Swivel 認証ソリューション

AuthControl Sentry®

使いやすさとセキュリティを両立した トークンレス / 二要素認証ソリューション

使いやすさとセキュリティを両立した PINsafe® テクノロジーを核とし、リスクベース認証やソフトウェアトークンによる認証にも対応。クラウド・オンプレミスなど、柔軟な導入方法に対応した英 Swivel Secure 社のトークンレス/二要素認証ソリューション

swivelsecure

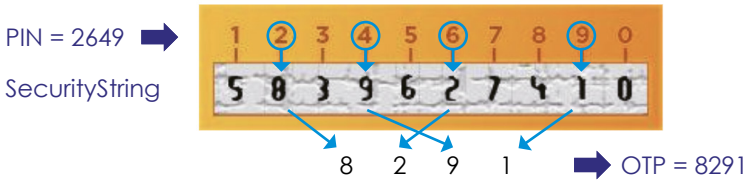
目から鱗の新方式！覚えやすくセキュアな
トークンレスワンタイムパスワード

形やパターンでワンタイムパスワード（OTP）を生成する方式とは異なり、Swivelでは4～10桁のPIN番号を使用して、ユーザが頭の中で、またはシステムが自動的にOTPを生成して認証を行います。

会社の認証用途でしか使用しない「形」を覚えることは、ユーザにとっては苦痛でしかありません。そのため、覚えやすい簡単な形にする、紙に書く等のセキュリティリスクが発生することに繋がっています。

その点、4桁の数字であれば「絶対に忘れない」コードを誰でも数種類は持っているはずです。これをうまく使えるならば、紙に書く必要はありません。

Swivelはその点に着目し、PIN番号から動的にOTPを生成できるPINsafe®を開発しました。PINsafeではPIN番号そのものは絶対にネット上に流れることはありません。認証方式は「TURingイメージ」「PINPad」から選択できます。

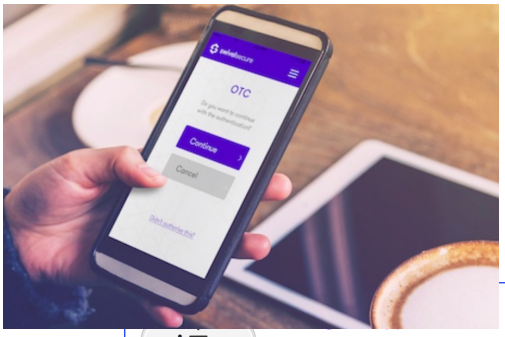


■ TURingイメージの使い方
PINsafeは1~0の数値に対応したランダムな文字列（SecurityString）を生成します。（SecurityStringは認証の度に異なる配列の文字列で、数字の他にアルファベットも使用可能です）PINの順番に上段の固定数字を見て、その下にある文字列を入力すると、それが１回限り有効なOTPになります。
例えば上の例では、ユーザが覚えているPINが「2649」の場合、ユーザはSecurityStringの2番目、6番目、4番目、9番目の値を読み取り、「8291」がOTPとなります。

■ PINPadの使い方
PINPadでは、パッドに毎回異なる配列の数字が表示され、ユーザがPINを入力するだけでシステムがOTPを自動生成し、安全に認証を行います。
この例の場合、ユーザはパッドの「2649」を順番にクリックすることで認証されます。PINPad認証は直感的な操作が可能で、ATMでお金を下ろすことができるユーザであれば、誰でも簡単かつセキュアに認証を行うことができます。

