# Voltage SecureData

## 新しいデータ主導型経済に対応したデータセントリックなエンドツーエンドセキュリティ

### データセキュリティの課題

データ量、ユビキタスコンピューティングの高度化、データフローのボーダーレス化によって、個人情報がどのように利用されているかを把握するのはますます困難になっています。このようなデータ主導型の経済では、さまざまな理由から、消費者は個人データの使用に関して企業を信頼するのは困難だと考えています。たとえば、データの不正使用に対する消費者の反応は、企業への支出を約 3 分の 1 に減少させる可能性があります。[1] また、企業や政府に対するサイバー攻撃は、世界的にその頻度と深刻さが増加し続けています。

Ponemon Institute の Cyber Crime Study[2] の調査結果によると、暗号化技術を使用している企業はサイバー攻撃の検出と抑制においてより効率的であることが示唆されています。Ponemon Institute の 2021 Cyber Crime Study[2] によると、1,000 件から 10 万件までのレコードの場合、企業に発生する一般的なデータ侵害のコストは、現在 1 件あたり 424 万ドルとなっています。これは過去最高記録です。いわゆる「大規模な」データ侵害で 5,000 万件から 6,500 万件のレコードが漏えいした場合、解決するためのコストは現在平均 4 億 100 万ドルに達しています。

しかし、このレポートによれば、人工知能 (AI)、機械学習 (ML)、ゼロトラスト、分析、暗号化をベースにしたセキュリティソリューションを採用している企業はいずれもデータ侵害の潜在的なコストを低減しました。高水準な暗号化を使用している組織 ( 保存中と転送中に少なくとも AES 256 の暗号化を使用 ) の場合、データ侵害の総コストは平均 362 万ドルでした。これに対し、低水準な暗号化を使用または暗号化を使用していない組織は 487 万ドルで、両者の差額は 125 万ドル (29.4%) でした。

1. Bridging the Trust Gap in Personal Data, BCG, March 2018
2. Cost of a Data Breach Report 2021, Ponemon Institute, July 2021

### Voltage SecureData 機能の特長

- あらゆる機密データを保護：さまざまなフォーマットを保持するデータ保護手法を使用してプライバシー、決済に関する規格と法規のコンプライアンスや、データセキュリティのニーズに対応
- FIPS 140-2 とコモンクライテリア (Common Criteria) の認定済みソリューション：機密データは、Micro Focus が先駆けとなった AES 暗号化の NIST 規格 FF1 モードで保護
- 演算負荷の高い作業や、マルチクラウド、オンプレミス、ハイブリッド IT インフラストラクチャのデータ急増を想定して設計
- REST API、ローカルクライアントライブラリ、プロキシインターセプターとドライバーインターセプターなどの柔軟性の高いさまざまなインターフェイス、および幅広いデータベース、オペレーティングシステム、アプリケーション、プラットフォームとの連携が容易なクラウドネイティブ機能
- オブジェクトストレージ、ストリーミングサービス、データディスカバリ、データウェアハウス、API ゲートウェイ、サーバーレスコンピューティング (FaaS)、マネージド Kubernetes サービス、KMS、シークレットマネージャーなど、主要なクラウドサービスプロバイダーが提供するサービスとの連携が可能
- シームレスなキーローテーション、Bring Your Own Key (BYOK) など、ステートレスなソフトウェアと HSM ベースのキー導出と管理により、高い可用性とスケーラビリティを実現
- Voltage Structured Data Manager でデータの発見、分析、分類を統合し、データ保護とリスク軽減を自動化

Voltage SecureData は、エンタープライズデータ保護のためのエンドツーエンドのデータセントリックなアプローチを提供します。ライフサイクル全体、つまりデータが収集された時点から、企業内で転送している全過程にわたってデータを保護できる唯一の包括的なデータ保護プラットフォームとなります。高リスクで脅威の多い環境に生データがさらされることはありません。これがデータセントリックなセキュリティの本質です。

