オンサイト監査から見えるPCI DSS

2010/2/16

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について

会社名	国際マネジメントシステム認証機構（株）
業務内容	情報セキュリティに関する審査／監査、 第三者認証サービスのご提供
所在地	東京本社、札幌営業所
認定	・財団法人日本情報処理開発協会 （以下JIPDEC）からJIS Q 27001 （ISO/IEC27001）の認証機関として認定（ISR010） ・米国PCIセキュリティ基準審議会より 認定セキュリティ評価機関（QSA）として承認

PCI DSS概論

クレジットカードを取り巻く環境①

- 米国における最大規模の情報漏えい事件
  - データ処理会社が4,000万件のカード情報を漏洩
  - 国内でも2008年になって10万件規模のｶｰﾄﾞ情報漏洩が複数発生
- 個人情報保護法をトリガーとしたプライバシーマークの普及と不足要素の顕在化
  - 経済産業省からガイドラインが発行
    「クレジットカード情報を含む個人情報の取扱いについて」
  - JIS Q 15001はあくまで国内限定の規格
- 改正割賦販売法が可決
  - クレジット事業者に対して、個人情報保護法ではカバーされていない
    クレジット情報の保護のために必要な措置を講じることを義務づけると
    ともに、カード番号不正提供・不正取得をした者等を刑事罰の対象とする。
  - 違反事業者に対する行政処分が法制化
- 接続技術の変化
  - インターネットに接続した統合店舗販売時点管理（IPOS）
    システムの増加
  - カード会員データのIPベース送信の増加

クレジットカードを取り巻く環境②

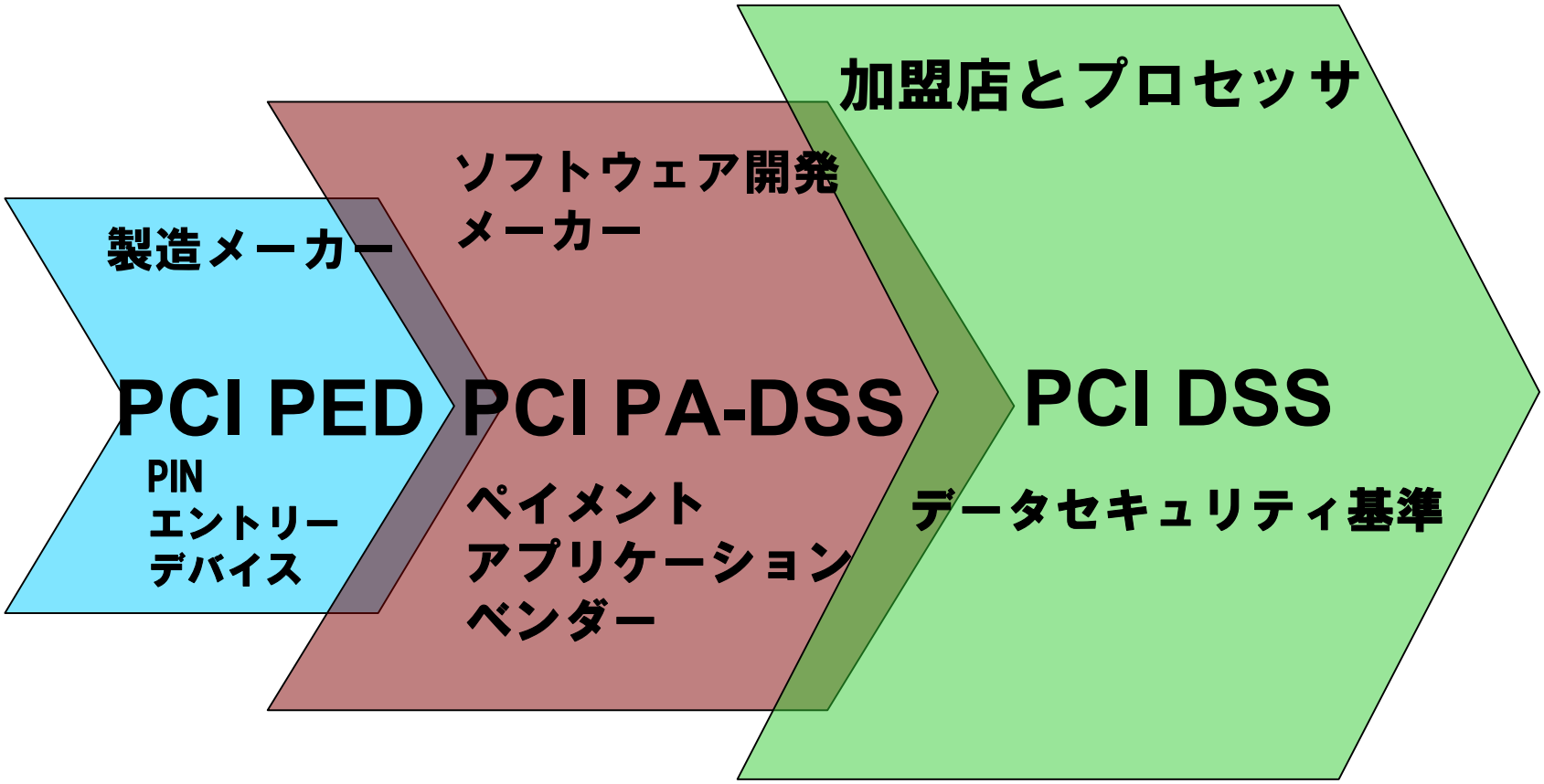
- クレジットカード情報の漏洩事件が多発
  - サウンドハウスのECサイト（音響機器）から約2.7万件流出（08年4月）
  - ナチュラムのECサイト（アウトドア）から約8.6万件流出（08年8月）
  - アリコジャパンの情報システムから約3.3万件流出（09/7月）
  - アミューズのECサイト『アスマート』から約5万件流出（09/8月）
  - デジタルダイレクトのECサイト『saQwa（サクワ） ネットショッピング 』から約5.2万件流出（09/9月）

