06) 本部セッション

PCIDSS導入義務のウソとホント

●本当にPCIDSSに準拠しなければいけないのか。同業他社は現在どれくらい準拠済みなのか。カード情報を持たなければ、PCIDSSに準拠する必要はない？等々、国が定めた法令ではないせいか、加盟店からするとどうも判然としない点が多々あります。
●JCDSC運営委員会を構成する各社合同で、PCISSC(国際評議会)や、カードブランド、アクワイアラ、担当行政機関等からの情報に基づき、総合的に分析・解説します。

2015年7月28日(火)
JCDSC運営委員会

■1.日本国内のPCIDSS浸透状況は？

JCDSC

①PCIDSS訪問審査の必要な企業数と、認証済み企業数は

②認証取得企業名の公表サイトは

③広く公表されているサイトは
VISA/MasterCard/JCB/AmericanExpress/・・・

■2.割賦販売法でPCIDSS準拠は進んだ？

JCDSC

日本クレジット協会によるPCIDSS準拠の実行計画　2012年5月31日公表

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	PCIDSS準拠対応	PCIDSS検証方法
決済代行業者	形態問わず全て	全て		①PCIDSS準拠	オンサイトレビュー ネットワークスキャン
加盟店	非対面/ネット	4ブランドにより決定(※3)	A	②センシティブ認証情報(※2)非保持	
				③PCIDSS準拠	
	対面/POS			④センシティブ認証情報(※2)非保持	
				⑤PCIDSS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ン
				⑦PCIDSS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以外(※4)		⑧センシティブ認証情報(※2)非保持	
				⑨PCIDSS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	⑩PCIDSS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		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	⑫PCIDSS準拠	オンサイトレビュー ネットワークスキャン
	イシュイングのみ	100万件以上	B	⑬PCIDSS準拠	自己問診 ネットワークスキャン
		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

