PCIDSS 準拠の現実とベストプラクティス

～よくある誤解や課題、陥りがちな落とし穴の事例解説～

The power to do more

2014年7月

小川 真毅, PCI QSA, CISSP, CISA, CISM, CBCI, CCSK, PMP

プリンシパル コンサルタント

セキュリティ＆リスク コンサルティング

Dell SecureWorks

Dell SecureWorks について

Dell SecureWorks の概要

- 15年以上のサービス提供実績
- 2009年、VeriSign社からマネージドセキュリティサービス（MSS）事業を買収
- 2011年、Dell のサービス事業部門に統合
- 全世界で3,800社以上のお客様にサービスを提供
- マネージドセキュリティサービス、コンサルティング、情報分析に関してあらゆるサービスをグローバルで提供
- 世界有数の調査チーム「Counter Threat Unit℠」（セキュリティ上の脅威への対策部隊）を保持
- 1日あたり380億件のログ処理実績を誇るMSSを、世界7箇所のSOC（セキュリティ・オペレーション・センター）で運営
- GIAC GCIA など各種の専門認定を取得したセキュリティ・アナリスト
- ベンダー・ニュートラルのサポート
- 業界での高い評価とアワードの受賞

SC MAGAZINE AWARDS 2006 WINNER
SC MAGAZINE AWARDS 2007 WINNER
SC MAGAZINE AWARDS 2008 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2009 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2011 WINNER Honored in the U.S.
SC MAGAZINE AWARDS 2012 WINNER Honored in the U.S.

DELL SecureWorks

セキュリティ脅威をグローバル規模で可視化

70+ ケ国

3,800+ 社のお客様

1,000+ のセキュリティ専門家

200+ のソフトウェアエンジニア

15万台+ デバイス監視

760億+ 1日のサイバーイベント

3,000+ 1日の報告

24 x 7 x 365

Dell SecureWorks サービスの全容

MSS	CTU	Consulting
マネージド・セキュリティ・サービス	**スレット・インテリジェンス**	**セキュリティ＆リスク・コンサルティング**
世界最大級の監視サービス	世界有数の調査チーム	豊富な経験と実績
➢ IDS/IPS 管理 ➢ Firewall 管理 ➢ Web Application Firewall 管理 ➢ ログ・モニタリング ➢ 脆弱性管理 ➢ Web Appスキャニング ➢ オンデマンドのSIM (セキュリティ情報管理) ➢ HIPS ➢ ログ管理	➢ 脅威&脆弱性情報 ➢ アドバイザリ情報 ➢ 拡大中の脅威速報 ➢ マイクロソフト更新プログラムの分析 ➢ 情報分析ブリーフィング ➢ 隔週の総合サイバーセキュリティニュース ➢ マルウェアの分析 ➢ CTU サポート ➢ 攻撃者DBの提供	➢ テスト&アセスメント ➢ コンプライアンス & セキュリティ認定 ➢ インシデント対応&原因調査 ➢ ポリシー開発・実装 ➢ アーキテクチャ・デザインと実装 ➢ 専門家の常駐

PCI 業界における Dell SecureWorks の強み

世界最大規模のPCI業界認定機関	QSA (Qualified Security Assessor:認定審査機関) ASV (Approved Scanning Vendor: 認定スキャニングベンダー) PFI (Payment Forensics Investigator: 認定フォレンジック調査機関)
PCI業界リーダーとしての活動と実績	PCI業界コミュニティにおけるグローバルな活動参画と世界中でのPCIDSS関連サービス提供実績
業界プロフェッショナル集団	平均10年以上の業界経験を持つセキュリティコンサルタントが持つ豊富なナレッジを融合して、最適な改善案やアドバイザリーを提供
セキュリティリスク分析における専門性	インシデント対応やフォレンジック解析サービスを通じたセキュリティリスクと技術動向に関する深い理解とPCI要件の柔軟な解釈に基づく的確な分析

数字で見る Dell SecureWorks PCI サービス実績

Dell SecureWorksは、豊富な PCI DSS 準拠支援および審査実績に基づき、多様なお客様環境にとって最適な対策と運用環境の構築を支援することができます