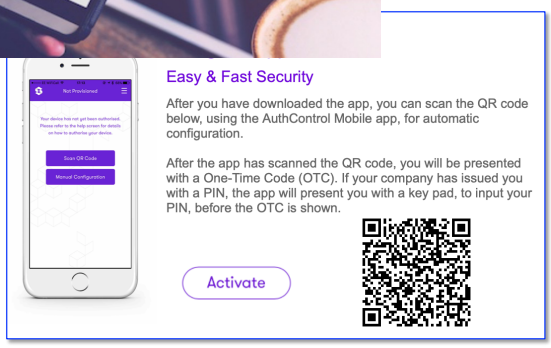
Swivel 4

管理負荷・運用コストも心配無用の
ソフトウェアトークン



トークンを使用した二要素認証では、トークンのユーザとの紐付け作業（プロビジョニング）が管理者の手作業になってしまうために、管理・運用工数が大きな負担になってしまいます。また、ハードウェアトークンの場合、コストも大きな負担となる恐れがあります。

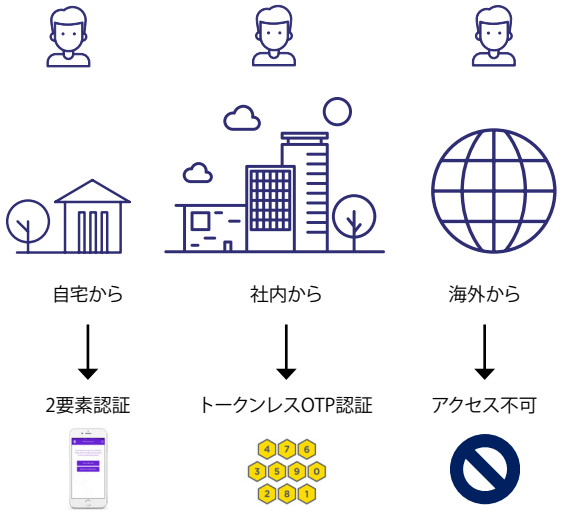
Swivelでは、サーバに登録されたユーザに送られてくるQRコードをスマホで撮影するだけで、ソフトトークンのセットアップとプロビジョニングを自動的に行うことができます。



ユーザ自身の簡単な操作でプロビジョニングを完了できますので管理者の工数を限りなくゼロにすることができます。

もちろん、モバイルアプリ（ソフトウェアトークン）の費用は無料です。

利用条件に応じて適切な認証方法を自動適用する
リスクベース認証



■ リスクベース認証の適用イメージ
アクセス元(社内・社外・海外)、アクセスするデバイス(家庭PC、会社PC、不明)、アクセス時間帯(業務時間内、深夜)、ユーザの権限などによりリスクスコアを設定し、トータルのスコアに応じて認証方法を自動適用します。また、アクセスするアプリケーション毎に閾値を変えることも可能で、オフィスソフトなら低いスコアでもアクセス可能にし、業務ソフトは閾値を上げるなど、きめ細かい設定が可能です。

ユーザ認証は、セキュリティレベルを上げると利便性が下がり、利便性を上げるとセキュリティレベルが下がってしまいます。

Swivelの「リスクベース認証」は、常に同じセキュリティレベルと使い勝手をユーザに強いるのではなく、その時の利用条件に応じた認証方法を自動的に選択できます。

具体的には

- どこからのアクセスか(社外/社内 等)
- 何を使用してアクアセスしているか
- どの時間帯でのアクセスなのか
- どの国からアクセスなのか
- ユーザの権限(所属するSecurity Group)

の組み合わせによってリスクスコアを計算し、最適な認証方法を自動的に選択します。

例えば、同じWebアプリケーションへのアクセス認証でも、社内から会社貸与のPCを使用してアクセスしてきた場合にはPINPadを使用したトークンレスOTP認証を行い、社外から個人PCを使用してアクセスしてきた場合には、ソフトトークンを使用した二要素認証を行う。海外からのアクセスは禁止、といったことが可能になります。

4つの特長

クラウド・オンプレミスなど
様々な導入方法を選択可能

Swivelでは導入方法として

- Swivel Cloud
- オンプレミス(仮想アプライアンス)
- MSP専用システム(仮想アプライアンス)

