ボットネットワークに対する
ヒントとアドバイス

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

ボットネットは犯罪行為です。

正当な理由がないのに、ボットを作成する行為または、他人のコンピューターに対し無断で不正プログラムをインストールする行為は「不正指令電磁的記録に関する罪」に問われる可能性があります。そして、ボットネットによって行われる活動は違法である場合があります。

どのようにして、ボットを防ぐことができますか？

100パーセントの予防は不可能ですが、あなたのコンピューターに対する感染リスクを劇的に低減させるちょっとした「ヒントとアドバイス」があります。それが「STOP. THINK. CONNECT.」を意識することです。この活動はオバマ大統領の声明で「全米サイバーセキュリティ意識向上活動」（National Cyber Security Awareness Campaign）として認められています。

パソコンを常にクリーンに保とう。

● セキュリティ対策ソフトウェア等を常に最新の状態に保つ

└ セキュリティ対策ソフトウェア、ウェブブラウザー及び、OSを最新に保つことが、ウイルスやマルウェア（不正プログラム）などのオンライン上の脅威から守る上で最善の策です。

● 「自動的にソフトウェアを更新する」をオンにする

└ ブラウザーや OS を最新版に保っておくことは、ウイルス、マルウェアや他のオンライン上の脅威から守るためにまずやるべき選択です。多くのソフトウェアには、既知のリスクから自身を保護するために自動的に最新版に更新する機能があります。お使いのソフトウェアに自動更新オプションがあれば必ずオンにしてください。

● インターネットに接続するあらゆる端末を守る

└ コンピューター、スマートフォン、ゲーム機やウェブを閲覧する機能を持つ端末すべては、ウイルスやマルウェアからの保護が必要です。

● USBメモリは接続時にセキュリティ対策ソフトウェアを使ってスキャン

└ USBポートなどに接続する外部機器がウイルスやマルウェアに感染していた場合、パソコンに接続すると感染する恐れがあります。接続するときはセキュリティ対策ソフトウェアを使ってスキャンしてください。

STC普及啓発WG事務局 stc-sec@antiphishing.jp

ボットネットワークに対する
ヒントとアドバイス

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

インターネットへの接続にはご用心。

● 怪しいと思ったら返事をしない

メール、ツイッター、BBS、オンライン広告などはあなたをサイバー犯罪の危険に陥れる手段に使われることもあります。信頼している友人・知人・場所からの情報でも、もしその情報が怪しいと感じたら削除するのが適当です。メールの場合は スパムメールとして処理しましょう。

● 無線LAN（Wi-Fiホットスポット）について正しい知識を身につける

自宅および会社など限られた人が使う無線LANなのか、誰でも使えるカフェや空港の公衆無線LANかによって、自分の端末のセキュリティ設定を変更し、自分のパソコンや端末にアクセスできるユーザーを限定しましょう。

● 偽のウイルス警告 詐欺ソフト「スケアウェア」に注意

サイバー犯罪者はあなたが使っているコンピューターを危うく見せかけ不安をかき立てることで、個人情報の窃盗を狙っています。狙われている個人情報には、クレジットカード番号や金融機関のログイン証明書が含まれます。もし、「ウイルスに感染している」「ソフトウェアの購入が必要である」との通知が表示されたら疑うべきです。これはあなたのコンピューターが改ざんされた時に生じる、よく知られた症状です。

あなたが感染を疑っているならば。

もしあなたのコンピューターがボットに感染したり、感染の通知を受け取ったり、自覚症状がある場合には直ちに不正プログラムを取り除くための処置をとってください。
不正プログラムに関する日本国内の取り組みについては、こちらをご覧ください。

- **官民連携による国民のマルウェア対策支援プロジェクト | ACTIVE**
  http://www.active.go.jp/index.html

- **サイバークリーンセンター**
  https://www.ccc.go.jp/

※2006年より国の事業として行われてきた「サイバークリーンセンター」の活動は、2011年3月で終了しています。このため、参考情報としてご確認ください。
ここでは不正プログラムを駆除できる駆除ツールやオンラインスキャンの紹介をしています。駆除ツールとは様々なセキュリティ対策企業から提供されている、不正プログラムを検知・駆除するためのツールです。
駆除ツールは常駐監視機能が利用できないなど、一般的なセキュリティ対策ソフトウェアよりも機能的に劣っている部分もあります。このため、あくまで一時的な対処法として利用してください。

ボットネットワークに対する ヒントとアドバイス

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

ボットネットワークとは

「ボットネットワーク（以下 ボットネット）」とは、不正プログラム「ボット」（ロボット/Robotを短縮した名称）というマルウェア（コンピューターウイルス、キーロガーなどの不正プログラム）に感染したコンピューターによって作られ、サイバー犯罪者により遠隔操作されているネットワークです。サイバー犯罪者は金銭的な利益獲得や、ウェブサイトまたはネットワークに対する攻撃のためにこのネットワークを使用します。ボットはノートパソコンやデスクトップパソコン、スマートフォン、サーバ、ルータといった様々なネットワーク機器に感染し悪用を行い、深刻な被害をもたらします。

