

第1回 安心安全なAIの使い方

個人情報漏洩・AIなりすましから身を守る

2026年6月21日（日） 10:30–11:30

主催：小林 正和

本日の流れ

- 1 AIアプリの個人情報設定
- 2 AIフィッシング詐欺
- 3 AIなりすましの犯行手順デモ
- 4 見分け方と検知ツールのデモ
- 5 今日から守る3原則

みなさんのスマホ内AIアプリ設定を確認

認証コードを狙う手口

これからはビデオ通話も怪しい

少しでも怪しいと思ったら確認

迷った時の行動ルール

難しい専門用語を噛み砕いて説明することを優先します。



設定

個人情報を守る



防御

詐欺を防ぐ



確認

なりすまし対策

今日のゴール

スマホを設定して個人情報をAI学習から除外する。

実際のデモを通じてなりすましを見抜く。

AIに入れてはいけない情報

まず「入力前に止まる」ことが大切です

そのまま入力しない

本名／住所／電話番号／勤務先／
顧客情報／パスワード／認証コード

入れる前に加工する

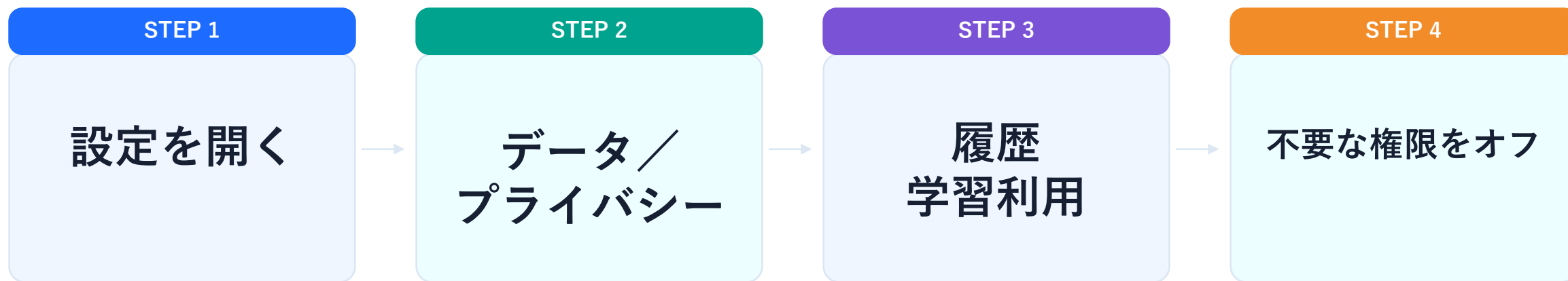
写真・PDF・メール本文は、個人情報
を消してからAIに相談します。



ぼかす例：「横須賀市日の出町1-5」 → 「横須賀市内」

AIアプリを使う前の設定確認

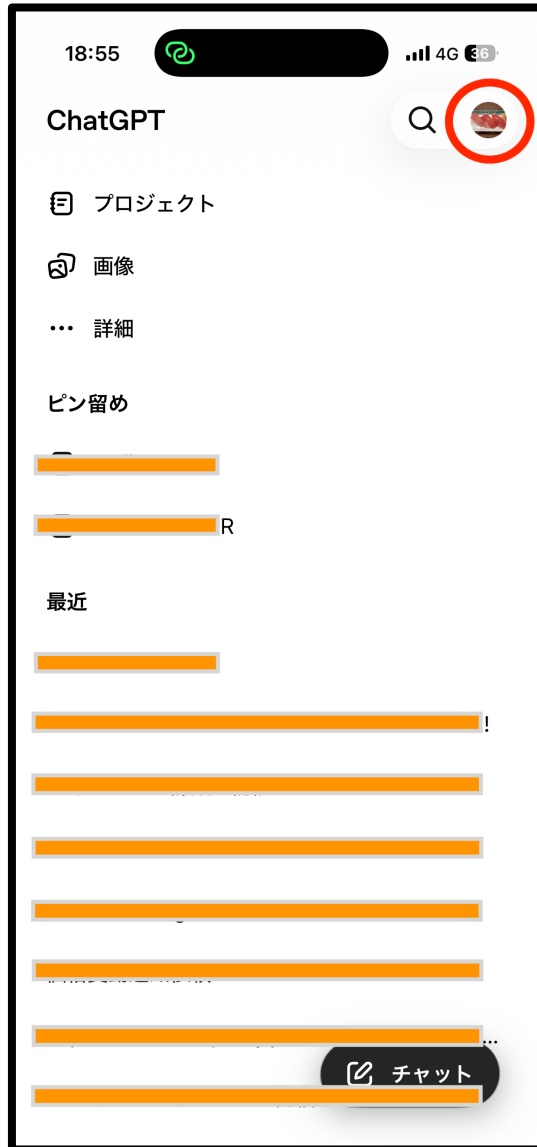
設定名は変わることがあるため、探すキーワードを覚えます



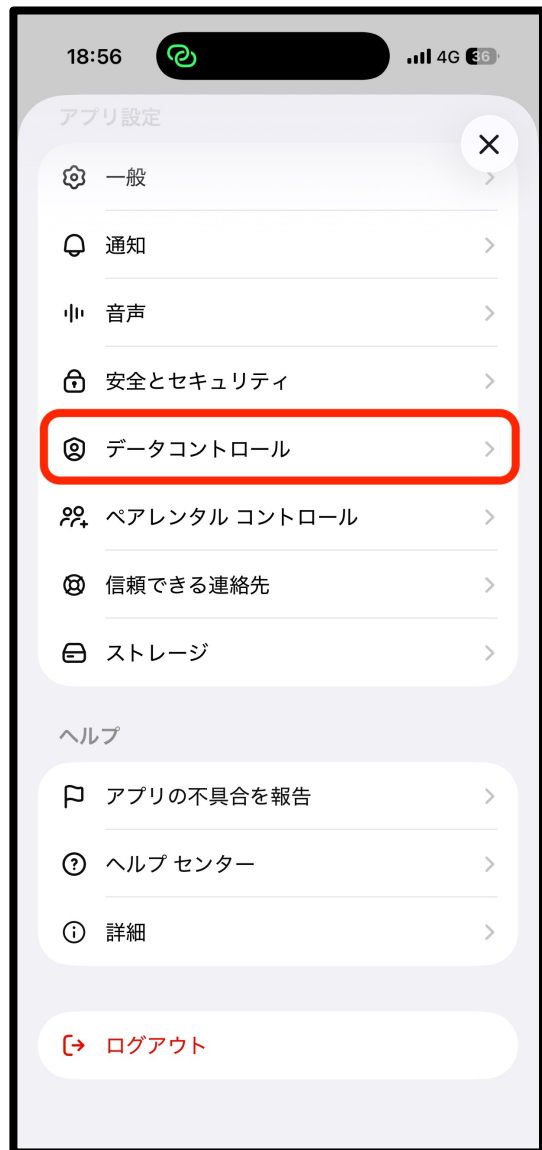
探す言葉：データ／プライバシー／学習／履歴／
モデル改善／音声／写真／位置情報

それでは、設定していきましょう！

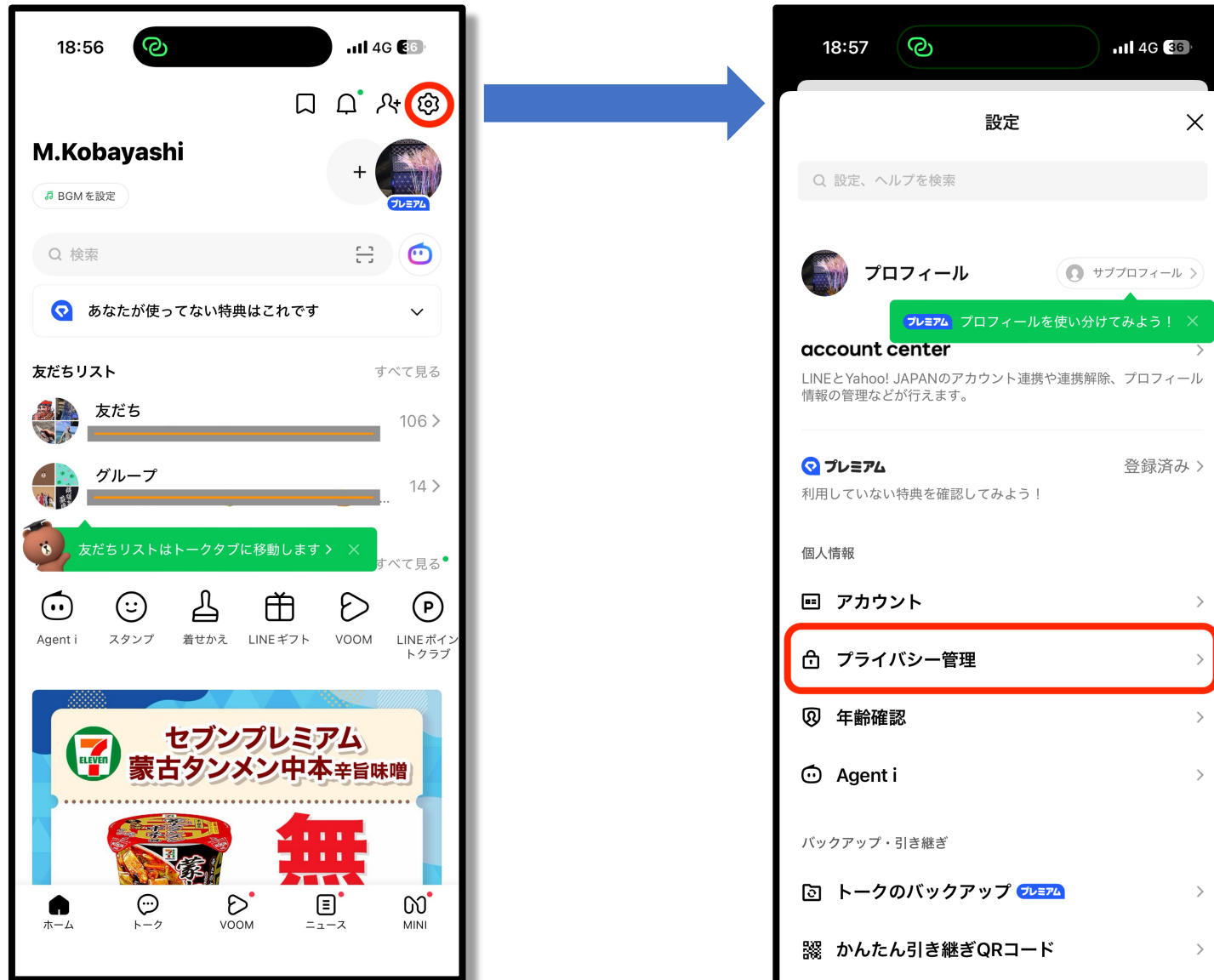
実際に設定していきましょう①（ChatGPT編）



実際に設定していきましょう②（ChatGPT編）



実際に設定していきましょう① (LINE編)



