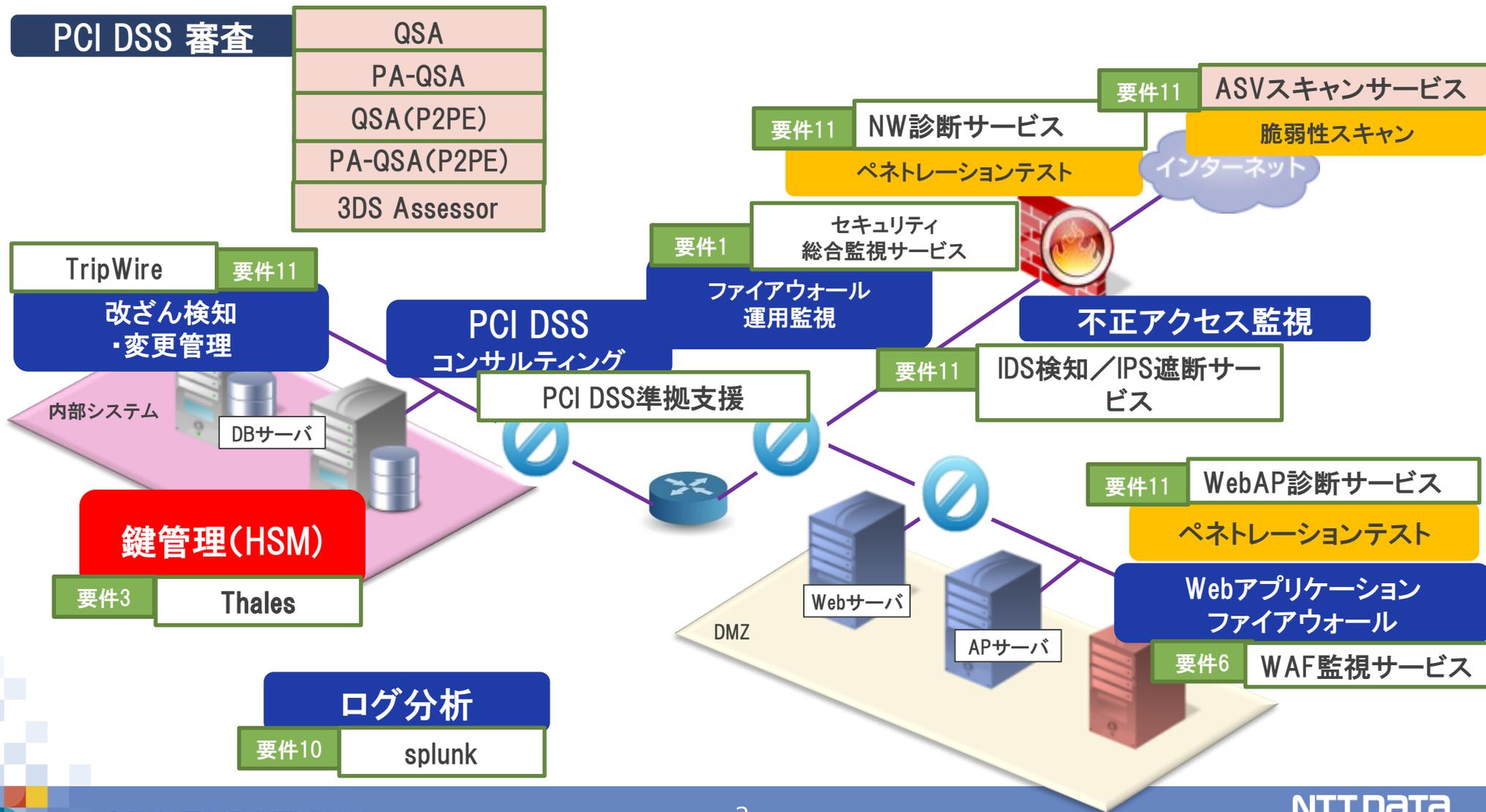


NTTデータ先端技術の「PCIトータルサービス」のご紹介

2020年11月
NTTデータ先端技術株式会社
セキュリティ事業本部セキュリティレジリエンス事業部

NTTデータ先端技術の「PCIトータルサービス」

弊社ではPCI DSS準拠のためのさまざまなソリューションを提供しております。



暗号鍵管理専用アプライアンスで情報漏洩リスクを低減させるソリューション

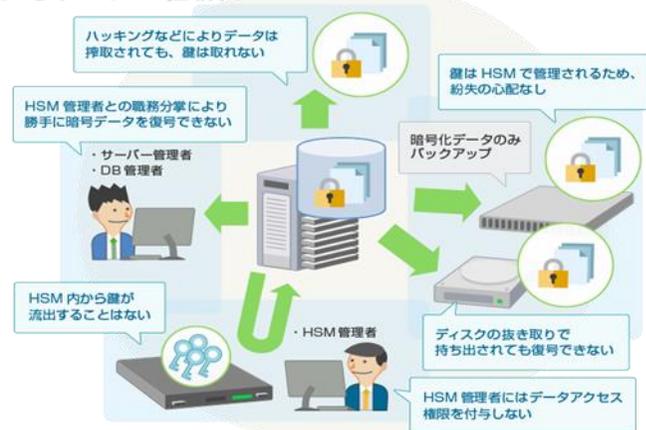
Luna Network HSMはネットワーク対応型の汎用HSM(ハードウェアセキュリティモジュール)です。

