SJ2020 ID:5

ゼロから作る品質マネジメントシステム（QMS）

~QMS構築の効率性を高めたプロセスアーキテクチャのエッセンス~

2020年10月15日

特定非営利活動法人　ITプロ技術者機構
和良品　文之丞

目次

0. 自己紹介と組織紹介

• 個人

氏名	わらしな　ぶんのじょう 和良品　　文之丞
所属	特定非営利活動法人 ITプロ技術者機構
経験	ソフトウェア開発　12年 開発管理　　8年 プロセス改善　　19年
今の仕事	CIO補佐官スタッフ 情報セキュリティ監査 情報処理技術者試験委員

• 組織

名称	特定非営利活動法人 ITプロ技術者機構
特徴	技術士を中心とした IT技術者の集団
組織情報	内閣府設立認証2007年4月 https://www.npo-homepage.go.jp/npoportal/detail/011088071
事業	CIO補佐官、同スタッフ CISOアドバイザー 情報セキュリティ監査

1. 概要

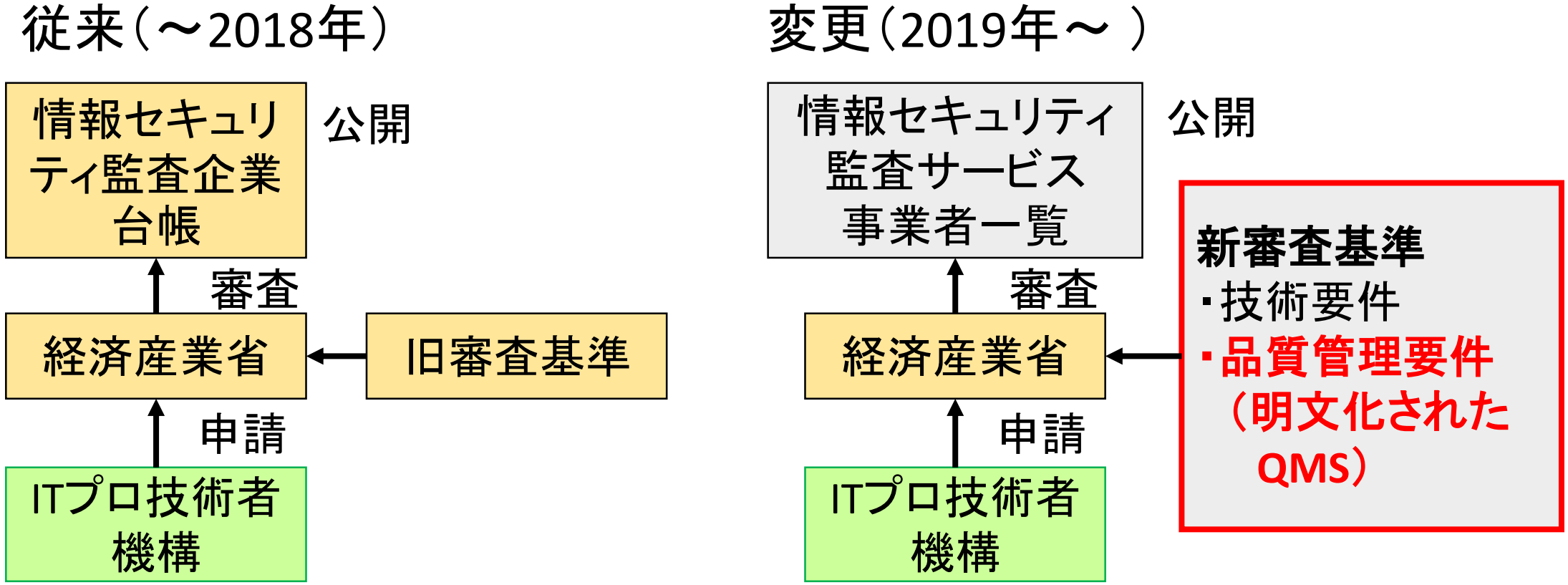
- 情報セキュリティ監査サービスを提供する組織に対して、新たに品質マネジメントシステム（QMS）を構築した。

- 従来経験したソフトウェア開発とは異なるサービスが対象だったが、過去のプロセス改善推進の知見を活用できた
  - 改善対象に対する共通点に注目、ヒントとなる知見の引き出し
  - プロセスアーキテクチャの考え方を発展

