THALES

タレスの提供する安心・安易な非保持化ソリューション（トークナイゼーション）

タレスジャパン株式会社
e-Security事業部

2018.06.22

Agenda

- Thales Group および Thales e-Securityの会社紹介
- トークナイゼーションとPCI-DSSについて
- Thales Vormetricのトークナイゼーションについて
- 国内外事例のご紹介
- まとめ

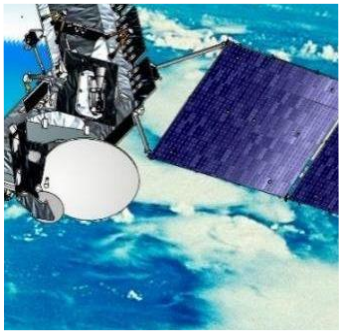
THALES

Thales Group および
Thales e-Securityの会社紹介

Thales Groupについて

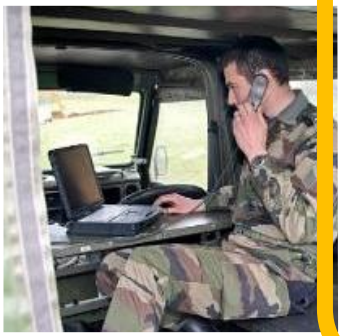
航空産業

宇宙産業



交通システム

防衛



セキュリティ

従業員数： 67,000人

技術・開発：22,500人
専門エンジニアと研究スタッフ

売上高：150億ユーロ

営業拠点： 56か国

タレスは「安全」「セキュリティ」が不可欠な分野でスマートなソリューションを提供しています！

OPEN
THALES GROUP INTERNAL
THALES GROUP CONFIDENTIAL
THALES GROUP SECRET

THALES

Thales e-Security Inc. について

❖ Global Headquarters

2860 Junction Avenue
San Jose, CA 95134 USA

- 50数ヵ国にてビジネスを展開750人強の従業員
- 100ヵ国以上で10,000以上のカスタマー
- グローバルでサービス＆サポートを提供
- セキュリティサービスのリーディングカンパニー - FIPS, Common Criteria, PCI HSM
- 20のクラウドサービス会社より弊社のソリューションを提供

❖ APAC Headquarters

Thales Transport & Security(Hong Kong) LTD.

Unit 4101-03, 41/F.,
248 Queen's Road East, Wanchai, Hong Kong, PRC

タレスのプレゼンス

#1 worldwide

Payloads for telecom satellites

Air Traffic Management

Sonars

Security for payment transactions

#2 worldwide

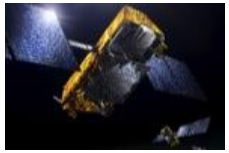
Rail signalling systems

In-flight entertainment

Military tactical radio

#3 worldwide

Avionics



Civil satellites

Surface radars

€15 bn
Revenues

64,000
Employees

56
Countries

Leadership in Security

タレスのセキュリティ技術とサービスは、世界の決済取引の80%以上を担い、企業と政府の最も重要な情報を保護します。

We currently protect data for:

- NATO加盟国を中心に50ヵ国
- 世界の20の大手銀行のうち19社
- 世界中の3,000の金融機関
- トップ5のエネルギー会社のうち4社
- 航空会社5社中4社
- 世界トップ10のうちの9つのインターネット関連会社の サイバーセキュリティ
- 130の顧客向け、クリティカル情報システムの運用とサイバーセキュリティ

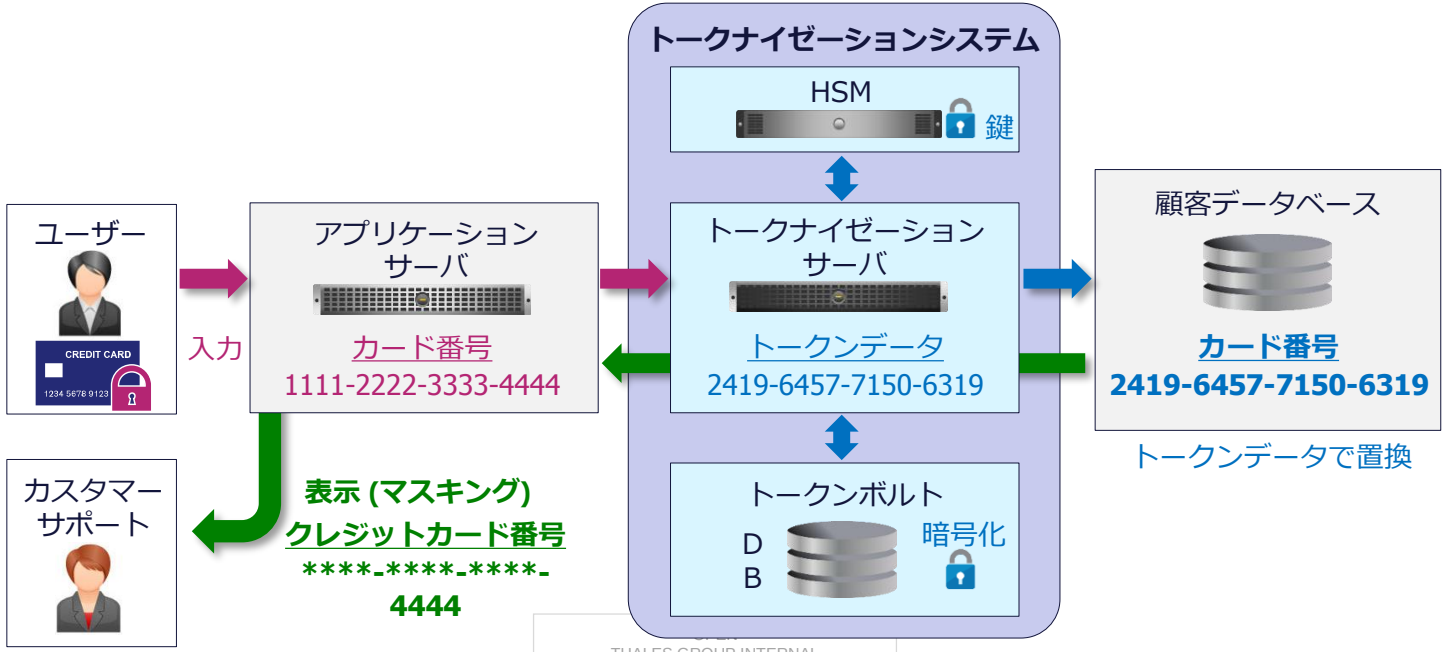
THALES

THALES

トークナイゼーションと PCI-DSSについて

一般的なトークナイゼーションの仕組み

・指定されたデータをトークンデータで置き換えます。
・既存のデータベースには置き換えられたトークンデータが保管されます。
・原本データは暗号化されトークンボルトと呼ばれるデータベースに暗号化保存されます。
・データの呼び出し時にマスキング機能を用いることもできます。

