

# サイバセセキュリティと脅威モデリング技術

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

# 自己紹介

## ■ 倉地 亮 (くらち りょう)

- 博士(情報科学)
- 所属: 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 特任准教授



## ■ 現所属にて何をしているのか？

- リアルタイムネットワークのスケジューリング解析手法
- 車載制御システムの設計技術
- // のセキュリティ強化技術

## ■ 学外での活動

- 自動車技術会 サイバーセキュリティ講座委員会 委員長
- 自動車技術会 教育会議 委員
- J-Auto-ISAC 学会会員
- 電子情報通信学会 情報セキュリティ研究会(ISEC) 専門委員
- SIP 自動走行システムの社会的影響に関する検討委員会 委員
- Trusted Computing Group (TCG) Invited Expert
- AUTOSAR WP-SEC, FT-ST member など

# アジェンダ

---

- 1. サイバーセキュリティモデリングの動向
  - 研究背景
  - 脅威モデリング
  
- 2. セキュリティサブワーキングの活動紹介
  - 活動概要
  - 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
  - 現在の議論
    - － 議論1. 機能安全とサイバーセキュリティの連携プロセス
    - － 議論2. Concept Phaseで取り扱うべき抽象度(粒度)

# 背景. 自動車のサイバーセキュリティ強化が要求

- 研究者らにより自動車のセキュリティ上の脅威が指摘
- 実際に販売される車両にもセキュリティ強化技術が適用されつつある
- 現在では一部車両の型式認証にサイバーセキュリティ強化が必須



<https://spectrum.ieee.org/jeep-hacking-101>

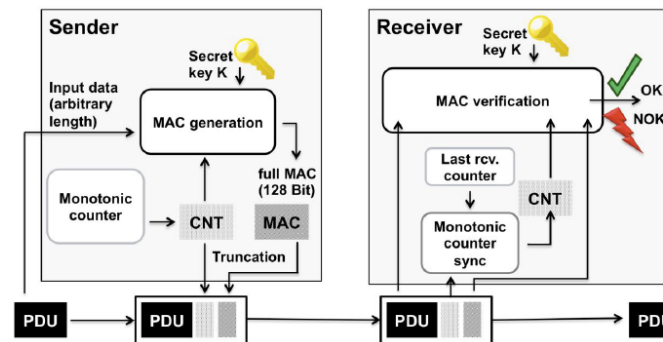
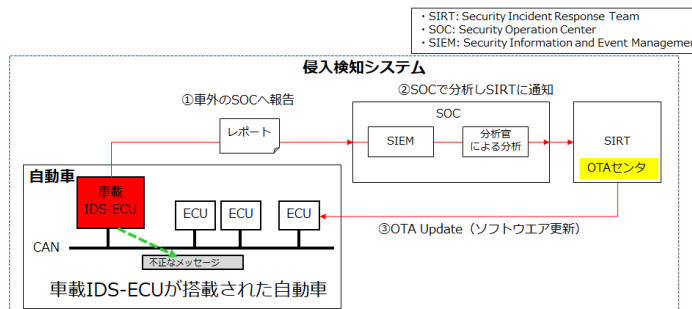
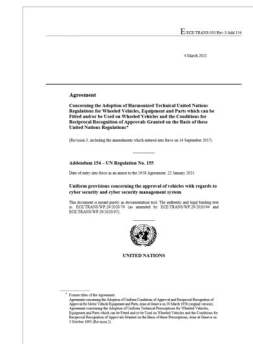


Figure 1: Message Authentication and Freshness Verification

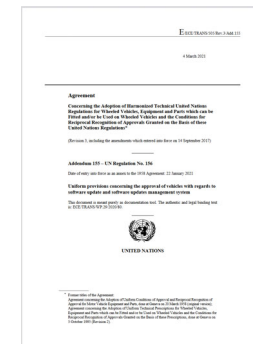
適用されつつある技術の例1. メッセージ認証  
AUTOSAR version R21-11 Requirements on  
Module Secure Onboard Communication



適用されつつある技術の例2. 侵入検知システム



国際基準 UN-R155  
(サイバーセキュリティ)



国際基準 UN-R156  
(ソフトウェアアップデート)

脅威事例  
(2010~)

セキュリティ強化  
(2019~)

国際基準と法制度化  
(2022~)

# 背景. 自動車のサイバーセキュリティ強化が要求

- 2016年1月にSAEからCybersecurity Guidebook for Cyber-Physical vehicle Systems (J3061)が発行
- 2021年8月にISO/SAE 21434正式発行
- 2021年7月 Automotive SPICE for Cybersecurityが発行

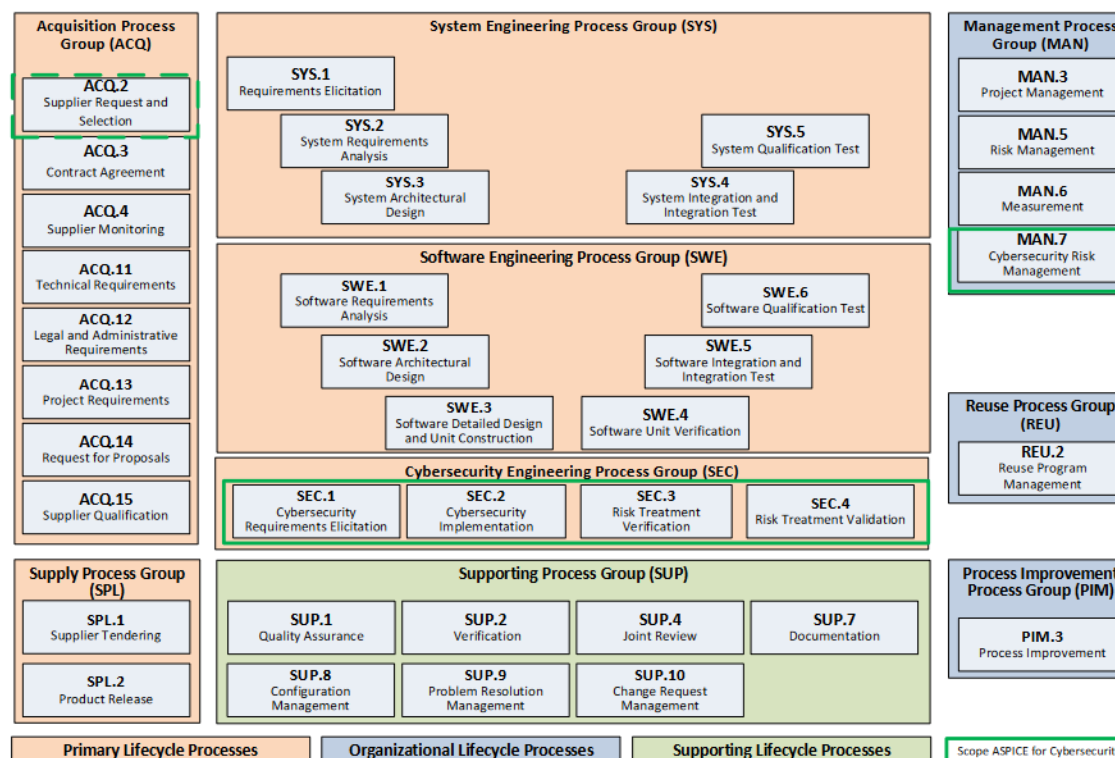
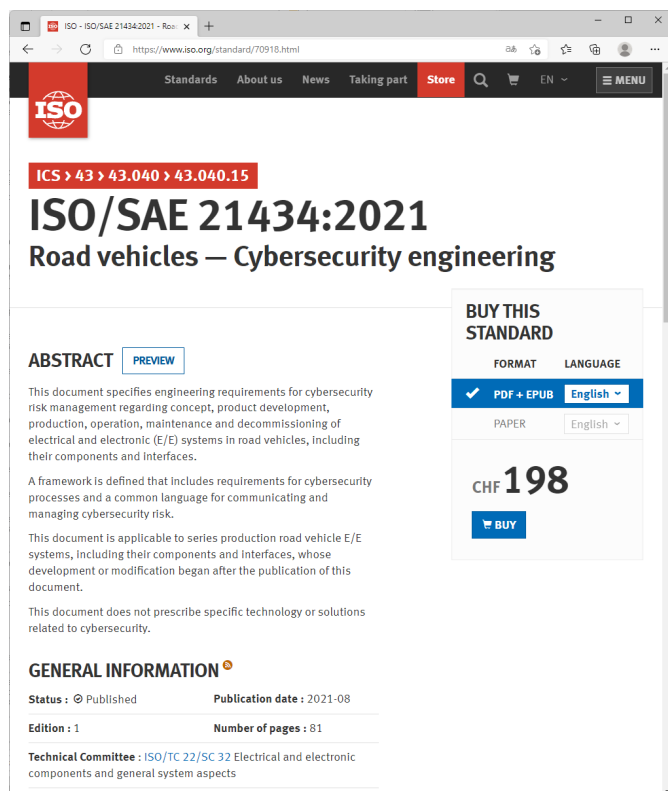


