車載システムを想定した機能安全機能とセキュリティ機能の統合要件定義手法

左近 透[※1]　　中本 幸一[※1]

車両ソフトウェア開発における，ISO 26262 と自動車セキュリティ分析ガイド JASO TP15002 をベースとした機能安全機能とセキュリティ機能の要件定義手法を提案する．機能安全とセキュリティ双方の要件定義を統合するための動作モデルと開発プロセスモデルを定義した．これは安全に対する要求を詳細化し，要件を定義する過程で，セキュリティ脅威を詳細化しセキュリティ要件を特定するものである．また，セキュリティリスク評価を，機能安全要件の定義段階に応じて行う．まず, ASIL 導出時に利用する過酷度と回避可能性に対応する対処の規準値となるリスクスコアを定める．更に具体的な脅威の特定が可能になった時点でリスクスコアリングを実施し，そのスコアから対応すべき脅威を選択し，対処すべきセキュリティ機能を決定する．

A requirement definition method to integrate functional safety and security for vehicle software development

Toru Sakon[※1], Yukikazu Nakamoto[※1]

We propose an integrated requirement definition method the functional safety based on ISO 26262 and the security functions based on the risk assessment guide JASO TP-15002 in vehicle software development. We define a behavior model and a development process model. The security risk assessment is performed depending on the development phases in the functional safety. The threshold of risk scores are determined corresponding to the severity and evasiveness to be used when ASIL is derived. The risk scoring is carried out when the specific threats can be derived. With the score, the threats to be dealt with are identified and the security functions for the threats are obtained.

1　はじめに

自動車や製造機械，発電所，鉄道や医療用器械に代表される制御機器の設計に際しては，故障や動作異常の発生により生命や設備を危険にさらすことの阻止が優先度の高い目標である．安全には，危険そのものを発生させない本質安全と，危険につながる事象が発生した場合に，それに対処する機能により危険回避を行う機能安全がある．ISO 26262[1] は自動車の機能安全に関する規格である．

一方，制御機器の安全動作に対する脅威として，機器の故障などに加えて，サイバー攻撃の懸念が高まりつつある．また，研究者による自動車のセキュリティホールを利用した攻

※1　兵庫県立大学(University of Hyogo)

撃の発表や，プラントに対するサイバー攻撃の実例も発生した。ICS-CERT によると 2009 年以降，インシデント報告は増え続け，2013 年の ICS-CERT 報告書[2] では 250 件超の報告がされている．

このような制御機器に対するサイバー攻撃に対する対応として，電気・電子・プログラマブル電子機能安全システムに対する機能安全規格，IEC 61508 に対応したセキュリティ規格，ISA/IEC 62443[3] が制定されている．自動車産業においても，米国 SAE が開発した SAE J3061 -Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[4] などサイバー攻撃に対するガイドラインや規格が提案されている．

しかし，機能安全とセキュリティは安全動作保護の観点から密接に関係すると考えられるが，開発プロセスや相互の機能の関係などは明確でなく，議論が継続されている．例えば，SAE J3061 はセキュリティ機能開発プロセスを中心に規定して記述されており，機能安全機能との関係性は，対応する機能安全開発プロセスとの情報交換が例示されているのみである．同種の規格，ガイドラインである EVITA[5] などでも同様である．

本論文では，車両開発を想定した場合の機能安全機能とセキュリティ機能の統合要件定義手法を提案する．まず，開発対象の定義を行うアイテム定義では，セキュリティ攻撃にさらされる点とそこで発生し得る脅威の組み合わせである Exposure Control Point（以下，ECP と略す）を導入する．次にハザード分析とリスクアセスメントでは，セキュリティ分析手法に，JASO TP15002 で記載されている車載システム向けセキュリティ分析手法を適用する．ECP をハザード要因とし，対応するハザード事象及び回避可能性を求め，これらを元にした対策基準指標を決定する．次に機能安全規格の機能安全コンセプトとシステム設計に相当したセキュリティ仕様の導出において，ECP を段階的に詳細化して脅威を具体化しつつ対応する対策を定める．この各段階において，機能安全における故障モード対策と脅威対策との対応を確認させ，対応しない部分について技術セキュリティ要求の定義を行う．

2 関連研究・標準

自動車におけるセキュリティ機能開発に関連する標準は幾つか提案されている．この中で，明示的に機能安全開発とセキュリティ開発の関連性について述べたものに，SAE J3061[4] がある．しかし，概念的な説明にとどまり，手法や統合モデルの提案には至っていない．一方，研究レベルでは，安全とセキュリティに関するリスクを統合して扱うリスクアセスメント手法[6][7][8] が幾つか検討されている．しかし，統合された手法による機能安全機能とセキュリティ機能の要件定義プロセスの検討は行われていない．

本研究と同じく要件定義に対する研究では Automotive Spice をベースにした Macher らの研究[9] がある．Macher らは，研究[10] で提案されたリスクアセスメント手法を利用する．この手法は，機能安全のハザード分析を実施するタイミングで脅威分析を行い，ハザードの大きさや脅威の起こしやすさなどから対処のレベル分けを決定する．脅威への対策要件は，車両ネットワークの階層から対策を検討する静的手法，更に機能間の呼び出し階層から対策を検討する動的手法で検討される TrustZone と呼ばれる境界面を定義し，その境界面からの攻撃を防御する方策として対抗策が検討される．この境界面上のハードウェアとソフトウェア間のインターフェース（HSI）にレベル付けされた脅威対抗策が配置される．Macher らは仮想ステアリングシステムを対象に要件分析を行った．

