cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Enctyption（透過暗号化）

変化する環境と増大する脅威の中で機密データを保護

機密データを保護するには、データセンターのオンプレミス環境にあるデータベースやファイルを保護するだけでは不十分です。現在の一般的な企業は、3社以上のIaaSまたはPaaSプロバイダー、50以上のSaaSアプリケーション、ビッグデータ環境、コンテナ技術、独自の内部仮想環境とプライベートクラウドを利用しています。

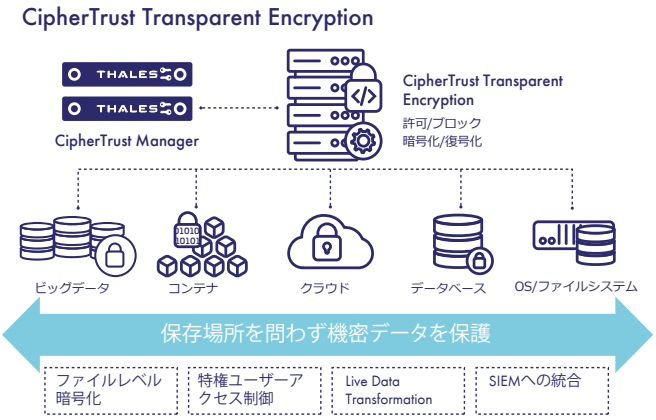
問題をさらに複雑にしているのは、サイバー攻撃が高度化し強力になっていることです。そのため、機密情報の保護に関する新たなコンプライアンスや規制が次々と制定され、既存の規制もさらに厳しくなっています。

ソリューション：CipherTrust Transparent Encryption（透過暗号化）

CipherTrust Transparent Encryption（透過暗号化）は、充実したアクセス制御機能を備えており、データにアクセス可能なユーザー、データにアクセス可能なタイミング、付与するアクセス権限のタイプを決定できます。

保存場所を問わず、機密データを保護

- 実証済みのハードウェアアクセラレーション暗号化ソリューションを使用することで、暗号化、アクセス制御、データアクセスログに関するコンプライアンス要件とベストプラクティス要件に対応します。このソリューションでは、ファイル、ボリューム、リンクされたクラウドストレージを保護しつつ、物理環境、仮想環境、クラウド環境でアクセス制御とデータアクセス監査ロギングを実現します。
- マルチクラウド、オンプレミス、ビッグデータ内、コンテナ環境の全体にわたる一元的な鍵管理、暗号化、アクセスポリシーにより、シンプルで拡張性に優れた環境を迅速に導入できます。
- 特権ユーザーアクセス制御を容易に実装できるため、管理者の通常業務を妨げずに、データへの脅威となる可能性があるユーザーやグループからデータを保護できます。
- 実用的で詳細なセキュリティイベントログを活用することで、ファイルアクセスアクティビティに関して、これまで得られなかった有用な情報を入手できるため、脅威を迅速に検出して阻止できます。



- 業界で最も幅広いプラットフォームをサポートしています。Linux、AIX、Windowsシステムからアクセスされる構造化データおよび非構造化データを保護するほか、S3バケットに保存されているデータの透過的な暗号化とアクセス制御を行います。
- Live Data Transformationオプションを追加することで、初期暗号化や鍵の再生成処理のためにシステムを停止する必要がなくなります。これは、他のデータ暗号化ソリューションにはない独自の機能です。

主なメリット

透過的なデータ保護。ファイルレベルの暗号化を継続的に適用することでユーザーやプロセスによる不正アクセスからデータを保護しつつ、アプリケーション、インフラストラクチャ、システム管理タスク、ビジネスプラクティスを変更することなく、すべてのアクティビティについて詳細なデータアクセス監査ログを作成できます。

シームレスかつ容易な展開。CipherTrust Transparent Encryptionエージェントは、サーバーのファイルシステムまたはボリュームレベルに展開でき、ローカルディスクとクラウドストレージ環境（Amazon S3やAzure Filesなど）の両方をサポートします。

きめ細かなアクセス制御の定義。きめ細かい、最小権限のユーザーアクセスポリシーを適用することで、外部からの攻撃や特権ユーザーによる悪用からデータを保護します。システム、LDAP/Active Directory、Hadoop、コンテナ内のユーザーやグループに対して、個別のポリシーを適用できます。また、プロセス、ファイルタイプ、時刻、その他各種パラメータに基づいて、アクセスを制御することもできます

高性能なハードウェアアクセラレーション暗号化。CipherTrust Transparent Encryptionは、データ暗号化用のAES（Advanced Encryption Standard）や鍵交換用のECC（Elliptic Curve Cryptography; 楕円曲線暗号）など、標準ベースの暗号化プロトコルのみを採用しています。また、最新のCPUで利用可能なAESハードウェア暗号化機能を活用して、暗号化のオーバーヘッドを最小限に抑えています。

包括的なセキュリティインテリジェンス。コンプライアンス要件を満たすだけでなく、データセキュリティ分析にも利用できる詳細なデータアクセス監査ログにより、脅威を迅速に検出して阻止します。また、セキュリティインテリジェンスログとレポートにより、コンプライアンスに関するレポート作成を効率化し、主要なSIEM（Security Information and Event Management; セキュリティ情報イベント管理）システムを利用して脅威を迅速に検出します。

非常に幅広いシステムと環境をサポート。エージェントは、Windows、Linux、AIXのさまざまなプラットフォームに対応しており、基盤となるストレージテクノロジーに関係なく、物理、仮想、クラウド、コンテナ、ビッグデータの環境で使用できます。

高度なセキュリティ

インテリジェントな保護。データを迅速に検出および分類し、暗号化とアクセス制御ポリシーを使用して非構造化機密データをプロアクティブに保護できます。運用効率の向上、コンプライアンス準拠までの時間の短縮、セキュリティギャップのプロアクティブな解消を実現します。

ダウンタイムのないデータ変換。Live Data Transformationオプションにより、初期暗号化や鍵の再生成処理時のダウンタイムがなくなります。この特許技術により、アプリケーションをオフラインにすることなく、データ使用中にデータベースやファイルを暗号化したり、新しい暗号鍵で再暗号化したりすることができます。

SAP HANA認定。CipherTrust Transparent Encryptionは、SAP HANA v2.0の認定を受けており、データ暗号化、鍵管理、特権ユーザーアクセス制御、きめ細かなファイルアクセス管理ログを実現します。

CipherTrust Transparent Encryption UserSpace。Linuxサーバーのカーネルアップグレードによる影響を受けないLinux FUSEを基盤とする、拡張性に優れた強力なファイル暗号化ソリューションを提供します。

ソリューションアーキテクチャ

導入環境は、CipherTrust Transparent Encryptionコネクタと CipherTrust Managerアプライアンスで構成されます。ポリシーと鍵は、CipherTrust Managerで一元管理されます。CipherTrust Managerは、FIPS 140-2 Level 1/2/3準拠アプライアンスとして使用可能です。

CipherTrust Data Security Platform

CipherTrust Transparent Encryptionは、CipherTrust Data Security Platformの一部です。CipherTrust Platformは、データ検出、分類、データ保護を統合して、これまでにないきめ細かなアクセス制御を提供し、すべて一元的に鍵管理が行えます。これにより、データセキュリティの運用効率化、迅速なコンプライアンス準拠、クラウド移行の保護、ビジネス全体のリスク軽減が可能になります。Thales CipherTrust Data Security Platformを利用すれば、保存場所を問わず、企業の機密データを検出、保護、制御することができます。

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。

> cpl.thalesgroup.com/ja <

お問い合わせ先 – 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。