クレジットカード情報の保護とPCI DSSの最新動向

日本カード情報セキュリティ協議会(JCDSC)
運営委員長　武藤　敏弘

2017年9月6日

クレジットカードを取り巻く状況

日本カード情報セキュリティ協議会（JCDSC）

安全なカード社会の実現をめざして

日本カード情報セキュリティ協議会

JAPAN CARD DATA SECURITY CONSORTIUM

JCDSC Japan Card Data Security Consortium

日本カード情報セキュリティ協議会とは | サイトマップ | FAQ | お問合せ

協議会について

- 日本カード情報セキュリティ協議会とは
  - 概要・ごあいさつ
  - 会員企業一覧
  - 会則
  - 入会案内
- カード業界を取り巻く環境とセキュリティーの重要性

PCI DSS

- グローバルセキュリティ基準 PCI DSSとは
  - 概要
  - 認定取得のメリット
  - 認定取得について
  - 認定審査機関について
  - 導入が必要な企業
  - QSA/ASV 企業一覧
- PCI DSS 準拠への参考資料集
  - 会員専用コンテンツ

NEWS

2017年09月05日	NEW! 当協議会の会員企業が205社になりました
2017年08月23日	NEW! ISAとQSA育成講習会が11月に東京で開催されます
2017年08月04日	“カード情報非保持”支援セミナー開催のお知らせ 2017年9月28日（木）日本橋公会堂（人形町・水天宮前）
	NEW! “カード情報非保持”支援セミナー 2017.9.28 開催
2017年07月13日	NEW! 2018年東京・PCI SSC-CMの日程が決定
2017年06月28日	NEW! PCI P2PEセミナー 2017.7.26 開催
2017年06月27日	NEW! PCI DSS セキュリティフォーラム 2017 レポート
2017年05月19日	NEW! PCI DSSの各種SAQ v3.2 日本語版が公開されました
2017年05月15日	NEW! PCI DSS 基準書v3.2 日本語版が公開されました
2017年05月02日	NEW! JCDSC 2017年度総会レポート
2017年03月09日	カードセキュリティの「実行計画2017」を経済産業省が公表
2017年02月28日	PCI DSS の優先的なアプローチv3.2日本語版が公開されています
2017年02月23日	「PCI DSS対応 実務者セミナー」3/22(水)開催のお知らせ

過去のニュースはこちらからご覧頂けます。>>

セミナー情報

開催日	セミナー/研修会等の名称	開催地
8/4(金)	クラウド活用で実現するPCI DSS準拠 主催：株式会社リンク ／ 参加費用：無料 PCI DSS準拠が必要な通販事業者、旅行代理店、BPO/コールセンター事業者等向けにクラウドの活用によって、準拠を短納期・低価格で実現する方法を解説します。	株式会社リンク（東京 赤坂）

広告掲載について

外部のサイトへリンクします。

PCI-DSS最新資料を一括請求 PCI-DSSナビ

Sun Partners Co.,Ltd

Xseed

ASR ・QSA(PCIDSS) ・ISO 認証機関 エイエスアール株式会社

DL DATA LINKS

PCI DSS Ready Cloud

bsi.

ネット取引と不正利用による被害

【クレジットカード決済の動向】

ネット取引の急拡大に伴い、近年、**クレジットカード取引高は一貫して増加**。

- 直近では、**約５４兆円**（消費全体の**約１８%**）を占める。

（参考）主要各国のカード利用率　韓国：５４%、中国：５５%、米国：４１%

【クレジットカードの不正利用】

・ 昨今、**セキュリティ対策が不十分な加盟店を狙った不正アクセス**により、**カード情報の漏えいが拡大。**

・ これに伴い、窃取したカード情報を使って、偽造カードや本人になりすました**不正使用による被害は増加**。（2016年**140.9億円**と4年間で約2.1倍。　＊2012年は６８．１億円）

・ 不正使用は国境を越えて行われ、換金性の高い商品の購入を通じて、**犯罪組織に多額の資金が流出**しているとの指摘あり。

最近の主な国内カード情報流出事件

件数	流出内容
9,426件	氏名（カード名義人名）、クレジットカード番号、有効期限
719,830件	クレジットカード番号・クレジットカード有効期限・メールアドレス等 （※622件は**セキュリティコード**流出可能性有）
17,085件	カード番号、カード名義、有効期限、**セキュリティコード**
29件	カード名義、カード番号、有効期限
578件	カード番号、有効期限、**セキュリティコード**、カード名義、氏名、住所
835件	カード番号、カード名義、有効期限、**セキュリティコード**
99件	カード番号、有効期限、**セキュリティコード**、会員名、住所
不明	クレジットカード情報　※詳細不明
65,820件	会員名、カード番号、住所、有効期限
1,066件	氏名、住所、電話番号、メールアドレス、クレジットカード番号、有効期限

「実行計画」における対策の３本柱

(1) カード情報の漏えい対策

◇カード情報を盗らせない

- 加盟店におけるカード情報の「非保持化」
- カード情報を保持する事業者のPCIDSS準拠

(2) 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

(3) ECにおける不正使用対策

◇ネットでなりすましをさせない

- 多面的・重層的な不正使用対策の導入

9．ｸﾚｼﾞｯﾄｶｰﾄﾞ情報の漏えい防止（カード情報非保持/PCI DSS準拠）

現 状 ・ 課 題

- 近年、サイバー攻撃によるEC加盟店等からの**カード情報の漏えい事故が頻発**※2015年30件（前年比2.3倍）。
- カード情報を狙うハッカーの**攻撃手口のグローバル化・巧妙化**。
- 加盟店等において、カード情報を取り扱っている**当事者意識が希薄**で対策が不十分。

目 標

○ 加盟店は、原則、**カード情報の非保持化**

○ カード情報を取り扱う事業者は、セキュリティに関する**国際規格（PCI DSS）準拠**

各主体の役割

カード会社・PSP（決済代行業）

・**PCI DSS準拠を完了(2018年3月まで)**
・カード会社は、PCI DSSに準拠していないPSPとの取引を見直し(2018年4月目途)
・加盟店に対して非保持化又はPCI DSS準拠に向けた要請・支援

加盟店

※2018年5-６月頃 改正割販法の施行→義務化
・カード情報の**非保持化又はPCI DSS準拠**（**EC加盟店は2018年3月まで、対面加盟店は最終的には2020年3月までに完了**）
・最新の攻撃手口に対応したセキュリティ対策の改善・強化を不断に実施

行政

・カード情報の適切な保護について、事業者や消費者に情報発信
・NISC、JPCERT等の**セキュリティ関係機関との連携・情報共有**

改正割賦販売法、実行計画2017

「割賦販売法の一部を改正する法律」が公布

2016年12月9日 → 2018年6月施行予定

http://www.meti.go.jp/policy/economy/consumer/credit/112kappuhanbaihoukankeishiryou.html

1. 本法律案の趣旨

近年、クレジットカードを取り扱う販売業者におけるクレジットカード番号等の漏えい事件や不正使用被害が増加しています。（中略）また、カード発行を行う会社と販売業者と契約を締結する会社が別会社となる形態が増加し、これに伴ってクレジットカードを取り扱う販売業者の管理が行き届かないケースも出てきています。こうした状況を踏まえ、革新的な金融サービス事業を行うFinTech（フィンテック、Finance×Technologyの略。）企業の決済代行業への参入を見据えつつ、安全・安心なクレジットカード利用環境を実現するための必要な措置を講じます。本措置は、2020年の東京オリンピック・パラリンピックに向け、インバウンド需要を取り込むことにも資するものです。

「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2017」公開

2017年3月8日公開

http://www.meti.go.jp/press/2016/03/20170308003/20170308003.html

「未来投資戦略2017－Society 5.0の実現に向けた改革」

我が国経済の再生に向けて、経済財政諮問会議との連携の下、必要な経済対策の実施や成長戦略の実現のための司令塔として日本経済再生本部を設置しています。
また、日本経済再生本部の下、「未来への投資」の拡大に向けた成長戦略と構造改革の加速化について審議するため、未来投資会議を開催しています。
(http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_t.pdf)

キャッシュレス化の推進 （31/383）

（残された課題）
・海外諸国と比較して、キャッシュレス化が十分に進展していない。**キャッシュレス決済の安全性・利便性の向上、事務手続の効率化、ビッグデータ活用による販売機会の拡大**等を図ることが課題である。

（主な取組）
・クレジットカード利用時の加盟店における書面交付義務の緩和について、電子メール等の電磁的方法も可能とすることで、カード決済のコスト削減や消費者の利便性の向上を図り、キャッシュレス化を後押しする。
・クレジットカードデータ利用に係るAPI 連携の促進を図りつつ、レシートの電子化促進のためのフォーマットの統一などの環境整備を本年度内に行う。

PCI DSSとは

非保持化
（非保存、非処理、非通過）

または

PCI DSS準拠

PCI DSS準拠の重要性

実行計画2017” P5

・**我が国がセキュリティホール化**し、不正使用被害が**国境を越えて流入するリスク**が高まっていることへの危機意識を各主体は共有した上で、本実行計画を早急に実行することが求められる。

実行計画2017” P19

・カード情報を取り扱うカード会社及びPSPについては、業務上大量のカード情報を管理・利用しており、カード取引に係るインフラの一端を担う重要な役割に鑑み、**PCI DSSの準拠は当然の責務**である。仮に、このような重要なポジションを占める事業者がPCI DSSに準拠しない場合、**クレジットカード取引システム全体への脅威ともなりかねない**ことから早急な対応が必要である。

これらのカード情報を取り扱う事業者については、PCI DSS準拠に加えて、巧妙化するサイバー攻撃への対応を含むセキュリティ対策の改善・向上・維持に向けた継続的な取組が重要であることを認識する必要がある。

実行計画2017” P23

・カード情報を取り扱うカード会社及びPSPは、2018年3月末までに確実にPCI DSS準拠を完了することを目指すとともに、未だ準拠していない場合には、目標期限に向け、早急に取組を進める。

