クレジットカード情報セキュリティフォーラム
～PCI DSSへの効率的な対応を探る～

PCI DSS準拠のポイントと ネット加盟店向けサービスのご紹介

2012年 7月 25日

TIS株式会社
IT基盤サービス第1事業部 シニア
エキスパート　三木 基司

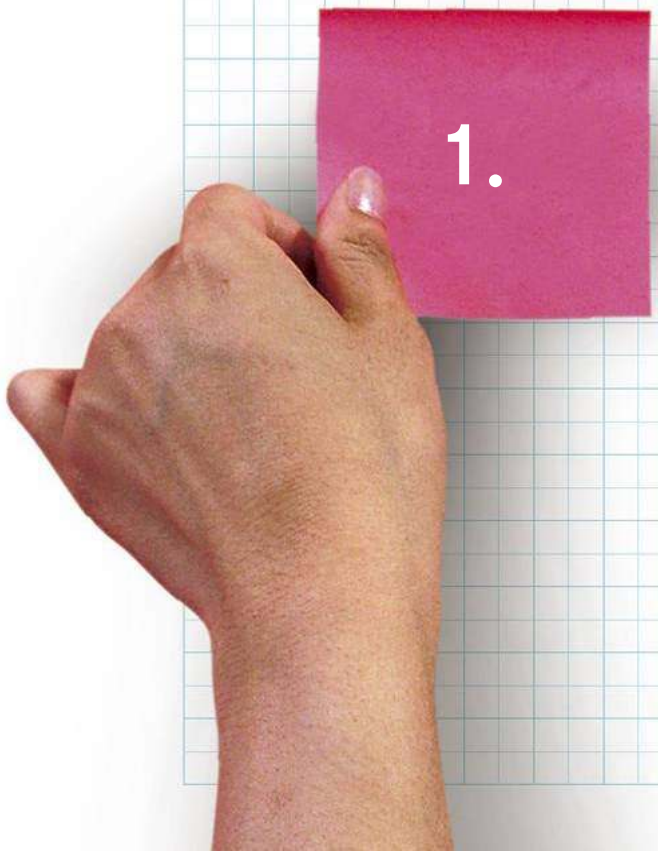
本日のアジェンダ

第1部　PCI DSS準拠のための事例紹介

1. PCI DSS制度におけるTISの位置付け
2. 当社取り組み姿勢
3. PCI DSS要件に対するシステム化要件
4. PCI DSS要件に対するシステム化ポイント
5. PCI DSS準拠のTISフレームワーク
6. ギャップ分析後の改善方針検討
7. セキュリティツールの選定・評価
8. PCI DSS準拠のコスト
9. PCI DSS準拠コストの削減事例

第2部　インターネット加盟店様向けサービスのご紹介

10. インターネット加盟店様向けサービスのご紹介
11. 『インターネット加盟店認証プログラム』全体フロー
12. 『インターネット加盟店認証プログラム』実施フロー



PCI DSS準拠のための事例紹介

1. PCI DSS制度におけるTISの位置付け

2. 当社取り組み姿勢

- ASV技術者として対象システムのセキュリティ対策全般をご支援
- SI事業のノウハウを活かし、最適なソリューションの組合せをご提供
- PCI DSS準拠対象のすべての企業様を全国規模でサポート

カード会社様 加盟店様	PCI DSS準拠支援 コンサルサービス
インターネット加盟店様	インターネット加盟店様向け 認証プログラム
カード情報取扱いデータセンタ様	SIサービス、ソリューション提供

3. PCI DSS要件に対するシステム化要件

◆ PCI DSS要件と情報システムのセキュリティ対策として考慮点

PCIDSS	セキュリティ上の管理策	関連するシステム構成要素または管理策
要件1	ネットワークセキュリティ	ファイアウォール、通信制御
要件2	サーバセキュリティ	サーバ機器の堅牢化(デフォルト変更)
要件3、4	データセキュリティ	保管データ、DB、通信経路の暗号化
要件5	ウイルス対策	ウイルス対策
要件6	アプリケーションセキュリティ	WAF、セキュアWEB開発(ソースレビュー)
要件7、8	アクセス制御(アカウント管理)	ID/Pass管理、アクセス制限
要件9	物理セキュリティ	入退室管理、施錠管理
要件10	ログ管理	ログ管理、時刻同期
要件11	システムのテスト	侵入検知、改ざん検知、脆弱性検査
要件12	ポリシー(マネジメントシステム)	ポリシー作成、委託先管理、教育