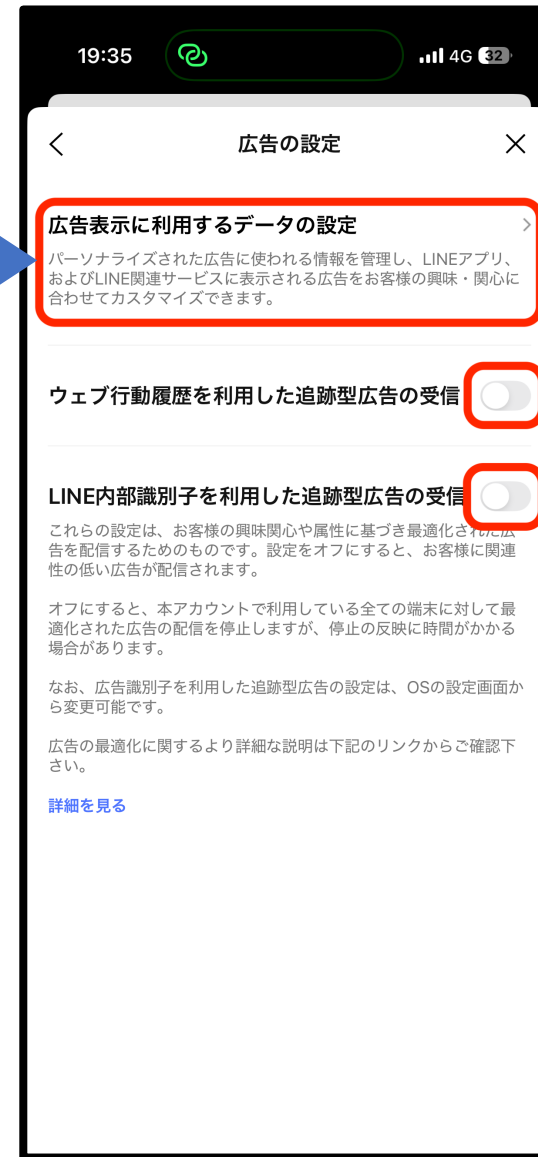
実際に設定していきましょう②（LINE編）



実際に設定していきましょう③（LINE編）



1. 個人情報設定



Komsa AI Security Seminar 2026

実際に設定していきましょう④（LINE編）



実際に設定していきましょう⑤（LINE編）



実際に設定していきましょう⑥（LINE編）



スマホで確認するチェックリスト

✓ **AIアプリの履歴・学習利用**
モデル改善に使われる設定を確認

