Informatica

ホワイトペーパー

セキュリティ侵害から マスターデータを保護する ための4つの戦略

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、俊敏性を高め、新たな成長機会を実現するだけでなく、新たなイノベーションを生み出すことさえ可能にする将来への洞察力を提供します。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。

目次

エグゼクティブサマリー

顧客データ、製品データ、サービスデータ、業務データといった業務上重要な企業情報の信頼できるビューを構築するため、企業はマスターデータ管理（MDM）に投資をしています。MDMでは、欠かせないデータ要素を全社規模で組み合わせて統合レコードを作成し、これらを必要とするユーザーやアプリケーションに共有可能な信頼できるデータとして提供します。これは、顧客中心主義を追求するあらゆる企業に計り知れないメリットをもたらします。カスタマーサービスやロイヤリティプログラムを強化したり、製品管理やソリューションの効率を高めたり、安全にクラウドへ移行することが可能になります。

信頼できるデータは、企業の顧客／製品イニシアチブにとって重要な資産となり、競争優位性をもたらします。しかし、統合された機密データは、外部からの攻撃の格好の標的となり、データセキュリティ侵害や社内での悪用につながることもあります。そのため、EU一般データ保護規則（GDPR）やカリフォルニア州消費者プライバシー法（CCPA）などのプライバシー関連規制の対象となっています。

このような環境におけるデータ保護とコンプライアンスについて、次のような疑問がわくのは当然です。

- データはどこに保存され、どのように移動しているのか?
- どこからリポジトリにデータが供給され、誰がどのようなアプリケーションを使用してデータにアクセスするのか?
- 現在のアクセスや利用は、規制や承認済みのデータ使用ポリシーに従っているか?
- データの保護は適切であり、データのリスクは許容可能なレベルか、または改善すべき不適切なリスクを生む状況か?

機密性の高い顧客データの検出と分類の結果が、マスターデータのリスク、保護、プライバシー法規制へのコンプライアンスに関する意思決定をサポートする基盤となります。

このホワイトペーパーでは、次のことを可能にするデータ中心型ソリューションによってリスクを軽減するための考慮事項と戦略のフレームワークを紹介します。

- アナリティクス、メタデータ主導のインテリジェンス、自動化、AIを活用して機密性の高いマスターデータを識別し、保護する。
- 変化するデータガバナンスおよびプライバシー規制に対応する。
- 監査に備えた管理体制が整っていることを証明する。
- 調査が必要となるユーザーの異常な挙動が発生した際に関係者へアラートを通知する。

はじめに

調査企業IDC社は、2025年には世界中で生成されるデータ量が175 ZB（ゼタバイト）に達すると予測しています（2018年は33 ZB）[1]。収益の向上、顧客へのサービス提供、生産性の向上、業務の最適化、および他のミッションクリティカルな業務プロセスを実現する上で、すべての業界の企業・組織がデータの精度、可用性、保護を必要としています。

データの量や用途は爆発的に増加し続けており、オンプレミスおよびクラウドの複数のサイロにさまざまなデータ形式で保存されている機密性の高いマスターデータも例外ではありません。このような条件があるために、従来のデータセキュリティは時代遅れとなり[2]、企業全体のマスターデータのセキュリティに対する新たなアプローチが必要とされています。

しかし、ほとんどの企業は高い機密性が必要なマスターデータがどこに置かれ、どこからアクセスされているのかを正確に特定できません。これは非構造化形式のマスターデータの場合に顕著です。このような可視性の欠如はリスクの増大につながります。実際、このような背景からデータセキュリティ侵害が現在のITセキュリティリスクのトップとなっています[3]。

機密性の高いマスターデータの不適切な使用に伴い、データセキュリティ侵害が増加しています。そこで、企業はリスク緩和戦略を策定する必要があります。この戦略には、次のような重要な機能を備えたデータ中心型セキュリティ製品の導入も含まれます。

- 全社規模で機密性の高いマスターデータを特定して分類するための、すべてのデータソースに対する可視性
- 機密性の高いマスターデータの保護メカニズムを導入してデータセキュリティ侵害を緩和する機能
- 現在のプライバシー関連規制へのコンプライアンス（ユーザーの動きを監視して異常な挙動をニアリアルタイムに報告するためのメタデータ主導のインテリジェンス、自動化、AIの活用を含む）
- リスク評価および機密データ管理のための機能豊富なアナリティクス視覚化ツール
- 監査に対応する管理体制を実証するための透明かつ包括的なレポート機能

