cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

タレスのデータセキュリティプラットフォーム
CipherTrust Data Security Platform

次世代の統合データ保護により、機密データが
どこに保存されていても検出、保護、制御を実現

検出 **保護** **制御**

データシートv17

CipherTrust Data Security Platform

セキュリティ侵害が驚くべき頻度で発生し続けており、データ保護のコンプライアンス要件が厳格化する中、組織はより多くの環境、システム、アプリケーション、プロセス、ユーザにわたってデータ保護を拡大する必要があります。タレスのデータセキュリティプラットフォーム「CipherTrust Data Security Platform」は、次世代の統合データ保護により、組織の機密データがどこに保存されていても効果的に検出、保護、制御することができます。

CipherTrust Data Security Platformは、データ検出、分類、データ保護、きめ細かなアクセス制御をすべて統合し、鍵を一元管理します。このソリューションはデータセキュリティの複雑さを排除し、コンプライアンスに要する時間を短縮し、セキュアなクラウド移行を実現します。これにより、データセキュリティの運用にかかるリソースを削減し、ユビキタスなコンプライアンス管理を実現し、ビジネス全体のリスクを大幅に減少させます。

このプラットフォームは、データベースやファイルへのアクセスを検出、保護、制御する機能を備えており、クラウド、仮想、ビッグデータ、および物理環境に存在する資産を保護できます。このスケーラブルで効率的なデータセキュリティプラットフォームにより、緊急の要件に対処でき、次のセキュリティ課題やコンプライアンス要件が発生した際に迅速に対応できるようになります。

機能

- 一元管理コンソール
- 監視とレポート
- データの検出と分類
  - データの可視化によるリスク分析
- データ保護技術
  - ファイル、データベース、ビッグデータの透過的暗号化
  - アプリケーション層のデータ保護
  - フォーマット保持暗号化
  - 動的データマスキングによるトークン化
  - 静的データマスキング
  - 特権ユーザアクセス制御
- 一元化されたエンタープライズ鍵管理
  - FIPS 140-2準拠のエンタープライズ鍵管理
  - KMIP統合の比類のないパートナーエコシステム
  - マルチクラウドの鍵管理
  - Transparent Data Encryption（透過的データ暗号化）の鍵管理

環境

- IaaS、PaaS、SaaS： Amazon Web Services、Google Cloud Platform、Microsoft Azure、IBM Cloud、Salesforce、Microsoft Office365、Service Now、Oracle Cloudなど
- 対応OS: Linux、Windows、Unix
- ビッグデータ: Hadoop、NoSQL、SAP HANA、Teradata
- データベース: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, Oracle, Sybase, Teradata, その他
- あらゆるストレージ環境

プラットフォームの優位性

- 次世代の統合データ保護により、組織の機密データがどこに保存されていても検出、保護、制御
- 物理、仮想、クラウド、およびビッグデータ環境において、一貫したセキュリティとコンプライアンスを実現
- 追加のユースケースを迅速にサポートできる柔軟性と拡張性
- FIPS 140-2 Level 3認証などを取得したHSM（ハードウェアセキュリティモジュール）が、プラットフォームの安全な信頼の基点”Root of Trust”として機能

主なメリット

データセキュリティの簡素化 – 次世代の統合データ保護により、機密データがどこに保存されていても検出、保護、制御します。CipherTrust Data Security Platformは、単一の一元管理コンソールでデータセキュリティ管理を簡素化します。これにより、データがクラウドに保存されていても、強力なツールを使用して、機密データの検出および分類、外部からの脅威への対処、内部関係者による悪用からの保護、永続的な制御の確立が可能になります。デジタルトランスフォーメーションを実施する前に、プライバシーのギャップを簡単に発見して解消し、保護の優先順位をつけ、プライバシーとセキュリティ要件について十分な情報に基づく意思決定を行うことができます。

コンプライアンス対応時間の短縮 – 規制当局や監査人は組織に対し、規制対象の機密データを管理し、それを証明するレポートを作成するよう要求します。CipherTrust Data Security Platformのデータの検出および分類、暗号化、アクセス制御、監査ログ、トークン化、鍵管理といった機能は、ユビキタスなデータのセキュリティとプライバシー要件に対応しています。これらの制御は新規展開に対して、または進化するコンプライアンス要件に応じて迅速に追加できます。一元化された拡張可能なプラットフォームの性質により、ライセンスを追加したり、新たなデータ保護要件に応じて必要となるコネクタをスクリプトで展開したりすることで、新たな制御を迅速に追加できます。

セキュアなクラウド移行 – CipherTrust Data Security Platformは、機密データをクラウドに安全に保管できる高度な暗号化と一元化された鍵管理ソリューションを提供します。

また、高度なマルチクラウドのBYOE（Bring Your Own Encryption：独自の暗号化の持ち込み）ソリューションを提供することで、クラウドベンダーによる暗号化のロックインを回避し、一元化され独立した暗号鍵管理によって複数のクラウドベンダーにわたるデータを効率的に保護し、データの移行性を確保します。独自の暗号化を適用できない組織でも、CipherTrust Cloud Key Managerを使用して外部で鍵を管理することで業界のベストプラクティスに従うことができます。CipherTrust Cloud Key Managerは、複数のクラウドインフラストラクチャとSaaSアプリケーションにまたがるBYOKのユースケースをサポートしています。CipherTrust Data Security Platformを使用すれば、最も強力な保護手段でクラウド上にある機密データとアプリケーションを保護でき、コンプライアンス要件を満たしつつ、データの作成、使用、保存場所にかかわらず、より高度にデータを制御できるようになります。

製品紹介:

CipherTrust Manager は、CipherTrust Data Security Platformの中央管理ポイントであり、暗号鍵とデータアクセスポリシーを一元管理します。FIPS 140-2 Level 3まで準拠した物理と仮想フォームファクタの両方で使用できます。

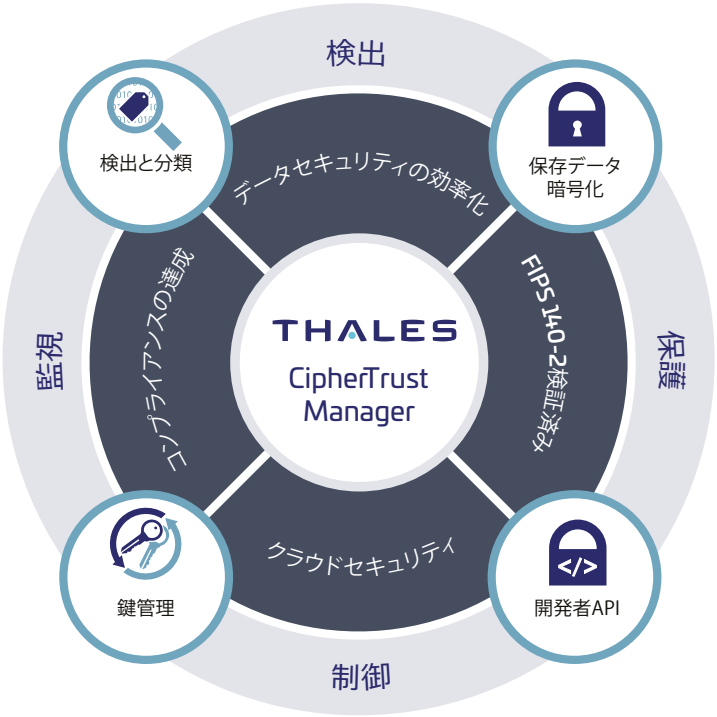
Data Discovery and Classificationは、単一のコンソールで機密データの検出と分類を実行できます。これにより、リスクを把握し、ギャップを発見し、第三者とのデータ共有やクラウド移行についてより適切な意思決定が行えます。

CipherTrust Enterprise Key Management は、企業全体のさまざまなソースと環境の暗号鍵を管理し、暗号鍵管理を効率化します。CipherTrust KMIP Serverは、CipherTrust Manager上で動作し、多くのKMIPクライアントとパートナー検証済みソリューションの鍵を一元管理します。CipherTrust Transparent Data Encryption鍵管理は、多くの一般的なデータベースで利用でき、CipherTrust Cloud Key Manager はさまざまなIaaS/PaaS/SaaSクラウドプロバイダーに対応し、クラウドBYOKのライフサイクル管理を提供します。

保存データ暗号化は、ビジネスやデータ管理プロセスの変更を必要とせずにデータを保護します。CipherTrust Transparent Encryptionは、最も悪質な攻撃を阻止できる包括的なデータアクセス制御により、オンプレミス、クラウド、データベース、ビッグデータ環境にわたってデータを暗号化します。Live Data Transformationなどの拡張機能により、ダウンタイムのないデータ暗号化と鍵ローテーションが可能になります。

CipherTrust Data Security Platformは、鍵管理、暗号化、トークン化のための開発者向けAPIを備えた一連の製品を提供します。CipherTrust Application Data Protectionは、サーバまたはRESTful APIベースの鍵管理と暗号化サービスを提供します。CipherTrust Tokenizationソリューションは、動的データマスキング機能を備えたボルト無しとボルト有りトークナイゼイーションで提供され、ユースケース要件に基づいて選択できます。

