いち早く。より深く。さらに高みへ。

The Only One Value

決済HSMで実現するソリューション概要

～安全なクレジットカードネットワーク実現に向けて～

本日の内容

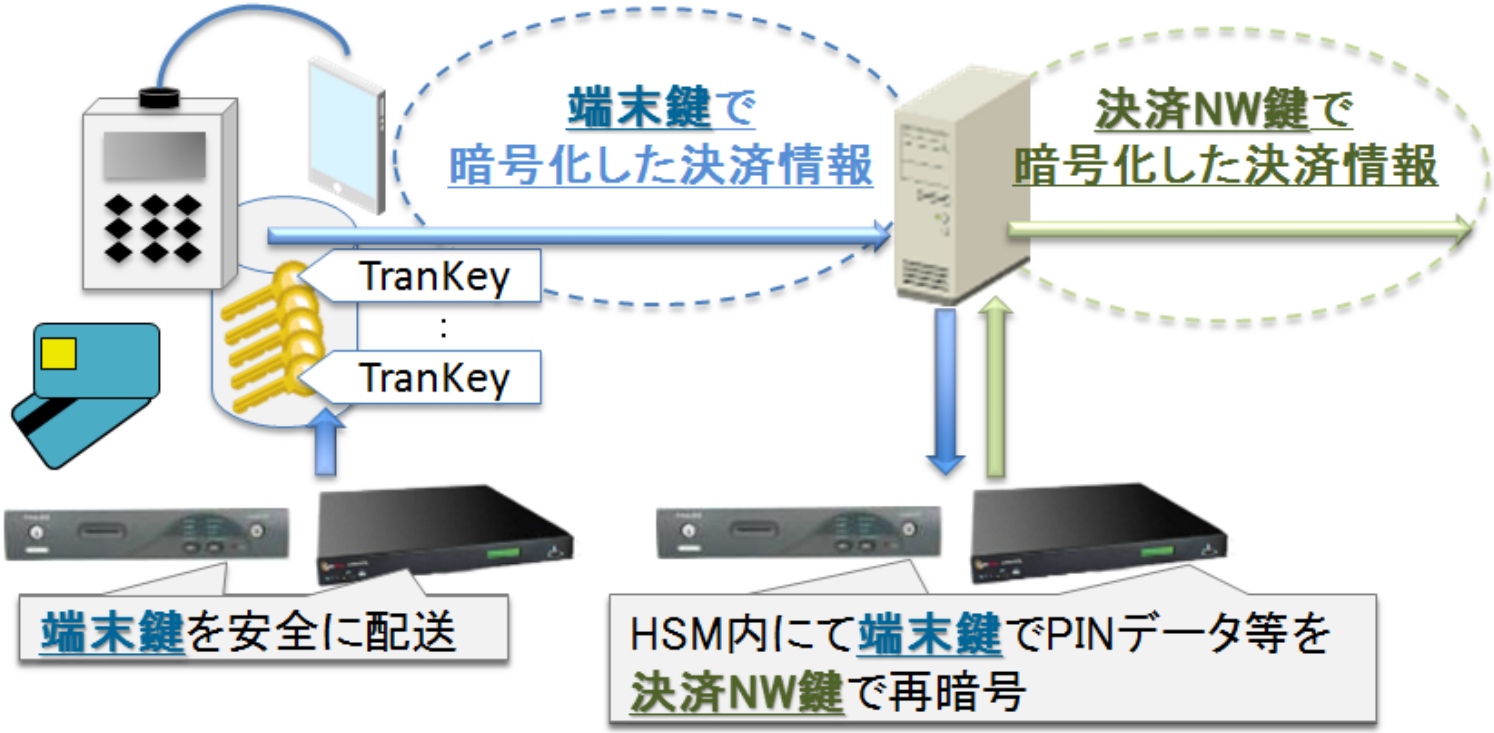
1. 決済HSMで実現するシステム概要
2. 決済HSMで権限を強固に分掌管理し悪用を阻止
3. まとめ

