Vormetric Data Security Platform

よくあるご質問

Vormetric Data Security Platform 共通のFAQ

Q. ライセンスは買い取りですか？

A. はい。

基本、製品は買い取りになります。
保守契約を締結いただいたお客様は、無償でバージョンアップモジュールをダウンロードできます。
注）クラウド暗号化サービスの鍵管理（CCKM）は、サブスクリプション契約となります。

Q. ライセンスのみ購入は可能ですか？

A. いいえ。

ライセンスと保守サービスを同時にご購入いただきます。
他に、オプションとして24時間365日対応サービスや、オンサイトサービスなどをご用意しております。
保守サービスの契約期間は1年単位で、その後は毎年更新となります。

Q. クラウド環境でも利用できます？

A. はい。

Microsoft AzureやAmazon Web Servicesといったパブリッククラウドに、
オンプレミスと同様の環境を構築することができます。

Q. 評価版を借りられますか？

A. はい。

試用期限付きの評価ライセンスをご用意しております。（最大1ヶ月）
お問合せフォームからお申込みください。

Q. 評価版から製品版へ乗り換えられますか?

A. はい。

ライセンスファイルを入れ替えるだけで、評価版から製品版へ移行できます。

Q. 保守は、日本語で対応してくれますか?

A. はい。

保守を締結いただいたお客様に対しては、弊社の保守窓口で日本語対応いたします。

鍵管理サーバーのFAQ
【DSM：Data Security Manager】

Q. 鍵管理サーバーは仮想アプライアンス版を提供していますか？

A. はい。

「VMware ESXi」や「Microsoft Hyper-V」などの仮想環境に対応しております。
提供形式：OVA、ISO、KVMイメージ、Azure VHD、AWS AMI

Q. 鍵管理サーバーを1台で使用することはできますか？

A. いいえ。

最低2台以上のHA構成が必須となります。（但し、開発・検証環境は1台での利用も可能です。）

Q. 鍵管理サーバーを2台以上で構成する場合、ロードバランサが必要ですか？

A. いいえ。

鍵管理サーバーのクラスタ内で状態監視しており、万が一障害が発生した場合は自動的に切り替わります。

Q. 暗号化は鍵管理サーバーが行うのですか？

A. いいえ。

暗復号は各機能コンポーネントで行います。
鍵管理サーバーは、鍵の生成や管理、ポリシーなどの設定情報のみ保存しており、データは保存しておりません。

Q. 設定情報をエクスポート/インポートできますか？

A. はい。

Web GUI画面から設定した情報は、エクスポート/インポートできます。
但し、CLIで設定するIPアドレスなどの情報は、手動設定となします。

Q. 暗号化する際のアルゴリズムを選択できますか？

A. はい。

鍵管理サーバー（DSM）で暗号化キー生成時に、「AES128」「AES256」「ARIA128」「ARIA256」の何れかを選択できます。

Q. 各機能コンポーネントで使用している鍵を統合管理できますか？

A. はい。

鍵管理サーバーのWeb GUI 画面で一元管理できます。

Q. 監視用エージェントをインストールできますか？

A. いいえ。

Linuxベースの OSですが、入力可能なコマンドが制限されています。

Q. Web GUI に対応しているブラウザーは何ですか？

A. Internet Explorer 10, 11、Google Chrome、Mozilla Firefox に対応しています。

透過暗号のFAQ
【VTE：Vormetric Transparent Encryption】

Q. サーバーへエージェントをインストールする必要がありますか？

A. はい。

対象のファイルサーバーやデータベースサーバーにエージェントソフトウェアをインストールします。
詳細はこちらのサイトにてご確認ください。

Q. サーバーへエージェントをインストール後、サーバー再起動は必要ですか？

A. はい。

エージェントをインストール/アンインストール後に、サーバー再起動が必要です。

Q. ファイルサーバーを冗長構成で運用している場合、エージェントのライセンスは幾つ必要ですか？

A. サーバーOSの数分ライセンスが必要です。

2台の冗長構成の場合は、2本になります。
「ホットスタンバイ」「コールドスタンバイ」にかかわらず、エージェントをインストールしたサーバーOSの数分ライセンスが必要です。

