情報技術解析平成 23 年報

～平成 23 年中のインターネット観測結果等～

平成 24 年3月

警察庁情報通信局情報技術解析課

目次

平成 23 年中のインターネット観測結果等について

1 はじめに

警察庁では、国民生活や社会経済の活動に重大な影響を及ぼすおそれのある、情報システムに対する犯罪を未然に防止するとともに、発生時の被害の拡大を防止するために必要となる情報を収集する手段の一つとして、インターネット定点観測システム(注)（以下「定点観測システム」という。）を活用し、全国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・分析しています。

本資料は、一般の利用者を始めとした、インターネット利用者の情報セキュリティ対策の参考としていただくため、インターネットを利用していく上で発生するリスクについて、警察庁が定点観測システムで観測・分析した情報を含め、様々な方面から収集した情報を取りまとめて公表するものです。

本資料が、安全・安心なインターネット社会への取組の一助となれば幸いです。

注 ： 全国の警察施設（58 拠点）のインターネット接続点にセンサーを設置して、センサーに対するアクセスの状況を観測するシステム

2 概況

平成23年、定点観測システムで観測したアクセスは、一日・1IPアドレス当たり252.9件でした(注1)。これは、インターネット上の1つのコンピュータに対して、約5分 40 秒に1回の割合で不審なものを含むアクセスが行われていることを示しています。これを 22 年の観測結果である約4分 30 秒に1回の割合と比較すると、23 年のアクセスは減少しています。

一方で、23年中は、防衛産業関連事業者等に対する標的型メール攻撃、政府機関等のウェブサーバに対するDDoS攻撃事案が発生しました。さらに、ボットネットや意図しない動作をするソフトウェアの脅威も認知しています。

● 標的型メール攻撃

標的型メール攻撃とは、特定の組織や個人に電子メールを送信する手法によるサイバー攻撃(注2)であり、電子メールに不正プログラムが添付されていたり、電子メールの本文中に不正プログラムを感染させるような悪意のあるウェブサイトへ誘導するリンクが記述されていたりします。

防衛産業関連事業者等に対する標的型メール攻撃では、電子メールの件名には受信者に関係する会議や、時候のあいさつを装ったものなどが使われ、電子メールの本文には、時節に合った内容を記載して、巧みに添付ファイルを開かせようとするものが見られました。

警察では、標的型メール攻撃に関して、不正プログラムの動作実態の解明、被害の未然防止・拡大防止のための調査・分析を行うとともに、分析結果を提供元に還元し、事業者等の情報セキュリティ対策の充実・強化に資することにより、被害の未然防止・拡大防止を図りました。

● DDoS 攻撃(Distributed Denial of Service Attack、サービス不能攻撃)

本資料において、DDoS 攻撃とは、攻撃目標のサーバに対して、複数のサーバやパソコンから同時に大量のデータを送りつけ、その機能を停止させる電子的攻撃を指しています。

7月及び9月には、政府機関等のウェブサーバに対し、この DDoS 攻撃が行われる事案が発生しました。いずれの事案でも、海外に所在する大手検索サイトの掲示板等に、攻撃ツールを使用したサイバー攻撃を呼び掛ける記述がありました。

警察では、攻撃元である可能性が高い IP アドレスが所在する海外の捜査機関に対し、捜査協力要請とともに再発防止措置を依頼したほか、攻撃対象として指定された政府機関や、実際にウェブサイトの閲覧に支障が生じた政府機関に対し、DDoS 攻撃

注1:「情報技術解析平成 23 年報別冊」(@police) p. 6 ,
http://www.npa.go.jp/cyberpolice/detect/pdf/H23_betsu.pdf

注2: 情報通信ネットワークや情報システムを利用した電子的な攻撃

に関する注意喚起を実施しました。

● ボットネットの脅威

攻撃者が、不正プログラムに感染させ、意のままに操ることのできる状態にしたコンピュータはボットと呼ばれ、これを多数用意してネットワークを形成したコンピュータ群はボットネットと呼ばれ、DDoS 攻撃、迷惑メールの送信や感染したコンピュータからの情報窃取など、様々な攻撃活動に悪用されています。

警察は、23 年中に、日本国内にボットネットの指令サーバが所在することを認知し、当該指令サーバを停止させるとともに、指令サーバに仕立てられたコンピュータの管理者に対して、コンピュータが攻撃者に再び悪用されないよう、再発防止のための助言等を行いました。

● 意図しない動作をするソフトウェアの脅威

コンピュータの使用者が海外の動画共用サイトからダウンロードすると意図しない動作をして踏み台として利用できるソフトウェアを新たに認知しました。定点観測システムによる観測の結果、同ソフトウェアを探索していると見られるアクセスが昨年8月から増加しており、コンピュータの使用者が意図しないにもかかわらず、DDoS 攻撃、不正アクセス等の踏み台になるおそれがあるため、警察はインターネットを通じて注意を喚起しました。

3　標的型メール攻撃

政府機関や企業等、特定の組織からの情報窃取が目的とみられるサイバー攻撃事案が発生しています。平成 23 年は、防衛産業関連事業者等のコンピュータがサイバー攻撃を受け、不正プログラムに感染した事案が明らかになりました。このような攻撃によって、組織等の機微な情報が窃取されると、我が国の治安、外交や安全保障に重大な影響が生じるおそれがあります。

警察では、情報通信技術を用いた諜報活動（サイバーインテリジェンス）の手口の一つである「標的型メール攻撃」に関して、動作実態の解明、被害の未然防止・拡大防止のための調査・分析を行っています。

標的型メール攻撃とは、特定の組織や個人に電子メールを送信する手法によるサイバー攻撃であり、電子メールに不正プログラムが添付されていたり、電子メールの本文中に不正プログラムを感染させるような悪意のあるウェブサイトへ誘導するリンクが記述されていたりします（図3-1）。

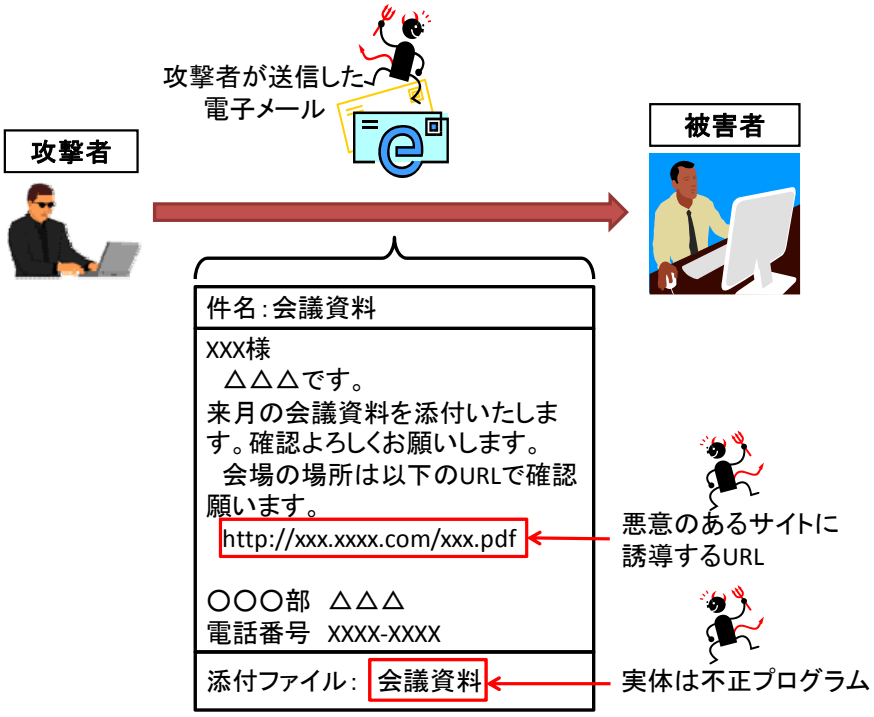


図3-1　標的型メール攻撃の一例

電子メールの受信者が、添付された不正プログラムを実行したり、悪意のあるサイトに誘導されたりすることで、市販のウイルス対策ソフトでは検出できない不正プログラムに感染し、組織等の機微な情報を窃取されることがあります（図3-2）。

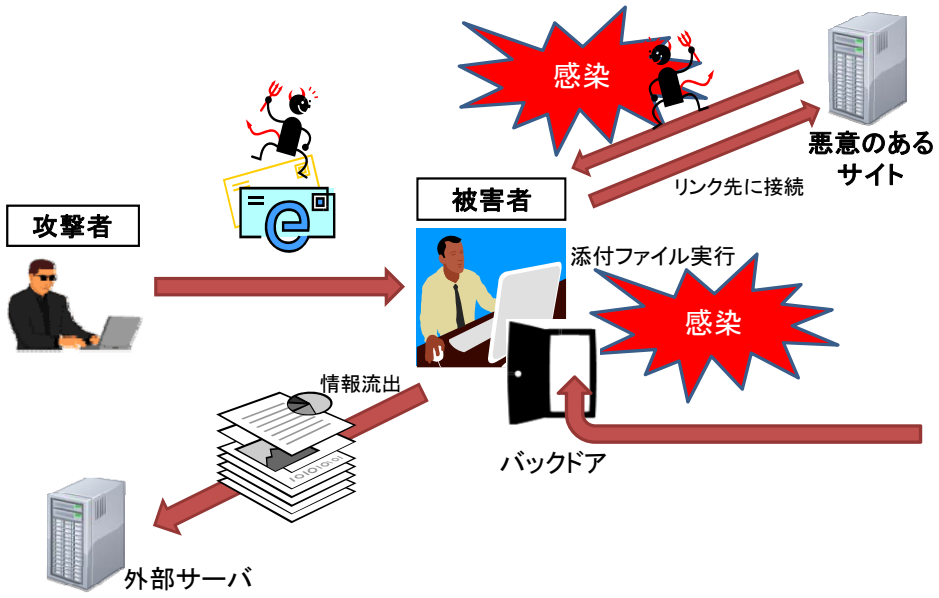


図3-2　標的型メール攻撃の概要

標的型メール攻撃は、一見しただけでは正当なメールと区別がつかないよう工夫されており、電子メールや添付ファイルを受信者に開かせるために、知人や関係者を装って送付したり、関心を誘う件名を付けたりするなど、巧妙な手法が使われます。また、市販のウイルス対策ソフトでは検出できない不正プログラムが添付されているため、電子メールの受信者は攻撃を受けたことに気付かず、被害の拡大に繋がってしまう可能性があります。

3.1 標的型メール攻撃の事例等

ここでは、警察が分析した、主に政府機関や防衛産業関連事業者等に対して行われた標的型メール攻撃に関する事例等を紹介します。

標的型メール攻撃で用いられる電子メールの件名には、受信者に関係する会議や、時候のあいさつを装ったものなどが使われ、件名だけで標的型メール攻撃によるものか否かを見分けることは困難です。特に、本年は時事的関心が寄せられている、東日本大震災や原子力発電所の事故に関係する件名も見られました。

以下に件名の事例を挙げます。

- 「会議出席報告」
- 「歓迎会のお知らせ」
- 「被災者の皆様、とくにお子さんをお持ちの被災者の皆様へ」
- 「需要逼迫による計画停電の実施」

また、標的型メール攻撃で用いられる電子メールの本文には、時節に合った内容を記載して、巧みに添付ファイルを開かせようとするものが見られました（事例1～事例4）。

これらの中には、本文の一部に、日本では使用されない漢字が含まれていたり、不自然な日本語の表記が含まれたりした事例がありました（事例3、事例4）。

事例1　歓迎会の開催を呼びかけ、添付ファイルを開かせようとするもの

各位 **お元気ですか。 今度歓迎会を開くことになりました。 詳しくは添付ファイルをご覧ください。**
添付ファイル：歓迎会.zip

事例2　資料送付を装って添付ファイルを開かせようとするもの

■■ ●●様 **プライベートアドレスよりの送信にて失礼致します。 ご請求いただいた資料を発送いたしました。 ご確認するようお願いします。**
添付ファイル： 2011_08.doc

事例3　時候のあいさつを装って添付ファイルを開かせようとするもの
（不自然な表記があるもの）

■■　様 **旧年中は、ご交誼を賜りまして□ありがとう存じました□。なにとぞ本年もよろしくお願い申し上げます。 平成 24 年の新春の際、新年のよろこびを申上げます。また、□クリスマスを楽しく過ごすようにお祈りします□。**
添付ファイル： MERRY_CHRISTMAS.pdf

事例4　時候のあいさつを装って添付ファイルを開かせようとするもの
（不自然な表記があるもの）

■■　様 **新年あけましておめでとうございます。 ▲▲の●●です。 旧年中は大変お世○話になりました。今年もよろしくお○願いいたします。ご健康とご多幸を祈り申し上げます。 添付のとおり、作成した平成 24 年の□かレンダ□ーを送付致します。 ご査収のほど宜しくお願い致します。**
添付ファイル： 2012 calendar.pdf

凡例　○－日本では使われない漢字　　□－不自然な日本語の表記

標的型メール攻撃では、電子メールの送信元に、官公庁のドメイン名を用いた偽装メールアドレスが使われていたものもありました。そのため、送られてきた電子メールの送信元アドレスに使われているドメイン名だけでは、標的型メール攻撃によるものか否かを見分けることは困難です。

警察で分析した標的型メール攻撃に使用されていた不正プログラムには、次のような傾向が見られました。

ファイル形式を見ると、約半数が実行形式のファイルでした。それ以外では、WORD ファイルや PDF ファイル等の文書形式のファイルが、そのほとんどを占めています（図3-3）。

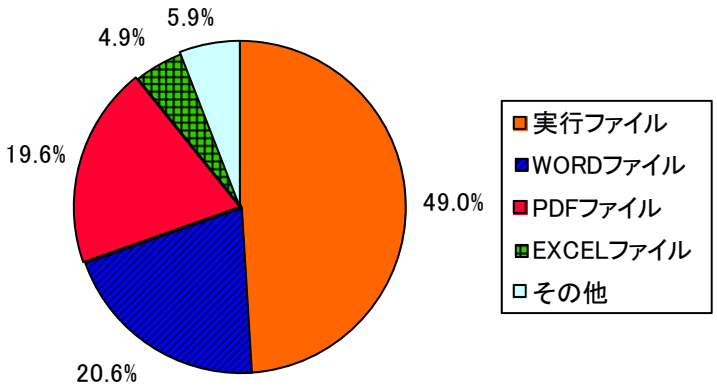


図3-3　不正プログラムのファイルの種類

中には、不正プログラムをパスワード付きの圧縮ファイルとして電子メールに添付し、そのパスワードを電子メールの本文に記載した事例がありました。この場合、メールサーバ等でウイルスチェックを行っていても、パスワード付きの圧縮ファイルの内容を確認することができないため、チェックをすり抜けてしまいます。このような電子メールを受信した利用者は、本文に記載されたパスワードを使って、圧縮された不正プログラムを開いてしまうと、その不正プログラムに感染してしまいます。また、「RLO（Right-to-Left Override）(注)」と呼ばれる機能を使用して、実行形式のファイルを WORD ファイルや PDF ファイル等に見せかけて添付するという、巧妙な手口もありました。

注 ： アラビア語等に対応するため、RLO ファイル名を右読みから左読みに変える機能で、例えばファイル名「fdp.exe」に RLO を使用すると「exe.pdf」と表示することが可能になり、実行ファイルを PDF ファイルのように偽装させることができます。

不正プログラムの動作を見ると、そのほぼすべてが、感染したコンピュータからインターネット上のコンピュータへの接続を試みるものでした（図3-4）。その際に、感染したコンピュータのIPアドレス、OS名やコンピュータ名等を取得し送信を試みるものも確認しています（図3-5）。また、感染した不正プログラムが取得したデータを暗号化したファイルとして保存した上で、インターネット上のコンピュータに送信を試みるものもありました（図3-6）。

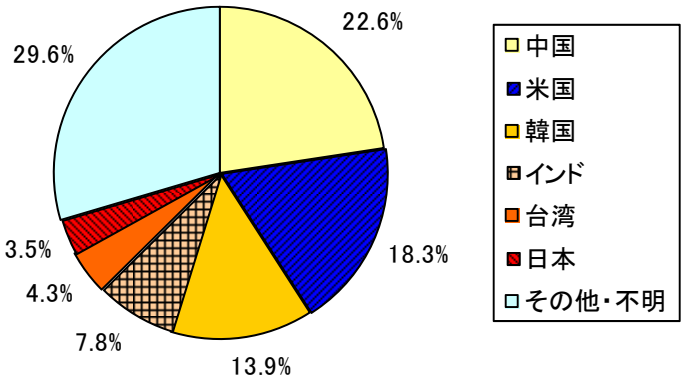


図3-4　不正プログラムの外部接続先

```
:h786 Na me:user-
67a51472 2b IP:19
2.168.13 6.40 os:
xPSP3
```

図3-5 外部へ送信されたデータの例

```
.ZF.....Hp.p=b8
JVO@..VOP,¥Ae2ID
¥X.^+V%Bebk@DMOK
:7Wz.+Rdn~wni).y
3I..]T..',1...Q.
```

図3-6 不正プログラムが取得したデータを暗号化したファイルとして保存していた例

3.2 推奨する対策

標的型メール攻撃による被害を完全に防止することは極めて困難です。しかし、次に掲げる対策は、標的型メール攻撃による被害の防止に有効です。

一般のインターネット利用者向けに推奨する対策を示します。

- 一部でも不審に感じる点があるメールは開かないことを原則とし、やむを得ず開く必要がある場合には、送信者への電話等による確認を行う。また、組織にあっては、システム管理者への相談や報告等の手続きを明確にし、徹底する。
- メールや添付ファイルを開いた後に、パソコン操作に対する応答が一時的に急に遅くなった、添付ファイルのアイコンが変化したなど、少しでも不審な動作があった時には、直ちにシステム管理者に報告する。
- 使用している OS やアプリケーションには、最新の更新プログラムを適用する。
- ウイルス対策ソフトのパターンファイル等を定期的に更新して最新の状態に保つとともに、ウイルス対策ソフトが正常に動作していることの確認や、全ファイルのウイルスチェックを定期的に行う。

また、管理者向けに推奨する対策を示します。

- ルータやファイアウォール等のログを定期的に確認し、不審な通信の有無を確認する。
- SPF（Sender Policy Framework）(注)等の送信ドメイン認証技術を導入し活用する。

3.3 警察の対応

警察では、防衛産業関連事業者等に対する標的型メール攻撃に関し、標的型メール攻撃に使用された不正プログラムに関する分析を行うとともに、分析結果を提供元に還元し、事業者等の情報セキュリティ対策の充実・強化に資することにより、被害の未然防止・拡大防止を図りました。また、サイバー攻撃の標的となるおそれのある事業者等やウイルス対策ソフト提供事業者等を始め、海外の治安機関との連携を強化するとともに、多くのコンピュータ利用者にインターネット等を通じて情報提供し、社会全体の情報セキュリティの向上に努めています。

注 ： メールの送信元アドレスの偽装を識別する技術の一つ

4 DDoS 攻撃等

国内では、平成 23 年7月に、警察庁のウェブサーバに対する「DDoS 攻撃」事案が発生しました。本資料において、DDoS 攻撃（Distributed Denial of Service Attack、サービス不能攻撃）とは、攻撃目標のサーバに対して、複数のサーバやパソコンから同時に大量のデータを送りつけ、その機能を停止させる電子的攻撃を指しています。同年9月には、日本の政府機関や民間企業のウェブサーバに対する DDoS 攻撃やウェブページ改ざん事案が発生しました。事案発生時には、警察庁で運用している定点観測システムによって、攻撃対象とされたウェブサーバからの SYN-flood 攻撃(注1)を受けている可能性を示す跳ね返りパケット(注2)等を認知しました。また、海外で発生した事案では、3月に韓国政府機関等に対する DDoS 攻撃について把握しております。

4.1 DDoS 攻撃の事例等

平成 23 年7月 10 日から 11 日にかけて、警察庁のウェブサーバに対する DDoS 攻撃事案が発生しました。その後、警察庁が調査したところ、中国の大手検索サイトの掲示板に、7月4日の尖閣諸島における航空自衛隊の中国偵察機に対する緊急発進のニュース内容とともに、攻撃ツールを使用して日本へのサイバー攻撃を呼び掛ける記述があり、警察庁ウェブサイトが攻撃目標に指定されていたことが判明しました。ここには、攻撃に使用するソフトウェアのダウンロード先や、攻撃ツールの使用方法を説明する動画へのリンク先も、記述されていました（図4-1）。

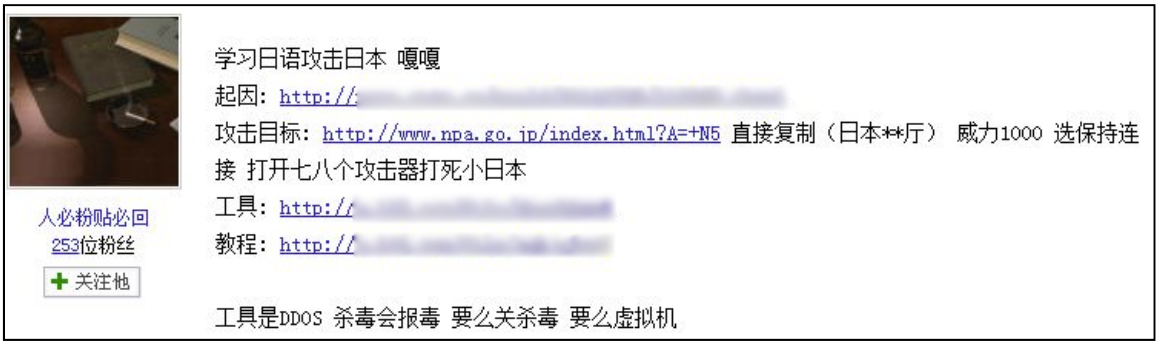


図4-1　中国の大手検索サイトの掲示板に記述された内容

注1：「SYN flood 攻撃被害観測システムについて 2 章 SYN flood 攻撃」（@police） p. 2, http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/synflood_detect.pdf

注2：DDoS 攻撃の際、攻撃者の判別を困難にするために、発信元を不特定多数の IP アドレスに詐称することが多く、被害サーバはこの詐称された IP アドレスに対し、応答パケットを返信します。この応答パケットを「跳ね返りパケット」と呼んでいます。

攻撃を受けた期間について、警察庁ウェブサーバのアクセスログを分析した結果、攻撃ツールを使用したリロード攻撃が主になされており、他にも、通常の閲覧では発生しない特定の URL への不審な閲覧要求が過剰になされていたこと、複数の攻撃ツールが使用されていた模様であることがわかりました。

これらの攻撃によって、警察庁ウェブサイトの閲覧に支障が生じていました。

23 年9月 12 日から 18 日にかけて、警察庁では、中国大手チャットサイト等で、9月 18 日に日本の複数の政府機関等に対するサイバー攻撃を実施する旨の呼び掛けが記述されていることを把握していました。そこには、サイバー攻撃を行う期間、攻撃に使用するソフトウェアのダウンロード先等が記述されていました(図4-2)。

図4-2 攻撃ツールダウンロード先 URL、攻撃対象の記述

警察庁では、定点観測システムにより、攻撃対象とされたウェブサイトに関する観測を強化しました。その結果、予告された攻撃期間に、DDoS 攻撃被害の可能性を示す跳ね返りパケットを検知しました(表4-1)。さらに、攻撃対象とされたウェブサイトの閲覧に支障が生じたことを確認しました(表4-2)。

表4-1 跳ね返りパケット検知状況

機関	検知期間	検知回数
金融機関A	9月 15 日 14:50 頃～14:59 頃	101 回
政府機関B	9月 18 日 20:06 頃～20:33 頃	5回

表4-2 閲覧に支障が生じた状況

機関	閲覧に支障が生じた期間
政府機関C	9月 17 日 20:45 頃～21:00 頃、 9月 18 日 20:55 頃～21:15 頃
政府機関D	9月 18 日 13:50 頃～16:10 頃、 9月 18 日 21:00 頃～21:15 頃
政府機関E	9月 18 日 21:05 頃～21:15 頃

23 年3月3日から5日にかけては、韓国政府機関等の 40 のウェブサイトに対するDDoS 攻撃が行われ、一部のウェブサイトの閲覧に支障が生じました。

この攻撃に関して、日本国内で発見された攻撃の踏み台となっていたコンピュータのうち1台は、何者かによって攻撃指令サーバに仕立てられた家庭用として使用していたパーソナル・コンピュータであり、意図せずにサイバー攻撃に加担していたとみられます。

4.2 推奨する対策

警察庁の定点観測システムでは、日常的に世界各地からの多くの跳ね返りパケットを観測しており、DDoS 攻撃が頻繁に行われていることがうかがえます。特に、平成 23 年は、22 年に比べ DDoS 攻撃被害の観測が約3倍に増えており（図4－3）、日本国内に限定すると約 60 倍に増加していました(注)（図4－4）。

今後は、DDoS 攻撃が行われることを前提に、サーバの管理者、一般利用者それぞれが対策を行うことが重要です。

サーバの管理者の方に平時から推奨する対策を示します。

- 攻撃を想定した、リソースに余裕のあるシステムの構築
- 平素の稼働状況の把握
- 攻撃を受けた際の対応に係る事前の検討

また、攻撃を受けた際に推奨する対策を示します。

- 攻撃元からアクセスや平素と異なる不審なアクセスについて、自ら設置したネットワーク機器や上位プロバイダによるアクセス遮断の検討
- ログ等の確認と分析による効果的な対策の検討

なお、攻撃を受けた際、次の対策が有効な場合もあります。

- 攻撃元IPアドレスの主な所在国が判明した場合には、当該国に割り当てられた IP アドレス帯域からの全アクセスの遮断
- 単一のコンピュータからの極めて頻繁なアクセスの遮断
- プロキシサーバ（中継サーバ）を経由したアクセスの遮断

一般利用者が不正プログラムに感染し、意図せず DDoS 攻撃に加担させられないために推奨する対策を示します。

- 使用している OS やアプリケーションには、最新の更新プログラムを適用する。
- ウイルス対策ソフトのパターンファイル等を定期的に更新して最新の状態に保つとともに、ウイルス対策ソフトが正常に動作していることの確認や、全ファイルのウイルスチェックを定期的に行う。

サイバー攻撃への参加の呼び掛けがなされることもありますが、犯罪行為に該当する可能性や事件に巻き込まれるおそれもあるので絶対に参加しないでください。

注 ：「情報技術解析平成 23 年報別冊」(@police) pp. 27 -29 ,
http://www.npa.go.jp/cyberpolice/detect/pdf/H23_betsu.pdf

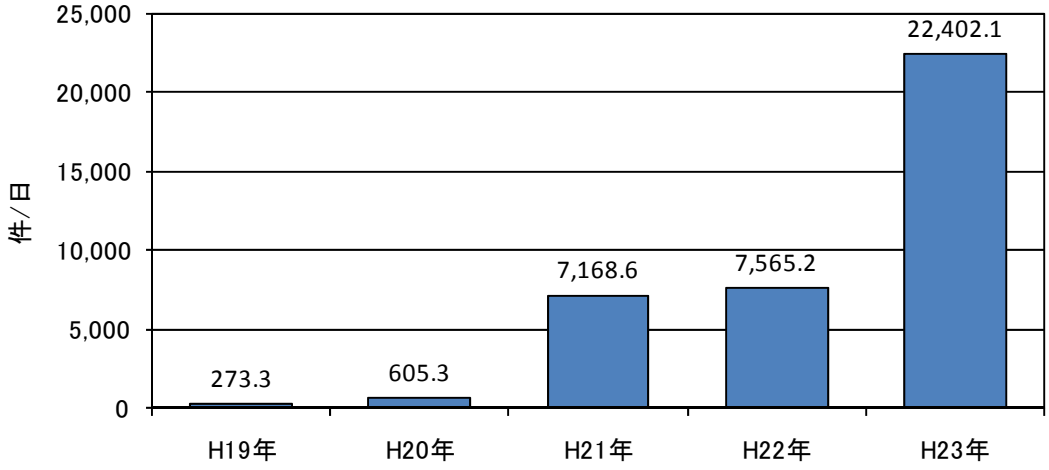


図4-3 DDoS 攻撃被害の観測件数(世界)(注)

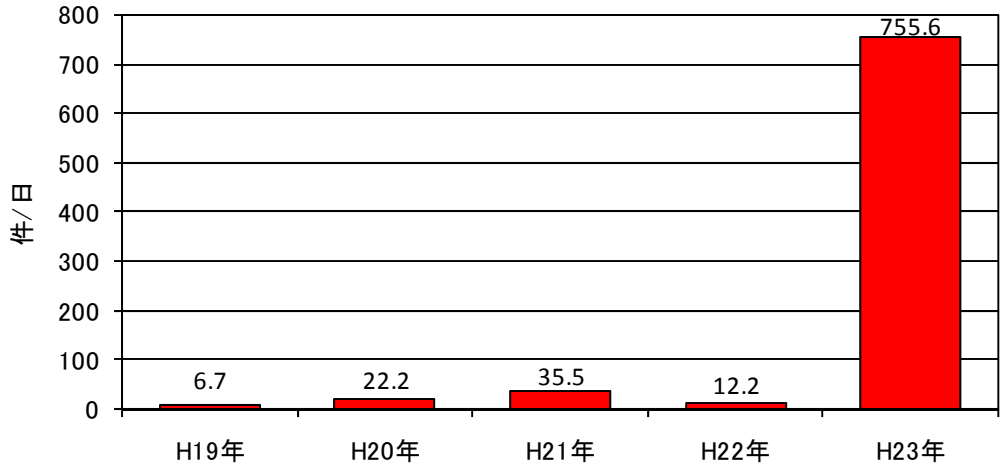


図4-4 DDoS 攻撃被害の観測件数(日本)(注)

注: 定点観測システムの観測拠点数が、平成 21 年3月より前は 57 拠点だったが、平成 21 年3月以降は 58 拠点になった。

4.3 警察の対応

警察は、7月に発生した DDoS 攻撃、9月に発生した DDoS 攻撃及び3月に発生した韓国政府機関に対する DDoS 攻撃について、次の対応をしました。

7月に発生したDDoS攻撃について、攻撃を受けたウェブサーバのアクセスログを分析し、攻撃元である可能性が高いIPアドレスを抽出し、これらIPアドレスの所在を調査したところ、そのすべてが海外所在のものであることが判明しました。このため、ICPOを通じ、それぞれの国の捜査機関に対し、捜査協力要請を行うとともに再発防止措置を依頼しました。

9月に発生した DDoS 攻撃について、警察では、攻撃対象として掲示されたウェブサイトに対する観測態勢を強化するとともに、攻撃に関する情報を収集し、内閣官房と連携して、攻撃対象として指定された政府機関や、実際にウェブサイトの閲覧に支障が生じた政府機関に対し、DDoS 攻撃に関する注意喚起を実施しました。

さらに、DDoS 攻撃等の被害が生じた事業者等に対し、必要な対処について助言するなどの被害拡大防止措置を講じました。

3月に発生した韓国政府機関に対する DDoS 攻撃では、事業者等がサーバとして使用しているコンピュータだけでなく、家庭用のパーソナル・コンピュータも、攻撃指令サーバに仕立てられていたとみられることから、企業・業界団体のみならず、個人利用者に対しても、家庭用のパーソナル・コンピュータであっても大規模な攻撃に利用される可能性があることを踏まえた注意喚起を行うとともに、ウイルス対策ソフトの適切な導入等の情報セキュリティ対策に関する広報啓発活動を推進しました。

5 ボットネットの脅威

攻撃者が、不正プログラムに感染させ、自らの意のままに操ることのできる状態にしたコンピュータを「ボット」と呼びます。コンピュータをボット化する不正プログラムは、コンピュータ上で稼働している OS やアプリケーションの脆弱性を悪用するなどして、ネットワークを通じて、次々と他のコンピュータに感染を広げるものや、別の不正プログラムがコンピュータをボット化する不正プログラムをダウンロードさせ実行させることにより感染させるものがあります。多数のボット化したコンピュータがネットワークを形成したものを「ボットネット」と呼び、攻撃者からの指令によって、これらは一斉に操作できる状態になります。

ボットネットを操作する攻撃者は、攻撃者の命令を一斉にボットに伝達する「指令サーバ」と呼ばれるコンピュータに対して、攻撃の指令を出します。すると指令サーバは、ボットネットを構成している各コンピュータに対して、攻撃者からの指令を伝えます。指令サーバからの指令を受けた各コンピュータは、DDoS 攻撃、迷惑メールの送信や感染したコンピュータからの情報窃取など、様々な攻撃活動に悪用されています（図5-1）。

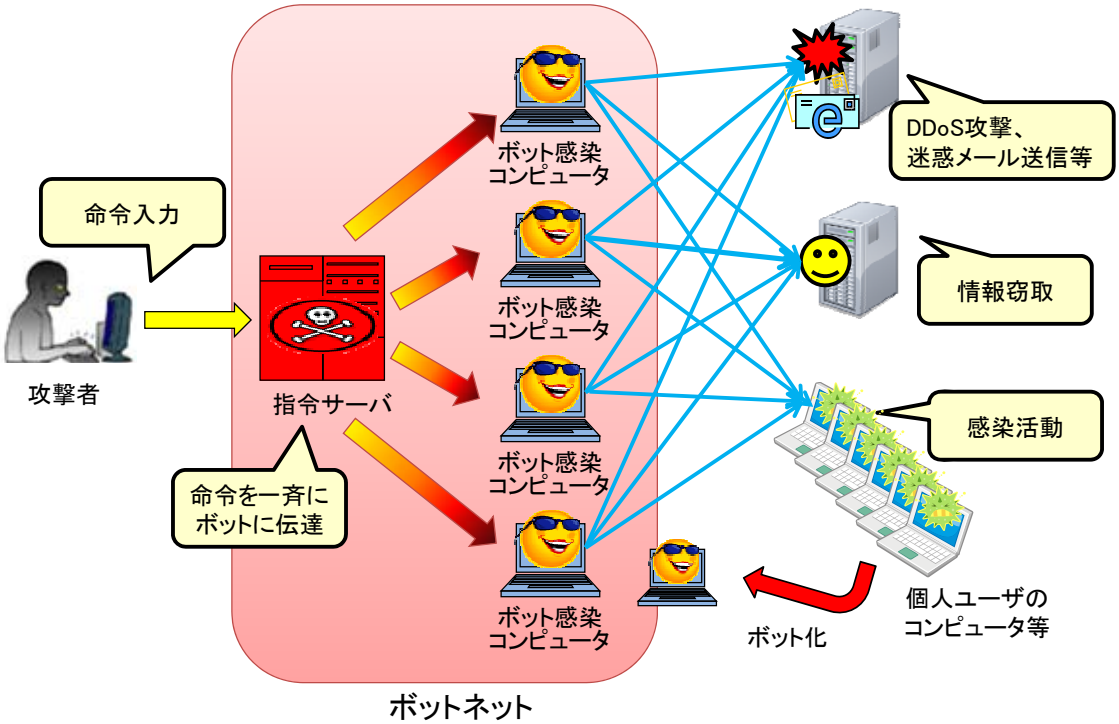


図5-1　ボットネットを悪用した様々な活動

5.1 ボットネットの事例等

警察庁で運用している、インターネット上の指令サーバの稼働状況等を観測するボットネット観測システムによる平成 23 年の観測数は、22 年より減少しました（図5-2）。また、23 年中に、日本国内に2個のボットネットの指令サーバが所在することを認知しました。このうちの一つは、自社を紹介するウェブサイトを開設したウェブサーバが、不正プログラムに感染し、指令サーバとしてボットネットを構成していることを確認しました。

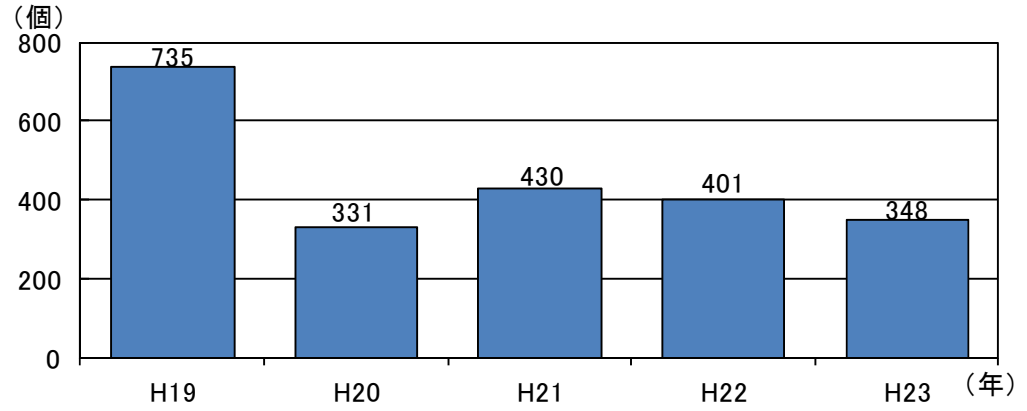


図5-2 ボットネット観測数

5.2 推奨する対策

コンピュータが、不正プログラムによって、ボットや指令サーバに仕立て上げられないようにするためには、次に掲げる対策が有効です。

一般のインターネット利用者向けに推奨する対策を示します。

- 使用している OS やアプリケーションには、最新の更新プログラムを適用する。
- ウイルス対策ソフトのパターンファイル等を定期的に更新して最新の状態に保つとともに、ウイルス対策ソフトが正常に動作していることの確認や、全ファイルのウイルスチェックを定期的に行う。
- パーソナルファイアウォール等を利用し不審な通信を遮断する。

5.3 警察の対応

警察庁では、ボットネット観測システムを運用し、ボットネットの実態把握に努めています。この観測を通じ、日本国内にボットネットの指令サーバが所在することを認知した場合、警察は、指令サーバを停止させ、ボットネットによる被害拡大防止措置を実施しています。

さらに、指令サーバとして仕立てられたコンピュータの管理者に対しては、コンピュータが攻撃者に再び悪用されないよう、再発防止のための助言等を行っています。

6 意図しない動作をするソフトウェアの脅威

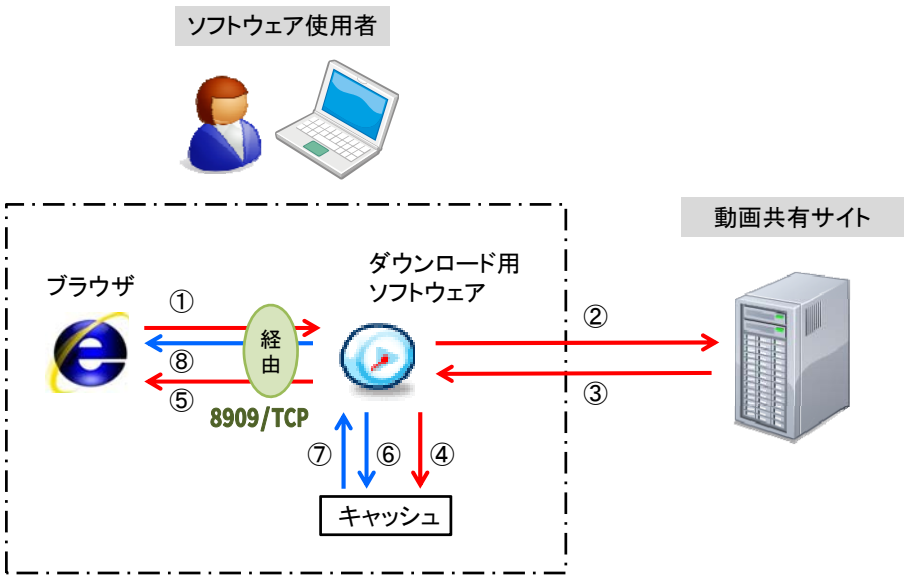
コンピュータの使用者が、海外の動画共有サイトからダウンロードすると、同使用者が意図しないにもかかわらず、公開プロキシサーバとして動作する動画ダウンロードソフトを認知しました。

公開プロキシサーバは、アクセスの中継をするサーバで公開されているものをいいますが、DDoS 攻撃や不正アクセスをするときの踏み台として使用が可能なものです。

同ソフトウェアにアクセスするためには、ポート 8909/TCP を使用しますが、定点観測システムによる観測の結果、平成 23 年8月以降、同ポートへのアクセスが増加しており、同ソフトウェアを探索しているものと思われます。

6.1 意図しない動作をするソフトウェアの事例

中国の動画共有サイトからダウンロードできる動画ダウンロードソフトウェアが、使用者が意図しないにもかかわらず、アクセス等を中継する公開プロキシサーバとして動作する機能を有することを分析して確認しました。同ソフトウエアは、ポート 8909/TCP を使用することも判明しています（図6-1）。



閲覧対象コンテンツが、キャッシュに無い場合、①～⑤の順

閲覧対象コンテンツが、キャッシュに有る場合、①、⑥、⑦、⑧の順にリクエストや応答が行われる。

図6-1 公開プロキシサーバとしての動作

一方、定点観測の結果、平成 23 年8月以降、ポート 8909/TCP に対するアクセスが増加したことを認知しました（図6-2）。

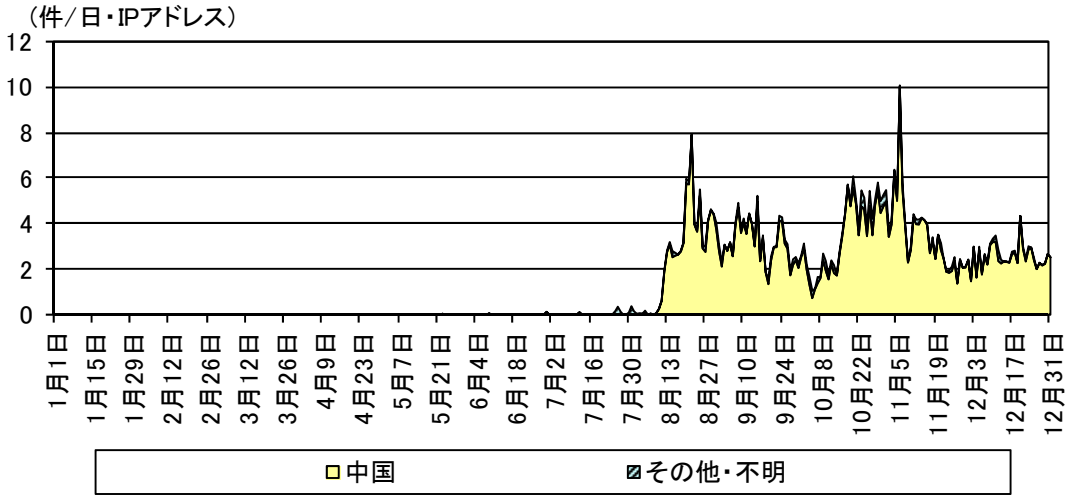


図6-2　8909/TCP に対するアクセスの推移

また、これらアクセスの内には、インターネット上に公開された外部サイトに対するリクエストが含まれていました（図 6-3）。

```
Internet Protocol Version 4, Src: [redacted] ([redacted]), Dst: [redacted]
Transmission Control Protocol, Src Port: 1449 (1449), Dst Port: 8909 (8909), Seq: 23
Hypertext Transfer Protocol
⊞ GET http://[redacted]/ HTTP/1.1\r\n
  Host: [redacted]\r\n
  Accept: */*\r\n
  Pragma: no-cache\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)\r\n
  \r\n
```

図6-3　8909/TCP に送信された外部サイトのデータをリクエストするパケット

これまでも、この現象については類似の機能を有し、サービスにポート 9415/TCP を使用する別の動画ダウンロードソフトウェアについて認知しており、インターネット上で公開プロキシサーバを探索しているものと推測されます。

なお、9415/TCP のアクセスは減少しており、探索対象の移行が推測されます（図6-4）。また、アクセス元の IP アドレスを分析したところ、そのほとんどが中国所在の IP アドレスでした。

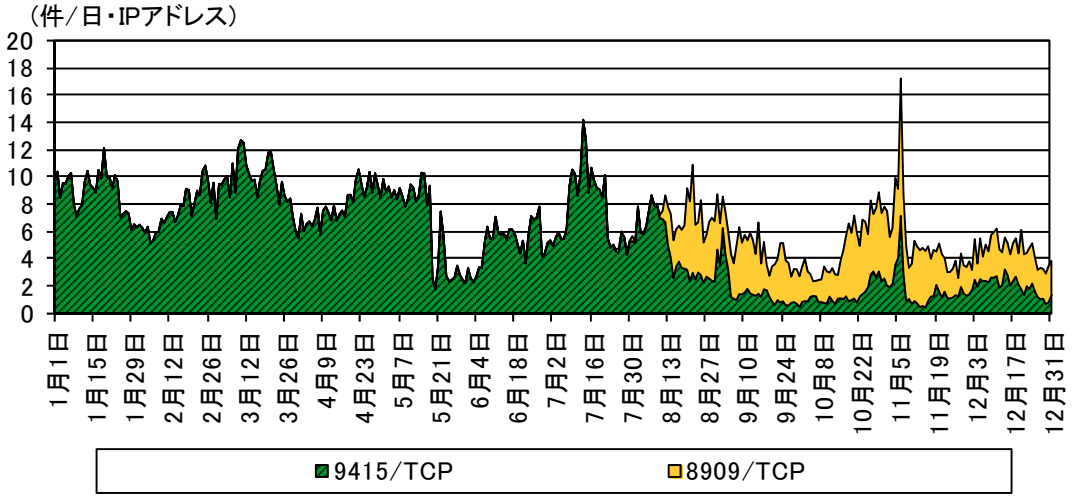


図6-4　9415/TCP から 8909/TCP への遷移

6.2 推奨する対策

パーソナル・コンピュータを、攻撃者に踏み台として利用されないために推奨する有効な対策を示します。

- 機能が明確でないソフトウェアを不用意に使用しない。
- 必要がなければ、公開プロキシサーバとして動作するソフトウェアを使用しない。
- ルータやファイアウォール、セキュリティ対策ソフトを利用して、外部ネットワークからの接続を制限する。

6.3 警察の対応

公開プロキシサーバは、踏み台として悪用されると、攻撃の加害者とみなされるおそれがあります（図6-5）。警察は、これら、動画ダウンロードソフトについて、いずれもサイバー攻撃に悪用される可能性があることから、インターネット等を通じて情報提供を行いました。

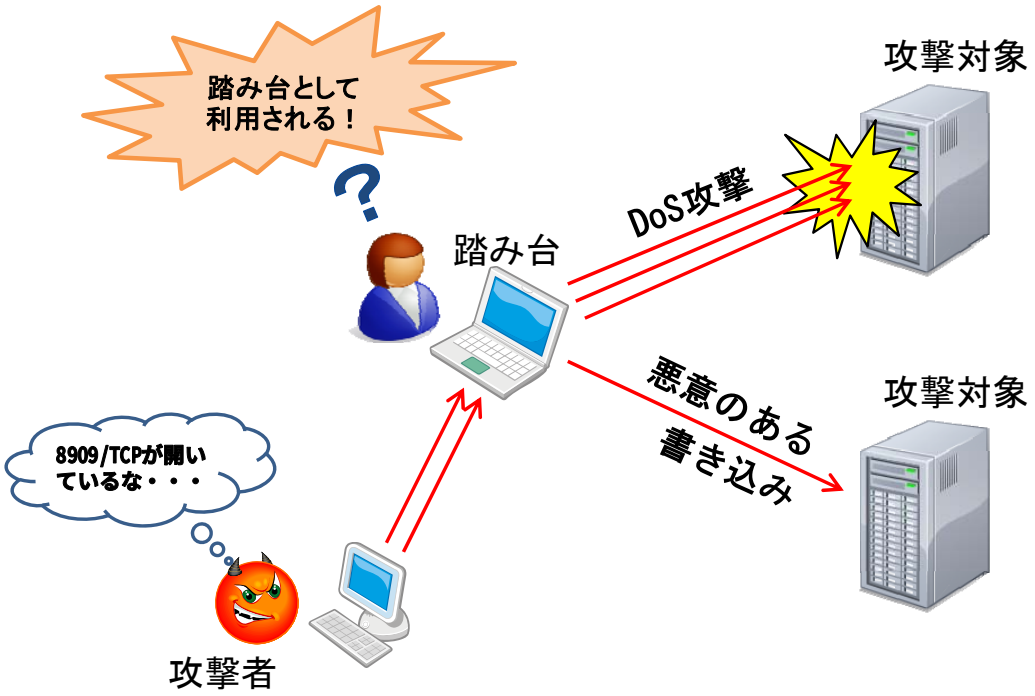


図6-5　公開プロキシサーバを利用した攻撃