AuthControl Sentry®

英国＆アイルランド(UK & Ireland)
・オフィス
North
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA

HQ: +44（0) 1134 860 123
Support: +44（0) 1134 860 111
hq@swivelsecure.com

South
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

米国＆アジア・パシフィッ
（USA & APAC）・オフィス
Seattle
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle, WA 98154

+1 949 480 3626（Pacific Time）
Toll Free: 866.963.AUTH（2884）
usa@swivelsecure.com

EMEA（Europe & Middle East）
オフィス

ポルトガル
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H, Piso 0,
2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

スペイン
Calle Punto Mobi 4,
28805 Alcala de Henares
Madrid

+34 911 571 103
espana@swivelsecure.com

インテリジェントな認証技術でIDを保護します

PINsafe® テクノロジーをコア技術に使用し、究極のセキュリティとリスクベース認証を実現します。AuthControl Sentry® 数々の受賞歴があり、ダイナミックコントロールを提供する認証ソリューション。ビジネス向けにインテリジェントな多要素認証ソリューションを提供します。

swivelsecure

www.swivelsecure.com/jp

swivelsecure

AuthControl Sentry® インテリジェントな多要素認証ソリューション

AuthControl Sentry®は世界52カ国以上にビジネス展開され、各国政府機関、金融、医療、教育、製造、流通等の組織/企業で使用されています。

非常に優れた多要素認証技術により、アプリケーション/データへの不正アクセスを防御します。

AuthControl Sentry®のソリューション・ダイアグラムを見るためにQRコードをキャプチャしてください。企業/組織に完成された多要素認証ソリューションをご提供します。

AuthControl Sentry®には、さまざまなアーキテクチャ要件をサポートする柔軟性があり、また幅広い認証要素の選択肢があることにより、多くのお客様の要求仕様にお応えできる能力があります。モバイルアプリケーションを使用するのか、もしくは最新の指紋リーダーを使用した生体認証を使用するか、AuthControl Sentry®はサイバーセキュリティ業界をリードするソリューションとして地位を確立しています。

何が違うのでしょうか

- 究極のセキュリティを提供する特許取得済みPINsafe®テクノロジー – 8ページをご参照ください。
- 全てのアーキテクチャーは、オンプレミスとCloudでご利用可能です。
- シングルテナントと単一階層型Cloudソリューションは、最適化されたカスタマイズと制御を保証します。
- 標準機能としてリスクベース認証とシングルサインオン(SSO)を提供します。
- 多くのアプリケーションとシームレスに統合可能です。
- 広範な認証要素(最大10要素まで)の導入を保証します。

Office365へのログイン、Eコマースによる取引、在庫管理のためのERPへのアクセスなど、すべての企業ユーザに対する認証アクセスをします。

✓ 従業員　✓ 顧客

✓ サプライヤー

アーキテクチャ

可変的アーキテクチャのオンプレミスとCloudをサポートします。

AuthControl Sentry®には制限はありません。Cloud、またはオンプレミスのアプリケーションのいずれでも、ユーザーが顧客、従業員、またはサプライヤーの誰でも、アクセスを認証するように設計されています

オンプレミス・アーキテクチャ

Swivel Secure社提供のAD Agent経由で社内システムへアクセスし、ローカルにインストールされたソフトウェア・アプリケーションは、インターネット経由でADを共有する必要がなく、ユーザーアカウントの同期も維持します。

Cloudベース・アーキテクチャ

固定IP：各顧客のAuthControlは、それぞれの仮想インスタンス用に専用の固定IPを保持します。共有リソース、共有API、共有エントリポータルまたは共有DBはありません。

専用サービス：AuthControl Cloudは顧客専用の仮想マシンを提供します。 共有型のマルチテナントサービスではありません。つまり、顧客のニーズに合わせたソリューションを柔軟に構成/構築出来、個別の維持管理が可能です。

プライベート・ファイアウォール：顧客毎に専用の独立したファイアウォールを提供し、セキュリティとアクセス制御リストをカスタマイズすることが出来ます。

機能

シングルサインオン（SSO） – 標準機能

AuthControl Sentry® のシングルサインオン（SSO）機能は、ユーザが全てののアプリケーションに一回の認証プロセスでアクセス出来る機能であり、ユーザはセキュリティを損なうことなく効率的に作業出来ます。

継続的なセキュリティ

Swivel Secure社は、ユーザにスムーズなアクセスを提供する統合ポータルを提供します。 この単一アクセスポイントを使用することにより、ユーザの特権を管理し、監査目的で動作を追跡、セキュリティを強化し、説明責任を果たすことが出来ます。

費用対効果

ITサポートデスクへのパスワード関連の問い合わせが無くなるため、SSOを利用することで大幅なTCOを実現出来ます。 ユーザが一回のログインで許可された全てのアプリケーションにアクセスすることが出来、結果として生産性が向上し、時間を節約出来ます。

直感的

SSOは、リスクベース認証のポリシーエンジンを使用して、一回の認証でユーザが全てのアプリケーションにアクセス出来るようにすることで、効率を高めるように設計されています。 ユーザがVPN、オンプレミス、またはCloudのどのアプリケーションにアクセスしても、統合ポータル内の直感的なSSO機能を使用して認証するように自動的に指示されます

認証のためAuthControl Sentry®を構築します：

- 従業員，サプライヤー、顧客など全ての利用者
- Office365、Salesforce、SAPなどのアプリケーションへのアクセス
- 金融サービスなどの特定の市場

機能

リスクベース認証（標準機能）

リスクベース認証は、AuthControlSentry®のダイナミックな機能であり、アプリケーションにアクセスするために適切なレベルの認証を自動的に要求するように設計されています。ポリシーエンジンで設定されたパラメーターに基づいて、リスクベース認証はユーザ、使用デバイス、およびアプリケーションに基づいた適切なレベルの認証を要求して、アプリケーションにアクセスします。

ダイナミック＆インテリジェント

以下のユーザ環境に適応します：

- どのようなアプリケーションにアクセスしようとしているのか
- どのようなグループメンバーに属しているのか
- どこからアプリケーションにアクセスしているのか
- どのようなデバイスを使用しているのか

ポリシーエンジン

ポイントシステムに基づいて、認証ポリシーエンジンにより、管理者はユーザ毎、アプリケーション毎にパラメータを設定出来ます。

- グループメンバー
- アクセスしているアプリケーション
- IPアドレス
- 最終認証
- X.509証明書
- 使用デバイス
- 所在地（GeoIP）
- Geo Velocity

リスクベース認証：例1

T購買アシスタントは、購買マネージャーと一緒にサプライヤを訪問するために、東南アジアに出張しました。彼女はレストランで食事を終えた際、翌日の会議のためにいくつかの部品在庫を確認するのを忘れていたことに気付きました。 彼女は会社提供のモバイルデバイスを使用して、ERPシステムにすばやくログインを試みました。

ERPシステム	
120ポイント必要（アクセス許可に）	
LAN	0ポイント
既知のIP	0ポイント
マネージデバイス	50ポイント
IP範囲（アジア）	-100ポイント
認証要求	
U&P	10ポイント
モバイルアプリ	60ポイント
指紋	20ポイント

結果 – 失敗

彼女は会社提供のデバイスを使用してERPにアクセスを試みましたが、IP範囲は設定ポリシーの範囲外のため-100ポイントとなります。 多要素認証の使用に関係なく、合計ポイントが認証に必要な120ポイントに足らず、ERPへのアクセスは許可されませんでした。

リスクベースの認証：例2

営業マネージャは、今日オフィスで働いており、会議の後にCRMに商談を作成するためにアクセスしようと考えています。 会社提供のノートPCを使用し、オンプレミスにあるCRMアプリケーションにアクセスします。

CRMシステム	
120ポイント必要	
LAN	50ポイント
既知のIP	50ポイント
マネージデバイス	50ポイント
IP範囲（日本）	50ポイント
認証要求	
U&P	10ポイント
モバイルアプリ	60ポイント
指紋	20ポイント

結果 – 成功

営業マネージャは明らかに、CRMにアクセスするために必要な（合計）ポイントを超えていてアクセス可能となります。認証されると、シングルサインオン（SSO）を使用して他のアプリケーションにもアクセスすることが出来ます。

究極の柔軟性と制御機能

ポリシーエンジンを使用すると、新しいルールを作成して既存のルールと組み合わせたり、複雑さが増した様々なシナリオをサポートし、ポリシーとして実装することが出来ます。

機能

ユーザ・ポータル

ユーザ・ポータルはAuthControlSentry®の機能です。管理者に基本的な自己管理タスクをユーザに任せることが出来るソリューションを提供します。

ユーザが直接ユーザ・ポータルにアクセス出来るようになり、PINの変更やリセット、モバイルアプリのプロビジョニングなどの定期的な要件をユーザ自身が実行出来るようになります。

モバイルアプリのプロビジョニング

ユーザがPINを変更、及びリセット出来るようにするだけでなく、モバイルアプリも簡単にプロビジョニング出来ます。 ユーザにモバイルアプリのプロビジョニング手順の詳細と設定用のQRコードがメールで送信されます。 プロビジョニング後、ユーザはワンタイムコード（OTC）又はプッシュ通知を使用して、通常のアプリケーションへのアクセスを認証することが出来ます。。

セルフサービス

セルフサービスのユーザーポータルは、これらのアクションのサポートの提供に通常関連するコストを削減します。

より良い効率性

Swivel Secureのユーザ・ポータルは、ユーザが次のような基本的な要件をユーザ自身で実行出来るように(効率を高めるように)設計されています。

- PINの変更
- PINのリセット
- モバイルアプリのプロビジョニング
- ハードウェアトークンの再同期 .

ポリシーが確実に実行されるように制限事項を実装し、アクションがセキュリティプロトコルに従っていることを確認出来ます。

技術

PINsafe®：特許取得技術

PINsafe®は、AuthControl Sentry®で利用可能な一連の認証要素である画像認証要素PINpad®、PICpad、およびTURingの背後にある特許技術です。企業/組織で使用するアプリケーション、ネットワーク、データ等への不正アクセスから保護するために設計された多要素認証ソリューションです。

PINsafe®はどのように機能するか

各ユーザはPIN番号を設定します。しかし、このPIN番号は入力しません。

ユーザが安全に認証をする必要がある場合、ユーザに10桁のセキュリティ文字列(ランダムな文字列または数字)が送信されます。 セキュリティ文字列は、グラフィック、すなわちTURing、PINpad®、又はPICpadを表示するか、電子メール、又はSMSで送信することが出来ます.

PINを位置インジケータとして使用することにより、認証用のワンタイムコードを抽出出来ます。

例えば、

以下の例では、PINが1370であることを示しています。この場合、セキュリティ文字列は5721694380であるため、ログインコードは5240となります。

セキュリティ文字列は、完全な柔軟性を実現するために様々な方法で多くのデバイスやアプリケーションと連携することが出来ます。
例えば：

- Windowsにログイン
- F5、Citrix、NetScaler、Cisco VPN等によるリモートアクセス
- OWA、Apache、Microsoft ILS等のWebアクセス

PINsafe®は、ユーザがPINを入力する必要がないため、中間者(Man-In-The-Middle)攻撃などの侵入を防ぎます。

要素

認証要素

Swivel Secureは広範囲で使用可能は認証要素を提供し、各企業/組織で最大限に活用されますようご支援いたします

モバイルアプリ（AuthControl Mobile®）でOTCを使用して認証するか、従来のハードウェアトークンを使用するか、指紋を使用するかを問わず、Swivel SecureのAuthControl Sentry®は、皆様のビジネスのセキュリティニーズに合わせて究極のセキュリティと容易な導入形態を提供します。

AuthControl Mobile®: OTC

認証する度に、アプリに表示されるOTCを使用するだけです。 99個のコード（プリインストールされた）があるため、OTC機能は汎用性が高く、オフラインで使用出来ます。 コードを入力すると、アプリケーションへのアクセスが許可されます。

Image factor: PINpad®

10桁のコードは、ユーザのWebブラウザーに番号グリッドの形式で表示されます。ユーザは、PINを表す画像をクリックするだけです。 クリックされた各画像は、異なるOTCコードをAuthControl Sentry®に送信してユーザを認証します

Image factor: PICpad

PICpadは、様々なユーザの多様化する言語環境に対して、通常のオプションを超越する認証要素です。

PINpad®と同じ原理を使用して、PICpadは数字ではなく絵を表示し、多国籍環境でも使用出来るソリューションを提供します。

AuthControl Mobile®: PUSH

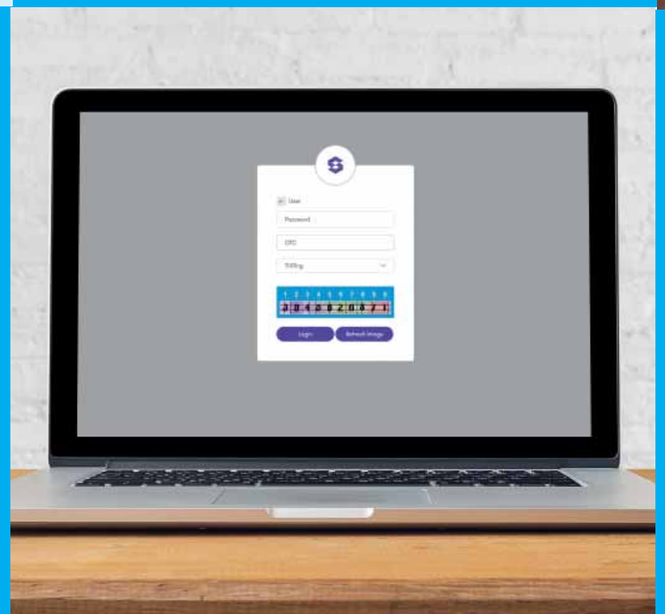
モバイルアプリのボタンを押すだけで、モバイルに直接送信される通知で認証を確認出来ます。

最小限の設定でSwivel OneTouch®機能を迅速に実装出来ます。

Image factor: TURing

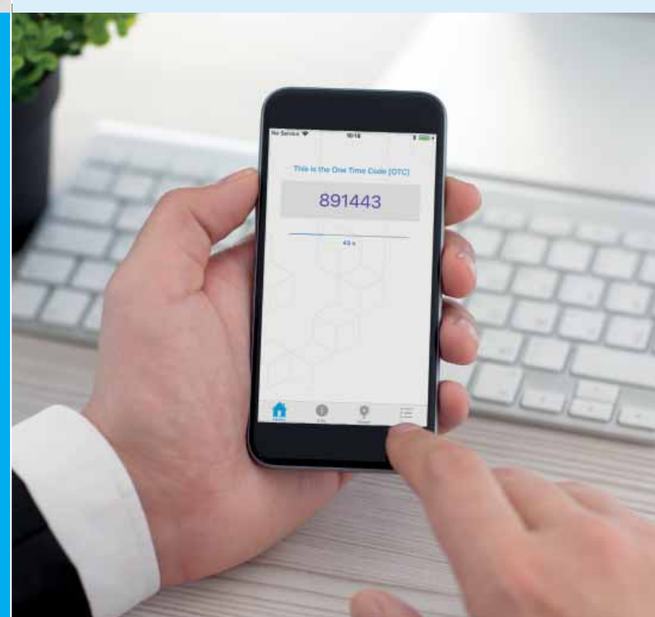
10桁のコードは、ユーザのウェブブラウザー上に長方形の画像形式で表示されます。ユーザは、PIN番号で表される文字（番号）を取得します。

例：PINが1370の場合、提示された画像から1番目、3番目、7番目、および10番目の文字を取得します



AuthControl Mobile®: OATH

OATHソフトトークンは、0から60までカウントする時間ベースのトークンであり、VPNを介してアプリケーションにアクセスするために使用される従来のハードウェアトークンに似ています。 OATH準拠のソフトトークンは、認証する6桁のコードをユーザーに提供します。



Mobile: SMS

OTCを（SMSを介して）不正な傍受から保護するために、SMSはPINsafe®によって保護されています。 つまり、SMSには2つの英数字シーケンスのセキュリティ文字列が含まれており、ユーザのPINと組み合わせるとOTCが提供されます。

Biometrics（指紋）

指紋認証は、Windows10生体認証フレームワークとNITGEN指紋認証アクセスコントローラーを使用して、AuthControlCredential® Providerで利用出来ます。 ユーザは、NITGEN指紋コントローラーまたはラップトップに組み込まれた指紋リーダーを使用して認証出来ます。

AuthControl Voice

ユーザに電話をかけ、AuthControl Voiceはワンタイムコード（OTC）またはプッシュ通知（YESまたはNO）を発声して、アプリケーションへのアクセスを認証します。電話の音声で配信されたOTCは、要求に応じてPC等のウィンドウに入力します。

