HITACHI
Inspire the Next

STAMP/STPAを用いた テスト観点導出による重大障害未然防止

2020/09/10

株式会社 日立製作所
システム＆サービスビジネス統括本部　品質保証統括本部
サービスプラットフォーム品質保証本部
アプリケーションサービス品質保証部

〇前田 竜宏，高山 啓

e-mail:tatsuhiro.maeda.pk@hitachi.com

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

1. はじめに

HITACHI
Inspire the Next

STAMP/STPA

STAMP(Systems-Theoretic Accident Model and Processes)
システム理論に基づく事故モデル
STPA(System-Theoretic Process Analysis)
システム理論に基づく安全解析手法

システム理論

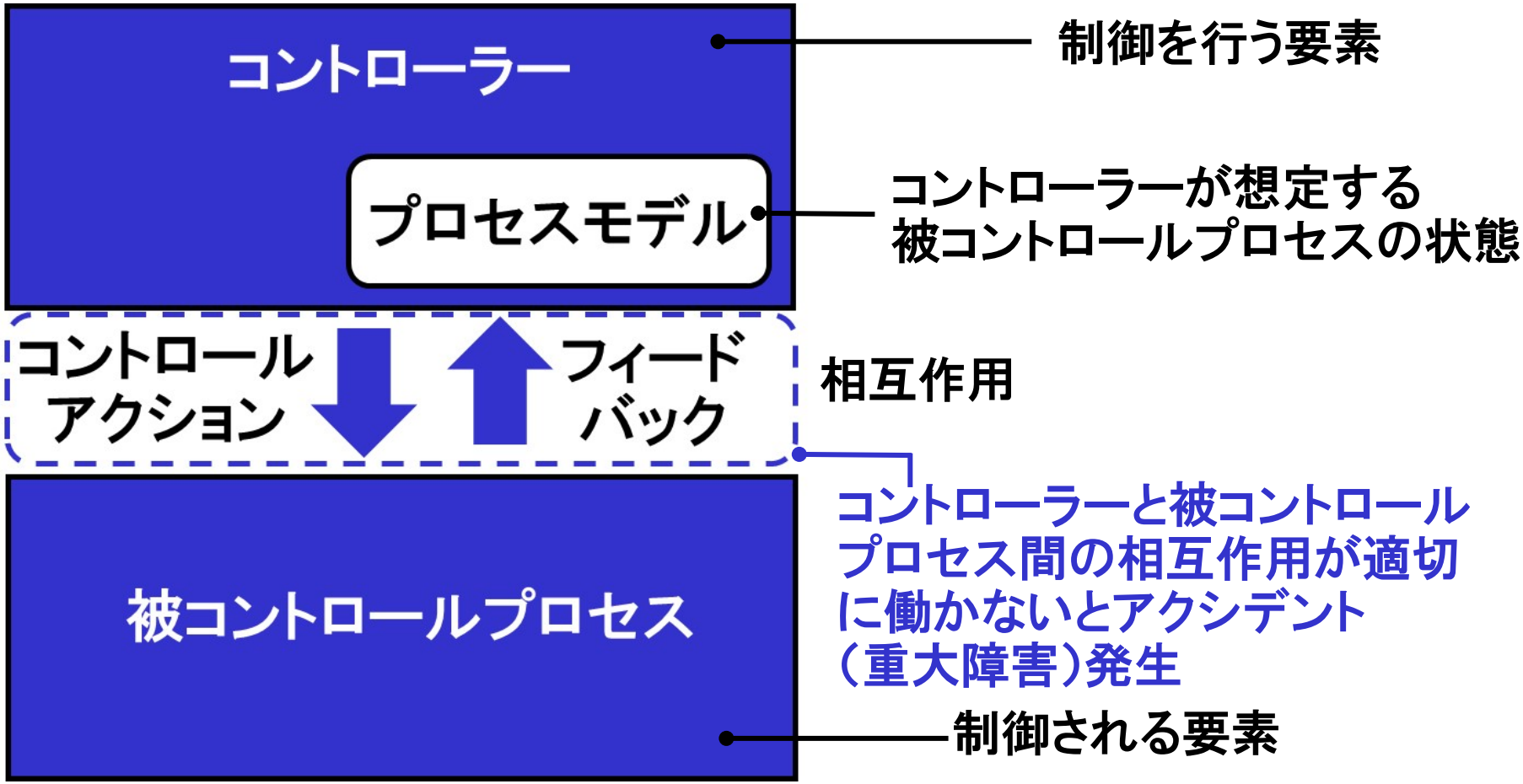
システムを部品の集合ではなく、全体で捉える。
システムを構成するコンポーネント間(インタフェース)の繋がりや関係性、相互作用するときに発生する特性に着目する。

