リスクを排除する安全な認証基盤

ー多層型認証環境を実現するRSA Adaptive AuthenticationとIceWall SSOの連携ー

（ Last Update : 2017.4.21）

Webサービスの利用拡大に伴い、正規業者を装って個人情報を盗み取るフィッシングや、ユーザーになりすました不正アクセスなど、セキュリティ上の脅威も増大・高度化しています。特に金融や流通などの分野で、リスク低減と安全性確保は、Webサービスの活用における最優先課題となっています。

日本ヒューレット・パッカードとEMCジャパン株式会社は、これらのニーズに対応する高機能なセキュリティ・ソリューションとして、複数のWebサービスの認証機能を統合しユーザーに認証の利便性と安全性を同時に提供するWebシングルサインオン・ソリューション「IceWall SSO」を、EMCジャパン株式会社のオンラインセキュリティ強化ソリューション「RSA Adaptive Authentication」と組み合わせて提供します。

RSA Adaptive Authenticationとは

「RSA Adaptive Authentication」は、「リスクベース認証」を実現する認証ソリューションです。
「リスクベース認証」は、利用者のPCやアクセス環境の情報を基に、通常と異なる要素をリアルタイム分析し、リスクが高いと判断される時に追加認証を行って正しいユーザーを保護する認証方法です。
本ソリューションには、オンライン犯罪に使用されたIPアドレスや、犯罪パターンに関する情報がリアルタイムで通知され、フィッシングサイトなどに対する迅速な対処を可能とする「RSA eFraudNetwork」も含まれています。
「RSA eFraudNetwork」は、RSAが運用するオンライン不正防止共有ネットワークです。数多くのグローバルな大手金融機関や世界有数のISP数社が参加しており、参加各社はオンライン犯罪に使用されたIPアドレスや、犯罪パターンに関する情報をリアルタイムで共有します。

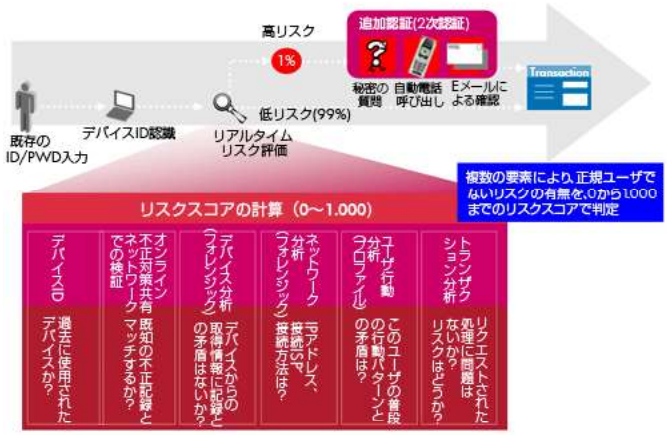

図1.【リスクベース認証】

リスクベース認証・Webシングルサインオン連携ソリューション

日本ヒューレット・パッカードは、RSA Adaptive Authenticationの「リスクベース認証」機能と連携するアプリケーションである「IceWall SSO リスクベース認証オプション」を用意しています。

IceWall SSO　リスクベース認証オプション

- 本オプションによって、RSA Adaptive AuthenticationをIceWall SSOにシームレスにアドオンすることができます。
  - 既存の業務アプリケーションを改修する必要はありません。
- 以下のユーザーインタフェースをパッケージとして提供します。
  - ログイン時（Sign-In）のリスク評価のためのユーザーインタフェース（秘密の質問またはOTPメール）
  - 秘密の質問・回答の登録および、更新（Maintenance）のためのユーザーインタフェース
- また、WebアプリケーションからIceWall SSO、および、リスクベース認証に必要な情報を初期登録（サインアップ）するためのライブラリを提供します。

IceWall SSOとRSA Adaptive Authenticationとの連携によるリスクベース認証　動作例

1. リクエストがブラウザよりWebアプリケーションに向けて送信されると、「IceWallサーバー」によって「IceWall SSOリスクベース認証オプション」が動作する「ログインサーバー」にリダイレクトします。
2. 「ログインサーバー」はブラウザにIDを入力する画面を返します。
3. ユーザーは画面に従いIDを送信します。
4. 「ログインサーバー」は送信されたIDと共にリスク評価の材料となるPC情報を収集します。
5. 「ログインサーバー」はIDと一緒に収集したPC情報をRSA Adaptive Authenticationに渡します。
6. RSA Adaptive Authenticationは、渡されたPC情報のリスク評価を実施し、結果を「ログインサーバー」に返します。
7. 「ログインサーバー」はRSA Adaptive Authenticationから返された結果に基づき、ユーザーへ認証を要求します。
8. リスクが低いと判断された場合は、パスワードの入力画面がユーザーに返されます。ユーザーはパスワードを送信し、認証を受けます。
9. リスクが高いと判断された場合は、追加認証（秘密の質問またはOTPメール）が要求されます。
10. 認証が終了したら、「ログインサーバー」はセッションIDをブラウザに渡します。
11. そのセッションIDを使用して、認証を受けたブラウザは「IceWallサーバー」と通信を開始し、そのユーザーの持つ権限に従いWebアプリケーションを使用できるようになります。

