実行計画を実現するための
PCI DSS要件のポイント

国際マネジメントシステム認証機構
International Certificate Authority of Management System

会社概要

国際マネジメントシステム認証機構
International Certificate Authority of Management System

会社名	：	国際マネジメントシステム認証機構株式会社 略称：ICMS（ International Certificate authority of Management System ）
資本金	：	20,000,000円（2015年3月1日現在）
業務内容	：	情報セキュリティに関する第三者認証及び / 監査サービスの提供
役職	：	代表取締役会長　海老原 邦夫 代表取締役社長　上野 洋一
認定	：	一般財団法人 日本情報経済社会推進協会（JIPDEC）よりJIS Q 27001（ISO/IEC27001）の認証機関として認定 米国PCIセキュリティ基準審議会（PCI SSC）より認定セキュリティ評価機関（QSAs）として承認
所在地	：	本社）　〒141-0021　東京都品川区上大崎2-24-11　目黒西口M2号館5F TEL：03-5719-7533 札幌営業所）　〒060-0061　北海道札幌市中央区南1条西16-1-323 TEL：0120-796-115
URL	：	http://www.icms.co.jp/
関連会社	：	Payment Card Forensics

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR℠

PCI Security Standards Council POINT-TO-POINT ENCRYPTION ASSESSOR

実行計画

国際マネジメントシステム認証機構
International Certificate Authority of Management System

クレジットカード情報の漏えい防止

- カード情報の非保持化
- 保持する場合、PCI DSS準拠

カード会社・決済代行業者、非対面加盟店は2018年3月末までに、
対面加盟店は2020年3月末までに、準拠の完了。

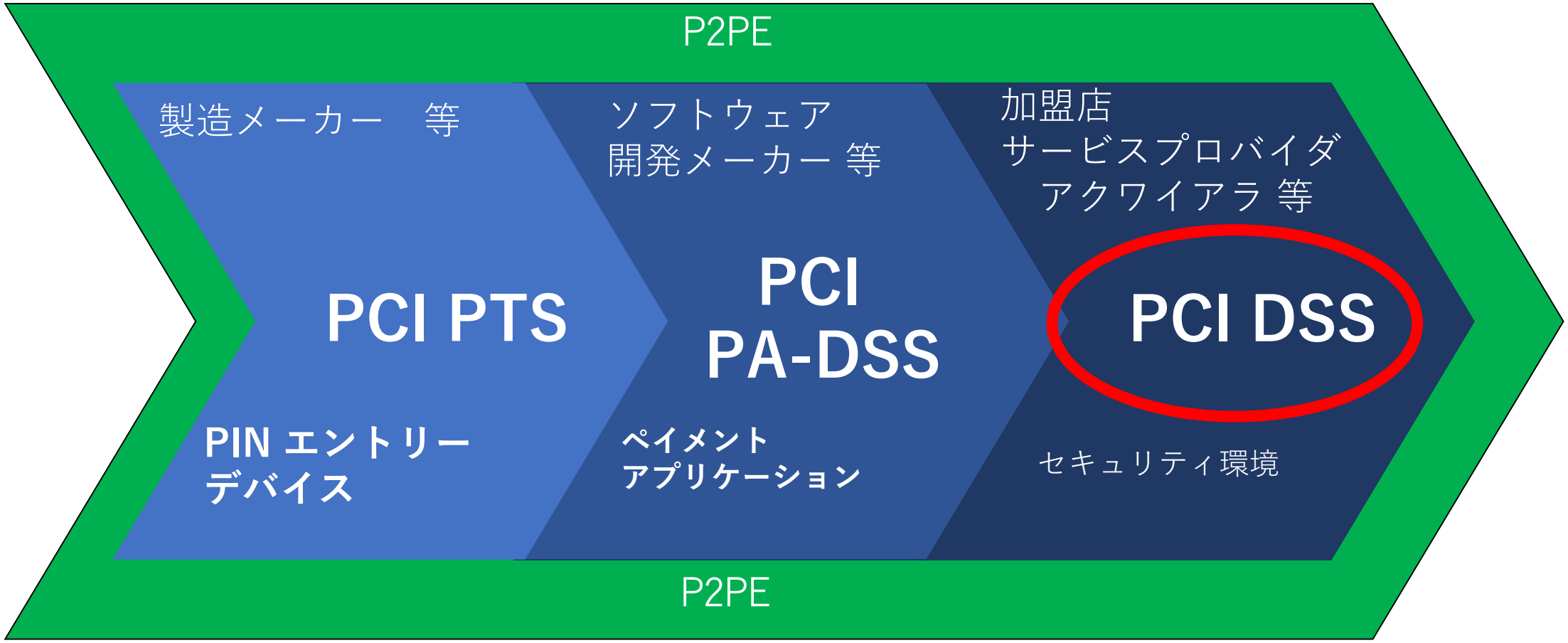
非保持化と「同等/相当」のセキュリティ方策についての評価

暗号化等の処理によりカード番号を特定できない状態及び自社内で復号できない仕組みとし、非保持と同等/相当のセキュリティが確保できる場合、「非保持化」と同等/相当の措置として扱う。　例:PCI P2PE

参考：一般社団法人日本クレジット協会「クレジットカード取引セキュリティ対策協議会実行計画-2017-の概要について」
http://www.j-credit.or.jp/security/pdf/overview_2017.pdf

PCI基準とは？

国際マネジメントシステム認証機構
International Certificate Authority of Management System



PCI基準

国際マネジメントシステム認証機構
International Certificate Authority of Management System

認　定　資　格	業　務　内　容
QSA （認定セキュリティ評価機関）	加盟店、サービスプロバイダに対し、年次と事故発生時にオンサイト（訪問）調査を実施
PA-QSA （認定ペイメントアプリケーション評価機関）	決済アプリの安全性（PA-DSS準拠）を検証
P2PE　QSA （認定P2PE評価機関）	エンド～エンドで暗号化された決済システムの安全性を検証
P2PE-PA　QSA （認定P2PEアプリケーション評価機関）	P2PEに利用されるアプリケーションの安全性を検証
ASV （認定セキュリティベンダー）	加盟店、サービスプロバイダに対し、四半期に1度、ネットワーク経由で脆弱性検査を実施
PFI （認定フォレンジック調査機関）	カード会員データの漏えい事故の際、フォレンジック調査の実施
QIR （認定インテグレータ&リセーラ）	PA-DSSに準拠した決済アプリケーションのインストール、設定を行なう
ISA （認定内部監査人）	組織内部でPCI DSS準拠を推進する内部監査人
PCIP （PCIプロフェショナル）	PCI DSS準拠を推進する内部監査人。ISAは組織内の個人を承認するが、PCIPは個人でも登録できる

