FUJITSU
shaping tomorrow with you

効果的なPCI DSS準拠に向けて
～サイバー攻撃事例にみるPCI DSS視点からの対策～

2013年7月10日

富士通株式会社
情報セキュリティセンター
センター長　奥原　雅之
PCI DSS QSA

目次

FUJITSU

1. クレジットカードを取巻く環境と最近の攻撃事例
2. 標的型サイバー攻撃対策とPCI DSS要件
3. 効果的なPCI DSS準拠のポイント
4. 富士通の対策ソリューション

FUJITSU

1. クレジットカードを取巻く環境と最近の攻撃事例

- 国内の情報漏えい事故事例
- （事例）ショッピングサイト決済ページ改ざん
- 標的型サイバー攻撃は経営リスク

国内の情報漏えい事故事例

FUJITSU

■ 国内でのクレジットカードの情報漏えい事故の被害例

- 2007年7月　パソコンソフトのインターネットショッピングサイトが外部から不正アクセスを受け、1万3,252人のクレジットカード情報が漏えいし、サイト閉鎖を余儀なくされた。
- 2010年8月　スーパーマーケット７社のクレジットカード会員情報約1万2千件が不正アクセスによりネットスーパー業務を委託する会社から漏えいした。
- 2010年12月　大手百貨店のインターネットショッピング用サーバから不正アクセスにより2,079人分のクレジットカード会員情報などが漏えいした。
- 2012年9月　ネット中古販売を行う企業のサーバが不正アクセスを受け、顧客の情報やクレジットカード情報が最大1万589件漏えいした。

・・・

・クレジットカードの情報漏洩事故は継続的に発生している
・最近は標的型サイバー攻撃の事故が多発

セキュリティニュースサイト：Security NEXTより抜粋(http://www.security-next.com/)

（事例）画面表示のみ

FUJITSU

（事例）画面表示のみ

FUJITSU

標的型サイバー攻撃は企業の経営リスク

FUJITSU

- 技術情報や知的財産が外部へ流出
- システムやデータが破壊され業務がストップ

得られるべき利益が得られなくなる可能性
お客様の信頼を失う可能性
企業の存続にかかわる**経営リスク**です

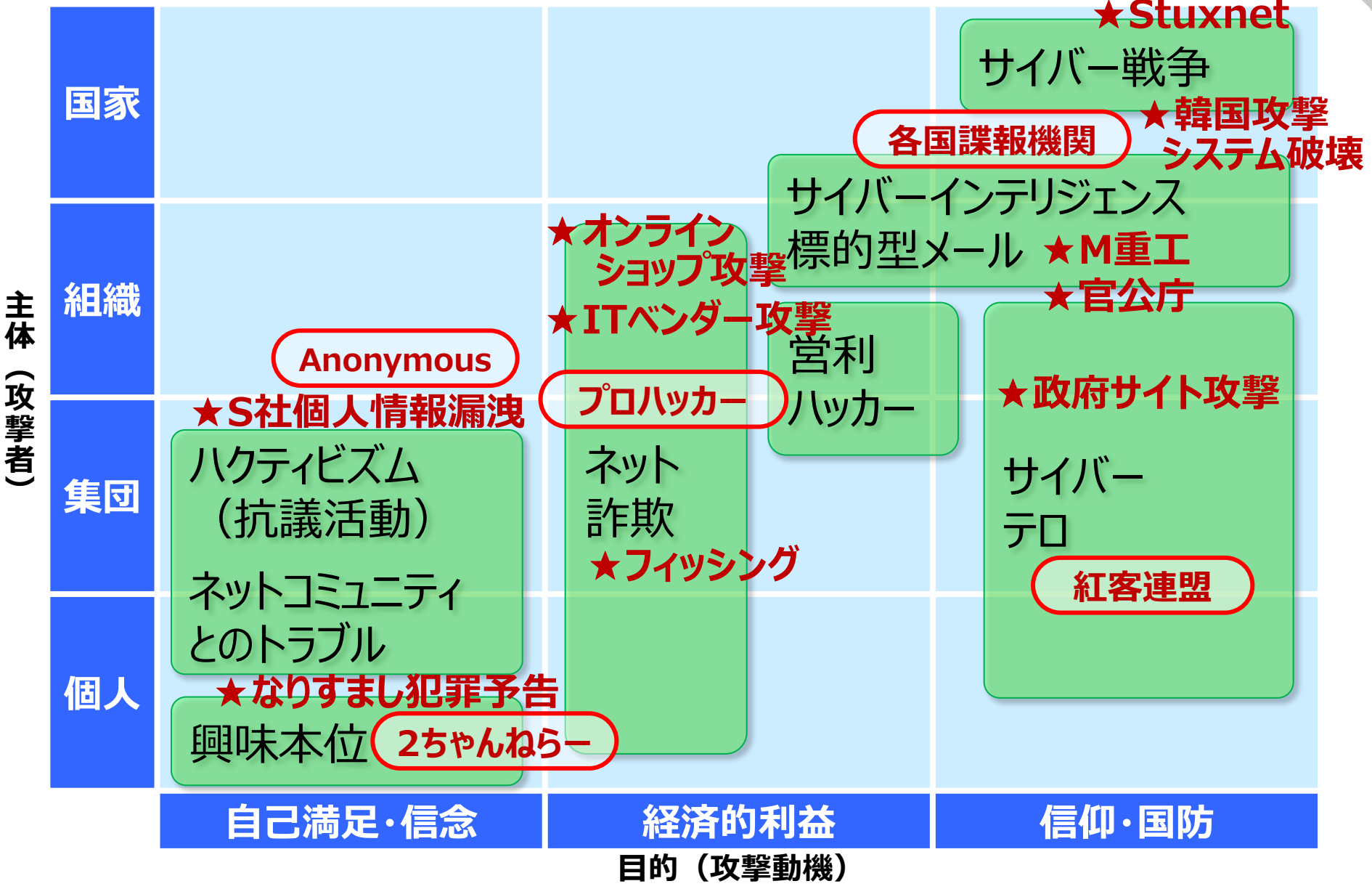
・経営に直結する脅威であり、至急の対策強化が必要

FUJITSU

2. 標的型サイバー攻撃対策とPCI DSS要件

- ハッカーの生態系を知る
- セキュリティ脅威の変化とその対策
- 標的型サイバー攻撃に対する対策は？
- 標的型サイバー攻撃対策とPCI DSS要件の比較
- 標的型サイバー攻撃への対策アプローチ

