安全設計技術をセキュリティに

セキュリティ管理にも応用できる ZIPC TERAS

大崎人士
産業技術総合研究所

産業技術総合研究所のご紹介

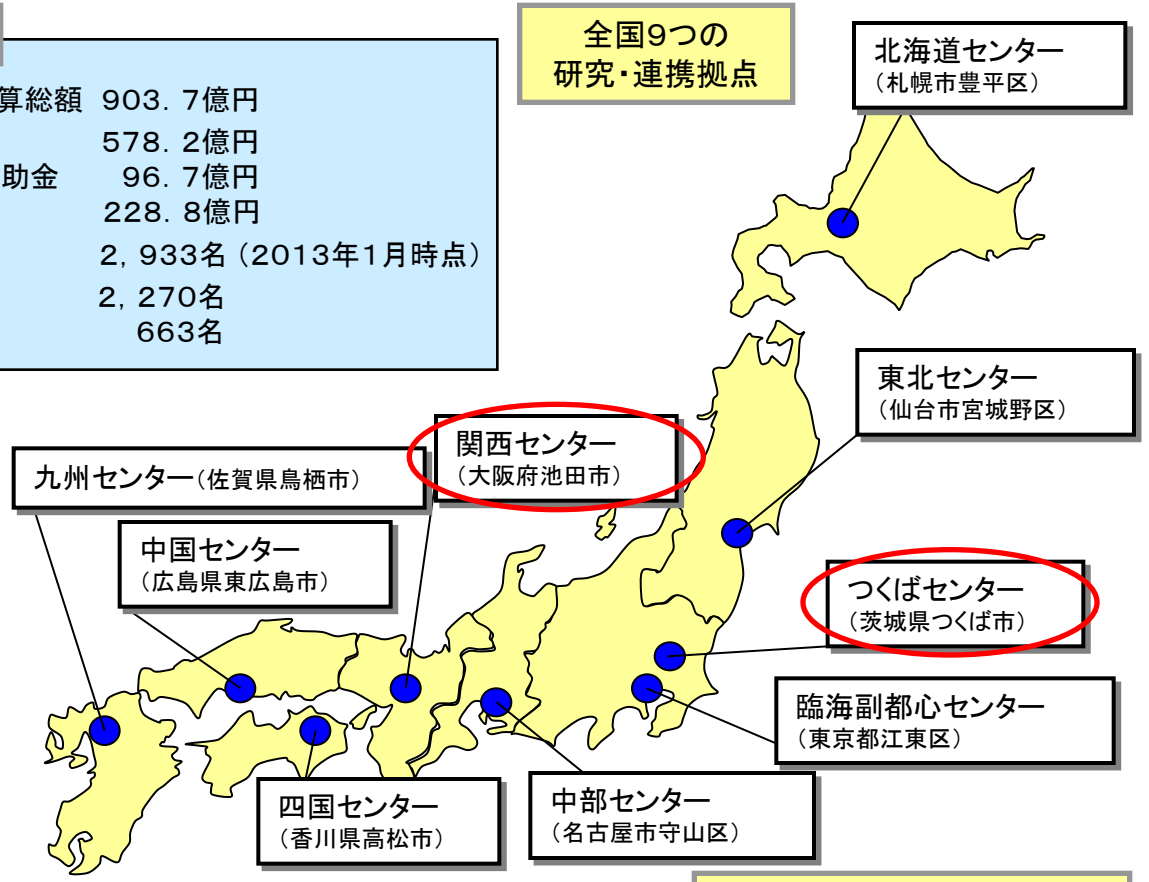
目的

鉱工業の科学技術に関する研究及び開発等の業務を総合的に行うことにより、産業技術の向上及びその成果の普及を図り、もって経済及び産業の発展並びに鉱物資源及びエネルギーの安定的かつ効率的な供給の確保に資すること

予算・人員

■2012年度予算総額　903．7億円
運営費交付金　578．2億円
施設整備費補助金　96．7億円
自己収入　228．8億円
■常勤職員数　2，933名（2013年1月時点）
研究職員数　2，270名
事務職員数　663名

全国9つの研究・連携拠点



産総研関西センターの三大発明

- PAN系炭素繊維

- ITO透明電極

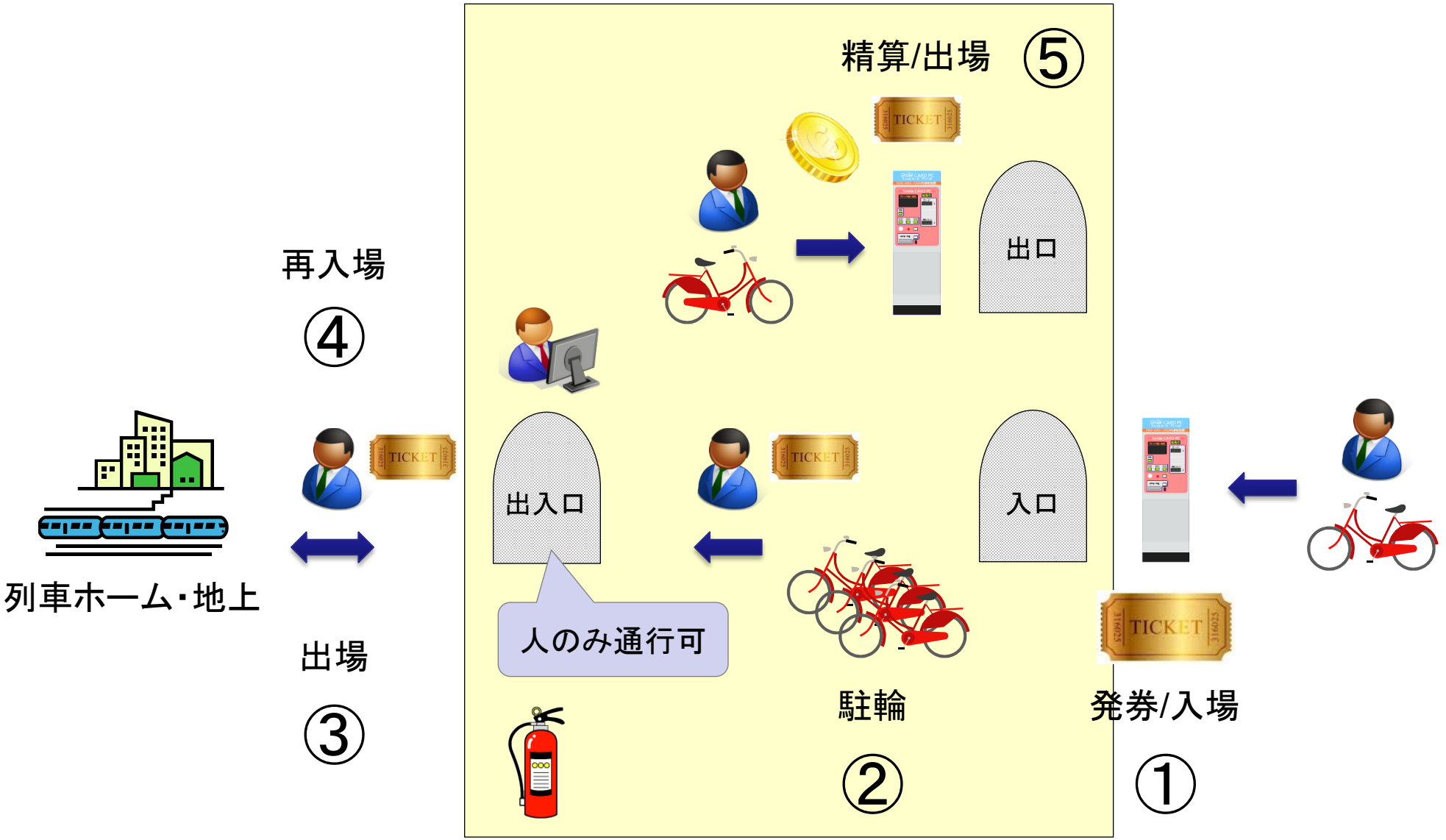
- 水素吸蔵合金とニッケル水素電池

人材受入実績(産総研全体)

