PCI DSSセキュリティフォーラム2013
～PCI DSSへの効率的な対応を探る～

TIS
あなたのビジネスに最適を

PCI DSS準拠にむけた課題例とツールによる解決策

2013年 7月 10日

TIS株式会社
IT基盤サービス第1事業部
シニアエキスパート　三木 基司

本日のアジェンダ

TIS
あなたのビジネスに最適を

第１部　PCIDSS制度における当社の位置付け

1. PCI DSS制度におけるTISの位置付け
2. 当社取り組み姿勢
3. PCI DSS準拠支援のTISフレームワーク

第2部　よくあるPCI DSS推進課題

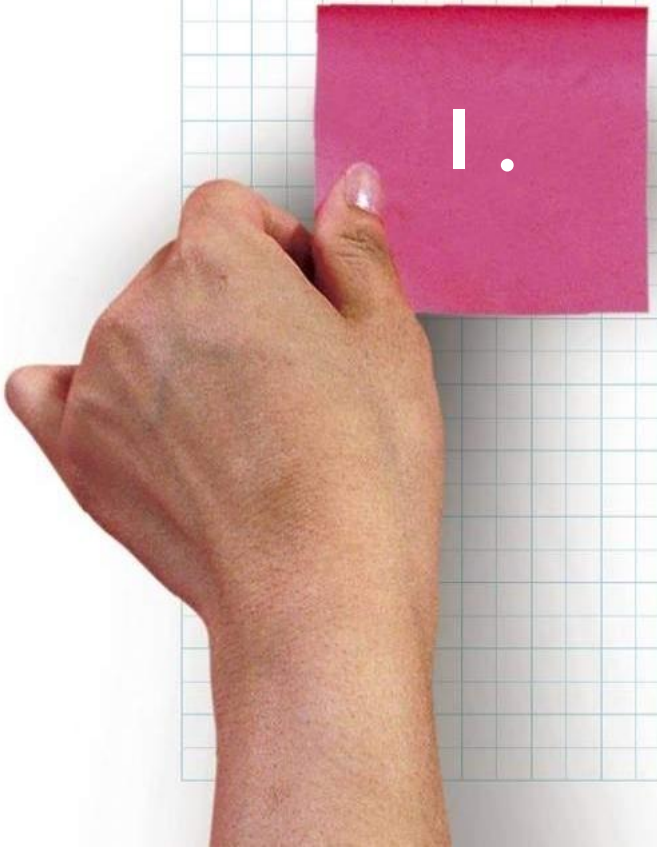
4. よくあるPCI DSS準拠対応への質問
5. 準拠対象範囲明確化の課題
6. カード会員情報の取扱い範囲の決め方

