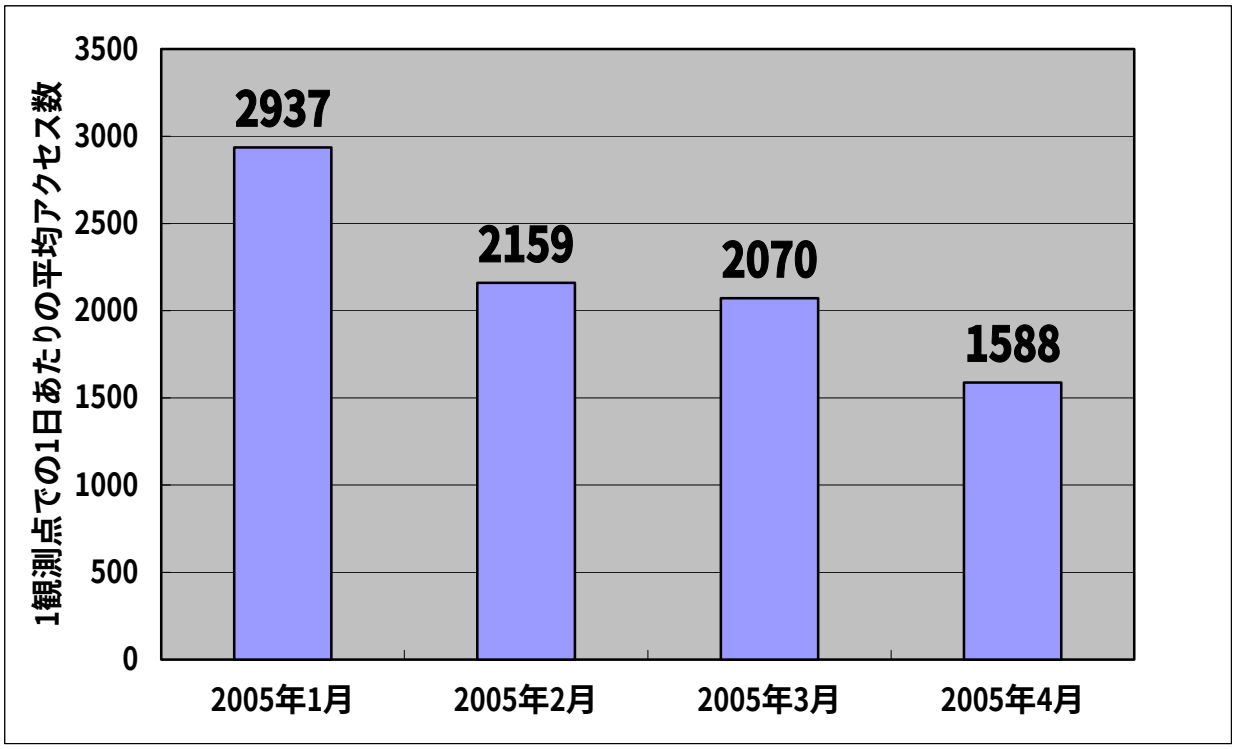
別紙 3

インターネット定点観測(TALOT2)での観測状況について

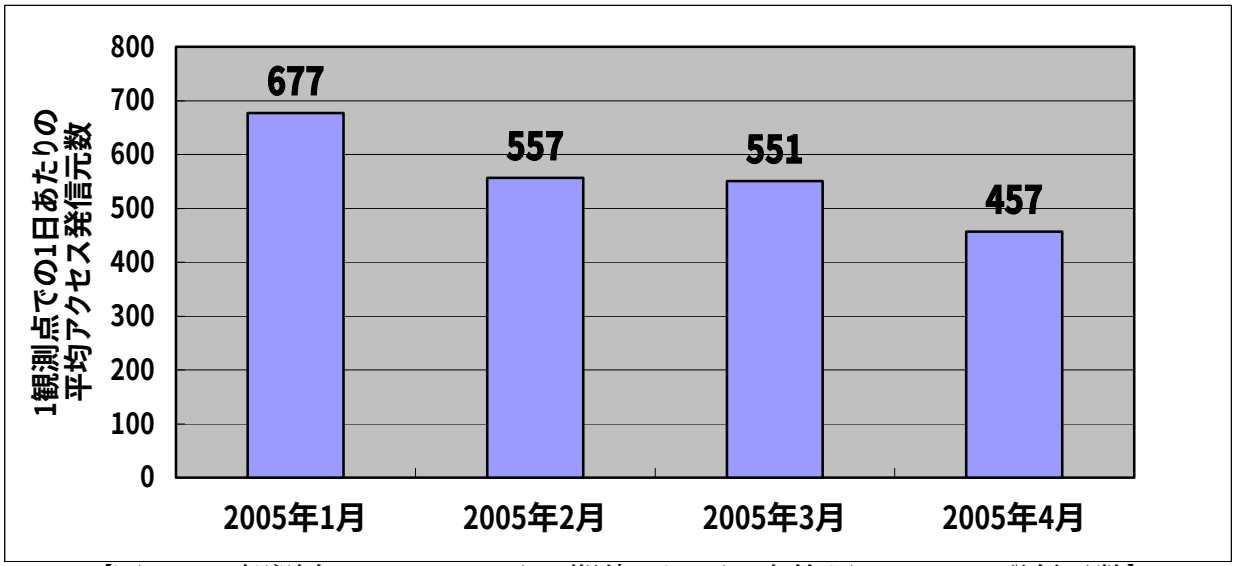
1．一般のインターネット利用者の皆さんへ

インターネット定点観測(TALOT2)では、2005 年 4 月の期待しない（一方的な）アクセスの総数は、10 観測点で **476,320 件**ありました。これは、1 観測点で 1 日あたり**約 1,600 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。



【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】



【図 1.2　1 観測点での 1 日あたりの期待しない(一方的な)アクセスの発信元数】

2005 年 1 月～4 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を図 1.1 に、それらのアクセスの平均発信元数を図 1.2 に示しています。これらの図を見る限り、2005 年 1 月から 4 月にかけては、一方的なアクセスおよびアクセス発信元数が減少傾向にあることが示されています。これらの一方的なアクセスがボット系と呼ばれるワームに起因するとすれば、ボットに感染しているコンピュータの数が減少していると言うことになります。

また、アクセスの発信元地域として国内の比率が若干下がってきていること(後述の図 3.2.1 および図 3.2.2 を参照下さい)を考え合わせると、特に国内でのボットに感染しているコンピュータの数が少しずつ減少していると言うことになります。

インターネットを利用される皆さんのコンピュータについて、皆さんが不正なアクセスに加担(ボットに感染等)していないことを確認するために、今一度ウイルスやワームに感染していないかどうかの確認をお願いします。

- **ウイルス対策ソフトやウイルス対策ベンダーが提供するオンラインウイルス検査による、定期的なウイルスチェックの実施**

また、インターネットを利用される皆さんのネットワーク環境において、以下に示す対策をお勧めします。

- **ルータやファイアウォールでの継続的な防御**
- **コンピュータの状態を最新なものにしておくためのパッチの適用(Windows Update 等)や、使用するアプリケーションのバージョンアップ**
- **サーバ等を利用されている方は、不要なサービスの停止**

