

「PCI DSS v3.0準拠対応事例と関連サービスのご紹介」

～まだ間に合う！情報システムに対する早く正確なFIT & GAPの秘訣～

TIS株式会社
IT基盤サービス第4部 シニアエキスパート
三木 基司

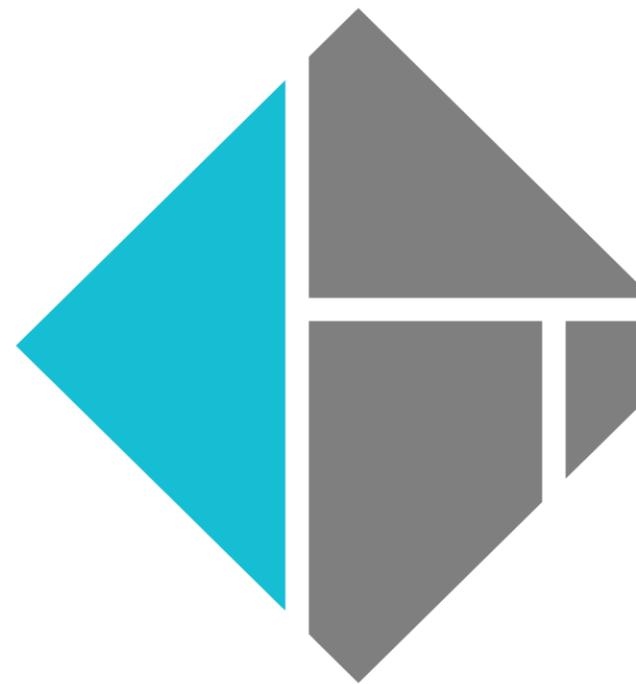
PCI DSSセキュリティフォーラム 2014

2014.07.29

TIS株式会社

IT基盤サービス第1事業部 IT基盤サービス第1営業部

IT基盤サービス第1事業部 IT基盤サービス第4部



自己紹介

氏名 三木 基司 (ミキ モトジ)
 略歴

- 1987年 長銀情報システム(株) 入社(現TIS)
 - ・ 通産省の安全対策基準認定事業所制度の対応
- 2000年 2000年問題を契機に情報セキュリティの必要性を痛感
 - ・ イスラエルのCOMSEC Consulting社において、BS7799による情報セキュリティコンサルティング技術を修得
 - ・ セキュリティコンサルティング会社を立上
 (国内企業のISMS・PMS取得支援、セキュリティ対策支援)
- 2003年 MasterCard様のSDP(Site Data Protection)ベンダとして
 クレジットカード会社のセキュリティ対策を支援
- 2004年 PCI DSS制度の立上り時期より国内普及活動へ協力中

保有資格	公認情報セキュリティ主任監査人 PCIDSS認定コンサルタント ISO27001審査員補 ネットワークスペシャリスト 情報セキュリティアドミニストレータ 防犯設備士 CSPM of Technical認定講師	(日本セキュリティ監査協会) (国際マネジメントシステム認証機構) (日本規格協会) (経済産業省) (経済産業省) (警察庁所管 日本防犯設備協会) (SEA/J)
------	--	---

参加団体 日本カード情報セキュリティ協会 日本情報セキュリティ監査協会

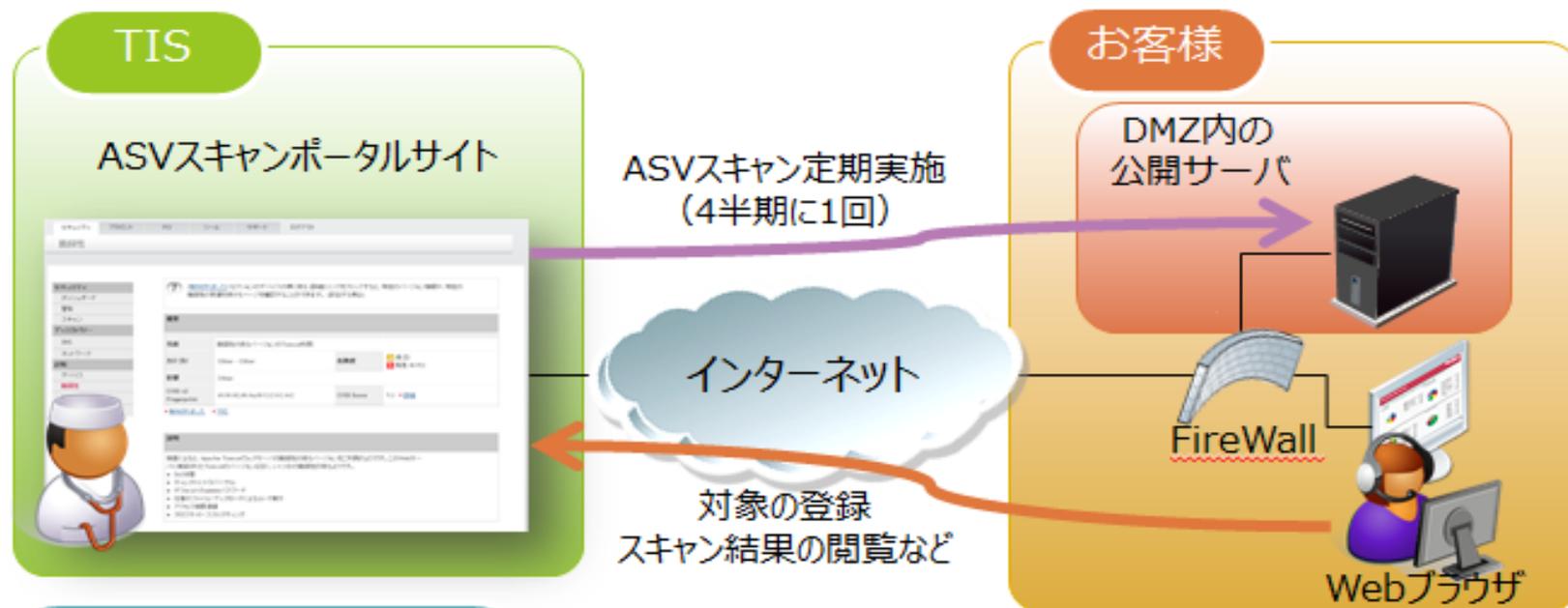
TIS株式会社のご紹介

- ◆ 認定ASV事業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



ASVクラウドサービスリリースのご案内

認定ASVであるTISが、お客様の外部ネットワークの脆弱性スキャンをクラウド型で定期的
に実施します。お申し込みやスキャン結果の閲覧など一連の操作はWebブラウザから実施
でき、お客様は手軽に素早く確実なASVスキャンを受けることができます。



サービスの特長

- ・お客様はWebブラウザのみご準備いただければOK!
- ・ASVスキャン登録作業は一度だけでOK!
- ・ご希望の日時に合わせてスキャン可能!
- ・定期スキャンの実施時期もTISが管理するため、作業漏れがなくなり安心!

