opentext™ | Cybersecurity

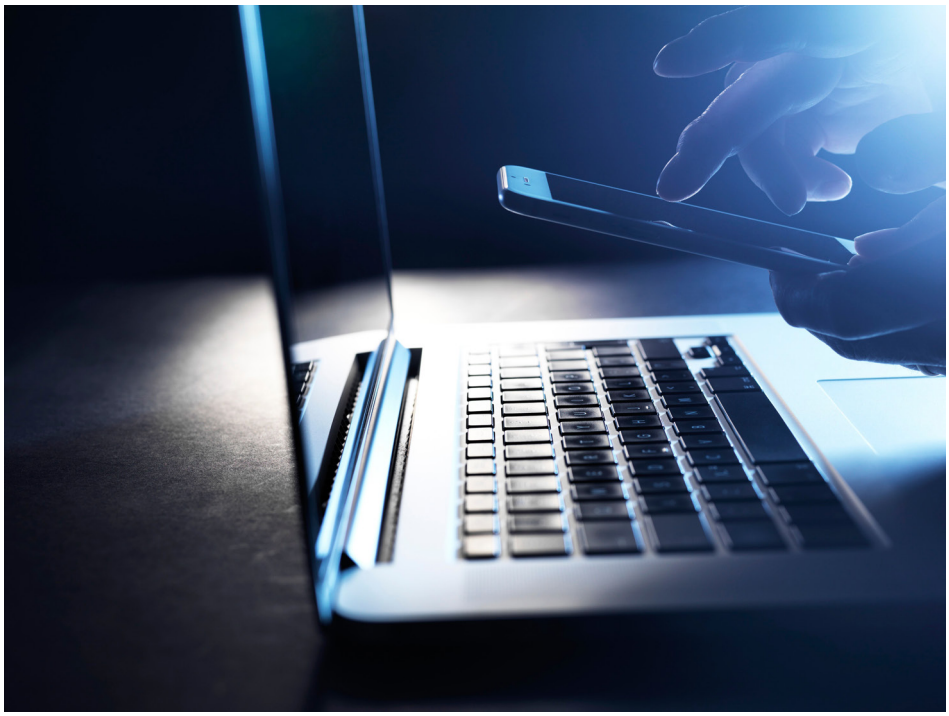
製品ハンドアウト

NetIQ Advanced Authentication をお客様のビジネスに

認証フレームワークを導入することで、コストを削減し、セキュリティを強化して、組織全体でより多くの認証オプションを提供できるようになります。

NetIQ Advanced Authentication の概要

- 1つのフレームワークであらゆる認証ニーズに対応
- 認証方式をさまざまな組み合わせで統合できる柔軟性を提供
- さまざまな統合 (RADIUS、VPN、OpenID、OATH、FIDO、RACF Windows、Mac OS、Linux、Citrix、VMware など) をサポート



標準ベースの認証フレームワーク

絶え間ないサイバー脅威にさらされる現代のコネクテッドワールドでは、認証戦略がサイバー脅威から身を守るための中核的な要素となっています。このイニシアチブは、リスク管理と政府の規制によって推進されるのが一般的ですが、多くの場合、シンプルで強力な ID 検証を含む特定のビジネス要件によって推進されます。

認証が適切に行われると、以下のことが可能になります。

- 顧客からの信頼を高め、組織とのデジタルなやり取りを安心して行ってもらえるようにする。
- ユーザーの不便さや手間を最小限に抑えながら、セキュリティ侵害への耐性の高い ID 検証を提供することで、ビジネス環境を整える。
- 従業員、契約業者、パートナーの所在地に関係なく、ビジネスプロセスが簡素化および最適化されるように設計されたサービスアーキテクチャの一部に認証を組み込む。