  (詳細は「SOHO・家庭向けの情報セキュリティ対策マニュアル（Ver1.20）」
  http://www.ipa.go.jp/security/fy14/contents/soho/mokuji.html
  を参照下さい)

2．4 月のアクセス状況

2005 年 4 月の一方的なアクセスの変化(宛先(ポート種類)別アクセス数の変化)を、図 2.1.1 に示します。あいかわらず、135(TCP),445(TCP)ポートへのアクセスが多いようです。

次に、図 2.1.2 に宛先(ポート種類)別アクセス数ではなく、宛先(ポート種類)別発信元数の状況を示します。宛先(ポート種類)別発信元数とは、特定の宛先(ポート種類)へアクセスしている発信元(発信 IP アドレス)の数のことです。

135(TCP),445(TCP)ポートへのアクセスについては、アクセス数の場合と同様に発信元数も多いことが分かります。

ただし、複数の宛先へ同一の発信元からアクセスされる場合もあるので、図 2.1.2 の縦軸に示された発信元数が、実際の発信元数ではないことに注意して下さい。

図 2.1.1 と図 2.1.2 の違いは、ちょうどウイルス発見届出での検知件数と届出件数の違いと、同じ理屈になっており、図 2.1.1 のアクセス数でのアクセス状況は実際のアクセスの脅威を示し、図 2.1.2 の発信元数でのアクセス状況からはアクセスの原因となるコンピュータ(発信元)の感染状況を示すと考えられます。

図 2.2.1 および図 2.2.2 には、宛先(ポート種類)別アクセス数の比率および宛先(ポート種類)別発信元数の比率を示します。135(TCP)や 445(TCP)へのアクセスが、アクセス数に比較して発信元数の比率が低いことが分かります。これは、135(TCP)や 445(TCP)へのアクセスが、他の宛先へのアクセスより多く同一の発信元から送られていることを示しています。コンピュータの脆弱性を狙うという意味では、一番狙いやすい宛先であるということになります。

図 2.3.1 および図 2.3.2 には、発信元地域別アクセス数の変化および発信元地域別発信元数の変化を 1 日単位で示しています。月初から月末にかけて、国内からのアクセスが緩やかに減少していることが分かります。図3.1.1や図3.1.2での宛先(ポート種類)別アクセス数数の比率や宛先(ポート種類)別発信元数の比率にも表れているような、国内からのアクセスの緩やかな減少傾向が、そのまま 4 月の日毎のアクセス状況にも表れていると言うことで、国内の状況が緩やかに改善されていることを示していると考えられます。この変化が、時期あるいは季節によるパターンでないことを期待する次第です。

＜IPA からのお知らせ＞

⑴ 観測データについて

22(TCP)へのアクセスのうち、IPA での観測環境(TALOT2)の 22 番ポートが開いていることに起因するパスワードクラッキング攻撃については、4 月分の観測報告データから除外することに決めました。これは、観測状況が一般的なインターネット利用者と同じ状況のものではないと考えられるからです。また、3 月分までは Ping(ICMP)を除いたデータでしたが、4 月分の観測報告データからはこれらを含めることにしました。

さらに、3 月分まではアクセス数をベースにグラフを掲載していましたが、今回は発信元数(発信元 IP アドレス数)をベースとする情報も掲載することにしました。発信元数をベースとした情報も掲載する理由は、以下の通りです。

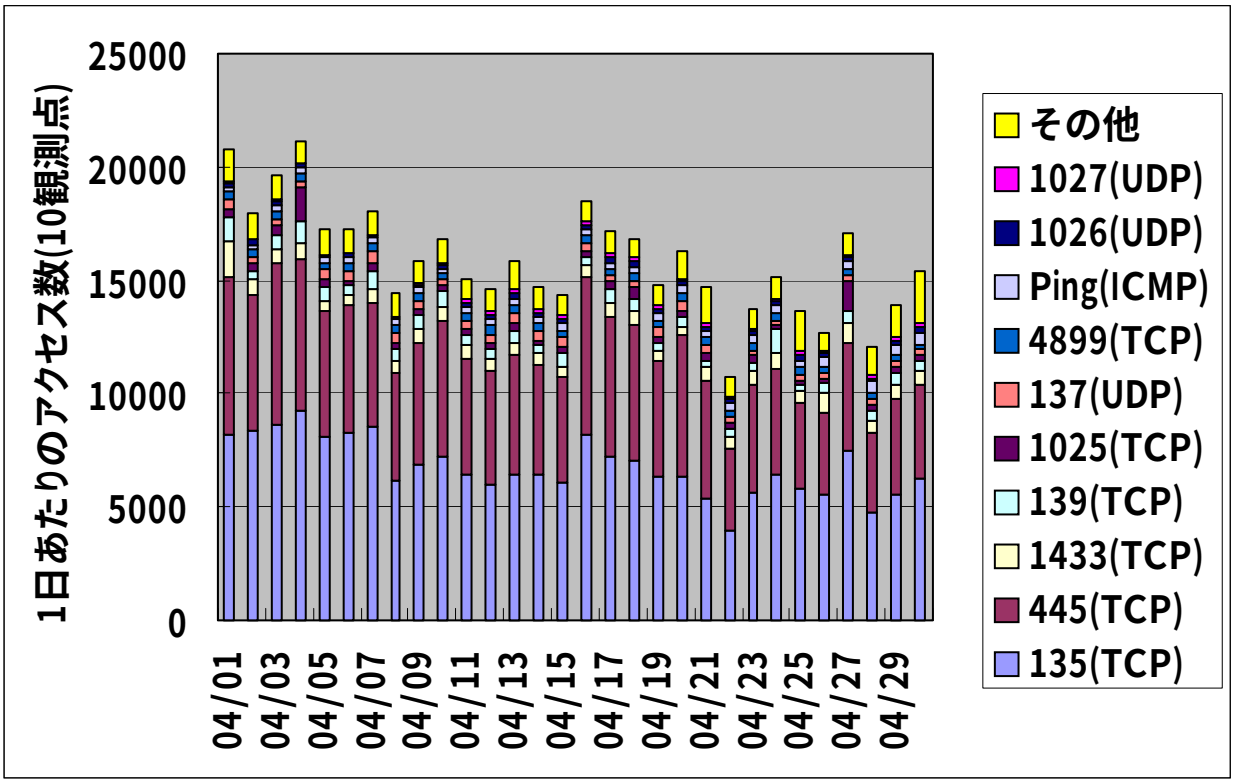
- アクセス数ベースの情報はアクセスの脅威をそのまま表現できるが、特定の発信元が大量のアクセスを発信した場合に、グラフに特異点が表示される場合がある
- 発信元数ベースであれば特定発信元によるグラフ上の特異点は表示されにくいが、アクセスの脅威と言う意味では脅威度が損なわれる可能性がある
- 発信地域別の情報については、発信元数ベースのほうが、より発信元比率の精度が高いと考えられる