ハッカーの生態系を知る



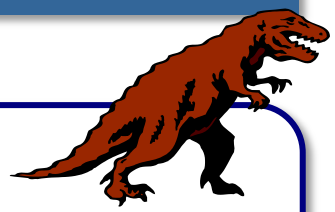
セキュリティ脅威の変化とその対策

FUJITSU

- 標的型サイバー攻撃は攻撃者が明確な目的をもってターゲットを選定し、目的を達成するまで繰り返し高度かつ巧妙な攻撃を仕掛けてくる点がこれまでと異なります。

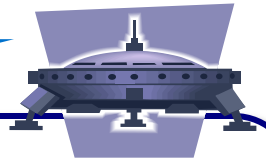
脅　威

これまで



- 怪獣来襲モデル
  - 脅威は一過性
  - 撃退すればハッピーエンド

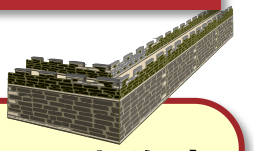
これから



- 悪の秘密結社モデル
  - 狙いを定めて目的達成まで繰り返し襲来
  - 防御側を研究した高度な攻撃

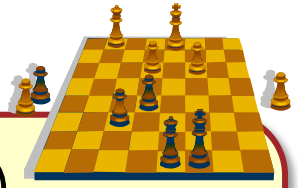
対　策

これまで



- 水際防御（ペリメーター防御）
  - 境界を全力で守る
  - 境界の内側は安全地帯

これから



- 多層防御（総力戦）
  - 複数の対策を組み合わせ多種の脅威に対応する
  - 技術的対策だけに頼らず、組織として対策する

対抗

標的型サイバー攻撃に対する対策は？

FUJITSU

IPA(独立行政法人情報処理推進機構のプレス発表

組織の重要情報の窃取を目的としたサイバー攻撃に関する注意喚起
プレス発表　標的型サイバー攻撃の事例分析と対策レポートを公開
http://www.ipa.go.jp/about/press/20110920.html
http://www.ipa.go.jp/about/press/20120120.html

【対応策】

出典：IPA(独立行政法人情報処理推進機構　プレス発表
http://www.ipa.go.jp/about/press/20110920.html　をもとに再編集

インターネットやウェブサイトを利用している事業者や組織においては、改めて、セキュリティ対策を検証し、
便利でより安全なインターネット社会の確立と維持に向けた継続的な尽力をお願いいたします。
対策の基本的な観点は、以下のとおりです。

【対策1】：入口（ネットワーク経路）を **“しっかり”** 守る
【対策2】：ファイアウォールを抜けてもシステムにつけ入られる **“隙（脆弱性）を与えない”**
【対策3】：ウイルスの活動（組織内蔓延（まんえん）や外部通信）を阻害、抑止する。<出口対策>
【対策4】：重要な情報はその利用を制限（アクセス制御）する
【対策5】：情報にアクセスされても保護するための鍵（暗号）をかける
【対策6】：操作や動き（ログ証跡）を監視・分析し不審な行為を **”早期に”** 発見する
【対策7】：万一被害が発生したら”**”早急な”**対応（ポリシーと体制）をとる

・各対策の具体的な実施レベルまでは示されていない

標的型サイバー攻撃対策とPCI DSS要件比較

No.	項目	対策内容	PCI DSS要件	PCI DSS レベル
1	ネットワークの入口と経路での防御	■ ファイアウォール、侵入検知システム／防止システム ■ 最新のウイルス対策ソフト（ネットワーク、サーバ、クライアント） ■ 通信路の暗号化（Virtual Private Network などの利用） ■ ネットワーク構造／設計（重要なサーバに対するルート制御）	■要件1,11 ■要件5 ■要件4 ■（要件7）	・6か月毎 （FWルールチェック）
2	脆弱性対策	■ OSやサーバソフトウェアの定期的な脆弱性診断 ■ ウェブサイトで使用しているOSやサーバソフトウェアに関する脆弱性情報の時期を逸しない収集とパッチの反映 ■ウェブアプリケーションへの脆弱性の作り込みの回避 ■ ウェブアプリケーションの定期的な脆弱性診断 ■ ウェブアプリケーションファイアウォール（WAF）	■要件11 ■要件6 ■要件6 ■要件6,11 ■要件6	・4半期毎 ・1月（or3）以内 ・OWASP ・年1回 ・防御する
3	ウイルス活動の阻害および抑止（出口対策）	■ 端末間／他部署間の通信制限（ウイルスの組織内蔓延抑止） ■ 組織の端末からの外部通信はプロシキを経由する等の経路制御 ■ ネットワーク量監視（異常を早期検知しウイルス蔓延を早期発見） ■ 知財等のある重要サーバはインターネットから隔離	■要件1、7 ■要件1 ■要件11	・2因子認証 ・設置ポイント ・セグメンテーション
4	アクセス制御	■ ユーザ認証、アクセスするプログラムの特定（ホワイトリスト化）	■要件8	・2因子認証
5	情報の暗号化	■ 暗号／ 暗号鍵管理	■要件3	・業界で評価
6	システム監視、ログ分析	■ ネットワークログ取得・分析／サーバログ取得・分析／アクセスログ監査	■要件10	・毎日確認
7	管理統制及びコンティンジェンシープラン	■ セキュリティポリシー、危機対応体制の整備 ■ 海外を含むグループ会社間でのセキュリティガバナンス	■要件12	・毎年テスト ・毎年確認