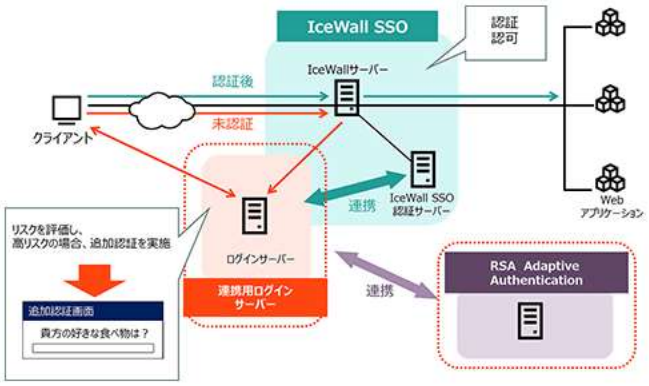

図2【IceWall SSOとRSA Adaptive Authenticationとの連携(1)】

RSA Adaptive AuthenticationとIceWall SSO 連携のメリット

リスクベース認証の導入が容易になります。

従来、RSA Adaptive Authenticationを用いてリスクベース認証システムを構築する場合、導入には個別のプログラム開発が必須でした。今回のリスクベース認証オプションの使用により、既存Webアプリケーション側には手を入れることなく、前段にIceWall SSOとリスクベース認証オプションを置くことにより、リスクベース認証の環境を構築することができるようになりました。本連携により、既存Webアプリケーションのリスクベース認証環境への移行のみならず、新たなWebアプリケーションの追加も、リスクベース認証との連携を意識せずに追加できます。

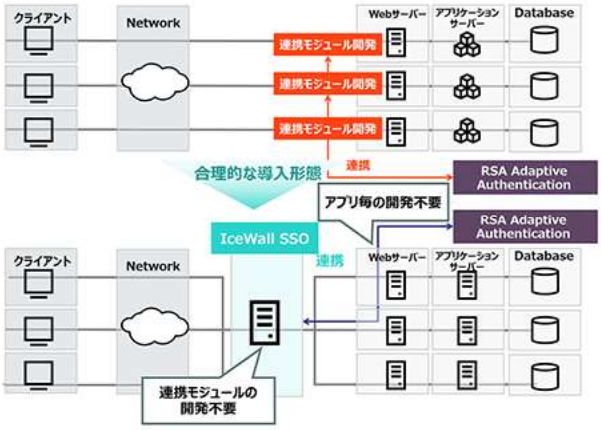

図3【IceWall SSOとRSA Adaptive Authenticationとの連携(2)】

Webシングルサインオンへの認証が強固になります。

一度の認証でユーザー権限を持つリソースにアクセス可能となるシングルサインオン環境では、認証の強度は非常に重要です。RSA Adaptive Authenticationとの連携により、シングルサインオン環境への更に強固な認証を実現します。IceWall SSOは、本リスクベース認証との連携のみならず、証明書、ICカード、トークンや携帯電話による認証など、ニーズの高い最新の認証製品との連携ソリューションの開発を継続して実施しています。セキュリティレベルや利便性など、お客様のニーズにあわせ、多様な認証方式を選択いただくことが可能です。

IceWall SSOとRSA Adaptive Authenticationの連携による強固な認証基盤の迅速な導入で、企業の信頼性向上とビジネスの拡大をご支援します。

≫ 日本ヒューレット・パッカードとEMCジャパン株式会社、Webサービスのリスクを排除する安全な認証基盤の提供に向けて協業
－「IceWall SSO」と、EMCジャパン株式会社の多層型認証環境を実現する「RSA Adaptive Authentication」を組み合わせ、高機能ながら導入が容易なソリューションを提供 －

≫ IceWall ソフトウェア 技術レポート一覧ページへ

2007.12.18 掲載
2013.8.22 加筆修正
2014.10.10 加筆修正
2017.4.21 加筆修正