ハードウェア内で暗号鍵を厳重に管理し、暗号化データと暗号鍵を物理的に分ける事により、仮に暗号データが盗まれても、復号されるリスクが低減できます。

データ暗号化とリスク



HSMでの鍵管理によるリスクの低減



特長

- FIPS140-2(Level2,Level3)検証済み
- どのような形でも暗号鍵がHSM外に保存されることはない
- MofN認証(ユーザーおよび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)で不正な運用を排除
- 物理的な攻撃が発生すると、不正利用防止機能が起動し暗号鍵が自動削除される
- 導入が容易なネットワーク接続タイプ
- パフォーマンス要件によりモデルを選択可能
- 冗長化構成により信頼性とパフォーマンスの向上が可能
- 各種APIサポート(PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, REST等)

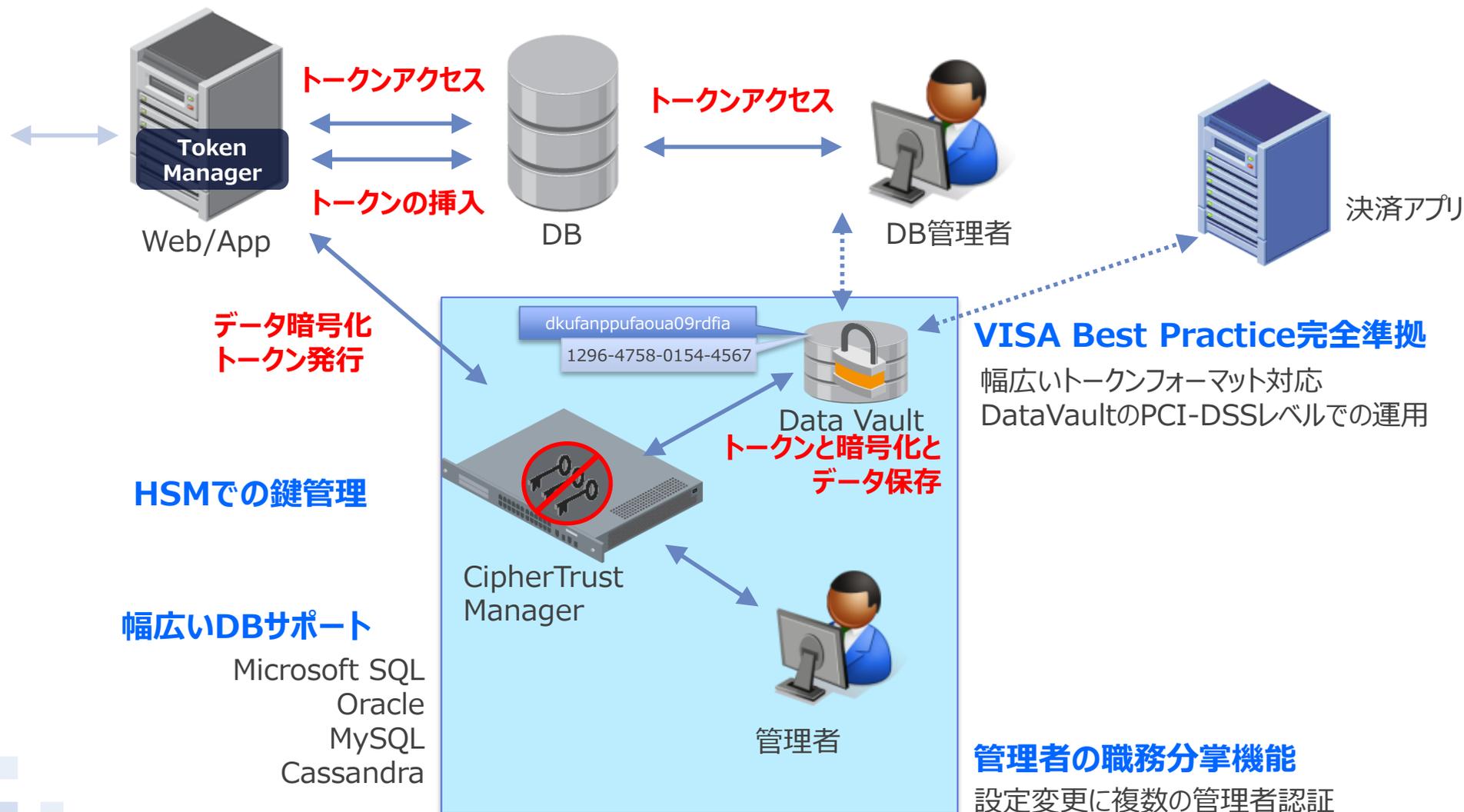
導入効果

- **機密情報の暗号化と厳重な鍵管理による情報漏洩対策**