1. 決済HSMで実現するシステム概要

決済HSM概要

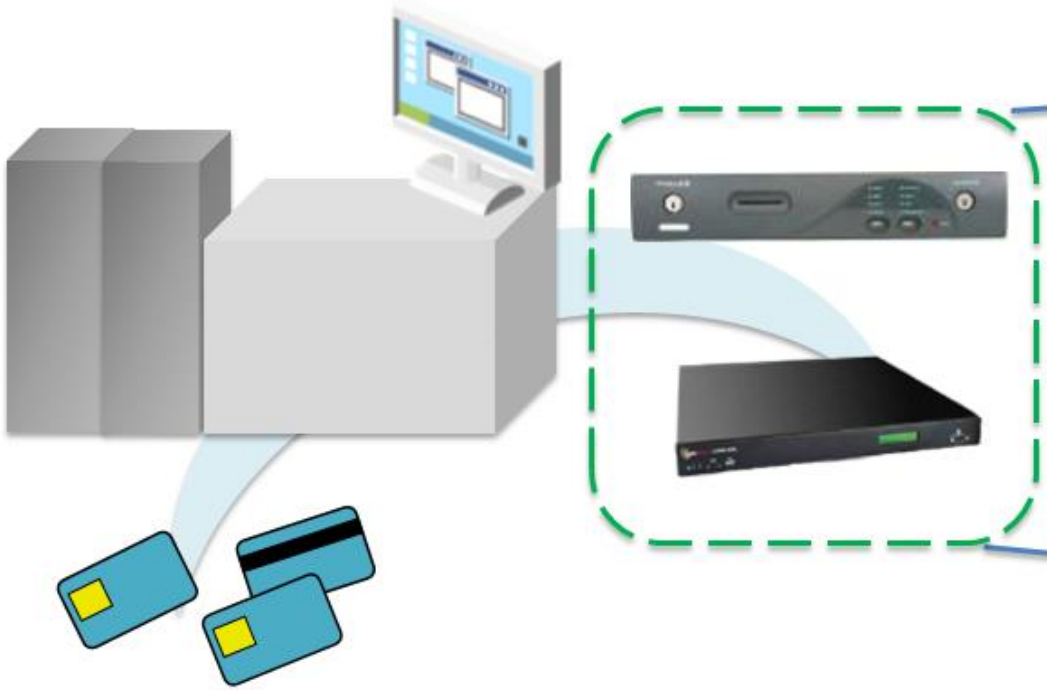
- 決済HSM
  - 決済システムの要件（PCIDSS）など、決済ネットワークのセキュリティ要件に追従し、暗号機能を追加
  - アクセスを厳重に管理して、セキュアに運用
- 利用形態
  - 端末鍵の発行
  - 決済ネットワークのスイッチ（暗号鍵の付け替え）
  - 各種クレジットカードブランドに対応した機能を提供

安全な決済の実現(P2PE)



P2PEに対応した鍵管理によって安全に決済を実現

各種国際クレジットブランドをサポート



1.クレジットカードPIN 生成
2.各種クレジットブランドCard 認証、検証、生成
3. EMV関連の機能
ETC.....

各種国際クレジットブランドのカードスキームに対応
クレジットカード情報を強固に保護

決済HSMで実現するシステム

- 暗号プロトコル変換
- PINデータの保護
（フォーマット変換etc..）
- 端末暗号鍵管理

- 「アクワイヤリング/銀行/カード発行業者」間での暗号鍵交換
- PINデータの保護
（フォーマット変換etc..）

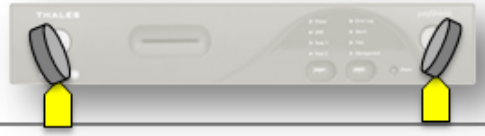
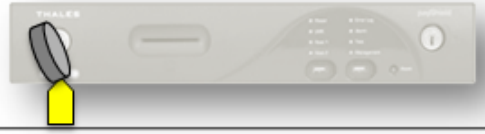
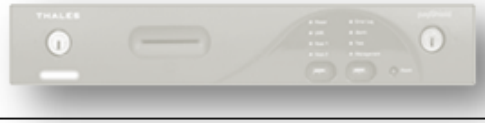
- 決済SWとの暗号鍵交換
- Card番号,PIN発行
- 決済データ検証
- EMV認証