Figure 2 – Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model - Overview

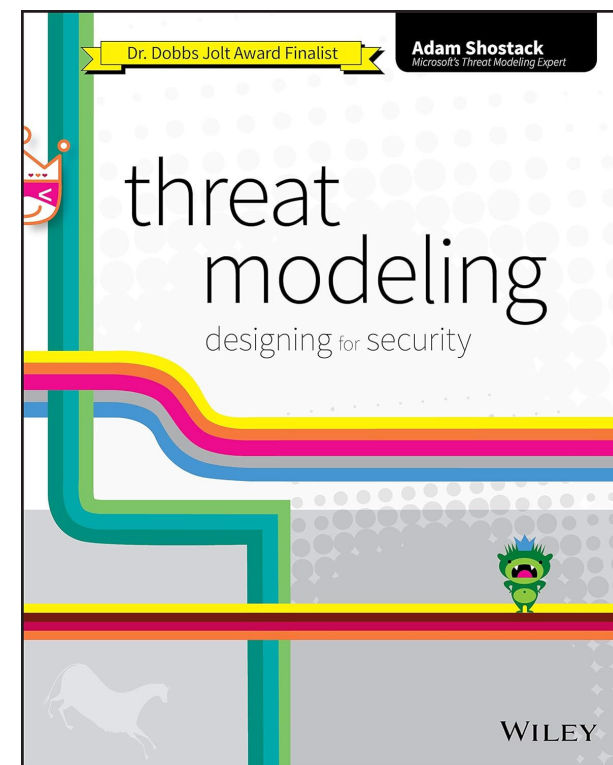
<https://www.iso.org/standard/70918.html>

<https://vdachina.com.cn/upload/default/20210316/4b7fa0169a65d1812962b169f2464969.pdf>

脅威をどのように扱うか論証していくことが重要になっている

## 脅威モデリングとは

- 設計対象のシステムやソフトウェアに関するセキュリティ上の脅威を明確にし、抽出した脅威に対する対策を考えるために利用
- 計の上流工程など早い段階で行うことで、脅威に対する対策を機能要求や非機能要求として抽出し、設計に反映



# 脅威モデリングの重要なポイント

## ■ 何をモデリングするか？

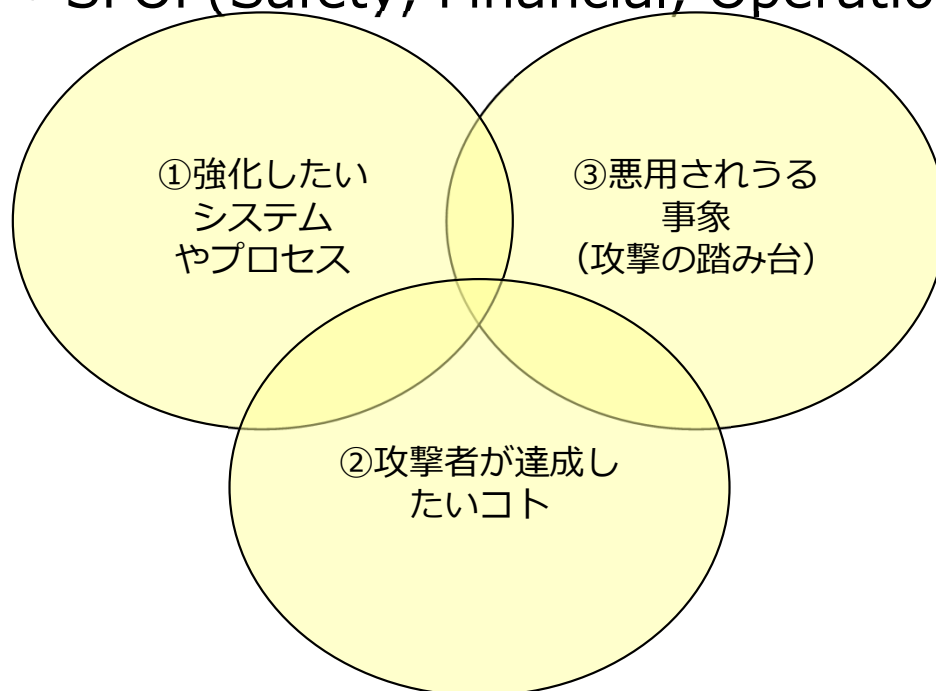
- ①強化したいシステムやプロセス
- ②攻撃者が達成したいコト
- ③悪用されうる事象

明確に定義できていますか？

## ■ ②攻撃者が達成したいコト

- 資産ベースの脅威分析
- SFOP(Safety, Financial, Operation, Privacy)のリスク

ISO/SAE  
21434の  
基本



攻撃者について良く  
プロファイリングすることが重要

## 攻撃者のプロファイリング

---

- 潜在的な脅威を特定し対策を講じるため、攻撃者の特徴や動機、行動パターンを分析するプロセス
  
- 代表的なフレームワーク
  - MITRE ATT&CK
    - － 攻撃者の手法やテクニックに関する情報を収集し、攻撃者のプロファイリングに役立つフレームワーク
  
  - Cyber Kill Chain
    - － 攻撃者の攻撃フェーズを定義し、攻撃者の行動パターンを理解するためのフレームワーク



# MITRE ATT&CK

■ サイバーセキュリティの分野で攻撃者の手法やテクニックに関する情報を整理・分類し、攻撃者のプロファイリングやセキュリティ戦略の構築に役立つフレームワーク

■ MITRE社が開発し広く普及

## ■ 特徴

● 戦術 (Tactics) と攻撃手法 (Techniques)

- 攻撃者が使用する可能性のある戦術や攻撃手法を定義
- 例えば、偵察, アクセス, 実行, 特権昇格, 探索, 収集, 乗っ取り

## Tactics

Techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (3) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (6) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Cloud Administration Command Command and Scripting Interpreter (6) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (6) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication Process (6) Office Application Startup (6) Power Settings	Abuse Elevation Control Mechanism (3) Access Token Manipulation (5) Account Manipulation (6) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host Event Triggered Execution (16) Exploitation for Privilege Escalation Hijack Execution Flow (12) Hijack Execution Flow (12) Impair Defenses (11) Impersonation Indicator Removal (9) Valid Accounts (4)	Abuse Elevation Control Mechanism (3) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Impair Defenses (11) Impersonation Indicator Removal (9) Indirect Command Execution	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (6) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Authentication	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3) Archive Collected Data (2) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4)	Application Layer Protocol (4) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (2) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (2) Web Service (3)	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

