



IPA

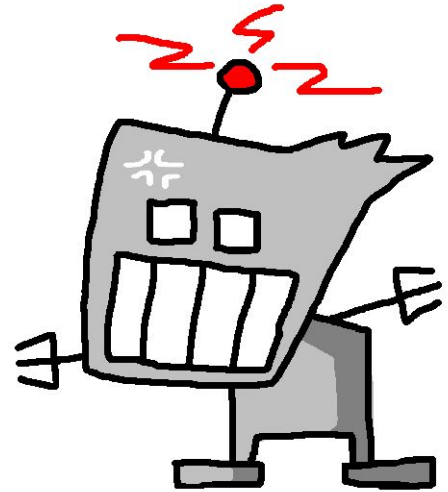
独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/>

1. ボットとは

ボットとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。

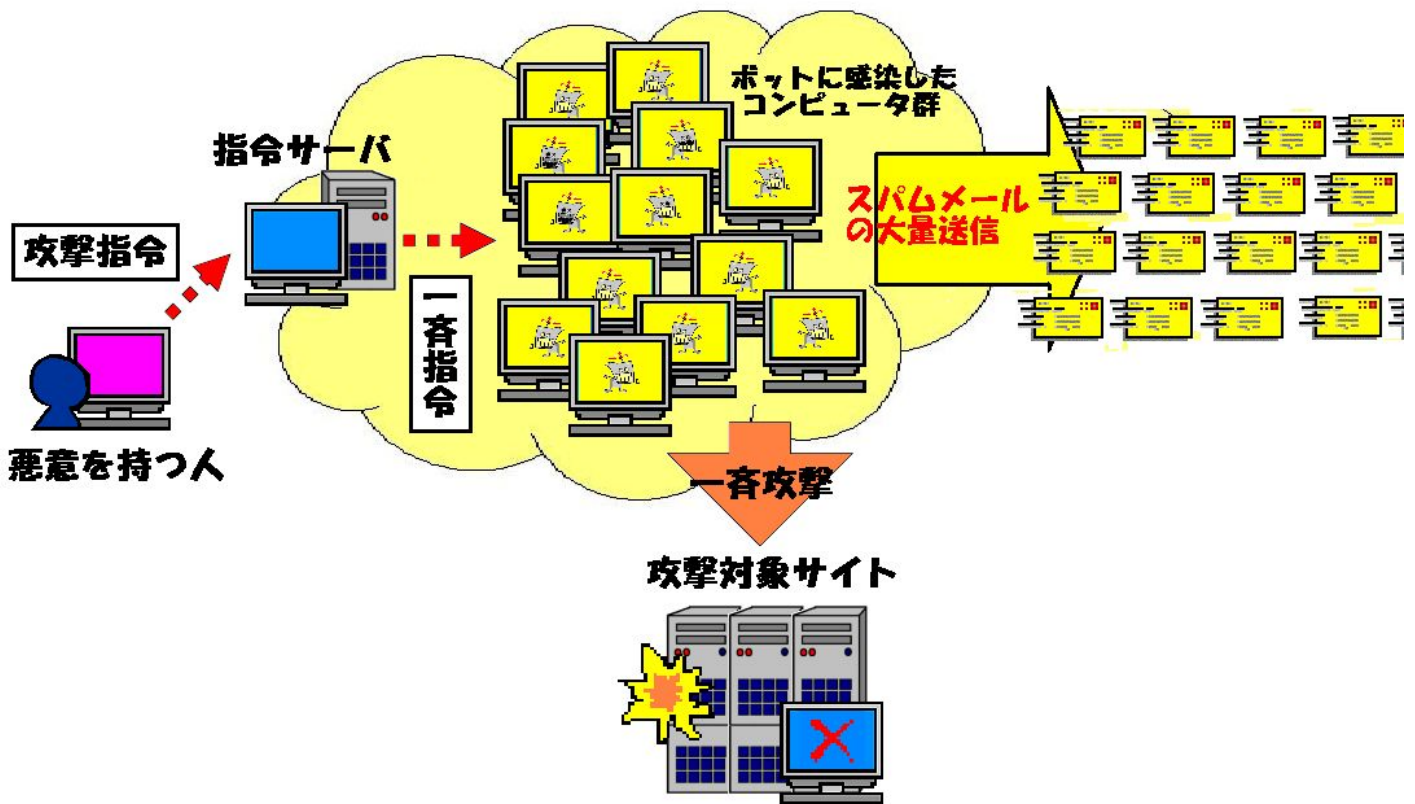
感染すると、外部からの指示を待ち、与えられた指示に従って内蔵された処理(後述)を実行します。この動作が、ロボットに似ているところから、ボットと呼ばれています。



2. ボットネットワークの脅威

同一の指令サーバの配下にある複数(数百~数千・数万になる場合もある)のボットは、指令サーバを中心とするネットワークを組むため、ボットネットワークと呼ばれています。

