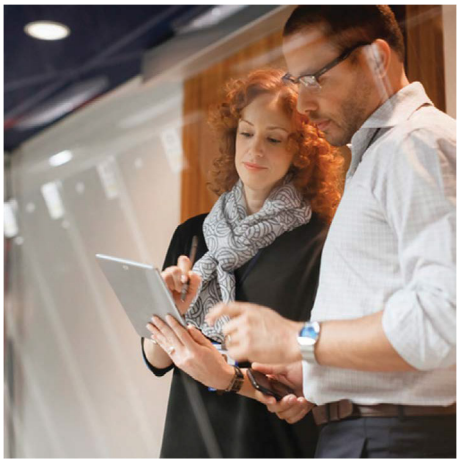
MICRO FOCUS

ケーススタディ
セキュリティ

欧州の保険会社

革新的なデータ中心型セキュリティ戦略では、Micro Focus® Voltage SecureDataを使用して、個人データの使用に関連するプライバシーの懸念に対処します。



概要

保険会社は、保有している顧客データを分析することで、ビジネスに役立つ貴重な情報を入手できます。ただし、このデータを不適切に使用した場合の法的リスクは増加しています。ここでは、欧州のある保険会社の事例を紹介します。この保険会社にとっては、国内のデータプライバシー規制と、2018年5月に発効するEUの一般データ保護規制 (GDPR) への対応が課題でした。同社は、Micro Focus Voltage SecureData Enterpriseを使用して、このようなリスクに対処しました。これにより、従業員は安心して顧客データを分析し、収益機会を発見できるようになりました。

課題

2018年にGDPRが発効すると、顧客情報の使用に対する制限はますます厳しくなると予想されます。この規制や他のプライバシー法規では、企業は、顧客の名前や誕生日といった個人を識別できる情報 (PII) を、特定の目的でしか保有できないと定められています。

「これは非常にスマートで高度に洗練されたテクノロジーです。他のベンダーも検討しましたが、このようなものはありませんでした。」

欧州の保険会社
ビジネスインテリジェンスマネージャー

これによって、データウェアハウスやビジネスインテリジェンスツールを使用している組織には、法的リスクが生じます。このようなツールは通常、できるだけ多くのデータを長期間にわたって保存するように設計されており、データを保存する目的は、データがレポートにまとめられるまで明確に定義されていません。このようなツールを使用しながらプライバシー規制に適合するためには、PIIに対するきわめて高度な保護が必要です。

「保険業界は、GDPRによる影響の範囲が特に広い業界の1つです」と語るのは、この欧州の保険会社のビジネスインテリジェンスマネージャーです。GDPRに違反した場合、罰金を科されたり、顧客の信頼を失ったりするおそれがあります。

AESCBC (Advanced Encryption Standard-Cipher Block Chaining) のような一般的な暗号化技術では、誕生日などの情報が、ハッシュと呼ばれる、数字、文字、記号からなる長い文字列に変換されます。データは元の形式で保存されなくなるため、開発者は、既存のデータベース構造と、暗号化されたデータを処理するプログラムを変更する必要があります。これはきわめて時間のかかる作業で、データの品質とシステムの信頼性が損なわれる危険性が高くなります。

一般的な暗号化方法を使用する場合のもう1つの問題点は、従業員が暗号化キーの管理に時間

概要

- **業界**
  保険/金融サービス
- **課題**
  コストを管理しながらデータプライバシー法規へのコンプライアンスを達成すること。
- **製品とサービス**
  Voltage SecureData Enterprise
- **成果**
  + データベースコンテンツの抽出、変換、ロードといった開発者の何年分もの作業が不要に
  + 顧客の個人情報とプライバシーの保護
  + データプライバシー法規へのコンプライアンスの達成
  + データセキュリティ統合のコストの削減

を取られることです。また、暗号化ソリューションは、この保険会社が使用しているデータ統合ソフトウェアのInformatica PowerCenterと組み合わせて使用できる必要があります。このソフトウェアは、さまざまなソースからデータを抽出して変換し、データウェアハウスなどの新しいシステムにロードする役割を果たします。

解決策

このような課題に対処するため、この保険会社は、Micro FocusのVoltage SecureData (SD) プラットフォームを利用することを決めました。 このデータ中心型セキュリティプラットフォームは、組織のさまざまなシステムを通過するデータを一貫して暗号化した状態で扱うことで、データを保護します。この暗号化プロセスを企業が容易に統合して展開できるように、いくつかの技法が用いられています。

Voltage SecureData Enterpriseの利点の1つは、Format-Preserving Encryption (FPE) が用いられていることです。クレジットカード番号、誕生日、電子メールアドレスといった情報は、長い文字列に変換されるのではなく、元の形式を維持したままで暗号化されます。

たとえば、誕生日を表す“07/07/1973”は、“04/03/2585”のような形に暗号化されます。数値が英数字のハッシュに変換されることはありません。これによって、統合に必要な作業が圧倒的に少なくなります。暗号化された情報は、会社のデータウェアハウスがもともと扱うように設計されている形式だからです。

また、FPEでは、データの意味、ロジック、値も保持されます。たとえば日付範囲内の関係などです。こういった要因は、一般的にビジネス分析にとって重要な意味を持ちます。

「これは非常にスマートで高度に洗練されたテクノロジーです。他のベンダーも検討しましたが、このようなものはありませんでした。SecureDataとそのFPEフレームワークを見つけたときは、本当にほっとしました」とビジネスインテリジェンスマネージャーは語っています。

Voltage SecureDataソリューションを使えば、暗号化キーの管理も容易になります。キーはキーデータベースに保管されるのではなく、ステートレスキー管理によってその場で作成されます。このため、キーデータベースの保護と維持にかかる費用を節約できます。

