NRI からのお知らせ
Notification from NRI

Nomura Research Institute

2026 年 7 月 7 日
株式会社野村総合研究所

野村総合研究所、API セキュリティ規格「FAPI 2.0」に準拠した ID 管理ソリューション「Uni-ID Libra」の最新版を提供開始

～金融・医療・公共など、あらゆる産業の API 連携をより安全かつシンプルに実現～

株式会社野村総合研究所（以下「NRI」）は、消費者向け Web サービス事業者に提供する ID・アクセス管理ソリューション「Uni-ID Libra」（ユニアイディー・リブラ、以下「本製品」）の最新バージョン（2.12.0）について、API セキュリティに関する国際規格である「FAPI 2.0」の認定を取得し、本日、提供を開始します。

近年、DX の進展に伴い、企業間でのデータ連携（API 連携）はあらゆる産業へと急速に拡大しています。一方で、個人情報や重要データを扱う API のセキュリティは、その抜本的な強化が必要になっています。

「Uni-ID Libra」は、顧客 ID の統合管理に加え、認証・API 認可やプライバシー保護をオールインワンで提供する CIAM（Customer Identity and Access Management）[1]ソリューションです。本バージョンでは、金融機関レベルの高いセキュリティ要件に対応する「FAPI 2.0」へ準拠したことにより、API 連携の安全性を一層強化しました。本製品を利用することで、金融・医療・公共など、あらゆる産業の API 連携をより安全かつシンプルに実現することが可能です。

■ 金融グレードの API セキュリティ標準「FAPI 2.0」

FAPI は、国際標準化団体 OpenID Foundation が策定する、API によるデータ連携を安全に行うための国際的なセキュリティ規格です。国内外のオープンバンキングをはじめ、高度なセキュリティが求められる領域で採用が進んでいます。2025 年に正式に仕様が確定した「FAPI 2.0」は、従来の FAPI 1.0 に比べ、よりシンプルかつ高い安全性を実現する設計にアップデートされました。

「Uni-ID Libra」はすでに FAPI 1.0 の認定を取得していましたが、本バージョンでは、「FAPI 2.0 Security Profile Final」および「FAPI 2.0 Message Signing Final」の 2 つの仕様について、新たに認定を取得しました。

■ 認定取得した仕様と、本製品の主な機能強化

1. FAPI 2.0 Security Profile Final

OAuth 2.0[2]や OpenID Connect[3]をベースとした安全な API 認可のための仕様です。トークンの不正利用防止や認可フローの保護のための機能を強化しました。

機能	対応内容
認可要求の保護	認可要求時の PAR（Pushed Authorization Requests）[4]を必須化し、各パラメータのセキュリティ要件を FAPI 2.0 に合わせて厳格化しました。リクエストパラメータの改ざんや漏えいを防止します。
認可応答の保護	認可コード方式および PKCE（Proof Key for Code Exchange）[5]を必須化することで、認可応答での ID トークンの漏えいを防ぎつつ、認可コードの横取り攻撃や CSRF（Cross-Site Request Forgery）[6]へのより強固な対策を実現します。
クライアント認証の保護	MTLS（Mutual-TLS）[7]および private_key_jwt 方式 [8]によるクライアント認証を必須化したことで、クライアントの正当性確認を厳格化し、なりすましを防止します。
アクセストークンの保護	MTLS および DPoP[9]による送信者限定トークンのみを発行します。これにより、トークンが漏えいした場合においても、不正なクライアントの悪用を防ぎます。 また、DPoP に対応したことで、TLS レイヤーとの連携が難しい環境でもアプリケーションレイヤーでの送信者限定トークンの実現が可能になりました。

2. FAPI 2.0 Message Signing Final

API でやり取りされるデータの改ざん・否認防止のための仕様です。実際にやり取りするデータの中身が改ざん・すり替えられていないかを証明するための機能が強化されました。

