SafeNet | THE DATA PROTECTION COMPANY

スキのないデータベースセキュリティの実装方法

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 シニアセキュリティエンジニア
髙岡　隆佳

30th ANNIVERSARY three decades strong

まずIT管理者に聞きました

ここ3年以内に自社で情報漏えいする気がする？

はい：66%

1/5は自社ネットワークを信頼していない

**Based on a SafeNet Survey of 230 security professionals.*

まずIT管理者に聞きました

境界線防御は機能してますか？

もちろん！：74%

すでに破られた：31%

**Based on a SafeNet Survey of 230 security professionals.*

まずIT管理者に聞きました

境界線が破られた場合、データ漏洩防げますか？

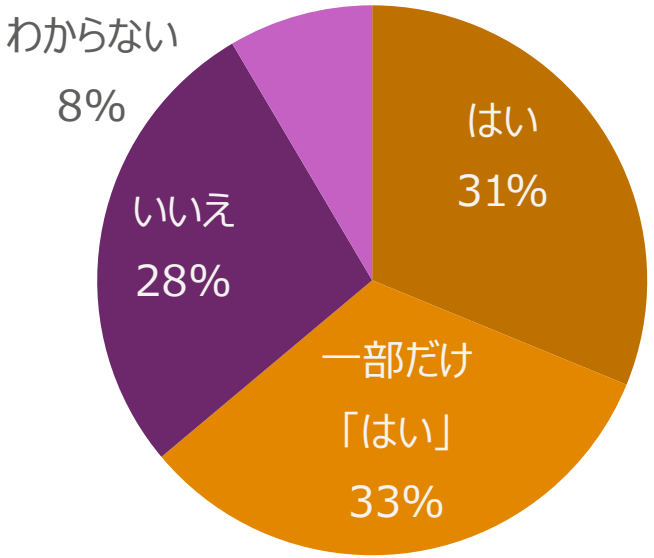
ユーザの皆さんすみません
持っていかれちゃいます
：59%

**Based on a SafeNet Survey of 230 security professionals.*

今度はDBAに聞きました

機密情報を格納する表・ビューなどの情報に対して、ユーザの業務に必要な最低限のアクセス権に限定して設定されていますか？

気にしてません：36%

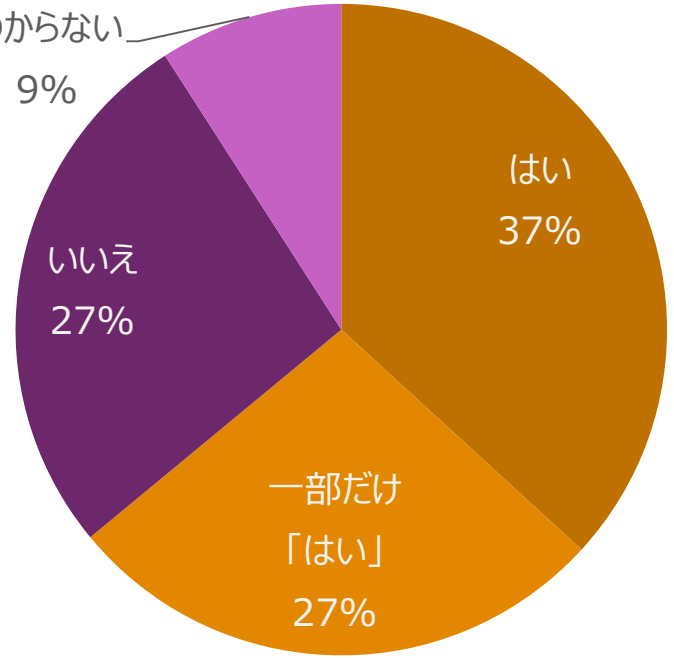


*Based on DBA実態調査WGによる管理者に対する独自調査

今度はDBAに聞きました

データベースの操作履歴・アクセス履歴をログとして取得していますか？

気にしてません：36%

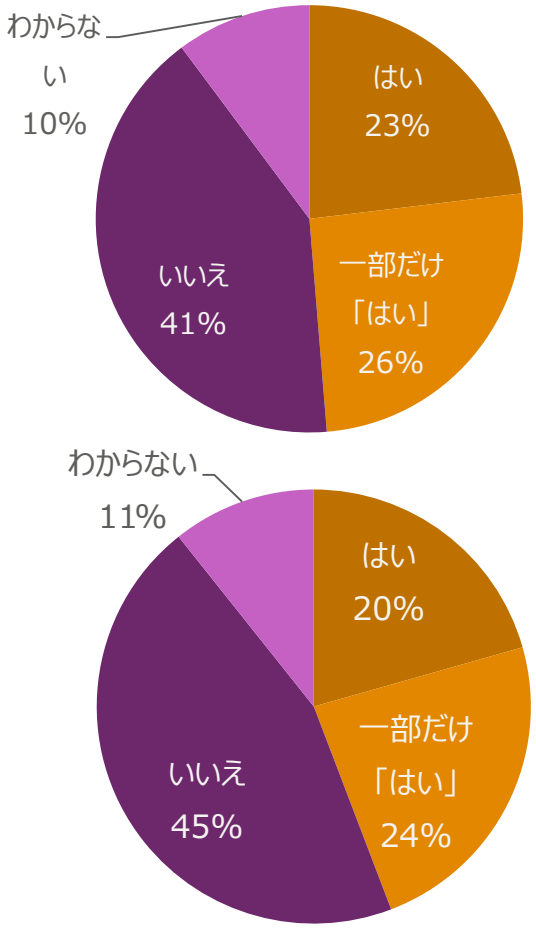


*Based on DBA実態調査WGによる管理者に対する独自調査

今度はDBAに聞きました

重要な機密情報などを暗号化機能・製品を使って暗号化していますか？

平文です：43%



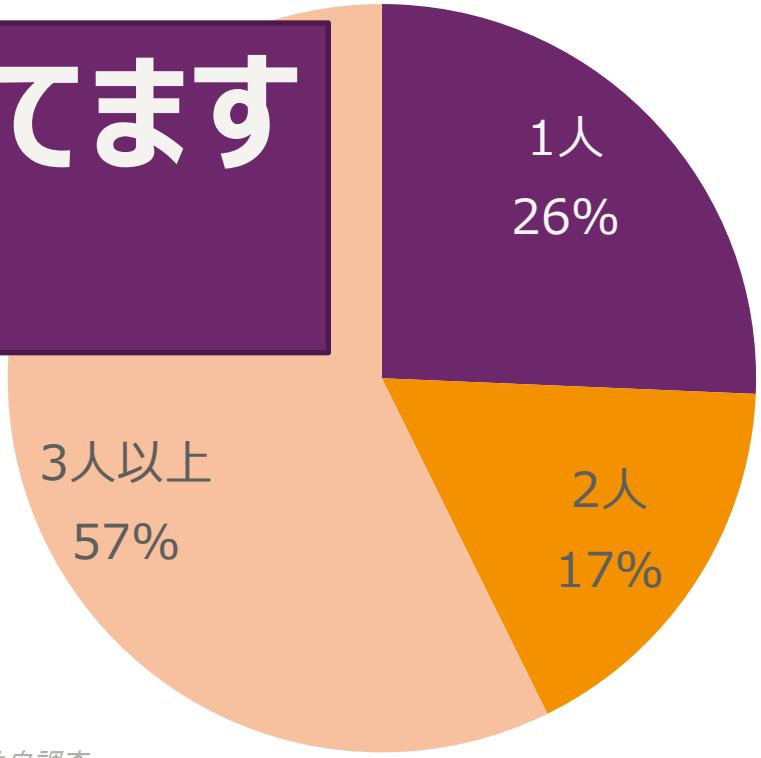
*Based on DBA実態調査WGによる管理者に対する独自調査

今度はDBAに聞きました

暗号化している環境でも・・・

-あなたの組織または会社にDBAは何人いらっしゃいますか？

一人で運用してます：25%



*Based on DBA実態調査WGによる管理者に対する独自調査

守るべき境界線の移行

いままでの境界線（社内・社外）防御は不十分

→漏洩は起きうるもの

→環境に応じて必要な準備は異なる

→共通するのは「データ」を境界線として対策を施すこと

ベストなDBセキュリティを考える

考えうるすべての対策を取る必要がある

- PCI-DSSは模範的なDBセキュリティ・ガイドライン

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

＝実装コストがかかる（アプリの改修、DB暗号化のライセンス、工数、等々…）

求められるソリューション

データそのものを守るアプローチ ＝ 暗号化

ただしPCI DSS準拠と事件後の対応比較：**2.65倍**

日本クレジットカード協会ではLevel1/2加盟店に対して対応期限を設ける

DB暗号化市場の動き

PCI DSSを中心としたECサイト等での対応増

- コストに応じた暗号化手法の選択とそのリスク掌握が必要
- レベル1加盟店ではトークナイゼーション適用も視野に
- TSP（Tokenization Service Provider）による中小企業でのPCI DSS適用も視野

個人情報保護「高度な暗号化」への適合

- 漏洩に対するリスクの回避
- 何を持って高度な暗号化とするかはグレー（法第20条）
  - 電子政府推奨暗号リスト又はISO/IEC18033に掲げられている暗号アルゴリズムによって、記録媒体内の個人情報の保存先として利用可能な全領域が自動的に暗号化されること。
  - 暗号化された情報及びその暗号化された情報を復号させる復号鍵の管理が適切にされていること。
- 十分な強度の暗号アルゴリズムの採用・暗号鍵に対する物理的保護・鍵への厳格なアクセス制御・管理者への管理・監査導入は必須

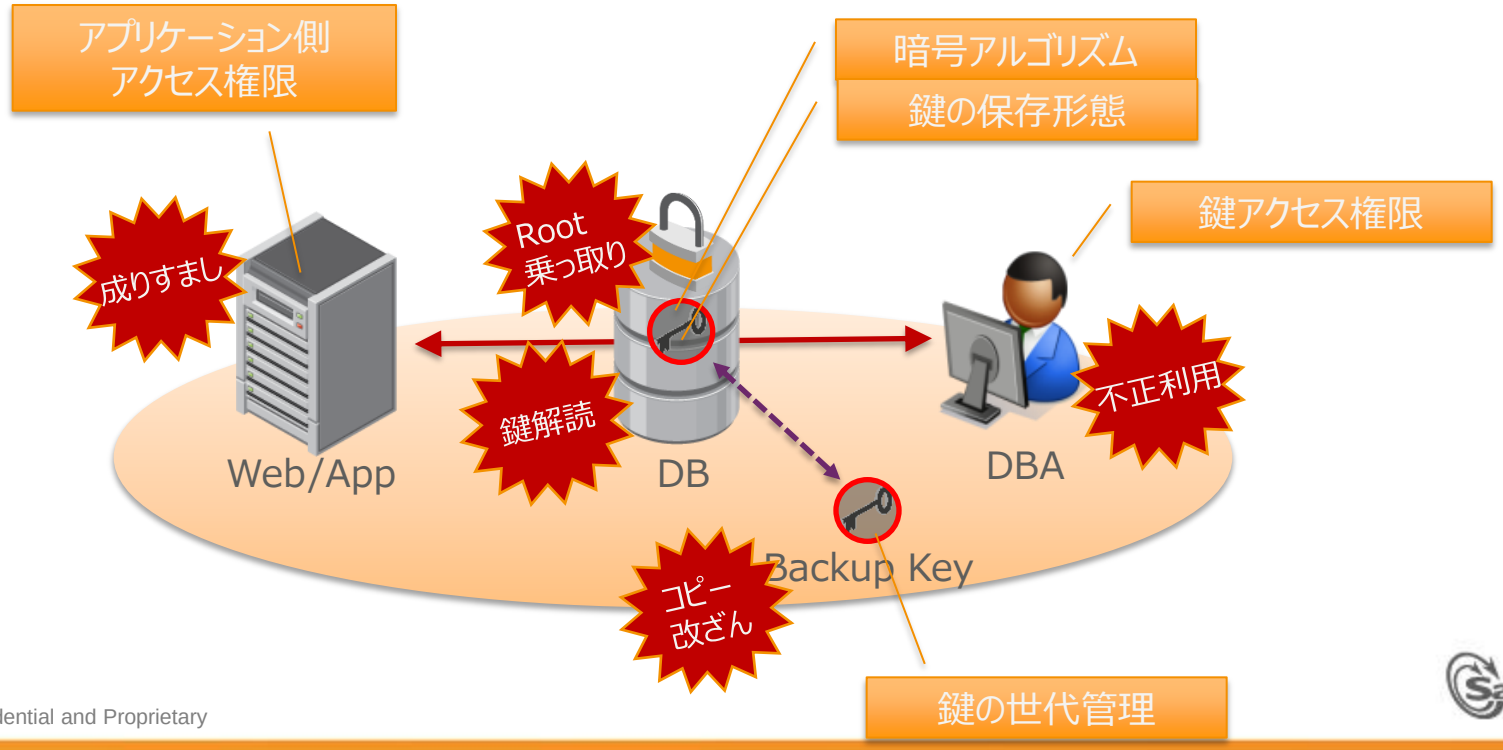
DBもクラウドへ

- AzureやAWSを始めクラウド上でDBサービスの提供が活発化
- 混在環境でのデータ保護をどうするか
- 暗号機能の提供レベル（ユーザではなくクラウド側依存）
- 暗号鍵のコントロールをクラウドないしはオンプレで実行するスキームの提供はじまる

暗号化のコンポーネント

暗号強度＝アルゴリズム強度ではない

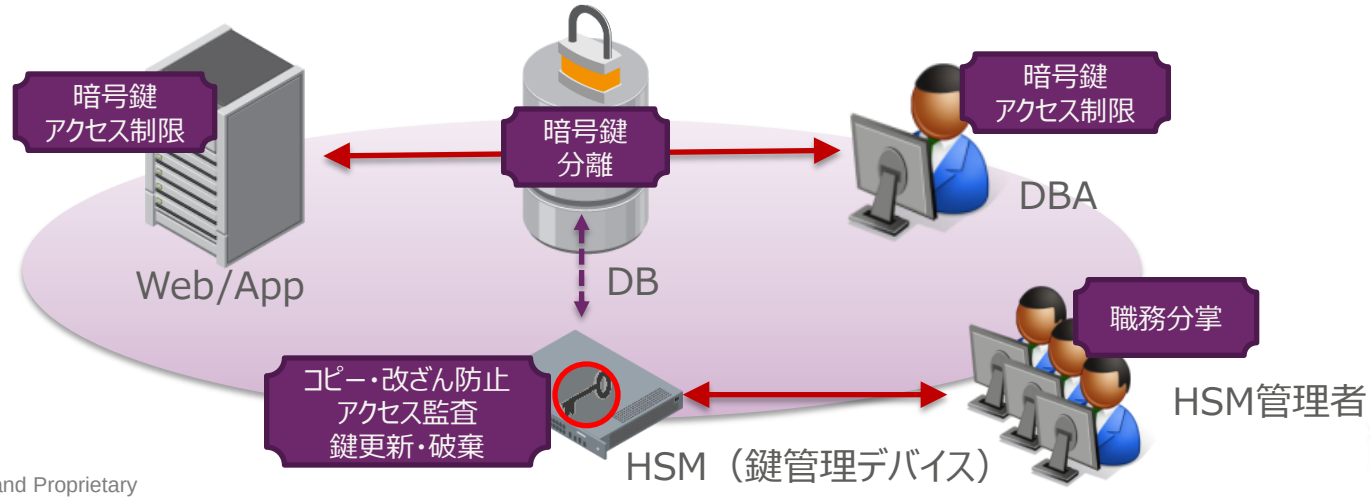
- 大事なのはアルゴリズムよりも「鍵」そのものに対する管理
- 鍵へのフルアクセスを1人の管理者に与えるのは危険
- 暗号データと鍵の同一プラットフォームでの管理はリスク