非保持化

カード情報そのものを扱わない。その他に？

PAN　1234 5678 9012 3456

↓

マスキング例　1234 56XX XXXX 3456

（始め**6桁**＋終わり**4桁**以外を**マスキング**）

トランケーション
トークナイゼーション（トークン化）

◆要件3.3

PANの最初の6桁および最後の4桁以外の数字を表示する（フル桁表示含む）場合は、正当な業務上の必要性が必要となる

PCI DSS データセキュリティ基準の歴史

2001年
- MasterCard ,VISAがﾃﾞｰﾀﾌﾟﾛﾃｸｼｮﾝﾌﾟﾛｸﾞﾗﾑ(SDP, AIS) 開始
  - ＊ SDP: Site Protection Program , AIS: Account Information Security

2004年12月
- MasterCard 、VISA提携でPCI DSS Ver1.0
- VISA、JCBがPCI DSS Ver1.0の日本語版を公表

2005年4月
- VISAが加盟店・プロセサを対象に無料脆弱性診断サービスを開始

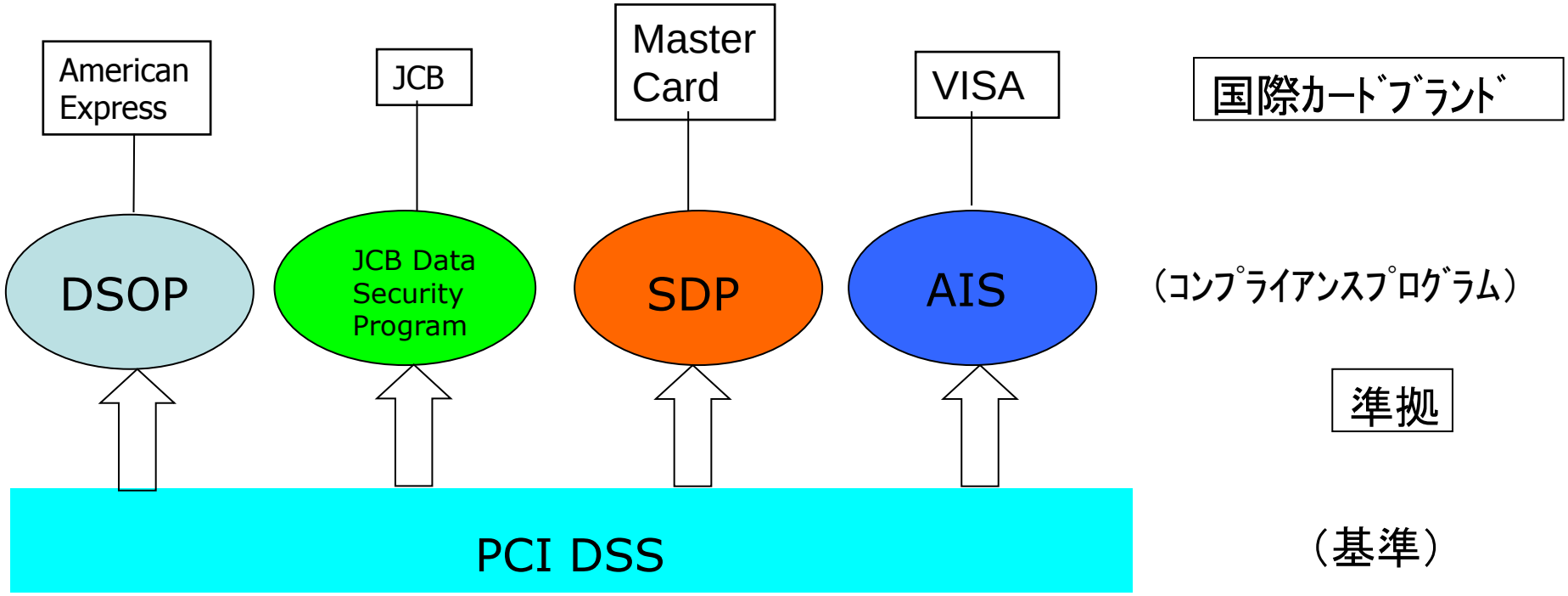
2006年9月
- 国際ﾍﾟｲﾒﾝﾄﾌﾞﾗﾝﾄﾞ5社(American Express, Discover, JCB, MasterCard, VISA)がPCI SSC (PCI Security Standards Council)を設立
- PCI DSS Ver1.1発行

2008年10月 PCI DSS Ver1.2発行
2010年10月 PCI DSS Ver2.0発行
2013年10月 PCI DSS Ver3.0発行
2015年 4月 PCI DSS Ver3.1発行
2016年 4月 PCI DSS Ver3.2発行

PCI セキュリティ基準

PCI セキュリティ基準は、PCI Security Standards Council （PCI SSC）がカード会員データを保護するために規定した技術面および運用面の要件です。 この基準はカード会員データを保存、処理、または送信するあらゆる組織に適用され、取引に使用するアプリケーションのソフトウェア開発者および製造業者にガイダンスを提供します。

各ﾌﾞﾗﾝﾄﾞのｺﾝﾌﾟﾗｲｱﾝｽ・ﾌﾟﾛｸﾞﾗﾑとの関連



DSOP: Data Security Operating Policy,　SDP: Site Data Protection,
AIS: Account Information Security

05/09/2017

各ブランドはそれぞれのコンプライアンスプログラムをもっている
・加盟店／サービスプロバイダのレベル分け、・審査結果の報告方法　他

PCI DSSとは？

PCI DSS

Payment Card Industry Data Security Standards

・クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界の**グローバル**なセキュリティ基準です

・国際カードブランド5社（American Express、Discover、JCB、MasterCard、VISA）が共同で設立したPCI SSC（Payment Card Industry Security Standards Council）によって運用、管理されています

・PCI DSSでは、他の多くの基準が曖昧にしている**数値基準を具体的に設定**されているのが特徴です

・**各ブランドのセキュリティ基準**（過去の事故事例対策）を基に2004年に策定され、最新バージョンは3.2となります。

PCI DSSの主な目的はカード情報の適切な保護

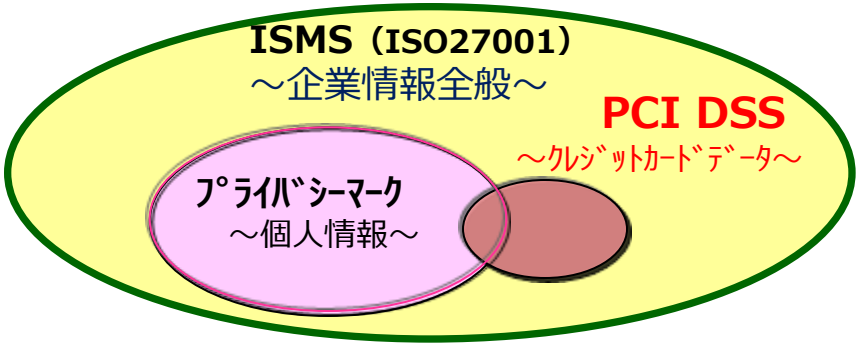
1）カード会員データを適切に、安全に
保護する。

2）カード会員データが漏洩しても使えない
状態にしておく（データの無価値化）。

PCI DSSの重要度

犯罪者に最も狙われやすいクレジットカード（企業の重要）情報を保護する為にPCI DSSの重要性が増してきています

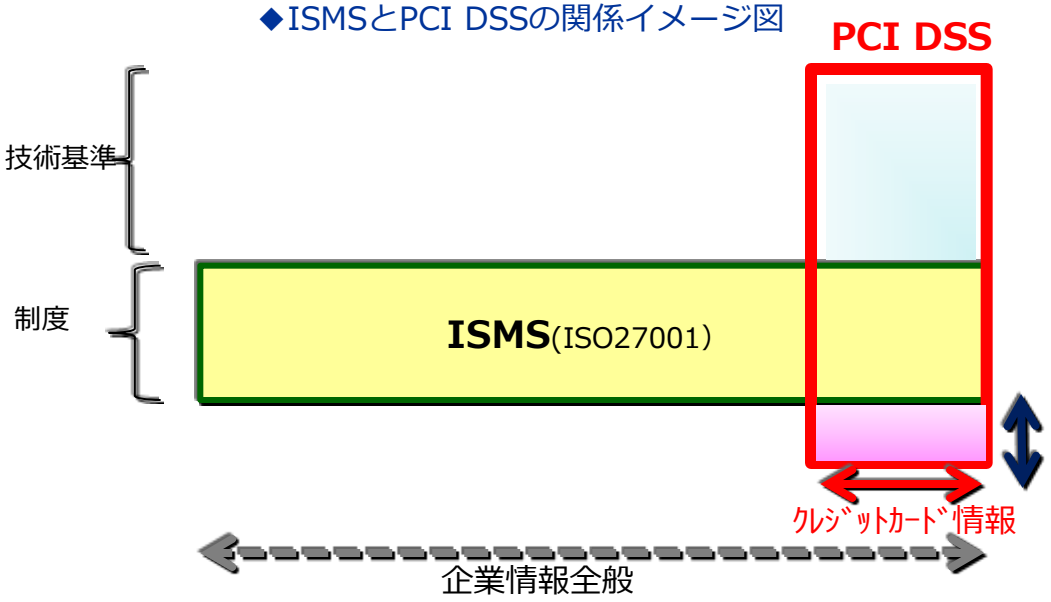
◆情報保護の範囲概念図



ISMS/ISO27001は、組織の大小に関係なく適用する事を前提にした基準の為、ISMSが定義する管理項目については、その適用選択は企業側のリスク重要基準に寄ります。

ISMSは組織が重要と判断する情報資産を対象としてPDCAサイクルを構築して情報セキュリティ運用管理をする事を要求するのに対して、PCI DSSはカード会員情報を保護するための具体的な技術基準となっており、カード会員情報を継続的に保護するためには、ISMS/PCI DSS両方の準拠が有効と言われています。

