

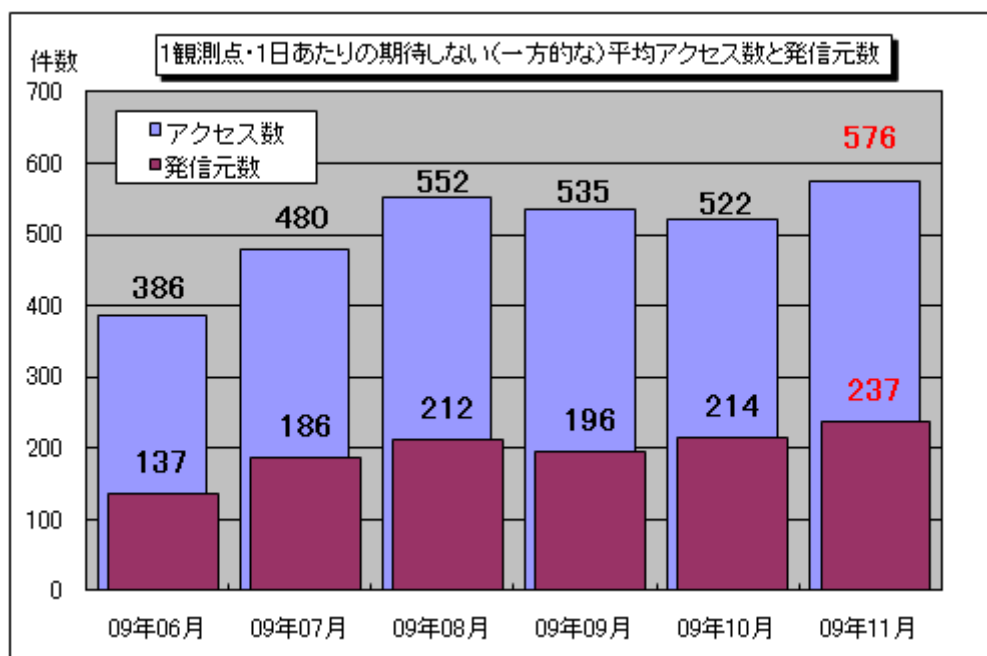
インターネット定点観測（TALOT2）での観測状況について

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、2009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172,802件、延べ発信元数^(※)は71,136箇所ありました。平均すると、1観測点につき1日あたり237の発信元から576件のアクセスがあったこととなります（図1-1参照）。

延べ発信元数^(※)：TALOT2の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、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は、発信元数を1としてカウントする。

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向的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】

2009年6月～2009年11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。11月の期待しない（一方的な）アクセスは、10月と比べて増加しました。

10月と11月の宛先（ポート種類）別アクセス数の比較を図1-2に示します。

11月は10月に全く観測されなかった60304/udpへのアクセスが多く観測されたことと、2967/tcpや139/tcp、1521/tcpなど複数のポートへのアクセスが10月より増加したことで全体数の増加につながっていました。

60304/udpへのアクセスは、11月の下旬に数日間だけ一つの観測点で観測されていたものであり、発信元はオーストラリアの1ヶ所のみでした。このアクセスが何を目的に送られていたかは不明です。

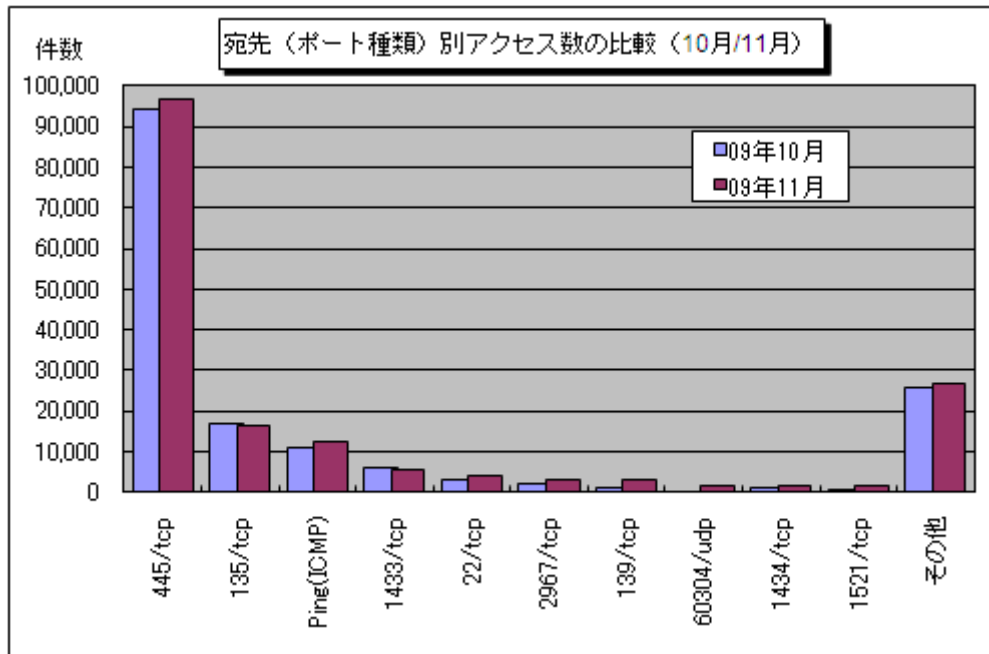
また、10月と比較して増加の度合いが最も大きかったのは1521/tcpへのアクセスです。1521/tcpはOracleデータベースがデフォルトで使用するポートです。TALOT2では2009年7月上旬あたりからこのポートへのアクセスの増加を観測しており、10月下旬頃からも若干増加していました（図1-3参照）。

