決済セキュリティセミナー2021　講演資料

NTT DATA
Trusted Global Innovator

PCI SSC の非接触モバイル決済ソリューション基準のご紹介

2021年6月8日

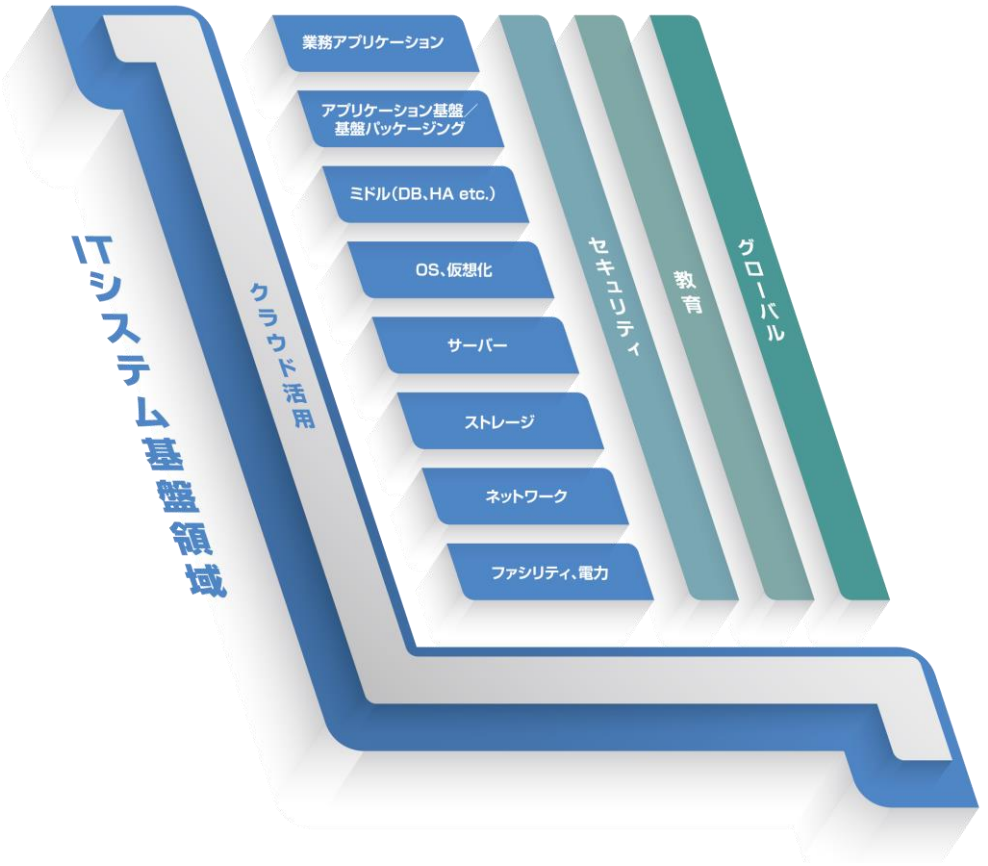
NTTデータ先端技術 株式会社
セキュリティ事業本部 セキュリティコンサルティング事業部

NTTデータ先端技術株式会社のご紹介

- 社　名　エヌ・ティ・ティ・データ先端技術株式会社
  （NTT DATA INTELLILINK CORPORATION）
- 代表者　　代表取締役社長　木谷　強
- 設　立　　平成11年8月3日
- 株　主　　株式会社エヌ・ティ・ティ・データ（100%）
- 連結社員数 1361名（2020年4月1日現在）

NTTデータ先端技術株式会社（NTT DATA INTELLILINK）は、NTTデータグループの一員として、ミッションクリティカルな情報通信システム基盤を最新技術を活用して、設計、構築、運用を行うことで、お客さまへの新たな価値の提供を目指しています。

インターネットによって世界中のあらゆる人々が、最新技術へのアクセスが可能となった今、オープンソースやクラウドサービスといった基盤技術の革新も急速に進んでいます。



わたしたちの英語名の一部「INTELLILINK」は、Intelligence（知性）をつなぐという意味を込めた造語です。オープンな環境下で先端技術を常に獲得し続けるために、生まれ続ける新たなIntelligenceをつなげ、お客さまへご提供していきます。

NTTデータ先端技術株式会社のご紹介：Security Domain

サービス概要

ミッションクリティカルなシステムに対応する現場のエンジニアやコンサルタントが登壇。
インフラ分野を中心に、各種認定トレーニングやオリジナルトレーニングを提供。人財育成に関する個別コンサルティング支援もサポート。

セキュリティソリューション

- SIEM（McAfee、IBM、Splunk）
- EDR（Tanium、LanScope、CrowdStrike、Cybereason、Exabeam）
- SSL/TLSサーバ証明書クーポン
- 改ざん検知（Tripwire、DeepDiscovery）
- 暗号管理　HSM（SafeNet、Thales）
- Web/DB対策（SecureSphere）
- Web分離無害化ソリューション（Menlo）
- 特権ID管理（iDoperation）
- シングルサインオン（SecureJoin）
- 統合ID管理ソリューション（VANADIS Identity Manager）
- ゼロトラストセキュリティ（Zscaler）
- サイバーレンジシステム
- 脅威インテリジェンスプラットフォーム(EclecticIQ)
- 脅威ディスカバリー&インテリジェンスプラットフォーム（DeCYFIR）

セキュリティシステム 構築数 **150**件超/年

セキュリティシステム 構築要員 **30**名超/年

セキュリティコンサルティング

- セキュリティ監査サービス
- セキュリティ強化支援サービス
- SOC/CSIRT構築支援サービス
- セキュリティ運用支援サービス
- 認定取得支援サービス
- ゼロトラストセキュリティサービス
- サイバー脅威インテリジェンスサービス

コンサル対応件数 **50**件超/年

コンサルタント **50**名超

セキュリティ診断

- ネットワーク診断サービス
- Webアプリケーション診断サービス
- スマートフォンAP診断サービス
- Webアプリケーションセキュリティ要件チェックサービス
- 脅威ベースペネトレーションテストTLPT

