

連休前後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予想されるため、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、早急に総合情報基盤センターへご相談ください。



連休前 (Before)

STEP1

- 【パソコンは・・・】
- OSのアップデートをしましょう。
 - Windows <https://www.microsoft.com/ja-jp/safety/protect/musteps.aspx> (Microsoft社)
 - Mac <https://support.apple.com/ja-jp/HT201541> (Apple社)

- 【ネットワーク機器は・・・】
- ファームウェアのアップデートをしましょう。
 - 各メーカーのウェブサイト (サポート) で手順を確認

STEP2

- 【パソコンは・・・】
- パソコンにインストールされているソフトウェアのアップデートをしましょう。
- [参考] 脆弱性情報 <https://www.ipa.go.jp/security/index.html> (IPA)

STEP3

- 機器の電源を切りましょう (=シャットダウン)。
- Point** 機器によっては、一時停止 (スリープ) モード中でもネットワーク機能がONになっている場合があるので長期不在時は電源を切りましょう。

STEP4

- LANケーブルを抜きましょう。
- Point** 万が一、何かの拍子で機器の電源がONになった場合でも、ネットワークに繋がらない状態であれば、事故を未然に防ぐことができるかもしれません。

連休明け (After)

STEP1

- LANケーブルを挿しましょう。

まずはこれ!

STEP2

- 【パソコンは・・・】
- ウイルス対策ソフトをアップデートしましょう。
- 【ネットワーク機器は・・・】 ※連休中も起動していた場合
- 必ず通信ログの確認をしましょう。
 - 各メーカーのウェブサイト (サポート) で手順を確認

利用前の確認事項

STEP3

- 心得**
- いつも以上に迷惑メールや怪しいメールが届きます。
 - 接続先のウェブサイトが改ざんされている場合があります。
 - 「なんとなく」「よくわからないけど」で機器を使う利用者が攻撃者のメインターゲットです。

Point サーバ管理者等は基本的に適切な対策を講じているため、末端の利用者をターゲットとして、踏み台にするのが主流の攻撃手法です。

利用OK!

STEP4

- 少しでも不審な点に気づいたら、操作する前に誰かに相談しましょう。

* 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>

お知らせ (事前告知)

Windows 7 のメーカーサポートが2020年1月14日に終了します。詳細については、次回のニュースレターで情報提供を行います。

[参考] 2020年1月14日に、Windows 7のサポートが終了 (Microsoft社)
<https://support.microsoft.com/ja-jp/help/4057281/windows-7-support-will-end-on-january-14-2020>



富山大学 総合情報基盤センター
2019年4月26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/>