別紙 3

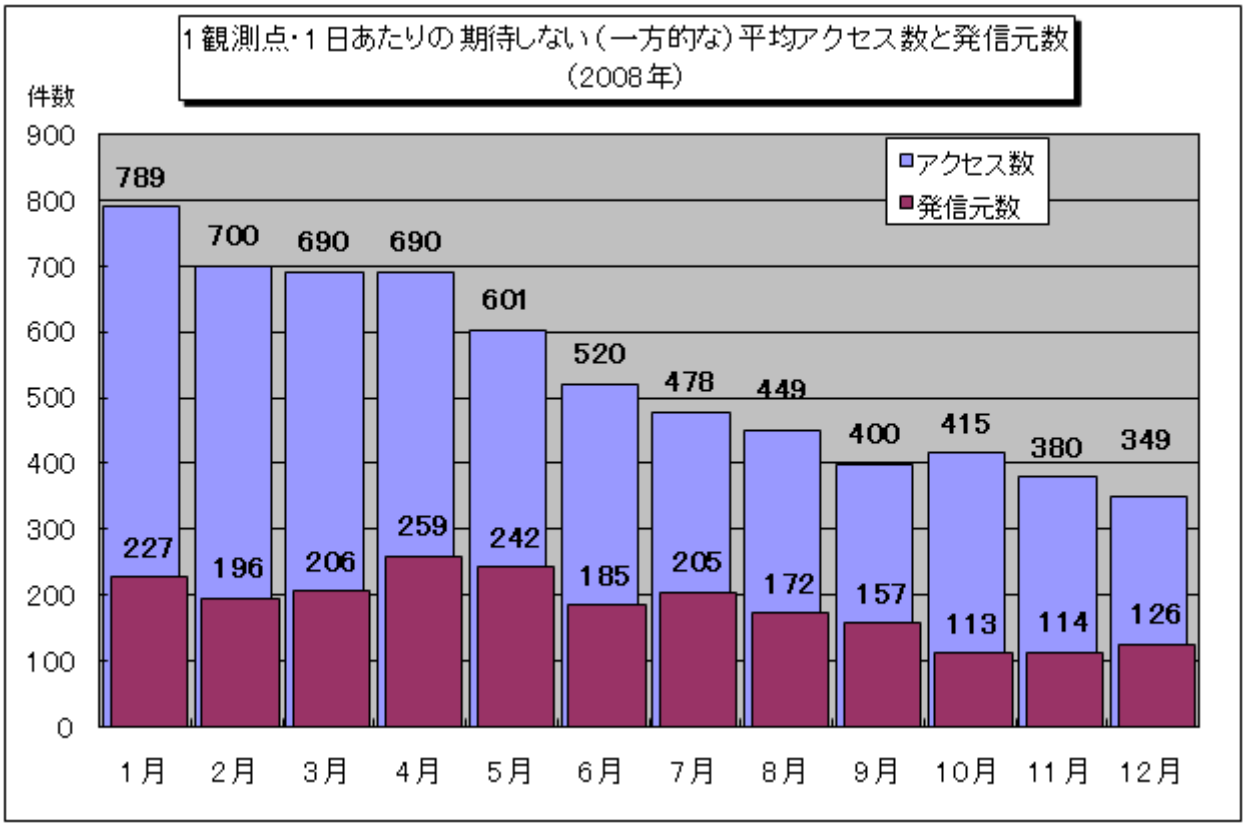
インターネット定点観測(TALOT2)での観測状況について

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、2008 年 12 月の期待しない(一方的な)アクセスの総数は 10 観測点で 108,338 件、総発信元(※)は 38,976 箇所ありました。平均すると、1 観測点につき 1 日あたり 126 の発信元から 349 件のアクセスがあったことになります。

総発信元(※)：TALOT2 にアクセスしてきた発信元の総数。同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合でも、発信元数は 1 としてカウント。

TALOT2 における各観測点の環境は、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。

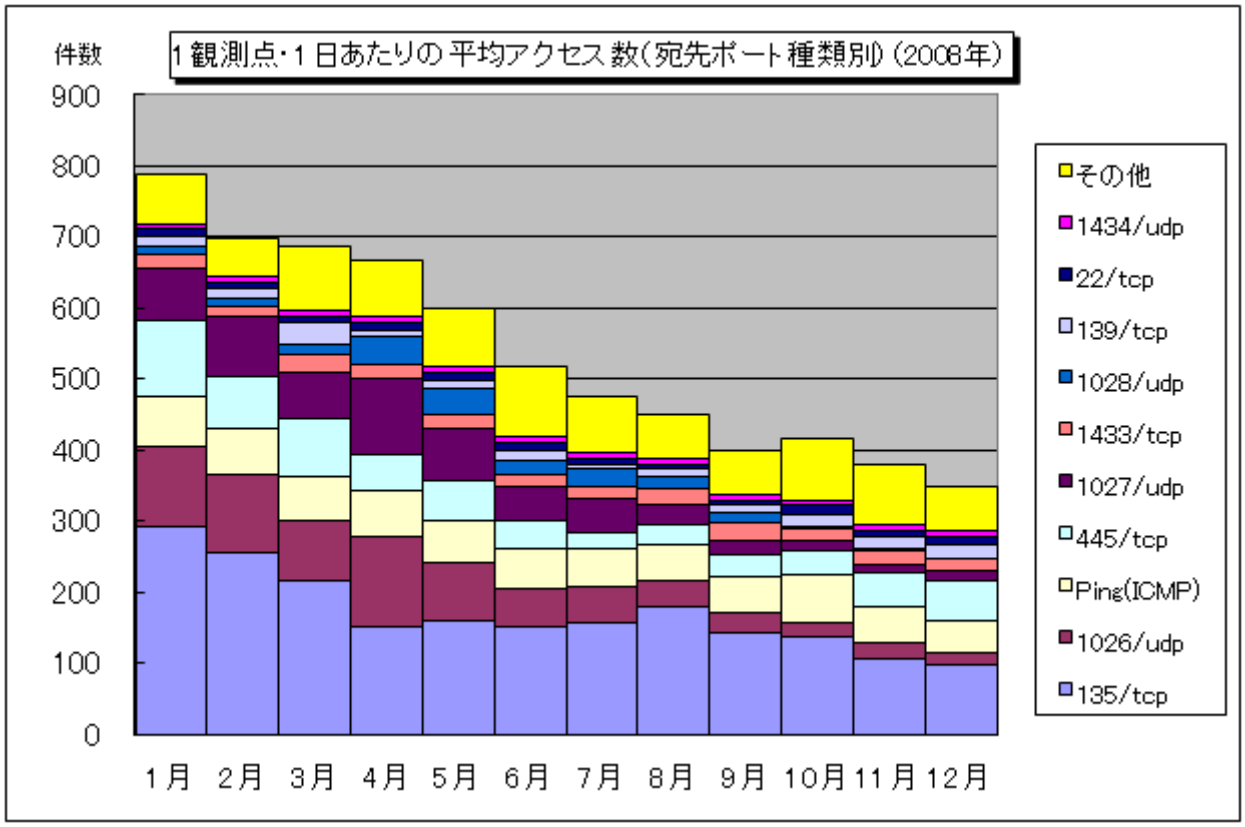


【図 1-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 1 月～2008 年 12 月までの各月の 1 観測点・1 日あたりの平均アクセス数と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、12 月の期待しない(一方的な)アクセスは 11 月と比べて若干減少しました。年間を通してみると、減少傾向にあると言えます。

2008 年の各月の 1 観測点･1 日あたりの平均アクセス数を宛先ポート種類別で表したものを図 1-2 に示します。この図を見ると、全体のアクセス数の推移において支配的と言える 135/tcp、1026/udp へのアクセスの減少が目立っており、それがアクセス数全体の減少に影響していると言えます。