- 職務分掌により内部からの情報漏洩リスクを低減
- PCI DSSの一部要件に適合可能
- 暗号鍵削除による論理的なデータ消去で安全にデータ廃棄

導入実績

- 主に金融機関、官公庁
- PKI鍵生成と保管(認証局)
 - 証明書検証と署名
 - データベース暗号化及び鍵管理
 - マスター鍵管理

CipherTrustManager(旧KeySecure)を利用したトークン化システム



トークン化と暗号化の違い

暗号化 : 1234-5678-0123-4567 → Fmqjper1m+j54!f@passu1a4jq&

アルゴリズムで暗号化・復号化
データ形式が変更される

トークン化 : 1234-5678-0123-4567 → 2963-4758-0154-2485

元のデータと関連のない意味のない文字列に変換
データ形式が変更なし

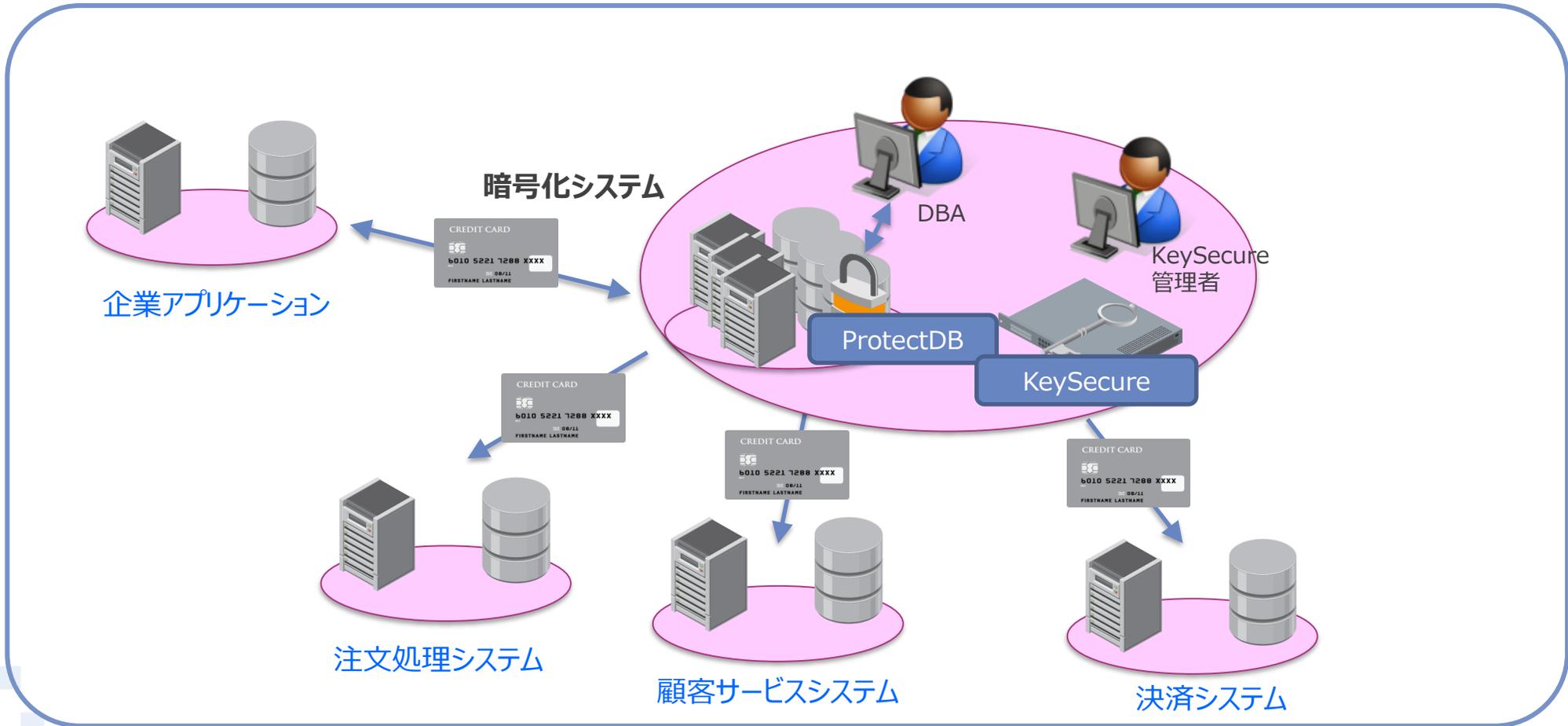
比較要素	暗号化	トークン化
システムパフォーマンスへの影響	大きい	小さい
既存システムに対する影響	大きい	小さい
PCI-DSS監査対象	対象	対象外
処理できるデータの種類	無制限	ID、アドレス、カード番号、生年月日等

