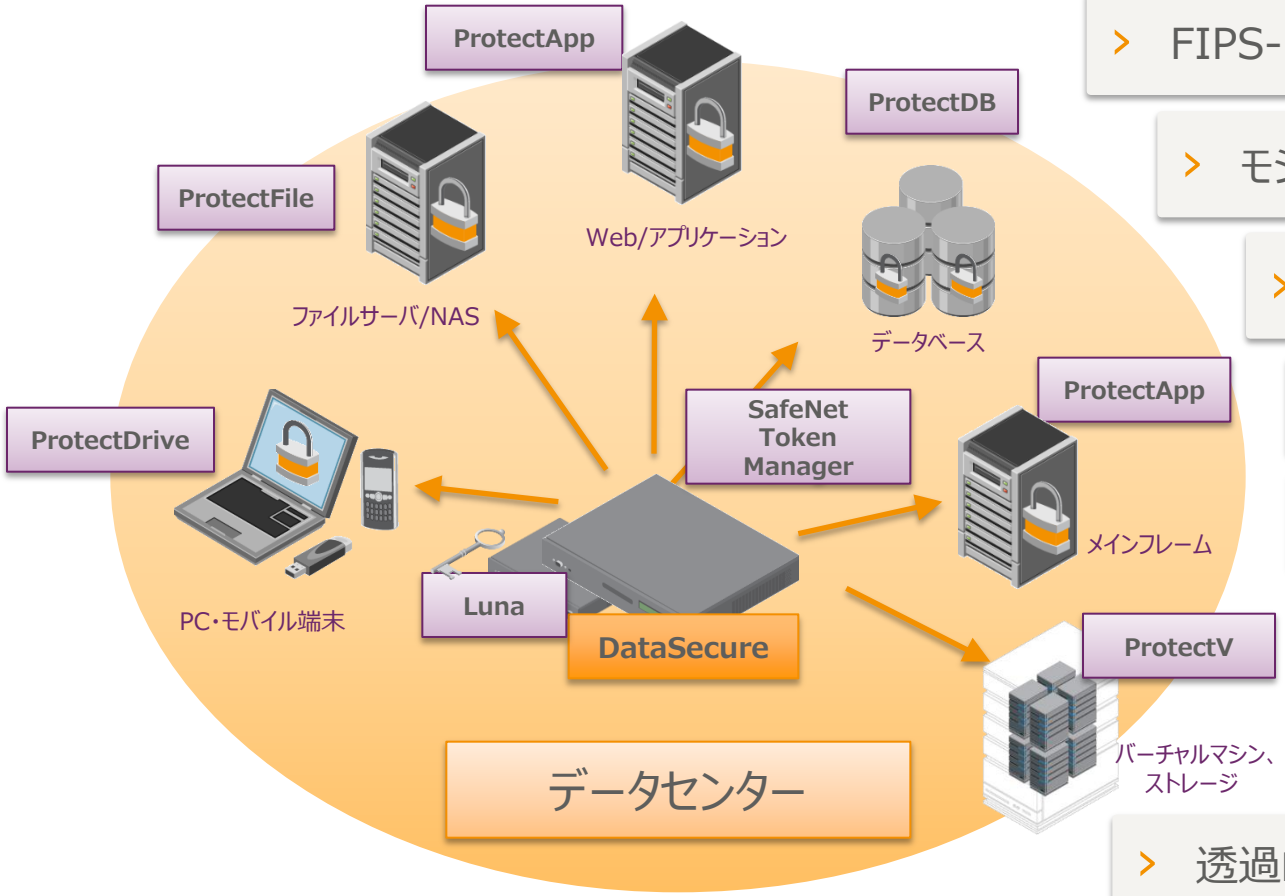
SafeNet DataSecure

オンプレミスからクラウドまでのデータ保護を可能にする

日本セーフネット株式会社
エンタープライズセキュリティ事業部

ライフサイクル・データ・プロテクション製品一覧

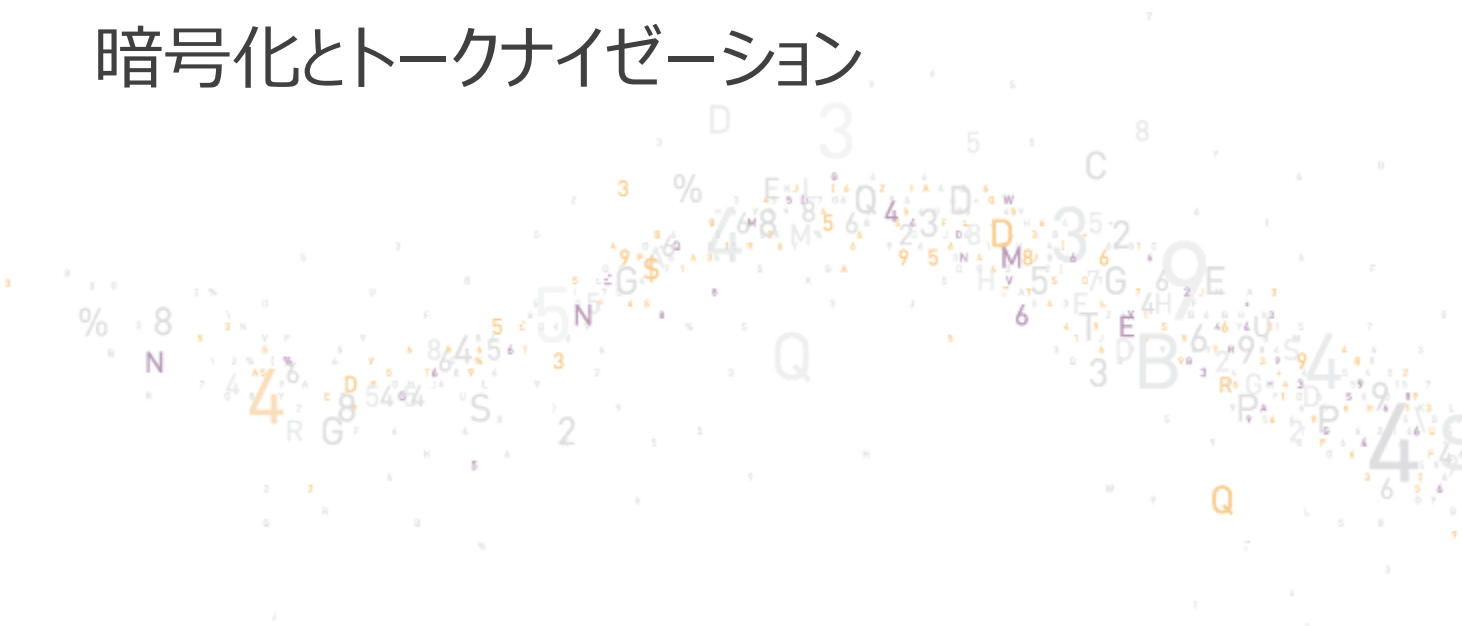


- FIPS-1402 level3 HSM機能内蔵
- モジュール形式での暗号機能提供
- 最大100,000暗号処理/秒
- 様々なコンプライアンス対応
- クライアント-サーバの保護
- 内部統制の徹底管理
- 400社以上での実績
- 透過的なトークナイゼーションの対応
- データ保存領域に対する内部統制・鍵管理デバイス

