Vormetric

THALES

Vormetric Data Security Platform

～ エンタープライズ暗号化ソリューション ～

製品紹介

Canon

キヤノンマーケティングジャパン株式会社

Ver 4.01
2020年3月6日

情報漏えい対策には 暗号化が効果的

情報セキュリティを取り巻く環境は年々複雑化し対策が難しくなってきています。

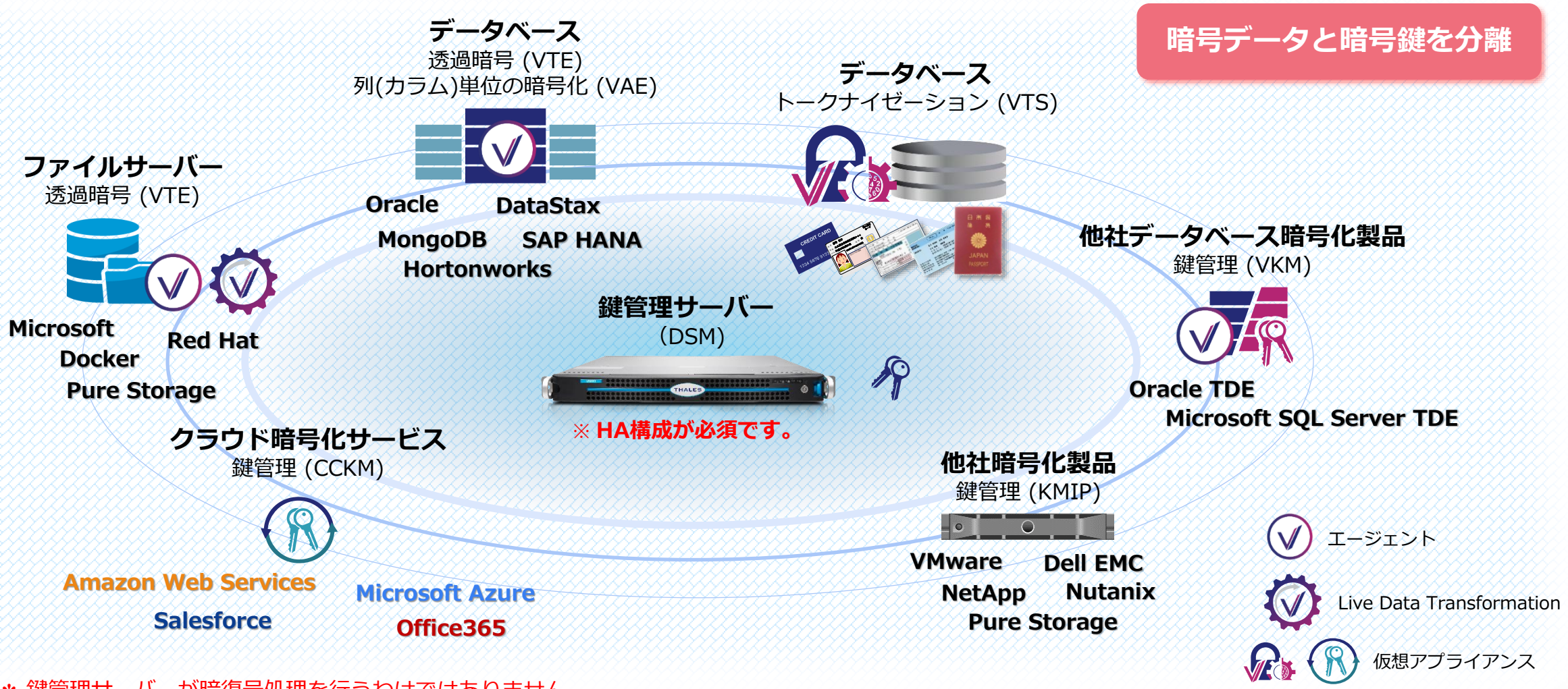
特に顕著なのが、OSやアプリケーションの脆弱性を突いた外部からの標的型攻撃や組織内部の人間による不正アクセスなどによる情報漏えいです。情報が流出すると企業の競争力や信頼を損なうだけではなく、損害賠償や訴訟問題へ発展し、企業イメージを大きく低下させてしまう可能性があります。

弊社は、重要な組織内のデータを守るため、国内外で導入実績のある Thales の暗号化製品
「Vormetric Data Security Platform」をご提供しています。

キヤノンマーケティングジャパンは、一次販売代理店(VAD)です。

Vormetric 製品構成

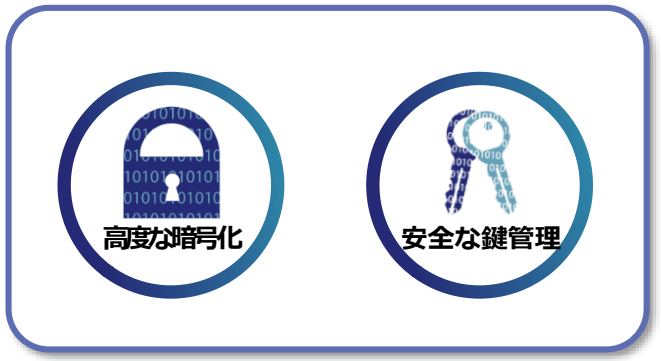
「Vormetric Data Security Platform」は、保存データ (Data at Rest) を保護する暗号化プラットフォームです。



＊ 鍵管理サーバーが暗復号処理を行うわけではありません。

製品別 データ保護レイヤ

機能コンポーネント別にデータ保護できるレイヤを示します。



鍵管理サーバー
(DSM)

データ保護レイヤ	機能コンポーネント
Key Management (On-Premises / Cloud Services)	**クラウド暗号化サービス** 鍵管理 (CCKM)
Application / Database	**データベース** トークナイゼーション (VTS) アプリケーション暗号 (VAE)
File System	**ファイルサーバー / データベース** 透過暗号 (VTE)
Disk	**他社暗号化製品** 鍵管理 (KMIP) **他社データベース暗号化製品** 鍵管理 (VKM)

鍵管理サーバー (DSM) のラインアップ

鍵管理サーバーは、物理アプライアンスと仮想アプライアンスを提供しています。

提供形態	鍵管理サーバー Data Security Manager ※ HA構成が必須です。 (最大8台)				
	DSM 物理アプライアンス			DSM 仮想アプライアンス	
外観	HSM対応 			OVA, ISO, KVMイメージ, Azure VHD, AWS AMI	
モデル	Physical DSM V6100	Physical DSM V6000		Virtual DSM	
型番	VDSM60L3	VDSM60L2	V25DSM60L2	VDSM60L1	V25DSM60L1
エージェント数	無制限	無制限	25 接続まで	無制限	25 接続まで
FIPS 140-2(※1)	FIPS 140-2 Level 3 HSM	FIPS 140-2 Level 2		FIPS 140-2 Level 1	
暗号アルゴリズム	共通鍵暗号方式：AES128, AES256, ARIA128, ARIA256 公開鍵暗号方式：RSA1024, RSA2048, RSA3072 or RSA4096				
本体重量	10kg	9.8kg			
ポート	Ethernet 1GB x2、IPMI x1、シリアルポート x1				
本体サイズ	1 U：43.18 x 52.07 x 4.5 cm				
電源	2 つの独立した電源 100-240V（電圧自動切替）、50-60Hz、400W				
価格(※2)	オープン価格				

- 仮想環境のシステム要件
  - CPU 2コア以上
  - RAM 8GB 以上
  - HDD 250GB （ シックプロビジョニング ）
- 対応ブラウザ
  - Internet Explorer 10, 11、Firefox、Chrome

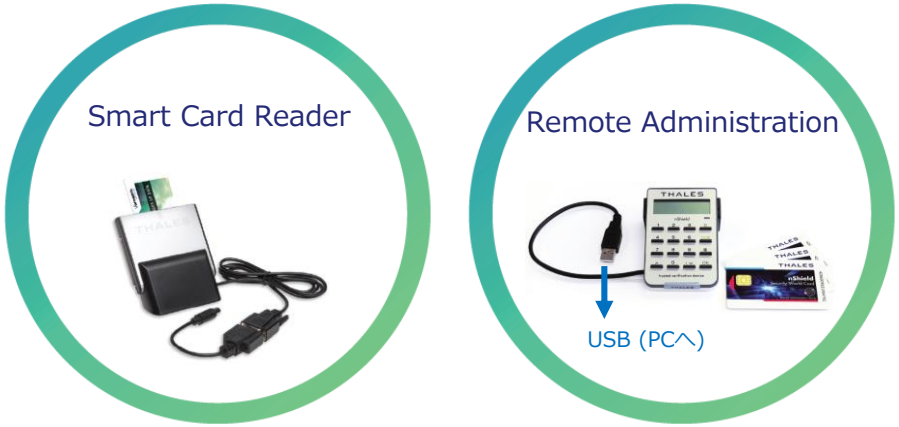
※1 「FIPS 140-2 」は暗号モジュールに関する要件を規定した米国連邦標準規格
Level 1：暗号化のセキュリティレベルにおいて基本的な要件を満たしていること。
Level 2：Level1に加えて物理的な改竄の痕跡を残せること。
Level 3：物理的な改竄への耐性（耐タンパー性）を持つこと。

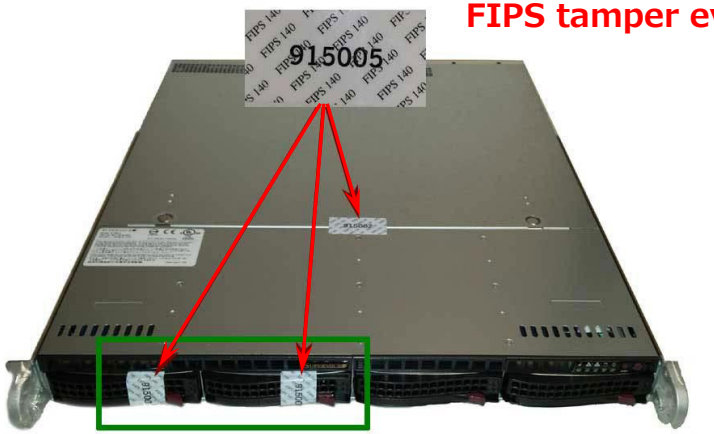
※2 製品には別途、年間製品保守費用が掛かります。

鍵管理サーバー (物理アプライアンス) の機能・特徴

■ 機能・特徴

- 鍵の生成/管理
- 米国国立標準技術研究所 (NIST) が制定した暗号アルゴリズムを搭載
- ポリシーの生成/管理
- ユーザー、グループ情報は、AD/LDAPと連携可能
- HA機能によりクラスター内で鍵を含む設定情報を同期
- 鍵とポリシーをExport/Import可能
- ログ管理
- 管理画面にて各コンポーネントを集中管理
- V6100（HSM対応）は、スマートカード認証をサポート

