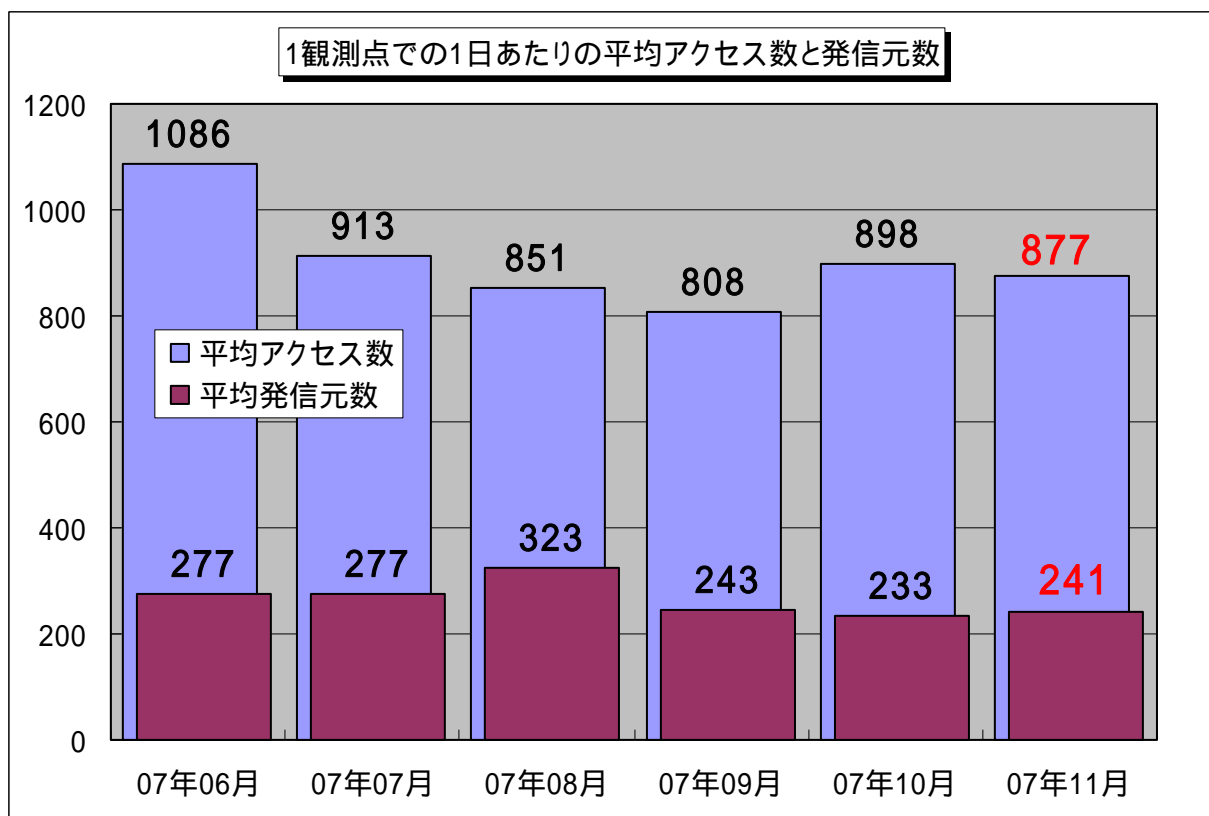


インターネット定点観測(TALOT2)での観測状況について

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11月の期待しない(一方的な)アクセスの総数は、10観測点で263,077件ありました。1観測点で1日あたり241の発信元から877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、241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】

2007年6月～2007年11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、10月とほとんど同じ傾向にあります。

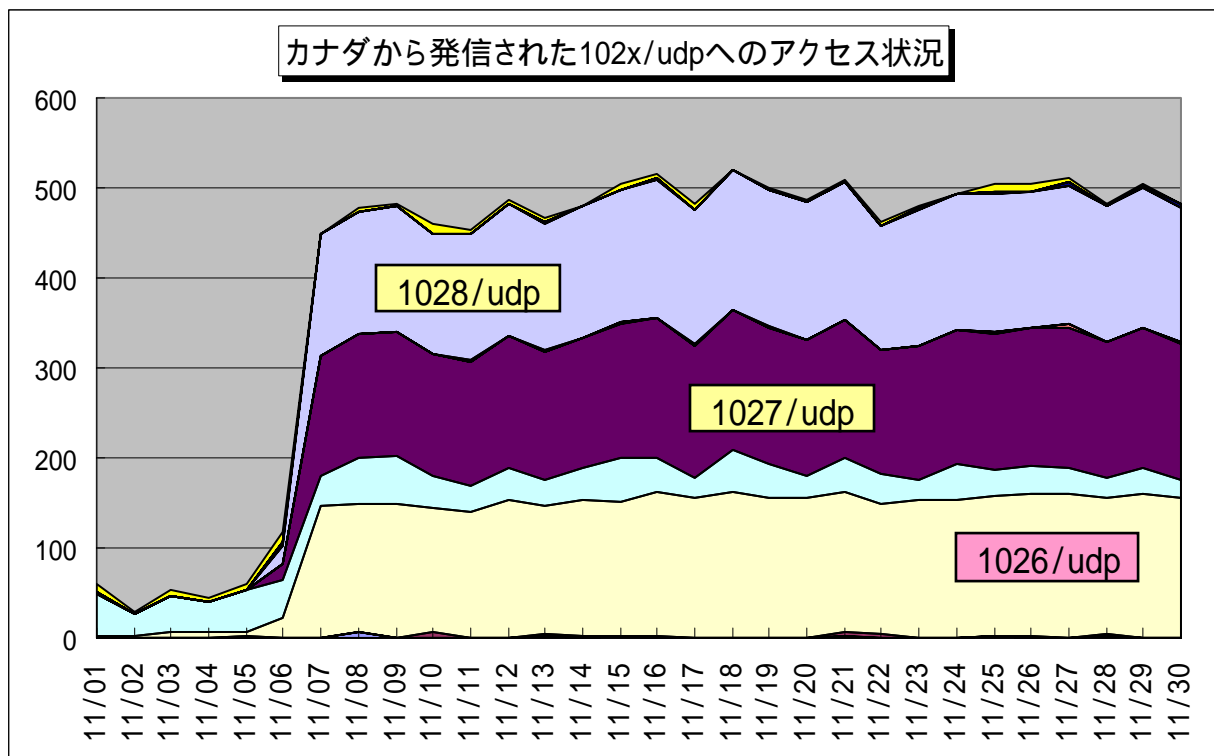
2. 11月のアクセス状況

2007年11月のアクセス状況は、10月と比べても変わりなくほとんど同じ状況でした。その中で、Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスの内、1028/udpが増加しました。