PCI DSS普及までのあゆみ

昨年は、クレジットカード会社様のPCI DSS準拠対応が本格化

【PCI DSS普及のポイント】

ポイント1

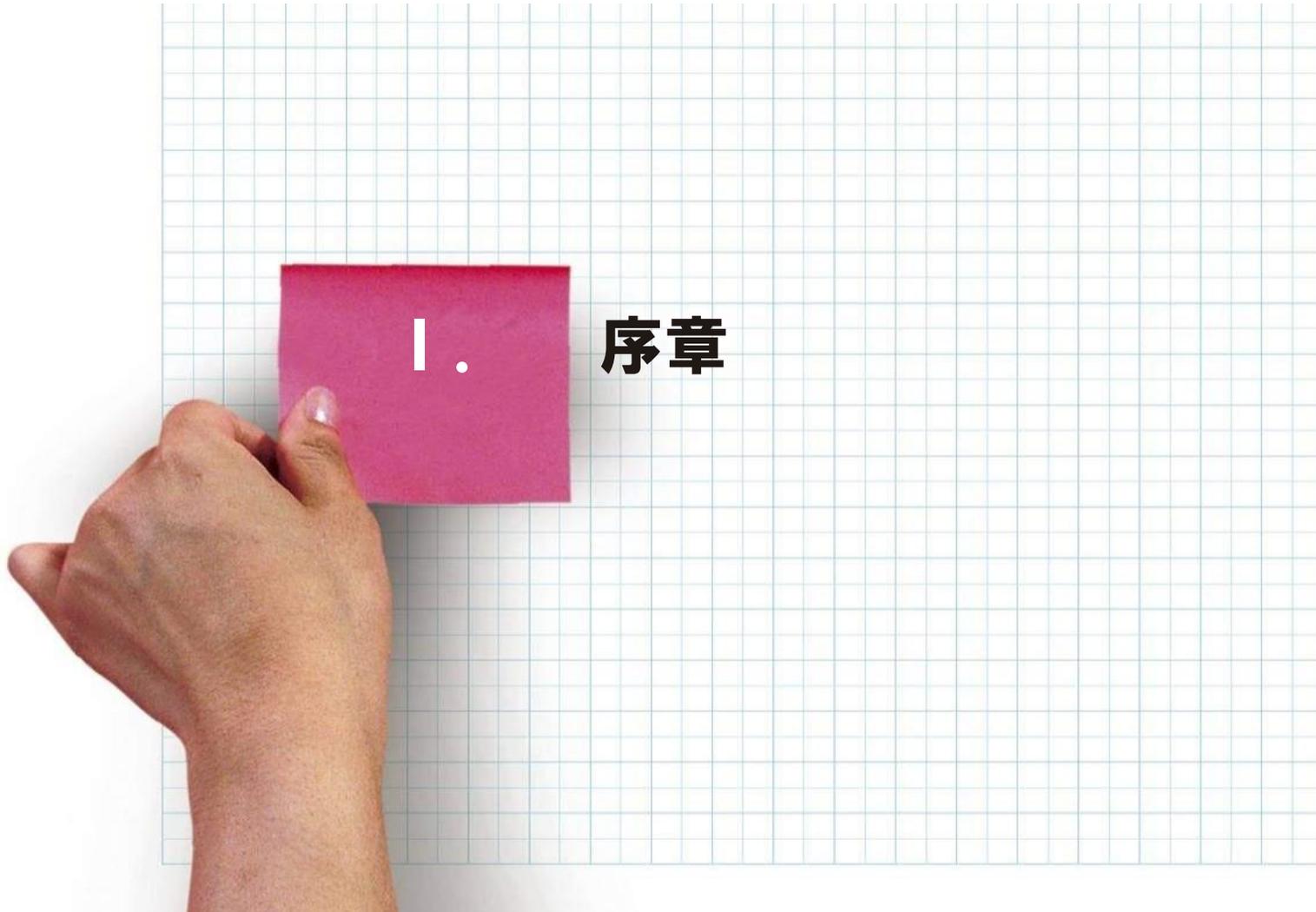
2004年 国際カードブランド5社による、業界のセキュリティ標準が誕生！
 ・その後、国内では一部組織を除き、数年間は認知さえされていない状況
 ～ PCI DSSに対する認知度、準拠への取組みは停滞 ～

ポイント2

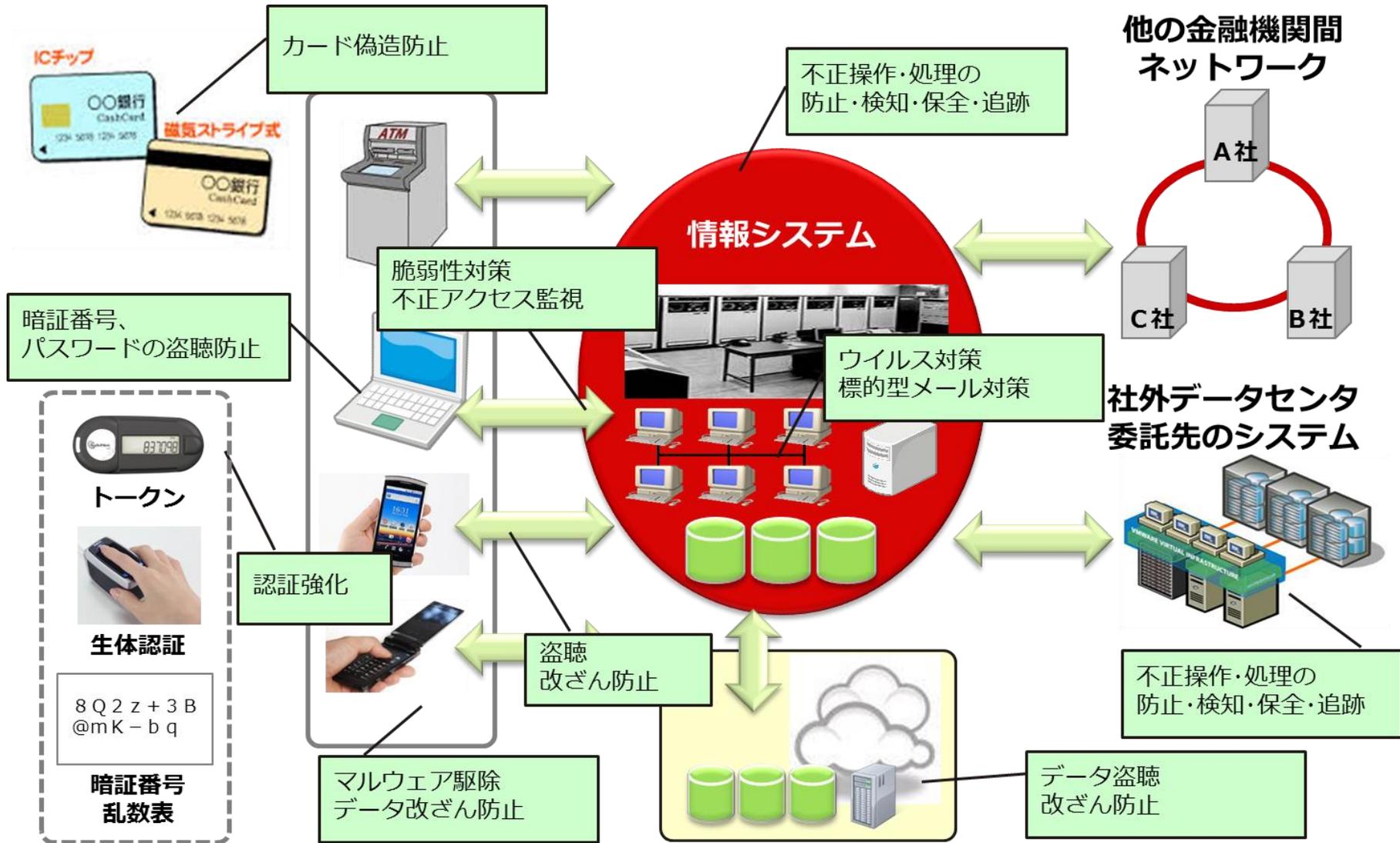
2012年 日本クレジット協会が準拠の実行計画を公表
 「日本におけるクレジットカード情報管理強化に向けた実行計画」
 ・具体的な目標感が定まった
 ・勉強会やPCI DSS完全準拠を意識した行動計画の作成が始まった

ポイント3

2013年 PCI DSS ver3.0 の公開
 ・様子見のクレジットカード会社様でもPCI DSS準拠対応の機運高まり
 ・先行するクレジットカード会社様では、取組み範囲を一部から全体へ拡張
 ・他業種組織でもPCI DSSをセキュリティ評価基準に取込む動き



1. 情報システムのセキュリティ対策 (現在)



