
http://www.ipa.go.jp/security/ciadr/vul/20030126ms-sql-worm.html

■ 「W32/MSBlaster」ワームに関する情報
http://www.ipa.go.jp/security/topics/newvirus/msblaster.html

■ 「W32/Welchia」ワームに関する情報
http://www.ipa.go.jp/security/topics/newvirus/welchi.html

■ 新種ワーム「W32/Sasser」に関する情報
http://www.ipa.go.jp/security/topics/newvirus/sasser.html

■ ボット対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/3_bot_v5.pdf

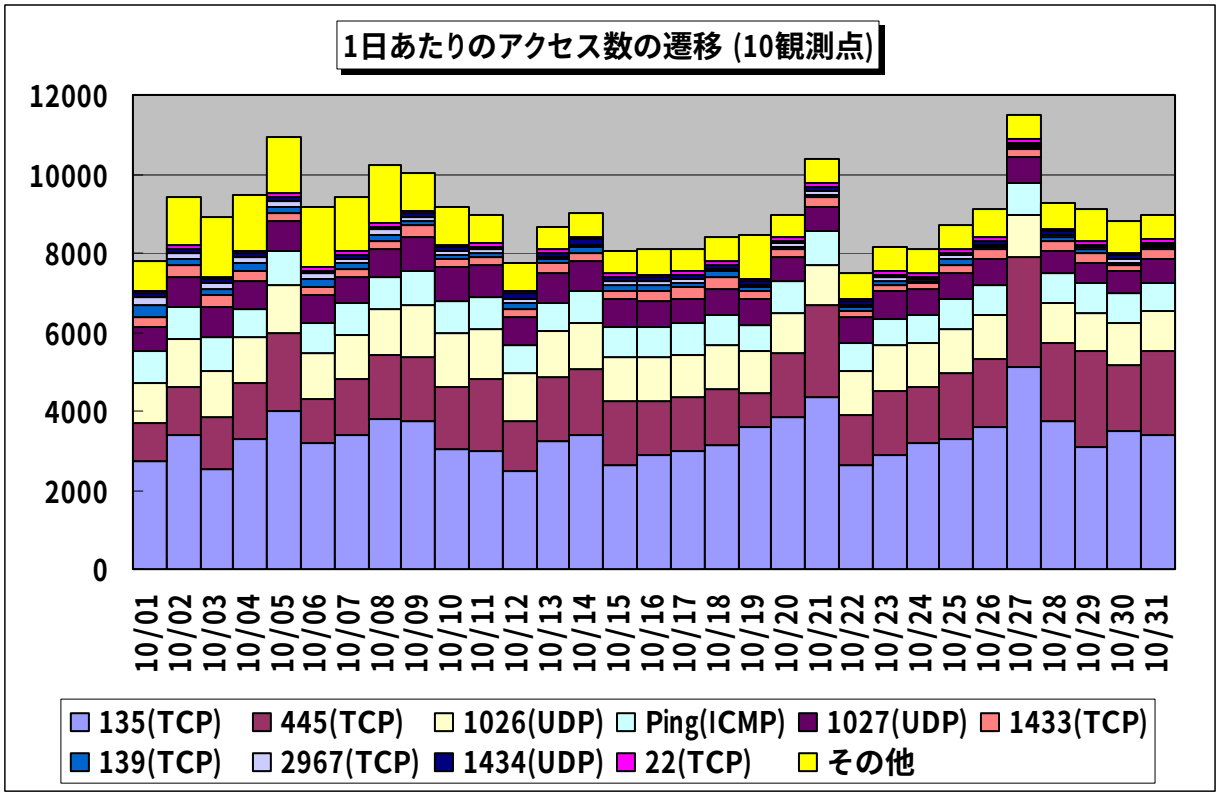
■ 総務省･経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/

