「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

TIS
IT Holdings Group
Go Beyond

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

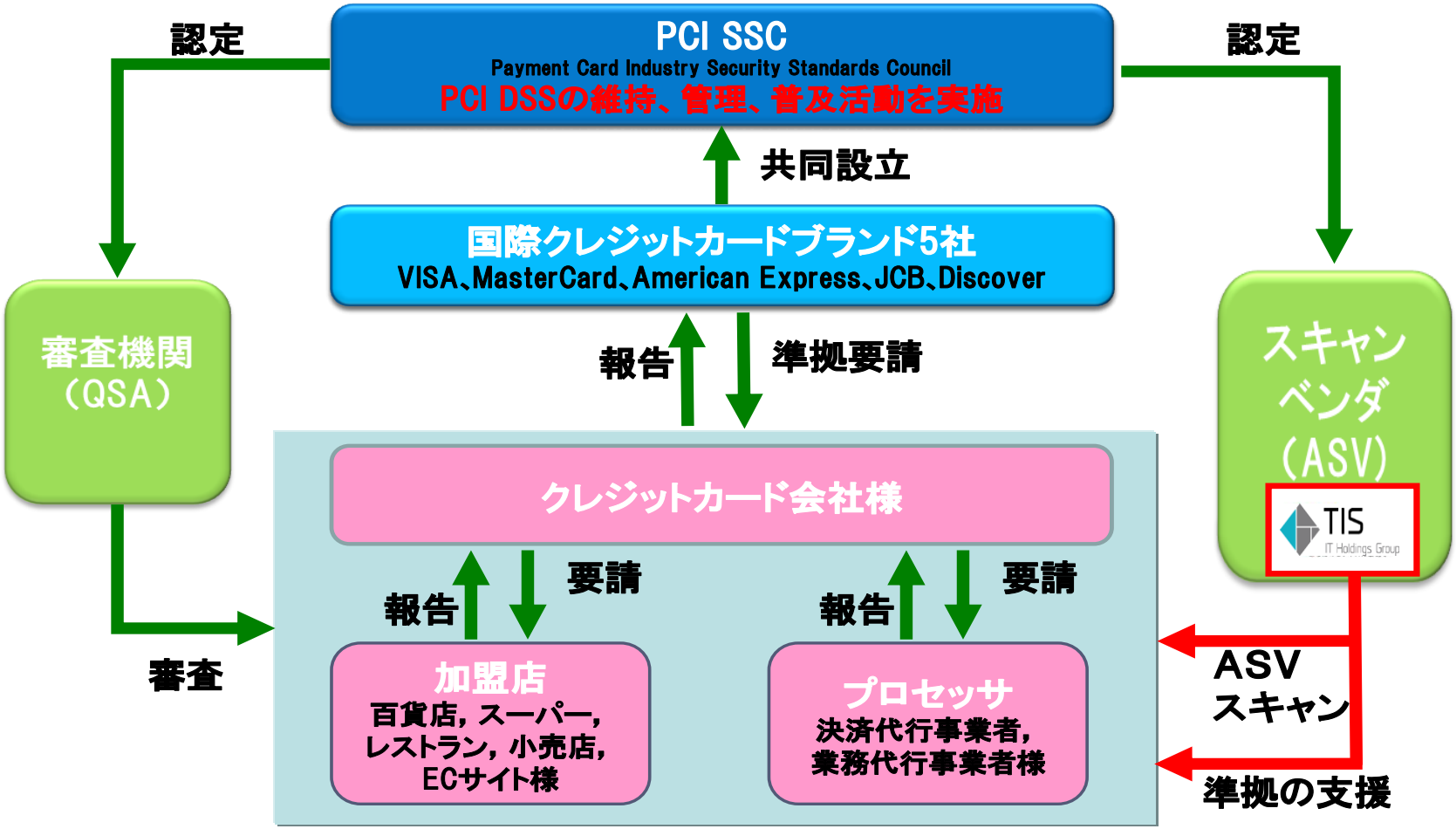
氏　名　三木　基司（ミキ　モトジ）
略　歴

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

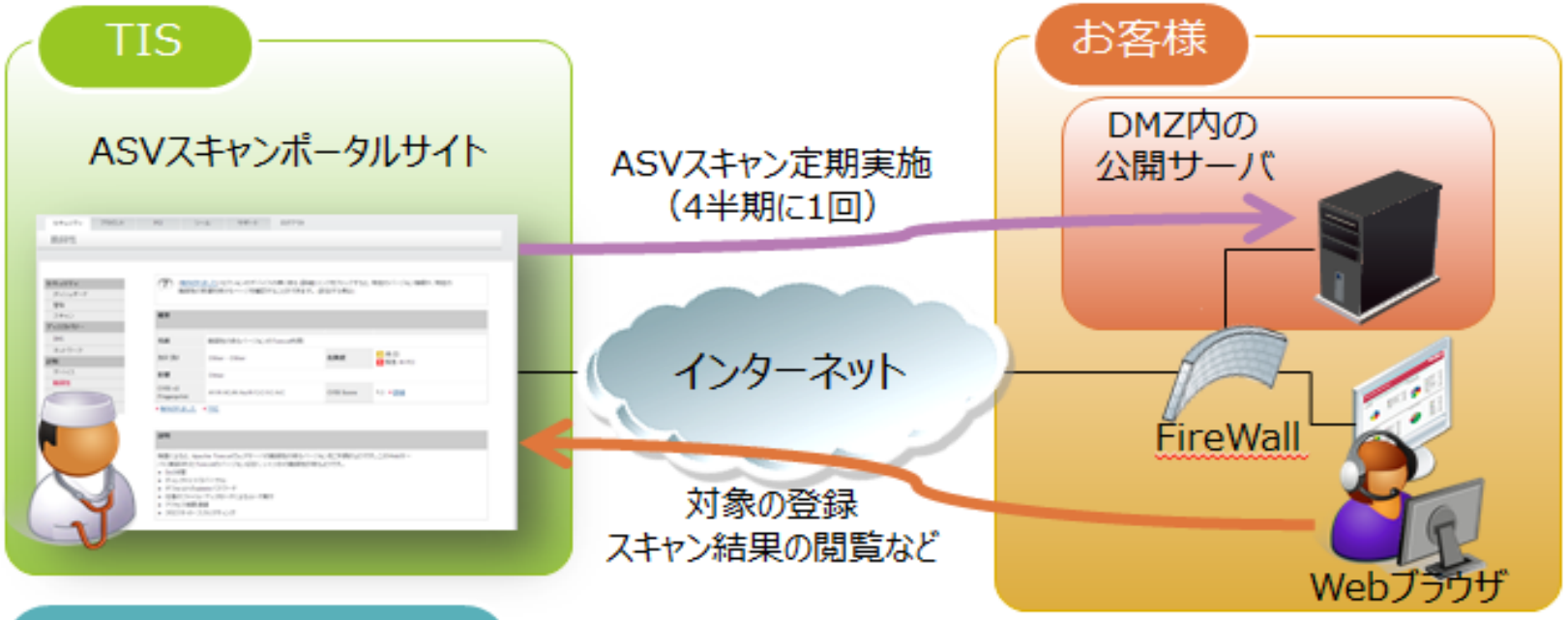
TIS株式会社のご紹介

- ◆ 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出来ます。



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 ～