Agenda

- 暗号化とトークナイゼーション
- クラウドでのセキュリティ

暗号化とトークナイゼーション



Tokenization（トークン化、トークナイゼーションとは）

TokenizationはDB暗号化以上にセキュアなデータ保存方式です。

- クレジットカードデータを無作為なトークンに置き換える
- 業務アプリケーションはトークンを使用するため、暗号化データアクセスに比べ処理が軽い
- 実データが必要な場合のみ暗号化済みクレジットカードデータにアクセス
- 大部分のカードデータアクセスがトークン化されることでPCI-DSSの対象から外れ、結果としてセキュリティ強度を上げながら**コストメリットが受けられる**

Tokenizationを後押しするもの

従来のDB暗号化の課題

- 暗号化によりデータは保護されるが、すべての鍵アクセスについてはアクセス制御がしかるべき形で取られる必要がある
- 監査についてはすべての鍵アクセスに対するログ提出が求められる
- 暗号鍵の管理
- 業務アプリケーションにおいては復号されるため、通信におけるセキュリティ対策も必要不可欠

PCI-SSC

- トークン化による監査負荷軽減の考慮（Emerging Technologyとして紹介）
- ガイドラインのリリース予定あり

VISA

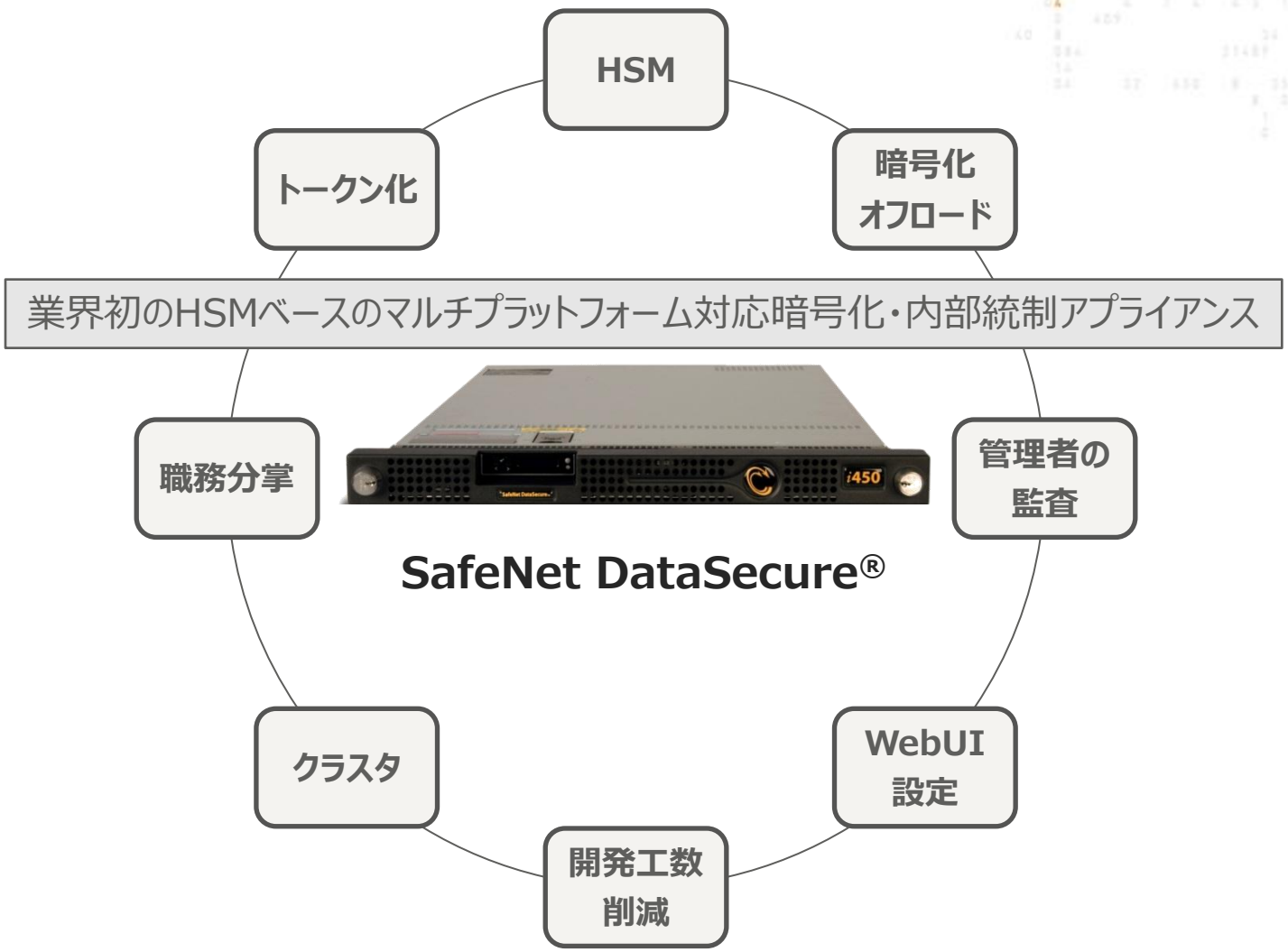
- Best Practices for Tokenization Version 1.0 リリース（2010年７月）
- 理想的なトークン化インプリ基準について言及

PCI-DSS カバレージ

1. F/Wの導入の適切な設定
2. パラメータの適切な設定
3. 機密データの保護
4. ネットワーク転送における暗号化
5. アンチウイルスの導入と更新
6. システムの開発とメンテナンス
7. 必要最小限のデータアクセス権限
8. 各個人へのID付与
9. 機密情報への物理アクセス制御
10. 機密情報アクセスの監視
11. システムの定期的なテスト
12. 内部統制の見直し

