PCI DSSセキュリティフォーラム　2013

「QSA監査のポイントと新バージョン3.0」

2013年7月10日

日本カード情報セキュリティ協議会
運営委員長　武藤　敏弘
（BSIグループジャパン株式会社）

PCI Security Standards Council

BSIグループとは？

Who we are.

- 【沿革】
- 1901年：英国の貿易産業省の支援を受けて設立。世界最古の国家規格協会
- 1929年：英国王室より
  英国王室憲章授与
- 1979年：品質ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ規格BS5750の発行
- 1999年：BSIジャパン株式会社 設立

本日の内容は
BSIの解釈です。

- 【BSIが開発した主な規格】
- 1979年 BS 5750 -> ISO 9001
- 1992年 BS 7750 -> ISO 14001
- 1995年 BS 7799 -> ISO/IEC 27001
- 1996年 BS 8800 -> OHSAS 18001
- 1999年 BS 8600 -> ISO 10002
- 2002年 BS 15000 -> ISO/IEC 20000
- 2003年 PAS 56 -> BS 25999 – 1
- 2006年 BS 25999-1 -> ISO 22313
- 2007年 BS 25999-2 -> ISO 22301
- 2007年 BS 8901 -> ISO 20121
- 2008年 PAS 2050 -> ISO 14067
- PAS220 -> ISO/TS 22002-1
- 2009年 BS EN 16001 -> ISO 50001
- 2010年 PAS2060
- 2011年 PAS223 PAS222

「日本におけるクレジットカード情報管理強化に向けた実行計画」

日本におけるクレジットカード情報管理　スキーム

対　象	形　態	基　準 決済代行業者／加盟店の場合⇒年間カード売上件数 カード会社の場合　⇒　発行枚数	レベル		PCI DSS準拠対応	PCI DSS検証方法
決済代行業者	形態問わず全て	全て	I	①	ＰＣＩＤＳＳ準拠	オンサイトレビュー ネットワークスキャ
加盟店	非対面／ネット	４ブランドにより決※3)	A	②	センシティブ認証情報（※２）非保持	
				③	ＰＣＩＤＳＳ準拠	
	対面／ＰＯＳ			④	センシティブ認証情報（※２）非保持	
				⑤	ＰＣＩＤＳＳ準拠	
	非対面／ネット	レベルＡ以外	B	⑥	センシティブ認証情報（※２）非保持	自己問診 ネットワークスキャ
				⑦	ＰＣＩＤＳＳ準拠またはクレジットカード情報非保持	
	対面／ＰＯＳ	１００万件以上、レベルＡ以※4)		⑧	センシティブ認証情報（※２）非保持	
				⑨	ＰＣＩＤＳＳ準拠またはクレジットカード情報非保持	
	対面／ＰＯＳ	１００万件未満※5)	C	⑩	ＰＣＩＤＳＳ準拠またはクレジットカード情報非保持（※１）	
	対面／スタンドアローン	全て	I	⑪	クレジットカード情報非保持（※１）	
クレジットカード会社	ＡＣＱまたはプロセッシング	全て	A	⑫	PCIDSS準拠	オンサイトレビュー ネットワークスキャ
	イシュイングのみ	１００万件以上	B	⑬	PCIDSS準拠	自己問診 ネットワークスキャ
		１００万件未満	C	⑭	他社クレジットカード情報非保持（※１）	

