NTT DATA
Trusted Global Innovator

PCI DSSの維持ポイントのご紹介！

２０１８年６月２２日
ＮＴＴデータ先端技術株式会社

はじめに

PCI DSSは準拠を維持するのが難しいセキュリティ基準とよく言われます。

PCI DSSの現場ではどんな問題が起きていて、どう対処すべきなのか事例を交えて解説します。

また暗号化、改ざん検知、脆弱性スキャン等、準拠維持をサポートするソリューションをご紹介します。

NTTデータ先端技術株式会社

社　名　エヌ・ティ・ティ・データ先端技術株式会社
（NTT DATA INTELLILINK CORPORATION）
代表者　　代表取締役社長　青木　弘之
設　立　　平成11年8月3日
株　主　　株式会社エヌ・ティ・ティ・データ（100%）
連結社員数 1123名（平成30年4月1日現在）

事業内容【セキュリティ事業部】
1）情報セキュリティに関するトータルソリューションの提供
2）企業情報システムのセキュリティコンサルティング
　サービスの提供
3）セキュリティ診断・不正アクセス監視・セキュアSI等の
　サービス提供
4）セキュリティ教育に関する各種サービスの提供

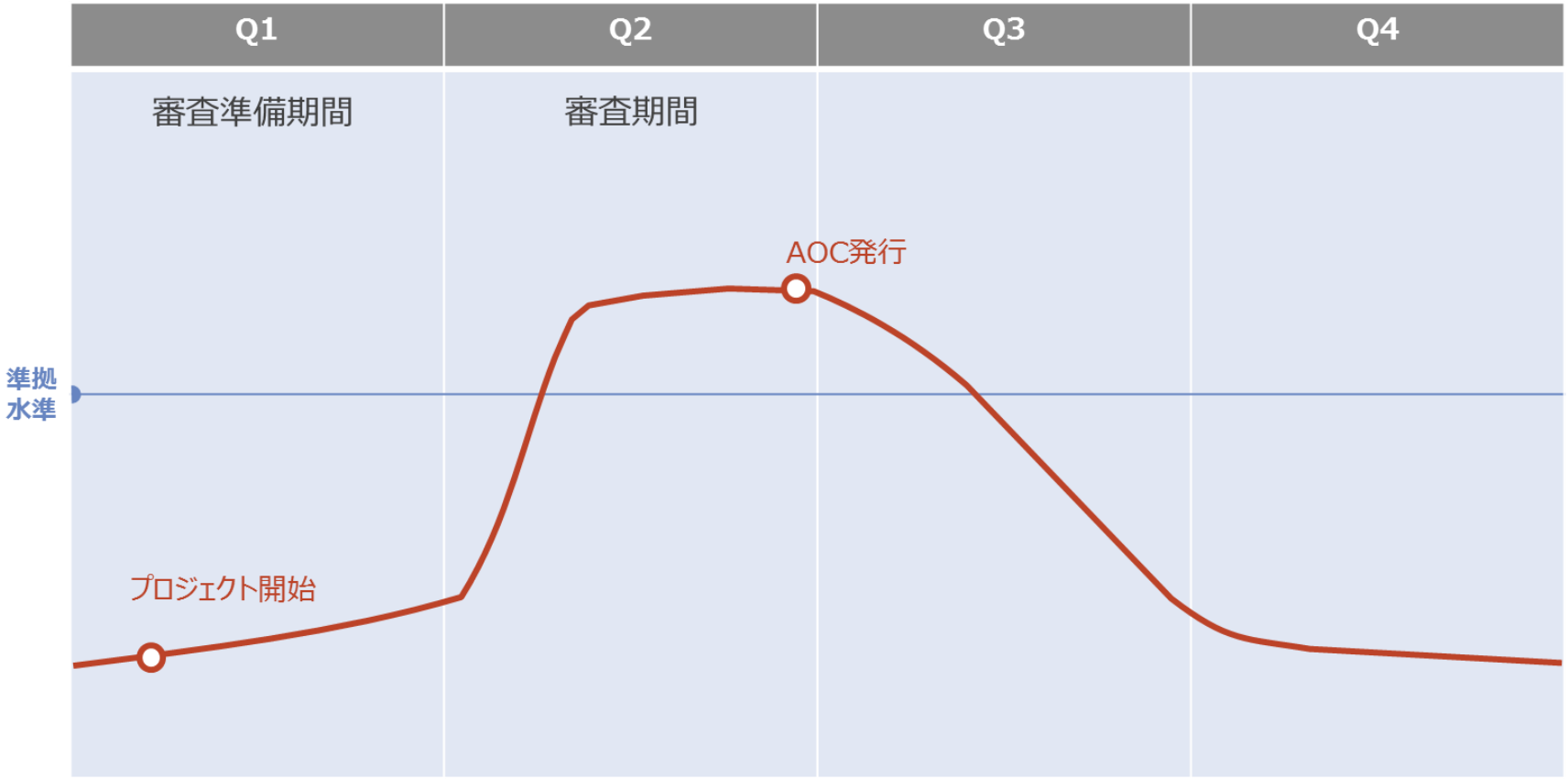
保有資格
1）QSA（PCI DSS認定セキュリティ評価機関）
2）PA-QSA （PA-DSS認定セキュリティ評価機関）
3）QSA(P2PE) （P2PE認定セキュリティ評価機関）
4）PA-QSA(P2PE) （P2PEアプリケーション認定セキュリティ評価機関）
5）3DS Assessor （3DS評価機関）
6）ASV （脆弱性スキャニングベンダー）

