THALES
Building a future we can all trust

“PCIDSS 4.0対応:
暗号化と鍵管理のスムーズな導入手法”

タレスDISジャパン株式会社
データ保護事業本部
セールスエンジニア
豊田　健杜

タレス会社概要

THALES

80,000 以上
社員

68
か国
への事業展開

自己資金による
研究開発費
€10億
(1400億円)

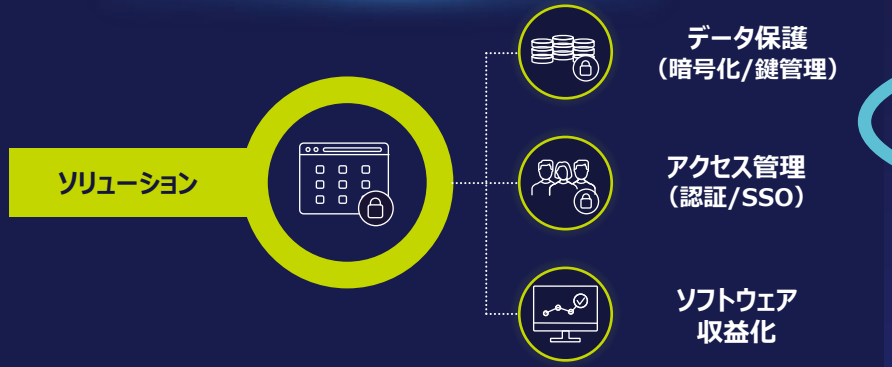
2020年度
売上
€170億
(2兆3500億円)

データセキュリティ事業本部

THALES

タレス会社概要-データセキュリティ事業本部

ハードウェア セキュリティ モジュール (HSM) は、デジタル キーを保護および管理し、デジタル署名の暗号化および復号化機能、強力な認証、およびその他の暗号化機能を実行する物理的なコンピューティング デバイスです



世界的リーダー
汎用HSM、クラウド
HSM HSMs

世界的リーダー
データ暗号化 及び
暗号鍵管理

世界的リーダー
多要素認証

世界的リーダー
ソフトウェア収益化

2,500+
従業員

25 カ国で
ビジネス展開

750人
世界のエンジニア

30,000 世界の
導入ユーザー数

BUILDING A FUTURE WE CAN ALL TRUST

Thalesのテクノロジーとサービスは、毎日 5兆ドルを超える銀行間金融取引と、
最も価値のある企業および政府の情報を保護しています。

世界における採用実績

金融

BARCLAYS
UBS
JPMorgan Chase & Co.
Deutsche Bank

テクノロジー

Microsoft
salesforce
Verifone

ヘルスケア

CVS pharmacy
McKESSON
DELTA DENTAL
MOLINA HEALTHCARE

決済

VISA
DISCOVER
AMERICAN EXPRESS

政府機関

Australian Government
Department of Defence
Ministry of Defence
UNITED STATES POSTAL SERVICE

サービスプロバイダー

FUJITSU
orange Business Services
AT&T
rackspace technology

リテール

Walmart
Office DEPOT OfficeMax
GAP
WILLIAMS SONOMA

製造

SAMSUNG
Kellogg's
BOSCH
3M
MICHELIN

日本国内でも、政府の基幹システム、金融機関の決済システム、
製造業IoT、小売業など、多数の採用実績

タレスは3,000以上の金融機関における
世界中のバンキングおよび決済サービスの保護をサポートしています

タレスのソリューションにより、金融サービスのコンプライアンスの簡素化、セキュリティ監査の促進、顧客データの保護、データ侵害の回避、最終的には新しいテクノロジーを採用するコストとリスクの削減を実現できます。