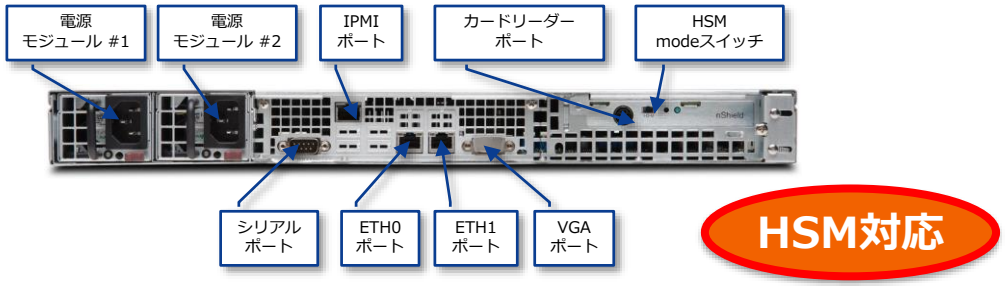




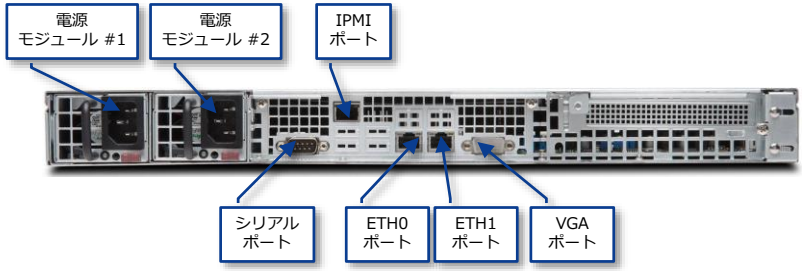
FIPS tamper evident stickers

フロントベゼル無し

V6100/V6000 前面



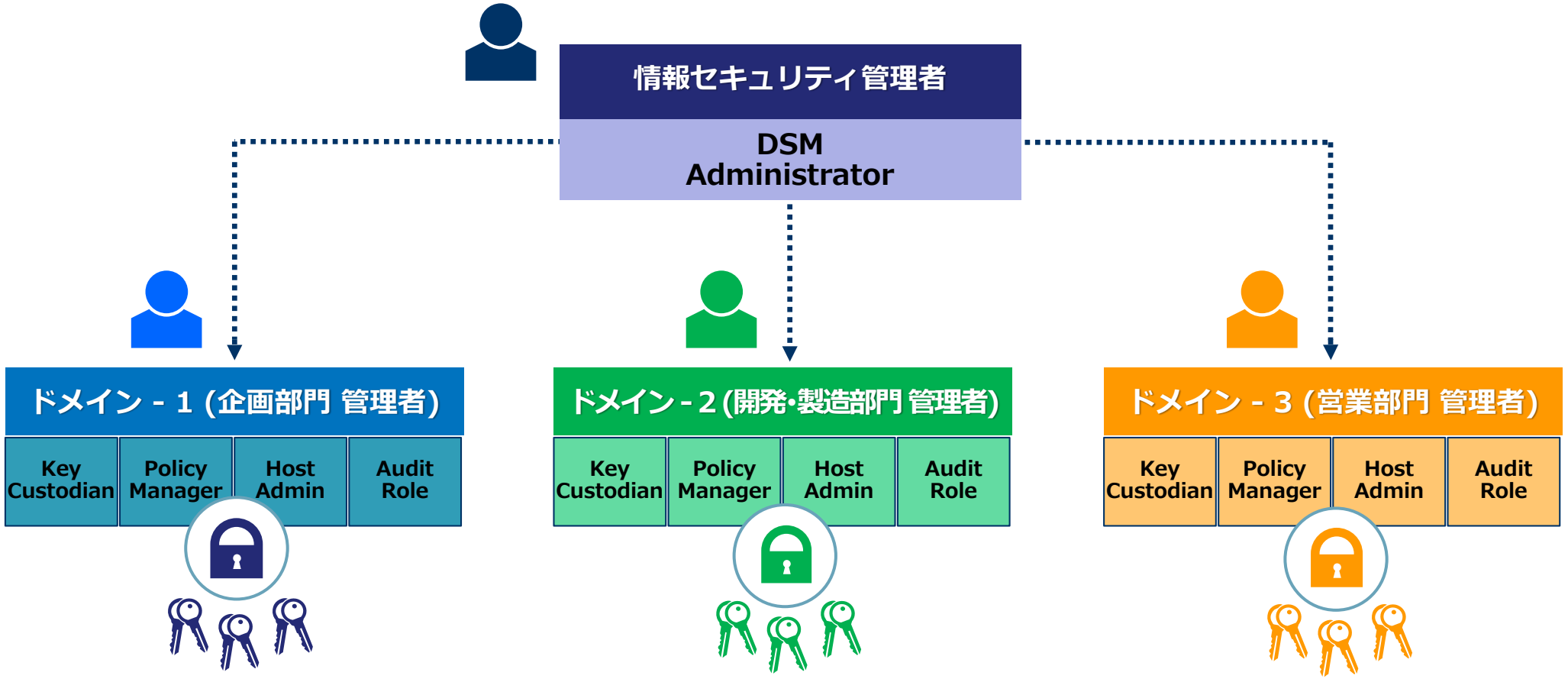
V6100 (HSM搭載) 背面



V6000 背面

鍵管理サーバーのドメイン構成

DSMは2階層になっており、トップレベルとその下に管理部門単位のドメインが存在します。
各ドメイン単位に管理者を割り当て、ドメイン管理者はドメイン内部で個々に対象サーバーの登録や鍵の作成、ポリシーなどの設定を行うことができます。



* VDSM60L3、VDSM60L2、VDSM60L1 モデルは、1,000ドメインまで設定できます。
* V25DSM60L2、V25DSM60L1 モデルは、2ドメインまで設定できます。

透過暗号のコンポーネント

■ **システム構成**
- 鍵管理サーバー
- 透過暗号エージェントソフトウェア

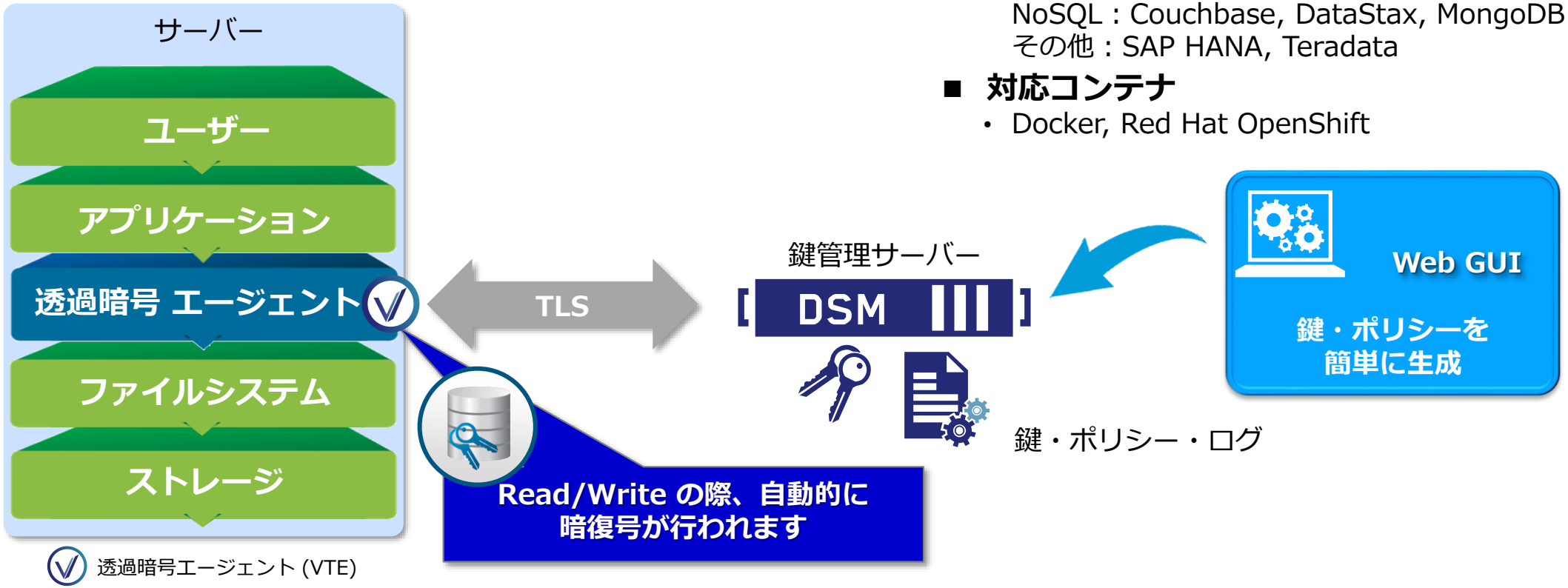
■ **対応プラットフォーム**
- Windows Server
- Red Hat Enterprise Linux
- SuSE Linux Enterprise Server
- Ubuntu
- IBM AIX

■ **対応データベース**
- IBM DB2, MySQL, Oracle, SQL Server, Sybase 他

■ **対応アプリケーション**
- Microsoft, Documentum, SAP, SharePoint, カスタムアプリケーション 他

■ **対応ビッグデータ**
- Hadoop：Cloudera, Hortonworks, IBM
  NoSQL：Couchbase, DataStax, MongoDB
  その他：SAP HANA, Teradata

■ **対応コンテナ**
- Docker, Red Hat OpenShift



透過暗号の機能・特徴

■ **機能・特徴**

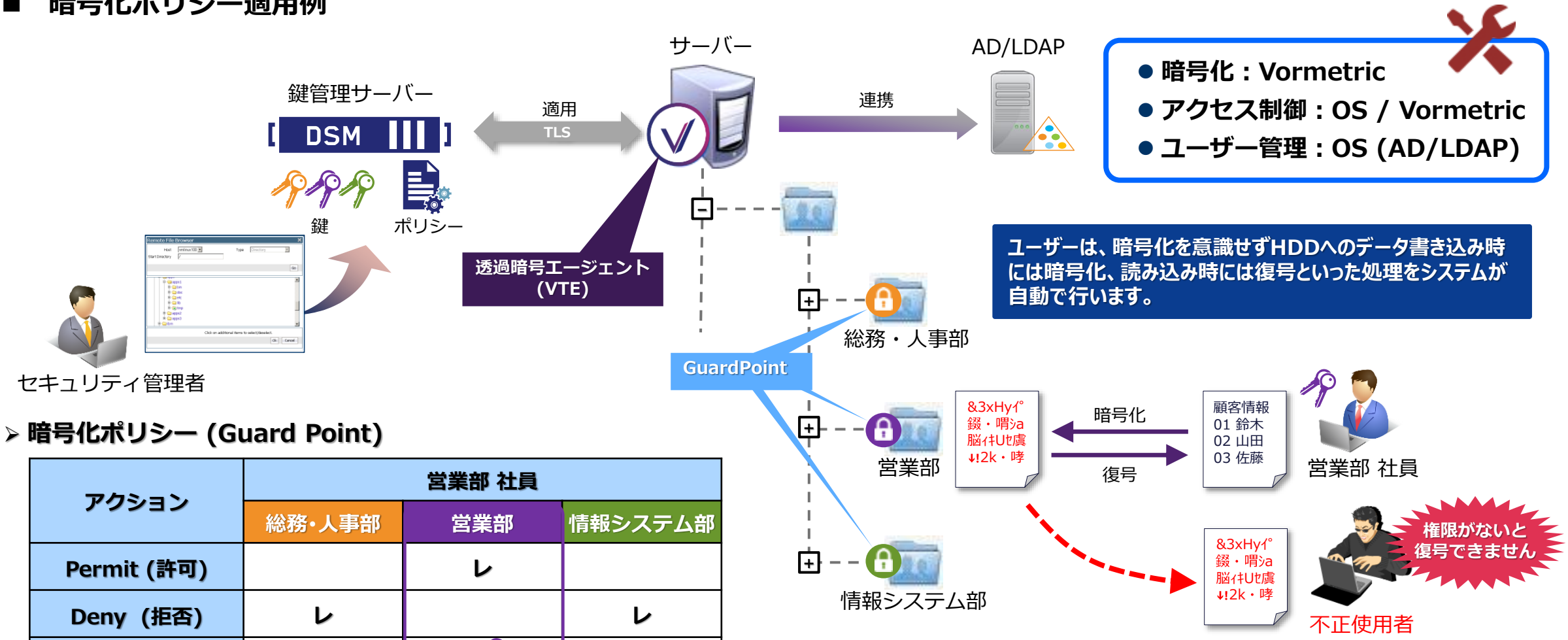
- クライアントPCに特別なソフトウェアは必要ありません
- 既存ファイルやデータベース、アプリケーションの変更は不要です
- ユーザーやシステムに対して自動的に暗復号が行えます
- ユーザーはパスワード管理が不要です
- 構造化データと非構造化データを暗号化できます (ファイルの種類を問いません)
- 「いつ」「だれが」「なにを」といった操作をログに記録します
- AES-NI（Advanced Encryption standard New Instruction）搭載のサーバーでは、暗復号を高速に行えます

AES-NI 搭載

＊AES-NI (Advanced Encryption Standard New Instructions)
暗復号を高速に実行するための拡張命令セット。 (インテル Xeon 5600番台からサポート)

透過暗号による暗号化 (構造化/非構造化データ)

■ 暗号化ポリシー適用例



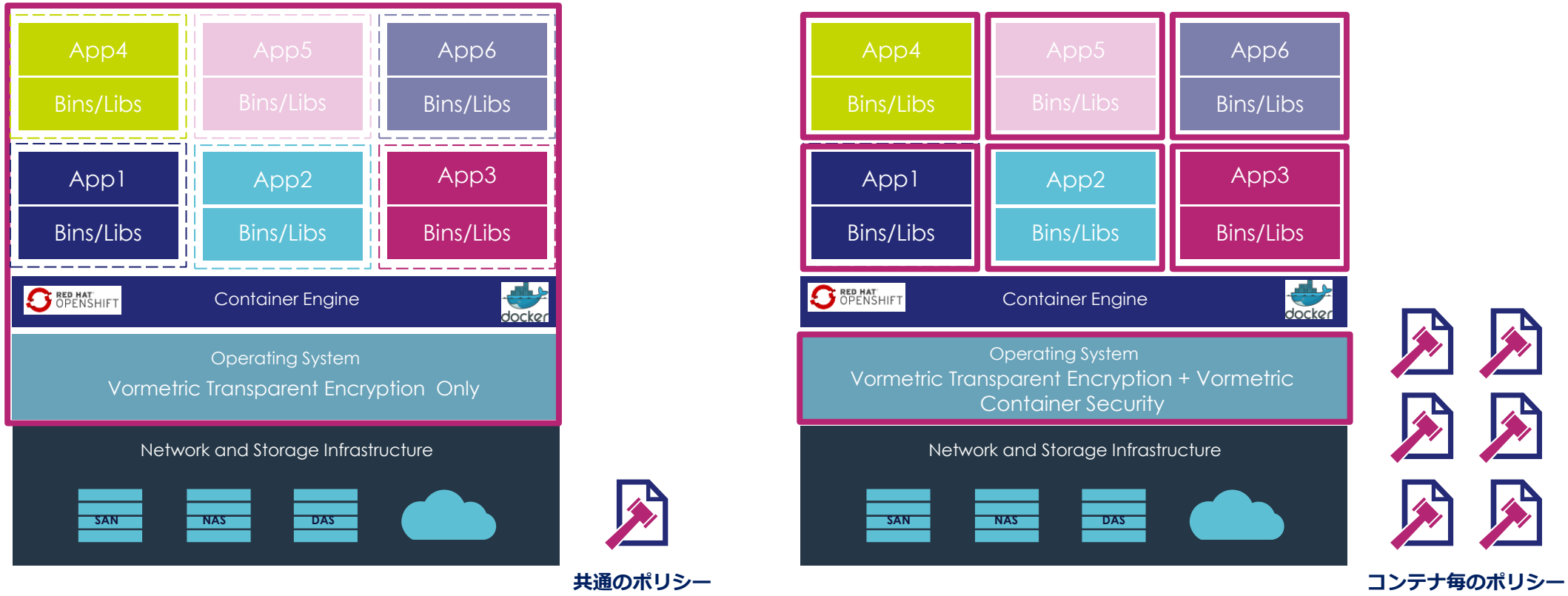
➢ 暗号化ポリシー (Guard Point)

