Informatica

ホワイトペーパー

ハイブリッド環境向けのデータ中心型セキュリティ

クラウドおよびオンプレミス環境におけるGDPRコンプライアンス

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。

インフォマティカはエンタープライズ向けクラウドデータ管理で
世界をリードしています。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。

目次

エグゼクティブサマリー

今日、多くの企業が、数多くの多様なプラットフォームや世界中の物理的な場所に、機密性の高い顧客情報や商品情報、その他の重要なデータを保存しています。このような業務上不可欠なデータは、多くの場合パブリッククラウド、オンプレミス、SaaS（サービスとしてのソフトウェア）アプリケーションに保存されています。Informatica Intelligent Cloud Services™の使用により、インフォマティカはフェイルオーバーデータセンターの形でインフラストラクチャセキュリティ、ユーザー認証とアクセスコントロール、ネットワーク セキュリティ プロトコル、暗号化、オペレーティングシステムのセキュリティ層、データベース、アプリケーションレベルなどを提供します[1]。

ハイブリッド環境は、データコンプライアンスおよびセキュリティのチームに新たな課題を提示します。データ、ユーザー、アプリケーションは動的な性質を持つため、企業の重要なデータを常に追跡、把握、保護するための方策を追加する必要があります。世間の耳目を集めたクラウドやオンプレミスのセキュリティ侵害や、EU一般データ保護規則（GDPR）などの新たな規制が科している罰金など、リスクは仮定のものではありません。

このように動的なハイブリッド環境では、インテリジェンスと自動化によってデータ保護とコンプライアンスを維持し、次のような質問への答えを明確にしておく必要があります。

- 保護が必要なすべてのデータはどこにあるのか?
- 誰がどのアプリケーションを使用してデータにアクセスしているのか?
- 現在のアクセスや利用は、規制やデータ使用ポリシーに準拠しているか?
- データ保護は適切で、データのリスクは許容可能なレベルにあるか?または対応すべきリスクが発生する恐れがあるか?

機密データの検出と分類は、ハイブリッド データエコシステムにおけるデータリスク、セキュリティ、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、ハイブリッド環境におけるセキュリティの考慮事項や戦略のフレームワークと、以下のことを実現できるデータ中心型アプローチについて説明します。

- ダッシュボードおよびレポート作成の単一インターフェイスを使用して、アナリティクス、自動化、人工知能（AI）を適用し、ハイブリッド環境のすべてのソースからの機密データを保護する。
- 進化を続けるデータガバナンスおよびセキュリティに関する規制に対応する。
- 監査の準備を整える。
- ユーザーの異常行動が発生した場合に、主要な関係者にアラートを通知する。

Informatica Data MaskingとInformatica Secure@Source®は、これらの機能を実行するための優れた機能を提供し、ハイブリッドエコシステムにおけるすべての機密データソース向けに、統合されたデータ中心型のセキュリティ層を追加します。

[1] David Monahan著「Informatica Cloud Security Architecture Overview」Enterprise Management Associates（EMA）社 2016年3月

ハイブリッドの現実に即したデータセキュリティ

調査企業IDC社は、2025年には世界中で180ZB（ゼタバイト）のデータが生成されると予測しています（2015年は10ZB未満）[2]。すべての業界の企業が、収益の向上、顧客へのサービス提供、生産性の向上、他のミッションクリティカルな業務プロセスのサポートを実現できるかどうかは、データの精度、可用性、セキュリティにかかっています。

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保存されているさまざまなデータ形式の機密データも例外ではありません。このような状況から、従来のデータセキュリティは時代遅れとなり、全社規模のデータ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[3]。

企業が使用するデータの多くが、外部ソースから取得される傾向も強くなっています。データを複数のシステムに蔓延させたり、アナリティクスに利用したりする前に、このデータを社内へオンボーディングした時点での機密性を理解しておくことが重要です。しかし、多くの企業はすべての機密データがどこにあるのかを正確には特定できません。特に、非構造化データである場合や、さまざまなオンプレミス／クラウドアプリケーション、リレーショナルデータベース、データウェアハウスアプライアンス、ビッグデータソースに分散している場合には特定が困難です。このような知識がないことで、組織のリスクは高まります。また、このことが原因で、現在ではデータ侵害がITセキュリティリスクのトップとなっています[4]。

機密データの蔓延と同時にデータ侵害が増加する中、企業はリスク低減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
- 機密データの保護メカニズムを導入し、侵害を緩和する機能
- 現在のデータセキュリティおよびデータプライバシーに関する規制へのコンプライアンス（ユーザーの行動やレポートの異常を準リアルタイムで監視する自動化とAIの活用を含む）
- 機密データ管理のための、豊富なアナリティクス視覚化ツール
- 監査に備えるための透過的で堅牢なレポート作成機能

Gartner 社は、2020年までに大企業の40%で、異種で分断化されたデータ セキュリティツールが、データ中心型の監査および保護製品に代わると予測しています（現在は5%未満）[5]。Informatica Data MaskingやInformatica Secure@Sourceを含むこのようなデータ中心型保護ソリューションは、リスクに晒されるデータを一元表示することで、企業のすべての主要関係者が機密データの動きを追跡し、ガバナンスのポリシーや規制に必要な保護メカニズムを適用できるようにします。

[2] 「2016 IoT Midyear Review – The Report Card for Everyone」IDC社、2016年8月4日
[3] 「Market Guide for Data-Centric Audit and Protection」Gartner社、2017年3月21日
[4] 「Data Breaches and Sensitive Data Risk」Ponemon Institute、2016年2月
[5] 「Market Guide for Data-Centric Audit and Protection」Gartner社、2017年3月21日