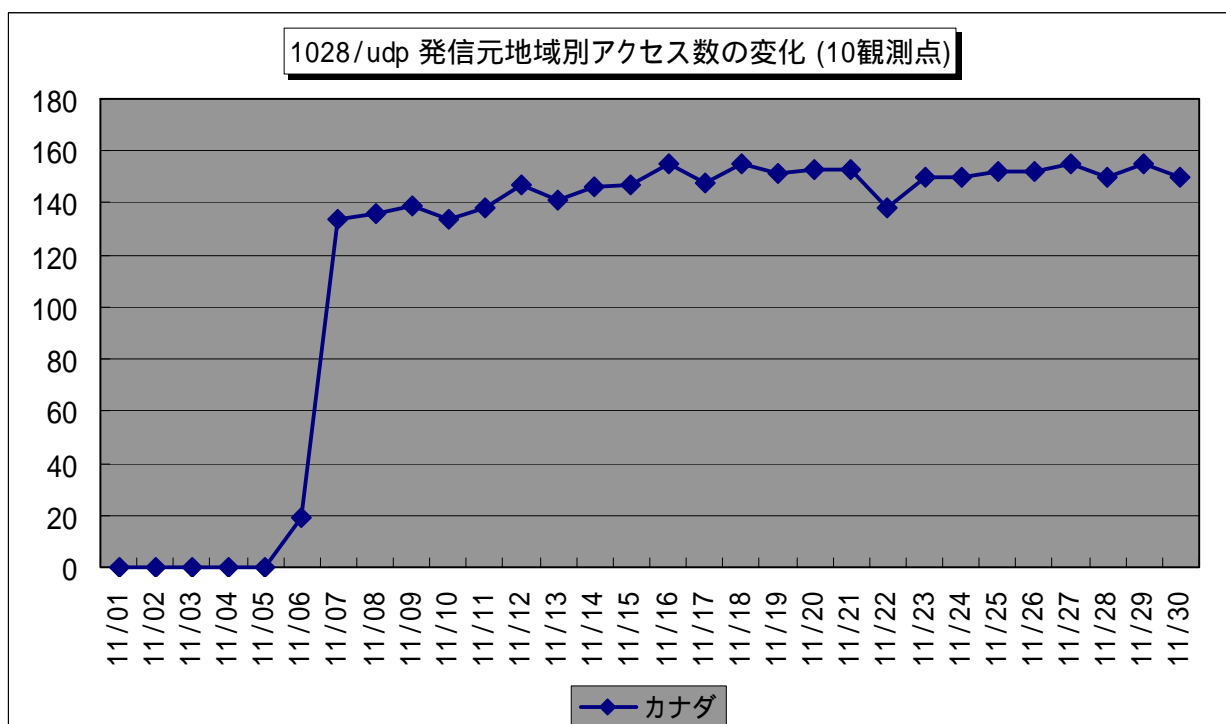
2.1. Windows Messenger サービスを悪用したアクセスの発信元状況

Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスは、1026/udp、1027/udp、1028/udp に対して行なわれますが、11月は1028/udp に対するアクセスが多く見受けられました。

これらの発信元は、そのほとんどがカナダからで、1026/udp、1027/udp に対するアクセスも、アクセス数1位の中国(中華人民共和国)に次いで、多く見受けられます。(図2.1.1 参照)



【図 2.1.1 2007 年 11 月 カナダから発信された 102x/udp へのアクセス状況】



【図 2.1.2 2007 年 11 月 1028/udp 発信元地域別アクセス数の変化 (10 観測点)】

これらのアクセスは、迷惑メールと似ていて、Windows Messenger サービスを悪用してポップアップメッセージを送りつけてくるもので、「コンピュータに重度の障害が発生しました」旨の嘘の内容で脅し、特定の URL をクリックさせようとしています。

ほとんどがスパムメッセージと思われるので、無視をしていけばよいのですが、迷惑メールの様に増加していく可能性もあります。

この様なアクセスへの対策としては、Windows Messenger サービスを停止することを勧めます。ただし、企業内 LAN 等で使用しているコンピュータの場合は、システム管理者の指示に従って下さい。

(参考情報)

インターネット広告を含む Messenger サービスウィンドウが表示される

<http://support.microsoft.com/kb/330904/ja>

また、Windows Messenger サービスのぜい弱性のセキュリティパッチも発表されていますので、適用されているか確認を行なうこともお勧めします。

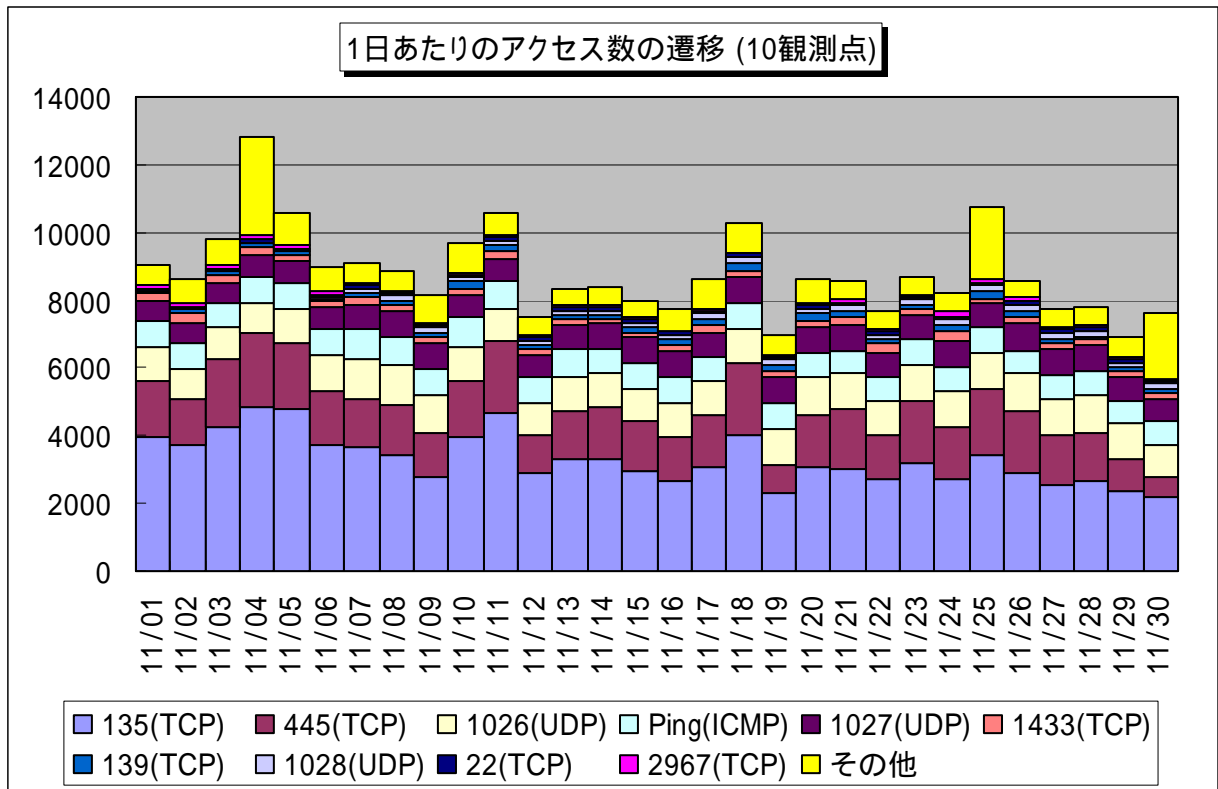
(参考情報)