⑵ 訂正

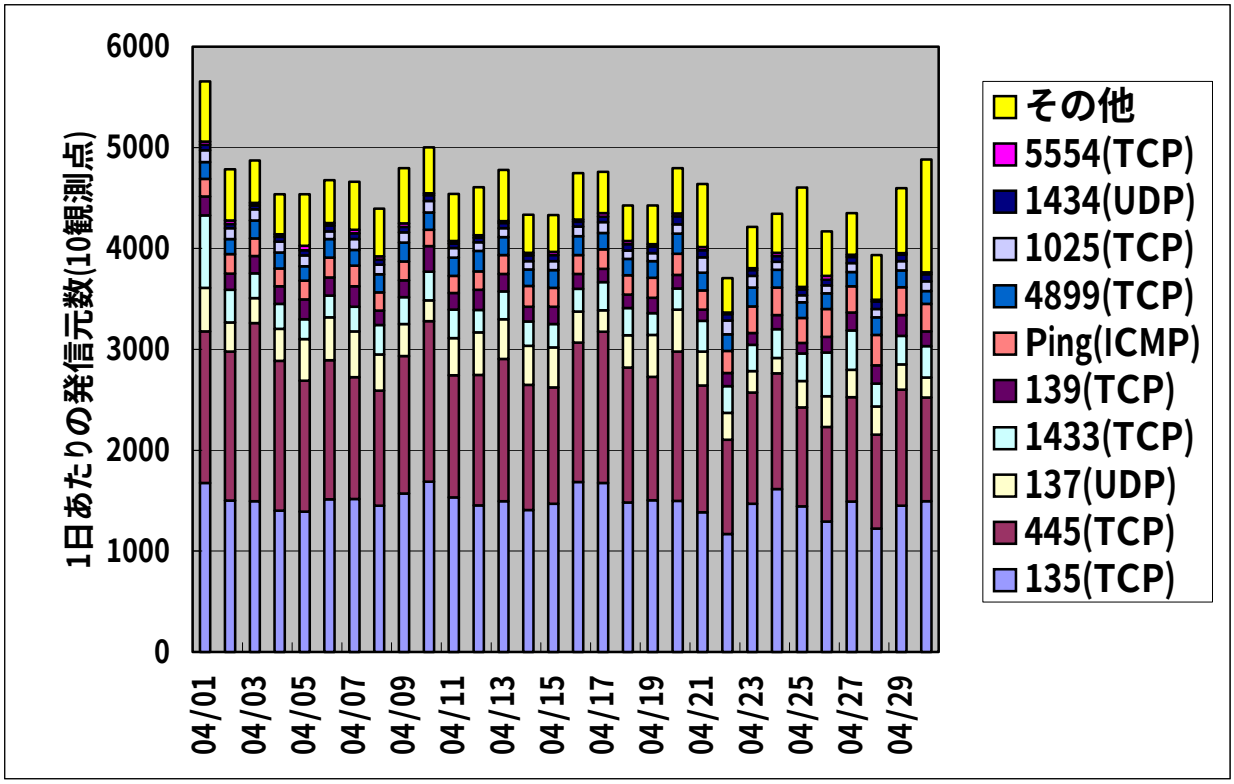
3 月分までの観測報告で、観測データの分析に誤りが見つかりました。データの誤りは、発信元地域情報です。発信元の IP アドレスから発信元地域を求める処理で使用していた発信元地域変換テーブルに一部誤りデータが含まれていました。実際に3月分までの観測データで発信元地域がオーストリアと発表していたもののうち、ほとんどが国内のものであることが判明しています。