このような傾向は定点観測を行っている他の組織でも観測されています。アクセスが増加し始めた

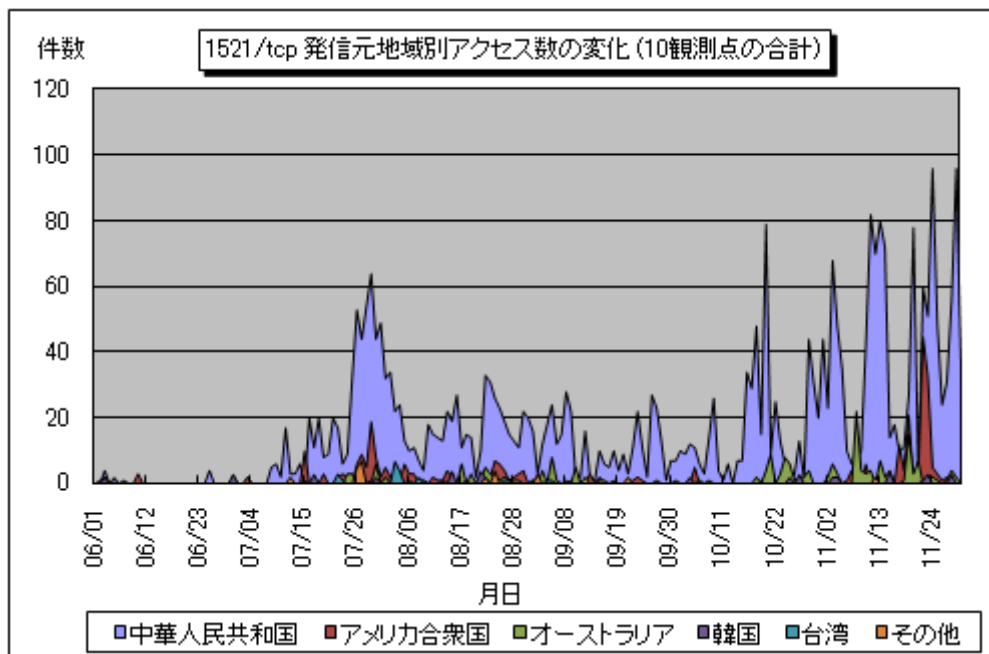
7月上旬に、1521/tcp に対してスキャンを行うためのツールの配布サイトが中国で発見されたという情報も確認していることから、このツールが使われて脆弱な Oracle データベースを探索しようとするアクセスが継続的に発生していた可能性があります。

このような行為への考えられる対策としては、以下の手段が挙げられます。

- ・ファイアウォールによる、外部からのアクセスの制限や接続可能な IP アドレスの制限
- ・Oracle データベースで使用するポートをデフォルトの 1521 番から別の番号に変更する
- ・Oracle データベースのユーザーのパスワードを推測されにくいものに設定し直す
- ・OS やその他のアプリケーションソフトなどの脆弱性の解消



