安心安全なスマートシステム構築を目指すスマートシステム検証技術協会（SVA）の活動について

2016年4月

一般社団法人スマートシステム検証技術協会
理事長　有馬仁志

一般社団法人

スマートシステム検証技術協会

- 名称
  - 一般社団法人スマートシステム検証技術協会
  - **S**mart System **V**erification and Validation Technology **A**ssociation (SVA)
- 設立目的
  - 複数の企業から提供されるシステムが有機的に結合して構成されるスマートシステムの全体システムとしての信頼性、安全性などの利用者が求める品質を第三者が検証するための検証手法・検証技術を確立することにより、安全・安心・快適なスマート社会の実現に資することを目的とする。
- 実施事業
  - スマートシステムの検証手法・検証技術の確立のための事業
  - スマートシステムの検証手法・検証技術の普及・啓発のための事業
  - スマートシステムの検証手法・検証技術の応用に関する事業
- 設立日：2012年6月1日
- 事務局　（株式会社ガイア・システム・ソリューション内）

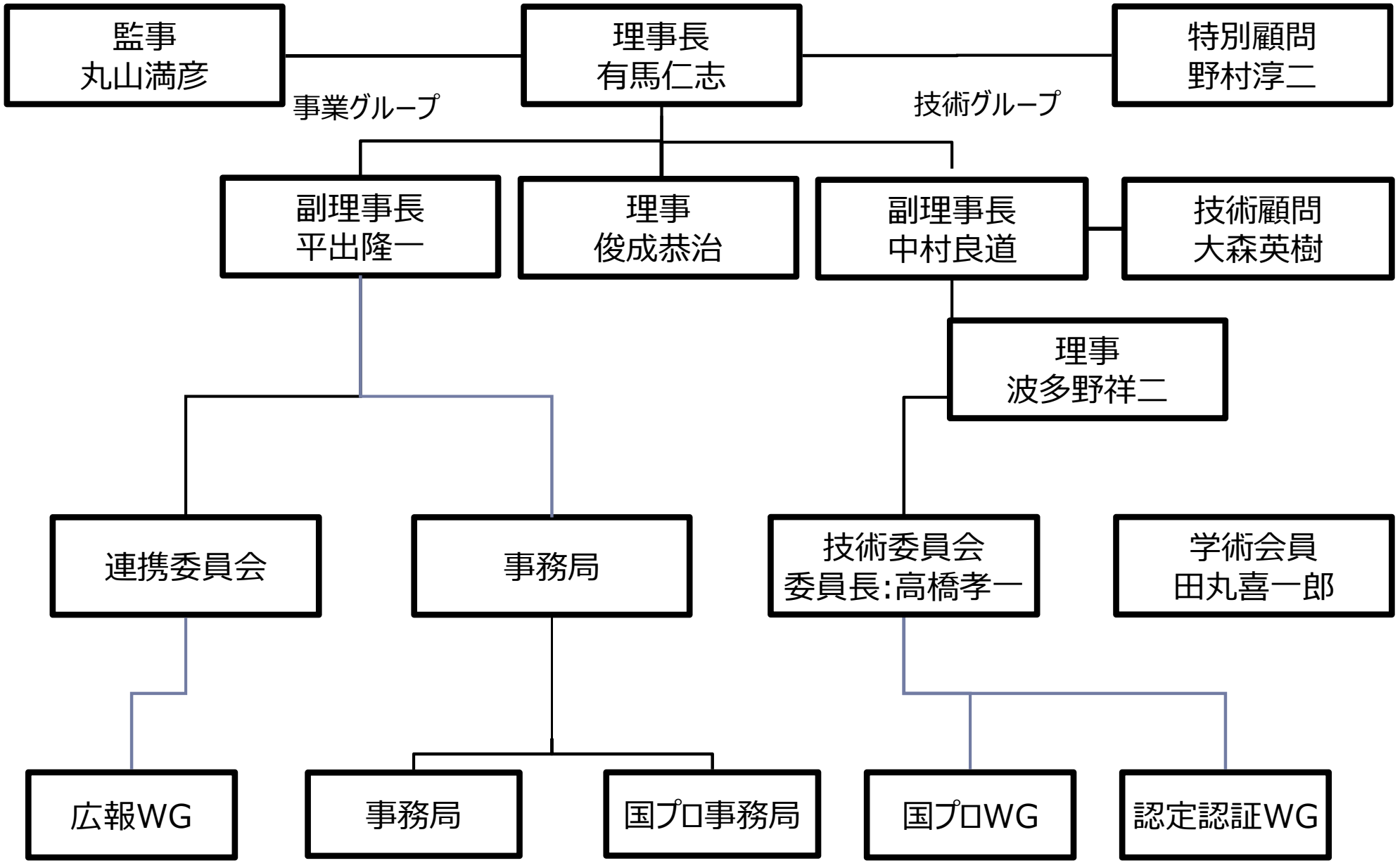
  〒141-0031 東京都品川区西五反田2-25-2 飯嶋ビル 5F
  - WEB ：http://www.smartsystem.or.jp/