PCI DSS準拠維持における課題

PCI DSS準拠は維持・強化に努めることが必要

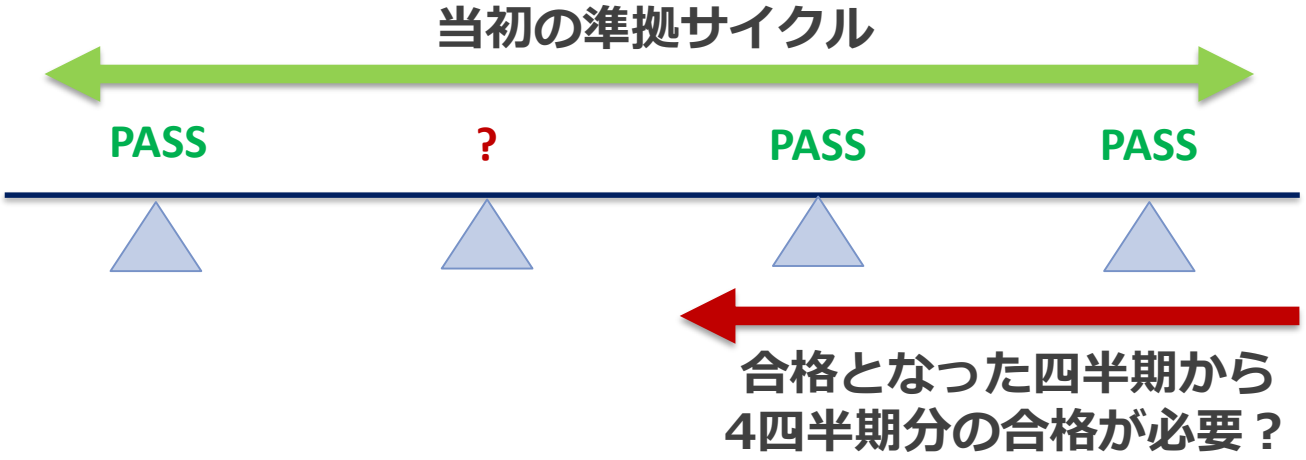
- 目的は、準拠証明（AOC）ではなく、セキュリティの維持・強化

Compliance Curve（準拠曲線）の例



よくある問題：脆弱性スキャンの不合格・脆弱性の未解決

第2四半期の外部脆弱性スキャンに「合格」できなかった…
準拠のためには第3四半期から一年間必要？



なぜ「合格」できなかったのか？

- スキャンを実施しなかった
  - スキャンを実施できない理由があった
  - スキャンの実施を忘れていた（新しく追加されたシステムだった？）
- スキャンは実施したが、期間中に脆弱性の対応が完了できなかった

