

PCI DSS 最新情報と セキュリティ国際標準の企業への活用

PCI DSS とは

Payment Card Industry Data Security Standardとは、国際クレジットカードブランドが、カードビジネス関連事業者向けに、**カード会員情報**を保護するためのセキュリティ対策の最低水準(ベースライン)を確立するために策定した実装要求規格。

Web好評連載中！

日経BP社 Itpro

総合トップ 情報システム 業務アプリのトレンドを追う

セキュリティ基準「PCI DSS」

<http://itpro.nikkeibp.co.jp/article/COLUMN/20080407/298166/?ST=system>

ソフトバンク ビジネス+IT

トップ セキュリティ ITコンプライアンス

「PCI DSSから学ぶグローバルセキュリティ標準」

<http://www.sbbit.jp/article/9136/>



価格 : 2,940円(税込み)
判型 : B5変形判 / 約247ページ
ISBN : 4-8222-6223-5
発行 : 日経BP社
発売 : 日経BP出版センター
2008年4月14日発行

PCI DSS とは

	PCI DSS	PA-DSS	PED
正式名称	Payment Card Industry Data Security Standard	Payment Application Data Security Standard	PCI PIN Entry Device
基準概要	カード会員データに対するデータセキュリティ基準	ペイメントアプリケーション・ソフトに対するデータセキュリティ基準	POSデバイス等に対するセキュリティ基準。以下の2つの基準で構成 ・ PCI POS PIN Entry Device Security Requirements ・ PCI Encrypting Pin Pad (EPP) Security Requirements
対象	クレジットカード情報を取り扱う事業者	支払いアプリケーションを開発するソフトウェア・ベンダー	POSを開発する製品ベンダー
バージョン	Ver 1.2	Ver 1.1	Ver 2.0
リリース	2008年10月	2008年4月	2007年7月
項目数	6つのセキュリティ目的 12のセキュリティ要件	14のセキュリティ要件	POS PED- 6領域 40項目 EPP - 4領域 32項目
備考			準拠製品のリストが公開中

PA-DSS

■ PA-DSS対象のアプリケーション

- ソフトウェアベンダーによるカスタマイズが不要のパッケージのペイメントアプリケーション

■ PA-DSS対象外のアプリケーション

- 特定顧客向けにカスタマイズされたペイメントアプリケーション
- サービスプロバイダや加盟店内部で使用される社内業務用アプリケーション

■ PA-QSAによる審査

- PCISSCが認定したトレーニングを受けた認定評価担当者 (PA-QSAs) によって実施される
- いい加減な報告を行ったPA-QSAsに対する罰金制裁

■ テストラボでの製品検証

- PA-QSAsはペイメントアプリケーションの審査時にQSA,もしくはベンダーのテストラボで手順に従い検証を実施する
- 認定製品リストへの掲載
- PCI SSCのWebサイトにて2008年9月30日以降に掲載予定

■ 認証期間は1年間

- 毎年再審査が必要

PA-DSSのセキュリティ要件(仮訳)

1. 磁気ストライプのすべての情報、カード認証コードや値(CAV2,CID,CVC2,CVV2)やPINブロックデータを保管しないこと
2. 保存されたカード会員データを安全に保護すること
3. 安全な認証機能を提供すること
4. ペイメントアプリケーション(PA)の動作ログを記録すること
5. 安全性の高いPAを開発すること
6. 無線伝送を保護すること
7. PAをテストし、脆弱性へ対処すること
8. 安全なネットワークの実装を促進すること
9. カード会員データはインターネットに接続されたサーバに決して保存しないこと
10. 安全なリモートからのソフトウェア・アップデートを促進すること
11. PAへの安全なリモートアクセスを促進すること
12. 公衆ネットワーク上のセンシティブなトラフィックを暗号化すること
13. 非コンソール管理アクセスはすべて暗号化すること
14. 顧客、リセラー、インテグレーター向けの教育用ドキュメントとトレーニングプログラムを整備すること

参照: PA-DSS Security Audit Procedures 拙訳

https://www.pcisecuritystandards.org/pdfs/pci_pa-dss_security_audit_procedures_v1-1.pdf

PCI-DSS

1 ダースの要求事項

安全なネットワークの構築・維持	要件 1：カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること 要件 2：システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと
カード会員データの保護	要件 3：保存されたカード会員データを安全に保護すること 要件 4：公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
脆弱性を管理するプログラムの整備	要件 5：アンチウイルス・ソフトウェアを利用し、定期的に更新すること 要件 6：安全性の高いシステムとアプリケーションを開発し、保守すること
強固なアクセス制御手法の導入	要件 7：カード会員データへのアクセスを業務上の必要範囲内に制限すること 要件 8：コンピュータにアクセスする利用者毎に個別の ID を割り当てること 要件 9：カード会員データへの物理的アクセスを制限すること
定期的なネットワークの監視およびテスト	要件 10：ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること 要件 11：セキュリティシステムおよび管理手順を定期的にテストすること
情報セキュリティー・ポリシーの整備	要件 12：情報セキュリティーに関するポリシーを整備すること

PCI-DSS

■ 自己責任のISMS vs PCI DSS

「パスワードの選択及び利用時に正しいセキュリティ慣行に従うことを利用者に要求しなければならない。」ISO/IEC27001:2005 (JIS Q27001:2006)

■ 要件 8 : コンピュータにアクセスする利用者毎に個別の ID を割り当てること

- 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を使用しないこと。
- 8.5.9 ユーザー・パスワードは少なくとも90 日ごとに変更する。
- 8.5.10 最小パスワード長は少なくとも7 文字以上にする。
- 8.5.11 数字と英字の組合せから成るパスワードを使用する。
- 8.5.12 直近4回に使用されたのと同じパスワードは、新しいパスワードとして 使用できないようにする。
- 8.5.13 ユーザーIDをロックアウトすることにより、連続したアクセス試行を6回以内に制限する。
- 8.5.14 ロックアウト時間は30分間、またはアドミニストレータがユーザーIDを有効にするまでとする。

