成果発表会資料

多様なステークホルダの満足度に着目したシステムの安全性・セキュリティ要件の抽出と検証

System Requirements Analysis for Safety and Security with Multiple Stakeholder Perspectives on STAMP/STPA

2020年2月21日

日本科学技術連盟 2019年度 ソフトウェア品質管理研究会
研究コース５「要求と仕様のエンジニアリング」

研究員（チームGOBIT）：
ブラザー工業 株式会社　柳原 靖司
オムロン 株式会社　吉田 邦雄★
指導員：
ソニー 株式会社　栗田 太郎（主査）
国立情報学研究所　石川 冬樹（副主査）

Agenda

0. 研究コース５：要求工学上の位置づけ

1. 課題と背景、解決策の提案

2. 提案手法の説明

3. 実験

4. 実験結果

5. 考察・まとめ

“要求工学上”の研究の位置づけ

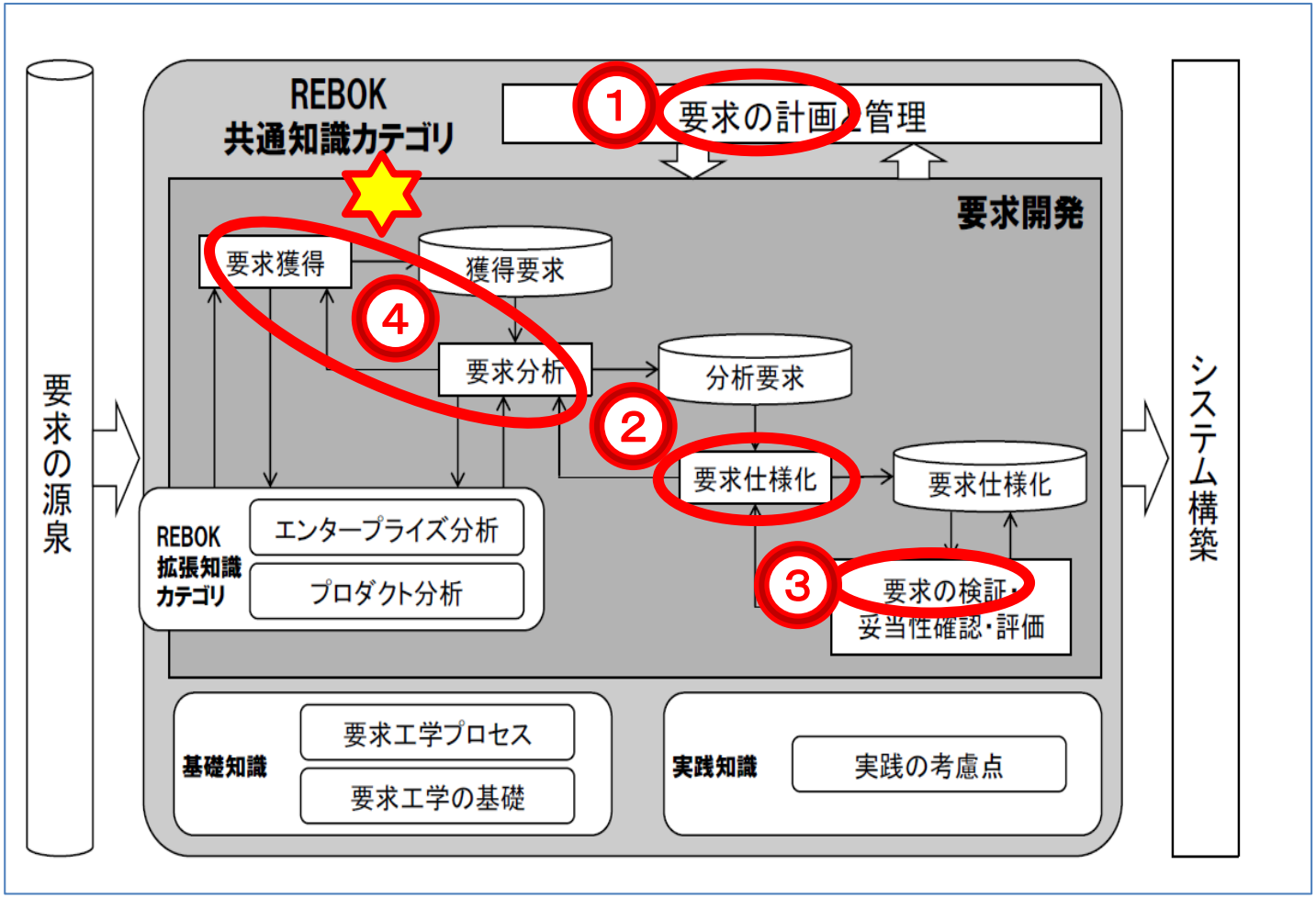
①チームＤＨＣ

②チームＫＮＴ

③チーム形式仕様

④チームGOBIT

↑　本発表



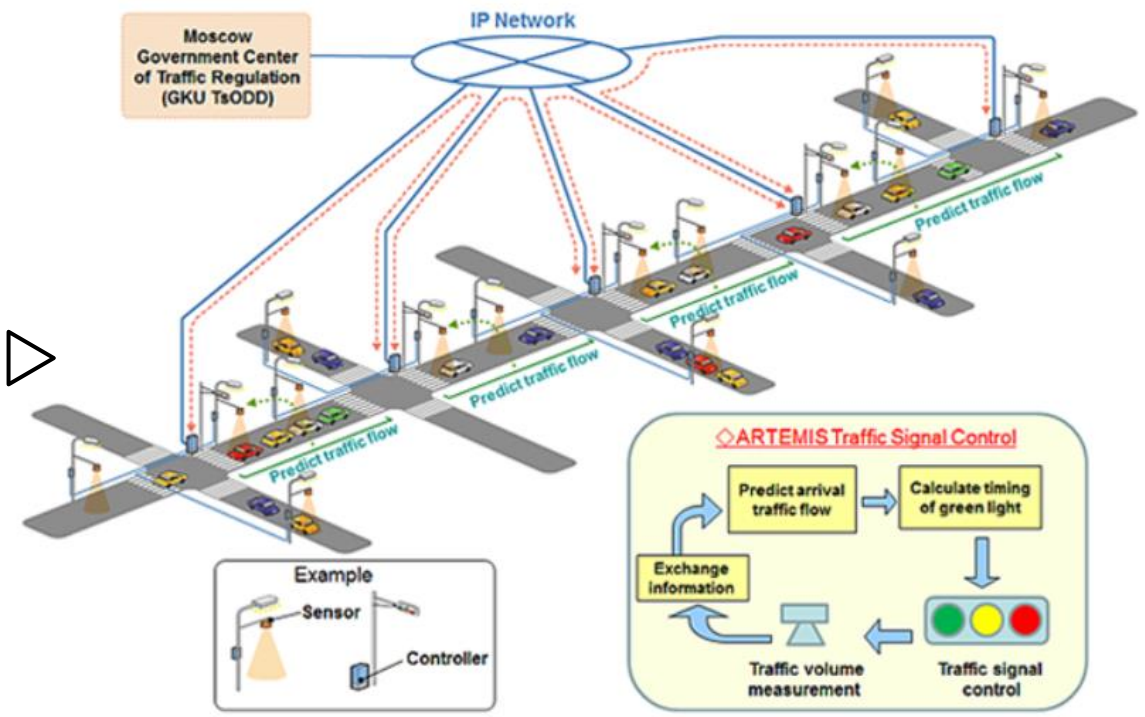
出典元：IPA　要求工学知識体系（REBOK）概説

