DATA SHEET

CA Advanced Authentication

CA Advanced Authentication は、モバイル・アプリケーションと Web アプリケーションを保護するために、ユーザにとって便利でコスト・パフォーマンスに優れた安全な方法を提供します。このソリューションを使用すれば企業は、サイレントでトランスペアレントにデータを収集し、デバイスの識別、位置情報およびユーザ動作などに基づいて、リスク評価を行えます。CA Advanced Authentication はソフトウェアベースの幅広い 2 要素認証クレデンシャルによって、ログインのセキュリティを強化します。リスク・アセスメントと多要素クレデンシャルを組み合わせることで、インテリジェントな階層型セキュリティ・アプローチを使用して、ユーザ・エクスペリエンスに影響を及ぼす不正なアクセスやオンライン ID 詐欺を防止できます。

主なメリット / 成果

- トランスペアレントなリスク分析とソフトウェアベースの 2FA クレデンシャルによって、スムーズなユーザ・エクスペリエンスを提供
- データ違反、不正なアクセス、アイデンティティ盗用の可能性を低減
- オンライン詐欺を抑制することで、運用コストを削減
- 強力な本人認証に対する政府規制および業界ガイドラインへの適合が可能

主な機能

- リアルタイムのリスク・アセスメントを実行し、機密性の高いログインやトランザクションを保護
- デバイスの識別、位置情報、ユーザ動作、その他の要因に基づきリスクを評価
- E メール、テキスト、音声でステップアップ認証を行うプッシュ通知やワンタイム・パスワード（OTP）など、帯域外の方法をサポート
- 一般的な不正パターンに対応するデフォルトのルール・セットによって、容易に使用できカスタマイズも可能
- パスワード、セキュリティに関する質問、2FA ソフトウェア、ハードウェア・トークンなど、各種のクレデンシャルをサポート
- Web およびモバイル・チャネルの保護と、データの統合によって、包括的な不正防止管理が可能
- 使いやすく実装が簡単な RESTful インタフェースによって安全な DevOps を実現し、革新を加速
- CA Single Sign-On と CA Mobile API Gateway を緊密に統合

ビジネス上の課題

社員、パートナー、および顧客はすべてオンライン・アプリケーションに簡単にアクセスできることを必要としていますが、同時に機密データを不正アクセスから保護することも重要です。企業は以下のことを行う必要があります。

オンライン・トランザクションのセキュリティの強化：パスワードは、簡単に破られます。ユーザを識別し、不正なアクセスから保護するための適応的な方法が必要です。

モバイル・デバイスの安全な推進：ユーザは企業とやり取りを行う手段として、好んでモバイル・デバイスおよびアプリケーション「を使用するようになりました。あらゆるアクセス・チャネルとデバイスに対応する一貫した本人認証方法が必要です。

法令順守指令への対応：規制や業界ガイドラインの多くで、本人認証方式の強化が推薦されたり要求されたりしています。企業はこうした要件に、コスト・パフォーマンスに優れた方法で対応する必要があります。

優れたユーザ・エクスペリエンスの実現：ユーザは気が変わりやすく、待つことを好みません。企業はユーザ・エクスペリエンスに影響を与えずに、セキュリティを強化する必要があります。

ソリューションの概要

CA Advanced Authentication は、以下の 2 つの代表的な本人認証製品を組み合わせたパッケージ・ソリューションです。

CA Risk Authentication：トランスペアレントでインテリジェントなリスク評価を実行できるため、ユーザが本人の主張どおりの人物であるという保証が大幅に強化されます。このソフトウェアはすべてのオンライン・トランザクションについて、デバイス、位置情報、ユーザ動作に基づいてリスクを評価し、定義されたしきい値をリスク・スコアが上回ると、ステップアップ認証を開始します。

CA Strong Authentication：広範なクレデンシャルや方法により、Web アプリケーションおよびモバイル・アプリケーションの多要素認証が可能です。このソフトウェアでは、アクセス対象のアプリケーションに基づいた、適切なセキュリティ・レベルの適切なクレデンシャルをデプロイでき、コスト・パフォーマンスに優れた一元的な方法で適用が可能です。

これらの製品を組み合わせることで、コスト、利便性、セキュリティの適切なバランスをとった階層型セキュリティ・アプローチを実現でき、アプリケーションとユーザ・アイデンティティの保護に役立ちます。その結果、セキュリティが向上し、コンプライアンス・プロファイルが改善し、運用コストを削減できます。

重要な差別化要因

ホワイトボックスの考え方：各リスク・ルールに関する判断と結果を可視化し、リスクとユーザの利便性のバランスを企業に合わせて向上させることができます。

ユーザ動作のプロファイリング：各ユーザ動作のパターンを学習し、通常とは異なる場合に検知することで、手間を軽減します。

柔軟なルール・エンジン：環境を完全に制御できます。特に、カスタム・ルール、ポリシー、アクションを構築し、特定のユースケースとトランザクションにリスク・エンジンを適応させることができます。

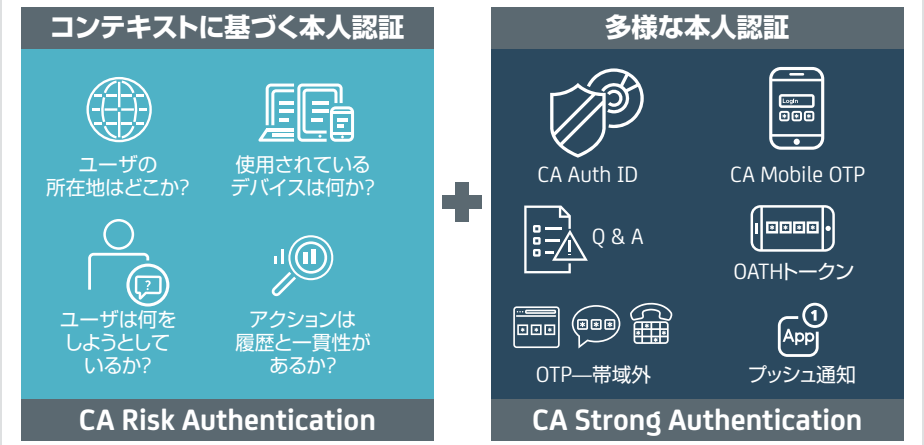
柔軟な本人認証：多様な本人認証クレデンシャルおよびフローに対応し、リスク・レベルに基づき各種のステップアップ認証方式を設定できます。

ケース管理：ポリシーベースのシステムにより、疑わしい行為の事例を確認し、管理できます。

パスワードの保護：パスワードをユーザのデバイスやバックエンド・システムに保管せず、また、パスワードをインターネット上で送信しないようにするため、パスワード・ファイルの盗用リスクがなくなります。

暗号カモフラージュ：独自の CA Auth ID および CA Mobile OTP クレデンシャルを総当り攻撃および辞書攻撃から保護するため、特許取得のキー隠蔽技術が使用されています。

最善の組み合わせの 2 つのコンポーネントは、別々または一緒にデプロイできます。



関連製品

- **CA Mobile API Gateway：**ユーザ、アプリケーション、デバイス間に信頼関係を構築し、デバイスとバックエンド・システムの通信を保護します。
- **CA Single Sign-On：**一元化されたセキュリティ管理の基盤が提供されるため、顧客とビジネス・パートナーはオンプレミス、ホストまたはパートナーベースのアプリケーション全体で Web のシングル・サインオンを使用できます。

詳細については、**ca.com/jp/multifactor-authentication** をご覧ください。

CA Technologies（NASDAQ：CA）は、企業の変革を推進するソフトウェアを作成し、アプリケーションケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

Copyright © 2017 CA, Inc. All rights reserved. 本書に記載されているすべての商標、商号、サービス・マーク、ロゴは、該当する各社に帰属しています。この文書は保証を含むものではなく、情報の提供のみを目的としています。機能に関する記述は、本書に記載された顧客に固有のものである可能性があり、実際の製品性能は異なる場合があります。
CS200-290570_0717