対応期限　（年度単位⇒2017年＝2018年3月まで）

2010 Q3 Q4 / 2011 Q1 Q2 Q3 Q4 / 2012 Q1 Q2 Q3 Q4 / 2013 / 2014 / 2015 / 2016 / 2017

インフラ整備部会における検討期間

日本クレジット協会HPにて2012年5月31日公開

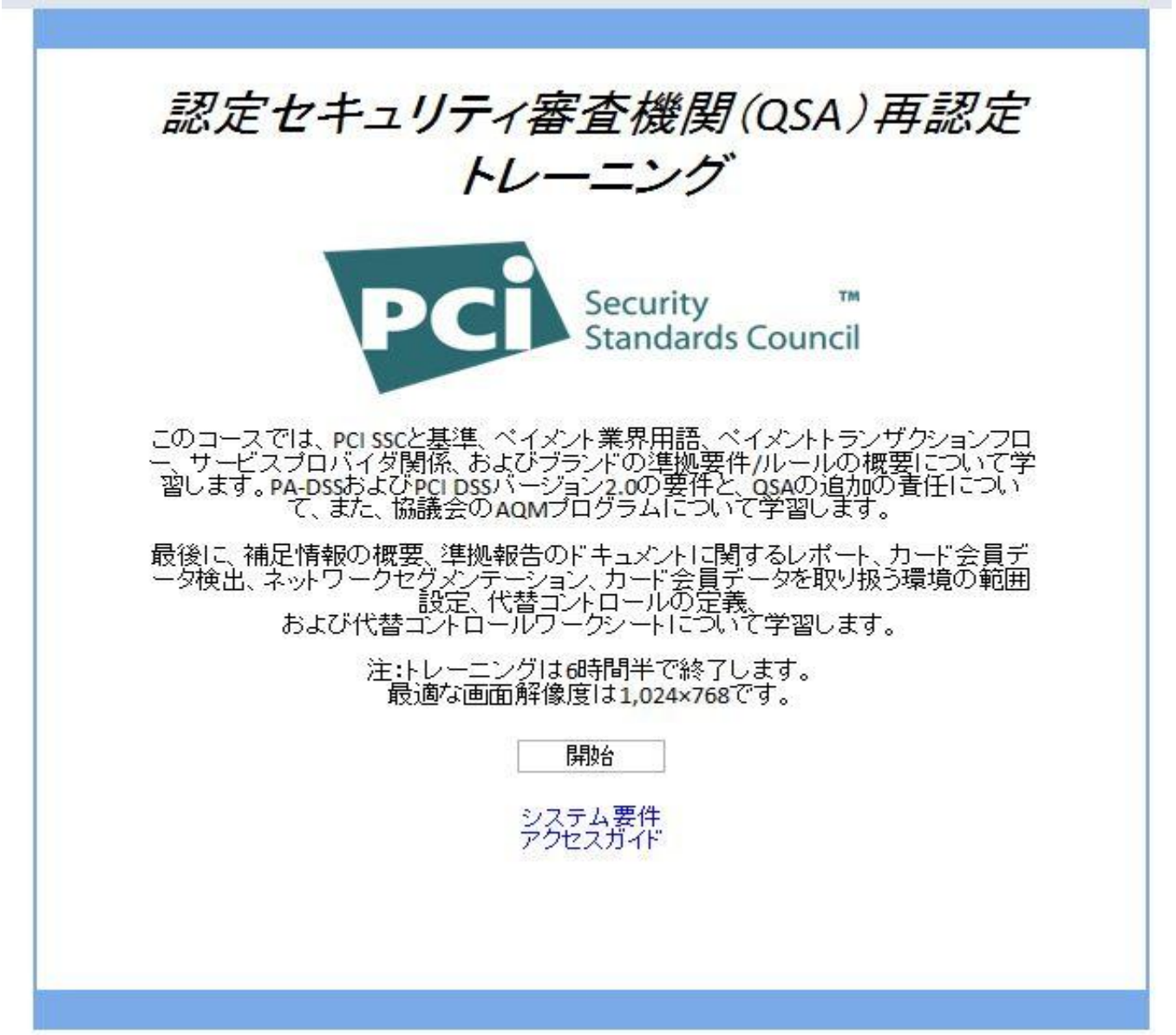
出典：日本クレジット協会　HPより＊ http://www.j-credit.or.jp/download/120530_news.pdf

