フィッシング詐欺を 無力化 する 5原則

見分けるより、危険な導線に近づかない。

本日のアジェンダ

01	**なぜ見分けにくいのか**	巧妙化するフィッシングの現状
02	**5原則の全体像**	危険な導線に近づかない考え方
03	**運用ルール**	リンク・広告・公式アプリ
04	**心構えと予防策**	焦らない、パスキーを使う
05	**今日からの行動**	自分の「引っかからない仕組み」を作る

INTRODUCTION

はじめに

フィッシング詐欺は「見分けるゲーム」になった

5原則の概要

完璧に見抜くより、危険な導線を使わない。
無理なく続く運用ルールに変える。

01 リンクは押さない
メール・SMS・DM

02 検索広告は押さない
スポンサー枠を避ける

03 公式アプリを使う
自分から開く

04 焦らない
一呼吸して確認

05 パスキーを活用
被害そのものを減らす

原則1：リンクは押さない

「重要そう」でも、リンクからアクセスしない。

対象：メール、SMS、LINE、SNSのDM、チャット

理由：偽サイトへ誘導される入口を最初に遮断できる

代替：公式アプリ、ブックマーク、手入力で確認する

どうしても迷うときは、本文・URL・緊急表現をAIに確認させる方法もある。
ただし、AIの判定も絶対ではない。

原則2：検索広告は押さない

検索結果の上部にある「スポンサー」「広告」は、正規サイトとは限らない。

広告枠が危険になり得る理由

検索結果の順位をお金で買えるため、偽サポートサイトや詐欺サイトが混ざる可能性がある。

公式サイトを探すときは、広告枠の下にある自然検索を使う。

検索結果そのものも偽装され得る。迷ったら、公式アプリやブックマークに戻る。

原則3：公式アプリを使う

通知を見たら、リンクではなく自分でアプリを開く。

メール・SMS 「不正利用」「再配達」	→	公式アプリ 銀行・カード・EC・配送

例：「荷物を届けられない」→ 配送会社アプリで確認
例：「カードの不正利用」→ カード会社アプリで確認

原則4：焦らない

焦らせる言葉は、判断力を奪うための仕掛け。

本日中に対応　至急確認　アカウント停止　不正利用を検知　本人確認が必要

まず一呼吸。

1. その場で操作しない　→　2. 公式アプリを開く　→　3. 明細・通知を確認する

原則5：パスキーを活用する

パスワードを入力する場面そのものを減らし、被害を防ぐ。

なぜフィッシングに強い？

パスキーは登録したサイトやアプリの識別情報に結び付く。偽サイトでは認証に使えない。

FIDOとGoogleも、フィッシング耐性を主要な利点として説明している。

使い方と注意点

端末の指紋・顔認証・PINで承認する。生体情報そのものは端末外へ送られない。

ただし、端末や基盤アカウントの保護、多要素認証も併用する。

出典：FIDO Alliance「Passkeys」、Google Developers「Passkeys」

まとめ — 次のステップ

大切なのは、見抜く力だけではない。
危険な導線に近づかない仕組みを、自分の中に作ること。

今日からのアクション

- メール・SMSのリンクを押さない
- 検索広告を避け、公式アプリを開く
- 焦らず、パスキーや多要素認証を設定する

「近づかなければ、無力化できる。」

記事：wnkhs.net「フィッシング詐欺を無力化する5原則」／補足：警察庁・FIDO Alliance・Google