



Identity Spotlight

Vol. 4



okta

アイデンティティで世界は It's possible.

日常にあふれるログイン

「ID」とは似て非なる「アイデンティティ」へ注目が集まる

あなたは今朝、起きてからこの「Identity Spotlight」を手に取るまでの間に何回ログインをしたか覚えていますか？ 人々の行動がモバイル端末に移行し、多くのデジタルサービスがクラウド上で展開される「クラウドトランスフォーメーション」が進んだ結果、提供されるサービスが機能単位に細分化され、アプリに分散しました。その結果、人の日常生活におけるログイン行動の数は飛躍的に増えています。

ログインに利用される ID に注目すると、そこには「アイデンティティ」という概念が存在することは意外と知られていません。ID (Identity Document) とアイデンティティとは似て非なるもので、企業はいま、アイデンティティへの投資を加速しています。

企業の課題解決を阻む断片化

「アイデンティティ」が解決の突破口になる理由

アイデンティティとは、人に紐づくさまざまな属性情報です。人の氏名、行動履歴、利用デバイス、IP アドレス など多種多様な属性情報によってアイデンティティが構成され、ID も構成要素の一つです。アイデンティティに注目が集まる背景には、企業が抱えるコスト・収益・セキュリティの3つの課題を阻む断片化があります。

個別の目的で導入されて断片化したテクノロジーはコスト最適化の実現を遠くしています。テクノロジーの断片化はデジタルサービスの断片化を生み、顧客情報が分断され、一貫性のない体験を引き起こします。この断片化を放置すると全体像

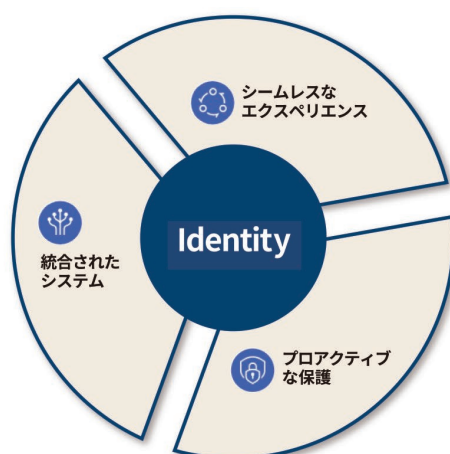
が見えずにセキュリティリスクが生まれるという悪循環に陥ってしまうのです。

この分断を解決する基盤技術として、アイデンティティ管理が注目を集めています。顧客や従業員がアクセスできるリソースや実行できる機能を体系化して管理するアイデンティティ管理によって、統合されたシステム（コスト最適化）、シームレスなエクスペリエンス（より良い体験の向上による収益性向上）、プロアクティブな保護（セキュリティ向上）を実現し、企業を悩ませる3課題の解決が可能です。

コスト・収益・セキュリティの課題解決を阻む
“断片化”



これらの課題を解決する基盤技術
“アイデンティティ”



変わる。 It's Okta.



Okta Japan株式会社
代表取締役社長
渡邊 崇

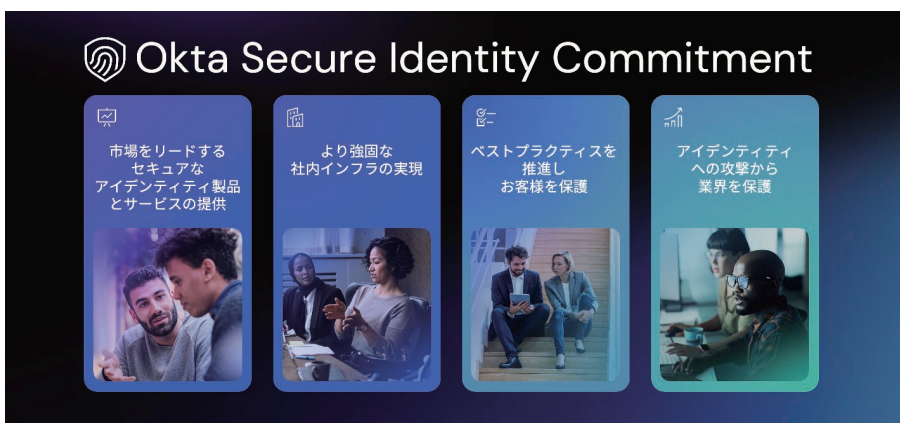
7,000以上の連携を提供するOktaの中立性

企業活動の根幹にある基盤技術だからこそ Okta が重要視しているのが「中立性」です。アイデンティティ管理を通じて、企業で導入されている多くのサービスと連携するには、中立性を抜きにしては実現できません。2024 年 10 月時点で 7,000 以上のサービスとの連携を実現できているのはその証左ともいえるでしょう。

さらに企業の成長性に伴走する基盤技術として「拡張性」・「体験」（顧客や開発者にとって使いやすい設計）・「信頼性」も重視しており、中立性・拡張性・体験・信頼性の 4 つをアイデンティティに対する Okta のアプローチと位置づけています。

Oktaのコミットメント "Okta Secure Identity Commitment"

