通販サイトを騙るメールに注意！

通販サイト（Amazonや楽天等）やクレジットカード発行会社になりすました偽メール・ＳＭＳが複数確認されています。
メールに記載されているリンクにアクセスせず、正規サイトからアクセスしましょう。

メール例１

※記載例以外にも多数の内容があります。

企業ロゴ

件名：支払い情報一致していません

客様
お客様のアカウントで異常な行為が検出されたため、お客様の注文とアカウントを停止させていただいております。
アカウントにログインして画面の指示に従うことで、アカウントの停止状態を解除していただけます。
恐れ入りますが、以下の情報をご確認のうえ、お支払い方法の変更。

〇〇ログイン>

メール例２

件名：アカウントの支払い方法を確認できず、注文を出荷できません。

〇〇e-NAVIお客様
残念ながら、あなたのアカウント
〇〇e-NAVIを更新できませんでした。
これは、カードが期限切れになったか。請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。
アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため〇〇e-NAVI情報を確認する必要・ェあります。今アカウントを確認できます。

〇〇e-NAVIログイン

対　策

1　メールに記載されたリンクにアクセスしない（アクセスしただけで、ウイルスに感染する場合もある）
2　リンク先にアクセスした場合、個人情報やID・パスワードを入力しない
3　不審なウェブサイトにID・パスワードを入力した場合は、速やかに停止、変更措置を執る
4　OSやセキュリティソフトは最新の状態に保つ
5　各会社のホームページ上に掲載されている注意喚起をよく確認する

参考リンク

- Amazon.co.jp　ヘルプ＆カスタマーサービス
  https://www.amazon.co.jp/gp/help/customer/display.html/ref=hp_gt_aiwem_al_pc?nodeId=201909120
- 楽天市場　ヘルプ・問い合わせ
  https://ichiba.faq.rakuten.net/detail/000013315?l-id=top_normal_footer_info_20200423
- 一般財団法人日本データ通信協会　迷惑メール相談センター
  https://www.dekyo.or.jp/soudan/index.html

秋田県警察本部　サイバー犯罪対策課