メッセンジャ サービスのバッファオーバーランにより、コードが実行される。(MS03-043)

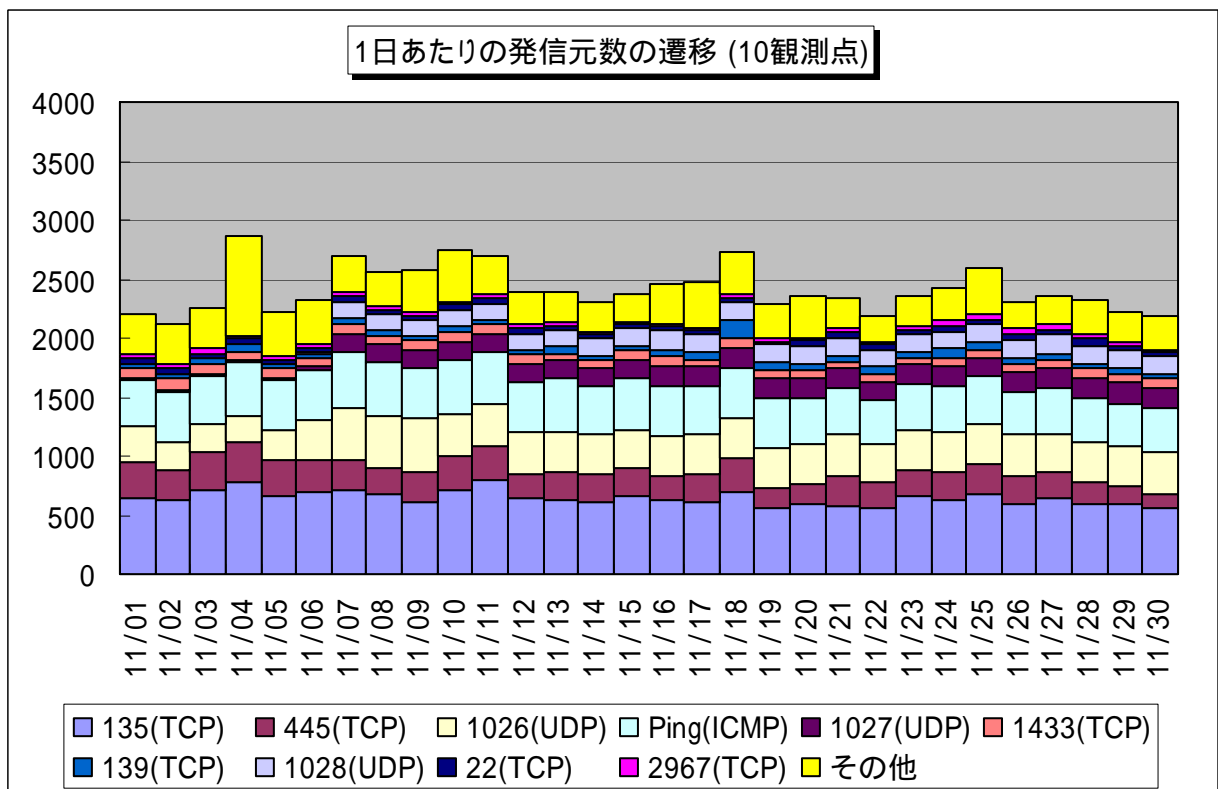
<http://www.microsoft.com/japan/technet/security/Bulletin/MS03-043.msp>