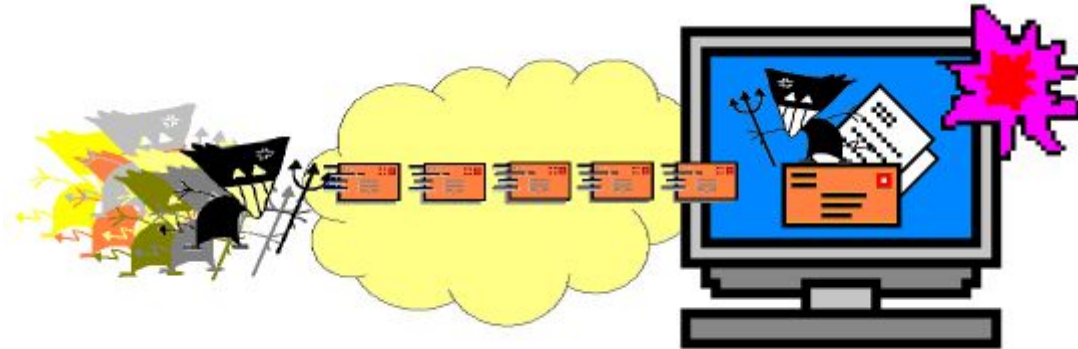
ボットネットワークが、フィッシング^(*1) 目的などのスパムメール^(*2) の大量送信や、特定サイトへの DDoS 攻撃^(*3) などに利用されると、とても大きな脅威になります。



3. どのようにして感染するのか

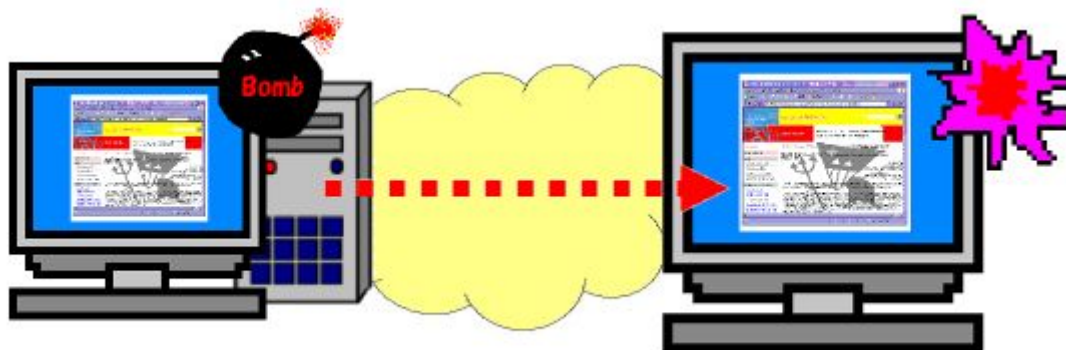
感染方法は、以下のものが挙げられます。

1) ウイルスメールの添付ファイルの実行による感染

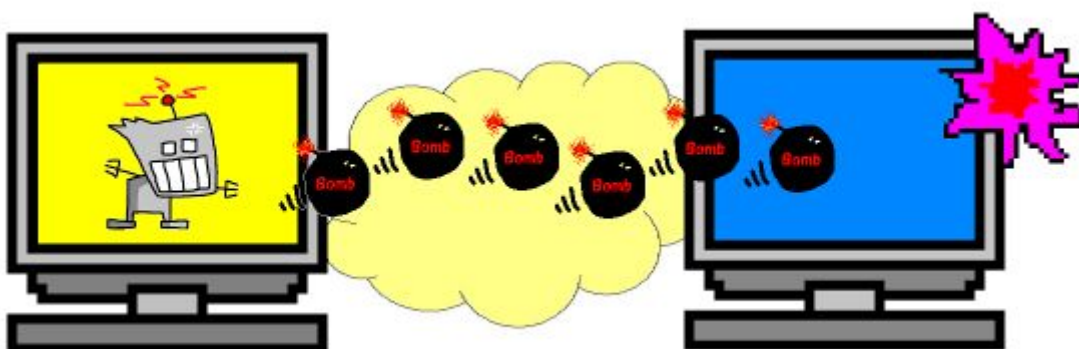


2) 不正な(ウイルスの埋め込まれた)Web ページの閲覧による感染

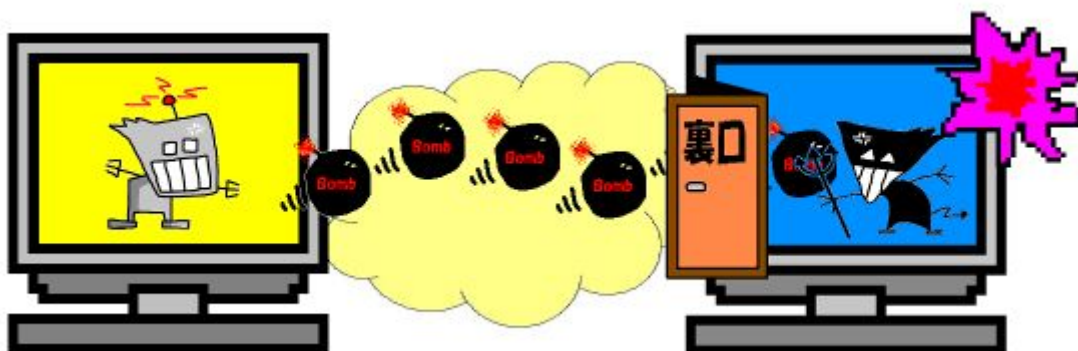
3) スパムメールに示されたリンク(URL)のクリックにより不正なサイトに導かれて感染



