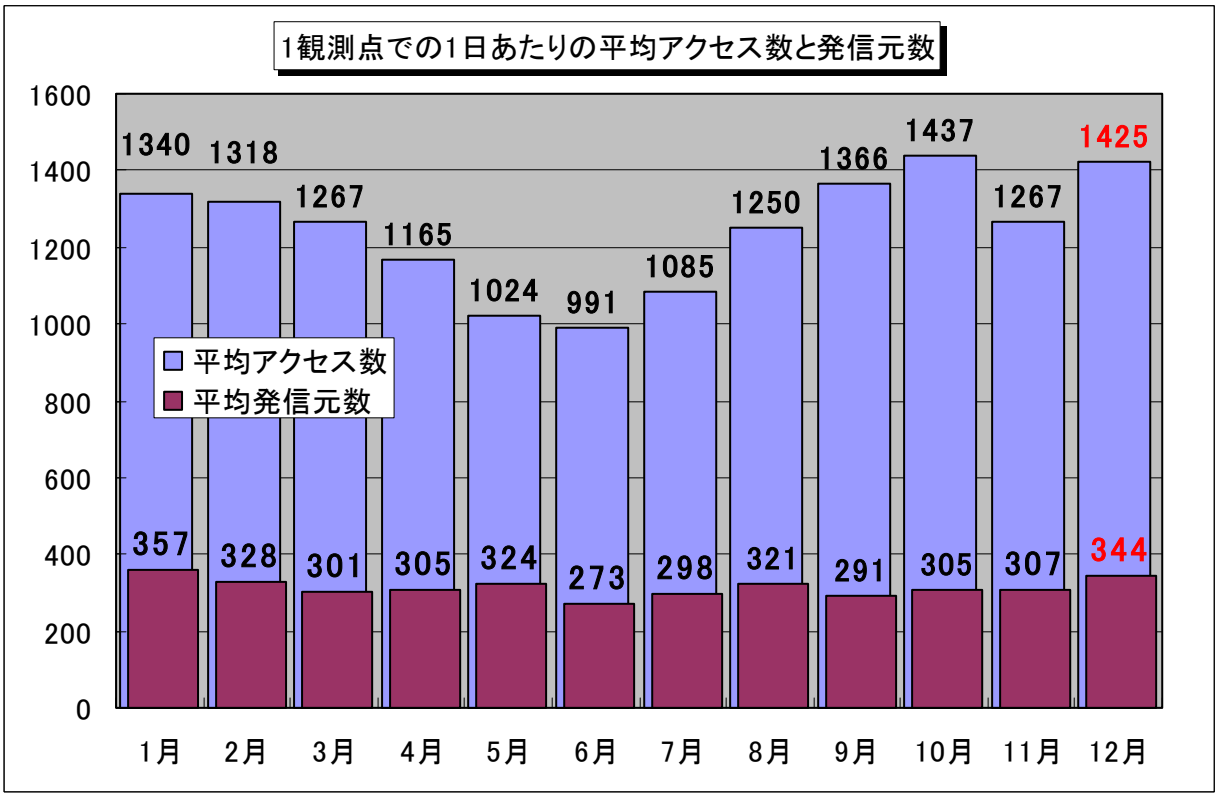
別紙 3

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、2006 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 **441,658 件**ありました。1 観測点で 1 日あたり **344** の発信元から **1,425 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、344 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 1 月～2006 年 12 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、11 月に比べて多少の増加傾向です。この増加傾向は、Ping(ICMP)の増加が原因です(図 1.3)。

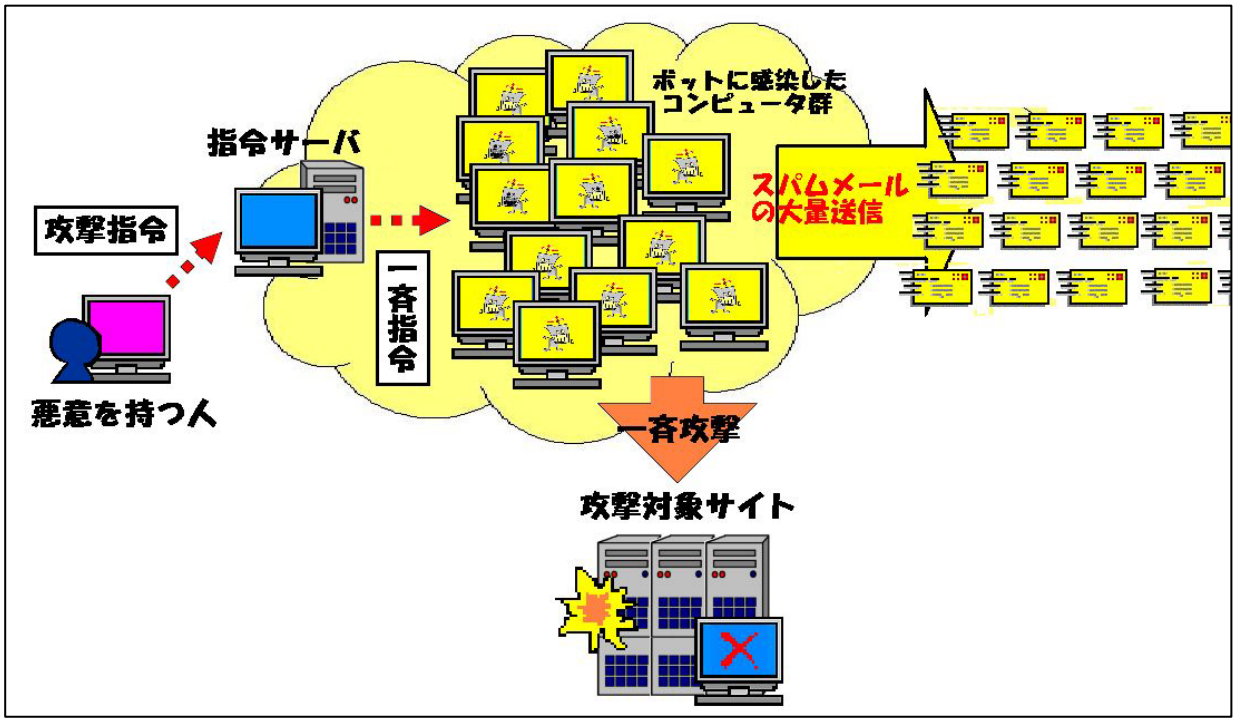
ただし、全体的なアクセス内容については定常化していると言え、主に、ボットに感染したコンピュータからのボット感染活動(コンピュータのぜい弱性を狙い、ボットの感染を広げようとしているアクセス)のためのアクセスであると考えられます。

ボットの機能詳細の解明や国内でのボット感染の実態が明らかになり、複数のボット感染コンピュータが集まったボットネットワークの脅威(図 1.2)が明確になっています。そのため、2006 年 12 月、総務省・経済産業省および関連機関・大手 ISP(インターネットサービスプロバイダー)・大手セキュリティベンダーが連携して、国内でのボット感染を減少させるための、新しいプロジェクトがスタートしました。

■ 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/

■ 総務省・経済産業省連携事業 ボット対策プロジェクトを推進するポータルサイト「サイバークリーンセンター」の開設について
http://www.soumu.go.jp/s-news/2006/061212_1.html

上記の Cyber Clean Center のホームページには、既知のボットを駆除するための手順やボットに感染しないための対策、ボットについての最新情報が記載されています。既知のボットに感染しているかどうかの確認のためにも、手順にしたがってボット駆除を実行することをお勧めします。

