

# サイバーセキュリティ パートナーシップだより



## 新年度、引継ぎを受けた端末を使用する際の注意事項!!

**引継ぎを受けた端末は、セキュリティ対策の確認を!!**

- ① 前任者のセキュリティ対策が甘かったりすると、OSやセキュリティソフト、各種ソフトウェアが長らく更新されていない可能性があり、脆弱性がそのままになっている可能性があります。
- ② 退職者等のアカウントが残っていると、退職者や第三者（攻撃者）から、不正にアクセスされるなど、知らない間に犯罪者に悪用されることがあります。



Check Point

### 修正プログラムの適用

OSや各種ソフトウェアの修正版の有無の確認と更新

OK

Check Point

### 適正なアカウント管理

退職者等の不要なアカウントは、管理者に連絡し、削除や停止

OK

Check Point

### セキュリティソフトの定義ファイルの更新とスキャン

- ・セキュリティソフトの定義ファイル(パターンファイル)を確認し、常に最新版に更新
- ・端末内だけでなく、USBメモリ等の外部記録媒体にもウイルスが混入していないか、利用する前にセキュリティソフトでフルスキャン

OK

Check Point

### パスワード管理

- ・新年度、引継ぎを受けた端末で、共有のアカウントを使用する際は、必ずパスワードを変更
- ・パスワードは「できるだけ長く」「複雑に」「使いまわさない」が基本

OK

### システム管理者の方へ

- ① **サーバ等の各種ログの定期確認**～不審なアクセスが発生していないか
- ② **アクセス権管理**～必要な部署(人)に必要なアクセス権を与えているか、 unnecessary アクセス権を与えていないか、退職者等の不要なアカウントを削除しているか
- ③ **パスワード以外の認証方法の導入**～生体認証等の導入を検討



サイバー犯罪相談事例  
対処法と対策・相談窓口



山口県警サイバー課LINE友達募集中!  
サイバー犯罪に関する防犯情報を配信中です。  
(詳しくは二次元バーコード参照)

