Tya-net Newsletter
富山大学
総合情報基盤センター
No.50

連休明けのセキュリティ対策について

年末年始はサイバー攻撃の頻度が高くなるため，個々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等を簡潔にまとめましたので，必ずご確認願います。

なお，**不審な点を発見された場合は，早急に総合情報基盤センターへご相談ください。**

パソコン編

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　重要！

ネットワーク機器編

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

複合機は要注意！　重要！

※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。

サーバ編

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）　重要！

メール編

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ペ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手間を加えましょう
- □ 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，ついうっかり，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）

Web管理編

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は便利な半面，運用には多くのプログラムが必要な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

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
2019年1月4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/