PCI DSSとは？

- 国際的なクレジット産業向けの
データセキュリティ基準（Payment Card Industry Data Security Standard）

- VISA、MasterCard 、American Express、JCB、Discover、5つの国際ペイメントブランドによって2006年9月に設立されたPCIセキュリティ基準審議会（米国）が制定した事実上の基準

PCI基準とは？



PCI基準の概略と相関

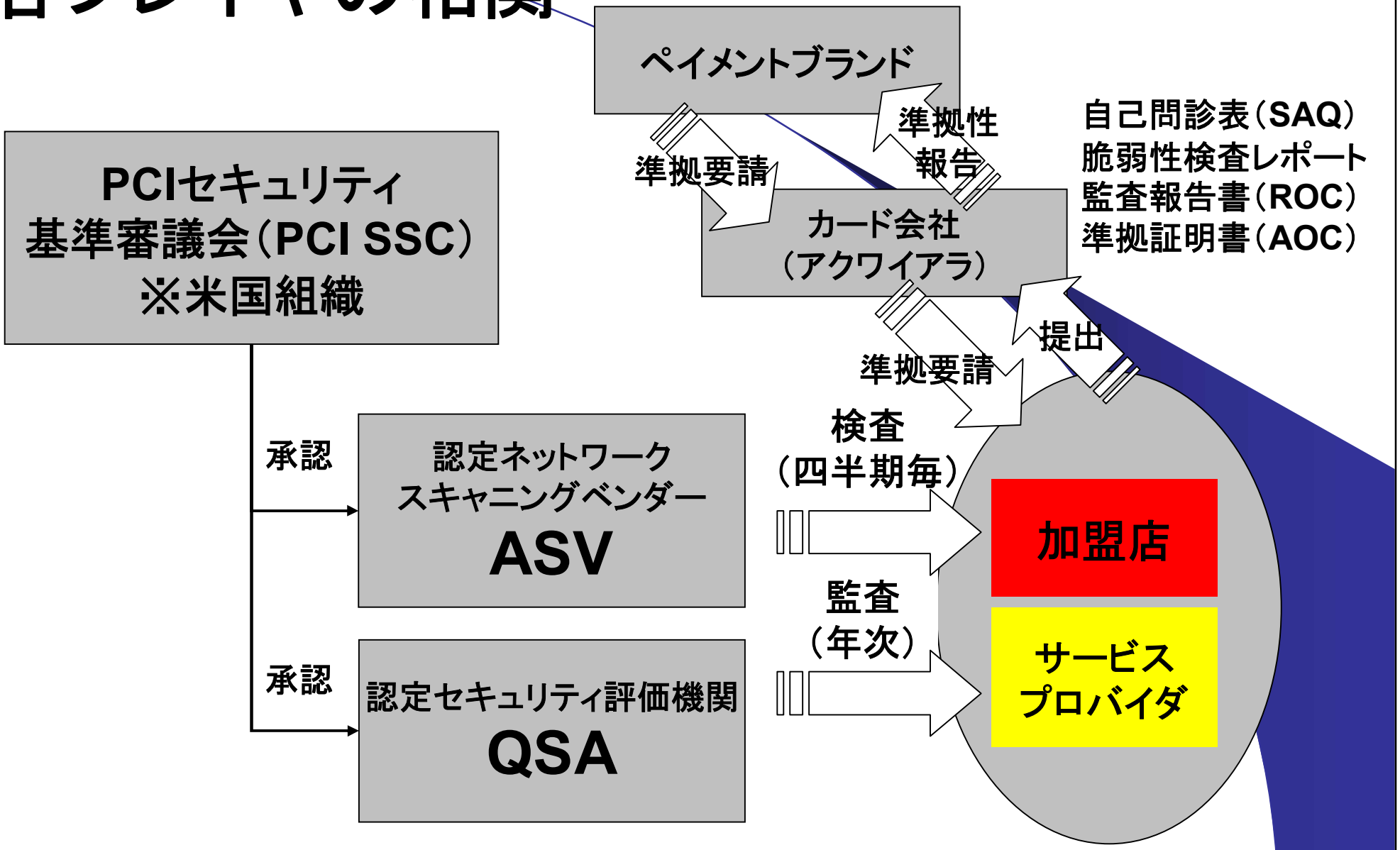
- PCI PEDは、
  - PINデバイスの暗号化プロセスやPINの保護に関するメカニズムを対象し、暗号化されたPINがペイメントアプリケーションやハードウェア端末に実装される。
- PA-DSSは、
  - パッケージのペイメントアプリケーションを対象とし、PCI DSSへの準拠をサポートする。
- PCI DSSは、
  - カード会員データの伝送／処理／格納を行うシステム、ネットワーク及びアプリケーションを対象としている。

