DATA SHEET

CA Strong Authentication

概要

CA Strong Authentication では、幅広い強力な認証方法を効率よく一元的にデプロイできます。また、柔軟で使いやすい一連の多要素クレデンシャルにより、ユーザやヘルプデスクに負担を掛けることなく、セキュリティを強化し、コンプライアンスを改善します。CA Strong Authentication を CA Risk Authentication と合わせて使用すると、認証セキュリティをさらに強化し、ユーザの利便性を向上します。さらに、CA Identity および Access Management ポートフォリオ全体を統合できます。

主なメリット / 成果

- 不正アクセス、データ侵害、攻撃のリスクを低減
- エンドユーザのログイン・エクスペリエンスに影響を及ぼさずに、セキュリティを強化
- パスワード盗用によるリスクを排除
- 組織のニーズに応じて拡張可能

主な特長

- パスワードやナレッジベース認証（KBA）方式から二要素ソフトウェア・トークンやハードウェア・トークンまで、さまざまなクレデンシャルをサポート
- テキスト、音声、または E メールによるワンタイム・パスワード（OTP）を使用した、帯域外（OOB）認証を提供
- パスワードの保存を行わないことにより、パスワード・ファイル盗用のリスクを排除
- ワークステーション、スマートフォンまたはタブレットを 2 要素トークンへと変換
- SAML、API、RADIUS などのさまざまな統合オプションを提供
- Web アプリケーションまたはネットワーク・パフォーマンスを劣化させることなく、多数のユーザを保護
- クラウド・サービス、MSP ホスト・サービスまたはオンプレミス・ソリューションとして利用可能

ビジネス上の課題

オンライン・ログイン / 機密性の高いトランザクションのセキュリティを強化します。パスワードは、簡単に破られます。組織は、ユーザに負担を掛けることなく、ユーザを識別し、機密データや重要なオンライン・トランザクションを保護できる、順応性の高いソリューションを必要としています。

モバイル・エコノミーをサポートします。ユーザは組織とやり取りを行う手段として、好んでモバイル・アプリケーションおよびデバイスを使用するようになりました。組織は、あらゆるデバイスに対応する一貫した認証方法が必要です。

法令順守指令を満たします。多数の規制で、機密性の高いトランザクションには強力な認証を推奨し、義務付けています。多くの組織にとって目下の課題は、コスト・パフォーマンスの高い方法で適切な認証方式を実装することです。

エンドユーザの操作の簡略化ユーザは気が変わりやすく、多くの企業がモバイル・アプリケーションの受け入れに苦慮しています。ユーザ・エクスペリエンスに影響を及ぼさずに、セキュリティを強化することが求められます。

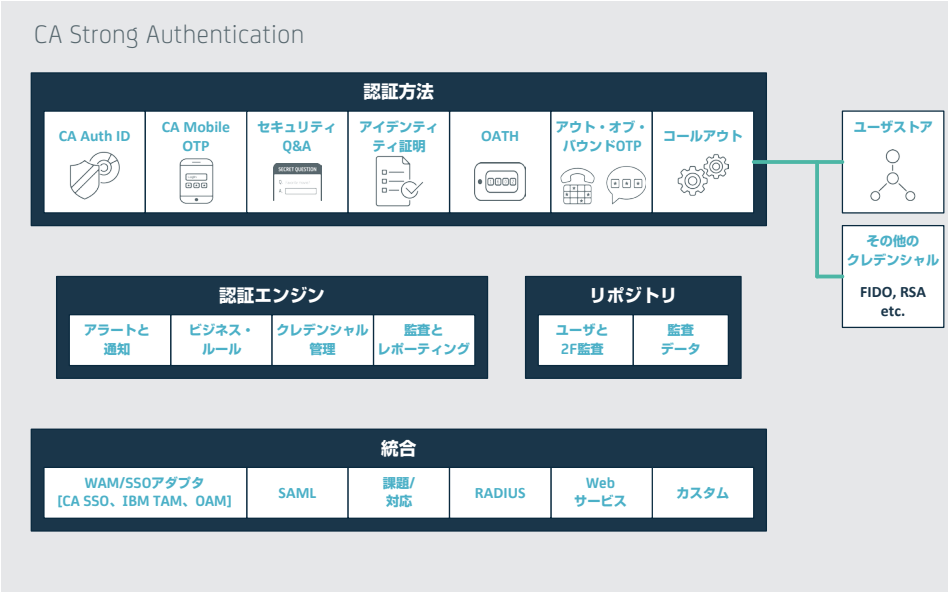
ソリューションの概要

CA Strong Authentication は、広範なクレデンシャルにより、Web アプリケーション、ポータルおよびモバイル・アプリケーションで多要素認証を実現します。アクセスしているアプリケーションに基づいて、適切なレベルのセキュリティを持つ正しいクレデンシャルをデプロイできます。認証プロセスに不要な矛盾を生じることなく、ビジネス・ポリシーに基づいて、優れたコスト効果と一元形式で多要素認証を簡単に導入できます。これにより、セキュリティの強化、コンプライアンス・プロファイルの改善、運用コストの削減、および顧客維持率の向上を可能にします。CA のソフトウェア専用アプローチでは、Web リソースおよび Web ユーザーのアイデンティティ保護を強化する場合に、コスト、利便性および強度の正しいバランスが得られます。このソリューションは、CA Risk Authentication と合わせて、マルチレイヤの認証セキュリティを提供します。

CA Strong Authentication の特長

10年以上に渡り、CA Strong Authenticationは、多要素認証分野のリーダー的存在で、オンラインおよびモバイル・ユーザの識別とアプリケーションおよびクラウド・サービスへのアクセスの管理という重要なニーズに対応してきました。

- **破れないパスワード：**お客様はパスワードをそのまま使用できます。ただし、パスワードは、インターネットを介して送信されることがなく、ユーザのデバイスやバックエンド・システムには保存されないため、ユーザの頭の中にだけ存在する完全なシークレットとなります。
- **独自のクレデンシャル：**利用可能な幅広い認証方法やクレデンシャルを使用するか、既存のクレデンシャルを一元化認証方法の中で使用できます。
- **暗号化カモフラージュ：**独自の多要素 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。
- **総所有コスト：**このソリューションは、クレデンシャルごとではなくユーザごとにライセンスが許可されるため、組織は、無制限のクレデンシャルを使用して、無制限のユーザおよびデバイスをサポートできます。



関連製品

CA Risk Authentication. 行動プロファイリング、モバイル・デバイス・リスク評価、DeviceDNA™ および動的ルールを使用した、リスク・ベースの認証。

CA Single Sign-On:従業員、顧客およびパートナーを対象に、オンプレミス、ホスティングまたはクラウド・ベースのアプリケーションでの Web シングル・サインオン。

CA Privileged Identity Manager：特権アカウント管理、プラットフォームおよびオペレーティング・システム全体でサーバ / アプリケーション / デバイスの保護。

サポートする環境

デバイス – アンドロイド、iOS、PC、Win8 Mobile

ブラウザ - Apple Safari、Google Chrome、Microsoft® Internet Explorer®、Mozilla Firefox

シングル・サインオン – CA Single Sign-On、IBM® Tivoli® Access Manager、Oracle Access Manager

標準とプロトコル – EMV CAP/DPA、HOTP/TOTP、HTTP/HTTPS、RADIUS、SAML、SOAP

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・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。