OneWelcome Identity Platform – リスク管理

デジタルバンキングサービスのセキュリティとユーザーエクスペリエンスを強化

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

OneWelcome Identity Platform - リスク管理

クラウドベースのリスク管理テクノロジーでデジタルバンキングサービスのセキュリティとユーザーエクスペリエンスを強化

クラウドの保護とライセンシング

リスク管理がデジタルバンキングの鍵である理由

デジタルチャネルの増加やモバイルバンキングの採用が急速に進む中、金融機関は、サイバー攻撃の急速な拡大に直面しています。フィッシング、アカウント乗っ取り、ソーシャルエンジニアリングは、サイバー攻撃者によるセキュリティ対策への止むことない挑戦の一例に過ぎません。スムーズなユーザーエクスペリエンスを維持しつつ、これらに先手を打つのは困難です。しかしながら、それは必要なことであり、利便性がその鍵になります。デジタルバンキングを提供する金融機関は、顧客の摩擦を少なくし、便利で安全なユーザーエクスペリエンスを提供しつつ、EUのPSD2などの最新のセキュリティ規制のコンプライアンスも達成する必要があります。

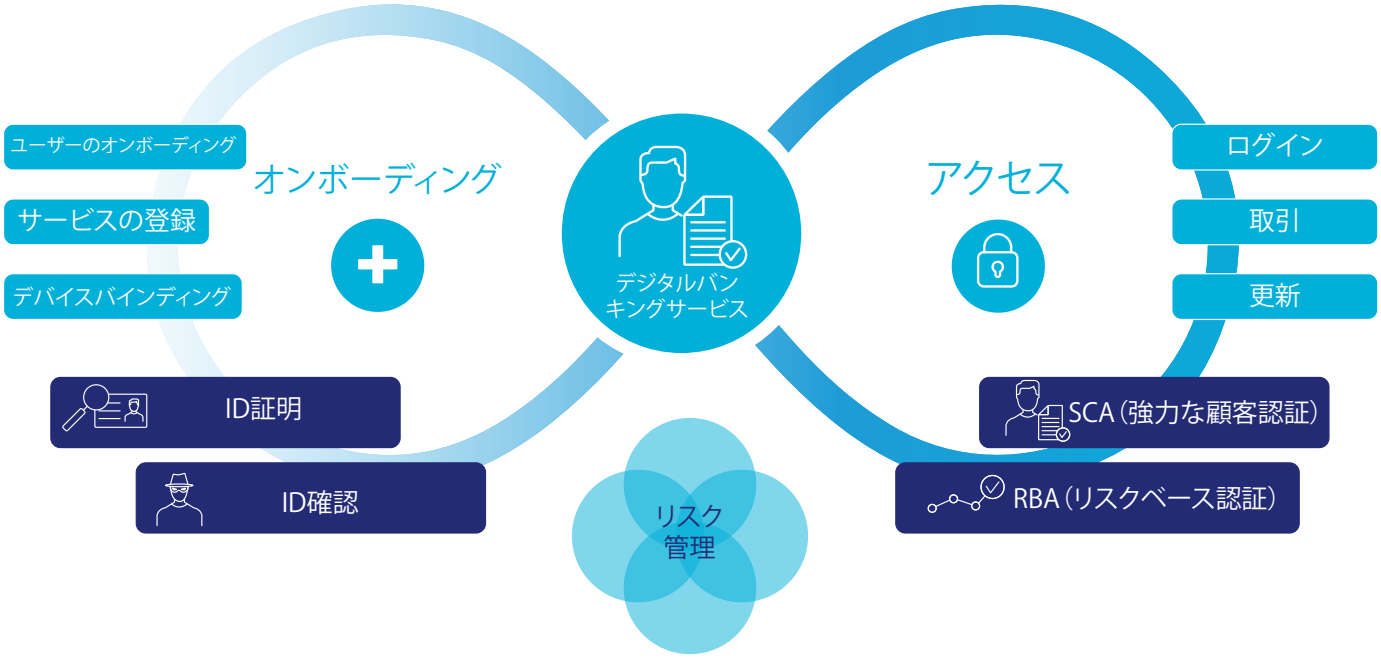
リスク管理サービスは、すべてのデジタルバンキングサービスの中核として、セキュリティに新たなレイヤーを追加し、ユーザーエクスペリエンスを向上させます。オンボーディング、ログイン、アカウントのサインアップ、取引のいずれにおいても、

