クレジットカード情報　セキュリティフォーラム講演資料

加盟店向けPCI　DSS準拠支援サービス

～　効果的な現状分析と対策のご紹介　～

2012年　7月25日

トッパン・フォームズ株式会社

1．はじめに

TOPPAN FORMS

トッパンフォームズの取り組み

- セキュリティ対策ソリューションを展開
- 「課題の抽出」から「対策の実施」を効率的にトータルサポート
- マルチベンダーだからこそできるトータルサービスを提供

セキュリティ対策ソリューションの事例紹介

- ワンタイムパスワード認証サービス
- 機密文書回収、溶解処理装置
- 監視カメラ
- 鍵管理システム　　など

◆ PCI DSS(Ver2.0)要件に対応するソリューション(事例1)

PCI DSS要件

要件8 コンピュータにアクセスできる各ユーザーに一意のIDを割り当てる。
(8.3)従業員、管理者、及び第三者によるネットワークへのリモートアクセスには**2因子認証**を組み込む。

テスト手順

(8.3)すべてのリモートネットワークアクセスに2因子認証が実装されていることを確認するために、ネットワークにリモート接続する従業員(管理者など)を観察し、パスワードと**追加認証アイテム**(スマートカード、**トークン**、PINなど)の両方が要求されていることを確認する。

要件に対応するためのアプリケーションと特徴

本要件は、カード会員データへのリモート接続をする際の認証強化を要求
この要求に対して、**ワンタイムパスワード認証サービス**をご提案

ワンタイムパスワード認証サービスの特長

①ハードトークン(キーホルダ、カード)、ソフトトークンを提供
②トークンの申込受付、製造、発行、認証までトータルでサポート

導入実績

- 国内製造業　B2B ECサイトのログイン
- 韓国投資証券会社　インターネットバンキング用パスワードトークン
- 国内オンラインゲーム　オンラインゲームのログイン

カード型トークン

キーホルダー型トークン

ソフトトークン

◆ PCI DSS(Ver2.0)要件に対応するソリューション(事例2)

PCI DSS要件

(9.10.1) カード会員データを再現できないよう、ハードコピー資料を裁断、焼却、またはパルプ化する。

テスト手順

(9.10.1.a) ハードコピー資料が、再現できないことを合理的に保証するように、クロスカット裁断、焼却、パルプ化されていることを確認する。

(9.10.1.b) 破棄される情報に使用される保管コンテナを調査して、コンテナが安全であることを確認する。たとえば、"裁断予定"のコンテナに、中身にアクセスする鍵がつけられていることを確認する。

要件に対応するためのアプリケーションと機能

本要件は、ハードコピー資料(紙媒体)の廃棄の管理について要求
この要求に対して、機密文書回収BOXによる管理方法と溶解装置による廃棄方法について提案

セキュリティソリューションの特長

①機密文書を確実に回収・溶解することで、情報漏えいを防ぎ、情報セキュリティーを確保
②機密文書を古紙として再利用することで、廃棄コストの削減を見込む
③再生した紙を使用し印刷物を製造することで、環境貢献や企業ブランドの向上につながる

オフィスにおける機密文書の回収パターン

お客さまご担当者の声

- Ｐマーク、ＩＳＭＳは取得しているがＰＣＩＤＳＳはどこが違うのか?
- セキュリティ評価基準が理解しにくい
- コンサルに依頼するとかなりの費用がかかる
- どのように社内に展開していけばよいのか?
- 社内に説明するための材料がない
- **準拠するためにかかる費用は**?
- なるべく費用をかけないで出来ないか?

