

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

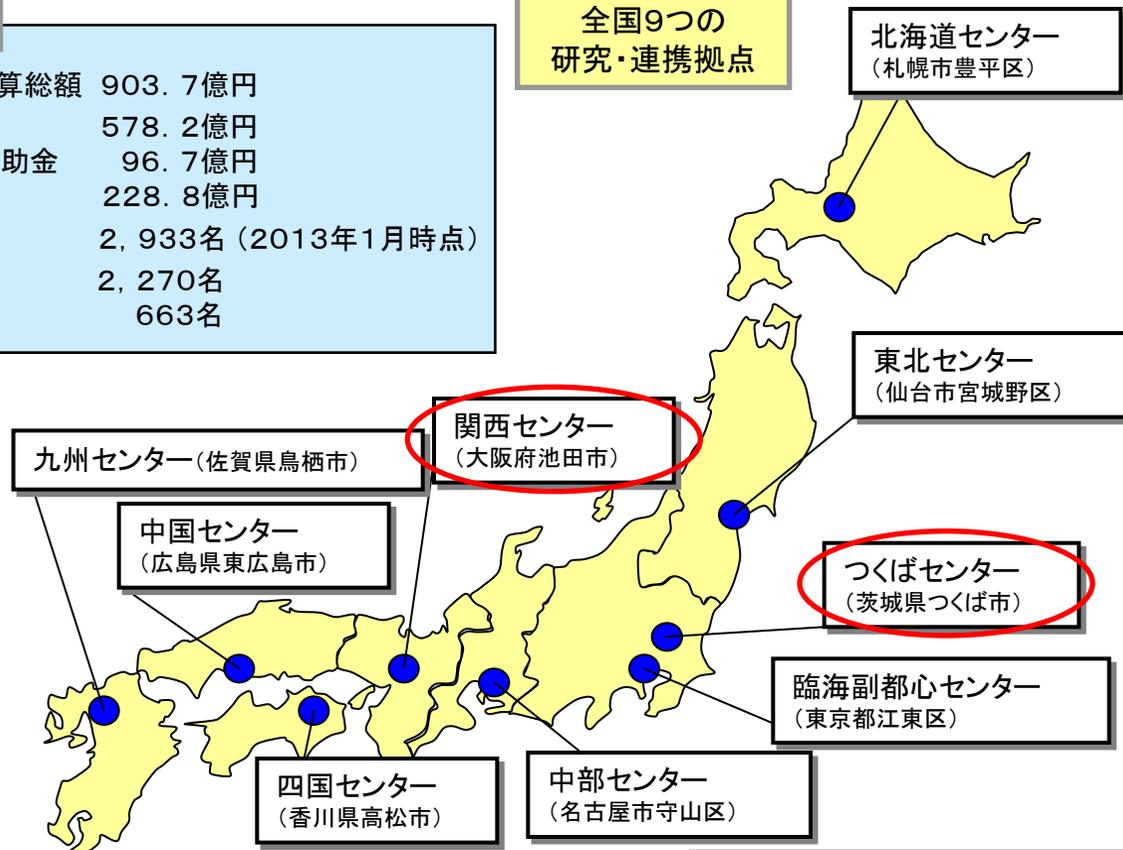
目的

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



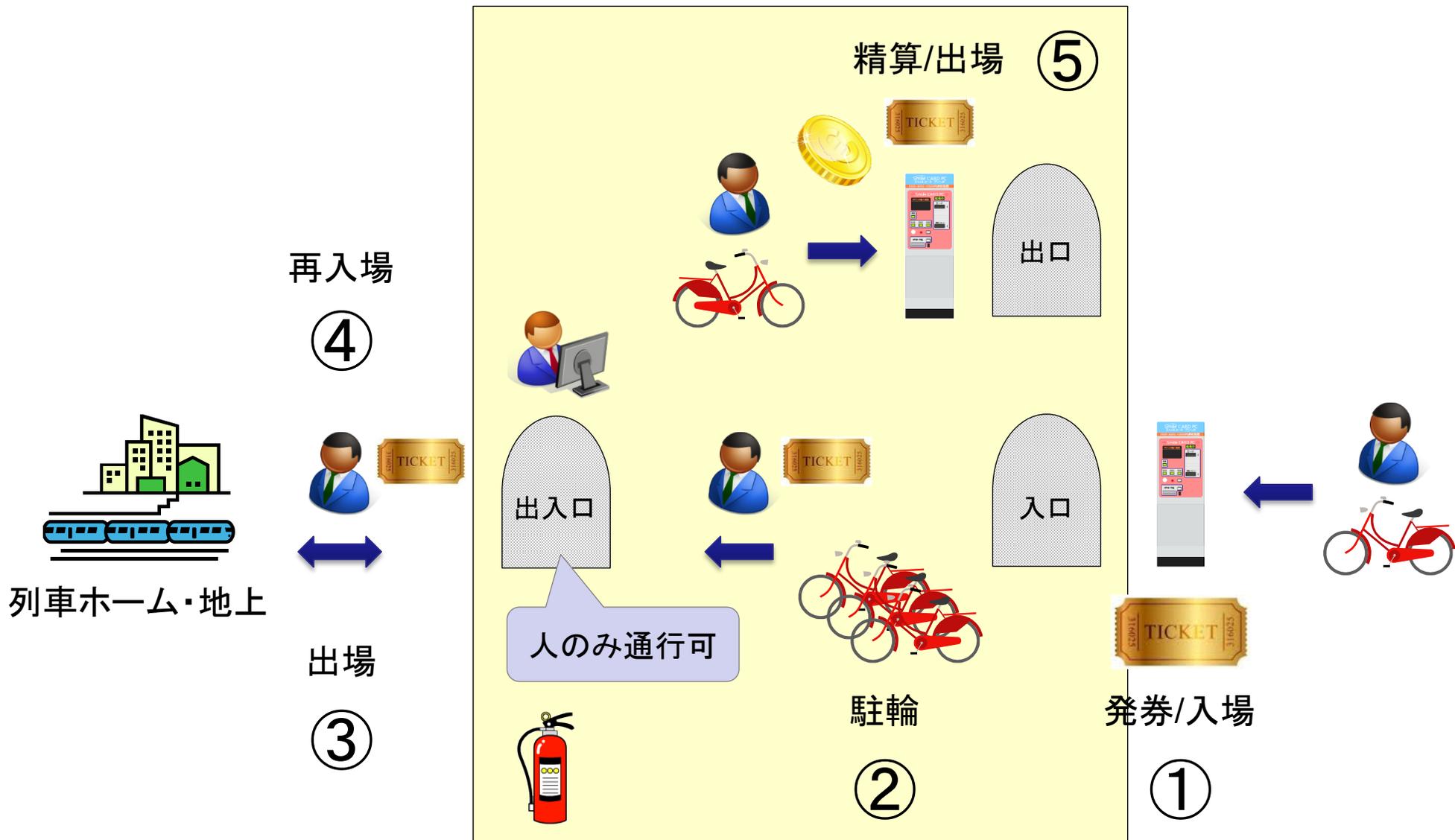
・ 水素吸蔵合金とニッケル水素電池

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

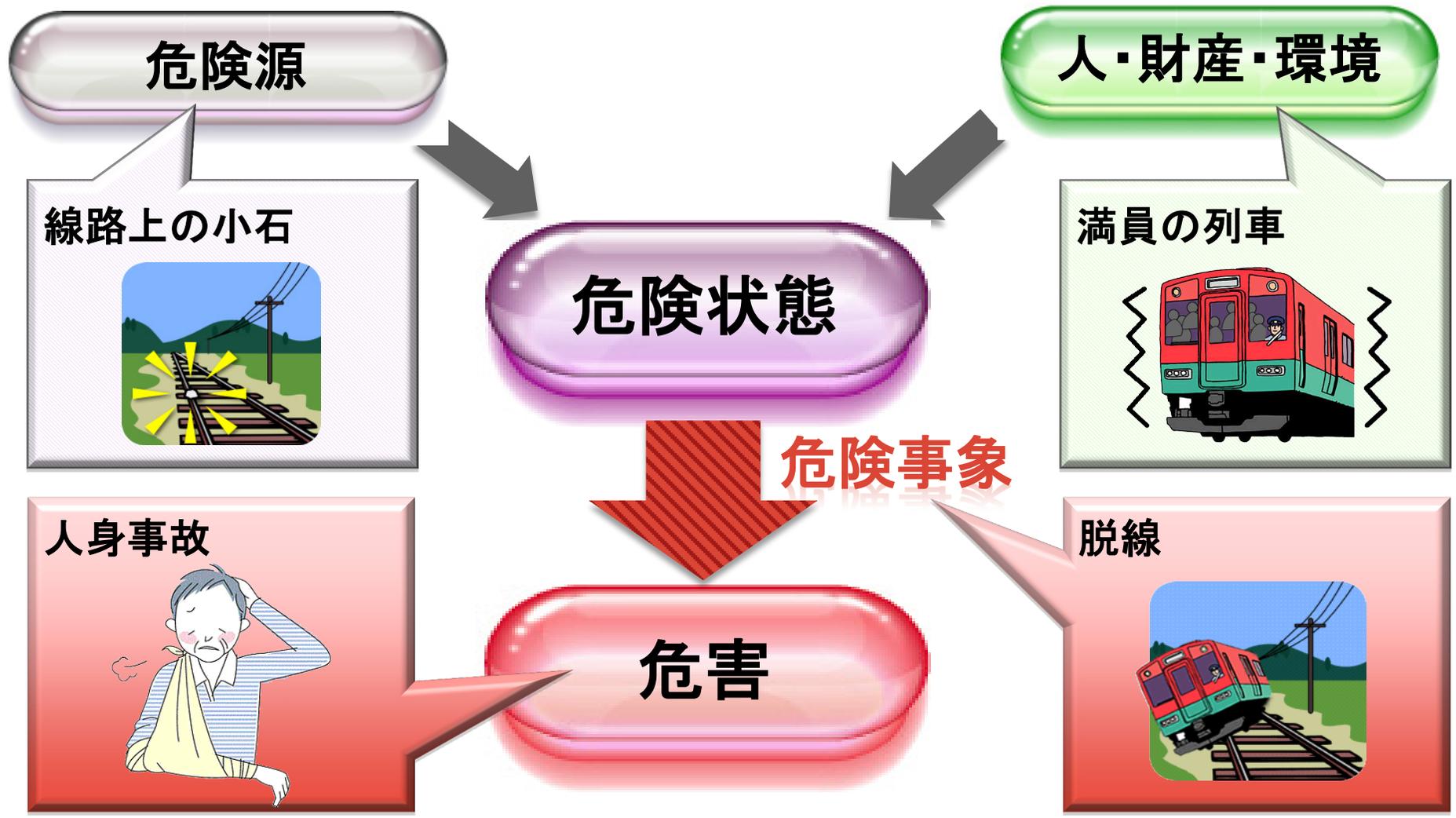
とある駐輪場



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



リスクを軽減するための要件

絶対安全

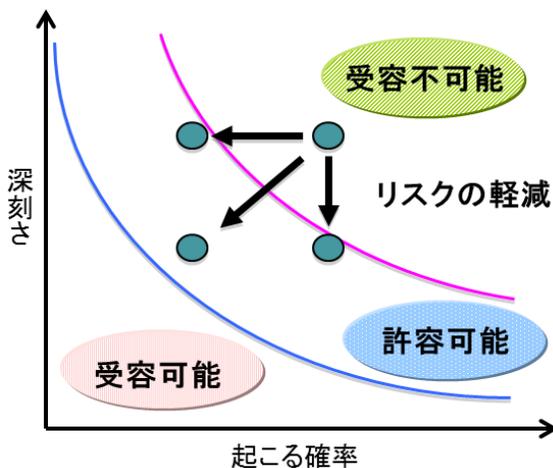