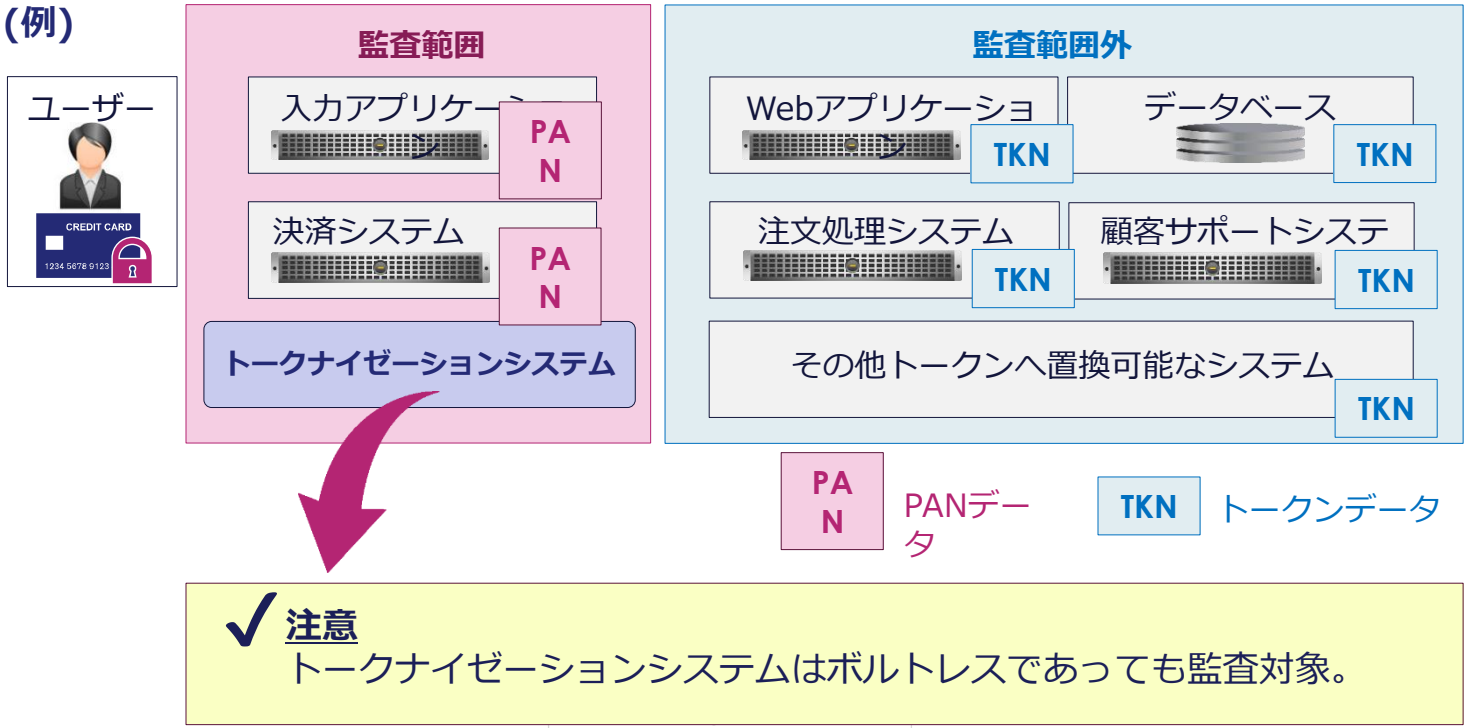


THALES

PCI DSSとトークナイゼーション

■監査対象からの除外

トークナイゼーションにより匿名化された箇所はPCI DSSの監査対象から除外されます。



✓ **注意**

トークナイゼーションシステムはボルトレスであっても監査対象。

トークナイゼーションのメリット

■技術面

・既存データベースのカラム改修を行う必要がありません。
・既存システムへのトークナイゼーションの組み込みがカラム暗号と比較して容易です。
・マスキング機能によって表示内容を制御することができます。

暗号化 (データベースカラム暗号) の場合

氏名	カード番号
鈴木	1111-2222-3333-4444

→

氏名	カード番号
鈴木	w6ｶ。ru?!PJQRMqｲ2ﾁﾀﾂ

・データ長が変わってしまう
・データタイプが変わってしまう
・既存プログラムの改修工数が大きい
・復号すると原本データが表示される

トークナイゼーション (トークナイズ)

氏名	カード番号
鈴木	1111-2222-3333-4444

→

氏名	カード番号
鈴木	2419-6457-7150-6319

・データ長は変わらない
・データタイプは同じ
・既存プログラムの改修工数は小さい

トークナイゼーション (デトークナイズ)

