ホワイトペーパー

Okta Secure Identity Commitment

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を提供する

企業インフラを強化する

お客様のベストプラクティスを推進し、お客様を確実に保護する

アイデンティティ攻撃から守るために業界の知識を向上させる

okta

目次

エグゼクティブサマリー

アイデンティティは、すべての従業員向けおよび消費者向けアプリケーションのための、企業の主要なセキュリティの入り口です。一方、大小を問わず、企業に対する攻撃の量と複雑さは加速し続けています。これらの攻撃を検知し保護することはミッションクリティカルです。

世界をリードする独立系アイデンティティ企業として、Oktaはアイデンティティ攻撃との戦いにおける最前線にいます。その結果として、当社は今後の取り組みを掲げた「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を提供する
- 企業インフラを強化する
- お客様のベストプラクティスを推進し、お客様を確実に保護する
- アイデンティティ攻撃から守るために業界の知識を向上させる

この取り組みの一環として、当社は企業インフラと製品ポートフォリオの両方において、多くの重要な機能とアップグレードを提供し、発表してきました。 これらのアップデートのサマリーについては下記に詳しく説明しています。

私たちの仕事に終わりはありません。そして、ダイナミックなサイバー脅威の状況を先取りし、それに対応するために、必要に応じて投資を続けていきます。

はじめに

2009年にOktaを設立した当時、私たちは主にIT管理、そして特に、人々とテクノロジーをつなぐ手段としてアイデンティティを利用することに集中して取り組んでいました。

それ以降、2つの大きなトレンドが、アイデンティティのとらえ方と、アイデンティティソリューションの需要に劇的な変化をもたらしてきました。

1. **アイデンティティは、今やすべての従業員および消費者向けアプリケーションのための主要なエンタープライズセキュリティの入り口**です
2. **サイバー攻撃の量と複雑さは増大しており、**ランサムウェアグループ、国家的脅威アクター、悪意のある内部関係者など、さまざまな攻撃者が、防御を迂回し、検知を回避するための高度な戦術、技術、手順 (TTP) を開発しています

このようなトレンドは、業界に大きな変化をもたらしており、それによって当社に課された責任は人々をテクノロジーでつなぐことから、あらゆる組織の重要なデータを保護するための重要な入り口としての役割を果たすことへと進化しています。