シングルサインオンは、利便性の高いアクセスに不可欠な要素であり続けており、セキュリティのための強力な認証への依存度をさらに高めています。

フレームワークが重要な理由

認証の新規購入は通常は事業部内で提案されるため、多くの場合、特定の戦術的観点から行われます。こうしたアプローチでは、組織は認証において複数のサイロ (アクセスの構築、リモートアクセス、コンプライアンス要件など) を抱えることになります。このようにばらばらの実装が行われると、管理オーバーヘッドが高くなり、プロセスが非効率になります。しかし、さらに重要な点は、一貫性のない認証ポリシーが原因で脆弱性が発生することです。

要約すると、認証フレームワークによって次のことが可能になります。

- 統合によるコストの削減。
- 1 つの共通ポリシーライブラリによるセキュリティの強化。
- 組織全体で提供される認証オプションの増加。

組織の幅広いニーズに対応できるフレームワークを構築することは容易ではありません。たとえば、次のような問題があります。

- 小規模な組織にとっては導入や管理が簡単であり、一方で大規模な組織にとっては拡張性の要件を満たすものでなければなりません。
- 特定の地域に集中している組織か、世界中に広く分散している組織かにかかわらず、組織の形態に合わせて成形できる必要があり、組織の形態に関係なく、フレームワークは認証要求に迅速に応答しなければなりません。
- フレームワークでサポートされる方式が多ければ多いほど、認証のサイロを 1 つに統合するための組織の柔軟性が増します。また、新しい認証技術が市場に現れた際に、フレームワークを容易に拡張できる必要もあります。

標準ベースのオープンアーキテクチャ

CTO やアーキテクトは長期にわたって、オープンスタンダードの利点を理解してきました。本質的に相互運用性を備えているため、アプリケーションやプラットフォームに依存することはなく、アーキテクチャの長期的な整合性を確保できます。しかし、独自のプロトコルで構築された認証ソリューションを導入すると、ニーズに最も適したデバイスを最良の価格で購入する自由はその組織にはもうありません。また、ベンダーロックインにも陥る可能性があります。

OpenText™ のサイバーセキュリティ事業部門は、FIDO (Fast Identity Online) Alliance のメンバーであり、強力な支援者です。FIDO U2F (Universal 2nd Factor) は、ユーザー自身が認証デバイスを管理する環境を組織がサポートできるようにします。NetIQ Advanced Authentication by OpenText™ では、堅牢なフレームワークによって上述した機能がお使いのアプリケーションに提供されます。開発の手間をかける必要はありません。トークンコストを先送りできるというメリットを得られるばかりか、ユーザーはデジタルライフの他の側面にも高いレベルのセキュリティを導入できるようになります。

NetIQ Advanced Authentication が提供する高度なサポートを考慮に入れれば、U2F 認証環境を提供するフレームワークとして、これほど優れたものはありません。

- FIPS 140.2 準拠
- OAuth2 統合
- OATH 認証
- Google Authenticator
- Microsoft OATH
- NFC ISO/IEC のサポート
- RADIUS との統合
- Kerberos との統合
- PKSCS7 および PKCS11 のサポート

IT グループは、今日の最新の認証規格を最低限しかサポートしていないソリューションを選択することには用心深くなる必要があります。

最多のネイティブの方式によって最大限のアプリケーションに対応

NetIQ Advanced Authentication では、RADIUS で使用できる認証タイプ以外にも、市場に出回っている他のどのソリューションよりも多くの認証方式がネイティブで用意されています。それがなぜ重要なのかと言えば、社内外のユーザーが、さまざまな状況下で複数のデバイスから機密情報にアクセスするからです。NetIQ Advanced Authentication は、導入後すぐに使用可能な一連のアプリケーション統合機能 (RADIUS、OpenID、OATH、FIDO、RACF、z/OS、Windows、Mac OS、Linux、Citrix、VMware など) を備えているため、既存の環境に幅広く対応できます。さらに、多様な認証リーダーや認証方式を広範にサポートすることで、これまでにない柔軟性を提供します。

SaaS、Docker、アプライアンス— どのプラットフォームでも妥協なし

当社の NetIQ Advanced Authentication のフレームワークは、既存の環境の規模にかかわらず、中断のない継続的な運用を実現する高可用性と内部負荷分散を提供するように設計されています。プライマリサーバーとセカンダリサーバーの間のレプリケーションにより、(LAN または WAN 経由の) データ整合性と障害復旧を提供します。

NetIQ Advanced Authentication は、次のような複数のフォームファクターで使用できます。

- 従来のオンプレミス
- ソフトアプライアンス
- Docker コンテナ
- OpenText から直接提供される SaaS (Software-as-a-Service)

アプライアンスのシンプルさ

NetIQ Advanced Authentication のソフトアプライアンスエディションは、SMB の環境に最適です。すべてのコンポーネントが 1 つのパッケージに統合されており、通常必要とされる設定作業の多くが不要となっています。仮想イメージをロードするだけで使用を開始できます。さらに、アプライアンスは凝縮され強化された仮想アプライアンス環境であるため、必要なことだけを行い、それ以外のことは行いません。そのため、ハッカーやマルウェアに悪用される可能性のある不要なサービスの露出から保護されます。Docker の経験がない場合、多くの企業にとって最適の選択肢です。

管理しやすい Docker コンテナ
各企業が複雑なハイブリッド環境全体にわたってアーキテクチャを進化させ続けている中、アプリケーションの導入と配布を容易にすることがこれまで以上に重要になっています。NetIQ Advanced Authentication が Docker コンテナとして利用できるようになったのはこのためです。すべての依存関係が小規模の Docker コンテナのセットにバンドルされているため、互換性の問題なく必要に応じて転送することが可能です。また、互換性の問題を回避できるからこそ、Docker コンテナは Amazon Web Services (AWS) などのクラウド環境で選ばれるフォームファクターになっているのです。コンテナとして導入された NetIQ Advanced Authentication は、ニーズに最適な仮想化、ハイパーバイザー、クラウドベースのさまざまなテクノロジー上で実行できます。パフォーマンスや可用性に最適化された専用モデルで構成することもできます (バージョン 6 以降)。

Office 365 および Azure 環境向けの強力な認証

各企業が Office 365 や Microsoft の Azure プラットフォームに移行するようになるにつれ、Active Directory Federation Services (ADFS) の使用が拡大しています。これらの製品の持つリスクに対処できるように、認証の強度をアップデートすることが重要です。NetIQ Advanced Authentication は、 統合によってユーザーが使用しやすい形で環境へのアクセスを保護する一方で、MFA (多要素認証) によって高いレベルのユーザー認証を提供しています。つまり、お使いのアプリケーションがオンプレミス環境またはクラウド環境のいずれで実行されているかにかかわらず、NetIQ Advanced Authentication は ADFS を中心としたシステムを強化して不正アクセスから保護することができます。

パスワードレス戦略に最適なフレームワーク

パスワードレスソリューションは何十年も前から利用可能でしたが、コストと導入の複雑さの両方が、普及の障壁となっていました。しかし近年、市場に変化が見られます。ビジネスでもプライベートでもスマートフォンが普及したことで、指紋リーダーが一般的なものになりました。同様に、虹彩認識にスマートフォンのカメラを使用するモバイルアプリも注目を集めています。

しかし、パスワードレステクノロジーの最大の後押しとなったのは、多要素認証をいつでもどこでも使えるようにすることを求める圧力です。主要産業におけるさまざまな政府の規制により、企業はパスワードに勝る認証技術の導入を余儀なくされています。企業は保護されたリソースにアクセスする際のユーザーの負荷を軽減するテクノロジーを常に求めているため、認証市場は進化し続けています。

ほぼすべての認証タイプをサポート
こうしたパスワードレステクノロジー (知識情報、所持情報、生体情報) は、多要素認証だけでなく、単一要素認証の場合にも強力な選択肢となります。これらのテクノロジーは、犯罪者が資格情報をハッキングするための武器であるフィッシングに対して非常に耐性があります。認証の種類として、カード、生体認証、Bluetooth、行動認証 (タイピング、ジェスチャーなど) などが挙げられます。現在、パスワードレス認証市場は約 350 億米ドル規模ですが、2030 年には 12 倍以上の 4500 億米ドル規模に成長すると予測されています[1]。このように、現在から将来にわたって、さまざまな認証ニーズに対応できるように設計されたフレームワークがあれば、お客様の投資は保護されます。