4) コンピュータのぜい弱性(*4)を突く、ネットワークを通じた不正アクセスによる感染



5) 他のウイルスに感染した際に設定されるバックドア^(*)5)を通じてネットワークから感染



また、以下の感染方法もありうるので、注意が必要です。

6) ファイル交換(PtoP)ソフトの利用による感染

7) IM(インスタントメッセンジャ)^(*)6)サービスの利用による感染

これらのうち、4)のぜい弱性を突いた手法は、ネットワークに接続しただけで感染してしまうこととなります。被害者にとっては、見かけ上何もしていないのに感染することになり、感染に気が付きにくいので、特に注意が必要です。このケースでは、Microsoft Update などによりぜい弱性を解消しておくだけでなく、ネットワークからの不正なアクセスを防ぐ対策(後述)を行うことで防御します。

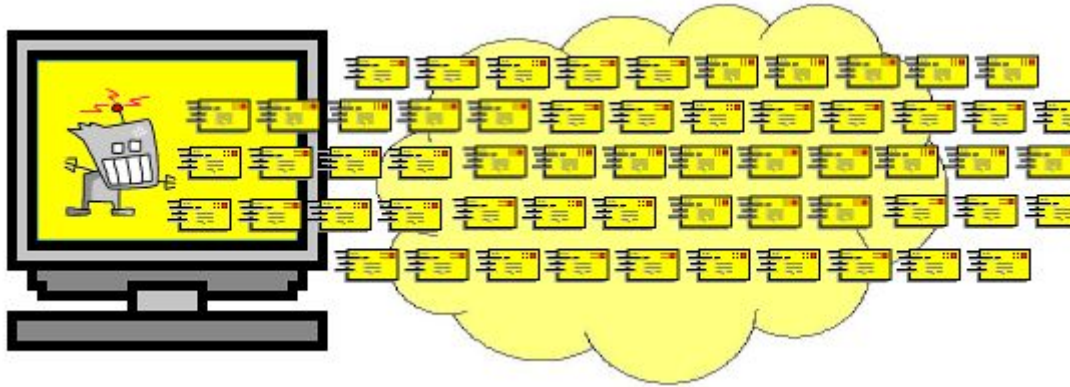
4. 感染後の動作

感染すると、自らネットワークを通じて外部の指令サーバ(多くのボットはIRC(Internet Relay Chat)^(*)7)を使うようです)と通信を行い、外部からの指示により指定された処理(スパムメール送信活動・DoS 攻撃^(*)3)などの攻撃活動・ネットワーク感染活動・ネットワークスキャン活動^(*)8)など)を実行します。さらに、自分自身のバージョンアップや、指示を待つ指令サーバの変更なども実行します。

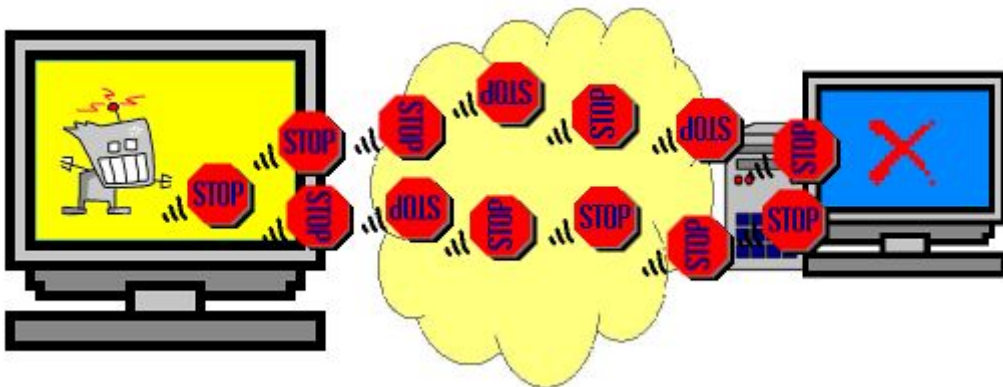
しかしながら、これらの動作は目立たず、陰で実行されますので、利用者はほとんど気付くことがなく、たいへん厄介なものとなっています。



