

# 学んで活かそう パソコン教室

PCセキュリティの実践

- 1 章：メールによる攻撃の種類と対処方法
- 2 章：ブラウザの攻撃の種類と対処方法
- 3 章：SNSのセキュリティ設定
- 4 章：質疑応答タイム

# 1章：メールによる攻撃の種類と対処方法

# 標的型メール攻撃

## 情報セキュリティ10大脅威2017

順位	組織	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	7位
3位	ウェブサービスからの個人情報の窃取	3位
4位	サービス妨害攻撃によるサービスの停止	4位
5位	内部不正による情報漏えいと それに伴う業務停止	2位
6位	ウェブサイトの改ざん	5位

\* IPA（情報処理推進機構）の2017年1月31日の発表資料より

# どんな攻撃なのか？

標的型メールとは、特定の相手を狙ってまるで疑う余地のない件名や本文でメールを送り付け添付のファイル経由で相手に**ウイルス**や**マルウェア**を感染させます。

この添付ファイルにはPDFファイルやWord、Excel、などの業務ファイルにウイルスが埋め込んであるケースが多いため、ウイルス対策ソフトで検知されにくい上にメールの受信者も不審に思わず開封して感染してしまうのです。

**マルウェア(malware)とは**：不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称で、コンピュータウイルスやワームなどがある。

**ランサムウェアとは**：マルウェアの一種である。これに感染したコンピュータは、利用者のシステムへのアクセスを制限する。この制限を解除するため、被害者がマルウェアの作者に身代金（ransomランサム）を支払うよう要求する。

# メールの特徴

難易度	特徴
低難易度	<p>他国語が混じっていたり、日本語の「てにをは」がおかしいなどの特徴を持つもの。 標的型攻撃に使われるなりすましメールの特徴をいくつか知っていれば、見分けられる可能性がある。 標的型メールではないもの。 広告メールやフィッシングメールなど、不特定多数の人に送られたもの。 基本的なセキュリティリスクをいくつか知っていれば、見分けられる可能性がある。</p>
中難易度	<p>業務に関連しているように見せかけたメールを攻撃者が作ったもの。 IPAなどのWebサイトにある記述をそのままコピーして利用したもの。 自分に関わりの無い内容が書かれていた場合は、見分けられる可能性がある。 セミナーの案内等見分けが難しいものもあるが、添付書類は安易な実行ファイルレベル。</p>
高難易度	<p>マルウェアを使って実際の業務メールを盗み出し、流用している本文や件名は過去に送受信された業務メールであり、見分けることは困難。添付書類もゼロデイが使用されるなど見極めは不可能。</p>

引用元 株式会社ラック

<https://www.lac.co.jp/library/guidebook/14.html>

# 対策は？

- ・添付ファイルを開かない。

  - ⇒ 実際には難しい。プレビューしただけで感染するタイプのものもある。

- ・メールサービスに危険性のあるメールを排除するゲートウェイサービスを経由させる。

  - ⇒ 有償サービス。（準推奨）

- ・管理者ユーザーでパソコンを使わないで標準ユーザーで運用する。

  - ⇒ 無償、インストールが自動で始まらないので安全性が高い。慣れた人に設定をお願いする必要がある。（推奨）

セキュリティのことを勉強するには

まずはここを抑える

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



# 様々なセキュリティ対策を学べる

[https://www.ipa.go.jp/security/antivirus/shiori.html#management\\_guidebook](https://www.ipa.go.jp/security/antivirus/shiori.html#management_guidebook)

IPA対策のしおりシリーズ			
1		<a href="#">ウイルス対策のしおり (第10版)</a> (815KB) ～コンピュータウイルスからあなたのパソコンを守るには!!～ (注1)	<a href="#">[英語版]</a> (1.6MB)
2		<a href="#">スパイウェア対策のしおり (第10版)</a> (822KB) ～気付かぬうちにスパイウェアに侵入されていませんか?～ (注1)	<a href="#">[英語版]</a> (4.4MB)
3		<a href="#">ボット対策のしおり (第10版)</a> (1.0MB) ～あなたのパソコンはボットに感染していませんか?～ (注1)	<a href="#">[英語版]</a> (2.1MB)
4		<a href="#">不正アクセス対策のしおり (第6版)</a> (779KB) ～大丈夫ですか、あなたのパソコン? (パソコン利用者向け) ～ (注1)	<a href="#">[英語版]</a> (3.2MB)
5		<a href="#">情報漏えい対策のしおり (第7版)</a> (795KB)	<a href="#">[英語版]</a>