CipherTrust Database Protection ソリューションは、ソフトウェアエンジニアリング支援を必要とせずにデータベースのカラムレベルの暗号化を提供します。このソリューションは、機密データへのアクセスに対して最高レベルの職務分掌を実現します。



CipherTrust Manager

概要

CipherTrust Managerは、CipherTrust Data Security Platformの中心で、すべてのCipherTrust Data Security Platform製品の鍵、管理、ポリシーを一元管理します。CipherTrust Managerは拡張可能なマイクロサービスアーキテクチャ上に構築されており、プライバシーとデータ保護の規制要件に効率的に対処し、暗号化とIT要件の進化に容易に適応できます。:

CipherTrust Managerは、鍵の生成、バックアップと復元、無効化、削除などのアクティビティを含む鍵のライフサイクル管理を効率化します。鍵やポリシーへのロールベースのアクセス、マルチテナンシーのサポート、鍵の使用や運用の変更に関する強力な監査とレポートが、この製品の中核機能です。

CipherTrust Managerは、仮想と物理アプライアンスの両方のフォームファクタで使用でき、パブリッククラウドやプライベートクラウドから、物理的なセキュリティ制御を伴うオンプレミスのセキュアな展開まで、さまざまなユースケースに対応しています。最高レベルの品質の信頼の基点"Root of Trust"を確保するために、ハードウェアアプライアンスでは、FIPS 140-2 Level 3に準拠した組み込み型のLuna PCI HSM を利用できます。ハードウェアおよび仮想アプライアンスでは、Luna Network HSMまたは他のいずれかのネットワーク接続型HSMを利用できます。

最高の可用性を実現するActive/Activeクラスタリングは、ハードウェアと仮想アプライアンスを組み合わせて構成できます。これにより、鍵管理とデータ暗号化の要件を満たす、24時間365日の稼働時間の保証が実現します。

メリット

- 鍵の一元管理により、複数のアプリケーション、データストア、アプライアンスにわたるオンプレミスとクラウドの暗号鍵の統合を実現
- Ciphertrust Data Security Platformの基盤を提供し、データの検出、分類、機密データの保護により、ビジネスリスクを軽減
- セルフサービスのライセンスポータルや、利用可能および使用中のライセンスの可視化により、管理を効率化
- AWS、Azure、Google Cloud、VMware、Oracle Cloud、OpenStackなどをサポートした、クラウドに対応した展開オプション
- HSM(ハードウェアセキュリティモジュール)サポートによる拡張により、優れた鍵の制御と生成を実現
- 拡張可能なマイクロサービスアーキテクチャによる、ダウンタイムなしのメンテナンスとアップグレード
- ストレージ、サーバ、データベース、アプリケーション、クラウドの主要ベンダーとの統合を実現する、比類のないパートナーエコシステム

主な機能

- セキュアな鍵の生成、ローテーション、無効化、削除、バックアップ/復元など、完全な鍵のライフサイクル管理
- 鍵管理の操作をロールベースのアクセス制御と完全な監査ログレビューと統合し、管理を一元化
- コネクタライセンスのプロビジョニングと継続的な管理を効率化する、セルフサービスライセンシング
- シークレット管理により、プラットフォーム上で使用するシークレットオブジェクトやOpaqueオブジェクトを作成および管理する機能を提供
- マルチテナンシーは、大規模なエンタープライズ環境をサポートするために、職務分掌による複数ドメインを作成するために必要な機能を提供
- 反復的な管理や暗号化タスクを自動化するREST API
- 物理アプライアンスや仮想アプライアンスのクラスタリングを可能にする、柔軟なHAクラスタリングとインテリジェントな鍵共有
- 鍵の状態の変化、管理者のアクセス、ポリシーの変更を複数のログ形式(RFC-5424、CEF、LEEF)で追跡し、SIEMツールとの統合を容易にする機能を備えた、強力な監査とレポート作成

CipherTrust Managerの技術仕様

ハードウェア仕様（k470、k570）

シャーシ寸法	19.0インチ（幅）x 21インチ（奥行）x 1.75インチ（高さ）
重量	12.7 kg（28lbs）
CPU	Intel Xeon E3-1275v5
メモリ	16 GB
ハードディスクとプロテクション	2TB SATA SE（スピニングディスク）X 1個
シリアルポート	1個
Ethernet / NIC	1GB x 4個または10GB/2X1GB x 2個
電源	• 平均電力（ワット）0.7A @120V (84W) • 最大電力（ワット）0.83A @120V (100W) • 電圧: 100～240V、50～60Hz
電源コードオプション	• PSE認証済み • 複数国のプロファイル
MTBF Telcordia	153,583時間
シャーシ侵入検知	タンパシール。k570組み込み型HSMはタンパを検知するとそれ自体がゼロにリセット
動作周囲温度	0 to ~35°C
保存温度	-20 to 60 °C
動作相対湿度	5%～95%（結露なきこと）
FFIPS 140-2認証	https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3519
組み込み型HSMの管理	k570（Thales Luna HSM内蔵）、HSM設定用の管理コンソールとREST API
取り付け金具	• 非スライドレール金具とロッキングマウント付属 • スライドレールが利用可能

ソフトウェア仕様

管理インターフェース	Webベースの管理コンソール、REST API、ksctl（コマンドラインインターフェース）、NAE XML			
最大鍵数	k470 1,000,000	k570 1,000,000	k170v 25,000	k470v 1,000,000
APIサポート	REST, NAE-XML, KMIP, PKCS#11, JCE, .NET, MCCAPI, MS CNG			
セキュリティ認証	• ローカルユーザ • AD/LDAP		• 証明書ベースの認証 • k570: マスター鍵の設定と構成用のローカルまたはリポートPED	
信頼の基点としてサポートされるHSM	Luna Network HSM, Luna T-Series Network HSM, Luna Cloud HSM, Data Protection on Demand, AWS CloudHSM			
クラスタサポート	Active/Active。最大ノード=10クラスタ クラスタメンバーは任意の物理/仮想モデルで構成可能。k170vは2ノードクラスタに限られる			
バックアップ	手動とスケジュール。CMバックアップを暗号化するHSM鍵のオプション			
ネットワーク管理	SNMP v1、v2c、v3、NTP、Syslog-TCP			
syslog形式	RFC-5424、CEF、LEEF			
ソフトウェア認証および検証	k570組み込み型Thales Luna HSM: 組み込み型Luna HSMのFIPS 140-2 L3			

仮想マシン展開用の仕様

	k170v	k470v
最小CPU数	2	4
最小RAM（GB）	4	16
最小ハードディスク（GB）	100	200
最小vNIC	1	2

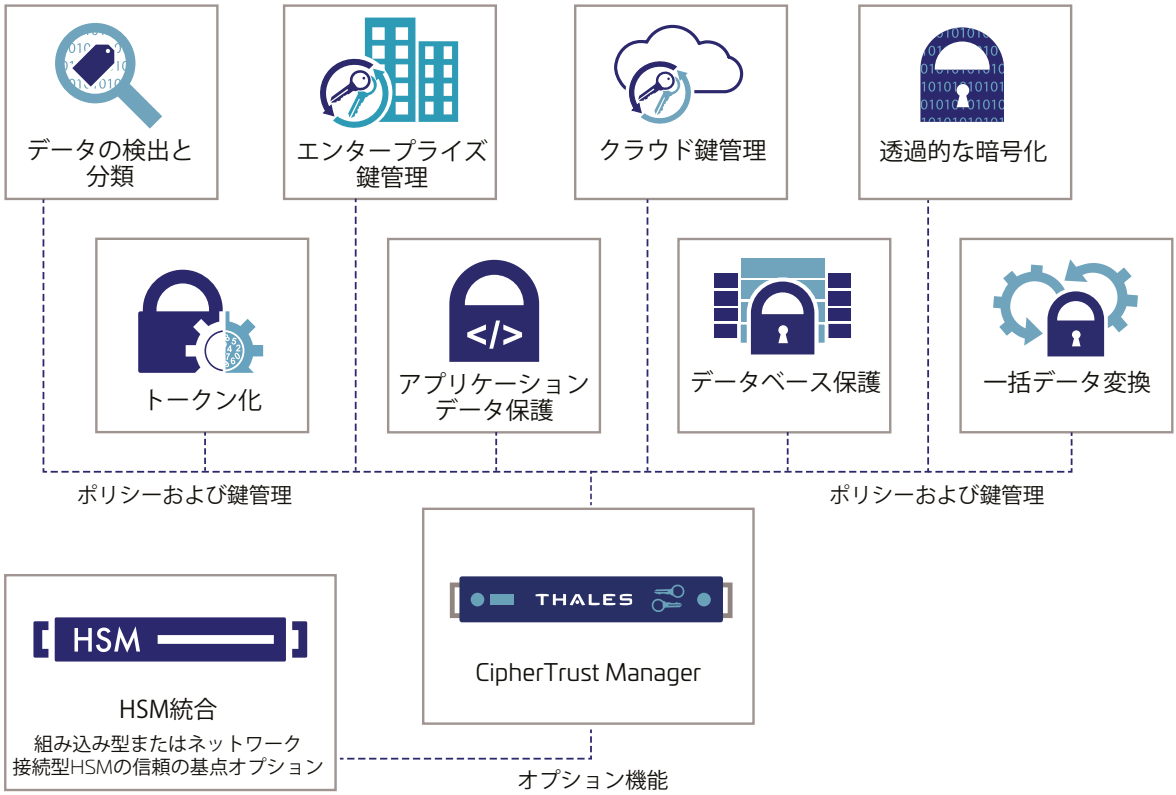
安全認証	適用される行政単位
CBスキーム	44カ国
CSA-UL	カナダ/米国

