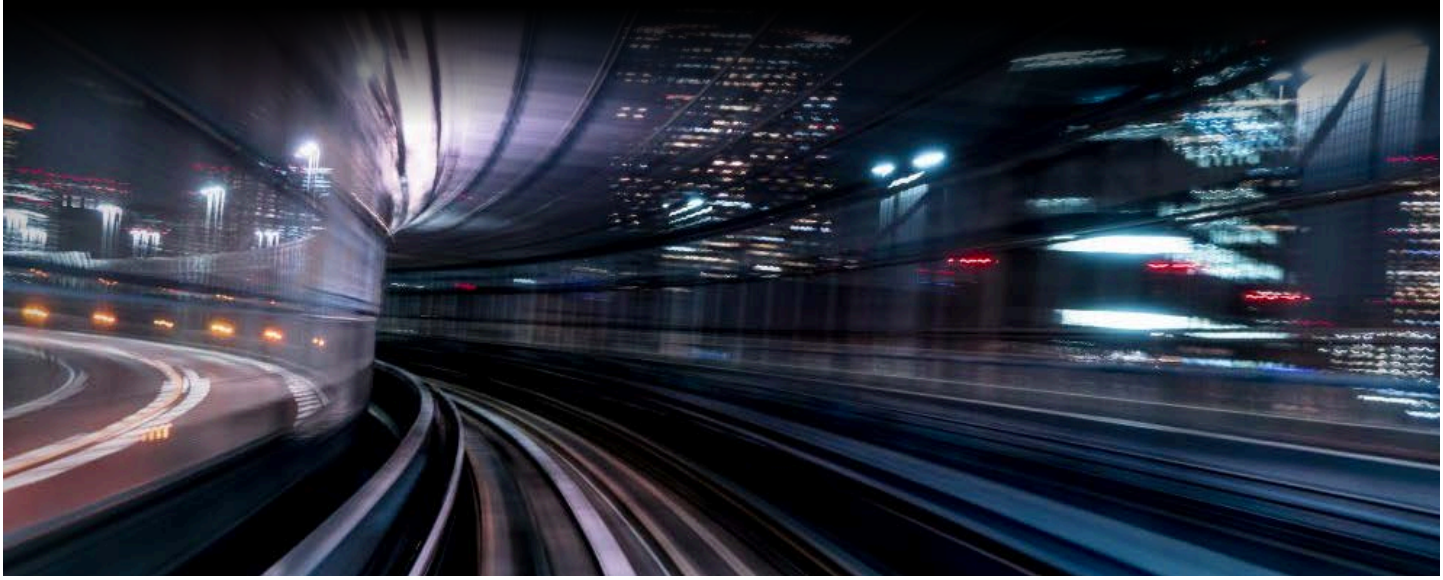
行動的生体AI認証ソリューション「BioCatch」とIceWall MFAとの連携

IceWall技術レポート



1. はじめに

本レポートでは、IceWall MFAと、SCSK株式会社が提供する行動的生体AI認証ソリューションBioCatchの連携について、その効果と具体的な設定方法をご紹介します。

2. ソリューション概要

IceWall MFAは、さまざまな認証ソリューションとの連携が可能です。プラグインを追加することで、ID/パスワード以外の認証方式をサポートします。IceWall MFAにBioCatchプラグインを導入することで、BioCatchとの連携が可能になります。

本ソリューションは、主に金融機関の顧客向け認証基盤の、不正アクセス対策強化して効果が期待できます。

3. システム利用中のふるまいも検知-行動的生体AIソリューション BioCatchについて

BioCatchは、利用者が端末（スマホやPC）を操作する際の操作情報を収集、操作の傾向（くせ）から、本人らしさを分析することで、第三者のなりすましによる不正送金などのサイバー犯罪を防ぐことができる製品です。インターネットバンキングを始めとする、金融機関のWebサービスに対する不正アクセス対策としてご活用いただけます。以下のような特徴がございます。

- 各種情報からユニークなプロファイルを作成：ブラウザでは500、スマホでは2,000以上の情報を収集して利用者ごとにユニークなプロファイルを作成します。
- 「本人らしさ」を可視化：0から1000のスコア、利用者ごとのプロファイルを用いた「本人らしさ」の判定結果などを可視化します。
- リアルタイムに本人識別：リアルタイムでアップデートされるプロファイルを使って、リアルタイムに利用者が本人であるかどうかを判断するために利用できます。
- マシンラーニングによる継続的な検知精度の向上：BioCatch社は50件以上もの特許を製品全体に活用して非常に高度な分析を行います。
- ワンタイムパスワード攻撃にも対応：近年増加しているワンタイムパスワードを突破する攻撃に対しても有効です。
- 豊富な実績：BioCatch社は行動バイオメトリクスの分野で先進的な製品を開発しており、月間20億以上のセッションデータを分析し、世界で2億人以上のユーザーを守っています。