安全

利害関係者にとって受け入れることができないような損失が発生しないこと。

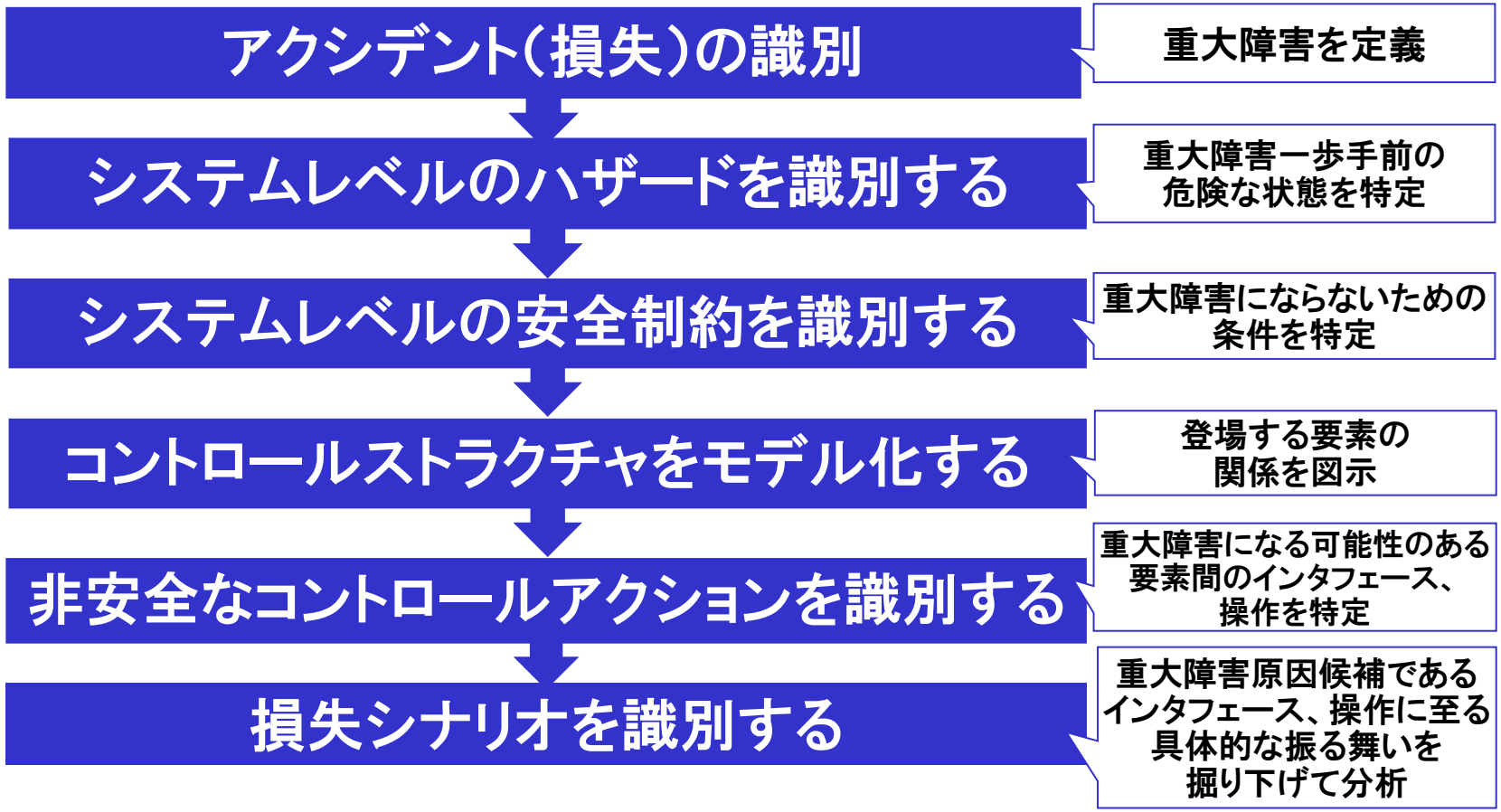
HITACHI
Inspire the Next

STAMPによる相互作用のモデル（コントロールストラクチャ）



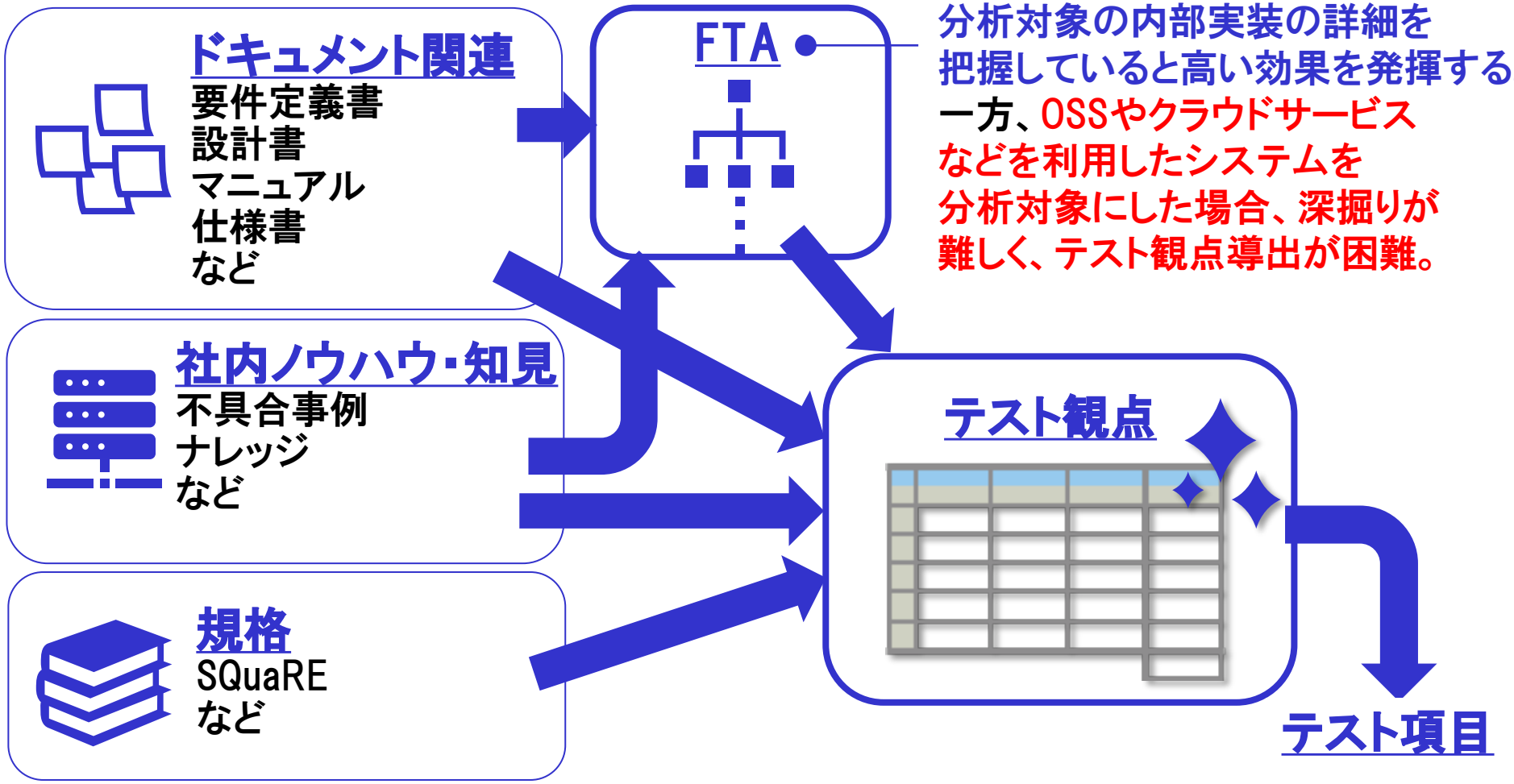
HITACHI
Inspire the Next

STPA:STAMPに基づく安全解析手法



1-4 従来のテスト観点の導出

HITACHI
Inspire the Next

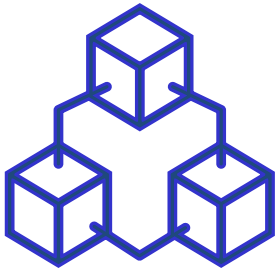


FTA:Fault Tree Analysis 故障の木解析
SQuaRE:Systems and software Quality Requirements and Evaluation

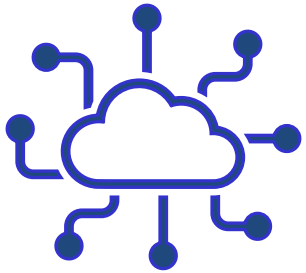
HITACHI
Inspire the Next

目的:重大障害の未然防止

背景



OSS



クラウド

システムのブラックボックス化

テスト観点の導出が難しくなりつつある
重大障害のリスクが高まっている

課題

ブラックボックス化したシステムの重大障害を
未然防止するためのテスト観点の導出

手段

ブラックボックス化に対応した手法の適用

1-6 本発表の内容

HITACHI
Inspire the Next

本発表は、
STAMP/STPAを用いて
重大障害を未然防止するための
テスト観点を導出し、
テストを実施した
経験発表です。

HITACHI
Inspire the Next

2. STAMP/STPAの適用

2-1　STAMP/STPA適用に向けて

HITACHI
Inspire the Next

・専門書は難解でしきいが高いため、
　今後、STAMP/STPAを他のエンジニアが適用するのが困難
・ITシステムのテスト観点導出が主目的の手法ではない

工夫点

STAMP/STPAの適用に関するガイドの作成(25ページ)
STAMP/STPAの正確な適用が目的ではなくテスト観点導出が目的
・極力シンプルに説明
・FTAとの使い分け方

