# 情報技術解析平成１７年報

～平成１７年のインターネット治安情勢～

平成１８年３月

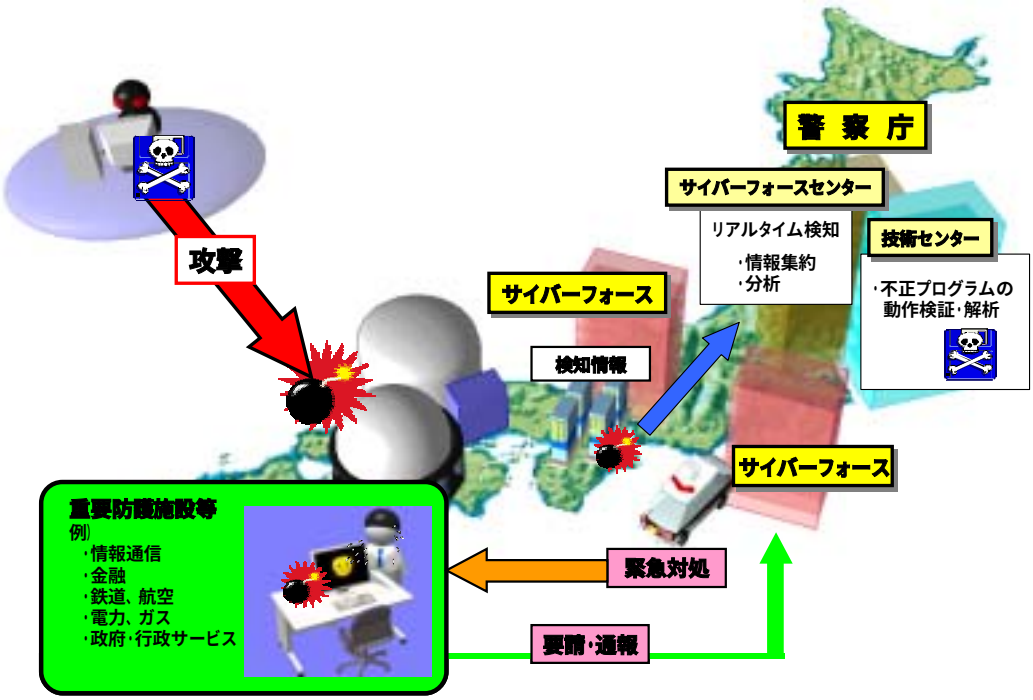
警察庁情報通信局情報技術解析課

## はじめに

インターネットや携帯電話に代表される情報通信技術の発展は、多くの人々に大きな利便をもたらしました。他方、犯罪の手段、方法にこうした技術が悪用され、新たな手口の犯罪を生み、被害の拡大・広域化を招いています。平成17 年中には、スパイウェアを用いた不正アクセス禁止法違反・電子計算機使用詐欺事件やファイル共有ソフトを介した重要情報の漏出事案等のほか、中央省庁等の Web サーバに対する大規模なサイバー攻撃も発生しました。

「情報技術解析平成 17 年報」では、まず第１章で、17 年中におけるインターネット上で発生した、治安に影響を及ぼす事象の特徴的動向を概観しました。第２章では、国内のみならず世界中から日本の警察施設に対して送られるアクセス（接続）動向を観測した「インターネット定点観測」システムによる分析結果を取りまとめました。第３章では、話題となった主なサイバー犯罪・攻撃例を紹介し、さらに第４章では、安全で安心なインターネット社会形成に向けての警察庁情報通信局情報技術解析課の幅広い取組みを紹介しています。

本年報は、技術的な視点から 17 年中のインターネットを中心とした治安情勢を分析したものです。安全で安心なインターネット社会への取組みの一助となれば幸甚です。



# 1　インターネット治安情勢

インターネットの利用が、企業のみならず一般家庭にも深く浸透している一方で、新しいウイルスやワーム、又はインターネットを利用した新しい犯罪手口も発生しています。特に、重要インフラのようなライフラインに攻撃を仕掛けられた場合には、国民生活に甚大な被害を生じるおそれがあります。このような被害を未然に防止し、あるいは被害の拡大防止を図るため、情報技術解析課では、全国の警察施設のインターネット接続点におけるアクセス状況の観測・分析結果、公開の情報等を元に、「インターネット治安情勢」＝「今、インターネットで起きていること」の把握と国民への周知に努めています。また、特異な状況を認知した場合は、警察庁セキュリティポータルサイト「@police[1]」を通じて、タイムリーに情報提供しています。

本章では、当課で把握した平成 17 年のインターネット治安情勢を概観します。

## 1.1 概況

■ ***総アクセス件数は減少したが、金銭目的の個人情報窃取など新たな脅威となる事案が発生***

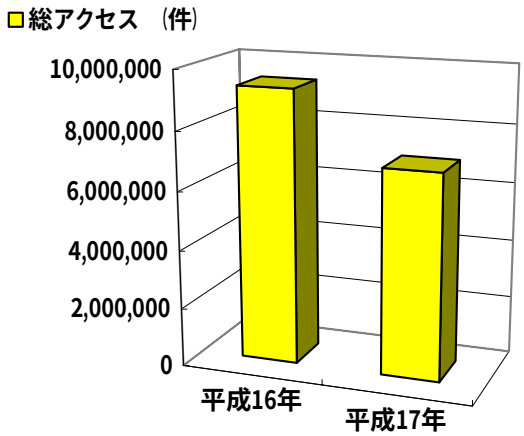



図 1.1 総アクセス件数の推移

図 1.1 は、全国の警察施設のインターネット接続点における総アクセス件数の推移です。昨年との比較では減少していますが、これは、検知しているアクセスのほとんどを占めているマイクロソフト社の Windows の欠陥をねらったワーム等の感染活動に伴うアクセスが減少したためです。アクセス件数減少の背景として、従来製品と比較してセキュリテ

[1] http://www.cyberpolice.go.jp/

ィに関する基本性能が高いバージョンの Windows が普及したことや、ウイルス対策ソフトウェア等の浸透によるものと推察されます。

しかし、ボットネットによる DoS 攻撃等の活動を多数認知するとともに、スパイウェアやフィッシングなどの新たなサイバー犯罪手法を用いた金銭目的の個人情報窃取事案や企業のコンピュータの中にある情報を不正に入手しようとする事案が発生するなど、新たな脅威となる事案が発生しました。

## 1.2 特徴

■ ***Windows の欠陥をねらったと思われるアクセスを年間を通して検知***[2]

図 1.2 は、Windows の欠陥をねらったと思われるアクセス件数の推移です。アクセスの状況からそのほとんどがワームによるものと推察されます。悪意のある者の命令に従ってサイバー攻撃等を行うボット系ワームの多くは Windows の欠陥をねらって感染を広げるため、これらのワームによるアクセスも多いものと思われます。

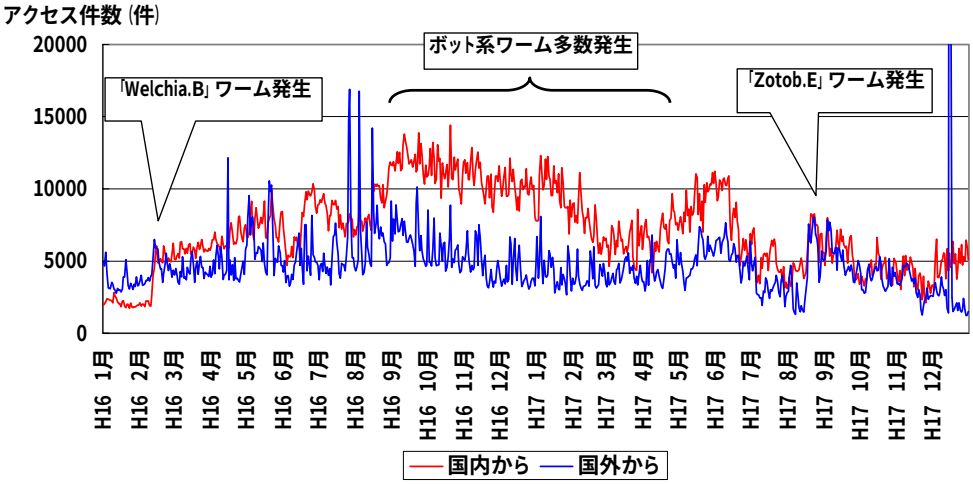



図 1.2 Windows の欠陥をねらったと思われるアクセス件数の推移

■ ***ワームに感染しているコンピュータが中国に多く存在***[3]

不特定多数のコンピュータに一方的に感染活動のためのデータを送りつける SQL Slammer ワームは、15 年 1 月の発生以来、中国国内で蔓延し続けているようです。また、ボット系ワームに感染したコンピュータ等によって構成されたボットネットに接続されているコンピュータも、