企業の 3 つの課題の一つであるセキュリティについて、その脅威はとどまるところを知りません。Okta はセキュリティが事業運営の礎になると信じ、Okta Secure Identity Commitment を発表しました。「市場をリードするセキュアなアイデンティティ製品とサービスの提供」「より強固な社会インフラの実現」「ベストプラクティスを推進しお客様を保護」「アイデンティティへの攻撃から業界を保護」という 4 つの柱からなるこの「約束」のもと、Okta は「Okta Launch Week」で製品の最新情報やトレンドを発表しています。



1 つ目の「市場をリードするセキュアなアイデンティティ製品とサービスの提供」は Okta の競争優位性でもあり、提供価値の根幹をなすものです。2 つ目と 3 つ目は、Okta 自身の社内インフラをより強固にし、外部からの脅威から守り、そこで得た知見をお客様やパートナー企業に提供することで価値の連鎖を生みだします。そして 4 つ目の「アイデンティティへの攻撃から業界を保護」をも視野に入れるところまでが Okta のコミットメントです。

この壮大な構想は Okta だけで実現できるものではありません。Okta はより安全な業界を目指し、NIST、OpenID、FIDO といった、業界標準を策定する団体と連携して進めています。

これらの取り組みはすでに目に見える効果が出始めています。悪意あるアクセスの遮断や、盗まれたアカウント資格情報で仕掛けられた自動ログイン要求(クレデンシャルスタッフィング)の大幅削減、8 億以上のユーザーの継続的保護などのように、数字で現れはじめました。



日本においては、セキュリティに関する迅速な情報共有（日本語・英語）、パートナーとの共同の取り組み、日本法人における CSO (Chief Security Officer) 職の創設を通じて、日本国内におけるセキュリティ支援体制を着実に強化し、本国との連携も含めて全方位的に進めていきます。

企業の重要課題であるコスト、収益、そしてセキュリティを解決するアイデンティティ。アイデンティティで世界は変わると Okta は信じ、業界をより良くしていきたいと考えています。

新しい世界への入口： 最新アイデンティティソリューション

Okta が宣言した Okta Secure Identity Commitment は、新たなソリューション発表の中でもその考え方が色濃く反映されています。「Okta Launch Week」では製品の最新情報やトレンドが発表されており、本章では 2024 年 9 月以降の内容から特筆すべきソリューションを取り上げます。

Workforce Identity Cloud で使える 2 つの新ソリューション ～セキュリティ戦略の根幹となるセキュリティ～

Okta の調査では、83% の企業が「管理対象のアイデンティティが今後 1 年で増加する」と回答しました。企業が自社を防御するためのアイデンティティ管理は、より高度な機能が求められています。

管理状況の可視化と制御：Identity Security Posture Management

情報漏えいにおいて認証情報の悪用が起因する割合は高まり続けており、ある調査ではその割合が 80% 以上に上る * とされています。システムの複雑さが増す中、誰がどんな管理者権限を持ち、その権限がどのシステムに紐づいているか、その権限が本当に使われているかを把握するのが困難になってきました。Identity Security Posture Management はそれらを可視化するダッシュボードを提供します。当ソリューションでは、可視化された内容に基づいて、ダッシュボードから直接、管理者権限の削除が可能です。複雑化するユーザー管理の状況の可視化と制御、そして対応までが一気通貫でできるようになりました。

*Verizon Data Breach Investigation Report, 2024

検知と即時対応：Identity Threat Protection with Okta AI

セキュリティの防御点はログインだけではありません。ログインによる認証後も狙われています。Fortune 1000 の企業から窃取されたセッションクッキーは 18 億以上 ** とされ、ログイン後の対策も必要です。Identity Threat Protection with Okta AI はログイン後の通信まで監視し、AI によってリアルタイムでリスクを検出、適切な対応が即座に実行される仕組みを提供します。

**SpyCloud Fortune 1,000 Identity Exposure Report, 2023

Customer Identity Cloud で使える 2 つの新ソリューション ～セキュリティと売上のバランスを～

Okta の調査では、認証したユーザー全体の 25% が盗まれたアカウント資格情報で仕掛けられた自動ログイン要求（クレデンシャルスタッフィング）だったことが判明しています ***。Web を通じてサービス提供する企業にとって、顧客への提供サービスの安全性は喫緊の課題であるものの、売上に犠牲にすることはできません。Okta のソリューションではそのバランスを維持しながらセキュリティを向上させるサービスが発表されました。

***Okta, The State of Secure Identity 2023

トランザクションの保護：Highly Regulated Identity

オンライン決済が浸透する中、欧州を中心に、決済機能に厳しい基準が設けられるようになりました。当ソリューションでは、強力な顧客認証機能を通じて、欧州の基準に準拠したサービスを実装できます。さらに銀行における口座連携・資金移動といったトランザクションにおいても、業界が求める技術仕様（Financial Grade API）に対応しました。

利便性とのバランスも考慮され、高い機密性が求められるトランザクションを保護すると同時に、ユーザーにストレスを与えることなく、本当に必要なときのみ認証することも可能で、利便性との両立を実現します。