4. ソリューションが活躍するユースケースについて

IceWall MFA と BioCatch の連携ソリューションが活躍するユースケースをご紹介します。

シナリオ①　ワンタイムパスワードなどの多要素認証を突破しての不正送金を防止する

[課題]　フィッシングサイトやその他攻撃手法を用いて、利用者のログイン情報を不正に入手。利用者の口座から第三者の口座へ不正送金などの取引を実行される。

[対応]　IceWall 統合認証基盤を導入し、BioCatch Pluginを追加する。

[導入効果]　第三者のなりすましログインを検知し、不正送金などの取引が実行されることを未然に防ぐ。

シナリオ②　不正送金被害などの防止をする一方で、利用者の利便性が向上させる

[課題]　フィッシングサイトやその他攻撃手法を用いて不正送金される被害が増加。それを防ぐために利用者がログインや取引を行う際にワンタイムパスコードを発行して入力させるなど、利用者の操作の手間が発生。

[対応]　IceWall統合認証基盤を導入し、BioCatch Pluginを追加する。

[導入効果]「本人らしさ」のスコアリングの結果、「本人らしさ」が高いと判定された場合は、ワンタイムパスコードの入力を要求しないなど、利用者の手間を省くことで利便性を向上させる。

BioCatch社BioCatchの詳細は以下ページをご参照ください。

BioCatchホームページ →

5. 連携の効果

IceWall MFAとBioCatchを連携して導入することにより、期待できる効果をご紹介します。
セキュリティを強化したい対象Webアプリケーションに対して、BioCatchをシステム個々に導入する時と比べ（図①）、IceWallのバックエンドに対象システムを配置することで（図②）、対象Webアプリケーションの改修工数を削減することが可能です*1。また、このWebアプリケーションは複数配置することもできます。

検証のシナリオとして、ユーザーはマイページ等に既にログイン済みのものとし、送金サービス等のページへ遷移した際の動きとして記載しております。

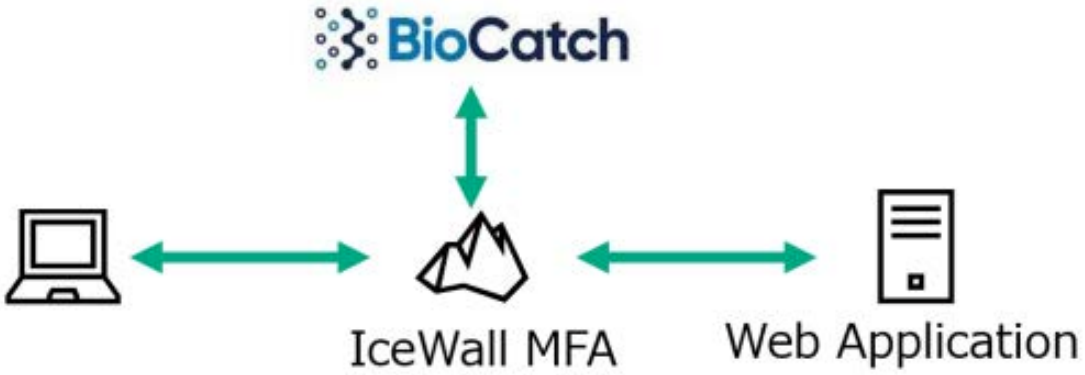
改修工数削減メリット① API連携

IceWall MFAがBioCatch API連携機能を提供することで、WebアプリケーションがBioCtach APIと直接通信する必要がなくなります。そのため、API連携部分をWebアプリケーション側に組み込む必要がありません。

改修工数削減メリット② リスク判定&追加認証

BioCatchの算出したリスクスコアに基づきIceWall MFAがリスク判定を行い、追加認証の有無を決定します。また追加認証には、IceWall MFAが提供する認証方法を利用可能です。そのためWebアプリケーションに対して、リスク判定機能および追加認証機能を追加改修が不要です。