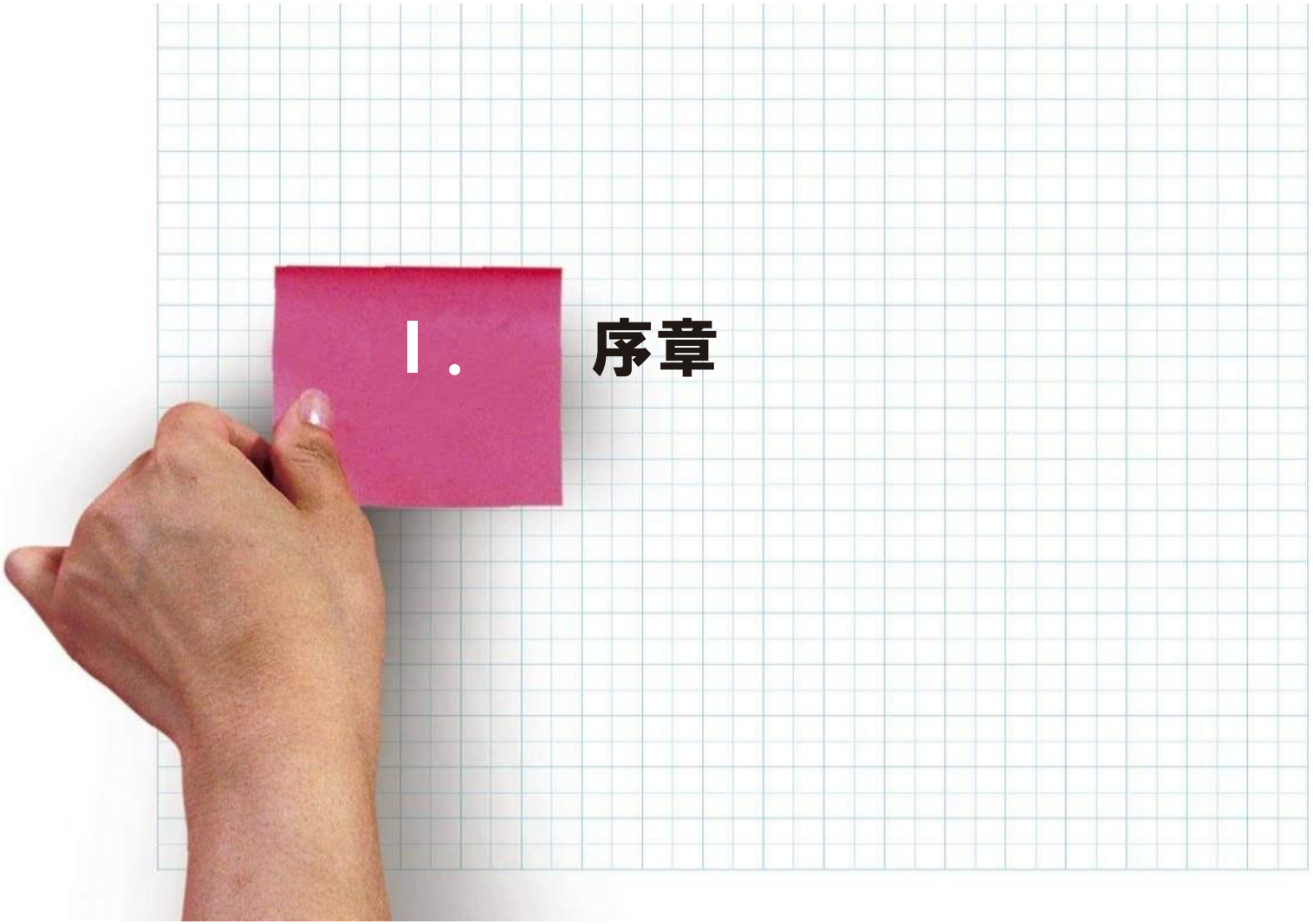
ポイント2 2012年　日本クレジット協会が準拠の実行計画を公表

「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

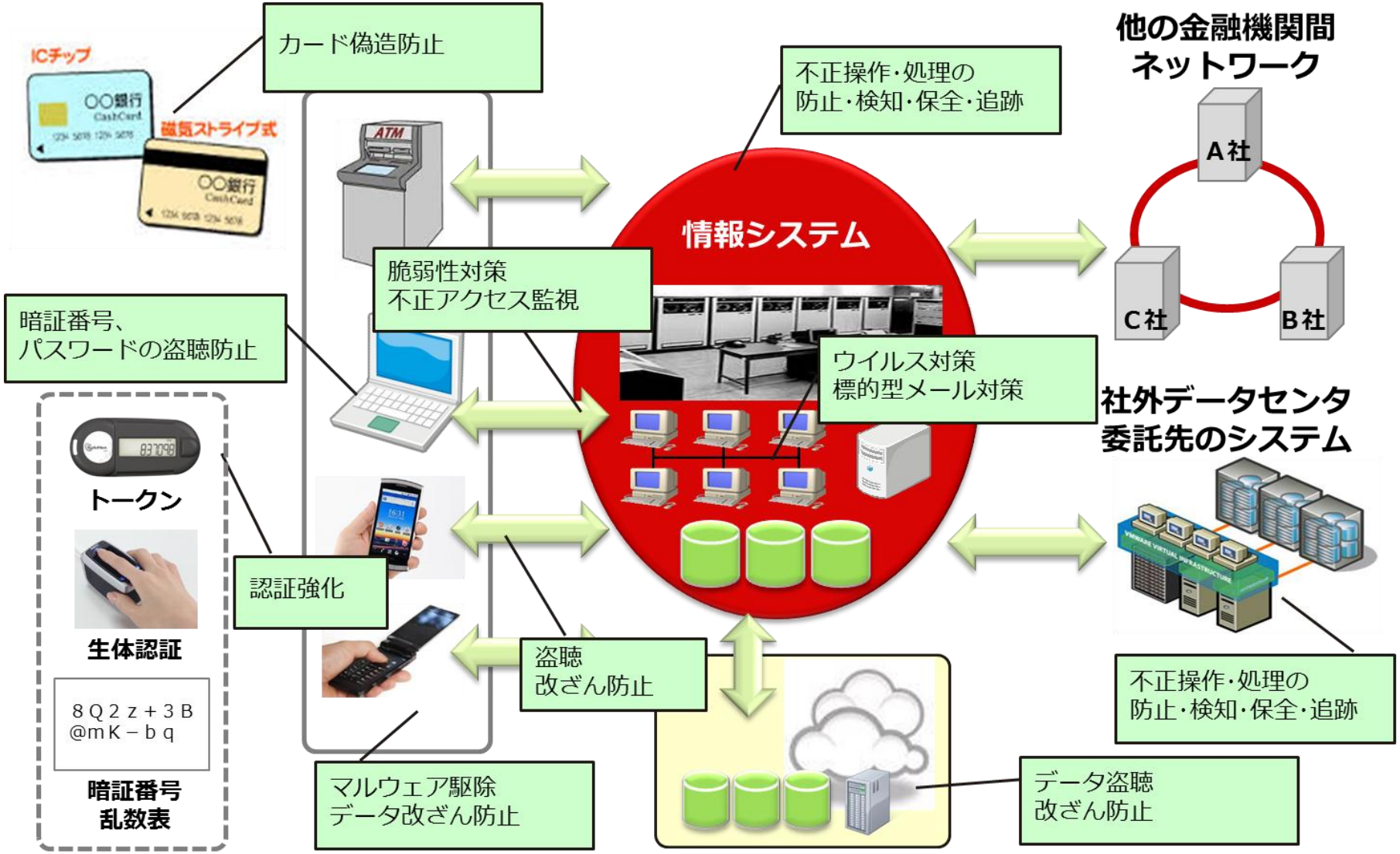
ポイント3 2013年　PCI DSS ver3.0 の公開

- 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



Ⅰ. 序章

1．情報システムのセキュリティ対策（現在）



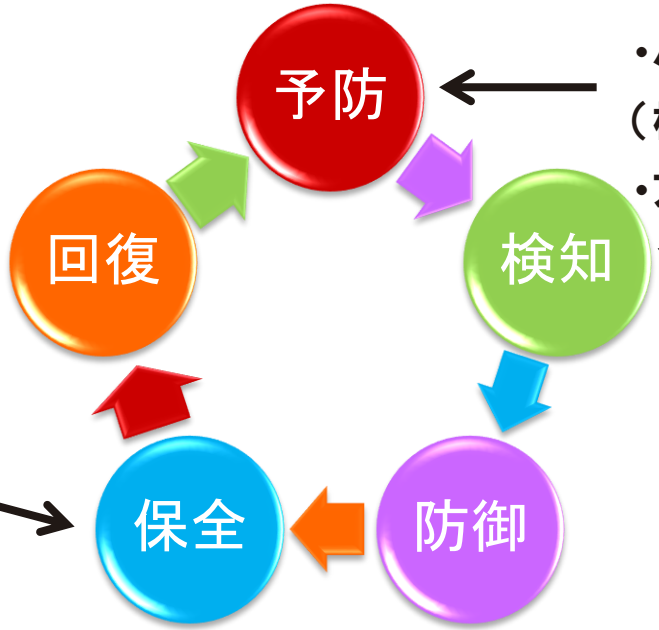
引用元：日本銀行金融研究所第14回情報セキュリティ・シンポジウム（2012年12月20日）

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。



・利用者認証方式強化（2因子認証）
・パスワード強化
