＼ 電話による本人認証で「なりすまし」を防止します ／

既存システムとも連携可能な強固なセキュリティ認証

不正アクセスからお客様を守る
電話による本人認証システム

DHKクラウド 電話認証サービス

IVRによって、不正ログインによる
情報漏えい・改ざんを防ぎます。

インターネットにおける不正アクセス被害が拡大しています。

不正アクセスを受けると「機会損失」「売上の減少」「信頼の失墜」など甚大な損害が発生します。

しかし、セキュリティをいくら強化しても不正アクセスを完全に防ぐことはできません。メールアドレスまで乗っ取られた場合「メールによる2段階認証」も役に立たなくなります。

インターネットセキュリティの重要ポイント

不正ログインされないための

! 監視強化

不正アクセスが巧妙化しており
すべての攻撃を防ぐのは不可能。

利用者へのID管理における

! 注意喚起

複数のID管理の手間で使い回しも減らない。
利用者まかせの対応。

- 不正ログインされても、重要機能に本人認証プロセスを導入することで、信頼性の向上や情報保護の強化、管理リスクへの意識づけにも効果があります。
- 電話認証は本人だけが持っているデバイス（携帯・固定電話）を活用するため、従来のネット上だけの認証よりも本人精度が高くなります。

DHKクラウド電話認証サービスが本人認証によるセキュリティ強化を実現します。

電話認証とほかの二段階認証との比較

スマートフォンアプリによる二段階認証

OSのバージョンアップにともなうメンテナンス費用や、操作に関するサポート費用が高額になりやすく、スマートフォンをお持ちでない方は利用できないといった問題があります。

ハードウェアトークン

ハードウェアの初期費用や、紛失・故障時の対応コストが高額になりやすく、ハードウェアトークンは持ち歩くものではないため、サービスによってはご利用者様にとって不便となります。

電話認証

既存の電話機を利用するため初期投資が低く、どなたでも操作方法がわかりやすいため、サポートの対応コストも低く抑えることができます。運用もしやすく、長期的な運用に向いています。

DHKクラウド IVR本人認証サービスの特長

IVRとWEBの連携による本人認証

お客様がWEB上で個人情報の確認・変更、セキュリティの設定・変更といった重要な情報を閲覧・操作する際、ご登録の電話番号へIVRが自動発信して本人認証を行うセキュリティシステムです。

高い認証精度

事前登録された実在する電話番号を活用することで、従来のネット上だけの認証よりも本人確認の精度が高まります。

インバウンド/アウトバウンド対応

インバウンド、アウトバウンド、両方での対応が可能です。

簡単な認証方法

電話認証は、誰もが所有し誰もが操作方法を知っている電話を活用した認証方法です。

IVR本人認証サービス仕様

- **アウトバウンド機能概要(インバウンド可)**
  登録された電話番号へ発信し認証します。※インバウンドの場合は発信者番号を取得、判定。
- **データ連携機能(インバウンド/アウトバウンド)**
  HTTPS通信(POST)によるデータ連携インターフェースをご提供します。

ご活用例

登録会員情報閲覧、変更

情報の不正取得や
改ざんリスクの低減。

オンラインゲームなどの情報移行、端末移行

ゲーム情報の移行にともなう
不正リスクの低減。

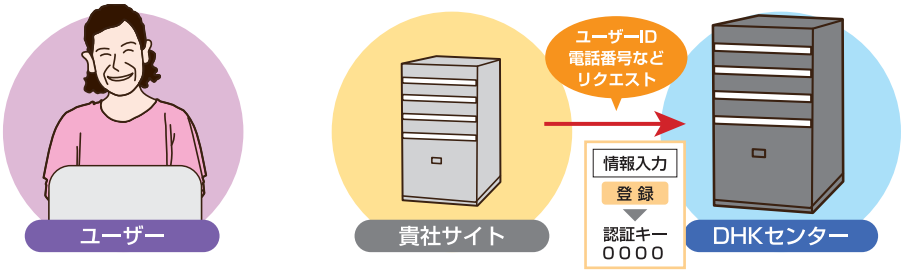
商品購入などにおけるオンライン決済時

オンライン決済における
不正利用リスクの低減

パスワード再発行時の認証フロー（アウトバウンド例）

1 お客様が、貴社のパスワード再発行WEBページにて、ユーザーID・登録電話番号を入力して、登録情報の照合を行います。

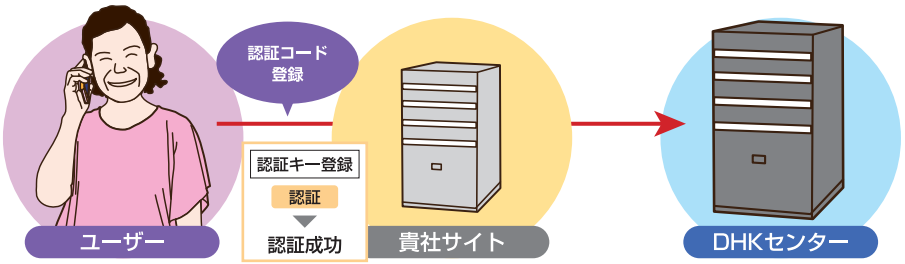
2 貴社サイトで照合できたID・電話番号・認証パスワードを電話認証センターへリクエストします。IVRは認証データを受信し、データベースへ登録します。



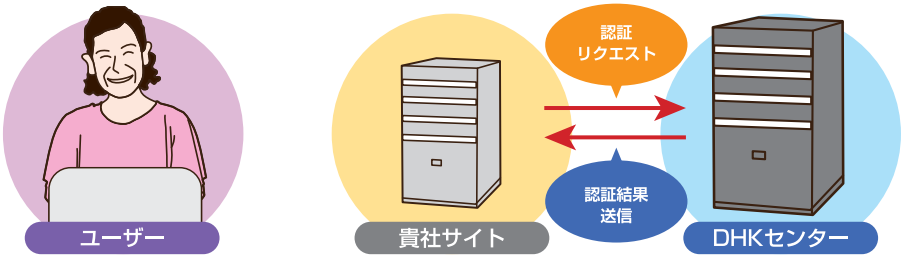
3 登録された電話番号でIVRより発信します。

※インバウンドではあらかじめご案内した電話番号へ、お客様にお電話をしていただきます。

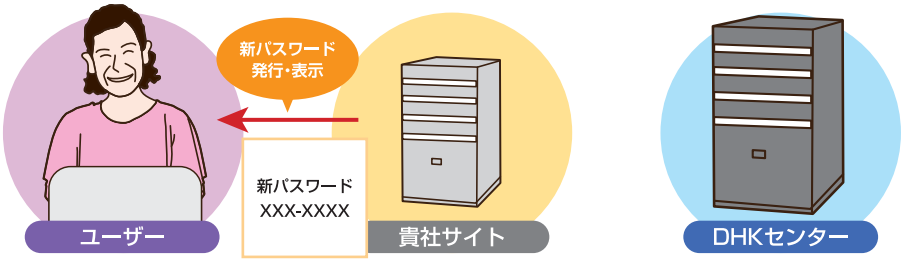
4 ユーザー応答後、認証コードをプッシュ操作で取得し、登録電話番号＋認証コードを受付データと照合・結果更新を行います。



5 貴社Webサイトから電話認証データの認証結果を照会リクエストいただきます。IVRは認証結果を送信します。



6 認証がOKであれば、お客様へ新しいパスワードを発行・表示していただきます。



ご担当者様の声

某個人向けインターネットサービス

アウトバウンド型で導入

重要な情報をご登録いただいているお客様のセキュリティ強化に導入

毎日のように、不正アクセスの報道がされ、当社でも対策が急務でした。リスト型アカウントハッキングの被害は、複数のサービスで同一のメールとパスワードの組み合わせを利用している場合、リスクが高くなります。メールとパスワードによる本人確認では、悪意のある第三者による、なりすましを防ぐことができず、不正なアクセスから守る手段として、十分な安全性が確保できなくなっていました。カード情報など重要な情報をご登録をいただいているお客様に対しメールによる本人認証に代わり、なりすましが困難である電話番号による本人確認、電話認証を導入しました。

インバウンド型で導入

誰でも操作可能な電話認証で十分なセキュリティを確保

チェーン店向けにサービスを提供していますが、クライアントより、店舗から他店舗へとアクセスできるように仕様の変更を求められました。店舗の責任者が利用するため、仕様変更には誰もが操作可能で、十分なセキュリティも確保できる認証の仕組みが必要でした。また、本人認証の導入にあたって、各店舗の代表電話番号で認証をおこなうことで、店舗間の誤アクセスや、なりすましが発生しにくい運用も可能となりました。

よくある質問

Q メール認証とは違うのですか？

A メールアカウントが乗っ取られた場合、
メール認証型の本人確認は“なりすまし”が可能となってしまいます。
その点、電話認証はすでにご登録されている電話番号を利用して確認するため、
本人確認性が高く、また「電話をかける」「電話機のボタンを押す」という操作は
誰もが知っている動作なので、認証手段として導入される企業が増加しています。

すぐに導入していただきやすい「電話認証サービス」ご利用料金

インバウンド	アウトバウンド	SMS
150,000円	60,000円／月	20,000円／月
※ 初期費用／500,000円～ 10,000件を越える従量課金@10円	※ 初期費用／100,000円～ 1,000応答超過従量課金 固定電話@21円　携帯電話@32円	※ 初期費用／100,000円～ 1件～@18円

サービス提供元

株式会社電話放送局
denwa housou kyoku

大阪本社 06-6313-8000
東京支店 03-3645-1711

問い合わせ先