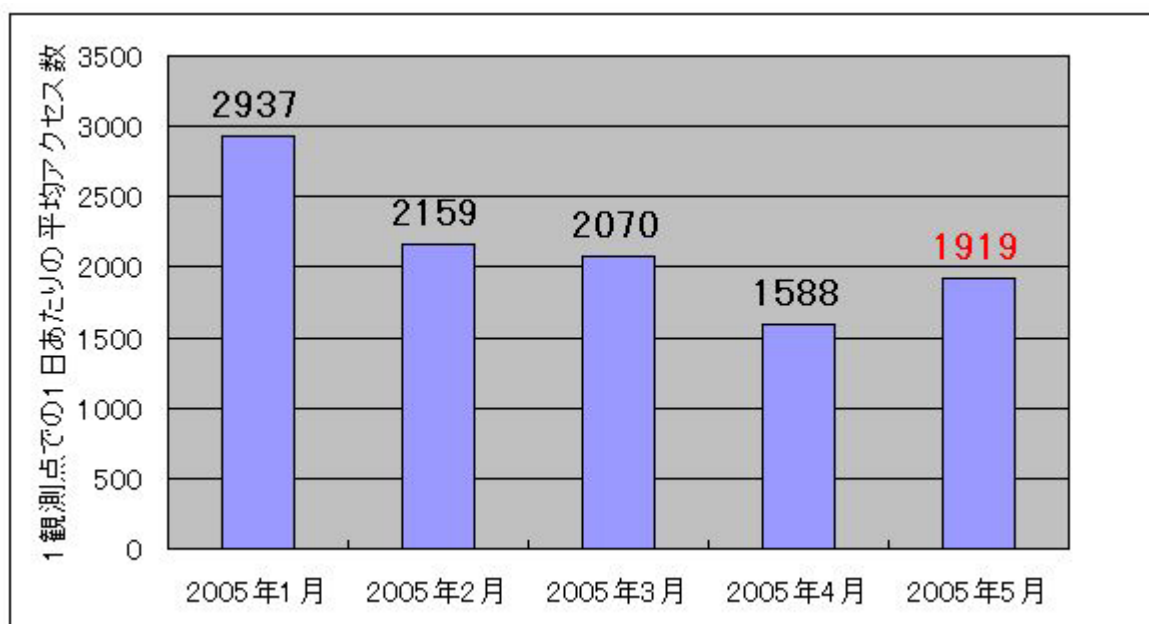


インターネット定点観測(TALOT2)での観測状況について

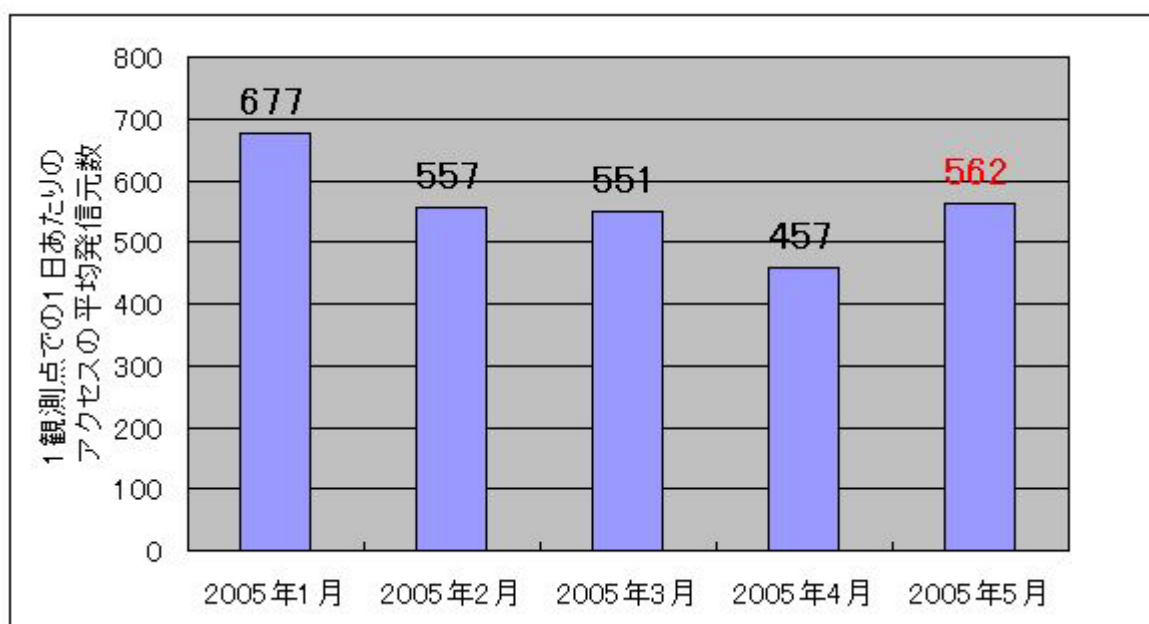
1. 一般のインターネット利用者の皆さんへ

インターネット定点観測(TALOT2)では、2005年5月の期待しない(一方的な)アクセスの総数は、10観測点で594,960件ありました。これは、1観測点で1日あたり約1,900件のアクセスがあったこととなります。

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向的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】