何から進めたらよいか、わからない。
コストを抑えたい。

「加盟店向け　PCI　DSS準拠支援サービス」をご利用ください！

2. 加盟店向けPCI DSS 準拠支援サービスの概要

TOPPAN FORMS

PCI DSS準拠の導入ステップとトッパンフォームズのサポート範囲です。

サポート範囲

Ⅰ 課題の抽出

1 **現状確認**
- 簡易版自己問診票
- ネットスキャン テストサービス

特長1

2 自己診断

3 脆弱性のスキャンテスト
- 外部ネットワークスキャンテスト
- ペネトレーションテスト 他

Ⅱ 対策の実施

4 **準拠範囲縮小の検討と対策**

特長2

5 改善活動（ユーザー支援／コンサルティング）

6 QSA訪問監査

7 PCI DSS認定

TOPPAN FORMS

課題の抽出

特長1

現状の確認

簡単に、早く、安く行う現状確認方法を2つ提案

1）簡易自己問診票

2）ネットスキャン　テストサービス

TOPPAN FORMS

簡易版自己問診票のコンセプト

注） 簡易版のなりますので、PCIDSSの要求を全て網羅したものではありません。

- 簡易版自己問診票は、PCIデータセキュリティ基準で定めた約290項目の評価手順から20項目を抜粋し、わかり易い言葉に置き換えて作成
- PCI DSSの要件に対して、対応できているかのレベル感を認識する

＜簡易版自己問診票（一部）＞

PCI DSS準拠状況 自己チェック表（簡易版）

※（ ）はPCI DSS Ver2.0の要求事項番号です。

1	店頭でクレジットカードを取り扱う場合、カードをお客様の視界の範囲内で取り扱わなければならないことを、ルールに定めていますか。(12.6)	□
2	クレジットカードの取扱いガイドラインを含めて、関係する従業者（アルバイトを含む）全員に、採用時および年1回以上の、個人情報保護・セキュリティ研修を行っていますか。(12.6)	□
3	従業者への研修は、アンケートや確認テストなどで理解度を測定し、理解不足の人にはフォローアップ教育を行っていますか。(12.6)	□
4	カード番号が印字された伝票の控えは、施錠できるキャビネットで保管し、カギの管理者を定めていますか。(9.5)	□
5	廃棄する伝票は、クロスカットシュレッダーまたは焼却、溶解などの処理、または信用できる廃棄業者を利用していますか。(9.10)	□
6	カード決済を行うPOSレジを使用している場合、そのメーカーがPA-DSSの認証を得ていることを確認していますか。(6.5)	□
7	顧客のカード情報を見ることができるPCに、アクセスする従業員を限定していますか。(7.1)	□
8	カード番号の情報を保存する場合、暗号化しており、またセンシティブデータは保存していないことが、確認できますか。(3.2)	□
9	インターネットでカード情報を送受信する際、暗号化を施していますか。(4.1)	□
10	ウィルス駆除ソフトは、常に最新のパターンファイルに更新されており、その監査ログを確認していますか。(5.2)	□
11	すべてのWebアプリケーションが、OWASPなどの安全なコーディングガイドラインに基づいて開発されていることを、確認していますか。(6.5)	□

簡易版自己問診票の設問の紹介（抜粋）

PCIDSSの要件（原文）

【12.6】
正式なセキュリティに関する認識を高めるプログラムを実施して、すべての担当者がカード会員データセキュリティの重要性を認識するようにする。

（12.6.1）
雇用時および少なくとも年に一度担当者を教育する。

（12.6.2）
セキュリティポリシーおよび手順に目を通して理解したことについての同意を、少なくとも年に一度担当者に求める。

簡易自己問診票の設問

1 （12.6）
店頭でクレジットカードを取り扱う場合、カードをお客様の視界の範囲内で取り扱わなければならないことをルールに定めていますか。

2 （12.6）
クレジットカードの取扱いガイドラインを含めて、関係する従業者（アルバイトを含む）全員に、採用時および年１回以上の、個人情報保護・セキュリティ研修を行っていますか。

3 （12.6）
従業者への研修は、アンケートや確認テストなどで理解度を測定し、理解不足の人にはフォローアップ教育を行っていますか。

２）ネットスキャンテストサービス

TOPPAN FORMS

ネットスキャンテストサービス

ネット環境が PCI　DSS の要件を満たしているかを確認いただくASVスキャニングツール「バルネラ・アセッサー」

※　日本オフィス・システム株式会社が日本国内で展開

バルネラ・アセッサーの特長

★コンプライアンス上も価値のあるリスク対策

- PCIセキュリティ基準審議会（PCISSC）認定スキャニングベンダ（ASV）
- Control Case 社が開発したスキャンニングツール。米国を中心に世界で100社以上の訪問監査実績

★日本語の診断レポート

- ギャップ分析と対策のアドバイスを、英文と日本語にまとめたレポートを提出

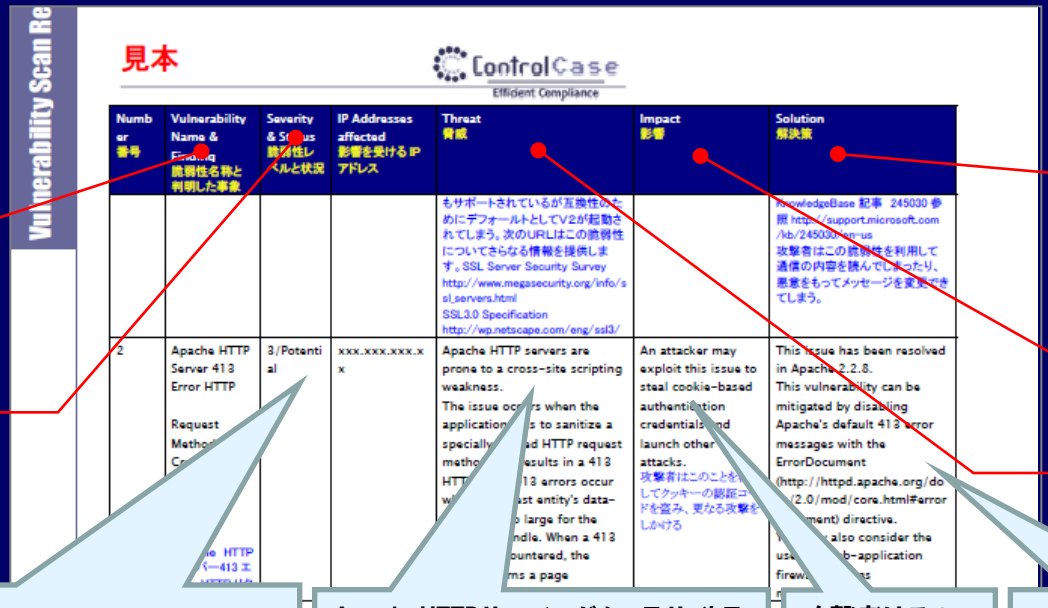
キャンペーン実施中

・1IPアドレス　1回のみに限り **無料診断 実施中**

（2012年12月末日迄　有効）

バルネラ・アセッサー結果報告レポート

＜詳細結果のイメージ(一部抜粋)＞



脆弱性名称と判明した事象

脆弱性レベルと状況

解決策

影響

脅威

レベル5　Urgent(緊急を要す)

侵入者は容易にホストに侵入できてしまい、結果、ネットワークセキュリティ全体の侵害につながります。

レベル4　Critical(重大)

侵入者はホストへの侵入の可能性があり、重要情報の漏えいにつながります。

レベル3　High(高い)