課題と背景、解決策の提案

背景と課題：大規模化・複雑化するシステム開発

昭和9年　我が国初最初の押ボタン式信号機

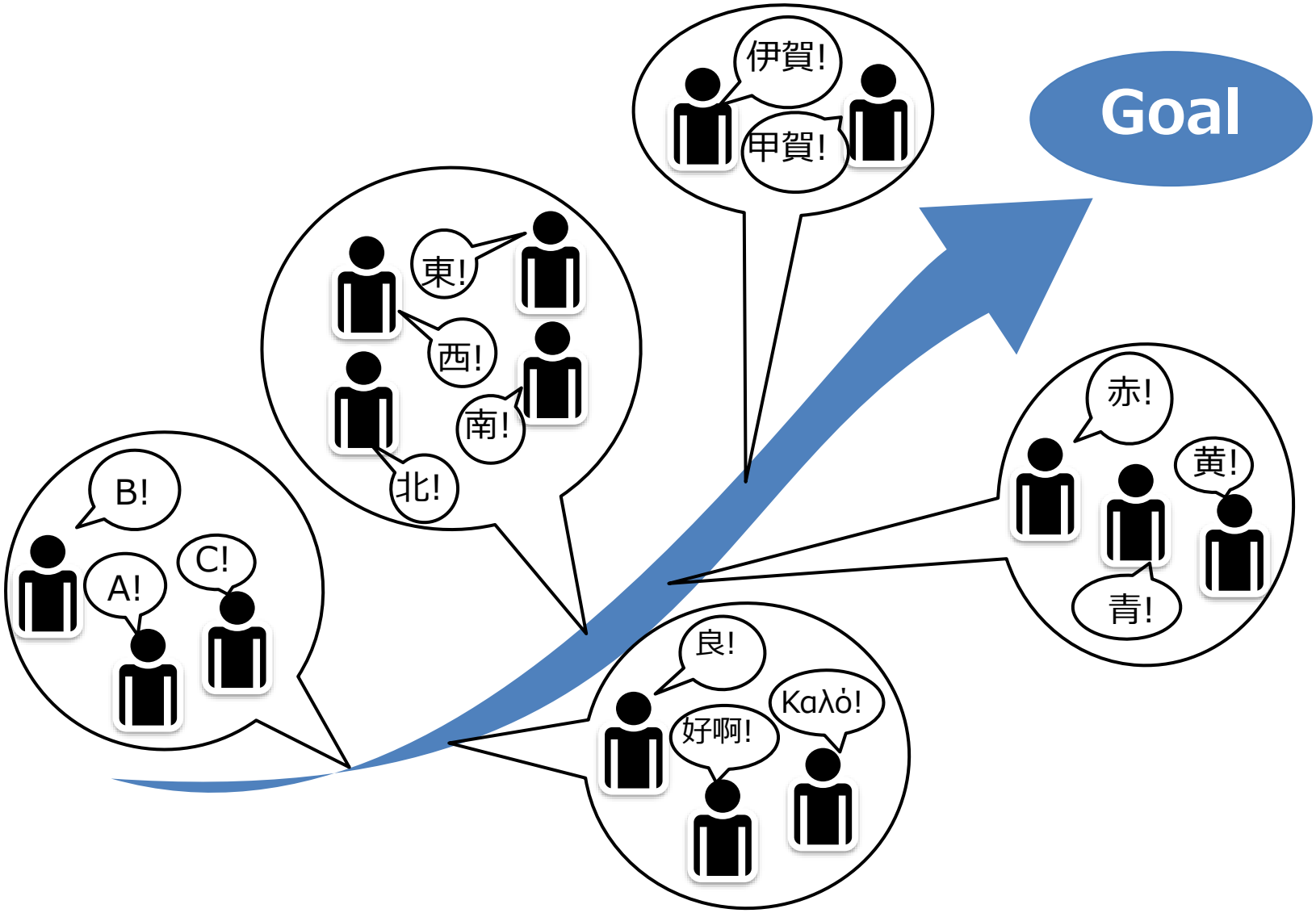
[出典]警察庁HP



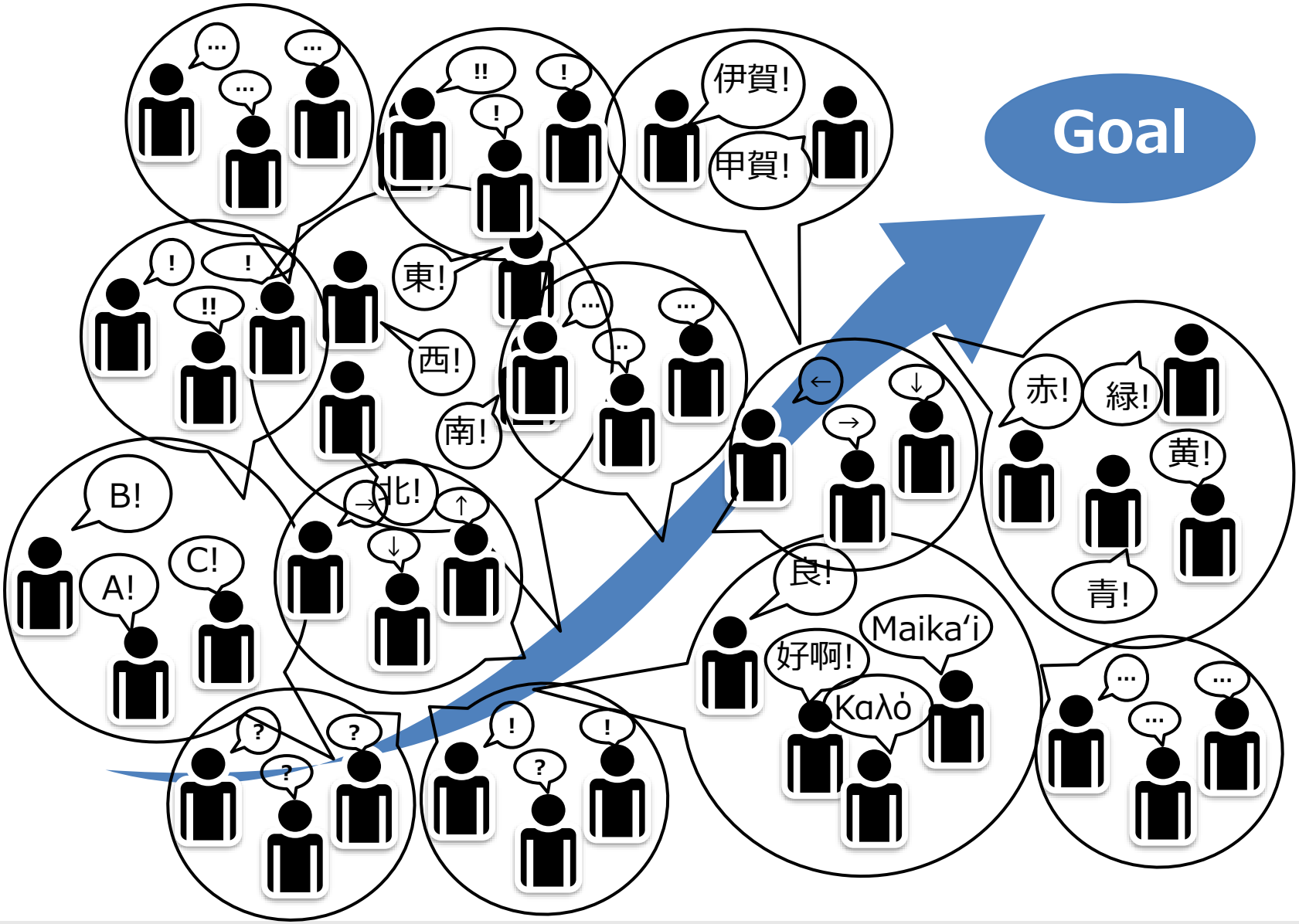
ロシア・モスクワ市における高度交通信号システム実証

[出典] NEDO　ニュースリリース　2017

背景と課題：多様化するステークホルダ



背景と課題：多様化するステークホルダ



背景と課題：要件定義フェーズの重要性は重々承知。だが。

要件定義は難しい

- 抜け漏れなくシステムの要件を抽出する
  ことが難しい
- ステークホルダ間で合意形成する
  ことが難しい

解決策の提案：要件定義の新しいプロセスモデルを提案

要件（安全性とセキュリティの対策）を

- 網羅的に抽出
  できる
- 定量的に評価
  できる

▷ ステークホルダ間の合意形成の促進に寄与

SSMS法

（**S**afety and **S**ecurity requirements analysis method with **M**ultiple stakeholder perspectives on **S**TAMP/STPA）