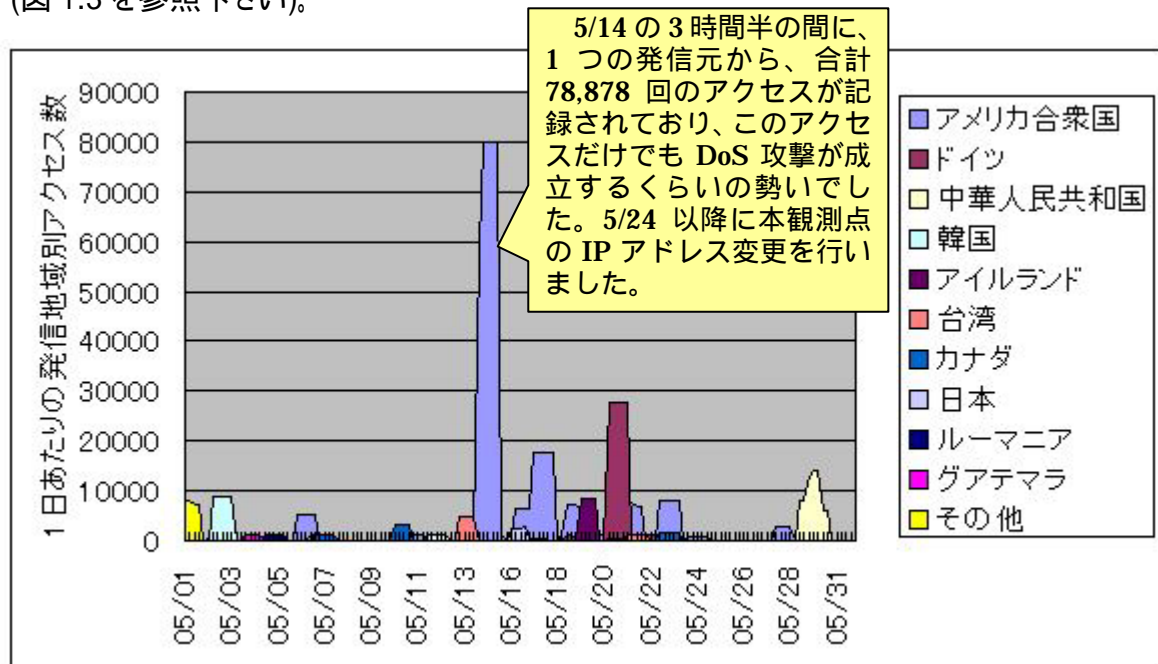


【図 1.2 1観測点での1日あたりの期待しない(一方的な)アクセスの発信元数】

2005年1月～5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。これらの図を見ると、2005年4月まで緩やかに減少傾向にあった1日あたりのアクセス数および発信元数が、5月に増加したことになります。

5月中旬にはMicrosoftのWindows上で動作するSQL Serverを探す目的と思われる宛先ポート1433(TCP)へのポートスキャンが、広い範囲で増加(通常の4～5倍程度)しました(後述の「2.4 1433(TCP)ポートへのアクセスについて」を参照下さい)。

また、観測データとしては公開していませんが、あいかわらずSSH(Secure Shell)を通してコンピュータに侵入しようとするパスワードクラッキングアクセス(22(TCP)へのアクセス)も続いています(図1.3を参照下さい)。



【図1.3 特定観測点での1日あたりのSSH(Secure Shell: 22(TCP)ポート)への攻撃<参考情報>】

2.5月のアクセス状況

2005年5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。特に、5月20日前後に445(TCP)や1433(TCP)ポートへのアクセス増加が観測されています(詳細は後述)。

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。

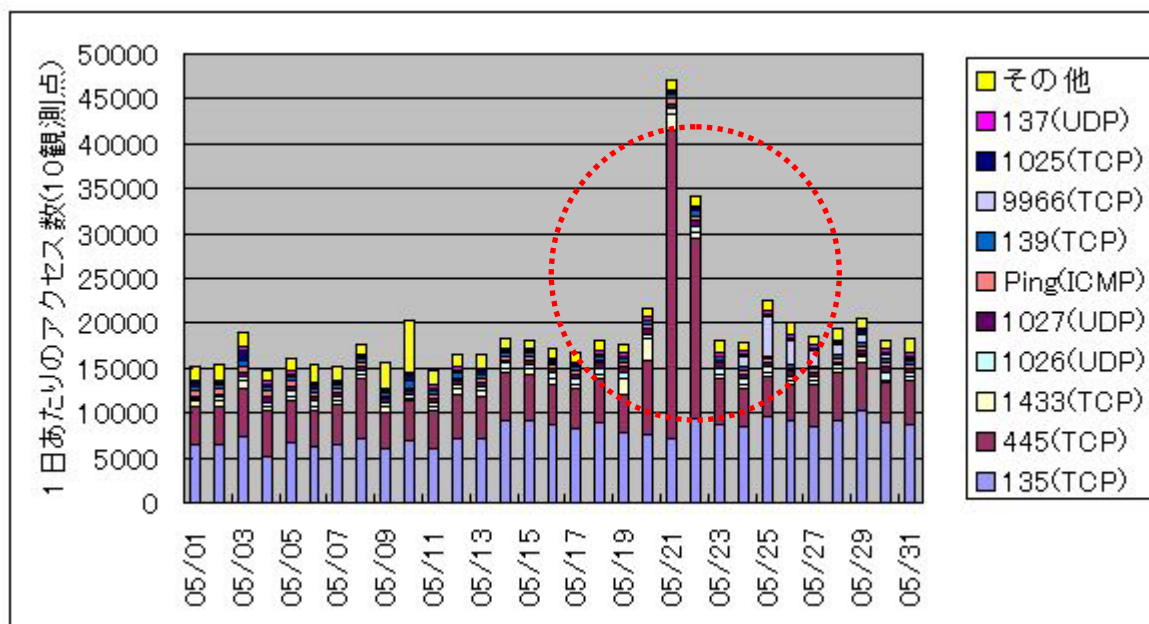
図2.1.1と図2.1.2の違いは、ちょうどウイルス発見届出での検知件数と届出件数の違いと、同じ理屈になっており、図2.1.1のアクセス数でのアクセス状況は実際のアクセスの脅威を示し、図2.1.2の発信元数でのアクセス状況からはアクセスの原因となるコンピュータ(発信元)の感染状況を示すと考えられます。

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。

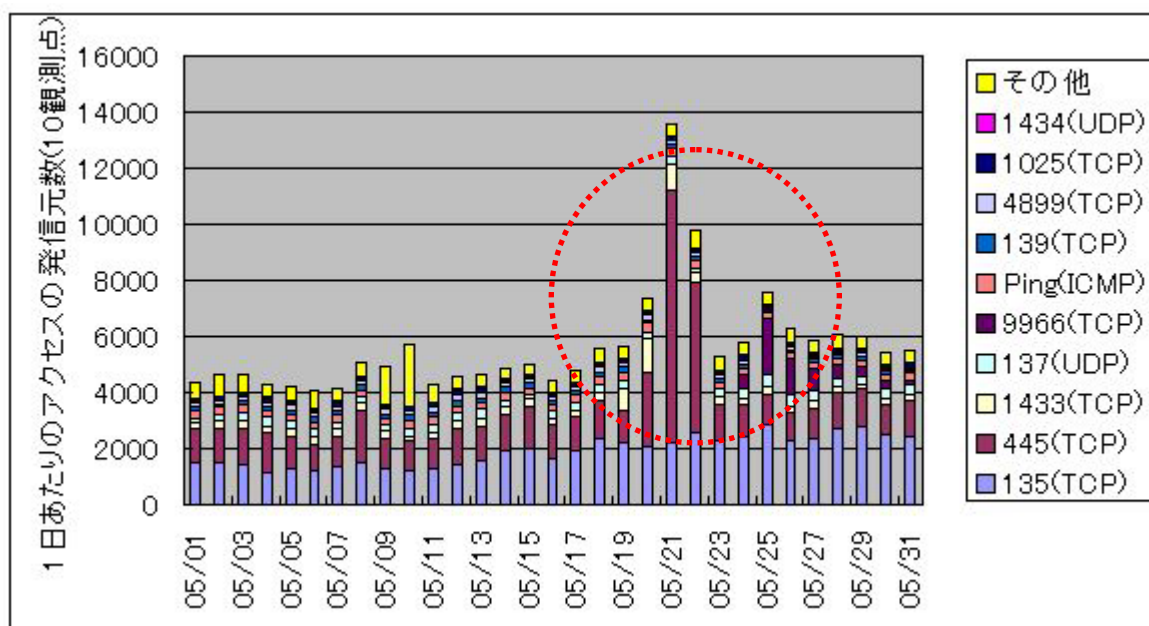
図2.3.1および図2.3.2には、発信元地域別アクセス数の変化および発信元地域別発信元

