Press Release

2022年11月10日
Okta Japan株式会社

報道関係者各位

【抄訳】Okta、企業のワークフォースアイデンティティ管理の統合ソリューション「Okta Workforce Identity Cloud」を発表

フィッシング対策機能を備え、ガバナンスと特権アクセス機能を強化した統合ソリューション

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であるOkta, Inc.（本社：米国・サンフランシスコ 以下Okta）は、本日Oktane22において、企業のワークフォース（従業員など）向けアイデンティティ管理の統合ソリューション「Okta Workforce Identity Cloud」を発表しました。この統合ソリューションには、様々なユーザーやリソースに対するフィッシング対策機能や、エンドユーザーやIT管理者が使いやすい統合アクセス管理、ガバナンス、特権アクセス機能が含まれます。

今日の企業のワークフォースは、従業員、請負業者、ビジネスパートナーで構成され、オンプレミス、クラウド、ハイブリッド環境のテクノロジーを業務で活用しています。複雑かつ急速に変化するテクノロジーのエコシステムにおいて、アイデンティティは、社員と、社員が仕事をするために必要なテクノロジーのエコシステム間をつなぐ重要な役割を担っています。ベライゾンの「2022年度データ漏洩/侵害調査報告書」によると、ソーシャルエンジニアリングによるデータ侵害の60%以上が認証情報の乱用に起因しており、特にフィッシングは今後も最も緊急な問題の1つとなっています。企業における異種混在環境が進む中、企業はアイデンティティを狙った脅威の増加から従業員、サードパーティ、重要なインフラを保護するために、統合されたアイデンティティのアプローチを必要としています。

OktaのWorkforce Identity担当プレジデント兼最高開発責任者のSagnik Nandyは、次のように述べています。「Oktaは、企業の保護に加え、あらゆるデバイスや場所からアクセスするすべてのユーザーに素晴らしい体験を提供することを容易にします。そのためには、今日の幅広いテクノロジーのエコシステムにおいて相互運用性を実現するだけでなく、技術スタックやユースケースに関係なく、業務展開の迅速姓とITの生産性を維持するシンプルさと包括性を提供するアイデンティティ基盤が必要です。Okta Workforce Identity Cloudは、アイデンティティ市場のこれまでサイロ化されていたレガシーソリューションを統合し、アイデンティティを企業の成長ドライバーとする、一貫性のある総合的なソリューションにします。」

Kyndrylの最高情報セキュリティ責任者であるCory Musselman氏は、次のように述べています。「Kyndrylは、世界が日々依存している基幹業務システムの設計、構築、管理、モダナイゼーションを行なっています。この仕事を推進するためには、チームの迅速な動きとシステムの安全性が必要です。Oktaの統合アイデンティティソリューションは、当社のIT資産とグローバル社員のアクセスとガバナンスをシンプルかつ安全に行うために大きな役割を担っています。すべての社員とリソースに手が届くことで、Kyndrylの事業は常に加速しています。」

フィッシング対策認証と脅威への対応で、企業と接するあらゆる人々を保護
数多くの著名なサイバーセキュリティ侵害が示すように、今日の企業は常に攻撃にさらされており、企業を構成する従業員、契約社員、パートナー、ベンダーを含むあらゆる人々が主要なターゲットとなっています。今回、Oktaは、認証情報を狙ったフィッシングから、様々なデバイスを使うあらゆるユーザーを保護するセ

キュリティ機能をOkta Workforce Identity Cloud向けに提供します。Okta Workforce Identity Cloudの独立性と中立性により、お客様は、異種混在環境の端末やオペレーティングシステムから企業リソースにアクセスするワークフォースユーザーのエコシステム全体にフィッシング対策を適応できます。

企業は、以下の新しいセキュリティ機能により、フィッシングやサードパーティの脆弱性に対抗できます。

- **Okta FastPass**のための高度なフィッシング耐性アクセス機能：MacOS、Windows、Android OSのすべての管理対象デバイスと非管理対象デバイスにフィッシング防止機能を提供します。
- **WebAuthn Allow List**：WebAuthnの登録を特定の組織が発行したハードウェアキーに限定することで、フィッシングの試みを防ぐことができます。
- **Passkey Management**：Passkey（パスキー）のようなマルチデバイス対応FIDO認証資格情報（マルチデバイスFIDOクレデンシャル）でユーザーが登録できないようにし、管理されていない安全でないデバイスが機密性の高いアプリケーションにアクセスする潜在的なリスクを事前に回避します。
- 非管理対象デバイスの**Security Checks**を新たに強化：セキュリティチームがアプリケーションやデータにアクセスしようとするデバイスをより深く理解できるようになり、全てのワークフォースやサプライチェーン全体にわたって組織のゼロトラストセキュリティイニシアチブを実現します。