- 暗号化とアクセス制御、暗号鍵の管理が重要
- 対応には一般的に1000万～以上の費用がかかる
- QSAによっては監査レベルが異なる場合も

暗号化＋鍵管理＋職務分掌＝DataSecure



SafeNetのDB暗号化

DB暗号化＋HSM

- **既存アプリケーションに対し透過的**：インストーラーによる暗号化機能の統合
- **暗号化アプライアンスによる暗号処理オフロード**：DBに負担をかけない設計
- **HSMによる鍵管理とライフサイクル管理**：オンライン鍵交換のサポート
- **ハードウェアによる職務分掌の徹底**：特権ユーザに対する強制力発揮

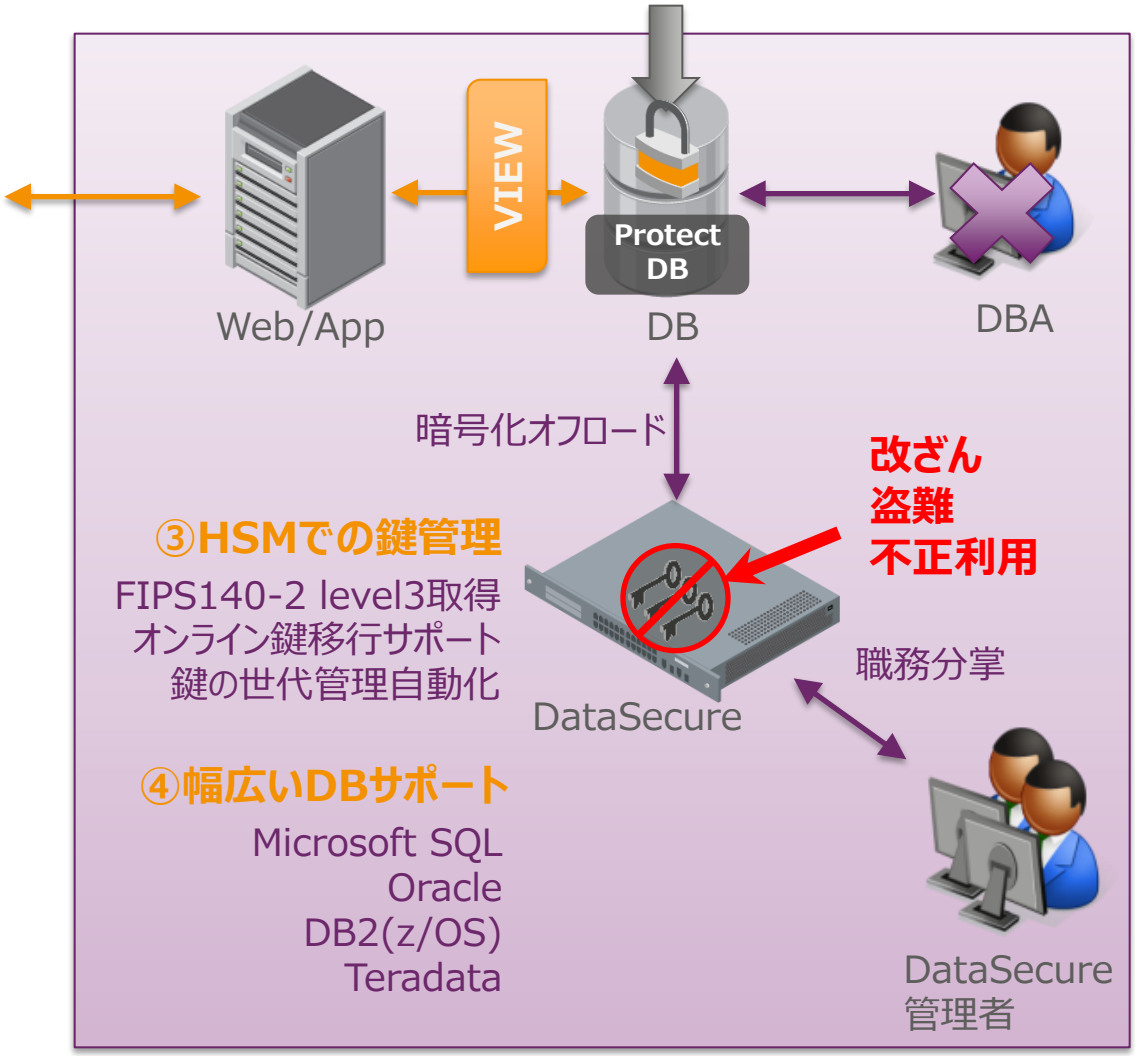
トークン化＋HSM

- **フォーマットを変えないトークン化**：既存アプリケーション改修影響が少ない
- **VISA Best Practiceに対する網羅性**：単一のソリューションで理想的なトークン化実装
- **HSMによる鍵管理とライフサイクル管理**：Data Vaultの完全な保護
- **ハードウェアによる職務分掌の徹底**：特権ユーザに対する強制力発揮

DB暗号化＋HSM

①アプリケーションに透過的な暗号データアクセス

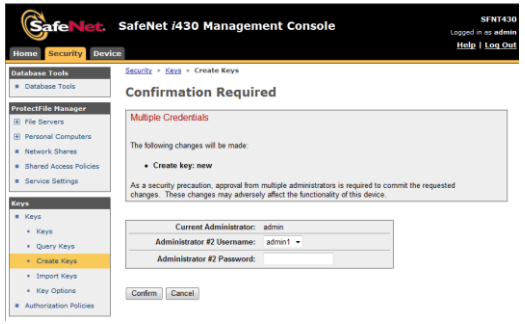
Fmqjper1m+j54!f@passu1a4jq&



	Employee#	Name	Salary
1	1	横浜太郎	NULL
2	2	港花子	NULL
3	3	根岸次郎	NULL
4	4	金沢八郎	NULL
5	5	神奈川一	NULL
6	6	私鉄社長	NULL
7	7	小泉順次郎	NULL
8	8	上大岡翔子	NULL
9	9	安全第一	NULL
10	10	正給勤	NULL

