SCDLのセキュリティサブワーキングの取り組みと今後の課題 - ASAM Workshop向け -

名古屋大学 大学院情報学研究科
附属組込みシステム研究センター
倉地　亮

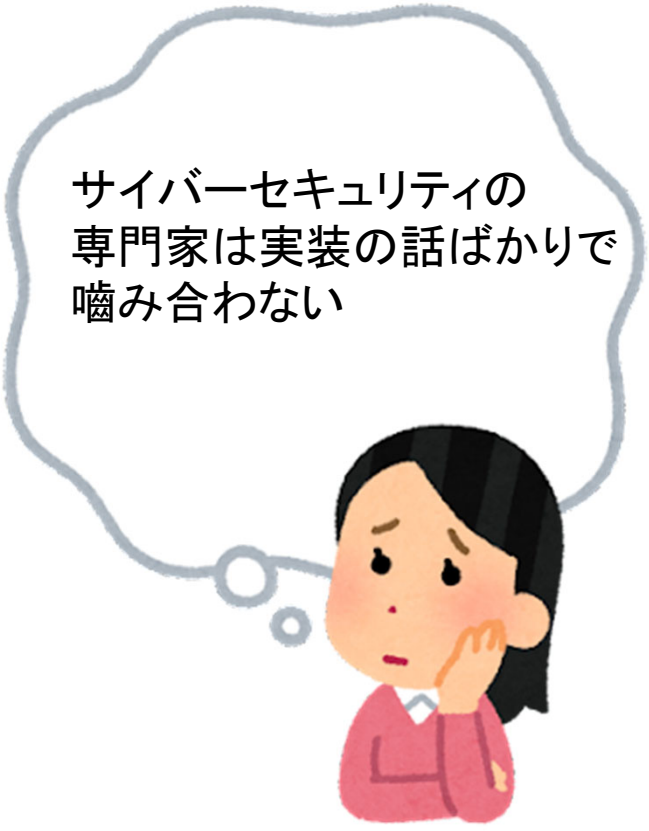
アジェンダ

- 1. セキュリティサブワーキングの活動紹介
  - 研究背景
  - 活動概要
  - 現状の成果物
- 2. セーフティとサイバーセキュリティのエンジニアリングの課題
  - 課題1. 前提となる専門性/知識の違い
  - 課題2. セーフティとセキュリティの開発プロセスの統合/連携
  - 課題3. SCDLを活用するには
- 3. 最後に

1. セキュリティサブワーキングの活動紹介

■ 背景

- 機能安全でのSCDLの活用は進められている
- 一方で,「サイバーセキュリティでSCDLは活用できるか？」という課題が存在



機能安全の専門家

サイバーセキュリティの専門家

うまく連携するにはどうしたら良いか（＝SCDLが役に立たないか）

1. セキュリティサブワーキングの活動紹介

活動目的

- SCDLの成果物をサイバーセキュリティ適用について検討を進めている

活動概要

- 昨年度の成果であるSAFECOMP2020の論文を基に，セキュリティエンジニアリングにおけるSCDLの課題点を洗い出すため，脅威分析を実施中
- 現状でも色々な課題が出てきており，SCDLを活用しセーフティとセキュリティの違いや課題点について整理中

活動体制

- 月1回のWeb会議で実施(次回 12/20(水) 13:00～)

1. セキュリティサブワーキングの活動紹介

■ 参加者(2021年9月10日時点): 38人(昨年，今年度共に増加傾向)

(一財)日本自動車研究所	伊藤　寛
	福田　和良
(株)アトリエ	水口　大知
(株)今仙電機製作所	山内　保尚
DNV GLビジネス・アシュアランス・ジャパン(株)	小澤　弘正
おおた開発効率化プロジェクト	小笠原　豊和
おがたコンサルティング	緒方　健
オムロン(株)	廣部　直樹
ガイオ・テクノロジー(株)	田中　伸明
(株)アドヴィックス	河野　文昭
(株)構造計画研究所	太田　洋二郎
	市村 健太朗
	東道　徹也
(株)三菱総合研究所	石黒　正揮
産業技術総合研究所	三科　雄介
	寶木　和夫
スズキ(株)	村松　稔久
住友電気工業(株)	左近　透
名古屋大学	倉地　亮
日本大学	松野　裕
ベクター・ジャパン(株)	中村　伸彦
マレリ(株)	佐々木　喜好
三菱電機(株)	友永　一生
仙台高等専門学校	岡本　圭史
DNV GLビジネス・アシュアランス・ジャパン(株)	高田　聖
	山下　修平
	平野　薫
	松並　勝
(株)チェンジビジョン	岩永　寿来
ガイオ・テクノロジー(株)	猪狩　秀夫
	岡田 利一
	小野 嘉翔
	三宮　雅人
	肥田野 文之
	大西 建児
	光山　栄太
	荻野(Web担当)
(株)シーエーブイテクノロジーズ	田口　研治

