IPA 対策のしおり シリーズ (10)

標的型攻撃メール
<危険回避> 対策のしおり

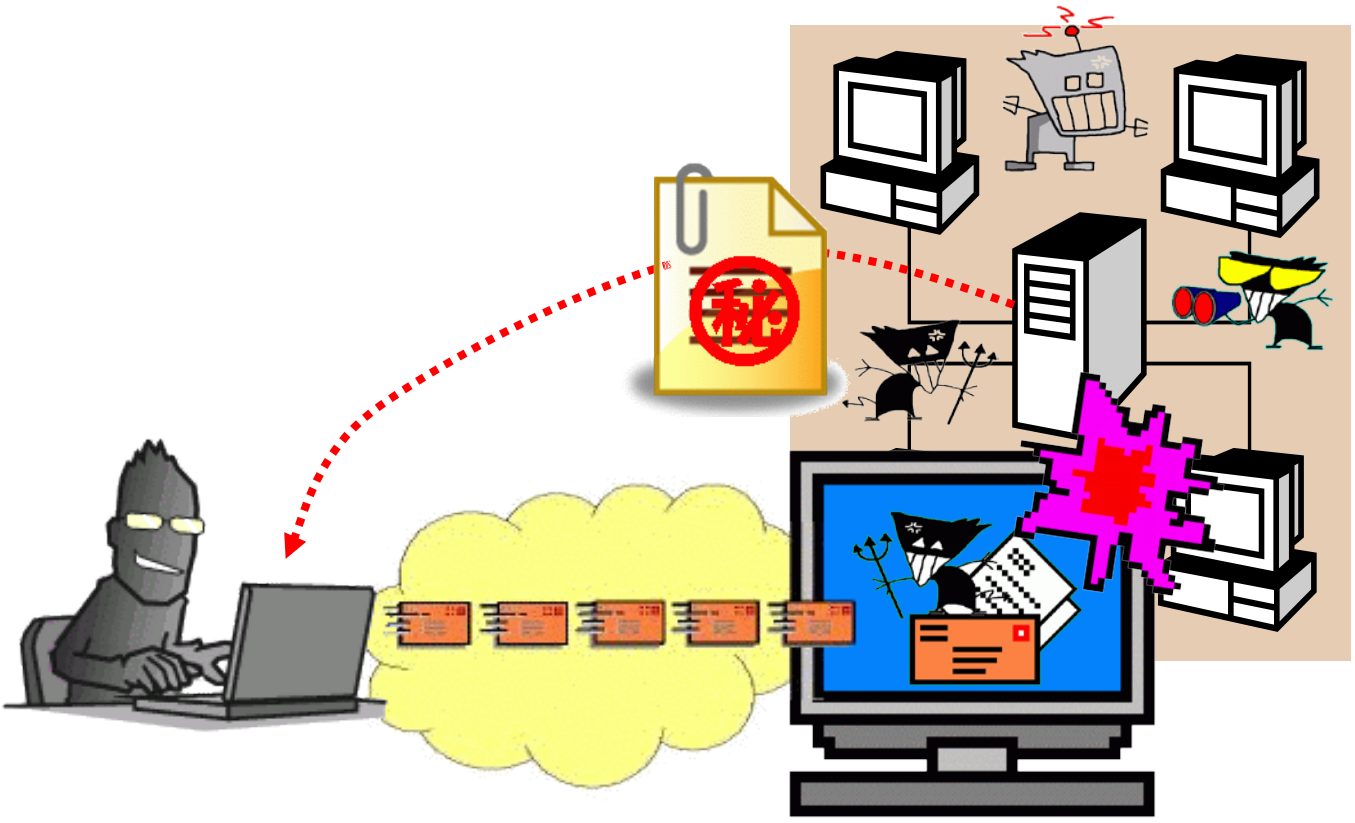
特定企業・組織への
狙い撃ち攻撃 その発端となる
最初の攻撃はメールから始まる!!

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/

2012年1月30日 第1版

目次



はじめに

本しおりは、コンピュータの一般利用者ではなく、企業･組織の従業者向けに作成したものです。企業･組織内でのセキュリティ教育等にご利用いただけると幸いです。

特定の企業･組織を狙い打ちする標的型攻撃と呼ばれる攻撃が流行しています。多くの場合、政府機関、仕事の関係者、友人･知人を装って、コンピュータウイルス付きの電子メールを攻撃の発端として送りつけてきます。

添付ファイルに仕込まれたウイルス*1を実行させるために、メール受信者の不信感を低減させる様々な「だましのテクニック」を駆使し、添付ファイルを開かせようとします。

- 受信者が興味を引くように、巧妙に細工された件名、本文
- 関係者を装った差出人
- ファイル名やアイコンに細工を施し、あたかもドキュメントファイルのように見えるアプリケーションファイル
- OSやアプリケーションの脆弱性を悪用して、内部に埋め込んだプログラムを実行させるドキュメントファイル