# Cyber Kill Chain

- 攻撃者の行動パターンを段階的に分析し、攻撃のプロセスを理解するためのフレームワーク
- Lockheed Martin社によって提案

## ■ 特徴

- (以下の)攻撃の段階を定義

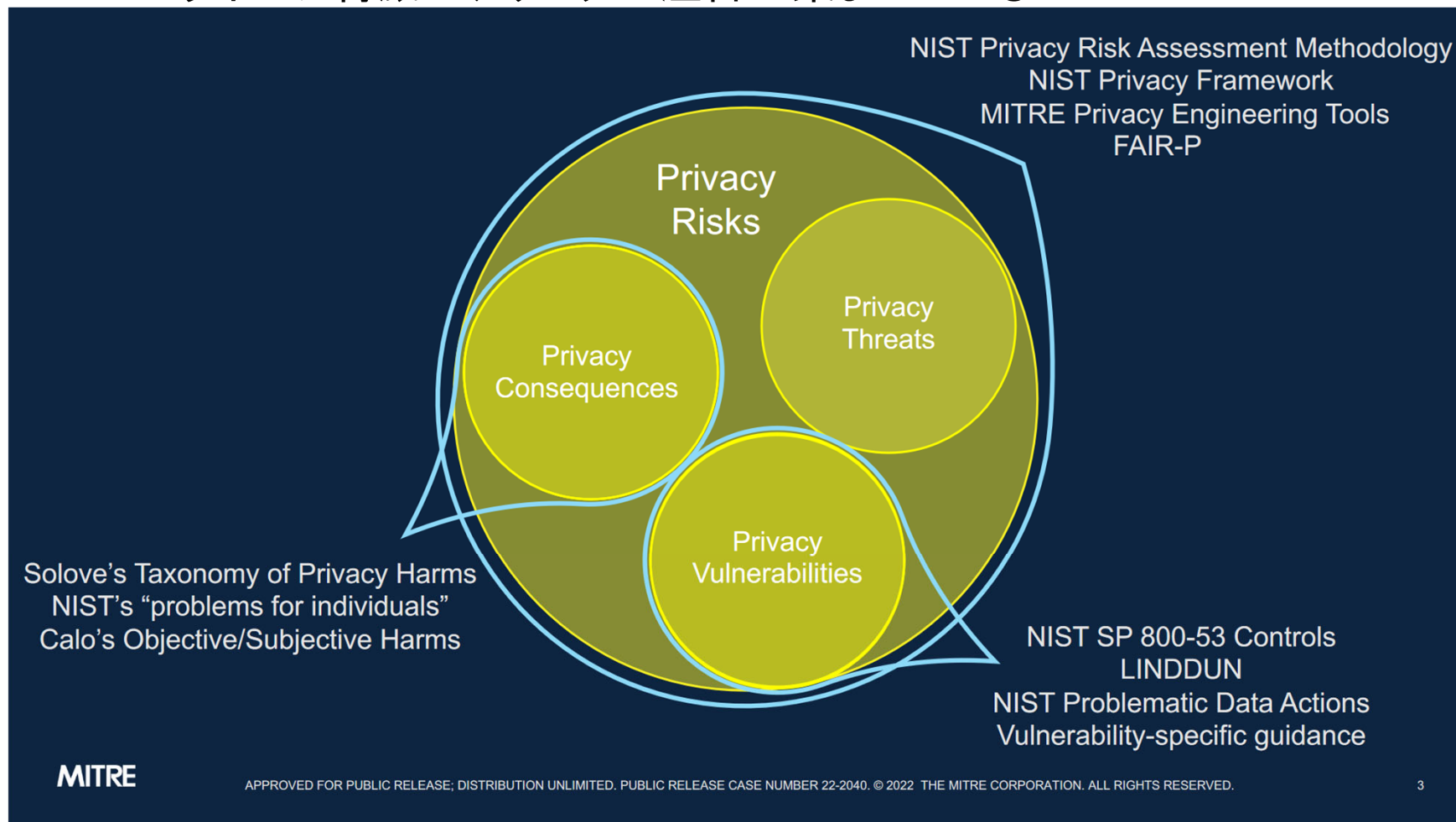
偵察 (Reconnaissance)	攻撃者はターゲットを選定し、情報を収集
武装化 (Weaponization)	攻撃者は攻撃に使用するツールやマルウェアを準備
配信 (Delivery)	攻撃者は攻撃対象に対して悪意のあるコードやファイルを送り込む
悪用 (Exploitation)	攻撃者は脆弱性を悪用して侵入を試み
インストール	攻撃者は侵入したシステムにバックドアやマルウェアをインストール
指揮統制 (Command and Control)	攻撃者は侵入したシステムをコントロール
目的達成 (Actions on Objectives)	最終的な目的を達成し、データ窃取やシステム破壊など実行

Cyber Kill Chainは攻撃者の行動を可視化し防御戦略を構築するための貴重なツール

# それでも難しいのが, Privacy

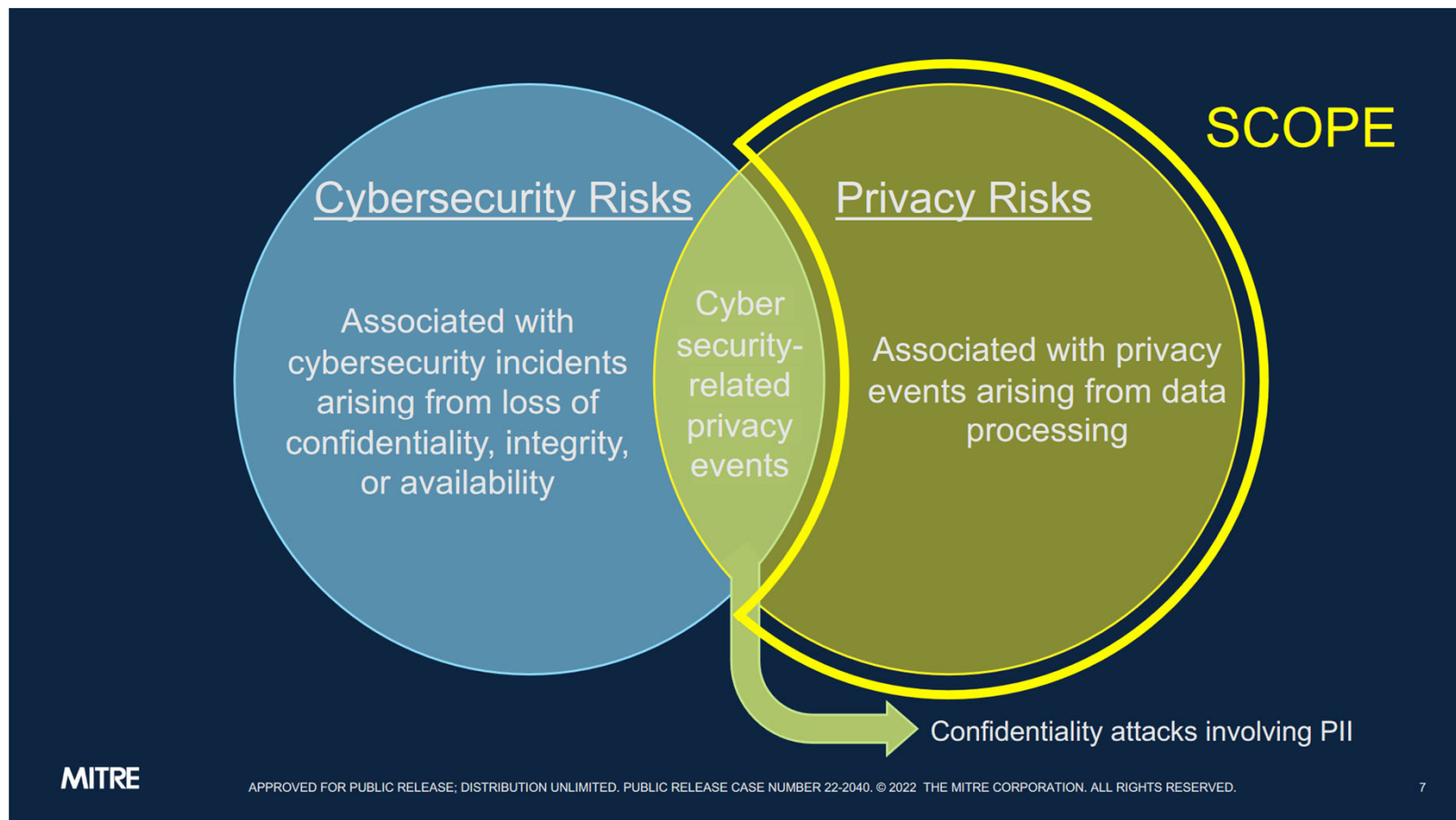
## ■ Privacy Threat Modeling MITRE@USENIX Security 2022