ノーコードで実現するフォームの仕組み：Actions

Web アプリケーションで実装される、ソーシャルログインとの連携、同意管理（メールアドレス確認や利用規約への同意を経てアプリを使うようにする仕組み）についても、ノーコードで作れるようになりました。エンジニアの稼働が不要となるだけでなく、各種テンプレートの提供も利用して短期間で実装することができます。



ーション



Okta Japan株式会社
ソリューションマーケティング
シニアソリューションマーケティングマネージャー
高橋 卓也

ベストプラクティスの共有と業界への貢献

Okta Secure Identity Commitment は「アイデンティティ攻撃への対策において業界をリードするための長期的施策」と位置づけることもできます。年間最大のアイデンティティに関するグローバルイベントである Oktane でも、このコミットメントに沿って新たな製品が発表されました。特に目立ったのはベストプラクティスの共有と業界への貢献に関するものです。

"Okta 利用のベストプラクティス" : Secure Identity Assessment

Secure Identity Assessment (SIA) は、Okta 製品が持つポテンシャルを十分に発揮させることで、投資の効果を最大化させるアセスメントサービスです。Okta 社内での取り組みや、お客様支援の中で得た知見がベースになっており、まさに Okta Secure Identity Commitment の一つである「ベストプラクティスを推進しお客様を保護」を体現するものです。当サービスでは専門家主導の評価を受け、自社に合ったロードマップを策定して、セキュリティ成熟度を追跡・強化することができます。

初の業界標準 : Interoperability Profile for Secure Identity in the Enterprise (IPSIE)

Okta はアイデンティティを守るテクノロジーにおいても、業界のリーディングカンパニーとして標準化に取り組む必要があると考えました。Okta は世界初のアイデンティティセキュリティ標準である Interoperability Profile for Secure Identity in the Enterprise (IPSIE) について、OpenID Foundation のワーキンググループにて提言しています。

これによって企業アプリ全体にわたり、より強化されたエンドツーエンドのセキュリティが実現可能です。IPSIE は業界への貢献を意識したものであります。標準の仕組みができることで、サービスを開発する企業（ベンダー）が、容易に強固なセキュリティ機能の提供と、高い製品訴求力が実現できます。

SaaS アプリとの統合 : Secure Identity Integrations (SII)

Okta 製品の特徴でもある中立性を体現するものとして、新たに 125 以上の SaaS アプリとの新しい統合が実現しました。導入済みアプリケーションとの統合がより進むことで、セキュリティ態勢の強化が図れます。

「だれもがあらゆるテクノロジーを安全に使えるようにする」

Okta Launch Week は今後も定期的 to 実施され、Okta Secure Identity Commitment に沿ってさまざまな新機能や取り組みが発表されます。Okta のミッションである「だれもがあらゆるテクノロジーを安全に使えるようにする」の実現へ向け、新機能や情報の提供を続けていきます。

Okta Identity Summit Tokyo 2024 の視聴はこちら

<https://www.okta.com/jp/resources/okta-identity-summit-tokyo-2024>



Customer Story 01



“Oktaは費用以上に投資対効果を重視できるもの”

急成長の中で生まれた業務やシステムの断片化

採用支援・就労支援・業務支援と、HR領域で幅広くサービスを提供する株式会社ネオキャリアは、2022年にDX推進部が設立され、デジタル戦略において中長期のゼロトラスト化に向けてIDaaSの検討を開始しました。

多数の事業を抱えて急成長した同社では、事業がサイロ化し、システムやオペレーションが断片化してしまったとのこと。同時に、多くのSaaSが利用されることでシャドーITが乱立する課題もあったといいます。

“重要なのは思想”
定量的にも定性的にもIDaaS製品を比較検討

同社が進めるDXの大前提はゼロトラストセキュリティ。すべての情報資産の安全を担保しながらも、事業のスムーズな運営を後押しする必要があります。同社はその基盤としてクラウド型ID管理・統合認証サービス（IDaaS）製品の検討をはじめました。

ネオキャリアがIDaaS推進で掲げたROIの考え方とは

選定に際しては、定性面・定量面の双方で総合評価が進められ、定性面では「操作性」「保守性」、定量面では数多くの指標を比べつつ、「導入によるオペレーションコストの削減効果」が重要視されました。

また、費用対効果を重視する上では製品の思想も確認ポイントの一つでした。「長期で使えることが重要で、のちに考え直すのはコストがかかる」という考え方です。「柔軟性と中立性をコアに置く」というOktaの考えが、同社のアーキテクチャ思想にマッチし、以上の重点項目を中心に検討した結果、Okta Workforce Identity Cloud（WIC）が採用されました。

まずはQuick Winを。
次に定着化、そして最大化へ

導入に際しては「中長期の視点でゴールから逆算してアジャイルに取り組む」ことを念頭に置いて進められました。最初に小さな成功である「Quick Win」を目指し、その後に定着を、そして会社全体へ広げて効果を最大化する考え方です。並行して各事業部のステークホルダーへ説明し、そこではROIの説明責任を果たして進められました。事業部門への説明を先に実施したのは、情報システム部門ではなく事業部門で効果を出し、その結果社内で認められ、広がっていくという狙いがあったためです。