既に発表しているグラフ情報は訂正できませんが、今月の発表情報中に同一の情報を掲載します。この訂正により、本データの利用者の皆様へのお詫びとさせて頂きます。

2.1 2005 年 4 月の一方的なアクセス状況

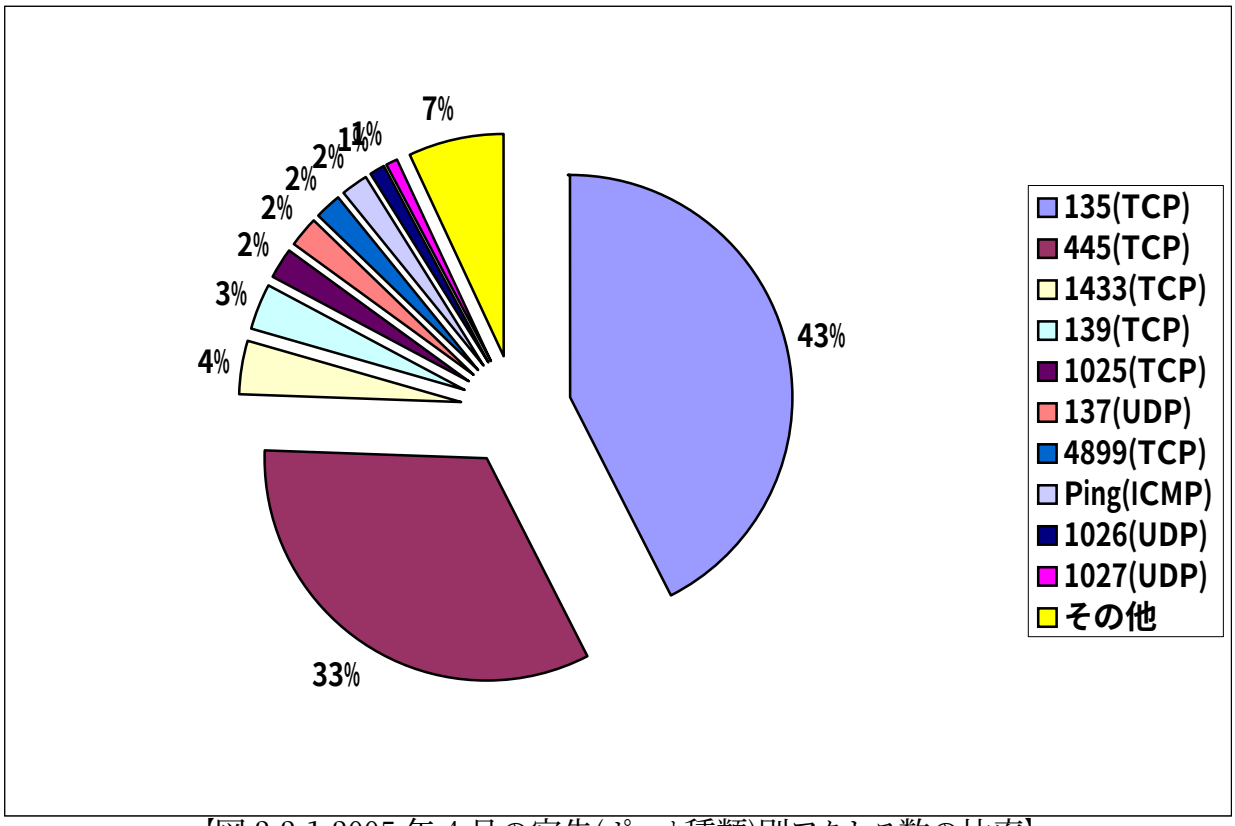


【図 2.1.1 2005 年 4 月の一方的なアクセス状況(アクセス数)】

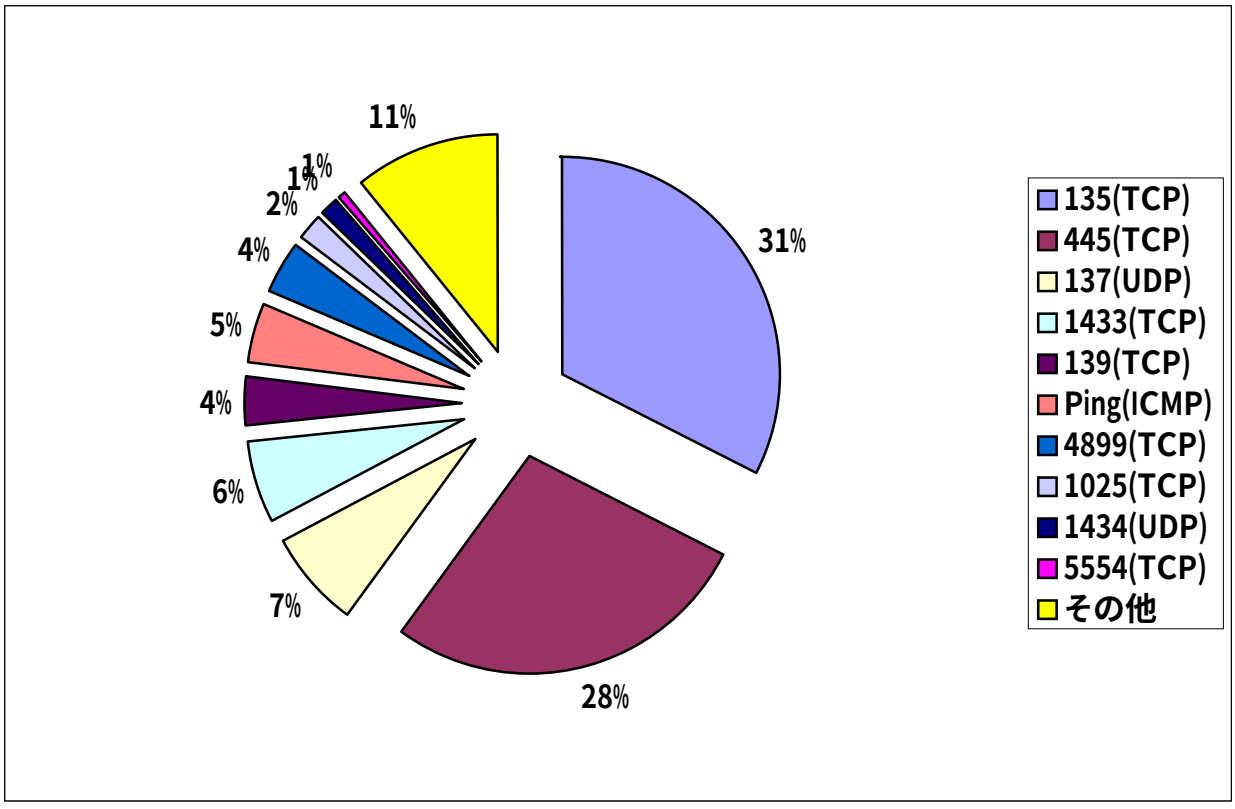


【図 2.1.2 2005 年 4 月の一方的なアクセス状況(発信元数)】

2.2 2005 年 4 月の宛先(ポート種類)別の比率

