cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

# データベース保護ソリューション

## データベースセキュリティの課題

今日の企業のデータベースには、極めて機密性の高い、厳格に管理されたデータが格納されています。そのデータは、内部不正や外部攻撃者の格好の標的となっています。近年、広く報道されているように多くのデータベース攻撃が発生して数億件のレコードが流出しており、影響を受けた組織には金銭的損失や風評被害が生じています。

### 中央集権型の障害

データベースは、中央集約ポイントであり、攻撃者が目を付けるポイントです。そこには顧客の支払いデータ、患者の記録、知的財産など、機密性の高い規制対象のリソースを含む、さまざまな企業資産が存在します。つまり、オンプレミスかクラウドかを問わず、データベースには、ビジネスにとって重要なデータが格納されており、攻撃者にとって非常に価値のあるものとされています。

### 不十分なセキュリティ管理

セキュリティ管理が不十分だと、組織は不正行為やデータ侵害の危険にさらされます。たとえば、データベースの暗号化とそれに対応する鍵管理の両方がデータベース内で処理される場合、データベース管理者（DBA）はデータと鍵の両方を管理することになります。データベース暗号化ソリューションでは、攻撃者による特権ユーザなりすましや、内部不正の可能性が軽視されがちです。

### 複雑で非効率な鍵管理

データベース環境が拡大するにつれて、鍵管理の課題も増えています。複数の鍵管理ツールの使用は複雑であり、エラーや不正を増やすことになります。データベースベンダーは鍵の管理機能を提供していますが、これは企業がそのベンダーの特定のデータベースを使用する場合にのみ機能します。ベンダーのデータベースの各インスタンスには個別の暗号鍵が必要なため、異なるデータベースの鍵を管理すると複雑さが増し、鍵の紛失や盗難のリスクが高まります。

### TDE（透過的データ暗号化）で十分なのか？

OracleやMicrosoft SQL Serverは、Transparent Data Encryption（TDE：透過的データ暗号化）機能を備えており、データベースやセルレベルでの暗号化を可能にします。しかし、おそらくはこれらのデータベースに関する機密データを含むログファイルやレポートファイルの暗号化する必要性が高くなります。また、多くの組織では、他のアプリケーションやデータベースのデータも暗号化する必要があり、複数の暗号化製品、鍵の管理およびストレージシステムへの投資、および実装作業が必要になります。

## 従来型アプローチの限界とリスク

これまでセキュリティチームは、境界とエンドポイントの防御に重点を置いてきました。そのため、この防御に失敗した場合、組織のデータは危険にさらされることになります。

- **可視性の欠如**

  機密データがさまざまなデータベースのどこに存在するかを把握していなければ、機密データを効果的に保護することはできません。

- **信頼性とパフォーマンスの問題**

  設計が不十分なデータベースの暗号化を実装すると、データへのリアルタイムでのアクセスのパフォーマンスに影響を与えることがよくあります。

- **不十分なセキュリティ管理**

  データベース管理者は暗号化されたデータと暗号鍵の両方にアクセスできるため、ネイティブのデータベース暗号化ツールは、内部不正の懸念が存在します。

- **複雑な鍵管理**

  データベース環境が拡大するにつれて、鍵管理の課題も増えています。各データベースベンダーが提供するそれぞれの鍵管理ツールを使用すると、コストと複雑さが増します。

組織のポリシーと規制要件の両方に準拠するために、セキュリティチームは、データベースの強力な防御を確立して脅威に対処する必要があります。

## 強力なアクセス制御によるデータベースの暗号化と鍵管理

タレスのソリューションを利用することで、組織はデータベースとそこに含まれる資産に対する強力で包括的な防御を確立できます。タレスのソリューションは、データの検出と分類、堅牢な暗号化、トークン化、鍵管理、きめ細かなアクセス制御、ロギングなどの機能を備えており、オンプレミスとクラウドのデータベース環境の保護を支援します。セキュリティチームは、機密データを暗号化し、そのデータを復号化するためのアクセス権限を制限するきめ細かいポリシーを適用することができます。

## データベース暗号化ソリューション

### CipherTrust Manager（CM：暗号鍵管理）

CipherTrust Manager（CM：暗号鍵管理）は、組織にる暗号鍵の一元管理、詳細なアクセス制御機能を提供し、セキュリティポリシーの設定が可能です。FIPS 140-2 Level 3まで準拠した仮想と物理フォームファクタの両方で使用できます。

### CipherTrust Data Discovery and Classification（DDC：機密データの検出と分類）

コンプライアンスの重要な最初のステップは、機密データの構成要素、データの保存場所と保存方法、誰がデータにアクセスできるのかを把握することです。効率的なスキャンにより、データプライバシーとセキュリティ全体に対し強固な基盤を構築できます。ソリューションごとに異なるベンダーを頼る必要はありません。タレスのCipherTrust Data Discovery and Classification（DDC：機密データの検出と分類）は、ファイルサーバと、Oracle、IBM DB2、Microsoft SQL Serverなどの従来のデータベース全体で、ほとんどの種類のデータを効率的に検出できます。

