正しい認証ソリューションを選択するために

概要

本ホワイトペーパーは、ここ 10 数年間のセキュリティ環境および認証技術の変化について俯瞰し、企業のアクセス管理システムがサイバー犯罪の進化についていけているかどうかを考えます。そして、自社の環境に合った適切な認証ソリューションを選択するために何を重視すべきかを検討し、企業がその最も価値ある資産を守るための方法をご提案します。

SecurityStrings

SWIVEL
the power of knowing

始めに

過去 10 年間で、インターネットの普及とモバイル技術の進化により、個人も企業も、コミュニケーションとビジネスの進め方が全く変わりました。これらの変化は効率化と生産性の向上をもたらしましたが、同時に全く新しいセキュリティ問題を引き起こしており、人々と企業に広範囲な影響を与えています。

本ホワイトペーパーは、ここ 10 数年間のセキュリティ環境および認証技術の変化について俯瞰し、企業のアクセス管理システムがサイバー犯罪の進化についていけているかどうかを考えます。そして、自社の環境に合った適切な認証ソリューションを選択するために何を重視すべきかを検討し、企業がその最も価値ある資産を守るための方法をご提案します。

認証技術から見た IT セキュリティ環境の変化

インターネットの基本的な部分は過去 10-15 年間変わっていませんが、ブロードバンド接続の普及と WiFi の登場、インターネットに接続するデバイスの増加とクラウドコンピューティングの出現が組み合わさり、現在のデジタル革命を引き起こしました。携帯電話が煉瓦ほどの大きさで、ほとんど会社との連絡にしか使われていなかったことや、昔は電子メールでは無く Fax に頼っていたことなど、もはや想像もできません。

また同じ時期、IT 技術は主に大企業や公的機関が彼らの手作業での管理業務 (特に会計処理) をサポートするためのものでした。しかし現在では、あらゆるビジネス活動が完全にネットワークに頼っており、そこにビジネスアプリケーションが集約されています。重要なデータには世界中のどこからでも、いつでもアクセスすることができます。

ほとんどのビジネスは、インターネットあるいはモバイルネットワークへのアクセスが無ければ、今日の相互に連結された市場から孤立してしまいます。しかし、そのためのアクセスを可能にするためには、本質的にはネットワークセキュリティ境界を取り除くか、少なくとも一部のユーザーに対してなんらかの VPN ゲートウェイ経由でアクセスを認めなければなりません。

こういった形態のリモートアクセスは 1990 年代に始まりましたが、当時は少数のユーザーに対して限定されたアクセス権を認めているだけでした。アクセスするためにユーザーは自宅の PC に専用のクライアントソフトを入れ、ユーザー名とパスワードで自分の身元を証明する必要があったのです。

21 世紀になると、企業はより多くの従業員にリモートアクセスを許可するために、これらの技術を強化しました。SSL VPN の登場により、ユーザーはインターネット接続とブラウザさえあれば、電子メールのチェックをしたり、重要な文書にアクセスできるようになりました。

この時すでに、ユーザーネームとパスワード (UNP: Username and Password) による認証では、ネットワーク管理者はそのユーザーが本物であるかどうかについて十分な信頼性を得られないことは認識されていました。そこで、ID トークンを使った二要素認証 (2FA: Two Factor Authentication) が生まれたのです。これらの二要素認証デバイスは、ユーザーがログインプロセスを完了するために UNP に加えて時刻同期されたワンタイムコードを提供します。この方式は、リモート環境においてユーザー ID を確認する方法としてはこの時点では極めて安全なものでした。

その後、ビジネス上の要望やブロードバンドや 3G ネットワークの普及により、自宅またはモバイルからのアクセスが指数関数的に増加し、多くの組織にコスト削減と生産性の向上をもたらしました。

こういった環境の変化の中で、トークンを使った認証の限界が明らかになると共に「ソフトウェアトークン」形態の複数要素認証が台頭し、より柔軟で安全なソリューションを、はるかに優れたコストパフォーマンスで提供できるようになりました。

現代の認証問題への対応

ここ数年で起きたネットワークアーキテクチャの大きな変化のひとつに、アプリケーションとデータが外部で「ホスト」されたことがあります。もはや、日々のビジネスを動かすサーバーが自社のビル内にあるかどうかはわかりません。それどころか、同じ大陸にさえ無いかもしれないのです。多くの企業が、中核となるネットワークやサーバー群をホステッドプライベートクラウドに移すか、SaaS モデルの利用に移行しています。

世界的な調査会社のガートナーは、2015 年までに企業の 70% がなんらかの形でクラウドまたは Web ベースのサービスを利用することになるだろうと予測しています。実際、ここ数年多くの組織が Microsoft Office Outlook Web Access を使ってメールをチェックし、CRM のために Salesforce.com を利用しています。ただ、それらをクラウドと認識することはほとんどありません。

> 「2015 年までに、企業の 70% がなんらかの形でクラウドまたは Web ベースのサービスを利用することになるだろう」
>
> ガートナー

こういった IT 投資の「オフショア化」アプローチを推進するためには、ユーザーがビジネスに必須のサービスにどのようにしてアクセスするか、あるいはリモートかつ仮想化された環境において IT 管理者が企業セキュリティをどのように制御するかについて、新しい考え方が必要になります。ユーザーは地球の裏側からアクセスしてくるかもしれないのです。

それはまた、ホステッドであれオンプレミスであれ、ネットワークリソースへの VPN アクセスに加えて CRM や Web メール、仮想デスクトップ環境を含む全てのアプリケーションについて、別々の認証手続きが必要になることを意味しています。このシナリオは、認証という側面から見た場合に、組織やユーザーに様々な問題を投げかけます。

クラウドへの移行

IT セキュリティの世界では、パスワードはハッカーに対してほとんど効果を持たないというのが共通の認識ですが、ほとんどのクラウドサービスにおいては、未だに UNP がデフォルトのユーザーログイン方法なのです。ハッカーに対して何らかの効果を持たせるためには、パスワードを非常に複雑にして、常に変更し続けなければなりません。しかしそうするとユーザーはそれをどこかに書き留めなければならなくなり、その時点でそれ自身が大きな脆弱性となってしまいます。

クラウドサービスのプロバイダーは、ユーザーがシンプルで簡単なアクセス手順を望んでいること、ログインプロセスにおけるほんのわずかな手間もサービス全体の評価を落とすことを知っています。これらのサービスにおいては「いくつかの基本的なルールに則った最低 6 文字から 8 文字の英数字の組合せ」がパスワードの要件として極めて一般的で、結果として、同じパスワードを全てのオンライン認証に使うことになります。これは、ある意味では仕方のないことです。

> 一人のユーザーは平均して 26 個の異なるアカウントを持ちながら、たった 5 種類の異なるパスワードしか設定していない
>
> Experian

大手の信用調査会社 Experian の依頼によって行われた 2010 年の調査によると、一人のユーザーは平均して 26 個の異なるアカウントを持ちながら、たった 5 種類の異なるパスワードしか設定していないということです。このレポートは、それが 2008 年に比べて 300% もオンライン詐欺が増加した理由だとしています。

この他の多くの調査結果も同様で、多くの人がソーシャルメディアとビジネスアプリケーションに同じパスワードを使っているということです。現代のセキュリティにおいて、パスワードの使い回し問題が急速に最大の問題になりつつあることは決して誇張ではありません。

アプリケーションに適切な認証プラットフォームを適合させる

ほとんどの IT セキュリティ管理者が、UNP ベースの認証が深刻な問題を抱えていることに同意しています。しかしその一方で、二要素認証ベースの認証ソリューションを企業の全ユーザーについて適用する事にもまた、いくつかの大きな問題が存在しています。コストの問題を無視するとしても、その他に多くの技術的、実務的、そしてセキュリティ上の問題があるのです。リスクとのバランスの問題で最も基本的な問いかけには、二要素認証は全てのアプリケーション、全てのユーザーにとって最適なソリューションなのか？というものがあります。

どのような組織にも、様々なユーザーのグループが存在し、職務上必要な企業データに対して各々のグループが別々のアクセスレベルを持っています。最高レベルの管理職は機密情報にアクセスできる必要があるが、一般の従業員は自分のメールや業務上必要なファイルのみにアクセスできれば良い、などです。組織の全員になんらかの ID トークンを配布するというのは、明らかに非現実的で、コストもかかります。

二要素認証における利用デバイスとして、携帯電話やスマホがキーホルダータイプのトークンに置き換わりつつあります。しかし、このような認証も、一日に一回デスクトップにログインするだけのユーザーにとっては最適なソリューションとは言えません。

VPN、Web、クラウドおよび VDI アプリケーションなどの様々な環境用の認証ポリシーと格闘しているセキュリティチームにとっては、こういった問題が自社の新たな脆弱性を生み出しかねません。これは Active Directory のようにユーザーリポジトリが集中管理された環境でも同様で、特にユーザーの登録 / 削除、あるいはトークンを忘れたユーザーへの対応のようなルーチン化されたタスクにおいて問題が発生する可能性があります。

しかし幸いなことに、認証技術は進化を続けており、これまでのようにたったひとつのトークンベースのソリューションを無理矢理に全てのケースに適用するような「万能サイズ」のソリューションでは無くなってきています。必要なところに二要素認証を提供し、リスクが低い環境向けにはより簡便な、しかし UNP よりは強力な認証を提供できるようになっているのです。

2FA か強力な認証か？

自社のネットワーク環境に最適な技術を選択する前に、IT 管理者は以下の様な基本的な質問に答える必要があります。

- 組織内の誰が、どのアプリケーションにアクセスする必要があるのか？
- アクセスするのは重要な機密データなのか？
- どこから (社内、自宅、モバイル) データにアクセスするのか？
- アプリケーションをホストして動作させているのはどこか？
- どのようなタイプのデバイスを使ってアクセスするのか？

これらの質問への回答が得られた時点で、組織にとって最適なソリューションへの方向性が見えてきます。そうして初めて、どのソリューションが最適かの検討を始められます。

その際に重要なのは以下の質問です。

- そのプラットフォームは幅広い認証レベルとユーザーの登録オプションをサポートしているか？
- ログインプロセスはユーザーにとって使いやすいか？
- そのシステムは既存のネットワークインフラと統合できるか？
- 同じシステムがコアネットワーク、デスクトップおよびクラウド内の全てのビジネスアプリケーションで利用できるか？
- ユーザーは複数の ID を持つ必要があるか？
- その技術は最新の PCI および GCSx CoCo 規制に準拠しているか？

これらの質問への答えが全て「Yes」であれば、最適なソリューションを見つけられたと言えるでしょう。

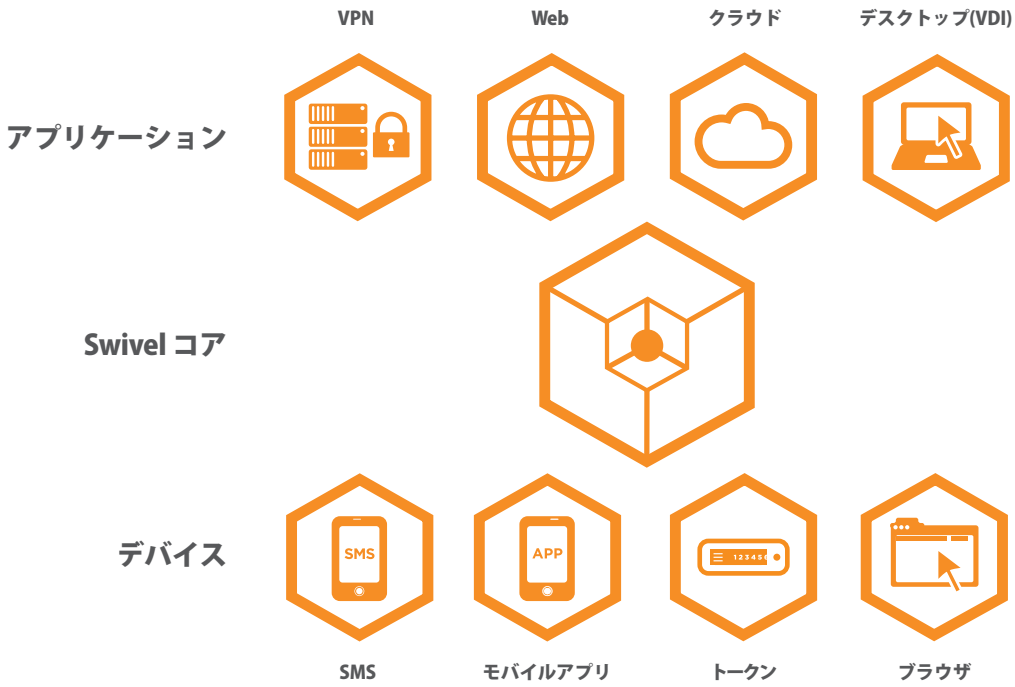
Swivel Secure 社の認証プラットフォーム

Swivel Secure 社の認証プラットフォームは、お客様のセキュリティポリシー、ビジネス上のニーズおよび予算に合わせた適切な認証ソリューションをご提供します。

Swivel 概要

Swivel は多要素認証システムです。システムの中核はチャレンジ - レスポンス型の認証エンジンで、ユーザーにチャレンジを送り、レスポンスが正しければアクセスを許します。

Swivel の認証プラットフォームは VPN、クラウド、Web およびデスクトップの幅広いアプリケーションに対して均質なユーザー体験を提供します。



Swivel の認証プラットフォームはトークンレスのソリューションで、企業の既存のインフラ上で様々なデバイスをサポートできるため、Swivel には認証プロセスを管理するために様々なインターフェースオプションが用意されています。

PINsafe

Swivel ソリューションのユニークな特徴として「PINsafe」ワンタイムパスワード抽出プロトコルがあります。PINsafe が発行する「セキュリティストリングス」をユーザーが受信し、PIN と組み合わせてワンタイムパスワードを生成し、それを使って認証を行います。

