情報技術解析平成 21 年報

～平成 21 年中のインターネット観測結果等～

平成 22 年3月

警察庁情報通信局情報技術解析課

目次

平成 21 年中のサイバーフォースセンターでの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（以下「定点観測システム」と言います。）により、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、サーバの管理者を始め、インターネット利用者の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、警察庁が様々な方面から収集した情報や、前述の観測・分析により把握した情報を取りまとめて公表するものです。

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。

2 概説

平成 21 年は、攻撃手法の巧妙化が進み、米国及び韓国への大規模なサイバー攻撃、いわゆる「ガンブラー」と呼ばれる不正プログラムに関係した攻撃手法（以下「ガンブラー攻撃」と言います。）によるウェブサイト改ざん被害、Conficker ワームの感染拡大など、大きな脅威が顕在化しました。

平成 21 年7月7日から9日にかけて、米国及び韓国の政府機関など 35 機関のウェブサイトが、3次にわたる DDoS 攻撃[1]を受けるという、大規模なサイバー攻撃が発生しました。警察庁では、このサイバー攻撃の影響とみられる通信を検知しています。今回のサイバー攻撃では、検知した通信の種類から、複数の攻撃手法が用いられたと考えられます。

平成 21 年5月頃から、「ガンブラー攻撃」による、ウェブサイトの改ざん被害が発生しています。「ガンブラー攻撃」における改ざんでは、一般利用者が改ざんされたウェブサイトを閲覧すると気付かないうちに特定のサイトへ誘導され、不正プログラムに感染するおそれがあります。特に、ウェブサイト管理者が感染することでウェブサイト改ざんの連鎖が起こり、被害の拡大につながっています。

平成 20 年 11 月下旬から流行している Conficker ワームの感染拡大が、平成 21 年も継続したと考えられます。警察庁でも、Conficker ワームの影響と考えられる通信の増加を確認しました。

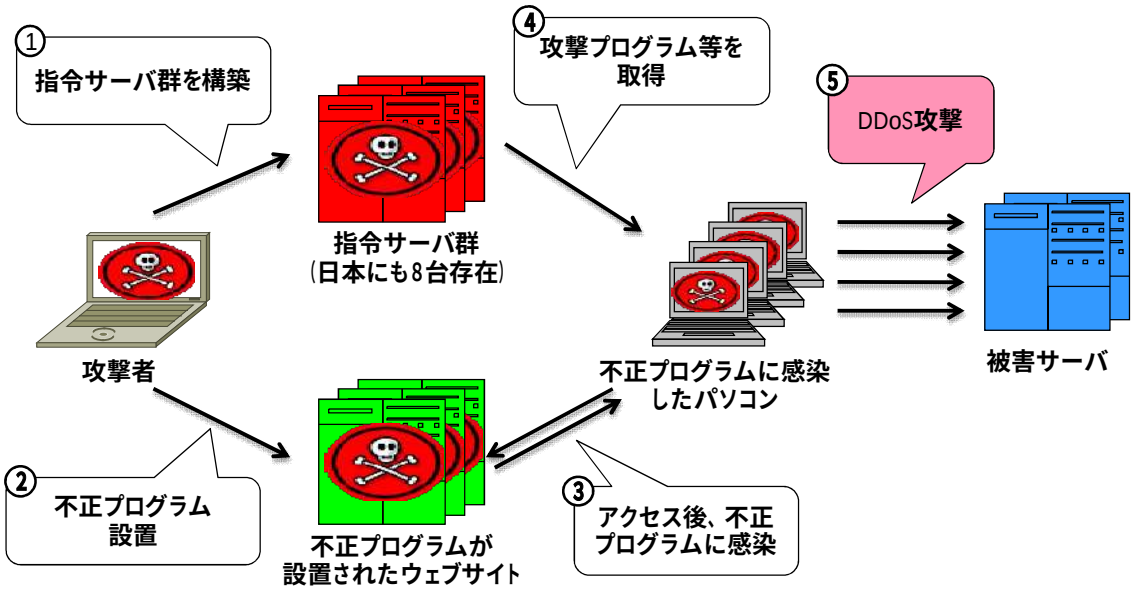
[1] Distributed Denial of Service。多数のコンピュータを使用して、ウェブサイトにアクセスを集中させて、その機能を麻痺させる攻撃のことです。

3 米国･韓国に対するサイバー攻撃

3.1 概要

平成21年7月7日から9日にかけ、米国及び韓国の政府機関等35機関のウェブサイトが、3次にわたるDDoS攻撃を受けて、一時閲覧不能になりました。

この攻撃は、大規模なボットネットを構築した上で、あらかじめ指定した時刻に、DDoS攻撃を実行したものです。（図3-1）



① 攻撃者がコンピュータに侵入し、「指令サーバ群」を構築。
② 攻撃者がウェブサイトに侵入し、不正プログラムを設置。
③ パソコン利用者が②のウェブサイトにアクセスし、不正プログラムに感染。
④ 不正プログラムに感染したパソコンが「指令サーバ群」から最新の攻撃プログラム等をダウンロード。
⑤ 感染したパソコンが、指定された時刻に攻撃対象に対して自動的にDDoS攻撃を実行。

図3-1 ボットネットによる大規模なDDoS攻撃

警察庁では、韓国当局と連携し、今回の攻撃に関する情報収集を行い、我が国所在のものとして、攻撃指令を行うサーバ8台を把握するとともに、これらのサーバの一部から攻撃に使用されたと思われる不正プログラムを検出しました。

3.2 警察庁における検知状況

韓国のウェブサイトが大規模なサイバー攻撃を受けたとされる時間に、警察庁では、韓国の特定のサイトから、サイバー攻撃の影響とみられる通信を定点観測システムで検知しました。（図3-2）

