

インフォマティカのビッグ データセキュリティ

機密データの場所、保護状態、量、拡散状況、利用、価値を評価することで、セキュリティへの投資を優先付けし、データ保護のリソースとプロセスを重視するためのリスクベースのビューを作成できます。

インテリジェントなデータセキュリティをビッグデータのインサイトと意思決定の基礎に

貴社のデータは本当に安全ですか？消費者も政府機関も企業も機密データの安全性とコンプライアンスを懸念しています。データ侵害は増加しており、「もし」発生したらどうするかではなく、「いつ」発生するののかということが重要になっています。GDPR（EU一般データ保護規制）などの新しい個人情報保護規則は、データとその利用についてプライバシー保護を確保するための要件を定めています。境界でのセキュリティの確立はある程度の保護にはなりますが、高いスキルを持ち、組織化されている攻撃者の断固たる攻撃を防ぐことはできません。データセキュリティに新しいプロアクティブなアプローチを実行する時機が来たと言えるでしょう。

企業には、ビッグデータを活用して顧客と運用環境への理解を深め、独自のビジネスチャンスを手にする機会があります。データを民主化すれば、データの悪用やデータ侵害のリスクを注意深く管理しながら、社内の部署および担当者を横断したデータアクセスが可能になります。最初の段階から攻撃を阻止するための新しい境界をセキュリティに加えることで、データ中心のプライバシー規則を遵守し、データ侵害に対する回復性を高めることができます。この新たな境界すなわちデータ境界は、企業の重要な資産である機密データや個人データの保護とリソースを重視しています。ただし、新たに境界を追加するだけでは十分なデータ保護にはなりません。

データセキュリティへ、新しいデータ中心のアプローチを採用する時機が来ています。機密データの場所、保護状態、量、拡散状況、利用、価値を評価することで、セキュリティとコンプライアンスへの投資を優先付けし、データ保護のリソースとプロセスを重視するためのリスクベースのビューを作成できます。さらに、IT担当者は地理やアプリケーション、サーバーに基づくデータの詳細な分析機能を使用して、最適な改善措置に関するインサイトを提供し、機密データのリスクを軽減できます。

データをビッグデータ環境へ移行する前に、リスク分析と改善措置によってデータプライバシーやセキュリティに影響を与えずに、データ環境を拡張することが可能になります。機密データの継続的な分析によって、効果的なリスク管理を実現できます。

データ中心のセキュリティを基盤にするデータアナリティクスとインテリジェンス機能が、機密データのリスクを明確にし、データ自体を保護します。また、対象のリスクに応じて、従来型のセキュリティソリューションをビッグデータ環境に導入することもできます。

ビッグデータセキュリティソリューション

インフォマティカのビッグデータ向けインテリジェントデータセキュリティソリューションには、数々の賞に輝く Informatica Secure@Source[®]とデータマスキングソリューションが含まれます。Secure@Sourceは機密データの探索、分析、可視化のプロセスを自動化し、データ保護チームが機密データのリスクを迅速に把握して、データに適切な制御やポリシーを適用できるようにするとともに、時間とコストを要する手作業のデータ監査に代わって機密データのリスクを定義、検出、分析する精度の高いプロセスを提供します。

インフォマティカのデータマスキングソリューションを使用すれば、企業はレポーティングアプリケーションやアナリティクスアプリケーション、またミッションクリティカルなアプリケーションのデータを匿名化および非機密化して、プライバシーや規制における懸念をなくすことができます。データマスキングは、単なる暗号化を超えて、顧客アプリケーションや業務アプリケーションで使われているデータを保護します。

主なメリット

法規制へのコンプライアンスの促進

法規制では、複数のシステム、部門、役割、場所全体で、データの保管場所、増殖、保護、使用状況に基づいてリスクを正確に把握することが求められます。どこにデータがあり、誰がアクセスし、どのような制御が行われているのかを知っておく必要があります。しかし、ビッグデータの急激な増加と増殖により、これらを把握することはますます困難になっています。

データ中心のセキュリティでは、規制対象のデータについてリスクベースの分析を実行し、単にデータが移動するエンドポイントやネットワーク、アプリケーションではなくデータ自体を保護するので、いつでもデータを探索、分類、分析、保護できます。

ビジネスのスピードに合わせた機密データの保護

業務要件を妨げることなくデータの増加スピードにペースを合わせることは、難しい場合があります。Persistent Data MaskingとDynamic Data Maskingによって匿名化と非機密化を実行することで、このような要件に応える柔軟性を確保できます。Dynamic Data Maskingはミッションクリティカルなアプリケーションのプライバシーを保護し、高速エンジンによりユーザーのスループットに影響を与えません。Persistent Data Maskingはコンテキストと参照整合性を保持したままデータを匿名化するので、テスト環境、分析、サポート環境でデータを使用できます。

インフォマティカについて

デジタルトランスフォーメーションによって我々の期待値が変化しています。より良いサービスを、素早く、便利に、低コストで利用したいという期待が高まっているのです。企業も状況に応じて変化する必要があります。そしてそのヒントは「データ」にあります。

エンタープライズ向けクラウドデータ管理で世界をリードするインフォマティカは、俊敏性の向上、新たな成長機会の獲得、新しいソリューションの開発を実現するための洞察を通じて、あらゆる産業や分野の企業がインテリジェントにビジネスをリードできるよう支援します。インフォマティカは、あらゆるデータを徹底的に重視し、企業の成功に必要とされる汎用性を提供します。

インフォマティカは、企業がこれからのインテリジェントな破壊的イノベーションを推進できるよう、当社が提供するあらゆるサービスを通じてデータの力を継続的に引き出すことを支援します。

機密データの特定とリスクの分析

数多くの複雑なプライバシー保護法や業界規制では、データのリスクを正確に把握するとともに、一定の条件下でアラートを発することが求められます。このため、ユーザーの行動や権限を分析し、高リスクなユーザーを特定してデータリネージを視覚的に追跡するとともに、ビジネス上の優先課題やガバナンスに基づいて機密データのリスクを評価する必要があります。

インフォマティカのビッグデータセキュリティでは、リスクを高めることなく、より多くのデータソースやデータプラットフォームから収集したビッグデータを活用することが可能になります。インフォマティカ独自のメタデータ主導の人工知能（AI）を使ったデータセキュリティアプローチにより、完全に自動化した体系的な方法でビッグデータを保護できます。

