MarkLogic®

アドバンスセキュリティ

データシート

MarkLogic®は、最も安全なNoSQLデータベースです。開発当初からエンタープライズレベルのセキュリティ機能に注力しており、組織が求める認証済みのきめ細かいセキュリティで現代のサイバー脅威からデータを守ります。MarkLogicには、ドキュメントレベルのセキュリティ、要素レベルのセキュリティ、監査、外部認証（LDAPとKerberos）のサポート、コンプライアンスアーカイブ、暗号化などが標準機能として備わっています。

これに加えて特定の用途のために、「アドバンスセキュリティ」オプションが準備されています。このオプションには、次の3つの追加機能があります。

- 外部鍵管理 – KMIP 1.2準拠の外部のサードパーティ鍵管理システムをサポート
- リダクション – MarkLogicとの間でデータをインポート、エクスポート、またはコピーする際、許可されていないユーザーへの機密情報の流出を防止
- コンパートメントセキュリティ – ドキュメントを操作するには、適切なロールをいずれか1つだけではなく、すべて持つことをユーザーに義務付け、セキュリティ制御を強化

MarkLogicのセキュリティの概要

MarkLogicは10年以上にわたり、データの保護およびセキュリティ対策に携わってきました。MarkLogicは、コモンクライテリア認証を得た唯一のNoSQLデータベースです（データベースベンダー全体でも、この認証を受けているのは6社しかありません）。Common Criteria for Information Technology Security Evaluation（情報技術セキュリティ評価のためのコモンクライテリア、通称「コモンクライテリア」）は、IT製品のセキュリティに関して、最も広範に利用されている国際的な相互認証です。

MarkLogicは、非常に厳しい要件を満たすデータベースが必要とされるシステムにインストールされ、実業務に利用されています。ここでは、アクセス、ユーザー認証、管理、監査、ロールの分離、システム保証などに関する厳しい基準を満たさなければなりません。これらを満たすことができるMarkLogicは、安全に関する要求が最も厳しい、投資銀行や大手のヘルスケア組織、政府の機密システムなどにおいて、基幹業務のアプリケーションの中核として採用されています。

MarkLogicにはデフォルトで、RBAC（ロールベースのアクセス制御）セキュリティモデルがあります。このモデルでは、各ユーザーに任意の数のロールを割り当て、そのロールを任意の数の権限やパーミッションに対応付けます。権限では、ドキュメント作成と機能実行（URIおよび実行権限）を管理します。パーミッションでは、ドキュメントに対する操作（読み取り、挿入、更新、実行）を管理します。