このような、様々な「だましのテクニック」を組み合わせて、受信者のパソコンにウイルスを感染させます。

自分は狙われない、うちの会社は攻撃のターゲットにはならないと思っていませんか？

攻撃者は攻撃しやすい相手を探し、狙い撃ちの攻撃を仕掛けてきます。普段からの自覚（セキュリティ意識）と、こまめな対策が貴方や貴方の会社を攻撃の魔手から守る手段です。

貴方が企業･組織の脆弱性（セキュリティ上の弱点）とならないように、日々の対策を実施しましょう。貴方がウイルスに感染すると、そこを突破口として企業･組織全体へウイルスのセキュリティの脅威が広がります。企業･組織が定めたセキュリティポリシーに即した、セキュリティ対策手順に従い、突破口とならないようにしてください。

*1）本文中に不正なウェブサイト(訪問者をウイルスに感染させるサイト)に誘導するリンクを持ったメールもあります。本しおりでは取り上げませんが、ご注意ください。

1. 標的型攻撃と標的型攻撃メール

標的型攻撃とは、主に電子メールを用いて特定の組織や個人を狙う手法です。典型的な例として、メール受信者の仕事に関係しそうなニセの話題等を含む本文や件名で騙し、添付ファイル（ウイルス）のクリックを促す場合が確認されています。

添付ファイルを実行（開いて）してしまうと、ウイルスに感染し、パソコン内の情報が漏えいする可能性があるだけでなく、パソコンが接続された企業･組織のネットワークにウイルスがばら撒かれ、企業･組織全体がセキュリティ上危険な状態になる可能性があります。

報道された標的型攻撃メールの事件

- 標的型攻撃で総務省の複数 PC がウイルス感染
  - 震災関連資料に見せかけたウイルス
- 参院に対しても衆院同様の標的型攻撃が発生
- 日本を含む世界の化学･防衛関連企業 48 社に標的型攻撃
- 外務省に標的型攻撃、一部在外公館で感染 － 情報漏洩は確認されず
- 防衛産業を狙ったウイルス攻撃が相次ぐ、日本や米国などで 8 社が被害
- 三菱重工がウイルス感染被害、
  「製品や技術情報の流出は確認されていない」
- 職員の PC のウイルス感染で、886 名分の個人情報流出の可能性（国土交通省四国地方整備局）

