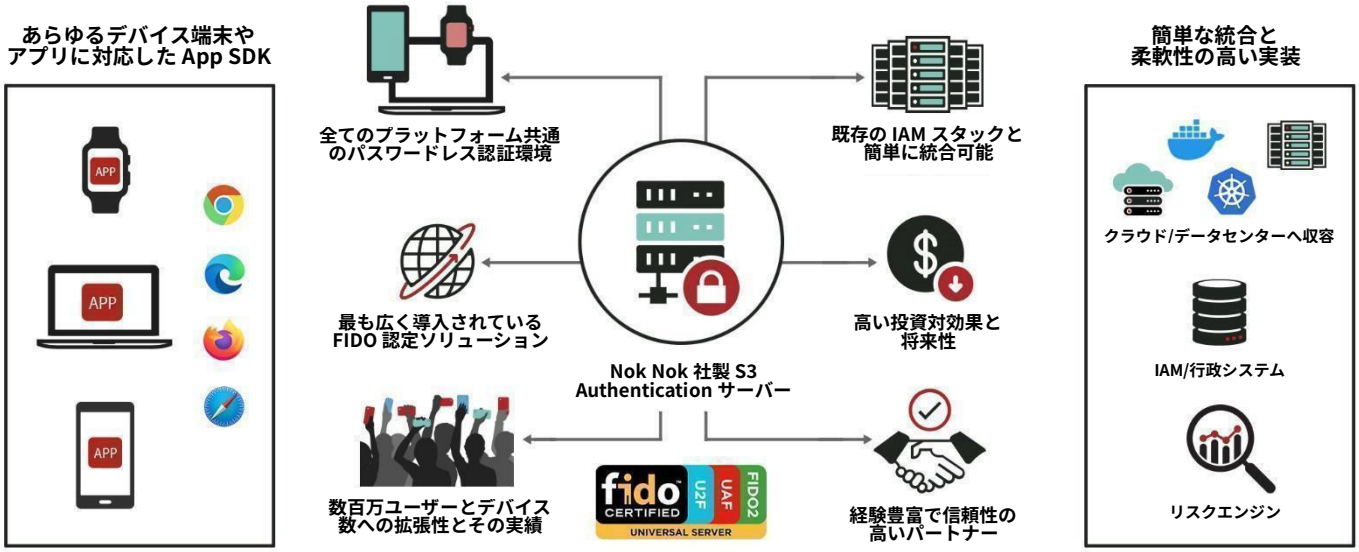
S3 AUTHENTICATION SUITE V9.2

データシート

Nok Nok Labs 社製 S3 Authentication Suite (以下、S3 Suite)製品 は、従来の認証よりも大幅にユーザーフレンドリーで、従来の 2 要素認証よりも安全なパスワードレス認証を提供し、ユーザーエクスペリエンスを大幅に向上させ、アカウントの乗っ取りなどの不正ログインを減少させます。
S3 Suite には、モバイル端末、Web、スマートウォッチ向けアプリケーション用のウィジェットを備えた認証サーバーと App SDK が含まれています。ユーザーのデバイスにすでに搭載されているセキュリティ機能を活用して、あらゆるアプリケーションに強力で便利な認証を提供します。
S3 Suite を使用すると、デバイス・バインド・パスキーや同期パスキーなど、すべての FIDO プロトコルをサポートすることで、組織はユーザーのデバイスを強力な多要素認証に簡単に変えることができます。
また、S3 Suite の豊富な機能セットにより、組織はスムーズなオンボーディング、プログレッシブ プロファイリング、新しいデバイスの簡単なブートストラップ、アカウントの回復、一時停止、プロビジョニング解除、コールセンター認証サポートなど、顧客のライフサイクル全体をサポートできます。



詳細はこちら

Nok Nok Labs 社製 S3 Authentication Suite 製品の詳細については、以下 URL をご覧ください。
https://noknok.com/products/s3-authentication-suite/

Nok Nok Labs 社は、S3 Authentication Suite のさまざまな試用方法(Software-as-a-Service、コンテナ イメージ、インストール可能なソフトウェアなど) を提供しています。

Nok Nok Labs 社のソリューションを試すには、次の URL にアクセスしてください。
https://www.noknok.com/demonstration

