SafeNet | THE DATA PROTECTION COMPANY

DB暗号化と鍵管理の重要性

日本セーフネット株式会社　エンタープライズ事業部　シニアセキュリティエンジニア
DBSC DB暗号化WGリーダー
高岡　隆佳

SafeNet会社概要

SafeNet

What We Do

SafeNetは幅広いデータ保護ソリューションを提供しており、
お客様の価値ある情報を守り続けています。

SafeNet

Who We Are

世界中の信頼されているブランド企業の価値あるデータを保護、そして我々もまた信頼されています。

We protect the most money that moves in the world, $1 trillion daily.

グローバルな金融トランザクションの保護

We protect the most digital identities in the world.

グローバルなデジタル署名保護

We protect the most classified information in the world.

グローバルな機密情報の保護

創立

1983

オーナーシップ

Private

利益

~500m

グローバルな実績

+25,000

Customers in 100 countries

社員数

+1,500

In 25 countries

信頼と認定

最高のセキュリティスタンダード認定を受けた製品群

SafeNet

DB暗号化WG活動の背景

- DB暗号化の必要性↑↑
  - コンプライアンス対策
    - PCI-DSS対応
    - 個人情報保護法
    - 各業界におけるレギュレーション
    - クラウド（マルチテナント型）環境におけるセキュリティ
  - 情報漏えいリスク対策
    - 莫大な賠償金の負担
    - 企業に対するイメージ悪化
    - 業績悪化に繋がる恐れ

SafeNet

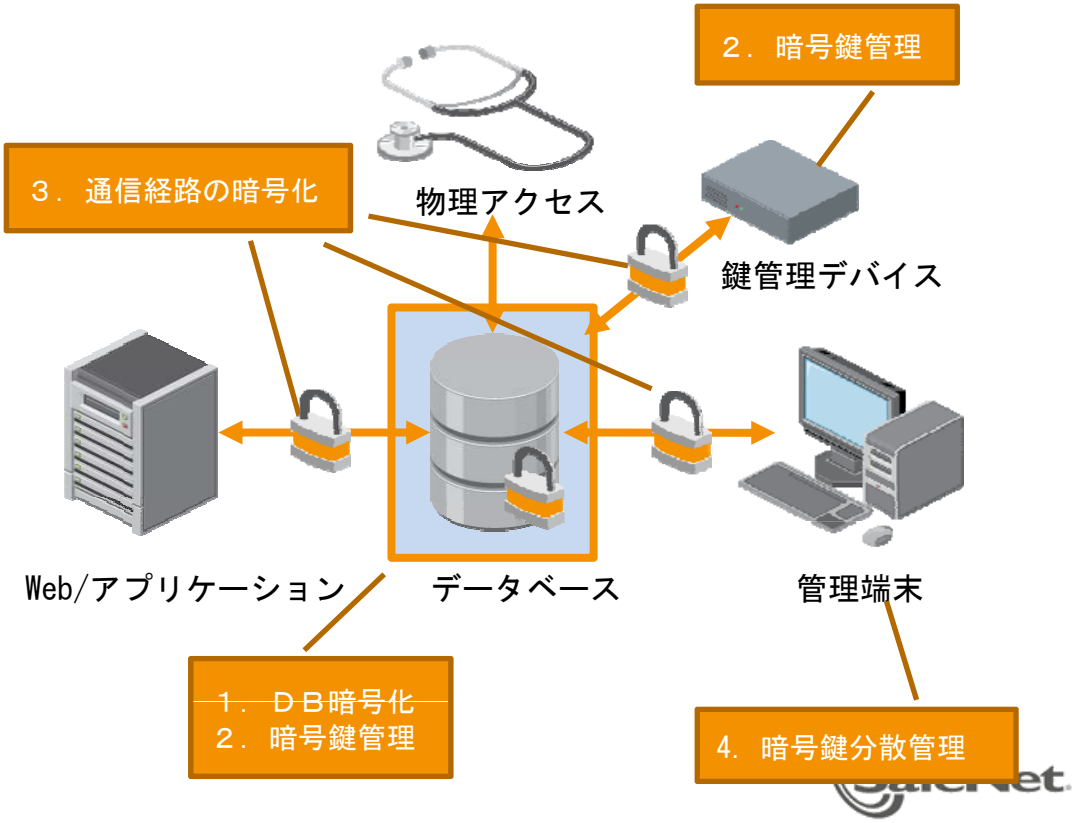
活動目的

- 暗号化WGではデータベース暗号化の意義を市場に広めるとともに、業界におけるさまざまな暗号化ソリューションを整理しながら
  - **データベース暗号化の手法と効果**
  - **運用上のリスクや注意点**
- を明確にし、
  - **ユーザ環境に適した暗号化が何であるのか**
  - **暗号化による効果と正しい運用方法**
- を提示することにより、暗号化に対する正しい知識を市場に提供することを目的とする。