■企業から　1,741名
■大学から　2,063名
■独法・公設研等から　862名
（うち海外から　442名）
※2012年度受入延べ数

セーフティとセキュリティ

とある駐輪場



利用シーンからシステム要件を考える

危険源を識別し、危害を特定する

危険源

人・財産・環境

線路上の小石

危険状態

満員の列車

危険事象

人身事故

危害

脱線

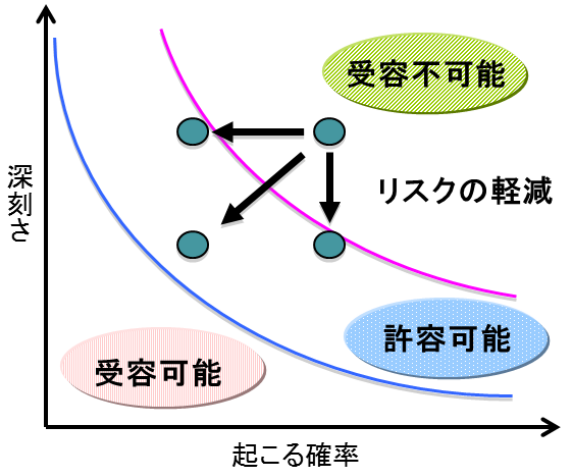
リスクを軽減するための要件

絶対安全

高品質のよい製品を作ることに労力を集中させる

「リスク」とは

「危害」が起こる確率×結果の深刻さ



機能安全

故障時の危険事象の程度や頻度を見積もる

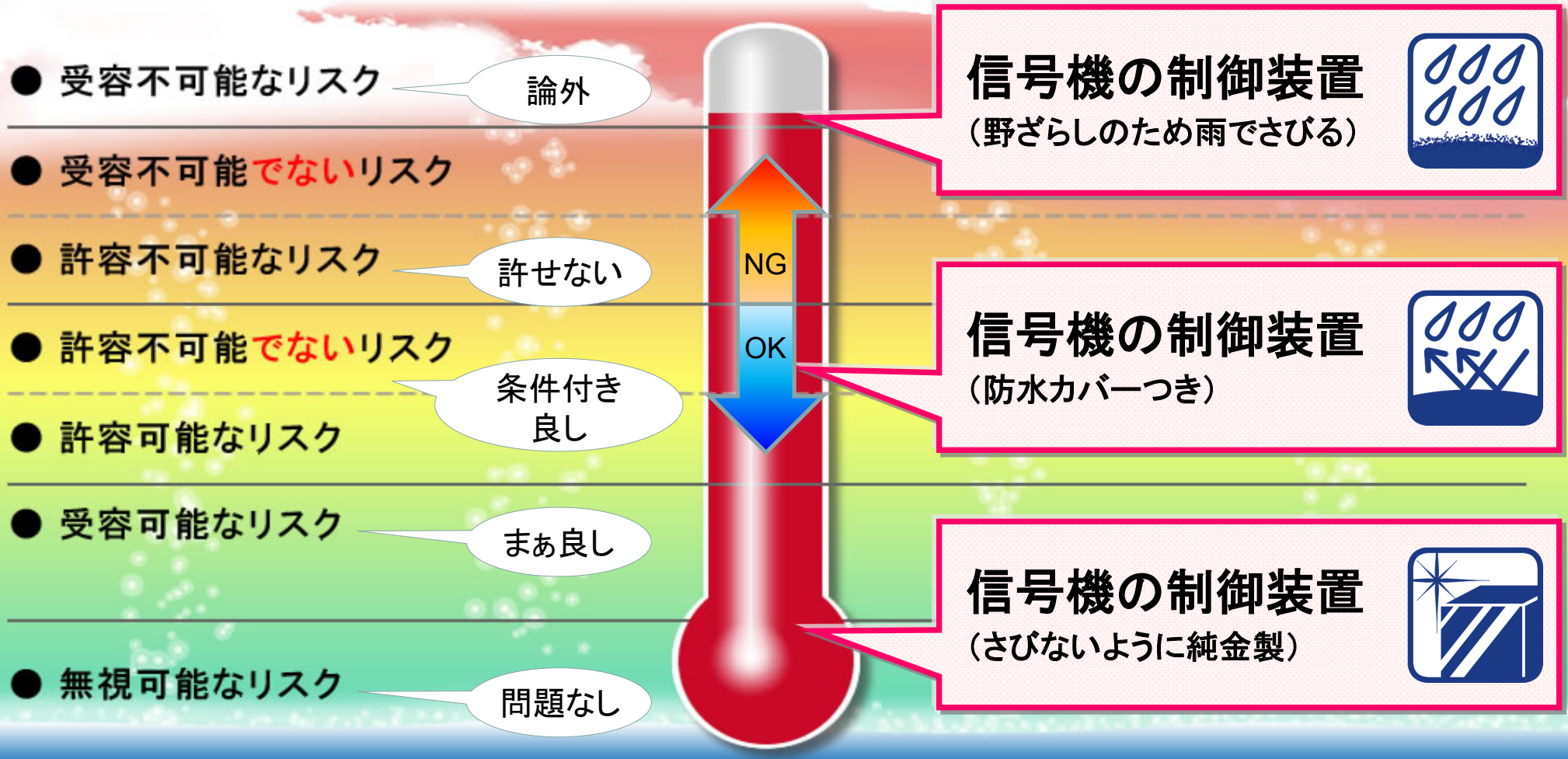
合理的に最大限安全であることを示す証跡を整備

立体交差

踏切

受容できるリスク

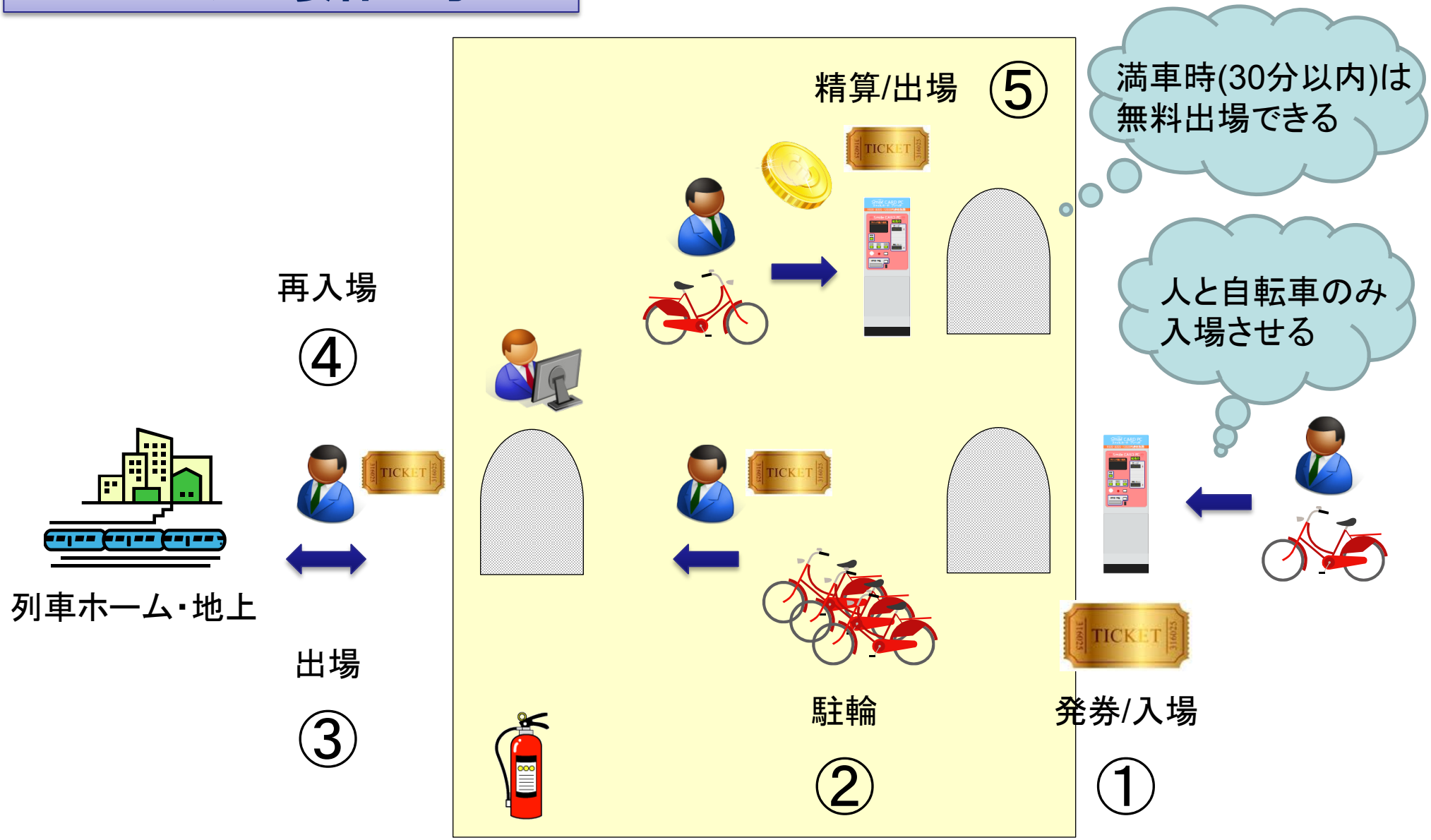
【前提：特別な状況を除きリスクは正当化されない】



IEC 61508-5で示されるALARP原理

［制御システムの安全］

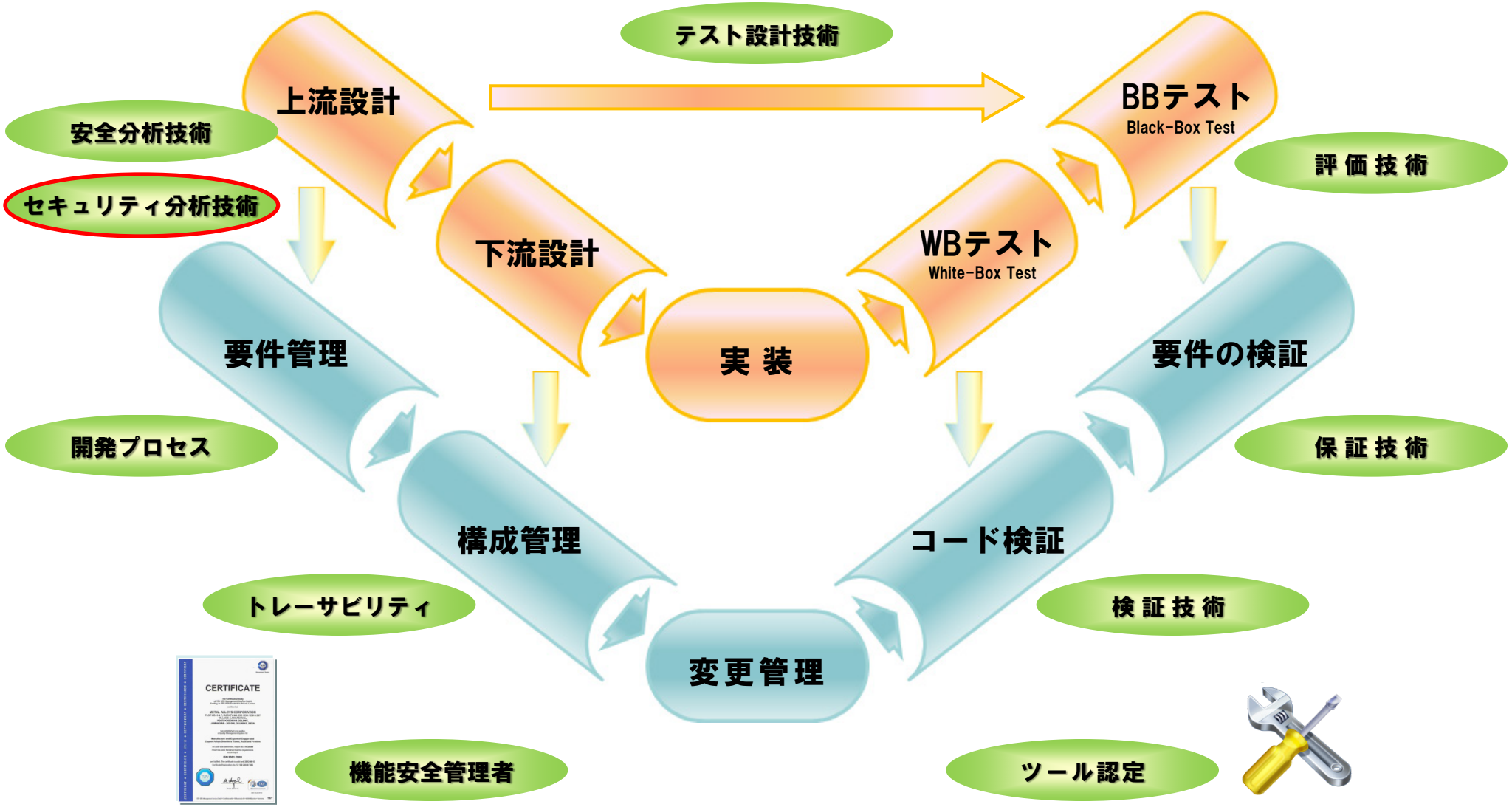
セキュリティ要件を考える



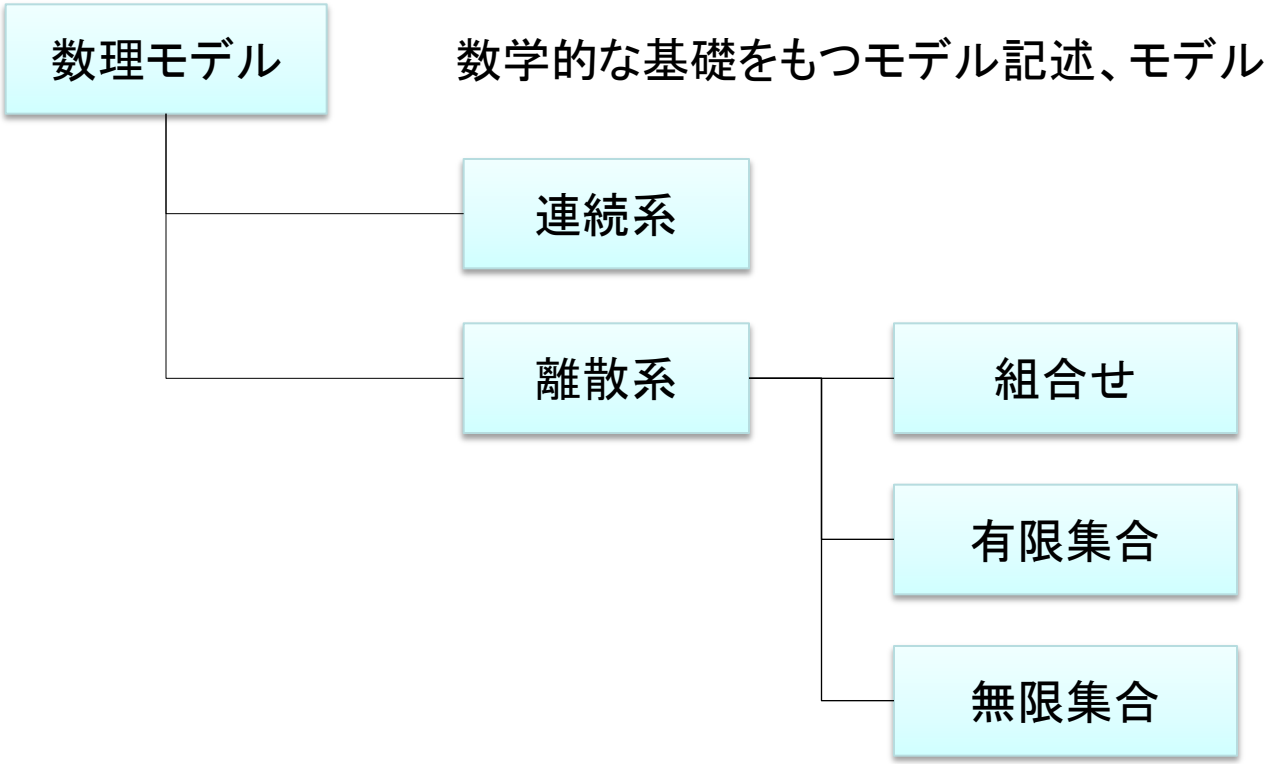
情報セキュリティとリスク

- 情報セキュリティとは、機密性・完全性・可用性を維持すること。
- 機密性とは、認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。（外的要因）
- 完全性とは、正確さ及び完全さの特性。
- 可用性とは、認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。
- 情報セキュリティリスクは，脅威（リスク源）が情報資産（被害の度合）のぜい弱性（弱点）又は情報資産グループのぜい弱性に付け込み，その結果，組織に損害を与える可能性に伴って生じる。（JIS Q 27000:2014）

