自動車メーカー業界のセキュアな分析の使用事例

自動車メーカーは膨大な量のデータを保有しています。予測分析により、このデータから、収益化、製品の改善、業務の最適化、新機能の提供による顧客サービスの向上に役立つ知見を引き出すことができます。オートモーティブ IoT やコネクテッドカーは、ユーザー、企業、そして経済に大きな価値をもたらすと期待されています。

セキュアな分析と自動車産業の概要

路上を走行する何百万台もの自動車から、昼夜を問わず膨大な量のデータが生み出されています。自動車メーカーは、リアルタイムのセンサーデータなどの交通データと履歴データを取得するためにデータレイクを導入していますが、そこには大きな課題があります。それは、いかにして分析に使用する機密データをセキュアかつプライベートに維持するかということです。

『Upstream Security Global Automotive Cybersecurity Report 2019』によると、2010 年から 2018 年の間に、自動車関連のサイバー攻撃は 6 倍に増加しました *。コネクテッドカー分野におけるサイバー攻撃の急増は、ティア 1 企業から、OEM 企業、フリート事業者、レンタカー会社、保険会社などに至るまで、この業界のすべての関係者に影響を与えています。

*出典：Upstream Security Global Automotive Cybersecurity Report 2019

IoT を複数の業界に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の急成長に伴い、データ量とリスクは今後も増加すると見込まれています。IoT のメリットは疑いの余地のないところですが、データ侵害のリスクが高まり、データプライバシー規制のコンプライアンス違反が生じた場合には、メリットが相殺されてしまう可能性があります。

隔離によるデータの保護 対データのオープンな使用

データを分析対象としてオープンにアクセスできるようにして新たな価値を創出することと、使用できない形でデータを隔離して保護することは対立する概念です。IT アーキテクトと意思決定者は、GDPR や CCPA などのデータプライバシー規制のコンプライアンス違反とサイバー攻撃を防ぎながら、分析プラットフォームとデータレイクへのアクセスを提供する必要があります。IoT に投資しながらも、セキュリティやプライバシーへの懸念からデータへのアクセスを禁止している組織は、テクノロジー投資に対して必要なリターンを実現することができません。

自動車メーカーは、地理的位置コード、車両識別番号、個人データなど、保護が必要な機密データをストリーミング、フィード、保管しています。たとえば、1 人の運転者に関する複数の地理的位置コードが分析プラットフォームで組み合わされた場合、個人の特定に利用される可能性があります。データの不正利用が発生すれば、規制当局から罰則が科されたり、顧客の信頼を失ったりする可能性があります。明確なデータ保護戦略がない場合は多くのリスクがあります。

整備すべき従来型の IT セキュリティ管理対策としては、ネットワークの境界の保護、ユーザーの活動やネットワーク活動の監視などが考えられます。しかし、データのアクセスと分析の必要性を考慮すると、システム中心の管理には信頼性がありません。

ストレージレベルでのデータ保護は、データプライバシー法規制へのコンプライアンスという点では合格かもしれませんが、分析環境で使用することができません。データマスキングは、一方向の変換であり、結果を複製できません。

静的な管理によって、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している場合、知見と ROI を追求することはできません。

有用なデータの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は、機密の個人データを保護してコンプライアンスを実現するためのメカニズムとして、暗号化と仮名化を推奨しています。仮名化とは、仮名データまたはサロゲートデータを使用できるビジネスプロセスにおける様々なデータ匿名化手法を表す用語です。こうした手法には、フィールドレベルの暗号化やトークン化が含まれます。

コネクテッドカー関連ビジネスの成長に合わせてセキュリティを拡大するための方法

大規模なデータの利用とリスクの低減を両立するには、取り込んで分析するデータの量に合わせて保護を拡大する必要があります。データのソースにできる限り近い形で、保護のギャップを解消するため、データを分析プラットフォームやデータレイクに取り込む前に、データの形式、振る舞い、意味を維持しながら、匿名化されたサロゲート値で機密のデータ要素を暗号化する必要があります。

解決策：フォーマット保持型暗号 (FPE) により保護をデータに埋め込む

セキュアに分析を行うには、保護の拡大とリスク軽減を両立させることが大前提です。これには、データに保護を埋め込むことにより、インフラストラクチャシステムおよびネットワーク境界の管理を強化することが不可欠です。