第3部　よくある課題

7. PCI DSS準拠対応上のよくある課題①
8. PCI DSS準拠対応上のよくある課題②
9. PCI DSS準拠対応上のよくある課題③

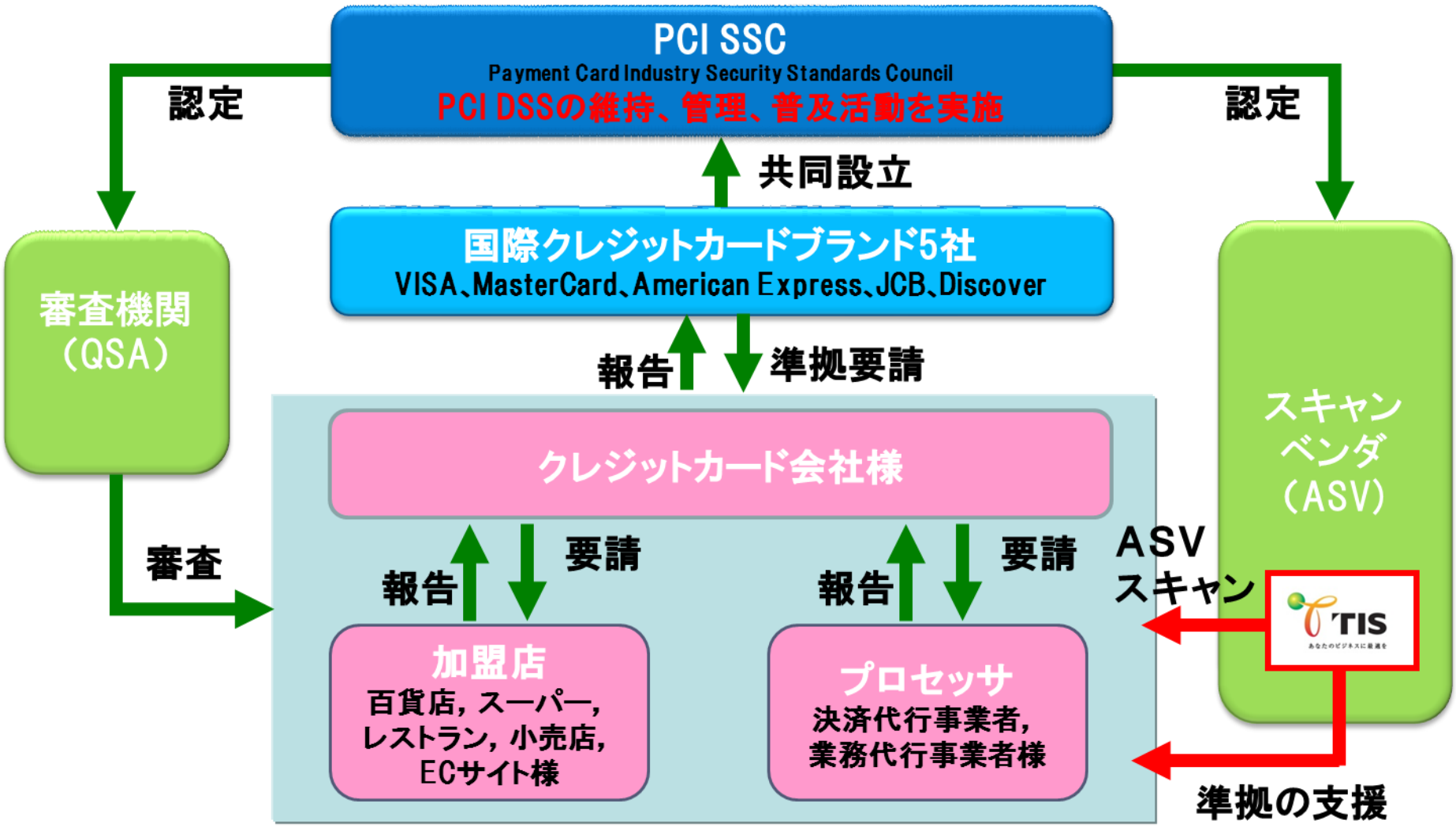
第4部　ツールによる解決策

・ツールによる課題解決①「特権ID管理」
・ツールによる課題解決②「DB暗号化」



Ⅰ. PCIDSS制度における当社の位置づけ

1. PCI DSS制度におけるTISの位置付け



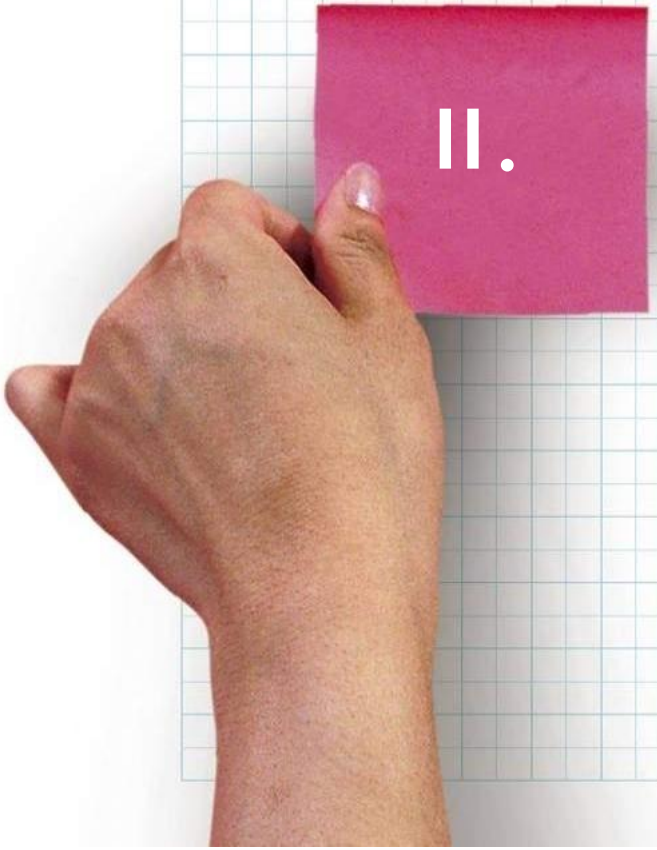
2. 当社取り組み姿勢

- 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
- PCI DSS準拠対象のすべての企業様を全国規模でサポート

カード会社様 加盟店様	▶	PCI DSS準拠支援 コンサルサービス
インターネット加盟店様	▶	インターネット加盟店様向け 認証プログラム
カード情報取扱いデータセンタ様	▶	SIサービス、ソリューション提供

3. PCI DSS準拠支援のTISフレームワーク

※★印はQSA実施タスクです。
※グリーンの網掛けタスクは、別途お見積りとなります。また、ピンクの網掛けは、認定機関による作業タスクです。



II. よくあるPCI DSS推進課題

4. よくあるPCI DSS準拠対応への質問

TIS
あなたのビジネスに最適を

◆ PCI DSS準拠対応の場面でよく耳にする話題

- これさえあれば大丈夫というソリューションはあるのか
- 情報システム部だけで対応すればよいか
- 社内にある情報システムはすべて対応しなければならないのか
- 現在のセキュリティ施策と整合できるのか

準拠対応に向けて考える事

◆ PCI DSS要件への**準拠対象範囲を明確**にする
◆ 運用負荷をこれ以上増やさない**ツールありきの運用**を検討する
◆ ISMSやプライバシーマークのセキュリティ対策との整合性を考慮する

