



# あさまセキュリティニュースレター

利用者の多いサービスからのメールは常に注意を！！ (2019年1月15日)

Amazonを装った偽メール



偽のログイン画面



偽のログイン画面  
今回は  
Amazon.co.jp  
となっているため、  
おかしいと気づく方  
も多いと思いますが、  
誤字のない本物そっ  
くりな場合もござい  
ますので、メールの  
リンクから開かない  
ように

利用者の多いネットのサービスは、悪用する  
攻撃者も多いと常に意識を！**文面もより信憑性  
を高める内容に日々進化！！**  
確認する場合も、メールのリンクからアクセス  
せず、正規のURLをお気に入り等に登録、毎回  
WEBブラウザから開き、確認しましょう



フィッシング対策協議会 HP抜粋

## 攻撃のパターン

- 日常使用する各種サービスからのメールを装い、偽サイトへ誘導、ID・パスワード情報を入力させる (本物そっくりのサイトを簡単に作成できるサービスがある)
- 入力した情報を元に、各サービスへログイン、他サービスでもログインを試みる (同じメールアドレス・パスワードの組み合わせを利用していると、他サービスでも不正ログインされてしまう)

## 被害

不正アクセス

登録情報の搾取

サービスの不正利用

他サービスでも不正アクセス被害

## 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する
- JC3等で最新の情報を得る、最新の脅威を知る、手口を知る、**全社員**がセキュリティに対し意識をもつ

## 情報源

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

フィッシング対策協議会 <https://www.antiphishing.jp/>