フィッシング詐欺メールの見分け方

騙されないための実践チェックリスト

フィッシング詐欺は「見た目」では見分けられない時代に

- 文章が自然で、差出人名も有名企業に見える
- 決済・配送・銀行・クラウドなど日常業務を狙う
- 忙しいときほど判断が鈍る



本質はシンプル：偽サイトへ誘導し、情報を盗む

フィッシングが狙う「人間の反射」

技術より心理を突く5つの反射スイッチ



緊急性 —「24時間以内に停止」



恐怖 —「不正アクセス」「アカウント凍結」



利益 —「返金」「ポイント当選」



手間の回避 —「ワンクリックで解決」



権威 —— 銀行・役所・大企業を名乗る

内容に飛びつく前に「まず疑う」動作へ切り替える

見分け方の基本は3点セット

判断は「差出人」「リンク」「要求内容」で決める



差出人が本物か

- 表示名ではなくアドレス/ドメインを確認



リンク先が本物か

- 見た目ではなく実際のURLを確認



要求が不自然ではないか

- "今ここで入力"を迫っていないか確認

チェックポイント①：差出人アドレス

表示名ではなく「@以降のドメイン」を見る



- **Example:**
  - 表示名: Amazon カスタマーセンター
  - 実アドレス: support@amazo0n-security.example（偽物の例）
- **Check:** @以降が公式サイトと一致するか確認
- **Warning:** フリーメール（@gmail.com等）からの企業サポートは高確率で偽

チェックポイント②：リンク先URL（最重要）

URLは「右から読む」癖をつける



https://support.**amazon.com**/...

Core to Check
(確認すべき核心部)

マウスを重ねて
実際のURLを確認
（スマホは長押し）

危険サイン

- ドメインが公式と違う
- 不自然に長い、意味のない記号が多い
- **http://**（暗号化されていない）[×]
- 公式名の一部だけ含む紛らわしいドメイン

- http://amazon-support.example.com
- https://login-update.xyz123.com

チェックポイント③：要求内容

企業がメールで求めないことは明確

- ID・パスワードの入力をメールから促す
- カード番号、暗証番号、セキュリティコードの入力
- 本人確認のための"再ログイン"をリンクで誘導
- 添付ファイルを開いて確認（請求書・領収書など）



本物の連絡は、公式アプリ/公式サイトで確認する導線になっている

代表的な手口パターン

よくある4つのフィッシングパターン



パターンA：アカウント凍結・不正ログイン通知

アカウントの緊急性や不正利用を装い、個人情報を入力させようとする手口。



パターンB：配送不在・関税・再配達

荷物の不在通知や関税未納を偽り、偽の追跡サイトや支払いページに誘導する手口。



パターンC：請求書・領収書（添付ファイル型）

未払いの請求書や領収書を装ったメールに、マルウェアを含むファイルが添付されている手口。



パターンD：クラウド共有通知

クラウドサービスの共有通知を装い、偽のログインページでアカウント情報を盗む手口。

いずれもメールのリンクは踏まず、公式から確認

安全な確認手順（迷ったらこれ）

事故を減らす5ステップの確認手順

1



リンクを踏まない・添付を開かない

(Don't click links / Don't open attachments)

2



公式アプリ or ブックマークから確認

(Check via official app or bookmark)

3



本当に必要な手続きなら公式サイト内で完結する

(Legitimate procedures can be completed on the official site)

4



不明なら公式サポートへ

(If unclear, contact official support - search the number yourself)

5



職場なら担当へ相談

(If at work, consult IT/Security)

メール内の電話番号やリンクから確認してはいけません

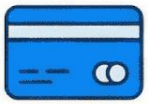
うっかり踏んだ・入力した場合の初動

被害を最小化する即座の対応



1. ID/パスワードを入力した場合

即座にパスワード変更、二要素認証を有効化



2. クレジットカード情報を入力した場合

カード会社に連絡し、利用停止や再発行



3. 添付を開いた場合

ネットワークから切り離し、担当部署へ連絡

早いほど被害が小さくなる

予防策：現実的な対策

個人でも職場でも効く5つの予防策

- **パスワードの使い回しをやめる（No Reuse）**
- **二要素認証を有効化（Enable 2FA）**
- **ブックマーク運用（Use Bookmarks）**
  - よく使うサービスは検索せずブックマークから
- **メールの自動フィルタ（Email Filters）**
  - 怪しい件名を振り分け
- **"迷ったら相談"をルール化**

まとめ

判断は"内容"より"導線"で決める



フィッシングの目的は常に同じ
リンクを踏ませる / 入力させる / 添付を開かせる

見分けるコツ
不安や焦りに乗らず、**3点（差出人・リンク先・要求内容）を機械的に確認**

怪しければ別経路で確認

5分で理解、一生使える防御スキル