PCI DSS V3.1と
JIS Q 27001:2014(ISO/IEC27001:2013)

国際マネジメントシステム認証機構株式会社
代表取締役社長
上野 洋一

2015/7/28

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

本日のアジェンダ

- 弊社の紹介
- 1. PCI DSS運用の課題
- 2. PCI DSSとISMSの親和性
- 付録1 PCI DSS要件とJIS Q 27001:2014詳細管理策
- 付録2 PCI DSS V3.1　SSL/TLS1.0　1.1のベストプラクティス

弊社の紹介

弊社の紹介

会社名	国際マネジメントシステム認証機構株式会社 （略称：ICMS）
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	・一般財団法人日本情報経済社会推進協会 （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（QSAs）として承認
関連会社	Payment Card Forensics株式会社 （株式会社UBICとの合弁会社）

PCI DSSオンサイト監査実績

- 国内の主要インターネット決済代行事業者全てのオンサイト監査実績を持つ

1. PCI DSS運用の課題

PCI DSS V3.0 以降強化された点

- PCI SSC曰く
  以下のものがそろっていれば規格は確実に実践できると考えていた
  - ① テクノロジー
  - ② プロシジャー

- しかし、米国で続発する大量カード情報漏えい事故により視点が足りないものがあったと評価した
  - ③ ヒューマン
    - 運用する人のコントロールを確実に行うことが重要

PCI DSS V3.0 以降強化された点

- ポリシー文書、手順書を作成する
- 手順書に沿った記録を確認する
- 手順書に沿った運用プロセスを確認する
- 手順書が利用する担当者に周知されていることを確認する

PCI DSSが要求するリスク評価事項

- 要件2.2.3.c　2.3.f　4.1.i
  - SSL V3.0　Early TLSを利用することに対するリスク評価
- 要件6.1
  - システム脆弱性に対するリスク評価
- 要件9.9.2
  - POI等のカード読み取り装置の評価方法と頻度決定のためのリスク評価
- 要件10.6.2.b
  - 要件10.6.1の対象とならないログレビュー実施に対するリスク評価
- 要件12.2
  - 組織の情報資産に対するリスク評価

PCI DSSが要求する定期的評価

- 1年毎
  - 要件9.5.1　保管場所のセキュリティ状況の確認
  - 要件9.7.1　媒体の在庫確認
  - 要件11.3.1 外部からインフラ及びアプリケーションに対するペネトレーションテスト
  - 要件11.3.2 内部からインフラ及びアプリケーションに対するペネトレーションテスト
  - 要件11.3.4 セグメント有効性確認のためのペネトレーションテスト
- 半年毎
  - 要件1.1.7　Firewall及びルータの定期的レビュー