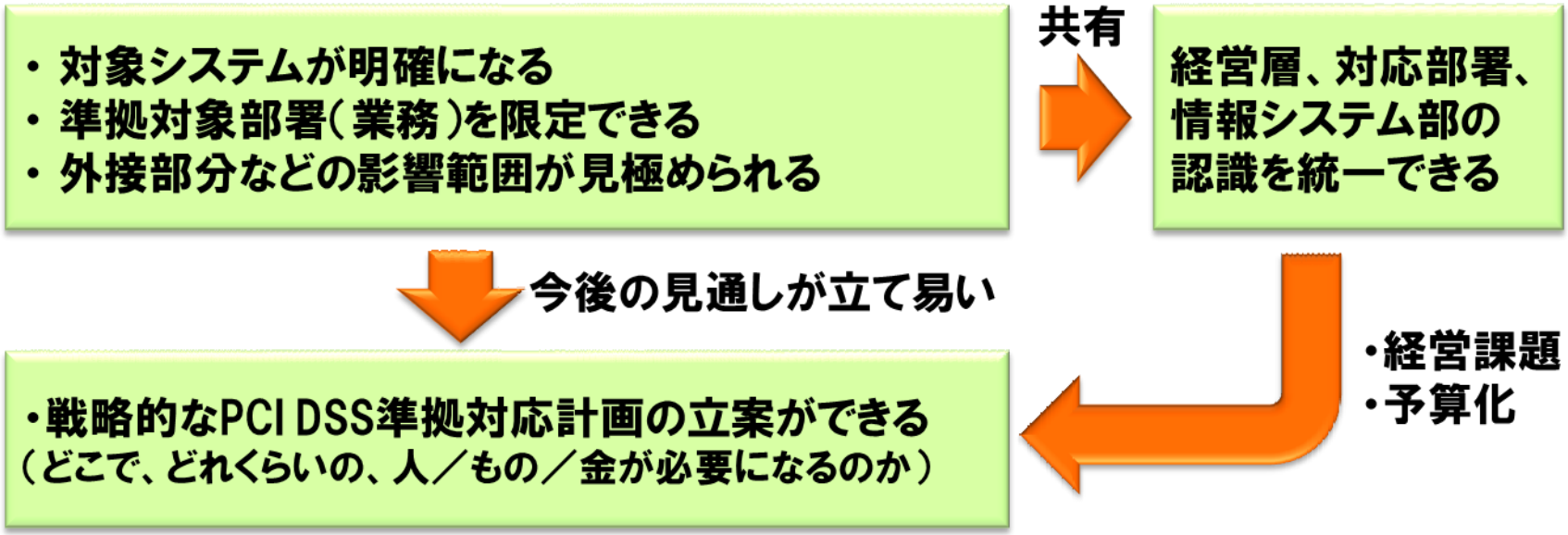
5. 準拠対象範囲明確化の課題

◆ 準拠対象範囲が整理(または把握)ができていない
※ 準拠対象範囲＝カード会員情報の保管・伝送・処理の取扱い範囲

◆ カード会員情報の取扱い範囲を表現する方法が分からない

※制度的に少し問題もあるかも．．．と感じます。
「統一的な準拠対象範囲の決定手法が規定されず、
QSA側の判断基準も曖昧に感じる」

【準拠対象範囲明確化のメリット】



6. カード会員情報の取扱い範囲の決め方

◆ カード会員情報の取扱い範囲を3つの観点で明確にしておくことで
QSAに対する適切かつ合理的な説明が可能

その1： 情報システム上の取扱い範囲の確認

システム構成図やネットワーク図をもとに、
どのようにカード会員情報が保管・伝送・処理
されているのか確認する。

その2： カード会員情報取扱い部署の確認

部署（または業務フロー）ごとに、カード会員情報の
取扱い状況を確認する。

その3： オフィス環境での取扱い範囲の確認

情報システムの設置場所やバックアップ媒体などの
情報の保管場所について確認する。
また、情報システムの操作（閲覧・検索・更新 等）を行う
場所を確認する。

Ⅲ. よくある課題

7. PCI DSS準拠対応上のよくある課題①

TIS
あなたのビジネスに最適を

◆ PCI DSS準拠対応上のよくある課題

- **技術的な課題**
- 技術的な対応以外の課題
- 世間のセキュリティ事故をふまえた対応課題

◆ 技術的な課題

• 管理アクセスのための製品が暗号化に対応できていない	要件2.3
• DB等を暗号化作業する際の既存業務への影響が大きい	要件3.4
• 暗合化キーがアプリケーションに組み込まれている為変更が不可能	要件3.6
• 利用しているログインシステムでは対応できない	要件8.5
• ウイルスの自動更新ができない	要件5.1
• 必要な項目がログとして出力できない	要件10.3

8. PCI DSS準拠対応上のよくある課題②

TIS
あなたのビジネスに最適を

◆ PCI DSS準拠対応上のよくある課題

- 技術的な課題
- **技術的な対応以外の課題**
- 世間のセキュリティ事故をふまえた対応課題

◆ 技術的な対応以外の課題

・カード会員データの暗号化キーの管理手順が複雑すぎて運用が困難	要件3.6
・リモートアクセスをする保守業者に2因子認証を要求するのが困難	要件8.3
・四半期に一度のワイヤレスアクセスポイントの検査拠点が多すぎて困難	要件11.1
・本番環境へのペネトレーションテストの調整が困難	要件11.3
・外部委託先のPCI DSSの準拠状況のモニタリングの実施が困難	要件12.8