機能	利点
Adaptive Rulesets (アダプティブルールセット)	S3 Suite のアダプティブルールセットは、登録と認証のためのコードに依存しないポリシーサポートを提供します。ポリシーでは、S3 Suite App SDK によって生成される強力なシグナル、ビジネス アプリケーションによって提供されるコンテキスト情報、サードパーティのリスクツールによって提供されるリスク シグナルなど、複数の入力を使用します。 さらに、S3 Suite アダプティブルールセットは、追加の認証プロンプトを回避する (例: 最終ログインが最近でリスクが低い場合)、認証シーケンスをトリガーする (例: トランザクション金額が高い場合、またはデバイスでマルチデバイスの認証情報が初めて使用される場合)、またはアクセスを拒否する (例: 特定のデバイスが信頼されていない場合) 柔軟性を提供します。
認証プロトコルと方式	FIDO UAF、FIDO U2F、FIDO2、WebAuthn – 同期パスキー、デバイス・バインド・パスキー、認証、および FIDO メタデータを含む。NIST SP 800-63 で指定された FIDO セキュリティキー、 FIPS 認証ステータスと認証インテントの検出。在庫追跡向けエンタープライズ認証。Apple App Attest および Google Play Integrity に対応。 Nok Nok のクイック認証、インテリジェント パスワードレス認証、および 粒度適応型ポリシー。 認証子登録の提案、ネイティブ アプリケーションと Web アプリケーション間の資格情報共有、エンドユーザーが優先するカスタム認証子名のサポート。アウトオブバンド: QR コードとプッシュ通知。アプリ不要の帯域外認証 PSD2-SCA、W3C セキュア決済認証 (SPC)、3DS2 委任認証、動的リンク (否認防止) のサポート サードパーティ サービスによるメール OTP、SMS OTP、写真 ID + ライブ画像 (セルフィー) サードパーティ IAM システムによる OpenID Connect (OIDC) および SAML のサポート
デバイスとリスクシグナル	既知のデバイス、デバイスの健全性、デバイスのモデル、デバイスの種類、デバイスのメーカー、デバイスの OS バージョン、App SDK バージョン、IP アドレス、場所、速度、Wi-Fi ネットワーク、デバイスの「オンコール」、およびフレンドリー詐欺。サードパーティが提供するリスクエンジンや行動バイオメトリクスシステムとの簡単な統合のためにコンテキスト データをサポートします。
管理コンソール	認証サーバーを管理するための Web ベースの UI。管理者は、ポリシーの構成、プロパティの変更、構成のエクスポートとインポート、サーバー分析の詳細の確認を行うことができます。
きめ細かな管理者権限	きめ細かな管理者権限により、コール センターやヘルプ デスクのエージェント、ビジネスアナリスト、管理者など、さまざまな運用ロールに最小限の権限を簡単に適用できます。
マルチテナント対応	単一の認証スイートから複数の分離されたユーザーグループにサービスを提供して、運用効率を向上します。
レポートと分析	統計データと認証レポートを表示、生成、ダウンロードします。指定された期間のユニークユーザー、デバイスモデル、認証器、認証、トランザクション、登録解除などのユーザーベースの分析情報を提供します。コンプライアンス要件を満たす改ざん防止監査ログ。
統合	セッション プラグイン、シークレット ストア、暗号化統合を含む完全なサーバー側プラグイン サポート。カスタマイズ可能な REST API、JWT 認証トークン、EMVCo 3DS FIDO データ (「FIDO Blob」)。 Keycloak、ForgeRock® Identity Platform、Microsoft® Azure B2C、PingFederate® との統合。フェデレーションアプリとしてカスタマイズ可能なサインインアプリと資格情報管理ページ。
認証サーバーがサポートするプラットフォーム	**クラウド：**AWS, Microsoft Azure, Google Cloud Platform **オペレーション・システム：** Rocky Linux 9, RHEL 8, RHEL 9, **Java：** Adoptium、Red Hat OpenJDK 17 および 21、Oracle JDK 17、Oracle JDK 21。Bouncy Castle Java FIPS 1.0.2.x。 **アプリケーション・サーバー：** Apache Tomcat 10.1 **データベース：** Oracle 19c and 23c; MySQL 8.0 and 8.4; PostgreSQL 14, 15, and 16; AWS Aurora **DevOps：** Docker および Kubernetes 対応したクラウド開発ツールキット。ベースイメージ: デフォルトは Red Hat UBI9 とし、サポートされている各オペレーティング・システムのカスタム・ベースイメージを使用可。 **IoT 対応：** IoT SDK（別ライセンス）を介して、IoT デバイスへのユーザー認証を実行。 **UberEther を通じて FedRAMP High および DoD IL5 サービスとしても利用可能** (https://uberether.com/)
App SDK 対応プラットフォーム	**プラットフォーム：** Android 5.0+、Wear OS 1.0+、iOS 8+、watchOS 4.2+、WebAuthn API 用 JavaScript **プログラミング環境：** Objective-C、C++, Swift、Cordova、Java、JavaScript、ReactJS **アプリ種：** Web Apps、Progressive Web Apps (PWA)、Mobile Apps、WebView または App Links/Universal Links によるモバイルブラウザを用いたハイブリッドアプリ、activity-less Silent Authentication を備えた Android Widgets **ウィジット：** サインイン、トランザクション、サインアップ、クレデンシャル 用の UI フルカスタマイズ **セキュアハードウェア：**Secure Elements、Trusted Execution Environments (TEE)、Secure Enclave **認証器**: あらゆるモダリティをサポートする FIDO2/WebAuthn プラットフォーム認証器とローミング認証器 (「セキュリティ キー」)、ネイティブ API を使用する認証 (パスキー、Touch ID、Face ID、Android 生体認証 API、Android Keyguard など)、PIN/パスコード認証、ユーザー プレゼンス認証、サイレント認証、ローミング認証としての電話 - CTAP2「ハイブリッド」、あらゆるモダリティをサポートするサードパーティ認証 ASM (スピーカー認識など)、クラス 2 生体認証センサーに対応、Huawei Mobile Services を使用した FIDO 認証、CTAP/NFC FIDO2 決済カードに対応。

このカタログの記載内容は 2024 年 11 月現在のものです。記載内容は予告なしに変更することがありますのでご了承ください。

Nok Nok Labs 社について

Nok Nok Labs 社の技術により、FIDO 標準規格に基づいたパスキーベースのパスワードレス認証を提供し、より安全で高速なユーザー エクスペリエンスを実現できます。これにより、世界中のユーザーおよびデータ プライバシー規制に準拠できます。Nok Nok Labs 社はパスワードレスユーザ認証のリーダーであり、BBVA、Mastercard、Intuit、NTT ドコモ、スタンダードチャータード銀行、T-Mobile、Verizon などの大手銀行、通信会社、およびフィンテック企業から高い信頼を得ています。

Nok Nok Labs, Inc. 〒100-0005 東京都千代田区丸の内 1-6-2 新丸の内センタービル 21 階 www.noknok.com/ja/