- 短期間で効率良くQMSを構築、目的とした審査に合格した。
  - 最終成果物（QMS）を意識して、関連する作業成果物を作成

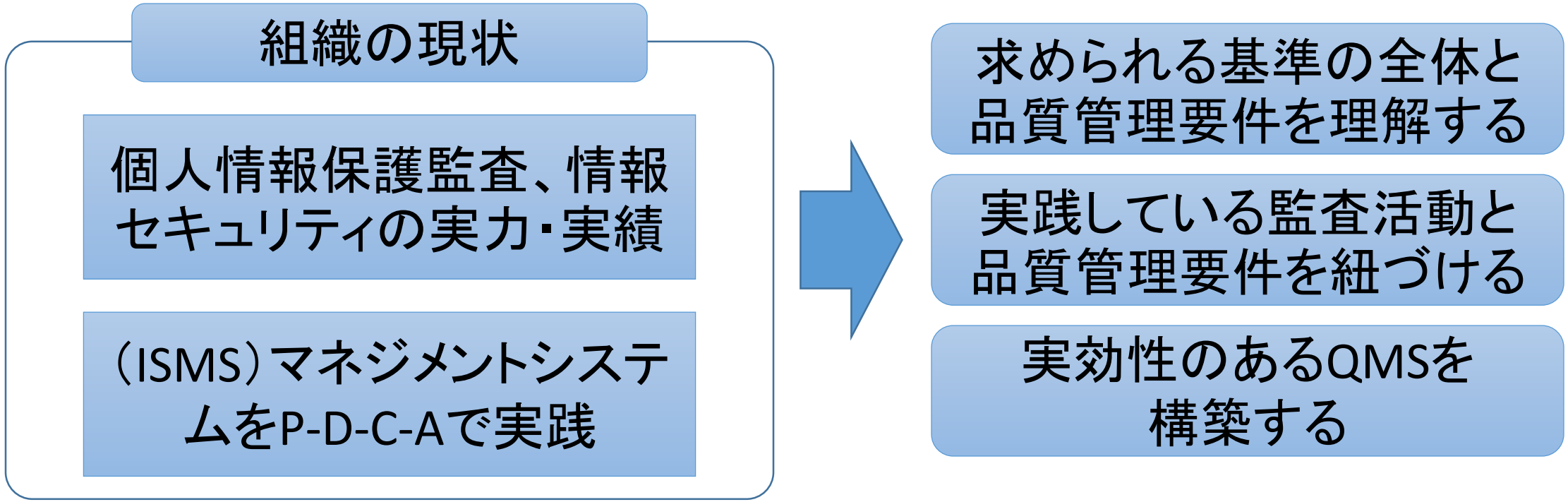
2. 背景

- 情報セキュリティ監査を行う事業者に対する経済産業省の審査基準の変更に伴い、明文化されたQMSが必要

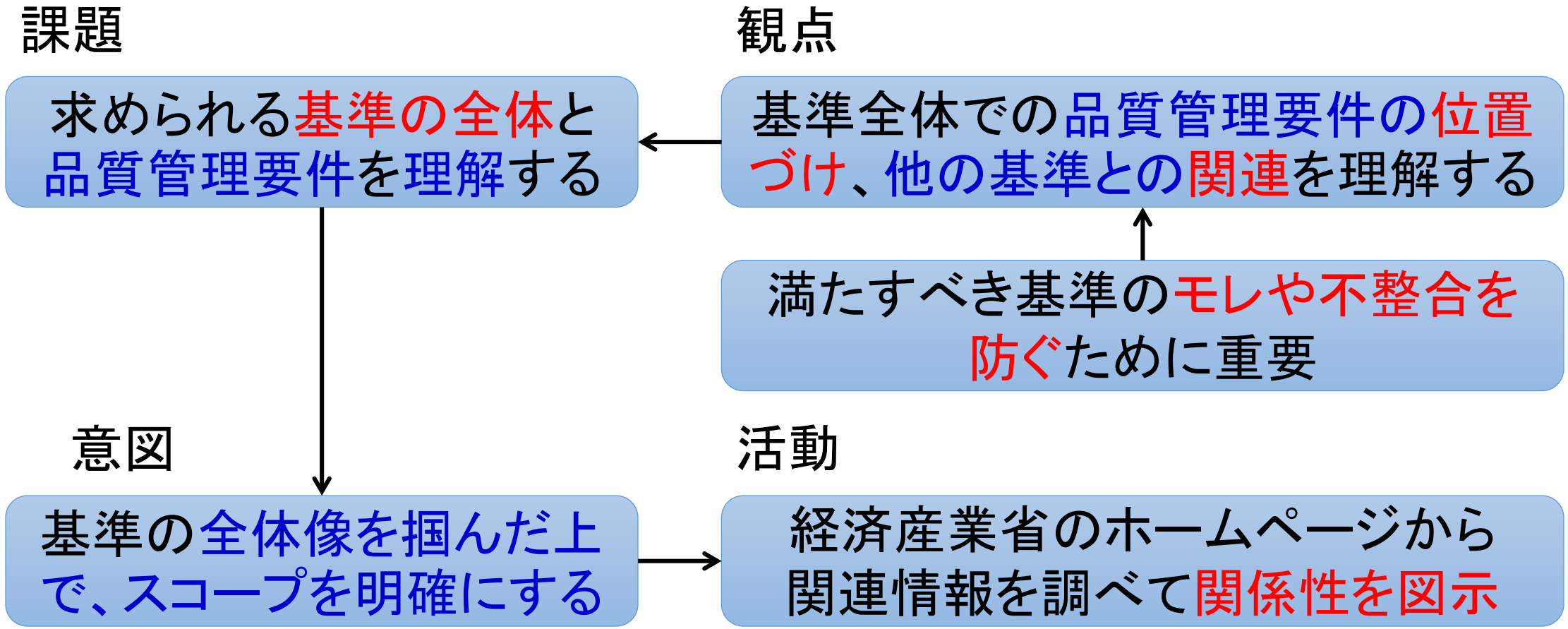


3. 課題

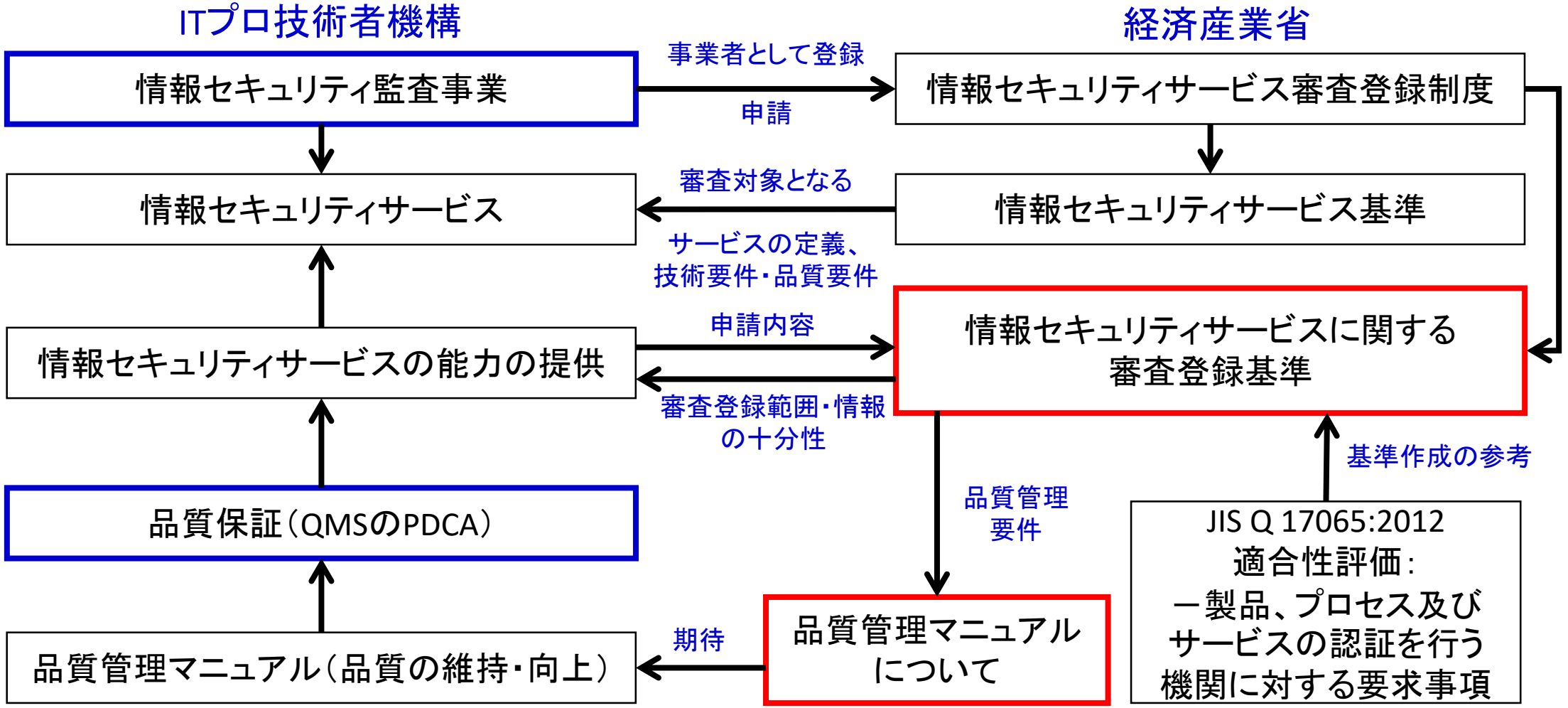
- 情報セキュリティ監査の実績・実力があり、情報セキュリティのマネジメントシステム（ISMS）があるのに、明文化されたQMSがない