引用元：日本銀行金融研究所第14回情報セキュリティ・シンポジウム（2012年12月20日）

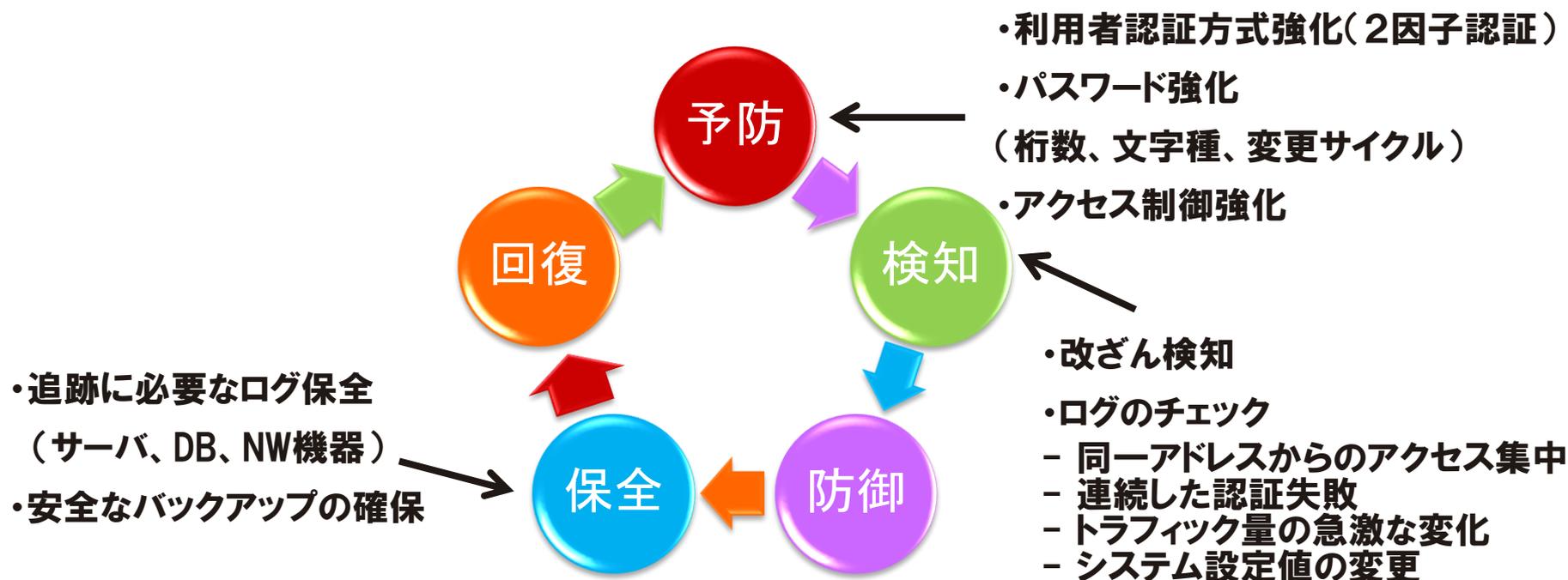
2. 日々狙われるクレジットカード情報



情報システムの管理部門およびその担当者は、次々と発生する内外のセキュリティ問題に素早く対応しなければならない状況

3. 今、見直すべきセキュリティ対策①

- ◆ これまでのセキュリティ対策は、「抑止・予防」、「防御」に力が注がれてきた。
- ◆ 今後のセキュリティ対策は、脅威の発生をいち早く「検知」、発生した場合有効な対処(フォレンジックスによる原因や影響調査)を施し、速やかに回復をさせることが重要になってきている。



4. 今、見直すべきセキュリティ対策②

- ◆ たとえISMSやプライバシーマークの認証を得ていても、対策としてはまだまだ安心できるレベルでは、ないかもしれません。
- ◆ 例えば、PCI DSSでは、システムへアクセスするためのユーザID管理を以下のように規定しています。

【PCI DSS要件によるセキュリティ要求事項の例】

- ✓ 90日ごとに非アクティブなユーザアカウントを削除/無効する。(8.1)
- ✓ 保守用ユーザIDは、通常無効化。必要な期間内だけ有効化する。(8.1)
- ✓ 連続パスワード試行時の6回以下でのロックアウト制御する。(8.1)
- ✓ パスワードは7文字以上とする。(8.2)
- ✓ 英数を含むパスワードを使用する。(8.2)
- ✓ 90日以内のパスワード変更サイクルとする。(8.2)
- ✓ 4世代分のパスワード再利用設定を禁止する。(8.2)
- ✓ 初期パスワードおよびリセットパスワードを一意化する。(8.2)

5. 本フォーラムにてお伝えしたいこと

- ◆ 当社が過去に行なった、これまでのフォーラム講演では、その時の時流に応じたメッセージを発信してきました。

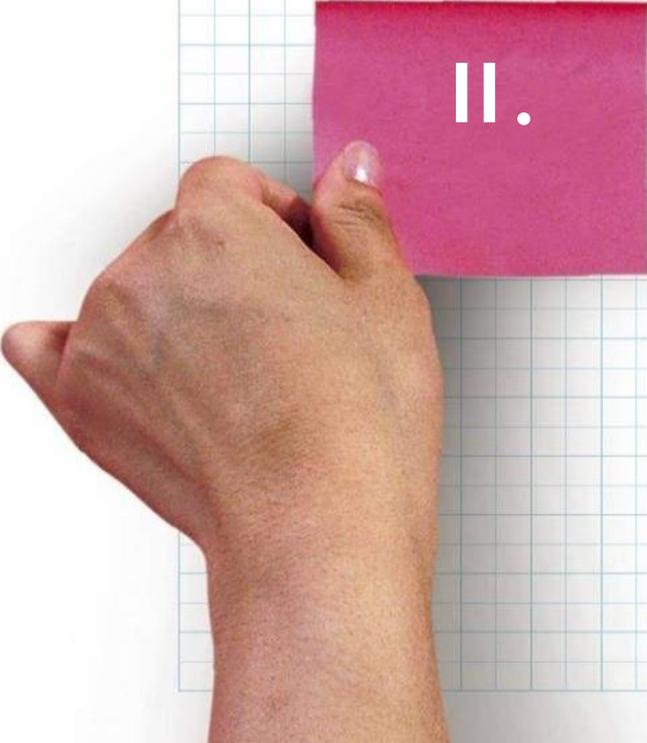
過去のセキュリティフォーラムでお伝えしたこと。

2012年 「PCI DSS要件について、よくある課題を事例に**理解しましょう**」

2013年 「PCI DSS準拠対応は**対象範囲の明確化から始めましょう**」

今年のメッセージ：

この一年間で、**PCI DSS準拠の必要性**はグンッとアップ！しています。
但し、2018年3月を期限とすると**システム対応時間は残り少ない**です。
まずは情報**システム強化のための予算感を掴み**、期限内にどのように
準拠対応を進めていけるのかを**検討する材料を揃える**ことです。
ポイントとなるのは、現場負担の少ないギャップ分析と情報システムの
運用負荷をこれ以上増やさない**ツールありきの運用検討**だと考えます。

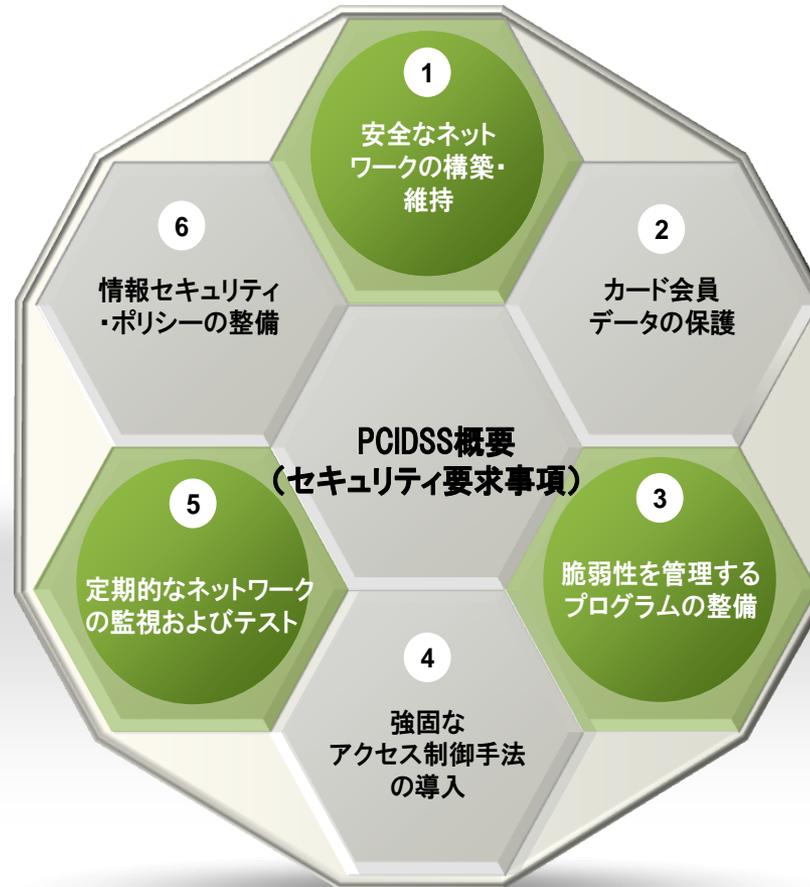


II.

PCI DSS要件とは (復習)

6. PCI DSS要件概要

要件1: データを保護するためにファイアウォールの導入をし、最適な設定を維持すること
 要件2: システムまたはソフトウェアの出荷時の初期設定値をそのまま利用しないこと



要件12: 情報セキュリティに関するポリシーを保持すること

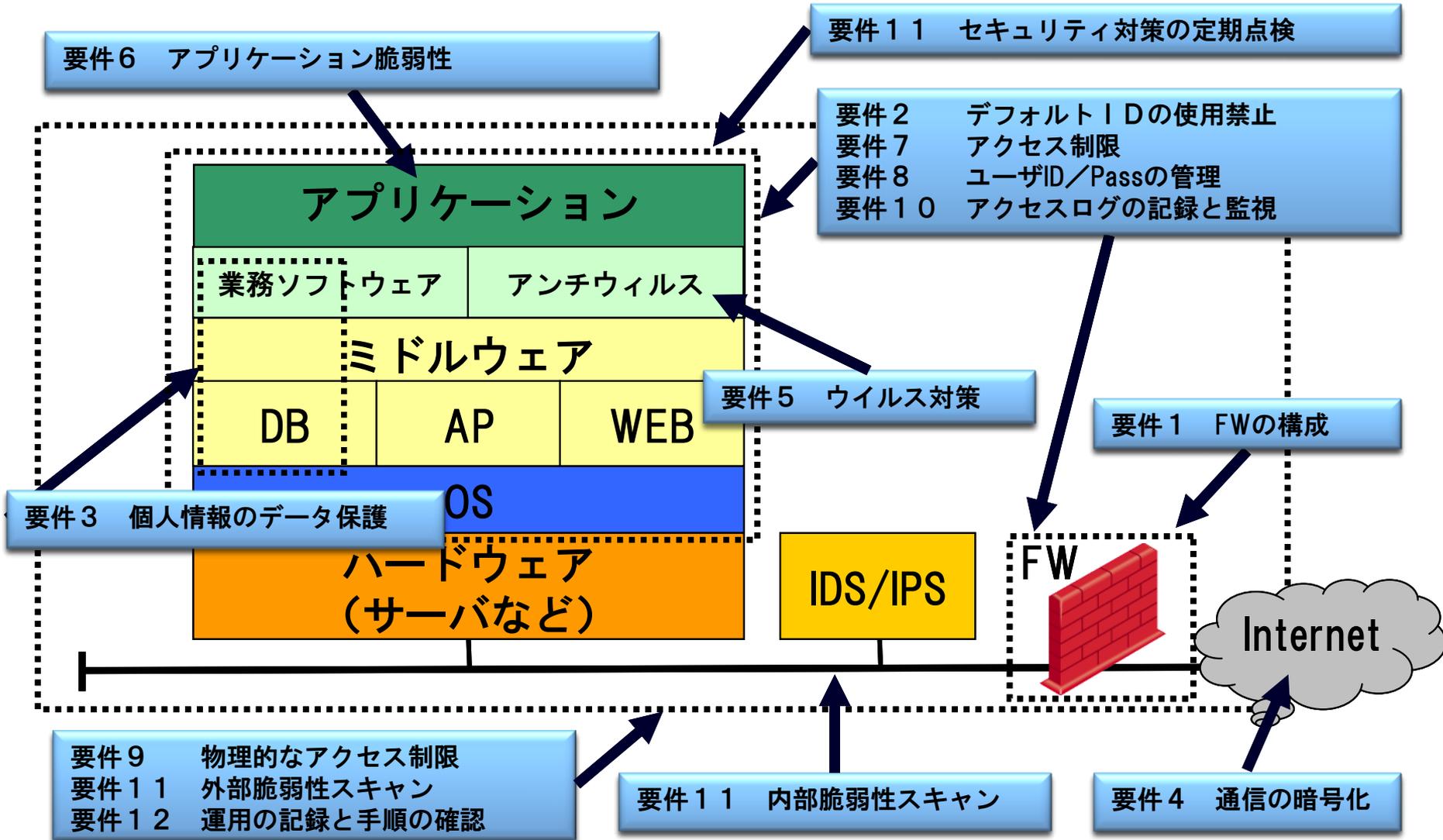
要件3: 保存されたデータを安全に保護すること
 要件4: 公衆ネットワーク上でカード会員情報・センシティブ情報を送信する場合、暗号化すること

要件10: ネットワーク資源およびカード会員情報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有事の対応手順を定期的にテストすること

要件5: アンチウイルスソフトを利用し、定期的にソフトを更新すること
 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

要件7: 業務目的別にデータアクセスを制限すること
 要件8: コンピュータにアクセスする際、利用者毎に識別IDを割り当てること
 要件9: カード会員情報にアクセスする際、物理的なアクセスを制限すること

7. PCI DSSとシステム構成要素の関係



8. 情報システム強化視点から見たver3.0

- ◆ PCI DSS要件は、ver2.0→ver3.0となりましたが情報システムの強化・改修検討への影響は少ないです。

PCI DSSver3.0の変更は、208件あります。

- ・追加要件 … 新たに追加された要件(17件)
- ・発展型要件… ver2.0の要件にさらに要求を加えた要件(40件)
- ・明確化要件… ver2.0ではあいまいだった点を具体化した要件(151件)

- 追加要件 : 主にシステム責任者がシステムを把握していることを確認する為に追加された要件。
情報システム構築に対する要件ではないため、情報システムの強化・改修には影響はありません。
- 発展型要件 : 実装時のセキュリティレベル向上を要求する要件。
本要件の対応については、設計書、手順書の内容をしっかりと実装することです。
- 明確化要件 : ver2.0であいまいであった点を具体化した要件。
PCI DSS要件を運用手順書などに正しく反映させることです。
特別なことを要求されているわけではないため、通常の対応範囲内です。



III.

PCI DSSについてよく聞く話 現状と解決策のご提案

9. PCI DSS準拠対応検討前の課題



【PCI DSS準拠対応について、よく聞く課題？】

とにかく対応する要件数が多すぎる

「大変そう」

どの要件を誰に聞けばよいのか解らない

「チェックに時間が掛かりそう」

何を確かめるのか解りづらい

「解り難そう」

いったい幾らコストが掛かるのか不安

「とにかくコストが掛かりそう」



【TISからのご提案】

- ◆ 「～そう」の仮定が邪魔をして、なかなか検討が進まないことはないですか？
- ◆ PCI DSS要件は、情報システムに対するセキュリティ標準です。
- ◆ 情報システムの強化が必要なのかどうか、的を絞ってチェックしましょう！