エミッション認証

FCC Part 15, Subpart B, Class B	米国
EN55032:2010, EN55035:2017, EN61000-3-2:2006 +A1:2009 +A2:2009EN61000-3-3:2008	EU
ICES-003 Issue 7 - October 2020	カナダ
AS/NZ CISPR 32:2015	オーストラリア/ニュージーランド
VCCI V-3/2009.04	日本
KN22, KN24, KC Mark	韓国
NOM	メキシコ
BIS	インド

ハイブリッドエンタープライズ全体にわたる管理の一元化

CipherTrust Managerは、CipherTrust Data Security Platform製品、Microsoft SQL TDE、Oracle TDE、KMIP準拠の暗号化製品用に生成された鍵を含む、さまざまな暗号鍵の中央管理ポイントを提供することで、設備や経費を最小限に抑えます。CipherTrust Managerは、エンタープライズ全体の暗号鍵、ポリシー、監査を管理するための直観的なWebベースコンソールとAPIを備えています。



CipherTrust Data Discovery and Classification

Data Discovery and Classificationは、クラウド、ビッグデータ、従来のデータストア全体にわたり、構造化および非構造化の両方の規制対象データを特定します。単一のコンソールで機密データとそのリスクを把握できるため、セキュリティギャップの解消、修復の優先順位付け、クラウド移行のセキュリティ保護について、より適切な意思決定が行えます。

Data Discovery and Classificationは、ポリシーの策定、検出、分類から、リスク分析とレポート作成までの合理的なワークフローを提供し、セキュリティの盲点や複雑さを排除するために役立ちます。

エンタープライズ規模のデータプライバシー

CipherTrust Data Discovery and Classificationは、展開や拡張が容易なエンタープライズ規模のデータプライバシーソリューションを提供します。すぐに使えるテンプレートと合理的なワークフローを提供し、従来のリポジトリと最新のリポジトリ全体で規制対象データを迅速に特定できるようにします。

単一コンソールによる明確な可視性

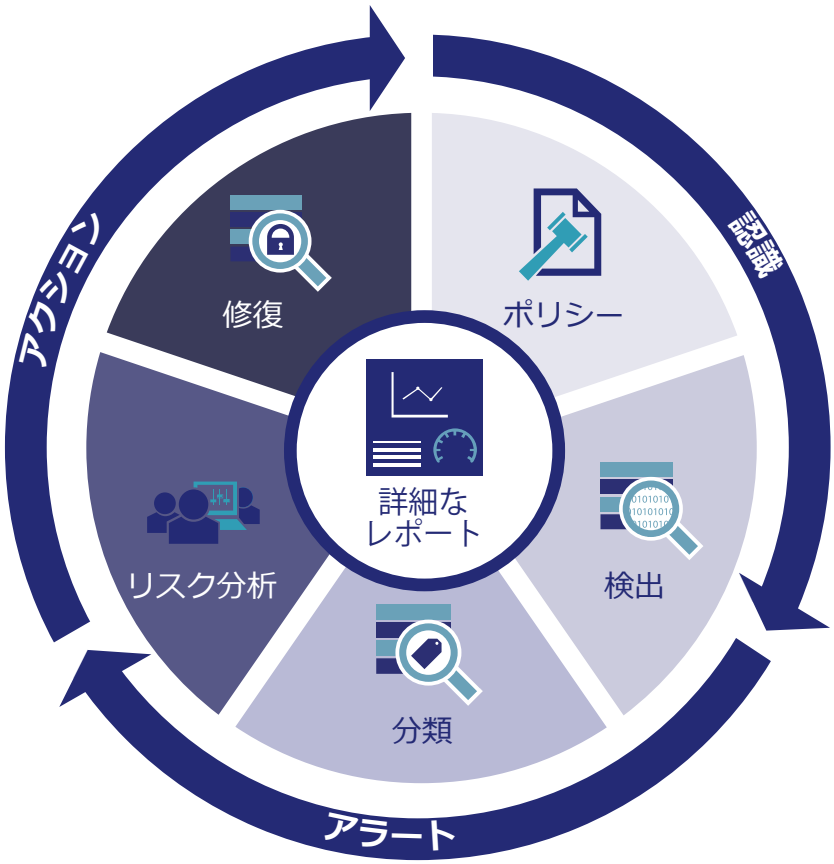
Data Discovery and Classificationでは、機密データ、使用状況、漏洩のリスクを単一のコンソールで明確に把握できます。可視化されたデータと集計レポートを含む一元化されたコンソールにより、データ共有、デジタルトランスフォーメーション、修復の優先順位付けなど、情報に基づいて意思決定を行えます。

柔軟性のあるクイックスタート

Data Discovery and Classificationは、GDPRやCCPAなど、一般的に求められるデータプライバシーやセキュリティの規制に対応するための組み込みの分類テンプレートのほか、特定のパターンやアルゴリズムなどに基づくカスタムポリシーに容易に対処する柔軟性も備えています。

コンプライアンスの実証

CipherTrust Data Discovery and Classificationは、監査人に対してさまざまな規制や法律への準拠を実証できる詳細なレポートを提供します。効率的なスキャンを実行することで、データプライバシーとセキュリティ全体に対し強力な基盤を構築できます。



柔軟な展開オプション

Data Discovery and Classificationは、エージェントベースとエージェントレスの両方の展開モードで利用可能です。これにより、セキュリティチームとITチームは、最適な結果と効率的な総所有コストを得るために、展開モードを選択できます。

メリット

- 組織固有の合理的なワークフローにより、複雑さとリスクを軽減
- 単一のコンソールからプライバシーギャップを迅速に発見し、修復の優先順位をつけ、規制やビジネス上の課題に積極的に対応
- 多様なデータストア全体で構造化データと非構造化データの両方を検出する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力な基盤を構築
- 事前に機密データをスキャンし、必要に応じて削除することで、第三者と安全にデータを共有

Data Discovery and Classificationの技術仕様

データストア

- ホスト上のローカルストレージとローカルメモリ
- ネットワークストレージ
  - Windows Share (CIS/SMB)
  - Unix File System (NFS)
- データベース
  - IBM DB2
  - Oracle
  - SQL
- ビッグデータ
  - Hadoopクラスタ

サポートされるファイルの種類

- データベース: Access、DBase、SQLite、MSSQL MDFおよびLDF
- 画像: BMP、FAX、GIF、JPG、PDF（埋め込み）、PNG、TIF
- 圧縮形式: bzip2、Gzip（全種類）、TAR、Zip（全種類）
- Microsoftバックアップアーカイブ: Microsoft Binary / BKF
- Microsoft Office: v5、6、95、97、2000、XP、2003以降
- オープンソース: Star Office / Open Office
- オープンスタンダード: PDF、HTML、CSV、TXT

識別されるデータの種類

- 保険（オーストラリアのメディケアカード、ヨーロッパのEHIC、アメリカの健康保険請求番号など）
- 金融（American Express、Diners Club、Mastercard、VISAカード番号、銀行口座番号など）
- 個人（名前、姓、住所、生年月日、メールアドレスなど）
- 国民ID（社会保障番号、スペインのDNIなど）
- カスタム情報

組み込みテンプレート

ソリューションには、すぐに使える幅広いテンプレートが含まれており、一般的な規制やビジネスポリシーの要件を満たすために役立ちます。

- CCPA
- GDPR
- HIPAA
- PCI DSS
- PII
- PHI

最小必要RAM

- 16GB

ネットワーク接続

- At least 1GB

CipherTrust Enterprise Key Management

CipherTrust Key Management 製品は、CipherTrustプラットフォームアプリケーションだけでなく、サードーティ製デバイス、データベース、クラウドサービス、アプリケーションの鍵管理を一元化します。これにより、データセキュリティを向上させると同時に、鍵をより強力に制御できます。CipherTrust Key Management製品は標準インターフェースを通じてアプリケーションに接続し、堅牢な鍵管理と暗号化機能へのアクセスを提供します。

Enterprise Key Management ソリューション

CipherTrust Enterprise Key Managementソリューションは、以下のさまざまなアプリケーションをサポートします。

KMIP(Key Management Interoperability Protocol)

KMIPは、クライアント(アプライアンスやアプリケーション)とサーバ(鍵ストア)間で暗号鍵を交換するための業界標準のプロトコルです。標準化により、SANおよびNASストレージアレイ、自己暗号化ドライブ、ハイパーコンバージドインフラストラクチャなどのストレージソリューションにおける外部鍵管理が容易になります。KMIPは、暗号化されるデータから鍵を分離する要件を簡素化し、これらの鍵を共通のポリシーセットで管理できるようにします。CipherTrust Managerは、KMIPクライアントとして動作する幅広いサードパーティ製アプリケーションやデバイスに対して、KMIPサーバとして動作します。

