

不審なメール・SMSを受け取ったときの確認チェックリスト

2026年10月22日更新・第1版 | webtechnote.com | <https://webtechnote.com/tools/suspicious-message-checklist>

この資料は、見た目だけで真正性を判断したり、安全性を保証したりするものではありません。迷ったときは、メッセージ内ではなく公式の経路から確認します。

1. まず操作を止める

- ・ 確かめるためでも、本文内のリンクをクリック・タップしない。
- ・ 予期しない添付を開かない。案内されたアプリを入れない。
- ・ メッセージ内だけに書かれた電話番号や返信先へ連絡しない。
- ・ ID・パスワード・カード・銀行口座・ワンタイムコード・個人情報・本人確認書類の画像を、その流れで入力・送信しない。

2. 公式の経路から別に確かめる

- ・ 自分で保存したブックマークや公式アプリからサービスを開く。
- ・ ブックマークがなければ、公式サイトを自分で探す。検索広告や検索結果だけを根拠にしない。
- ・ 公式のサービス内で、お知らせ・利用状況・注文・配送・支払いを確認する。
- ・ 連絡先は、公式サイト・公式アプリ・信頼できる手元の記録から探す。

送信者名、メールアドレス、ロゴ、自然な日本語、HTTPSの鍵マーク、急がせる文面だけでは、本物である証拠にはなりません。

3. いったん立ち止まる目印

- ・ 利用停止、未納、法的手続き、セキュリティ上の問題などを理由に急がせる。
- ・ 予期しないログイン、支払い、インストール、更新、コードの入力を求める。
- ・ 表示と異なるURL・ドメイン、短縮URLを使っている。
- ・ いつものサービス外へ支払い・連絡を移すよう求める。
- ・ アプリのインストールやコマンドの実行を求める。

これらは詐欺だと断定するためのものではなく、別経路で確認する理由です。

4. すでに操作した場合

リンクを開いただけ：画面を閉じて先へ進まず、公式の経路から状況を確認します。アプリやOSの更新も確認します。

IDやパスワードを入力した：公式の経路からサービスを開き、心配がある場合はパスワード変更、ログイン中の端末・セッション、多要素認証やパスキー、復旧手段を確認します。

カード・銀行口座・支払い情報を入力した：公式の金融機関またはカード発行会社の連絡先から、利用状況や必要な手続きを早めに確認します。

アプリを入れた・コマンドを実行した・端末に異常がある：状況に応じて操作を中止し、公式の案内や信頼できる支援先を確認します。自己判断で新しい削除ツールを追加しません。

出典（確認先） 警察庁「フィッシング対策」 <https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html> フィッシング対策協議会「利用者向けフィッシング詐欺対策ガイドライン 2026年度版」 https://www.antiphishing.jp/report/guideline/consumer_guideline2026.html 情報処理推進機構（IPA）「日常における情報セキュリティ対策」 <https://www.ipa.go.jp/security/anshin/measures/everyday.html>

年に一度、または重要な公式案内の変更時に見直します。PDFの最新版とHTML版は <https://webtechnote.com/tools/suspicious-message-checklist> を確認してください。