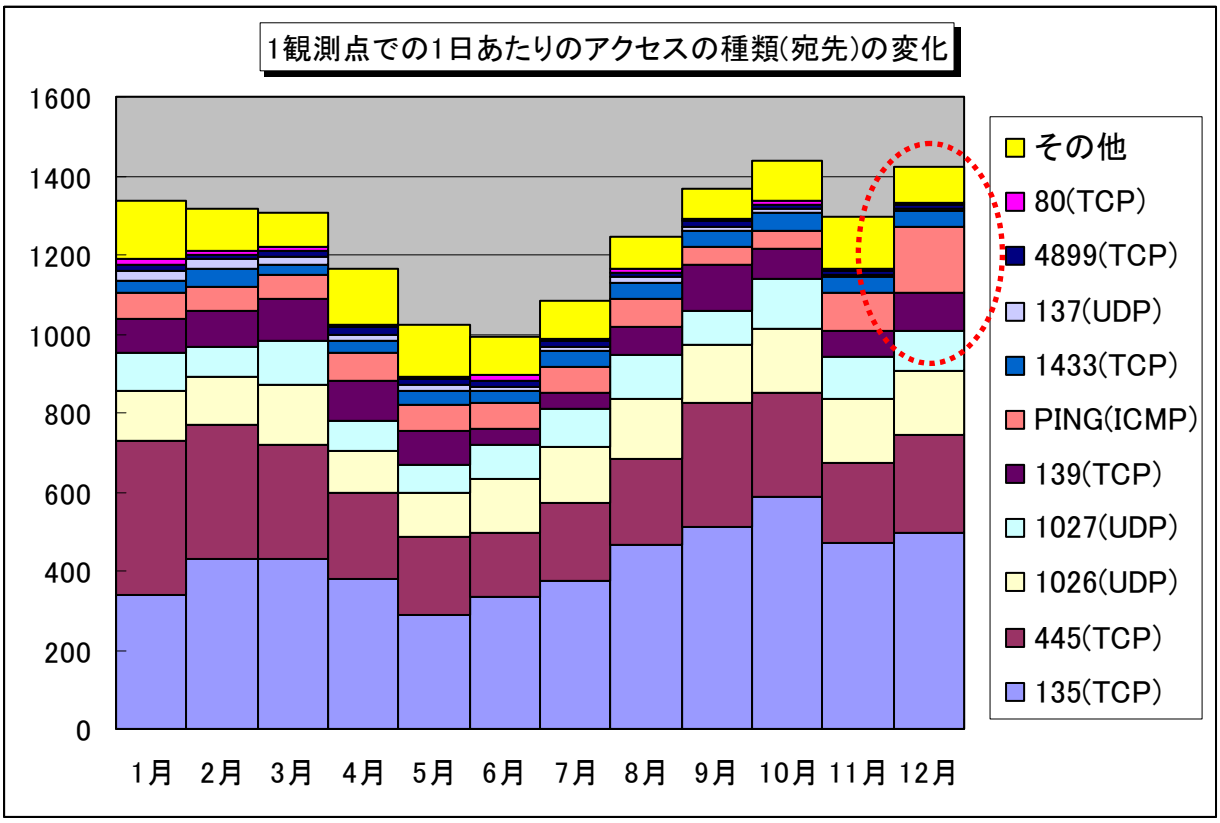


【図 1.2 ボットネットワークの脅威(イメージ)】

■ 図 1.2 の解説

同種類のボットに感染したコンピュータが集まると、ボットネットワークを構成します。このボットネットワークに対して、悪意を持つ人(ハーダーと呼ばれています)が攻撃指令を出すと、ボットネットワークを構成するコンピュータから、大量のスパムメッセージが発信されたり、特定のサイトに対する一斉攻撃(DDoS 攻撃等)が行われたりすることになります。構成されるボット感染コンピュータの数が多ければ多いほど、その脅威は増大します。

これらの脅威を減少させるためには、ボットに感染したコンピュータを減らすしかありません。



【図 1.3　1 観測点での 1 日あたりの期待しない(一方的な)アクセスの種類(宛先)の変化】

増加傾向にある Ping(ICMP)は、2003 年 8 月に発した W32/Welchia(*1)が行ったと同じような、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かも知れません。また、12 月 19 日前後に中国(中華人民共和国)方面から Ping(ICMP)の一時的な急増も見受けられました(図 2.1.1)。

さらに、新たなぜい弱性(*2)を狙った攻撃と思われるアクセスも発生しています。具体的には、2967/tcp ポートへのアクセスです(図 2.1.2)。

(*1) W32/Welchia

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

(*2) 狙われているぜい弱性

■ 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

2. 12 月のアクセス状況

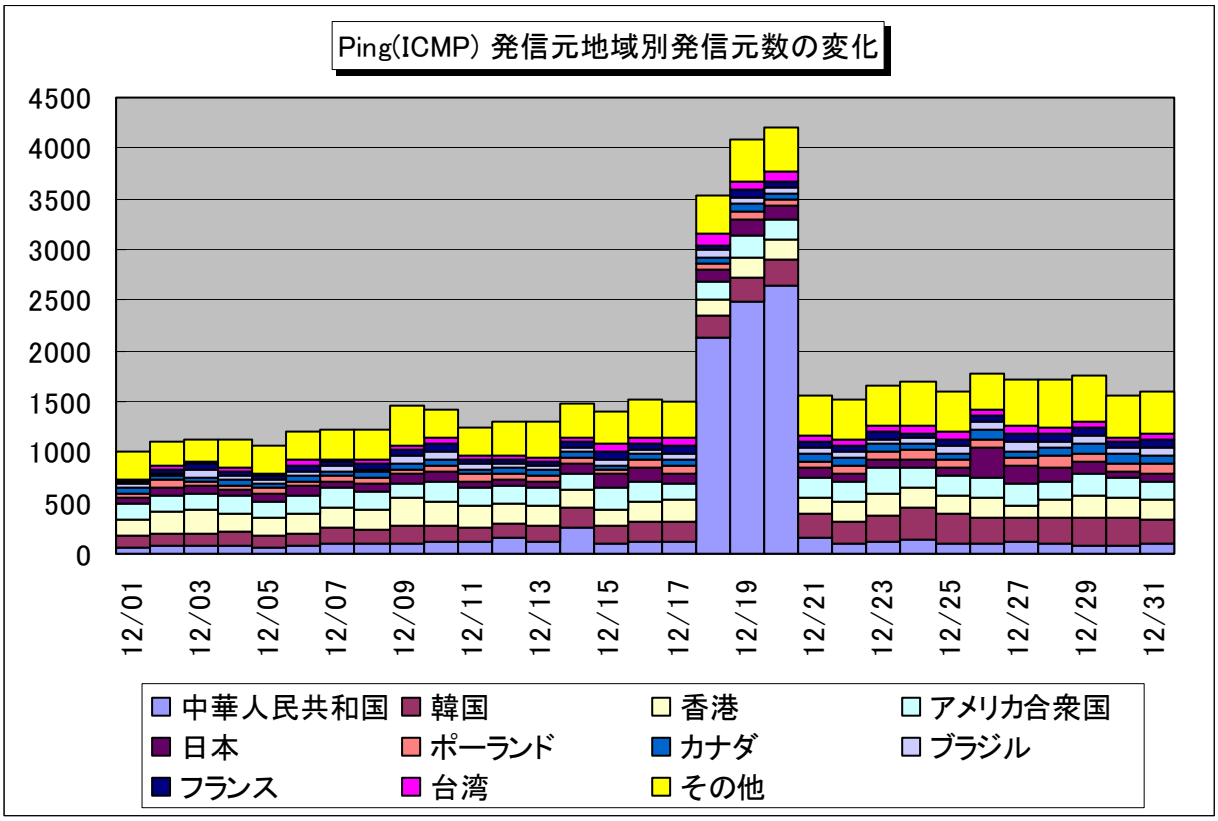
12 月のアクセス状況は、全体的には 11 月とほぼ同じ状況ですが、前述したようにPing(ICMP)アクセスの増加、および新たなぜい弱性を狙ったアクセス(2967/tcp ポートへのアクセス)が見られます。

2.1 12 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)に応答した場合の、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。

今回の中国方面からの一時的なアクセス増加についても、詳細な分析ができない状況です。しかしながら、定点観測の情報交換を行っている他組織からの情報によれば、Ping(ICMP)に応答すると、何らかのぜい弱性を狙ったアクセスが続くと言う事で、2003 年 8 月に発した W32/Welchia が行ったと同じような、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 Ping(ICMP)アクセス】

