暗号化の要点とトークナイゼーションに向けたロードマップ

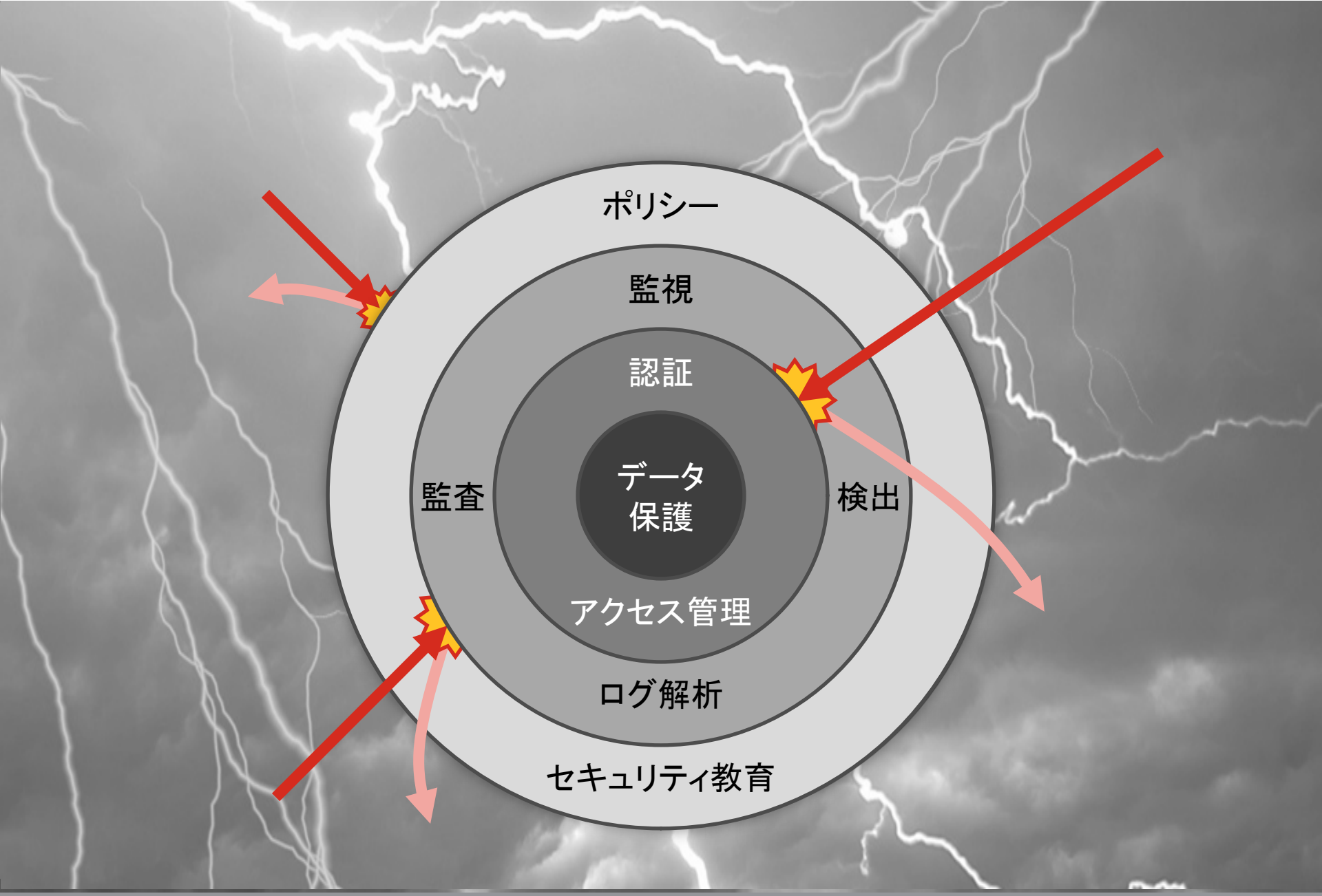
（PCI DSS 要件3、審査範囲縮小）

EMCジャパン株式会社
RSA事業本部　マーケティング部
シニア マーケティング プログラム マネージャー
関 真 （makoto.seki@rsa.com）

2012年 7月 25日

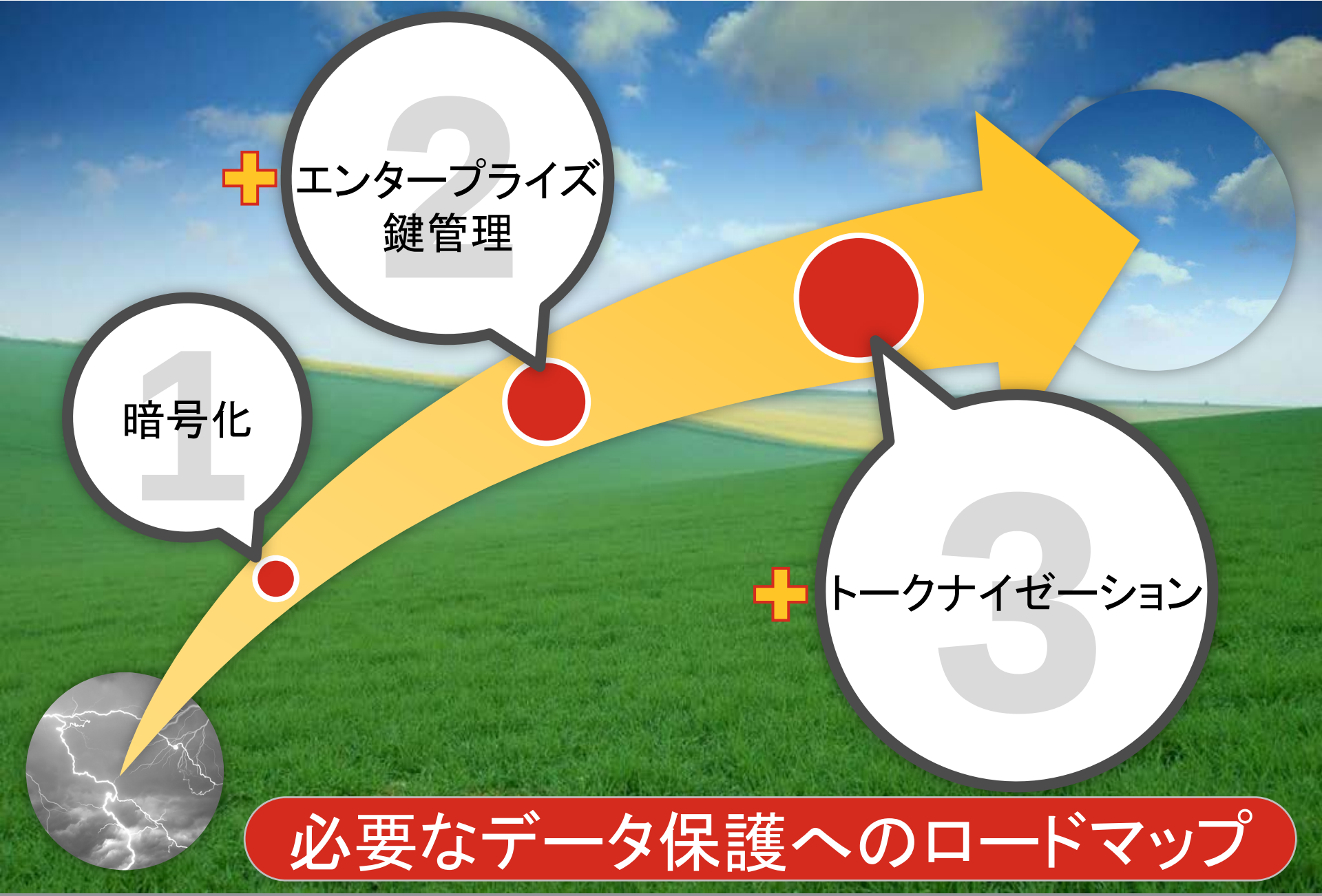
キーワード

- 多重的セキュリティ
- データ保護へのロードマップ