## 2章：ブラウザの攻撃の種類と対処方法

# Webサイト経由の悪意のある攻撃

- A ワンクリック詐欺(不正請求) サイト
- B フィッシングサイト
- C 偽セキュリティ対策ソフトを提供するサイト
- D 迷惑ブログサイトあるいは迷惑ブログコメント・トラックバック

# 利用者の対策（IPAガイドより）

- パソコンの OS やアプリケーション（ブラウザやメールを含む）のぜい弱性を解消し（最新の状態にする）、**セキュリティゾーン設定**を強化（ActiveX、JavaScript の動作抑止）する
  - ウイルス対策ソフトで定期的にウイルス検査を実施する
  - 見知らぬ人からのメールや添付ファイルは安易に開かない
  - 銀行や信販会社からのメールを安易に信用しない
  - OS が表示する警告メッセージが出たら、慌てずに、自分の意思でないダウンロード要求はキャンセルする
- 
- 標準ユーザーでパソコンを使う（追加）

# 詳細情報リンク

- 身に覚えのない不正請求などの防止

<http://www.ipa.go.jp/security/personal/protect/oneclick.html>

- フィッシング (Phishing)対策

<http://www.ipa.go.jp/security/personal/protect/phishing.html>

- AntiPhishingJapan フィッシング対策協議会

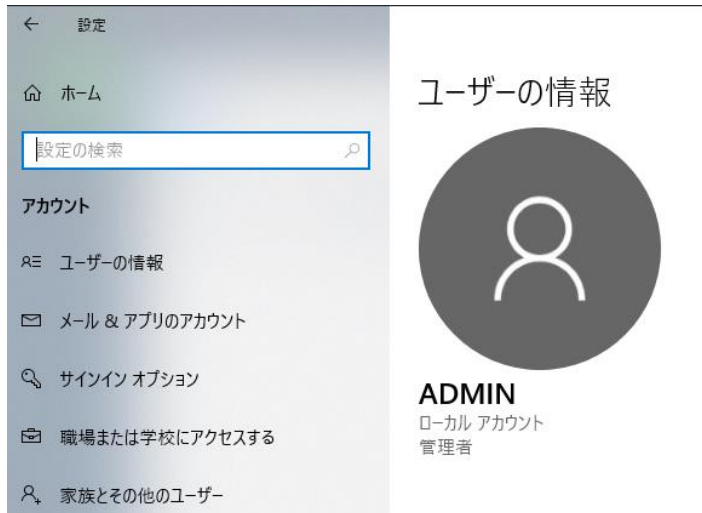
<http://www.antiphishing.jp/>

- セキュリティゾーンの設定

<http://www.microsoft.com/japan/windows/ie/using/howto/security/setup.mspx>

# ユーザーの違い

## 管理者



- ユーザーを作成・変更・削除可能
- アプリのインストール可能

## 他のユーザー

家族以外のユーザーが、各自のアカウントを使ってサインインすることを許可します。このようなユーザーは家族には追加されません。

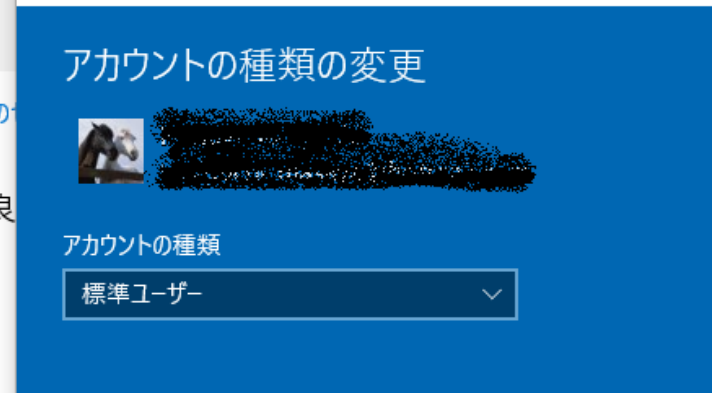
+ その他のユーザーをこの PC に追加



割り当てられたアクセスの

Windows をより良

フィードバックの送信



- ユーザーを変更可能
- ×アプリのインストール可能
- \*管理者の許可が必要になる

# 3章：SNSのセキュリティ設定

# Facebookプライバシー設定

https://www.facebook.com/settings?tab=privacy

検索

ホーム 友達を検索

一般  
セキュリティとログイン  
あなたのFacebook情報  
**プライバシー**  
タイムラインとタグ付け  
位置情報  
ブロック  
言語  
顔認識機能