氏名	トークン番号
鈴木	2419-6457-7150-6319

→

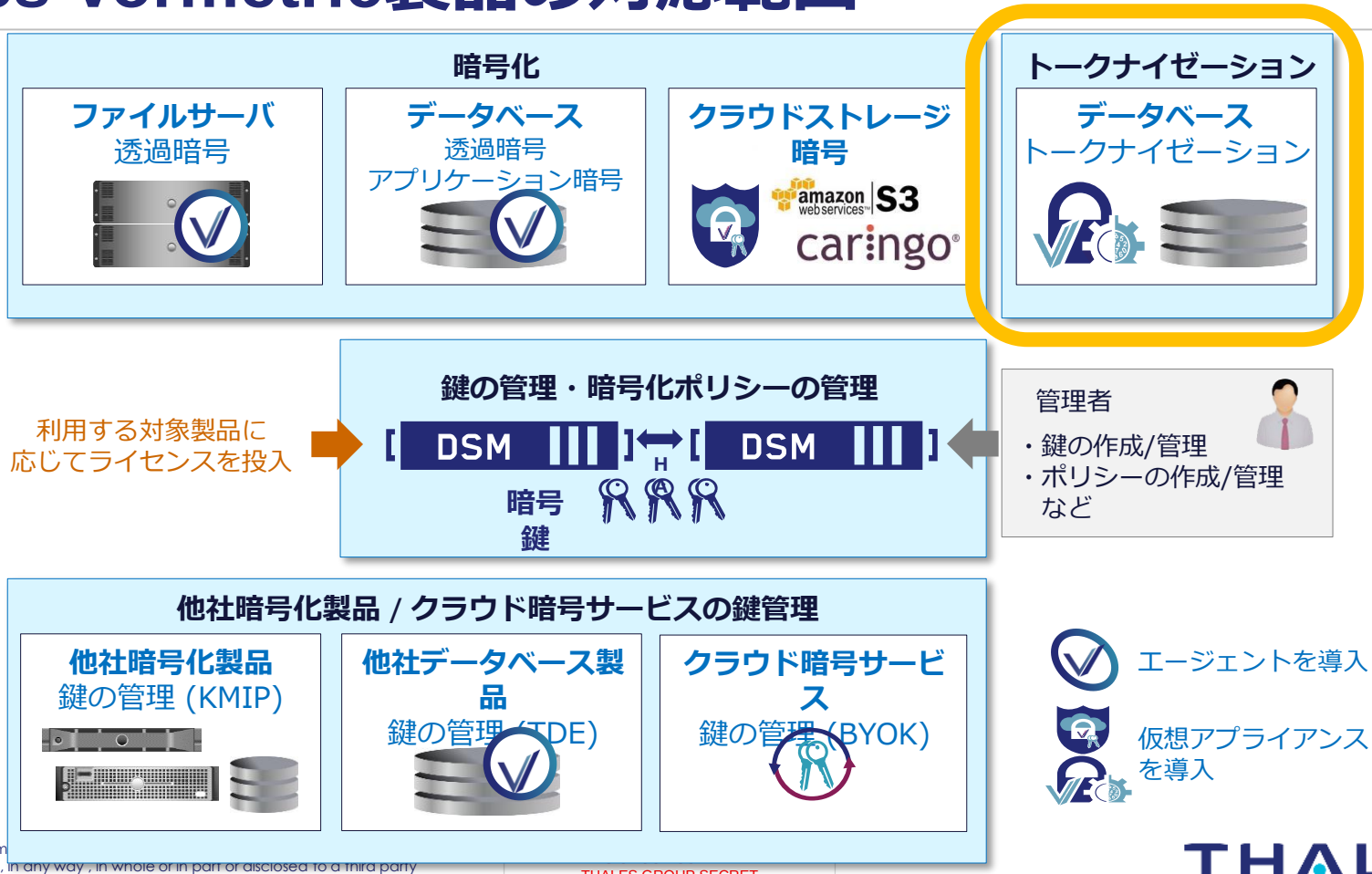
氏名	カード番号
鈴木	****- ****- ****-4444

・ユーザー別に表示内容を変更可能
・マスクデータからの復号は不可

THALES

Thales Vormetricの
トークナイゼーション

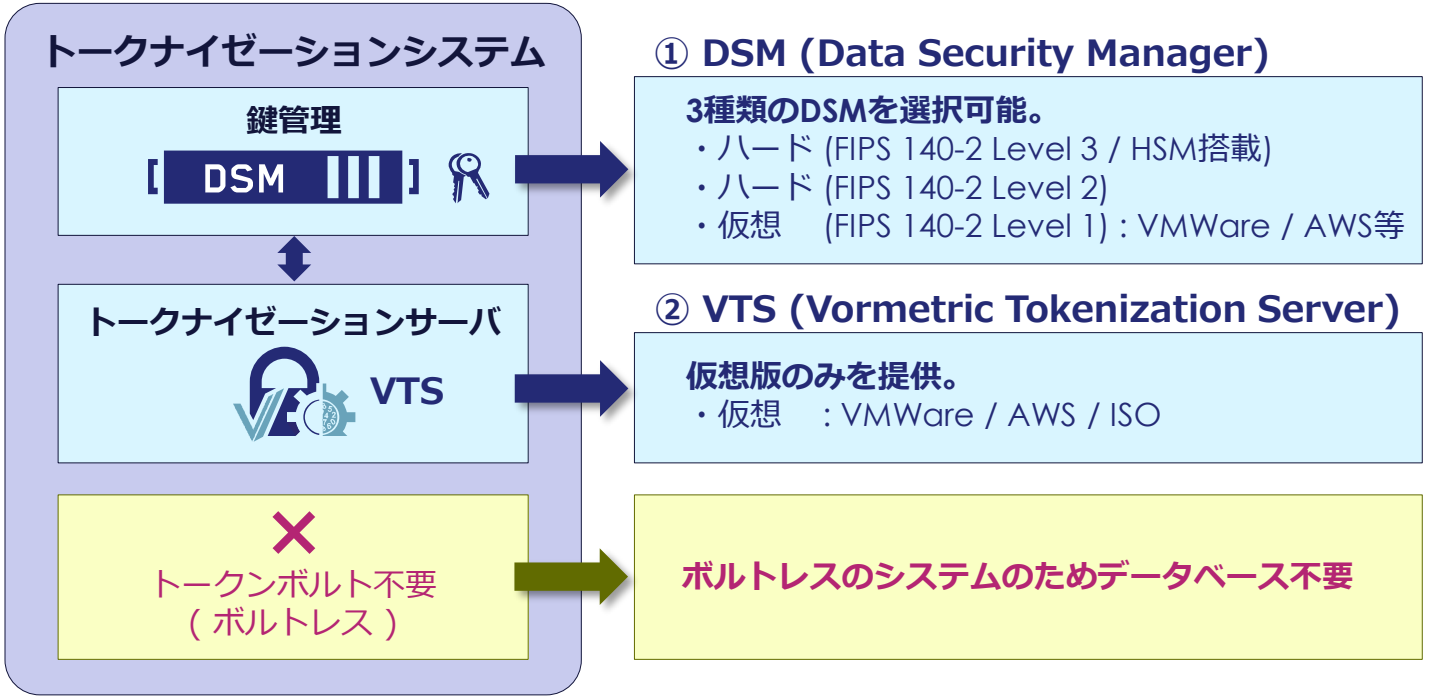
Thales Vormetric製品の対応範囲



THALES

Vormetricトークナイゼーション (VTS) のコンポーネント

