



簡易ガイド・リスク・なりすまし詐欺

新しいお客様は、偽りの身元ではない ですか？ 契約の前に、確認できるシグナルをチ ェックできます。

会員登録をする人や契約を申し込む人は、まず自分が誰であることを名乗ります。この簡易ガイドでは、PaperOfficeがメールアドレス、IPアドレス、デバイス、身分証明書を、確認できるシグナルとしてどのように提供するかを示します。ショップ、プラットフォーム、賃貸人、分割払いで販売する小売業者が対象です。

重要なポイント

どの確認も、ルールが使える項目を返します。メールアドレスへの推奨、VPNやTorの識別、デバイスID、そして元の位置付きの身分証明書の項目です。最終的な判断はチームが行います。

01・課題の内容

名前は正しい。 でも、その背後にいる人は違います。

新しいお客様がオンラインで契約を結び、スマートフォンが分割払いで届きます。氏名、住所、メールアドレスは本物に見えます。支払いが止まってから初めて分かります。そのデータは別の人のものだったか、そもそもその人物が存在しなかったのです。

なぜ起こるのか

盗まれたデータと作られたデータ

詐欺師は、データ流出で入手した実在の氏名や住所を使うか、それに架空の情報を混ぜます。フォーム上では、どちらも同じように見えます。

ネットワーク上での隠れ方

使い捨てのアドレス、VPN、Tor、レンタルサーバーは、誰が注文しているのかを隠します。同じ人が、少しの手間で多くのアカウントを開設できます。

急いでの身分証明書の確認

カウンターでは、身分証明書のコピーはさっと見られ、そのまま入力されます。誤字や記入漏れは、簡単に見過ごされてしまいます。

気づくポイント

- メールアドレスが使い捨てサービスのものか、そのドメインにメールサーバーがない。
- 登録が、通常の接続ではなく、VPN、Tor、またはデータセンター経由で行われている。
- IPアドレスの国が、記載された住所と一致しない。
- 同じデバイスが、異なる名前で複数の登録に現れている。
- フォームの記載事項と身分証明書の記載事項が異なっている。

02・PAPEROFFICEでの進め方

シグナルから 判断まで。

PaperOfficeは、メールアドレス、ネットワーク、デバイス、書類に関するシグナルを、REST API、SDK、およびアプリ内で提供します。その後の対応は、あなたのルールに従います。通す、再度確認する、審査に回す、拒否する、のいずれかです。

1 メールアドレスを評価する

POST /fakeemail/checkは、使い捨てドメイン、MXレコード、SPF、DMARCを確認し、risk_scoreと推奨（ACCEPT、REVIEW、REJECT）を返します。

モジュール: 偽メールアドレス検出

2 ネットワークと所在地を確認する

/ip2location/fullは、国、地域、プロバイダーを返し、さらにis_vpn、is_proxy、is_tor、is_datacenterを返します。typeの項目は、該当したリストの名前を示します。

モジュール: VPN検出

3 デバイスを識別する

ブラウザーSDKは、デバイスごとにvisitor_idを返します。次のログイン時に、/fingerprint/verifyが同じデバイスかどうかを確認し、risk.factorsが異常な点を示します。

モジュール: デバイス・フィンガープリント

4 身分証明書を読み取る

IDP Agentが、写真またはスキャンから、氏名、生年月日、住所、書類番号、有効期限を読み取ります。各値は、元の文書内での位置とともに示されます。

モジュール: IDP AGENT

5 判断する

お使いのアプリケーションが、項目をルールにまとめます。たとえば、使い捨てアドレスやTorであれば、担当者による審査とします。最終的な判断はチームが行います。

03・アプリでの操作

キー、SDK、エージェント： 設定方法。

シグナルの確認はREST APIとSDKで実行され、身分証明書はアプリ内のIDP Agentで処理されます。名称はアプリの表示と一致しています。

1

バックエンド用のAPIキー

APIと開発者 › APIキー で、新しいキーを作成 を使って APIキー を作成します。バックエンドは、これを使ってメールアドレスとIPアドレスを確認します。キーはいつでもそこからコピーできます。

2

ブラウザーSDK用のキー

APIと開発者 › APIキー で、新しいキーを作成 を使い、種類として 公開可能なキー を選び、お使いのWebサイトのドメインを入力します。サイトはこのキーでフィンガープリントSDKを読み込みます。

3

身分証明書用のIDP Agentを作成する

サンプルの写真を選択し、アクション › エージェントとワークフロー › IDP と 新規エージェントを作成 を使います。身分証明書のテンプレートを選ぶか、項目を自分の言葉で記述してください。

4

値を元の資料と照合する

データフィールド タブでは、各値が身分証明書の該当箇所の抜粋と並んで表示されます。IDP Review の表示では、フィールドを開いたすべての文書が確認できます。

5

審査タスクを処理する

必須項目が欠けている場合、選んだ審査キューにタスクが作成されます。Workflow AI › Human In The Loop タスク では、担当者が身分証明書と項目を確認して審査を完了します。

現場からのヒント

複数のシグナルを合わせて評価する VPNだけでは、多くの場合、無害な理由があります。使い捨てアドレスや、システム内の他のアカウントにすでに紐づいたデバイスと組み合わせると、初めて意味を持ちます。担当者がいつ審査するかを定めてください。

04・事例

携帯電話の小売店。 分割払いの契約。



六店舗とオンラインショップを持つ携帯電話の小売業者は、スマートフォンを契約と分割払いプランで販売しています。店舗では、チームが身分証明書をコピーし、データを一項目ずつ入力します。オンラインでは、フォームだけで足りる。支払いが止まり、顧客に連絡がつかないことが何度も起きています。