Gartner社は、サイロ化した連携のないデータセキュリティツールから統合型保護製品に移行する大規模企業は、2020年までに40%に達すると予測しています（現在は5%未満）[4]。このようなデータ中心型保護ソリューションは、リスクに晒されているデータの一元ビューを提供します。グローバル組織のすべての主要関係者は、機密データの動きを追跡し、ガバナンスポリシーや規制で求められる保護メカニズムを適用することができます。

機密データのプライバシーリスクを緩和するための4ポイント戦略

機密データのプライバシーリスクとは、不適切な露出で機密データを失うことによる影響で、最も一般的な原因はデータ侵害または内部ユーザーによる誤用です。リスクを緩和するには機密性の高いマスターデータの場所を特定するだけで十分であるというのは、よくある誤解です。このデータの特定と分類は、包括的なリスク緩和戦略の最初のステップに過ぎません。

[1] IDC社ホワイトペーパー「The Digitization of the World – From Edge to Core」2018年11月
[2] Gartner社「Market Guide for Data-Centric Audit and Protection」2017年3月21日
[3] Ponemon Institute LLC社「Data Breaches and Sensitive Data Risk」2016年2月
[4] Gartner社「Market Guide for Data-Centric Audit and Protection」2017年3月21日

続くステップでは、特定と分類の分析結果に基づいて、優先的に対応すべきリスクを評価します。そして、上位リスクを緩和する戦略を決定します。自動制御によってデータガバナンスポリシーを適用し、IT部門だけでなくすべての主要関係者の関与を促す必要があります。戦略の一環として、法規制へのコンプライアンスのための機能（リスク可視化ダッシュボードおよびコンプライアンスコントロールの監査レポート向けの充実した機密データアナリティクス視覚化、社内のすべての機密マスターデータタイプの保護など）を備えた、信頼できる、データ中心型のプライバシーおよび保護ソリューションを導入します。

1. 検出と分類

検出の一般的なアドホックアプローチは、既存のソースを確認して質問票を送信するというものです。しかし、手作業のアプローチは、貴重な時間とリソースを消費するため不適切です。加えて、ユーザーの行動やデータフローを実際にモニタリングせずに自己報告に頼っているため、多くの場合、不正確ですぐに時代遅れとなります。

次のことを自問自答する必要があります。

- どのようなデータを保存しており、誰がどのような目的でアクセスするか?
- ユーザー権限の管理とデータ権限のプロビジョニングをどのように実行するか?
- 機密性の高いマスターデータをどのように保護し、適切な制御をどのように確保するか?

検出と分類のコンプライアンスに関するその他の考慮すべき事項には、次のようなものがあります。

- データベースや非構造化データを含めたデータ環境の定義と理解
- 機密マスターデータを格納しているシステムのマッピングおよびデータとIDのマッピング
- 組織のエコシステム全体においてこのデータの移動をマッピングできるソリューションの調達と、アナリティクスおよびレポート作成ツールを使用するニアリアルタイムのビューの管理

2. コンプライアンス

企業はデータのリスクを特定、監視、軽減することで、データプライバシー規制に準拠しようと努めています。さらに、コンプライアンス違反につながる可能性のあるデータアクセスまたはデータの移動を監視、分析し、発生時にはアラートを出す必要があります。

2018年5月25日発効のGDPRは、EU内のすべての個人のデータ保護を強化・統一して国際ビジネスの規制環境を簡素化する目的で採択されました。同様に、2020年1月1日施行のCCPAは、プライバシーの基準をさらに強化したもので、保護対象が世帯データにまで広げられています。

多くの企業はまだこれらの規制への対応準備が整っておらず、十分に準拠できていませんが、違反すれば多額の罰金を科せられ、評判が低下します。逆に、準拠態勢を確立できれば、マスターデータのプライバシーに関する差別化要因として競争優位性を高める機会となり、顧客のロイヤリティを強化して、デジタルトランスフォーメーションを促進することも可能になります。さらに、優れたデータ保護を実証できれば、データの取り扱いに関して顧客の信頼を獲得し、現在の5倍もの個人情報にアクセスできるようになります。[5]

