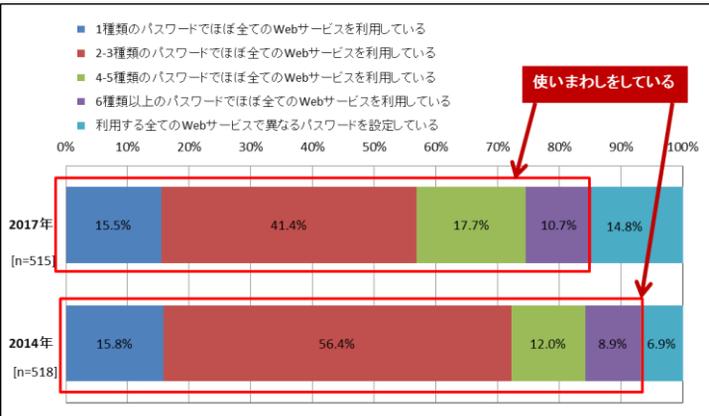




パスワード使いまわしのリスクとは！！

(2019年8月8日)



トレンドマイクロ - パスワードの利用実態調査 2017-  
[https://www.trendmicro.com/ja\\_jp/about/press-release/2017/pr-20171005-01.html](https://www.trendmicro.com/ja_jp/about/press-release/2017/pr-20171005-01.html)  
 パスワードを使いまわしている利用者が8割以上

Appleをご利用いただきありがとうございます。お客様のApple ID情報の一部は不足、あるいは正しくありません。お客様のアカウント情報を保護するために、検証する必要があります。  
**Appleを装った偽メール**  
 ご注意：24時間以内にお客様からのお返事がない場合にはアカウントはロックされます。

アカウント検証

**Rakuten 楽天を装った偽メール** 文ありがとうございます 入金で5,000ポイント

なぜこのメールを...  
 この電子メールは、完全に満足して...

Amazonを装った偽メール

ご注意ください...  
 Amazonをご利用いただきありがとうございます。アカウント管理チームは最近Amazonのアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを助ため、アカウント管理チームによってアカウントが停止されています。

様々なWEBサービスがある今、同じID・パスワードを使ってますよね  
 攻撃者もどれか一つの偽メールでID・パスワードがわかれば、他のWEBサービスにログインを試み、金銭につながる活動を行います！



JC3 犯罪被害につながるメールの具体例



攻撃のパターン

- 日本語メール、よく使われるサービスを装う = 日本は、パスワードを使いまわしが多く  
 どれか引っかければ他サービス (WEBメール・SNS・他サービス等) でも不正利用が可能
- 各サービスへログイン、不正利用、個人情報、業務ファイル等搾取

被害

- ・WEBメール (Yahoo、Gmail等) 盗み見、悪用、迷惑メール発信
- ・SNS (Line、Facebook等) なりすまし、情報搾取、金銭要求
- ・ショッピングサイト 不正利用・個人情報搾取
- ・AppleID 不正決済、iCloud情報 (連絡先、写真、ファイル等) 搾取
- ・オンラインストレージ (BOX、DropBox、OneDrive、GoogleDrive等) 情報搾取、悪用 ... etc.

対策

- よく利用しているサービスは不正メールがあることを知る、パソコン・スマホ問わず注意する
- 件名、差出人、本文が巧妙化しているため、少しでもおかしいと思ったら、サービス提供元に確認
- フィッシング対策の確認、メールのリンクからアクセスせず、お気に入り等からアクセスする
- WEBメールで利用しているパスワードは、他サービスのパスワードで絶対使わない！

情報源

日本サイバー犯罪対策センター (JC3) <https://www.jc3.or.jp/>