2.2 2007年11月の一方的なアクセス状況

2007年11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。



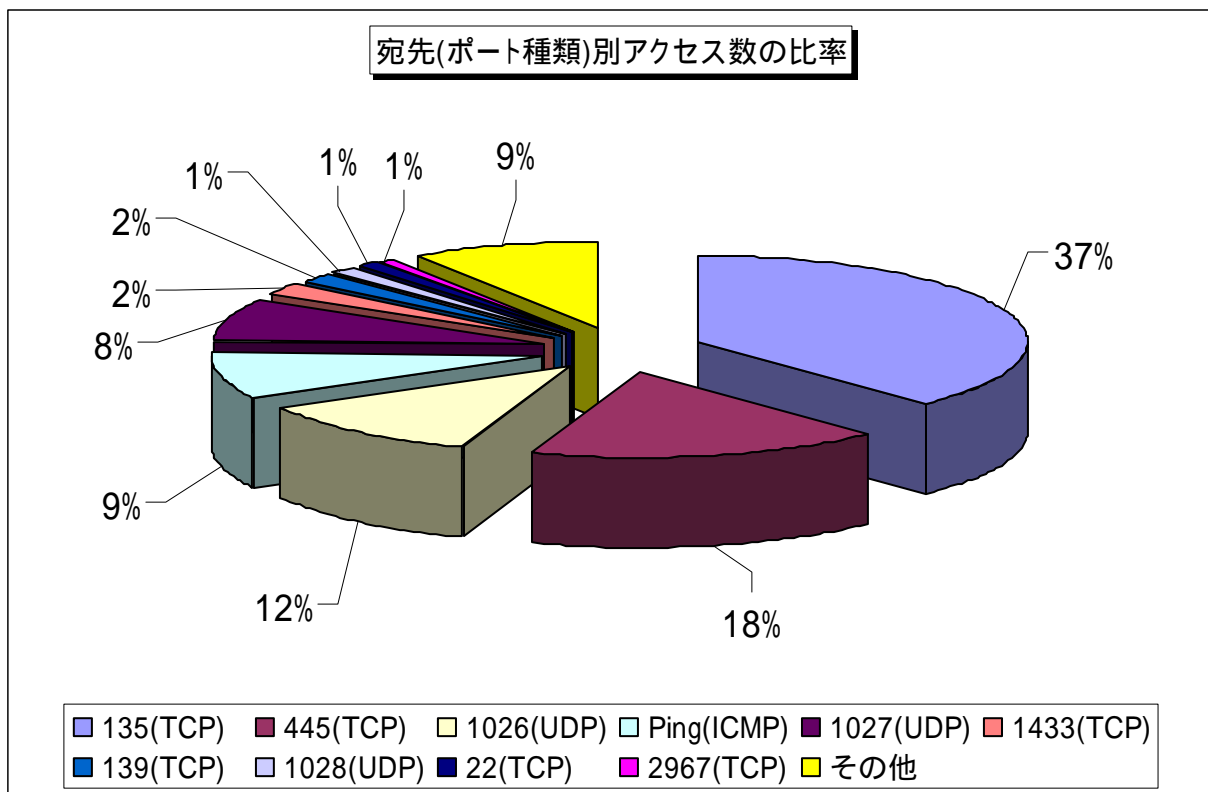
【図 2.2.1 2007年11月の一方的なアクセス状況(アクセス数)】



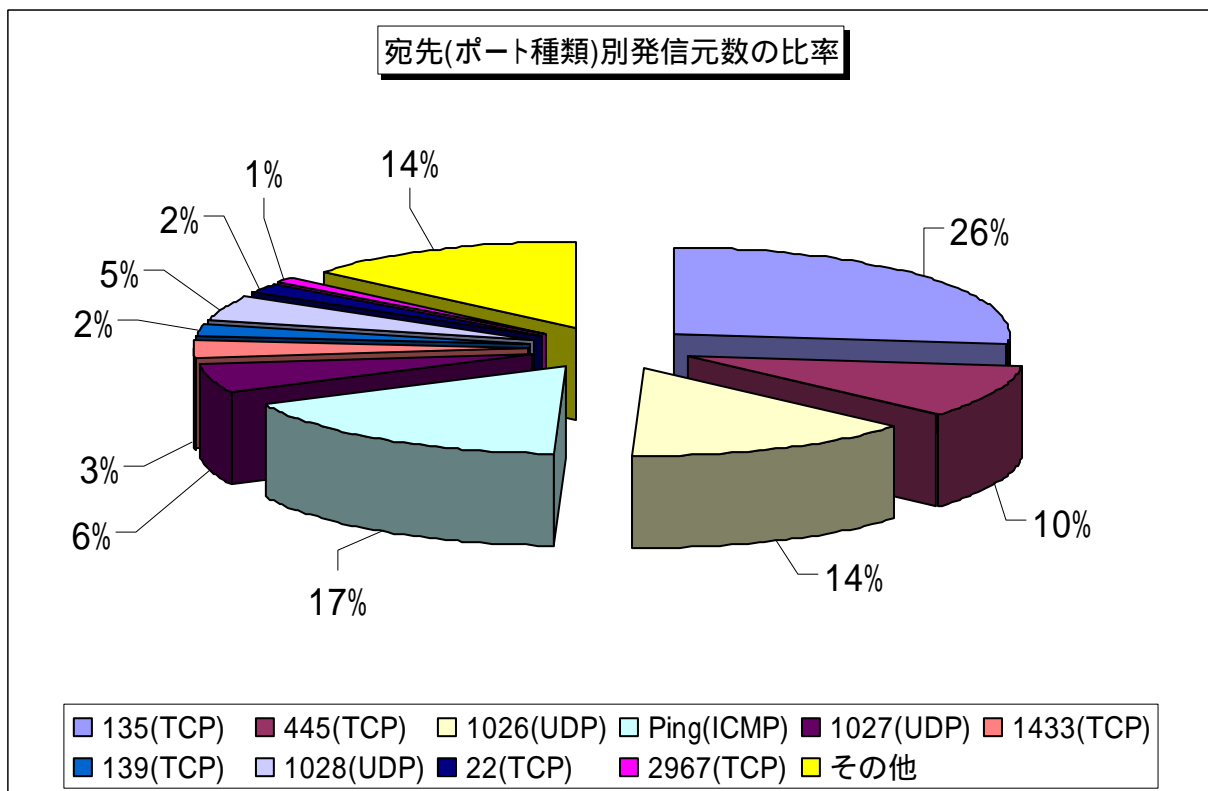
【図 2.2.2 2007年11月の一方的なアクセス状況(発信元数)】

2.3 2007年11月の宛先(ポート種類)別の比率

