payment navi
カード情報ポータルサイト

SaT
Security&Assistant Tools

不正使用対策・PCIDSSセキュリティセミナー2017

POS加盟店向けクレジットカード セキュリティ対策のご紹介

2017/9/5

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

- ✓ **IC（EMV）化対応済み**
- ✓ **PCI P2PE 認定取得対応中**

SaAT ポケレジ

NetMove CORPORATION

本日のお話し

- ✓ 決済端末の IC 化対応について
- ✓ PCI P2PE について
  （カード情報非保持化措置の一例）

IC化（EMV対応）について

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】

B. クレジットカード偽造防止対策等の強化に向けた実行計画

６．2017 年度中に重点的に実施すべき具体的な取組について

本実行計画を踏まえて、安全・安心なクレジットカードの利用環境の実現を図ることとする。平成 28 年度経済産業省委託調査（平成 28 年 10 月時点）によれば、加盟店の決済端末の IC 対応完了は全体で 16.7%であり、規模の大きい加盟店ほど対策が遅れている結果が得られている。

改正割賦販売法により、加盟店における不正利用防止措置が義務化されることを踏まえ、その施行に向け、決済端末の IC 対応を早急に進めていく必要がある。

２０１７年３月８日

クレジット取引セキュリティ対策協議会

2014年版研究会中間報告書引用（参考）

クレジットカード決済の健全な発展に向けた研究会

（ＩＣ化）
国内決済の約８３%が「磁気端末」で決済され、クレジットカード等がＩＣ化されてもＩＣ決済が進んでいないのが現状である。

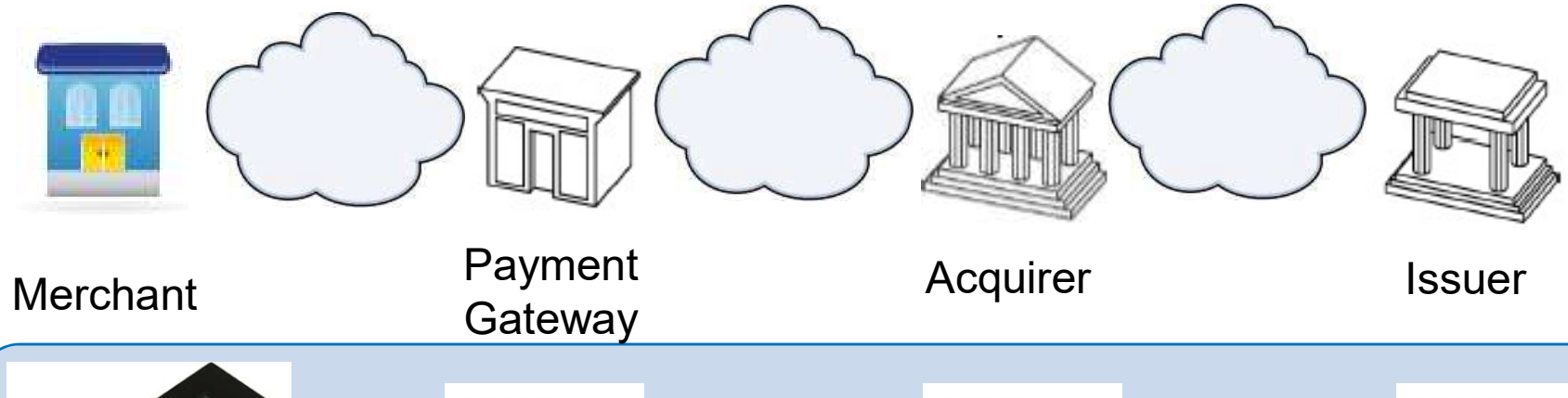
課題

- ✓IC 化対応オペレーションの導入
- ✓IC 化対応システム固有の導入プロセス

平成２６年７月

経済産業省

IC 化（EMV）ブランド認定テスト