SSMS法の説明

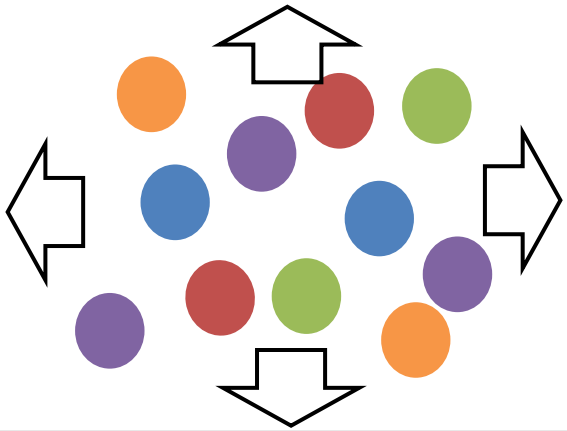
手法のアイデア

要件の抽出 → 要件の合意形成

システミック・アプローチによる要件の抽出

↓

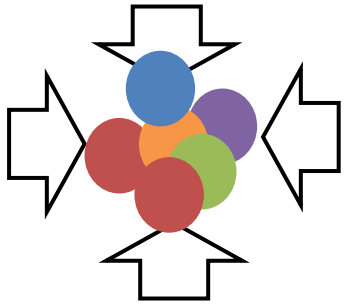
STAMP/STPA



ゴール指向要求分析手法に基づいた要件の整合

↓

属性つきゴール指向要求分析法で用いられる満足度行列

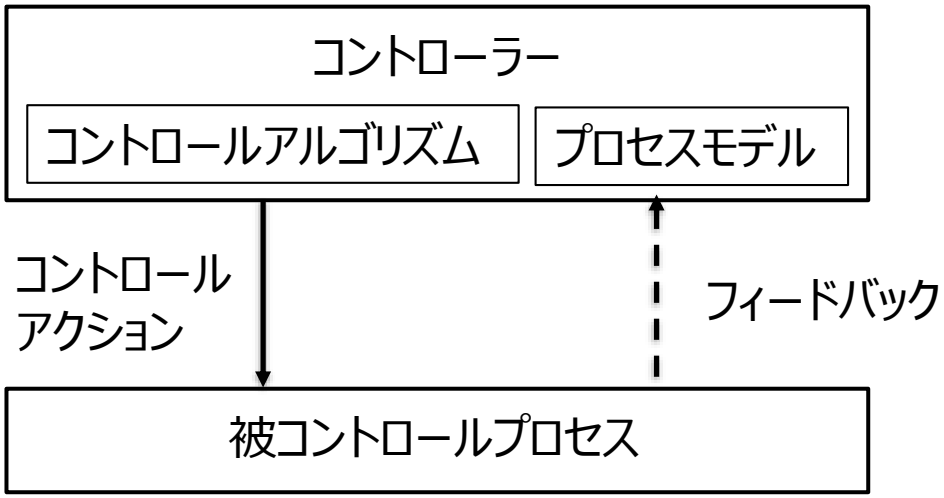


前提知識①：STAMP/STPA

STAMP/STPAとは

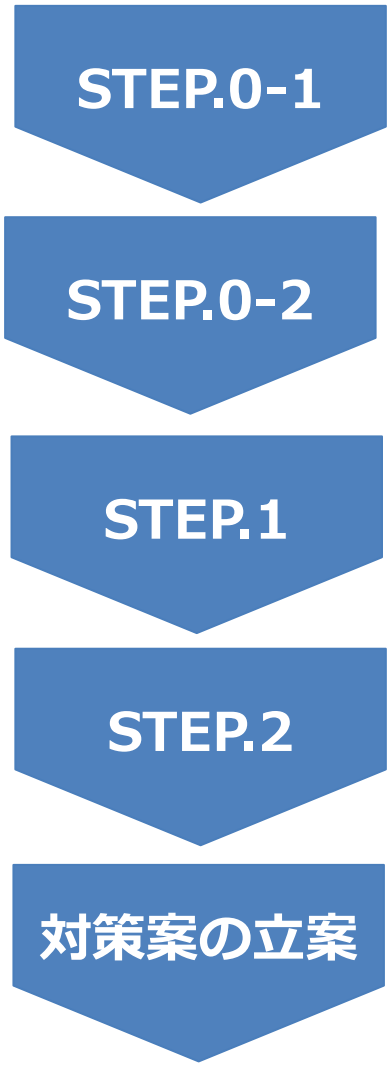
STAMP ：システム理論に基づくアクシデントモデル
STPA　：STAMPに基づく安全解析手法