2. セーフティとサイバーセキュリティのエンジニアリングの課題

課題1. 前提となる専門性/知識/アプローチの違い

- 機能安全 ： 安全工学
- サイバーセキュリティ： 情報セキュリティ，暗号数学，暗号実装

➡ **機能安全とサイバーセキュリティの専門家の連携方法が必要**

課題2. セーフティとセキュリティの開発プロセスの統合/連携

- 開発プロセスの連携についても議論が存在
- ただし，従来の議論は理想的な人員や体制，開発期間に応じた理想的なモデル

➡ **現実的なモデルを検討する必要あり**

課題3. SCDLを活用してもらうためには

- 具体的な事例が必要
- SCDLの言語拡張の必要性は？

以降では，上記課題3点についてそれぞれ概説する

2. セーフティとサイバーセキュリティのエンジニアリングの課題

■ 課題1. 前提となる専門性/知識/アプローチの違い

■ 1. 機能安全

- 機能的な工夫（安全を確保する機能）により極力安全を確保
- 信頼性が重視

➡ **安全性を確保するための機能を実装**

■ 2. 情報セキュリティ

- 情報の機密性，完全性および可用性の維持
- さらに真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める
- 機密性(Confidentiality)
  ― アクセスに認可された者だけが情報にアクセスできること
- 完全性(Integrity)
  ― 情報及び処理方法が正確であること及び完全であること
- 可用性(Availability)
  ― 認可された利用者が，必要なときに情報及び関連する資産にアクセスできること