【図 1-2：宛先 (ポート種類) 別アクセス数の比較 (10月/11月)】

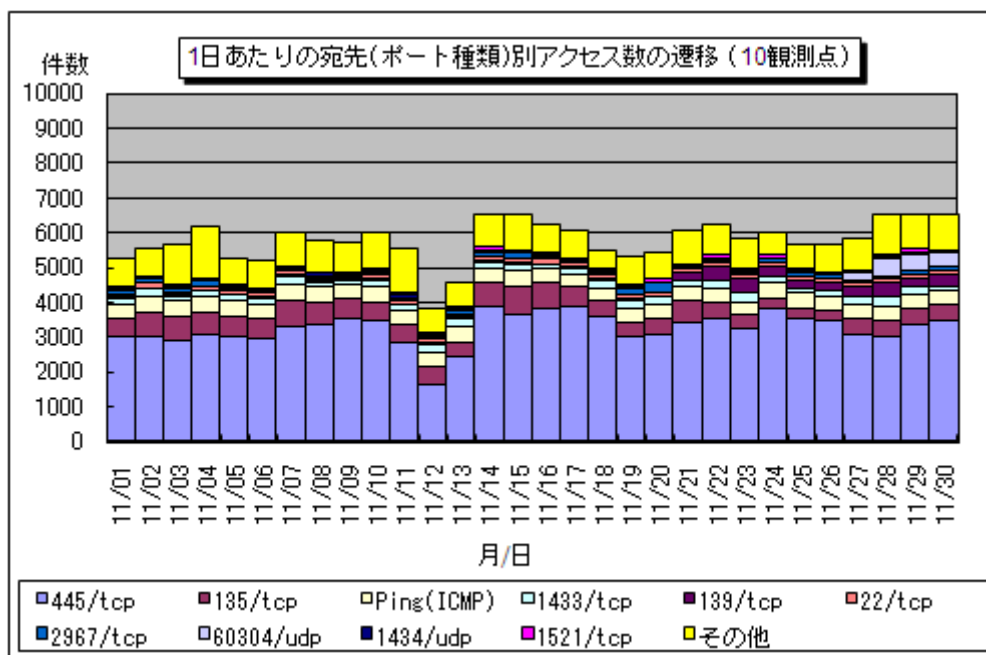


【図 1-3：1521/tcp 発信元地域別アクセス数の変化 (10 観測点の合計)】

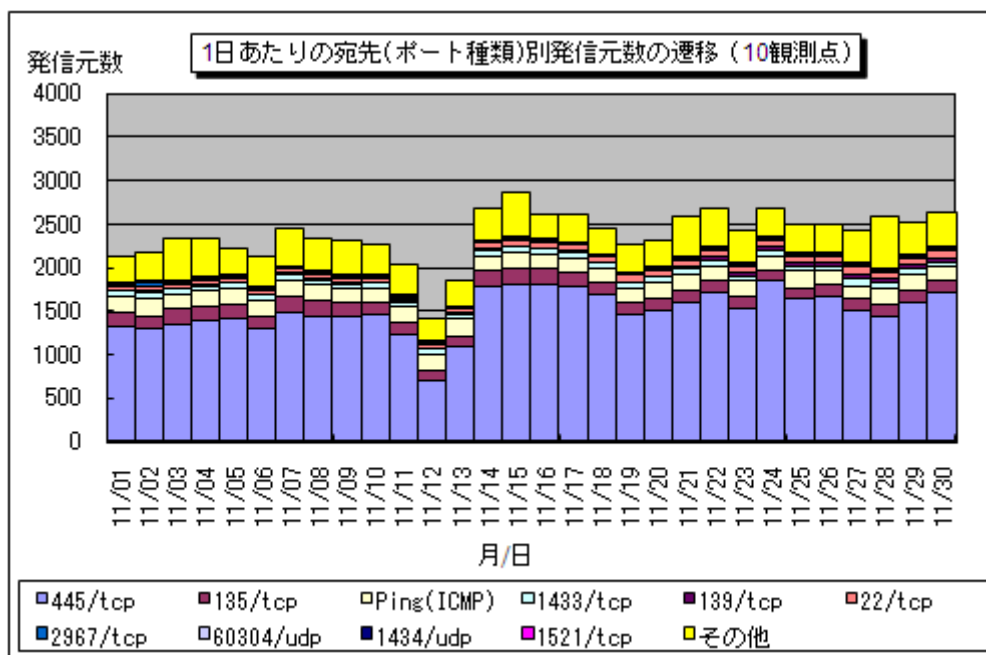
2. 2009年11月の一方的なアクセス状況

(1) 宛先（ポート種類）別のアクセス状況

2009年11月の一方的なアクセス状況（アクセス数）の遷移を図2-1に、一方的なアクセス状況（発信元数）の遷移を図2-2に示します。