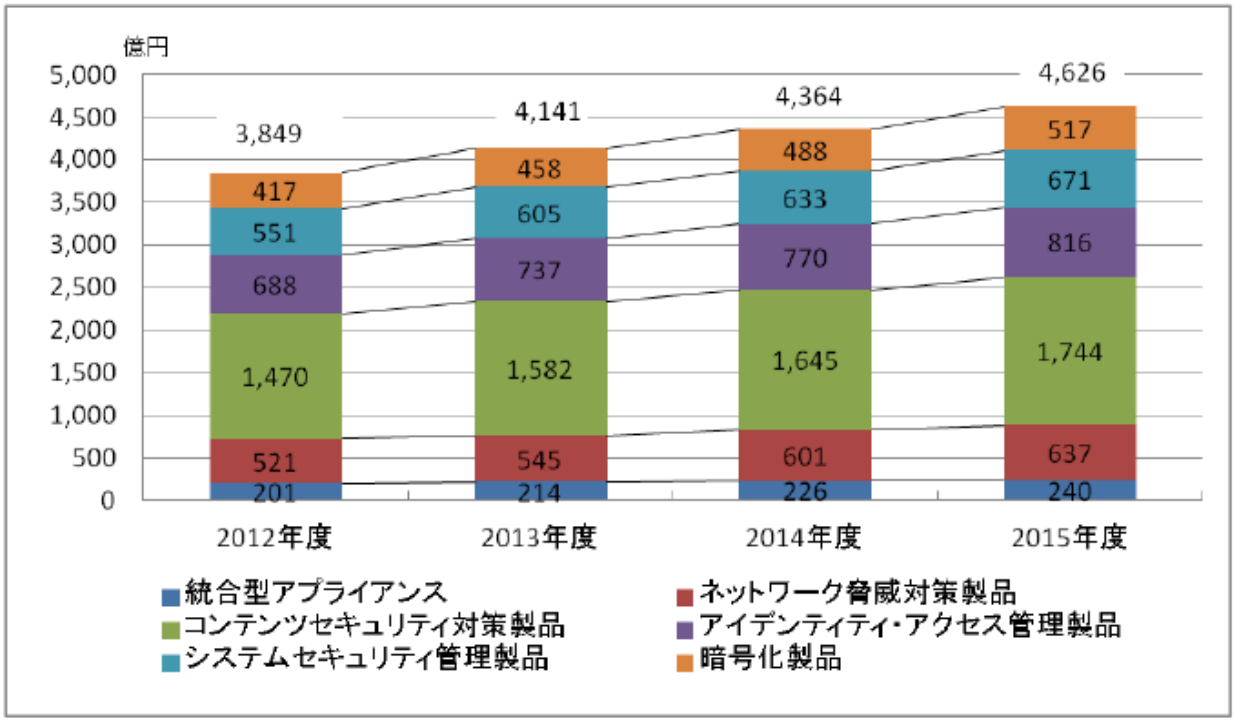
インフラ整備部会における検討期間

●2018年3月末までに、PCIDSSへの準拠を要請、指導責任はカード会社に。

参考/国内セキュリティツールの市場推移

JCDSC

セキュリティ製品には各企業が右肩上がりで投資を増やしている。



（引用）JNSA2015年6月発行 情報セキュリティ市場調査報告書

■3.レベル2企業もPCIDSS準拠してきている？

JCDSC

年間決済取扱い件数によるレベル分類（VISA）

レベル 1
年600万件超
※ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞｰは年30万件以上

必須

・内部、外部ネットワークのぜい弱性スキャン（**ASVで四半期ごと**）
・ネットワーク層とアプリケーション層への、内部、外部**ペネトレーションテスト**（年1回）

レベル 2
年100万～600万件
※ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞｰは、年30万件未満はすべて

推奨

必須

レベル 3
年2万～100万件

必須

四半期ごとに、**ASV**による外部ネットワークの脆弱性スキャン

（Approved Scanning Vendors：認定スキャンベンダー）

レベル 4
年2万件未満

必須

QSA による訪問監査
（Qualified Security Assessors:認定審査機関）

※適用基準はカードブランドによって異なります。また、加盟店とサービスプロバイダーでは異なります。

自己問診票（SAQ）
（Self-Assessment Questionnaire）

●MasterCardの適用基準は、VISAとほぼ同じ。JCBは、年間100万件以上をレベル1とし、ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞｰには件数に関わらず監査とスキャンを要請。

