



## セキュリティ対策情報



### 大型連休明けのセキュリティ対策について

大型連休は大規模なサイバー攻撃が発生するため、**個人が各々適切に対策を実施しなければ甚大な被害が発生する場合があります。**以下にセキュリティ対策方法を簡潔にまとめましたので、必ずご確認ください。

なお、不審な点を発見された場合は、最寄りの総合情報基盤センターへ早急にご相談ください。

Check!

- OSに修正プログラムを適用する
  - Windows → Windows Update
  - Mac → ソフトウェア・アップデート
- 導入しているアプリケーションに修正プログラムを適用する
  - Adobe製品全般 (特にReader/Acrobat)
  - Java  Flash
  - JustSystem製品全般 (特に一太郎)
- ウイルス対策ソフトの定義ファイルを最新の状態に更新し、完全スキャンを行う

パソコン編



重要!

Check!

- 迷惑メールや標的型メール攻撃を防ぐ手段はありません
  - 上記のようなメールは必ず届くものと自覚する
  - ユーザの勘違いや操作ミスが狙われている点を自覚する
- メール情報の改ざんは容易に可能であることを理解する
  - 差出人情報はメールソフトの設定レベルで改ざんできます
  - HTML形式のメールは正規メールのソースコードをコピーするだけで誰でも全く同じものが作成できます
- メール本文にURLやリンクがある場合はまずは疑う
  - 少しでも疑問に思った場合は、インターネットで正規ウェブサイトを確認する一時間を加えましょう
- 標的型メール攻撃の添付ファイルはウイルス対策ソフトで検出できない場合があります
  - 標的型メール攻撃の添付ファイルは原則新種のコンピュータウイルスなので、注意が必要です
  - 確認が必要な場合は、最寄りの基盤センターへ相談ください
- 自身の操作に責任を持つ
  - 「気づかずに、ついすっかり、よく分からない」は免責の理由になりません
  - Enterやクリックは、押印署名と同様です (あなた自身が許可して、実行したものと解釈されます)
- 被害軽減のポイントは「初期対応」です
  - “しまった!”と思ったら、すぐに最寄りの基盤センターへ連絡を! (迅速に適切な初期対応をすることで被害は軽減できます)

メール編



Apple  
楽天  
...etc



Check!

- ネットワーク機器 (複合機やルータ等) に適切なセキュリティ対策を行う
  - 最新のファームウェアを適応する
  - 管理画面へ適切なパスワードを設定する
  - セキュリティ機能を活用し、適切な設定/管理を行う
    - アクセス制限機能
    - MACアドレス制限機能
  - 通信/利用記録等のログ (履歴) に不審な点がないか確認する

ネットワーク  
機器編



※ 機種やメーカーによって対応事項/方法が異なります。メーカーサイトを確認する/メーカーサポートに問い合わせる等、ご自身で適切に対応してください。

Check!

- 各種修正プログラムを適用する (yum update等)
  - 稼動サービス等の脆弱性に関する情報収集に努め、適切に対応する
- サーバーの設定や履歴の確認を行う
  - 強固なパスワードの設定 (8文字以上かつ大文字や数字を組み合わせる)
  - 稼動サービスの確認 (psコマンド)
  - アクセス制限等の適切な設定/管理
  - 接続/ログイン/操作等履歴の確認 (lastコマンド、/var/log配下の確認)

サーバ編



重要!

Check!

- CMSは最も狙われやすいシステムであることを理解する
  - CMSは便利な反面、運用には多くのプログラムが必要のため脆弱性やバグ等へ迅速に対応する必要があります
  - CMSは“使う”ものではなく“管理”するためのシステムです (システムの管理ができるからこそ運用が成立し、利用することができます)
  - 脆弱性に関する情報収集に努め、常に最新パッケージを適用する
- パスワード管理や履歴管理は適切に行う
  - 強固なパスワードの設定 (8文字以上かつ大文字や数字を組み合わせる)
  - ファイル/コンテンツの作成日時、アクセス/操作等履歴の確認

Web  
管理者編

Wordpress  
Joomla  
...etc



※ 記載事項は一般的な必要最低限の対策事項です。機器管理者は管理状況に合わせて適切に対応してください。

[参考] 情報セキュリティ (IPA)  
<https://www.ipa.go.jp/security/index.html>



富山大学 総合情報基盤センター  
2018年5月7日  
<http://www.itc.u-toyama.ac.jp/>  
内線 : 6946 (五福)

▶ バックナンバー : <http://www.itc.u-toyama.ac.jp/cn/>

Win10ユーザへ

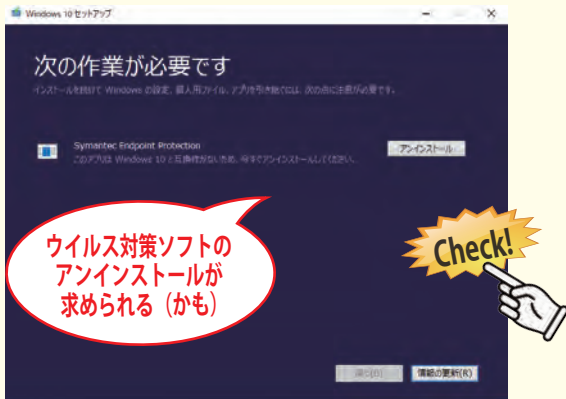
## Windows 10 April 2018 Updateにご注意!