OpenText は、市場に登場する新たなテクノロジーをサポートするため、新しい方式を製品に積極的に取り入れています。組織の ID 検証戦略を進化させる際には参考にしてください。

ゼロトラスト環境に最大の柔軟性を提供
アプリケーション層における ID の観点からゼロトラストを環境に適用する場合、重要な機能は継続的な認証と権限付与です[2]。

- 継続的な認証とは、セッション内で急上昇したリスクスコアに応じて、必要な回数だけ ID を再検証する機能です。認証方式の強度によっては、リスクスコアを下げるために 1 回以上認証に成功することが必要になる場合があります。
- セッション内の任意の時点でリスクスコアが上がった場合、アクセス要求が制限されるか、終了する可能性があります。

セキュリティチームと IT チームが自由に使える方式 (特にパッシブな方式) が多いほど、業務のペースを低下させないゼロトラスト環境を適切に設計することができます。このモデルは、機密性の高い情報が保護されている B2B、B2C、G2C のやり取りにも適用できます。さらに、いくつかのパッシブな認証方式を連鎖させることで、非常に強力な方式と同等の強度を実現することも可能です。パスワードレス認証は、利便性を高めるだけでなく、セキュリティの向上にもつなげることができます。

NetIQ Advanced Authentication でテレワークに対応

各企業は、機密性の高い情報にアクセスするリモートユーザーのセキュリティを確保するという課題に長い間直面してきました。一般的には、出張の多いビジネスマン、財務の専門家、経営幹部、規制されたデータにアクセスする人たちなどが、こうしたユーザーに当たりました。しかし、パンデミックによって、すでに拡大しつつあったテレワークというトレンドが劇的に加速しました。そのため、かつては従業員の中でも比較的少数派だったテレワーカーが、多くの企業で組織全体に広がっています。

1. **www.nextmsc.com/report/passwordless-authentication-market**
2. **https://community.microfocus.com/cyberres/b/sws-22/posts/achieving-zero-trust-without-driving-your-users-crazy**

「他の製品では解決できない認証の問題も、NetIQ Advanced Authentication なら解決できます」

セキュリティ導入専門チーム、シニアディレクター

お問い合わせ
www.opentext.com

リモートユーザーモデルのこうした進化により、認証に対する基本的な要件に次のような変化が生じています。

- ユーザー数が大幅に増えた現在、ユーザー数は選択肢を絞り込む際の主要な要因となります。
- ユーザー登録のパラダイム全体を変える必要があります。これまで以上に、シンプルなセルフサービス登録ツールへのリモートアクセスが必須となります。複雑なものは IT 部門のサポート能力を超えてしまいます。
- 認証のコストのオーバーヘッドとセキュリティの脆弱性が倍増します。
- サービスやリソースのパスワードレスでの利用を検証するには、より詳細なデューデリジェンスが必要になります。

認証のアプローチを戦術的なものから戦略的なものへとまだ進化させていない企業は、テレワークのトレンドが加速することで、その方向に進むことを余儀なくされるでしょう。

当社製品を選ぶ理由

統合 MFA アプローチのおかげで、NetIQ Advanced Authentication の構成や維持は他のソリューションほど複雑ではありません。また、導入後すぐに統合できるため、構成可能な認証オプションを豊富に利用できる点も強みです。当社製品を導入することで、企業全体のセキュリティとユーザビリティを向上させることができます。また、MFA インフラストラクチャの新規構築、置き換え、統合を自由に行うことができるため、コストを管理し、投資を最大限に活用することができます。コスト削減とセキュリティの向上を実現することによって、NetIQ Advanced Authentication は市場をリードするソリューションとしての立場を築き上げています。

NetIQ Advanced Authentication フレームワークの詳細および評価版の利用については、こちらをご確認ください。

YouTube チャンネル「NetIQ Unplugged」もぜひご覧ください。

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

761-JA0055-003 | O | 04/24 |