■4.レベル3-4企業はSAQの自己申告で“準拠”？

JCDSC

PCI DSS自己評価問診票 （Self-Assessment Questionnaire）

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、すべてのカード会員データ機能を外部委託

B1: インプリントのみの加盟店、カード会員データを電子形式で保存しない

B2: スタンドアロン型ダイアルアップ端末の加盟店、カード会員データを電子形式で保存しない

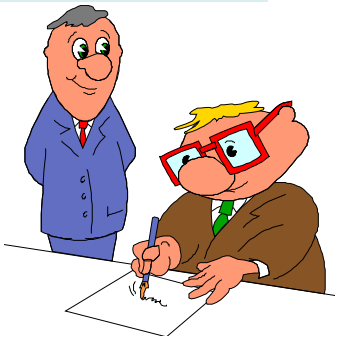
C: ペイメントアプリケーションシステムがインターネットに接続されている加盟店

D: ペイメントブランドによって SAQ を完了する資格があると定義されたその他のすべての加盟店とサービスプロバイダー

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

PCI Security Standards Council

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



■SAQガイドラインと各問診票

https://ja.pcisecuritystandards.org/minisite/en/saq-v3.0-documentation.php

■5. 専門コンサルなしでは認証を得られない？

JCDSC

①PCIDSS認証取得済み企業のコンサル支援比率は
　コンサルに依頼する際の注意点は

②QSA(審査会社)はアドバイスしてくれるか
　審査会社によって、どの程度異なるか

③数あるセキュリティ商材の切り札（オールインワン）はあるか

■6. カード情報非保持ならPCIDSS準拠は不要？

JCDSC

①決済代行業者からのカード売上げ明細報告データに、カード情報は入っていない？

②委託する決済代行業者が、PCIDSSに準拠していることの確認は、加盟店の責任？

③カード決済を扱う店舗従業員の教育は、どこまで求められる？

■7. カード情報非保持の認証制度はある？

JCDSC

①QSAは、カード情報非保持の審査をして証明を出せる？

②審査工程は少ないからPCIDSS準拠認定は安く済む？

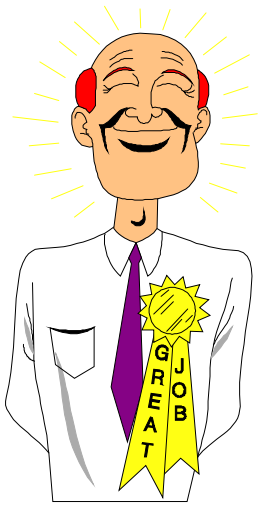
③「カード情報非保持」を自社宣言で表示してよい？

■8. PCIDSS準拠の認定統一マークは？

JCDSC

①QSA各社が独自に、認定マークを発行している。

②PCISSC（国際評議会）の考えは？



JCDSC/QSA部会に同席した、PCISSC
のマーケティング・マネージャー・J.King氏
2015.5.27 NTTデータ先端技術社にて

■9. PCIDSS準拠2018年3月期限は見直される？

JCDSC

改正割賦販売法が施行後5年を迎え、経産省の産業構造審議会は見直し検討結果の報告書を今月3日に公表した。

【カード情報セキュリティに関する部分】

1) 法令等により、特定の技術的手段を求めることには、なじまない面がある。…PCIDSSに特定することに疑問を提起

2) 各加盟店のシステム更改・改修期に配慮した現実的な対応を求めることが必要。…“2018年3月“のPCIDSS準拠期限を見直し？

3) カード番号に対する当事者意識が低い加盟店もあり、加盟店にも直接の責任を負担させる制度整備が必要。…加盟店への規制強化

4) 2015年3月発足の「クレジット取引セキュリティ対策協議会」における具体的・実効的な取組を推進することが適切である。…日本クレジット協会が1年かけて練ったナショナルプランを見直し？

■10. PCIDSS準拠は法令化なしでは達成できない？

JCDSC

①米国では州によっては、PCIDSS準拠が法律で義務になっている

②米国ターゲット社はPCIDSS認証取得していた
日本のB社も、プライバシーマーク認証企業・・・

③認証合格が目的化する弊害も

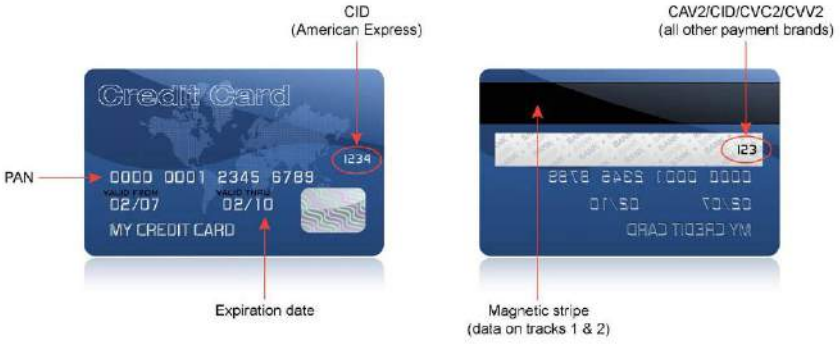
セキュリティは短距離走じゃなくて、マラソンだ

Maintaining Security is Running a Marathon, not a Sprint

●PCIDSSセキュリティフォーラム2014（7/29）
PCISSC-General Manager Bob Russo氏の基調講演より

すべては、カード利用者の安全のために

インターネット社会には国境がない。サイバーテロは明日にも襲う。



日本カード情報セキュリティ協議会（JCDSC）

代表事務局：NTTデータ先端技術株式会社
メール　jcdsc@intellilink.co.jp
事務局：日本オフィス・システム株式会社
メール　forum@jcdsc.org