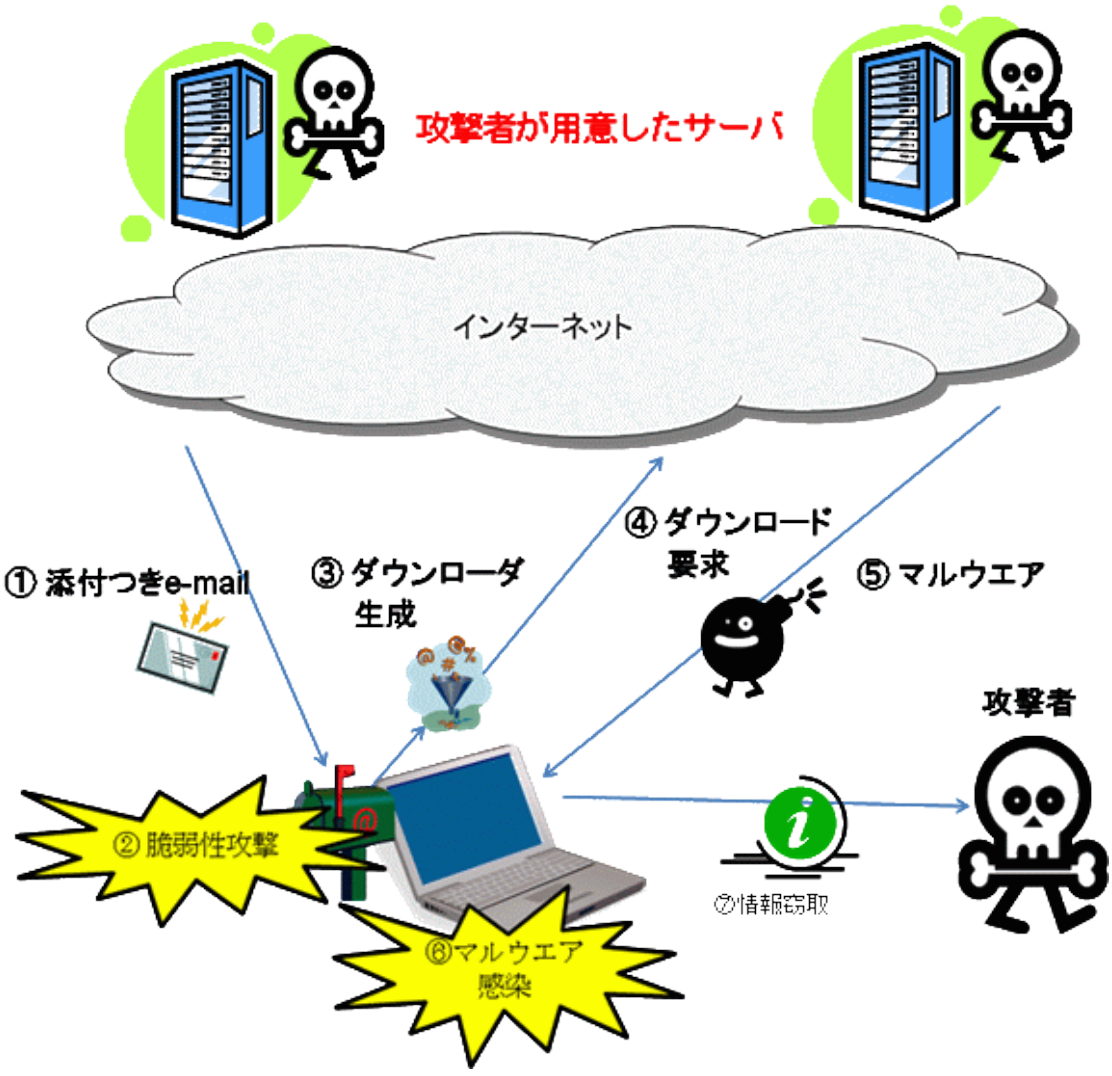
標的型攻撃が増加傾向

- ■ 公的機関や特定企業を狙った標的型攻撃が増加傾向である
  （事前にソーシャルエンジニアリングが駆使されている可能性大？）
- ■ 電子メールの添付ファイルに注意が必要!!
- ■ 定番のソフトウェアの脆弱性を悪用した攻撃が多い
  - ➢ **Adobe Reader、Flash Player、Word、Excel、一太郎など**
- ■ 添付ファイルからトロイの木馬に感染
- ■ 感染したら後は何が起こるかわからない

ホントに怖いトロイの木馬

- □ 一度侵入(感染)すると、別のマルウェア(ウイルス)を次々に取り込む(ダウンローダ)
- □ 自分自身をUpdateする(ウイルス定義の無効化)
- □ ウイルス対策ソフトを無効化しようとする
- □ 自分自身を隠蔽(Rootキット)する
- □ ウイルス対策ソフトのウイルス検査でトロイの木馬を検知したら、業務パソコンなら初期化(OS のクリーンインストール)がベター!!

