PCI DSSとは

Payment Card Industry Data Security Standard

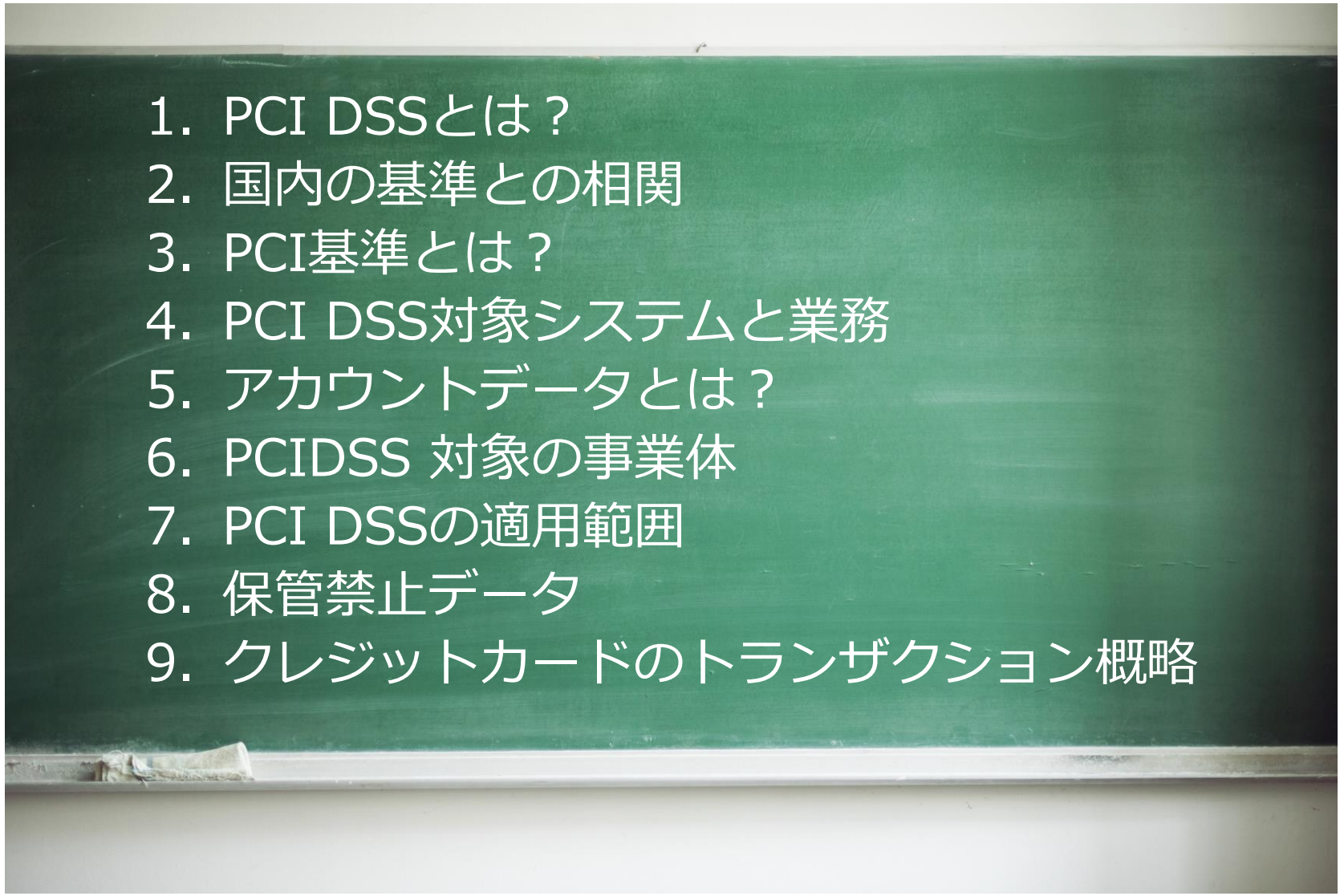
2023.11月改訂

国際マネジメントシステム認証機構

International Certificate Authority of Management System

目次

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



1: PCI DSSとは？

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

クレジットカードの会員データを安全に取り扱う
国際的なデータセキュリティ基準。
（Payment Card Industry Data Security Standard）