- 暗号化、エンタープライズ鍵管理、トークナイゼーション
- 実績のRSA DPM



RSA

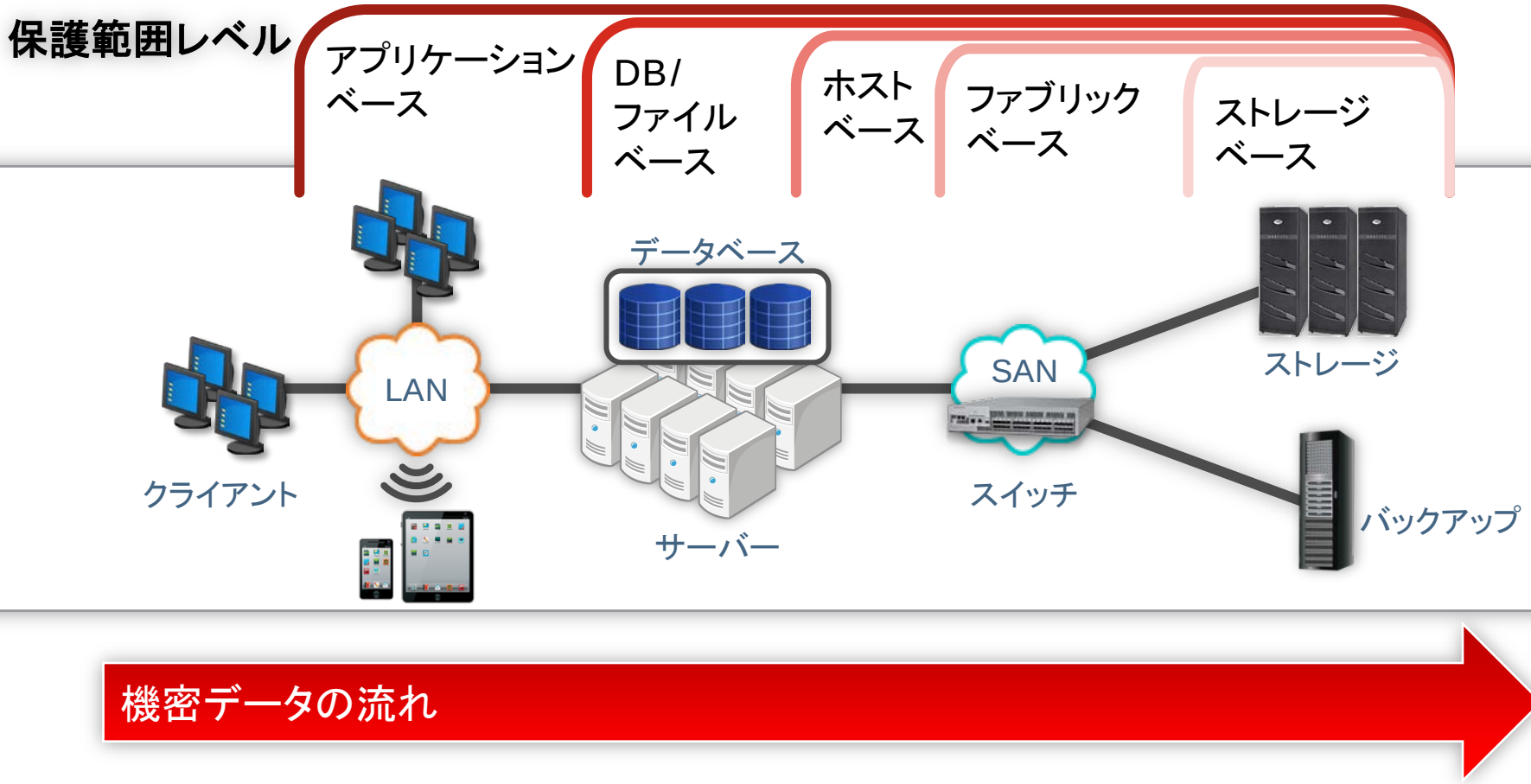
EMC²



ステップ 1 :

暗号化

どこで暗号化するか？



各暗号化手法と特徴

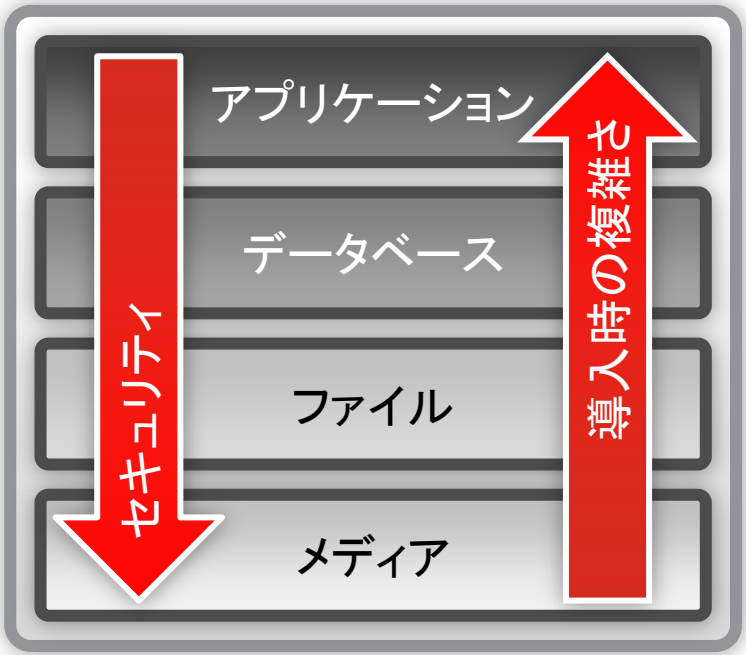
- 「ホストベース」、「アプリケーションベース」
  - サーバー上でデータを暗号化
  - データ暗号化を行うソフトウエアを使用
  - ネットワーク上のトラフィックは暗号化
  - サーバーのCPUを消費

- 「ストレージベース」
  - ストレージデバイスでデータを暗号化
  - システムに影響を与えない
  - ネットワーク上のトラフィックは暗号化されない
  - データ書き込み/読み取り時のパフォーマンスを要考慮

- 「ファブリックベース」
  - 暗号化機能付きのSANスイッチでデータを暗号化
  - システムに影響を与えない
  - ストレージ機種混在環境に対応可（ディスク、テープ）
  - 「スイッチ-ストレージ間」のトラフィックは暗号化