- PCI DSS要件はサイバー攻撃対策をほぼ網羅。
- 実施レベルも規定

出典：IPA (独立行政法人情報処理推進機構　プレス発表　別紙チェックリスト

標的型サイバー攻撃への対策アプローチ

どれほど“しっかり”した対策を
どれまで“早期に”実施すれば“隙を与えない”
ようにできるのか？ 具体的な対策実施レベルは…

⇒対策レベルは**PCI DSS基準**を利用して、
まずは、出来る対策から行う。

※PCI DSS準拠認定に向けての手戻りも防止可能

- PCI DSSを基準として標的型サイバー攻撃への対策を始める
- 今後の準拠認定を視野に入れる

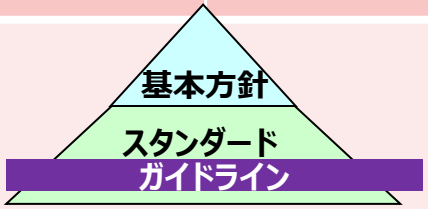
FUJITSU

3. 効果的なPCI DSS準拠のポイント

- Point1. 現状を知り全体最適な対策強化計画を策定する
- Point2. PCI DSSの意図を正確に汲み取る

Point1.
現状を知り全体最適な対策強化計画を策定する

- ムリ、ムダ、ムラを無くすため、対策強化対象のシステム単独で考えるのではなく、他システムの対策や他マネジメント運用を含めて考える。

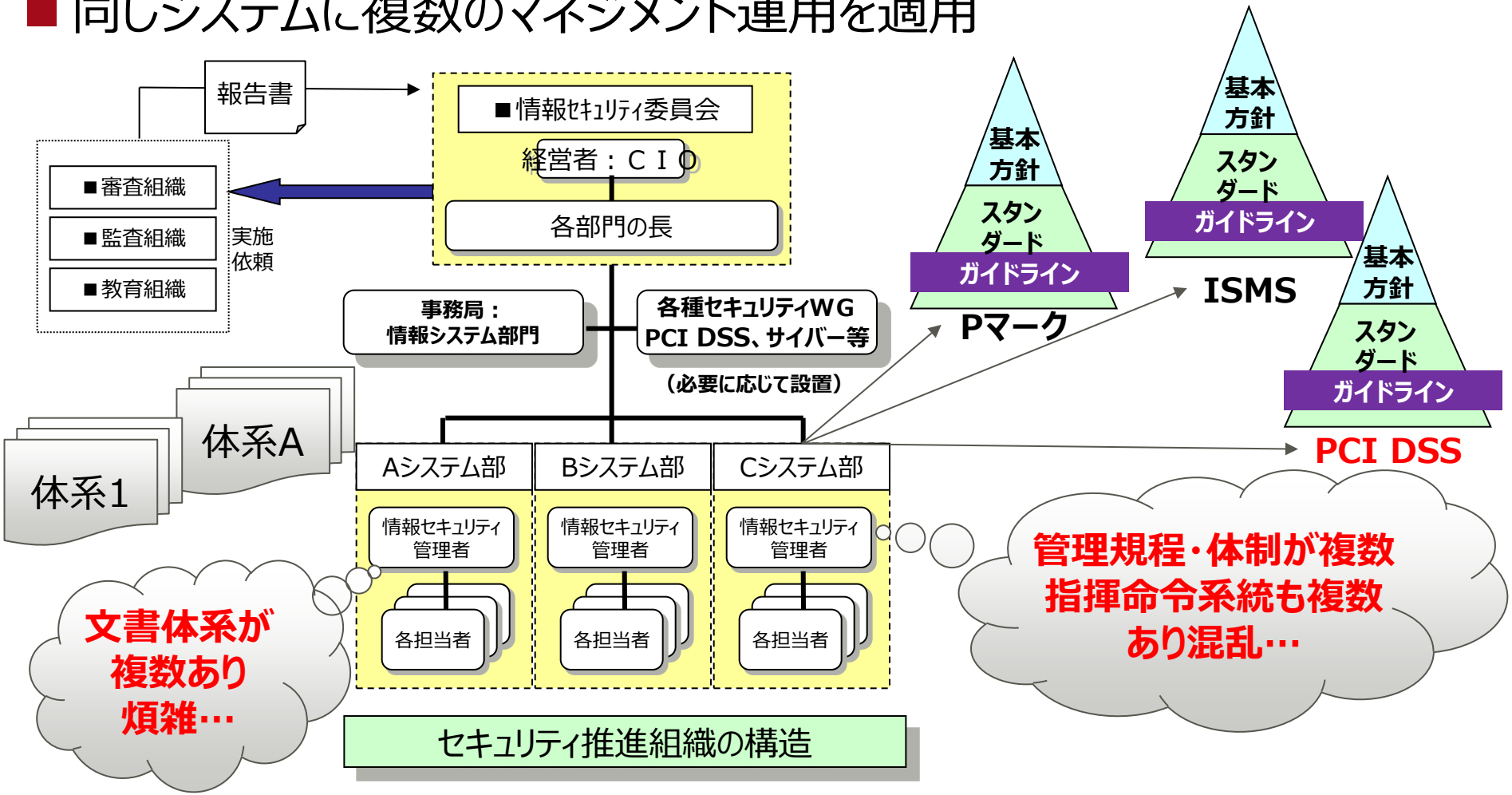
検討項目	システムA	システムB
・ポリシーの統合 ・管理体制の統一化 ・文書のスリム化		
・対策の共通化 ・ツールの共通化 ・共同利用(NW,FW等)	スキャンツール ログ管理ツール 暗号化ソフト 改ざん検知ツール ・・・	
・運用方法の統一化 ・手順の共通化	脆弱性対処検討 鍵管理運用検討 ログ運用検討 アラート対応検討 ・・・	

・基準や対策は横串で考えることで効率化／企業統制する

Point1.