国際カードブランド５社（VISA、 MasterCard 、American Express、JCB、 Discover）が共同で設立し、2020年より銀聯が参加、計6社による*PCIセキュリティ基準審議会(米国）が制定する事実上の基準）。

*PCIセキュリティ基準審議会：PCI SSC(Payment Card Industry Security Standards Council）2006年9月に設立

PCI SSC公式サイト：https://www.pcisecuritystandards.org/

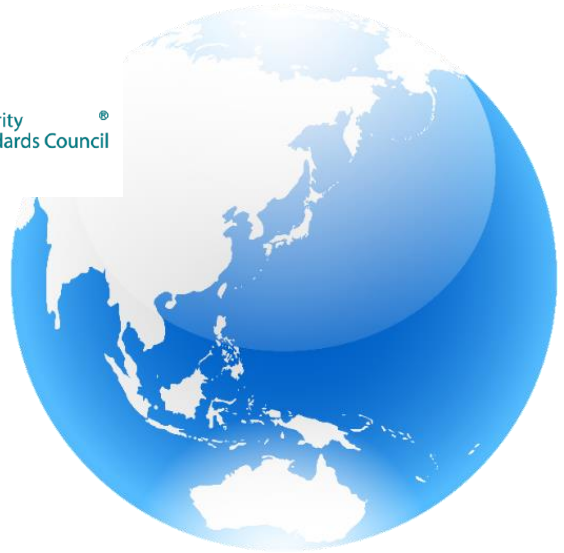
2: 国内の基準との相関

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

PCI SSC

PCI DSS
クレジット業界における
グローバルセキュリティ基準

PCI Security Standards Council



セキュリティ対策に
PCI DSSの適用

日本

クレジット取引セキュリティ
対策協議会

クレジットカード・セキュリティガイドライン

3: PCI基準とは？

PCIの基準には、PCI DSSのほかに、PCI PTS、PCI SSF、PCI P2PEがある。
PCI PTS（PIN　Transaction Security）は、PIN（暗証番号）入力用のデバイスを製造する端末メーカー、PCI SSF（Software Security Framework）は、パッケージソフトウェアメーカーを主な対象にした規格である。
そしてP2PE（Point to Point Encryption）は、エンドツーエンドで暗号化するシステムに関する規格で、ペイメントアプリケーションやハードウェアメーカーなどを主な対象としている。

PCI基準の対象事業者と領域

基準	対象事業者	領域
PCI DSS	加盟店/サービスプロバイダ/カード会社	セキュリティ環境
PCI SSF	ソフトウェアメーカー/開発会社	ペイメントアプリケーション
PCI PTS	決済端末・デバイスメーカー	PINエントリーデバイスなど
PCI P2PE	ソリューション/コンポーネント/アプリケーションプロバイダ	エンドツーエンドの暗号化
PCI 3DS	非対面加盟店/サービスプロバイダ/カード会社	非対面決済の本人認証