アクション	営業部 社員		
	総務・人事部	営業部	情報システム部
Permit (許可)		レ	
Deny (拒否)	レ		レ
Apply Key (鍵)			
Audit (監査ログ)	レ	レ	レ

コンテナの暗号化 (透過暗号：オプション機能)

■ **機能・特徴**

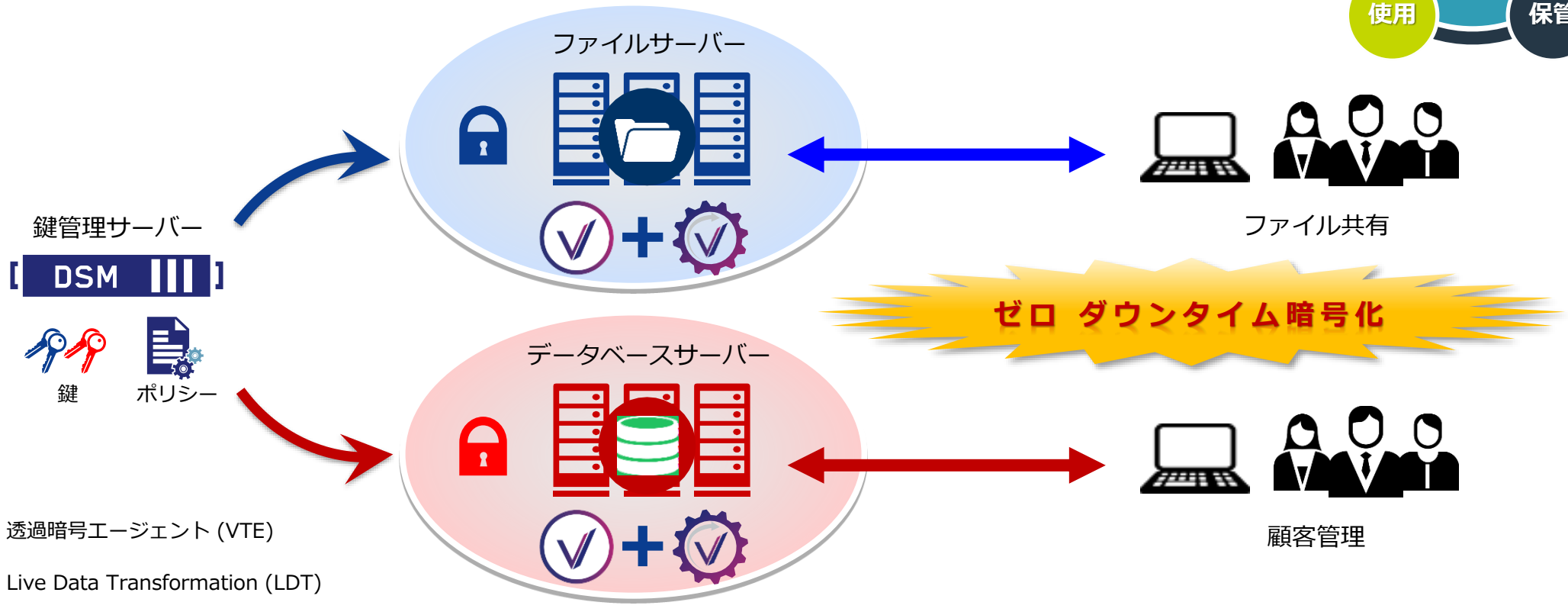
- アプリケーション、コンテナ、インフラストラクチャの変更は不要です
- コンテナ内の特定のユーザー、プロセス、リソースセットに基づいてポリシーを設定可能です
- アクセスログをコンテナ単位で出力できます



保存データの自動暗号・Rekey (透過暗号：オプション機能)

■ **機能・特徴**

- Live Data Transformation (LDT) は、オンライン稼働中でもデータの暗号化が可能です
- 定期的に暗号鍵を変更する必要があるコンプライアンス要件を満たします
- オンライン状態のままで鍵の変更によるデータ再暗号化が可能です
- サービス利用者への影響がないよう、CPUリソースをスケジューリングできます



検証用モードによるプロセス洗い出し (透過暗号 標準機能)

業務ソフトやデータベースに対して透過暗号を導入する場合は、事前に対象プロセスの洗い出しが必要です。
その対象プロセスを洗い出すために、「Learn Mode (検証用モード)」が用意されています。

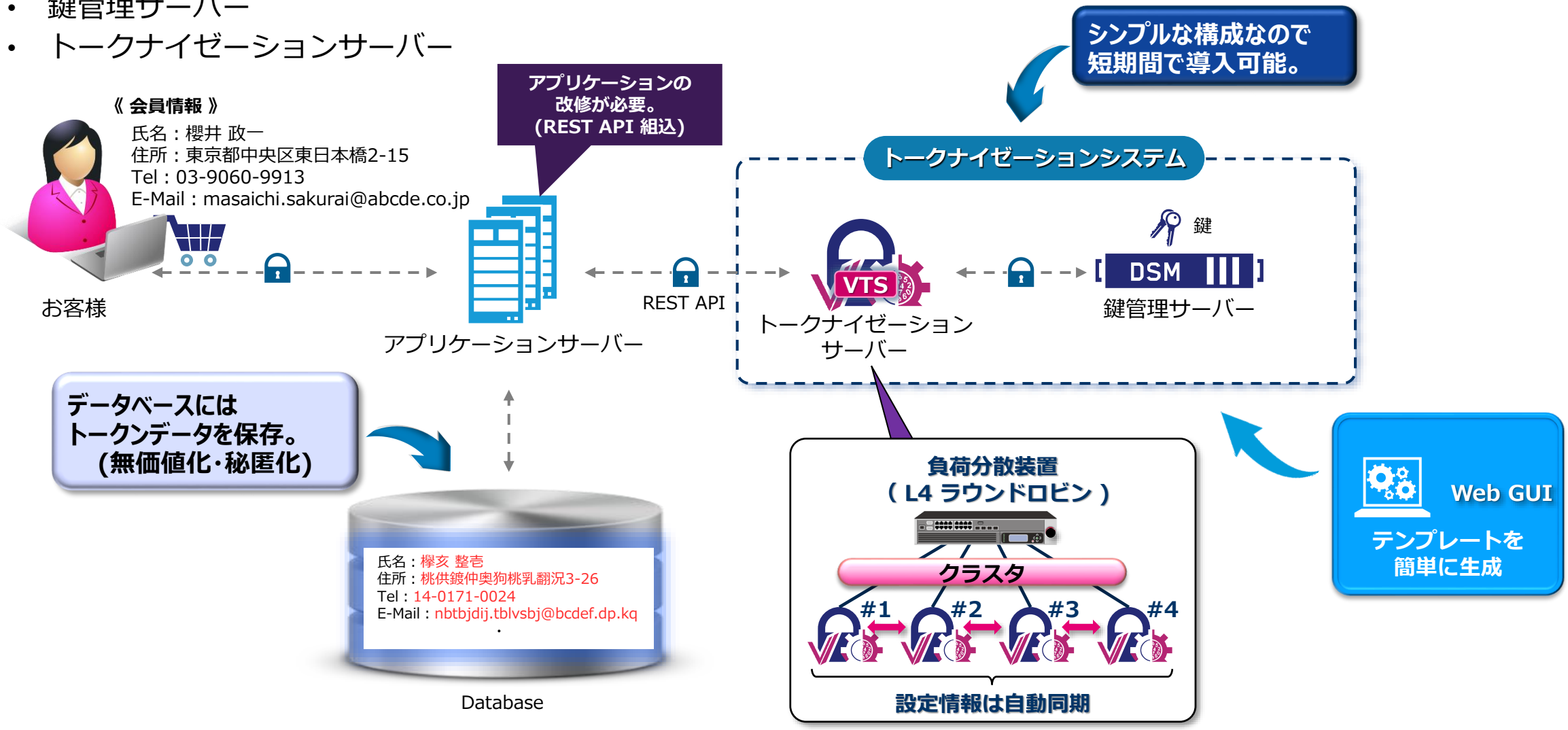
注)「Learn Mode」を適用している間は、対象ディレクトリーのポリシーが ”Deny” であってもアクセス可能です。

管理画面のポリシー設定にて、「Learn Mode」のチェックボックスをチェックします。

トークナイゼーションのコンポーネント

■ **システム構成**

- 鍵管理サーバー
- トークナイゼーションサーバー



トークナイゼーションの機能・特徴

■ 機能・特徴

- トークナイズ/デトークナイズのテンプレートを生成します
- 重要データの無価値化・秘匿化が行えます
- 桁数やデータ形式を維持した高度な暗号化が行えます
- データ長の最大は128kiB (131.072Kbytes) です
- カード番号や電子メールアドレスなどの英数字に加え、住所や氏名などのマルチバイト文字にも対応しています
- 復元する際は指定した桁数をマスキングできます
- RESTful API で連携します
- 高パフォーマンス (単体エンジン性能：約30万トークン/秒)
- クラスタ構成による容易なスケールアップで、高可用性を実現します (最大48台)

■ トークナイゼーションサーバーの仕様

- 仮想アプライアンス (ISO / OVA ファイル) で提供しています
  - ＊ Azure, AWS, GCP にも対応

《 システム要件 》
- CPU 4コア 以上
- RAM 24GB 以上
- HDD 100GB 以上

＊ Web GUI client が利用できる環境が必要になります。

【 原本データ】

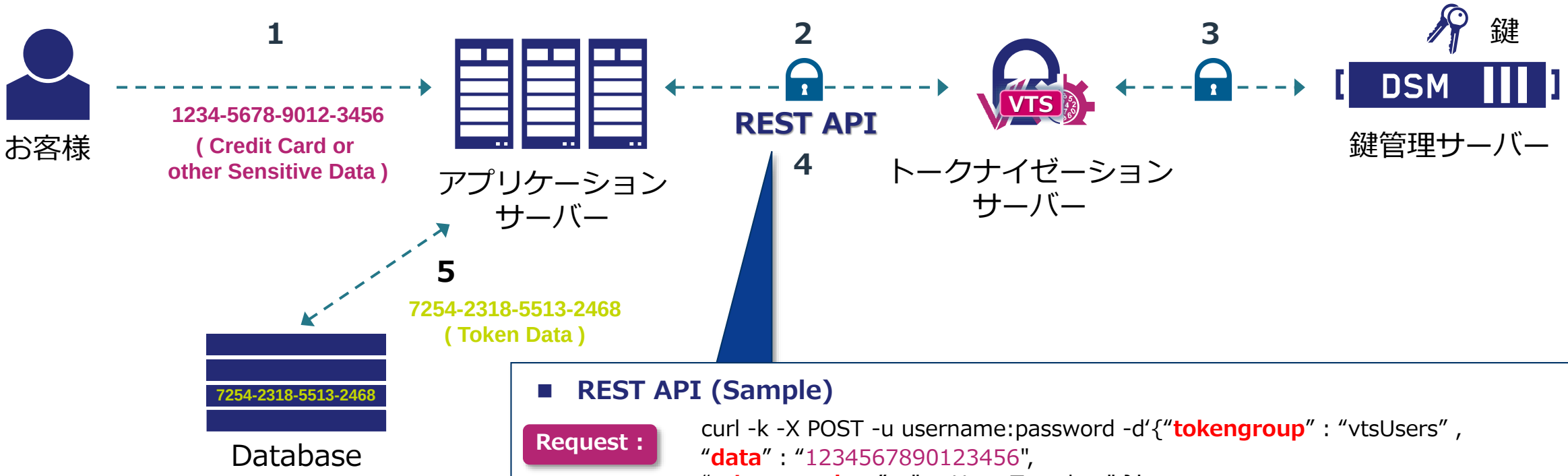
ID	氏名	住所	Tel	E-Mail
1	櫻井 政一	東京都中央区東日本橋2-15	03-9060-9913	masaichi.sakurai@abcde.co.jp
2	宮地 隆一	千葉県市原市山木2-18	04-0098-4336	ryuuichi.miyaji@fghij.co.jp
3	山脇 茂	神奈川県平塚市虹ケ浜4-13-15	046-197-8241	shigeru.yamawaki@klmno.co.jp