### 概要:

4月30日にMicrosoft社からWindows10向けの大型アップデートが提供されました。初期設定の状態では、自動でアップデートが適用されます。

### 注意点:

古いバージョンのウイルス対策ソフトを導入している場合は、アップデート時にアンインストールを求められる場合がある。



### 原因:

Microsoft社ではセキュリティ向上のため、通常のアップデートでもOSのアップグレード並にシステムを大幅変更する仕様になりました。よって、ウイルス対策メーカーも大型アップデートには対応しきれず、基本的に事後対応(プログラムの改修が必要)になります。

### 対応と回避策:

ウイルス対策ソフトは最新バージョンをご利用ください。現在貸出を行っている最新バージョンは、動作することを確認しています。

正式対応版が提供され次第、アナウンスを行いますので、順次入れ替え作業を行ってください。

(参考)

Windows 10 April 2018 Update を発表 (Microsoft Windows Blog)  
[https://blogs.windows.com/japan/2018/04/27/windows10\\_april\\_2018\\_update\\_announcing/](https://blogs.windows.com/japan/2018/04/27/windows10_april_2018_update_announcing/)



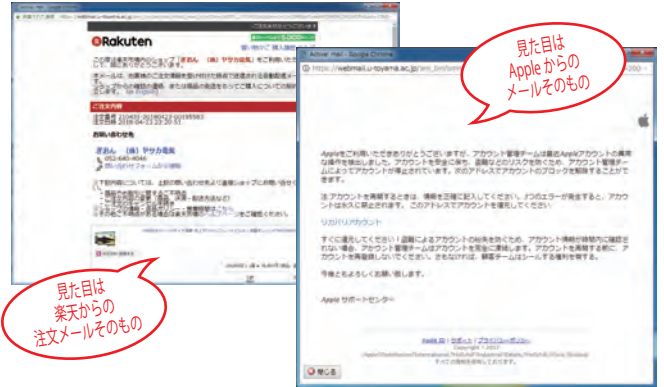
## 巧妙なフィッシングメールが届いています!



このところ見た目は正規のメールと遜色のないフィッシングメールが多数届いています。

このようなHTML形式のメールは、オリジナルのソースコードをコピーすることで、誰でも容易に同じメールが作成できます。リンク先がフィッシングサイトであったり新種のコンピュータウイルスが仕込まれている場合があります。

また、HTML形式のメールは、開いただけでウイルスに感染する場合もあるので、不審なメールは絶対に開かないでください。



## ウイルス対策ソフトの貸出しについて

センターではウイルス対策ソフトのライセンス貸与サービスを行っています。所定の利用申請手続きを行うことで、ウイルス対策ソフトが利用可能になります。ウイルス対策ソフトは2種類から選択可能です。

### ○ Symantec = 統合管理型セキュリティ対策ソフト

(AntiVirus機能に加えて、ファイアウォール等様々な機能を搭載し、機器のセキュリティを総合的に管理)

### ○ ESET = ウイルス対策ソフト

(AntiVirus機能に特化、機能を厳選しているため動作が軽快)

2つのソフトは「性格」が異なります。お好きな方を!

詳細は、センターのウェブサイトをご覧ください。

ITC HOME > サービス > ソフトウェア・ライセンスの貸与サービス(職員向け)  
<http://www.itc.u-toyama.ac.jp/service/license.html>

### 【最新バージョン】

- Symantec Win / Mac : 14.0.1 (RU1)
- ESET Win / Mac : 6.4~6.5系

macOS 10.13に対応しました!



## ～ OS以外もアップデートしていますか? ～

おまけのコラム

最近のOSは、初期設定で自動アップデートが実行される仕様になっているため、攻撃者やコンピュータウイルスはOS以外の脆弱性を狙っています。皆さんは、OS以外にアップデートが必要な事項を意識していますか?

Check!

- 導入しているアプリケーション (Java, Flash, 一太郎...etc)
- PCのBIOSやドライバ
- 周辺機器のファームウェア

ご存知ですか?

- アプリケーションにも自動アップデート機能が搭載されています。自動アップデートの設定を見直してみましょう。
- ハードウェアとOSを連携させるプログラムとしてドライバが必要です。メーカーのサポートサイトで修正バージョンが配布されている場合があります。また、パソコンにはドライバなどをアップデートするためのアプリケーションが付属している場合があります。
- アップデートが必要なものはパソコンだけではなく、インターネットに接続するものは、基本的にすべてにおいてアップデート必要になります。メーカーのサポートサイトを確かしてみましょう。

ちょっと解説



総合情報基盤センター

<http://www.itc.u-toyama.ac.jp/>