Tya-net Newsletter
2014
富山大学
総合情報基盤センター
No.35

重要 長期休暇に係るセキュリティ対策について 重要

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。特に長期休暇明け直後は，セキュリティ対策に不備がある可能性が高くなります。

セキュリティ対策方法を機器毎に簡潔にまとめましたので，必ず実施願います。なお，不審な点を発見された場合は，最寄の総合情報基盤センターへご相談ください。

セキュリティ対策セルフチェックリスト

Check! パソコン編

- □ 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
  - □ Flrash
  - □ 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

Check! サーバ編

- □ 各種修正プログラムを適用する
  - □ 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／管理体制の確認を行う
  - □ ユーザ / パスワードの適正な設定／管理
  - □ 稼動サービス / スクリプト等の適切な設定／管理
  - □ 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
- □ 適切な連絡体制の整備を行う
  - □ 不測の事態に備え、管理業務を委託している業者および部署内の連絡体制を確認する

Check! ネットワーク機器編

- □ 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

⚠ あなたの機器，本当に安全ですか？

☑パソコン □無線LANルータ □プリンタ ...etc

（参考）

ITC HOME ＞ ウイルス・セキュリティ対策関連情報
http://www.itc.u-toyama.ac.jp/security/index.html

長期休暇を控えて 2014/04 (JPCERT)
https://www.jpcert.or.jp/pr/2014/pr140001.html

富山大学総合情報基盤センター
2014年8月18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/