すべての人があらゆるテクノロジーを安全に利用できるようにするという、私たちのビジョンにおいて、この責任を認識しています。

Okta Secure Identity Commitment

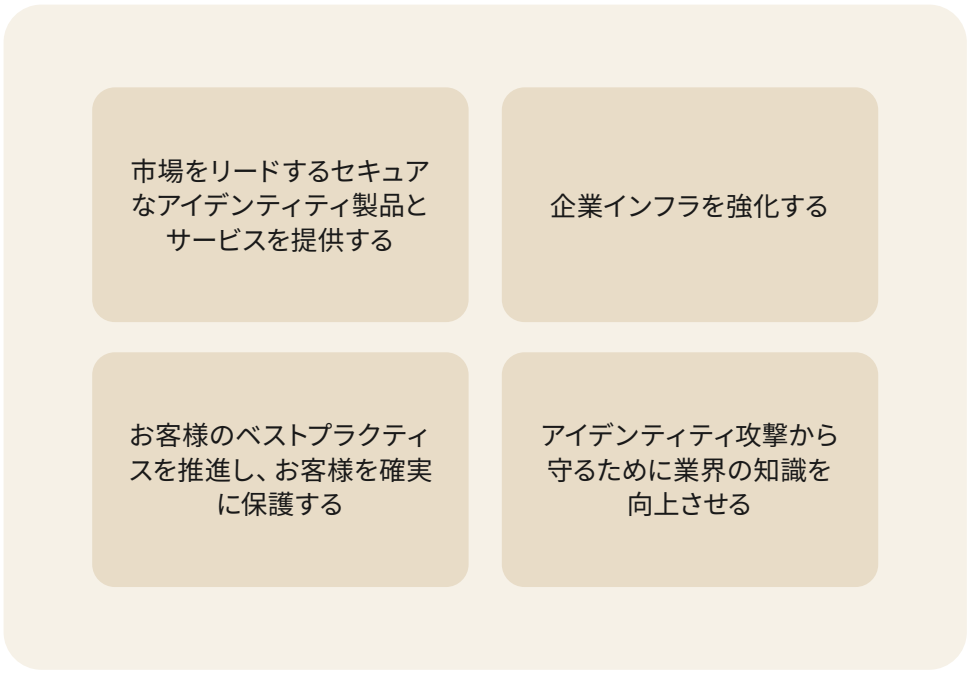
アイデンティティはミッションクリティカルなセキュリティインフラとなっています。

Oktaは、世界をリードする独立系アイデンティティ企業として、アイデンティティ攻撃との戦いにおける最前線にいます。当社の製品、エンジニアリング、セキュリティ、ビジネステクノロジーのチームは、18,000社以上におよぶお客様を保護するために、当社のテクノロジープラットフォームを革新し続けています。以下がその例です。

- Okta ThreatInsightは、30日間以内に20億以上の悪意のある要求を検知し防ぎました(出典：Okta社内ソース - 2024年1月)
- 当社では、90日間にわたり、一部の大手顧客において、クレデンシャルスタッフィングの試行と悪質なボットトラフィックを90%以上削減しました（出典：OktaのThe State of Secure Identity Report 2023)
- 当社は業界のベストプラクティスを形成しています。 Oktaの従業員の100%がフィッシング耐性の要素として、Okta FastPassとAdaptive MFA (AMFA)を使用しています（出典：Okta社内ソース - 2024年2月)

当社はアイデンティティ攻撃との戦いにおいて、業界をリードすることに全力を注いでいます。その結果として、当社は、Okta Secure Identity Commitmentを発表しました。

このコミットメントは4つの柱に基づいています：



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を提供する

当社のセキュリティ態勢がお客様のセキュリティ態勢であると認識し、アイデンティティ製品とサービスにおけるセキュリティ機能の向上と優先度を高めることに取り組んでいます。

このような継続的な取り組みを通じて、世界的に認知されたブランドからの信頼に応えるべく、最も強力かつ革新的な保護手段を提供してまいります。

企業インフラを強化する

社内のすべての人、プロセス、テクノロジーを、お客様向けの製品と同じ厳格なセキュリティ基準で管理し、セキュリティに対する包括的なアプローチを重視しています。

さらに、周辺システム（例：本番環境に隣接したシステム）や企業システムをさらに強化するための投資を加速させています。

お客様のベストプラクティスを推進し、お客様を確実に保護する

誤って設定されたアイデンティティは、攻撃者や悪意ある内部関係者にとって、新たな入り口となります。15年以上の経験と18,000社以上のお客様を持つOktaには、お客様が適切なアイデンティティの設定を行うための、独自の専門知識があります。

当社の豊富な経験をお客様に活用していただくため、私たちは顧客ポリシーをより強化しています。

さらに、当社製品をOktaのセキュリティにおけるベストプラクティスに基づいて導入することで、アイデンティティ関連の侵害に対するお客様の防御を強化できるように取り組みます。

アイデンティティ攻撃から守るために業界の知識を向上させる

アイデンティティのセキュリティをリードすることは、Oktaにとって必須です。当社は、業界におけるアイデンティティ攻撃の検知と軽減の支援に注力します。そのために、当社の能力をさらに向上させ、AIなどの新しいテクノロジーを取り入れてまいります。また、アイデンティティセキュリティに対する業界のアプローチを形成する上で当社は積極的な役割を果たしてまいります。これには、非営利団体のデジタル変革への資金提供やテクノロジー分野への包括的な進路を促進するOkta for Goodの支援も含まれます。