異常な行動を検知することで、多数のユーザーエンドポイントを保護します。Thalesのリスク管理は、オンラインのあらゆるやり取りでのユーザーの行動を監視して、高精度の行動プロファイルをリアルタイムで作成することで、アカウントの強奪や乗っ取りなどの攻撃からユーザーを保護します。この継続的な監視により、企業は、良いユーザーを認識して、摩擦を解消することで、優れたユーザーエクスペリエンスを実現することができます。

デジタルバンキングのライフサイクル全体を保護

同じプラットフォームを使用して初期段階の顧客オンボーディングと日常的なアクセスの両方を保護することで、金融機関に多くのメリットがもたらされます。どちらのシナリオでも同じリスク管理テクノロジーを使用してバックグラウンドチェックを実行することで、セキュリティとユーザーエクスペリエンスが向上します。デジタルオンボーディングにおいては、これはID確認を意味し、入力されたIDの裏付けとなる証拠を提示することで、信用のレベルを高くし、不正申請に対抗します。日常的なアクセスにおいては、これはリスクベース認証（RBA）を意味し、

リスクのレベルに応じた認証戦略を採用することで、何回もアクセスする顧客の摩擦を減らし、アカウント乗っ取り攻撃を防止します。すべてがバックグラウンドで密かに動作することで、最高のエンドユーザーエクスペリエンスを提供します。



リスク管理テクノロジーの4つのレイヤーが連携

Thalesのリスク管理テクノロジーは、インテリジェンスの4つのレイヤーが連動することで、強力な機能を提供します。各レイヤーで、異常な活動をさまざまな観点から分析することで、被害が発生する前にリスクの高い活動を特定します。

デバイスとネットワークのインテリジェンス

デバイスインテリジェンスは、クライアント（ノートPCやモバイル）とネットワーク環境に関する情報を収集します。その目的は、場所、タイムゾーン、言語、OS、ブラウザのバージョンの間の矛盾に加えて、不審なネットワークから接続が確立されたなどの異常を検知することです。返却デバイスを正確に認識し、新しいデバイスが使用される際のリスクのレベルを引き上げることができます。

Thalesのソリューションが使用する永続的なデバイスIDは、デバイスID、デバイスフィンガープリント、秘密鍵を組み合わせることで一意のIDを作成します。このIDは、ソフトウェアアップデートやCookieの消去などのデバイス内での大幅な変更があっても存続します。

行動的生体認証

人間の行動は個人ごとに異なります。Thalesのリスク管理は、ユーザーの行動を分析することで、正規のエンドユーザーを認識します。このレイヤーは、ユーザーのタイプ、マウスの動きやデバイスの持ち方などに注目することで、エンドユーザーごとの固有のプロファイルを構築します。行動的生体認証は、これらの重要なメトリクスを利用して、個人、グローバル集団、ボット（自動化された攻撃）のプロファイルを構築します。