暗号化のコンポーネント

データと暗号鍵が別管理のケース

- データと鍵が別管理のため、DBAの権限を不正に利用されたとしても暗号鍵は別ポリシーで保護可能
- 指定時間当たりの鍵利用回数や、アクセス時間帯の制御をかけることで、管理者からの不要・不正なアクセスを排除
- 鍵管理者に職務分掌を強制させることで単一の管理者では各管理機能を実行させない（不正な操作を防御）
- 承認されたアクセスのログ監査を手元で取ることが可能
- 鍵を消去することでデータが復号されないことを保証可能（デジタルッシュレディング）



暗号化の効果

暗号化＝暗号化されていないデータとの分離→漏洩対策

効果は鍵の強度、管理手法に依存する

- 鍵が誰にでも（管理者含む）アクセスされては暗号化の意味がない
- 必要なときに必要な人が必要な分だけ鍵にアクセス
  - 鍵に対するユーザ（管理者）アクセスポリシーはどうする？
- 暗号鍵が安全で完全性を保たれなければならない
  - 暗号鍵の適切な保存・管理をどうする？

鍵管理とアクセス制御が正しく設定されると・・・

- 物理的な漏洩に効く！（HDD持ち出し、ベーステーブル持ち出し）
- 内部不正に効く！（特権ユーザによる職権乱用）

注意点

- 管理者の権限を最小限に運用することが大事
- 成りすまし、セッションハッキングがされないよう前段での対策（WAF等）も必要

HSMでの鍵管理

信頼できるハードウェアへの保存

- どのような形でも鍵がHSM外に保存されることはない
- バックアップテープやドライブの監査は不要

鍵をマスター鍵で暗号化

- 物理的な攻撃が発生すると、不正利用防止対策が起動

MofN認証で不正な運用を排除

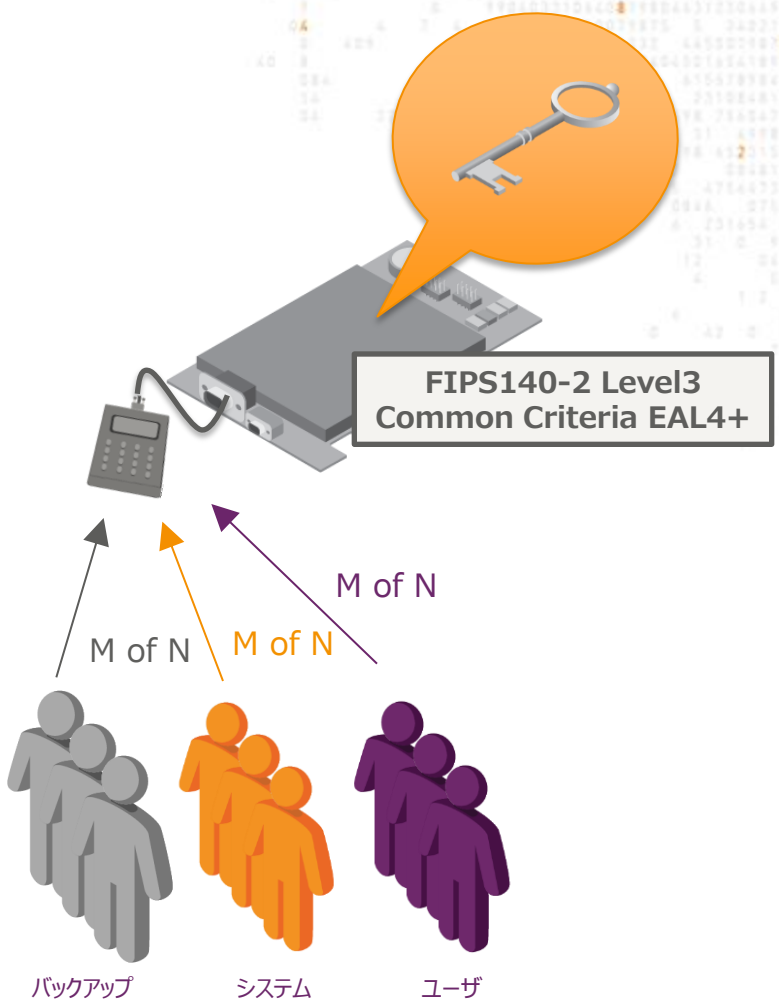
- ユーザおよびRoleごとに異なる物理的に安全なインターフェースを使用した認証システム

鍵のセキュアな運用の自動化

- 世代を通じた鍵更新
- 暗号データ破棄＋鍵の破棄

暗号鍵と暗号データの分離

- 暗号鍵の正当性が保証されてこそ



暗号化モジュールの強度

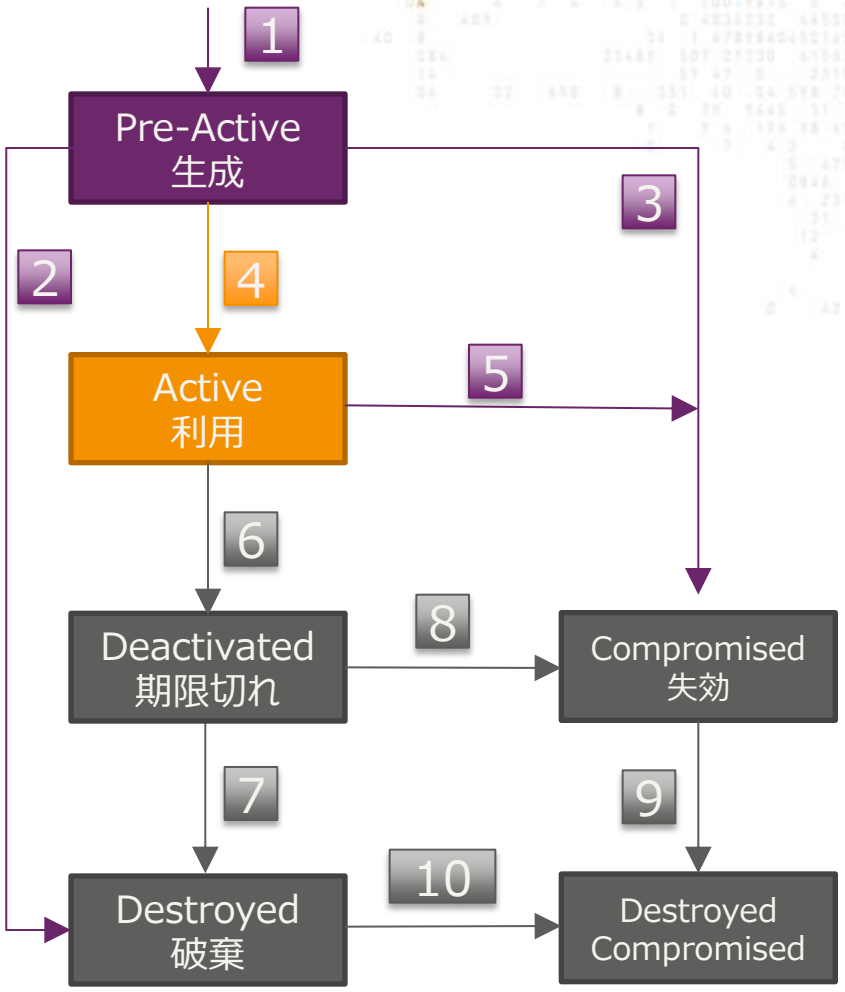
FIPS140-2とは？

- 米国政府主導にて制定された暗号モジュールにおけるハードウェアおよびソフトウェアの要件
- 取得にあたり、NIST等第三者外部監査機関の技術的攻撃に耐える必要があるため、未取得製品より安全性が高いとされる
- ネットワークケーユの攻撃では、内部の情報が漏えいしないことを担保