米国における法整備の状況

- マサチューセッツ州（2007年2月）、ミネソタ州（2007年4月）、テキサス州、カルフォルニア州（ともに2007年5月）、ネバダ州（2009年9月）にPCI DSSの順守を州法により義務化した。

- テキサス州法では、漏洩事故を起こした事業者は金融機関(カード会社）に対してPCI DSSを順守していたことを証明できれば（30日以内に書面により提出）損害賠償を免れる。

各プレイヤの相関



PCIセキュリティ基準審議会の役割

- PCI DSSなど基準の発行及びライフサイクルの管理
- 基準に関しての解釈を正式に回答する唯一の機関
- QSA／ASVなどの承認
- QSA監査員資格の承認
- QSA／ASVの活動の品質管理

加盟店のレベルと取引件数

- 加盟店のレベルはペイメントブランドが定義する。
  注）ペイメントブランド毎に異なる。
- 加盟店レベルは主に取引件数によって区分される。
- 取引件数は契約するアクワイアラが判定する。
- 取引件数の総数は事業体の名称またはチェーン店の合計取引件数を基に判定する。

加盟店のレベル①

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP)
1	・当該ブランドの年間の取引件数が600万件以上、または地域のVISAがレベル1と判断したグローバルな加盟店	・当該ブランドの年間の取引件数が600万件以上 ・他のブランドがレベル1と判断した加盟店 ・過去にカード情報の漏洩事件を起こした加盟店	・当該ブランドの年間の取引件数が100万件以上 ・過去にカード情報の漏洩事件を起こした加盟店	・当該ブランドの年間の取引件数が250万件以上またはAmerican Expressがレベル1とみなす加盟店
2	・当該ブランドの年間の取引件数が100万～600万件	・当該ブランドの年間の取引件数が100～600万件以上 ・他のブランドにおいてレベル2の基準を満たす加盟店	・当該ブランドの年間の取引件数が100万件未満	・当該ブランドの年間の取引件数が5万～250万件以上またはAmerican Expressがレベル2とみなす加盟店