高品質のよい製品を作ることに労力を集中させる



立体交差

「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拠を整備



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】

- 受容不可能なリスク 論外

- 受容不可能でないリスク

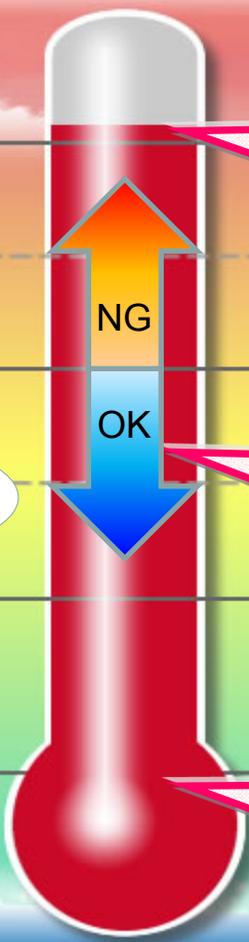
- 許容不可能なリスク 許せない

- 許容不可能でないリスク 条件付き
よし

- 許容可能なリスク

- 受容可能なリスク まあよし

- 無視可能なリスク 問題なし



信号機の制御装置
(野ざらしのため雨でさびる)

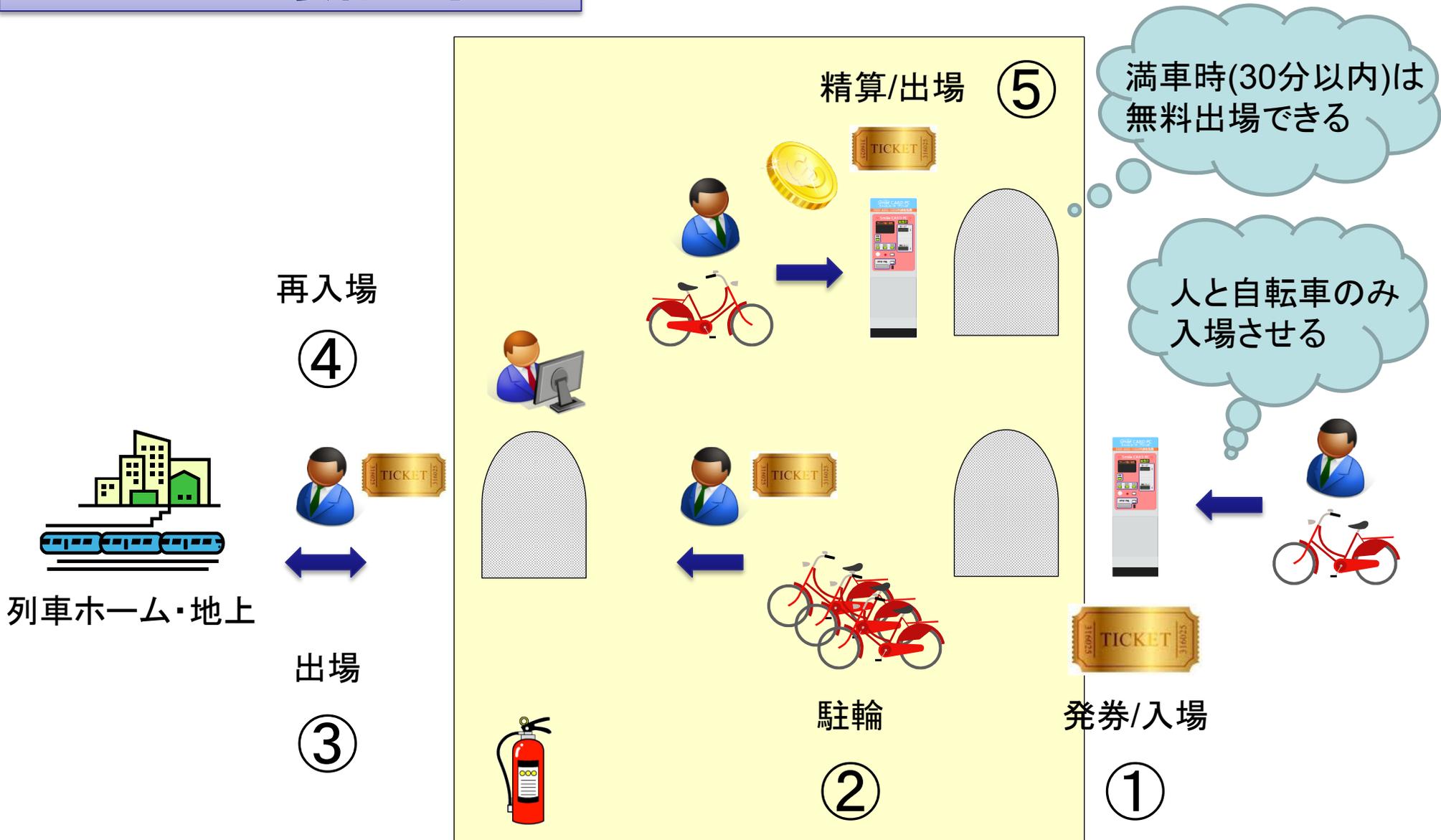
信号機の制御装置
(防水カバーつき)

信号機の制御装置
(さびないように純金製)