セキュリティ要件の評価分野		
1	暗号モジュール仕様	暗号モジュールの仕様、「FIPS 140-2」の適用範囲を規定
2	暗号モジュールのポート・インタフェース	情報の入出力に関する規定
3	役割、サービス、および認証	ユーザーの役割や役割ごとに提供されるサービス、ユーザーの認証方法を規定
4	有限状態モデル	状態遷移の記載を規定
5	物理セキュリティ	表面処理やカバー等といった物理的しくみによるセキュリティ要件を規定
6	動作環境	暗号モジュールが動作する環境に関する規定
7	暗号鍵管理	鍵生成、鍵の入出力等を規定
8	電磁妨害／電磁両立性(EMI/EMC)	電磁波に対する要件を規定
9	自己テスト	暗号モジュールが正しく動作できることを確認するためのテストに関する規定
10	設計保証	ガイドライン等に関する規定
11	その他の攻撃の対処	「FIPS 140-2」では規定されていないその他の攻撃の対処方法の記載

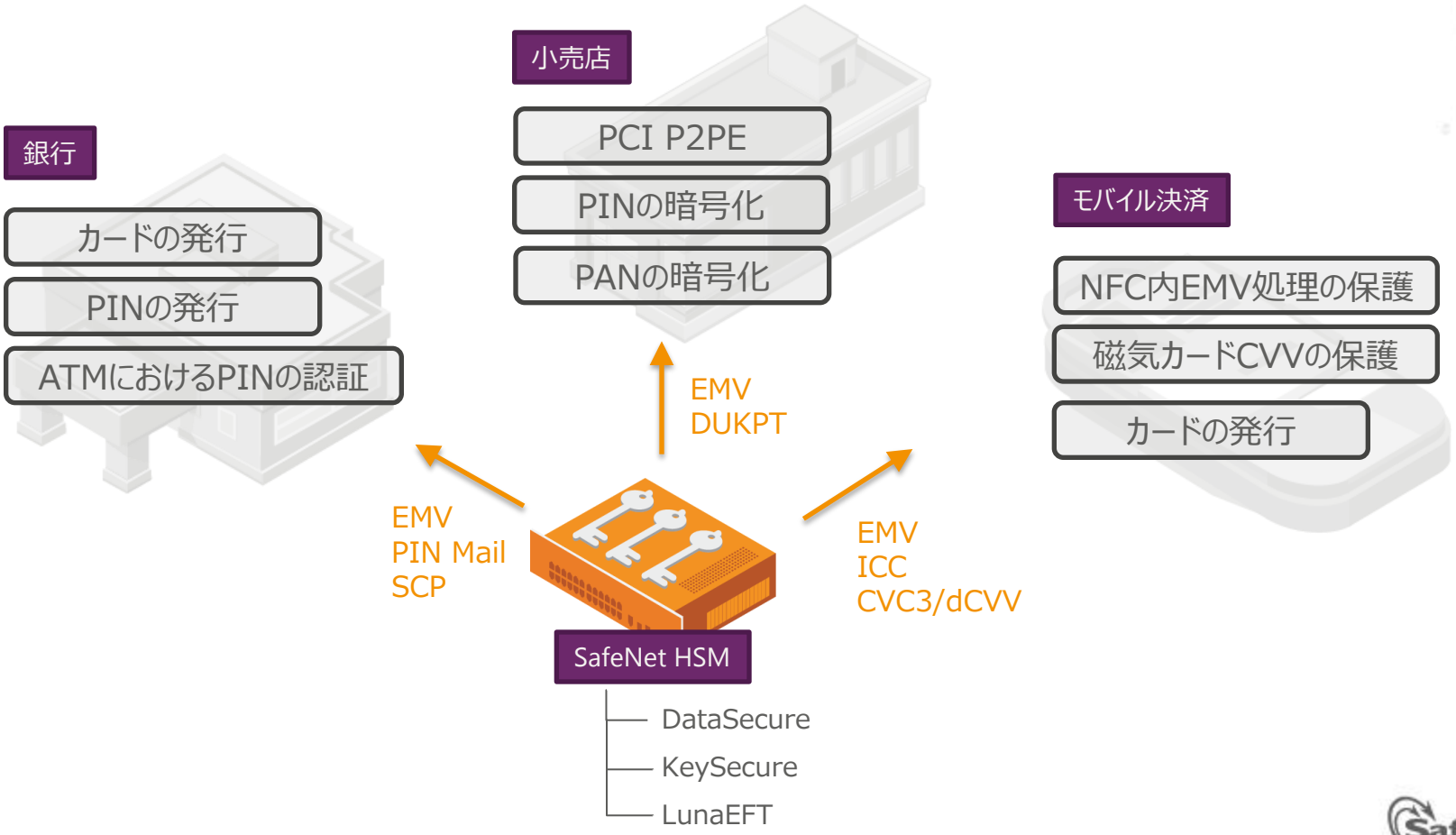
NIST SP800-57 鍵ステータス管理

- → KeySecureにおける鍵の世代管理
- → Deactivatedについては手動or事前に設定されたスケジュール（有効期限）に従う
- → CompromiseおよびRevoke機能は最新版6.4にて対応
- → NIST SP800-57はIPAにおける「安全な鍵管理のライフサイクルマネージメントに関する調査」において指標として取り上げられている



金融業界におけるHSMの幅広い用途

暗号鍵管理を含め幅広いトランザクション保護に利用



PCI-DSSに見るDB暗号化のハードル

要件3:機密データの保護

- 暗号化の実装に伴うアプリケーションおよびDB改修作業負荷
- 実装後のパフォーマンスへの影響
- 暗号鍵の安全な管理手法の実装
- 鍵の更新によるシステム停止等

