

# サイバーセキュリティ パートナーシップだより



R6-13



## 偽通知メールによる「フィッシング」に注意

フィッシングとは、実在する組織をかたって、アカウントのID やパスワード、ATM の暗証番号、クレジットカード番号といった個人情報を騙し取ることです。

電子メールやSMS のリンクから偽サイト（フィッシングサイト）に誘導し、そこで個人情報を入力させる手口が一般的に使われています。

### Eメールの例

件名：【重要】ご利用制限のお知らせ  
更新についてはこちらから（リンク）

### SMS の例

お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。下記よりご確認ください。<http://●●●.xyz>

### 精巧に作られた偽サイト（見分け困難）

#### アカウント

Eメールまたは携帯番号

パスワード

ログイン

#### クレジットカード

カード名義

番号

セキュリティコード

登録

入力した情報を盗み取り、悪用！！

フィッシング対策協議会によると、令和6年7月中は、**運送会社からの荷物配送**をかたるフィッシングの急増、次いで、**通信販売業者、電力会社、クレジットカード会社**をかたるフィッシングが大量に報告されているため、注意が必要です。

（引用記事：<https://www.antiphishing.jp/report/monthly/202407.html>）

メールやSMS で通知が来ても、確認する時は、

「いつもの」  
公式アプリ



「いつもの」  
公式サイト  
（ブックマーク）



フィッシング情報は、「**インターネット・ホットラインセンター**」へ通報を！



フィッシングに関する情報は、インターネット・ホットラインセンター（警察庁委託事業）の全国統一窓口となる「フィッシング 110 番」で受理しています。

寄せられた情報は、セキュリティ事業者等へ情報提供されますので、見つけた方は下記 URL から通報をお願いいたします。

インターネット・ホットラインセンター <https://www.internethotline.jp>

フィッシングにより実際に被害に遭われた場合は、警察へ通報・相談してください。



サイバー犯罪相談事例  
対処法と対策・相談窓口



県警ホームページにて広報資料や  
動画を公開中です。

（詳しくはQRコード参照）