決済要求
決済応答

2.　決済HSMで権限を強固に分掌管理し悪用を阻止

【payShield9000】権限分掌管理

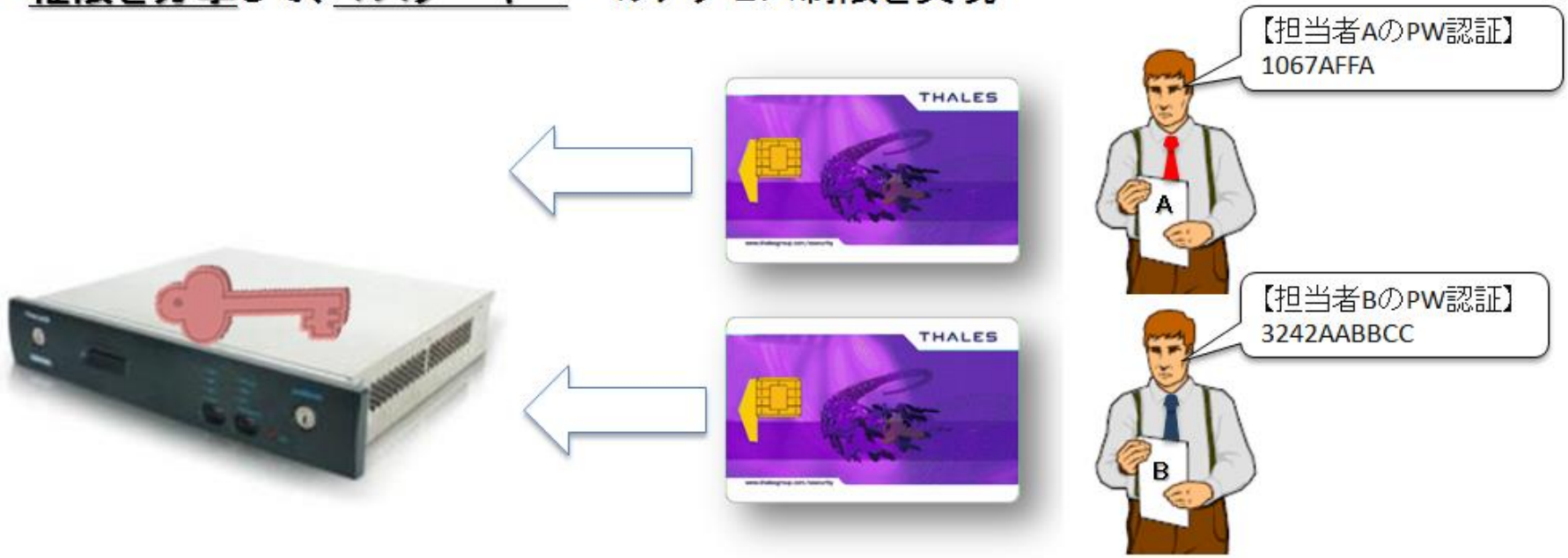
- 各物理鍵の状態と決済HSMのモード

payShieldのモード	説明
セキュリティ設定モード （Secure mode） 	決済HSMのセキュリティ設定を行うモード。 初期導入時や、セキュリティ設定を変更する際に本モードにて設定。
隔離モード （Offline mode） 	IPアドレスなどの1部の設定値を変更できるモード。 ログ確認の際に、本モードを推奨。
業務モード （Online mode） 	本モードにて決済処理を行える。 （TCP/IP通信にてコマンド投入可能）

セキュリティ設定の変更を物理鍵で制限

【payShield9000】権限分掌管理

- 2つ以上のスマートカードを使用して、マスターキーを生成
  ⇒**権限を分掌**して、**マスターキー**へのアクセス制限を実現



2人の権限者の許可（**スマートカード**と**暗証番号**）
がないと**マスターキー**の設定変更が不可能

【LunaEFT】USBトークンを用いて各種権限を分掌

各種USBトークン	説明
	移設等、機器設置時に使用許可を確認する際に認証
	EFTの設定変更等の操作権限を確認する際に認証
	暗号鍵バックアップ、リストア等の権限を確認する際に認証
	監査ログにかかわる操作権限を確認する際に認証

USBトークンとパスワード認証で各機能へのアクセスを個別に制限

3. まとめ

クレジットカードネットワーク中の決済HSM

- **クレジットカードネットワークの要所にて選ばれている理由**
  - 製品が提供する**厳格**な鍵管理によって悪用を阻止
  - **各種国際クレジットブランド**をサポート
  - 日々進歩する**セキュリティ要件に追従**

決済HSMで安全なクレジットカードネットワークを実現！

SaT
Security & Assistant Tools

クレジットカード取引におけるセキュリティ対策（PCI P2PE ソリューションについて）

2017/6/22

ネットムーブ株式会社

高田　理己

takada@netmove.co.jp

NetMove CORPORATION

What‘s provided by NetMove?

SaAT Security&Assistant Tools

セキュリティサービス

決済サービス

https://www.saat.jp

PCI Security Standards Council

PCI P2PE 認定取得に向けて監査対応中

NetMove CORPORATION

本日のお話し

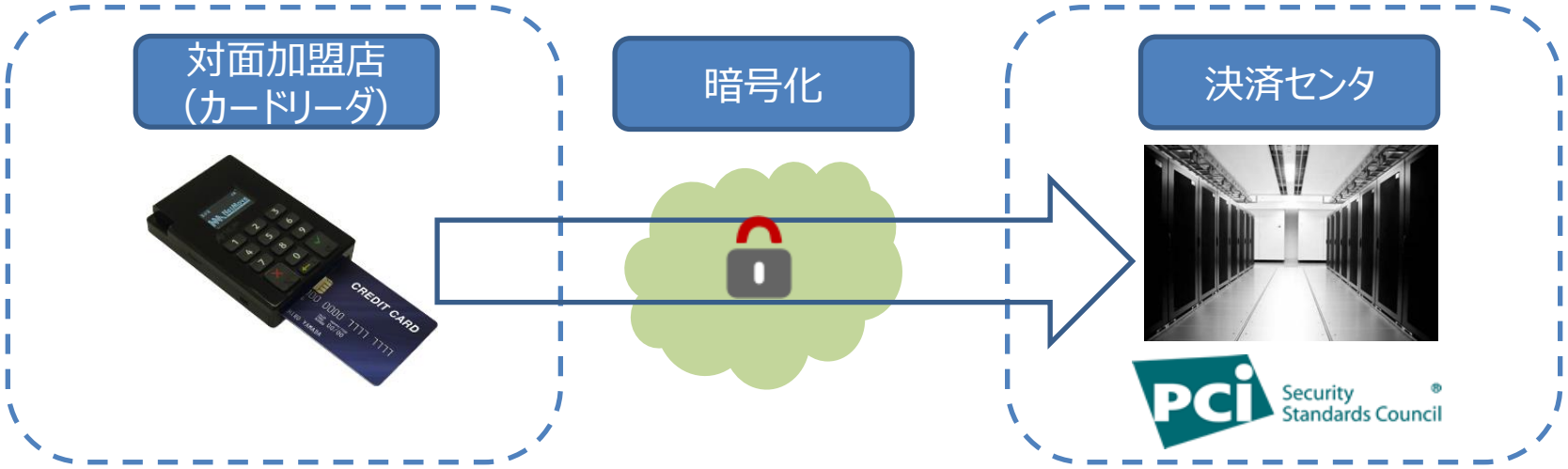
- ✓ PCI P2PE の概要
- ✓ PCI P2PE コンポーネント
- ✓ HSM を利用した P2PE キーマネジメント