Macher らの研究では，機能安全のハザード分析と同じタイミングでリスクアセスメントを行うため，機能安全と並行してセキュリティ要件分析のプロセスが定義できる．しかし，脅威の起こしやすさなどは対象システムの詳細な情報を必要とする場合が多く，ハザード分析段階ではこれらの情報は必ずしも入手できない．そのため，リスクアセスメント時のリスクスコアリング値が本来のリスクを正しく反映していない可能性がある．また，ISO 26262 の各プロセス段階に相当する作業は定義されているが，それら作業及び出力と各プロセスの入力情報が関連付けられていない．また，脅威から機能を保護する機構の要件分析であり，脅威発生時の車両の安全な振る舞いの検討は行われていない．

3 ISO 26262とJASO TP15002

自動車制御システムの機能安全規格である ISO 26262 と，自動車のセキュリティ分析を目的としたセキュリティ分析ガイド JASO TP15002[11] の概要を述べる．

3.1 ISO 26262

ISO 26262 は，自動車の機能安全の実現のための安全管理，要件定義，設計，製造，評価 / 検証，生産と運用，それを支える要件定義や開発上必要支援プロセス，並びにガイドラインなどから成る．自動車の機能安全とは，通常動作状態で機器の故障が発生し故障モードに陥った場合，機能安全機能により事故が発生しないような安全状態への移行を実現することである．開発プロセスは，ウォーターフォール型プロセス（V 字プロセス）を基本として定義されている．ここでは，本論文の検討対象である要件定義からシステム設計に至るプロセスを述べる．

(1) アイテム定義（開発対象定義）

アイテムとは，車両観点で見た機能を実現する開発対象である．形式的には，センサなどの外部入力，演算などの内部処理，アクチュエータへの出力から成る要素を組み合わせたものである．例えば，パワーステアリング機能は，ハンドルにかかるトルク，車速と舵角を入力とし，それに対応したトルク出力を計算し，アクチュエータにトルク調整出力を出す（図 1）．

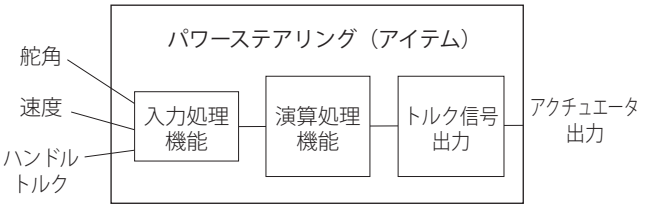

図 1　パワーステアリングアイテムの構成

(2) ハザード分析とリスクアセスメント

ISO 26262 ではリスクを「危害発生確率とその危害の過酷度との組み合わせ」で定義している．

そのために，まず，ハザード（危機事象）とハザードが発生する状況を特定し，帰納的 / 演繹的手法で発生可能性の分析を行う．一般には，HAZOP（Hazard and Operability Study）手法で不作動，勝手な動作，過大，過小などのガイドワードで制御出力の期待値からのズレを想定し，ハザードを導出する．次に FTA（Fault Tree Analysis）でハザードの原因となる事象を洗い出す．最後に FMEA（Fault Mode and Effect Analysis）を適用し，個別の故障要因から FTA の正しさを検証する．

次に特定されたハザードと状況に対してリスクアセスメントを行う．ISO 26262 では不具合発生時にその状況や操作者の回避可能性を考慮した，達成すべき安全度の指標としてのリスク低減目標 ASIL（Automotive Safety Integrity Level）を定める．ASIL はハザードの過酷度，発生頻度，回避可能性から，定められた分類表に従って 4 段階の ASIL と一般品質保証レベルに分類される．開発では，ASIL のレベルに応じた開発手法や検証，システム構成を取ることが要求される．

この後，ハザード発生に対する安全機能を実現するための要件（セーフティゴール）を導出する．

(3) 機能安全コンセプトの導出

セーフティゴール実現のために，アイテムを構成する各要素またはアイテムの外部に，安全実現のための機能を割り当てた機能安全コンセプトの導出を行う．

まず，セーフティゴールを詳細化して，達成に必要な機能（機能安全機能，以下，安全機能と略す）を導出する．次に，機能安全要求の抽出を行う．機能安全要求とは，セーフティゴールに基づくアイテムの安全な振る舞いの仕様，及び実装に依存しない安全方策である．更に，作業時点で判明しているアイテムの具体的な構成に基づいて機能安全要求をアイテムの構成要素またはアイテム外部の実装に割り当て，機能安全コンセプトの導出が完了する．安全機能の追加により，アイテムの構成にも安全機能が追加される（図２）．

