issue 01
Japan

iDentity Spotlight

Brought to you by okta

Okta Showcase Japan 2022
パネルディスカッションレポート
アイデンティティで変革する日本のビジネスの未来

PUBLISHER'S NOTE

アイデンティティにスポットライトをあてる「Identity Spotlight」創刊にあたって

社内外の業務をデジタル化やクラウド活用などで改革する際に、重要なキーワードの1つとなるのが「アイデンティティ」です。アイデンティティを適切に管理して活用できるようにすることによって、企業は従業員や顧客の体験を変革させ、生産性や競合優位性を高めることができます。

しかし、このアイデンティティに対する理解と認知が日本国内でまだまだ低いと感じています。アイデンティティがなぜ重要なのか、どのような役割を果たしているのか、その理解を促進していくことを目的にして、アイデンティティにスポットライトをあてる「Identity Spotlight」を創刊しました。

アイデンティティに関する識者の視点や、最新トレンド、ベストプラクティスなどを共有することで、皆様がアイデンティティを少しでも理解する一助となれば幸いです。本誌の発刊頻度は年２回を予定しております。

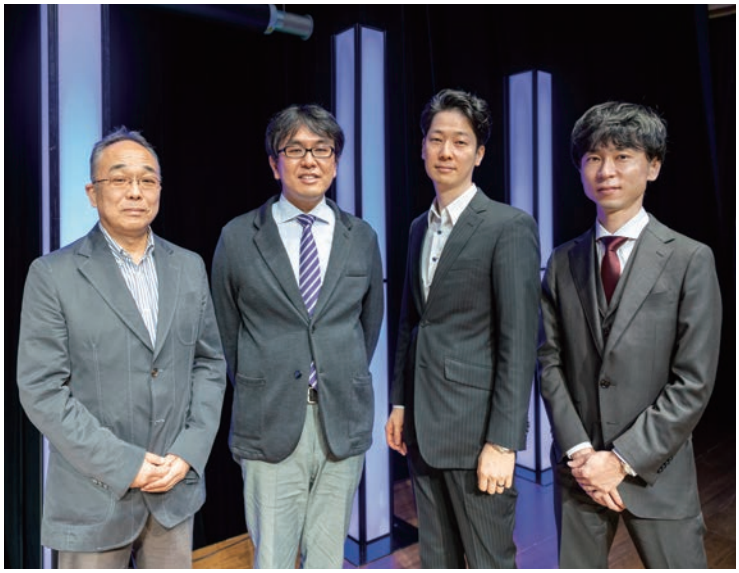
創刊号では、11月に開催したイベント「Okta Showcase Japan 2022」で非常に好評だったパネルディスカッション「アイデンティティで変革する日本のビジネスの未来」の内容をカバーストーリーとしてご紹介します。ビジネス環境の変化と課題、アイデンティティ管理が従来のID/パスワードによる管理と何が違うのかなど、アイデンティティに焦点をあてた議論が展開されております。また、サントリー様、コープさっぽろ様、DNP様がどのような課題を解決するためにアイデンティティを活用されているのかご紹介します。

本誌は、アイデンティティに関する考えや視点を共有できるオープンな場であり続けるよう努力してまいります。皆様のご意見をお寄せいただいたり、貴社内での課題を解決するために成功した事例をご紹介いただくなど、ぜひ本誌の寄稿者としてご参加ください。アイデアの大小は問いませんので、皆様の知見を共有して頂ければ幸いです。

そうした皆様の知見や成果を発表する場として、この「Identity Spotlight」が皆様のお役に立てることを願って、創刊の言葉とさせて頂きます。

Okta Japan株式会社
代表取締役社長
渡邉 崇

CONTENTS

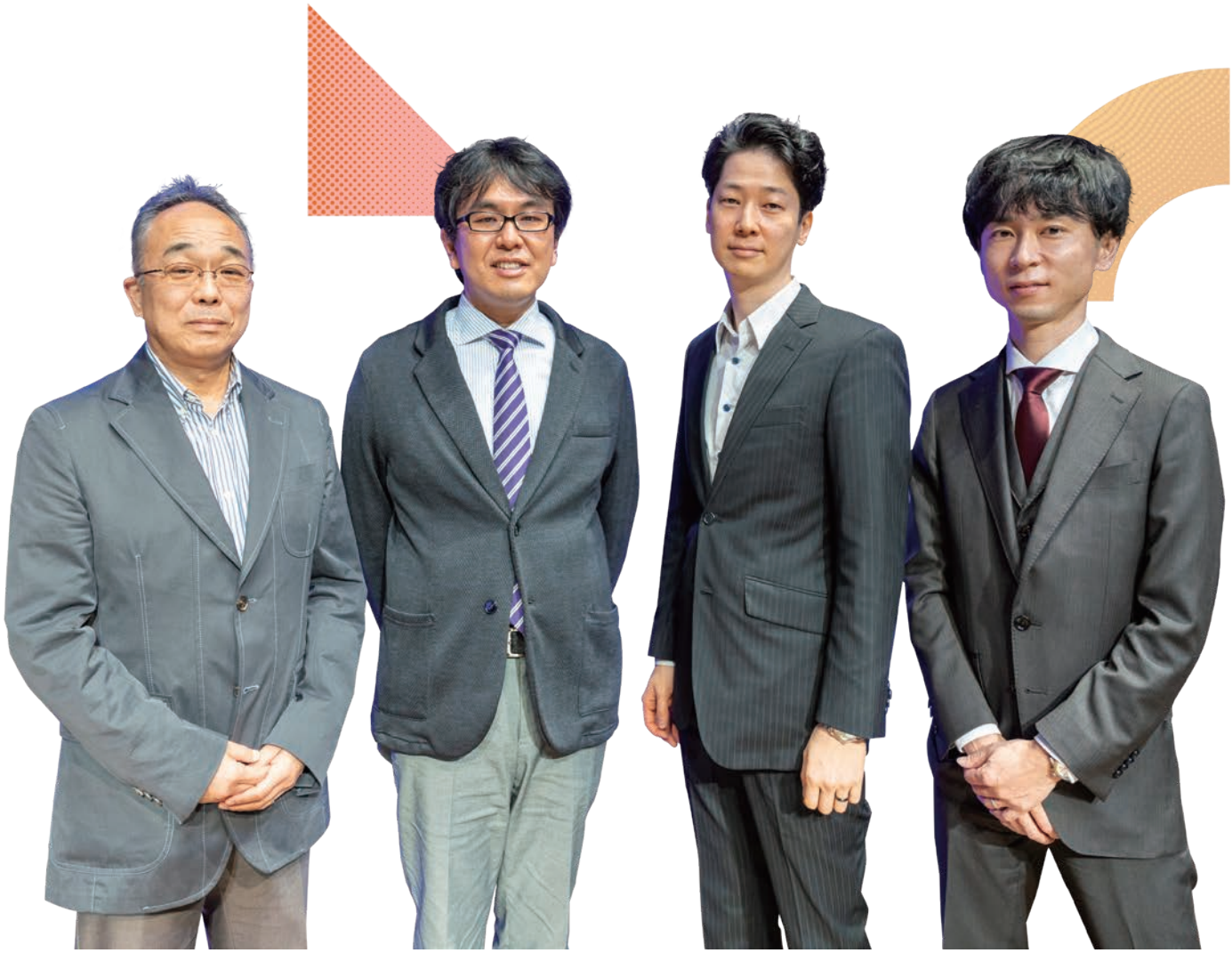


COVER
STORY

パネルディスカッションレポート

アイデンティティで変革する日本のビジネスの未来

なぜ今アイデンティティが急に注目されているのでしょうか？ その疑問に答えるべく、アイデンティティ分野の最前線でご活躍されている有識者によるパネルディスカッション「アイデンティティで変革する日本のビジネスの未来」が、11月30日に開催された「Okta Showcase Japan 2022」の中で行われました。