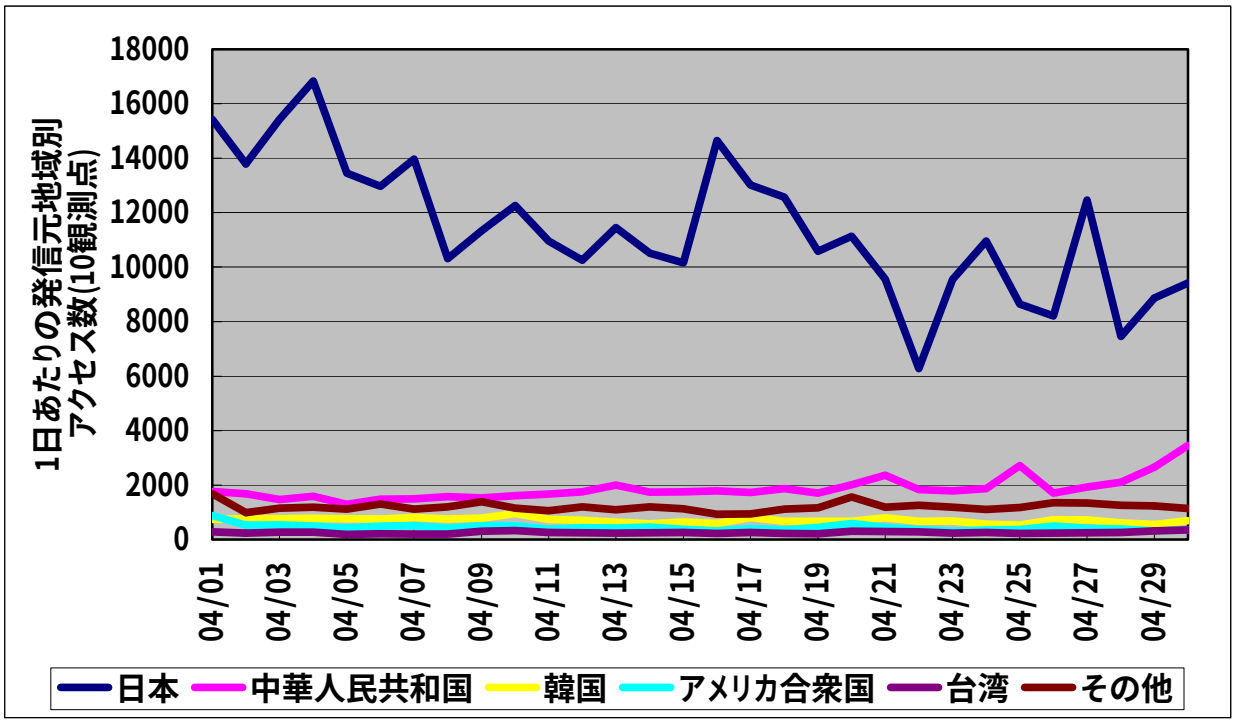


【図 2.2.1 2005 年 4 月の宛先(ポート種類)別アクセス数の比率】

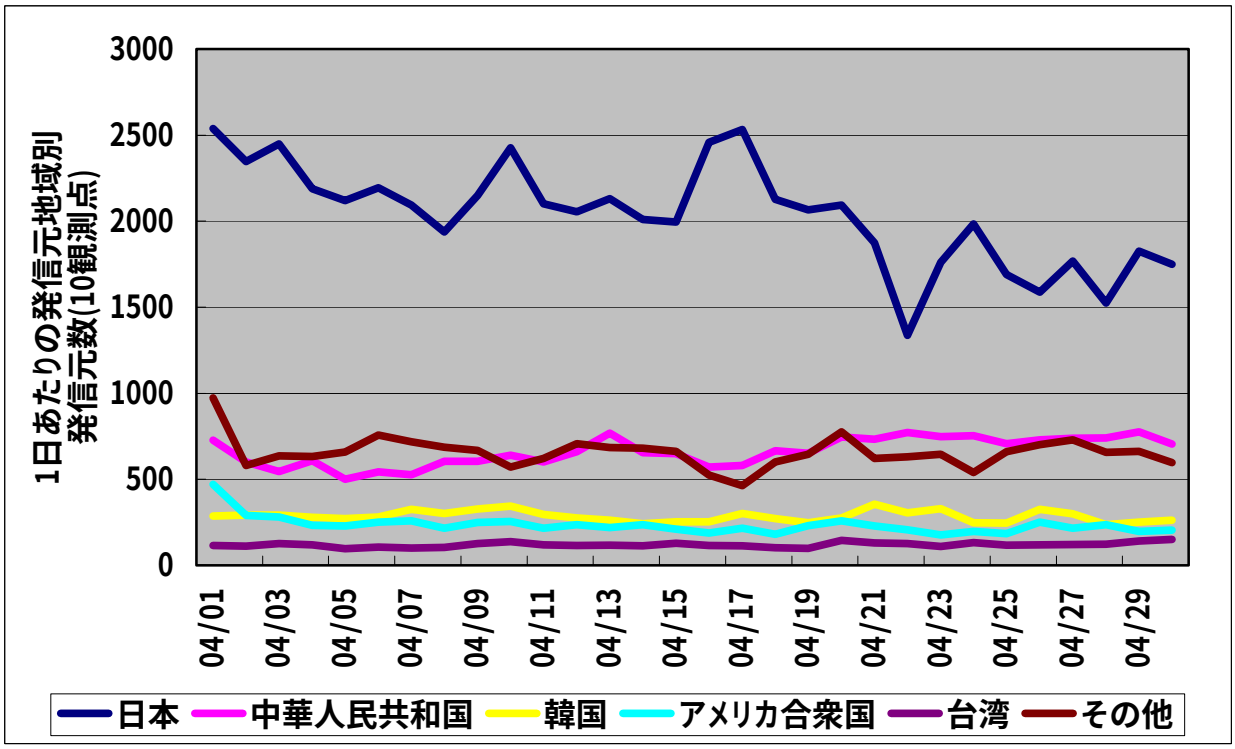


【図 2.2.2 2005 年 4 月の宛先(ポート種類)別発信元数の比率】

2.3 2005 年 4 月の発信元地域別アクセス状況



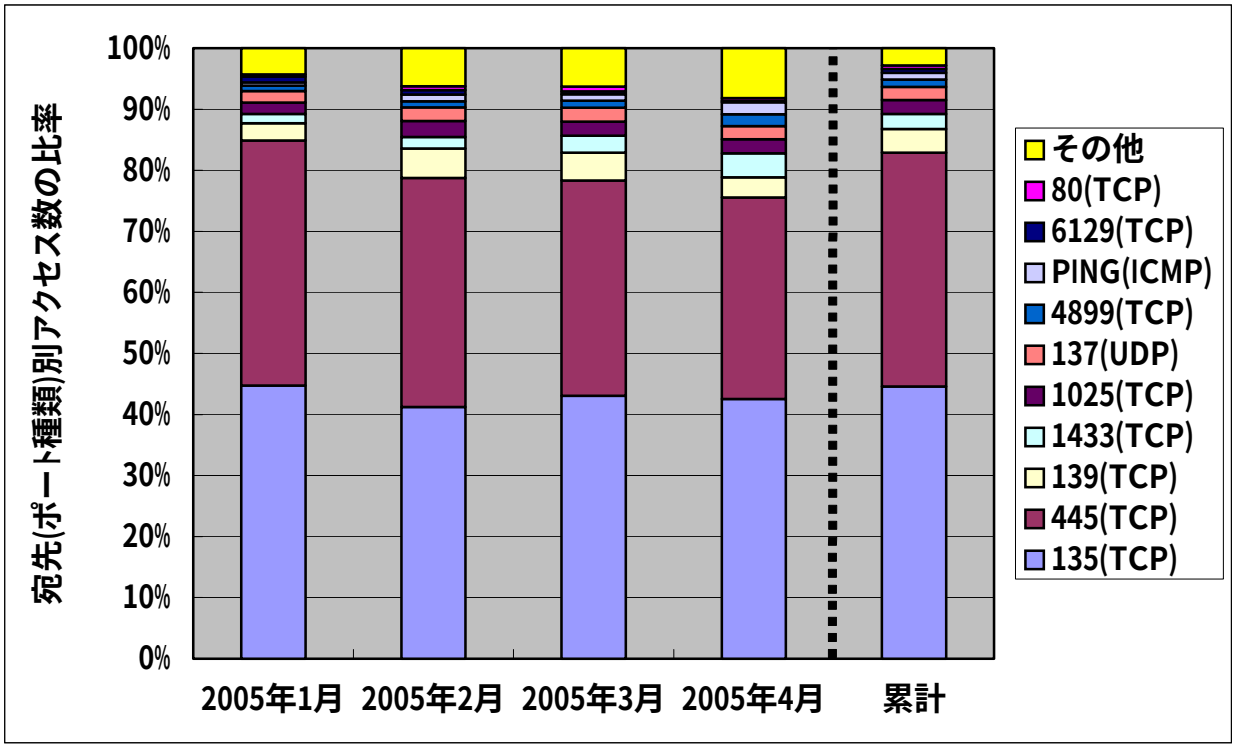
【図 2.3.1 2005 年 4 月の発信元地域別アクセス数の変化】



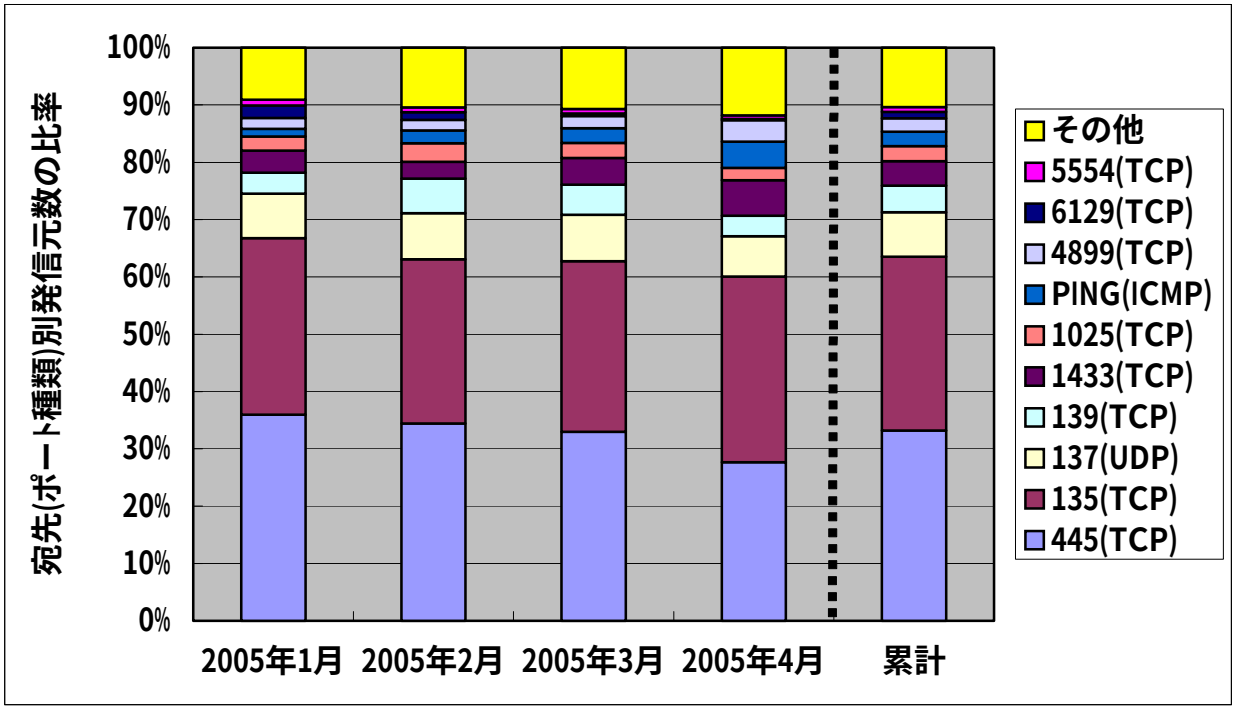