■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html

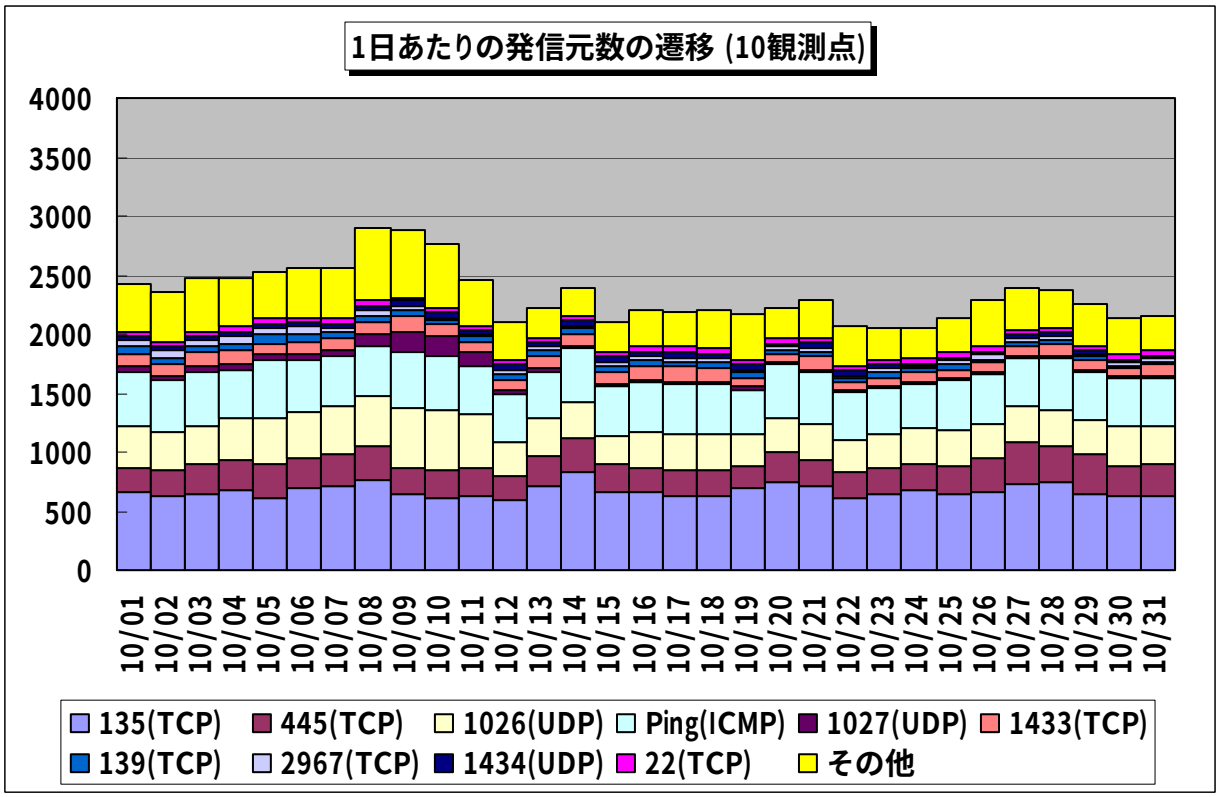
■ 「Microsoft Update と Windows Update の利用の手順」（マイクロソフト社）
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx

2.3 2007 年 10 月の一方的なアクセス状況

2007 年 10 月の一方的なアクセス状況（アクセス数）の遷移を図 2.3.1 に、一方的なアクセス状況（発信元数）の遷移を図 2.3.2 に示します。



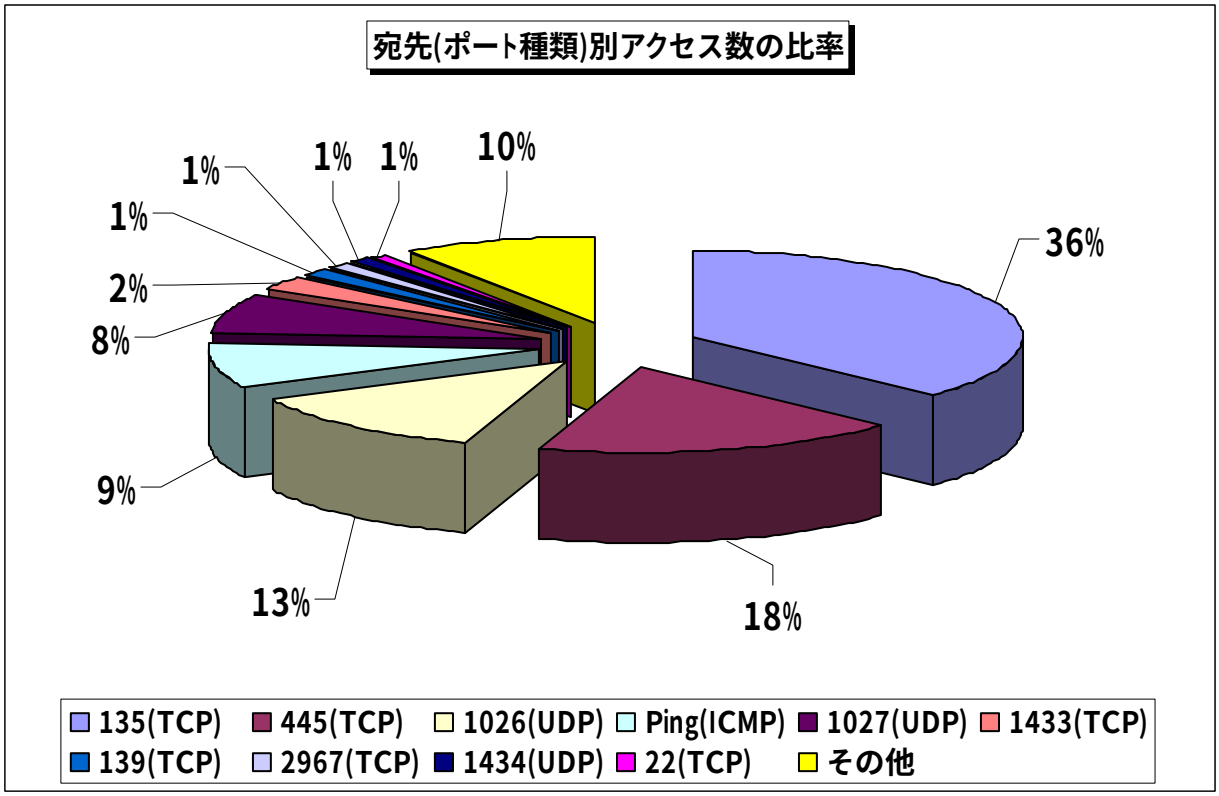
【図 2.3.1 2007 年 10 月の一方的なアクセス状況(アクセス数)】



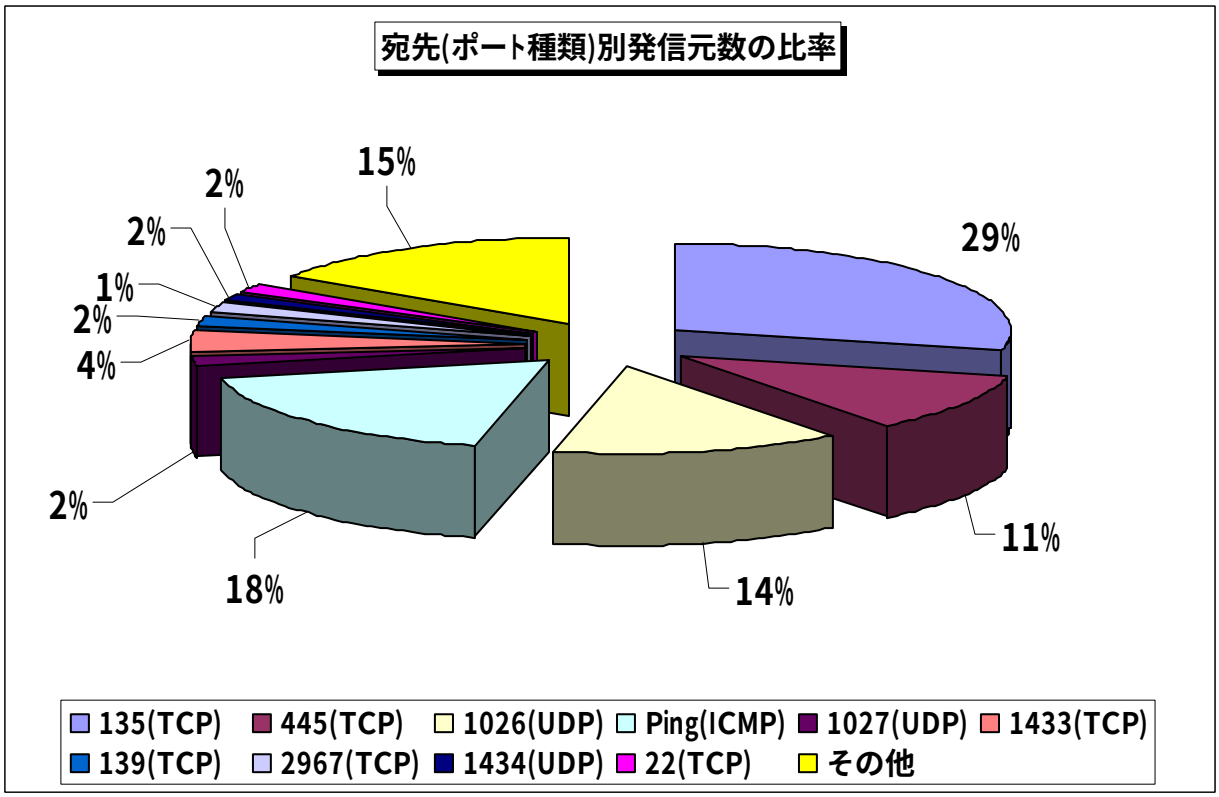
【図 2.3.2 2007 年 10 月の一方的なアクセス状況(発信元数)】

2.4 2007 年 10 月の宛先(ポート種類)別の比率

2007 年 10 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 2.4.1 に、宛先(ポート種類)別発信元数の比率を図 2.4.2 に示します。