数の変化を1日単位で示しています。4月の緩やかな減少傾向から、5月は緩やかな増加傾向に転じたようです。これらの図にも5月20日前後のアクセス状況の乱れが表れています。

2.1 2005年5月の一方的なアクセス状況



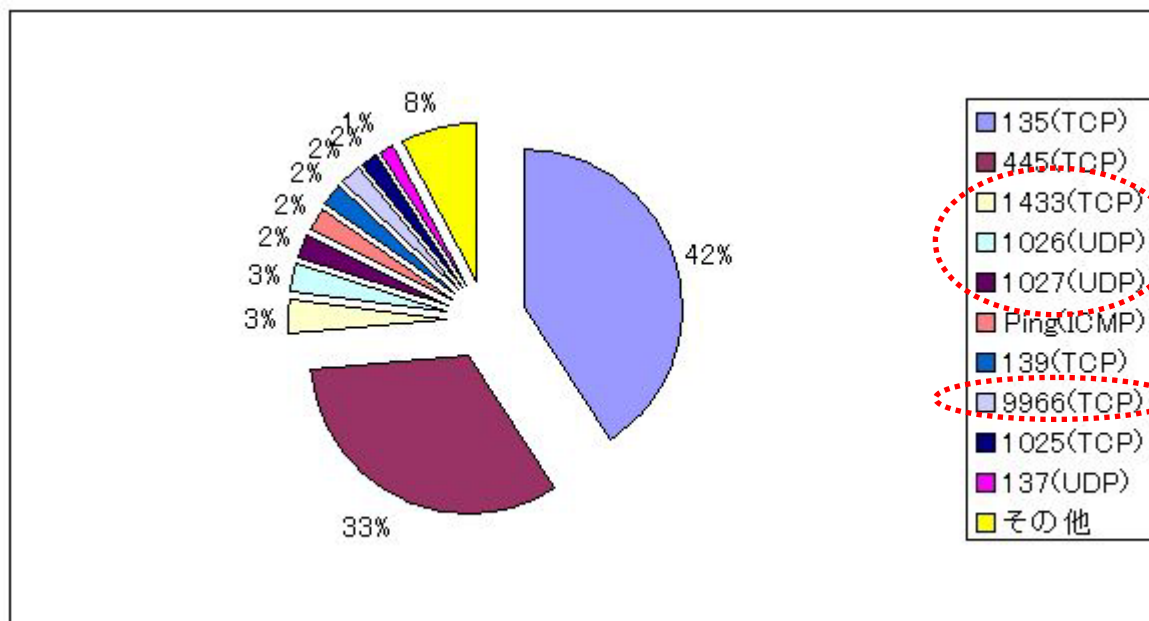
【図 2.1.1 2005年5月の一方的なアクセス状況(アクセス数)】



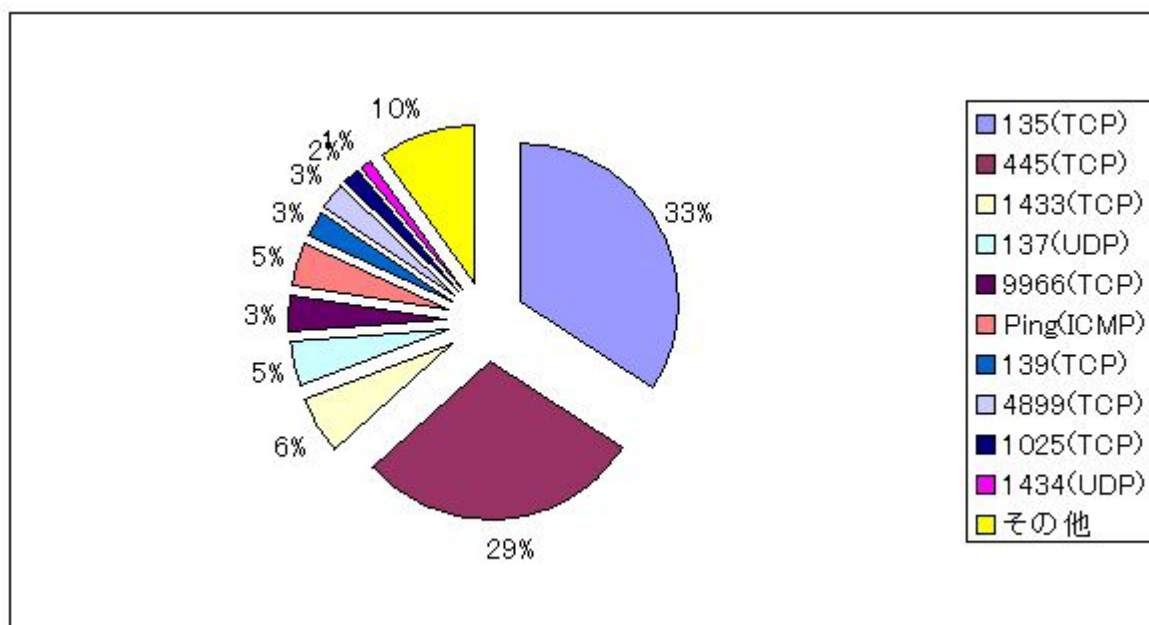
【図 2.1.2 2005年5月の一方的なアクセス状況(発信元数)】

- 5月19日から21日にかけて、1433(TCP)ポートへのアクセスが増加しました。このアクセスについては、「2.4 1433(TCP)ポートへのアクセスについて」を参照下さい。
- 5月20日から22日にかけて、445(TCP)ポートへのアクセスが増加しました。このアクセスについては、「2.5 特定観測点における 445(TCP)ポートへのアクセスについて」を参照下さい。ただし、このアクセスは特定観測点でのみ観測されているものです。
- 5月24日以降の9966(TCP)ポートへのアクセス(次頁を参照下さい)が見られますが、このアクセスは特定観測点でのみ観測されているものです。