9. PCI DSS準拠対応上のよくある課題③

TIS
あなたのビジネスに最適を

◆ PCI DSS準拠対応上のよくある課題

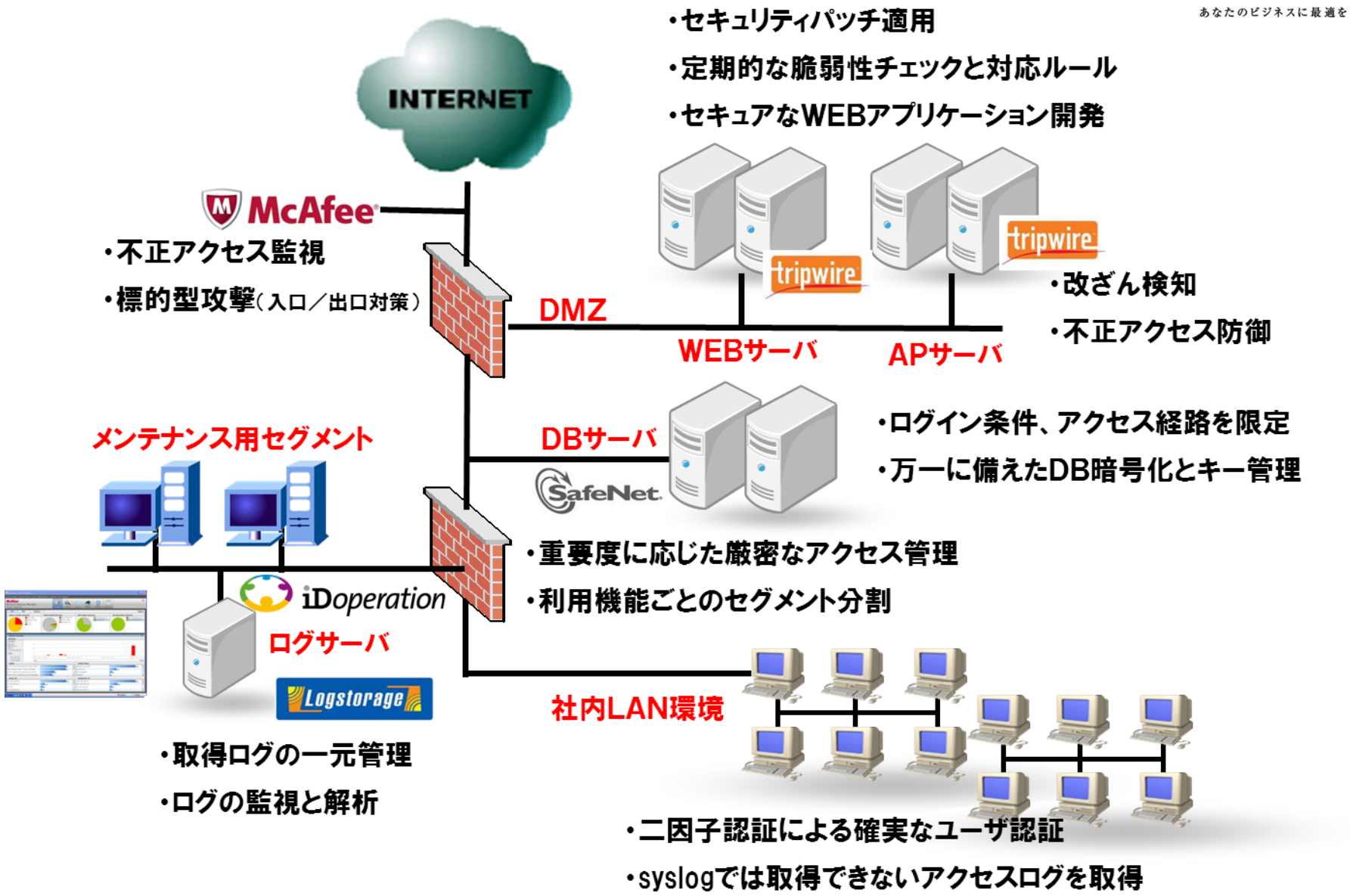
- 技術的な課題
- 技術的な対応以外の課題
- **世間のセキュリティ事故をふまえた対応課題**

◆ 万一の情報セキュリティ事故発生時の対応に関わる要件

• ウイルス対策ソフトの未導入	要件5
• セキュリティ修正プログラム(パッチ)の未適用	要件6.1
• 四半期ごとの脆弱性テスト	要件11.2
• アクセスログの未取得	要件10
• ファイルの改ざん検知未導入	要件11.5