インターネットに接続されているすべてのコンピューターは不正プログラムに感染しやすいといえます。ボットネットに使用される不正プログラムは、あなたのコンピューター上にこっそりとインストールさせることができます。あなたがメールの添付ファイルをクリックしたとき、または不正プログラムが埋め込まれたホームページを見ただけで、あなたのコンピューターはボットに感染し、ボットネットに荷担することになるかもしれません。もしあなたのコンピューターがボットネットに荷担したならば、「指令サーバ」（「コマンド アンド コントール サーバ」、「C&C サーバ」、「C2 サーバ」とも呼ばれています。）からサイバー犯罪者の命令を待ち続け、自動化された攻撃、例えばキーボードの操作履歴の監視などをあなたに気づかせることなく行うかもしれません。サイバー犯罪者はボットネットを好んでいます。なぜならボットネットはたった1回の操作で何千ものコンピューターを犯罪目的で使うことができます。そしてボットネットはサイバー犯罪者の身元を隠す手助けをします。

ボットに感染した場合に、あなたのコンピューターがとる行動はサイバー犯罪者が企てている犯行によって変わってきます。多くのボットネットはパソコン内の情報（パスワードやクレジットカード番号、住所、電話番号などの個人情報）を集めるように設計されています。集められた情報は不正な目的（個人情報の窃盗、クレジットカード詐欺、迷惑メール、不正プログラムの配布など）の為に使用されます。ボットはウェブサイトまたはネットワークに対する攻撃のために使用できます。このような攻撃を DDoS(Distributed Denial of Service：分散サービス妨害）攻撃と呼びます。

どのようにして、コンピューターがボットネットに荷担しているか知ることができますか？

ボットに感染していることに気づくことは難しいです。その昔、コンピューターの起動が遅い、動作が重いといった症状や迷惑な広告の表示は、あなたのコンピューターが不正プログラムに感染していることを示す徴候でした。昨今、不正プログラムに感染したことを示す見た目の徴候はほとんどありません。サイバー犯罪者はより多くのコンピューターに不正プログラムの感染を実現するために、不正プログラムを隠そうと取り組んでいます。

インターネット接続会社（「インターネットサービスプロバイダー」）では、彼らのネットワーク機器からボットネットの通信を発見したときに、感染者に対して注意喚起する率先的なアプローチが行われています。あなたはこうしたサービスに参加していくべきです。もしあなたがこうした注意喚起を受け取った場合、その通知の正当性を確かめてください。その上で提供される駆除ツールの使用または、あなたのネットワーク機器を確認して、不正プログラムを取り除くための処置をとってください。より詳細な情報はご利用のインターネット接続会社にお問い合わせください。

ボットネットワークに対する ヒントとアドバイス

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

- **株式会社カスペルスキー | Kaspersky Virus Removal Tool**
  http://support.kaspersky.co.jp/viruses/utility
- **株式会社シマンテック | ノートン セキュリティスキャン**
  https://security.symantec.com/NSS/GetNSS.aspx
- **トレンドマイクロ株式会社 | トレンドマイクロ オンラインスキャン**
  http://safe.trendmicro.jp/products/onlinescan.aspx
- **日本マイクロソフト株式会社 | Microsoft Safety Scanner**
  http://www.microsoft.com/security/scanner/
- **マカフィー株式会社 | McAfee Security Scan Plus**
  http://home.mcafee.com/downloads/free-virus-scan

独立行政法人 情報処理推進機構（IPA）では、インストールされているソフトウェア製品が最新のバージョンであるかを確認することができるセキュリティツール「MyJVN バージョンチェッカ」を公開しています。最新のバージョンでない場合は、ソフトウェア製品ベンダーのバージョンアップページへ容易にアクセスが可能です。
また、パソコンで使われているWindowsのセキュリティ設定項目を簡単な操作で確認することができるセキュリティツール「MyJVN セキュリティ設定チェッカ」を公開しています。設定を変更するための説明ページへ容易にアクセスすることが可能です。

- **独立行政法人 情報処理推進機構 | MyJVN**
  http://jvndb.jvn.jp/apis/myjvn/

STOP. **立ち止まる**	ボタンやリンクをクリックする前に、安全なものなのか一旦立ち止まって確認しましょう。どのような画面表示にリスクがあるのか知っておきましましょう。
THINK. **考える**	これから何が起きるのかじっくり考えましょう。警告が出ていないかどうか気を配り、自分の行動によって、ご自分やご家族の安全にどのような影響が出そうなのか考えるようにしましょう。
CONNECT. **楽しむ**	自分とコンピューターを守るための適切なステップをとっていることを理解した上で、自信をもってネットを楽しみましょう。