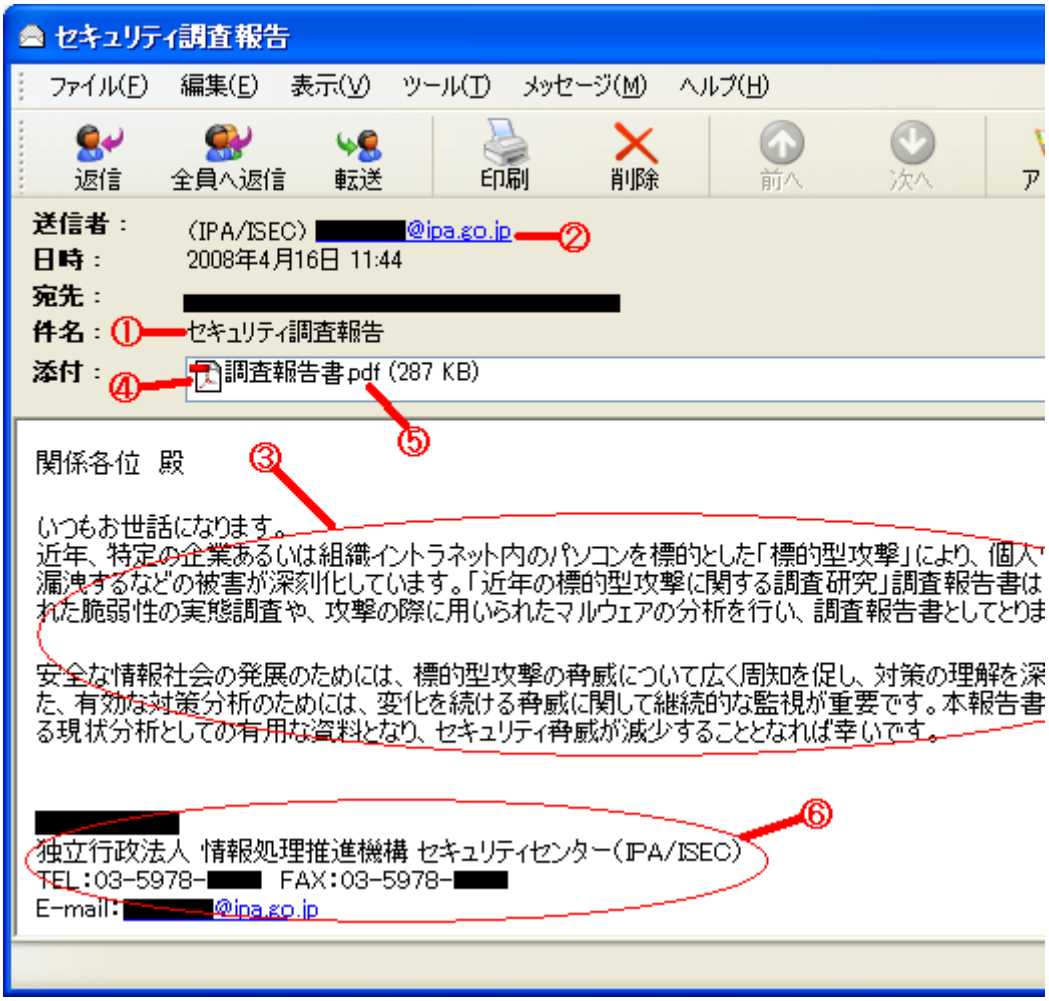
標的型攻撃によくある継続攻撃のイメージ



標的型攻撃メールの事例

標的型攻撃メールの特徴として、『ウェブ等で公開されている情報をメール本文にコピーしたり、ウェブに掲載された PDF の報告書を加工してウイルスを埋め込んだりする』事例が約4割あります。

以下に示す事例は、2008 年 4 月に、IPA を騙って政府関係組織に送られた標的型攻撃メールです。



メール本文や PDF ファイルは、2008 年 3 月に IPA のウェブに公開した報告書のプレスリリースの情報を利用しているため、メール受信者をだます次の条件を満たしています。

① メールの受信者が興味を持つと思われる件名
② 送信者のメールアドレスが信頼できそうな組織のアドレス
③ 件名に関わる本文
④ 本文の内容に合った添付ファイル名
⑤ 添付ファイルがワープロ文書や PDF ファイルなど
⑥ ②に対応した組織名や個人名などを含む署名

IPA（実在する担当者名）を騙り、Adobe Reader の脆弱性を悪用した仕掛けの施されたPDFファイルを添付ファイルとし、受信者に開かせようとした標的型攻撃メールの事例です。

このメールは、政府関係組織に対して送付されました。

本文には、IPA のホームページで掲載されたコンテンツの内容を切り出し、貼り付けたもので、ある程度日本語を解する攻撃者による犯行と推測されます。

このメールの添付ファイルを、受信者が、脆弱性を解消していないバージョンのAdobe Reader で開くと、受信者のパソコンが、添付ファイルに仕込まれたウイルスに感染するものでした。

実際に、宛先が不明のいくつかのメールがIPAに返送されたことから発見されましたが、セキュリティ関係者でIPAを知っている受信者であったならば、興味を引かれて添付ファイルを開くと考えられます。しかしながら、発見時点では感染報告はありませんでした。

こういった事例の他に、企業･組織内で実際に取り交わされたメールが悪用された事例もあります。

詳細は以下の資料を参照ください。

IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート
～だましのテクニックの事例 4 件の紹介と標的型攻撃メールの分析・対策～
http://www.ipa.go.jp/about/technicalwatch/20111003.html

2. 従業者の対策

OSやアプリケーションの脆弱性の解消

セキュリティベンダーであるトレンドマイクロ社の調べ*2によれば、標的型攻撃メールの添付ファイルの 50%はOSやアプリケーションの脆弱性を悪用したウイルスが仕込まれていました。

したがって、パソコン利用者は自分のパソコンで利用する OS やアプリケーションの脆弱性を解消し、常に最新の状態で利用することをお勧めします。

脆弱性を悪用される代表的なアプリケーションは、前述したように Adobe Reader、Flash Player、Word、Excel、**一太郎など**ですが、利用者はこれらのアプリケーションの脆弱性情報を収集し、常に最新の状態で利用する必要があります。

Microsoft 社の OS や Office 製品(Word、Excel など)の場合は、OS の機能として実装されている Microsoft(Windows) Update **機能**を利用して、これらを最新の状態にすることをお勧めします。

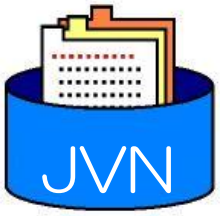
Adobe Readerの場合は、ヘルプ機能として実装された**"アップデートの有無をチェック"**機能で最新版かどうかを定期的に確認することをお勧めします。このチェックの際に利用可能なアップデートがある場合は、必ず適用することをお勧めします。また、**Flash Playerの場合**は、以下のサイトで利用中のバージョンが確認できます(使用中のブラウザ毎の対応*3が必要です)ので、最新版でない場合は最新版へのバージョンアップをお勧めします。

Adobe Flash Plyer (**使用中のバージョン確認サイト**)
http://www.adobe.com/jp/software/flash/about/

一太郎の場合は、以下のサイトを参照し、一太郎アップデートモジュールをご利用ください。

- **JUST SYSTEM サポート アップデート**
  http://www3.justsystem.co.jp/download/ichitaro/

これらのOSやアプリケーションおよび悪用される可能性のあるアプリケーションの脆弱性が発見された場合は、IPAとJPCERT/CC*4が共同運営するJVN（Japan Vulnerability Notes）のサイトに情報公開されます。コチラのサイトも参考にしてください。