[5] Boston Consulting Group社「Bridging the Trust Gap in Personal Data」から抜粋

企業はGDPRやCCPAなどのプライバシー規制関連の「データドメイン」を含むデータストアを特定する、インテリジェントなポリシーを作成する必要があります。このようなポリシーは、どの組み合わせがプライバシーの脅威をもたらすかを判断するデータインテリジェンスロジックを含む、多元的なものとなります。

3. 保護

2019年第3四半期の時点で5,000件以上のデータ侵害が発生し、80億近くのレコードが漏洩しています。[6]データプライバシーおよびセキュリティに多額の投資が行われているにもかかわらず、依然として重要な個人データは危険に晒されています。企業はリスクの高いデータを継続的に保護し、疑わしい行動、不正使用、不正移動を特定して、改善措置を自動化して調整する必要があります。

従来のサーバーアクセスコントロールやファイアウォール、システム中心のサイバーセキュリティツールだけに頼るのではなく、最も重要なデータリスクを特定して、データモビリティ（移動性）をサポートするデータ中心のコントロールを通じて、これらのリスクを優先的に改善する必要があります。データ中心のコントロールとは、マスキング、アイデンティティ（ID）ベースのコントロール、暗号化などです。

また、データプライバシーを制御するだけではなく、IDベースのデータアクセスや行動を監視する必要もあります。過度なアクセスや通常とは異なる行動は、ユーザーがプライバシーポリシーを遵守していない、またはユーザーの資格情報が盗まれた可能性があることを示している場合があります。

4. 監査の準備と対応

企業は以前よりも、機密データの監査や評価を実施するようになっています。重要なデータを可視化し、保護していることの証拠を監査人に示そうとしているからです。

組織は、迅速に監査人に対応して、データの場所、リスク、保護方法、使われ方を認識している証拠を提示できなければなりません。部門または地域ごとに要約され特定のデータドメインを詳細に確認できるレポートや可視化情報を監査人が求める場合があるということを、組織は頭に入れる必要があります。

結論

企業は、マスターデータ管理を活用することで業務とサービスを変革することが可能になります。マスターデータは明確なメリットをもたらすと同時に、社内外での不正使用の標的にもなり得ます。絶え間ないデータ侵害の攻撃やコンプライアンス要件の増加を背景に、企業は機密データを特定、分析、保護するためのプロセスやツールをあらためて検討・評価する必要があります。

プライバシーのリスクや日常的なデータ侵害が増加している現在、企業は堅牢なデジタル戦略を構築して、機密性の高いマスターデータのリスクを継続的に監視、分析、改善、緩和しなければなりません。企業は、不正利用やデータセキュリティ侵害の兆候、異常なアクセスと行動、国境を越えた不正転送などをニアリアルタイムに監視する必要があります。このような不断の努力によって、MDMを活用してデータリスク対策の効果を高め、データ侵害や社内の不正使用の影響を緩和し、地域や業界の厳しい規制要件を満たすことが可能になります。

[6] Risk Based Security「Q3 2019 Data Breach QuickView Report」

提案

1. データプライバシーリスク評価を実施して、機密性の高いマスターデータがどこにあるのか、それがデータエコシステムを介してどこまで伝搬するのか、どの機密データセットの脆弱性が一番高いのかを明確に把握します。
2. 評価結果に基づいて、社内で最も機密性の高いマスターデータのソースに優先順位を付け、それらを保護する戦略とスケジュールを決定し、この戦略をデータプライバシーおよび保護アプローチとして試験導入します。
3. 自社のプライバシーコンプライアンスポリシーと、プライバシー法規制へのコンプライアンスの責任を負う主な関係者を規定して文書化し、これを配布します。今年および来年以降に向けて、戦略的計画を策定します。

詳細な調査

機密データのセキュリティリスクと保護に関する考慮事項の詳細については、以下の発行物と動画を参照してください。

Informatica Data Privacy Management

Informatica Master Data Management–Customer 360

ホワイトペーパー：データプライバシーの新たなパラダイム

Bloorレポート：機密データを検出

〒105-6226
東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー26階 電話：03-6403-7600（代表）FAX：03-3433-1021

IN09_0520_03409