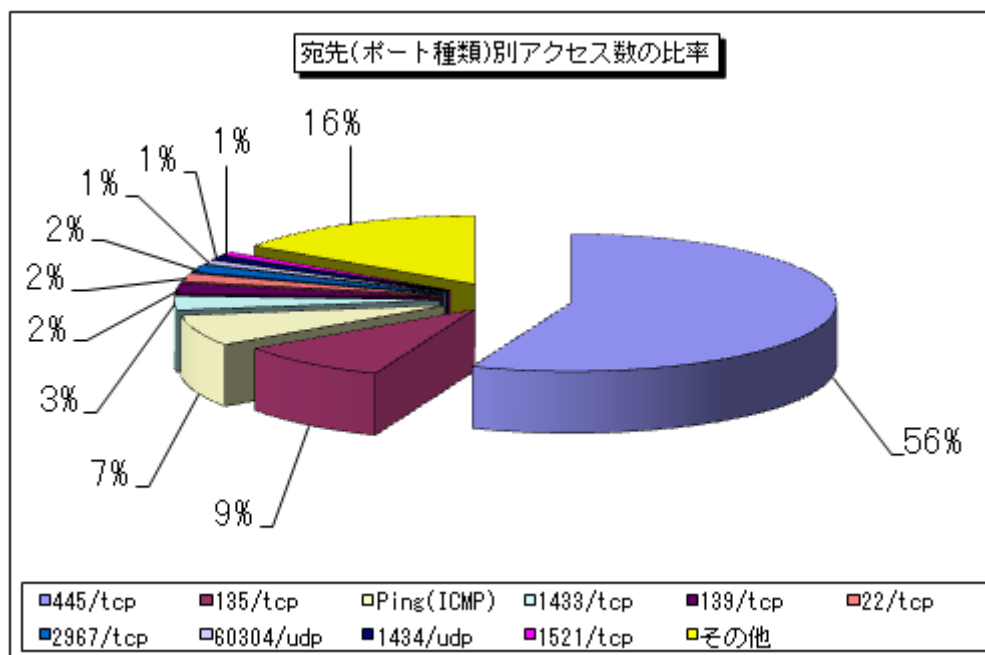
【図2-1：2009年11月の1日あたりの宛先（ポート種類）別アクセス数の遷移】



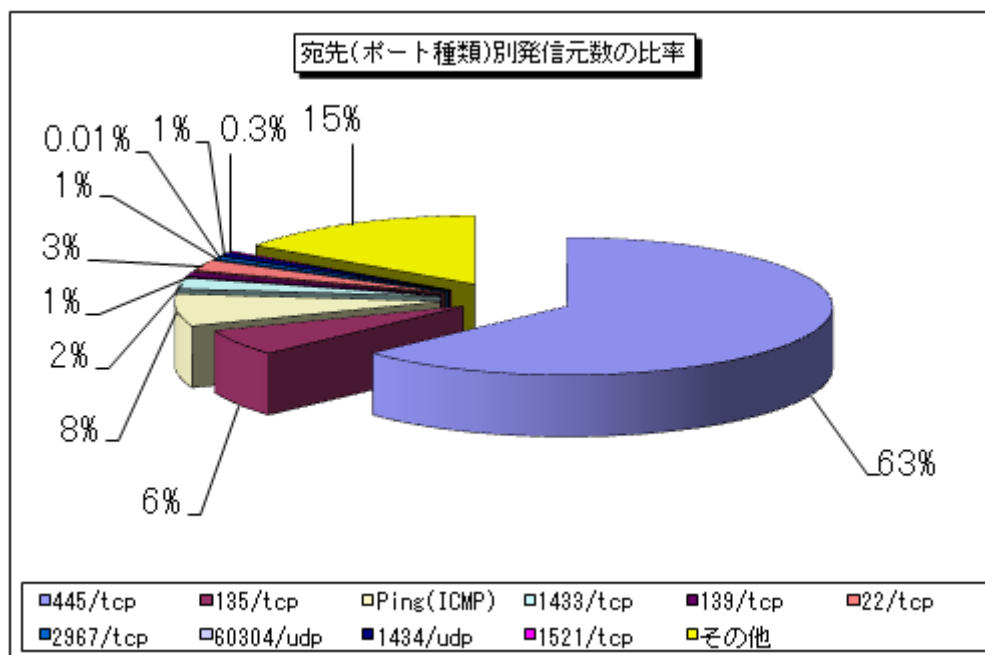
【図2-2：2009年11月の1日あたりの宛先（ポート種類）別発信元数の遷移】

(2) 宛先（ポート種類）別の比率

2009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に、宛先（ポート種類）別発信元数の比率を図2-4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。