EMVCo VISA MasterCard JCB

EMV認定済み
端末(POI)を利用

AMERICAN EXPRESS Diners Club INTERNATIONAL

ブランド指定のパラメータ
テストカードで
End To End でテスト

ポケレジ　ブランド認定の歩み（ご参考）

SaT Security&Assistant Tools

SaT ポケレジ

VISA

ADVT:Jan-2015

MasterCard

MTIP:Mar-2015

接触IC

JCB

TCI:Feb-2015

AMERICAN EXPRESS

AEIPS:Feb-2017

Diners Club INTERNATIONAL

DPAS:Jun-2017

非接触IC

VISA

qVSDC:Apr-2016

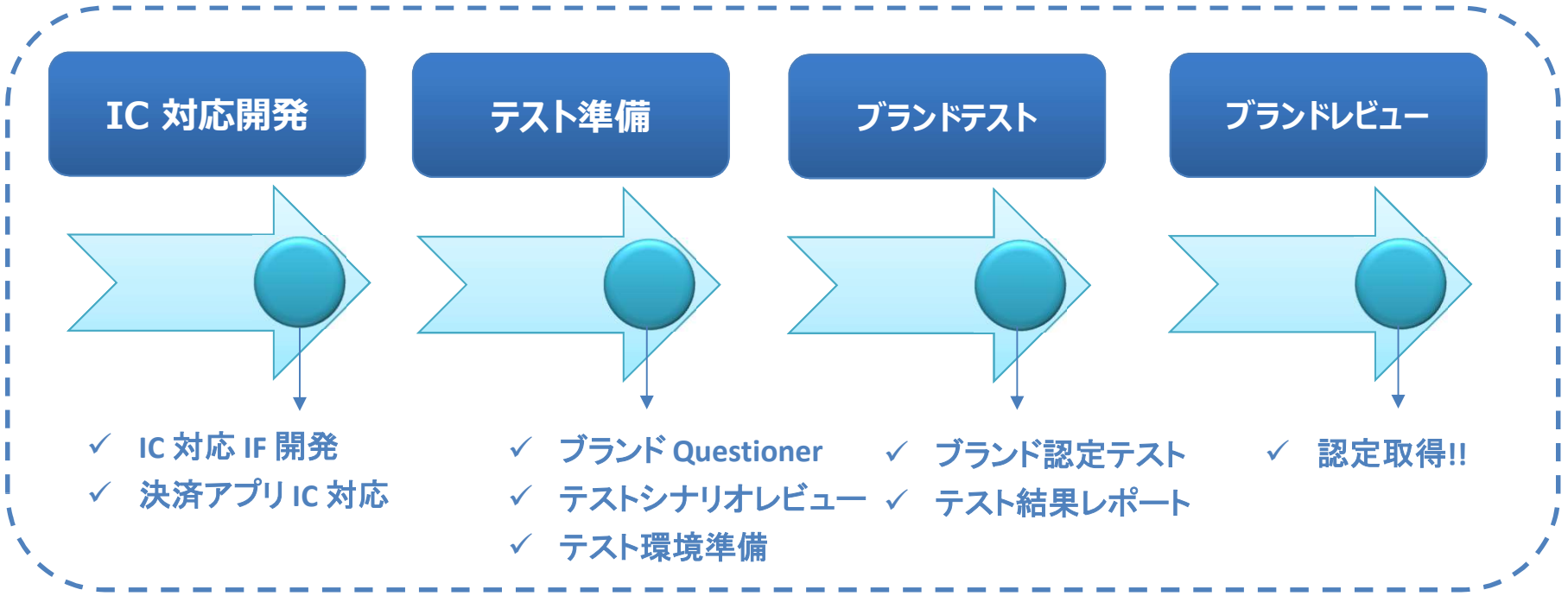
MasterCard

MastercardContactless:
Jul-2016

NetMove CORPORATION

ブランド認定取得プロセス