2 「2.2 ポート別アクセス状況」参照

3 「2.1.3 不正侵入検知システムによる検知状況」参照

中国国内で多く確認されています[4]。

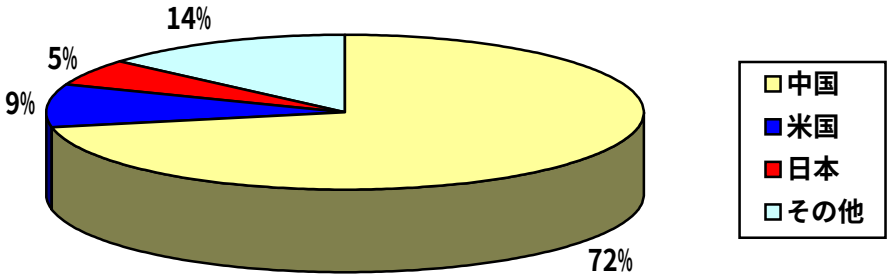



図 1.3 SQL Slammer ワームの国別検知状況

■ ***ボットネットによる DoS 攻撃等の攻撃活動を多数認知***[5]

ボットネット観測システムにおいて、ボットネットの様々な活動を観測しています。特に DoS（サービス不能）攻撃[6]を始めとした攻撃活動を数多く認知しています。

■ ***インターネット利用者から個人情報を窃取する事案が発生***

特定の企業名を騙って、スパイウェア[7]等の不正プログラムを送りつけたり、インターネット上にフィッシング[8]サイトを開設したりするなどの手口で、金銭獲得のためにインターネット利用者から個人情報を不正に入手しようとする事案が発生しました。

■ ***企業のコンピュータの中にある情報が標的に***

SQL インジェクション[9]等の手口を用いて、企業のコンピュータの中にある情報を書き換えたり、不正に入手しようとする事案が発生しました。

■ ***新種の不正プログラムは大規模感染から金銭目的の小規模感染へ***

総アクセス件数が減少しているにも関わらず、当課における新種不正プログラム（ワーム等）認知件数（図 1.4）は増加しています。これは、ワーム等の作成者が、大規模、無差別の単発的感染活動ではなく、金銭

---

4 「2.3.1 ボットネットの国／地域別比率」参照
5 「2.3.2 攻撃命令の手法別件数」参照
6 「3.1 DoS 攻撃」参照
7 「3.2 スパイウェア」参照
8 「3.3 フィッシング」参照
9 「3.4 SQL インジェクション」参照

等を目的として標的を絞り込んだ、比較的小規模ながら反復的な感染活動を指向している状況がうかがえます。

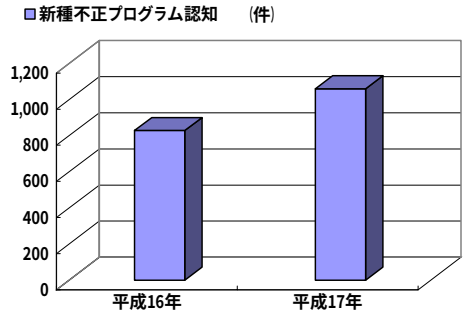



図 1.4 新種不正プログラム認知件数の推移

## 1.3 情報セキュリティ対策向上のために

17 年は、Windows を標的としたウイルスやワームが数多く発生・蔓延するとともに、数年前に欧米で発生したサイバー犯罪の手口が日本に上陸するなど、企業におけるサーバ等の管理者ばかりでなく、一般のインターネット利用者にとっても新たな脅威となる事象が発生しました。

しかしながらこれらの事象は、一般家庭においては、ウイルス対策ソフトウェアの導入及びパターンファイルの継続的な更新、セキュリティ修正プログラムの適用、不審な Web サイトを閲覧しないなどの基本的なセキュリティ対策を確実に実施していくことで、被害のほとんどを防ぐことが可能なのです。

また、企業においては、企業自身を守るための対策に加えて、顧客等に被害を及ぼさないためにも、Web アプリケーションの堅牢化、システムのアクセス権限の設定、通信記録の定期的な確認といった対策を継続的に行うことが重要です。

当課では、今後とも、この種情報を積極的に広く国民の皆様に提供し、安全で安心なインターネット社会の確立に努めてまいります。

# 2　インターネット定点観測結果の分析

## 2.1 アクセス状況の分析

この分析結果は、全国 57 か所の警察施設のインターネット回線に設置されたファイアウォール及び不正侵入検知システムに対するアクセスを分析したものです。これらが設置されているインターネット回線は、警察が保有していることを公表していませんので、一般家庭においてインターネットに接続しているコンピュータも、ほぼ同じ傾向のアクセスを受けているものと思われます。

設置されているファイアウォールは、インターネット側からのアクセスを全て遮断しており、その状況を定期的に集計するよう設定されています。

不正侵入検知システムは、インターネット側からの有害なアクセスを検知するように設定されていますが、インターネット上で発生する事象のうちの一部分しか検知できませんので、検知結果は必ずしも全体の情勢を反映したものではありません。

### 2.1.1　検知件数の推移

図 2.1 に、平成 16 年 1 月以降の、半年毎の検知件数の推移を示します。

ファイアウォールに対するアクセス件数は減少傾向にあり、17 年下半期は、16 年下半期と比較して約 35%減少しています。

一方、不正侵入検知システムの検知件数は徐々に増加しており、17 年下半期は、16 年下半期と比較して約 81%増加しています。

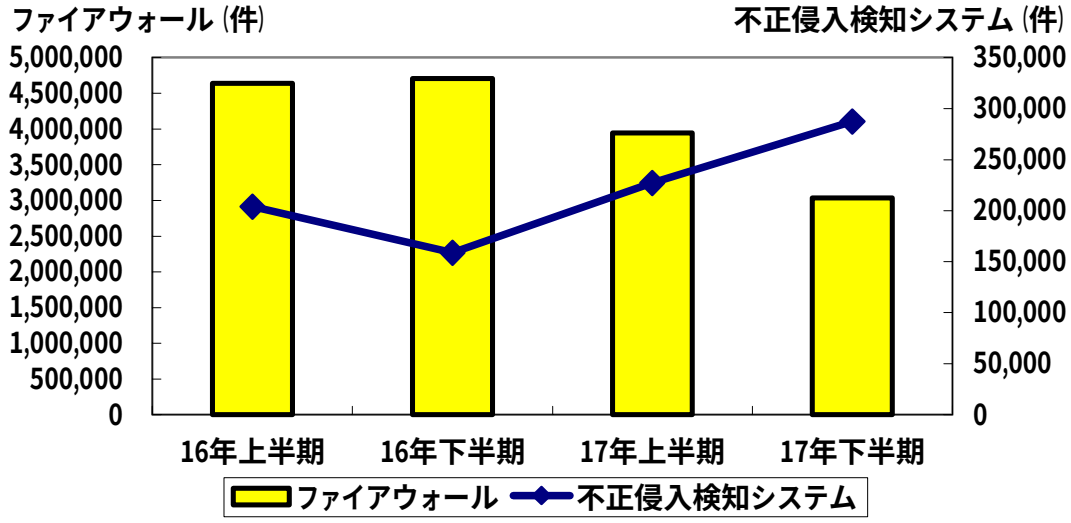



図 2.1 半年毎の検知件数推移

### 2.1.2 国／地域別のアクセス状況

図 2.2 に示すように、17 年における国／地域別のアクセス状況は、国内を始めとする東アジアの国／地域からのアクセスが多くなっています。この要因の一つとして、ウイルスやワームの感染活動の影響が挙げられます。感染活動においては、感染しているコンピュータの IP アドレスと第一及び第二オクテットが同一の IP アドレスへ接続を試みる場合が多いため、同じアジア地域に属し、IP アドレスの割当て領域が近接している国内、中国、韓国等からのアクセスが占める割合が多くなっていると思われます。

17 年は、国内からのアクセスが約 38%を占め、次いで中国の約 20%、韓国の約 12%となっています。16 年と比較すると、国内、韓国、米国及び台湾からのアクセスはいずれも減少していますが、中国からのアクセスは増加しています。そのため、相対的に中国からのアクセスの占める割合が大幅に増加しています。

