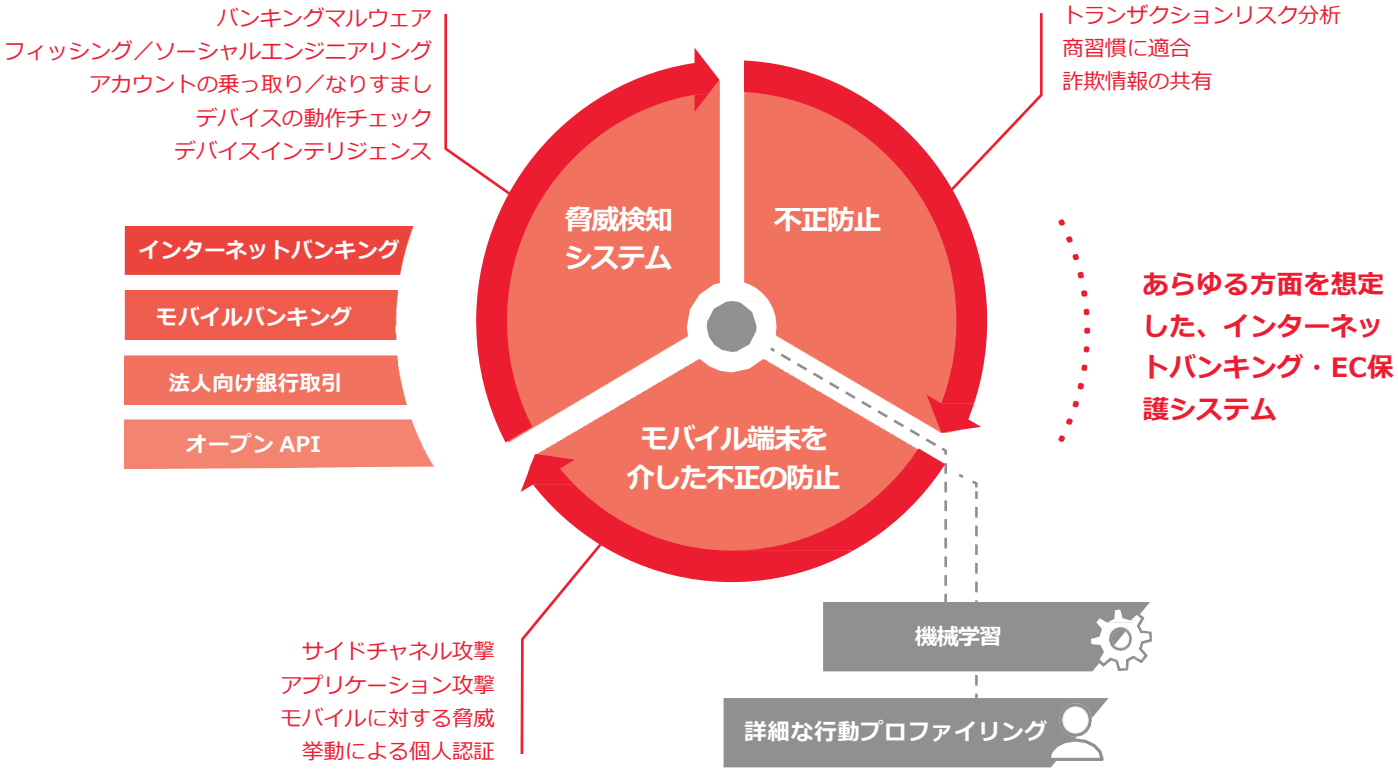
ThreatMark
不正防止対策ソリューション

■ ThreatMark Anti Fraud Suite (AFS)とは

さまざまな形態のサイバー犯罪、詐欺、および規制の課題に常に直面している金融サービス業界の苦悩に応える次世代の不正防止ソリューションです。

- **数百項目のパラメータを継続的なモニタリングにより、詳細な行動プロファイリングを生成します。**
- **機械学習機能により、各支払操作または有効な取引をリアルタイムで分析し、怪しいふるまいを検知できます。**
- **証拠に基づくサイバー脅威検出メカニズムを使用し、ユーザを妨害することなく攻撃を検出できます。**