IEC 61508-5で示されるALARP原理

【制御システムの安全】

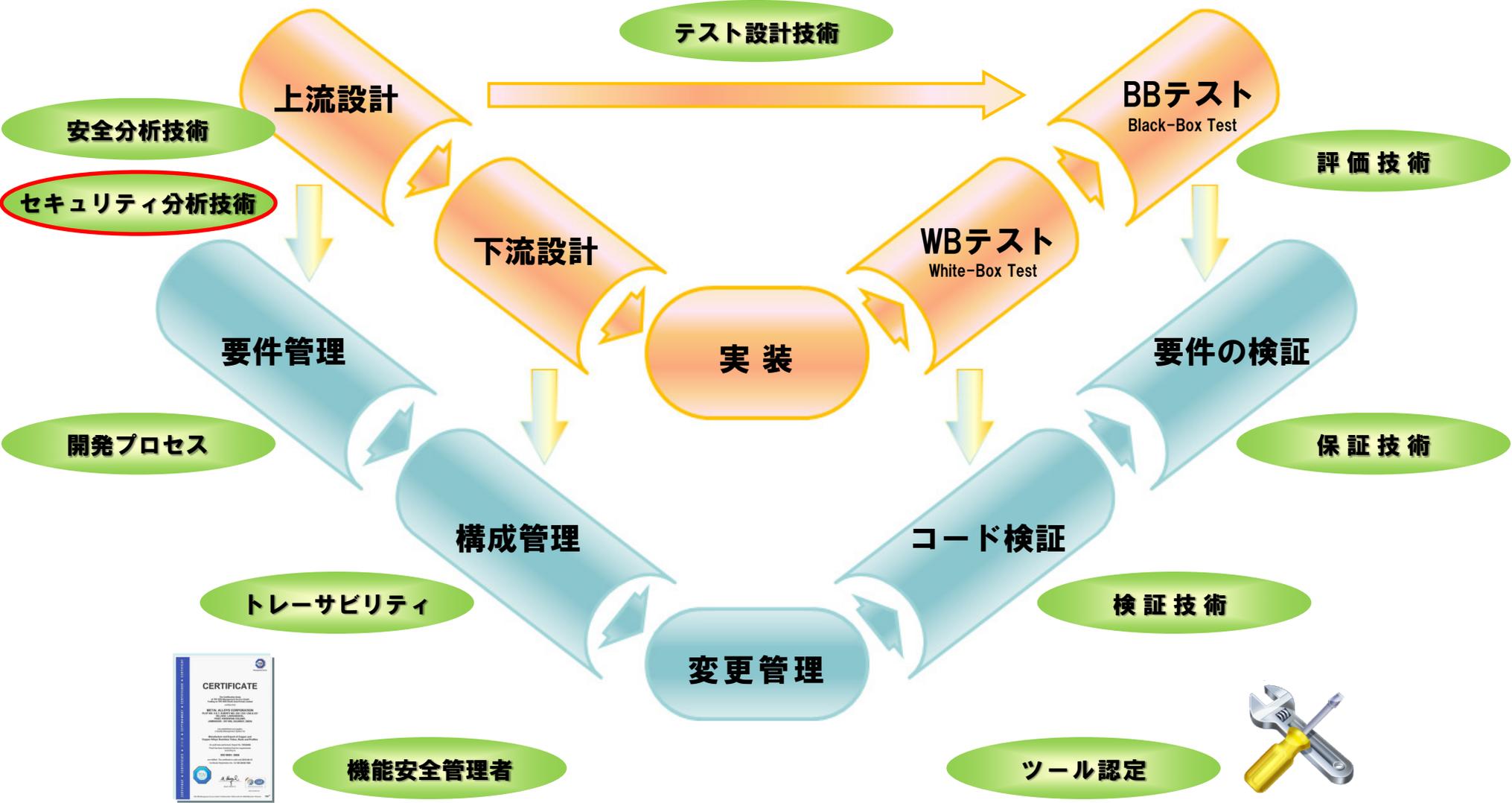
セキュリティ要件を考える



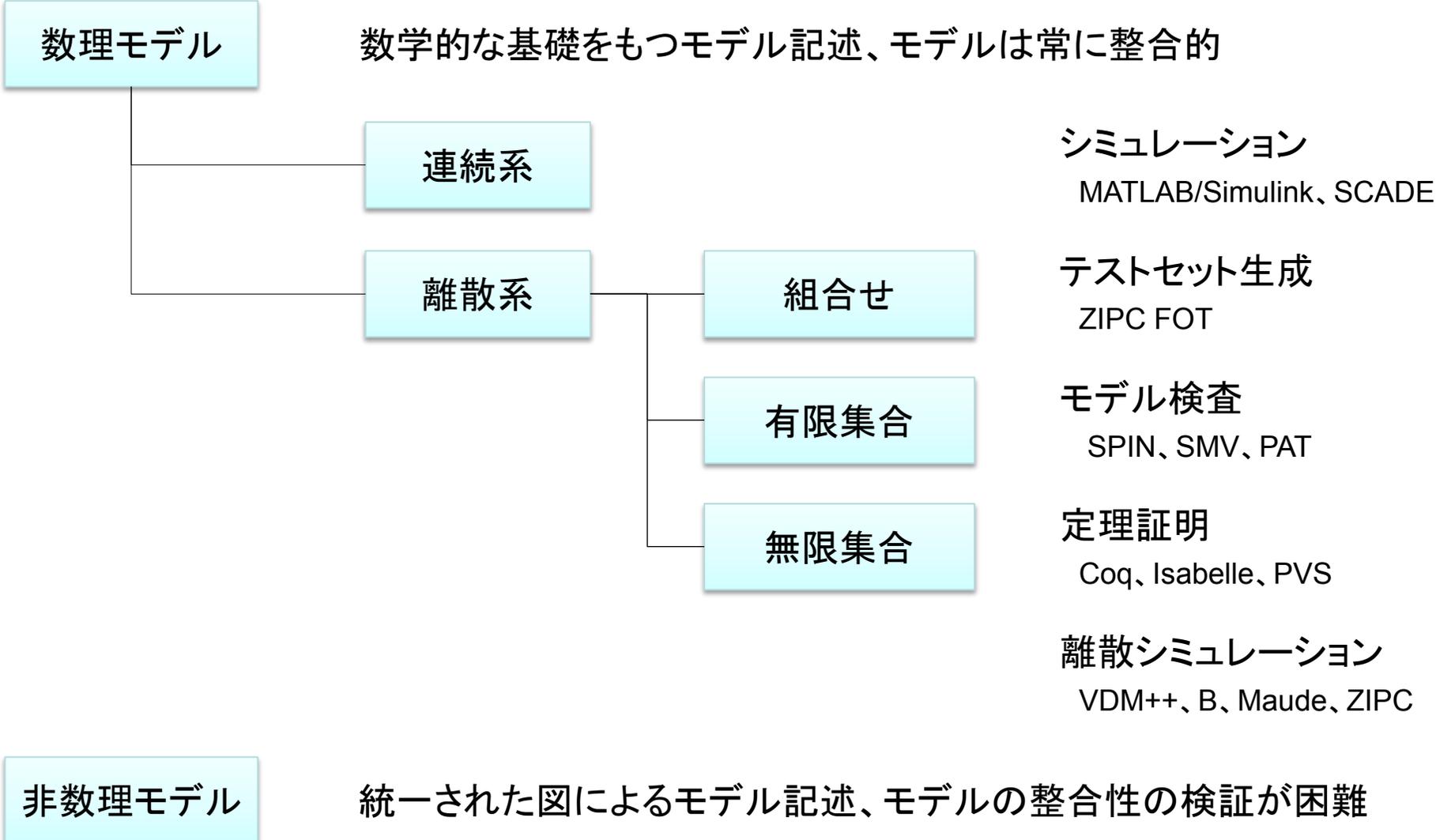
情報セキュリティとリスク

- 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**
外的要因
対して、情報を使用させず、また、開示しない特性。
- 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。
リスク源
被害の度合
弱点
- 情報セキュリティリスクは、脅威が情報資産のぜい弱性又は情報
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)

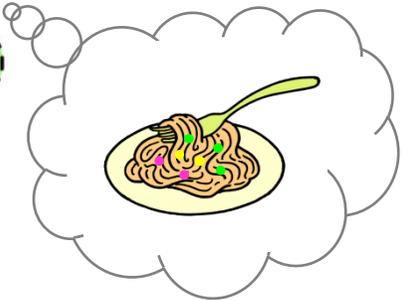
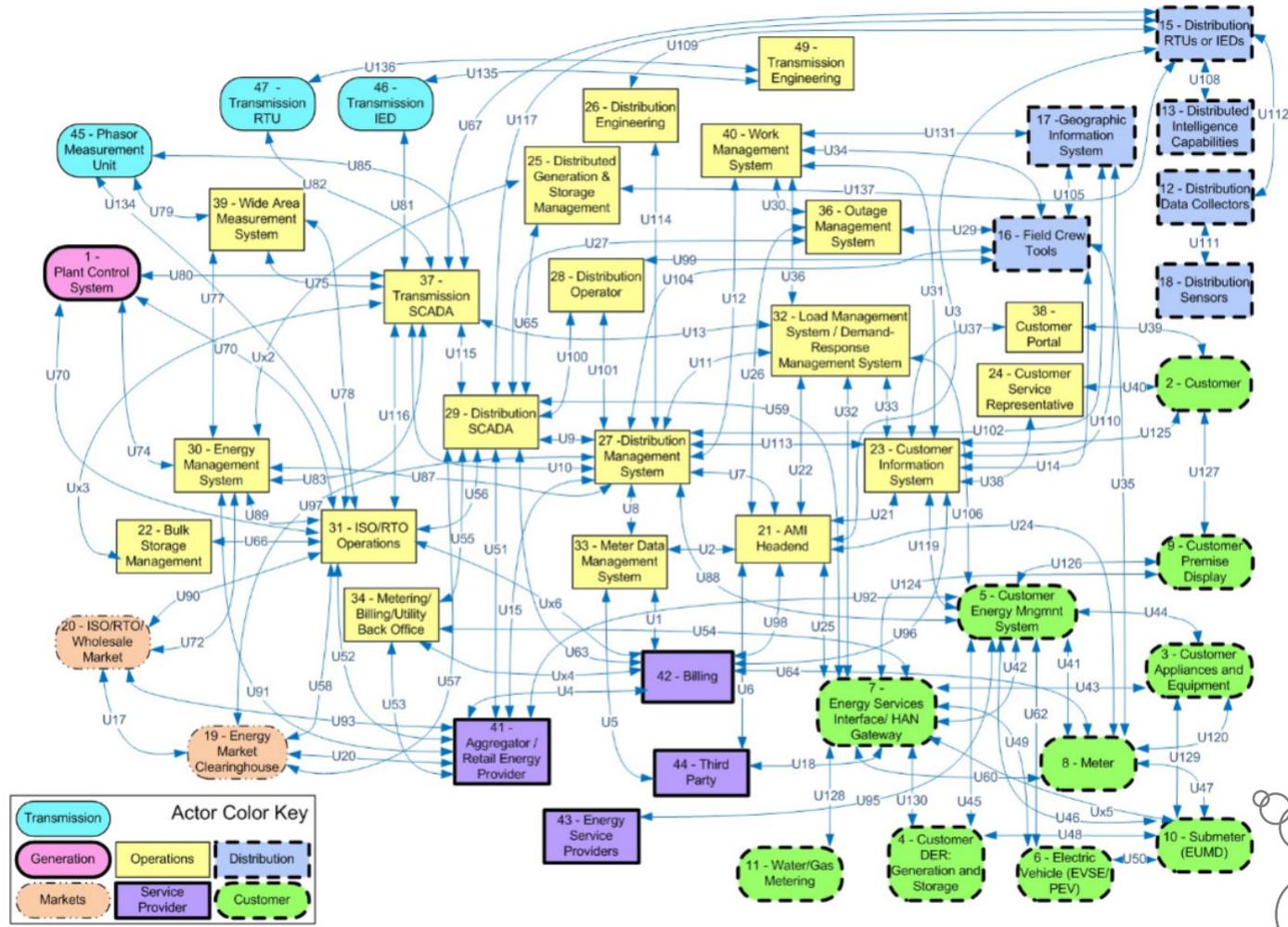
開発工程（V字開発）と開発技術