セキュリティ効果 vs 導入時の複雑さ

- 高度なセキュリティは、アプリケーションレベルでのデータ保護によってのみ可能



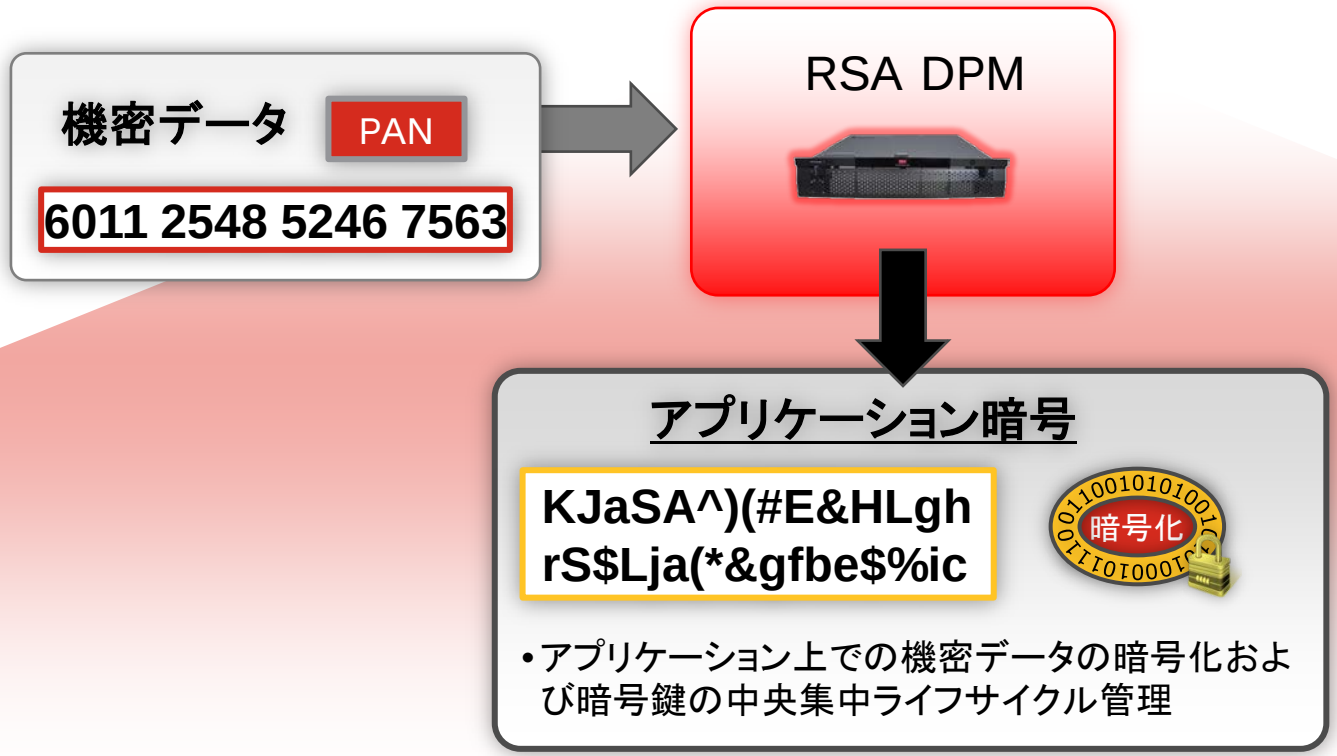
- より高度なセキュリティには、より複雑な設計・構築作業が伴う。
- セキュリティ効果と導入時の容易さ/複雑さはトレードオフ

2009年1月に最大規模のカード情報漏洩事故を起こした（1億件～6億件）決済代行大手の米Heartland Payment Systemsは、「カードデータが入力された時点で暗号化しなければ、データ漏洩の再発を防ぐことはできない。そうすれば、暗号化されていないカードデータがネットワーク上を流れることはなくなる」と述べています。