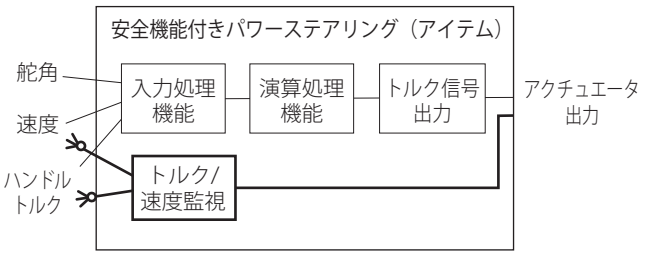

図２　安全機能付きパワーステアリングアイテムの構成

(4) 技術安全要求の導出とシステム設計

安全機能の設計対象であるアーキテクチャ（前提アーキテクチャ）に当てはめて，実装に関する要件を導出したものが技術安全要求である．これらをアイテムの構成要素に安全機能実装要件として割り当てたものが技術安全コンセプトである．システム設計では技術安全要求を元に，ハードウェア・ソフトウェア・ハードソフトインターフェースに機能要求を割り振り，実装仕様が決定される．

3.2 JASO TP15002 セキュリティ分析

JASO TP15002 は公益社団法人自動車技術会の開発した自動車システム向けのセキュリティ分析ガイドである．このガイドのセキュリティ分析は，分析対象の定義，脅威分析，リスクアセスメント，対策方針決定，セキュリティ要件の選択という 5 つのフェイズから成る．

分析対象の定義では，分析対象の構成要素及び構成要素間のデータフローのモデルを作成する（図 3）．更に構成要素ごとに，保護すべき機能とデータを保護資産として抽出する．

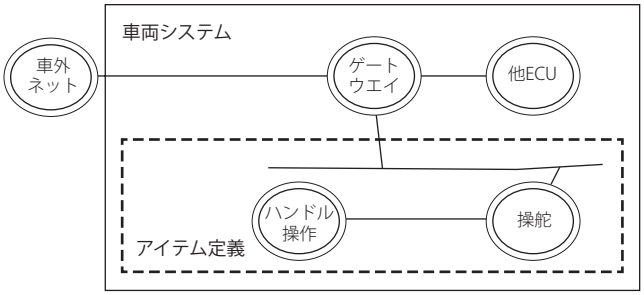

図３　分析対象モデル例

次に対象システムのライフサイクルで対象システムに関与可能な人・組織（ステークホルダ）を定める．これは，次の脅威分析に際して，対象システムの攻撃目標や攻撃傾向・動機の分類に利用する．

脅威分析では，まず分析対象システムの置かれた環境や条件を定義する．次に当該条件における保護資産に対する脅威を，どこ（Where）から，誰が（Who），いつ（When），どのような動機（Why）で，どのように引き起こされる脅威（What）かの形式で整理する．

リスクアセスメントでは，抽出された脅威のスコアリングを行う．保護資産の重要度と攻撃困難さを元にする CRSS(Common Risk Scoring System) と RSMA（Risk Scoring Methodology for Automotive system）が手法として示されている．ある基準以上の脅威は FTA などで原因を抽出，対策方針を決定する．

最後にセキュリティ機能要件とセキュリティ保証要件を定義する．前者は，ISO/IEC15408 CC（Common Criteria）Part2 で定義されるセキュリティ機能コンポーネントの実装を要件としたものである．後者は，CC Part3 の Evaluation Assurance Level で指定し，相当する保証要件を確認検証する．

4　機能安全･セキュリティ開発の問題点

機能安全・セキュリティ開発で解決すべき考える問題点を列挙する．

(1) 安全機能とセキュリティ機能の関係の明確化

セキュリティ脅威の一部は安全機能で対処可能な場合があ

る．例えば，車載ネットワークの Flooding によるサービス拒否攻撃では，当該ネットワークに接続された ECU 間の通信が途絶する．しかし，安全機能で，断線などによる ECU 間の通信途絶が想定される場合は安全機能により安全状態へ移行する．しかし Flooding による車載ネットワーク攻撃は複数の機能が同時に影響を受ける場合が想定され，安全機能の想定外の挙動をする可能性がある．また，セキュリティ機能の対応の結果，安全機能が想定しない故障モードを引き起こし，ハザードを引き起こす可能性もある．

したがって，機能安全とセキュリティそれぞれで想定している故障モードの内容と脅威内容を対比し，更に対処決定の際，対処内容の相互に与える影響を検討する手順の定義が必要である．

(2) 安全とセキュリティのリスク評価手法の相違

ISO 26262 では，アイテムが定義された次の段階で脅威分析とリスクアセスメントが実施される．ハザードが抽出されたのち，ハザードとその発生状況における過酷度，発生頻度，回復可能性からリスク軽減度の目標である ASIL を定める．

一方，JASO TP15002 おけるリスク評価は保護資産の特定，保護資産に対する脅威分析と，脅威の結果引き起こされる被害の評価で実施される．ところが，これら資産が，ISO 26262 のリスク評価段階で明確になっているとは限らない．例えば，ある資産は実装方式が決まった後に明らかになる．これは，ISO 26262 の機能安全コンセプト導出以降の作業に相当する．すなわち，安全とセキュリティで，プロセス上の同じタイミングでリスク評価が実施できないことを意味する．

(3) 安全とセキュリティの機能仕様導出方法の相違

ISO 26262 では，アイテム定義→ハザード・リスクアセスメント→機能安全コンセプト導出→技術安全要求導出→システム設計と段階が進むに従い，詳細化された各機能の故障に対応して安全機能が仕様化される．一方，セキュリティ機能設計では，データフローダイヤグラムによる抽象モデルの作成後，攻撃可能地点の決定，網羅的な脅威の抽出と，リスク評価実施後，特定された対応すべき脅威に対してセキュリティ機能が仕様化される．この詳細化の過程の相違により，要件の分析や仕様作成の各段階において安全機能と，セキュリティ機能との対応を取る事が複雑になる．