トークナイズ

【 トークンデータ】

ID	氏名	住所	Tel	E-Mail
1	欅亥 整壱	桃供鍍仲奥狗桃乳翻況3-26	14-0171-0024	nbtbjdij.tblvsbj@bcdef.dp.kq
2	弓弛 竜壱	占蓉肩師厳師惨黙3-29	15-1109-5447	szvvjdij.njzbkj@ghijk.dp.kq
3	惨惑 妄	秦那戦肩弊栂師廿コ瀬5-24-26	157-208-9352	ibsvlp.tfljnpup@qrstuv.dp.kq

トークナイゼーションによる暗号化



■ **REST API (Sample)**

Request :

curl -k -X POST -u username:password -d'{"**tokengroup**" : "vtsUsers" ,
"**data**" : "1234567890123456",
"**tokentemplate**" : "vtsUsersTemplate" }'
https://192.168.1.1/vts/rest/v2.0/tokenize (デトークナイズ時は detokenize)
※ 認証情報と下記送信データをPOSTする。

[リクエストパラメータ]

① **トークングループ　　：鍵管理サーバーで生成した鍵を指定**
② **送信データ　　：原本データ (デトークナイズ時はトークンデータ)**
③ **トークンテンプレート　：変換形式などを指定**

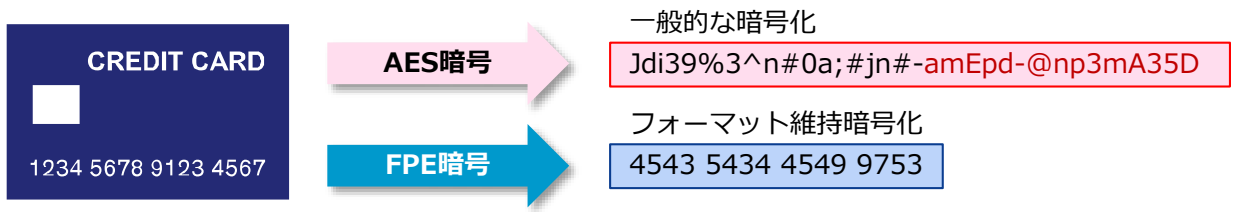
Response :

{"token":"1234-5678-9012-3456","status":"Succeed"}

トークナイゼーションのアルゴリズム

■ FPEとは

- Format-preserving encryption の略称
- 桁数/データ形式を維持した暗号技術
- NIST Special Publication 800-38G にて承認
  (https://dx.doi.org/10.6028/NIST.SP.800-38G)



※ 既存データベースのカラム変更を行う必要がありません。

■ アルゴリズム

No	アルゴリズム	PCI の分類	特徴
1	FPEモード (FF3)	暗号化(RC)	暗号鍵を用いたFPE FF3モードでトークナイゼーションを実行。
2	FPEモード (FF1)	暗号化(RC)	暗号鍵を用いたFPE FF1モードでトークナイゼーションを実行。
3	Randomモード	非暗号化(RN)	VTSで最初に指定する暗号鍵を用いて独自のアルゴリズムを生成し、このアルゴリズムを用いてトークナイゼーションを実行。

＊ アルゴリズムは、PCI SSC「Tokenization Product Security Guidelines Version: 1.0」に準拠
＊ Randomはメーカー独自仕様
＊ 複数のアルゴリズムを併用できます。

■ アルゴリズムの特徴

- FPE (FF3、FF1)　：半角英数字だけでなく、日本語や中国語、韓国語などのダブルバイト文字も変換可能
- Randomモード　：半角英数字だけ変換可能

個人データのトークナイズ / デトークナイズ (例)

	原本	トークナイズ (変換)	デトークナイズ (復元)
名前 (漢字)	山田　太郎	裉洁　犴櫮	山田　太郎
名前 (カナ)	ヤマダ　タロウ	ダヤヮ　ツマズ	ヤマダ　タロウ
性別	男	蝔	男
生年月日	2016/04/01	1060/11/05	2016/04/01
メールアドレス	yamada.taro@canon-mj.co.jp	tkptezbvmgisjosc-ataaoremad	yamada.taro@canon-mj.co.jp
クレジットカード番号	1111-2222-3333-4444	4374-3447-1911-4152	****-****-****-4444
郵便番号	140-8526	856-7806	マスキング 140-8526
都道府県	東京都	鵘軑拗	東京都
地名・番地等	港区港南２－１６－６	倨鑣繄翍翬澀齤楏瘧毗	港区港南２－１６－６
建物名・室番号等	キヤノンＳタワー	洞钳罋褒芊屈胹鉢	キヤノンＳタワー
法人名・団体名	キヤノンマーケティングジャパン株式会社	鵘陯鷺淈尧旄劃吒岖惦欻歧屘酎谇鵁諀咐	キヤノンマーケティングジャパン株式会社
電話番号	03-6701-3477	71-8670-3601	03-6701-3477

無価値化・秘匿化

価値あるデータに復元

フォーマット維持暗号化 (FPE : Format Preserving Encryption)

アプリケーション暗号のコンポーネント

■ **システム構成**

- 鍵管理サーバー
- アプリケーション暗号エージェントソフトウェア

■ **サポートOS、言語**

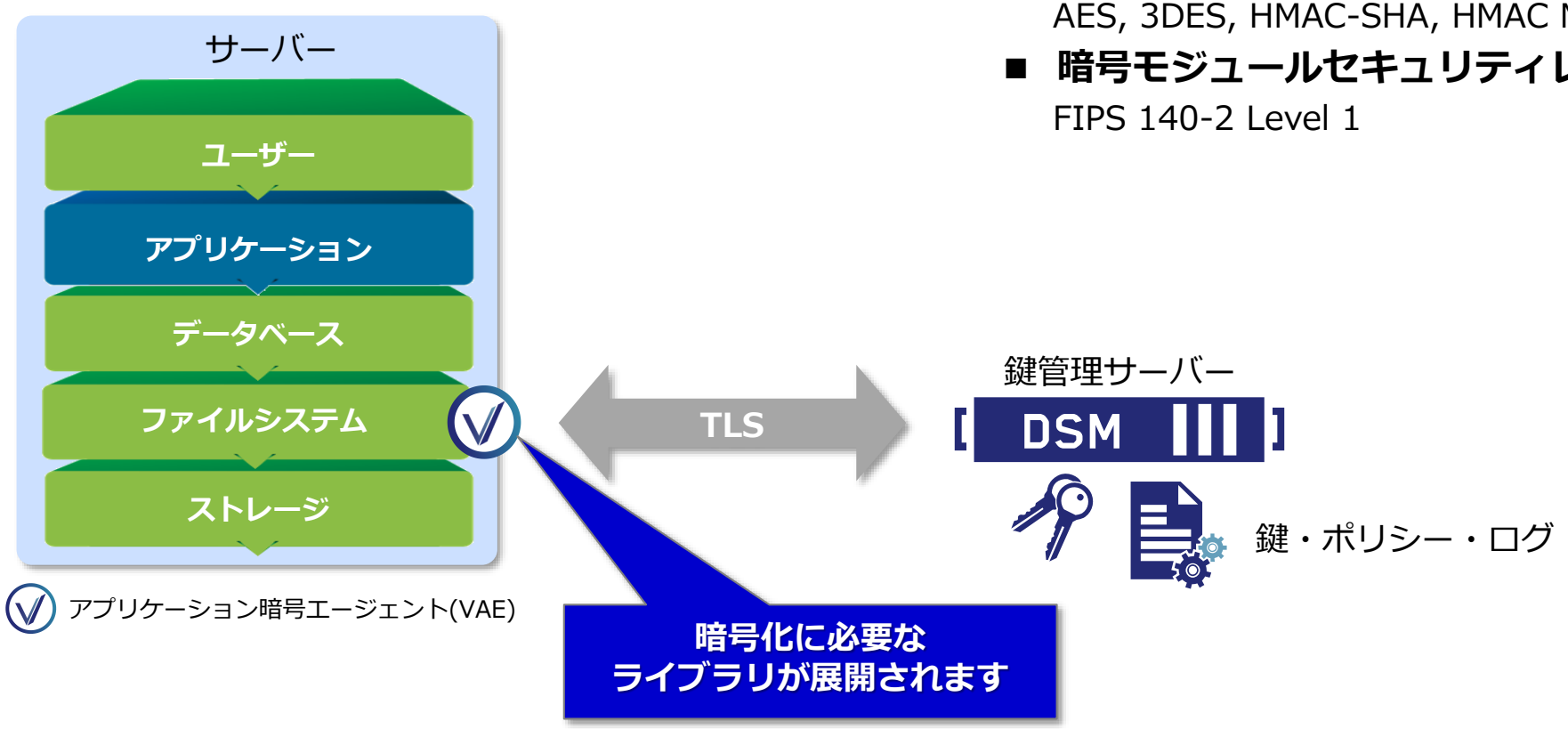
Windows Server：C, .NET, Oracle/Sun JDK
Linux：C, Oracle/Sun JDK
＊ PKCS #11 規格に準拠しています。

■ **暗号アルゴリズム**

AES, 3DES, HMAC-SHA, HMAC MD5, RSA, FPE

■ **暗号モジュールセキュリティレベル**

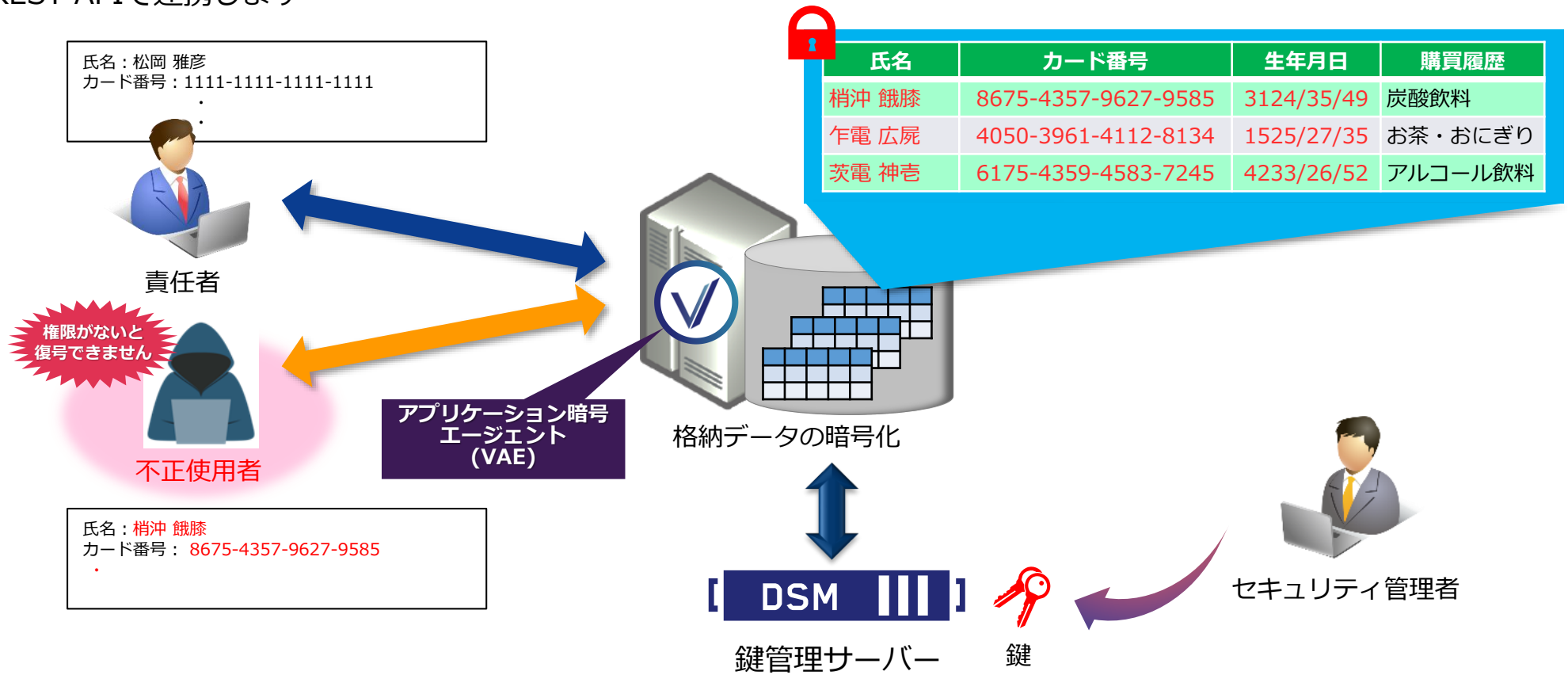
FIPS 140-2 Level 1



アプリケーション暗号の機能・特徴

■ **機能・特徴**

- 独自開発アプリケーションの鍵管理
  - ➢ 様々なアプリケーションに対する列(カラム)単位の暗号化が行えます
  - ➢ PKCS#11ライブラリでの開発できます
  - ➢ REST APIで連携します