本日のアジェンダ

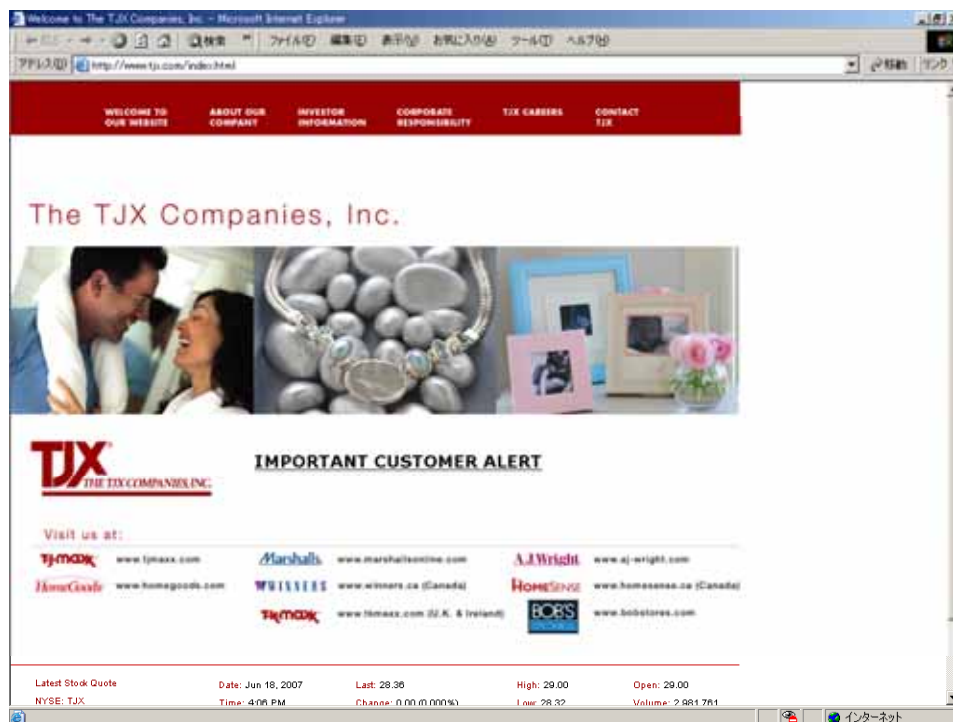
- 1 . 事例が示すPCI DSSの導入意義
- 2 . PCI DSSは、普及するか
- 3 . PCI DSS最新バージョン
- 4 . PCI DSSと10の神話
- 5 . 導入が求められるエンタープライズDSS

1. 事例が示すPCI DSSの導入意義

事例が示すPCI DSSの導入意義

■ 相次ぐ大量のカード情報漏洩事件

- TJX 4500万人のクレジットカードデータ漏洩
- ## ■ 増大するカード不正使用にともなうコスト増
- ## ■ 急がれるブランド・プロテクション対策



被害総額
86億 \$
! ?

事例が示すPCI DSSの導入意義

■ 相次ぐSQL injection 攻撃

「アイドラッグストア」「アイビューティーストア」などネット通販を展開するオズ・インターナショナルのウェブサイトが中国国内から行われたSQLインジェクション攻撃を使用した不正アクセスを受け、カード情報など個人情報情報が漏洩した。クレジットカード番号や有効期限、ログインパスワードが流出しており、カードの不正利用も発生している。同社では今回の流出を受け、クレジットカード情報を削除した。



■ 不正アクセスに関するお詫びとお知らせ 2008年5月20日

6. 今回の不祥事は一切私代表取締役社長、大関和樹の監督責任であり、お客様の信頼に背く形となりました事を、真摯にお詫び申し上げます。この件を受けまして**米国最高の強固なハードウェア、ソフトウェアを採用し、強化をいたしました。**引き続き改善に全力投入してまいります。弊社はいつでもお客様をお守りするのが基本であり、今回の事件を深く反省し顧客満足の向上を今後更に頑張る参ります。

事例が示すPCI DSSの導入意義

■ 不正アクセスに伴うお客様情報流出に関するお詫びとお知らせ

2008年4月18日

株式会社サウンドハウス 代表取締役社長 中島尚彦 様

(全22ページ<http://www.soundhouse.co.jp/news/20080418.pdf>)

■ 事件の経過

2008年3月21日

クレジットカード会社2社が突然来社、サウンドハウス利用者のクレジットカードの不正利用があり、ハッキングされている可能性を指摘

2008年3月30日

調査の結果「SQLインジェクション」による顧客情報流出を確認

情報流出対象者 最大97,500名

2007年1月1日から 2008年3月22日までに新規会員登録した122,884名全員に補償として1,000円分のクレジット進呈

事例が示すPCI DSSの導入意義

■ お客様からの指摘「個人情報管理が甘かったのではないか」

- 通常、企業が取るべき対策は取っており、完璧ではないが、落ち度があったと言えるレベルでもない
- FW導入率14.4% IDS導入率12.1% 警察庁調査報告書(2008年2月)

