

情報技術解析平成18年報

～平成18年のインターネット治安情勢～

平成19年2月

警察庁情報通信局情報技術解析課

はじめに	2
1 インターネット治安情勢の総括	3
1.1 概況	3
1.2 傾向	4
1.3 情報セキュリティ対策向上のために	5
2 インターネット定点観測結果の分析	6
2.1 観測結果の推移	6
2.1.1 ファイアウォールに対するアクセス状況	7
2.1.2 不正侵入検知システムによる検知状況	8
2.2 アクセス状況の詳細分析	10
2.2.1 TCP ポートに対するアクセス状況	10
2.2.2 TCP 各ポートの状況	11
2.2.3 UDP ポートに対するアクセス状況	13
2.2.4 UDP 各ポートの状況	13
3 ボットネット観測結果の分析	15
3.1 ボットネットの脅威	15
3.2 ボットネット観測数の推移	16
3.3 ボット観測数の推移	16
3.4 ボットの感染活動	17
3.5 ボットネットのサービス不能攻撃 (DoS 攻撃) 活動	18
4 サイバー犯罪・攻撃例	19
4.1 情報流出型ウイルス	19
4.2 ワンクリック請求	20
4.3 詐称メール	21
4.4 スピア型攻撃	22
5 安全・安心なインターネット社会への取組み	24
5.1 重要インフラ事業者等との連携	24
5.2 産学との連携	24
5.3 国際連携	25
5.3.1 アジア地域におけるリーダーシップ	25
5.3.2 二国間の技術協力	25
5.3.3 FIRST との連携	26
5.4 デジタルフォレンジックの確立に向けた取組み	26

はじめに

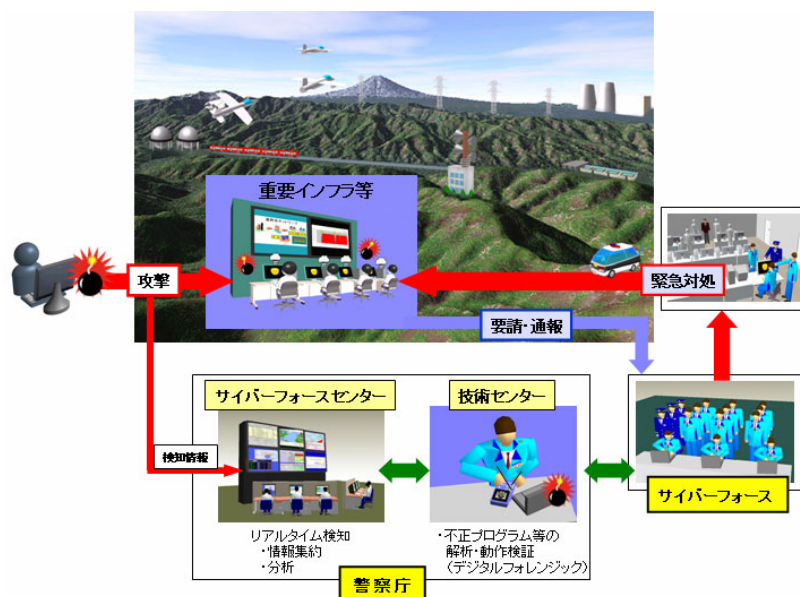
情報通信ネットワークは、国民生活の利便性を向上させ、社会・経済の根幹を支えるインフラとして機能しています。他方、コンピュータウイルスを利用した不正アクセス事件等の情報技術を利用した犯罪（サイバー犯罪）が増加を続けており、特に近年では「ボット」と呼ばれる不正プログラムのまん延といった情報セキュリティに対する脅威も増大しています。

このような中、警察庁では18年8月に「治安再生に向けた7つの重点」を策定し、その中でも「サイバー空間の安全確保」を1つの柱として、各種取組みを推進しています。

本年報は、インターネットの治安情勢を技術的な視点から分析して取りまとめ公表するものです。

まず「1 インターネット治安情勢の総括」では、18年中におけるインターネット上で発生した情報セキュリティ事案の技術的特徴を概観します。「2 インターネット定点観測結果の分析」では、全国の警察施設のインターネット接続点に対するアクセス情報を分析した結果を取りまとめています。「3 ボットネット観測結果の分析」では、脅威が増大しているボットネットを観測・分析した結果を取りまとめています。「4 サイバー犯罪・攻撃例」では、話題となった主なサイバー攻撃を紹介し、さらに「5 安全・安心なインターネット社会への取組み」では、警察庁情報通信局情報技術解析課のさまざまな取組みを紹介しています。

本年報が、安全・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いです。



1 インターネット治安情勢の総括

インターネット上では、コンピュータウイルスによる無差別な攻撃から、電子メールアドレスを指定するなどして対象を明確にした攻撃まで、さまざまな情報セキュリティ事案が発生しています。

警察庁情報通信局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情報等を観測・分析することで、「インターネット治安情勢」、すなわち「今、インターネットで起きていること」を把握し、警察庁セキュリティポータルサイト「@police」等を通じて提供することなどにより、情報セキュリティ意識の向上に努めているほか、国民生活又は社会経済活動に重大な影響を及ぼすおそれのある情報システムへの影響が懸念される場合には、個別に、犯罪の未然防止・被害の拡大防止を講じています。

1.1 概況

- インターネット上のコンピュータに対する不審なアクセスは減少するも依然として高水準。ボット²の感染やスパイ型攻撃³により深刻な被害の発生が懸念される。

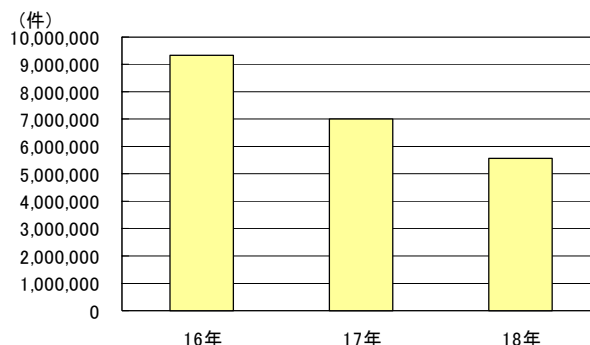
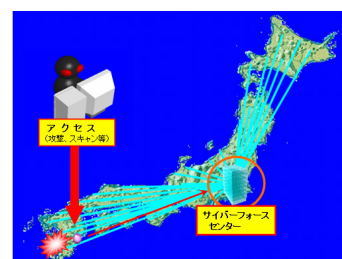


図 1.1 総アクセス件数の推移

図 1.1 は、全国の警察施設のインターネット接続点へのアクセス件数の推移です。これらのアクセスは、要求することなく受信した不審なアクセスであり、インターネット上のコンピュータに対する無差別な攻



¹ <http://www.cyberpolice.go.jp/>

² 不正プログラム的一种。被害コンピュータは外部から操作可能なものとなる。

³ 不正プログラムを電子メールに添付し、関係者からの電子メールであると巧妙に装うなどして感染させようとする攻撃。

撃の傾向を示すものと考えられます。18年は、インターネットからの不審なアクセスは減少していますが、インターネット上の一箇所あたりで換算すると約3分に1回の割合で受信している状況にあります。減少の主な要因としては、大規模に感染を拡大する不正プログラムの新たな発生がみられなかったことが挙げられます。

また、この不審なアクセスの中には、コンピュータを外部から操作可能なものとしてしまう不正プログラムであるボットの感染活動によるものが含まれることが確認されたほか、不正プログラムを電子メールに添付し、関係者からの電子メールであると巧妙に装うなどして感染させようとする「スパイ型攻撃」と呼ばれる情報セキュリティ事案が発生しています。これらの攻撃が成功した場合には、コンピュータで扱う個人情報等を外部に漏えいさせるなどの深刻な被害の発生が想定されます。

1.2 傾向

■ 増加するボットネット

17年1月に運用を開始した「ボットネット観測システム」による分析の結果からは、複数のボットを協調した動作ができるようネットワーク化した「ボットネット」が増加する傾向が見られます。ボットに感染したコンピュータは外部から操作可能なものとなり、個人情報の漏えい等、深刻な被害の発生が懸念されます。

■ スパイ型攻撃の発生

不正プログラムを電子メールに添付し、関係者からの電子メールであると巧妙に装うなどして感染させようとする、一般に、「スパイ型攻撃」や「標的型攻撃」と呼ばれる情報セキュリティ事案が発生しています。

■ 未知の脆弱性を悪用した攻撃⁴の発生

不正プログラムを感染させるために悪用されるプログラムの脆弱性について、広く利用されるワープロソフトであるマイクロソフト社のワードやジャストシステム社の一太郎等の未知の脆弱性が利用される情報セキュリティ事案が発生しています。