5　提案手法

本論文では，機能安全とセキュリティ開発を統合するモデルを設定する．モデルは機能安全・セキュリティ動作モデルと機能安全・セキュリティ要件定義統合プロセスから成る．

(1) 機能安全・セキュリティ動作モデル

本論文での機能安全・セキュリティ機能の動作モデルを図 4 に示す．

動作モデルは 6 要素で構成される．

①　車両本来機能：通常状態での車両機能部．制御機能（コントローラ）と車両のセンサ類やほかの ECU，運転車が相互に情報を交換して機能している．

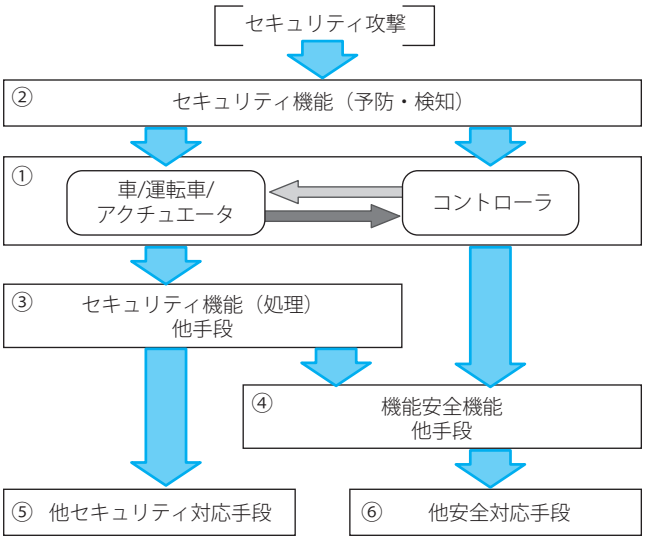

図 4　機能安全・セキュリティ動作モデル

②　セキュリティ機能（予防・検知）：車両本体機能及び安全機能をセキュリティ脅威から保護する．脅威の予防・検知機能を持つ．脅威発生の場合，セキュリティ処理機能を起動する．

③　セキュリティ機能（処理）セキュリティ脅威が発生した場合の処理機能．脅威に対する直接対処や，安全機能へ処理を移行し安全状態へ移行させる．対処困難な場合には，ほかのセキュリティ対抗手段（強制リセットなどを想定）へ移行する．

④　安全機能：車両本来機能の構成要素を監視し，故障の場合は，安全状態に移行する機能を持つ．もし安全機能で対処できない場合には，ほかの手段，例えばエンジンが停止しない場合，Kill スイッチでエンジンを強制停止させるなどの手段を取る．

⑤ ⑥ 他セキュリティ対応手段・他安全対応手段：セキュリティ機能や安全機能で対応できない事象への別手段による対応を行う．

通常状態では，コントローラと車両・ドライバーやアクチュエータは正常な相互作用を行なっている．セキュリティ脅威が発生した場合セキュリティ機能（処理）を起動し，必要な対処を行う．この対処は，セキュリティ侵害事象の中で，侵害事象の結果が安全機能で故障モードに類似しているために，枠組みで対処する事が妥当なものと，そうでないものに分割し，前者については安全機能を呼び出す事により，安全モードに動作を移行する．それ以外の事象については，セキュリティ機能内の対処もしくは他セキュリティ機能の対処とする．

この動作モデルは利点を持つ．

- 車両がセキュリティ攻撃を受けた際に，ハザード事象の発生を防ぐ為に安全状態に移行することが望ましい．このモデルではセキュリティ脅威発生と安全機能を関連付けており，脅威発生時の安全状態移行を実現する動作のモデル化している．
- 上の利点の実現のため安全機能とセキュリティ機能の関係を分離・単純化している（4 節，問題（1））．これにより，

相互の機能の対応を明確化することが可能となる．

- 安全機能とセキュリティ機能の対応を取る必要から，要件定義プロセスで脅威やハザード・リスクの詳細度で整合性が確保される．（4 節，問題（2）（3））．

(2) 機能安全・セキュリティ要件定義統合プロセス

この動作モデルに基づき，機能安全とセキュリティ機能の要件定義プロセスを定義する（図 5）．

このプロセスは，機能安全の要件定義プロセスとそれに並行するセキュリティ要件定義プロセスから成る．このプロセスでは，脅威，ハザード，リスクの詳細度を機能安全とセキュリティで整合的に取り扱う必要上，並行するプロセス間では，要件分析に使われる情報の詳細度は同程度でなければならない．そのために，a）セキュリティ脅威分析は機能安全の要件分析のレベルに合わせた詳細度とする．機能安全の要件分析が進み，その詳細化に合わせて脅威を記述する．すなわち，脅威は，脅威種別，対象及び脅威の明確になった段階で記述する．b）セキュリティ脅威により損なわれてはならないのは安全である．そのため，対処の徹底度は，安全のハザード分析とリスク分析の時点で導出される．しかし，対処すべき脅威が具体化されていないため，この時点ではリスク対処の基準を作るしかない．c）セキュリティ機能自身も安全機能の対象である．そのため，機能安全で求められるレベルでのプロセスで開発されなければならない．そのために ASIL レベルが導入される．d）実装要求になる辺りで攻撃がある程度具体化されるため，脅威分析とリスクスコアリングを実施する．このときに b）での脅威を利用する．