タレスは世界のPOS取引の **80%** を保護しています。

トップ **10** の銀行のうち **10** 行がタレスと提携しています。

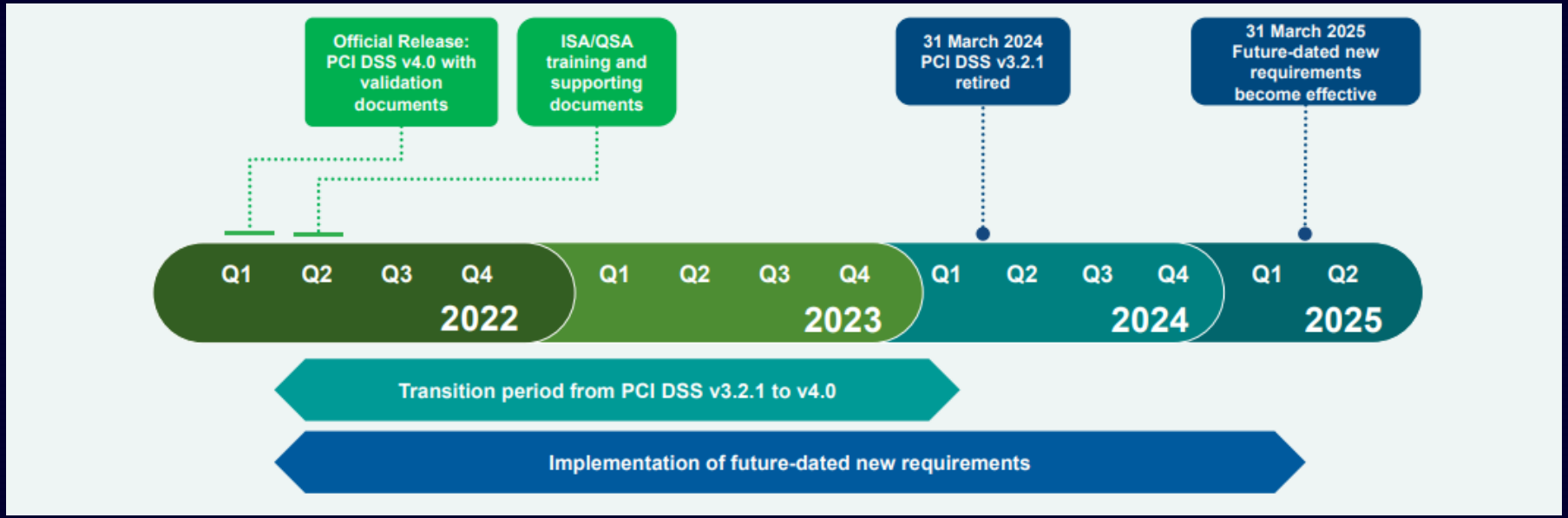
セミナー概要と背景

- **どこのデータを守る必要があるのか**
  - 守るべきデータと要件
  - 強力な暗号化技術とは
- **どのようにしてPCIDSS要件を対処するか**
  - Control
  - Protect
- **暗号化と鍵管理の運用**
  - コストメリット
- **まとめ**

THALES

PCI DSS v4.0タイムライン

2025年3月までにv4.0への準拠が必要

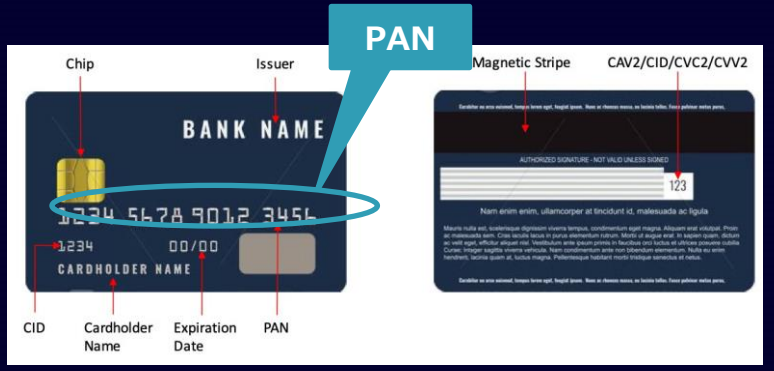


Source: PCI SSC

THALES

どこのデータを守る必要があるのか？

カード会員データ（CHD）	機密認証データ（SAD）
プライマリアカウント番号(PAN)	フルトラックデータ
カード会員名	セキュリティコード
有効期限	PIN/PINブロック
サービスコード	



PCI DSS v4.0変更点の一部抜粋

・PAN
保存時には暗号化が必要
(PCI DSS v4.0 3.5.1.2)

・SAD
取り扱いの明確化
(PCI DSS v4.0 3.2.1,3.3.2)

・暗号鍵管理
本番/テスト環境で同じ鍵が使用されないようにすること
(PCI DSS v4.0 3.6.1.1)

PANを保存する場合の暗号化方法（PCI DSS v4.0 3.5.1.2）

メディア	暗号化方法
リムーバブルメディア	・ディスクレベル暗号化 ・パーティションレベル暗号化
“リムーバブルでない電子メディア” ・内蔵HDD/SSD ・外部ストレージ(SAN/NAS等)	・一方向ハッシュ ・トランケーション ・インデックストークン ・強力な暗号化技術と、 関連する鍵管理プロセス及び手順

