GMO トラスト・ログイン

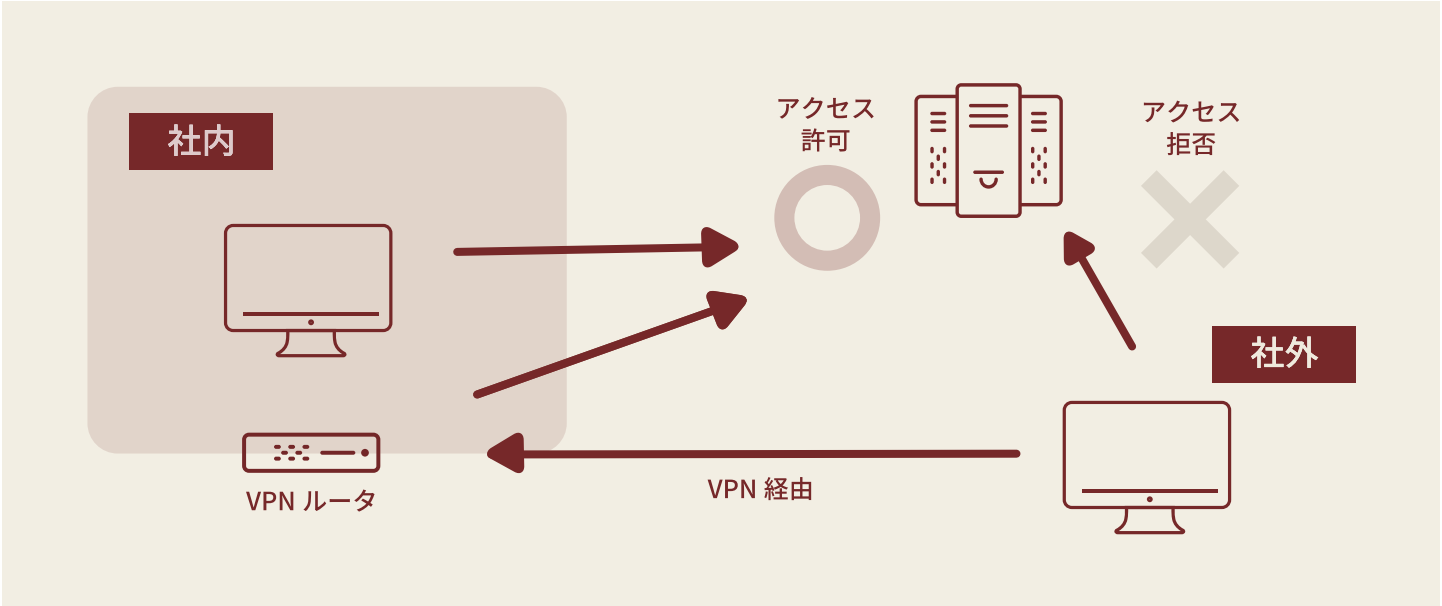
最終回

IP 制限、リスクベース認証、クラウドサービスへの多要素認証

前回は「マトリックス認証」、「PKI 認証」、「IC カード認証」について解説しました。今回は多要素認証の要素ではないのですが、接続制限として一般的な「IP 制限」とユーザのアクセス情報から脅威を判断して制限を行う「リスクベース認証」、クラウドサービスへの多要素認証の対応について解説いたします。

アクセスしてくる場所を制限したい（IP 制限）

クラウドサービスを使用している場合に、社員がどこからアクセスしているかによって、そのクラウドサービスの利用を許可するかどうか制限したいという要望があります。例えば「社内からは許可する、社外からは許可しない。社外から使用する場合は一旦 VPN で社内にアクセスしてから許可する」など。このような制限を実現する場合、アクセスしている場所の「IP アドレス」を判別する仕組みが「IP 制限」となります。