- **JVN（Japan Vulnerability Notes）**
  http://jvn.jp/

[JVN に掲載されている情報]

JVN ではさまざまな脆弱性関連情報を収集し、原則として製品開発者との調整を通じて対策方法を準備したうえで、それらを分かりやすくまとめた形で掲載しています。製品開発者の対応状況には、脆弱性に該当する製品の有無、回避策（ワークアラウンド）や対策情報（パッチなど）も含まれます。

*2) トレンドマイクロ調べ
2011 年 11 月 8 日に公表された以下の資料
- **インターネット脅威マンスリーレポート － 2011 年 10 月度**
  http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20111107015156.html

*3) ブラウザ毎の対応
Adobe Flash Player は IE（Internet Explorer）用と、その他のブラウザ（例えば Firefox）用があります。それぞれのブラウザで上記のサイトを訪れて確認する必要があります。

*4) JPCERT/CC
JPCERT コーディネーションセンター（JPCERT/CC）は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデント(以下、インシデント) について、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっています。特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいます。

ウイルス対策ソフトは必須

標的型攻撃メールの添付ファイルに仕掛けられた不正コード（プログラム）が既知のウイルスであるならば、ウイルス対策ソフトで検知可能です。
また、既知のウイルスでない場合も、最新の“振舞い（ヒューリスティック）検知”機能が実装されたウイルス対策ソフトであれば、不正な動作を検知できる可能性があります。

パソコンには**ウイルス対策ソフト**を入れるなどのように、怪しいWebサイトや不審なメールを介したウイルスから、パソコンを守るための対策を実施することをお勧めします。

さらに、ウイルス対策ソフトの**ウイルス定義ファイルを自動更新**するなどのように、常に最新のウイルス定義ファイルにすることをお勧めします。

ただし、ウイルス対策ソフトは万能薬ではありません。**仮にウイルスの感染を許してしまった場合、ウイルスが変更したり破壊したりした設定や情報を復元することはできません。**ウイルス対策ソフトを入れているから絶対安全というわけではありません。過信は禁物です。あくまでも予防策としての利用が前提ですので、ご注意ください。

添付ファイルの拡張子や属性に注意

セキュリティベンダーであるトレンドマイクロ社の調べ(前述)によれば、標的型攻撃メールの添付ファイルの 50%は実行形式ファイル(Zip 形式で圧縮されている場合が多い)でした。

標的型攻撃メールの添付ファイルの 50%が実行形式ファイルであれば、添付ファイル(あるいは圧縮解凍後のファイル)の拡張子を確認することで、その脅威(ウイルスの実行)を抑止できる可能性があります。

実行形式ファイルを、別の形式のファイルと偽って、開かせようとするテクニックは、標的型攻撃以外のウイルス感染にも利用されるものです。ご注意下さい。

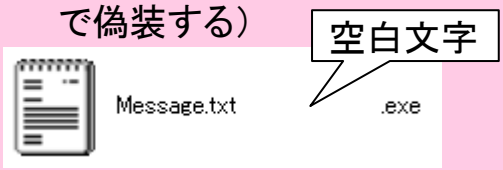
① ファイル偽装の手口

アイコンの偽装

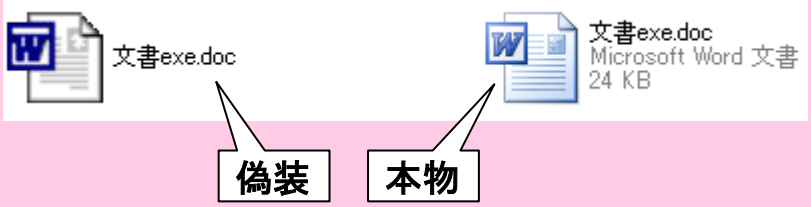
➔ 実行形式ファイルなのに文書ファイルや動画ファイル、画像ファイルのアイコンで表示

ファイル名の偽装

➔ 二重拡張子(本来の拡張子の前に空白文字を埋め込みニセの拡張子で偽装する)



➔ RLO トラップ(Unicode の制御文字[RLO:Start of right-to-left override]を利用してファイル名の拡張子を偽装する)



★偽装アイコンは理解し易いように簡易化してあります

ファイル属性の偽装

- ➔ 拡張子を非表示（Microsoft Explorer のフォルダオプション）を悪用してファイル属性を偽装
- ➔ 自己解凍形式の圧縮ファイルを偽装
- ➔ 「暗号化しています」等で何らかの操作を要求することで、利用者の注意をそむける偽装
- ➔ 圧縮前のファイルも偽装されている可能性があるので注意（**解凍したファイルも注意が必要**）