⁴ 発生の段階で一般には知られていないプログラムの脆弱性が悪用された攻撃のこと。

1.3 情報セキュリティ対策向上のために

インターネット上では様々な情報セキュリティ事案が次々と発生していることから、インターネットの利用者は常に情報セキュリティに関する意識を持ち、被害に遭わないよう適切に準備・行動することが大切です。

個人利用者は、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、不審なメールやファイルは開かないなどの基本的な情報セキュリティ対策を確実に実施することで、多くの被害を防ぐことが可能となります。

また、企業等においては、企業自身を守るだけでなく顧客等に被害を及ぼさないためにも、個人利用者が行うべき対策に加え、Web サーバなどインターネット上でサービスを提供するコンピュータのセキュリティ強化、適切なパスワードの管理・利用、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。

情報技術解析課では、今後とも、この種の情報を積極的に提供し、安全・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

インターネット定点観測は、全国 57 箇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に対するアクセス及び不正侵入検知システムによる検知結果を分析しているものです。

2.1 観測結果の推移

図 2.1 に、観測結果の推移を示します。ファイアウォールに対するアクセス件数は、18 年も減少する傾向にありました。また、不正侵入検知システムでの検知件数も 17 年と比較して減少しています。

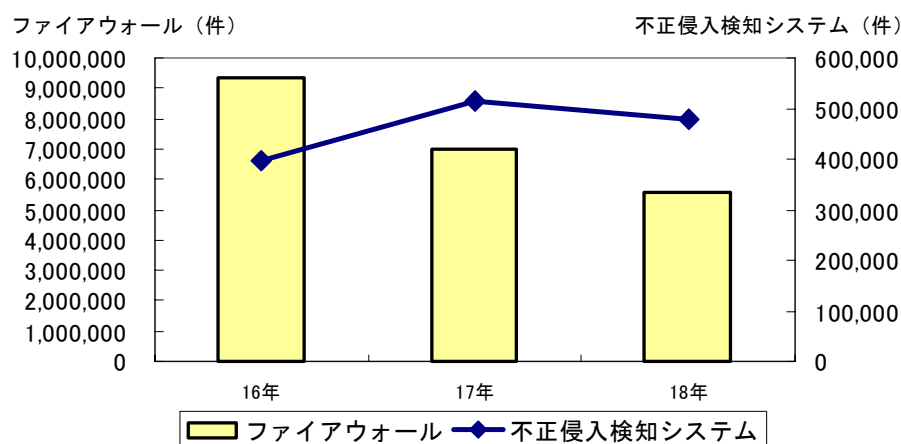


図 2.1 観測結果の推移

設置しているファイアウォールは、インターネット側からなされる全てのアクセスを記録しますが、これらアクセスに対して如何なる反応もしないように設定されています。また不正侵入検知システムは、インターネット側からのアクセスに対して既知の不正アクセスパターンと比較することで不正なアクセスを検知するように設定されています。

なお、これら以外の機器についても外部からのアクセスに対して如何なる反応もしないように設定されています。

2.1.1 ファイアウォールに対するアクセス状況

図 2.2 に、ファイアウォールに対する国・地域別のアクセス状況を示します。18 年の内訳は、国内からのアクセスが約半数を占め、次いで中国、米国と続いています。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い理由の一つに、ウイルス等不正プログラムの感染活動にみられる特徴的な動作パターンが挙げられます。すでに感染したコンピュータからの感染活動においては、感染しているコンピュータの IP アドレスの近く（第一及び第二オクテットが同一の IP アドレス等）に接続を試みる場合が多いため、同じアジア地域に属し、IP アドレスの割当て範囲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考えられます。

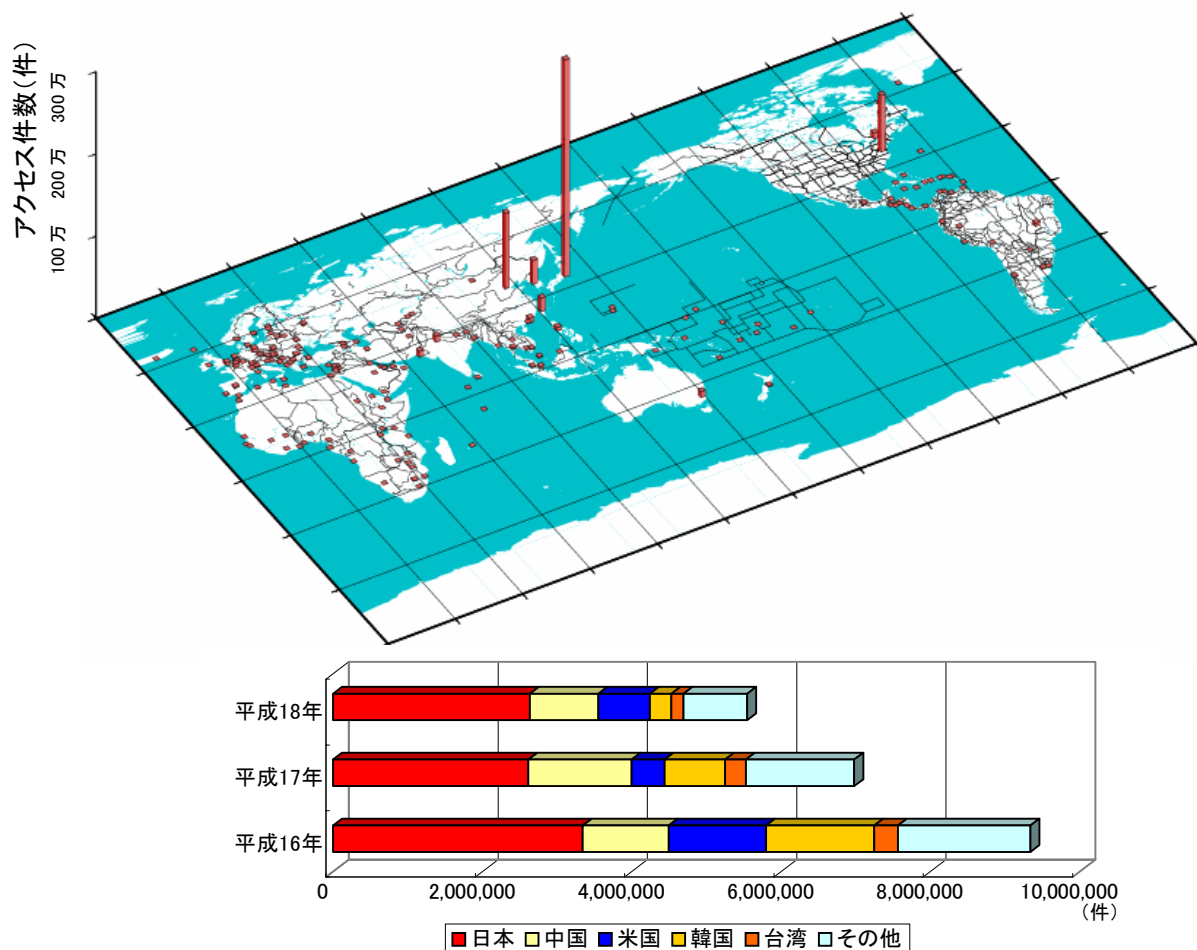


図 2.2 国・地域別のアクセス状況

18 年は、大規模に感染を広げる不正プログラムが新たに出現しなかったことや、スパイ型攻撃等、定点観測には反映されにくい攻撃手法が用いられるよう

になってきたため、総アクセス件数が減少したものと考えられます。

アクセス状況の詳細については、「2.2 アクセス状況の詳細分析」をご覧ください。

2.1.2 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により不正なアクセスと判断されたものを技術的に分類した検知状況を示します。18年に検知された結果では、不正プログラムの一つである「Worm」(SQL Slammer ワーム⁵)の感染活動によるものが全体の約92%、インターネットに接続されたコンピュータを探索する「Scan」によるものが約7%を占めています。18年の傾向は前年とほぼ同様のものと判断されます。

