PCIにおける自動化アプローチと弊社サービスのご紹介

株式会社GRCS
川島祐樹 CISSP, QSA

会社概要

会社名	株式会社GRCS（**旧NANAROQ**／2018年3月1日商号変更）
設立	2005年3月
決算期	11月
資本金	1億円（2017年11月30日）
役員構成	代表取締役社長 佐々木慈和（ササキヨシカズ） 取締役 兼 COO　榎本司 取締役 兼 CTO　塚本拓也 取締役 兼 CFO　田中郁恵 社外取締役　　久保恵一
所在地	東京都千代田区五番町1-9　MG市ヶ谷ビルディング9F
従業員数	60名（2018年6月現在）
所属団体	一般社団法人日本CISO協会（代表理事） 日本カード情報セキュリティー協議会（運営委員）
資格	PCI DSS認証審査機関

GRC+Sとは

Governance（ガバナンス）Risk（リスク）Compliance（コンプライアンス）の頭文字をとったもので、企業等が抱える複合的リスクを統合的に管理する手法を指します。
具体的には、GRCとそれを支えるSecurity（セキュリティ）を加え、以下の活動が含まれています。

G Governance

企業がその目標達成を実現するために、企業の方針・ルールを徹底させ、
経営管理を強化する活動

R Risk Management

ガバナンスとリスクを前提とし、その阻害要因となるリスクを評価し対応策を講じ、モニタリングを行う一連の活動

C Compliance

法令遵守そのものだけでなくリスクマネジメント方針やリスク対応（評価と低減、移転等）プロセスが遵守、運用されているかをモニタリングする活動

S Security

企業に不可欠のセキュリティマネジメントや全てのIT領域をGRCのアプローチで管理する活動

自己紹介

川島祐樹@GRCS

2006
QSA/ASV/PA-QSA @ 某QSA

2012
CSIRTリーダー @ 某ISP
- セキュリティ監視
- セキュリティ診断
- IR&フォレンジック

2018
NOW
QSA@GRCS

PCIデータセキュリティ基準
完全対策（日経BP） 2008

実践Metasploit（O'Reilly）2012

連載 オール・ザッツ・PCI DSS (@IT) 2008-2011

PCIにおける自動化アプローチ

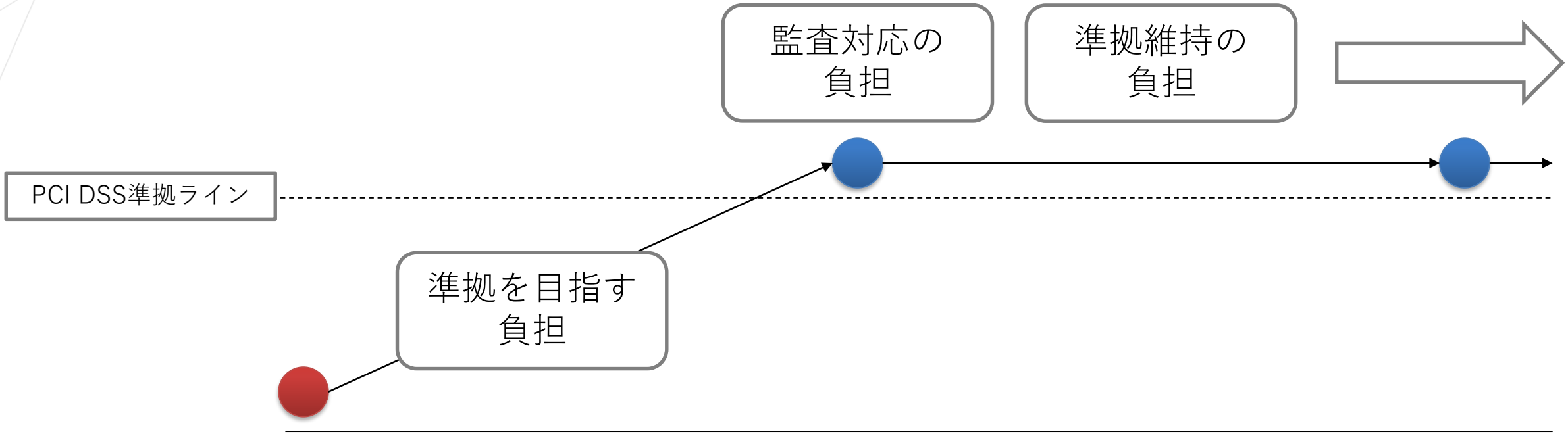
PCI DSSを取り巻く状況

- 準拠企業、目指す企業の増加
- PCI DSSの成熟、関連情報増加
- 法整備、実行計画

PCI DSSを取り巻く状況

- 準拠企業で発生する事故
- 監査や準拠維持活動の負担

様々な負担



そして、負担に見合う効果は？

監査の現実

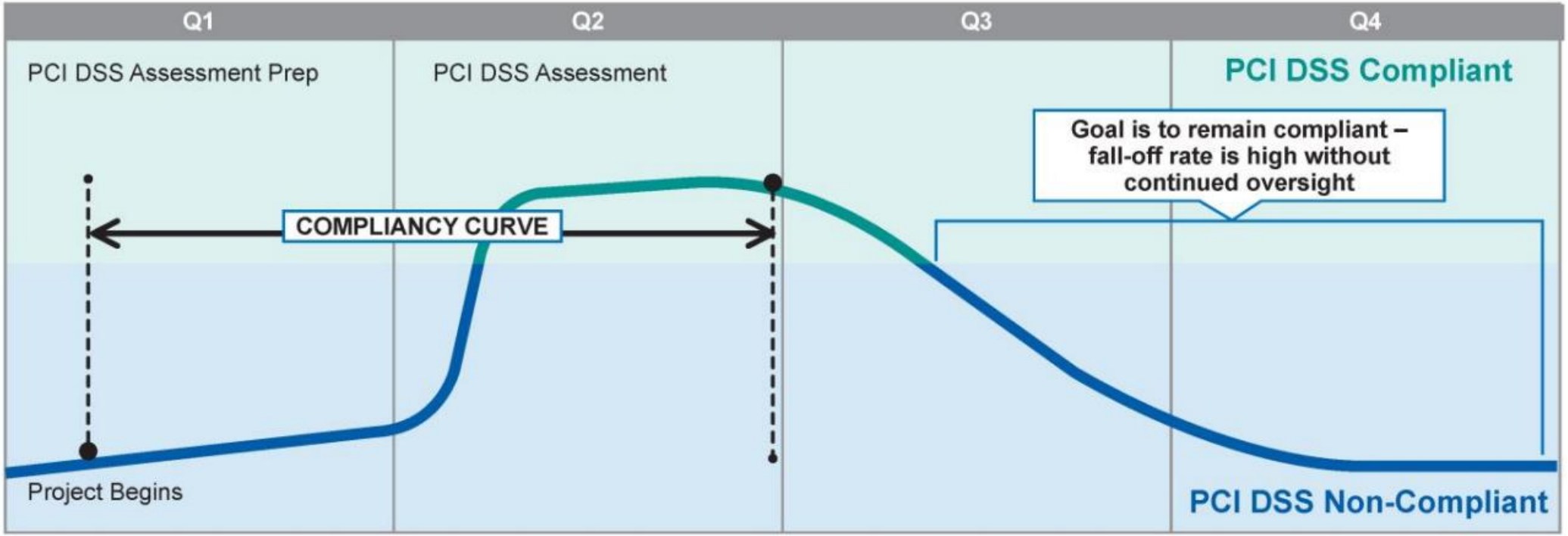
? 監査時に証跡が足りないことに気づいた・・・

? 監査は無事合格・・・

? 今回、監査人が変わった・・・

監査と準拠状態の維持

- 年次の監査にだけフォーカスしてしまうと
  準拠状態が維持できない傾向



引用： https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

Best Practice

1. Maintain the Proper Perspective
2. Assign Ownership for Coordinating Security Activities