Q. サーバー内のフォルダー構成を変更する必要がありますか？

A. いいえ。

既存のフォルダー構成に対して暗号化ポリシーを適用します。
ポリシーが適用されたフォルダーに対しては、たとえアクセス権があったとしても、復号権限がないとファイルの中身を見ることはできません。

Q. 暗号化可能なデータの種類を問いますか？

A. いいえ。

Microsoft Office形式のファイル、.pdf ファイルおよびCADデータ、動画、画像などファイルの種類は問いません。
RDBMSやNoSQLといったデータベースファイルも暗号化できます。

Q. データベースを暗号化する際、データベースのスキーマやプログラムを変更する必要がありますか？

A. いいえ。

データベースが格納されている対象のフォルダーに暗号化ポリシーを適用するだけで、透過的（自動）に暗号化します。

Q. コンテナも暗号化できますか？

A. はい。

DockerやRed Hat OpenShiftに対応しており、コンテナ単位で暗号化できます。

Q. 暗号化/復号によりファイルの読み書き速度は低下しますか？

A. いいえ。

サーバーのCPUにAES-NI（Advanced Encryption Standard New Instructions）が搭載されていて
当該機能が有効な場合、パフォーマンスの低下は殆ど感じません。

Q. 既にデータが保存されているフォルダーに暗号化ポリシーを適用した場合、自動的に暗号化されますか？

A. はい。

オプションの自動暗号ツール（LDT：Live Data Transformation）を使用することで、既存データをバックグラウンドで暗号化できます。
透過暗号単体では既存データを手動で暗号化しなければならなく、手順が煩雑です。

Q. 暗号鍵を定期的に変更できますか？

A. はい。

オプションの自動暗号ツール（LDT：Live Data Transformation）を使用することで、オンライン稼働中でも鍵を変更できます。
透過暗号単体では手動で実施しなければならなく、手順が煩雑です。

Q. クライアントPCに暗号化した状態でファイルを保存できますか？

A. いいえ。

暗復号はサーバーにインストールしたエージェントが処理するため、クライアントPCには復号されたファイルが保存されます。

Q. NAS（Network Attached Storage）に対応していますか？

A. いいえ。

NAS用のエージェントは提供しておりません。

トークナイゼーションのFAQ
【VTS：Vormetric Tokenization with Dynamic Data Masking】

Q. 物理アプライアンスは提供していないのですか？

A. はい。

仮想アプライアンスで提供しているトークナイゼーションサーバーを仮想環境にデプロイします。

Q. トークナイゼーションサーバーは、VMwareやMicrosoft Hyper-Vに対応していますか？

A. はい。

「VMware ESXi」や「Microsoft Hyper-V」などの仮想環境に対応しております。
提供形式：OVA、ISO、Azure VHD、AWS AMI、GCP

Q. トークナイゼーションサーバーを1台で使用することはできますか？

A. はい。

性能要件を満たす場合は、トークナイゼーションサーバー1台でも運用可能です。

Q. トークナイゼーションサーバーを2台以上で構成する場合、ロードバランサは必要ですか？

A. はい。

トークナイゼーションサーバーのクラスタ内で設定情報を同期しますが、
状態監視および障害時の切り替えはロードバランサで制御いただくことになります。

Q. プログラム改修は必要ですか？

A. はい。

アプリケーションにREST API（トークナイズ/デトークナイズ リクエスト）を追加します。
トークナイゼーションサーバーに対してREST APIを用いてデータをPOSTする必要があります。

Q. トークン化したデータをデータベースに保存する場合、データベースのスキーマ変更が必要ですか？

A. いいえ。

元のデータの桁数やデータ型を維持した状態で変換しますので、データベースの変更は不要です。

Q. クレジットカード番号以外の住所、氏名、電話番号などもトークナイズできますか？

A. はい。

日本で使用されている漢字，カナ以外に、世界共通の文字コード「Unicode」表に掲載されている文字は変換可能です。

Q. カード番号などをトークナイズする際、指定した桁を維持することはできますか？

A. はい。

トークナイゼーションサーバーに設定するテンプレートで設定します。
例えば、16桁のカード番号の先頭6桁を維持し、下10桁をトークナイズすることが可能です。
他に、先頭6桁、下4桁を維持し、真ん中の6桁をトークナイズすることも可能です。
但し、トークナイズ対象データの桁数が少ないと、セキュリティ上の安全性が低下しますのでお勧めしません。

