フライヤー
セキュリティ

自動車業界におけるセキュア分析事例

自動車メーカーは、大量のデータを収集し、そこから予測分析を使用して得られた貴重な情報を、収益化、製品の改善、業務の最適化、および顧客サービス向上のための新機能提供に役立てています。その際、利用者、自動車関連企業、そして経済全体に大きな価値をもたらすものとして、自動車 IoT、すなわちコネクテッドカーに期待がかけられています。

セキュア分析と自動車業界の現状

走行中の何百万台もの車から昼夜問わず生み出される大量のデータを処理するため、自動車メーカーはデータレイクを導入し、リアルタイムのセンサーデータおよびその他の交通に関するデータを、過去の履歴データと共に取得しています。ただし、ここで大きな課題となるのが、分析で使用する機密データに対する安全性およびプライバシー保護の確保です。

『Upstream Security Global Automotive Cybersecurity Report 2019』によると、自動車のサイバー攻撃は、2010 年から 2018 年の間に 6 倍に増加しています。* コネクテッドカー業界でのサイバー攻撃の急増は、自動車メーカーから OEM、運送会社、レンタカー会社、保険会社などにまで及び、この事業分野全体に影響が波及しています。

出典：Upstream Security Global Automotive Cybersecurity Report 2019

さまざまな業界で IoT を導入する際の最大の障壁は、セキュリティです。しかし、コネクテッドカー市場は急成長しており、データ量とそれに伴うリスクは今後も増加すると見込まれています。IoT がもたらすメリットに疑う余地はないものの、データ侵害やデータプライバシー規制に対するコンプライアンス違反のリスクが高まれば、メリットが相殺されてしまう可能性があります。

アクセスを制限することによるデータ保護対データのオープン化による利便性

分析のためにデータへのアクセスをオープンにして新たに価値を創出することと、アクセス制限によるデータ保護は、潜在的に相反する概念です。IT アーキテクトと意思決定者には、分析プラットフォームとデータレイクへのアクセスを可能にすると同時に、GDPR や CCPA などのデータプライバシー規制へのコンプライアンス違反に加えてサイバー攻撃に対しても、保護対策を講じることが求められます。せっかく IoT に投資したにも関わらず、その後、セキュリティとプライバシーに対する懸念からアクセスを厳しく制限している組織は、テクノロジーへの投資に対して必要な見返りを実現することができません。

自動車メーカーは、位置情報コード、車両識別番号、および保護対象となる顧客の個人データを含む、機密データのストリーミング、供給、保管を行っています。たとえば、ひとりのドライバーの複数の位置情報コードは、分析プラットフォームで結合すると、個人の特定に利用される可能性があります。データ侵害が発生すれば、規制当局から罰則が科されたり、顧客の信頼を失う事態に陥りかねません。明確なデータ保護戦略がないと、多くの危機にさらされます。

ファイアーウォールなどによる境界線の防御や、ユーザーとネットワークのアクティビティ監視といった従来型 IT セキュリティ制御は、導入しておく必要があります。しかし、データへのアクセスと分析の必要性を考慮すると、システム中心型の制御による保護だけでは信頼性に欠けます。

ストレージレベルのデータ保護は、データプライバシーのコンプライアンス観点では基準を満たしているかもしれませんが、分析環境では使用できません。データマスキングは一方向の変換であり、分析結果からもとのデータに戻ることができません。

固定化された制御によって、分断されたデータへのアクセスを数名のデータサイエンティストに限定する方法では、分析効率と投資回収率（ROI）の向上は見込めません。

データプライバシーの維持

GDPR、CCPA などのデータプライバシー規制では、機密性の高い個人データを保護し、コンプライアンスの実現を支援するために使用できるメカニズムとして、暗号化と仮名化（psuedonymization）を推奨しています。仮名化（psuedonymization）は、ビジネスプロセスで仮名またはサロゲートデータを使用するなどの、データ匿名化手法の総称です。フィールドレベルの暗号化とトークン化も、この方法に該当します。

コネクテッドカービジネスの成長に合わせて、セキュリティを迅速に拡大させる方法とは

膨大な量のデータ利用とリスクの低減を同時に実現するには、取り込んで分析するデータ量に合わせてスケールする保護機能が必要です。分析プラットフォームやデータレイクへ機密データを取り込む際には、フォーマット、振る舞い、意味を保持し、つまり分析に利用可能でありつつも匿名化された、サロゲートデータによって保護します。さらに、機密データが保護されていない状態にあることを避けるため、データソースにできるだけ近い位置で暗号化する必要があります。

解決策：Format-Preserving Encryption (FPE) を使用してデータに保護手段を組み込む

安全に分析を行うためには、データ漏洩リスクを軽減しながらデータを保護する必要がある一方、インフラストラクチャーシステムとセキュリティ境界制御による防御を、データそのものに保護手段を組み込むことによってさらに強化することが不可欠です。