2007年11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。



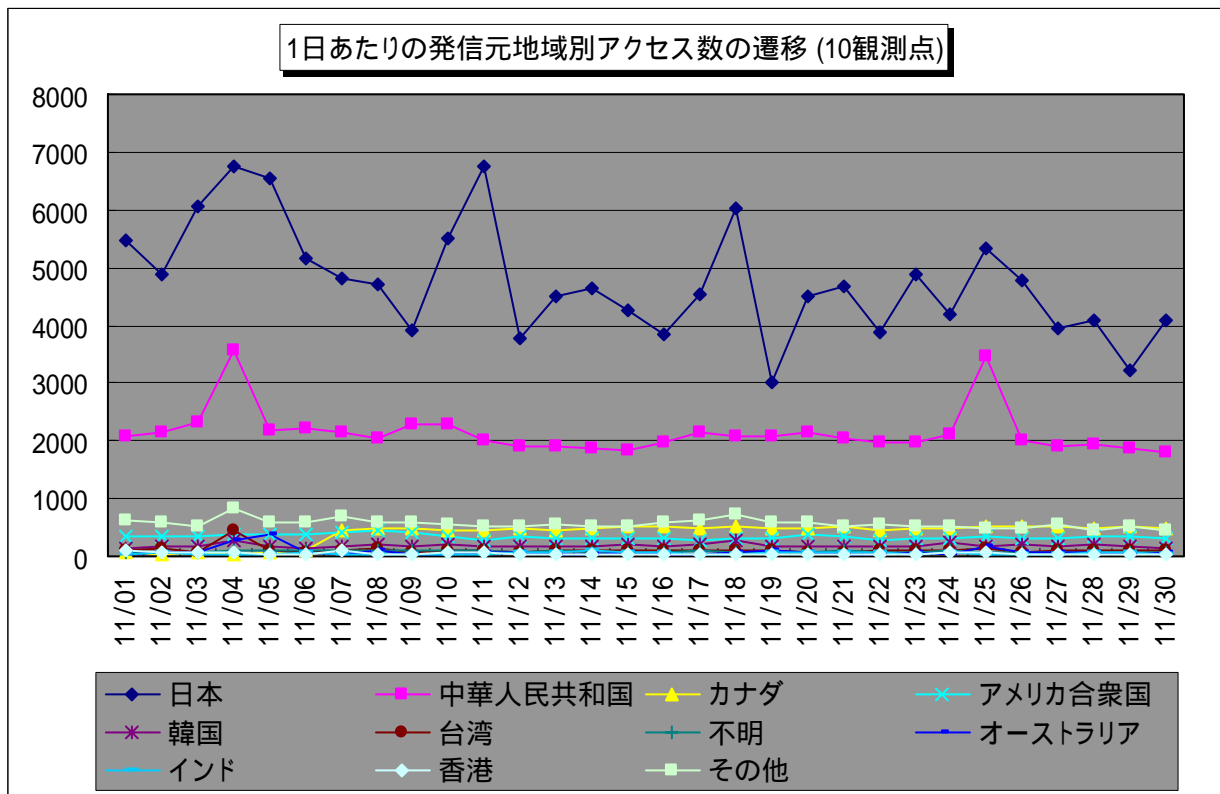
【図 2.3.1 2007年11月の宛先(ポート種類)別アクセス数の比率】



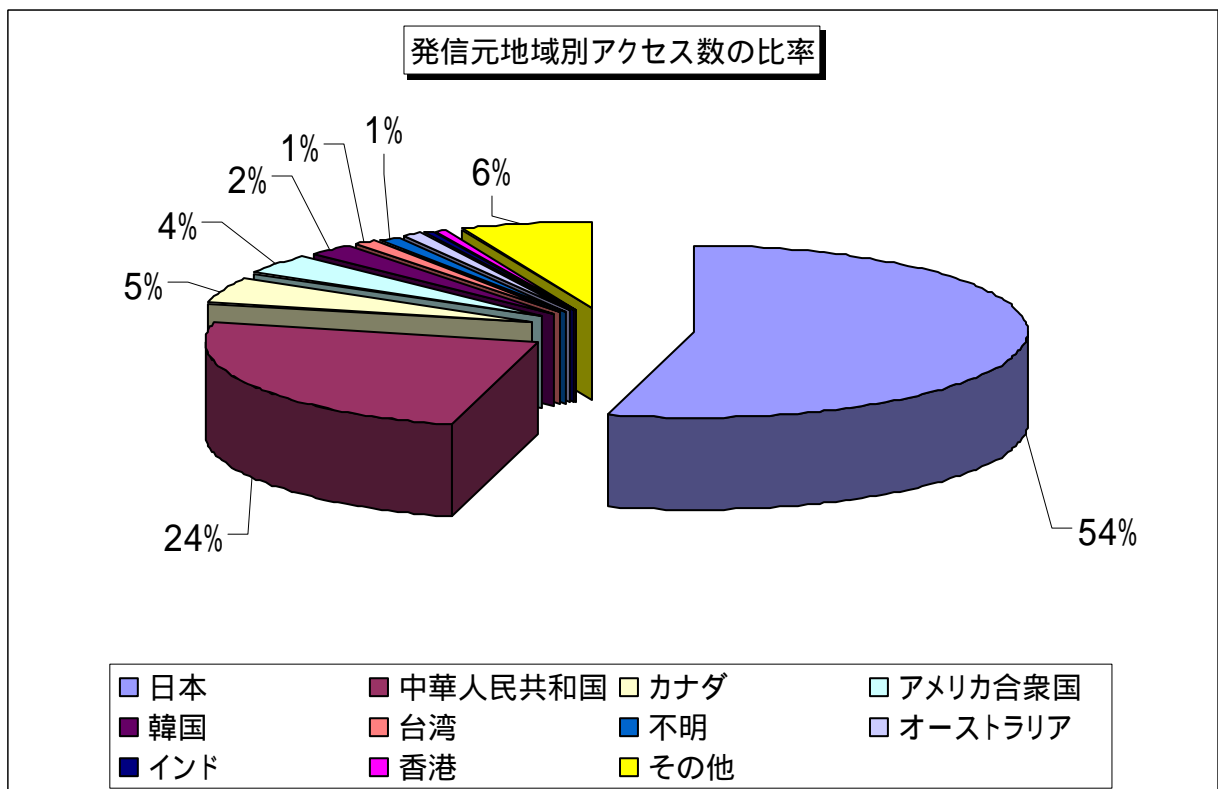
【図 2.3.2 2007年11月の宛先(ポート種類)別発信元数の比率】

2.4 2007年11月の発信元地域別アクセス状況