PCI DSSの動きは？

クレジットカード環境の変化

- 利用機会の増加
- メインカード
- 支払い方法の変更
- オンラインショップの増加
- Vプリカ

QSAは、毎年、再認定トレーニングを受け、試験に合格しなければなりません。



PCI DSS（Payment Card Industry Data Security Standards）の目的とは？

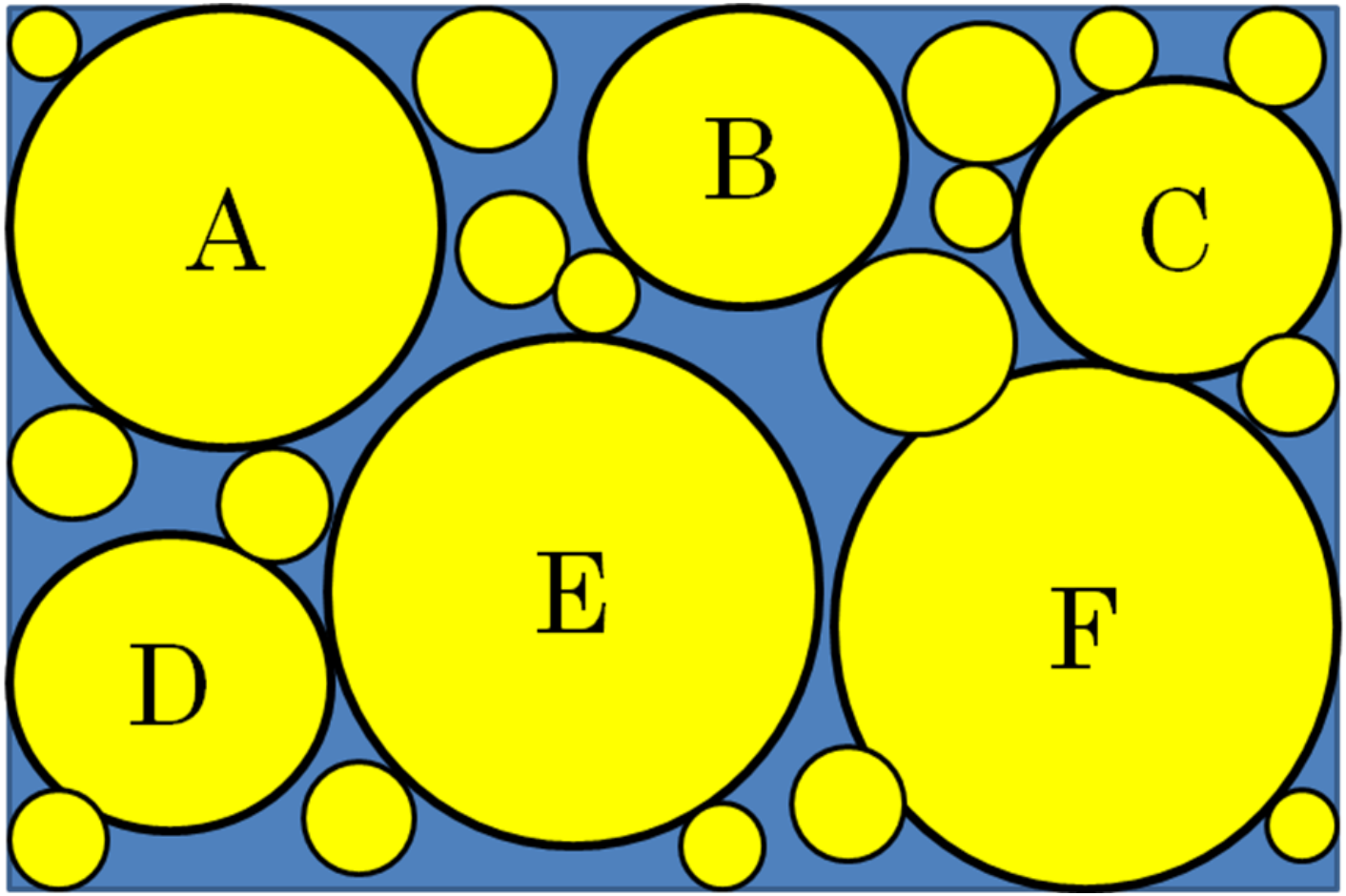
PCI DSSの主な目的はカード情報の適切な保護

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。

「リスクの度合い」に応じたコントロール

リスクの考え方