分析のためのモデリング技術



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)

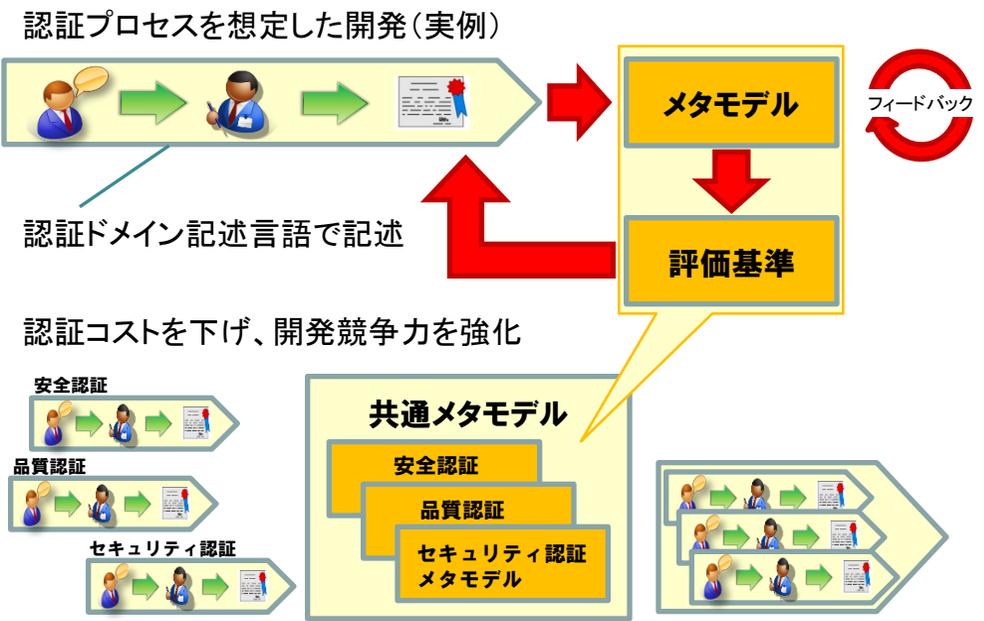
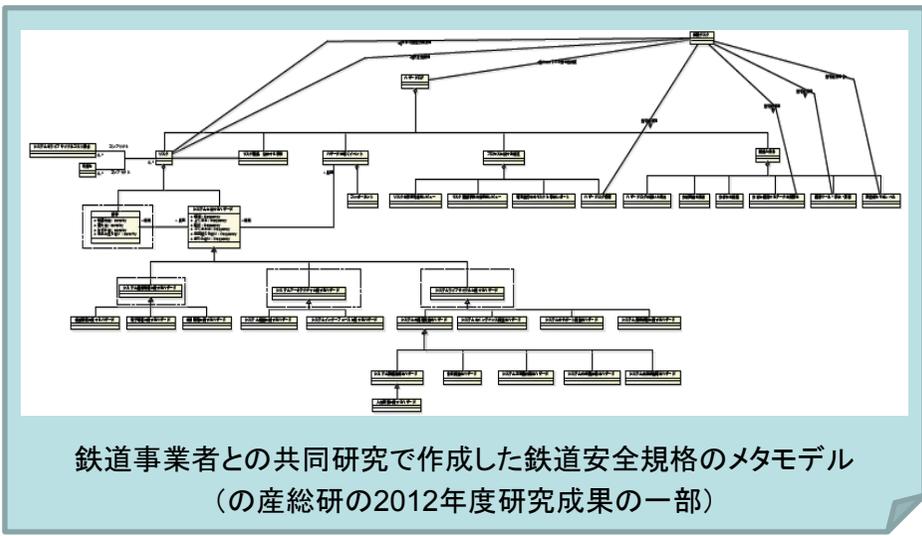
保証技術とメタモデリング