⇒**TokenizationはDB暗号化以上にセキュアなデータ保存方式**

トークン化によるPCI-DSS監査範囲の低減

データベース暗号化の場合のPCI-DSS監査対象

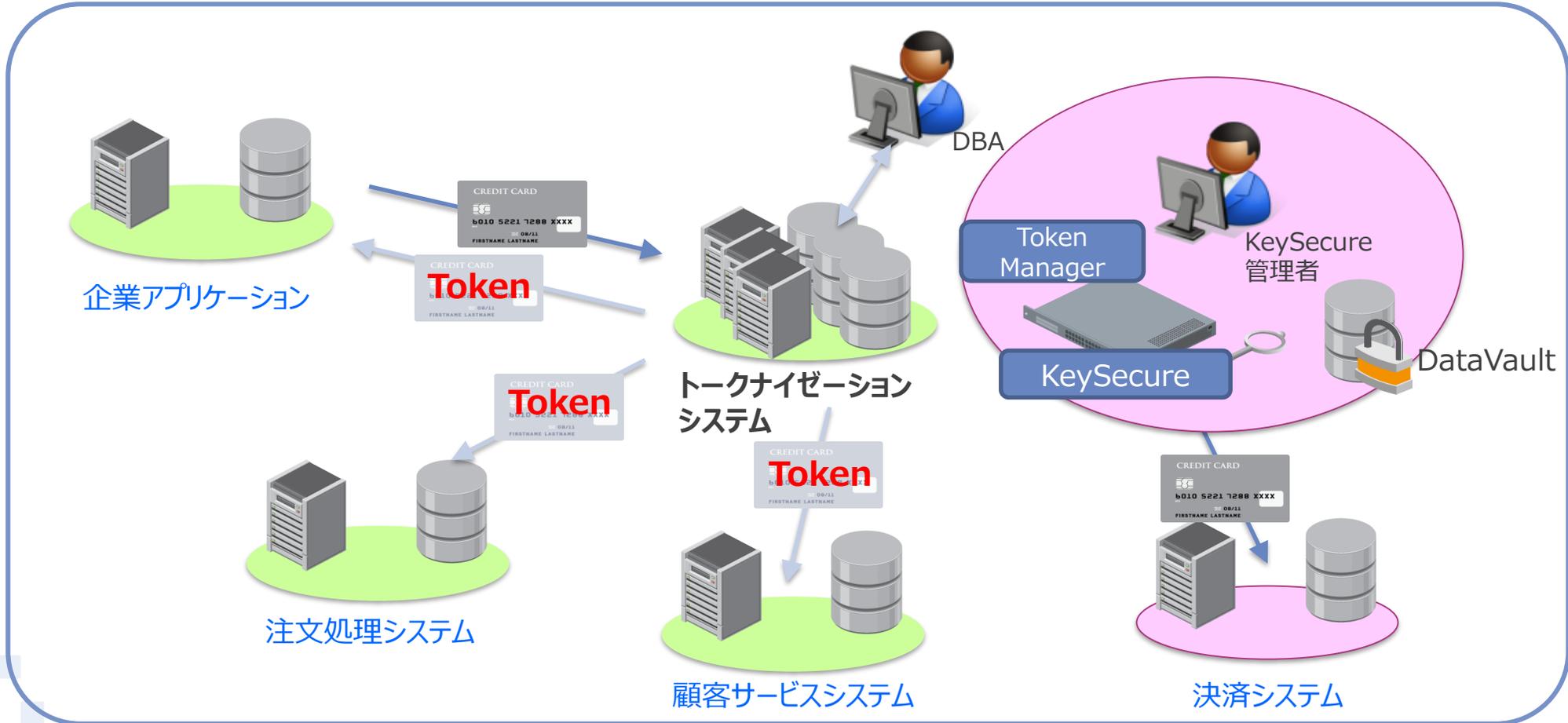
 : PCI-DSS監査範囲



トークン化によるPCI-DSS監査範囲の低減

トークン化の場合のPCI-DSS監査対象

○ : PCI-DSS監査範囲



ご清聴ありがとうございました。

製品の詳細説明や、お見積等のご相談は
お気軽にご連絡ください。

NTTデータ先端技術株式会社 セキュリティ事業部
Thales製品担当
il-HSM-sales@intellilink.co.jp





NTT DATA

Trusted Global Innovator