ArcSight Data Platform 用 の ArcSight Secure Data フォーマット保持型暗号 (FPE) アドオンを備えた Voltage SecureData Enterprise by OpenText™ 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、フィールドレベルまたはサブフィールドレベルで機密の構造化データを暗号化します。数値、記号、文字、数値の関係性、複数の分散データセットにわたる参照の整合性といった、元のデータの特性は保持されます。

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。保護されたデータは、データ侵害の発生時には無価値なものとなるため、保護がない場合に発生する可能性がある罰則とコストを回避できます。

主な使用事例：予測分析、自動車のメンテナンス

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

自動車メーカーは、様々な使用事例に予測分析を利用することにより、需要感知、サプライチェーンの問題の予測、新たな安全性や品質の問題の特定などが可能になります。ビジネス上の成果には、顧客満足度、車両の安全性、ブランド認知度の向上が含まれます。または、品質保証にかかる総コストの削減にもつながります。

サイバー攻撃の脅威が高まり、データプライバシー規制が増加するなか、分析時にすべての機密情報が保護される仕組みを設けることが重要な目標となります。自動車メーカーに必要なのは、データサイエンティスト、データベース管理者、サードパーティが、リレーショナル / 非リレーショナルデータベースやストレージにわたって機密情報をセキュアに使用できる、実証済みの統合アーキテクチャです。

今日、自動車メーカーはこのビジョンを Voltage SecureData Enterprise によって実現しています。あらゆるデータタイプ、数百ものアプリケーション、データレイクにわたって、ペタバイト級のデータのセキュリティを確保できます。OpenText Simple API により、幅広いビッグデータ製品や ETL 製品に簡単に統合することができます。既製のコードにより、Hive、Spark、Kafka/NiFi、Kafka/Storm、Map Reduce、Impala、Sqoop 用のテンプレートが提供されます。エッジノードを機密データのランディングゾーンとして利用した後、その機密データを HDFS に保存できます。

使用事例の 1 つとして、パフォーマンス分析に使用するリアルタイムなセンサーデータの保護が挙げられます。データは IoT エッジで保護され、路上を走行する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 やその他の環境に保存され、オーケストレーションされます。

お問い合わせ
www.opentext.com

使用事例：自動車メーカーのデータフロー

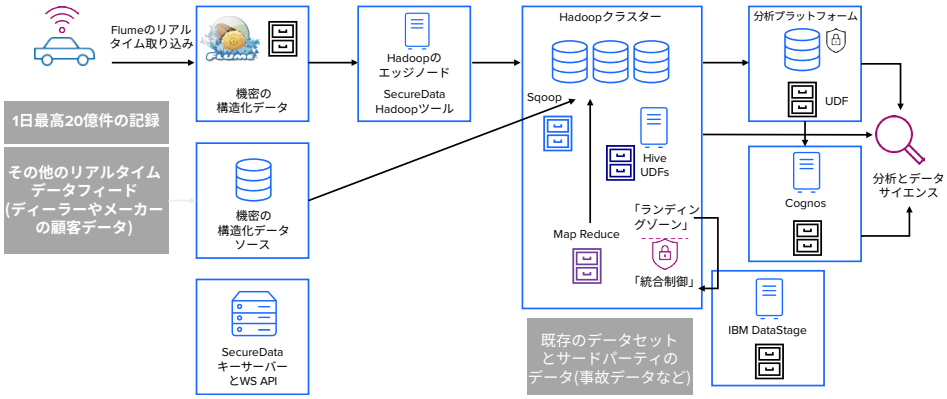

図 1. 自動車メーカーのデータフロー

顧客分析のためにビッグデータの力を安全に解放する

自動車メーカーは、Voltage SecureData と FPE および SST により、次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用の値を安全に抽出
- GDPR、CCPA、PCI DSS などのデータ保護規制を遵守
- 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

分析で得た知見をより多くのユーザーとアプリケーションに提供してビジネスの価値創出を促進するには、ビッグデータの力を解き放つ必要があります。

詳細はこちら：
www.microfocus.com/sdhadoop

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。