Source: BusinessWeek – July 6th 2009

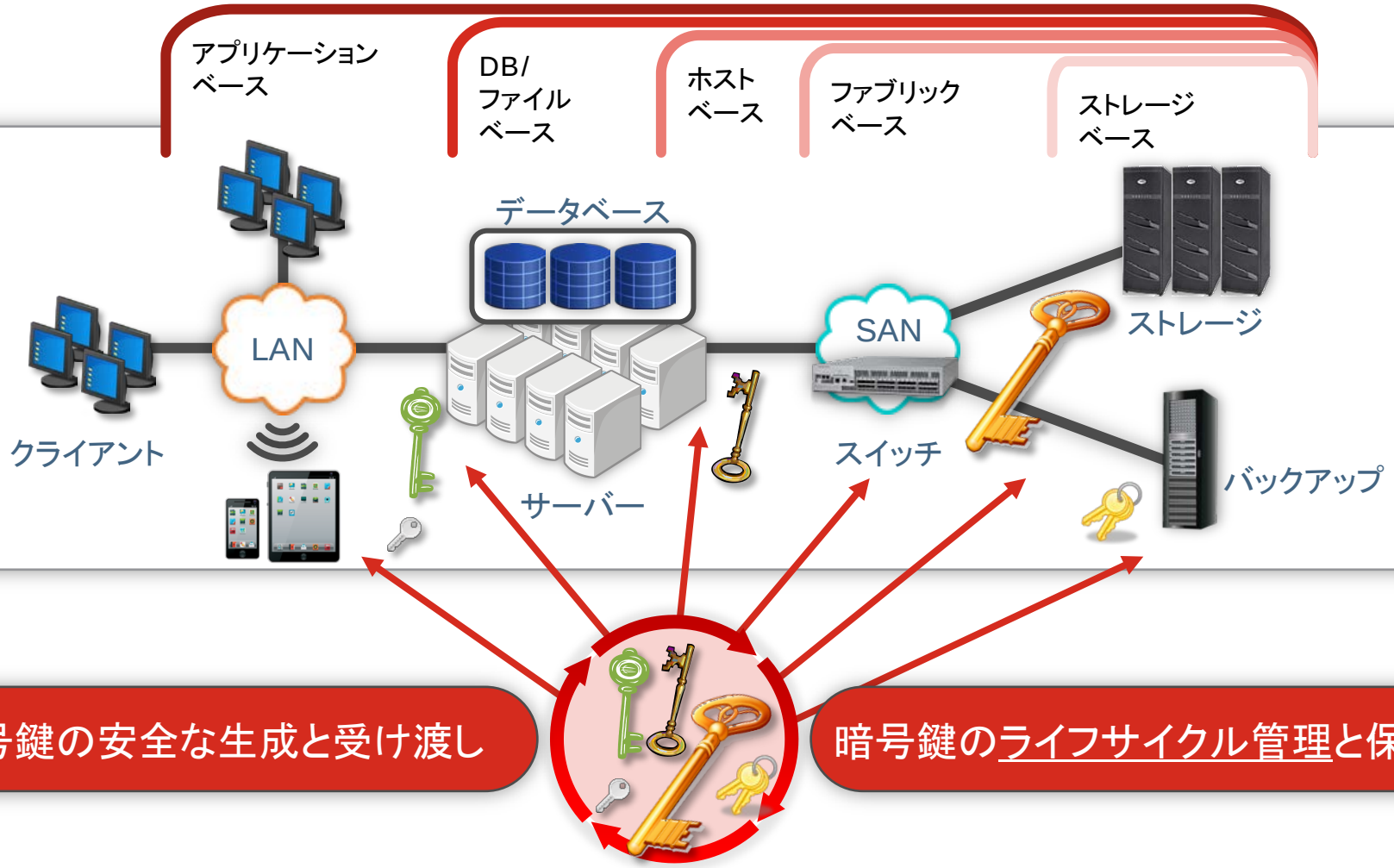
注目

RSA Data Protection Manager (DPM) アプリケーション暗号化とその鍵管理



ステップ2:
エンタープライズ鍵管理

どこで暗号鍵の管理をするか？



暗号鍵の安全な生成と受け渡し

暗号鍵のライフサイクル管理と保存

注目

RSA Data Protection Manager (DPM) エンタープライズ鍵管理

機密データ　PAN

6011 2548 5246 7563

RSA DPM

その他 様々な暗号化

- ストレージ、テープ、DBなどの暗号化/統合鍵管理

アプリケーション暗号

KJaSA^)(#E&HLgh
rS$Lja(*&gfbe$%ic

- アプリケーション上での機密データの暗号化および暗号鍵の中央集中ライフサイクル管理

幅広い機器にDPMクライアントを事前に組み込んでいます

RSA Data Protection Manager

様々な暗号化機器との事前統合により、企業内の暗号鍵を一元管理

KMIP 1.0

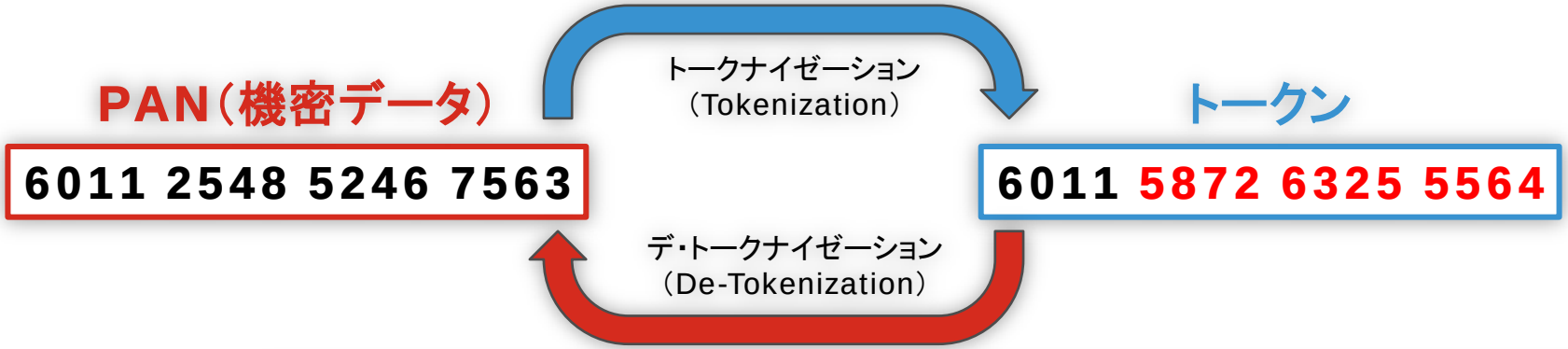
- Virtual Desktops and Servers
- BusTech Virtual Tape Library
- Oracle Retail Point of Sale
- Database Encryption
- Switch Encryption
- EMC Backup to Disk
- EMC Symmetrix Encryption
- EMC PowerPath Encryption
- Connectrix Encryption
- VNX Host Encryption
- Tokenization トークナイゼーション
- Application Encryption
- Native Tape Encryption (Sun, Quantum)
- Celerra (NAS) Encryption