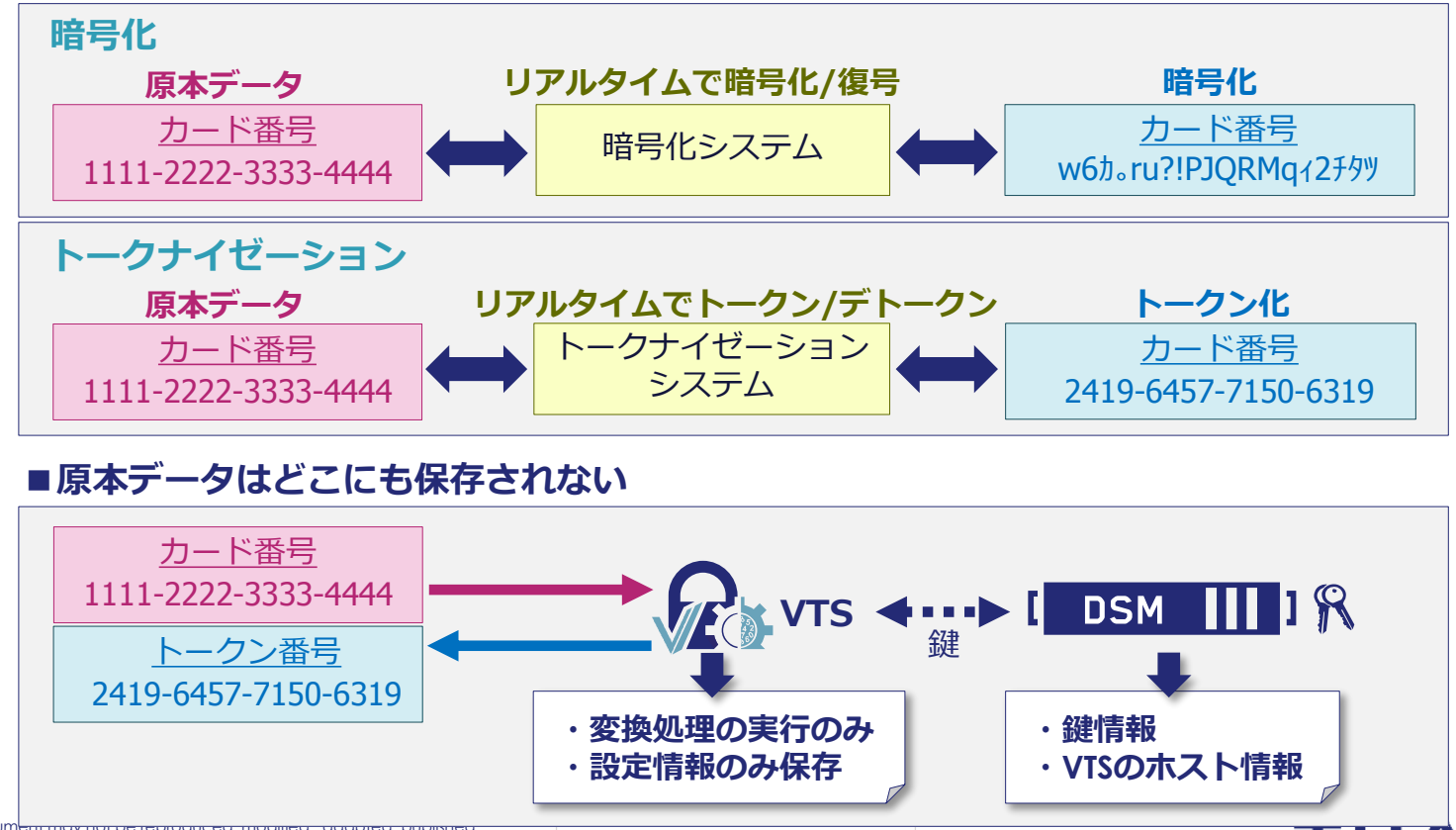
■2つのコンポーネントのみ



※DSMの最小構成は2台になります。(HA構成)

ボルトレストークナイゼーションの仕組み

■考え方は暗号化と同じ

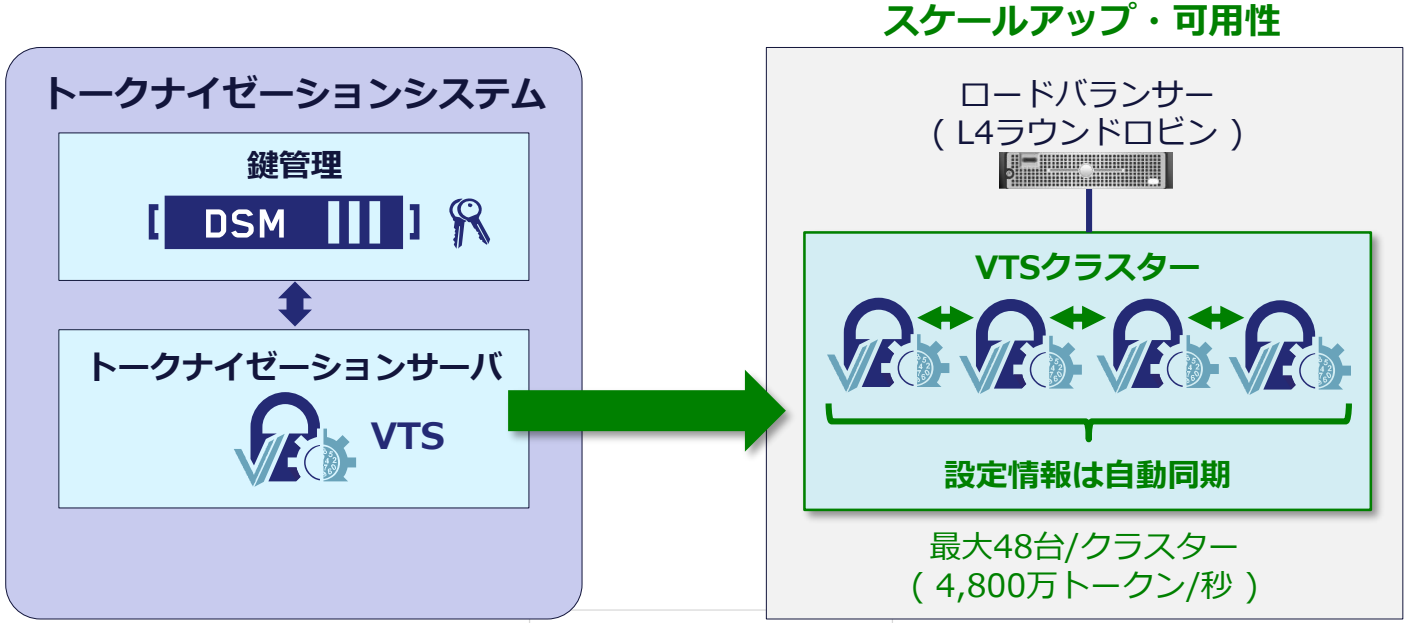


Vormetricトークナイゼーション (VTS) の特徴 - 1

(1) パフォーマンス / 高可用性

・ボルトレスによる導入コストや運用コストの削減。
・高パフォーマンス。(単体エンジン性能: 100万トークン／秒)
・クラスター構成による容易なスケールアップ、高可用性の実現。