Voltage SecureData は、保存中、転送中、使用中の機密データを保護するプラットフォームです。ユースケースが 1 つでも数百でも、オンプレミスおよびマルチクラウドハイブリッド IT のあらゆるデータ保護要件に対応できるように拡張することができます。データを「匿名化」して攻撃者にとって無意味なものにすると同時に、データプロセス、アプリケーション、サービスに対する操作性、有用性、参照整合性を維持します。保護対象のデータが本番システム、分析システム、テスト / 開発システム ( トレーニングや品質保証など ) のいずれにある場合でも、攻撃者にとってまったく価値のないものにすることによりデータ侵害を無害化します。

## 独自のアプローチによるエンドツーエンドのデータ保護

Voltage SecureData では、実績のある独自のデータセントリックな保護アプローチを取り、アクセスポリシーがデータと共に移動します。データのフォーマットや整合性を変更することなくデータを保護でき、証明書やキーの発行と管理のコストを削減し、複雑さを解消します。その結果、金融サービス、保険、小売、医療、エネルギー、輸送、通信、その他の業界における大手企業が、わずか 60 ～ 90 日という短期間で、全社でのエンドツーエンドのデータ保護を実現しています。これは、アプリケーションやデータベーススキーマの変更がほとんどの場合に必要ないためです。

### 短時間でデータセキュリティの成功を達成

ほとんどのアプリケーションは、変更なしで保護されたデータを利用できます。機密データを最初に収集するアプリケーションやビジネスの管理上の目的で生データを必要とするアプリケーションの場合、Voltage SecureData は、数十年前のカスタムアプリケーションから最新のエンタープライズプログラムまであらゆるシステムと簡単に連携が可能です。強力な集中管理型のポリシー制御 API により、Vertica、NonStop、Teradata、IBM メインフレーム、Linux や他のオープンシステム、オンプレミス、ハイブリッド、およびすべての主要なクラウドなど、さまざまなプラットフォームで暗号化とトークン化を実行できます。API により、ETL、データベースとアプリケーション、ネットワークアプライアンス、API ブローカー、Hadoop ディストリビューションなどのポートフォリオに広範に導入できます。SIEM システムでは、Voltage SecureData からイベントデータを取得して、データガバナンスレポーティング、アクティビティモニタリング、監査を実行できます。

Voltage SecureData は、PCI DSS、HIPAA、GLBA、世界各国のデータプライバシーに関する諸規制 (GDPR、CPA/CPRA、KVKK、POPI など ) に準拠して情報を保護します。また、Voltage SecureData は、ポイントツーポイントの暗号化 (P2PE) の PCI DSS 要件にも対応しているため、コンプライアンスの促進と、PCI 監査の対象範囲、時間、コストの削減が可能になります。

## 主な利点

Voltage SecureData により、機密データ漏洩のリスクを増大させることなく、リスクの管理、コンプライアンスの達成、デジタルトランスフォーメーションのメリット享受を実現できます。

### 業界標準のフォーマット保持テクノロジー

Micro Focus は、National Institute of Standards and Technology (NIST) の AES FF1 Format-Preserving Encryption（FPE）モード規格の特許保有者兼公式ライセンサーとして業界をリードしています。この NIST 規格は、政府機関向けの承認済み、実証済みのデータセントリックな暗号化方式で、グローバル企業でのデファクトスタンダードとして採用されています。NIST 規格は、組織が法規制や監査のコンプライアンスを維持し、実証済みの方法を使用してデータ漏えいを防止するために基準を設定するうえで重要な役割を担っています。

Voltage SecureData は FIPS 140-2 とコモンクライテリア (Common Criteria) の認定を取得しており、多数の標準化団体やワーキンググループでピアレビューを受けながら、業界の発展を推進し続けています。

CyberRes Voltage が、NIST、ANSI、IEEE、IETF、および独立したセキュリティ評価の専門家と協力して行っていることは、世界最大の金融サービス、銀行および保険機関、小売業者、製造業者、通信業者、決済処理業者に対して、当社がリーダーおよび信頼されるアドバイザーの立場であることを反映しています。

**ステートレスなキー管理 ( トランスペアレントで動的 )**

ステートレスなキー管理は、アプリケーションとそのユーザーが集中管理されたポリシーに従って適切に認証・承認された後、アプリケーションの要求に応じてその場で必要なキーを安全に導出します。ステートレスキー管理は、次のようにして IT コストを削減し、管理上の負担を軽減します。

- キーデータベースの必要がないほか、データベースを継続的に保護したり、サイト間でキーを複製またはバックアップしたりするためのハードウェア、ソフトウェア、IT プロセスも不要です。
- ネイティブおよび Web サービス経由の両方 で、シンプルなアプリケーション API を通じて管理上または法的な電子情報開示要件を自動化します。
- ID およびアクセス管理フレームワークと容易 に連携し、役割の変化に合わせて、ポリシーにより、データフィールドまたは部分フィールドへのデータレベルのアクセスを動的に適用することで、アクセスポリシーインフラストラクチャを最大限に再利用します。

GDPR などのプライバシー規制は、データセントリックな保護とポリシーをサービスとしてアプリケーションチームやプラットフォームチームに提供するようにグローバル企業に対して新たなプレッシャーを与えています。

Voltage SecureData は、個人識別情報 (PII)、Protected Health Information (PHI/ 保護されるべき健康情報 ))、Payment Card Industry (PCI) などの機密データを匿名化してプライバシーを保護し、エンドツーエンドのデータセントリックなセキュリティを提供します。Voltage SecureData は、個人データを保護し、新しい GDPR の仮名化ガイダンスに適合するための強力で柔軟な暗号化を提供します。

政府機関で価値の高いデータを保護しています。Voltage SecureData は、Federal Information Processing Standard FIPS 140-2 とコモンクライテリア (Common Criteria)、Format-Preserving Encryption (FPE) の認定を業界で初めて達成しました。政府機関や、政府機関を顧客としている民間請負業者は、民間企業のサイバーセキュリティを変革した実証済みの強力な技術を利用できます。

## 暗号化とトークン化

CBC、GCM、CTRなどのモードにおけるAES 256のような従来の暗号化アプローチは、図1に示すように、データ構造、スキーマ、アプリケーションに大きな影響を与えます。Voltage FPEは、AES (Advanced Encryption Standard)アルゴリズムのNIST規格FF1モードを使用するトークン化方式です。暗号化強度を低下させずに、データの元の形式を維持しながら、機密データを暗号化することができます。社会保障番号、クレジットカード、口座番号、生年月日、給与のフィールド、電子メールアドレスといった構造化データについては、データベースを変更したり、アプリケーションの機能やパフォーマンスに影響を与えたりすることなく保護できます。

従来の暗号化方式では元のデータフォーマットが大幅に変更されます。たとえば、16 桁のクレジットカード番号を AES で暗号化すると長い英数字文字列が生成されます。そのため、互換性のない形式に対応するためにはデータベーススキーマの変更が必要です。Voltage SecureData はデータのフォーマットが維持されるため、データベーススキーマの変更やアプリケーションの変更はごくわずかです。バルク暗号化用のツールを使用すると、ファイルやデータベース内の大量の機密データをすばやく非識別化できます。通常はシステム全体を保護するのに数日しかかからないので、コストを大幅に削減できます。Voltage SecureData は、暗号化パフォーマンスを高速化してビッグデータ、クラウド分析、IoT の大量のデータ処理ニーズに応えられ、ほぼ無制限のデータタイプをサポートします。

**納税者番号**
934-72-2356

**名：**Gunther
**姓：** Robertson
**SSN：**934-72-2356
**生年月日：**08-07-1966

| | | |
|---|---|---|
| **FPE**<br>AES-FF1モード | **253-67**-2356 | **名：**Uywjlqo **姓：** Muwruwwbp<br>**SSN：253-67**-2356<br>**生年月日：**08-07-1966 |
| **通常の**<br>AES-CBCモード | 8juYE%Uks&dDFa2345^WFLERG | lja&3k24kQotugDF2390^32 0OWioNu2(*872weW Oiuqwriuweuwr%olUOw1@ |

**図 1.** Format-Preserving Encryption (FPE) と通常の AES 暗号化の比較

トークン化にはさまざまな種類があります。

- **可逆 (Reversible)：**トークン解除のプロセスが存在する ( プライバシー用語でいう仮名化 ) ことを意味します。
  - **暗号：**強力な暗号技術を使用してデータ要素から生成されたトークン。クリアテキストのデータ要素は保存されず、暗号キーのみが保存されます。Voltage SecureData には、暗号トークン化用の Format- Preserving Encryption (FPE) を提供します。
  - **非暗号：**ステートレストークナイゼーション：無作為に生成されたメタデータに、トークンを構築するために安全に組み合わされるデータが格納されています。Voltage SecureData には、非暗号トークン用に Secure Stateless Tokenization (SST) が用意されており、高いパフォーマンス、セキュリティ、拡張性を提供します。

    **メモ：**Voltage SecureData は、他のトークナイゼーション・ソリューションで中心的な役割を担うトークンデータベースが不要であるため「ステートレス」で、カード所有者などの機密データを保存する必要がありません。SST では、FIPS 乱数生成器で作成された乱数を含む静的な生成済みテーブルのセットを使用しています。これらの静的テーブルを使用して、クリアテキスト PCI または PII の入力ごとに一意のランダムトークンを一貫した方法で生成します。その結果、元のデータと関係がないトークンが生成されます。SST ではトークンデータベースは不要であるため、トークナイゼーションプロセスの速度、スケーラビリティ、セキュリティ、管理性が向上します。
- **不可逆 (Irreversible)：**トークンを元の値に戻すことが現実的でない ( プライバシー用語でいう匿名化 ) ことを意味します。
  - サードパーティの分析、下位環境での本番データの使用などのためにデータ要素を匿名化するために一方向関数を使用してトークンを作成します。Voltage SecureData には、不可逆トークン化用に Format-Preserving Hash (FPH) が用意されています。

### VOLTAGE FORMAT-PRESERVING HASH を使用したデータの匿名化

クリックストリーム分析など、特定のユースケースでは、マスキングされたデータの復元が不必要なリスクとなるか、明らかに望ましくない場合があります。Voltage Format-Preserving Hash (FPH) には、FPE と同様にデータのフォーマットと参照整合性を維持するというメリットがありますが、元のデータを復元しないというメリットもあります。これにより、FPH は、従来の一方向変換技術 (SHA-256 など ) とは異なり、とぎれのない柔軟なアプローチで、高パフォーマンスのデータ操作性を提供できます。

| 機密データのタイプ | クリア内のデータの例 | 保護対象データの例 |
|---|---|---|
| クレジットカード番号 | 1111-2222-3333-4444 | 1111-2287-9581-4444 |
| 納税者番号 | 111-22-3333 | 740-36-3333 |
| 住所 | 1234 Maple Street | 7321 Uqhap Fbzir |
| 電話番号 | 415-555-1234 | 819-913-0471 |
| eメールアドレス | surfer1@mycompany.com | d8wLa2k @ cPAzlu3la .8fq |
| 運転免許証番号 | A1234567 | P9162047 |
| 生年月日 | 20-12-1970 | 10-01-1956 |
| 名前 | 王秀英 | 樂魚快的 |
| IPアドレス | 130.57.66.19 | 910.48.17.26 |
| ジオロケーション | 37.3974044, -121.9770816 | 81.7380129, -391.0193528 |
| VIN | 2W87Z7N139933 | UV19PA07CBL13 |
| 治療コード | 81082 | 81XXX |

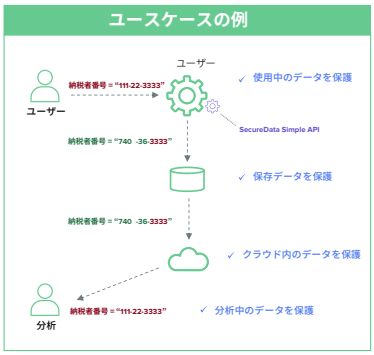


**図 2.** SecureData は世界で最も機密性の高いデータを保護

### テストデータの安全な管理とコンプライアンス

Voltage SecureData は、テストデータ管理のユースケースでは、本番環境データを匿名化し、開発者やユーザーが QA やデータの分析を実行できるように、構造的に有効なテストデータを作成します。Voltage SecureData Management Console により、ポリシーを簡単に制御して監査機能を利用できます。Voltage Structured Data Manager (SDM) は、ライフサイクル全体にわたる構造化データの完全な管理を可能にします。SDM では、オンプレミス、クラウド、ハイブリッドシステム内の機密データを検出し、社内ポリシーに基づいてアーカイブ、保護、削除、その他の廃棄を定義して、対象データを分類できます。SecureData と SDM の連携により、テストデータ管理を自動化してプライバシーのコンプライアンスをサポートし、テストおよび分析のユースケースで機密データを保護します。