PCI DSSの定期的実施事項

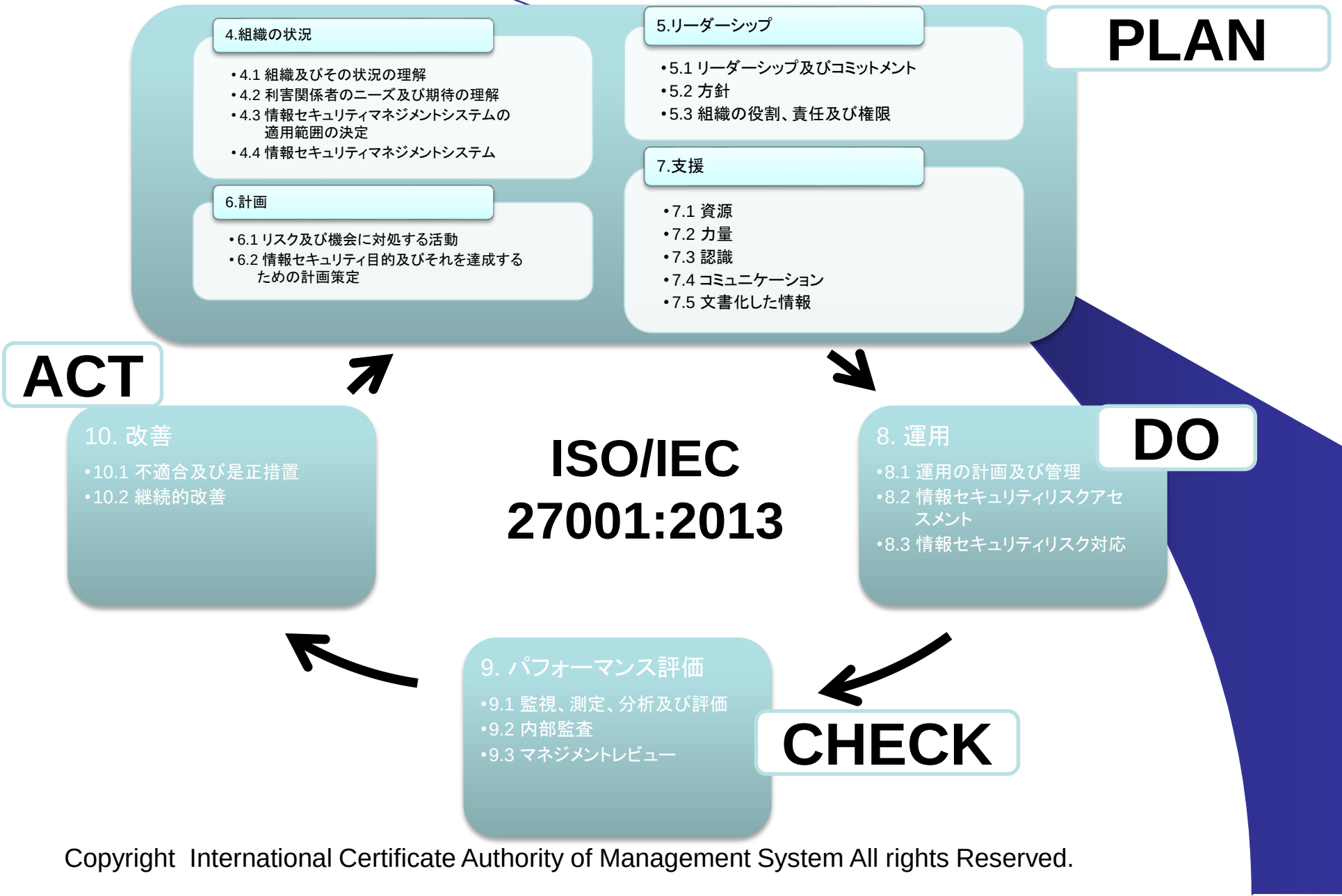
- 四半期毎（90日）
  - 要件3.1　四半期毎に削除期間を超えたデータの削除プロセスの実行
  - 要件11.1 四半期毎に不許可のワイアレスアクセスポイントの検出テスト
  - 要件11.2 四半期毎に内部外部の脆弱性検査の実施
  - 要件8.1.4 90日以内に不要アカウントの削除/無効化を行う
  - 要件8.2.4 90日毎にパスワード変更の実施
- 週次
  - 要件11.5　重要ファイル、システムファイル等の変更検出
- 日次
  - 要件11.6.1 重要ログの日次確認

PCI DSSオンサイト監査で発見される問題点

- PCI DSSが要求するリスク評価
  - 定期的に実施されていない
  - 手順書通り実施されていない
- PCI DSSが要求する定期的評価
  - 決められた周期で作業が実施されていない