✓ **写真・マイク・位置情報**
不要な権限をオフ

✓ **連携アプリ・ログイン端末**
知らない連携を解除

✓ **入力前のマスキング**
氏名・住所・番号を消す

覚える一言：AIに入力する情報は、個人情報を「消す・ぼかす・置き換える」

AIフィッシング詐欺：本物の画面に見えても危険

認証コードやログイン許可を狙う攻撃があります

Kali365型の特徴

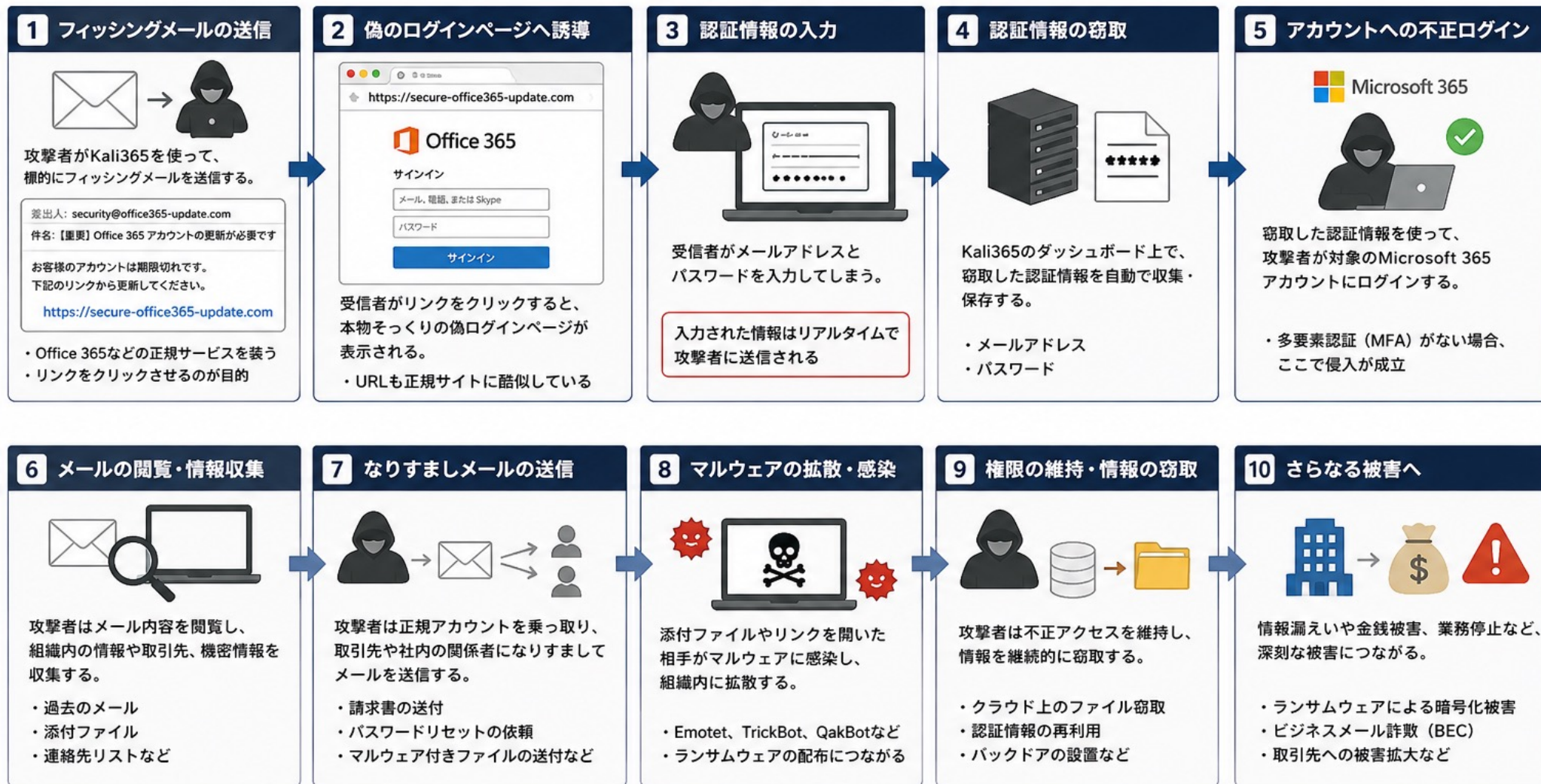
AIで自然な文章を作り、Microsoft 365の認証を悪用してアクセス権を奪います。

