

## データをアクセス可能で保護されたものに

最初是一元管理の記録システムでデータを安全に保護していたはずが、いつの間にか管理も制御もされていないサイロでデータが危険にさらされているケースがあまりにも多すぎます。

データをリスクから守りましょう

### データが脆弱であることを示す3つの兆候

#### 1 データ統合によりデータガバナンスが損なわれる

ロールおよびポリシーベースのアクセス制御は、データへの権限の管理、保護、監査に不可欠です。これらの制御をデータ統合のライフサイクルで管理していない場合、不要な複雑さとリスクが生じます。

#### 2 データセキュリティがアプリケーション開発者の負担になる

複数のデータサイロに散在するデータを完璧に保護することはきわめて困難です。残念ながら、多くの場合、セキュリティが単一のデータレイヤーでテストおよび保守されることはありません。そのため、新しいアプリケーションを導入するたびにアプリケーションレイヤーでデータを保護しなければならないことが開発者の負担になっています。

#### 3 インサイダー脅威のリスクが把握、管理されていない

過去に発生した大規模なデータ侵害の原因の一部は、内部関係者がデータへのアクセス権を所有していたことでした。残念ながら多くのデータベースは、セキュリティ制御がきめ細かくなく、オールオアナッシングのデータアクセス権しか設定されていないため、このような攻撃に対して脆弱です。これでは、データガバナンスと監査は不可能です。

以上の状況に該当する場合、最も安全で信頼性が高いNoSQLデータベースであるMarkLogicが必要です。

「顧客は、ニーズに合わせて素早く対応するサービスを期待しています。また、情報を安全かつプライベートに保存したいとも考えています。しかし、あまりに多くの企業が、アジャイル性を高めようとするあまりに、セキュリティやプライバシーを軽視してしまっています。」

- Joe Pasqua, MarkLogic, executive vice president of product strategy (上級副社長、製品戦略担当)

## 企業に信頼されるMarkLogicのセキュリティ

世界中の大手投資銀行、主要医療機関、政府の機密システムでは、最も要求の厳しいミッションクリティカルなシステムを実行するためにMarkLogicを採用しています。MarkLogic®は、コモンクライテリア認証を受けた唯一のNoSQLデータベースです。MarkLogicは、米国の情報機関、国防総省、法執行機関の機密性の高いシステムでも稼働しています。

きめ細かいアクセス制御、職務分掌、データセグメンテーション、高度な暗号化など、MarkLogicは、機密性、整合性、可用性(CIA)の3つの組み合わせを提供する上で必要な機能を備えています。ITエグゼクティブやセキュリティマネージャ、セキュリティ監査や情報セキュリティの担当者、あるいはアプリケーション開発者やソフトウェアサプライチェーンの安全性確保の担当者などは、MarkLogicを利用すれば、必要なデータ保護と同時に、ダイナミックな業務に必要なアジャイル性を獲得できます。



## MarkLogicでデータを保護し、アクセス可能にする

### KPMG

KPMGは、MarkLogic搭載のアプリケーションを構築し、規制、納税、報告義務の遵守を目的としたクライアントオンボーディングをサポートしています。このアプリケーションにより、複雑な手動プロセスをインテリジェントに自動化し、完全な追跡および監査が可能なデータワークフローを維持しています。

### Deutsche Bank

MarkLogicは、Oracleに代わって、同行の金融取引データのグローバルストアになりました。30を超すトレーディングシステムを統合した最初の本番システムは、わずか6ヶ月で稼働を開始し、安全で一貫性のあるトランザクションを維持しています。

### 米国情報機関

MarkLogicは、軍用メッセージングシステムを支えています。高度なアラート機能と検索機能により、数億件の記録や3万人を超えるユーザーのために、信頼性の高いきめ細かなアクセス制御を提供しています。

## MarkLogicでデータを保護

MarkLogicのデータベースプラットフォームは、複数のサイロのデータを統合する世界最高のデータベースとして、すべてのデータを統合し、それに関するアクセス、保護、管理を確保するために設計されています。

[jp.marklogic.com](http://jp.marklogic.com)にアクセスしてください