要件7:必要最小限のデータアクセス制限

- 適切な鍵アクセスの実装
- 内部DBAは？

要件9:機密情報への物理アクセス制御

- DBのテーブル情報流出をどう保護するか
- 目視での漏洩に対する対策など

要件10：機密情報アクセスの監視

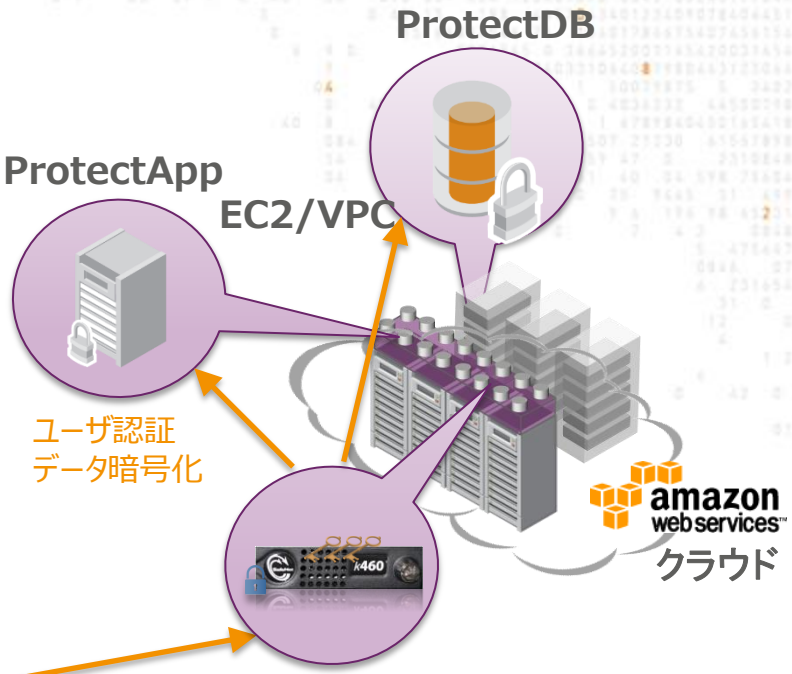
- 膨大なアクセスログの管理
- 監査対応とその費用

クラウド上のDB保護

*KeyServer in Cloud*モデル

仮想鍵管理サーバをクラウドに

- 金融・コンプライアンス対策ユーザ向け
- 鍵はクラウド上の自分が管理できる仮想インスタンス内で管理
- vKSないしvDS（FIPS140-2 level1）で鍵管理を実現
- オンラインでデータにアクセスが発生する環境（Web/App/DB）のインスタンスにおけるデータの保護