【図 2.3.2 2005 年 4 月の発信元地域別発信元数の変化】

3．統計情報

3.1 2005 年 1 月～4 月の宛先(ポート種類)別の比率

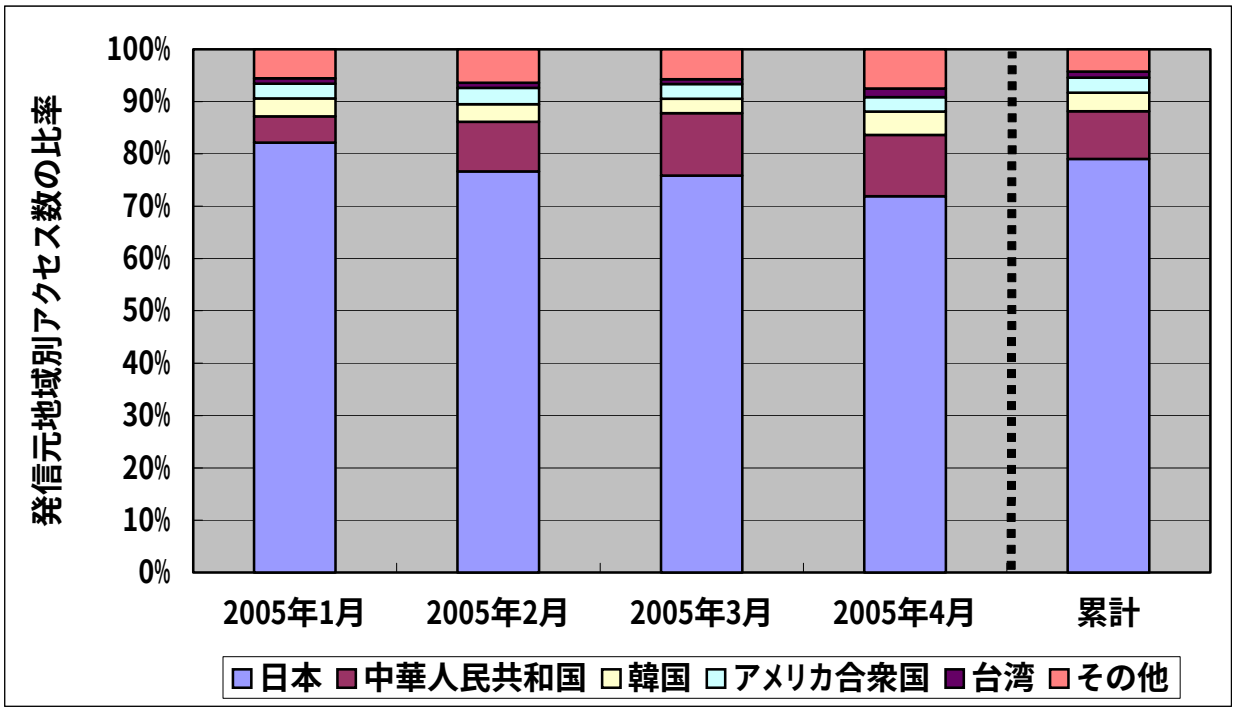


【図 3.1.1 2005 年 1 月～4 月の宛先(ポート種類)別アクセス数の比率】

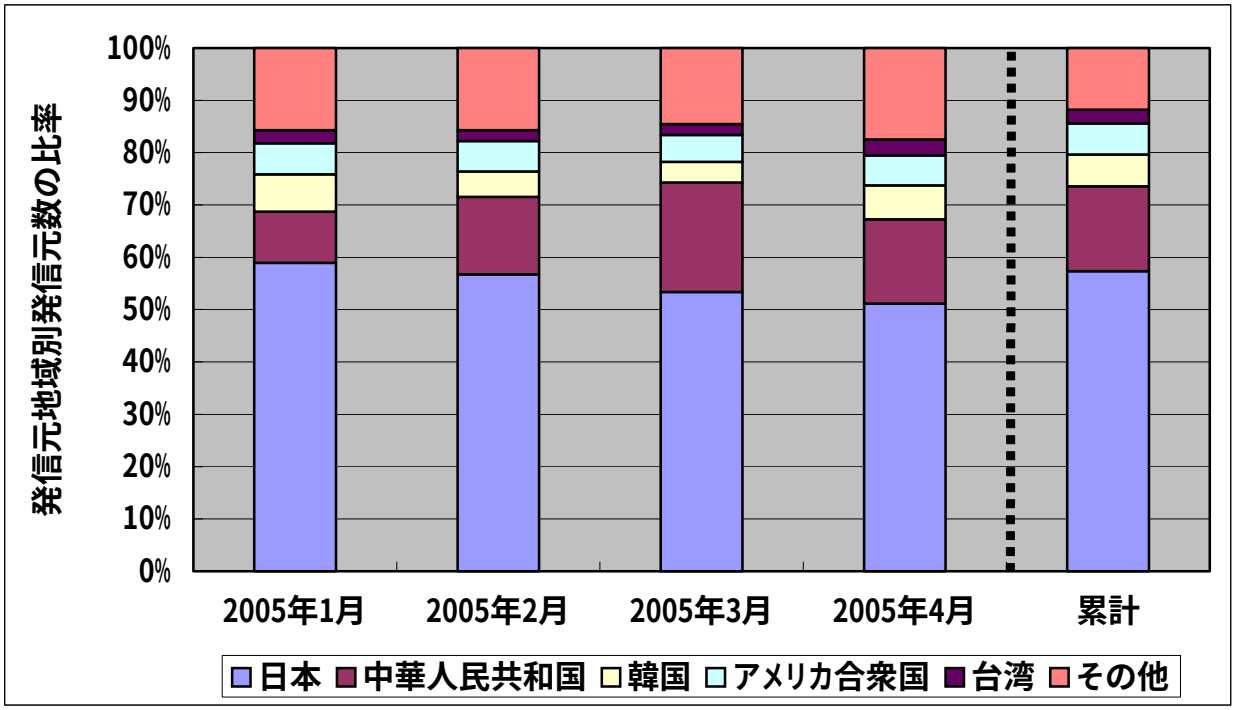


【図 3.1.2 2005 年 1 月～4 月の宛先(ポート種類)別発信元数の比率】

3.2 2005 年 1 月～4 月の発信元地域別の比率



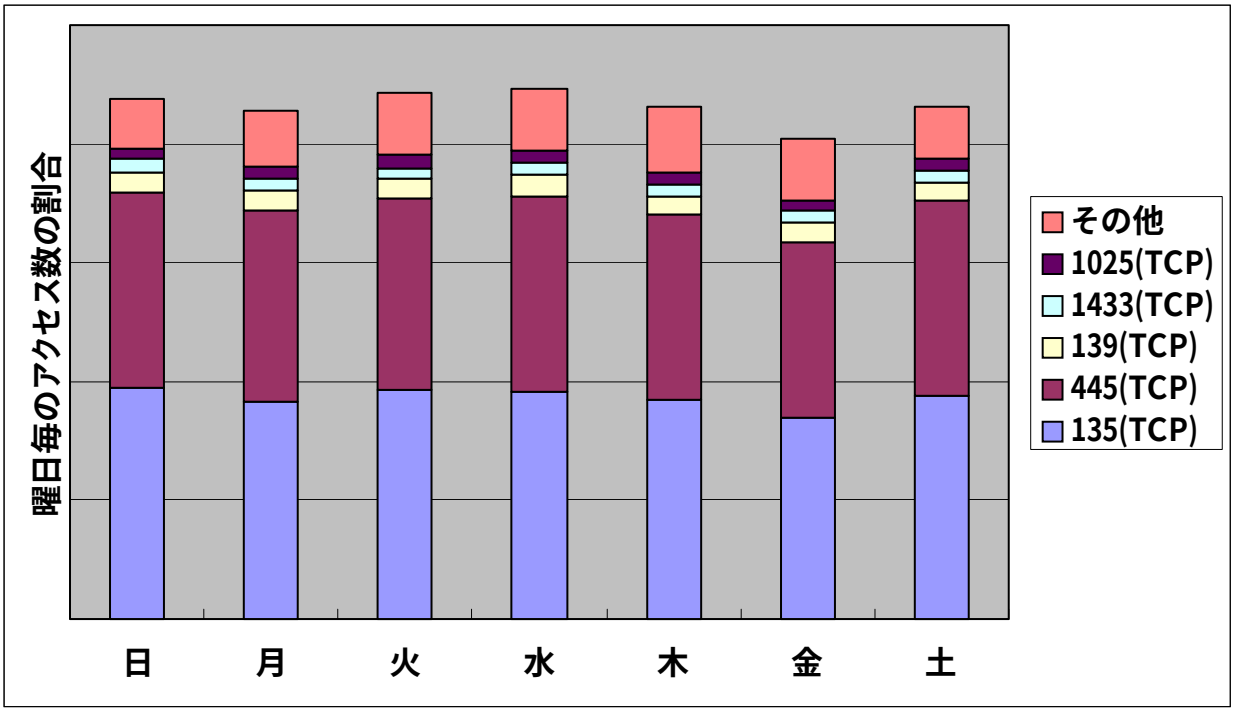