さらに、これらを組み合わせた高度な偽装を施す場合もあります。

② ファイル偽装の見破り方法

メールに添付された実行形式ファイルは安易に開いては危険です。

一番手っ取り早い方法は、**送信者に確認する**ことです。送信者が知り合いであれば、何らかの手段（電話等）で、メールを送信したか、添付ファイルを付けたか等の確認を行いましょう。

送信者に確認が取れない場合は、

- 確認する必要のある添付ファイルは、まずフォルダに移動する（必要なら圧縮･解凍ソフトで解凍する）
- 次に、**ファイルの属性（プロパティ）を確認する**（Windows OSの場合はファイル名にカーソルを当て、右ボタンクリックでプロパティを開く）
- ファイルの属性が偽装されているようなら開いてはいけません
- **自分で判断できない場合は、システム管理者等のセキュリティ専門家に相談しましょう**

詳細は、「IPA 対策のしおり シリーズ(1) ウイルス対策のしおり」を参照してください。

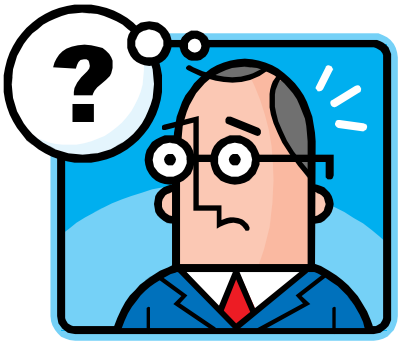
http://www.ipa.go.jp/security/antivirus/shiori.html

メールの差出人(送信者)･内容に注意

普段やり取りのない人からのメール、差出人にそぐわない内容、差出人と署名が別人などの不自然さがあれば、要注意‼ 可能ならば、差出人に確認しましょう。

自分で判断できない場合は、やはり、**システム管理者等のセキュリティ専門家に相談**しましょう。自分勝手な(中途半端な)判断が、企業･組織に大きな問題を引き起こす可能性があることを認識しておきましょう。

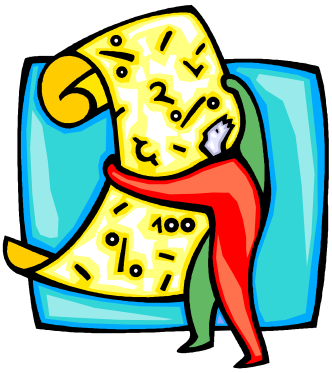
① 例えば、こんなメールも要注意‼



- 件名や本文が拙い日本語(自動翻訳？)
- 知らない差出人･企業からのメール
- 自分の業務とは無縁の内容
- あからさまに添付ファイルを開かせようとする内容
- 【大事なお知らせ】【緊急】【お急ぎ】【重要】などのキーワードが誇張されている件名

② こんな対策も有効

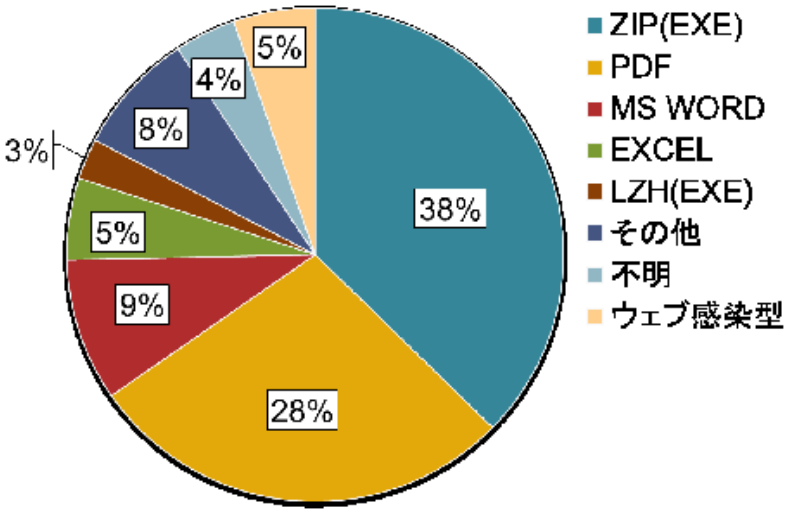
- 単純な署名からフィンガープリント(内容を保障)や電子署名(送信者を認証)まで、署名を有効に利用する
- いつもメールのやり取りをする人(企業)とは、あらかじめ符牒(お互いにしかわからない合言葉等)を取り決めておくのも有効です