Q. デトークナイズする際、指定した桁をマスキング「＊」することはできますか？

A. はい。

トークナイゼーションサーバーに設定するテンプレートで設定します。
例えば、16桁のカード番号の先頭12桁をマスキングし、下4桁を復元することが可能です。

Q. 監視用エージェントをインストールできますか？

A. いいえ。

LinuxベースのOSですが、入力可能なコマンドが制限されています。

Q. 設定情報をエクスポート/インポートできますか？

A. はい。

Web GUI画面から設定した情報は、エクスポート/インポートできます。
但し、CLIで設定するIPアドレスなどの情報は、手動設定となります。

Q. Web GUIに対応しているブラウザーは何ですか？

A. Internet Explorer 10, 11、Google Chrome、Mozilla Firefoxに対応しています。

アプリケーション暗号のFAQ
【VAE：Vormetric Application Encryption】

Q. サーバーへエージェントをインストールする必要がありますか？

A. はい。

対象のサーバーにエージェントソフトウェアをインストールします。
詳細はこちらのサイトにてご確認ください。

Q. サーバーへエージェントをインストール後、サーバー再起動は必要ですか？

A. はい。

エージェントをインストール/アンインストール後に、サーバー再起動が必要です。

Q. 暗号化する際のアルゴリズムを選択できますか？

A. はい。

共通鍵暗号3DES、AESと公開鍵暗号RSAをサポートしています。

他社データベース暗号化製品の鍵管理のFAQ
【VKM：Vormetric Key Management】

Q. サーバーへエージェントをインストールする必要がありますか？

A. はい。

対象のデータベースサーバーにエージェントソフトウェアをインストールします。

Q. Oracle TDEやMicrosoft SQL Server TDEで使用している鍵を鍵管理サーバーで管理できますか？

A. はい。

Oracle TDEやMicrosoft SQL Server TDEで使用する鍵や、KMIP準拠のストレージ製品の鍵を専用の鍵管理サーバーで管理できます。

他社暗号化製品の鍵管理のFAQ
【KMIP：Key Management Interoperability Protocol】

Q. ライセンスはどのように提供されますか？

A. 鍵管理サーバーにインポートするライセンスファイルの提供となります。

暗号化対象デバイス（KMIP Client Connection）の数分ライセンスをご購入いただきます。

Q. VMware環境の暗号化に使用する鍵を管理できますか？

A. はい。

暗号化を実施する場合は、暗号鍵を管理するサードパーティの鍵管理サーバー（KMS：Key Management Server）が必要です。
Vormetricの鍵管理サーバーはKMSとして使用できます。
＊ VMware vSphere 6.5 から仮想マシンの暗号化を利用できるようになりました。

Q. KMIP準拠のストレージの暗号化に使用する鍵を管理できますか？

A. はい。

Dell EMCやNetAppなど、KMIP準拠のストレージ暗号化に使用する鍵を鍵管理サーバーで管理できます。

クラウド暗号化サービスの鍵管理のFAQ
【CCKM：CipherTrust Cloud Key Manager】

Q. 物理アプライアンスは提供していないのですか？

A. はい。

仮想アプライアンスで提供しているクラウド暗号化サービスの鍵管理を仮想環境にデプロイします。

Q. クラウド暗号化サービスの鍵管理は、VMwareやMicrosoft Hyper-Vに対応していますか？

A. はい。

「VMware ESXi」や「Microsoft Hyper-V」などの仮想環境に対応しております。
提供形式：OVA、Azure VHD、AWS AMI

Q. 複数のパブリッククラウドの暗号化サービスで使用している鍵を統合管理できますか？

A. はい。

MicrosoftのAzure Key VaultやAWSのKey Management Service、SalesforceのShield Platform Encryptionといった暗号化サービスで使用している鍵を、クラウド暗号化サービスの鍵管理で統合管理できます。
詳細はこちらのサイトにてご確認ください。

製品のお問い合せは、当社サイトよりお受けしております。

Vormetric 製品サイト　https://cweb.canon.jp/it-sec/solution/vormetric/