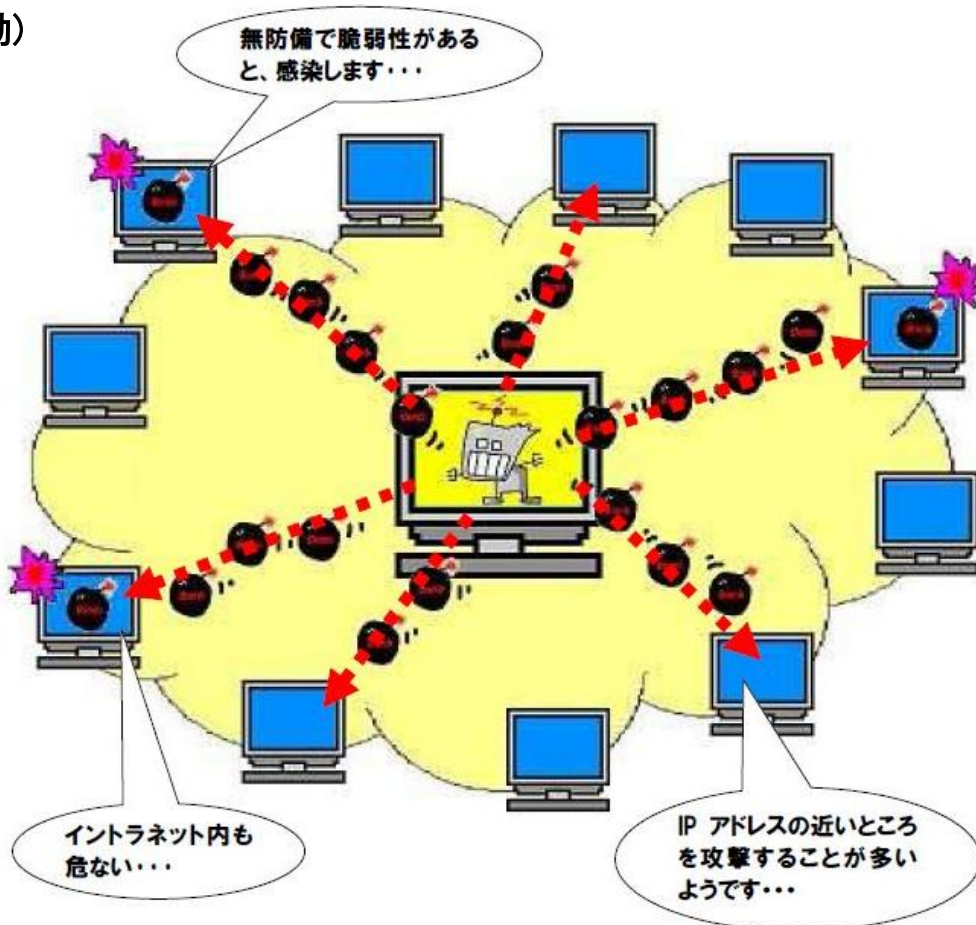
1) スпамメール送信活動（多量のスパムメールを送信する）



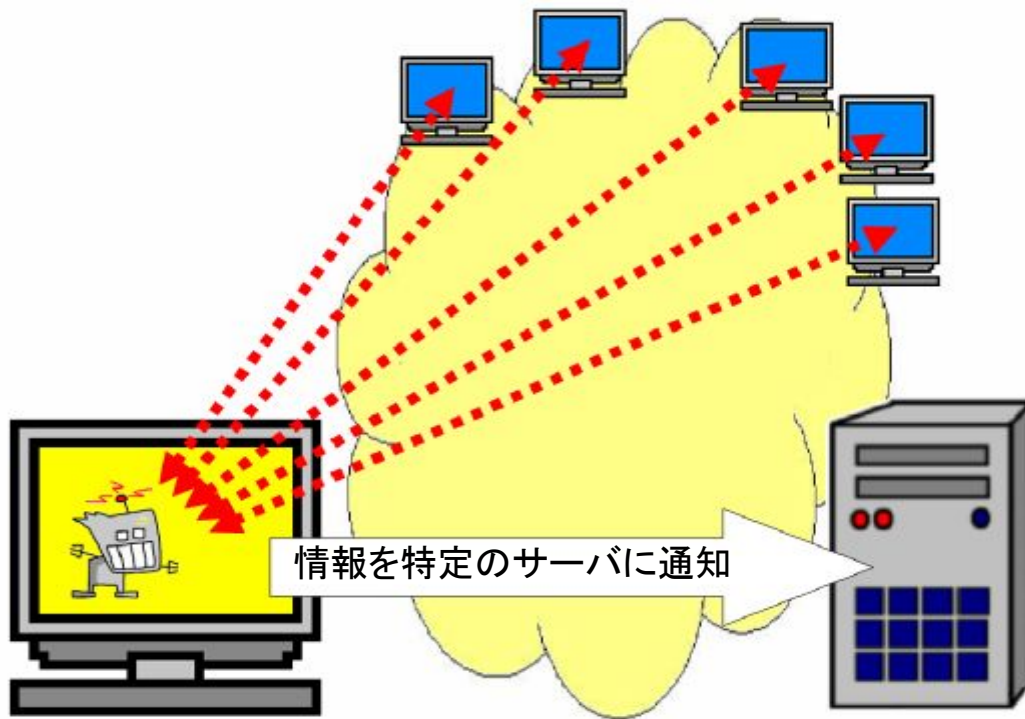
2) DoS 攻撃などの攻撃活動（特定のサイトへのサービス妨害攻撃を行う）



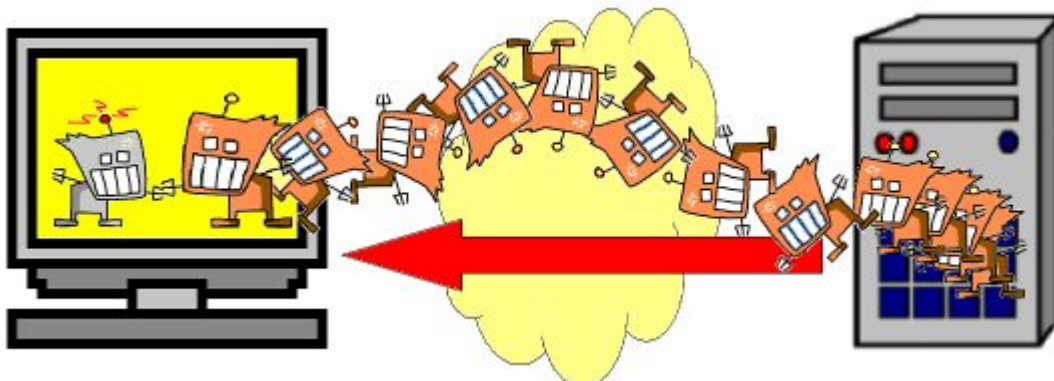
3) ネットワーク感染活動（コンピュータのぜい弱性を狙った不正アクセスによる感染活動）



4) ネットワークスキャン活動（感染対象やぜい弱性を持つコンピュータの情報を集める）



5) 自分自身のバージョンアップや指令サーバの変更



6) スパイ活動（感染したコンピュータ内の情報を外部へ送信）



5. ボットに感染しているか確認し駆除する方法

(Windows 利用者の場合)

最近のボットは、感染したコンピュータの利用者に気付かれないように、さまざまな手法を用います。例えば、ウイルス対策ソフト(ワクチンソフト)を使用している場合は、それらのソフトが最新のウイルス定義ファイルを取り込むことを妨害したり、ソフト自体を止めてしまったりします。また、動作中のプロセスを参照しても、システム本来のプロセスと区別が付きにくい名称を使うこともあるようですし、場合によってはプロセスが参照できない場合もあるようです。

このような状況なので、おかしいなと思ったら、以下の確認手段で、ボットに感染しているか調べてみて下さい。

1) コンピュータを最新の状態にする

Microsoft Update を実施して下さい。

この際、Microsoft のサイトに接続できないようであれば、ボット(あるいはウイルス)による特定サイトへの接続を妨害されている可能性がありますので、3)の確認を行ってください。不正な設定をされていた場合は、不正の訂正後、再度 Microsoft Update を実施して下さい。



●Microsoft Update

<http://www.update.microsoft.com/microsoftupdate/v6/default.aspx>

Microsoft Update の使い方については、以下の Web サイトが参考になります。

● Microsoft Update の使い方