◆ISMSとPCI DSSの関係イメージ図



犯罪者の攻撃対象に・・・

ISMSの要求基準（フレームワークと管理策）

- パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うことを、利用者に要求すること

PCI DSSの要求基準（技術要件）

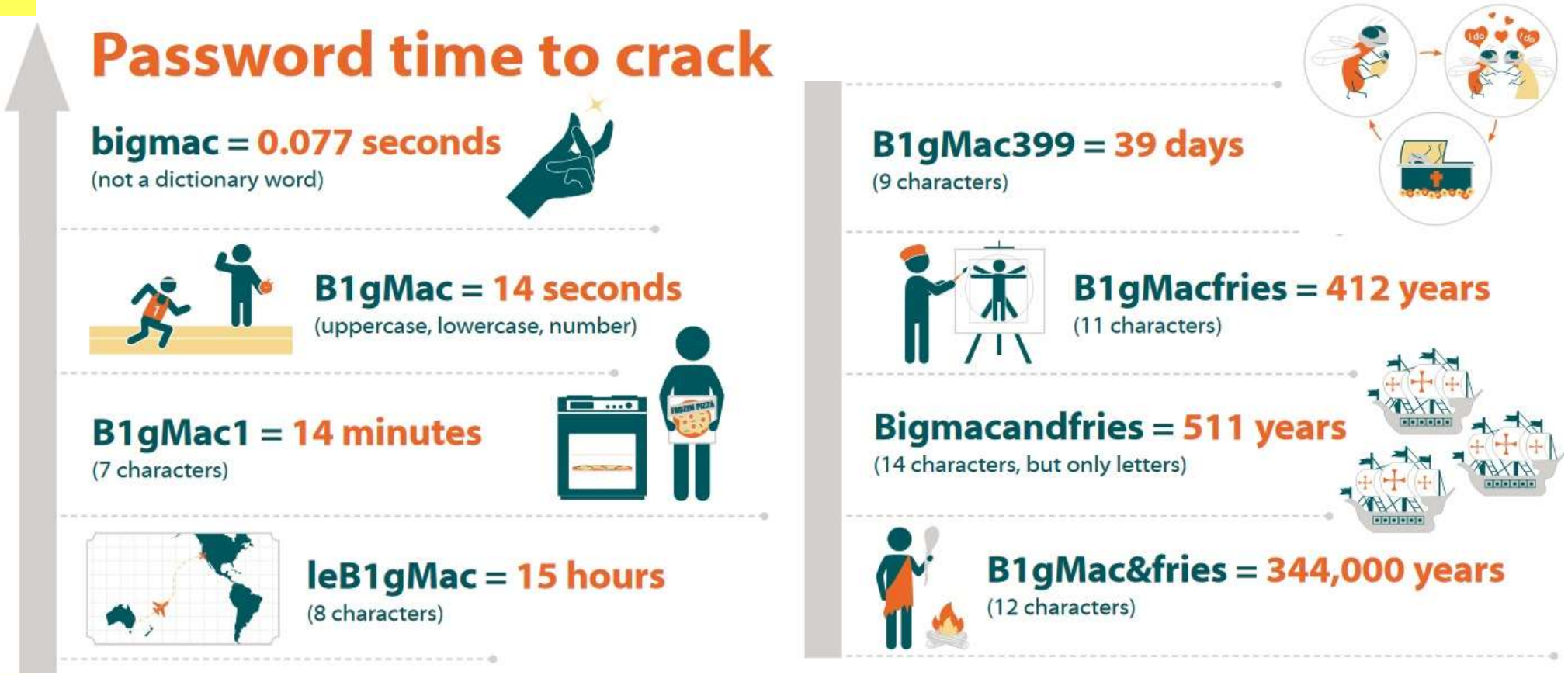
- 数字と英字の両方を含むパスワードを使用する。
- パスワードの長さは、少なくとも７文字にする。
- パスワードは少なくとも90日ごとに変更する。
- 直近４回使用されたパスワードは、新しいパスワードとして使用できないようにする。
- ユーザーＩＤのロックアウトにより、連続したアクセス試行を６回以内に制限する。
- ロックアウト時間は最低30分間、またはアドミニストレーターが許可するまでとする。
- セッションのアイドル時間が15分を超えた場合、パスワードの入力を再び要求する。

「最悪のパスワード」ワースト25　2017年1月23日

2016年「最も危険なパスワード」	
1位	123456
2位	123456789
3位	qwerty
4位	12345678
5位	111111
6位	1234567890
7位	1234567
8位	password
9位	123123
10位	987654321
11位	qwertyuiop
12位	mynoob
13位	123321
14位	666666
15位	18atcskd2w
16位	7777777
17位	1q2w3e4r
18位	654321
19位	555555
20位	3rjs1la7qe

21位	google
22位	1q2w3e4r5t
23位	123qwe
24位	zxcvbnm
25位	1q2w3e

参考：強くて覚えやすいパスワードの作り方



※ [It's time to change your password](#) （PCI SSC）

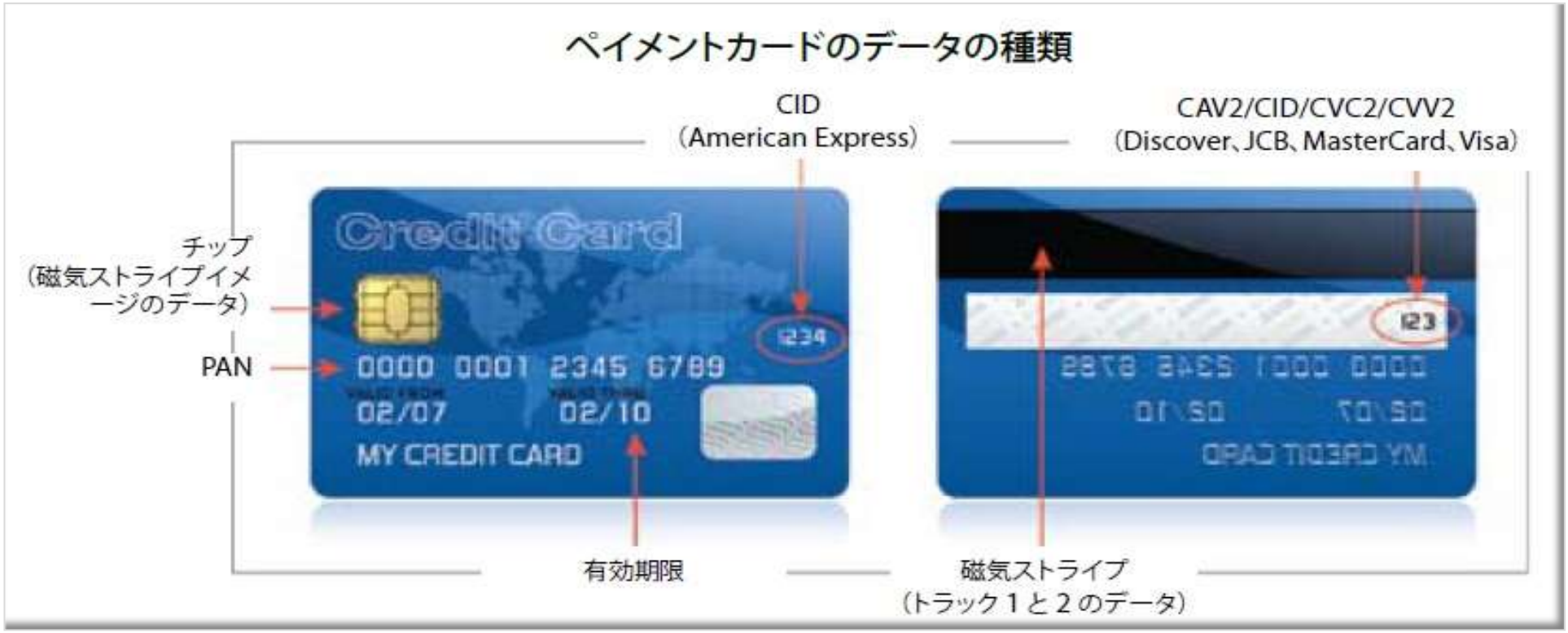
PCI DSS準拠にむけて

PCI DSSで対象となるカードデータ

PCI DSS は加盟店、プロセサー、取得者、発行者、サービスプロバイダのほか、**カード会員データ**や**機密認証データ**を**保存**、**処理**、または**送信**するその他の事業体などの、ペイメントカードの処理を行うすべての事業体に適用されます。

		データ要素	保管可否	保護の必要性	PCI DSS 要件 3.4
アカウントデータ	カード会員データ	カード番号(PAN)	YES	YES	YES
		カード会員名[1]	YES	YES	NO
		サービス コード[1]	YES	YES	NO
		有効期限[1]	YES	YES	NO
	センシティブ認証データ	完全な磁気ストライプデータ	NO	N/A	N/A
		CAV2/CVC2/CVV2/CID	NO	N/A	N/A
		暗証番号(PIN) / PINブロック	NO	N/A	N/A

ペイメントカードのデータ種類



※参考　「PCIクイックレファレンスガイド」

※PANは「Primary Account Number（プライマリアカウント番号）」の頭字語で、「アカウント番号」とも呼ばれます。イシュアおよび特定のカード会員アカウントを識別する、一意なカード番号（一般に、クレジットカードまたはデビットカード）です。