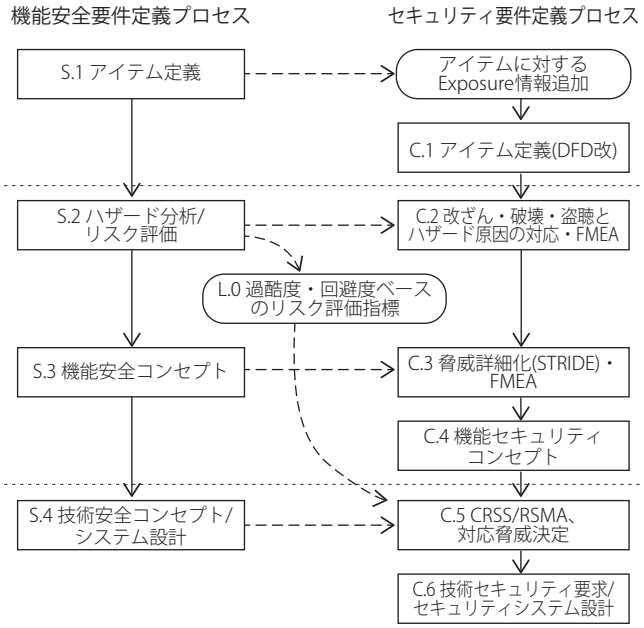

図５　機能安全・セキュリティ統合プロセス

以下，セキュリティ要件定義プロセスの各ステップを説明する．

5.1 拡張アイテム定義（図 5.C.1）

このプロセスでは，機能安全要件定義プロセスのアイテム定義（図 5 S.1）で定義されたアイテムを入力とする．プロセスの出力は，入力されたアイテムに，セキュリティ脅威の情報を追加した拡張アイテム定義である．車載セキュリティでは攻撃の開始地点は必ずしもアイテムに含まれない．例えば，車載ネットワーク上の機能上関係ない ECU からの攻撃が相当する．このような場合を含めて脅威を明示的に表記するために Exposure Control Point（ECP）を導入する（図 6）．

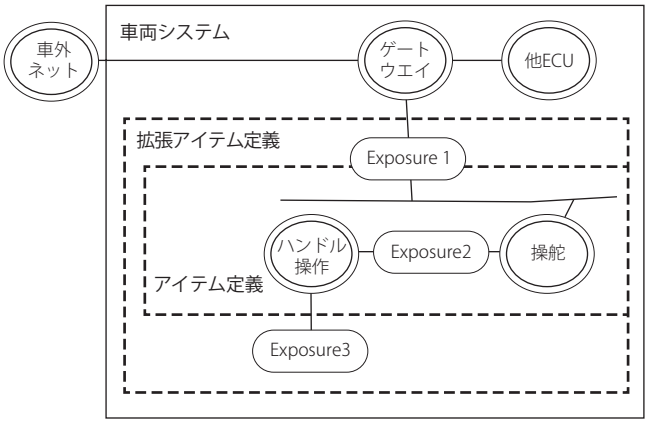

図６　拡張アイテム定義（丸四角が ECP）

この，ECP は情報セキュリティの脅威分析で Data Exposure Control Point として Fisher[12] により導入されたものを，データに対する脅威に加えて，サイドチャネル攻撃など物理的な脅威まで含むように概念拡張したものである．ECP はアイテムにおいて物理攻撃を含む脅威にさらされる点とそこで発生する脅威の組み合わせである．図 6 の場合，アイテム外のネットワーク，アイテム内部のネットワーク，操作機能への直接の脅威が ECP として表記されている．また，アイテム定義の段階の情報では，必ずしも脅威の具体化できないため抽象度の高い，改ざん / 破壊 / 開示の 3 つを脅威とする．このようにして，ECP が追加された拡張アイテム定義をプロセスの出力とする．

5.2 ハザードと脅威対応（図 5.C.2,L.0）

機能安全要件定義では，定義されたアイテムを元に，ハザードを導出し，その発生状況における過酷度，発生頻度，回避可能性から ASIL を導出する（図 5 S.2）．一方，本提案では，5.1 の拡張アイテム定義と機能安全でのハザード及びリスク分析の内容を入力とする．

初めに，各 ECP に割り当てた脅威からハザードを導出する．ハザードの導出には FMEA など帰納的手法を用いる．更に，機能安全ハザードとの対応付けを行う．もし，対応付けがない場合は，機能安全にハザードを追加し，脅威が原因のハザードに対する安全機能の要件が導出されるようにする．次に対応する機能安全ハザードの過酷度と回避可能性から，リスクスコアリングのパラメータ及び対処要否の境界値の決定を行う．ここでは具体的な数値及び決定方法は言及しない．また，セキュリティ機能の保護対象の機能の部品であると考え，保護対象機能の ASIL 値をセキュリティ機能の安全指標とする（図 5 L.0）．ここでの出力は，セキュリティを考慮したハザードが追加され詳細化された拡張アイテム定義，セキュリティ機能のリスク評価及び安全指標である．