この場合、QSA はどのように判断するか？

PCI DSSの日常業務（BAU）プロセスへの組み込み（1/2）

すべての組織を対象とした要件

- **システム変更時**におけるPCI DSS要件の実装（要件6.4.6）
  - ✓ ネットワーク構成図のアップデート
  - ✓ システム構成基準の適用（デフォルトパスワードの変更および不必要なサービスの無効化を含む）
  - ✓ 要件で求められるシステムの保護（例：ファイル整合性監視、アンチウイルス、パッチ、監査ログ）
  - ✓ 機密認証データの非保持、保存されるカード会員データの文書化、データ保管ポリシーや手順への反映
  - ✓ 新しいシステムを四半期毎の脆弱性スキャンプロセスに含める　など

PCI DSSの日常業務（BAU）プロセスへの組み込み（2/2）

サービスプロバイダ向け要件

- 正式なPCI DSS準拠プログラムの確立（要件12.4.1）
- 暗号アーキテクチャの文書化（要件3.5.1）
- **四半期毎**の従業員のポリシー順守状況チェック（要件12.11、12.11.1）
  - ✓ 日次ログレビュー
  - ✓ ファイアウォールのルールセットレビュー
  - ✓ 新たなシステムへの構成基準の適用
  - ✓ セキュリティアラートへの対応
  - ✓ 変更管理プロセス
- **6カ月毎**のセグメンテーション制御のペネトレーションテスト（要件11.3.4.1）
- 重要なセキュリティ制御システムの**障害**検知/報告/対応（要件10.8、10.8.1）
  - ✓ ファイアウォール
  - ✓ IDS/IPS
  - ✓ FIM（ファイル整合性監視）
  - ✓ アンチウイルス
  - ✓ 物理的アクセス制御
  - ✓ 論理的アクセス制御
  - ✓ 監査ログメカニズム
  - ✓ セグメンテーション制御（使用されている場合）など

PCI DSS準拠カレンダー（一部）

【S】：サービスプロバイダ向けの追加要件

➢ 日次

要件	領域	DSS3.2	活動
10	ログ管理	10.6.1	すべてのCDEおよび重要なコンポーネントのログおよびセキュリティイベントをレビューし、疑わしい活動を識別する

➢ 週次

要件	領域	DSS3.2	活動
11	(ファイル)整合性監視	11.5	ファイル完全性監視ソフトウェアのような変更検知メカニズムを使用し重要なファイルを比較する

➢ 四半期毎

要件	領域	DSS3.2	活動
3	データ保持	3.1.b	定義済みデータ保持期限を超えたいかなるカード会員データを識別し安全に削除する
8	アクセス管理	8.1.4	非アクティブなユーザーを削除/無効化する
	ユーザー認証管理	8.2.4	システムコンポーネントのパスワード/パスフレーズを少なくとも90日に1回変更する
11	ワイヤレスアクセスポイント	11.1	すべてのアクセスポイントの存在をテストし、承認済みまたは不正なワイヤレスアクセスポイントを識別する
	脆弱性スキャン	11.2.1	必要に応じて内部脆弱性スキャンを実施し、要件6.1で特定されたすべての脆弱性が解決するまで行う
		11.2.2	ASVによる外部脆弱性スキャンを実施し、すべて合格するまで再スキャンを行う
12	担当者の業務レビュー	12.11【S】	セキュリティポリシーや手順で定義された作業が担当者に遵守されているかをレビューする

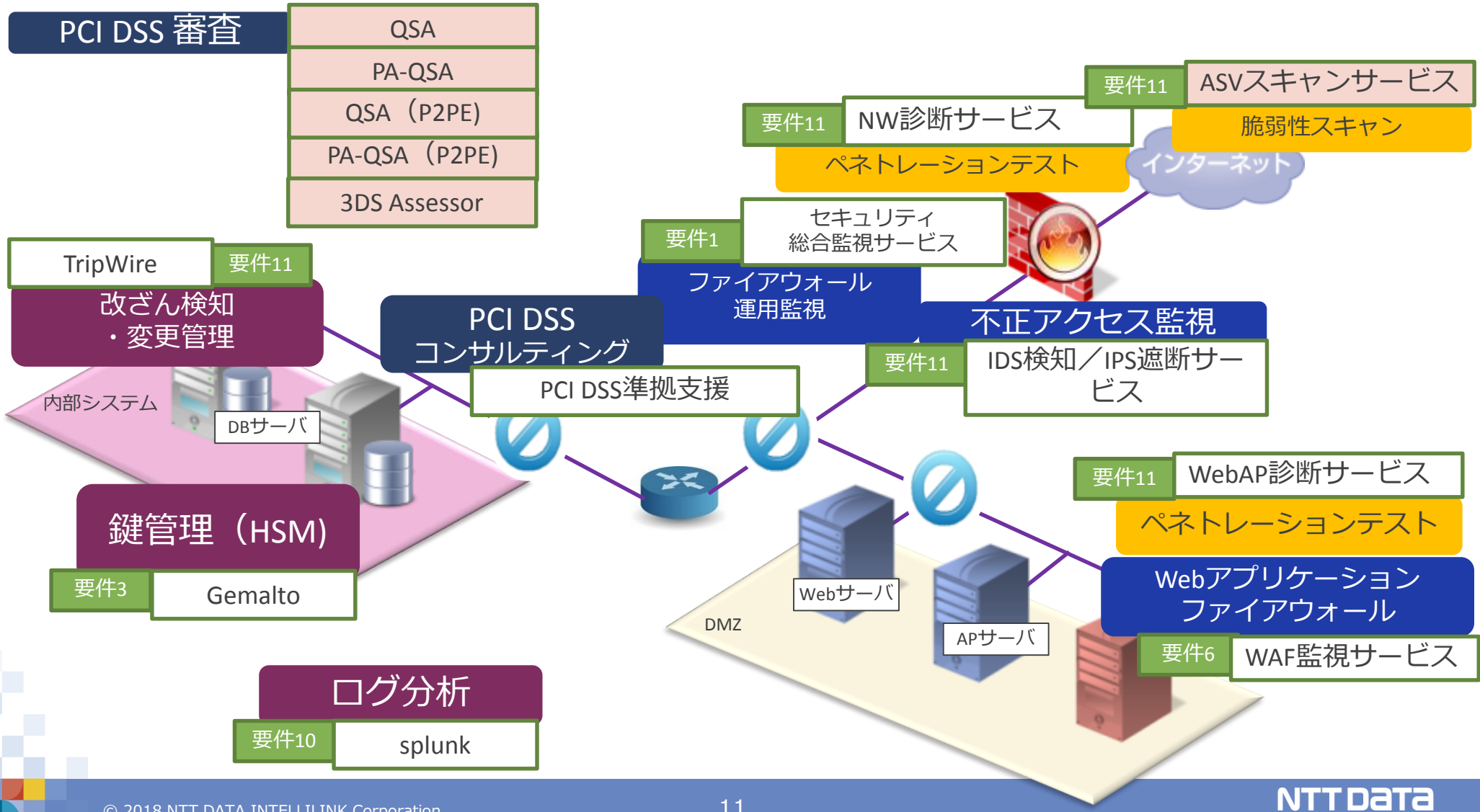
➢ 半期毎

要件	領域	DSS3.2	活動
1	ファイアウォールおよびルータ	1.1.7	すべてのファイアウォールとルータのルールセットについて最低6ヵ月毎にレビューする
11	ペネトレーションテスト	11.3.4.1【S】	ペネトレーションテストによるセグメンテーション制御の有効性を少なくとも6ヵ月毎にテストする

NTTデータ先端技術の
「PCIトータルサービス」のご紹介

NTTデータ先端技術の「PCIトータルサービス」

弊社ではPCI DSS準拠のためのさまざまなソリューションを提供しております。



NTTデータ 先端技術株式会社

改ざん検知・変更管理ソリューション「Tripwire Enterprise」

要件11

変更管理プロセスを強化し、改ざん検知/コンプライアンス証明の提供により確実で効率的なIT運用を実現

マルチベンダー環境にある、さまざまなサーバ、ネットワーク機器に加えられる変更を一元管理。単に変更検知するだけでなく、その変更があらかじめ予定されていたものかを自動的に評価し、管理プロセスが有効に働いていることを証明できます。

特長

- 誰が、何を、いつ、どのように変更したのかなど、豊富な観点
- インフラやプロセスの整合性の証拠を蓄積
- 計画された変更が予定通りに実施されたかの確認が可能
- 変更状況、変更履歴、承認/未承認の割合など、グラフィカルなレポートを自由にカスタマイズ可能

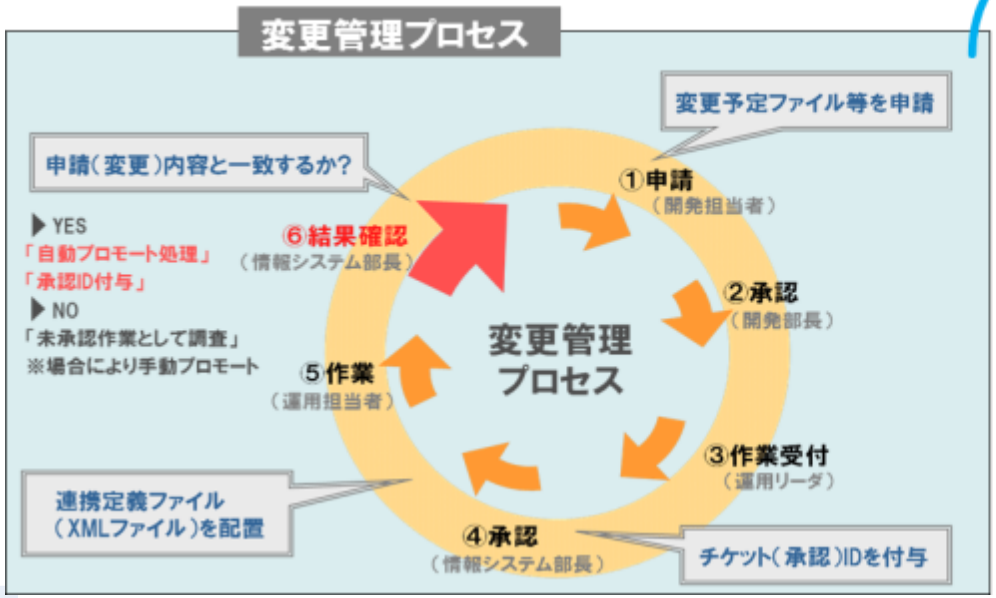
導入効果

- 改ざんチェック
- コンプライアンスの証明
- 確実で効率的なITシステムの運用（IT全般統制）

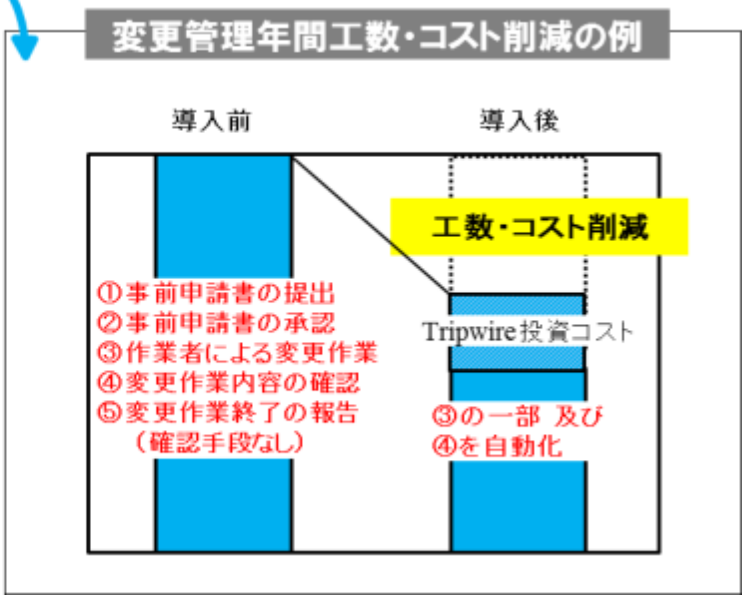
導入実績

大手金融機関、情報サービス、通信、流通、製造、エネルギー、官公庁など

変更管理プロセス



変更管理年間工数・コスト削減の例



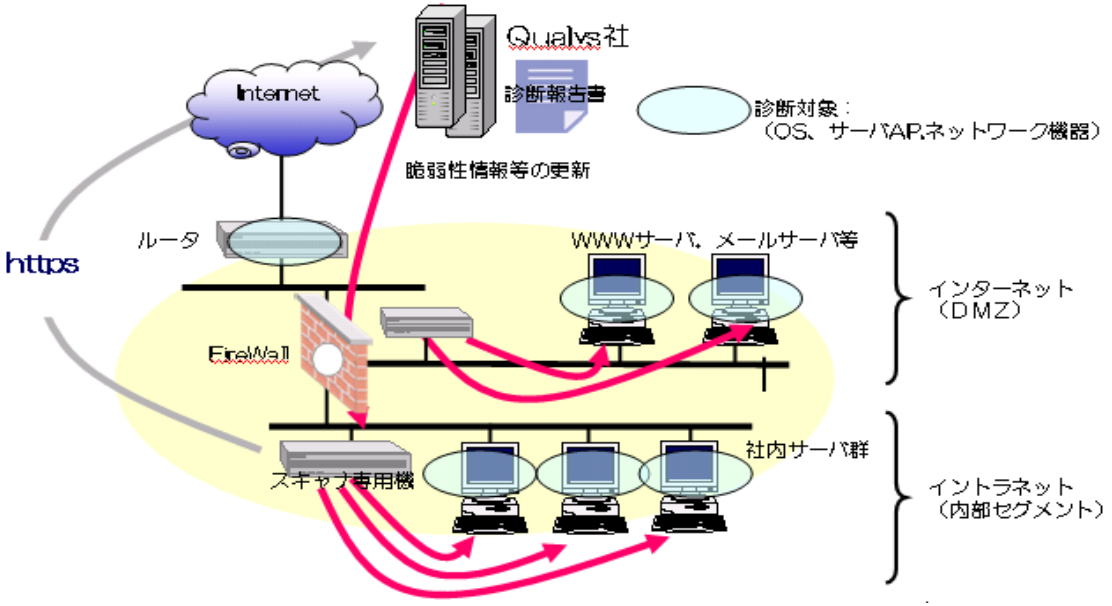
NTT DATA
NTTデータ 先端技術株式会社

脆弱性管理ソリューション　「QualysGuard」

要件11

脆弱性管理プロセスをシステム化することにより、運用コストの長期的な削減や、高速な脆弱性診断を可能とするSaaS型ソリューション

QualysGuardExpress(中小規模)　QualysGuardEnterprise(大規模)※**ASVスキャンNinjaSCAN(PCI DSS)**



- **脆弱性検出**
  高速でかつ、安全性が高い脆弱性診断の実施が可能。
- **世界最大規模の脆弱性DB**
  業界最大規模の脆弱性シグニチャナレッジベース を備えており、かつ週4～5回程度と高頻度でアップデート。
- **自動化**
  予めテンプレートやスケジュールを設定することで、脆弱性管理のステップを自動化。
- **脆弱性管理**
  検出された脆弱性だけではなく、チケット発行によってその後の対応状況まで可視化

導入効果

- 脆弱性の洗い出し
- 脆弱性の管理(前回との対比、対応状況など)
- 内製化によるコスト低減

導入実績

世界で1.5億IPの実績
PCI DSSのASVスキャンで採用

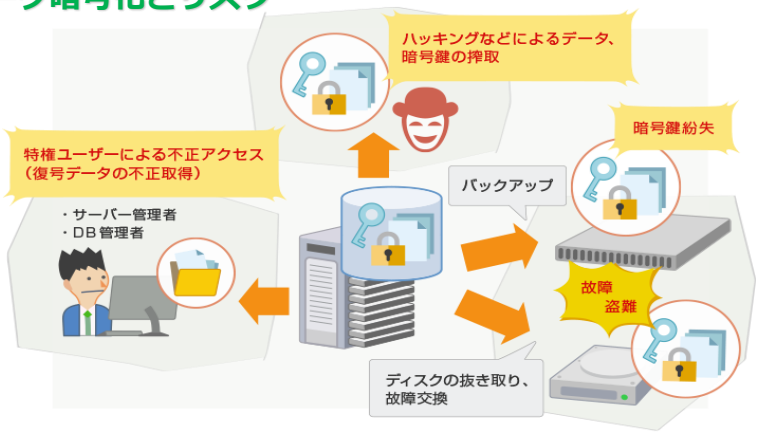
暗号鍵管理 SafeNet Network HSM

要件3

暗号鍵管理専用アプライアンスで情報漏洩リスクを低減させるソリューション

SafeNet Network HSMはネットワーク対応型の汎用HSM（ハードウェアセキュリティモジュール）です。
ハードウェア内で暗号鍵を厳重に管理し、暗号化データと暗号鍵を物理的に分ける事により、仮に暗号データが盗まれても、復号されるリスクが低減できます。

データ暗号化とリスク



HSMでの鍵管理によるリスクの低減

特長

- FIPS140-2（Level2,Level3）検証済み
- どのような形でも暗号鍵がHSM外に保存されることはない
- MofN認証（ユーザーおよびRoleごとに異なる物理的に安全なインターフェースを使用した認証システム）で不正な運用を排除
- 物理的な攻撃が発生すると、不正利用防止機能が起動し暗号鍵が自動削除される
- 導入が容易なネットワーク接続タイプ
- パフォーマンス要件によりモデルを選択可能
- 冗長化構成により信頼性とパフォーマンスの向上が可能
- 各種APIサポート（PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, REST等）

導入効果

- **機密情報の暗号化と厳重な鍵管理による情報漏洩対策**
- 職務分掌により内部からの情報漏洩リスクを低減
- PCI DSSの一部要件に適合可能
- 暗号鍵削除による論理的なデータ消去で安全にデータ廃棄

導入実績

主に金融機関、官公庁

- PKI鍵生成と保管（認証局）
- 証明書検証と署名
- データベース暗号化及び鍵管理
- マスター鍵管理

まとめ

まとめ

PCI DSSは準拠状態を維持することが重要

- PCI DSSで求められている活動を日常業務に組み込むことで準拠を維持
- 定期的なモニタリングにより準拠状況の維持を確認
- 上記を実現する各種ソリューション提供のご相談もお受けしています

NTT DATA

Trusted Global Innovator