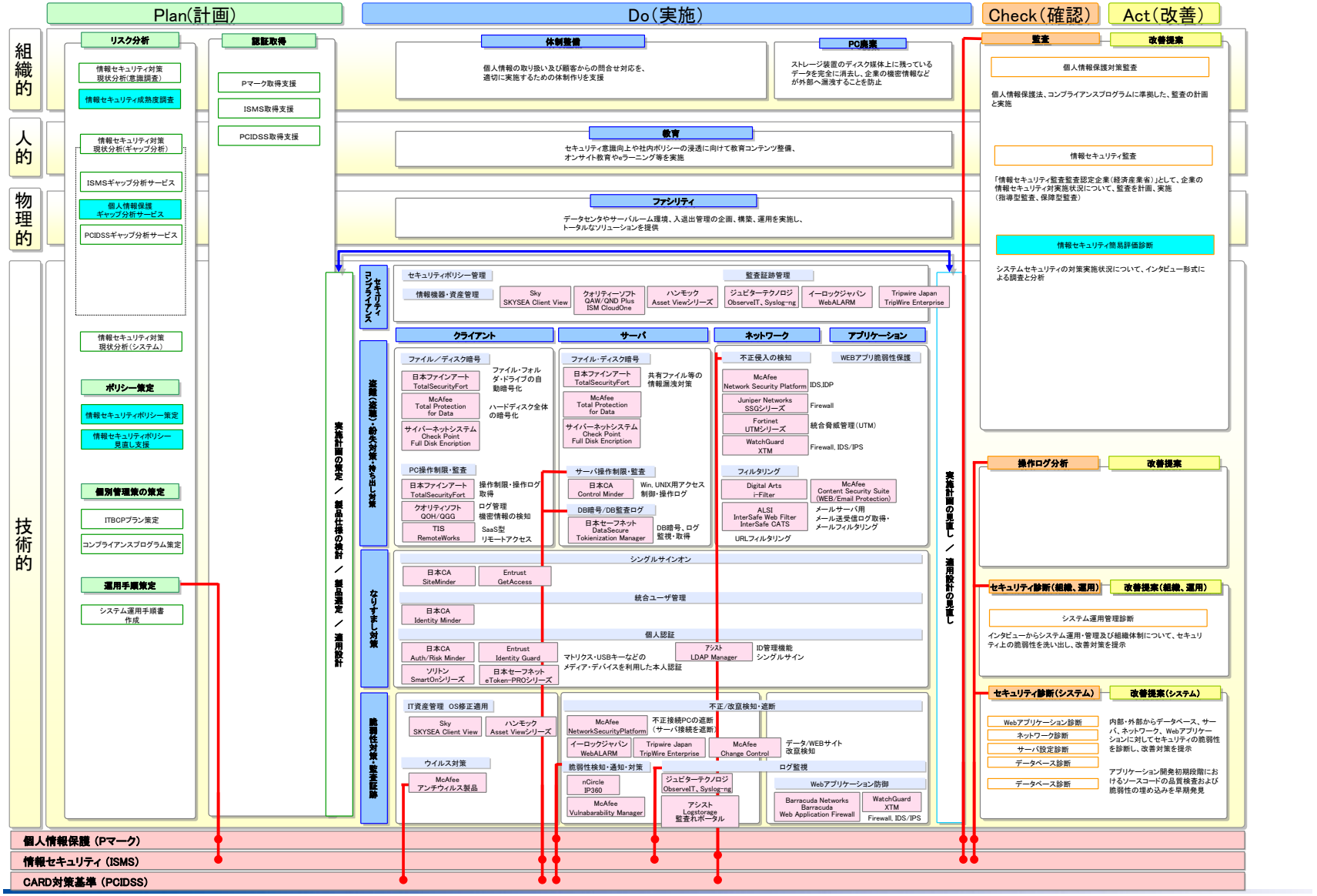
Ⅳ. ツールによる解決策

10. PCI DSS準拠事例



11. PCI DSS要件に対するシステム化ポイント①

TIS
あなたのビジネスに最適を

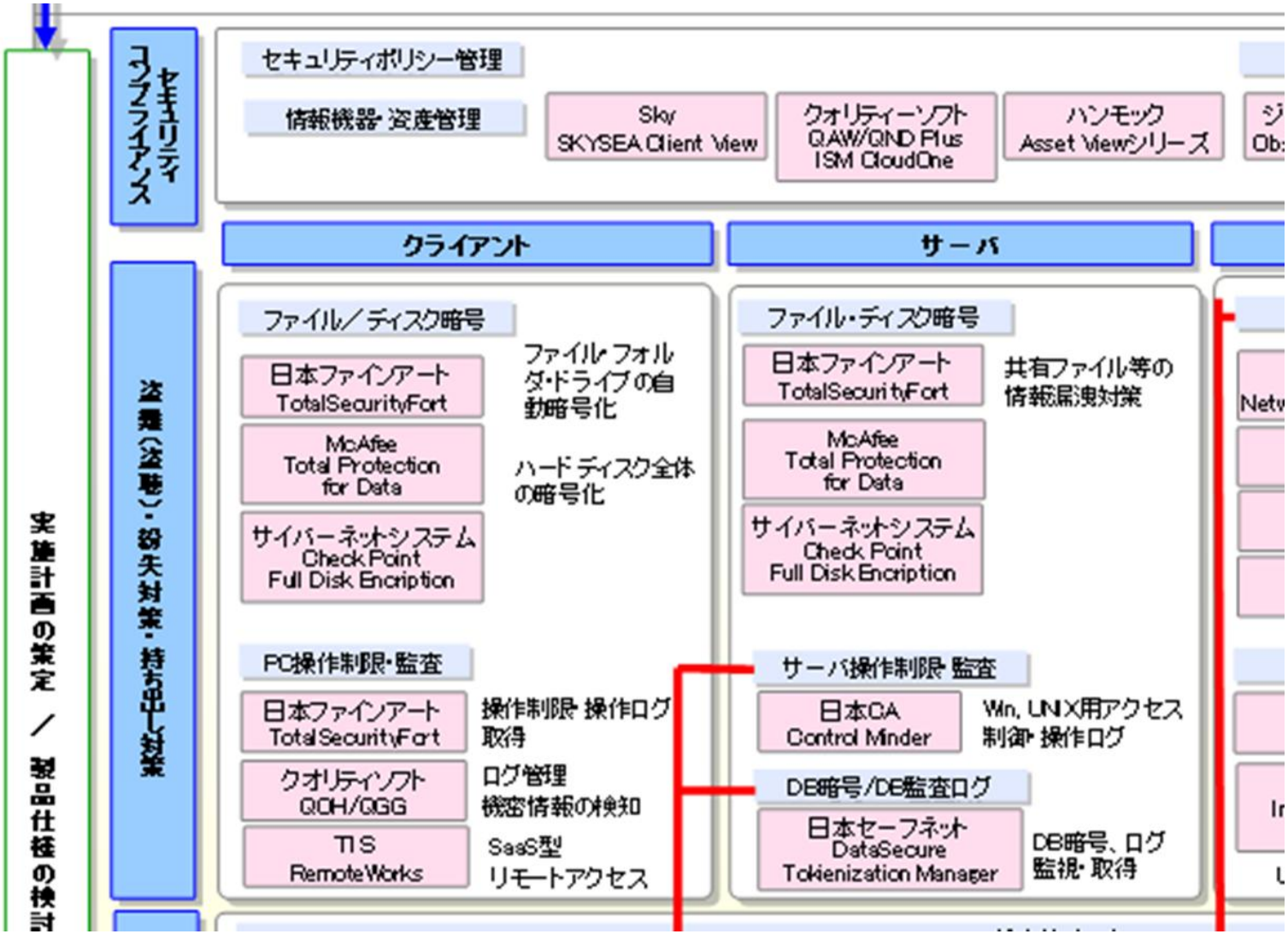


IT Holdings Group

11. PCI DSS要件に対するシステム化ポイント②

TIS
あなたのビジネスに最適を

◆ ソリューションマップ拡大版



12. ツールによる課題解決① 「特権ID管理」

TIS
あなたのビジネスに最適を