THALES

強力な暗号化技術とは

PCI DSS v4.0による「強力な暗号化技術」の定義

強力な暗号化技術	暗号は、可逆的な暗号化プロセスを通じてデータを保護する方法であり、多くのセキュリティプロトコルやサービスで使用される基礎的なプリミティブです。強力な暗号化技術は、業界でテストされ受け入れられているアルゴリズムと、最低 112 ビットの有効な鍵長、および適切な鍵の管理方法に基づいています。 有効な鍵の強度は実際の鍵の「ビット」長よりも短くすることができます。そのため、より大きな鍵を持つアルゴリズムは、実際の鍵のサイズは小さいが有効な鍵のサイズがより大きいアルゴリズムよりも保護が弱くなる可能性があります。*すべての新しい実装では、最低でも 128 ビットの有効鍵強度を使用することが推奨されています。* 暗号アルゴリズムと鍵長に関する業界の参考文献の例としては、以下のようなものがあります。 • *NIST 特別刊行物 800-57 第 1 部,* • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 アルゴリズム、鍵のサイズ、プロトコルのレポート(2018 年)、および* • ISO/IEC 18033 暗号化アルゴリズム、および • *ISO/IEC 14888-3:2-81 IT セキュリティ技術 - 付録付きデジタル署名 - 第 3 部：離散対数ベースのメカニズム ISO*

“強力な暗号化技術は、業界でテストされ受け入れられているアルゴリズムと、最低112ビットの有効な鍵長、および適切な鍵の管理方法に基づいています。”

→アルゴリズムと鍵長、鍵管理が必要

※出典：PCI SSC『Payment Card Industry Data Security Standard』

THALES

暗号化と鍵管理の運用

Control

CipherTrust Managerの機能

- 暗号鍵の堅牢な管理
  - GUIベースで鍵のライフサイクル管理
  - クラウドとオンプレミスを問わない鍵管理
  - 鍵の管理者の職務分掌
  - KMIPやTDEでの外部鍵管理機能
  - シークレット管理
- 様々な暗号化モジュールの提供
  - ファイルシステムレベルの透過的な暗号
  - トークナイゼーション
  - アプリケーションレベルの暗号化
  - DBカラム単位の暗号化
  - データ検知、分類、リスク分析

FIPS Level 3 Validated 140-2

※NIST制定のFIPS 140-2 L1とL3認証取得済み

提供しているアルゴリズムの一例

（例）GUI で作成可能な鍵
・AES
・RSA
・EC等

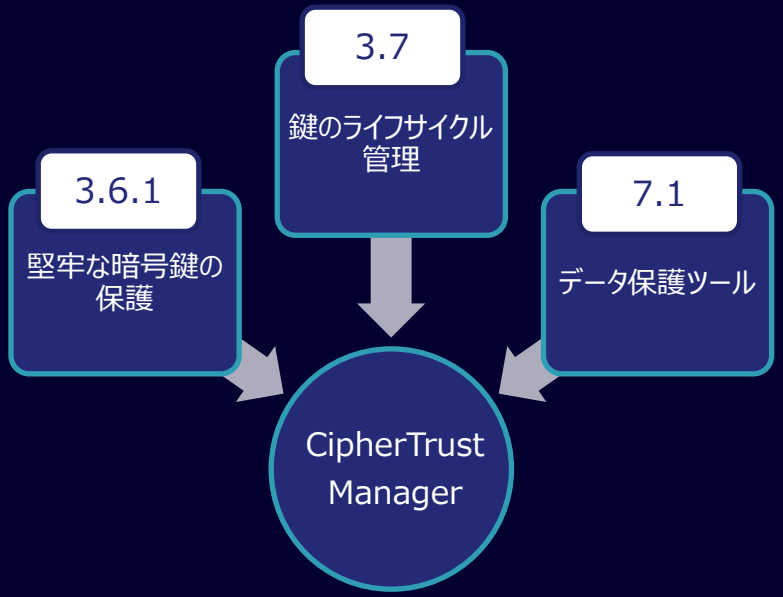
https://thalesdocs.com/ctp/cm/2.13/admin/cm_admin/keys/index.html

THALES

どのようにしてPCIDSS要件を対処するか

Control

CipherTrust Managerで提供可能



3.6.1

- 保存されたアカウントデータを開示や誤用から保護するために使用される**暗号鍵を保護する**

3.7

- 保存されているアカウントデータを保護するために暗号が使用されている場合、**鍵のライフサイクルのすべての側面を網羅する鍵管理プロセスおよび手順が定義され、実施されている**