PCI P2PE の概要についてお話しします

PCI P2PE（Point To Point Encryption）とは？

SaT Security&Assistant Tools

- ✓ 対面加盟店向けソリューション
- ✓ Point To Point でカード情報を暗号化



NetMove CORPORATION

経産省実行計画2017年版からの引用

クレジットカード取引における

セキュリティ対策の強化に向けた実行計画

－２０１７－

【公表版】

(2)対面加盟店におけるカード情報の非保持化についてより抜粋

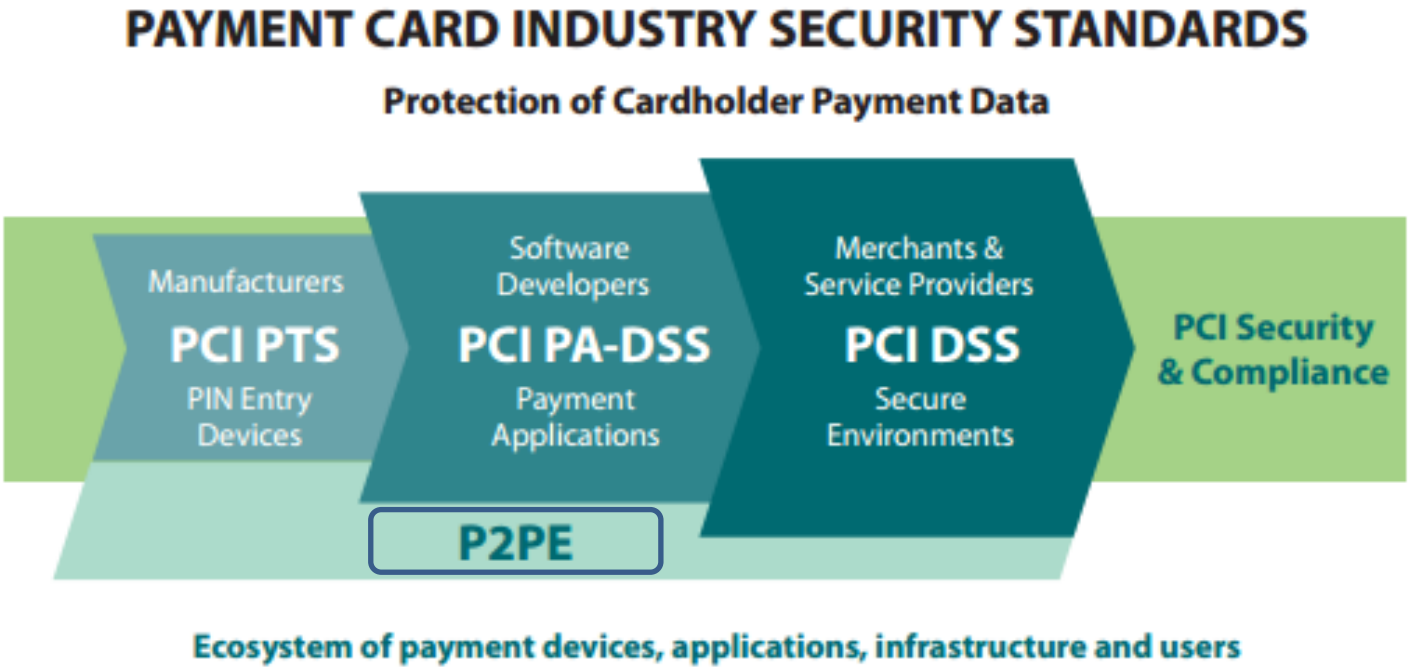
ただし、暗号化等の処理によりカード番号を特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正使用することは極めて困難であり、非保持と同等/相当のセキュリティが確保できるため、本実行計画においては、これを「非保持化」と同等/相当のセキュリティ措置として扱うものとする。こうした措置の一例として、PCI P2PE[6] (PCI Point to Point Encryption) がある。(「非保持化」と同等/相当のセキュリティ措置については後述（４）を参照)

２０１７年３月８日

クレジット取引セキュリティ対策協議会

PCI P2PE Overview（PCI SSC サイト引用）

- Only Council-listed P2PE solutions are recognized as meeting the requirements necessary for **merchants to reduce the scope of their cardholder data environment** through use of a P2PE solution. (PCI P2PE FAQ)



PCI DSS Quick Reference Guide Understanding PCI DSS v3.0

SAQ Validation Type P2PE

v3.2 SAQ Validation Type	Eligibility Criteria*	ASV Scan Required	Penetration Test Required
A Of Questions:22	Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage	No	No
D-MER Of Questions:331	All other SAQ-eligible merchants	Yes	Yes
P2PE Of Questions:33	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	No	No

PCIP2PE Solution Provider Service
利用時は自己問診33項目で加盟店は
PCIDSS準拠相当とみなされる

Self-Assessment Questionnaire P2PE（参考）

Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire P2PE and Attestation of Compliance

Merchants using Hardware Payment Terminals in a PCI SSC-Listed P2PE Solution Only – No Electronic Cardholder Data Storage

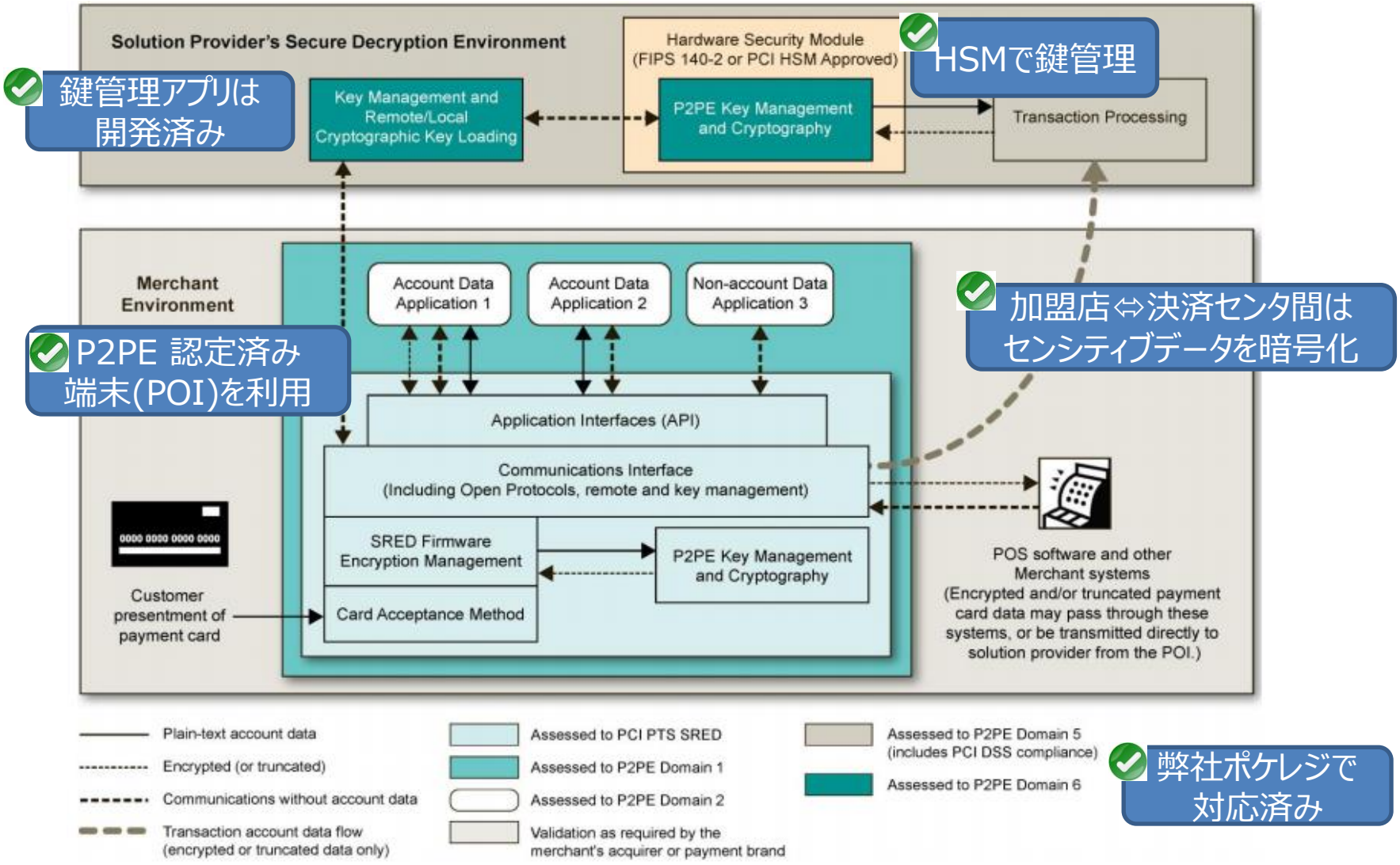
For use with PCI DSS Version 3.2

Revision 1.1

January 2017

続いて、P2PE において構成される コンポネントとソリューション全体の管理 について

PCI P2PE Components



鍵管理アプリは開発済み

HSMで鍵管理

P2PE 認定済み端末(POI)を利用