開発工程（V字開発）と開発技術



分析のためのモデリング技術



数学的な基礎をもつモデル記述、モデルは常に整合的

シミュレーション
MATLAB/Simulink、SCADE

テストセット生成
ZIPC FOT

モデル検査
SPIN、SMV、PAT

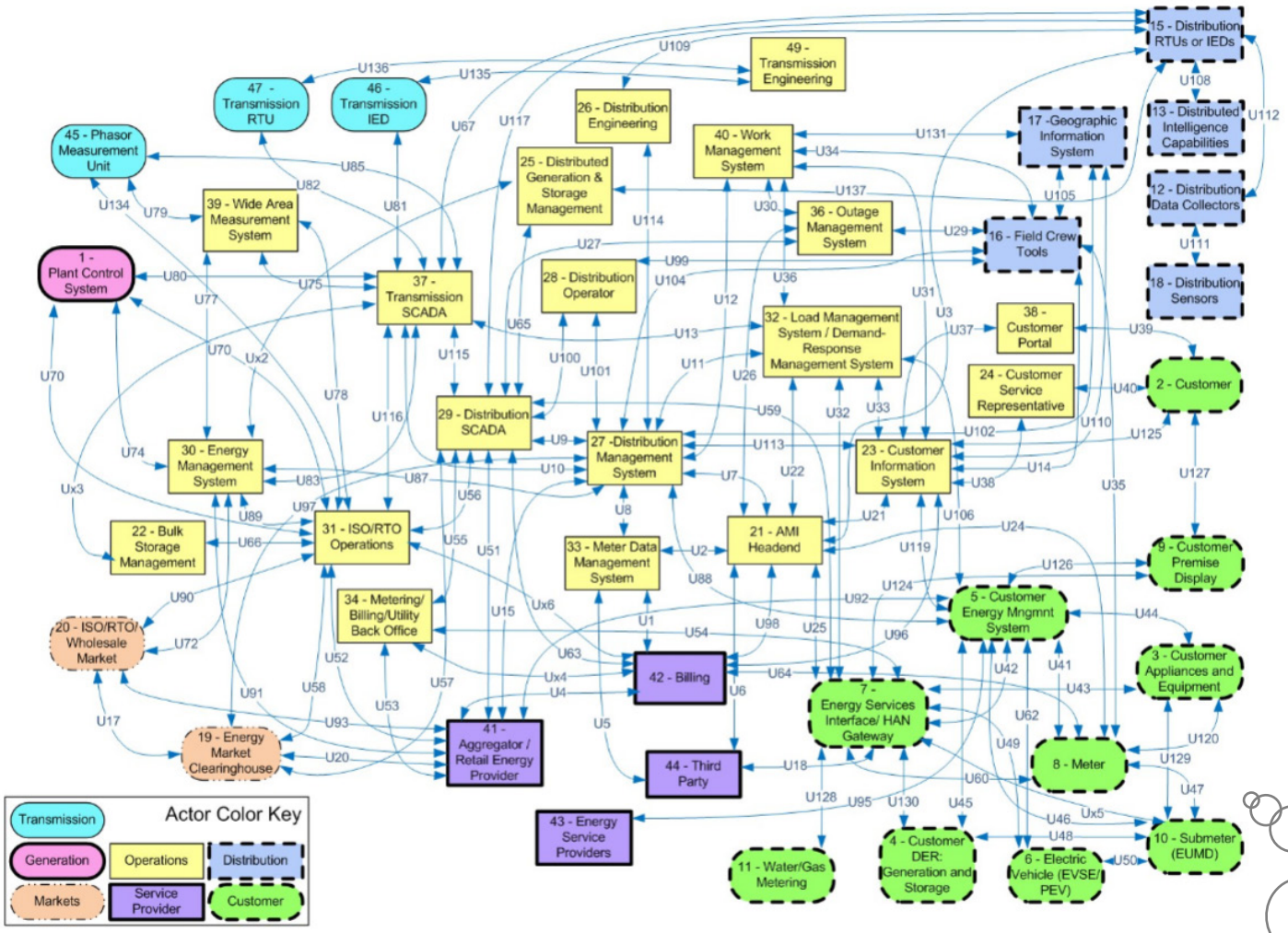
定理証明
Coq、Isabelle、PVS

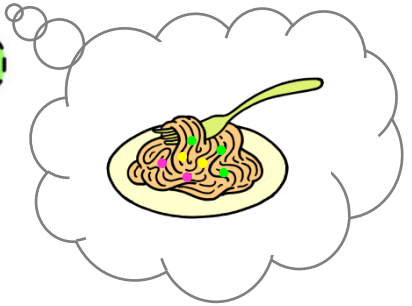
離散シミュレーション
VDM++、B、Maude、ZIPC

非数理モデル

統一された図によるモデル記述、モデルの整合性の検証が困難

外部要因のモデル化…





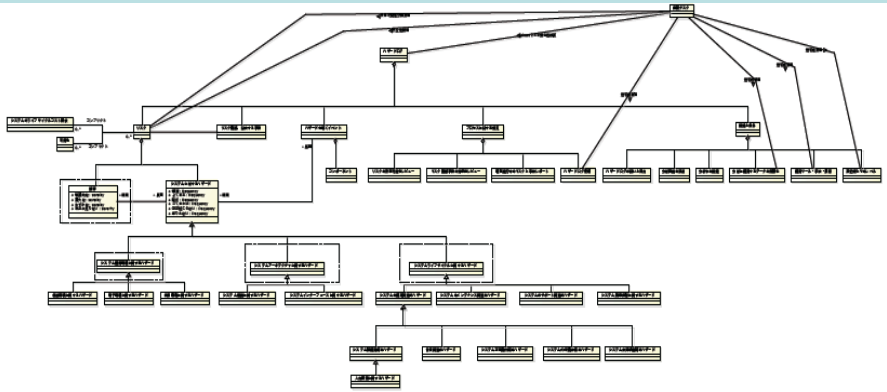
リファレンスモデル（米国基準NIST IR 7628より）

保証技術とメタモデリング

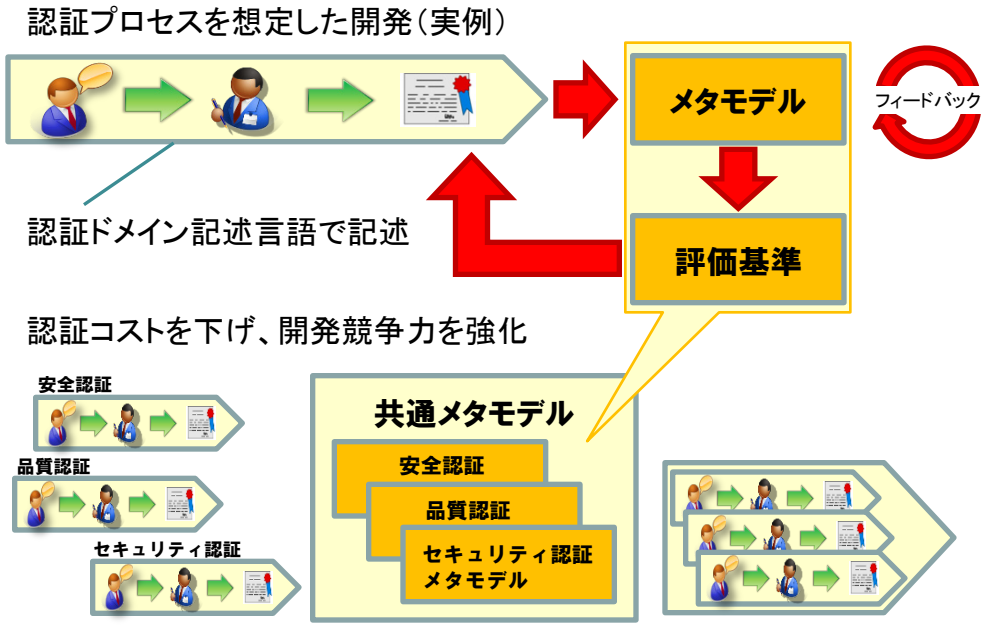
- **認証品質を検証する方法がない**
  - 認証にかかるコストと、審査内容（品質）の関係を明確に
- **認証プロセスのリスクを見積もれない**
  - 評価基準が、認証機関ごとに異なり、現場の対応はまちまち
- **認証側の要求を開発側に伝える方法がない**
  - 認証プロセスで使う共通言語が必要

安全認証プロセスのための技術が必要

メタモデリング



鉄道事業者との共同研究で作成した鉄道安全規格のメタモデル
（の産総研の2012年度研究成果の一部）



情報セキュリティとモデリング技術

我が国の情報セキュリティ対策

IT戦略本部（本部長：内閣総理大臣）

情報セキュリティ政策会議（議長：内閣官房長官）　2005年 設置

・基本戦略
・国際戦略
・政府総合対策
・重要インフラ対策
・事案対処支援

NISC National Information Security Center　内閣官房情報セキュリティセンター

協力

重要インフラ（１０分野）
所管省庁
（金融、国交、厚生）

警察庁　総務省　外務省　経済産業省　防衛省　庶務５省庁

●サイバー犯罪対策

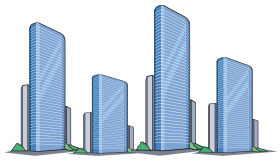
●国家防衛

●政府対策基準の策定
●政府機関へのサイバー攻撃防御

●情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

●通信ネットワーク対策
●自治体の対策

●すべての基礎を支える情報システムの対策
●重要インフラ（電力、ガス）
●企業・個人の対策

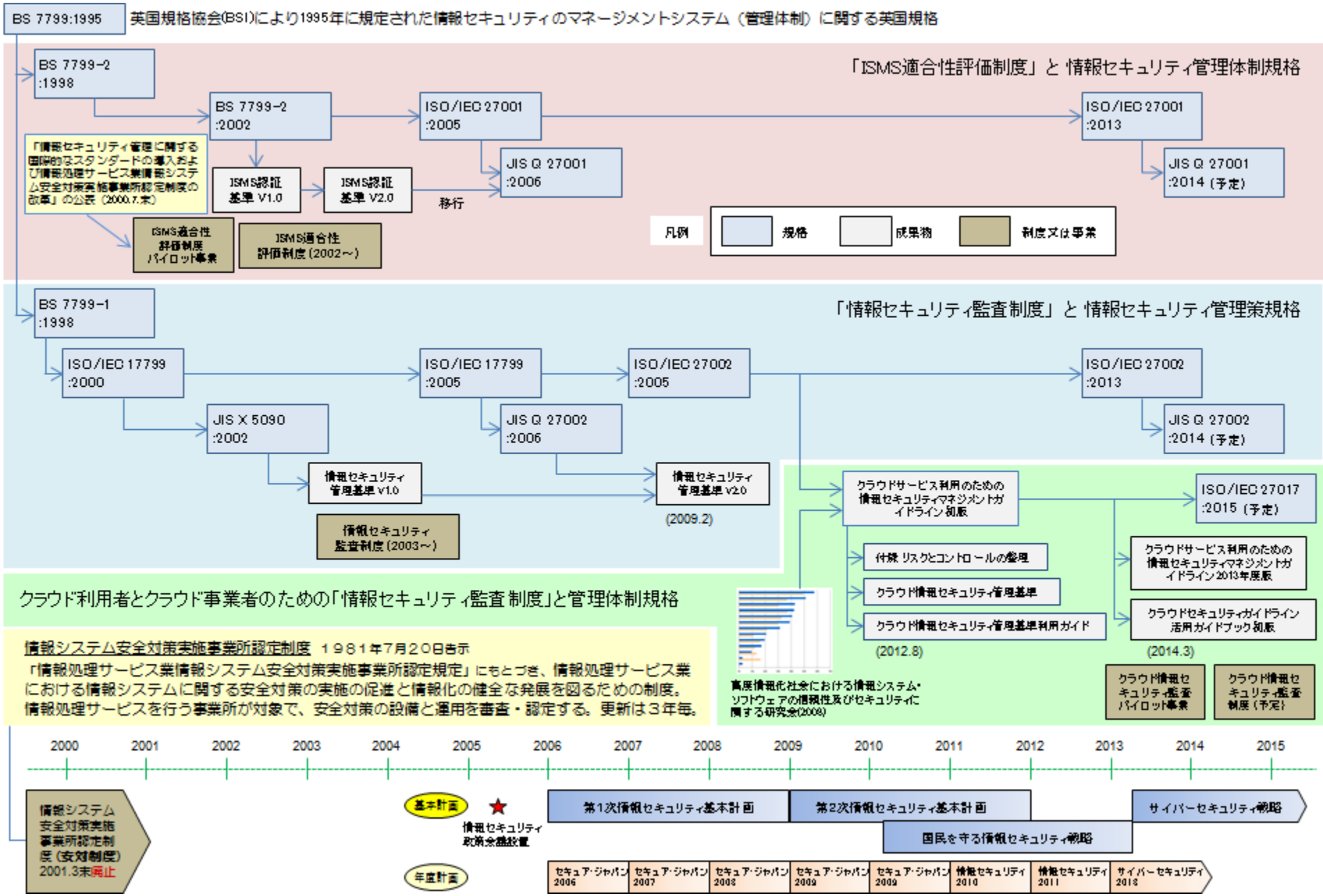


政府機関

重要インフラ

企業

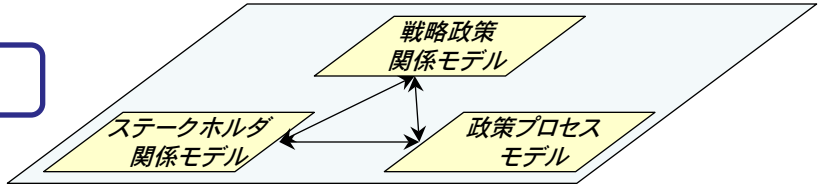
個人


BS 7799:1995
英国規格協会(BSI)により1995年に規定された情報セキュリティのマネージメントシステム（管理体制）に関する英国規格
「ISMS適合性評価制度」と 情報セキュリティ管理体制規格
BS 7799-2 :1998
BS 7799-2 :2002
ISO/IEC 27001 :2005
ISO/IEC 27001 :2013
「情報セキュリティ管理に関する国際的なスタンダードの導入および情報処理サービス業情報システム安全対策実施事業所認定制度の改革」の公表（2000.7.末）
ISMS認証基準 V1.0
ISMS認証基準 V2.0
移行
JIS Q 27001 :2006
JIS Q 27001 :2014（予定）
ISMS適合性評価制度パイロット事業
ISMS適合性評価制度（2002～）
凡例
規格
成果物
制度又は事業
「情報セキュリティ監査制度」と 情報セキュリティ管理策規格
BS 7799-1 :1998
ISO/IEC 17799 :2000
ISO/IEC 17799 :2005
ISO/IEC 27002 :2005
ISO/IEC 27002 :2013
JIS X 5090 :2002
JIS Q 27002 :2006
JIS Q 27002 :2014（予定）
情報セキュリティ管理基準 V1.0
情報セキュリティ管理基準 V2.0
(2009.2)
情報セキュリティ監査制度（2003～）
クラウドサービス利用のための情報セキュリティマネジメントガイドライン初版
ISO/IEC 27017 :2015（予定）
付録 リスクとコントロールの整理
クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版
クラウド情報セキュリティ管理基準
クラウド情報セキュリティ管理基準利用ガイド
(2012.8)
クラウドセキュリティガイドライン活用ガイドブック初版
(2014.3)
高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会(2008)
クラウド情報セキュリティ監査パイロット事業
クラウド情報セキュリティ監査制度（予定）
クラウド利用者とクラウド事業者のための「情報セキュリティ監査 制度」と管理体制規格
情報システム安全対策実施事業所認定制度 １９８１年７月２０日告示
「情報処理サービス業情報システム安全対策実施事業所認定規定」にもとづき、情報処理サービス業における情報システムに関する安全対策の実施の促進と情報化の健全な発展を図るための制度。
情報処理サービスを行う事業所が対象で、安全対策の設備と運用を審査・認定する。更新は３年毎。
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
情報システム安全対策実施事業所認定制度（安対制度）2001.3末廃止
基本計画
情報セキュリティ政策会議設置
第1次情報セキュリティ基本計画
第2次情報セキュリティ基本計画
サイバーセキュリティ戦略
国民を守る情報セキュリティ戦略
年度計画
セキュア・ジャパン 2006
セキュア・ジャパン 2007
セキュア・ジャパン 2008
セキュア・ジャパン 2009
セキュア・ジャパン 2009
情報セキュリティ 2010
情報セキュリティ 2011
サイバーセキュリティ 2013

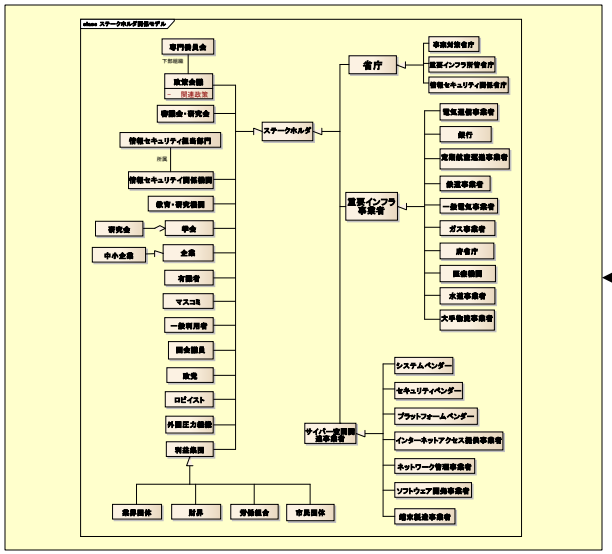
情報セキュリティ政策分野のモデル化

経済産業省 平成25年度情報セキュリティ対策推進事業

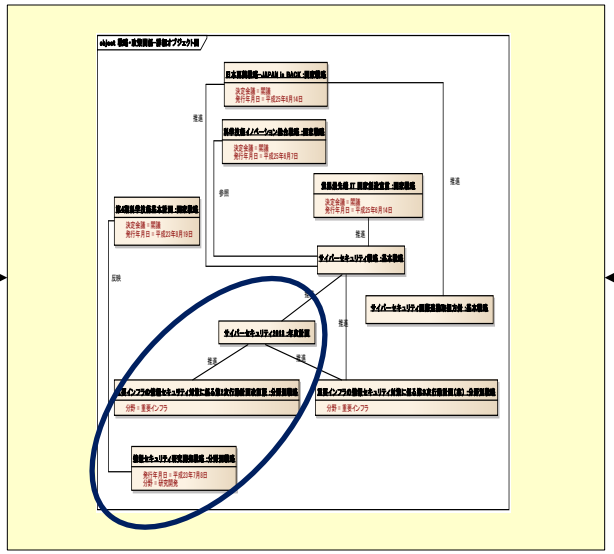
抽象モデル



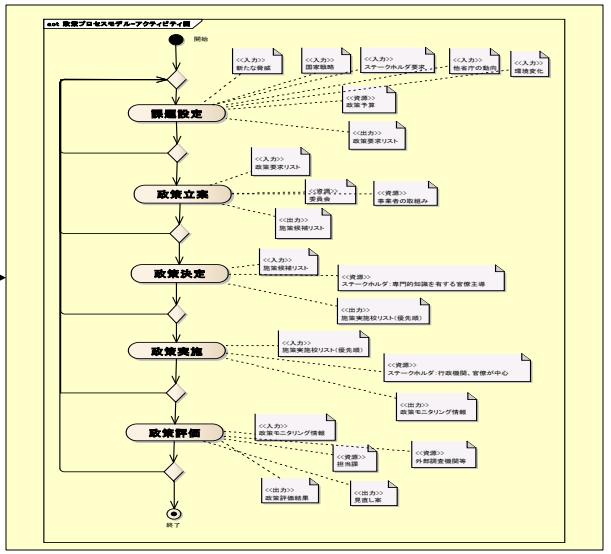
ステークホルダ



戦略・政策



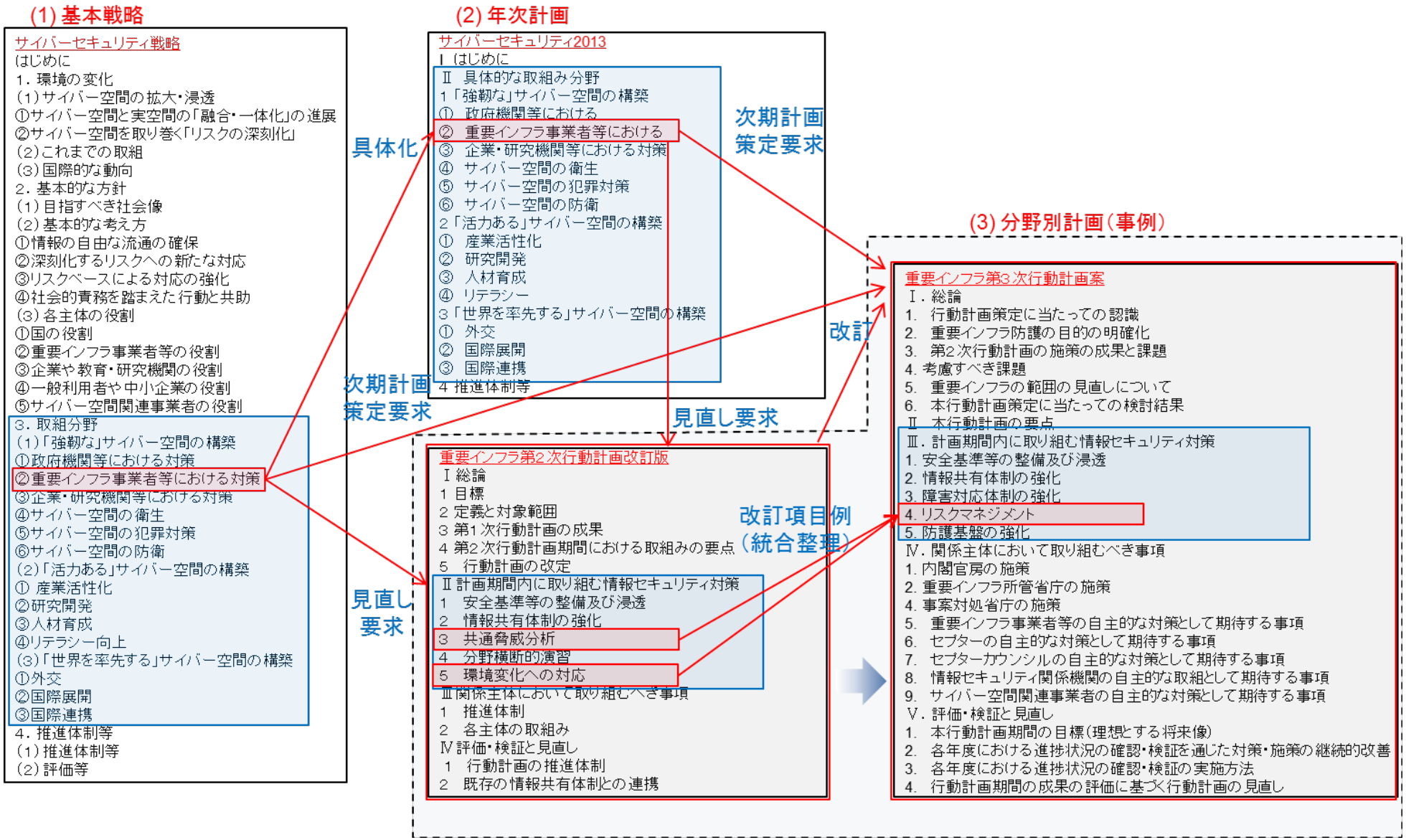
政策プロセス



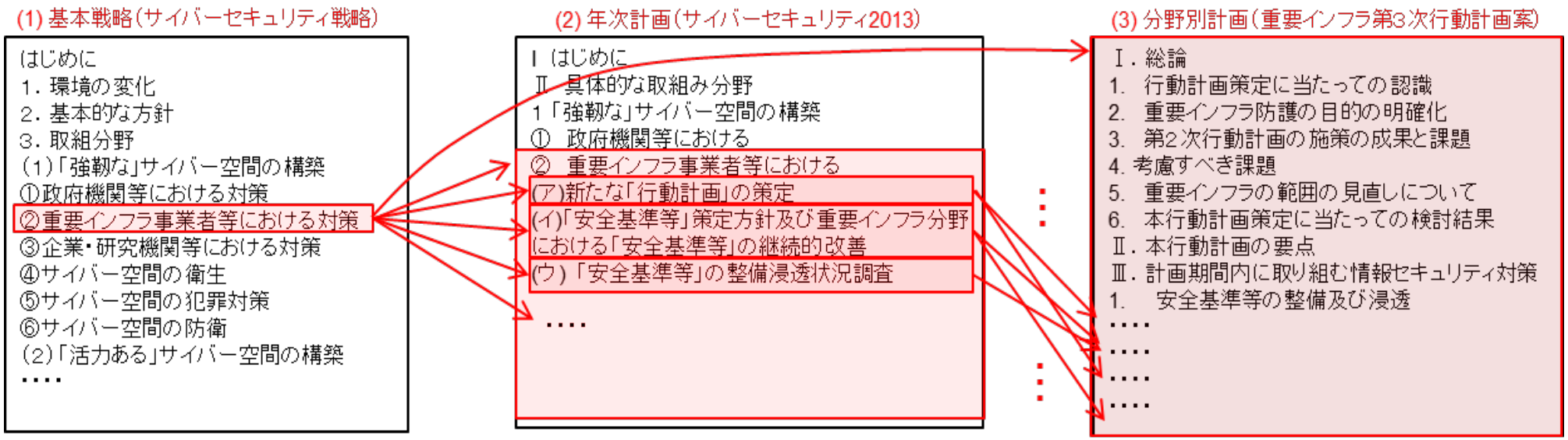
詳細モデル（一部）

基本戦略 ⟷ 年次戦略 ⟷ 分野別戦略

重要インフラのセキュリティ対策



基本計画、年次計画、分野別計画



- **基本計画（アークテクチャ設計）**

詳細化

- **年次計画（システム、基本設計）**

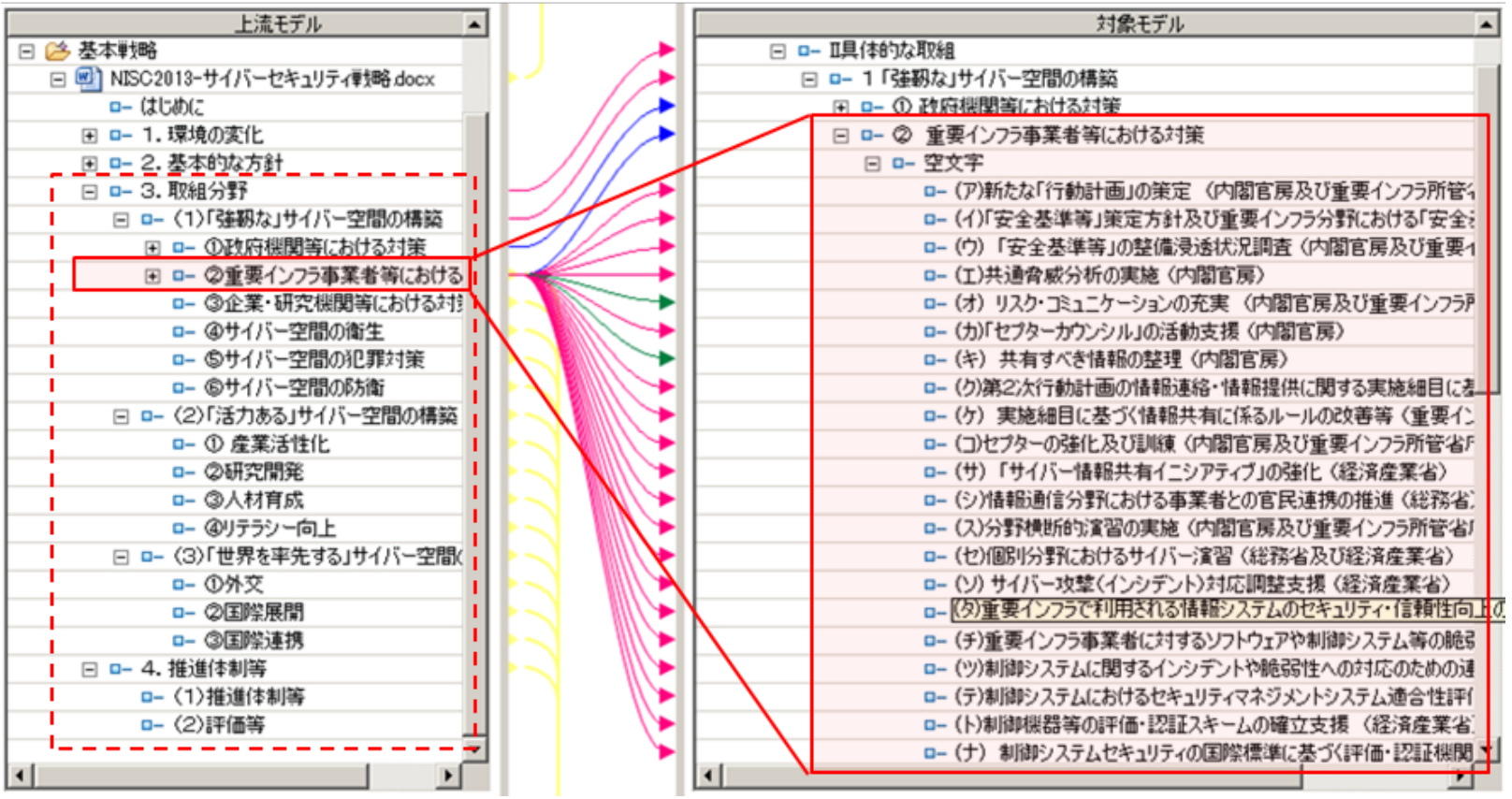
詳細化

- **分野別計画（部品、詳細設計）**

計画文書のトレース関係（基本計画と年次計画）

基本戦略の章構成（一部）

年次計画の章構成（一部）

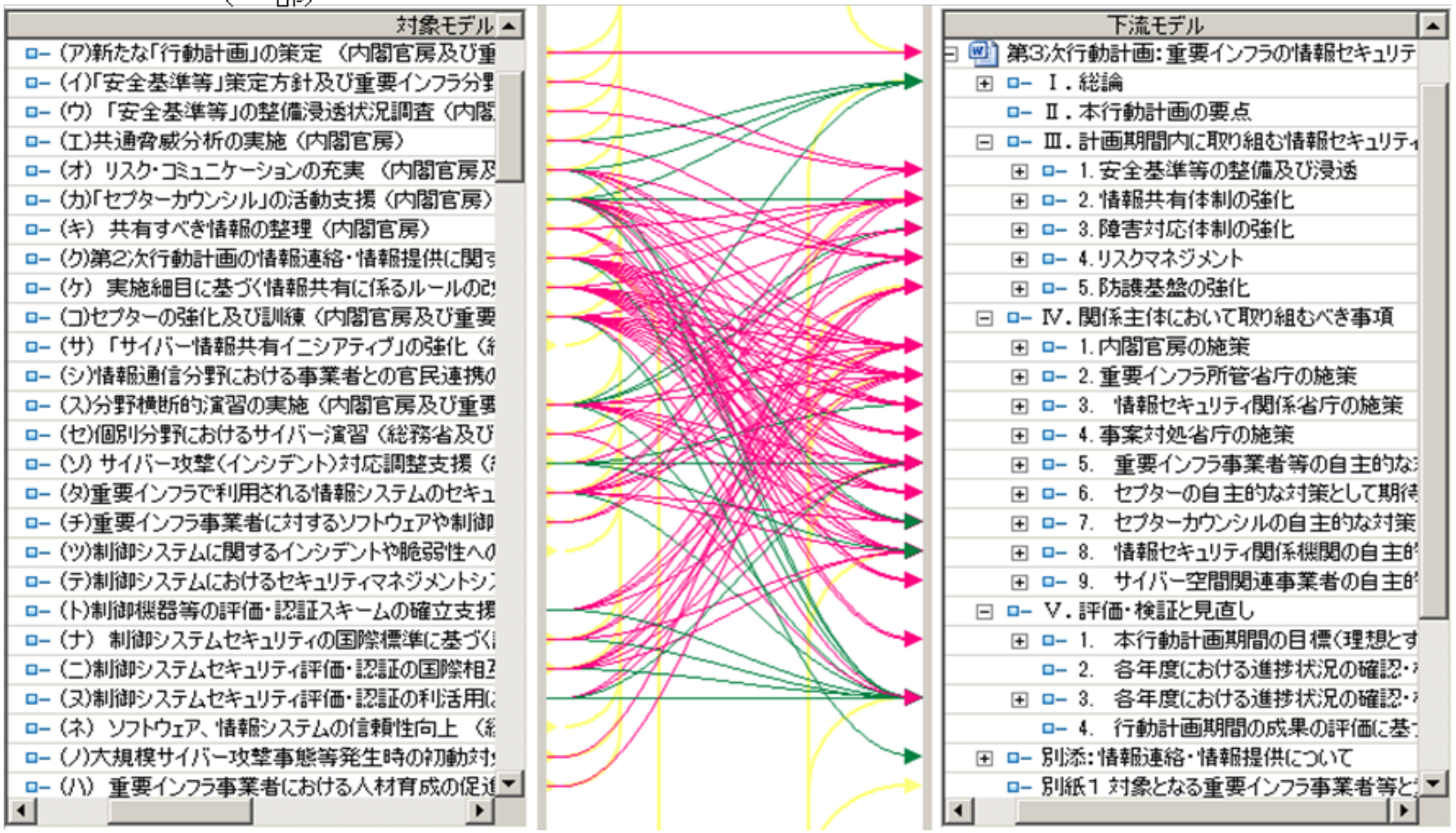


弱い関係（緑色）、デフォルト（青色）、強い関係（ピンク色）、表示範囲外（黄色）

計画文書のトレース関係（年次計画と分野別計画）

年次計画の
「II.1.②重要インフラ事業者等における対策」
（一部）

重要インフラ第３次行動計画
（一部）



計画文書の品質を維持する

- **基本方針は、どのように具体化されたか**

  基本計画～分野別計画等への前方トレース分析

- **追加、削除された計画はどれか**

  年次計画間の前方トレース分析

- **無理な課題設定がないか**

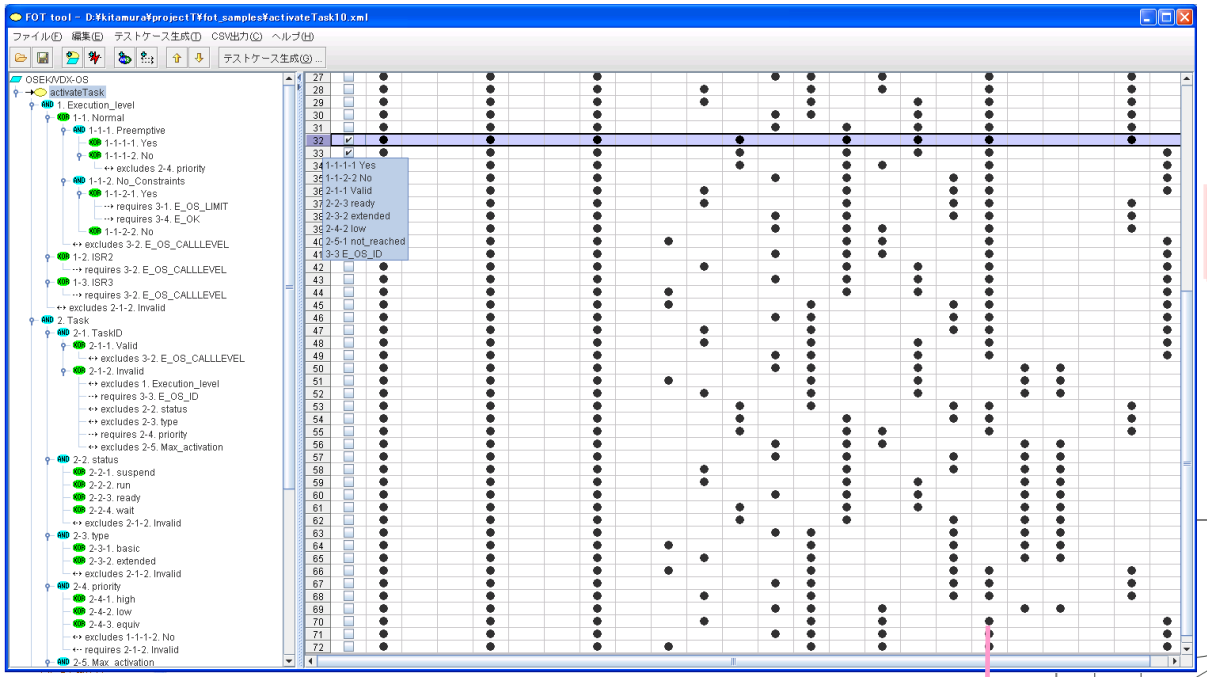
  基本計画－年次計画、年次計画－分野別計画等の多重度分析

- **あれは、どこいった？（改訂後の計画のモレヌケ確認）**

  トレース関係の有無の確認

省庁間、省内調整では、とても大事

テスト設計技術



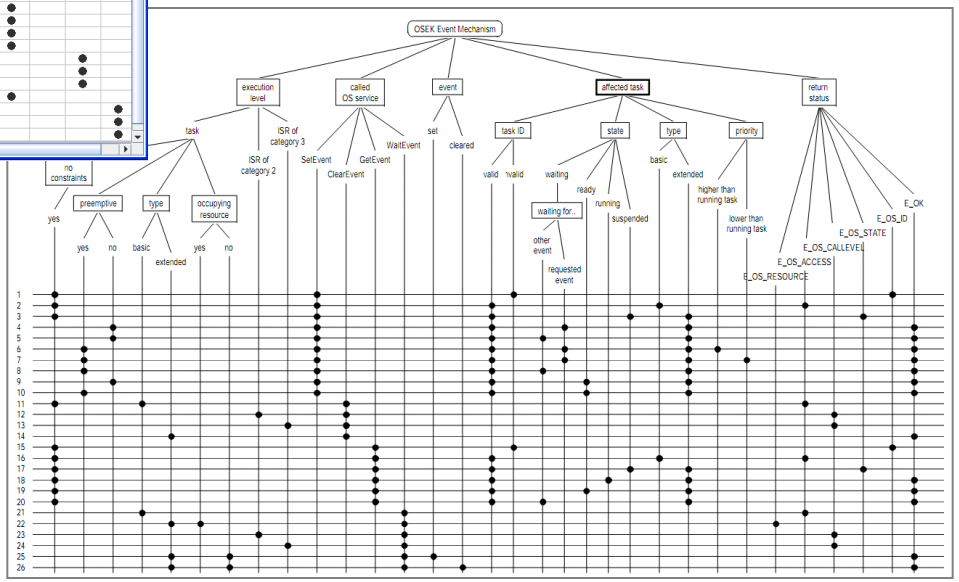
1. テスト設計

2.テスト生成

自動生成による過不足のない
「安全な」テストセット

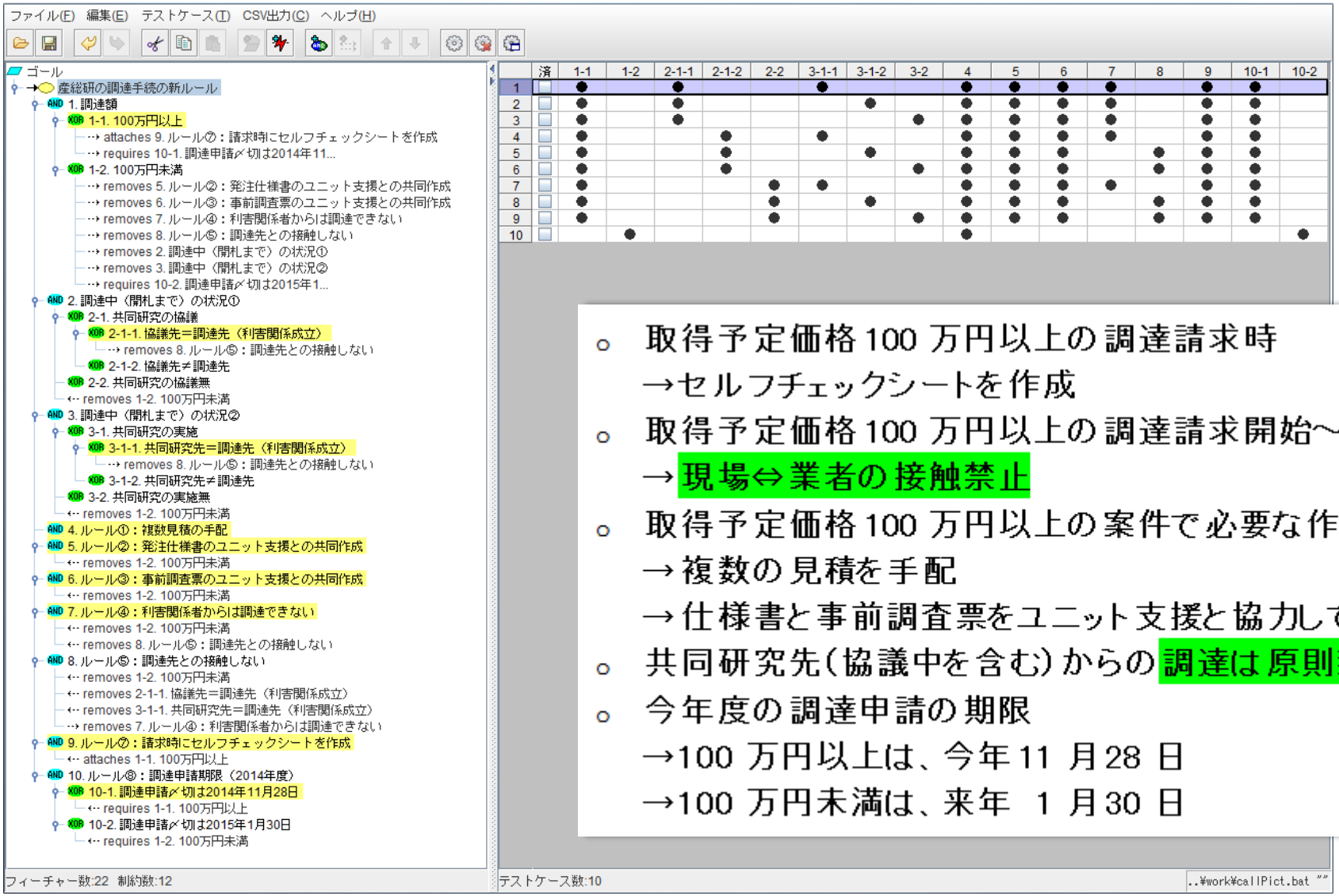
説明文書を自動で作成

3. ドキュメント化



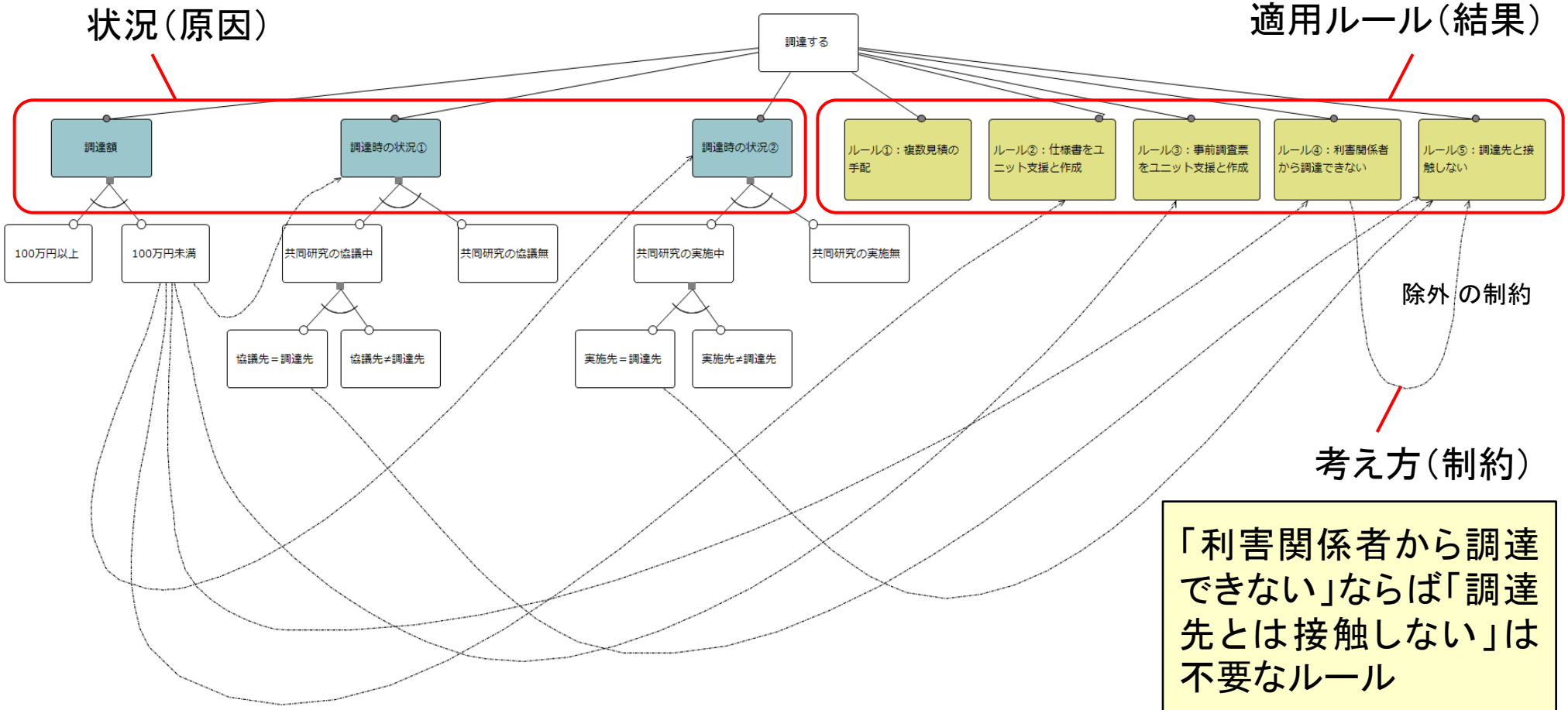
印刷イメージ

管理策のモデル化



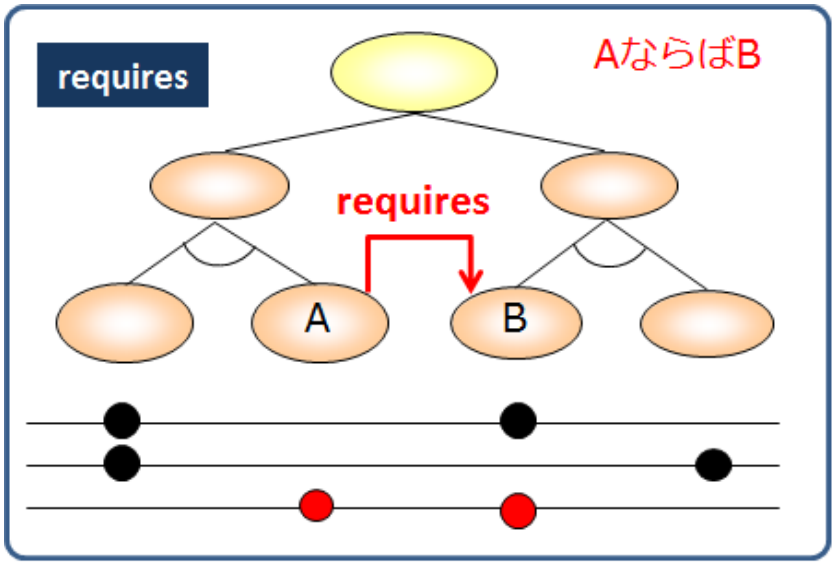
- 取得予定価格 100 万円以上の調達請求時
  →セルフチェックシートを作成
- 取得予定価格 100 万円以上の調達請求開始～開札まで
  → 現場⇔業者の接触禁止
- 取得予定価格 100 万円以上の案件で必要な作業
  →複数の見積を手配
  →仕様書と事前調査票をユニット支援と協力して作成
- 共同研究先（協議中を含む）からの 調達は原則禁止
- 今年度の調達申請の期限
  →100 万円以上は、今年 11 月 28 日
  →100 万円未満は、来年 1 月 30 日

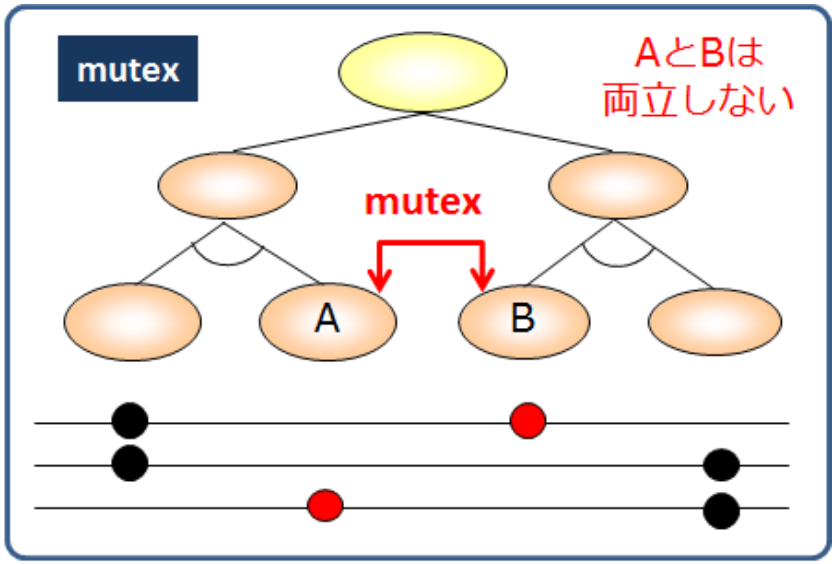
考え方をモデルに反映する

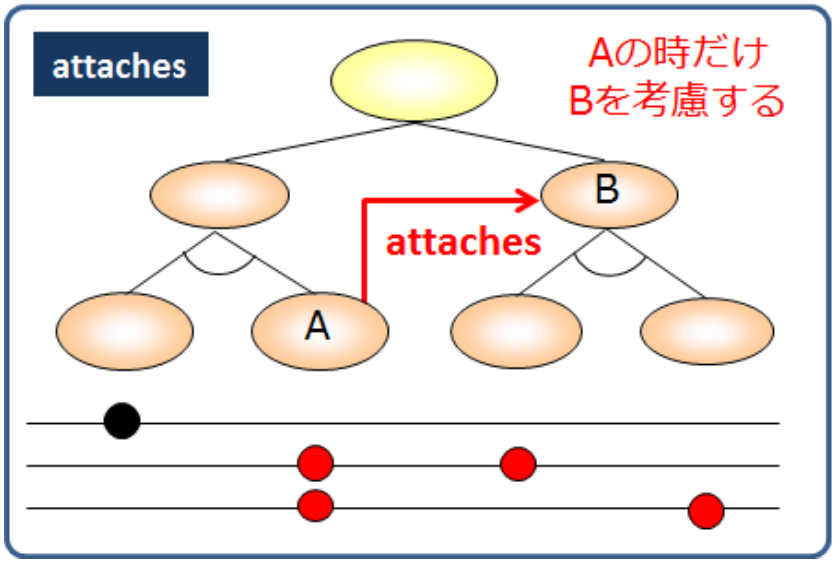


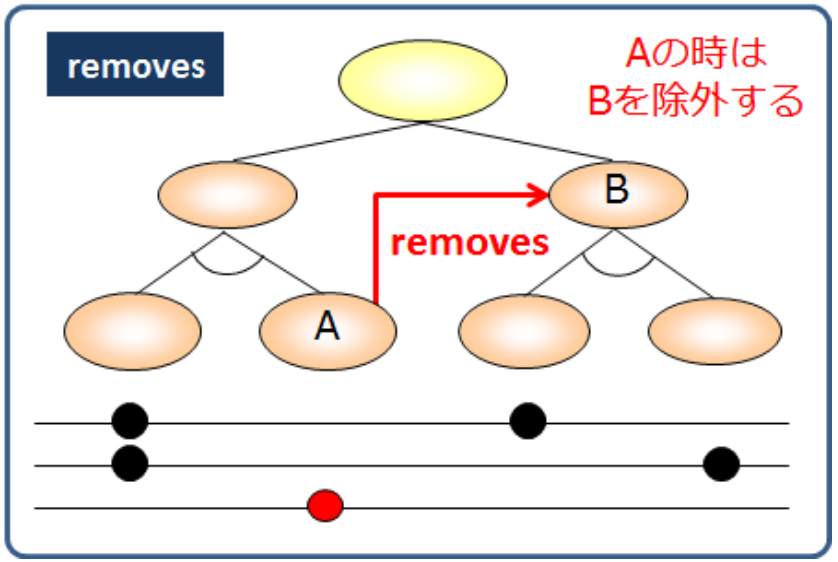
ZIPC FOTのフィーチャーモデル表現

フィーチャーモデル表現に必要な４つの制約









まとめ

- **モデリング技術**

  用途に応じて、最適なモデリング技術を選ぶ

- **我が国の情報セキュリティ政策**

  年々、多様化・複雑化する情報セキュリティ政策には、組込み業界と同じ問題がある

- **トレサビツールによるセキュリティポリシーの管理**

  理想的な計画文書の管理方法の紹介

- **管理策のモデル化**

  考え方をモデルに反映して、暗黙知や「欄外ルール」をなくす