(左から)ITジャーナリスト　**谷川 耕一** さん(ファシリテーター) ／ KPMGコンサルティング株式会社 シニアマネジャー　**畠山 誠** さん ／ 株式会社日立ソリューションズ セキュリティサイバーレジリエンス本部 認証セキュリティ部 セキュリティスペシャリスト　**松本 拓也** さん ／ 株式会社ラック セキュリティソリューション統括部 ソリューション推進第二部 プラットフォームソリューションサービスグループ グループマネージャー　**稲毛 正嗣** さん

リモートワーク優先からセキュリティへの回帰

パネラーとして登壇したのは、企業のITの戦略策定や導入を支援するKPMGコンサルティングの畠山さん、Oktaの販売パートナーであり、アイデンティティ管理のプロジェクトに関わる日立ソリューションズの松本さん、セキュリティソリューション企業としてシステム構築を行うラックの稲毛さんの3人。ITジャーナリストの谷川さんが、ファシリテーターを務めました。

はじめに谷川さんが、コロナ禍から現在までの仕事の変化を聞きました。畠山さんは、最近は「リモートワークからセキュリティへの回帰」が始まっているとの見方を示します。

「コロナ禍のはじめの頃は、『セキュリティではなくリモートワークが優先』でした。社員のリモートワークPCや、VPN不足もあり、禁止していたBYODを例外処置として認める会社もありました。最近では、あらためてセキュリティのルール重視に戻りつつあります。社員のアイデンティティに余分な権限が付与されるなど、ルールが曖昧化していたため、もう一度引き締めようという動きです。ゼロトラストやDXの観点から、見直しが始まっています」（畠山さん）

松本さんも完全にリモートワークになり、働き方が大幅に変わったと語り、また顧客からの相談としては、2つの変化があったと明かしました。

「BtoCの案件で、CIAM（Customer Identity and Access Management）といわれるIDaaSの相談が増えました。もう1つは従業員向けのアイデンティティ管理の範囲が変わってきたことです。取引先のアイデンティティもOktaで管理したいという相談が増えました」（松本さん）

稲毛さんは、最近では「攻めのビジネスへの転換」が始まったと語ります。最近のプロジェクトでは、流通・小売などBtoC企業が、リアル店舗からECに軸足を移していることから、アイデンティティの新たな役割が生まれているようです。

「BtoC企業では、お客様と店員を紐付けるためにアイデンティティが重要になっています。店員はタレントでお客様がファンのような関係を作り、リアルとデジタル両方の価値を上げていく。そのためにアイデンティティが活用されているのです」（稲毛さん）

アイデンティティこそが攻撃者の標的になった

アイデンティティ管理といえば、ずっと昔からあるテーマ。これまでも企業は「ID／パスワード管理」に取り組んできたにもかかわらず、なぜ今アイデンティティ管理が注目され、Oktaが急成長しているのかと谷川さんが問いかけました。

畠山さんは、SaaS、クラウドの普及に加え、サイバー攻撃の変化があると答え、次のように続けます。

「以前のマルウェアなどは、企業のデータを手当たり次第に攻撃していました。最近では、企業が持つアイデンティティを奪い、さらに侵入を拡大して身代金を要求します。犯罪者の視点に立つと、『庭先に落ちているものを盗む』ことから、『建物の鍵を奪う』ことに変わりました。攻撃者にとって、アイデンティティは旨味があるのです」（畠山さん）

松本さんも、アイデンティティ管理へのニーズが高度化しているという見方に同意し、こう補足します。

「IT戦略として、アイデンティティ管理に特別注目していない場合でも、実装を進める中でアイデンティティ管理の重要性に気づく場合もあります。例えば、ゼロトラスト案件で、SASE（Secure Access Service Edge）のためのツールを導入するには、ユーザーリストのインポートが必要になるケースが少なくありません。そのリストは、最新の従業員情報に更新し続けることが重要です。従業員の入社から退社のライフサイクルを把握し、管理する手段として、IDaaSが検討されます」（松本さん）

社会課題としての「アイデンティティの証明」

このイベントの最初の基調講演で、Okta Japanの渡邉社長は「アイデンティティがあなたのものである世界をつくる」というブランドパーパスを掲げました。社会課題としても「アイデンティティの証明」が重要となってきています。松本さんは、「アイデンティティのデジタル化」についての思いを語ります。

「アイデンティティを証明するために、多くの労力とコストをかけています。たとえば選挙では、投票は住所に送られた投票券で認証しています。選挙がデジタル化できると、大きな変化が予想され、技術的には可能なのに実現できていない。そこには心理的な面などでのネックがあります」（松本さん）

国民のアイデンティティという意味では、政府もマイナンバーの普及に積極的。納税や給付金、医療などの行政サービスでのメリットはあるものの、今でも各種の手続きに、住所や氏名などの手書きが伴うことを谷川さんが指摘しました。これに対し、稲毛さんと畠山さんは、プライバシーの問題があるといいます。

「アイデンティティはユーザーの行動履歴など属性の集合で、マーケティング活用でもプライバシー重視にシフトしています。将来は会社と個人の関係が変わり、個人としてのアイデンティティが重要になると思います」（稲毛さん）

「アイデンティティの利用の推進には、プライバシーという観点や社会的な合意が必要。グローバルでプライバシー保護法制の整備が進む中、『自分の情報を自分でコントロールできること』が重要になってきています」（畠山さん）

Oktaの「中立・信頼・専業」が、エコシステムを生む

続いて、Oktaがなぜ市場で受け入れられ、成長しているのかが話題となりました。松本さんは、Oktaの優位性は「変化する力」に裏付けられているといいます。

「象徴的なことは、OktaのコアのエンジンをClassicからOkta Identity Engineにリニューアルしたことです。開発のコストを価格に転嫁することなく、従来築きあげてきたものを失うリスクも恐れず大胆な変更を実施し、ユーザーの移行を進めてきました。このように投資を惜しまないところが、Oktaの強みです」（松本さん）

稲毛さんは、Oktaの「中立・信頼・専業」というポリシーがあるからこそ、業界のエコシステムが生まれ、技術力の源泉になっていると

し、次のような見方を示しました。

「中立と信頼がベンダーの協力を生み、クラウドやSaaSの企業が、自ら進んでOkta Integration Networkに対応しています。最近では、ユーザーの利用情報からのインテリジェンスを導くための、Okta Insightsに専業としての技術の差を感じます。他社が有償で提供してきたサービスをIDaaSの中に取り込んだことは、セキュリティベンダーとして衝撃的でした」（稲毛さん）

最後に、企業の担当者へのメッセージが以下のように送られました。

「ツール導入に終わらず、権限の管理や業務プロセス、組織の変革のため、経営と現場の目線を合わせてDXプロジェクトに取り組んでもらいたい」（畠山さん）

「今後アイデンティティのデジタル化が進みます。その流れが、新しいビジネスを生み出すチャンスだと捉えていただければと思います」（松本さん）

「とにかくツールを試してほしい。Okta Cloud Connect（OCC）という無償版もあり、顧客向けにはCustomer Identity Cloudの無償版もあるので、ぜひ使っていただきたい」（稲毛さん）

最後に、「DXを実現するためのステップとして、アイデンティティ活用の可能性がある」と谷川さんが今後の期待を語りました。登壇者全員が意見の一致を見て、パネルディスカッションを終えました。