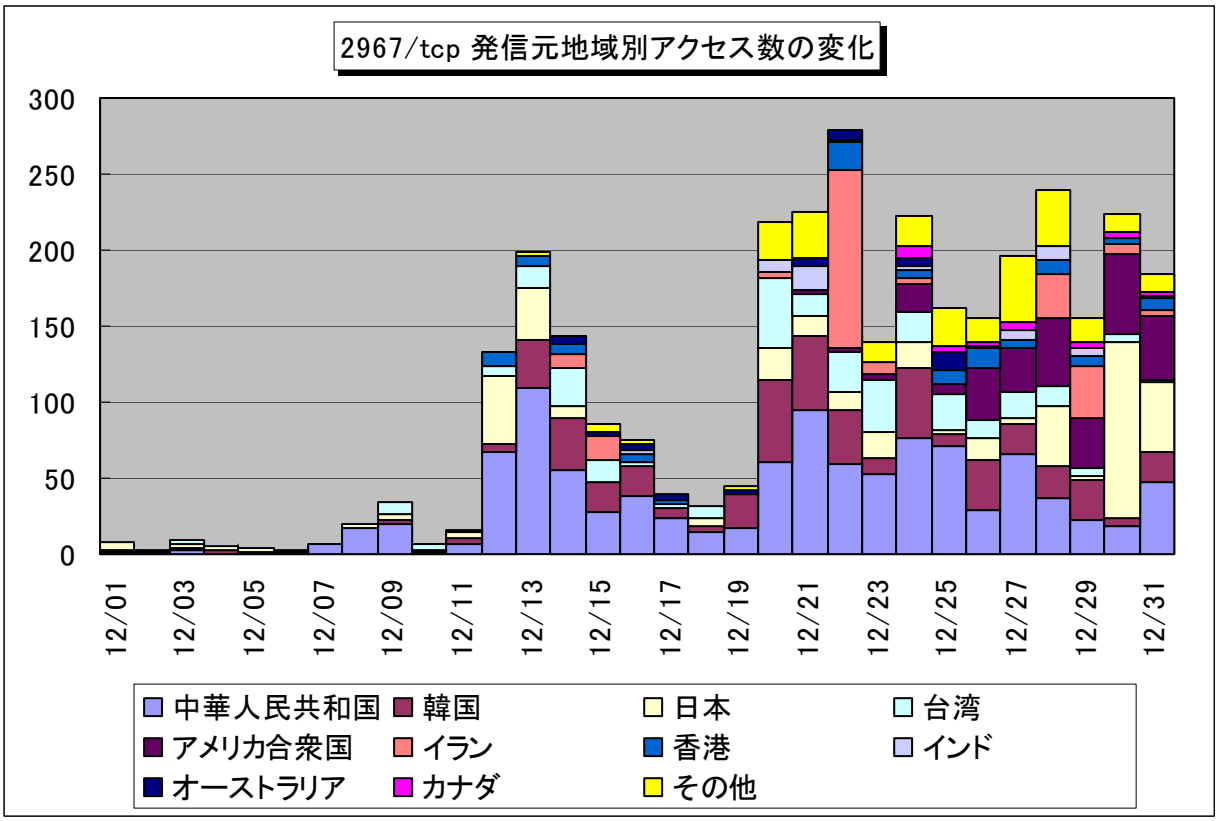
2.1.2 2967/tcp ポートへのアクセス

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。

このぜい弱性を狙った攻撃手法が、ボットに使用されている可能性(*3)があります。Symantec Client Security や Symantec AntiVirus の利用者は、早急に Symantec 社が提供する対応策や緩和策を参考に、ぜい弱性対応を実施して下さい。

TALOT2 の観測によれば、国内企業からのアクセスも発生しています。ご注意下さい。

■ 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



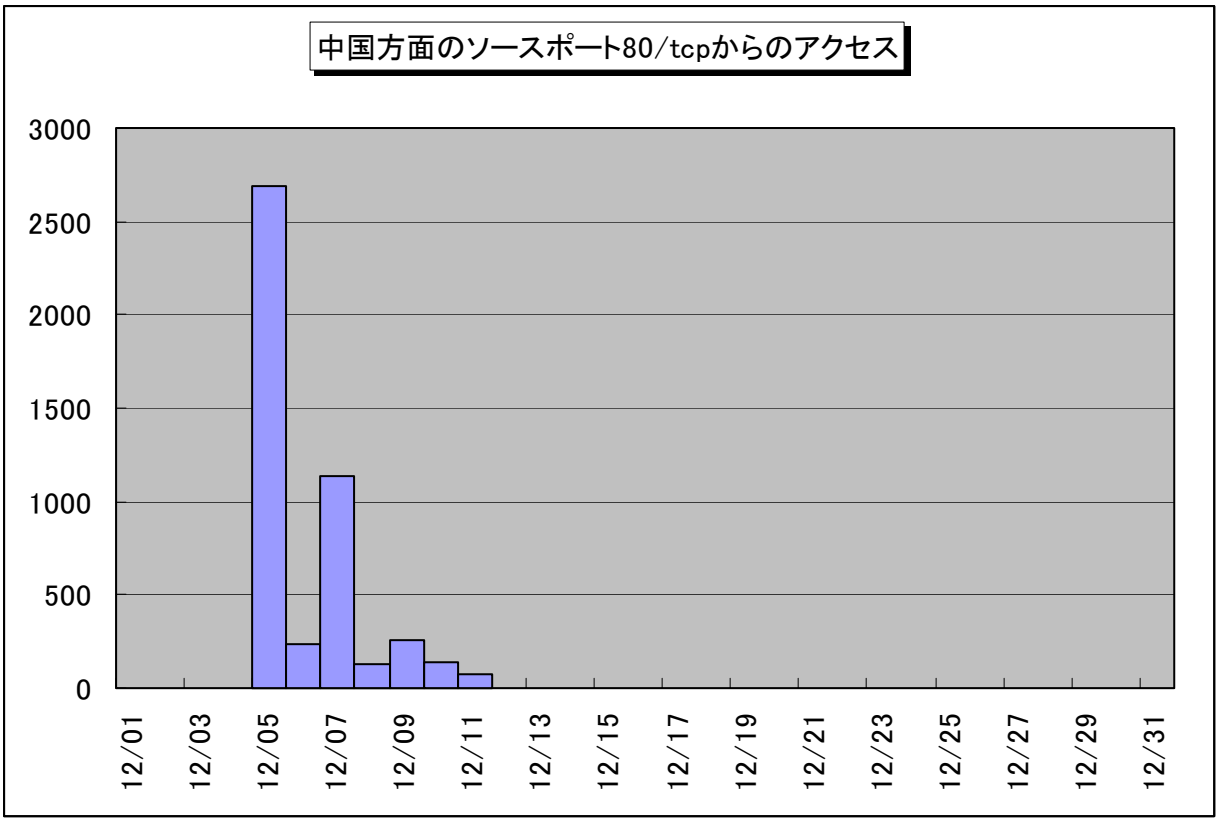
【図 2.1.2 Symantec 社製品のぜい弱性を狙っている思われるアクセス】

(*3) ボットに使用されている可能性

TALOT2 で観測された国内からの 2967/tcp へのアクセスの発信元を調査したところ、同一の発信元から 135/tcp や 139/tcp、さらには 445/tcp と組み合わされたアクセスがあることが判明しています。これらのアクセスの多くはボットに感染したコンピュータがボットの感染活動を行っているアクセスと考えられるため、2967/tcp に関してもボットから発信されている可能性があると推定されます。

2.1.3 その他

観測状況を示す各種統計を取るための観測データからは除外していますが、12 月 5 日から 13 日にかけて中国(中華人民共和国)方面の一部の通信事業者サイトや検索サイトを狙った DoS 攻撃(SYN Flood 攻撃)(*4)の影響と思われるアクセス(ソースポート 80/tcp からの ACK+SYN アクセス)が観測されています(図 2.1.3)。



【図 2.1.3 中国方面への SYN Flood 攻撃のなごりアクセス(バックスキャッタ)】

(*4) DoS攻撃(SYN Flood 攻撃)