SafeNet

暗号化対策概要

- DB暗号化ガイドラインにおける暗号化対策
  - DB暗号化
  - 暗号鍵管理
  - 通信経路の暗号化
  - 暗号鍵分散管理



DB暗号化

- 暗号化分類
  - ハードディスク（HDD）暗号化
  - DBテーブル暗号化（オブジェクト含む）
  - DBカラム暗号化（アプリケーションでの暗号化、DBでの暗号化）
  - バックアップデータの暗号化

- 各ソリューション毎にその概要・メリット・デメリット・導入ガイドライン・実際の導入事例についてはDB暗号化ガイドライン1.0版にて紹介。

SafeNet

脅威と対策のマッピング

対応箇所	HDD抜き取り	バックアップ盗難	メモリダンプ解析	暗号鍵の盗難	パケットの盗聴	内部DBAによる暗号鍵の悪用
DB暗号化（HDD暗号化）	●	x	x	△	x	x
DB暗号化（DBテーブルの暗号化）	●	●	●	△	x	x
DB暗号化（DBカラムの暗号化）	●	●	●	△	x	x
アプリでのDB暗号化（DBカラムの暗号化）	●	●	x	△	x	x
暗号鍵管理（ソフトウェア）	–	–	●	△	–	△
暗号鍵管理（HSM）	–	–	●	●	●	●
通信経路の暗号化	–	–	–	●	●	–
暗号鍵アクセス制御	–	–	–	–	–	●
暗号鍵の分散管理	–	–	–	–	–	●

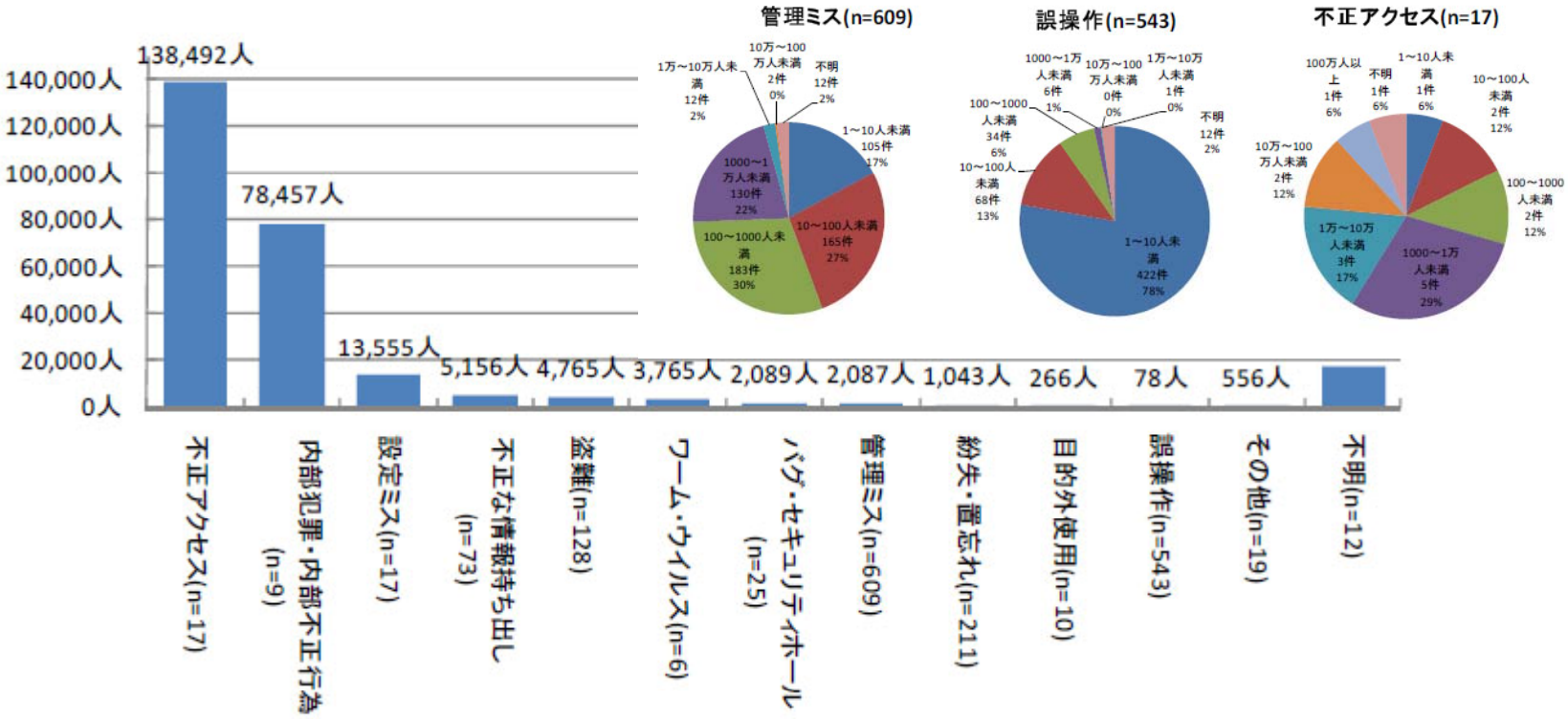
● –対応可能、 △ –製品によっては対応可能、 x –対応不可能、 ー –範疇外