他社暗号化製品の鍵管理のコンポーネント

■ **機能・特徴**

- 鍵管理サーバー
- TDE機能を備えたデータベース製品の暗号鍵管理 (VKM)
- 他社暗号化製品の鍵管理 (KMIP)

鍵管理サーバー
(DSM)

他社データベース暗号化製品の鍵管理 (VKM)

- データベース付属TDEの暗号鍵管理
- Oracle、Microsoft SQL Server 対応

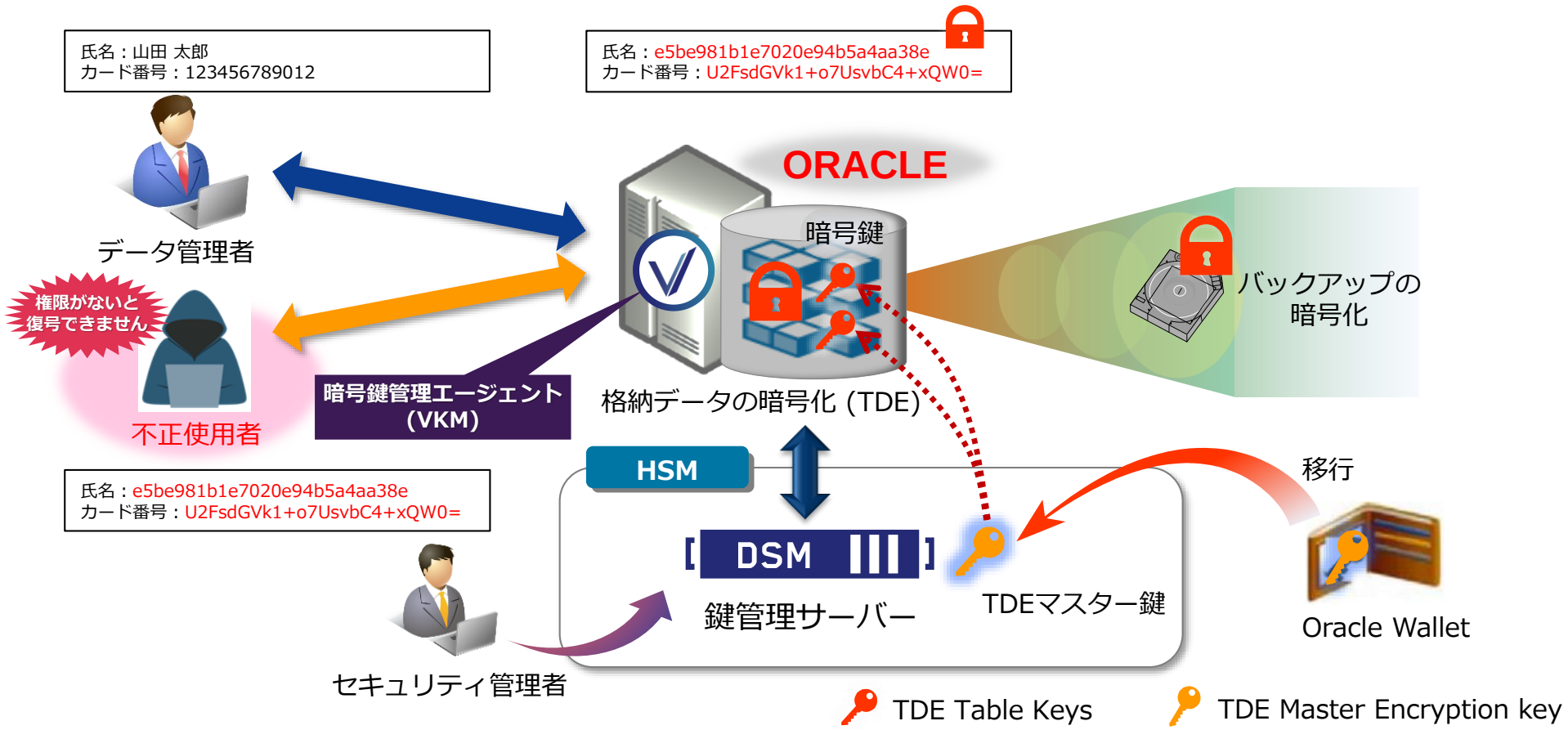
他社暗号化製品の鍵管理 (KMIP)

- 仮想マシンの暗号鍵管理 (VMware vSphere 6.5 以上)
- ストレージデバイスの暗号鍵管理

Oracle TDE, MS SQL Server TDEの機能・特徴

■ **機能・特徴**

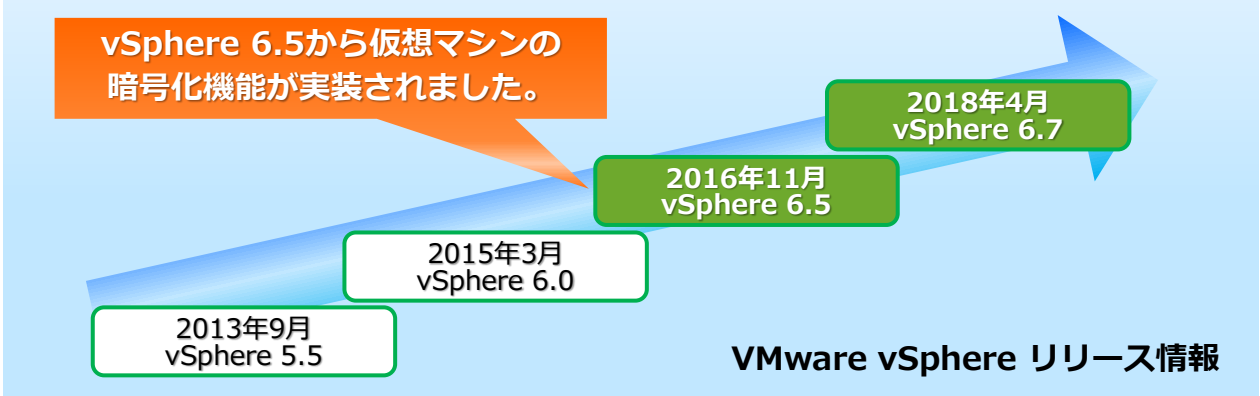
- Oracle TDE Master Encryption Key (MEK) を、ハードウェアセキュリティモジュール (HSM) として機能するDSMに格納できます
- Microsoft SQL Server の TDE database encryption key (DEK) は、鍵管理サーバーに保管された非対称キーで暗号化します
- 鍵管理サーバーは、KMIPプロトコルをサポートしています

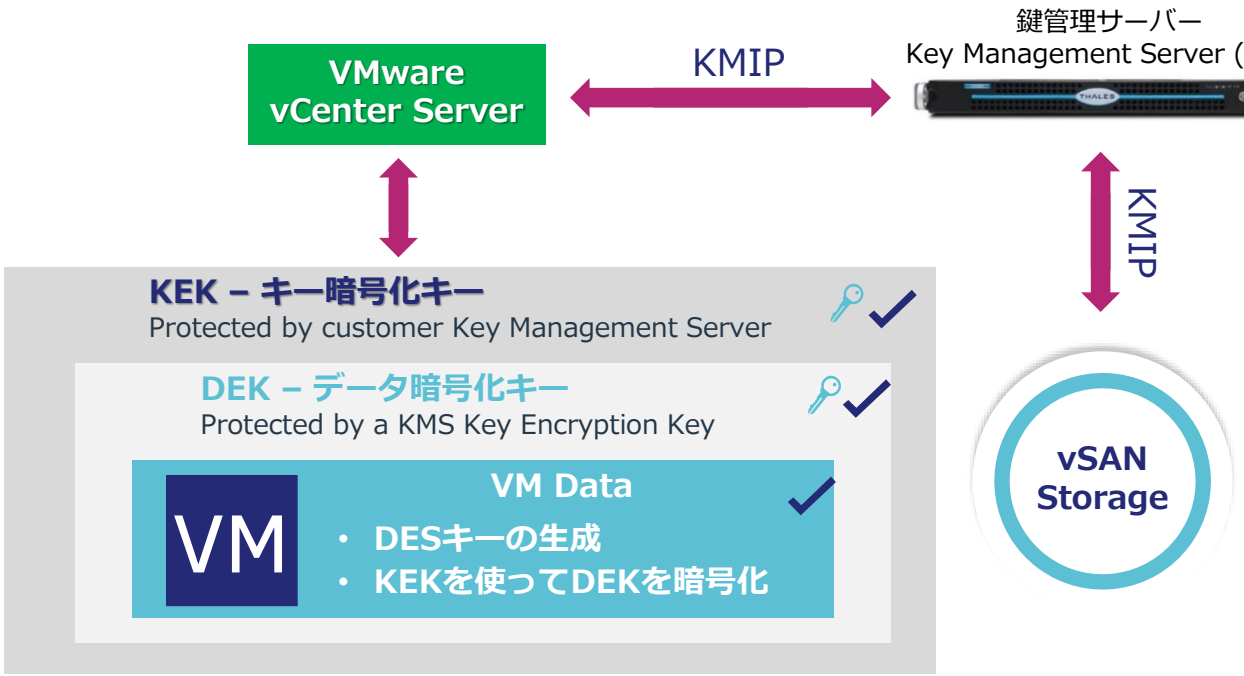


仮想マシン暗号化の機能・特徴

■ **機能・特徴**

- 暗号鍵は鍵管理サーバー (KMS) に保管
- 主クライアントはVMware vCenter Serverになります
- ESXiカーネルレベルで暗復号できます
- ゲストOS毎に暗号化できます
- インテルAES-NIを利用すると、暗復号のオーバーヘッドを抑えられます
- スナップショット/構成ファイルも暗号化できます
- vMotionに対応しています
- 高度な暗号鍵(AES 256)を使用できます
- 鍵管理が容易です
- KMIPに準拠しています