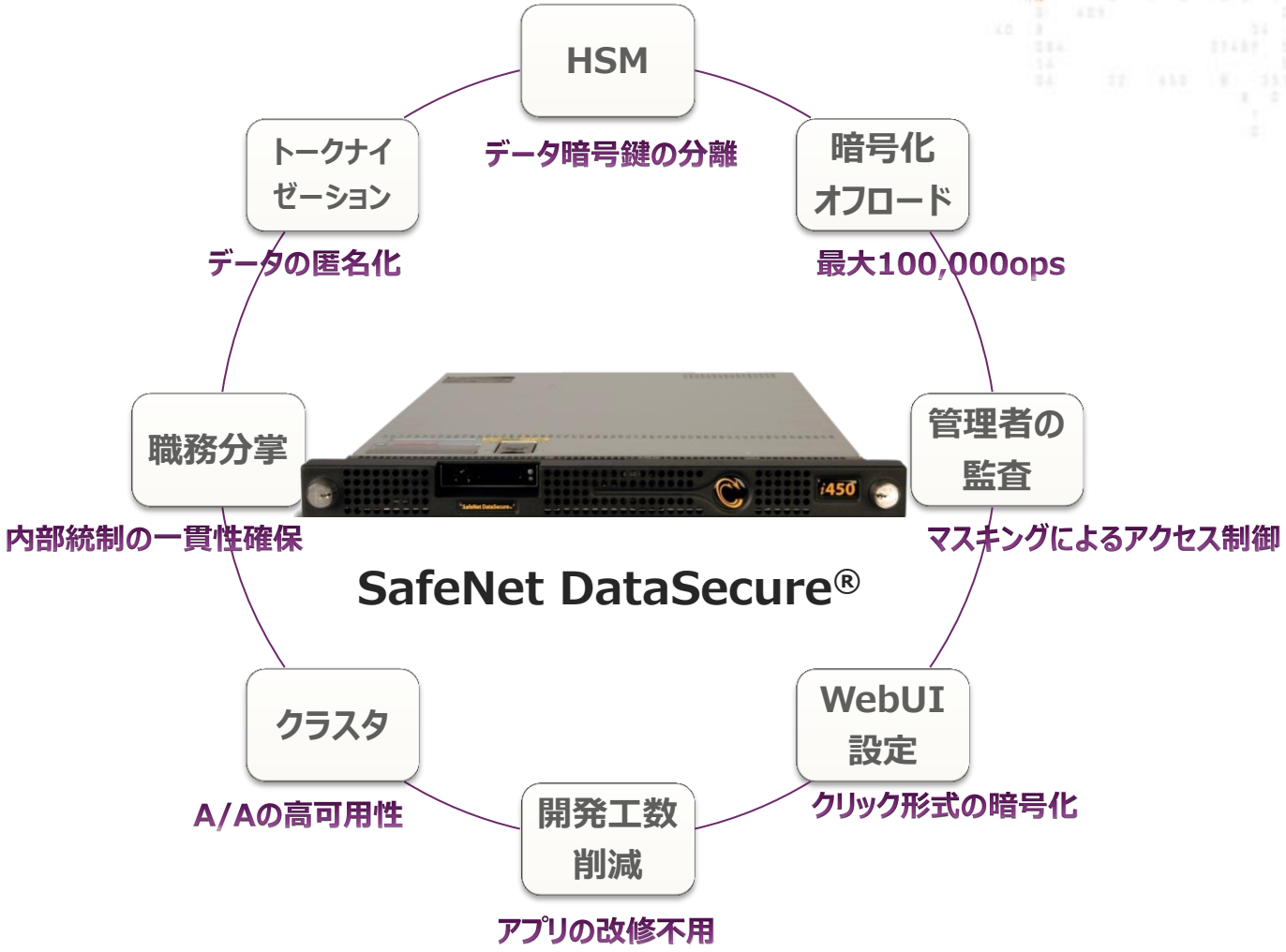
オンプレミス

ポリシー・鍵の管理

- 短期間でもセキュアにクラウドを利用したいお客様
- 開発環境としてクラウドを利用するお客様

暗号化＋鍵管理＋職務分掌＝DataSecure

業界初のHSMベースのマルチプラットフォーム対応暗号化・内部統制アプライアンス

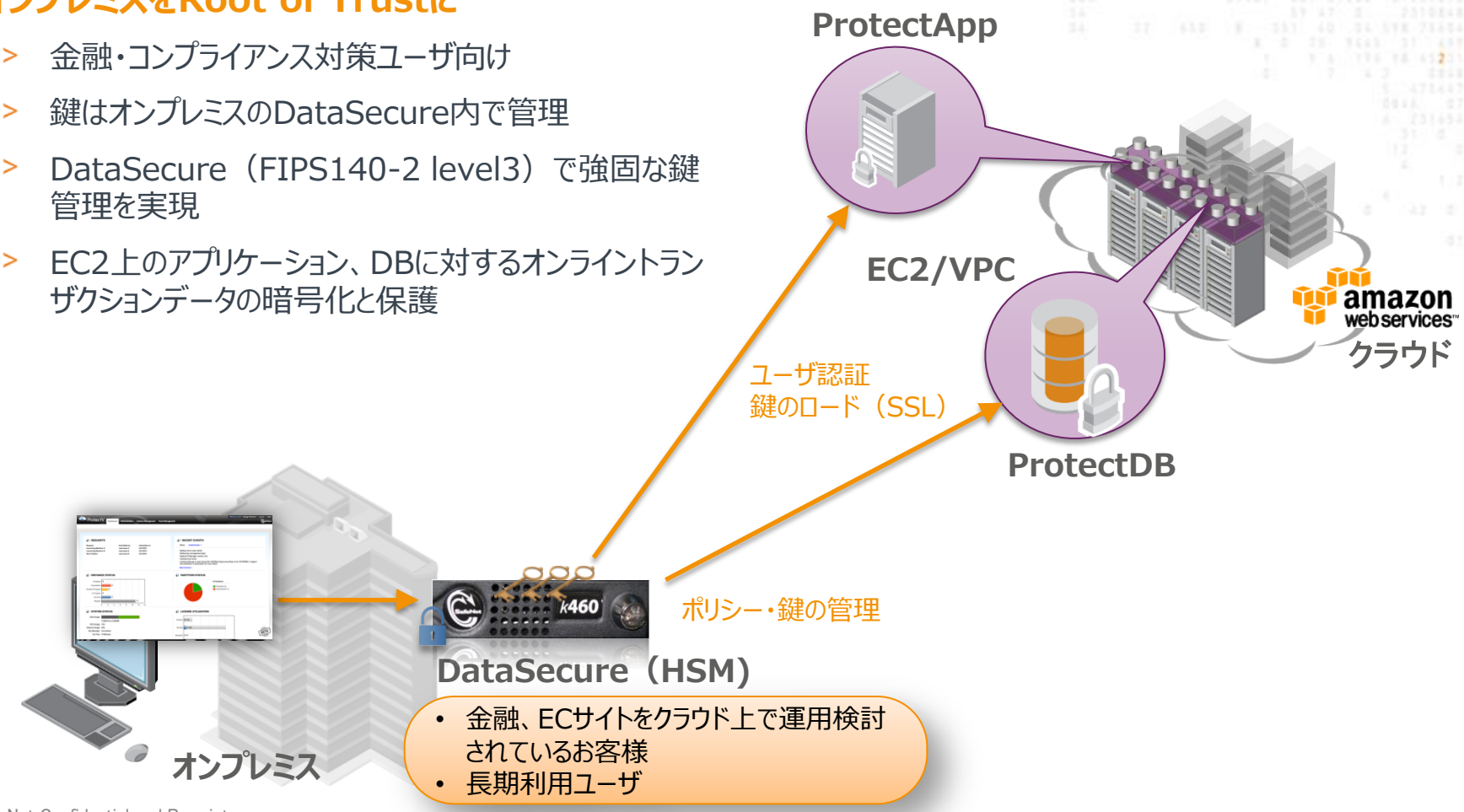


21

クラウド上のDB保護
Key on Premiseモデル

オンプレミスをRoot of Trustに

- 金融・コンプライアンス対策ユーザ向け
- 鍵はオンプレミスのDataSecure内で管理
- DataSecure（FIPS140-2 level3）で強固な鍵管理を実現
- EC2上のアプリケーション、DBに対するオンライントランザクションデータの暗号化と保護



SafeNetのDB暗号化

透過的な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

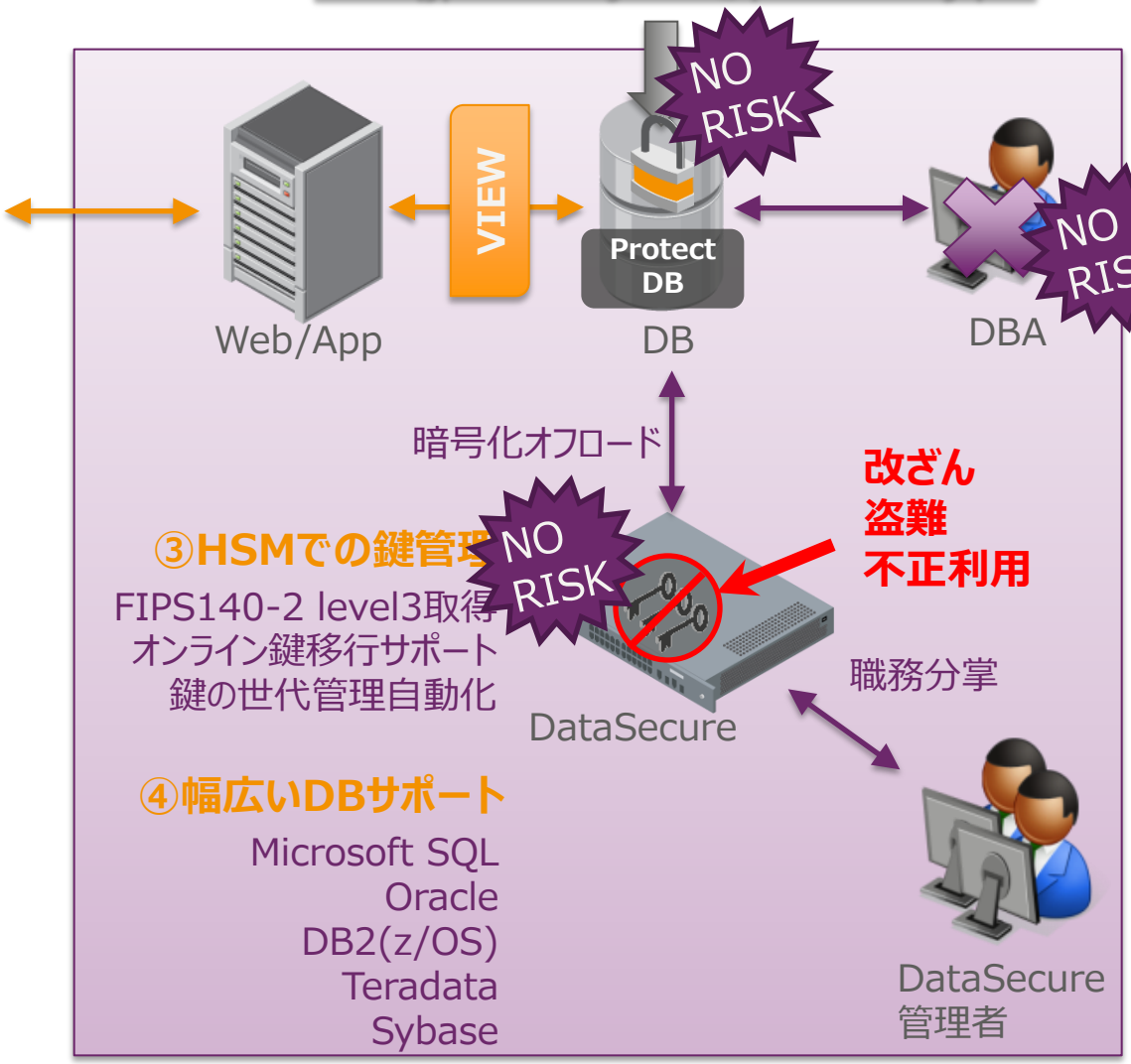
パフォーマンスの高いトークナイゼーション＋HSM

- **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	上大岡雅子	NULL
9	9	安全第一	NULL
10	10	正給勤	NULL

②データのマスキング

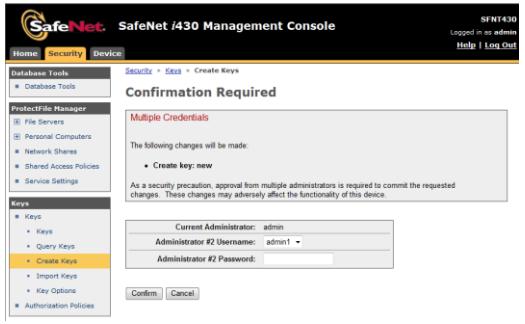
内部DBAの目視によるデータ漏洩を防御

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
Sybase



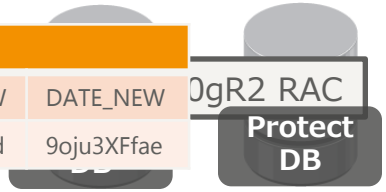
⑤管理者の職務分掌機能

設定変更に複数の管理者認証

ECサイトにおける事例

TABLE(VIEW)		
USER	CCN	DATE

TABLE_NEW				
USER	CCN	DATE	CCN_NEW	DATE_NEW
USER1	NULL	NULLL	hja98ek2d	9oju3XFfae



