（資料2）

IPA Better Life with IT

組込みシステムの品質向上セミナー（演習付き）
～設計・実装フェーズでのミス防止～
2019年1月29日（火）14:00～17:00

障害未然防止のための設計知識の整理手法

（演習付き）

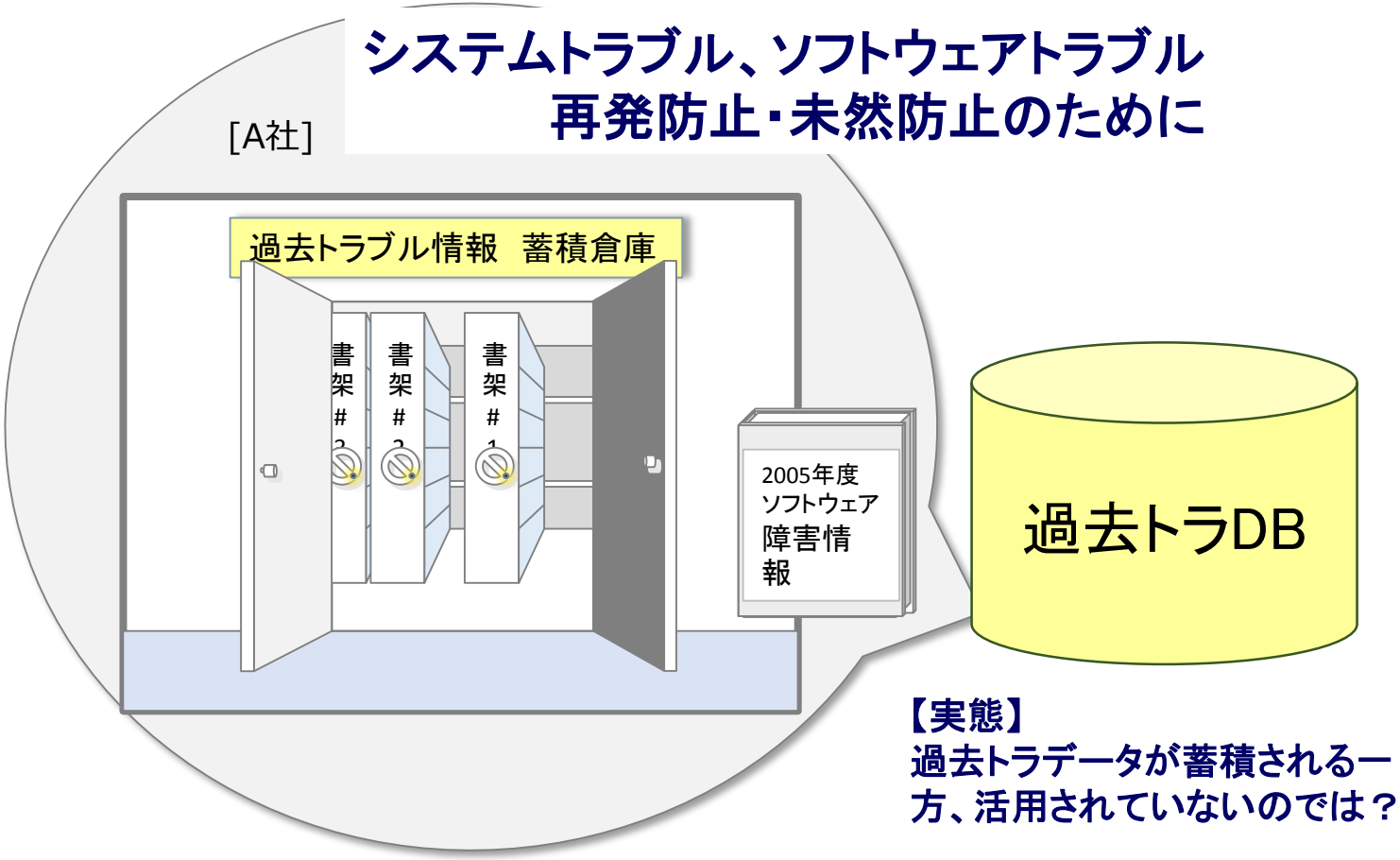
独立行政法人 情報処理推進機構(IPA)
社会基盤センター(IKC)

AGENDA

1. 背景と目的
2. 本手法の位置づけ
3. 障害の発生を未然防止する設計知識とは
4. 設計知識の活用
5. 設計知識の構造化
6. 設計知識の再利用
7. 設計知識の整理手法（ミニ演習）
   - **設計知識の抽出**
   - **設計知識の分類とタグ付け**
8. まとめ

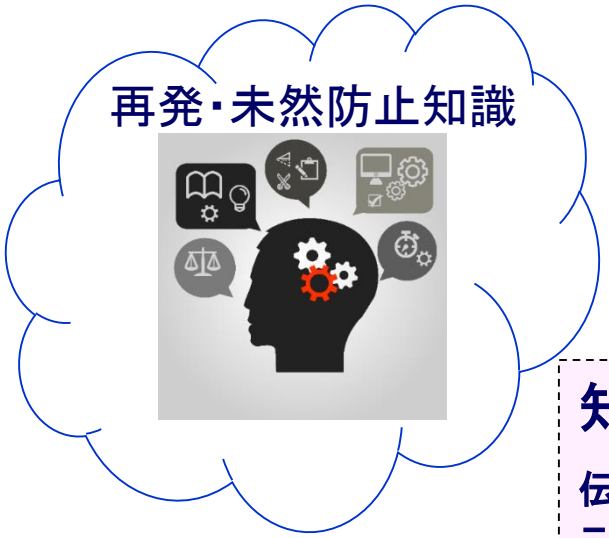
https://www.ipa.go.jp/sec/reports/20170321_1.html

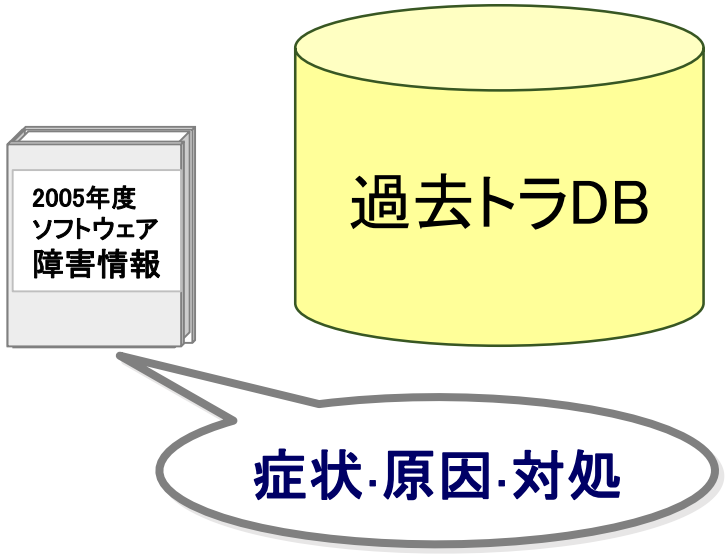
1. 背景と目的



1. 背景と目的

【実態】
症状・原因・対処が具体的に記録されているが、知識として整理されていないのでは？

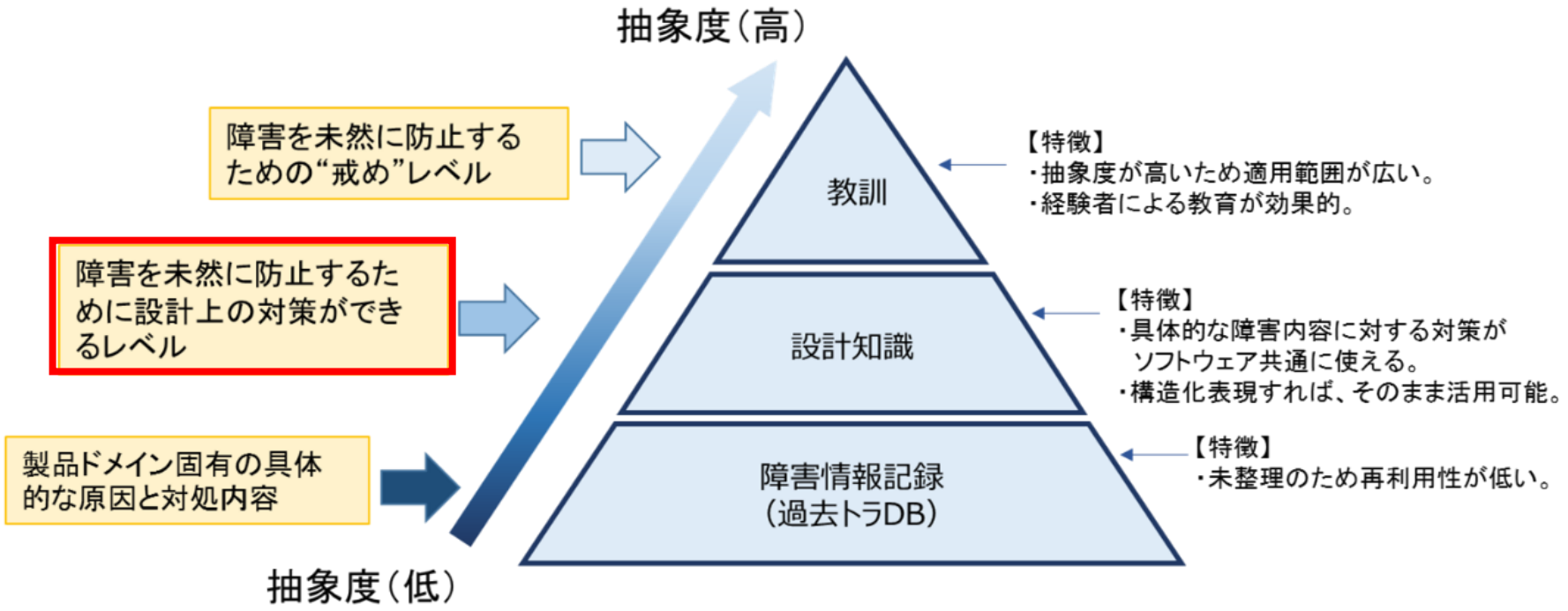




知識は 経験者個人の頭の中にあるもので、
伝承させるために **整理して形にする**
ことが必要。

2. 本手法の位置づけ

「教訓」、「設計知識」「障害情報記録」の関係



「教訓」の例

■ 装置・設備に関わる教訓

（1）危険源の同定
重要・主要と思っていないところに、危険・問題は含まれていないか？

a）「左警戒、右注意」の精神を忘れるな。
b）“法令は最低限”と心得て、個別具体の危険を検討せよ。

（2）センサーからの情報
センサーは測定すべきものを正しく測定できるか？

a）センサーは本当に“測りたいもの”を測っているか、確認せよ。
b）センサーにはもともと限界がある。

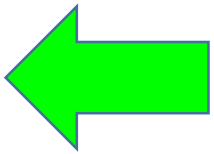
（3）多重化・冗長化
同じ場所、同じもの、同じ情報（データ）を用いた部分はないか？

a）同じ場所・同じものでは、機能喪失も同時に起こりやすい。
b）「見かけ」の多重化に、だまされるな。

出典：「巨大システム事故・トラブル教 訓 集」独立行政法人 原子力安全基盤機構
（原子力・航空・鉄道・化学・宇宙開発分野の事故・トラブル98事例から学ぶ）

3. 障害の発生を未然防止する設計知識とは

設計知識



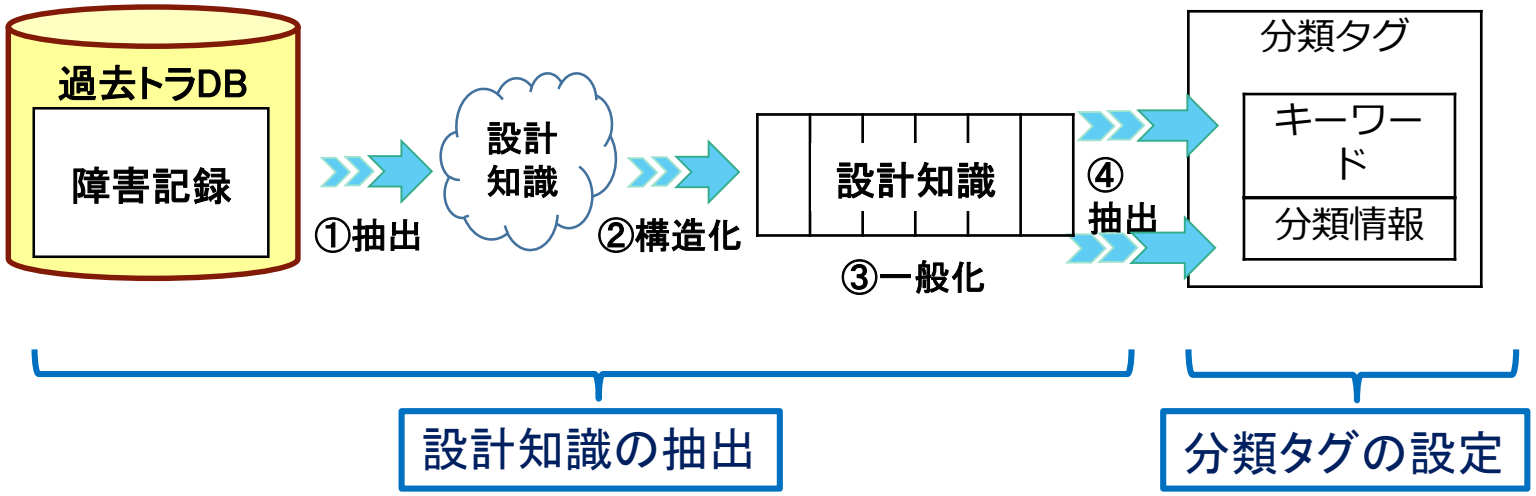
機能や処理を設計することが出来る知識。その機能や処理についての知識が無ければ設計出来ない。ここで言うところの機能や処理はソフトウェアで実現する機能や処理。

（参考）手法・技法に関する知識

- リスク分析に関する知識（例：HAZOP、STAMP（参考文献[5]））
- レビュー手法に関する知識（例：ピアレビュー、インスペクション）
- テスト技法に関する知識（例：同値分割、境界値分析）

3. 障害の発生を未然防止する設計知識とは

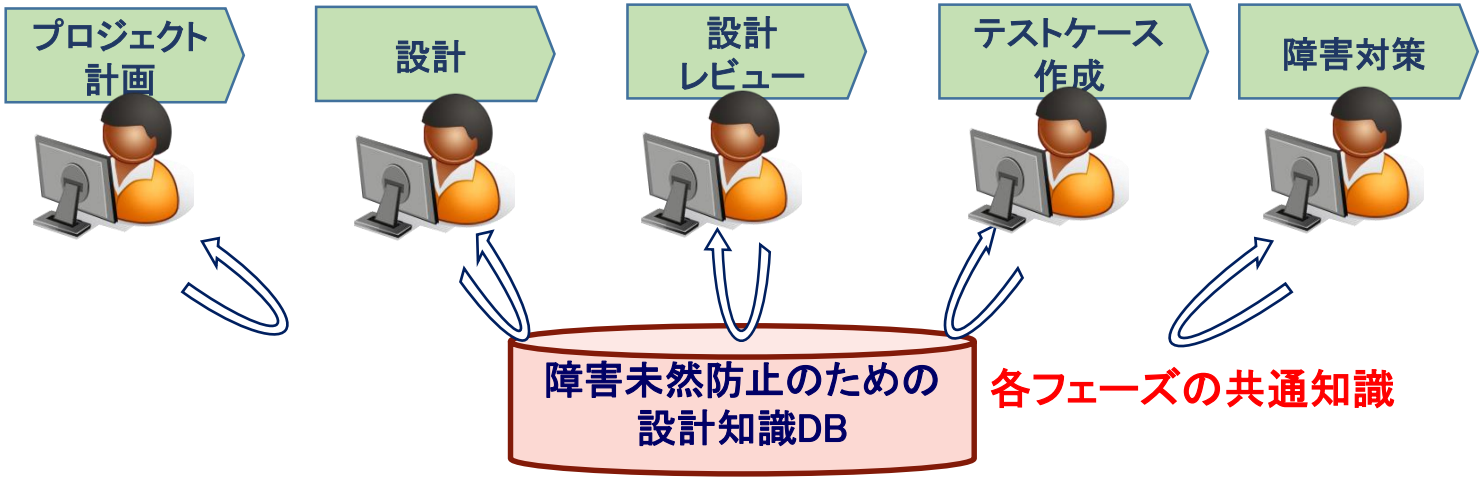
設計知識の整理手順（概要）



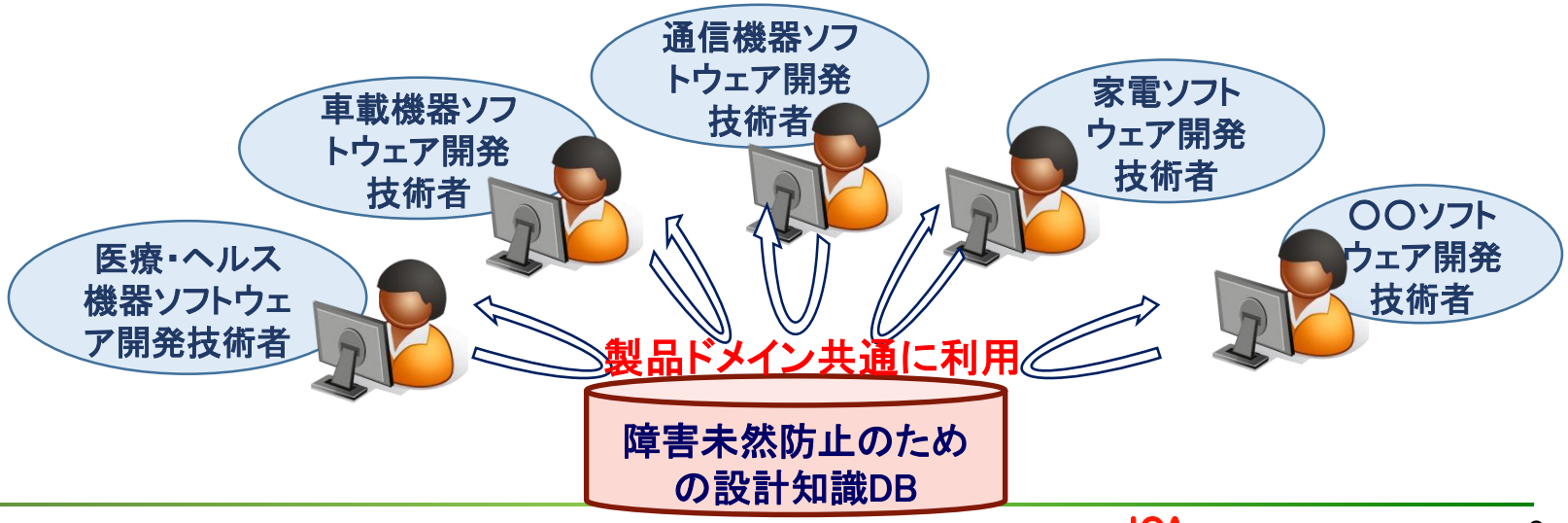
①「過去トラDB」の障害情報記録から設計知識を抽出する
②抽出した設計知識を構造化する
③さらに設計知識を一般化表現に変換する
④設計知識の再利用を促すための分類タグを抽出する

4. 設計知識の活用

- ソフトウェア開発の様々なフェーズの共通知識として利用



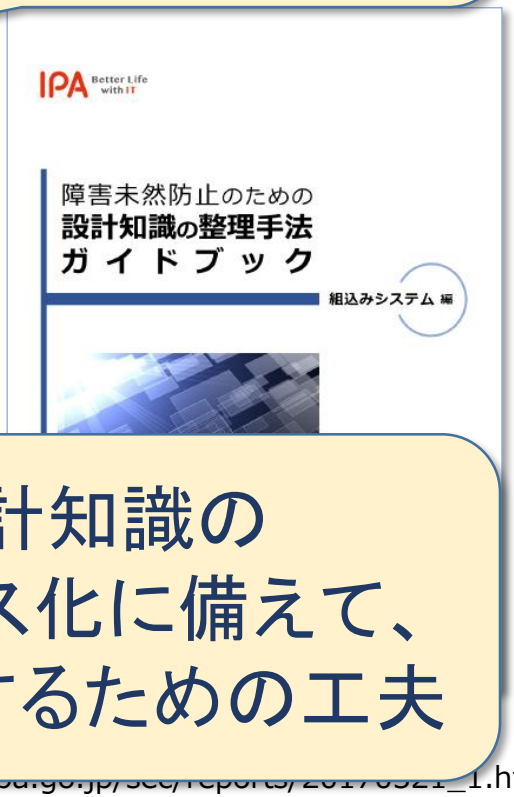
- 製品ドメインに依存しない共通の設計知識として利用



AGENDA

1. 背景と目的
2. 本手法の位置づけ
3. 障害の発生を未然防止す
4. 設計知識の活用
5. 設計知識の構造化
6. 設計知識の再利用
7. 設計知識の整理手法（
   - 設計知識の抽出
   - 設計知識の分類とタグ付
8. まとめ

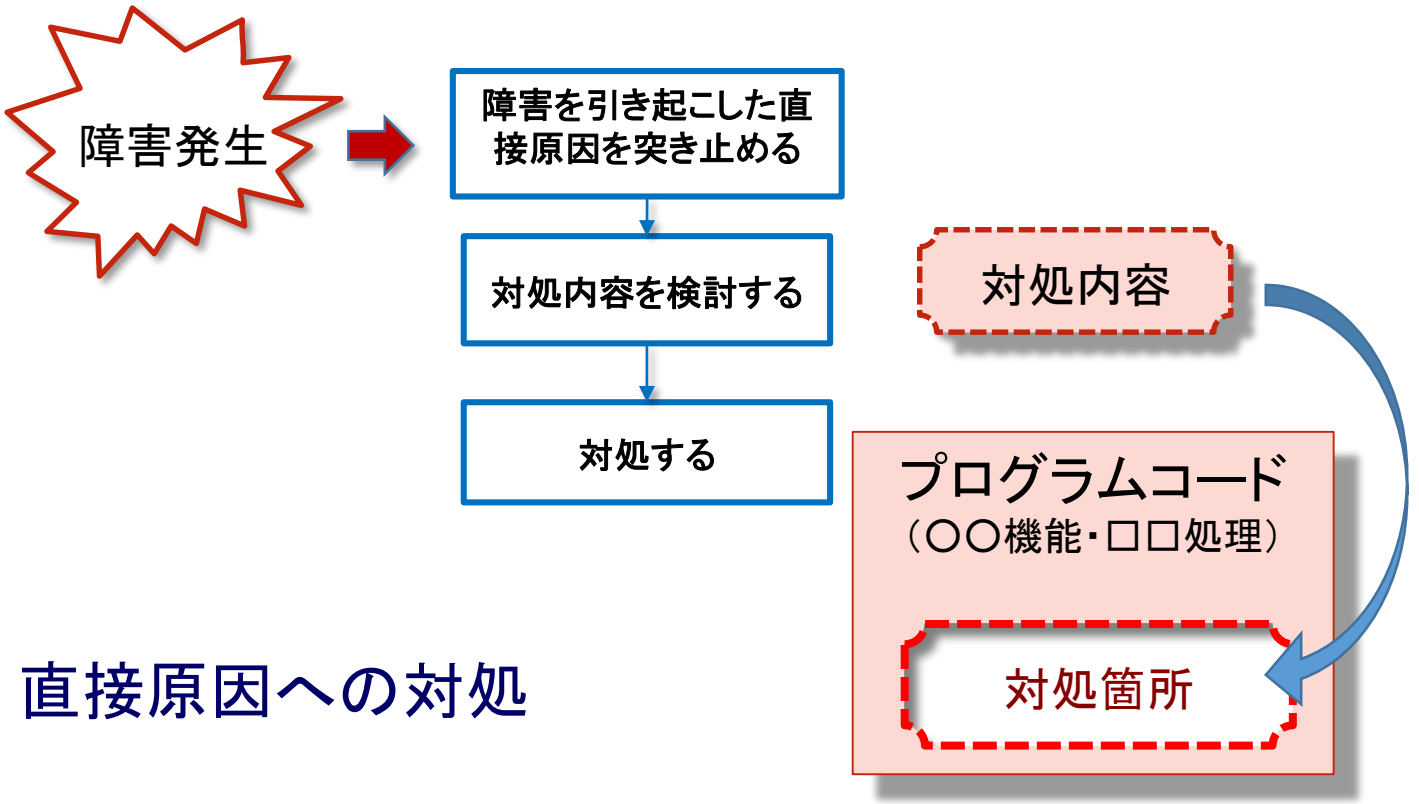
障害未然防止のために
伝えるべき内容と、
その表現の仕方



抽出した設計知識の
データベース化に備えて、
活用し易くするための工夫

https://www.ipa.go.jp/sec/reports/20170321_1.html

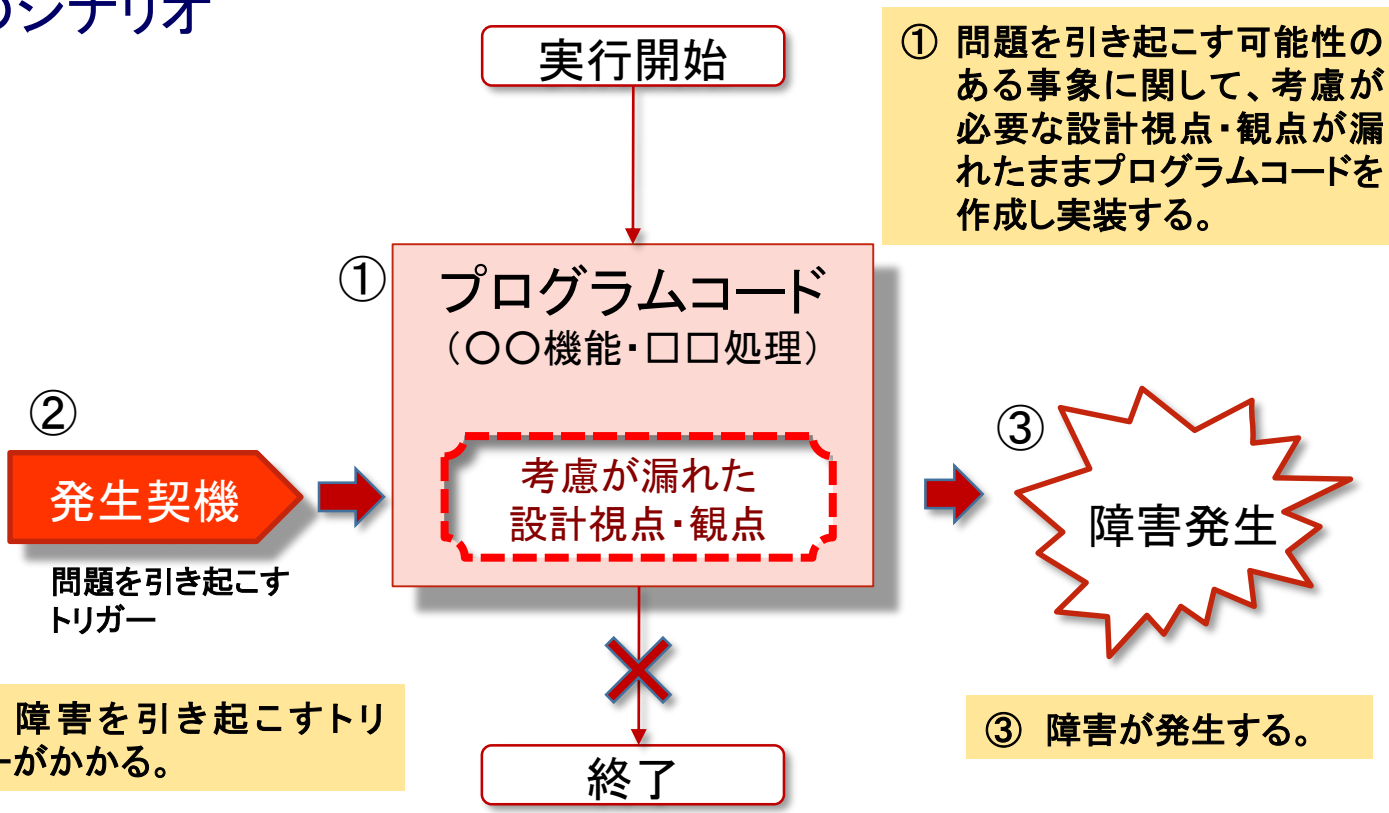
設計知識として伝えるべき事(1)「障害未然防止の対処」



〇〇〇機能には△△△が必要であることを伝える。障害未然防止のために。

設計知識として伝えるべき事(2)「何故問題を引き起こすのか」

障害発生のシナリオ

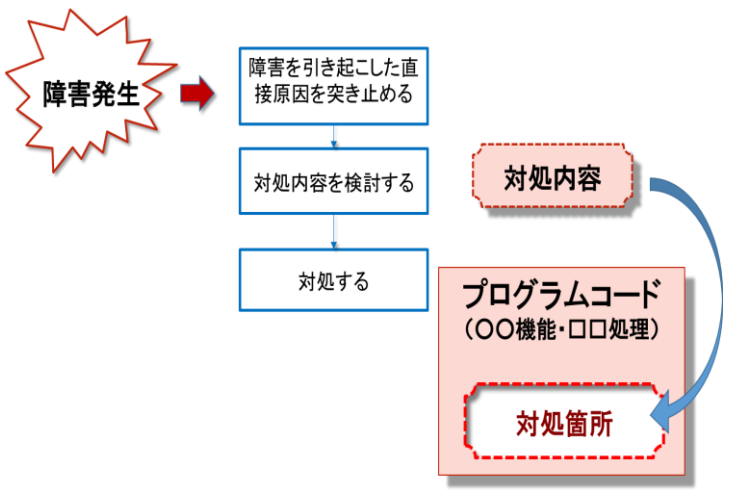


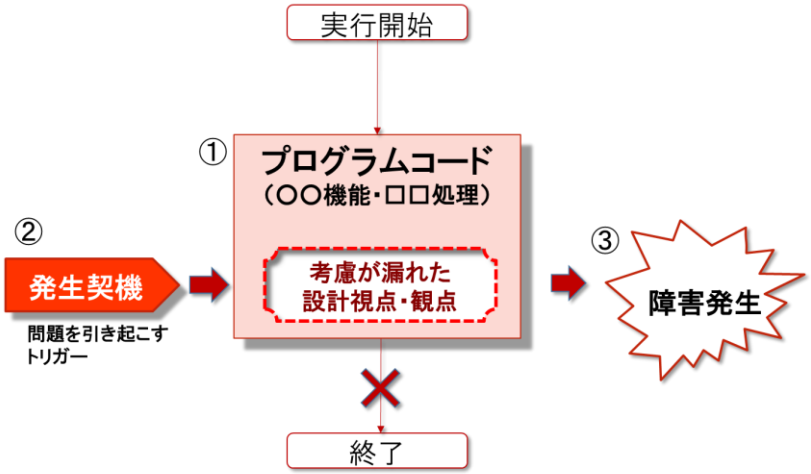
問題を引き起こす「発生契機」を伝える。
「考慮が漏れていたこと」や「不足していた知識」を伝える。

5. 設計知識の構造化

設計知識の文脈と構造（1）

設計知識の知識要素を文脈にする

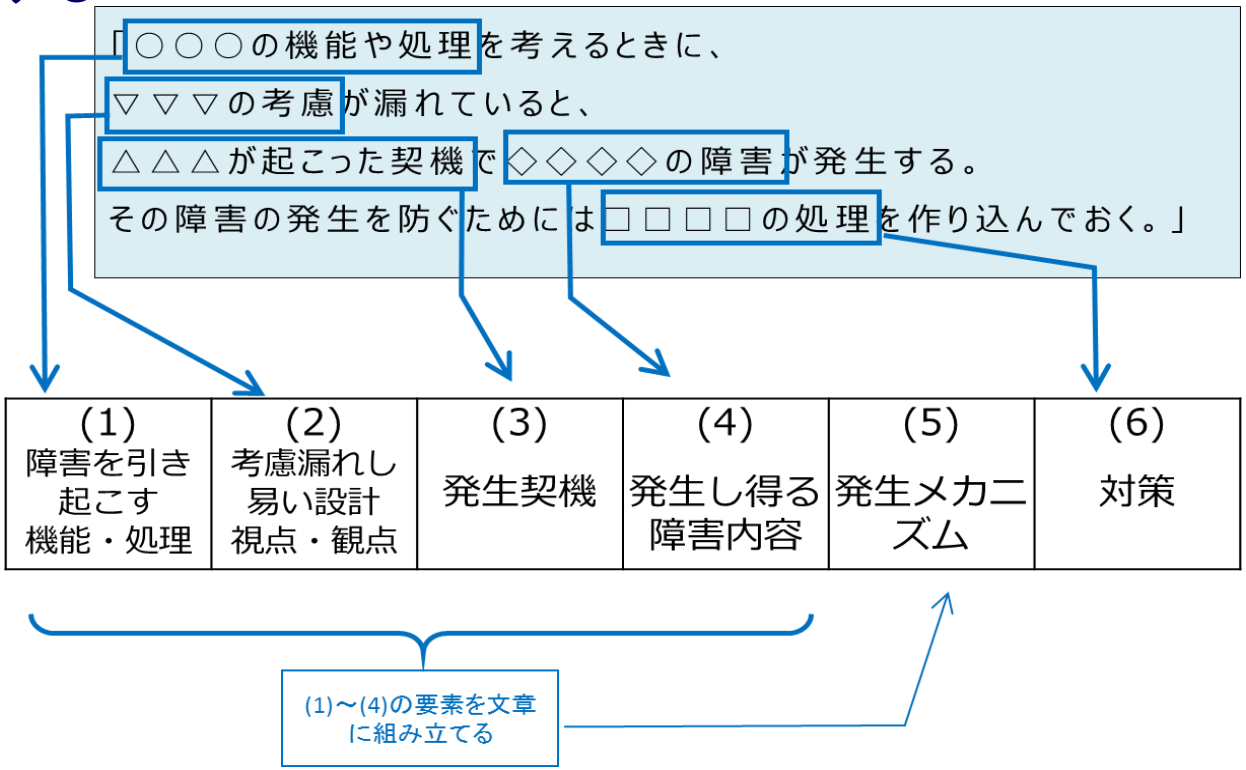




設計知識の文脈：
「〇〇〇の機能や処理を考えるときに、
▽▽▽の考慮が漏れていると、
△△△が起こった契機で◇◇◇◇の障害が発生する。
その障害の発生を防ぐためには□□□□の処理を作り込んでおく。」

設計知識の文脈と構造(2)

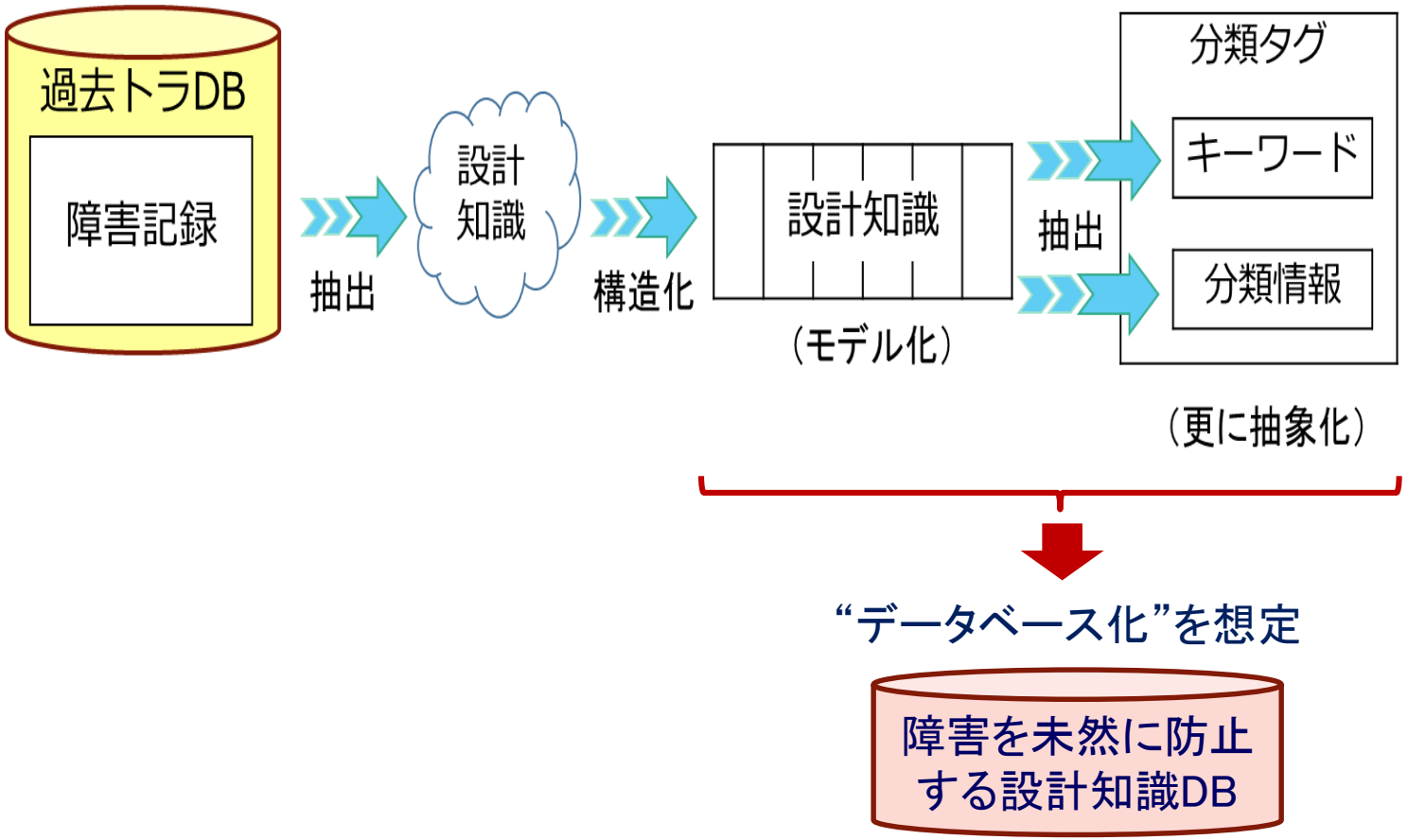
設計知識を構造化する



- 設計知識をパターン化して頭の中に整理し易くする
- 知識要素(1)～(4)は、不具合を混入させて障害が発生するシナリオの構成要素を表す。
- 知識要素(5)は、(1)～(4)の要素を文章に組み立てた「何が」、「どうして」、「どうなる」を表す。
- 知識要素(6)は対策を表す。※(5)と(6)は文章で簡潔に説明する。

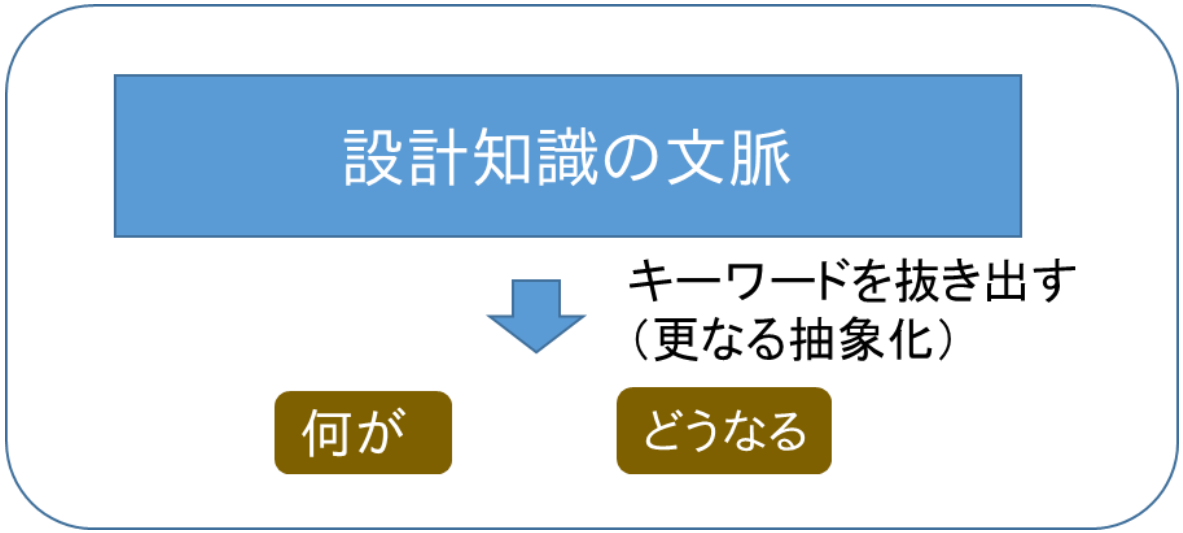
6. 設計知識の再利用

設計知識の再利用性を高める更なる抽象化



6. 設計知識の再利用

キーワード抽出



- 直観的に何に役立つ知識なのか分かる工夫をする
- 障害が発生する観点で、設計知識の文脈から「何が」「どうなる」を抜き出す　⇒　“キーワード”
- “キーワード”をタグに設定

6. 設計知識の再利用

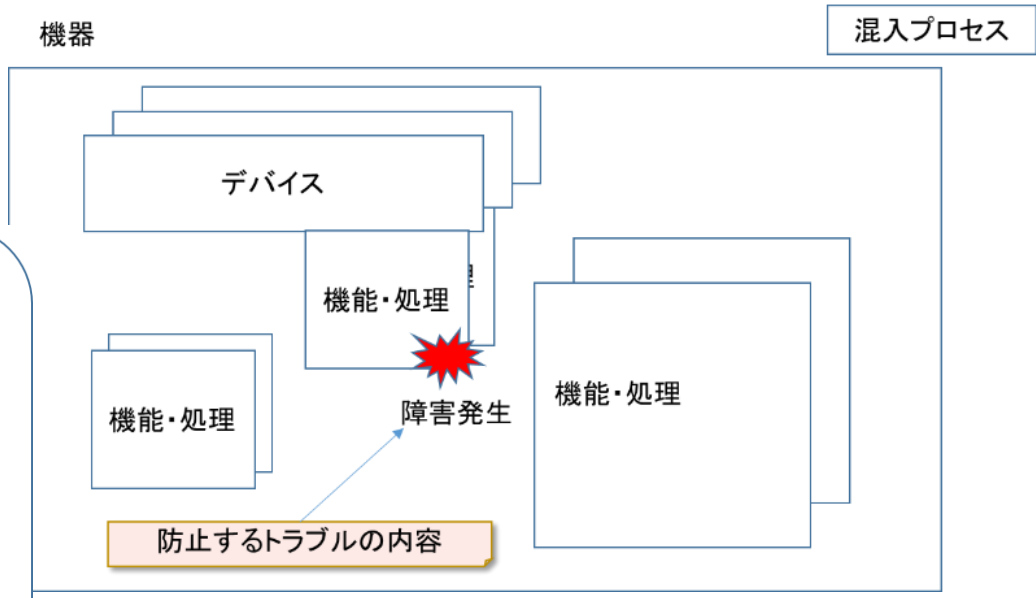
分類情報の抽出

設計知識の文脈

分類情報を抜き出す

機能・処理　デバイス・機器

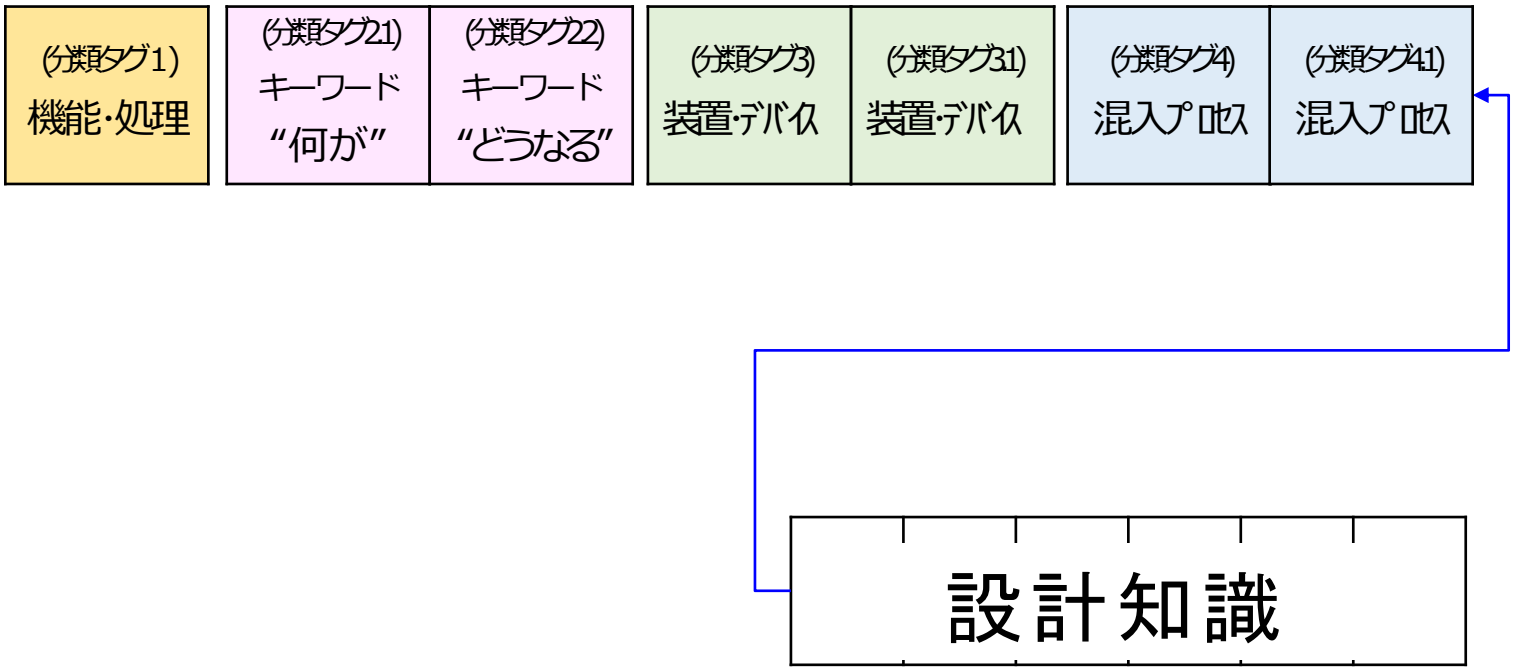
混入プロセス



設計知識の分類モデル（参考）

- ソフトウェア技術者の頭の中でどんな切り口で整理されていると、思考時に参照され易いか。
- このような観点で設計知識を分類。

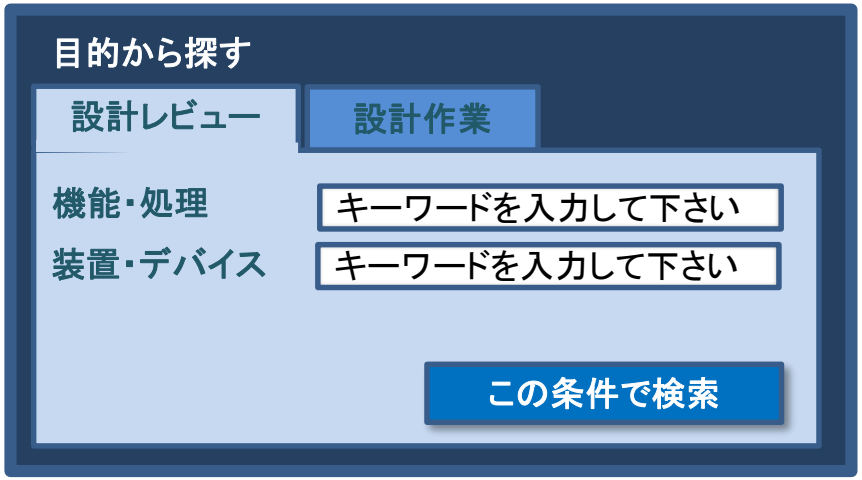
分類タグの設定

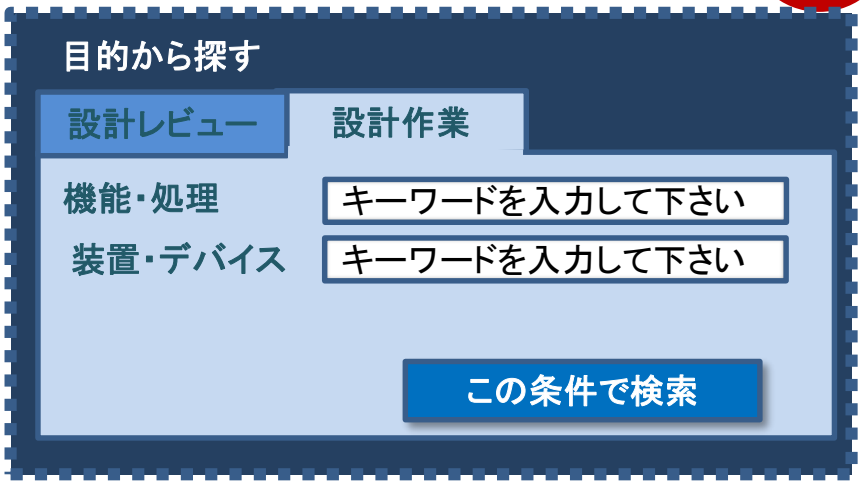


設計知識データベースの検索イメージ（参考）

◆検索の観点でタグを設定する(例1)「利用者の目的別に設計知識を探し易くする」

例





◆検索の観点でタグを設定する(例2)「利用者の関心を引くような分類を示して検索を促す」

設計知識データベースの検索イメージ（参考）

◆検索結果の観点でタグを設定する　「利用者が知りたい情報を短い見出しで表示」

例

並べ替え:　登録日付順　知識レベル順　〇〇〇順

101件中　1～25件を表示　[1 | 2 | 3 | 4 | 5]次の25件▼

知識ID　A-200213

●機能／処理: 割込み・例外割込み　●装置／デバイス: －　●トラブル症状: システム異常、停止　●混入プロセス: －

【発生契機】　ノイズ
【機能・処理】　割り込み処理
【考慮漏れし易い設計視点・観点】　想定していない例外割り込みが発生したときの考慮漏れ
【発生し得るトラブル内容】　機能実行中に例外割り込みが発生することでシステム異常・停止等の障害を引き起こす
【発生メカニズム】　割り込み要求端子にノイズが入力すると、不定な値を使用して割り込み処理が起動される場合がある。・
【対策】　割り込み処理起動時に正常割り込みであるかを判断し、不正な割り込みであれば何もせずに割り込みプログラムを・・
（登録日）2016年9月1日

■トラブル事例：教訓集No8

知識ID　A-500225

●機能／処理: デバイス管理TBL　●装置／デバイス: －　●トラブル症状: デバイス接続エラー　●混入プロセス: －

【発生契機】　最大接続数
【機能・処理】　複数の接続先に接続可能なシステム／装置において、接続先管理テーブルを動的に作成する処理
【考慮漏れし易い設計視点・観点】　接続オプションにより、接続先管理テーブルに登録するデータサイズが変動する場合

AGENDA

1. 背景と目的
2. 本手法の位置づけ
3. 障害の発生を未然防止する
4. 設計知識の活用
5. 設計知識の構造化
6. 設計知識の再利用
7. 設計知識の整理手法（ミニ演習）
   - **設計知識の抽出**
   - **設計知識の分類とタグ付け**
8. まとめ

【ミニ演習】障害事例（2件）を用いて設計知識を抽出し、再利用のための分類タグを設定します。

https://www.ipa.go.jp/sec/reports/20170321_1.html

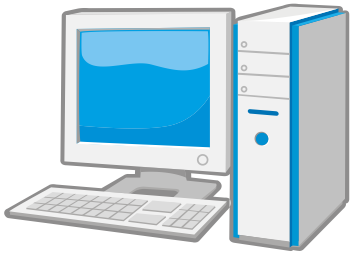
障害事例①

製品の特長

- 店舗用の窓口対応業務システム。
- 業務処理に必要なデータは、日次でセンターサーバから受信する。
- 当日行った業務処理の集計データは、バッチ処理で自動的に所定の時間にセンターサーバに送信される。

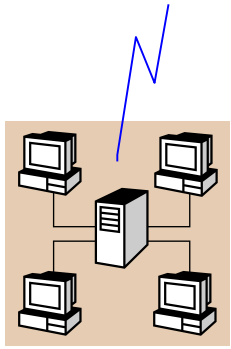
観察できる現象

①ある日、窓口対応員が当該装置の電源をOFFにして帰宅。
②翌朝、業務システムが正常に立ち上がらず。
⇒ 店舗業務運営ができない状態が発生。



内部の事象

前日の業務処理集計データの送信状態が途中で停止し、未完了状態であった。



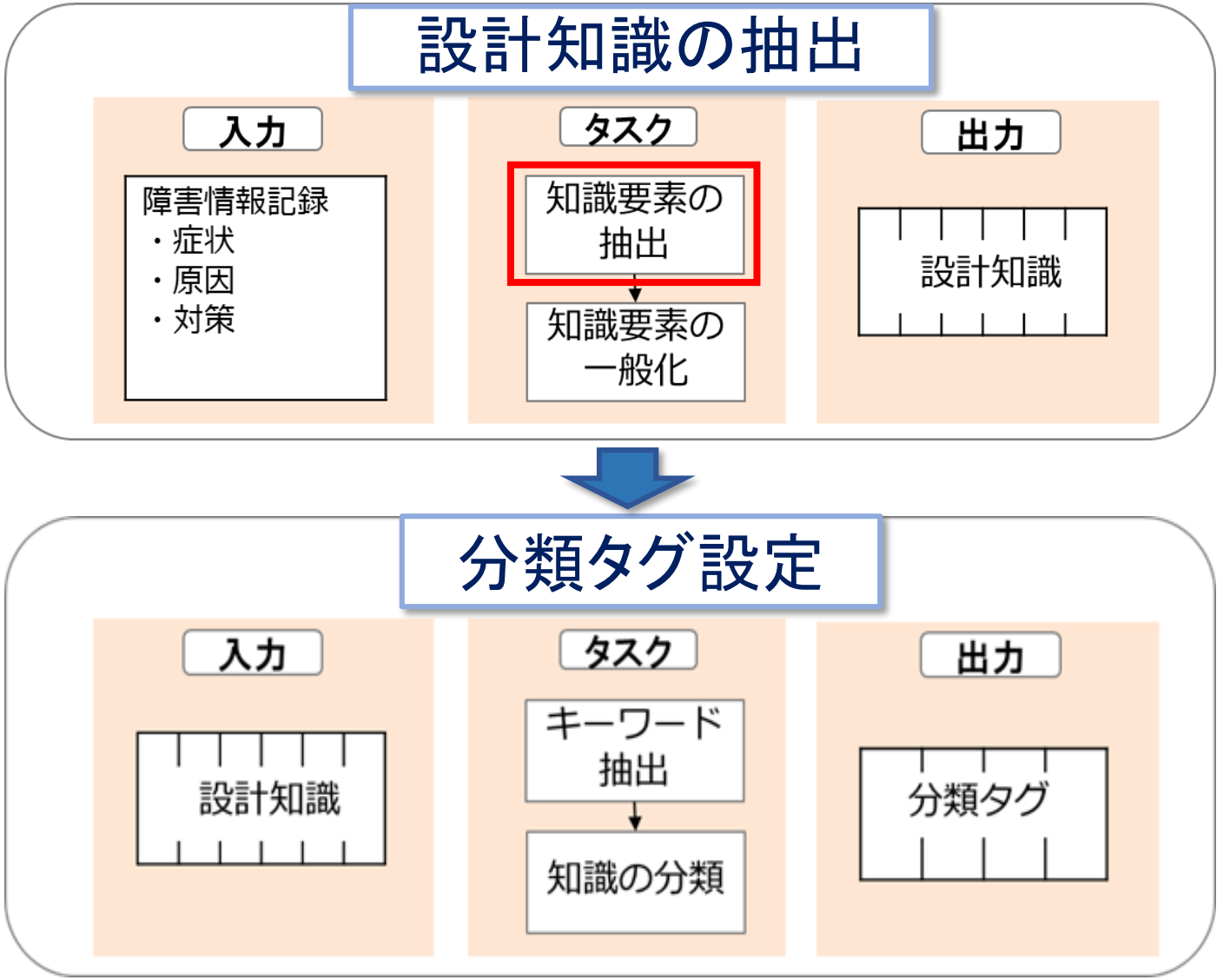
直接の原因

前日の業務処理集計データをセンターサーバに送信中にバッチ処理が強制終了されたことが直接原因。本来、送受信中に強制終了されたとしても、次回再開した際に送信未終了分を再送する等のリカバリ処理が実施されるべきであったが、そうした事態が想定されておらず、リカバリ機能が未実装だった。

直接原因への対策

センターサーバとの送受信処理中に強制終了された場合の再送、再開時処理を実装する。

設計知識の整理プロセス



設計知識の抽出

知識要素の抽出（1）

（手順）

障害情報記録

状況(症状)	直接原因	対処

障害発生シナリオを「何が」「どうして」「どうなった」の文脈で捉える。

何が	どうして	どうなった

背景にある要因を考える。

考慮漏れ？
考慮不足？
知識不足？

【ガイド】
経験を積んだベテラン技術者であれば、その障害を未然に防止できたかどうか考えてみる。ベテラン技術者は仕様書等に明示されていなくても、経験によって必要な対策を施すことができる。

障害事例①で試す

何が　窓口対応業務システム

どうなった　正常に立ち上がらなくなった

どうして　前日のバッチ処理が未完了であったため

考慮漏れ？
考慮不足？
知識不足？

バッチ処理が途中で強制終了された場合に、リカバリ処理が要ること。

設計知識の抽出

知識要素の抽出(2)

障害事例①から知識要素を抽出する

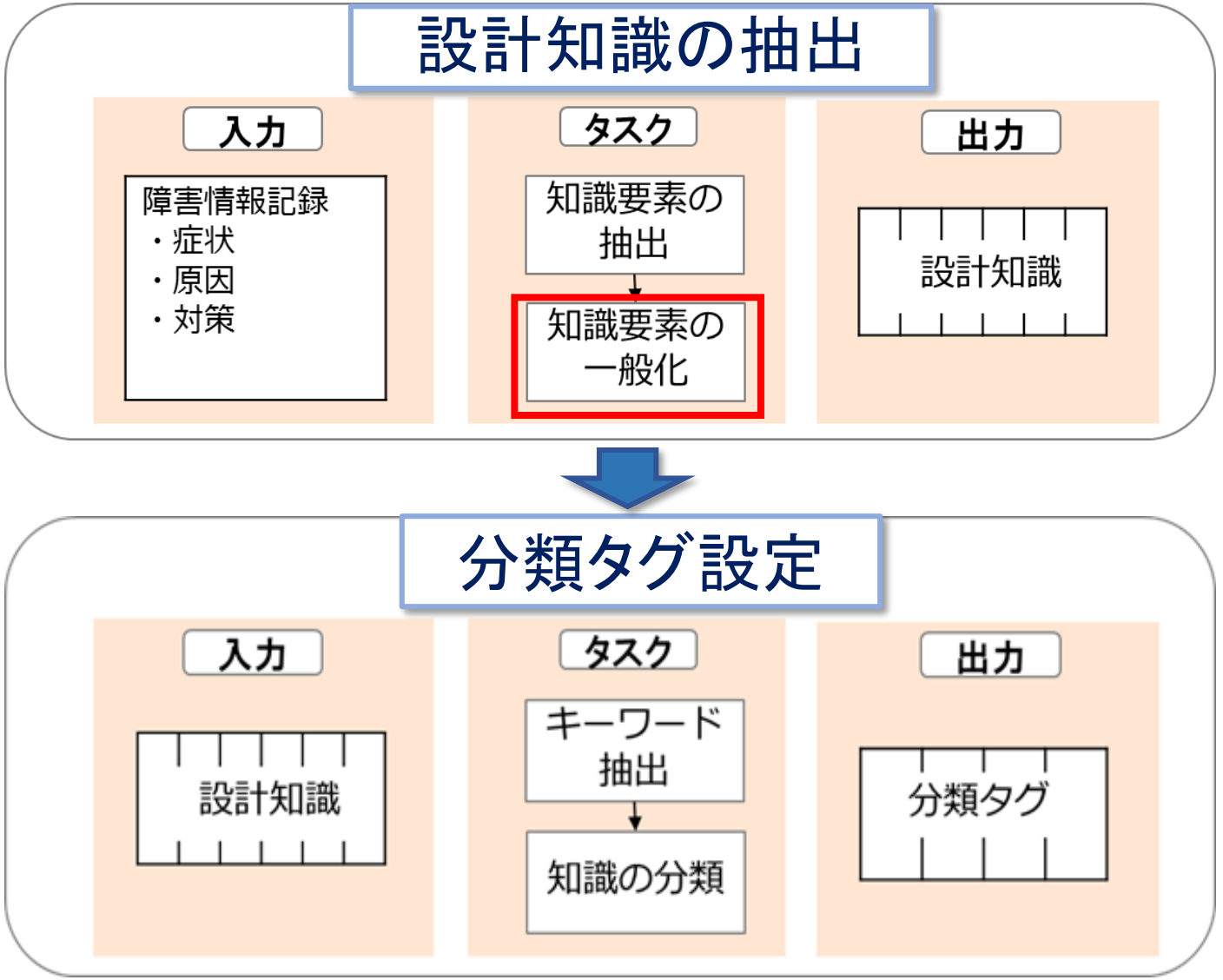
(手順) 前ページの「何が」「どうして」「どうなった」「考慮漏れ？・・」を
知識要素(1)～(4)対応させ、【ガイド】の文脈で簡潔に表現できるように修正する。

【ガイド】(1)の機能や処理を考えるときに、(2)の考慮が漏れていると、(3)が起こった契機で(4)の障害が発生する。
その障害の発生を防ぐためには(6)の処理を作り込んでおく。(5)は(1)～(4)を文章に組み立てたもの。

	(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策
[1]	バッチ処理	バッチ処理シーケンスが異常終了した後のリカバリ処理	バッチ処理の強制終了	バッチ処理が再起動できない。	集計データをバッチ処理でサーバに送信中にシステムを強制終了すると、データ送信処理が未完了の状態になる。 このような事態を考慮せず業務システムを設計すると、業務システムを再起動した際データ再送などのリカバリ処理が行われず、システムが正常に立ち上がらない。	起動処理には、その前の異常終了を想定したリカバリ処理を組み込む。
[2]	業務システムの起動処理	前回異常終了していた場合のリカバリ処理	システムの異常終了	業務システムが正常に立ち上がらない。	(同上)	(同上)

イメージの発想を構造的に表すことが目的なので、新たな発想があれば、構造的に表してみる。[1]を抽出したら“業務システムの起動処理”に観点が移り、[2]を抽出した。

設計知識の整理プロセス



設計知識の抽出

知識要素の一般化

入力	タスク概要	出力
・設計知識 （未一般化）	抽出した設計知識の各要素を一般化する。	・設計知識 （一般化）

入力

抽出した設計知識

(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策

タスク

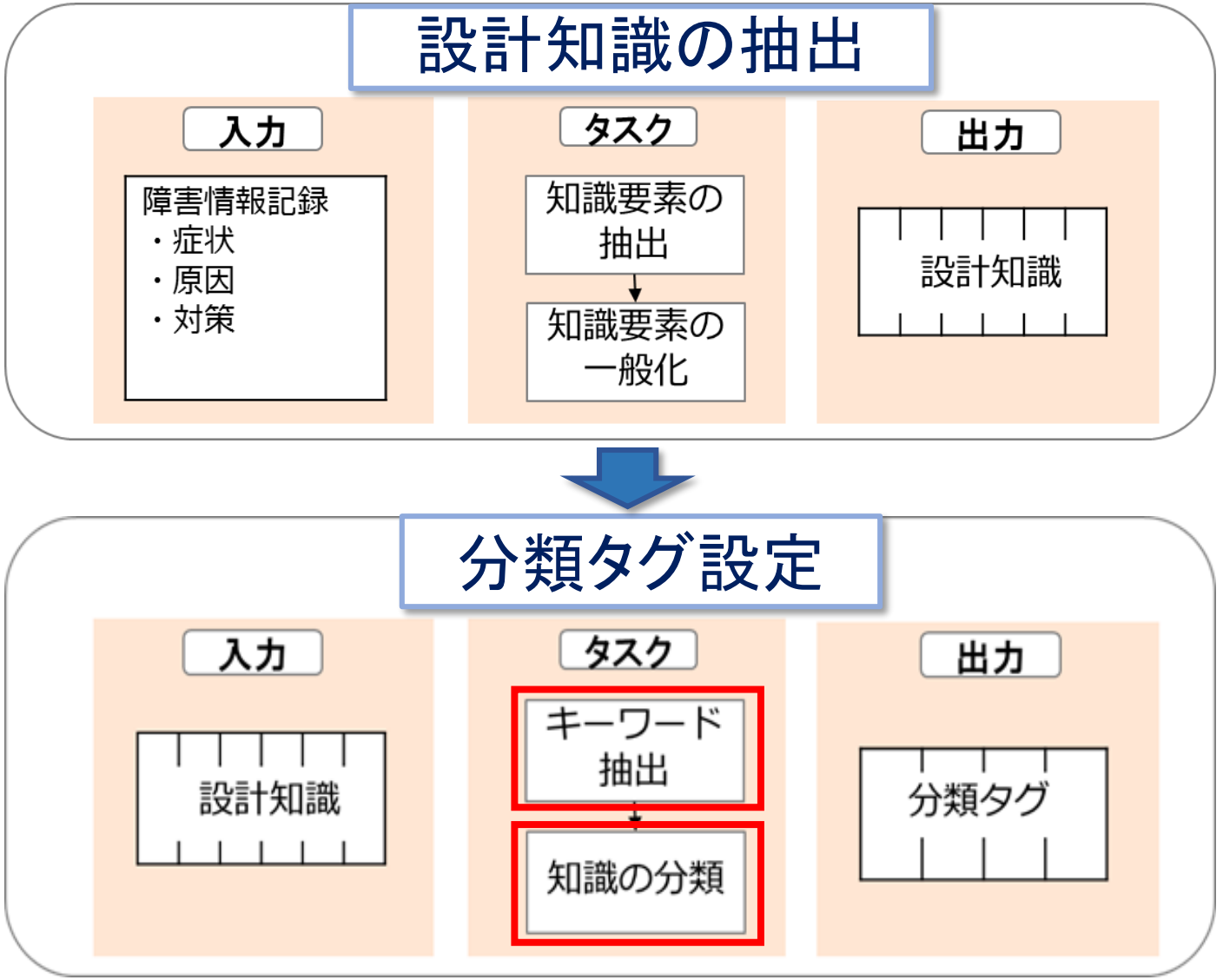
前のタスクで抽出した知識を

- **(1)～(6)の各要素に製品ドメインに依存する機能や処理を表す用語や表現等がある場合は、ソフトウェア共通に通じる用語や表現に修正する**
- **複数製品開発部門から検討グループを作り、メンバーが担当する製品に適用可能か否かを確認しグループとして結論をまとめる**

ことで一般化する。

※「一般化」手順の演習は省略。

設計知識の整理プロセス



分類タグ設定

キーワード抽出

障害事例①から抽出した設計知識にタグを設定する

(分類タグ21) キーワード “何が”	(分類タグ22) キーワード “どうなる”
業務システ…	正常に立ち…ない

→ 異常終了後の起動処理 / 起動失敗

下記の設計知識(1)～(6)を読まなくても直観的に、この知識が何に役立つのか分かるようにキーワードを設定する。

(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策
業務システムの起動処理	前回異常終了していた場合のリカバリ処理	システムの異常終了	業務システムが正常に立ち上がらない。	前日の業務処理で集計データをサーバに送信中にバッチ処理が強制終了され、データ送信処理が未完了のまま終了した。 このような事態を考慮せず業務システムを設計していたため、業務システムを再起動した際データ再送などのリカバリ処理が行われず、システムが正常に立ち上がらなかった。	起動処理には前回異常終了を想定したリカバリ処理を組み込む。

分類タグ設定

知識の分類

IPA

障害事例①から抽出した設計知識のタグを設定する（その2）

(分類タグ1) 機能・処理	(分類タグ21) キーワード “何が”	(分類タグ22) キーワード “どうなる”	(分類タグ3) 装置・デバイス	(分類タグ31) 装置・デバイス	(分類タグ4) 混入プロセス	(分類タグ41) 混入プロセス
起動処理	異常終了後の起動処理	起動失敗	業務システム	店舗用窓口システム		

・“機能・処理”を設定する。
・装置やデバイスに関連付けたい場合、“装置・デバイス”を設定する。

(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策
業務システムの起動処理	前回異常終了していた場合のリカバリ処理	システムの異常終了	業務システムが正常に立ち上がらない。	前日の業務処理で集計データをサーバに送信中にバッチ処理が強制終了され、データ送信処理が未完了のまま終了した。 このような事態を考慮せず業務システムを設計していたため、業務システムを再起動した際データ再送などのリカバリ処理が行われず、システムが正常に立ち上がらなかった。	起動処理には前回異常終了を想定したリカバリ処理を組み込む。

■演習

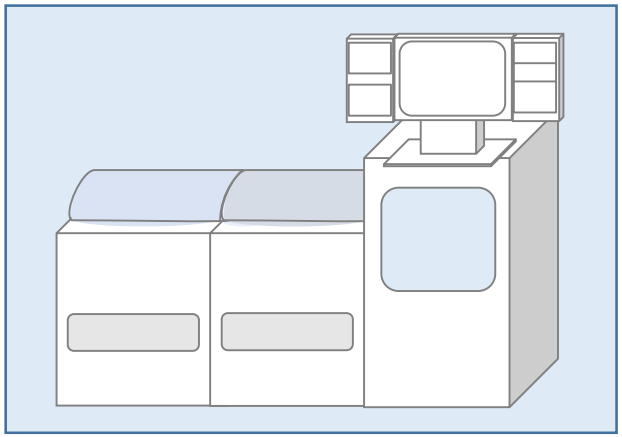
（30分）

演習

障害事例②

製品の特長

・電子部品がスペック通りの機能・性能を満たしているかを検査する装置。
・電子部品の検査は複数のテストで構成され、その全てのテストが良の場合は検査結果が良品となる。一方で、あるテストで不良になった場合は不良品と判断され、検査時間の効率化のため、通常その後のテストは行わない。
・検査機能をマスクできるモードがある。



観察できる現象

電子部品の検査では、一定の割合で不良品が発生するが、検査した全てが良品となった。しかし、その後の検査の工程で通常より多くの不良品が検出された。

内部の事象

①調査担当者が調査のため、不良にならないようにマスク設定した。
⇒調査終了後は、マスク解除しなければならないが、調査担当者がマスク設定を解除しない状態で放置。
②そのまま量産検査を開始。⇒検査は全て良品となった。

直接の原因

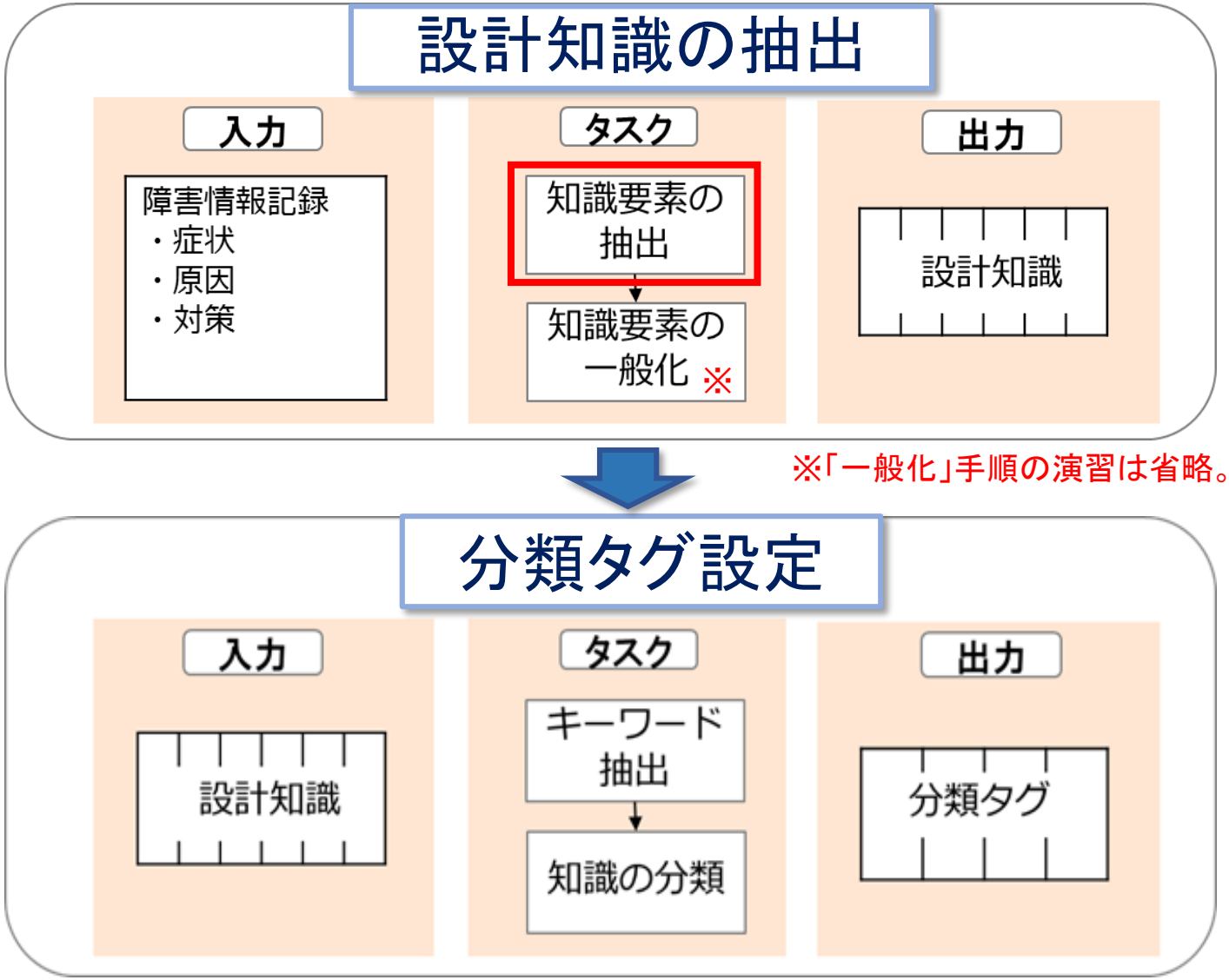
・全て良品となった場合には、異常の可能性があるとみなしていなかった。
・全て不良品の場合は直感的に検査が異常であるとわかるが、全て良品の場合にも検査が異常であると考えが及ばなかった。

直接原因への対策

全て不良品の場合と同様に、全て良品の場合も異常を通知するよう修正した。

演習

設計知識の整理プロセス



演習

設計知識の抽出　知識要素の抽出（1）

（手順）

障害情報記録

状況(症状)	直接原因	対処

障害発生シナリオを「何が」「どうして」「どうなった」の文脈で捉える。

何が	どうして	どうなった

背景にある要因を考える。

考慮漏れ？
考慮不足？
知識不足？

【ガイド】
経験を積んだベテラン技術者であれば、その障害を未然に防止できたかどうか考えてみる。ベテラン技術者は仕様書等に明示されていなくても、経験によって必要な対策を施すことができる。

障害事例②で試す

何が ＿＿＿＿＿＿＿＿

どうなった ＿＿＿＿＿＿＿＿

どうして ＿＿＿＿＿＿＿＿

考慮漏れ？
考慮不足？
知識不足？ ＿＿＿＿＿＿＿＿

演習 設計知識の抽出

知識要素の抽出（2）

障害事例②から知識要素を抽出する

（手順） 前ページの「何が」「どうして」「どうなった」「考慮漏れ？・・」を
知識要素（1）～（4）対応させ、【ガイド】の文脈で簡潔に表現できるように修正する。

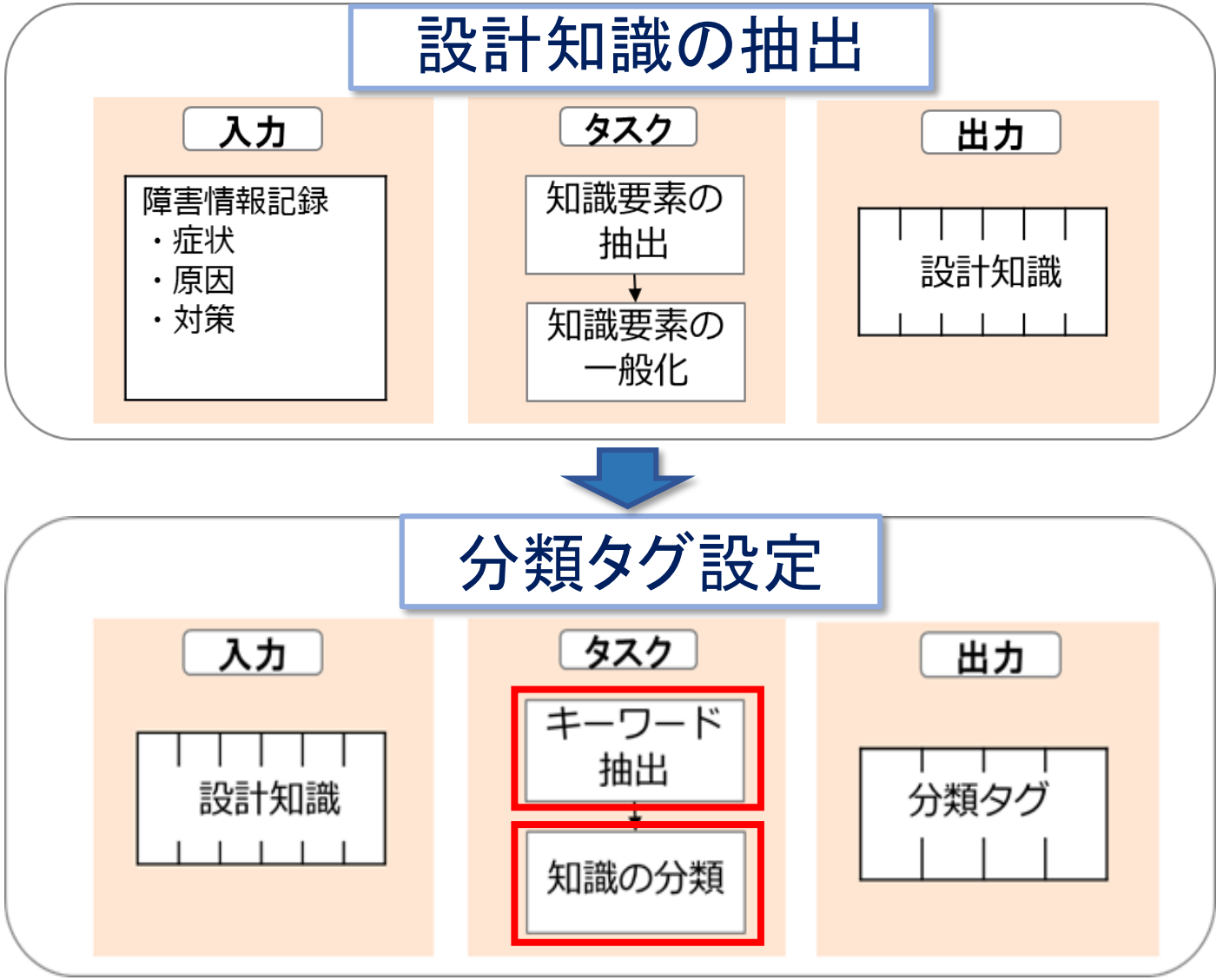
【ガイド】（1）の機能や処理を考えるときに、（2）の考慮が漏れていると、（3）が起こった契機で（4）の障害が発生する。
その障害の発生を防ぐためには（6）の処理を作り込んでおく。（5）は（1）～（4）を文章に組み立てたもの。

(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策

※障害を未然に防止することを念頭に置いて考えてください。

演習

設計知識の整理プロセス



演習

分類タグ設定

キーワード抽出

知識の分類

IPA

障害事例②から抽出した設計知識にタグを設定する

(分類タグ1) 機能・処理	(分類タグ21) キーワード “何が”	(分類タグ22) キーワード “どうなる”	(分類タグ3) 装置・デバイス	(分類タグ31) 装置・デバイス	(分類タグ4) 混入プロセス	(分類タグ41) 混入プロセス

・“キーワード”を設定する。

・“機能・処理”を設定する。

・装置やデバイスに関連付けたい場合、“装置・デバイス”を設定する。

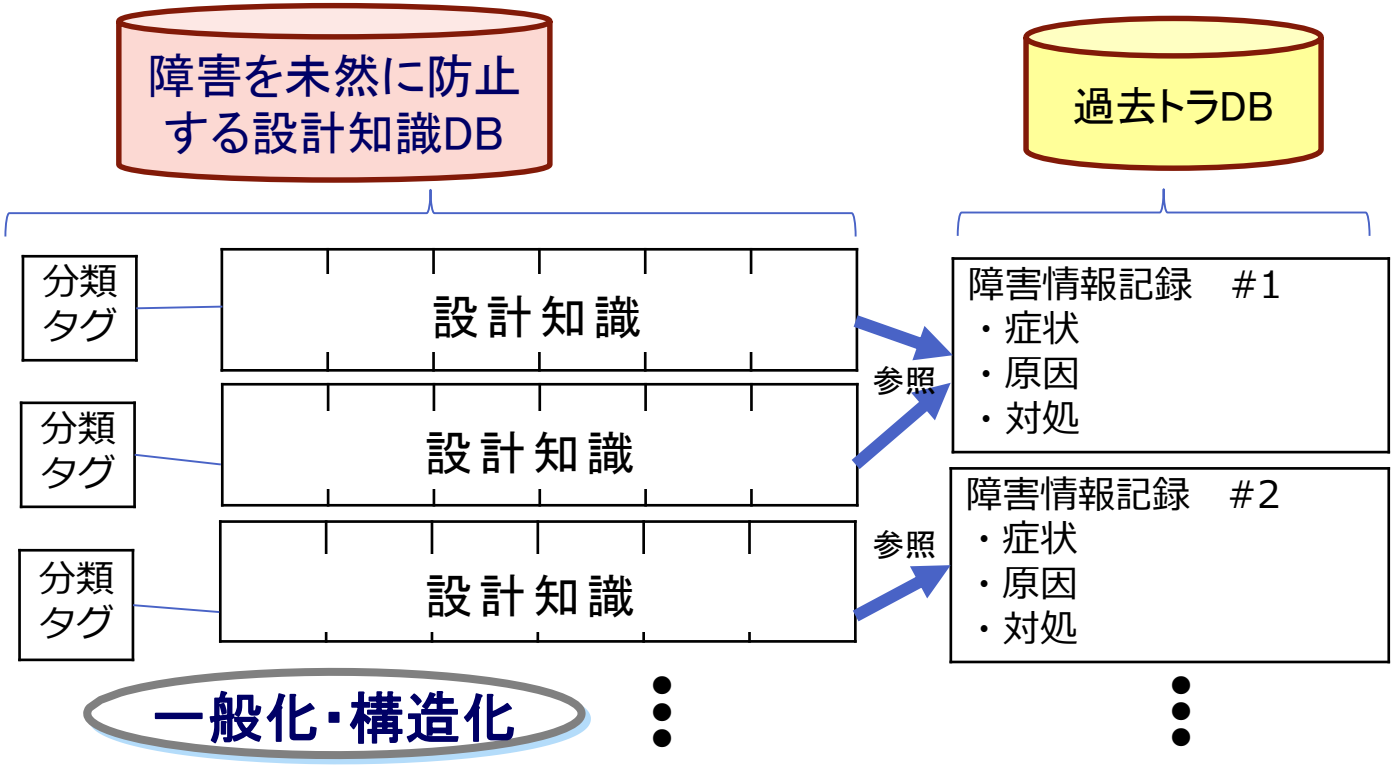
(1) 障害を引き起こす機能・処理	(2) 考慮漏れし易い設計視点・観点	(3) 発生契機	(4) 発生し得る障害内容	(5) 発生メカニズム	(6) 対策

まとめ

設計知識の活用

①設計知識の抽出 ⇦ 障害記録情報の活用

②分類タグの設定 ⇦ DB化による活用



ご清聴有難うございました