SaT Security&Assistant Tools



マネージド EMV サービス

✓EMV 対応インフラのご提供

✓ブランドテストプロセス支援

※現在 3ベンダー5機種、弊社EMV対応インフラでブランド認定取得済み

NetMove CORPORATION

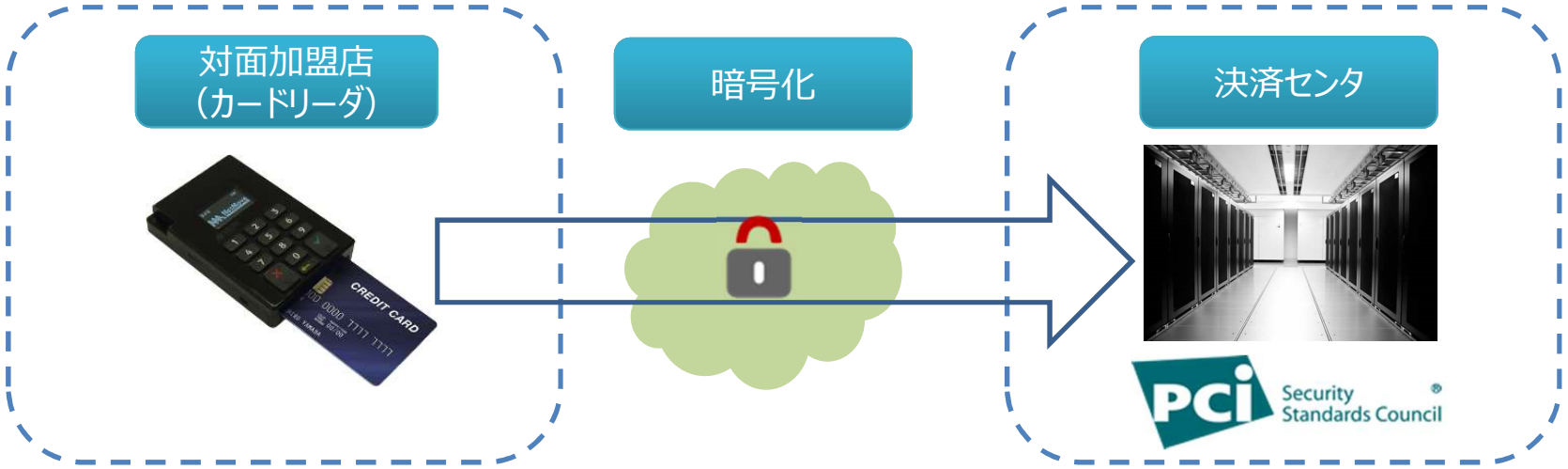
カード情報非保持化措置の一例
PCI P2PE について

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】

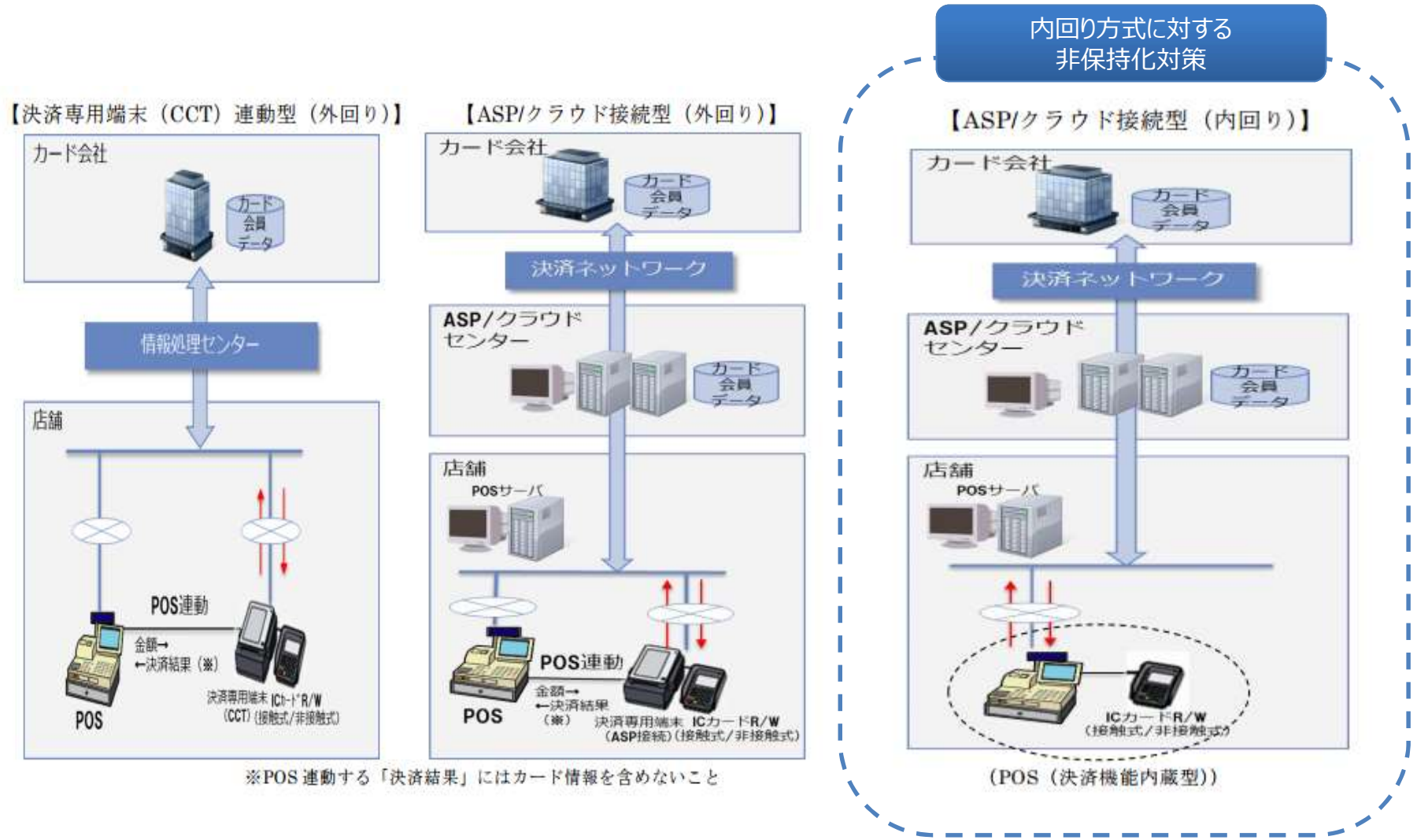
(2)対面加盟店におけるカード情報の非保持化についてより抜粋

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

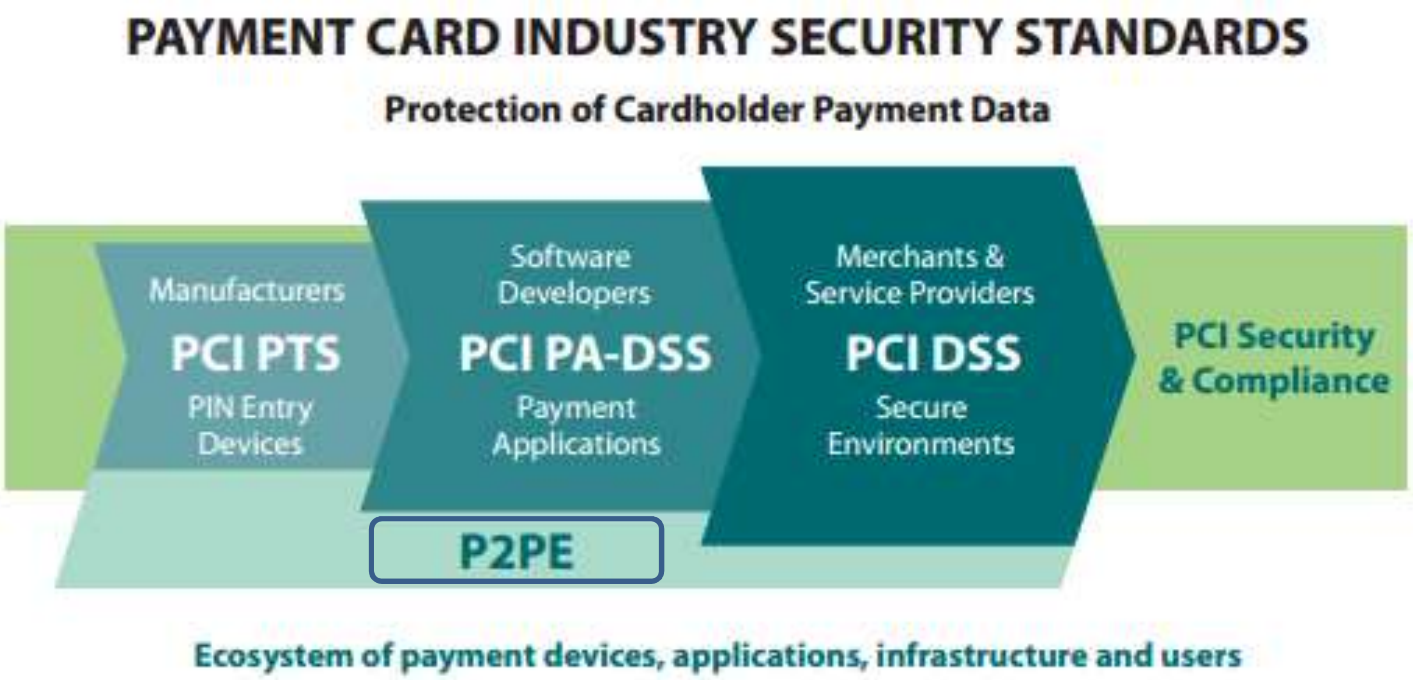
経産省実行計画2017年版からの引用



※POS 連動する「決済結果」にはカード情報を含めないこと