- プライバシに関するガイダンスやフレームワーク, ツールが存在
- プライバシ脅威モデリングに注目が集まっている



# プライバシーリスク

- サイバーセキュリティリスクと関連し、2つに分類
- データ処理に起因するプライバシーイベントに関連するリスク
- プライバシーイベントに関するサイバーセキュリティ



# Solveの分類法

- Solveの分類法では4つのカテゴリーが定義
- この4つのカテゴリーは、さらに次の小カテゴリーに分割

カテゴリ	意味（上段）と小カテゴリー、ガイドワード（下段）
情報収集	行動様式を変えるほど、特定の方法による継続的な監視を指すこと
	監視する／される、尋問する／される
情報処理	断片的なデータを組み合わせ、収集すること
	集計、識別、セキュリティ、二次利用、排除
情報の流布	暴露や情報を歪めることにより利益を得ようとする
	守秘義務違反、開示、露出、脅迫、収用、歪曲
侵略	合理的な人にとって非常に不快なもの、権威による不本意な侵入に関係すること
	侵害、意思決定妨害

# MITRE社のアプローチ

## ■ MITRE ATT&CKに対し、以下の手順と小さな修正で対応可能

- § 攻撃を個々の脅威アクションに分解
- § 類似した脅威アクションを持つ攻撃を脅威クラスターにクラスター化
- § データセット内のすべての攻撃を既存のグルーピングにマップし、必要に応じて脅威クラスターを絞り込み、名称を変更
- § 各脅威クラスターを分類法にマップ
- § 分類法の脅威アクションを使用して、各クラスターの一般的なキルチェーンを構築 (脅威パターンと呼ぶ)

NOTICE	CONSENT	COLLECTION	INSECURITY	IDENTIFICATION	QUALITY ASSURANCE	MANAGEABILITY	AGGREGATION	PROCESSING	SHARING	USE	RETENTION & DESTRUCTION	DEVIATIONS
OUT OF SEQUENCE	OUT OF SEQUENCE	APPLICATION USE	LACK OF ACCESS CONTROLS	FINGERPRINT	AGE NOT VERIFIED	NO SUBJECT ACCESS	PII WITH OTHER DATA	BEHAVIORAL ANALYSIS	SHARING SENSITIVE DATA	IMPLICATE	DATA RETAINED AFTER USE	STATED POLICY
UNCLEAR	MISLEADING	REGISTRATION	INSUFFICIENT ENCRYPTION	TRACE	UNVETTED DATA SOURCE	NO SUBJECT MANAGEMENT	SENSITIVE DATA WITH OTHER DATA	TRAWLING FOR INFORMATION	SHARING DEROGATORY DATA	TARGET	DATA IMPROPERLY DESTROYED	DUA
MISLEADING	INSUFFICIENT	TRACKING	UNDERMINING AUTHENTICATION	RE-IDENTIFICATION	UNVETTED DATA ACCURACY	NO SUBJECT DELETION	MULTI-SOURCE AGGREGATION	INSUFFICIENT DOWNSTREAM REQUIREMENTS	UNANTICIPATED SHARING	EXTORT		CLAIMED CERTIFICATION
INSUFFICIENT	ABSENT	SNIFFING	DETECTION FAILURE	PERSISTENT IDENTIFIER	UNVETTED RECIPIENT	SETTINGS AFFECTED BY OUTSIDE FORCES	PROFILING	INTERNAL APPROPRIATION	UNANTICIPATED PUBLISHING	MANIPULATE		REGULATION
ABSENT	NO OVERALL OPT OUT	PRETEXTING	INSUFFICIENT DOWNSTREAM REQUIREMENTS		UNVETTED SECURITY	CONFOUNDED USER CONTROLS		INTRODUCING BIAS	EXPOSURE	INTRUDE		
INCORRECT	NO GRANULAR OPT OUT	EXTERNAL APPROPRIATION	MISCONFIGURED PERMISSIONS		UNEVALUATED DATA BIAS	BYPASS		CLUSTERING	DOXXING	TAILORED DISPLAY		
	INHERITED	INTERCEPTION			DATA NOT DE-IDENTIFICATION	PREEMPTION OF SETTINGS		INSUFFICIENT DE-IDENTIFICATION	INSUFFICIENT CONTEXT	SELL		
		SOLICITING						INDESCRIMINATE PROCESSING	INSUFFICIENT DUA			
		RECORDING						DERIVING DEROGATORY INFORMATION	RECIPIENTS ACTING OUTSIDE DUA			
								INFERRING ABOUT SENSITIVE INFORMATION	AFFORDING REVELATIONS			


Example: Data De-identification Threat Pattern

SCDLでも将来的には  
プライバシーを  
分析する必要は？

# 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



サイバーセキュリティの  
専門家は実装の話ばかりで  
噛み合わない

機能安全の専門家



機能安全の専門家に  
相談しても話が難しい

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～)



## 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

以降では, 上記課題2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

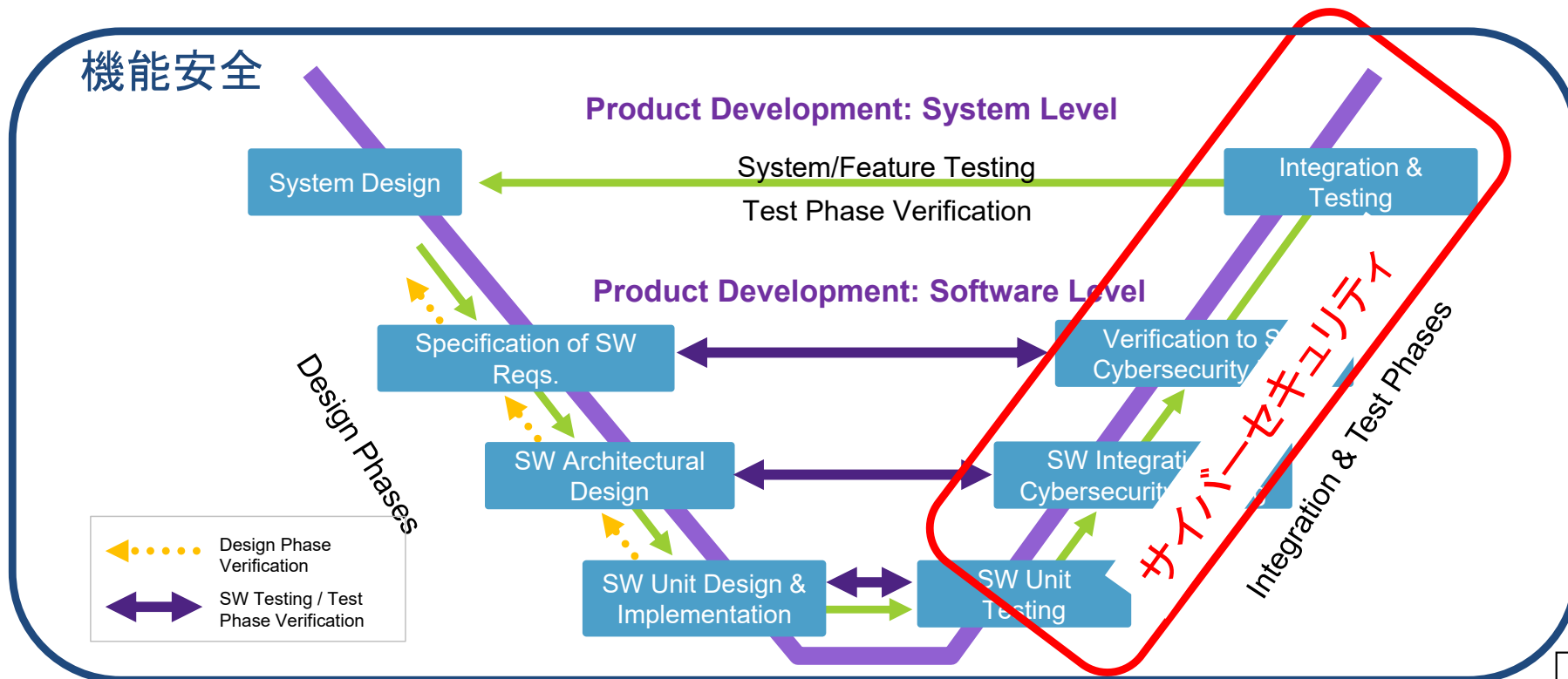
- 情報の機密性, 完全性および可用性の維持
  - さらに真正性, 責任追跡性, 否認防止, 信頼性などの特性の維持を含める
  - 機密性(Confidentiality)
    - アクセスに認可された者だけが情報にアクセスできること
  - 完全性(Integrity)
    - 情報及び処理方法が正確であること及び完全であること
  - 可用性(Availability)
    - 認可された利用者が, 必要なときに情報及び関連する資産にアクセスできること
- ➔ システムの弱い点(≒脆弱性)を保護する機能を実装