OKTA
SPOTLIGHT
JAPAN

SUNTORY

サントリーグループにおける グローバルIT戦略とID管理

サントリーシステムテクノロジー株式会社
グローバルサービス部
グローバルグループ 課長
紺谷 光康 氏

Okta Japan株式会社
リージョナルセールスマネージャー
渡部 和人

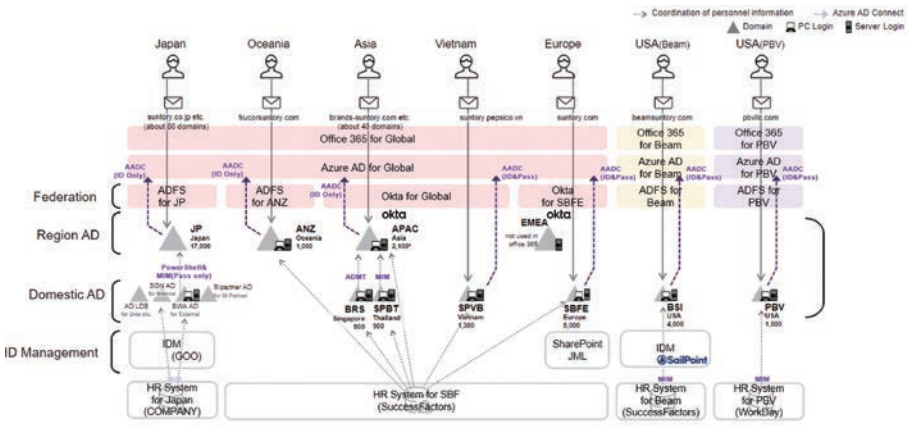
渡部：サントリー様は、日本を始めとして、北米、ヨーロッパ、アジア地域にトータルで4万人の社員がいらっしゃると伺っています。その中で、グローバルのシステムの設計や運用に携わっている紺谷さんにお話をいただきます。まず紺谷さん簡単に自己紹介をお願いします。

紺谷さん：サントリーシステムテクノロジーというサントリーのIT部門の会社に所属しています。2009年入社で、ずっとインフラをやっていました。当時は、プライベートクラウドやVMwareの仮想化みたいなことをやっていて、2015年頃から、サントリーがグローバルの市場になっていくことに伴って、グローバルのITインフラの活動、たとえばOffice 365をグローバル導入するといった仕事をやっていました。そして2018年頃にOktaを知りました。

- ID/認証基盤が各社ごとに存在する複雑な構成
- 新たにグローバルで使うアプリケーションが出来ると…

→ 従業員のIDを集められない
→ IT部門は各社ごとにログインページ作成…

■以前のシステム構成



渡部：Oktaを2018年頃知って頂いたきっかけからお伺いしたいのですが、Oktaを使ってどうにかしようという課題があったと思いますが、それを掘り下げていただけますでしょうか。

紺谷さん：アジア各地でセキュリティをもっと高めたいというときに、ちょうどヨーロッパのグローバル会社がOktaを使っていて、Oktaは全然トラブルがないのでいいよと聞いたことでOktaを導入しました。その後、徐々にサントリーがグローバルに活動していく中で、グローバルのアプリケーションを導入したいとなったときに、各国のADもばらばらだし、とにかくまずIDをどう集めればいいんだという話に始まり、今度IDがそれぞれのADにあると分かっていたとしても、日本用のログインページ、他国用のログインページといった感じでIDが統合しておらず、今の構成ではどうしようもないなということを課題として、改めてOktaを導入しました。

渡部：ありがとうございます。かなりつまびらかなお話だったと思います。システムのご導入においてクラウドが先行するクラウドファーストというコンセプトがあると推察されるのですが、そのあたりのお考えはいかがですか。

紺谷さん：どこの会社さんもある程度進んでいると思うのですが、サントリーは特にクラウド推進は進めている方だと思います。インフラ周りのデータセンター、プラットフォーム周りをグローバルでクラウド化していこうという動きを2020年頃から加速させています。また、SaaSサービスなどはIT部門がセキュリティチェックした上で安全に使えるようにしてクラウド化を推進しています。

渡部：クラウド化をワールドワイドで推進するにあたり、紺谷さんがリードされていると思うのですが、具体的にOktaをどういう風に使っていただいているか教えて頂けますでしょうか。

紺谷さん：こだわっているポイントは1つで、とにかく今まで動いていた各社の仕組みへの影響をなるべく小さくし、大きな変更がない形でOktaの基盤を作りたいということでした。もともとヨーロッパでOktaを使っていたので、グローバルでOktaを改めて使うにあたって、もともと使っていたOktaへの影響をなるべく少なくするためにHub & Spokeという形をとって、SpokeにあたるEMEAの社員が今までどおり使えるようにしました。また、Azure ADを主に認証として使っていた子会社には、Okta側からインバウンドフェデレーションという技術を使って、もともとの認証のやり方は変えずにグローバルの基盤に取り込めるようにしました。

渡部：Microsoftさんのソリューションが主体となっているところを取り込むにはOktaが一番だったということでしょうか？

紺谷さん：そうですね。なぜOktaかというところもあるのですが、これをAzure ADというかMicrosoft一色で全部やろうとすると、何年かかるか分からないような壮大な設計と期間を要するので、とにかくグローバルで1つの基盤を作りたいためにOktaを選択しました。

渡部：Oktaを選んでよかったところはどこですか？

紺谷さん：とにかくスピードです。導入するのに敷居が低いということが一番いいと思います。

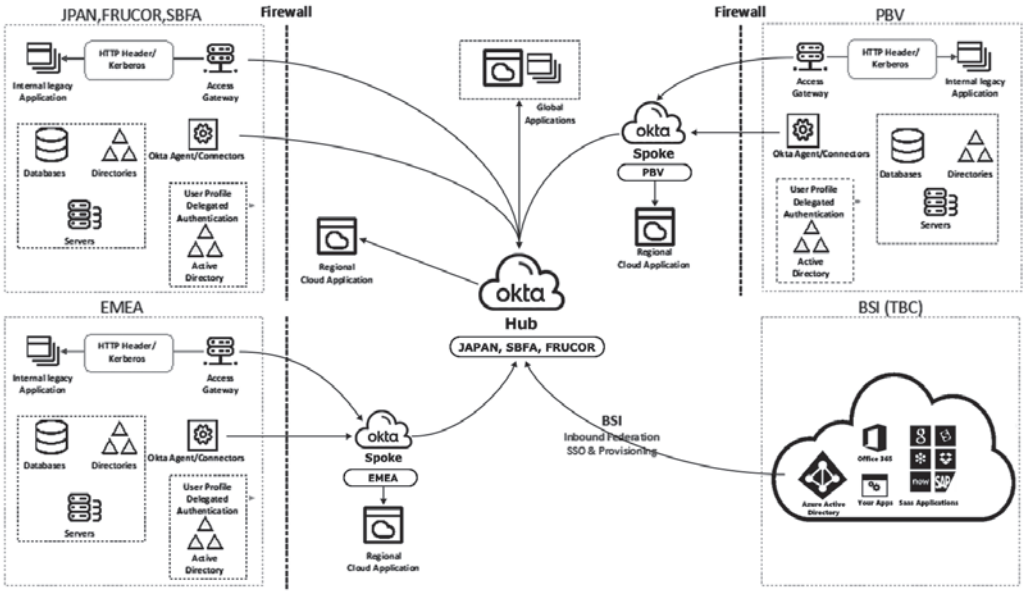
渡部：逆にOktaのここがまずいよというところは何でしょうか？

紺谷さん：1つだけあって、トラブルが起きたときに分かりにくいです。我々の使い方もあるのかもしれませんが、たまにトラブルが起きた時に何に影響があって、どうなのかということが分かりにくいです。

渡部：もう少し突っ込んでお聞きすると、たとえばそのパラメーターがよく分かりにくいということをおっしゃっていますか？

紺谷さん：Oktaで障害がありましたとアラートがあった時に、どこまで影響があるのか分かりにくい。当社のように4万人も社員がいると、その4万人のうち何人このOktaのアラートで影響を受けているのか把握することがなかなか難しいというのが悩みではあります。

渡部：グローバルでの運用体制について、深掘りしてご説明いただけますか。



紺谷さん：我々サントリーシステムテクロジーが主体となって、各地域の会社の運用を見ているのですが、協力会社さんと一緒に24時間365日グローバルで運用を見るという体制をとっています。ある程度の権限は各地域に一応ありますが、主なことはグローバルにエスカレーションしてきて、それを僕たちが運用するという体制をとっています。