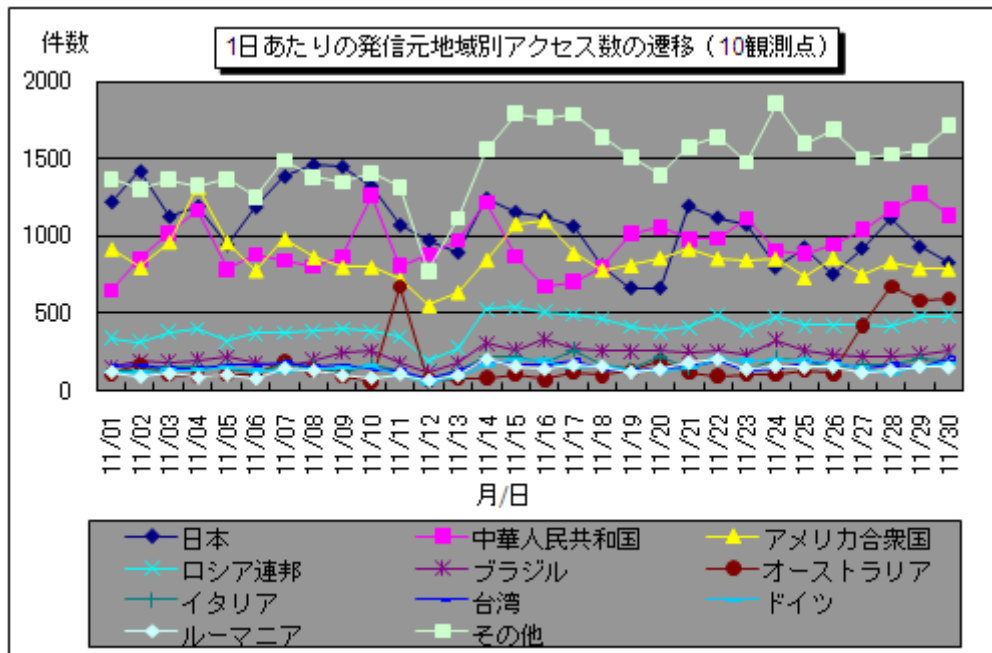
【図 2-3 : 2009 年 11 月の宛先（ポート種類）別アクセス数の比率】



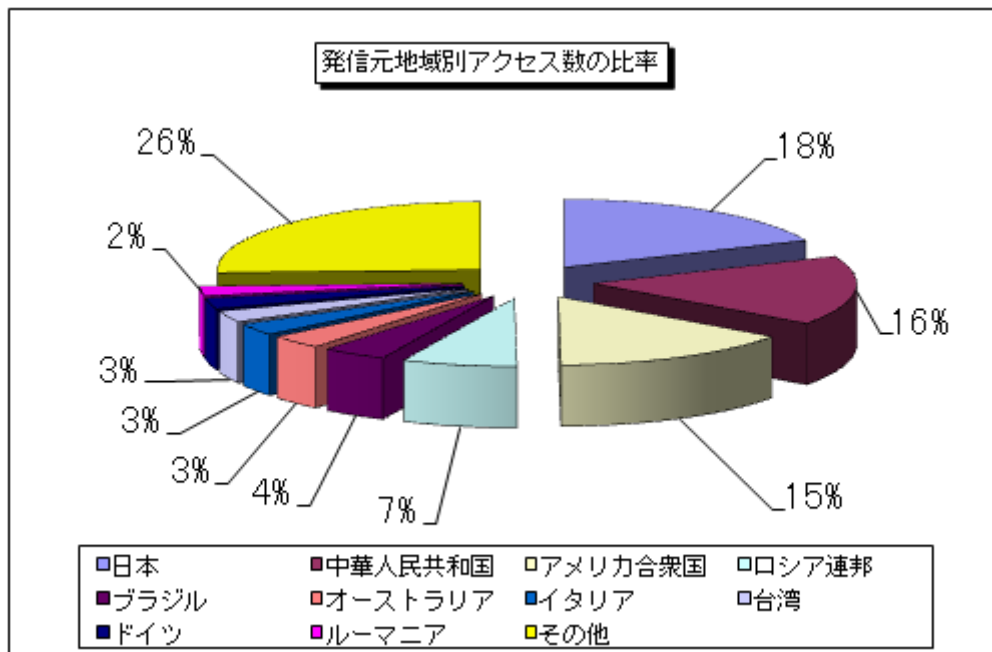
【図 2-4 : 2009 年 11 月の宛先（ポート種類）別発信元数の比率】

(3) 発信元地域別のアクセス状況

2009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2-5に、発信元地域別アクセス数の比率を図2-6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。