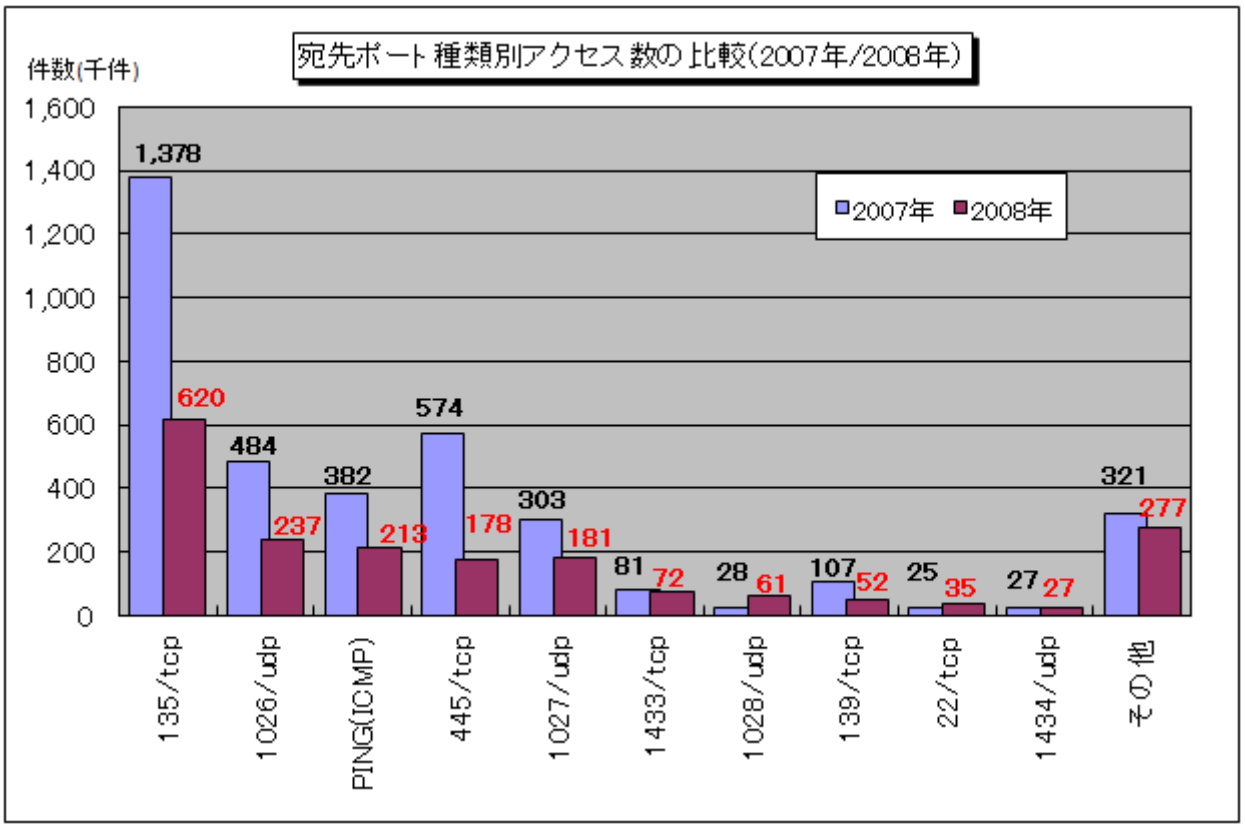
135/tcp は Windows の脆弱性を狙った攻撃を行う際に狙われる可能性が高いポートであり、1026/udp は 1027/udp とともに Windows のメッセンジャサービス機能を利用して、悪意あるメッセージを送りつける際に狙われる可能性が高いポートです。



【図 1-2 1 観測点・1 日あたりの平均アクセス数（宛先ポート種類別）（2008 年)】

2．2008 年のアクセス状況

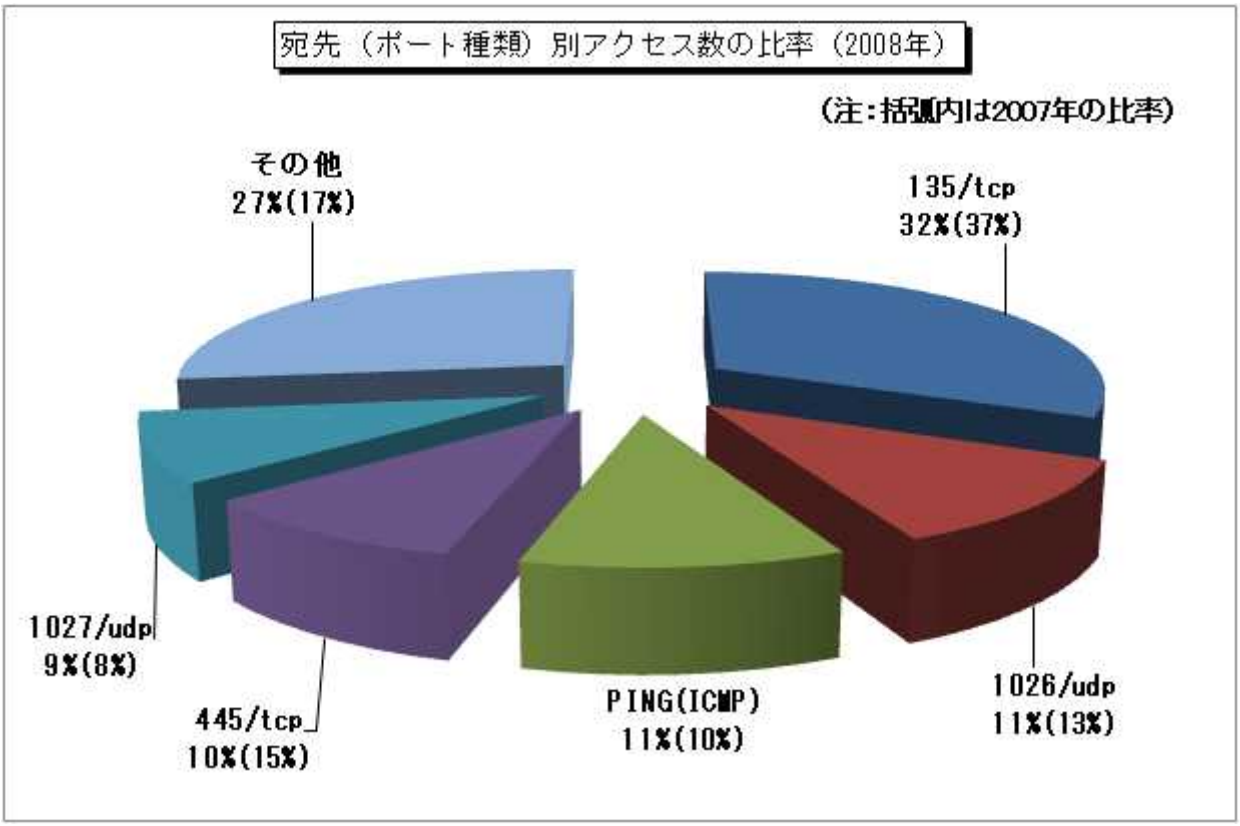
2007 年と 2008 年の宛先ポート種類別アクセス数の比較結果について図 2-1 に示します。大幅に減少したのは、135/tcp へのアクセスであり、約 760 万件の減少（2007 年比で約 45%）でした。次いで、445/tcp が約 450 万件の減少（2007 年比で約 31%）で、1026/udp が約 250 万件の減少（2007 年比で約 49%）でした。アクセス数の推移において支配的なこれらのポートへのアクセスが大幅に減少していることが、全体のアクセス数の推移に影響していると言えます。



【図 2-1 宛先ポート種類別アクセス数の比較（2007 年/2008 年)】

2008 年の宛先ポート種類別アクセス数の比率を図 2-2 に示します。135/tcp をはじめ、上位 5 位までのアクセス数の合計で、全体の 73%を占めていることが分かります。

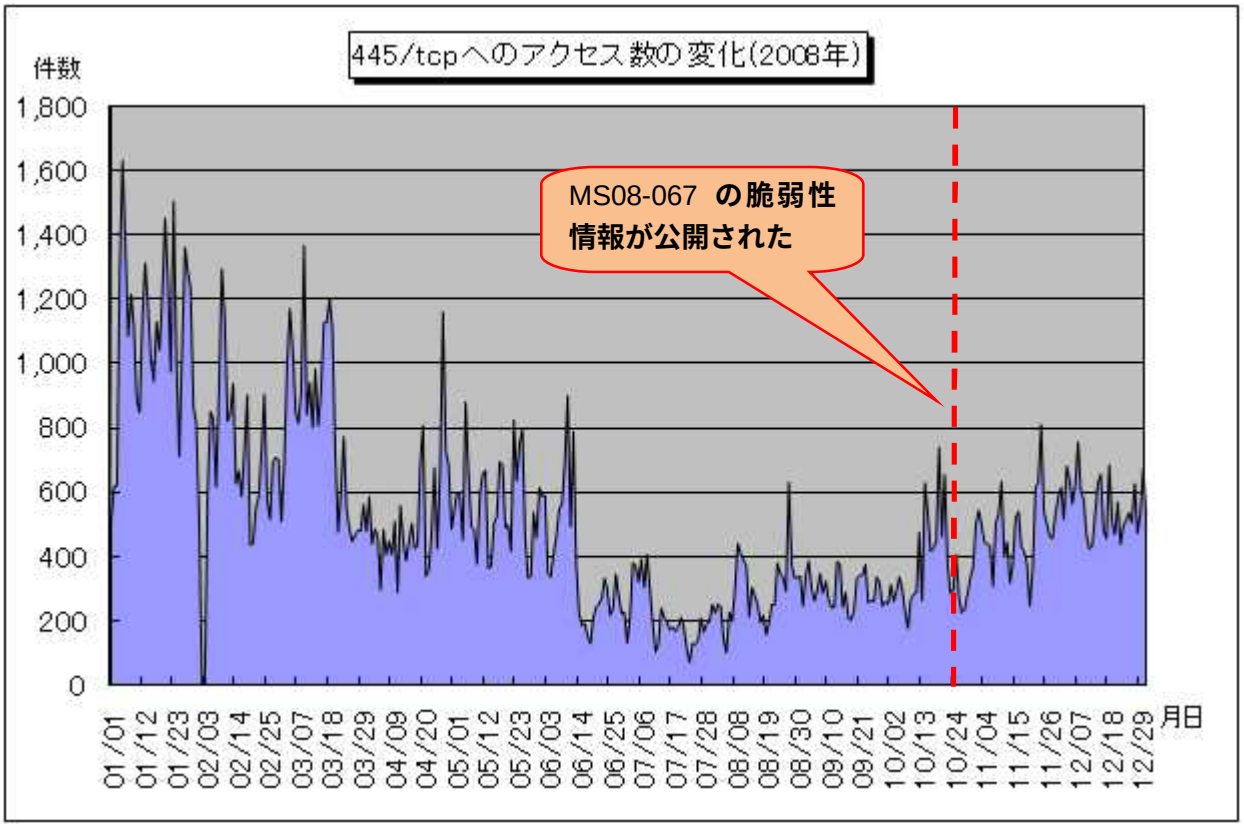
なお、2007 年においても上位 5 位の組み合わせは同様であり、それらの合計は全体の 83%を占めていました。