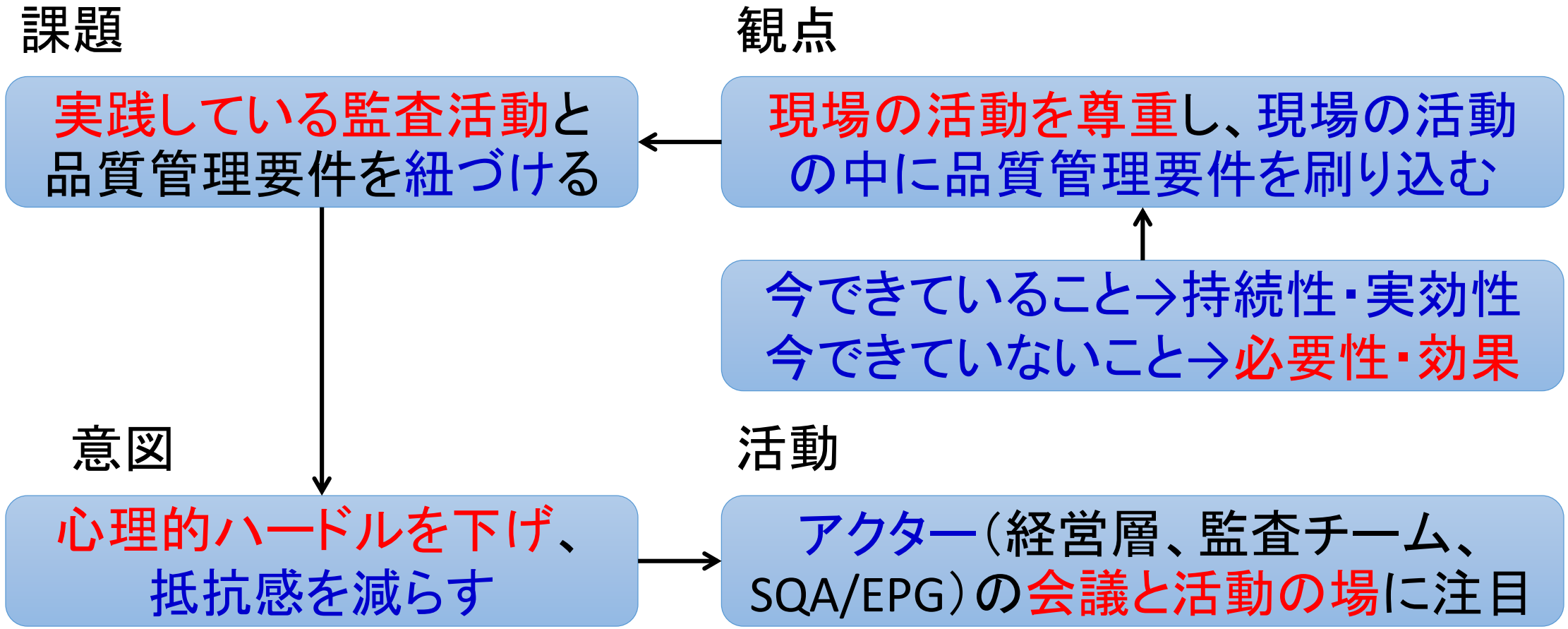
4. 改善策を導き出した経緯1/4



参考4.1.実際に作成した関係図
【経済産業省情報セキュリティ監査サービス審査登録制度】



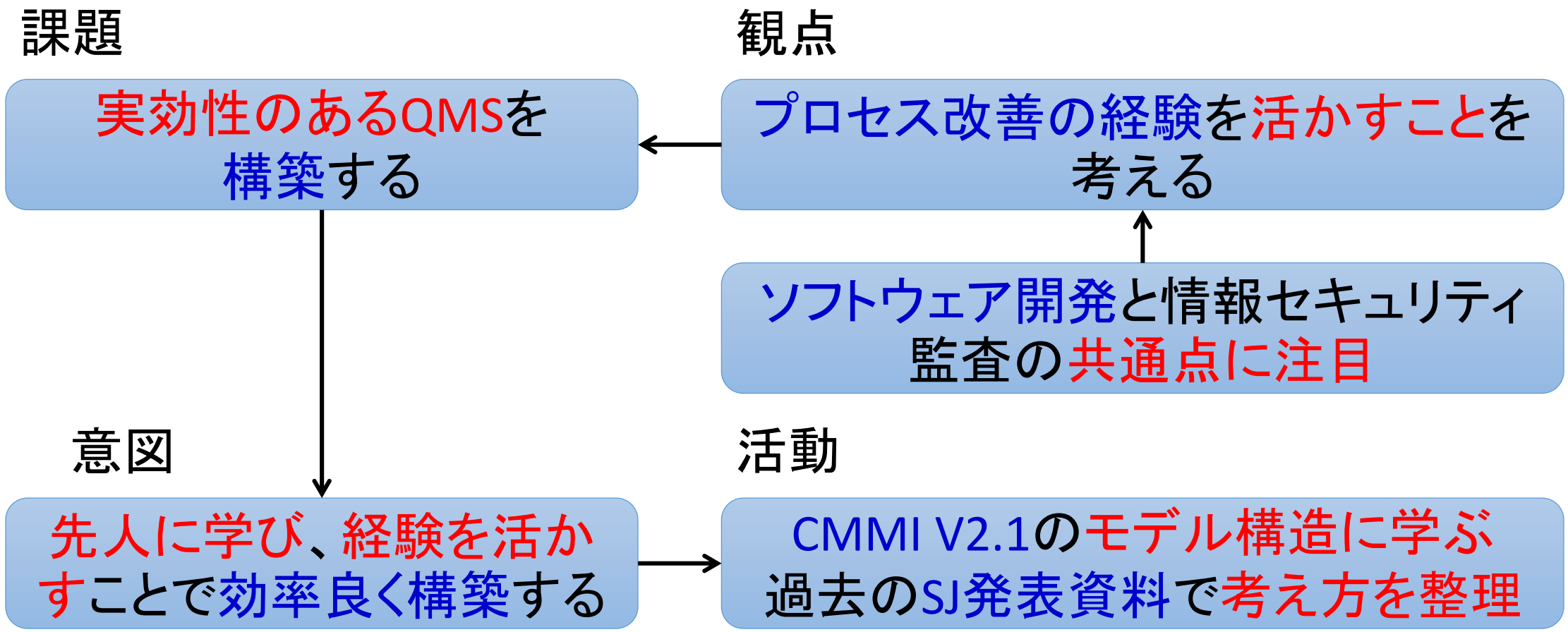
4. 改善策を導き出した経緯2/4



参考4.2. アクターと会議・活動の場

アクター	会議・活動の場			
経営層	事業計画	監視（月例会）	教育（OJT）	管理（レビュー）
監査チーム	受注（提案）	計画（キックオフ）	実施（監査）	フォローアップ
SQA/EPG（相当）	受領物管理（ISMS）	品質管理（レビュー）	進捗管理（月例会）	成果物管理（インフラ）