◆ 特権IDの管理は、PCI DSSに限らず情報セキュリティ対策の必須項目

【課題】

- 特権IDは、複数人で共有するケースが多い
- サーバとは異なり、通信機器は特権IDの管理ができない
- パスワード変更によるシステム障害リスクが気になる

【解決策】

- 「ID管理＋ログ管理＋ワークフロー」のソリューションを組合せ、特権IDの一元管理を実現する

- ✓ ID登録申請
- ✓ サーバ利用申請

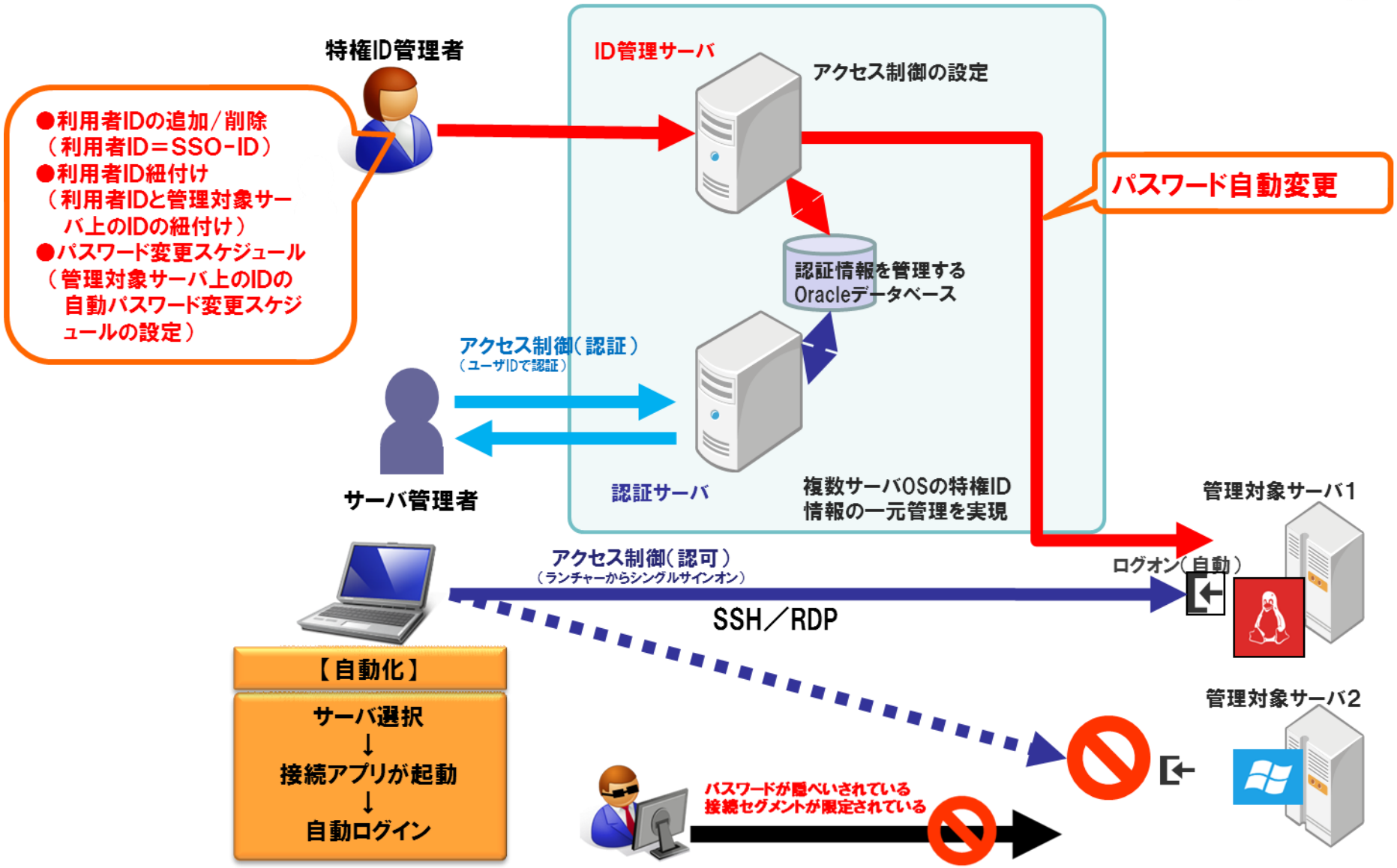
- ✓ ユーザ管理
- ✓ アクセス権管理
- ✓ パスワード変更
- ✓ ID棚卸