10. 情報システムの現状確認①

PCI DSS要件 (V3.0)				要件区分				対応チーム		ギャップ分析評価対象システム記入欄		TIS記入欄			
要件 Ver.3.0 ※公開されている情報です。		テスト手順 Ver.3.0 ※公開されている情報です。		確認ポイント ※TISによる確認です。		環境/設定	文書化	インポート	運用/アプデ	アプリケーション	インフラ	現状確認結果 0:未対応 1:一部対応 2:対応済	確認内容 ※左側の「現状確認結果」の理由を記入してください。	評価結果	改善方針
【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	2.1.1	2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイเลส環境の場合、インストール時にすべてのワイレスベンダのデフォルト値を変更する。これには、デフォルトのワイレス暗号化キー、パスワード、SNMPコミュニティ文字列が含まれるが、これらは限定されない。	2.1.1.a	2.1.1.a 担当者をインタビューし、関係文書を読んで、以下を確認する。 • 暗号化キーがインストール時のデフォルトから変更されていること。 • 暗号化キーの知識を持つ人物が退社または異動するたびに、そのキーが変更されていること。	ワイレス関連文書に以下の記載があることを確認する。 • 暗号化キーの知識を持つ人物が退社または異動するたびに、そのキーが変更されていること。										
【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	2.1.1	2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイเลส環境の場合、インストール時にすべてのワイレスベンダのデフォルト値を変更する。これには、デフォルトのワイレス暗号化キー、パスワード、SNMPコミュニティ文字列が含まれるが、これらは限定されない。	2.1.1.b	2.1.1.b 担当者をインタビューし、ポリシーと手順を調べることで、以下を確認する。 • デフォルトの SNMP コミュニティ文字列をインストール後に変更する必要があること。 • アクセスポイントのデフォルトのパスワード/パスフレーズをインストール後に変更する必要があること。	ワイレス関連文書に以下の記載があることを確認する。 • デフォルトの SNMP コミュニティ文字列をインストール後に変更する必要があること。 • アクセスポイントのデフォルトのパスワード/パスフレーズをインストール後に変更する必要があること。										
【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	2.1.1	2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイเลส環境の場合、インストール時にすべてのワイレスベンダのデフォルト値を変更する。これには、デフォルトのワイレス暗号化キー、パスワード、SNMPコミュニティ文字列が含まれるが、これらは限定されない。	2.1.1.c	2.1.1.c システム管理者の協力を得て、ベンダ文書を読む、ワイレスデバイスログをレビューし、以下を確認する。 • ワイレスデバイスのデフォルトの SNMP コミュニティ文字列が変更されていないこと。 • アクセスポイントのデフォルトのパスワード/パスフレーズが変更されていないこと。	システム管理者の協力を得て、ベンダ文書を読む、ワイレスデバイスログをレビューし、以下を確認する。 • ワイレスデバイスのデフォルトの SNMP コミュニティ文字列が変更されていないこと。 • アクセスポイントのデフォルトのパスワード/パスフレーズが変更されていないこと。										
【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	2.1.1	2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイเลส環境の場合、インストール時にすべてのワイレスベンダのデフォルト値を変更する。これには、デフォルトのワイレス暗号化キー、パスワード、SNMPコミュニティ文字列が含まれるが、これらは限定されない。	2.1.1.d	2.1.1.d ベンダ文書を読む、ワイレス構成設定を総観して、ワイレスデバイスのファームウェアが、以下の強力な暗号化をサポートするために更新されていることを確認する。 • ワイレスネットワーク経由での認証 • ワイレスネットワーク経由での送信	ベンダ文書を読む、ワイレス構成設定を総観して、ワイレスデバイスのファームウェアが、以下の強力な暗号化をサポートするために更新されていることを確認する。 • ワイレスネットワーク経由での認証 • ワイレスネットワーク経由での送信 (設計書、またはベンダ提供文書で確認できること)										

ポイント1: PCI DSSver3.0の要件1～12における詳細項目のうち、情報システムに関連する項目に絞り込みチェック可能です。

ポイント2: 要件項目ごとにリスク対応の目的と何を確認すれば良いのか具体的なチェック方法が解ります。

ポイント3: 当社コンサルタントがQSAと共に記載内容を確認し、評価を報告を作成、返答します。

11. 情報システムの現状確認②

ポイント4: まずは、システム強化が必要な「要件は何か？」に答えを出します。

PCIDSS要件 (V3.0)				要件区分							対応チーム		キャップ分析評価対象システム記入欄		TIS記入欄							
要件 Ver3.0 <small>※お取扱いの要件です。</small>		テスト手順 Ver3.0 <small>※お取扱いの要件です。</small>		確認ポイント <small>※TISによる確認です。</small>		構成/設定	文書化	インフラ	運用プロセス	アプリケーション	インフラ	PCI DSS運用	評価結果	確認内容	評価結果	改善方針						
<small>※左欄の「現状確認結果」の理由を記入してください。</small>																						
【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ーが提供したデフォルト値を使用しない	2.1.1	2.1.1	2.1.1	2.1.1.a	2.1.1.a	○	○				✓											
PCIDSS要件の対応状況を確認するときの観点では不明瞭なところに対し、これまでの監査の対応実績からTISが補足させていただいている部分です。				PCI DSS要件がシステム構成要素の何を求めているのかを整理しています。							要件区分		対応チーム									
				要件区分							対応チーム											
				構成/設定							文書化		インフラ		運用プロセス		アプリケーション		インフラ		PCI DSS運用	

PCIDSS要件の対応状況を確認するときの観点では不明瞭なところに対し、これまでの監査の対応実績からTISが補足させていただいている部分です。

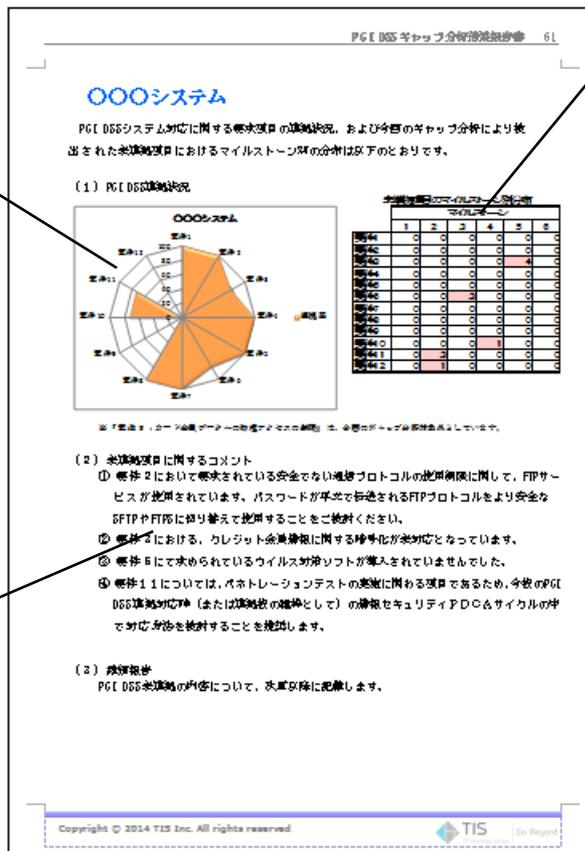
PCI DSS要件がシステム構成要素の何を求めているのかを整理しています。

PCI DSS要件の現状を回答するチームを整理しています。

12. PCI DSS要件準拠度合いの確認

ポイント5: 評価の結果、PCI DSS要件への未準拠検出部分について12要件への準拠度合い(%)とPCI SSC指定のマイルストーンレベルの分布を判りやすく表示、PCI DSS要件への対策優先順位の検討にお役立てください。

準拠対応状況の偏りをレーダーチャートを使って分析。要件毎の評価対象項目数に対する準拠度合いをパーセント換算してあります。



未準拠の要件内容を確認し、PCI SSCが公表している要件の優先度(マイルストーン)※(下記参照)ごとに表示しています。

※ PCI SSCが公開している優先度(マイルストーン)

優先順位	リスク 低減効果	目的	具体的実施策
1	大 ↑ ↓ 小	不要な情報の削除	クレジットカード番号/機密関連データの削除
2		ネットワーク境界の保護	ネットワーク管理、セキュリティパラメータ設定 通信路の暗号化、ウィルス管理、脆弱性管理
3		アプリケーションの保護	サービスの制限、セキュリティパッチ適用 安全なアプリケーション開発
4		監視とアクセス制御	ID/パスワード管理、アクセス権限管理 ログ管理(監視含む)、ファイル整合性監視
5		保管データの保護	PANのマスキング・暗号化、媒体の保護
6		その他(文書化等)	ポリシー整備、運用手順書整備、運用確認書整備

対象となる情報システムにおけるPCI DSS準拠のためのシステム化検討ポイントに記載しています。

PCI DSSの要求事項を導入した場合のリスク低減効果の大きさを根拠に6つの優先順位付け

13. PCI DSS要件準拠対応方針

ポイント6: PCI DSS準拠のために必要な情報システムの強化方針に関する情報を検出したPCI DSS未準拠要件ごとに取り纏めご提供します。

PCI DSSギャップ分析結果報告書 6

ID	1
要件番号	8.1.4
要件	少なくとも 90 日ごとに無アクティブなユーザーアカウントを無効化する。
解説	日時に使用されていないアカウントは、パスワードの変更、アカウントの不正確性をされてもユーザーに気付かれないで、攻撃の対象となりやすくなります。アカウントが凍結されるとカードホルダーへのアクセスに制限されることになるため、無期間使用していないアカウントは、無効されないようなシステム的な対策が望めます。
現状	パスワードの有効期限 (90 日) を延滞すると、周期的にパスワード変更を要求する機能は実装済、無効化の機能は実装していません。
従来対応	4
対応方針	<p>90 日無効化されなかったアカウントにしていただき、これは、アプリケーションを改善します。</p> <p>例: アプリケーションを改善するべく、本要件を実装する。実装してないワークアラカセスを無効する。</p> <p>【代替コントロール】 代替的な理由、コストが膨大にかかる代替コントロールを適用することもできます。</p> <p>① ログの監視において 91 日以上アカウントがアクティブに検出される、 ② 検知内容に宛先、アクセス元、アクセス先を通知する。 ③ ①、②について、通知方法を構築 ④ 上記の内容が有効に機能している</p>