渡部：各リージョン、各エリアで運用される方々や技術の方々を配されていると思うのですが、そういう体制面は自社でまかなってらっしゃるのですか？

紺谷さん：基本自社です。みなさんあまりご存知ないと思うのですが、もともと海外のグループ会社がM&Aをしてサントリーグループになった会社で、もともとの海外のグループ会社にもIT担当者がいたので、その方々はそのまま役割をスライドしながらグローバルで一緒にやっているので、現地IT社員が引き続き一緒に仕事しているという体制です。

渡部：グローバルの運用体制で言語の問題はありますか？

紺谷さん：言語の問題は正直ないですね。私はそれほど英語はしゃべれませんが、IT用語の話なので、そんなに、英語が極端にしゃべれないからといって仕事ができないということはなく、意外とそういうところに問題はありません。

渡部：今の一言は、これからグローバルで私どものサービスをご展開されるお客様にとって、勇気を与える言葉だったと思います。私どもとしても運用の体制としてはCSMなどをご提供させていただいていますし、言語を話せる人間も配していますので、そこは波長を合わせてサービスを提供しているかなと自負しています。最後に、Oktaと今後どういう未来を描いていきたいか教えてください。

紺谷さん：まずは今の時点で従業員のIDは集め切りました。ここからは、もっとOktaのプロビジョニング機能などを使いこなして、IDの管理を簡単にしていって、よりクラウドサービスの導入スピードをあげていくことができたらいいと考えています。

渡部：本日は大変ありがとうございました。

RESEARCH
REPORT

4つの数字から見る IDへの攻撃の最新動向

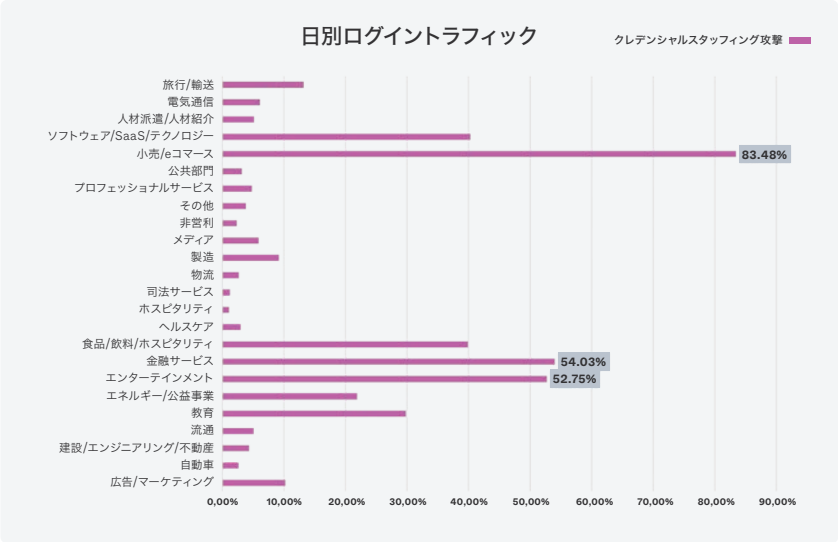
Oktaが発行した「2022 State of Secure Identity Report」では、ID管理プラットフォームであるAuth0における数十億の認証を観察することで明らかになった傾向や例、所見を紹介しています。ここで得られた洞察に光を当てることで、組織が顧客IDに対する脅威を理解する助けとなるでしょう。ここでは非常に重要な4つの数字にフォーカスし、ID侵害の最新動向について解説します。

Okta Japan株式会社
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

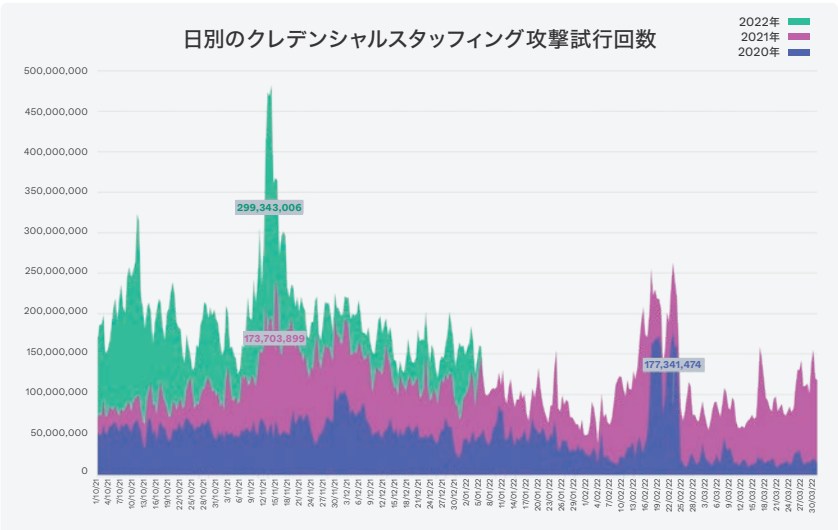
100億件のクレデンシャルスタッフィング攻撃

2022年の最初の90日間で、OktaのID管理プラットフォーム上において約100億件のクレデンシャルスタッフィング攻撃を検出しました。これは全体のトラフィック/認証イベントの約34%に相当します。攻撃は2021年後半から増加し、2022年も継続していることが見て取れます。また、攻撃は業種によるばらつきが見られました。

- **小売業、eコマース系で80%以上**
- **金融、エンターテインメント系で50%以上**
- **その他の業界では10%未満**



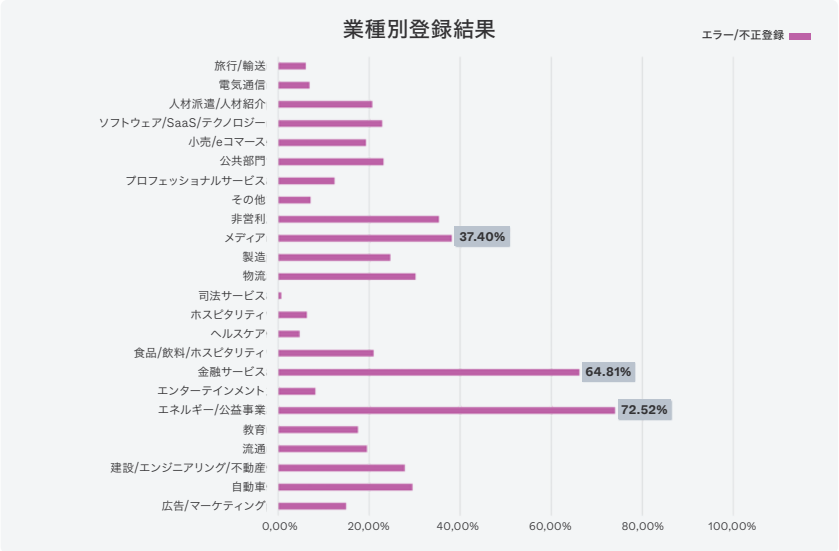
クレデンシャルスタッフィング攻撃
攻撃者がインターネット上に流出したIDとパスワードを不正に取得し、それらを用いてターゲットのWebサイトに自動的にログインを試みる攻撃を指します。ユーザーは同一のIDとパスワードの組み合わせを使いまわしていることが多いという習慣を悪用した攻撃で、botを用いて大量かつ自動的に実施されます。

