

SafeNet OTP 111 および SafeNet OTP 112

安全性とコンプライア
ンスを両立する認証
ソリューション

SafeNet OTP 111 および SafeNet OTP 112 は、OATH 認証を取得したワンタイムパスワード(OTP)デバイスであり、多様なシステムやサービスへのユーザー認証を強化します。時間ベースおよびイベントベースの構成に対応し、防水仕様の筐体を備えたこれらのトークンは、従来の固定パスワードを使用している環境に容易に導入でき、セキュリティの向上と業界規制への対応を同時に実現します。

本製品は、実績ある SafeNet OTP 110 トークンの後継モデルとして位置づけられており、OTP 111 は完全な下位互換性を提供し、OTP 112 は最新の認証規格に準拠しています。SafeNet OTP 111 は SafeNet OTP 110 の後継として、SafeNet OTP 112 は eToken PASS の代替として、それぞれ展開されています。



クラウド、VPN、オンプレミス環境 への安全なアクセスの確保

OTP(ワンタイムパスワード)認証は、固定パスワードに伴うセキュリティリスクを排除し、ユーザーアクセス制御の強化に寄与します。本認証方式は、以下のような多様な環境における安全なアクセスを実現します：

- ローカルネットワークへのアクセス
- リモートネットワーク(VPN)への接続
- クラウドベースのアプリケーションの利用
- 仮想デスクトップインフラ(VDI)へのログイン
- Webポータル利用
- カスタムアプリケーションの保護

OTP認証の導入により、これらのシステムに対する不正アクセスのリスクを低減し、全体的なセキュリティレベルの向上が期待されます。

SafeNet 認証サービスソリューション によるサポート

SafeNet OTP 111 および SafeNet OTP 112 トークンは、SafeNet Authentication Service Private Cloud Edition (SAS PCE)および SafeNet Trusted Access(STA) ソリューションと連携し、高度に自動化されたセキュアなワンタイムパスワード(OTP)認証を提供します。柔軟なトークンオプションにより、各組織のニーズに応じた導入が可能であり、運用コストの大幅な削減を実現します。

SafeNet OTP 111-112 OTP デバイスの主な特長と利点

市場規制への準拠

- MFA(多要素認証)システムで使用可能
- OATH 認証済み

持ち運びやすい

- キーリングに付けて持ち運び可能

簡単に使用できる

- PC 不要: ボタンを押すだけで OTP を取得

さまざまなシステムへの安全なアクセス

- ネットワーク(VPN)
- SaaS アプリケーション
- VDI
- ウェブポータル
- カスタムアプリケーション

管理が容易

- 簡単なバックエンド構成
- 低メンテナンス
- 長寿命バッテリー
- 頑丈な設計

カスタマイズ可能

- ケースカラー
- ロゴ
- OTP 桁数
- イベントまたは時間ベース

• SafeNet Trusted Access(STA)

クラウドベースのアクセス管理サービスであり、ポリシーベースのアクセス制御および多要素認証(MFA)を提供します。多様なトークンの一元管理、保守、導入を可能にし、クラウド環境におけるセキュリティ強化を支援します。

- **SafeNet Authentication Service Private Cloud Edition (SAS PCE)**

オンプレミス環境向けの認証管理ソリューションであり、企業ネットワークの境界を越えた認証サービスの拡張を可能にします。ユーザーは、社内ネットワークで使用しているユーザーIDおよびトークンをそのまま利用して、安全に認証を行うことができます。

OTP（ワンタイムパスワード）とは

OTP(One-Time Password／ワンタイムパスワード)とは、1回限り有効な認証コードを使用するセキュリティ手法です。従来の静的なパスワードに代わり、ログインやトランザクションごとに異なるコードを生成・使用することで、不正アクセスのリスクを大幅に低減します。

この一時的なパスコードは、一定時間または1回の認証操作に限って有効であり、使い捨てであるため、パスワードの漏洩やリプレイ攻撃に対する高い耐性を備えています。

OATH（Open Authentication）とは

OATH(Initiative for Open Authentication) は、強固な認証技術の普及と標準化を目的として、複数のセキュリティベンダーによる業界横断的な協力のもとに策定された、オープンな参照アーキテクチャです。

このアーキテクチャは、ITおよびセキュリティ分野の専門家が、既存のインフラストラクチャに強力な認証機能を統合する際のガイドラインまたはテンプレートとして活用されており、相互運用性の高い認証ソリューションの実現を支援します。

SafeNet OTP 111 および 112 の OATH 認証対応

SafeNet OTP 111 および SafeNet OTP 112 は、いずれも OATH(Initiative for Open Authentication) に準拠したハードウェアトークンです。これらのトークンは、OATH によって定義されたオープンな認証標準 (HOTP/TOTP) に基づいて設計されており、相互運用性と高いセキュリティを両立しています。