2.2 2005年5月の宛先(ポート種類)別の比率



【図 2.2.1 2005年5月の宛先(ポート種類)別アクセス数の比率】



【図 2.2.2 2005年5月の宛先(ポート種類)別発信元数の比率】

1433(TCP)

Microsoft SQL Server が使用するポートで、SQL インジェクション等による攻撃を行うために、攻撃先のコンピュータを探しているものと思われます。

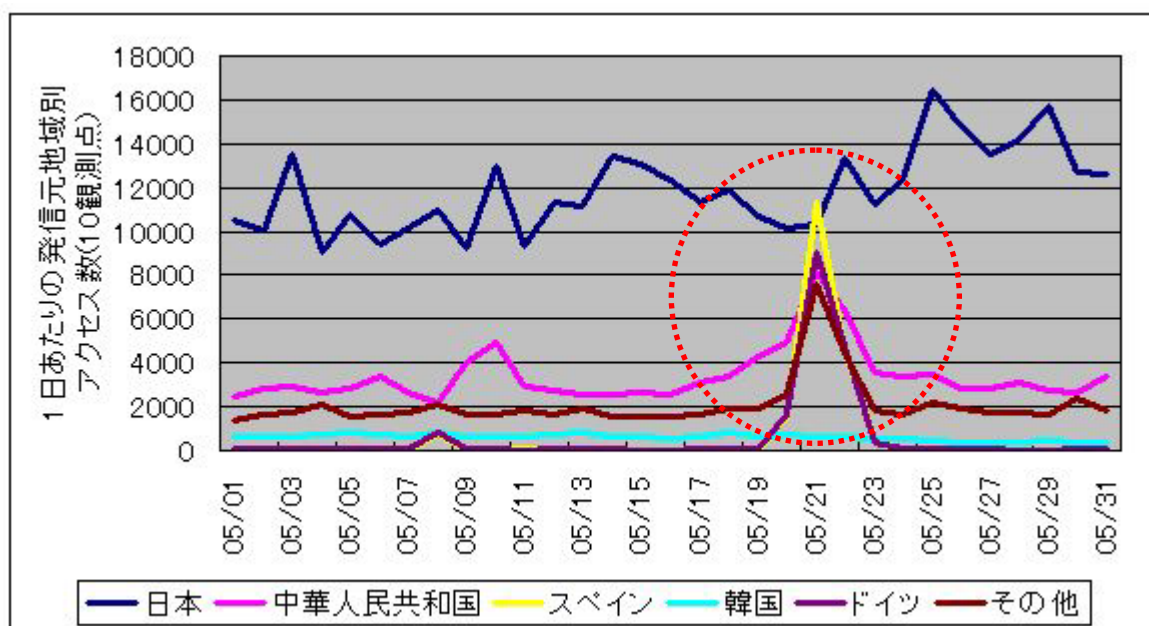
1026 および 1027(UDP)

Windows Messenger サービスを利用した spam 広告(ポップアップメッセージ)のアクセスです。

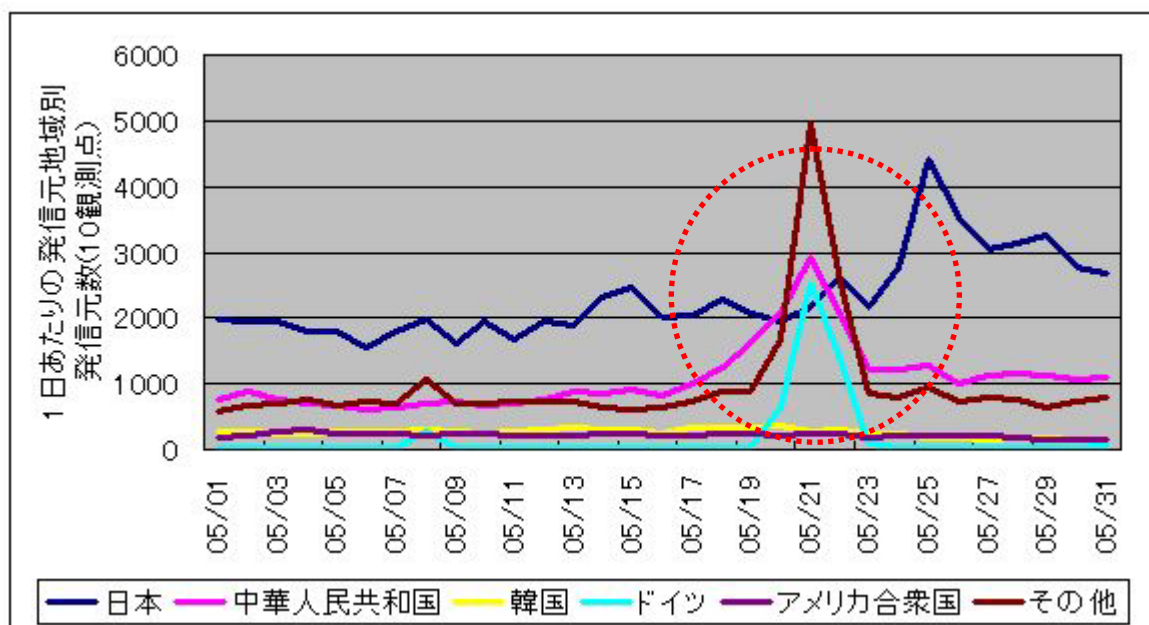
9966(TCP)

WinMX(ファイル交換ソフト)によるアクセスで、TALOT2 の観測点IPアドレスの変更にともない、変更後の IP アドレスが、以前このソフトの利用者に使用されていたために発生しているアクセスと思われます。