お知らせ  
モバイル  
公開投稿

アプリとウェブサイト  
インスタントゲーム

## プライバシー設定とツール

アクティビティ	今後の投稿の共有範囲	友達	編集する
	自分のすべての投稿と自分がタグ付けされたコンテンツを確認		アクティビティログを使用
	友達の友達とシェアまたは公開でシェアした投稿の共有範囲を変更		過去の投稿を制限
検索と連絡に関する設定	私に友達リクエストを送信できる人	全員	編集する
	友達リストのプライバシー設定	公開	編集する
	メールアドレスを使って私を検索できる人	友達	編集する
	電話番号を使って私を検索できる人	全員	編集する
	Facebook外の検索エンジンによるプロフィールへのリンクを許可しますか？	はい	編集する

【ポイント】 最初の状態だと友達になりやすい（情報がオープン）になっている



# Facebook ブロック設定

The screenshot shows the Facebook interface with the 'Block List Management' page. The left sidebar contains various settings, with 'ブロック' (Block) highlighted. The main content area is titled 'ブロックリストを管理' (Manage Block List) and includes the following sections:

- 制限リスト (Restrict List):** Explains that adding someone to the restrict list prevents them from seeing your posts in your feed, but they can still see public posts and posts shared with mutual friends. A link to 'リストを編集' (Edit List) is provided.
- ユーザーをブロック (Block User):** Explains that blocking a user prevents them from viewing your posts, tagging you, or interacting with you in apps and games. A form allows blocking by name or email address, and a button labeled 'ブロックする' (Block) is visible. Below the form, it says 'さん ブロックを解除' (Unblock).
- メッセージをブロック (Block Messages):** Explains that blocking a contact in Messenger prevents them from contacting you. A form allows blocking the next message from a specific contact.
- アプリへの招待をブロック (Block App Invitations):** Explains that blocking app invitations prevents automatic acceptance. A form allows blocking invitations from a specific friend.
- イベントの招待をブロック (Block Event Invitations):** Explains that blocking event invitations prevents automatic acceptance. A form allows blocking invitations from a specific user.

不幸にしてトンでもない人から誹謗中傷を受けたら「ブロック」できる<sup>17</sup>

# Twitterプライバシー設定

ホーム

モーメント

16 通知

メッセージ



キーワード検索



ツイート



ユーザー情報

プライバシーとセキュリティ

パスワード

モバイル

メール通知

通知

Web通知

友だちを見つける

ミュートしているアカウント

ミュートするキーワード

ブロックしたアカウント

モバイル端末

## プライバシーとセキュリティ

### プライバシー

ツイートの公開設定

ツイートを非公開にする

オンにした後に投稿するツイートは非公開になります。現在のあなたのフォロワーと今後フォローを許可したアカウントのみにあなたのツイートが表示されます。オンにする前に投稿したツイートは公開された状態で残る場合があります。 [詳細はこちら](#)。

位置情報をツイート

位置情報付きでツイート

この機能をオンにすると、ウェブサイトやサードパーティアプリケーションから、都市や正確な現在地などの位置情報をツイートに追加できます。Twitter for iOSやTwitter for Androidには影響を与えません。 [詳細はこちら](#)

位置情報を削除

ツイートに追加した位置情報ラベルはTwitter.com、Twitter for iOS、Twitter for Androidに表示されなくなります。この変更が適用されるまで時間がかかることがあります。

自分を画像にタグ付けすることを許可

画像へのタグ付けをすべてのアカウントに許可する

画像へのタグ付けをフォロー中のアカウントのみに許可する

画像へのタグ付けを許可しない

見つけやすさ

メールアドレスの照合と通知を許可する

電話番号の照合と通知を許可する

この設定は電話番号を追加すると有効になります。 [今すぐ追加](#)

# 4章：質疑応答タイム