Uni-ID Libra ユースケース

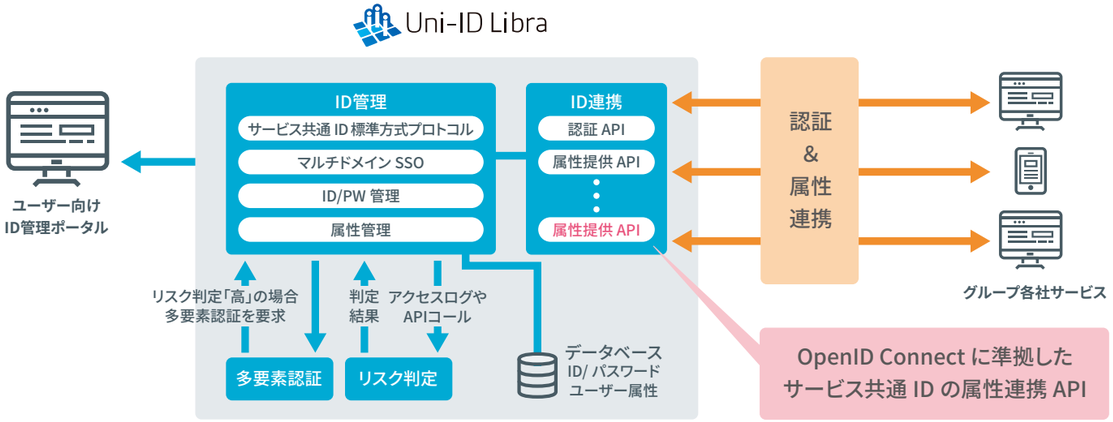
グループ各社が提供するサービスのユーザー ID 統合と認証強度の最適化を実現

課題

- グループ各社で会員情報および認証を個別管理している
- なりすましなどの巧妙な不正アクセスに対応したい
- 一律の認証強化でユーザビリティが低下、サービス離反を防ぎたい

解決

- グループ各社の ID 統合、認証&会員属性連携を実現
- 認証時や取引時のユーザーのふるまいから、「なりすまし」や「不正取引」を検知
- 不正アクセスの疑いや脅威レベルが高い場合のみ多要素認証を要求する「リスクベース認証」を実現



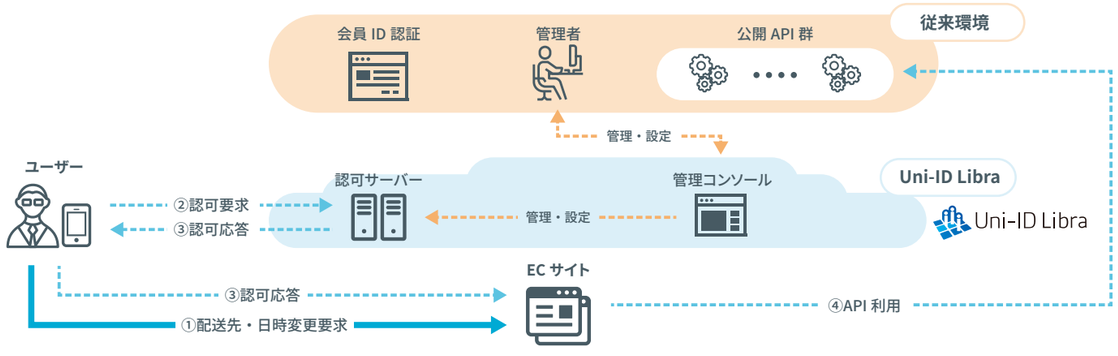
パートナー事業者向け公開 API の認可基盤を整備

課題

- 自社サービスで提供しているサービスを、パートナー事業者（EC サイト）を通じて提供し、顧客により便利なサービスを提供したい

解決

- パートナー事業者向けに機能の一部をAPI基盤として整備
- Uni-ID LibraをAPI認可基盤として活用し、OAuth2.0に準拠した認可制御を行うことで実現



お問い合わせ

info@nri-secure.co.jp ☎ 03-6706-0500 受付時間 9:00-17:00 月曜日～金曜日(祝日・当社休業日を除く)