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

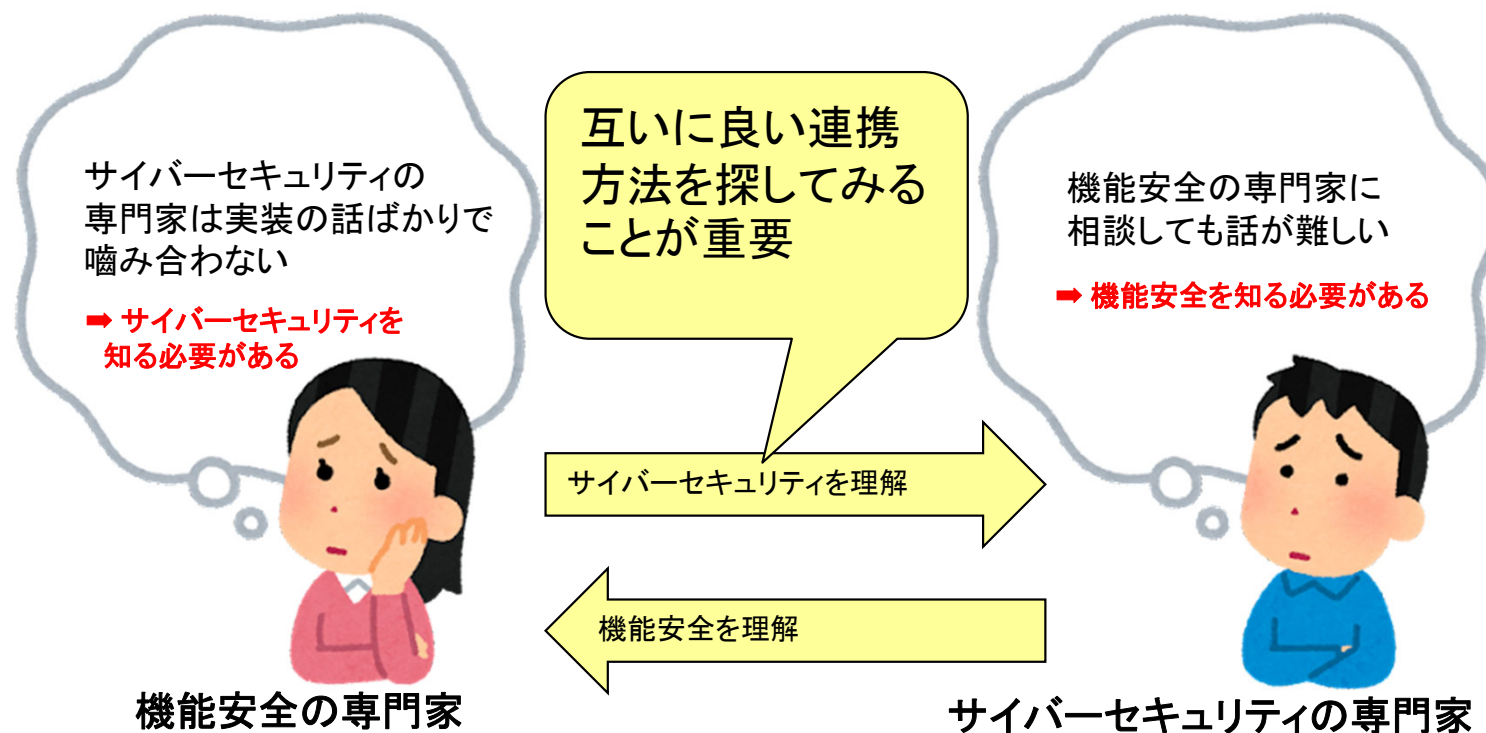
### ■ 課題1. 前提となる専門性/知識/アプローチの違い

- 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. そして, 擦り合わせも必要
- 機能安全とサイバーセキュリティの重要度は対等