リスクベース認証

リスクベース認証とはユーザがアクセスしてきた利用環境をもとに通常と異なるアクセスであるかどうかを判断し、リスクがあると認識した場合、アクセス制限を行うテクノロジーです。リスクベース認証を使用すると社員がアクセスしている状況からリスクが低いと判断された場合、パスワード認証だけを要求し、リスクがある可能性があると判断した場合は、追加として多要素認証のあるメソッドで認証を要求し、明らかに高いリスクがあるアクセスであると判断した場合はアクセスを拒否するというようなアクセス制限を実現することができます。

例えば、ユーザがシステムにログインする場合、アクセスしてきたときの利用環境が「①社内に設置されているいつも使用している PC から昨日に続いて勤務時間内にアクセスしている」、「②未知の IP アドレスから今まで使用したことのない端末を使用して深夜にアクセスしている」と二つの場合を考えてみましょう。

この二つを比較した場合、①はリスクが低いと判断でき、②はリスクが高いと判断することができます。①の場合はパスワード認証のみ、②の場合はパスワード認証に追加してワンタイムパスワードを要求するというようにアクセス制限を実施します。

使用例	リスクレベル	認証形式
社内のIPアドレス、ログイン履歴のあるPC、最後のログインから１日、勤務時間内アクセス（平日の9:00から18:00）	リスク低	・パスワード認証
社外の IP アドレス、ログイン履歴のない PC、勤務時間外アクセス	リスク高	・パスワード認証 ・ワンタイムパスワード

リスクベース認証ではリスクを判断するアクセス環境から確認可能な項目をコンテキスト要素といいます。さまざまなコンテキスト要素のリスク値を分析し、その合計が一定以上でリスクがあると判断します。

コンテキスト要素には主に次表のようなものがあります。

リスクベース認証の主なコンテキスト要素

コンテキスト要素	概要
IPアドレス	特定のIPアドレス、IPアドレス範囲、サブネット
地域、国、ロケーション	アクセスしてきている国や地域
デバイスフィンガープリント	デバイス構成から計算される固有ID
ログイン時刻	ログイン時の曜日、時間帯
クッキー	以前の同じブラウザからアクセス時に設定したクッキーの有無
最終ログイン	デバイス構成から計算される固有ID

リスクベース認証の主なコンテキスト要素

コンテキスト要素	概要
HTTP ヘッダー	アクセス時のHTTPヘッダー情報
地域ログイン間隔	遠距離の地点から短時間の間隔でのアクセス

このリスクベース認証はそれだけで使用されるのではなく、リスクがないときはパスワード認証のみ、リスクが中程度ではパスワードに加えてワンタイムパスワード、リスクが高い場合はさらに生体認証や IC カードを要求するなど、多要素認証と組み合わせることでユーザの利便性とリスクがある場合の本人確認の徹底を行うことが可能となります。

スクベース認証でのリスク判定

アクセス場所	社内
時刻	平日 AM 10:00
前回アクセス	昨日 PM 5:00
クッキー	あり
デバイスフットプリント	既知デバイスと一致

▼

リスク判定
低

ID/PASS のみで アクセス許可

アクセス場所	国内 (社外)
時刻	平日 AM 10:00
前回アクセス	昨日 PM 5:00
クッキー	あり
デバイスフットプリント	既知デバイスと一致

▼

リスク判定
中

ID/PASS & ワンタイムパスワード

アクセス場所	海外
時刻	平日 AM 2:00
前回アクセス	なし
クッキー	なし
デバイスフットプリント	不明なデバイス

▼

リスク判定
高

ID/PASS & ワンタイムパスワード & PKI 認証

組織のシステム管理部門の視点では、どこからどのような状況でアクセスしているのか判定できるだけでリスク低減の効果が期待できます。また、利用者の視点では、日常業務時のログインを簡単に済ますことができる為、利便性向上の効果が期待できます。
しかしながら、往々にして認証の強化と利便性はトレードオフとなり、コストも大きくなります。そこで今後注目される仕組みがリスクベース認証と言われています。