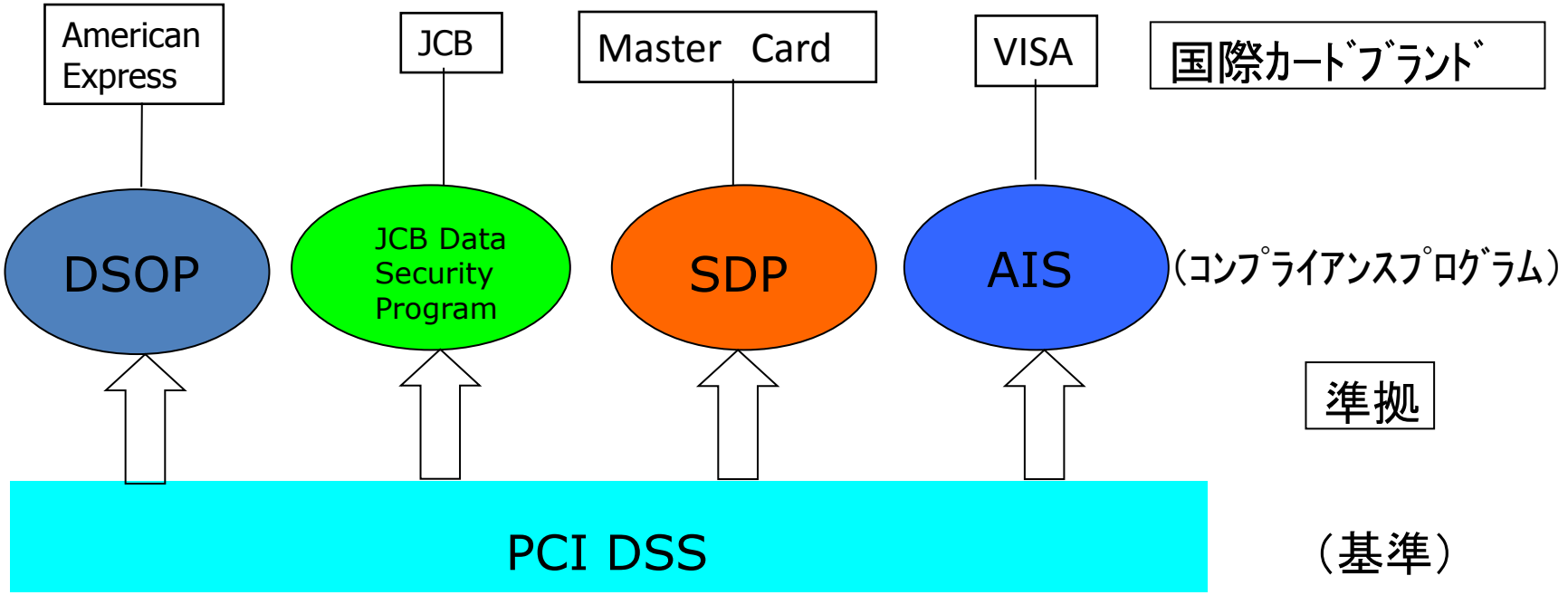
頻度の高い・影響の大きいリスクをコントロールすれば
全体の80%以上を管理できる



PIC DSSの対象カードデータ

		データ要素	保管可能	保護の必要性
アカウントデータ	カード会員データ	カード番号(PAN)	YES	YES
		カード会員名[1]	YES	YES
		サービス コード[1]	YES	YES
		有効期限[1]	YES	YES
	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
		CAV2/CVC2/CVV2/CID	NO	N/A
		暗証番号(PIN) / PINブロック	NO	N/A

