

# 大手国際金融 サービス企業

Voltage と SDM により、メインフレームと Azure 間の安全なデータのやり取りが可能となり、規制への準拠とデータ分析をわずか 8 週間で実現しました。

## PSD2 コンプライアンスによって複雑になるデータ管理

ヨーロッパの銀行と同様に、この大手企業も新たなオープンバンキング時代の中でビジネスを行っています。オープンバンキングは、欧州経済地域全体で第三者が銀行情報を利用できるようにするものです。その目的は、銀行業務を最適化し、顧客が自身の財務データをよりきめ細かく管理できるようにすることです。顧客の同意を得ることで、顧客の財務データを第三者と自由に共有できます。その結果、銀行は、顧客に合わせてよりパーソナライズされた新しいサービスを提供できるようになります。オープンバンキングの安全性を確保するために、ヨーロッパのすべての銀行が決済サービス指令 2(PSD2)に準拠する必要があります。これにより、銀行の競争力が高まることで顧客にメリット

「Voltage と SDM はわずか 8 週間で実装され、すぐにメリットを実感できました。Micro Focus には独自の革新的なサイバーセキュリティソリューションがあるため、機密データを Azure クラウド環境にシームレスに複製し、必要に応じていつでも活用して分析できます」

シニアプログラムマネージングアーキテクト  
大手国際金融サービス企業

がもたらされます。また、自身の口座情報に誰がアクセスし、どのようにアクセスできるかをコントロールすることもできます。

金融データの安全なやり取りはすべての銀行が直面する課題です。この企業のデータセキュリティエンジニアは次のように説明しています。「大規模な銀行であるため、20TB を超える口座データを保有しています。その多くは非常に機密性が高いものです。こうしたデータはメインフレーム環境に保存され、さまざまなデータセンターでホストされています。PSD2 で定められているすべてのデータをメインフレームから公開しようとしたことが、このデータを持続的に共有する効果的かつ安全な方法はありませんでした」

さらに次のように続けます。「メインフレームといえば、誰もが非常に堅牢なデータセキュリティを想像します。これは事実ですが、規制や新しい働き方に対応するには、データを安全に転送する必要があります。これが閉じられたメインフレーム環境では問題となっていました。Microsoft とのパートナーシップをきっかけに、データセンターから毎日レプリケーションを行う Azure のクラウドアプローチを採用しました。Azure にはいくつかのセキュリティ機能があります。ただ、転送中の機密データやデータ分析のためにクラウドで使用するデータにはこれでは不十分だと考えていました。そこで、Microsoft とコンサルタントパートナーである Accenture 協業してソリューションを探しました」



## 概要

### 業界

金融

### 所在地

スペイン

### 課題

メインフレームに保存されているデータを安全に活用することで、オープンバンキングの規制に準拠し、より柔軟なレポート作成やデータ分析を実現する

### 製品とサービス

Micro Focus Voltage SecureData Enterprise

Micro Focus Structured Data Manager

### 主な成功要因

- レポート作成機能とデータ分析機能の大幅な強化
- 堅牢な暗号化アルゴリズムを使用したシームレスなクラウド統合
- PSD2、PCI、GDPR の各規制への完全準拠
- 実装期間はわずか 8 週間

# 「Voltage と SDM を組み合わせることで、データをオンザフライで安全に復号化できます。これは、当社のシナリオで非常に役立ちます。高い柔軟性により、レポート作成と分析の実行がはるかに容易になりました。おかげで、組織の将来の成功に不可欠なデータ主導の意思決定も可能になりました」

シニアプログラムマネージングアーキテクト  
大手国際金融サービス企業

## Voltage の強固な暗号化と Azure クラウドとの統合

データの爆発的な増加、そして一般データ保護規則 (GDPR)、Payment Card Industry Data Security Standard (PCI DSS)、PSD2 などの規制強化により、情報ライフサイクル全体にわたって確固たるポリシーと手順を実施することが求められています。Micro Focus Voltage SecureData Enterprise では、オンプレミス、クラウド、ビッグデータ分析プラットフォームなど、機密データが流れる場所を問わず、そのデータを安全に保護します。SecureData integrations for Azure の機能によって Voltage が提供する強固なデータ保護を Accenture と Microsoft は高く評価しました。Voltage が同社のアーキテクチャに最適であるとチームは感じ、Micro Focus と Microsoft の共同契約でソリューションが導入されることになりました。

「Voltage の暗号化と仮名化の機能が特に気に入っています」と、同社のシニアプログラムマネージングアーキテクトは述べます。「他のソリューションでは、転送中のデータを暗号化することはできません。これでは、分析目的でデータが必要な場合に役に立ちません。Voltage の仮名化は、個人識別情報 (PII) フィールドが1つまたは複数の人工識別子または仮名に置き換えるため、安全に可逆的な双方向データ変換を実現できます」

## Voltage+SDM がチームに成功をもたらす

パフォーマンスを損なうことなく、信頼性の高いプロセスと分析で大量のデータを管理するために、同社のチームは Micro Focus Structured Data Manager (SDM) を選択しまし

た。これにより、GDPR、PCI DSS、PSD2 などの最新のコンプライアンスおよび保護要件に従ってデータを保護できます。SDM と Voltage SecureData が連携することで、フォーマット保持型暗号 (FPE) を使用して、使用中またはアーカイブ中の機密データが自動的に暗号化されます。FPE を使用すると、データレベルの暗号化を従来のビジネスアプリケーションに統合できます。これが成功の鍵となります。FPE を使用しない場合、企業のデータアナリストはカスタムクエリとアルゴリズム、および手動プロセスを開発する必要があります。

メインフレームから企業のデータレイクである Azure Big Data への夜間増分データレプリケーションは Voltage と SDM によって管理されます。必要なデータ変換はすべて Azure Databricks によって実行されます。つまり、姓と名のフィールドからフルネーム (氏名) が作成された後、データは企業の Azure SQL データベースに保存されます。サードパーティプロバイダーは、クラウド API コネクタを介してこのデータを使用するため、隙のないデータセキュリティを確保できます。

SDM の使用範囲を拡張して、企業が見落としている可能性がある機密データを特定できます。使用可能なすべてのデータをスキャンすることで、SDM でデータを検出、分析、分類できます。その後、承認済みアルゴリズムによって、Voltage の暗号化プロセスを通じてこのデータを保護することも、データが冗長である場合はアーカイブもしくは削除対象として推奨することもできます。こうした自動化プロセスにより、コストを大幅に削減し、安全なデータの削除によるさ

お問い合わせ先: [CyberRes.com](https://www.cyberres.com)

この記事はいかがでしたか? シェアはこちら



らなるリスク軽減が可能になります。同社ではこれらについて今後検討する予定です。

## わずか8週間で完全な分析と柔軟なレポートングを実現

「Voltage と SDM を組み合わせることで、データをオンザフライで安全に復号化できます。これは、当社のシナリオで非常に役立ちます」と同社のシニアプログラムマネージングアーキテクトは述べます。「高い柔軟性により、クラウドサービスで安全にレポートを作成し、分析を実行することがはるかに容易になりました。おかげで、組織の将来の成功に不可欠なデータ主導の意思決定も可能になりました」

彼はこのように締めくくります。「Voltage と SDM はわずか8週間で実装され、すぐにメリットを実感できました。Micro Focus には独自の革新的なサイバーセキュリティソリューションがあるため、機密データを Azure クラウド環境にシームレスに複製し、必要に応じていつでも安全に使用して分析できます」

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](mailto:jp-info-enterprise@microfocus.com)  
[www.microfocus-enterprise.co.jp](http://www.microfocus-enterprise.co.jp)