Futures

ステップ3:
トークナイゼーション

トークナイゼーションとは

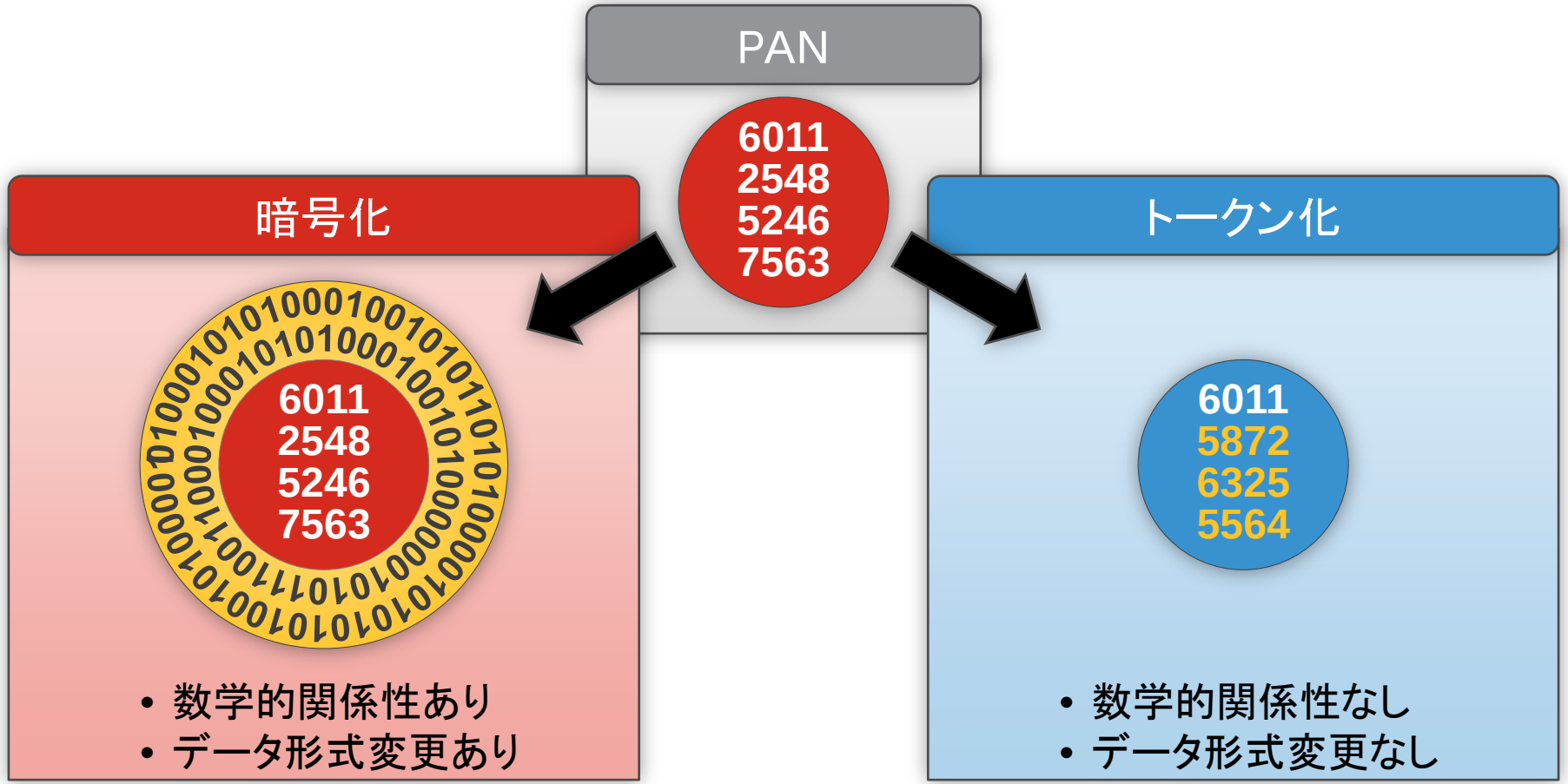
- トークナイゼーション（Tokenization）とは、PANを「トークン」と呼ばれる代替えの値に変換するプロセスの事を言います（トークン化とも言う）。また、デ・トークナイゼーション（De-Tokenization）は、その逆で、トークンから対応したPANを取得するプロセスのことを言います（デトークン化とも言う）。