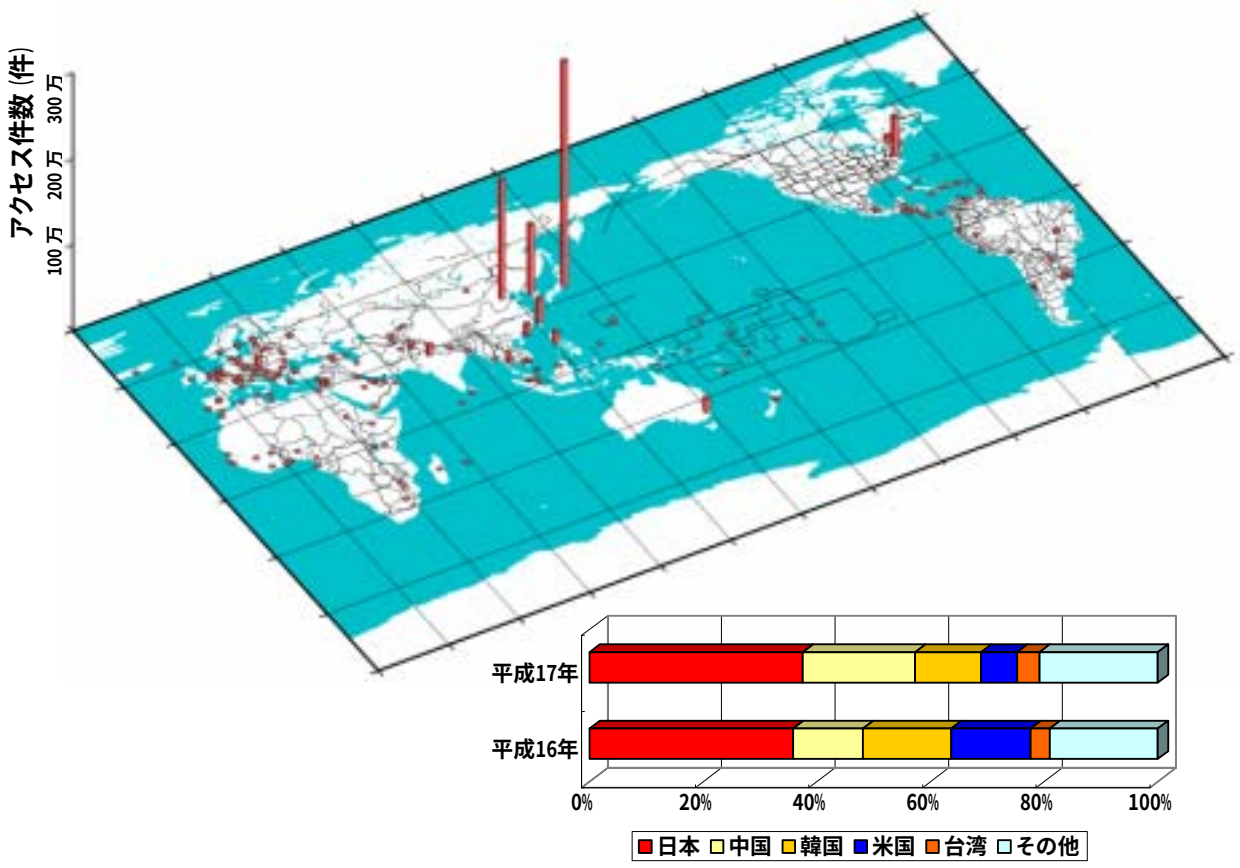



図 2.2 国／地域別のアクセス状況

### 2.1.3 不正侵入検知システムによる検知状況

図 2.3 に、不正侵入検知システムで１年間に検知されたアラートの、攻撃手法別検知比率を示します。

17 年に検知されたアラートでは、「Worm」(SQL Slammer ワーム)が約 92%、「Scan」が約６％と上位２つが全体の約 98%を占めています。

16 年と同様に、SQL Slammer ワーム以外では、サイトに侵入するための準備段階の攻撃に関連するアラートが中心となっており、サーバ等に対する脆弱性を悪用した直接的な攻撃等は約２％以下に留まっています。これは、当システムが設置されているネットワークには、サーバ等の攻撃対象になる可能性のある機器が一切接続されていないためと推察されます。

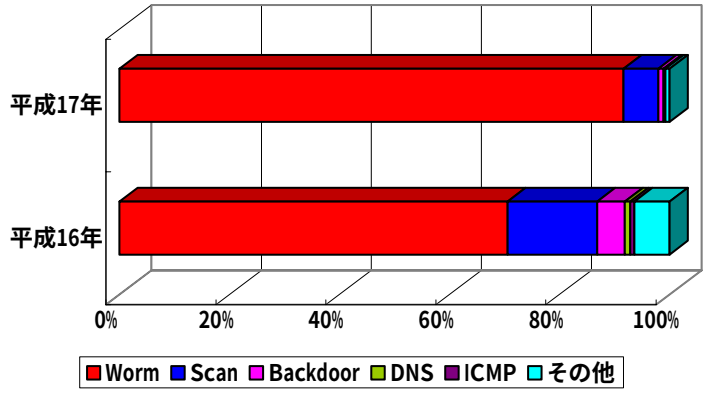



図 2.3 攻撃手法別検知比率

図 2.4 に、17 年におけるアラート検知状況、図 2.5 に、発信の多い国／地域からの「Worm」検知件数の推移を示します。

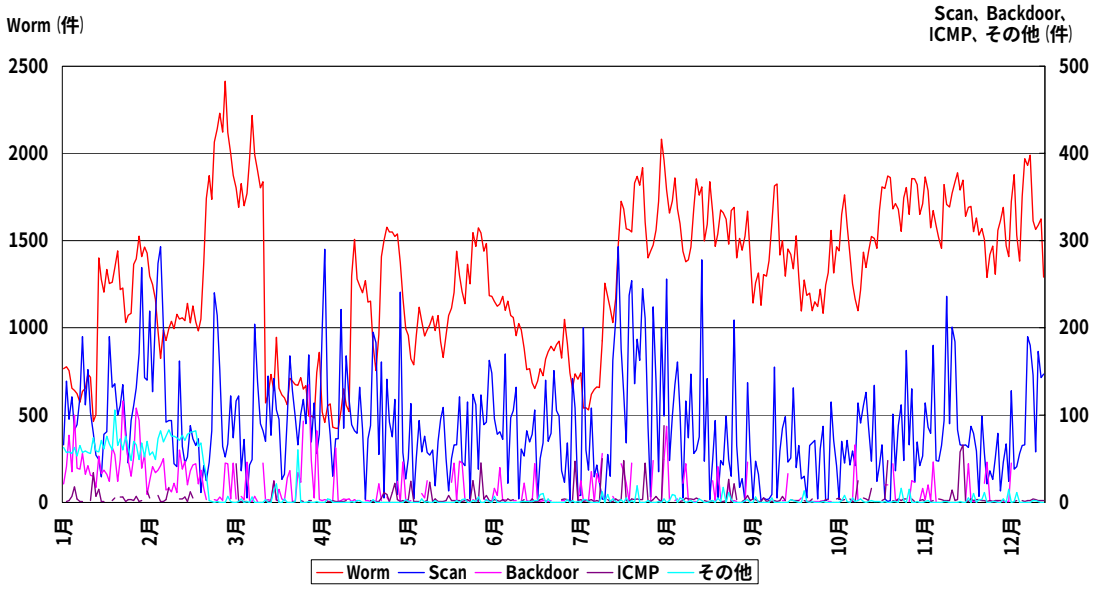



図 2.4 年間のアラート検知状況

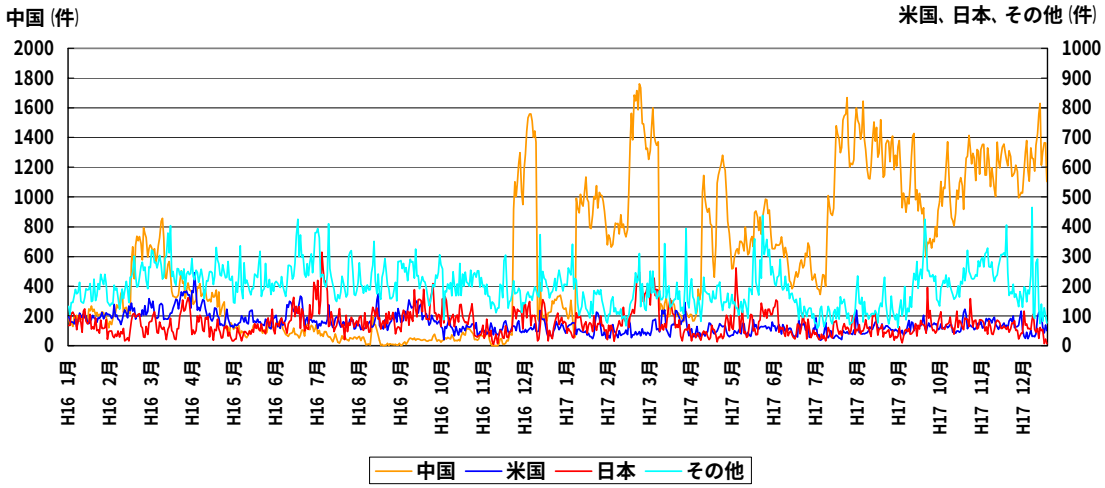



図 2.5 発信の多い国／地域からの「Worm」検知件数推移

16 年 11 月頃から、中国を発信元とするアラートが増加し、以降高い数値で推移しています。

SQL Slammer ワームの発生は 15 年 1 月[10]ですが、いまだに多く検知されています。これは、セキュリティ対策が施されていないサーバが、多数インターネットに接続されていることが原因と思われます。また、セキュリティ修正プログラムが適用されていないサーバソフトウェアが、海賊版として出回っており、これが利用されていることも要因と考えられます[11]。

[10] 新型ワーム（Slammer）に関する対策について
http://www.cyberpolice.go.jp/important/20030226_133843.html

[11] 中国は「海賊版」から逃れられるか（1/2）
http://plusd.itmedia.co.jp/pcupdate/articles/0504/18/news011.html

## 2.2 ポート別アクセス状況

アクセス状況をポート別に分析することにより、全インターネット規模での新種のワームや攻撃手法の出現等の特異な事象について、早期に把握することが可能となります。

### 2.2.1 TCP ポートに対するアクセス状況

図 2.6 に、17 年における TCP 宛先ポート別のアクセス件数推移の全体像を示します[12]。個々のポートを対象とした詳細な分析につきましては、次項をご覧下さい。