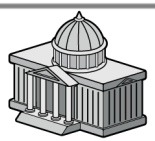
加盟店⇔決済センタ間はセンシティブデータを暗号化

弊社ポケレジで対応済み

Example P2PE Implementation at a Glance

PCI P2PE Domains (High Level Summary of Six P2PE Domains)

SaAT Security&Assistant Tools

Domain 1 – Security requirements for the 暗号化端末 アプリ管理	MIURA SYSTEMS  ロジスティクス  NetMove CORPORATION
暗号化アプリ セキュリティ	MIURA SYSTEMS
Domain 3 – For P2PE solution management P2PEソリューション管理	NetMove CORPORATION
加盟店管理 ソリューション	N/A(Not Applicable)
Domain 5 – Security 復号化環境	 gemalto security to be free macnica networks NetMove CORPORATION
Domain 6 – P2PE Key 鍵管理 運用全般	MIURA SYSTEMS    NetMove CORPORATION

NetMove CORPORATION

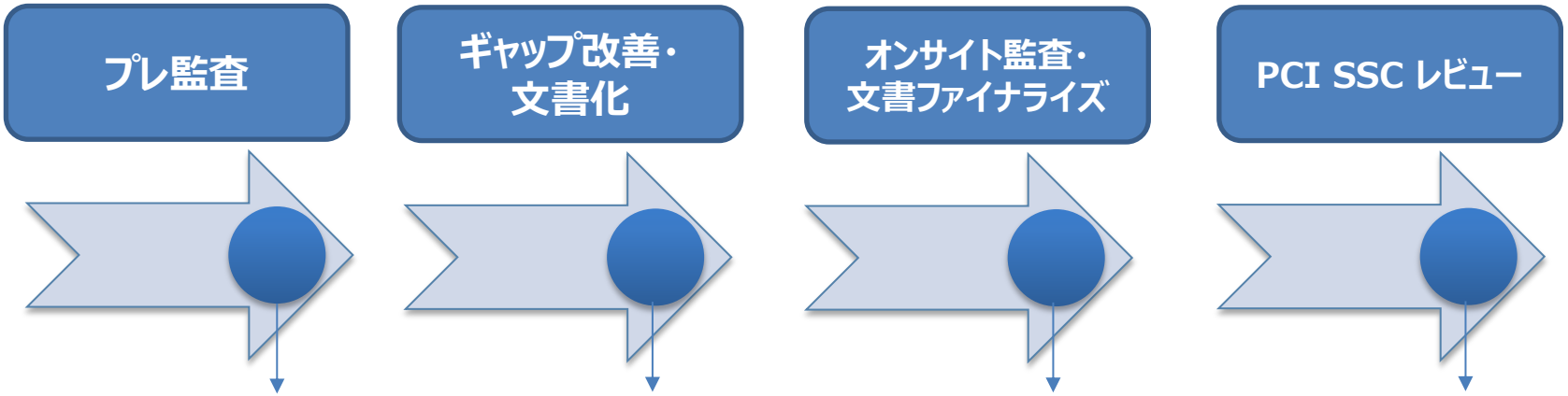
PCI P2PE Component Provider

Added new diagram to explain relationships between P2PE solution providers, **P2PE component providers**, and other third parties.(Summary of Change P2PE 1.1 to 2.0)

Miura Certified PCI P2PE Component Provider

- PCI P2PE Domain2 (Application Security):2016/10/10
- PCI P2PE Domain6 (Cryptographic Key Operations and Device Management) – Annex A2: (CA Operations): 2016/9/22

PCI P2PE 認定取得プロセス例



- ✓ プレ監査結果
- ✓ ギャップ分析結果

< ~2ヶ月

- ✓ ギャップ改善対応
- ✓ 監査用文書

< ~2ヶ月

- ✓ 監査報告書
- ✓ PCI SSC への報告

< ~1ヶ月

- ✓ 認定取得!!