コスト削減
短期導入

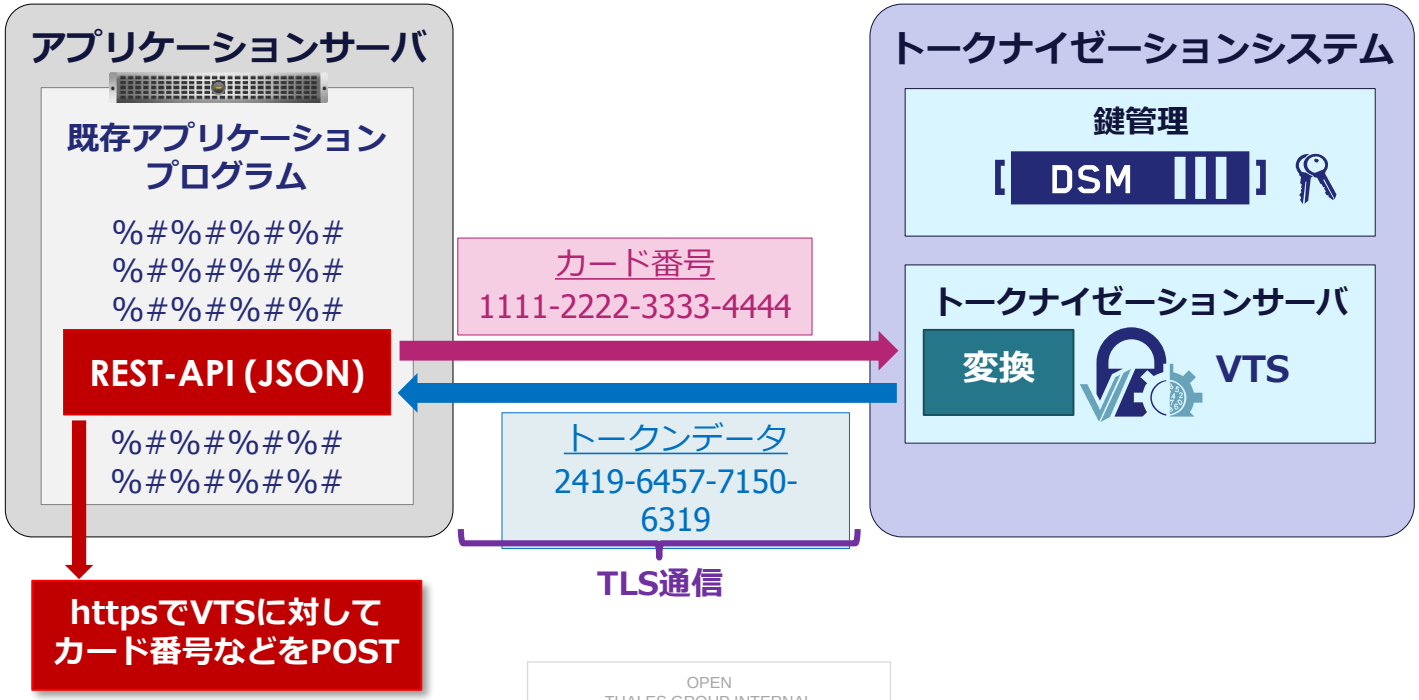


Vormetricトークナイゼーション (VTS) の特徴 - 2

(2) 容易な組み込み

・使用しているデータベースの種類は問いません。
・REST-APIを用いた既存アプリ環境への容易な組み込み。

短期導入



THALES

Vormetricトークナイゼーション (VTS) の特徴 - 3

REST API のフォーマット

■URL

https://<VTSのホスト名>/vts/rest/v2.0/tokenize (デトークナイズ時は /detokenize) に対して認証情報と共に以下の送信データをPOST。

■送信データ (1,000PAN単位での一括トークン処理も可能)

- トークングループ　：使用するDSM内の鍵を定義。
- 送信データ　：PANデータ。(デトークナイズ時はトークンデータ)
- トークンテンプレート　：変換形式などを定義。

```
{ "tokengroup":"TOKENGROUP1", "data":"1111-2222-3333-4444",
"tokentemplate":"TEMPLATE1" }
```