②データのマスキング

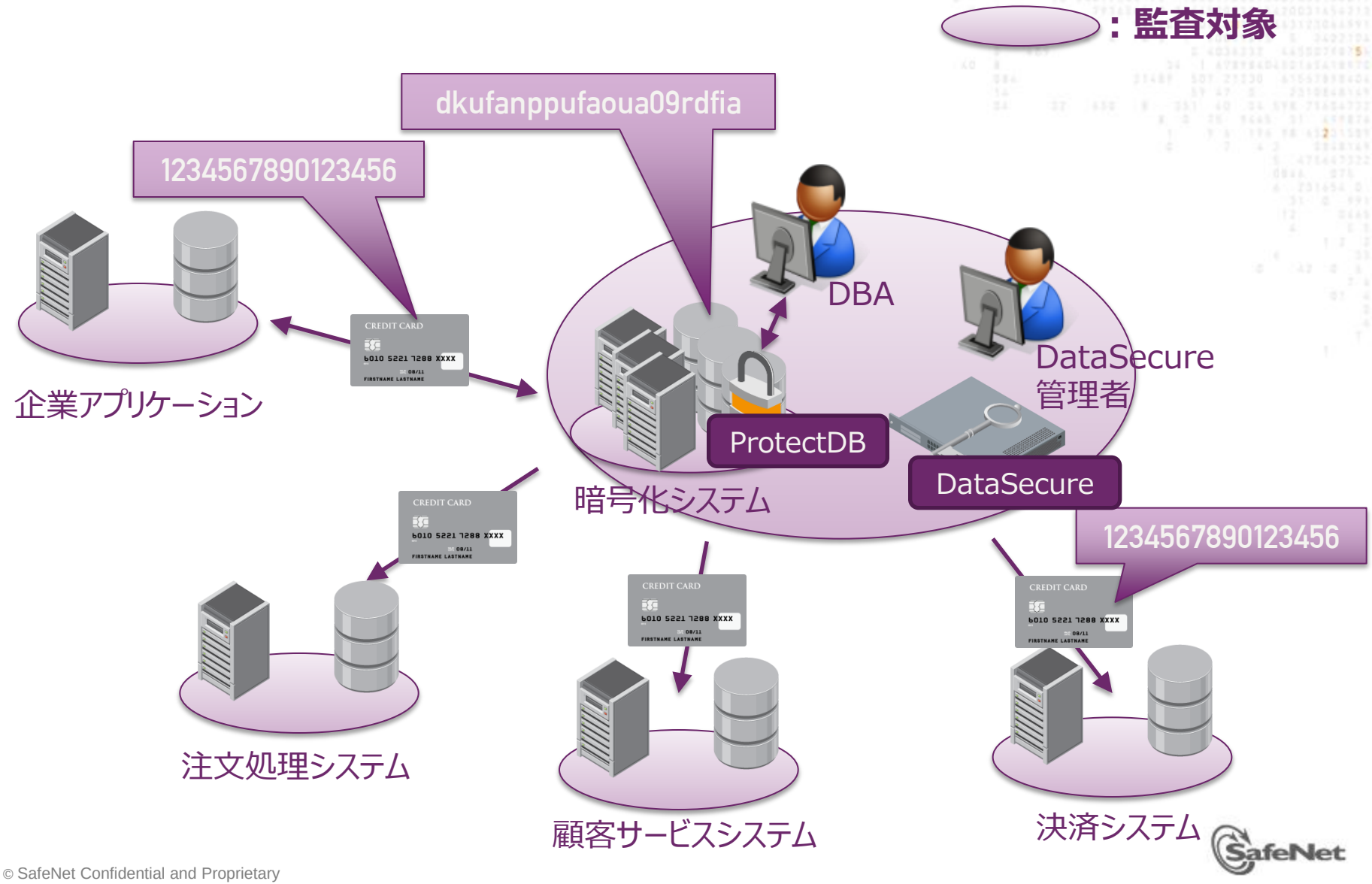
内部DBAの目視によるデータ漏洩を防御



⑤管理者の職務分掌機能

設定変更に複数の管理者認証

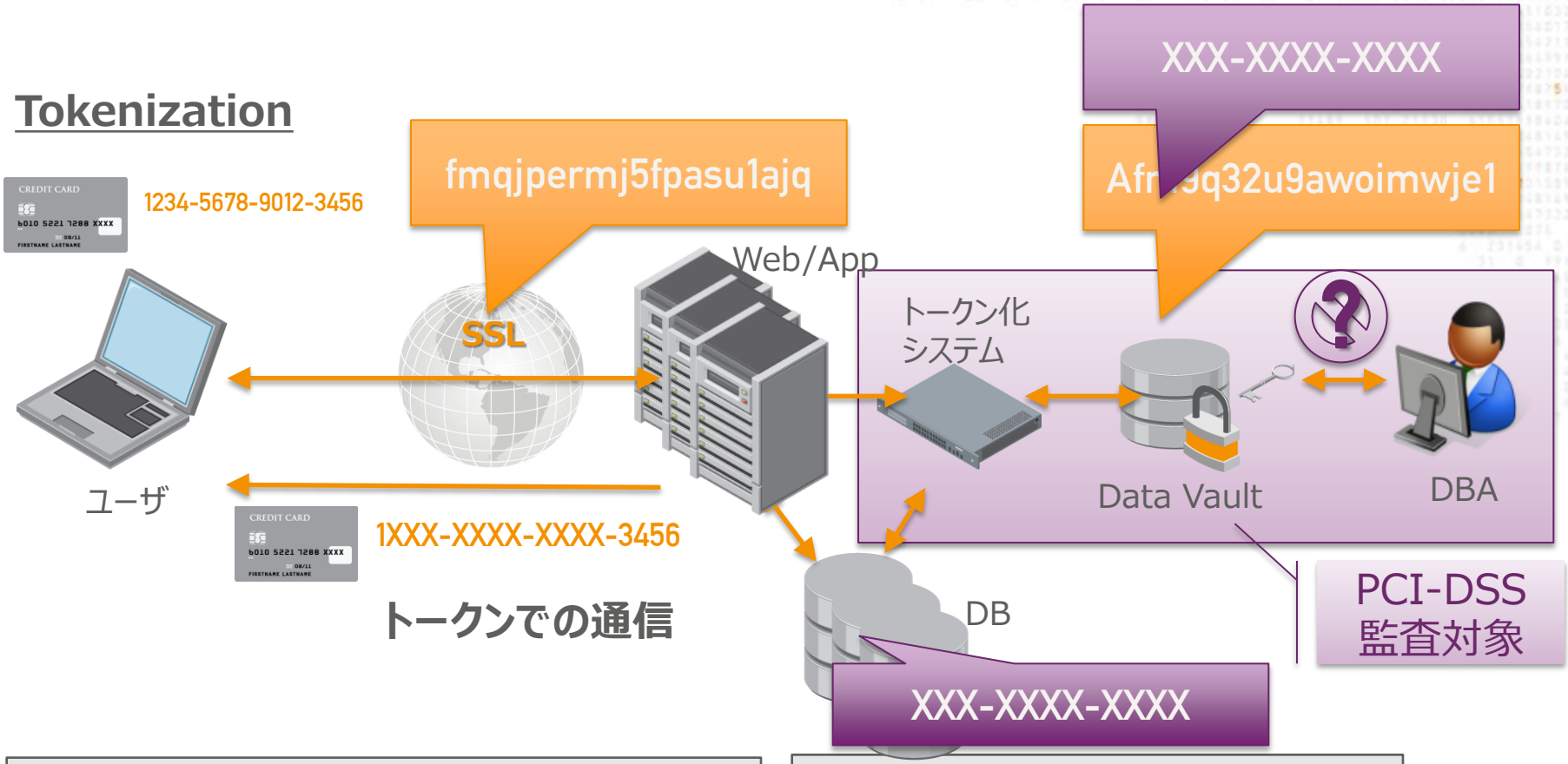
DB暗号化のPCI-DSS監査範囲



SafeNet ProtectDBの利点

1. PCIコンプライアンスを確保してセキュリティ強化