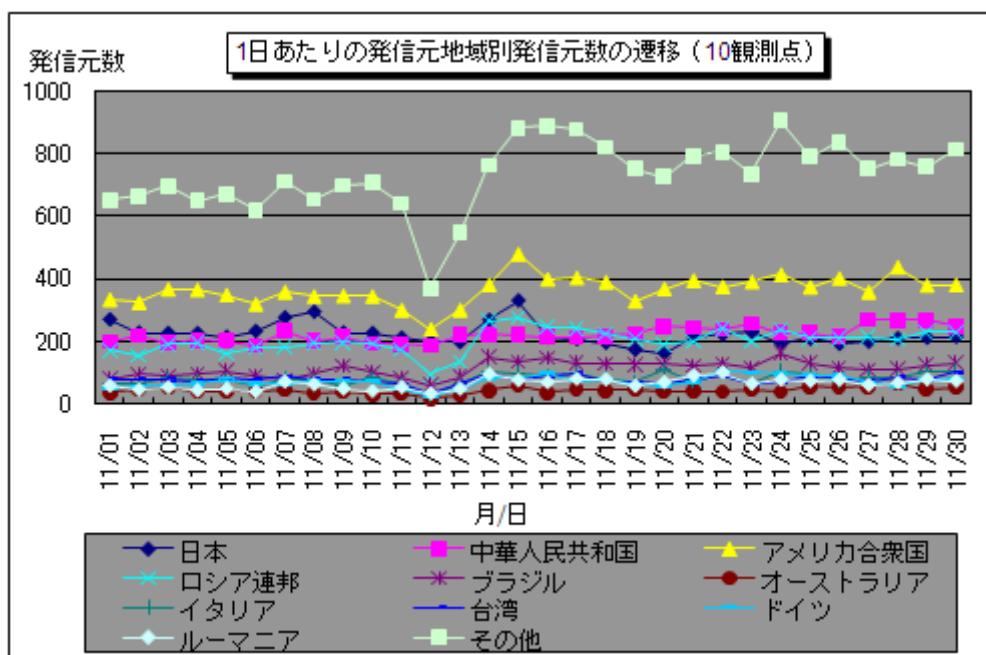


【図 2-5 : 2009 年 11 月の 1 日あたりの発信元地域別アクセス数の遷移】

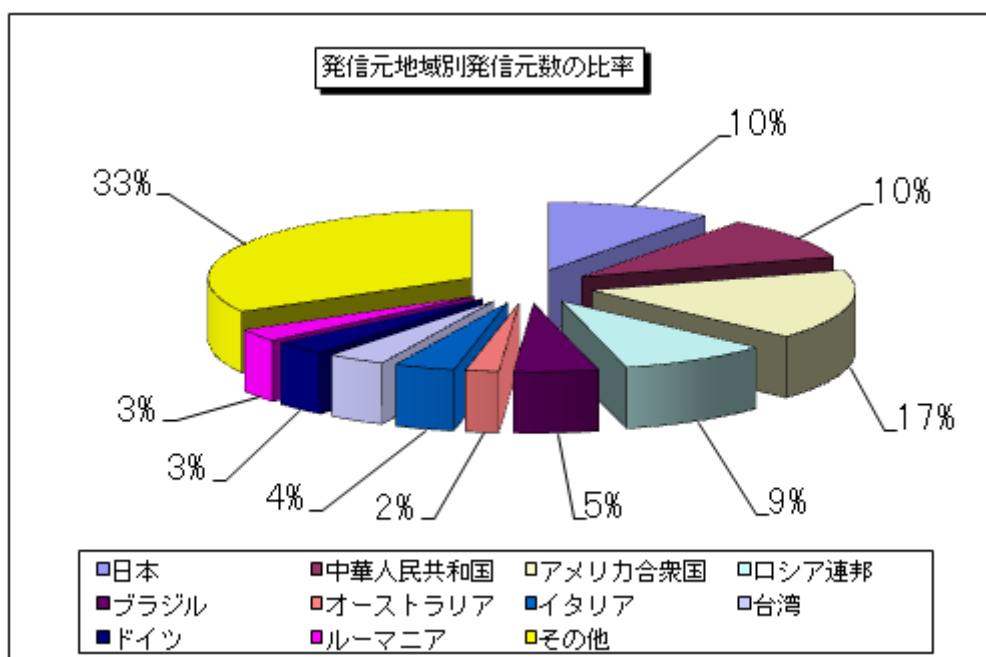


【図 2-6 : 2009 年 11 月の発信元地域別アクセス数の比率】

2009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2-7に、発信元地域別発信元数の比率を図2-8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 2-7：2009年11月の1日あたりの発信元地域別発信元数の遷移】

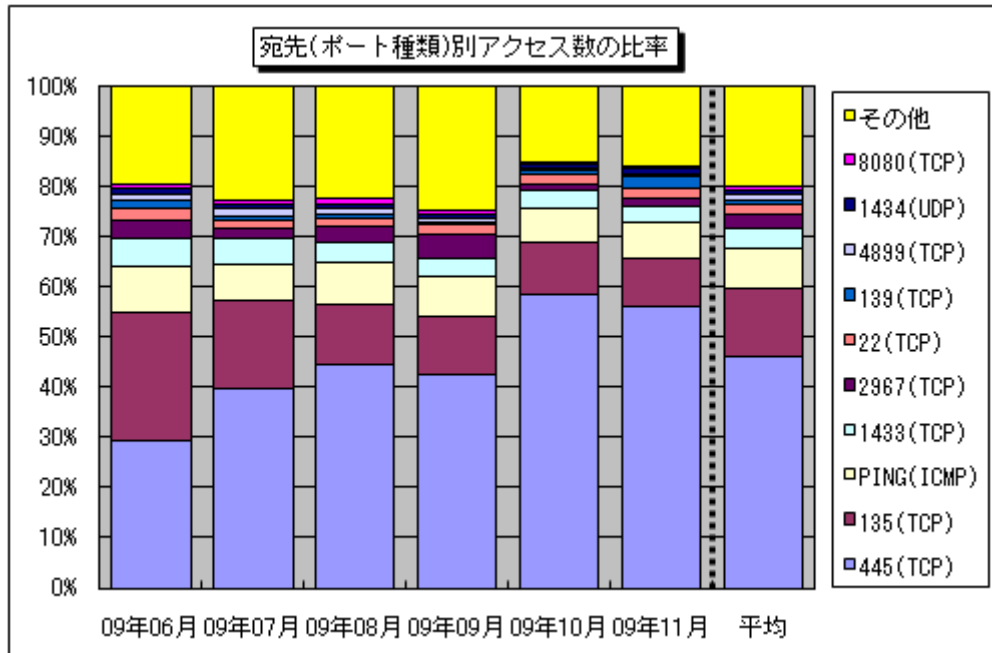


【図 2-8：2009年11月の発信元地域別発信元数の比率】

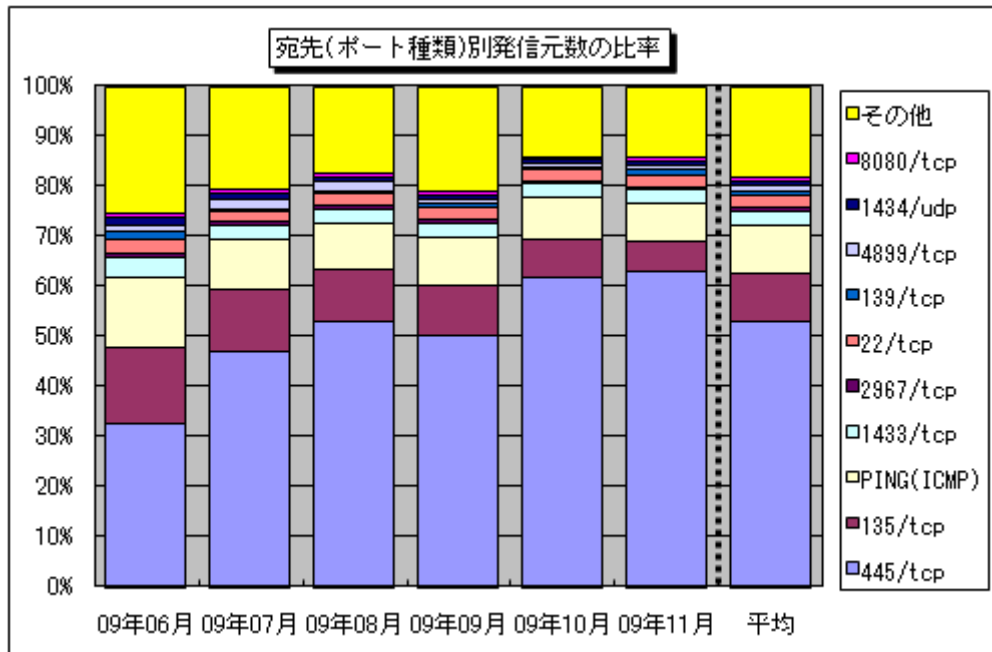
3. 統計情報

(1) 宛先（ポート種類）別の比率

2009年6月～2009年11月の宛先（ポート種類）別アクセス数の比率を図3-1に、宛先（ポート種類）別発信元数の比率を図3-2に示します。



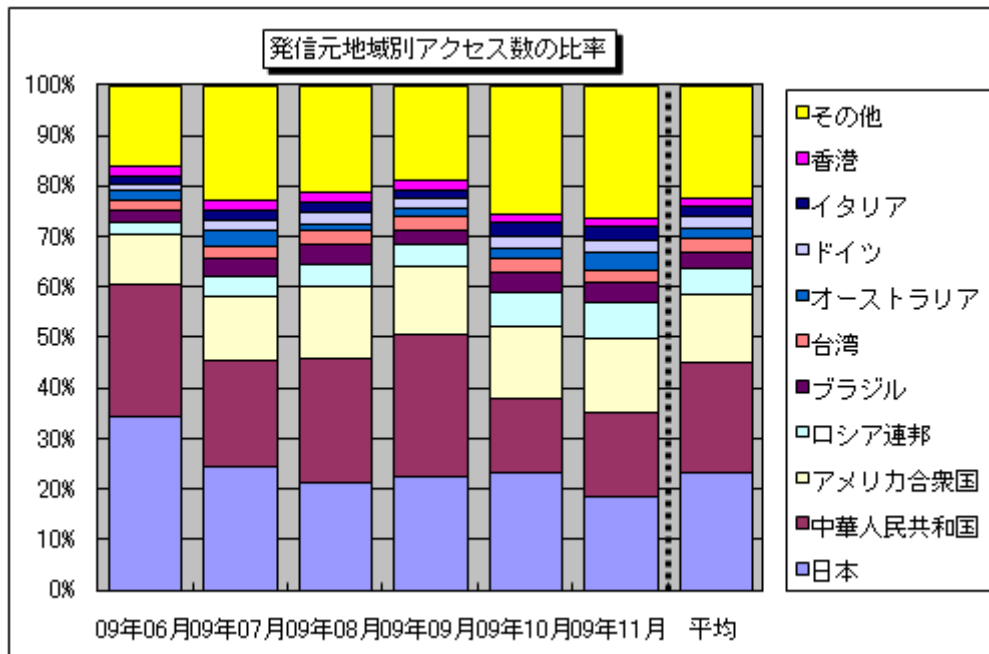
【図3-1：2009年6月～2009年11月の宛先（ポート種類）別アクセス数の比率】



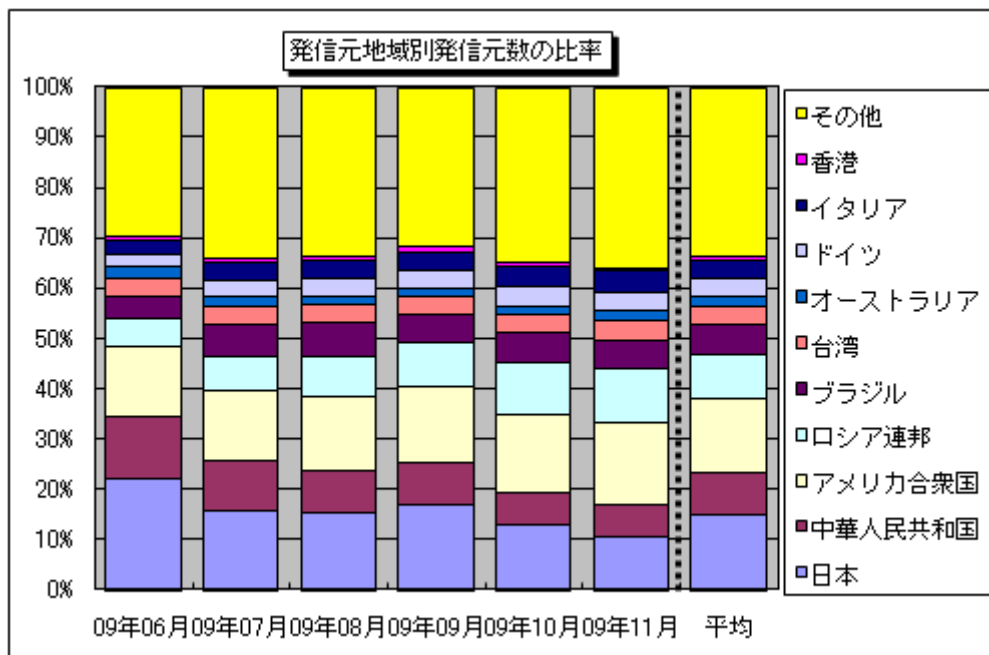
【図3-2：2009年6月～2009年11月の宛先（ポート種類）別発信元数の比率】

(2) 発信元地域別の比率

2009年6月～2009年11月の発信元地域別アクセス数の比率を図3-3に、発信元地域別発信元数の比率を図3-4に示します。



【図 3-3 : 2009 年 6 月～2009 年 11 月の発信元地域別アクセス数の比率】



【図 3-4 : 2009 年 6 月～2009 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、2009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
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）。また、Windowsの脆弱性（MS08-067）を悪用するワームが狙う可能性の高いポートでもある（W32/Downadなど）。
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）。
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の脆弱性を狙ったアクセスである可能性が高い。
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。
2967/tcp	Symantec製品（Symantec Client Security や Symantec AntiVirus など）の脆弱性を狙ったアクセスである可能性が高い。
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Windowsの脆弱性を狙ったアクセスである可能性が高い。
60304/udp	特定の発信元から1観測点のみに観測された、原因不明のアクセス。
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）。
1521/tcp	Oracleデータベースがデフォルトで使用するポートであり、ツールを用いて脆弱なOracleデータベースを探索していたアクセスである可能性が高い。

■お問い合わせ先

IPA 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