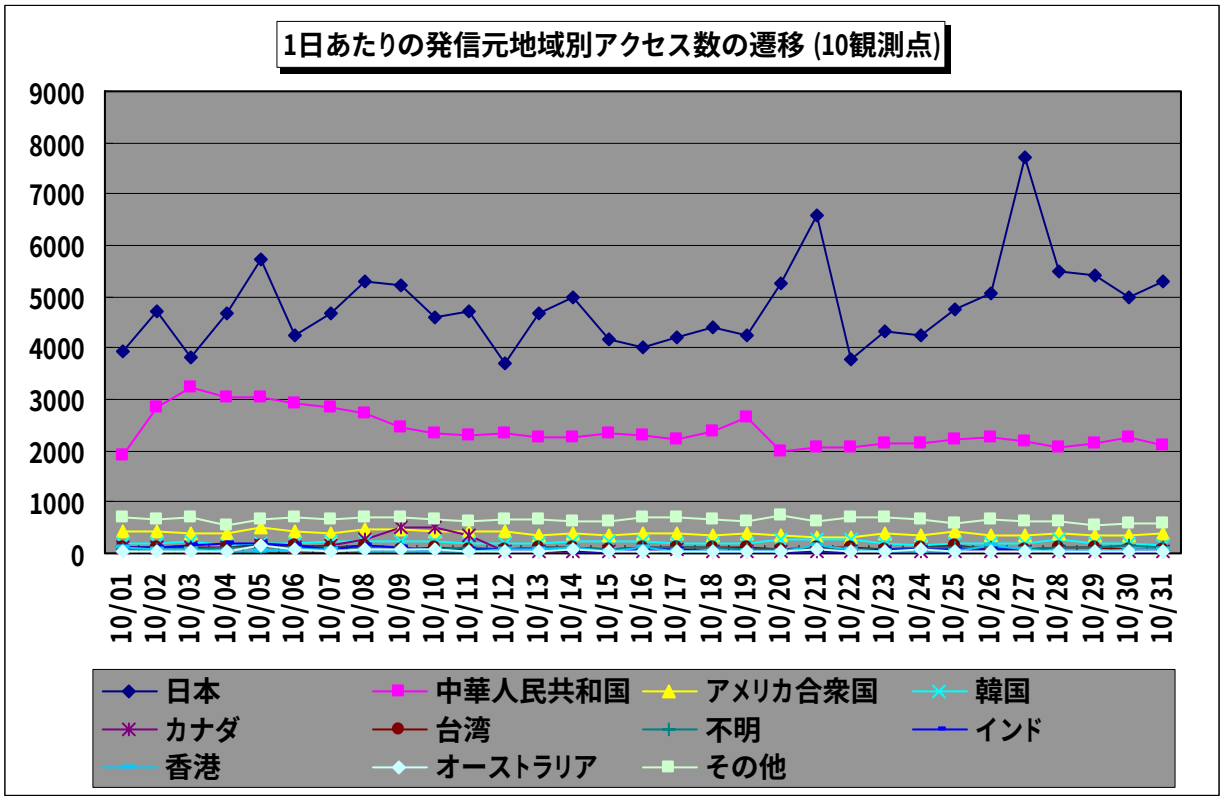
【図 2.4.1 2007 年 10 月の宛先(ポート種類)別アクセス数の比率】



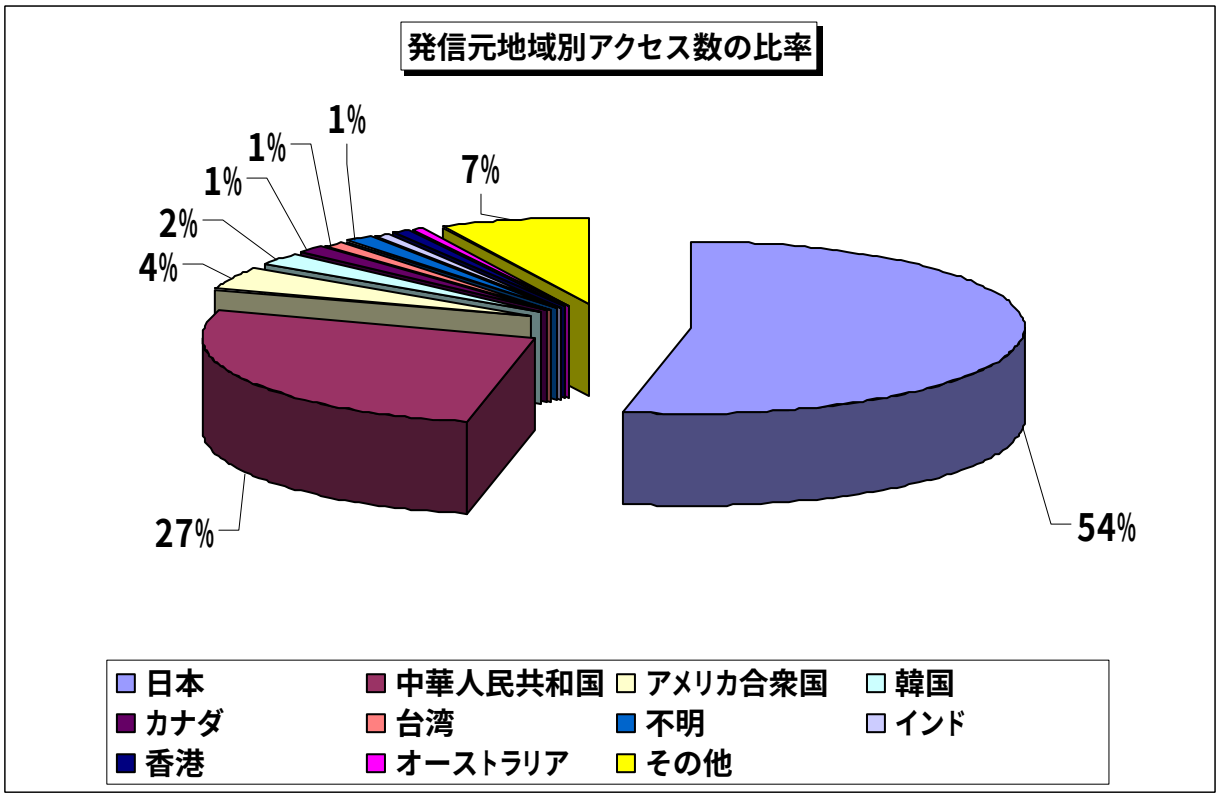
【図 2.4.2 2007 年 10 月の宛先(ポート種類)別発信元数の比率】

2.5 2007 年 10 月の発信元地域別アクセス状況

2007 年 10 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 2.5.1 に、発信元地域別アクセス数の比率を図 2.5.2 に示します。