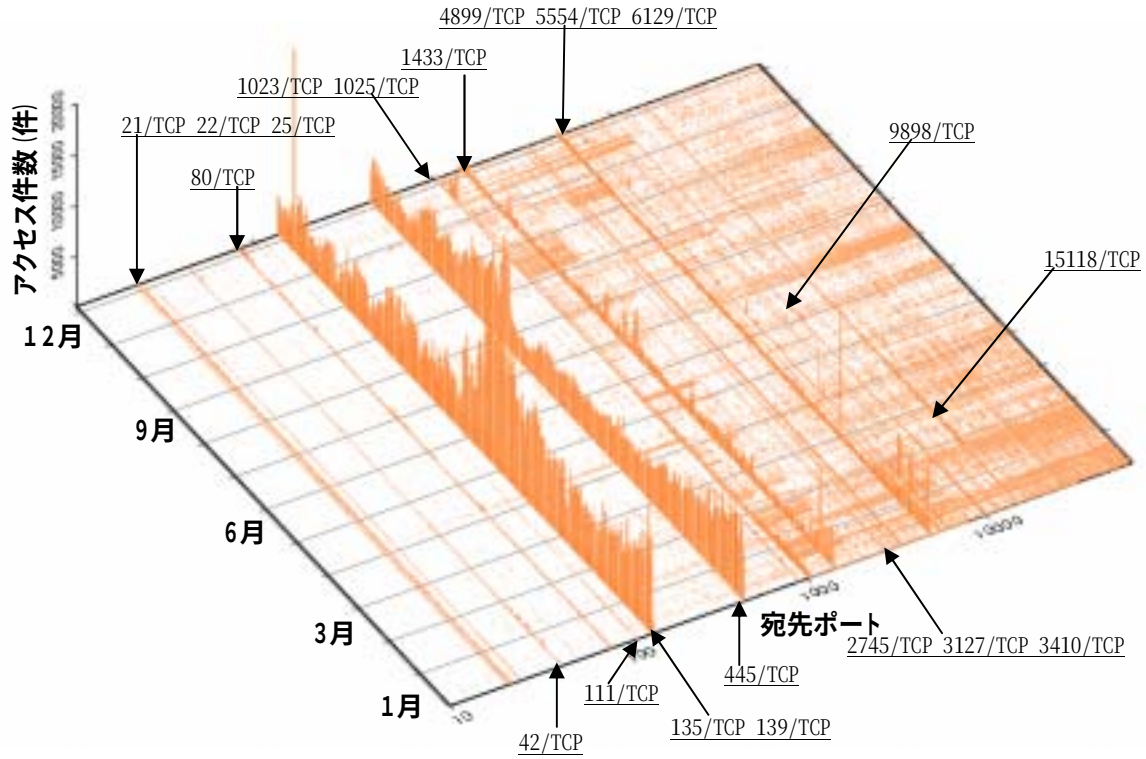



図 2.6 宛先ポート別アクセス件数の推移

### 2.2.2 TCP 各ポートの状況

図 2.7 に 135/TCP ポート、図 2.8 に 445/TCP ポートに対するアクセス件数の推移を示します。

これらのポートは、Welchia[13]を始め、数多くのワームで使用されています。

---

[12] 0/TCP～9/TCP ポートについては、ほとんど観測されていないため、省略しました。また、グラフを見やすくするため、アクセス数の最大値を 20,000 件としています。

[13] Welchia.B (NACHI.B) ワームの概要について

17 年においても、ワーム等の感染活動によると推察されるアクセスが数多く観測されました。

12 月 15 日及び 16 日には、135/TCP ポートに対する大量のアクセスが観測されました[14]。発信国／地域は、ポーランドが大半を占めており、次いでトルコ、中国の順でした。このアクセスは、特定のネットワークアドレス範囲に対して行われていることから、ボット系ワームの活動に起因し、感染の拡大をねらった活動であると推察されます。

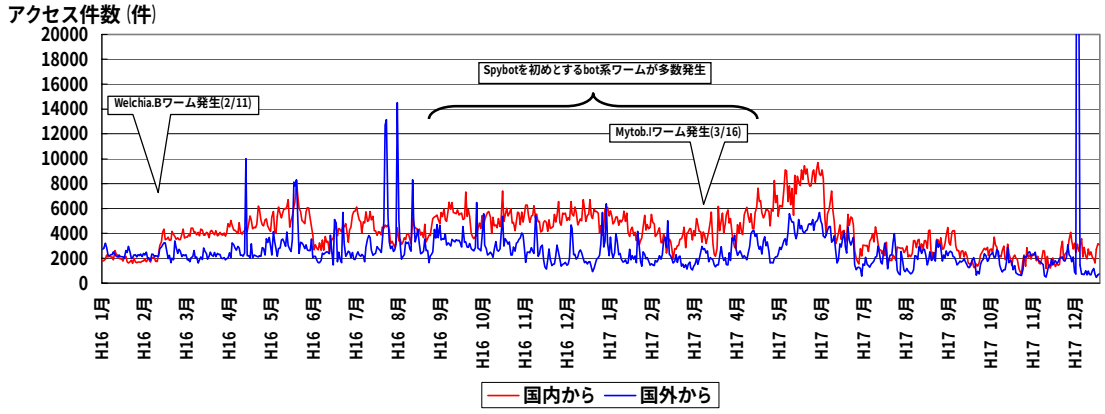



図 2.7 135/TCP ポートに対するアクセス件数の推移

17 年における 445/TCP ポートに対するアクセスは、16 年と比較すると減少しています。しかし、依然として多くのワームが感染の拡大手段として使用していることから、今後も動向に注意が必要です。

17 年 8 月 15 日以降、国内、国外いずれもアクセス件数が増加していますが、これはマイクロソフト社が 8 月 10 日に公表した、Windows プラグアンドプレイの脆弱性（MS05-039）を悪用する Zotob ワーム[15]及びその亜種[16]に起因するものと考えられます。

---

http://www.cyberpolice.go.jp/important/20040213_223241.html

[14] 12 月 15 日及び 16 日以外の推移を見やすくするため、グラフ縦軸の最大値を 20,000/日としています。

[15] Microsoft Windows の脆弱性（MS05-039）を悪用して感染するワームについて
http://www.cyberpolice.go.jp/important/2005/20050817_194602.html

[16] W32.Zotob.E ワームの解析結果について
http://www.cyberpolice.go.jp/important/2005/20050819_221211.html

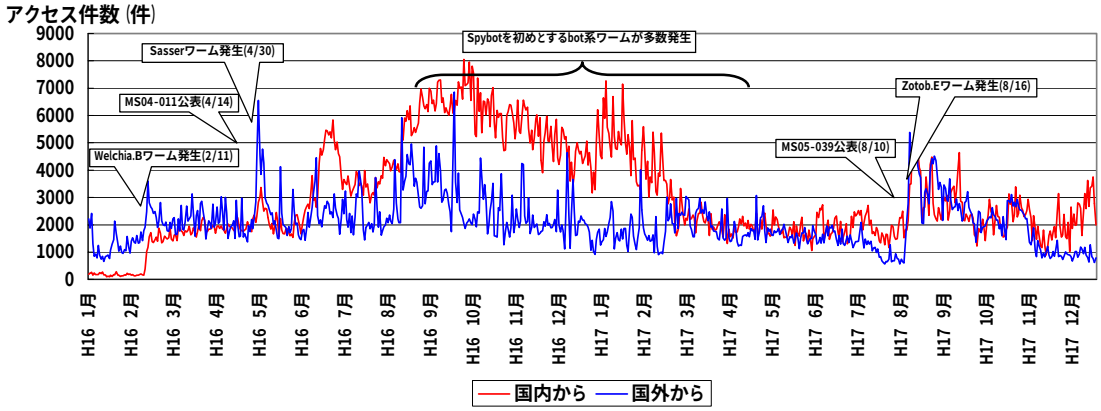



図 2.8 445/TCP ポートに対するアクセス件数の推移

図 2.9 に、1025/TCP ポートに対するアクセス件数の推移を示します。

135/TCP ポートや 445/TCP ポートと比較すると少数ですが、12 月 9 日から 18 日にかけて 1025/TCP ポートが急増しました[17]。これは、10 月 12 日にマイクロソフト社から発表された脆弱性「MSDTC および COM+ の脆弱性により、リモートでコードが実行される（MS05-051）」をねらったワーム等による大規模な感染活動と考えられます。