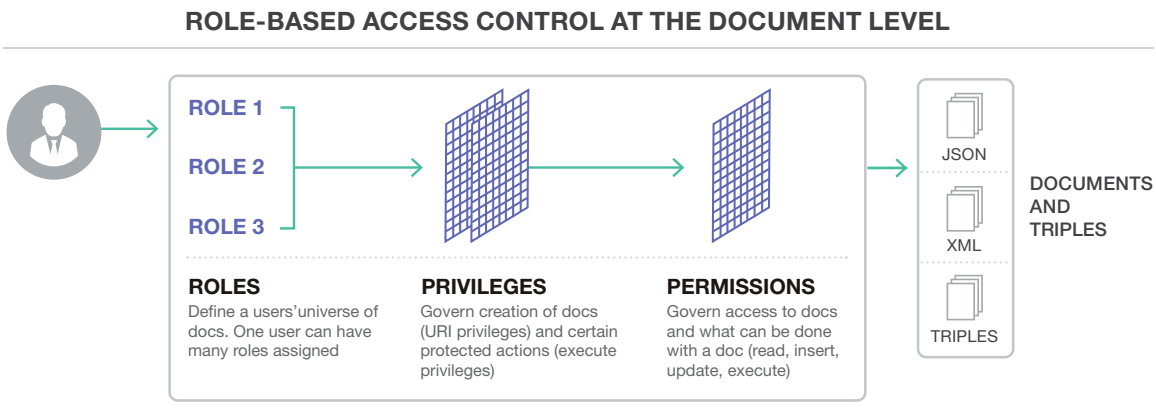

図1：各ロールには権限（書き込みと実行）とパーミッション（読み取りと変更）の両方がある

外部鍵管理

保存データの暗号化（Encryption at Rest）では、ローカルのKMS（鍵管理システム）または外部KMSの独立した強力な鍵管理機能を使用して、データベース、ログ、設定ファイル、バックアップを透過的に暗号化します。KMS（別名「キーストア」）とは、データの暗号化に使用したエンベロープ暗号鍵を格納する、安全な場所です。MarkLogicの鍵管理には、以下に示す機能があります。

- エンドツーエンドの暗号化 – MarkLogicでは保存データを暗号化できます（Encryption at Rest）。この暗号化では、ディスク（ローカルまたはクラウド）上にあるエンベロープデータを透過的かつ選択的に暗号化することが可能で、ディスク上のデータの機密性を守り、改ざんを防ぎます。

- 職務の分離 – 保存データの暗号化では、職務分離を要求することでデータセキュリティの制御を大幅に強化できます。ホストにアクセスできるシステム管理者と、暗号鍵自体と暗号鍵のライフサイクルを管理する担当者を別の人にすることで、APT攻撃（標的型攻撃）といったネットワーク上の脅威だけでなく、内部関係者からの脅威の可能性を小さくできます。

デフォルトでは、MarkLogicはローカルのKMSを使用します。しかし、保存データ暗号化のベストプラクティスとしては、アプリケーションサーバーとは別に外部のサードパーティ製KMSを導入および管理して使用すべきです。外部KMSは信頼できる認証（暗号）鍵を安全に保管し、認証されたシステムにオンデマンドで提供します。このように認証鍵をストレージシステムとは別に保管することで、セキュリティレベルがさらに上がります。しかも、認証鍵は常に安全に管理、保管されます。鍵が平文で表示されることは一切ありません。アドバンスセキュリティオプションで有効化された外部KMSは、以下の機能を提供します。

- セキュリティの強化 – 外部KMSは、暗号鍵のセキュリティを強化すると同時に、鍵の自動ローテーション、失効、削除などの鍵管理機能を提供します。

- 職務分離の追加 – 外部KMSを使用している場合、未承認のデータベース管理者、システム管理者、ストレージ管理者はデータベースにアクセスできません。暗号鍵へのアクセスは外部KMSの管理者が管理します。

- KMIPの順守 – KMIP（鍵管理相互運用性プロトコル）は、鍵管理サーバー上の暗号鍵を操作するメッセージフォーマットを定義した通信プロトコル標準です。Marklogicは、KMIP 1.2準拠のサードパーティ製外部KMSシステムと相互運用できます。KMIP準拠のシステムとしては、VormetricやSafeNetなどがあります。

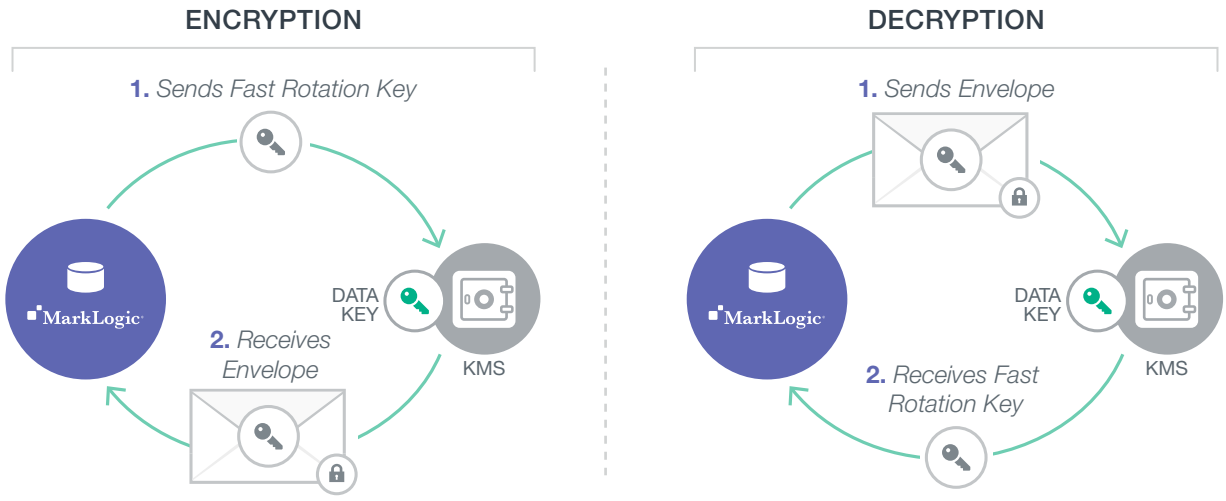

図2：保存データの暗号化では、下位レベルの鍵へのアクセスやファイルの読み込みを行うため、MarkLogicはエンベロープをKMSに送信します。その後、KMSからは暗号化されていない鍵が返されます。外部KMSを使用している場合、MarkLogicにはエンベロープ鍵へのアクセス権がありません。つまり、ファイルへのアクセスもデータの読み込みや漏洩もないということです。

図3:リダクションを使用すると、鍵情報のマスキングや削除が可能

リダクション

リダクションは、MarkLogicとの間でデータをインポート、エクスポート、またはコピーする際、許可されていないユーザーへの機密情報の流出防止に役立ちます。例えば、データサイエンティストに分析のためのデータを提供する場合や、開発者が本番データを必要としているものの、実際のクレジットカードデータや個人を特定可能な情報へのアクセスは認められない場合などに、リダクションはしばしば必要とされます。
リダクションの主な特徴は、以下のとおりです。

- ルールとポリシーに基づいている – 実装するには、MarkLogicセキュリティ管理者はリダクションが必要な機密情報を定義するルールを含むリダクションポリシーを作成し、エクスポート実行時に適用するポリシーを選択します。管理者は、ビルトインのルールやカスタムのルールを組み合わせ、さまざまなターゲットのニーズに応じたポリシーを作成できます。
- ビルトイン関数の活用 – さまざまな種類のリダクション用のビルトイン関数が用意されています。
  - Concealing:要素および/またはその値(JSONの場合はプロパティおよび/またはその値)を隠します。
  - Masking:ランダムマスキング(インスタンスごとに値が変わる)、決定論的マスキング(毎回同じ値を適用)、または辞書マスキング(指定した辞書の値を適用)を使用してデータを変更します。
  - Patterns:社会保障番号、米国の電話番号、メールアドレス、IPv4、正規表現などのパターンを使用してデータを変更します。
  - Custom:サーバーサイドJavaScriptまたはXQueryの関数を使用して、独自のルール(18歳未満の場合は名前をリダクションするなど)を適用します。
- 完全に監査可能 – ユーザーが実行するルールとアクションはすべて記録されるため、後ですべてのエクスポートアクティビティを監査できます。
- 拡張時にバッチ実行 – リダクションは、大規模な一括エクスポートを実行する際に使用できるよう設計されています。また、mlcp(MarkLogic Content Pump)を使用すると、アプリケーションレイヤーで実装したソリューションよりも処理速度と安全性が向上します。

コンパートメントセキュリティ

コンパートメントセキュリティでは、より複雑なロールベースのセキュリティルールをデータアクセスや更新に適用できます。ドキュメントへのアクセスや作成を行うには、適切なロールのいずれか1つだけではなく、すべて持つようユーザーに義務付けることが可能です。ロールをコンパートメント化する(まとめる)場合、リソースに関連付けられているすべての権限が同時に有効(AND集合)である必要があります。一方、ロールをコンパートメント化しない場合、任意の権限条件を満たしていれば(OR集合)十分です。