このシステムのメリットは、認証のためにはセキュリティストリングスと PIN が必要になるにもかかわらず、PIN 自体は認証プロセスの中で入力されることは絶対に無いことです。ワンタイムパスワードの抽出プロトコルの使い方は簡単で、ワンタイムパスワードにどのキャラクタをどういった順番で使うかを PIN によって決めるのです。

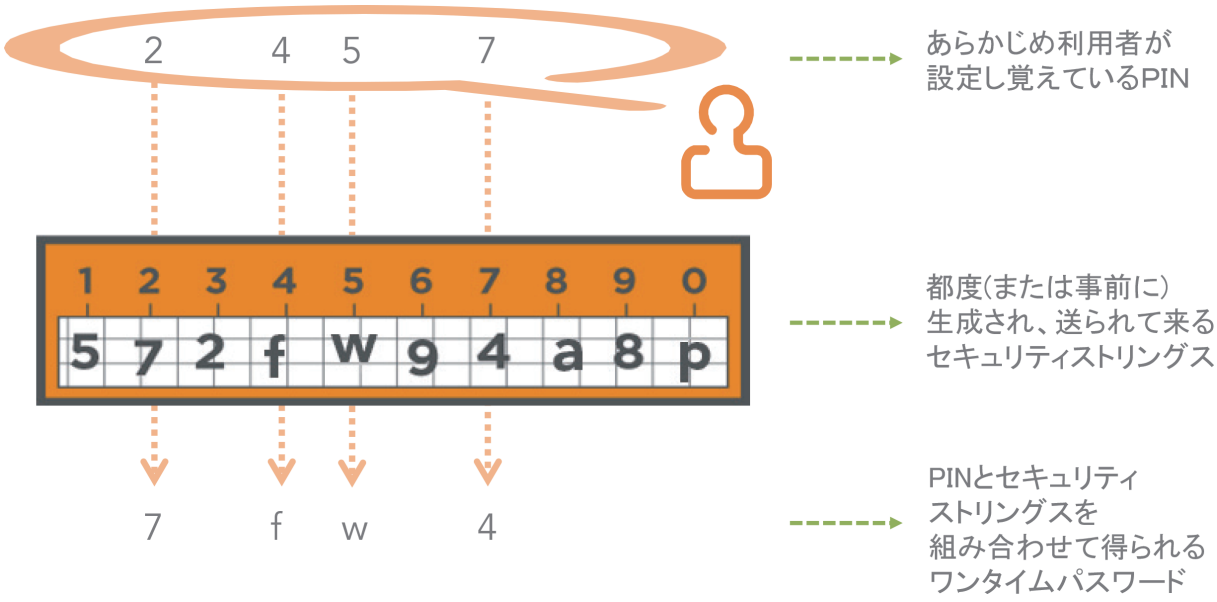


図 1 「PINsafe」ワンタイムパスワード抽出プロトコル

PINsafe は Swivel ソリューションが持つ非常にユニークな特徴ですが、それを使わなければならないわけではありません。例えば、ワンタイムパスワードの抽出を使わない認証を行う事もできます。

Swivel ソリューションのメリット

Swivel サーバーは柔軟で強力な認証システムとして設計されています。特定の認証トークンに頼らないため、コストや管理のための負荷を減らすことができ、配備のための時間も大幅に削減できます。

製品は非常に柔軟なため、同じ Swivel システム内で異なる認証ソリューションを異なるユーザーに提供でき、現在および将来の企業の認証システムへのニーズに末永く応えることができます。

また、オープンな設計のため、他システムとの統合が容易で、企業内の様々な IT リソースと統合できます。

これらの特徴により、Swivel は認証システムの低リスクな選択肢となっているのです。

結論

過去 10 年間、企業や公的機関はデジタル化のメリットを享受し、全てのビジネス活動を IT ネットワークおよび高速通信の上に構築しました。同時にハッカーおよびサイバー犯罪者はネットワーク境界に露出した「いつでも・どこでも」ベースによる脆弱性を攻撃するための手法を洗練させてきました。

コアネットワーク、Web あるいはクラウドなどのデータにリモートにアクセスする方法の多様化と共に、強力な二要素認証への要求は加速度的に高まっています。パスワードはその任に堪えず、トークンベースの二要素認証は一部のアプリケーションやユーザーに適合しません。

必要とされているのは柔軟な認証プラットフォームなのです。個々のユーザー毎に適切なセキュリティレベルを設定でき、重要なユーザーには二要素認証を、リスクの低いユーザーには強力な、あるいは拡張されたパスワード方式の認証を提供することなのです。

Security Strings 合同会社
〒 102-0082 東京都千代田区一番町 6 番地 相模屋本社ビル 7F
http://www.securitystrings.com/

SecurityStrings