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

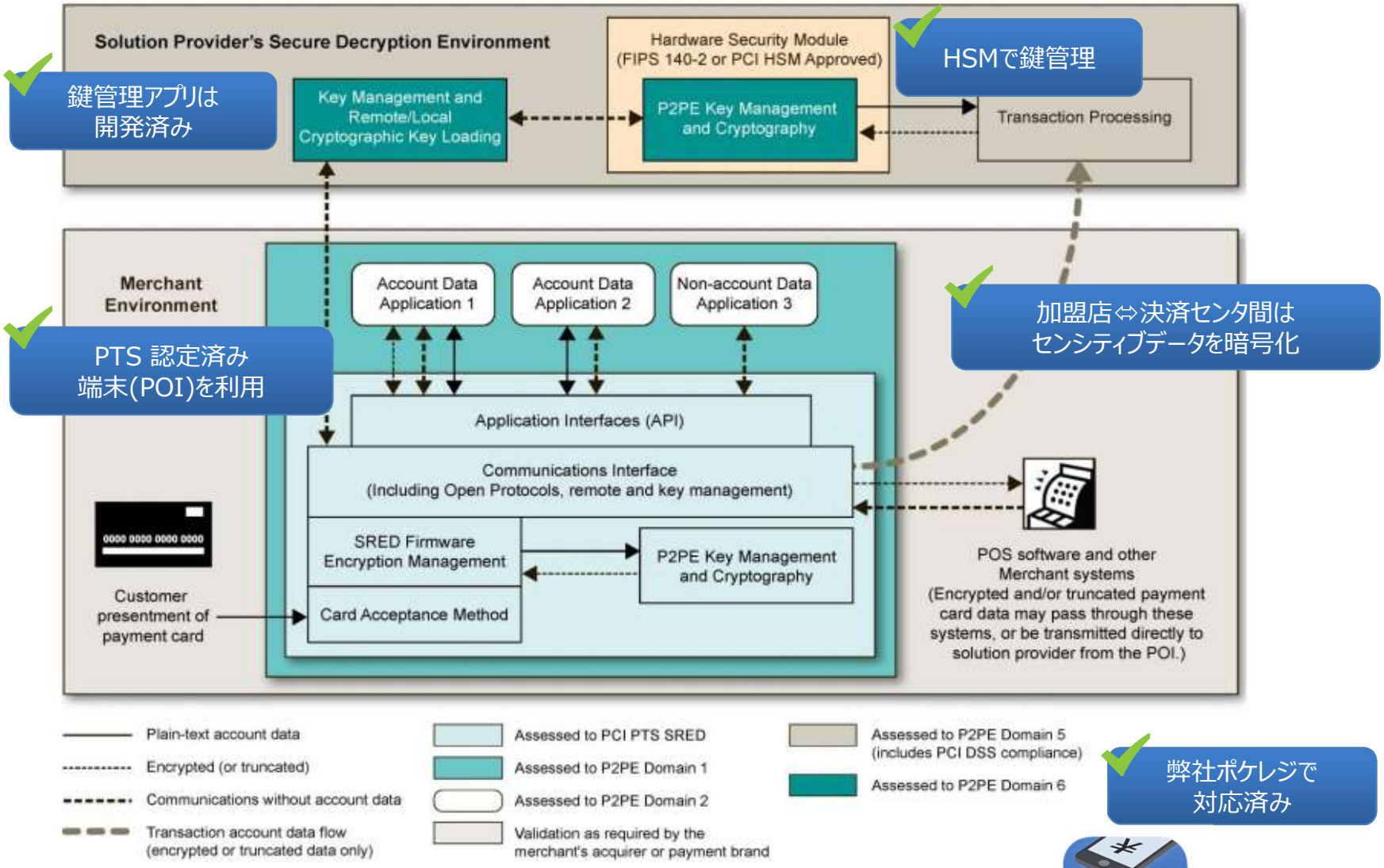
For use with PCI DSS Version 3.2

Revision 1.1

January 2017

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

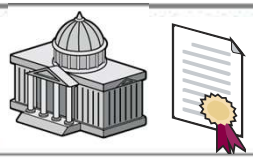
PTS 認定済み
端末(POI)を利用

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)

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  NetMove CORPORATION
Domain 6 – P2PE Key 鍵管理 運用全般	MIURA SYSTEMS  NetMove CORPORATION