2. PCI DSSとISMSの親和性

ISMS（JIS Q 27001:2014）のPDCAサイクル



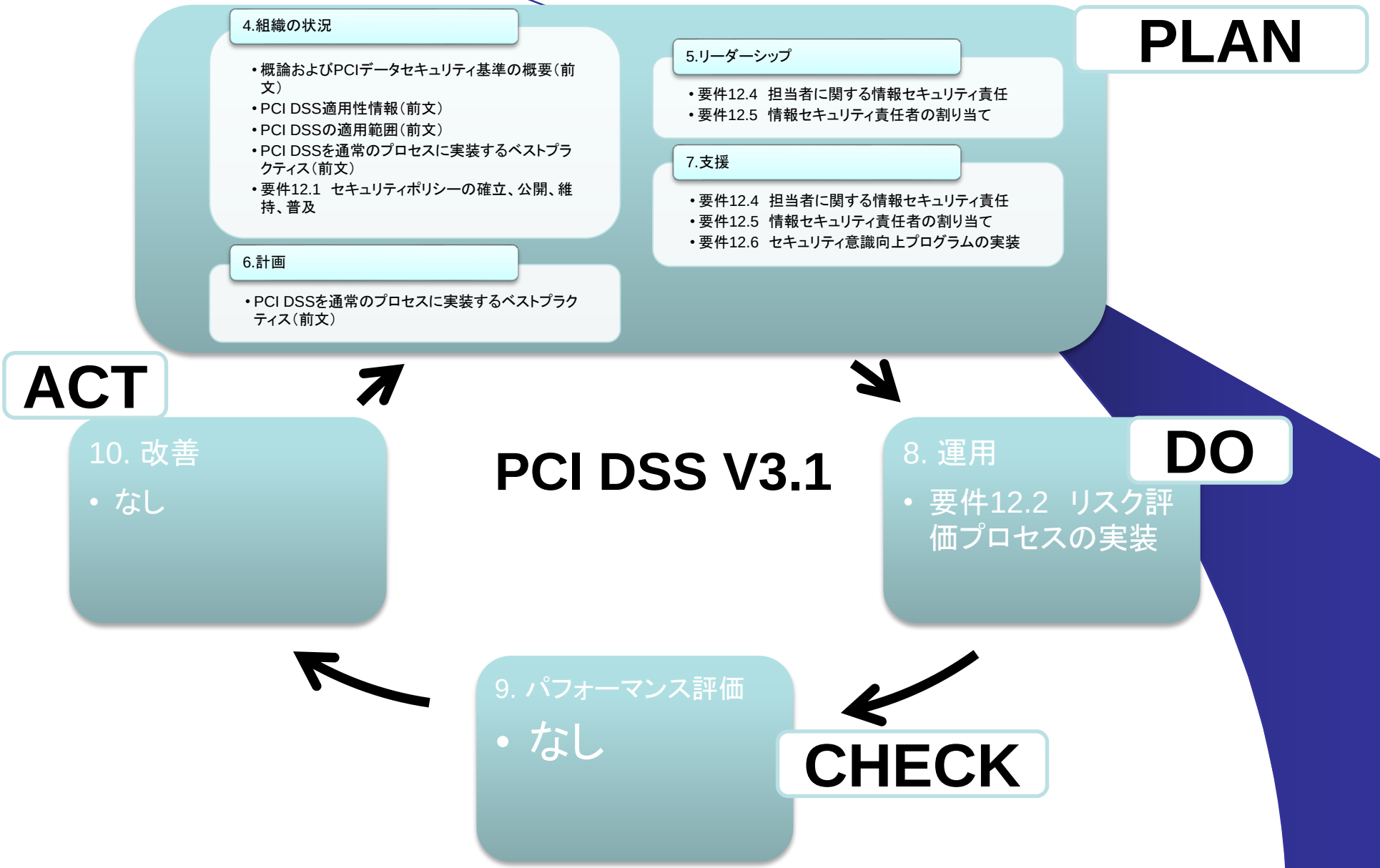
PCI DSS　Ver3.1のPDCAサイクル

- PLAN
  - 4.組織の状況
    - 概論およびPCIデータセキュリティ基準の概要（前文）
    - PCI DSS適用性情報（前文）
    - PCI DSSの適用範囲（前文）
    - PCI DSSを通常のプロセスに実装するベストプラクティス（前文）
    - 要件12.1　セキュリティポリシーの確立、公開、維持、普及
  - 5.リーダーシップ
    - 要件12.4　担当者に関する情報セキュリティ責任
    - 要件12.5　情報セキュリティ責任者の割り当て
  - 6.計画
    - PCI DSSを通常のプロセスに実装するベストプラクティス（前文）

PCI DSS　Ver3.1のPDCAサイクル

- PLAN
  - 7.支援
    - 要件12.4　担当者に関する情報セキュリティ責任
    - 要件12.5　情報セキュリティ責任者の割り当て
    - 要件12.6　セキュリティ意識向上プログラムの実装
- DO
  - 8.支援
    - 要件12.2　リスク評価プロセスの実装
- CHECK
  - なし
- ACT
  - なし

PCI DSS Ver3.1のPDCAサイクル



PCI DSS　PDCAの問題点

- CHECKプロセスの欠如
  - PCI DSS運用手順の有効性評価
  - 内部監査
  - マネジメントレビュー

- ACTプロセスの欠如
  - 運用違反等に対する是正処置（予防処置）
  - 継続的なPCI DSSの改善

PCI DSS と JIS Q 27001:2014との関係

- PCI DSSの各種要件は、**JIS Q 27001:2014 の詳細管理策を PCI SSCがリスクアセスメントした結果である**
  - 組織は自社で検討し作成すべき手順やルールが既に完成しており、ポリシーと運用手順を作成すればよい

- PCI DSSには、規格のPDCAを確実に運用するための手続きが無い
  - PCI DSSの運用を、ISMSのPDCAを利用し実践することでPCI DSSの継続的改善を図る

ICMSの提案

- ISMSのPDCAを利用しPCI DSS運用を行う
- ISMS認証とPCI DSS遵守を同時に行うことでカード番号だけでなく、組織の資産を保護する
- ISMS認証審査とPCI DSSオンサイト監査を同時行うことで組織の負荷を下げる