問題事例１

■ 同じシステムに複数のマネジメント運用を適用

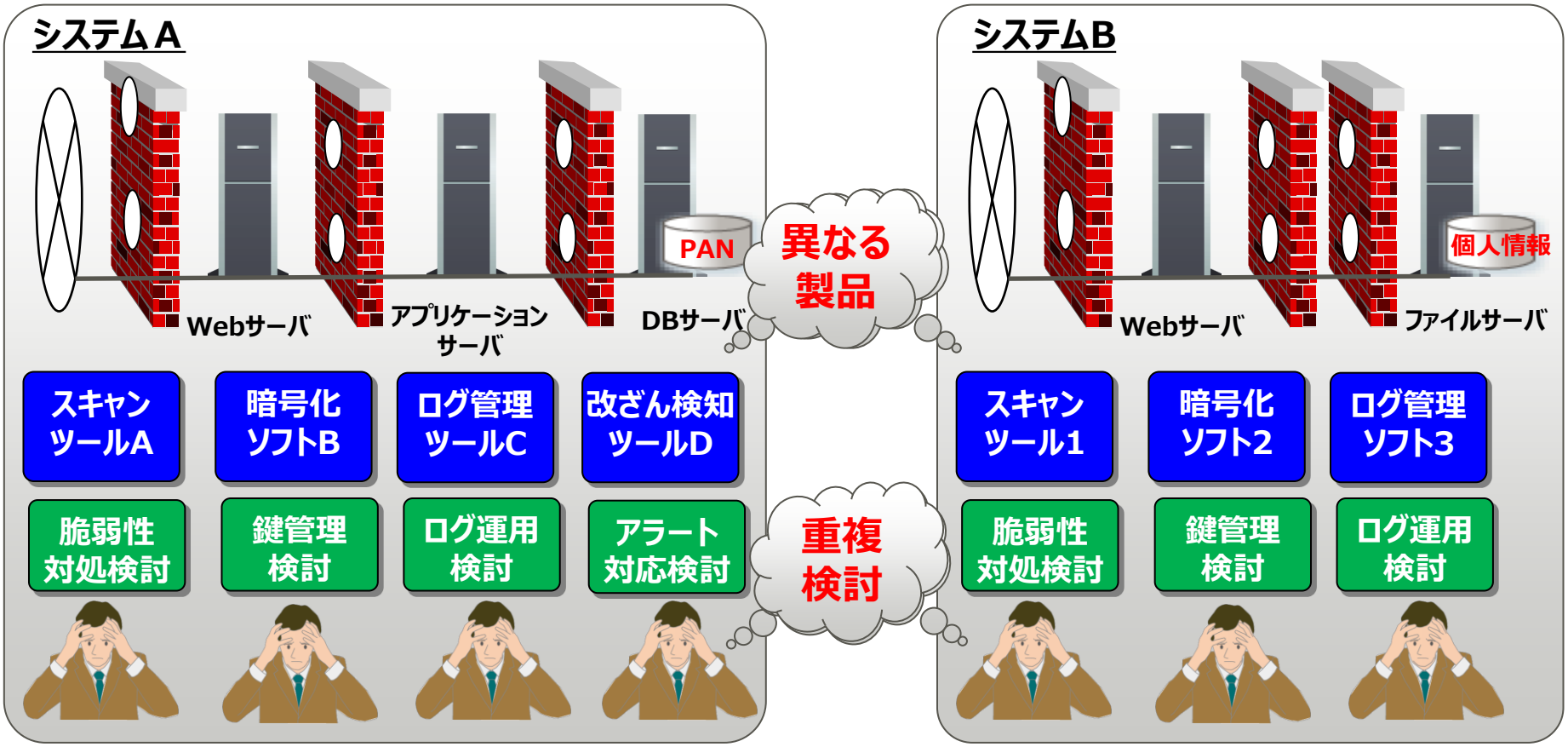


・複数のマネジメントシステムを独立して運用
⇒組織が成熟せず、効果が出ない。

Point1.

問題事例２

■ 各システム毎に同様の対策を個別に適用している。



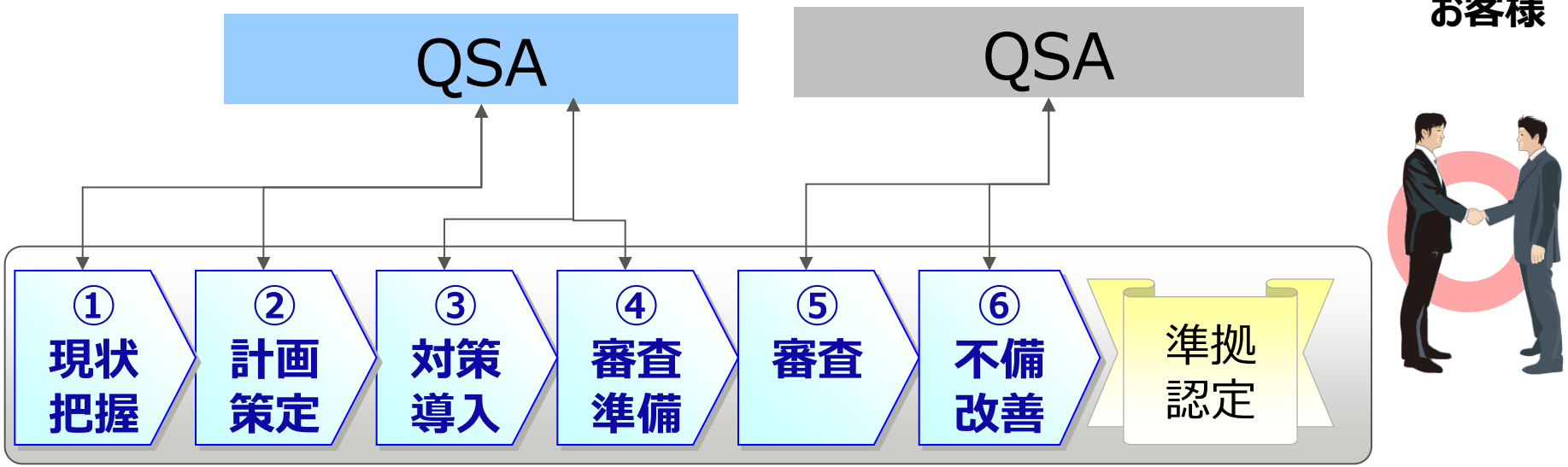
・対策技術や対策運用を共通化／共用化できない
⇒2重投資、2重検討によりコストがかかる

Point2.
PCI DSS要件の意図を正確に汲み取る

FUJITSU

- PCI DSSは具体的と言われるが、妥当性の判断をQSAに委ねられている部分が多い。

早い段階でQSA見解を入れる ・・・・・▶ **手戻りとなる不備改善はなし**



- **早い段階でQSAと連携し、設計/構築/運用までスムーズに進捗させる。**

Point2.