PCIに関する認証機関現状

国際マネジメントシステム認証機構
International Certificate Authority of Management System

QSA会社
　世界に367社（内Asia Pacific　99社）
PA-QSA
　世界に66社（内Asia Pacific 17社）
P2PE
　世界に31社（内Asia Pacific　11社）
ASV
　世界に109社（内Asia Pacific　89社）
PFI
　世界に22社（内Asia Pacific　7社）

PCIに関する認証機関現状

国際マネジメントシステム認証機構
International Certificate Authority of Management System

QSA：2041名

PA-QSA：179名

ASVs：299名

ISAs：1831名

PCIPs：2629名

QIR：893名

PCIDSS準拠方法

国際マネジメントシステム認証機構
International Certificate Authority of Management System

選択肢１

QSAによるオンサイト監査

加盟店　レベル1

VISA	年間600万トランザクション以上
MasterCard	年間600万トランザクション以上
JCB	年間100万トランザクション以上推奨 （2018年4月より非対面取引、2020年4月より対面取引は、必須となる）
DISCOVER	年間600万トランザクション以上
AMERICAN EXPRESS	年間250万トランザクション以上

PCIDSS準拠方法

国際マネジメントシステム認証機構
International Certificate Authority of Management System

選択肢１

QSAによるオンサイト監査

サービスプロバイダ レベル1

VISA	年間30万トランザクション以上
MasterCard	年間30万トランザクション以上
JCB	件数に関わらず推奨 （2018年4月より年間100万件以上は必須）
DISCOVER	年間30万トランザクション以上
AMERICAN EXPRESS	年間250万トランザクション以上

PCIDSS準拠方法

国際マネジメントシステム認証機構
International Certificate Authority of Management System

選択肢2

SAQによる自己問診

A	カードを提示しない（電子商取引または通信販売）加盟店で、カード会員データのすべての処理はPCI DSS 認定の外部に委託されている。対面式の加盟店に適用されることはない
A-EP	カードを提示しない（電子商取引または通信販売）加盟店で、支払ページを除くカード会員データのすべての処理はPCI DSS 認定の外部に委託されている。対面式の加盟店に適用されることはない
B	カード会員データを電子形式で保存しない、インプリントまたはスタンドアロン型のダイアルアップ端末のみの加盟店。インターネット加盟店に適用されることはない
B-IP	カード会員データを電子形式で保存しない、 IP 経由で接続されているスタンドアロン型 PTS 承認の加盟店端末装置(POI)（SCR を除く）のみを使用
C	カード会員データを電子形式で保存しない、インターネットに決済アプリケーションシステムを接続する加盟店
C-VT	カード会員データを電子形式で保存しない、Webベースの仮想端末のみを使用する加盟店
D	（上記の SAQ A-C の説明に含まれない）他のすべての加盟店、（上記の SAQ A-C の説明に含まれない）他のすべての加盟店、およびペイメントブランドにより SAQ を完了する必要があると定義されたすべてのサービスプロバイダ
P2PE	カード会員データを電子形式で保存しない、P2PEソリューションに適合した加盟店端末装置（POI）のみを使用する加盟店。インターネット加盟店に適用されることはない

PCI DSS準拠の要点

国際マネジメントシステム認証機構
International Certificate Authority of Management System

クレジットカード及びセンシティブ認証データフローの認識保存場所の把握が重要

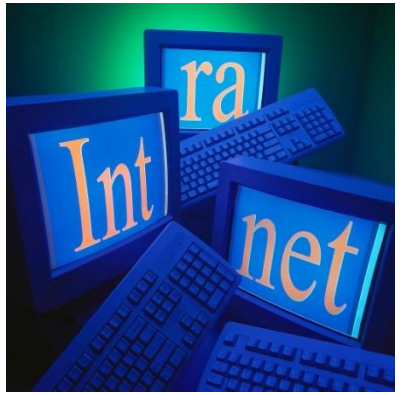
・クレジットカード・センシティブ認証データの流れと処理を把握する。
　ファイルは作成されていないか？
　ログが生成されていないか？
　保存されていないか？