- **個人のプロファイル**
  個人レベルの行動的生体認証プロファイルにより、以下の検知が可能になります。
  アカウント乗っ取り：不正行為者は、以前に偽のウェブサイトでのフィッシングや窃取されたデータベースから不正に手に入れたクレデンシャルを入力しようとします。ユーザーの行動を正規のユーザーの典型的な行動と比較することで、窃盗されたクレデンシャルを使用する不正行為者を検知できます。
  ソーシャルエンジニアリング攻撃：不正行為者は、正規のユーザーを誘導し、時にはリアルタイムで、自分の代わりに何かを実行させようします。データに不慣れであるとは、一般的には、入力に時間がかかり、修正回数が多く、入力の速度にばらつきがあることを意味します。例えば、情報を文書から情報をコピーする場合と電話で指示された場合を比べると、ユーザーが同じように入力するわけではありません。
- **集団のプロファイル**
  個人のプロファイルの構築に使用する統計を拡張することで、集団のプロファイルを構築し、未知のユーザーを顧客としてオンボーディングする場合に利用することができます。ユーザーのグループの場合、行動的生体認証が、個々のやり取りを集約して、全体としての「良いユーザー」と「悪いユーザー」のプロファイルを作成します。
  例えば、正規のユーザーによる特定のサービスでのマウスクリックやタッチの平均回数は、不正行為者とは異なります。正規のユーザーは、自分の個人情報はよく知っていますが、ウェブページやアプリケーションには慣れていないことが多く、不正行為者はその反対です。
- **自動化された攻撃の検知**
  基本的な自動化された攻撃では、攻撃者が多数のクレデンシャルを極めて高速でテストできますが、多くの場合に、同じIPアドレスや同じデバイスを繰り返し使用するなどのボットによくある行動が見つかります。結果として、セキュリティツールで簡単に検知することができます。
  模倣するスクリプトを実行することで、実際の人間のやり取りであるかのように見せかけます。
  高度な攻撃の数は現状では少ないものの、増加し続けています。これらの攻撃を一般的なセキュリティツールで検知するのはかなり困難ですが、Thalesの行動的生体認証レイヤーは、高度な攻撃も検知します。

行動分析

行動分析レイヤーは、ユーザーの習慣を個人レベルと集団レベルで分析することで、異常な状況を検知します。
このエンジンは、個人レベルでは、特定のユーザーの一般的に利用するデバイス、場所、支出パターンなどに注目します。集団レベルでは、サービス全体での代表的なパターンを作成します。特定のユーザーやサービスで、平均的な正規の利用からの逸脱を示すシグナルが多過ぎる場合、そのサービスとやり取りしているのが不正行為者であることを示す良い兆候です。

トラストコンソーシアム

このレイヤーでは、顧客ベースで選択されたデータポイントを集計して、レピュテーション分析を構築します。不正とレピュテーションのスコアを、データポイントが確認されたときの過去のスコアに基づいて構築します。データは、同じソリューションを使用している他の企業のデータを使用して構築されたグローバルコンソーシアムのデータベースから取得されます。

トラストコンソーシアムのインプット

- IPアドレス
- デバイスエンドポイント

リスク管理の例

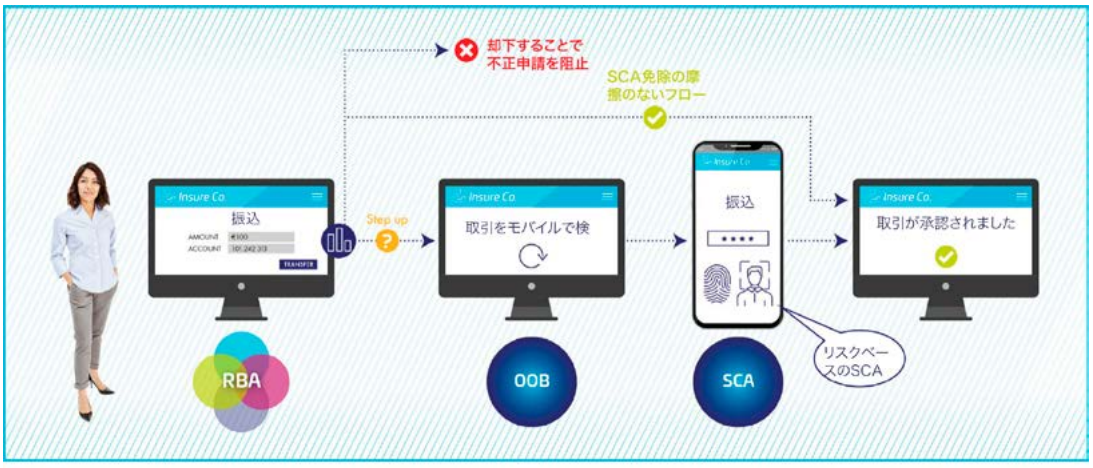
OneWelcome Identity Platformの優位性の1つとして、同じプラットフォームが使用して最初のオンボーディングから日常的なアクセスまでのライフサイクル全体のセキュリティと強化が実現する点が挙げられます。以下に、これらの両方のユースケースでリスク管理を実現する2つの例を紹介します。