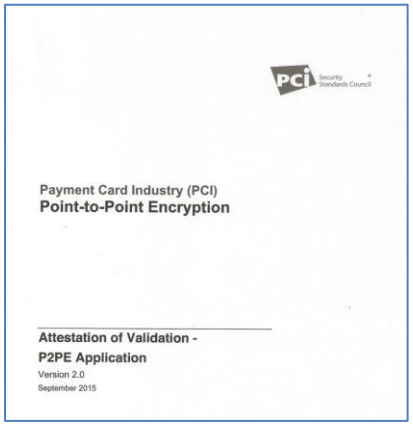
< 2~3 ヶ月

PCI P2PE ソリューションプロバイダの責務

- ✓ P2PE 対応可能なコンポーネントの選定
- ✓ 責任、役割分担を明確に規定
- ✓ 運用体制の確立

PCI P2PE 監査提出証跡例

Approval



3rd Party Agreement

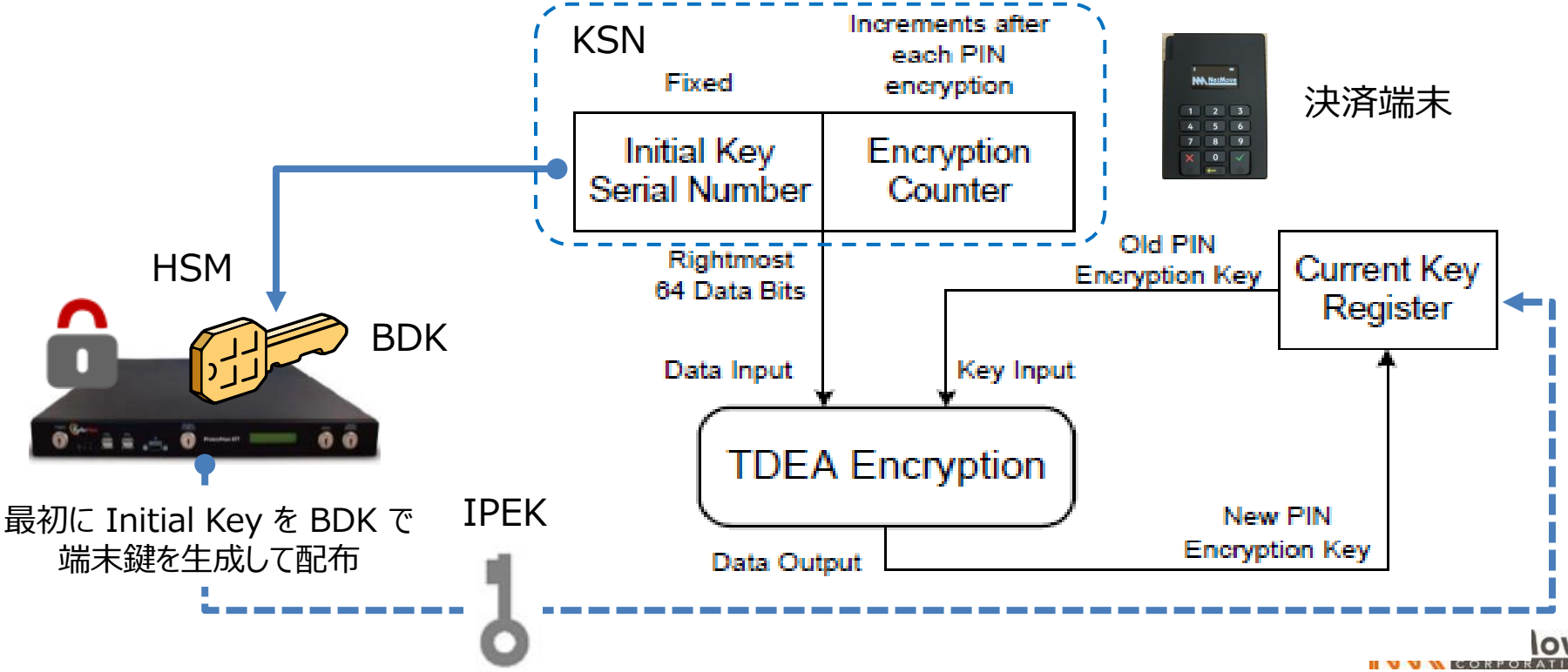
Manual

Logs

最後に、PCI-P2PE における HSM を利用したキーマネジメントについてお話しします

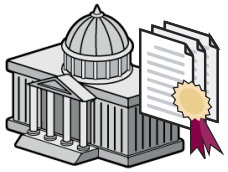
What's "DUKPT"? (P2PE Core Key Management)

- Derived Unique Key Per Transaction, トランザクション毎に異なるユニークな暗号鍵を使うことで暗号鍵の危殆化を防止する仕組み
- BDK（Base Derivation Key）を用いて端末毎に異なる鍵を生成
  - BDK が危殆化した際には決済システムの鍵が判別できてしまう
  - P2PE では BDK は HSM に格納して厳重に管理することが義務付けられている



Remote Key Injection

PCI P2PE Domain6 Annex A1
(Remote Key Distribution using Asymmetric Techniques)



