Iya-net Newsletter
富山大学
総合情報基盤センター
No.39

セキュリティ対策情報

重要

IT機器のセキュリティ対策について

情報セキュリティ対策を怠ったネットワーク機器を狙った攻撃が世界各国で報告されています。本学においても，IT機器が不正アクセス被害を受けたり，IT機器にソフトウェアを導入する際の不注意によりコンピュータウイルスに感染する等の情報セキュリティ事案が後を絶ちません。皆様には，IT機器の適正な管理を切にお願い申し上げます。

パソコン編

Check!

「緊急」のアップデートが公開されています。

- ☐ **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**
- ☐ **ソフトウェアを濫りに導入しない**
  （ソフトウェア導入時は，導入画面を注視し，適切な導入操作を行うこと）

サーバ編

Check!

- ☐ **各種修正プログラムを適用する（yum update等）**
  - ☐ 日ごろから稼動サービス等の脆弱性に関する情報収集に努め，都度適切に対応する
- ☐ **サーバーの適切な設定**

  - ☐ 適切なユーザ設定 / 管理
  - ☐ 適切なログイン設定
    - ☐ 強固なパスワードの設定（8文字以上かつ大文字や数字 / 記号を組み合わせる）
    - ☐ 公開鍵認証によるSSHログイン設定
  - ☐ アクセス制限等の適切な設定 / 管理
- ☐ **サーバーの履歴等の定期的な確認**
  - ☐ 稼動サービスの確認（psコマンド）
    - ☐ 不必要なサービスの停止
  - ☐ 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）

Linux系OSを利用中の方は必見！

※ 記載事項はLinux系OSを例とした必要最低限の対策事項です。サーバ機器を利用する前には，ご自信の知識 / 技術を考慮し，適切な管理方法をご検討願います。

ネットワーク機器編

Check!

無線LANルータ ネットワークプリンタ ご利用の方は要注意！

- ☐ **ネットワーク機器（複合機やネットワークプリンタ，ルータ，NAS（ネットワークストレージ）等）に適切なセキュリティ対策を行う**
  - ☐ 機器のセキュリティ対策状況を確認する。
  - ☐ 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設定する（8文字以上かつ大文字や数字 / 記号を組み合わせる）
  - ☐ 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

160.26.XX.XXのIPアドレスを設定したネットワーク機器は，初期設定では管理画面が学外からアクセス可能な状態です！ 重要

  - ☐ 通信 / 利用記録等の履歴に不審な点がないか確認する

※ 機種やメーカーによって設定事項 / 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。

番外編

ついでに確認！

LANケーブル ハブ編

- ☐ **LANケーブルの経年劣化を確認する**
  - ☐ 5年以上経過していないか（「カテゴリ5e」以上推奨）
  - ☐ 折れ曲がったり，ねじれたりしていないか
  - ☐ 接続部の"ツメ"が折れていないか
- ☐ **スイッチングハブの経年劣化を確認する**
  - ☐ 5年以上経過していないか（「ギガビット」対応製品推奨）
  - ☐ LEDが点灯していない or 接続が不安定なポートがないか

五福キャンパスでトラブル急増中！

[参考]

情報セキュリティ対策（IPA）
http://www.ipa.go.jp/security/measures/
国民のための情報セキュリティサイト（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

おまけのコラム

～「富山大学ネットワーク接続申請書」について～

ネットワーク管理におけるセンターと申請者（機器利用者含む）の責任分界点は，原則として情報コンセントとなります。この申請書は「学内ネットワークへIT機器を接続するための申請であると共に，機器に係る全ての責任を負う旨誓約する」ものです。申請者には，申請機器の管理責任が問われます。

⚠CAUTION⚠

富山大学 総合情報基盤センター
2015年6月15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/

Windows Server 2003 サポート終了

Windows Server 2003 および Windows Server 2003 R2 の公式サポートが2015年7月15日に終了します。サポート終了後は，新たな脆弱性が発見されても修正プログラム等のアップデートが提供されなくなり，脆弱性を悪用した攻撃による情報漏えいなどの危険性が非常に高くなります。**機器管理者は，Windows Server 2012 R2 へのアップグレードや機器更新等の対応を行ってください。**

※　Windows Server は，サーバのほかNAS（ネットワークストレージ）等のIT機器にも導入されている場合があります。
機器管理者の方は，機器の見落としにご注意ください。

[参考]
Windows Server 2003サポート終了（Microsoft社）
https://www.microsoft.com/ja-jp/server-cloud/products/windows-server-2003/

悪質なソフトウェアの導入に注意

フリーソフトや無料アプリ，ウェブサイト等の中には，悪意を持って（情報の搾取等を目的として）作成されたものがありますので，注意してください。

○ フリーソフト導入時の注意点

フリーソフトの中には導入時に余計なソフトウェアまで付随して導入される場合があります。導入画面内の記載事項を読み飛ばしたり，濫りに[OK]や[次へ]をクリックする等の不適切な操作はやめてください。

導入画面内に「○○ソフトウェアも導入する」，「○○へ匿名で情報を送信する」等の記載がされているにもかかわらず，[OK]や[次へ]をクリックした場合は，付随して導入されるソフトウェアがスパイウェアやマルウェア（※）であったとしても「許諾事項やソフトウェアの導入（インストール）に同意した」ことになります。

※ 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェア

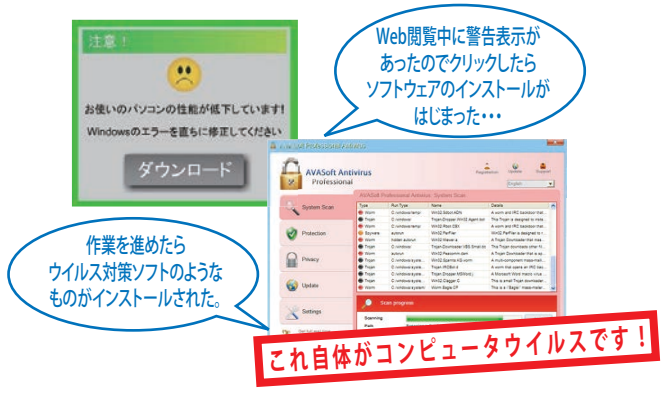
○ Webサイト閲覧時の注意点

Webサイト（管理元が不明確な海外のサイト等）の中には，コンピュータウイルス等が仕込まれている場合があります。最近では，セキュリティ対策を怠った機器がWebサイトを閲覧しただけでコンピュータウイルスに感染する事例も報告されています。ウイルス対策ソフトは導入していたが，パソコンに導入したJavaやFlash等ソフトウェアのアップデートを怠っていたことが主な原因です。

「OSのアップデート」と「ウイルス対策ソフトの導入」だけでセキュリティ対策が万全であるという考えは，もはや時代遅れです。

＜参考事例 ① ～付随されて導入されるソフトウェア～＞

＜参考事例 ② ～偽ウイルス対策ソフトの導入～＞



＜参考事例 ③ ～ランサムウェア（脅迫ウイルス）の感染～＞

総合情報基盤センター
http://www.itc.u-toyama.ac.jp/