IPA Software Engineering Center
Information-technology Promotion Agency, Japan

2012 Japan IT Week 春 ビッグサイト 内
第15回 組込みシステム開発技術展 ESEC

ソフトウェア品質監査制度(仮称)
～制度概要と審査基準の考え方～

2012年5月10日

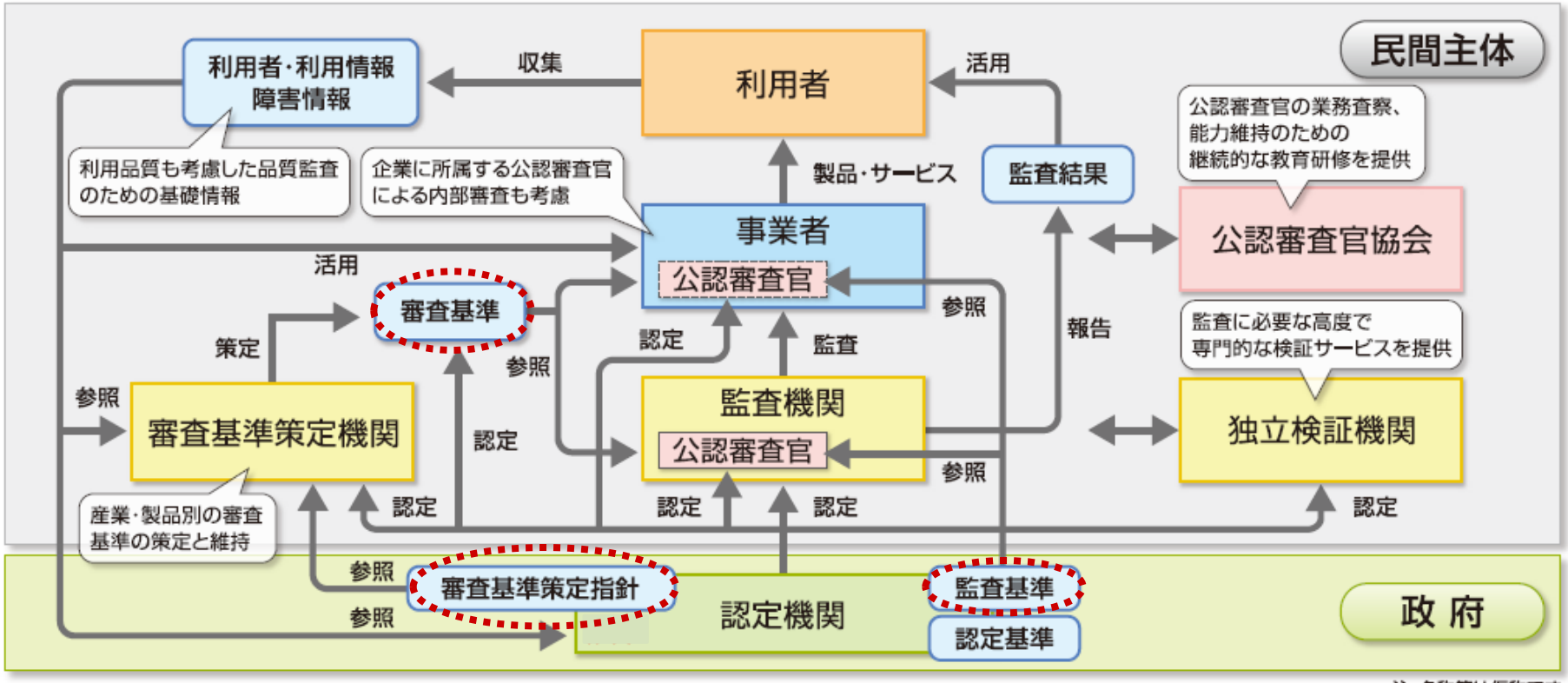
独立行政法人情報処理推進機構
技術本部ソフトウェア・エンジニアリング・センター
統合系プロジェクト 研究員　伊藤 克己