この保険会社は、これらの課題の解決に必要なテクノロジーを理解し、ソリューションを実装するために、Micro Focusパートナーの協力を得ました。両社の共同作業により、Voltage SecureDataをInformatica PowerCenterに 統合するのに1週間もかかりませんでした。ソリューションが実装され、テストされた結果、データウェアハウスでのデータの抽出、変換、ロードのプロセスに対して、すべての暗号化変換が正しく動作することが確認されました。この作業の完了後、この保険会社は、すべてのデータ環境でPIIの暗号化を通常のプロセスとして行う計画です。その開始は2018年初めに予定されています。

成果

コンプライアンスの達成

この保険会社は、Voltage SecureDataによる顧客の個人情報の暗号化が開始されれば、データプライバシー法規へのコンプライアンスを確実に達成できると予想しています。「当社はまだGDPR監査を受けていませんが、この戦略に従うことで、データのセキュリティとプライバシーに関するコンプライアンスを実現できると確信しています」とビジネスインテリジェンスマネージャーは語っています。

名前や誕生日といった情報をデータウェアハウスに平文で保存する代わりに、Voltage SecureDataではFPEを使用してデータを匿名化します。Informatica PowerCenterプロセスは、Voltage SecureDataを呼び出して、データウェアハウスの最初の永続的レイヤーにロードされるすべてのPIIを暗号化します。データは、データアウェアハウスのユーザーに提供されるまで、暗号化された状態でデータウェアハウス内に保持されます。

データウェアハウスのユーザーは、会社のセキュリティポリシーに基づく権限を持ち、正当なクエリを実行した場合のみ、顧客のPIIを見ることができます。これはデータプライバシー法規の中心的な要件です。

データセキュリティのコスト削減

実際にコストがどれだけ節約できたかは、プロジェクトが完了するまで計算できません。ただし、同社のビジネスインテリジェンスマネージャーによれば、Voltage SecureDataによって「間違いなく何年分もの時間と労力」を節約できたということです。

さらに、膨大なデータベース開発作業が回避されたことも、コスト節約に寄与しています。「Voltage SecureDataを見つける前に検討したすべてのソリューションでは、既存のデータベース構造、ETL (抽出、変換、ロード) プロセス、フロントエンドのデータウェアハウスモデル、レポートの変更に膨大な労力が必要でした」とビジネスインテリジェンスマネージャーは語っています。

このような余分な作業を行えば、開発者の他の仕事が滞ったはずだとマネージャーは述べます。「これ以外の方法で関連するすべてのデータプライバシー要件を満たそうとすれば、他の開発作業をおそらく何年もの間休止せざるを得なかったでしょう。」

これに対して、Voltage SecureDataの統合は、影響を最小限にするため、段階を踏んで行われました。「暗号化機能は、実装が完全に終わるまで、いわば休眠状態にあります」とビジネスインテリジェンスマネージャーは語ります。すべての要素の準備ができたら、開発者はいくつかのパラメーターを設定するだけで、データ中心型暗号化をオンにすることができます。「データウェアハウス内のPIIを含む属性を何千も暗号化する必要があることを考えると、データの危機を引き起こさずにデータ保護を実現する方法は他に考えられませんでした。」

「…この戦略に従うことで、データのセキュリティとプライバシーに関するコンプライアンスを実現できると確信しています。」

欧州の保険会社
ビジネスインテリジェンスマネージャー

「Voltage SDフレームワークの柔軟性のおかげで、サイレントモードでの実装が可能になりました。これにより、開発者やテスト担当者にとっての不都合や混乱を避けることができました。長い実装期間中に暗号化されたPIIと暗号化されていないPIIが混在していたら、これは避けられなかったでしょう」とマネージャーは語ります。「もちろん、最初にすべての環境ですべてのPIIを暗号化する際には、システムを停止する期間が必要になるでしょう。でも、その期間は数日かせいぜい数週間で、数か月とか数年という話ではありません。」

FPE以外にも、Voltage SecureDataには開発者の時間節約に役立ついくつかの機能があります。たとえば、開発者はシンプルなJavaアプリケーションプログラミングインタフェース (API) を使用して、Voltage SecureDataをInformatica PowerCenterに統合することができます。

「チームの数人のメンバーがわずかな労力をかけて、少数の再利用可能なコンポーネントを開発するだけで済みました。当社のデータ保護フレームワークは非常に小規模ですが、広範囲に広がっており、理解するのも維持するのも容易です」とマネージャーは語ります。

また、開発者は、暗号化プロセスに関する詳細な知識を持つ必要もありません。開発者の中でVoltage SecureDataのエキスパートは1人だけであり、暗号化プロセスは自動化されているので、他の開発者が行う技術的作業は少なくなっています。技術的知識とマンパワーはMicro Focusのパートナーから提供されるので、保険会社のデータウェアハウスチームはビジネス関連の作業に集中できます。

データ分析が使用可能

Micro Focusのソリューションを導入したことで、この保険会社は、安心してデータ分析を使用して収益機会を発見できるようになりました。

サービスやマーケティング活動の最適化のために、保険顧客に対するこのような情報の重要性はますます高まっています。

Voltage SecureData自体が直接顧客に関する情報を提供するわけではありませんが、データが保護されることで、従業員がデータにアクセスして分析できるようになります。従来は、PIIに対する保護が不十分だったため、PIIはデータウェアハウスシステムに統合されていませんでした。現在は、データは暗号化によって保護されているため、データウェアハウスにロードして保存しておくことができます。

その結果、Voltage SDによって、同社は責任ある方法でデータを取得し、保存し、使用し、そこから価値を抽出できるようになりました。

お問い合わせ先:
www.microfocus.com
この記事をシェアする。

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

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