サイバーセキュリティ月間

「サイバーセキュリティは全員参加！」
令和8年2月1日（日）～3月18日（水）

２月１日から３月１８日は、政府が定める「サイバーセキュリティ月間」です。

サイバー犯罪の手口を知り、その対策について皆で考え、セキュリティ知識を高めましょう！

フィッシングに御注意！

銀行の偽メール

【●●銀行からの重要なお知らせ】

弊社では、金融庁によるマネー・ローンダリング及びテロ資金供与対策に関するガイドラインを踏まえ、お客様が弊社に登録されている各種情報等について、現在の情報に更新されているかどうかの御確認をさせていただいております。

■対象項目
・氏名/住所/電話番号/口座番号/暗証番号/ID・パスワード　等

■ご利用確認はこちらから

https://△△△.net/index.html

クリックしないで！

オンラインショップの偽メール

フィッシングによる被害に遭わないための対策

- ○ メールに添付されたＵＲＬを安易にクリックしない
- ○ ウイルス対策ソフトを導入する
- ○ 公式サイトやアプリで正確な情報を確認する
- ○ ＩＤ・パスワードの使い回しをしない
- ○ サービスごとに多要素認証を設定する
- ○ パスワードレス認証（パスキー）を利用する

だまされないで！

偽メール、偽サイトは、実在の企業名やロゴを使っており、見分けるのは困難です。

全ての受信メールに注意を払い、安易にＵＲＬに接続しないようにしましょう！

SNSアカウントへの不正ログインに注意！

ＳＮＳアカウントの乗っ取りが多発！！

昨年、多かったＳＮＳアカウント乗っ取りの手口として、「なりすまし」が挙げられます。これは、知人やインスタグラマー等になりすまして、「〇〇のアンバサダーに立候補したので投票して」とダイレクトメッセージを送信してきます。これに応じて、相手の指示に従い、端末を操作すると、ＳＮＳアカウントが乗っ取られてしまいます。

乗っ取りを防ぐための対策

○　電話番号や暗証番号を教えない

犯人は知人等を装い、電話番号を教えるよう要求してきます。電話番号を教えてしまうと、さらに「投票に必要なコードをＳＭＳに送るのでその番号を教えて」と言ってきます。でも送られてくるコードは、ＳＮＳの本人確認用の暗証番号なので、これを教えると、アカウントのパスワードがリセットされてアカウントを乗っ取られてしまいます。絶対に教えないでください。

○　ログイン通知を有効化にしておく

第３者がＳＮＳアカウントに不正にログインしたことが早期に分かるよう、「ログイン通知」を有効化しておき、見覚えのない端末からのログインを全てログアウトできるようにしておきましょう。

もしも、乗っ取られた時は・・・

○　サービス会社に連絡をする

ＳＮＳ運営元によっては、乗っ取りや不正アクセスの被害を報告するための専用のフォームがありますので、そのフォームを利用してサービス会社に連絡をしてください。

○　友人・フォロワー等に注意喚起する

可能であれば、別のアカウントや他の連絡手段（メール、ＳＭＳ）を使って、友人やフォロワー等に乗っ取られたアカウントから不審なメッセージが送られてくる可能性があることを注意喚起してください。