※VISA Inc.とVISA Europeでは基準が異なる。

加盟店のレベル②

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP）
3	・当該ブランドの年間の電子商取引における取引件数が2万～100万件	・当該ブランドの年間の電子商取引における取引件数が2万～100万件 ・他のブランドにおいてレベル3の基準を満たす加盟店	**N/A**	・当該ブランドの年間の取引件数が5万件未満
4	・当該ブランドの年間の電子商取引における取引件数が2万件未満 ・当該ブランドの年間の取引件数が100万件未満	・レベル1～3以外のすべての加盟店	**N/A**	**N/A**

※VISA Inc.とVISA Europeでは基準が異なる。

加盟店の検証方法①

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP）
1	QSAまたは内部監査人による年1回の監査報告書（ROC） ・ASVによる四半期毎のネットワークスキャン ・準拠証明書	・QSAによる年1回の監査報告書（ROC） ・ASVによる四半期毎のネットワークスキャン	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン
2	・年1回の自己問診票（SAQ) ・ASVによる四半期毎のネットワークスキャン ・準拠証明書	・PCI SSC認定の内部監査人資格をもつ自己監査人またはQSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン	・年1回の自己問診 ・ASVによる四半期毎のネットワークスキャン	・ASVによる四半期毎のネットワークスキャン

加盟店の検証方法②

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP）
3	・年1回の自己問診 ・ASVによる四半期毎のネットワークスキャン	・年1回の自己問診 ・ASVによる四半期毎のネットワークスキャン	**N/A**	・ASVによる四半期毎のネットワークスキャン（強く推奨）
4	・年1回の自己問診（推奨） ・ASVによる四半期毎のネットワークスキャン（推奨） ・アクワイアラが定める準拠要件	・年1回の自己問診（推奨） ・ASVによる四半期毎のネットワークスキャン（推奨）	**N/A**	**N/A**

サービスプロバイダのレベル①

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP）
1	・Visa Netに接続するプロセッサ、または取引の伝送／処理／格納の件数が年間30万件以上あるサービスプロバイダ	・すべてのTPP※1 ・年間30万件超の取引を伝送／処理／格納するDSE※2 ・過去にカード情報の漏洩事件を起こしたことがあるすべてのTPP及びDSE	・すべてのTPP	・すべてのTPP
2	・取引の伝送／処理／格納の件数が年間30未満のサービスプロバイダ	・年間30万件以下の取引を伝送／処理／格納するデータストレージエンティティ（DSE）		

※1　TPP (サードパーティープロセッサ): 取引処理サービスをアクワイアラのために行うサービスプロバイダ(インターネットペイメントサービス等）

※2　DSE（データストレージエンティティ): 取引処理サービスを加盟店又は他のサービスプロバイダのために行うサービスプロバイダ（Webホスティングサービス等）

サービスプロバイダの検証方法

レベル	VISA Inc.（AIS）	MasterCard（SDP）	JCB（JCBデータセキュリティプログラム）	American Express（DSOP）
1	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン ・準拠証明書 ・VISA Incのサービスプロバイダリストに掲載	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン	・QSAによる年1回のオンサイト監査 ・ASVによる四半期毎のネットワークスキャン
2	・年1回の自己問診 ・ASVによる四半期毎のネットワークスキャン ・VISA Incのサービスプロバイダリストには掲載されない（レベル1として検証すれば掲載）	・年1回の自己問診 ・ASVによる四半期毎のネットワークスキャン		