危険なサイン

「このコードを入力」
「今すぐ確認」
「アカウント停止」

防御ルール：**多要素認証（MFA）**を設定する

Kali365の犯行手順（攻撃の流れ）



Kali365の特徴

- フィッシングキットをクラウド上で提供（サービス型）
- 誰でも簡単に高度なフィッシング攻撃を実行可能
- リアルタイムで認証情報を窃取
- 多要素認証を回避する仕組みも提供



対策のポイント

- 多要素認証 (MFA) の導入
- フィッシングメール訓練の実施
- 不審なメールやリンクを開かない意識
- セキュリティゲートウェイやメールフィルタの強化
- ログイン履歴の監視
- インシデント対応体制の整備

AIなりすましの犯行手順

「声が本物っぽい」だけで信じさせる手口です



止めるポイント

[急ぎ][秘密][認証コード][送金]が出たら、一度確認する思考を。
会話を切り、公式番号・別の連絡手段で確認します。

今までの個人情報流出による悪用例

1 偽メッセージが届く

銀行・宅配会社・ECサイト
などを装ったメールや
SMSが届く



2 リンクをクリック

「至急確認」「アカウント停止」
など不安をあおってリンクを
押させる



3 偽サイトへ誘導

本物そっくりのログイン画面や
支払い画面が表示される



4 情報を入力してしまう

ID・パスワード・クレジットカード
番号・認証コードなどを
入力してしまう



ユーザーID ●●●●●●	CREDIT CARD 1234 5678 9012 3456 00/00
パスワード ●●●●●●	認証コード 1 2 3 4 5 6

