THALES

“もたない”
“PCI-DSS準拠”だけでは不十分？

PCIDSSセキュリティフォーラム 2016
クレジットカード・決済情報保護の最前線

タレスジャパン株式会社
e-セキュリティ事業部
山神真吾

事実①：PCI-DSSに準拠した企業も漏洩事件を起こしている

- 2013年11月　米国：大型小売チェーン（カード情報：4000万件流出）
- 2015年12月　世界的なホテルチェーン（カード情報：件数非公開、日本国内も含む）

なぜ？

- 運用上の課題：「素晴らしい」システムが導入されていても使いこなせていない
- PCI-DSSへの取り組みが、実際のところ、年1回の監査のみに集中
- 審査後の実際の運用まで、セキュリティ・ポリシーが徹底されていない

PCI-SSC側の取り組み

→　PCI-DSS v3.0より「PCI-DSSを日常業務（BAU）プロセス内に実装すること」について言及しはじめる

→　PCI-DSS v3.2より要件6.4.6「変更管理プロセスに関する要件」が追加され、2018年以降、準拠がもとめられる

事実②：「非保持」なはずなのに漏洩事件が発生

カード情報は自社で保管していないはず…

- 2013年３月　　大手眼鏡チェーン（カード情報：2059件流出）
- 2016年4月　　EC・B2B卸　　（カード情報：7386件流出）

なぜ？

- ECサイト運営・システム開発の丸投げ？　→　カード情報を扱う「当事者意識」が希薄
- WEBサーバの脆弱性（Apache Struts2やHeartbleed）による不正アクセス
- カード情報の入力フォームを改ざん
- クレジットカード情報の不正取得

METI・JCCA側の取り組み

→　カード情報を保持する場合はPCI-DSSに準拠するように指導…

→　加盟店側のサーバーを通過しない「非通過型」決済導入を推進

THALES

事実③：「トークン化」「マスキング」でも漏洩の可能性はゼロではない

- 2016年3月 PCI-DSS レベル１の決済ゲートウエイサービス
- 直接的な不正利用被害はないにせよ、個人を特定する情報は漏れている
- PANが判読不可能であったとしても、PANに紐づくカード会員データ要素は保護が必要

なぜ？

- APIの実装の問題・使い方

対策

決済代行サービス事業者との定期的なAPIの使い方の確認

要件11「セキュリティシステムおよびプロセスを定期的にテストする」

「画面遷移型（リンク型）」 → **SAQタイプA**の自己問診の実施

「非画面遷移型（モジュール型）＋非保持サービス」 → **SAQタイプC**の自己問診の実施

（参考）PCI-DSS v2 e-Commerce Guidelines

- “E-commerce payment processor should provide instruction and guidance to the merchant for secure implementation and practices for the API on the merchant’s web site.”
- 「Eコマースの決済代行事業者は、EC加盟店側に組み込まれるAPIの安全な実装・運用を実現するための適切な手順と指示をEC加盟店に対して提供しなければならない。」
- “Merchant still has responsibility for PCI DSS requirements for some elements of the e-commerce infrastructure even though they have outsourced much PCI DSS responsibility for storage, processing, and transmission of cardholder data.”
- 「EC加盟店は、カード情報の格納、伝送、決済処理を外部委託しPCI-DSSの要件対応の大部分を決済代行サービスに任せても、EC環境のセキュリティに関するPCI-DSS要件を満たす責任がある」

事実④：業務委託先からの漏洩

委託元で保管しているカード情報は暗号化し、PCI-DSSの監査も受けていた…

- 2009年　世界的なソフトウエア企業（カード情報：件数は非公開）

なぜ？

- カスタマ・サービス業務の委託先からカード情報が漏洩
- カード情報を共有するグループ内での内部不正

委託元が実施した改善策

- 事件の引き金となった業務委託先との契約解除

PCI-SSC側の取り組み

＞PCI-DSS v3.0以降　要件12.8の明確化により、「カード会員データ委託元として、委託先を管理する責任」「委託先との責任分岐点の文書化」が求められるようになっている。

＞委託先監督責任は重要！

過去の事件からの教訓（まとめ）

- PCI-DSSの準拠はゴールではなく、スタート!
- 継続的なセキュリティ改善を進める意識
- 「落とし穴」を見つけ、対策する姿勢
- 日常業務（BAU）・運用プロセスの見直し
- 非保持サービス・決済代行サービスを利用しても、カード情報を保護する責任は免れない（SAQ-A, SAQ-C）
- 業務委託先の監督責任と責任分岐点の文書化

もちろん、簡単なことではありません！

タレスが提供するPCI関連コンサルティングサービス

ラグビーワールドカップや東京オリンピックの開催が決定し、訪日旅行者（インバウンド）の数が年間2000万人を超えるように予測されています。クレジット協会もすべての加盟店に対して、2018年3月までに、対面/POS取引のPCI-DSS準拠あるいはクレジットカード情報を保持せず、サーバ・クラウドで徹底管理するような実行計画を定めています。PCI-DSSは改正割賦法が求めるセキュリティ基準と位置付けられたこともあり、カード情報の安全性を確保することはもはや必然的な責務と言えます。

タレスはその専門知識を展開し、事前評価やコンサルティングサービスを通じてお客様の標準適合作業を支援することができるほか、一定の領域においてはQSA（PCI-SSC公認の監査人）として正式なPCI-DSSの監査を行うことも可能です。

- Scope Review / Reduction
- Gap Analysis
- Remediation
- Policies & Procedures
- Attestation (ROC & AOC)
- Awareness Training

タレス・サイバー・セキュリティ・コンサルティング

タレスはサイバー・セキュリティ/データ・セキュリティのエキスパートです。

リスク評価/診断	PCI-DSS PCI-PTS	脆弱性診断 ペネトレーション テスト	データ プライバシー診断	モバイル セキュリティ	DDOS スキャンサービス
					
• 情報セキュリティ 政策・戦略・監査 • リスク評価とデータのコントロール • 事業継続計画 • トレーニング	• PCI-DSS認定支援 • PCI-DSS監査（QSA） • PCI-PTS PIN Securityのコンサルティング • PCI-DSSトレーニング • 鍵管理 • PIN管理 • HSM管理	• ネットワークスキャン • アプリケーションスキャン • 脆弱性スキャン • ペネトレーションテスト • APTの検知	• データ分類のコンサルティング • データ流出対策 • プライバシーインパクトアセスメント（PIA） • データ保護の啓蒙トレーニング	• NFC・モバイル環境セキュリティコンサルティング • モバイル・クラウドサーバ脆弱性診断 • システムのライフサイクル（SDLC）コンサルティングとトレーニング • コードの精査	• DDOSスキャン（レイヤ３－レイヤ７） • 洗練された模擬攻撃手法暗号・ランダムetc • 多様な攻撃パターンに対応

セキュリティに関するあらゆる要求に応えるため、サービスを拡大しています。

THALES

Thales CSOC APAC, 2016 Soon!

タレスのセキュリティ・オペレーション・センター（SOC）は重要インフラやクリティカルな情報システムに包括的な監視を実施します。異常を未然に検知し、サイバー攻撃に適切な対処を実施し、安全な運用を約束します。

THALES

共通する目的 - セキュリティ改善：各団体の基準とフォーカス領域

Thalesは各団体のメンバーとして、意見を提出する立場です。

EMVCo	PCI SSC	GlobalPlatform
Evolution of EMV specifications and associated testing procedures ➢ Contact chip ➢ Contactless chip ➢ Common payment application (CPA) ➢ Card personalization ➢ Payment tokenization (issuer side) ➢ Mobile POS (mPOS) ➢ **3DS 2.0 (in progress)**	PCI DSS PCI PA DSS PCI P2PE Non-payment tokenization Card production PIN Transaction Security (PTS) ➢ PIN security ➢ **Hardware security module (HSM)** ➢ Point of interaction (POI) ➢ Unattended payment terminal (UPT)	Secure messaging Secure channel protocols Trusted Execution Environment (TEE) Common personalization

もちろん、ANSIのセキュリティ基準もThales決済HSMの設計に影響を与えています。

途上国以下のセキュリティ水準？

日本独自仕様の銀行カードとATMには、もう一つ問題がある。国際ブランドのカード会社や決済ネットワーク会社が接続の条件として求めている国際セキュリティ基準を満たしていない点である。日本のATMの通信暗号化処理は国際的に見て極めて脆弱であり、海外の金融機関と比べて情報漏えいなどが起きやすい状態にある。発展途上国の金融機関の国際対応ATMよりもセキュリティ水準が低い危険な状態といえる。

「キャッシュレス革命2020」p182

- 国際クレジットカード取引では、暗証番号（PIN）は取引認証の瞬間のみに利用されるべきものと考えられており、それを端末側で保存することはセキュリティ上のルールとして禁止されている。PCI DSSやISO 9564といった国際標準は、これを担保するために、PINを装置に入力した瞬間に暗号化することを規定しており、**そのための専用機器**が広く利用されている。

- これに対し、日本の銀行ATMについては、そのような明文の規定はない。銀行システム一般において、暗証番号のような機密情報を保存する場合には暗号化すべしというルールはあるものの、それをATMの内部でどのように適用するかは実装側に任されている。過去に、内部者が関与したセキュリティ侵害において、銀行ATMのログからPINが復元されてしまった事件があったが、そういう作りとなっていること自体が、欧米のルールでは容認されないことである

「情報セキュリティの観点から考える金融ITの将来像」p20 - 日本銀行 金融機構局

POSも国際基準対応が始まってきており、POSシステムに決済データを保持しない方向性でシステム更改が始まっている…

国際水準のセキュリティ環境を整備 - 実行計画（3本柱）

クレジット取引セキュリティ対策協議会（事務局：JCCA）

「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-2016-」（H28.2.23 公表）

安心・安全なカード利用環境の実現

カード情報の漏えい対策

カード情報を盗らせない！

- 加盟店側のカード情報の非保持化の推進する
- 保持する事業者はPCI-DSSの準拠を徹底する

偽造カードによる不正使用対策

偽造カードを使わせない！

- クレジットカードの「100%IC化」の実現
- 決済端末の「100%IC対応」の実現

ECにおける不正使用対策

ネットでなりすましさせない！

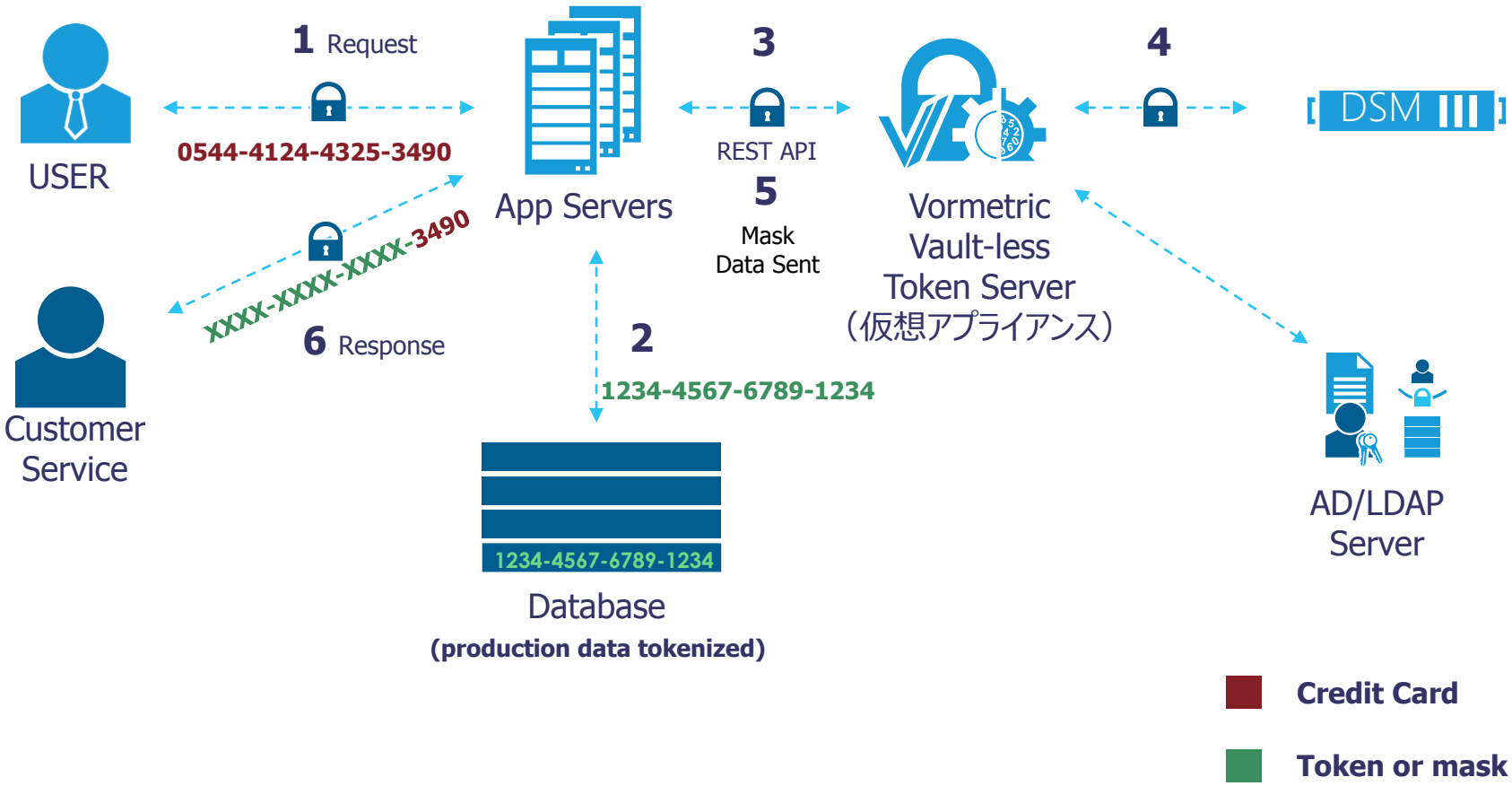
- 多面的・重層的な不正使用対策の導入

出典：http://www.meti.go.jp/press/2015/02/20160223005/20160223005.html

THALES

Vormetric トークナイゼーション/ダイナミック・データ・マスキング

Vormetric Tokenization w/
Dynamic Data Masking use case



従来型のPOSとモバイルPOSの比較

加盟店

決済サービス

従来型POS

信頼されたデバイス・アプリ・ネットワーク

モバイルPOS

決済ゲートウエイ

安全とは言い切れないデバイス・アプリ・ネットワーク

THALES

P2PE – 加盟店に決済データを残さない

購入する人は金額を
確認しPINを入力

モバイル端末上のPOSアプリ
が暗号済みの決済データ伝送
（復号しない）

暗号済PIN・
決済データの伝送

暗号済PIN・
決済データの伝送

HSM

一貫した暗号処理

Customer　Merchant　Open Network　Payment Gateway　Acquirer

ポイントTOポイント暗号 (P2PE) ゾーン

riU1h52t”ñ&>Ú³§[þïÍŸR["Ð3b€â;¤¿ Á¦æAÓú™I;6

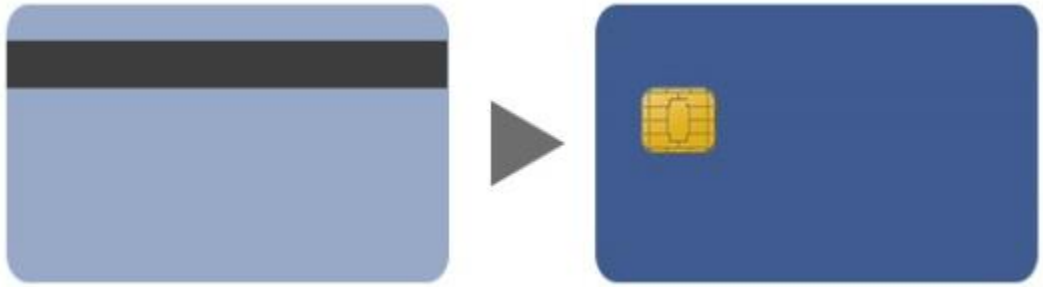
PCI P2PE･DUKPTがmPOSの決済処理データのセキュリティを支えている

- モバイル端末および加盟店側に決済データを持たない
- mPOSを構成するための重要な要素

THALES

決済のIC化・ライアビリティ・シフト

ライアビリティシフト：2015年10月から「偽造カード」の債務責務が移行
（ガソリンスタンドは2017年10月まで猶予）



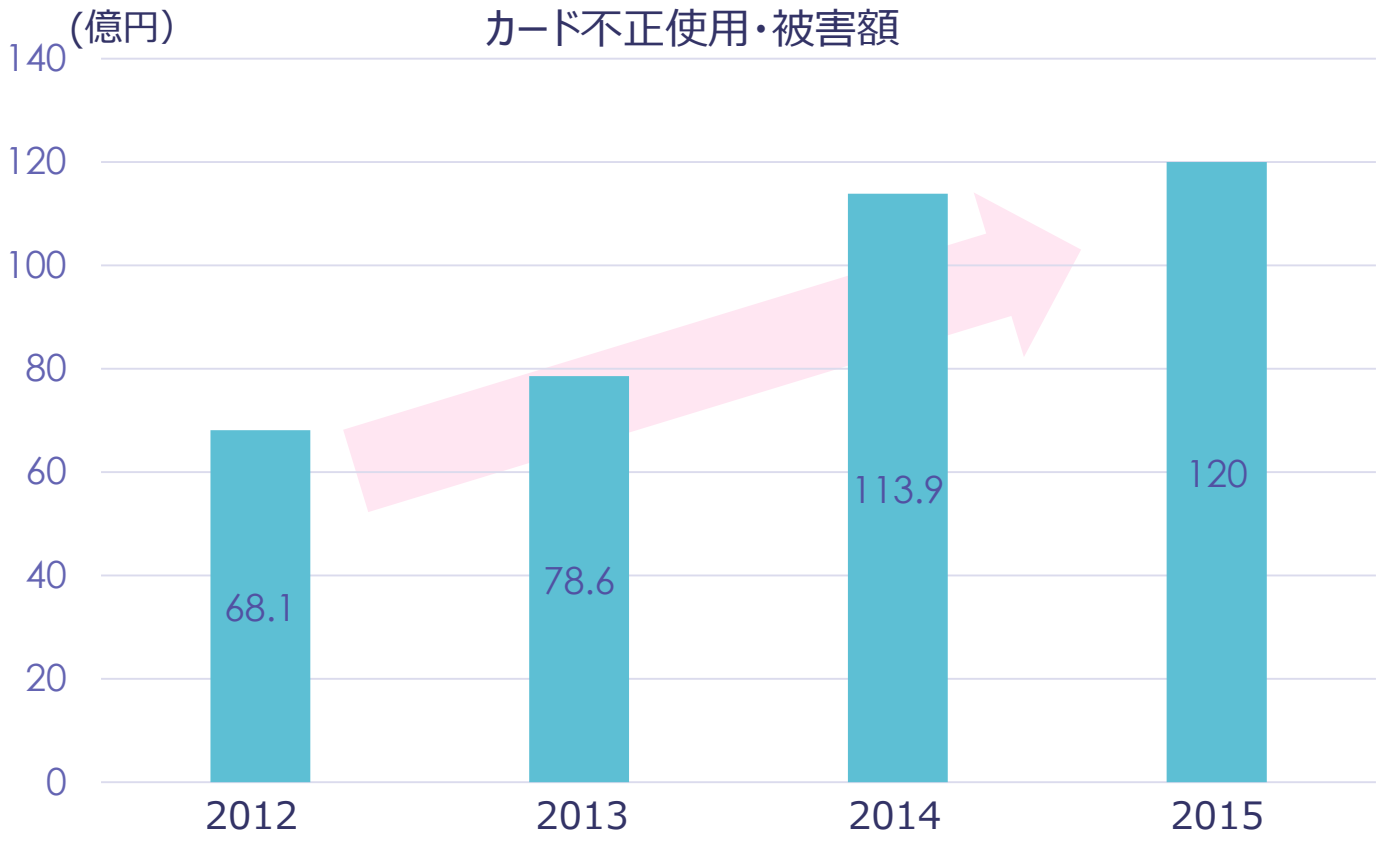
EMV/IC化していない加盟店の偽造カード被害

これまでは、イシュア（カード発行金融機関）や国際ブランドが債務を引き受けていた
これからは、アクワイラ（加盟店契約センター）や加盟店

＊銀行ATMは順次、EMV/IC化対応を進めている
＊現在は大規模展開しているPOSベンダーほど、対策に苦労している

出典：http://www.visa.co.jp/aboutvisa/mediacenter/NR_JP_070213.html

増え続けるカード不正使用と被害額



出典：一般社団法人日本クレジット協会「クレジットカード不正使用被害の集計結果について」の統計データを弊社にて編集

THALES

カード加盟店、ＩＣチップ対応を義務化　割賦販売法を改正へ

「経済産業省はクレジットカードの不正使用を防ぐため、ＩＣチップ付きカードに対応した読み取り端末の導入を加盟店に義務づける。早ければ今年の臨時国会に割賦販売法の改正案を出し、2018年にも義務化する。カード会社にも悪質な加盟店やセキュリティー対策が不十分な加盟店への調査義務を課す。」

「ＩＣチップ対応端末への切り替えには費用がかかるため、普及率は２割程度にとどまる。今後は切り替え費用の負担軽減策なども課題になる。日本クレジット協会によると、15年のクレジットカードの不正利用は約120億円で、12年の約68億円から急増した。経産省はカード業界と連携し、20年の東京五輪・パラリンピックまでに安心してカードを利用できる環境を整える。」

＊日本国内のＩＣチップ対応クレジットカードの発行は70%程度…
＊日本国内のＩＣチップ対応端末の普及は20%以下
＊ＩＣチップ後進国だった、アメリカは2015年には9割の大規模小売店でＩＣチップ対応端末を設置！

がんばれ、日本！

出典：　http://www.nikkei.com/article/DGXLASFS26H3J_W6A520C1EE8000/

THALES

非対面取引・EC加盟店における多層型保護

3Dセキュア	セキュリティコード	属性・行動分析	配送先情報
消費者に特定のパスワードを入力させることで本人確認	券面の数字（3～4桁）を入力し、カードが真正であることを確認	過去の取引情報等に基づくリスク評価によって不正取引を判定	不正配送先情報の蓄積によって商品等の配送を事前に停止

3Dセキュアの課題 – パスワード、覚えられますか？

- カード所有者自身が利用しなければ、加盟店側にどんなに普及しても使用することができない。
- カード所有者へ3Dセキュアの登録を促すキャンペーンが必要

3Dセキュア対応

- **認証システムの信頼性強化**

  Enable EMV-based Authentication
  (動的クリプトグラムを利用した認証方法)

  CAP - Chip Authentication Program
  （MasterCard）
  DPA - Visa‘s Dynamic Passcode
  Authentication （VISA)

より安全な認証・なりすまし防止・カード不正利用防止

VISA

Verified by VISA
VISA 認証サービス

VISA認証サービス

MasterCard

MasterCard. SecureCode.

SecureCode

JCB

JCB J/Secure

J/Secure

*An enhanced EMV 3DS 2.0 specification will support additional data available during the transaction to enable more intelligent risk-based decisioning, EMVCo said. The EMV 3DS 2.0 specification will be published and ready for market deployment in 2016.
注：EMVのとりまとめにより、3DS 2.0の仕様が2016年内をターゲットに確定してくる。パスワードの運用課題の他、リスクベースの認証方法の採用など新しい技術が盛り込まれることが予想されている…(3DS 1.0と2.0は並行稼働するようになる…)

THALES

タレスのHSM

Hardware Security Module

- 認定取得済みの耐タンパ性
- 強力な暗号処理・真の乱数生成機能
- 高品質な鍵管理システム

タレスHSMの国内マーケットシェアは
“68.8%”
日本でトップ！＊

nShield
多目的利用HSM

payShield
決済用HSM

*ソース:「情報セキュリティソリューション　市場の現状と将来展望2015」
第33節　HSMの市場動向（HSM総市場）
（株）ミック経済研究所調査による

THALES

モバイル決済の用語について

Secure Element

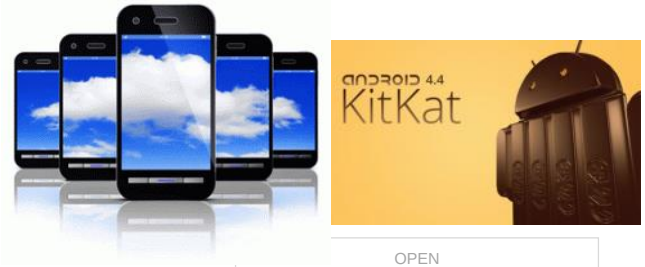
Near Field Communication (NFC)

Trusted Service Manager (TSM)

Mobile Wallet

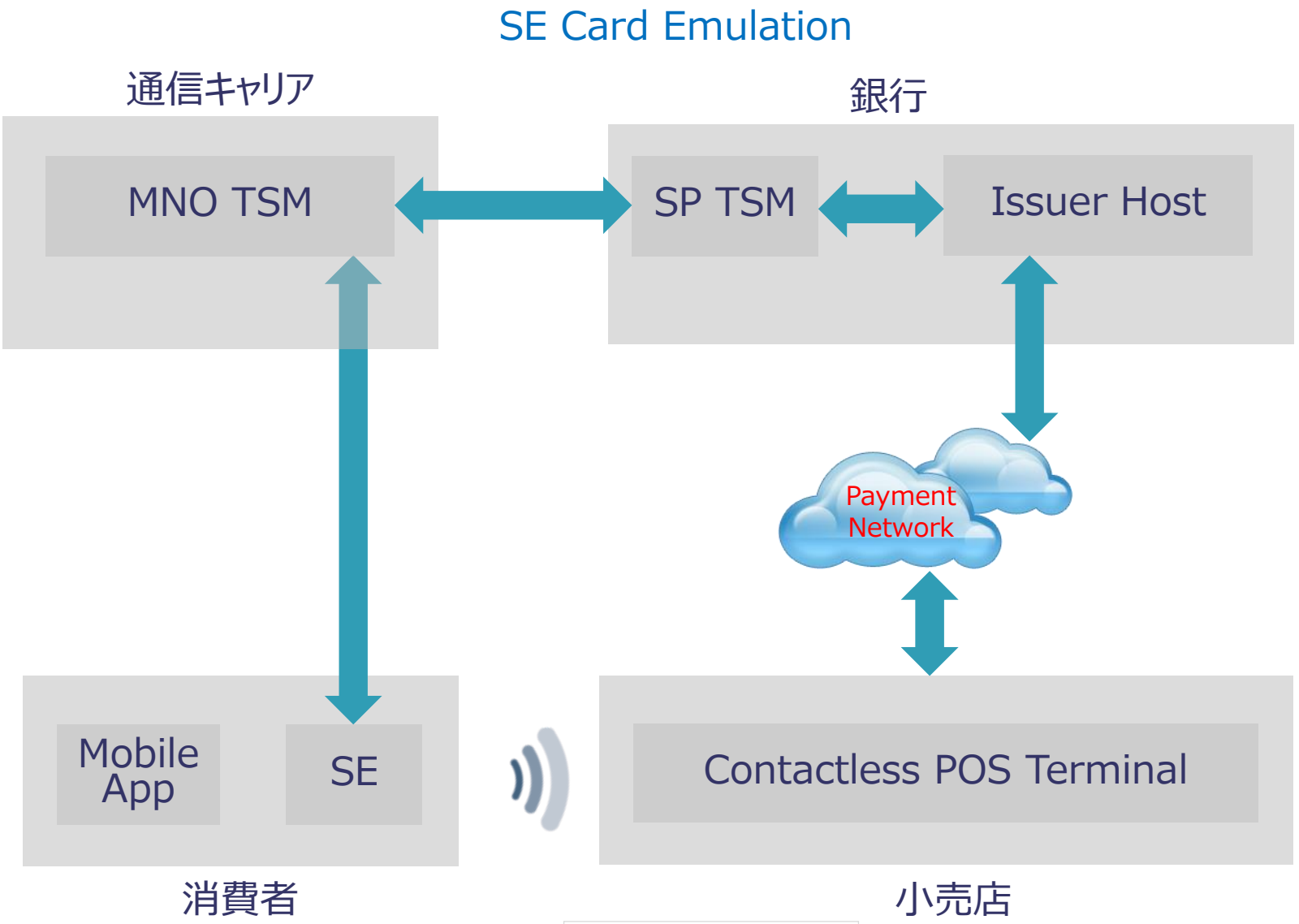
Bluetooth Low Energy(BLE)

Host Card Emulation(HCE)



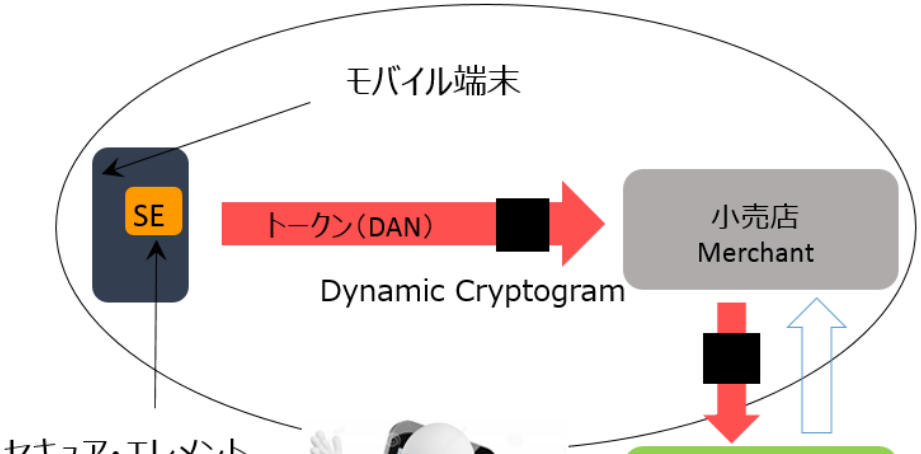
THALES

セキュアエレメント（SE）を利用した決済の課題



THALES

EMV Payment Tokenization（イシュア・国際ブランド向け）



小売店（Merchant）➡ 加盟店センター（Acquirer）
- ユーザ認証は携帯のバイオメトリックス認証を利用
- 動的な暗号文が生成され、トークン（DAN）とともに送信

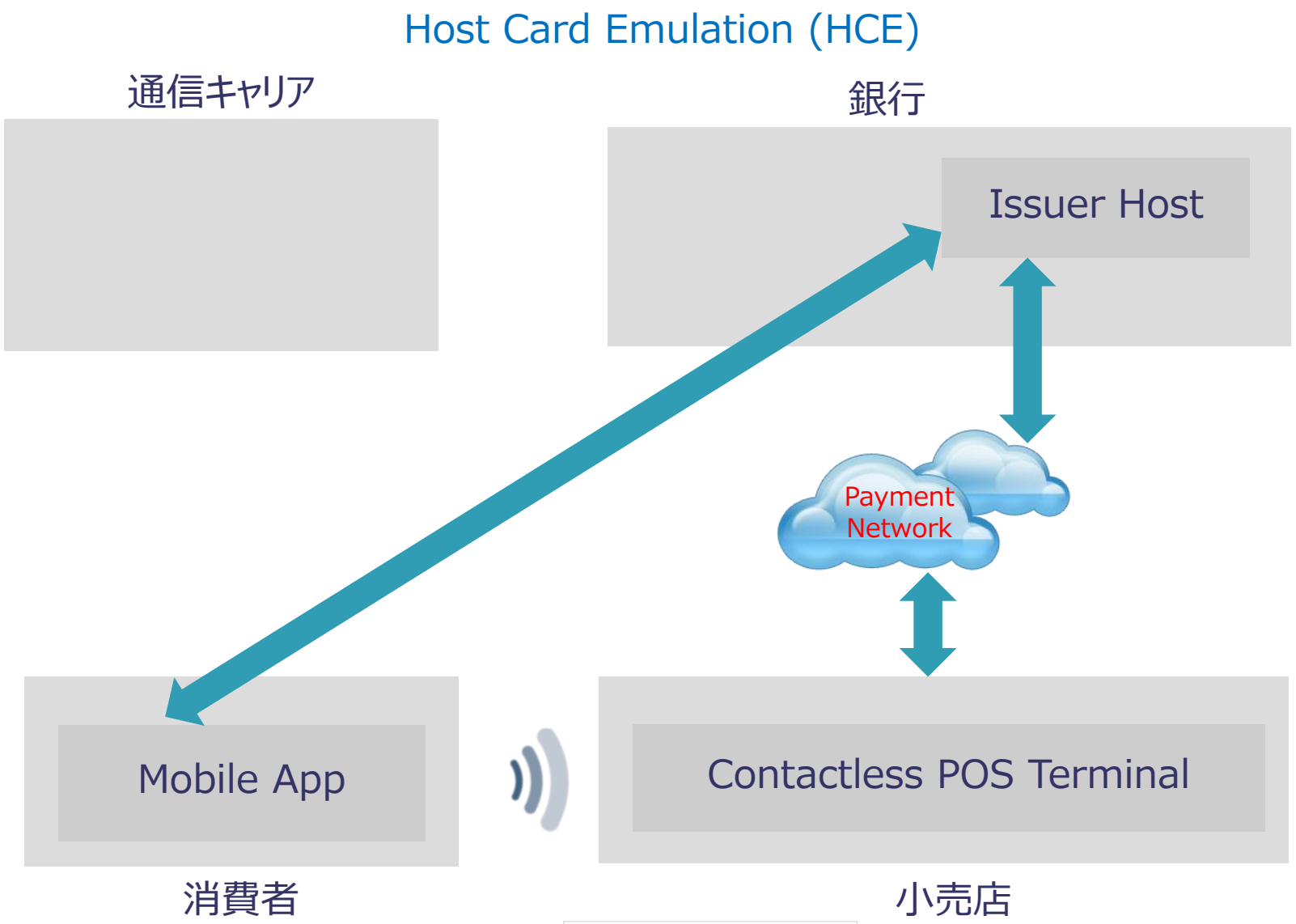
トークン（DAN）
PAN
販売承認
Dynamic Cryptogram

- トークンサーバへPANを照会
- DANを渡しPANを取得
- PANとDynamic Cryptogram をイシュアーへ送信

- PAN・Dynamic Cryptogram を照合
- 販売承認

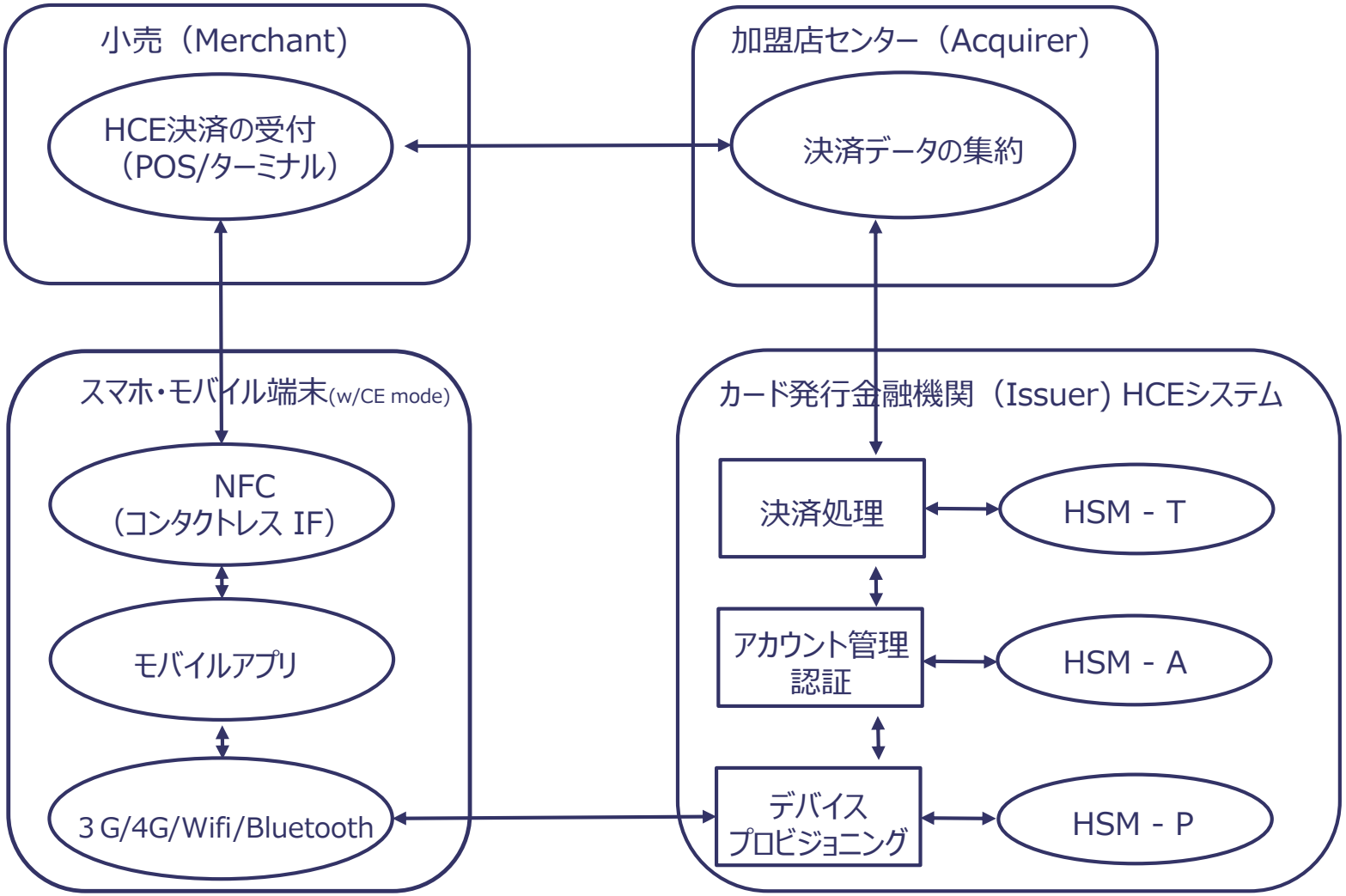
THALES

Host Card Emulation (HCE)



THALES

Host Card Emulation (HCE)



HCEの導入メリット

イシュアがコントロール掌握できる（➡　MNO・キャリアとの交渉不要）

クラウドに機密データを安全に保管し、細やかな管理作業を即座に反映

トークンサービスを組み合わせるため、モバイル端末を盗難・紛失しても、不正利用を防止できる

THALES

- 製品に関するお問い合わせ：

  タレスジャパン株式会社

  e-セキュリティ事業部：03-6234-8100

  Email：jpnsales@thales-esecurity.com

- 製品情報

  https://jp.thales-esecurity.com/

THALES

Together • Safer • Everywhere

ご清聴頂きありがとうございました。