3. Emphasize Security and Risk, Not Just Compliance
4. Continuously Monitor Security Controls
5. Detect and Respond to Security Control Failures
6. Develop Performance Metrics to Measure Success
7. Adjust the Program to Address Changes

引用： https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

準拠しているのにセキュリティ事故が発生？

CIO FROM IDG INSIDER Sign In | Register

Home > Compliance

FEATURE

The real reason you're failing at PCI DSS compliance

For more than a decade, organizations have struggled to achieve and maintain PCI DSS compliance. The problem isn't knowledge or technology; it's proficiency.

Strong compliance practices, strong security

van Oosten notes that of the nearly 300 payment card data breaches Verizon has investigated between 2010 and 2016, not one was fully compliant at the time of the breach. Some of those organizations did achieve compliance at one point, but they didn't maintain it, often because they treat compliance as a goal to be achieved rather than a process.

- 一度は準拠していても、セキュリティ事故発生時は準拠状態ではない傾向
- 準拠達成後に適切に維持していなかった
- コンプライアンスを「ゴール」ではなく「プロセス」ととらえる

引用： The real reason you're failing at PCI DSS Compliance
https://www.cio.com/article/3241035/compliance/the-real-reason-youre-failing-at-pci-dss-compliance.html

Best Practice

1. Consolidate for ease of management.
2. Invest in developing expertise.
3. Apply a balanced approach.
4. Automate everything possible.
5. Design, operate, and manage the internal control environment.

引用： The real reason you’re failing at PCI DSS Compliance
https://www.cio.com/article/3241035/compliance/the-real-reason-youre-failing-at-pci-dss-compliance.html

Best Practice, Best Practice, …

1. Maintain the Proper Perspective
2. Assign Ownership for Coordinating Security Activities
3. Emphasize Security and Risk, Not Just Compliance
4. Continuously Monitor Security Controls
5. Detect and Respond to Security Control Failures
6. Develop Performance Metrics to Measure Success
7. Adjust the Program to Address Changes

Best Practices for Maintaining PCI DSS Compliance

1. Consolidate for ease of management.
2. Invest in developing expertise.
3. Apply a balanced approach.
4. Automate everything possible.
5. Design, operate, and manage the internal control environment.

The real reason you're failing at PCI DSS Compliance

キー＝自動化

1. Maintain the Proper Perspective
2. Assign Ownership for Coordinating Security Activities
3. Emphasize Security and Risk, Not Just Compliance
4. **Continuously Monitor Security Controls**
5. Detect and Respond to Security Control Failures
6. Develop Performance Metrics to Measure Success
7. Adjust the Program to Address Changes

Best Practices for Maintaining PCI DSS Compliance

1. Consolidate for ease of management.
2. Invest in developing expertise.
3. Apply a balanced approach.
4. **Automate everything possible.**
5. Design, operate, and manage the internal control environment.

The real reason you're failing at PCI DSS Compliance

自動化！

自動化がもたらすメリット

- 自動化によって
  - ✓ 人の負荷が減る
  - ✓ ミスが減る
  - ✓ 効果を測定しやすくなる
- 自動化の仕組み検討・構築にあたって
  - ✓ 業務プロセスが明確になる
  - ✓ 人依存の業務が減る
  - ✓ 現場に改善の考え方が浸透する

自動化アプローチにおけるポイント

- リソースを確保する
  - 片手間の業務改善ととらえるべきではない
  - 自動化を検討、実証、運用するためのリソースを割り当てる
- 完璧を目指さない
  - スモールスタート、簡単なところから始める
  - 簡単な仕組みが回るようになったら、拡張していく
- 捨てる勇気
  - それを本当に人がやる必要があるのかどうか、徹底的に考える
  - 長年やってきている事でも、捨てた方が良いかもしれない

自動化アプローチの全体イメージ

スコープ内システム
関連システム

タスク管理

ドキュメント管理

メッセージング

自動化を行うための**土台**

スクリプト開発

自動化
ソリューション

対象システムと各種管理ツールを
つなぎ、自動化する

自動化アプローチ　タスク管理

- タスク管理ツールを使う（必須）

  例）JIRAなど、APIで操作可能なもの

  – 適用ポイント： メールでの依頼、EXCELの管理表
  – ワークフロー機能を活用して「承認」を記録する
  – 人が介在していないものも、タスクとして記録する
  – 年間タスク、定期タスク、非定期タスク

監査証跡のリポジトリになる

タスク状態を追跡して数値化も可能になる

自動化アプローチ　タスク管理　おすすめツール

当日説明

自動化アプローチ　ドキュメント管理

- ドキュメント管理ツールを使う（重要）
  - 例）Confluence、SharePoint…
- メリット
  - 全文検索が容易
  - 各要件に必要な文書名および内容のリストアップ、管理
  - バージョン＆更新履歴管理（→ タスク管理と連携）

自動化アプローチ　ドキュメント管理　例

当日説明

自動化アプローチ　メッセージングツール

- メッセージングツールを使う（重要）
  - 具体的には…Slack、HipChat、Teams・・・
- メリット
  - 人の活動と機械の活動を１つの場所で追跡可能
  - 発生した事案に対してその場でコミュニケーション可能
  - API連携、Botにより他ツールとの双方向連携も可能

自動化アプローチ　メッセージングツール　活用例

当日説明

自動化アプローチ　ケーススタディ（１）

要件1.2.2.b **ルーター構成を調べて、同期化されていることを確認**する。例えば、実行（アクティブ）構成ファイルが起動構成（マシンの再起動時に使用）に一致することを確認する

自動化アプローチ　ケーススタディ（1）

- 要件1.2.2.b **ルーター構成を調べて、同期化されていることを確認**する。例えば、実行（アクティブ）構成ファイルが起動構成（マシンの再起動時に使用）に一致することを確認する

当日説明

自動化アプローチ　ケーススタディ（1）

当日説明

自動化アプローチ　ケーススタディ（2）

要件11.2.1 四半期ごとの内部脆弱性スキャンを実施する。事業体の脆弱性ランク付け（要件 6.1 に基づく）に従ったすべての「高リスク」脆弱性が解決されたことを確認するため、脆弱性に対応し、再スキャンを実施する。スキャンは有資格者が実施する必要がある。

11.2.1.a スキャンレポートをレビューし、四半期ごとの**内部スキャンが過去 12 カ月間で 4 回行われたことを確認**する。

11.2.1.b スキャンレポートをレビューし、**すべての「高リスク」脆弱性が対応されたこと**と、スキャンプロセスに「高リスク」脆弱性（PCI DSS 要件 6.1 で定義された）が**解決された再スキャンの結果が含まれること**を確認する。

11.2.1.c 担当者をインタビューすることで、スキャンが**内部リソースまたは資格のある外部の第三者によって行われたこと**、該当する場合は、テスターの組織の独立性（QSA や ASV である必要はない）が存在することを確認する。

自動化アプローチ　ケーススタディ（2）

当日説明

自動化アプローチ　ケーススタディ（2）

当日説明

自動化アプローチ まとめ

自動化アプローチ　まとめ

- 自動化を検討する前段階の準備
  - タスク管理ツール、メッセージングツールの検討
  - 開発部門、運用部門とも相談
  - リソースを確保
- 自動化にあたって
  - 簡単なところから始める
  - 限界が見えてきたら自動化ソリューション導入検討
- 準拠維持運用のための活動へシフト
  - 監査も重要だが、日々の準拠維持運用が最重要
  - ただし、チェック頻度を増やすだけでは負担が大きすぎる
  - 自動化を行い、「日々監査している」状態を目指す

自動化アプローチ　まとめ

対象システム・関連システム

- 対象システム
- セキュリティ関連ツール
- 構成管理ツール
- 資産管理ツール

プロセス可視化
証跡レポジトリレイヤー

- タスク管理ツール
- ドキュメント管理ツール
- バージョン管理ツール
- 変更管理ツール

通知・コミュニケーション
レイヤー

- メッセージングツール
- 電話、SMSサービス
- （メール）

自動化処理実行レイヤー

スクリプト（初期、検証／中小規模向け）

ITプロセス自動化ツール、オーケストレーションツール（大規模向け）

弊社サービス紹介

PCI関連サービス

PCI関連サービス	セキュリティ監査・アセスメント	PIN Security PCI 3DS PCI Card Production PCI DSS
	教育	PCI DSS研修（基礎・応用）
	セキュリティ診断	セキュリティ診断内製化/自動化支援 脆弱性管理導入・運用支援
	※今後拡充予定・・・	PCI準拠維持運用支援 PCI準拠維持自動化支援

製品・クラウドサービス

サイバーセキュリティ リスク管理ソリューション CSIRT・教育	**自社開発**	CSIRT MT	CSIRTに必要な機能を実装したクラウドサービス
	自社開発	脆弱性TODAY	脆弱性情報日次配信サービス
	自社開発	ミニコブラス	ゲーム学習型教育クラウドサービス
インシデント検知・可視化 ソリューション 検知・フォレンジック	**自社開発**	SIEM.AI MT	オープンソースとAIを活用したSIEM
		RSA NetWitness	ネットワークフォレンジック・インシデント検知
		DARKTRACE	AIを利用した機械学習によるインシデント検知
次世代型エンドポイント 保護ソリューション EDR・DLP		Carbon Black.	エンドポイントを防御する次世代型AV＋EDR
		DIGITAL GUARDIAN	次世代データ・プロテクション・プラットフォーム
		DELL Dell Threat Defense	機械学習を利用したエンドポイントプロテクション
		Br Bromium	次世代仮想隔離型エンドポイントプロテクション
企業経営における リスク管理ソリューション GRC	**自社開発**	SUPPLIER RISK MT	外部委託先リスクマネジメントクラウドサービス
		RSA Archer GRC Platform	GRCの統合管理を実現

GRCS領域に関連するコンサルティング・製品開発を行っております

コンサルティングサービス

サイバーセキュリティ リスク管理コンサルティング CSIRT・教育	**セキュリティ監査・アセスメント**	PIN Security、３Dセキュア
	CSIRT構築・運用支援	組織立ち上げ、運用改善、アドバイザリ
	エンジニア教育	CSIRT研修、標的型メール対応
インシデント検知・可視化 コンサルティング 検知・フォレンジック	**エンタープライズパケット分析**	インシデント分析、レポート
	脆弱性検査	ネットワーク、サーバ、アプリケーションの検査
	SOC構築・運用	構築・運用および定期レポート報告
次世代型セキュリティ 製品導入 エンドポイント・SIEM	**エンドポイント製品導入**	次世代型エンドポイント製品の導入
	SIEM構築・導入	SIEM製品およびオープンソースの導入
企業経営における リスク管理コンサルティング GRC	**グローバルガバナンス**	規定策定・法令対応
	リスク管理効率化	全社リスクアセスメント
	各種認証取得支援	ISMS、PCIDSS、個人情報保護

www.grcs.co.jp