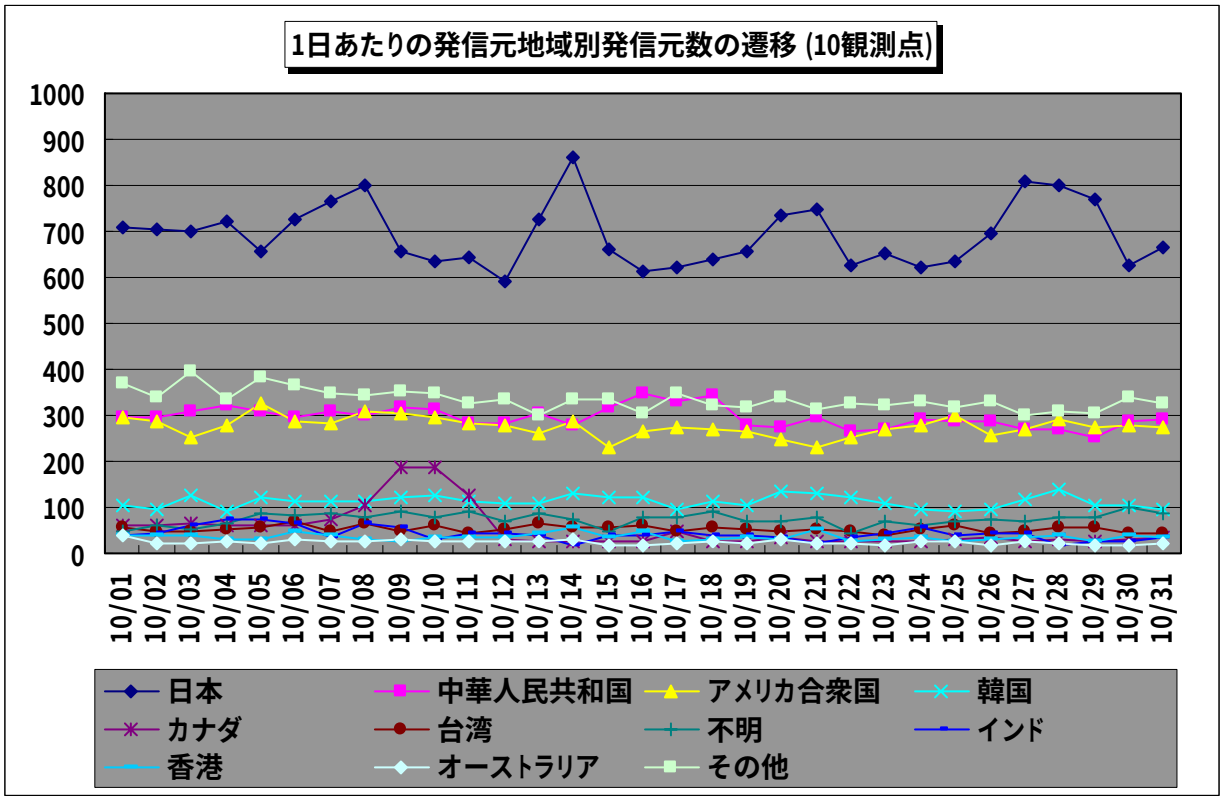


【図 2.5.1 2007 年 10 月の発信元地域別アクセス数の変化】

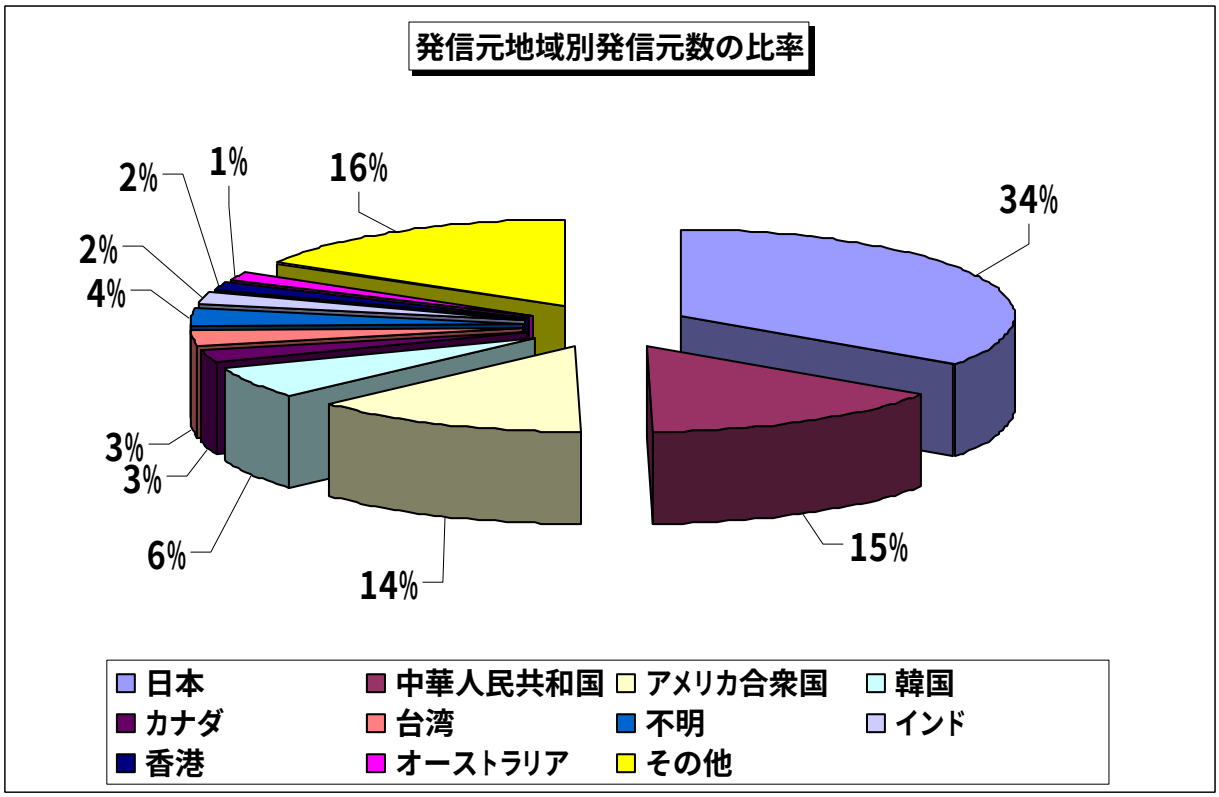


【図 2.5.2 2007 年 10 月の発信元地域別アクセス数の比率】

2007 年 10 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 2.5.3 に、発信元地域別発信元数の比率を図 2.5.4 に示します。