「PCI DSS トークナイゼーション ガイドライン、1.3 Introduction to Tokenization」より

暗号化データとトークン化データ

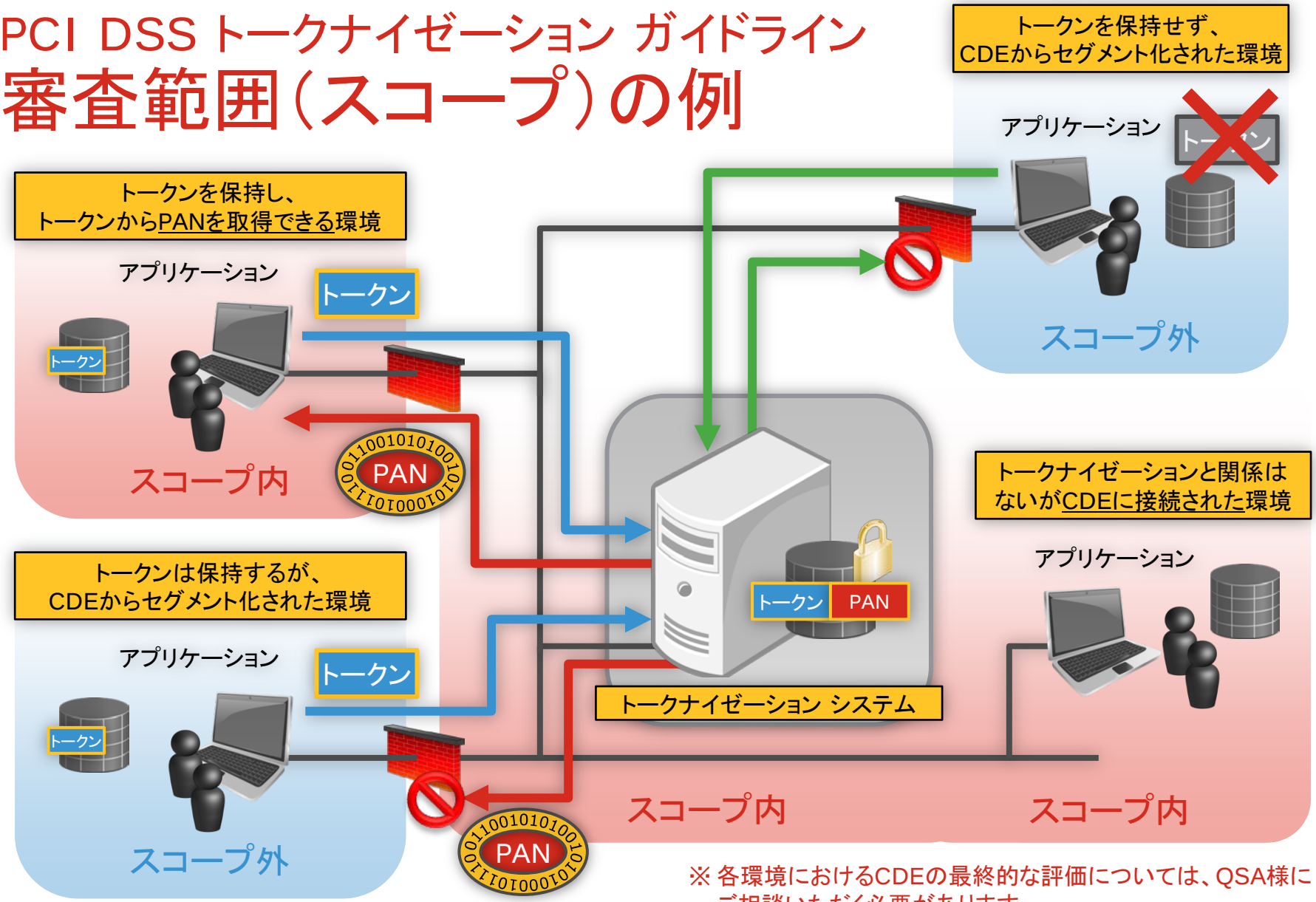
- PANデータを含む暗号化技術と含まないトークナイゼーションのイメージ



トークナイゼーションの一般的な特徴

1. PCI DSSの審査範囲を縮小可能（コスト削減）
2. セキュリティ能力を向上（PANの散在を防ぎ、PANを集中管理）
3. 既存システムへの影響が最小限（データタイプ変更無し）
4. 業務プロセス上の運用メリット（クレジットカードの下4桁を保持など）
5. PAN以外の様々な機密データにも対応（柔軟なトークンフォーマット）