（桁数、文字種、変更サイクル）
・アクセス制御強化

・改ざん検知
・ログのチェック
- 同一アドレスからのアクセス集中
- 連続した認証失敗
- トラフィック量の急激な変化
- システム設定値の変更

・追跡に必要なログ保全
（サーバ、DB、NW機器）
・安全なバックアップの確保

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**」

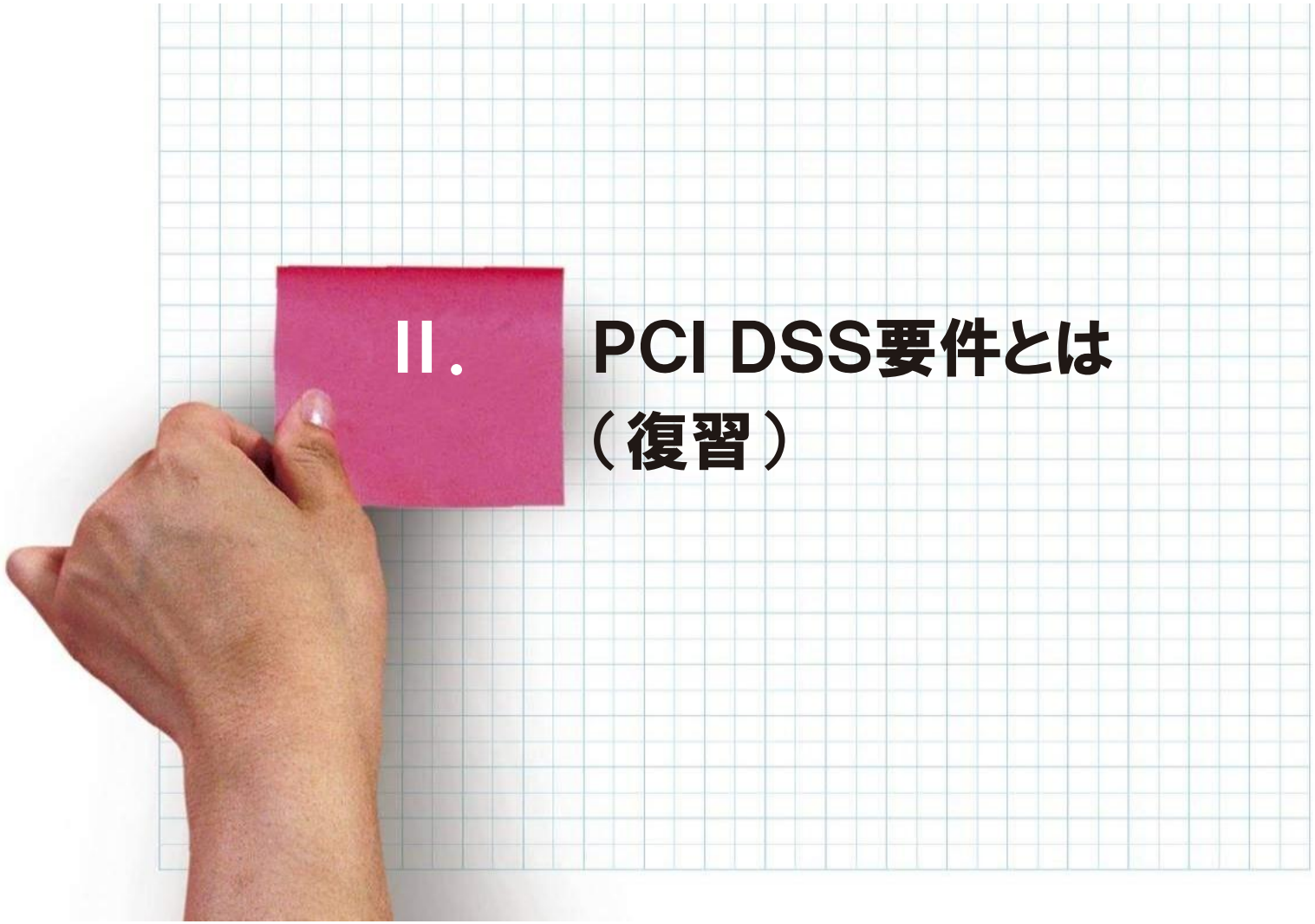
今年のメッセージ ：

この一年間で、**PCI DSS準拠の必要性**はグンっとアップ！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。

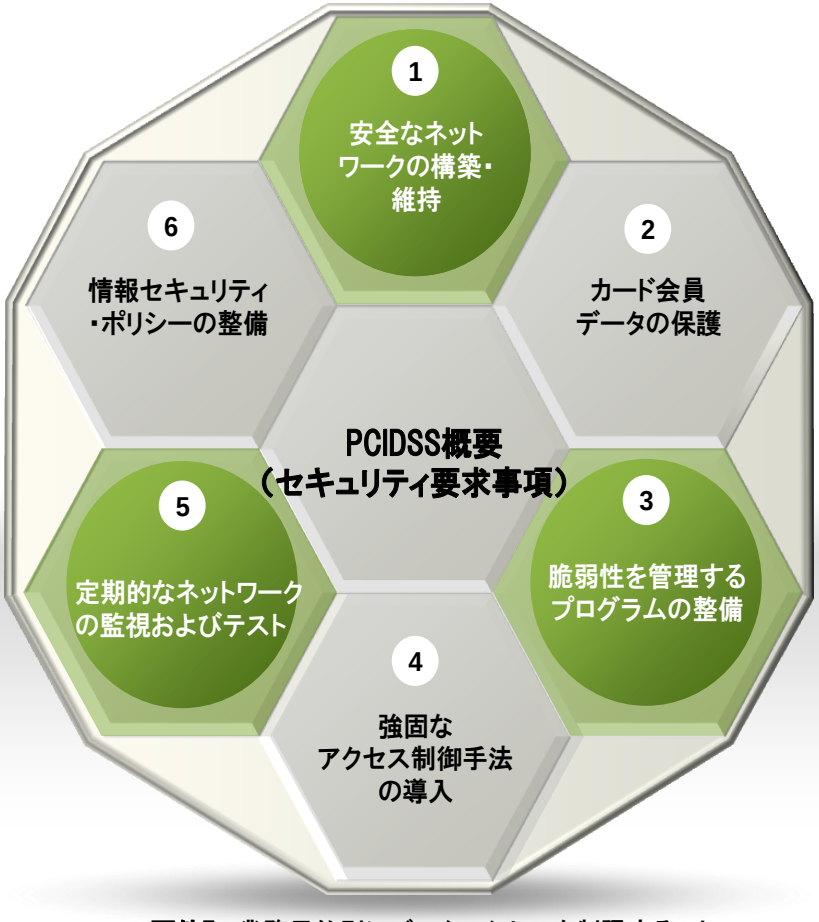
ポイントとなるのは、現場負担の少ないギャップ分析と情報システムの運用負荷をこれ以上増やさない**ツールありきの運用**検討だと考えます。



