



サイバー攻撃による**情報流出**に注意！！

現在、様々な事業者、団体、企業を狙って
様々な手口でサイバー攻撃が行われ
情報流出事案が続発しています

個人
情報



基本的なセキュリティ対策を再確認してください

◆ 企業や団体の皆様へ ～情報流出を起こさないために～

1 OSやソフトウェアは最新の状態に

- ファームウェアの更新、修正パッチの適用は確実に！
 - 脆弱性のあるバージョンだと狙われてしまう
- A P I**への不正なリクエストを通じて悪用される脆弱性も…



2 パスワードの強化、認証強化機能の利用

- パスワードは、文字数15桁以上が推奨（パスフレーズが有効）
- 可能であれば、多要素認証やパスキーを利用して、さらに強化！

PASSWORD...



3 共有設定、アクセス権限の見直し

- ファイルやフォルダの共有範囲は、必要最小限に限定を
- アクセス権限は、業務上必要な権限のみを個別に付与
- 適切に設定することで、万が一侵入されても被害を最小限に抑えられる



個人情報保護委員会も対策を注意喚起しています

「大規模な漏えい等事案を踏まえた対応について（注意喚起）」

https://www.ppc.go.jp/files/pdf/261007_houdou.pdf



事例や原因、
対策方法などが
掲載されてます

＜保存期間を過ぎたデータや利用目的を終えたデータを残さないように＞

◆ 本人確認を行う事業者の皆様へ ～なりすましを防ぐために～

- 犯罪収益移転防止法等に基づき、本人確認の徹底を！

◆ 少しでも不審に思ったら警察に通報・通報を！！

- 警察庁 サイバー事案に関する相談窓口
- 広島県警察本部サイバー犯罪対策課（代表☎082-228-0110）
- 最寄りの警察署