を選択可能です。

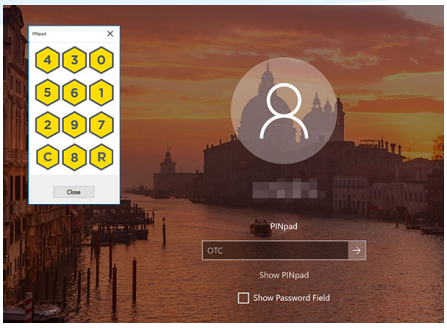
Swivel Cloudは共用クラウドではなく、お客様専用のクラウド基盤にお客様専用のサーバやDBを構築してサービスとしてご提供します。Swivel Cloudは日本リージョンも選択可能です。

オンプレミスシステムの場合はVMware、HyperV、Xen Serverに対応した仮想アプライアンスでご提供します。仮想アプライアンスにはサーバOS、Swivelアプリケーション、ユーザデータベース、各種サービスをオールインワンパッケージしていますので、サーバの構築はお客様の仮想基盤に仮想アプライアンスをデプロイするだけで完了します。仮想アプライアンスはお客様の規模や可用性に応じて、「Standard Appliance」「A/A(冗長) Appliance」「DR Appliance」を選択可能です。

MSP専用システムはサービス事業者様向けのシステムで、各クライアント向けのサーバをGUIでワンタッチで増設や削除することができ、ライセンスやログを集約管理・運用することができます。

Swivelのその他の特徴

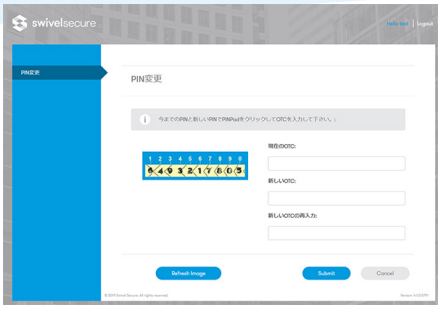
Windowsログイン認証に対応



Swivelは、Windows10やWindows8のログイン認証で使用することができます。

認証はPINPadやTURingイメージを使用したトークンレスOTPに対応しています。また、パスワードキャッシュをサポートしていますので、Windowsのログイン認証をIDとOTPのみで行うことができます。さらにサイレントインストールにも対応しており、大規模なユーザのWindows環境のセキュリティ向上にご使用いただけます。

日本語対応

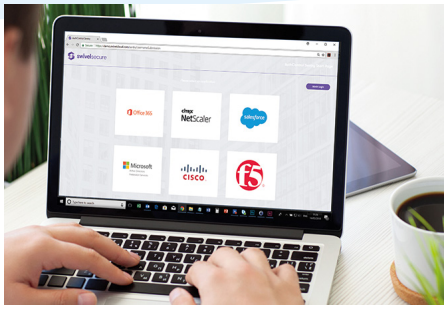


Swivelはエンドユーザが触れる全ての画面（モバイルアプリ(ソフトトークン)、ユーザポータル、システムから配信するメール、SAML認証画面）の日本語表記に対応しています。またそれらはお客様によるカスタマイズが可能です。

HOTP/TOTPトークンを選択可能

OTPの生成アルゴリズムにはカウンターベース方式(HOTP)、時間ベース方式(TOTP)があります。一般的にHOTPの方がセキュリティレベルが高いと言われていますが、Swivelのハードトークンはどちらかの方式を選択することができます。

SAML IDPとして活用可能



SwivelはSAMLの認証基盤として使用でき、SAMLのIDPとしてID管理の基盤として使用することができます。

さらにSwivel独自の固定パスワードを設定・管理・運用も可能です。

SECURITY STRINGS
AUTHORIZED VALUE ADDED DISTRIBUTOR
セキュリティストリングス株式会社

〒 102-0082 東京都千代田区一番町 6 番地 相模屋本社ビル 7F
Email: sales@securitystrings.com
URL: https://www.securitystrings.com

お問合せ

©2019 Security Strings 本カタログに記載の会社名、商品名は各社の商標または登録商標です。
本カタログに記載されている情報は 2019 年 10 月現在のものであり、製品仕様および機能は予告なく変更される場合があります。予めご了承下さい。