オンライン暗号化

難解な暗号化要件

- ECサイト上処理で発生するユーザのクレジットカード情報の暗号化
- 3テーブル、数百万件におよぶデータが対象
- 業務停止をすることなく暗号化が必要
- 暗号鍵に対する脅威を保護するシステムが必要
- 既存システムに修正を伴わない暗号化

SafeNetによる解決策

- カラム単位での暗号化とマスキング
- サービスクエリを受付けながらオンラインで暗号化
- FIPS140-2 level2認定HSMによる鍵管理と職務分掌による内部統制の提供
- OracleにProtectDBをインストールすることでアプリケーションには改修を伴わないスキーム

スキのないDB暗号化の実装

外部脅威に対する対策

境界線の保護：外部からの不正なアクセスに対する防御

- NGFW/IPS/UTM/WAF/DBFW etc
- アプリ・DBへのアクセス制御
- 亜種・未知の攻撃に対する対応
- アクセスログ収集

データへの脅威に対する対策

データの暗号化：不正なアクセス全てに対する防御

- DBまるごと・カラム単位
- 暗号鍵の管理
- 鍵に対するアクセス制御（管理者含む）
- データのマスキング
- 職務分掌による内部統制の強制

PCI-SSCからの提案

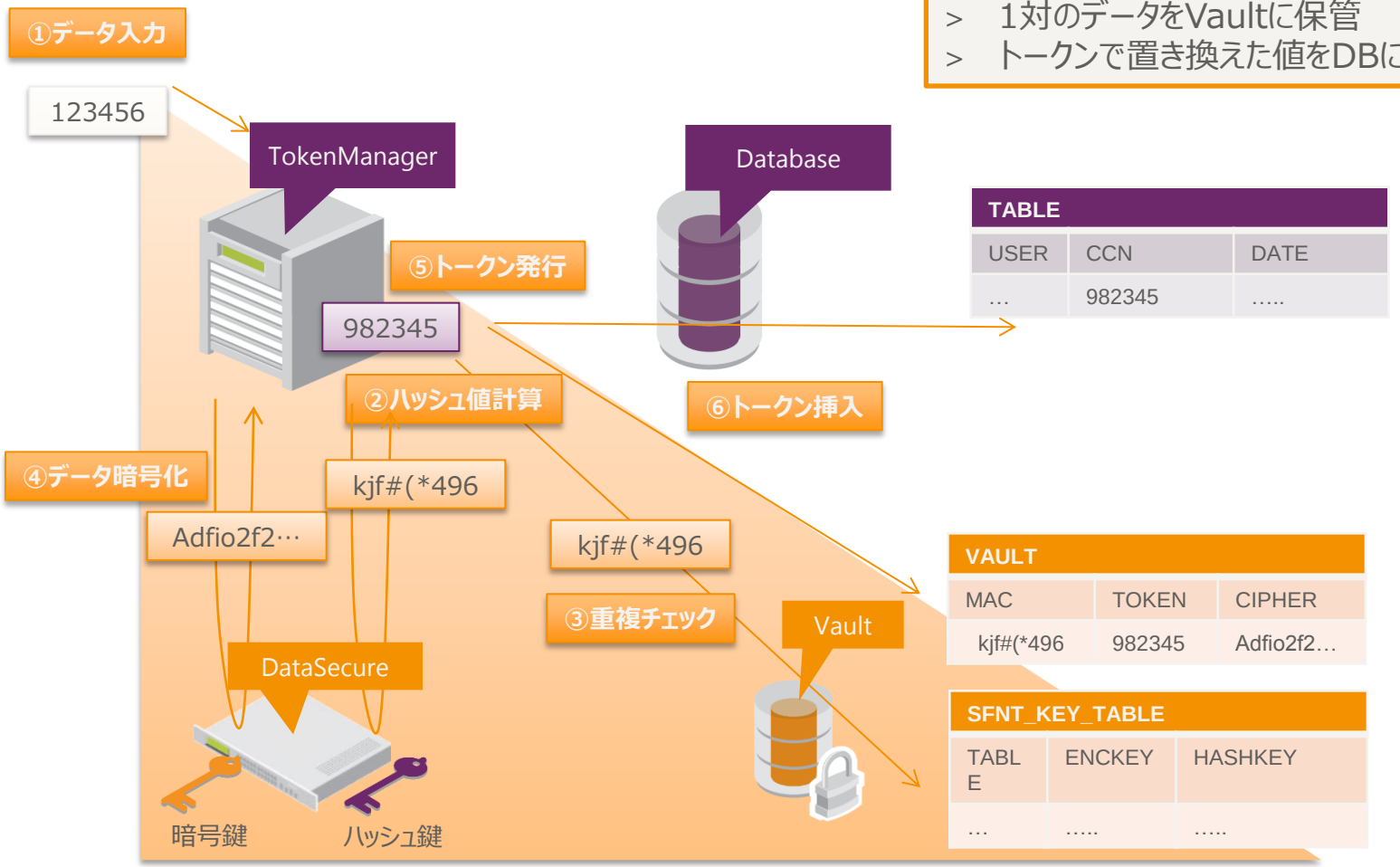
Emerging Technologyとしてのトークナイゼーション

- システムに透過的なデータ保護方式（データの匿名化）
- 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
  - **暗号化：** 1234-5678-0123-4567 → Fmqjper1m+j54!f@passu1a4jq&
    *データ長やデータタイプが変わる・パフォーマンス劣化・鍵管理・鍵更新時のシステム停止
  - **マスキング：** 1234-5678-0123-4567 → 12**-****-****-4567
    *データ復旧不可・ユーザへの明細などにのみ利用可
  - **トークン化：** 1234-5678-0123-4567 → 1296-4758-0154-4567
    *既存アプリケーションに対し透過的・パフォーマンス影響なし・鍵更新時のシステム停止影響なし
- 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**