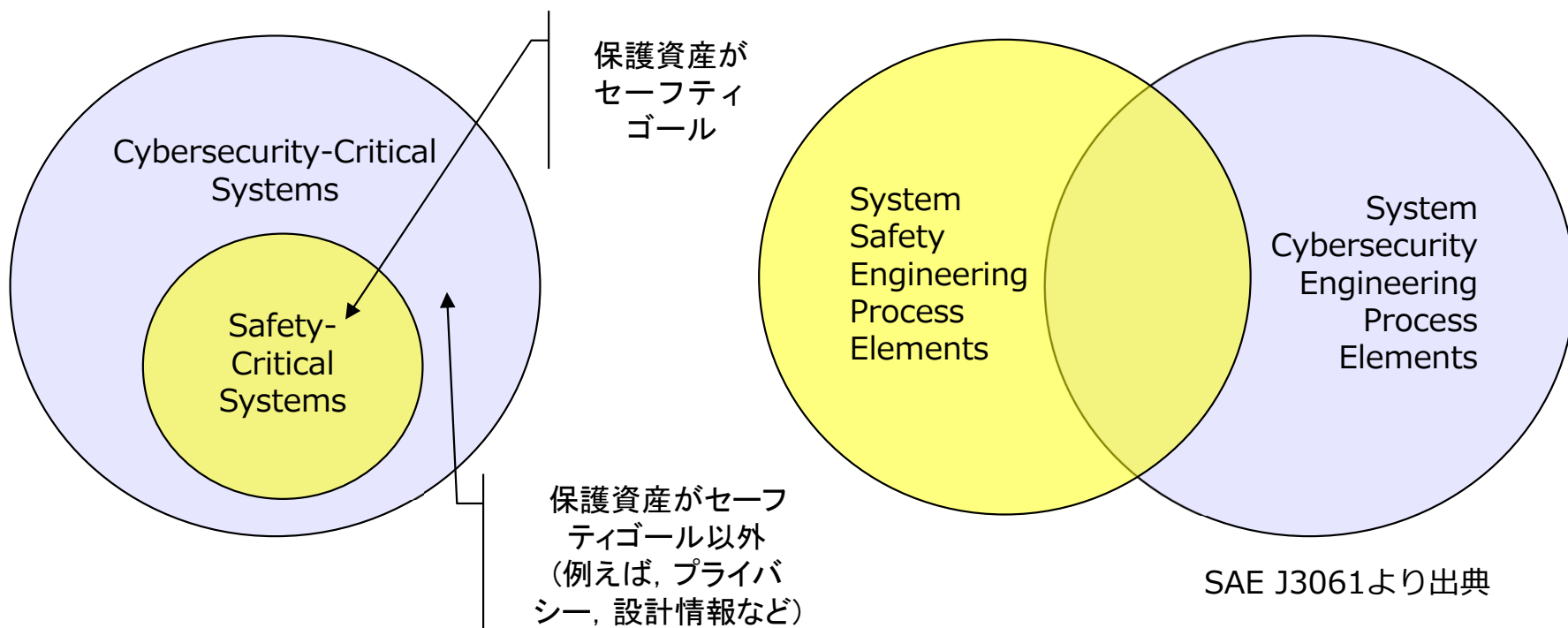


セキュリティSWGでは機能安全の専門家が脅威分析を実施

## 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

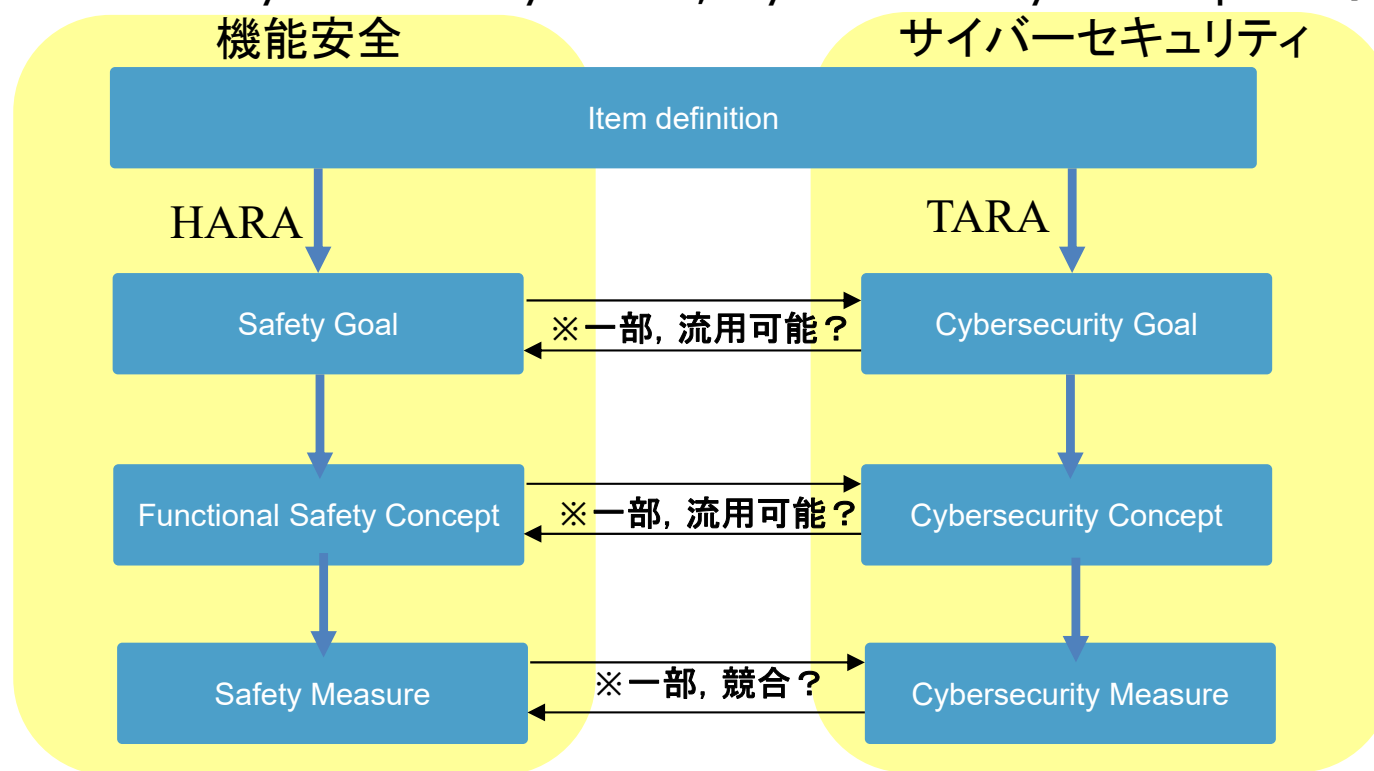
### ■ 課題2. セーフティとセキュリティの開発プロセスの統合/連携

#### ■ 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

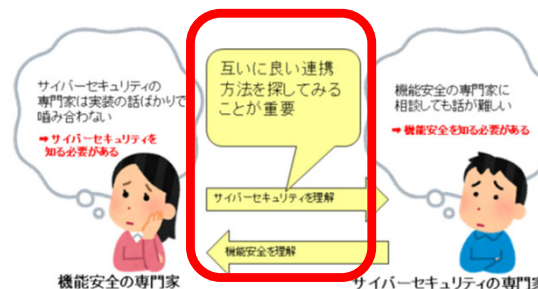
### ■ 開発プロセスの統合/連携をどのように進めるか？

➡ 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

# セキュリティSWGにおける過去の成果

## ■ 事例1. 機能安全の成果物を利用し脅威分析を実施

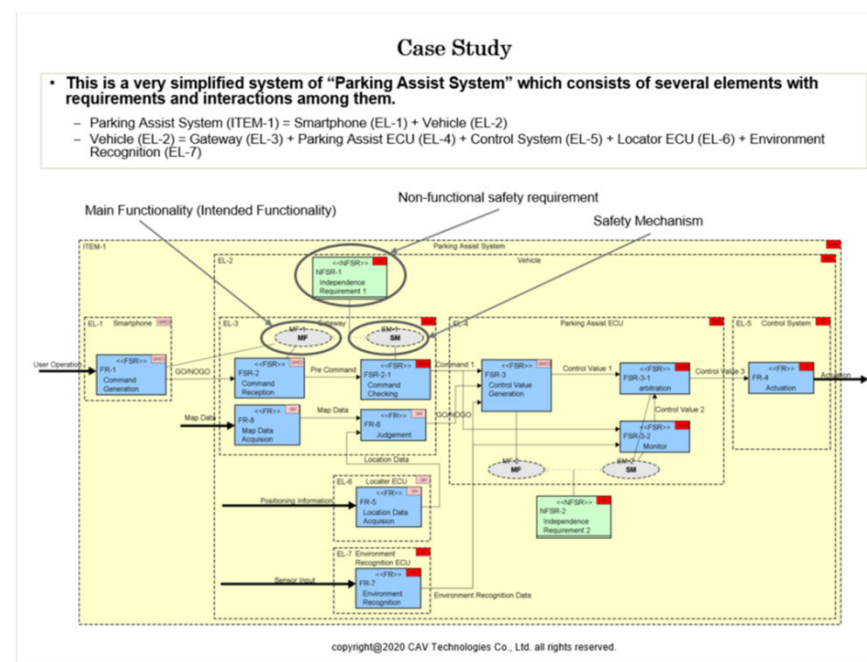
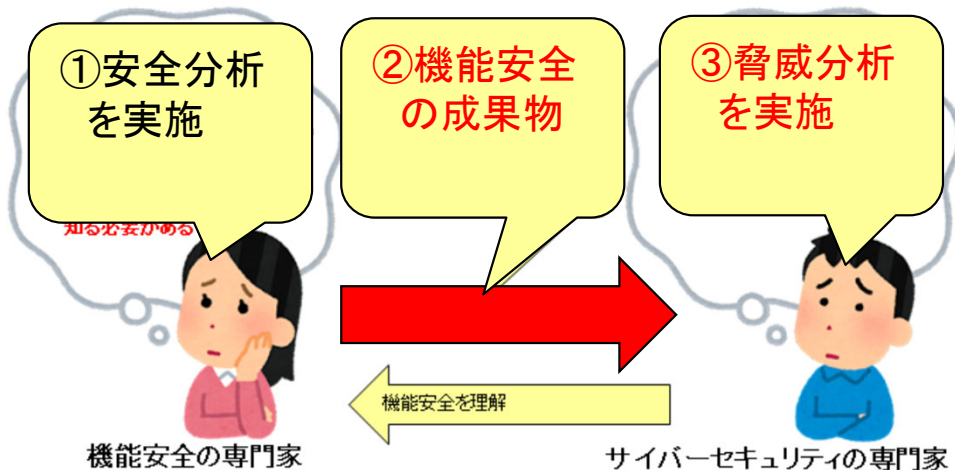
- ➔ 評価対象システムとして“(安全機構が入った)スマホでパーク“を使用
- ➔ 安全機構はセキュリティ強化策として有効か？