各ブランドのコンプライアンス・プログラムとの関連



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

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

カード情報のシステム・リスクを軽減する

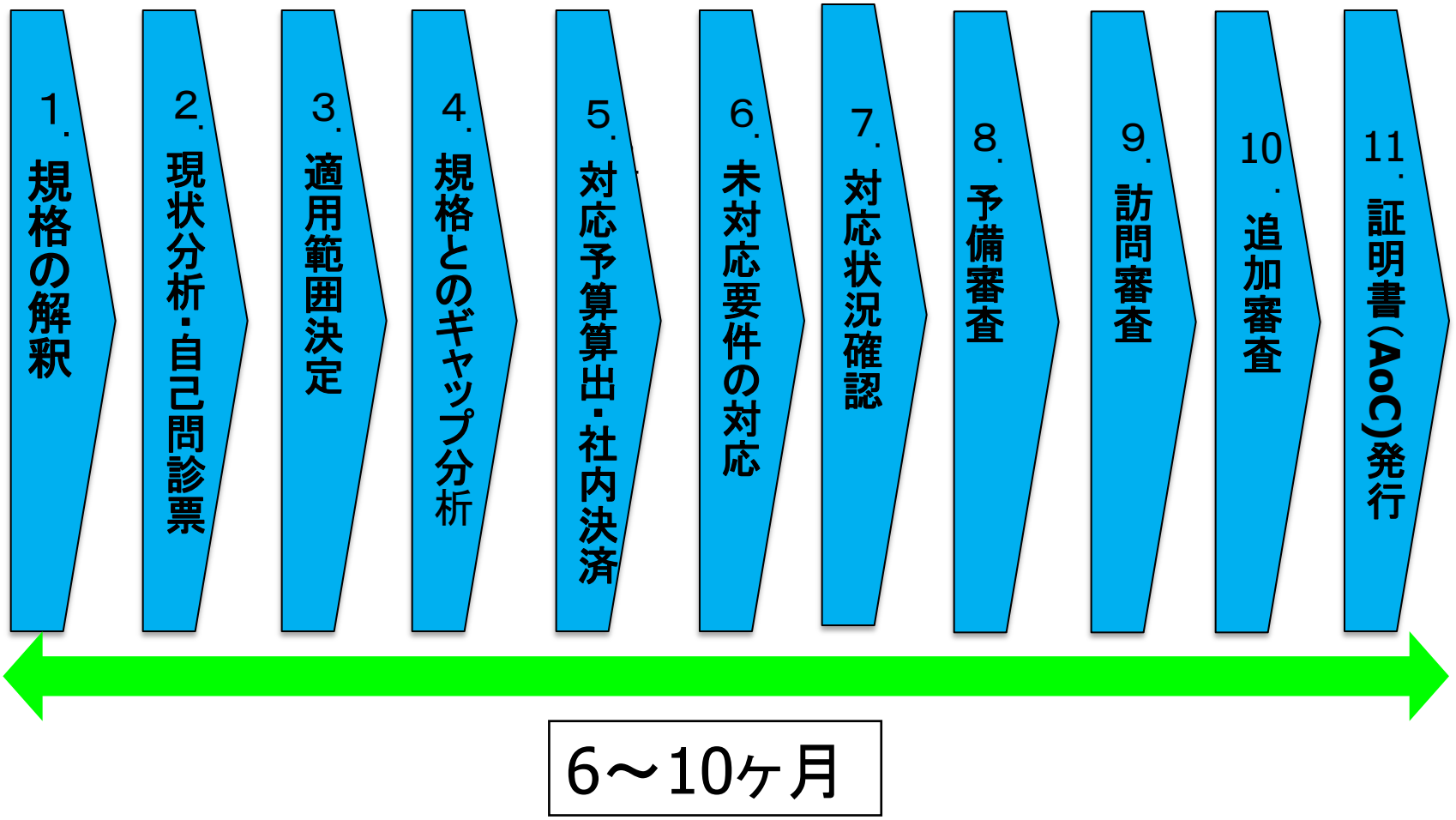
1. クレジットカード会員データを持たない。

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・維持負担軽減

PCI DSS完全準拠への一般的な流れ



コンサルは必要？

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 基準よりバージョン2.0より抜粋）

伝送、処理、保管のいずれかの環境は全て対象

代替コントロール

- 事業体が正当な技術的または文書化されたビジネス上の制約によって、規定どおりに要件を満たすことができず、代替コントロールの実装によって要件に関連したリスクを軽減している場合、大抵のPCI DSS要件で代替コントロールを考慮できます。

- 準拠を維持するには、プロセスおよびコントロールを設置して、評価が完了した後も代替コントロールが効果を発揮することを保証する必要があります。

- 評価機関は、毎年のPCI DSS評価で代替コントロールを詳細に評価する必要があります。

（PCI DSS 基準よりバージョン2.0より抜粋）

オリジナルの要件と同等、あるいはそれ以上のコントロール

基準の利用法①　「データセキュリティ基準　要件とセキュリティ評価手順」

PCI Security Standards Council

ベストプラクティス

強固なアクセス制御手法の導入

要件 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

権限を与えられた担当者のみが重要なデータにアクセスできるように、システムおよびプロセスでは、職責に応じて必要な範囲にアクセスを制限する必要があります。

「必要な範囲」とは、アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与されることを示します。

PCI DSS 要件	テスト手順	対応	非対応	目標期日/コメント
7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下の項目を含める必要がある。	7.1 データ管理に関する文書化されたポリシーを入手して検討し、ポリシーに以下が含まれていることを確認する。			
7.1.1 特権ユーザ ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されている	7.1.1 特権ユーザ ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されていることを確認する。			
7.1.2 特権の付与は、個人の職種と職能に基づく	7.1.2 特権の付与が、個人の職種と職能に基づいていることを確認する（「役割ベースのアクセス制御」（RBAC）とも呼ばれる）。			
7.1.3 権限を持つ関係者による、必須権限を指定する文書化された承認が要求される。	7.1.3 すべてのアクセスに対して、権限を持つ関係者による、必須権限を指定する文書化された承認が要求されることを確認する。			
7.1.4 自動アクセス制御システムを実装する	7.1.4 自動アクセス制御システムによるアクセス制御が実装されていることを確認する。			