5.3 脅威詳細化・機能セキュリティコンセプト（図 5.C.3,C.4）

ここでは，機能安全コンセプト（図 5 S.3）に対応する機能セキュリティコンセプトを導出する．この際，ECP の抽象的な脅威を詳細化する．機能安全コンセプト相当段階では，実装の前提となるアーキテクチャは定まっている．このアーキテクチャ及び拡張アイテム定義を入力とし，STRIDE 手法 [13] により脅威の詳細化を実施する．そして，先と同様に FMEA などの帰納的な手法により，新たなハザードの発生を確認する（図 5 C.3）．この場合も，既存の機能安全要件定義プロセスで分析したハザードにマッピングすることを原則とする．このことにより，セキュリティ事象とハザードに対応した安全状態を関連付ける．更に詳細化された脅威から，それぞれの脅威に対応したセキュリティ機能安全要求を導出する（図 5 C.4）．これらを前提としたアーキテクチャに割り当てた機能セキュリティコンセプトを出力とする．

5.4 リスク評価と対応，技術セキュリティ要求導出（図 5.C.5,6）

ここでは，技術安全要求に相当するセキュリティ要件の導出を行う．この段階では，技術安全要求導出段階で利用されるシステム設計の情報を元に導出された脅威を更に詳細化すると同時に，その対抗策を導出する．この詳細化された脅威に対してリスクスコアリングを行う．リスク対応を決める閾値やこれらで利用されるパラメータ値は，５．３で定められた値（図 5 L.0）を用いて行う．これにより，システム設計に対する具体的な脅威に対して，安全の観点から対処すべき脅威を選択する．最後に対処すべき脅威に対してセキュリティ機能を決定する．リスク評価の結果，対処の必要な脅威に対する直接防御（予防）及び攻撃検知，セキュリティ機能の通知と内部の安全機能と関連付けた処理の観点からのセキュリティ機能の実装要求（技術セキュリティ要求）と対応するセキュリティシステム設計を行う．

この段階で，ハザード，機能安全要求，技術安全要求，脅威，機能セキュリティコンセプト，技術セキュリティ要求の関連付けが完了する．

6 仮想的な開発ターゲットへの適用

ここでは仮想的な開発ターゲットを想定し，提案手法の適用検証を行う．ここでは，ハンドルと操舵装置の間を車載 LAN で接続した Fly-by-Wire 方式の操舵装置を例として検討する（図 6）．

6.1 拡張アイテム定義（図５S.1,C.1）

図 7 に対象システムを示す．ここでは，ハンドル操作機能と操舵機能は専用線通信で結ばれているが，速度はセンサなど外部との通信から得られる．

セキュリティ要件定義のアイテム定義では，セキュリティ脅威にさらされている部分を表現するため，データフローダイヤグラムに ECP を追加する（図８）．ECP の内容は，対象となるデータ（ここでは速度データ）や処理に対する破壊 / 改ざんとする．物理的制約条件として，通信 1 の通信路，操舵部分とハンドル操作部への直接攻撃は困難とする．この場合の ECP はセンサとの通信部分で暴露されている内容の破壊 / 改ざんとする．

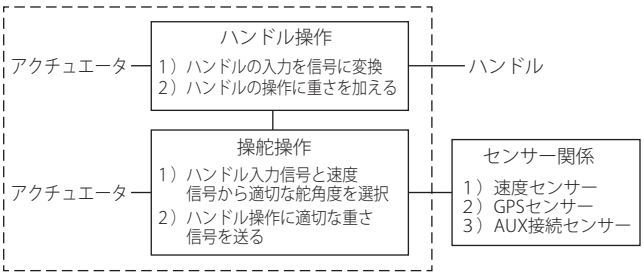

図７　対象アイテム定義（破線内）

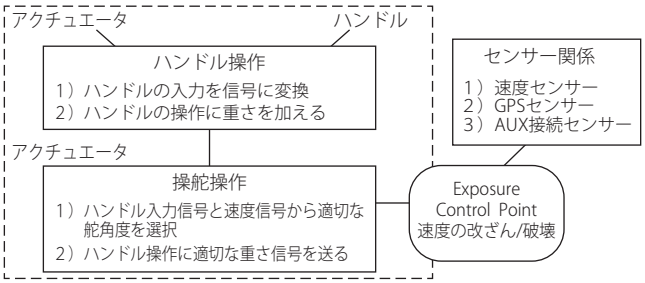

図８　拡張アイテム定義（破線内）

6.2 ハザードと脅威対応（図５S.2,L0）

次に，機能安全要件定義プロセスのハザード分析，リスク評価に対応するセキュリティ定義プロセスでの作業を行う．ここでは上のシステムで想定されるハザードのうち，速度に対応するハンドルが軽くなる場合を想定する．セキュリティ観点では通信路２には ECP としてデータ破壊及び改ざんの脅威が想定できる（表１）．

このハザードに対する過酷度及び回避可能性は機能安全側での HAZOP などを行って定められる．それに従い，後に使用されるリスクスコアリング手法でのリスク対処必要とされる閾値を定める．この決定方法はここでは議論しない．

表１　ハザード / ハザード要因と ECP

機能安全要件定義		セキュリティ要件定義
ハザード事象	ハザード要因	ECP
ハンドルの補助トルクが過大にかかって軽く動作し，ハンドルを大きく切って事故を起こす．	通信路がエラーを起こし，ハンドルと速度が連動しなくなる	破壊
		改ざん