4. PCI DSS要件に対するシステム化ポイント

◆ カード会員情報の伝送、処理、保管範囲を最小化する
- 業務上の取扱い範囲を見直す
- 情報システム上のカード会員情報を集約化または情報のトークン化

◆ カード会員情報へのアクセスできる人や場所を見直し最小化する
- アクセス権限の見直し
- アクセスするための認証方式の見直し

◆ 情報システムの新規／改修のための仕様書では、非機能要件と
PCI DSS準拠のためのセキュリティ要件は意識して書き分ける
- セキュリティ機能の導入（暗号化、IDS/IPS、ログ管理など）
- 脆弱性対策（どのような脆弱性への対応を何で行なうのか）

※脆弱性対処の方針は示されていますが、対処方法は不明確です。（要件6.5）
脆弱性対処についてはOWASPなどのベストプラクティスからの引用になっている。

◆ ISMSやプライバシーマークのセキュリティ対策との整合性を考慮する

5. PCI DSS準拠支援のTISフレームワーク

※★印はQSA実施タスクです。
※グリーンの網掛けタスクは、別途お見積りとなります。また、ピンクの網掛けは、認定機関による作業タスクです。
※QSA：国際マネジメントシステム認証機構株式会社、ASV：TIS株式会社が実施します。

6. ギャップ分析後の改善方針検討

- ◆ 改善方針は、実現性と導入コスト、運用負担を総合的に判断し決定
- ◆ 既存システムの安定・安全な動作を最優先に代替コントロールを検討
- ◆ 必要最小限のツール選定により、対応コストを最小化
- ◆ 戦略的なセキュリティ対策の実践に向け、改善方針は3方向に分けて整理
- ◆ 対応後なお残るお客様環境固有の残存リスクについても、確認方法を検討

【サンプル】

PCIDSS 要件番号	テスト手順	対策状況	具体的なリスク	改善方針			残存リスク	残存リスク確認方法
				システム設定	ツール導入	運用改善		
8.5.8 グループ、共有、または汎用のアカウントとパスワードなどの認証方法を使用しない。	システム管理作業およびその他の重要な機能のための共有ユーザ ID が存在しない。	システム運用管理のために共有IDを使用	なりす			・個別ID付与	不正操作	90日毎のたな卸し


代替コントロールワークシート

7. セキュリティツールの選定・評価

◆ ギャップ分析結果を要求仕様とした最適なツール化対応の組合せを
お客様に代わり評価・選定

◆ ツール選定時の視点
- 情報システム基盤技術となる点を重要視
「保守を含む国内実績」、「取扱いベンダの注力領域」

【サンプル】

事例紹介

8. PCI DSS準拠のコスト

◆「システム対応コストが高く、運用負担も大きのでは？」

◆ PCI DSS要件の目的を正しく解釈し、コストを抑えます

事例紹介企業様の情報	
準拠対象システム	新規開発のシステム
システム規模とOS	サーバ約30台（Windows、Linux、Nonstop）
対応期間	10ヵ月

