



高度化するフィッシング AIで巧妙化するオンライン詐欺

本物のメールだと思って開いたら、じつは詐欺だった。そんな経験はありませんか？これは、サイバー犯罪者が個人情報などをだまし取るために使う「フィッシング」と呼ばれる手口です。現在では、AIの活用によってフィッシング詐欺はさらに巧妙になり、見た目や内容がいわゆる本物らしくなっています。このドキュメントでは、AIによって進化するフィッシング詐欺の実態と、そうした巧妙な攻撃から身を守る方法をご紹介します。



AIの進化でますます巧妙化するフィッシング詐欺

パーソナライズ攻撃

AIはSNSなどやオンライン上を寄せ集めて、あたかも本人宛てであるかのようなフィッシングメールを作成します。メールの内容にリアリティがあるため、本物かどうかの見分けがつきにくくなっています。

高まる文章のクオリティ

AIは誤字脱字のない正確な文章を生成するだけでなく、内容にも説得力を持たせることができるため、本物と見分けがつかないほど自然なメールを作成できます。

偽物の音声と動画

AIは実在する人の声をそっくりに再現して、その人が話しているような動画を作ることができます。たとえば、AI技術を使えば、あなたの友人が金銭を求める電話をかけてきたように装うことも可能です。

ターゲットを絞った標的型攻撃

AIは、単に説得力のあるメールを作成するだけではなく、サイバー犯罪者が仕掛ける攻撃手法そのものを進化させています。AIができること：

- フィッシング攻撃の成果をリアルタイムで解析
- サイバー攻撃の手法を高度化
- 特定の個人を狙ったリアルなメールを作成
- 過去の攻撃手法を学習し、さらに巧妙化

こうした標的型攻撃により、個人やセキュリティ対策がAIを使ったフィッシング攻撃を見抜くことは、これまで以上に難しくなっています。攻撃の高度化とともに、個人を狙った手口もいっそう洗練されています。現代のフィッシングはますます巧妙になっており、従来のセキュリティ対策では防ぎきれないほどに進化し続けています。



注意すべき点

AIを使ったフィッシングには、次のような特徴が見られることがあります：

- 不自然な言い回しや口調の不統一
- 文体や表現の一貫性のなさ
- 内容にそぐわない言葉遣い
- 矛盾や不整合のある個人情報の記載

セキュリティ強化のために今すぐできる対策

- すべてのアカウントに多要素認証を設定する
- パスワードマネージャーを活用して、強力なパスワードを作成・管理する
- 送信者に見覚えがあっても、安易にリンクを開いたり、添付ファイルをダウンロードしない
- 個人情報や機密情報を確認する際は、別の連絡手段を使う

警戒心を忘れず、サイバー犯罪に備えましょう

日頃から警戒心を持ち、セキュリティ対策を習慣化することで、サイバー攻撃や詐欺から身を守ることができます。

不審な点に気づいたら、すぐに報告しましょう。少しでも違和感を覚えたら、慎重に行動し、自分で確認する姿勢を大切にしてください。個人情報や機密情報をオンラインで投稿・共有することは避けましょう。