NetMove CORPORATION

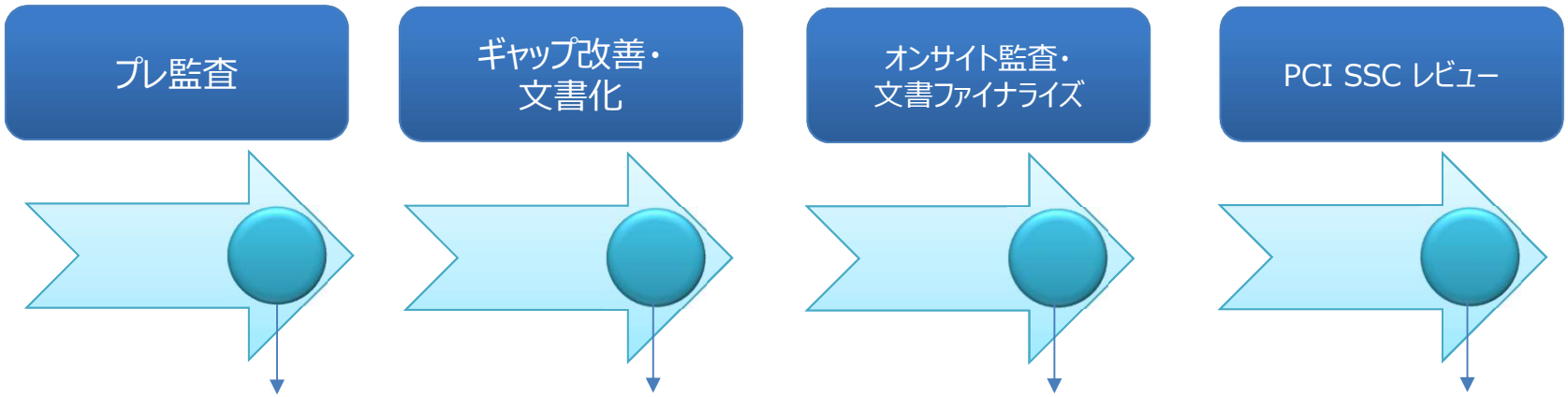
PCI P2PE Component Provider

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!!

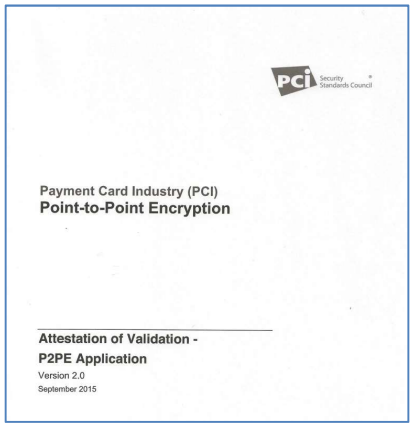
< 2~3 ヶ月

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

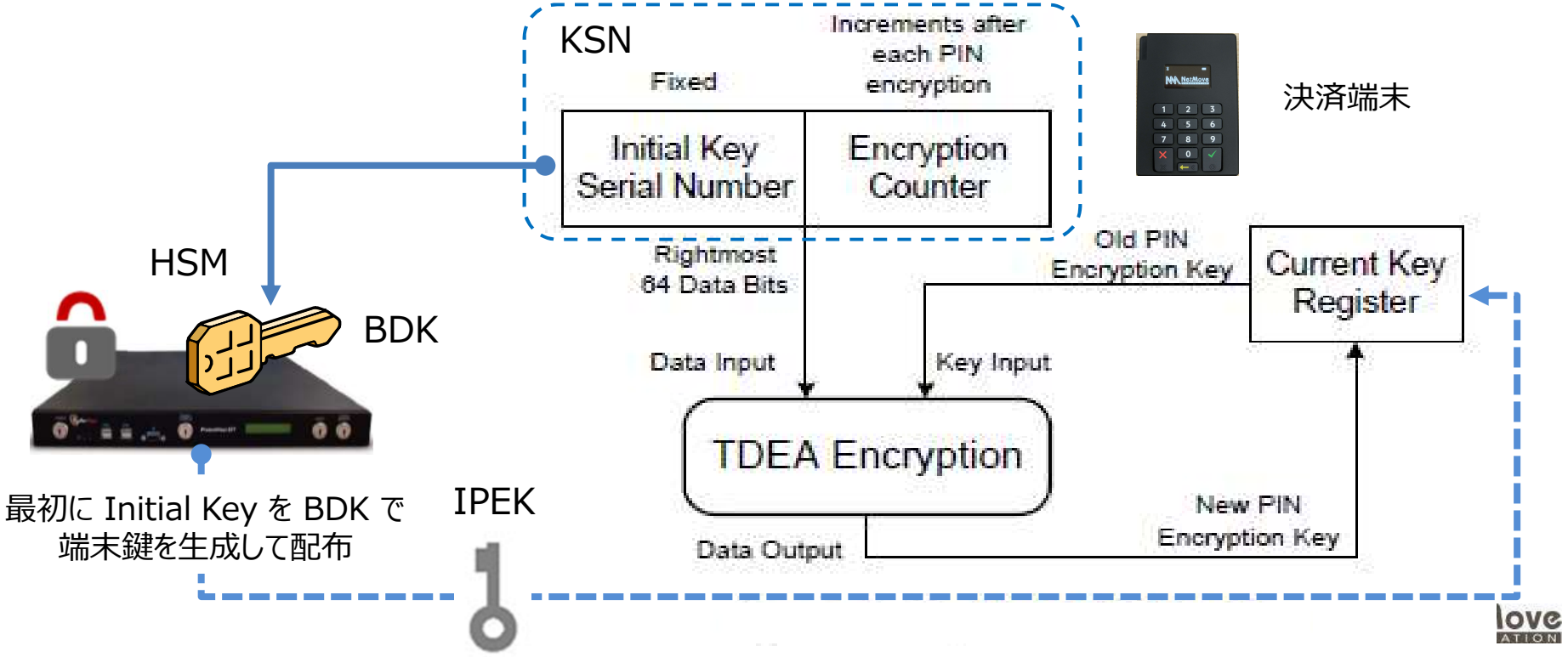
Logs

PCI-P2PE における
キーマネジメントについて

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

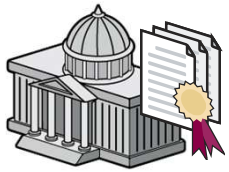
- Derived Unique Key Per Transaction,
  - トランザクション毎に異なるユニークな暗号鍵を使うことで暗号鍵の危殆化を防止する仕組み