6.3 脅威詳細化・機能セキュリティコンセプト（図 5．S3,C.3,4）

機能安全コンセプト相当段階では，ハザード要因に対して適切な機能安全コンセプトが導出されている．それに対応して脅威を割り付ける（表 2）． このとき，ECP を STRIDE 手法で詳細化する．表２では通信データ改ざんは，正常な場合と改ざんに

よる通信エラーデータが通信路上に流され，機能安全要求の通信エラー監視機能では対応できないため，空欄となっている．

表２　安全機能と脅威

機能安全要件定義		セキュリティ要件定義	
機能安全要求	安全機能	STIRDE による詳細化	ECP
通信２のエラーが多い場合には，操舵操作から出す重さ信号を最大に設定する．	通信状態を直接監視機能に入力・通信路異常を監視し，異常ならば重さ信号最大化	通信路上で，中間者によるデータ破壊	破壊
-	-	不正機器による偽データまたはデータ改ざん	改ざん

空欄部に対する機能安全要求を導出するため，FMEA でハザードを導出し，HAZOP を行う．ここではデータの改ざんによりハンドルが異常に軽くなり操作を誤ることをハザード事象とする．この場合，対策機能は正しい機器が発信したこと（発信元改ざん）及びそれが改ざんされていないこと（通信路改ざん）を保証する対策が必要となる．ここではこの２つを確認できるメッセージ認証機能（MAC 認証）を用いて対策機能とすることを想定する（表３）．

表３　機能セキュリティコンセプトと脅威（FMEA 後）

機能安全要件定義		セキュリティ要件定義	
機能安全要求	安全機能・機能セキュリティコンセプト	STIRDE による詳細化	ECP
通信２のエラーが多い場合には，操舵操作から出す重さ信号を最大に設定する．	通信状態を直接監視機能に入力・通信路異常を監視し，異常時は重さ信号最大化	通信路上で，中間者によるデータ破壊	通信データ破壊
正規と区別できない⇒メッセージ改ざん検出機能で検出したら重さ信号最大	MAC 認証（HMAC による MAC・鍵とシリアル値同期）	不正機器による偽データまたはデータ改ざん	通信データ改ざん

6.4　リスク評価と対応，技術セキュリティ要求導出（図 5.C.5,6）

前節で導出されたセキュリティに対する機能要求を元に，実装要件である技術セキュリティ要求の導出を行う．技術安全要求仕様相当段階では，機能安全コンセプトに対して，その実装要求（技術安全要求）が導出される．システム設計情報などを利用してセキュリティ脅威を更に詳細化し，これらの脅威に対して，JASO TP15002 に従い CRSS によるスコアリングを実施する（表 4）．

表４　詳細脅威とリスクスコアリング例

脅威 ID	対象に対する脅威	STRIDE による詳細化	スコア（判定）
T1	通信路上の設置デバイスで電気的に破壊する	通信路上データの破壊	8（要）
T2	中継デバイス（GW など）を改ざん / 破壊する		2（対処不用）
T3	送信側デバイスのアプリケーションを改ざん，不正メッセージを送出	システム改ざんによるデータ改ざん	2（対処不用））
T4	送信側デバイスを不正に入れ替え，不正メッセージ送出		6（要）
T5	通信路情で設置したデバイスでメッセージ入れ替え	データ改ざん	6（要）

この結果に対して，先に機能安全のハザード分析時に得られている評価指標（図 5 L.0）と比較し，スコアリング結果から対応すべき脅威を選別し，セキュリティ機能を検出予防と検出後措置の構成で設計する．表５では，表４で示された脅威に対する対処策を示している．ここでは，対処必要とされた脅威に対する対応策の導出手順を述べる．まず，T1 では，脅威の結果，現れるエラー通信の増加を検知指標とする．エラー通信数がある境界値を越えれば（検出１），表３で定めた検出後措置である，重さ信号送出（対処１）を実施する．次に T4,T5 では，不正デバイスからの送信検出に MAC 認証を採用する（検出２）．脅威が検出された場合，表３の対処方法である重さ信号送出（対処２）を実施する．

表５　技術安全要求と技術セキュリティ要求

技術安全要求と技術セキュリティ要求		セキュリティ ID	セキュリティ 対応
単位時間当たりの通信のエラー通信数を取得することで通信エラーを判定し，閾値を超えたときにハンドル重さを最大とする．	（検出 1）通信２の状態を直接監視機能に入力・エラー通信数をカウント．境界値より多ければ（対処 1）正規出力を停止し，監視機能から重さ信号送出	T1	要
		T2	非
デバイス側で対処		T3	非
MAC 認証を通らないメッセージを検出し，閾値を超えたら重さ信号最大とする	（検出 2）送信デバイスから送られてきたメッセージの MAC 値を検証し，（対処 2）不正データがあれば，対処 1 を実施	T4	要
		T5	要

これらの対策を図 4 のモデル図にマッピングしたものが図 9 である．セキュリティ脅威は予防検知の部分で検出される．機能安全設計で対処可能なセキュリティ脅威は，そのまま安全機能で対処される．安全機能で対処できないセキュリティ脅威は新たに実装されるセキュリティ機能（処理）で対処する．