100社＋

QSAとして過去に審査し、準拠報告書を提供したPCIDSS準拠企業の数

100社＋

QSAとして過去に準拠支援コンサルテーション(ギャップ分析)サービスを提供した企業の数

300社＋

ASVとして脆弱性スキャンを提供したPCIDSS準拠企業の数(マネージドセキュリティサービス利用企業含む)

50名＋

PCIDSS準拠支援コンサルテーションを提供可能なQSA有資格者およびセキュリティコンサルタントの数

PCIDSS 準拠にあたり、よくある誤解

PCIDSS への準拠はなぜ重要か

損害賠償

顧客信頼低下

ブランドイメージ低下

取引停止

- 不正被害や漏えい事件が発生した場合、影響を受けた顧客への補償や法的責任が追及される。
- 新たな脅威と犯罪行為の増加に伴い、漏えい事件は即座にメディアに取り上げられ、センセーショナルな報道によりブランドイメージの失墜が懸念される。
- 非準拠状態の場合、国・地域によっては罰金、罰則、取引停止などの措置を採られる場合がある。
- 日本国内では、JCA(日本クレジット協会)が、2017年度末までにすべての加盟店が準拠すべきという方針(ナショナルプラン)を打ち出しており、EC事業者の準拠期限はすでに過ぎている(2013年3月末)
- また、PCIDSS への準拠は、改正割賦販売法(2010年12月施行)に基づく事実上の法的義務になりつつある。

よくある誤解①

準拠が必要なほど
クレジットカードは取り扱っていない

ある加盟店担当者の声

『ほとんどが現金決済または銀行振り込みなので、クレジットカードでの決済は週に1回ぐらいしかありません。この場合は対象外でいいですよね？』

加盟店／決済サービスプロバイダの要件

PCIDSS はカード会員データを保存、処理、伝送する
すべての加盟店やサービスプロバイダが準拠する必要がある

業態	レベル決定条件	準拠要件	認定機関
加盟店レベル 1	年間トランザクション600万件以上	• 毎年のオンサイト審査 • 外部IPアドレスに対する四半期ごとのスキャン	• 認定セキュリティ機関 (QSA: Qualified Security Assessor) または内部監査者(組織の役員の署名がある場合) • 認定スキャニングベンダー (ASV: Approved Scan Vendor)
加盟店レベル 2	年間トランザクション100万件以上600万件未満	• 毎年の自己問診票 • 外部IPアドレスに対する四半期ごとのスキャン	• 加盟店 (自己査定) • 認定スキャニングベンダー (ASV: Approved Scan Vendor)
加盟店レベル 3	年間電子商取引トランザクション2万件以上100万件未満		
加盟店レベル 4	年間トランザクション100万件未満または電子商取引2万件未満	• 毎年の自己問診票 • 外部IPアドレスに対する四半期ごとのスキャン	• 加盟店 (自己査定) • 認定スキャニングベンダー (ASV: Approved Scan Vendor)
サービスプロバイダ レベル 1	年間トランザクションが30万件を超える	• 毎年のオンサイト審査 • 外部IPアドレスに対する四半期ごとのスキャン	• 認定セキュリティ機関 (QSA: Qualified Security Assessor) • 認定スキャニングベンダー (ASV: Approved Scan Vendor)
サービスプロバイダ レベル 2	年間トランザクション30万件以下	• 毎年の自己問診票 • 外部IPアドレスに対する四半期ごとのスキャン	• サービスプロバイダ (自己査定) • 認定スキャニングベンダー (ASV: Approved Scan Vendor)