「サービス妨害攻撃」Denial of Service の略からDoS攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。このDoS攻撃の1つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット(3 ウェイ・ハンドシェーク(*5)での接続確立の最初に送られるパケット)を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*5) 3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下に A と B の通信確立の手順を示します

①A から B へ SYN パケットの送信

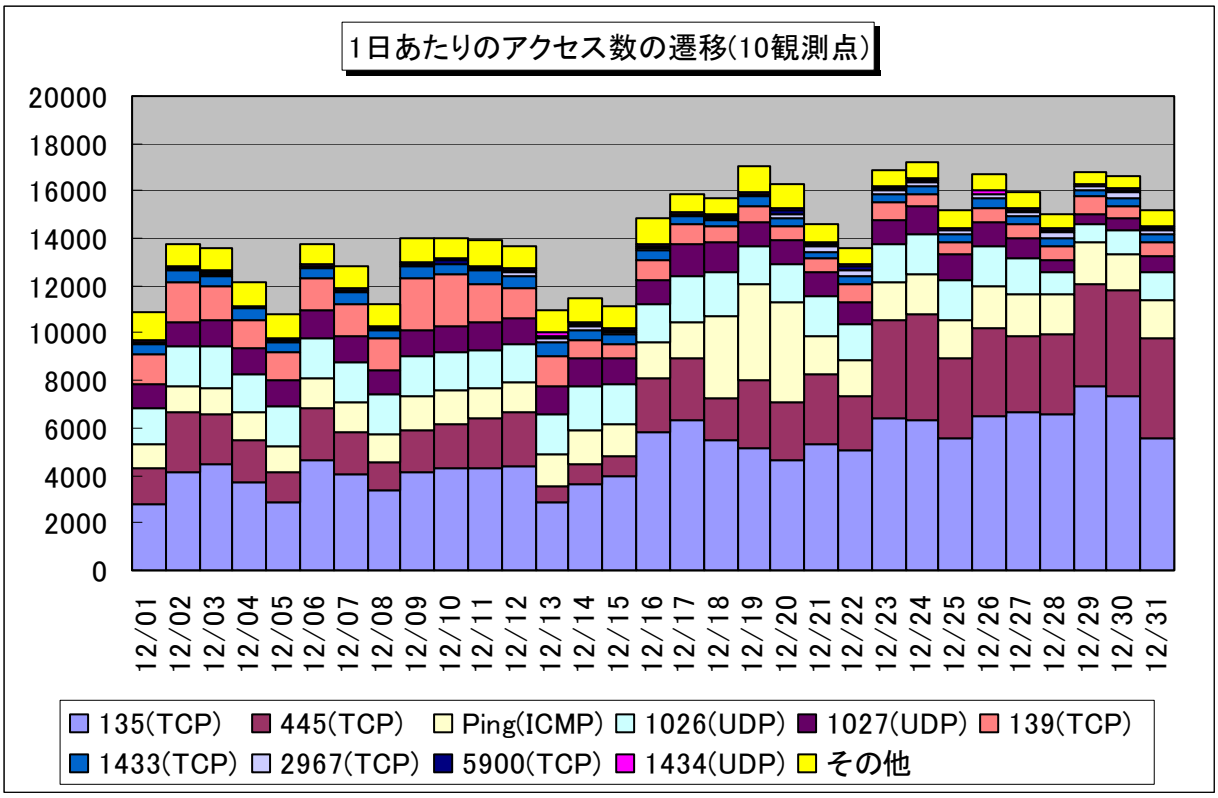
②B から A へ ACK+SYN パケットの送信

③A から B へ ACK パケットの送信

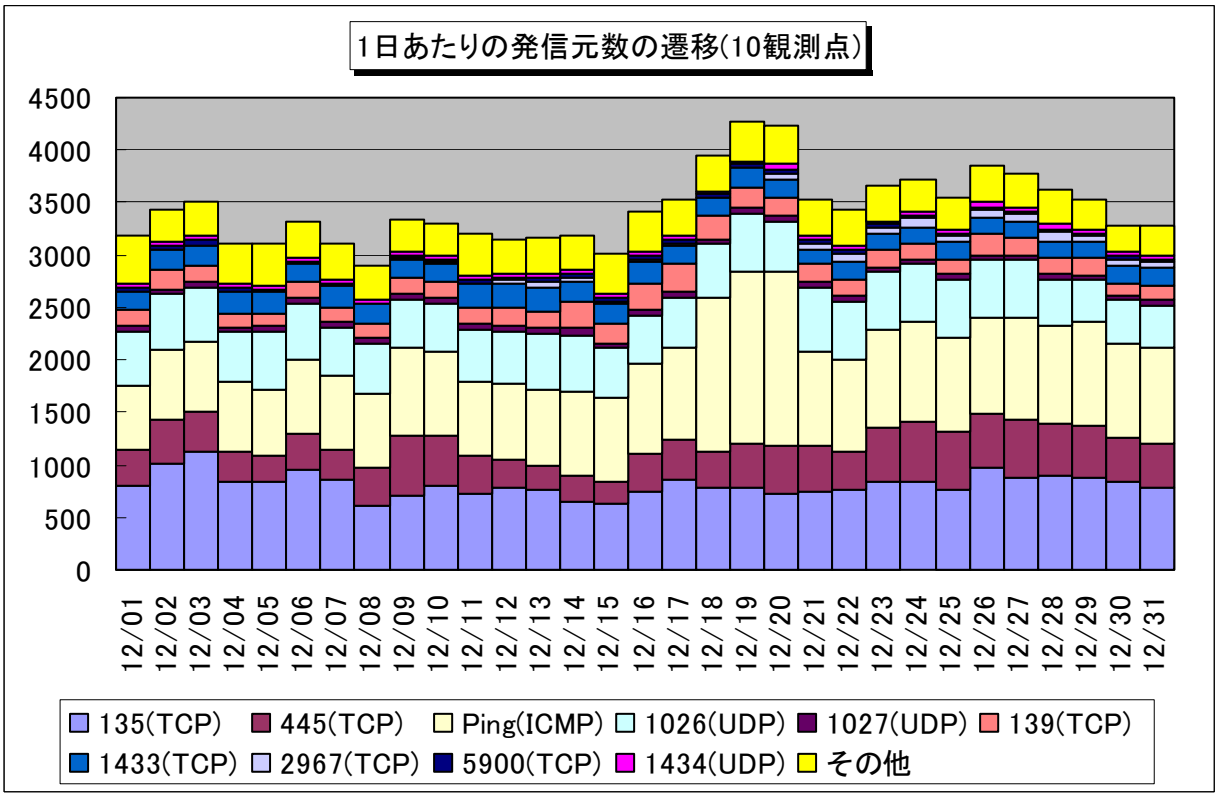
これで、AB 双方の通信が確立されます。