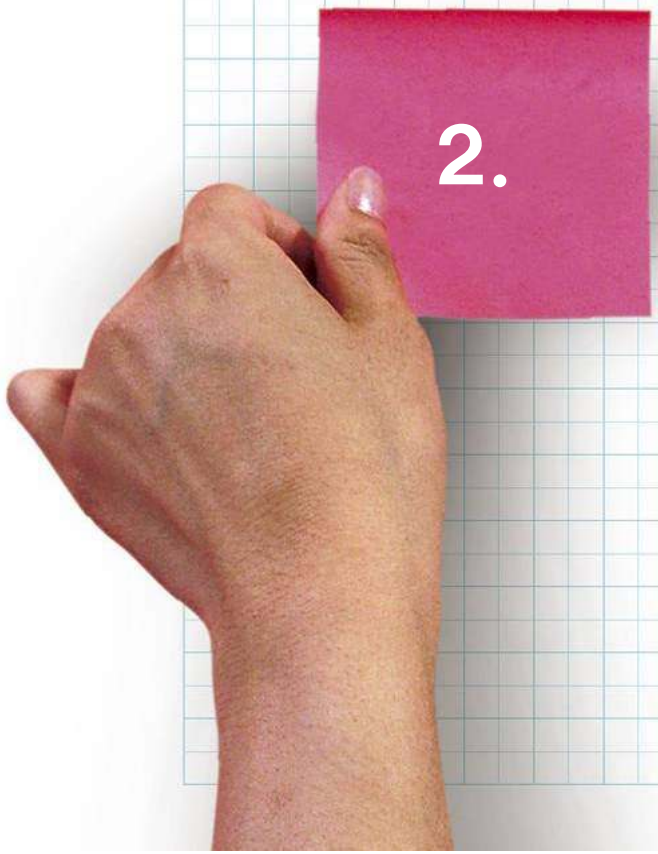
事例紹介

9. PCI DSS準拠コストの削減事例

◆ セキュリティツールの機能を上手く組合せてコスト削減

※ 赤文字は代替コントロール対応ヶ所

システム化要件	準拠対応内容	削減費用 （単位：M円）
要件2 サーバ機器の堅牢化（デフォルト変更）	・サーバ設定シートの提供 ・管理コンソールの暗号化実施せず	▲1.5
要件3、4 保管データ／DB／メール等の暗号化	・DBは暗号化せず ・代替コントロールによる対応	▲12.0
要件5 ウイルス対策	・ウイルス対策ソフトを導入 ※IDS機能付きウイルス対策ソフト	2.7
要件6 WAF、セキュア開発（ソースレビュー）	・WAFは導入せず ※年一回のペネトレーションテストで対応	▲4.0
要件7、8 ID管理、アクセス制限	・自動アクセス制御システムを導入 ※改ざん検知機能付きのツール	16.6
要件10 ログ管理	・ログ管理サーバを導入	4.9
要件11 システムのテスト、侵入検知、改ざん検知	・侵入検知ツールは導入せず ・ペネトレーションテスト、内部スキャン	▲6.0
要件12 ポリシー整備、既存規程類との整合性	・ISMSを利用し、追加コストなし	▲3.0