基本動作イメージ

トークナイゼーション処理

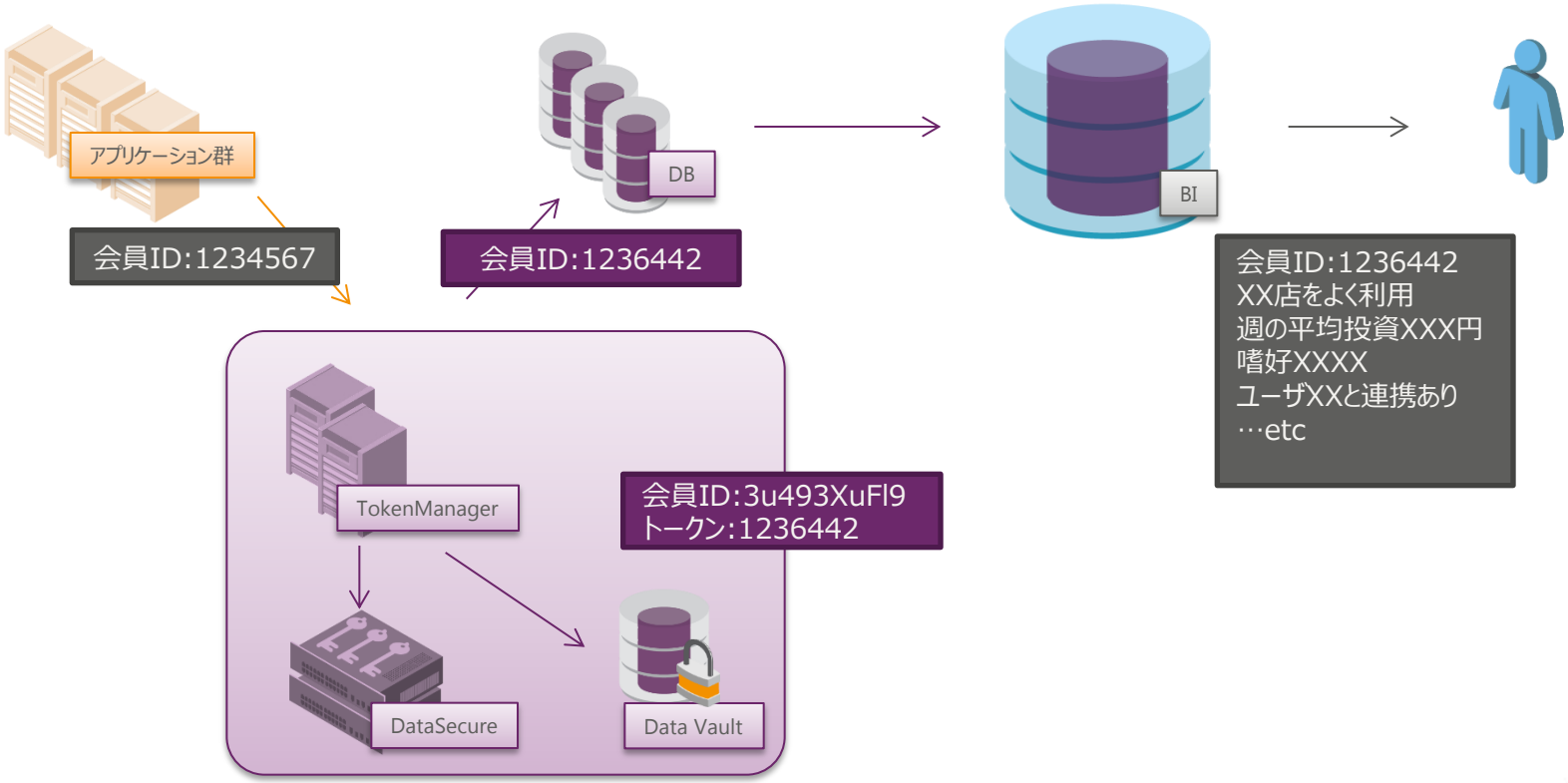
> 機密データはDataSecureで暗号化
> 暗号データに対しトークンを発行
> 1対のデータをVaultに保管
> トークンで置き換えた値をDBに格納



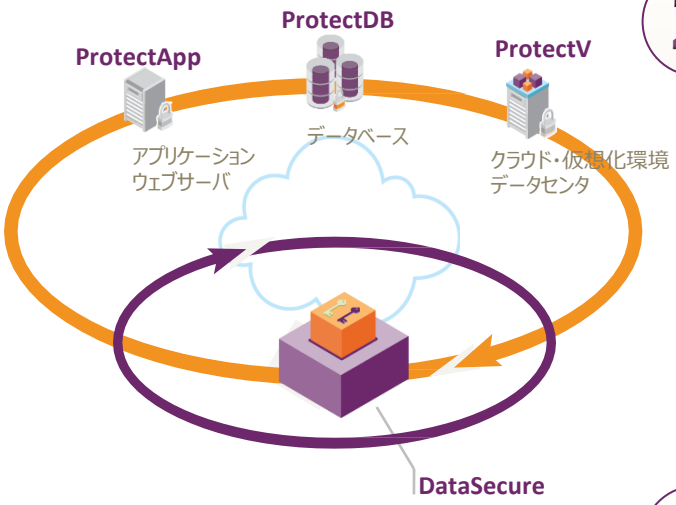
ビッグデータへの活用

DB内の個人情報をトークン化で匿名化

- 個人を特定されないようデータを匿名化
- その他データに対する関連性などは残るためBI用データとして解析利用に支障なし

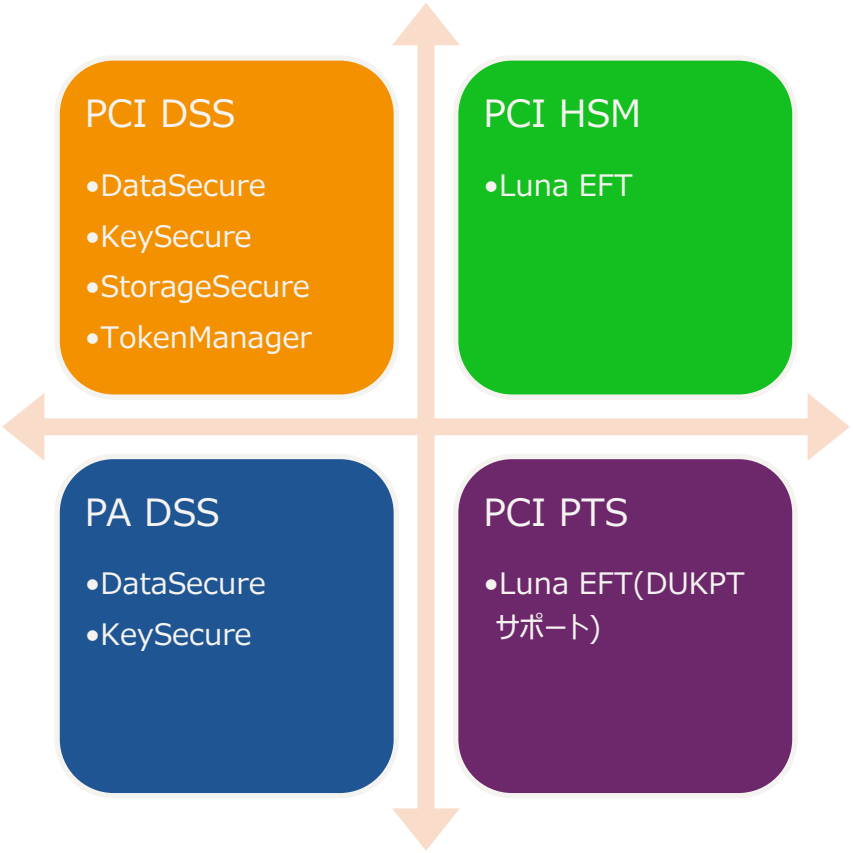


SafeNet DataSecureのメリット



1. PCIコンプライアンスを確保してセキュリティ強化
2. アプリケーション改修を伴わない透過的な暗号化
3. WebUIによる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による情報漏えい対策
5. システムを止めないオンラインでのデータ移行対応
6. トークン化オプションによる監査範囲削減とデータの匿名化
7. 混在環境（Web/App/DB/オンプレ・クラウド）へのシンプルな暗号化適用

PCIに対するソリューションセット



幅広い要件をサポートする製品群

- HSMを中心とした鍵管理
- 最新暗号要件DUKPTへの対応
- DBを止めない暗号化機能の提供
- POSからDBまでのさまざまな暗号モジュールの提供
- トークナイゼーションモジュールとHSMの連携機能提供
- DBストレージの暗号化オプションもあり（ディスク全体：KeySecure、シェア単位：StorageSecure）

Thank you.

お手元のアンケートへの回答をお願い致します。
ご協力頂いた方には、セキュリティスタンプを差し上げています。

アンケート用紙は、出口付近にて弊社社員が回収しています。