- どこまでのリスクに対する対応が必要か判断

SafeNet

情報漏洩の原因と規模

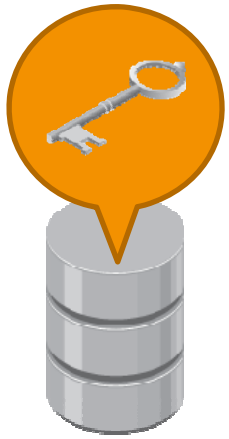
- 一般的に盗難などよりも不正アクセス・内部犯罪による漏洩件数およびインパクトが大きい



＊NPO日本ネットワーク・セキュリティ協会　2010年情報セキュリティインシデントに関する調査報告書より抜粋

暗号化の効果

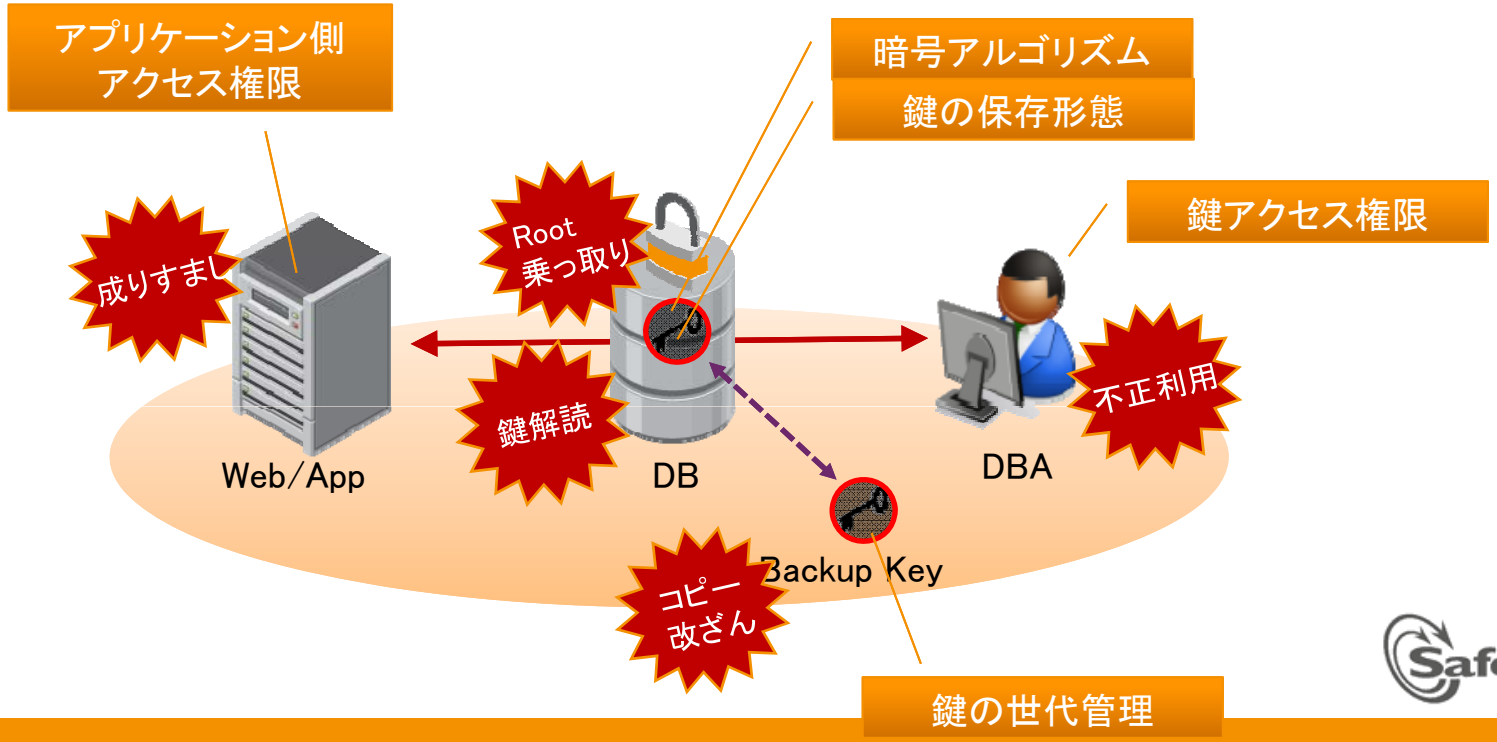
- 暗号化＝暗号化されていないデータとの分離→漏洩対策
- 効果は鍵の強度、管理手法に依存する
  - 鍵が誰にでも（管理者含む）アクセスされては暗号化の意味がない
  - 必要なときに必要な人が必要な分だけ鍵にアクセス
  - 鍵に対するユーザ（管理者）アクセスポリシーはどうする？
  - 暗号鍵が安全で完全性を保たれなければならない
  - 暗号鍵の適切な保存・管理をどうする？
- 鍵管理とアクセス制御が正しく設定されると・・・
  - 物理的な漏洩に効く！（HDD持ち出し、ベーステーブル持ち出し）
  - 内部不正に効く！（特権ユーザによる職権乱用）