機密データを保護するための4つの戦略

「機密データのリスク」は機密データを損失することの影響であり、この損失の大きな原因はデータ侵害です。よくある誤解は、リスクを低減するには機密データの場所を特定するだけでよいというものですが、このデータの特定と分類は、包括的なリスク低減戦略の第一歩に過ぎません。

次のステップでは、特定と分類の分析結果に基づいて組織のリスク評価を行い、データ ガバナンス ポリシーを強制する自動制御機能によって（IT部門だけでなく）すべての主な関係者に関係があるリスクを低減するための戦略を策定します。戦略には、法規制へのコンプライアンス、ダッシュボードおよび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の視覚化、および組織全体のすべての機密データタイプの保護を提供する、堅牢なデータ中心型セキュリティ製品の調達と導入が含まれます。選択したデータ中心型セキュリティ製品は、ハイブリッド環境のすべてのソース（パブリック クラウド、SaaSアプリケーション、オンプレミスのアプリケーションおよびデータベース、非構造化データ、データ ウェアハウス アプライアンス）からの機密データも保護できるものでなければなりません。

1. 検出と分類

検出の一般的なアプローチは、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、手作業の多いこのアプローチは、貴重な時間とリソースを消費するため不適切であるだけでなく、ユーザーの行動を実際に監視せずに自己報告に頼っているため、多くの場合不正確で時代遅れのアプローチと言えます。

企業は次のような質問への答えを明確に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それにアクセスするか。
- ユーザー権限とデータの権利をどのように管理するか。
- 機密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事項には、次のようなものがあります。

- 自社のデータ環境の定義および理解（オンプレミス／クラウドのデータベース、アプリケーション、非構造化データを含む）
- 社外から取得したデータの管理計画の策定
- 機密データを含むシステムのマッピング
- 自社エコシステム全体における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した準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やセキュリティに関する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日より発効されるEU一般データ保護規則（GDPR）は、EU（欧州連合）内のすべての個人データの保護を強化、統一し、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。多くの企業はまだこ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。その一方で、コンプライアンスは機密データのプライバシーおよびセキュリティに関する差別化要因として競争優位性の機会を提供し、データ主導のデジタルトランスフォーメーションの成果を促進する可能性があります。

企業はGDPR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考え方により、多元的なものとなります。

3. 保護

2017年には1,120件のデータ侵害事案が発生し、約1億7,100万件のレコードが流出しました[6]。インフラストラクチャレベルのセキュリティに莫大な金額の投資が行われているにもかかわらず、重要なデータの脆弱性は変わりません。企業はリスクの高いデータのセキュリティを継続的に確保し、疑わしい行動や、重要なデータ資産の不正使用または移動を特定して、改善措置の自動化とオーケストレーションを行う必要があります。

企業は重要なデータリスクを特定し、（従来のサイバー セキュリティ ツールではなく）データ中心型の制御によって改善措置を行う必要があります。例えばこのような制御には、データマスキングや暗号化ソリューションがあります。これらの他にも、企業はユーザーのアクセスや行動を監視しなければなりません。過度なデータアクセスや異常な行動は、ユーザーがプライバシーポリシーを遵守していないか、ユーザーの資格情報が盗まれたことを示します。

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。

企業は迅速に監査人に対応して、データの場所やデータリスクの意味、データの保護方法、データの使われ方を認識していることの証拠を提示できる必要があります。監査人はドリルダウンして特定のデータドメインを確認できる、部門または地域ごとに要約したレポートや可視化情報を求めるということを企業は頭に入れておく必要があります。

[6] 「2016 Data Breach Category Summary」Identity Theft Resource Center、2016年12月31日

結論

ユーザー、世界中のデータセンターサーバー、クラウドアプリケーション全体に機密データを転送するハイブリッド環境を保護するには、最高レベルのインフラストラクチャ セキュリティプロトコルが必要となります。データ違反の継続的な発生やコンプライアンス要件の増加を考えれば、企業は機密データを特定、分析、保護するための適切なプロセスやツールを導入しなければならないことは明らかです。

セキュリティリスクが高まっているとともにデータ侵害が日常的になっている今、企業は堅牢なデジタルセキュリティ戦略を確立して、機密データに対するリスクを継続的に監視、分析し、軽減措置をとらなければなりません。企業は、不正利用や侵害の兆候、過度なアクセス、異常な行動、国境を越えた転送などを準リアルタイムに監視する必要があります。Informatica Data MaskingやInformatica Secure@Sourceなどのデータ中心型のセキュリティソリューションを使用することで、企業はデータリスクに対する心構えを改善してデータ侵害や社内における不正利用の影響を軽減し、地域や業界の厳しい規制の要件を満たすことができます。

推奨事項

1. リスク評価を実施して、機密データがどこにあるのか、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が最も脆弱なのかを明確に把握します。
2. 評価の結果に基づき、機密性の高い上位10のデータソースを優先し、それらのデータを保護するための戦略と製品を決定して、データセキュリティの戦略を導入します。
3. 組織のコンプライアンスポリシーと、GDPR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。2018年5月のGDPR発効後に向けて、戦略的計画を策定します。

詳細情報

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、以下の発行物を参照してください。

- 『脅威の検知と保護：データ中心のセキュリティ戦略』インフォマティカ、2017年4月
- 『Data Breaches and Sensitive Data Risk 』Ponemon Institute、2016年2月

Informatica

〒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_0418_03429