効果計測の指標は「オペレーション効率化によるコスト削減額」と「インシデント発生時の想定損失額」の2点でした。この指標を短期と中長期それぞれで定期的に計算し、毎年のチェックポイントで各ステークホルダーに説明して回ったといいます。

機能理解と適用箇所拡大でROIは想定4倍に

導入後の定性評価としては想定通りにプロジェクトを推進できた点が評価されました。定量効果は導入から1年で想定4倍にもなっています。事業とシステムの双方の理解が深まるにつれて高い効果が出るのが、導入チームの発見として残ったといいます。短期視点では旧システムの廃止、BPO事業のオペレーションコスト低減、アカウント管理の工数削減など、約1,400万円のコスト削減効果がありました。中でも、Oktaは連携アプリが多く、半年で1,200を超える連携ができたことが評価されました。結果的にシャドーITの問題にも対応できています。

今後はOkta Workflowsを使ってオペレーションをさらに効率化し、B2C事業に対してのOkta Customer Identity Cloud（CIC）検討、そしてCICとWICのシナジー創出にもチャレンジするという展開を同社は検討中です。

業務効率化とシステム代替により短期間でリターンあり

リターン	リプレイス（廃止）	XX万円	● 旧IDシステム廃止
	事業改善（BPO事業）	XX万円	● 月240時間削減（200システム対象）
	新規システム導入作業	XX万円	● 月10時間削減（10システム対象） ● ID管理効率化
	ヘルプデスク業務	XX万円	● 月10時間削減 ● ID問い合わせ効率化
	総計	1,400万円相当	

※社外スライド用として詳細数値は非公開
※2024年6月時点

Customer Story 02

LINEヤフー

8ヶ月で完遂したLINEヤフーグループの認証基盤統合



LINEヤフー株式会社
コーポレートIT統括本部 IT戦略本部
ITプラットフォームサービス2部 リーダー
齊藤 隆弘 氏

“Oktaなしでは 短期間での統合は 実現できませんでした”

巨大グループ誕生を支えた認証基盤の統合

検索・ポータル、eコマース、メッセージャー、広告など、多様な領域で事業展開するLINE ヤフー株式会社。同社は2023年10月にLINE 株式会社やヤフー株式会社などの5社再編を経て誕生しました。連結従業員28,000人を数える巨大グループ誕生を支えた、認証基盤の統合に迫ります。

8ヶ月という短期で挑む

実は旧Zホールディングスではこの大再編前からグループ全社で利用する統合認証基盤の構築構想が

ありました。「再編はトップシークレットで基盤チームも知りませんでした。発表から完了まで残された時間はわずか8ヶ月。超短期で実現する必要がありました」と、LINEヤフー株式会社 コーポレートIT統括本部 IT戦略本部 ITプラットフォームサービス2部 リーダーの齊藤 隆弘氏は振り返ります。

同社では認証基盤としてはOkta Workforce Identity Cloudの採用は決まっていたものの、大再編によって、より多くの人やユースケースに対応する必要性に迫られました。そこで人事データの集約は予定通り実行しつつ、セキュリティに関する認証要素を追加し、認証統合は最適なバランスを考慮する形で進められました。

Oktaのメリットを負荷なく享受する作戦 「Migration & Federation」

認証統合のコンセプトは「Migration & Federation」。新しい環境に移行する「Migration」と、既存の仕組みを活用する「Federation」の組み合わせです。「全社員が使うものはMigrationで、それ以外は各社のIDPを流用しました。Federationでは旧アカウントの運用が残りますが、移行の負荷なくOkta認証のメリットが受けられます」と、齊藤氏はそのメリットを説明します。

統合認証基盤実現の3要素

このように同社の認証基盤の統合については、以下の3つの柱を軸に進められました。

● 人事データの集約

各社の人事情報をマージしてOktaに取り込む構想は当初の予定通りです。「各社の人事データをマージして、Oktaの中で最大公約数的なプロファイルを定義して差異を吸収しています」（齊藤氏）

● セキュリティ要素の追加

生体認証に加え、FastPassとSecurity Key (FIDO2) が追加されました。「多くの職種がある当社ではスマートフォンが使えずに生体認証ができないケースもカバーすることにしました」と齊藤氏はその理由を説明します。

● 認証統合

認証機能をOktaに集約することは外せない大命題でした。旧Zホールディングスグループ統合IDP構想をベースに「Migration & Federation」の考え方で最適化し、Okta認証のメリットを受けられるように実装されました。

完遂した超短期ビッグプロジェクト

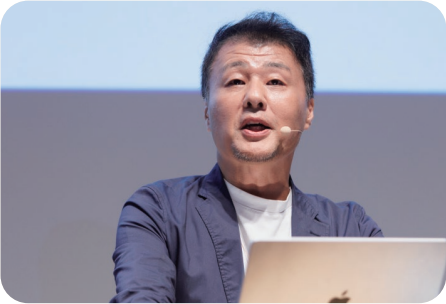
プロジェクトは8ヶ月で完遂。実に39,000ものユーザー数、SSO（シングル・サインオン）を使用するアプリはなんと550。セキュリティもMFA（多要素認証）の利用率は90%以上を達成しています。「Oktaなしでは短期間での統合は実現できませんでした。実現できたのはひとえにOktaの柔軟な設計によるものです」と齊藤氏は評価します。同氏が例として挙げたのは、「ポリシー適用の柔軟さ」「SSO導入の手軽さ」「ドメイン集約のやりやすさ」でした。同時に齊藤氏はこの先の運営も見据え、「セキュリティの脅威は手口が高度化しています。端末やセッションを乗っ取られた場合など、防御の範囲は認証以外にもあります。さらなるセキュリティの強化はOktaにも期待しています」と締めくくりました。

Okta導入による効果

数字で見るOktaの導入効果



Customer Story 03



Sansan 株式会社
情報セキュリティ部 部長
竹脇 竜 氏

“これからも業務や
IT環境を変革し続ける。
Oktaによってセキュリティと
利便性は両立できる”



Sansan 株式会社
コーポレートシステム部 部長
三浦 俊介 氏

Sansanのゼロトラスト
～セキュリティと利便性は両立できる？～

成長を続ける企業が目指した
ゼロトラストの形とは

2007年の創業後、上場を経ていまま成長を続ける Sansan 株式会社。直近3年間では700人以上が入社し、人員拡大の規模もより大きなものになっています。同社の情報システムでは新しいテクノロジーを積極的に使いながら、ユーザーが安心・安全かつ使いやすい環境が模索され、3つのフェーズに分けてゼロトラスト実現への取り組みが行われました。

「セキュリティと利便性を両立させる」
という前提

「Sansanには企業文化としてのMVV（ミッション、ビジョン、バリュー）に加え、『セキュリティと利便性を両立させる』というPremise（前提）を掲げています」と、情報セキュリティ部部長の竹脇 竜氏は企業としての姿勢を強調します。「一見相反する2つを高度にバランスさせ、両立させるのです。これはセキュリティに携わる者の理想形です」（竹脇氏）。

まずは多様な働き方への対応
～ゼロトラスト環境の構築

同社が最初に取り組んだのはゼロトラスト環境の構築です。「サイバー攻撃の高度化に伴い、従来の境界型防御が難しくなりました。拠点拡大や在宅勤務への切り替えへの柔軟な対応ニーズもありました」と、竹脇氏はその背景を説明します。同氏は「最も重要となるのが認証基盤。ここにOkta Workforce Identity Cloud (WIC)を採用しました」とし、選定の決め手として「機能の豊富さと柔軟性」「連携可能なサービスの多さ」を挙げました。

これによってオンプレミス型のActive Directory（Windowsシステムでの認証）はOktaとなり、「多要素認証の必須化とあわせて脆弱性の不安を克服できた」と竹脇氏は評価します。堅牢性とのトレードオフで語られがちな利便性・効率性についても、WICのプロビジョニング機能でアカウント管理担当者1名分程度の工数を削減するとともに「柔軟な多要素認証対応によってUXをシンプルにし、認証ステップを約半分にしてユーザーの利便性を担保できました」と同氏は振り返ります。

「超本気」のペネトレーションテスト
～高度なサイバー攻撃への対応強化～

同社におけるゼロトラストの構築は次のステップへ進みます。高度なサイバー攻撃への対応強化を目的に「超本気」のペネトレーションテストを定期的に行いました。作業員になりすましてのオフィス侵入や、優秀なハッカーたちによる攻撃を実施し、その取り組みは社外からも注目が集まりました。性質的に詳細説明は控えられたものの、「より高度なデバイス認証も導入し、そこでも機能面・コスト面の双方からOktaの採用を決めています」と竹脇氏は説明します。

ゼロトラストの理想形へ
～アカウント完全集中管理～

ゼロトラストの理想形に向けて同社が取り組んだのはアカウントの完全集中管理です。「情報システムの運用は、費用対効果が見合うことが必須。アカウントの集中管理は効率的に運用していくために大事な論点」と同社 コーポレートシステム部 部長の三浦 俊介氏は情報システムを俯瞰的に見る立場から、その重要性を説明します。「WICが連携できるサービスはとて多い一方で、連携するもう一方のサービス側でライセンスコストが上がるものがあります。コスト面でOkta連携を見送ったサービスについても一元管理できる仕組みを検討しています」と三浦氏は狙いを説明します。

そこで同氏が注目しているのがOkta Workflowsです。Okta連携のないサービスについても、APIを通じてアカウントの作成・削除が実施できるため、アカウントの完全集中管理が実現できます。「アカウントの作成・削除漏れが減り、インシデント発生時のアカウント権限の可視化も可能です。結果的にセキュリティ面だけでなく、利便性・効率性においても効果が見られます」と三浦氏はその効果に期待を寄せ、「ゼロトラストの理想形にまた一步近づくと考えています」締めくくりました。