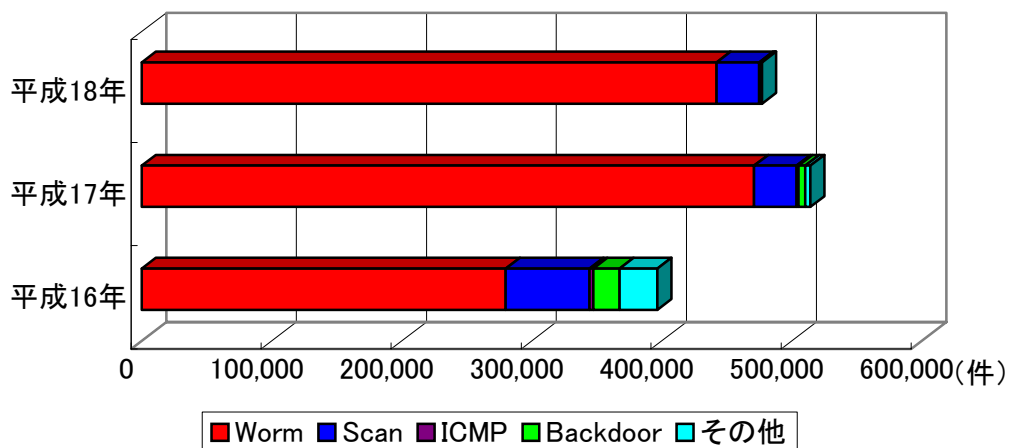


図 2.3 攻撃手法別検知状況

⁵ 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

図 2.4 に、18 年の攻撃手法別検知件数の推移を、図 2.5 に、国別の Worm 検知件数の推移を示します。

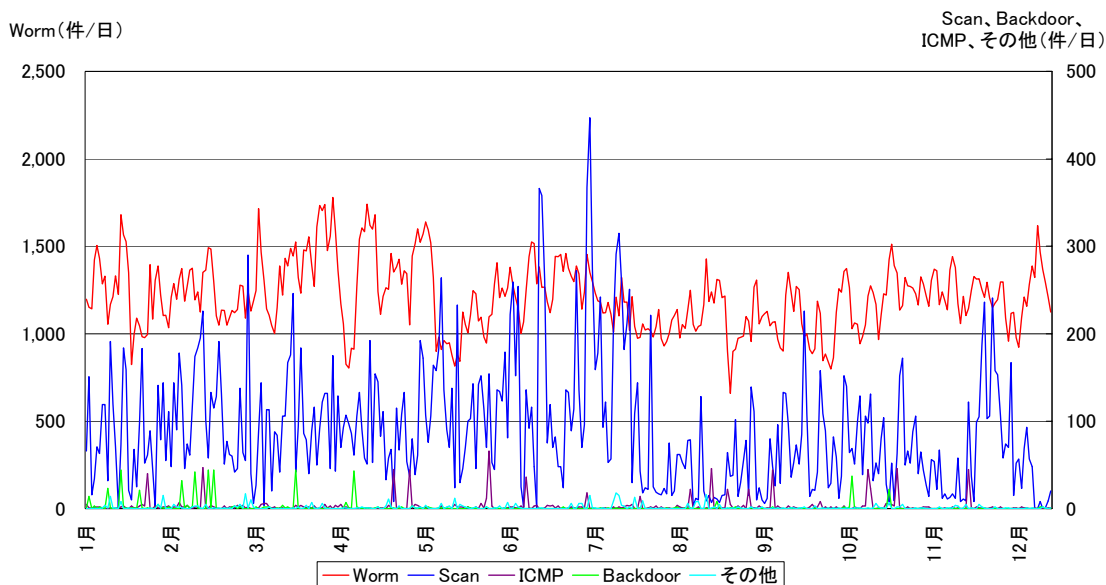


図 2.4 18 年の攻撃手法別検知件数の推移

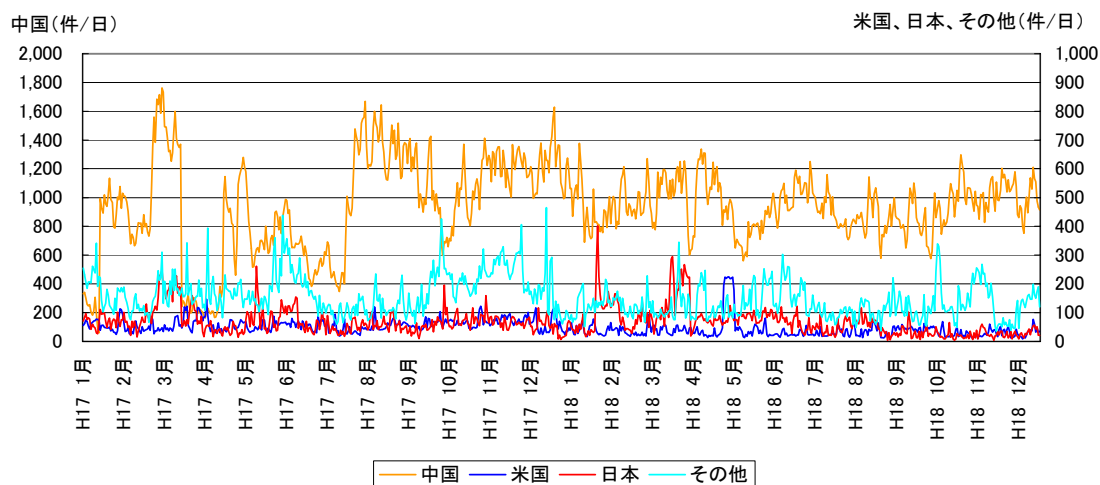


図 2.5 国別の Worm 検知件数の推移

国別の状況では、中国を発信元とする Worm 検知件数が、他の国からのものに比較して、高い数値で推移しています。SQL Slammer ワームは 15 年 1 月に発生したのですが、いまだに数多く検知されています。この不正プログラムが悪用する脆弱性の修正プログラムが提供されているにもかかわらず、それを適用していないサーバが、インターネット上に数多く存在しているものと考えられます。

2.2 アクセス状況の詳細分析

ファイアウォールに対するアクセス状況をポート別に分析することにより、如何なるプログラムが攻撃の対象となっているかを把握することができるとともに、新たな不正プログラムの出現等の特異な事象について、認知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、18 年における TCP の宛先ポート別アクセス件数の全体像⁶を示します。135/TCP ポート、445/TCP ポート及び 139/TCP ポートに対して多くのアクセスがなされている状況が把握できます。

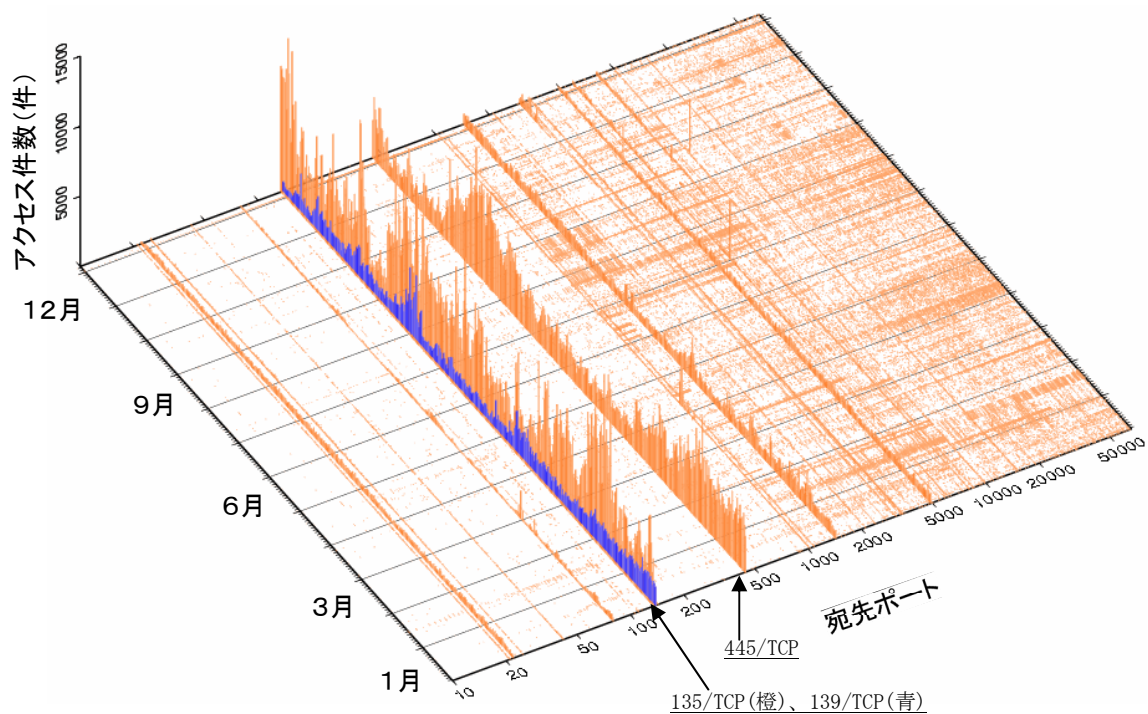


図 2.6 TCP 宛先ポート別アクセス件数

⁶ 0/TCP～9/TCP については、ほとんど観測されていないため省略しています。

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、図 2.9 に 139/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、Windows の各種の機能を実現するために利用されているものですが、不正プログラムによっても感染を広げるためなどに利用されています。