7.1

- 業務上知る必要のある**システムコンポーネントおよびカード会員データへのアクセスを制限**するためのプロセスおよびメカニズムが定義され、理解されている。

THALES

暗号化と鍵管理の運用

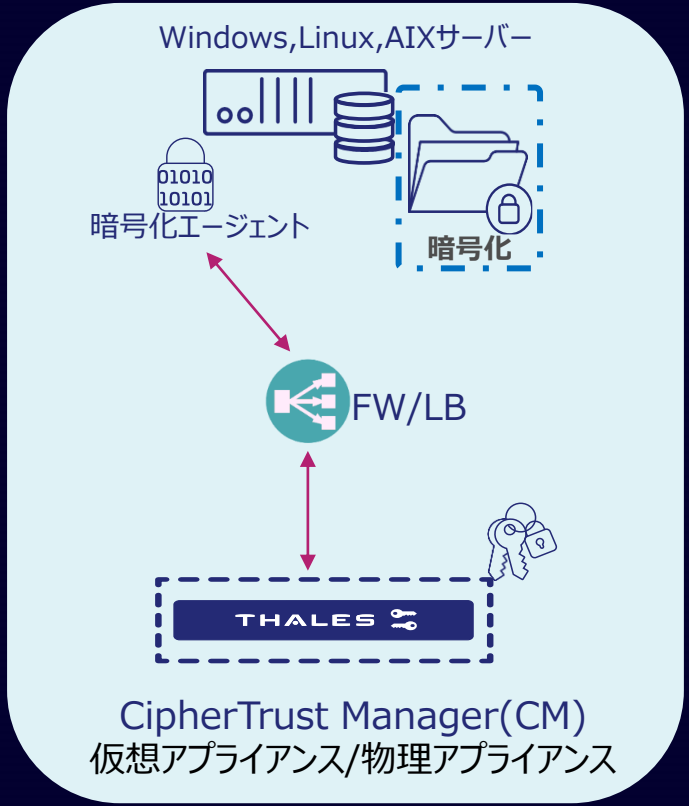
Protect

ファイルシステムレベルでの透過暗号

- ファイル形式の機密データ暗号化
- 処理性能を落とさずDBの暗号化
- 特権IDを含めたユーザーアクセス制御
- 不正プロセスのデータアクセス防止
- ダウンタイムゼロの暗号化(Option)
- 自動での鍵ローテーション(Option)

ディスクレベル暗号と ファイルシステムレベル暗号比較	ディスクレベル 暗号化	ファイルシステムレベル 暗号化(CTE)
ストレージ紛失 /盗難時データ回復不可	✓	✓
ファイル /ディレクトリ単位での暗号化		✓
特権ユーザを含むアクセス制御		✓
ランサムウェア/内部不正対策		✓
ファイルアクセス対象 監査ログ対応		✓

CipherTrust Transparent Encryption(CTE)



THALES

Appendix CTE

Protect

CipherTrust Manager

THALES

Windows Server

①CTE Agent(SW)をサーバへインストール
②CipherTrustManagerでCTE PolicyとGuard Pointを設定
③データの暗号化とアクセスを制御