付録1
PCI DSS要件とJIS Q 27001:2014詳細管理策

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 安全なネットワークの構築と維持
  要件1 要件2
  - A.6.2.1　モバイル機器の方針
  - A.6.2.2　テレワーキング
  - A.8.1.1　資産目録
  - A.8.1.2　資産の管理責任
  - A.9.1.1　アクセス制御方針
  - A.9.1.2　ネットワーク及びネットワークサービスへのアクセス
  - A.9.4.1　情報へのアクセス制限
  - A.10.1.1 暗号による管理策の利用方針
  - A.12.1.1 操作手順書
  - A.12.1.2 変更管理
  - A.12.5.1 運用システムに関わるソフトウェアの導入

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 安全なネットワークの構築と維持
  要件1 要件2
  - A.12.6.2 ソフトウェアのインストールの制限
  - A.14.2.5 セキュリティに配慮したシステム構築の原則
  - A.13.1.1 ネットワーク管理策
  - A.13.1.2 ネットワークサービスのセキュリティ
  - A.13.1.3 ネットワークの分離
  - A.14.1.3 アプリケーションサービスの保護

PCI DSS要件とJIS Q 27001:2014詳細管理策

- カード会員データの保護
  要件3 要件4
  - A.8.1.1　資産目録
  - A.8.2.3　資産の取扱い
  - A.9.2.4　利用者の秘密認証情報の管理
  - A.10.1.1 暗号による管理策の利用方針
  - A.10.1.2 鍵管理
  - A.12.1.1 操作手順書
  - A.13.2.1 情報転送の方針及び手順
  - A.13.2.2 情報転送に関する合意
  - A.14.1.3 アプリケーションサービスのトランザクションの保護
  - A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護
  - A.18.1.5 暗号化機能に対する規制

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 脆弱性管理プログラムの維持
  要件5 要件6
  - A.6.1.2　職務の分離
  - A.6.1.5　プロジェクトマネジメントにおける情報セキュリティ
  - A.9.4.5　プログラムソースコードへのアクセス制御
  - A.12.1.1 操作手順書
  - A.12.1.2 変更管理
  - A.12.1.4 開発環境，試験環境及び運用環境の分離
  - A.12.2.1 マルウェアに対する管理策
  - A.12.6.1 技術的ぜい弱性の管理
  - A.14.1.1 情報セキュリティ要求事項の分析及び仕様化
  - A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 脆弱性管理プログラムの維持
  要件5 要件6
  - A.14.2.1 セキュリティに配慮した開発のための方針
  - A.14.2.2 システムの変更管理手順
  - A.14.2.5 セキュリティに配慮したシステム構築の原則
  - A.14.2.6 セキュリティに配慮した開発環境
  - A.14.2.7 外部委託による開発
  - A.14.3.1 試験データの保護

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 強力なアクセス制御手法の導入
  要件7 要件8 要件9
  - A.7.2.2　情報セキュリティの意識向上，教育及び訓練
  - A.8.1.1　資産目録
  - A.8.1.3　資産利用の許容範囲
  - A.8.2.1　情報の分類
  - A.8.2.3　資産の取扱い
  - A.8.3.1　取外し可能な媒体の管理
  - A.8.3.2　媒体の処分
  - A.8.3.3　物理的媒体の輸送
  - A.9.1.1　アクセス制御方針
  - A.9.1.2　ネットワーク及びネットワークサービスへのアクセス

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 強力なアクセス制御手法の導入
  要件7 要件8 要件9
  - A.9.2.1　利用者登録及び登録削除
  - A.9.2.2　利用者アクセスの提供（provisioning）
  - A.9.2.3　特権的アクセス権の管理
  - A.9.2.4　利用者の秘密認証情報の管理
  - A.9.2.5　利用者アクセス権のレビュー
  - A.9.2.6　アクセス権の削除又は修正
  - A.9.3.1　秘密認証情報の利用
  - A.9.4.1　情報へのアクセス制限
  - A.9.4.2　セキュリティに配慮したログオン手順
  - A.9.4.3　パスワード管理システム
  - A.9.4.4　特権的なユーティリティプログラムの使用
  - A.11.1.1 物理的セキュリティ境界
  - A.11.1.2 物理的入退管理策