18 年は、前年と比較してファイアウォールに対するアクセス件数の総数が減少しましたが、特に、図 2.7～2.9 に示す TCP ポートへの国外からのアクセスの減少による要因が大きなウエイトを占めています。これは、前年に見られたような、ネットワークを介して大規模に感染を広げる不正プログラムの新規の出現がなかったためと考えられます。

一方、これらポートに対する国内からのアクセスには、時折、突発的なアクセス数の増加が観測されました。その要因としては、Windows に存在する脆弱性に対し、その修正プログラムが提供されていない又は提供されていてもその適用が広がっていない段階で、これを悪用する手段がボットなど不正プログラムに組み込まれ使用されたことが挙げられます。

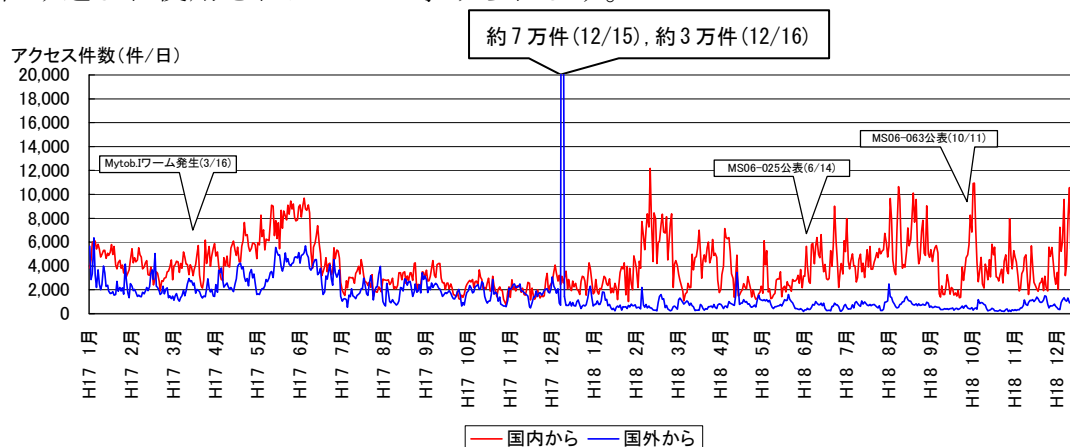


図 2.7 135/TCP ポートに対するアクセス件数の推移

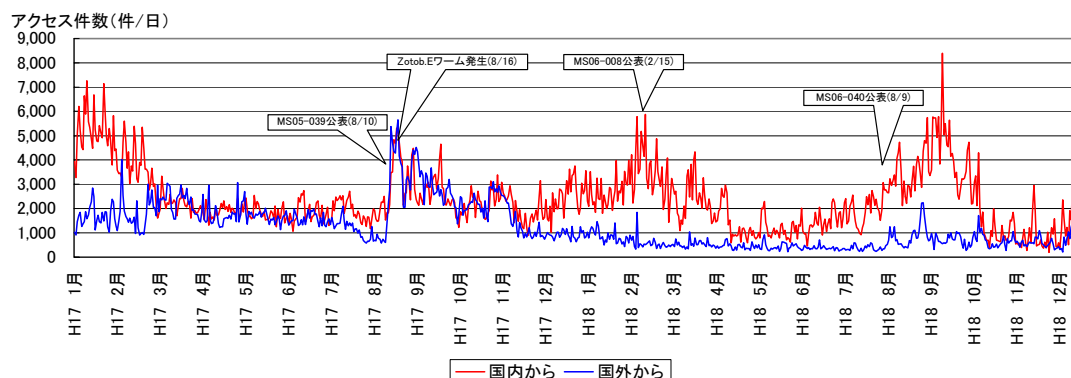


図 2.8 445/TCP ポートに対するアクセス件数の推移

例えば、139/TCP ポートに対するアクセス結果において、8月18日から9月中旬にかけてアクセス数の増加が観測されました⁷。これは8月9日に発表されたWindowsの脆弱性「Server サービスの脆弱性により、リモートでコードが実行される (MS06-040)」の悪用可能性を探索するためにインターネット上で大規模なコンピュータの探索行為が行われた可能性を示しています。

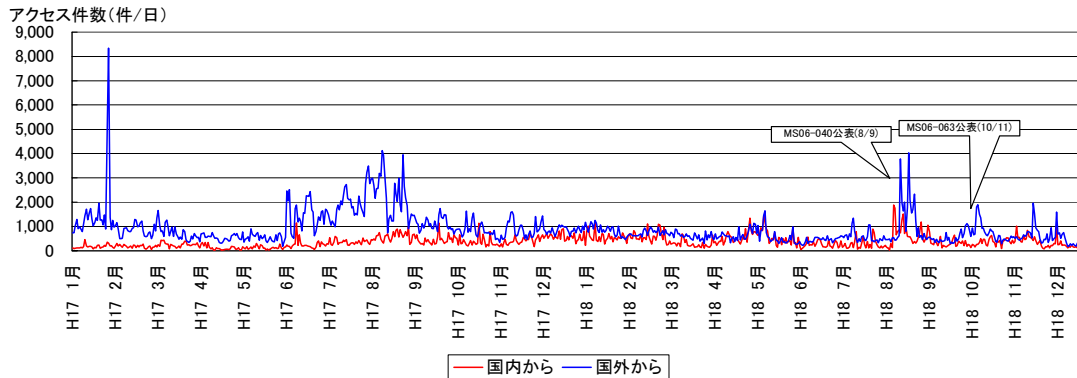


図 2.9 139/TCP ポートに対するアクセス件数の推移

⁷ TCP139 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/2006/20060823_181802.html

2.2.3 UDP ポートに対するアクセス状況

図 2.10 に、18 年における UDP の宛先ポート別アクセス件数の全体像⁸を示します。1026/UDP ポート、1027/UDP ポート、137/UDP ポートに対して多くのアクセスがなされている状況が把握できます。

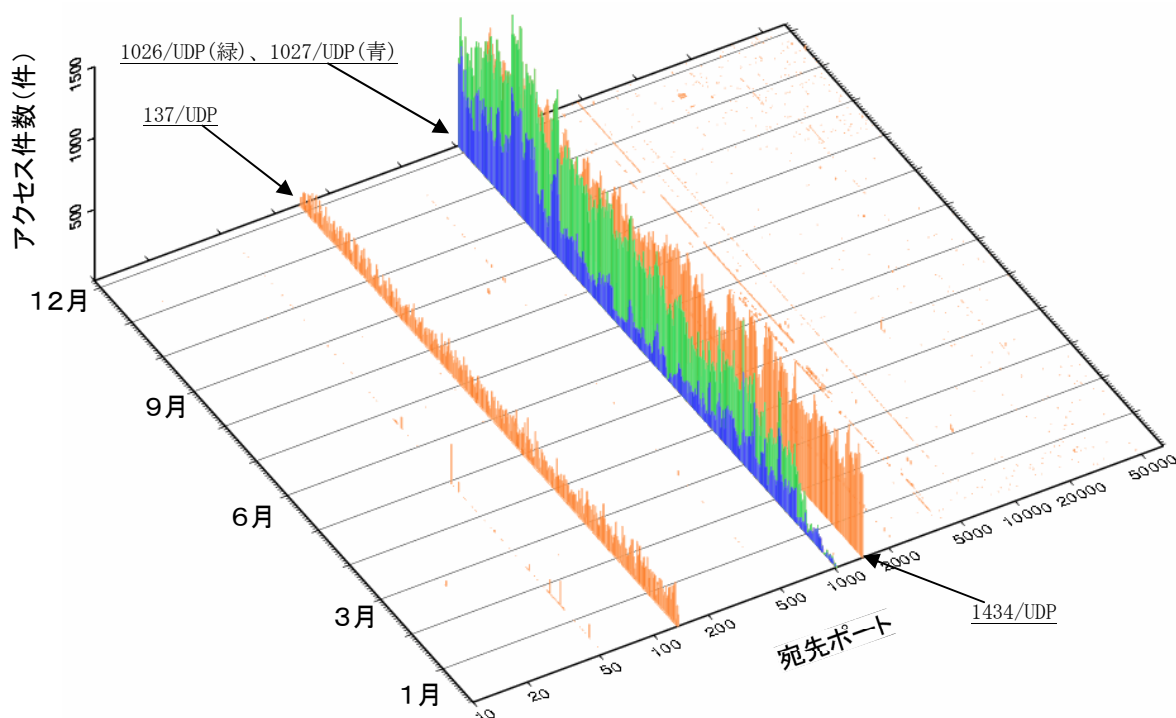


図 2.10 UDP 宛先ポート別アクセス件数

2.2.4 UDP 各ポートの状況

図 2.11 に、1026/UDP 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、Windows の Messenger サービスで使用されているポートです。観測されたアクセスの多くは、受信したコンピュータにおいて商品等の購入を促す広告を表示させるためのもの（Messenger スпам）とみられ、18 年 2 月以降、増加が続いています。