サービスの登録

ユーザーが個人情報を入力し開始した直後に、バックグラウンドチェックによるユーザー活動の監視が開始するため、不正のリスクをすぐに警告できます。この例では、不正行為でプロセスが開始した疑いがすでに高い場合に、IDと顔認識のサービスがすべて実行されることはありません。

取引を実行

リスクベース認証（RBA）と強力な顧客認証（SCA）を組み合わせることで、ユーザーエクスペリエンスとサービスのセキュリティを同時に向上させることができます。ノートPCからの代表的なアクセスフローを示す以下の例では、RBAを使用して、摩擦のないアクセスをほとんどの認証の試行に提供し、リスクエンジンの評価で必要と判断された場合にのみ、OOBのSCAに使用することで不正アクセスを防止します。



規制のコンプライアンスとセキュリティの認証

OneWelcome Identity Platformは、PSD2やFFIECなどの規制でコンプライアンスが求められるようになった新しいセキュリティ要件に対応する完璧なソリューションです。金融機関は、SCAとダイナミックリンクに関するPSD2の要件に対応し、PSD2のRTS（Regulatory Technical Standards）の要求に従い、認証と取引のプロセスのリスクをリアルタイムで監視できるようになります。FFIECによる推奨に従い、リスクレベル、取引の種類、ユーザープロファイルに基づき、複雑なセキュリティポリシーを定義できます。強力なリスク管理の要件への対応を可能にすることで、増加する攻撃や不正行為に対抗します。

v欧州のGDPRや米国のCCPAなどがそうであるように、データプライバシーに関する規制が厳格化されています。複数の異なるベンダーがリスク評価データを処理する場合、そのコンプライアンスは容易ではありません。OneWelcome Identity Platformは、GDPRとCCPAのコンプライアンスを考慮して設計されています。

信頼できるパートナー

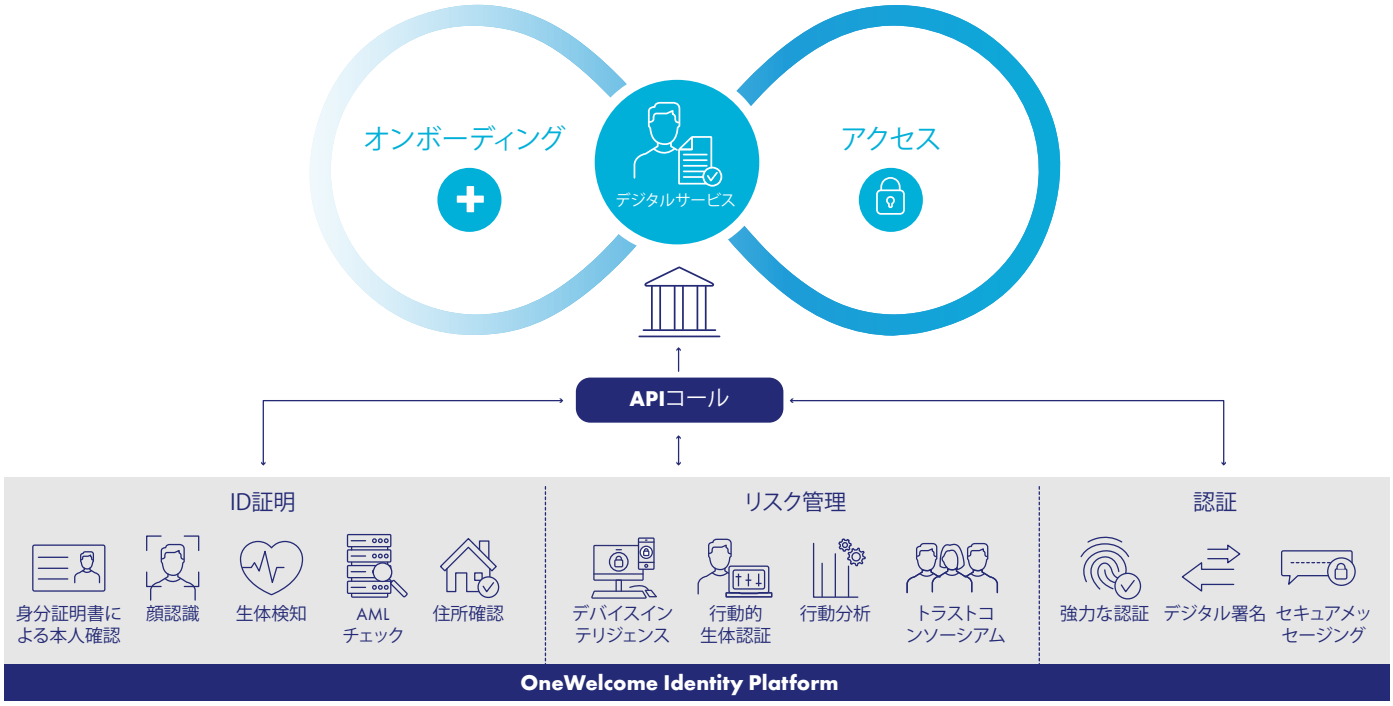
強力なID認証のソリューションのマーケットリーダーであるThalesは、サービスのセキュリティを強化し、規制のコンプライアンスを達成したいと考える銀行や金融機関の信頼できるパートナーです。Thalesのソリューションが提供する、

