

PCI DSSとは

Payment Card Industry Data Security Standard

Ver.1
2025.1.31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

1. PCI DSSとは？
2. 国内の基準との相関
3. PCI基準とは？
4. PCI DSS対象システムと業務
5. アカウントデータとは？
6. PCIDSS 対象の事業体
7. PCI DSSの適用範囲
8. 保管禁止データ
9. クレジットカードのトランザクション概略

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)

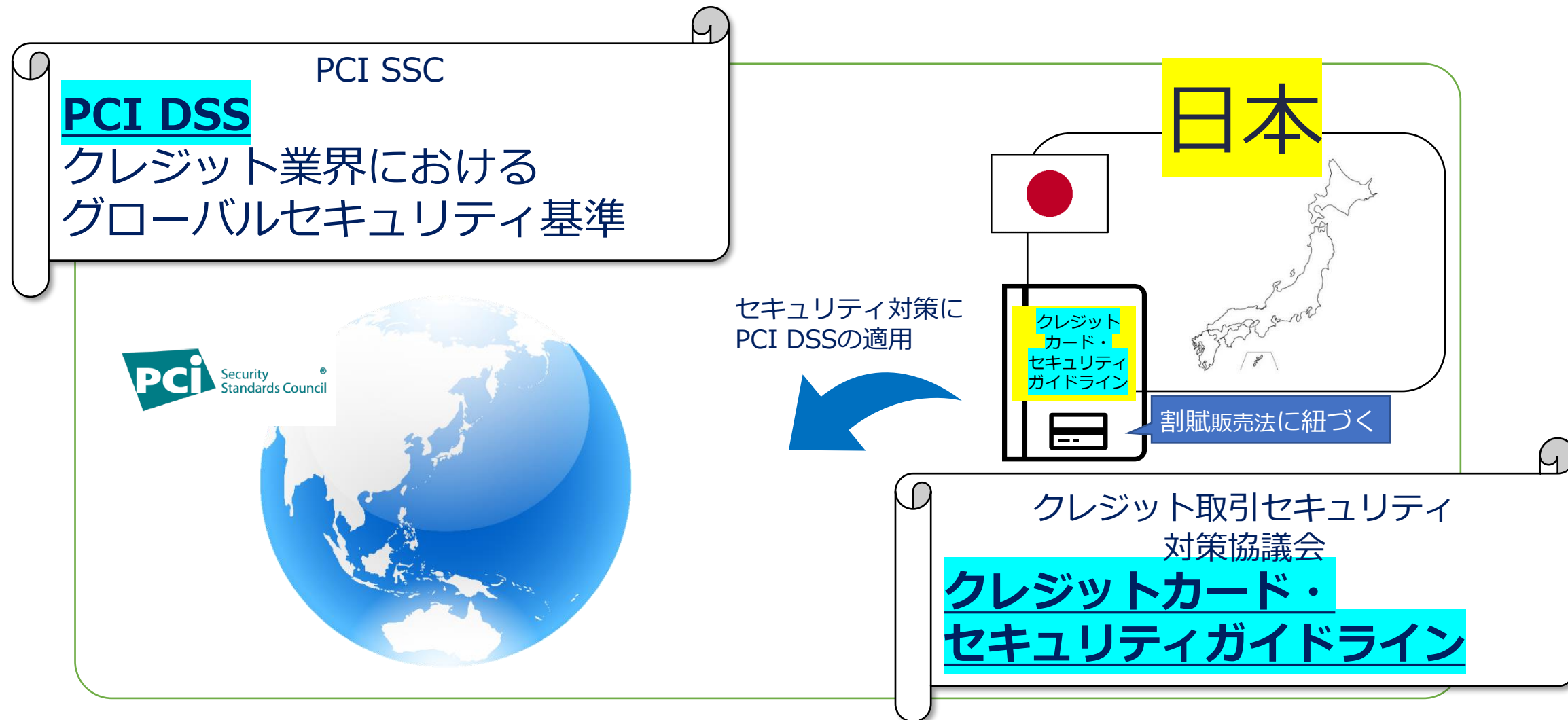
国際カードブランド5社（VISA、MasterCard、American Express、JCB、Discover）が共同で設立し、2020年より銀聯が参加、計6社による*PCIセキュリティ基準審議会(米国) が制定する事実上の基準）。

*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



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？

PCI DSSの保護対象であるカード情報を「アカウントデータ」と定義している。

アカウントデータには、「カード会員データ」と「機密認証データ」が含まれる。

アカウントデータ	
カード会員データ	機密認証データ
・プライマリアカウント番号（PAN） ・カード会員名 ・有効期限 ・サービスコード	・フルトラックデータ（磁気ストライプデータ またはチップ上の同等のデータ） ・カード検証コード（セキュリティコード） ・PIN/PINブロック

5: アカунデータとは？

アカウントデータ

カード会員データ (CHD)