【要件】
　対応すべき 内容

【テスト手順】
　QSAの確認手順

基準の利用法②　「PCI DSS ナビゲート　基準要件の目的の理解」

PCI Security Standards Council

要件 7、8、9 のガイダンス: 強固なアクセス制御手法の導入

要件 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

権限を与えられた担当者のみが重要なデータにアクセスできるように、システムおよびプロセスでは、職責に応じて必要な範囲にアクセスを制限する必要があります。「必要な範囲」とは、アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与されることを示します。

要件	ガイダンス
7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下の項目を含める必要がある。 **7.1.1** 特権ユーザ ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されている **7.1.2** 特権の付与は、個人の職種と職能に基づく **7.1.3** 権限を持つ関係者による、必須権限を指定する文書化された承認が要求される。 **7.1.4** 自動アクセス制御システムを実装する	カード会員データにアクセスする人が増えるほど、ユーザのアカウントが不正に使用されるリスクが高まります。アクセスを、業務上必要とする強い理由がある人に限定すると、組織での経験不足や悪意によるカード会員データの不適切な処理を防ぐことができます。アクセス権が職務の実行に必要な最小限のデータ量および特権にのみ付与される場合、これは「最小限の特権」および「必要な範囲」と呼ばれます。特権が職種と職能に基づいて個人に付与される場合、これは「役割ベースのアクセス制御」（RBAC）と呼ばれます。役割ベースのアクセス制御の実施は、アプリケーション層または特定の承認ソリューションに限定されません。たとえば、Active Directory または LDAP、アクセス制御リスト（ACL）、TACACS などのディレクトリサービスを含むテクノロジは、適切に構成され、「最小限の特権」と「必要な範囲」の原則に従っている限り、有望なソリューションです。 組織では、必要な範囲に基づいたデータアクセス制御のための明確なポリシーとプロセスを作成し、役割ベースのアクセス制御を使用して、適切な管理者承認プロセスを含めたアクセスの付与方法および付与対象を定義する必要があります。
7.2 複数のユーザが使用するシステムコンポーネントで、ユーザが必要とする範囲に基づいてアクセスが制限され、明示的に許可のない限り「すべてを拒否」に設定された、アクセス制御システムを確立する。 アクセス制御システムには以下の項目を含める必要がある。 **7.2.1** すべてのシステムコンポーネントを対象に含む **7.2.2** 職種と職能に基づく、個人への特権の付与 **7.2.3** デフォルトでは「すべてを拒否」の設定	ユーザが必要とする範囲に基づいてアクセスを制限するメカニズムがないと、ユーザは知らないうちにカード会員データへのアクセスを付与される場合があります。複数のユーザを管理するには、自動化されたアクセス制御システムまたはメカニズムの使用が不可欠です。このシステムは、組織のアクセス制御ポリシーおよびプロセス（「必要な範囲」と「役割ベースのアクセス制御」を含む）に従って確立され、すべてのシステムコンポーネントへのアクセスを管理し、このようなアクセスを明確に付与するルールが確立されない限り誰にもアクセスが付与されないよう、デフォルトの設定が「すべて拒否」になっている必要があります。

「狙い」「目的」「チェックすべき事象」は、何か？
適切な解釈とは？
前提の対象OSは？

QSAによる訪問監査

審査日数　4.0～5.0日前後（過去の平均）＋　ﾚﾎﾟｰﾃｨﾝｸﾞ3日
（オンサイト）　（オフサイト）

＊インターネット接続の有無、ｻｰﾊﾞｰの台数、
拠点数、システムの規模・複雑さにより増減。

＊予備調査（推奨）
システム構成、適用範囲、準備状況の確認

＊実機上で審査をする。

PCI　DSS準訪問監査(オンサイトレビュー)

オープニング　ミーティング

業務概要の理解、レビュー対象範囲の特定

インタビューと文書レビュー

サイト訪問／設定内容確認

クロージング　ミーティング

報告書、証明書発行

PCI　DSS準拠マーク

成果物：準拠証明書（AoC)、準拠レポート（RoC)、認証証

FAQ

1. 審査は受けなければいけないの？
2. 毎年審査を受けるの？
3. 審査費用っていくらかかるの？
4. 構築までいくらかかるの？
5. 準拠の維持にはいくらかかるの？
6. 審査員の判断基準って？

効率的な構築・運用

1. 既存の仕組み・ルールの最大限の活用

2. 規格の理解（共通言語）

3. クラウド等各種サービスの利用

4. 部分準拠（パーシャル準拠）

PCI DSS
バージョン3.0!

