これからの品質保証部門のあり方
～モノ作り から コト作り への変化に対応する品質保証～

第14期 ソフトウェア品質保証部長の会　第2グループ

梯 雅人（株式会社日立システムズ）
神崎　和洋（SCSK株式会社）
小松澤　敦（株式会社日立ドキュメントソリューションズ）
長谷川　直人（日立Astemo株式会社）
陸野　礼子（株式会社日新システムズ）

（五十音順）

はじめに

「これからの品質保証部門のあり方」は13期からの継続テーマです。
13期の提言を深掘りし、品質保証部門に求められる具体的な活動案の提示を目標に活動いたしました。

本発表会では、

・品質保証部門に求められる活動「コト作りのハブ」

について報告します。

ご意見や今後の活動についてご意見があればアンケートに記載していただけるようお願いします。

以降、品質保証部門は品証部門と表記します。

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

1．背景（13期の振り返り）

部長の会発足当時（2010年頃）の品証部門

「成果物の品質保証」「プロセスの標準化・品質管理」の役割を担う

・過去の失敗をプロセスに反映し、標準化

・プロセス標準、組織メトリクス標準と比較した品質判定

モノ作り から コト作り への変化

・成果物の保証から**ビジネスモデル・ビジネスライフサイクル全体**の保証へ

新しい品証部門への変革

過去にノウハウがない脅威シナリオや影響の想定、
新しいリスク対応策を生み出せる部門へ変革

・変化を察知し、**他組織や専門家とつながり**ながらリスク対応策を策定

・新技術に詳しいメンバを部門内に育成、専門家の知見で品質作り込み

・エンジニアリング技術を使った品質作り込みを主導、効率化に寄与

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

2．コト作りのハブ（14期の検討テーマ）

変化を察知し、**他組織や専門家とつながり**ながらリスク対応策を策定

品証部門は品質に関して、専門部門の「ハブ」になる

横展開

全方位展開

「モノ作りのハブ」 から 「コト作りのハブ」 へ

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

2．コト作りのハブ（14期の検討テーマ）

「コト作りのハブ」としての基本活動

- **専門部門と共に課題となる要素を洗い出す**
  - 法令、規格、規制情報など（法務）
  - 資産、キャッシュフロー（財務）
  - 顧客契約管理や調達先管理（営業、調達）など
- **課題に対して保証すべき品質を定義**
  - ゴールの明確化
- **品質を保証するための新しいルールや仕組みを構築**
  - ステークホルダーに対して変化への気づきを与える
- **ルールや仕組みの教育、実行の監査**
  - 継続的な意識教育や監査　（教育、監査）

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

3．コト作りが直面している状況

ビジネスライフサイクル全体に関わる状況

- **社会情勢の変化による各種レギュレーションの変更**
  - 働き方改革、少子高齢化、安全保障、個人情報保護
  - 品質コンプライアンス、CSR、SDGs
  - 企業関係（共創、エコシステム、調達・・・）

- **企業等が直面するリスクの増加**
  - サイバー攻撃、内部不正、ネット炎上

- **新技術由来の品質課題**
  - 顧客満足の変化、スピード重視、アジャイル
  - DX、AI、ビッグデータ、IoT 自動運転
  - 新しいハードウエア、仮想現実、Digital Twin

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

４．具体的な取り組み（CSR） 1

CSR (Corporate Social Responsibility)とは

- **企業が社会的存在として果たすべき責任のこと**
- **企業が社会からの信頼を維持するためにCSRを適切に果たすことが重要**
- **CSR７つの原則**
  - 説明責任
  - 透明性
  - 倫理的な行動
  - ステークホルダーの利害の尊重
  - 法の支配の尊重
  - 国際行動規範の尊重
  - 人権の尊重

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

4．具体的な取り組み（CSR）2

なぜ近年注目されるようになったのか？

持続可能な世界に向けた取り組みが企業にも求められている

- **サステナブルな社会を実現**するために、企業には、地球環境や人間社会を守り、持続させる取り組みが求められている。

インターネットとSNSの普及によるリアルタイムな情報の拡散

- 不透明な経営体制やコンプライアンス違反、ステークホルダーに対する**不誠実な姿勢**、信頼できない商品・サービスなどは**リアルタイムで拡散**される。反対に、より良い社会の構築や意欲的な環境保護といった**善良な活動も共有**され、**企業イメージや利益を大きく左右**する。