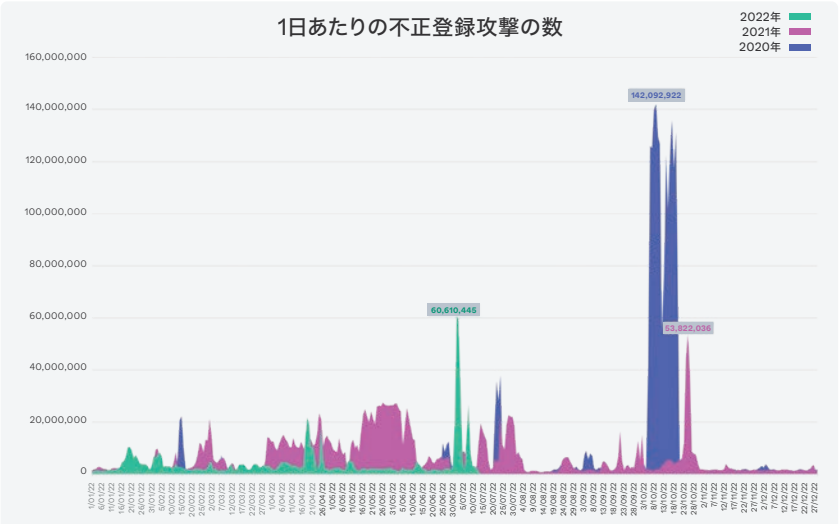


3億件の不正アカウント登録

2022年の最初の90日間で、OktaのID管理プラットフォーム上において約3億件の不正なアカウント作成の試みを観測しました。これはサインアップ試行の約23%を占め、昨年の同時期の15%から大幅に増加しています。この攻撃にも特定の業種に突出しており、2021年度と比較しても大きな変動が確認できます。

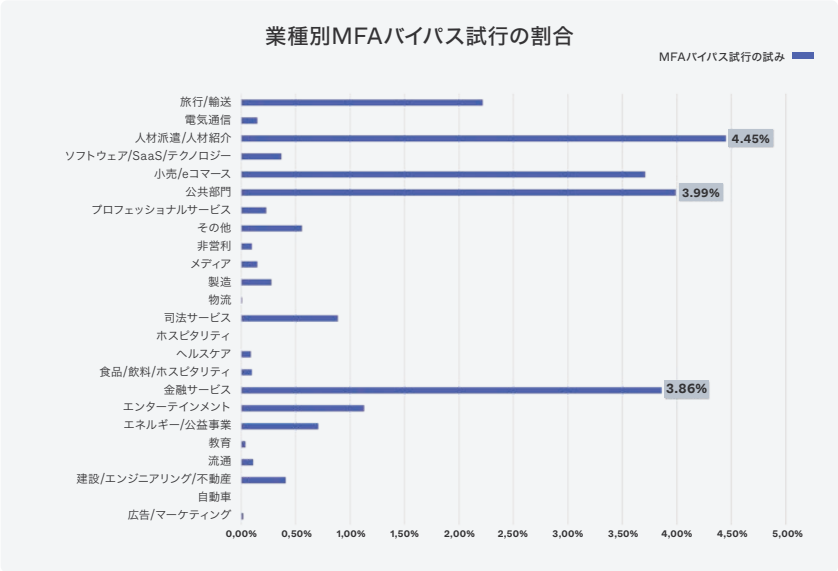
- **エネルギー、公共が70%以上**
- **金融が60%以上**

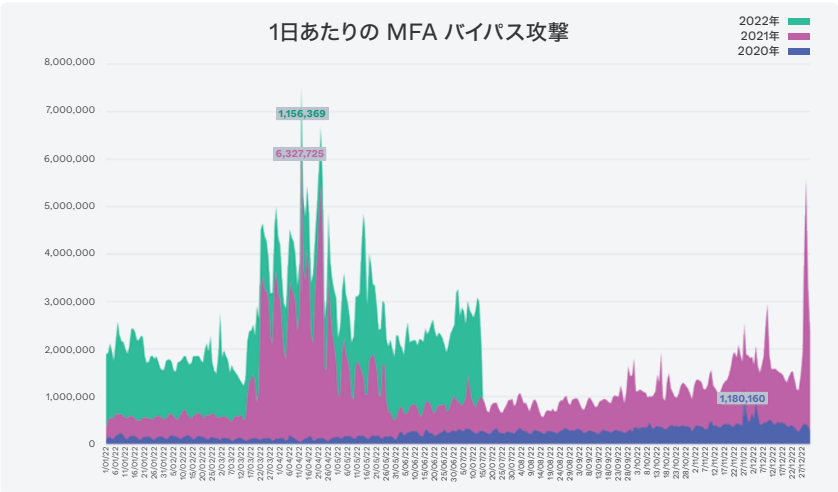




1億1,300万件のMFAバイパス攻撃

2022年の最初の90日間で、OktaのID管理プラットフォーム上において約1億1,300万件のMFAに対する攻撃を観測しました。MFAバイパス攻撃は手間がかかるため、社会的な重要度が高いターゲットに集中する傾向が見られます。具体的には「人材派遣/人材紹介」、「公共」、「小売/eコマース」、「金融サービス」に集中していました。MFAバイパス攻撃は長期的にも増加しており、過去2年よりも明らかに増加していることが読み取れます。



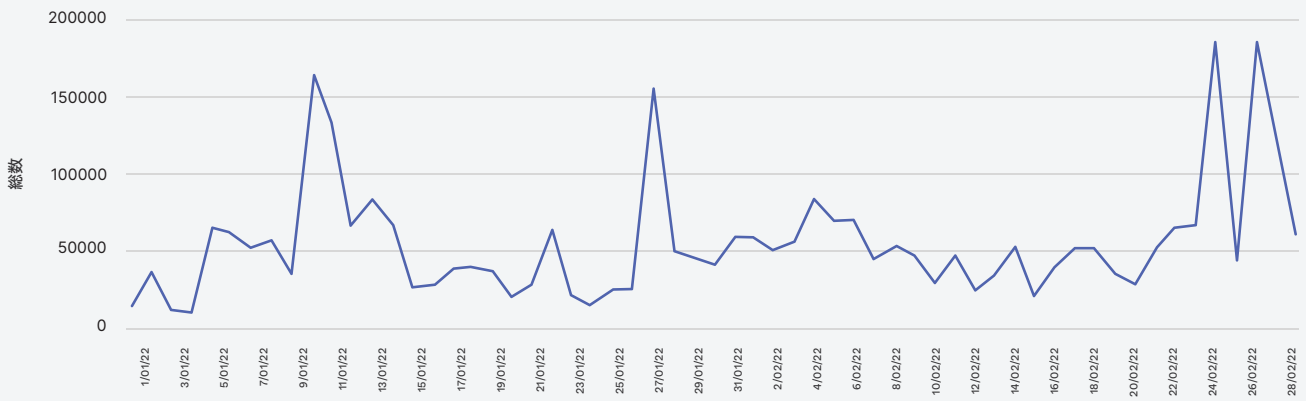


MFAバイパス攻撃

MFAとは「Multi-Factor Authentication」の略称で多要素認証を指します。現在、多くのWebブラウザはユーザー認証の維持やパスワード記憶の機能を実装していますが、これを悪用し、不正に窃取したセッションCookieなどにより多要素認証をバイパスする強力な攻撃です。

58%のアプリケーションが攻撃を経験

OktaのID管理プラットフォームを利用するすべてのお客様企業のアプリケーションの58%は、漏洩した認証情報を利用した攻撃を少なくとも1回は経験していることが報告されています。さらに25%のお客様企業は複数回にわたる攻撃を経験しています。
下のグラフでは5万回/日の検出件数がありますが、この大部分は実際のユーザーが漏洩したパスワードを再利用していることに起因して検出されており、実際の攻撃の割合は多くありません。一方、突出している箇所の大半は実際の攻撃であり、大規模な攻撃が何度も発生していることを示しています。



IDへの攻撃を防ぐための基本的な対策

- **MFAの採用**
  MFAは攻撃を阻止するもっとも効果的な方法の一つとなります。攻撃者はMFAを採用した企業への攻撃を躊躇し、ときには攻撃を中止する要因のひとつになりえます。
- **回数制限**
  ブルートフォース攻撃、クレデンシャルスタッフィング攻撃、パスワードスプレイング攻撃はログインの失敗が増加します。ログインの失敗回数を検出できるようにしましょう。
- **漏洩対策**
  ユーザーは複数のサイトで同一のパスワードを利用しがちです。漏洩したパスワードの利用を検出できるようにし、利用しようとしたユーザーに変更を促すことで、効果的な対処を行うことが可能になります。

