

GSNを用いて設計品質を 可視化してみよう

JASPICトワイライトフォーラム
2016.02.05, 港勤労福祉会館
(株)デンソークリエイト 宇都宮浩之

本日の予定

1 / 19

No.	項目	内容	時間
1.	(講義)GSN基礎	GSNの描き方について説明	5分
2.	(講義)事例紹介	ソフトウェア開発現場での活用事例の紹介	10分
3.	(演習)ソフトウェア開発に関する事例を使った演習	演習内容の説明	5分
4.		個人演習	20分
5.		休憩	10分
6.		グループ演習 ・個人演習結果に関する意見交換 ・グループ案のまとめ	50分
7.		グループ案の発表	15分
8.		まとめ＆質疑応答	5分
Total			120分

トヨタ車の大規模リコール問題から得られる示唆

～2010年：トヨタ車の「意図しない加速」にて被害を受けたと計320件以上の訴訟発生

2011年：米国運輸省・NASAによる原因調査により、トヨタ車には欠陥がないことが判明

2012年：訴訟の長期化によるイメージ低下を恐れ、トヨタは和解（支払い）に応じる

Q: そもそも、なぜ米国運輸省・NASAによる原因調査、第三者検証がなされたのか？

A: 「電子スロットルに欠陥がないこと」を証明する客観的な証拠をトヨタ側が提示できなかったため、米当局の指示によって第三者検証が実施された



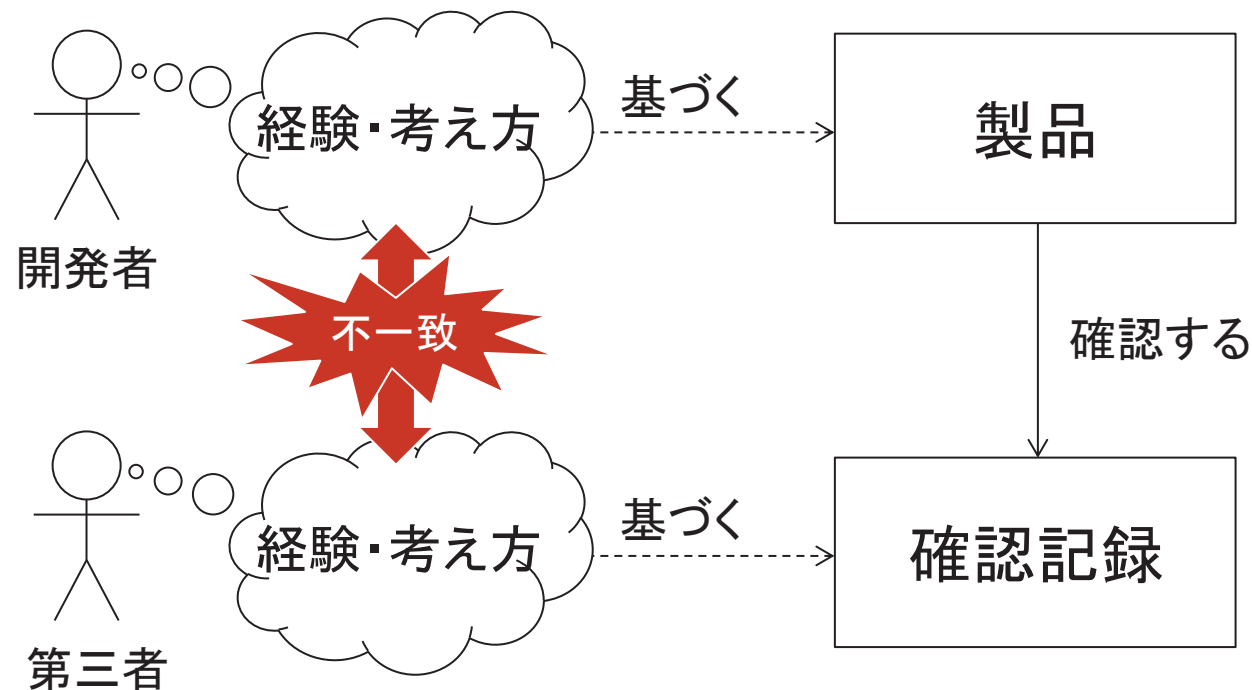
もしも、トヨタ側が早い段階で「電子スロットルに欠陥がないこと」を証明する客観的な証拠を提示できていれば、もっとうまく、そして早く経済的に和解できた可能性がある

今後のシステム開発における「転ばぬ先の杖」が期待されている

「転ばぬ先の杖」に期待されること

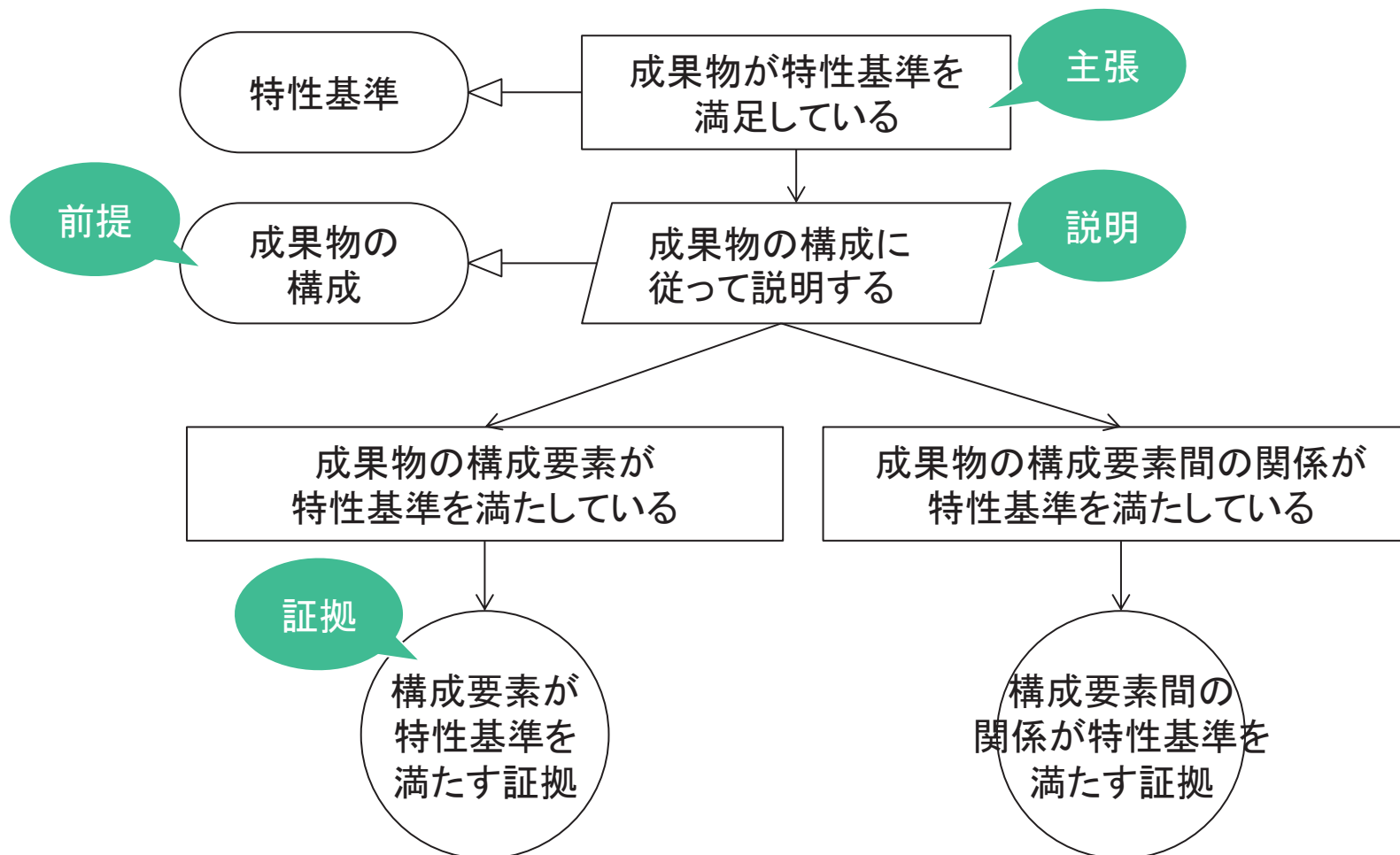
3 / 19

- 製品開発の過程を経験していない第三者は製品の品質を知る術がない
 - 開発者は高品質な製品を作ってきた自信はある
 - しかしながら、その高い品質を論理立てて説明できる道具がない...

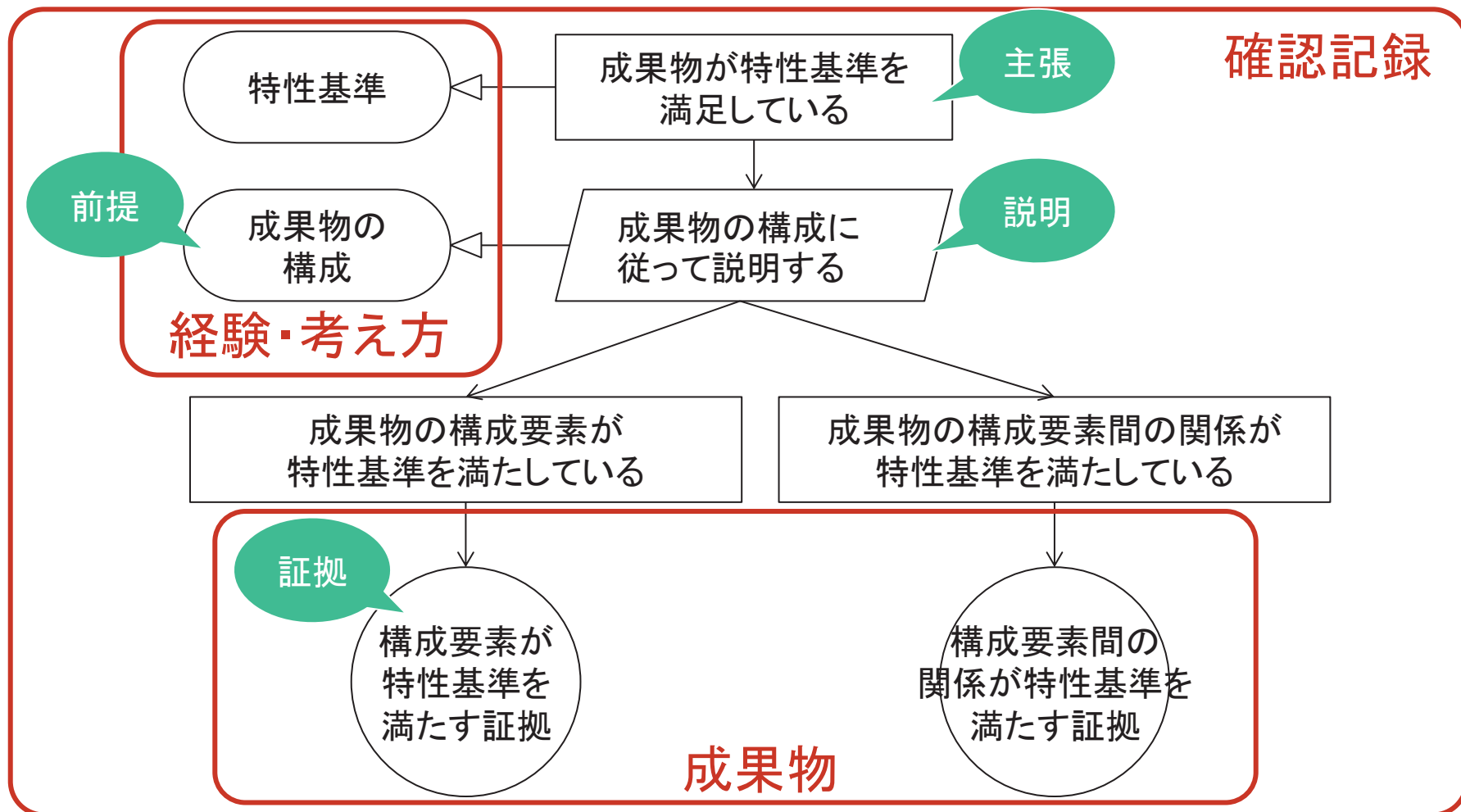


開発者の意図を正しく第三者に説明できる必要がある

- 相手と合意形成できている前提に基づき上位の主張を下位の主張に分解
- 最下位の主張の妥当性を証拠に基づいて説明することで主張全体が特性基準を満足できていることを説明する

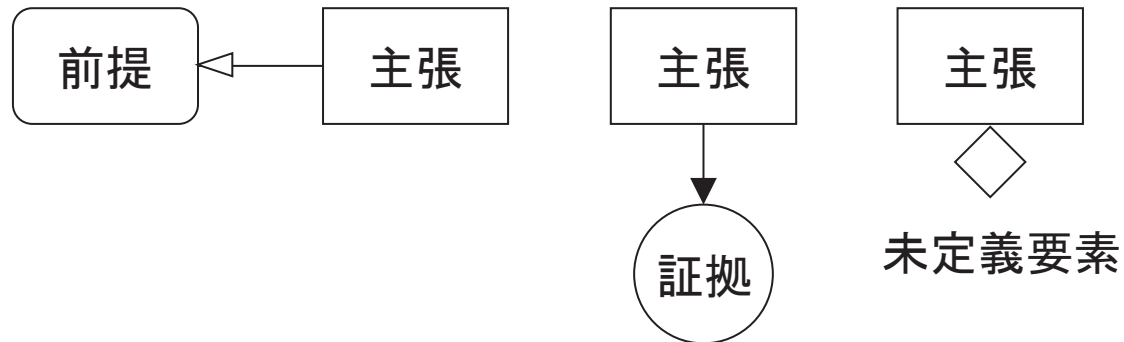


- 相手と合意形成できている前提に基づき上位の主張を下位の主張に分解
- 最下位の主張の妥当性を証拠に基づいて説明することで主張全体が特性基準を満足できていることを説明する

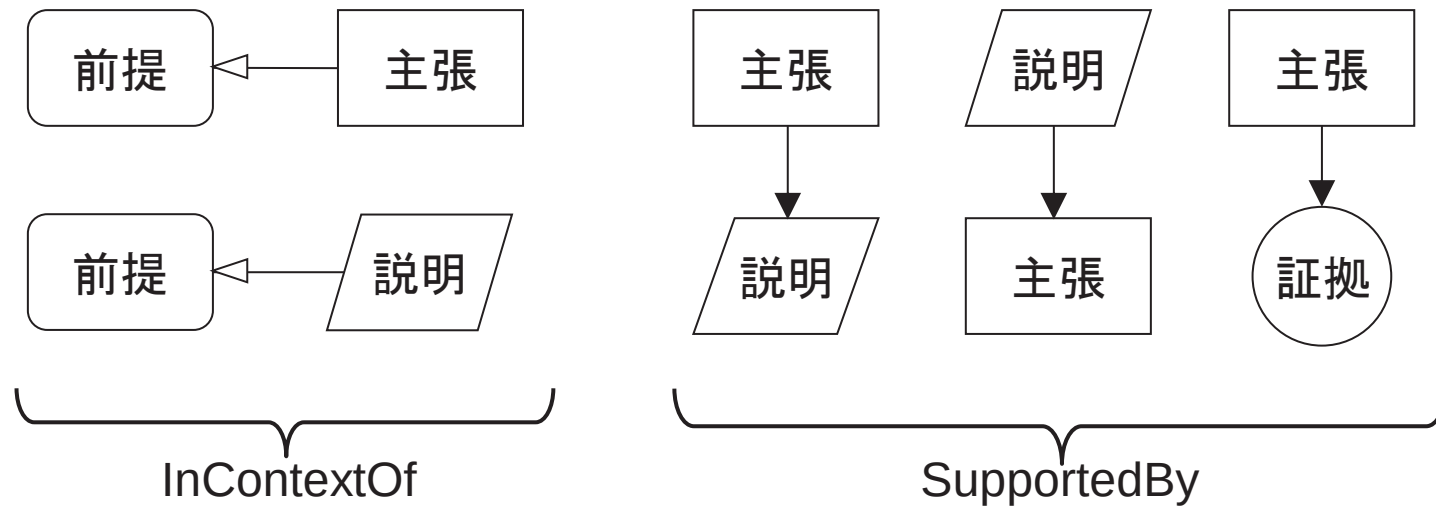


ノード名	記号	説明
Goal		相手に説明したい「対象が達成すべき状態」を示す。 S+Vの形をした命題であるべき。 例)「システムは安全である」
Strategy		上位の主張を下位の主張に分解する仕方の説明を示す。 例)「識別されたハザード毎に説明する」
Context		主張や説明が基づく相手と合意済みの情報を示す。 例)「リスク分析の結果得られたハザードのリスト」、 「ソフトウェアの構造」など
Solution		主張が達成できていることを示す証拠(証跡)を示す。 証拠は明確に定義されたドキュメントです。 例)「テスト報告書」、「運用記録」
Undeveloped		まだ具体化できていない主張や説明であることを示す (未定義要素)。

- リーフは「前提」、「証拠」、「未定義要素」のいずれかです。



- 矢印は2種類あります。「前提」は「主張」もしくは「説明」に付与されます。



ソフトウェアの品質を見える化してみます

8 / 19

<インタフェース仕様>

```
ret = ConvMsec(unsigned short sec, unsigned long *msec);
```

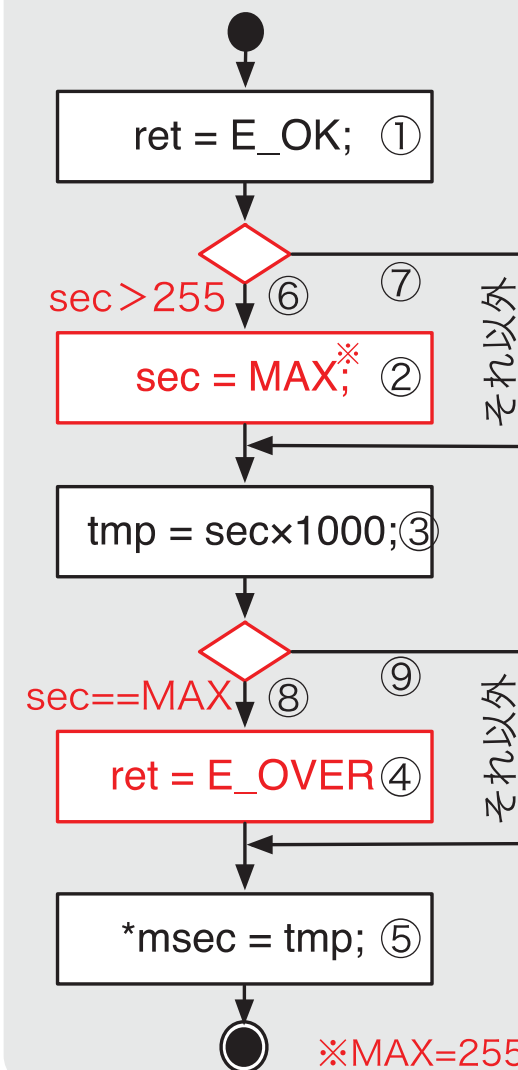
<変換規則>

- ・ secを1000倍した値を*msecに格納し、E_OKを戻り値とする。
- ・ **secが255より大きい場合は*msecに255000を格納し、E_OVERを戻り値とする。**

<設計品質レビューの報告内容>

確認事項	妥当性判断	証拠	妥当性判断の根拠
テスト項目数は十分であるか？	OK	テスト仕様書	既存処理をコードレビューで押さえ、追加処理の境界値に関するテスト項目を抽出。
：	：	：	：
仕様を満足することが確認されているか？	OK	テスト報告書	テスト仕様書の該当項目がすべて合格している

<処理の流れ>



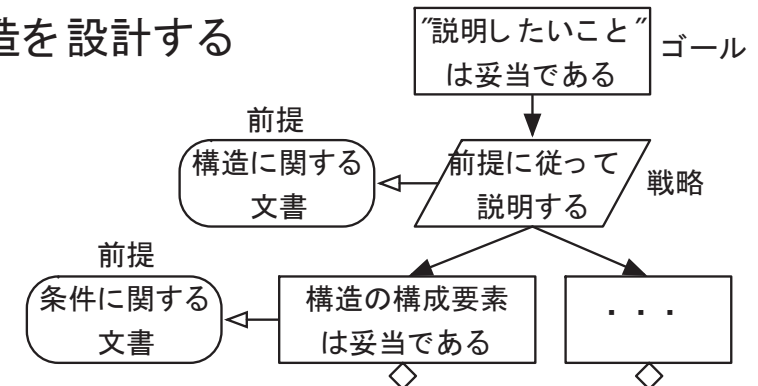
手順1：前提となる文書を揃える

- ・ 相手と合意形成できている文書を揃える
- ・ 不足する場合は右記の4 状態を念頭に新規に用意する

相手	知らない	③文書化して理解を得る	④一緒に文書化する
	知っている	①合意形成できている	②教えてもらって文書化
		知っている	知らない
		自分	

手順2：説明の構造を設計する

- ・ 手順1 で揃えた文書を前提として説明の構造を設計する

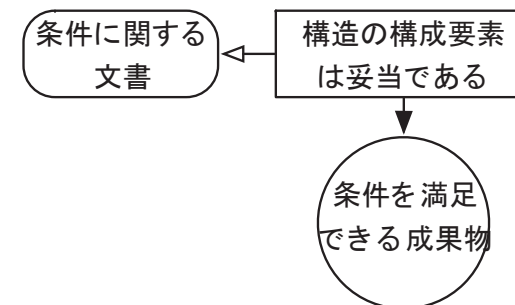


手順4：GSNで説明する

- ・ “構造に関する文書”に基づいて説明したいことを手頃な大きさに分解して説明する
- ・ 説明の妥当性は、“条件に関する文書”を成果物が満足していることで納得を得る
- ・ 上記流れで相手の納得を得られなければ手順1 から再チャレンジ！

手順3：成果物を証拠に紐づける

- ・ 説明の妥当性を最終的に支える証拠として条件を満足できる成果物を紐付ける



手順1：前提となる文書を認識する

① 手書きの文書を読み取る
② 文書中の文字を認識する
③ 不明な箇所をOCRの
O-A 装置に送る
④ 装置に送る前に
手書きに加工する

手順2：説明の構造を設計する

① 設計した説明と文書を認識した文字と物類の
構造を設計する

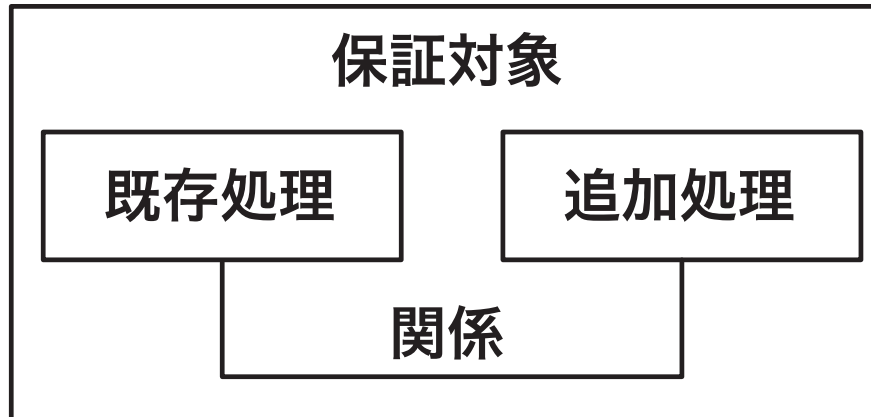
手順3：成果物を生成しに組む

① 説明の生成と知識を照合して生成した説明と
条件を決定する作業を行う

手順4：D-Caseで説明する

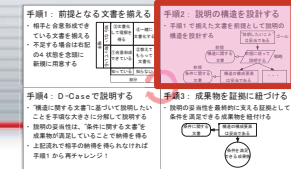
① “構造”と文字とを一致して説明したい
② このとき文字と一致して説明する
③ 説明の生成は、“条件”による文字を
生成する
④ 生成した文字と条件を一致させる
⑤ 一致した条件と物類を一致させれば
手書きに再現可能

- 「保証対象の構造」に従って上位者の考える合格基準を明文化



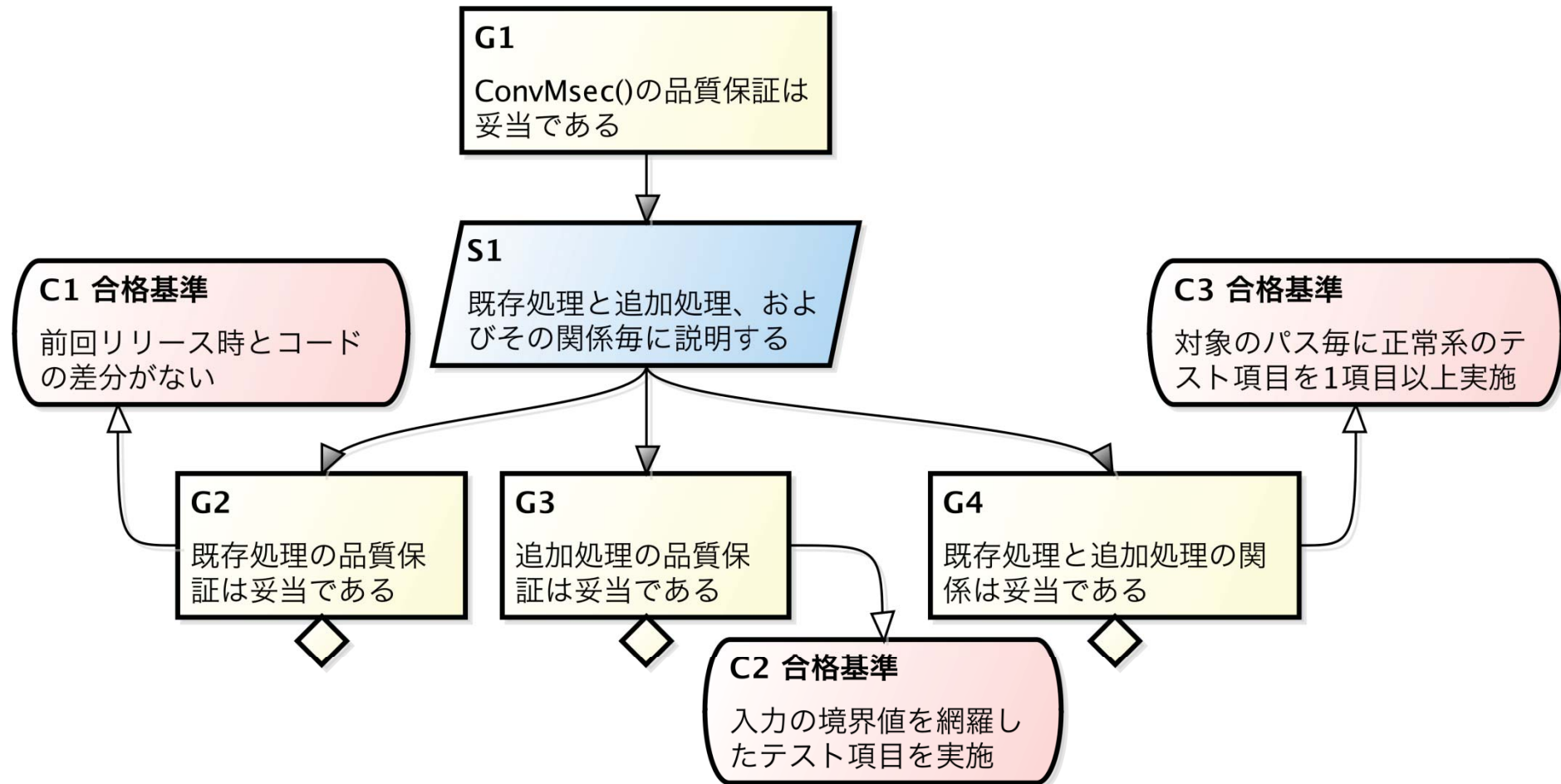
品質保証対象	合格基準
既存処理	(C1) 前回リリース時とコードの差分がない
追加処理	(C2) 入力の境界値を網羅したテスト項目を実施
既存処理と追加処理の関係	(C3) 対象のパス毎に正常系のテスト項目を1項目以上実施

手順2: 説明の構造を設計する

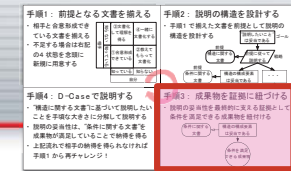


11 / 19

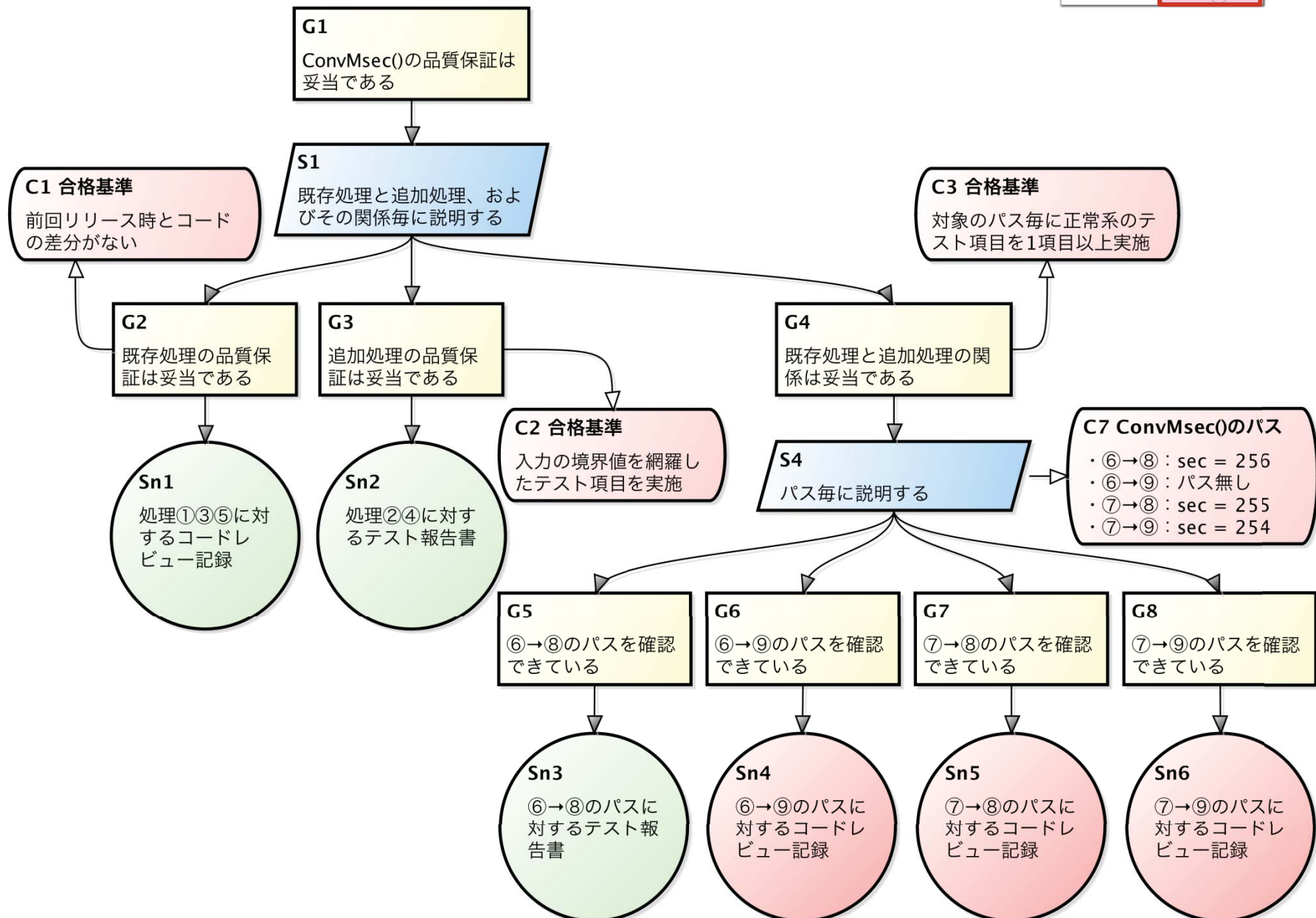
- 上位者の考える合格基準を前提として説明の構造を見える化



手順3: 成果物を証拠に紐付ける

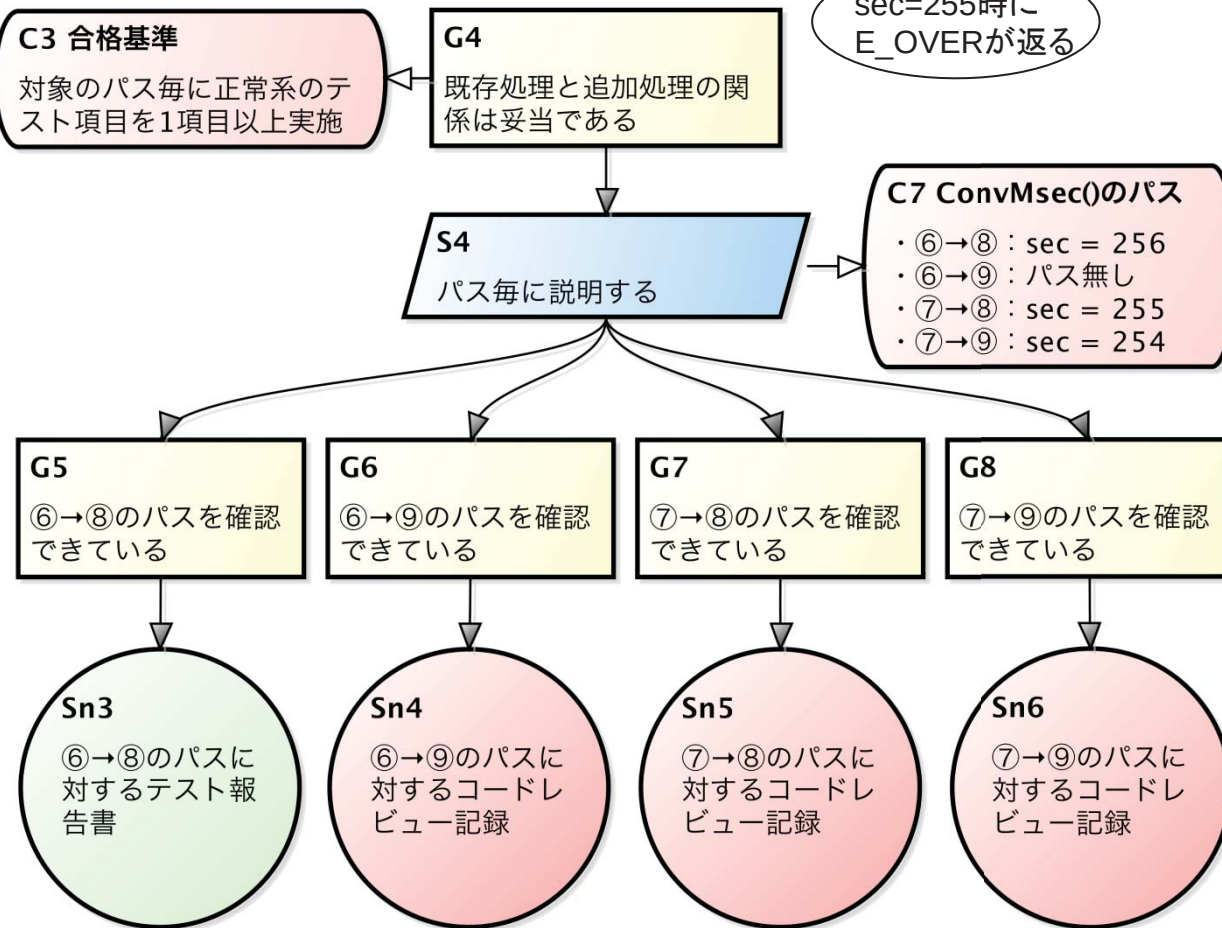


12 / 19

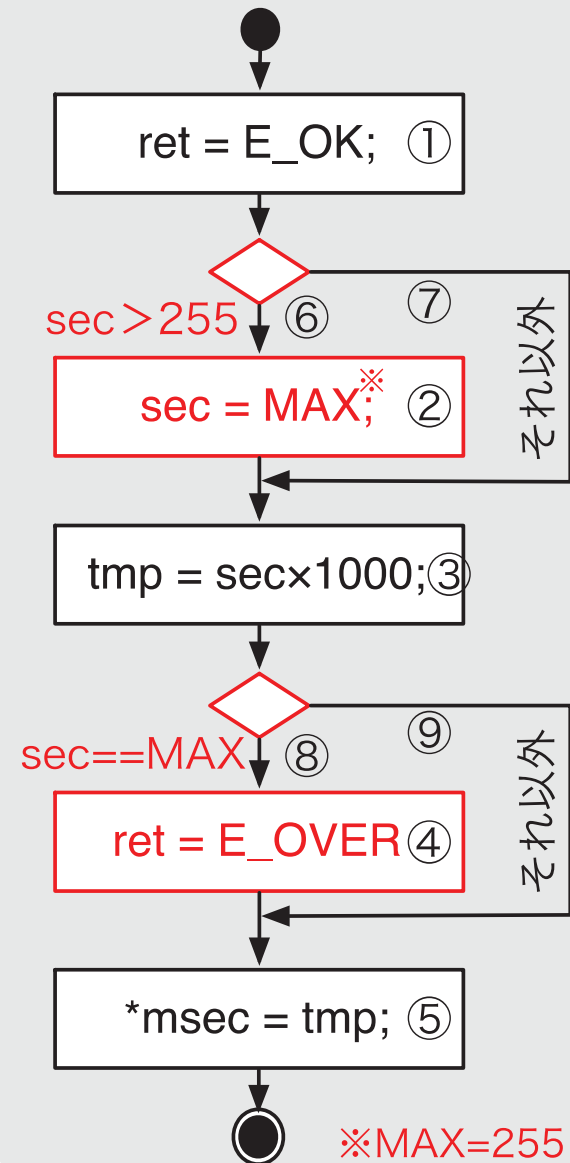


手順4: GSNで説明する

- 既存処理と追加処理の関係についてGSNで確認
- 承認者の合格基準(C3)未達の証拠(Sn4, 5, 6)を検出
⇒ Sn5の追加テスト時に不具合発見!

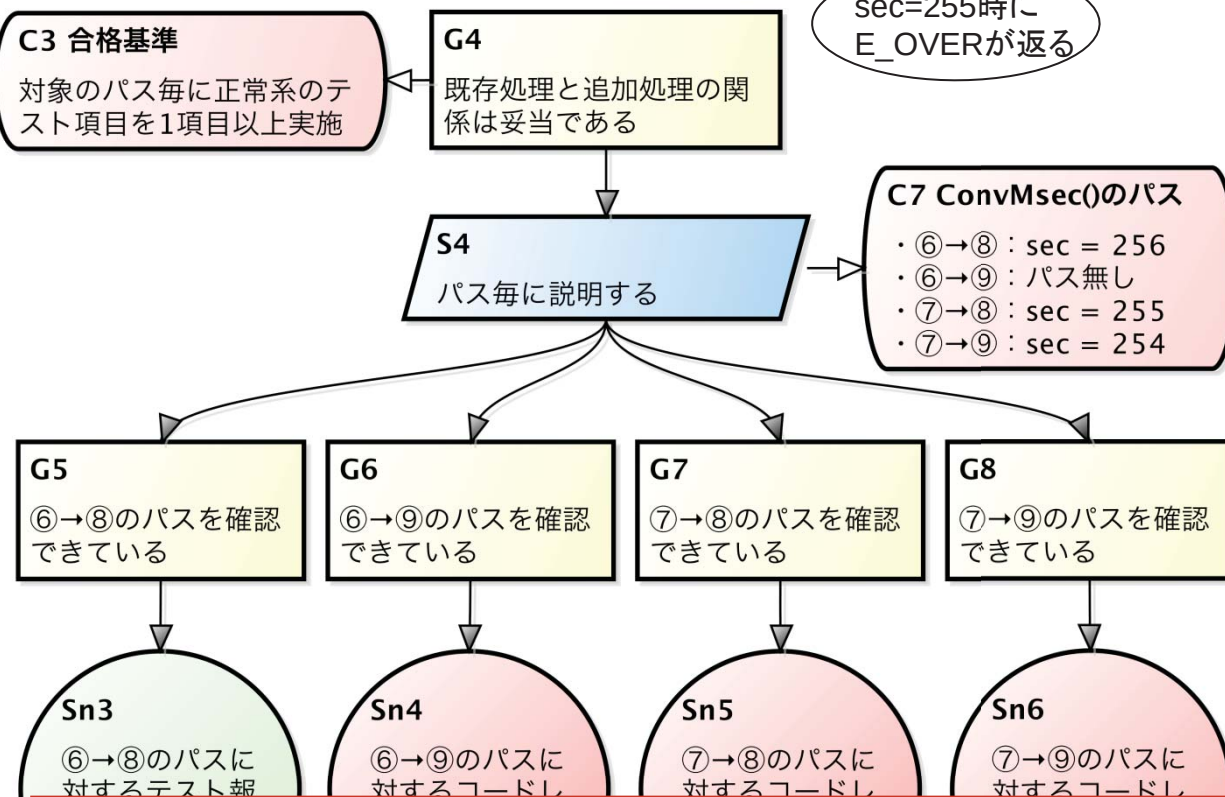


<ConvMsec実装>

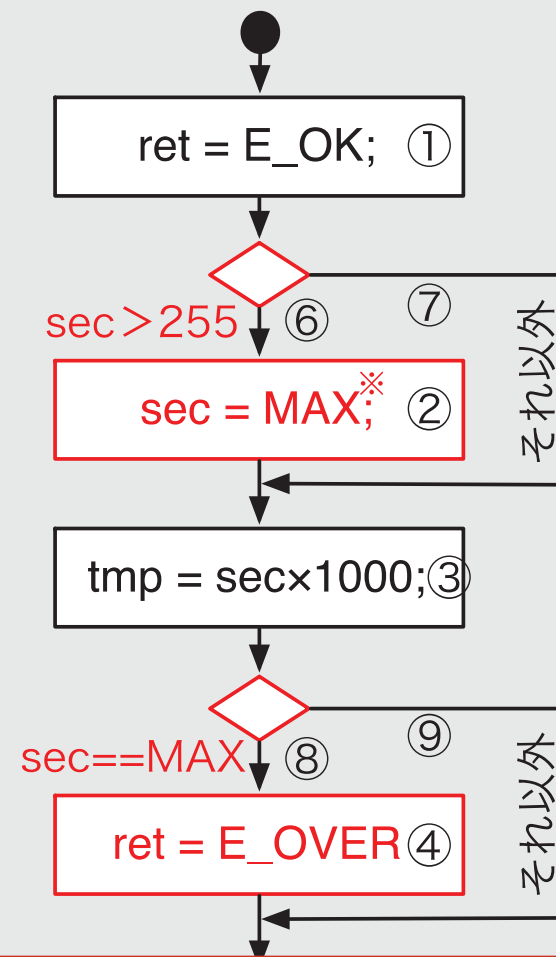


手順4: GSNで説明する

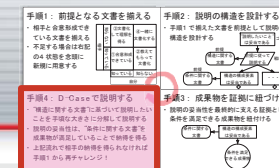
- 既存処理と追加処理の関係についてGSNで確認
- 承認者の合格基準(C3)未達の証拠(Sn4, 5, 6)を検出
⇒ Sn5の追加テスト時に不具合発見!



<ConvMsec実装>



前提ノードと証拠ノードの関係を評価することで
ソフトウェアの品質を見える化できた



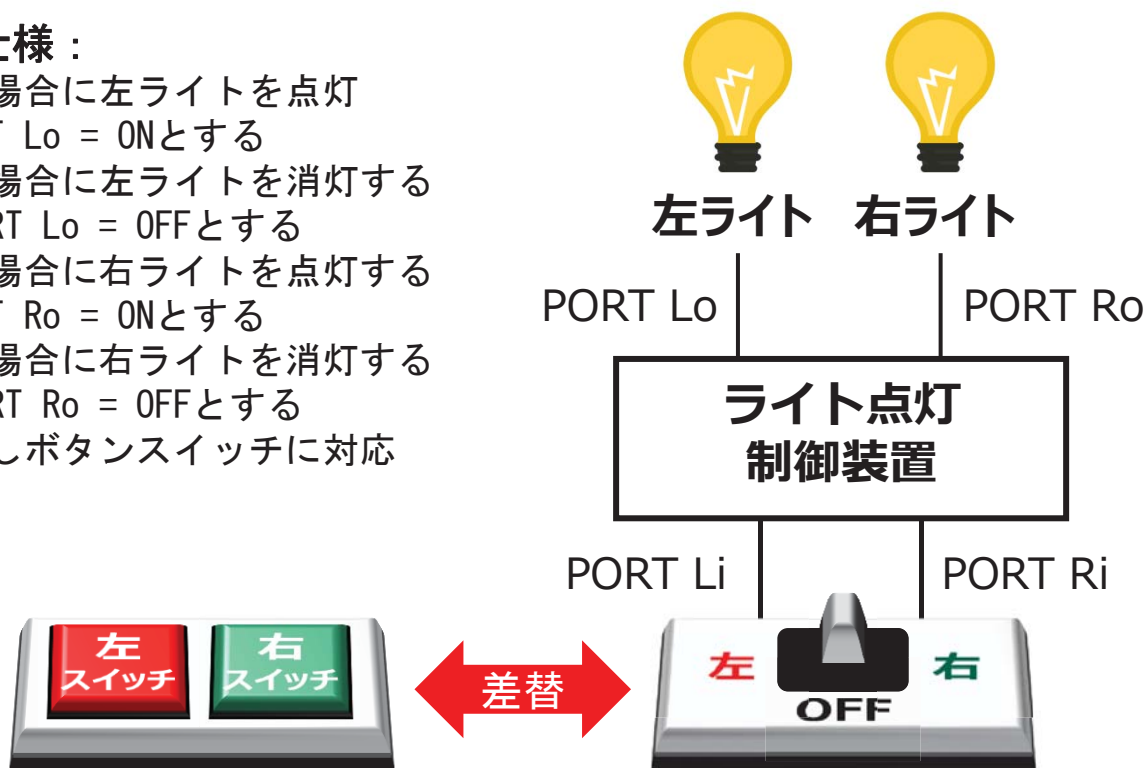
演習：部下からのプログラム修正報告を確認してみましょう

15 / 19

- ライト点灯制御装置のプログラム修正の妥当性を後述する部下からの報告内容だけで説明できているかGSNで確認してみましょう
 - トップゴールは「修正後のライト点灯制御装置プログラムの品質は妥当である」として下さい
 - GSN作成時に部下からの報告内容以外の証拠が必要となった場合、適切な名称を付けて自由に追加してもらって構いません(考慮不足として部下に指示する内容に相当します)

ライト点灯制御装置プログラム仕様：

- ID1: 左スイッチが押下状態である場合に左ライトを点灯
⇒ PORT Li = ONである場合にPORT Lo = ONとする
- ID2: 左スイッチが押下状態にない場合に左ライトを消灯する
⇒ PORT Li = OFFである場合にPORT Lo = OFFとする
- ID3: 右スイッチが押下状態である場合に右ライトを点灯する
⇒ PORT Ri = ONである場合にPORT Ro = ONとする
- ID4: 右スイッチが押下状態にない場合に右ライトを消灯する
⇒ PORT Ri = OFFである場合にPORT Ro = OFFとする
- ID5: スイッチは3点スイッチと押しボタンスイッチに対応

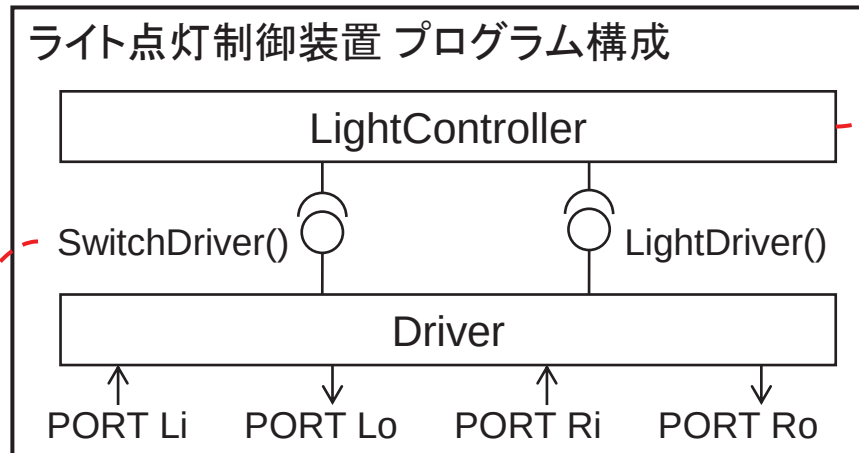


左右スイッチ同時押下時のライト未点灯問題の修正(1/2)

16 / 19

(問題) 押しボタンスイッチを接続したところ、左右スイッチの同時押下時に右ライトが点灯しない

(修正方法) 左右スイッチの同時押下時に左右両方のライトを点灯する処理を追加



```
unsigned char SwitchDriver(void) {
    unsigned char status = 0x00;
    if (PORT_Li == ON) {
        status = 0x01; // LEFT ON
    }
    // else if (PORT_Ri == ON) {
    //     status = 0x02; // RIGHT ON
    // }
    return status;
}
```

変更

```
// Change for ver.1.1:start
if (PORT_Ri == ON) {
    status |= 0x02; // RIGHT ON
}
// Change for ver.1.1:end
```

```
void LightController(void) {
    unsigned char ret;
    ret = SwitchDriver();
    switch (ret) {
        case 0x01: // LEFT ON
            LightDriver(PORT_Lo, ON);
            LightDriver(PORT_Ro, OFF);
            break;
        case 0x02: // RIGHT ON
            LightDriver(PORT_Lo, OFF);
            LightDriver(PORT_Ro, ON);
            break;
        // Add for ver.1.1:start
        case 0x03: // BOTH ON
            LightDriver(PORT_Lo, ON);
            LightDriver(PORT_Ro, ON);
            break;
        // Add for ver.1.1:end
        default:
            LightDriver(PORT_Lo, OFF);
            LightDriver(PORT_Ro, OFF);
            break;
    }
    return;
}
```

- SwitchDriver 単体テスト報告書

ID.	入力条件	期待値	結果
1.	PORT_Li=OFF, PORT_Ri=OFF	戻り値=0x00	○
2.	PORT_Li=ON, PORT_Ri=OFF	戻り値=0x01	○
3.	PORT_Li=OFF, PORT_Ri=ON	戻り値=0x02	○
4.	PORT_Li=ON, PORT_Ri=ON	戻り値=0x03	○

- ライト点灯制御装置プログラム 外部テスト報告書 押しボタンスイッチ編

ID.	入力条件	期待値	結果
1.	PORT_Li=OFF, PORT_Ri=OFF	PORT_Lo=OFF, PORT_Ro=OFF	—
2.	PORT_Li=ON, PORT_Ri=OFF	PORT_Lo=ON, PORT_Ro=OFF	—
3.	PORT_Li=OFF, PORT_Ri=ON	PORT_Lo=OFF, PORT_Ro=ON	—
4.	PORT_Li=ON, PORT_Ri=ON	PORT_Lo=ON, PORT_Ro=ON	○

凡例)

- ・○:合格、×:不合格、—:対象外
- ・赤字項目:今回追加した項目

- 弊社における導入の進め方

- ① GSNの基本的な知識の教育(記法や注意点等)
- ② 事例ベースで実際にGSNを用いて演習
- ③ 使い勝手の良いツールの導入(astah GSN)
- ④ 活用できる場の提供(設計成果のレビュー)
- ⑤ 期待するGSNの構造の共有(レビュー時に指導)

- スムーズな導入のためのポイント

- GSNの良し悪しを判断できる人が“一人”居ると良いです。
⇒ 何をどう描いたら役に立つか自信が持てなくなるので...
- はじめの“一人”の育成は、DEOS協会、D-Case部会に協力を仰ぐと良いかと思います。

- D-Case推進団体
 - DEOS協会（ディペンダビリティ技術推進協会）
 - <http://deos.or.jp/index-j.html>
 - D-Case研究会
 - <http://www.dcase.jp>
- D-Caseに関するツール
 - astah GSN
 - <http://astah.change-vision.com/ja/product/astah-gsn.html>
 - D-Case Editor
 - <http://www.dcase.jp/p/jeditor.html>
- D-Case関連の公開記事
 - 折り紙かぶとに関する記事
 - <http://qiita.com/kenjihiranabe/items/b2349449102b70f37bf5>
 - <http://qiita.com/nobuhide/items/94b65dafa15799d0507f>
 - <http://qiita.com/nobuhide/items/2acea0dad2699256b4b8>
 - Youtube: モデリングしてますか? - GSN/D-Case/安全コンセプト
 - https://www.youtube.com/playlist?list=PLcb1q4H_P-HTyrGX_y47XIQzXORGD3D2g



お問い合わせ先:
・株式会社デンソークリエイト 宇都宮 浩之
・E-mail: hiroyuki@dcinc.co.jp