

Micro Focus Data Privacy Manager

データのライフサイクル全体を通じたプライバシーの管理と保護

主なメリット:

- + 短期間でのコンプライアンス徹底: ビルトイン分類ライブラリと設定済みルールにより、迅速に実装
- + 透明性: ハイブリッドIT全体のデータプライバシーのガバナンスの一つの画面から管理
- + 生産性: ビジネス運用を停止せずにプロダクションデータベースのデータ管理と保護を実現
- + 使いやすさ: 分析とビジネスプロセスに使用可能な状態のままでデータを保護
- + 防衛的廃棄: アクションの各段階を文書化し、製品コンプライアンスレポートを提供



データ主導型ビジネスの プライバシーの課題

今日のデータ主導型ビジネスは、分析から得られた情報を利用し顧客価値を創造し、運用効率を最大化し、競争優位性を実現しています。かつてないほどの大量のデータが企業全体を通じて収集され、ネットワークのエッジにある何百万台ものIoTスマートデバイスから、何千種類ものアプリケーションを通して、自社内、パブリッククラウド、プライベートクラウドに存在するリポジトリへと流れています。しかし、企業が収集する何テラバイトものデータの中には、重要な機密データも含まれています。このようなデータがもし漏洩すれば、経営陣は深刻な苦境に陥ります。漏洩が起きれば、売上減少にとどまらず、企業とその社員たちが長年にわたる努力で築いてきたブランドのイメージが損なわれます。

IT部門が扱うデータの量が増え続けているのに対して、現在のセキュリティやプライバシーの制御手法は、サイロ間の連携や集中的なポリシー管理が存在しないため、もはや効果がありません。企業は、どのような機密データがどこに存在し、どこを流れて、誰がそれを使用しているかを把握できておらず、データプライバシーポリシーの管理とガバナンスを集中制御できていません。さらにGDPR (EU一般データ保護規則) やその他のプライバシー法規制によって、データプライバシーの要件が厳格化し、データ漏洩に対するペナルティはますます厳しくなっています。これに対処するには、機密データの使用と廃棄を集中管理できる、信頼できるプライバシー管理が必要となります。

中央の一画面から集中して機密データを識別し、分類し、適切なレベルのプライバシーを適用して保護できる新しい手法が必要です。

データプライバシー管理の必要性

この新しい環境で機微なデータのプライバシーを実現するには、データのプライバシーをさらに高いレベルで調整し、統制することが必要です。これにより完全な可視性が実現され、制御のギャップを無くし効率を高め、企業のポリシーを一貫した形で統合することができます。ビジネス、IT、ガバナンス、コンプライアンス、セキュリティといった主要部門の関係者が関与することで、データのライフサイクルとセキュリティニーズ全体にわたるデータプライバシーポリシーの総合的な見方を確立できます。この包括的な「データプライバシー管理」手法を採用することで、プロセスを自動化し、データの秘密性に基づいて企業全体にわたる適切なプライバシーポリシーを定義できます。これにより、リスクの大きさと、競争優位性のためのデータ利用の間の必要性のバランスを取ることができます。

データプライバシー管理の最も重要な機能としては、企業内のあらゆる場所にある機微なデータを識別して分類できることが挙げられます。ポリシーを使用して機微なデータを集中的に自動管理し、ビジネスプロセスにおける使用可能性を維持しながらデータに必要な保護を加えることと、制御の証明となる監査レポートを作成して、プライバシー規制へのコンプライアンスを維持する機能が必要です。

Micro Focus Data Privacy Managerの概要

Micro Focus® Data Privacy Managerは、業界をリードするMicro Focusのガバナンスおよびセキュリティ製品であるStructured Data ManagerとSecureDataを統合して、機微な構造化データを持つ企業のプライバシーガバナンスのニーズに応える包括的ソリューションを実現します。Data Privacy Managerソリューションを使えば、機微な構造化データの管理と保護

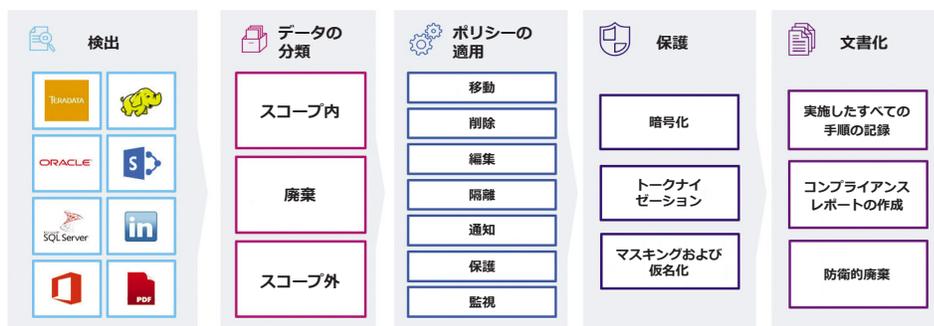


図 1: Data Privacy Manager

を、検出と分類から保護とレポート作成までのライフサイクル全体にわたって実現できます。

集中管理されたデータプライバシーガバナンス

Data Privacy Managerを利用することで、ハイブリッドIT環境全体から機微なデータを検出して、スコープ内データを処理のために分類できます。データは、設定済みのポリシーに従って、アーカイブ、保護、削除といった処理の対象とされます。

Data Privacy Managerは、Hyper Format Preserving Encryption (FPE) を利用することで、データが収集された時点から、拡張された企業内のデータまで、データのライフサイクル全体でギャップの無い保護を実現します。Hyper FPEは、データを「匿名化」することで、データの有意性とデータプロセス、アプリケーション、サービスでの参照整合性を維持しながら、データを攻撃者にとって無意味なものにします。