- 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

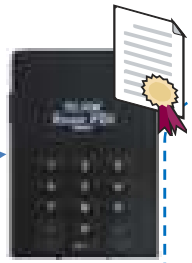
PCI P2PE Domain6 Annex A1
(Remote Key Distribution using Asymmetric Techniques)



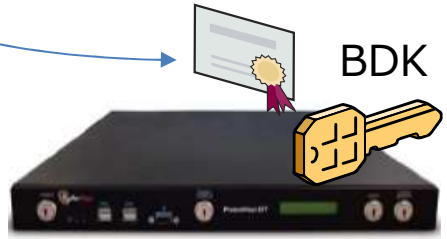
CA

Terminal + CA Cert

HSM + CA Cert



Verify



BDK

Suggested IKSN

Terminal Cert

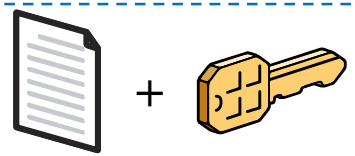
Inject

Decrypt

IPEK

TMK

Generate

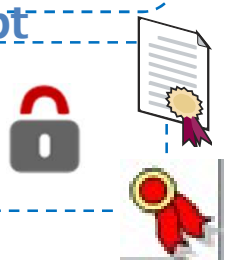


IPEK

TMK

Encrypt