よくある誤解②

すべてアウトソースしているので
自社として準拠の必要はない

ある加盟店担当者の声

『弊社のECサイトはシステムから運用まですべてアウトソースしていて、社内にはカード番号も保管していません。この場合は準拠する必要がないですよね？』

アウトソース先サービスプロバイダに対する要件

アウトソース先サービスプロバイダの PCIDSS 準拠状態を管理・監督する義務は残る

No	要件
12.8	カード会員データがサービスプロバイダと共有される場合は、次の項目を含め、サービスプロバイダを管理するポリシーと手順を維持および実装する。
12.8.1	サービスプロバイダのリストを維持する。
12.8.2	サービスプロバイダは、プロバイダが、顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について責任を持つことを認める内容の書面による契約書を維持する。 注: 同意の正確な言葉づかいは、提供されるサービスの詳細、各事業体に割り当てられる責任など、2 つの事業体間の同意よって異なります。同意の正確な言葉づかいに、この要件で提供されているのと同じものを含める必要はありません。
12.8.3	契約前の適切なデューデリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されている。
12.8.4	少なくとも年に一度、サービスプロバイダのPCI DSS準拠ステータスを監視するプログラムを維持する。
12.8.5	各サービスプロバイダに対し、どのPCI DSS要件がサービスプロバイダによって管理され、どのPCI DSSが事業体によって管理されるかについての情報を維持する。

よくある誤解③

PCIDSS への準拠は
IT部門に任せておけばよい

ある加盟店担当者の声

『PCIDSSはデータの保護が目的なので、総務部の私には関係ないですよね？』

PCIDSS準拠の維持に必要な活動

技術的対策以外にも教育や入退室管理など、組織全体に渡る対応が必要です

<table>
<tr><th>運用領域</th><th colspan="3">頻度</th></tr>
<tr><td rowspan="4">技術的</td><td>常時
要件５
• アンチウイルス定義の更新</td><td rowspan="3">３ヶ月ごと
要件３
• 不要なカード会員データの削除
要件１０
• 監査証跡のオンライン保管
要件１１
• 不正な無線アクセスポイントの検出
• 外部脆弱性スキャン（ASVによるスキャン）
• 内部脆弱性スキャン</td><td rowspan="4">１年ごと
要件３
• キー暗号化キーの変更（推奨）
要件６
• Webアプリケーション脆弱性診断
要件１０
• 監査証跡のオフライン保管
要件１１
• 外部/内部ペネトレーションテスト</td></tr>
<tr><td>１日ごと
要件１０
• すべてのシステムコンポーネントのログ確認</td></tr>
<tr><td>１週間ごと
要件１１
•重要ファイルの整合性監視</td></tr>
<tr><td>１ヶ月ごと
要件６
•重要なセキュリティパッチのインストール
要件８
•不要なアカウントの削除、パスワードの変更</td><td>６ヶ月ごと
要件１
• ファイアウォール設定のレビュー</td></tr>
<tr><td>人的
物理的</td><td>常時
要件１２
• セキュリティ警告への２４時間対応体制</td><td>３ヶ月ごと
要件９
• 監視カメラ記録の保管
• 訪問者記録の保管</td><td>１年ごと
要件９
• 物理媒体保管場所と在庫チェック
要件１２
• 情報セキュリティポリシーのレビュー
• 情報セキュリティ教育と同意
• 外部委託先のPCI準拠ステータス確認
• インシデント対応計画のテスト</td></tr>
</table>

PCIDSS 要件ドメインごとの課題や落とし穴

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インストールして構成を維持する

ファイアウォールに求められる主な機能

(要件1.3.6) ステートフルインスペクション

(要件1.3.8) ネットワークアドレス変換(NAT)

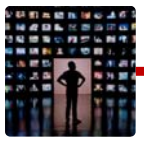
(要件1.3.4) アンチIPスプーフィング v3

注意!!

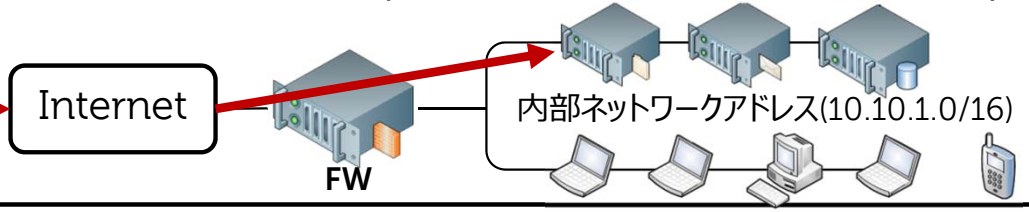
機能として持っていても、デフォルトで有効になっていなかったり、正しく設定されていなければ当然非準拠

IPスプーフィングとは・・・

内部IPアドレスを詐称することで、本来外部からはアクセスできないはずの内部システムに不正にアクセスしようとする行為



攻撃者が本来のアドレス(208.89.41.129)を
内部アドレス(10.10.1.129)に詐称して不正アクセス



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

(要件2.1)
- ベンダ提供のデフォルト値を変更する
- 不要なデフォルトアカウントは無効にする

- **OSだけでなく、ネットワーク機器やアプリケーションの管理者パスワードも変更**
- **無線アクセスポイントへの接続パスワードも変更**
- **SNMPコミュニティストリングを『public/private』のままにしない**
- **OSのGuest アカウントやアプリケーションのデモユーザーは無効にする**

(要件2.2.3) 安全性の低いサービスを保護する

- **FTPは利用せず、SFTPを利用する**
- **Anonymousアクセスは許可しない**
- **管理共有を無効にする**
- **暗号化されていないファイル共有プロトコルは使用しない （SMB3.0やSharepointなどを活用する）**

要件③ カード会員データを保護する

コールセンターにおける会話録音時の注意

大原則

(要件3.1) 不要なCHDは保存しない

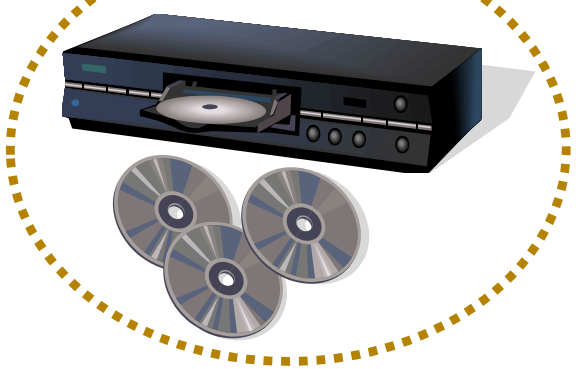
(要件3.2) オーソリ後はSADを保存しない

CHD – Card Holder Data (カード会員番号など)
SAD – Sensitive Authentication Data (CVV/CV2など)

録音

アナログ？

デジタル？



ポイント システム的にCHDが検索可能ならスコープ内であり、対策が必要

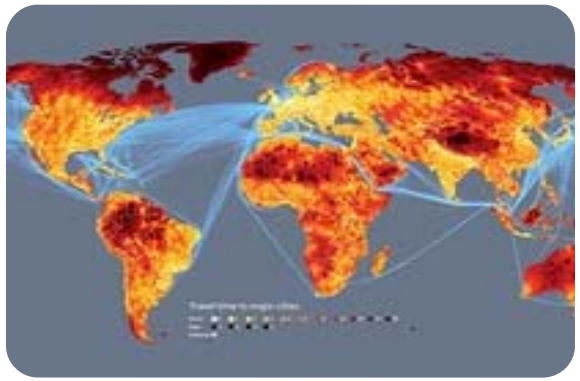
	CHD (カード会員データ)	SAD (センシティブ認証データ)
アナログ	録音可 (スコープ外)	録音可 (スコープ外)
デジタル	録音可 (スコープ内)	録音不可 (スコープ内or外)

要件④ オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

(要件4.1) 公共ネットワークでの通信は強力な暗号化とセキュリティプロトコルで保護する

- **決済ページはすべてHTTPS(SSL)だから保護できている**
- **リモート管理にはSSHを利用しているから安全**
- **無線通信はWEPで暗号化しているから盗聴されない**

- **SSLはバージョン3.0以上またはTLSバージョン1.0以上を利用している**
- **SSHはバージョン2.0以上を利用している**
- **無線通信はWPA2 – PSK(AES)で暗号化している**



注意!!

『暗号化プロトコルを使っている』=『準拠』ではない。

※ こうした脆弱なプロトコルを使用している場合、そもそもASVによる外部ネットワーク脆弱性スキャンをパスできない可能性が高い。

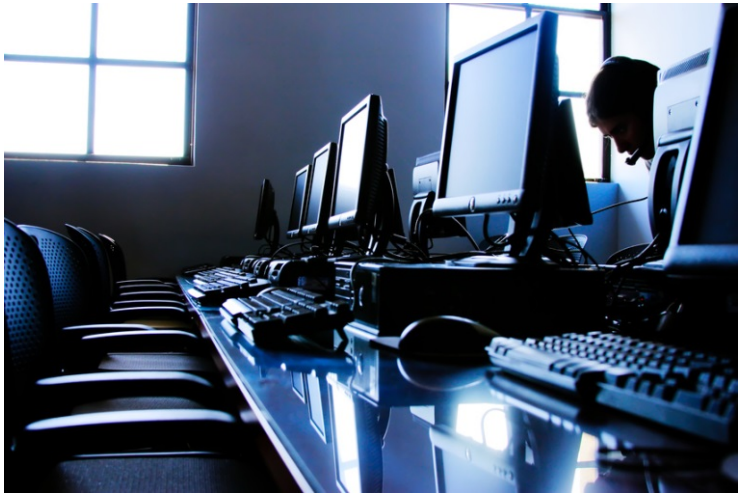
要件⑤ すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する

(要件5.1.2) **悪意のソフトウェアに影響されないとみられているシステム**でも、定期的にマルウェアの脅威を評価し、ウイルス対策ソフトウェアが必要ないか判断する　v3

- **Linux/Unix 系、Mac OS 系はこれに該当すると考えてよい**
  (最近ではスマホやタブレット用OSの考慮も必要。特にAndroidは悪意のソフトウェアに影響され"やすい"システムとして、ウイルス対策が必須となる要件5.1.1を適用する方が好ましい。)
- **ウイルス対策ソフトウェアの導入は必須ではないが、マルウェア脅威の定期評価が必要**

つまり・・・

脆弱性評価機関（JPCERT/JVN/CVEなど）やアンチウイルスベンダー、OS開発元などが公開する各種セキュリティ情報を入手し、評価する取り組みが必要（実際に、Linux/Unix/Mac OSに感染するウイルスやワームも存在する）



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

(要件6.4.2) 開発/テスト環境と本番環境での責務の分離

開発環境と本番環境の責務/担当者を分ける必要があるが、、、

実際は・・・

開発者が本番環境の保守も担当しているケースが非常に多い（弊社経験則では、ほぼ100%！！）

準拠するには

- 開発担当者とは別に運用担当者をアサインし、役割を明確に分担することがベスト
- 担当者の分離が困難な場合、開発担当者が不正に本番環境を変更できないよう、作業承認プロセスを徹底する
- 不正や不注意による変更が発生した際に、担当者や原因を追跡できるよう、ID管理とログ取得を厳格に実施する

要件⑦ カード会員データへのアクセスを、業務上必要な範囲内に制限する

アクセス権限定義のベストプラクティス

(要件7.1.1) 各役割のアクセスニーズを定義する
- 各役割が職務上アクセスする必要のあるシステムとデータ
- リソースへのアクセスに必要な特権レベル

ポイント 役割ごとのアクセス制御（**RBAC: Role Base Access Control**）手法に基づく定義表（**ACM: Access Control Matrix**）をつくる

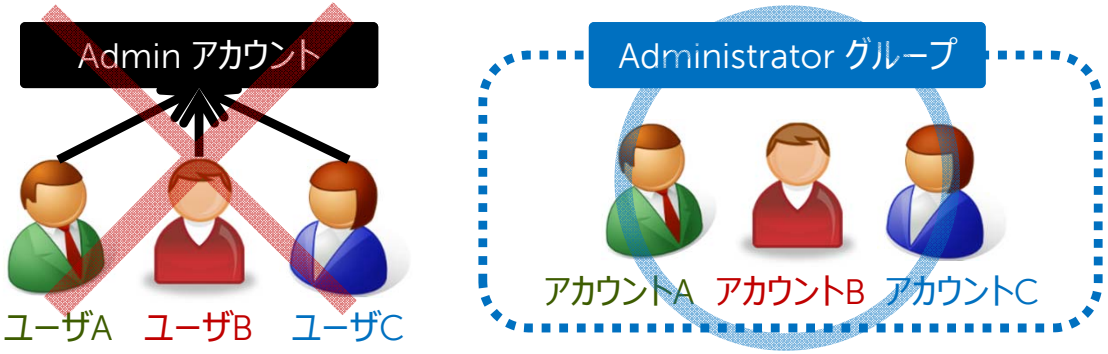
アクセスコントロールマトリクス

役割	PCIDSSスコープ内			PCIDSSスコープ外		
	決済アプリ	データベース	開発環境	CRMアプリ	会計アプリ	ファイルサーバ
セキュリティマネージャー	—	ユーザ	ユーザ	特権	特権	ユーザ
システムマネージャー	特権	特権	特権	—	—	特権
オペレーター	ユーザ	特権	—	—	—	ユーザ
プログラマー	ユーザ	ユーザ	特権	—	—	ユーザ
ファイナンスマネージャー	ユーザ	ユーザ	—	ユーザ	特権	ユーザ
ファイナンススタッフ	ユーザ	—	—	ユーザ	ユーザ	ユーザ
その他一般従業員	—	—	—	ユーザ	—	ユーザ

要件⑧ システムコンポーネントへのアクセスを確認・許可する

(要件8.1.1) すべてのユーザに一意のIDを割り当てる

管理者アカウントを共有していませんか？



(要件8.2.2) パスワードリセット前にユーザの身元を確認する V3

パスワードリセットが簡単すぎませんか？

非対面式の場合、ヘルプデスクに氏名とアカウント名を伝えるだけでは簡単になりすましができてしまう

ポイント 本人以外知ることが難しい情報（パスポート番号、保険証番号）やあらかじめ設定した秘密の質問と答えなどを利用する。

要件⑨ カード会員データへの物理アクセスを制限する

(要件9.5) すべての媒体を物理的に保護する

- **対象にはレシートの控えやFAX、郵便物なども含まれるが、電子媒体ほど厳重に管理されていないケースが多く、権限のない従業員やメンテナンス業者が不正に盗み取ってしまうリスクがある**

対策例

- カード決済業務に関与しない他部署とコピー機やファックスを共用しない
- パスコード入力やeFAXなどを使って受信者本人しか受け取れないようにする

要件⑩ ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

統合ログ管理システムは事実上必須？

(要件10.5.3) 監査ログは、一元管理ログサーバまたは媒体に**即座に**バックアップする

(要件10.6.1) **毎日一度以上**ログをレビューする
- すべてのセキュリティイベント
- すべての重要なシステムコンポーネントのログ
- ファイアウォール/IDS/IPS/認証サーバ/ECサーバなどのログ

これらをすべてマニュアルで実現するのは困難

時刻同期に関する注意

(要件10.4.3) 時刻は、**業界認知されたソース**から受信する

プロバイダが提供するものや、国内であればnict.go.jp、海外であればntp.orgなどを参考に、上位NTPサーバを指定

要件⑪ セキュリティシステムおよびプロセスを定期的にテストする

定期スキャン実施に関する注意

(要件11.1) 四半期ごとにワイヤレスアクセスポイントを検出するプロセスを実施する

注意!!

カード会員データ取扱い環境で無線デバイスを使用していなくても、不正なアクセスポイントが設置されていないか定期的にスキャンする必要がある

※ 無線IDS/IPSやネットワークアクセス制御(NAC)でも代替可能

(要件11.2.1) 高リスク脆弱性がなくなるまでスキャンを繰り返す
(要件11.3.3) 悪用可能な脆弱性の修正をテストして確認する

- **脆弱性がないことを確認して初めて脆弱性スキャンやペネトレーションテストを1回分完了したとみなすことができる**

※ 再診断や再テストは実施回数にカウントされない

要件⑫ すべての担当者の情報セキュリティに対応するポリシーを維持する

教育実施に関する注意点

(要件12.6.2) 担当者は、年に一度セキュリティポリシーおよび手順を読み、理解したことを認める必要がある

- **ただ単に教育を受講した、ということだけでは不十分**
- **明示的に書面での同意または電子的な署名が必要**

(要件12.10.4) セキュリティ違反への対応を担当するスタッフに適切なトレーニングを提供する。

- **ここでいうトレーニングは、一般的な情報セキュリティ教育ではない**
- **インシデントレスポンスに必要な、問題の特定、被害拡大防止、証拠保全、原因究明、復旧、事後分析といった一連の活動に必要なスキルの習得を目的としたもの**

全要件 – 文書化に関する要求事項

ドメイン	要件
1	1.5 ファイアウォールの管理に関する セキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知らされていることを確認する。
2	2.5 ベンダデフォルト値およびその他のセキュリティパラメータの管理に関する セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
3	3.7 保存されているカード会員データを保護するための セキュリティポリシーと操作手順が文書化および使用されており、影響を受ける関係者全員に知られていることを確認する。
4	4.3 カード会員データの伝送を暗号化するための セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
5	5.4 マルウェアからシステムを保護するための セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
6	6.7 セキュアシステムとアプリケーションを開発・保守するための セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
7	7.3 カード会員データへのアクセスを制限するための セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
8	8.8 識別と認証に関する セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
9	9.10 カード会員データへのアクセスを制限するための セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
10	10.8 ネットワークリソースとカード会員データへのすべてのアクセスを監視するための セキュリティポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを確認する。
11	11.6 セキュリティ監視とテストに関する セキュリティポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを確認する。
12	12.1 セキュリティポリシーを確立、公開、維持、普及させる

注意!!

全ての要件について文書化が必要！

Dell SecureWorks
PCI DSS サービス

PCIDSS ギャップ分析のススメ

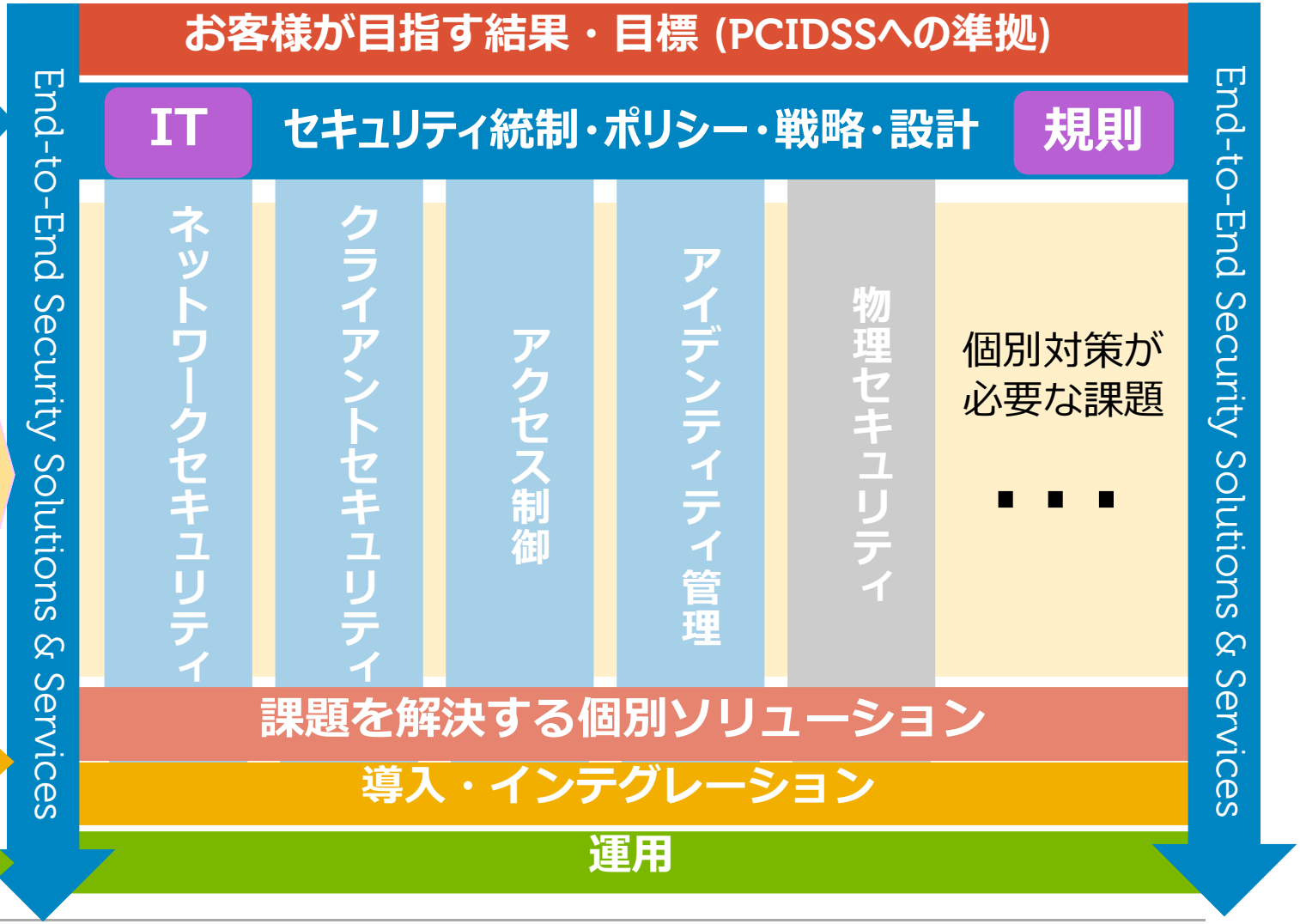
準拠支援コンサルテーション (≒ギャップ分析)

※各STEPの必要期間は、対象環境の規模や現状セキュリティ対策状況によって大きく変動する可能性があります。

PCI DSS 改善作業および準拠維持に関する支援

ギャップ分析で発見された改善事項を実行するにあたり、弊社はPCI認定機関としての豊富なソリューションやコンサルティング、全体のプロジェクトマネジメントなどを提供することができます

- SecureWorks
  コンサルティング
- SonicWALL
- KACE
- Wyse
- Quest
- DDPE
- Etc.
  ＋
- 3rd Vendor
- SecureWorks
  インフラストラクチャ
  コンサルティングサービス
- SecureWorks
  セキュリティ監視サービス



Dell SecureWorks の PCIDSS サービス概要

Dell SecureWorksは、PCI DSS への準拠および準拠後のセキュリティ環境維持に必要な各種サービスを一貫して提供可能です

SRC
セキュリティ＆リスクコンサルティング
アセスメントや審査、ポリシー策定

- ギャップ分析
- 模擬審査
- 審査と準拠報告書 (ROC: Report on Compliance) 作成
- 自己問診 (SAQ: Self-Assessment Questionnaires) 作成支援
- 準拠計画策定とプロジェクト管理
- ペネトレーションテスト

MSS
マネージドセキュリティサービス
日々の監視・管理や改善作業

- PCI認定脆弱性スキャン
- ログ監視と管理
- 侵入検知と監視管理
- ファイアウォール監視管理
- 脆弱性管理
- セキュリティ脅威動向とリスクトレンド配信

すべてのサービスは、弊社が誇る世界有数のセキュリティ脅威調査チーム **CTU (Counter Threat Unit)** の監修により、常に最新のセキュリティ技術動向を反映した効果的なソリューションです。

ご清聴いただきまして、
誠にありがとうございました

この文書について

この文章に記載されている仕様は、2014年7月現在のものであり、予告なく変更される場合があります。
最新の仕様については、弊社営業またはホームページにてご確認下さい。