SafeNet

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



PCI DSSに見るDBセキュリティ要件

- 暗号化における要件は共通している

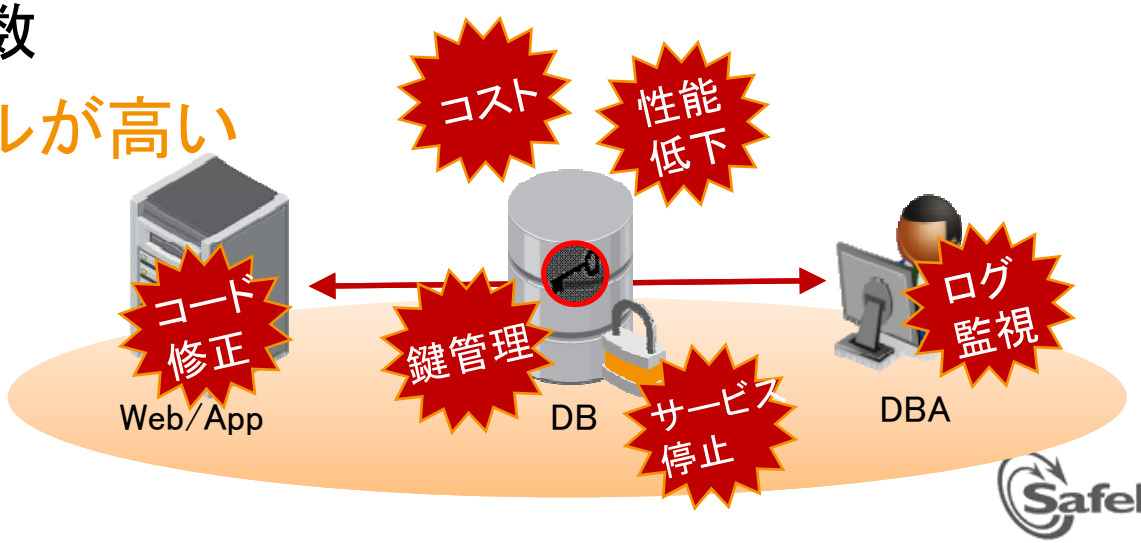
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data
	4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

暗号化と鍵管理

鍵へのアクセス制御と監査

DB暗号化の課題

- 様々な懸念事項
  - パフォーマンスの低下（フルテーブルスキャン等）
  - 導入、および鍵更新に伴うシステム停止
  - 暗号化に伴うデータの肥大、データ長変更等
  - 暗号鍵の徹底した管理
  - 鍵に対するアクセスログの監査、管理
  - 導入コスト、工数
- →導入のハードルが高い



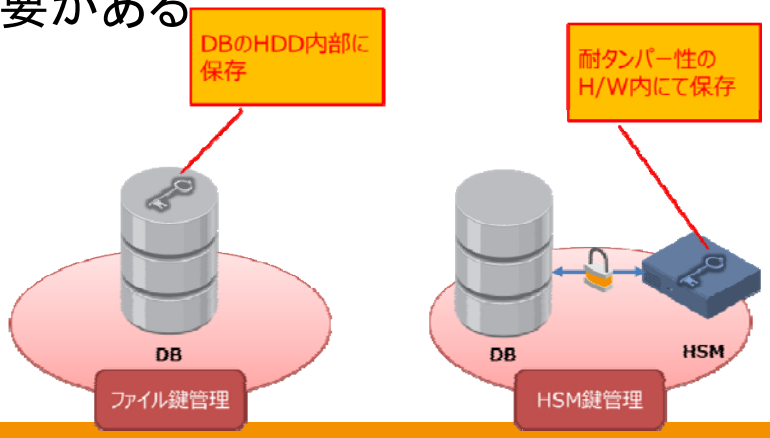
SafeNet

近年のDB暗号化ソリューション

- 課題の克服と新機能の登場
  - 暗号化のH/Wオフロード
    - AES-NI（インテル）との連携
    - 専用H/Wでの暗号化（TPM, HSM）
  - オンライン暗号化機能
    - システム停止なく暗号化の導入をサポートする機能
  - 専用H/Wでの鍵管理
    - 改ざん、不正利用の防止、鍵更新の自動化など
    - 開発を伴わないインテグレーション
  - トークナイゼーション（Tokenization）
    - データの匿名化による監査対象の削減
    - セキュリティ対策箇所の縮小
    - TSP（Tokenization Service Provider）による中小企業でのPCI DSS対策費用負荷の軽減