Decrypt

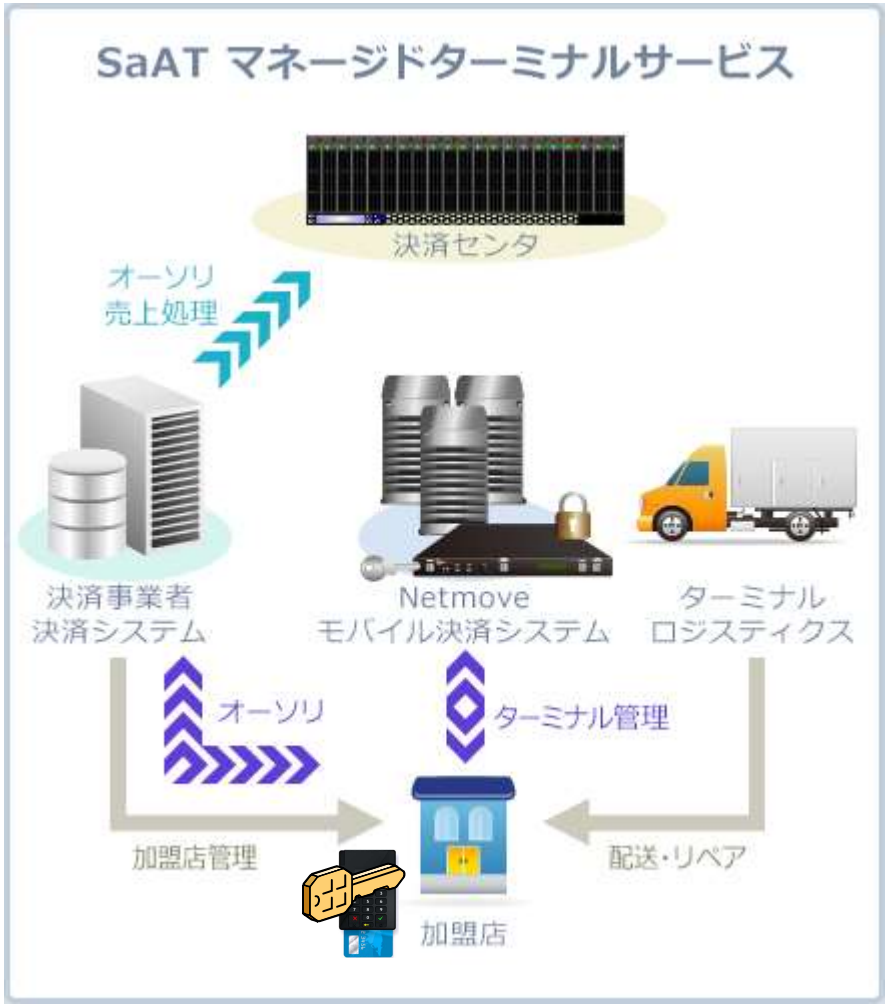


Verify

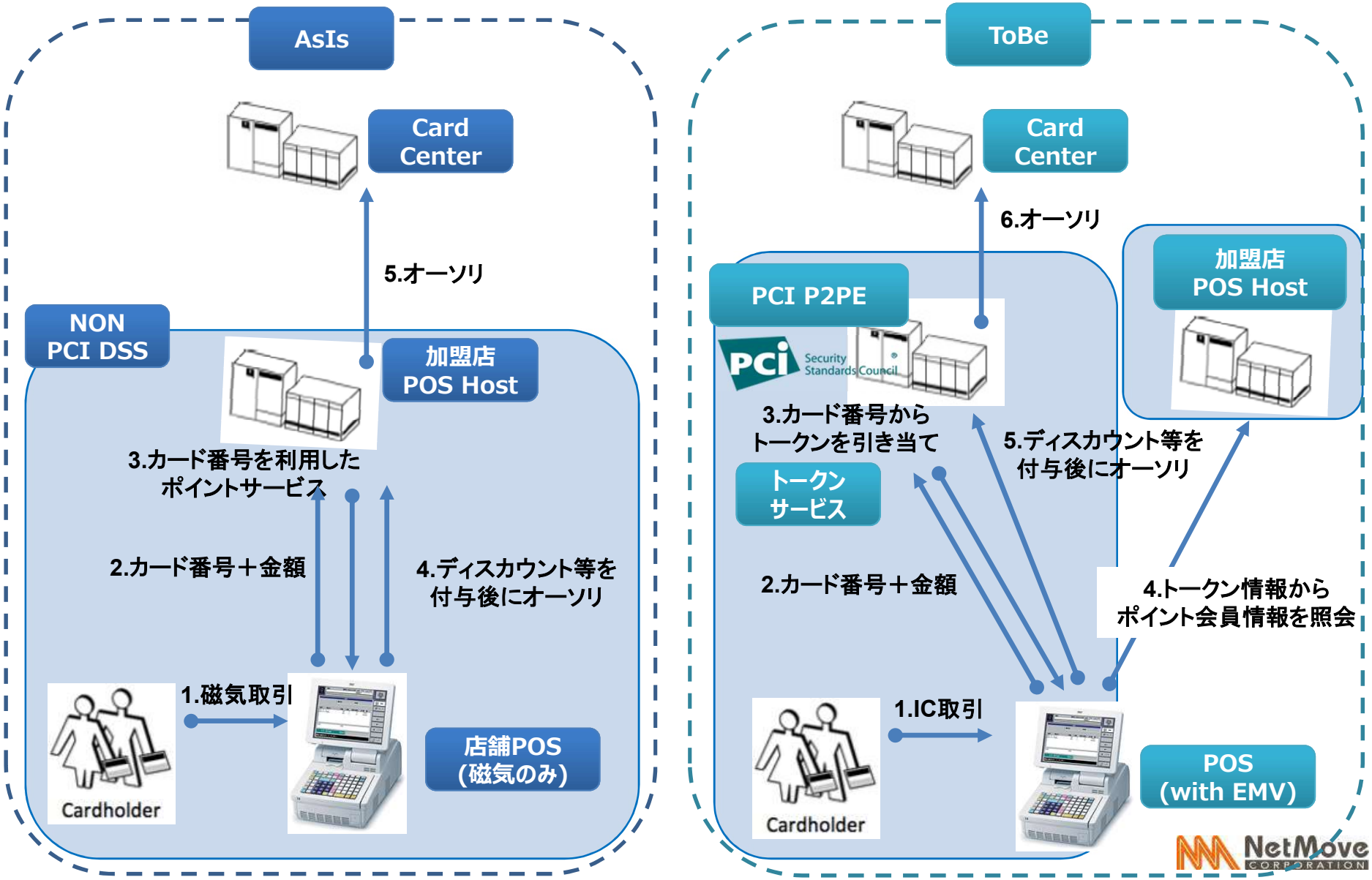
Encrypt & Sign

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)



本日のまとめ

SaT Security&Assistant Tools

IC化対応

✓単に IC 端末を導入すれば良いというわけではない

✓IC 化システム導入プロセスを支援するサービスが必要

非保持化措置における PCIP2PE

✓ 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

NetMove CORPORATION

本件のお問合せ先

ネットムーブ株式会社　ITC事業部　ポケレジ担当

Tel：03-6256-9628
E-mail：credit@netmove.co.jp