Hardware token

HWトークンはユーザにワンタイムコード（OTC）を提供し、ユーザはアプリケーションに安全にアクセスすることが出来ます。 HWトークンのボタンを押す度に、新しいコードが提供され、不正アクセスが防止出来ます。

swivelsecure

連携

AuthControlSentry®は、市場で最も柔軟なソリューションの1つであり、RADIUS、ADFS、SAML、および独自のAPIであるAgentXMLを介して数百のアプリケーションおよびアプライアンスと連携することが出来ます。

Salesforceへのアクセス、モバイルアプリでの認証、又はTURing，PINpad®等を使用したWindowsへのログインが必要な場合でも、AuthControlSentry®は様々なアプリケーションとデバイスをサポートし、企業/組織全体でシームレスな認証に必要な柔軟性と効率性を提供することが出来ます。

ライセンス

全ての企業/組織に適した柔軟なライセンス形態と価格設定モデルです。 ライセンス費用は、指定ユーザ毎に課金されます。

ユーザ・ライセンス

全ての企業/組織に適した柔軟なライセンス形態と価格設定モデル。

- AuthControl Sentry®のライセンスはユーザ毎です。
- 各ライセンスには、全ての認証要素が含まれています
- 多要素認証、リスクベース認証、SSOはAuthControl Sentry®に含まれています
- 1年間、3年間、5年間等の複数年契約で利用可能です

オンプレミス

オンプレミスソリューション、またはプライベートクラウドでホストされるソリューションのライセンスはサブスクリプション形式です。 価格設定は、ユーザ毎にスライドスケールで、最小10ユーザーから利用可能で、ユーザ数が大きくなれば、ユーザ単価は安くなり、大量のライセンスを購入する場合、非常に費用対効果の高い方法です。 費用をOPEXしたい企業に最適であり、利用ユーザ数が可変です。

Cloud

Cloud利用での費用はサブスクリプション形式で利用可能であり、企業は需要の変化に応じてユーザ要件を変更することが出来ます。 柔軟でペナルティのない契約および解約が可能です。 サービスコストをOPEXしたい企業に最適であり、利用ユーザ数が可変です。

ライセンスオプション

オンプレミス/Cloud・ライセンスのオプションを比較するには、以下の表を参照してください。

ライセンスの種類	オンプレミス	Cloud
リスクベース認証	✓	✓
連携手段（SAML / ADFS / RADIUS）	✓	✓
オンプレミスとCloudアプリケーション	✓	✓
すべての認証要素	✓	✓
AD Agent & AD Sync	✓	✓
統合ポータルサイト（SSO付き）	✓	✓
レポート	✓	✓
仮想アプライアンス	✓	✗
Amazon AWSイメージ	✗	✓
24x7x365	オプショナル	✓

サービス＆サポート

顧客が技術サポートと最新機能にアクセス出来るように、ユーザ向けにプレミアムレベルのサポートを提供しています。 アップグレード、実装、移行、複雑なシステム連携のためのプロフェッショナルサービス（有償）も利用出来ます。

プレミアムメンテナンス契約（サブスクリプション費用に含む）

サポート時間：24x365対応、年中無休のサービス。専門家によるサポートを直ぐに必要とするユーザに最適です。

プロフェッショナルサービス

Swivel Secureは、多要素認証を実装し、既存システム、又はアプリケーション等との互換性を確保する際に、別途技術リソースを必要とするユーザに様々なプロフェッショナルサービスを提供します。

テクニカルアカウントマネージャー（TAM）サービス

Swivel Secure TAMサービスは、プロアクティブな予防ガイダンスと一元化されたサービス管理を提供します。

Swivel Secureのアプライアンスをアップグレードする必要がありますか？

Swivel Secureは、アップグレード中に発生する可能性のある幾つかの問題を事前に認識し、サービスとビジネスの中断を最小限に抑えることを目的に開発されたアップグレードサービスを提供します。

多くの連携/統合が必要な、非常に複雑なネットワーク基盤がありますか？

当社のエキスパートエンジニアチームは、御社テクニカルアーキテクトおよびサービスデリバリーチームと緊密に連携して、以下ことを保証します：

- 提案は全て、御社ネットワークアーキテクチャに合わせて設計されます。
- 設計は、御社のアーキテクチャと変更管理の要件を満たしています。

新しいデバイスとRADIUS又はSAMLで連携/統合する必要がありますか？

弊社ソフトウェア開発者チームは、次のサポートを提供します：

- 新しい連携/統合の評価とその開発
- 新しいプラグインを導入する
- 機能要求に応じて、ソフトウェアを継続的に改善します。