安全で利便性の高いオンボーディングとアクセスは、世界中のデジタルバンキングサービスのエンドユーザーにすでに利用されています。Thalesは、お客様のデータのセキュリティとプライバシーの両方の保護を支援します。

OneWelcome Identity Platform - デジタルバンキングへのオンボーディングとアクセスを保護するクラウドプラットフォーム

Thalesのクラウドベースのマネージドサービスを利用することで、金融機関は、ID証明とSCA（強力な顧客認証）によるデジタルバンキングへの安全なオンボーディングとアクセスを提供できます。リスク管理は、ID確認とリスクベースの認証によるセキュリティの強化とカスタマーエクスペリエンスの向上を可能にします。これらすべてを1つのプラットフォームで実現します。

詳細情報: ソリューション解説をダウンロード



OneWelcome IDおよびアクセス管理ソリューションについて

Thalesのデジタルソリューションは、世界中の何十億の人やモノにデジタルIDを提供しています。ThalesのOneWelcome Identity & Access Managementポートフォリオを利用することで、顧客、ビジネスパートナー、従業員に対する、摩擦のない、信頼できる、安全なデジタルフローを構築できます。OneWelcome Identity Platformは、ID確認、シングルサインオン、パスワードレス認証、

多要素認証から、不正管理、アダプティブアクセス、動的認証、同意/嗜好管理までの多様な機能を提供することで、最高レベルの保証を実現します。30,000以上の組織がThalesのソリューションを利用して、IAMやデータセキュリティのニーズを解決し、安全なデジタルサービスをユーザーに提供しています。

Thalesについて

今日の企業や政府機関は、クラウド、データ、ソフトウェアを積極的に利用して、信頼できるデジタルサービスを提供しています。世界中の有名企業や組織がThalesを採用し、クラウドやデータセンター、さらには、デバイスやネットワークまでのあらゆる場所に作成、保存、アクセスする機密情報やソフトウェアを保護しています。データセキュリティ、ID/アクセス管理、ソフトウェアライセンシングのグローバルリーダーであるThalesのソリューションは、安全なクラウドへの移行とコンプライアンスの確実な達成を支援し、ソフトウェアから多くの価値の創出、数百万人のユーザーへのシームレスなデジタルエクスペリエンスの提供を可能にします。

THALES

Building a future we can all trust

お問い合わせ先

Email：cpl.jpsales@thalesgroup.com

すべてのオフィスの所在地と連絡先情報につきましては、
cpl.thalesgroup.com/contact-us をご覧ください。

cpl.thalesgroup.com/ja