OKTA
SPOTLIGHT
JAPAN

つなぐ
COOP
SAPPORO

28事業のシナジーを生み出すために Oktaの顧客ID管理製品で 認証システムを統合

Oktaの導入で実現できたこと

- 開発工数の削減とセキュリティの担保
- ECサイトとアプリの利用者数増加
- 問い合わせへのスピーディーな対応
- ログを活用したマーケティング分析
- 事業部ごとに独立していた認証の統合

ユーザビリティとセキュリティを 重視したDXを実現

年間3000億円規模の売上高を誇り、1万人以上の従業員と190万以上の組合員を抱える生活協同組合コープさっぽろ（以下、コープさっぽろ）は、2020年3月にデジタル推進本部を設置し、本格的なDX（デジタルトランスフォーメーション）に取り組んでいます。全国の生活協同組合の中でも非常に大きな組織であるコープさっぽろがDXに注力するのは、長年運用してきた古びたシステムや基盤を改善し、業務そのものや組織、プロセス、企業文化・風土を変革するため。"コープさっぽろがもっと使いやすく、買い物しやすく、働きやすく"を目指し、多彩なバックグラウンドを持つ優秀なIT人材を社外から招き入れ、デジタルの力で"レガシーな地方の巨大小売業"からの脱却を図っています。

そんなコープさっぽろでデジタル推進本部が真っ先に取り組んだのが、宅配システム「トドック」のECサイトおよびアプリのリニューアルです。トドックは、カタログから選んで注文したコープこだわりの商品を組合員の自宅まで届ける宅配サービス。2009年からはECサイトやアプリからもオンライン注文可能ですが、若年層に親しみにくいUI

やUX、システムの老朽化、セキュリティ面の改善、パスワード忘れへの対応などが求められていました。

「北海道は全国平均を上回る速さで高齢化が進んでおり、『自宅から半径500m以内に生鮮食品販売店がない』そして『自家用車も保有していない』という65歳以上人口が多くいます。そうした買い物弱者に向けて生活インフラを届ける役割をトドックが今後も担うためには、若年層を積極的に取り込む必要があります。一定の組合員数を維持し続けなければ、現在の週1回の配送無料宅配が困難になるかもしれないからです」（デジタル推進本部 システム部 樋口 修也 氏）

そこでコープさっぽろが導入したのが、Oktaの顧客ID管理製品「Okta Customer Identity Cloud」（以下、Okta CIC）です。2020年4月にトドックのECサイトやアプリのユーザー認証のために利用開始し、その後、セキュリティ面の考慮やログインの保持などにも活用。具体的には、UIやUXの改善に加えて、ブルートフォースアタックなどの攻撃に対応するためのセキュリティ機能や、パスワード忘れの問題を解決するためのSNS認証およびパスワードレス認証の実装を行いました。その結果、2019年からECサイト・アプリの利用者数は3年連続で増加し、2022年には利用率は3倍にも達しました。しかも、その間、起きたセキュリティインシデントの件数はゼロ。企業や事業の性質上、一度でも信頼を損なうことができない中、Okta CICによってユーザビリティとセキュリティを両立したDXを実現したのです。

認証システムを一新した「トドック」のアプリ

“グローバルでNo.1の製品を選ぶことを ポリシーとしているので、 必然的にOkta CICにたどり着きました”

生活共同組合コープさっぽろ 最高情報責任者 CIO／ デュアルカナム株式会社　取締役社長 **長谷川 秀樹** 氏

「グローバルでNo.1」を選ぶことがポリシー

ECサイトやアプリへ認証・認可の機能を組み込むことは自社開発でも可能ですが、コープさっぽろではそれを選択しませんでした。

「今はデジタルの世界ですから、その中でサービスを提供しようとすると、ログインをどうするかという問題が多くの企業の悩み事として立ちはだかります。そうしたとき、各企業でスクラッチで作っている場合ではないというのが私の考えです。企業内で構築するとエンジニアの力量によってセキュリティの度合いが決定されてしまいますが、専用のソリューションであれば自社開発をしなくても機能が追加され、最新のセキュリティに対応してくれます。ですから『安全を買う』という意味で、グローバルで定評のある製品を探していたのです」（最高情報責任者 CIO 長谷川 秀樹 氏）

そして、数あるソリューションの中から、「グローバルでNo.1」という理由で、Okta CICを選びました。

「企業がサービスを導入する際には、いろいろな製品を比較検討すると思います。そこで私が重要視しているのは、その業界、そのカテゴリのNo.1の製品を選ぶことです。もちろんNo.1の製品でなくてもパンフレットや説明資料には同じことが書いてあるかもしれませんし、お抱えのベンダーが同様のソリューションを提案してくることもあるでしょう。しかし、それらを選ぶ理由はどこにあるのでしょうか。クラウドでいえば『AWS』のように、グローバルで一番使われていて、一番セキュリティが高くて、一番使いやすい製品を選んだほうがいい。グローバルで打ち勝っている製品というのは、それだけセキュリティアタックを受けていて、それだけソフトウェアアップデートをしているということなのですから。常にグローバルでNo.1の製品を選ぶこと

をポリシーとしているので、必然的にOkta CICにたどり着きました」（長谷川氏）

パフォーマンスを引き出す充実したリソース

Okta CICで実際に認証システムを開発するにあたり、コープさっぽろがもっとも大きなメリットとして感じたのは、国際基準の品質のよい認証システムを素早く構築できる点です。

「認可フレームワークである『OAuth 2.0』に準拠した認証システムをいちから自社構築すると、要件定義や設計、開発、テストで3ヵ月はかかると思います。一方で、Okta CICであればOAuth 2.0に準拠した形で、1週間で作成することができました。OAuth 2.0を理解してコードに落とし込むにはエンジニアの能力がかなり必要となりますが、Okta CICであればOAuth 2.0に準拠した認証の仕組みの作り方がドキュメントになっているので簡単に構築できます」（樋口氏）

また、組合員の方々に出資をしてもらうことでサービスを運営しているコープさっぽろでは、まさに銀行に似たような形でセンシティブな情報を取り扱う必要があることから、迅速に開発した認証システムが"運用実績のある安全な仕様でセキュリティ担保された形である"という信頼性も重要だったと言います。

“Okta CICのメリットは
国際基準のセキュリティ品質を担保した認証システムを
簡単に開発できることです”

生活共同組合コープさっぽろ デジタル推進本部
システム部　**樋口 修也** 氏

リソースが充実しているから使いやすい

「たとえば、"身に覚えのない注文がある"という問い合わせを受けたとき、通常はまず不正ログインを疑いますが、Okta CICであればセキュリティはしっかりとしているのでその可能性は低いと判断でき、それ以外のことから調査を開始できます。また、たとえば"ログインできない"という問い合わせがあった場合も、管理コンソールから詳細なログを確認できますし、GUIで操作できるのでエンジニアではない人も対応に当たれます。運用の観点からいくと、管理コンソールがあることは非常に大きいと思います」（樋口氏）

加えて、ドキュメントやサポートが充実していることも大きなメリットだと言います。

「コープさっぽろに来て初めてOkta CICを使ったのですが、問い合わせ対応やシステムの不具合を回収する際に、日本語のドキュメントがしっかりしていて、とても使いやすく感じました。たとえばAPIを叩いて情報を取得しなければならない場合、ドキュメントにそのやり方が記載されているので、それを参照しながら簡単に解決できます。また、たとえドキュメントに載っていなくても、サポートに問い合わせたり、ユーザーコミュニティのフォーラムの情報を参照したりすればすぐに解決のためのヒントが得られます。製品がいくらよくても、使い方がわからなかったらパフォーマンスは出せません。ですから、パフォーマンスを出すための充実したリソースがあることはOkta CICの大きなメリットだと思います」（デジタル推進本部 システム部 和泉 僚 氏）