Copyright © 2014 TIS Inc. All rights reserved

【記載情報】

- PCI DSS要件が求めている強化策 (オリジナル要件)
- よくある代替コントロールの考え方
- 関連ツールの情報

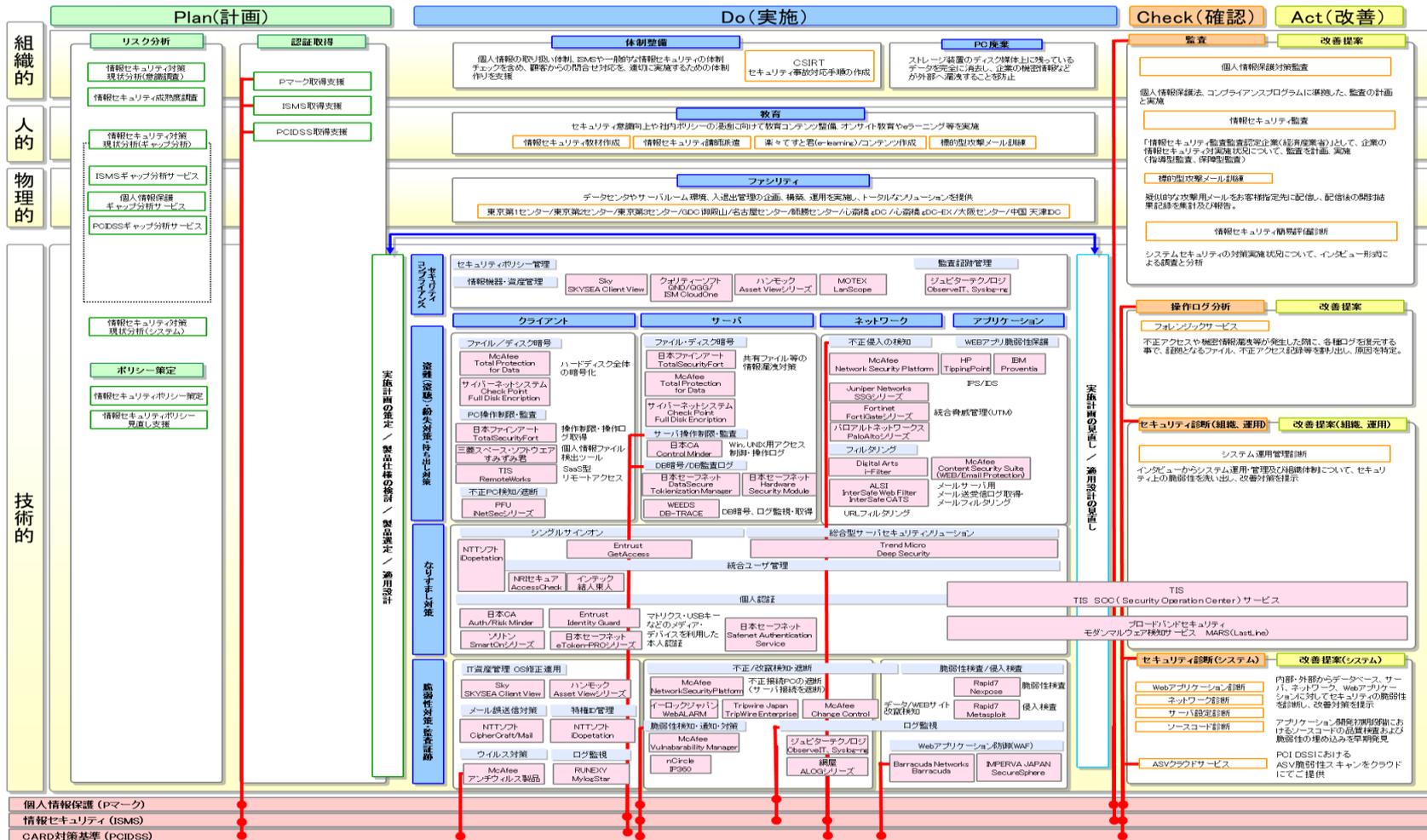
項目	インフラシステム	運用	インフラシステム	運用
1	インフラシステム	運用	インフラシステム	運用
2	インフラシステム	運用	インフラシステム	運用
3	インフラシステム	運用	インフラシステム	運用
4	インフラシステム	運用	インフラシステム	運用
5	インフラシステム	運用	インフラシステム	運用
6	インフラシステム	運用	インフラシステム	運用
7	インフラシステム	運用	インフラシステム	運用
8	インフラシステム	運用	インフラシステム	運用
9	インフラシステム	運用	インフラシステム	運用
10	インフラシステム	運用	インフラシステム	運用
11	インフラシステム	運用	インフラシステム	運用
12	インフラシステム	運用	インフラシステム	運用
13	インフラシステム	運用	インフラシステム	運用
14	インフラシステム	運用	インフラシステム	運用
15	インフラシステム	運用	インフラシステム	運用
16	インフラシステム	運用	インフラシステム	運用
17	インフラシステム	運用	インフラシステム	運用
18	インフラシステム	運用	インフラシステム	運用
19	インフラシステム	運用	インフラシステム	運用
20	インフラシステム	運用	インフラシステム	運用
21	インフラシステム	運用	インフラシステム	運用
22	インフラシステム	運用	インフラシステム	運用
23	インフラシステム	運用	インフラシステム	運用
24	インフラシステム	運用	インフラシステム	運用
25	インフラシステム	運用	インフラシステム	運用
26	インフラシステム	運用	インフラシステム	運用
27	インフラシステム	運用	インフラシステム	運用
28	インフラシステム	運用	インフラシステム	運用
29	インフラシステム	運用	インフラシステム	運用
30	インフラシステム	運用	インフラシステム	運用
31	インフラシステム	運用	インフラシステム	運用
32	インフラシステム	運用	インフラシステム	運用
33	インフラシステム	運用	インフラシステム	運用
34	インフラシステム	運用	インフラシステム	運用
35	インフラシステム	運用	インフラシステム	運用
36	インフラシステム	運用	インフラシステム	運用
37	インフラシステム	運用	インフラシステム	運用
38	インフラシステム	運用	インフラシステム	運用
39	インフラシステム	運用	インフラシステム	運用
40	インフラシステム	運用	インフラシステム	運用
41	インフラシステム	運用	インフラシステム	運用
42	インフラシステム	運用	インフラシステム	運用
43	インフラシステム	運用	インフラシステム	運用
44	インフラシステム	運用	インフラシステム	運用
45	インフラシステム	運用	インフラシステム	運用
46	インフラシステム	運用	インフラシステム	運用
47	インフラシステム	運用	インフラシステム	運用
48	インフラシステム	運用	インフラシステム	運用
49	インフラシステム	運用	インフラシステム	運用
50	インフラシステム	運用	インフラシステム	運用

14. ツールによるPCI DSS準拠の検討①

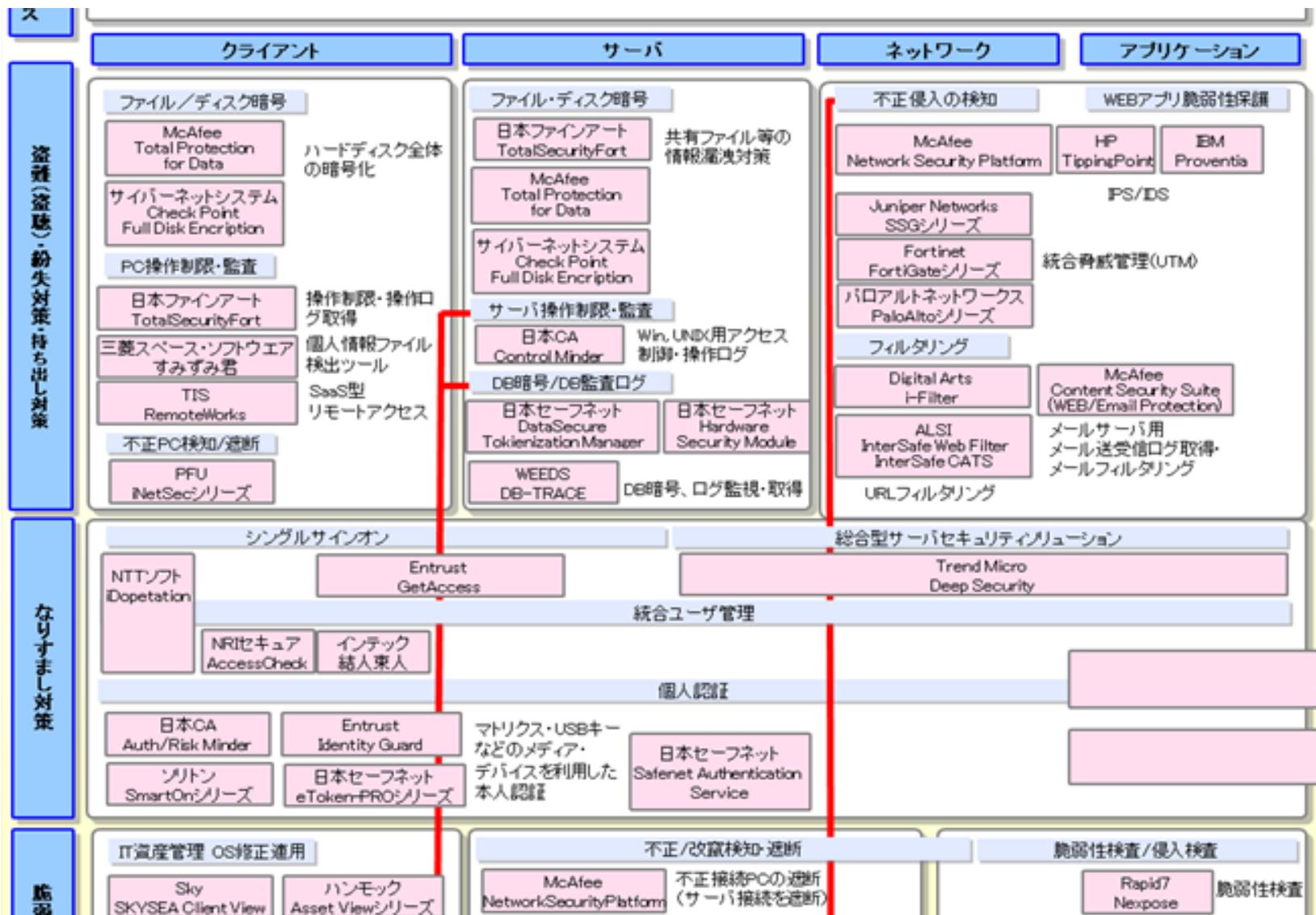
ポイント7: セキュリティツールを対策目的ごとにマップ化した資料を使い
ツール・コンシェルジュが最適ツールの情報をご提供します。

TIS 株式会社 情報セキュリティ対策マップ

更新日: 2014年06月18日



15. ツールによるPCI DSS準拠の検討②



16. 代替コントロールの考え方

◆ 代替コントロールの採用にあたっては、代替策とその理由、代替策の運用方法、代替策の有効性をチェックする手順について整理する必要があります。(専用シートを使い上述情報の整理をご支援します。)

■ 代替コントロールワークシート [01]

バージョン	1.0
発行履歴日	2014/XX/XX

案件番号: 34

以下の手法を使用して、すべての保存場所で PAN を読み取り不能にする(ポータブルデジタルメディア、バックアップメディア、ログを含む)。

- 強力な暗号化技術をベースにしたワンウェイハッシュ(PAN全体をハッシュする必要がある)
- トランケーション(PANの切り捨てられたセグメントの置き換えにはハッシュを使用できない)
- インデックストークンとパッド(パッドは安全に保存する必要がある)
- 関連するキー管理プロセスおよび手順を伴う、強力な暗号化

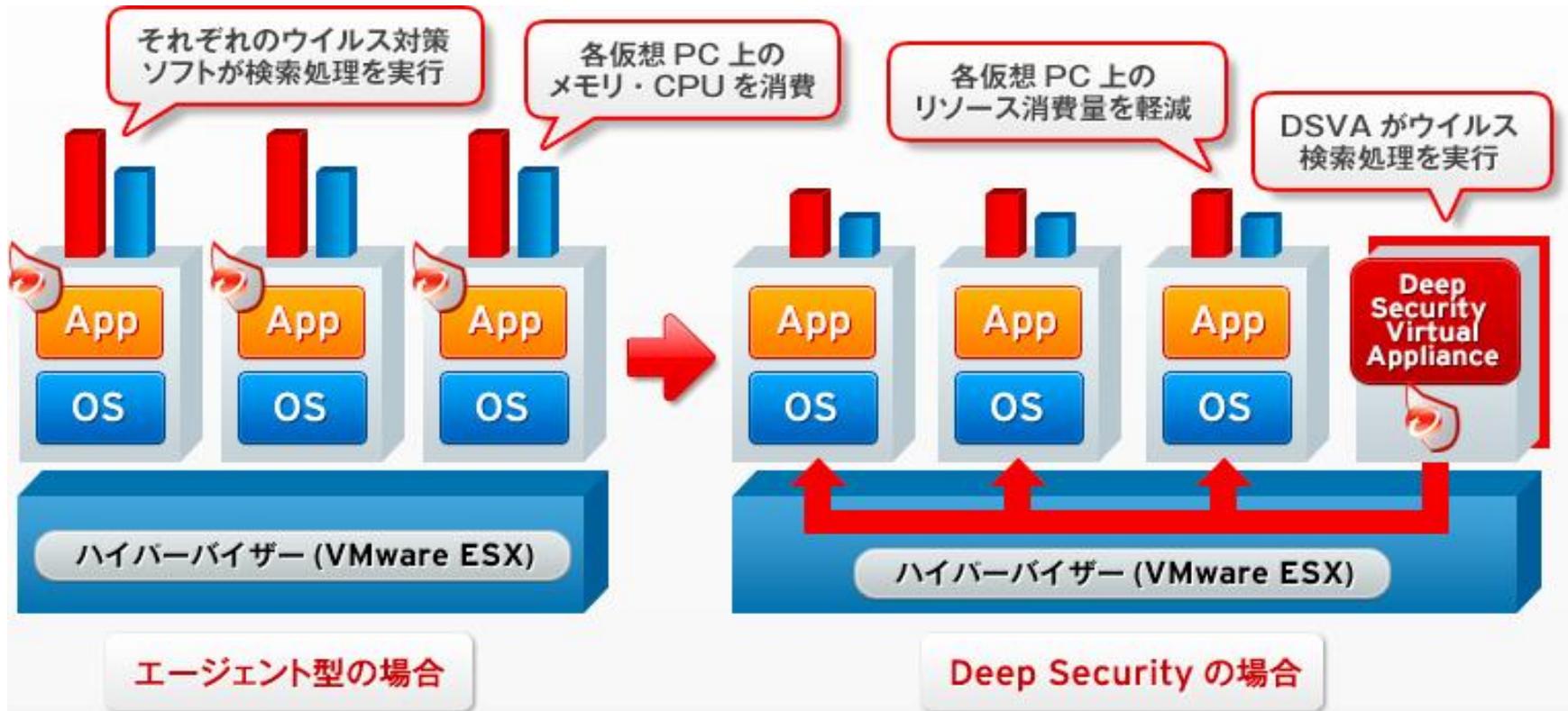
	必要な情報	説明
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	以下を考慮し、暗号化が実施できない。 ・DB暗号化によるパフォーマンス劣化の懸念。 ・イニシャルコストの懸念。
2. 目的	元のコントロールの目的を定義し、代替コントロールによって満たされる目的を特定する。	カード会員データが保管されているストレージもしくはデータを暗号化することで、悪意のある人物からのデータ閲覧、盗難されるリスクを低減する。
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	カード会員データは暗号化されていないため、悪意のある人物からのデータアクセスを閲覧、盗難される可能性がある。
4. 代替コントロールの定義	代替コントロールを定義し、元のコントロールの目的および追加リスク(ある場合)にどのように対応するかを説明する。	悪意のある人物等によるカード会員データ非取外しの対策として、以下を実施する。 ・アクセス制御。 DBへのネットワーク接続は、アプリケーションサーバと限られた保守環境のみとする。 ・アカウント制御。 DBへのアクセスは、限られた保守要員のみとする。 ・セキュリティ監視。 DBへのアクセスは申請制とし、申請書とログインの統合チェックをおこなう。 DBへのログイン情報を監視対象とし、リアルタイム監視をおこなう。 脆弱性検査時。 四半期に一度の脆弱性検査にてネットワーク制御が正常に機能していることを確認する。

	必要な情報	説明
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	アクセス制御。 DBへアクセスする権限のない機材からアクセスを試み、アクセスが拒否されることを確認する。 ・アカウント制御。 DBへアクセスする権限のないアカウントからアクセスを試み、アクセスが拒否されることを確認する。 ・セキュリティ監視。 DBの操作内容がロギングされていることを確認する。 DBログインを試み、リアルタイムアラート発報されることを確認する。 脆弱性検査時。 四半期に一度の脆弱性検査時、ネットワークの脆弱性が検知されないことを以って、制御の正当性を確認する。
6. 維持	代替コントロールを維持するためのプロセスおよび管理を定義する。	アクセス制御。 アカウント制御。 不正なログインの検知するための方法を標準化する。 ・セキュリティ監視。 DBのアクセス申請書とログインの統合チェックを行い、作業とログの正当性を確認する。 DBのアラート発報による管理者通知フローを、改善(フォロー、実質等)化する。 脆弱性検査時。 四半期に一度の脆弱性検査時、要件1.1.6に定められた、ファイアウォールのレビューに加え、検疫機能を実施することで、許可された通信のみ検知されることを確認する。

IV.

PCI DSS対応事例のご紹介

17. 仮想化環境のウイルス対策

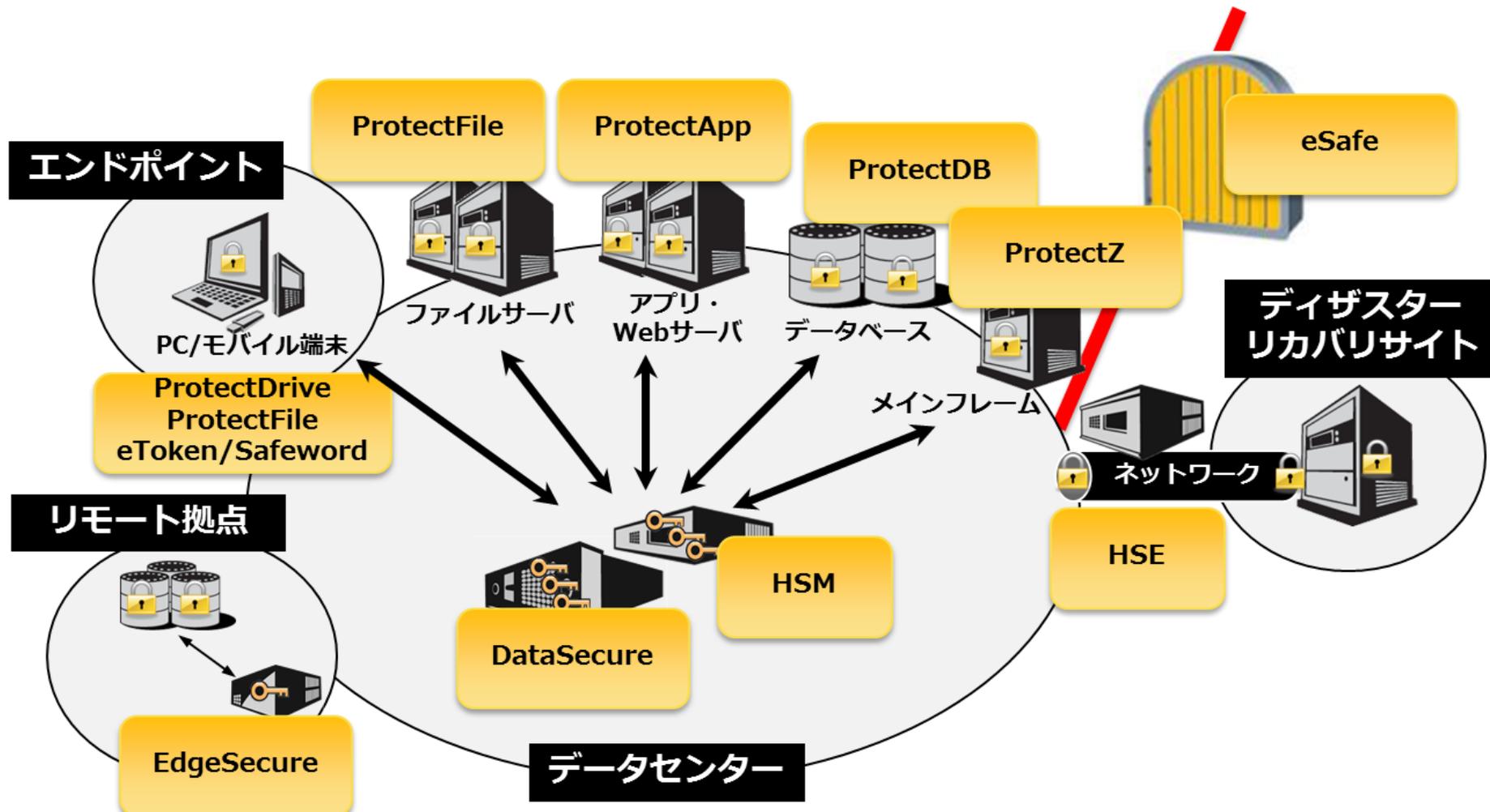


- ✓ 各仮想OSにウイルス対策ソフトのインストール
- ✓ 各仮想OSにウイルスパターンファイルが配信
- ✓ 各仮想OS毎にウイルス対策の設定管理が必要

- ✓ ESXに1つのVirtual Applianceをインストール
- ✓ Virtual Applianceにパターンファイルを配信
- ✓ Virtual Applianceで設定を一括管理

18. クレジットカード情報の難読化

◆ 暗号鍵管理用のハードウェアを使った暗号化対応のソリューション提供。
インターネット



19. 次世代ワンタイムパスワード認証

- ◆ 急激に増えている中間者攻撃による不正送金を水際で阻止
- ◆ 北米・南米・欧州で採用が始まっている。(邦銀は採用検討中)



**1.画面上から
トランザクションデータを
読み取り**

**2.トランザクションデータ表示
(振込額、口座等)
3.ユーザが目視確認
4.正しいことを確認してボタン
押下、署名データが表示**

Click 1
Verify amount transferred

Click 2
Verify account number

Click 3
Numeric signature is generated

**署名データ生成ロジック:
トークン内部の160bits鍵
(トークン毎にユニーク)+
時刻 (GMT)+トランザク
ション値**

トランザクション画面:
TRANSFERS Step 1 2 3
Enter the sum you want to transfer:
\$9,088.00
Enter the destination account number:
88334-8838797

トランザクション画面:
TRANSFERS Step 1 2 3
798037
SUBMIT

まとめ

今年のメッセージ：

この一年間で、**PCI DSS準拠の必要性**はグンッとアップ！しています。
但し、2018年3月を期限とすると**システム対応時間は残り少ない**です。
まずは情報**システム強化のための予算感を掴み**、期限内にどのように
準拠対応を進めていけるのかを**検討する材料を揃える**ことです。
ポイントとなるのは、現場負担の少ないギャップ分析と情報システムの
運用負荷をこれ以上増やさない**ツールありきの運用**検討だと考えます。

**一刻も早くシステム投資の予算感を掴み
リスクの高いところから対策を行なっていく
戦略的なセキュリティ対策が求められています**

ご清聴ありがとうございました...



この資料は、著作権法と不正競争防止法上の保護を受けています。本書の一部あるいは全部について、TIS株式会社から文書による承諾を得ずに、いかなる方法においても無断で複写、複製、ノウハウの使用、企業秘密の展開等を行うことは禁じられています。

●お問い合わせ

<http://www.tis.co.jp>

TIS株式会社

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