Format-Preserving Encryption (FPE) 機能を備えた Micro Focus® Voltage SecureData は、大量のデータを取り込むデータレイクおよび分析プラットフォームでの安全な分析を可能にします。Voltage FPE は、機密情報を含む構造化データをフィールドレベルとサブフィールドレベルで暗号化します。その際、数値、記号、文字、数値の関係性、複数の分散データセットでの参照整合性など、元データの特性は維持されます。

保護された形式のデータは、アプリケーション、分析エンジン、データ転送、およびデータストアで使用できるだけでなく、本当に必要とする特定のアプリケーションとユーザーに対しては、容易かつ安全に元データへのアクセスを可能にします。万が一、データ侵害が発生した場合、保護されたデータは無価値化されていますので、保護がない場合に発生した際に科せられる制裁金や対応に必要なコストを回避することができます。

主な使用事例：予測分析、車両メンテナンス

エコシステムの範囲：ビッグデータ分析、ミッションクリティカルな IT、クラウド、IoT データ

様々な事例に予測分析を利用することにより、需要変動分析からサプライチェーンの問題の予測、新たな安全性と品質の問題の特定が可能になります。ビジネス成果につながる顧客満足度、車両の安全性、およびブランド認知度も向上します。さらには、品質保証にかかる総コストの削減にもつながります。

サイバー攻撃による脅威が高まり、データプライバシー規制が強化される中、分析時にはすべての機密データが確実に保護されていることが、重要な目標となっています。自動車メーカーが必要としているものは、データサイエンティスト、データベース管理者 (DBA)、およびサードパーティが、リレーショナルおよび非リレーショナルデータベースとストレージ全体で機密情報を安全に使用できる、実証済みの統合アーキテクチャーです。

現在、複数の自動車メーカーが、あらゆるデータタイプ、数百のアプリケーション、およびデータレイクにわたって、Voltage SecureData によりペタバイト級のデータを保護することで、このビジョンを達成しています。Voltage Simple API は、幅広いビッグデータ製品および ETL 製品に簡単に統合できます。既製のコードには、Hive、Spark、Kafka/NiFi、Kafka/Storm、Map Reduce、Impala、および Sqoop のテンプレートが用意されています。エッジノードは、機密データのランディングゾーンとして使用し、それを HDFS に格納することが可能です。

ユースケースの一例として、パフォーマンス分析用のリアルタイムセンサーデータの保護があります。データは、IoT エッジで保護されます。走行中の自動車からリアルタイムでストリーミングされ、暗号化されてから分析プラットフォームに取り込まれます。その後、保護されたデータは、HDFS やその他の環境に送られます。

お問い合わせ先：
www.microfocus.com

ユースケース：自動車メーカーのデータフロー

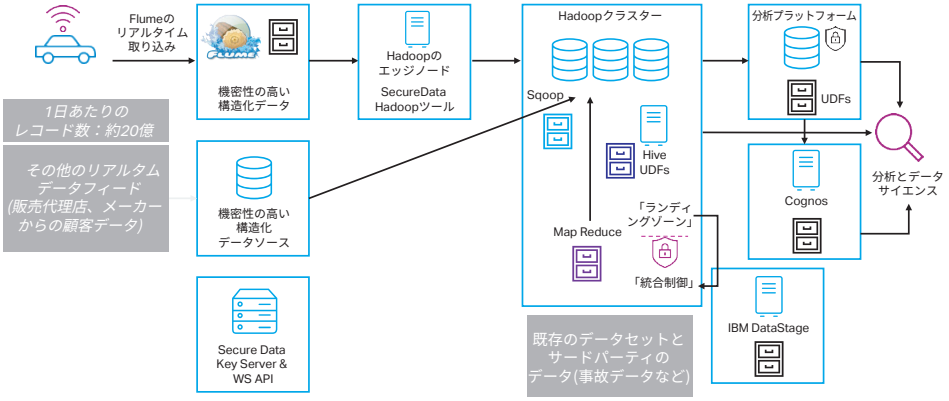

図 1. 自動車メーカーのデータフロー

顧客分析のための安全なビッグデータ活用

FPE および SST を備えた Voltage SecureData により、自動車メーカーは以下のことを実現できます。

- Hadoop データレイク、リレーショナル / 非リレーショナルデータベース管理システム内の保護されたデータから分析結果を安全に抽出
- GDPR、CCPA、PCI DSS など各種データ保護規制への準拠
- データソースの取り込みからエンドツーエンドのライフサイクル全体にわたってデータを保護

さらなるビジネス価値を創出するために、より多くのユーザーとアプリケーションに対して、「解き放たれた」ビッグデータ分析のパワーをぜひご活用ください。

詳細情報はこちら：
www.microfocus.com/sdhadoop

マイクロフォーカスエンタープライズ株式会社
jp-info-enterprise@microfocus.com
www.microfocus-enterprise.co.jp