2.2 2006 年 12 月の一方的なアクセス状況

2006 年 12 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。



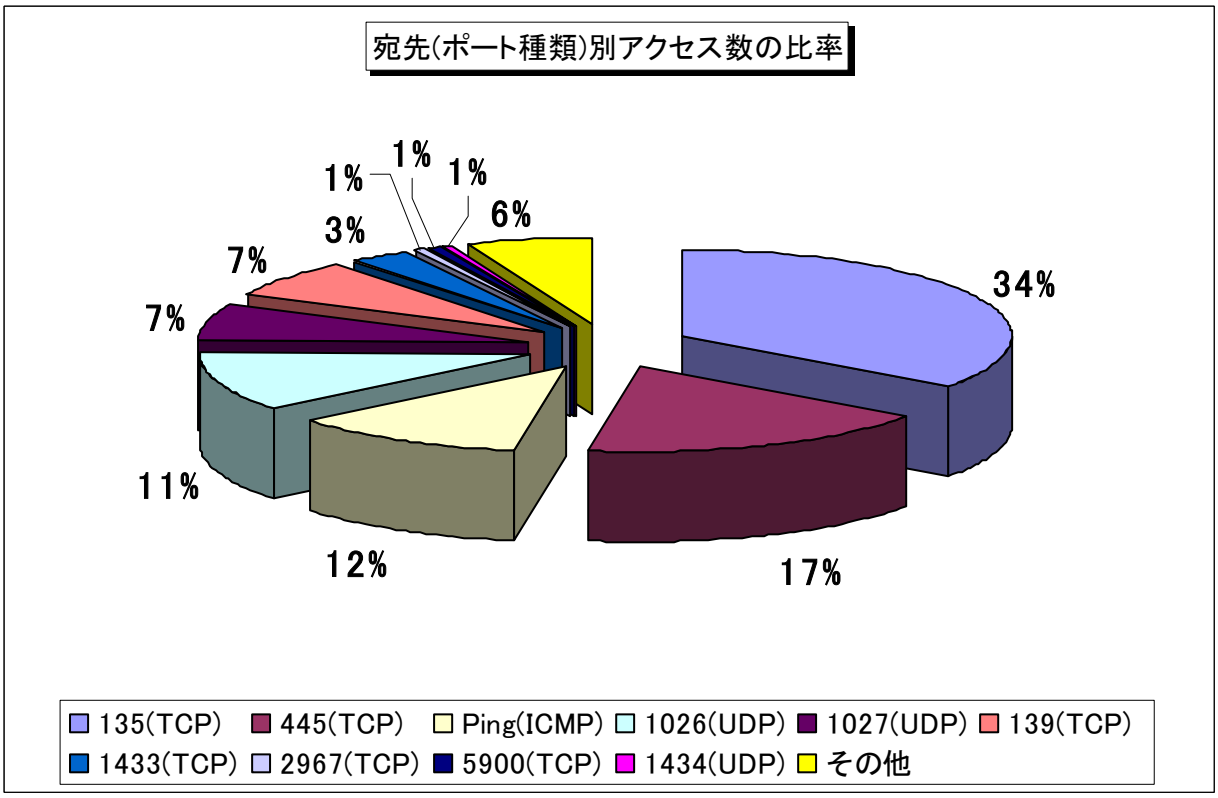
【図 2.2.1 2006 年 12 月の一方的なアクセス状況(アクセス数)】



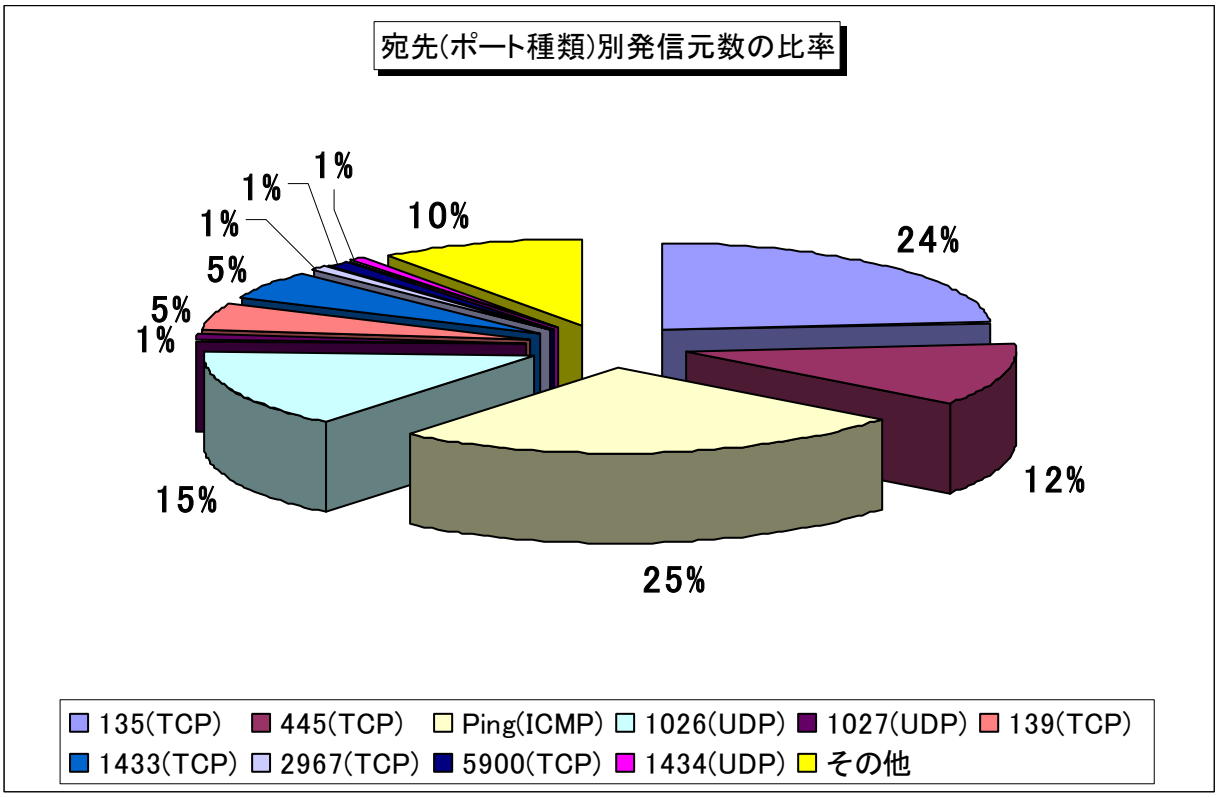
【図 2.2.2 2006 年 12 月の一方的なアクセス状況(発信元数)】

2.3 2006 年 12 月の宛先(ポート種類)別の比率

2006 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 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。



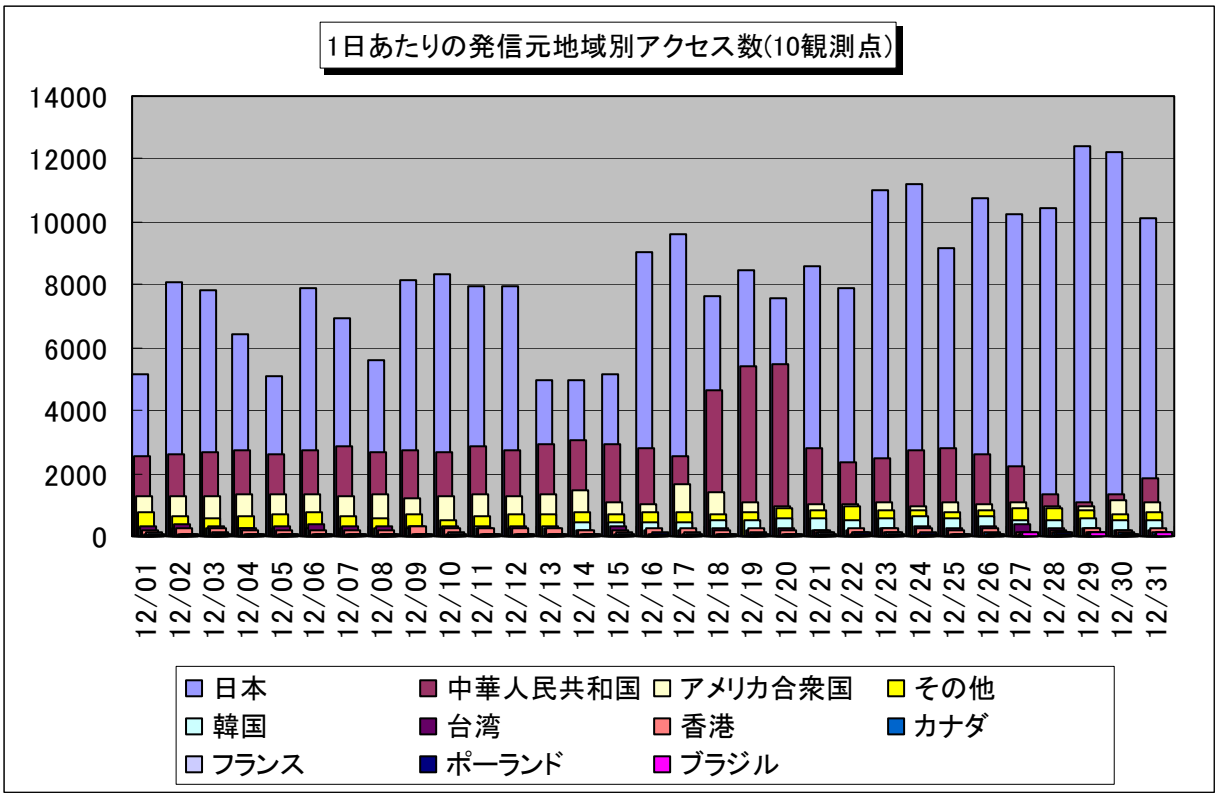
【図 2.3.1 2006 年 12 月の宛先(ポート種類)別アクセス数の比率】