機能	対応内容
認可要求の署名	PAR エンドポイントにおいて、JAR（JWT-Secured Authorization Request）[10]の仕様に則った認可要求のリクエストパラメータ群（リクエストオブジェクト）の署名付き JWT[11]に対応しました。これにより、リクエストパラメータの完全性・機密性が確保されます。
認可応答の署名	JARM（JWT Secured Authorization Response Mode）[12]を用いた認可応答に対応し、改ざん検知を可能にしました。
イントロスペクション応答の署名	JWT 形式での応答に対応し、完全性を確保しました。

「Uni-ID Libra」の詳細は、下記の Web サイトをご参照ください。

https://uni-id.nri.co.jp/service/libra

NRI は、今後も、グローバルな技術動向とお客様のニーズに合わせた製品バージョンアップ・機能追加を行い、安全・安心なデジタル社会の実現に貢献してまいります。

---

[1] CIAM（Customer Identity and Access Management）：顧客（消費者）を対象に、ID 情報とアクセス権限を一元的に管理し、安全性と利便性の両立を図る仕組み。

[2] OAuth 2.0：OAuth とは、Web サービス間の連携において、外部からのデータやサービスに対するアクセスを、利用者の同意に基づいて認可するための仕様。OAuth に対応したサービス連携では、利用者が外部サービスに ID やパスワードを漏らすことなく、必要最低限のアクセス権限のみを委譲することができる。2012 年に策定された OAuth 2.0 が最新バージョン（2026 年 6 月時点）であり、現在は OAuth 2.0 の追加仕様やベストプラクティスを統合した OAuth 2.1 が公開へ向けて議論中である。

[3] OpenID Connect：Web サービスを提供する複数のサイト間で、ユーザーの同意に基づき、ID 情報を流通するための標準仕様。ユーザーは OpenID Connect 対応サイトに登録した ID 情報を使って、他の OpenID Connect 対応サイトにログインすることが可能となり、利便性の向上につながる。

[4] PAR（Pushed Authorization Requests）：認可要求のパラメータを、ブラウザの URL（クエリ文字列）経由ではなく、クライアントから認可サーバーへ直接バックチャンネル（サーバー間通信）で送信（Push）する仕組み。

[5] PKCE（Proof Key for Code Exchange）：認可コードの横取り攻撃を防ぐための仕様。

[6] CSRF（Cross-Site Request Forgery）：ユーザーがログインしている状態を悪用し、本人の意図しないリクエスト（操作）を強制的に実行させる攻撃手法。

[7] MTLS（Mutual-TLS）：サーバーとクライアントが互いに証明書で認証し、発行するアクセストークンをその証明書に紐付けることで、正当な送信者のみがアクセストークンを利用できるようにする仕組み。

[8] private_key_jwt 方式：OAuth 2.0／OpenID Connect におけるクライアント認証方式の一つで、クライアントが秘密鍵で署名した JWT を用いて認可サーバーに対し自身の正当性を証明する仕組み。

[9] DPoP（Demonstrating Proof of Possession）：アプリケーション層（HTTP ヘッダー）で公開鍵暗号を用いてアクセストークンの送信者証明を実現する仕組み。

[10] JAR（JWT-Secured Authorization Request）：認可要求のパラメータを従来のクエリ文字列ではなく、JWT（JSON Web Token）を使用して署名・暗号化されたオブジェクト形式にまとめて送信する仕様。

[11] JWT（JSON Web Token）：システム間で JSON（JavaScript Object Notation）形式の情報を安全にやり取りするためのデータ規格。

[12] JARM（JWT Secured Authorization Response Mode）：認可サーバーが認可応答全体を「JWT」で署名・暗号化して安全に引き渡す仕様。

【お知らせに関するお問い合わせ】

株式会社野村総合研究所　コーポレートコミュニケーション部　日下部

TEL：03-5877-7100　E-mail：kouhou@nri.co.jp

【本件に関するお問い合わせ】

株式会社野村総合研究所　ID ソリューション事業部

https://uni-id.nri.co.jp/contact