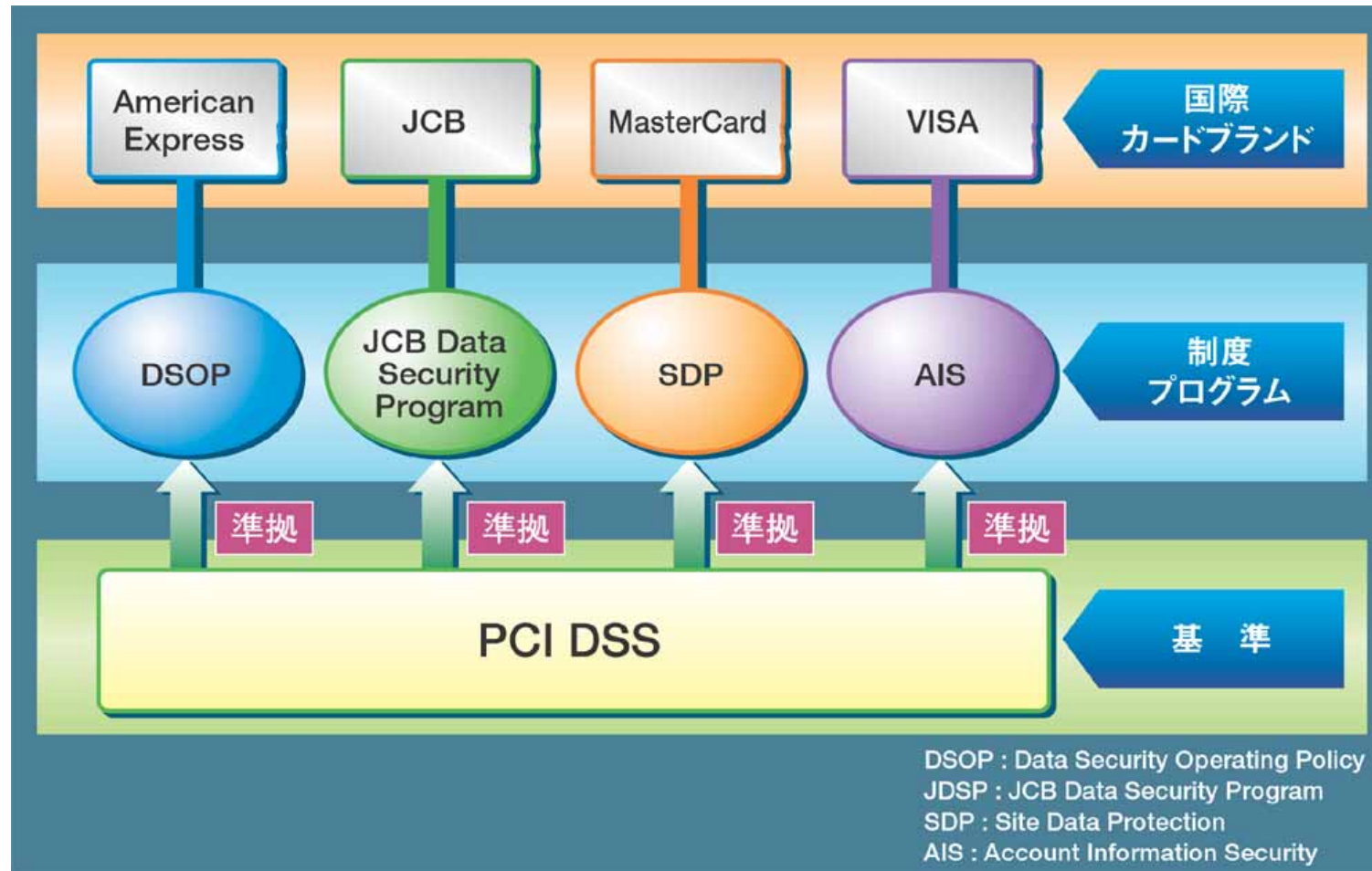
■ 「単に一企業のみではなく

…(中略)…本来ならば、クレジットカードの取扱を開始するにあたって、インターネットセキュリティ構築のガイドラインがあってしかるべきであり、少なくとも最低限のセキュリティレベルが明示されているべきです。ところが、どこまであれば十分か、という明確な基準が無いため、加盟店は、それぞれが独断で実行している部分があることを否認しません。」

2 . PCI DSSは、普及するか

国際カードブランド各社の普及施策

■ 国際カードブランド各社の普及施策プログラム



出典:ソフトバンク ビジネス+IT「PCIDSSから学ぶグローバルセキュリティ基準」

国際カードブランド各社の普及施策

■ テキサス州 CSHB3222 (2007年5月)

- PCIDSSに準拠しておらず漏洩事件・事故を起こした場合、金融機関は損害賠償訴訟を起こすことができる
 - 直接的損害
 - 弁護士費用
 - アクセスデバイスの取り消しならびに再発行費用
 - 口座の閉鎖、支払い停止、口座再開費用
 - 不正により生じた損害の口座開設者への返金費用
 - 口座開設者への通知費用
 - 金融機関が被った全ての費用
- 事件・事故を起こした組織は90日以内にPCIDSSに準拠していた事を証明する証明書を提出しなければならない。30日以内に証明できれば訴訟を免れる

国際カードブランド各社の普及施策

■ 続々と提出されるPCIDSS義務化法案

- マサチューセッツ州(2007年2月)
- ミネソタ州 Plastic Card security Act(2007年4月)
- カリフォルニア州 AB779(2007年5月)

■ Safe Harbor(免責事由)か Regulation(法規制)か

- 求められるスキームの転換



法律



民が策定した
ガイドライン

国際カードブランド各社の普及施策

■ VISA PCI DSS遵守に期限を設定(2008年11月13日)

Visaは、本日、ペイメントカード業界のデータセキュリティ基準(PCI DSS)遵守の国際的な義務化に向けたタイムラインを発表しました。これにより、加盟店、サービスプロバイダおよびプロセッサにおける基準の遵守に必要な統一された枠組みが整いました。

レベル1 / 2の加盟店向け保管禁止データの廃棄期限 2009年9月30日

Visaは、アクワイアラに対し、レベル1 / 2加盟店が全磁気ストライプデータ、セキュリティコード又はPINデータを含むセンシティブなカード関連情報を取引認証後に保管していないことを確認、報告する期限を2009年9月30日としています。

期限経過後、Visaは必要なリスク管理施策を実施します。例えば、レベル1 / 2加盟店が保管禁止データを保管していないことの証明書をアクワイアラがVisaに対し提出しなかった場合、罰金が科されることもあります。

レベル1加盟店向けPCI DSS遵守バリデーションの期限 2010年9月30日

Visaは、アクワイアラに対し、レベル1加盟店のPCI DSS完全遵守バリデーション完了の遵守証明書を提出する期限を2010年9月30日としています。2010年9月30日以降、Visaは必要なリスク管理施策を実施します。例えば、レベル1加盟店のPCI DSS完全遵守バリデーションが完了したことの証明書をアクワイアラが、Visaに対し提出しなかった場合には、罰金が科されることもあります。ただし、それ以前に設定された期限やリスク関連の実施プログラムがある場合には、その限りではありません。

出典: VISAメディアセンター (http://www.visa-asia.com/ap/jp/mediacenter/pressrelease/NR_JP_131108.shtml)

事例が示すPCI DSS普及施策

サウンドハウス ご利用ガイド - Microsoft Internet Explorer

アドレス http://www.soundhouse.co.jp/guide/kaimono.asp

音響機器、楽器、レコーディング、照明機器、ステージ、カラオケ機材の全国通販

PA&レコーディング 楽器 DJ&VJ DTM・DAW デッキ・記録メディア 照明・ステージシステム スタンド各種 ラック&ケース ケーブル各種 ヘッドホン・イヤホン

ご利用案内 | 会社案内 | 採用情報 | NEWS | 掲示板 | 登録の変更 | ウィッシュリスト | カート読込 | カートを見る | TOP | English Guide

検索 お支払い方法にPay-easy(ペイジー)、ジャパンネット銀行、イーバンク銀行が新たに加わりました。

ログイン
新規会員登録
English Guide
Register / Login

ブラウズ
メーカー別
全カテゴリーを表示
衝撃特価品
これっきり大バーゲン
特選推奨品
数量限定特価
アウトレット
ランキング

カテゴリー
PA&レコーディング
ギター
ベース
ドラム&パーカッション
キーボード
その他楽器
DJ&VJ
DTM/DAW

ご利用ガイド

ご注文方法について

- 商品をカートに入れる**
 - ご希望の商品のカートに入れるボタンをクリックし、商品をカートに入れます。
・お買い物を続ける場合は左メニュー、もしくは買い物続けるボタンをクリックしてください。
- ご注文画面に進む**
 - 商品の選定が終わりましたら、カートページもしくは画面右上メニュー内の「カートを見る」から「注文へ進む」をクリックしてください。
次にログイン画面が表示され、ログインすると注文画面へ進みます。
※既にログインしている場合は、そのまま注文内容の確認ページへ進みます。
- 支払方法の選択**
 - 注文内容を確認し、お支払方法を選択してください。

銀行振込の場合	ショッピングローンの場合
オンラインショッピングローンの場合	コンビニエンスストア/ゆうちょ銀行支払の場合
代金引換の場合	
- 配送先の指定**

インターネット

スタート Quick Launch 19:05

2009年02月22日現在

国際カードブランド各社の普及施策

■ アクワイアラ中心の普及施策

Card Brand

国際カードブランド

Issure

カード発行会社

Acquirer

加盟店開拓会社

Merchant

加盟店(小売店)

Service
Privider

情報処理会社

アクアイアラ
への
罰金制裁開始

避けたい
ダブル
スタンダード

■ 普及の妨げになる日本の特殊事情？

- ブランド、カード発行会社、アクアイアラの一体化
- 改正割賦販売法

国内の普及動向

■ 国内のPCI DSS準拠状況

■ 「オンサイトレビュー」「脆弱性スキャンテスト」「自己評価問診」 完了 12社

- SBIベリトランス(2007年3月28日)
- 株式会社NTTデータ(2006年9月21日)
- GMOペイメントゲートウェイ株式会社(2006年6月28日)
- 株式会社ジー・ピー・ネット(2006年6月12日)
- 株式会社ゼウス(2006年7月14日)
- 株式会社ソニーファイナンスインターナショナル(2006年11月17日)
- 株式会社デジタルチェック(2006年11月17日)
- 株式会社日本カードネットワーク(2006年10月19日)
- ヤマトシステム開発株式会社(2006年7月7日)
- 三井住友カード株式会社(2007年9月28日)
- ソフトバンク・ペイメント・サービス株式会社(2006年12月22日)
- 楽天株式会社(2007年12月25日)

参照) http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais_companylist.shtml

国内の普及動向

PCI SSC PO Japan連絡会発足 (2009年2月20日)

The screenshot shows a Microsoft Internet Explorer browser window displaying an article from Enterprise Watch. The article title is "PCI DSSの国内浸透を進める連絡会、8社により発足". The main text discusses the launch of the PCI SSC PO Japan network, a collaboration of eight domestic companies to promote PCI DSS compliance. It mentions that while PCI DSS is an international standard, other standards like PCI PED and PA-DSS are also relevant. The network aims to provide knowledge and practical know-how to various industries. A URL for the news release is provided: <http://www.netone.co.jp/newsrelease/2009/20090220.html>. On the right side of the browser, there are advertisements for GrapeCity's ActiveReports and Fujitsu's FMV 2009 Spring promotion.

Enterprise Watch
最新ニュース
【2009/02/20】
■ PCI DSSの国内浸透を進める連絡会、8社により発足 [19:18]
■ 「仮想化はもろ刃の剣、優れた道のりでの導入を」 - 米 Dell [19:09]
■ 富士通、九州地区の3社を統合 - グループ内でもトップクラスのSE会社 [14:24]
■ ソフトイーサ、3月に終了する「DesktopVPN」の後継サービスを提供 [14:23]
■ アニモ、キーワードで特定音声を検索できる「VoiceTracking / KeywordFinder」 [12:52]
■ アイログ、動的に安全在庫を決定できる生産計画ソフト「LOG PPO 3.1」 [12:23]
■ シーメンスPLMと日本HP、PLMソリューション [12:23]

PCI DSSの国内浸透を進める連絡会、8社により発足

カードセキュリティ基準「PCI DSS」の運営団体「PCI SSC」に参加する国内企業8社(2月20日、関連団体・企業との連携を通じ、クレジットカード情報の安全確保の取組みを推進する「PCI SSC PO Japan連絡会」を発足した。

PCI DSSは、クレジットカード情報を取り扱う企業が順守しなければならない国際基準。このほかにも、POSベンダーなどが対応しなければならない「PCI PED (PIN入力機器基準)」や「PA-DSS (支払アプリケーション基準)」などが、PCI SSCによって定められているが、その理解・浸透にはまだ不十分な状況だ。

そこで同連絡会は、これら基準に対する知識向上・実装ノウハウを必要とする、カード加盟店・金融機関・サービスプロバイダ・POSベンダーなどの幅広い業種の受け皿となり、日本国内における課題を共有。情報交換・技術交流を通じて、クレジットカード情報の保護に積極的に取り組むことを目的としている。

会員企業は、日本ATM、コマタ、eCURE、インテリジェントウェイブ、ラック、ネットワークシステムズ、SBIベリトランス、東芝テック、事務局をネットワークが担当し、会長として、同社 営業推進グループ セキュリティ事業推進部長の山崎文明氏が就任する。

ネットワークは、発足メンバーとしてメンバー間の連携や各団体との交流を行っていくほか、同連絡会の活動を通じて、ペイメントカード業界に限らず、官公庁・自治体・学校法人・事業法人などにも、ISMSなどを補完する実装基準として利用促進する意向。

■ URL
PCI SSC PO Japan連絡会
<http://www.netone.co.jp/pcisscpojapan/>
ニュースリリース
<http://www.netone.co.jp/newsrelease/2009/20090220.html>

■ 関連記事
・ PCI DSSは普及するか？ ダブルスタンダード化などの阻害要因を考える (2008/12/26)

GrapeCity
ふるA HP: 8 MP: 64
ふるB HP: 256 MP: 32
ふるまね HP: 512 MP: 256
.NET専用の帳票作成ツール ActiveReports
Replay ▼

Special Topics
IT業界で転職したい人 専任コンサルタントがきめ細かくサポート!
インプレスキャリアは IT 業界に特化した転職サービスです。業界を熟知した専任コンサルタントが豊富な求人案件をご紹介します。キャリア相談から面接の指南まで、転職をサポートします。まずは登録を!

FUJITSU 2009 春 FMV

3 . P C I D S S 最新バージョン

PCI DSS最新バージョン

- PCI DSSバージョンアップ
 - PCI SSCメンバーの協議によるバージョンアップ
 - 2006年のPCI SSC設立以来、2,000件以上の意見が寄せられている
 - 透明な議論の下に形成されるコンセンサス
 - ネットワンシステムズは、PCI SSCメンバーとしてバージョンアップに関して先行して情報入手が可能かつ提案が可能
 - PCI DSS 1.2
 - 5月14日 バージョンアップに関する発表解禁
 - 6月上旬 PCI SSCメンバーへニュースレターにて告知
 - 7月 現行バージョン1.1との差分に関するサマリー公開
 - 9月上旬 バージョン1.2のプレビュー開始
 - 9月24-25日 年次総会にて承認
 - 10月1日 正式公開

PCI SSC 年次総会

- 2008年9月23日～25日 オーランド(フロリダ州)
- 参加者697名
 - 310社
 - 153社 QSA / ASV / PED
- 拡大するSSC
 - QSA 164社
 - 1000名以上
 - ASV 147社
 - PA - QSA 100名以上
 - PED Lab 8社
 - 認証製品93社 249製品認証
- SSCの組織説明
- PCI DSSの改定ポリシー 2年毎
- 新バージョン解説と意見交換
- QSA監査制度の説明



PCI S S C 年次総会

■ バージョン1.2改定の目的

- 要求事項の明確化
- 柔軟な対応方法の提供
- 進化する脅威とリスクへの対応
- ベストプラクティスの取り込み
- 適用範囲と報告の明確化
- 冗長な要求事項の排除
- 文書類の統合

■ 厳しさを増すQSAの選別

- QSAへの被監査対象からの評価報告の義務化
- QSAへの監査制度導入

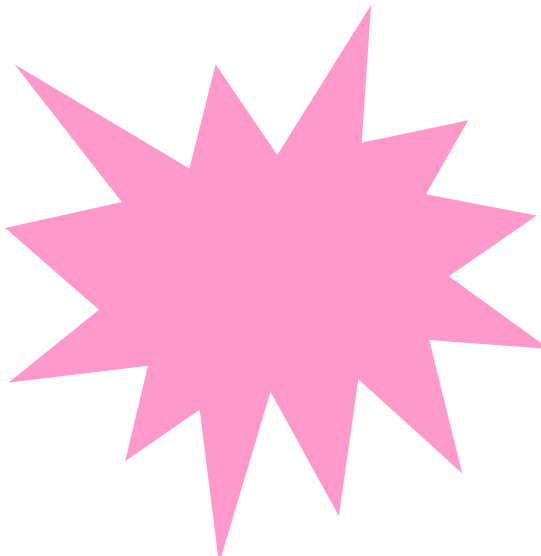
PCI DSS Version 1.2

■ 主な改定内容

- FWの設定レビュー 4半期毎 → 6ヶ月毎
- IEEE802.11iの実装要求
- WEPの使用禁止 2009年3月31日以降の新規導入禁止
2010年6月30日以降の使用禁止
- 外部との接点を持つ装置が生成するログの内部サーバーへの複製
- 無線アナライザもしくは無線IDS/IPSの導入

■ 現行Version1.1は12月末で無効

- 新規QSA監査は12月までは、1.1の使用可
- 既QSA認証取得組織は、次回監査までに要準拠



高まる
無線環境
のリスク

DSSに関する米国での最新の話題

■ 仮想化された環境でのPCI DSSコンプライアンス

- ZERO guidance virtualization'role
 - SOX,HIPAA,GLBA..... PCI DSS What dose your QSA say?
It depends.....

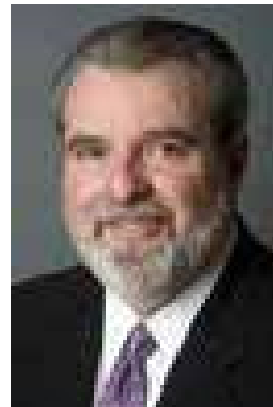
■ QSAの厳格な審査品質の均一化と向上

- QSA(Qualified Security Assessor)の品質保証プログラム

InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

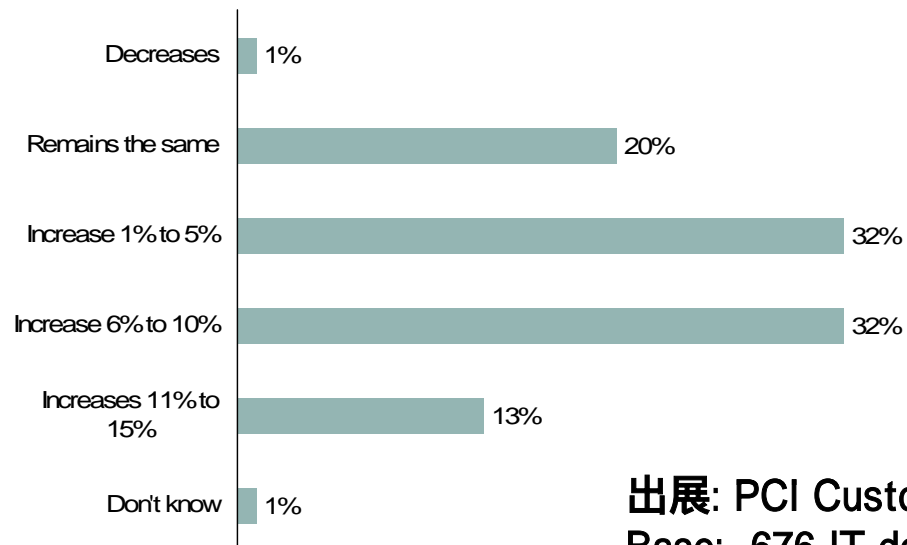
**"The goal is to make sure it's a level playing field so we don't have accusations from QSAs or merchants that some people are rubber-stamping" - Bob Russo
2/23/2008**



DSSに関する米国での最新の話題

■ PCI DSSへの適応コスト IT予算の+5%程度

“What are your organization's current budget trends for supporting/assisting credit card data protection for the next 12 months?”



出展: PCI Custom Study, Forrester Consulting, July 2007
Base: 676 IT decision makers

■ いかに低コストでPCI DSSに適合させるか

- スコープの限定
- 審査時の説明時間の短縮
 - 既存ドキュメントの有効活用

DSSに関する米国での最新の話題

- **ベンチマークとしてのPCIDSS**
 - クレジット決済に関係なく実装基準としての活用
 - 第三者への説明責任
 - ・ 「カード会社なみのセキュリティ対策」
- **サプライチェーンリスクの低減**
 - 「ISMSの認証取得していますか？」で十分か？
 - 実装基準の確約で高まる信頼関係

12.8 If cardholder data is shared with service providers, then contractually the following is required:

12.8.1 Service providers must adhere to the PCI DSS requirements

- **企業間の結びつきを益々深化するIT技術と脅威**
 - XMLコンピューティング、XMLルーター、DRM
 - Web2.0ハッキング、NGNハッキング

4 . P C I D S S と 1 0 の 神 話

PCI DSSと10の神話

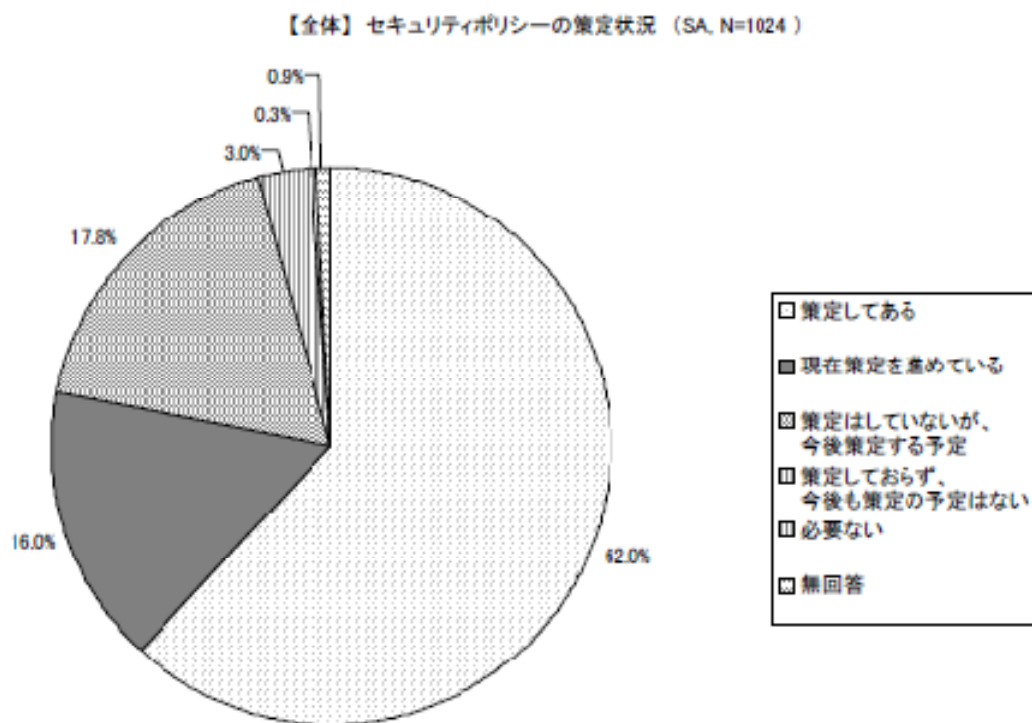
1. 「単一ベンダー・単一製品で準拠を実現できる」
2. 「カード決済代行をアウトソースすれば準拠できる」
3. 「PCI準拠はITプロジェクトである」
4. 「PCIがあればセキュリティは万全である」
5. 「PCIは実情にあわない～要求があまりに多すぎる」
6. 「PCI準拠にはQSA (Qualified Security Assessor) を雇う必要がある」
7. 「カード会員データを多く取り扱っていなければ準拠する必要はない」
8. 「自己評価問診を実施すれば準拠は完了する」
9. 「PCIはカード会員データを保存すべきといている」
10. 「PCI準拠はとても難しい」

5. 導入が求められるエンタープライズDSS

導入が求められるエンタープライズDSS

ISMS 95.8%の企業が導入

- 東証1部2部、店頭、通信、医療、教育、行政
- 策定済62.0% 策定中16.0% 策定予定17.8%



それでも
止まない
情報漏洩

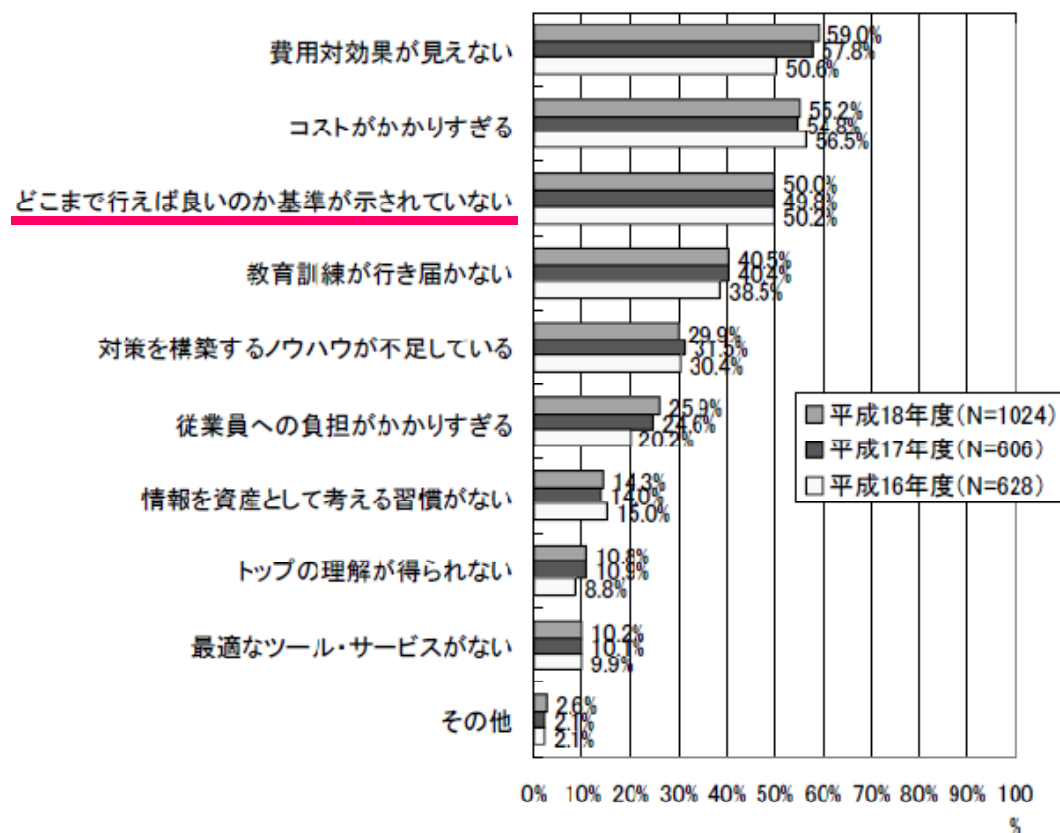
「平成19年1月不正アクセス対策等の実態調査（警察庁生活安全局情報技術犯罪対策課）」より抜粋

導入が求められるエンタープライズDSS

ISMSを導入してはみたものの

- 半数の企業は何をどこまでやればいいのかわからない

【経年変化】情報セキュリティ対策実施上の問題点



日本人が
最も苦手な
自己責任

「平成19年1月不正アクセス対策等の実態調査（警察庁生活安全局情報技術犯罪対策課）」より抜粋

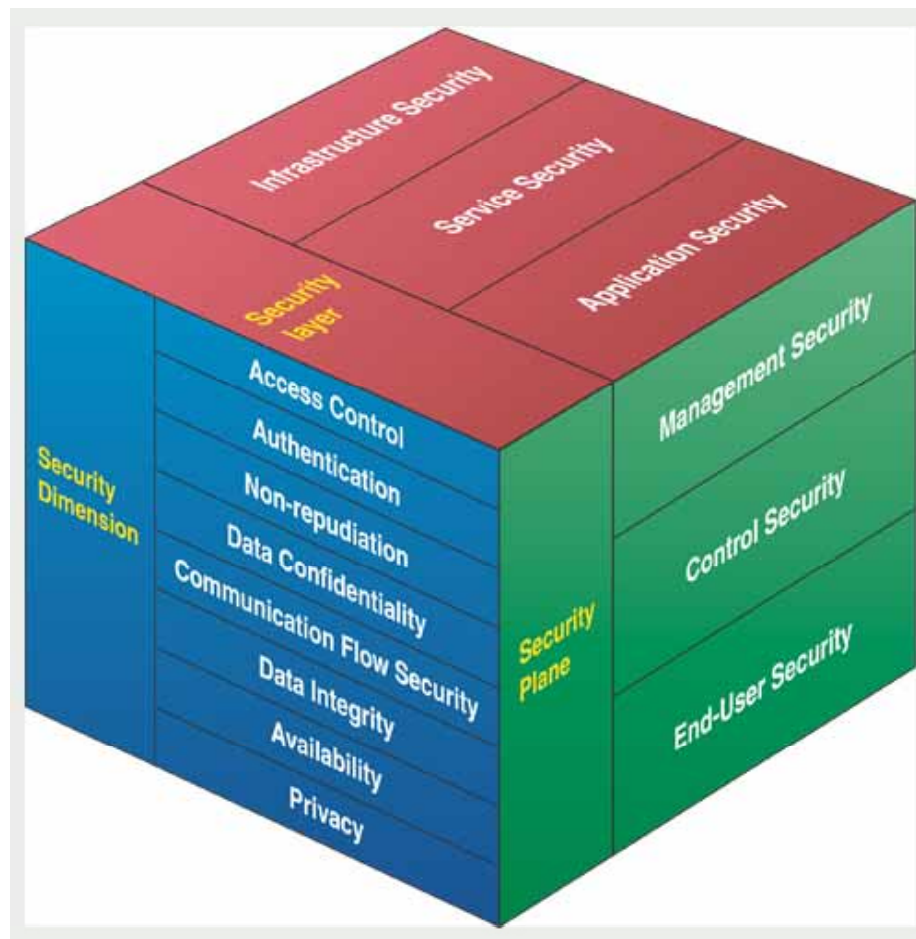
導入が求められるエンタープライズDSS

- 何をどこまでやればいいのか適切に判断できていない現実
 - わかりやすい説明責任 クレジットカード会社なみのセキュリティ対策
- エンタープライズとして各社のポリシーに委ねていて良いのか
 - セキュリティ対策のボトムラインを明確に関係会社に要求
 - 実装レベルのエンタープライズ標準仕様を固める時期
 - 欧米のエンタープライズでは使用製品まで規定
 - 12.3.7 Verify that the usage policies require a list of company-approved products.
- GAP分析が示す今後の道筋
 - あと幾ら投資が必要かは経営にとって重要な情報
- 入札仕様としても活用できるDSS

Enterprise Data Security Standard

導入が求められるエンタープライズDSS

- ISO 27033 (ISO 18028) をベースにしたDSS策定アプローチ



出典:ソフトバンク ビジネス+IT「PCIDSSから学ぶグローバルセキュリティ基準」

自己紹介



価格 : 9,975円(税込み)
判型 : B5変形判 / 約280ページ
ISBN : 4-8222-2131-8
発行 : 日経BP社
発売 : 日経BP出版センター
2004年10月1日発行

山崎 文明(やまさき ふみあき)

ネットワンシステムズ株式会社セキュリティ事業推進本部長
ビジネスアシュアランス株式会社 代表取締役社長
工学院大学 技術者能力開発センター客員講師
システム監査技術者(経済産業省)
英国規格協会 BS7799情報セキュリティ・スペシャリスト
(元)内閣官房 安全保障危機管理室 情報セキュリティ対策推進室WG委員
(元)警察庁不正アクセス犯罪等対策専科講師
平成19年度学校セキュリティ検討委員会委員
平成18年度学校セキュリティ検討委員会委員
平成17年度学校セキュリティ検討委員会委員
平成16年度経済産業省サイバーテロ実験評価委員
平成13年度警察庁不正プログラム調査研究委員会委員
平成12年度警察庁サイバーセキュリティ調査研究委員会委員



価格 : 1,680円(税込み)
判型 : 四六判 / 272ページ
ISBN : 4-8222-2061-3
発行 : 日経BP社
2005年1月11日発行

警察政策学会正会員

日本リスク・マネジメント学会正会員

システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。
大手会計監査法人にてシステム監査に永年従事。

著書に、「PCIデータセキュリティ基準 完全対策」(日経BP社)「すべてわかる個人情報保護」(日経BP社)、「情報セキュリティハンドブック」(オーム社)、「情報セキュリティと個人情報保護 完全対策」(日経BP社)、「システム監査の方法」(中央経済社)、「コンティンジェンシー・プランニング」(日経BP社)、「セキュリティマネジメント・ハンドブック」(日刊工業新聞社)等がある。



価格 : 2,940円(税込み)
判型 : B5変形判 / 約247ページ
ISBN : 4-8222-6223-5
発行 : 日経BP社
発売 : 日経BP出版センター
2008年4月14日発行