4: PCI DSS対象システムと業務

PCI DSS

■ PCI DSSは、

アカウントデータの

伝送/処理/保存を

行うシステム、ネットワーク及びアプリケーションの
セキュリティ及び業務を対象とする。

アカウントデータとは？
次スライドへ

5: アカウントデータとは？

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

クレジットカードの磁気ストライプ またはチップ内のデータ

アカウントデータ

カード会員データ（CHD）

- プライマリアカウント番号（一般に16桁）
- カード会員名
- サービスコード
- 有効期限

機密認証データ（SAD）

- 全磁気ストライプ/チップ上の磁気ストライプ イメージ
- CVC2/CVV2/CID/CAV2
- PIN/PINブロック

6: PCIDSS 対象の事業体

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

アカウントデータを扱う全ての事業体

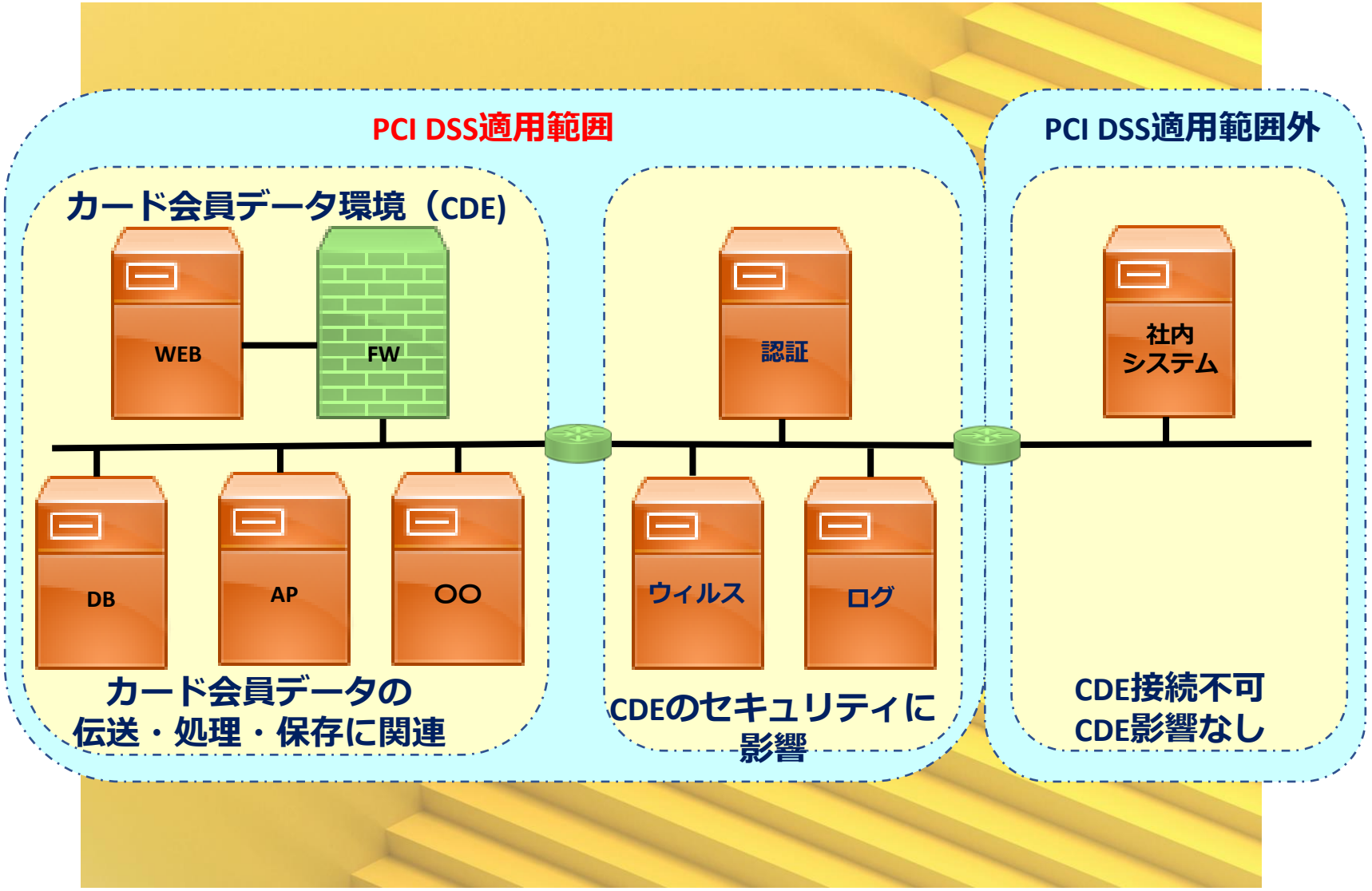
加盟店、プロセシング、アクワイアラ、イシュア、サービスプロバイダのほか、アカウントデータを伝送、処理、または保存するその他の事業体などのアカウントデータの処理を行うすべての事業体が対象となる。

※アカウントデータの「伝送」 「処理」 「保存」を行わない事業体であっても、「カード会員データ環境（CDE）に無制限にアクセス可能なシステム」、および「CDEのセキュリティに影響を及ぼすシステム」やコンポーネント、業務、人に関わりが有る場合、対象となる。

PCI DSS準拠により「アカウントカードデータの保護」を目的としている。

7: PCI DSSの適用範囲

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



8: 保管禁止データ

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

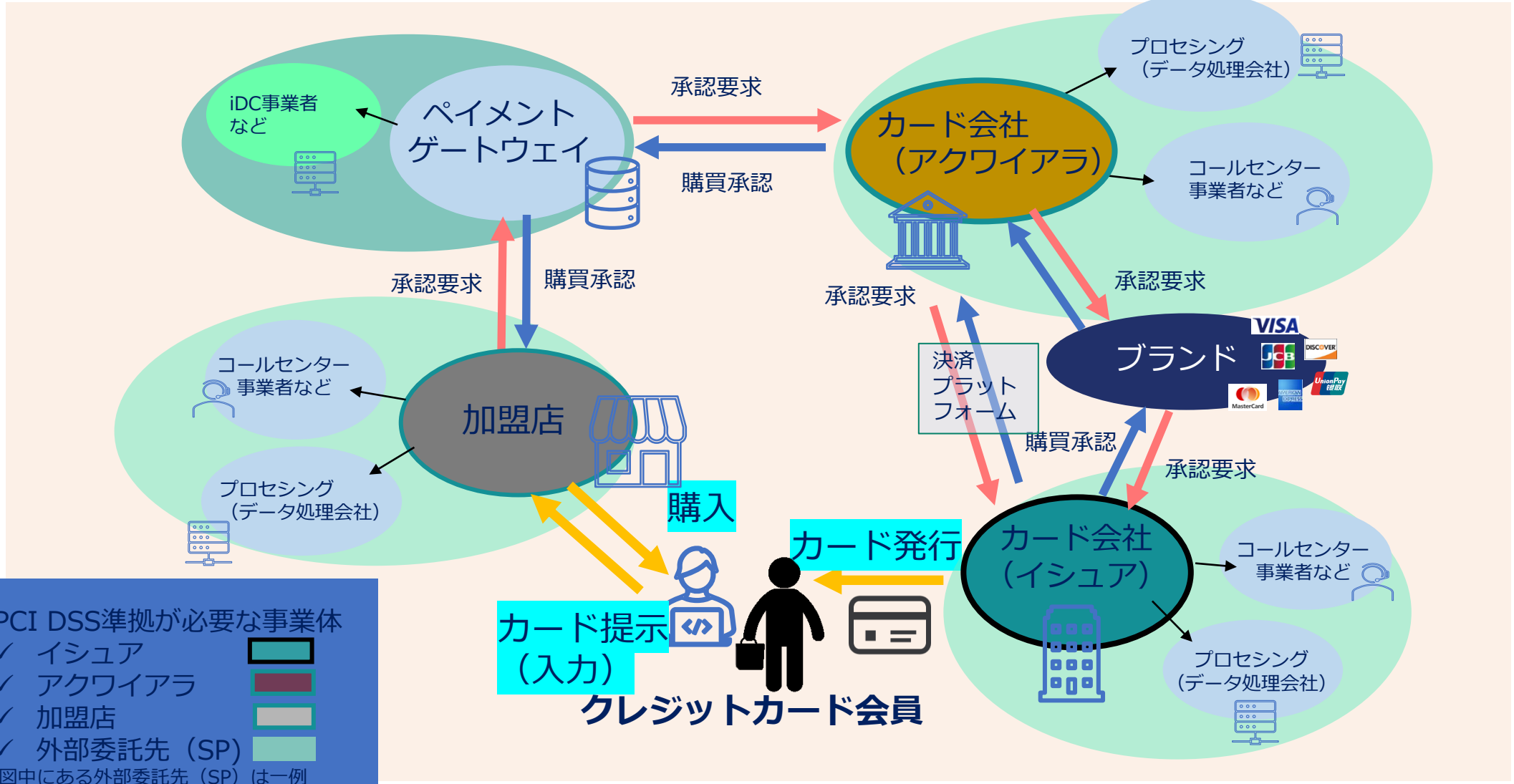
		データ要素	保存の許可	要件3.5に従い保存されたデータを読み取り不能にする
アカウントデータ	**カード会員データ**	カード番号（PAN）	要件3.2に従い最小限の保存を行う	YES
		カード会員名	要件3.2に従い最小限の保存を行う※5	NO
		サービスコード		
		有効期限		
	機密認証データ※1	全トラックデータ※2	要件3.3.1に従い**承認後は**保存できない※6	要件3.3.2に従い**承認前は**強力な暗号化で読み取り不能とする必要がある
		CAV2 /CVC2/CVV2CID ※3（セキュリティコード）		
		暗証番号（PIN）/ PINブロック※4		

- PANがカード会員データの他の要素と共に保存される場合、 PCI DSS 要件3.5.1に従い、PANのみ読み取り不能にする必要がある。

※1　機密認証データはオーソリ（承認）処理の後、たとえ暗号化していても保存してはならない。これはPANが保存されていない環境にも当てはまる。
※2　磁気ストライプの全てのトラックデータ、チップ上の同等のデータなど。
※3　ペイメントカードの前面または裏面に印字された 3 桁または 4 桁の数字。
※4　取引中にカード会員によって入力される個人識別番号、または取引メッセージ内に存在する暗号化された PIN ブロック、あるいはその両方。
※5　ただし、イシュアおよびイシュアサービス会社が許可された場合を除く。
※6　　イシュアおよびイシュアサービス会社に対する要件は、要件3.3.3にて別途定めている。

9:クレジットカードのトランザクション概略

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



PCI DSS準拠が必要な事業体
- ✓ イシュア
- ✓ アクワイアラ
- ✓ 加盟店
- ✓ 外部委託先（SP）

図中にある外部委託先（SP）は一例

国際マネジメントシステム認証機構について

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

略称：ICMS（International Certificate authority of Management System Co., Ltd.）

1999年設立。
2003年JIPDECから認定を受けたISO27001/JISQ27001審査認証機関としてISMS審査事業、2008年PCI SSCの認定セキュリティ評価機関（QSAs）としてPCI DSS監査事業を始めました。PCI DSS監査の実績は国内最多クラスとなります。

ISMS、PCI DSSともに規格の制定早期より携わる審査スキルを強みとし、ITエンジニアスキルをベースとした審査・監査事業を中心に、情報セキュリティ関連の教育、サービスを提供しています。

認定　　：　ISMS-AC認定　ISMS・クラウドセキュリティ認証機関：JIS Q 27001（ISO/IEC27001）
PCI SSC認定PCI評価機関：PCI DSS、P2PE、3Dセキュア、PINセキュリティ、PCI TSP

ICMSのサービス

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（ICMS）

審査/監査

■ISMS、ISMSクラウドセキュリティ
■PCI 各種監査（PCI DSS、PCI P2PE、PCI 3DS、PCI PIN、 PCI TSP）

ICMSソリューションズ株式会社

■カード情報セキュリティコンサルサービス
・PCI DSS/SAQ/P2PE/3Dセキュア/PINセキュリティ/PCI TSP/
割賦販売法/リスク分析

2023年9月よりPCI DSS評価機関
QSAカンパニーに認定

■SAQ AOC署名サービス
■セキュリティ各種診断
■セキュリティソリューション & SI
■セキュリティ教育・PCI DSS/情報セキュリティ教育研修/eラーニングPCI DSS v4.0
■フォレンジック

**セキュリティ
ソリューション**

お問い合わせ

国際マネジメントシステム認証機構株式会社（ICMS)
TEL　03-5719-7533
mail　suishin@icms.co.jp
URL　https://www.icms.co.jp/

****

※PCI DSS v4.0解説記事ならICMSのHP[監査Tips!]で！
https://www.icms.co.jp/tips/
※PCI DSS v4.0書籍[徹底解説書]はオンライン書店[fujisan]にて発売中！
https://www.icmssol.co.jp/news/2023/04/pci-dss-v40icms.html

****