NRIセキュアテクノロジーズ株式会社

〒100-0004 東京都千代田区大手町1-7-2 東京サンケイビル
www.nri-secure.co.jp

9213-0061-01-1901

NRI SECURE

顧客向けWebサービスのID・アクセス管理ソリューション

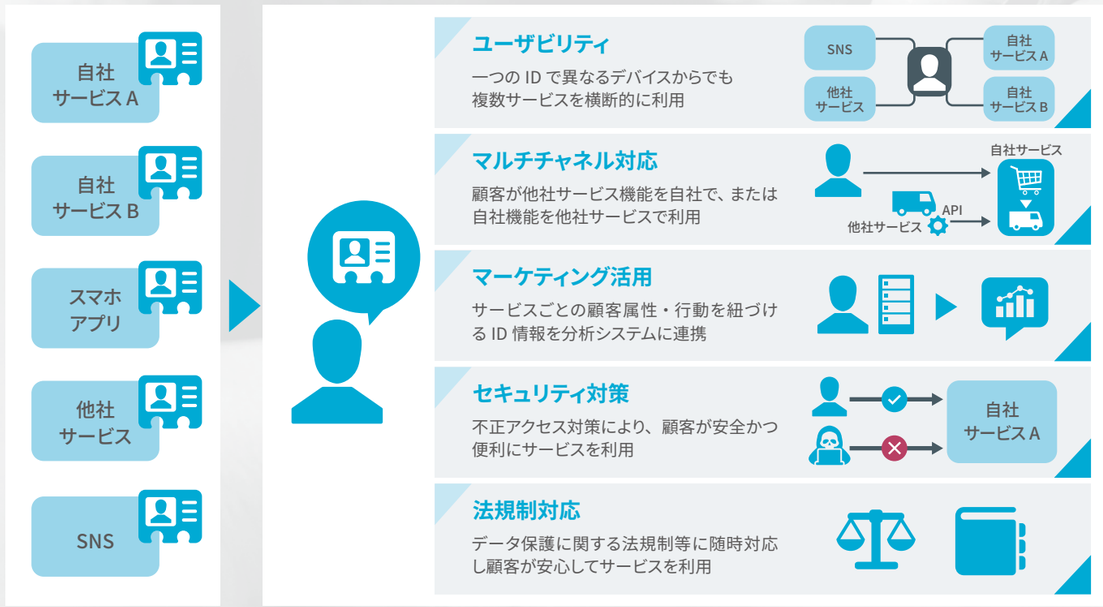
Uni-ID Libra

NRIセキュアテクノロジーズ株式会社

Uni-ID Libra | 顧客向けWebサービスのID・アクセス管理ソリューション

顧客IDの統合管理により
カスタマーエクスペリエンスの向上へ

さまざまなチャネルやデバイスからWebサービスを利用する現在において、複数のIDや属性を持つユーザーも少なくありません。
Uni-ID Libraは、顧客IDの統合管理に必要な機能を、オールインワンパッケージで提供するソリューションです。
不正アクセス防止といったセキュリティ対策や、情報保護規制などにも対応しながら、より正確な顧客理解と、カスタマーエクスペリエンスの向上をスピーディーに実現することができます。



Uni-ID Libraの特長

1 ID統合管理によるユーザビリティ向上

複数サービス間の共通ID利用や他社サービスIDの受け入れ（ID連携）、一度の認証（シングルサインオン）が実現できます。これにより顧客の複数ログインに対する手間を軽減させ、ユーザー離反防止にも貢献します。

2 オープンスタンダード技術に基づいた高い相互接続性

OpenID Connect※1、OAuth2.0※2に準拠し、複数サイト間の認証連携やソーシャルアカウントによるログイン、APIの外部公開を安全に実現します。ID属性情報のシステム間配信も、SCIM 2.0※3に対応しており、高い相互接続性を備えています。

3 セキュリティレベルに応じて使い分け・組み合わせできる多要素認証

認証機能はID/パスワード認証のほか、ハードウェアトークン/ソフトウェアトークン（Google Authenticatorなど）、電子メール/SMS/電話によるワンタイムパスワード認証（OATH TOTP準拠）、指紋/顔などによる生体認証の各方式に対応。これらを組み合わせて認証強度を高める多要素認証を実現できます。

Touch　OneTime

4 ふるまい分析による不正アクセス検知

ログイン時の条件だけでなく、ログイン後のユーザーふるまいも分析し、「なりすまし」を検知できます。また、検知したリスクレベルに応じて認証を追加要求（多要素認証との連携）することにより、「不正取引」を防止します。

5 コンプライアンス・法規制へのパッケージ対応

厳格化されつつある情報保護に関する法規制（個人情報保護法、GDPRなど）への対応も随時実施しています。顧客の同意に基づいた各種情報のサービス間連携も円滑に実現できます。

6 顧客への広範かつ的確なサービス提供への寄与

顧客IDの統合管理により、顧客を複数サービス、複数デバイス間でも一人のユーザーとして捉えることができ、顧客の最新属性や嗜好、行動情報の収集に貢献します。

Webサービスの個別管理で起こりうる課題やデメリット

ユーザー負担
サービスごとにログイン認証が発生

開発コスト
アプリや他社サービスと連携する場合、機能追加や個別開発がその都度発生

マーケティング課題
サービスごとのユーザー情報だけでは、顧客理解には十分ではないことも

不正アクセス
認証レベルの強化だけでは、なりすましなどの不正アクセスは検出されず

法的リスク
新たな法規制や業界ガイドラインが施行されるたびに、設計、運用の再検証がサービスごとに発生

現状分析から導入・運用までトータルで支援

現状分析・目標設定支援	戦略策定支援	全体設計	ロードマップ作成	導入・運用
ゴールの設定 ● ビジネス ● 運用 ● セキュリティ ● 法規制　など 棚卸と Fit&Gap 分析	実現手段の選定 ● UX 改善 ● API エコノミー ● セキュリティ強化 ● 法令順守 ● ID データ配置の整理 ● スケーラビリティ確保 など	全体概要整理 （サービス・システム・運用） 統合認証基盤要件整理 （認証、管理、API、セキュリティなど）	優先度整理 ● ビジネス面 ● システム面 スケジュール作成	Uni-ID Libra導入 運用支援

※1 OpenID Connect：Web サービスサイト間で、ユーザーの同意に基づいて ID 情報を流通するための標準仕様　※2 OAuth 2.0：Web サービス同士の連携において、外部からのデータやサービスに対するアクセスを利用者の同意に基づいて認可するための仕様　※3 SCIM 2.0（System for Cross-domain Identity Management）：アプリケーションやサービスにおけるユーザー情報のプロビジョニングと管理をするための標準技術仕様