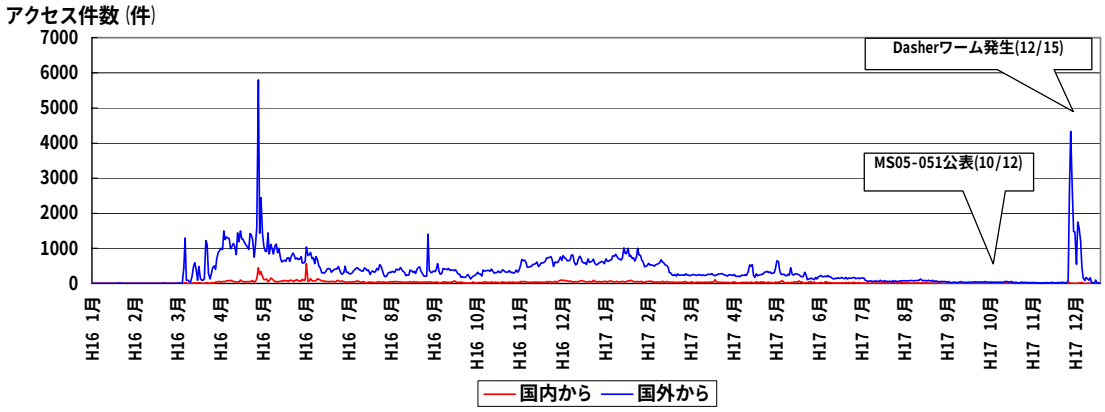



図 2.9 1025/TCP ポートに対するアクセス件数の推移

[17] TCP1025 番ポートに対するアクセスの増加について
http://www.cyberpolice.go.jp/important/2005/20051209_184920.html

### 2.2.3 UDP ポートに対するアクセス状況

図 2.10 に、17 年における UDP 宛先ポート別のアクセス件数推移の全体像を示します[18]。個々のポートを対象とした詳細な分析につきましては、次項をご覧下さい。

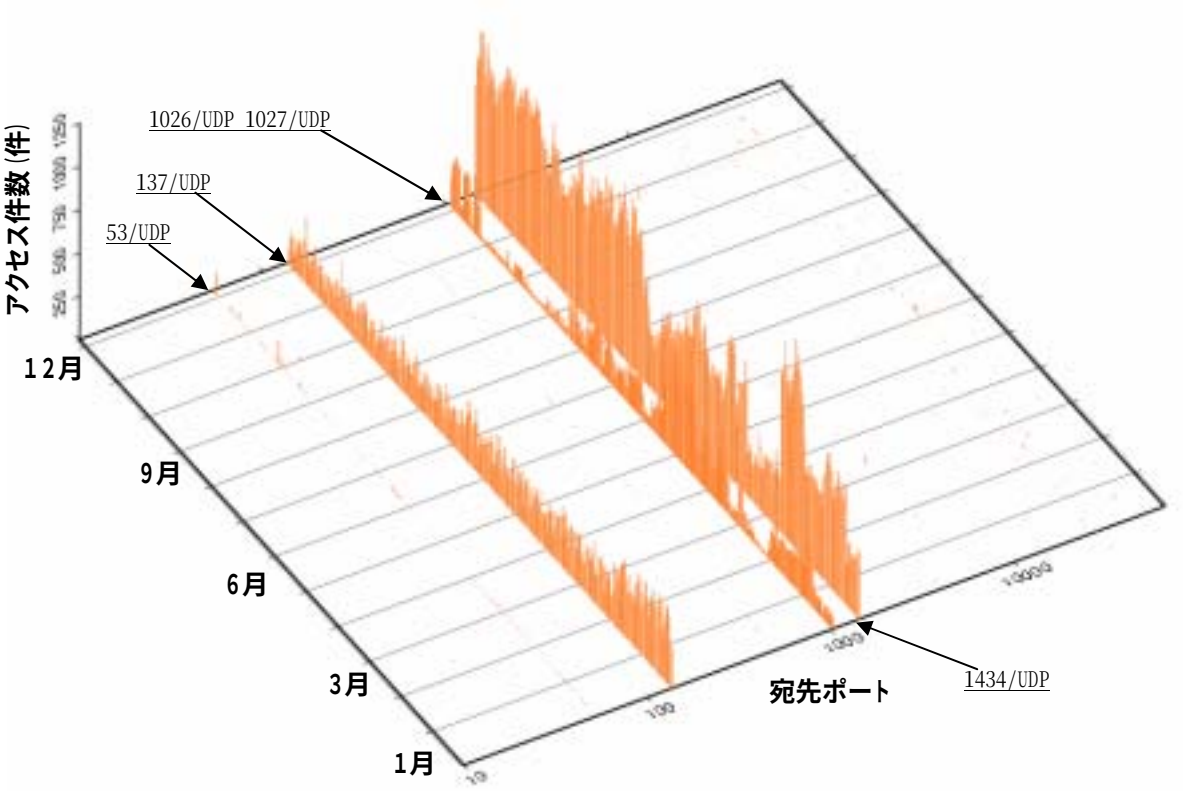



図 2.10 宛先ポート別アクセス件数の推移

### 2.2.4 UDP 各ポートの状況

図 2.11 に、1026/UDP ポート及び 1027/UDP ポートに対するアクセス件数の推移を示します。

これらはマイクロソフト社の Messenger Service が使用しているポートですが、アクセスの多くはこのサービスを使用したスパムとみられ、４月から６月にかけて、アクセス数の増加が顕著でした。なお、同様のアクセス増加は、16 年の３月から６月にかけても観測されています[19]。

---

[18] 0/UDP～9/UDP ポートについては、ほとんど観測されていないため、省略しました。

[19] UDP1026,1027 番ポートに対するトラフィックの増加について
http://www.cyberpolice.go.jp/important/20040318_182007.html

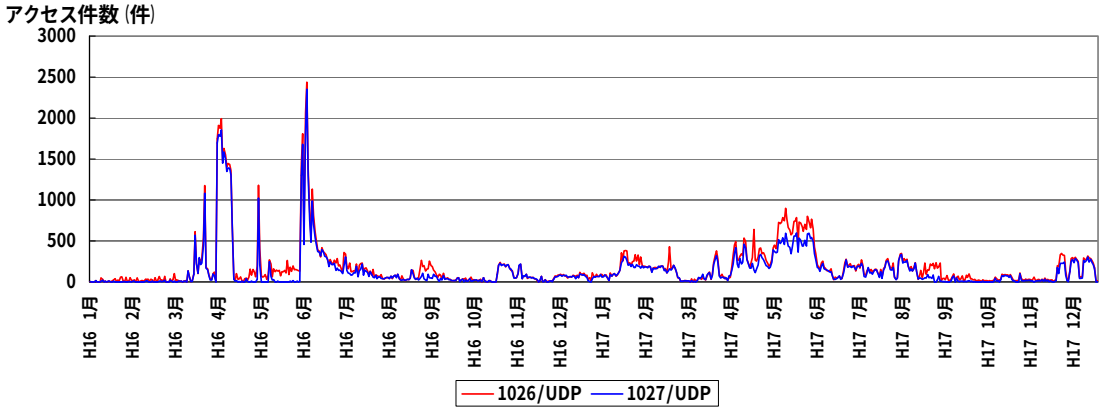



図 2.11 1026/UDP ポート及び 1027/UDP ポートに対するアクセス件数の推移

また、図 2.12 に 1026/UDP ポート、図 2.13 に 1027/UDP ポートに対する 17 年中のアクセスの国／地域別比率をそれぞれ示します。

前者は、中国が約 75%、米国が約 18%、後者は、中国が約 79%、米国が約 17%であり、ほとんどを上位２か国が占めています。このことから、主にこの２か国が、Messenger Service を利用したスパムの発信元となっていると推察されます。

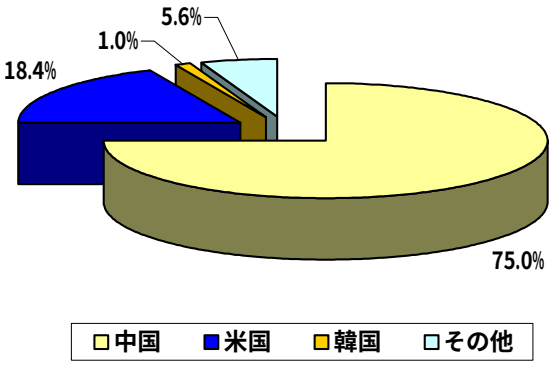



図 2.12 1026/UDP ポートの国／地域別比率

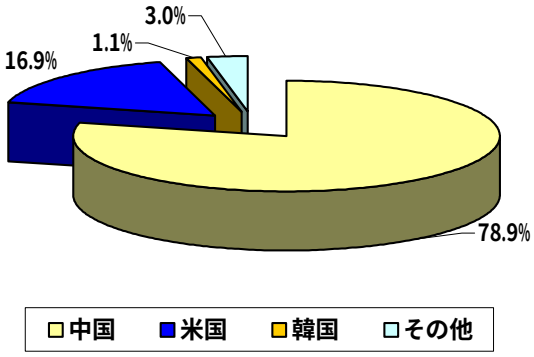



図 2.13 1027/UDP ポートの国／地域別比率

### 2.2.5 時間帯別アクセス状況

図 2.14 に、17 年に国内からのアクセスが多かった上位５ポートに対する時間帯別アクセス数を標準化[20]したグラフを示します。

1433/TCP ポートに対するアクセスは 12 時から 17 時頃が若干多くなっているものの、全体的に類似した傾向を示しています。19 時頃からアクセスが増加し、21 時から 22 時頃にピークに達しています。

このアクセス状況は、インターネットを利用している一般利用者と同じ傾向[21]であることから、一般家庭の多くのコンピュータがウイルスやワームに感染しているのではないかと推察されます。