PANデータ

■VTSからの応答データ

```
{ "token" : "2419-6457-7150-6319", "status" : "Succeed" }
```

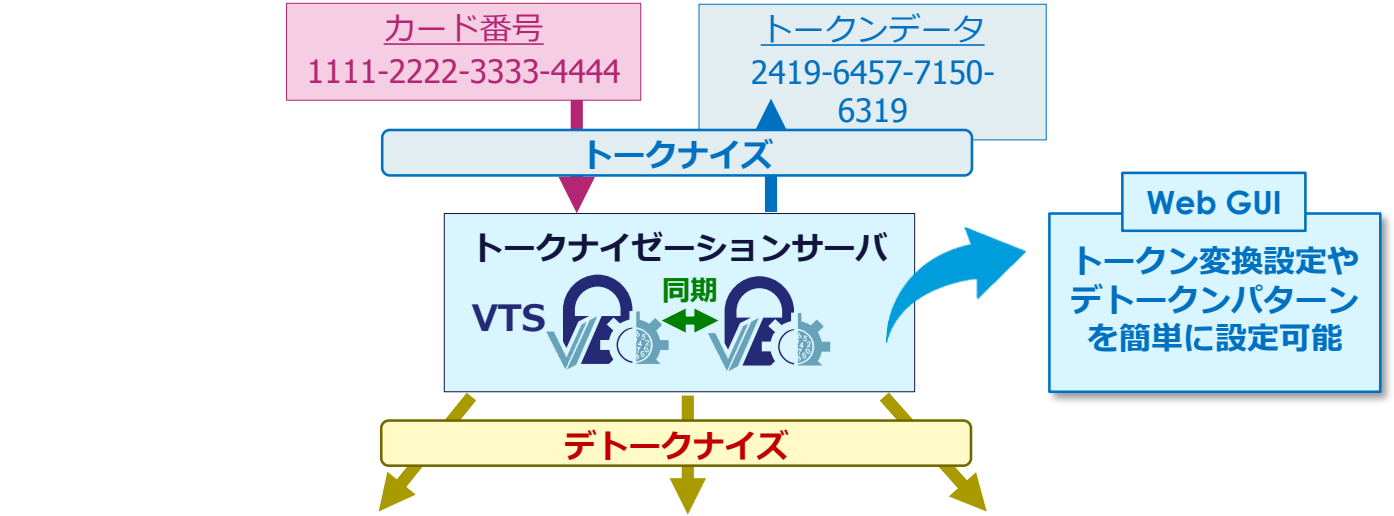
トークンデータ

Vormetricトークナイゼーション (VTS) の特徴 - 4

(3) 容易な設定

- Webベースの管理画面で容易に設定が可能。
- 設定情報はVTSクラスター内の全てのVTSへ自動同期。

短期導入



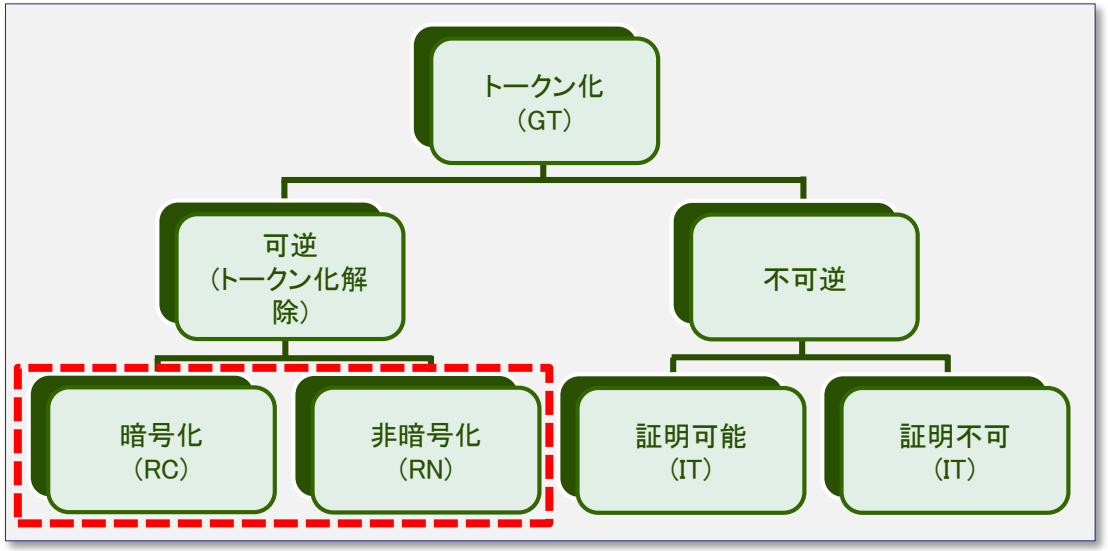
Vormetricトークナイゼーション (VTS) の特徴 - 5

(4) アルゴリズム

・PCI DSS暗号化トークン(RC) / 非暗号化トークン(RN)に対応。
・それぞれのアルゴリズムは併用可能。

PCI DSS対応

PCI DSS “Tokenization Product Security Guidelines”
P6の図1: トークン化の分類より



Vormetricトークナイゼーション (VTS) の特徴 - 6

■VTSでは複数のアルゴリズムを搭載

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。

■それぞれのアルゴリズムの特長

対応可能文字列

・FPEモード(FF3,FF1)　：数字だけでなく文字列・特殊文字も変換可能。
・Randomモード　：数字のみ変換可能。

使用するアルゴリズムの指定方法

・VTSでテンプレートを作成。(テンプレート内にはアルゴリズムも指定)
・変換クライアントがREST-APIを用いて、テンプレート名と共にPANデータを送信。

Vormetricトークナイゼーション (VTS) の特徴 – 7

(5) DSM (Data Security Manager)による鍵の管理

・鍵はDSMで作成され、運用開始後のマスター鍵の変更も可能。
・FIPS 140-2に対応した仮想・物理DSMを選択可能。

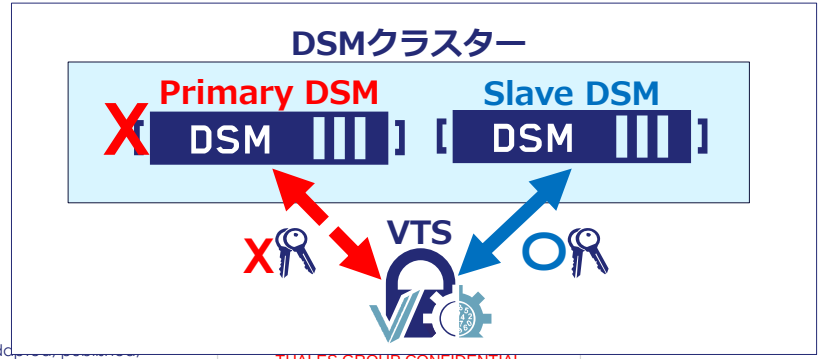
PCI DSS対応

DSMアプライアンスの種類

・ハードウェア (FIPS 140-2 Level 3 / HSM搭載)
・ハードウェア (FIPS 140-2 Level 2)
・仮想　　(FIPS 140-2 Level 1) : VMWare / Amazon AMI / Hyper-V / Azure

冗長機能

・DSMクラスター機能により、全ての設定情報や鍵はSlave DSMへリアルタイムで同期。
・Primary DSMの障害時はSlave DSMが鍵の提供を行います。



トークナイゼーションはカード情報だけが対象ではない

■原本データ

氏名	生年月日	電話番号	メールアドレス	カード番号
山田　太郎	1986-10-01	03-1111-1111	yamada@vormetric.com	4012-8888-8888-1881
鈴木　一郎	1972-04-23	045-222-2222	suzuki@vormetric.com	5105-1051-0510-5100

トークナイズ

■データベース内

氏名	生年月日	電話番号	メールアドレス	カード番号
山田　太郎	3071-96-38	70-3709-3682	iLz6vY@INA9JMNIX.qxo	2074-3188-3232-9053
鈴木　一郎	3509-90-81	909-913-4161	lCP2pb@wl0kugQPq.8LH	1632-9788-2850-4932

デトークナイズ

■アクセスクライアント

氏名	生年月日	電話番号	メールアドレス	カード番号
山田　太郎	****-10-01	**-****-1111	******@********c.com	****-****-****-1881
鈴木　一郎	****-04-23	***-***-2222	******@********c.com	****-****-****-5100

トークナイゼーションの導入～運用開始まで (例)

(1) 影響範囲/必要性能の調査	・導入後の既存サービスや業務への影響を調査 ・現在のピークトランザクションの調査
(2) 変換処理実行場所の確定	・トークナイズを実行するアプリケーションの確定 ・デトークナイズのポリシーとアプリケーションの確定
(3) システム設計/運用策定	・システムの配置場所、ネットワーク / セキュリティ設計 ・監視 / 運用方法の策定
(4) 対象製品の機能評価	・テスト環境でのトークナイゼーション機能の評価 ・障害発生時のサービス継続性テスト / 運用テスト
(5) 製品の調達/導入/設定	・トークナイゼーションシステムの導入、設定 ・ネットワーク / セキュリティ機器などの設定変更
(6) アプリケーション改修	・(2)で対象となったアプリケーションの改修、テスト ・アプリケーションシステムの切り替え
(7) 既存データの変換	・既存データベース内のPANを一括トークナイズ ・デトークナイズ (PAN復号/マスキング) のテスト
(8) 運用開始	・サービス、業務への影響有無を再確認 ・システム全体において性能劣化が発生していないか

まとめ: Vormetricトークナイゼーション (VTS) のメリット

(1) 構築 / 導入が容易
- VTSはVM仮想アプライアンス(ova/iso形式)・AWS AMIで提供。
- DSM(鍵管理)も仮想アプライアンス版を使用可能。
- 全てのコンポーネントのインストール/基本設定は数時間で完了。

(2) パフォーマンス
- VTS 1台あたり最大100万トークン/秒。
- ロードバランサーと複数台のVTSの設置によりさらにパフォーマンスの向上が可能。

(3) 可用性
- ロードバランサーと複数台のVTSを設置することでサービス停止をゼロへ。
- サービス稼働中もVTSを追加しスケールアップが可能。
- DSM(鍵管理)は鍵情報含め全ての情報がSlave DSMへ自動同期。

(4) 最小限のアプリケーション改修
- REST API を既存アプリケーションへ組み込むだけ。

(5) 価格体系
- トランザクションやトラフィックに依存しない価格体系。
- 開発 / テスト環境専用の価格体系も別途提供。

参考：PCI DSSへの適用

PCIDSS 要件	内 容	Vormetric製品の対応項目
2	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	2
3	保存されるカード会員データを保護する	3.3 / 3.4 / 3.4.1 / 3.5 / 3.6
4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	4.1
7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	7.1 / 7.1.1 / 7.1.2 / 7.1.3 / 7.1.4 / 7.2
8	システムコンポーネントへのアクセスを確認・許可する	8.2 / 8.2.1 / 8.7
9	カード会員データへの物理アクセスを制限する	9.8.2
10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	10.1 / 10.2 / 10.3 / 10.4.1 / 10.5 / 10.6

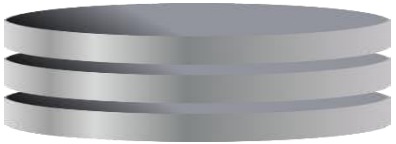
拡張性: カード情報の保護＋アルファのリスク管理の実現

短期導入・容易な運用

[DSM]

DSMで鍵/ポリシーを一元管理

データベース

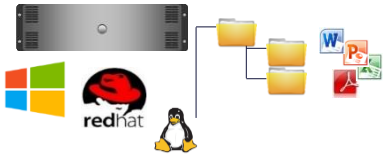


機密情報のトークン化
マイナンバー
電話番号
メールアドレス など

＋

データベースの暗号化

ファイルサーバ



非構造化データの暗号化
ファイルサーバ内の
顧客リスト・人事情報
知的財産情報・設計図
バックアップデータ
などを暗号化。
(ファイル種別の制限なし)

暗号鍵 / クラウド暗

暗号鍵の管理
データベース純正の暗号鍵やストレージ暗号などで使用する暗号鍵、パブリッククラウドサービスの暗号鍵をDSMでセキュアに管理。
(TDE鍵 / KMIP / CCKM)

PCI DSS・MAS対応 / カード・個人情報の保護 / 内部犯行対策・サイバーセキュリティ対策

オンプレミス・クラウド・ハイブリッド

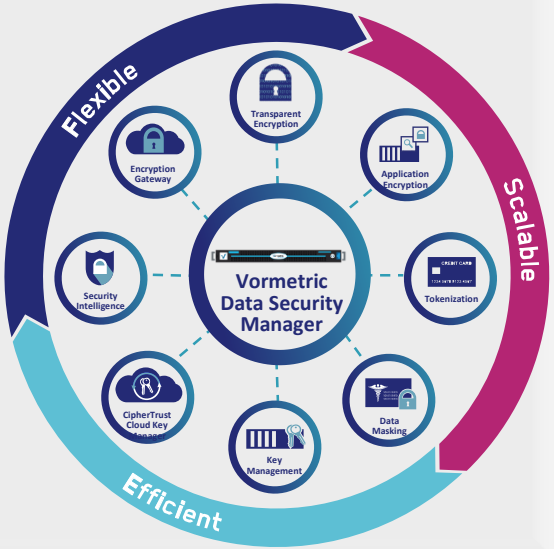
Thales Vormetric製品は

短時間での導入

シンプルな構成・容易な設定

ハイパフォーマンス

セキュアな鍵管理



VM

評価版

DSM・暗号化・トークナイゼーション製品の評価版を提供しています。

※ 評価版の機能は製品版と同じです。

THALES

国内外の導入事例

海外事例-1：アジア太平洋地域で展開する主要な保険会社

採用会社概要

- アジア太平洋地域で展開する保険のリーディングカンパニー
- シンガポール、香港、インドネシア、ベトナムなど12ケ国にわたるビジネス展開

課題

- PCI/DSS compliance
- PII データ保護
- MAS監査ガイドライン

ソリューション

- 構造データおよび非構造化データおよびクラウドの保護を、単一のVormetricソリューションで実現
- DSM（データセキュリティマネージャー）をシンガポールと香港に設置。
- 地域を越えた数百の重要なデータサーバーの保護：MSSQL/DB2/Sybase/Informix/Oracle

暗号化の展開

- 香港・シンガポールから10ケ国に展開: 複数のプラットフォーム、複数のドメイン
- データベース（DB）の暗号化から始まり、非構造化データとクラウドの (IAAS on Azure ,OF365 and Salesforce)暗号化へ展開。

海外事例-2: オーストラリアの主要銀行

採用会社概要

- オーストラリアの売上上位の銀行の一社

要求事項

- PCIコンプライアンスおよび内部監査
- Hadoop上へのビックデータのディブロイメント
- クラウド/Azure上のデータ保護

ソリューション

- Single Vormetric solution to protect both structured and unstructured data
- データベースとファイルサーバーへの透過暗号製品（VTE） 導入
- アプリケーションのトークナイゼーションに

  トークナイゼーションサーバー（VTS）導入
- Hadoop/Hive向けの設定を容易にするUDF（User Defined Functions)

導入プロセス

- 透過暗号製品（VTE）およびトーナイゼーションサーバー

  製品（VTS）から導入開始
- Hadoop向けUDFの導入に移行。Hadoop上のデータレイクを保護。

海外事例-3: アジアの主要な小売＆クレジット会社

採用会社概要

- 300の拠点を持つ、アジアの主要な小売＆クレジット会社

要求事項

- PCI DSS対応のためのデータ保護
- 安全な社内のアクセス
- 将来の拡張性に対応/保護する対象のデータが増えてもパフォーマンスが落ちない構成取れる
- Windows, Linux and UNIXシステムのサポート

ソリューション

- 構造化データと非構造化データを保護する単一のVormetricソリューション
- 透過暗号製品（VTE)：データベースと非構造化データの保護
- トークナイゼーションサーバー製品（VTS)：

  決済アプリケーション

導入プロセス

- 2016年以前に、データベースおよびファイルサーバーに対して、HSM（Hardware Security Module), 透過暗号（VTE）製品導入
- 2017年にトークナイゼーションサーバー製品（VTS） 追加