PCI DSS 要件への準拠の評価範囲

カード会員データ環境は、カード会員データまたはセンシティブ認証データを保存、処理、または送信する人、処理、およびテクノロジで構成されます。

（PCI DSS 基準より）

伝送、処理、保管のいずれかの環境は全て対象

役に立つドキュメント

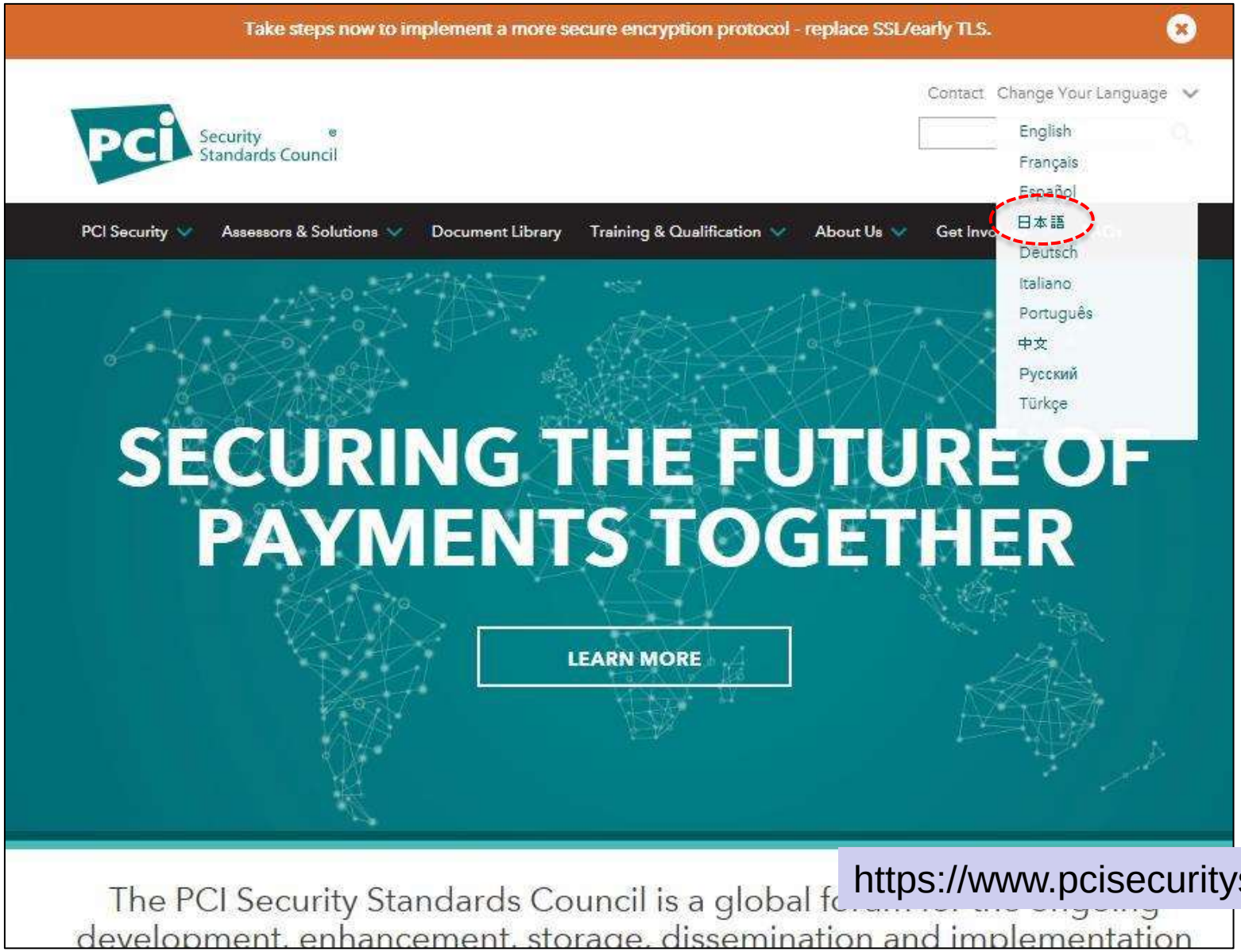
1. PCI DSS基準＊

2. 用語集＊

3. 各種SAQ（自己問診票）

4. PCI DSSスコーピングとネットワーク・
セグメンテーションに関わるガイダンス

PCI SSC（Payment Card Industry Security Standards Council）

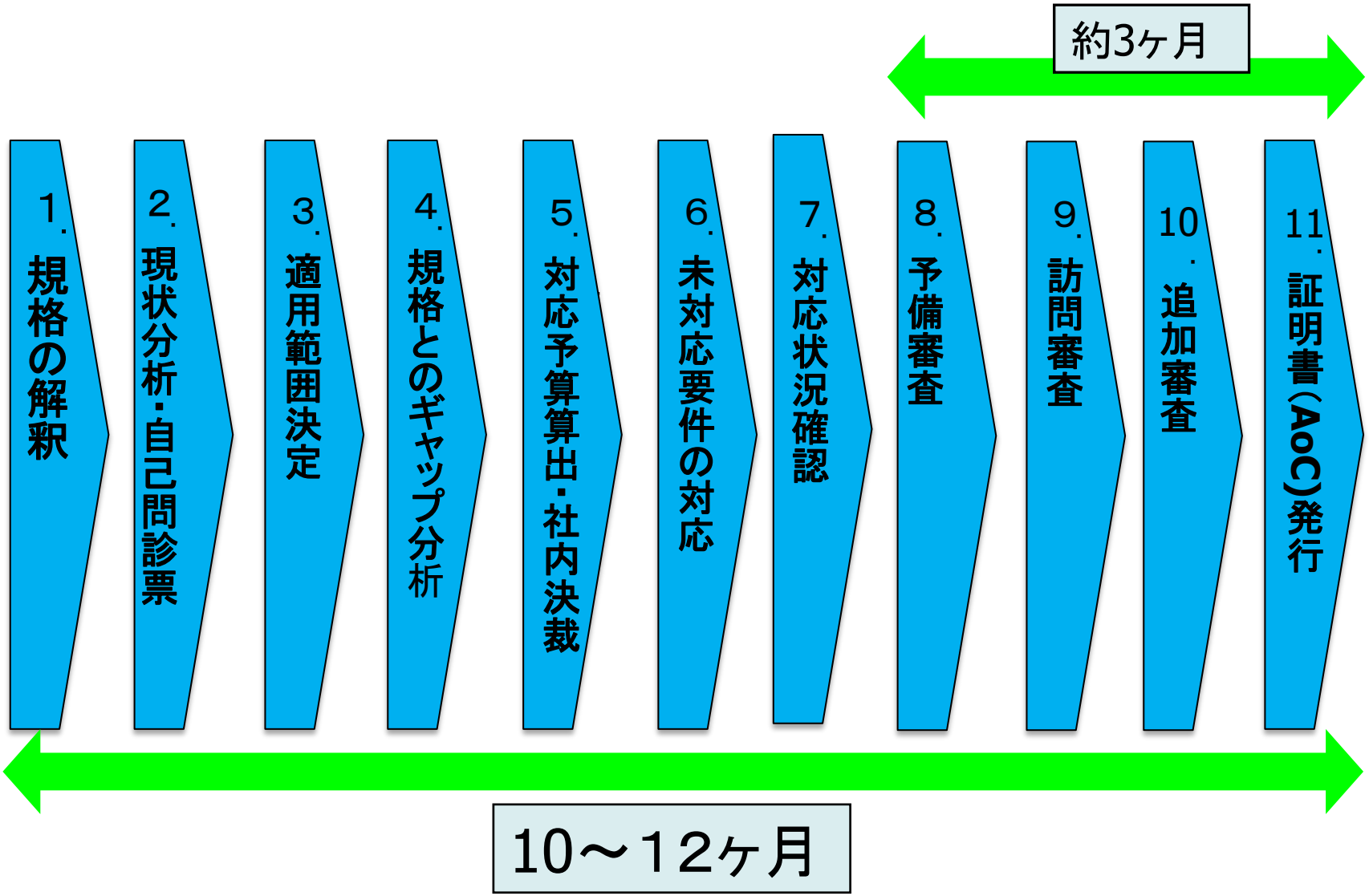


https://www.pcisecuritystandards.org/

PCI DSSの概要

安全なネットワークとシステムの構築と維持	1. カード会員データを保護するために、ファイアウォールをインストールして維持する 2. システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
カード会員データの保護	3. 保存されるカード会員データを保護する 4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱性管理プログラムの維持	5. マルウェアにしてすべてのシステムを保護し、ウィルス対策ソフトウェアを定期的に更新する 6. 安全性の高いシステムとアプリケーションを開発し、保守する
協力なアクセス制御手法の導入	7. カード会員データへのアクセスを、業務上必要な範囲内に制限する 8. システムコンポーネントへのアクセスを識別・認証する 9. カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	10. ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する 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
情報セキュリティポリシーの維持	12. すべての担当者の情報セキュリティに対応するポリシーを維持する

PCI DSS完全準拠への一般的な流れ



準拠を目指す企業の要望

１．できるだけ人的負担を抑えたい。
２．できるだけ予算を抑えたい。
３．できるだけ短期間で対応したい。
４．手戻り無く方向性を確実にした上で対応したい。

安く、早く、確実に手戻り無く！

カード情報のシステム・リスク、セキュリティ・リスクを軽減する

1. クレジットカード会員データを持たない。

2. システム上、カード会員環境をできるだけコンパクトにする。

3. カード会員環境にアクセスできる人を最小にする。

PCI DSS構築・維持の負担軽減

PCI DSS基準書の読み方

◆ PCI DSS基準書をよく読む

概論、概要、テスト手順、ガイダンスまでよく目を通す

PCI DSS 要件の適用範囲

PCI DSS のセキュリティ要件は、カード会員データ環境に含まれる、または接続されるすべてのシステムコンポーネントに適用されます。カード会員データ環境（CDE）は、カード会員データまたは機密認証データを保存、処理、または送信する人、処理、およびテクノロジで構成されます。「システムコンポーネント」には、ネットワークデバイス、サーバ、コンピュータ、アプリケーションが含まれます。システムコンポーネントの例には、次のものが含まれますが、これらに限定されるわけではありません。

- セキュリティサービス（認証サーバなど）を提供する、セグメンテーションを促進する（内部ファイアウォールなど）、または CDE のセキュリティに影響を及ぼす（名前解決や Web リダイレクションなど）システム。
- 仮想マシン、仮想スイッチ/ルーター、仮想機器、仮想アプリケーション/デスクトップ、ハイパーバイザなどの仮想コンポーネント。
- ファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器を含むが、これらに限定されないネットワークコンポーネント。
- Web、アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームサーバ（DNS）などを含むが、これらに限定されないサーバタイプ。
- 内部および外部（インターネットなど）アプリケーションを含む、すべての市販およびカスタムアプリケーション。
- CDE 内にあるか CDE に接続されているその他のコンポーネントまたはデバイス