システムを構成する各要素の相互作用によって発生する問題の発生要因を分析する



STAMPにおける相互作用のモデル

前提知識①：STAMP/STPA



アクシデント、ハザード、安全制約の識別

➡ 分析の目的を定義する

コントロールストラクチャの構築

➡ 分析対象を図示化する

非安全なコントロールアクションの抽出

ガイドワードを使って

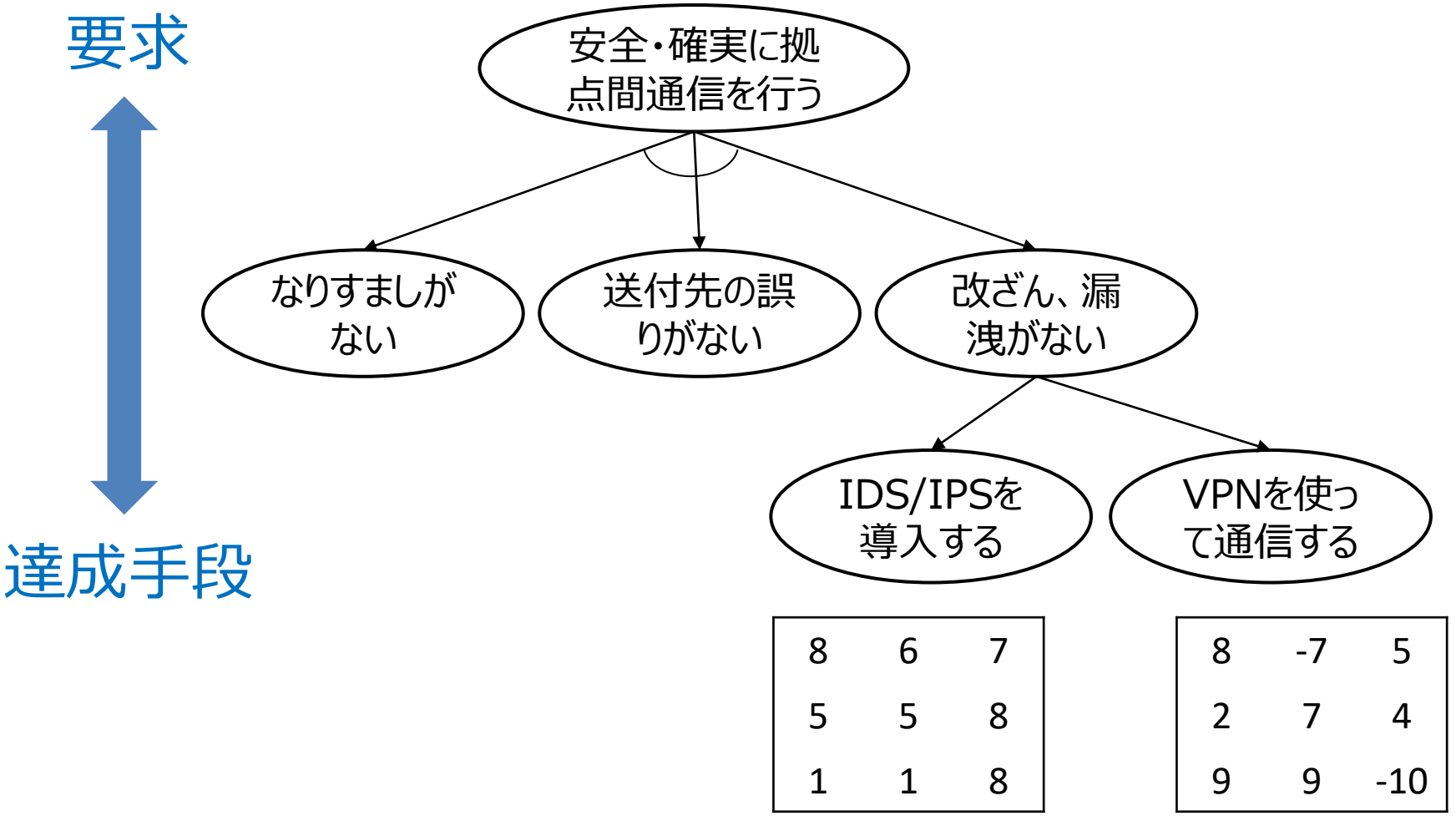
➡ 問題となりそうな振る舞いを抽出する

ハザード要因の特定

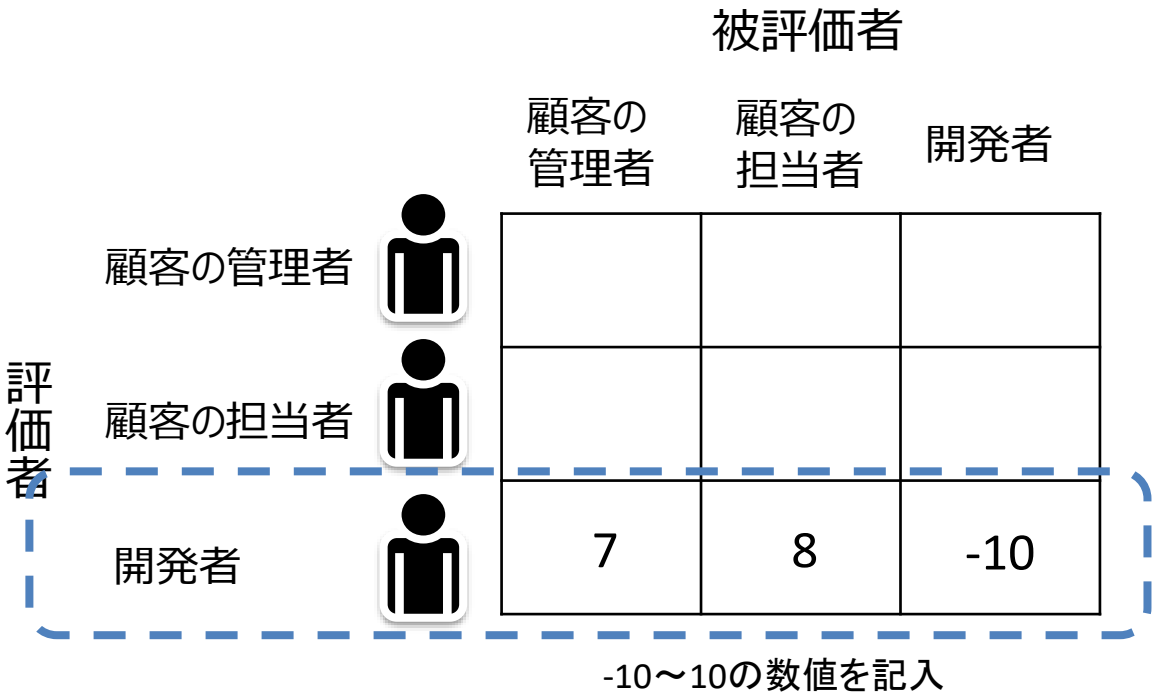
ガイドワードを使って

➡ 問題を誘発するシナリオを創発する

前提知識②：属性つきゴール指向要求分析法と満足度行列



前提知識②：属性つきゴール指向要求分析法と満足度行列

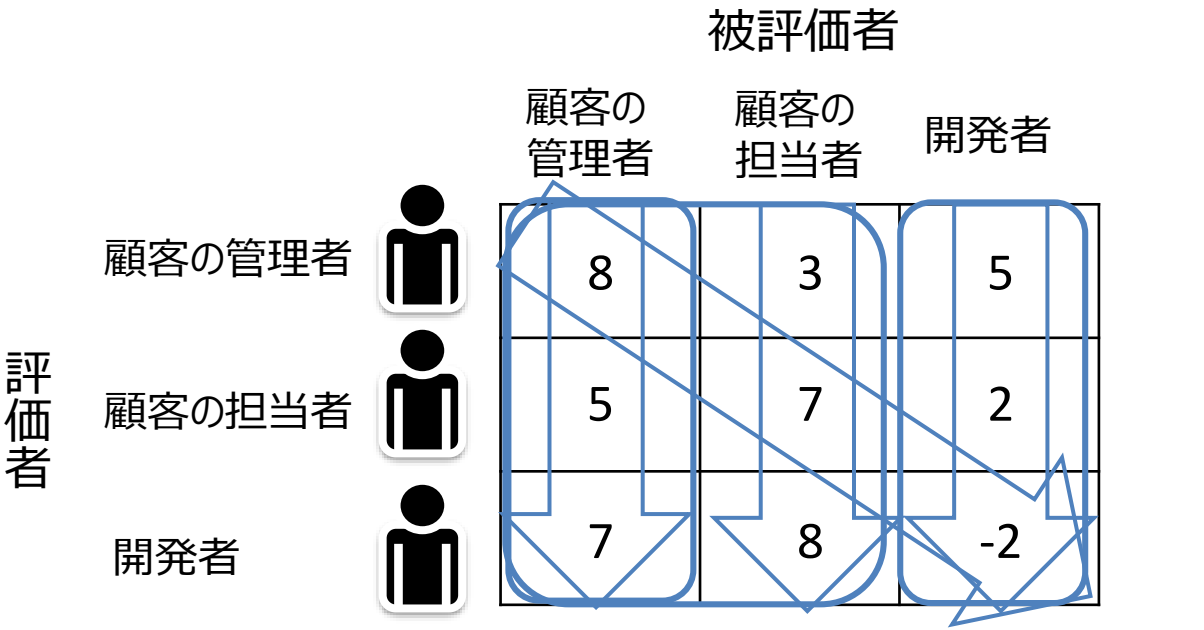


三様の評価者が
被評価者の立場を想定し、要件を評価する

●●すること。という要件に対して
開発者が　顧客の管理者の立場だったら、7
　　顧客の担当者の立場だったら、8
　　開発者の立場だったら、-10
のように、相手の視点に立った評価を行う