5 犯人が悪用

不正ログイン、送金、買い物、
個人情報の悪用につながる



これからの個人情報流出による悪用例

1 AI音声クローン詐欺

家族・上司・銀行員などの声をまねて、緊急送金や認証コードを要求する



2 ディープフェイク動画なりすまし

ビデオ通話や会議で本人そっくりの映像を使い、信用させて指示を出す



3 セーフティ機能を外したLLMの悪用

詐欺の会話文、フィッシング文面、反論への切り返し、標的別メッセージなどを自動生成して悪用する



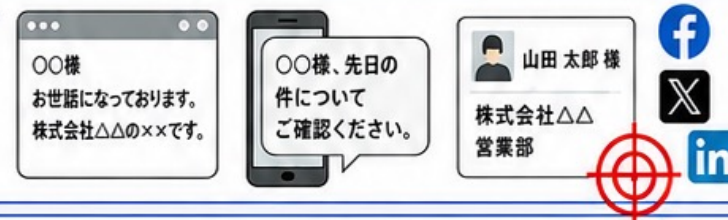
4 AIチャットボット型サポート詐欺

24時間自動応答で相手を安心させ、URLクリックやコード入力へ誘導する



5 超個別化フィッシング

漏えい情報やSNS情報を使い、氏名・勤務先・取引先に合わせた自然なメールやSMSを作る



6 ロマンズ・投資詐欺の長期会話自動化

自然な会話を長く続けて信頼を作り、送金やアプリ導入へ誘導する



7 多言語・大量配信の自動詐欺

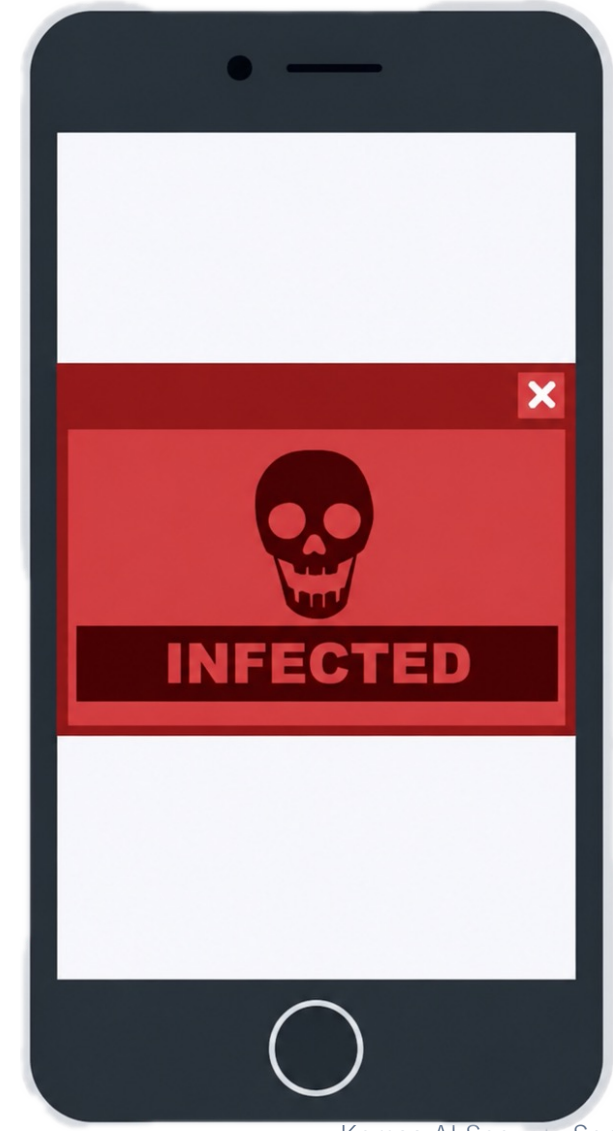
翻訳AIや音声AIで多言語化し、電話・SMS・メールを大量にばらまく



フィッシング詐欺の事例



リンクをクリックすると...



ディープフェイク音声の見分け方

見破るより、「確認する仕組み」が大切です

急な要求

お金・認証コード
個人情報を求める

話し方

間の取り方・感情
呼吸が不自然

受け答え

質問への返答が
少しずれる

決まり文句

「秘密」「今すぐ」
「この場で」

安全な対応：① 一度電話を切る ② 公式番号へかけ直す ③ 別手段で確認

声は「本人確認」ではありません。確認ルールで守ります。

ビデオ会議通話の見分け方

Teams・Zoomなどでも、映像のなりすましに注意します

口元 声と口の動きが少しずれる

輪郭 耳・髪・首の境界が揺れる

表情 まばたきや視線が不自然

画質 顔だけぼやける
背景と合わない

動き 横を向いた時に顔が崩れる

確認 本人しか知らない質問
(旧姓・ペットの名前)

判断基準：違和感が1つでもあれば、通話内で決めず、別ルートで確認します。

ビデオ会議通話の見分け方

Teams・Zoomなどでも、映像のなりすましに注意します



ビデオ会議通話の見分け方

Teams・Zoomなどでも、映像のなりすましに注意します



ビデオ会議通話の見分け方

Teams・Zoomなどでも、映像のなりすましに注意します



Trend Micro Deepfake Inspectorの紹介

ビデオ通話中のAI顔すり替えを検知する補助ツールです

何ができる？

Windows PC向けの無料ツール。
ビデオ通話中にAI顔すり替えの疑いを検知し、警告します。

使う時の注意

ツールは「補助」です。
送金・認証コード・個人情報の判断は公式確認を優先します。

検知ツール + 確認ルール の二段構え

※ 導入可否は利用環境・OS・会社ルールに従ってください。

怪しい連絡が来た時の返し方

電話の場合

「確認しますので、一度切ります。
公式の番号からかけ直します。」

メール・SMSの場合

「リンクは開かず、公式アプリから
確認します。」

家族・知人を名乗る場合

「合言葉を確認します。
別の電話番号・LINEで連絡します。」

職場・上司を名乗る場合

「社内の正式ルートで確認してから
対応します。」

質問タイム

今日の内容で不安なこと・設定の詳細や影響について
遠慮なくご質問ください。

参考資料

- OpenAI Help Center : Data Controls FAQ
- FBI IC3 PSA (2026年5月21日) : Kali365 Phishing-as-a-Service Kit
- Microsoft Learn : Device code flow / authentication security guidance
- Trend Micro Help Center : Deepfakes and Deepfake Inspector
- Trend Micro Free Tools : Deepfake Inspector for Windows PCs

※ 本資料は初心者向け講習用に、危険な手順の詳細は省き、防御方法に絞って説明しています。