2. アプリケーションに対し透過的な暗号化
3. セキュリティ管理および運用の簡易化
4. DBAに対するマスキング
5. オンラインでのデータ移行対応

トークン化イメージ



理想系

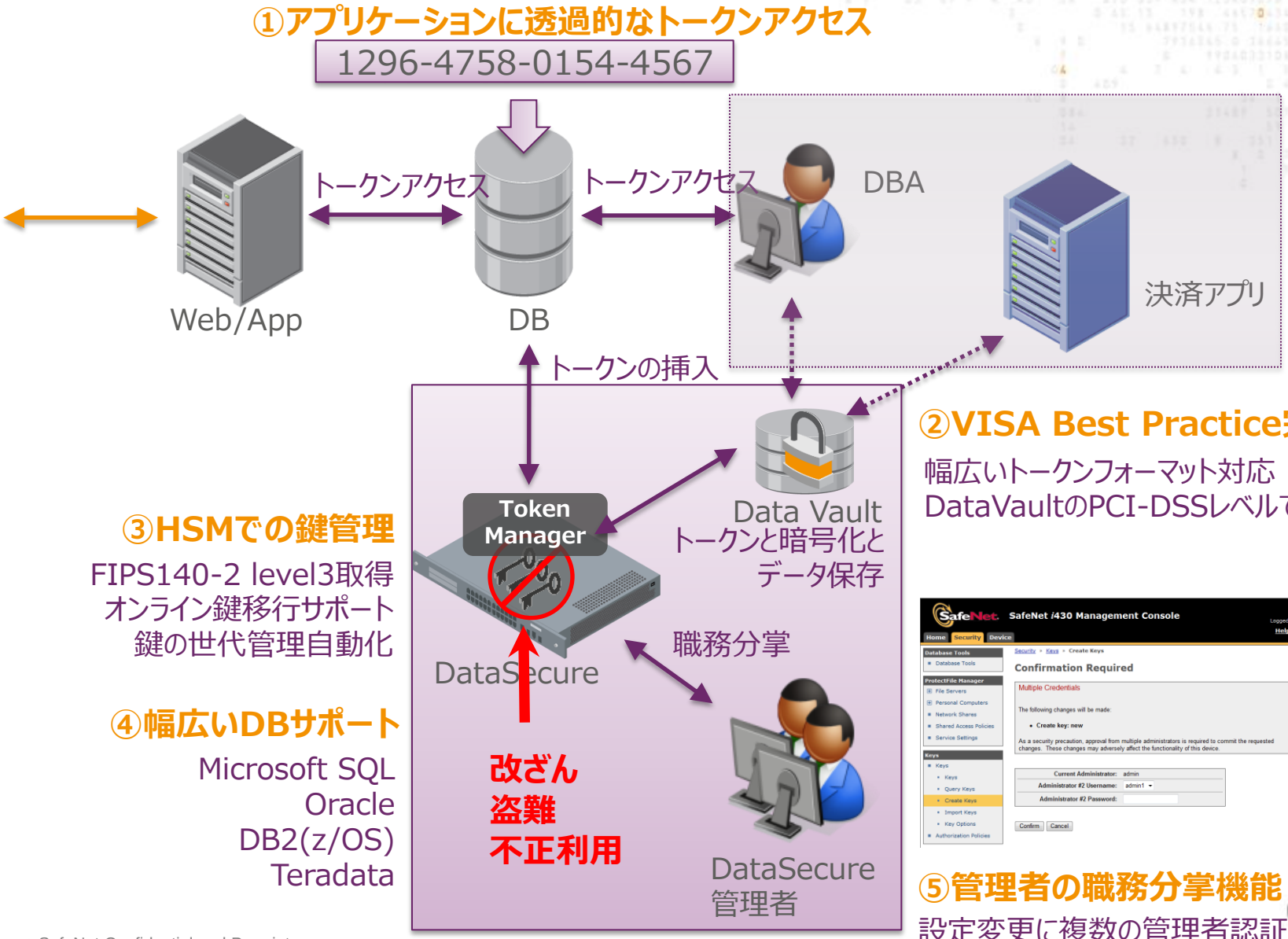
- 機密データの置き換えによる監査負荷軽減
- システムのセキュリティ強度アップ
- 軽いトークン処理