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エ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

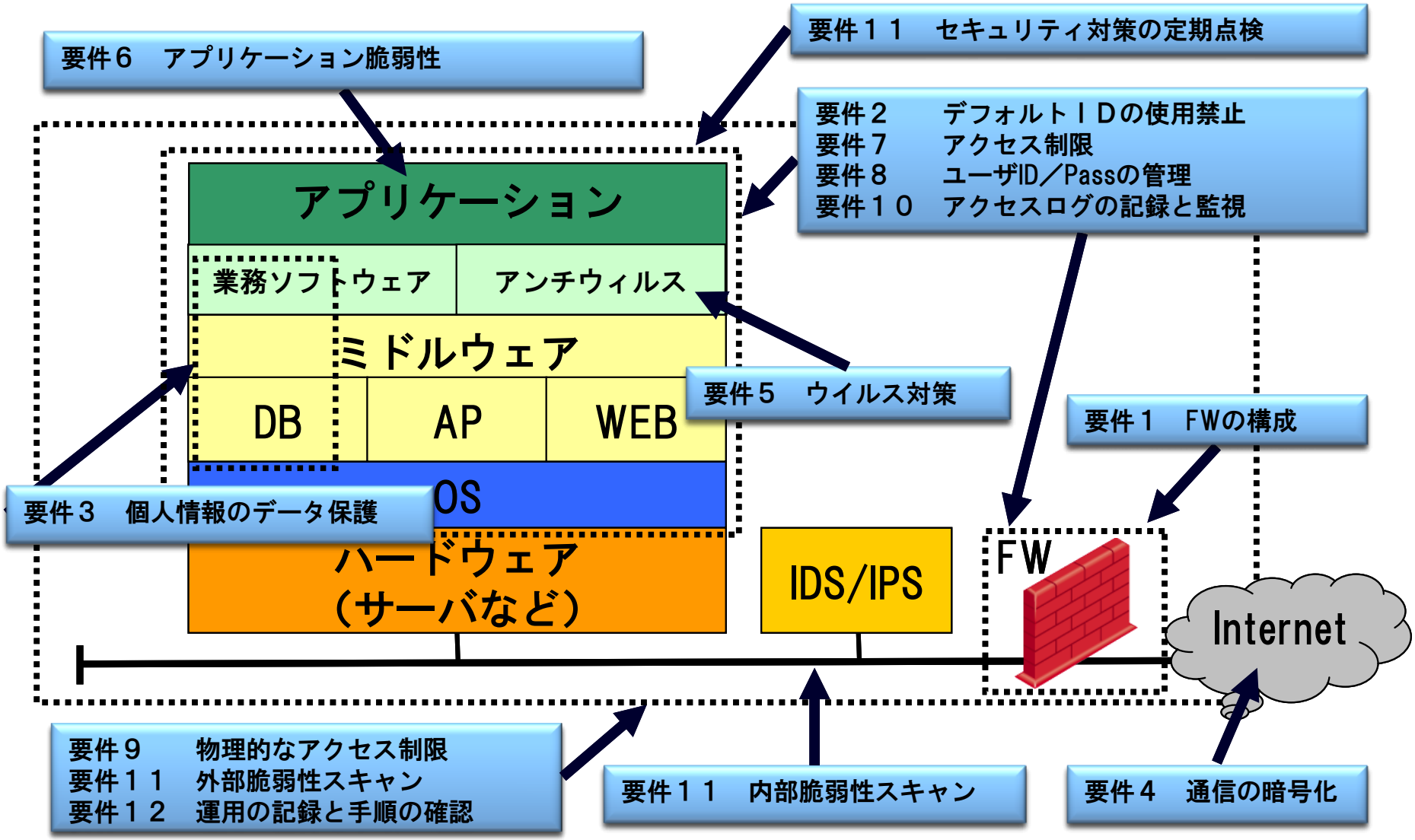
要件3：保存されたデータを安全に保護すること
要件4：公衆ネットワーク上でカード会員情報・センシティブ情報を送信する場合、暗号化すること

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 DDS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！

ご提案1：

10. 情報システムの現状確認①

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。

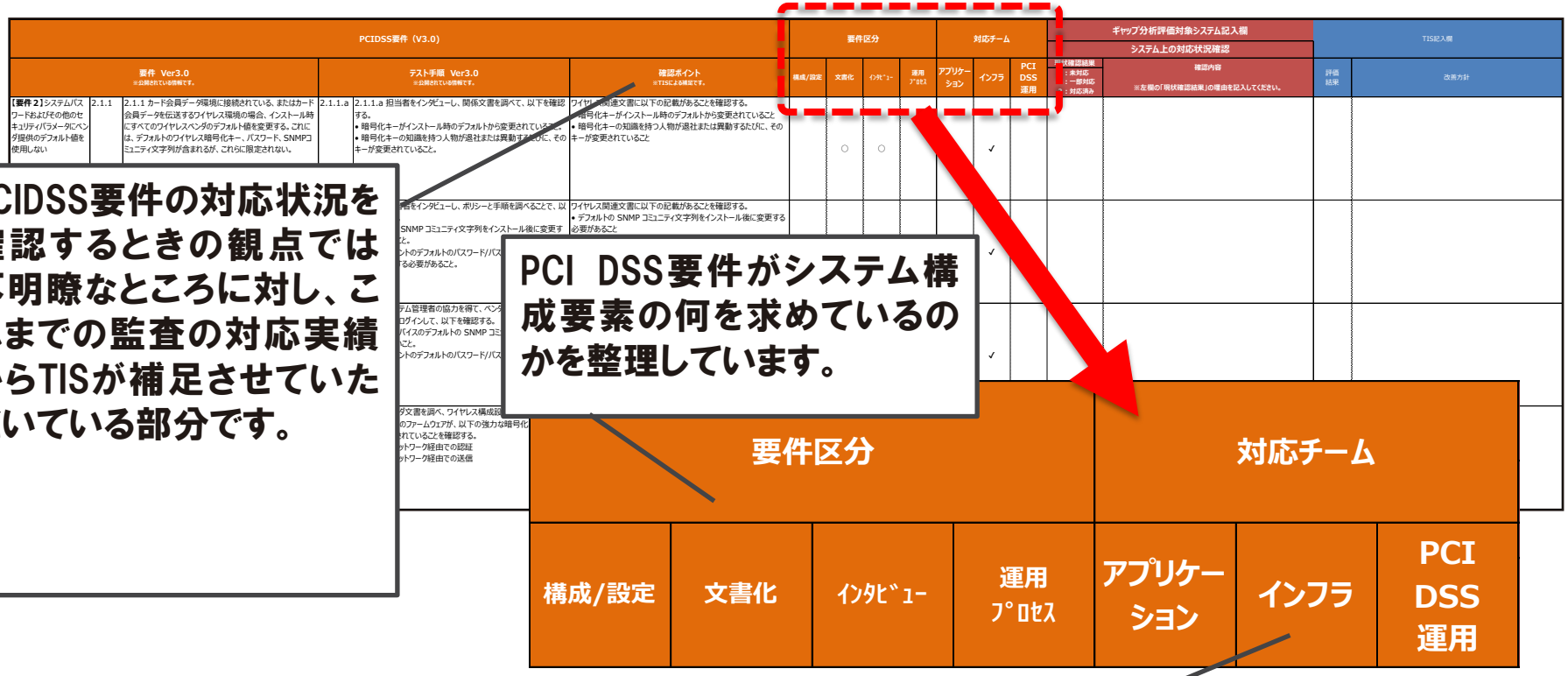
ポイント2：要件項目ごとにリスク対応の目的と何を確認すれば良いのか具体的なチェック方法が解ります。