<http://www.microsoft.com/japan/protect/computer/updates/mu.msp>

Microsoft Update を実施すると、「悪意のあるソフトウェアの削除ツール」が実行されます。このツールは、数多くの種類のボットプログラムを探索し、見つかった場合は削除します。ある意味では、無償の対策ソフトと言うことになりますが、Microsoft Update を実施したタイミングでしか実行されないため、必要であれば、自分自身で、このツールを Microsoft Download サイトからダウンロードして下さい。ダウンロードしたツールがあれば、逐次実行することができます。

- 悪意のあるソフトウェアの削除ツール

<http://www.microsoft.com/japan/security/malwareremove/>

2) ウイルス対策ソフトを最新の状態にしてウイルス検査を実施する

ウイルス対策ソフトを使用している方は、ウイルス定義ファイルを最新にして、ウイルス検査を実施して下さい。

ウイルス対策ソフトを使用していない方は、オンラインスキャンを提供するウイルス対策ベンダーがありますので、そちらを利用して下さい(12頁を参照下さい)。

この際、ウイルス対策ベンダーのサイトに接続できないようであれば、ボット(あるいはウイルス)による特定サイトへの接続を妨害されている可能性がありますので、3)の確認を行ってください。不正な設定をされていた場合は、不正の訂正後、再度ウイルス対策ソフトを最新の状態にして、ウイルス検査を実施するか、オンラインスキャンを実施して下さい(注意:オンラインスキャンでは駆除できない場合があります。検出されたウイルス毎に指定された駆除方法を参考に、駆除を実施して下さい)。



最近のウイルス対策ソフトは、統合セキュリティ対策ソフトへシフトしようとしています。統合セキュリティ対策ソフトの場合は、ファイアウォール機能も実装されているので、ネットワークからの感染を防止することができるようです。

また、感染した場合でも、パソコン内部からの、利用者の意図しない外部へのアクセスも監視/抑止してくれるので、ボットなどの不正プログラムに感染していることが、利用者に分かりやすくなっているようです。このようなセキュリティ対策ソフトを活用することも重要な対策になります。