SEの手戻り事例１

FUJITSU

■ 対策立案時、設計時、構築時は、その妥当性の判断に苦慮する。

【 SEからの相談事例】

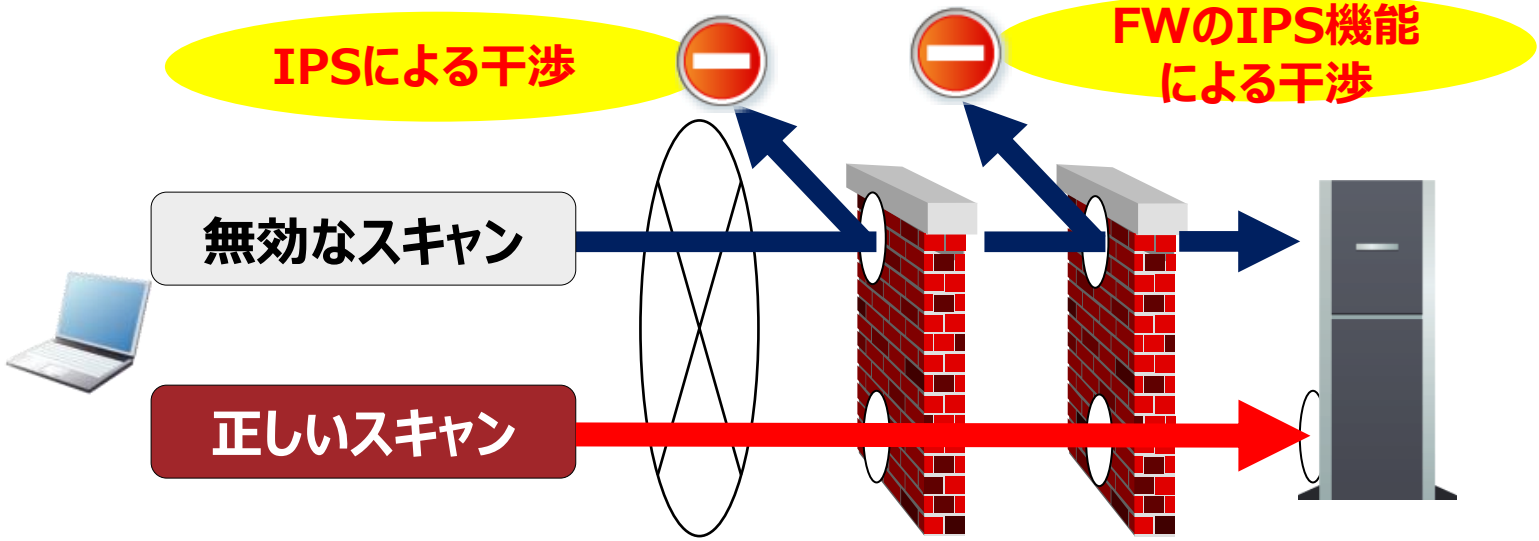
- 手戻り例1）
  専用ツールである vCenter Configuration Managerの導入が不可能であり、VmwareのESXiのファイル整合性監視ができない。他の方法として、アクセス制御機能を利用して、想定で設計構築を進めていた。
  後の予備審査の段階で、その選択は代替コントロールであることが分かったので、リスクを再評価し、追加の管理策を検討し、サーバの設定変更が発生した。
- 手戻り例2）
  サーバ更改時に、ファイル整合性監視ツールをTripwireからTrendMicro Deep Security ™へ変更した。
  しかし、製品仕様が異なるため、運用方法を変更しなければならず、予備審査の段階で運用設計の変更が発生した。

・独自解釈での対策を進めると、実際の審査でＮＧ判定となり、手戻り発生で工数拡大／スケジュール延伸が発生する。

Point2.

SEからの手戻り事例２

- 対策立案時、設計時、構築時は、その妥当性の判断に苦慮する。
  - 手戻り例1）
    IDSを有効にしてASVのスキャンを実施していたので、本来見つからなければならない脆弱性が見つけられなかった。　審査準備時に、IDSを無効に再スキャンを行い、脆弱性の対処を再度しなければならなくなった。また、対象となるべきルータとＦＷもスキャンしていなかった。