・クレジットカード保存方法を把握する。
　保存場所の把握
　保護方法の把握（暗号化、トランケーション、ハッシュ等

PCI DSS準拠の要点

こんな所に、クレジットカード番号が
・Webアクセスログ
・アプリケーションログ（3D、決済アプリケーション）
・売上伝送ファイル　等々

こんな所に、センシティブ認証データが
・Webアクセスログ
・アプリケーションログ
・オーソリファイル　等々



PCIDSS準拠の要点

国際マネジメントシステム認証機構
International Certificate Authority of Management System

セグメンテーション

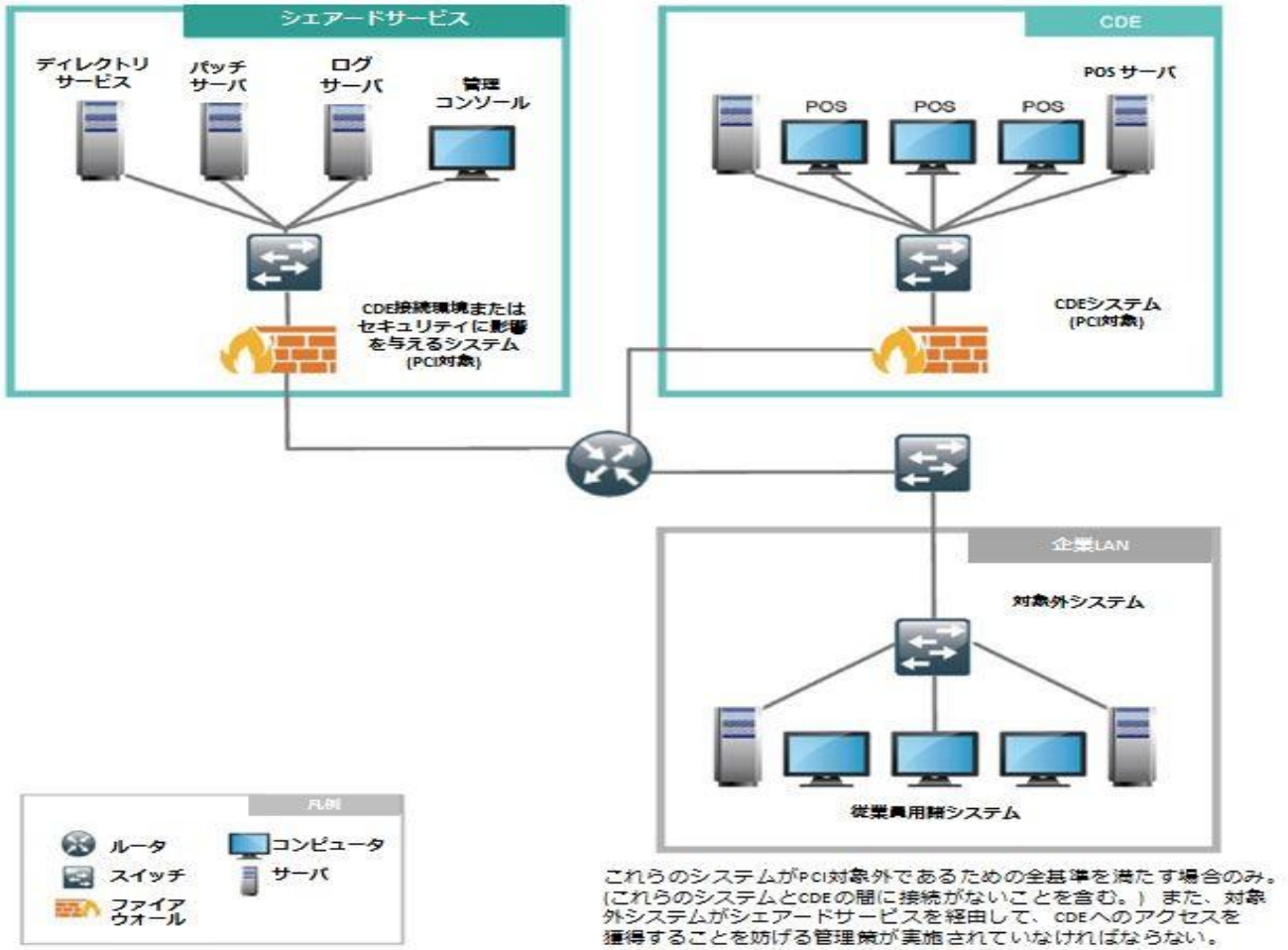
PCI DSSの対応範囲を削減する有効な手段

・多い勘違い

アクセスコントロールを利用し、通信制御を行っているだけでは対象範囲の削減にならない
PCI DSSの対象範囲を削減するには、カード会員データ環境から分離（isolate）されてることが必要

セグメンテーションの考え方は、世界的にPCI SSCの意図とは違う解釈が広がっていることもあり、2016年12月に「Guidance for PCI DSS Scoping and Network Segmentation」
がリリースされセグメンテーション方法が明確になった