**メモ：**CyberRes Voltage パートナーとプロフェッショナルサービスは、お客様がプロジェクトの範囲を決めて、高度な脅威に対処し、コンプライアンスの負担を軽減し、データプライバシーに関する困難な課題を迅速に解決できるように支援します。

### VOLTAGE SECUREDATA のアーキテクチャ

Voltage SecureData プラットフォームには、柔軟な導入オプションが用意されており、マルチクラウドハイブリッド IT インフラストラクチャ全体で高可用性と高パフォーマンスを確保します。仮想アプライアンスを導入する場合でも、Kubernetes クラスター内で実行されるクラウドネイティブなコンテナ化マイクロサービスを導入する場合でも、SecureData を拡張して、最も要求の厳しいエンタープライズ要件を満たすことができます。

これにより、複数の製品を導入・管理するコストと複雑さを回避しながら、さまざまな環境のユースケースに対応する適切な技術の組み合わせを選択することができます。

### VOLTAGE SECUREDATA SENTRY：透過的な導入により価値実現までの時間を短縮

ハイブリッド IT への移行や SaaS アプリケーションへの依存度が高まる中、企業や組織は API レベルの連携を行うためのアクセシビリティや開発リソースを持っていない場合もあります。Voltage SecureData Sentry は、ネットワークを流れる機密データを傍受することにより透過的なデータ保護を実現します。SecureData Sentry は、ハイブリッド IT への移行を簡素化してセキュリティコンプライアンスを迅速に実現することにより、価値実現までの時間を短縮します。また、アプリケーションを拡張したり、IT アーキテクチャを大幅に見直すことなく一貫した方法でエンドツーエンドのデータ保護を実行します。

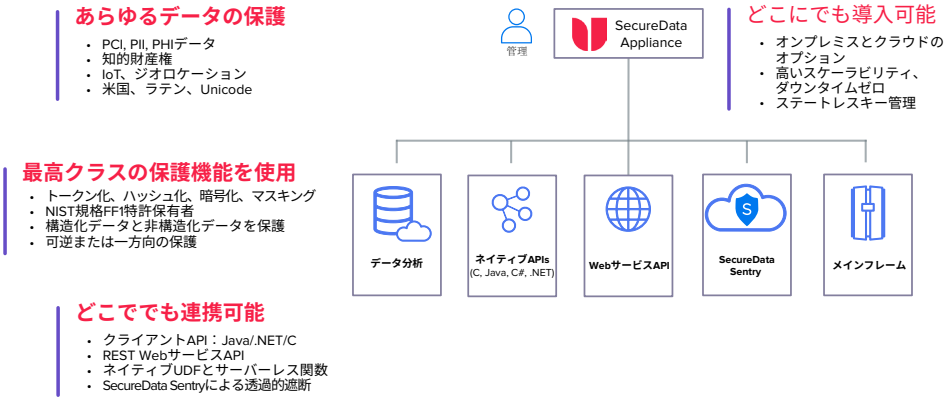


**図 3.** Voltage SecureData のアーキテクチャ

お問い合わせ先：CyberRes.com
この記事はいかがでしたか？
シェアはこちら

**「弊社は最新の金融サービス規制に完全に準拠しています。Voltage SecureData のおかげで、既存のインフラストラクチャを変更することなく業務への影響を最小限に抑えながらこれを実現できました。弊社は、複雑で分散した環境においてコスト効率の高い方法で機密データを保護しています」**

Christian Stork氏
戦略プロジェクト責任者
SIX

詳細情報はこちら：
www.microfocus.com/ja-jp/cyberres/data-privacy-protection/securedata-enterprise


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




CyberRes
A Micro Focus Line of Business