アイデンティティの セキュリティチェックリスト

アイデンティティへのサイバー攻撃から組織を守るための40の質問

過去1年間におけるセキュリティ侵害は、アイデンティティがサイバー犯罪者や国家的脅威アクターにとって、重要な攻撃ベクトルであることを明確に示しています。アイデンティティは単なるログインボックスではなく、企業の最も機密性の高いデータや、インフラストラクチャに対する最初で最後の防御線です。

このことはデータが裏付けています。クレデンシャルを再利用する問題が蔓延しており、Web アプリケーションの侵害の 86% は漏洩したクレデンシャルに起因しています[1]。当社の「The State of Secure Identity Report 2023」によると、Customer Identity Cloud の顧客アプリケーションの半数以上が、漏洩したクレデンシャルを使用した攻撃を少なくとも 1 回経験しています[2]。さらに、ソーシャルエンジニアリングを実行するコストが低下し続けているため、MFAをバイパスすることが攻撃者の焦点であり続けています。当社のプラットフォームでは、MFA試行の12.7%がMFAバイパス試行で占められていました[2]。

これらのデータから明らかなのは、アイデンティティはセキュリティであるということです。

Oktaはアイデンティティ攻撃との戦いにおいて、お客様と業界を支援する最前線にいます。全世界で100億回以上のログインをサポートし、18,000社以上のお客様を、月間20億回以上の悪質な要求から保護しています。業界のリーダーとして、当社はこのチェックリストのようなベストプラクティスを共有することで、お客様が可能な限り強力なアイデンティティセキュリティ態勢を導入できるようにご支援してまいります。なお、これは一般的なアドバイスであることをご留意ください。

[1] ベライゾン： 2023年データ漏洩/侵害調査報告書

[2] Okta : The State of Secure Identity Report 2023

統合アイデンティティセキュリティとゼロトラスト

基礎編

1. 貴社のアイデンティティセキュリティソリューションは、アイデンティティとアクセス管理、インシデント対応、リスク管理、継続的改善への取り組みを含む、総合的なサイバーセキュリティ戦略に寄与していますか？
2. アクセス要求のコンテキストにおいて、ユーザー、デバイス、アプリケーションを動的に認証・認可する手段を導入していますか？
3. 特権アクセスの承認、レビュー、更新のプロセスが確立されていますか？
4. 攻撃対象となる可能性のある領域を最小限にするために、アイデンティティセキュリティソリューションに最小特権アクセスを実装していますか？特に、可能な限り管理者権限を最小化または削除していますか？

上級編

5. ユーザーやデバイスの行動を継続的に監視・評価し、異常な行動や不審な行動を検出する強固な戦略がありますか？
6. ITサポートスタッフが、高度な特権を持つユーザーに対して操作を実行できないように、ITサポートスタッフの権限を制限していますか？例えば、これらのユーザーにカスタム管理者ロールを作成し、割り当てていますか？
7. 目視確認など、特権ユーザーに対する強力なヘルプデスクのアイデンティティ検証の仕組みを導入していますか？
8. 最も重要なリソース内で、ユーザーのやりとりを通じ、継続的にユーザーのアイデンティティを確認するための手段を講じていますか？
9. 貴社のIT環境にアクセスする第三者にゼロトラストのセキュリティを要求していますか？特に、サードパーティがネットワーク境界を維持する能力を暗黙のうちに信頼するのではなく、第三者の態勢を検証し、監査していますか？

アイデンティティとアクセス管理

基礎編

10. すべての機密リソースへのアクセスにはフィッシング耐性のあるMFAを導入していますか？
11. フィッシング対策は、従業員の登録/オンボーディングから回復までのライフサイクル全体に及んでいますか？
12. 管理者が機密性の高い操作を行う際に、ステップアップ認証を要求していますか？
13. アカウントの MFA 要素がすべてリセットされたときや、新しいデバイスを使用してアカウントにアクセスしたときなど、リスクの高いイベントが発生したときにユーザーに自動的に警告を発していますか？
14. オンボーディング、オフボーディング、アクセスレビューなど、アイデンティティのライフサイクル管理を自動化し、正確性と効率性を確保していますか？
15. 貴社では、どのような基準でアイデンティティアカウントを休眠アカウントとして定義していますか？休眠アカウントのレビューはどのくらいの頻度で行っていますか？
16. 定期的にパスワードをローテーションしたり、インタラクティブなアクセスごとにパスワードをローテーションしたりするなど、サービスアカウントの認証情報に対する戦略を持っていますか？
17. アイデンティティガバナンス戦略を策定し、業界標準やベストプラクティスとどのように整合させていますか？
18. ユーザーのアクセス権を定期的に認証・検証する仕組みがありますか？
19. 企業および個人デバイス（ノートPCとモバイルの両方）のリモートユーザーに対して、リソースへのセキュアでシームレスなアクセスを保証する仕組みがありますか？

上級編

20. 貴社のアイデンティティガバナンスソリューションは、有害なアクセスの組み合わせを防ぐために、職務の分離を実施していますか？
21. 特権アカウントは、 堅牢なフィッシング耐性のある多要素認証で強化され、高度なセキュリティレベルが確保されていますか？
22. 包括的な特権アクセス管理（PAM）ソリューションを導入し、特権アカウントの発見、保護、記録、監視を行っていますか？
23. すべてのワークプレイスアプリケーションについて、IT環境にアクセスする第三者に対してIAMソリューションによる認証を要求していますか？
24. 重要なリソースへのユーザー認証にIPバインディングを適用していますか？APIまたはWebリクエスト中に観察されたIPアドレスが、セッション確立時に記録されたIPアドレスと異なる場合、管理者は管理セッションを自動的に取り消すことができますか？
25. ネットワークタイプ（匿名化プロキシなど）によって、アイデンティティソリューションへのリクエストをブロックしていますか？

修復と軽減の戦略

基礎編

26. 特権アカウントの監視を強化するために、どのような 既存の方法やツールを使っていますか？
27. ユーザー行動分析は、検知と対応能力のために、全体的なアイデンティティセキュリティ戦略にどのように統合されていますか
28. オンプレミスのADエージェントに変更が加えられたときに、自動的にアラートが出ますか？
29. アイデンティティプラットフォームは、システム構築と保守のための「Infrastructure-as-Code」アプローチをサポートしていますか？
30. アイデンティティソリューションは、ブルートフォース攻撃によるアカウントのロックアウトを防ぐために、既知のデバイスからのリクエストを認識できますか？

上級編

31. ユーザーアクセスとマシン間アクセスの両方にロケーションベースの制限をかけることができますか？
32. 管理者は、IPアドレスがアノニマイザーのアドレスに関連付けられているかどうかの評価に基づいて、アノニマイザーからのリクエストを検出してブロックできますか？
33. 認証されたアプリケーションだけがAPIにアクセスするためにトークンを使用できるようにするために、所有証明を使用してマシンツーマシン（M2M）統合のトークンバインディングを強制していますか？
34. 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か？
35. アプリケーションを構築する際、セッション管理コントロールとトークンセキュリティの強化を実装していますか？特に、ユーザーエクスペリエンスを調整するために、独自のセッション管理ダッシュボードを構築していますか？

従業員トレーニングと意識向上

基礎編

36. 最新のセキュリティ脅威やベストプラクティスについて従業員を教育するために、定期的にフィッシングに関する意識向上トレーニングや一般的なサイバーセキュリティトレーニングを実施していますか？
37. 従業員は、強力なパスワードポリシーとパスワードレス認証オプションの導入と利点について、情報を与えられ、教育されていますか？
38. フィッシングの模擬演習を実施し、従業員のフィッシング攻撃に対する耐性をテストし、そのような攻撃の被害に遭う可能性のある従業員に的を絞ったトレーニングを提供していますか？
39. 従業員がセキュリティ上の懸念を報告したり、セキュリティ関連事項について説明を求めたりできる仕組みがありますか？
40. 従業員は、ソフトウェアやデバイスを最新のセキュリティパッチに更新することの重要性について教育されていますか？

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。