本文書の残りの部分では、当社がどのようにコミットメントを実現しているかを説明します。

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を提供する

Oktane 2023では、Okta AIを活用した機能など、数多くのセキュリティ強化機能発表しました。

今後、私たちがどのように製品とサービスを強化していくかにあたり、以下のようないくつかの重要なテーマがあります。

- Okta Orgにおける管理者アクセスの強化
- セッションセキュリティの強化
- お客様基盤全体でセキュリティのベストプラクティスをサポート

最近提供されたもの	2024年2月に予定されている機能	2024年7月に予定されている機能
• Okta Privileged Access • エンタイトルメント管理 • Passkeys • Highly Regulated Identity • Okta Expert Assist • Spera買収 • Okta Help Centerでのケースアクセスの変更 • 管理セッションの認証 • 管理API - Okta APIの呼び出しには管理者セッションが必要 • その他	• Okta Admin ConsoleへのアクセスにMFAを要求 • Okta Admin Consoleで保護されたアクションにはMFAが必要 • 管理者があらゆるアノニマイザーからのリクエストを検出し、ブロック • Okta Admin ConsoleにIPバインディングを適用し、Okta Admin ConsoleにIPまたはASNバインディングを適用 • APIに対して許可リスト付きネットワークゾーンを施行 • Oktaの管理者ロールにZero Standing Privilegesを提供 • M2Mアプリケーションサービス統合のためのトークンバインディングの強制 • Oktaユーザーのアカウントロックアウトを防ぐ • 特権アクセス管理（PAM）にIPバインディングを適用 • その他	• Oktaアプリケーションのデバイスバインドセッションcookie • ボット検出の強化 • デフォルトCAPTCHAの強化 • セッション管理制御の拡張とトークンセキュリティの強化 • Okta Privileged Accessの保護されたリソースとして、SaaSやハイパースケーラのサービスアカウントを加速化 • FastPass登録を管理デバイスに制限 • 製品内ベストプラクティスガイドの拡充 • その他

最近発表/提供されたもの

お客様のセキュリティ強化のための最近の製品と、発売予定の機能には以下が含まれます。

- **Okta Privileged Access**は、お客様がゼロスタンディング権限を導入し、リスクを低減するのに役立ちます
- **エンタイトルメント管理**は、エンタイトルメントを自動的に検出し、適切なサイズに設定することで、設定ミスによる潜在的な脅威を低減します
- **Passkeys**は、消費者向けアプリにパスワード不要のセキュアなアクセスを提供します
- **Highly Regulated Identity**は、アイデンティティワークフローに、金融グレードのセキュリティを提供します
- **Okta Expert Assist**は、Oktaのセキュリティ専門知識でお客様のセキュリティ強化や設定を支援します
- **Spera買収**により、アイデンティティを活用したセキュリティが強化され、企業はリスクを削減し、断片化した企業ITとコストを削減することができます
- **Identity Threat Protection with Okta AI**は、近日中に早期アクセスを開始します。Universal Logout（例：お客様のエコシステム全体の脅威に対応）のような強力なアクションが含まれます

Okta Expert Assist

お客様はOktaと提携することで、セキュリティと全体的な設定を強化するための追加措置を講じることができます。

Okta Expert Assistサービスの利用方法をご紹介します。

1. **発見する：アイデンティティのセキュリティ専門家とのマッチング。** Oktaアーキテクトは、2週間にわたってOktaテナントの包括的なセキュリティレビュー（ワークショップ経由）を実施します。
2. **分析する：セキュリティ専門家が特定した実行可能な手順。** Oktaアーキテクトは、Okta製品の最新機能や脅威の進化を考慮したベストプラクティスに照らして、お客様の設定を総合的に検討します。
3. **計画する：現在、そして将来のセキュリティ態勢を強化。** Oktaアーキテクトは、お客様のセキュリティ態勢を改善し、増大するセキュリティ脅威に先手を打つために、優先順位付けされた実践的かつ具体的なガイダンスを提供します。

→ **詳細はこちら**: https://www.okta.com/expert-assist/

最近追加されたアップデートには以下が含まれます。

- **Okta Help Centerでのケースアクセスの変更：**Okta Help CenterでOktaサポートケースにアクセスできるのは、サポートケースを開いた管理者ユーザーのみです。
- **管理セッションの認証：**Okta Admin Consoleのデフォルトのタイムアウトは、セッションの有効期間が12時間、アイドル時間が15分に設定されます。お客様にはこれらの設定を編集するオプションがあります。
- **管理API - Okta APIの呼び出しには管理者セッションが必要：**Oktaがベストプラクティスとしてお勧めするのは、自動化またはTerraformでAPIコールを行う際にAPIトークンを使用することです。今回の製品変更により、これが実施され、お客様の管理者のセキュリティが向上します。

早期アクセスは2024年2月を予定：

- **Okta Admin ConsoleへのアクセスにMFAを要求：**すべてのOkta管理者ロールにMFAを必須にすることで、Okta Admin Consoleへの更に安全なアクセスへと改善します。Okta Admin ConsoleにMFAを施行し、侵害のリスクを軽減するためのキュリティレイヤーをもう1つ加えます。段階的なアプローチをとっており、最初の段階では、MFAなしで新しい管理アプリの認証ポリシーを作成できないようにしています。
- **Okta Admin Consoleで保護されたアクションにMFAが必要：**影響度の高いアクションを実行する管理者にステップアップ認証を要求することで、Oktaの重要なアクションをさらに保護します。
- **管理者があらゆるアノニマイザーからのリクエストを検出し、ブロック：**Oktaは、IPアドレスがアノニマイザーに関連付けられているかどうかの評価に基づいてアクセスを許可または拒否する機能を管理者に提供し、このようなソースからの不正アクセスに対する組織の制御を強化します。
- **Okta Admin ConsoleにIPバインディングを適用し、Okta Admin ConsoleにIPまたはASNバインディングを適用：**セッションの乗っ取りを防止するため、APIまたはWebリクエスト中に観測されたASN（Autonomous System Number）が、セッションの確立時に記録されたASNと異なる場合、Okta Admin Consoleのセッションを自動的に取り消します。お客様の管理者は、以下のOkta製品でアクティブなセッション中に観測されたIPアドレスが変更された場合、管理セッションを自動的に取り消すことができるようになります：Workflows Admin、Okta Access Requests（Inbox）、Okta Privileged Access (OPA)、Okta Admin Console.

- **APIに対する許可リスト付きネットワークゾーンの施行：**攻撃者やマルウェアがSSWSトークンを盗んだり、不正アクセスを行うために、指定されたIP範囲外で再生したりすることを制限します。
- **Oktaの管理者ロールにZero Standing Privilegesを提供：**Okta Identity Governance (OIG)で、Okta管理者ロールを管理します。Oktaは、管理者権限にアクセス要求と認証を要求することで、内部脅威や不正アクセスを軽減し、最小権限アクセスを可能にします。

*OIGのお客様には2024年2月に早期アクセス（EA）を開始し、3月にはより多くのお客様にEAを開始します。

2024年2月に一般提供を予定している機能：

- **M2Mアプリケーションサービス統合のためのトークンバインディングの強制：**Oktaは、認証されたアプリケーションのみがトークンを使用してOkta APIにアクセスできるようにするため、所有証明を使用したマシン間（M2M）統合におけるトークンバインディングをデフォルトで施行することで、自動トランザクションのセキュリティを強化します。
- **Oktaユーザーのアカウントロックアウトを防ぐ：**Oktaは、未知のデバイスからの不審なサインイン試行をブロックする機能を提供します。この機能を有効にすると、Oktaが知らない別のデバイスがロックアウトを引き起こした場合に、管理者を含む正当なユーザーがロックアウトされるのを防ぐことができます。
- **特権アクセス管理（PAM）にIPバインディングを適用：**お客様の管理者は、APIまたはWebリクエスト中に観察されたIPアドレスが、セッション確率時に記録されたIPアドレスと異なる場合、管理特権アクセス管理セッションを自動的に取り消すことができるようになります。この機能を無効にするには、サポートチケットが必要です。