図① IceWall MFAを使用しない場合



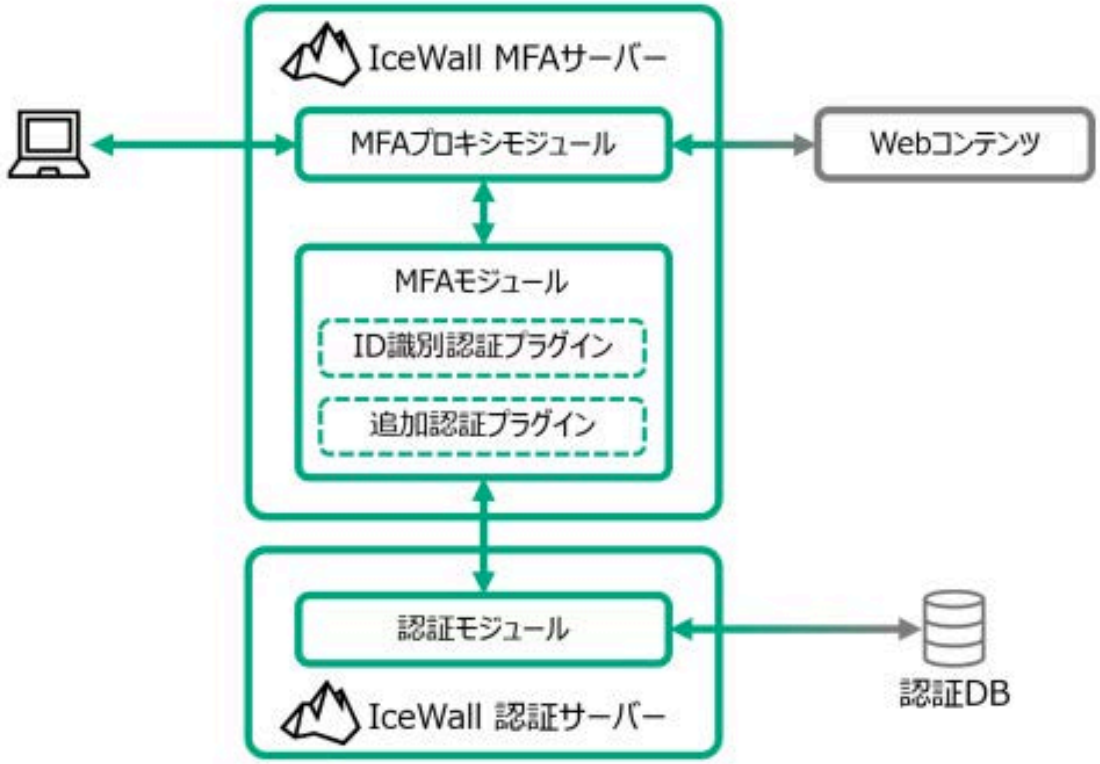
図② IceWall MFAをBioCatchと連携させた場合

*1 BioCatchがユーザーのふるまい情報を収集するためのJavaScriptをWeb Applicationの画面に埋め込む必要があります。

6. 構成概要とBioCatchプラグインについて

6.1 IceWall MFAの基本構成

IceWall MFAはプラグインを追加することで、認証方式の追加や他ソリューションとの連携など、機能拡張ができるプラグインアーキテクチャーを採用しています。プラグインの例として以下が挙げられます。



- ID識別認証プラグイン
  ユーザーを特定するための認証を提供するプラグインです。

例：パスワード認証プラグイン、統合Windows認証プラグイン

- 追加認証
  ユーザー特定後に追加認証を提供するプラグインです。

例：Mail OTPプラグイン、マトリックス認証プラグイン

6.2 BioCatchプラグインと構成概要

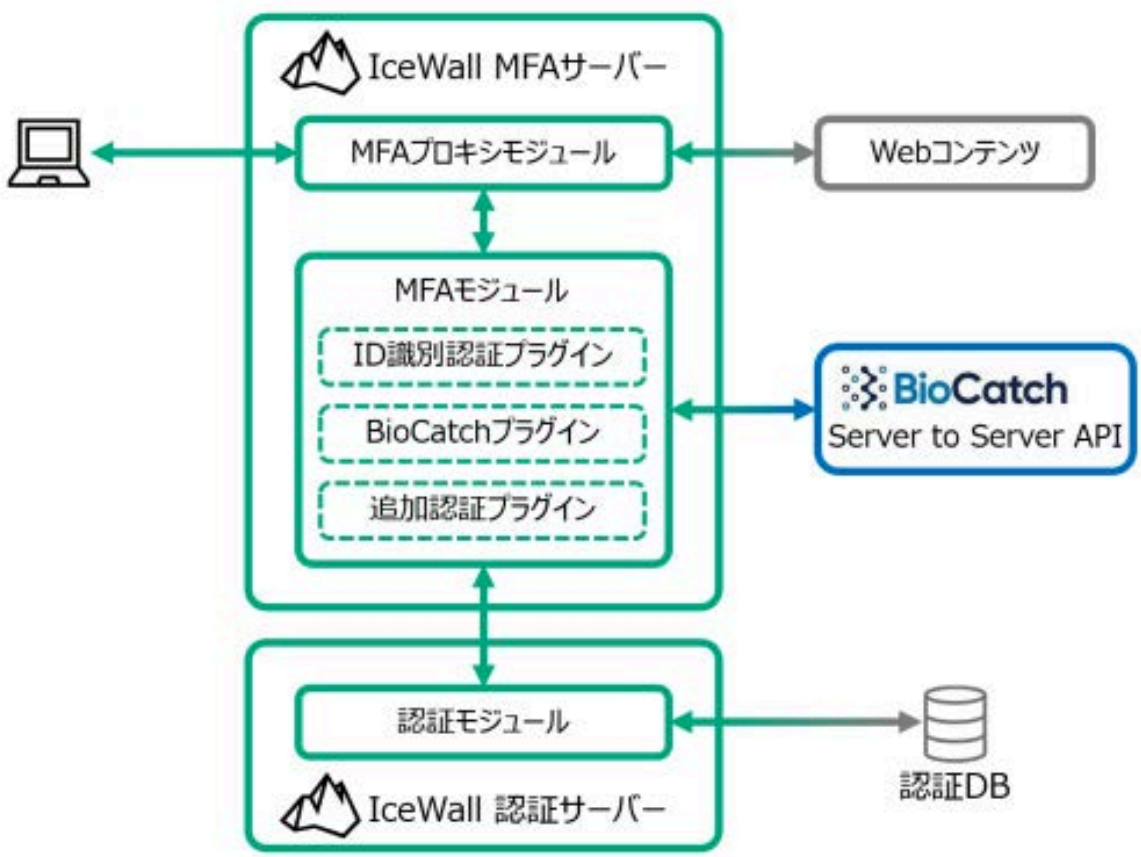
BioCatchプラグインとはIceWall MFAのプラグインであり、BioCatch API連携、リスク判定および追加認証の有無を決定する機能を提供するプラグインです。