プロセスの完了時に、Data Privacy Managerはプロセスで実行された操作を記録するので、コンプライアンス監査のための詳細なレポートを作成できます。これらすべての機能は、使いやすいインターフェイスを通じて実行され、企

業全体の構造化データを1か所から管理できます。

Data Privacy Managerの主な機能

- **検出:** 企業全体のアクティブシステムと非アクティブシステムから秘密の構造化データを発見
- **分類:** データを分析し、設定済みのライブラリに基づいて、名前、社会保障番号、IDなどに分類
- **適用:** 集中的に設定されたプライバシーポリシーとセキュリティポリシーを適用し、企業全体のデータを1か所から管理 (移動、削除、隔離、通知、保護など)
- **保護:** 暗号化やトークナイゼーションを利用して秘密データをマスクまたは仮名化することで、プライバシーを保護しながら、ビジネスプロセスや分析での有用性を維持
- **文書化:** プロセス全体を通じて実行されたすべての操作を文書化し、コンプライアンス監査のためのレポートを作成

Micro Focus: 業界をリードする情報ガバナンスおよびセキュリティポートフォリオ

Micro Focusは、世界で最も包括的な情報ガバナンスおよびセキュリティポートフォリオを

持つ企業の1つです。当社のソリューションを利用することで、企業は、情報管理とガバナンス、セキュリティ確保を実現し、データ漏洩を検出して対応し、IDとアクセスを管理できます。当社の情報ガバナンスおよびセキュリティソリューションには、以下が含まれます。

- **非構造化データ管理:** ControlPointは高度なファイル分析ツールであり、接続されたデータソースでの非構造化データに関する情報ガバナンスを容易にします。ControlPointを使えば、データの形式や場所にかかわらず、ポリシーを簡単に定義して適用できます。
- **コンテンツの自動分類:** Content Managerは、ガバナンスベースのエンタープライズコンテンツ管理システムであり、政府機関、規制産業、グローバル組織などでの、ビジネスコンテンツの作成から廃棄までの管理を支援します。
- **ユーザー行動分析 (UBA):** ArcSight User Behavior Analytics (UBA) を使用することで、セキュリティアナリストは、サイバー攻撃のリスクと影響をリアルタイムで可視化できます。ArcSight UBAは、専用のセキュリティ分析を通じて未知の脅威を検出します。そのために、ユーザーとエンティティの通常の動作のベースラインを作成し、ユーザーとエンティティに関する異常が発生した場合に特定します。
- **IDガバナンス:** NetIQ® アイデンティティ管理は、効果的なアクセス検証方式を実現するためのソリューションであり、IDガバナンス制御を実装することで、コンプライアンス義務を果たしながらプロアクティブにリスクを削減できます。

- **アプリケーションセキュリティ:** Fortifyは、エンドツーエンドのアプリケーションセキュリティソリューションです。オンプレミスおよびオンデマンドの柔軟なテスト実行によってソフトウェア開発のライフサイクル全体をカバーし、セキュリティを組み込むことで開発期間を短縮できます。

Data Privacy Managerは、以下の2つの主要な製品を統合したものです。

Micro Focus Structured Data Manager: 構造化データのライフサイクル全体を通じた完全な管理を可能にします。Structured Data Manager (SDM) は、オンプレミス、クラウド、またはハイブリッド環境内の機微なデータを検出し、スコープ内データを廃棄のために分類できます。SDMではポリシーベースのデータ処理が可能であり、設定した企業ポリシーに基づいて、アーカイブ、保護、削除と任意の処理を定義できます。プロセスの完了時に、Structured Data Managerは実行されたすべての操作を記録するので、コンプライアンス監査のための詳細なレポートを作成できます。SDMのこれらすべての機能は、使いやすいインターフェイスを通じて実行され、企業全体の構造化データを1か所から管理できます。

Micro Focus Voltage SecureData: エンドツーエンドのデータ中心型アプローチによる企業データ保護を実現します。SecureDataは、Hyper Format Preserving Encryption (FPE) を利用することで、データが収集された時点から、企業全体の中でのデータ移動を通じて、データのライフサイクル全体でセキュリティギャップのないデータ保護を実現します。SecureDataは、データを「匿名化」することで、データの使いやすさおよびデータプロセス、アプリケーション、サービスでの参照整合性を維持しながら、データを攻撃者にとって無意味なものにします。

データの保護と有用性: Hyper FPEは、分析やビジネスプロセスでの有用性を保ったままデータを保護し、利便性を損なわずに保護を実現できます。Hyper FPEは、ID、VIN、銀行口座など、事実上無制限のタイプをデータの形式を維持した状態で暗号化できます。このため、データは既存のデータベースやアプリケーションでそのまま処理できます。また、Hyper FPEはデータの関係性、コンテキスト、意味を保持するので、ビッグデータ、クラウド、IoTのデータを匿名化し分析に利用できます。

GDPRなどのグローバル法規制への適合、ビッグデータプロジェクトの保護、ハイブリッドITの採用、あるいはレガシーシステムの保護などの課題に対して、Data Privacy Managerは構造化データのライフサイクル全体を通じてプライバシーの管理と保護を実現できます。クラウド、レガシーシステム、商用環境、ストレージサーバーなど、組織のあらゆる場所に存在する機密データの検出、分類、保護、管理、監査が可能です。

詳細情報

<https://software.microfocus.com/en-us/products/voltage-data-encryption-security/privacy-compliance/overview>

www.microfocus.com



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