⁸ 0/UDP～9/UDP については、ほとんど観測されていないため省略しています。

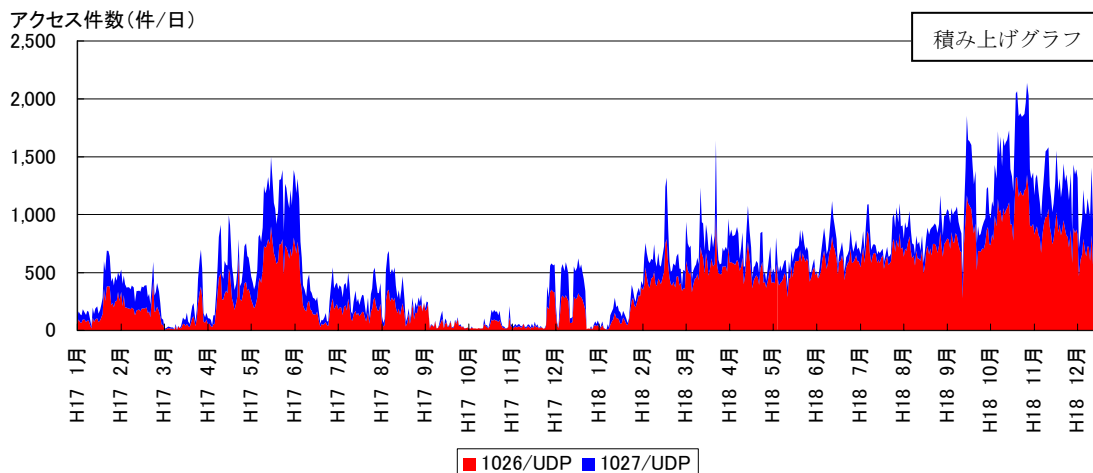


図 2.11 1026/UDP 及び 1027/UDP ポートに対するアクセス件数の推移

図 2.12 に、1026/UDP 及び 1027/UDP ポートに対するアクセス元コンピュータの国別の推移を示します。17 年の Messenger スпам発信元のは中国でしたが、18 年は米国がほとんどを占めています。

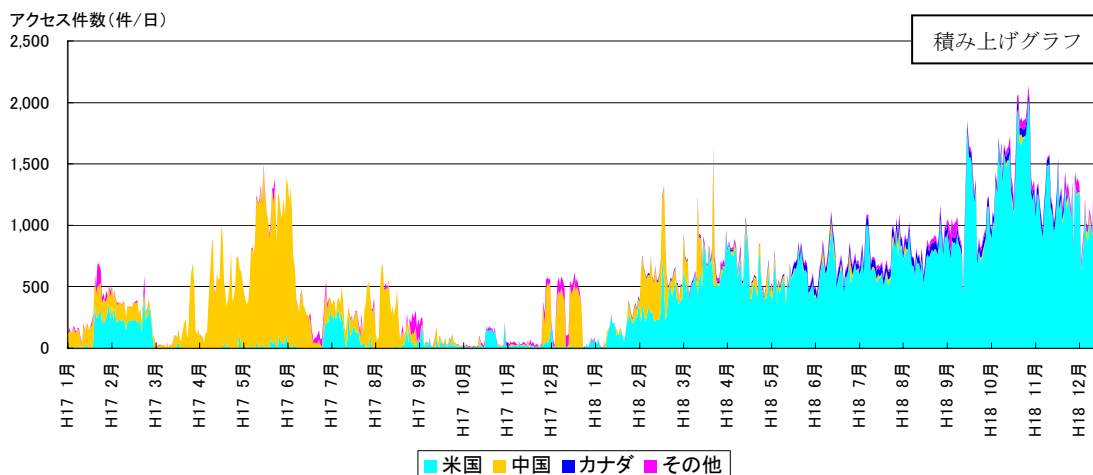


図 2.12 1026/UDP 及び 1027/UDP ポートに対する国別アクセス件数の推移

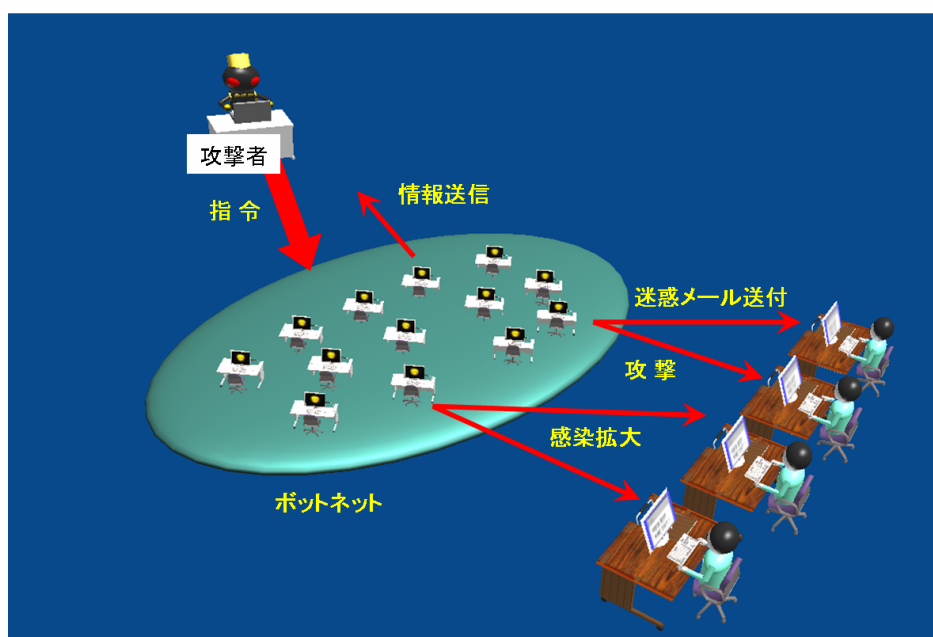
137/UDP ポートは、Windows においてファイル共有等を行うための手続き (NetBIOS) で使用されており、年間を通してアクセスが観測されています。また、1434/UDP ポートは、SQL Server で使用されており、観測されたアクセスは、SQL Slammer ワームの感染活動と考えられます。

3 ボットネット観測結果の分析

3.1 ボットネットの脅威

ボットは、不正プログラム的一种で、OS やアプリケーションの脆弱性を悪用するなどしてコンピュータに感染し、攻撃者から操作できる状態とします。また、ボットに感染した複数のコンピュータをまとめて協調した動作をさせることができるように、ボットをネットワーク化した「ボットネット」と呼ばれる仕組みが構築されています。これにより、例えば家庭のコンピュータがボットに感染した場合、気付かないうちに、コンピュータに保存した個人情報や盗取されたり、ボットネットの一員として、ほかのコンピュータへの感染の拡大やサービス不能攻撃（DoS 攻撃）の実施、迷惑メールの送信等に利用されたりするなどの被害に遭う可能性があります。

ボットには、攻撃者の命令に従いインターネットからファイルをダウンロードして実行する機能が盛り込まれているものがあります。この機能が利用された場合、次々と新しい未知のプログラムが実行されることになり、コンピュータの中でどのような不正な行為が実行されたのかを把握することは非常に困難となります。例えば、18年に警察庁の観測システムで認知したボットによりダウンロードされたファイル 1,145 個について分析したところ、ウイルス対策ソフトで検出できたものが 317 個と全体の約 28%にとどまりました。



3.2 ボットネット観測数の推移

警察庁では、17年1月から「ボットネット観測システム」の運用を開始し、ボットネットの脅威について「@police」等を通じて注意喚起を行っています。

図 3.1 に、ボットネット観測数の推移(半期毎)を示します。18年下半期に観測したボットネットは473個で、18年上半期の327個に比べ約45%増加しました。そのうち18年下半期に新たに把握したものが248個あり、18年上半期から継続して存在しているものが225個、18年下半期に観測できなくなったものが102個あります。18年中、最も大きなボットネットは、約17万台のボットから構成されていました。