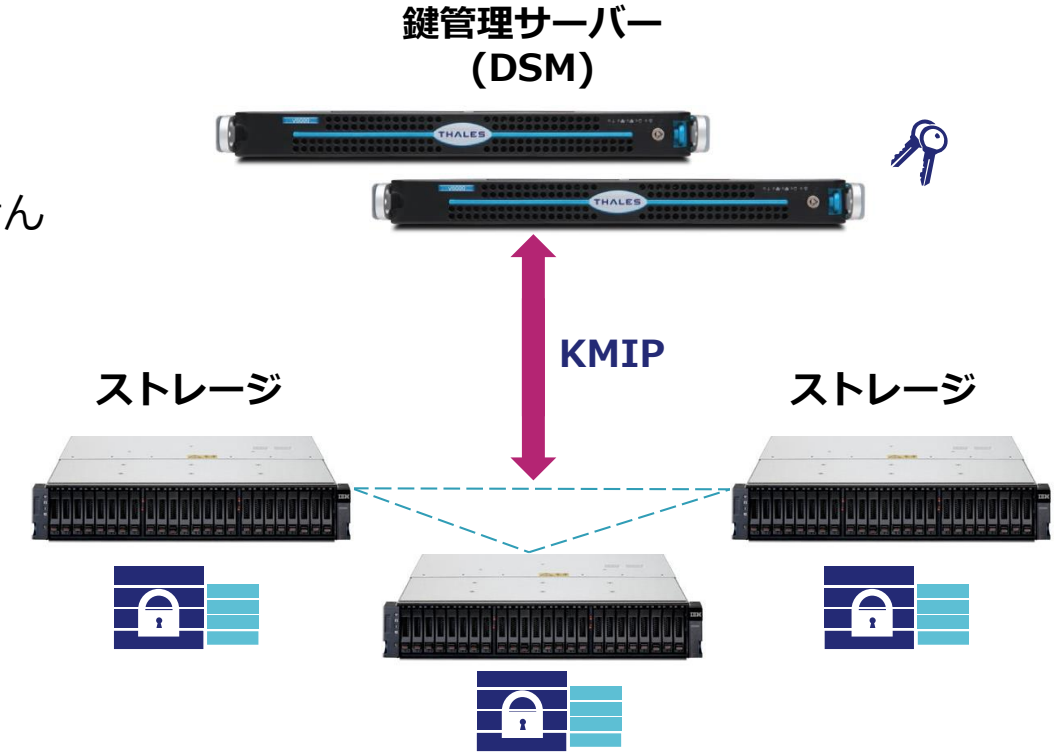


ストレージ暗号化の機能・特徴

■ **機能・特徴**

Data at Rest Encryption

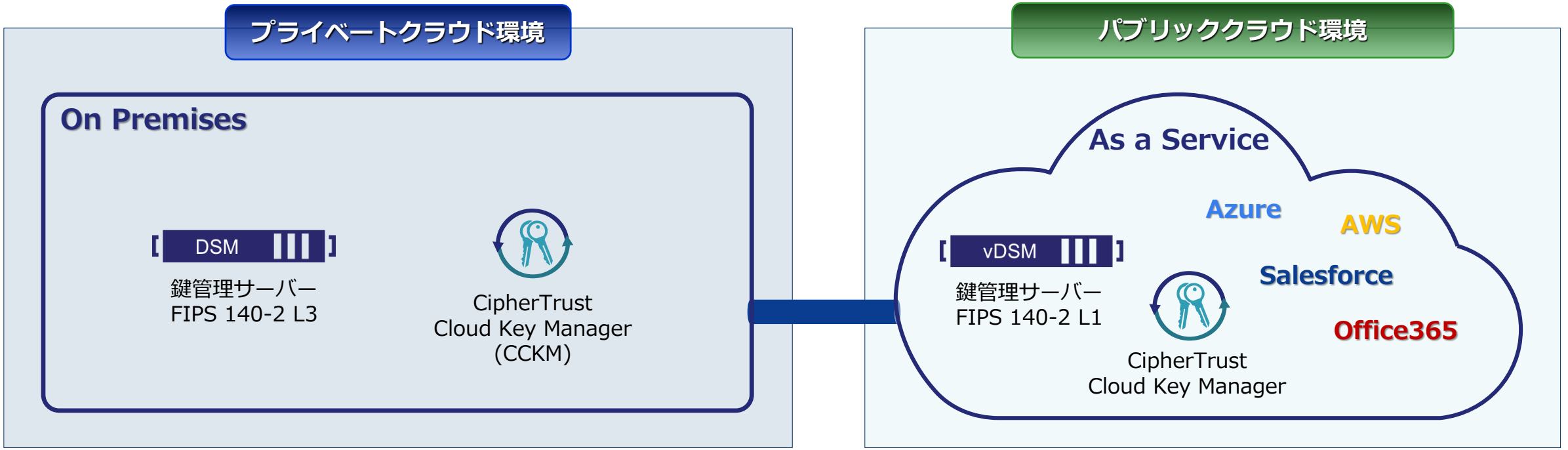
- コントローラベースの暗号化を実現します
- ユーザーの操作性は、これまでと変わりありません
- 暗号鍵は外部の鍵管理サーバーでセキュアに保管します
- 暗号アルゴリズム (AES) を使用します
- FIPS 140-2 Level 1 に準拠しています
- 暗号化を有効にしてもパフォーマンスの劣化等はありません
- ストレージシステムから取り出されたディスクの中身は見れません



クラウド暗号化サービス鍵管理のコンポーネント

■ **システム構成**
- 鍵管理サーバー
- CipherTrust Cloud Key Manager (CCKM)

■ **サポート対象のパブリッククラウドサービス**
- Microsoft Azure
  前提条件：Microsoft Azure Key Vault
- Amazon Web Services
  前提条件：AWS Key Management Service
- Salesforce
  前提条件：Shield Platform Encryption



＊ 鍵管理サーバーとCCKMは、オンプレミス/クラウドどちらの環境にも構築できます。

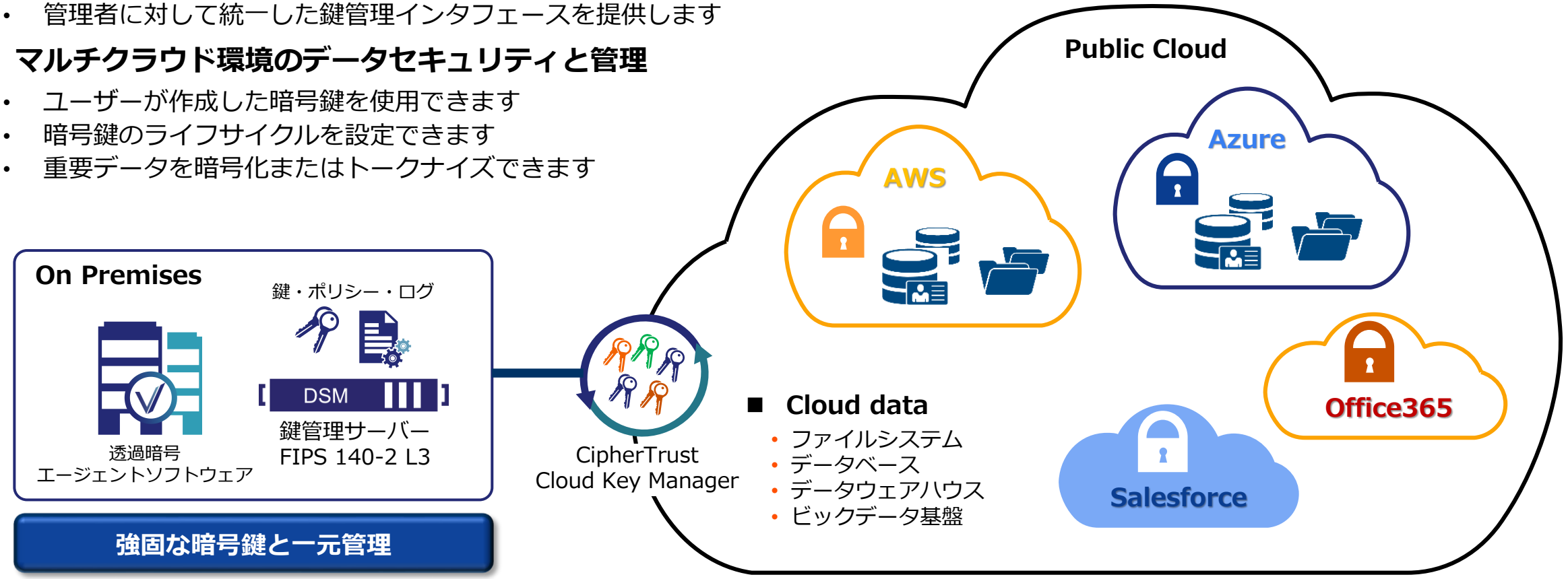
クラウド暗号化サービス鍵管理の機能・特徴

■ 機能・特徴

- クラウド環境にデータを保存する際に暗号化します
- 暗号鍵を自社で保管することにより、クラウド環境でも安全にデータを保護できます
- オンプレミスとクラウド更にはハイブリット環境で、高度な暗号化と鍵管理を実現します
- 複数のクラウドサービスの暗号鍵を一元管理できます
- 管理者に対して統一した鍵管理インタフェースを提供します

■ マルチクラウド環境のデータセキュリティと管理

- ユーザーが作成した暗号鍵を使用できます
- 暗号鍵のライフサイクルを設定できます
- 重要データを暗号化またはトークナイズできます



Vormetric セキュリティー・インテリジェンス

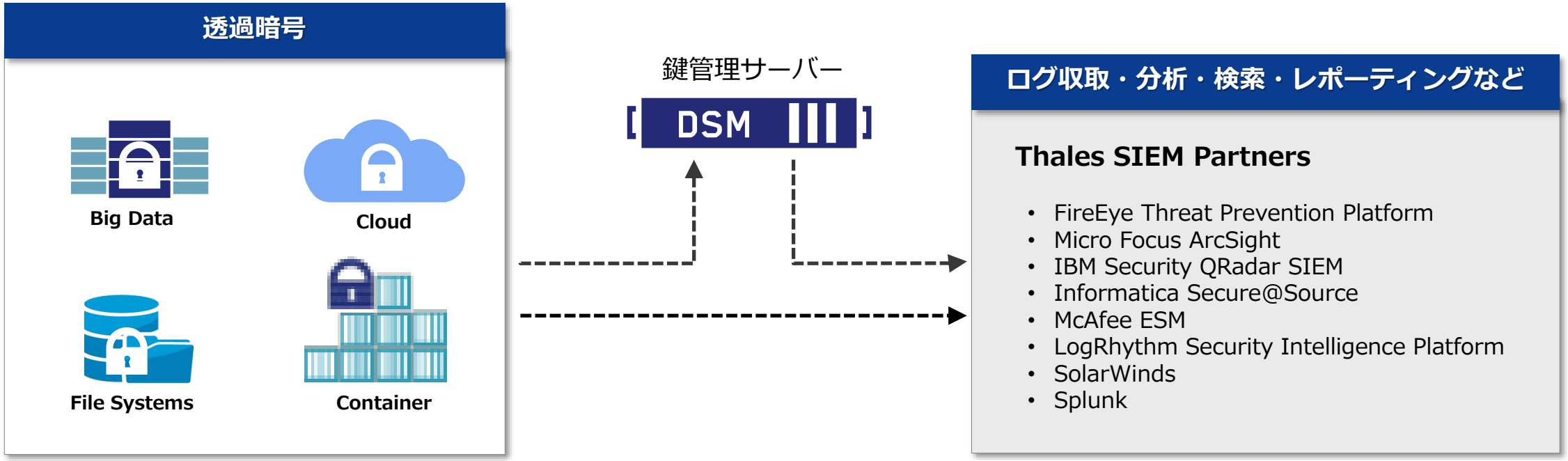
■ 鍵管理サーバーがサポートしているログフォーマット形式

- Plain Message
- Common Event Format (CEF)
- RFC5424
- Log Event Extended Format (LEEF)

■ ログレベル

DEBUG	デバッグ情報
INFO	情報
WARN	警告
ERROR	エラー
FATAL	致命的なエラー

＊ DEBUG > INFO > WARN > ERROR > FATAL



透過暗号によるアクセスログ (ポリシー：許可)

「企画部」フォルダに対し、以下ポリシーを設定（ **Apply Key, Audit, Permit** ）

Select	Order	Resource	User	Process	Action	Effect
☐	1		kikaku-group			Apply Key, Audit, Permit
☐	2		gijutu-group			Audit, Permit
☐	3		eigyou-group			Audit, Deny
☐	4					Audit, Deny

「企画部」グループ内のユーザーにて、「企画部」フォルダへのアクセスと暗復号を許可

→ ポリシーの「1番目」にマッチし、**暗復号可能**

Feb 13 16:23:41 — **いつ：2月13日 16時23分41秒**

Policy[kikaku] — **ポリシー名：kikaku**

User[abe¥Domain Users,企画部...¥CANON-MJ,canon-mj.local] — **だれが：阿部 (企画部)**

Process[C:¥Program Files¥Windows NT¥Accessories¥wordpad.exe]

Action[read_file] — **何を：ワードパッド (WordPad) で読み込み**

Res[C¥企画部¥sample.txt] — **どのファイルに対して：企画部フォルダーのsample.txt**

Key[kikaku-Key01] — **カギ名：kikaku-Key01**

Effect[PERMIT Code (1M)] — **適用されたポリシー：1番目のポリシーにマッチ (許可)**

透過暗号によるアクセスログ (ポリシー：拒否)

「企画部」フォルダに対し、以下ポリシーを設定（ **Audit, Deny** ）

Select	Order	Resource	User	Process	Action	Effect
☐	1		kikaku-group			Apply Key, Audit, Permit
☐	2		gijutu-group			Audit, Permit
☐	3		eigyou-group			Audit, Deny
☐	4					Audit, Deny

サーバーへの不正アクセスを早期発見

「営業部」グループ内のユーザーにて、「企画部」フォルダへのアクセスを拒否

→ ポリシーの「3番目」にマッチし、**Deny権限のため、フォルダへのアクセス不可、**

Feb 13 16:39:02 — **いつ：2月13日 16時39分02秒**

Policy[kikaku] — **ポリシー名：kikaku**

User[yamada¥Domain Users,営業部...¥CANON-MJ,canon-mj.local] — **だれが：山田 (営業部)**

Process[C:¥Windows¥explorer.exe] — **何を：エクスプローラー (Explorer) で読み込み**

Action[read_dir]

Res[C:¥企画部¥] — **どのファイルに対して：企画部フォルダー**

Effect[DENIED Code (1U,2U,3M)] — **適用されたポリシー：3番目のポリシーにマッチ (拒否)**

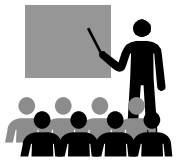
構築サービス・構築ステップ

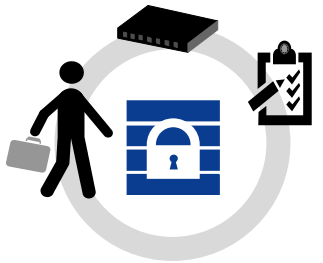
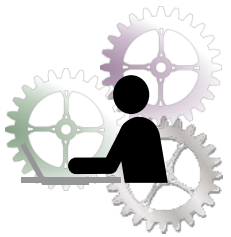
事前検討段階から設計、構築、保守に至るまで一貫したサービスを提供します。
『簡単』『迅速』『既存システムの影響最小限』といった点に軸足を置いた製品です。