懸念点

- DBAによる不必要なデータアクセス
- 鍵の物理管理・アクセス管理
- 既存環境への組み込み

トークン化＋HSM

①アプリケーションに透過的なトークンアクセス



②VISA Best Practice完全準拠

幅広いトークンフォーマット対応
DataVaultのPCI-DSSレベルでの運用

③HSMでの鍵管理

FIPS140-2 level3取得
オンライン鍵移行サポート
鍵の世代管理自動化

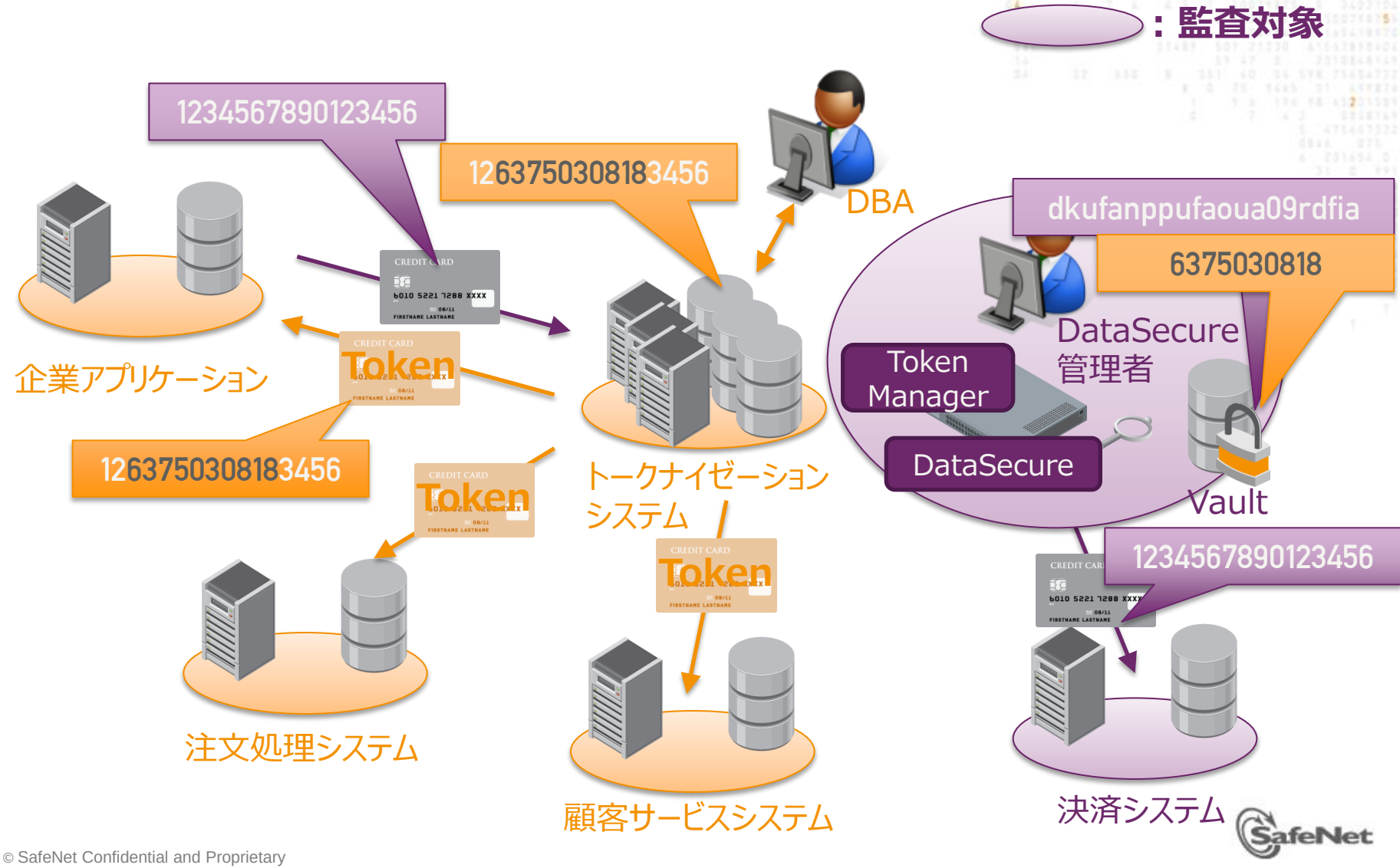
④幅広いDBサポート

Microsoft SQL
Oracle
DB2(z/OS)
Teradata

⑤管理者の職務分掌機能

設定変更に複数の管理者認証

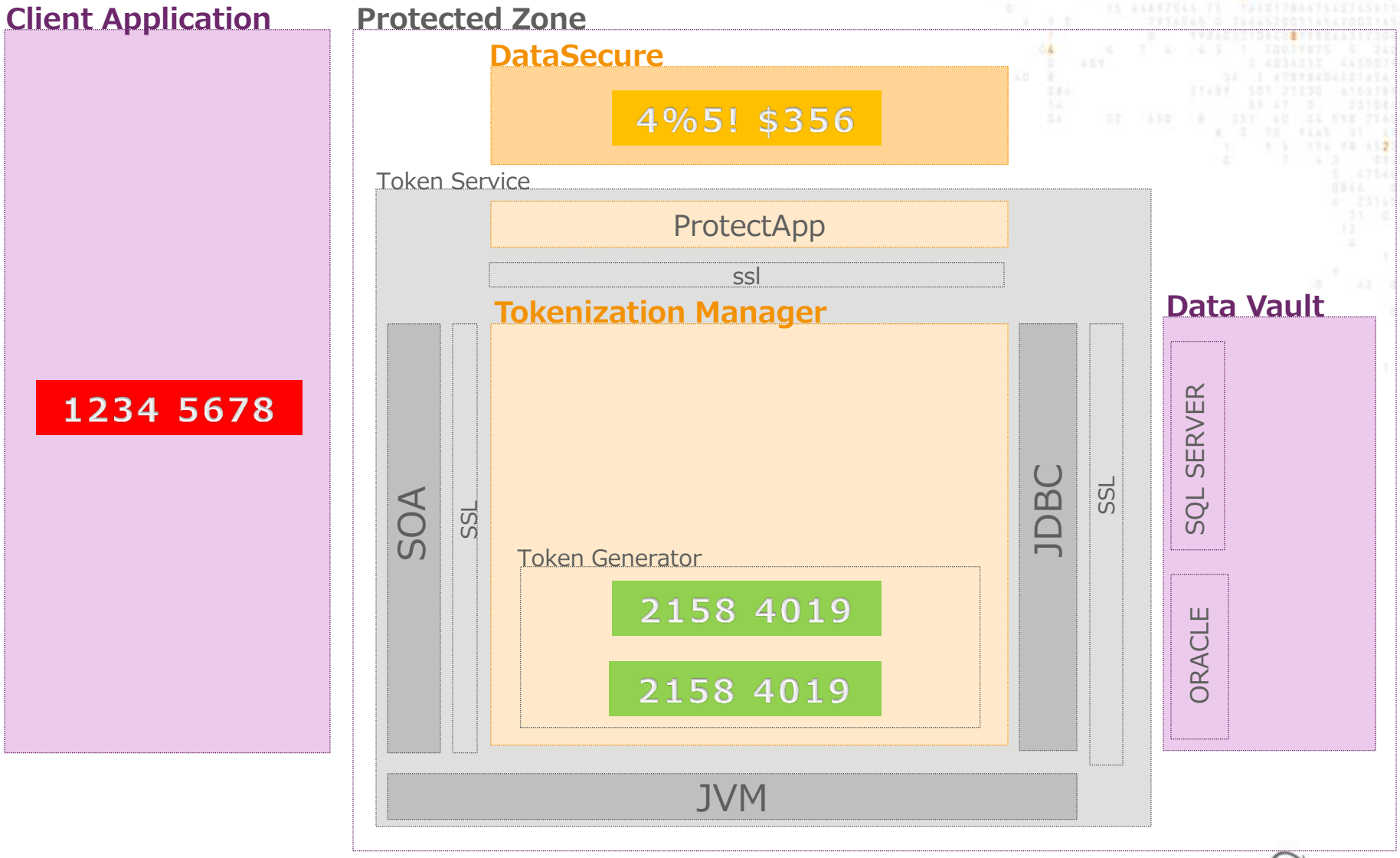
トークナイゼーションのPCI-DSS監査範囲



SafeNet Tokenizationの利点

1. PCIコンプライアンスを確保してセキュリティ強化
2. 監査コストの削減の実現
3. セキュリティ管理および運用の簡易化
4. VISAベストプラクティスとの整合性
5. 既存環境への影響少・パフォーマンスの最適化

トークン化フロー



トークンフォーマット一例

クラウドでのセキュリティ

クラウド上でのセキュリティ

データ保護の境界

- 組織が物理アクセス権を管理
- 組織がOSスタックを管理
- 組織がアプリケーションスタックを管理