PCI DSS トークナイゼーション ガイドライン
審査範囲（スコープ）の例



※ 各環境におけるCDEの最終的な評価については、QSA様にご相談いただく必要があります。

ご参考

注意！支払手段として使用可能なトークン “High-value Token"（高価値トークン）

- もし、トークンがカード取引においてPANの代わりに使用できたら、もはやトークンはPANなのでは？

支払手段として使用可能なトークン ＝ “High-value Token” 高価値トークン

↓

犯罪者にとって「収益源」になりえたり、不正トランザクションを実行できる可能性あり

↓


犯罪者のターゲットになり得る

↓

PANを直接取得することができない環境においても、カード支払処理が可能

↓

セキュリティ上の黄色信号！ PCI DSSの審査対象となる可能性！？

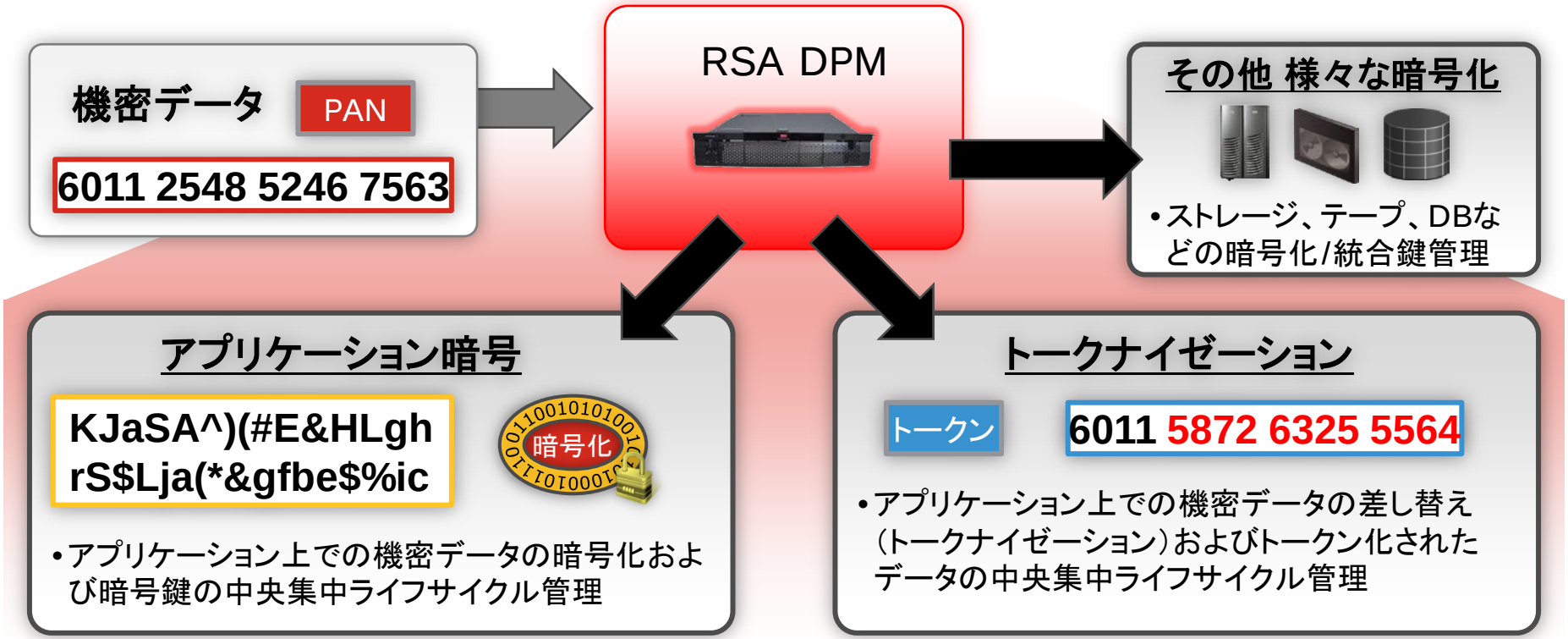
「4.1 Tokens as Payment Instruments」より

より全体セキュリティを考えた、信頼出来るデータ保護の導入が必須

注目

RSA Data Protection Manager (DPM) トークナイゼーション（ガイドライン準拠済）

- 利用環境および目的に応じて暗号化とトークナイゼーションの両方が完全統合された環境で利用可能。強力で柔軟なデータ保護が可能



RSA DPMの特徴まとめ
高信頼性の統合データ保護ソリューション

- 柔軟、強力、実績のある統合データ保護ソリューション
  - RSAの実績ある暗号化/鍵管理にトークナイゼーションをシームレスに統合
  - PCI DSSのトークナイゼーション ガイドラインに全て対応
  - ワールドワイドでのノウハウを蓄積、大規模環境における実績多数
    - いち早くサービス化（2009年11月）、製品化（2010年11月）、順次バージョンアップ
- 幅広い機器をサポートするエンタープライズ鍵管理
  - 事前インテグレーションおよびKMIP対応により実現
  - ポリシーベースによる暗号鍵およびトークン両方の自動ライフサイクル管理
- 柔軟な導入形態
  - ソフトウェア版、アプライアンス版、仮想アプライアンス版を提供
  - 暗号化とトークン化の両方を利用可能（ハイブリッド データ保護）
- 実績ある導入支援サービスを利用可能

NEXT

1 トークナイゼーションの全体と注意点を理解したい

PCI DSS トークナイゼーション ガイドライン解説させていただきます

トピック: トークン化とは、トークン・フォーマット、判別可能なトークンの注意、
2つのトークンの利用形式、機能コンポーネント、処理オペレーション、
3つのトークン生成方法、審査範囲の考え方、審査範囲縮小のための推奨事項、
セキュリティ検討事項、3つの導入方法、協力会社との責任分担、
高価値トークンの注意、リスクの理解

使用時間: 1時間～1時間半程度

2 とりあえず、追加資料を見たい

PCI DSS解説冊子プレゼントさせていただきます

トピック: 「PCI DSS 2.0解説」、「トークナイゼーション ガイドライン解説」
月刊「消費者信用」2011年2月号、3月号、2012年5月号掲載

3 その他も聞いてみたい

お声掛けください！

トピック: PCI DSSを考えた全体セキュリティ、暗号化/鍵管理、
サイバー攻撃対策、マルウェア感染システム発見サービス、
仮想デスクトップ認証などなど

RSA EMC²


trust
in the digital world
ありがとうございました
RSA