DB暗号化ガイドラインにおける鍵管理

- ファイル（データ）としての暗号鍵管理
  - メリット
    - 鍵の管理が容易／簡易である。
  - デメリット
    - DBサーバ内での鍵管理はデータと暗号鍵が同じHDD内に存在するため、HDD盗難時の漏えいリスクが存在する。
    - パスワードによる鍵の保護が主となるため、管理者のパスワード管理が重要となる。
    - 暗号化処理をDBで行うため、導入時はパフォーマンスへの影響を十分検討する必要がある



DB暗号化ガイドラインにおける鍵管理

- 専用H/W(HSM)での暗号鍵管理
  - メリット
    - 暗号鍵の生成から廃棄までのライフサイクルがHSM内部で一元的に管理されるため、暗号鍵がHSM外部に漏えいしない事が保証される。
    - 複数のDBサーバで暗号化を実施する際の暗号鍵管理をHSMに集約する事によって、暗号鍵管理の運用を容易にする。
    - DBサーバから独立した独自のアクセス制御機構を持っているため、DB管理と暗号鍵管理を分離する事が可能となる。
    - 暗号処理をHSMへオフロードする事によって、サーバのCPU負荷を軽減する。
  - デメリット
    - 導入時の機器調達、運用の見直し等に伴う初期費用の発生。
    - API組み込みのための工数。
    - 管理が必要なデバイスの増加。
    - 効果的な管理のためには複数の管理者による運用が必須。

SafeNet

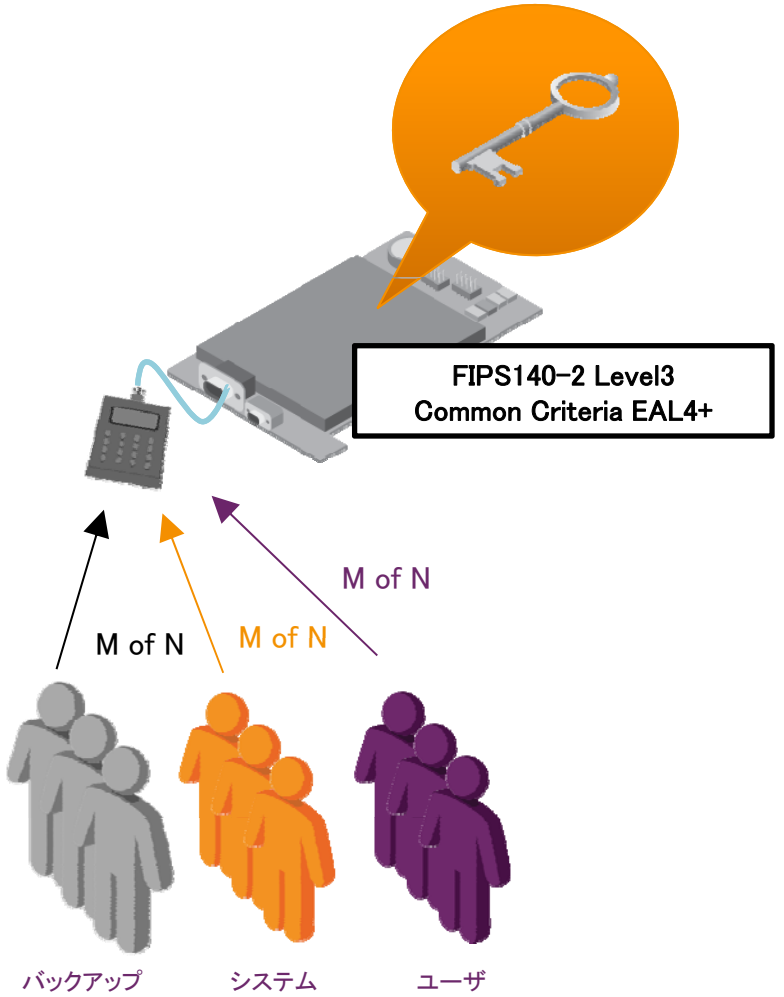
DB暗号化ガイドラインにおける鍵管理

- 暗号鍵へのアクセス制御
  - 暗号化の正当性を保障するためには、暗号鍵の物理的な保管に対する制御だけではなく、暗号鍵にアクセスできるユーザの制御も合わせて重要である。暗号鍵のアクセス制御を適切に設定することができなければ、暗号化の効力を十分に発揮することはできない。暗号鍵へのアクセスを制御するということは、その鍵で暗号化されているデータに対するアクセス制御と同義である。
  - 一般的には、ユーザアプリケーションからのアクセスについてはサービスに影響のない形でのアクセス制御が必要だが、DBAからの通常アクセスの部分については、運用上必要な部分を除いて最小限のアクセスに止めることが重要である。
  - アクセス制御の効果範囲については、暗号鍵がその暗号対象としている範囲によって変化する。