- 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



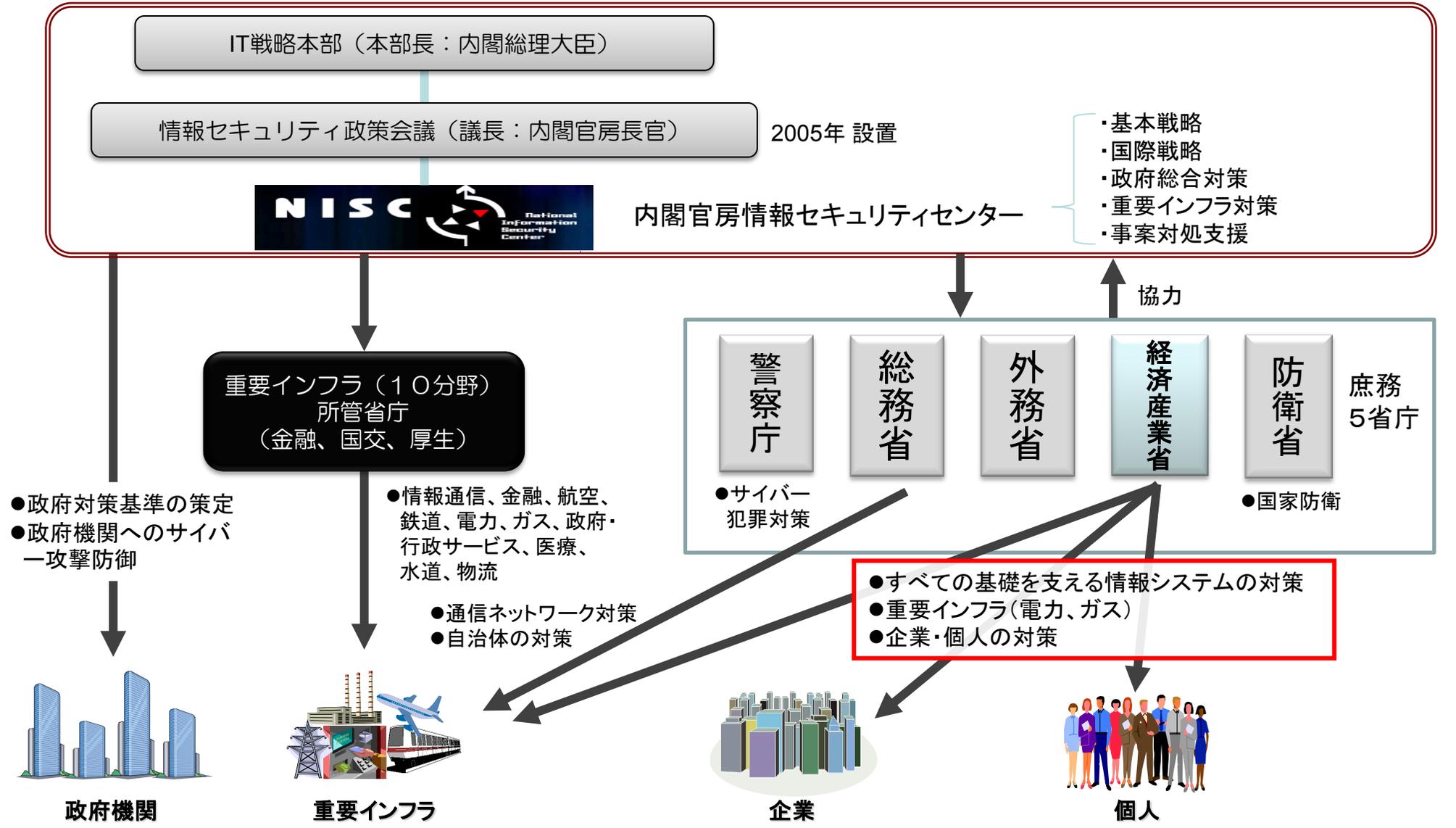
安全認証プロセスのための技術が必要

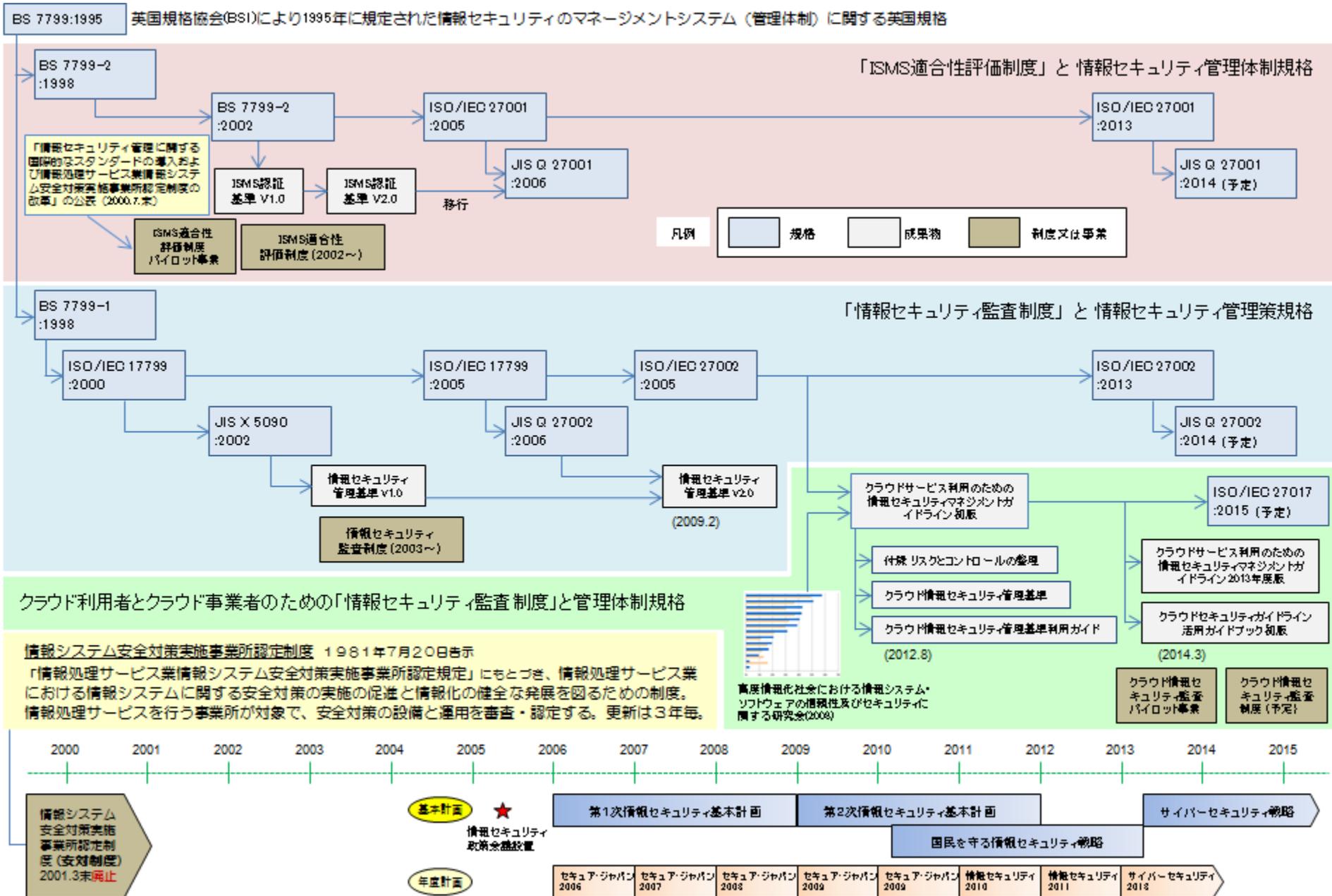
メタモデリング



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





重要インフラのセキュリティ対策

(1) 基本戦略

サイバーセキュリティ戦略
はじめに
1. 環境の変化
(1) サイバー空間の拡大・浸透
① サイバー空間と実空間の「融合・一体化」の進展
② サイバー空間を取り巻く「リスクの深刻化」
(2) これまでの取組
(3) 国際的な動向
2. 基本的な方針
(1) 目指すべき社会像
(2) 基本的な考え方
① 情報の自由な流通の確保
② 深刻化するリスクへの新たな対応
③ リスクベースによる対応の強化
④ 社会的責務を踏まえた行動と共助
(3) 各主体の役割
① 国の役割
② 重要インフラ事業者等の役割
③ 企業や教育・研究機関の役割
④ 一般利用者や中小企業の役割
⑤ サイバー空間関連事業者の役割
3. 取組分野
(1) 「強靱な」サイバー空間の構築
① 政府機関等における対策
② **重要インフラ事業者等における対策**
③ 企業・研究機関等における対策
④ サイバー空間の衛生
⑤ サイバー空間の犯罪対策
⑥ サイバー空間の防衛
(2) 「活力ある」サイバー空間の構築
① 産業活性化
② 研究開発
③ 人材育成
④ リテラシー向上
(3) 「世界を率先する」サイバー空間の構築
① 外交
② 国際展開
③ 国際連携
4. 推進体制等
(1) 推進体制等
(2) 評価等

(2) 年次計画

サイバーセキュリティ2013
I はじめに
II 具体的な取組み分野
1 「強靱な」サイバー空間の構築
① 政府機関等における
② **重要インフラ事業者等における**
③ 企業・研究機関等における対策
④ サイバー空間の衛生
⑤ サイバー空間の犯罪対策
⑥ サイバー空間の防衛
2 「活力ある」サイバー空間の構築
① 産業活性化
② 研究開発
③ 人材育成
④ リテラシー
3 「世界を率先する」サイバー空間の構築
① 外交
② 国際展開
③ 国際連携
4 推進体制等

重要インフラ第2次行動計画改訂版
I 総論
1 目標
2 定義と対象範囲
3 第1次行動計画の成果
4 第2次行動計画期間における取組みの要点
5 行動計画の改定
II 計画期間内に取り組む情報セキュリティ対策
1 安全基準等の整備及び浸透
2 情報共有体制の強化
3 **共通脅威分析**
4 **分野横断的演習**
5 **環境変化への対応**
III 関係主体において取り組むべき事項
1 推進体制
2 各主体の取組み
IV 評価・検証と見直し
1 行動計画の推進体制
2 既存の情報共有体制との連携

次期計画
策定要求

具体化

次期計画
策定要求

見直し
要求

改訂項目例
(統合整理)

(3) 分野別計画(事例)

重要インフラ第3次行動計画案
I. 総論
1. 行動計画策定に当たっての認識
2. 重要インフラ防護の目的の明確化
3. 第2次行動計画の施策の成果と課題
4. 考慮すべき課題
5. 重要インフラの範囲の見直しについて
6. 本行動計画策定に当たっての検討結果
II. 本行動計画の要点
III. 計画期間内に取り組む情報セキュリティ対策
1. 安全基準等の整備及び浸透
2. 情報共有体制の強化
3. 障害対応体制の強化
4. **リスクマネジメント**
5. **防護基盤の強化**
IV. 関係主体において取り組むべき事項
1. 内閣官房の施策
2. 重要インフラ所管省庁の施策
3. 事案対処省庁の施策
4. 重要インフラ事業者等の自主的な対策として期待する事項
5. セクターの自主的な対策として期待する事項
6. セクター・カウンシルの自主的な対策として期待する事項
7. 情報セキュリティ関係機関の自主的な取組として期待する事項
8. サイバー空間関連事業者の自主的な対策として期待する事項
V. 評価・検証と見直し
1. 本行動計画期間の目標(理想とする将来像)
2. 各年度における進捗状況の確認・検証を通じた対策・施策の継続的改善
3. 各年度における進捗状況の確認・検証の実施方法
4. 行動計画期間の成果の評価に基づく行動計画の見直し

改訂



基本計画、年次計画、分野別計画

(1) 基本戦略(サイバーセキュリティ戦略)

- はじめに
- 1. 環境の変化
- 2. 基本的な方針
- 3. 取組分野
- (1)「強靱な」サイバー空間の構築
- ①政府機関等における対策
- ②重要インフラ事業者等における対策**
- ③企業・研究機関等における対策
- ④サイバー空間の衛生
- ⑤サイバー空間の犯罪対策
- ⑥サイバー空間の防衛
- (2)「活力ある」サイバー空間の構築
-

(2) 年次計画(サイバーセキュリティ2013)

- I はじめに
- II 具体的な取組み分野
- 1 「強靱な」サイバー空間の構築
- ① 政府機関等における
- ② 重要インフラ事業者等における
- (ア)新たな「行動計画」の策定**
- (イ)「安全基準等」策定方針及び重要インフラ分野における「安全基準等」の継続的改善**
- (ウ)「安全基準等」の整備浸透状況調査**
-

(3) 分野別計画(重要インフラ第3次行動計画案)

- I. 総論
- 1. 行動計画策定に当たっての認識
- 2. 重要インフラ防護の目的の明確化
- 3. 第2次行動計画の施策の成果と課題
- 4. 考慮すべき課題
- 5. 重要インフラの範囲の見直しについて
- 6. 本行動計画策定に当たっての検討結果
- II. 本行動計画の要点
- III. 計画期間内に取り組む情報セキュリティ対策
- 1. 安全基準等の整備及び浸透
-
-
-
-
-

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）

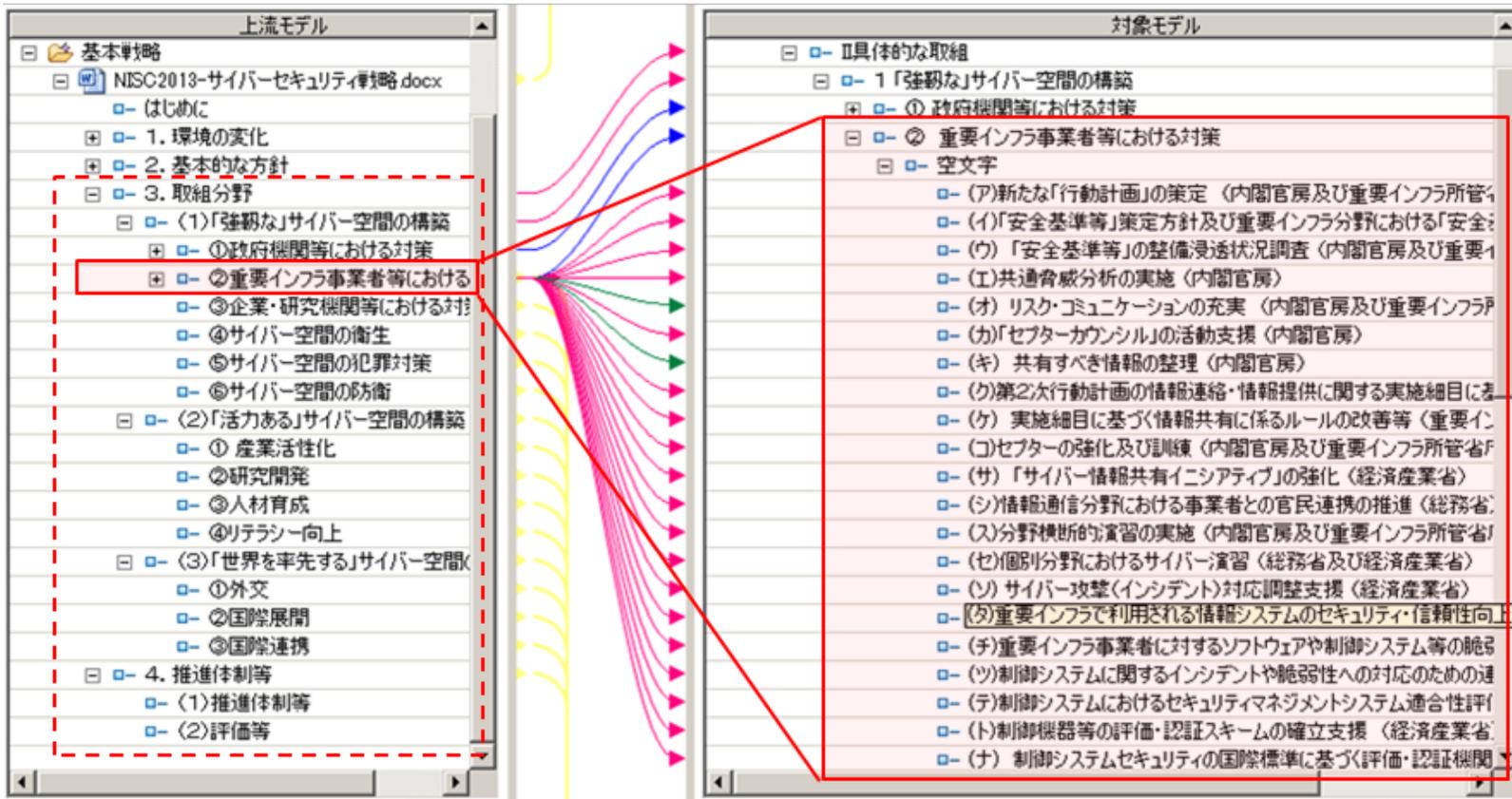
詳細化

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）

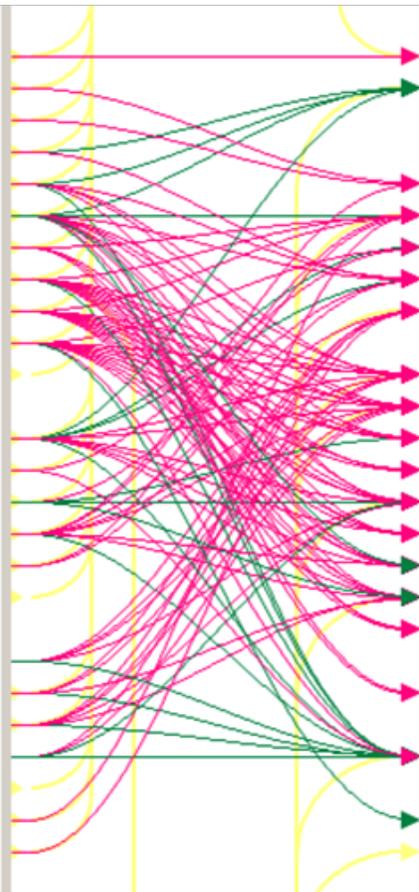


弱い関係（緑色）、デフォルト（青色）、強い関係（ピンク色）、表示範囲外（黄色）

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）

対象モデル
<input type="checkbox"/> (ア)新たな「行動計画」の策定（内閣官房及び重
<input type="checkbox"/> (イ)「安全基準等」策定方針及び重要インフラ分野
<input type="checkbox"/> (ウ)「安全基準等」の整備浸透状況調査（内閣
<input type="checkbox"/> (エ)共通脅威分析の実施（内閣官房）
<input type="checkbox"/> (オ) リスク・コミュニケーションの充実（内閣官房及
<input type="checkbox"/> (カ)「セクターカウンシル」の活動支援（内閣官房）
<input type="checkbox"/> (キ) 共有すべき情報の整理（内閣官房）
<input type="checkbox"/> (ク)第2次行動計画の情報連絡・情報提供に関
<input type="checkbox"/> (ケ) 実施細目に基づく情報共有に係るルール
<input type="checkbox"/> (コ)セクターの強化及び訓練（内閣官房及び重要
<input type="checkbox"/> (サ)「サイバー情報共有イニシアティブ」の強化（
<input type="checkbox"/> (シ)情報通信分野における事業者との官民連携
<input type="checkbox"/> (ス)分野横断的演習の実施（内閣官房及び重要
<input type="checkbox"/> (セ)個別分野におけるサイバー演習（総務省及び
<input type="checkbox"/> (シ)サイバー攻撃（インシデント）対応調整支援（
<input type="checkbox"/> (タ)重要インフラで利用される情報システムのセキュ
<input type="checkbox"/> (チ)重要インフラ事業者に対するソフトウェアや制御
<input type="checkbox"/> (ツ)制御システムに関するインシデントや脆弱性への
<input type="checkbox"/> (テ)制御システムにおけるセキュリティマネジメントシ
<input type="checkbox"/> (ト)制御機器等の評価・認証スキームの確立支援
<input type="checkbox"/> (ナ) 制御システムセキュリティの国際標準に基づく
<input type="checkbox"/> (ニ)制御システムセキュリティ評価・認証の国際相
<input type="checkbox"/> (ヌ)制御システムセキュリティ評価・認証の利活用
<input type="checkbox"/> (ネ) ソフトウェア、情報システムの信頼性向上（
<input type="checkbox"/> (ノ)大規模サイバー攻撃事態等発生時の初動対
<input type="checkbox"/> (ハ) 重要インフラ事業者における人材育成の促



重要インフラ第3次行動計画
（一部）

下流モデル
<input type="checkbox"/> 第3次行動計画:重要インフラの情報セキュリティ
<input type="checkbox"/> I. 総論
<input type="checkbox"/> II. 本行動計画の要点
<input type="checkbox"/> III. 計画期間内に取り組む情報セキュリティ
<input type="checkbox"/> 1. 安全基準等の整備及び浸透
<input type="checkbox"/> 2. 情報共有体制の強化
<input type="checkbox"/> 3. 障害対応体制の強化
<input type="checkbox"/> 4. リスクマネジメント
<input type="checkbox"/> 5. 防護基盤の強化
<input type="checkbox"/> IV. 関係主体において取り組むべき事項
<input type="checkbox"/> 1. 内閣官房の施策
<input type="checkbox"/> 2. 重要インフラ所管省庁の施策
<input type="checkbox"/> 3. 情報セキュリティ関係省庁の施策
<input type="checkbox"/> 4. 事案対応省庁の施策
<input type="checkbox"/> 5. 重要インフラ事業者等の自主的な
<input type="checkbox"/> 6. セクターの自主的な対策として期待
<input type="checkbox"/> 7. セクターカウンシルの自主的な対策
<input type="checkbox"/> 8. 情報セキュリティ関係機関の自主的
<input type="checkbox"/> 9. サイバー空間関連事業者の自主的
<input type="checkbox"/> V. 評価・検証と見直し
<input type="checkbox"/> 1. 本行動計画期間の目標(理想とす
<input type="checkbox"/> 2. 各年度における進捗状況の確認
<input type="checkbox"/> 3. 各年度における進捗状況の確認
<input type="checkbox"/> 4. 行動計画期間の成果の評価に基
<input type="checkbox"/> 別添:情報連絡・情報提供について
<input type="checkbox"/> 別紙1 対象となる重要インフラ事業者等

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**

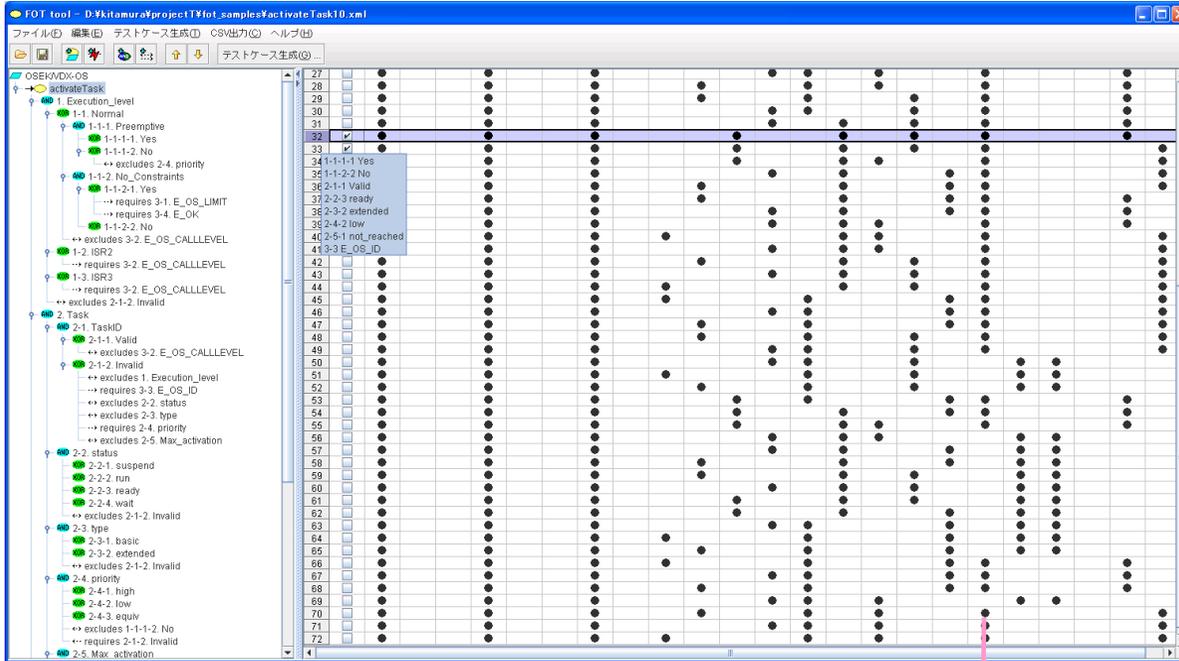
基本計画-年次計画、年次計画-分野別計画等の多重度分析

- **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



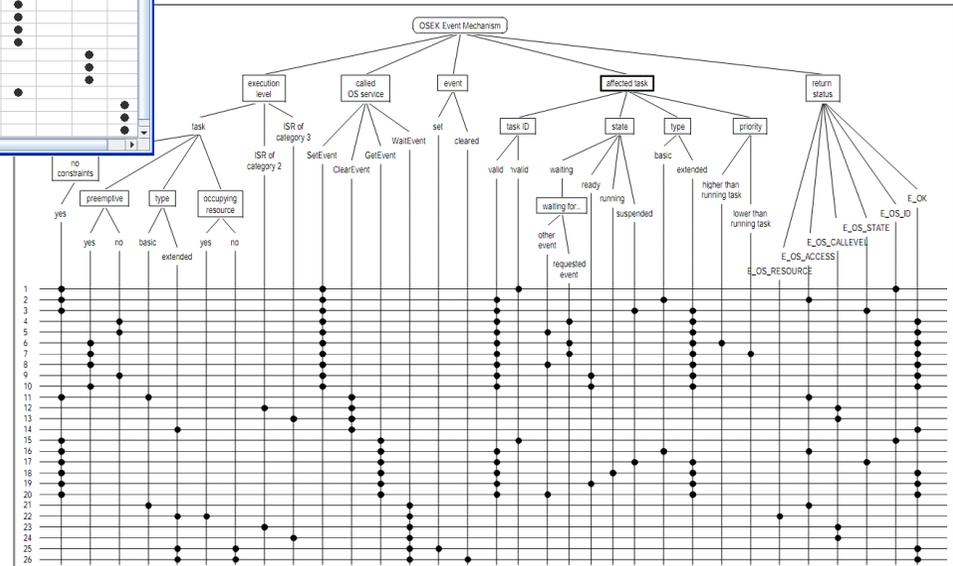
1. テスト設計

2. テスト生成

説明文書を自動で作成

3. ドキュメント化

自動生成による過不足のない
「安全な」テストセット



印刷イメージ

管理策のモデル化

ファイル(E) 編集(E) テストケース(T) CSV出力(C) ヘルプ(H)

ゴール

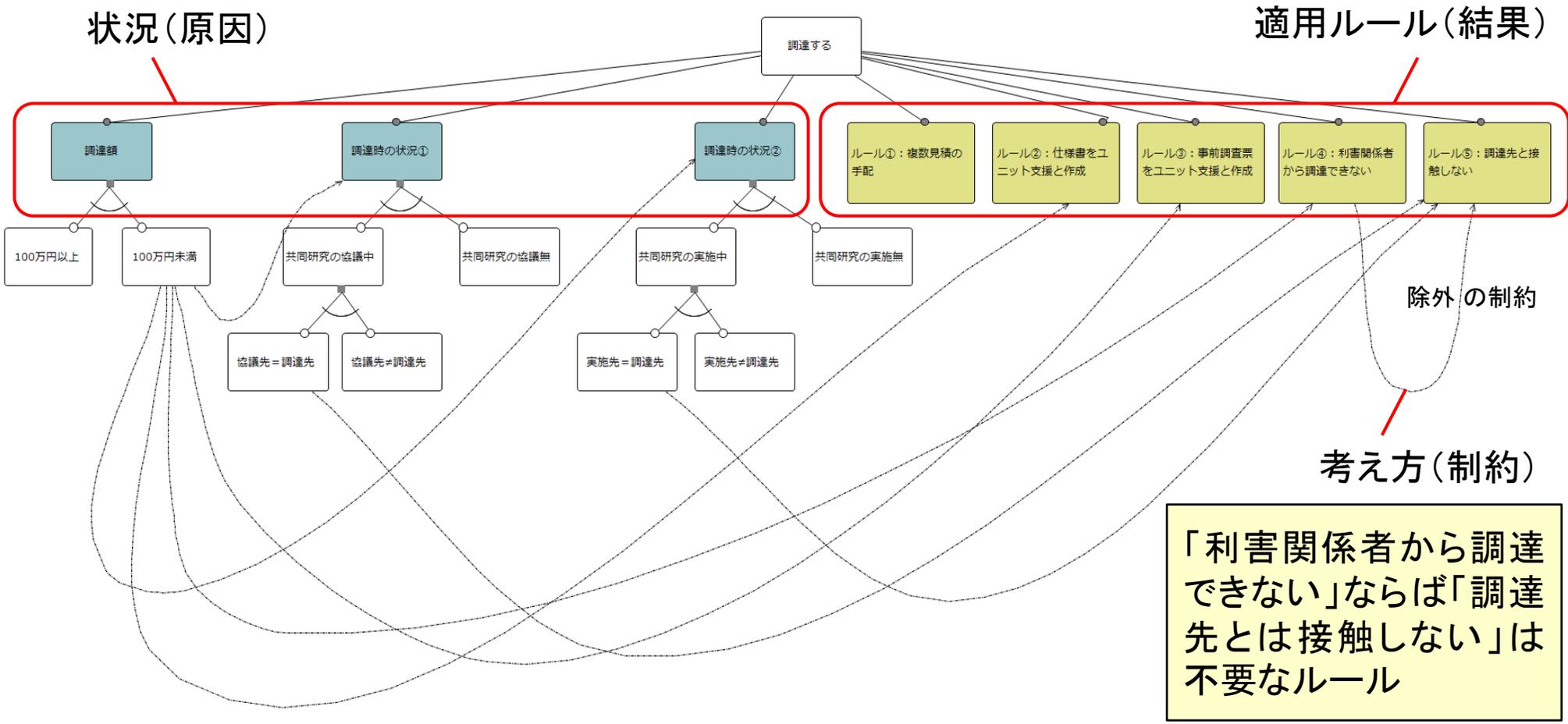
- AND 1. 調達額
 - AND 1-1. 100万円以上
 - attaches 9. ルール④：請求時にセルフチェックシートを作成
 - requires 10-1. 調達申請×切は2014年11...
 - AND 1-2. 100万円未満
 - removes 5. ルール②：発注仕様書のユニット支援との共同作成
 - removes 6. ルール③：事前調査票のユニット支援との共同作成
 - removes 7. ルール④：利害関係者からは調達できない
 - removes 8. ルール⑤：調達先との接触しない
 - removes 2. 調達中（開札まで）の状況①
 - removes 3. 調達中（開札まで）の状況②
 - requires 10-2. 調達申請×切は2015年1...
- AND 2. 調達中（開札まで）の状況①
 - AND 2-1. 共同研究の協議
 - AND 2-1-1. 協議先＝調達先（利害関係成立）
 - removes 8. ルール⑤：調達先との接触しない
 - AND 2-1-2. 協議先≠調達先
 - AND 2-2. 共同研究の協議無
 - removes 1-2. 100万円未満
- AND 3. 調達中（開札まで）の状況②
 - AND 3-1. 共同研究の実施
 - AND 3-1-1. 共同研究先＝調達先（利害関係成立）
 - removes 8. ルール⑤：調達先との接触しない
 - AND 3-1-2. 共同研究先≠調達先
 - AND 3-2. 共同研究の実施無
 - removes 1-2. 100万円未満
- AND 4. ルール①：複数見積の手配
- AND 5. ルール②：発注仕様書のユニット支援との共同作成
 - removes 1-2. 100万円未満
- AND 6. ルール③：事前調査票のユニット支援との共同作成
 - removes 1-2. 100万円未満
- AND 7. ルール④：利害関係者からは調達できない
 - removes 1-2. 100万円未満
 - removes 8. ルール⑤：調達先との接触しない
- AND 8. ルール⑤：調達先との接触しない
 - removes 1-2. 100万円未満
 - removes 2-1-1. 協議先＝調達先（利害関係成立）
 - removes 3-1-1. 共同研究先＝調達先（利害関係成立）
 - removes 7. ルール④：利害関係者からは調達できない
- AND 9. ルール⑥：請求時にセルフチェックシートを作成
 - attaches 1-1. 100万円以上
- AND 10. ルール⑦：調達申請期限（2014年度）
 - AND 10-1. 調達申請×切は2014年11月28日
 - requires 1-1. 100万円以上
 - AND 10-2. 調達申請×切は2015年1月30日
 - requires 1-2. 100万円未満

	済	1-1	1-2	2-1-1	2-1-2	2-2	3-1-1	3-1-2	3-2	4	5	6	7	8	9	10-1	10-2
1		●		●			●			●	●	●	●		●	●	
2		●		●				●		●	●	●	●		●	●	
3		●		●					●	●	●	●	●		●	●	
4		●			●		●			●	●	●	●		●	●	
5		●			●			●		●	●	●	●		●	●	
6		●			●				●	●	●	●	●		●	●	
7		●			●		●			●	●	●	●		●	●	
8		●			●			●		●	●	●	●		●	●	
9		●			●			●		●	●	●	●		●	●	
10			●							●							●

- 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 万円以上の案件に必要な作業
→ 複数の見積を手配
- 取得予定価格 100 万円以上の案件で必要な作業
→ 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

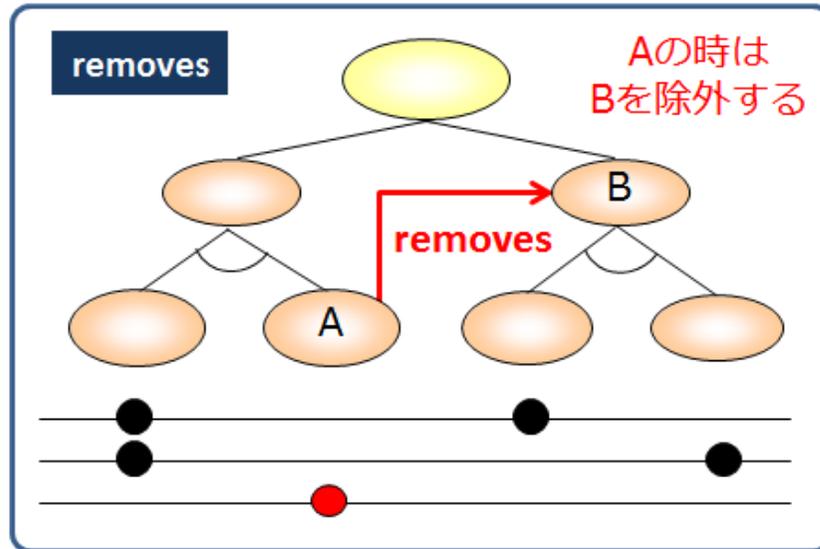
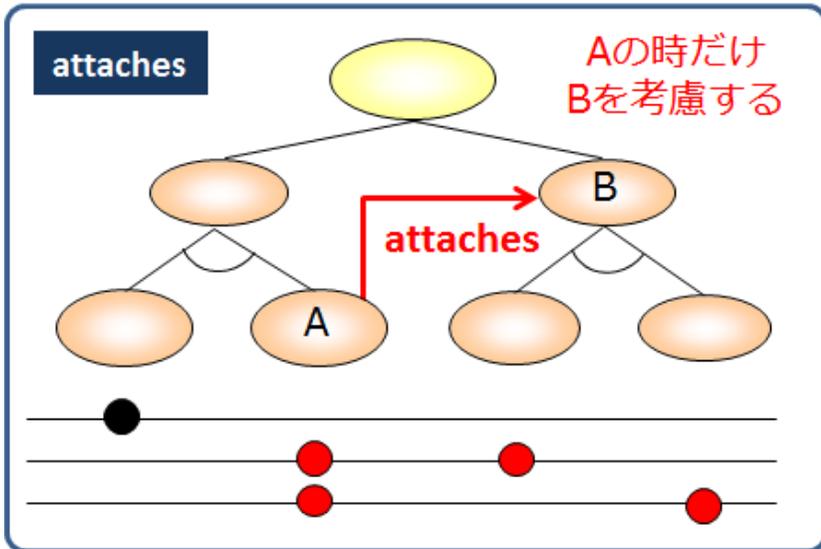
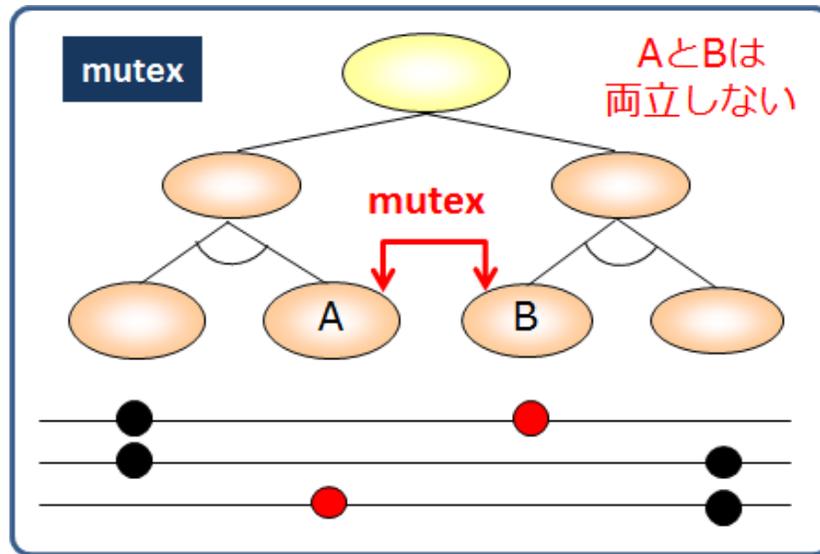
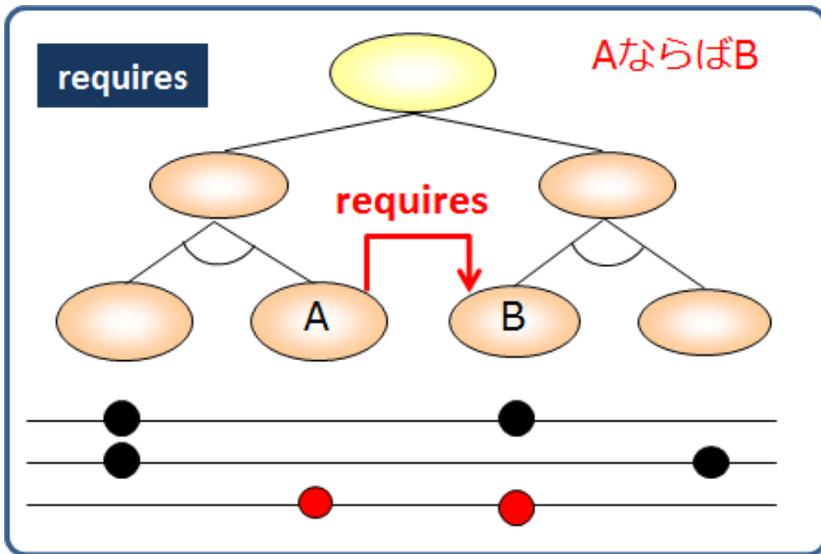
フィチャー数:22 制約数:12 テストケース数:10 ..\work\callPict.bat ""

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