2007年11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。

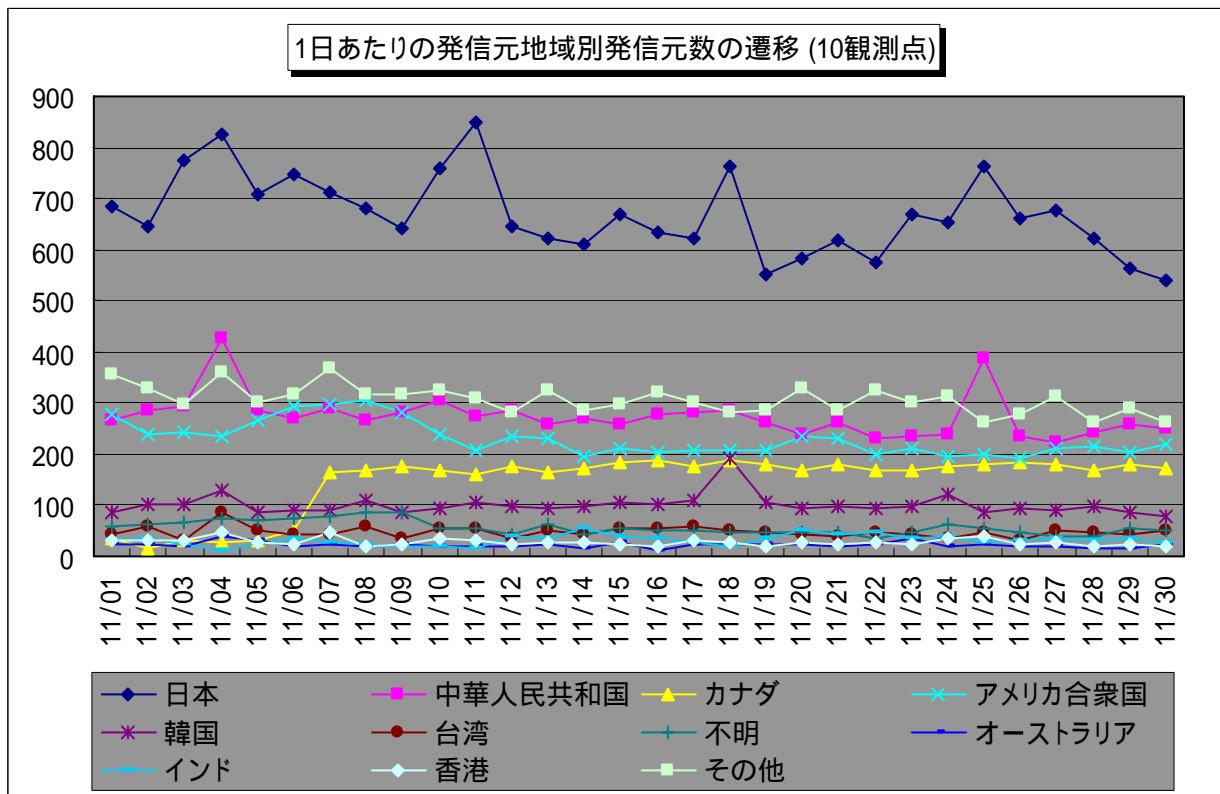


【図 2.4.1 2007年11月の発信元地域別アクセス数の変化】

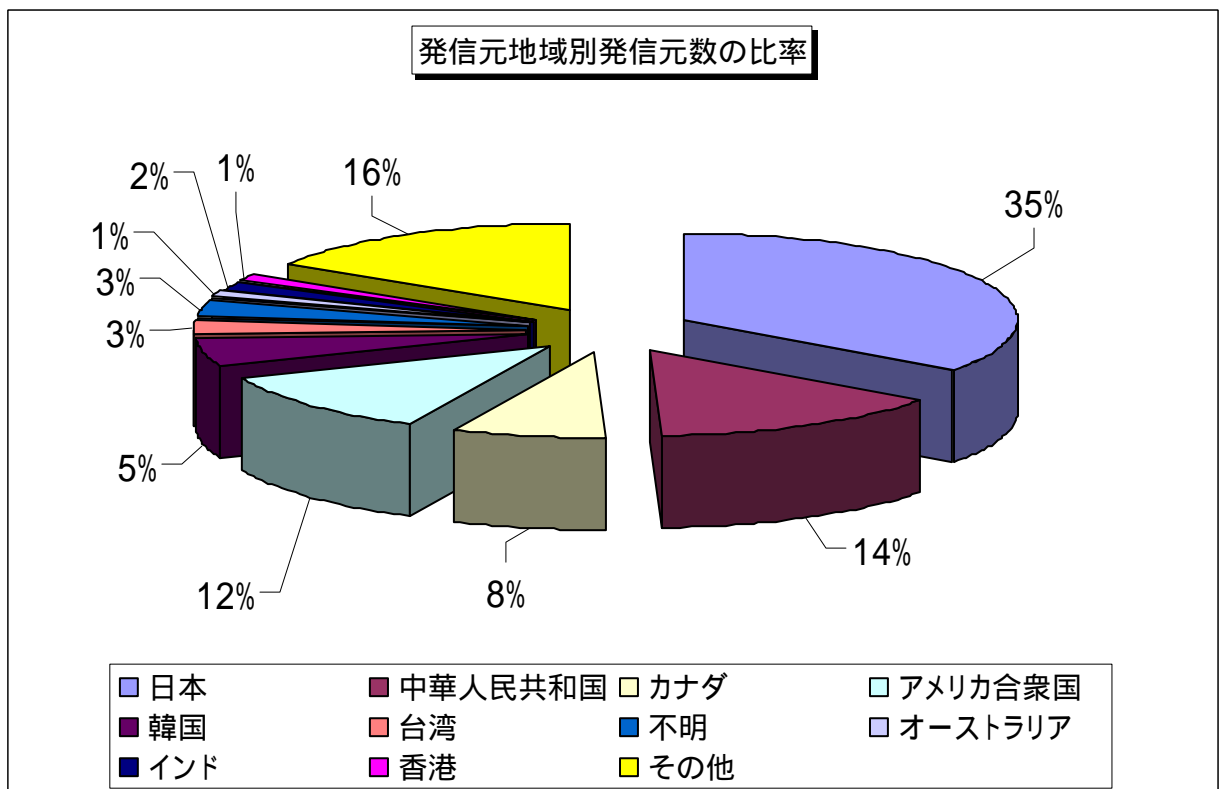


【図 2.4.2 2007年11月の発信元地域別アクセス数の比率】

2007年11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 2007年11月の発信元地域別発信元数の変化】