- ✓ ユーザへのアクセス権限
- ✓ パスワード隠ぺい

- ✓ ログ統合・保管
- ✓ 利用監査
- ✓ ログの突合せ

iDoperation
＋
OpenCube Workflow
＋
Logstorage

13. ツールによる課題解決① 「特権ID管理」



14. ツールによる課題解決② 「DB暗号化」

日本セーフネット社：DataSecureによる対応事例

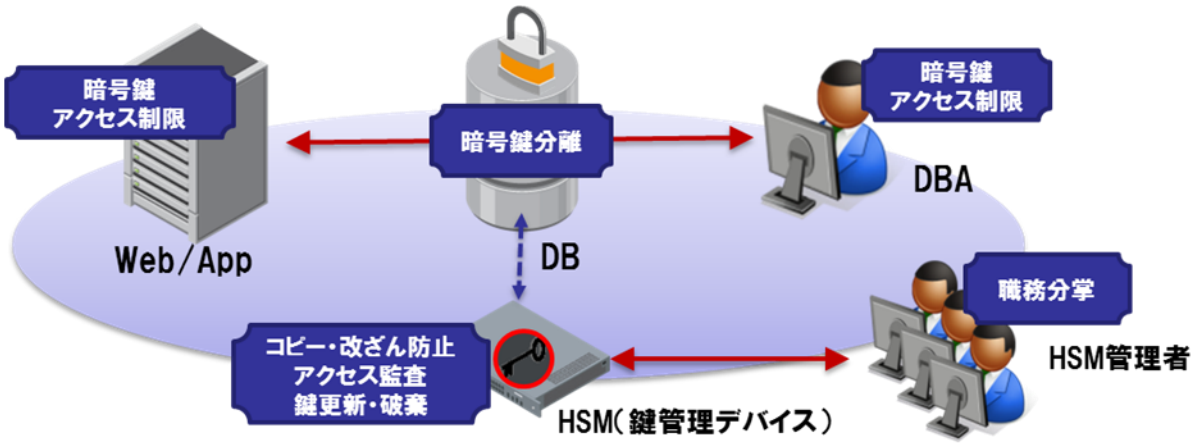
暗号化要求
- ユーザのクレジットカード情報の暗号化
- 業務停止をすることなく暗号化が必要
- 暗号鍵に対する脅威を保護するシステムが必要
- 既存システムに修正を伴わない暗号化

SafeNetによる解決策
- カラム単位での暗号化とマスキング
- サービスクエリを受付けながらオンラインで暗号化
- FIPS140-2 level2認定HSMによる鍵管理と職務分掌による内部統制の提供
- アプリケーションには改修を伴わないスキーム