セグメンテーション

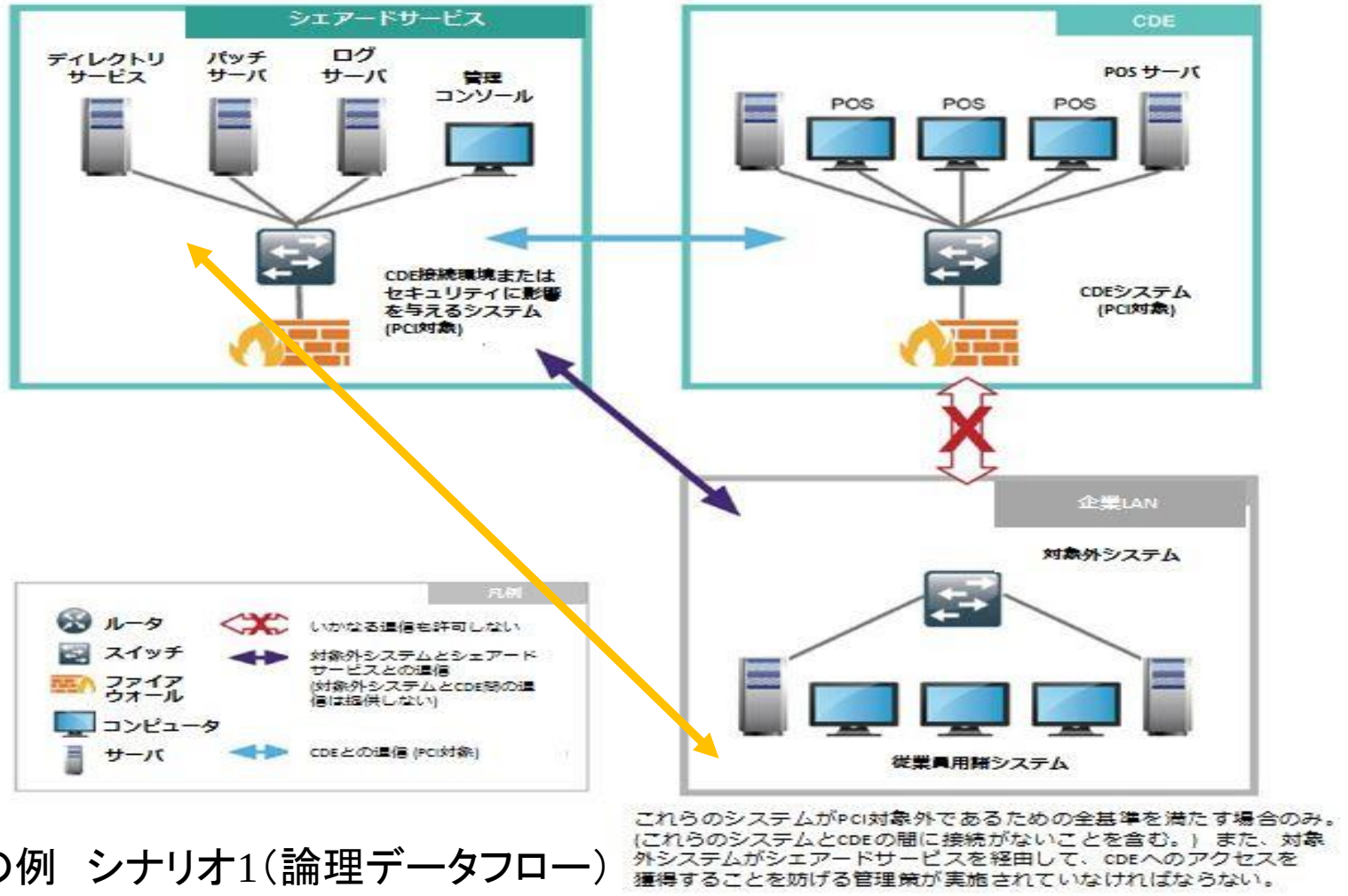


セグメンテーションの例　シナリオ1

出典：PCI SSC 「Guidance for PCI DSS Scoping and Segmentation」

※上記資料をICMSが抄訳

セグメンテーション

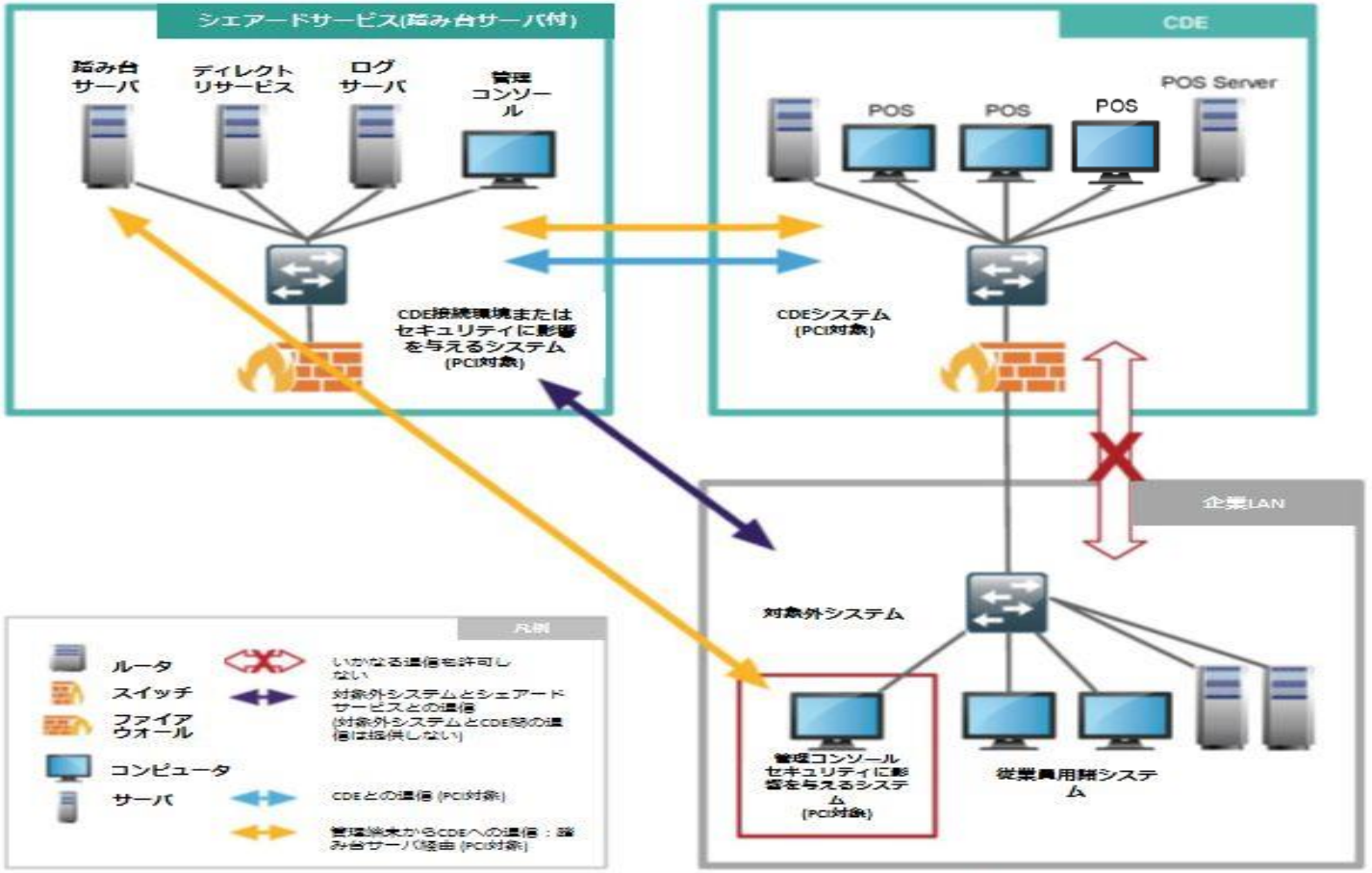


セグメンテーションの例　シナリオ1（論理データフロー）

出典：PCI SSC 「Guidance for PCI DSS Scoping and Segmentation」

※上記資料をICMSが抄訳

セグメンテーション



セグメンテーションの例　シナリオ2

出典：PCI SSC 「Guidance for PCI DSS Scoping and Segmentation」

※上記資料をICMSが抄訳

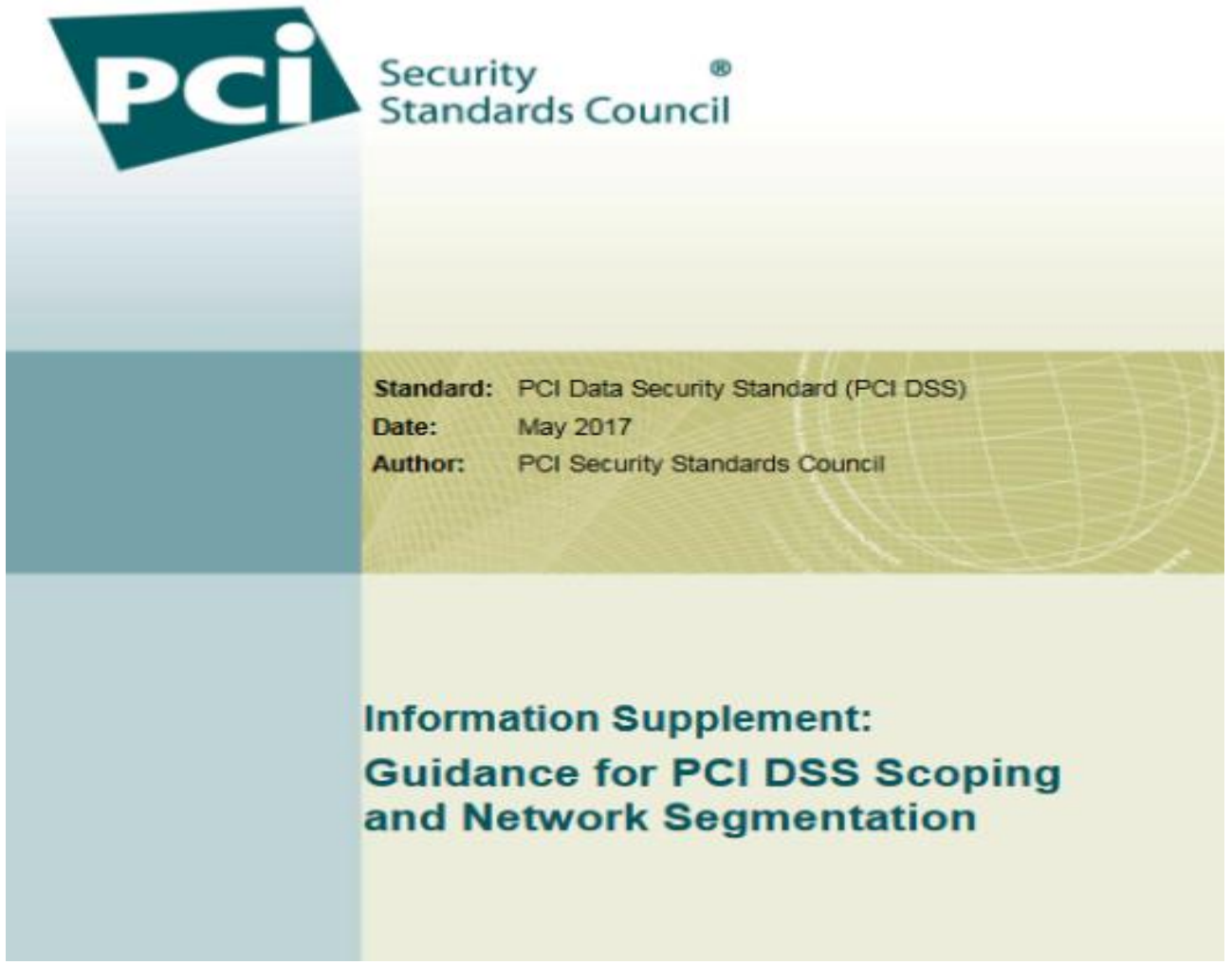
PCIDSS準拠の要点

国際マネジメントシステム認証機構