2024年7月に予定されている機能：

- **Oktaアプリケーションのデバイスバインドのセッションクッキー：**デバイスバインドのセッションクッキーは、ユーザーデバイスに保存された秘密鍵の所有証明を要求することで、Oktaセッションの再生をさらに防止します。このチャレンジにより、セッションとデバイスの間に強い絆が生まれ、トークンの盗難やリプレイ攻撃のリスクを減らすことができます。
- **ボット検出の強化：**サードパーティのスコアやエッジベースのコンポーネントシグナルを使用して、ボット検知と保護を強化しています。
- **デフォルトCAPTCHAの強化：**デフォルトにより、Okta Customer Identity Cloud で CAPTCHA をトリガーするイベントは、観察されたリスクに比例した複雑さを用いて処理されます。
- **セッション管理制御の拡張とトークンセキュリティの強化：**セッションの完全なプログラム制御を提供することで、お客様が独自のセッション制御ダッシュボードを構築し、ユーザー体験をカスタマイズできるようにします。
- Okta Privileged Accessの保護されたリソースとして、**SaaSやハイパースケーラのサービスアカウントを加速化します。**
- **FastPass登録を管理デバイスに制限：**Oktaは、モバイルデバイス管理（MDM）ソリューションを使用して、Okta VerifyおよびFastPassへのユーザーの事前登録を可能にすることで、管理者に大きなコントロールを提供します。これにより、顧客は認証者の登録を管理対象デバイスに制限することができます。
- **製品内ベストプラクティスガイドの拡充：**Oktaは、お客様がOktaテナントを保護するためのベストプラクティスを実施するのに役立つ、更に多くの製品ガイドを提供する予定です。

企業インフラの強化

周辺システム（本番環境に隣接するシステム）と企業システムをさらに強固にするための投資を加速させています。

最近提供されたもの	2024年4月に予定されているアップデート	2024年7月に予定されているアップデート
• Google Chromeアカウントへの個人アクセスをすべて排除 • すべてのサービスアカウントの監視と検出のレベルを向上 • Okta Help Center内の機密データを検出しHARファイルをサニタイズ • ソースコード管理とデータベース監視の強化	• 従業員のライフサイクル全体にわたってフィッシング耐性を拡張 • SaaSアプリケーションにおけるM2Mサービスアカウントの発見と報告の自動化 • 内部セキュリティ評価の実施 • SaaSアプリケーションセキュリティアセスメントの実施	• 検知・対応能力の強化 • 脆弱性管理、資産管理、CSPMの標準化と一元化 • セキュリティリスク管理のために標準化され、一元化されたレポーティング • ノートパソコンの保護の強化 • モバイル機器保護の強化

最近提供されたもの：

Oktaの企業インフラに対する最近の変更、アップグレード、強化は以下の通りです：

- Google Chromeアカウントへの個人アクセスをすべて排除
- すべてのサービスアカウントの監視と検出のレベルを向上
- Okta Help Center内で機密データ（セッショントークンなど）を検出してHARファイルをサニタイズ
- ソースコード管理とデータベース監視の強化

2024年4月に予定されているアップデート：

- **従業員のライフサイクル全体にわたってフィッシング耐性を拡張：**当社は、フィッシング耐性のあるMFAとしてOkta FastPassを以前から導入しています。従業員の登録/入社から回復に至るまで、従業員のライフサイクル全体にわたってフィッシング耐性を実装します。
- **SaaSアプリケーションにおけるM2Mサービスアカウントの発見と報告の自動化：**SaaSアプリケーション内に作成されたローカルサービスアカウントを可視化するツールを導入し、認証に使用されるシークレットの管理とローテーションを改善します。
- **内部セキュリティ査定の実施：**Oktaは、世界有数のアドバイザリー会社と提携し、当社の製品、インフラ、企業システムの包括的なセキュリティレビューを実施しています。
- **SaaSアプリケーションセキュリティアセスメントの実施：**Oktaは、サードパーティのセキュリティ専門家と提携し、Okta Help Centerを含む重要なSaaSアプリケーションのセキュリティの査定を行っています。