境界線をいかに制御するかが今までのセキュリティ対策

- 境界線の物理アクセスコントロール
- VLANs, Firewalls, IPSのコントロール
- パッチ管理、コードの確認、アプリケーションのセキュリティ対策

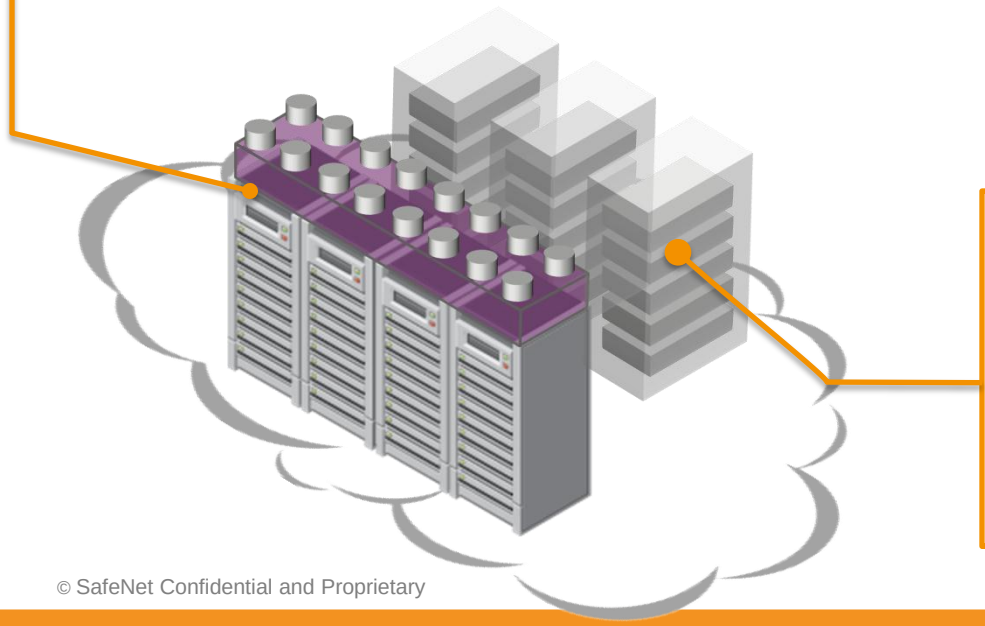
クラウドには境界線が存在しない

- 物理アクセス、スイッチファブリック、OS、アプリケーション等はクラウドプロバイダーが管理
- アプリケーションデータはクラウド上で作成・削除される
- セキュリティ制御を可視化できない（されない）
- クラウドプロバイダーを管理する法・規制が存在しない

クラウド上のデータに対する懸念

仮想化インスタンス

- 仮想化されたサーバ、アプリケーション、データベース
- 機密データ保存に適しない入れ物
- 無制限にコピーされる危険性
- ブルートフォース攻撃にさらされる危険性



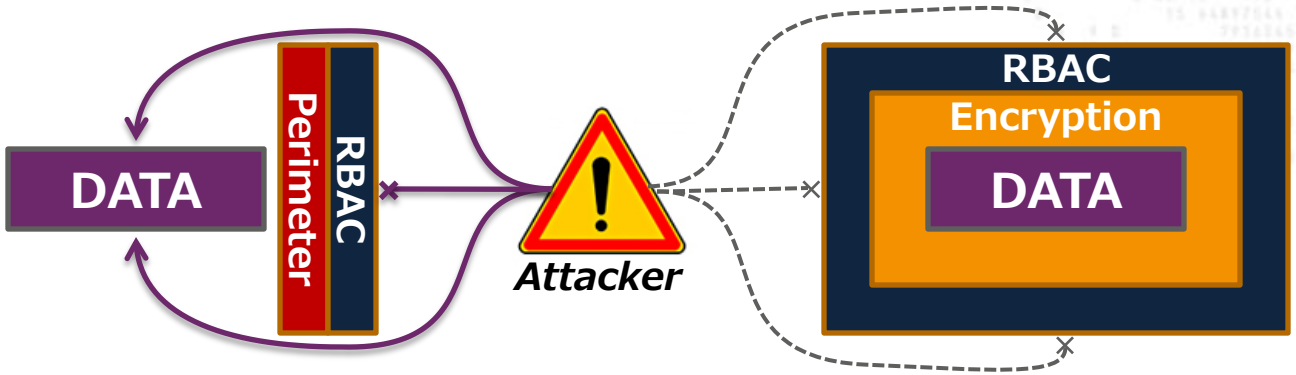
クラウド上のデータは…

- マルチテナント環境に置かれるかもしれない
- クラウド管理者に操作されるかもしれない
- 移動・コピーされるかもしれない
- 法規制外に置かれるかもしれない
- データの破壊や曖昧な保管を受け入れなければならない

仮想化ストレージ

- 情報漏洩にさらされる危険性
- クラウド管理者にアクセスされる危険性
- 管理者の設定ミス等によるデータ漏洩の危険性
- クラウド側暗号化サービスは職務分掌や監査上の問題を引き起こす