例:アクセスのパターン

営業

営業ユーザーが
C:¥SalesTeam¥all **内**
にドキュメントを書き込み

人事

人事ユーザーが
C:¥SalesTeam¥all **内**
のドキュメントにアクセス

Administrator

Administratorが
C:¥SalesTeam¥all **内**
のドキュメントを読む

CTE Policy

User Set	Action	Effect
営業	読み取り	許可
人事	書き込み	拒否
Administrator	すべての操作	鍵の適用

Guard Point

C:¥SalesTeam¥all

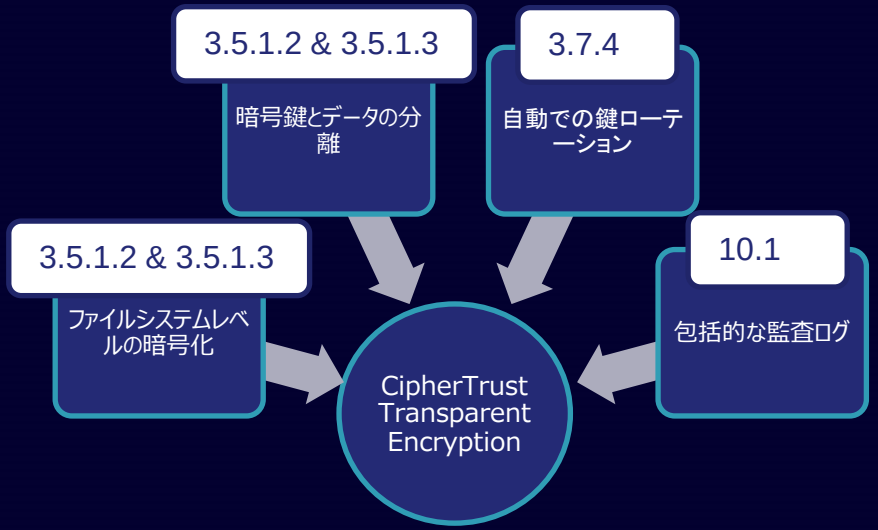
商談情報.txt

A社 最終見積
1234円
B社　最終見積
1234円
・・・・

THALES

どのようにしてPCIDSS要件を対処するか

Protect



CTEで提供可能

3.5.1.2 & 3.5.1.3

- ディスクレベルまたはパーティションレベルの暗号化（**ファイル、列、フィールドレベルのデータベース暗号化ではない**）を使用してPANを読み取り不能にする場合、以下のようにのみ実装される。リムーバブル電子メディア上、または…

3.7.4

- 鍵管理のポリシーおよび手順が、関連するアプリケーションベンダまたは鍵の所有者によって定義され、以下を含む業界のベストプラクティスおよびガイドラインに基づき、**暗号期間の終わりに達した鍵の変更**について実装されている。

10.1

- システムコンポーネントおよび**カード会員データ**へのすべてのアクセスを**記録および監視**するためのプロセスおよびメカニズムが定義され、文書化されている。