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。

ご提案1：

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。



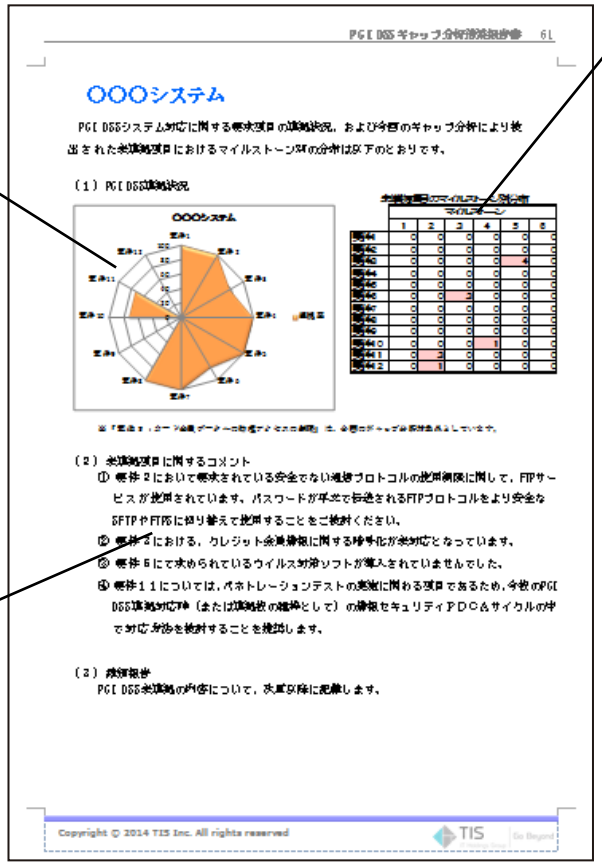
ご提案2：

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。

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を記載しています。



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。

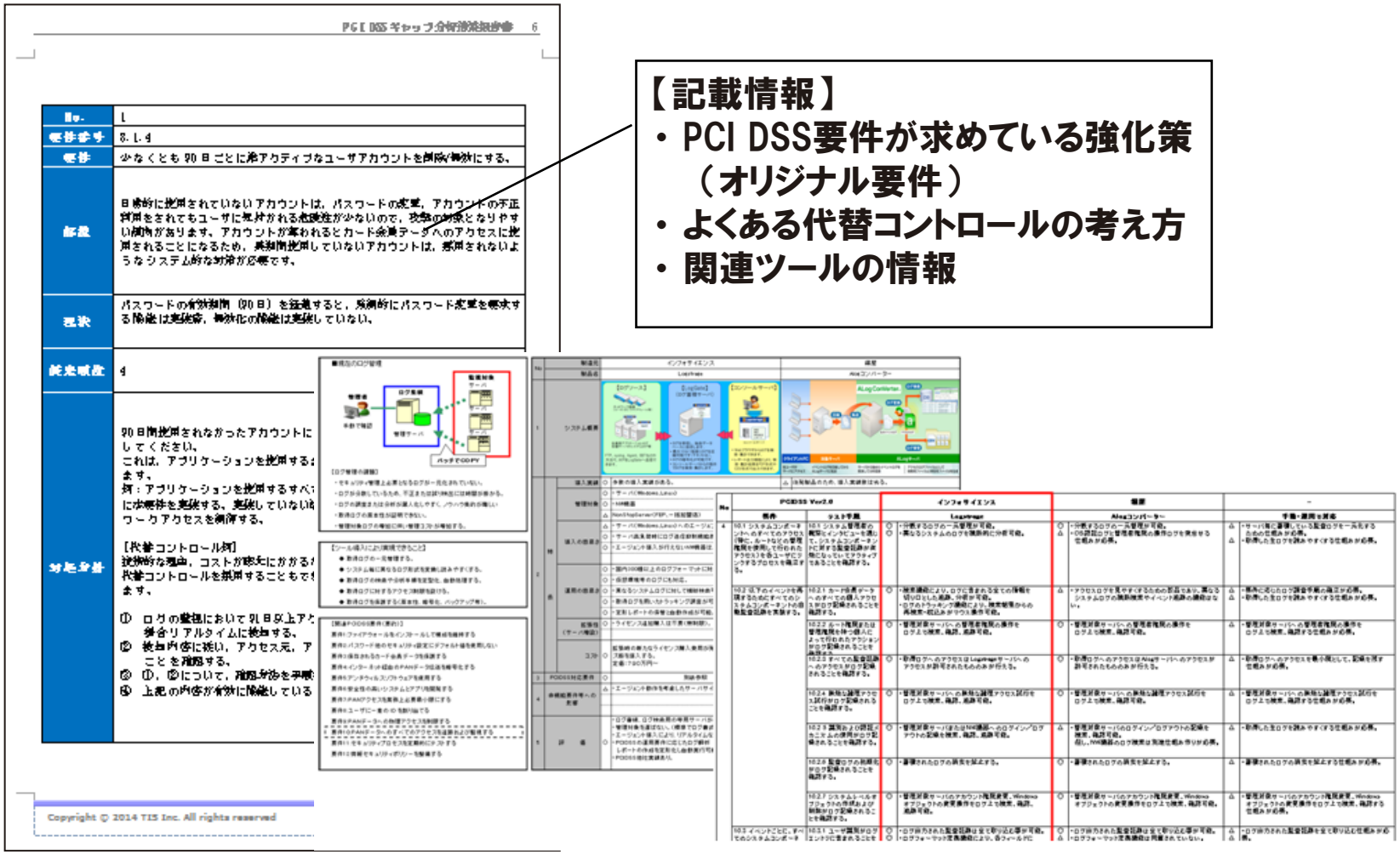
※ PCI SSCが公開している優先度（マイルストーン）

優先順位	リスク低減効果	目的	具体的実施策
1	大	不必要な情報の削除	クレジットカード番号/機密認証データの削除
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 通信時の暗号化、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/PW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	小	その他（文書化等）	ポリシ整備、運用手順書整備、運用確認書整備