OATH 認証を受けていることで、SafeNet トークンは他の OATH 準拠システムとの統合が容易であり、幅広い認証基盤に対応可能です。

SafeNet OTP 111/112 は MFA/2FA ですか？

いいえ。これらは 1FA トークンであり、MFA システムに統合することができます。

SafeNet OTP 111/112 の Thales プラットフォームとの互換性

SafeNet OTP 111 及び SafeNet OTP 112 は、Thales の認証プラットフォームである SafeNet Trusted Access (STA) および SafeNet Authentication Service Private Cloud Edition (SAS PCE) と完全

な互換性があります。これにより、両トークンはクラウドおよびオンプレミス環境における多要素認証ソリューションとして柔軟に導入可能です。

詳細については、以下の技術文書をご参照ください：

- [SafeNet Trusted Access 技術文書]
- [SafeNet Authentication Service Private Cloud Edition 技術文書]

SafeNet OTP 111 および 112 による VPN／VDI 認証の対応

SafeNet OTP 111 および SafeNet OTP 112 は、VPN (Virtual Private Network) および VDI (Virtual Desktop Infrastructure) 環境におけるユーザー認証に対応しています。これらのトークンは、SafeNet Trusted Access (STA) および SafeNet Authentication Service Private Cloud Edition (SAS PCE) と互換性があり、RADIUS、SAML、LDAP などの標準プロトコルを通じて、多要素認証 (MFA) を実現します。

これにより、企業ネットワークやリモートアクセス環境において、より高いセキュリティレベルを確保することが可能です。

SafeNet OTP 111／112 の動作概要

SafeNet OTP 111 および SafeNet OTP 112 は、ワンタイムパスワード (OTP) を生成するハードウェアトークンです。これらのトークンは、ユーザー認証の際に以下のように機能します：

1. ユーザー認証の開始

ユーザーが VPN、VDI、またはその他の保護されたデジタルリソースにアクセスする際、ユーザー名とともに、トークンによって生成された一時的な数値コード (OTP) を入力します。

2. OTP の検証

入力された OTP は、バックエンドの認証サーバー（例：SafeNet Authentication Service や SafeNet Trusted Access）によってリアルタイムで検証されます。

3. アクセスの許可

OTP が正当であると確認された場合、ユーザーは対象のシステムまたはアプリケーションへのアクセスを許可されます。

このプロセスにより、静的なパスワードに比べてセキュリティが大幅に強化され、不正アクセスのリスクを低減します。

SafeNet OTP 111 と SafeNet OTP 112 の違いは何ですか？

SafeNet OTP 111 および SafeNet OTP 112 は、いずれも Thales のハードウェア OTP トークンですが、主な違いは使用されているOTP 生成アルゴリズムにあります。

トークン名	対応アルゴリズム
SafeNet OTP 111	HMAC-SHA1 (HOTP/TOTP)
SafeNet OTP 112	HMAC-SHA256 (HOTP/TOTP)

これにより、セキュリティポリシーやシステム要件に応じて、より強度の高いハッシュアルゴリズム(SHA256)を必要とする環境では OTP 112 が推奨されます。

SafeNet OTP 110 とは

SafeNet OTP 110 は、SafeNet OTP 111の前世代にあたるハードウェアベースのワンタイムパスワード(OTP)トークンです。ユーザー認証のために一時的な数値コードを生成し、セキュアなアクセス制御を実現します。

このトークンは、HMAC-SHA1 アルゴリズムに基づく OTP を生成し、SafeNet 認証プラットフォーム(例: SafeNet Authentication Service や SafeNet Trusted Access)との互換性を備えています。後継モデルである OTP 111 は、セキュリティや機能性の向上を目的として設計されていますが、OTP 110 も引き続き多くの環境で使用されています。

HOTP (HMAC-Based One-Time Password) とは

ハッシュベースの OTP (HOTP): ハッシュアルゴリズムに基づいて生成される OTP で、ユーザーに送信されます。OTP コードは、ユーザーがアクセスするたびにインクリメンタルに変化するカウンターと同期します。

TOTP とは何ですか？

時間ベースの OTP (TOTP): OTP コードが有効となる時間枠を提供します。通常、時間間隔は 30～60 秒です。ユーザーが指定された時間内に OTP コードを入力しなかった場合、新しいコードを要求する必要があります。

Thalesについて

今日の企業や政府機関は、クラウド、データ、ソフトウェアを積極的に利用して、信頼できるデジタルサービスを提供しています。世界中の有名企業や組織がThalesを採用し、クラウドやデータセンター、さらには、デバイスやネットワークまでのあらゆる場所に作成、保存、アクセスする機密情報やソフトウェアを保護しています。データセキュリティ、ID/アクセス管理、ソフトウェアライセンスのグローバルリーダーであるThalesのソリューションは、安全なクラウドへの移行とコンプライアンスの確実な達成を支援し、ソフトウェアから多くの価値の創出、数百万人のユーザーへのシームレスなデジタルエクスペリエンスの提供を可能にします。