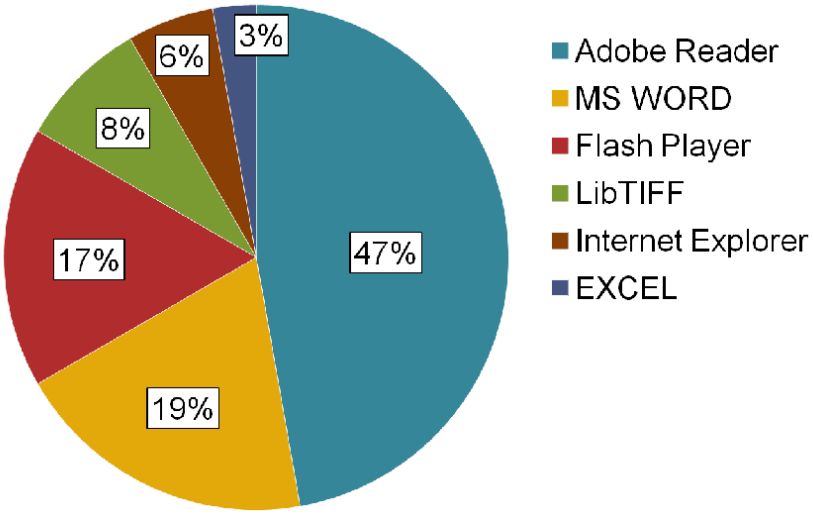
参考までに(IPA への届出・相談から)

IPA に届出や相談があった標的型攻撃メールの添付ファイルの形式を集計した結果は以下の通りです。

IPA が標的型攻撃メールの相談を受け付け始めた頃は、マスメール型ウイルスは、exe ファイル や exe を圧縮した zip ファイルがほとんどであり、標的型攻撃メールは MS Word や Excel、PDF ファイル などの文書ファイルでしたが、最近では exe を圧縮した zip ファイルが増えてきています。



次は、脆弱性を悪用されたアプリケーションを集計した結果です。
文書ファイルの多くは Adobe Systems 社の製品の脆弱性を悪用しています。



どちらのデータも、前述のトレンドマイクロ社のデータと同じ傾向を示しています。

詳細は以下の資料を参照してください。

IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート
～だましのテクニックの事例 4 件の紹介と標的型攻撃メールの分析・対策～
http://www.ipa.go.jp/about/technicalwatch/20111003.html

3. 組織の対策

ソーシャルエンジニアリング対応

標的型攻撃が行われる場合、攻撃者は、攻撃対象となる企業･組織についてソーシャルエンジニアリング*5を実施している可能性があります。攻撃のための事前調査ということになりますが、明らかにセキュリティ対策が軟弱である場合は、狙われやすいということになります（破れ窓理論*6）。

例えば、標的型攻撃メールの事例として、企業･組織内で実際に送受信されたメールを悪用されたものがあります。実際に使われたメールであれば、疑われずに開かれる確率が上がります。この事例がそうであるとは言いませんが、メールの誤送信や、メールが何らかの方法で盗聴された場合、あるいは不用意にSNS 等に掲載すると、攻撃者に悪用される可能性が高まります。メールの誤送信や重要情報の平文での送受信（本文テキストに直に重要情報を載せるような行為）は非常に危険です。それ以外にも、関係者のメールアドレスを流出させたりするセキュリティ事故も危険です。流出させた企業･組織を騙って、関係者に標的型攻撃メールが送信される可能性があるからです。

ソーシャルエンジニアリングと言えば、昔から企業･組織のゴミ箱漁りや、システム管理者と偽って従業者のアカウント情報を電話等で問合せるような行為が有名です。そういった意味では、情報（紙媒体や電子媒体）の安易な廃棄は危険です。また、不自然な問合せに安易に対応するもの危険です。

企業･組織の従業者には、こういった問題があることを意識させ、日頃からセキュリティ事故を起こさないための教育･指導が必要となります。

*5) ソーシャルエンジニアリング
ネットワークの技術やコンピュータ技術を用いずに、人間の心理や社会の盲点を突いて、パスワードなどの機密情報を入手する方法。例えば、言葉巧みにパスワードを聞き出す、廃棄物から重要な情報を読み取る、社員になりすまして盗み見や盗み聞きをする、など。ソーシャルハッキング、ソーシャルクラッキングと呼ばれることもあります。

*6) 破れ窓理論
「破れた（修理されない）窓のあるビル（管理がいい加減なビルなので防犯対策も緩いだろうと…）は、いずれ別の窓もすべて破られる（泥棒に狙われやすい）」といった理論。
同じ理屈で、情報セキュリティ対策の緩い企業･組織はサイバー攻撃の対象として狙われやすいと考えられます。

セキュリティ上のルールの指導と徹底

ソーシャルエンジニアリング対応と同じように、従業者に対する、企業･組織で定めたセキュリティポリシーにしたがったセキュリティ上のルール(対策手順)の指導と徹底は重要です。

標的型攻撃を水際で防止するためには、企業･組織の従業者のセキュリティ意識が統一されている(標的型攻撃に対して同じ問題意識を持つ)必要があります。たった一人の不注意から、企業･組織全体に問題を拡大させる可能性があることを認識させてください。

特に、一般的な従業者の対策に示した各種の対策については、ルール化し、教育･指導することをお勧めします。

情報共有

標的型攻撃は、特定の企業･組織を狙う場合が多いようです。不審なメールを受け取った場合は、それらのメールの情報をいち早く共有することで、被害の拡大を防止することができます。