- ・プライマリアカун番号 (PAN) (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



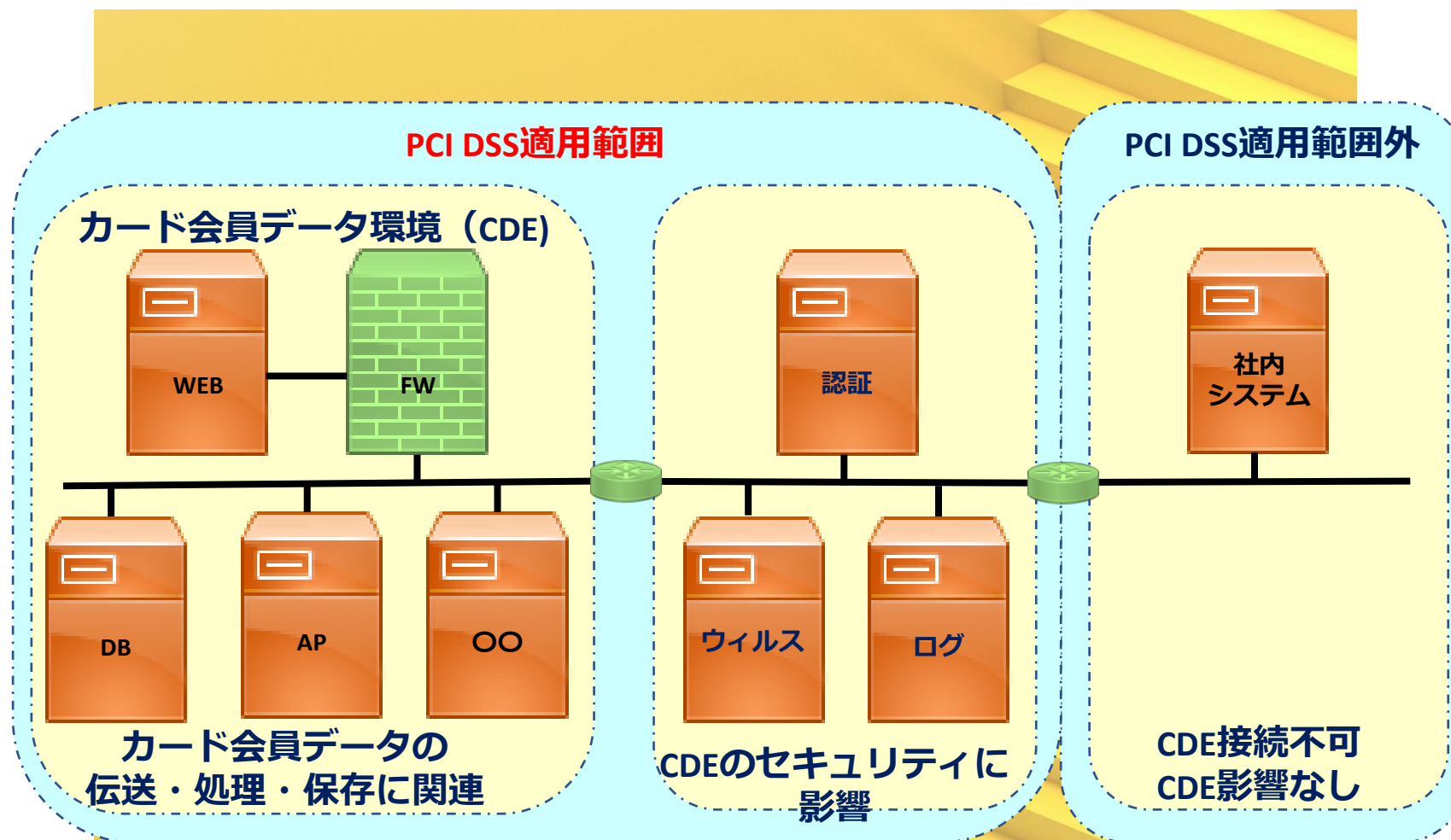
アカウントデータを扱う全ての事業体

加盟店、プロセッシング、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



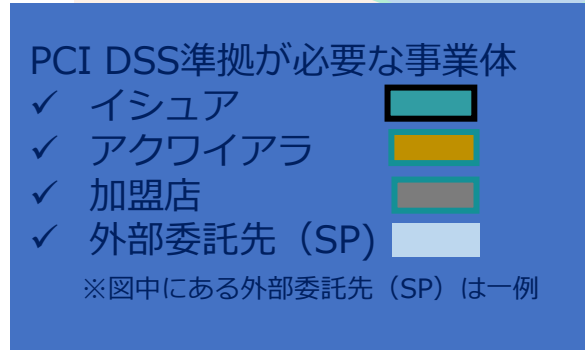
8: 保管禁止データ



PCI DSS Ver.4.0.1		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。

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。

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グループ お問い合わせ先



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

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）
- SAQ AOC署名サービス



ソリューション



- PCI DSS、SAQ、カード情報セキュリティコンサルサービス
- セキュリティ診断/セキュリティソリューション&SI
- セキュリティ教育/フォレンジック



フォレンジック



- デジタル・フォレンジック
- 情報漏えい/内部不正調査/コンサルティング
- インシデント対応/フォレンジック初級～上級トレーニング

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/>



※QSAから要件を学ぶ[監査Tips!]

<https://www.icms.co.jp/tips/>

※QSAによる解説PCI DSS v4.0書籍[徹底解説書]

<https://www.icmssol.co.jp/>