## ■ 結論

- 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
  - 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

## ■ 取り組み

- セキュリティ強化策の導出
- 安全分析へのフィードバック





# 現在の議論

- 議論1. 機能安全とサイバーセキュリティの連携プロセス
  - 安全機構(セキュリティ強化策)への影響や干渉がないか？
- 議論2. Concept Phaseで取り扱うべき抽象度(粒度)
  - SCDLの記法も拡張が必要か？

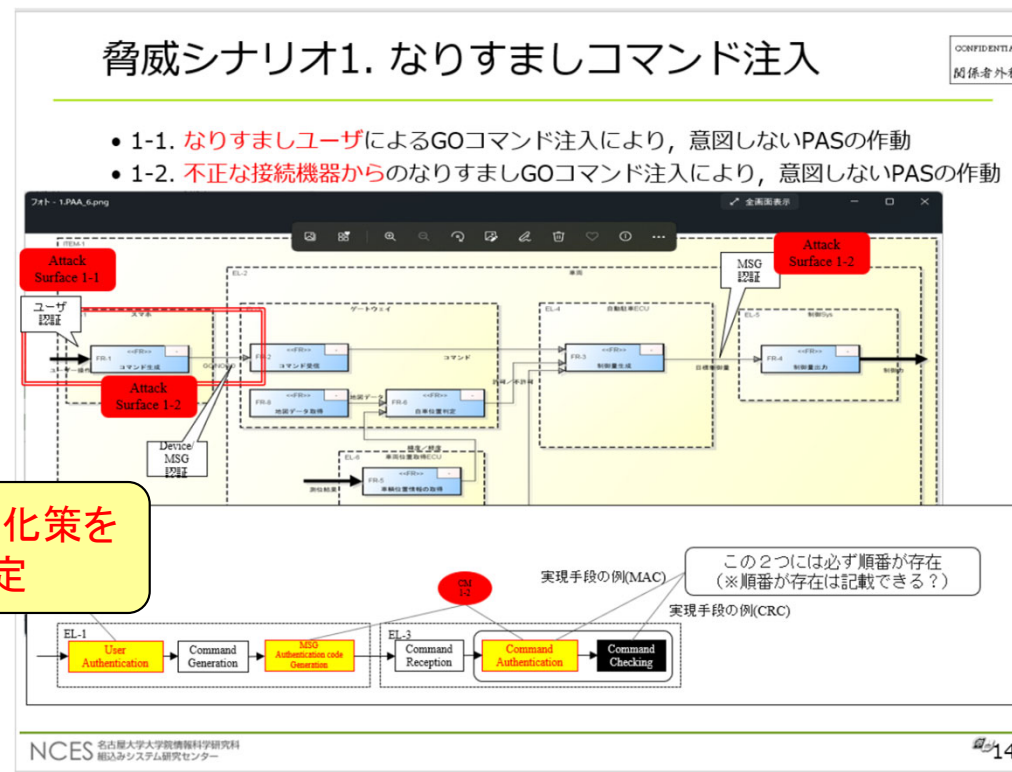
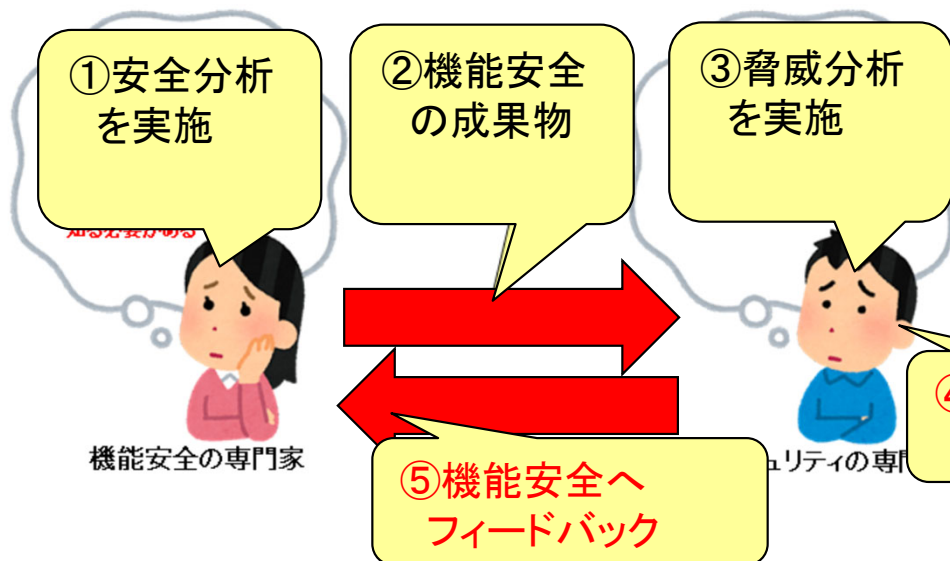
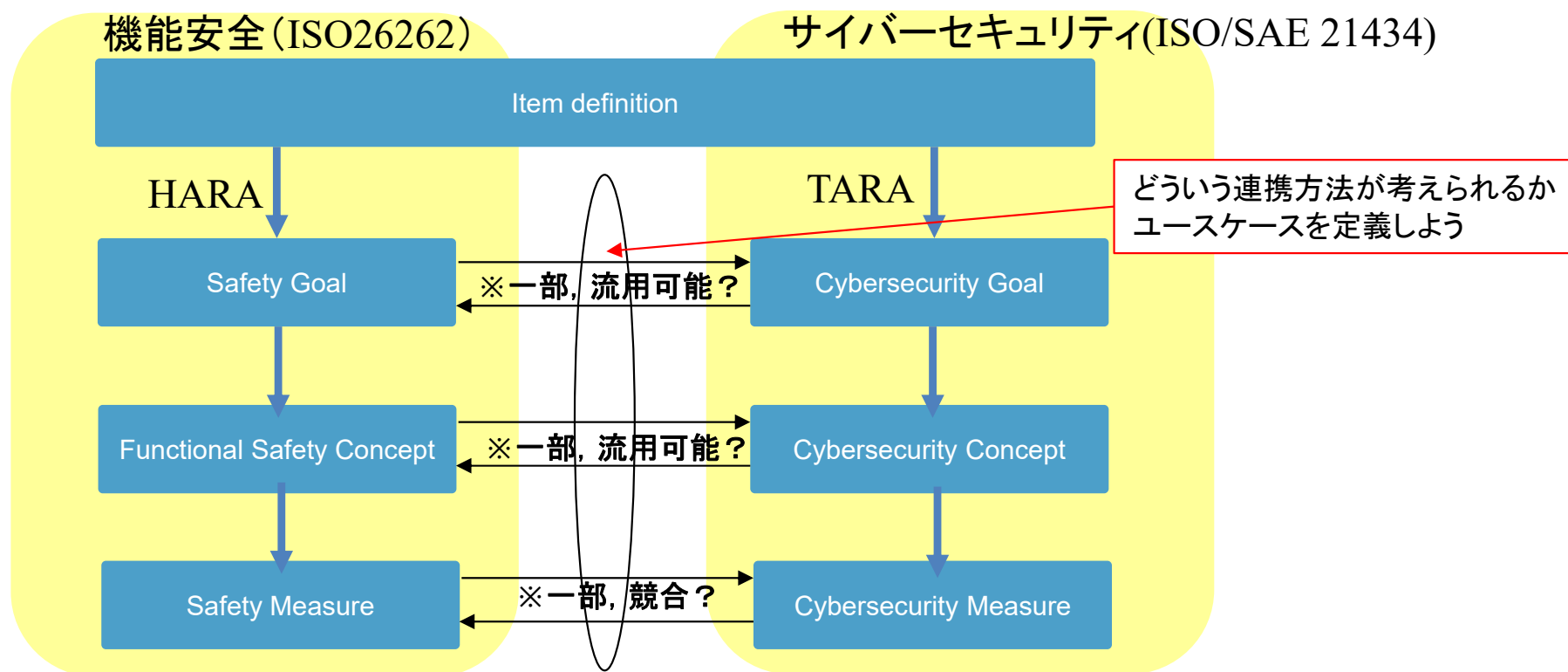