2.3 2005年5月の発信元地域別アクセス状況



【図 2.3.1 2005年5月の発信元地域別アクセス数の変化】

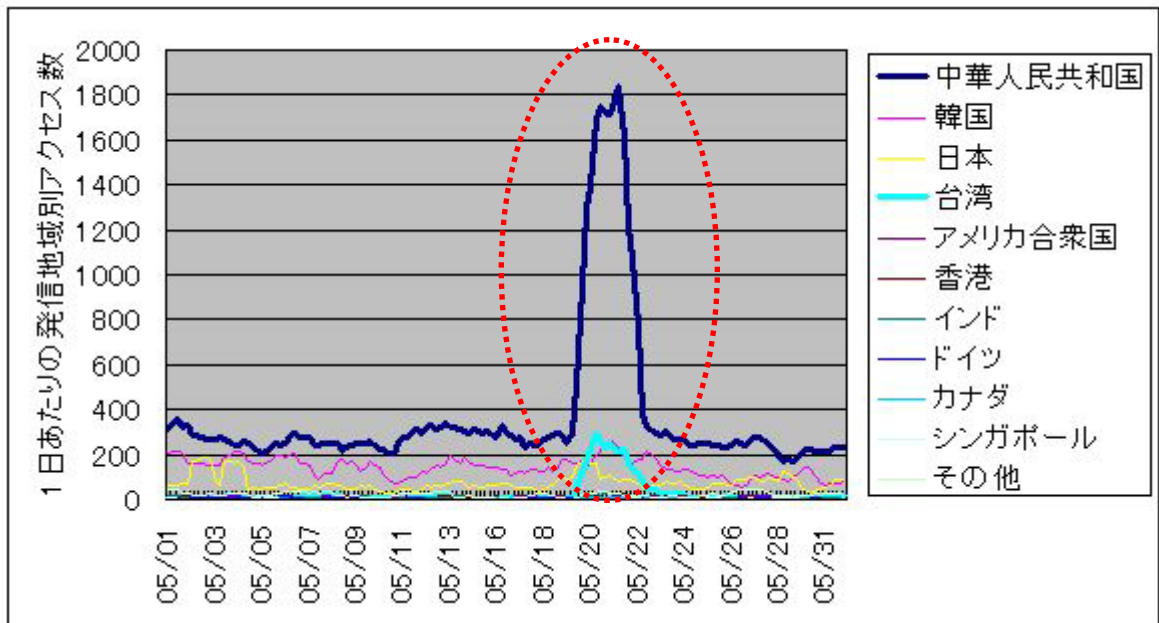


【図 2.3.2 2005年4月の発信元地域別発信元数の変化】

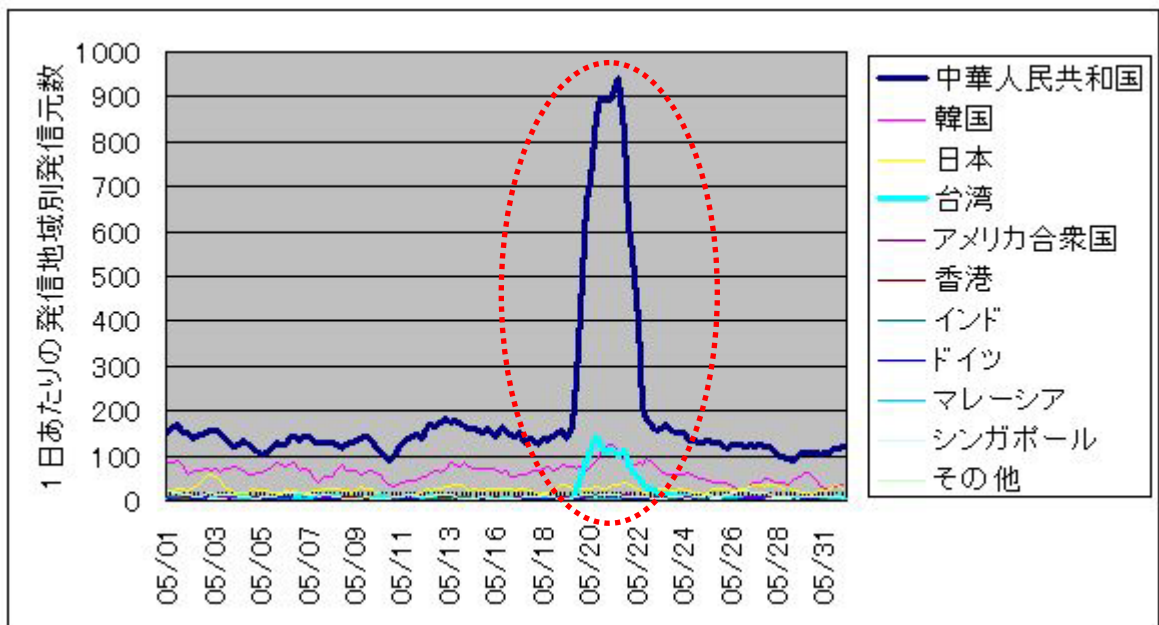
- 5月20日から22日にかけて、445(TCP)ポートへのアクセスが増加しました。このアクセスにより、この期間、欧州方面(スペイン、ドイツ、フランス等)および中国方面からのアクセス数および発信元数が増加したものです(「2.5 特定観測点における445(TCP)ポートへのアクセスについて」を参照下さい)。

2.4 1433(TCP)ポートへのアクセスについて

5月19日から21日にかけて、1433(TCP)ポートへのアクセスが増加しました。このアクセス増加については、IPA のもう 1 つの定点観測システム(TALOT)および国内の他機関による定点観測(JPCERT/CCのISDAS,@police等)でも観測されており、かなり広範囲で観測されているようです。