セキュリティ診断 技術者 **50**名超

セキュリティ診断 実績 **500**件超/年

セキュリティ監視・運用

- 次世代ファイアウォール監視サービス
- 不正アクセス監視遮断サービス
- WAF監視サービス
- インシデントレスポンスサービス
- CSIRT運用支援サービス
- サイバー攻撃対応演習サービス

セキュリティ監視システム数 **120**超

インシデント対応件数 **60**件超/年

セキュリティ監視 技術者 **30**名超

セキュリティ資格（CISSP,CISA,PCI QSA,情報処理安全確保士,など）　有資格者数 **110**名超

PCI 関連保有資格
1)QSA(PCI DSS認定セキュリティ評価機関)
2)PA-QSA (PA-DSS認定セキュリティ評価機関)
3)QSA(P2PE) (P2PE認定セキュリティ評価機関)
4) PA-QSA(P2PE) (P2PEアプリケーション認定セキュリティ評価機関)
5) 3DS Assessor (3DS評価機関)
6) QPA(認定PIN評価機関)
7) ASV (脆弱性スキャニングベンダー)

アジェンダ

1. イントロダクション：CPoCとは何か
   - PCI SSC のモバイル決済基準
   - SPoC
   - CPoC
2. CPoCの概要
   - CPoC ソリューションの構成要素
   - CPoC ソリューション上のコンタクトレス決済の処理フロー
   - CPoC プログラムのステークホルダー
   - CPoC ソリューションの構成要素と評価対象
   - CPoC 要件の構成
   - CPoCソリューションの構成要素とモジュール
   - CPoC で許容される暗号アルゴリズムと最小の鍵長
   - HSM が要求される CPoC 要件
3. まとめ

1.イントロダクション：CPoCとは何か

PCI SSC のモバイル決済基準

PCI SSC が策定しているモバイル決済に関する基準2つ：

- SPoC: Software-based PIN Entry on COTS （すぽっく）
  ソフトウェアベースの COTS デバイス上の PIN 入力ソリューションに関する基準
  2020/6 ver. 1.1 リリース（2018/1 ver. 1.0 リリース）
- CPoC: Contactless Payments on COTS （しーぽっく）
  COTS デバイス上のコンタクトレス（非接触）決済ソリューションに関する基準
  2019/12 ver. 1.0 リリース

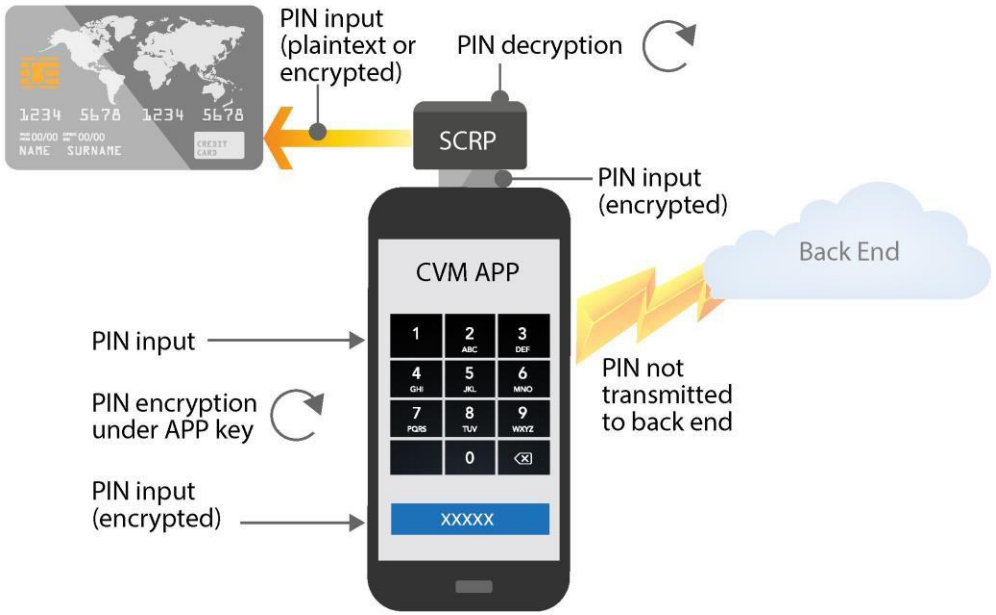
COTS: Commercial Off-The-Shelf, 商用オフザシェルフ

一般的な意味としては市販されている既製品のことですが、文脈によってソフトウェア、ハードウェアのいずれか、またはその両方を指す場合があります。SPoC/CPoCではハードウェア、特にスマートフォンやタブレットのような一般消費者向けのモバイルデバイスを指します。

CPoC プログラムガイドでは、決済ブランドが準拠を要請するプログラムを管理することになっている(Program Guide 2.2.2)ので、CPoCソリューションをサービス提供しようとした場合、決済ブランドから準拠を求められることが想定されます。

SPoC

- PIN をCOTSデバイス上の専用アプリケーション(PIN CVM Application)から入力する。
- PIN 以外のカードデータを読み取るために、加盟店のCOTSデバイスに外付けのカードリーダが必要。カードリーダは、PCI PTS の SCRP (Secure Card Reader PIN) Approval class 認定を取得している必要がある。