データベースとLinuxの鍵管理

データベースとLinux向けのCipherTrust Enterprise Key Managementソリューションは、 IT効率をせながら、高度なセキュリティを提供します。TDE(Transparent Data Encryption)鍵管理とLUKS(Linux Unified Key Setup)の両方において、データベースまたはLinuxサーバ上のエージェントは、CipherTrust Managerに鍵を要求し、それらをTDEまたはLUKSインターフェースに提供します。

独自アプリケーションの鍵管理

暗号化の実行だけでなく鍵の一元管理も必要とするアプリケーションへの最も便利な統合を可能にするために、CipherTrust Managerは、幅広いアプリケーション環境で活用できる開発者向けAPIを提供します。パフォーマンスを最も重視するアプリケーションのために、CipherTrust Application Data Protectionは、Microsoft Crypto Next-Generation(CNG)、Crypto Services Provider(CSP)およびPKCS#11の鍵管理「プロバイダ」による、Java、C、C++、 .NET、.NET COREを実装したアプリケーション層ライブラリを提供します。

Key Managementの技術仕様

管理
- セキュアWeb、CLI、API
- コマンドラインスクリプト

検索、アラート、レポート用の鍵のフォーマット
- 対称暗号鍵アルゴリズム: AES、ARIA
- 非対称暗号鍵アルゴリズム
  - RSA
  - 楕円曲線: brainpool、prime、secp

サードパーティによる暗号化
- Microsoft SQL Server EKM, Microsoft SQL Always Encrypted, Oracle TDE

APIサポート
- PKCS#11
- Microsoft Crypto API (CAPI), Cryptographic Service Provider (CSP), Cryptographic Next Generation Provider (CNG), Java Cryptographic Extension (JCE), Microsoft Extensible Key Management (EKM)
- KMIP

暗号鍵の可用性と冗長性
- 自動バックアップによる複数のアプライアンス間でのセキュアな鍵の複製

検証済みのKMIP統合

HCI
- Cloudian HyperStore, VMware vSAN/VMCrypt, Nutanix, Dell EMC ECS, NetApp Cloud ONTAP, Hedvig Distributed Storage Platform, Dell EMC PowerOne, Dell EMC PowerFlex

バックアップ
- Commvault Data Protection Advanced

メインフレーム
- Syncsort Assure Encryption for IBM i-Series

ストレージ
- DellEMC Data Domain, DellEMC PowerEdge, NetApp FAS, HPE Proliant/StoreEasy (iLO)*, HPE 3PAR, HPE Primera, IBM DS8000 Series

フラッシュストレージ
- Dell EMC PowerMax, IBM , Dell EMC PowerStore

テープライブラリ
- HPE StoreEver、Quantum Scalarシリーズ

データベース/ビッグデータ
- MongoDB, IBM DB2, Oracle MySQL

*NAE-XML APIを介した統合

CipherTrust Cloud Key Management

多くのクラウドサービスプロバイダーは、保存データ暗号化機能を提供しています。一方、多くのデータ保護のベストプラクティスでは、暗号鍵をクラウドサービスプロバイダーから離れた場所で管理することが推奨されています。クラウドプロバイダーの「BYOK（Bring Your Own Key：独自の鍵の持ち込み）」サービスやAPIは、これらの要件を満たせます。

ユーザによる鍵制御

BYOKベースのユーザによる鍵管理により、暗号鍵またはその作成に使用されるテナントシークレットの分離、作成、所有、失効を含む管理が可能になります。BYOK APIを活用することで、CipherTrust Cloud Key Managerは、一元管理と可視性を備えた暗号鍵の完全なライフサイクル管理を提供し、鍵管理の複雑さと運用コストを削減します。

主なメリット

- 複数のクラウド環境にわたる鍵の一元管理、自動鍵ローテーションと有効期限管理により、IT効率を向上
- 完全なクラウド暗号鍵のライフサイクル管理により、「BYOK」サービスの価値を実現
- セキュアな鍵の生成と鍵の使用状況のログとレポートにより、最も厳しいデータ保護要件に対応

IT効率の向上

IT効率をサポートする機能は、以下のとおりです。

- 単一のブラウザウィンドから各クラウドプロバイダーへの一元的なアクセス
- ネイティブクラウド鍵の管理
- 自動同期により、クラウドコンソールの操作を一元的に把握することが可能
- 有効期限切れの鍵に対応した自動鍵ローテーションで、年間数千時間の時間短縮が可能

暗号鍵のセキュリティ

セキュアな鍵生成は、CipherTrust Managerまたは Vormetric Data Security Managerを利用し FIPS 140-2 Level 3までのセキュリティ要件を満たします。

必要なコンプライアンスツール

鍵のアクティビティログとパッケージ済みのレポートにより、迅速にコンプライアンスレポートを作成できます。ログは、複数のsyslogサーバやSIEMシステムへ転送できます。

技術仕様

CipherTrust Cloud Key Managerは、スタンドアロンアプライアンスと、CipherTrust Managerに組み込まれたサービスの2つのエディションで提供されます。鍵のライフサイクル管理機能は、エディション間で同一です。

BYOKとクラウドネイティブ鍵管理

- 作成
- アップロード
- 有効化/無効化
- 取り消し
- 削除
- ローテーション
- 自動ローテーションと有効期限
- 鍵のメタデータとポリシーの管理
- クラウド鍵管理システムとの同期の自動化

	アプライアンス	組み込み型
サポートされるクラウド	• Azure、Azure Stack、Azure Germany、中国のソブリンクラウド • Office365 • AWS • Salesforce および Salesforce Sandbox • IBM Cloud • Google Cloud CMEK	• Azureおよび Azure GovCloud • Office365 • AWS, AWS GovCloud, AWS China
キーソース	• CipherTrust Manager • Vormetric Data Security Manager	• 組み込み型動作 CipherTrust Manager
ユーザ認証	• クラウドプロバイダーへのパススルー	• CipherTrust Manager上でのユーザ管理
展開オプション	• VMware • Azure Marketplace • AWS • Azure Stack	• VMware • OpenStack • Azure Marketplace • Azure GovCloud • AWS • AWS GovCloud • Google Cloud • Oracle Cloud

CipherTrust Transparent Encryption

CipherTrust Transparent Encryptionは、鍵の一元管理、きめ細かなアクセス制御、データアクセス監査ログを備えた保存データ暗号化を提供することにより、組織がデータ保護のためのコンプライアンスレポートとベストプラクティスの要件に対応できるようにします。

このソリューションの透過的アプローチは、複数のクラウド環境にわたって、また、ビッグデータの実装内で、構造化データベースや非構造化ファイルを保護します。実装はシームレスで、ビジネスと運用の両プロセスとも変更の必要がありません。

コンプライアンス要件への対応

暗号化、アクセス制御、データアクセスログは、PCI DSS、HIPAA/Hitech、GDPRなど、ほぼすべてのコンプライアンスやデータプライバシーに関する規格や要件において、基本の要件または推奨のベストプラクティスとなっています。CipherTrust Transparent Encryptionは必要な制御を提供します。

スケーラブルな暗号化

CipherTrust Transparent Encryptionは、サーバ上のファイルシステムまたはボリュームレベルで実行され、Microsoft Windows Server、多くのLinux、IBM AIXオペレーティングシステムで利用可能です。物理環境、仮想環境、クラウド環境、ビッグデータ環境において、基盤となるストレージ技術に関係なく使用できます。管理者はCipherTrust Managerを介してすべてのポリシーと鍵の管理を実行します。

サーバベースの暗号化は、Intel AES-NIやIBM POWERなど、CPUに内蔵された暗号アクセラレーションを活用することで、パフォーマンスとスケーラビリティの両方をさらに向上させ、ボトルネックを解消します。

きめ細かなアクセス制御

きめ細かな最小権限のアクセスポリシーにより、外部からの攻撃や特権ユーザによる悪用からデータを保護します。ポリシーは、システム、LDAP/Active Directory、Hadoopのユーザやグループによって適用できます。制御には、プロセス、ファイルタイプ、その他のパラメーターが含まれます。

アクセスポリシーを定義して「信頼できる」アプリケーションの許可リストを作成することで、信頼できないバイナリ(ランサムウェアなど)がCipherTrust Transparent Encryptionで保護されたデータストアにアクセスするのを防いだり、特権ユーザがファイルやデータベースのユーザデータにアクセスするのを防いだりすることができます。これらのアクセスポリシーにより、侵入者がそのバイナリの実行権限と、ビジネスクリティカルなデータを含むターゲットファイルへの読み取り/書き込み権限を持っていても、不正なバイナリによるファイル/データベースの暗号化をブロックできます。

非侵入型の、透過的な展開

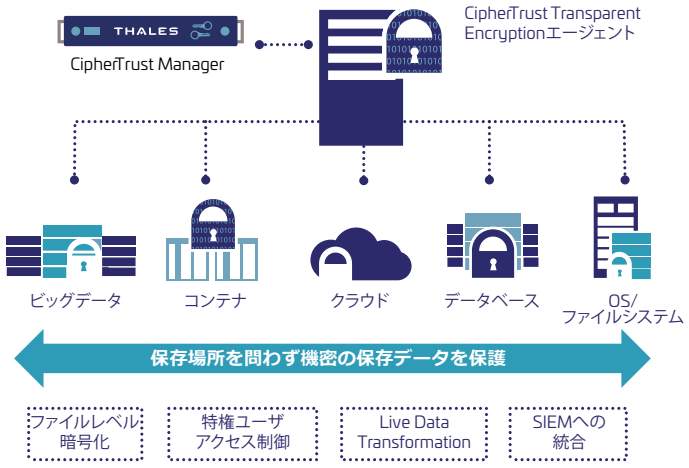
このソリューションでは、アプリケーション、ワークフロー、ビジネスや運用の手順を変更する必要はありません。