侵入者は、セキュリティのセットなどホスト上の特定の情報にアクセスできる可能性があります。

レベル2　ネットワークに脆弱性存在の可能性

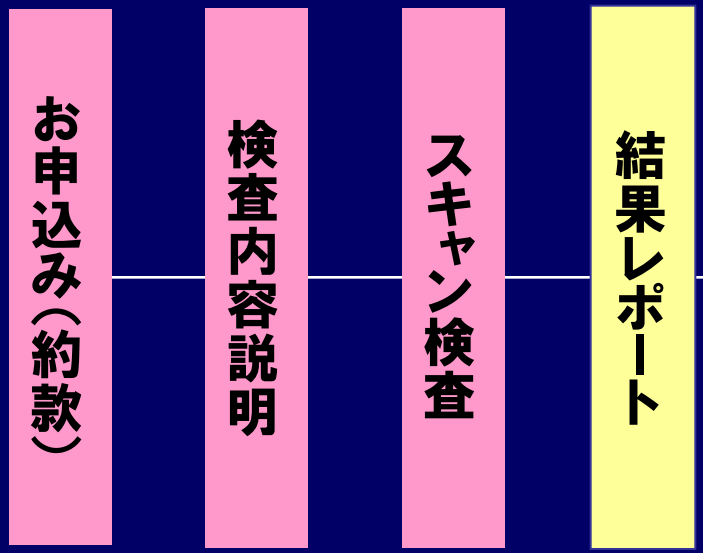
ApacheHTTPサーバーがクロスサイトスクリプティングに対し脆弱です。
この問題は、413HTTPエラーになってしまうような、巧みに工作されたHTTPリクエストをアプリケーションがうまく識別処理できなかったときに起こります。413エラーはリクエスト自体のデータストリームが大きすぎてサーバー処理できないときにおこります。サーバーはこの問題に対したとき起こった自称を記述したページを送り返します。

攻撃者はこのことを利用してクッキーの認証コードを盗み、更ななる攻撃をしかける。

この問題はApache2.2.8では解決されています。この脆弱性はApacheのデフォルト413エラーメールメッセージを使用不能することで緩和できます。

あるいは、アプリケーション用のファイアーウォールを使用することもあわせて考慮してください。

バルネラ・アセッサーのサービス手順



脆弱性
Level3以上

PCI認定まで改善コンサルを実施。

脆弱性の改善⇒再スキャン

※ Level2以下は、基準を満たすレベル

・申込みからスキャン実施まで約10日
・スキャン実施からレポート到着まで約10日

主なテスト項目

1) 不正操作しているパラメータ
2) クッキーPoisoning
3) セッションハイジャック
4) ユーザー特権エスカレーション
5) 認証のごまかし
6) バックドアとデバッグオプション
7) Configuration Subversion
8) Input validation bypass
9) SQL インジェクション
10) クロスサイト・スクリプティング　など

TOPPAN FORMS

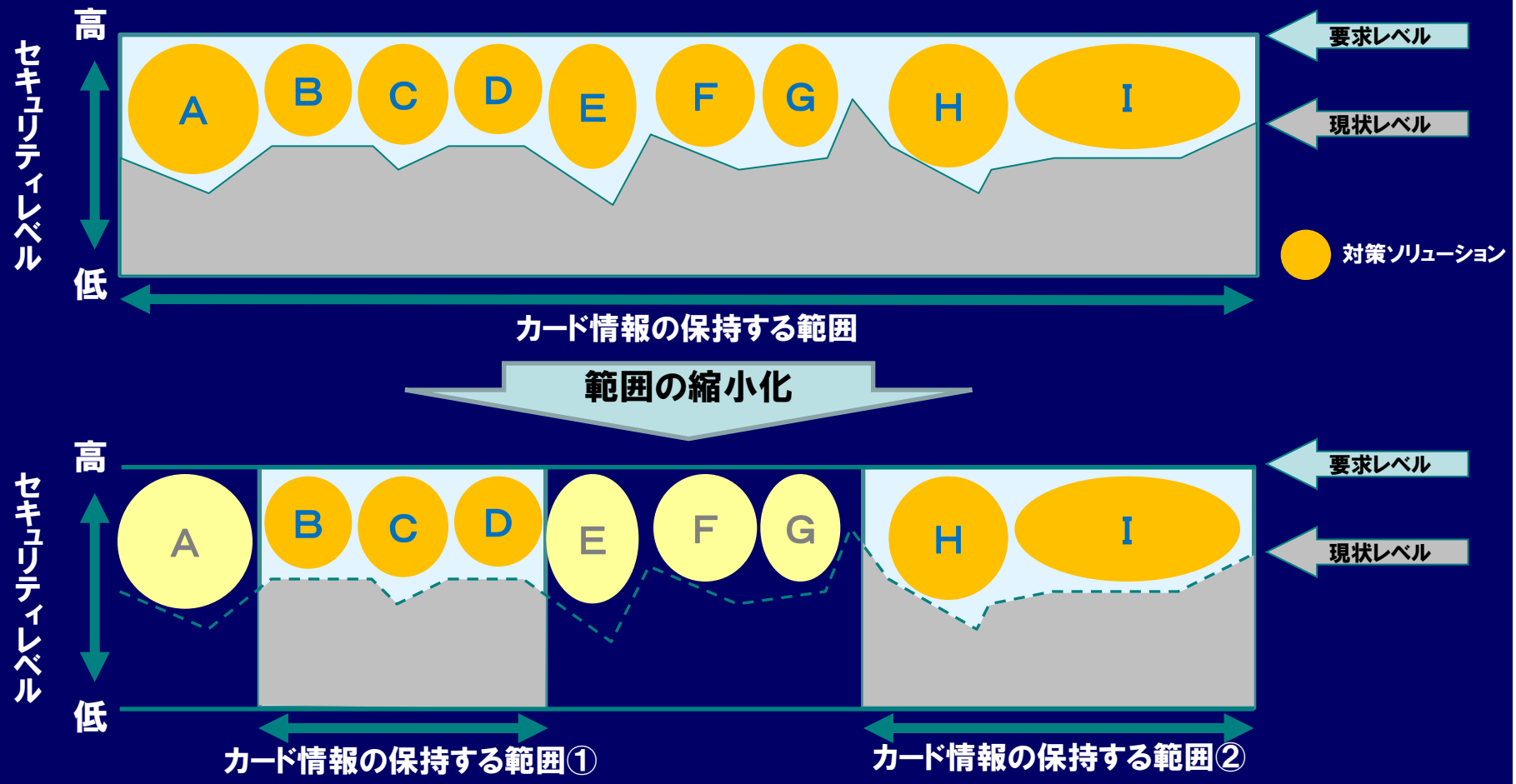
対策の実施

特長2

準拠範囲縮小化の検討と対策

準拠範囲を絞り、対策を取り組むことで
早期実現を可能にする

準拠範囲縮小の考え方（イメージ）



PCIDSSの要件とギャップ分析後、カード情報の範囲縮小をすることで時間短縮とコスト低減

範囲縮小の具体的方法

1. カード情報の非保持

- オーソリ処理から決済処理までをアウトソースすることで準拠範囲を縮小
- クレジット端末での処理

2. トークナイゼーションの導入

- トークンサーバーでカード番号（情報）をトークン番号に変換
- トークン番号が保存、通過するシステムは、準拠範囲外

3. カード情報の縮小化

- ファイアーウォールなどにより、カード情報が必要とされてない範囲へカード情報が流れないように再構築し準拠範囲を縮小

5. まとめ

TOPPAN FORMS

期待できる効果

【特長１】現状確認

- PマークやISMSとPCIDSSの違いや、PCIDSSで定めてる基準を理解
- 簡易自己問診票およびネットスキャン　テストサービスを利用により、PCI DSSの要件に対するギャップを発見

【特長２】準拠範囲縮小の検討対策

- トータルコストの削減が可能
- 早期にPCIDSS準拠

ご清聴ありがとうございます。

下記お問い合わせ先まで、ご連絡ください。

お問い合わせ先

トッパン・フォームズ株式会社
東京都港区東新橋1－7－3

企画本部　TEL（03）6253－6697
営業推進本部　TEL（03）6253－9366