“Okta CICはドキュメントやサポート、
フォーラムがとても充実しているので、
やりたいことをすぐに参照して実践できます”

生活共同組合コープさっぽろ デジタル推進本部
システム部　**和泉 僚** 氏

一度のログインで複数事業へ連携できるシステムを構築

自社サービスの入り口となるユーザーのログイン画面。ともすれば、企業によって軽視しがちな認証基盤の構築をコープさっぽろが重視するのは、認証こそがすべてのオンラインサービスの始まりだからです。「"誰であるか"の認証さえ担保してしまえば、決済の機能を追加するなど、WEBでできることが格段に増えていきます。逆にいえば、認証ができていないとユーザーに対して何も価値提供できないのです」（樋口氏）

コープさっぽろでは、開発工数の削減によって創出された時間を、カテゴリ機能や通知機能を実装するなどのWEBサイトやアプリの機能強化に費しています。また、Okta CICの管理コンソールを使えばログイン人数や注文情報をCSVで書き出して集計できるので、マーケティング分析にも役立てています。

「新しい機能を実装したときにユーザー離れがないかなどの調査に利用したり、新たなマーケティング戦略を行った際に顧客単価を割り出し、PDCAのチェックの部分に活用しています」（和泉氏）

そして、今後は、Okta CICで構築した認証システムをトドックのECサイトやアプリにとどめるのではなく、さらに広げていく予定です。

「コープさっぽろでは電力や店舗、宅配、給食といった28の事業を展開しており、さまざまなECサイトが存在します。これまでのように各事業部でサービスの認証情報を持っているとセキュリティのリスクがありますし、利用者の利便性もよくありません。各サービスに個別にログインするのではなく、一度だけログインすればすべてのサービスにアクセスできる環境を構築したいと考えています」（樋口氏）

Okta CICを用いて認証を統合することで、28事業のシナジーを生み出す。これこそが、コープさっぽろでOktaを導入した真の目的です。そして、それを実現するために、コープさっぽろは組織構造の形をも変えました。これまで事業部ごとに独立してシステム構築していた環境から、デジタル推進本部がすべての事業部のハブとなり、デジタル（D）で事業の横串（X）を刺して、ユーザーに最適化された開発を行う環境へ。コープさっぽろが目指すDXは、一歩ずつ着実に前へ前へと進んでいるのです。

認証の統合で28事業のシナジーを生み出す

OKTA
SPOTLIGHT
JAPAN

DNP

DNPがOkta導入で海外拠点のITインフラ整備の迅速化とガバナンス強化を実現

Okta導入で実現できたこと

- 海外拠点で活用するITインフラの整備
- 本社側でガバナンスを効かせつつ、現地側で柔軟に運用ができるようなシステム
- 新規ユーザー登録の運用管理負担を大幅に削減
- 従来のIDaaSからOktaへの移行
- SaaSアプリケーションの連携強化

海外拠点で活用するITインフラの標準化に取り組む

大日本印刷株式会社（DNP）は、1876（明治9）年の創業から数えると間もなく150周年になる長い歴史を誇る企業です。社名にあるとおり出版印刷を祖業としていますが、事業ビジョンに、独自の「P&I」（印刷と情報）の強みを活かした「P&Iイノベーション」を掲げ、現在では出版印刷・商業印刷に加えて、ICカード、セキュリティ関連ビジネス、包装、産業資材、電子部材などのエレクトロニクス分野まで幅広い事業を展開しています。国内事業だけでなく海外展開にも力を入れており、海外事業の売上比率は、現在で約20%を超える状況になっています。

このように海外事業を強化しているDNPですが、今後さらにグローバル化が進展していくことを考えた場合、海外拠点でいかに迅速に業務を開始できるか、ITインフラを含めた環境整備の迅速化が課題となっていました。そこで同社では、クラウドサービスを中心に海外拠点で活用するITインフラの標準化に取り組み、新たな海外拠点を設立する場合にもまずインターネット接続さえできれば迅速に業務ができる環境を整えました。その環境を構築するために必要なアイデンティティ管理基盤としてOktaが採用されました。

“OktaのHub & Spokeモデルを採用することにより、
本社側（Hub）が中央集権型で管理しながら現地側（Spoke）に権限を移譲できるほか、
現地で管理しているものを本社側でも把握できるようになりました”

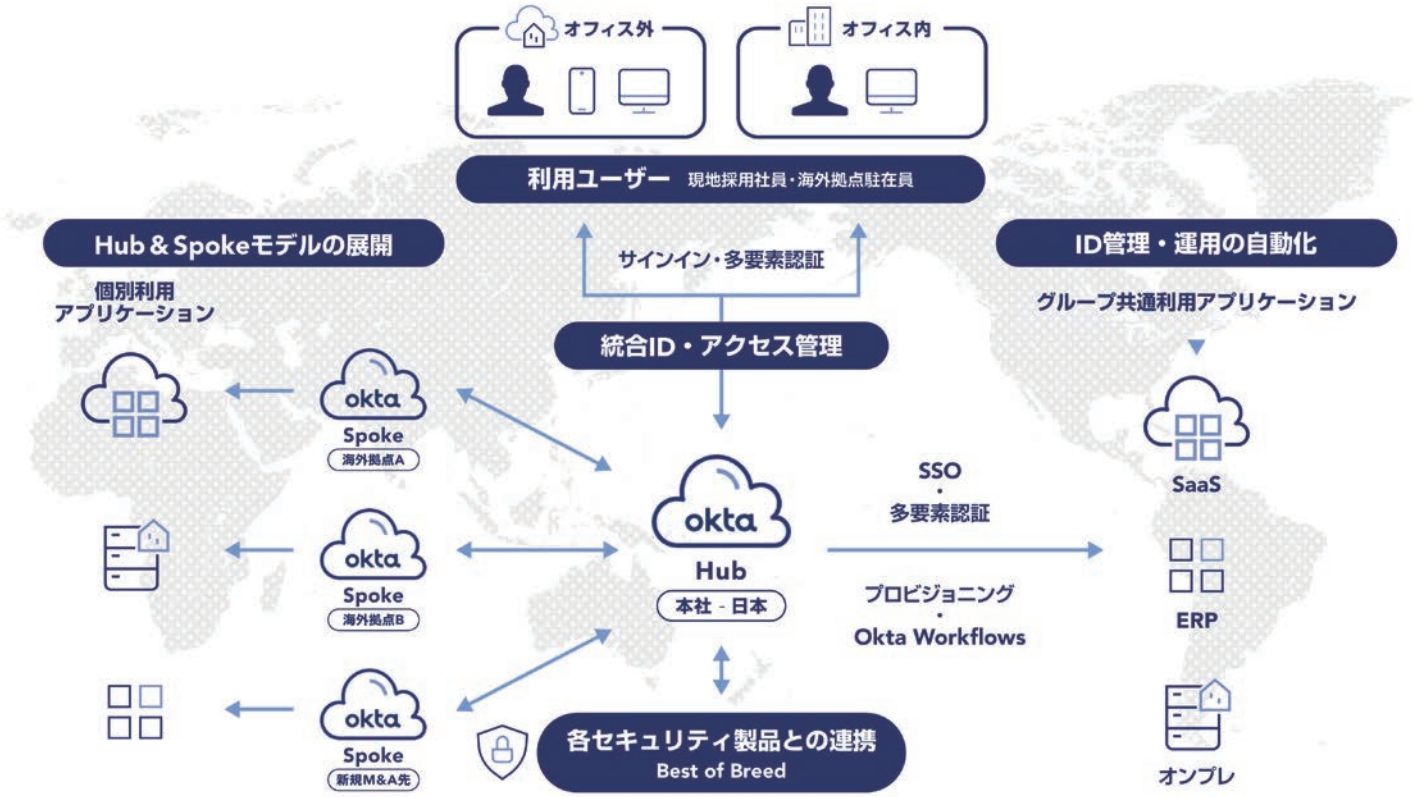
株式会社DNP情報システム　システム第3本部 グローバルICT推進部 第1課
課長　**本間 圭介** 氏