多要素認証とクラウドサービス

これまで多くの多要素認証のソリューションは「社内システムへの認証を強化すること」、「金融サービスのようにお客様向けの認証を強化すること」が目的でした。このため、オンプレミスで認証システムを構成するのが一般的でした。これは認証先が特定のシステム群であったためそれらのシステム向けに認証を強化すればよかったからです。

一方現在では、企業向けのクラウドサービスが一般的となり、認証を強化したいアクセス先にクラウドサービスが含まれます。この場合、そのクラウドサービスが多要素認証に対応しているのか、どのメソッドをサポートしているのかによって導入可能かどうかに影響します。また複数のクラウドサービスを使用している場合はクラウドサービス毎に多要素認証を設定し、トークン等を管理、運用しなければなりません。場合によっては異なるトークンを持ち歩く必要があります。

このようにクラウドサービスを複数利用している場合、それぞれ異なる認証の仕組みを利用するのでは無く、同じ認証メソッドを使用して運用する方法はないでしょうか。
これを可能にするのがシングルサインオンと多要素認証の組み合わせです。

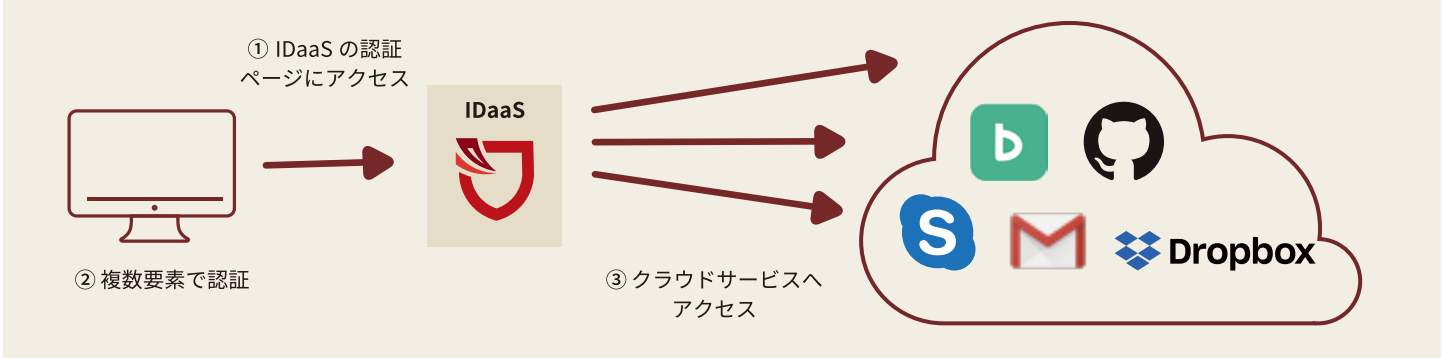
シングルサインオンと多要素認証

シングルサインオンと多要素認証を組み合わせて使用する場合、社員は最初にシングルサインオンの認証サーバへ本人確認として多要素認証を行います。その後はシングルサインオンサービスに登録されていて本人に許可されているシステムへは追加の認証を必要とせずにシームレスにアクセスすることができるようになります。

例えると、関所で身分証明書と通行手形の両方を見せて関所を通過したあとは、町の中のさまざまなお店へ行けるようなものです。

シングルサインオンシステムが統合可能なアクセス先としてさまざまなクラウドサービスに対応した場合、シングルサインオンの認証サーバへ多要素認証した後は契約しているクラウドサービスへアクセス可能となります。多要素認証として運用管理が必要なのはシングルサインオンシステムの認証サーバだけになりますので各クラウドサービス個別に管理する必要がありません。また、認証の入り口が１つに集約されるため、複数のトークンを持ち歩く必要もなくなります。トークンの紛失や社員の退社時の無効化の処理もシングルサインオンシステムに対して実施するだけで良いということになります。