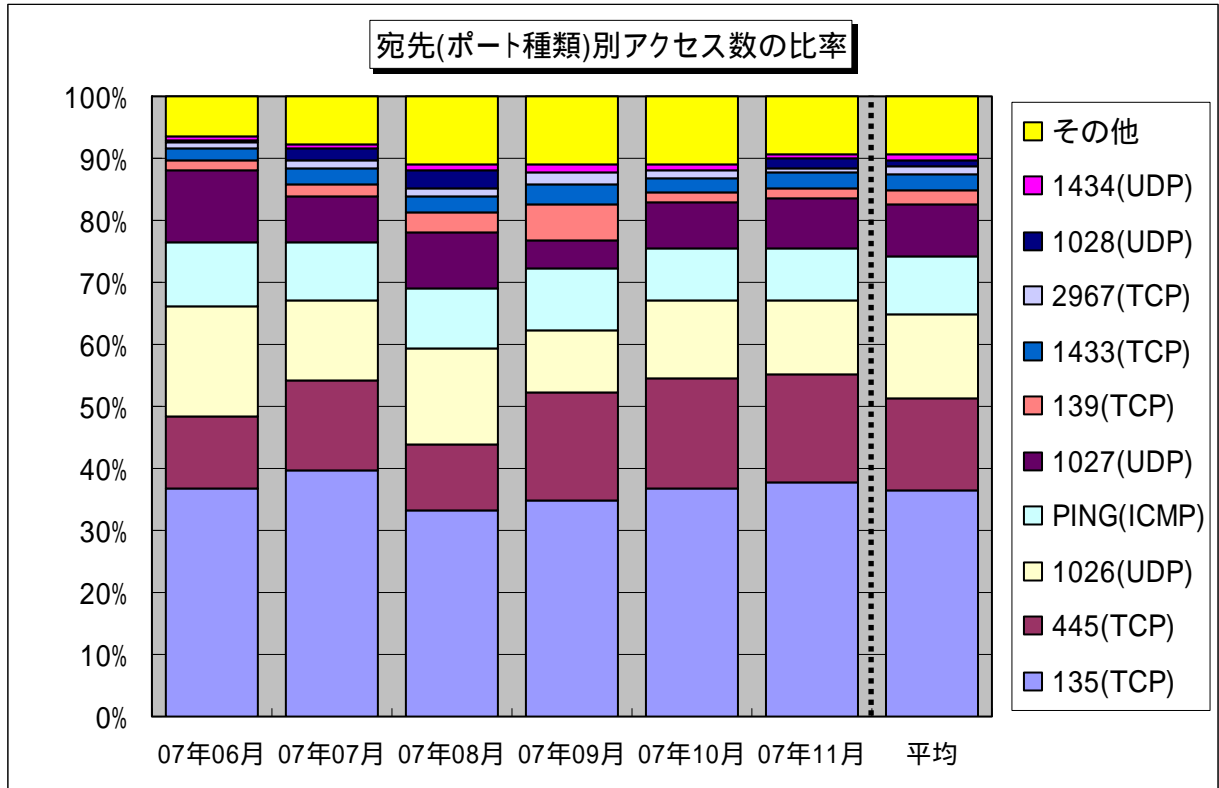


【図 2.4.4 2007年11月の発信元地域別発信元数の比率】

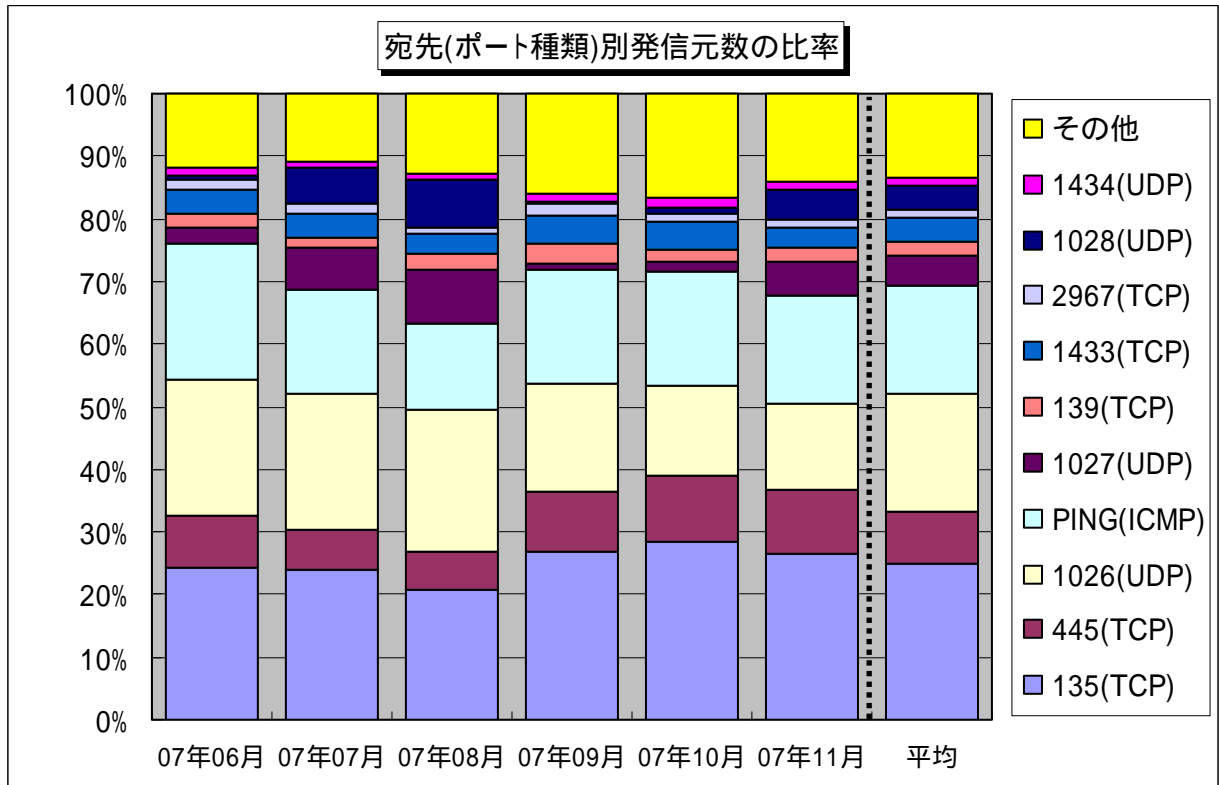
3. 統計情報

3.1 2007年6月～2007年11月の宛先(ポート種類)別の比率

2007年6月～2007年11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。



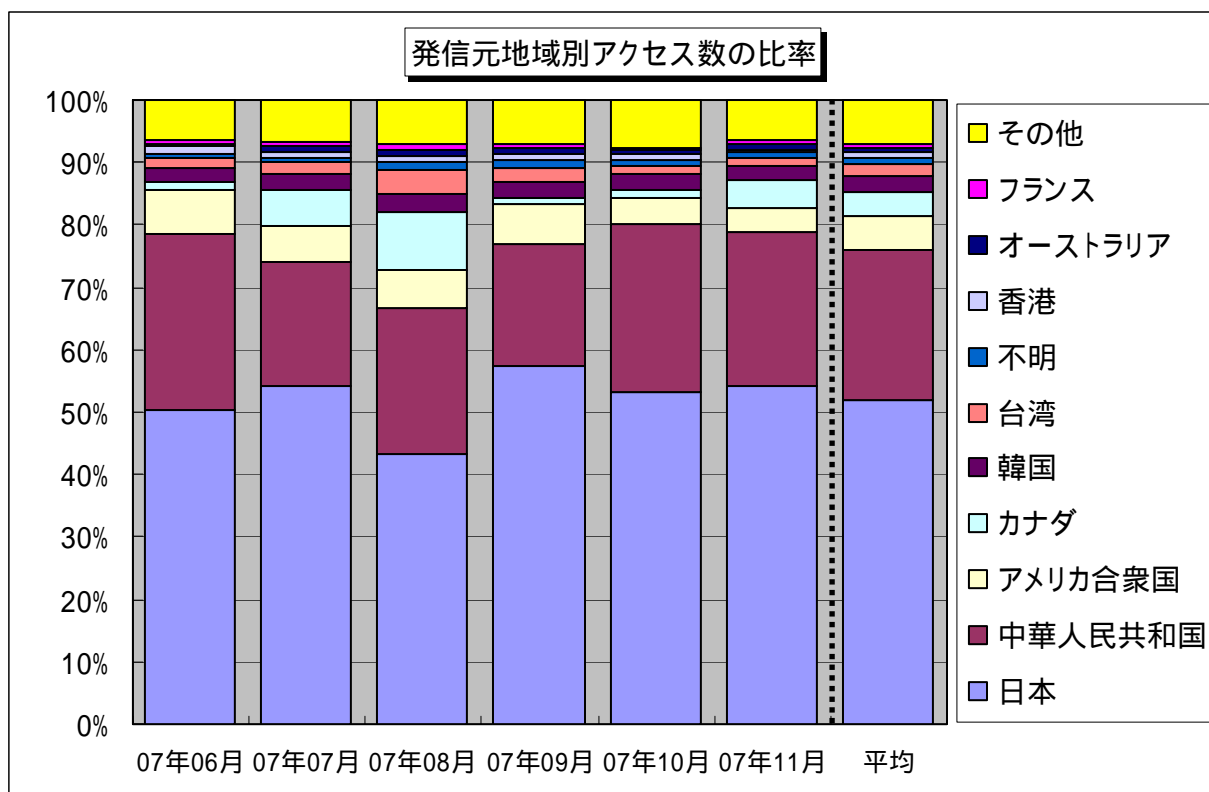
【図 3.1.1 2007年6月～2007年11月の宛先(ポート種類)別アクセス数の比率】



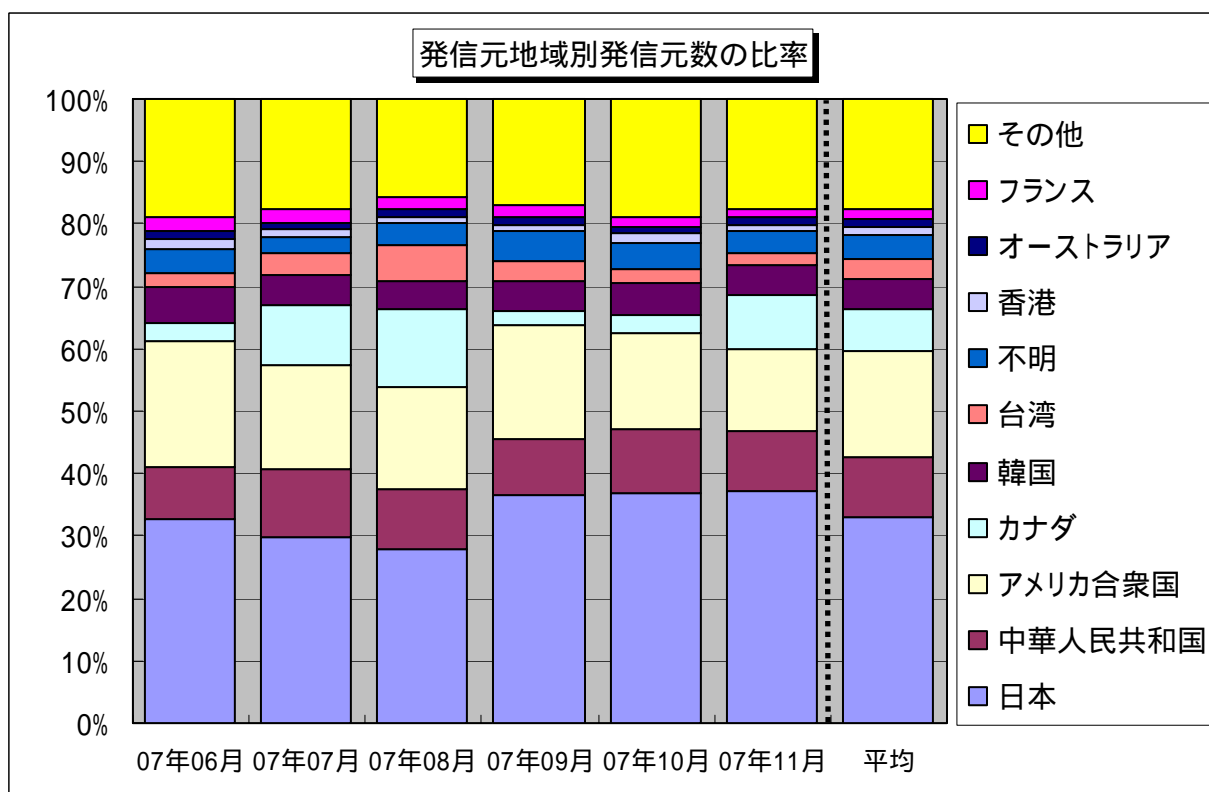
【図 3.1.2 2007年6月～2007年11月の宛先(ポート種類)別発信元数の比率】

3.2 2007年6月～2007年11月の発信元地域別の比率

2007年6月～2007年11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6月～2007年11月の発信元地域別アクセス数の比率】



【図 3.2.2 2007年6月～2007年11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11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) /1028(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
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りリモートからのコマンド実行ツール)を狙ったアクセス
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

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@jpa.go.jp