適用手順の説明

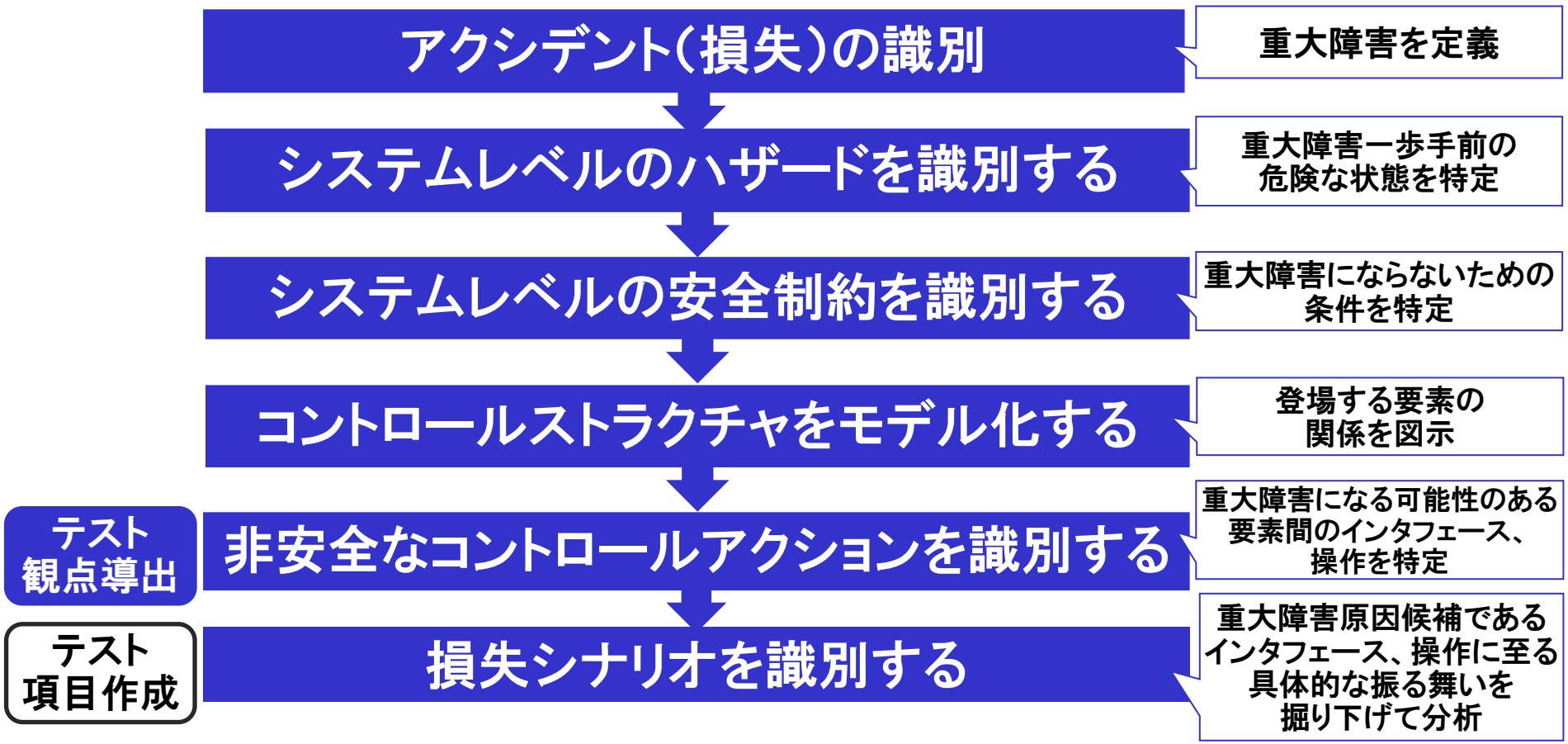
FTAとSTAMP/STPAの整理

分析手法	メリット	適用効果のあるプロジェクト
FTA	分析対象の内部実装の詳細を把握していると高い効果を発揮。	・ソフトウェア(APP、UPなど)単体の開発 ・自社開発品など内部実装や修正内容の詳細が把握できるドキュメントが存在するもの
STAMP /STPA	システム間/コンポーネント間のインタフェースに着目して観点を考えられる。	・大規模システム ・複数の製品で構成されるシステム ・他社クラウドやサービスの利用などブラックボックスの割合が高いシステムやサービス

2-2 STAMP/STPA適用手順

HITACHI
Inspire the Next

STPAの適用手順



2-3 アクシデント(損失)の識別

HITACHI
Inspire the Next

◆重大障害を定義する
アクシデントは、利害関係者が受け入れることができないシステムの問題

ITシステムにおける一般的なアクシデントの検討

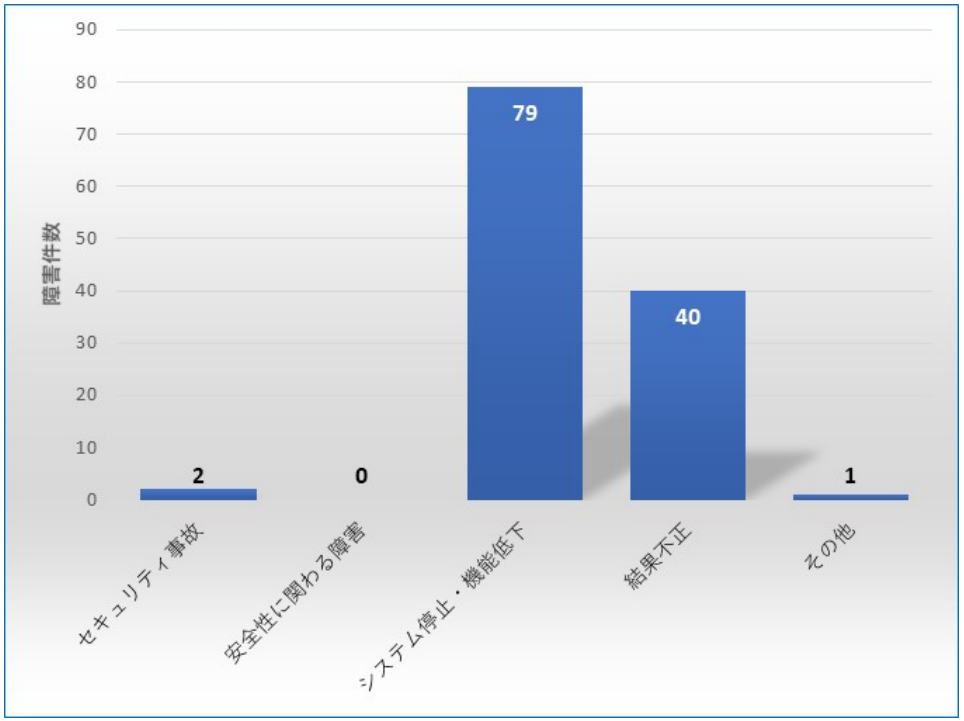
ITシステム障害を引き起こす脅威	
脅威の類型	発生する障害・事故
意図的な要因 (サイバー攻撃、犯罪など)	(1)セキュリティ事故
偶発的な要因 (操作・設定ミス、プログラム上の 欠陥、機器故障など)	(2)安全性に関わる障害 (3)機能停止・機能低下
環境的な要因 (災害による電力設備破壊など)	(4)結果不正
その他の要因	