【図 2.4.1 1433(TCP)ポートへの発信地域別アクセス数の変化】

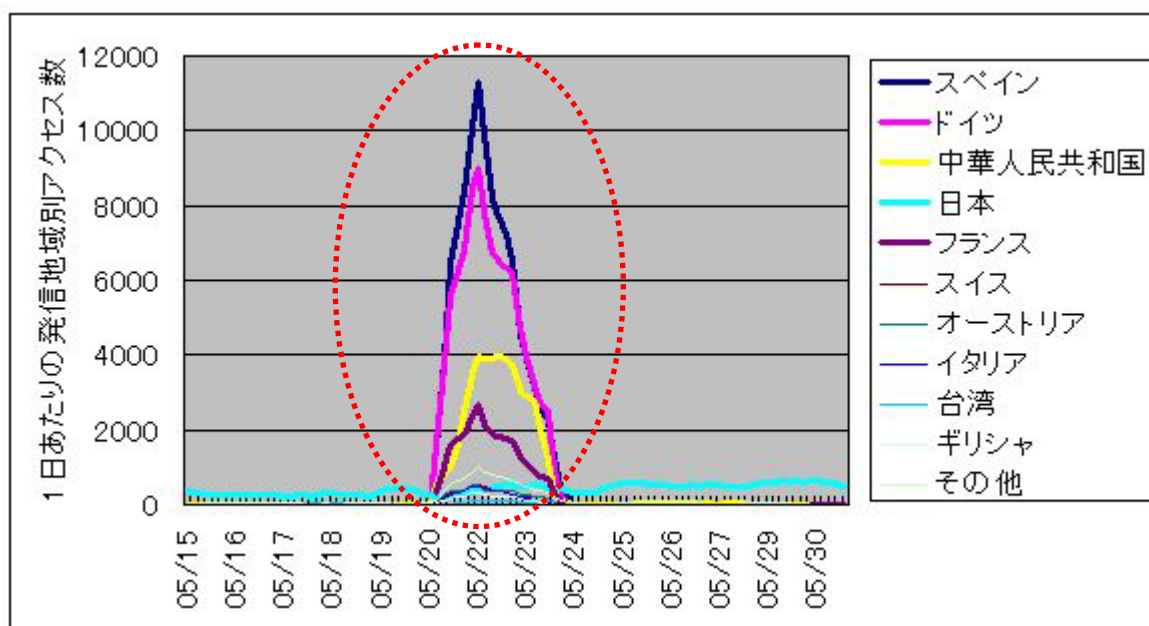


【図 2.4.2 1433(TCP)ポートへの発信地域別発信元数の変化】

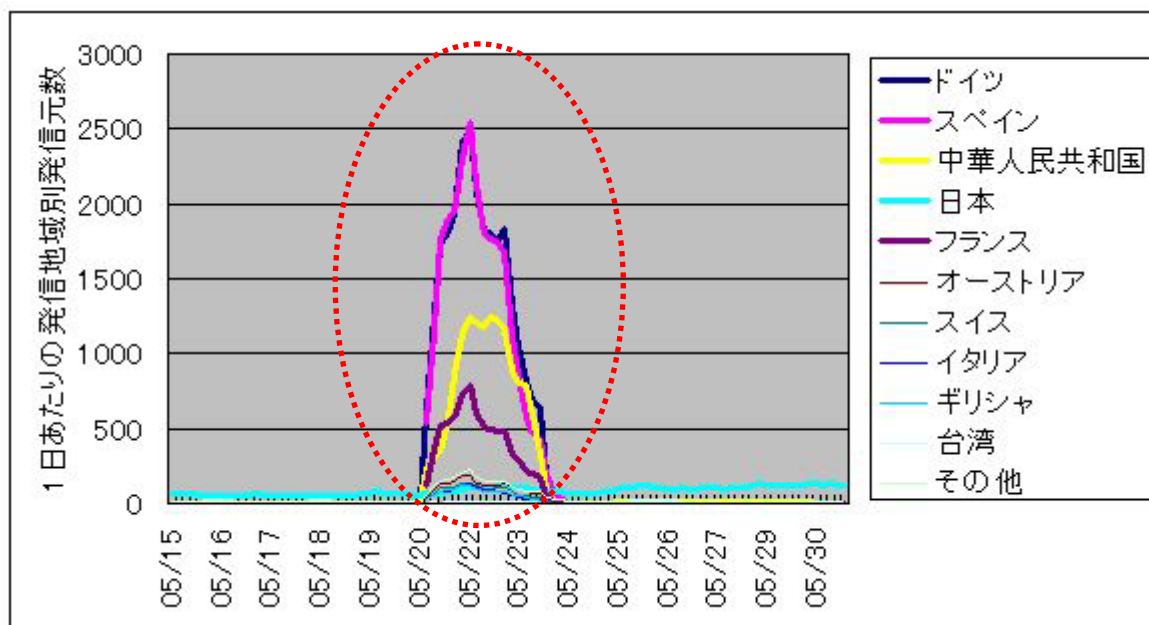
- 今回のアクセス増加の発信地域は、中国および台湾方面でした。他の発信地域からのアクセスは定常値(安定的にアクセスがきている状態)を示しています。
- 1433(TCP)ポートは、通常では Windows SQL Server が使用するポートであり、一般的に SQL サーバが動作している Windows サーバを探す目的で、このポートがスキャンされる場合が多いようです。
- 同一の発信元から、TALOT2 上の複数の観測点(観測点同士の因果関係なし)に対して、アクセスするものもあり、かなり広い範囲へのポートスキャンが行われていることが分かっています。
- 今回のアクセス増加を引き起こしているアクセスのうち、アクセス数の多い発信元からは、ソース(発信)ポート番号が 6000 で固定されているアクセスが多いようです。このことから、発信元の多くが同一種類のワームあるいはボットに感染している(同一の攻撃ツールを使用している)可能性が高いと考えられます。

2.5 特定観測点における 445(TCP)ポートへのアクセスについて

5月20日から22日にかけて、445(TCP)ポートへのアクセスが増加しました。定点観測としての観測データとしては、特定観測点のみでのアクセス集中なので、一般的なものとは思えません。しかしながら、集中的であること、特定の地域からのアクセスが多いことなど特徴的なので、ここに報告します。