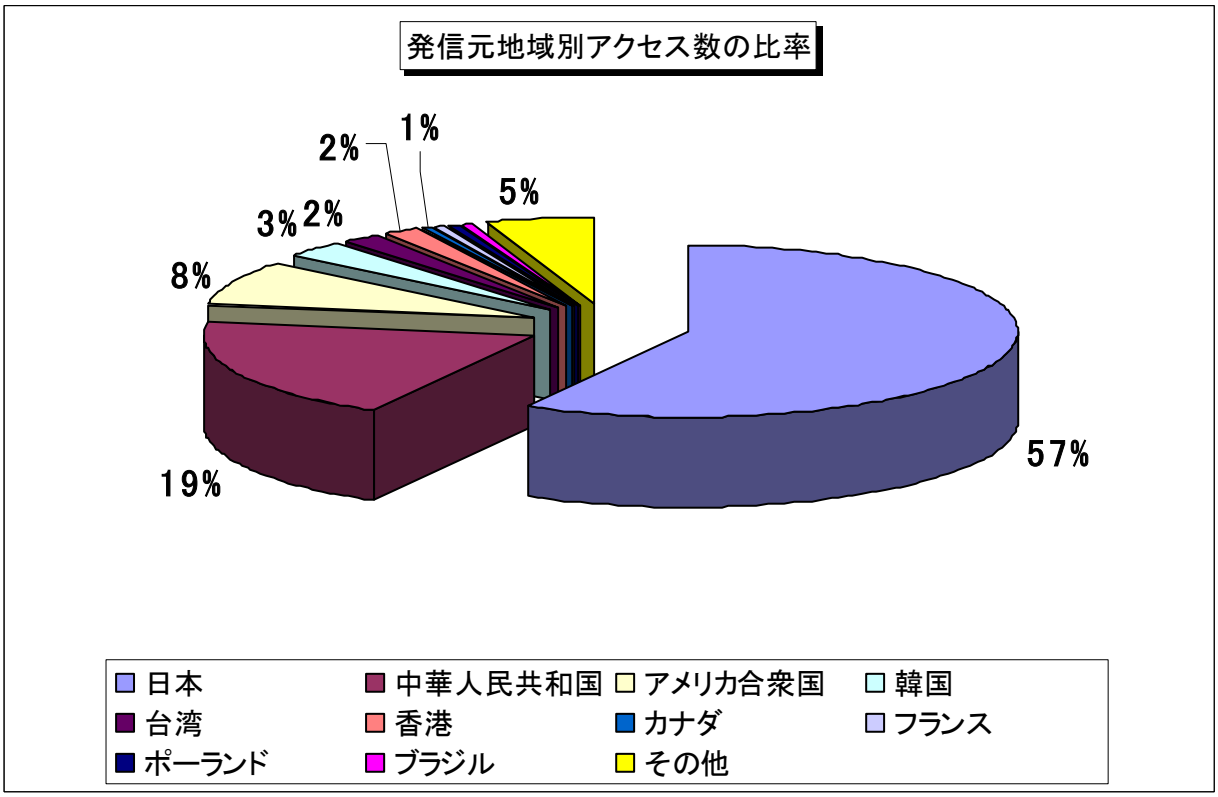
【図 2.3.2 2006 年 12 月の宛先(ポート種類)別発信元数の比率】

2.4 2006 年 12 月の発信元地域別アクセス状況

2006 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。

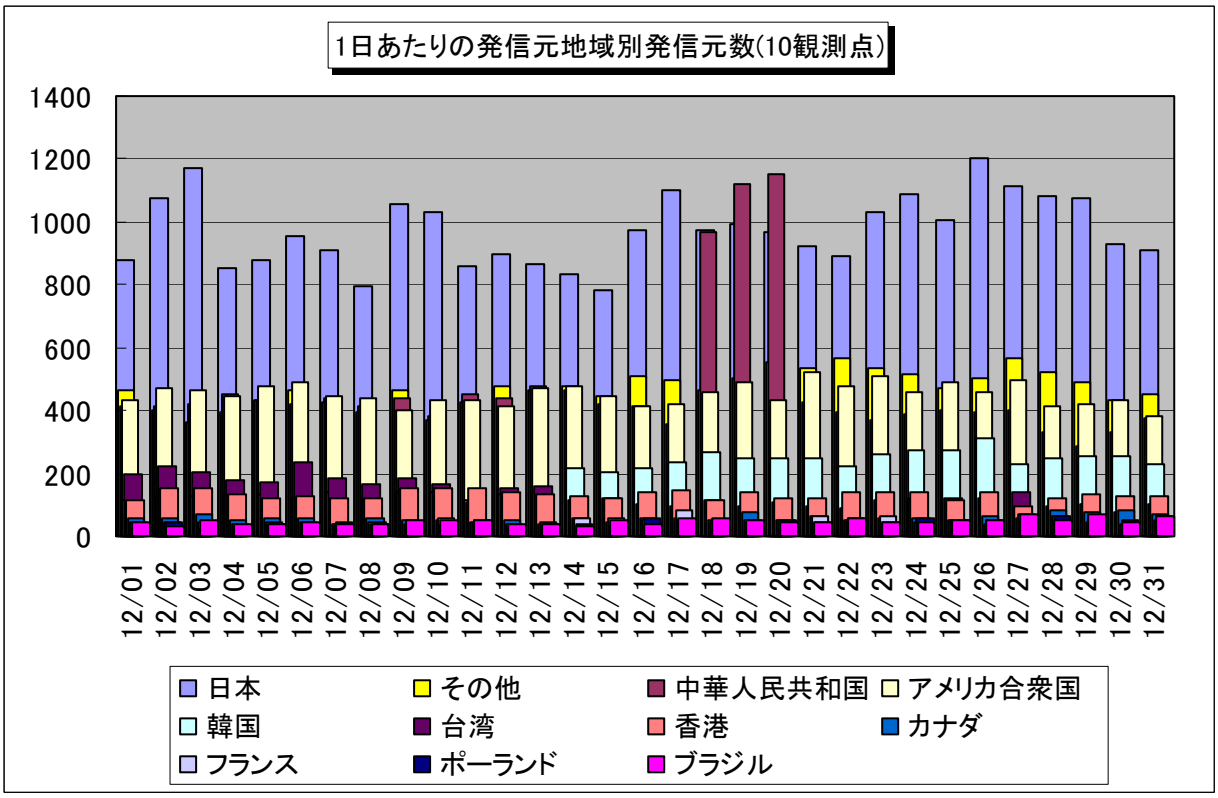


【図 2.4.1 2006 年 12 月の発信元地域別アクセス数の変化】

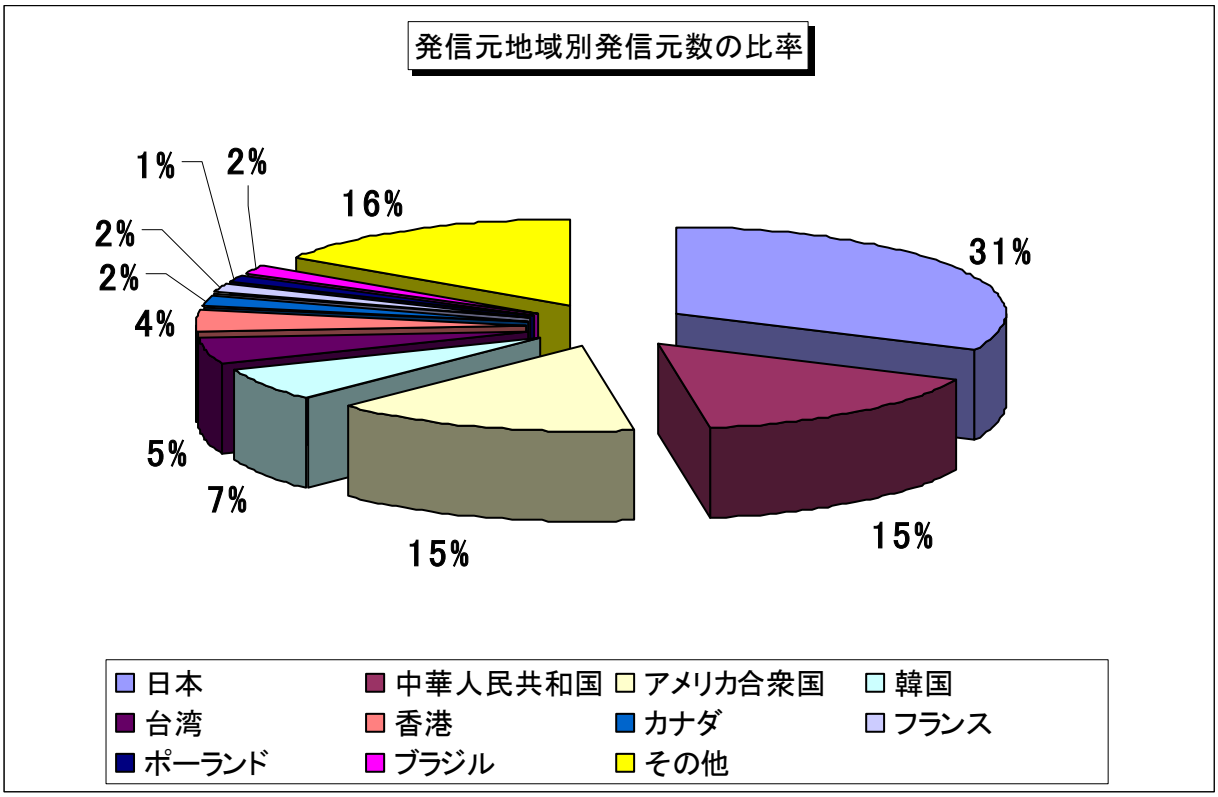


【図 2.4.2 2006 年 12 月の発信元地域別アクセス数の比率】

2006 年 12 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 2006 年 12 月の発信元地域別発信元数の変化】