最新の法律への対応

- 例えば、改正民法においては、瑕疵外の不具合であっても、契約内容と異なる点があることが判明した時に、賠償責任が求められる。（賠償問題＝企業イメージ、信頼の失墜）

コンプライアンスを徹底するだけでは不十分。それに加えて、企業がその能力を活かして、社会に対してどのように貢献できるかを考え、行動することが求められる

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

4．具体的な取り組み（CSR） 3

CSR対応によるコト作りの品質向上

- 顧客、社会への貢献に繋がるコト作りはCSRに直結
  →**企業の姿勢は、その企業が創出する全ての品質に反映される**
- コト作りは魅力的品質の具現化が大きな要素
  →**社員のエンゲージメント向上により 品質＝価値 を創出する仕組みを構築**

品証部門が**ハブとして**取り組むべきこととは？

- 企業の姿勢に関わる課題は、それぞれ担当部門に割り振られるが、
  部分最適になりがち。問題発覚を防止できないリスクが高い。

- **品証部門が横ぐしを通し、全体最適を図る**
  - コト作りとしての企業姿勢＝**「企業品質」**の定義と目標設定
  - 社内各部門が持つ課題をまとめ、共有化することで**全体最適な改善**に繋げ、
    全体俯瞰の視点から監査実施
  - **社内外の知恵を集めナレッジ化**を推進

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

5．具体的な取り組み（サイバー攻撃） 1

年々、サイバー攻撃の脅威が増加！！

- 「情報セキュリティ10大脅威 2023」（IPA）の**上位3件はサイバー攻撃が占めている**（補足1 参照）

なぜ近年脅威が増加しているのか？

システム環境の変化　⇒　情報資産を守ることが難しい！

- テレワーク、バーチャルオフィス等の増加により、作業環境の多様化
- クラウドサービス利用の増加により、インターネット上にシステムを構築
  - ✓ **社内と社外の境界が曖昧に！**
    - ➢「社内のシステムを社外から守る」という概念が通用しない

大量の情報を一元管理　⇒　不正取得時のメリットが大きい！

- 紙媒体から電子媒体に！
- ビックデータやAIの活用、情報共有による利便性の追求
  - ✓ **大量データが一度に流出！**
    - ➢不正アクセス（犯罪）による情報取得のメリットが増加
    - ➢情報流出により、企業の信頼や経営へ多大な影響
  - ✓ **情報を人質に！**
    - ➢情報の完全性、可用性が失われることで、事業継続に影響

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

5．具体的な取り組み（サイバー攻撃）２

サイバー攻撃対応によるコト作りの品質向上

- **コト作りは中間工程の活動の保証が重要**

  →**成果物が良くても、開発・運用中の情報漏洩があれば全ての価値を失う**

品証部門が**ハブとして**取り組むべきこととは？

- **複数の技術部門と連携し、実効性のある対策を主導**
  - **様々な専門知識が必要！**
    - ✓ デバイス制御、ネットワーク、クラウド、暗号化など**複数領域の対策を組み合わせる**ことで、情報セキュリティリスクを低減する
  - **個別に対策を考え、推進すると、、、**
    - ✓ **過剰な対策**となり、現場運営が回らない
    - ✓ 対策の**優先順位や時間軸がバラバラ**
    - ✓ 対策全体としては**抜け漏れ**が発生
- **顧客や委託先を含めた関係者間の合意形成を主導**（観点は補足２ 参照）
  - **顧客との契約・合意（情報セキュリティ対策の費用負担、役割分担など）**
  - **委託先との契約・合意（機密情報の運用ルール、作業環境など）**

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

5．具体的な取り組み（サイバー攻撃）補足１

- **情報セキュリティ10大脅威の半分以上はサイバー攻撃**

昨年順位	個人	順位	組織	昨年順位
1位	フィッシングによる個人情報の詐取	**1位**	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	**2位**	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	**4位**	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	**5位**	テレワークなどのニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	**6位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	**7位**	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	**8位**	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネットバンキングの不正利用	**9位**	不注意による情報漏えいなどの被害	10位
NEW	ワンクリック請求等の不正請求による金銭被害	**10位**	犯罪のビジネス化（アンダーグラウンドサービス）	NEW