役員等

- 理事長　有馬仁志　（有馬マネジメントデザイン株式会社 代表取締役社長、横浜スマートコミュニティ代表）
  - モデルベース開発技術、モデルベース開発環境・ツール
- 副理事長　平出隆一　（株式会社ガイア・システム・ソリューション 代表取締役会長）
  - 事業推進、事務局統括、国プロ統括
- 副理事長　中村良道　（株式会社スマートエナジー研究所 ファウンダ・CTO、福岡スマートハウスコンソーシアム代表）
  - システム設計技術・システム検証技術、技術委員会
- 理事　波多野祥二　（株式会社OTSL 代表取締役）
  - 認定・認証事業
- 理事　俊成　恭治　（株式会社村田製作所）
  - システム設計技術・認証事業
- 監事　丸山満彦　（有限責任監査法人トーマツ 取締役執行役員）
- 特別顧問　野村淳二　（IEC 次期会長、パナソニック株式会社 顧問）
- 技術顧問　大森英樹　（大阪工業大学 教授、電気学会 産業応用部門家電民生技術委員会 委員長）
  - 産学連携、学会連携
- 技術委員会 委員長　高橋孝一　（独立行政法人産業技術総合研究所 セキュアシステム研究部門）
- 学術会員　田丸喜一郎　（独立行政法人情報処理振興機構 技術本部 ソフトウェア・エンジニアリング・センター調査役）
- 事務局　（株式会社ガイア・システム・ソリューション内）

  〒141-0031 東京都品川区西五反田2-25-2 飯嶋ビル 5F

体制図



スマートシステムとは

- IT融合システム
  - IT(情報技術)を取り入れ融合させることによって実現されたシステム
  - 医療・食料・住環境（電力・交通・水等）といった生活の基盤を支えるインフラシステムを効率化する

  - IT＋電力 → スマートグリッド
  - IT＋家電など → スマートハウス
  - IT＋農業 → スマートアグリ
  - スマートグリッド＋スマートハウス＋・・・
    → スマートシティ、スマートコミュニティ

- これらを総称して、「スマートシステム」と我々は呼ぶ

SVA活動概要

- **目的：**
  - **個々の機器をネットワークで接続して構成される**
    スマートシステムの安全性の検証に必要な技術基盤の確立
    - このような基盤があれば、開発業者が提供する個々の機器のモデル等から
      スマートシステム全体の安全性を第三者が検証することが可能となる
- **目標：**
  - **スマートシステムの安全性検証フレームワークの確立**

安全性検証フレームワーク

- **リスク・ハザード分析手法**
  - スマートシステムが安全であることを示すには、
    考えうる限りのリスクやハザードに対する対応が取られ、かつその対応が適切であることが必要
- **スマートシステム全体のモデル記法**
  - 個々の機器のモデルを接続
  - 分析されたリスクやハザードへの対応を盛り込む
- **モデル上での検証技法**
  - スマートシステムのモデルが求められる安全性を充足することを検証

SVA 事業目標の全体像

事業目標

SVAの成果

スマートシステムの安全検証フレームワークの策定と普及

・開発・検証技術の開発、普及
・規格・ガイドラインの策定
・標準化の推進

国プロ事業（平成２５年度）
ＩＴ融合システムの信頼性・安全性等を確保する開発・検証技術等の確立
①リスク・ハザードの分類
②リスク・ハザードの分析
③スマートセルのシステムモデル化
④リスク・ハザードの分類と分析の実証
⑤信頼性・安全性の第三者による検証のガイドラインの検討

市場へのインパクト

スマートシステム市場の拡大、安全、安心な社会の実現、日本の国際競争力強化

認定事業者（例えばSVA）
・検証事業者の認定等の事業運営

システム開発者
・SVA の規格やガイドラインに沿ったシステム開発
・製品の安全性、信頼性向上による事業の拡大

検証事業者
・認定を受けた検証事業者として、スマートシステムの検証、認証事業の運営

システムインテグレータ
・SVAの規格やガイドラインに沿ったシステム統合
・システムの安全性、信頼性向上による事業拡大

ツールベンダー
・SVA の規格やガイドラインに沿ったツールの開発と販売

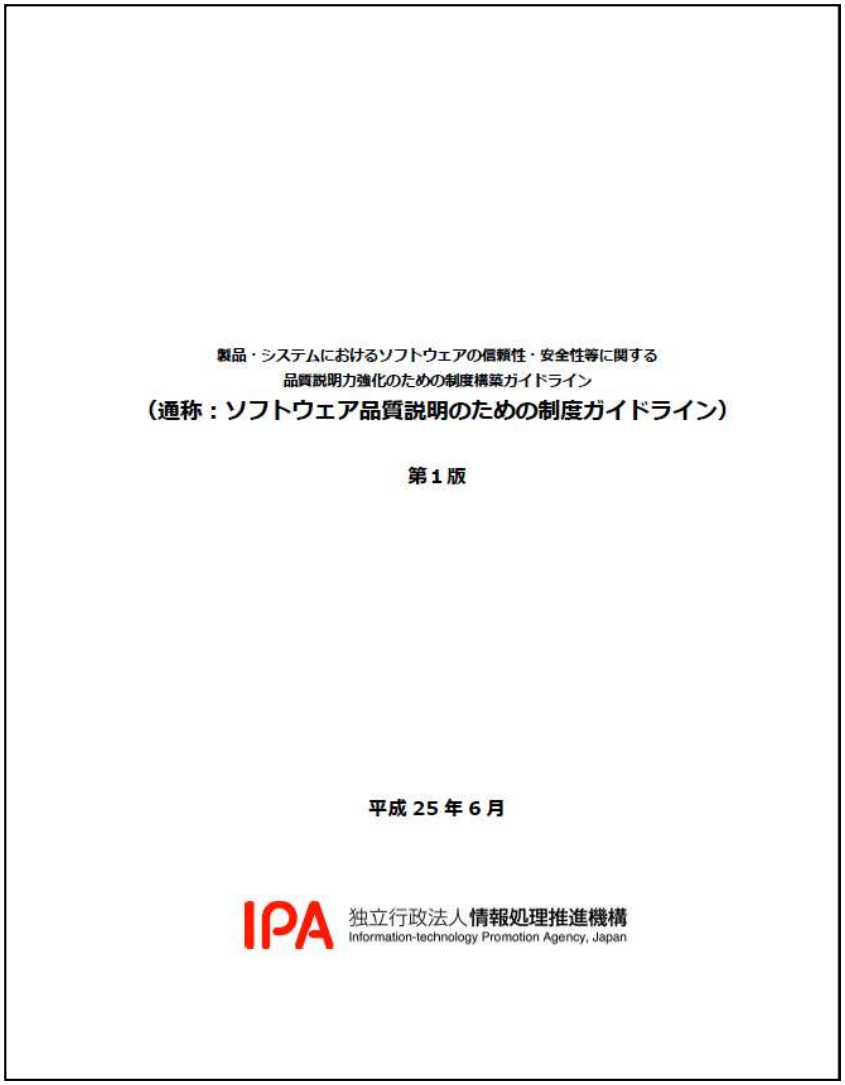
システムユーザ
・製品の信頼性、安全性向上による安心で快適な生活

SVA事業

- 安全性検証フレームワークの調査
  - リスクハザード分析
    - 既存のリスクハザード分析方法の調査
    - ハザード分類案、リスク分類案、リスク・ハザード分析プロセス案の策定
  - モデル記述（記法）、モデル解析
    - システムモデルの作成とシミュレーション
    - エラーモデルの作成とエラー解析トライアル
  - SVA国プロ 実施『平成２４年度産業技術実用化開発事業費補助金(組込みシステム基盤開発事業(ＩＴ融合システムの信頼性・安全性等を確保する第三者検証技術・手法の確立))』補助事業実施済
- 技術委員会活動
  - 実証評価
    - 横浜スマートコミュニティの実システム（スマートセル）による安全性検証フレームワークの評価と改良
    - リスクハザード分析でのセキュリティの考慮
    - リスク回避/低減策の検討
    - ディペンダビリティー仕様の作成
  - 認証（品質表示）制度の検討
    - IPA殿の「**ソフトウェア品質説明のための制度ガイドライン**」を基に検討
    - 認証制度の準備（審査基準の策定等）
  - ガイドライン化
    - リスクハザード分析ガイドライン、モデル記述・モデル解析ガイドライン等の整備
  - エネルギーシステムの認証制度策定
  - エネルギーシステム認証（品質表示）制度実施

IPA制度ガイドライン

ソフトウェア品質説明のための制度ガイドライン


製品・システムにおけるソフトウェアの信頼性・安全性等に関する
品質説明力強化のための制度構築ガイドライン
（通称：ソフトウェア品質説明のための制度ガイドライン）

第１版

平成 25 年 6 月

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目的：

第三者が品質説明の適切性を確認する仕組みを構築するアプローチについて記述している。

構成：

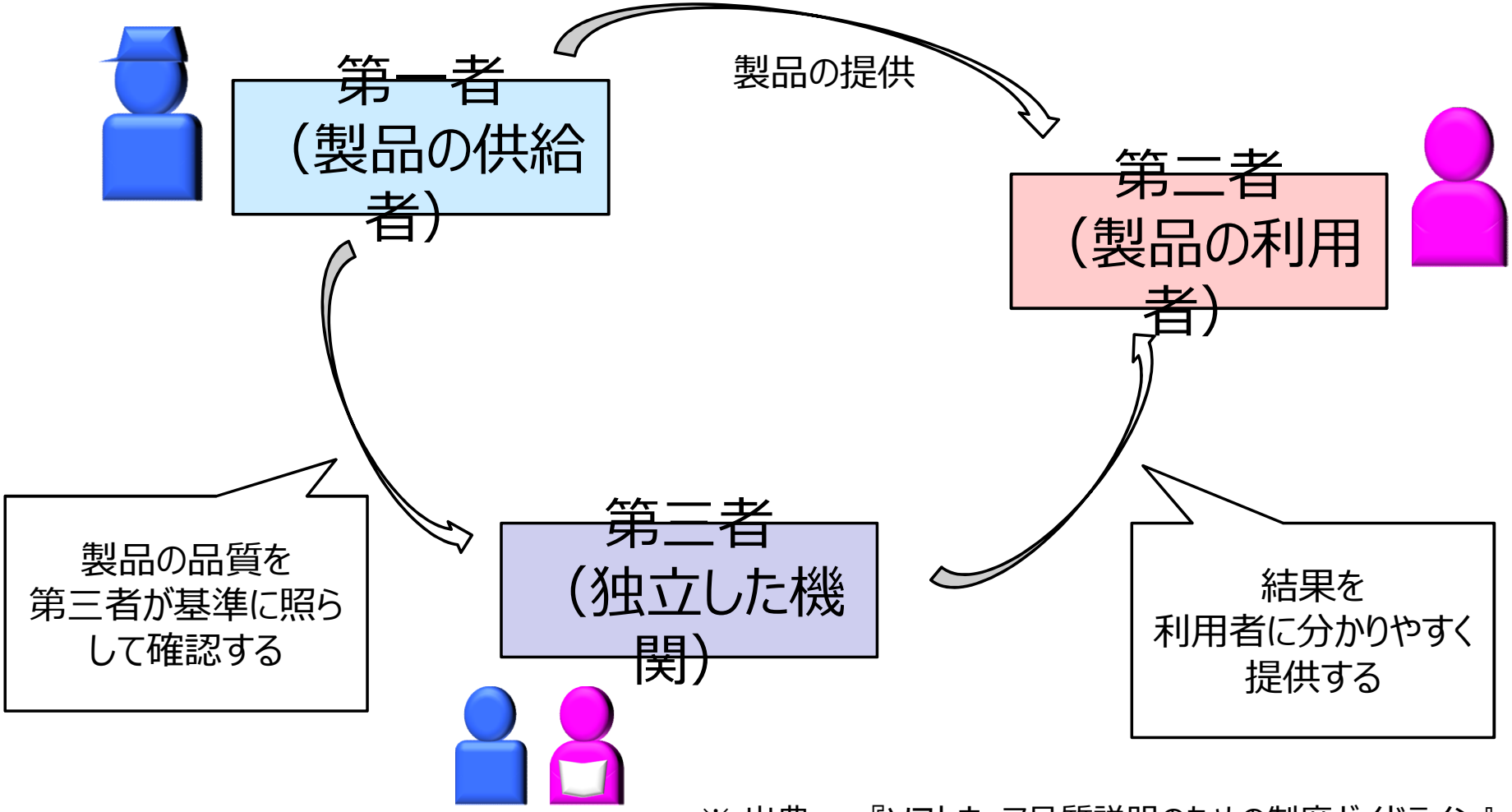
第１章～第３章： 用語の定義、基本的な考え方及び制度構築の方法
第４章： 制度への要求事項
第５章： その他（ガイドラインの準拠表示）

発行日：２０１３年６月

著者：独立行政法人　情報処理推進機構（IPA）

第三者認証制度

第三者による認証制度

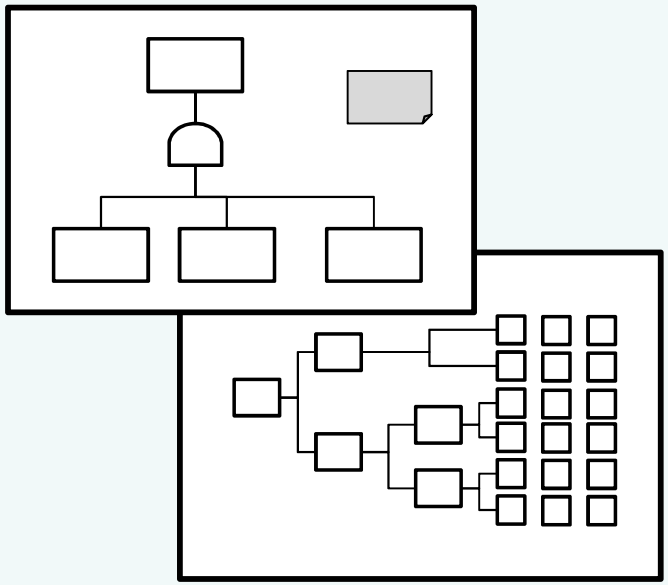


※ 出典： 『ソフトウェア品質説明のための制度ガイドライン』
独立行政法人 情報処理推進機構 （IPA/SEC）様

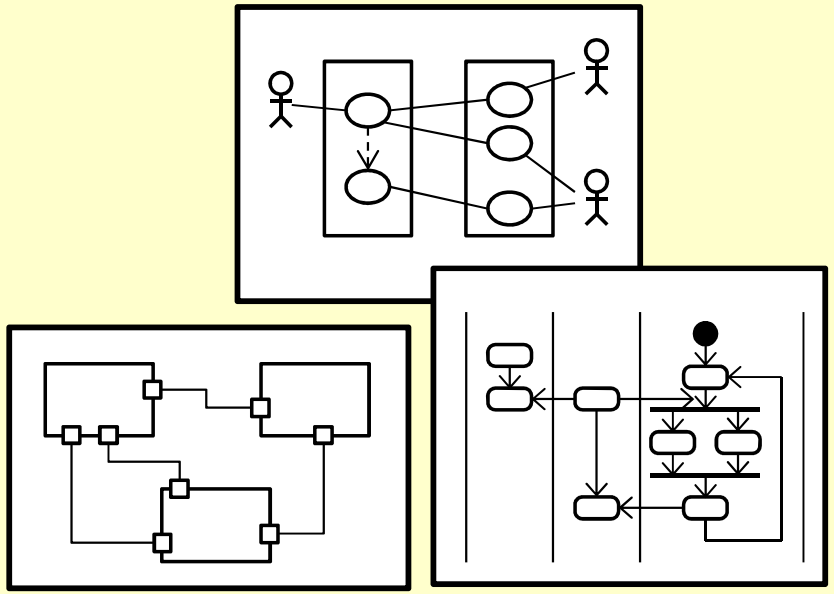
モデルベース認証

エネルギーシステムのモデルベース認証

STEP-1： **安全性とセキュリティ**の分析



STEP-2： **モデルによる記述**



STEP-3： **認証制度**（モデルベース）

認証レベル

認証レベル

	BRONZE	SILVER	GOLD
設計開発手法	**トレーサビリティ**を証明するエビデンスが用意されていること。	**モデルベース開発(MBD)**の手法が取り入れられていること。	**設計から検証まで一貫したMBD** を実現できていること。
安全性とセキュリティの分析	**リスクと安全性**が**分析**され、必要な**対策**が実施されていること。 安全性を**評価**していること。	BRONZEが実施できていること。 **脅威とセキュリティ**が**分析**され、必要な**対策**が実施されていること。 セキュリティを**評価**していること。	SILVERが実施できていること。 **安全性とセキュリティを含む品質/信頼性**が**分析**され、必要な**対策**が実施されていること。 品質/信頼性を**評価**していること。

ポイント
- リスク分析を重視し、**MBDの導入は任意**とする。
- システムの**ライフサイクル**を対象とする。

END
御清聴ありがとうございました