【図 2.5.3 2007 年 10 月の発信元地域別発信元数の変化】

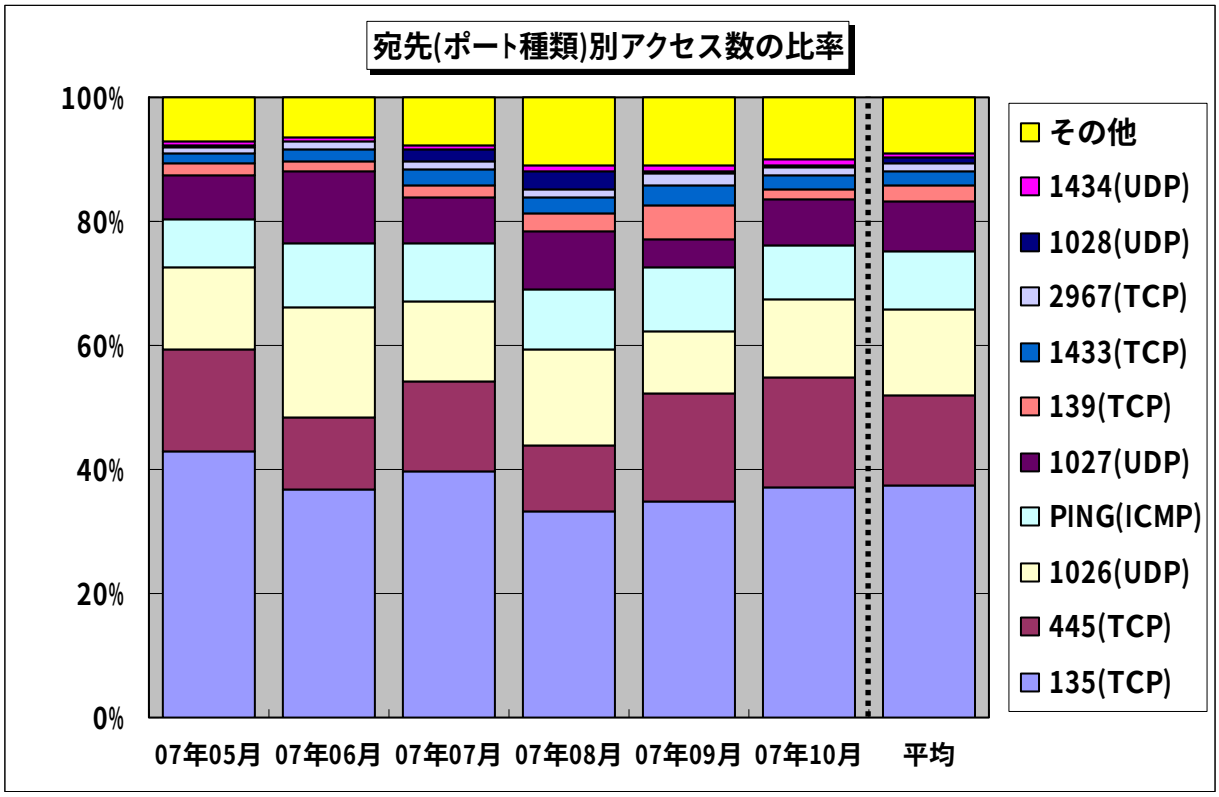


【図 2.5.4 2007 年 10 月の発信元地域別発信元数の比率】

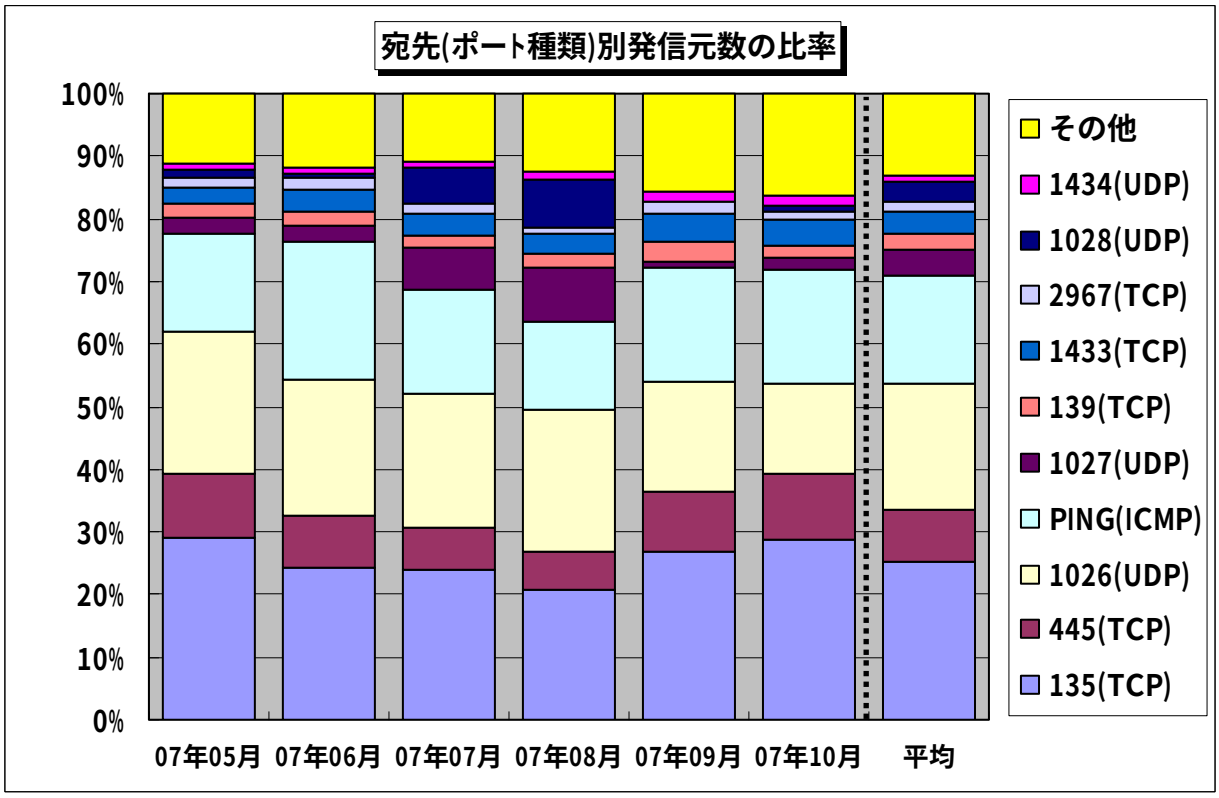
3．統計情報

3.1 2007 年 5 月～2007 年 10 月の宛先(ポート種類)別の比率