国内事例: 主要銀行

採用会社概要

- 売上上位4位以内の国内大手銀行

要求事項

- PCI DSS と決済セキュリティ
- シンガポール金融管理局（MAS）テクノロジーリスク管理（TRM）コンプライアンス

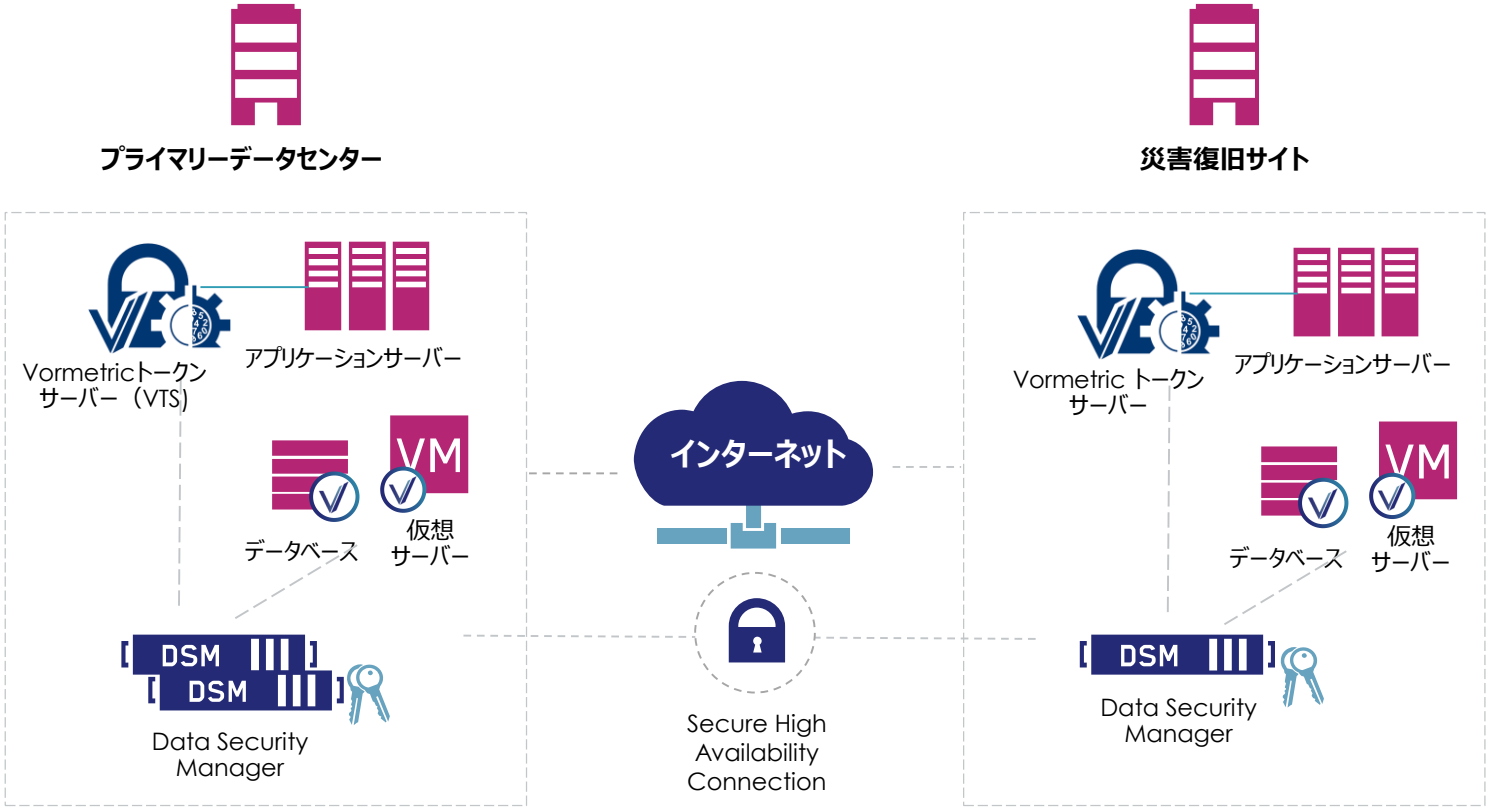
ソリューション

- 構造化データと非構造化データを保護する単一のVormetricソリューション
- 透過暗号製品（VTE）：データベースと非構造化データの保護
- トークナイゼーションサーバー製品（VTS）：決済アプリケーション

導入プロセス

- 2016年以前にデータベースおよびファイルサーバーに対して、HSM（Hardware Security Module), 透過暗号（VTE）製品導入
- 2017年にトークナイゼーションサーバー製品（VTS） 追加

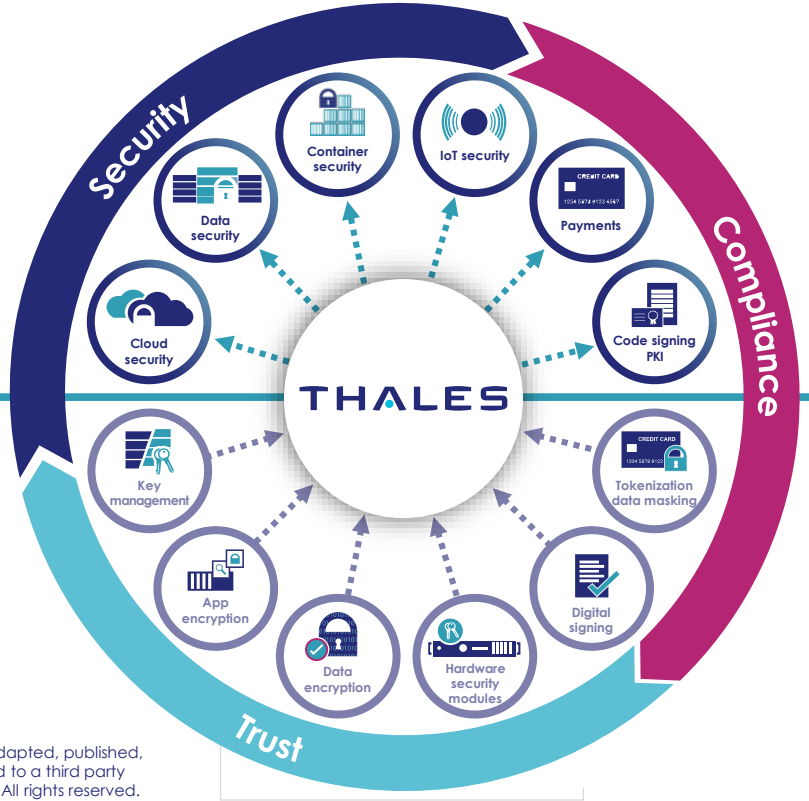
構成例



幅広いお客様のニーズに合わせたタレス製品やソリューション群

Customer use cases

Thales products/solutions



THALES

製品に関するお問い合わせ

タレス ジャパン株式会社
e-セキュリティ事業部
TEL　：03-6234-8100
Email　：jpnsales@thales-esecurity.com
Web　：https://www.thalesesecurity.com/