海外拠点のガバナンス強化の一環として共通プラットフォームを構築

DNPでは、セキュリティ強化、グループポリシー統一、グローバル経営の見える化などを目的として企画・パッケージ化し、海外拠点へ提供するシステムとして、「海外ICTインフラ（DGiPla：DNP Global ICT Platform、デジプラ）」を2017年から構築・展開しています。この取り組みの背景について同社の情報システム本部 本部長の宮本 和幸さんは「海外進出をそれなりにやってきていますが、すぐに業務を立ち上げたくても環境構築を個々にやっていては時間もコストも掛かってしまいます。そこで、共通したサービスを本社側で用意しておき、インターネットさえ接続できればすぐに海外拠点での業務を立ち上げられる環境がないと今後グローバル展開していくのは難しいと判断し、こうした構想を進めてきました」と語ります。

セキュリティ面でも、現在はランサムウェアを始めとして企業を対象としたサイバー攻撃が激化しており、攻撃手法も高度化しています。さらに、グローバルなサプライチェーンやネットワークの中で一番脆弱な場所が攻撃を受けた結果、全体が深刻な被害を被った例なども報道されている通り、グローバルに事業を展開する企業ではセキュリティ対策も現地任せにはできず、グローバルで一貫した高水準の防御態勢を構築する必要に迫られています。DNPのDGiPlaの取り組みは、まさにこうした昨今の状況を見越して構築されたものと言えます。

また、DNPでは海外拠点を含む基幹業務システムの共通化にも以前から着手しており、SaaS型ERPを海外拠点で共同利用できるような環境を構築していました。こうした取り組みも併せて、海外でのICT環境を各種SaaSなどを組み合わせて構築したプライベートクラウドのようなイメージの環境としてパッケージ化し、インターネット接続さえ準備すればすぐにグローバルで共通の業務環境が利用できる形にしたのがDGiPlaとなります。以前は、海外拠点に事務所



を設立することになっても、そこから業務ができるだけの環境を整えるのに何ヶ月もかかってしまうことがあったのが、現在では短期間で環境整備が完了するようになったと言います。

OktaのHub & Spokeモデルを採用

DNPの海外事業では、同社の事業分野の中でも生活・産業分野やエレクトロニクス分野の比率が高いと言います。DGiPlaのプロジェクトマネージャー役を務めた同社の情報システム本部 システム企画部 営業革新推進グループ リーダーの永田 智康さんは「食品の包装材や各種生活用品のパッケージ、生活空間で使われる壁紙や建具等の内装化粧材を手がけています。また、自動車の内外装に使われる加飾材や、エレクトロニクス分野では半導体の部品・部材となるものやスマホの画面に使われる材料などを製造していたりもします」と説明します。印刷技術の応用分野としての共通性がある一方、業種としても広範で、従業員の中にはITに対するリテラシーがそれほど高くない場合もあります。そのため、以前は何かITのトラブルがあった際には、現地ごとに異なる環境情報をその度に引きずり出してきて、どういう環境で業務を行っているのかを把握しながらリモートでサポートを行なうような状況で、IT部門としても大変な負荷の掛かるサポート作業を行なっていました。DGiPlaが構築されたことでこうしたサポートについても本社側にて一括で行なえるようになり、大幅な負担削減に繋がりました。

とはいえ、特にエレクトロニクス分野の海外拠点などでは現地のITリテラシーも高く、対応のスピードや柔軟性の観点からも現地側にある程度の管理権限を移譲したほうがよいところもあります。そのためには、本社側でガバナンスを効かせつつ、現地側でIT担当が柔軟に運用できるようなシステムが必要になります。実は、当初のDGiPlaでは他社のIDaaSソリューションが使われていましたが、現地側への権限移譲の仕組みが備わっておらずDNPのニーズに合わなかったため、Oktaへの移行が検討されたという経緯がありました。DGiPlaの構築やOkta導入の実作業を担当した、DNPのグループ企業である株式会社DNP情報システムのシステム第3本

部 グローバルICT推進部 第1課 課長の本間 圭介さんは、「OktaのHub & Spokeモデルを採用することにより、本社側（Hub）が中央集権型で管理しながら現地側（Spoke）に権限を移譲できるほか、現地で管理しているものを本社側でも把握できるようになりました」と言います。さらに、「以前利用していたIDaaSでは多要素認証の機能は備わっていたものの、それを実装する作業のハードルが高かったところが、OktaではUIの画面で簡単に実装できました」と説明します。

Okta導入で運用管理負担を大幅に削減

Oktaの導入効果として、本間さんは「以前のIDaaSでは、新規ユーザーの登録なども基本的には手作業で実施していましたが、Oktaではあらかじめ用意しておいたCSVファイルからのインポートで一括で自動登録することが可能になりました」と、作業効率が大きく向上したことを指摘します。従来は、一人の登録作業に10分以上かかっていましたが、Okta導入による自動化により数分で登録を完了でき、運用管理の負担を大幅に削減できるようになりました。さらに「今後はOktaのWorkflows機能を活用し、各拠点から申請が上がってきたら、そこから承認プロセスを回して自動的にユーザー登録までが完了するような形にしていくことも考えています」と語ります。

大きなメリットが生まれたOktaへの移行ですが、ゼロからの新規導入とは異なり、既存のIDaaSからOktaに切り替える際に空白期間やトラブルが生じないように準備する必要がありました。永田さんはこの点に関して、「導入の検討を開始したのが2021年10月頃で、その後2022年1月末にOktaの導入を決定し、2022年5月に全拠点での展開を行ないました」と説明します。実運用中のシステムで、700名以上のユーザーの認証情報を一気に切り替えるというプロジェクトとなり、失敗すれば業務停止等の重大トラブルに繋がる可能性もありました。しかも、導入時期はちょうどコロナ禍の時期とも重なってしまったため、海外拠点に日本から直接出向くことはできず、すべての作業を日本からリモートで実施せざるを得ないという状況でしたが、Okta側からも検証環境の提供などを行ない、国内の環境との違いを踏まえた連携の確認など、事前の準備をしっかり取り組んだことで特にトラブルもなく、約3ヶ月間でスムーズに移行を成功させることが出来たと言います。

移行後のDGiPlaは、認証・認可の基盤となるOktaが入口に置かれ、さらにゼロトラストアーキテクチャに基づくセキュリティサービスとなるZscalerを経由して各種のSaaSアプリケーションを利用する形で構成されています。標準的なアプリケーションについてはパッケージとして含まれていますが、さまざまなアプリケーションと連携しやすいOktaを活用して、今後は特定の国や拠点で使われているSaaSなどもOktaと連携させて組み込んでいくことも計画中だと言います。具体的には、現地で利用しているKintoneなどもOktaと連携させていくことが検討されています。また、セキュリティに関しても今後も継続的に強化していく予定で、たとえば現状のエンドポイントセキュリティの仕組みに加えてさらにEDRを導入し、Oktaと連携させてより強固なエンドポイントセキュリティを実現することや、海外拠点で使うアプリケーションのガバナンスを強化していくことで、シャドーITをなくしていくことが検討されています。

現在はビジネスにおけるIT活用が重要性を高めていく一方で、ICTに詳しくない企業が迅速に環境整備を行なえるようにするための支援体制や、そうした企業がサイバー攻撃に遭って深刻な被害を受けてしまわないような防御態勢の構築など、検討課題も増えています。新たにグループに加わった海外拠点に共通化されたセキュアなICTサービスとしてパッケージ化して提供することで環境整備を迅速化し、かつ高水準なセキュリティを担保するDNPの取り組みは、多くの企業にとって参考になる優れた取り組みと言えるでしょう。

Thank You

本誌をお読み頂き、ありがとうございました。

本誌の内容に関するお問合せやご要望は

IdentitySpotlight@okta.com 宛てにご連絡ください。

その他のご質問については、

以下の二次元コード先にあるフォームよりお問合せください。