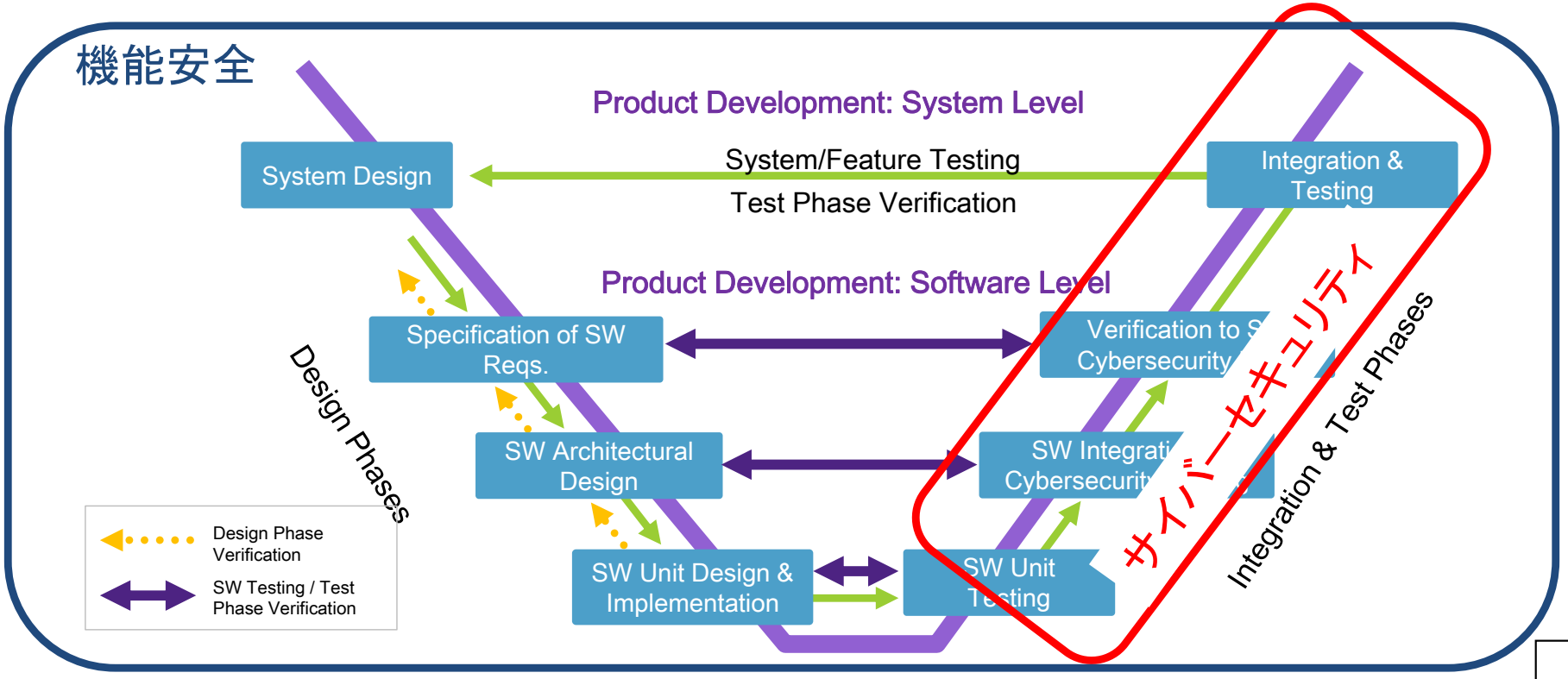
➡ **システムの弱い点(≒脆弱性)を保護する機能を実装**

2つの異なる分野の専門家が開発時にすり合わせる必要性あり

2. セーフティとサイバーセキュリティのエンジニアリングの課題

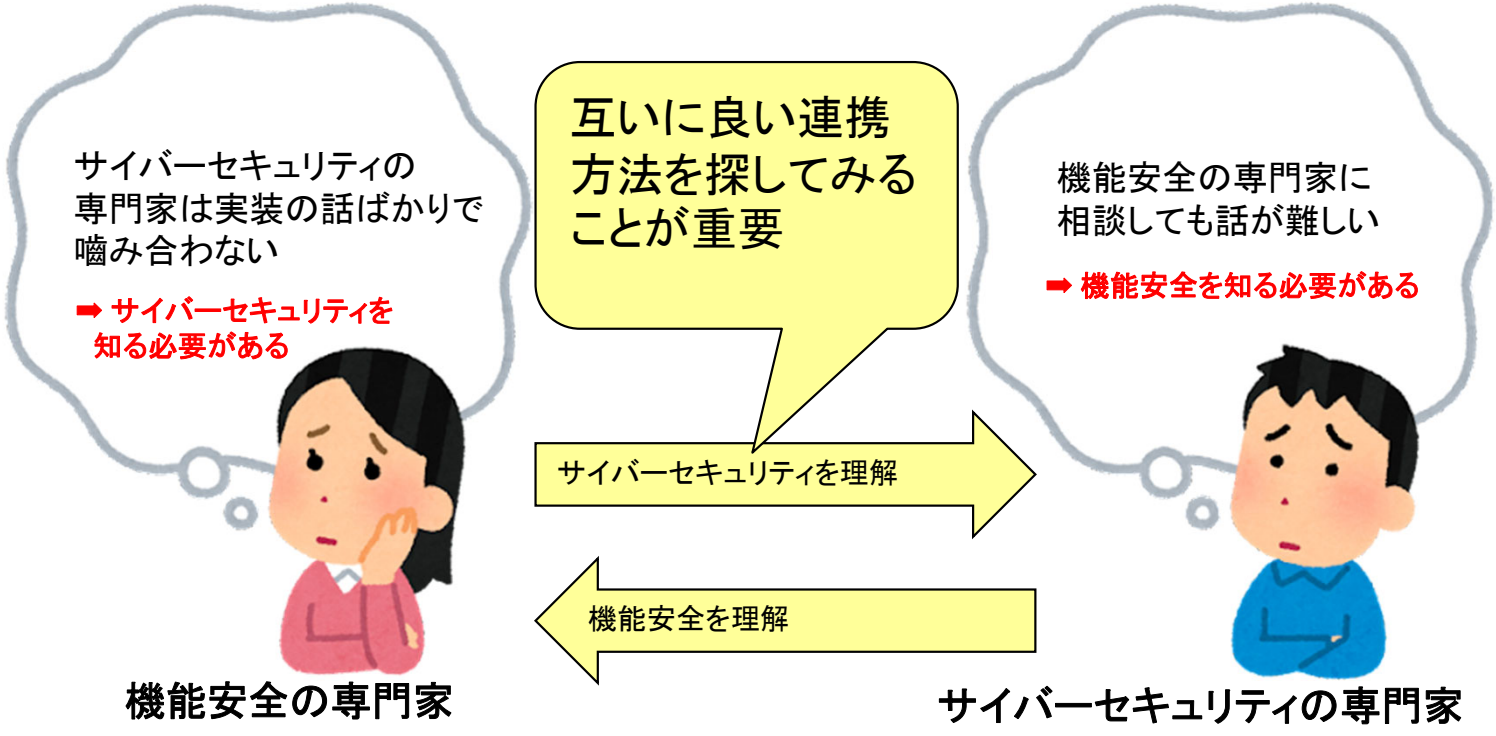
課題1. 前提となる専門性/知識/アプローチの違い

- **機能安全の文化: 保証ケースを重視**
  - ― 上流から保証ケースを決定したい
- **サイバーセキュリティの文化: ベストプラクティスの文化**
  - ― 動作検証/テストにより脆弱性がないことを保証したい
  - ― Security by design(近年，上流設計から考慮することも重要視されている)



2. セーフティとサイバーセキュリティのエンジニアリングの課題

- 専門性の違い/考え方のギャップをどのように埋めるか？
  - ➡ “知識/経験が重要”
  - ➡ お互いを知ることが大切で，その上で擦り合わせる必要がある
- 機能安全とサイバーセキュリティの重要度は対等