Payment Card Industry（PCI）データセキュリティ基準 v3.2日本語版 (P11)

「データセキュリティ基準　要件とセキュリティ評価手順」

ーガイダンスの効果的な利用ー
＊対応するためのヒント
「目的」「チェックすべき事象」は、何か？
適切な解釈とは？
危険な環境とは？

PCI Security Standards Council

カード会員データの保護

要件 3:　　保存されるカード会員データを保護する

暗号化、トランケーション、マスキング、ハッシュなどの保護方式は、カード会員データ保護のための重要な要素です。侵入者が他のセキュリティコントロールを回避し、暗号化されたデータにアクセスできても、正しい暗号化キーがなければ、そのデータを読み取り、使用することはできません。保存したデータを保護するための効果的な別の方法として考えられるのは、リスクを軽減する方法です。たとえば、リスクを最小限にする方法として、カード会員データが絶対的に必要でない限り保存しない、完全な PAN が不要ならカード会員データを切り捨てる、電子メールやインスタントメッセージングなどのエンドユーザメッセージング技術を使用して保護されていない PAN を送信しない、などがあります。

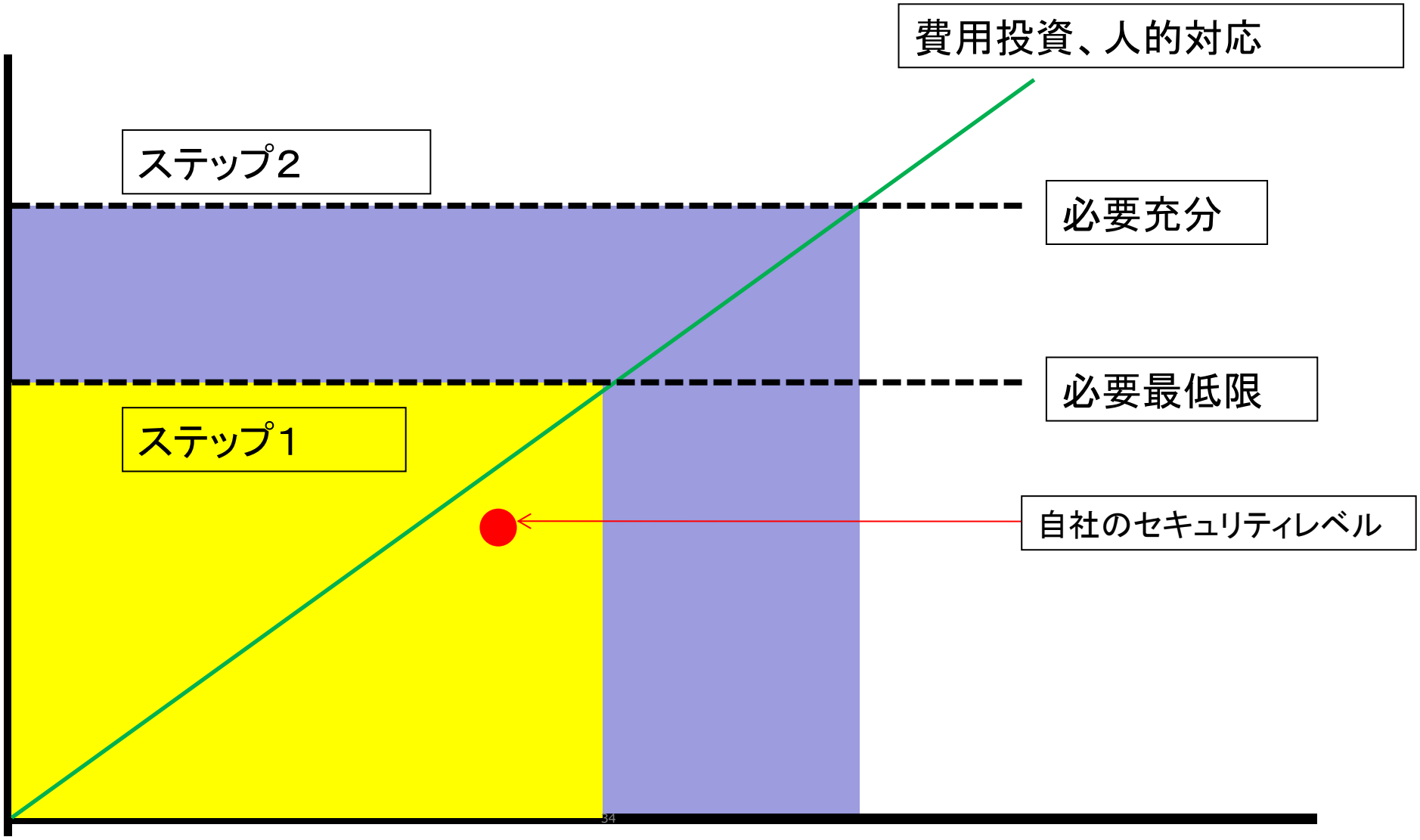
「強力な暗号化技術」および他の PCI DSS 用語については、『PCI DSS と PA-DSS の用語集（用語、略語、および頭字語）』を参照してください。

PCI DSS 要件	テスト手順	ガイダンス
3.1 データ保存および廃棄ポリシー、手順、プロセスを実装し、すべてのカード会員データ（CHD）ストレージに少なくとも以下のものを含めようにすることで保存するカード会員データを最小限に抑える。 • 保存するデータ量と保存期間を、法律上、規則上、業務上必要な範囲に限定する。 • 必要性がなくなった場合のデータを安全に削除するためのプロセス • カード会員データの特定のデータ保存要件 • 定義された保存要件を超えるカード会員データを安全に廃棄する四半期ごとのプロセス。	**3.1.a** データの保存および廃棄について、ポリシー、手順、プロセスを調べ、少なくとも以下のことが含まれていることを確認する。 • 以下を含むデータ保存についての、法律上、規制上、業務上の要件 • カード会員データの保存についての特定の要件（カード会員データは、X の期間、Y という業務上の理由で保存する必要がある、など）。 • 法律上、規制上、または業務上の理由で不要になったカード会員データの安全な削除 • カード会員データの保存すべてを対象とする • 定義された保存要件を超えるカード会員データを安全に廃棄する四半期ごとのプロセス。	正式なデータ保存ポリシーで、保存する必要があるデータとそのデータの保存場所を識別し、不要になった場合は即座に安全な方法で破棄または削除できるようにしておきます。 承認後に保存できるカード会員データは、プライマリアカウント番号（PAN）（読み取り不能に処理したもの）、有効期限、カード会員名、サービスコードのみです。 カード会員データを正しく保存し、必要なくなったときに破棄するためには、それがどこにあるかを知っていること[illegible]定義するには、ま[illegible]ニーズと、業界ま[illegible]るいはその両方）[illegible]上の義務を理解す[illegible] 特定の保存期間を[illegible]

【要件】
　対応すべき 内容

【テストの手順】
　QSAの確認手順

セキュリティ対策に対する投資



PCI DSS検証・評価方法

1．第三者であるQSAによる審査
2．自己問診

PIC DSS要件対応はどちらも同じ

QSAによる審査後の成果物

1）準拠証明書（AoC）＊
2）準拠レポート（ROC）＊
3）認証書

加盟店の証明書

SAQ（自己問診票）の概要①

SAQは「Self-Assessment Questionnaire（自己問診）」の頭字語です。事業体の PCI DSS 評価からの自己問診結果を文書化するために使用するレポートツールです。

タイプ	業態	カード情報の取り扱い携帯	準拠項目数（付録含）
A	決済サービスプロバイダ（PSP)のリンク（リダイレクト）型の決済サービスを使用するEC加盟店 ・カード情報の全ての処理を外部委託するEC/通信販売加盟店	ECまたは通信販売の加盟店でカード情報をシステムまたは加盟店内で電子形式で通過、処理、保存しない	22
A-EP	決済サービスプロバイダ（PSP）のJavaScript型の決済サービスを使用するEC加盟店	ECの決済をPCI DSS準拠済みのサービスプロバイダに部分的に委託しているECの加盟店でカード情報をシステムまたは加盟店内で電子形式で通過、処理、保存しない	193
B	CCTなどの決済端末をダイアルアップ接続する主に対面加盟店	インプリンタ、スタンドアロン型のダイアルアップの決済端末のみによってカード情報を処理する加盟店であり、カード情報を保存していない。	41
B-IP	CCTなどの決済端末をIP接続する主に対面加盟店	決済ネットワークまたはASP/クラウド事業者にIP接続されるスタンドアロン型のPCI PTS認定の決済端末のみによってカード情報を処理する加盟店であり、カード情報を保存していない。	88
C-VT	電話やハガキ/FAXでカード処理する主に通信販売加盟店	Webブラウザなどの仮想端末のみでインターネットを経由して、1件ずつカード情報を処理し、カード情報をコンピュータシステムに保存しない。決済に利用するWebアプリケーションはPSP、アクワイヤラーなどサードパーティから提供される必要がある。	85

参考：「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　－２０１７－　【公表版】」　P54-55

SAQ（自己問診票）の概要②

タイプ	業態	詳細	準拠項目数（付録含）
C	POSをインターネットに接続してカード処理する主にPOS加盟店	POSシステムまたはその他のインターネットに接続されているペイメントアプリケーション経由でカード情報を処理するが、カード情報をコンピュータシステムに保存しない加盟店	162
D-M	・決済サービスプロバイダ（PSP）のモジュール（プロトコル）型を使用するEC加盟店 ・カード情報をサーバやPCで保存するPOSや通信販売加盟店 ・カード情報をPOSシステムで通過、処理、保存する加盟店	・カード情報を自社のサーバで処理する加盟店 ・カード情報を電子形式で保存する加盟店 ・カード情報を電子形式で保存しないが他のSAQタイプの基準を満たさない加盟店 ・他のSAQタイプを満たす環境にあるが、自社の環境に他のPCI DSS要件が適用されるような加盟店	331
D-S	・カード発行のみ行うカード会社（イシュア） ・決済サービスプロバイダ（PSP）	ペイメントブランドに定義されたSAQを完成させる義務のある全てのサービスプロバイダ	366
P2PE	PCI P2PEソリューションを導入した主にPOS加盟店	PCI P2PEに認定されたソリューションを導入し、それらに含まれる決済端末のみでカード情報を処理する加盟店であり、カード情報を保存していない。	33