© 2012, Information-technology Promotion Agency, Japan

制度フレームワーク（案）

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

ソフトウェア品質監査制度（仮称）の枠組み
産業・製品分野別への対応と内部監査を考慮したフレームワーク

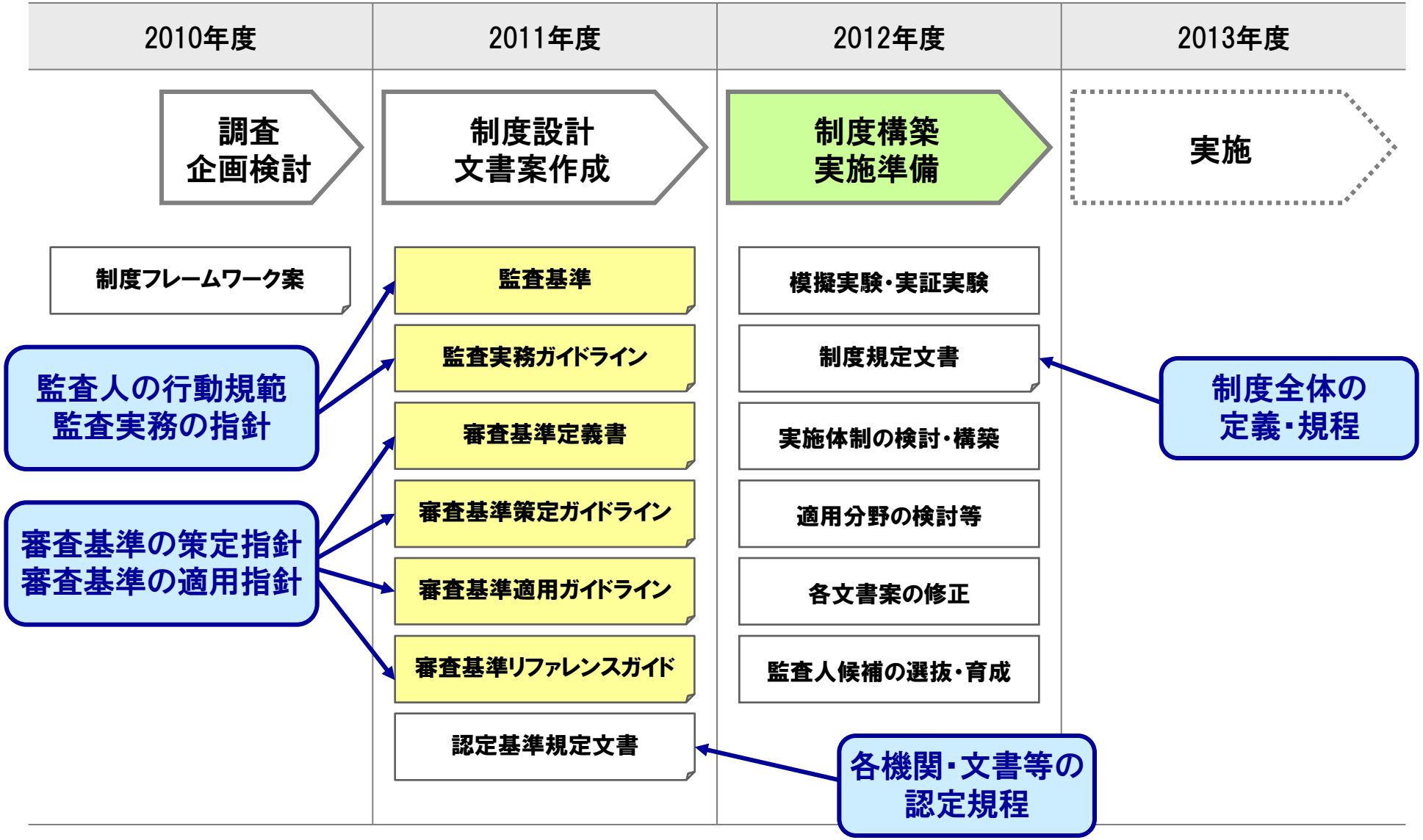


注：名称等は仮称です

© 2012, Information-technology Promotion Agency, Japan

これまでの振り返りと現在、今後

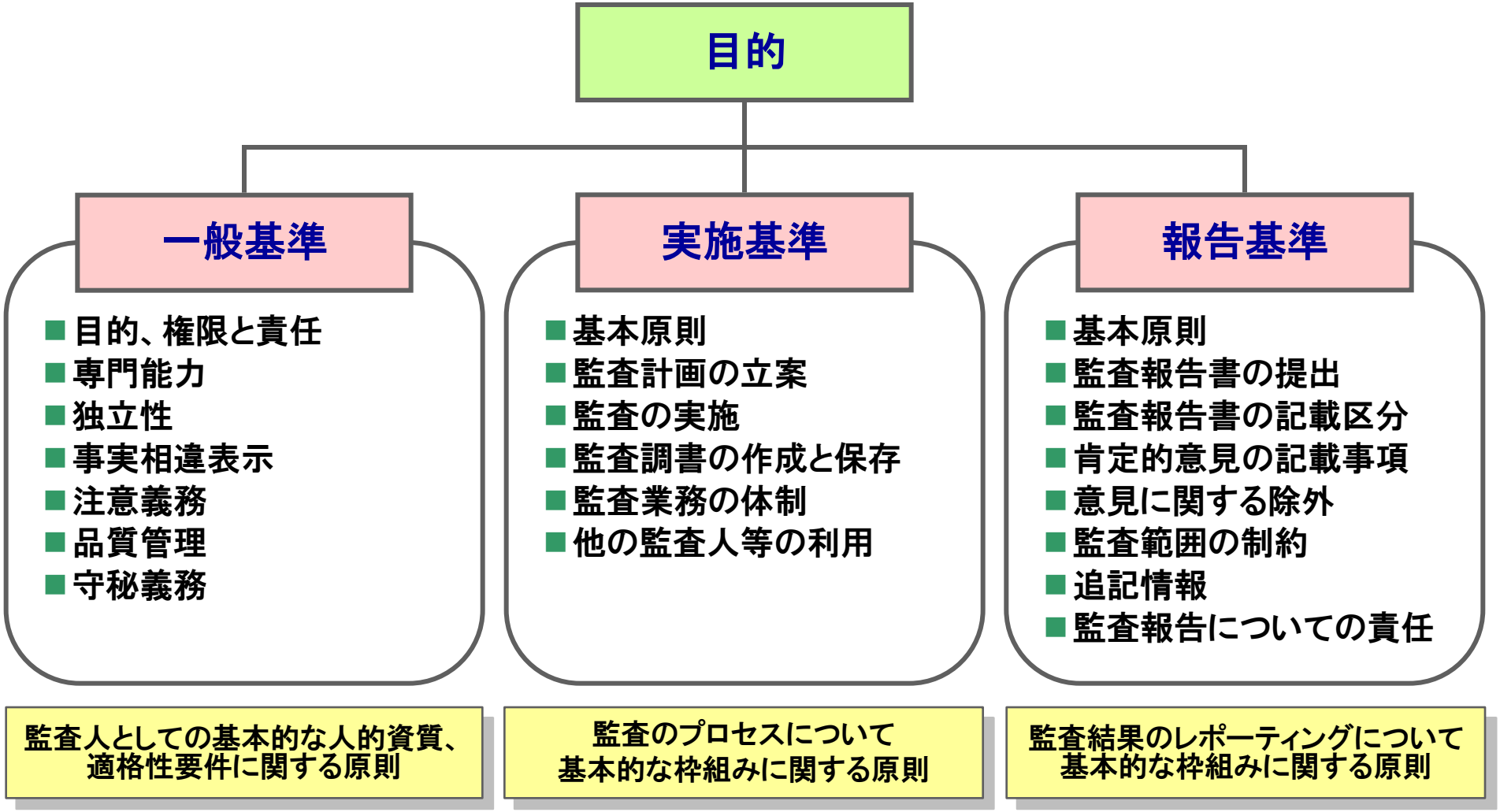
SEC
Software Engineering for Mo·No·Zu·Ku·Ri



© 2012, Information-technology Promotion Agency, Japan

監査基準の構成

監査人が監査を行う場合に遵守しなければならない行動規範を示したもの



© 2012, Information-technology Promotion Agency, Japan

監査実務ガイドラインの構成

監査基準で定める原則の解説や留意事項、監査実務を実施する際の留意事項等を示したもので監査基準のような一般的な規定ではなく、詳細な指針を示したもの。

- はじめに
  - 本ガイドラインの目的、「ソフトウェア品質監査制度（仮称）」の概要
- 本監査業務の構成要素と定義