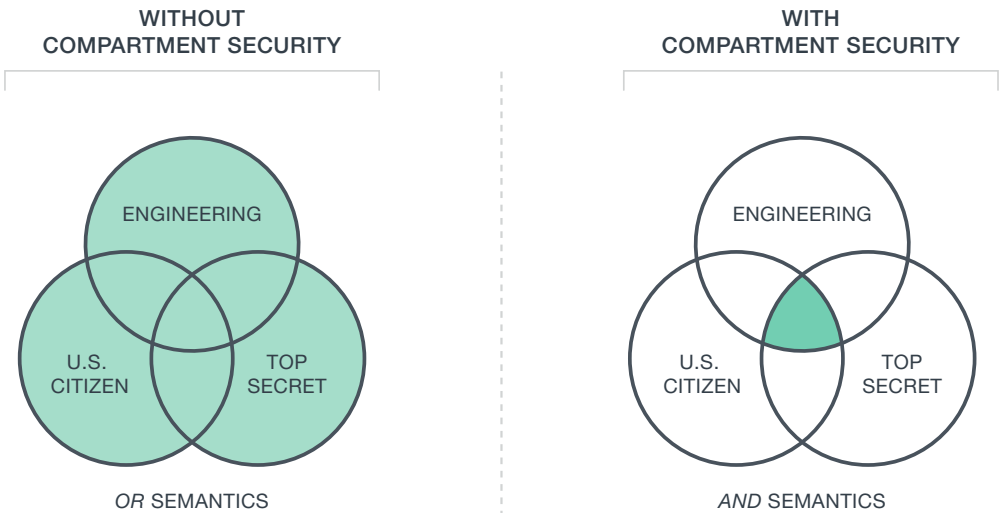

図4：コンパートメントセキュリティでは、「Top Secret」、「US Citizen」、「Engineering」の組み合わせのロールを持つユーザーのみがデータにアクセスできるよう指定できます。コンパートメントセキュリティを使用しない場合、これらの役割を1つでも持っているユーザーは誰でもデータにアクセスできるようにしかできません。

例えば、コンパートメントセキュリティを使用すると、「Top Secret」レベルに分類され、「NOFORN」（外国人不可）としてセキュリティが追加された政府文書は、「Top Secret」のロールとその国の国民のロールの両方を持っているユーザーしか読めません。

使用すべき状況

外部KMS – 暗号鍵に対する懸念を分離し、格納を管理しやすくするには、外部KMSを使用します。このオプションは、組織内ですでに使用している外部KMSを活用する場合にも便利です。

リダクション – データを共有するためにエクスポートする際、特定のデータを削除したり、わからないようにしたりする場合は、リダクションを使用します。この機能は、コンプライアンスガイドライン（HIPAA、SEC17a-4、FINRA、GDPRなど）の順守においても役立ちます。

コンパートメントセキュリティ – データアクセスをさらに制限するため条件のAND集合を使用する必要がある場合は常に、コンパートメントセキュリティを使用します。政府機関システムで機密情報を保護するために採用されることが多いです。

MarkLogicについて

MarkLogicは、サイロ化したデータの統合に世界で最も適したデータベースです。オペレーショナルでトランザクショナルなエンタープライズNoSQLデータベースのプラットフォームにより、データをより適切かつ迅速に、低コストで統合します。詳細については、jp.marklogic.comをご覧ください。

マークロジック株式会社 MARKLOGIC K.K.
150-0043 東京都渋谷区道玄坂 1-12-1渋谷マークシティウェスト 22 階
+81 3 4360 5354 | jp.marklogic.com | MarkLogic-JP@marklogic.com