参考：「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　－２０１７－　【公表版】」　P54-55

自己問診表

PCI (Payment Card Industry)
データセキュリティ基準

サービスプロバイダ用自己問診
（Self-Assessment
Questionnaire）D および準拠証明書

SAQ 適用サービスプロバイダ
PCI DSS バージョン 3.2 用
2016 年 4 月

Payment Card Industry (PCI)
データセキュリティ基準

加盟店用自己問診（Self-Assessment
Questionnaire） D および準拠証明書

その他すべての SAQ 適用加盟店
PCI DSS バージョン 3.2 用
2016 年 4 月

SAQへの署名は担当役員

SAQ（自己問診票）は機械的に“Yes“を付けてはいけない

SAQの回答チェック

安全なネットワークとシステムの構築と維持

- *要件 1:　　カード会員データを保護するために、ファイアウォールをインストールして維持する*

PCI DSS 質問		必要なテスト	回答 (各質問に対して1 つ回答を選んでください)				
			はい	はい、CCW 付	いいえ	N/A	未テスト
1.1	確立され実装されたファイアウォールおよびルーター構成基準には、以下が含まれていますか？						
1.1.1	すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセスがありますか?	▪ 文書化されたプロセスのレビュー ▪ 担当者のインタビュー ▪ ネットワーク構成の調査	☐	☐	☐	☐	☐
1.1.2	(a) ワイヤレスネットワークを含め、カード会員データ環境と他のネットワークとの間のすべての接続を文書化した最新のネットワーク図はありますか?	▪ 最新のネットワーク図のレビュー ▪ ネットワーク構成の調査	☐	☐	☐	☐	☐
	(b) 図が最新に保たれていることを確認するプロセスがありますか?	▪ 責任者のインタビュー	☐	☐	☐	☐	☐
1.1.3	(a) システムとネットワーク内でのカード会員データのフローを示す最新の図がありますか?	▪ 最新のデータフロー図のレビュー ▪ ネットワーク構成の調査	☐	☐	☐	☐	☐
	(b) 図が最新に保たれていることを確認するプロセスがありますか?	▪ 担当者のインタビュー	☐	☐	☐	☐	☐

SAQの回答チェック

回答	説明
はい	必要なテストが実施され、要件の全要素が記載されているとおり満たされました。
はい、CCW 付 (代替コントロール ワークシート)	必要なテストが実施され、代替コントロールの助けを借りて要件が満たされた。 この欄の回答にはすべて、SAQ の付録 B の代替コントロールワークシート (CCW) への記入が必要です。 ワークシートの記入方法についての代替コントロールとガイダンスの使用に関する情報は、PCI DSS に記載されています。
いいえ	要件の要素の全部または一部が満たされていないか、導入中、あるいは確立したかを知るためにさらにテストが必要です。
N/A (該当なし)	この要件は会社の環境に該当しません（「特定の要件が適用されない場合」を参照）。 この欄に回答した場合はすべて、SAQ 付録 C の説明が必要です。
未テスト	この要件は評価の対象に含まれておらず、全くテストされていません。（このオプションを使用する場合の例は、下の「*該当なしと未テストの違いについて*」を参照してください。） この欄に回答した場合はすべて、SAQ 付録 D の説明が必要です。

※ **CCW＝代替コントロールワークシート（Compensating Control Worksheet）**

スコーピング（適用範囲）

スコーピング確認・確定

① 準拠の必要性有無を確認

■PCI DSS 要件は**アカウントデータ**（カード会員データや機密認証データ）が**保存、処理、または送信**される**組織**に適用されます。一部のPCI DSS 要件は支払業務やCDE 管理を**アウトソースしている組織**にも適用されます。
■機密認証データは承認後、たとえ暗号化していても保存してはなりません。

		データ要素	保存の許可	PCI DSS要件3.4に従って、保存されたアカウントデータを読み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	プライマリアカウント番号（PAN）	はい	はい
		カード会員名	はい	いいえ
		サービスコード	はい	いいえ
		有効期限	はい	いいえ
	機密認証データ	完全な磁気ストライプデータ	いいえ	要件3.2に従って保存できない
		CAV2/CVC2/CVV2/CID	いいえ	要件3.2に従って保存できない
		PIN/PINブロック	いいえ	要件3.2に従って保存できない

引用：要件およびセキュリティ評価手順「PCI DSS適用性情報」

スコーピング確認・確定

② 適用範囲(スコープ)の確認

PCI DSS セキュリティ要件は、カード会員データ環境に含まれる、または接続される**すべてのシステムコンポーネント**に適用されます。

■**カード会員データ環境（CDE）**は、カード会員データまたは機密認証データを**保存、処理、または送信する人、処理、およびテクノロジ**で構成されます。

■**「システムコンポーネント」**には、ネットワークデバイス、サーバ、コンピュータ、アプリケーションが含まれます。システムコンポーネントの例には、次のものが含まれますが、これらに限定されるわけではありません。

- セキュリティサービス（認証サーバなど）を提供する、セグメンテーションを促進する（内部ファイアウォールなど）、またはCDEのセキュリティに影響を及ぼす（名前解決やWeb リダイレクションなど）システム。
- 仮想マシン、仮想スイッチ/ルーター、仮想機器、仮想アプリケーション/デスクトップ、ハイパーバイザなどの仮想コンポーネント。
- ファイアウォール、スイッチ、ルーター、ワイヤレスアクセスポイント、ネットワーク機器、その他のセキュリティ機器を含むが、これらに限定されないネットワークコンポーネント。
- Web、アプリケーション、データベース、認証、メール、プロキシ、ネットワークタイムプロトコル（NTP）、ドメインネームサーバ（DNS）などを含むが、これらに限定されないサーバタイプ。
- 内部および外部（インターネットなど）アプリケーションを含む、すべての市販およびカスタムアプリケーション。
- CDE 内にあるかCDE に接続されているその他のコンポーネントまたはデバイス

引用:要件およびセキュリティ評価手順「PCI DSS要件の適用範囲」

スコーピング確認・確定

③ 適用範囲(スコープ)の確認

■PCI DSS 評価の最初の手順は、レビューの範囲を正確に決定することです。少なくとも年に一度、毎年の評価前に、評価対象の事業体は**カード会員データの場所とフローをすべて識別**し、さらにすべての**接続されている**、または（例えば、認証サーバなどの）**侵害された場合 CDE に影響を与える可能性のあるシステム**を識別し、それらがPCI DSS の範囲に含まれていることを確認することによって、PCI DSS の範囲の正確性を確認する必要があります。

■CDEの定義の正確性と適用性を確認するには、以下を実行します。

- 評価対象の事業体は環境内に存在するすべてのカード会員データを識別および文書化して、現在定義されているCDEの外部にカード会員データが存在していないことを確認します。
- カード会員データのすべての場所を識別および文書化したら、事業体はその結果を使用してPCI DSSの範囲が適切であることを確認します（例えば、結果はカード会員データの場所を表す図やインベントリである場合があります）。
- 事業体は、見つかったすべてのカード会員データをPCI DSS評価範囲内にあり、CDEの一部であるものと見なします。事業体が現在CDEに含まれていないデータを見つけた場合、そのようなデータは完全に削除するか、現在定義されているCDEに移行するか、このデータを含むようにCDEを再定義する必要があります。
- 事業体はPCI DSSの範囲がどのように決められたかを示す文書を保持します。この文書は、評価担当者のレビューのためか、翌年のPCI SCCの範囲確認作業で参照するために保持されます。

引用：要件およびセキュリティ評価手順「PCI DSS要件の適用範囲」

スコープ定義の手順

① 準拠の必要性確認

当該システムでは、PANが伝送・処理・保管されていますか？

→

伝送・処理・保管、いずれかを行っていればPCI DSS準拠の必要があります
（PCI DSSの対象です）

PANを全て外部委託先に預ける

PANを取り扱わない

② 直接対象となる範囲の確認

PANが伝送・処理・保管されているシステムコンポーネントはどれですか？

→

あてはまるシステムコンポーネントはすべて対象です

対象システムを外部サービスに切り替える

③ 間接的に対象となる範囲の確認

（PANを伝送・処理・保管していなくても）そこに直接接続（フラットネットワーク）しているシステムコンポーネントはどれですか？

→

そのシステムコンポーネントも、すべて対象です

接続するシステムを限定、分離（セグメンテーション）

セグメンテーションとは

ネットワークセグメンテーションとその効果

■カード会員データ環境のネットワークセグメンテーション、またはカード会員データ環境の残りの事業体ネットワークからの隔離（セグメント化）は、PCI DSS 要件ではありません。ただし、ネットワークセグメンテーションは以下を引き下げる方法として強く推奨されます。

- PCI DSS 評価の対象範囲
- PCI DSS 評価のコスト
- PCI DSS コントロールの実装と維持に関するコストおよび難易度
- 組織のリスク（カード会員データをコントロールが強化された少数の場所に統合することで、低減します）

引用：要件およびセキュリティ評価手順 p.13「ネットワークセグメンテーション」

適用範囲を極小化することにより・・・
□ネットワークセグメンテーションにより、スコープを縮小できる
□スコープ縮小により、対応コストおよび審査コストを抑えられる
□カード会員データが漏えいするリスクも低減できる

では、ネットワークセグメンテーションはどう行うのか？

ネットワークセグメンテーションの方法（１／４）

■ネットワークセグメンテーションが適切に設定されていない場合（「フラットネットワーク」とも呼ばれます）、ネットワーク全体が PCI DSS 評価の対象範囲になります。**ネットワークセグメンテーションは、適切に構成された内部ネットワークファイアウォール、ネットワークの特定セグメントへのアクセスを制限する強力なアクセス制御リストまたは他のテクノロジを持つルーターなどのいくつかの物理的または論理的手段を通じて実現できます。**PCI DSS の範囲外と見なされるシステムコンポーネントは、範囲外のシステムコンポーネントが侵害された場合にもCDE のセキュリティに影響しないようにCDE から適切に分離（セグメンテーション）する必要があります。

引用：要件およびセキュリティ評価手順「ネットワークセグメンテーション」

□「強力なアクセス制御リスト」によってネットワークを分割することを「ネットワークセグメンテーション」と呼ぶ

※ネットワークセグメンテーションとは、ブロードキャストドメインの分割ではない
（一般的なネットワーク用語とは異なる）

ネットワークセグメンテーションの方法（２／４）

■カード会員データ環境の範囲を狭めるための重要な前提条件は、**カード会員データの保存、処理または伝送に関するビジネスニーズおよびプロセスを明確にする**ことです。不必要なデータの削除および必要なデータの統合により、**カード会員データをできるだけ少ない場所に制限する**には、長期にわたるビジネスプラクティスのリエンジニアリングが必要になる可能性があります。

引用：要件およびセキュリティ評価手順「ネットワークセグメンテーション」

□まずは「そのカード会員データが必要か？」を調査する
□必要ないことが分かった場合、持たない
□どうしても必要なら、一か所に集めて強力なアクセス制御リストでネットワークを分割し、孤立させる
□このような変更には、業務フローやシステム構成の大幅な変更を伴う可能性が高い

ネットワークセグメンテーションの方法（３／４）

■データフロー図を使用してカード会員データフローを文書化することによって、すべてのカード会員データフローを把握し、すべてのネットワークセグメンテーションがカード会員データ環境を効果的に隔離していることを確認できます。

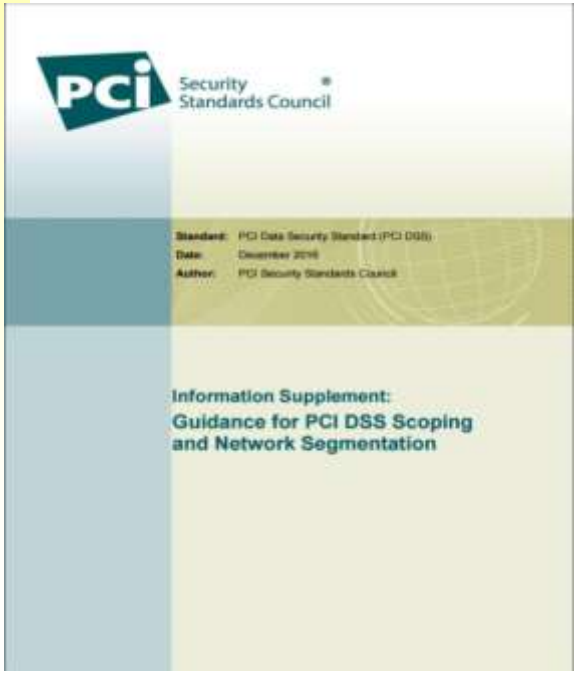
引用：要件およびセキュリティ評価手順「ネットワークセグメンテーション」

□「データフロー図」を作成し、カード会員データをどの部分に孤立させているか、適切なアクセス制御が行われているかを確認する
□「データフロー図」は、ネットワーク構成図にカード会員データのフローと保管、処理を行う箇所、アクセス制御の方法を書き込む

ネットワークセグメンテーションの方法（４／４）

■ネットワークセグメンテーションが設定されていて、PCI DSS 評価範囲の縮小に使用されている場合、評価担当者はネットワークセグメンテーションが評価範囲の縮小に適していることを確認する必要があります。ネットワークを適切にセグメント化することによって、カード会員データを保存、処理、伝送するシステムはそれ以外のシステムから高いレベルで隔離されます。ただし、**ネットワークセグメンテーションの特定の実装が適切であるかどうかは、特定ネットワークの構成、導入されているテクノロジ、および実装されている他のコントロールによって大きく左右されます。**

引用：要件およびセキュリティ評価手順「ネットワークセグメンテーション」



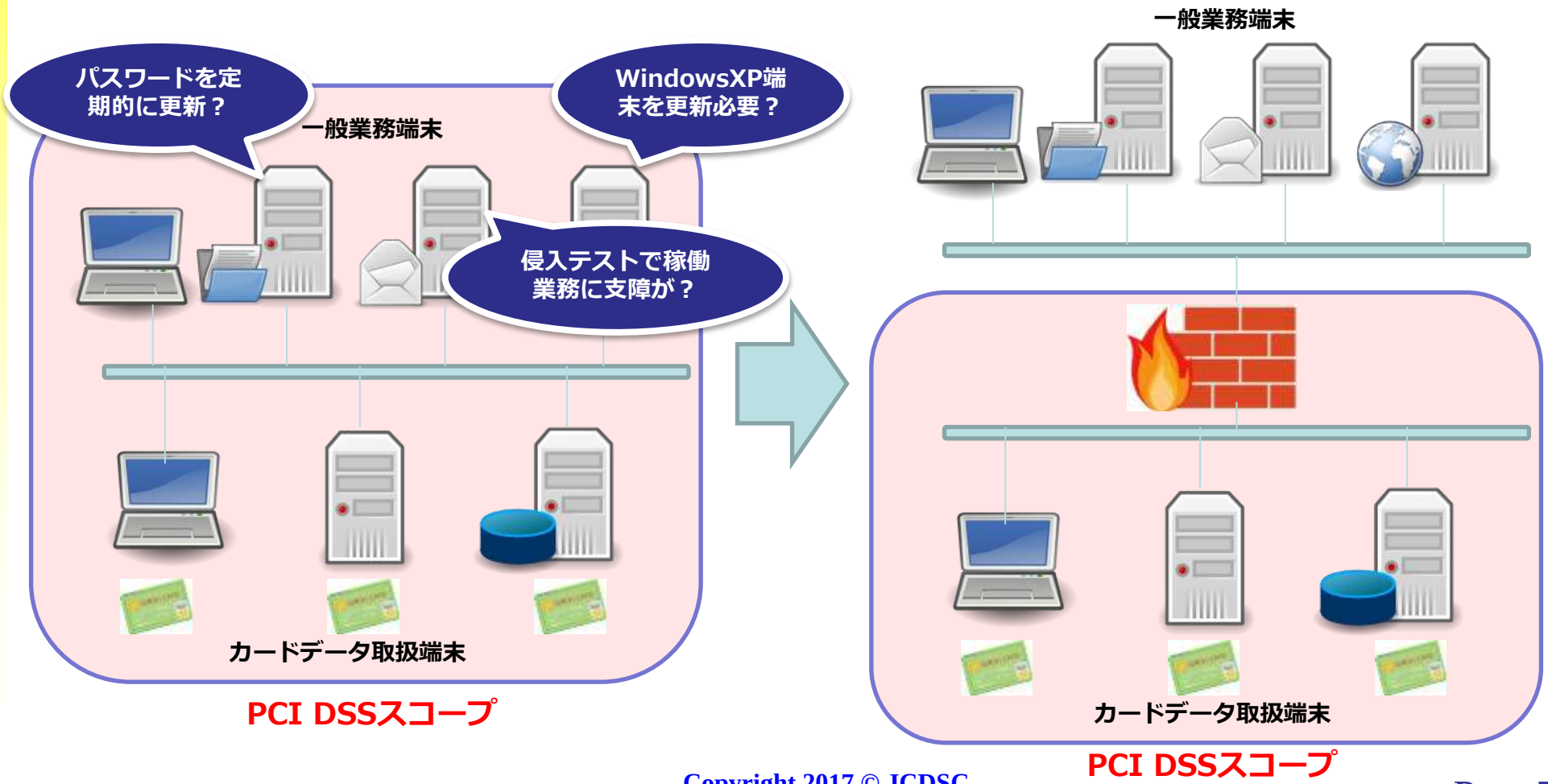
参考資料
Information Supplement:
Guidance for PCI DSS Scoping
and Network Segmentation
（December 2016）

PCI DSSスコーピングとネットワークセグメンテーションに関わるガイダンス

ネットワークセグメンテーション（スコープの極小化）

◆ スコープ軽減にはネットワーク分離が有効

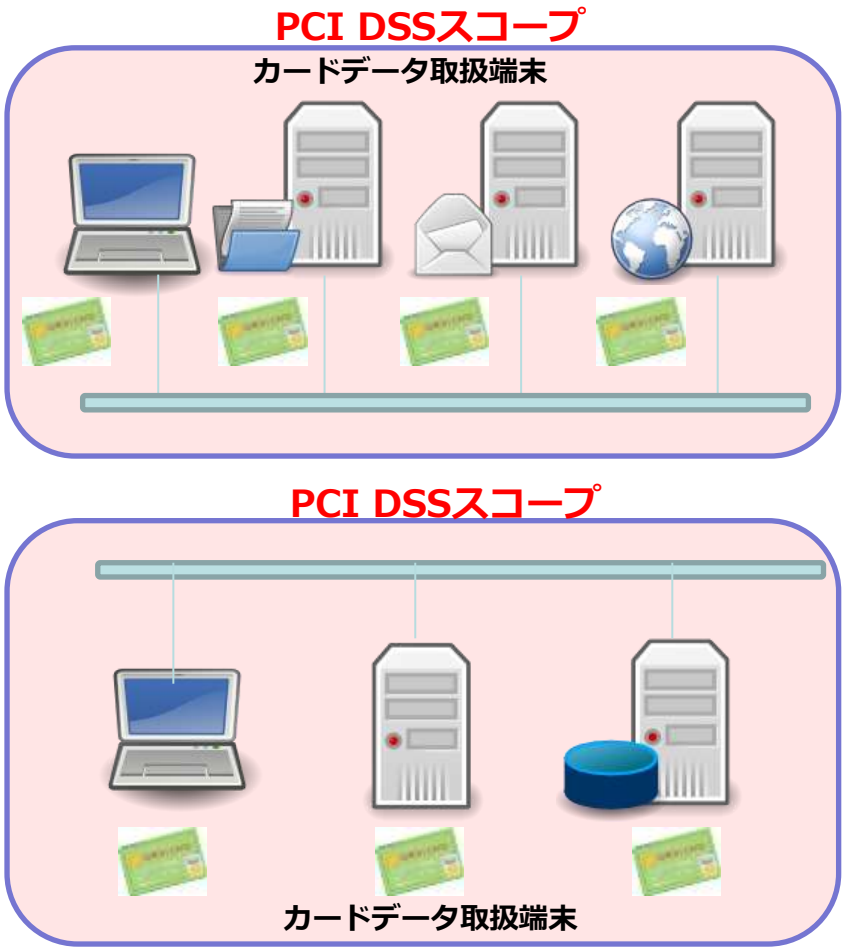
カードデータ環境に“接続可能”な端末にもPCI DSS要件が適用されてしまう



ネットワークセグメンテーション

◆ スコープのネットワークは集約する

カードデータを保有するネットワークを極力まとめる事で対応負荷は軽減される



主な関連要件：要件11.3（11.3.4, 11.3.4.1）

SAQ:付録B　代替コントロール①

- 事業体が正当な技術上の制約または文書化されたビジネス上の制約のために記載されているとおりに明示的に要件を満たすことができないが、その他の（つまり代替の）コントロールを通じて要件に関連するリスクを十分に軽減している場合、ほとんどの PCI DSS 要件に対して代替コントロールを検討することができます。

SAQ:付録B　代替コントロール②

- 代替コントロールは、以下の条件を満たす必要がある。
  1. 元の PCI DSS 要件の目的および厳密さを満たす。
  2. 元の PCI DSS 要件で防御の対象とされているリスクを代替コントロールが十分に相殺するよう、元の PCIDSS 要件と同様のレベルの防御を提供する。（各 PCI DSS 要件の目的については、「PCI DSSナビゲート」を参照。）
  3. その他の PCI DSS 要件 “以上” のことを実現する。（単なるその他のPCI DSS 要件への準拠は代替コントロールになりません。）
  4. PCI DSS 要件に従わないことによって課せられるその他のリスクを考慮する。

- 代替コントロールはすべて、***PCI DSS*** レビューを実施する評価者によって、その十分性がレビューおよび検証される必要がある。

6. ISAについて

実行計画2017（2017/3/8公表）

3．カード情報を保持する加盟店の PCI DSS 準拠の推進について

（1）PCI DSS に関する認知度の向上及び準拠への取組促進に向けた情報提供

本協議会は JCDSC 等の協力を得て、クレジットカード取引に関係する各事業者の PCI DSS 準拠への取組促進のため、PCI DSS に関するセミナーの開催等の周知・啓発活動を行う。

（2）PCI DSS 準拠に向けた加盟店等へのサポート体制について

JCDSC 等は本協議会と協力して、カード情報を保持する加盟店等が PCI DSS 準拠に向けた対応を円滑に図ることをサポートするため以下の対応に取組むこととする。

⑤専門人材の育成

・PCI DSS 準拠に取組む加盟店等へのサポートニーズの拡大に対応するため、QSA の人員体制の整備・拡充を図る。

・PCI DSS 準拠に関し、QSA による審査に代替し得る内部監査を行うことのできる専門人材として、**ISA**[8]（Internal Security Assessor）等の人材育成を支援する。

引用：「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　－２０１７－　【詳細版】」　P17-18

PCI ISAとは

Internal Security Assessor（ISA）とはPCI SSC認定の資格であり、QSAと共に自社のPCI DSS準拠をサポート可能な専門的な知識を持った内部監査評価）人です。

引用：
https://ja.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_certification

JCDSC
Japan Card Data Security Consortium

2017 ISA Training Schedule

Be a PCI champion for your organization

The Internal Security Assessor (ISA) Program trains, tests, and qualifies organizations and individuals to assess and validate their company's adherence to PCI Security Standards.

2017 ISA Training Schedule:

Upcoming Classes	
7-8 or 9-10 September	Orlando, FL
19-20 October	Barcelona, Spain
6-7 November	Washington, DC
6-7 November	Melbourne, Australia
15-16 November	Tokyo, Japan *(simultaneous translation in Japanese)*

https://training.pcisecuritystandards.org/isa-ilt-training-2017-training-schedule

Please complete the form below to request more information. All fields required.

First name* Last name*

Company Name*

Please complete this mandatory field.

Country*

内部監査人（ISA)を持つメリット

オンサイト監査免責（*対象組織の場合）以外には、QSAと同等の知見を持つISAを自組織に持つ事により、PCI DSSの組織浸透を効率的に進める事が期待されます。

“Business as Usual”実践への近道

監査のためのPCI DSSではなく、組織の末端までPCI DSSが浸透する事が企業を守る

QSAとの連携による監査/コンサル負荷の軽減

QSAとの連携によりISAが監査前準備を効果的に行う事により、QSAの監査負荷を軽減する

PCI DSS新仕様情報の早期入手

PCISSCの監査改訂/監査ポイントに関する最新情報を早期に入手する事で、自組織の新仕様対応を余裕を持って進める

最後に

日本が世界の“セキュリティホール“になってきた!

全国のコンビニATMから、偽造クレジットカードで約20億円の不正引き出し被害発生。

出し子100人以上を動員した、大規模組織犯罪。(2016.5.24)

・米国は大統領令でICカード化を急速に推進。

・国際犯罪組織は、犯行が困難な欧米を回避して、日本をターゲットにする傾向にある。

①南アフリカの銀行で漏えい

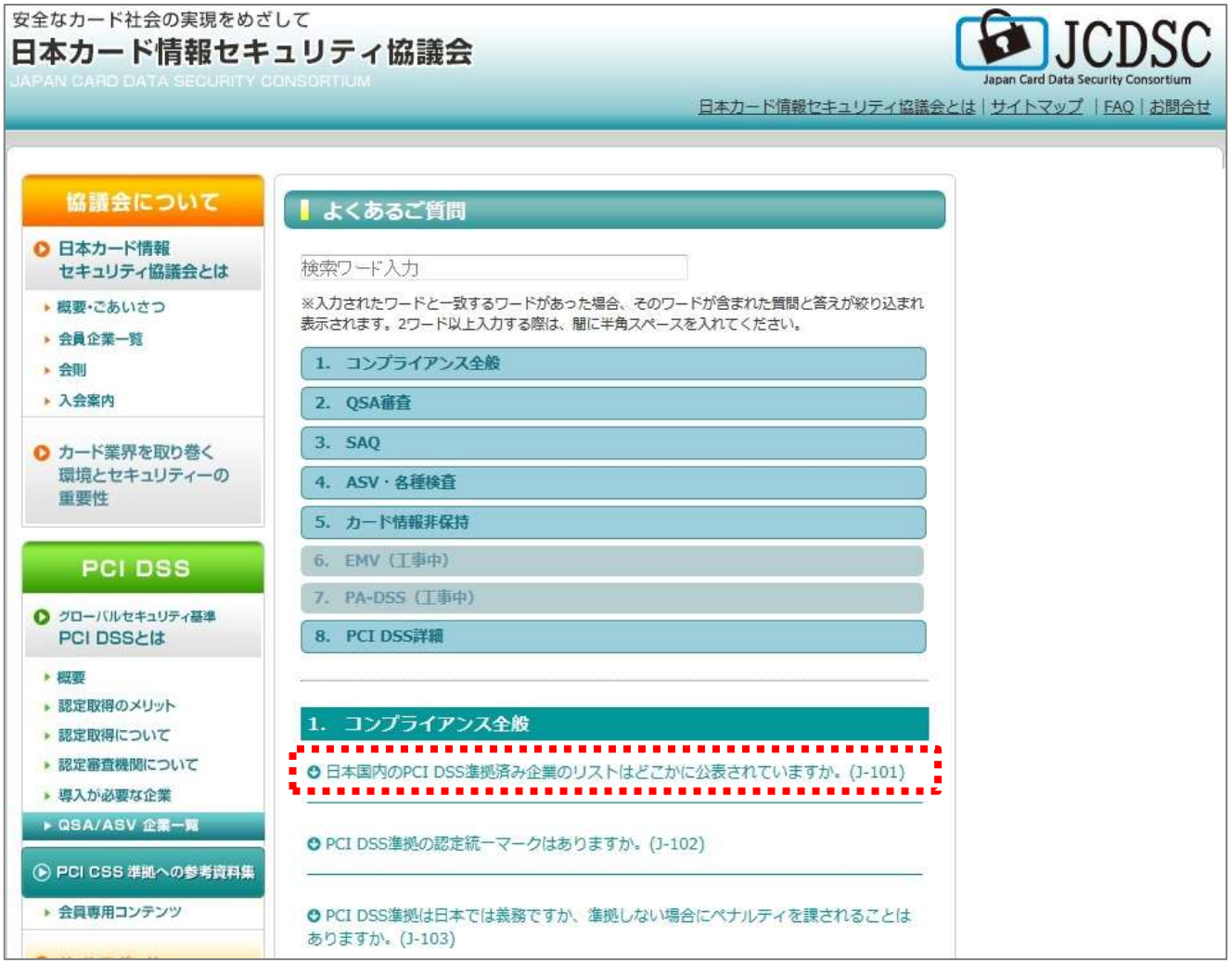
②中国系焼き肉店の磁気カード

③日本のATMが被害に

イラストの出典:PCISSC / Educational Resources

PCI DSSに関するよくある質問（JCDSC)

JCDSCサイト http://www.jcdsc.org/faq.php　にPCI DSSに関するよくある質問と回答が掲載されています。



ご清聴ありがとうございました

安全なカード社会の実現をめざして
日本カード情報セキュリティ協議会
JAPAN CARD DATA SECURITY CONSORTIUM