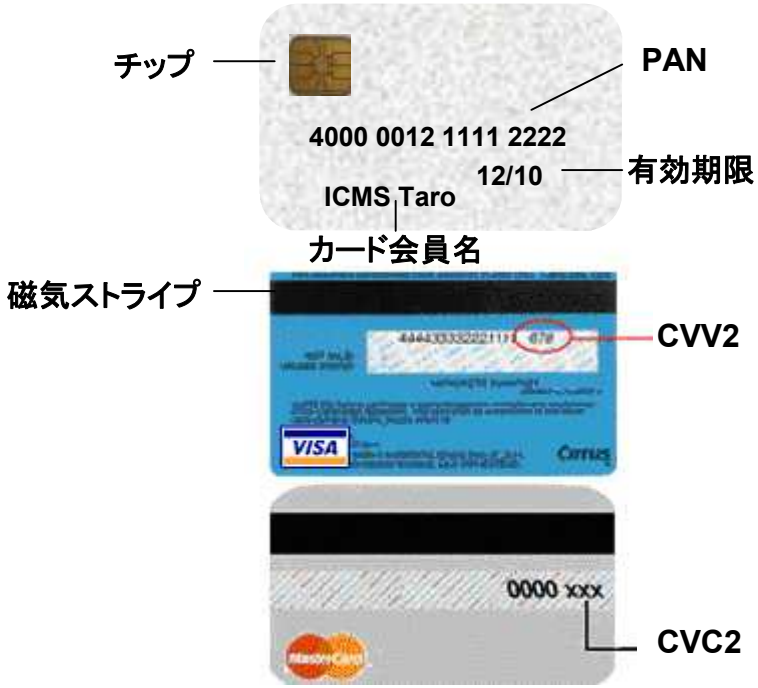
サービスプロバイダの再検証

VISA Inc. （AIS）	MasterCard （SDP）	American Express （DSOP）
・ROC承認日より12ヶ月以内に年1回の再検証を行わなければならない。 ・検証書類は期日までに承認されなければならない。 ・期日を過ぎた検証書類は義務の不履行とみなされ次のように色分けされたリストに記載される。 －期日超過が60日までの場合は黄色 －期日超過が61日以上の場合は赤色 ・期日超過が90日以上となったサービスプロバイダは検証書類が受領及び承認されるまでリストから削除される。	・レポート日より12ヶ月以内に年1回の検証を行わなければならない。 ・QSAは準拠証明書または検証証明書をMasterカードに提出しなければならない －ROCが承認されなかった場合 ・準拠証明書または検証証明書を期日までに提出しなければならない期日までに提出できない場合は義務の不履行とみなされMasterCardのWebサイトに掲載する準拠サービスプロバイダのリストから削除されることがある。また該当するアクワイアラに準拠していないと評価されることがある。	・ROCレポート日より12ヶ月以内に年1回の再検証を行わなければならない。 ・Amexは顧客に対し、スキャン期日の30日前までに、またROC期日の30日前及び90日前までに再検証を行わなければならないことを通知 ・ROCは顧客の年1回の再検証期日までに承認されなければならない。その期日を過ぎたROCは義務の不履行とみなされ、Amex独自の義務履行管理プロセスが実行される。ROCが承認されると、その後のROCのレポート日から12ヵ月後として新たに再検証が設定される。

※JCB（JCBデータセキュリティプログラム）では再検証についての定めはない

カード会員データ

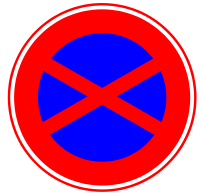
- クレジットカードの磁気ストライプまたはチップ内のデータをさす。
- カード会員データ
  - プライマリアカウント番号（15 ～16桁）：PAN
  - カード会員名
  - サービスコード
  - 有効期限
- センシティブ認証データ
  - 全磁気ストライプ／チップ上の磁気ストライプイメージ
  - CVC2／CVV2／CID／CAV2
  - PIN／PINブロック



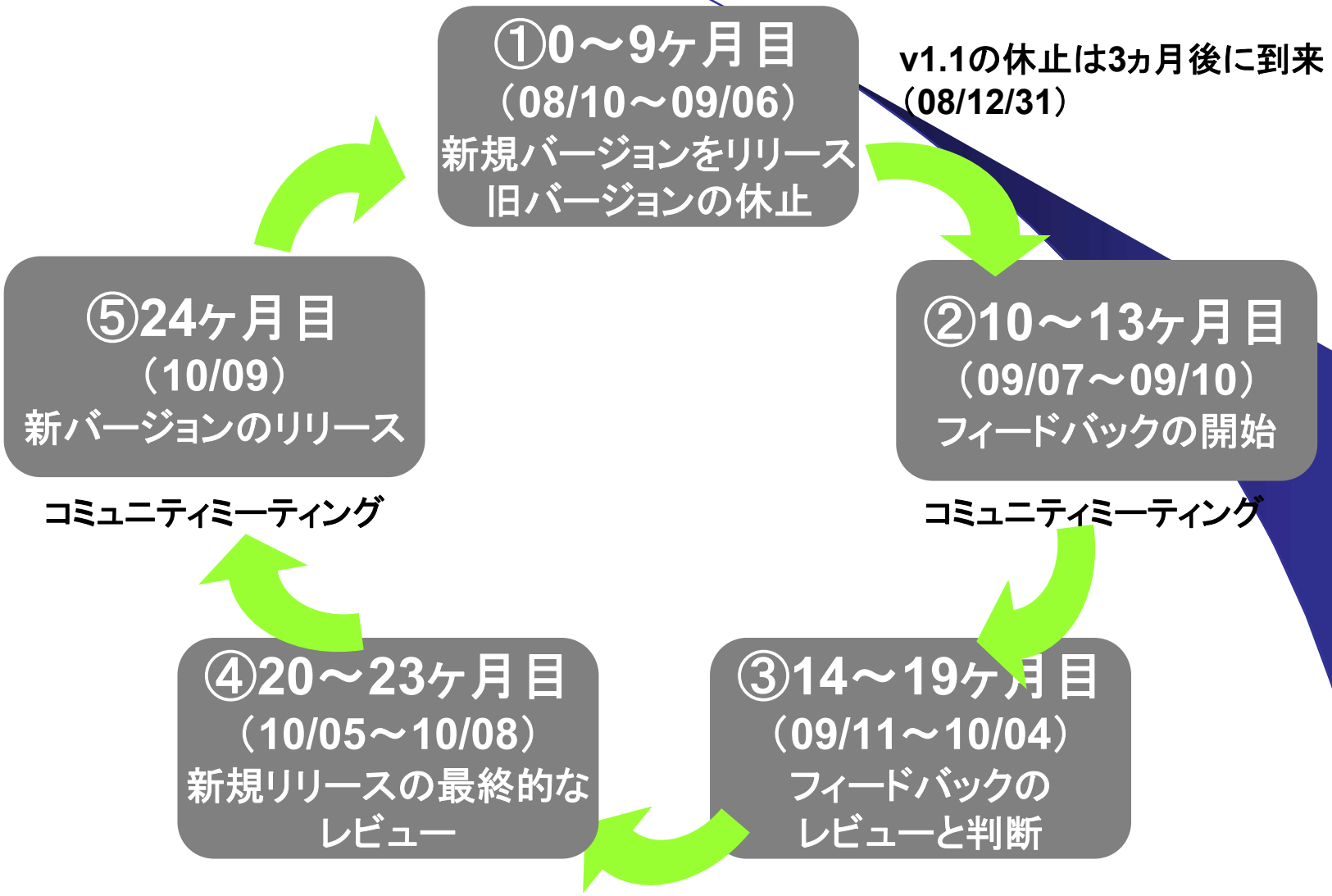
保管禁止データ①

	データ要素	保管可能	保護必須	PCI基準 要件 3.4
カード会員データ	カード番号（PAN）	YES	YES	YES
	カード会員名	YES	YES※1	NO
	サービスコード	YES	YES※1	NO
	有効期限	YES	YES※1	NO
センシティブ認証データ※2	完全な磁気ストライプデータ	NO	N/A	N/A
	CVC2／CVV2／CID／CAV2	NO	N/A	N/A
	暗証番号（PIN）／ PINブロック	NO	N/A	N/A

※1　これらのデータ要素はPANと共に保管される場合は保護が必要です。
※2　センシティブ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）保管してはならない。



PCI DSSのバージョンアップサイクル



オンサイト監査の実情

PCI DSS対象範囲決定のキーワード①

- 保存
- 処理
- 伝送

この3つのキーワードの1つでも該当するものは
PCI DSSの対象範囲となる

PCI DSS対象範囲決定のキーワード②

- ネットワークセグメンテーション

カード会員データを取扱う環境をできる限り
企業ネットワークから隔離する

PCI DSS対象範囲決定のキーワード③

- 第三者/アウトソーシングの取り扱い

保存、処理、伝送に係わる外部組織対応

1. 外部組織自らPCI DSSに準拠していることを証明する
2. 自身のオンサイト監査の対象範囲とする

組織の悩み

PCI DSS対象範囲の決定①

- 対象ネットワーク
  クレジットカード関連システム以外との共存
  - 電子マネー関連システム
    （Edy、WAON、Suica、PASMO、iD等々）
  - 社内OAシステム
  - 基幹システム

既存システムとのセグメント分けが困難

PCI DSS対象範囲の決定②

- 対象拠点
  - 本社、各拠点（店舗等含む）、データセンター、バックアップデータセンター

- 対象部門
  - システム部、営業部、カスタマーサポート部、各拠点

カード会員データの取扱範囲が把握されていない

ネットワークのセグメント分けが曖昧

PCI DSS対象範囲の決定③

- 外部組織の取扱
  - MSP事業者、ホスティング業者、アプリケーション保守業者、データセンター、データ保管業者等々
  - 子会社（海外含む）

カード会員データを取扱う先の対応が曖昧

代替コントロールの選択が多い要件①

- 要件2

  システムパスワードおよび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こと

  - 要件2.3

    すべてのコンソール以外の管理アクセスを暗合化する。Webベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、またはSSL/TLSなどのテクノロジを使用する。

    - ネットワーク機器等でTelnetやhttp接続以外できないものがある。

代替コントロールの選択が多い要件②

- 要件3

  保存されたカード会員データを保護すること

  - 要件3.4

    すべての保存場所でPANを少なくとも読み取り不能にする。

    - DB等が暗号化されておらず、大幅なシステム改修が必要
    - システム改修へ大規模な投資が必要
    - DB等を暗号化作業する際の既存業務への影響が大きい（ディスク暗合化等実施の場合）

代替コントロールの選択が多い要件③

- 要件3

  保存されたカード会員データを保護すること

  - 要件3.6.3

    安全な暗合化キーの保存。

    - 暗合化キーがアプリケーションに組み込まれている為変更が不可能

代替コントロールの選択が多い要件④

- 要件3

  保存されたカード会員データを保護すること

  - 要件3.6.4

    定期的な暗合化キーの変更

    - DBの再暗合化を行った場合の業務への影響が大きい
    - 暗合化キーがアプリケーションに組み込まれている為変更が不可能

代替コントロールの選択が多い要件⑤

- 要件3

  保存されたカード会員データを保護すること

  - 要件3.6.5

    古いキーまたは危険にさらされた疑いのあるキーの破棄また取替

    - 暗合化キーがアプリケーションに組み込まれている為変更が不可能

代替コントロールの選択が多い要件⑥

- 要件3

  保存されたカード会員データを保護すること

  - 要件3.6.6
    暗合化キーの知識分割と二重管理
    （キー全体を再構築するには、2～3人を必要とし、各自がキーの一部のみをしっている）

    - システム上暗合化キーを複数に分けることが出来ない
    - 運用管理上暗合化キーを知る管理者複数名必要

代替コントロールの選択が多い要件⑦

- 要件8
  コンピュータにアクセスできる各ユーザに一意のIDを割り当てる）
  - 要件8.5.5
    少なくとも90日ごとに非アクティブのユーザアカウントを削除/無効化する
    - システム運用上ログイン実績のないアカウントでも削除できないものがある

代替コントロールの選択が多い要件⑧

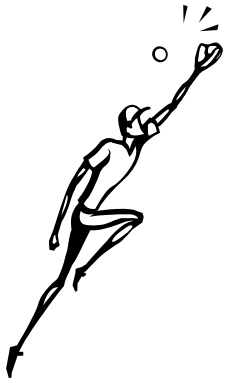
- 要件8
  - 要件8.5.9　少なくとも90日ごとにユーザパスワードを変更する
  - 要件8.5.10 パスワードに7文字以上を要求する
  - 要件8.5.11 数字と英文字の両方を含むパスワードを使用
  - 要件8.5.12 最後に使用した4つのパスワードと同じもの利用しない
  - 要件8.5.13 最大6回の試行後にユーザIDをロックアウトする
  - 要件8.5.14 ロックアウト期間を最小30分間または管理者が有効にするまでとする。

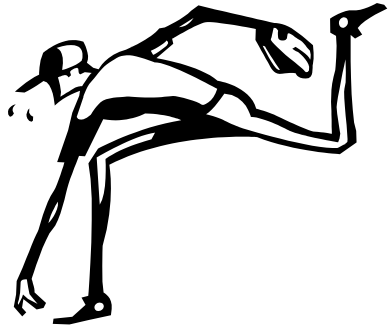
  以下の要求を全て自動設定することを要求されている

    - 利用のOSによっては自動設定できないものがある
    - 利用しているログインシステムよっては対応できない要件がある

要件事項への対応状況

- 組織は12要件204項目へ全ての対応が出来ているか？
  - オリジナル要件どおり対応できる組織は少ない。
    - 既に稼動しているアプリケーションの改修が困難
    - 既に稼動しているサーバ等の設定変更に伴う業務への影響が見えない
    - ネットワークセグメントの変更に伴う業務への影響が見えない
  - 多くの企業が代替コントロールを利用している。





今後の動向

国際カードブランドからの要求①

- **VISA International（以下VISA Inc.）による AIS（アカウントインフォメーションセキュリティ）プログラム**
  - VISA Inc.に直接賠償責任を負うのは加盟店募集のクレジットカード会社（アクワイアラ）
  - レベル1加盟店のPCI DSS完全準拠の期限
    - 2010/9/30
  - 期限を超過した場合はVISA Inc.は、当該加盟店と契約しているクレジットカード会社（アクワイヤラ）に対して罰金を含む何らかのリスクコントロールを課すことを表明している。
  - Visa、グローバルなPCI DSS推進のための奨励金制度を制定
    加盟店がPCI DSSへ完全準拠すると
    →レベル1　加盟店につき $50,000
    →レベル2　加盟店につき $10,000
    がクレジットカード会社（アクワイアラ）に支給される
    - 2010年9月10日まで
    - 予算が無くなり次第終了
  - http://www.visa-asia.com/ap/jp/mediacenter/pressrelease/NR_JP_150110.shtml

国際カードブランドからの要求②

- **MasterCard**
  SDP（サイトデータプロテクション）プログラム
  - MasterCardに直接賠償責任を負うのはアクワイアラ
  - 四半期に一度のPCI DSS準拠に関する報告を怠った場合に対するペナルティ
    →最大$25,000
  - PCI DSSの非順守に対するペナルティ
    →レベル1加盟店／レベル1,2サービスプロバイダ：最大$25,000
    →レベル2加盟店：最大$10,000、レベル3加盟店：最大$5,000
  - PCI DSSの非順守のよるクレジットカード情報の漏洩のペナルティ
    →保管禁止データの違反 $100,000（最大$500,000）
    →当該加盟店が順守を達成するまで最大$25,000/1日につき
    →調査費その他関連費用
  - イシュアに支払われる補償金
    →再発行1カードあたり最大$ 25、モニターすべきカード1カードあたり最大$5

日本カード情報セキュリティ協議会
QSA部会のご紹介

QSA部会の目的

1. PCI DSS要件の解釈や代替コントロールなど
   クリティカルイシューを議論することにより参加される
   QSA監査員の監査技術を向上する

2. 国内QSAにおけるPCI DSS要件の解釈を緩やかに
   統一する。解釈の許容範囲のストライクゾーンを
   統一していく

3. QSA監査員の地位向上

QSA部会の活動

- 2009年3月より活動を開始
  現在まで5回の会合を実施（約3ヶ月1回実施）
- 活動内容
  - 要件解釈の検討
  - オンサイト監査等からの問題点討議
  - クレジット業界の動向確認
- 今後の予定
  - コンサルタントとの意見交換会
  - 各種協議会との意見交換会

QSA部会参加企業

- NRIセキュアテクノロジーズ(株)
- NTTデータ・セキュリティ(株)
- 国際マネジメントシステム認証機構(株)
- 日本アイ･ビー･エム(株)
- BSIグループジャパン(株)
- ビジネスアシュアランス(株)
- (株)ブロードバンドセキュリティ

関連情報

- 関連リンク
  - 日本カード情報セキュリティ協議会
    http://www.jcdsc.org/
  - VISAインターナショナル
    加盟店向け情報»リスクマネージメント
    http://www.visa-asia.com/ap/jp/merchants/riskmgmt/index.shtml
  - JIPDEC ISMS制度推進室
    組織の認証取得に関する基準・ガイドなど»ISMS認証取得に関する文書
    http://www.isms.jipdec.jp/doc/JIP-ISMS116-30.pdf
    http://www.isms.jipdec.jp/doc/JIP-ISMS118.pdf
  - PCI Security Standard Council
    https://www.pcisecuritystandards.org/

ご清聴ありがとうございました

- PCI DSS準拠に関するお問い合わせ、セミナー内容に関するご質問、お気軽にご連絡ください。

- お問い合わせ先
  gyoumu@icms.co.jp
  0120-796-115