Sansanゼロトラストの変遷とOktaの活用

	過去：2020～ Phase 1	現在：2023～ Phase 2	未来：2024～ Phase 3
ゼロトラスト の変遷	働き方の多様性への 対応	高度なサイバー攻撃への 対応強化	アカウント 完全集中管理
Okta の活用	Okta WIC	Okta Device Trust	Okta Workflows

Customer Story 04



株式会社 LegalOn Technologies
執行役員 CTO

深川 真一郎 氏

“新規プロダクトにおいて、コストをかけなくても、がっちりセキュリティが担保された状態になりました”

LegalOn TechnologiesがOktaで実現した 爆速グローバル × マルチプロダクト戦略

異なるライフサイクルの複数製品を どうまとめ上げるか

リーガルテックの国内フロントランナーである株式会社 LegalOn Technologies は、Okta の導入により、グローバル展開とマルチプロダクト戦略を強化。事業フェーズに応じた活用で、5 つの主要サービスのうち 4 つで Okta を採用し、コスト最適化と高いセキュリティを実現しました。

“早く低コストで、将来性も” アーリーフェーズ新規プロダクト (0→1) での採用

プロダクトの初期フェーズでは「とにかく早く、コストをかけずにサービス提供することが必要」と同社執行役員 CTO 深川 真一郎氏。同社が求めた要件は、サービスに低工数で組み込めること、将来的な拡張性があること、安価であることです。この条件下で Okta Customer Identity Cloud (CIC) が採用された決め手は即時に必要な機能のバンドルと、認証方式の追加の容易性（拡張性）、成長に応じた柔軟なプライシングモデルにありました。

“高度なセキュリティとSLA対応” グロースフェーズ既存プロダクト (10→100) での採用

プロダクトの実績が積まれてくると、次はグロース（拡大）フェーズです。同社では複数の実績あるプロダクトが拡大フェーズにありました。「エンタープライズ顧客に販売セグメントを広げたい、様々な顧

客要望に対応したい、今後のグローバル展開も視野に入れたい、といった要請がありました」と深川氏は振り返ります。求められた要件は「高度なセキュリティ要件と SLA 要求への対応」・「より高度なカスタマイズ」・「対応リージョンの豊富さと、各国の個人情報保護規制への対応」です。グロースフェーズにあるプロダクトへの採用においては、Bot 検知などの高度な攻撃保護機能と 99.99% の SLA、独自認証フローが作れるカスタマイズ性、GDPR や CCPA 等の保護規制への対応が決め手となりました。

グローバル展開は“法対応とカスタマイズ性”

深川氏が特に強調したのはグローバル展開を見越した要件です。「個人情報保護規制に対応できるようにデータを域内に配置・アクセスでき、ログインの体験を現地の志向性に合わせてカスタマイズできる点を評価しました」（深川氏）。さらにレイテンシーの観点から利用者から近いリージョンにアクセスでき、CIC は GDPR への確実な準拠を実現しています。

マルチプロダクト利用で生まれた思わぬ効果 ～コスト負担なしでセキュリティが強固に～

Okta の導入によって、同社は高いセキュリティを小さな体制で維持し、「自前で認証基盤を構築した場合と比較して約 90% のコスト削減効果が見られました」と深川氏は説明します。認証に関する数多くのベストプラクティスがあらかじめ実装されていることによって、品質だけでなく、短期間でのリリースをも実現しました。

さらに、マルチプロダクトで Okta を利用した結果、「思わぬ恩恵を得ることができた」と深川氏は付け加えます。「新規プロダクトも追加コストなく上位プランの高度なセキュリティ機能を利用でき、新規プロダクトにありがちなセキュリティの弱みを強みに昇華できました」（深川氏）。

現代のプロダクトに求められるセキュリティ水準は上がり続けています。UX と堅牢さを合わせた認証基盤への要求も高まっています。「当プロジェクトで Okta を選んだのは正解だったと思っています。グローバル展開を見据えたさらなる柔軟性を期待します」と深川氏は締めくくりました。

Oktaを採用した効果

Quality

- 脆弱性診断で、認証基盤に起因する指摘は過去6年で **0件** ※設定不備を除く
- （エンタープライズに対応するための）SAML連携機能を **キックオフからリリースまでエンジニア3名体制で2ヶ月**で実際にリリース

Cost

- 自前で認証基盤を構築した場合と比較し、**約90%**のコスト削減効果
- 他IDaaSを利用して開発した場合と比較し、**約40%**のコスト削減効果

Deliver

- 事業初期、認証に詳しいエンジニアが **0人**の状態ですサービス提供開始
- LegalOn Cloudの複雑な統合プロジェクトを**1年**という厳しい納期内に予定通りリリース
 - 参考: リリース時点(2024/4/15)でマージされたPullRequest数: **約12,000PR**

Customer Story 05



株式会社 SUBARU
国内営業本部 ビジネスイノベーション部
カスタマーエクスペリエンスグループ 主査
吉田 隆幸 氏

“ID登録者数は4年間で 約2倍の200万件にまで 到達しています”

変化が続く自動車業界

世界に誇る日本の基幹産業である自動車業界はいま、目まぐるしい変化にさらされています。特に日本では高齢化や若者のクルマ離れによる販売台数の鈍化といった現象を受け、業界各社は顧客に選ばれ続けるための試行錯誤を重ねています。

「安心と楽しさ」をコンセプトに、衝突回避をサポートするアイサイトを提供し、歴史ある水平対向エンジンで根強いファンを持つ SUBARU は、国内市場における顧客体験の変革に取り組みしました。

顧客体験を進化させるSUBARUのID戦略

国内市場の課題

株式会社 SUBARU 国内営業本部 ビジネスイノベーション部 カスタマーエクスペリエンスグループ 主査 吉田 隆幸氏は、国内市場の課題を、高齢化・若者のクルマ離れによる「市場縮小」、資材高騰とクルマづくりの高度化による「高価格化」、そして基本性能差の縮小による「コモディティ化」だと説明します。これによって顧客体験向上による高付加価値・差別化の重要性がさらに高まっています。

しかし、顧客体験の多くがデジタル空間上で享受される中、「SUBARU には体験の分断によって顧客利便性が欠如していた」と吉田氏は振り返ります。同社が顧客に提供する SUBARU ID に対応するサービスが限定的で、SSO（シングル・サインオン）にも未対応の状態となっていました。「キャンペーンに申し込んだ SUBARU ID、カタログ請求で使われる ID、オンラインショップで使う ID が異なっていたことで顧客体験が分断されていました」（吉田氏）。

SUBARU IDによる 統合顧客ID管理基盤の構築へ

サービスごとに ID が分散すると、顧客利便性の欠如だけでなく、顧客データのサイロ化も発生します。「データがバラバラで顧客ごとの行動やニーズが捉えられない」と吉田氏は指摘します。そこで同社は、「SUBARU ID をキーに、オンライン/オフラインのあらゆる接点で顧客にパーソナライズされた体験を

提供する」ことを目的に統合顧客 ID 管理基盤の構築に取り組みました。

ID 管理基盤のプラットフォームとして導入されたのは Okta の Customer Identity Cloud です。「選定の理由はセキュリティ、性能・機能、開発・保守、コストの4点の側面です。中でも、多要素認証への対応、ソーシャルログイン種類の豊富さ、対応言語の豊富さが重視したポイントでした」と吉田氏は選定の決め手を振り返ります。そして「最新認証トレンドへの対応は安心感につながっています」と同氏は付け加えました。

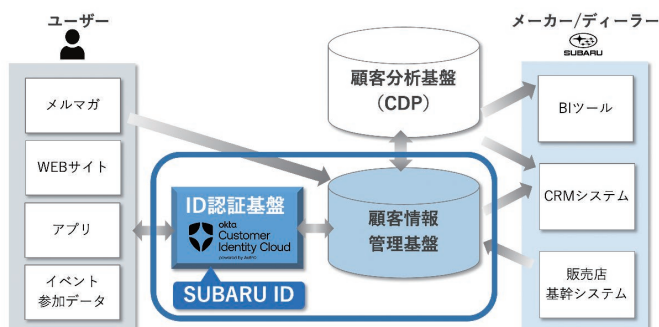
5割で成約するセグメントも。 ID戦略がもたらした変化

顧客 ID 管理基盤が統合されたことにより、同社はシームレスなサービス提供とパーソナライゼーションによる満足度向上ができる土壌が整いました。データの一元化は業務効率の改善とデータ統合によるマーケティング効果の向上をもたらしました。データから発見できたインサイトは新たなサービスの種にもなります。

ID 活用によってリード情報（見込み案件）のデータを分析し、成約確率を機械学習で予測、それをディーラーに共有することができるようになりました。「付与した成約率の最高ランクではなんと5割で成約できています。これは精度が非常に高いと評価しています」（吉田氏）。

顧客の情報はより可視化され、Web の回遊履歴や見込み情報なども統合されています。ID をキーに集約した顧客データからはロイヤルカスタマーの特性もあぶりだし、ドライブの楽しさを重視するファン顧客に向けたドライブアプリも生まれました。

「顧客中心の考え方でパーソナライズされたより良い体験を提供し続けられるよう、お客様の笑顔を作り続けるための価値づくりを続けていきます」と吉田氏は意気込みを語りました。



Customer Story 06

MS&AD

MS&AD InterRisk Research & Consulting

MS&AD インターリスク総研株式会社
DI 推進部 開発第一グループ上席コンサルタント

芝田 達郎 氏

“私自身も認証機能の
実装をやってみたところ、
その簡単さに衝撃を受けました”

TC3 株式会社
代表取締役
須藤 義人 氏

「スモールスタートとスケーラビリティ」で挑戦した MS&ADインターリスク総研の顧客認証基盤

B2B SaaSビジネスへの挑戦

MS&AD ホールディングスのグループ企業としてリスクコンサルティング事業・調査研究事業を手掛ける MS&AD インターリスク総研株式会社は、2022 年から全社で DX を推進し、その一貫として、企業向け SaaS の形で「リスクマネジメント ナビ」を軸とする各種サービスを新規展開しています。

「リスクに強い組織づくりをする企業の課題解決に向けた、各種データとコンサルティングを中心に提供しています」と、MS&AD インターリスク総研株式会社 DI 推進部 開発第一グループ上席コンサルタントの芝田 達郎氏はその狙いを説明します。

各種サービスの提供にあたって同社が実装したのは、MS&AD が提供する事業者向けデジタルソリューションへのアクセスを可能にする共通 ID「InterRisk ID」。InterRisk ID に求められたことは、顧客企業がユーザーを一元管理でき、同社が提供する複数の B2B SaaS ソリューションへのアクセス範囲を、顧客企業が個人単位で細かく設定できたことでした。さらに短期間で複数サービスを提供していくため、スピードとサービス間の相乗効果も欠かせない要件となっていました。

Okta選定の決め手は 「コスト・セキュリティ・フレンドリーさ」

新規ビジネスの認証基盤として同社が採用したのは Okta の Customer Identity Cloud。決め手は「コスト・セキュリティ・フレンドリーさ」にあったと芝田氏は説明します。「1 つ目はコストです。スモールスタートで新規事業を開始するため、初期投資を抑えつつ、必要な機能をあとから追加する方法を取り

ました。Okta の課金の柔軟性がこれにフィットしました」（芝田氏）。

2 つ目はセキュリティです。リスクベースでの多要素認証、Bot 検知、パスワード侵害検知など、多種多様なセキュリティ対策は顧客認証基盤では欠かせません。「すべての機能を自前で作り上げるのは大変です。ベストプラクティスが集約された Okta を利用する結論に至りました」と芝田氏はその合理性を説明します。

最後に芝田氏が挙げたのが「開発者に対してフレンドリーなプラットフォームである」ことでした。「大規模になる共有の顧客認証基盤の開発には多くのパートナーの力が必要です。すべての開発者にとって使いやすく、言語を問わない SDK、ドキュメント、活発な開発者コミュニティが揃っていました」と芝田氏は強調します。「検証フェーズで私自身もユニバーサルログインを使った認証機能の実装をやってみたところ、その簡単さに衝撃を受けました」（芝田氏）

顧客ID管理の仕組みは 従業員向けのそれとは考え方が異なる

しかし、「これまで従業員向けの ID 管理はやってきたものの、顧客向けとなると事情が異なった」と芝田氏はその苦労を振り返ります。「ID のセルフメンテはユーザーのリテラシーが顧客ごとに異なるため、ユーザビリティが重要です。顧客一人ひとりが最初の実施するセルフサインアップについては、ユーザー増加の予測が社内向けと違って困難で、必要なスケーラビリティが大きく異なります」（芝田氏）。さらにユーザー組織のデータベース管理構造や、マルチ SaaS・マルチベンダー開発など、開発者も利用也多様で複雑に絡み合う状況にも技術的困難さがありましたが、「TC3 の顧客向け認証基盤向けの過去の知見を活用しつつ、Okta 側のベストプラクティスも参照し課題を乗り越えました」と、実装パートナー企業である TC3 株式会社 代表取締役須藤 義人氏は振り返ります。

MS&AD インターリスク総研が取り組んだ企業向けの SaaS サービスはさらなる拡大を見据え、「他社が持つ認証基盤と自社の認証基盤がシームレスに連携していけるようにしていく」と、芝田氏はこの先の豊富を語りました。

プロジェクトで挑んだ 4 つの挑戦

ポイント 1	セルフメンテナンス 顧客管理者でのタイムリーな メンバー追加削除 わかりやすい 権限付与
ポイント 2	セルフサインアップ 離脱を防ぐ 会員登録フロー
ポイント 3	ユーザーアイソレーション 複数組織兼務、副業が進むなか求められる ID 設計とは
ポイント 4	マルチSaaS マルチSaaS・マルチベンダー開発における 共通認証基盤



Thank You

Okta について

Okta は世界のアイデンティティ企業です。独立系アイデンティティ管理のリーディングカンパニーとして、だれもが、どこでも、どんなデバイスやアプリでも、あらゆるテクノロジーを安全に使えるようにします。最も信頼されているブランドが Okta を信頼し、安全なアクセス、認証、自動化を実現しています。柔軟性と中立性を中核に備えた Okta Workforce Identity Cloud と Customer Identity Cloud により、ビジネスリーダーと開発者は、カスタマイズ可能なソリューションと 7,000 を超える事前構築済みの統合を活かすことができるため、イノベーションに集中し、デジタルトランスフォーメーションを加速することができます。私たちは、アイデンティティがあなたのものである世界を構築しています。

詳しい情報については、<https://www.okta.com/jp/> をご覧ください。



okta

Okta Japan 株式会社

〒150-8510 東京都渋谷区渋谷2-21-1 渋谷ヒカリエ30 階

[okta.com/jp/contact-sales/](https://www.okta.com/jp/contact-sales/)

WP-202501-D