2007 年 5 月～2007 年 10 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。



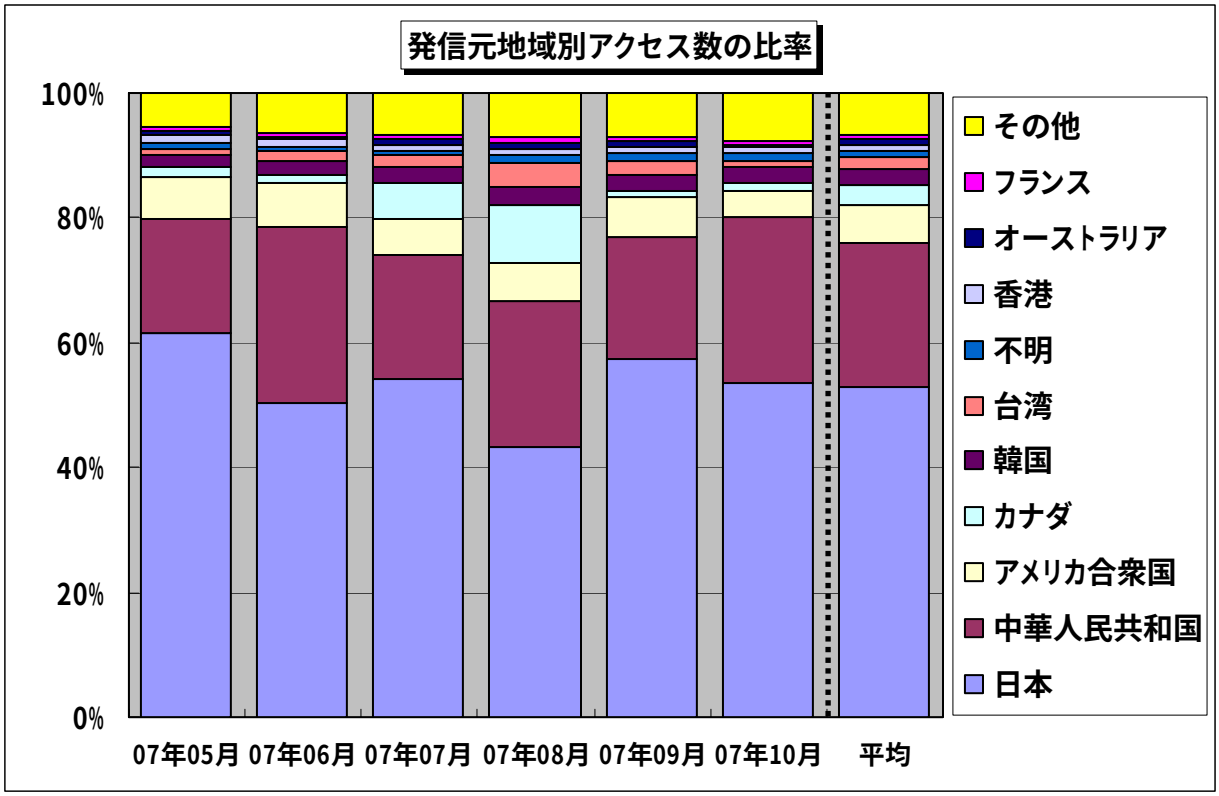
【図 3.1.1 2007 年 5 月～2007 年 10 月の宛先(ポート種類)別アクセス数の比率】