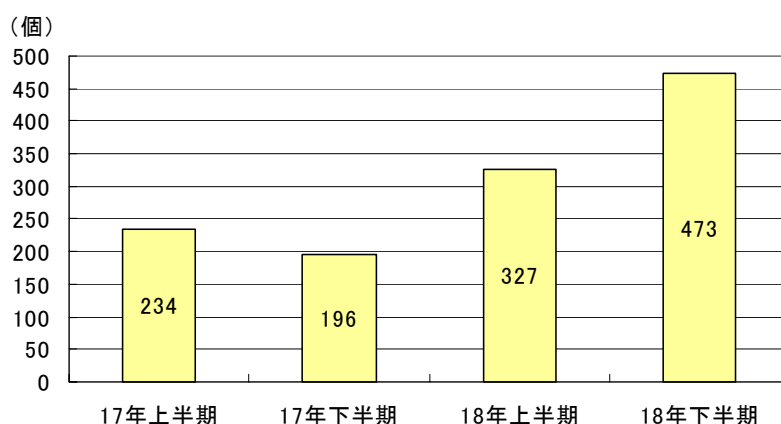


図 3.1 ボットネット観測数の推移(半期毎)

3.3 ボット観測数の推移

図 3.2 に、ボットネット観測結果の分析によるボット数の推定値の推移(半期毎)を示します。18年下半期のボットに感染したコンピュータの数は653,664台で、18年上半期と比べ約73%増加しています。17年下半期における減少は、攻撃者がボットの存在を故意に隠蔽する措置等の影響を大きく受けたものですが、18年はその影響を受けつつも大規模なボットネットを新たに認知したため、再び増加する傾向となっています。

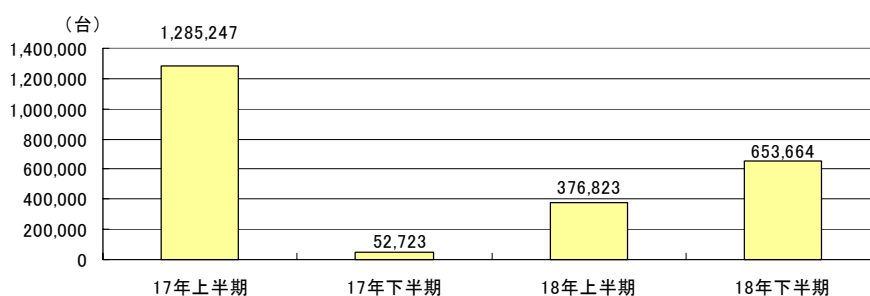


図 3.2 ボットに感染したコンピュータ数の推移(半期毎)

3.4 ボットの感染活動

ボットは、感染したコンピュータから他のコンピュータへ感染を拡大していきます。図 3.3 に、攻撃者がボットを感染させるために送信した命令の受信数を「ポート番号」で分類して示します。ポートとはコンピュータが外部からの通信を受け付ける窓口番号のようなもので、この番号を分析することで、どの受付窓口（実際はプログラム）が攻撃の対象となっているかが推定されます。

18年は、感染命令の観測数が前年と比較して約59%減少しています。Windowsの脆弱性（135/TCP、445/TCP、139/TCPの各ポートを利用）やSQL Serverの脆弱性（1433/TCPポートを利用）を悪用したと考えられるものが82%を超えていました。攻撃に悪用されるほとんどの脆弱性に対しては、それを解消するセキュリティ修正プログラムが提供されていますが、これらが適用されていないコンピュータを狙い、現在でもボットの感染手法として悪用が続いています。

なお、「その他」にはWindowsのファイル共有機能の脆弱なパスワードを突いた攻撃等の命令が含まれています。

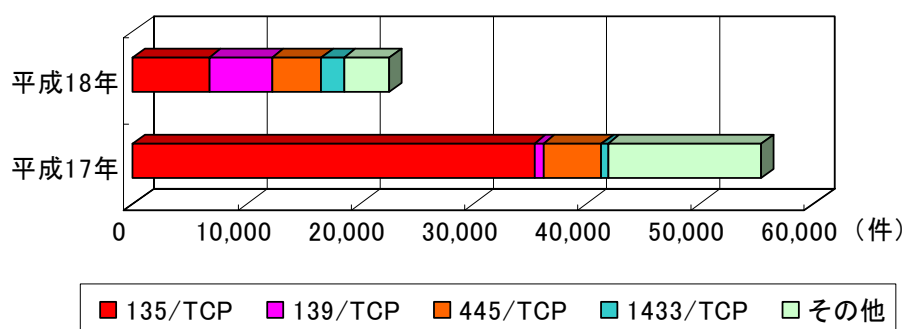


図 3.3 ポート別感染命令件数

3.5 ボットネットのサービス不能攻撃（DoS 攻撃）活動

図 3.4 に、観測された DoS 攻撃命令の件数を示します。18 年は、前年と比較して、約 3.4 倍と急増しています。18 年の内訳は、UDP Flood 攻撃が約 52%と最も多く、PING Flood が約 29%、SYN Flood が約 19%となっています。ボットネットによる DoS 攻撃は、これを構成する多数のボットによる一斉攻撃となり、DDoS（分散サービス不能）攻撃と呼ばれる強力な攻撃になります。

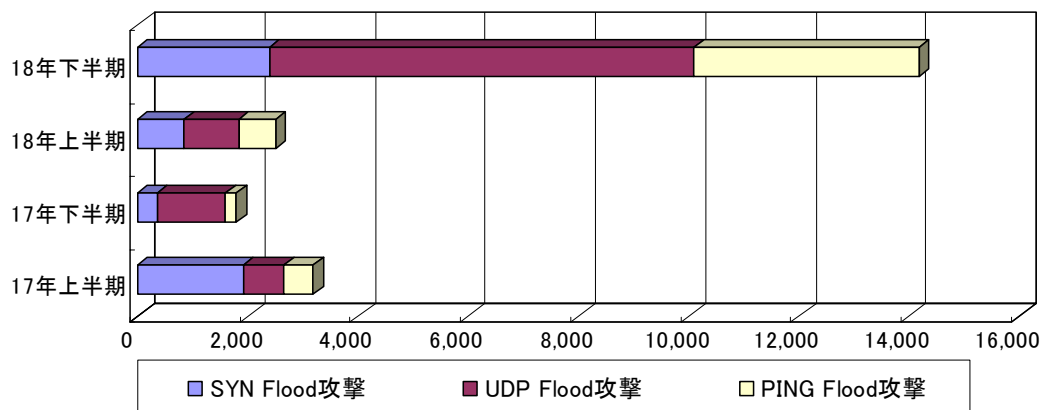


図 3.4 攻撃命令件数

4 サイバー犯罪・攻撃例

18年における主な不正アクセス禁止法違反・ネットワーク利用犯罪の事例として「情報流出型ウイルス」、「ワンクリック請求」、「詐称メール」について、また、新たな攻撃手法として「スパイ型攻撃」について紹介します。

4.1 情報流出型ウイルス

「Antinny (アンティニー)」、「山田オルタナティブ」に代表される情報流出型ウイルスは、インターネット利用者がウイルスであると気付かないよう、アイコンやファイル名を巧みに偽装しています。この一見無害なファイルを実行してしまうとウイルスに感染してしまい、パソコン内のデータが、インターネット上に公開されてしまいます。

基本的な対策としては、次のとおりです。

- ウイルス対策ソフトのパターンファイルを最新のものに更新する。
- 不審なファイルは開かない、実行しない。
- パソコン内にログインパスワード等個人情報を保存しない。

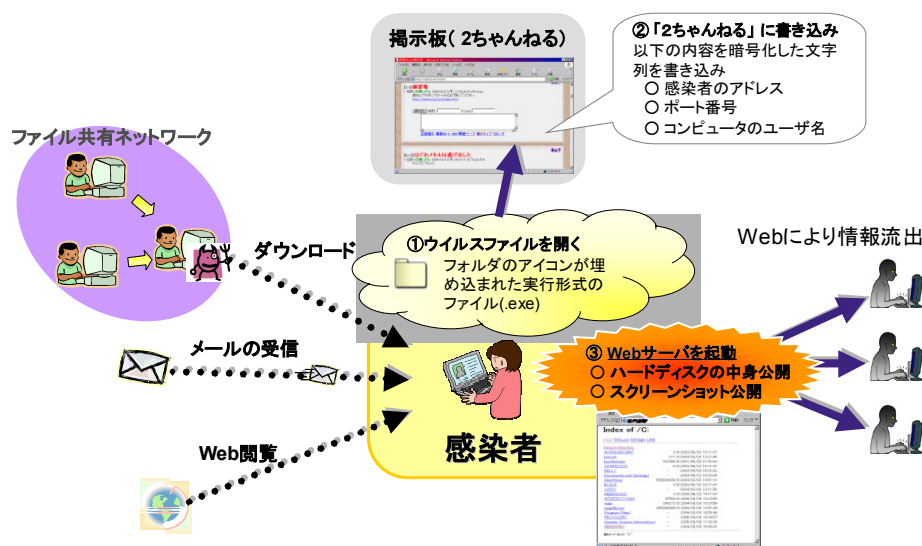


図 4.1 情報流出型ウイルスの動作 (例：山田オルタナティブ)

