cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Platform Community Edition
データ保護機能を追加する作業負荷を、数週間から数分に軽減

ビジネス上の問題

データ保護機能の追加する作業負荷が軽減されれば、より短時間でより多くの開発が可能となります。

従来のデータ保護ツールでは、データ保護を追加するにはアプリケーションを修正せねばならず、コードを書き換える必要がありました。データへの変更（新規フィールド、フィールド削除）や、データの保護方法の変更（暗号/鍵/パラメータの変更）があるたびに、従来のデータ保護ツールでは、データを保護するためのコードを書き換えなくてはなりません。

データやその保護方法の変更は、たびたび起こる可能性があります。従来のデータ保護ツールを使用していると、従来のデータ保護コードの書き換えによって開発者の集中が何度も妨げられるため、他のプロジェクトの実施ペースが下がります。

CipherTrustソリューション

Thales CipherTrust Platform Community Edition は、開発プロセスに新しいステップを強いる必要がなく、データ保護を自動化することでデータとファイルを保護し、プロジェクトのペース低下を防ぎます。CipherTrust Platform Community Editionは、Thales CipherTrust Manager、Data Protection Gateway Connector、及びCipherTrust Transparent Encryption for Kubernetes Connectorのライセンスを無償で提供します。

Data Protection Gateway (DPG) は、コードの書き換えを必要とせずに、レガシーおよびクラウドネイティブアプリケーションでのRESTful呼び出しで機密データを透過的に保護するCipherTrust Connectorです。DPGは、データの保護方法、そのデータへのアクセス権を持つユーザー、およびデータへのアクセス方法を、データセキュリティチームが完全に制御できるようにします。同時に、DPGは、オーケストレーションしやすいプル&デプロイモデルをDevOpsに提供し、現在の環境とのシンプルな統合を実現します。

CipherTrust Transparent Encryption for Kubernetes (CTE-K8s) は、承認済みのユーザーとプロセスを判別する包含リストを使用して、Kubernetesファイルストア内の機密データを透過的に保護します。攻撃者は権限の昇格に成功したとしても、包含リストにないユーザーを選択すると、その攻撃者は昇格した権限を行使できなくなります。たとえば、ランサムウェアはハードドライブのデータを暗号化します。CTE-K8sは、ファイルを保護し、ユーザーとプロセスによる不正な読み取りと書き込みを禁止します。これにより、ランサムウェアによる永続ボリューム内のファイルの損傷/ロックアップ/暗号化を防ぎます。

CipherTrust Managerは、業界をリードするエンタープライズ暗号鍵管理ソリューションです。企業が暗号鍵を一元管理し、セキュリティポリシーとアクセス制御を詳細なレベルで構成および制御できるようにサポートします。CipherTrust Managerは、CipherTrust Data Security Platformの基盤であり、CipherTrust Connectorの中央管理ポイントとしての役割を果たしま

す。CipherTrust Connectorは、データの検出、保護、制御を単一プラットフォームに統合するデータ中心のセキュリティ製品の統合スイートを提供します。

主なメリット

マルチクラウドアプリケーションに対する透過的なデータ保護

Kubernetesファイルストア内の機密データの透過的な保護

DevSecOpsの完全な職務分掌による効率の向上

サポートされるユースケース

CipherTrust Platform Community Editionを使用すると、DevSecOpsチームは次のユースケースを迅速に実装できます。

- **アプリケーションレベルのデータ保護:** CipherTrust Data Protection Gatewayにより、レガシーまたはクラウドネイティブアプリケーションでのRESTful呼び出しで機密データを透過的に保護します。
- **Kubernetesファイルの保護:** CipherTrust Transparent Encryption for Kubernetesにより、Kubernetes環境にデプロイされたコンテナ内のデータまたはコンテナからアクセス可能な外部ストレージを透過的に保護します。
- **暗号鍵管理:** 一元化された強固な鍵管理および暗号化ソリューションであるCipherTrust Manager Community Editionにより、RESTful呼び出しを使用してアプリケーションを保護します。

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。

決断の瞬間のための、確実なテクノロジー。

CipherTrust Manager 機能	Community Edition	Enterprise Edition
REST APIによる鍵管理	✔	✔
REST APIによるデータ保護	✔	✔
外部アイデンティティプロバイダー		✔
クラスタリング		✔
マルチドメインサポート		✔
組み込み型またはネットワーク型ハードウェアセキュリティモジュール(HSM)		✔
CipherTrust Data Security Platform Connectors		
Transparent Application Protection	✔	✔
Transparent Encryption for Kubernetes Environments	✔	✔
Cloud Key Management		✔
Data Discovery and Classification		✔
Transparent Encryption for Files/Folders		✔
Database Protection		✔
Application-level Data Protection		✔
Tokenization – Vaulted, Vaultless		✔
Batch Data Transformation		✔

> cpl.thalesgroup.com <

お問い合わせ先 – 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。