・QSAのみならず、ASVによる要件も決められており、正確なスキャン実施の把握が求められている。

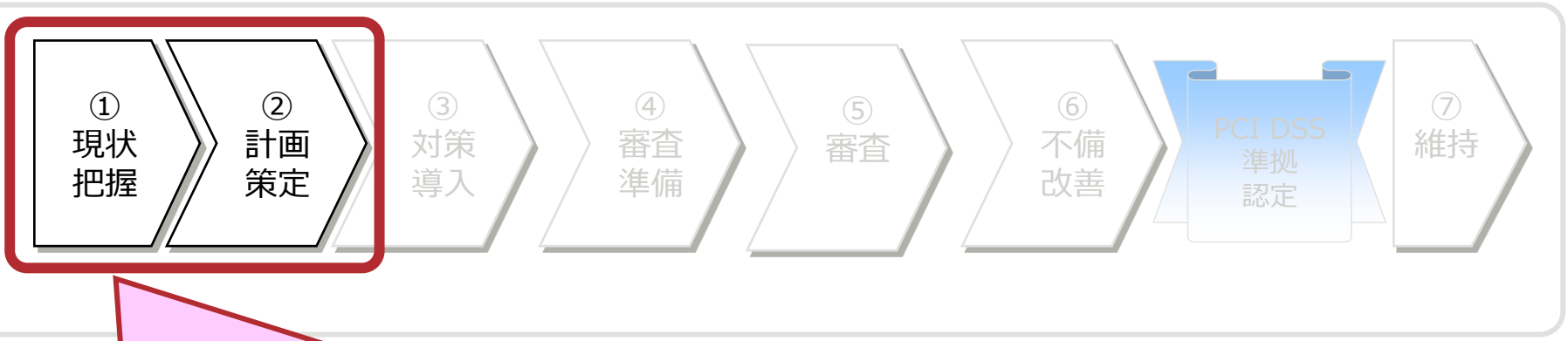
FUJITSU

4. 富士通の対策ソリューション

- 多角的かつ包括的なご支援
- QSA／ASV認定企業としての正確なご支援
- 対策ソリューション

多角的かつ包括的なご支援

FUJITSU



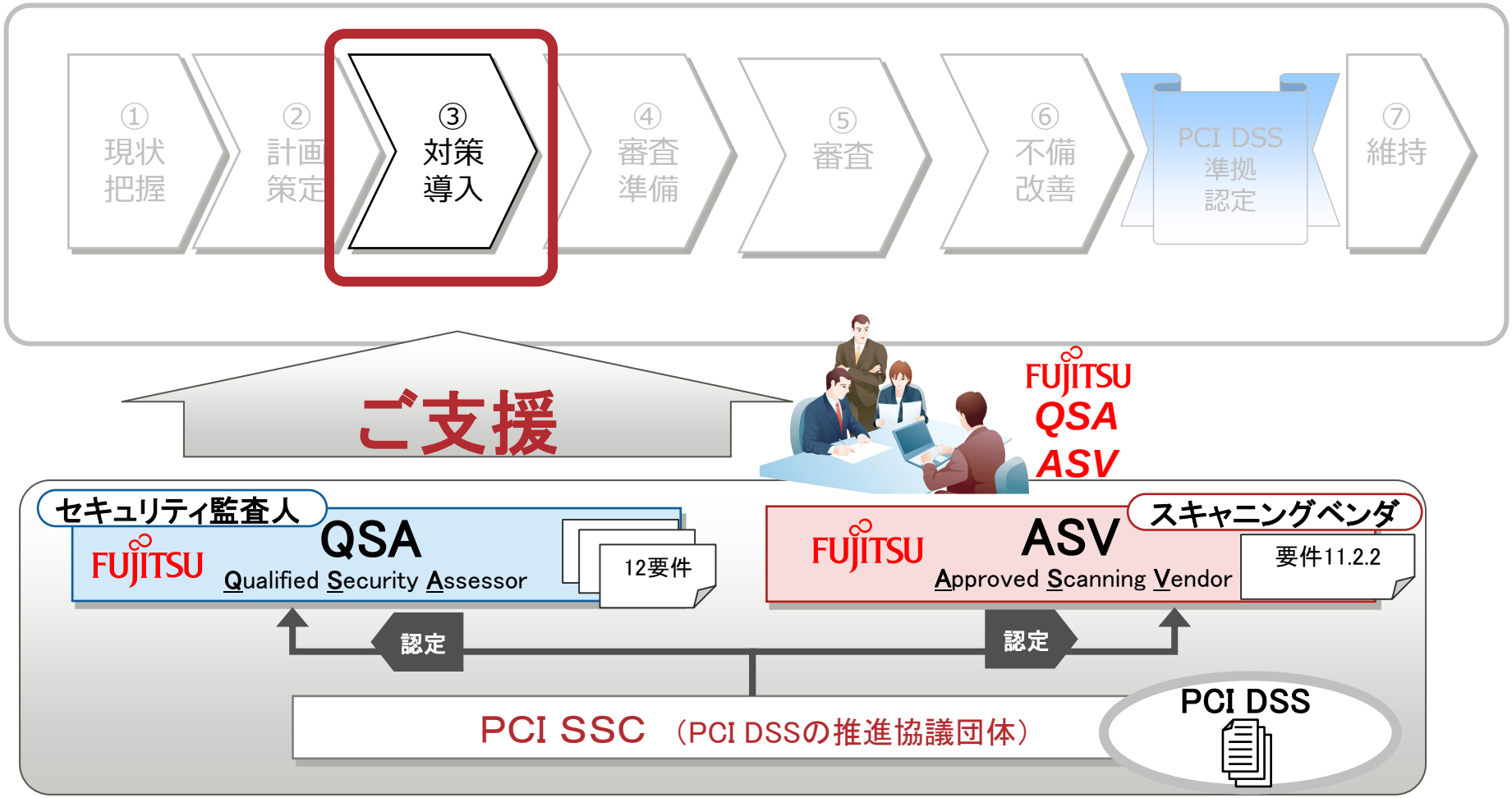
多角的な視点で、全体最適な
対策強化計画を策定します。
（情報セキュリティ強化支援コンサルティング）

- 民間企業、省庁及び地方自治体の情報セキュリティポリシーの作成及び適用支援、ISO27001認証取得支援、情報セキュリティ監査等、多くの情報セキュリティサービスを実施しております。
- これらの支援実績で得られたノウハウを活用し、ASV/QSA企業として効率的で効果的な支援を実現します。

QSA／ASV認定企業としての正確なご支援

FUJITSU

- 当社はQSA/ASVの認定企業であり、対策導入時にSIベンダ視点でご支援します。



・QSA,ASV,SIerとして、富士通グループで対策支援を致します

対策ソリューション①

要件	製品/サービス名	概要
要件1 (一部6)	ネットワークサーバ IPCOM EX SCシリーズ	IPCOM EX SCシリーズは、ファイアーウォール機能を搭載するネットワークサーバです。ファイアーウォール機能に加え、IDP機能、Ipsec-VPN機能を搭載し、強固なセキュリティを実現します。
	Check Pointアプライアンス	Check Pointのアプライアンスは、高いセキュリティレベルとパフォーマンスが必要とされる環境で、長年に渡る利用実績があるアプライアンス・ソリューションです。ファイアーウォール、VPN、侵入防御(IPS)、アプリケーションレベルのアクセス制御、URLフィルタリング、アンチウイルス、アンチボットなど、あらゆる環境で必要なレベルのセキュリティを実現可能です。
	Barracuda Web ApplicationFirewall Vx(仮想アプライアンス版)	Barracuda Web Application Firewall Vx版 は、Webアプリケーションを攻撃から防御する、仮想アプライアンス製品です。
	Check Point Software Blade	Check Point Software Bladeは、個々に独立し、集中管理に対応したモジュール型の論理セキュリティ・ビルディング・ブロックを意味し、組織固有のビジネス・ニーズに基づいて、適切なソリューションを素早く構成することができます。また、新たなニーズが発生した場合でも、既存の構成に新たなブレードを追加することで、同一のハードウェア・プラットフォーム上で素早くセキュリティを拡張することができます。
要件2	CA IdentityMinder(TM)	CA IdentityMinderは複数のICTシステム上に存在するID情報の管理を統合する商品です。
	LDAPManager	LDAPManagerは、LDAPサーバを中心としたユーザー情報統合管理システムを構築するためのメタディレクトリソフトウェアです。
	PMaid IDMaster	PMaid IDMasterは日本の企業文化に合った統合ＩＤ管理の機能を持つ製品です。
	Sun Java System Directory Server	インターネット標準であるLDAP(Lightweight Directory Access Protocol)V3準拠のディレクトリサーバです。大規模ネットワーク構成におけるネットワーク内の利用者や資源を一括管理することができます。
	BRidgeWARE	BRidgeWAREは、人事システムからの連携によってActiveDirectoryへアカウントの自動作成/削除を行う製品です。また、人事システムの情報を基にETERNUS NR1000FやWindows Serverのフォルダの自動作成/削除や、フォルダに対するアクセス権の自動設定をする製品です。

対策ソリューション②

要件	製品/サービス名	概要
要件3	マルチプラットフォーム暗号化ツールCOMPLOCKII	ＣＯＭＰＬＯＣＫ（コンプロック）は、メインフレームからPCに至るまで個人情報などの大切なデータを圧縮・暗号化するマルチプラットフォームで動作するツールで、電子政府推奨暗号の一つであるＡＥＳに対応しています。
	BSAFE	RSA BSAFEは、eビジネス・アプリケーション、企業内アプリケーション、携帯電話、PocketPC、PDA、Webブラウザー、複合型ネットワーク機器、デジタル複合機など、高い安全性を求められるソフトウェアやハードウェア開発用SDKです。
要件4	IPアクセスルータ Si-R	「GeoStream Si-Rシリーズ」は、高品質なIP-VPNサービスや、コストパフォーマンスの高いブロードバンドサービスを最大限に活用していただくためのIPアクセスルータ。高度なVPN機能やQoS機能、IPv6サポート機能など、次世代の企業ネットワークシステムを構築するための最適なソリューションをご提供します。
	Juniper Secure Access	Juniper Secure Accessは、お客様のネットワーク構成(ADSL・無線LAN・ホットスポットなど)に手を加えることなく通信を暗号化するセキュリティソリューションです。全ての通信はSSLにより暗号化されますので、クライアントPCに専用ソフトウェアをインストールすることなく簡単に安全なネットワーク環境を実現します。
	FENCE-Mail For Gateway	FENCE-Mail For Gatewayは、監査機能と暗号化機能の二重の対策により、メール誤送信からの情報漏えいを防止する対策を提供します。送信ルールに合致したメールは一時保留され、送信者や上長が再確認することで誤送信を防止します。さらに受信先の環境に適した形式でメールを自動的に暗号化することで安全にメールを送信できます。
	FENCE メール誤送信対策サービス	FENCE メール誤送信対策サービスは、大規模事業者に多くの実績があるオンプレミス型「FENCE-Mail For Gateway」の豊富な誤送信防止機能をそのままに、小規模からでも手軽に利用できるようSaaS型アプリケーションサービスです。
要件5	Server Protection for Windows	ファイルサーバ、WEBサーバ上のファイルへのウイルス感染の防止や、ウイルス疑惑活動の監視、さらにファイル感染したウイルス名称の特定など、さまざまなウイルス対策処理を行います。1つの管理サーバから複数の被管理サーバの設定が可能です。

対策ソリューション③

要件	製品/サービス名	概要
要件5	ServerProtect for Linux	企業内情報を共有するためのファイルサーバを、リアルタイム検索によりウィルスを自動検出し、社内システムへの感染を防止します。パターンファイルの自動アップデートにより、セキュリティ維持やTCO削減を実現できます。
	ServerProtect for NetApp	NR1000専用のウイルス対策製品です。NR1000F Series及びNR1000R Series上にあるファイルを効率的に検索して、ウイルスの検出および駆除を行います。
	Symantec Endpoint Protection	Symantec Endpoint Protectionは、ウイルスや未知のセキュリティ脅威からサーバやクライアントPCを守るために、先進のセキュリティ対策機能を掲載した法人向けエンドポイントセキュリティソフトです。
	ウイルスバスターコーポレートエディション Plus	ウイルスバスターコーポレートエディション Plusは、クライアントやサーバ、スマートフォンのウイルス対策、ファイアウォールや感染時の自動復旧、Webレピュテーションなど総合的なセキュリティ機能をオールインワンで利用できるウイルス対策製品です。
	Trend Micro Control Manager(TMCM)	ネットワーク上にインストールされているトレンドマイクロ株式会社のウイルス対策ソフトの設定、更新、監視などを集中管理します。企業のネットワーク全体にウイルス対策戦略を効果的に展開させることができます。
	IPCOMセキュリティサポートサービス	IPCOMセキュリティサポートサービスは、ネットワークサーバIPCOM EXシリーズのアンチウイルス機能、Webコンテンツ・フィルタリング機能、シグネチャー型IPS機能を実現するサービスです。常に最新のウイルス定義ファイルや不正アクセスシグネチャーファイルなどの該当セキュリティ環境を、最新の状態に維持することができます。
要件6	iNetSec Inspection Center	iNetSec Inspection Center は不正利用者や危険なパソコンやスマートデバイス（Android／iOS）をネットワークから排除するために必要なポリシーを定義するための検疫ポリシーサーバです。
	Systemwalker Patrol	Systemwalker Desktop Patrol(システムウォーカー/デスクトップパトロール)は、パソコンのセキュリティ管理と資産管理を容易に実現するデスクトップ管理製品です
	Webアプリケーションセキュリティ診断サービス	世界的に評価の高い診断ツールと富士通独自ノウハウで、インフラ・OS・ミドルウェアを診断するサーバスキャンでは対応していない、お客様固有開発のWebアプリケーションの脆弱性を診断・評価・分析し、その危険性と具体的な対策方針をご提示します。

対策ソリューション④

要件	製品/サービス名	概要
要件7	SHieldWARE	SHieldWARE(シールドウェア)は、お客様のサーバにある大切な情報をOSレベルで守るセキュアＯＳ製品です。 あらゆるユーザやプロセスに対して厳格なアクセス制御を行うことが可能です。また、OSへのアクセスログを詳細に記録することにより情報漏えいを抑止し、事後の監査に利用することもできます。
要件8	手のひら静脈認証 PalmSecure	「PalmSecureセンサー」は手のひら静脈を読み取る装置です。PCログインシステムなど様々なアプリケーションと連携することによりシステムに高度なセキュリティを提供します。また、ソフトウェア開発キット「PalmSecureSDK」により、既存のアプリケーション・ソリューションに手のひら静脈認証機能を組み込むことが可能です。
	SMARTACCESS/Premium	Windowsログオン/アプリケーションログオン認証を、各種PCセキュリティデバイスで実現。複数デバイスの組み合わせ利用により、幅広い運用と強固なセキュリティを提供します。
要件9	FutureyeII	リアルタイム映像伝送装置 IPシリーズを統合し、大規模な映像の収集・蓄積・配信を実現します。
	入退室管理システム SGシリーズ	入退室管理システム「ＳＧシリーズ」は、セキュリティポリシー、利用シーンに応じたセキュリティレベル分けを可能にするフィジカルセキュリティシステムです。
要件10	Systemwalker Centric Manager	システム運用のライフサイクル(導入/設定～監視～復旧～評価)に従い、ソフトウェア資源の配付、システムやネットワークの集中監視、リモートコントロールなどにより、運用管理作業の軽減と、信頼性の高いシステム構築を実現する統合運用管理製品です。
	BlueCoatシリーズ	BlueCoat(ブルーコート)はセキュア・プロキシ・アプライアンス製品です。
	Chakra	「Chakra」は、データベースへのアクセスをロギングするネットワークキャプチャ型の製品です。データベースへ「誰が、何時、何処で、何を使用して、何を実行したか」を記録します。また、不正なアクセスを定義して、アラートを検知する事も可能です。
	データベースセキュリティ強化 (PISO)	「PISO」は、内部統制対策や個人情報保護対策として、(1)何時、(2)誰が（ユーザID）、(3)何処から（IPアドレス）、(4)どのような操作を行って（実行SQL文）、(5)何件抜き出したかの4W2Hの記録をメモリから直接参照し負荷なく記録できます。また、記録したログに対して警告を発したり、万が一の際のログ追跡機能なども標準で提供しています。

対策ソリューション⑤

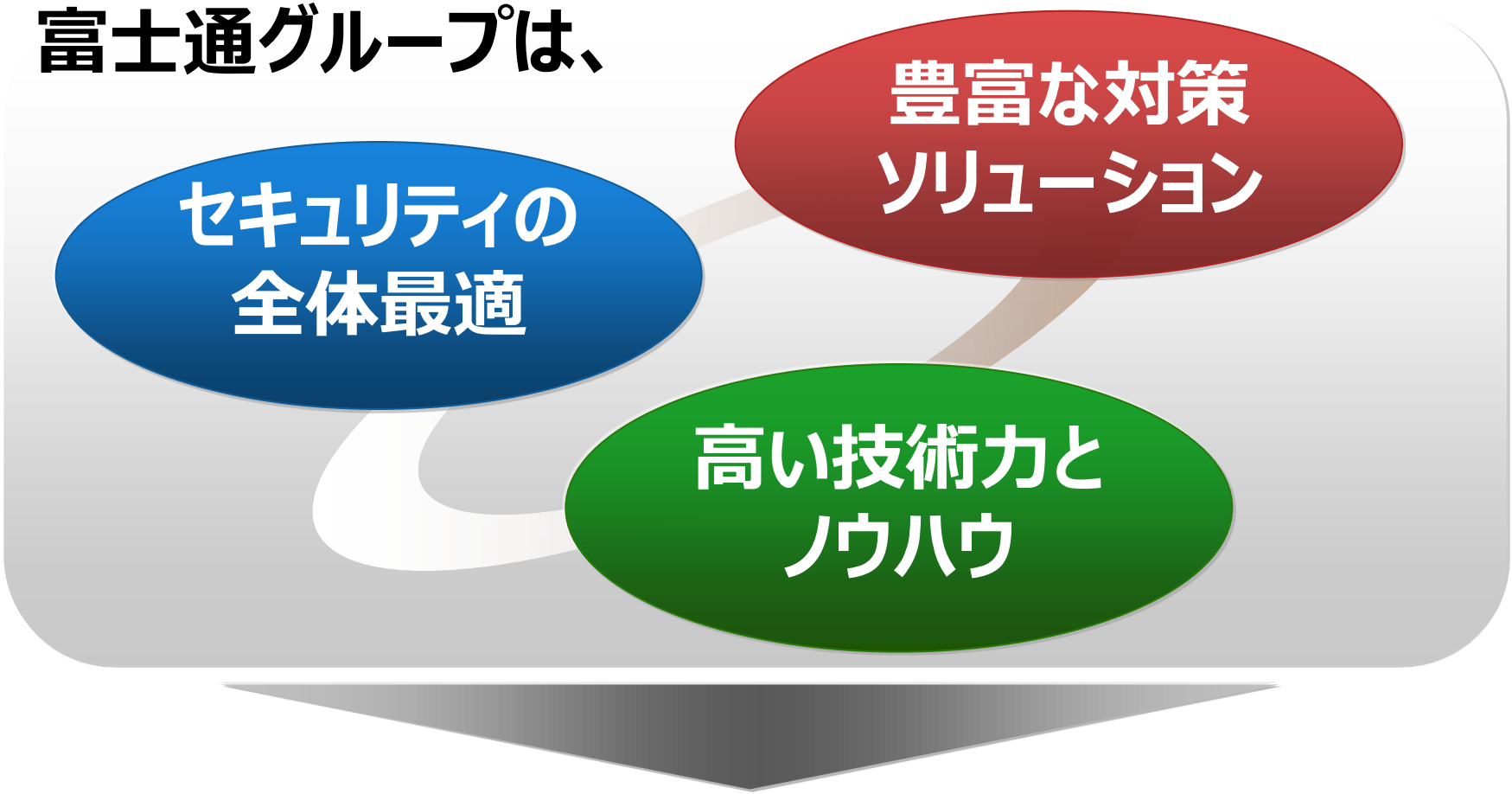
要件	製品/サービス名	概要
要件10	SHieldWARE NE	操作履歴のレコーディングやデバイスのアクセス制御、IDの一時払い出しなど多彩な機能により、セキュアなリモート・アクセスを実現します。
要件11	PCI DSS ASV認定スキャンサービス	PCI DSS ASV認定サービスは、PCI DSS要件11.2.2で規定されるASVによる外部ネットワークの脆弱性スキャンを実施、認定に向けたテクニカルサポートも行います。 当社は、PCI SSCよりASVとしての認定を受け、本セキュリティ基準を満たすサービスを提供いたします。
	IPCOMセキュリティ運用サービス スタンダード	IPCOMセキュリティ運用サービス スタンダードはUTM機器であるIPCOM EXシリーズにおいて稼働／性能状況やファイアーウォール、IPS等のリアルタイムインシデント検知・通報、ログレポート提供等、お客様にとって必要な運用作業を代行するサービスです。
	Proventia シリーズ	Proventia(R)(プロベンティア)アプライアンスシリーズは、IBM ISSの不正侵入防御テクノロジーとノウハウ、ナレッジを結集して開発されたセキュリティアプライアンス製品です。
要件12	情報セキュリティ方針立案コンサルティング	セキュリティに関する各種国際標準および当社のノウハウを基に、全社的な情報セキュリティ方針を立案します。
	統合マネジメント支援サービス（IMS-S）	組織の認証規格（ＩＳＭＳ等）遵守のための組織的なマネジメント活動を支援するSaaS型アプリケーションサービスです。各種機能・コンテンツを活用することで、容易な統合マネジメントシステムの運用を実現可能にします。

富士通グループ ソリューションご紹介・お問合せサイト
http://jp.fujitsu.com/solutions/safety/secure/solution/sol27.html

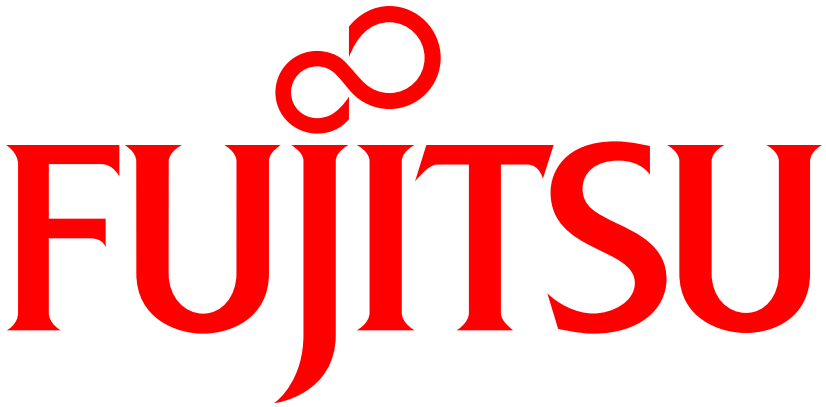
最後に

FUJITSU

富士通グループは、



PCI DSS／標的型サイバー攻撃対策は、
是非、富士通にご相談ください。



shaping tomorrow with you