■ 事例

情報流出型ウイルスに感染したパソコンから流出した、インターネットバンキングの顧客 ID・パスワードを取得し、これを悪用して銀行口座から金銭をだまし取ろうとした者が、不正アクセス禁止法違反・電子計算機使用詐欺未遂で検挙されました。(6月)

4.2 ワンクリック請求

ワンクリック請求とは、パソコンや携帯電話からワンクリックサイトにアクセスしたインターネット利用者に、実際には、会員登録等が行われていないにもかかわらず「登録が完了しました」、「料金をお支払いください」など嘘の利用料金請求画面を閲覧させ、料金を不当に請求する手口をいいます。

ワンクリック請求には、次のような特徴があります。

- メールやホームページにおいて、クリックする前に利用料金・利用規約等について明確な説明がなく、リンク先において即座に「登録完了」や「料金請求」といった内容を表示させる。
- 「あなたの IP アドレス」や「あなたが使用している携帯電話機種名」など、あたかもホームページ閲覧者の個人情報を取得したかのような情報が表示される。

基本的な対策は、次のとおりです。

- 興味本位で勧誘・広告メールに記載されたリンクをクリックしない。
- 不当な料金請求をされた時には、クリックする前のホームページ、電子メール等（携帯電話も含む。）に利用規約等が掲載されているか確認する。これが無い場合には契約の無効を主張できる。
- 支払う義務があると分かるまでは、料金を支払わない。不安になったり、関わりたくないと思って一度支払ってしまうと、更に請求される場合がある。
- 支払う義務があると分かるまでは、相手との連絡は控える。電話、メール等で返事をする、執拗に請求されるおそれがある。
- 詐欺や悪質な取り立て等の被害を受けた場合には、最寄りの警察署又は各都道府県警察のサイバー犯罪相談窓口にご相談する。

※全国警察サイバー犯罪相談窓口等一覧

<http://www.npa.go.jp/cyber/soudan.htm>

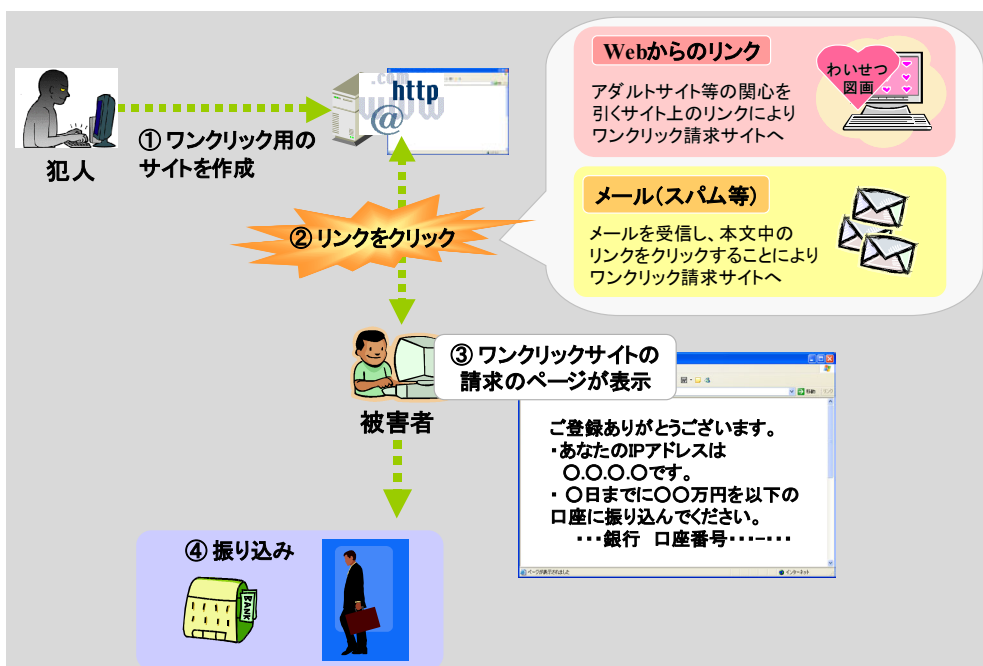


図 4.2 ワンクリック請求 (例)

■ 事例

ワンクリックサイトに接続させる目的で、芸能プロダクションの子役募集を装ったスパムメール（迷惑メール）を無差別に送信して、同サイト上の児童わいせつ画像をクリックした利用者に、入会手続きが完了したように思い込ませて、入会・退会料の名目で金銭をだまし取った者が詐欺、児童買春・児童ポルノ禁止法違反容疑で検挙されました。（6月）

4.3 詐称メール

電子メールが誰から送られてきたものかという送信者情報は容易に詐称することができます。また、フィッシングやワンクリック請求、迷惑メール等においても、その送信元の情報は詐称されている可能性があります。

それらの情報は、電子メールの仕組み上、容易に詐称することができる反面、真偽を見分けるのは困難となっています。

基本的な対策は、次のとおりです。

- 不審なメールは開かない。
- 送信元の電子メールアドレスは詐称することが簡単であることを踏まえ、送信元の電子メールアドレスのみに頼って内容を信用しない。

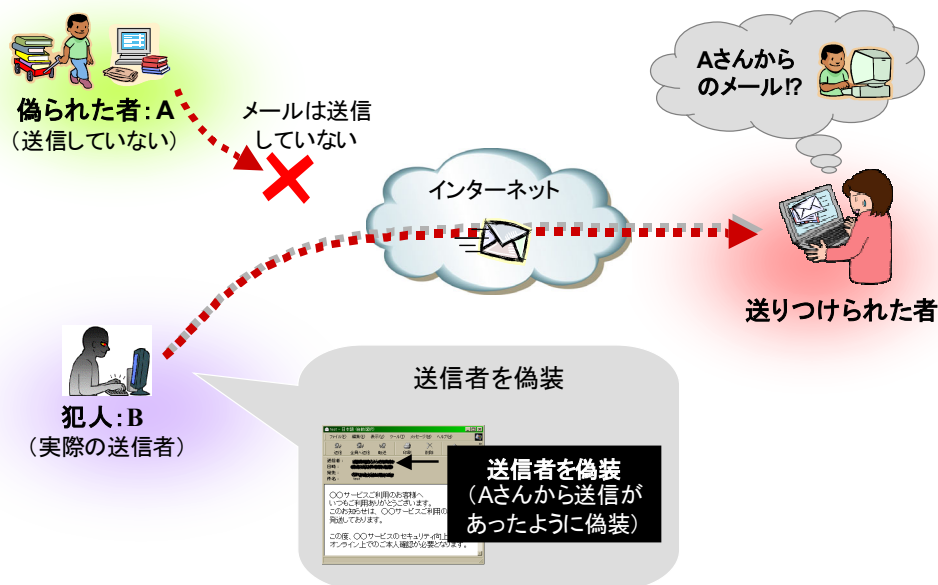


図 4.3 詐称メール (例)

■ **事例**

インターネット異性紹介事業（いわゆる出会い系サイト）を業とする会社の広告のために、複数の他人名義や架空のアドレスを使用した詐称メール約 300 万通を無差別に送信した者が、特定電子メールの送信の適正化等に関する法律（迷惑メール防止法）違反（送信者情報を偽った送信の禁止）で検挙されました。（5月）

4.4 スピア型攻撃

最近、標的を絞り、攻撃であることを相手に気付かせないよう、巧みに偽装した攻撃メールを送り込む攻撃が国内でも発見されるようになりました。こうした攻撃を「スピア型攻撃」又は「標的型攻撃」と呼んでいます。

スピア型攻撃には、次のような特徴があります。

- 特定の組織や個人を狙うため、世間に認知されにくい。
- 知人や仕事上の関係者等になりすましており、その差出人を信じる可能性が高い。
- 被害者が添付ファイルを開きたくなるような文面が記載されている。
- アプリケーションソフトの脆弱性を悪用するデータ・ファイルやそのアイコンを模した不正プログラムを添付される。