コンプライアンスとセキュリティ



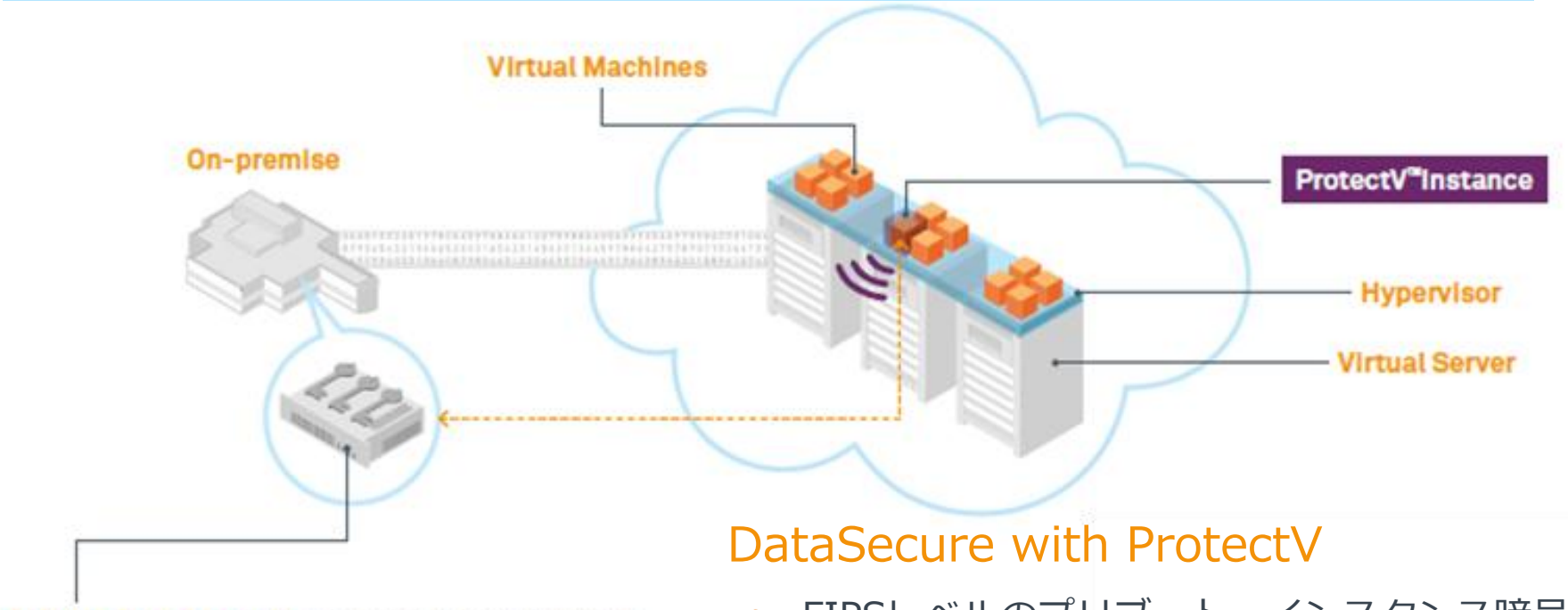
> **データ周辺に対するセキュリティ**
- これらのソリューションではデータ自信を保護できない
- 設備投資を減らすことはできない
- 継続的に漏洩の危険性があり、監査にも通らない
- クラウドには適用てきない

> **データの暗号化は、データに対するセキュリティに直結する**
- データを直接的に保護
- 職務分掌の解決
- マルチテナント環境問題の解決
- 監査対象の削減が可能

> **情報漏洩問題の解決**
- 漏洩対象の範囲を縮小
- ほとんどの法律・規約について準拠が可能となる

SOLUTION

クラウド上の仮想マシン保護



DataSecure with ProtectV

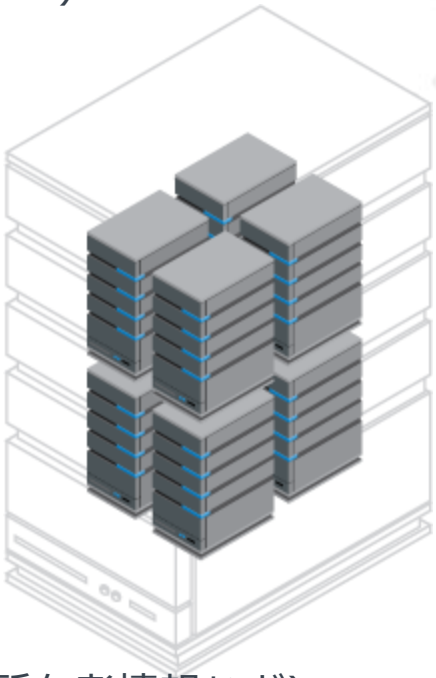
- FIPSレベルのプリブート・インスタンス暗号化
- セキュアなログインインターフェース（HTTPS）
- パスワード・OTP・証明書認証対応
- イベントのロギングおよびアクティベーションの通知
- 機密データ・インスタンスの保護

SOLUTION

お客様事例: Amazon Web Services

クラウドにおけるPCIコンプライアンス2.0対応

- サーバおよびストレージベースの暗号化をAmazon Elastic Compute Cloud (EC2) およびAmazon Virtual Cloud (Amazon VPC)上にて実現
- PCI-DSS 2.0レベルのデータ暗号化と制御を提供



サーバベースの暗号化

- インスタンスのラウンチ時における認証と承認を制御することで、仮想サービスにおけるホストレベルの管理を提供

ストレージベースの暗号化

- ブロック単位のストレージボリュームを保護し、コンプライアンス上対象となる情報を保護 (PIIやカード所有者情報など)

SafeNet 仮想化インスタンス・ストレージの保護

SafeNet ProtectV™はサーバおよびストレージレベルの暗号化を実現し、ユーザはコンプライアンスが必要となるデータをクラウド上の仮想マシンやストレージで利用することが可能になります。

ProtectV™Instanceにより、ユーザは仮想サーバ全体をセキュアに暗号化し、それらリソースが漏洩することを防ぐことが可能となります。

ProtectV™Volumeにより、クラウド上の仮想ストレージ内に含まれるファイルやフォルダのデータを暗号化することが可能となります。

ProtectV™ Managerにより、クラウド・セキュリティを大規模に、そして素早く適用することが可能となります。

主な機能:

- データの隔離
- 職務分掌
- 大規模エンタープライズ対応
- クラウドコンプライアンスの実現
- ラウンチ前の認証
- マルチテナント環境下での保護

信頼できるクラウド基盤の提供

SafeNetはクラウドユーザおよびクラウドベンダーに対し様々なセキュリティソリューションを提供しています。

- 社内利用の認証トークンをSaaSアクセスIDに統合
- クラウドのインスタンスやストレージの暗号化
- クラウドアプリケーションやデータベースの暗号化
- 安全なクラウド上でのライセンス管理・発行