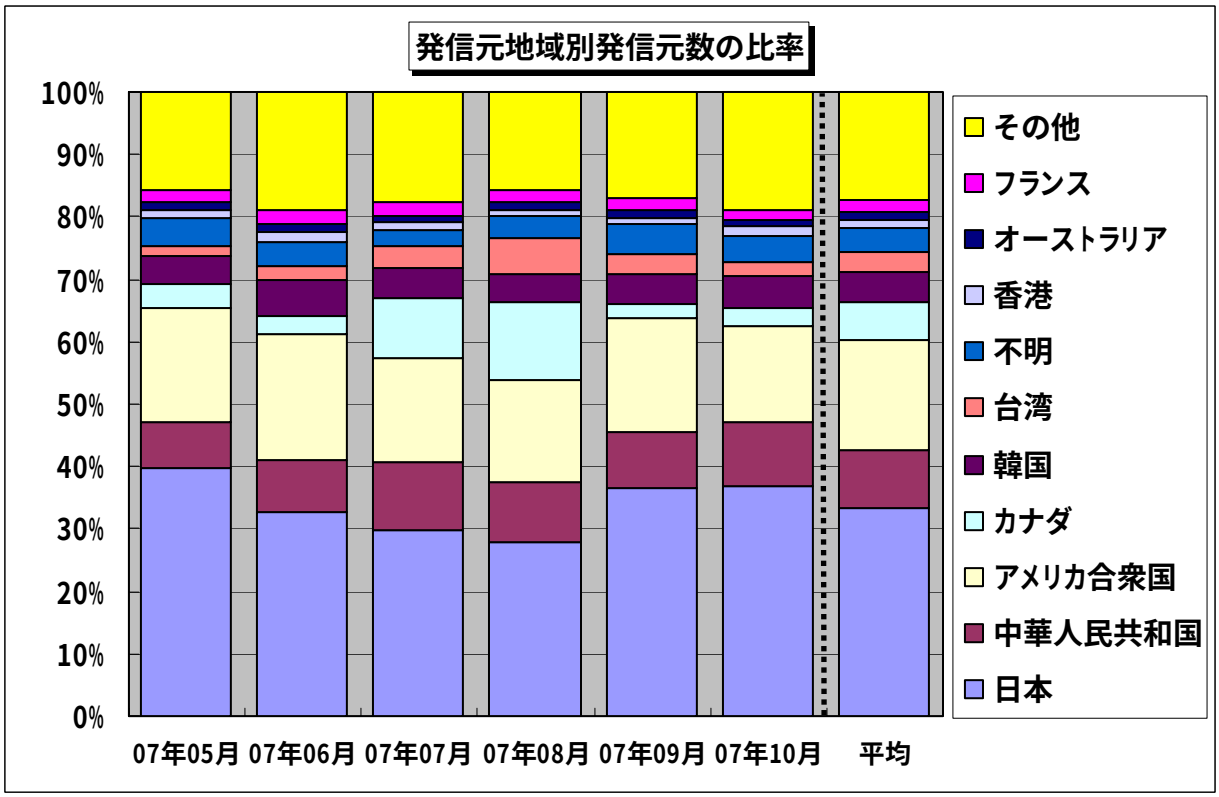
【図 3.1.2 2007 年 5 月～2007 年 10 月の宛先(ポート種類)別発信元数の比率】

3.2 2007 年 5 月～2007 年 10 月の発信元地域別の比率

2007 年 5 月～2007 年 10 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 2007 年 5 月～2007 年 10 月の発信元地域別アクセス数の比率】



【図 3.2.2 2007 年 5 月～2007 年 10 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 10 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
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
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
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
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)
22(TCP)	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）を狙ったアクセス

■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