SafeNet

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



SafeNet

鍵管理セキュリティの基準

- 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

Level1	Level2	Level3
・すべてのコンポーネントにおいて一定の品質が担保され、甚だしくセキュリティの欠如がないこと	・左に加え、物理的な改竄の痕跡を残すこと、及びオペレータの役割 ベースでの認証を行うこと	・上記に加え、**物理的な改竄への耐性を持つこと（耐タンパ性）**、オペレータのIDベースでの認証を行うこと、及び重要なセキュリティパラメータがモジュールに出入力するインタフェースと、その他のインタフェースとを　物理的又は論理的に分離すること

SafeNet

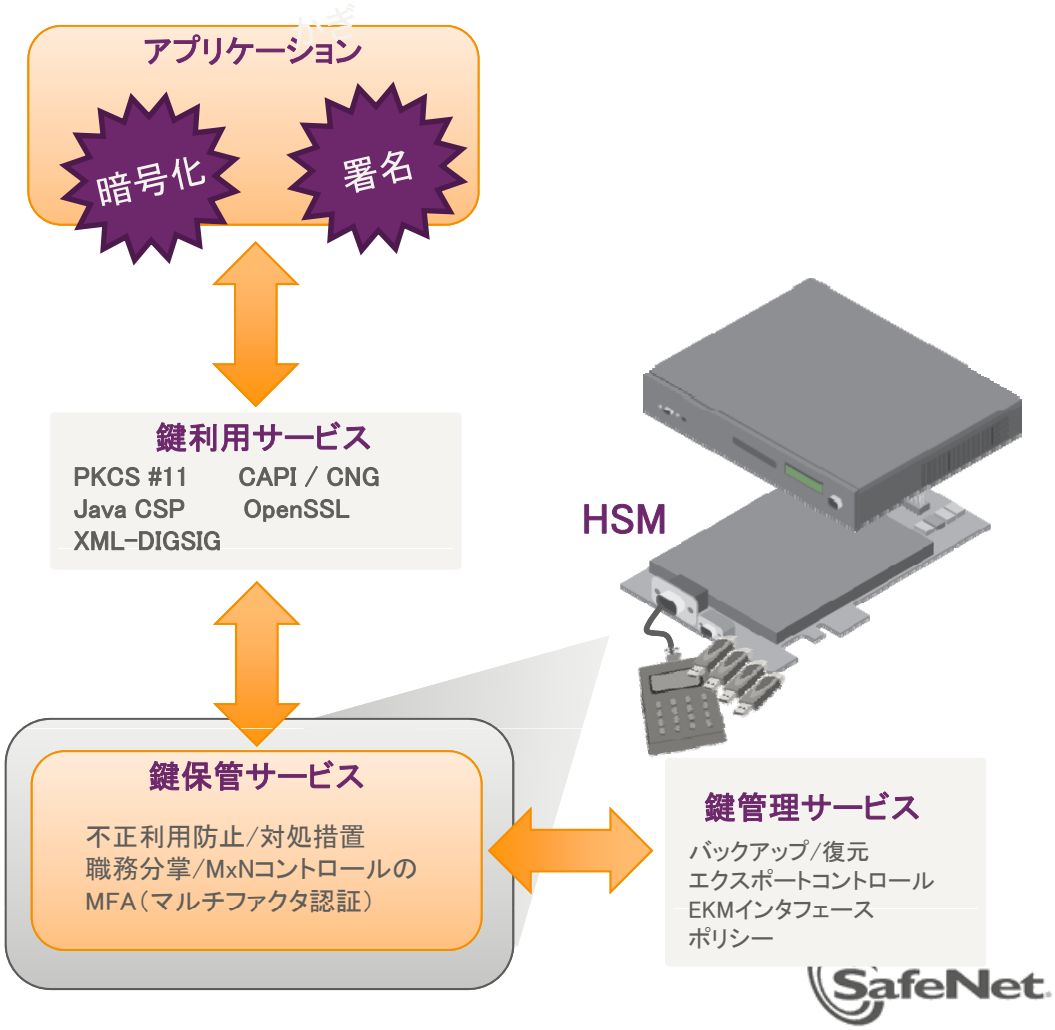
HSMに期待される効果とは?

標準化機関による認定	・CCおよびFIPS
パフォーマンス	・ECC & TLSの競合他社に比べて10倍
高いセキュリティレベル	・TLA資格認定
ハードウェア監査	・証跡によって、鍵管理の監査が可能
統合が容易	・Javaインターフェースあり
管理が容易	・HAモードで鍵を複製
柔軟性	・複数のアプリケーションからアクセス可能
スケーラビリティ	・ユーティリティ、運用、および鍵を複数のパーティションで管理可能
高可用性と災害復旧機能	・25年以上にわたりHSMのグローバルリーダーとして培った実績
ハードウェア鍵管理	・不可欠な機能!!!