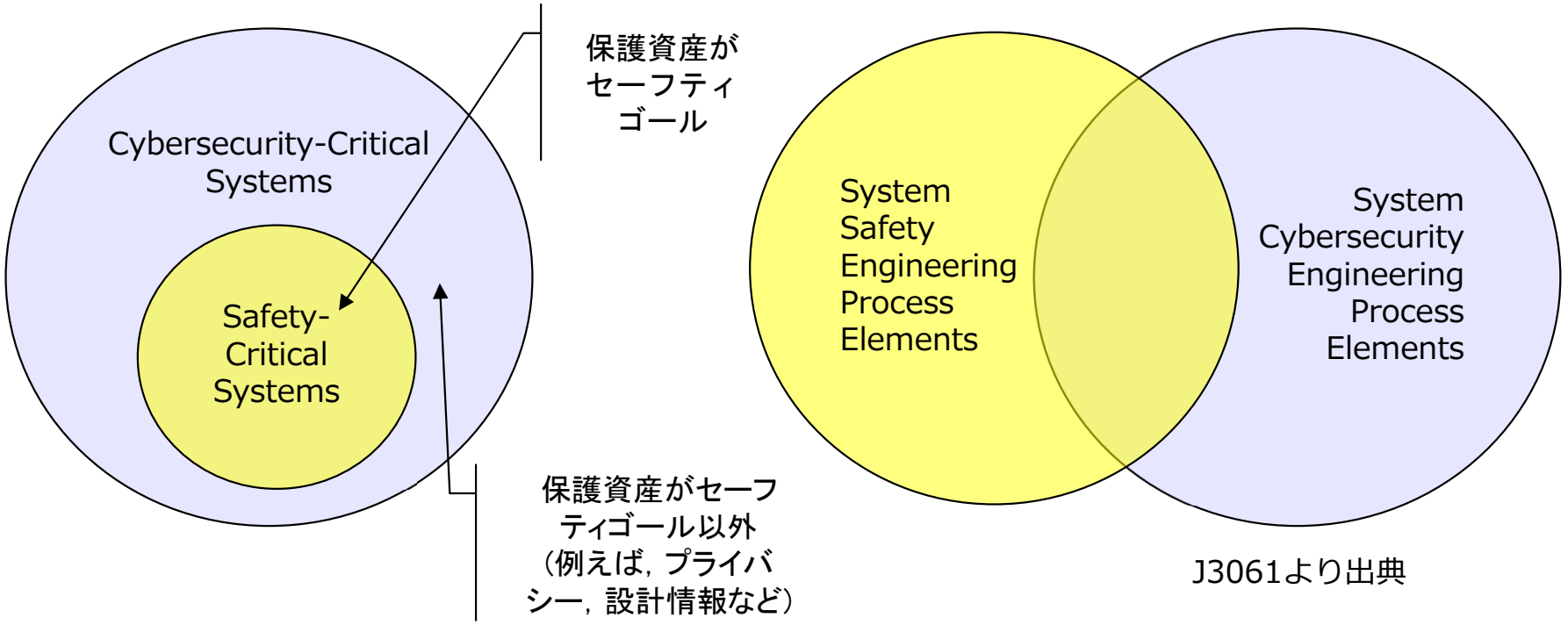


セキュリティSWGでは機能安全の専門家が脅威分析を実施!

2. セーフティとサイバーセキュリティのエンジニアリングの課題

課題2. セーフティとセキュリティの開発プロセスの統合/連携

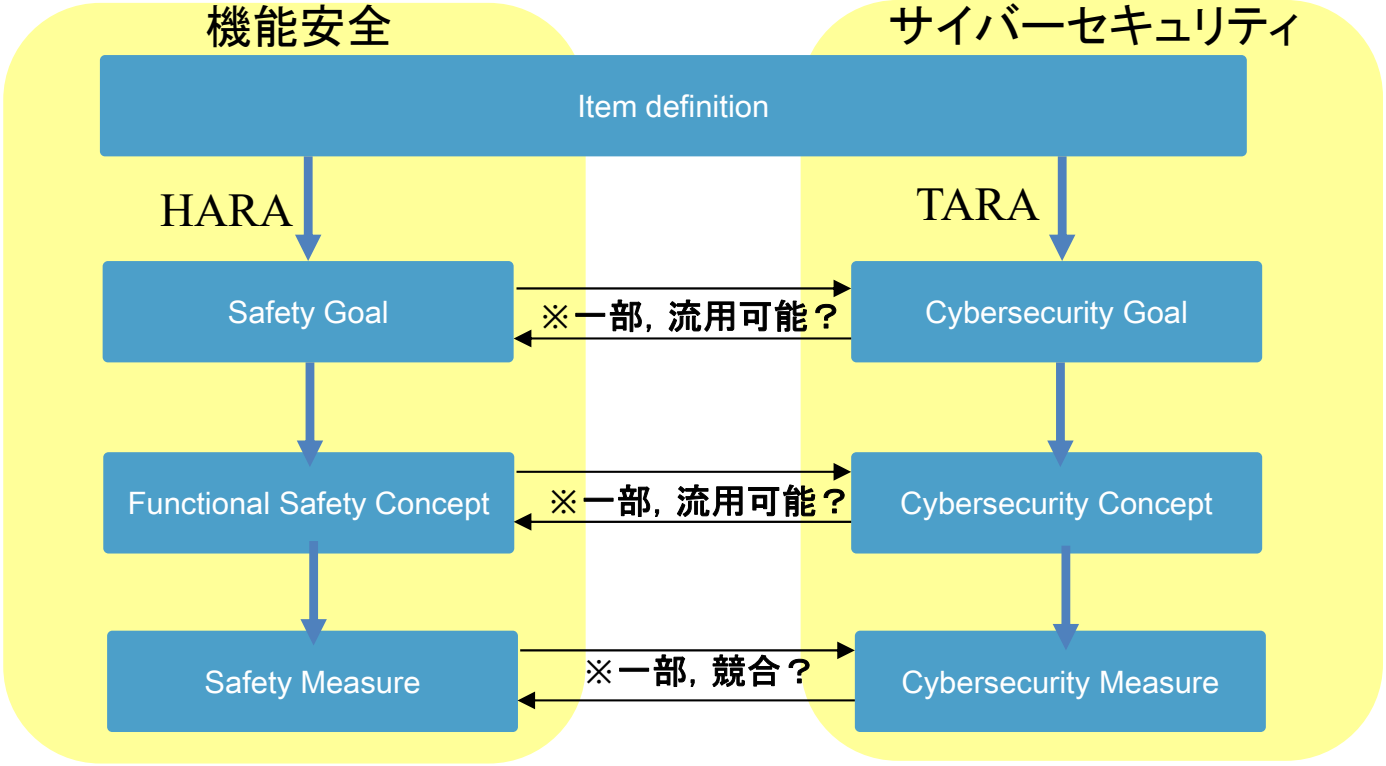
- セーフティクリティカルシステムはサイバーセキュリティクリティカルシステムとして扱われる
- 一方，エンジニアリングプロセスは，両者をうまくテーラリングすることが必要



2つの異なる分野の専門家が開発時にすり合わせる必要性あり

2. セーフティとサイバーセキュリティのエンジニアリングの課題

- 課題2. セーフティとセキュリティの開発プロセスの統合/連携
- 1. 機能安全（ISO26262）
  - Hazard Analysis and Risk Assessment (HARA) を実施
    - ―Safety Goals, Functional Safety Concept が導出
- 2.サイバーセキュリティ(ISO/SAE 21434)
  - Threat Analysis and Risk Assessment (TARA) を実施
    - ―Cybersecurity Goals, Cybersecurity Concept が導出