3) 以下のファイルを調べる

・HOSTS ファイル

Windows NT,2000 の場合は、

C:\%WINNT%\SYSTEM32\DRIVERS\ETC のフォルダにある HOSTS ファイル

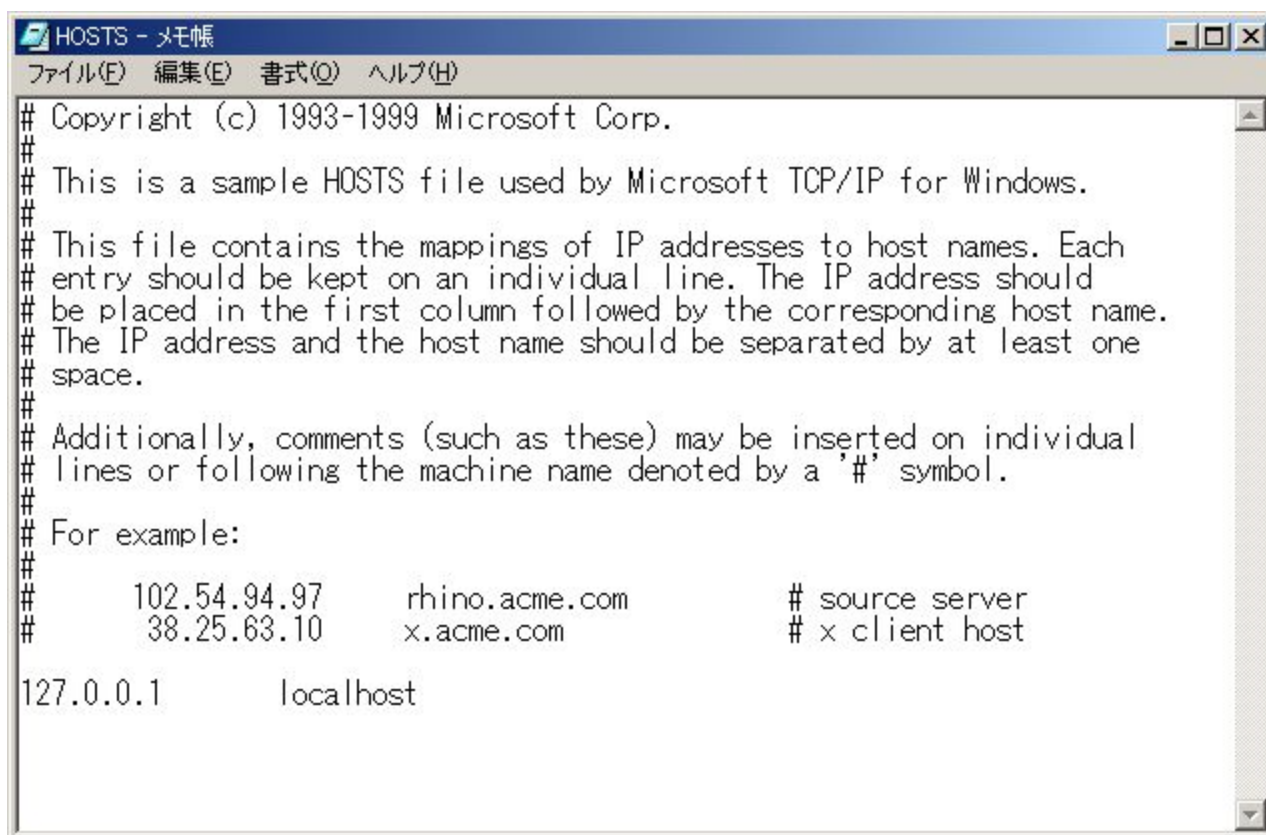
Windows XP,Vista の場合は、

C:\%WINDOWS%\SYSTEM32\DRIVERS\ETC のフォルダにある HOSTS ファイル

★内容の確認には、アクセサリのメモ帳(notepad.exe)を使うと便利です。

このファイルは、ネットワーク接続の接続先を特定するファイルです。

不正な設定をされると、特定のサイトの URL へ接続しようとする際に、別のIPアドレスへ接続させることができるものです。



```
HOSTS - メモ帳
ファイル(F) 編集(E) 書式(O) ヘルプ(H)
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host
#
127.0.0.1      localhost
```

このファイルを操作したことがない場合は、以下の定義(Localhost)しか登録されていないのですが、他の定義がある場合は、以下の内容を確認して下さい。

指定されている URL が Microsoft のサイトであったり、ウイルス対策ベンダーのサイトであったりする場合は、それらの定義を削除する必要があります(127.0.0.1 は自分自身のコンピュータを指しています)。

127.0.0.1 localhost

以下は、不正な指定の例

127.0.0.1 www.microsoft.com

127.0.0.1 www.nai.com

127.0.0.1 trendmicro.com

127.0.0.1 update.symantec.com

127.0.0.1 updates.symantec.com

ただし、行頭の文字が#の場合はコメント行なので、問題はありません。

6. 一般ユーザはどのような点に気を付ければよいか

ネットワーク(インターネット)を利用する一般ユーザは、ボットなどのウイルスに感染しないために以下に示すような対策を行う必要があります。

(1) セキュリティ対策ソフトの導入

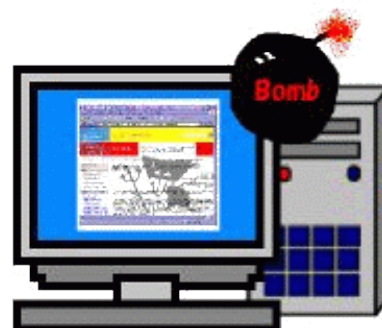
ウイルス対策ソフトやスパイウェア対策ソフトの導入(あるいは統合セキュリティ対策ソフトの導入)と、それらのソフトが使用する(ウイルス)定義ファイル等の定期的な更新およびウイルス検査を実施する。