IDaaS を使用したクラウドサービスへの多要素認証とシングルサインオン



クラウドサービス型シングルサインオンサービス

最近ではこのシングルサインオンシステム自体もクラウドで提供されています。このようにクラウド型で提供されているシングルサインオサービスのことを IDaaS（IDentity as a Service）と呼ばれています。IDaaS はシングルサインオン先のシステムとして多くのクラウドサービスを対象としています。

GMO グローバルサインでは IDaaS サービス「SKUID」を提供しています。SKUID は約 2100 の国内主力クラウドサービスに対応し（2017/11 集計）、ワンタイムパスワードにも対応しました。SKUID のユーザ企業様はクラウドサービスへの認証の強化と運用管理性の向上および、社員様のクラウドサービスへのアクセスの利便性の向上を同時に実現することが可能となります。

動作イメージとしてはブラウザに組み込まれている SKUID のブラウザプラグインにアクセスし、ID とパスワードを入力すると次に多要素認証が要求され、正しく認証されると自分のアクセスできるクラウドサービスのアイコンが表示されるので、どのアイコンをクリックしてもすぐにアクセスできるようになります。

クラウドサービス型多要素認証サービス

多要素認証の認証基盤をクラウドサービスとして提供するという取り組みも始まってきています。このようなクラウドサービス型の多要素認証は AaaS (Authentication as a Service）と呼ばれています。従来型のオンプレミスに認証基盤を構築して多要素認証を行うのは初期投資が大きく導入できるメソッドも一つだけのため、中小企業にとっては導入の敷居が非常に高いものでした。AssS を使用すれば今すぐに自社システムへの多要素認証が可能となります。また、運用を行っている途中で認証メソッドが気に入らなければ違うメソッドにすぐに変更することも可能となります。必要な人に必要なメソッドを最小限のコストで導入可能なのが AaaS の大きなメリットとなります。

また、クラウドサービスや B2C サービスを提供している企業にとっても自社で多要素認証の認証基盤を運用せずに AaaS を利用することで、複数の認証メソッドの提供や、最新の認証メソッドを使った多要素認証をお客様に提供できるようになります。

来年から本格的に普及が見込まれている FIDO2.0 認証メソッドの登場により、認証革命が起きるのではないかと期待されています。FIDO2.0 に対応した認証基盤をオンプレミスで一から構築するのではなく FIDO2.0 を認証メソッドとして提供している AaaS を使用することでいち早く FIDO2.0 を使用することが可能となります。また、AssS であれば当初はワンタイムパスワードを導入し、FIDO2.0 対応デバイスが増えてきたタイミングでワンタイムパスワードと FIDO2.0 を併用、FIDO2.0 対応デバイスが行きわたった段階で FIDO2.0 に完全にスイッチするといったロードマップを自社でシステムを持たずに描くことができるようになります。

GMO グローバルサインは、トラスト・ログインにおいて AaaS の提供も検討しており、日本市場および海外市場で IDaaS/AaaS のリーディングカンパニーとなることを目指しております。

まとめ

今回は多要素認証を補完する
「リスクベース認証」とクラウドサービスへの多要素認証の使用方法として
シングルサインオンと多要素認証の連携と
そのクラウドサービス版の IDaaS、
多要素認証のクラウドサービス版 AaaS について解説しました。

今後クラウドサービスの利用が拡大するにつれて
IDaaS や AaaS を活用したパスワード管理や認証強化が重要となります。

ユーザ企業が検討するポイントとして、
「既存の AD との連携」、「認証メソッドをどうする」、
「コストと利便性」が良く取り上げられます。

しかしながら、最初に考慮する事は、
「重要な認証情報をクラウドに任せられるサービスであるか」です。

私ども GMO グローバルサインは
20 年の実績を持つ電子証明書認証局であり、
認証局だからできるサービスと自負しております。

お問い合わせ
(GMO グローバルサイン株式会社)
03-4545-2303
support-jp@globalsign.com