International Certificate Authority of Management System

セグメンテーション

2017年3月にガイダンスリリース

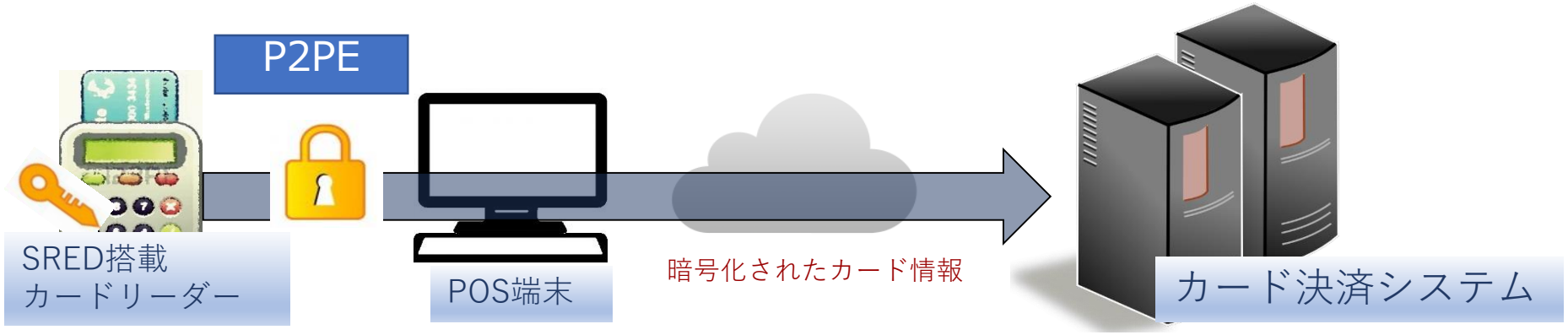
※ICMS抄訳版を、弊社ブースでお配りしています



PCI のこれから

カード会員データを保護するためのキーワード

- 3D Secure Ver2.0
- EMV対応
- P2PE
- Tokenization



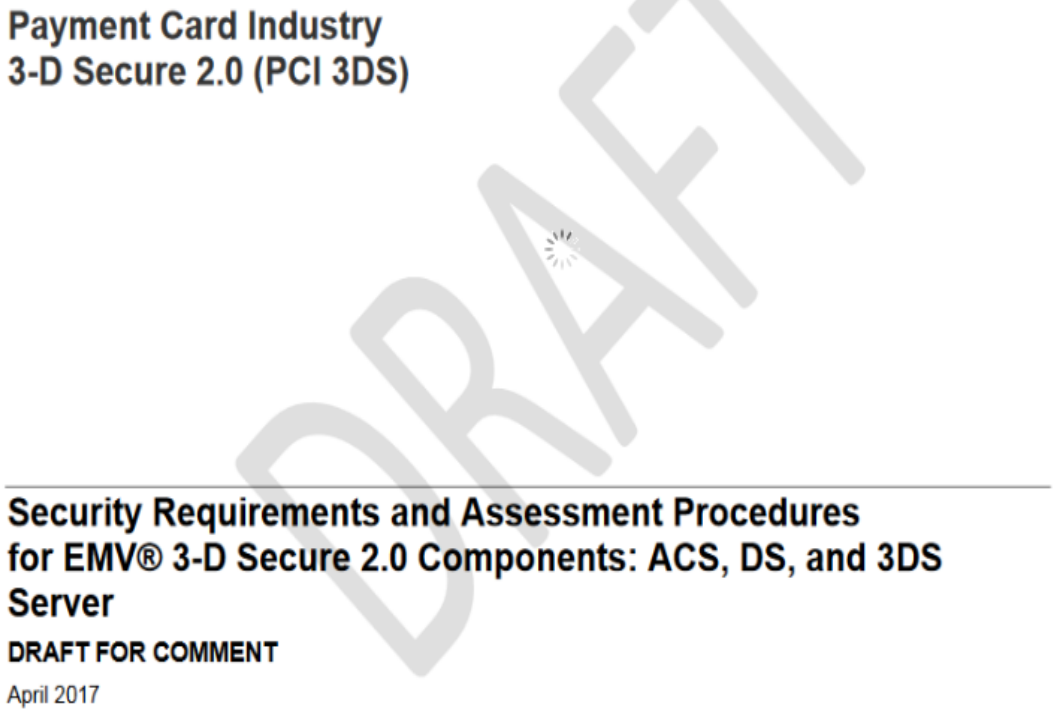
PCI のこれから

国際マネジメントシステム認証機構
International Certificate Authority of Management System

3D Secure Ver2.0

2017年4月
　3Dに関するセキュリティ要求事項ドラフト発表

対応組織
　ブランド等から要請があった組織のみ対応



PCI のこれから

国際マネジメントシステム認証機構
International Certificate Authority of Management System

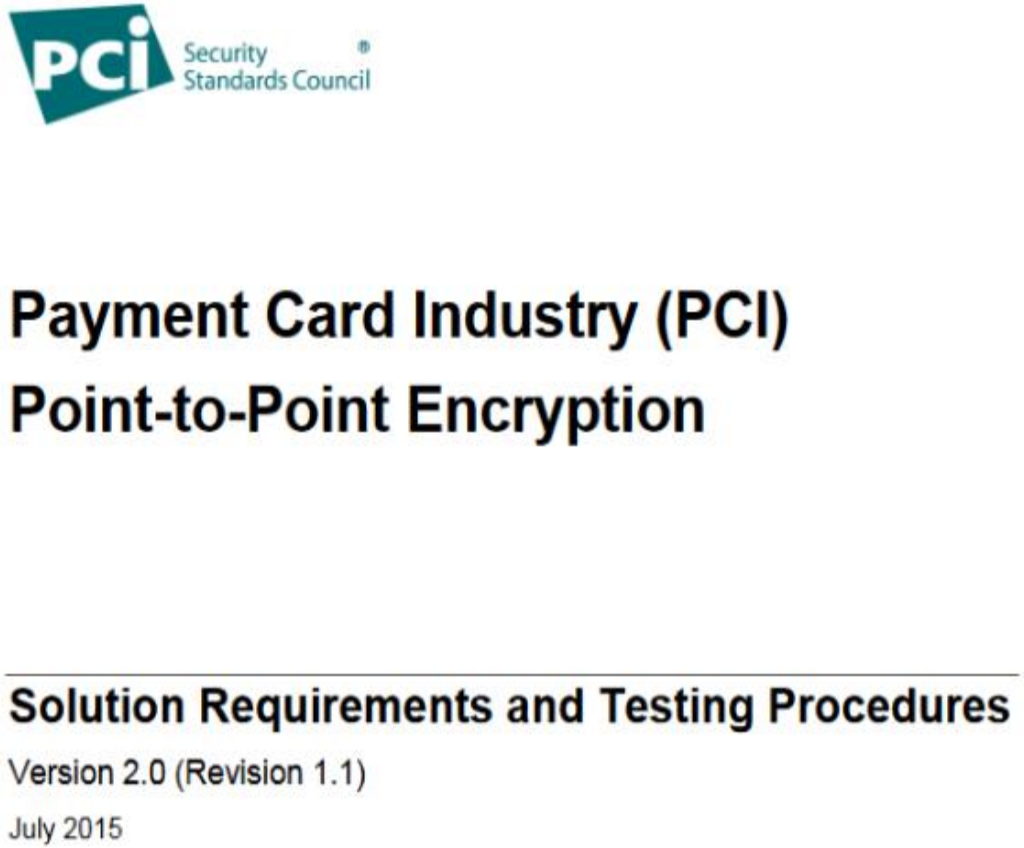
P2PE

2015年6月　Ver2.0リリース

対応組織

　P2PEソリューションプロバイダ

　P2PEコンポーネントプロバイダ



PCI のこれから

国際マネジメントシステム認証機構
International Certificate Authority of Management System

Tokenization

2015年12月

- Tokenに関連するサービスを提供する組織に対する要求事項発行
- EMVCoで作成されたものをPCI SSCが引き継いだ要求

対象組織

- ブランド等から要請があった組織のみ対応

PCI Security Standards Council

Payment Card Industry (PCI)
Token Service Providers

Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)

Version 1.0

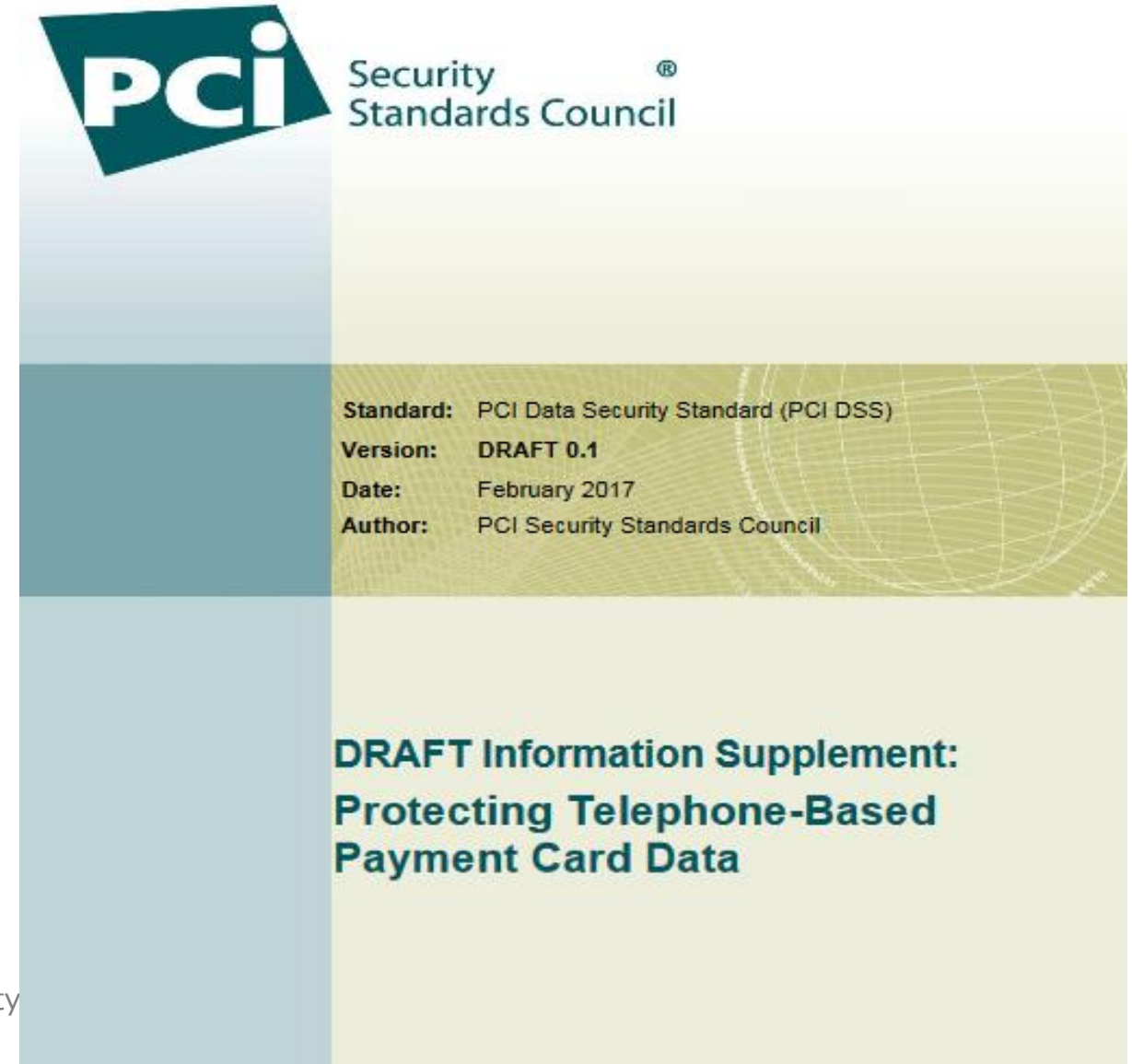
December 2015

PCI のこれから

コールセンター等

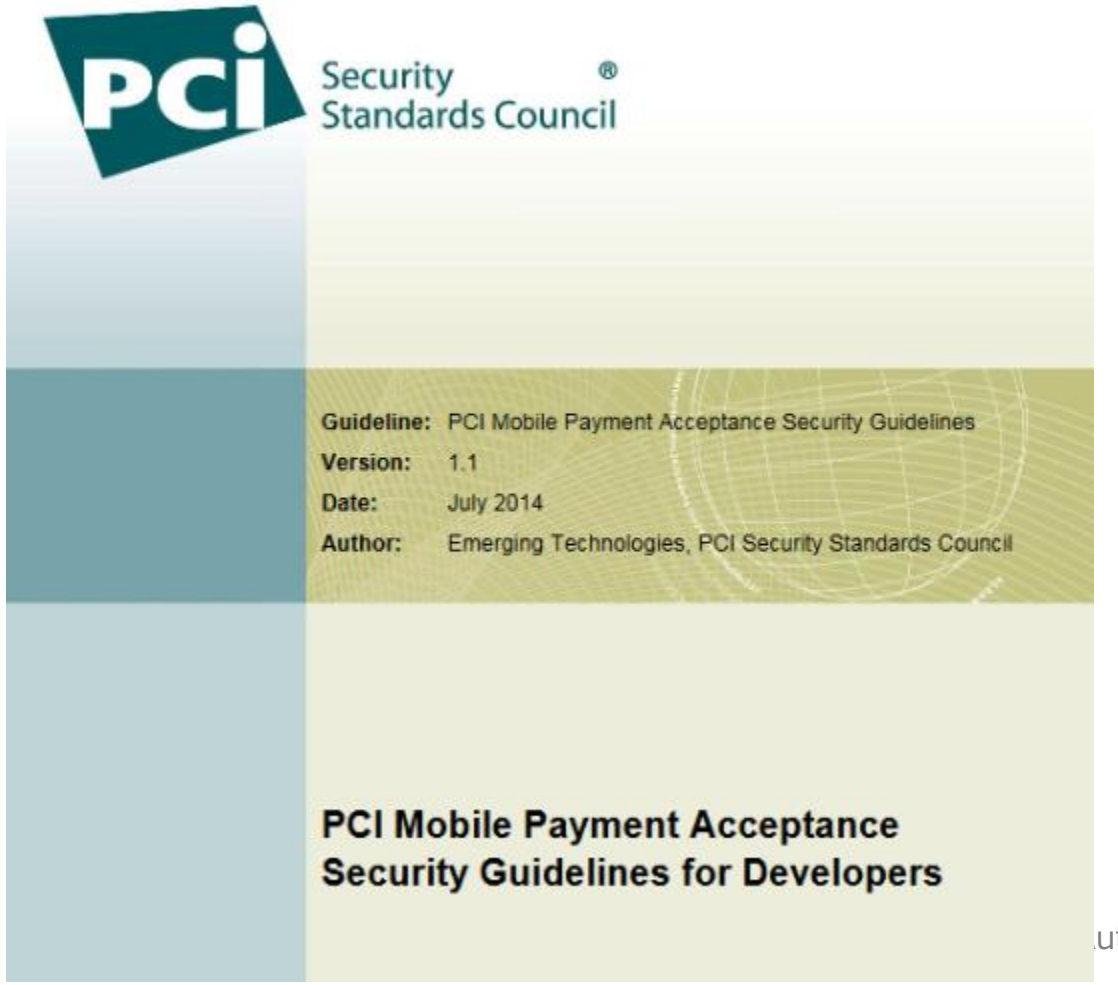
2011年に初版としてリリースされた
ガイダンスの修正版リリースの準備が
進んでいる