評価版貸出

一般的に運用フェーズに持っていくまでに約1ヶ月を要します。

Week 1	Week 2	Week 3	Week 4＋
ご契約・キックオフ	設計	構築・テスト	運用・保守
▪ 目的・ご要件の確認 ▪ 現状環境の確認 ▪ 実装形態の確認 ▪ スケジュールの確認	▪ 構成設計 ▪ システム設計 ▪ 設計レビュー	▪ Vormetric導入 ▪ 初期設定 ▪ カスタム設定 ▪ テスト・チューニング ▪ 管理者向け教育	▪ システム管理・監視 ▪ 継続的なチューニング ▪ バックアップ/リストア 保守開始
プロフェッショナルサービス			保守サービス

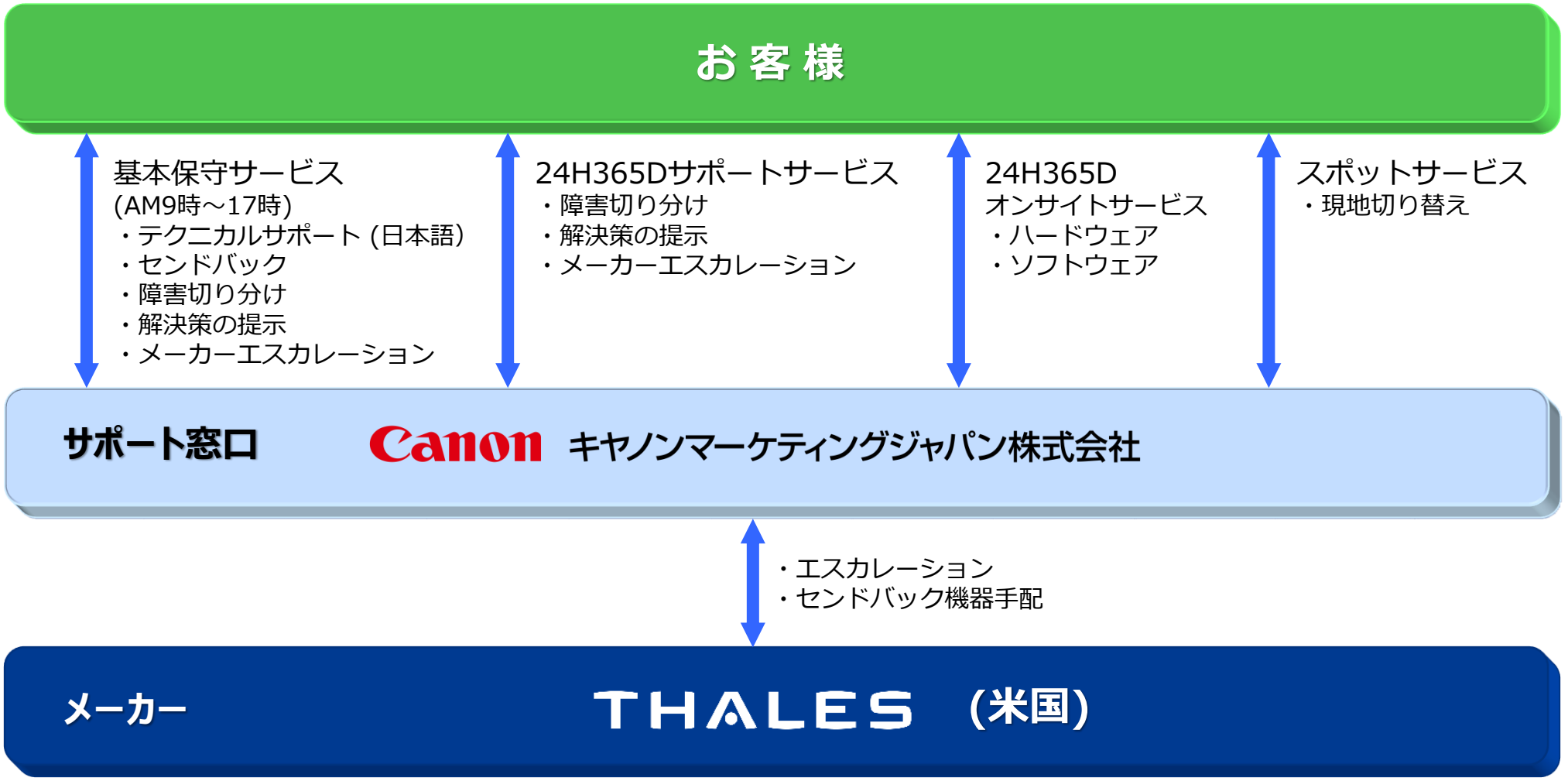


※ 構築サービスをご希望のお客様は、弊社担当営業までお問合せください。

保守サービス・体制のご紹介

■ メーカー保守と連動し、キヤノンマーケティングジャパンが各種サービスの1次窓口を提供します



製品保守サービス (その1)

■ 基本保守サービス

Thales が英語で提供するサービスを、キヤノンマーケティングジャパンが日本語で1次受付します。
また、ハードウェアの障害時にセンドバック手配を代行する国内限定のサポートサービスです。

サポート項目	サポート内容	ご提供条件
テクニカルサポート (日本語)	障害切り分け 解決策の提示 メーカーエスカレーション	• 年間契約となります。 • 弊社営業日9-17時対応となります。 • 初年度契約が必須です。 • 契約更新毎に最大3%の更新料が追加されます（メーカー取り決め）。 • 次年度契約更新を行わなかった場合、修理および取次対応が出来なくなりますのでご注意ください。
センドバック	ハードウェア交換	

■ 24H365Dサポートサービス

基本保守サービスのテクニカルサポートを24時間365日に拡張した国内限定のサービスです。

サポート項目	サポート内容	ご提供条件
テクニカルサポート (日本語)	障害切り分け 解決策の提示 メーカーエスカレーション	• 基本保守サービスの契約が必須です。 • 年間契約となります。 • 基本保守のテクニカルサポートの時間帯を24時間365日に拡張して対応します。 拡張した時間帯の対応は下記の通りです。 ▸ 障害に関する対応のみとなります。 ▸ 弊社にてQAと判断されるお問合せの場合、対応は翌営業日となります。

製品保守サービス (その2)

■ 平日オンサイトサービス

基本保守と併せて平日日中帯のみのオンサイトによる障害復旧サービスです。

サポート項目	サポート内容	ご提供条件
ハードウェア	ハードウェア交換 再構成作業	• 基本保守サービスの契約が必須です。 • 弊社営業日9-17時の対応となります。 • 年間契約となります。 • Thales より、機器交換もしくは再構成が必要と判断された場合、弊社エンジニアによるオンサイトによる復旧対応を実施いたします。
ソフトウェア	再構成作業	

■ 24H365Dオンサイトサービス

24H365Dサポートサービスに加えて、24時間365日のオンサイトによる障害復旧サービスです。

サポート項目	サポート内容	ご提供条件
ハードウェア	ハードウェア交換 再構成作業	• 24H365Dサポートサービスの契約が必須です。 • 年間契約となります。 • Thales より、機器交換もしくは再構成が必要と判断された場合、弊社エンジニアによるオンサイトによる復旧対応を実施いたします。
ソフトウェア	再構成作業	

■ スポットサービス

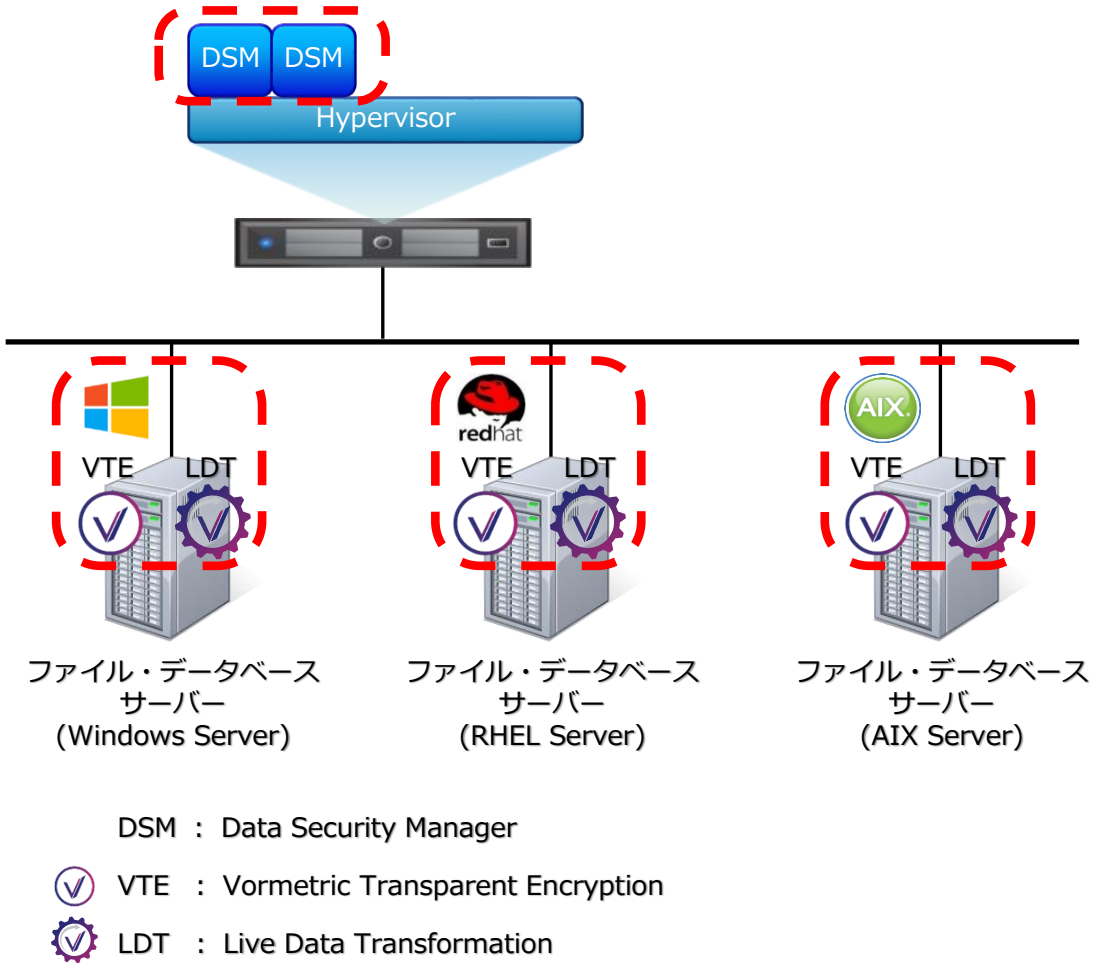
基本保守サービスと併せて弊社が提供するスポットサービスです。

サポート項目	サポート内容	ご提供条件
現地切り替えサービス	ハードウェア交換 再構成作業	• 基本保守サービスの契約が必須です。 • スポット対応となります。

ファイル・データベースの透過暗号 システム構成例

◆ システム構成例

Sample



◆ 製品構成

- Virtual DSM FIPS L1, 6.x Software
  2台
- Transparent Encryption Agent
  3本
- Live Data Transformation for VTE
  3本

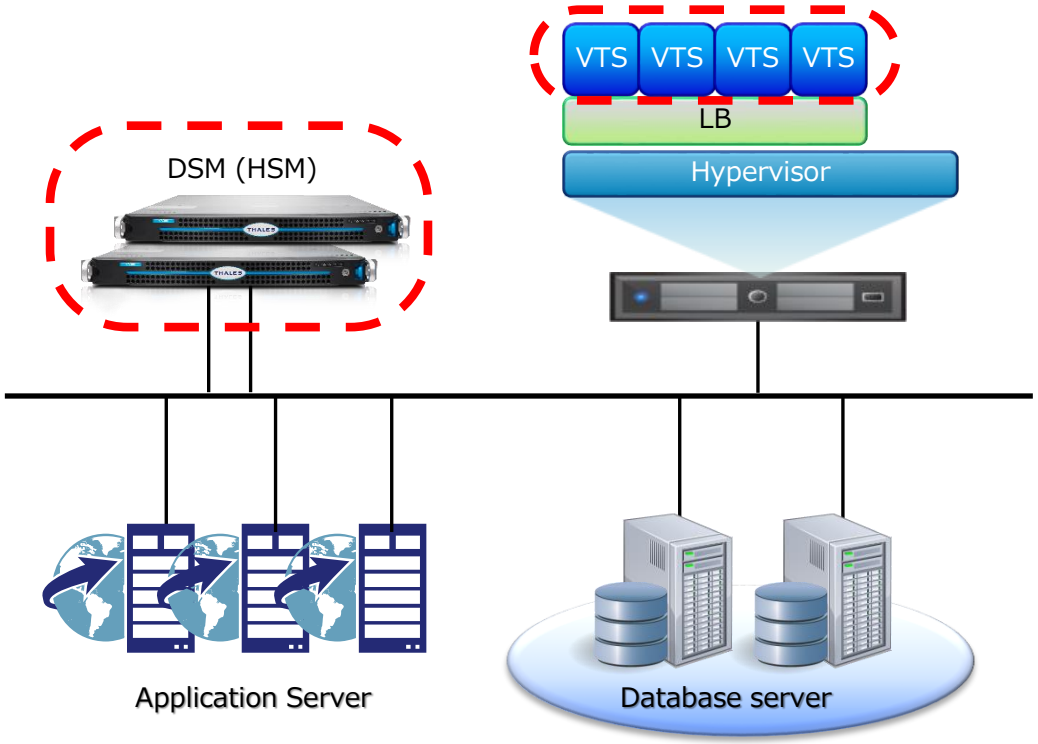
◆ 製品構成価格

営業担当にお問い合わせください。

※ Vormetric Transparent Encryption は、保護対象の
サーバー単位でライセンスをご購入いただくことになります。

トークナイゼーション システム構成例

◆ システム構成例



DSM ： Data Security Manager
VTS ： Vormetric Token Server

※ VTSを2台以上構成する場合は、負荷分散装置(LB)が必要です。

Sample

◆ 製品構成

- Physical DSM V6100 FIPS L3, 6.x Software
  2台
- Client License for Tokenization Server
  3本