  - 監査人、監査責任者、職業的専門家、監査人の職業倫理と誠実性、事業責任者、被監査先、監査の依頼者、想定利用者、独立検証機関、監査機関、主題及び主題情報、主題を評価又は測定するための規準、監査レベル、監査リスク、十分かつ適切な証拠、監査報告書
- 監査業務の契約締結に関する留意点
  - 監査実施の前提、受嘱の要件、受嘱における留意事項、契約書等に盛り込むことが想定される項目、合意した実施条件の変更
- 独立性の担保
  - 独立性の原則、独立性に対する脅威への適切な処置等
- リスク評価
  - 監査リスクとは、リスク評価手続、法的リスク及び社会的リスク、評価したリスクへの対応
- 監査上の重要性
- 監査計画の立案
  - 監査計画策定の留意事項、計画の修正、主題及び業務環境の理解とリスク評価、想定される製品・サービスの利用者、利用状況及び利用目的への考慮、監査計画で定めるべき事項
- 監査手続の実施
  - 職業的専門家としての懐疑心、監査レベルと監査手続、十分かつ適切な監査証拠の入手、監査証拠として利用する情報、他の監査人等の利用
- 監査調書の作成
  - 監査調書の作成
- 事業責任者の記述書、確認書の入手
  - 事業責任者の記述書の入手、事業責任者の記述書の記載項目、事業責任者確認書の入手、事業責任者確認書の記載項目、事業責任者確認書の陳述の評価
- 後発事象
- 監査報告書の記載
  - 留意事項、報告書の種類、監査報告書作成上の留意点
- 監査品質管理
  - 監査品質管理の方針、定めるべき監査品質管理に関する方針と手続、監査品質管理に関する責任、職業倫理及び独立性、監査契約の締結、監査人の採用・教育・訓練、評価及び選任、監査業務の管理、監査品質管理システムのモニタリング
- 文例
  - 監査報告書の文例、事業責任者の記述書文例、事業責任者の確認書文例