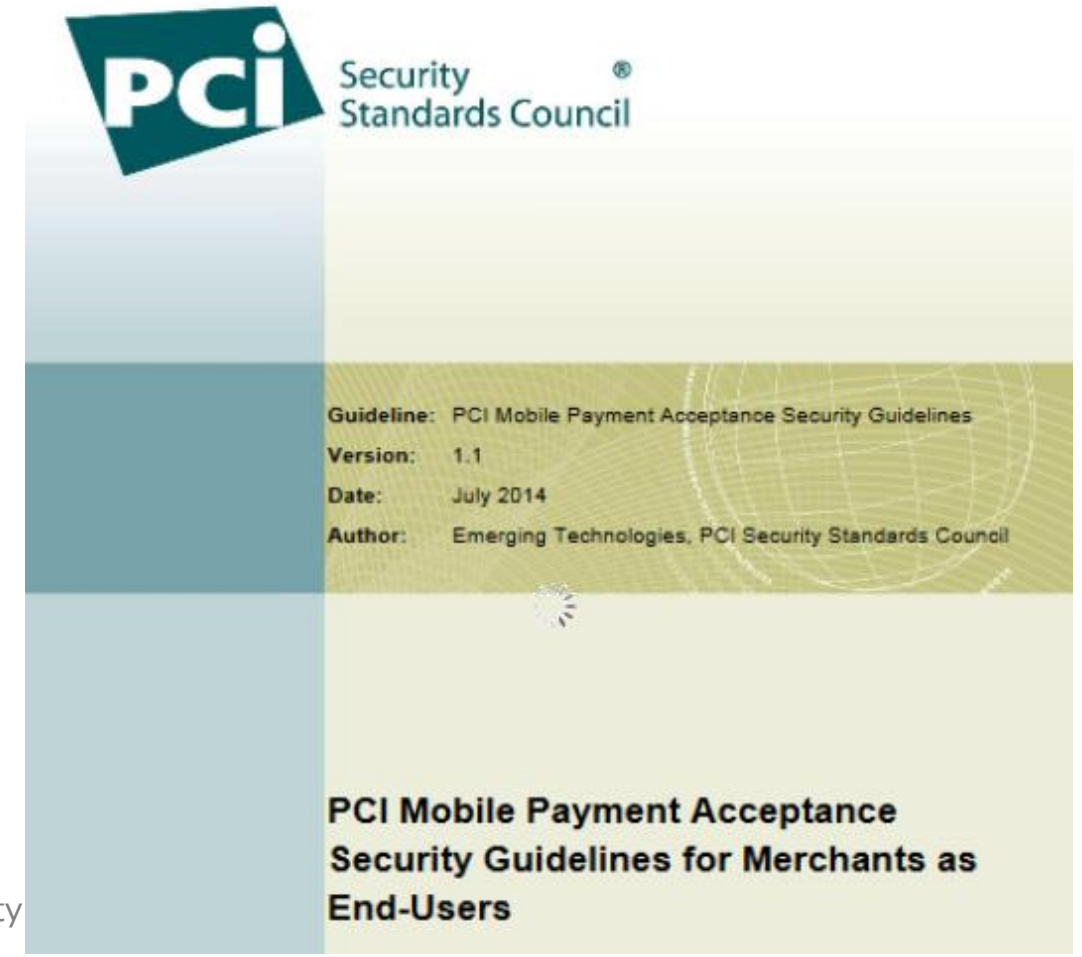
2017年2月にドラフト版がリリースされた



PCI のこれから

Mobile　2014年リリースされたガイダンスの見直しが行われている





PCI のこれから

国際マネジメントシステム認証機構
International Certificate Authority of Management System

多要素認証

2017年2月　ガイダンスリリース

マルチステップとマルチファクタについて
ガイドしている。

※ICMS抄訳版を、弊社ブースでお配りしています

INFORMATION SUPPLEMENT

Multi-Factor Authentication

Version: 1.0
Date: February 2017
Author: PCI Security Standards Council

お問い合わせ

国際マネジメントシステム認証機構
International Certificate Authority of Management System

国際マネジメントシステム認証機構株式会社

〒141-0021
東京都品川区上大崎2-24-11　目黒西口M2号館 5階
TEL　：　03-5719-7533
mail　：　info@icms.co.jp
URL　：　http://www.icms.co.jp/