BioCatchの提供するスコア等、様々な要素を用いてリスク判定が可能です。

IceWall MFAに本プラグインを追加することで、IceWall MFAの製品改修なしにBioCatch連携が可能になります。

6.3 BioCatchプラグインの設定

BioCatchプラグインを利用する為には、以下の設定が必要となります。



① IceWall MFA画面(HTML)へのJavaSprict埋め込み

パスワード認証などのID識別認証の画面(HTML)にBioCatchが振る舞い情報を取得するための
JavaScriptを埋め込みます。

② BioCatchプラグインに必要な設定

- BioCatch APIのURL

IceWall MFAがBioCatchと連携するためのAPI URLです。

IceWall MFAはインターネット上のBioCatch APIと連携するため、必要に応じてProxyも設定します。

- BioCatchのCustomer ID

BioCatchの発行するCustomer IDです。

- リスク判定基準

BioCatch APIより返却されるリスクスコアなどの要素に対して追加認証を求める閾値を設定します。

リスクスコア以外にBot・Rat判定に基づく設定も可能です。

7. ソリューション連携イメージ

本章では、ソリューションの連携イメージをご紹介します。低リスクの認証時はパスワード認証、高リスクと判定された際の追加認証にMail OTP認証を使用する例をご紹介します。

7.1. BioCatchが低リスクと判断した場合

① ユーザーはWebコンテンツのURLにアクセスします。

この時、IceWall MFAに未ログインのためIceWall MFAのパスワード認証画面が表示されます。

② パスワード認証成功後

パスワード認証が成功するとBioCatchプラグインが呼び出され、BioCatch APIに対してユーザーのリスクスコアを要求します。リスクスコアがBioCatchプラグインに設定された閾値より低い場合、IceWall MFAは認証完了としてWebコンテンツをユーザーに表示します。

7.2. BioCatchが高リスクと判断した場合

① ユーザーはWebコンテンツのURLにアクセスします。

この時、IceWall MFAに未ログインのためIceWall MFAのパスワード認証画面が表示されます。

② パスワード認証成功後

パスワード認証が成功するとBioCatchプラグインが動作し、BioCatch APIに対してユーザーのリスクスコアを要求します。リスクスコアがBioCatchプラグインに設定された閾値より高い場合、IceWall MFAは追加認証が必要としてMail OTP認証をユーザーに要求します。

③ Mail OTP認証成功後

Mail OTP認証が成功するとIceWall MFAは認証完了としてWebコンテンツをユーザーに表示します

9. まとめ

本レポートでは、IceWall MFAとBioCatchの連携による金融機関向け不正アクセス対策強化ソリューションについて、有効なシナリオと、連携することでの導入メリットをご紹介しました。

相乗効果の高いソリューションですので是非ご検討ください。

2021.12.3　新規掲載

執筆者　：SCSK株式会社
ミドルウェア営業部
硲　公志

日本ヒューレット・パッカード合同会社
Pointnext事業統括　Pointnextデリバリー統括本部
クロス・インダストリー・ソリューション本部 認証コンサルティング部
川上 大輔

技術レポート一覧へ →

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

コミュニティ

HPE Japan ブログ

リソース

お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録

ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

日本 (ja)