4. 改善策を導き出した経緯3/4



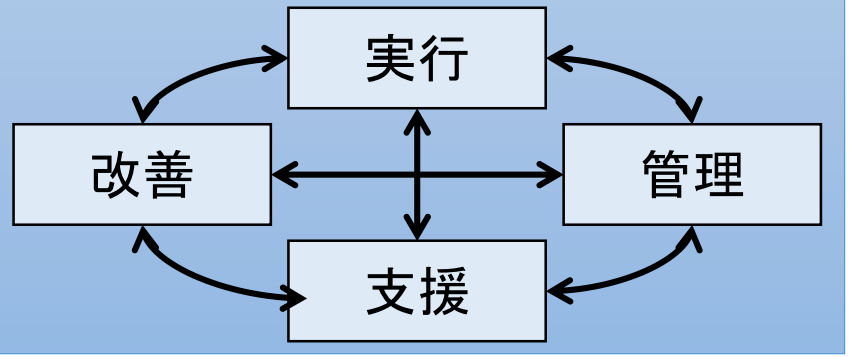
参考4.3. 学びと考えの整理

CMMI V2.1からの学び

モデル構造と構成要素

プロセス領域	プラクティス グループ
プラクティス	参考の要素

区分と能力領域



SJ発表から考え方の整理

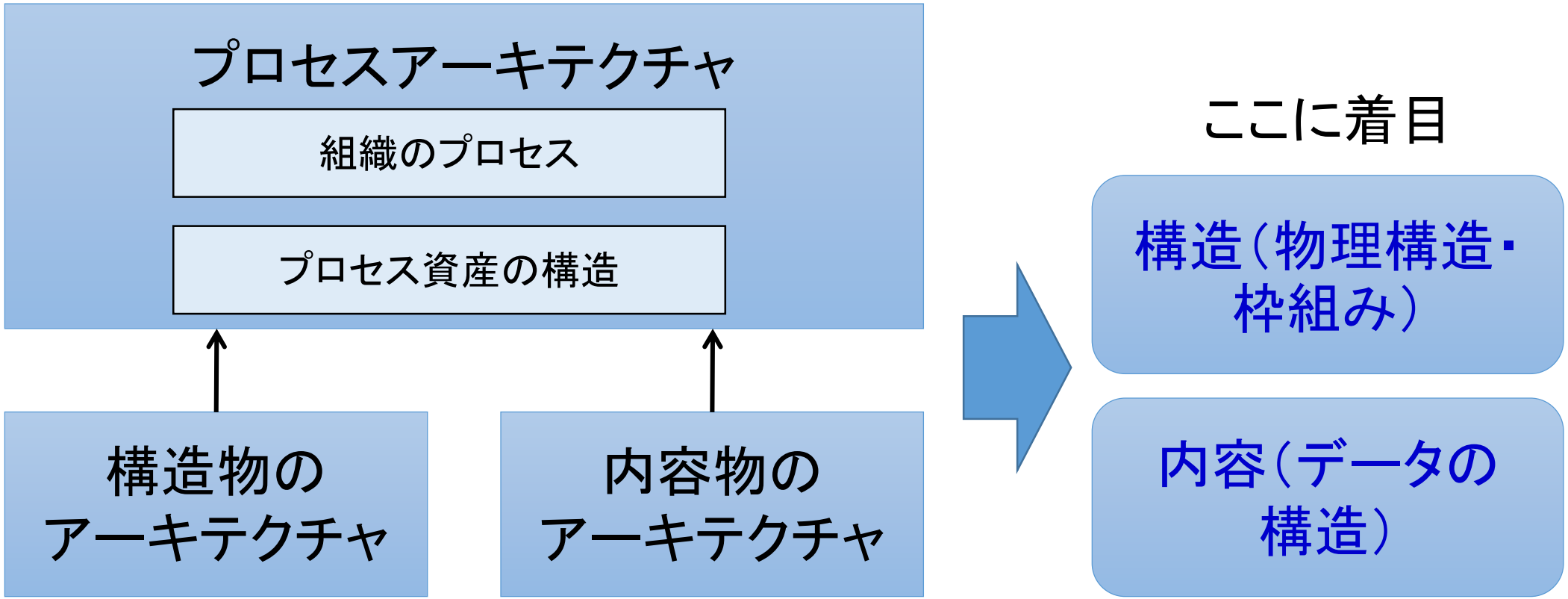
大型プロジェクト成功のツボ（2008）
→「見える化」と「場」の重要性

セルフ監査のススメ（2010）
→現場主体の活動を推進

全社活動によるプロセスの再改善・大改善（2013）
→プロセスの体系化・再構築

4. 改善策を導き出した経緯4/4

- 理事の承認を得るにはQMS構築のエッセンスが重要
  →CMMI V2.1の「プロセスアーキテクチャ」がヒントに



5. 改善策の内容

- プロセスアーキテクチャの構成を考案、承認後、そのままQMSに転用を図ると共に、最終成果物の構成を意識

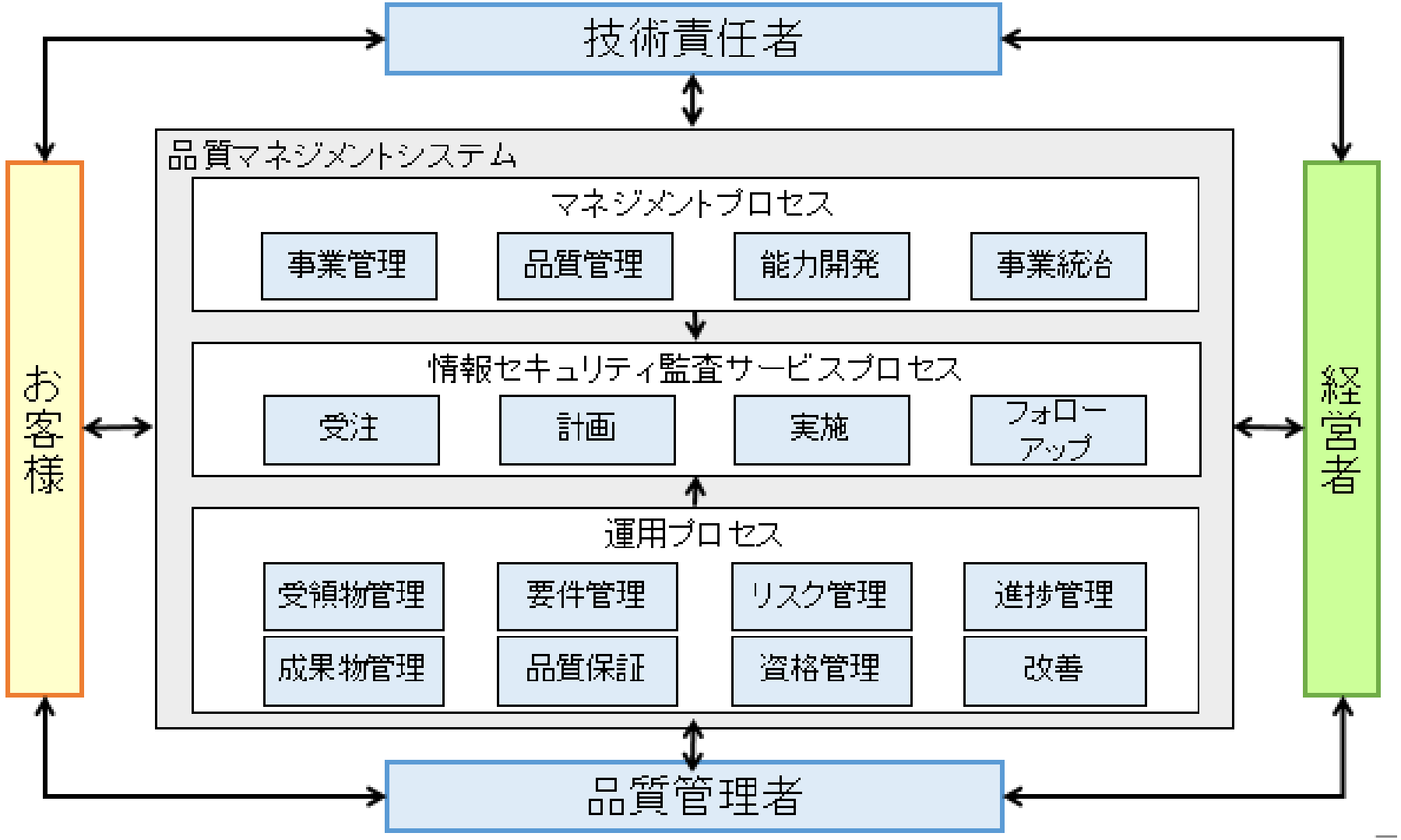
理事の観点	プロセスアーキテクチャ
(1)何を説明したいのか	(1)目的、目標
(2)何のためにやるのか	(2)背景、前提条件
(3)どんなものを作るのか	(3)全体像(構造)
(4)実行可能な内容か	(4)プロセス概要(内容)
(5)基準は満たせるのか	(5)品質への期待(基準)とのマッピング
(6)どのような成果物か	(6)品質マニュアルの構成

6. 改善策の実現方法

- 各項目に対するアプローチ

項目	アプローチ
(1)目的、目標	実効性のあるQMSを構築することを強調、手段としてプロセスアーキテクチャで説明
(2)背景、前提条件	経済産業省の情報セキュリティ基準適合サービスリストに掲載してもらうために、基準の全体像の図を活用(p.8参考4.1)
(3)全体像(構造)	監査サービスを中心に置き、マネジメントによる事業活動と、SQA/EPGの品質保証/プロセス改善の活動で挟む全体像で表現
(4)プロセス概要(内容)	各プロセスの内容を、プロセスに含まれる活動(プラクティス)と活動の内容(概要)の一覧表で提示
(5)品質への期待(基準)とのマッピング	定義したプロセスが経済産業省の品質への期待を満たしているかどうかを確認するために、マッピングを行い、一覧表を作成
(6)品質マニュアルの構成	簡素な記述、プロセスアーキテクチャの資料(パワーポイント)を転用、見開き20ページ、という具体的な内容を設定

参考6.1. QMSの全体像:アクターの活動をプロセスへ



参考6.2. プロセス概要：今できている→現実的な内容

グループ	プロセス	プラクティス	概要
情報セキュリティ監査サービス	受注	案件識別	公募・提案依頼による情報セキュリティ監査サービス案件の識別
		要件把握	依頼組織、仕様書、規格等による要件の把握
		体制構築	要件、提案期限、要員稼働を踏まえた体制構築
		サービス提案	サービス内容を決定し、提案書を作成、承認後提案
	計画	受注内容確認	情報セキュリティ監査サービスの受注内容の確認
		計画書策定	情報セキュリティ監査サービスの計画を策定、承認
		顧客合意	計画内容、顧客側準備内容、制限事項等を説明、顧客との合意
	実施	文書レビュー	関連する文書をレビューし、所見を作成、顧客に確認
		事前確認	事前確認項目の質問票を作成、顧客の承認を得て、書面回答受領
		インタビュー実施	インタビュー内容を作成、顧客の承認を得てインタビューを実施
		報告書作成	監査結果を踏まえて報告書を作成、内部承認後、顧客に確認
		報告会実施	監査結果を報告、納品物確認、納品、顧客検収
	フォローアップ	ニーズ収集	過去の記録、公募等からフォローアップ監査のニーズを収集
		フォローアップ判断	フォローアップ監査に要否を判断、要であれば受注活動へ

参考6.3. 基準とのマッピング：トレーサビリティマトリクス

凡例　◎：基本となる規定
　　○：実施、適用

	概要			マネジメント				情報セ監査サービス				運用							
経済産業省品質期待	品質方針	体制	サービス	事業管理	品質管理	能力開発	事業統治	受注	計画	実施	フォロー	受領物	要件管理	リスク	進捗管理	成果物	品質保証	資格管理	改善
品質管理者のレビュー事項					○									○			◎		○
受注基準							◎	○											
顧客へのサービス内容の説明			◎					○	○										
顧客のニーズの把握								○	○		○		◎						
監査チームの編成			○			○	◎	○									○	○	
監査人の行動指針			○				◎	○	○	○	○						○		
サービスの実施方法								○	◎								○		
サービスの進捗管理								○	○	○	○				◎				
顧客から提供された情報の管理							○					◎							
顧客からの要求、意見、クレーム等への対応				○	○										○		◎		○
アウトプットの管理								○	○	○	○					◎			○

参考6.4. 品質マニュアルの構成：パンフレットをイメージ

- 簡素な記述とし、見開き20ページ（パワーポイント2in1、40スライド）で構成する
  - 顧客に訴求できる体裁を目指す

ページ	内容	ページ	内容
1表紙	タイトル、発行日、承認者、目次	20裏表紙	変更履歴
2	品質方針、品質保証体制図	3	情報セキュリティ管理サービスの定義、種別
4	【マネジメント】 事業管理、品質管理	5	リスクに応じた体制、承認基準
6	【マネジメント】 能力開発、事業統治	7	独立性基準、倫理規定、行動指針
8	【情報セ監査サービス】 受注、計画	9	【情報セ監査サービス】 実施、フォローアップ
10	【運用】 受領物管理、顧客提供情報の管理	11	【運用】 要件管理、顧客ニーズの把握
12	【運用】 リスク管理、進捗管理	13	【運用】 成果物管理、品質保証
14	【運用】 資格管理、保有資格（個人）	15	【運用】 改善、組織資産
16	QMS全体像、情報セ監査サービスの計画要件	17	経済産業省の登録制度、QMSと要件のマッピング
18	情報セキュリティ基本方針、推進体制	19	ISMSマニュアル目次、セキュリティ関連資格（組織）

左右のページで見開きとなる

7. 改善による変化や効果1/4

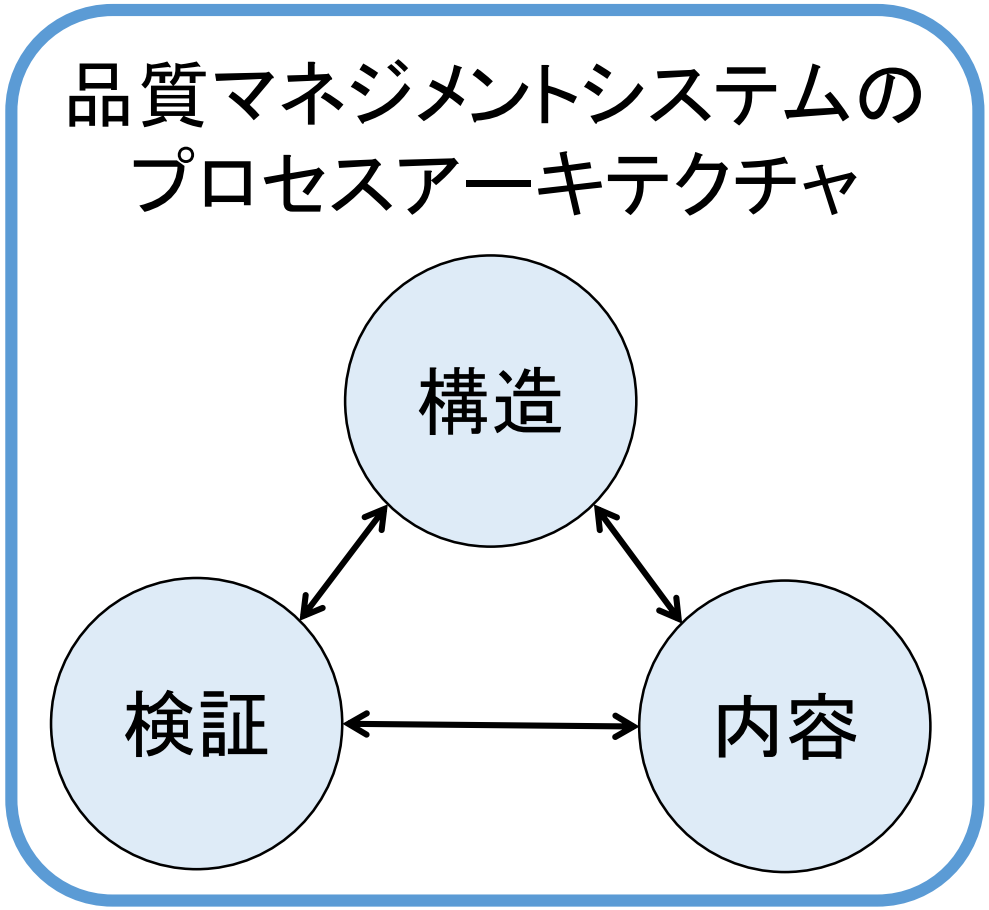
妥当性確認と変更が比較的容易

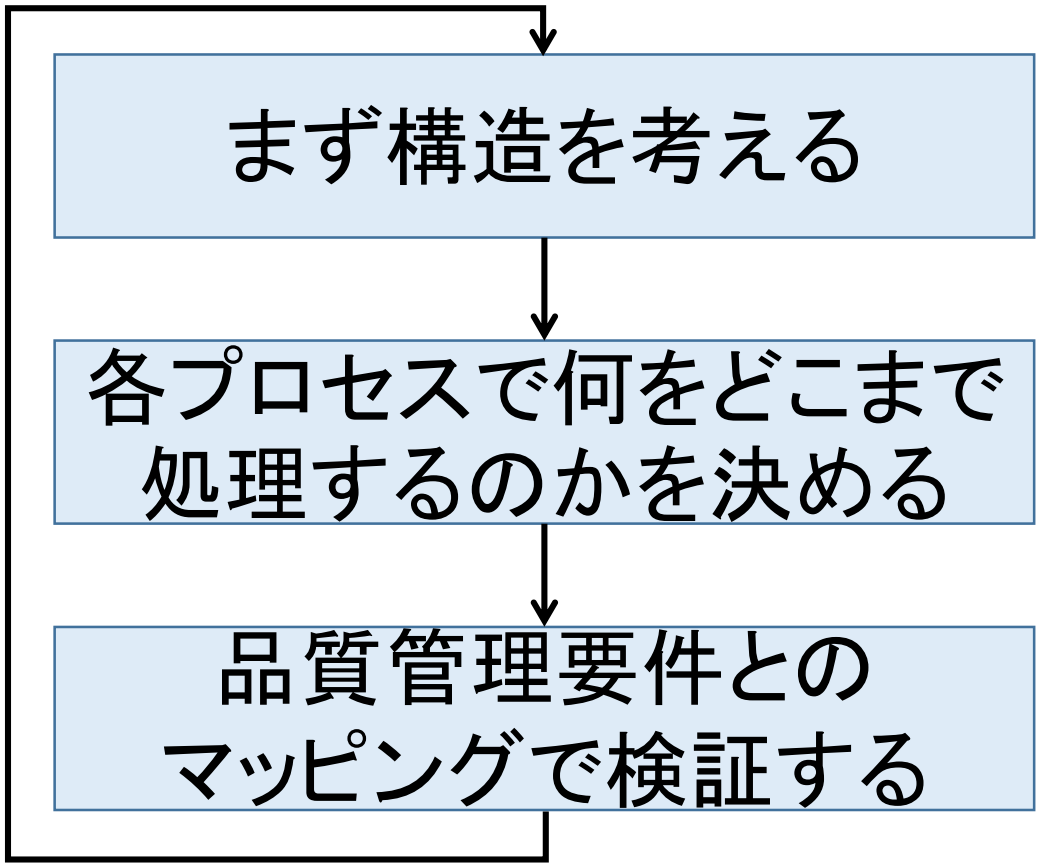
プロセスの「構造」と「内容」を示す
→理事が素早く理解し承認

プロセスアーキテクチャからQMSへ効率良く構築

7. 改善による変化や効果2/4

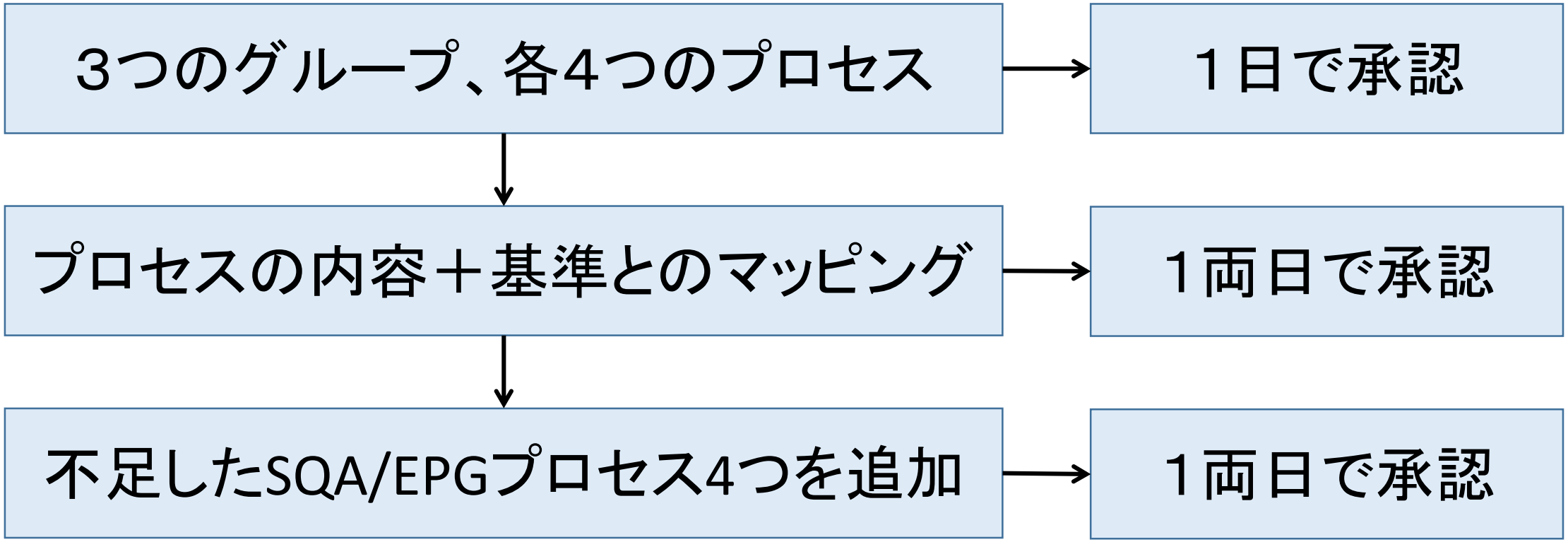
- 妥当性確認と変更が比較的容易





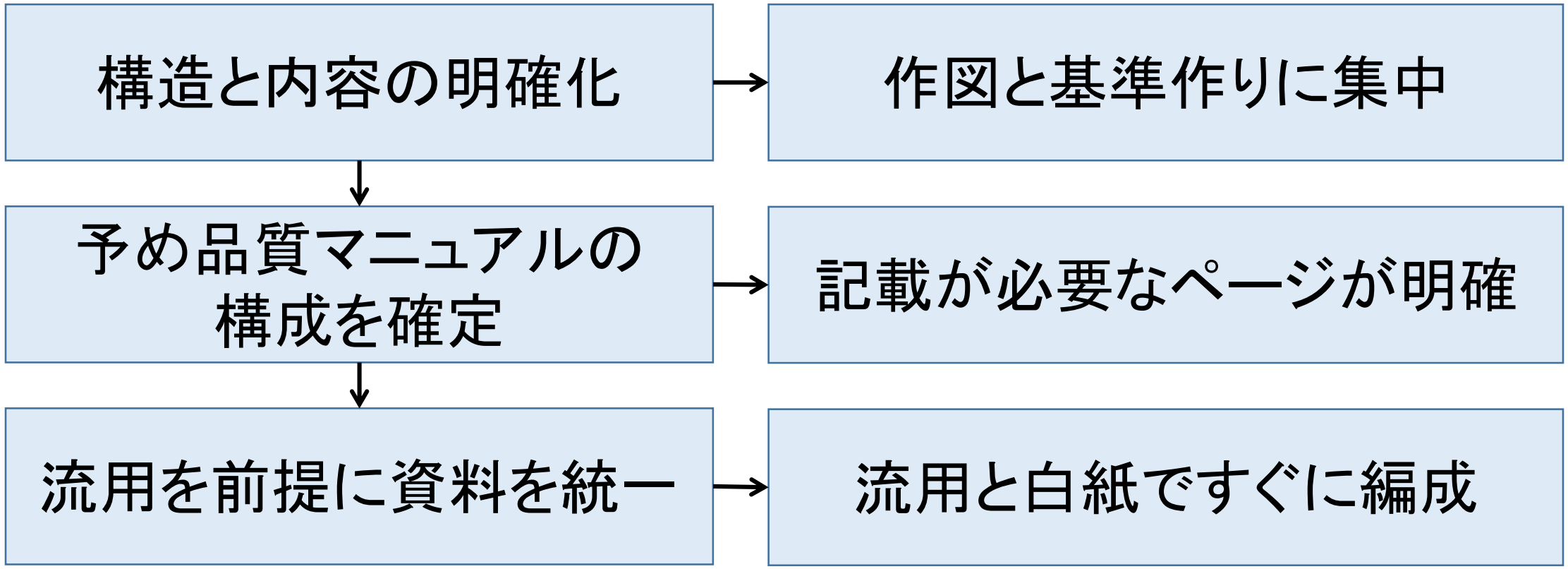
7. 改善による変化や効果3/4

- プロセスの「構造」と「内容」を示す→理事が素早く理解し承認



7. 改善による変化や効果4/4

- プロセスアーキテクチャからQMSへ効率良く構築



2週間、10時間で、40スライド、20ページを作成

8. 改善活動の妥当性確認

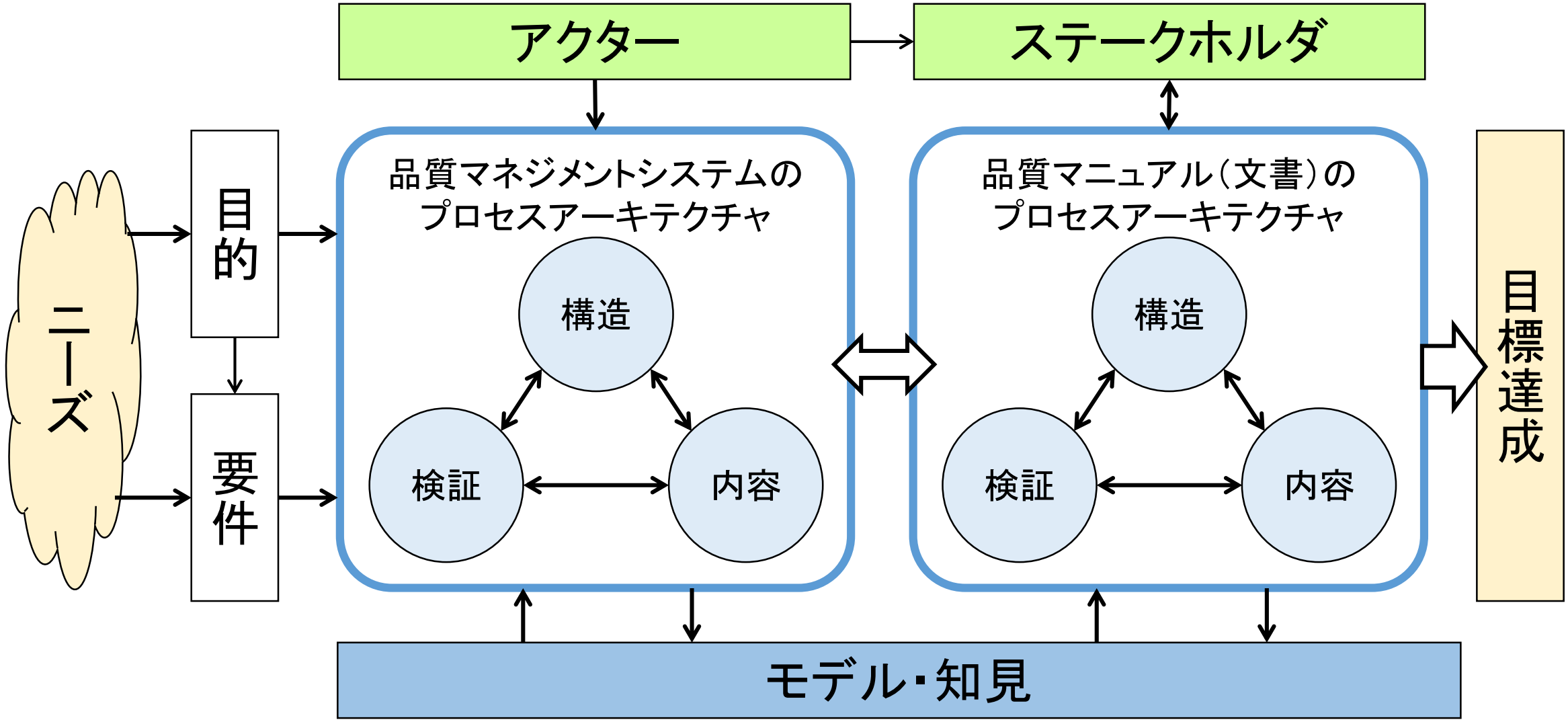
- 経済産業省の審査に合格、6/11付でセキュリティサービス基準適合サービスリストに掲載
- 行政機関の入札要件を満たし、情報セキュリティ監査を受注

情報セキュリティ監査サービス　　**掲載日：2020年6月11日**

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備・運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与え又は助言を行うサービスをいう。（経済産業省「情報セキュリティサービス基準」より）

サービス名称	事業者 ①名称 ②所在地	登録年月日	有効期限	審査登録機関名
情報セキュリティ監査サービス	①特定非営利活動法人ITプロ技術者機構 ②埼玉県 さいたま市 浦和区皇山町31番2号	2020/6/12	2022/6/11	日本セキュリティ監査協会 (JASA)

9. まとめ：プロセスアーキテクチャの活用の有用性



SJ2020 ID:5

ゼロから作る品質マネジメントシステム（QMS）

~QMS構築の効率性を高めたプロセスアーキテクチャのエッセンス~

Thankyou

参考情報

[1] 情報セキュリティサービス審査登録制度【経済産業省】
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

[2] 情報セキュリティサービス基準【経済産業省】
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf

[3] 情報セキュリティサービスに関する審査登録機関基準について【経済産業省】
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/tourokukizyun.pdf

[4] 情報セキュリティサービス基準適合サービスリスト【情報処理推進機構】
https://www.ipa.go.jp/security/it-service/service_list.html

CMMIの権利に関する記述

- CMMI V2.1の権利は、CMMI Instituteに帰属します。
- 参考文献
  - CMMI V2.0モデル早わかり
- スライド中のCMMI V2.1からの学び、モデル構造と構成要素、区分と能力領域は、記載内容を伝えるために発表者が要点を抽出したものです。詳細は原本でご確認ください。