2. セーフティとサイバーセキュリティのエンジニアリングの課題

■ 開発プロセスの統合/連携をどのように進めるか？

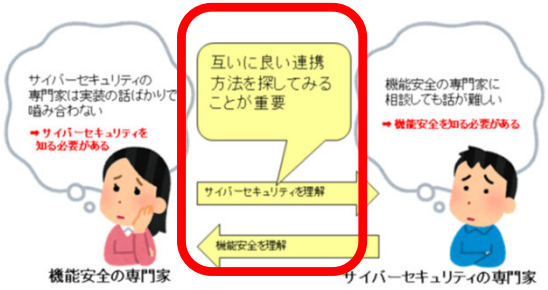
➡ 前提の違いを理解する

	Safety	Financial	Operational	Privacy
機能安全	◎ （詳細化）	△ （範囲外）	△ （範囲外）	× （対象範囲外）
サイバーセキュリティ	△ （詳細化は困難）	○ （対象範囲）	○ （対象範囲）	○ （対象範囲）

➡ 成果物の相互活用が重要

機能安全プロセスの成果物をサイバーセキュリティでも利用してみる

（逆の場合も同様）



SCDLがコミュニケーションツールになるのではないかと仮説

2. セーフティとサイバーセキュリティのエンジニアリングの課題

事例1. SAFECOMP2020でのアプローチ

➡ SCDLで記述された安全コンセプトを用いた脅威分析フレームワークを提案

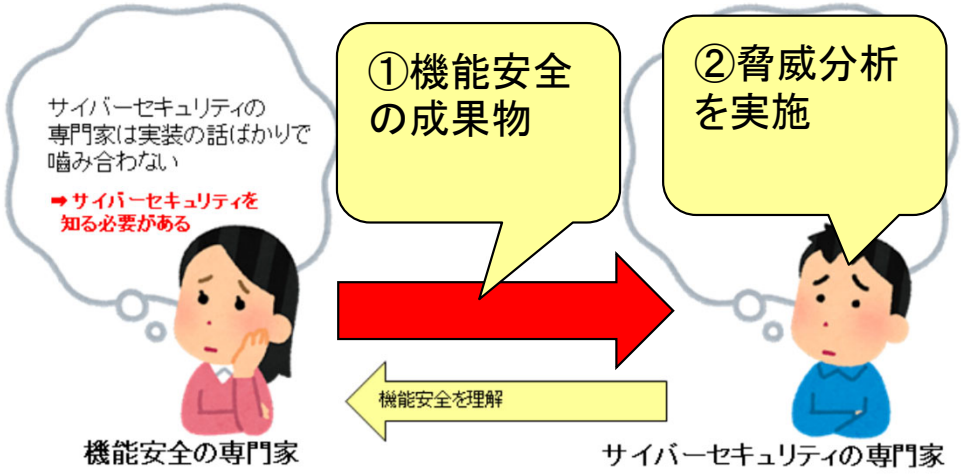
➡ つまり，機能安全の成果物を脅威分析で活用する事例

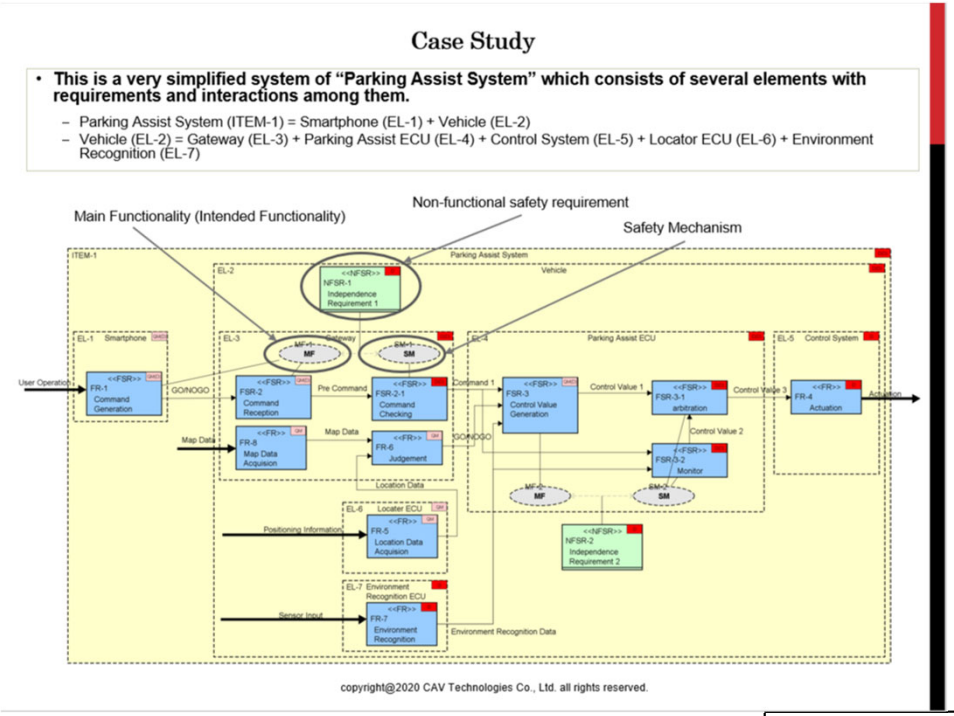
結論

- 攻撃者がなりすまし/多重故障を引き起こし安全ゴールを侵害可能
- 安全機構が役に立つ場合もあるが，セキュリティ強化策がないと不十分

今後の課題

- 安全分析へのフィードバック
- 抽象度の違い





2. セーフティとサイバーセキュリティのエンジニアリングの課題

■ 課題3. SCDLを活用してもらうためには

- SAFECOMP2020の続きとして，セキュリティ強化後の事例を検討中
  - ➡ **“安全分析へのフィードバック“について議論**
  - ➡ 具体例1. 一部の安全機能とセキュリティ機能の順序や関係性の明記が必要