出典：独立行政法人 情報処理推進機構（IPA） 「情報セキュリティ10大脅威 2023」より

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

5．具体的な取り組み（サイバー攻撃）補足２

サイバー攻撃対応で我々が意識すべきこと

- **どのような情報を扱っているのか**
  - 宅配業者やホテルのフロントなどでは、荷物を預かるときに必ず中身を確認する
    しかし、システム構築や運用を行っている我々は何故か取り扱う情報を確認していない
- **情報セキュリティリスクの評価（レベル）とは**

  影響度：情報漏洩が発生した時の被害の大きさ（取り扱う情報の重要度と件数）
  発生率：情報漏洩が発生する可能性があるルートの多さ（業務範囲×作業環境×関わる人）

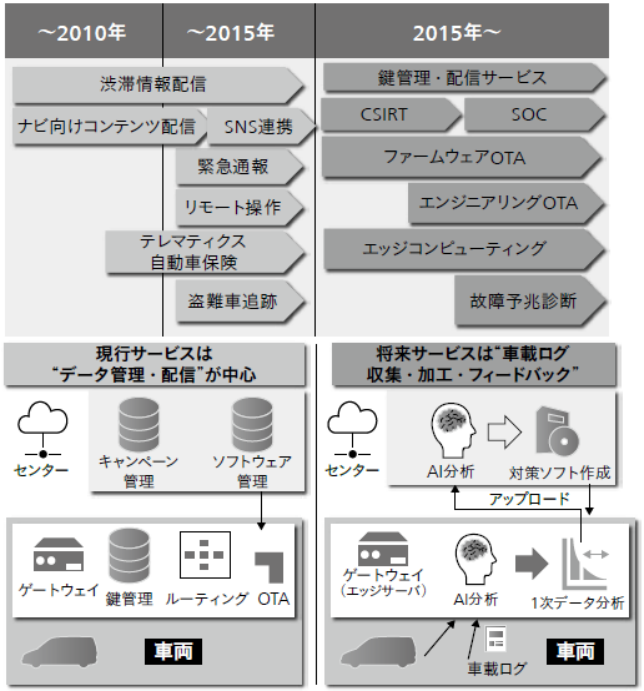
  ✓ **情報セキュリティリスクのレベルに応じた対策が必要**
- **システムを外部公開することとは**
  - **外部に公開したら必ずサイバー攻撃の対象になると認識すべき！**
  - **検証用環境や一時的な環境だからと言って気軽に公開してはダメ！**
    ⇒ 外部公開から数時間で侵入されることもある
- **顧客も含めた情報セキュリティマインドの醸成が不可欠**
  - **対策をベンダーに丸投げしてはダメ！**
    ⇒ 情報漏洩が発生したら結局は連帯責任！（発注者側も監督責任は免れない）
    ⇒ 関係者全員の認識合わせと平常時の取組みが重要

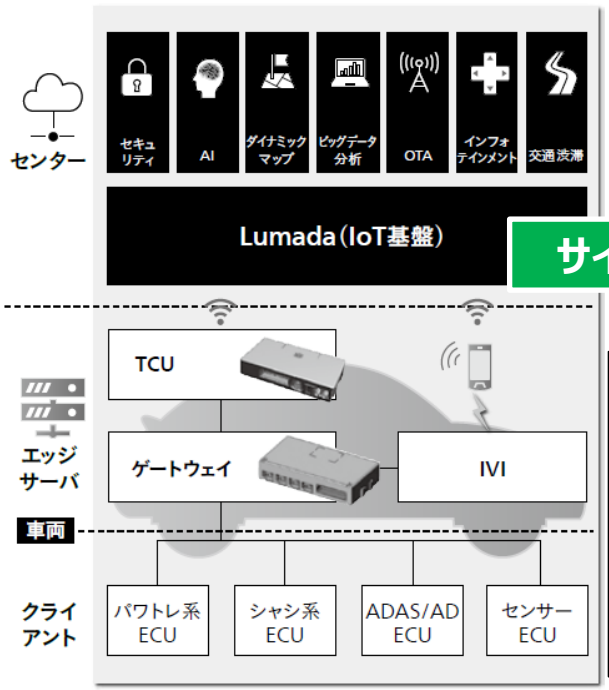
Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

6．具体的な取り組み（IoT） 1

自動車のIoT化(コネクテッドカー)とは

- コネクテッドカーとは、**通信端末としての機能を有する自動車**のことであり、車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析を行う。
- コネクテッドカーは運転者に様々な体験を提供する「コト作り」の代表





サイバー攻撃への対応が課題

SNS:Social Networking Service
CSIRT:Computer Security Incident Response Team
SOC:Security Operation Center
AI:Artificial Intelligence
OTA:Over the Air
TCU:Telematics Control Unit
IVI:In-vehicle Infotainment
ECU:Electronic Control Unit

https://www.hitachihyoron.com/jp/archive/2010s/2017/05/10a05/index.html

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

6．具体的な取り組み（IoT） 2

コネクテッドカーの課題は？

安全な運転の確保

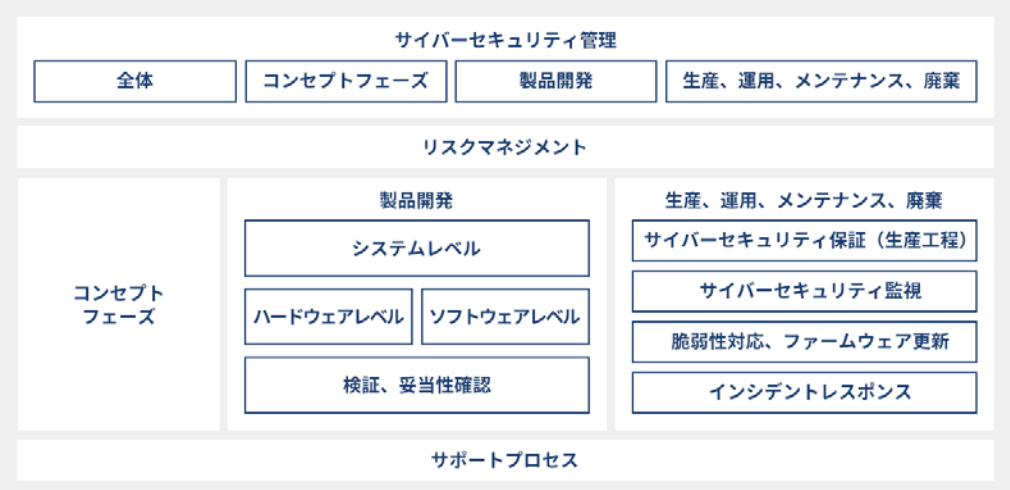
- 外部から運転機能を操作する等のサイバー攻撃の阻止

個人情報の保護

- ナビゲーション内の移動履歴などの個人情報が車内に存在

自動車用サイバーセキュリティ規格が制定され、適合がビジネス要件になっている

自動車用サイバーセキュリティ規格(ISO/SAE 21434)全体像



https://www.hitachiastemo.com/jp/products/connected/detail4.html

Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

6．具体的な取り組み（IoT） 3

コネクテッドカーの課題への対応事例

品証部門が**ハブとして**取り組むべきこととは？

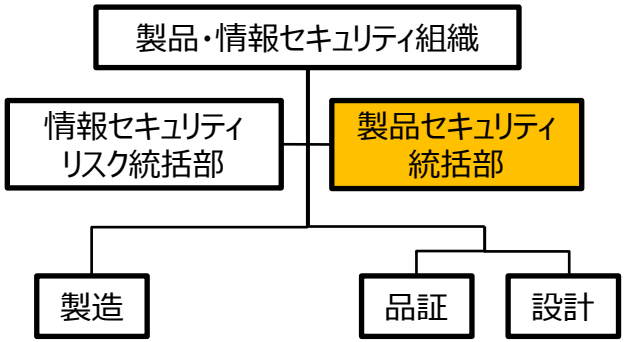
- **問題発生に備えた組織作り**

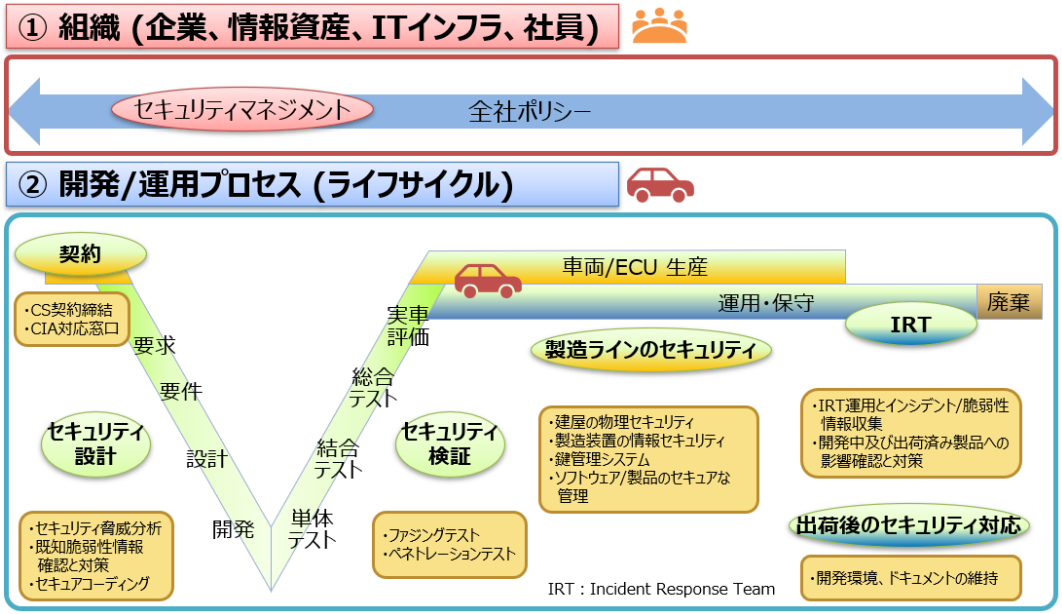
  ➡**品証部門からIRTの専門組織を設立しライフサイクル全体（契約から廃棄まで）のセキュリティ対応する。**

  IRT：Incident Response Team

- **自動車用サイバーセキュリティ規格への対応**

  ➡**専門エンジニアとコミュニケーションが取れる幅広い知識を品証部門も習得し、監査・アセスメントに対応する。**





Copyright (C) 2023 SQiPソフトウェア品質保証部長の会 All Rights Reserved

7．まとめ　1

「ハブ」の効果

情報が集まる

- ・情報から品質目標、ビジネス目標の設定
- ・プロアクティブに(問題発生前に)対応
- ・情報をナレッジ化し、改善サイクルを回せる

各部門の役割・責任範囲を俯瞰して見ることができる

- ・ヌケモレ防止
- ・部門毎の強み弱みを把握し、体制強化を提案

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

7．まとめ　2

「ハブ」になるためキーとなる能力

コミュニケーション能力（部門間のコミュニケーションを活性化）

- 定期的な会議や情報共有の場を設け、**部門間の課題を共有**

調整能力（異なる部門の利益や要求事項をバランス化）

- 公平で客観的な立場から異なる意見や**利害関係を調整**し、協働関係を構築

プロセス設計能力（部門間での業務プロセスを調整し、効率化）

- 異なる部門間の業務の連携や依存関係を理解し、**情報や作業が円滑に流れる**ようなプロセスを設計

プロジェクト管理能力（部門間の活動を適切に管理）

- 活動の計画、実行、監視、調整を行い、**適切なタイミング(時間軸)で各部門がプロジェクトに関与**

これまで培ってきた品証部門としての
リーダシップを発揮する

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

7．まとめ　3

- 社会情勢が変化し、技術革新が進む時代にあっても、これまで品証部門が築いてきた課題解決能力は有効である。

- これからの品証部門は、
「コト作りのハブ」としての役割を担い、
コト作りの共創パートナーとしての
「信頼」を顧客から得る。

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved

ご清聴
ありがとうございました。

Copyright (C)　2023　SQiPソフトウェア品質保証部長の会　All　Rights Reserved