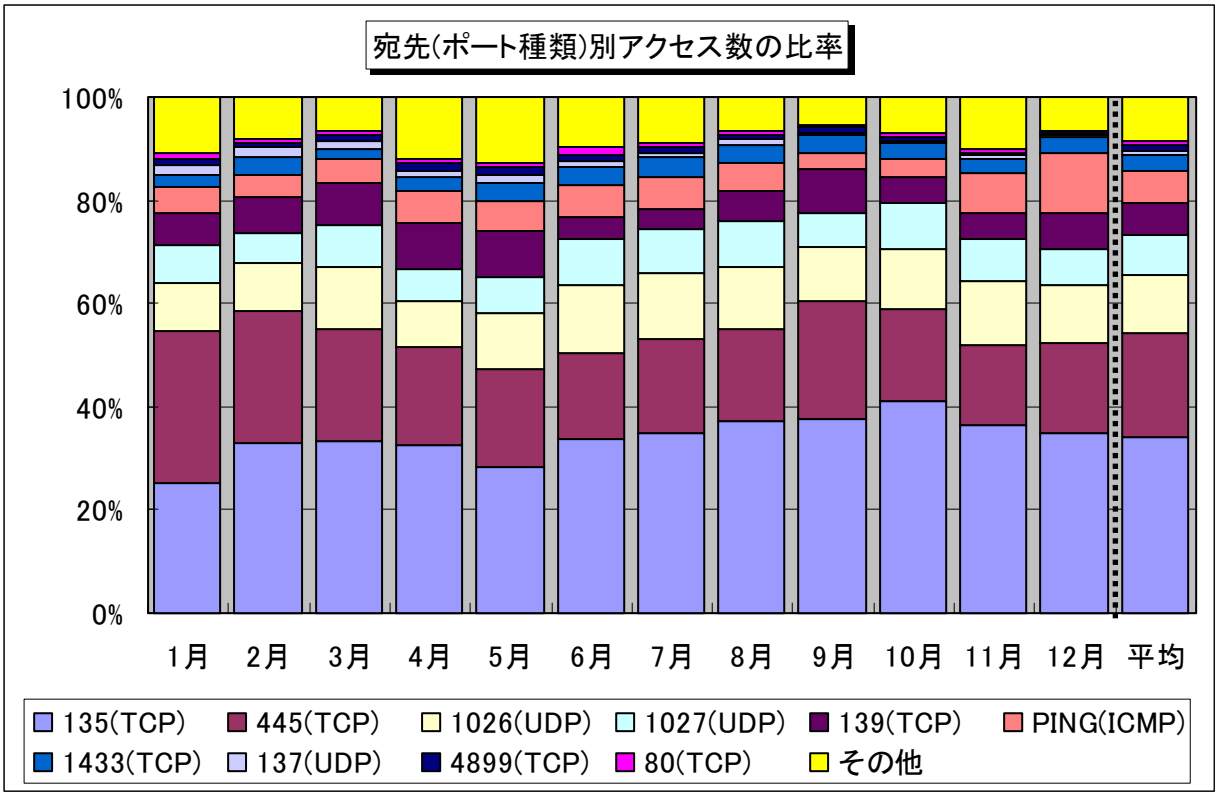


【図 2.4.4 2006 年 12 月の発信元地域別発信元数の比率】

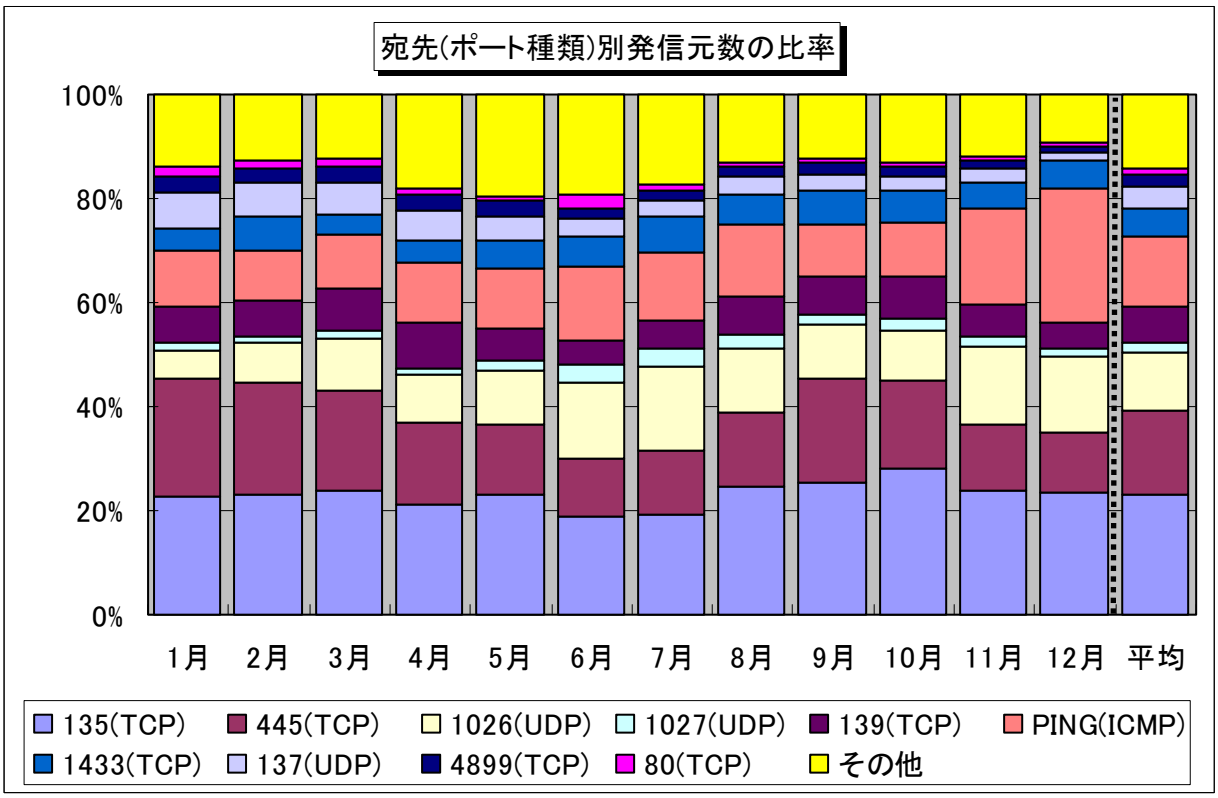
3. 統計情報

3.1 2006 年 1 月～2006 年 12 月の宛先(ポート種類)別の比率

2006 年 1 月～2006 年 12 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。



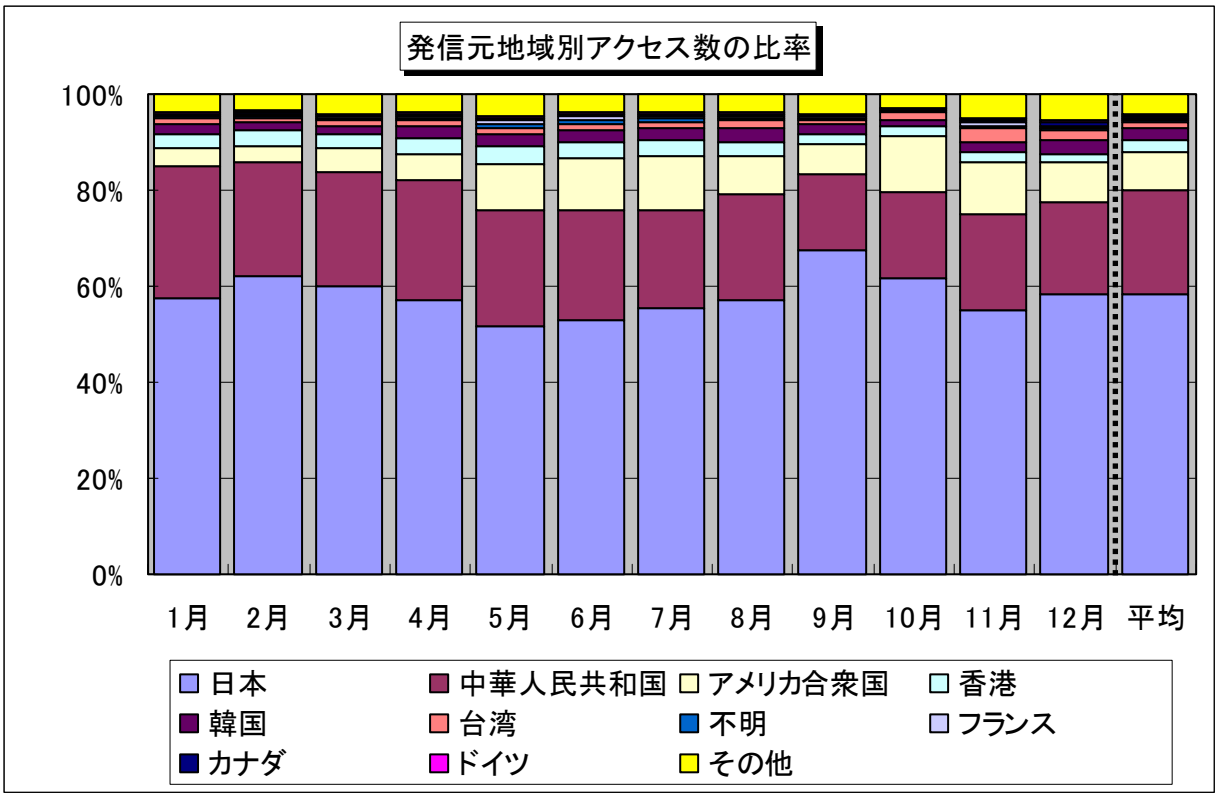
【図 3.1.1 2006 年 1 月～2006 年 12 月の宛先(ポート種類)別アクセス数の比率】



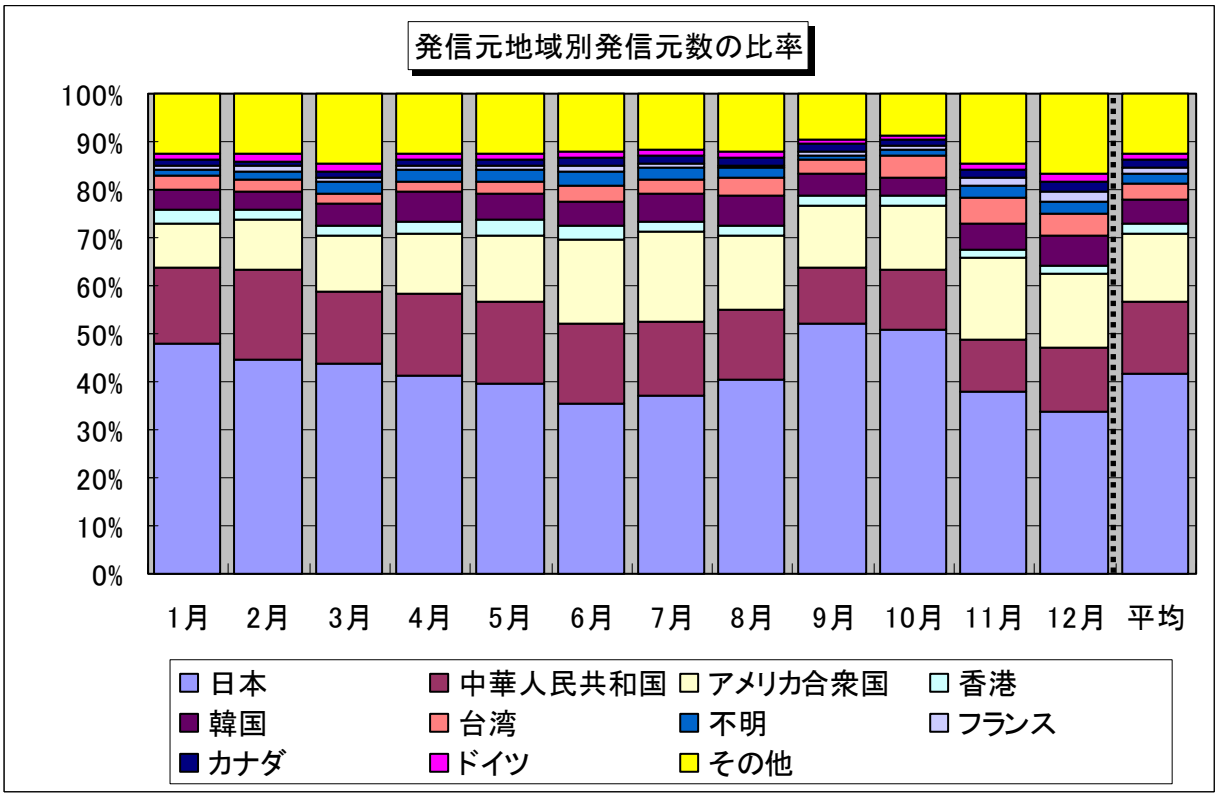
【図 3.1.2 2006 年 1 月～2006 年 12 月の宛先(ポート種類)別発信元数の比率】

3.2 2006 年 1 月～2006 年 12 月の発信元地域別の比率

2006 年 1 月～2006 年 12 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 1 月～2006 年 12 月の発信元地域別アクセス数の比率】



【図 3.2.2 2006 年 1 月～2006 年 12 月の発信元地域別発信元数の比率】

4. 補足説明

以下に、2006 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
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