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。

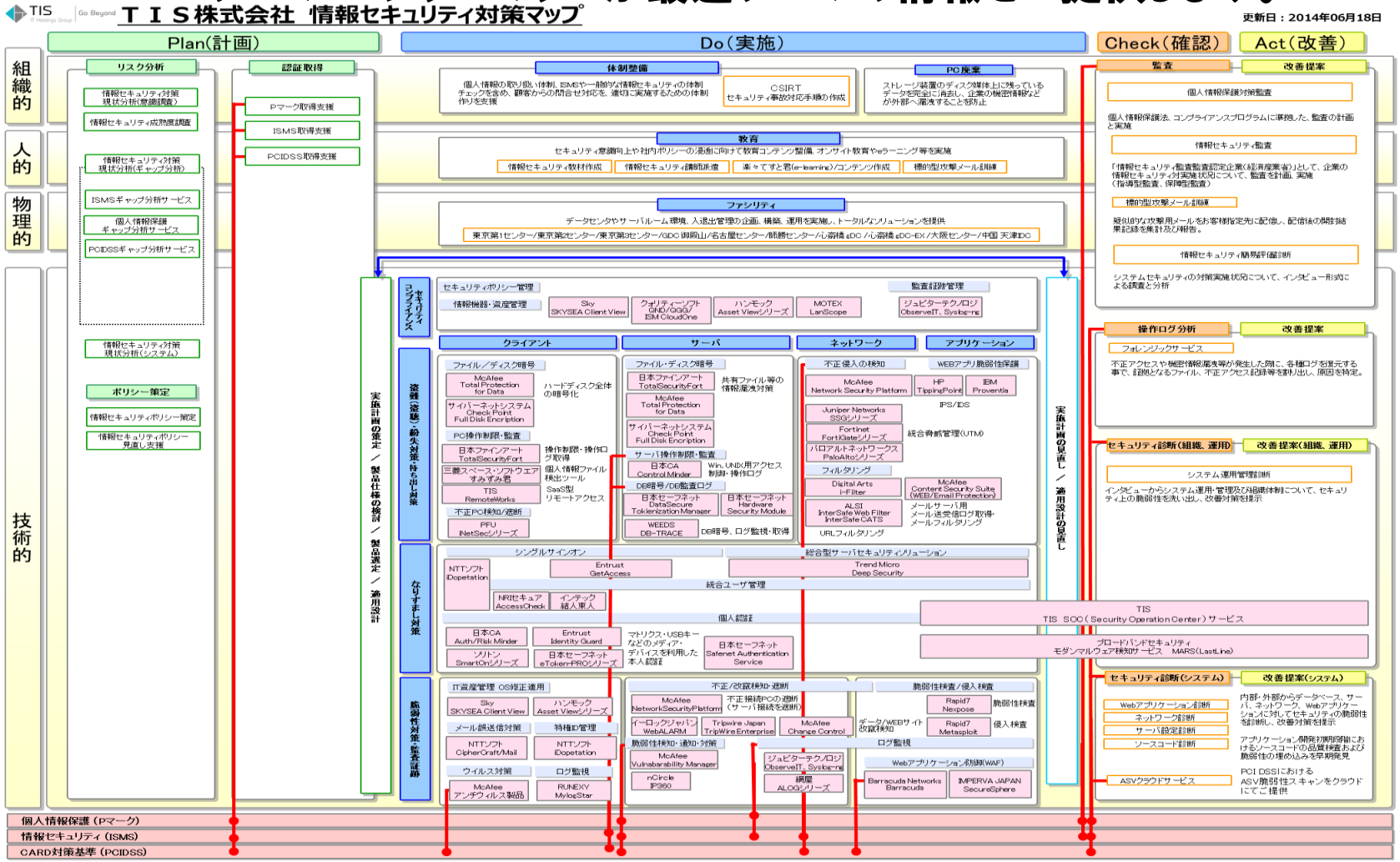


【記載情報】
- PCI DSS要件が求めている強化策（オリジナル要件）
- よくある代替コントロールの考え方
- 関連ツールの情報

ご提案3：

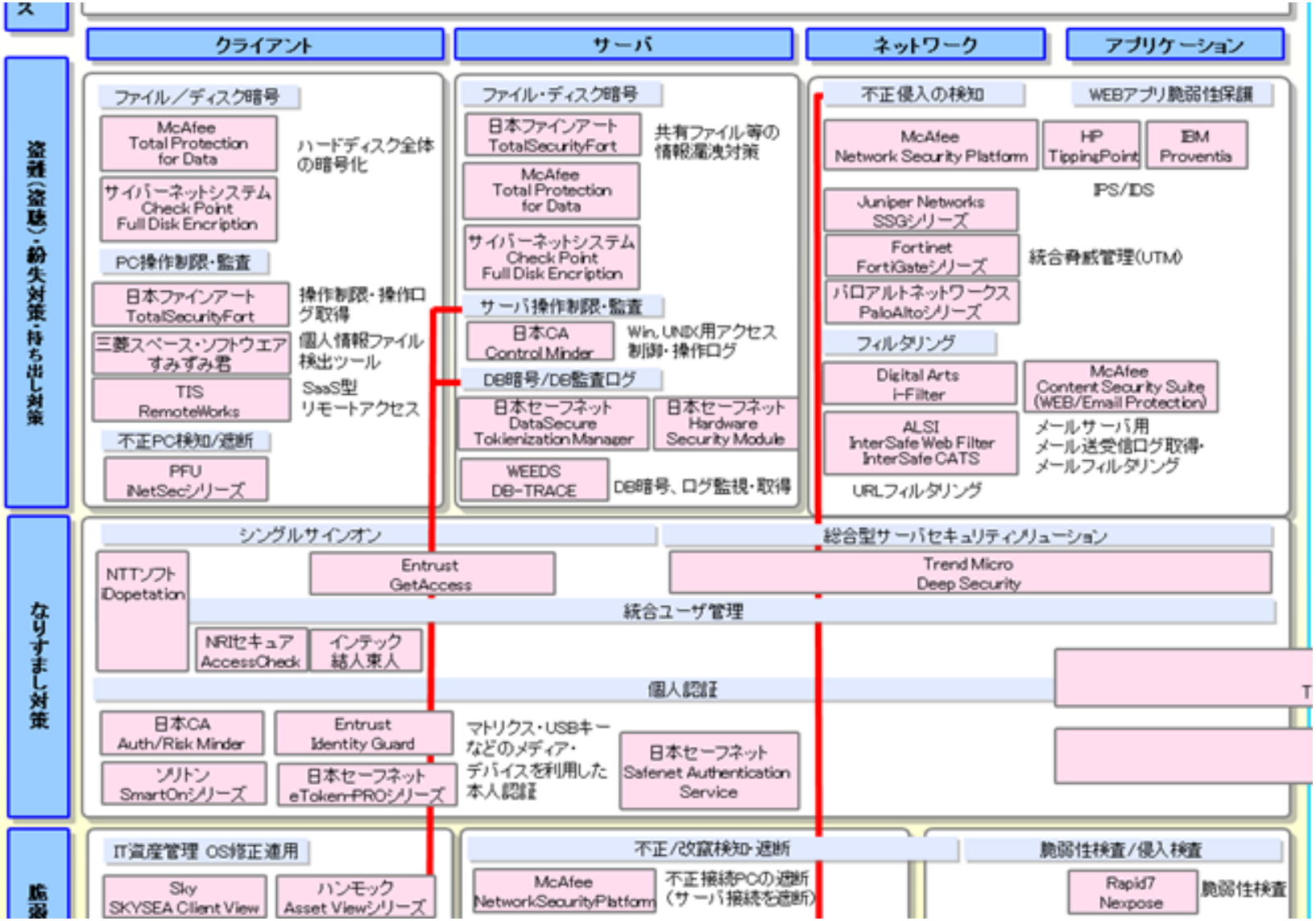
14. ツールによるPCI DSS準拠の検討①

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。



ご提案3：

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]