この最新のフィッシング対策機能は、Oktaのノーコード自動化ツールであるOkta Workflowsの新しいセキュリティユースケースによって、さらにサポートされます。企業はOkta Workflowsを活用することで、フィッシングのブロックなどのセキュリティ事象が発生した後に、セキュリティ対応を自動化し、予防措置として追加のセキュリティアクションを有効にすることができます。Okta Workflowsは、アイデンティティアクションの自動化に特化して設計されており、新しいユースケースにより、アイデンティティとセキュリティに基づく自動化の課題を解決し、サードパーティの組織、ユーザー、デバイスのリスクを軽減する、よりシンプルな方法をユーザーに提供します。

Okta Workflowsのユーザーは、以下の機能を使って、新しいセキュリティ自動化対応ができます。

- **Security Templates**：組織にリスクをもたらすユーザー行動の変化の特定、組織のセキュリティ態勢の継続的な監視と改善、アイデンティティレイヤーでのセキュリティポリシー施行の完全自動化など、チームが事前対策を講じるための機能を提供します。
- **Connector Builder**：Okta Workflows のノーコードデザイナーを使用して、コードを使用せずに新しいコネクタの構築を簡素化します。技術ベンダーは、Connector Builder を使用して顧客向けのコネクタを作成でき、管理者はカスタムツールを簡単に接続できます。

Recorded Futureの最高製品・エンジニアリング責任者であるCraig Adams氏は、次のように述べています。「Recoded Futureは、脅威から人々やインフラを安全に保つために、適切なタイミングで適切なインテリジェンスを企業に提供します。アイデンティティを狙った攻撃は増加傾向にあり、MFAでは十分ではありません。Recorded Futureの『Identity Intelligence connector for Okta Workflows』は、MFAを超えるもので、暴露された認証情報が攻撃に使われる前に、侵害されたアイデンティティ（MFAを回避できるものを含む）の自動化された可視性をお客様に提供します。」

Okta Workforce Identity Cloudの脅威防止と自動対応機能の詳細は、こちらをご覧ください：
https://www.okta.com/blog/2022/11/heres-how-to-prevent-phishing-in-a-heterogeneous-workforce/

ユーザーに必要な時のみにアクセス提供を管理する、包括的なガバナンス管理

Okta Identity Governanceは、エンドユーザーがどこにいてもニーズに合わせて、リソースへのアクセスを申請・承認するプロセスを簡素化します。Okta Identity Governanceは、Oktaのクラウドネイティブテクノロジーをベースにしたokta Workforce Identity Cloudに統合されており、ITチームやエンドユーザーにとって使いやすく、組織のセキュリティとコンプライアンス体制を向上させることができます。新しいイベントベースの認証（棚卸し）は、アイデンティティのガバナンスとアクセス管理に対するOktaの統一されたアプローチを活用し、組織の幅広いワークフォースに対してコンテキストに沿ったガバナンス機能を提供するためにプラットフォーム全体でシグナルを共有することができ、最終的にビジネスの安全性とコンプライアンスを維持します。

イノベーションを減速させずにすべてのリソースを安全に保つ、統合された特権アクセス
Okta Privileged Accessは、Okta Advanced Server Accessのインフラアクセス機能をベースに、特権管理者アクセスに必要なセキュリティとコンプライアンスのレイヤーを追加して構築されています。Okta Privileged Accessは、パスワードの自動ローテーションや共有アカウントへのアクセスに対する個人のアカウンタビリティを提供するOktaのVaultingサービスを使って、管理者やルートアカウントの高権限の認証情報を保護することが可能になります。また、Oktaのお客様は、Okta Privileged Accessを利用して、Oktaが管理するインフラに対する特権アクセスリクエストと承認の管理、監査やコンプライアンス要件を満たすための特権エンタイトルメントレポートの作成が可能になります。Okta Privileged Accessは、特権付きリソースのセキュリティ強化、特権付きアクセスの監視と記録、監査人向けの詳細なコンプライアンスレポートの実行に必要なツールを提供します。