【図 3.2.1 2005 年 1 月～4 月の発信元地域別アクセス数の比率】



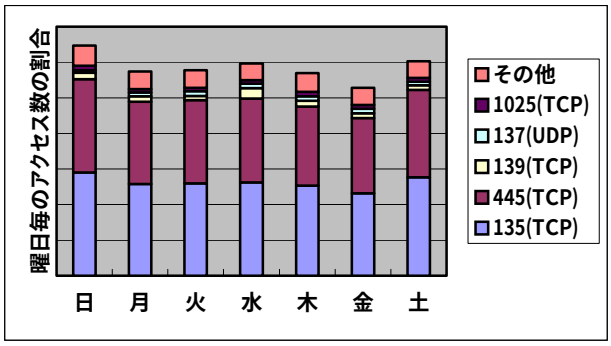
【図 3.2.2 2005 年 1 月～4 月の発信元地域別発信元数の比率】

4．その他の統計情報

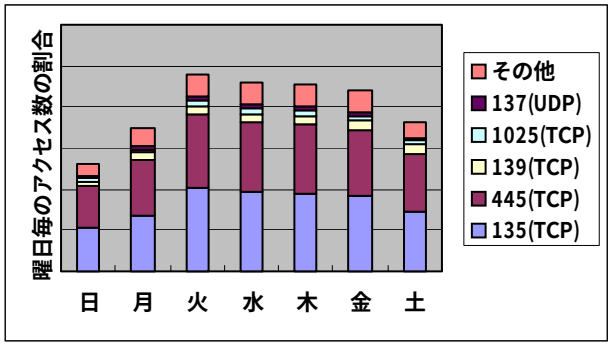
4.1 2005 年 1 月～4 月の曜日別統計



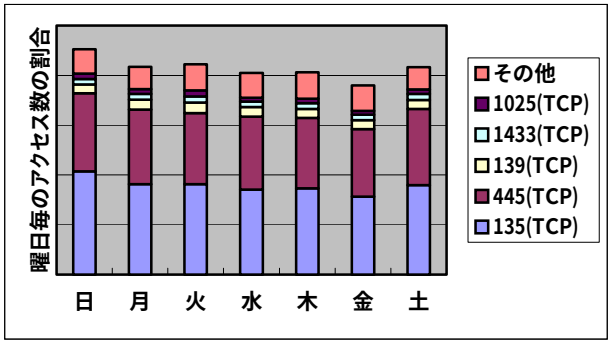
【図 4.1.1 2005 年 1 月～4 月の宛先(ポート種類)別アクセス数の曜日別統計】



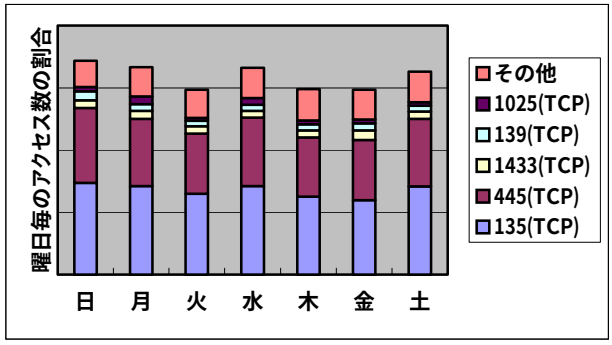
【図 4.1.2 2005 年 1 月の曜日別統計】



【図 4.1.3 2005 年 2 月の曜日別統計】



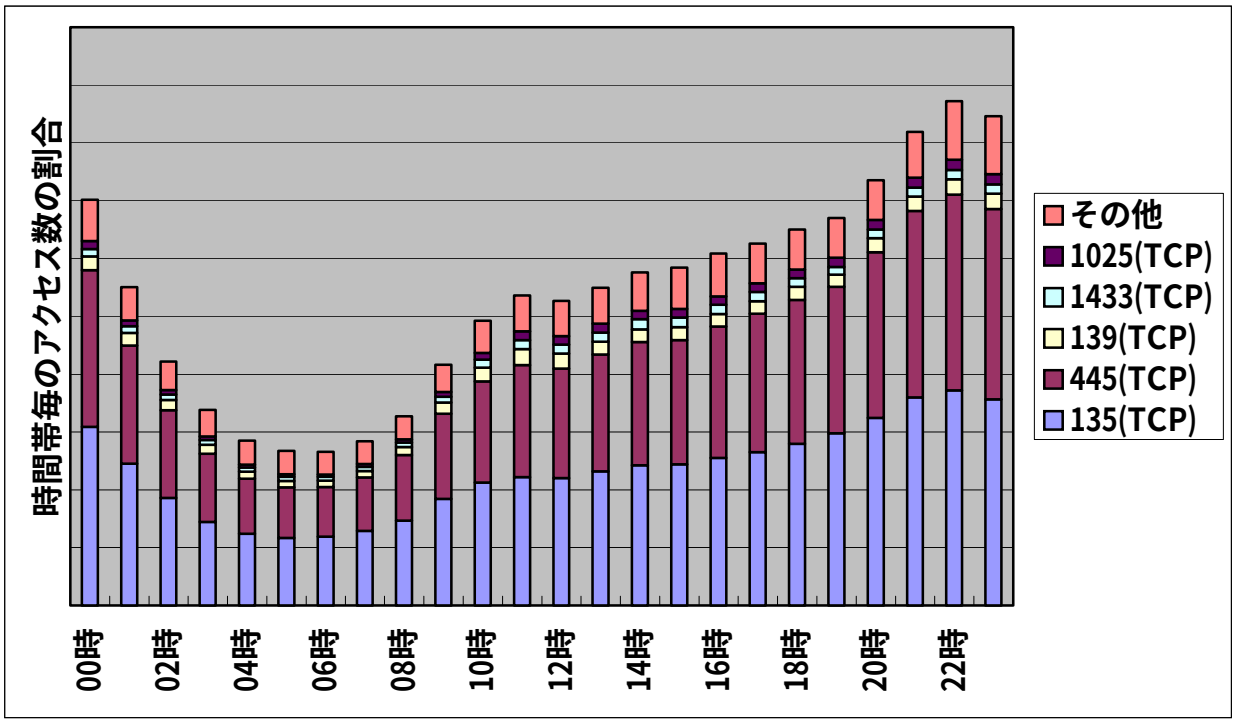
【図 4.1.4 2005 年 3 月の曜日別統計】



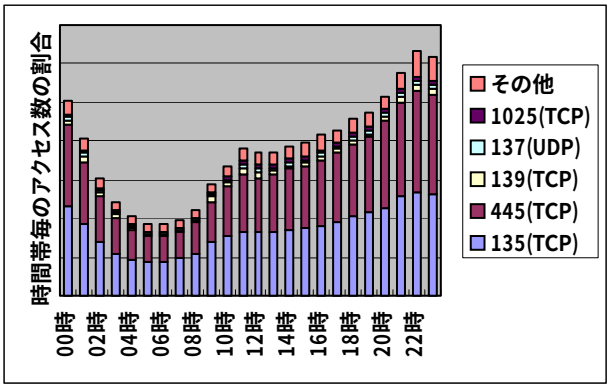
【図 4.1.5 2005 年 4 月の曜日別統計】

曜日別のアクセス数に関する統計については、結果的にあまり意味のない統計情報のようでした。何らかのパターンが出ることを期待したのですが、2 月の情報があまりに他の月と違うようで、もう少し長いレンジで検討する必要があるかも知れません。

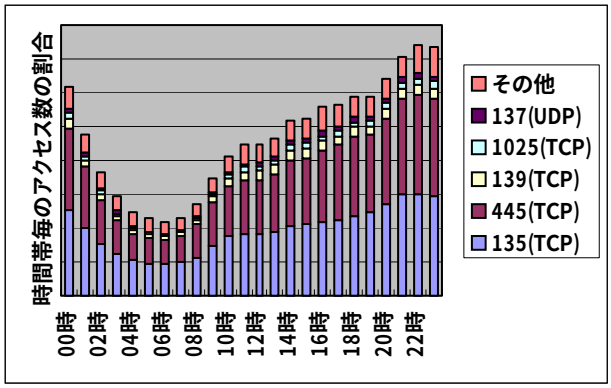
4.2 2005 年 1 月～4 月の時間帯別統計



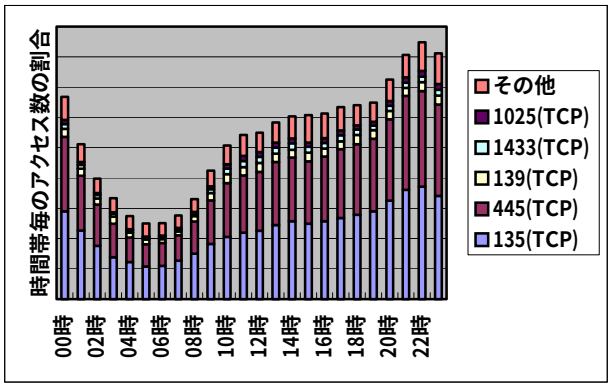
【図 4.2.1 2005 年 1 月～4 月の宛先(ポート種類)別アクセス数の時間帯別統計】



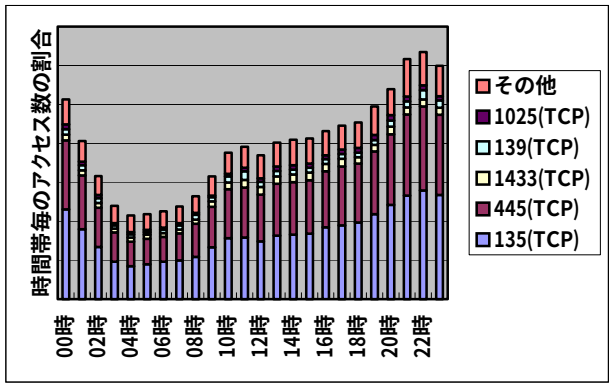
【図 4.2.2 2005 年 1 月の時間帯別統計】



【図 4.2.3 2005 年 2 月の時間帯別統計】



【図 4.2.4 2005 年 3 月の時間帯別統計】



【図 4.2.5 2005 年 4 月の時間帯別統計】

時間帯別のアクセス数に関する統計については、ほぼ良好なパターンを抽出することができています。ある意味で、コンピュータを利用する利用者の生活パターンが見えてくるようです。

・コンピュータ不正アクセス被害の届出制度について

コンピュータ不正アクセス被害の届出制度は、経済産業省のコンピュータ不正アクセス対策基準に基づき、’96 年 8 月にスタートした制度であり、同基準において、コンピュータ不正アクセスの被害を受けた者は、被害の拡大と再発を防ぐために必要な情報をＩＰＡに届け出ることとされています。

ＩＰＡでは、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータ不正アクセス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

○コンピュータ不正アクセス対策基準
- ・通商産業省告示第３６２号　平成 8 年 8 月 8 日制定
- ・通商産業省告示第５３４号　平成 9 年 9 月 24 日改訂
- ・通商産業省告示第９５０号　平成 12 年 12 月 28 日改訂
- ・経済産業省告示第３号　　平成 16 年 1 月 5 日改訂

■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