前提知識②：属性つきゴール指向要求分析法と満足度行列

例えば、開発者が立案した要件について評価する



ゴール適合度

解釈の違い

意見の対立度

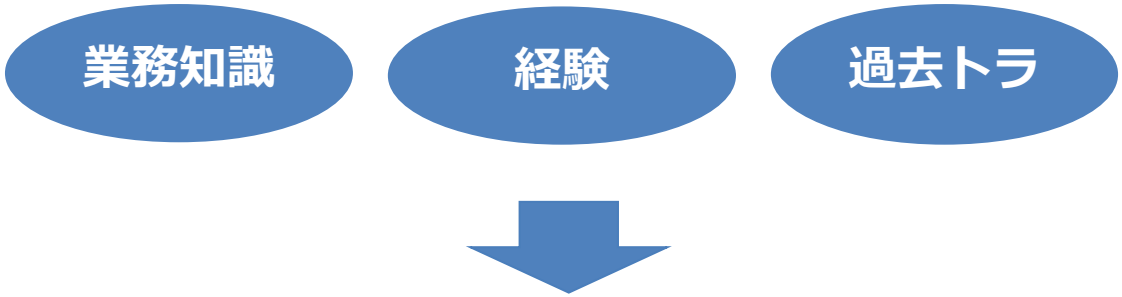
立場の違い

SSMS法：プロセスモデル構築上の工夫点

要件の抽出 → 要件の合意形成

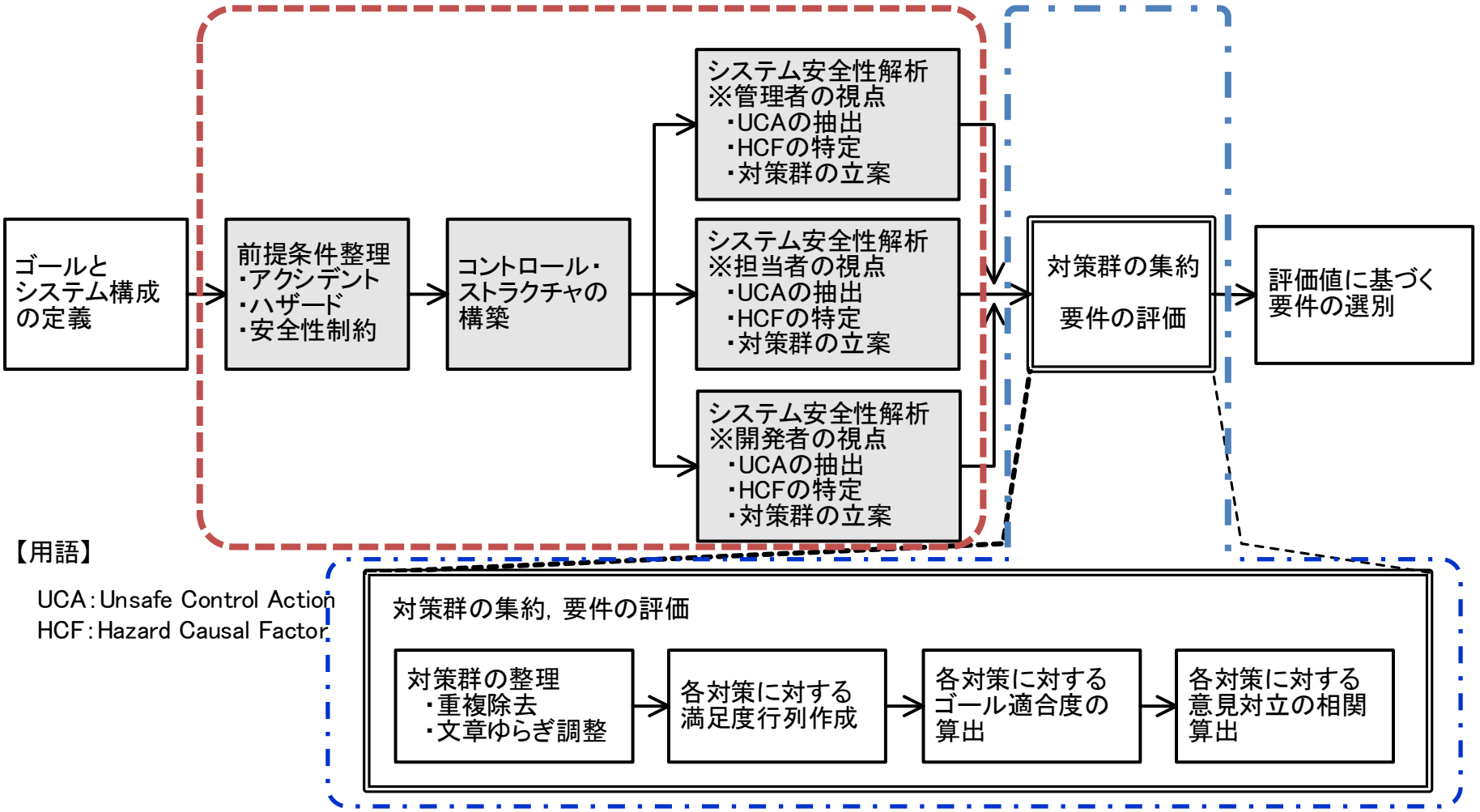
STAMP/STPAによる要件抽出時の課題

解析者が持つ思考特性により抽出されるハザードと脅威の対策群に偏りが生じる



利害関係が生じやすい複数のロールの立場で思考制約を設けてSTAMP/STPA による解析を実施することで、多様性を創出する

SSMS法：プロセスモデル



SSMS法：要点

STAMP/STPA＋多様なステークホルダの視点

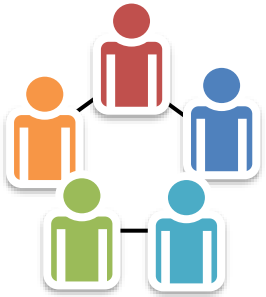
×

満足度行列による要件のスクリーニング

実験

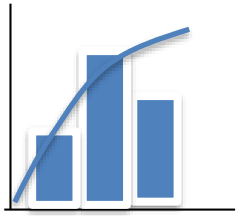
実験：仮説と研究設問

仮説　多様なステークホルダの視点をSTAMP/STPA に導入してシステムのハザードと脅威に対する対策群を抽出し、これらを要件として満足度行列で分析すれば、客観的かつ系統的に合意形成されやすい安全性・セキュリティ要件を獲得できる。

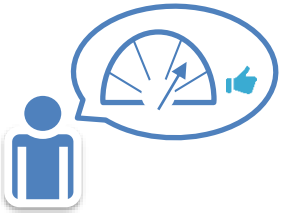


RQ1　解析者にロールを与えて要求分析することで、
多様な視点で安全性・セキュリティ要件を獲得できる。

RQ2　ドメイン知識を十分に有しなくても複数のロールを持たせて STAMP/STPA で解析することで、当該ドメインの有識者と同等**量**の安全性・セキュリティ要件を獲得できる。

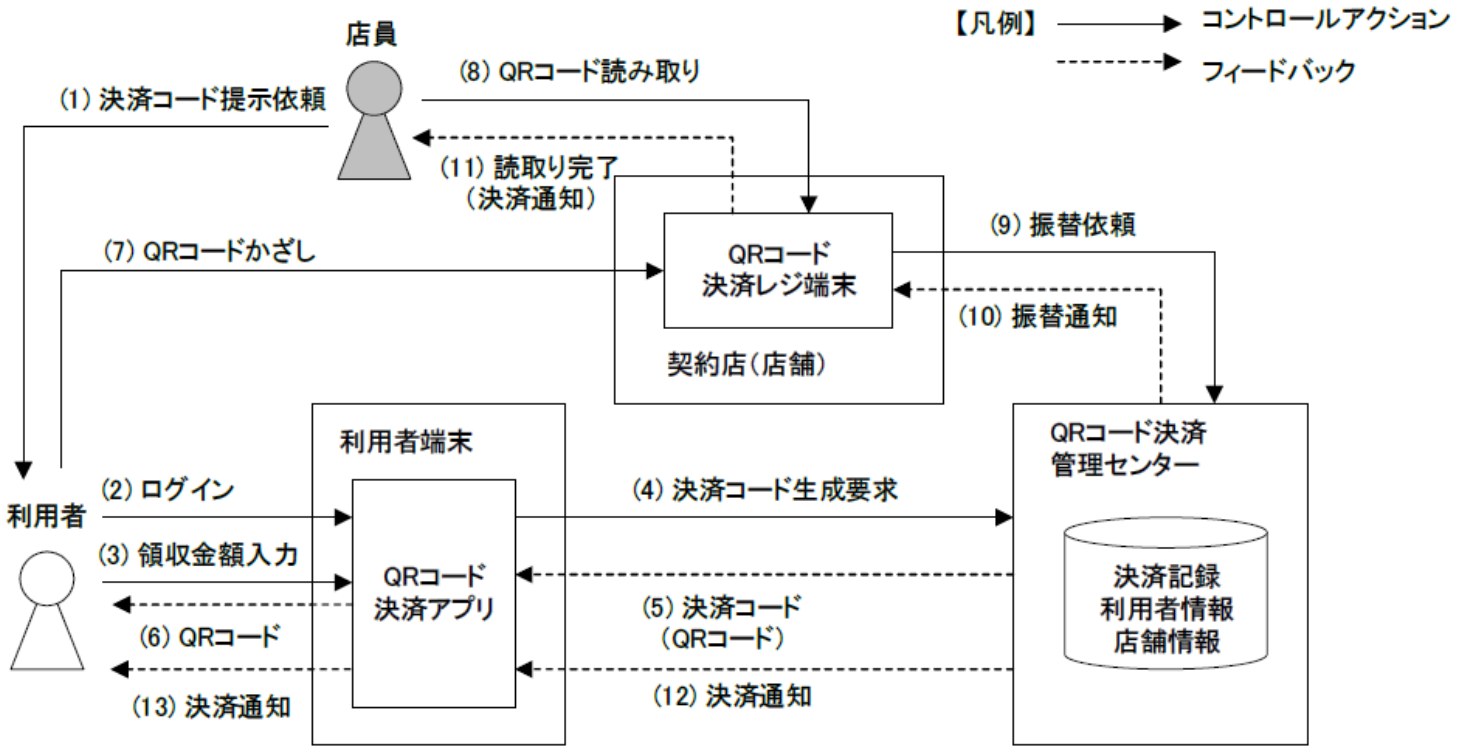


RQ3　ドメイン知識を十分に有しなくても複数のロールを持たせて STAMP/STPA で解析することで、当該ドメインの有識者が抽出した要件に近い**質**の安全性・セキュリティ要件を獲得できる。



実験：仮想QRコード決済システム(SQiP Pay)における安全性要件の抽出

SQiP Pay



要求

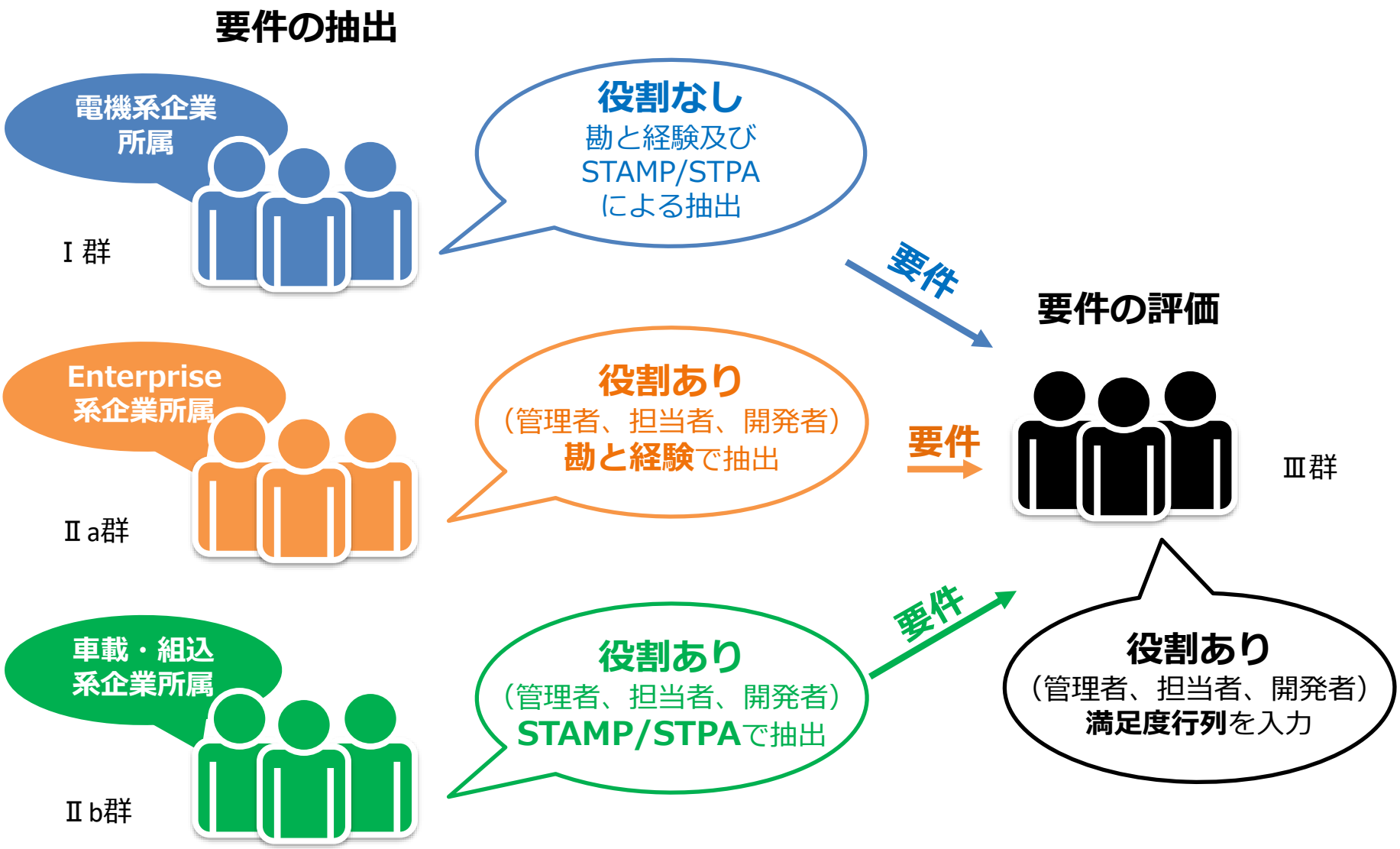
- 当人名義人外の口座間で金額の振替が発生してはならない
- 決済利用者外で振替が実施されてはならない
- QRコード決済がスムーズに行われず店舗売上の機会が損失してはならない

実験：仮想QRコード決済システム(SQiP Pay)における安全性要件の抽出

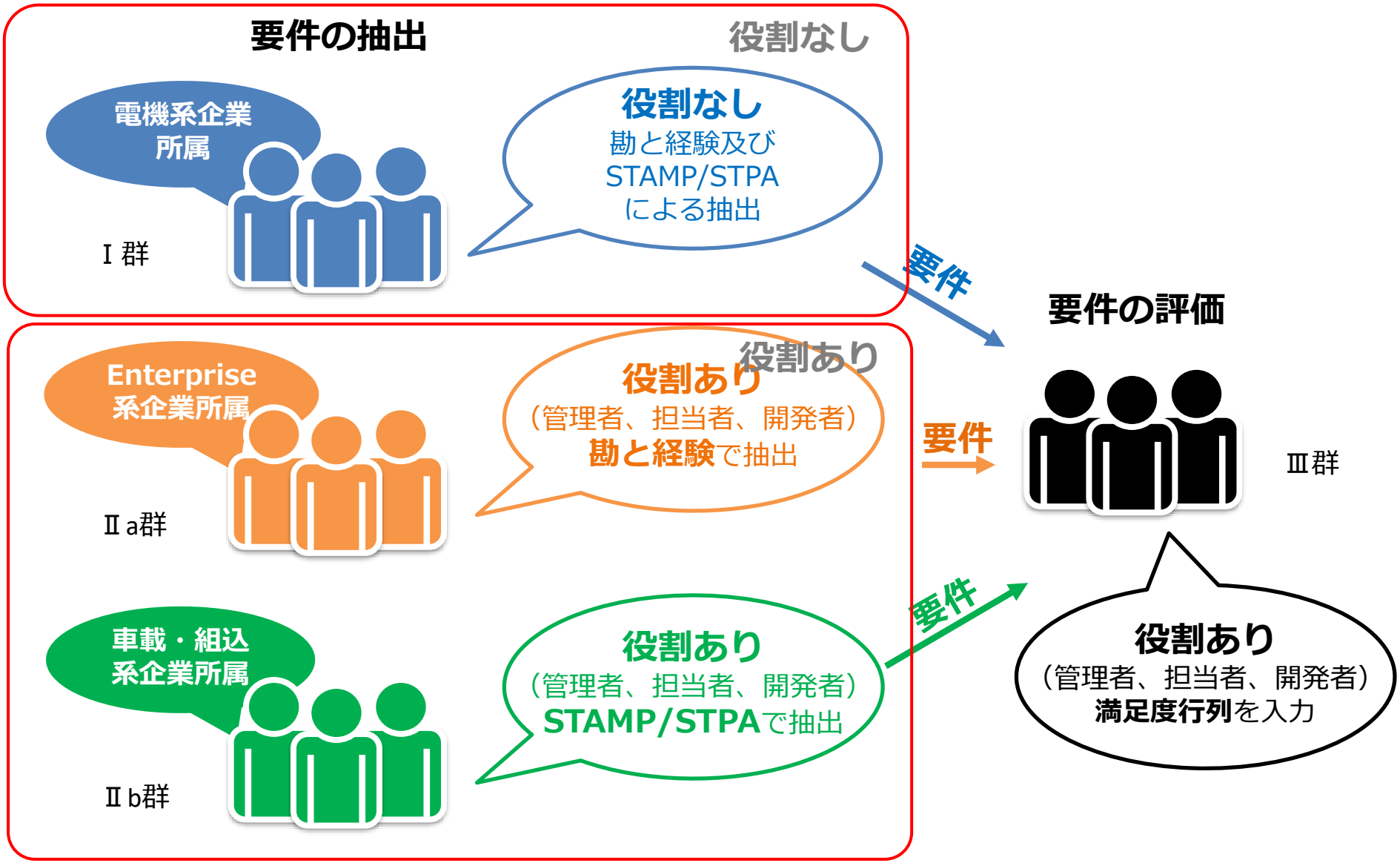
SQiP Pay

アクシデント	ハザード	安全制約
A1:当人名義外の口座間で金額の振替が発生する	H1:異なる利用者の口座から引き出す	SC1:決済利用者の口座から引き出さなければならない
A1:当人名義外の口座間で金額の振替が発生する	H2:異なる店舗への口座に預け入れる	SC2:店舗口座に預け入れなければならない
A2:領収金額以外で振替が実施される	H3:決済金額を間違う	SC3:決済金額を間違ってはならない
A3:QR コード決済がスムーズに行われず、店舗で待ち行列ができる	H4:QR コード（決済コード）の提示依頼から読取り完了までの所要時間が現金決済よりも遅い	SC4:QR コード決済に要する時間は現金決済よりも早い

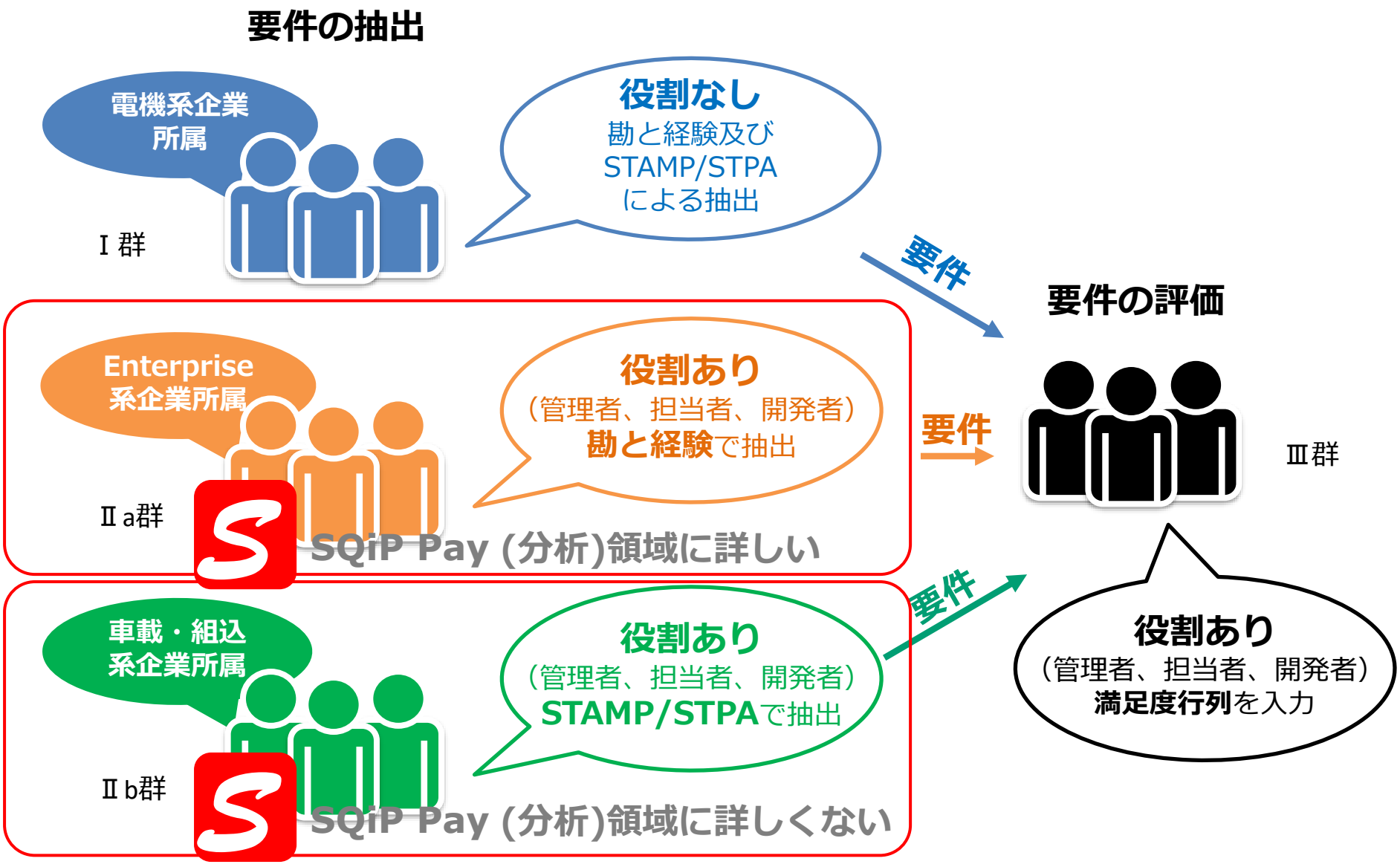
実験：実験のフレームワーク（被験者のグループ分け）



実験1：役割の有り無しによる抽出される要件の違い

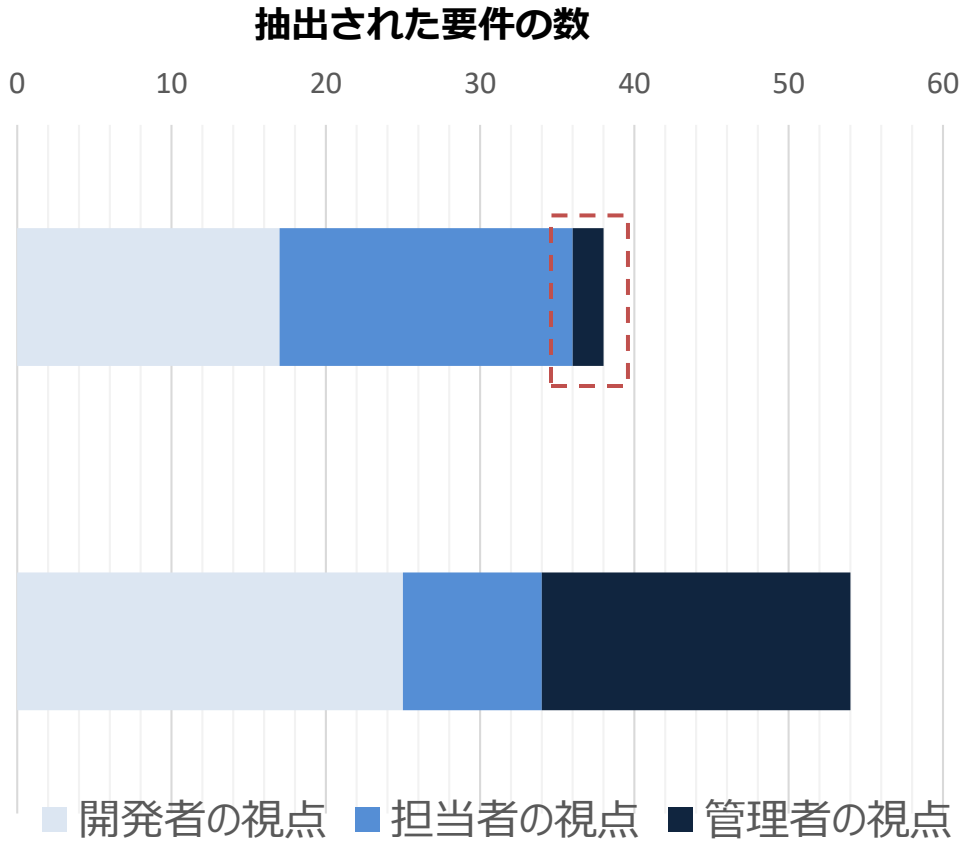


実験2、3：勘・経験と、STAMP/STPAにて抽出された要件の違い

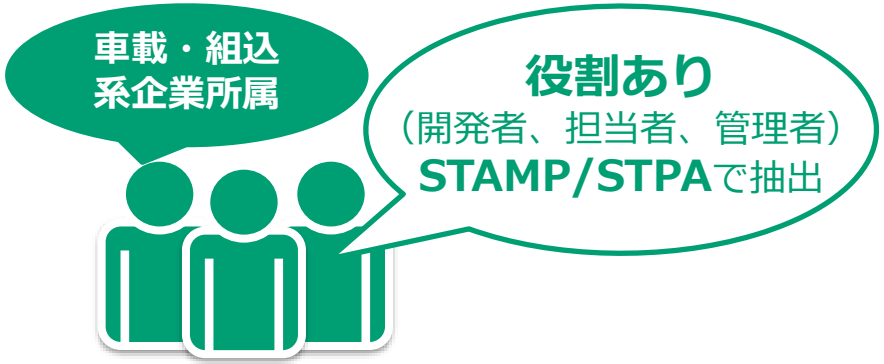


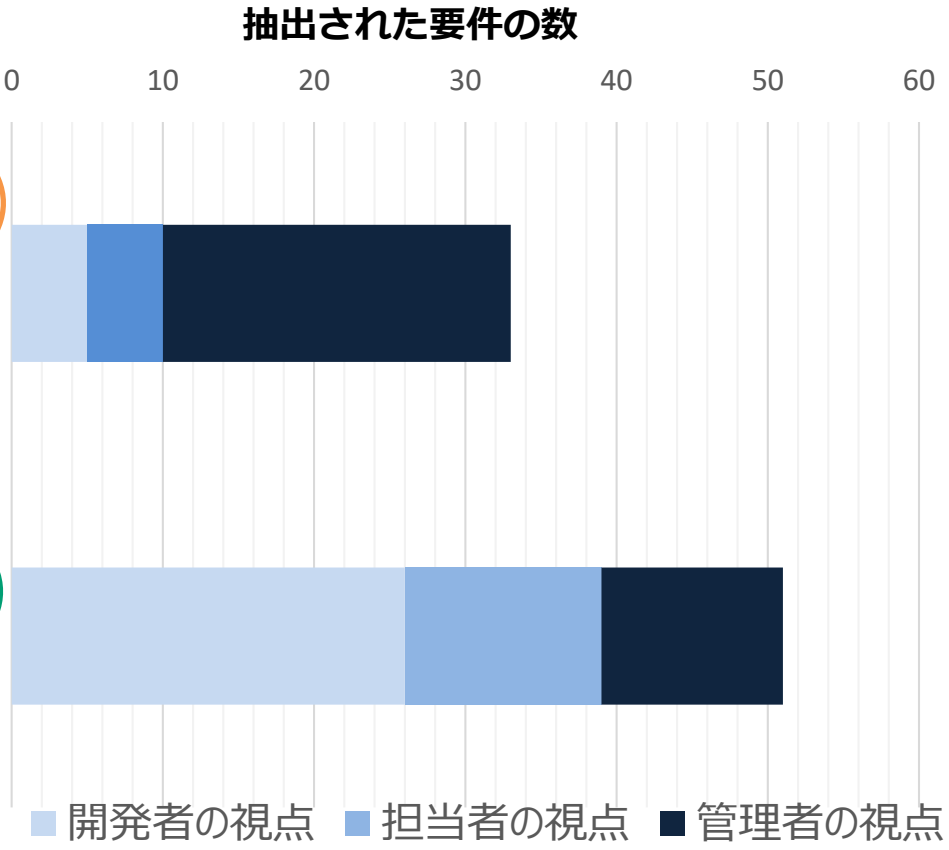
実験結果

実験結果１：役割を与えると多様な視点で要件を獲得できる

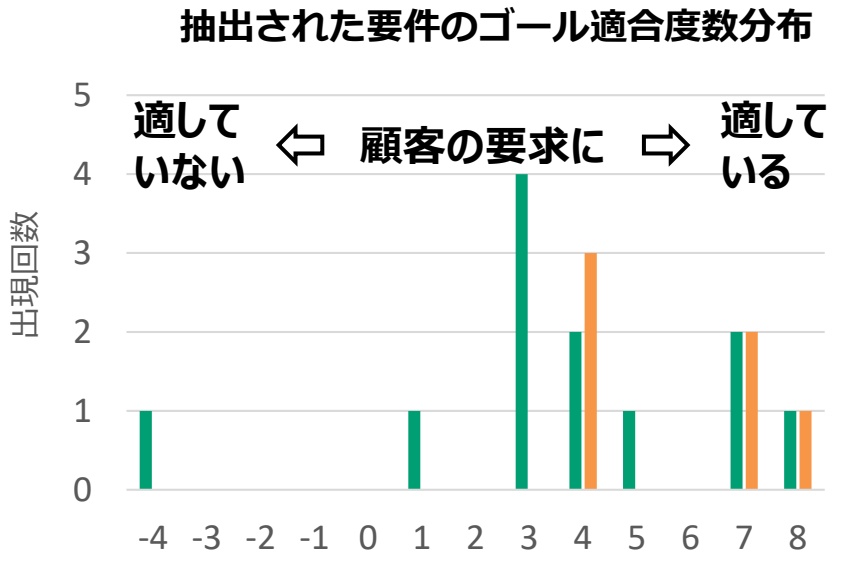


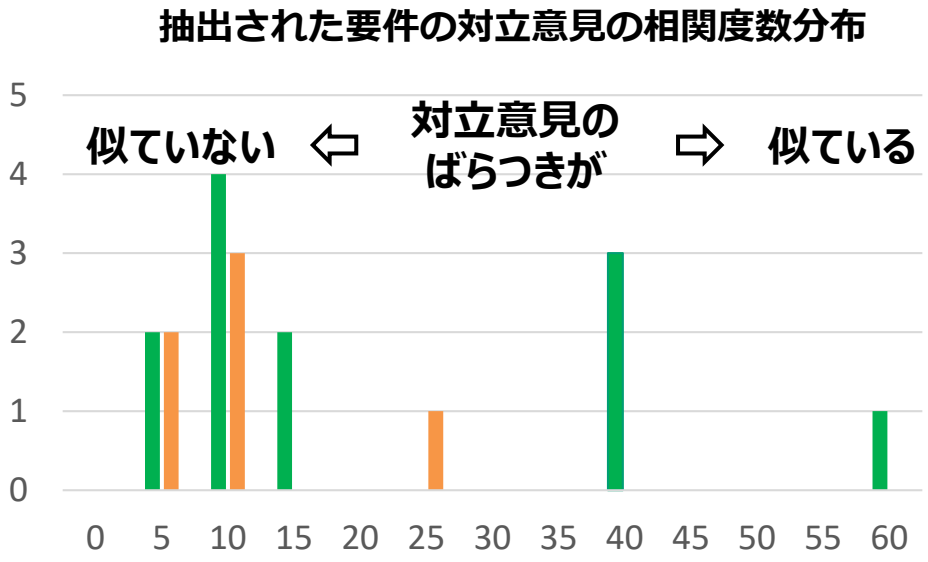
実験結果２：ドメイン知識が十分でなくとも有識者と同等の要件数を抽出できる

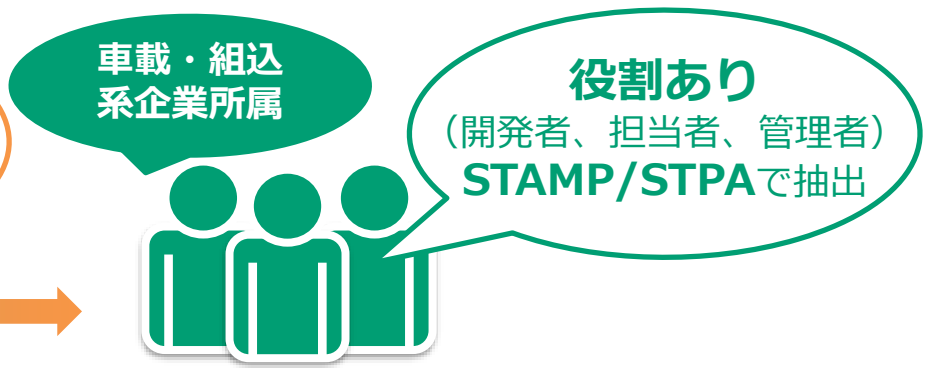




実験結果３：ドメイン知識が十分でなくとも有識者と同等の質をもった要件を抽出できる







ゴール適合度数、対立意見の相関度ともに**統計的有意差はなかった**

実験結果：抽出された要件の例

	管理者視点	担当者の視点	開発者の視点
CA	決済コード提示依頼（店員→ 利用者）	QRコードかざし（利用者→ QRコード決済レジ端末）	QRコード読取り（店員→ QRコード決済レジ端末）
UCA	QRコードによる決済の意図やアクションのタイミングが伝わらず、利用者が困惑する	QRコードの読み取りが完了していないのにかざし動作を止めてしまう	当該店舗での取引と無関係のQRコードを読み取ってしまう
HCF	店員から利用者に対するQRコード提示の働きかけ方が判りづらい	利用者が認知しづらいQRコード読取り完了の表現手段を採用した.	過去に生成されたQRコードがQRコード決済アプリ内部に保持されており、誤って使われてしまう
対策（要件）	接客応対に関するオペレーションの習熟をはかる（教育活動の強化） 	LED や効果音等の表現手段により，利用者に読取り完了状態を伝える 	QR コードの生成時刻等をQR コードに含め，期限切れの場合に警告を表示する 

考察

実験考察

1. 要件の抽出時にロールを与えると、多様性のある要件を抽出できた

ロールを付与することで経験・知識による制約が開放される

技術者はこれまでの業務経験や知識に縛られて、視野が狭くなり俯瞰的な解析が難しくなる

2. STAMP/STPAを用いると、要件（安全性とセキュリティの対策）を

・量
・質

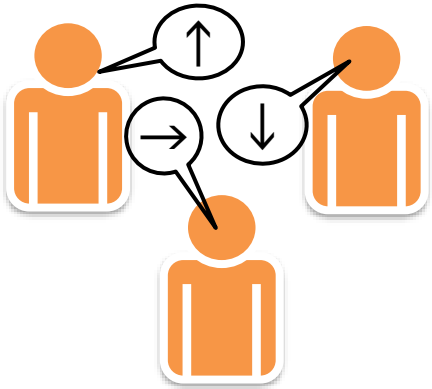
共に、充分に獲得することができた

STAMP/STPAの分析プロセスが作用した

✓ コントロールストラクチャ（モデル）作成による俯瞰的な視点
✓ ガイドワードによる強制発想

実験考察

3. 「合意形成されやすい要件を獲得できる」とは言えない



ドメイン有識者グループでも評価のバラつきが発生している

コミュニケーションを通して選択肢を選ぶ過程の共有が重要。
ステークホルダが議論をしながら要件に対する評価を繰り返しながら合意形成を促進する。

まとめ

SSMS法の効果

要件（安全性とセキュリティの対策）の抽出において

STAMP/STPA による分析の際に、分析者にロールを与えることで

業務経験による思考の偏りから**解放**される。
解析時の**視野が広がり**、**俯瞰的な解析**ができる。
創発性が生まれる。
ドメイン知識が十分でなくても要件が抽出できる。

抽出された要件を満足度行列で評価することで

要件に対するステークホルダ間の**満足**度合い
や**対立**度合いを**定量的**に表すことができる。

▷ ステークホルダ間の合意形成に寄与できる

ご清聴ありがとうございました