Okta Privileged Accessの主な新機能は以下の通りです。

- **Credential Vaulting**：ローカルユーザーアカウントと人間が管理する共有クレデンシャル保管とローテーションを提供し、人間、マシン、アプリケーションユーザーに対してジャストインタイム（JIT）アクセスリクエストと承認ワークフローを提供し、恒久的にアクセス可能な状態とすることを回避します。
- **Privileged Governance and Compliance**：特権アクセスレポートの生成とセッション管理機能の追加により、監査証跡を作成して不要な行動を検出・防止し、コンプライアンスの証明に役立てることができます。
- **Modern Infrastructure Access Management**：Kubernetes、Linux、Windowsサーバーなどの最新インフラ向けに、短時間のみ有効な証明書ベースの認証によるパスワードレスアクセス管理を提供します。

アイデンティティ管理を単一のコントロールプレーンに統合
Okta Workforce Identity Cloudは、Okta Identity GovernanceとOkta Privileged AccessをOktaのコアであるIAMテクノロジーと統合し、すべてのアイデンティティの全体的な可視性と制御を実現します。これらのコンポーネントを組み合わせることで、セキュリティやユーザーエクスペリエンスを犠牲にすることなく、IT部門に権限と制御を委ねることができます。また、この統合ソリューションにより、ワークフォースは複数のインタフェースをわたり歩く必要がなくなり、新たな俊敏性を得ることができます。また、サイロ化したアイデンティティシステムを統合する必要がないため、ITの効率も向上します。

Oktaの統合アイデンティティプラットフォームのアプローチにより、企業は以下を実現できます。

- **IAM、Okta Identity Governance、Okta Privileged Access**にわたるプロセスの自動化：複数のアイデンティティソリューションを、コードやAPIを使用することなく、短期間で単一のプラットフォームに統合します。
- アイデンティティのサイロ化を解消：アイデンティティのサイロ化を解消し、エンドツーエンドのガバナンスとアクセス管理を提供することにより、セキュリティとコンプライアンスの成果を向上させます。

- エンタープライズアイデンティティの管理を合理化：あらゆるリソース、あらゆるレベルのユーザー、あらゆる権限のアクセスとエンタイトルメントの管理を強化します。

Okta Workforce Identity Cloud の統合ソリューションの詳細は、こちらをご覧ください：
https://www.okta.com/blog/2022/11/new-with-oktas-workforce-identity-cloud-a-unified-identity-solution/

提供開始について

- フィッシング耐性が強化されたOkta FastPassは、2023年第1四半期に一般提供開始となる予定です。
- WebAuthn Allow Listは2023年第1四半期にMFAとAdaptive MFAからアーリーアクセスとなる予定です。
- Passkey Managementは、現在アーリーアクセス中で、MFAとAdaptive MFAから利用できるようになる予定です。
- 新たに強化された非管理対象デバイスのSecurity Checksは、Adaptive MFAを通じて、一般提供を開始しました。
- Okta WorkflowsのSecurity Templatesは一般提供を開始しました。
- Okta WorkflowsのConnector Builderは、2023年第1四半期に一般提供する予定です。
- Okta Identity Governanceは、本日より北米のみで一般提供開始となり、2022年第4四半期にはスタンドアロン製品として全世界で一般提供する予定です。
- Okta Privileged Accessは、2023年第2四半期にアーリーアクセスとなり、2023年第4四半期にスタンドアロン製品として一般提供する予定です。

本リリースで言及されている、現在利用できない製品、特性または機能は、予定通りに、またはまったく提供されない可能性があります。製品ロードマップは、いかなる製品、特性または機能の提供に対するコミットメント、義務または約束を表すものではなく、お客様は購入を決定するためにこれらに依拠するべきではありません。

Oktaのすべての製品発表はOktane22.comでご覧ください。
https://www.okta.com/oktane22/

Oktaについて
Okta は、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、あらゆる人があらゆる場所で、あらゆるデバイスやアプリで、あらゆるテクノロジーを安全に利用できるようにします。最も信頼されているブランド企業は、Oktaを信頼して安全なアクセス、認証、自動化を実現しています。OktaのWorkforce Identity CloudsとCustomer Identity Cloudsの中核には柔軟性と中立性があり、ビジネスリーダーや開発者はカスタマイズ可能なソリューションと7,400以上のアプリケーションとの事前統合により、イノベーションに集中し、デジタル変革を加速させることができます。私たちは、アイデンティティがお客様のものである世界を構築しています。詳しくは以下をご覧ください。
https://www.okta.com/jp/

【本件に関するお問い合わせ先】
■ Okta Japan株式会社
広報担当：中田清光
Email: kiyomitsu.nakata@okta.com
■Okta PR 事務局（株式会社プラップジャパン内） 担当：山本・中根・冨安・藤沢

TEL: 080-9821-6995（山本携帯）、080-6859-3639（中根携帯）
Email: okta@prap.co.jp