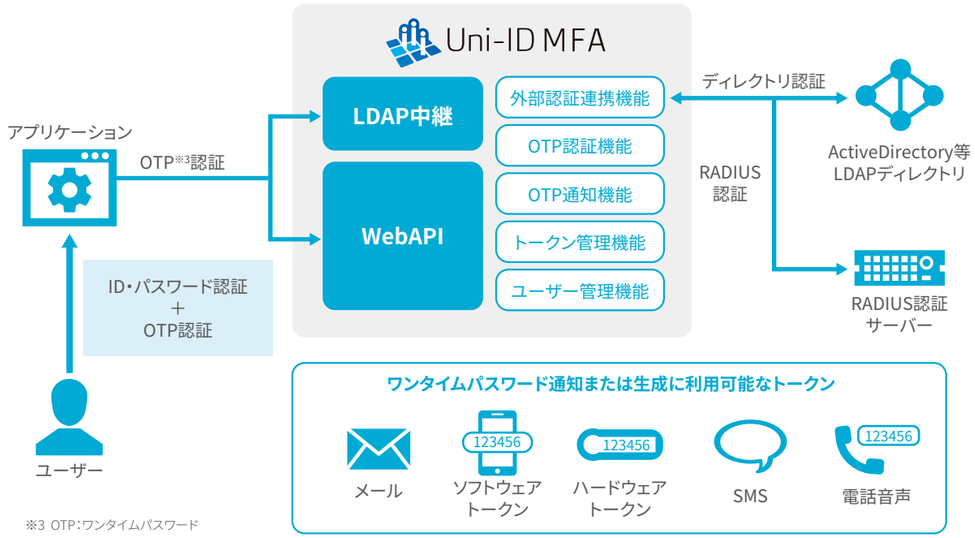
機能構成



※3 OTP：ワンタイムパスワード

アプリケーションからの認証要求は、WebAPI経由でも連携可能です。

動作環境（参考）

Uni-ID MFAは、以下の稼動環境で動作します。

稼働環境		バージョン
OS	Linux	Red Hat Enterprise Linux 6.x,7.x
ミドルウェア/DB	Java	Java Version 8
	Apache	Apache Web Server 2.2.x, 2.4.x Apache Tomcat 8.0.x
	DB	MySQL version 5.5以降
ハードウェア	CPU	Xeon E5-2670 2.5GHz相当　2コア以上
	メモリ	4GB以上の空き
	ディスク	10GB以上の空き

※10,000名程度の利用者を想定した場合のスペックとなります。詳しくはお気軽にご相談ください。

お問い合わせ

info@nri-secure.co.jp　☎ 03-6706-0500　受付時間 9:00-17:00 月曜日～金曜日(祝日・当社休業日を除く)

NRIセキュアテクノロジーズ株式会社

〒100-0004　東京都千代田区大手町1-7-2　東京サンケイビル
www.nri-secure.co.jp

9213-0057-02-1901

NRI SECURE

多要素認証エンジン

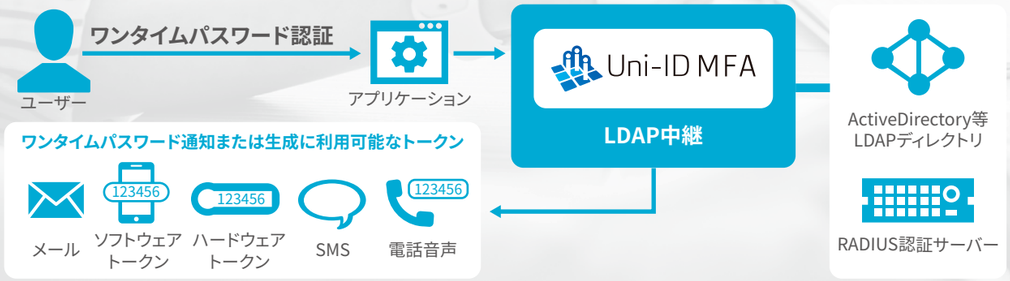
Uni-ID MFA

NRIセキュアテクノロジーズ株式会社

Uni-ID MFA　多要素認証エンジン

セキュアなログインを手軽に実現する ワンタイムパスワード認証エンジン

Uni-ID MFAは、ユーザー認証を強化するワンタイムパスワード認証エンジンです。
国際標準規格 OATH、TOTP※1に準拠し、通常のID・パスワード認証に
ワンタイムパスワード認証を追加することで、既存システムの認証を強化します。



Uni-ID MFAの特長

1 既存アプリケーションを改修せずに容易に実装

「LDAP中継機能」を組み合わせることで、既存アプリケーションに簡単に多要素認証の機能を追加することができます。

2 様々な種類のトークンを選択可能

認証に使用するトークンはユーザーの利用環境にあわせて柔軟にお選びいただけます。

3 不正アクセス検知と組み合わせ「リスクベース認証」も

不正アクセス検知ソリューション「Uni-ID IFD」と組み合わせることで、不正の疑いや脅威レベルが高い場合にのみ、追加認証としてワンタイムパスワードを要求できます。

4 信頼性の高さと低コストを兼備

金融機関で実績のある高い信頼性を誇る一方で、シンプルなワンタイムパスワード認証エンジンのため、低コストを実現しています。

ワンタイムパスワード認証のメリット

不正ログイン/なりすましを阻止

ユーザーが所有しているトークンでのみ認証が可能です。

「短時間のみ有効」「1回限りの使い捨て」による高い安全性

再利用されて不正にログインされることはありません。

国際標準規格化で、幅広いツール・手段が選択可能

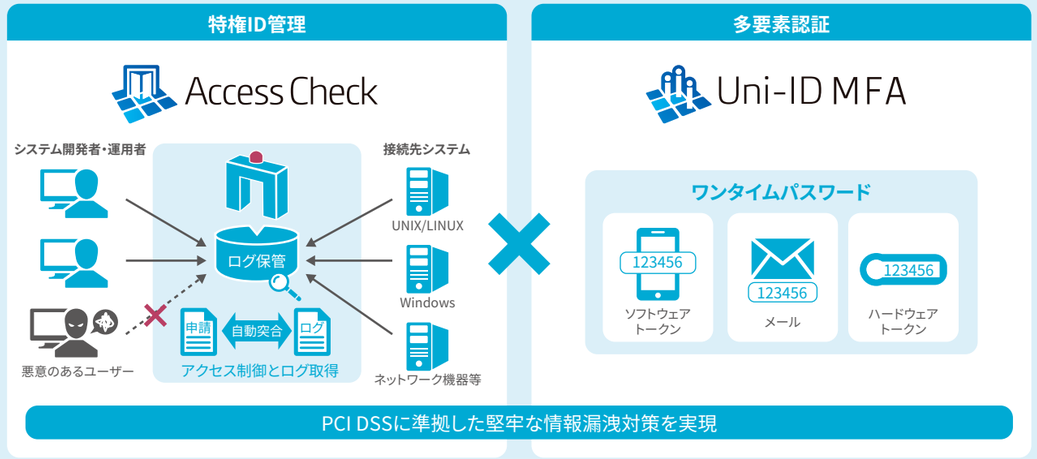
仕様の国際標準化により、様々なベンダー製品との相互互換性があります。

ワンタイムパスワードの利用が有効なユースケース

Use Case 1

PCI DSS※2 v3.2における多要素認証要件への対応

特権IDの不正利用による情報漏えい事件・事故は後を絶たず、その厳格な管理が求められています。クレジットカード業界向けのセキュリティ国際基準であるPCI DSS v3.2 の要件8.3では、管理者アクセスの「多要素認証」が必須要件となり、統制環境の整備が急務になっています。NRIセキュアテクノロジーズでは、特権ID管理ソリューション「SecureCube/Access Check」に多要素認証エンジン「Uni-ID MFA」を連携させることで、PCI DSSに準拠した堅牢な情報漏洩対策を実現しています。



Use Case 2

ECサイトにおけるユーザー認証の強化

増加するクレジットカード番号等の漏洩や不正使用被害の実態を踏まえ、2018年6月に改正割賦販売法が施行されました。これにより、カード加盟店は、カード番号等の適切な管理と不正使用の防止対策が義務付けられ、この実務ガイドラインである「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」に準拠した不正使用対策を講じる必要があります。当ガイドラインでは、ECサイト等の非対面取引における不正使用対策として、ワンタイムパスワードの利用が有効な対策として記載されています。
また、不正ログイン、不正取引対策としてもワンタイムパスワードは極めて有効です。

※1 OATH：Initiative for Open Authenticationで定義されているオープンスタンダードで強固な認証基盤（フレームワーク）の規格。 https://openauthentication.org/
TOTP：Time-based One-Time Password algorithm. IETFが発行するRFC6238で規定されているワンタイムパスワード認証に関する国際標準仕様。
※2 PCI DSS（Payment Card Industry Data Security Standard）：クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準。（2016年4月に発表された PCI DSS v3.2が最新）