TABLE		
USER	PAN	DATE
USER1	1234-5678-9123	2013/07/11

暗号化

TABLE		
USER	PAN	DATE
USER1	E#"Q#F0gkj3kf0	2013/07/11

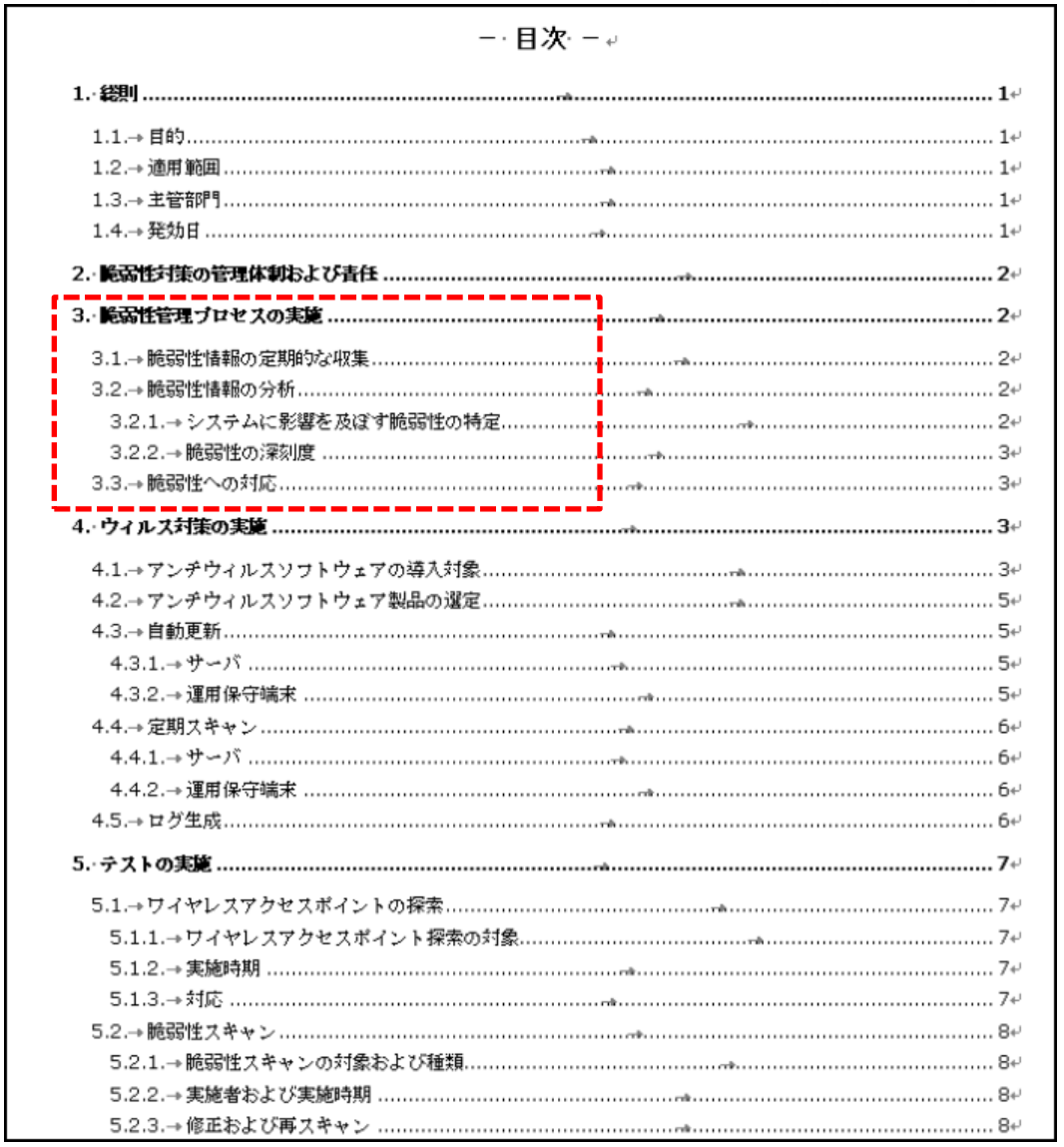


15.「セキュリティパッチ適用の考え方」

TIS
あなたのビジネスに最適を

◆ パッチ適用の運用設計では、
「パッチ適用が出来ない」場合の
フローを考えておくことが重要

・脆弱性情報の収集方法
・脆弱性への対応手順
※パッチ適用不可の理由定義
※パッチ不適用後の運用手順



－ 目次 －

IT Holdings Group

16.「セキュリティパッチ適用の考え方」

◆ パッチ適用の運用設計では、
「パッチ適用が出来ない」場合の
フローを考えておくことが重要

・脆弱性情報の収集方法
・脆弱性への対応手順
※パッチ適用不可の理由定義
※パッチ不適用後の運用手順

脆弱性情報の収集に便利なサイト： http://jvn.jp

- JVN は、“Japan Vulnerability Notes” の略です。
- 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。
- JPCERT コーディネーションセンターと独立行政法人情報処理推進機構（IPA）が共同運営しています。

17.「セキュリティパッチ適用の考え方」

◆ パッチ適用の運用設計では、
「パッチ適用が出来ない」場合の
フローを考えておくことが重要

・脆弱性情報の収集方法
・脆弱性への対応手順
※パッチ適用不可の理由定義
※パッチ不適用後の運用手順

パッチ適用を行なわない場合の管理手順：

（例）
・「3.3.2パッチ適用の優先度」で決定された
期間にパッチ適用ができない理由がある場合は、
以下の管理手順を代替CTLとして使用する。
- 設定変更または、ウイルス対策ソフト、IDSに
よって脆弱性への攻撃が防止できることを確認する。
- パッチ適用までの期間を180日以内とし、
180日毎に脆弱性を再評価する。

＜パッチ適用ができない理由＞
- パッチ適用によりシステムが正常に稼動しない。
- パッチ適用時の影響調査・検証にかかる日数が
90日以上を要する。
- パッチ適用のためのシステム停止による影響の方が
脆弱性が顕在化したときの影響よりも大きい。

本日のまとめ

◆ PCI DSS準拠の検討が前に進まない理由は
準拠対象範囲が決められないからではないですか？

◆ PCI DSS準拠の対応コストが掛かりすぎる原因は
初期ではなく、ランニングのコストではないですか？

◆ PCI DSS要件への**準拠対象範囲を明確**にすることから始めてください。

◆ 運用負荷をこれ以上増やさない**ツールありきの運用**を検討してください。

あなたのビジネスに最適を

●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２営業部
TEL ： 03-5337-4379
中村 敬 E-mail : nakamura.kei@tis.co.jp

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