図1. 強化策を導入した場合の事例

セキュリティ要求が安全要求に影響を与える可能性がある

# 議論1. 機能安全とサイバーセキュリティの連携プロセス

- 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ー



HARA: Hazard Analysis and Risk assessment  
 TARA: Threat Analysis and Risk assessment

## 議論2. Concept Phaseで取り扱うべき抽象度(粒度)

### ■ 抽象的に議論したい機能安全 vs 具体的に議論したいサイバーセキュリティ

- 落としどころが必要ではないか？
- 適切な抽象度を議論中
  - 脅威や強化策の抽象度を議論

表1. 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)

高い(抽象的)

↑

抽象度

↓

低い(具体的)

どういう抽象度で取り込むか？

脅威分析(=セキュリティの性質)

↓

脆弱性(=機器に)

- ・脆弱性
- ・攻撃方法
- ・強化技術

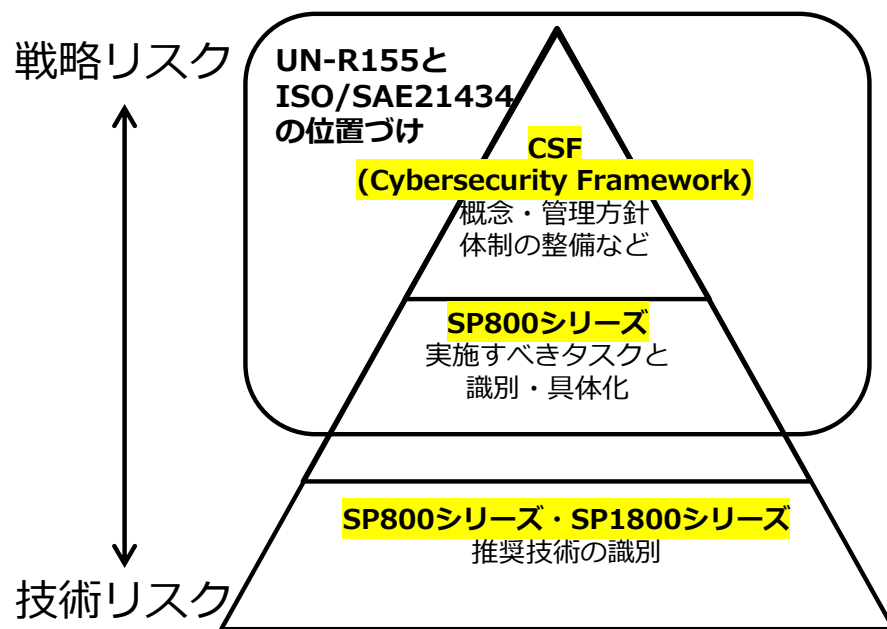
多層防御  
➡ Defense in depth

(※1) 脆弱性やCountermeasureと関連

# UN-R155とISO/SAE21434対応へ向けて

## ■ どのように分析するか的事例開発が必要

- 要求の抽象度が高いため、分析事例の開発が重要
- また、セキュリティレベル(例えば, CAL)の活用も重要



NISTが定義する対策アプローチ

[https://www.manageengine.jp/solutions/nist\\_publications/](https://www.manageengine.jp/solutions/nist_publications/)

Cybersecurity Assurance Level (CAL)の例

CAL	説明	評価の深度	どれくらい評価	誰が評価
CAL1	低度から中程度のサイバーセキュリティ保証が必要	要求ベースのテスト	既知の情報に基づいて脆弱性を分析や評価	特になし
CAL2	中程度のサイバーセキュリティ保証が必要			別の人
CAL3	中程度から高度のサイバーセキュリティ保証が必要	コンポーネント間の相互作用	探索的手法で脆弱性を分析や評価	異なるチーム
CAL4	高度のサイバーセキュリティ保証が必要	コンポーネント間の全組み合わせ		独立した人

CALをセキュリティレベルと見立てて分析する方法を検討

# 我々の提案. ISO26262ベースのセキュリティ論証手法の確立



## ■ 前提は自動車業界(機能安全)での設計の考え方の踏襲

- 機能安全と同様(例えば, SCDL図を用いたセキュリティ分析手法)

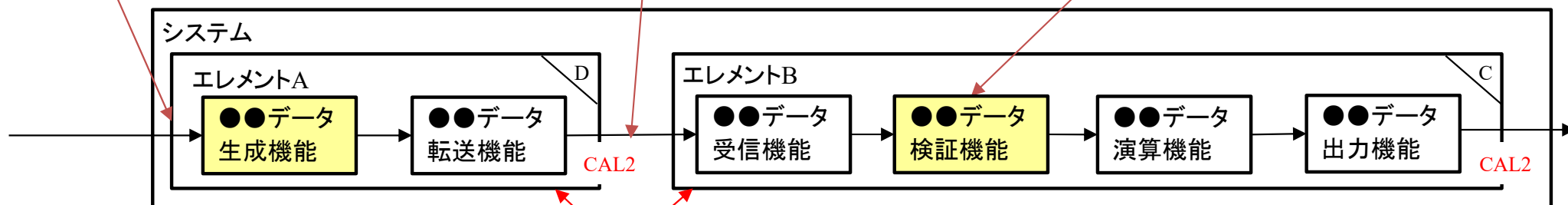
## ■ SCDL図を用いたセキュリティ分析手法

- 実現方法はセキュリティレベル(CAL)に追い出し, コンセプトフェーズではセキュリティレベルのみをエレメントに割り付ける
- セキュリティレベルにマッピングされる強化策は別で規定(次頁参照)

(例2) CANで通信することも実現方法であるため, コンセプトフェーズでは言うてはいけない.

(例1) エレメントAを”ECU A”で実現するとは言わない.

(例3) 安全方策の実現方法(CRC など) は決定しない.



提案  
の具体例

コンセプトフェーズではエレメントにCALを割り当てることを要求

強化策や実現方法(例. 通信コンポーネントのCAL2の強化策 = SecOC Profile 3))は別表で定義

(注) エレメントは機能安全の定義ですので, セキュリティ上はエレメントをコンポーネントと読み替えて下さい.



# 強化策や実現方法の表現方法

## ■ IEC62443と同様、各要素の機能属性ごとに強化策(技術)を規定

会社(あるいは業界)のベースライン ... Minimize(CAL<sub>i</sub>)

### FR 3 – System integrity

FR3における各セキュリティレベルの定義 (=このSLをCALとして見なす)	要素の機能属性				
	CR1 通信 機能	CR2 ソフトウェアの 完全性検証機能	CR3 入力検査 機能	CR4 監査情報の 保護機能	...
CAL 1 - 偶発的または偶然的な操作から自動車のインテグリティを保護する	× (選択不可)	○ (可)	× (選択不可)	× (選択不可)	...
CAL 2 - 低いリソース、一般的なスキル、および低いモチベーションで単純な手段を使用する人物による操作から自動車のインテグリティを保護する。	○ (可) SecOC Profile 3	○ (可) HSMベースSecure Boot (共通鍵)	○ (可)	○ (可)	...
CAL 3 - 中程度の資源、自動車特有のスキル、及び中程度の動機で、洗練された手段を用いる者による操作から自動車の完全性を保護する。	○ (可) AEAD	○ (可) 非対称鍵ベースSecure Boot	○ (可)	○ (可)	...
CAL 4 - 広範な資源、自動車特有のスキル、及び高い動機付けを持つ洗練された手段を使用する者による操作から自動車の完全性を保護すること。	○ (可) TLS	○ (可) Secure Element必須	○ (可)	○ (可)	...

①自動車に必要な要素の属性を定義する必要あり

②各機能属性のレベルごとに適用される強化策を決める  
また、最も低いレベルは業界団体に決定し、技術を定めることが必要

## 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
  - ➔ 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
- 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](mailto:scdlsec@scn-sg.com)