Terminal + CA Cert

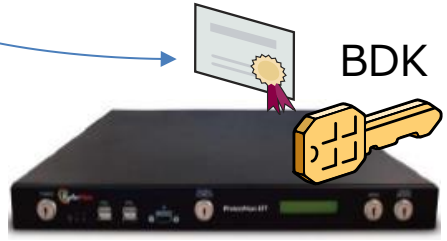
CA

HSM + CA Cert

Suggested IKSN

Terminal Cert

Verify



BDK

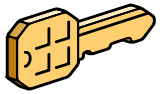
Inject

Decrypt

IPEK

TMK

+



Generate

IPEK

Encrypt

TMK

Decrypt

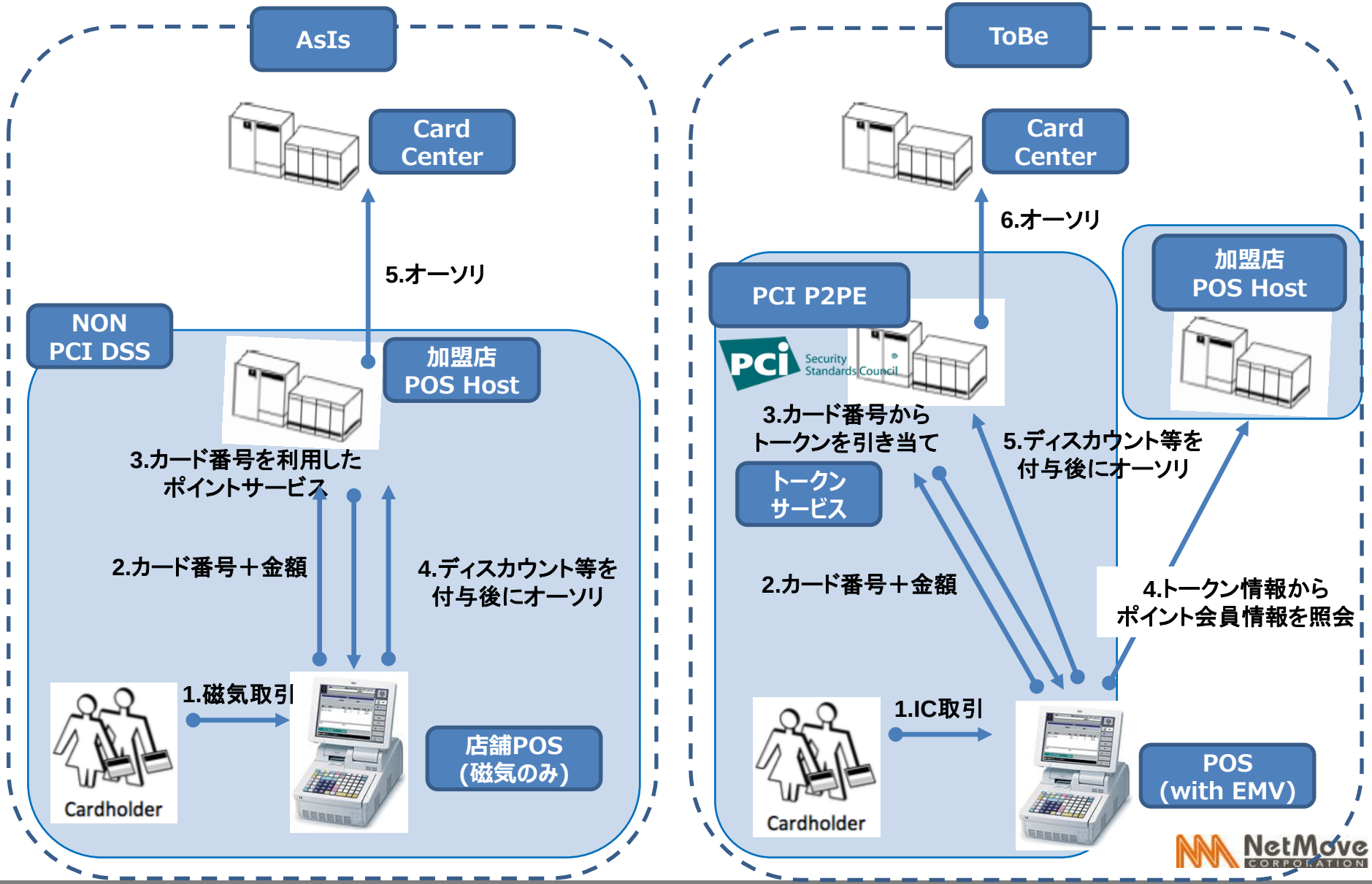
Verify

Encrypt & Sign

NetMove CORPORATION

ご提供サービス形態イメージ(ご参考)

PCI P2PE マイグレーション例（AsIs – ToBe)

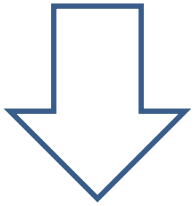


PCI P2PE ソリューションまとめ

SaT Security & Assistant Tools

✓ 対面式決済を Point To Point で暗号化

✓ 単に暗号化すれば良いというわけではない
- 適正な暗号鍵のキーマネジメント
- ソリューションとしての厳正な管理体制



✓ セキュリティを担保しつつ、加盟店の責務・負荷は軽減される

NetMove CORPORATION