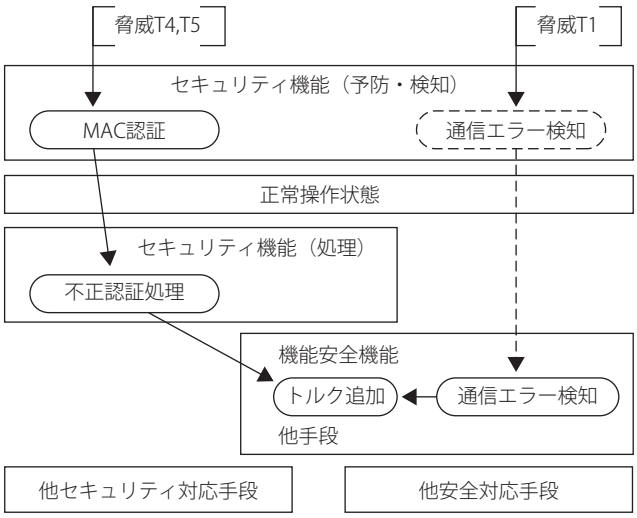

図９　セキュリティ対応対象システム

最終的に，セキュリティ攻撃の発生時に，機能安全要件定義で定義された安全状態への移行を設計に組み込み，発生が懸念されるハザードに対処する．

7　考察

本提案では，機能安全とセキュリティの開発を統合するため，機能安全での要件定義対象であるアイテムに ECP を導入し，機能安全と同じ対象でのセキュリティ要件定義を可能にした．また，脅威及び，セキュリティ機能の導出は，ISO 26262 で定義されている帰納的・演繹的手法を用いた対処抜け防止手順を流用し，セキュリティ対応手法の導入を最小限にとどめ，新たに発生するコストを抑えている．

本提案のリスク評価は，STRIDE 手法及び CRSS/RSMA を利用する．STRIDE は情報システムの分析では標準的な手法の一つであり，今回の分析も情報の動きに着目した分析を行うため，適合性が高いと考えられる．また，CRSS は情報処理システムの実績ある脆弱性評価方法である CVSS を，RSMA は情報セキュリティ管理とリスク管理プロセスにかかる作業を規格化したガイドラインで ISO/IEC 27005[14] での攻撃容易性と被害の概念を利用したリスクレベル決定表を用いており一般性があると考えられる．しかし，これらについては，結果の網羅性と実用性担保の観点から，更に検討が必要と考える．

次に，本研究と先行研究 [9] の比較を行う．本研究では，ECP から予想される被害からリスクスコアリングの基準を導出，システム設計段階で脅威の詳細度を高め，更にシステム設計情報と併せてリスクスコアリングを行う．先の基準に従い，対策実施するものと，残存脅威とするものの２つに分類する．これにより，対処しない詳細度脅威を管理できる一方，詳細度の高い脅威を対象として検討するため検討内容の詳細度が高く，対策の有効性や漏れの検証に有利である．更に，ステアリングシステムに対する適用結果を比較する．先行研究 [9] のセキュリティ対策は Trustzone の境界面の HSI に対する，ハザード分析段階でのリスク評価に基づきキーワードレベルの対策を定める．例を表６に示す．

表６　先行研究での対策例

信号名	ASIL	リスク／対策キーワード
車両速度シグナル	B/2	2／異常挙動検出，侵入検知，デバイス認証

表５と比較すると，同等ではあるが記述内容は本研究がより詳細である．また，本研究では，セキュリティ攻撃発生時の安全状態移行も対策化（図９）している．そのため，本提案の要件分析は，脅威発生時の安全動作も含む，より安全性の高いものである．

8　まとめ

本論文では，安全機能とセキュリティ機能の要件定義の手法を検討，提案した．本論文が，機能安全とセキュリティの統合に関連する議論の一助となれば幸いである．また，今後は実プロジェクトへの適用などを通じて有効性の検証と手法の洗練化を図りたい．

【参考文献】

[1] ISO 26262：2011. Road vehicles — Functional Safety —
[2] https://ics-cert.us-cert.gov/Year-Review-2013
[3] https://www.isa.org/isa99/
[4] SAE J3061：2016. Surface Vehicle Recommended Practice
[5] https://www.evita-project.com
[6] M.Steiner, et. al., Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. In SAFECOMP 2013
[7] D.Ward, et. al., Threat Analysis and Risk Assessment in Automotive Cyber Security, SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 6（2）:507–513, 2013
[8] K.Schmidt, et.al., Adapted Development Process for Security in Networked Automotive Systems," SAE Int. J. Passeng. Cars – Electron. Electr. Syst. 7（2）:516–526, 2014
[9] G. Macher, et.al., Integrated Safety and Security Development in the Automotive Domain, SAE Technical Paper 2017-01-1661, 2017
[10] G. Macher, et.al., SAHARA: a Security-Aware Hazard and Risk Analysis Method, in DATE, 2014
[11] 公益社団法人自動車技術会 :JASO テクニカルペーパー 自動車 - 情報セキュリティ分析ガイド , JASO TP15002, 2015.
[12] R. Baskerville, Information systems security design methods: implications for information systems development, ACM Computing Surveys, vol.25 no.4, pp.375-414, Dec. 1993
[13] A.Shostack, threat modeling. Wiley, 2014
[14] ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management