- 添付ファイルを開くと、インターネット上から他の不正プログラムをダウンロードするケースが多い。

基本的な対策は、次のとおりです。

- ウイルス対策ソフトやセキュリティ修正プログラムの適用といった基本的な対策を実施することはもちろんのこと、電子メールを開いた場合少しでも不審に感じるものがあれば、送信元に確認する。
- 重要な情報が流出しないよう、インターネットに接続可能なパソコンには重要なファイルを保存しないなど情報の適切な管理を徹底する。

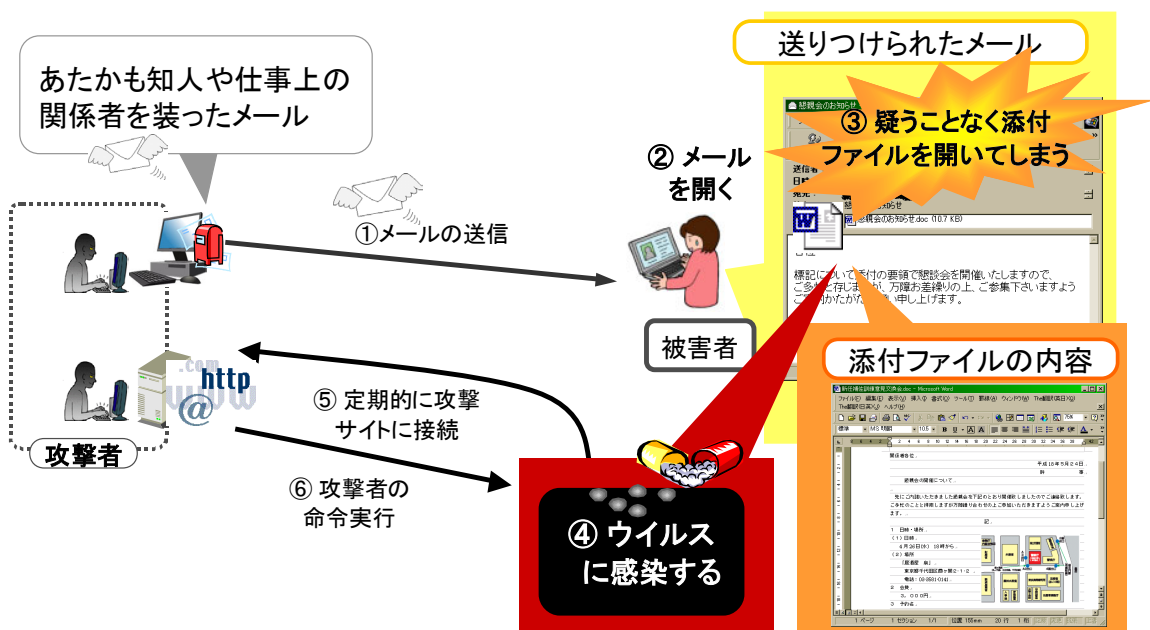


図 4.4 スピア型攻撃 (例)

5 安全・安心なインターネット社会への取組み

インターネットの情報セキュリティは予断を許さない情勢にあり、警察庁情報通信局情報技術解析課では、安全・安心なインターネット社会を目指して各種の取組みを推進しています。

5.1 重要インフラ事業者等との連携

サイバー攻撃が重要インフラに影響を与え、その機能が停止等した場合、国民生活や社会経済活動への多大な影響が考えられます。このような被害の発生の未然防止及び発生した際の被害の拡大防止並びに被疑者の検挙を実現するため、都道府県警察とともに、平素から、重要インフラ事業者等との連携のための様々な取組みを推進しています。

これら取組みの一環として、定期的な重要インフラ事業者等への個別訪問を実施し、情報セキュリティに関する助言や指導を行うほか、情報セキュリティセミナー等を通じて、国内外の情勢に関する講義や各種事例紹介等を行い、情報セキュリティ意識の向上に努めています。



18年には、重要インフラ事業者等の情報システムに対する DoS 攻撃事案について、攻撃を受けた被害システムのログ等の分析から攻撃手法を解明し、その対策方法を助言することで被害の再発防止を図るなどの対策を実施しています。また、サイバーテロ対処能力向上に向けた官民連携を深めるため、重要インフラ事業者等との共同訓練を実施しました。今後も引き続き共同訓練を積極的に実施していくこととしています。

5.2 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、情報通信分野の大学研究機関や企業等と協力し、犯罪捜査等に必要な技術情報の入手等に努めています。18年には、大学や企業と連携して、ファイアウォールのログの分析によるサイバー攻撃の予兆把握等に関する共同研究を実施したほか、米マイクロソフト社と情報共有のための機会を設けるなど、産学との連携強化を推進しました。

5.3 国際連携

サイバー犯罪に係る国際的な技術協力を進める上で、各国は、電磁的記録の解析手順や解析に使用するソフトウェア等について、必要な技術水準を確保していることが望まれます。そこで、各国の技術水準の向上のため、海外の法執行機関等との情報共有や人材育成のための国際連携を推進しています。

5.3.1 アジア地域におけるリーダーシップ

日本のリーダーシップにより、アジア大洋州地域の各国・地域のサイバー犯罪対策技術担当官が一堂に会する「アジア大洋州地域サイバー犯罪捜査技術会議」を開催しました。この会議では、サイバー犯罪対策に関する発表・討議、電磁的記録の解析に関する訓練を実施しています。

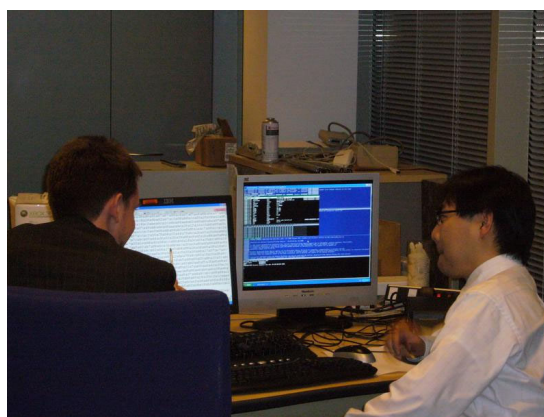
また、アジア地域のサイバー犯罪捜査技術の向上に寄与すべく、アジア地域における情報共有手段として、「サイバー犯罪技術情報ネットワークシステム」(CTINS⁹)を構築・運用しています。18年は、参加対象を大洋州地域にも広げ、新規に3か国1地域が加わり、12か国2地域が参加するネットワークとなっています。

さらには、国際刑事警察機構(ICPO)及び国際協力機構(JICA)と共に、ICPOアジア・南太平洋地域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を開催しました。

5.3.2 二国間の技術協力

多国間の技術協力のほか、二国間の技術協力も推進しています。5月に、英国の重大組織犯罪対策庁(SOCA¹⁰)電子犯罪部との間で、サイバー犯罪の防止及び取締りのための相互の協力を推進することを内容とする意図表明文書を作成・署名しました。

また、オランダ司法省のオランダフォレンジック研究所(NFI¹¹)やオランダ警察



⁹ Cybercrime Technology Information Network System

¹⁰ Serious Organised Crime Agency

¹¹ The Netherlands Forensic Institute

庁とデジタルフォレンジック¹²に係る取組状況について情報交換を行うなど、様々な国際的な技術協力関係の構築を推進しています。

5.3.3 FIRST との連携

6月に開催されたG8リヨン・グループとインターネット上の情報セキュリティ事案に対処することを目的とした組織の情報共有・連携の世界的枠組みであるFIRST¹³との合同ワークショップでは、サイバーフォースセンターの活動を報告するとともに、法執行機関とコンピュータセキュリティ事案対処チーム(CSIRT¹⁴)間の相互理解を深めるための議論を行い、情報セキュリティ事案への効果的な対処を可能とする連携のあり方について検討を進めています。

5.4 デジタルフォレンジックの確立に向けた取組み

コンピュータ、携帯電話等の情報通信機器が一般に普及し、あらゆる犯罪に悪用されるようになってきており、犯罪の取締りに当たっては、電磁的記録の解析が必要不可欠となっています。こうした状況を踏まえ、電磁的記録の解析に係る知見の集約・体系化、外国関係機関、民間企業等との技術協力を実施するなど、デジタルフォレンジックの確立に向けた取組みを推進しています。



¹² デジタルフォレンジックとは、犯罪の立証のための電磁的記録の解析技術及び手続きのことをいう。

¹³ Forum of Incident Response and Security Teams

¹⁴ Computer Security Incident Response Team