【図 2-2 宛先ポート種類別アクセス数の比率（2008 年)】

(1)脆弱性を突くウイルスによる攻撃と思われる 445/tcp へのアクセス数の増加

2008 年の 445/tcp へのアクセス数の変化を、図 2-3 に示します。2008 年の 445/tcp へのアクセス状況は、7 月頃まで減少傾向を示していましたが、その後、緩やかに増加傾向を示し、12 月末の時点でもその傾向が続いています。



【図 2-3 445/tcp へのアクセス数の変化（2008 年)】

このアクセス数の増加について原因は定かではありませんが、10 月頃からの増加に関しては、日本時間の 10 月 24 日にマイクロソフトから緊急に発表された、MS08-067 の脆弱性に関連した攻撃が影響していた可能性があります。マイクロソフトの情報によると、脆弱性情報が公開される 2 週間ほど前から、この脆弱性を突いた攻撃がすでに行われていたとのことです。

＜参考情報＞

■「Server サービスの脆弱性により、リモートでコードが実行される」（マイクロソフト）
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

この脆弱性情報の公開以降、445/tcp へのアクセス数の増加は、定点観測を行っている他の組織においても観測されており、この脆弱性を突くウイルスによる感染の試みであった可能性があります。また、実際に、この脆弱性を突くウイルスや攻撃ツールの存在が確認されています。

日頃から脆弱性情報には十分注意し、新しい脆弱性情報が公開されたら、速やかに対処することが基本的な対策となります。

＜参考情報＞

■「TCP 445 番ポートへのスキャン増加に関する注意喚起」
http://www.jpcert.or.jp/at/2008/at080019.txt

■「脆弱性 （MS08-067：CVE-2008-4250）を悪用したハッキングツールを確認」
http://blog.trendmicro.co.jp/archives/2115

(2)定点観測を開始してから 2008 年 12 月までのアクセス状況

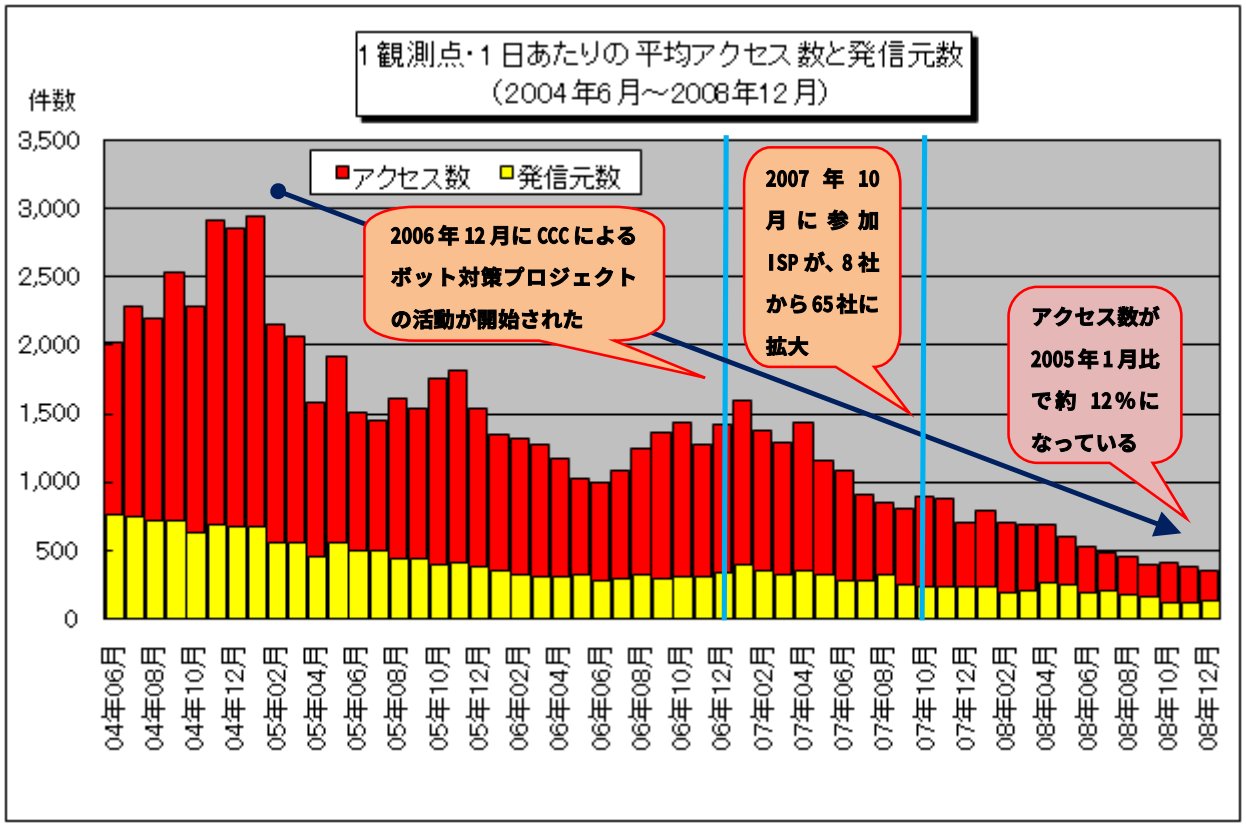
TALOT2 による定点観測を開始した 2004 年 6 月から 2008 年 12 月までの、1 観測点・1 日あたりの平均アクセス数と発信元数を図 2-4 に示します。2008 年 12 月の平均アクセス数は、2005 年 1 月比で約 12%になっています。このうち 2006 年 12 月からの減少傾向については、その頃に活動が開始された CCC（サイバークリーンセンター）によるボット対策プロジェクトの活動の効果が、要因の一つとして挙げられます。

CCC では、ボット検体の収集・解析、ボット駆除ツールの作成・配布、プロジェクトに参加している ISP(インターネットサービスプロバイダ)を通じて、ボットに感染していると思われるユーザへの注意喚起といった活動を行っています。また、2007 年 10 月には、プロジェクトに参加する ISP が 8 社から 65 社へ大幅に拡大されました。これによって、さらに 2007 年 10 月以降の国内からのアクセス数の減少につながっています。