2. インターネット加盟店様向けサービスのご紹介

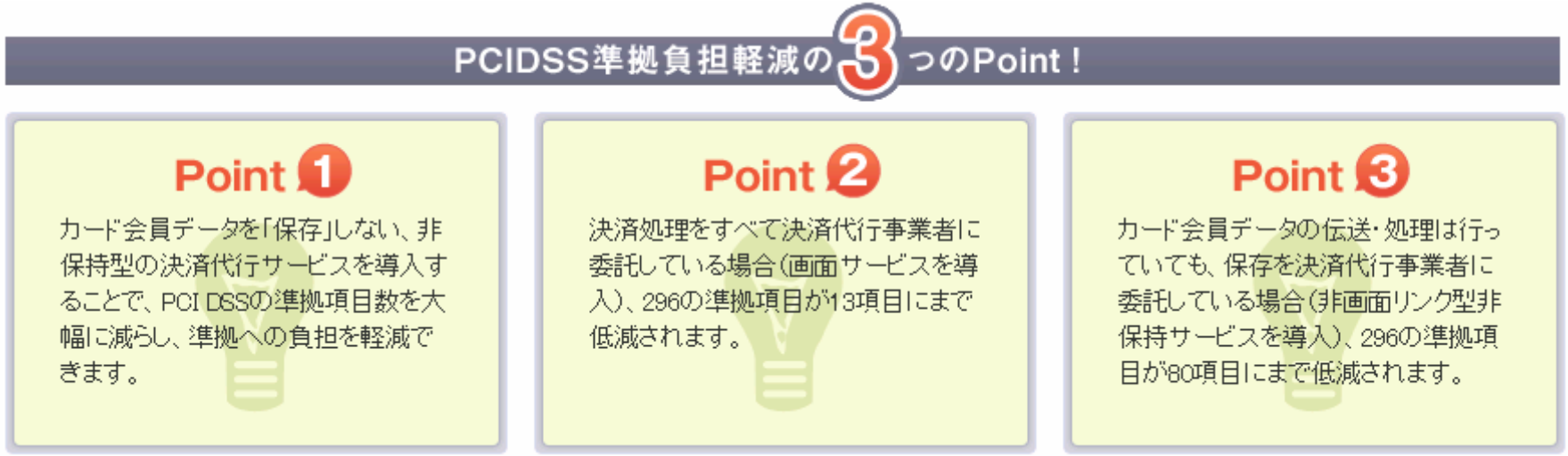
10. インターネット加盟店様向けサービスのご紹介

◆ インターネット加盟店様のPCI DSS準拠をお手伝いします

・ヒアリングと実査によるPCI DSS準拠対象範囲の明確化

・カード会員情報非保持化によるPCI DSS準拠負担の軽減

※本サービスには、国際マネジメント認証機構(QSA)様の認証プログラムを利用します。



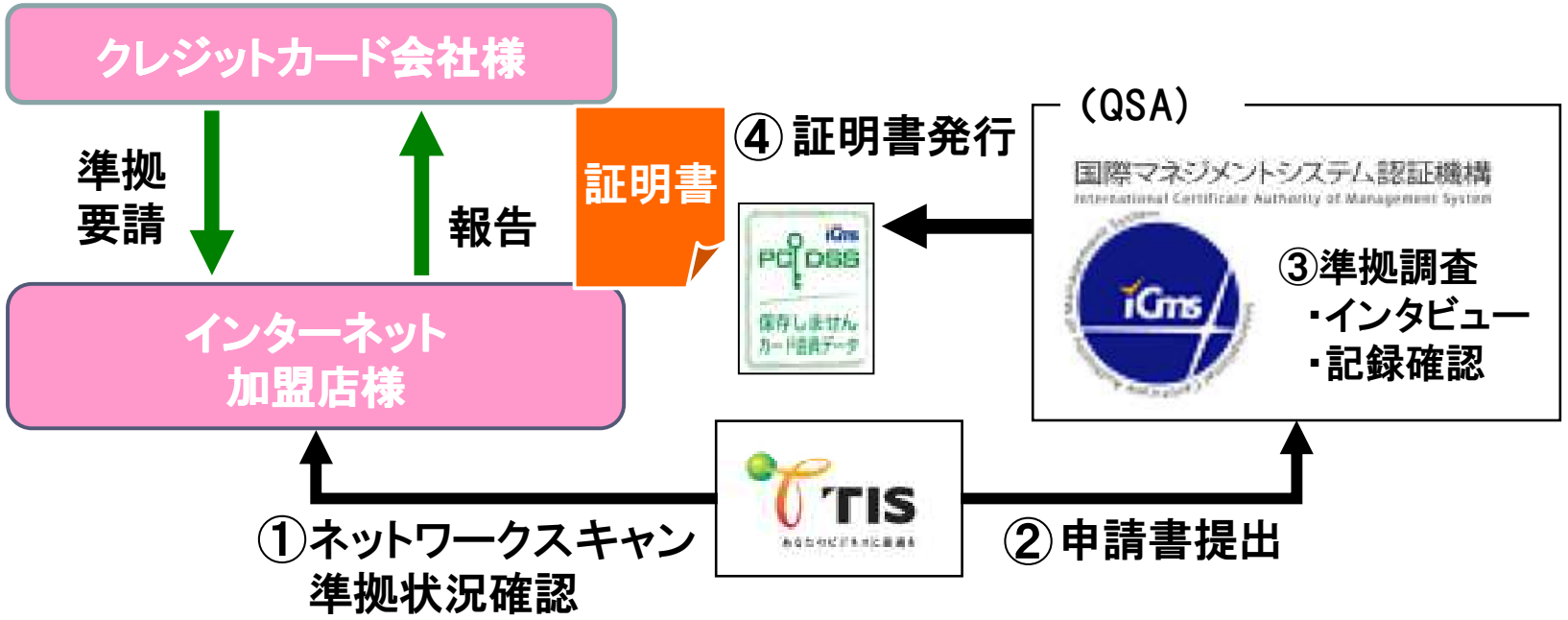
◆ 決済業務を外部委託している場合には
最大で必須準拠項目が「296→13項目」まで低減されます

11.『インターネット加盟店認証プログラム』全体フロー

インターネット決済代行事業者様の非保持サービスを導入した
インターネット加盟店様へ国際マネジメントシステム認証機構が
独自認証マークを発行するサービスです

◆ PCI DSSの準拠証明書にQSAのサインが入ります

◆ 加盟店様はアクワイアラ様へ状況をご報告いただけます



12.『インターネット加盟店認証プログラム』実施フロー

【サービス内容】

◆ 申込み書類、添付資料の作成

◆ 必要記録の事前確認

◆ 脆弱性スキャンの実施

◆ QSAインタビュー準備

◆ PCI DSSご質問受付(専用窓口)

【メリット】

◆ PCI DSS準拠対応の過大
過小投資を防止

◆ QSAインタビュー準備支援
・調査対象記録を事前確認します
・不足資料の雛形をご提供します
・インタビュー調査の準備をご支援します
（資料不備による再調査や調査延長を
防止します）

●お問い合わせ

http://www.tis.co.jp

IT基盤サービス本部　IT基盤サービス第１事業部
IT基盤サービス第４部
TEL　：　03-5337-4392
三木　基司　E-mail: miki.motoji@tis.co.jp