(2) メール添付ファイルに注意

見知らぬメールの添付ファイルは安易に開かない。特に添付ファイルが実行形式のものは要注意です。

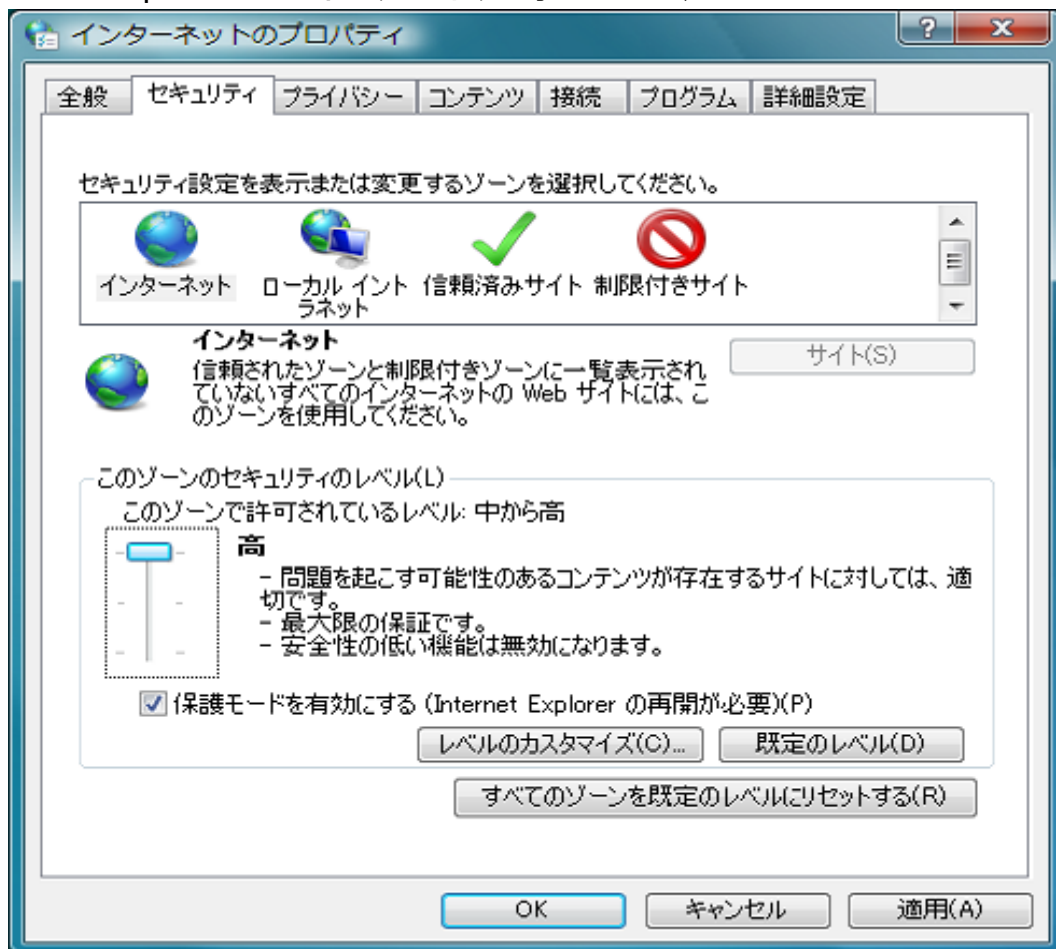
(3) 不審な Web サイトの閲覧を控える

不正なプログラムを利用者のパソコンに埋め込む目的のサイトが存在します。セキュリティ対策が不十分な設定で、このようなサイトを訪れるのは危険です。



(4) ブラウザ等のインターネットオプション(セキュリティオプション)の有効利用

信頼のおけるサイトとそうでないサイトを明確にし、信頼のおけないサイトを訪れる際には、セキュリティレベルを高め設定しておきましょう。(図は Internet Explorer 7 のインターネットオプション)



■ Internet Explorer でセキュリティを確保する(マイクロソフト株式会社)

<http://www.microsoft.com/japan/windows/ie/using/howto/security/settings.msp>

(5) スпамメールなどの、甘い誘いのリンクはクリックしない

スパムメールの甘い誘いに注意して下さい。(3)で示すような不審なサイトへ誘導されます。

素敵なおプレゼント?



(6) インターネット接続でのルータの利用や(パーソナル)ファイアウォールの導入と、それらの正しい設定・運用

インターネット経由の直接的な感染活動から、自分のパソコンやネットワークを守るために、ルータやファイアウォール(パーソナルファイアウォール)を導入することをお勧めします。

万が一、感染した場合でも、自分のパソコンあるいはネットワークの内部から、インターネット経由の情報漏えいや攻撃を未然に防ぐことができます。

(7) コンピュータ上のOSやアプリケーションを常に最新状態にしておく(Microsoft Update の実行など)

7. Web 運営者等におけるボット対策のポイント

Web の運営者等のインターネットを情報公開の場として利用するユーザは、ボットなどのウイルスの、感染活動の踏み台にならないために以下に示すような対策を行うべきです。

- (1) 侵入され、Web ページなどがボットの感染用に改ざん(ウイルスの埋め込みなど)されないように注意する**
- (2) コンピュータ上のOSやアプリケーションを常に最新状態にしておく**
- (3) 異常が見つかったら、即座に Web を閉鎖するなど被害拡大防止の措置をとる**