＜参考情報＞

■総務省・経済産業省 連携プロジェクト Cyber Clean Center

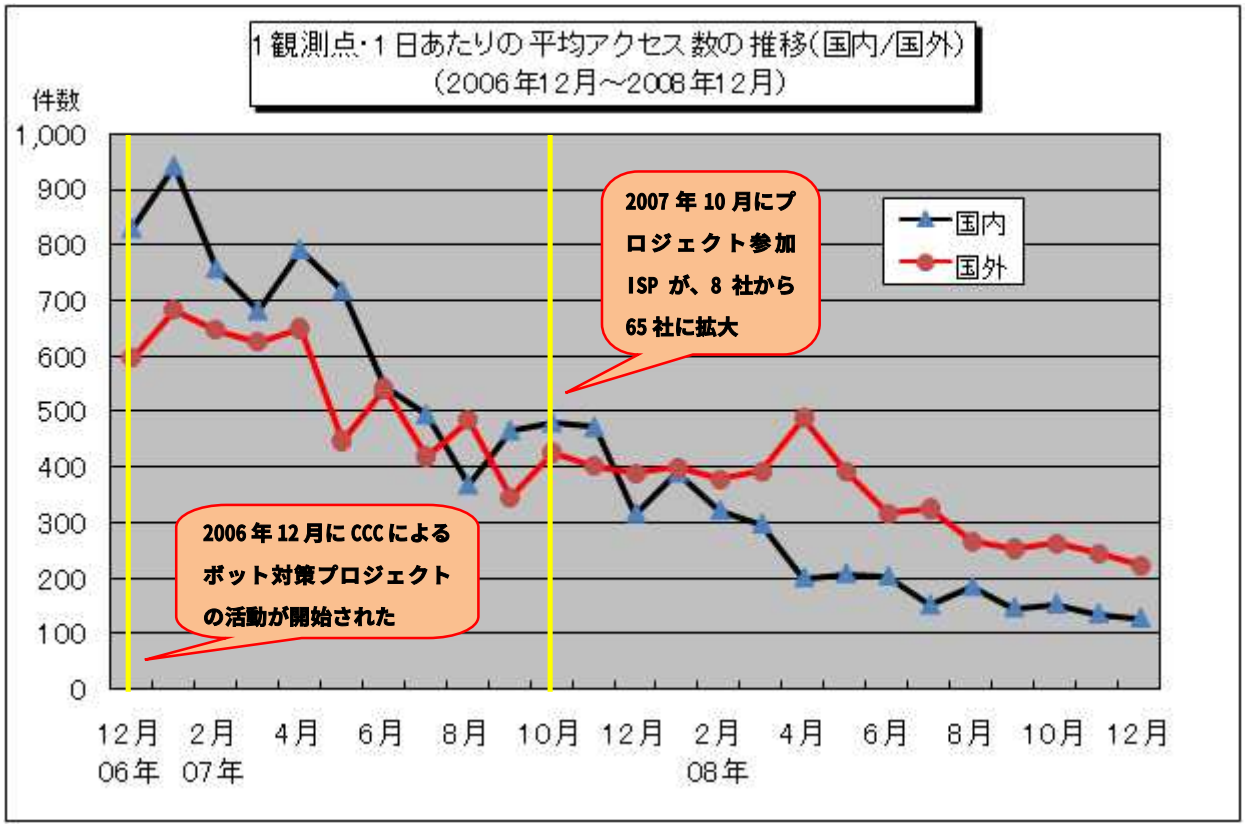
https://www.ccc.go.jp/



【図 2-4 1 観測点・1 日あたりの平均アクセス数と発信元数（2004 年 6 月～2008 年 12 月)】

CCC が活動を開始してから 2008 年 12 月までの、国内からと国外からの平均アクセス数の推移を図 2-5 に示します。この図を見ると、国内・国外ともにアクセス数が減少していますが、国内からのアクセス数の減少の方がより顕著です。

このことからも、国内のボットの駆除を進めている CCC の活動が効果を上げていると思われます。

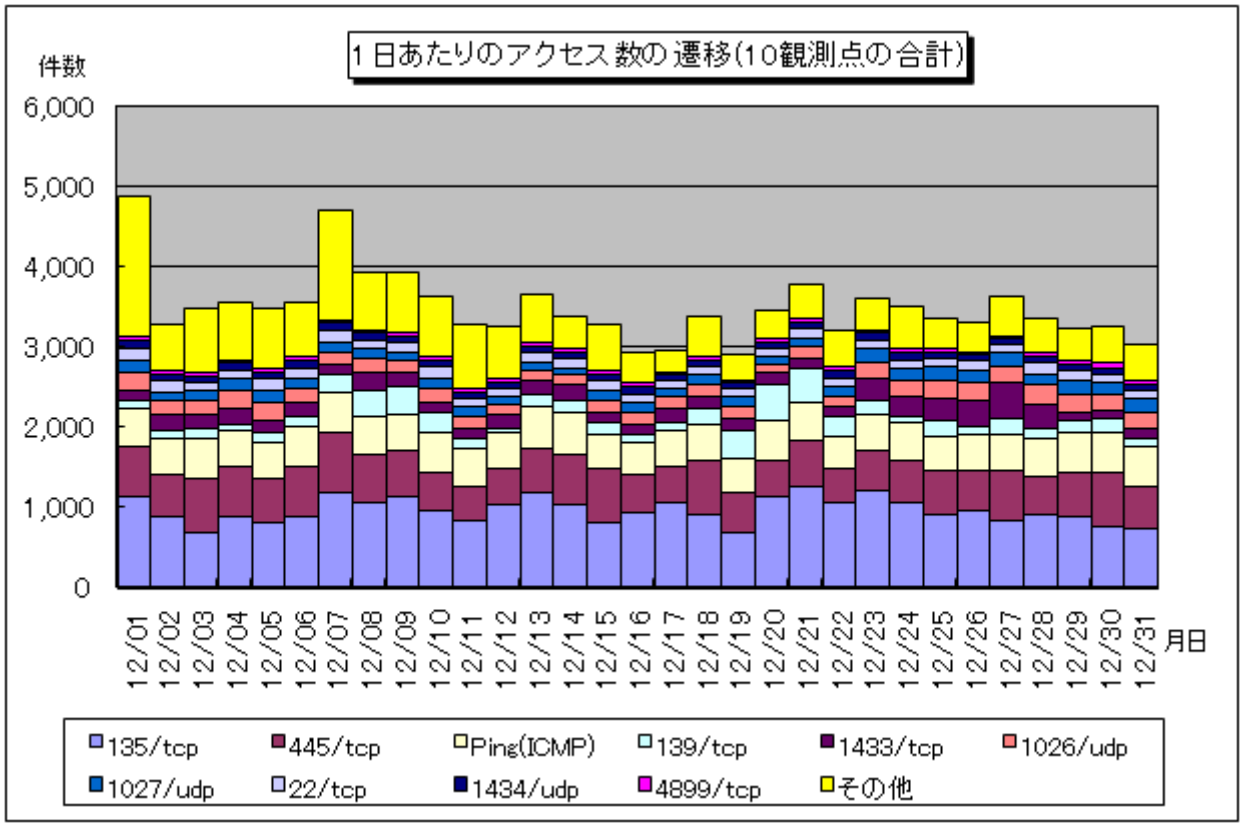


【図 2-5 1 観測点・1 日あたりの平均アクセス数の推移（国内/国外）
（2006 年 12 月～2008 年 12 月）】

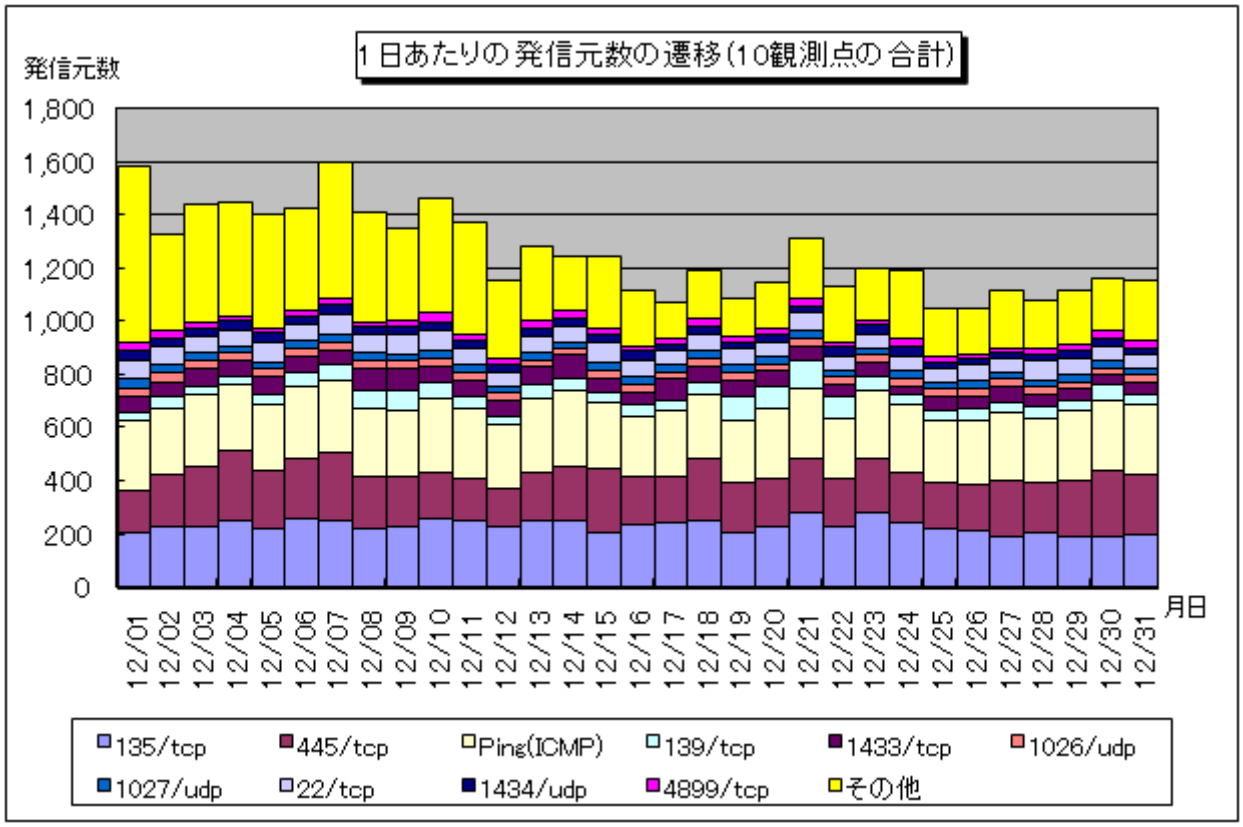
3．2008 年 12 月のアクセス状況

(1)宛先(ポート種類)別のアクセス状況

2008 年 12 月の一方的なアクセス状況(アクセス数)の遷移を図 3-1 に、一方的なアクセス状況(発信元数)の遷移を図 3-2 に示します。



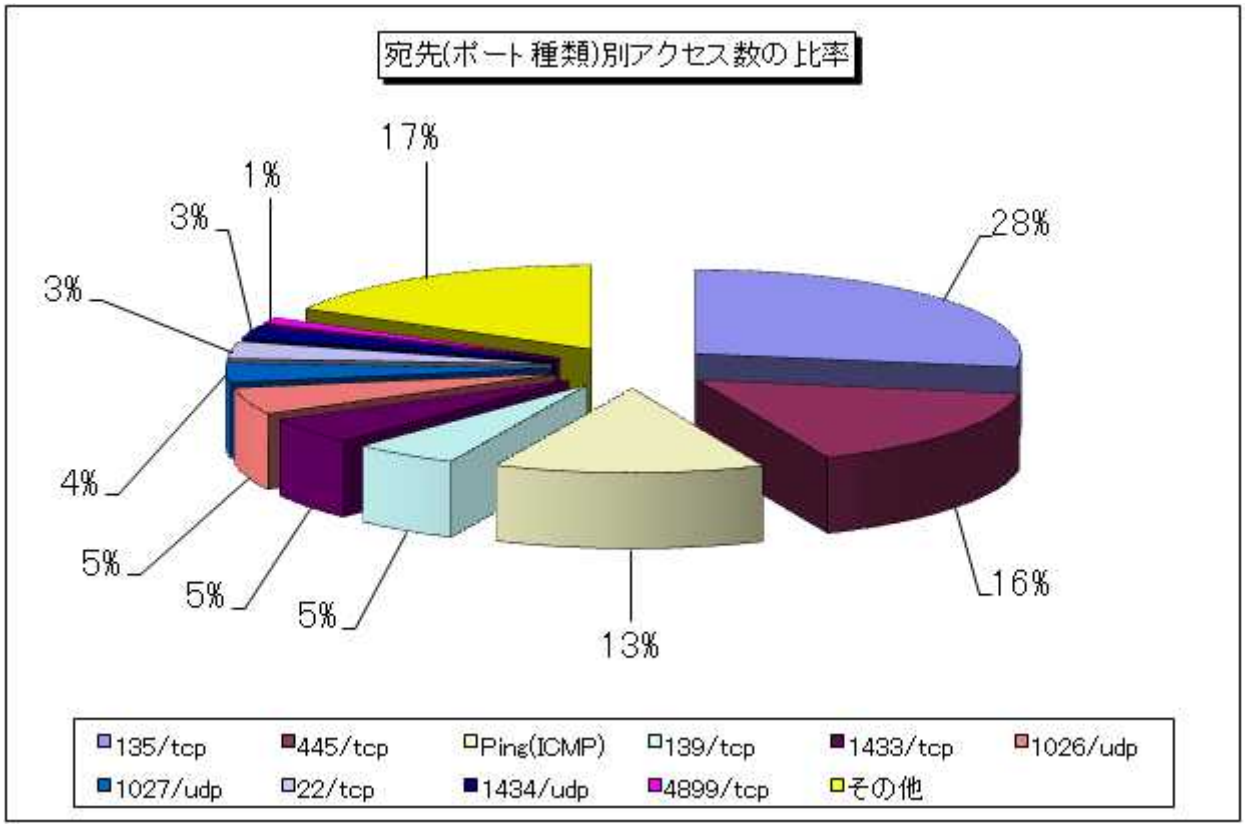
【図 3-1 2008 年 12 月の 1 日あたりのアクセス数の遷移】



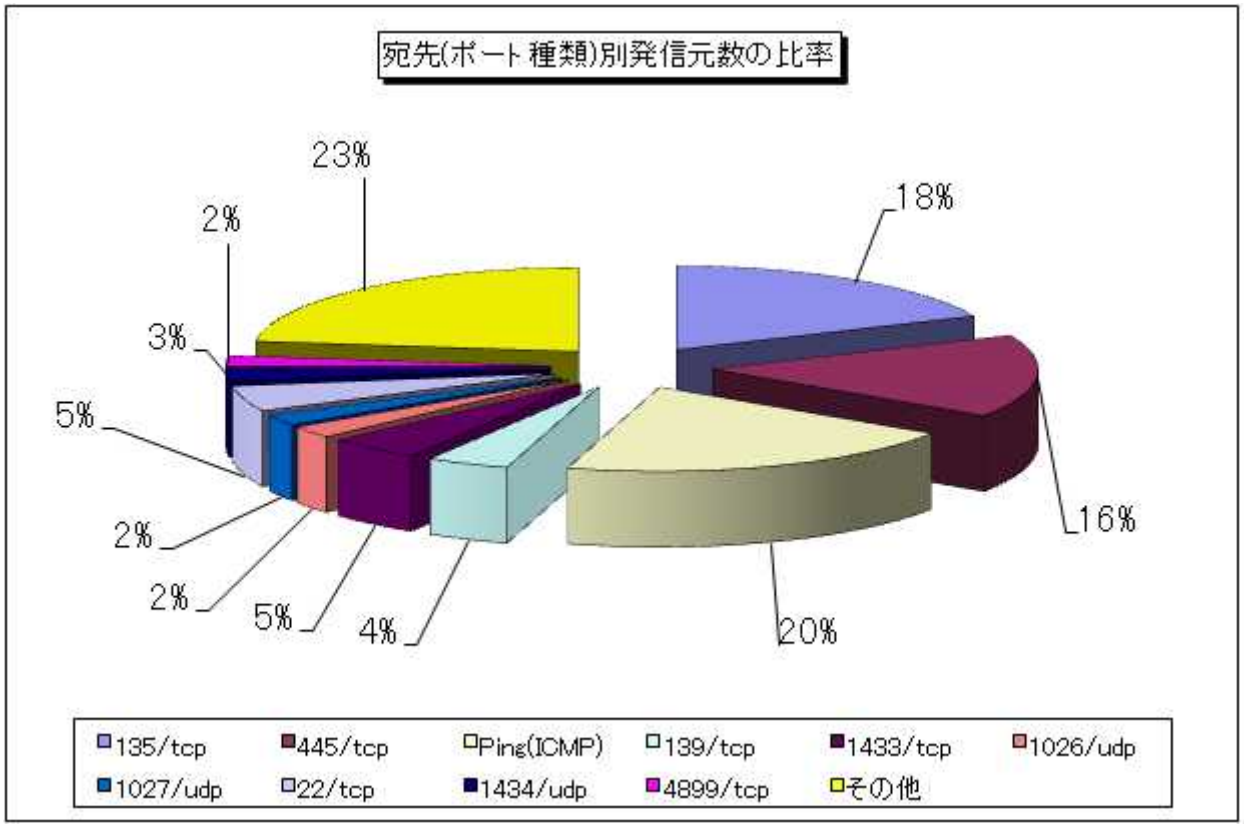
【図 3-2 2008 年 12 月の 1 日あたりの発信元数の遷移】

(2)宛先(ポート種類)別の比率

2008 年 12 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 3-3 に、宛先(ポート種類)別発信元数の比率を図 3-4 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



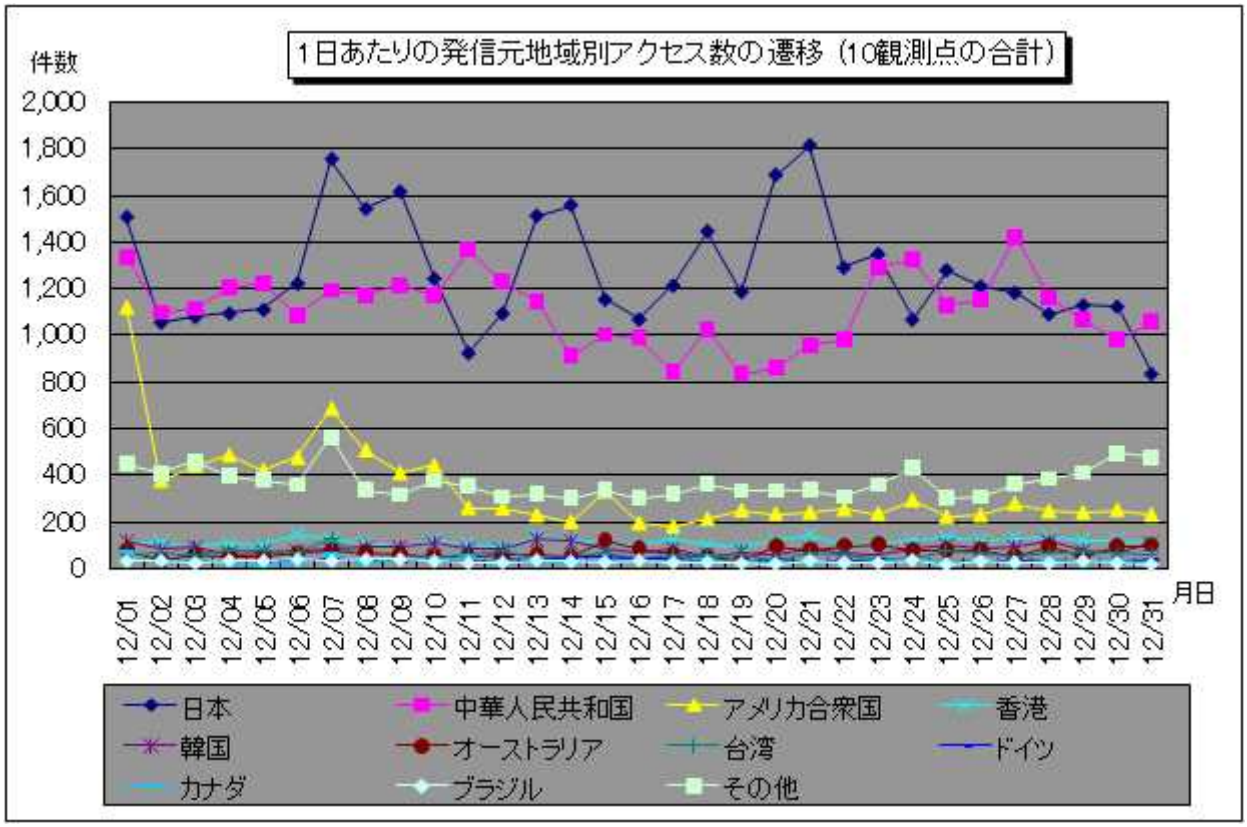
【図 3-3 2008 年 12 月の宛先(ポート種類)別アクセス数の比率】



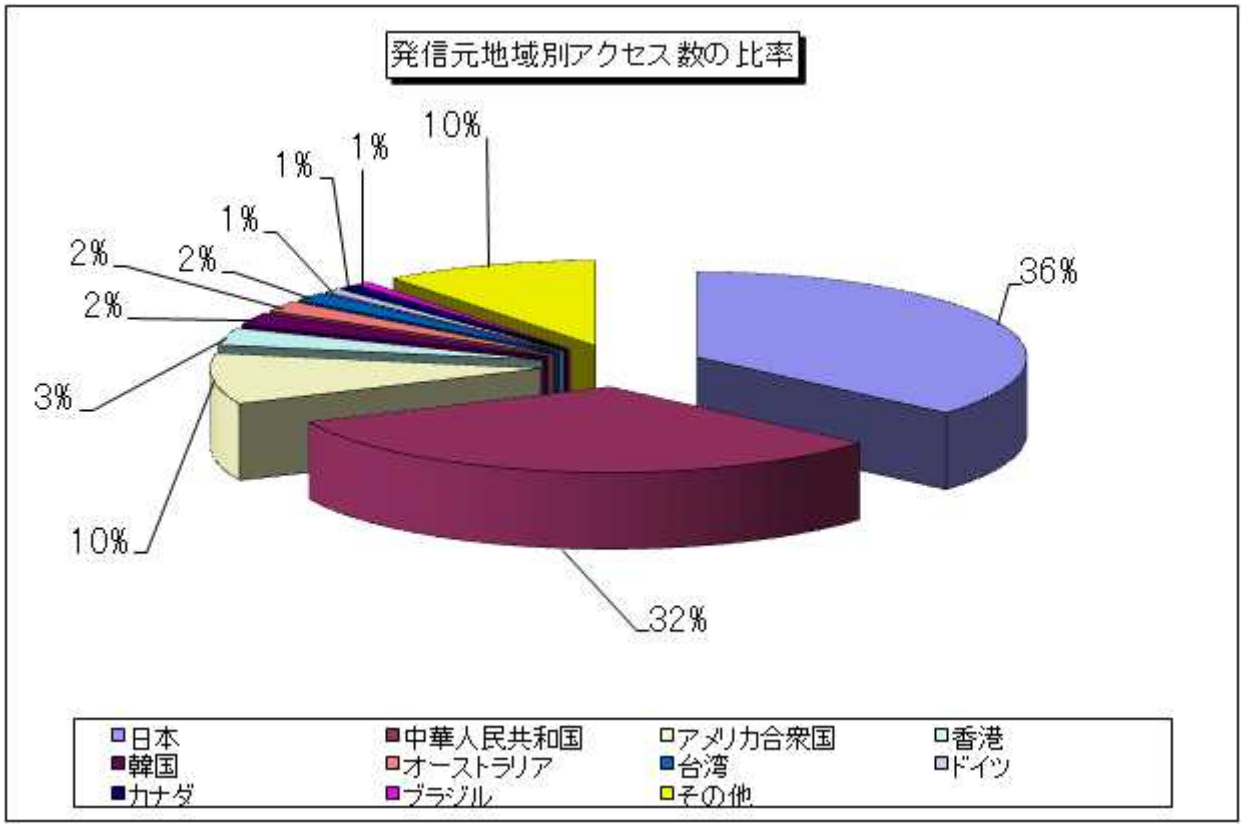
【図 3-4 2008 年 12 月の宛先(ポート種類)別発信元数の比率】

(3)発信元地域別のアクセス状況

2008 年 12 月の一方的なアクセスの発信元地域別アクセス数の遷移を図 3-5 に、発信元地域別アクセス数の比率を図 3-6 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。

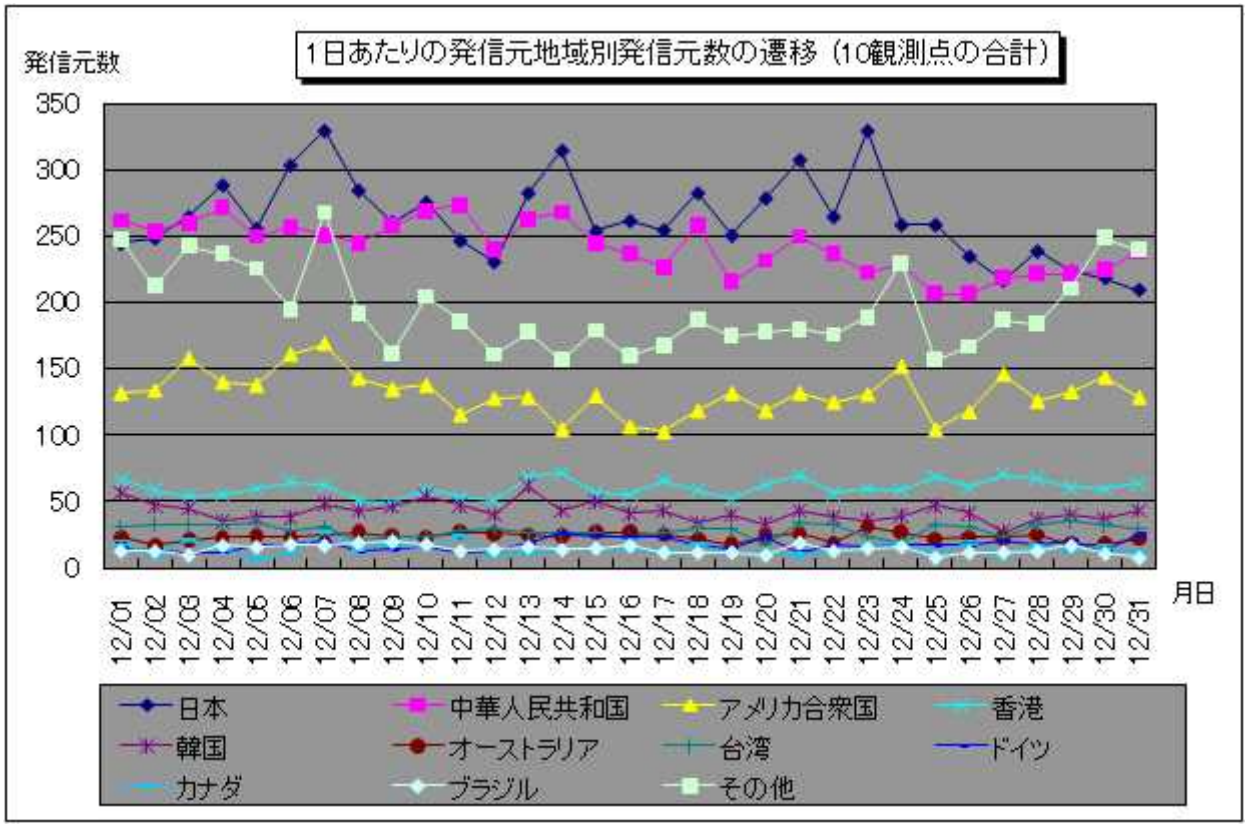


【図 3-5 2008 年 12 月の 1 日あたりの発信元地域別アクセス数の遷移】

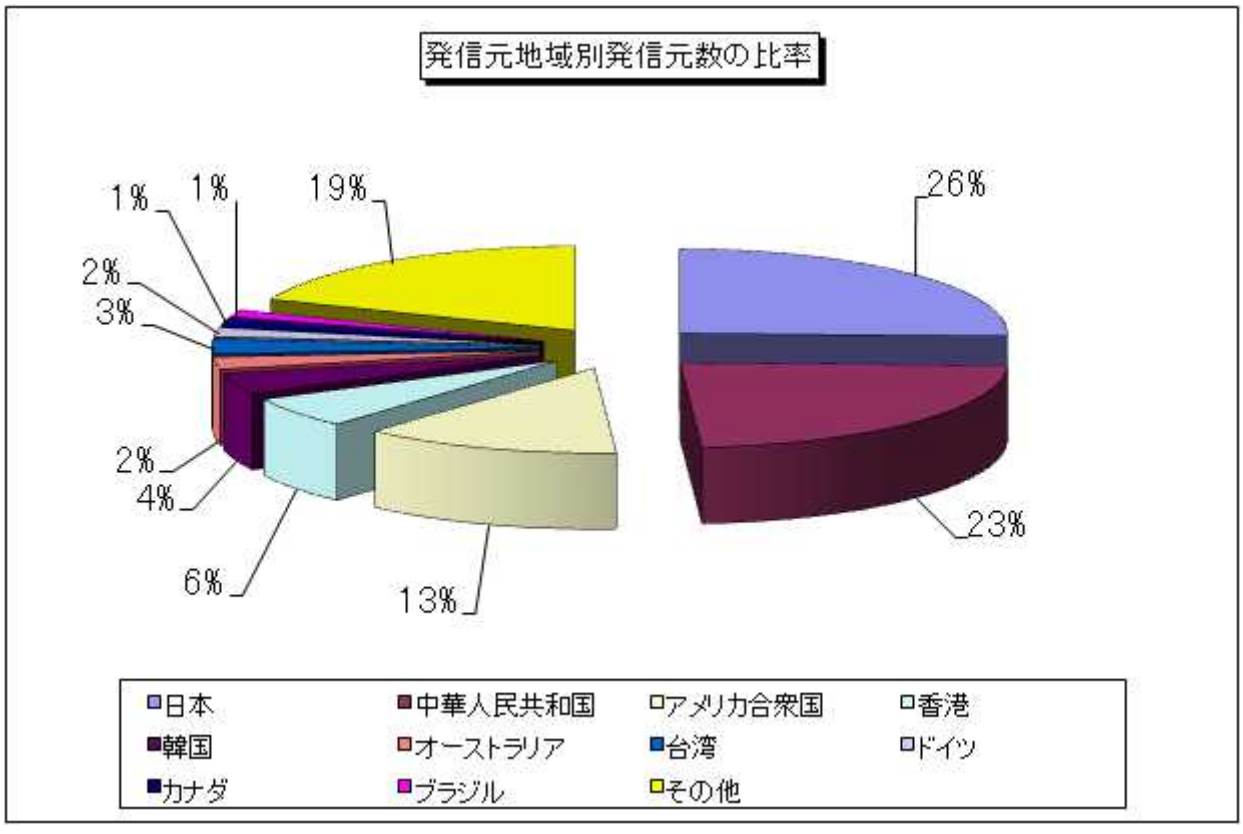


【図 3-6 2008 年 12 月の発信元地域別アクセス数の比率】

2008 年 12 月の一方的なアクセスの発信元地域別発信元数の遷移を図 3-7 に、発信元地域別発信元数の比率を図 3-8 に示します。なお、比率の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。



【図 3-7 2008 年 12 月の 1 日あたりの発信元地域別発信元数の遷移】

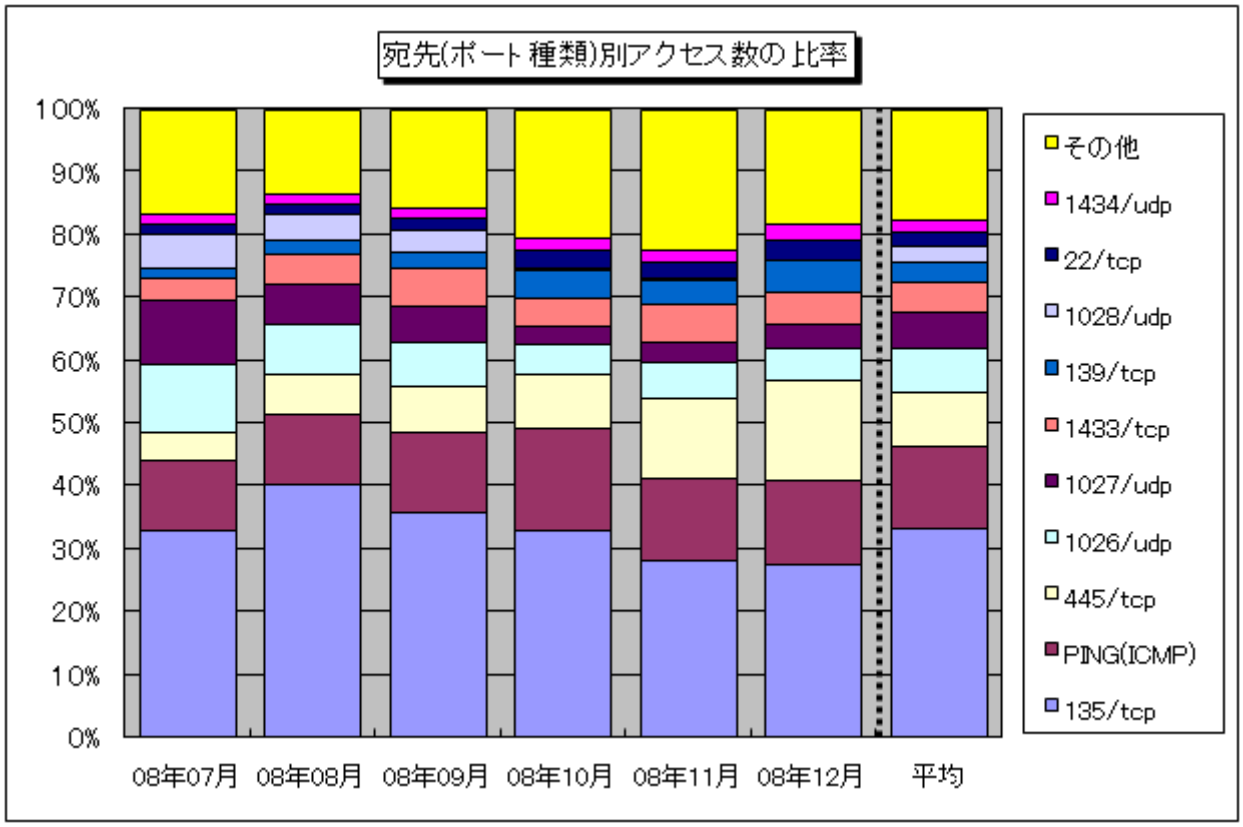


【図 3-8 2008 年 12 月の発信元地域別発信元数の比率】

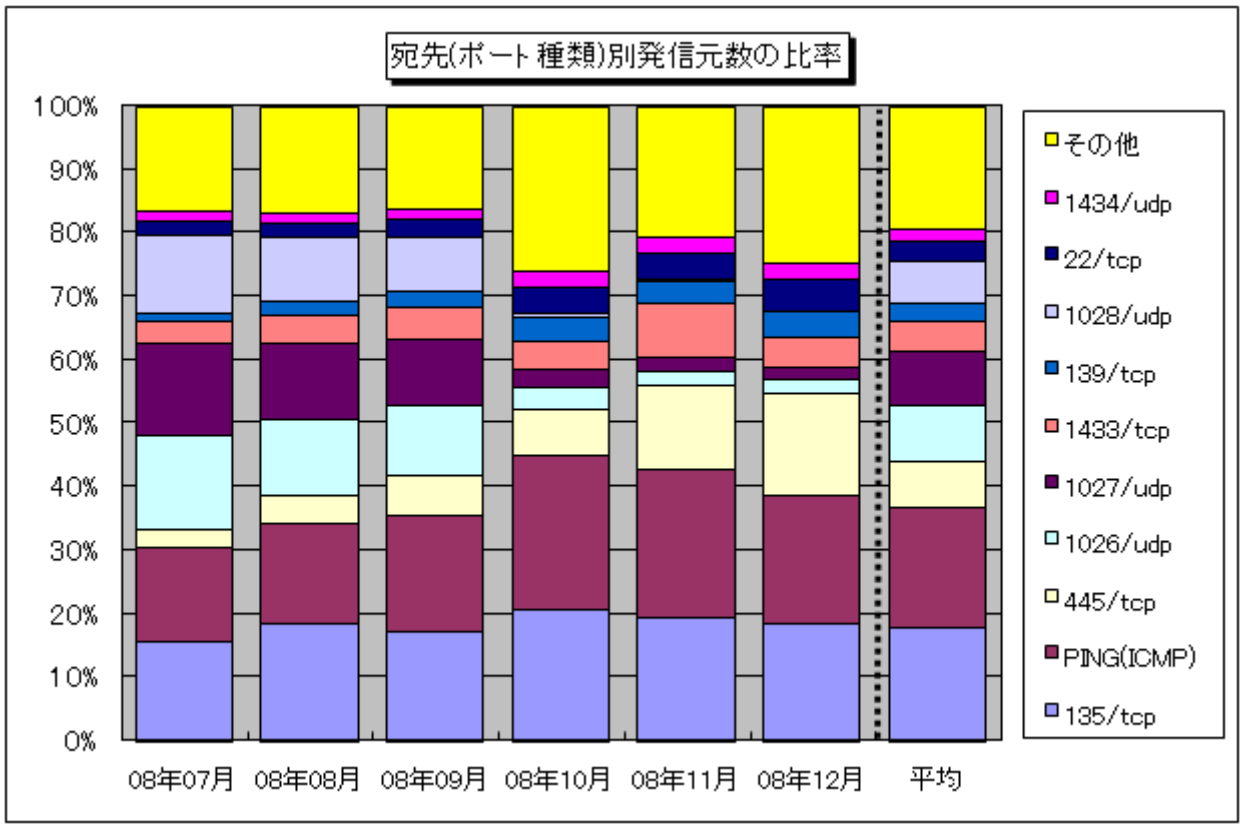
4．2008 年 7 月～2008 年 12 月のアクセス状況の比較

(1)宛先(ポート種類)別の比率

2008 年 7 月～2008 年 12 月の宛先(ポート種類)別アクセス数の比率を図 4- 1 に、宛先(ポート種類)別発信元数の比率を図 4-2 に示します。