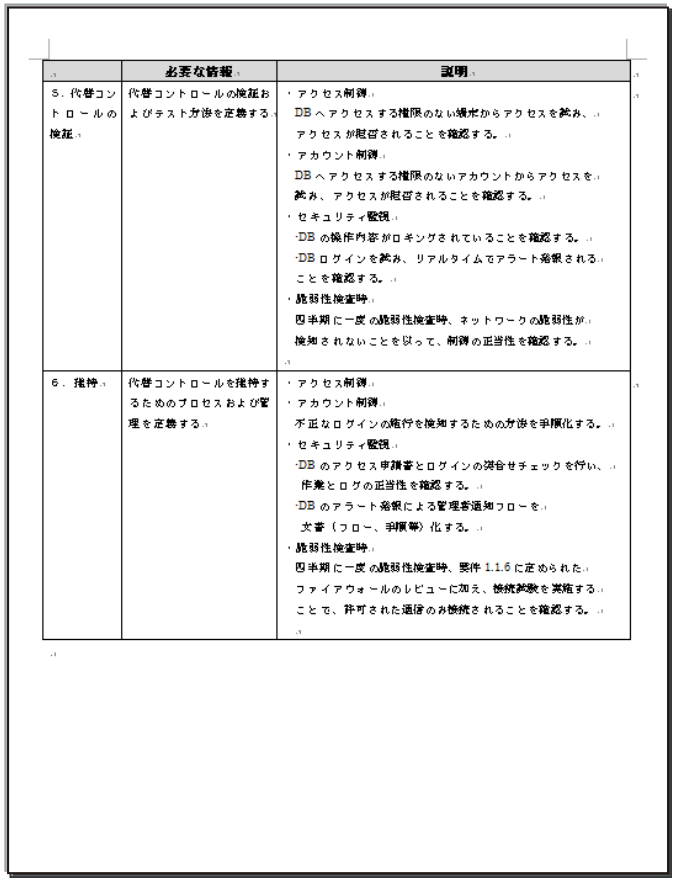
バージョン	1.0
改訂日	2014/XXXX

要件番号：3.4

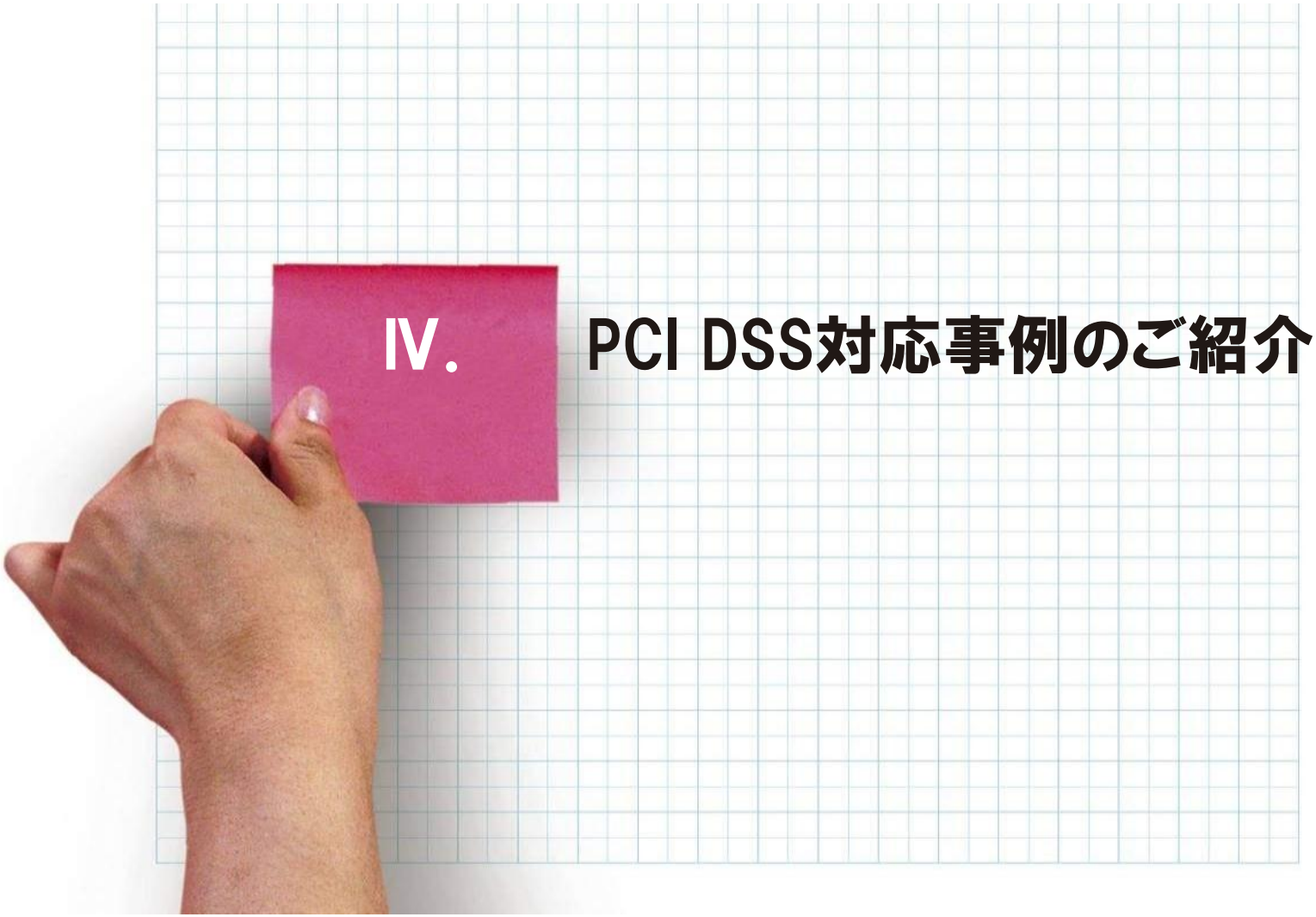
以下の手法を使用して、すべての保存場所で PAN を読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。

- 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軽減
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詐取への対策として、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端末のみとする。 ・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 ログインの突合せ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。