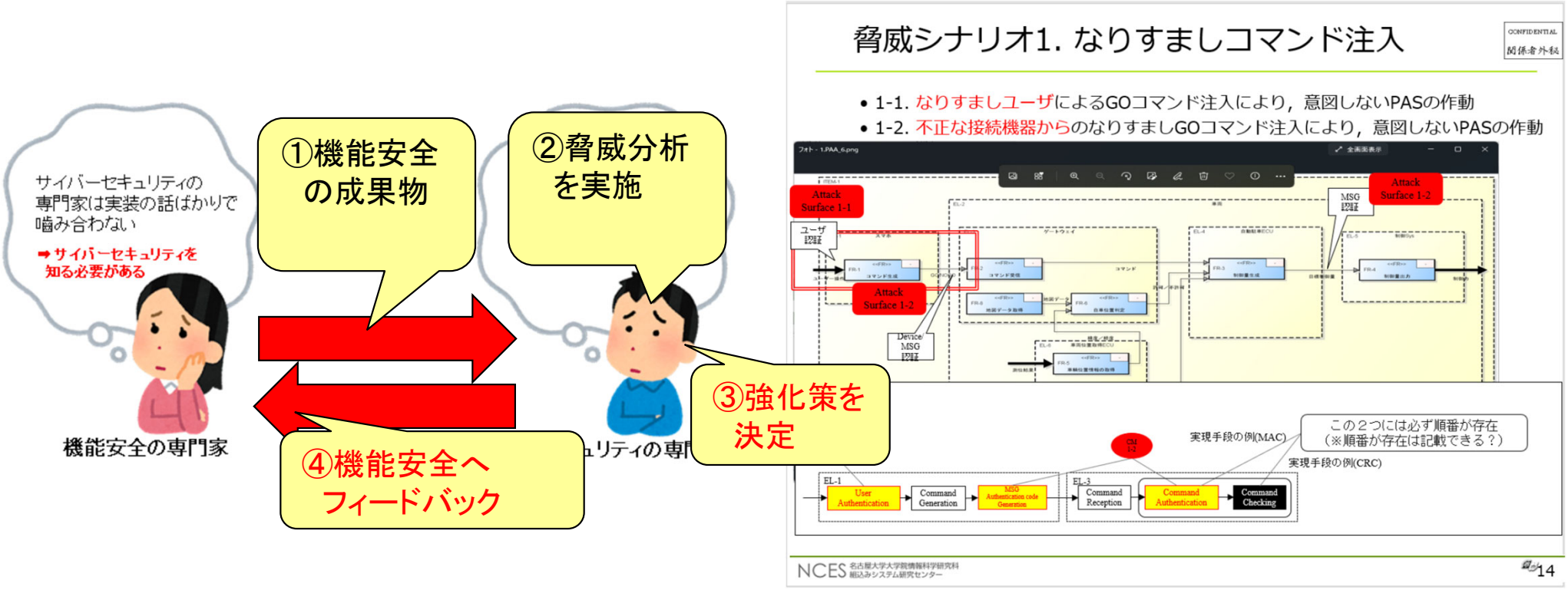


図1. 議論例1: 脅威分析事例

セキュリティ要求が安全要求に与える影響を探索中

2. セーフティとサイバーセキュリティのエンジニアリングの課題

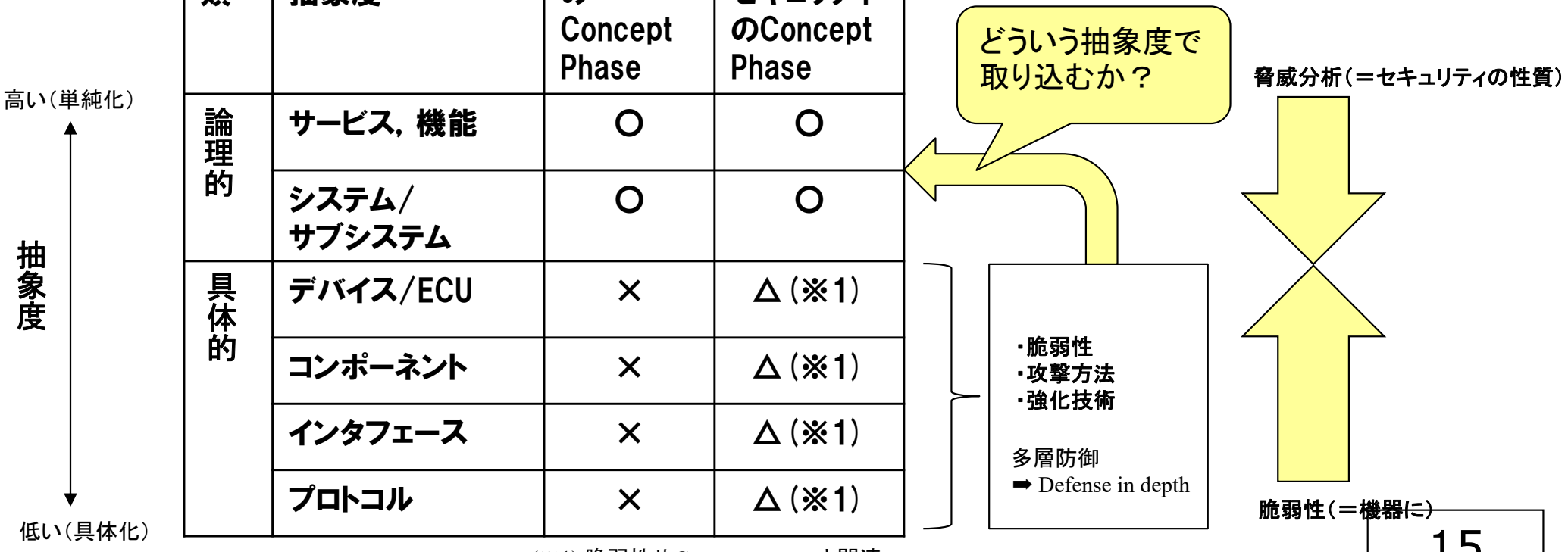
■ 課題3. SCDLを活用してもらうためには

- SAFECOMP2020の続きとして，セキュリティ強化後の事例を検討中
  - ➡ “抽象度の違い“についても議論
  - ➡ 具体例2. Concept Phaseで取り扱うべき抽象度(粒度)

表1. 具体例2: Concept Phaseで取り扱うべき抽象度(粒度)

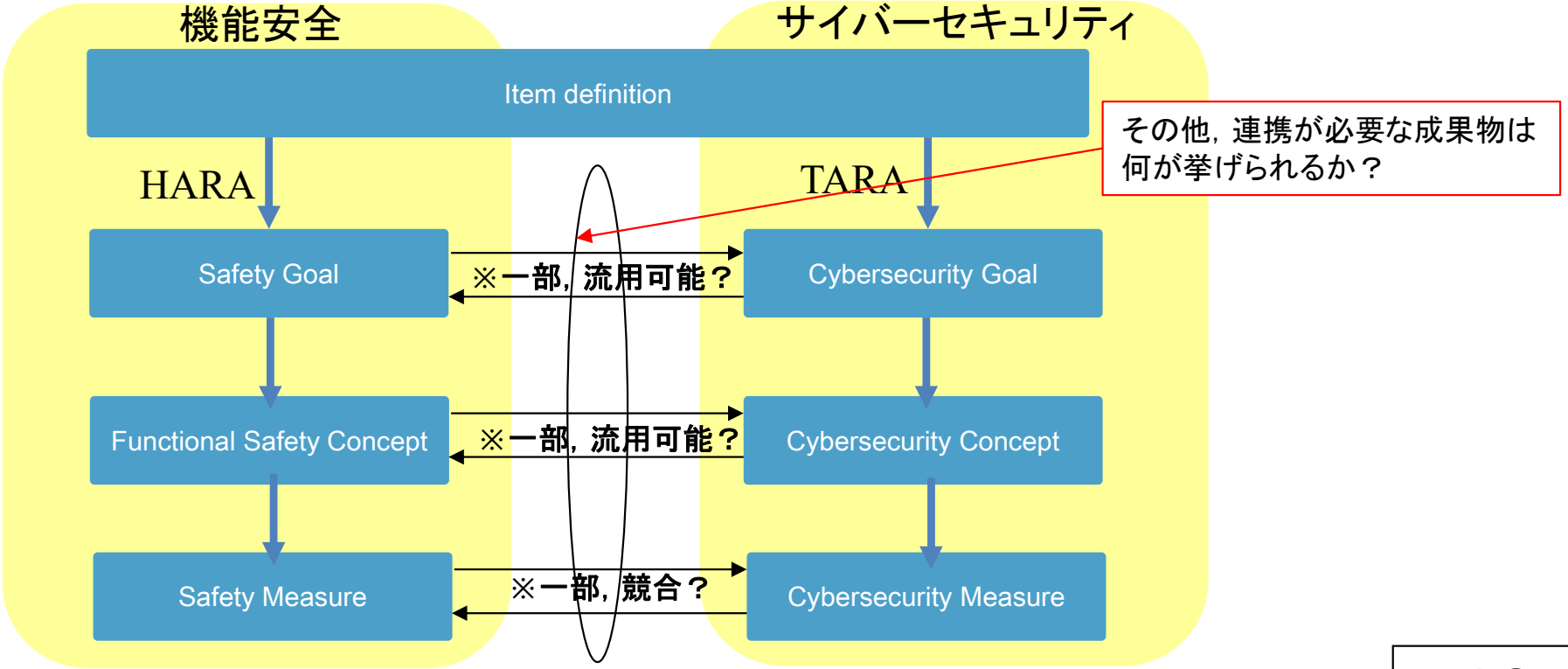
分類	システムの抽象度	機能安全のConcept Phase	サイバーセキュリティのConcept Phase
論理的	サービス，機能	○	○
	システム/サブシステム	○	○
具体的	デバイス/ECU	×	△(※1)
	コンポーネント	×	△(※1)
	インタフェース	×	△(※1)
	プロトコル	×	△(※1)

(※1) 脆弱性やCountermeasureと関連



議論1. セーフティとサイバーセキュリティで連携すべき成果物

- 機能安全（ISO26262）側から提供される成果物
  - セーフティゴール，機能安全コンセプト，セーフティメジャー
- サイバーセキュリティ(ISO/SAE 21434）側から提供される成果物
  - サイバーセキュリティゴール，サイバーセキュリティコンセプト，サイバーセキュリティメジャ