■ 多層的な不正検出チェックの仕組み

- ◆ 接続チェック (TOR、匿名プロキシサーバ)
- ◆ ブラウザやOSのセキュリティチェック
- ◆ マルウェア、フィッシング
- ◆ デバイスフィンガープリンティング

- ◆ GeoIPの確認
- ◆ ログイン時間の確認
- ◆ 生体認証でのログイン
- ◆ ベロシティチェック
- ◆ 行動の背景

- ◆ Webのページ遷移プロファイリング
- ◆ プログラムされたアクセスと自動検知
- ◆ セッションの乗っ取り
- ◆ 行動とアプリケーションを連携した個人認証

- ◆ マネーミュールブラックリスト
- ◆ 異常な取引
- ◆ 行動プロファイリング

- ◆ ビッグデータAI/ML
- ◆ 異常検出
- ◆ 信号の集約
- ◆ クラウドデータの比較

■ 特徴

◆ ユーザのネット利用状況をモニタリングし、数百の項目（行動パターン、セッションパラメータ、詳細にわたる取引内容、生体情報、ウェブ・モバイルアプリケーション間の相互連携等）により、評価を行います。ユーザに関する詳細な情報を取得することで、検出率が向上し、誤検知の件数を減少します。

◆ 最先端の機械学習と人工知能を用いて、ユーザの行動と数百もの、技術や金融に関するパラメータを分析します。これまでは攻撃の準備段階の摘発は不可能でしたが、この機械学習機能の搭載により、ユーザプロファイルをもとに、疑わしい挙動を検知したり、不正を防止したりすることができます。