※出典：PCI SSC『Payment Card Industry Data Security Standard』

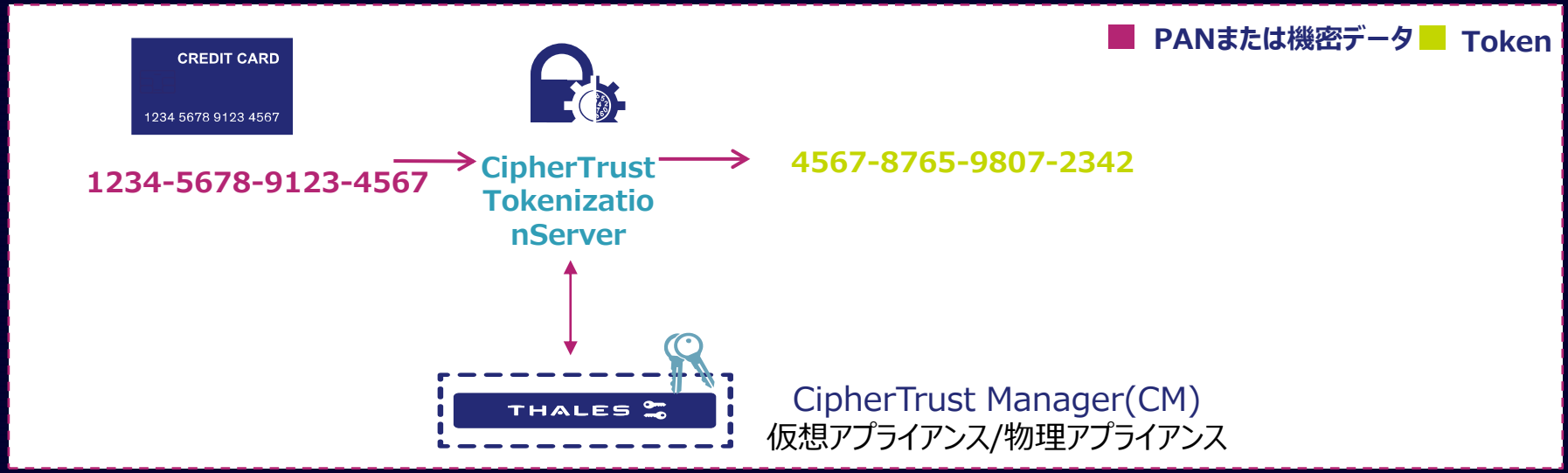
THALES

暗号化と鍵管理の運用

Protect

トークナイゼーション

- PCIDSS監査スコープの削減
- トークンボルト(DB)が不要
- トークナイズのためアプリケーション改修が原則不要
- パフォーマンス確保



THALES

Appendix Tokenization

Protect

PANまたは機密データ　Token

クレジットカード番号
1234-5678-9123-4567

トークナイズ

デトークナイズ

トークンデータ
4567-8765-9807-2342

決済システム

システム管理

トランザクション処理サーバ

PANを取り扱っているため
PCI DSS監査対象

システム管理

データベース

データベース

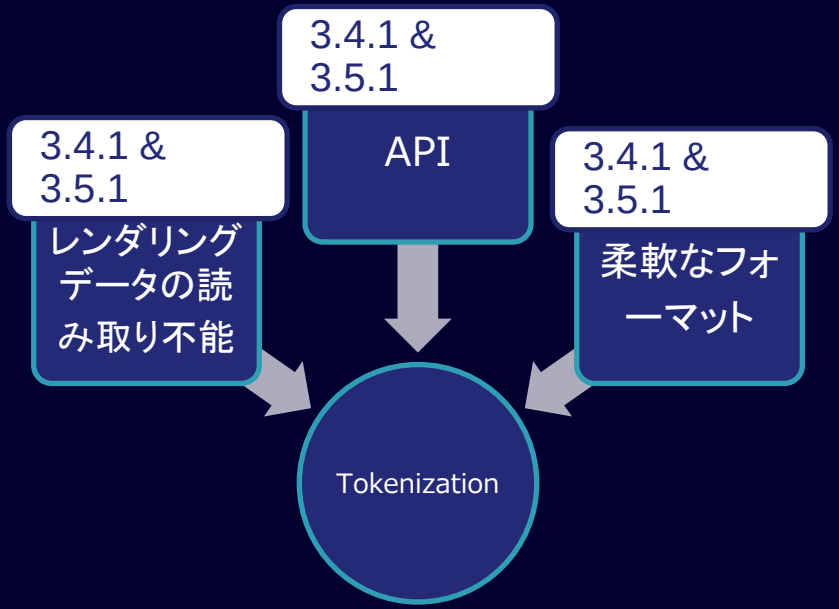
トークンのみ取り扱っているため
PCI DSS監査対象外

THALES

どのようにしてPCIDSS要件を対処するか

Protect

Tokenizationで提供可能



3.4.1 &
3.5.1

- PANは、以下のいずれかの方法を用いて、**保存されている場所の読み取りを不可能**にする。
- PAN は表示時に**マスク**され(BINと末尾4桁が最大表示桁数)、業務上の正当な理由のある担当者のみが**BINとPANの末尾4桁より多く見ることができる**。