バージョン3．0概要（予想）①

「準拠している」にもかかわらずカード情報
が流出した、という事例がある。
それらの事故を分析した結果、基準の曖昧さから
きちんと対策されていなかったことが多く見られた。

８月のPCI SSC エクゼクティブコミッティーで決定。

バージョン3．0概要（予想）②

1．センシティブデータのみでPANを持っていない組織。 → PCI DSS対象？
2．アウトソース先のPCI DSS準拠対応を明確化。
3．アンチマルウェアを止められないようにする。
4．パスワードのフレキシビリティをインクリース
5．ベンダーデフォルトチェンジ、デフォルトアカウント、パスワードに限定せずリスクのあるものへの対応。
6．ログの効果的な利用。ログレビューの精度を上げる。
フレキシビリティー

7．要件6.6 WAF以外にも同様の技術での利用。
8．要件11.5 アラートの対応まで確認。

2013 PCI SSC Community Meeting

性弱説

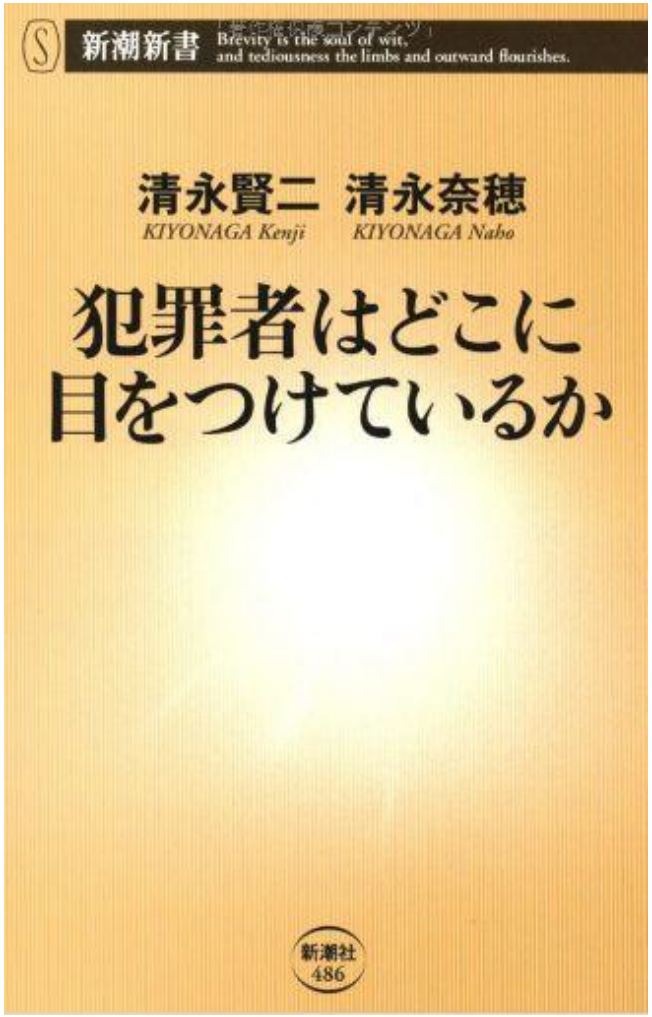
情報を売ることのメリットは無い。

- 性善説？性悪説？

- 人はおかれた状況で変わる可能性がある
  ＊病気、リストラ、減給、家族の入院、
  家族の死・・・