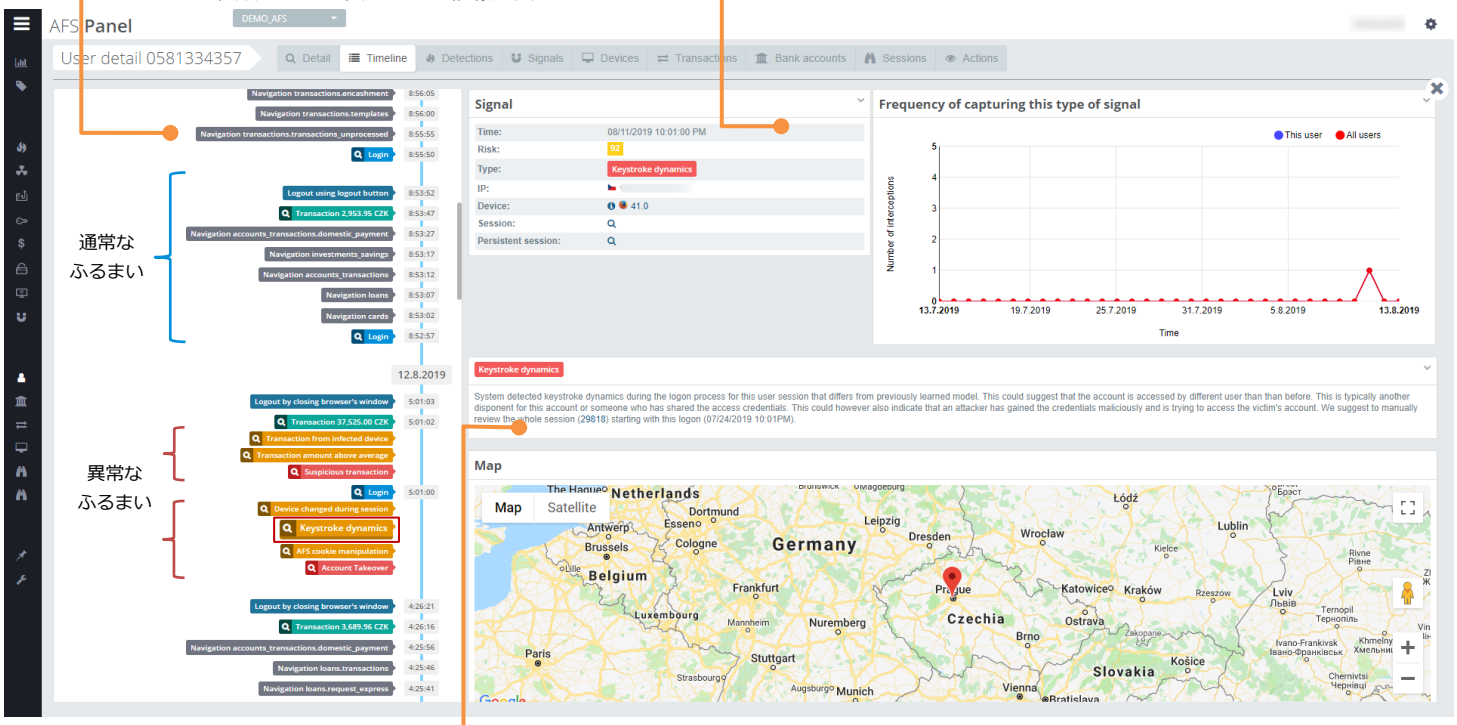
■ 異常なふるまい検出例

◆ ユーザのアクセス履歴とページ遷移

ルーペをクリックすることで検出した通常と異常のふるまい、脅威や取引の詳細が右側に表示されます。検出したイベントの種類によって表示される情報が異なります。

◆ 異常なふるまいを判断する要素・情報

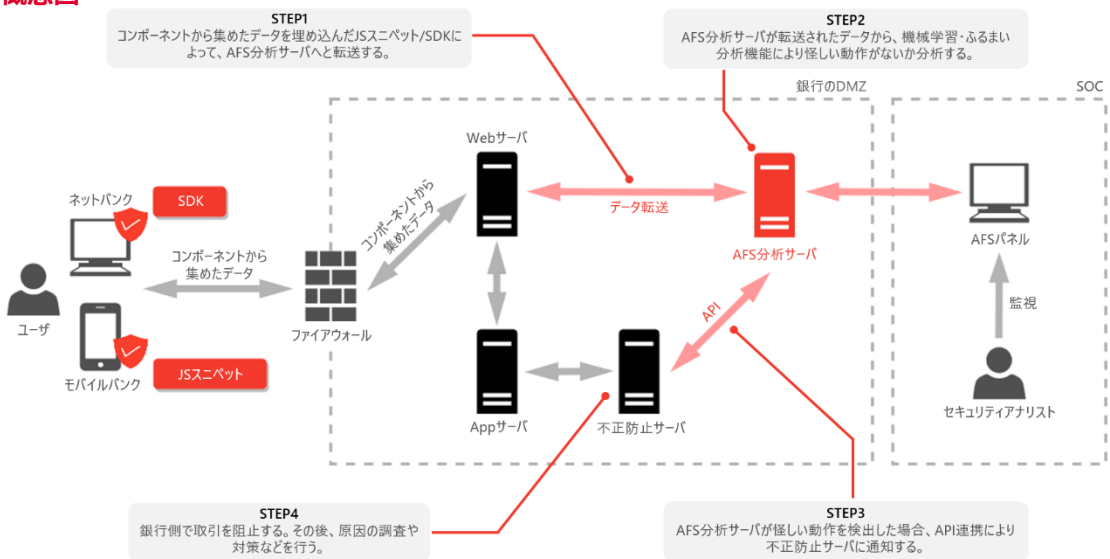
「Keystroke Dynamics（キーストローク力学）」の場合には、検出した時間、IPアドレス、端末情報、ブラウザ情報などが表示されます。



◆ イベントの説明

異常としてあげた理由、意味する脅威と推奨対応

■ 実装概念図



※内容は予告なく変更することがあります。（2020年12月作成）

情報セキュリティ株式会社

〒650-0012 神戸市中央区北長狭通4丁目9-26　西北神ビル3・8階
TEL：078-381-8980（10:00~17:00　土・日・祝除く）
FAX：078-381-8979
E-mail:　inquiry@isec.ne.jp　URL: https://www.isec.ne.jp