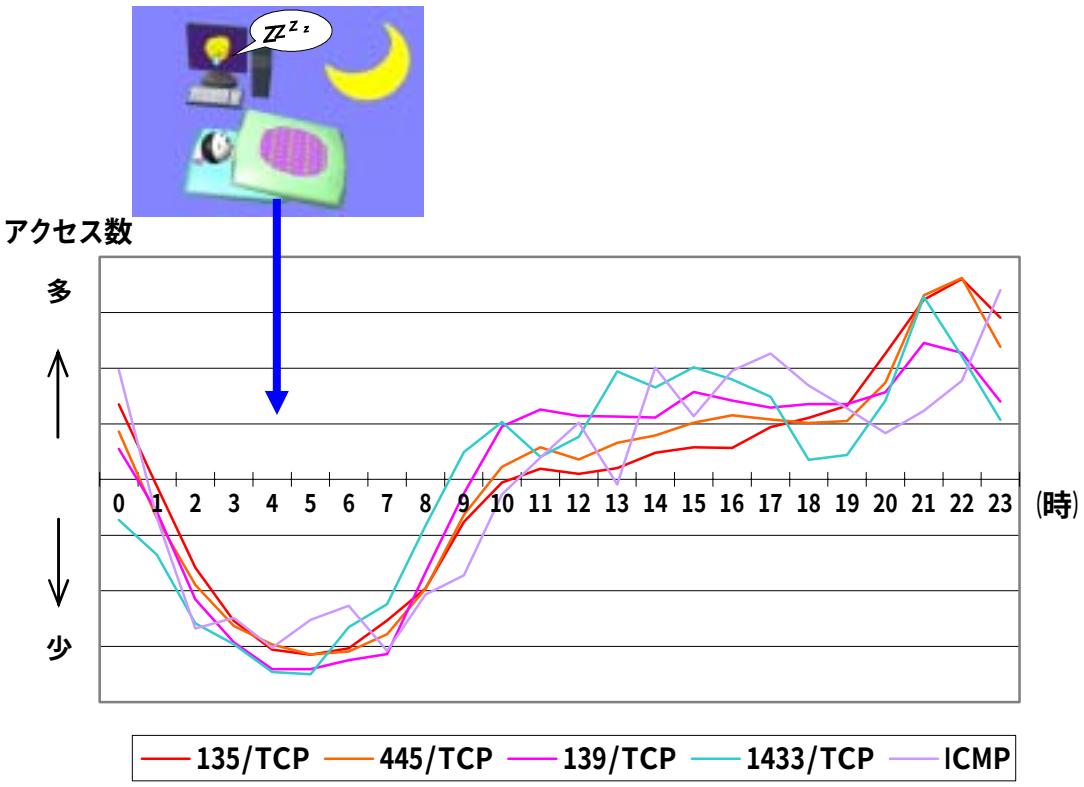



図 2.14 上位５ポートに対する時間帯別アクセス数（国内）

[20] 標準化 ＝ （各時間帯のアクセス数－平均値）／標準偏差

[21] 2005 年「ブロードバンド環境下における視聴行動」 Web 広告研究会
http://www.wab.ne.jp/pdf/20051031.pdf

## 2.3 ボットネットの観測結果

この分析結果は、17 年１月に運用を開始した「ボットネット観測システム」の観測結果を分析したものです。

### 2.3.1 ボットの国／地域別比率

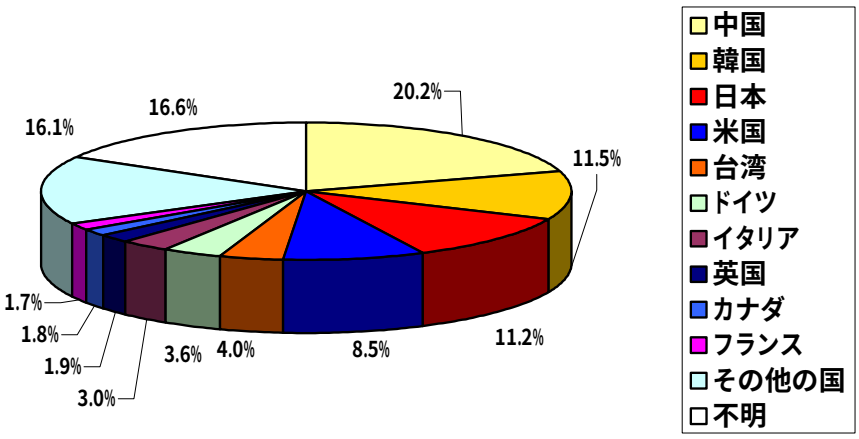



図 2.15 ボットの国／地域別比率

図 2.15 は、17 年に観測しているボットネットに接続されたコンピュータ（ボット）の国／地域別の比率です。ボットに感染したと推定される IP アドレスは約 130 万アドレス存在し、そのうち国内に所在すると推定されるものは約 15 万アドレスでした。このように、国内でも数多くのボットに感染したコンピュータが存在していると考えられます。また、上位には日本を含め東アジアの国／地域が非常に多く、中国、韓国、日本を合わせると全体の４割に達しています。

### 2.3.2 攻撃命令の手法別件数

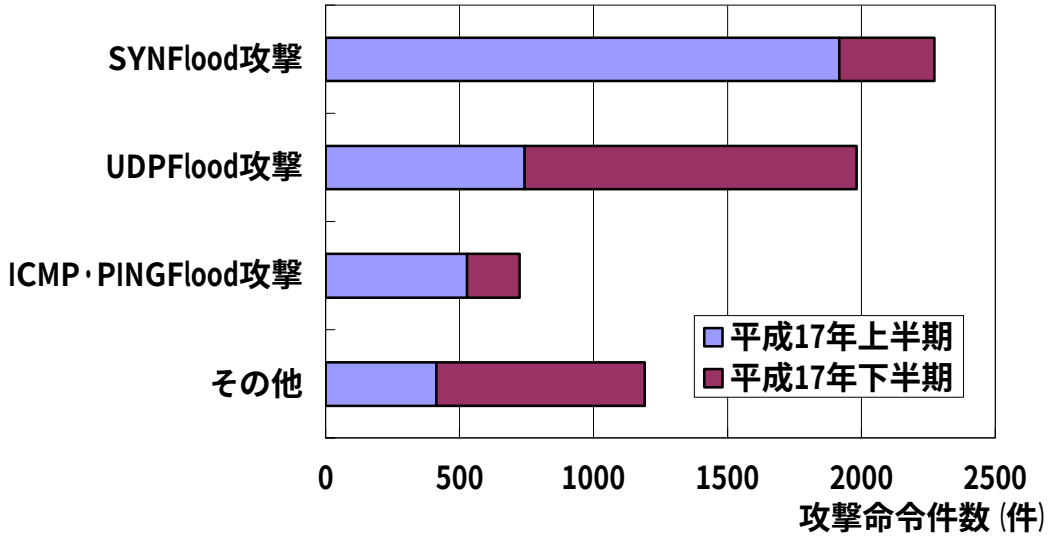



図 2.16 攻撃命令の手法別件数

図 2.16 は、ボットネット観測システムで観測された、攻撃命令の手法別件数です。SYNFlood 攻撃が最も多く、UDPFlood、PINGFlood などが続いており、一般的によく知られた DoS 攻撃が多くを占めています。
また、上半期は SYNFlood が最も多く観測されましたが、下半期は UDPFlood が最も多く観測されています。このことから、より防御が難しく、攻撃の送信元が特定しづらい攻撃手法へ移行してきている可能性があります。

# 3　サイバー犯罪・攻撃例

平成 17 年における主なサイバー犯罪・攻撃例として、DoS 攻撃、スパイウェア、フィッシング、SQL インジェクションについて掲載します。

フィッシング、スパイウェアについては、特に、各個人の注意・対策が必要ですが、DoS 攻撃、SQL インジェクションについては、管理者等の注意・対策が必要です。

## 3.1 DoS 攻撃

DoS（Denial of Service）攻撃とは、サービス不能攻撃とも呼ばれ、図 3.1 に示すように、インターネット上において様々なサービスを提供しているサーバに対して大量のデータを送りつけ、サーバに過剰な負荷をかけることによりその機能を麻痺させる攻撃のことを指します。

基本的な防御対策としては、ルータやファイアウォールなどのセキュリティ機能を利用し不要なパケットを削除する、システムや各機器が許容する通信量を超えないよう帯域を制御するなどが挙げられます。

実際にサービス不能の事態に陥った場合は、まず外部からの攻撃を受けているのかどうかを判断します。攻撃を受けているのであれば、通信の内容、各機器の状態及び負荷状況等から攻撃の種類を迅速に見極め、攻撃の性質、特徴に応じた対処をとる必要があります。