【参考】NISC: 重要インフラの情報セキュリティ対策に係る第2次行動計画

2-3 アクシデント(損失)の識別

HITACHI
Inspire the Next

◆重大障害を定義する
アクシデントは、利害関係者が受け入れることができないシステムの問題



報道された情報システムの
障害とほぼ一致

工夫点

アクシデント(損失)の分類
(1)セキュリティ事故
(2)安全性に関わる障害
(3)機能停止・機能低下障害
(4)結果不正
　(料金計算の結果不正など)
(5)その他

2019年度の社会に影響を与え全国紙等に報道された情報システムの障害情報(独立行政法人情報処理推進機構発行,URL:https://www.ipa.go.jp/sec/system/system_fault.html)の件数(122件)を独自にアクシデント別に分類して集計

2-4 ハザードの識別

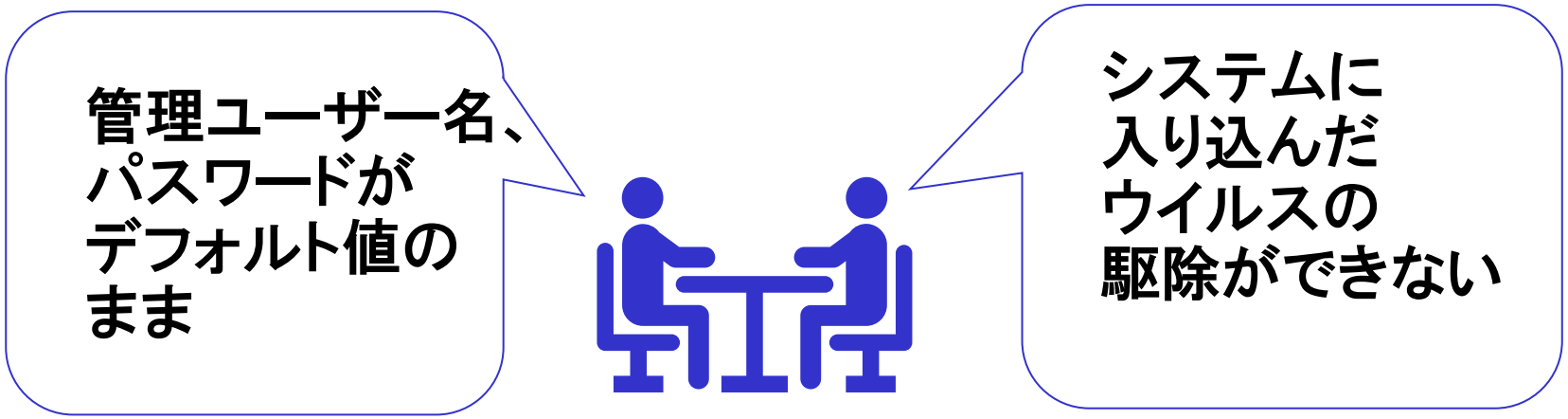
HITACHI
Inspire the Next

◆それぞれのアクシデントに対してハザードを検討する

- 最悪ケースの環境で損失につながる
- 防止されるべき状態または条件

- ブレストなどでハザードを検討

アクシデントの例：セキュリティ事故



2-5 安全制約の識別

HITACHI
Inspire the Next

◆それぞのハザードに対して安全制約を考える

- 安全制約はハザードの逆
- ハザードを防ぐために満たす必要がある、システムの状態や動作
- 損失を最小限に抑えるためにシステムがなすべきこと

安全制約の例：セキュリティ事故

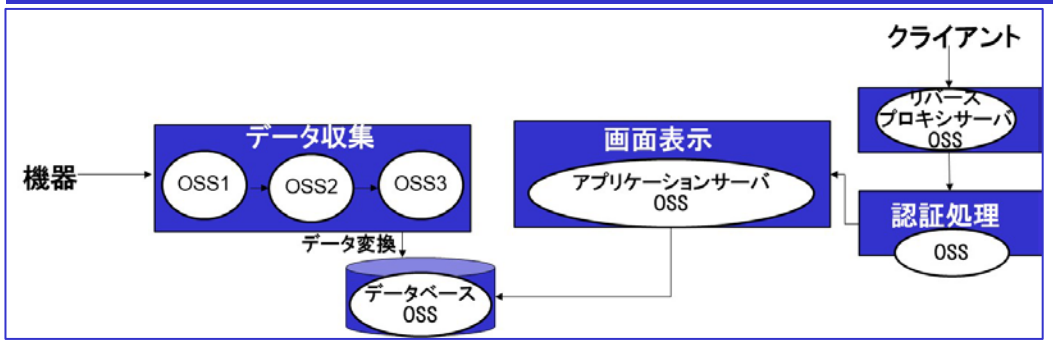
- 管理ユーザー名とパスワードがデフォルト値から容易に推測されない値に変更されている

- ウイルスの駆除ができること

安全制約は特定の解決法を指定しないこと。
特定の解決策を指定すると、他の潜在的に優れた解決策を見落とす結果になる可能性がある。

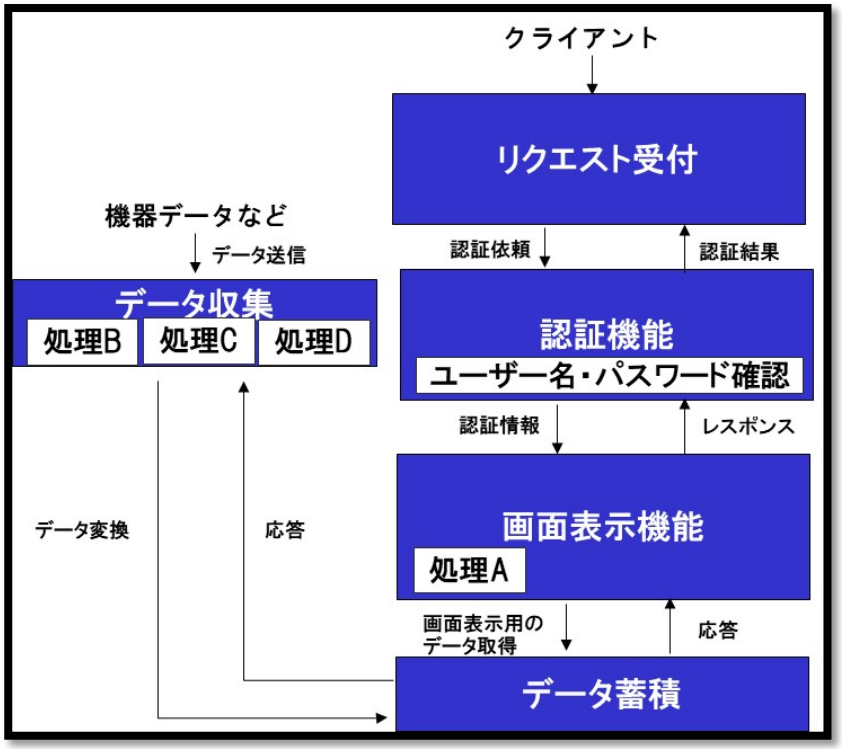
HITACHI
Inspire the Next

◆コントロールストラクチャのモデル化



今回、STAMP/STPAを適用したシステム(※)
OSSを多く使用している

コンポーネント間をまたぐ処理を抽出

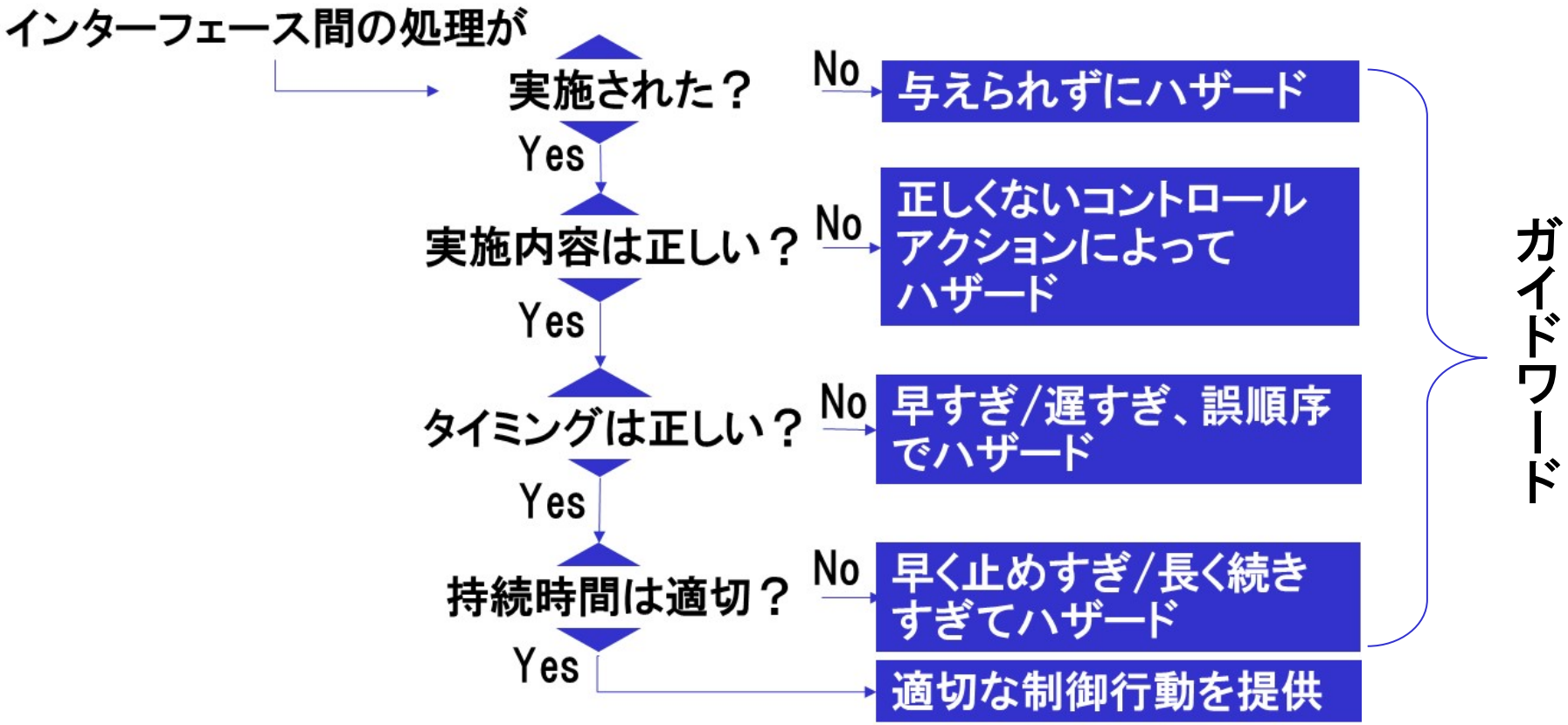


(※)実際に適用したシステムを簡素化しており、
正確な図にはなっていません。

HITACHI
Inspire the Next

◆非安全なコントロールアクションの識別

コンポーネントをまたぐ(インタフェース)の処理に着目して、ハザードになりうるかを検討する。



2-8 非安全なコントロールアクションの識別

HITACHI
Inspire the Next

コントロールアクション	アクシデント	実施された？	実施内容は正しい？	タイミングは正しい？	持続時間は適切？
認証依頼	セキュリティ事故	・ユーザーID、パスワードなしでログインできる（ユーザーID、パスワードの設定）	・単純なユーザーID、パスワードにより第3者がログインできる（単純なパスワードを登録させない） ・不正電文でログインできる（エラーにする）	N/A	・リクエスト完了までに時間をかける（タイムアウトする）
	安全性に関わる障害	N/A	N/A	N/A	N/A
	機能停止機能低下	N/A	・設計値を超えた長大電文でプロセスダウン（エラーにする）	N/A	・高負荷となり機能低下（流量制御の設定をする）
	結果不正	N/A	OSSの情報がエラー画面に表示される（独自のエラー画面の作成・設定）	N/A	N/A
認証処理	…	…	…	…	…

ここまででテスト観点は導出できる。
より詳細なテスト観点／テスト項目はハザードにいたる因果関係要因を考える。ヒントとしてガイドワードが用意されている。

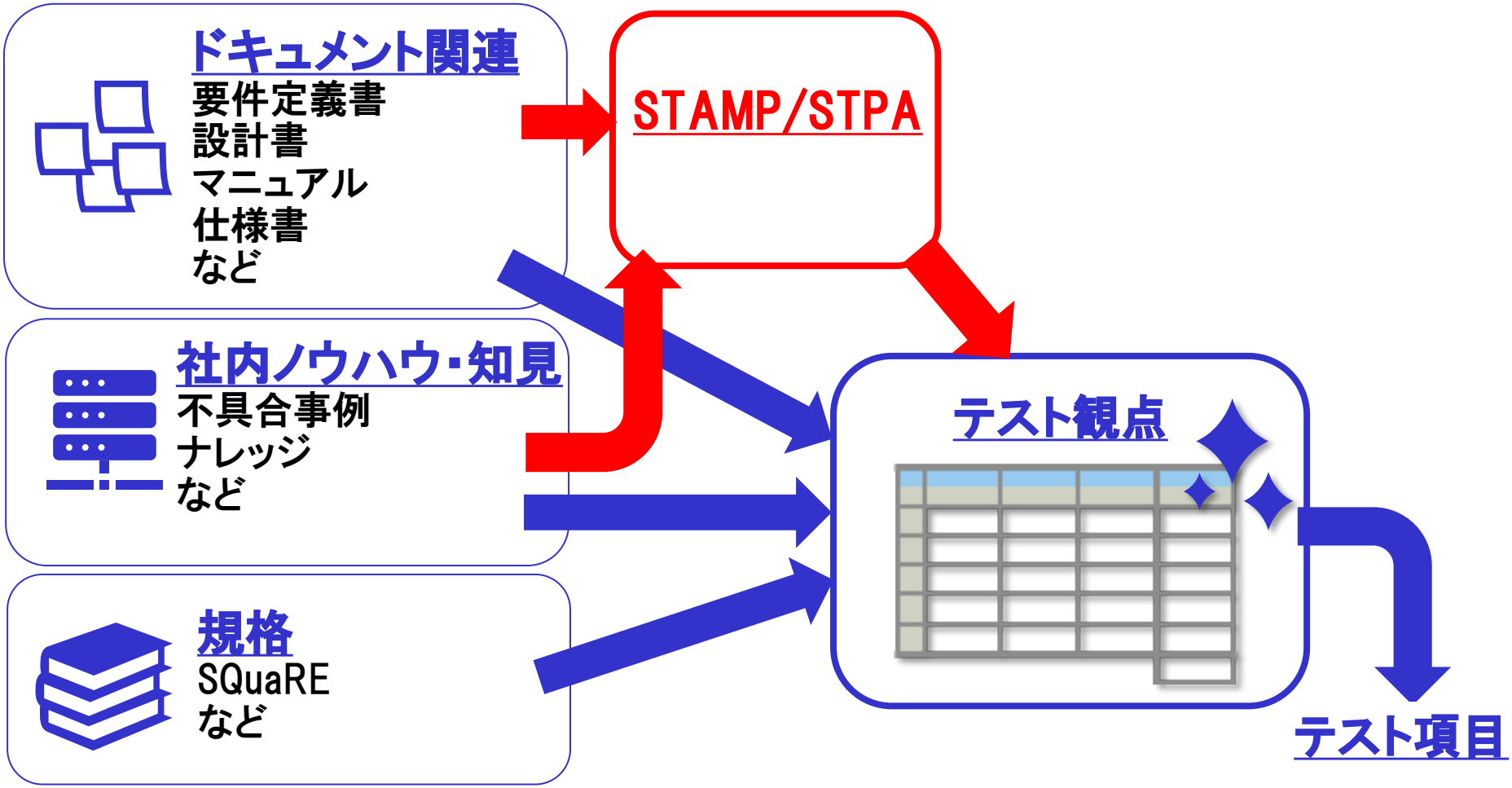
HITACHI
Inspire the Next

3. STAMP/STPAの適用結果

3-1　テスト観点の導出

HITACHI
Inspire the Next

2章で登場したシステムに対して、
従来のテスト観点に加えて、FTAではなくSTAMP/STPAを適用



3-2 STAMP/STPAの適用結果

HITACHI
Inspire the Next

2章で登場したOSSを使用しているシステム（OSSの前提知識がない状態で実施）

アクシデント	STAMP/STPAで導出したテスト観点数	従来の手法から導出したテスト観点と重複	不具合を摘出したテスト観点数
セキュリティ	8	5	0
安全性に関わる障害	0	0	0
機能停止 機能低下	4	2	0
結果不正	7	3	2

- 社内ナレッジと重複しないテスト観点は9点。
  テスト観点の補完ができた。
  重複しないテスト観点から不具合を2件摘出。
- OSSの知識がなくてもテスト観点を導出することが可能。

3-3 STAMP/STPA適用の感想

HITACHI
Inspire the Next

FTAより悩まずに

システム全体を俯瞰

OSSの知識がなくても、
ブラックボックスのままで

コントロールストラクチャ以降は
時間がかかる

HITACHI
Inspire the Next

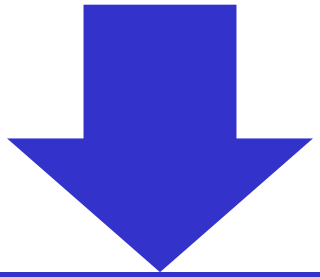
4. まとめ

4-1 まとめ

HITACHI
Inspire the Next

- STAMP/STPAは、事故モデルおよび安全解析手法であるが、本手法の適用により、論理的に重大障害発生可能性を洗い出すことで、テスト観点の導出が可能

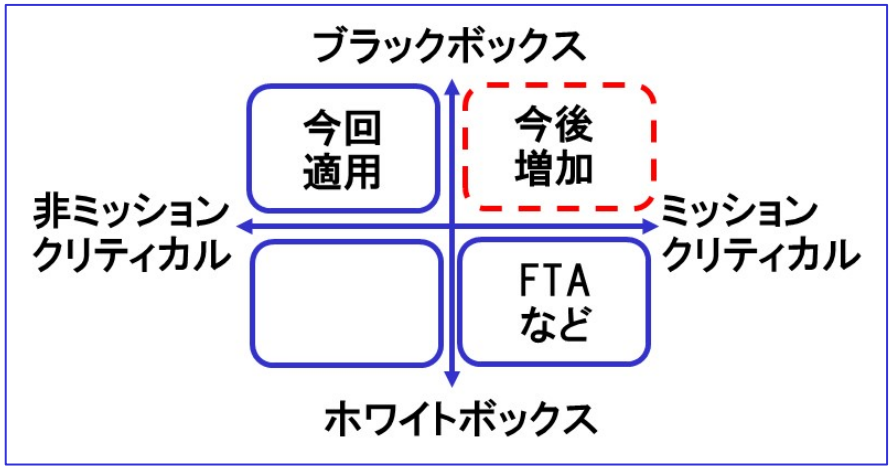
- ブラックボックスな箇所があっても大丈夫



STAMP/STPAの効果を実感

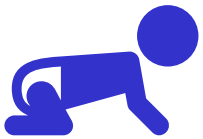
（※個人の感想です。）

4-2 今後に向けて



**ブラックボックスが多いシステムでも
安心・安全を提供**

経験を積んで、より効果的な
STAMP/STPAの適用



STAMP/STPA適用

実際の適用案件数が少ない
まだまだ工夫できる点は多いかも

ありがとうございました。

HITACHI
Inspire the Next

END

STAMP/STPAを用いた
テスト観点導出による重大障害未然防止

2020/09/10

株式会社 日立製作所
システム＆サービスビジネス統括本部　品質保証統括本部
サービスプラットフォーム品質保証本部
アプリケーションサービス品質保証部

○前田 竜宏，高山 啓

e-mail:tatsuhiro.maeda.pk@hitachi.com

付録 参考文献

HITACHI
Inspire the Next

はじめてのSTAMP/STPA

- https://www.ipa.go.jp/files/000055009.pdf

はじめてのSTAMP/STPA(実践編)

- https://www.ipa.go.jp/files/000059652.pdf

はじめてのSTAMP/STPA(活用編)

- https://www.ipa.go.jp/files/000065199.pdf

STPA HANDBOOK 日本語版

- http://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf