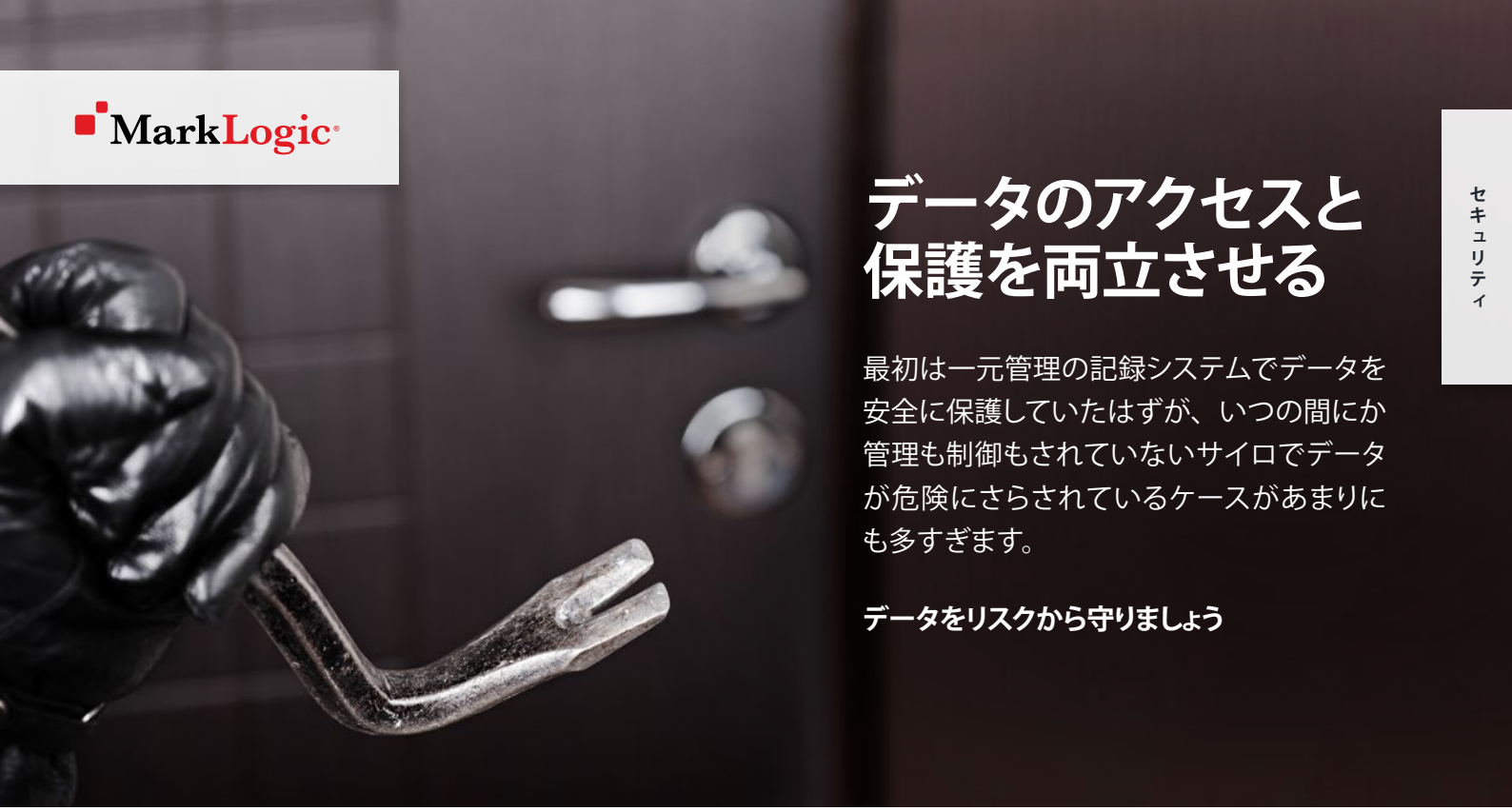

セキュリティ

データのアクセスと保護を両立させる

最初は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

複数のレイヤーやサイロに散在するデータを保護することは極めて困難です。残念ながら、セキュリティの検証や保守をデータレイヤーだけで完結できず、新しいアプリケーションごとに、開発者が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よくあります。

3 インサイダー脅威のリスクが把握、管理されていない

大規模なデータ漏洩事件のなかには、内部関係者にデータアクセス権があったことが原因のものもあります。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。

「顧客はニーズに素早く対応できるサービスを求めると同時に、情報は安全かつプライベートであるべきと考えています。しかしアジャイル性を高めようとするあまり、安全性やプライバシーが犠牲になってしまうケースが多々あります」

ジョー・パスクワ、MarkLogic 社上級副社長（製品担当）

MarkLogic®

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使われています。

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、完全性、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。

ドイツ銀行

MarkLogic は、オラクルに代わって、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 か月で稼働を開始し、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、軍事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。

詳細は jp.marklogic.com で

マークロジック株式会社 MARKLOGIC K.K.

150-0001 東京都渋谷区神宮前 1-5-8 神宮前タワービルディング 13F

03 4540 0337 | jp.marklogic.com | MarkLogic-JP@marklogic.com