【図 2.5.1 特定観測点における 445(TCP)ポートへの発信地域別アクセス数の変化】

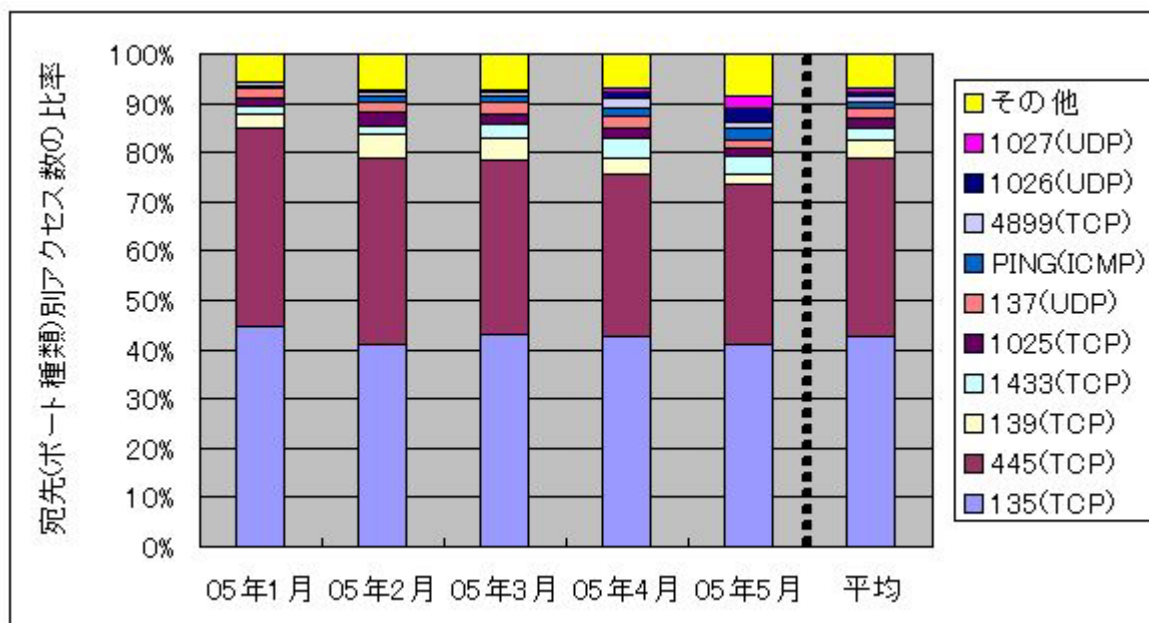


【図 2.5.2 特定観測点における 445(TCP)ポートへの発信地域別発信元数の変化】

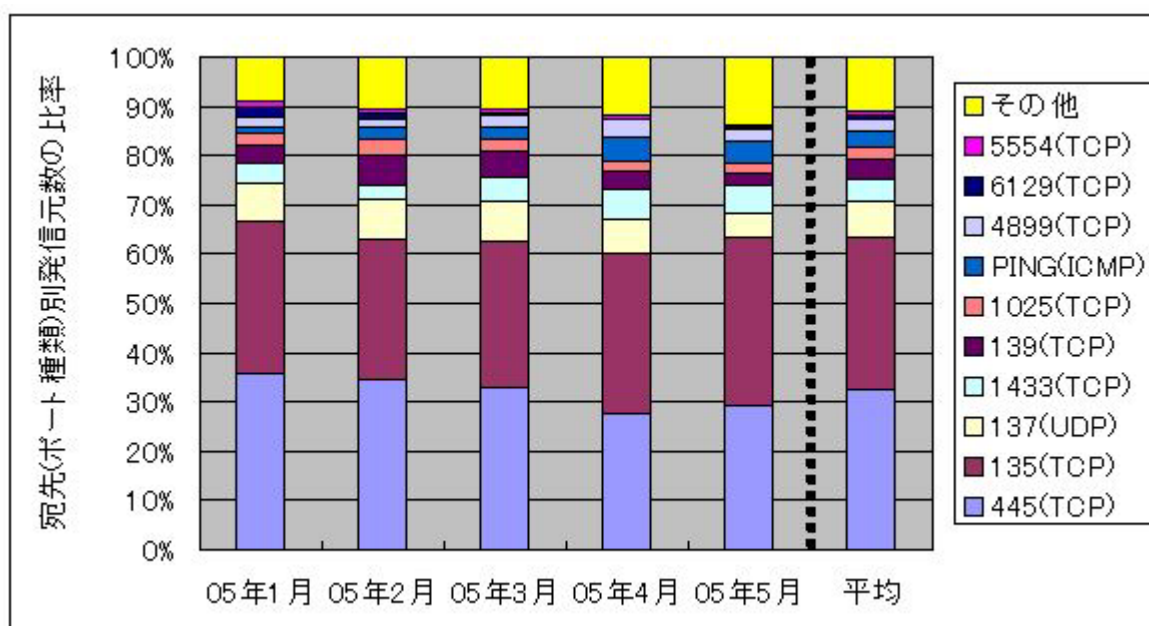
- 同一の発信元から 2 回ずつのアクセスが不定期に発信されているケースがほとんどで、最多アクセス数は同一発信元から 60 回以上を記録しています。
- 唐突に始まり、唐突に終わったと言う感じで、意図的な攻撃のようにも感じられますが、原因については不明です。このような集中的なアクセスは、まるで DDoS 攻撃のようです。
- 発信元 IP アドレスと観測点の IP アドレスについては、何の関連性(類似性)もないようです。