導入前

- 店舗では、身分証明書がコピーされ、契約フォームに一項目ずつ入力される。
- オンラインでは、使い捨てのものを含め、すべてのメールアドレスが受け入れられる。
- VPNやデータセンター経由の申込みは、ほかのものと同じに見える。
- 一つのデバイスがすでに複数の申込みをしていることには、誰も気づかない。

PAPEROFFICE導入後

- オンラインフォームがメールアドレスを確認し、REVIEWの場合は申込みが審査に回る。
- IPの確認はVPN、Tor、データセンターを報告し、申込みは国と住所を照合する。
- 各申込みはvisitor_idを保存するため、複数回使われたデバイスが目立つ。
- 店舗では、IDP Agentが写真から身分証明書を読み取り、チームは値を元の資料と照合する。

説明のための例です。会社とプロセスは架空のものです。どの身分証明書やデバイスのデータを収集し、どのくらいの期間保管するかは、データ保護責任者と確認してください。

05・チェックリスト

お客様の受付のための 十の項目。

これらの項目を、販売、IT、データ保護の担当者と一緒に確認してください。それぞれ、自社の業務で確認できます。

- ☐ すべての登録で、アカウントを有効にする前にメールアドレスを確認している。
- ☐ バックエンドが、顧客のIPアドレスをipパラメーターでAPIに送信している。
- ☐ IPアドレスの国が、記載された住所と照合されている。
- ☐ 既知のアカウントが見慣れないデバイスからログインした場合、アプリケーションが第二の要素を求める。
- ☐ 削除依頼について、POST /privacy/forgetによる手順が文書化されている。
- ☐ REVIEWとREJECTについて、どうするかが定められている。再度確認する、審査に回す、拒否する、のいずれかです。
- ☐ VPN、Tor、データセンターはそれぞれ別に評価され、各ケースにルールがある。
- ☐ visitor_idが、すべてのアカウントと申込みごとに保存されている。
- ☐ IDP Agentが身分証明書を読み取り、必要な項目が定義されている。
- ☐ デバイスデータの目的、法的根拠、保管期間が、データ保護と合意されている。

06・よくある質問

チームが始める前に 知りたいこと。

PaperOfficeは身分証明書を生体認証で確認しますか？

PaperOfficeは顔の照合を行わずに機能します。IDP Agentが身分証明書の項目を、元の位置とともに読み取り、ほかの確認はメールアドレス、ネットワーク、デバイスに関するシグナルを提供します。本人確認を承認するかどうかは、チームが判断します。

正当な理由でVPNを使う人はどうなりますか？

VPNは、ルールが重み付けするシグナルの一つにすぎません。レスポンスはVPN、プロキシ、Tor、データセンターを区別し、typeの項目に該当リストの名前を示します。ブロックリストに載ったアドレスは、is_vpnにも表示されます。

確認は、どのようにポータルに組み込みますか？

バックエンドからのREST API、ドメインに紐づいた公開可能なキーを使うフィンガープリントSDK、そしてMCPを通じてです。身分証明書は、IDP Agentが動作するWorkspaceにアップロードします。

リスクスコアはどこから来ますか？

メールの確認からです。risk_scoreは0から100、risk_levelはMINIMALからCRITICAL、推奨はACCEPT、REVIEW、REJECTのいずれかです。デバイスの確認では、VPNや不可能な移動速度など、独自のリスク要因が提供されます。

複数のアカウントの背後にある同じデバイスを見つけられますか？

はい。すべてのアカウントとともにvisitor_idを保存すれば可能です。そうすると、同じIDが複数のアカウントに現れます。/fingerprint/similarは似た特徴を持つデバイスを、/fingerprint/linkedは同じネットワークのデバイスを見つけます。

削除依頼はどのように処理しますか？

POST /privacy/forgetは、お使いの組織内の識別子について、デバイスのプロフィール、リンク、履歴、アラートを削除します。ブロックマーカにより、同じ識別子が再び記録されるのを防ぎます。

07・始め方

次の登録を、実際のシグナルで確認してください。

app.paperoffice.aiでアカウントを作成し、**APIと開発者** > **APIキー** でAPIキーを生成して、最初のメールアドレスをPOST /fakeemail/checkで確認してください。料金は従量課金で、詳細は料金ページにあります。

メールの確認を追加する

登録フォームが、バックエンドを通じてアドレスを/fakeemail/checkに送り、推奨の項目に基づいて動作します。

IPとデバイスを追加する

ネットワークと所在地には/ip2location/full、visitor_idにはフィンガープリントSDKを使います。両方を申込みとともに保存してください。

身分証明書を読み取らせる

身分証明書のテンプレートでIDP Agentを作成し、申込み用のWorkspaceで処理後に自動で実行させていただきます。

関連データシート

偽メールアドレス検出

paperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf

VPN検出

paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf

IPロケーションAPI

paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf

デバイス・フィンガープリント

paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf

IDP Agent

paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-ja.pdf

このテーマの関連情報

なりすまし詐欺

paperoffice.ai/ja/kaiketsu/risk/ai-identity-fraud-detection-prevention



このテーマの関連情報

paperoffice.ai/ja/kaiketsu/risk/ai-identity-fraud-detection-prevention

料金

paperoffice.ai/en/pricing

お問い合わせ

paperoffice.ai/ja/otoiawase