© 2012, Information-technology Promotion Agency, Japan

審査基準規定文書の構成

審査基準定義書

- 内容
  - 審査基準の定義と原則、審査基準に記載すべき項目とその考え方、判定の方法等を規定
- 利用者・利用シーン
  - 審査基準策定機関が審査基準を策定する際に参照

審査基準策定ガイドライン

- 内容
  - 審査基準の具体的な策定方法を規定
- 利用者・利用シーン
  - 審査基準策定機関が審査基準を策定する際に参照
  - 監査を受ける事業者(ベンダ)が審査基準の意図を理解するために参照

審査基準策定機関

審査基準（書）

審査基準適用ガイドライン

- 内容
  - 審査基準の適用方法(使い方)を規定
- 利用者・利用シーン
  - 監査人が審査基準を用いて製品・サービスの監査を行う際に参照

監査人(公認審査官)

審査基準リファレンスモデル

- 内容
  - 審査基準定義書と審査基準策定ガイドラインを用いて策定した審査基準の見本(事例)
- 利用者・利用シーン
  - 制度に関わる全ての関係者が参照

© 2012, Information-technology Promotion Agency, Japan

審査基準策定指針の検討における視点

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

品質ライフサイクル

- 開発プロセスのみをスコープとするのではなく、企画から廃却に至る製品・サービスの全ライフサイクルを対象とする

メタフレームワーク

- 審査基準の原理・原則を明確化し、審査基準策定機関が網羅性・妥当性をもって審査基準を策定できるように規定する

アウトカムデザイン

- ソフトウェア品質監査制度を利用することでの事業者と利用者の価値に留意する

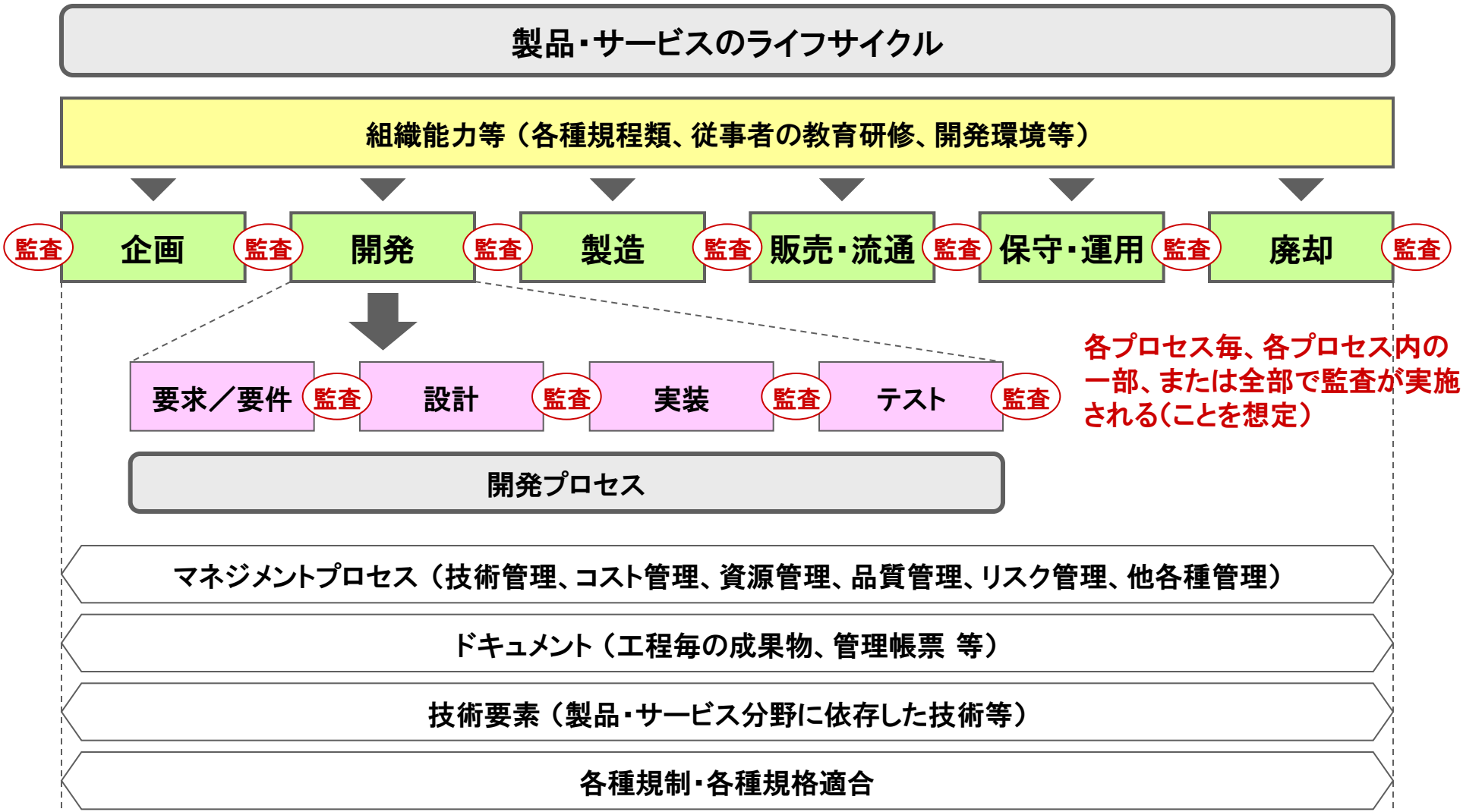
審査基準リファレンスモデル

- 監査人、審査基準策定機関、事業者等全てのステークホルダが活用できるサンプルを作成する

© 2012, Information-technology Promotion Agency, Japan

本制度が対象とする範囲：品質ライフサイクル

SEC
Software Engineering for Mo·No·Zu·Ku·Ri



© 2012, Information-technology Promotion Agency, Japan

メタフレームワークの概要

メタフレームワーク＝審査基準の原理・原則（一般原則）

基本的な思想

- **品質ゴールに対して品質懸念点を低減させ、残存品質懸念点を許容範囲内に収める**
- メタフレームワークに従うことで品質懸念点を低減させる過程で検討すべき事項を、高い網羅性をもって列挙することができる
  - 審査項目の半ば機械的な策定が可能
  - 策定される審査基準に対して一定レベルの品質保証が可能

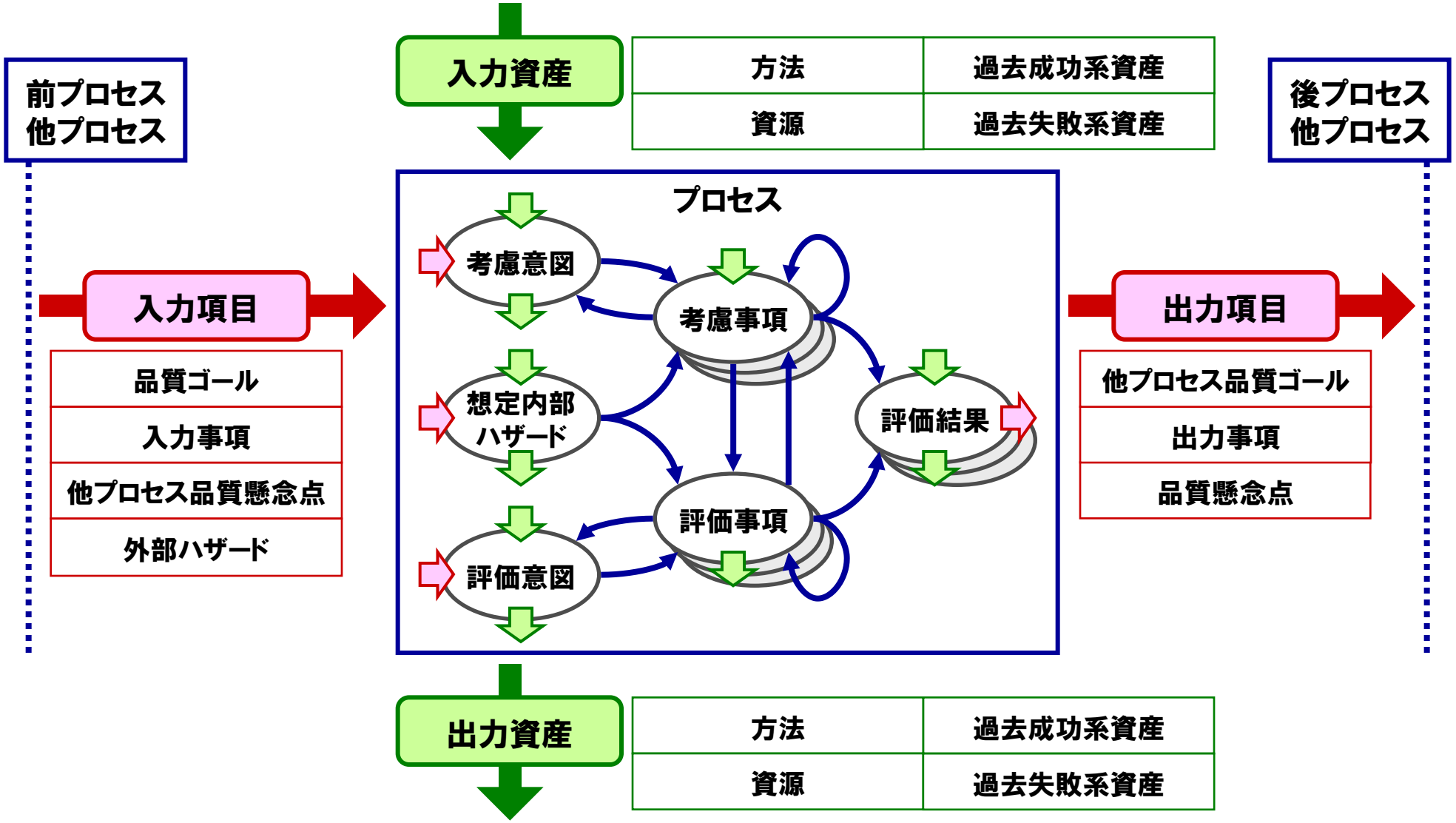
構成

- **メタフレームプロセス**
  - 1つのプロセスについてのメタ要件
  - 以下の5つの要素で構成される
    入力項目、プロセス項目、
    出力項目、入力資産、出力資産
- **メタ審査基準要件**
  - 一般化された審査基準要件
  - メタフレームプロセスの項目内、項目間で満たすべき以下の基本性質
    品質懸念点の払拭性、完備性、
    追跡性、俯瞰性、フィードバック性
    を抽象化し規定したもの

© 2012, Information-technology Promotion Agency, Japan

メタフレームプロセスの構造：プロセス内構造

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri



© 2012, Information-technology Promotion Agency, Japan

メタ審査基準要件の全体像

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

構成要素		払拭性	完備性	俯瞰性	（要素間の）追跡性・俯瞰性・フィードバック性				
					入力項目	入力資産	プロセス項目	出力項目	出力資産
入力項目	・品質ゴール ・入力事項 ・他工程品質懸念点 ・外部ハザード		○	○			追跡性 俯瞰性	フィードバック性	フィードバック性
入力資産	・方法 ・資源 ・過去成功系資産 ・過去失敗系資産		○	○			追跡性 俯瞰性	フィードバック性	フィードバック性
プロセス項目	・考慮意図 ・想定内部ハザード ・考慮事項 ・評価意図 ・評価事項 ・評価結果		○	○	追跡性 俯瞰性	追跡性 俯瞰性	追跡性 俯瞰性	追跡性 俯瞰性	追跡性 俯瞰性
出力項目	・他工程品質ゴール ・出力事項		○	○	フィードバック性	フィードバック性	追跡性 俯瞰性		
	・品質懸念点	○							
出力資産	・方法 ・資源 ・過去成功系資産 ・過去失敗系資産			○	フィードバック性	フィードバック性	追跡性 俯瞰性		

© 2012, Information-technology Promotion Agency, Japan

審査基準(書)の構成要素

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

要素のタイプ	文書の構成要素		区分	説明
前置き	表紙(文書名等)		必須	審査基準書の名称等
	改訂履歴		必須	改訂履歴
	目次		必須	目次
	序論		必須	序論
	目的		必須	審査基準の目的
	前提知識		任意	以下の章を読むために必要な知識
規定事項	一般規定	適用範囲	必須	審査基準の適用範囲
		引用規格・関連規格	必須	引用または関連する規格等
	技術規定	審査基準	必須	審査基準の本体
	その他規定	審査基準書のメンテナンス等	必須	審査基準書の更新に関する規定
補足	用語と定義		任意	用語とその定義
	記号及び略語		任意	記号と略語の意味
	付属書		任意	関連する参考情報等
	参考文献		任意	参考となる文献の一覧
	索引		必須	文書の要素への索引

© 2012, Information-technology Promotion Agency, Japan

審査基準の階層構造（例：企画品質）

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

第1階層	第2階層	第3階層	審査項目	確認方法	判定基準	説明
企画品質	企画計画	企画作業の要素特定				企画プロセスの作業要素を明らかにし、その実施計画を作成しているか審査する。
		製品開発の要求事項の抽出				マーケットリサーチを行うにあたってその範囲が特定できるようなターゲットの方向性を設定しているか審査する。
		利用者の特定				利用者とその範囲を特定しているか審査する。
	マーケットリサーチ	市場動向等の抽出				製品ターゲットに関わる分野の市場動向、事業環境を十分に実施しているか審査する。
		影響要因の特定				社会環境等が、製品の品質や設計に与える要因を検討しているか審査する。
		事故情報・評価情報の影響検討				同種製品の事故情報や評価情報から、製品に与える影響要因を検討しているか審査する。
	品質目標の特定	用途・利用環境等の特定				用途および利用状況とその範囲を特定しているか審査する。
		利用者の要求品質の特定				特定した用途の範囲で、要求する品質やユーザビリティを洗出し、特定しているか審査する。
		品質特性の目標設定				利用者の要求品質を達成するために必要なシステム/ソフトウェアの品質目標がステークホルダー間で合意されているか審査する。
		品質目標達成のためのシステム化				品質特性目標を達成するためのシステム化構想を行なっているか審査する。
	品質保証計画	品質目標を達成するための実施計画作成				特定された品質を達成するために必要な計画を策定しているか審査する。
		品質目標を達成するための実施計画の評価				策定した計画が、コスト制約、スケジュール制約を考慮して実現可能か評価していることを審査する。

製品・サービスの分野に応じて審査基準策定機関により具体的かつ詳細に策定される。

© 2012, Information-technology Promotion Agency, Japan

審査基準の策定方法

① 当該製品・サービス分野で既に行われている規格認証・審査基準そのまま使用する

② 類似製品・サービス分野の規格認証・審査基準における審査項目を流用するが審査方法は詳細化する

③ 類似製品・サービス分野の規格認証・審査基準における審査項目の一部を修整して使用する

④ 当該分野、類似分野に適当な審査基準がないため審査基準策定機関が新たに審査基準を策定する

© 2012, Information-technology Promotion Agency, Japan

製品・サービスの分野に応じた監査方法（TBD）

SEC
Software Engineering for Mo・No・Zu・Ku・Ri

産業・経済への影響の範囲	
4	我が国の産業への広範囲な影響
3	当該産業に限定された影響 当該企業以外の同一・類似産業のへの影響
2	当該企業に限定された影響 当該製品・サービス以外の他事業への影響
1	当該製品・サービス事業に限定された影響
0	影響はない／ほとんど影響はない

利用者・国民への影響の範囲・程度	
4	当該利用者ならびに当該利用者以外への重大な影響（代替手段による影響軽減が困難な影響） 国民への広範囲で重大な影響
3	当該利用者への重大な影響に加え、当該利用者以外への軽微な影響（代替手段による影響軽減が容易な影響）
2	当該利用者に限定された重大な影響
1	当該利用者に限定された軽微な影響
0	影響はない／ほとんど影響はない

※2011年度中間報告より抜粋

監査レベルと対応した監査内容			
監査レベル	審査対象項目	監査方法	独立検証
4	全項目	網羅監査（全件監査）	必須
3	重要項目	網羅監査（全件監査）	必須
3	その他の全項目	抜取監査（サンプル監査）	任意
2	全項目	抜取監査（サンプル監査）	任意
1	重要項目	抜取監査（サンプル監査）	任意
0	非対象	非対象	非対象

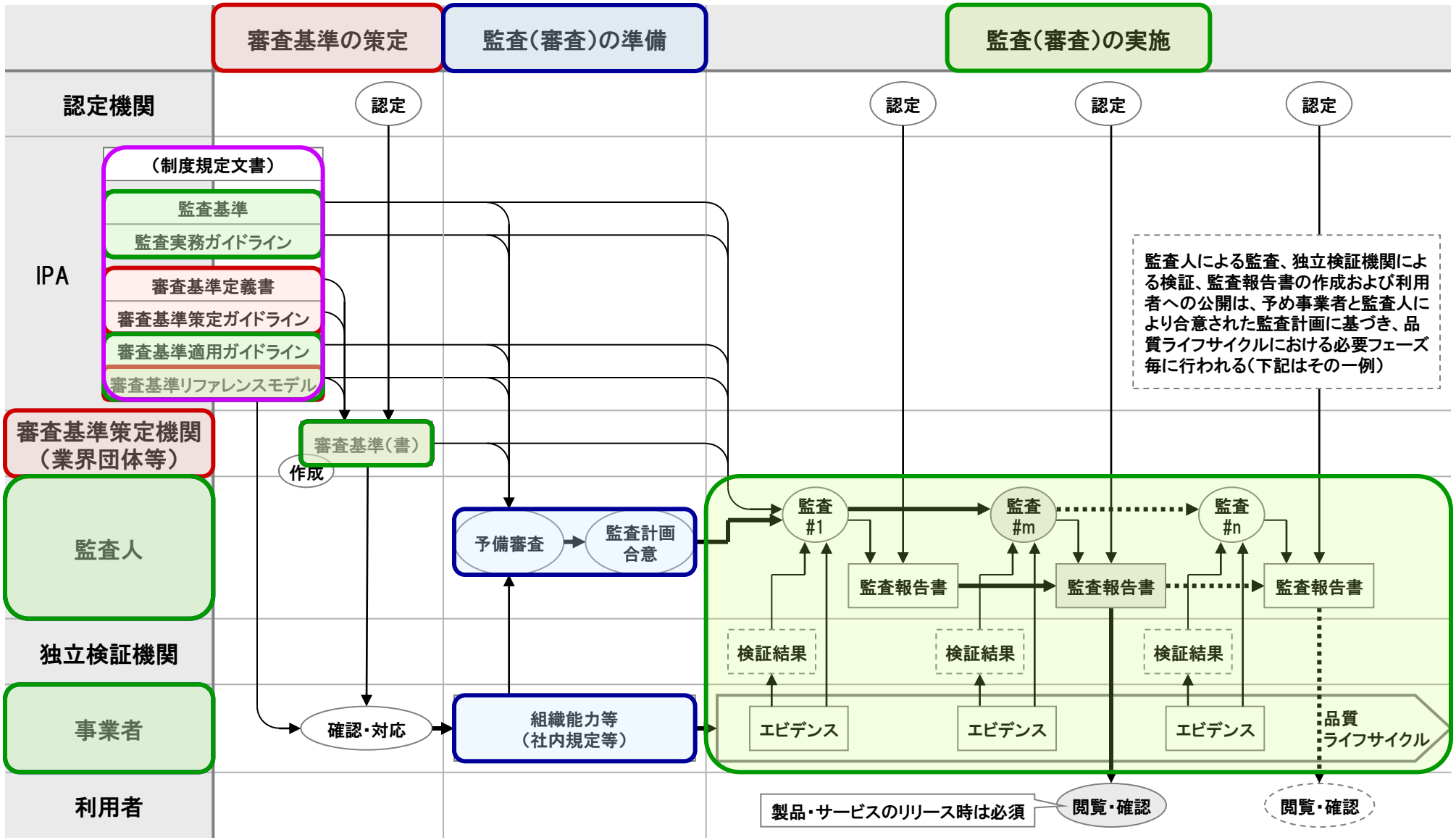
- 製品・サービス毎に要求される安心・安全の度合いに応じて、監査のレベルを設定。
- 設定した監査のレベルに応じて、対象とする審査項目や監査方法等が決定される（予定）。

制度文書に考え方を、審査基準規定文書で利用方法をそれぞれ明確化する予定

© 2012, Information-technology Promotion Agency, Japan

ソフトウェア品質監査制度（仮称）

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri



© 2012, Information-technology Promotion Agency, Japan

実施中の模擬実験

- パッケージソフトウェア品質認証制度のフィージビリティ評価及び監査制度導入によるコスト評価
- 独立検証機関による形式手法を用いた第三者検証のコスト評価
- ICカードを用いた社会情報基盤システムにおける、安全性とセキュリティの同時認証に関する実証実験
- CO2無線測定センサーを対象とした監査レベル別コスト評価
- ソフトウェア品質監査制度（仮称）導入に伴い発生する開発工程負荷の評価・分析
- カーナビゲーションシステムにおける利用品質（安全性）に対する監査内容の提案とコスト算出
- 既製システムをソフトウェア品質監査制度（仮称）に適用する場合のフィージビリティスタディ
- 製品利用情報を分類する際に係るコスト評価
- 製品マニュアルと製品テスト結果のトレーサビリティ確保に係るコスト評価
- 車載システム開発時に使用するソフトウェアツールに対してISO 26262の安全要求事項を満たす為に必要な具体的な作業項目の考察
- モデルベース開発ツールを活用した際のフィージビリティの効果検証
- トレーサビリティ確保におけるソフト開発データからの効果検証

9団体・12プロジェクトの模擬実験を実施中

© 2012, Information-technology Promotion Agency, Japan

模擬実験の分布

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

大分類	実験の種類	小分類	実験で焦点を当てる本制度の特色	実施数
ア	フィージビリティ評価	A	分野/企業横断的なシステムや製品	1
		B	市販のパッケージソフトウェアやフリーソフトウェアを用いたシステムや製品	1
		C	その他(A,B以外、制度フレームワーク案から読み取れるもの)	1
イ	コスト評価	A	独立検証機関の、監査や審査への参画の許容	2
		B	利用品質の確認や向上への、利用者情報や利用情報の活用	3
		C	監査の指摘事項反映の影響を抑える、開発と監査の並行実施(同期監査)	0
		D	機密情報漏洩リスク低減のための、開発者内部と外部の審査官の間の連携	0
		E	その他(A～D以外、制度フレームワーク案から読み取れるもの)	5
ウ	ギャップ分析	A	既存の認証制度や監査制度を補完	2
		B	その他(A以外、制度フレームワーク案から読み取れるもの)	0
エ	その他	-	制度フレームワーク案から読み取れるもの	0

© 2012, Information-technology Promotion Agency, Japan

利用価値のある、よりよい制度にするために
皆様の貴重なご意見・ご質問をお待ちしております。
詳細は、ブース担当の研究員までお願いします。

ご清聴ありがとうございました。

© 2012, Information-technology Promotion Agency, Japan