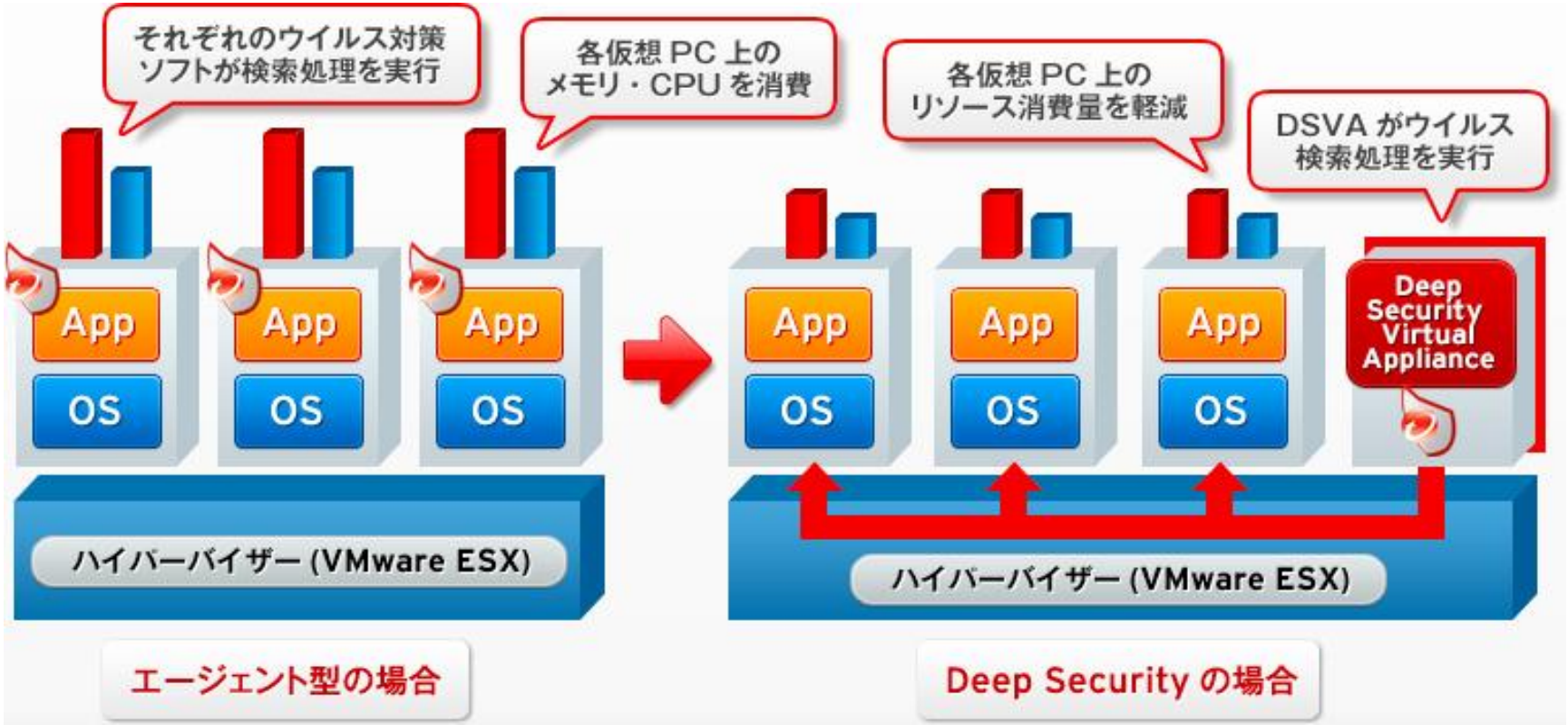


	必要な情報	説明
5．代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	・アクセス制御： DBへアクセスする権限のない端末からアクセスを試み、 アクセスが拒否されることを確認する。 ・アカウント制御： DBへアクセスする権限のないアカウントからアクセスを 試み、アクセスが拒否されることを確認する。 ・セキュリティ監視： -DBの操作内容がロギングされていることを確認する。 -DBログインを試み、リアルタイムでアラート発報される ことを確認する。 ・脆弱性検査時： 四半期に一度の脆弱性検査時、ネットワークの脆弱性が 検知されないことを以って、制御の正当性を確認する。
6．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： 不正なログインの実行を検知するための方法を手順化する。 ・セキュリティ監視： -DBのアクセス申請書とログインの突合せチェックを行い、 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 文書（フロー、手順等）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、接続試験を実施する ことで、許可された通信のみ接続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



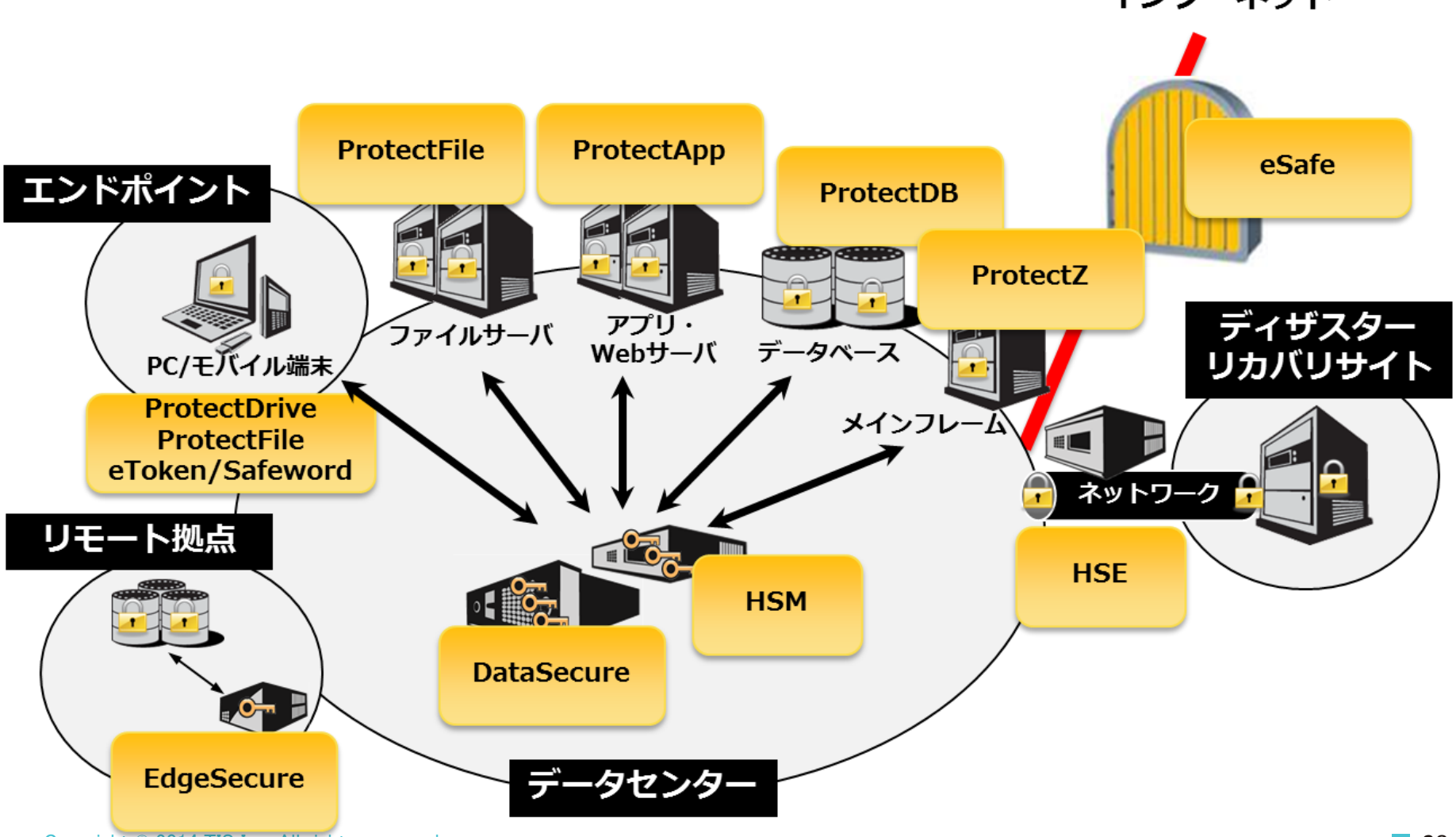
- 各仮想OSにウイルス対策ソフトのインストール
- 各仮想OSにウイルスパターンファイルが配信
- 各仮想OS毎にウイルス対策の設定管理が必要

- 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

事例紹介：

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。



事例紹介：

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）

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っとアップ！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．．．

●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