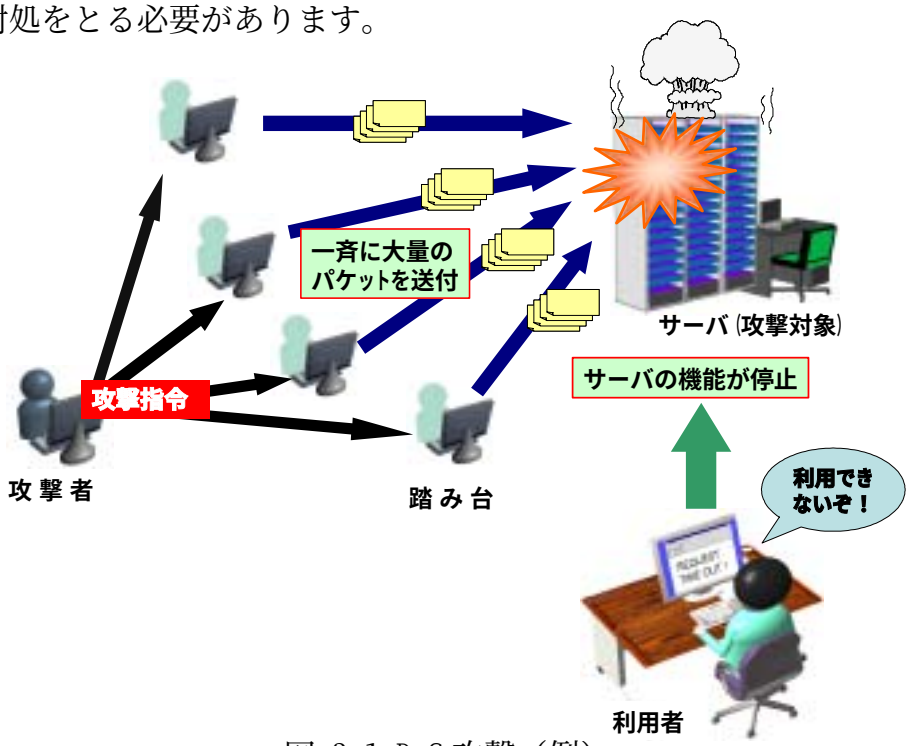



図 3.1 DoS 攻撃（例）

■ ***事例***

２月から４月にかけて、中央省庁等の Web サーバに対して大規模な DoS 攻撃が行われ、一時的にこれらの Web サイトへの接続が困難な状況になるなどの被害を受けました。

## 3.2 スパイウェア

スパイウェアとは、コンピュータ利用者の IP アドレスや Web サイトの閲覧履歴等の情報を密かに収集して外部へ送信するプログラムのことをいいます。広告やマーケティングのためにデータを集めるものが多数を占めていますが、インターネットバンキングへのアクセスに必要な ID・パスワードの窃取を目的とした極めて悪質なものも数多く存在しています。

スパイウェアは、他のソフトウェアと共に配布、インストールされることが多いため、利用者がスパイウェアの存在に気付くことは困難です。また、一般のウイルス対策ソフトウェアでは検出されない場合もあり、その発見と駆除を専門としたスパイウェア対策ソフトウェアが存在しています。

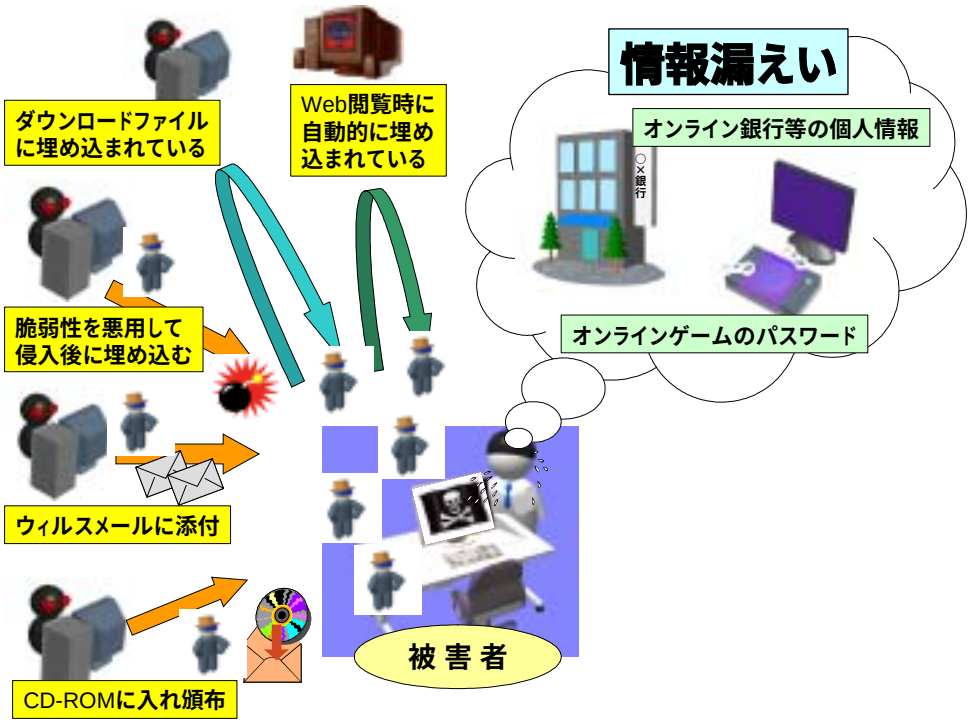



図 3.2 スパイウェアによる犯罪手法（例）

■ ***事例***

スパイウェアを使って、インターネットバンキングを利用している顧客のID・パスワードを取得し、これを悪用して顧客の口座から自己の管理する口座に送金した者が、不正アクセス禁止法違反及び電子計算機使用詐欺罪で検挙されました。(11月)

## 3.3 フィッシング

フィッシング（phishing）とは、実在するクレジットカード会社や銀行などを装った内容のメールを無作為に発信して、メールの受信者を偽の Web サイト（フィッシングサイト）にアクセスさせ、個人情報を入力するように仕向け、その個人情報を騙し取ることをいいます。

個人情報等を聞き出そうとするメールが届いた場合、送信元企業の窓口に電話等で事実を問い合わせ、確認するなどし、メールに記載されている URL を信用して、不用意にフィッシングサイトにアクセスし、個人情報等を入力しないように注意する必要があります。

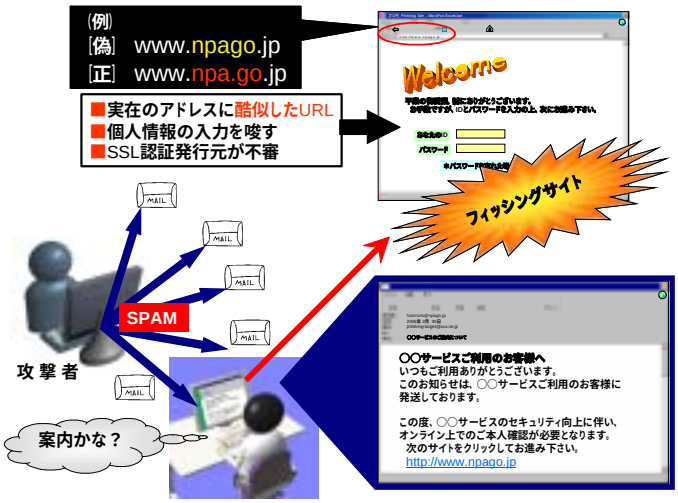



図 3.3 フィッシングによる犯罪手法（例）

■ ***事例***

インターネットサービス会社会員の ID・パスワードを不正に入手することを企て、同社のサイトを偽装したフィッシングサイトをインターネット上に公開することにより、正規のサイトと誤信して入力した同社会員の ID・パスワードを入手して、同会員になりすまして不正アクセスを繰り返していた者が、著作権法違反及び不正アクセス禁止法違反で検挙されました。(６月)

## 3.4 SQL インジェクション

SQL インジェクションとは、データベースサーバに不正な命令が中継されるような特殊な入力を Web アプリケーションに与え、データベースを不正に操作する攻撃手法のことをいいます。

攻撃によって、Web アプリケーションの作成者が意図しない SQL 文が実行されると、データベースに格納されているデータの改ざんや個人情報の窃取等の被害を受ける可能性があります。

被害を防ぐためには、Web アプリケーションのプログラムにおいて、特殊文字をエスケープ処理する、準備済み SQL 文（プレースフォルダ、バインドメカニズムともいう。）を使用したりすると共に、データベースにおいて、Web アプリケーション用のユーザに必要以上の権限を与えないなどの対策が必要です。