SafeNet

HSMの導入事例

- 暗号化の完全性が必要なシステムへの導入
  - 証明書（電子署名）の秘密鍵保護
    - 官公庁・金融・エンタープライズ業界を問わず
    - セキュア・マニュファクチュアリング
    - スマート・メーター
  - 暗号鍵の保護
    - DB、ストレージ、EMV処理を実行するホスト等
    - クラウド上の暗号データに対するオンプレでの暗号鍵管理



データセキュリティへの対応

誰が？

・ユーザ
・パートナー
・管理者

何に？

・自分のPC
・共有ドライブ
・データベース
・ストレージ

どこまで？

・ドライブ単位
・ファイル・フォルダ単位
・データ単位

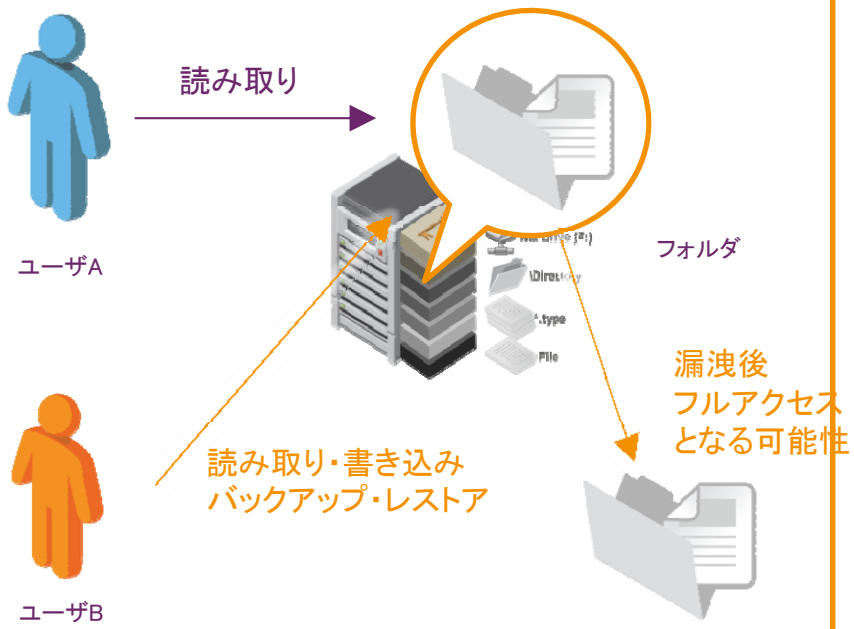
正しいアクセス範囲・認証ポリシーの定義 ＝鍵管理

SafeNet

アクセス制御と暗号化の違い

アクセス制御

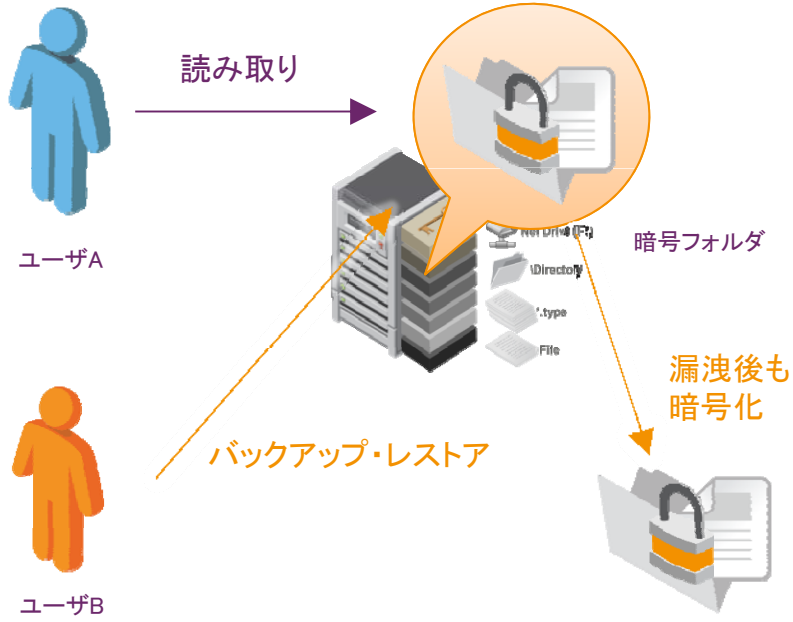
■アクセスポリシー
ユーザA：読み取り専用
ユーザB：フルアクセス権限



管理アクセス＝不要な読み取り・データ盗難の可能性

暗号化

■アクセスポリシー
ユーザA：復号専用
ユーザB：鍵アクセスなし



管理アクセス＝鍵へアクセス不可、データ管理のみ

SafeNet

DB暗号化製品一覧

- DBMS付属の暗号化オプション
  - DB2 EE
  - MS SQL TDE
  - Oracle TDE（Advanced Security/Label Security Database Vault等）
  - Protegrity Database Protector for Teradata
- 3rdパーティ社製暗号ソフトウェア
  - CypherGate eCypherGate
  - D’Amo
- 3rdパーティ社製暗号ハードウェア
  - SafeNet DataSecure
  - Thales nShield
- 暗号化製品全般
  - HDD暗号化製品
  - ストレージ暗号化製品
  - その他