※出典：PCI SSC『Payment Card Industry Data Security Standard』

THALES

暗号化と鍵管理の運用

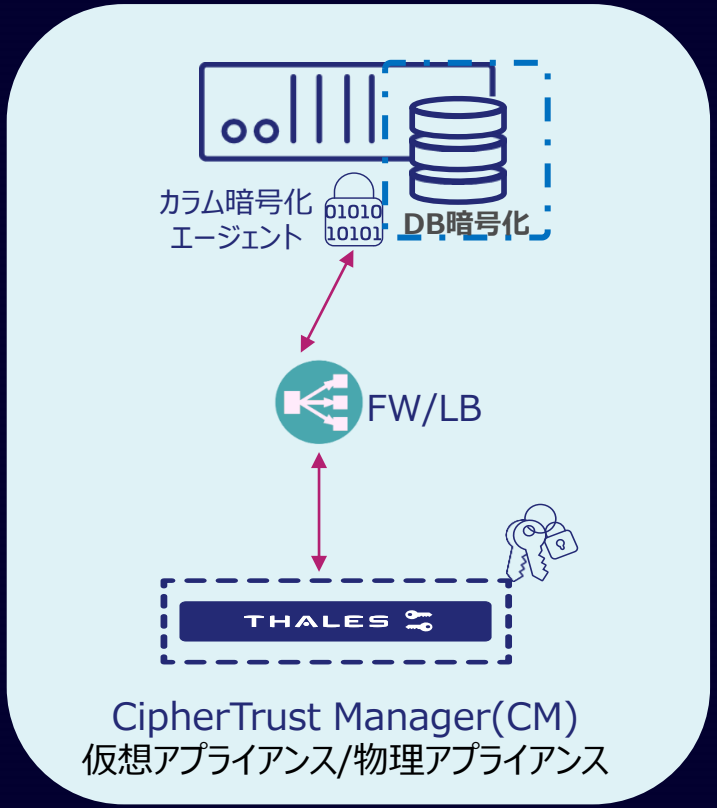
Protect

CipherTrust DatabaseProtectionでの暗号化

- カラム単位での暗号化
- DBユーザーへの暗復号制限
- TDEとは異なりマスター鍵の管理が可能（CTEでも可能）

- カラム単位のため負荷がかかってしまう

汎用的なDBイメージMSSQL/Oracle



THALES

Appendix Column Encryption

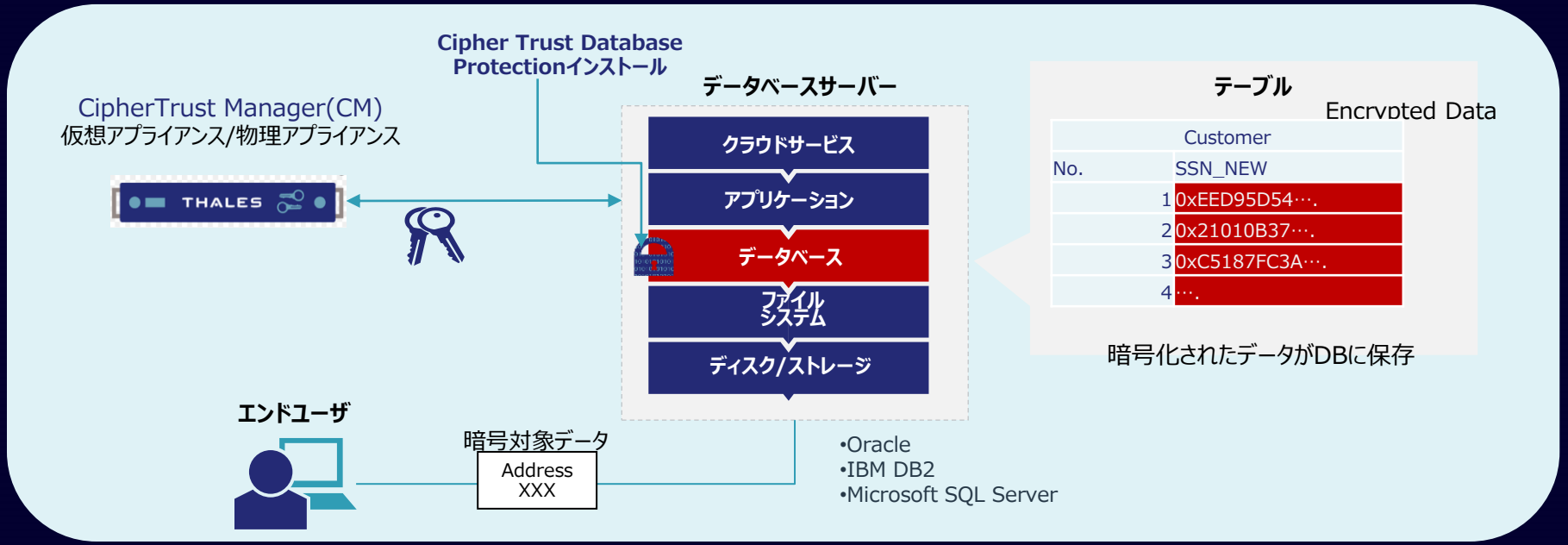
Protect

データベースレイヤでの暗号化と鍵管理

- カラム単位での暗号化
- アプリケーション側の変更は基本的に必要なし(要確認、POC必須)
- DBサーバにタレスが提供するSWをインストールすることでトリガーとビュー等が作成
- カラム単位数、暗号化対象カラムのデータ型等検討項目あり

システム構築例

- **コネクターをデータベースサーバーにインストール**
- **CMと連携**
- 暗号化対象のDB/カラムを選択
- 暗号化を開始

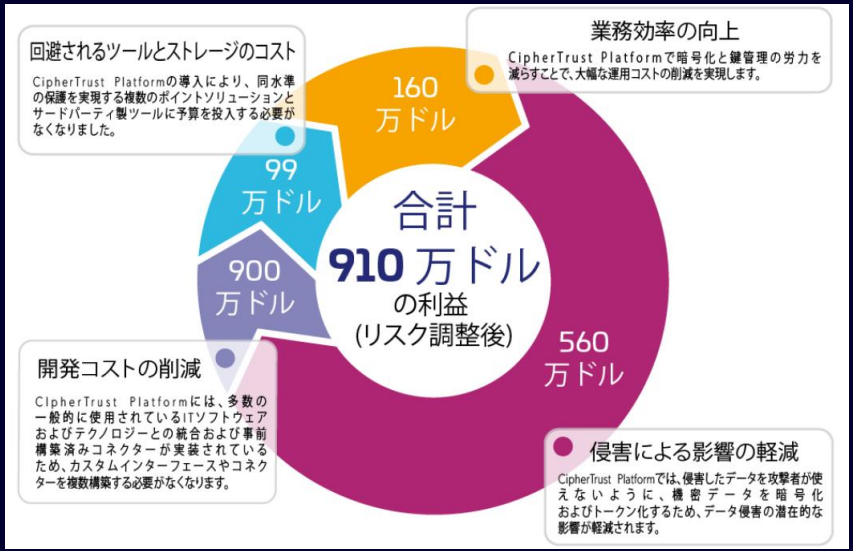


THALES

コストメリット

今回触れた運用面でのコストメリット

- GUIベースで鍵のライフサイクル管理
  - CipherTrustManager
- 自動での鍵ローテーション(Option)
  - CTE-LDT(特許取得技術)
- PCIDSS監査スコープの削減
  - Tokenization