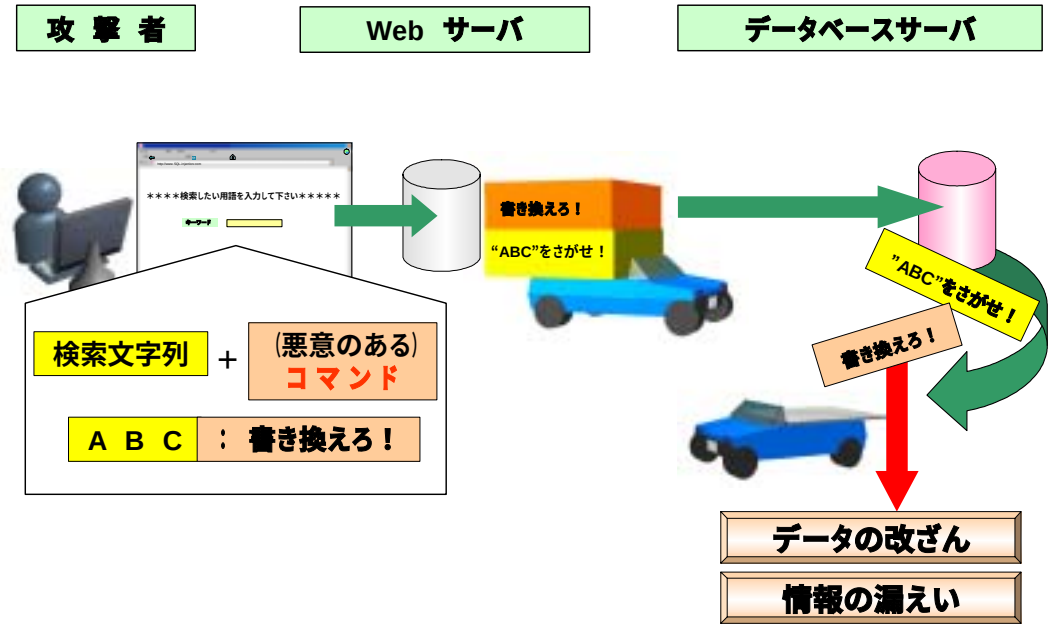



図 3.4 SQL インジェクションによる攻撃手法（例）

■ ***事例***

旅行会社のサーバコンピュータに数万回にわたり不正な指令を送信する不正アクセスを繰り返し、同社が管理する会員の個人情報を不正に取得した者が不正アクセス禁止法違反で検挙されました。（６月）

# 4　安全・安心なインターネット社会への取組み

第１章で述べたとおり、インターネット上の治安は予断を許さない情勢にあるといえます。そこで、情報技術解析課が行った安全・安心なインターネット社会を目指した各種の取組みについて紹介します。

## 4.1 重要インフラ事業者等との連携

電力、金融等の重要インフラがサイバー攻撃を受けて機能停止に陥った場合、国民生活への甚大な影響が懸念されます。このようなサイバーテロによる被害の未然防止及び発生した際の被害拡大防止と被疑者の検挙のためには、重要インフラを担う事業者と警察の平素からの強い連携が必要です。

そのため当課では、都道府県警察とともに事業者を個別に訪問し、情報セキュリティに関する助言や指導を行うとともに、情報セキュリティセミナーや研修会を開催し、国内外の情勢に関する講義、緊急対処の実演、各種事例の紹介等を行っています。また、重要インフラ事業者等と合同でサイバーテロを想定した緊急対処訓練を実施するなど、より実戦的な活動にも取り組んでいます。

平成 17 年には、中央省庁や地方公共団体、重要インフラ事業者等に対して、DoS 攻撃や Web サイトの改ざん、情報漏えいなど、社会的に影響の大きいサイバー攻撃事案が多数発生しました。当課では、攻撃を受けた重要インフラ事業者等に対して対策を助言し、被害の拡大や再発の防止に努めました。

## 4.2 産学との連携

情報通信技術の発展に伴い、これを悪用した新たな犯罪手口が次々と現れています。これらに適切に対応していくためには、情報通信分野の研究開発主体である大学研究機関や企業等と協力し、最新の技術動向を把握していかなければなりません。17 年には、大学[22]や企業[23]と共同で情報セキュリティに関する論

[22] 東京大学生産技術研究所へ研究生を派遣し、サイバー攻撃の検知に関する研究を実施
○「定点観測システム収集データを利用したインターネット空間補間手法の提案と早期異常検知への適用」／2005 年暗号と情報セキュリティシンポジウム(SCIS2005)
○Various viewpoints analysis of the actual and large-scale data by using the data mining technique

文を発表したほか、米マイクロソフト社と技術協力協定を締結[24]するなど、産学との連携強化を推進しています。

## 4.3 国際連携

情報通信技術を利用した犯罪は、時間的、距離的な制約を受けないことから国際的性質が強くなっているため、当課では、Ｇ８ハイテク犯罪サブグループ等の国際会議に出席するほか様々な国際連携を行っています。

アジアでの国際連携を進めるため、当課では、アジア地域サイバー犯罪捜査技術会議を開催し、カード犯罪技術対策等の発表・討議をするとともに、実戦形式訓練を行いました。

また、アジアの９カ国・１地域を結ぶサイバー犯罪技術情報ネットワークシステム(CTINS :Cybercrime Technology Information Network System)を構築、運用しており、９月の ICPO アジア・南太平洋地域 IT 犯罪作業部会において、CTINS をアジアにおける情報共有手段の一つとすることが合意されるなど、国際的に高い評価を受けています。

開発途上国に対する技術協力としては、３月にインドネシアに職員を派遣し、解析ソフトウェアの使用方法等を教授しました。その結果、重要事案の捜査において当該ソフトウェアが活用されるなど、同国の能力向上に寄与することができました。

さらに、６月には第２回 ICPO・IT 犯罪捜査技術に関するトレーナー養成ワークショップに、第１回ワークショップに引き続き、職員を講師として派遣し、国際的な捜査技術の向上に寄与すべく、法執行機関との連携を強化しています。

また、サイバーフォースセンターでは、サイバーテロ対策の推進に必要となる情報セキュリティの情報を収集するため、情報セキュリティ関連組織との連携を推進しており、11 月には、加盟組織間における非公開の技術的情報の共有を通じた各加盟組織の適切な事案対処の促進を目的とする世界的な機関である

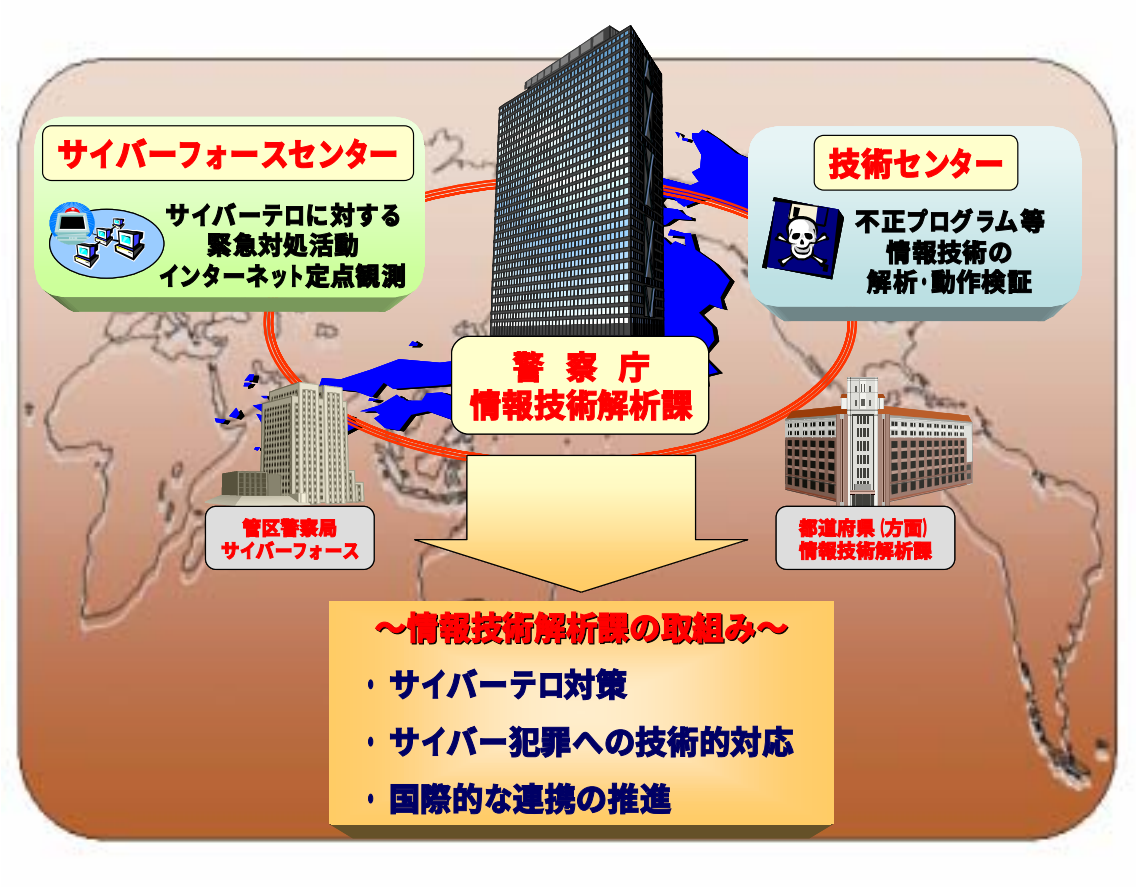
---

／2005 IEEE International Carnahan Conference on Security Technology (ICCST2005)

[23] 民間企業と協力し、サイバーテロ対策に係る技術に関する調査及び研究開発を実施
○「囮サーバで送受信されたパケット系列を統計分析することによるワーム検知システムの提案」／第 30 回コンピュータセキュリティ研究発表会

[24] 技術情報の提供に関する民間企業との協力について
http://www.cyberpolice.go.jp/important/2005/20050628_172719.html

FIRST[25] (Forum of Incident Response and Security Teams) に、警察機関として世界で初めて加盟を承認されました。




[25] http://www.first.org/