### CipherTrust Transparent Encryption（CTE：透過的暗号化）

CipherTrust Transparent Encryption（CTE：透過的暗号化）は、保存データの暗号化、特権ユーザアクセス制御、および詳細なアクセス監査ログを提供します。アプリケーションやデータベースを変更することなく、ファイルやボリュームレベルで展開できます。CTEにより、Oracle、IBM DB2、Microsoft SQL Server、MySQL、Sybase、NoSQL 環境、またはそれらの任意の組み合わせのいずれを使用している場合でも、企業全体にわたるデータベースの機密データを保護できます。

### CipherTrust Application Data Protection（CADP：アプリケーションデータ保護）

CipherTrust Application Data Protection（CADP：アプリケーションデータ保護）は、鍵管理、署名、ハッシュ化、暗号化などのAPIを提供し、開発者がアプリケーションやデータベースのデータ保護を容易に実装できるようにします。サンプルコードが付属しており、個別のデータセキュリティソリューションの開発を加速させると同時に、鍵管理の複雑さを取り除きます。

### CipherTrust Database Protection（CDP：データベース保護）

CipherTrust Database Protection（CDP：データベース保護）は、保護されていないデータベースとほぼ同じ速度でデータベースの書き込みと読み取りを行うことを保証する高可用性アーキテクチャにて、高性能なカラムレベルのデータベース暗号化を提供します。データベースアプリケーションに変更を加えることなく、鍵を安全かつ一元的に管理します。きめ細かいアクセス制御により、許可されたユーザまたはアプリケーションのみが保護されたデータを表示できるようになります。各カラムに特定の鍵を使用することで細分性を確保し、CipherTrust Managerによってデータセキュリティに不可欠な要素である職務分離を保証しながら、各鍵に対して多様で強力なアクセス制御を提供します。

### CipherTrust Tokenization（CT-V/CT-VL：トークン化）

CipherTrust Tokenization（CT-V/CT-VL：トークン化）は、機密データをトークン化する方法として、ボルト型とボルトレス型の両方を提供しています。ボルトレス型トークナイゼーションでは動的データマスキングがサポートされていますが、ボルト型トークナイゼーションでは環境固有のAPIを使用する必要があります。

### CipherTrust Cloud Key Manager for Cloud Services（CCKM：クラウド暗号鍵管理）

Amazon Web Services、Microsoft Azure、Google Cloud Platform、Salesforce、IBM Cloudなど、マルチクラウド環境のBYOK（Bring Your Own Key：独自の鍵の持ち込み）管理を効率化します。このソリューションは、包括的なクラウド鍵ライフサイクル管理と自動化を提供し、セキュリティチームの効率を高め、クラウド鍵管理を簡素化します。

## CipherTrust Database Protection Benefits（データベース保護）のメリット

タレスのデータベース暗号化ソリューションには、いくつかの重要なメリットがあります。

**パフォーマンスに顕著な影響を与えないデータベース保護**

タレスの CipherTrust Data Security Platform（CDSP：データセキュリティプラットフォーム）ソリューションは拡張性が高く、パフォーマンスを低下させることなくデータベース環境を保護します。CipherTrust Transparent Encryptionは、パフォーマンスを重視する環境でフィールドテストされており、1秒あたり50,000件の暗号化トランザクションをサポートするスケーラビリティが実証されています。

**シームレスな実装**

タレスのCipherTrust Data Protectionは、アプリケーション、インフラストラクチャ、ビジネスプラクティスに変更を加えることなく、高性能なカラムレベルでのデータベース暗号化を可能にします。そのため、仮想、クラウド、ビッグデータ、および、従来の環境等の全体にアプリケーション層の暗号化を簡単に拡張できるようになります。

**コンプライアンス対応の改善**

タレスのCipherTrust Data Discovery and Classificationは、データの検出と分類、リスク評価、優れた視覚化、詳細なレポートにより、規制対象のデータを迅速に識別してセキュリティリスクを強調し、コンプライアンスギャップを特定できるようサポートします。これにより組織は容易に、プライバシーギャップを見つけてその差異を埋め、修復に優先順位を付け、プライバシーに関する懸念について十分な情報に基づいて意思決定を行うことができるようになります。

## サポートされるデータ環境

データベース: IBM DB2、Microsoft SQL Server、MongoDB、MySQL、NoSQL、Oracle、Sybase、ビッグデータ: Hadoop、NoSQL、SAP HANA、Teradata

## さらなる情報

機密データベース保護方法について詳しくは、cpl.thalesgroup.com/ja をご覧ください。

## タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。



> cpl.thalesgroup.com/ja <

**お問い合わせ先 –** Email: cpl.jpsales@thalesgroup.com

すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。