3. 統計情報

3.1 2005年1月～5月の宛先(ポート種類)別の比率

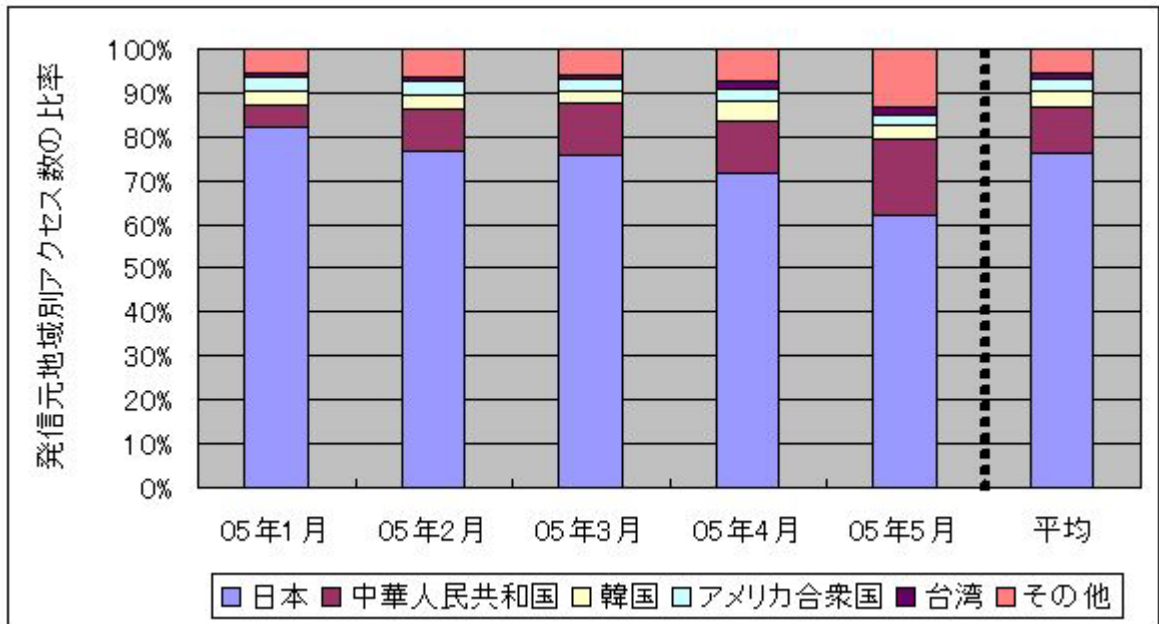


【図 3.1.1 2005年1月～5月の宛先(ポート種類)別アクセス数の比率】

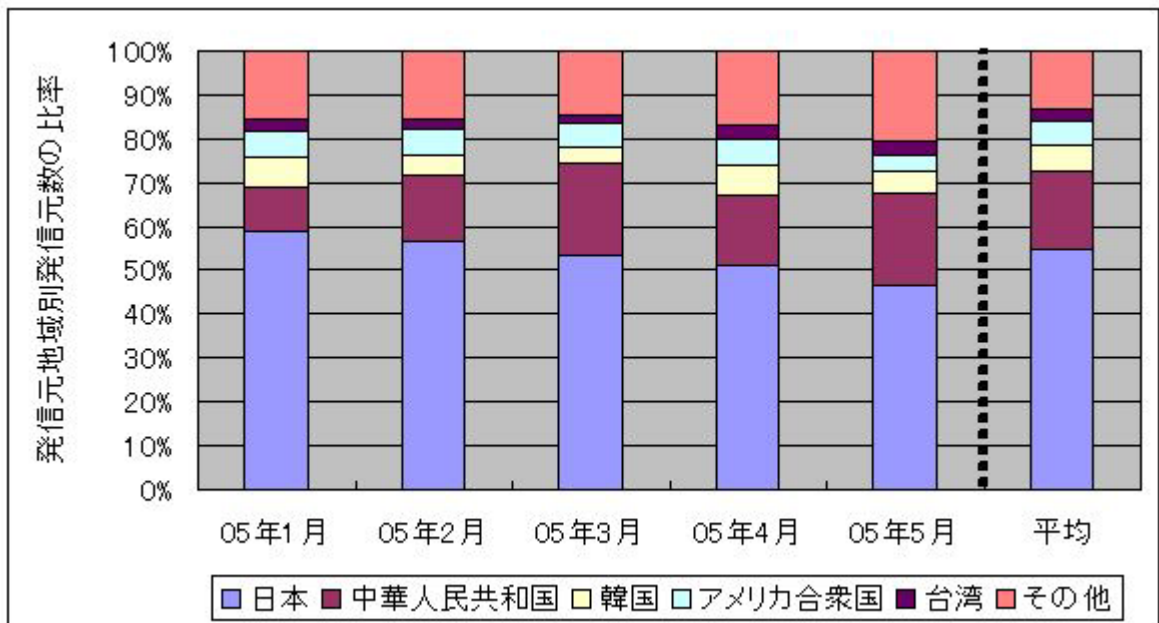


【図 3.1.2 2005年1月～5月の宛先(ポート種類)別発信元数の比率】

3.2 2005年1月～5月の発信元地域別の比率



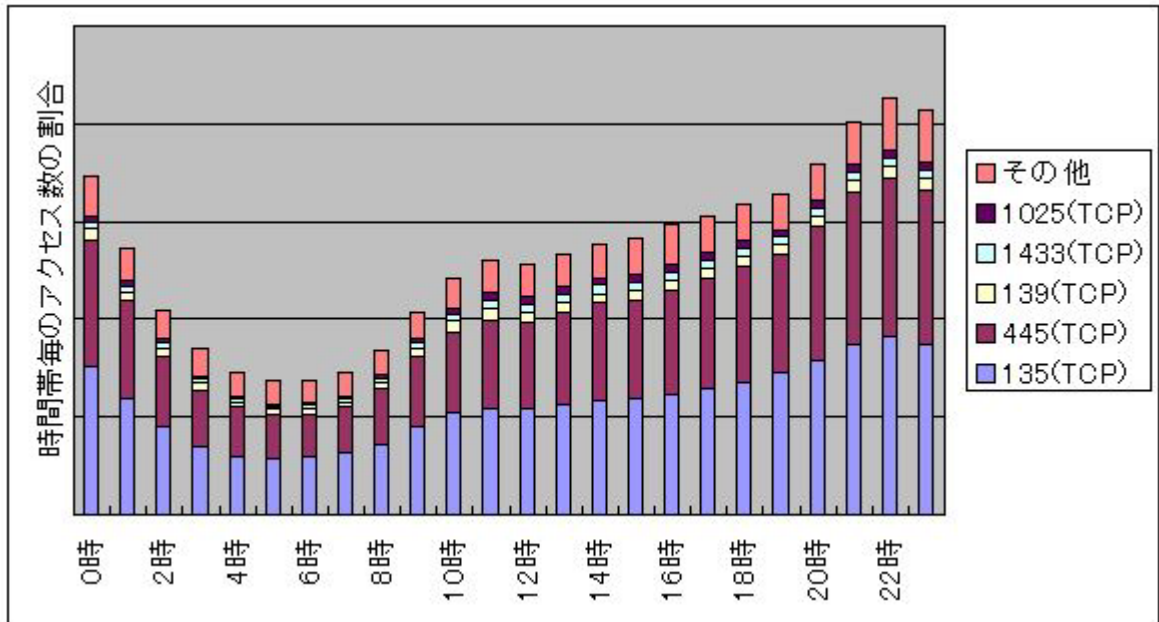
【図 3.2.1 2005年1月～5月の発信元地域別アクセス数の比率】



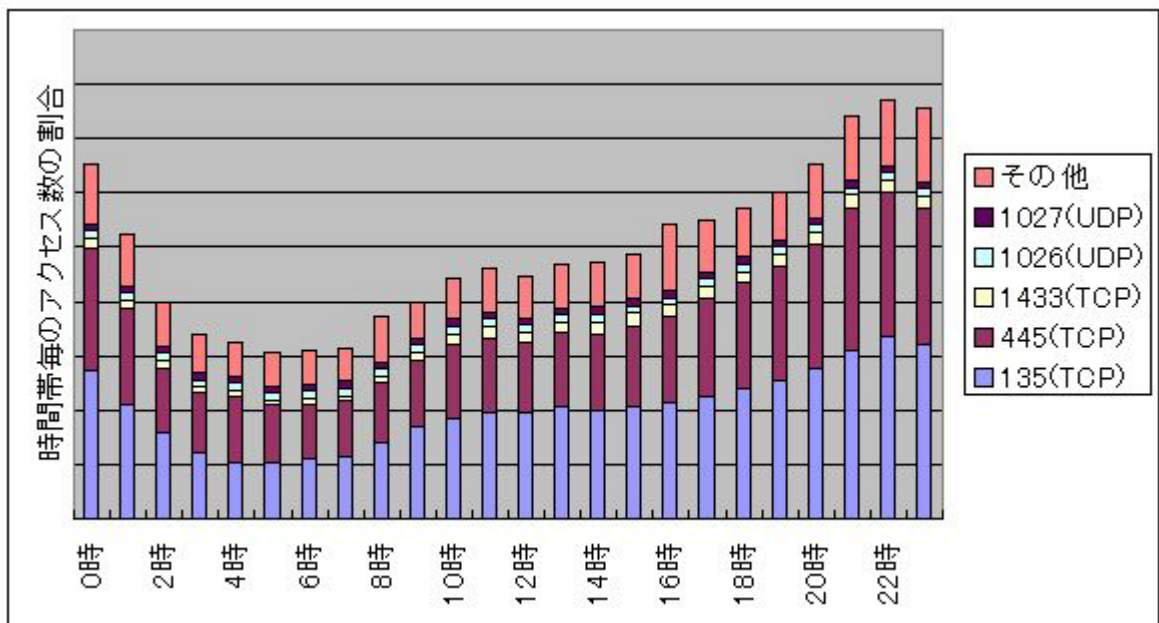
【図 3.2.2 2005年1月～5月の発信元地域別発信元数の比率】

4. その他の統計情報

4.1 2005年1月～5月の時間帯別統計



【図 4.1.1 2005年1月～5月の宛先(ポート種類)別アクセス数の時間帯別統計】



【図 4.1.2 2005年5月の時間帯別統計】

・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