主なメリット

- コンプライアンスやベストプラクティスの要件に対応し、拡張性のある暗号化とアクセス制御を実現
- 展開が容易: アプリケーションのカスタマイズが不要
- 特権を持つ内部関係者による悪用や、盗まれた資格情報を利用したマルウェアに対する強力な保護を確立

主な機能

- 業界で最も幅広いプラットフォームをサポート: Windows、Linux、AIXオペレーティングシステム
- 高性能な暗号化: ホストCPUに内蔵されたハードウェア暗号化機能を使用 - Intel、AMD AES-NI、IBM POWER AES暗号化
- ユーザ、アプリケーション、プロセスからのアクセス試行の許可、拒否、制限をログに記録
- ロールベースのアクセスポリシーにより、誰が、どのデータに、どのようにアクセスできるかを制御
- 特権ユーザが、クリアテキストデータにアクセスすることなく業務を遂行

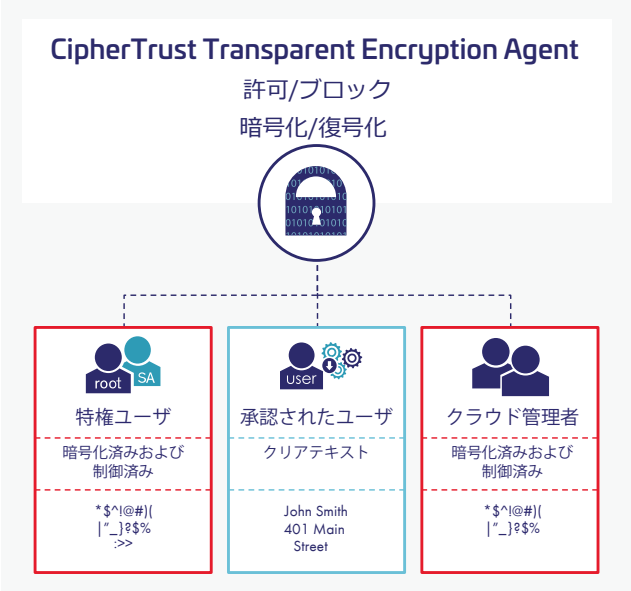


CipherTrust Transparent Encryptionは保存場所を問わずデータを保護します

オンプレミスまたはクラウド上のデータの保護

クラウドデータのセキュリティは、最初は簡単に思えるかもしれません。パブリッククラウドプロバイダー用のフルディスク暗号化に相当するものを有効にするのは簡単です。しかし、今やマルチクラウドの世界です。複数のパブリッククラウドやさまざまなクラウドストレージオプションにわたるデータセキュリティの管理は、すぐに複雑化します。CipherTrust Transparent Encryptionは、複数のIaaS(infrastructure as a service)クラウドで一元化された共通の制御と鍵を使用することで、クラウドネイティブの暗号化よりも多くの脅威からクラウドデータを保護できます。その結果、運用コストが削減され、クラウド間のデータ移行性が向上します。

CipherTrust Transparent Encryptionは、IaaS環境のオペレーティングシステムで利用可能な、ほぼすべてのストレージを保護します。また、Amazon S3のバケットの機密データに透過的な暗号化とアクセス制御を適用できます。CipherTrust Transparent Encryptionソリューションは、非構造化ファイル、半構造化データ、構造化データベースをAmazon S3バケットに書き込む前に暗号化します。このソリューションはFIPS 140-2 Level 3まで準拠したCipherTrust Managerと連携して動作し、鍵とポリシー管理のデータからの分離を保証します。S3バケットをCipherTrust Transparent Encryptionで保護すると、そこに保管されたファイルはすべて自動的に暗号化され、不正アクセスが発生した場合でも、内部のデータは無意味となります。CipherTrust Transparent EncryptionによるAmazon S3のサポートにより、クラウドに保存される大量のデータの安全性を確保し、また最も厳しいセキュリティ規制への準拠し、クラウド業界で最も一般的なセキュリティギャップを解消することができます。



セキュリティインテリジェンス

CipherTrust Transparent EncryptionとCipherTrust Managerとの連携により、ファイルアクセスアクティビティに対する洞察を得ることができます。データアクセスログには、CipherTrust Transparent Encryptionが動作している場所であればどこでも、許可されたデータアクセスと許可されていないアクセス試行の両方に関する詳細が含まれます。提供される情報には、コンプライアンス監査のために必要なもう一つの項目、セキュリティ管理者の行動も含まれます。

セキュリティインテリジェンスログは、SYSLOGやCEFなどのプロトコルを介してSIEMシステムに転送され、脅威の検出を迅速化します。

また、データセットを用いてアクセスパターンのベースラインを作成し、ベースラインから逸脱した挙動を示す脅威を迅速に特定できます。

CipherTrust Transparent Encryptionの技術仕様

暗号化アルゴリズムと機能
- AES

拡張ライセンス
- Live Data Transformation

プラットフォームサポート
- Microsoft: Windows Server 2022, 2019 and 2016
- Linux: Red Hat Enterprise Linux (RHEL)、SuSE Linux エンタープライズサーバ、Ubuntu
- UNIX: IBM AIX

データベースサポート
- IBM DB2、Microsoft SQL Server、Microsoft Exchange Data Availability Group(DAG)、MySQL、NoSQL、Oracle、Sybase、その他

アプリケーションサポート
- SAP、SharePoint、カスタムアプリケーションなど、すべてのアプリケーションに透過的に使用可能

ビッグデータサポート
- Hadoop: Cloudera, IBM
- NoSQL: Couchbase, DataStax, MongoDB
- SAP HANA

暗号化ハードウェアアクセラレーション
- AMDおよびIntel AES-NI
- IBM POWER9暗号コプロセッサー

エージェント認証
- FIPS 140-2 Level 1

クラウドサポート
- AWS: EBS, EFS, S3, S3I, S3 Glacier
- AZURE: Disk Storage, Azure Files
- GCP: Persistent Disk, Local SSD, Filestore

CipherTrust Transparent Encryptionの拡張と追加機能

CipherTrust Live Data Transformation

保存データ暗号化の展開と管理にあたっては、最初の暗号化の間や、すでに暗号化されたデータの再暗号化する際に、計画的なダウンタイムやデータのクローン作成と同期が必要となる課題が生じる可能性があります。CipherTrust Transparent EncryptionのLive Data Transformationは、前例のない稼働時間と管理効率で暗号化と鍵ローテション時の再暗号化を可能にします。

ダウンタイムのない暗号化と鍵ローテーション

管理者は、ダウンタイムやユーザ、アプリケーション、ワークフローの中断を発生させることなく、データを暗号化できます。暗号化の実行中も、ユーザやプロセスが通常どおりデータベースやファイルシステムとの通信を続けることができます。

セキュリティのベストプラクティスと規制要件に対応するには、定期的な鍵ローテーションが必要です。Live Data Transformationは、オンラインの鍵ローテーションとデータの再暗号化により、これらの要件に迅速かつ効率的に対応します。

Live Data Transformationは、暗号化とビジネスニーズのバランスを取るためのリソース管理機能を提供します。管理者は、営業時間中は暗号化にシステムCPUの10%のみを消費し、夜間や週末は暗号化にCPUの70%を消費できるというルールを定義できます。同様の制御がI/O操作にも使用できます。

Live Data Transformationは、より高速な再暗号化を提供します。データ復号処理では、CipherTrust Managerから前の暗号鍵を取得しデータセットに自動的に適用されます。復元されたデータには、現行の暗号鍵で暗号化されます。

Live Data Transformationの技術仕様

オペレーティングシステムサポート

- Microsoft: Windows Server 2019, 2016 and 2012
- Linux: Red Hat Enterprise Linux 7および8、SuSE Linux Enterprise Server 12および15

クラスタサポート

- Microsoft Cluster: File Cluster, SQL Server Cluster

データベースサポート

- IBM DB2、IBM Informix、Microsoft SQL Server、Oracle、Sybase、その他

ビッグデータサポート

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

バックアップ/レプリケーションサポート

- DB2バックアップ、NetBackup、NetWorker、NTBackup、Oracle Recovery Manager（RMAN）、Windows Server Volume Shadow Copy Service（VSS）

SAP HANA用CipherTrust Transparent Encryption

CipherTrust Transparent Encryptionは、SAP HANAデータを保護し、企業が厳格なセキュリティ、データガバナンス、コンプライアンスの要件に準拠できるようにします。このソリューションは、すべてのSAP HANAデータおよびログパーティションに強力なデータ暗号化を適用し、SAP HANAの永続化レイヤーへのアクセスを保護および制御します。このソリューションは迅速に導入でき、SAP HANAや、基盤となるデータベースまたはハードウェアインフラストラクチャに変更を加える必要はありません。さらに、SAPは、CipherTrust Transparent Encryptionを評価し、SAP HANA 2.0環境に適したソリューションとして認定しています。

CipherTrust Tokenization

トークン化により、EU一般データ保護規則（GDPR）やPCI-DSS（Payment Card Industry Data Security Standard）などのセキュリティポリシーや規制要件に準拠するために必要なコストと労力を削減します。CipherTrust Tokenizationは、動的データマスキング機能を備えたアプリケーションレベルのトークン化サービスをボルト有り/無し両方で提供し、顧客へ完全な柔軟性をもたらします。どちらのソリューションも、データセンター、ビッグデータ環境、クラウドを問わず、機密資産の保護と匿名化を実行します。

Vaultless Tokenization

CipherTrust Vaultless Tokenizationは、保存データを保護し、そのポリシーベースの動的データマスキング機能により、使用中データを保護します。RESTful APIを一元管理およびサービスと組み合わせることで、フィールドごとに1行のコードによってトークン化できます。Vaultless Tokenizationは、分散型クラスタに対応した専用のトークナイゼーションサーバによって提供され、完全な職務分掌を実現します。トークン化の管理および設定は、便利なトークン化設定ワークフローを備えた運用ダッシュボードを含め、グラフィカルユーザインターフェースで実行できます。

動的データマスキング。ADまたはLDAPサーバによって制御されるユーザ識別情報に基づいて、フィールド全体をトークン化して返すか、フィールドの一部をマスキングして返すかをポリシーで定義します。たとえば、カスタマーサービス担当者はクレジットカード番号の下4桁のみを確認でき、売掛金担当者はクレジットカード番号全体を確認できるようにポリシーを設定できます。

中断なし。フォーマット保持トークナイゼーションにより、データベーススキーマを変更することなく、機密データを保護します。

Vaulted Tokenization

CipherTrust Vaulted Tokenizationは、幅広い既存フォーマットとカスタムトークナイゼーションフォーマットの定義機能をサポートし、無停止のフォーマット保持トークナイゼーションを提供します。Vaulted Tokenizationは機密性の高いデータに高レベルのセキュリティを提供し、そのインスタンスをサーバ単位でインストールしたり、複数のクライアントをサポートするWebサービスとしてインストールしたりすることもできます。

迅速な統合

CipherTrust Tokenizationソリューションは、標準プロトコルと環境バインディングを活用し、最小限のソフトウェアエンジニアリングで迅速に統合されます。

Vaultless Tokenizationの技術仕様

トークナイゼーション機能:

- 不可逆なフォーマット保持トークンオプション
- 最大128Kまでのデータ長に対応したランダムトークン
- データトークナイゼーション
- Unicode UTF-8文字セットのサポートにより、ほとんどの言語でデータのトークン化が可能
- FPEとランダムトークンのLuhnチェックオプション

動的データマスキング機能:

- ポリシーに基づき、左または右の文字数を表示し、マスク文字のカスタマイズが可能
- Lightweight Directory Access Protocol（LDAP）またはActive Directory（AD）を使用した認証

展開フォームファクタとオプション:

- オープン仮想化フォーマット（.OVA）および
- 国際標準化機構（.iso）
- Microsoft Hyper-V VHD
- Amazon Machine Image (.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

システム要件:

- ハードウェア最低必要条件: 4 CPUコア、16～32 GB RAM
- ディスク最低必要条件: 80GB

アプリケーション統合:

- RESTful APIs

パフォーマンス:

- 16 GBのRAMを搭載した32コアサーバ（デュアルソケットXeon E5-2630v3）で、トークンサーバ（複数のスレッドとバッチ（またはベクター）モード使用）ごとに、1秒あたり100万以上のクレジットカードサイズのトークナイゼーション処理を実行

Vaulted Tokenizationの技術仕様

トークナイゼーション機能:

- フォーマット保持トークン
- ランダムトークンとシーケンシャルトークンの生成
- 元のデータの消去と同等に、オンデマンドで特定のトークンを消去
- マスキング: 最後の4桁、最初の6桁、最初の2桁など
- 固定長、固定幅のマスキング
- ユーザ定義のカスタムフォーマット
- 正規表現（Javaスタイル）

サポートされるトークンボルトデータベース

- Microsoft SQL Server
- Oracle
- MySQL
- Cassandra

アプリケーション統合

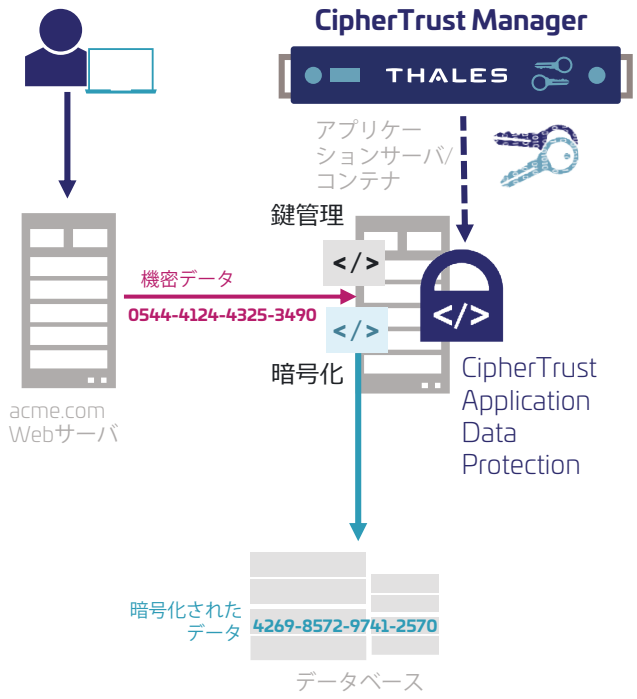
- RESTful APIs
- Java
- .NET

CipherTrust Application Data Protection

概要

CipherTrust Application Data Protectionは、機密データのアプリケーションレベルの暗号化に加え、鍵管理操作のためのDevSecOpsに対応したソフトウェアツールも提供します。このソリューションは、アプリケーションを通過するほぼすべてのタイプのデータを暗号化できる柔軟性を備えています。アプリケーション層でのデータ保護は、データの作成時や最初の処理時にすぐに実行でき、データのライフサイクル状態（転送、使用、バックアップ、コピー中など）に関係なく暗号化された状態を維持できるため、最高レベルのセキュリティを実現できます。CipherTrust Application Data Protectionは、物理、プライベート、パブリッククラウドのインフラストラクチャに展開でき、ある環境から別の環境に移行する場合でも、既存の暗号化やデータ処理ポリシーを変更することなく、データを保護できます。

CipherTrust Application Data Protectionは、複数のアプリケーション、環境、またはサイトにわたって鍵とポリシー管理を一元化するアーキテクチャである、CipherTrust Managerとともに展開されます。この組み合わせによるソリューションは、管理業務をデータおよび暗号鍵へのアクセスと分離し、きめ細かなアクセス制御を提供します。たとえば、追加の承認なしに管理者が単独で重要な設定変更を行えないようにするためのポリシーを適用できます。



CipherTrust Application Data Protectionとインストール可能なライブラリ

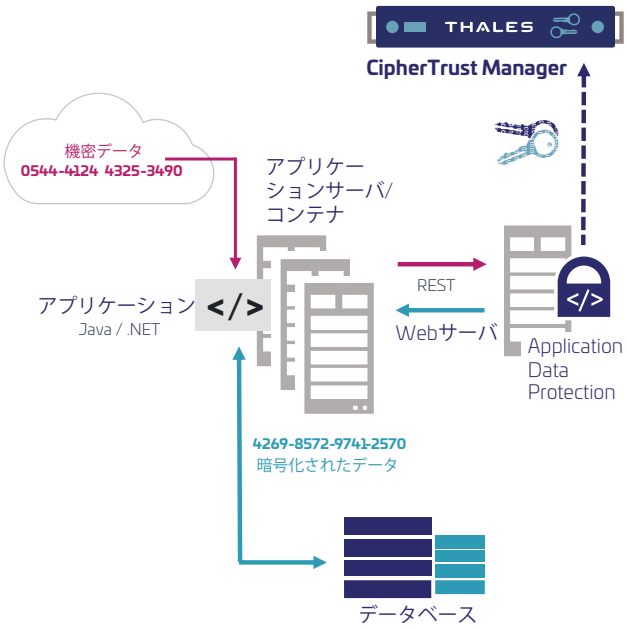
CipherTrust Application Data Protectionは、組み込みの自動鍵ローテーション機能を備え、暗号化、復号化、デジタル署名と検証、安全なハッシュアルゴリズム（SHA）、ハッシュベースのメッセージ認証コード（HMAC）などの幅広い暗号化操作を提供します。

CipherTrust Application Data Protectionは機能が豊富で、開発と運用の両方の柔軟性を提供します。

豊富な機能を、組み込みのサーバヘルスチェックやフェイルオーバと多層ロードバランシング、組み込みの鍵ローテーションを備えた形で提供します。

開発の柔軟性を、REST、C、.Net Core、Net、Javaの暗号ライブラリにより、幅広いプログラミングスキルに対応した暗号アプリケーションの作成を可能にすることで提供します。

運用の柔軟性は、以下の2つで提供されます。1つ目に、幅広い暗号化プロバイダー、ネイティブC、PKCS#11、Windows用のCryptographic Service Provider（CSP）、Crypto Next Generation（CNG）プロバイダー、 Java Crypto Engine（JCE）などが利用できます。

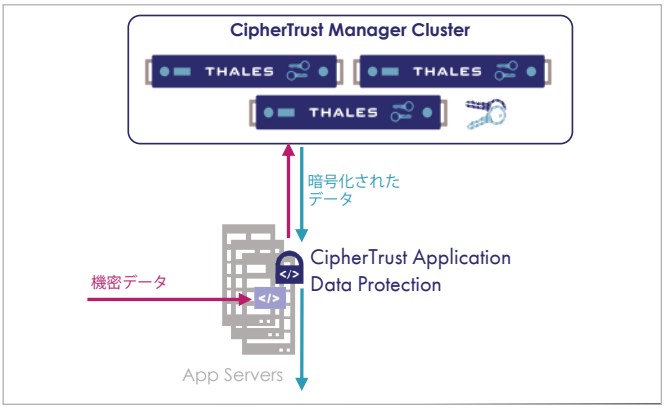


Webサービスとしてインストールされた**CipherTrust Application Data Protection**

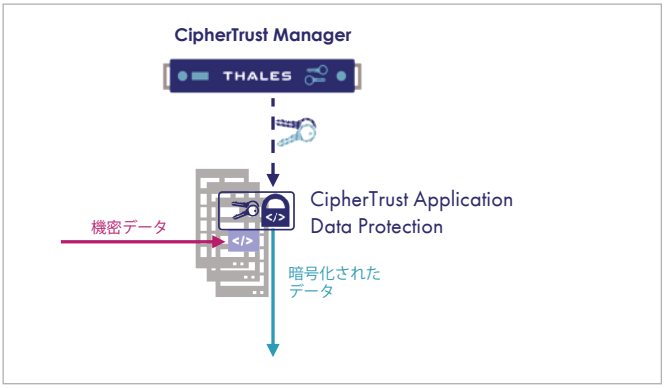
2つ目に、**暗号化運用の柔軟性**を、製品のライブラリまたはWebサービスエディションにおいて、コードを変更することなく、ローカルまたは CipherTrust Manager で暗号化するかの選択を可能にすることで提供します。この選択は、簡単な設定変更で行えます。

暗号化する場所には選択肢があり、それに伴うメリットがあります。

- CipherTrust Managerでの暗号化はセキュリティ、パフォーマンス、スケーラビリティのメリットをもたらし、鍵が信頼できるCipherTrust Managerから流出することがないため、最高レベルのセキュリティを実現できます。アプリケーションサーバから暗号化をオフロードすることで、アプリケーションサーバのパフォーマンスを向上させることができます。また、CipherTrust Application Data Protectionライブラリには、暗号化の負荷をCipherTrust Managerのクラスタに分散させることができるロードバランシングメカニズムが組み込まれています。



- アプリケーションサーバでの暗号化は、特定のタイプの暗号化ワークロードに対してより高いパフォーマンスを提供できる可能性があります。オープンソースのソリューションとは対照的に、鍵は使用中でないときはメモリ内で暗号化され、使用中はメモリ内に分散されます。どちらのメカニズムも、重要な暗号鍵を悪用から保護します。



CipherTrust Application Data Protectionは CipherTrust Managerとの連携により、保護されたデータと暗号鍵へのアクセスのログ、監査、レポート作成を行うための単一のインターフェースを提供します。

豊富な暗号化エコシステム

CipherTrust Application Data Protectionは、上述した鍵管理統合に加え、 Microsoft Crypto Next Generation(CNG)、 Microsoft Crypto Service Provider(CSP)、Microsoft Online Certificate Status Protocol(OCSP)、 Hashi Vault、 HortonWorks、Apache HTTPおよびNGINX Server、 Lieberman ERPM、その他多数との統合が可能です。

メリット

- 鍵の一元管理により、開発者を複雑でリスクの高い鍵管理ストアから解放
- セキュリティを強化し、コンプライアンスを確保
- 最大限のセキュリティを確保したクラウドを利用
- セキュリティアプリケーション開発を加速
- アプリケーションサーバのパフォーマンスを最適化
- ストレージ、サーバ、データベース、アプリケーション、クラウドの主要ベンダーとの統合を実現する比類のないパートナーエコシステム
- 幅広いネイティブ暗号化ソリューションの鍵管理

Application Data Protectionの技術仕様

開発ライブラリとAPI

- Java、C、.NET Core用のC#、.NET
- KMIP標準
- XMLオープンインターフェース
- Webサービス: REST

暗号化サービスプロバイダーとサポートされるOSのCプロバイダー

- Windows
- Linux
- AIX
- MacOS

KMIPサーバ/プロバイダー

- CipherTrust Manager上

PKCS#11プロバイダー

- Windows Server
- Linux
- AIX
- Solaris

CSPおよびCNGプロバイダー

- Windows Server
- Linux
- Solaris
- HP-UX
- AIX

CSP and CNG Providers

- Windows Server 2008以降

暗号化アルゴリズム

- 3DES、AES 256(CBCとXTS)、SHA 256、SHA 384、SHA 512、RSA 1024、RSA 2048、RSA 3072、RSA 4096、ECC
- フォーマット保持: FF1/FF3、トークン化

Webアプリケーションサーバ

- Apache Tomcat、IBM WebSphere、JBoss、Microsoft IIS、Oracle WebLogic、SAP NetWeaver、Sun ONEなど

クラウドおよび仮想インフラストラクチャ

- AWS、Azure、IBM Cloud、Google、VMwareなど、あらゆる主要クラウドプラットフォームで動作

CipherTrust Database Protection

概要

CipherTrust Database Protection製品は、クレジットカード、社会保障番号、国民ID番号、パスワード、電子メールアドレスなど、データベースに存在する構造化された機密データをカラムレベルで透過的に暗号化します。CipherTrust Database ProtectionとCipherTrust Teradata Database Protectionは、データベース保護で役立つ選択肢を提供し、どちらもCipherTrust Managerを利用して鍵を一元管理します。さらに、CipherTrust Database Protectionの設定は、CipherTrust Managerコンソールで一元的に行われます。

このソリューションにより、データベース内の機密データフィールドを効率的に保護し、セキュアに保てます。どちらのソリューションも、アプリケーションやビジネスプロセスに対して透過的であり、変更を必要としません。また、どちらもクラウドに対応しています。効率性のため、両製品とも、コードを変更することなく、パフォーマンスのためにローカルで暗号化するか、暗号鍵がセキュアなエンクレーブから離れることがないようにCipherTrust Managerで暗号化するか、いずれかのメカニズムを選択できます。この選択は簡単な設定変更で行えます。

CipherTrust Database Protection

CipherTrust Database Protectionは、データベースビューとトリガーを利用してデータを暗号化し、暗号化されていないフィールドと暗号化されたフィールドへのアクセスをアプリケーションに対して透過的に保ちます。鍵の粒度はフィールド単位です。

展開と初期使用

CipherTrust Database Protection は各データベースサーバにインストールされます。手動およびサイレントモードでのインストールに加え、Chefレシピによるインストールなども可能です。

インストールが完了すると、データベースサーバ上のソフトウェアがCipherTrust Managerにセキュアにリンクされ、鍵にアクセスできるようになり、一部の構成やデータベースでは、暗号化および復号化サービスも利用できるようになります。

通常、インストール後は、暗号化するデータ（通常はカラム）の選択、データベーステーブル、ビュー、トリガー設計の定義、そして最後に一括データ暗号化を含んだデータ移行プロセスが行われます。

それ以降は、トリガーとビューで以下が可能になります。

- 新しいデータを暗号化する
- 許可されたユーザに対してデータベースの読み取りを復号化する
- データベースの更新は、ユーザやワークフローに対して完全に透過的に暗号化される

Database Protectionの技術仕様

サポートされるデータベース

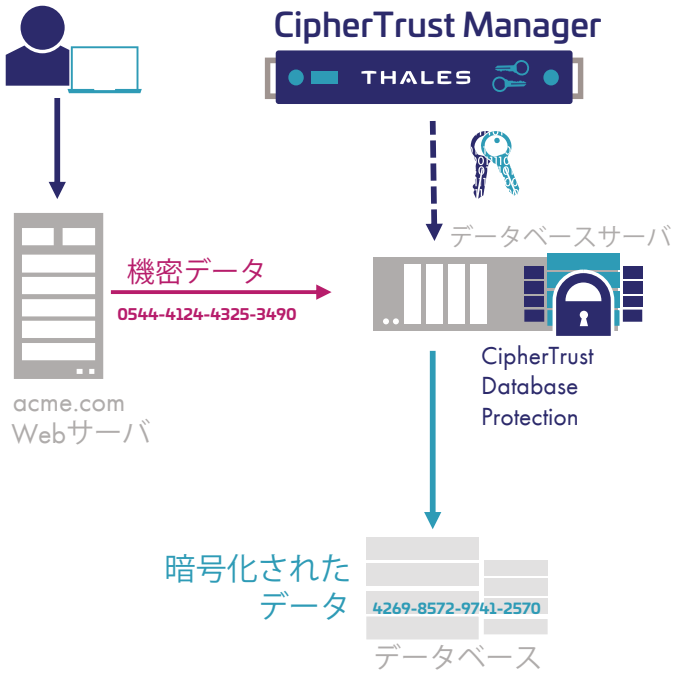
- Oracle
- Microsoft SQL Server
- IBM DB2

サポートされるプラットフォーム

- Microsoft Windows
- Linux
- Solaris
- AIX

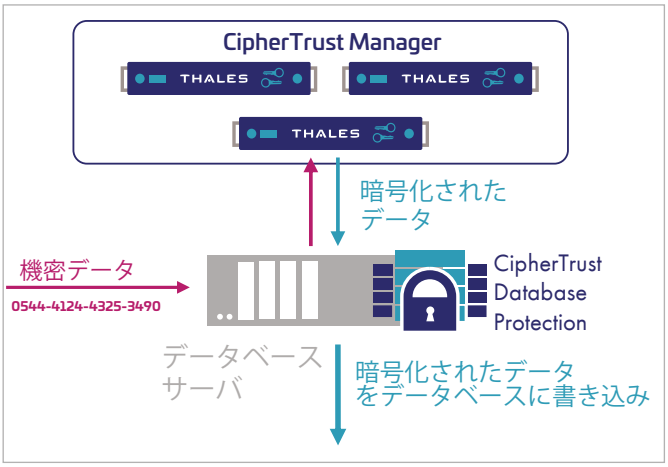
暗号化アルゴリズム

- FPE (FF1, FF3), AES, 3DES, RSA, ECC

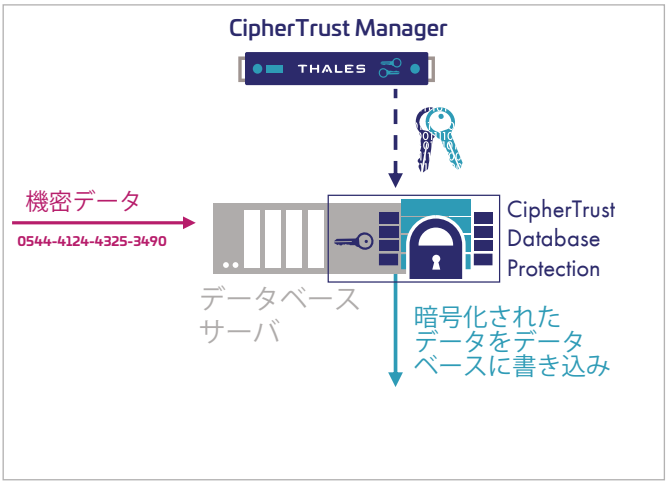


CipherTrust Database Protectionを使用する際、暗号化する場所を選ぶことでメリットがもたらされます。

- CipherTrust Managerでの暗号化はセキュリティ、パフォーマンス、スケーラビリティのメリットをもたらし、鍵が信頼できるCipherTrust Managerを流出することがないため、最高レベルのセキュリティを実現できます。データベースサーバから暗号化をオフロードすることで、データベースサーバのパフォーマンスを向上させることができます。また、CipherTrust Database Protectionライブラリには、暗号化の負荷をCipherTrust Managerのクラスタに分散させることができるロードバランシングメカニズムが組み込まれています。



- データベースサーバでの暗号化は、データベース暗号化の特定フィールドに対してより高いパフォーマンスを提供できる可能性があります。オープンソースのソリューションとは対照的に、鍵は使用中でないときはメモリ内で暗号化され、使用中はメモリ内に分散されます。どちらのメカニズムも、重要な暗号鍵を悪用から保護します。



CipherTrust Teradata Protection

CipherTrust Protection for Teradata Databaseは、Teradata Vantage SQL Databseの機密データを含むカラムを保護するプロセスを簡素化します。このソリューションは、従来の暗号化とNIST承認のフォーマット保持暗号化(FPE)機能の両方を提供し、フォーマットを変更することなくフィールドを保護できるため、関連アプリケーションやワークフローへのデータ保護による潜在的な影響を最小限に抑え、従来型暗号化アプローチのストレージ要件の増加を回避します。また、このソリューションは、動的データマスキングを提供し、特定のユーザに対してさまざまなレベルの復号化とデータの表示を設定できます。

暗号化の展開と利用の効率化

このソリューションは、データベースエンジンのユーザー定義関数(UDF)としてのTeradata Vantage SQLに対するデータ保護から生じる潜在的な複雑さを軽減し、データベースユーザや管理者とは別にデータアクセスを制御することを可能にします。

セキュリティ管理者は、暗号化方式やユーザ固有の許可・拒否リストを定義したデータアクセスプロファイルを指定します。また、データベースのカラムごとに異なる暗号鍵を使用し、固有の鍵を1人または複数のTeradata Vantage Databaseユーザにバインドすることが可能です。さらに、特定の拒否動作をユーザごとに割り当てることも可能です。データは一度暗号化されると、たとえUDFが管理上無効になったとしても、データは保護されたままになります。

メリット

- ビッグデータ分析の価値を損なうことなくセキュリティを強化
- サイバー攻撃や特権ユーザによる悪用に対する防御を確立
- 迅速で便利な導入と設定

技術仕様

サポートされるデータベース
- Teradata Database、最小バージョン16.2

サポートされるプラットフォーム
- SUSE Linux Enterprise Server(SLES)、最小バージョン11SP3

暗号化アルゴリズム
- AES, FPE (FF1, FF3)

最大列幅
- ASCII—16KB, Unicode—8KB

暗号化制御
- 列ごとのIDベースのアクセス
- IDに基づく動的マスキング
- 許可/拒否アクセス制御

暗号化キーソース
- CipherTrust Manager

CipherTrust Batch Data Transformation

静的データマスキング

静的データマスキングは、機密データの不正利用を防止しながらデータセットを活用するために、選択データを判読不能な形式に変換します。

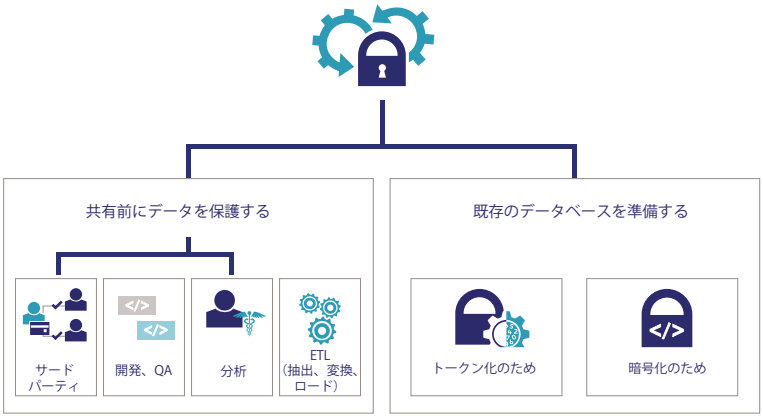
CipherTrust Batch Data Transformationは、暗号鍵の一元管理によって高パフォーマンスなデータマスキングを提供し、CipherTrust Application Data ProtectionとCipherTrust Tokenizationを活用して膨大な量のデータを迅速に保護します。

静的データマスキングには多数のユースケースがあります。次の4つは、「機密データのマスキング」が主語となります。

1. 第三者とデータを共有する前に行う。
2. 開発、QA、R&D、分析で共有するデータベースで行う。
3. ビッグデータ環境にデータセットを追加する前に行う。
4. ETL（抽出、変換、ロード）操作の前に行う。

その他、以下のようなユースケースがあります。

- トークン化または暗号化の展開のためにデータベースを準備する。
- 鍵ローテーション後に暗号化されたデータカラムを再暗号化する。



CipherTrust Batch Data Transformationによる、大量かつ柔軟なデータマスキング、トークン化、暗号化の実現

主なメリット

- 最大FIPS 140-2 Level 3のソースから供給されたデータ暗号鍵の一元管理により、安全でコスト効率の良い静的データマスキングを実現
- リスクを軽減したデータベース共有が可能
- CipherTrust Data Discovery and Classificationの展開後の既存データの保護を加速
- 必要な場所での静的データマスキング。オンプレミス、クラウド、ハイブリッド展開が可能

技術仕様

データ変換オプション:

- トークン化、データ暗号化
- アルファベット/数字を保持するフォーマット

ポリシーファイルオプション:

- 個々のカラム変換ごとの特定のアクション – 暗号化、復号化、トークン化、トークン化解除、再暗号化
- アプリケーションの変更を必要としない、暗号化の容易な適用
- 柔軟な鍵管理オプション - CipherTrust Managerまたはサーバ内の鍵、複数鍵のサポート

データセキュリティプラットフォーム要件

- キーソース: CipherTrust Manager、Vormetric Data Security Manager、KeySecure Classic
- 前提条件となるコンポーネント: トークン化にはCipherTrust Tokenization Serverの展開とライセンス、暗号化にはCipherTrust Application Data ProtectionまたはVormetric Application Encryptionのいずれかとライセンスが必要です。

ハードウェアとオペレーティングシステム要件:

- 4コアのプロセッサ、16GB RAM（最小）
- Java Runtime Environment (JRE)
- Windows Server 2012以上
- Linux – RedHat, CentOS, Ubuntu and SUSE

THALES

Building a future we can all trust

お問い合わせ

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。

> cpl.thalesgroup.com/ja <