教育を繰り返す。認識を植え付ける。
その気にさせない環境づくり。

犯罪者はどこに目をつけているか



著者:
清水賢二
東京学芸大学大学院修了。
警察庁犯罪予防研究室室長を経て、日本女子大学教授。現在、ステップ総合研究所特別顧問。

清水奈穂
立教大学大学院修了。科学技術振興機構（JST）研究員など。現在、ステップ総合研究所代表

忍びの弥三郎（のびのやさぶろう）
猿の義ちゃん（ましらのぎちゃん）

自らを「賊」と称し、警察も含め周囲から「最後の賊」と呼ばれた。犯罪者の中でも天才的と評された。

対策への誤解・過信　→　リスクに対する適切な対応

リスクに対する対策が適切であり充分かの検証を継続して実施する

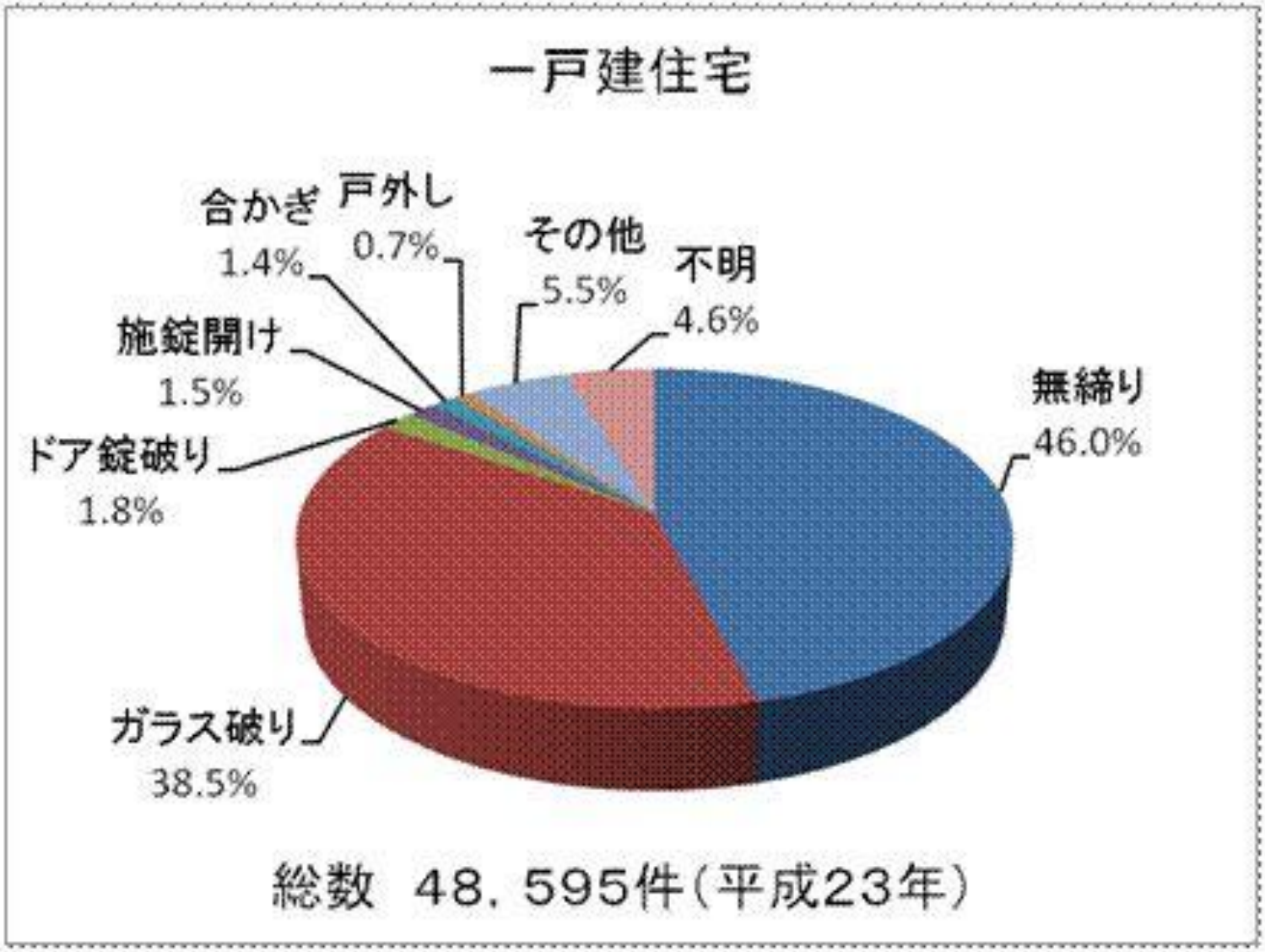
クレセント錠

ディスクシリンダー

防犯対策ではない！

侵入窃盗の侵入手段

システム、重要な情報に鍵をかけていますか。



出典：警察庁　住まいる110番 http://www.npa.go.jp/safetylife/seianki26/theme_a/a_d_1.html

日本国内どこへでも参ります。

ご清聴ありがとうございました。

日本カード情報セキュリティ協議会
http://www.jcdsc.org/