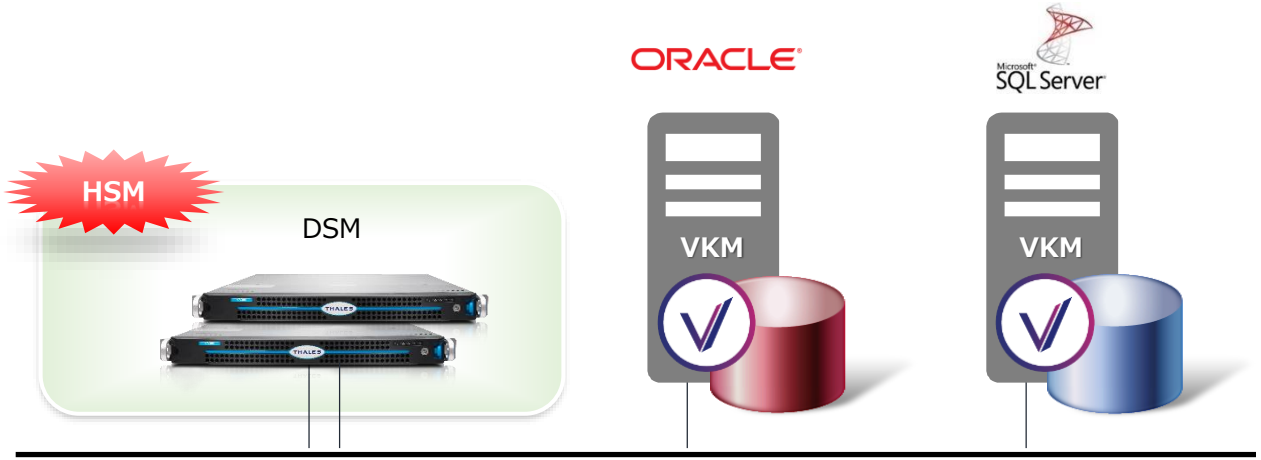
◆ 製品構成価格

営業担当にお問い合わせください。

※ Token Server Client は、データを要求するアプリケーションサーバー単位でライセンスをご購入いただくことになります。

Oracle/MS SQL TDEの鍵管理 システム構成例

◆ システム構成例



Sample

◆ 製品構成

- Physical DSM V6100 FIPS L3, 6.x Software
  2台
- Key Management Client
  2本

◆ 製品構成価格

営業担当にお問い合わせください。

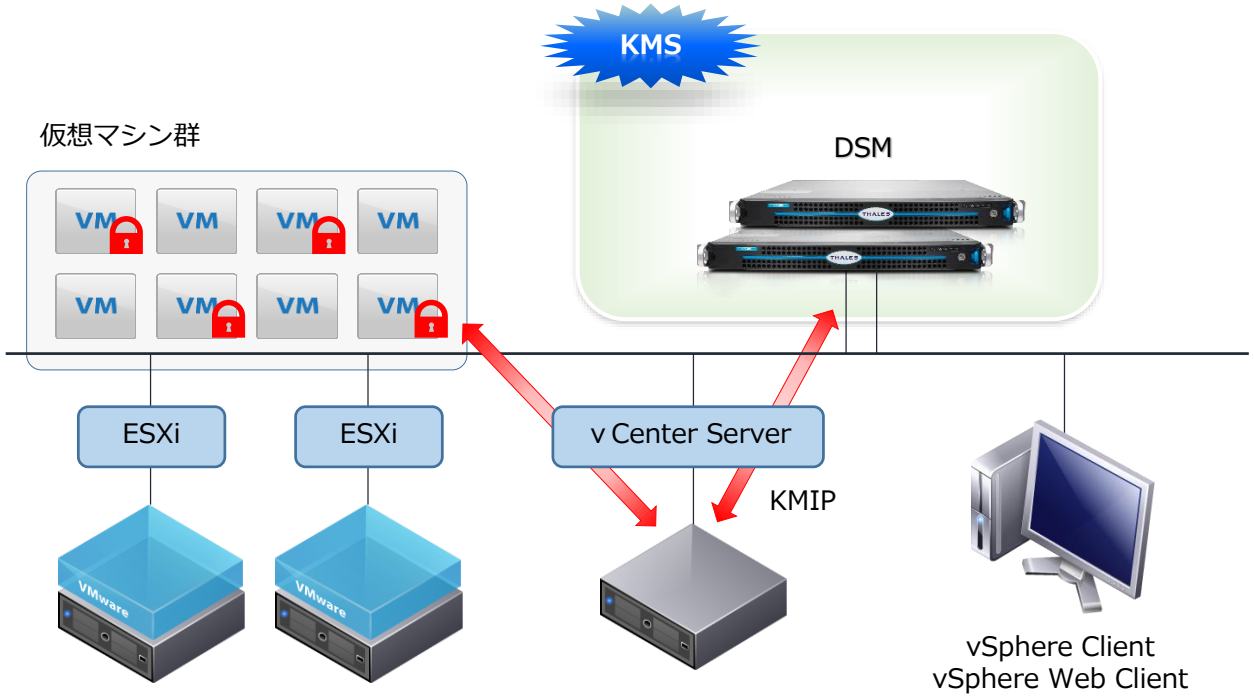
DSM ： Data Security Manager

VKM ： Vormetric Key Management

仮想マシンの暗号化 システム構成例

◆ システム構成例

Sample



KMS ： Key Management Server
(DSM ： Data Security Manager)

※ DSMは、VMware 認定のKMSです。
https://www.vmware.com/resources/compatibility/pdf/vi_kms_guide.pdf

◆ 製品構成

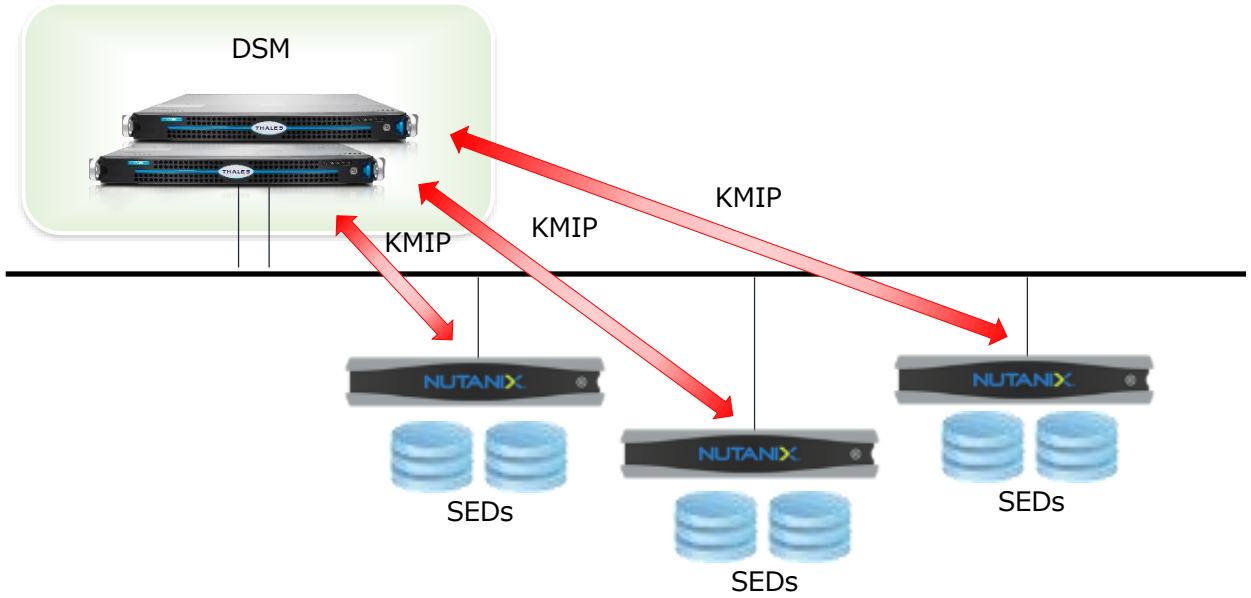
- Physical DSM V6000 FIPS L2, 6.x Software
  2台
- KMIP Client Connection
  1本

◆ 製品構成価格

営業担当にお問い合わせください。

KMIP対応デバイスの暗号化 システム構成例

◆ システム構成例



Sample

◆ 製品構成
- Physical DSM V6000 FIPS L2, 6.x Software
  2台
- Key Management Client
  3本

◆ 製品構成価格
  営業担当にお問い合わせください。

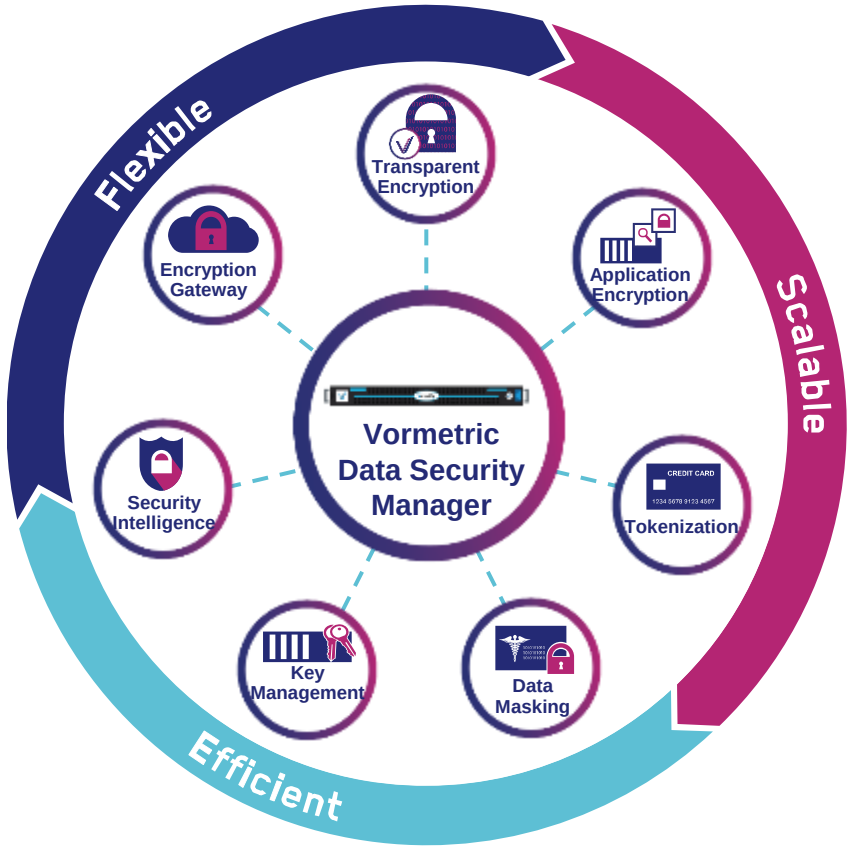
DSM ： Data Security Manager

KMIP ： Key Management Interoperability Protocol
データ暗号化のための暗号鍵を管理する「鍵管理サーバー」と「クライアント」との通信方式を定める通信プロトコル。

Vormetric Data Security Platform

エンタープライズ向け暗号化ソリューション

- シンプルな構成・容易な設定
- 短期間での導入
- ハイパフォーマンス
- セキュアな鍵管理



Vormetric 製品は、コンプライアンス要件や情報漏えい対策として使用できます。

個人情報保護法	GDPR	PCI DSS	JSOX	HIPAA	NIST SP800シリーズ

Vormetricをご検討ください。

キヤノンマーケティングジャパン株式会社

ゲートウェイセキュリティ企画本部

https://cweb.canon.jp/it-sec/solution/vormetric/

Vormetric 評価版無償貸出サービス実施中！

（ 評価版は仮想アプライアンスでのご提供となります ）