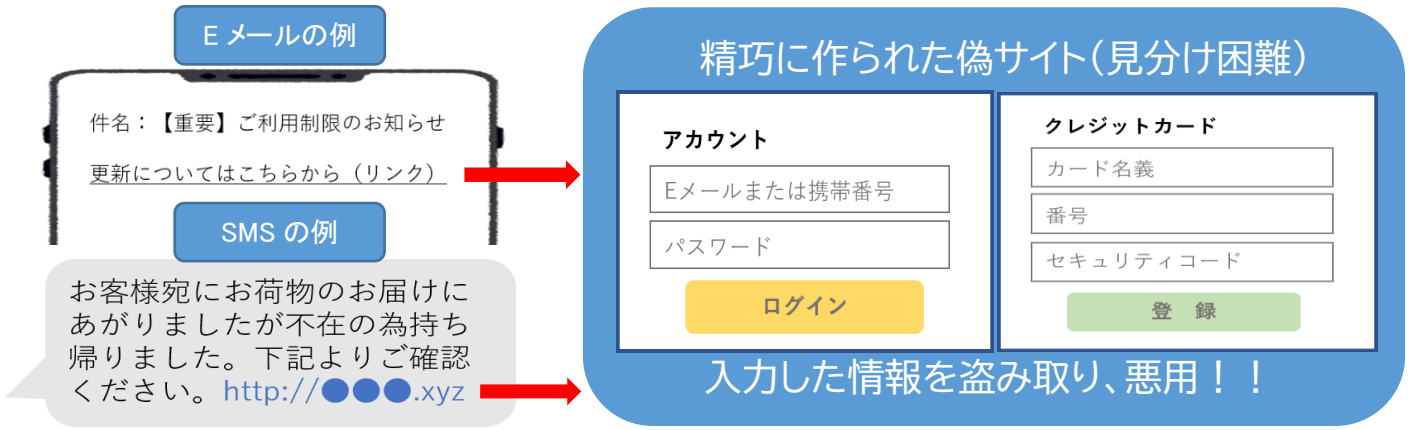
サイバーセキュリティ パートナーシップだより

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。



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、

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）

山口県警察本部サイバー犯罪対策課