2024年7月に予定されているアップデート：

- **検知・対応能力の強化：**新たなセキュリティインシデントケース管理ツール、新たな脅威インテリジェンスプラットフォーム、ダークウェブ監視機能の追加など、検知・対応能力を強化するソリューションを展開します。
- **脆弱性管理、資産管理、クラウドセキュリティポスチャ管理（CSPM）のための標準化・一元化されたレポーティング：**本番環境と企業環境にわたるすべての脆弱性関連情報を一元化するために、単一ベンダーのソリューションを導入します。
- **セキュリティリスク管理のために標準化され、一元化されたレポーティング：**単一のベンダーソリューションを導入することで、第三者リスク管理を含め、当社のガバナンス、リスク、コンプライアンスプログラムに関連するリスクおよび問題管理を一元化します。
- **ノートパソコンの保護の強化：**従業員によるOktaのノートパソコンの使用方法をさらに制限し、限定します。すべての社員からローカル管理者アクセスを削除しましたが、免除された開発者やエンジニアからもローカル管理者アクセスを削除する予定です。
- **モバイル機器の保護の強化：**モバイル機器のセキュリティに厳しい態度で臨んでいきます。Okta Verify製品はすでに、PIN、暗号化、オペレーティングシステムのバージョンチェックなど、機器のセキュリティ体制に関する保証を提供していますが、企業アプリケーションへのアクセスにはMDMソフトウェアが必要になります。

お客様のベストプラクティスを推進し、お客様を確実に保護する

業界のベストプラクティスを最適化し、脅威の状況に足並みを揃えています。

- **フィッシング耐性のある要素：**Okta従業員の100%がOkta FastPassとAdaptive MFAをフィッシング耐性の要素として使用しています。フィッシング耐性のある要素を、どのようにアイデンティティスタックに組み込むことができるか検討することを、お客様に推奨しています。
- **MFAエンロールメントとセルフサービス:**MFAの重要性を強化し、すべてのMFA登録（管理者＋ユーザー）に対するお客様の可視化と、セルフサービスによる登録機能の提供に注力しています。
- **お客様に合った専門家によるサポート：**お客様がOktaのセキュリティに関する専門知識を活用し、セキュリティと設定を強化できるよう、Okta Expert Assistを立ち上げました。ぜひ、これを活用し、お客様御社に合った推奨案を入手してください。
- **意識向上とトレーニング：**フィッシングに対する意識向上トレーニングを強化し、フィッシング耐性のある認証方法を導入しています。
- **製品内ベストプラクティスガイドの拡充：**Oktaは、お客様がOktaテナントを保護するためのベストプラクティスを実施するために、さらなる製品ガイドを提供する予定です。

アイデンティティ攻撃から守るために業界の知識を向上させる

サイバーセキュリティ業界の発展に向けたOkta for Goodの最近の取り組みには、以下があります：

- **NetHopeのグローバル人道的情報共有・分析センター**（ISAC）は、NetHope、USAID、Oktaの官民パートナーシップとして発足し、世界の人道的NGOが増大するサイバー脅威に対応できるよう支援しています。
- **Cybersecurity Futures 2030**、Oktaは、カリフォルニア大学バークレー校の長期サイバーセキュリティセンターおよび世界経済フォーラムのサイバーセキュリティセンターと共同で、このグローバルリサーチに資金を提供しました。その目的は、政府、産業界、市民社会が直面するサイバーセキュリティの新たなトレンドとリスクを特定し、これらの将来の課題に対処するための、より良い共同作業を可能にすることです
- **サイバーセキュリティ人材開発イニシアティブ**は、テクノロジーおよびサイバー業界への包括的な進路を促進し、業界のスキルギャップを解消するために、新たな慈善および教育助成金を提供します。
- **非営利団体のサイバーセキュリティ助成金ポートフォリオ**、2年間で100万ドル以上を拠出し、非営利団体のサイバーセキュリティ対策強化を支援

最後に

Oktaは、アイデンティティ攻撃との戦いにおいて業界をリードすることに取り組んでいます。その結果として、次の4つの柱に基づき、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を提供する
- 企業インフラを強化する
- お客様のベストプラクティスを推進し、お客様を確実に保護する
- アイデンティティ攻撃から守るために業界の知識を向上させる

これは長期的なコミットメントであり、私たちはテクノロジーや脅威の状況とともに進化し続けてまいります。

Okta会社概要
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。