NOTICE FROM

AIRPORT POLICE BOX

福岡空港警察署からのお知らせ

2026 2

サイバー犯罪の手口・対策

身近なサイバー犯罪として

○ **フィッシング**
実在する企業等を装った偽のメール又はショートメッセージ（SMS）を送り、その企業等を模した偽サイト等に誘導して、当該サイトでIDやパスワード、クレジットカード番号等を不正に入手する行為

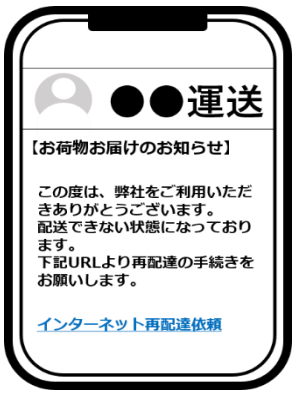
○ **偽サイト**
正規の企業等のホームページを模して作成されたサイト

○ **詐欺サイト**
商品を注文して代金を支払っても商品が届かないなど、実際に詐欺被害が発生したサイト

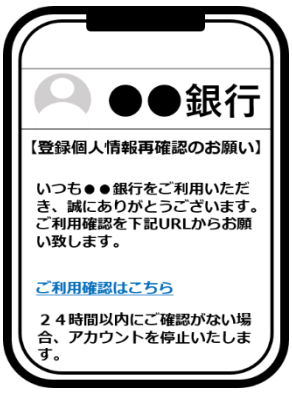
等の手口があります。

① あなたの個人情報等を狙う「フィッシングメール」の手口

宅配業者



金融機関



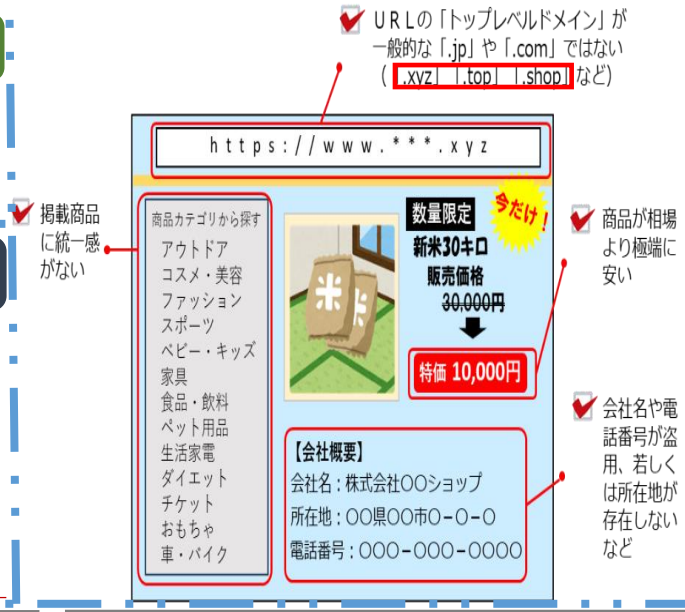
② 「フィッシングメール」の特徴

★ 宅配業者、金融機関等の実在する企業を装っている。
★ 他にも、クレジットカード会社、通信販売事業者、ETCサービス会社、官公庁を装ったフィッシングメールも多数存在する。
★ メール本文中に、「**重要、アカウント利用制限、至急、豪華特典**」等の言葉を巧みに利用し、リンクをクリックさせようとする。
★ 金融機関の口座番号、クレジットカード番号、暗証番号、住所等の個人情報、各種サービスのID・パスワード等の入力を求められる。

③ 「フィッシング」被害防止対策

★ **メールやSMSのリンクは開かない。**
★ **公式アプリや公式サイトから確認する。**
★ **ID・パスワードの認証情報や個人情報等を安易に入力しない。**

「偽・詐欺サイト」を見破るための着眼点



「偽・詐欺サイト」の被害に遭ってしまったら

★ **クレジットカード会社等に連絡する。**
クレジットカード番号等を入力してしまった場合は、カード会社に連絡して、支払いの停止を依頼してください。

★ **ID・パスワード等を変更する。**
ID・パスワード等を入力してしまった場合は、そのID・パスワード等を利用している全てのサービスにおいて、変更をしてください。

★ **サイト情報や相手とのやり取りの内容等を保存する。**

怪しい人・物を見かけたら
１１０番 または
福岡空港警察署
０９２－６２１－０１１０
へ通報のご協力をお願いします！

今からできる防犯対策

ダウンロードはこちら→