CipherTrustによる総経済効果(Forrester)

- Forrester は、CipherTrust プラットフォームの財務上のメリットを
  3 年間で 910 万ドルと計算しました。
- これらの節約は、業務効率の向上、
  侵害による影響の軽減、開発コストの削減、
  回避されるツールとストレージのコストに起因すると考えられます
  - https://cpl.thalesgroup.com/ja/forrester-research-shows-economic-impact-ciphertrust-platform

THALES

ThalesのCDSPソリューションで対応できるPCI DSS要件

要件	PCI DSS	タレスが提供できる機能
カード会員データの保護	3.4/3.5/3.6	 透過的な暗号化 ファイル/DB  アプリケーション レベル暗号化  トークナイゼーション  マルチクラウド データセキュリティ  エンタープライズ 鍵管理
データ転送時の暗号化	4.1	 WAN 暗号化
カード会員データへのアクセス制限	7.2	 ポリシーベースのアクセス制御  ユーザー認証 デバイス認証
システムへのアクセス認証	8.1/8.3/8.7	 ユーザー認証 デバイス認証  ポリシーベースのアクセス制御  HSMによる 暗号鍵の保護
カード会員データへのアクセスログ	10.2/10.2/10.3	 データアクセス監査ログ  ポリシーベースのアクセス制御

ThalesのCDSPソリューション

CipherTrust Manager

鍵管理と暗号機能、各種ポリシー管理、監査ログ

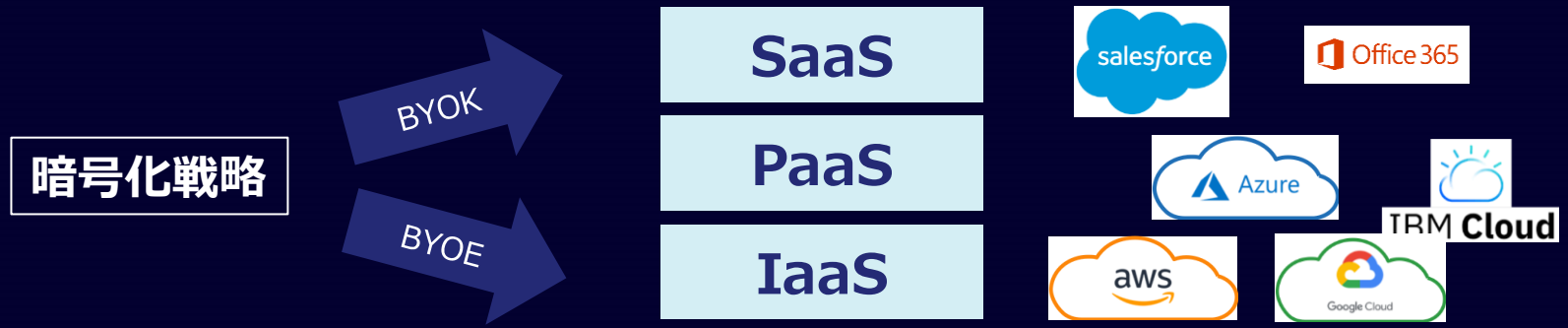
CipherTrust コネクタ

データ検知と分類	ファイル透過暗号とアクセス管理、ランサムウェア対策	データベース保護 TDEまたはカラム単位暗号	アプリケーションデータ保護/各種SDK	トークナイゼーション	鍵管理サーバ	マルチクラウド	各種シークレット管理
					KMIP		
データ検知	暗号処理とトークナイゼーション				鍵管理		シークレット管理

THALES

クラウドサービスにおけるデータ保護テクニック

- **オンプレミスと同様の暗号環境の持ち込み (Bring Your Own Encryption: BYOE)**
  - 暗号機能を利用者自身で用意し、クラウド上で実装・実行する
  - 機密性の高いデータに対するきめ細かい効率的な保護が可能
  - オンプレミスと同レベルのセキュリティ確保できスムーズな移行が可能
- **利用者自身で管理する鍵の持ち込み (Bring Your Own Key: BYOK)**
  - すべての企業データ資産を包括的に保護
  - クラウドが用意するネイティブ暗号機能を利用するが、暗号鍵自体は利用者自身で用意して管理
  - HYOK等の技術も一部クラウドサービス事業者が提供開始



THALES

まとめ

強力な暗号化技術には鍵管理が必要

- 鍵のライフサイクルも考慮するべき

暗号化のハードルは高くない

- 暗号化の検討時はタレスへご相談ください

暗号化と暗号鍵の管理はコストメリットもある

THALES