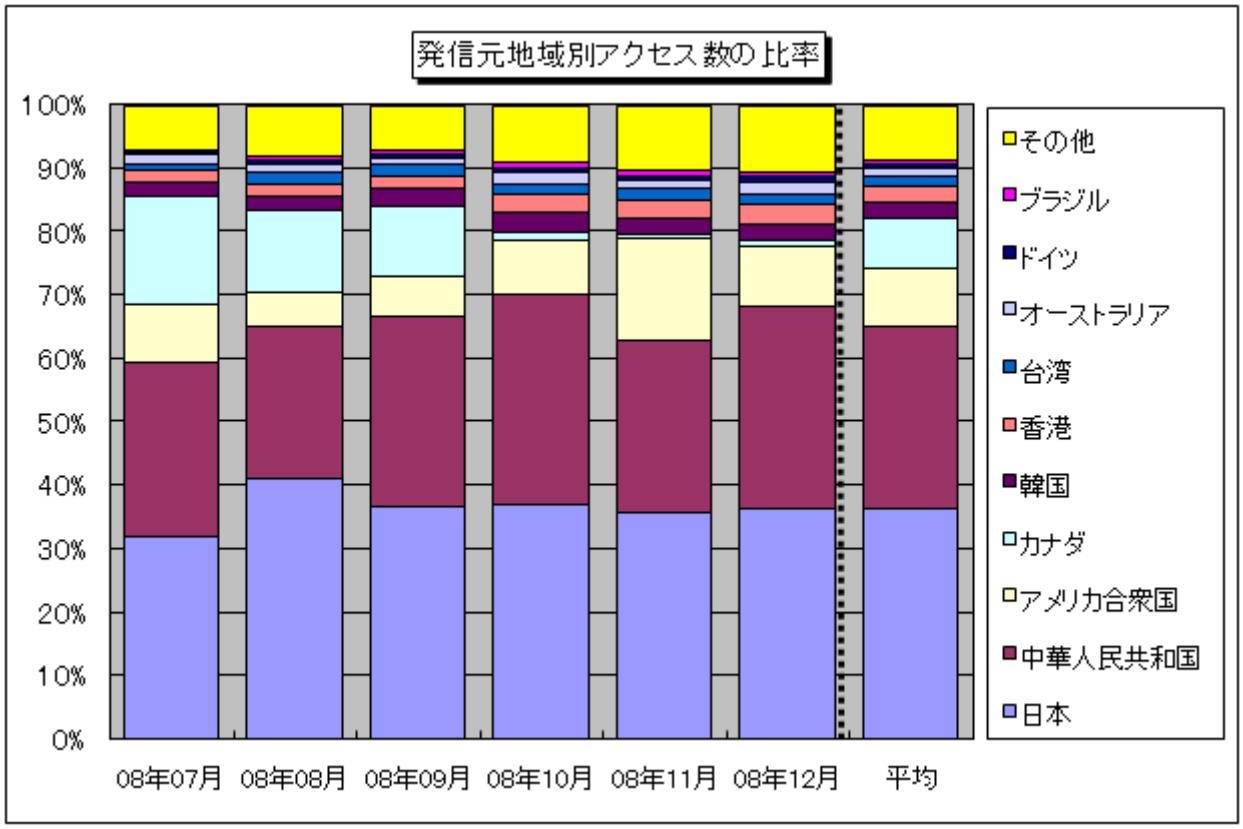
【図 4-1 2008 年 7 月～2008 年 12 月の宛先(ポート種類)別アクセス数の比率】



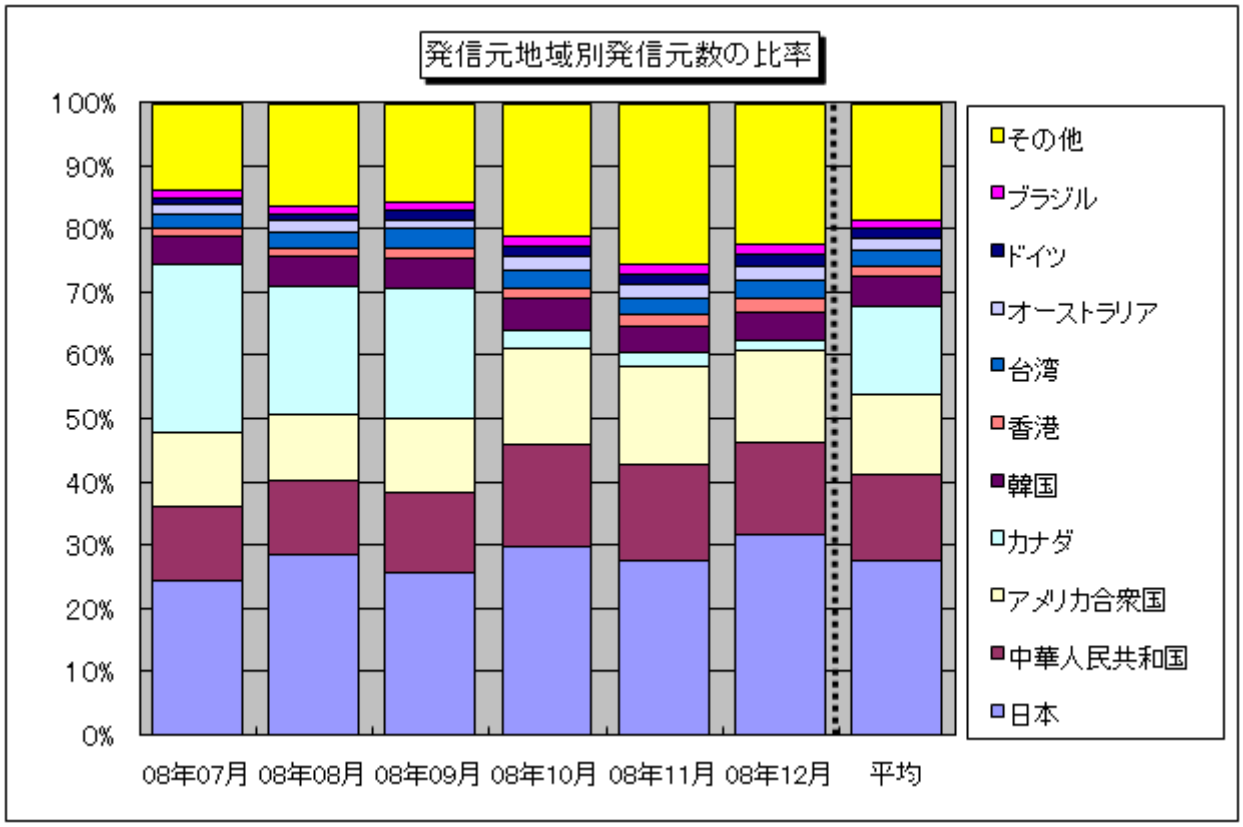
【図 4-2 2008 年 7 月～2008 年 12 月の宛先(ポート種類)別発信元数の比率】

(2)発信元地域別の比率

2008 年 7 月～2008 年 12 月の発信元地域別アクセス数の比率を図 4-3 に、発信元地域別発信元数の比率を図 4-4 に示します。



【図 4-3 2008 年 7 月～2008 年 12 月の発信元地域別アクセス数の比率】



【図 4-4 2008 年 7 月～2008 年 12 月の発信元地域別発信元数の比率】

5．補足説明

以下に、2008 年 12 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
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
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 … ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ)を狙ったアクセスです
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)
139/tcp	保護の甘いファイル(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 Window の脆弱性を狙ったアクセスである可能性が高いです
445/tcp	保護の甘いファイル(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 ,1028/udp	Windows のメッセンジャサービス機能を利用して、悪意あるメッセージを送りつけることに使われる
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
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)
4899/udp	リモート操作を行うための RAdmin のぜい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
大浦／花村／加賀谷
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp