一般社団法人ディペンダビリティ技術推進協会
第6回 DEOS協会　オープン シンポジウム

IEC 62853の現場適用
～規格の効率的な理解と活用～

2019年6月11日

一般社団法人ディペンダビリティ技術推進協会　理事
技術活用部会　主査
山浦一郎
（富士ゼロックス株式会社）

1. IEC 62853の超高速理解!

2. どの辺りが難しいか？

3. 効率的な理解に向けて

1. IEC 62853の超高速理解!

2. どの辺りが難しいか？

3. 効率的な理解に向けて

IEC 62853には
何が書かれているか？

IEC 62853には

・オープンシステム　を
・ディペンダブルにするために
・実施する項目

が書かれている

IEC 62853のもくじの一部

合意形成 プロセスビュー

説明責任プロセスビュー

障害対応プロセスビュー

変化対応プロセスビュー

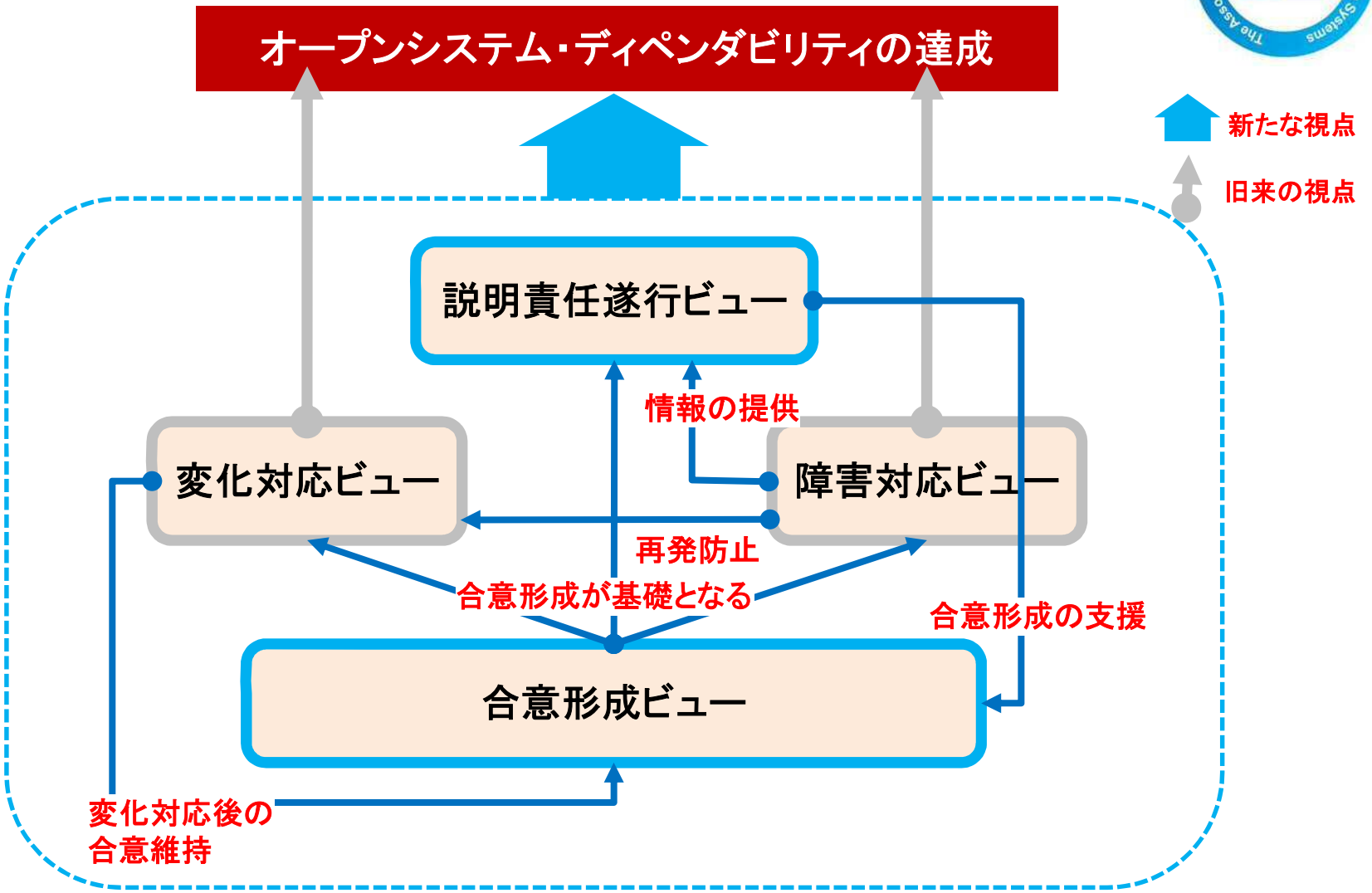
IEC 62853の肝です！ (p.15～p.48 全148ページ中)

1. IEC 62853の超高速理解!

2. どの辺りが難しいか？

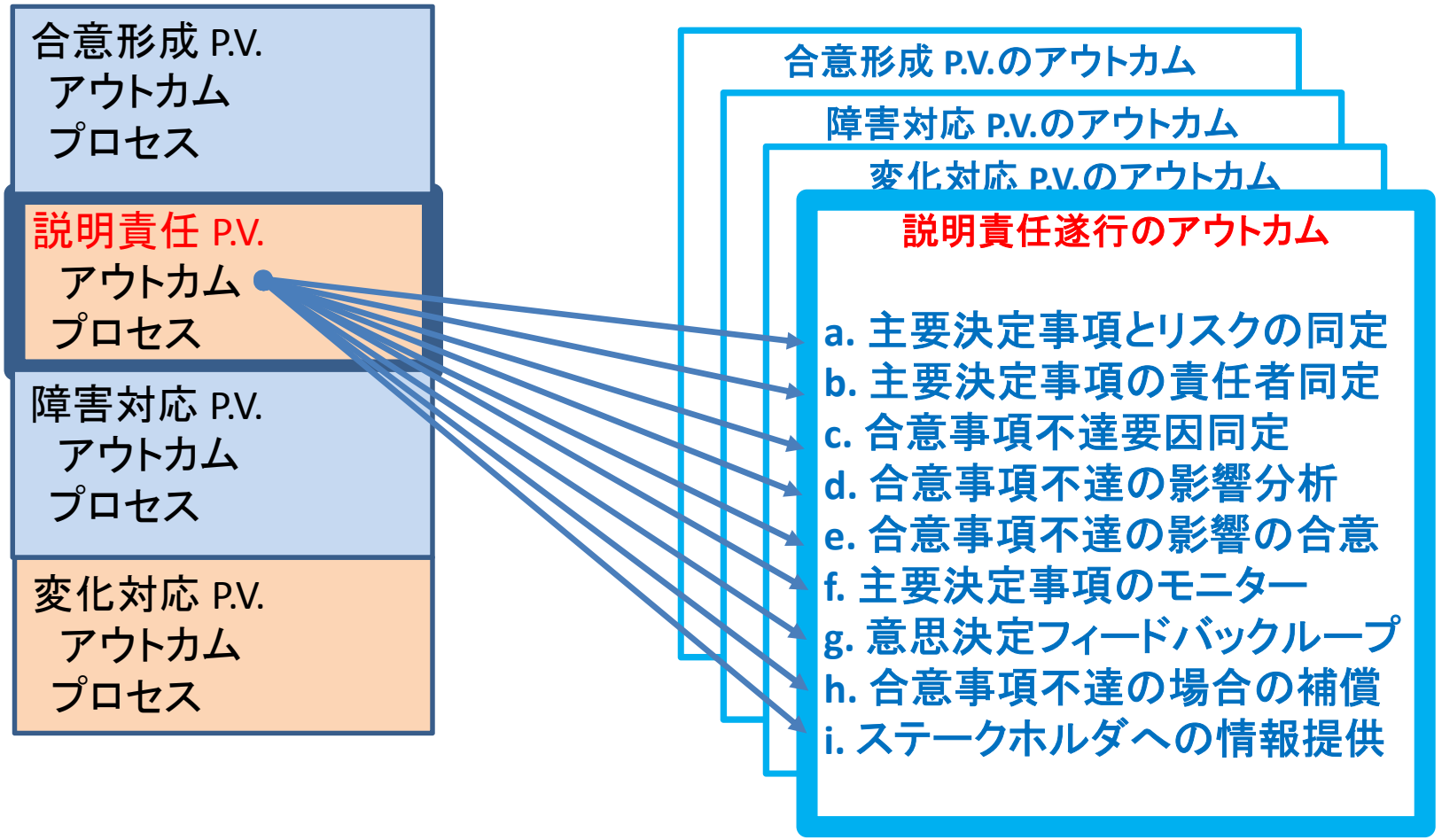
3. 効率的な理解に向けて

4つのプロセスビュー間の関係



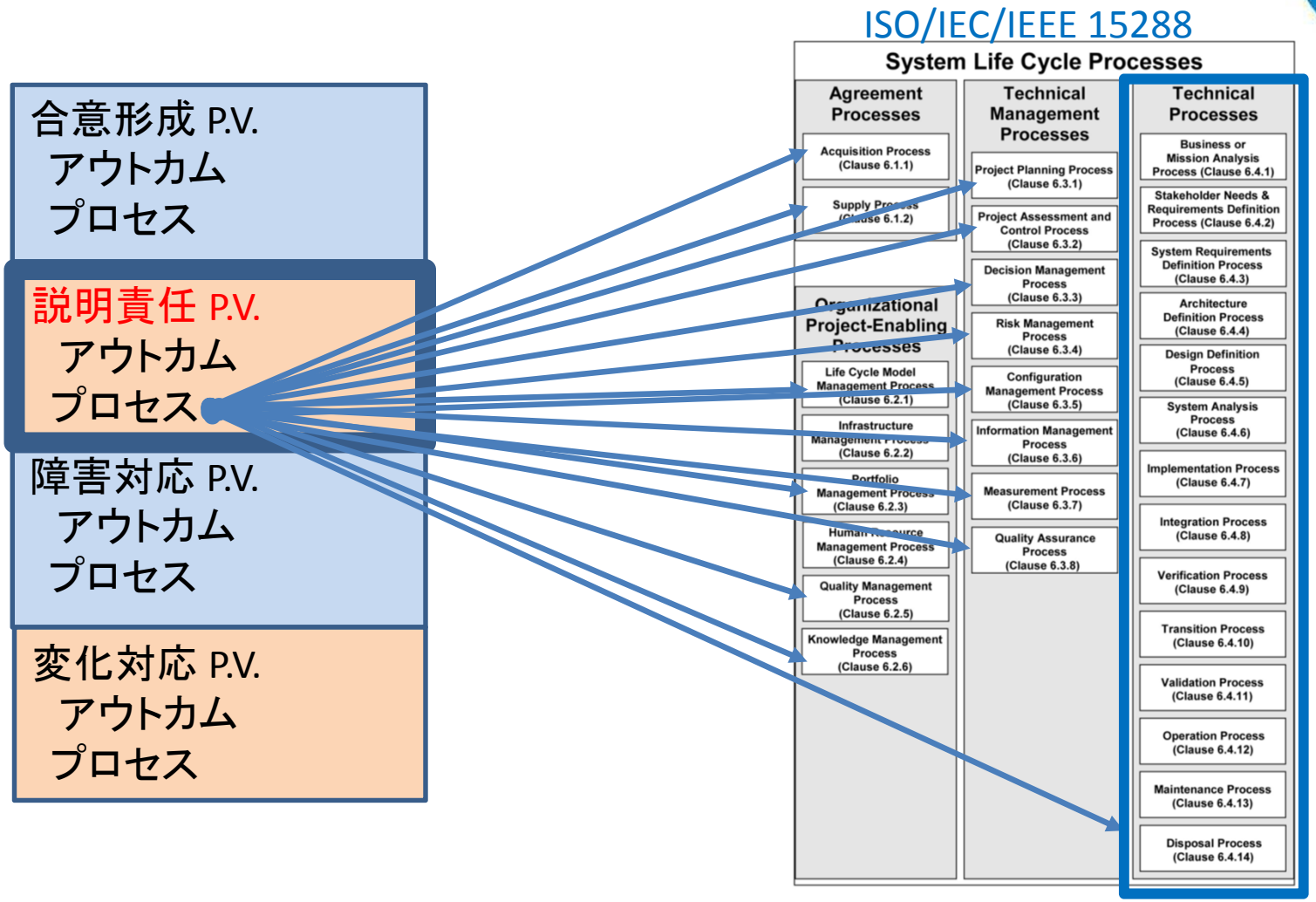
1つの項目がライフサイクルのあちこちのプロセスと関連する

各プロセスビューのアウトカム



これを読んだだけで、何をどうすればいいかわかるか？

各プロセスビューのプロセス



プロセスはベースとなる他の標準(15288)を参照している

ISO/IEC/IEEE 15288(system life cycle processes)と ISO/IEC/IEEE 15289(information items)との関係

入力情報(15289) ➡ 処理(15288) ➡ 出力情報(15289)

Typical Input information items	ISO/IEC/IEEE 15288:2015 reference	Output information item
PORTFOLIO MANAGEMENT		
Organizational procedure, project plan, business action plan	6.2.3.3.a)8	Project management plan
Agreement, project life-cycle policies and procedures	6.2.3.3.a)7). B.1	Progress report (Progress Initiation Report, Project Closure Report)
Agreement, Business strategy, risk management plan	6.2.3.3.a)7), B.1	Evaluation report (Portfolio analysis report)
HUMAN RESOURCE MANAGEMENT		
Employee Skill record, project management plan	6.2.4.3.b)	Training plan
Knowledge management policy, training plan, user documentation, validation procedure	6.2.4.3.b)	Training documentation
Project management plan, staffing plan, training plan	6.2.4.3.a)1), B.1	Evaluation report (required skills)
QUALITY MANAGEMENT		
Project management plan	6.2.5.3.a), 6.2.5.3.c)	Quality management plan
Organizational procedure, quality management plan, customer satisfaction report, problem report	6.2.5.2.a), 6.2.5.3.a), B.1	Quality management policy and procedure
Survey, interview, requirements specification, quality assurance evaluation results, customer satisfaction assessment results	6.2.5.3.c.3),, B.1	Monitoring and control report (Corrective and preventive action report)
KNOWLEDGE MANAGEMENT		
Project management plan, configuration management plan,	6.2.6.3.a)	Information management plan (Knowledge management plan)
Knowledge assets, reference architectures, process		

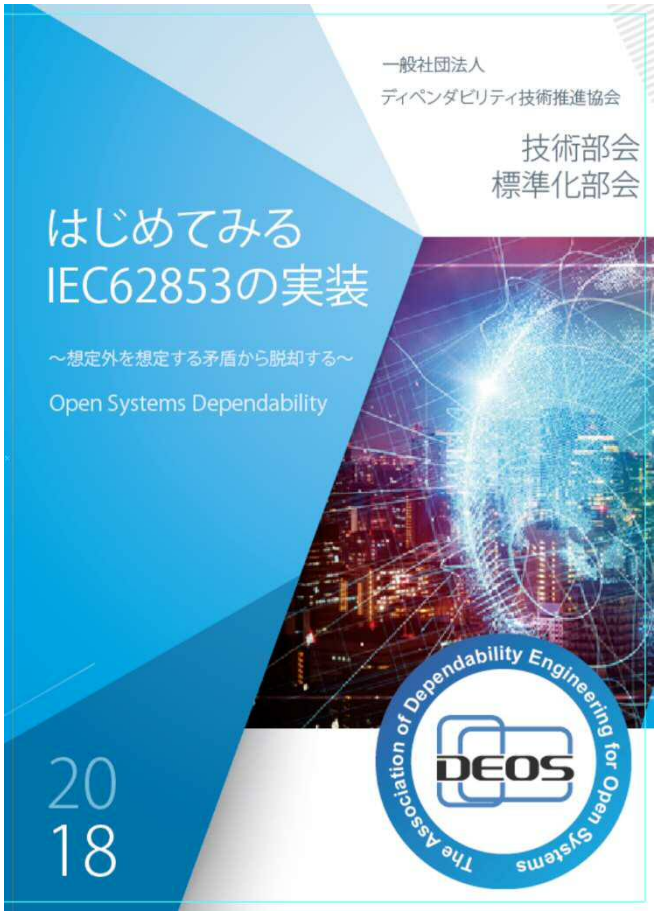
各プロセスに関係する情報項目も他の標準(15289)をベースに

1. IEC 62853の超高速理解!

2. どの辺りが難しいか？

3. 効率的な理解に向けて

実施例-1



はじめてみる IEC62853 の実装

DEOS 協会　技術部会・標準化部会　はじめてみる IEC62853 の実装

広く含めた範囲でステークホルダを捉えている

- ディペンダビリティケース
  - 総合信頼性(Dependability*1)要求を実現していることの根拠となる論理的整合性のある説明構造とその証拠とがリンクされた論証書類
- プロセスビュー
  - ディペンデビリティケースに基づいて夫々のステークホルダが関係する、システムに対する機能限界、性能限界、責任分界の提示に必要な要件の集合
- アウトカム
  - 各プロセスビューが要求する活動内容の結果

4. IEC62853 の 4 つのプロセスビュー

IEC 62853 は OSD を達成するために、四つのプロセスビューを規定しています。各プロセスビューの目的と、実施に成功した場合に期待されるアウトカムに関する規定の抄訳を以下に示します。

4.1. 合意形成

目的　合意形成プロセスビューの目的は、システム、システムの目的、目標、環境、性能、ライフサイクル、及びこれらの変化に関する共通理解と明示的合意を確立し、維持することである。

アウトカム

a) システム等に関して、ステークホルダ間で共通の理解と明示的合意が確立されている。

1) 誰がシステムのステークホルダか明確にされている。

2) 記述や判断の枠組として、全てのステークホルダに分かる枠組がひとつ確立されている。枠組には、語彙(用語集)やシステムの環境に関する基本的仮定が含まれる。

3) 枠組みの中で、各ステークホルダはシステムの目的等とそれらの変化について

13

教科書を作成。

→　教科書を読む人より、作成者のほうが理解が進んでしまった

実施例-2

つながる世界のリスク

1.2 つながる世界のリスク

1.2.1 つながる世界のリスクの特徴

つながる世界には、従来の情報システムや重要インフラと異なり、以下のようなリスク要因がある。

(1) 想定しないつながりが発生する

近年の機器やシステムには汎用 OS や標準規格の通信インタフェース
ており、メーカ以外の事業者でも容易に IoT サービスを構築できる上、
が興味本位でつなげてしまうケースもある。このため、想定しないつ
発生し、外部から攻撃を受けたり、情報が漏えいすることも懸念され

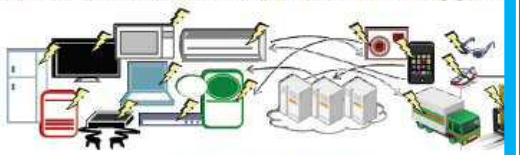


図 1-6 想定しないつながりが発生

(2) 管理されていないモノもつながる

企業の情報システムと異なり、IoT にはウェアラブル機器、駐車場の
車、家庭の住宅設備や家電、廃棄される機器など、管理担当者がいな
つながる。このため、悪意がある者が直接、機器やシステムに不正な
ェアを埋め込んだり、廃棄された機器からデータやソフトウェアを読
とも比較的容易である。また、10 年以上経過し、適切に保守されてい
も混在することで、全体としての安全安心が低下する可能性もある。

図 1-7 メーカにより物理的に管理されない家庭や公共空間の機器やシ

17の開発指針

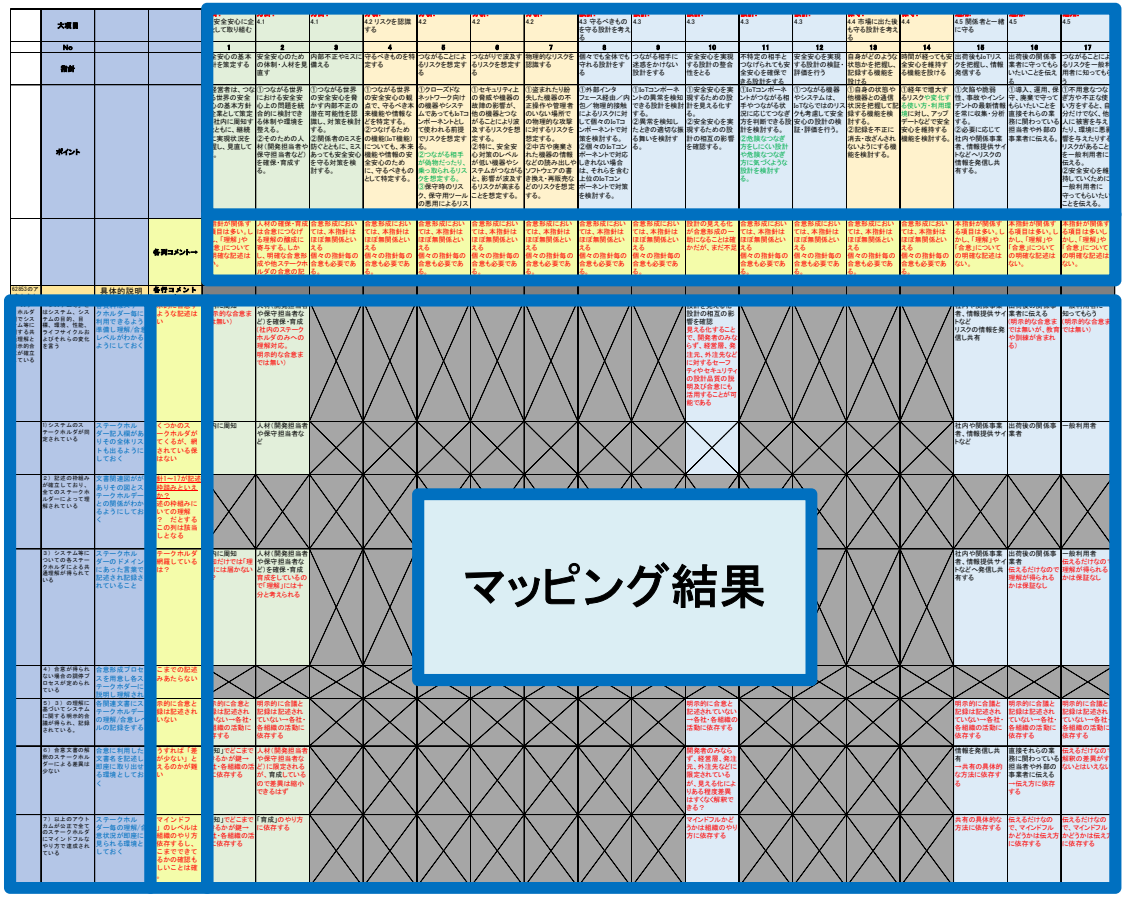
表 4-1 検討して欲しい開発指針一覧

大項目		指針
方針	4.1 つながる世界の安全安心に企業として取り組む	指針 1 安全安心の基本方針を策定する
		指針 2 安全安心のための体制・人材を見直す
		指針 3 内部不正やミスに備える
分析	4.2 つながる世界のリスクを認識する	指針 4 守るべきものを特定する
		指針 5 つながることによるリスクを想定する
		指針 6 つながりで波及するリスクを想定する
		指針 7 物理的なリスクを認識する
設計	4.3 守るべきものを守る設計を考える	指針 8 個々でも全体でも守れる設計をする
		指針 9 つながる相手に迷惑をかけない設計をする
		指針 10 安全安心を実現する設計の整合性をとる
		指針 11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針 12 安全安心を実現する設計の検証・評価を行う
保守	4.4 市場に出た後も守る設計を考える	指針 13 自身がどのような状態かを把握し、記録する機能を設ける
		指針 14 時間が経っても安全安心を維持する機能を設ける
運用	4.5 関係者と一緒に守る	指針 15 出荷後も IoT リスクを把握し、情報発信する
		指針 16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針 17 つながることによるリスクを一般利用者に知ってもらう

IPA SECの「つながる世界の開発指針」にIEC 62853を適用してみた

実施例-2

つながる世界の17の開発指針

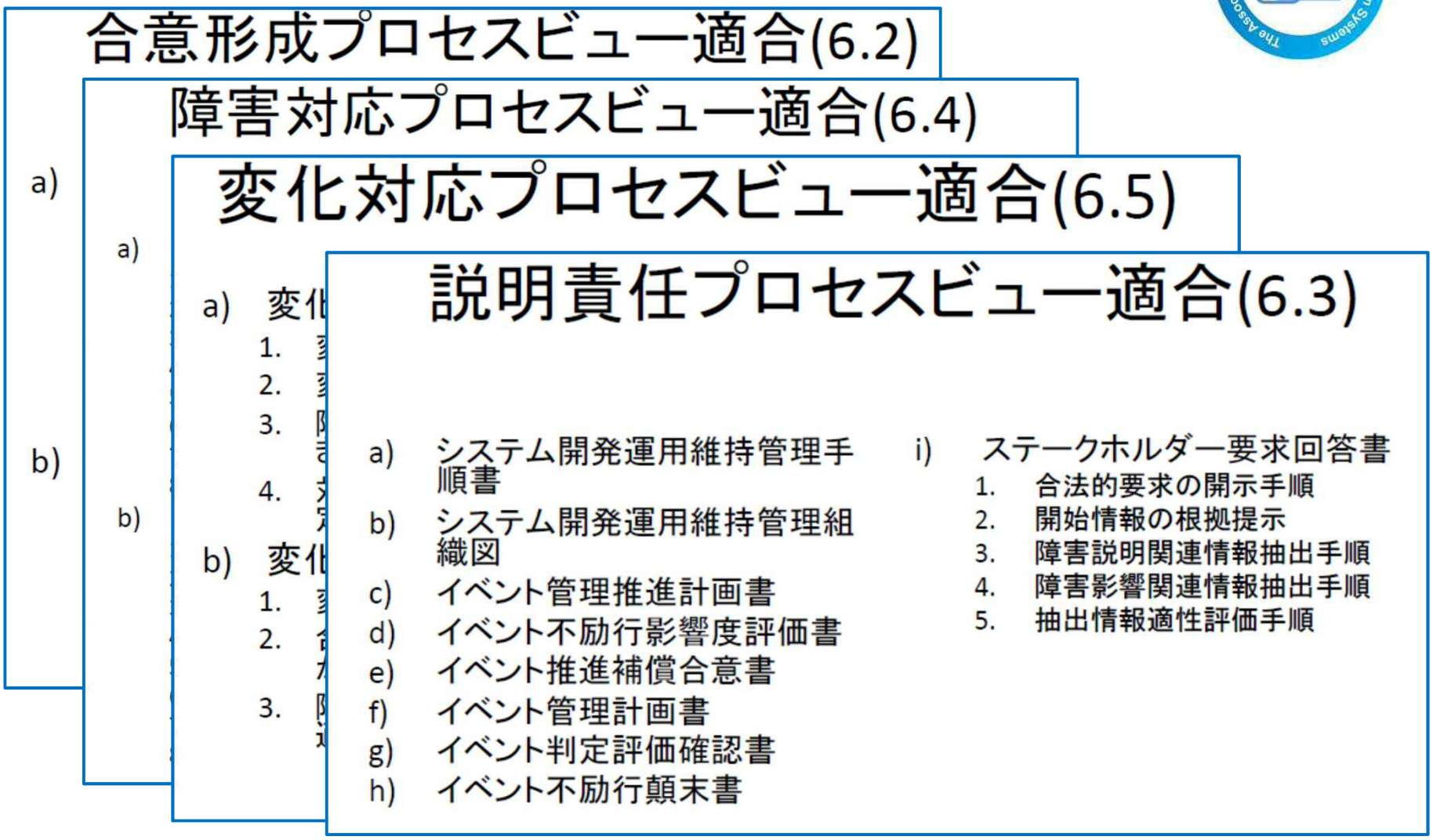


IEC62853で要求されるアウトカム

マッピング結果

この成果をまとめる作業で、IEC62853の理解がさらに進んだ

実施予定



IEC62853のアウトカムと開発文書のマッピングをしたい！

→ 現場の既存の開発文書への適用が容易になる


The Association of Dependability Engineering for Open Systems
DEOS

まとめると...

IEC 62853を理解するために、
参考書などはある。

が、やはり、
手を動かして作業するのが
一番理解が進む！
（IEC 62853を推進した先生と共に）


The Association of Dependability Engineering for Open Systems
DEOS

そこで…

技術活用部会で活動しませんか？

- 定期開催（奇数月の第3月曜日　17:00～）

各会員企業にとってより価値が出るように部会を以下の①の活動を主とする。
①のテーマは完了しだい、次のテーマを検討し選定する。
メンバの要望や参加に応じて、複数Working Group活動も予定する。

– ①IEC62853の開発文書とのマッピングWorkingGroup

参加: 作業する会員メンバ限定
※会員の方で、参加希望の方は随時連絡ください

– ②上記①の活動成果報告（年数回）

目的: 会員へのアウトプットの展開
参加: 会員は誰でも参加可能（今までと同様）

ぜひ一緒に作業して効率的にIEC 62853を体で理解しましょう！