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 強力なアクセス制御手法の導入
  要件7 要件8 要件9
  - A.11.1.3 オフィス，部屋及び施設のセキュリティ
  - A.11.1.4 外部及び環境の脅威からの保護
  - A.11.1.5 セキュリティを保つべき領域での作業
  - A.11.1.6 受渡場所
  - A.11.2.1 装置の設置及び保護
  - A.11.2.3 ケーブル配線のセキュリティ
  - A.11.2.4 装置の保守
  - A.11.2.5 資産の移動
  - A.11.2.7 装置のセキュリティを保った処分又は再利用
  - A.11.2.8 無人状態にある利用者装置
  - A.11.2.9 クリアデスク・クリアスクリーン方針

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 強力なアクセス制御手法の導入
  要件7 要件8 要件9
  - A.12.3.1　情報のバックアップ
  - A.12.4.1　イベントログ取得
  - A.12.1.1　操作手順書

PCI DSS要件とJIS Q 27001:2014詳細管理策

- ネットワークの定期的な監視およびテスト
  要件10 要件11
  - A.9.1.1　アクセス制御方針
  - A.12.1.1　操作手順書
  - A.12.4.1　イベントログ取得
  - A.12.4.2　ログ情報の保護
  - A.12.4.3　実務管理者及び運用担当者の作業ログ
  - A.12.4.4　クロックの同期
  - A.12.7.1　情報システムの監査に対する管理策
  - A.16.1.5　情報セキュリティインシデントへの対応
  - A.18.2.3　技術的順守のレビュー

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 情報セキュリティポリシーの維持
  要件12
  - 6.1.2　情報セキュリティリスクアセスメント
  - 6.1.3　情報セキュリティリスク対応
  - 8.2　　情報セキュリティリスクアセスメント
  - A.5.1.1　情報セキュリティのための方針群
  - A.5.1.2　情報セキュリティのための方針群のレビュー
  - A.6.1.1　情報セキュリティの役割及び責任
  - A.7.1.1　選考
  - A.7.2.2　情報セキュリティの意識向上，教育及び訓練
  - A.8.1.3　資産利用の許容範囲
  - A.9.1.1　アクセス制御方針

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 情報セキュリティポリシーの維持
  要件12
  - A.6.1.3　関係当局との連絡
  - A.6.1.4　専門組織との連絡
  - A.7.2.1　経営陣の責任
  - A.7.2.3　懲戒手続
  - A.7.3.1　雇用の終了又は変更に関する責任
  - A.8.2.2　情報のラベル付け
  - A.13.2.4　秘密保持契約又は守秘義務契約
  - A.15.1.1　供給者のための情報セキュリティの方針
  - A.15.1.2　供給者との合意におけるセキュリティの取扱い
  - A.15.1.3　ICTサプライチェーン
  - A.15.2.1　供給者のサービス提供の監視及びレビュー
  - A.15.2.2　供給者のサービス提供の変更に対する管理

PCI DSS要件とJIS Q 27001:2014詳細管理策

- 情報セキュリティポリシーの維持
  要件12
  - A.18.2.2　情報セキュリティのための方針群及び標準の順守
  - A.16　　情報セキュリティインシデント管理
  - A.17.1.1 情報セキュリティ継続の計画
  - A.17.1.2 情報セキュリティ継続の実施
  - A.17.1.3 情報セキュリティ継続の検証，レビュー及び評価
  - A.18.2.1　情報セキュリティの独立したレビュー

PCI DSS要件とJIS Q 27001:2014詳細管理策

- PCI DSS要件にない、JIS Q 27001:27001の詳細管理策
  - A.11.2.2 サポートユーティリティ
  - A.11.2.4 装置の保守
  - A.12.1.3 容量・能力の管理
  - A.17.2.1 情報処理施設の可用性
  - A.18.1.2 知的財産権

付録2　PCI DSS V3.1
SSL/TLS1.0　1.1のベストプラクティス

SSL/TLS1.0　1.1のベストプラクティス

- 2016年6月30日までは、SSL/TLS1.0　1.1の利用は可能だが利用する場合は以下の文書化が必要
  - 使用目的の記述
    - SSL/初期TLSを使用及び/またはサポートするデータの種類、タイプとシステムの数が含まれる
  - リスク評価結果に基づくリスク軽減管理手順
  - SSL/TLS1.0 1.1に関しての新しい脆弱性をモニタするための手順
  - SSL/TLS1.0 1.1を新規環境に実装しないことを確実にする変更管理手順
  - 移行計画の概要に移行完了の目標を2016/6/30以前に設定する

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

〒141-0021

東京都品川区上大崎2-24-11 目黒西口M2号館 5F

TEL　0120-796-115

mail　gyoumu@icms.co.jp

URL　http://www.icms.co.jp/