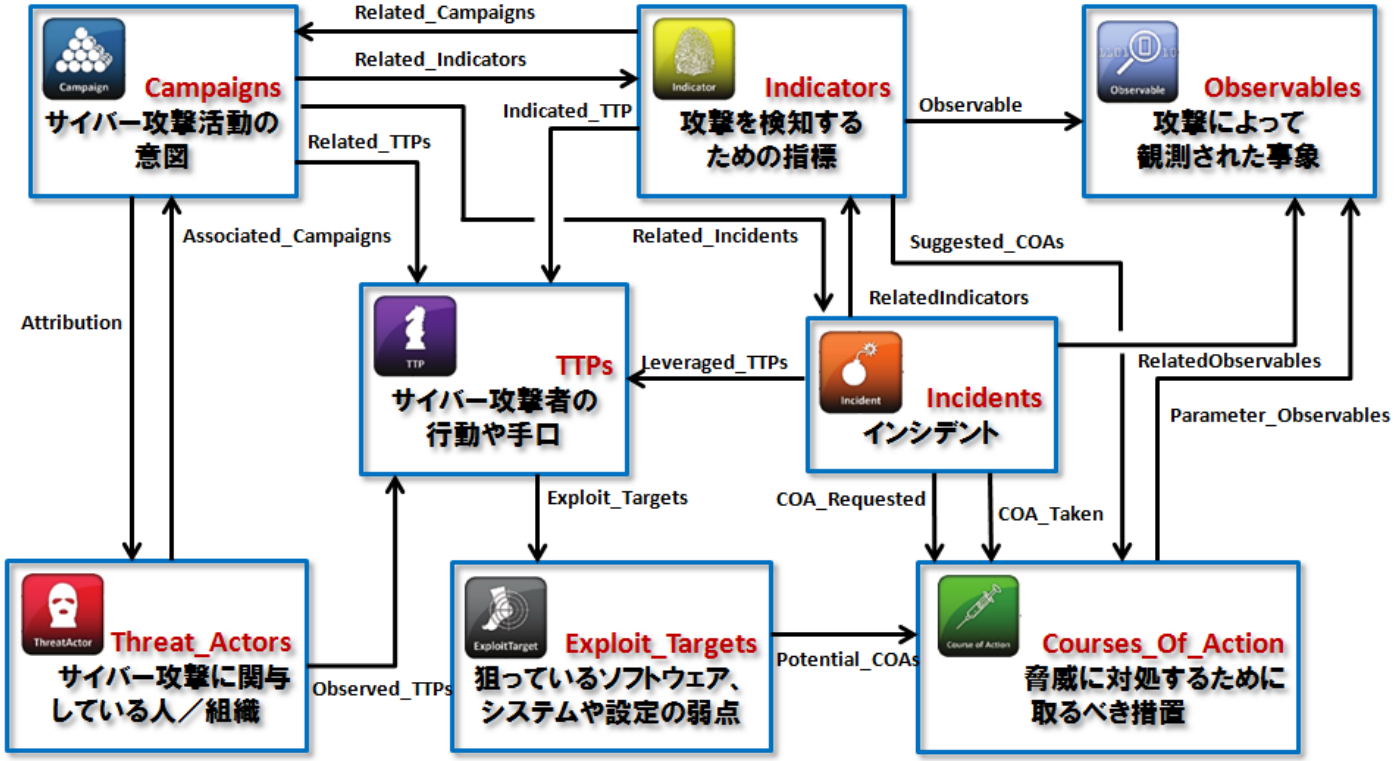
議論1. セーフティとサイバーセキュリティで連携すべき成果物

- ISO/SAE 21434観点では，以下の情報も必要か
  - Damage scenarios, assets
- Concept Phaseでの成果物は互いに確認する必要があるか
  - 例えば，Cybersecurityの下記成果物の内，機能安全で必要な項目は何か？

Activities		Work Products
Risk Assessment	8.3 Asset Identification	[WP-08-01] Damage scenarios [WP-08-02] Identified assets and cybersecurity properties
	8.4 Threat Scenario Identification	[WP-08-03] Threat scenarios
	8.5 Impact Rating	[WP-08-04] Impact rating, including the associated impact categories of the damage scenarios
	8.6 Attack Path Analysis	[WP-08-05] Identified attack paths
	8.7 Attack Feasibility Rating	[WP-08-06] Attack feasibility rating
	8.8 Risk Determination	[WP-08-07] Risk value
	8.9 Risk Treatment Decision	[WP-08-08] Risk treatment decision per threat scenario
Concept Phase	9.3 Item Definition	[WP-09-01] Item definition
	9.4 Cybersecurity Goals	[WP-09-02] Threat analysis and risk assessment [WP-09-03] Risk treatment decisions [WP-09-04] Cybersecurity goals [WP-09-05] Cybersecurity claims [WP-09-06] Verification report
	9.5 Cybersecurity Concept	[WP-09-07] Cybersecurity concept [WP-09-08] Verification report of cybersecurity concept

議論2. どういう形式で連携すべきか？

- データ形式として，XMLのタグ(メタデータ)を定義すべきか？
  それとも自然言語のドキュメントがあれば十分か？
  - 例えば，Cybersecurityでは脅威情報構造化記述形式(STIX)のような形式が存在
  - これらを機能安全側でも把握することができるか？



https://www.ipa.go.jp/security/vuln/STIX.html

3. 最後に

- セキュリティSWGでは，SCDLのサイバーセキュリティでの活用法を検討
- 脅威分析事例を通じて，安全分析と比較し違いの明確化を議論中

➡ <u>自動車のサイバーセキュリティにおけるベストプラクティスを目指す</u>

- 皆様へのお願い事項
  - 是非，セキュリティに興味がある方はセキュリティSWGにもご参加下さい．
  - たまに顔を出す程度のオブザーバ参加も歓迎いたします

本内容に関するお問い合わせはどうぞお気軽に．

scdlsec@scn-sg.com