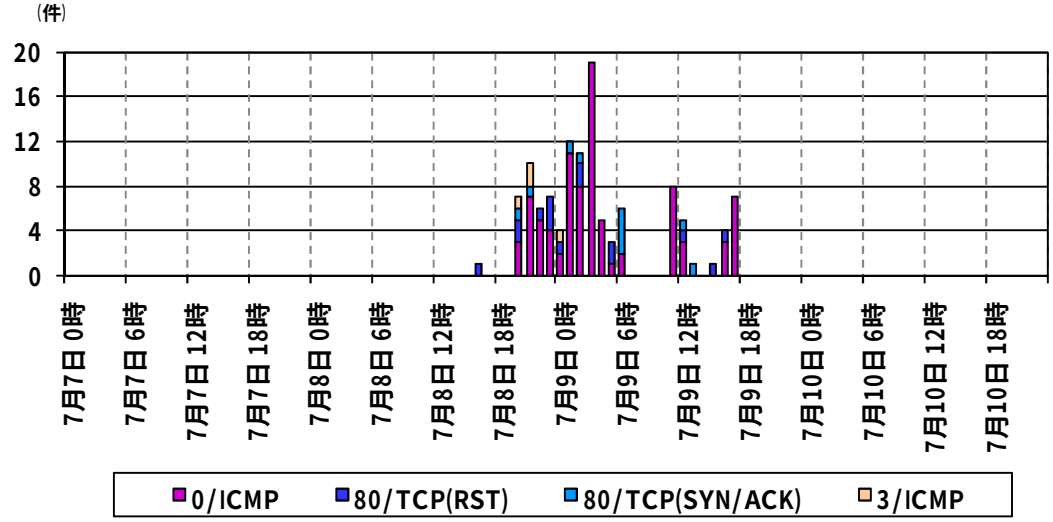


図3-2　韓国を発信元とする通信の検知状況

表3-1　今回検知した通信とDDoS攻撃の種類

通信の種類	推測されるDDoS攻撃の種類
0/ICMP	PING flood
80/TCP(RST)、80/TCP(SYN/ACK)	SYN flood (80/TCP)
3/ICMP	UDP flood (80/UDP)

警察庁の観測で検知された通信は3種類でした。（表3-1） これらの通信から、今回のサイバー攻撃は、複数の手法によるDDoS攻撃であると考えられます。

3.3 コンピュータのセキュリティ確保

今回の攻撃において、多くのパソコンが不正プログラムに感染した原因については、韓国国内のファイル共有サービス等を提供するサイトが配布する、専用ソフトウェアの更新プログラムが書き換えられ、この書き換えられたプログラムをダウンロードした一般利用者のパソコンが不正プログラムに感染したと言われています。

こうしたプログラムのインストールに際しては、パソコンにインストールされているソフトウェアやウイルス対策ソフトを最新の状態にするなどの自衛策を講じて下さい。また、こうしたプログラムを配布するサイトの管理者にあっては、侵入や改ざんの未然防止及び早期発見のために、サーバの点検を可能な限り短い周期で行うことが有効です。

また、今回の攻撃に関し日本国内において発見された一部の攻撃指令サーバの管理状況を確認したところ、次のような問題がありました。

- セキュリティパッチ等の更新プログラム適用が失敗したまま放置されていた。
- ウイルス対策ソフトの導入から自動更新の設定がなされるまでに数か月が経過しており、その数か月間、ウイルス対策ソフトが更新されていなかった。

いずれも、セキュリティ対策に無関心であった訳ではなかったものの、適切な対策を十分に講じてはいなかったため、サイバー攻撃に利用されました。

不正プログラムに感染したことが判明した場合には、他にもウイルス対策ソフトで検知等ができない不正プログラムにも感染している可能性があることから、パソコンを初期状態に戻して、すべてのアプリケーションを入れ直していただくことが適切です。

また、サーバ管理者にあっては、今一度、管理状況の点検をお願いします。

3.4 まとめ

今回のサイバー攻撃は、大規模なボットネットを構築した上で DDoS 攻撃を行ったものです。このことから今後、日本国内においても同様の手法を用いて多数のパソコンに不正プログラムを感染させ、大規模サイバー攻撃が行われる可能性を否定できません。

皆様の管理するコンピュータがサイバー攻撃に利用されることのないよう、日頃からのセキュリティ対策が重要になります。

4 「ガンブラー」によるウェブサイトの改ざん

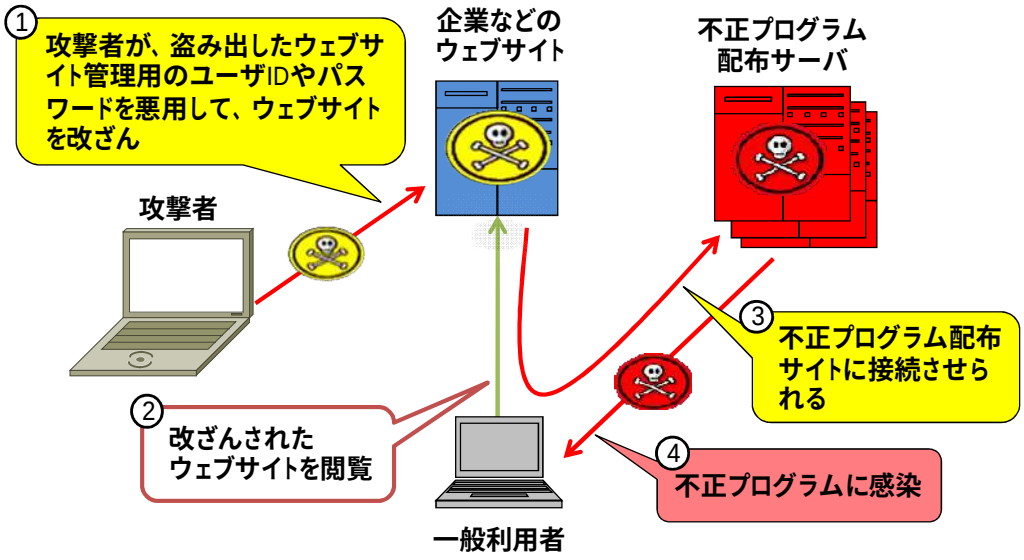
報道によると、平成 21 年5月頃に一時被害が広がった、「ガンブラー攻撃」によるウェブサイトの改ざん被害は、平成 21 年末頃から更に増加しています。

この攻撃は、改ざんされたウェブサイトを閲覧すると、一般利用者が気付かないうちに特定のサイトへ誘導され、不正プログラムに感染するおそれがある、危険性の高いものです。

特にウェブサイトの管理者が使用するパソコンが不正プログラムに感染した場合には、管理するウェブサイトに接続するためのユーザ ID やパスワードが盗み出され、管理先のウェブサイトの改ざんが起こります。

4.1 一般利用者の不正プログラム感染

一般利用者が、改ざんされたウェブサイトを閲覧するだけで、不正プログラムに感染するおそれがあります。(図4-1)



① 攻撃者が、盗み出したユーザ ID やパスワードなどを悪用して、ウェブサイトを改ざんし、不正プログラム配布サーバへの誘導を行うスクリプト[1]を埋め込む。

② 一般利用者が、改ざんされたウェブサイトを閲覧。

③ ウェブサイトに改ざんで埋め込まれたスクリプトが自動的に実行され、一般利用者が知らない間に、不正プログラム配布サーバに接続させられる。

④ 一般利用者のパソコンに存在する脆弱性が悪用され、不正プログラムに感染。

図4-1 一般利用者の不正プログラム感染[2]

---

[1] スクリプトとは、ウェブページを表示させるときに使われる、命令やプログラムです。

[2] ウェブサイトの改ざん方法については、すべてを確認することができないため、「ガンブラー被害」といわれているサイトの中には、他の方法による改ざんが含まれている可能性があります。

不正プログラムの感染には、Adobe Flash Player や Adobe Reader など、ウェブサイトを閲覧する際によく使用されるアプリケーションの脆弱性が利用されます。（表4-1）

表4-1　脆弱性を攻撃されるアプリケーションの例[1]

- **ウェブブラウザ**
  - **Internet Explorer 7**
- **ウェブサイト上の動画や文書などを閲覧するためのもの**
  - **Adobe Flash Player**
  - **Adobe Reader**
  - **Microsoft Office Web コンポーネント**
  - **Office Snapshot Viewer**
- **ウェブサイトの動的コンテンツを閲覧するために必要なもの**
  - **Java Runtime Environment**

警察庁では、パソコンに感染する不正プログラムの一つとして、偽セキュリティソフトを確認しています。（図4-2） 偽セキュリティソフトは、「警告！○件の感染が見つかりました！」などと頻繁に虚偽の表示をして、パソコンが使用困難になります。

図4-2　偽セキュリティソフト「Security Tool」の画面

「ガンブラー攻撃」では、この他にも、FTP[2]で使用するユーザ ID やパスワードを盗み出す不正プログラムなど、様々な不正プログラムに感染させられる可能性があります。

[1] これ以外の脆弱性を攻撃される可能性があります。

[2] File Transfer Protocol。ネットワークでファイルをやり取りするための通信手順。ウェブサイトにファイルを送るなど、ウェブサイトの管理でよく利用されます。

4.2 ウェブサイト管理用パスワードなどの盗み出し

前述のとおり、「ガンブラー攻撃」では改ざんされたウェブサイトを閲覧するだけで、一般利用者のパソコンが不正プログラムに感染してしまうおそれがあります。

この不正プログラムはパソコンに感染すると、その通信内容を監視したり、アプリケーションの設定を読み出したりして、ユーザ ID やパスワードといった情報を盗み出します。特にユーザ ID やパスワードを暗号化することなく送信している場合は、不正プログラムによって、ユーザ ID やパスワードを盗み出される危険性が更に高くなります。

ウェブサイトの管理者がウェブサイトに接続するための情報が盗まれた場合は、攻撃者に悪用され、ウェブサイトの改ざん連鎖につながり、被害拡大の危険性があります。

また、別のウェブサイト管理者が、改ざんされたウェブサイトを閲覧することで不正プログラムに感染し、さらにウェブサイトが改ざんされるという、改ざんの連鎖が起こり、不正プログラムの感染が拡大するおそれがあります。

4.3 改ざんされたウェブサイトに埋め込まれるプログラム

「ガンブラー攻撃」では、改ざんの際に不正プログラム配布サーバへ誘導を行うスクリプト（図4-3）が埋め込まれる特徴があります。不正プログラム配布サーバに誘導された後に、複数のサーバへの接続を繰り返しながら偽セキュリティソフトやパスワード情報を盗む不正プログラム等、様々な不正プログラムを次々とダウンロードさせると言われています。

図4-3 改ざんされウェブサイトに埋め込まれたスクリプトの例

図4-3に示したスクリプトは、一見しただけでは内容がわからないよう、難読化されています。平成21年5月頃は、難読化されていないスクリプトが目立ちましたが、平成21

年末以降は、難読化されたスクリプトを埋め込む手法の改ざんが見受けられるようになっています。

また、スクリプトについては、図4-3のように「<script>/*LGPL*/」で始まるもののほか、「<script>/*CODE1*/」や「<script>/*Exception*/」で始まるものなど、数種類を確認しており、新たなスクリプトが次々と出現していることがうかがえます。[1]

このほか、ウェブサイトで共通して使用するテキストやプログラム等をまとめたファイルが改ざんされると、そのファイルを参照しているすべてのウェブサイトのページが改ざんされた状態になり、その影響はさらに大きくなります。

4.4 警察庁における観測

改ざんで埋め込まれたスクリプトには、誘導先となるサーバの URL が記述されています。警察庁で確認した、これらの URL には、すべてロシアのドメイン名[2]であることを示す「.ru」が含まれています。しかし、URL を IP アドレスに変換して、その IP アドレスを国・地域別でみると、多くがヨーロッパのものでした。(図4-4)

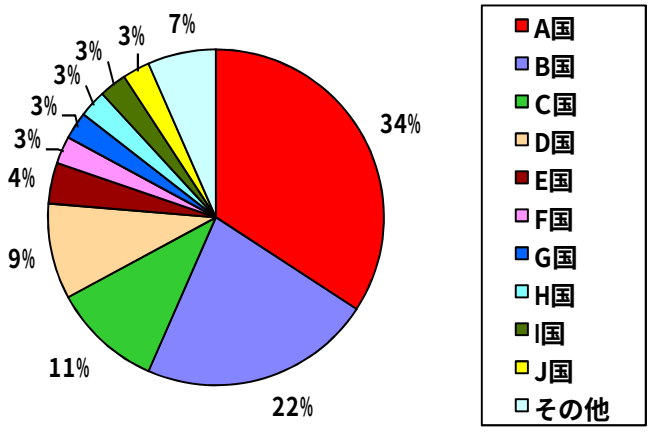


図4-4 誘導先となるサーバの IP アドレスの国・地域別比率[3]

インターネットでは、ウェブサイトへの接続要求が URL で行われた場合、DNS[4]サーバを使用して、IP アドレスに変換してから接続する仕組みになっています。

---

[1] コメント(/* ～ */で囲まれた部分)がない種類の誘導プログラムも確認されています。今後も様々な種類の誘導プログラムが出現することが考えられます。

[2] インターネット上でコンピュータを識別するための名称。

[3] 当データは、小数点第一位で四捨五入しているため、合計が 100%にならないことがあります。

[4] Domain Name System。IP アドレスを人間が扱いやすい名前で扱えるようにするため、ドメイン名と IP アドレスを相互に変換する仕組み。

改ざんサイトに埋め込まれたスクリプトに含まれる誘導先の URL は、それぞれ異なっており、これらの URL を DNS サーバで IP アドレスに変換してみると、誘導先となる IP アドレスは頻繁に変更されていることが分かりました。

これらの IP アドレスと URL の関係を分析したところ、URL は同じ IP アドレス群を使ういくつかのグループに分類できることを確認しました。しかし、異なる IP アドレス群でも一部の IP アドレスは共通に用いられているなど、全体のつながりもみられます。

さらに、不正プログラム配布サイトは、アクセス元の IP アドレスを記憶し、二度目以降のアクセスでは不正プログラムを配布しない仕組みであることも確認しています。これらは、不正プログラムの解析を行わせないための対策と考えられます。

「ガンブラー攻撃」では、大企業のウェブサイトから個人のブログサイトまで、多くのサイトが被害を受けましたが、個別の攻撃目標を狙って行っているというよりも、ボットネット等の大掛かりな犯罪基盤の構築を目的として行われているように思われます。

4.5 まとめ

以上のように「ガンブラー攻撃」では、改ざんされたウェブサイトを閲覧するだけで、利用者のコンピュータに存在する脆弱性を悪用され、不正プログラムに感染するおそれがあります。

また、ウェブサイトを管理している者の使用するパソコンが感染した場合、管理しているウェブサイトのユーザ ID やパスワードが攻撃者の手に渡り、ウェブサイトの改ざんが行われ、さらに他のウェブサイトが改ざんされるという連鎖が起こり、不正プログラムの感染拡大につながります。

パソコンを利用されている皆さんは、ウイルス対策ソフトを導入の上、最新のパターンファイルを適用した状態を保ち、不正プログラム感染の有無をチェックするほか、パソコンにインストールされているソフトウェアを最新の状態に保ち、脆弱性を修正しておくなどのセキュリティ対策が重要です。

また、使用しないアプリケーションの機能は、思わぬ脆弱性となり得ることから、無効にしておくことも大切です。

ウェブサイトの管理者の方は、管理するウェブサイトが改ざんされ、不正プログラムの頒布に利用されないよう、ログの監査等のセキュリティ対策を怠らないことが必要です。

「ガンブラー攻撃」は、ウェブサイト管理用パソコンの脆弱性を利用して盗み出したユーザ ID やパスワードを使用してウェブサイトが改ざんされますので、管理用パソコン以外からのウェブサイトの更新を許可しないような措置を採ることが有効です。ウェブ

サイトの管理を自身で行っている場合はもとより、組織や部署ごとに別々の管理用パソコンを使用して、ウェブサイトの管理をしている場合や、業務委託先で管理をしている場合にも、ウェブサイト管理用パソコンの運用や管理に十分配意してください。

特に、管理用パソコンの用途をウェブサイト管理に限定し、ウェブサイトの閲覧には別のパソコンを使用するといった運用面への配意も検討してください。

また、万一、管理用パソコンで不正プログラムが検知された場合には、検知できたもの以外の不正プログラムに感染している可能性がありますので、管理用パソコンを初期状態に戻して、すべてのアプリケーションを入れ直す措置が適切です。

これは、ウェブサイトを閲覧した一般のパソコン利用者が、不正プログラムに感染することを防ぐため、ウェブサイト管理者として重要な措置です。

5 Conficker ワームの感染の拡大

平成 21 年に大きな問題となったのが、平成 20 年 11 月に発生した Conficker（コンフィッカー）ワーム[1]の感染が拡大し続けていることです。様々な亜種が存在する Conficker ワームは、感染すると被害パソコンを外部から遠隔操作できるような仕組みを構築したり、インターネットを通じて別のパソコンに感染しようと試みたりします。

後述のとおり、警察庁においても、Conficker ワームが感染活動を行っていると考えられるアクセスを多数確認しています。

5.1 Conficker ワームの概要

平成 20 年 11 月頃に発生した Conficker ワームは、Windows パソコンにおける特定のサービスの脆弱性（MS08-067）を悪用して感染活動を行います。

また、様々な特徴のある亜種が存在し、セキュリティ対策が十分ではないパソコンを狙いインターネットや USB メモリを介して感染していきます。

5.2 Conficker ワームの脅威

Conficker ワームの脅威は、感染経路が多様化したことにあります。

前述のとおり、Conficker ワームには、様々な亜種が存在し、同一ローカルネットワーク内で通信しているパソコンに感染するものや USB メモリ等を介して感染するものがあります。これが、会社の社内ネットワーク等、インターネットには直接接続されていないローカルネットワーク内にも、感染が拡大した要因の一つと考えられます。

このほかにも Conficker ワームは、不正プログラムを配布するサーバ等から、他の不正プログラムを自動的にダウンロードして感染させる機能を持っています。したがって、いったん Conficker ワームに感染したパソコンには、大規模なサイバー攻撃や破壊活動に利用されるボットプログラムや、パソコン利用者が Conficker ワームの感染に気付き、対策を行った後でもパソコンを乗っ取ることができるように、バックドア等を作成されるなど、Conficker ワーム以外の不正プログラムが導入されている可能性があります。ダウンロードされる不正プログラムは、ウイルス対策ソフトで検知等されない可能性があります。これらの不正プログラムを駆除するときは、パソコンを初期状態に戻して、すべてのアプリケーションを入れ直していただくことが適切です。

---

[1] ワーム：悪意のあるプログラムの一種で、インターネット等を介して自己増殖する機能を持った不正プログラムのことです。

5.3 Conficker ワームの検知状況

Conficker ワームにおける亜種の多くは、感染活動を行うに当たり、Windows パソコンが特定のサービスを行う際に使用する 445 番ポートを利用して TCP 手順により通信を行います。

定点観測システムでは、Conficker ワームの感染活動は 445/TCP へのアクセスとして検知されます。

一方、同じ亜種に感染しているパソコンを探し出し、直接に接続する P2P 通信で、他の不正プログラムのダウンロードなどを行う亜種も存在します。この場合、P2P 通信を行おうとするアクセスが、定点観測システムにおいて検知されます。(図5-1)

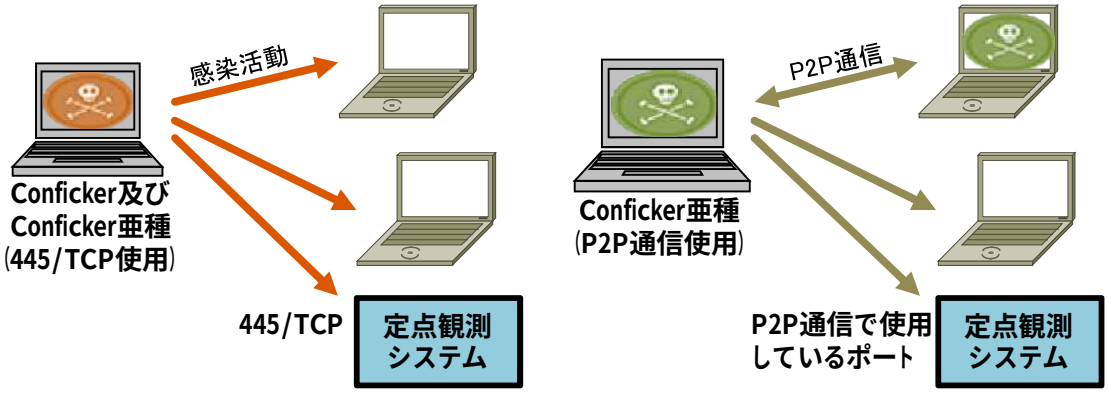


図5-1　Conficker ワームの検知

Conficker ワームに感染したと考えられる、定点観測システムの 445/TCP にアクセスしたホスト数[1]の推移を見ると、平成 20 年 12 月頃から急増し、それ以降も増加傾向が続いています。(図5-2) USB メモリなどを介して感染する亜種の発生が 12 月 29 日に確認されており、会社内などの、外部のインターネットには直接接続されていない閉じたネットワークでも感染が拡大している可能性もあります。したがって、12 月 29 日以降の Conficker ワームに感染したホスト数は、グラフの数値よりも多くなるものと考えられます。

また、平成21年3月上旬から中旬にかけて、445/TCP へのアクセスが減少し、それを補うように P2P 通信が急増しています。この期間、Conficker ワームの活動が、445/TCP への感染活動から、P2P 通信を行う亜種によるものへと変化したのではないかと推測されます。その後、P2P 通信を行う亜種の感染活動は減少し、再び 445/TCP

[1] インターネットに接続するパソコンやサーバなどを総称してホストといいます。ホストには IP アドレスが割り当てられており、ホスト数は、定点観測システムにアクセスしてきた IP アドレスの数で算出しています。

への攻撃による感染活動に移行したものと思われます。

なお、445/TCP へのアクセスの増加速度はゆるやかになりつつありますが、発生から1年以上が経過しても、増加が続いています。Conficker ワームの感染力が非常に高く、また、いまだに対策が取られていないパソコンが多いものと考えられます。

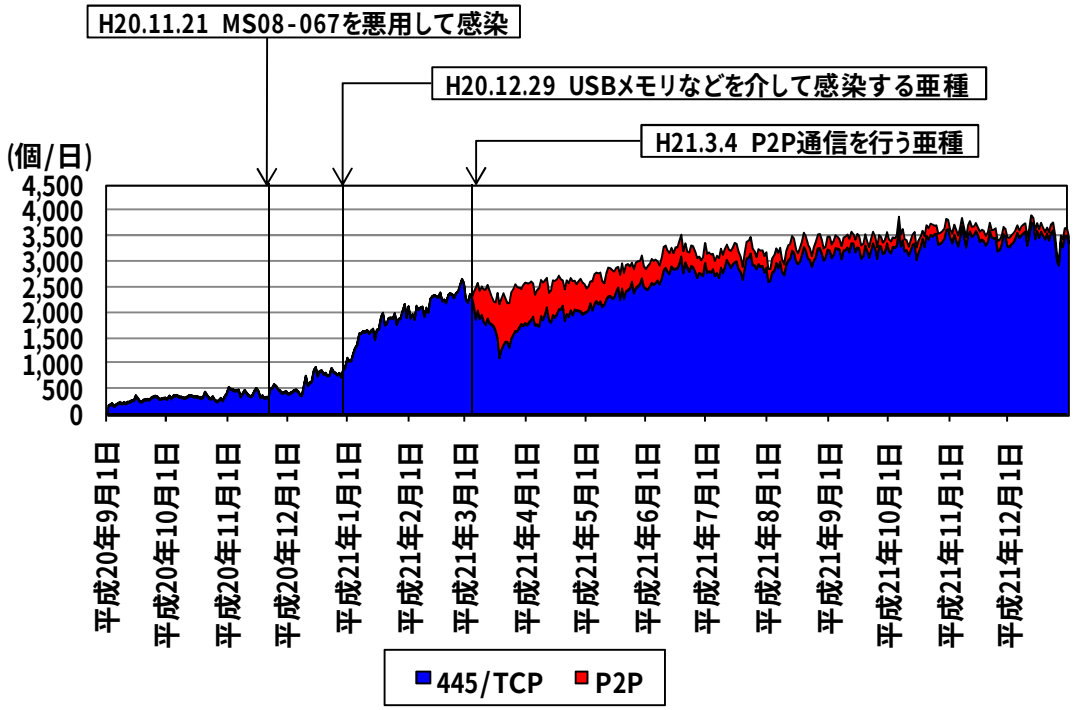


図5-2 Conficker の発信元 IP アドレス数[1]の推移

[1] 一日にシステム全体で観測した 445/TCP 及び P2P 通信それぞれの発信元 IP アドレス数を計上しています。このため、同一の発信元 IP アドレスが 445/TCP 及び P2P 通信の双方に含まれる場合があります。また、平成 21 年 3 月にシステムを更新し、センサーの機能が向上したため、システム更新後は検知できる発信元 IP アドレス数が増えました。グラフでは、システム更新前後を比較するため、システム更新後の発信元 IP アドレス数を、システム更新前相当に換算して表示しています。

5.4 まとめ

Conficker ワームは感染方法を多様化させることで、爆発的に感染数を増やしました。MS08-067 の脆弱性が発表されてから1年以上が経過した平成 21 年末においても、445/TCP にアクセスしたホスト数の推移を見ると、Conficker ワームに感染したパソコンの数は依然として増加傾向にあると考えられます。

一方、P2P 通信を行う亜種の活動は、観測される P2P 通信が減少していることから、収束しつつあると考えられますが、それ以外の 445/TCP を感染経路に持つ亜種は、世界中でいまだに駆除されずに存在していると思われます。

日本国内においても、445/TCP のアクセス数は、MS08-067 が発表される前の平成 20 年9月と平成 21 年 12 月を比較すると、3.6 倍と大幅に増加しています。また、一日における時間帯ごとのアクセスを見てみると、日本においては 21 時から 23 時にかけての時間帯に多く、深夜・早朝は少ないことから、家庭用パソコンが多く感染していると考えられます。

Conficker ワームに一度感染したコンピュータは、より悪質な破壊活動を行うような不正プログラムに感染している可能性があります。例えば、気付かないうちに、パソコンを外部から操作され、大規模な攻撃や破壊活動に悪用されてしまうボットプログラムに感染してしまうこともあります。また、パソコン上で入力した個人情報やクレジットカードの番号などの情報が、気付かないうちに他人に盗み出されてしまうこともあります。

445/TCP にアクセスしたホスト数の推移を見ると、Conficker ワームに感染したパソコンの数は依然として増加傾向にあると考えられ、今後も被害の拡大が懸念されます。

Conficker ワームは、Windows パソコンの脆弱性（MS08-067）を悪用して感染活動が行われることから、Windows パソコンに対する更新プログラムの適切な適用が重要です。また、ウイルス対策ソフト等を適切に運用して、既に感染してしまった Conficker ワームの駆除や、新たな感染を防いでください。

特に、USB メモリなどを用いて感染する Conficker ワームの亜種がありますので、「USB メモリなど外部記録媒体の自動再生機能を無効にする、外部記録媒体の中にあるファイルの実行を禁止する」といった設定が有効です。

6 情報セキュリティの向上のために

ここまで見てきたように、平成 21 年は、米国及び韓国への大規模なサイバー攻撃、「ガンブラー攻撃」によるウェブサイト改ざんの発生、Conficker ワームの感染拡大など、大きな脅威が顕在化し、攻撃手法の巧妙化も進みました。

このようなインターネット上の脅威から、情報資産を守り、意図に反して攻撃者に荷担させられてしまうことがないよう、インターネットをご利用される皆様には、最低限、以下のような措置を講じることが大切となります。

- OS やアプリケーションの更新プログラムの適切な適用
- ウイルス対策ソフトやファイアウォールソフト等の適切な運用
- メールに添付されたファイルや、メール中のリンク先を不用意に閲覧しない

この他にも、コンピュータの利用状況に応じて、

- パソコンやユーザ・アカウント等の使い分け
- パソコン等の電源の切断
- 不要な機能を導入しない、若しくは使用不可にする
- データの暗号化

等を実施することも有効です。

また、企業等の情報セキュリティ管理者等の皆様にとって、情報資産に対する様々な被害を未然に防止したり、軽減したりするために、推奨される措置の例として、以下の対策があります。

- 各種ソフトウェアやコンピュータ機器の販売元等から提供される、脆弱性を修正するセキュリティ更新プログラムやウイルス対策ソフトの適切な運用
- 使用しているソフトウェアのバージョンの適切な更新
- パーソナルコンピュータ、ウェブサーバ等の機器の適正な設定とセキュリティ更新プログラムの適切な適用
- データベースを運用している場合は、外部からのデータベースへの不正な命令を遮断するといった、データベースを不正に操作されないような対策についての検証
- 証跡の定期的な確認による、異常の早期発見と必要な措置

なお、前述した対策の実施に当たっては、事前に実施に伴う不具合の発生等を検証するため、各種ソフトウェアやコンピュータ機器の販売元等から提供されているセキュリティ情報の確認に配意して下さい。

これらの対策に加えて、情報セキュリティ対策及び事業継続計画等についても、十分に検討の上、障害原因の究明や障害の兆候の迅速な発見・対応ができるよう、守るべき情報資産などに応じて、組織としての態勢を適切に構築することが重要です。

サイバー攻撃の手法は日々変化しています。これらに対処するため、インターネットを利用される皆様、企業等の情報セキュリティ管理者等の皆様が、可能な限りインターネット上の脅威や、その対策等について関心を持ち、状況に応じて適切な措置を行っていただくことが大切です。

警察庁では、今後とも様々な機会をとらえて、情報セキュリティ対策に資する情報を提供するなどして、安心して利用できる安全なインターネット社会の確立に努めてまいります。

7 付録 P2P 観測システムの運用 ～P2P の利用者の動向～

7.1 導入の経緯

P2P (Peer to Peer) の技術を利用したファイル共有ネットワークは、参加者の匿名性が高く、それに乗じて、多数の違法ファイルが流通しています。警察庁では、その実態を把握するため、P2P 観測システムを導入して、試験運用を実施してきましたが、平成 22 年1月1日から正式に運用を開始しました。

7.2 P2P 観測システムの概要

ファイル共有ネットワークにファイルを公開した場合、ファイルの所有者やファイル名等を含むファイル情報がネットワーク上に流れ、ファイルを必要とする者がその情報を元にファイルを検索し、ダウンロードする仕組みとなっています。

P2P 観測システムは、ファイル共有ネットワークを巡回してファイル情報を収集し、分析・検索を行うシステムです。

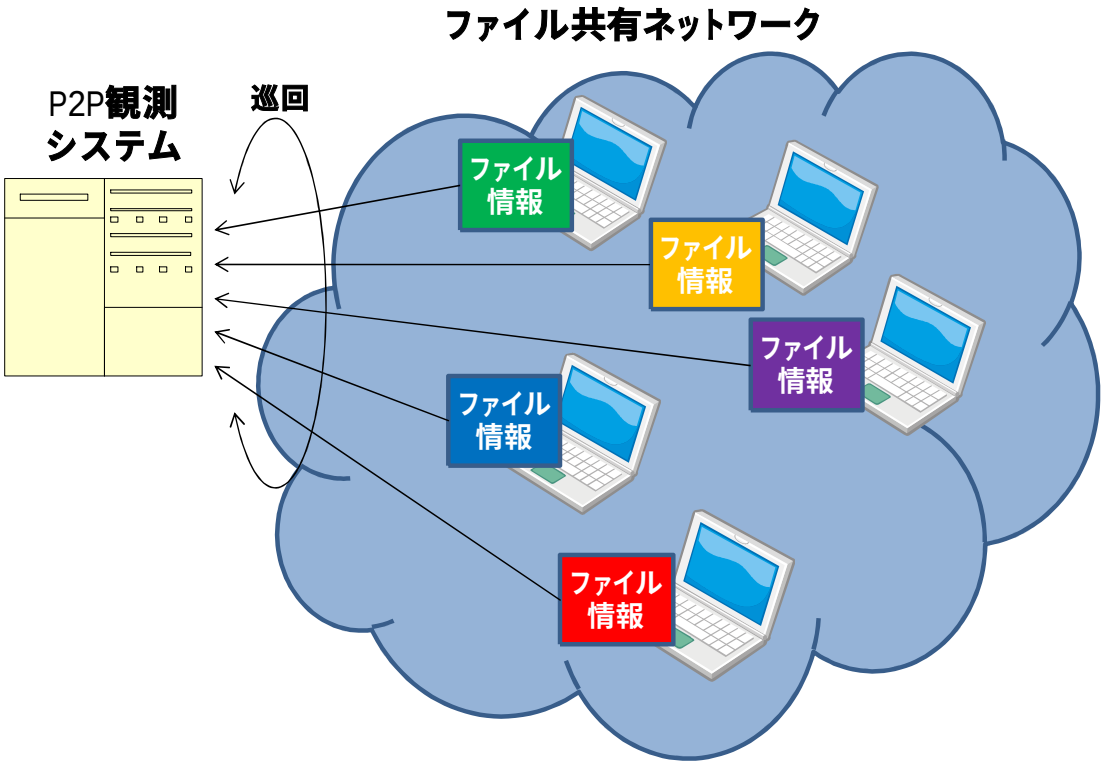


図7-1 P2P 観測システムとファイル共有ネットワーク

7.3 観測結果

7.3.1 接続コンピュータ数 (Share)

一日当たり、約 18～20 万台のコンピュータがファイル共有ネットワークに接続されており、深夜時間帯及び休日に増える傾向です。

昨年 11 月 30 日の一斉取締り (ファイル共有ソフトを利用した著作権法違反事件) 後、約1割減少しています。

本年1月1日の改正著作権法施行後、約2割減少しています。

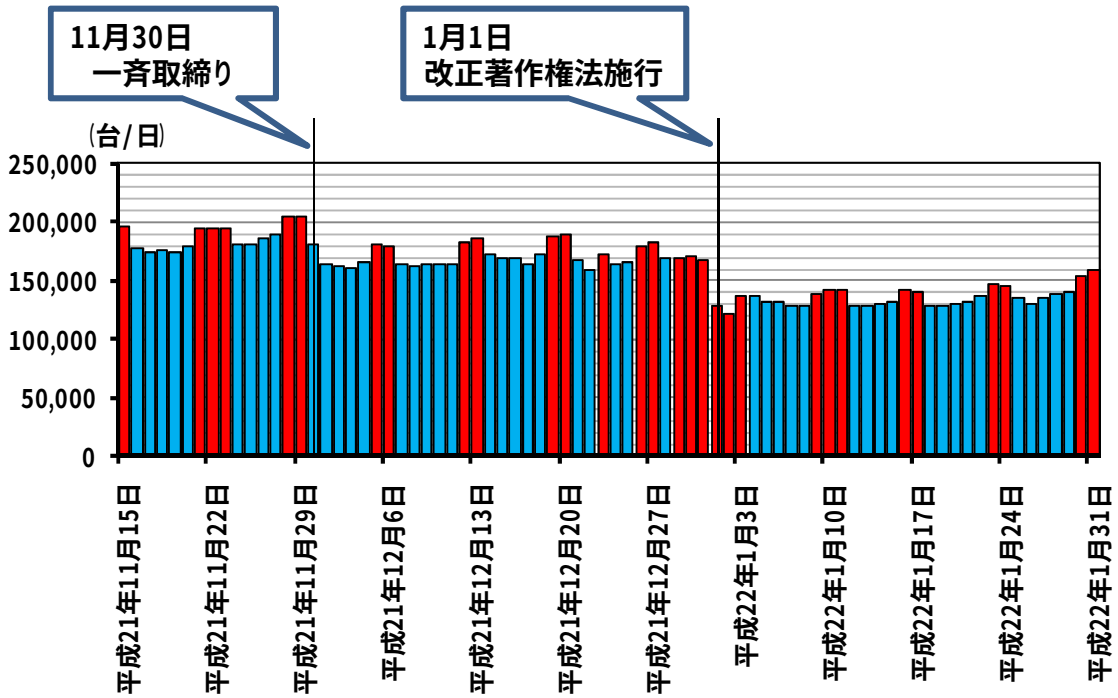


図7-2 ファイル共有ネットワークへの接続コンピュータ数の推移

7.3.2 流通ファイル数及び流通ファイルの動向（Share）

一日当たり、約 95 万個のファイルがファイル共有ネットワークで公開されています。昨年 11 月 30 日の一斉取締り後、約5万個減少しています。

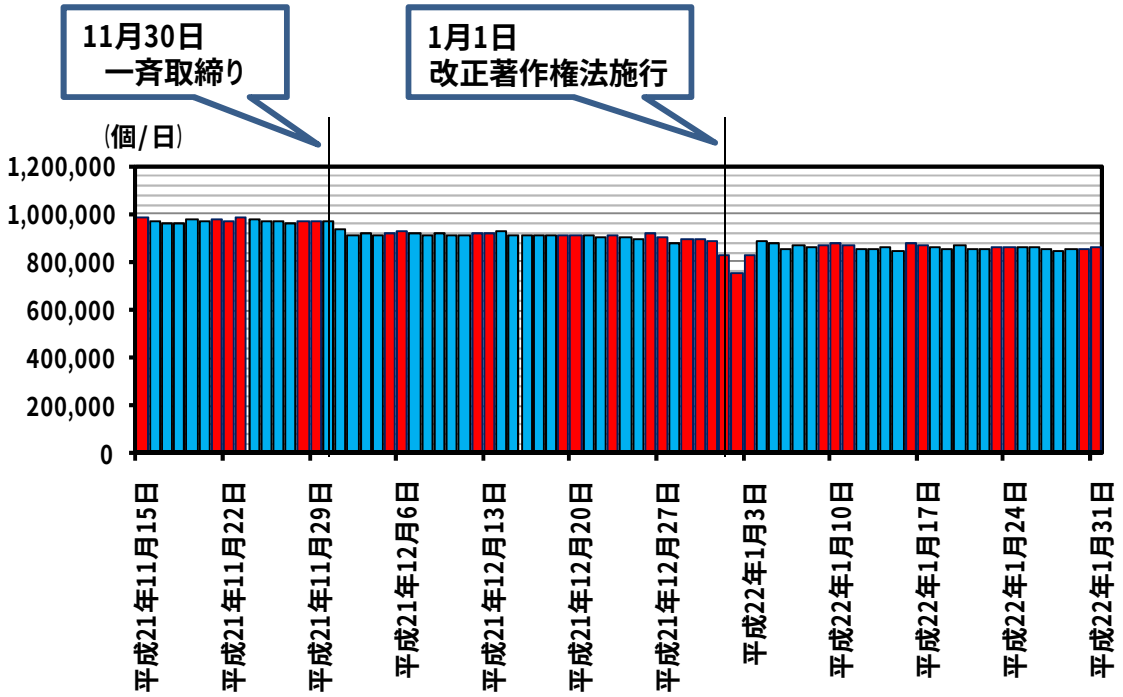


図7-3　流通ファイル数の推移

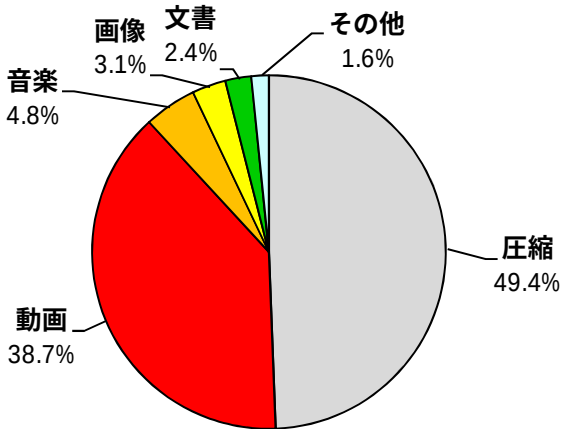


図7-4　流通ファイルの傾向

7.4 今後の予定

ファイル共有ソフトが依然として多く使用されており、多数のファイルが流通していることから、流通しているファイルの実態把握をさらに推進します。