＊会社名順

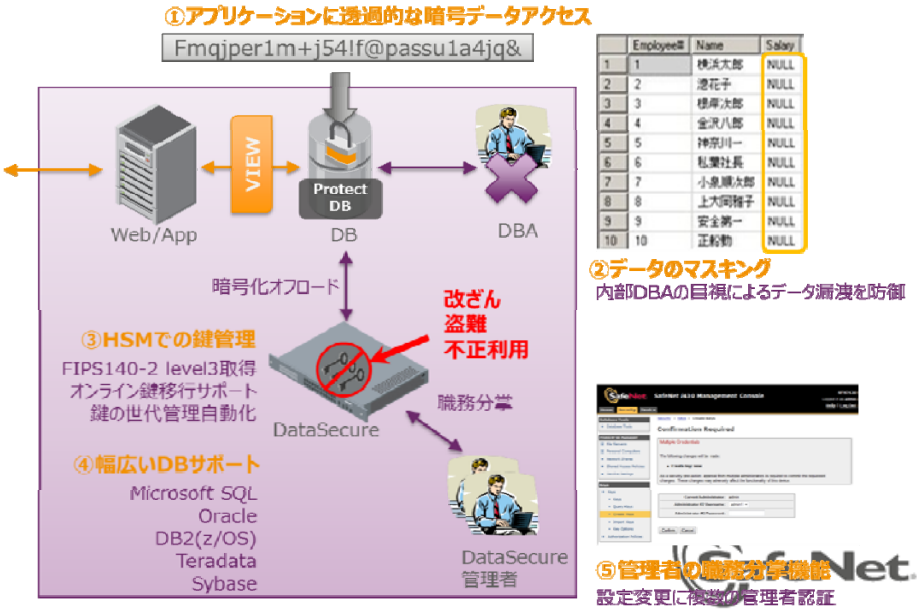
SafeNet

事例: 自社決済サービスDBのPCI DSS対応

DB	・Oracle 10gR2/MS SQL2008
暗号化対象	・クレジットカード番号、および一部個人情報を含む5カラム
テーブルサイズ	・100～200万件
データ移行時間	・約15分
暗号化製品	・SafeNet DataSecure i450
暗号化方式	・カラム単位
暗号鍵管理	・HSM（DataSecure）、鍵の世代管理自動化、オンラインでの鍵交換対応
アクセス制御	・ソフトウェア（鍵への時間単位、参照回数制限）
通信経路暗号化	・SSL（DB-DataSecure間、DataSecure-管理端末間）
導入までの期間	・4ヶ月
導入費用概算	・1,200万円

導入のポイント

・異なるDBの暗号化を単一の管理システムで提供、HSMによる鍵管理の自動化、既存アプリケーションに修正を必要としない導入形態、DBに対するオンラインデータ移行・鍵更新の対応、PCI-DSSコンプライアンスに対する幅広い網羅性（要件3、4、7、9、10）、内部DBAに対するマスキングによるデータ保護、Active/Activeクラスタ構成によるサービス継続性、サーバ単位での暗号化ライセンス体系。



事例: 自社決済サービスDBのPCI DSS対応

- 既存Oracle/MSSQL Server混在環境において、当初はそれぞれOracle /SQL2008の暗号化オプションの採用を検討していた。
- それぞれ別の管理を行うよりは、双方のDBMSを一元管理できるソリューションを、ということでDataSecureの検討を開始した。
- DataSecureがHSMであることからも、煩わしい暗号鍵管理がセキュアかつ自動化され、Oracle/MSSQL Serverに対する暗号鍵・セキュリティポリシーが一元管理できることで運用コストを下げることができた。
- クレジットカード番号を検索キーとしているが、DataSecureは暗号カラムにDomain Indexを適用できることから、一致クエリにおけるフルテーブルスキャンが回避でき、パフォーマンスを維持できた。
- 決済会社へ送信する決済ファイルを保存しているファイルサーバもDataSecureで暗号化対応することで、包括的にPCI DSSへ準拠ができた。
- サービスを止めずに鍵のオンライン更新が可能な点や、管理者一人の権限ではセキュリティポリシーを変更させない強固な内部統制機能により、PCI DSS各種管理要件の実装が容易だった。
- 鍵の使用を許可する時間帯、参照回数、参照権限を指定できる点は、PCI DSS要件7を実現するのに最適だった。

SafeNet

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による中小企業でのPCI DSS適用加速
- 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オンプレ側で実行・管理するサービスも
  - CSAにおいてもDomain11にて鍵管理の重要性が盛り込まれている
    11) Encryption and Key Management（暗号化、鍵管理）

SafeNet

Thank you.