参考情報

対策を含めて、以下の資料を参照下さい。

- 情報セキュリティ白書 2007 年版 - 10 大脅威「脅威の“見えない化”が加速する」 -
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html
- コンピュータ・セキュリティ ～2004 年の傾向と今後の対策～
http://www.ipa.go.jp/security/vuln/20050331_trend2004.html
- ワクチンソフトに関する情報
<http://www.ipa.go.jp/security/antivirus/vacc-info.html>
- 悪意のあるソフトウェアの削除ツール
<http://www.microsoft.com/japan/security/malwareremove/>
- ボットネット(botnet)に注意
http://www.npa.go.jp/cyberpolice/detect/pdf/H170127_botnet.pdf
- サイバークリーンセンター(CCC 総務省・経済産業省 連携プロジェクト)
<https://www.ccc.go.jp/>

オンラインスキャン(ウイルス検査サービス)

- ◆ サイバークリーンセンター ボットの駆除手順
<https://www.ccc.go.jp/flow/>
- ◆ シマンテック セキュリティチェック
<http://security.symantec.com/sscv6/home.asp>
- ◆ トレンドマイクロ オンラインスキャン
<http://www.trendflexsecurity.jp/housecall/>
- ◆ マカフィー フリースキャン
<http://www.mcafee.com/japan/mcafee/home/freescan.asp>

IPA 対策のしおり シリーズ

<http://www.ipa.go.jp/security/antivirus/shiori.html>

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ対策のしおり

用語の説明

(*1) フィッシング(phishing)

金融機関(銀行やクレジット会社)などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為。釣り(fishing)と、偽装の手法が洗練されている(sophisticated)ことからphishingと言われているようです。

(*2) スпамメール(spam mail)

迷惑メール(UBE: Unsolicited Bulk Email)とも呼ばれ、商用目的かどうかによらず、個人的、宗教的なものも含めて宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのことです。

(*3) DoS 攻撃 (サービス妨害攻撃)/DDoS 攻撃 (分散サービス妨害攻撃)

サービス妨害攻撃(DoS攻撃)には、インターネットプロトコルの特性を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供できなくするような攻撃があります。このような DoS攻撃の攻撃元が複数で、標的とされたコンピュータがひとつであった場合、その標的とされるコンピュータにかけられる負荷は、より大きなものになります。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。

攻撃元は、攻撃者(人間)自身であるとは限らず、むしろ、攻撃者が事前に標的以外の複数サイトに攻撃プログラムを仕掛けておき、遠隔から一斉にDoS攻撃をしかける手法が広く知られています。

(*4) ぜい弱性 (vulnerability)

情報セキュリティ分野におけるぜい弱性とは、通常、システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことをいいます。オペレーティングシステムのぜい弱性や、アプリケーションシステムのぜい弱性があります。また、ソフトウェアのぜい弱性以外に、セキュリティ上の設定が不備である状態も、ぜい弱性があるといわれます。ぜい弱性は、一般に、セキュリティホール(security hole)と呼ばれることもあります。

(*5) バックドア(裏口)

コンピュータへの不正侵入(アクセス)を目的に仕掛けられる仕組みで、特定のポートを開き、そのポートを利用するサービスとしてプログラムを起動させること。このサービスにより、外部からインターネットを通じて、コンピュータへ侵入することができます。

(*6) IM(instant messenger)

インターネットに接続したパソコン同士で、チャットやファイルのやりとりができるソフトウェア。同じソフトを利用している仲間がインターネットに接続しているかがわかり、リアルタイムにメッセージを送ることができます。AOL Instant Messaging や MSN Messenger が有名。

(*7) IRC(Internet Relay Chat)

チャットシステムのこと。インターネット上のIRCサーバに、専用のソフトウェアを利用してアクセスすることで、複数のユーザとの間でメッセージの交換をすることができます。

(*8) ネットワークスキャン活動

ポートスキャンと言う手段を使い、対象のコンピュータの各ポートにおけるサービスの状態を調査すること。他のウイルスが仕掛けたバックドアなどが動作しているかも調査することができます。

本しおりを作成発行するにあたり以下の企業の協力を得ています。

(社名五十音順)

●株式会社アンラボ

<http://www.ahnlab.co.jp/>

●株式会社 Kaspersky Labs Japan

<http://www.kaspersky.co.jp/>

●株式会社シマンテック

<http://www.symantec.com/ja/jp/>

●株式会社ソースネクスト

<http://www.sourcenext.com/>

●トレンドマイクロ株式会社

<http://jp.trendmicro.com/>

●マイクロソフト株式会社

<http://www.microsoft.com/ja/jp/>

●マカフィー株式会社

<http://www.mcafee.com/japan/>



ボット侵入禁止

IPA

**独立行政法人 情報処理推進機構
セキュリティセンター**

〒113-6591 東京都文京区本駒込2丁目28番8号
(文京グリーンコートセンターオフィス16階)

URL <http://www.ipa.go.jp/security/>

【情報セキュリティ安心相談窓口】(コンピュータウイルスおよび不正アクセス)

URL <http://www.ipa.go.jp/security/anshin/>

E-mail anshin@ipa.go.jp