SPoC のオフライン PIN 検証　（SPoC v1.1 p.25 図5）

バックエンドシステムは、
- アテステーション
- モニタリング
- プロセッシング

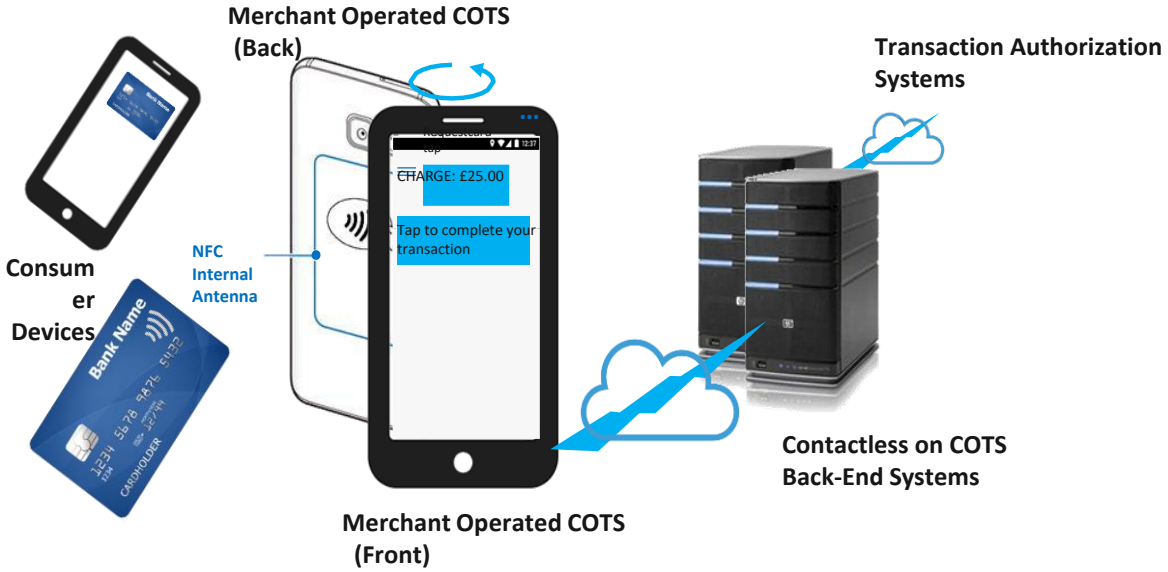
の各コンポーネントから構成されます。
これは CPoC でも同様です。

※ここでは国内で一般的な オフライン PIN の図を引用しましたが、オンライン PIN も可能です。

※2021/5/31 時点で、11個の認定ソリューションがあります。

CPoC

- コンタクトレス対応のクレジットカードやNFCを備えた消費者（エンドユーザ）のスマートフォンなどから、加盟店管理のNFCを備えたCOTSデバイス上の専用アプリケーション(CPoC Application)を利用して、カード情報をコンタクトレスで読み取り決済処理を行うソリューション。
- SPoCと比較して、加盟店デバイスに外付けカードリーダデバイスが不要なことが利点。ただし、消費者側が持つカードまたはCOTSデバイスが、コンタクトレス決済処理に対応している必要がある。
- またPIN入力は基準で禁止されているので、CVMリミット超えなどでPIN入力が必要とされる場合は処理ができず、他の決済手段を利用する必要がある。（ただし基準外のオプションとして、ブランドごとの追加要件を満たすことで、COTSデバイス上のMPOS等の別アプリからのPIN入力が許容される模様）



CPoC ソリューション実装の機能モデル（CPoC v1.0 p.17 図1）

※2021/5/31 時点で、9個の認定ソリューションがあります。

Mastercard: Tap on Phone

https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/tap-on-phone-implementation-guide-february-2021.pdf

1.3 What is this guide intended for?

This guide is intended to define the components of a Tap on Phone solution and provide guidance on how to enable and begin distributing a secure solution.

- Tap on Phone solutions are built around three solution elements: the merchant's existing NFC-enabled mobile device (COTS device), a Tap on Phone payment application (PCI CPoC™ application), and a back-end environment that engages in attestation, monitoring, and payment processing as part of the solution.
- The integrity of both the Tap on Phone payment application on the mobile device and on the host system are critically important to maintaining the security of transaction data and to helping prevent data compromise incidents.
- All Tap on Phone solutions must comply with PCI CPoC standards and relevant EMVCo and Mastercard testing requirements.

2.3 Solution options

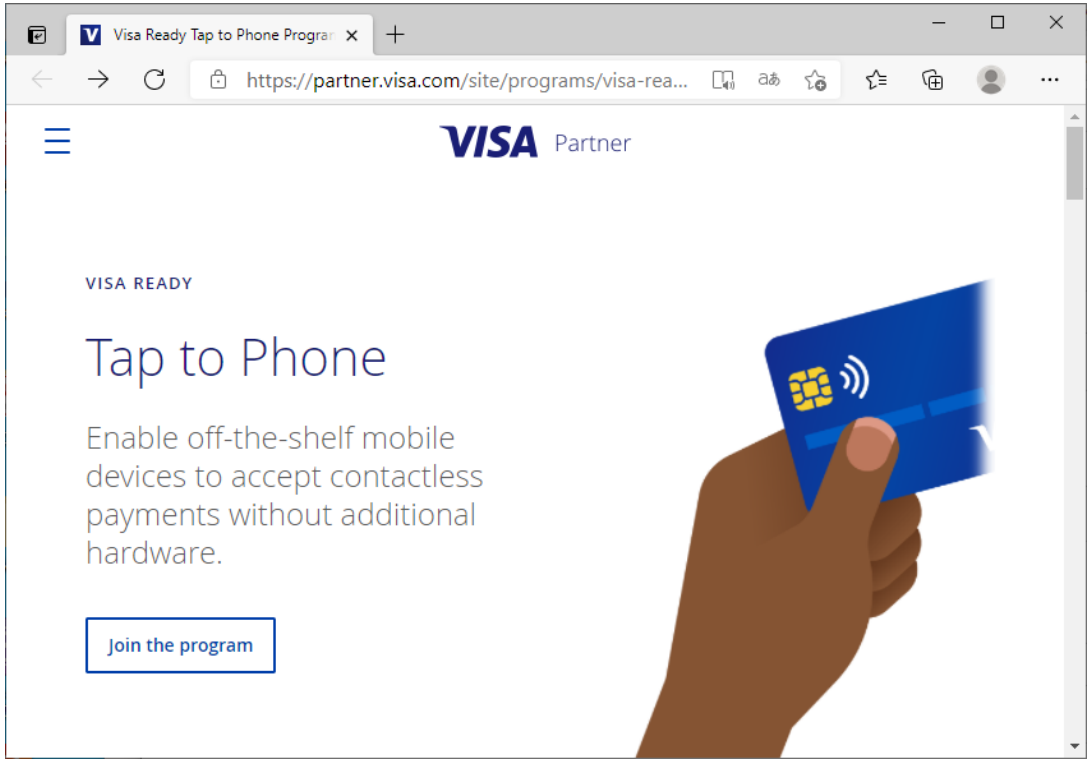
Below are options for entities looking to develop or deploy a Tap on Phone solution:

1. **PCI-Compliant Commercial Solution** [Tap on Phone without PIN: PCI CPoC]: Develop and certify proprietary solution against published PCI CPoC standard.
2. **Engage with Certified Vendor** [Tap on Phone without PIN: PCI CPoC]: Commercial agreement with vendor that offers an approved PCI CPoC solution.
3. **Pilot** [Tap on Phone with PIN: PCI CPoC w/ PIN]: Pre-PCI industry standard availability of support for PIN with PCI CPoC solutions.

- Tap on Phone ソリューションでは、CPoC 基準、および該当する EMVCo と Mastercard のテスト要件に準拠することが求められています。
- ソリューションオプションの3として、PIN 入力有のソリューションの提供が可能となっています。

VISA: Tap to Phone

https://partner.visa.com/site/programs/visa-ready/tap-to-phone.html



上記ページ内には CPoC と書いていませんが、内容的に CPoC ソリューションによるサービスであると思われます。VISAのパートナーとしてサービスを提供するには Tap to Phone Program に参加して認定を受けることが必要で、そこで求められる内容の一つとして CPoC 準拠が含まれているものと思われます。
また上記ページには “Visa’s Tap to Phone solution requirements with optional PIN capture” という記述があるので、Mastercard の Tap on Phone と同様、CPoC基準に加えて要求される追加の要件を満たすことで、PIN 入力が許容されるものと思われます。

参考文献

本資料の内容は、以下の各文書に基づいています。（主に 1.）

1. PCI Contactless Payments on COTS (CPoC)
   Security and Test Requirements Version 1.0
2. PCI Contactless Payments on COTS (CPoC)
   Program Guide Version 1.0
3. PCI Contactless Payments on COTS (CPoC)
   Technical FAQs for use with CPoC 1.0 Version 1.1
4. PCI Software-based PIN Entry on COTS (SPoC)
   Security Requirements Version 1.1

これらの文書は PCI SSC のサイトの Document Library からダウンロードできます。

https://www.pcisecuritystandards.org/document_library

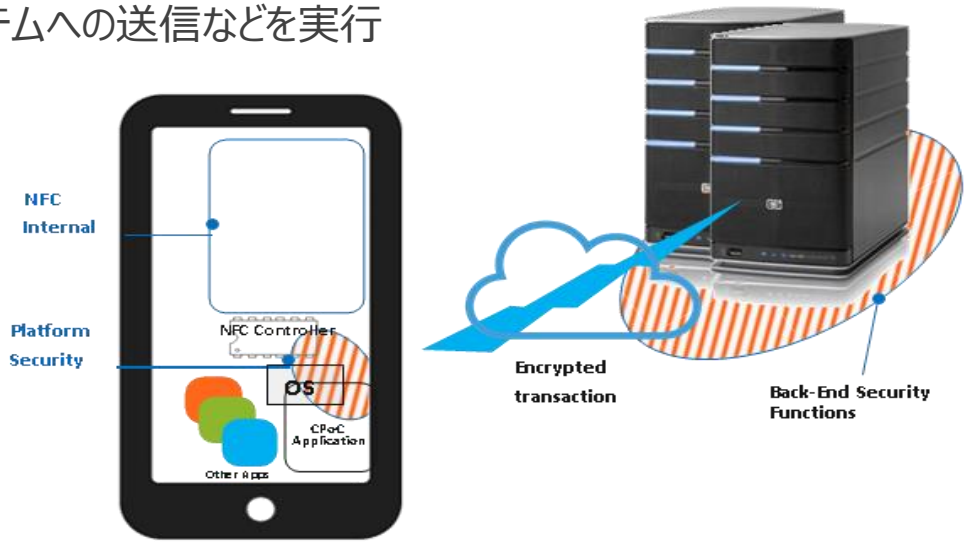
翻訳は弊社によるものであり、本資料は PCI SSC および弊社（NTT データ先端技術株式会社）の著作物です。

2. CPoC の概要

CPoC ソリューションの構成要素

CPoC ソリューションは、主に以下の 3 つのコンポーネントから構成されます。

- CPoC アプリケーション
  - COTS デバイス上で動作
  - バックエンドシステムと協同して COTS デバイスの状態チェック（アテステーション）を実行
  - PAN入力の受け付け、暗号化、バックエンドシステムへの送信などを実行
- COTS デバイス（加盟店が運用）
  - CPoC アプリケーションの動作環境を提供
  - NFCインターフェイスや、アテステーション に必要な情報を提供
- バックエンドシステム
  - トランザクション処理（プロセッシング）
  - セキュリティモニタリング
  - COTSデバイスおよびCPoCアプリケーションの アテステーション

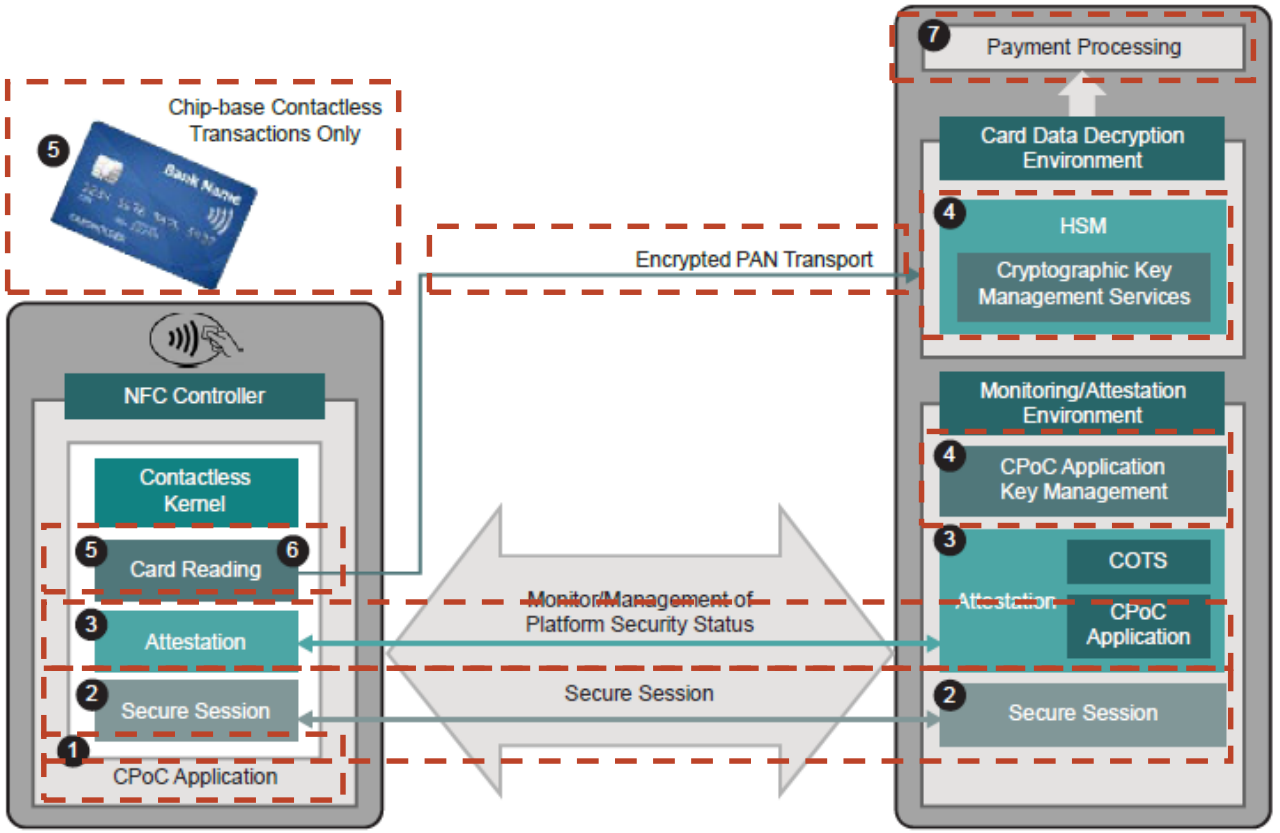


Merchant Operated COTS

CPoC ソリューションのセキュリティ要素（ CPoC v1.0 p.18 図2 ）

アテステーション(attestation)は、和訳すると認証や検証などになりますが、authenticationやverificationと区別が付かないので、ここではカタカナでそのままアテステーションとしています。CPoCにおけるアテステーションとは、COTSプラットフォームおよびCPoCアプリケーションがセキュアな状態であることを確認するプロセスを指しますが、CPoC基準のモジュール3の要件を満たす必要があります。

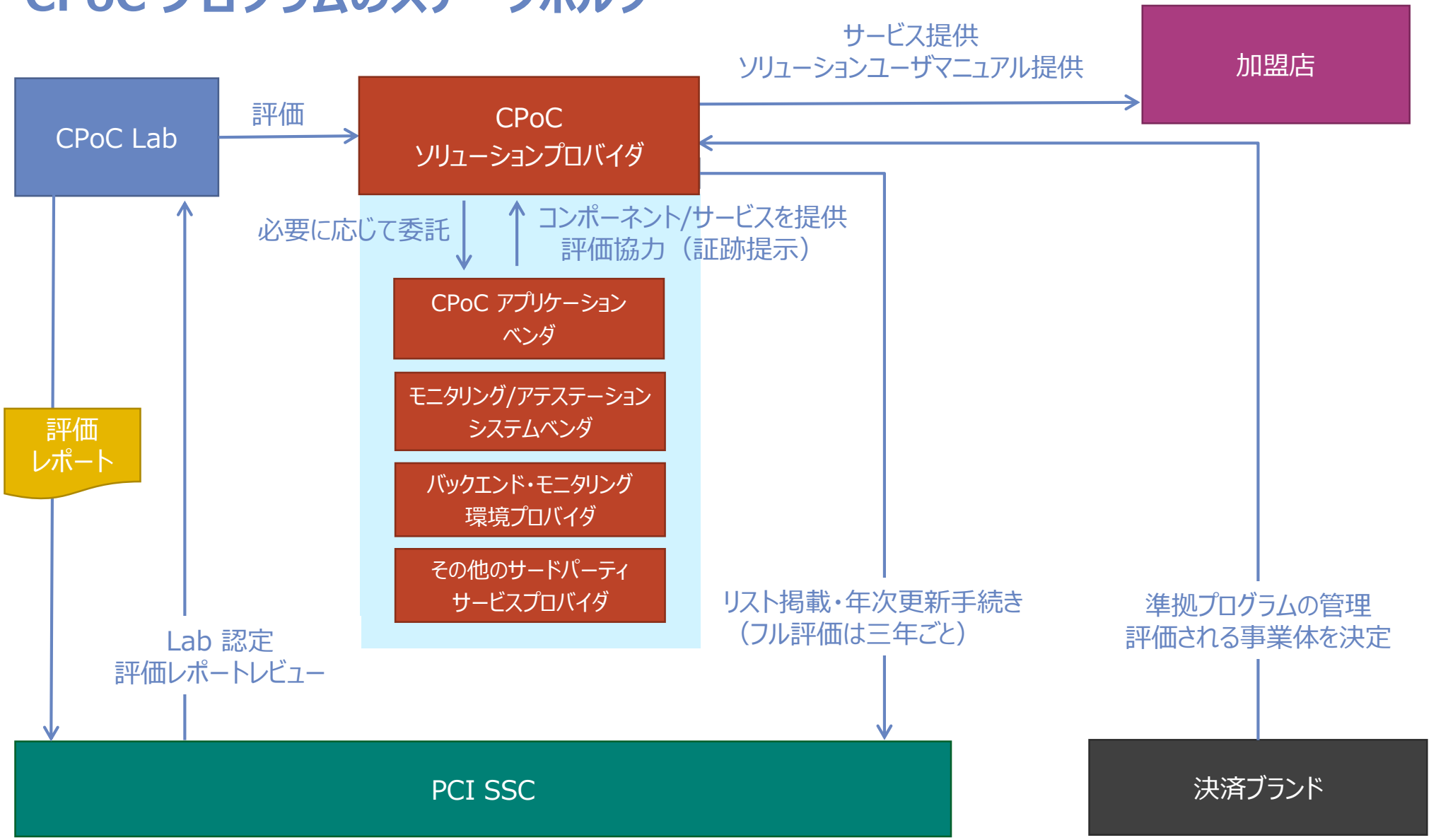
CPoC ソリューション上のコンタクトレス決済の処理フロー



1. CPoCアプリケーションのダウンロード
2. CPoCアプリケーションとバックエンド・アテステーションシステムとの間のセキュア通信チャネルの確立
3. アテステーション実行
4. CPoCアプリケーションの初期化（暗号鍵を含む）
5. トランザクション開始（コンタクトレスカードまたはデバイスの提示）
6. CPoCアプリケーションがアカウントデータを読み込み、暗号化してトランザクションデータを構成、バックエンドシステムに送信
7. 決済処理を実行

CPoC ソリューションのトランザクション処理フローの例
（CPoC v1.0 p.21 図4）

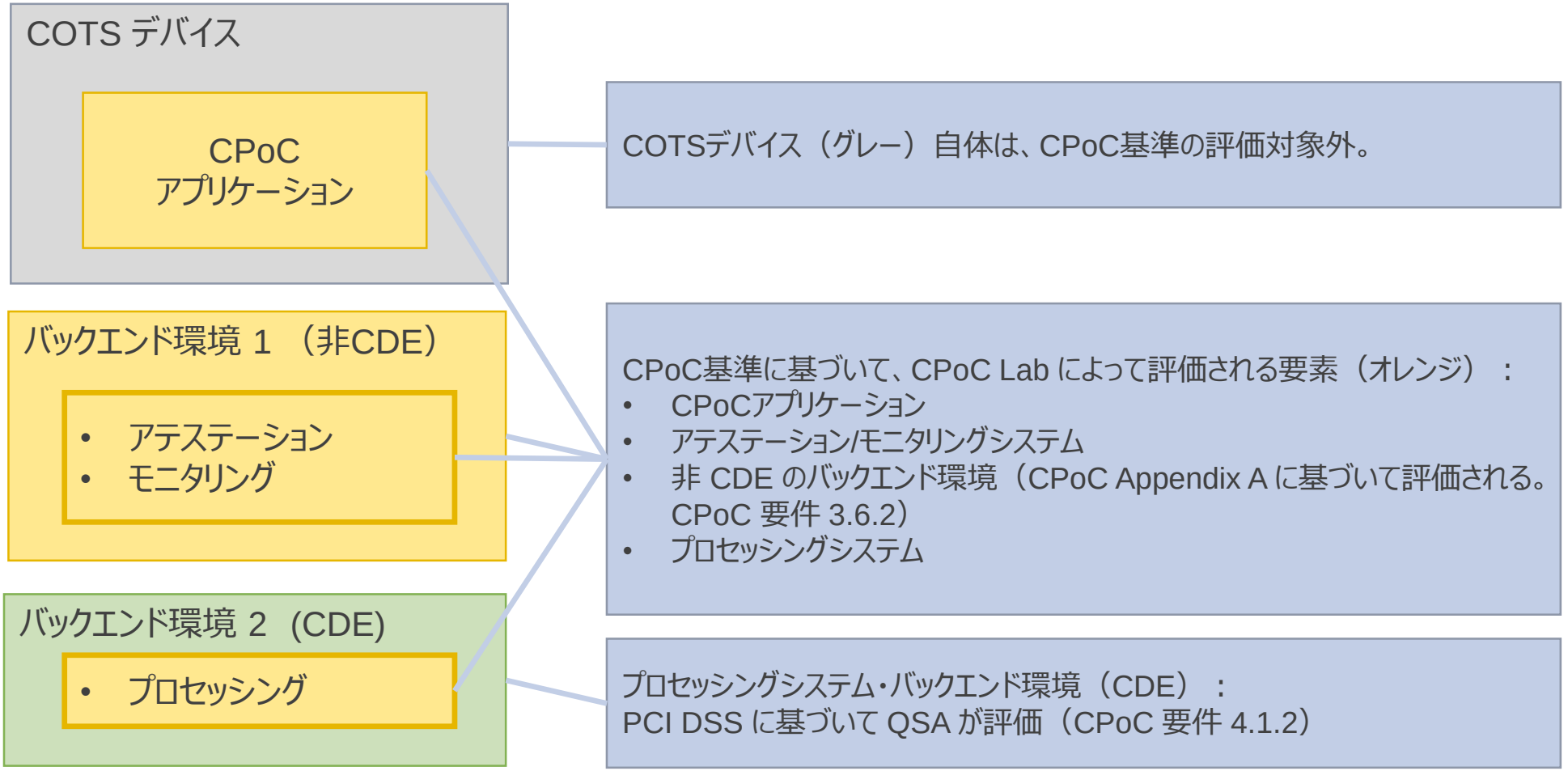
CPoC プログラムのステークホルダー



※CPoC Program Guide v1.0 の内容をもとに弊社作成

CPoC ソリューションの構成要素と評価対象（1）

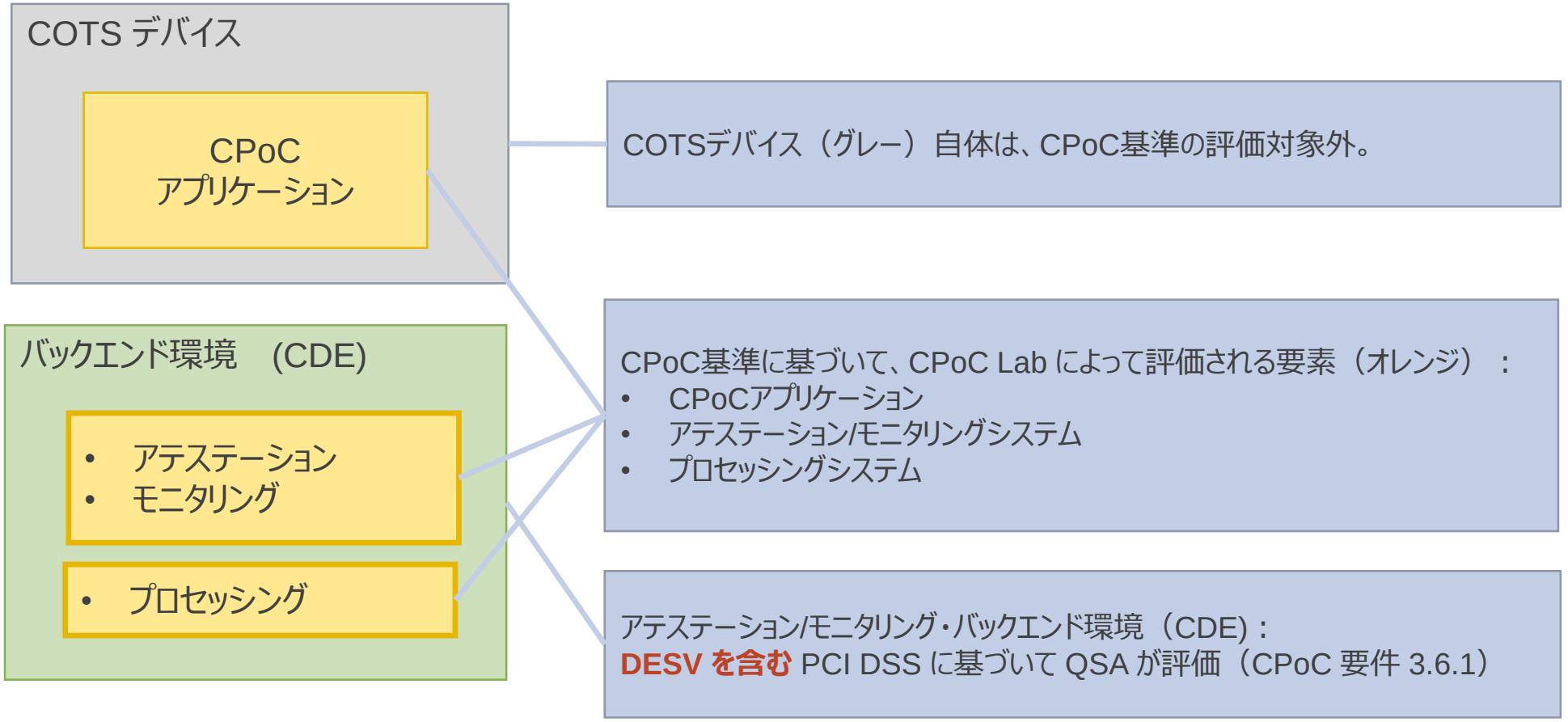
バックエンド環境は、アテステーション/モニタリングシステムを含む環境が CDE か非 CDE かによって、評価方法が変わります。アテステーション/モニタリングシステムのバックエンド環境が CDE でない場合、その環境は CPoC Appendix A に基づいて評価されます。



※CPoC および Program Guide v1.0 の内容をもとに弊社作成

CPoC ソリューションの構成要素と評価対象 (2)

アテステーション/モニタリングシステムを含むバックエンド環境が CDE の場合、その環境は DESV (Appendix A3) を含む PCI DSS に準拠する必要があります。



※CPoC および Program Guide v1.0 の内容をもとに弊社作成

CPoC 要件の構成

モジュール：CPoC 要件の階層構造の最上位。主に適用対象となるコンポーネントに対応して1から5まであり、モジュールごとにコントロール目標が定義されている。

モジュールの直下に複数設定された項目（名前が定義されていない）

Module 1: Core Requirements

Control Objective: All solution security requirements must work in concert to protect account data and support a secure mobile payment-acceptance transaction.

The entire solution must be assessed against these Core Requirements. All parties involved in the solution, including third-party service providers, are required to adhere to the requirements in this module. Solution providers are ultimately responsible for ensuring that all the requirements are met.

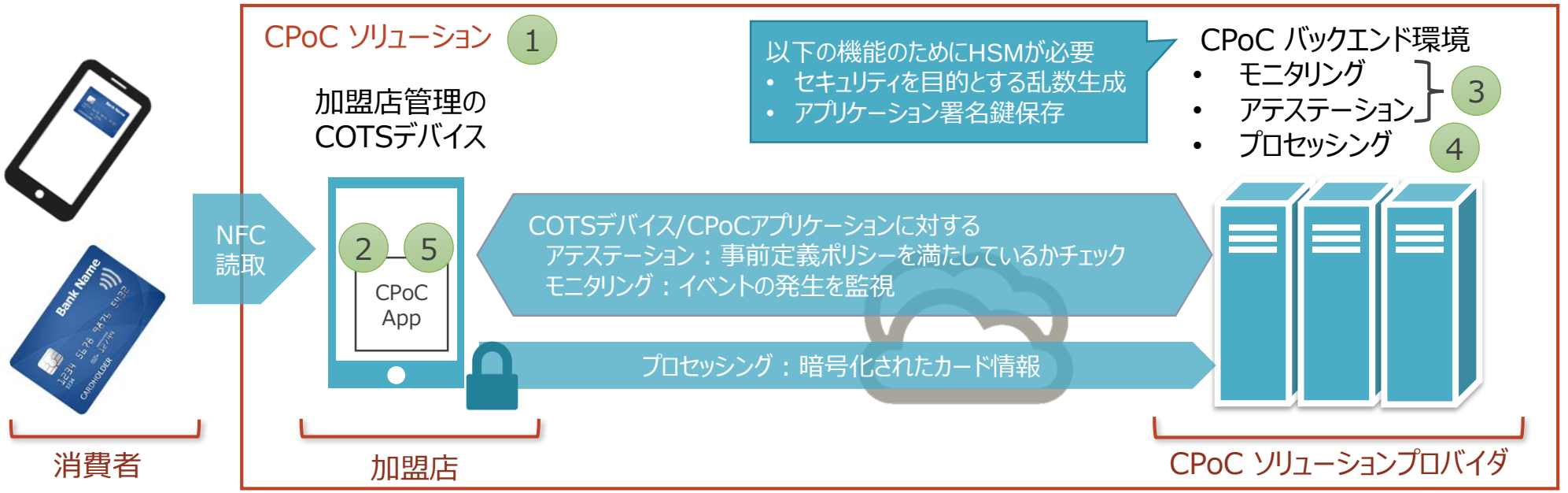
1.1 Protection of Sensitive Services

All sensitive services that support the confidentiality, integrity, and availability of the solution and its components are to be identified.

Security Requirements	Test Requirements	Guidance
1.1.1 Documentation detailing all sensitive services implemented by the solution and its components must exist, be reviewed at least annually and be updated as necessary. This must include, but is not limited to, key management, signing of applications, and signing of updates to the attestation services or configuration. ***Note:*** *This includes sensitive services on the COTS platform and the back-end systems.*	**1.1.1.a** The tester must confirm that solution provider documentation exists, is reviewed at least annually, and is up to date. **1.1.1.b** The tester must confirm that the documentation is consistent with the CPoC solution architecture. **1.1.1.c** The tester must confirm that documentation details all sensitive services implemented by the solution.	Proper identification of processes and functions that are fundamental to the security of the solution ensures common understanding, and assists with identifying roles and responsibilities for proper management and security of these processes and/or functions. Without this information, implementation of security controls may be overlooked, which could lead to unauthorized disclosure or compromise of the solution. It is expected that security vulnerabilities will be discovered throughout the year, and that the solution documentation must be updated to address them.

セキュリティ要件：CPoC 基準の要件
テスト要件：ソリューションを評価するCPoC Lab のテスターが実施すべきテストの内容
ガイダンス：各CPoC要件の背景となる意図やセキュリティ目標の記述

CPoCソリューションの構成要素とモジュール



モジュール	概要	ページ数
1. コア要件	CPoCソリューション全体に適用される要件	24pp.
2. COTSアプリケーション上のコンタクトレス決済	COTSデバイス上で動作し、バックエンドシステムとやり取りする CPoC アプリケーションに関する要件	36pp.
3.バックエンドシステム — モニタリング/アテステーション	ソリューションのセキュリティを保証するための主要なコンポーネントであるバックエンドのモニタリング/アテステーションシステムに関する要件	29pp.
4.バックエンドシステム — プロセッシング	暗号化されたアカウントデーを受け取り、決済処理を実行するプロセッシング・バックエンドシステムに関する要件	1p.
5.コンタクトレス・カーネル	コンタクトレス・カーネル（EMVCo 仕様に基づいてコンタクトレス決済処理を実行するためのソフトウェアライブラリ）に関する要件	4pp.

CPoC で許容される暗号アルゴリズムと最小の鍵長

Appendix C で、CPoC で利用可能な暗号アルゴリズムと最小の鍵長が定められていますが、現行の PIN Security や P2PE で許容されている TDES は、許容されるアルゴリズムに含まれないので注意が必要です。

ただし公開鍵暗号の最小鍵長については、3-key TDES と同等ビット強度となる RSA 2048 bit, ECC 224 bit となっています。

アルゴリズム	IFC(RSA)	ECC(ECDSA, ECDH, ECMQV)	FFC(DSA, DH, MQV)	AES
最初の鍵長（ビット数）	2048	224	2048/224	128

アルゴリズムと最小の鍵長（ CPoC v1.0 p.146 表 7 ）

IFC: Integer Factorization Cryptography

ECC: Elliptic Curve Cryptography

FFC: Finite Filed Cryptography

HSM が要求される CPoC 要件

セキュリティ要件

1.2.6 バックエンドシステム上でセキュリティのために使われる乱数は、少なくとも FIPS 140-2 Level 3（または FIPS 140-3同等）もしくは PCI 認定 HSM の NRNG から最初に提供された値をシードとしなくてはならない。

NRNG: Nondeterministic Random Number Generator. 非決定論的乱数生成器。対義語が DRNG (Deterministic Random Number Generator). 決定論的乱数（いわゆる疑似乱数）生成器。

セキュリティ要件

2.6.10 CPoCアプリケーションの実行可能ファイルおよびスクリプトに対する署名に使用するデジタル署名を生成するプロセスは、少なくとも FIPS140-2レベル3（またはFIPS 140-3と同等）または PCI HSM 認定の HSM の内部で保護されている暗号鍵に対するデュアルコントロールを用いて実行する必要がある。

3. まとめ

まとめ

PCI SSC の策定している２つのモバイル決済に関する基準のうち、CPoC の概要を紹介しました。

CPoC のメリット

- 加盟店は（ソリューションが対応している）COTS デバイスだけあれば、追加のカードリーダなど無しで、モバイル決済環境の導入が可能。

CPoC のデメリット

- 消費者が、コンタクトレス対応のカード（またはデバイス）を持っている必要がある。
- PIN入力が不要な決済しか対応できない。（他の手段が必要。ただしCPoC基準の範囲外で、ブランドごとにPIN入力を可能とするオプション仕様が提供されている模様）

CPoC のセキュリティ

- 主にアテステーション/モニタリングシステムによって実装されている。
- アテステーション/モニタリングシステムによって、COTSデバイス、およびその上で動作するCPoCアプリケーションが随時、一定のセキュリティレベルを保っていることが保証される。