標的型サイバー攻撃による被害拡大防止のため、2011 年 10 月 25 日、経済産業省主管の下、重工、重電等、重要インフラで利用される機器の製造業者を中心に情報共有と早期対応の場として、サイバー情報共有イニシアティブ(J-CSIP:Initiative for Cyber Security Information sharing Partnership of Japan)が発足し、IPA 内に『標的型サイバー攻撃の特別相談窓口』が設置されました。

標的型サイバー攻撃の特別相談窓口では、標的型攻撃に関する各種の相談に応じるだけでなく、情報の匿名化およびパートナー間での情報共有を行います。自分たちの企業･組織外へも影響のありそうな標的型攻撃メールを見つけた場合は、以下の連絡先に情報提供いただけると幸いです。

標的型サイバー攻撃の特別相談窓口

TEL: 03-5978-7509　　FAX: 03-5978-7518

メールサーバの設定

企業･組織が利用するメールサーバでは、メールに実行形式ファイルが添付できない、あるいは受信したメールに添付された実行形式ファイルを隔離する設定を行うことが、重要な対策となります。

思い出してください。標的型攻撃メールに添付されたファイルのうち 50%は実行形式ファイルであるという報告を…（本しおりの 9 ページを参照されたい）。

また、こういった設定は、標的型攻撃の実態と合わせて、企業･組織内の従業者に周知する必要があります。

フィルタリングの設定

トロイの木馬（ウイルス）は、いろいろな不正プログラムを、インターネットを介してダウンロードします（本しおりの 4 ページを参照されたい）。そこで、業務に無縁のウェブサイトを参照できないようにフィルタリングすることも、標的型攻撃による不正プログラムの侵入を抑止する効果があります。

ウェブサイトのフィルタリングをすると、いろいろな情報収集活動や営業活動に支障をきたす場合がありますが、従業者は、標的型攻撃から身を護るためにフィルタリングが必要であることを認識する必要があります。

物理的な対策

「はじめに」でも述べたように、本しおりは企業･組織の従業者向けに作成したものです。そのため、企業･組織のシステム管理部門が行うべき物理的な対策については詳細を掲載しません。

標的型攻撃に対する企業･組織がとるべき物理的対策については、以下の資料を参考にしてください。

- **「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を公開**
  http://www.ipa.go.jp/security/vuln/newattack.html

4. 参考情報

＜経済産業省＞

- 標的型サイバー攻撃への対応について ～参考資料～
  http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/005s_01_00.pdf
- サイバーセキュリティと経済 研究会 報告書 中間とりまとめ
  http://www.meti.go.jp/press/2011/08/20110805006/20110805006-3.pdf

＜JPCERT/CC 注意喚起＞

- 標的型メール攻撃に関する注意喚起
  http://www.jpcert.or.jp/at/2011/at110028.html

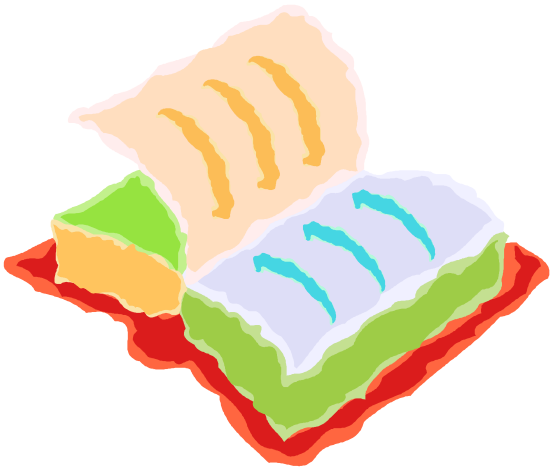
＜IPA 注意喚起＞

- プレス発表 標的型攻撃メールによるサイバー攻撃に関する注意喚起
  ～現実のものとなった国内基幹産業に対する攻撃を契機に、対策の見直しと徹底を～
  http://www.ipa.go.jp/about/press/20110929_3.html

＜IPA＞

- IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート
  ～だましのテクニックの事例 4 件の紹介と標的型攻撃メールの分析・対策～
  http://www.ipa.go.jp/about/technicalwatch/20111003.html

- 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を公開
  http://www.ipa.go.jp/security/vuln/newattack.html



＜しおり内に掲載した関連情報＞

- Adobe Flash Player（使用中のバージョン確認サイト）
  http://www.adobe.com/jp/software/flash/about/
- JUST SYSTEM サポート アップデート（一太郎）
  http://www3.justsystem.co.jp/download/ichitaro/index.html
- JVN （Japan Vulnerability Notes）：脆弱性関連情報の掲載サイト
  http://jvn.jp/
- インターネット脅威マンスリーレポート － 2011 年 10 月度 （トレンドマイクロ）
  http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20111107015156.html

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
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール 対策のしおり

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】
URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp