2018 年度　博士論文

セキュリティ対策を組み入れた
車載システム開発手法の研究

兵庫県立大学　大学院
応用情報科学研究科　応用情報科学専攻

ID10I204

左近　透

(2018 年 6 月 4 日　提出)
(指導教員　中本 幸一 教授)

要 約

自動車のエレクトロニクス化は 1960 年代に始まる．1970 年には，エンジン制御に，マイクロコンピュータを内蔵した Electric Control Unit (ECU) が導入された．今日では，レーダや画像処理と車両制御などを組み合わせた車線逸脱防止や自動駐車などの先進運転支援システム (ADAS) の導入などにより，車載エレクトロニクスは複雑化の一歩を辿っている．さらに，今後，車両とインフラストラクチャ側や車両間の通信により，さらなる安全性，利便性の向上が期待されている．

車両開発において最も重視されるものは，安全である．この安全とは，車両を構成する部品に不具合や故障が発生しても重大な損失に繋がらないことである．安全を実現するための考え方は，大きく本質安全と機能安全に分類できる．本質安全では，危害を及ぼす原因そのものを低減または除去することにより安全を実現する．本質安全による安全実現の具体例には，立体交差による交差点事故の除去である．一方，機能安全とは，「安全を損なうような状況が発生した場合に，それを軽減，防止する機能的な工夫（安全機能）により損失の発生を回避すること」である．車両開発での安全は機能安全設計で実現する．その設計開発は国際規格 ISO 26262:2011 に準拠して行われる．

一方，近年，車両に対する新たな脅威としてサイバー攻撃が指摘されている．これは，外部との通信を通じた車載電子システムのネットワークや電子機器に対する不正な干渉や改ざんの可能性が研究論文などでしめされたことを契機に認識されるようになった．さらに，近年，実現化への期待が高まる自動運転システムにおいても，システム全体が製造者の意図した通りのものであることや，センサー情報を含めた記録が完全かつ詐称不可能であることが，事故時の原因究明，解析において極めて重要性と認識されている．これらの要件もまた，セキュリティ技術の適用により実現されることが期待されている．

自動車において，サイバーセキュリティは電気電子システムにおける　1）対象 (電子制御ユニット，ネットワーク，OS，プロトコル，アプリケーションソフトウェア等)，2）開発手法 (技法，プロセス等)，3）開発管理 (情報システム，情報管理等) の側面がある．欧米を中心に車両サイバーセキュリティに関する開発プロセスの提案や，サイバーセキュリティ技術そのものの研究や提案が進められている．しかし，車載システムのサイバーセ

キュリティ開発では，機能安全とサイバーセキュリティ開発を統合して取り扱う必要がある．また，ISO 26262 に準拠した車両の開発スタイルと IT システムのそれとの相違などにより IT システムでのサイバーセキュリティ対策を適用することは困難である．

本研究では，セキュリティ対策を組み入れた車載システム開発手法の研究を行った．具体的には，車両のセキュリティと安全の統合を目指すため，ISO 26262 を中心概念とする機能安全開発とサイバーセキュリティ開発を整合的に行うための開発プロセスの研究，および開発管理において異常検知技術を用いた情報システムの不正利用の検出の研究を行った．これらの研究は重要であるにも関わらず，研究がまだ端緒についたばかりである．

機能安全開発とサイバーセキュリティ開発の統合の際，機能安全開発とサイバーセキュリティ開発のいずれからも整合性が取れるように開発対象となる車両機能の範囲を定義する必要がある．本研究では，高度な車両機能が増加している現在の傾向も踏まえた，機能安全とサイバーセキュリティ開発に対応した開発対象となる車両機能定義に関する手法の研究および，定義された車両機能にたいするセキュリティ対策のデザイン手法の開発を行なった．

まず，開発プロセスの研究では，機能安全とサイバーセキュリティとの整合を測るため，機能安全・セキュリティ動作モデルを開発，本モデルに従った処理を開発する手法として，ISO 26262 で用いられている機能的・演繹的な検証方法を利用することで機能安全機能とサイバーセキュリティ機能との整合を実現する．次に，本開発プロセスでは，開発対象の範囲定義とその外界との境界の決定が極めて重要である．そのため，境界の決定方法として，従来の機能インターフェースに基づく方法に変わって，情報や資源の共有に着目した方法を提案した．この手法では，直接の機能関係に加えて，資源共有などを通じた間接的な影響も導出することが可能となり，サイバー攻撃の対策の網羅性を高めることが可能となった．最後に，車載システムに対する脆弱性評価を容易化するために定義された開発対象に対するセキュリティデザイン手法として，開発対象の関連性を元に機能を分類し，分類された機能グループごとに保持すべきセキュリティ属性 (ポリシー) を定義する手法を開発した．この手法では，複雑化した開発対象を構成する各機能に対するセキュリティ対策を統合的に行うことができる．また，セキュリティ属性により，個別機能に対する脅威が整理されることによる脆弱性や残存リスクアセスメントを実施する上での利点についても検討した．

近年，情報技術に対する社会の依存度は増加する一方である．それと軌を一にして，社会の基盤である情報システムに対する攻撃，いわゆるサイバー攻撃や組織内の人的脅威などによる，障害や情報漏洩が増大している．それらに対抗するためのサイバーセキュリティに関連した技術や開発手法も高度化が進んでいる．しかし，一方で，既存技術や管理体制に対する適合性，人員の教育や費用を含めたコストなど導入の容易さを持たない限り，新技術の導入に遅れが発生したり，場合によっては導入が見送られ，そのためにサイバー攻撃による損害が発生するリスクが残存する危険性がある．

車載電子システムの開発では多くのステークホルダーが絡むため，機密情報管理が重要である．この観点から情報管理の研究では，異常検知技術を用いた情報システムの不正利用を検出の手法を研究した．近年，情報漏洩対策として，オフィス環境では，ユーザの情報システムの操作を記録することが一般化している．しかし，その主目的は社員に対する抑止および情報漏洩インシデントが発生してからのちの対策である．また，ユーザの操作を記録するに際して，データ量の問題から，ウィンドウシステムの操作履歴など操作内容の一部にその内容が限定されている．従来のユーザ操作記録から不正検出を検出する研究では，コマンドラインでの操作記録を利用しており，現状のウィンドウシステムの操作には直接応用できない．また，従来のウィンドウ操作履歴を使う研究では操作頻度や前後相関を元に異常検知を検討しており十分な精度が得られていなかった．この研究では，利用者のコンピュータの操作時に，利用者ごとに特徴的な操作系列の抽出方法を開発し，その分析に基づく異常検知の技術を開発した．事務所でのユーザの操作記録を利用して方式検証を行い，8 割から 9 割の正答率と従来方式と比較して大幅に良好な結果を得た．

今後の課題として，一つは，本研究で開発した機能安全・サイバーセキュリティを統合した開発プロセスを具体的に実現する手法の研究開発を進める必要がある．今回の研究では，機能安全・サイバーセキュリティ統合開発プロセスおよび当該プロセスにおける開発プロセスの定義ならびに定義された機能に対するセキュリティデザイン手法を開発した．しかし，実際に車両機能の開発を進めるためには，開発体制などを含めた車載電気システムの開発に適合性の高い脅威分析手法や，リスクスコアリング手法についてさらなる研究を進める必要がある．また，これらの知見を，現在，制定活動が進められている，車両開発の国際規格である ISO/SAE 21434 に対して日本発の知見として反映させることを試みたい．

今後，サイバーセキュリティ対策実施の要求は広範に求められる．しかし，既存システムに対する技術の適合性が低ければ，適用コストが膨大となる．結果，無適用状態の長期化や形骸化を生み，サイバー攻撃による損失リスクが残存する．このような事態を回避する面からも，セキュリティの要素技術に加えて，適用対象の基本的な性質に基づく適用手段や管理運用方法の研究開発は，今後，重要性を増すと考える．

目次

図目次

表目次

第 1 章

序論

1.1　本論文の動機・寄与および構成

ここでは，本研究の動機，寄与，および構成を示す．

1.1.1　動機

本研究は，自動車の電子システムの開発を対象としたサイバーセキュリティ技術の適用に関するものである．自動車のエレクトロニクス化は，1960 年台にエンジンの交流発電機への半導体の導入に始まる．つづいて，エンジン点火装置にパワートランジスタが採用され，エンジンスターターや複雑なエンジンにおける点火装置などに適用範囲が広がっていった．つづいて 1970 年台に入ると，エレクトロニクス化は急激に進展した．これは，1970 年に米国で制定された大気汚染防止法 (マスキー法) の対応が契機となっている．これに対応するために，マイクロコントローラを用いた Electric Control Unit (ECU) によるエンジン制御法が開発された．その後，「自動車の安全・快適・環境性能および情報化」に対応するため，ECU およびそこで動作するソフトウェアによるエレクトロニクス化が高度化している．特に近年では，自動駐車システムや車線維持システムなど従来単独で動作していた機能を統合して動作させる機能や，テレマティクスサービスなどによる地図，道路状況や最適経路情報の提供，ロードプライシングなどが実用化されている．このような高度な電子制御を実現するための電子制御の進展は，今や車全体が電子制御，言い換えればソフトウェア制御されていると言われるまで進んでいる．

車載電子システムの開発は，個別の電子システムとして開発されるのではなく，車両全体の機能との関連付けに基づいて開発される．特に，車が満たすべき最優先事項は安全

の実現である．特に，車の部品の一部の故障などにより制御が失われ，結果として事故が発生する事態は，開発側として避けなければならない．そのため，車の機能安全というアプローチで安全性能が実現されている．機能安全とは，不具合や故障，異常動作が発生した場合，それを検知し，速やかに操作者が制御可能な状態に移行する機能を追加することにより重大な事故につながることを防ぐアプローチである．現在は，電子制御系において機能安全を実現する開発プロセスとして，国際標準 ISO 26262 があり，国内外の車両の電子制御システムの開発に適用されている．

この ISO 26262 で表されるような車載電子システムの開発は，安全機能を実現するために，車両機能の企画段階から要件定義，設計開発から工場での生産に関わる部分まで綿密な連携を実現するために定義されたプロセスに従って行われている．このプロセスは，車を組み立てる車メーカーや車載システムを構築する Tier-1 とよばれるシステムサプライヤ，個別の部品を構築する部品サプライヤーなどにわたる分散した開発をサポートするため，プロセス間の入出力にくわえて，要件定義，変更管理などの開発に関わる補助的な管理作業までも含んで体系化され，関連する各企業において実際に運用されている．

一方，近年では，車の電子制御および情報化の進展の結果，サイバーセキュリティの要素も必要となっている．これは，2000 年台に入って，車載電子システムで使用されているネットワーク・プロトコルの脆弱性の指摘に始まり，BlackHat などのセキュリティ・カンファレンスや学会・国際会議でのデモンストレーションなどにより，その認識が一般化した．車両のサイバーセキュリティ対策で，最も重要とされるものが，車両の安全を脅かすサイバーセキュリティ攻撃に対する対抗策である．しかし，車両のサイバーセキュリティを実現するに対して，技術だけの問題では解決しない．特に，先に述べた，綿密に構築された開発プロセス全体における実現方法の検討が重要である．

自動車において，サイバーセキュリティは電気電子システムにおける　1）対象 (電子制御ユニット，ネットワーク，OS，プロトコル，アプリケーションソフトウェア等)，2) 開発手法 (技法，プロセス等)，3）開発管理 (情報システム，情報管理等) の側面がある．

1）の個別の対象は研究開発が進められている．一方、2)，3）においては特に安全の実現からは以下の問題がある．

- 情報システムにおけるサイバーセキュリティ対策は，基本的にサーバー，端末，ネットワークなどに既知のアーキテクチャが採用されており，脆弱性や攻撃手法につ

いても公開データベースなどで共有されている．一方，自動車の開発は，車メーカーである Original Equipment Manufacturing(OEM)，システムサプライヤである Tier 1，部品ベンダーである Tier 2 並びにチップやセンサなどのパーツベンダやソフトウェアコンポーネントの開発元などの Tier3 もしくはベンダをまたがって分散して進められる．また，通信部分を除きアーキテクチャや実装は個別となっている．そのため，開発対象ごとに個別に対策を検討する必要がある．また，車両開発メーカーのみが，その保有する情報から車両のリスクアセスメントを実施することができる．一方，攻撃の直接対象である部品の開発メーカーは，部品がサイバーセキュリティ攻撃を受けた場合の，車両挙動に対するリスクは，関連する車両機能の情報をもたないためアセスメントできない．

- 逆に機能安全のアプローチをセキュリティに適用することも困難である．機能安全は，部品の故障であり，二重化などによりその部品を利用する車両機能における障害発生確率を必要な水準まで下げることを目標とする．一方，セキュリティの場合，脆弱性の発見およびその攻撃手法が発見された場合には，障害の発生は再現可能である．また，情報システムに対するサイバーセキュリティ攻撃のように攻撃用ツールなどが開発され配布された場合には攻撃は極めて容易となる．
- 車載電子システムの開発管理において多数のステイクホルダーが絡む．その開発の中で，開発対象物に対する機密性を保持しなければならない．しかし，かつて漏洩事例があったように機密情報の漏洩は発生する．

1.1.2 本研究の寄与

本研究の最大の特徴は，機能安全とサーバーセキュリティの統合モデルを提案し，それに準拠した形で機能安全における開発手法をベースとした機能安全・セキュリティの統合開発プロセスを提案したことにある．本プロセスの特徴は次の 4 点にまとめられる．

1. 機能安全における動作モデルを拡張した機能安全・サイバーセキュリティ動作モデルを提案している．
2. サイバーセキュリティリスクアセスメントが可能なのは OEM であり，実際の攻撃に対する対抗策を具体的に検討するのが Tier 1，Tier 2，Tier 3 であることを考慮

し，サイバーセキュリティリスクアセスメントの結果をインデックス化し，そのインデックスに準拠して部品メーカーは開発している部品に対するリスクのスコアを評価，それに基づき対策を取捨する．このことで，OEM と Tier 1，Tier 2，Tier 3 間での過度の情報共有を避ける．

3. ISO 26262 で利用されている帰納・演繹的な検証方法を用いて，サイバーセキュリティ攻撃により発生する事象を機能安全事象に統合する．統合した際には，全てのサイバーセキュリティ事象も機能安全的な手法で制御可能な状態へ移行する機能を開発する．そのため，サイバーセキュリティ攻撃においても，制御可能性は維持される．
4. 開発プロセスを機能安全側の開発プロセスを基本としている．そのため，従来の開発プロセスを運用している企業における受容性を考慮している．

これらの研究は重要であるにも関わらず，研究がまだ端緒についたばかりである．

また，サイバーセキュリティ攻撃は，従来，機能安全で考えられていた開発対象の範囲の外部からも攻撃が可能である．しかし，機能安全機能開発・サイバーセキュリティ開発を統一的に行うためには，開発対象は同一でなければならない．また，機能の複雑化にも対応しなければならない．そのため，従来の機能安全開発と整合可能な開発対象の定義手法を検討した．また，IT で用いられる，データフローをベースにしてそれぞれに対してセキュリティ対策を立てる方式では，単一の ECU が複数の機能を持つ車両システムの特性上，極めて煩雑化する．そのため，ECU 機能をグループ化し，それらの間で満たされるべきセキュリティルールをポリシーとして定め，その階層でセキュリティ対策を記述する方法もあわせて検討した．

情報管理の研究では，機密情報管理の観点から異常検知技術を用いた情報システムの不正利用を検出の手法を研究した．開発やサポートやサービス運用の際に，担当する要員については内部犯行の可能性がある．これらの早期発見の可能性を検討するため，情報システムユーザの異常行動の検知技術の検討を行い，従来手法にくらべて良好な結果を得た．これは，ユーザの操作手順が作業内容によりパターン化されることに着目し，頻出操作手順を元にした分析を行うことにより，従来のここの操作の順番を分析する手法に比べて，8 割から 9 割の正答率を実現した．

1.1.3 本論文のアウトライン

本論文は，2 部で構成されている．第一部は 2 章から 4 章までに相当する．ここでは，車載電子制御システムの機能安全開発とサイバーセキュリティ開発との統合プロセスを取り扱う．最初に，開発プロセスについて議論する．そこでは，機能安全開発の国際標準である ISO 26262 を基礎に，サイバーセキュリティに関連するリスクアセスメント，要件定義，システムデザインを取り込んだ開発プロセスを示す．まず，OEM，Tier 1，Tier 2，Tier 3 ごとに保有する情報の相違に着目した開発プロセスフローを示す．このフローでは，車両全体に及ぼす影響を判定可能な OEM が機能異常に対するリスクスコアリング基準を決定する．このスコアリング基準に対応して，Tier 1，Tier 2，Tier 3 は個別のシステムや部品の脆弱性に対して対応するべきものを選択する．本研究では，Tier 1，Tier 2，Tier 3 は，JASA TP 15002[1] などのスコアリング手法を用いるものとしている．実際のサイバー攻撃に対する具体的な対抗策は，Tier 1，Tier 2，Tier 3 の持つ情報がなければ対抗策は決定できない．このように分散開発における各参加者の持つ情報量に応じて，リスク対応を行う．また，本研究では，機能安全・サイバーセキュリティ統合動作モデルを開発した．このモデルは，サイバーセキュリティによって起こる事象を，機能安全で故障やシステム異常により発生する事象を統合して扱うモデルである．このモデルに適合した形でシステムデザインを行うために，サイバーセキュリティで起こる事象について，帰納・演繹的な検証方法を用いて，サイバーセキュリティ攻撃により発生する事象を機能安全事象に統合する手法を示す (2 章).

次に，開発対象の定義方法について議論する．車両の開発での開発対象は，車両レベルでの機能をもって単位とする．しかし，近年の車両機能の複雑化により単一の部品が複数の機能で使われたり，サイバー攻撃のように車両レベルでの機能の関連外からの攻撃も想定される．従来は，部品間のコミニュケーションベースでの開発対象定義を行っていた．しかし，この手法では開発対象の複雑度が上がるにつれて記述の複雑度が急増する．これを避けるために，共有されている情報で，部品間の関係を表す手法の導入を提案した．この手法を導入することで，部品間の関係の記述を簡潔にすると同時に，コミュニケーションベースでの記述では記述しにくい間接的な影響も記述できることを示す (3 章).

Tier 1，Tier 2，Tier 3 は，このように定義された開発対象に対して，サイバー攻撃に

たいする脆弱性を評価する．しかし，一般の IT システムの開発で行われるデータフローを基礎にした対策設計は，単一の部品や機能が異なる保護水準が要求される車両システムでは整合的に実施するのは難易度が高い．また，脆弱性評価に際しても，対象に対する攻撃手法が特定されないため，膨大な攻撃手法に対応した脆弱性を検討しなければならず，未対応の残存脆弱性のリスクを排除するのは困難である．そこで，開発対象の関連性を元に機能を分類し，分類された機能グループごとに保持すべきセキュリティ属性 (ポリシー) を定義する手法を開発した．この手法では，複雑化した開発対象を構成する各機能に対するセキュリティ対策を統合的に行うことができる．また，セキュリティ属性により，個別機能に対する脅威が整理されることによる脆弱性や残存リスクアセスメントを実施する上での利点についても検討した (4 章).

第二部は，異常検知技術を用いた情報システムの不正利用を検出の手法を示す．内部犯行によるセキュリティ被害は，企業や組織にとって重大な損失を生む可能性が高い．現在，市場で普及しているコンピュータシステムはマイクロソフト社の製品に代表されるウィンドウシステムが主流である．現在主流のセキュリティアプライアンス製品でのユーザ操作の記録は，操作対象であるウィンドウのタイトルが記録されたアクティブウィンドウログが主流である．このアクティブウィンドウログを用いてユーザの異常行動を検出するために，本研究では，前後関係に限定されない，ユーザごとに特徴的な操作系列の抽出方法を開発し，その分析に基づく異常検知の技術を開発した．事務所でのユーザの操作記録を利用して方式検証を行い，8 割から 9 割の正答率と従来方式と比較して大幅に良好な結果を得た．第二部は 5 章が相当する．

なお、本博士論文の各章の基礎となる論文は以下の学術誌，国際会議で発表されたもの (予定を含む) である．

2 章: 左近透，中本幸一，“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”，SEC journal，vol. 14, no. 1, pp. 2-9，2018 年 8 月．

3 章: Toru Sakon and Yukikazu Nakamoto, Toward Safety and Security development by identifying interfaces of automotive functions, Proc. of the Seventh International Conference on Advances in Vehicular Systems, Technologies and Applications, IARIA, June 2018.

4 章: Toru Sakon and Yukikazu Nakamoto, Structured Policy-based Design Method for Cybersecurity of Automotive E/E System, Proc. of the 15th IEEE International Conference on Advanced and Trusted Computing (accepted), Oct. 2018. ©IEEE

5 章: 左近透，中本幸一，“ユーザ操作の繰り返しを考慮したウィンドウログの解析によるユーザの識別手法”，電子情報通信学会論和文論文誌 D, vol. J100-D, no.2, pp.171-179, 2017 年 2 月．©電子情報通信学会

第 2 章

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

2.1 車載システム開発に関連する標準

現代社会において，自動車は，移動手段に加えて，物流や地域の生活基盤などのインフラストラクチャの役割をも果たしている．そして，その機能は，環境性，安全性，快適性，効率化などの社会的な要請を受けて変化，拡大しつつある．この自動車の機能の変化・拡大を支えているのが車両機能の電子制御である．車両の電子制御は，車両に配置された電子制御ユニット (Electronic Control Unit，以下 ECU と称す) と ECU 間の通信により実現される．ECU は，マイクロプロセッサなどを実装したハードウエアおよび，そこで動作するソフトウェアで構成される．

現在も進行している車両機能の変化・拡大に応じて，ECU の数および，それを制御するプログラムの量は増大を続けている．2008 年に経済産業省が実施した「第一回高度情報化社会における情報システム・ソフトウェアの信頼性およびセキュリティに関する研究会」では，車載 Electrical and Electronic(E&E) システムのソフトウェア量は 2015 年以降は一億行を超える規模と推定されている．このような大規模開発におけるソフトウェア品質を確保するためには，要件定義を含めて工学的手法に則ったシステム開発手法が必要となる．

一方，自動車の開発は，車メーカーである OEM，システムサプライヤである Tier 1，部品ベンダーである Tier 2 並びにチップやセンサなどのパーツベンダやソフトウェアコ

ンポーネントの開発元などの Tier3 もしくはベンダをまたがって分散して進められる．その分散の範囲は一国の範囲に限定されず，また単一のベンダーが複数の OEM に製品を提供することも常に発生している．製品の品質ならびに車ビジネスに参画している各参加者間での開発における情報交換の共通の言語となる標準が必要である．現在，車載 E&E システムの開発において国際標準の適用は必須となっている．

本研究では，車の安全機能を実現するための開発プロセスを定めた国際標準規格を基本として，車のサイバーセキュリティ機能を整合的に定義する手法を開発した．車に対するサイバーセキュリティ攻撃は，可能性検討レベルでの研究に始まり，近年では実車の持つ脆弱性をついたサイバー攻撃の成功事例も発表されている．これに対応して，米国 Society of Automotive Engineering (SAE) などがサイバーセキュリティ対策ガイドやベスト・プラクティスを開発している．しかし，これらのガイドやベスト・プラクティスでは，サイバーセキュリティ機能の開発プロセスが安全機能開発プロセスと分離されている．しかし，サイバー攻撃の結果発生する障害に対して車の安全を維持するためには，車の安全機能とサイバーセキュリティ機能を関連付けて開発する観点が必要である．本研究は，この問題に対する解決策を提示している．

先に述べたように，本研究は車両の安全機能開発の国際標準規格をその基礎においている．そのため，序論において，本論の理解に必要な関連規格をはじめに述べる．また，一般にサイバーセキュリティ対策を行うにあたっては，サイバー攻撃の結果発生するリスクを評価した結果に基づき対策の要否を定める．そのため，サイバー攻撃とそれによって発生するリスクのアセスメント手法についても合わせて述べる．

2.1.1 車載 E&E システム開発に関する国際標準

ここでは，まず，本研究に関連する国際標準について述べる．国際標準における標準化の考えは，以下の文書で表される．

「標準化 (Standardization) とは，「自由に放置すれば，多様化，複雑化，無秩序化する事柄を少数化，単純化，秩序化すること」ということができます． また，標準 (=規格:Standards) は，標準化によって制定される「取決め」と定義できます．標準には，強制的なものと任意のものがありますが，一般的には任意のものを「標準 (=規格)」と呼んでいます」　(日本工業標準調査会 (JISC) ウェブサイトより [2])

現在，交通や情報などの社会システムや企業の情報管理，生産活動や製造物などにおいて International Standard Organization (ISO) や International Electrotechnical Commission (IEC) などの国際標準化団体の策定する標準に準拠することは必須要件になりつつある．これは，国際協定である WTO/GP 協定 (WTO: World Trade Organization) により政府調達する物品の性能が国際標準に準拠することが強く推奨されていることもあり，また，標準の目的である以下の項目が企業活動に必須であるゆえである．

1. 経済活動に資する機能

(1) 製品の適切な品質の設定

(2) 製品情報の提供

(3) 技術の普及

(4) 生産効率の向上

(5) 競争環境の整備

(6) 互換性・インターフェースの整合性の確保

2. 社会的目標の達成手段としての機能

3. 相互理解を促進する行動ルールとしての機能

4. 貿易促進としての機能

(日本工業標準調査会 (JISC) ウェブサイトより [2])

本論文に関連する車載電子電気システムの開発に関係する国際標準 ISO 26262[3] や車両のサイバーセキュリティ国際標準として現在制定中の ISO/SAE 21434[4] は主として 1. 経済活動に資する機能の (1) 製品の適切な品質の設定にかかる標準であり，また情報システムや個人情報の管理にかかる ISO/IEC 27001 シリーズの情報システムのセキュリティマネジメントに関する規格は 1. の (1) と 2. 社会的目的の達成手段としての機能，に主に関係するものとなっている．

本論文の 2 章では，自動車のサイバーセキュリティ機能の開発プロセスに関連した研究を行なっている．一方，現在，自動車の開発においては，国際標準 ISO 26262 を軸とした開発が行われている．ISO 26262 は自動車の安全の実現にかかる標準である．また，サイバーセキュリティのリスクアセスメント手法については，種々の提案があるが，本論文では，日本自動車技術会が発行した技術レポート TP15002 を想定した検討を行なっている．そのため，これらの解説を行う．

2.1.2 自動車の機能安全開発

自動車とは，高速で移動する重量物である．したがって，部品の故障や異常による車両の異常動作は，物品や人命の損失に容易につながる．したがって，自動車は，そのような損失を防ぐ「安全」の実現が設計上の最優先項目の一つである．安全の実現には，本質安全と機能安全の二つのアプローチが存在する．本質安全とは，安全を損なう事態が本質的に発生しないことである．交差点での交通事故を例とする．交差点では，人と車，もしくは車と車が相互の進路を横切る事態が多発する．事故とは，2 者以上の進路が交差し，なおかつ交差した点に同時に双方が存在することである．交差点を立体交差にして，人は歩道橋をつければ，進路の交差そのものが発生しなくなるため事故は発生しなくなる．このように，事故そのものを根本要因を取り除き，事故を本質的に不可能にすることが本質安全による安全のアプローチである．一方，機能安全とは，安全を実現するための機能を追加することにより，目的を達成するものである．交差点の例では，信号制御により進路の交差を避ける交通制御を行う，歩行者横断帯に踏み切りをつけるなど，危険な現象を抽出し，それを阻止するまたは軽減する機能を追加することで安全を実現するものである．ISO 26262 は車載電気電子システム (以下，車載 E&E システムと呼ぶ) の機能安全に関する標準である．

ISO26262 は IEC61508[5] をベースとした安全規格であり，3,500Kg 以下の自動車の制御システム開発に特化したものである．本規格は，全体の安全管理から，要件定義，設計，製造，評価/検証，生産と運用およびそれを支える要件定義や開発上必要な支援プロセス，Automotive Safety Integrity Level (ASIL) の解説並びにガイドラインからなる．全体の開発プロセスは，要件定義から設計，製造，検証に至るウオーターフォール型のプロセス (V 字プロセス) が定義されている．

2018 年 5 月現在，ISO 26262 は 2011 年 (一部 2012 年) に標準化されたものが使用されている．ISO 26262 は全部で 10 のパートからなる

Part1:用語集

Part2:機能安全の管理

Prat3:コンセプトフェーズ

Part4:システムレベルにおける製品開発

Part5:ハードウエアレベルにおける製品開発

Part6:ソフトウェアレベルにおける製品開発

Part7:生産および運用

Part8:支援プロセス

Part9:ASIL 指向および安全指向の分析

Part10:ISO 26262 ガイドライン

これらの各パート間の開発における関係は図 2.1 で表される．

車載 E&E の開発に直接関連する部分は，灰色の V 字と W 字が書かれている部分である．この V 字は，V 字左側に要件定義や設計作業が，右側に検証作業が配置されている．そのため，車載 E&E システムの開発を V 字開発と呼ぶ．

車載 E&E システムの開発は，図 2.1 にもある通り，Concept Phase (以下，コンセプトフェイズと呼ぶ)，Product development of System level (以下，システムフェイズと呼ぶ)，Product development of Hardware Level，Product development of Software level(以下，HW/SW 開発フェイズと呼ぶ) と段階的に進められる．コンセプトレベルでは，車両レベルからみた機能ごとに開発対象を定義し，その機能が損なわれた場合の事故のリスクを評価し，機能安全機能の開発目標を定める．システムフェイズでは，コンセプトレベルで定められた開発目標とそれに含まれる機能安全機能要件から，ハードウエア，ソフトウェアならびに双方のインターフェース (Hardware Software Interface，以下 HSI) の仕様を定義する．最後に HW/SW 開発フェイズで，仕様に従ったハードウエア，ソフトウェアの開発を行う．

この構造は，自動車業界の産業構造にも適合している．自動車業界は車両メーカーである OEM，システムサプライヤである Tier-1，システムの構成要素を開発する Tier-2，部品を供給する企業群という構造になっている (図 2.2)．

OEM は主としてコンセプトフェイズに関わり，車両の機能やそれが損なわれた時のリスクの判断や対策方針の決定に関わる．Tier-1 は主としてシステム設計者としてシステムフェイズに関わる．また Tier-2 以下は，主としてシステムを構成する個別要素のハードウェア・ソフトウェアの設計開発に携わる．コンセプトフェイズに関わる．コンセプトフェイズ，システムフェイズの間では，機能安全コンセプトが，システムフェイズと HW/SW 開発フェイズの間では，システムデザインが共有される．機能安全コンセプト

とは，車両機能としての機能安全を実現するための要求事項を個別の機能に割り当てたものと，リスク分析に基づき目標とすべき最上位の安全に対する要求を含む情報である．システムデザインは，機能安全コンセプトから技術安全コンセプトの導出をへて作成される．技術安全コンセプトは，機能安全コンセプトに含まれる機能要求事項を開発対象上で実装するために，機能要求事項から技術的な実現手法を意識して導出された技術的な要求事項 (技術安全要求) をシステムを構成する要素ごとに割り当てたものである．この割り当てられた個別の要求をシステムの構成要素の仕様にしたものがシステムデザインである．

これらの手順は，先行するフェイズから得られた要求事項を，システムフェイズ，HW/SW 開発フェイズの担当者が持つ詳細な設計情報に照らし合わせて，詳細化する手順である．また，原則的には，各フェイズの実施者間では上にあげた情報以外は共有しない．したがって，システムフェイズの実施者は，設計対象やリスク評価の内容の詳細についての情報は持たなくてもよい．逆にコンセプトフェイズの実施者は，対象システムの実現方法の詳細についての情報は持たなくてもよい．また，システムフェイズの実施者は HW/SW の実装に関わる詳細についての情報は持たなくてもよく，HW/SW 開発フェイズの実施者は，技術セキュリティコンセプトに内容については情報を持たなくてもよい．このように，各フェイズで共有される情報が分割されていることが，車載 E&E システム開発における特徴の一つである．

本章は，コンセプトフェイズおよびシステムデザインフェイズの V 字左側の開発プロセスにおいて，機能安全とサイバーセキュリティの開発の統合手法を提案するものである．以下，本章の内容の理解に必要十分な上記プロセスの解説を記載する．

コンセプトフェイズでは，車両レベルの機能から開発対象を定義し，損失を引き起こす事象の分析とその結果引き起こされる事故の程度などからリスク評価を行い，機能ごとにリスクを低減すべき目標を定める．さらにリスクの低減を実現するための機能要求を導出する一連の作業が行われる．コンセプトフェイズに含まれる作業は，アイテム定義，ハザード (危機事象) 分析とリスクアセスメント，機能安全コンセプトの導出である．

ここでは，本章の検討対象である要件定義から設計に至る手順を述べる．

(1) アイテム定義 (開発対象定義)

アイテムとは，車全体観点でみた機能を提供するシステムもしくはシステムの集合体と

して定義される開発対象である．アイテムは，形式的には，センサーなどの外部入力，入力，演算などの内部処理，アクチュエータへの出力からなる構成および機能および非機能要求，制約条件からなる．内部処理には，車全体としての機能要求，および機能を提供するためにエレメントと呼ぶサブ機能ブロックが定義されている．たとえば，パワーステアリング機能は，ハンドルにかかるトルクを検出し車速と舵角に対応してトルクを調整することである．これをアイテムとして示すと図 2.3 となる．

(2) ハザード分析とリスクアセスメント

ISO26262 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． 安全は，リスクの低減が目標である．

まず，ハザードとハザードが発生する状況の特定を実施する．一般には，HAZOP(Hazard and Operability Study) 手法で抽出，さらに FMEA(Fault Mode and Effect Analysis)/FTA(Fault Tree Analysis) で実際発生可能性の分析を行う．HAZOP では不作動，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 でハザードの原因となる事象を洗い出す．最後にアイテムのエレメントの FMEA を適用し，個別のエレメントの故障要因から 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評価をおこなう．

ISO26262 では到達すべきリスク軽減度の指標として ASIL(Automotive Safety Integrity Level) を定めている．ASIL 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てさだめる到達すべき安全度の指標としてのリスク低減目標である．ハザードの特定の結果，得られるハザードの過酷度，発生頻度，回避可能性からから，定められた分類表に従って 4 段階の ASIL および一般品質保証レベルでの対処 (QM) の分類を決定する．開発に際しては，ASIL のレベルに応じた開発手法や検証，システム構成をとることが要求される．

ハザード分析とリスクアセスメントの最後に，ハザードに対する安全に対する要求をセーフティゴール (安全目標) として定める．セーフティゴールには，ハザードに対して実現すべき安全目標，実現すべき安全状態と，ASIL を定める．パワーステアリングの例を下に示す (表 2.1).

(3) 機能安全コンセプトの導出

次に，安全目標を実現するために必要な，安全機能 (機能安全要件) の抽出を行う．ここ

表 2.1　セーフティゴールの例

ハザード	高速走行中ハンドルが軽くなり，急な操舵を行った結果，車両事故が発生する．
安全目標	高速走行中ハンドルが軽くならないようにする．
安全状態	走行中はパワーステアリングをオフにする．

で定義される，機能安全要件とは，安全目標に基づくアイテムの安全な振る舞いの仕様および実装に依存しない安全方策である．

まず，安全目標を達成するのに必要な機能を導出する．アイテムの構成図などから，機能安全目標を詳細化して安全機能を導出する．これらの機能安全要件を，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各エレメントもしくはアイテム外部での対策に割り当てる．この割り当ておよび機能安全要求のすべてを機能安全コンセプトと呼ぶ (表 2.2)．

表 2.2　技術安全コンセプトの例

安全目標	高速走行中ハンドルが軽くならないようにする．	
機能安全要求	速度とハンドル操作を補助しているトルクを監視し，速度に比べて補助トルクが異常に大きければ，補助トルクを出すアクチュエータを停止する．	
理由	高速走行中に大きなハンドルを切ると事故につながりやすい．低速走行時にハンドルが重くなった場合でも，事故は起こりにくい．また運転手の気づきにより修理工場へ行くことが促される．	
速度信号の検出	速度を直接監視機能に入力する．	監視機能
トルクの検出	トルクを直接監視機能に入力する．	監視機能
異常の検出	速度とトルクを比較して異常を検出する．	監視機能
アクチュエータオーバライド	監視機能からアクチュエータ出力をオーバライドする．	監視機能，アクチュエータ

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 2.4)

(4) 技術安全要件の導出とシステム設計

機能安全コンセプトを，機能安全機能の設計対象である前提アーキテクチャ (preliminary architectural assumptions) 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件である (表 2.3)．

システム設計では，実装に関する要件である技術安全要求を受けて，前提アーキテクチャに安全機能を追加して，ハードウェアまたはソフトウェアの基本設計を完了する．

表 2.3　技術安全要求の例

機能安全要求	速度とハンドル操作を補助しているトルクを監視し，速度に比べて補助トルクが異常に大きければ，補助トルクを出すアクチュエータを停止する．		
技術安全要求 1	速度信号と補助トルク信号を直接計測し，両者の値を比較することで異常を検知し，検知した場合にトルク信号出力をオーバーライドしアクチュエータを停止する．		
速度直接計測	信号線追加	速度信号を直接監視機能に入力する信号線を追加する．	監視機能，信号線
トルク直接計測	信号線追加	トルク信号を直接監視機能に入力する信号線を追加する．	監視機能，信号線
異常検出	速度信号数値化	速度信号を数値に変換	信号変換
	トルク信号数値化	トルク信号を数値に変換	信号変換
アクチュエータ　オーバライド	信号線追加	監視機能からアクチュエータ出力をオーバライドできる信号線を追加する．	監視機能, 信号線, アクチュエータ

2.1.3　自動車のサイバーセキュリティ分析

TP15002 は公益社団法人自動車技術会により取りまとめられた自動車システム向けのサイバーセキュリティ分析ガイドである．このガイドにおけるサイバーセキュリティ分析は，評価対象の定義，脅威分析，リスク評価，対策方針決定，サイバーセキュリティ要件の選択という 5 つのフェイズからなる．

評価対象の定義では，評価対象の構成要素および構成要素間の情報フローを明確したモデルを作成する (図 2.5)．

さらに構成要素毎に，提供機能と構成要素が含む保護資産を明確にする．保護資産には保護すべき機能とデータがある．例として，車外と車内の通信システムの中間に介在するゲートウエイ ECU の機能・保護資産を表 2.4 に示す．

次に対象システムのライフサイクルおよび各サイクルで対象システムに関与可能な人・

表 2.4　ゲートウェイ ECU の機能・保護資源

	機能	保護資源	C	I	A
ゲートウェイ ECU	認証機能	認証機能		○	○
		認証鍵	○	○	
	情報転送機能	情報転送機能		○	○

組織 (ステイクホルダー) を定義する．この定義は，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 (表 2.5).

表 2.5　ライフサイクルとステイクホルダーの例

ライフサイクル	機能	ステイクホルダー	役割	不正
輸送	配送	輸送業者	輸送	不正配送
運用	メンテナンス	ディーラー	検査・修理 (高度)	高度な改ざん
		修理工場	検査・修理	改ざん
	通常利用	ユーザー	運転	不正改造
廃棄	廃棄	廃棄業者	廃棄	データ抜き取り

脅威分析では，まず評価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脅威を，どのインターフェース (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) かを整理して洗い出す (表 2.6).

表 2.6　脅威の例

Where	ゲートウェイとサーバのインタフェースから
Who	第三者が
When	走行中に
Why	通信データ (認証データ) を
What	盗聴して漏えいさせる，なりすます

リスク評価では，抽出された脅威について CRSS(CVSS based Risk Scoring System) や RSMA(Risk Scoring System for Automotive systems) を用いてリスクスコアリングをおこなう．ある基準以上の脅威については FTA などにより原因を抽出し，すべての事象に対して対策方針を決定する (表 2.7).

表 2.7　対策方針の例

脅威	原因	対策目標	対策方針		
			#	種別	方針内容
走行中 (運用時) 偽センサー情報を流される.	ゲートウェイとセンターサーバ間の認証データを盗聴して成りすます.	ゲートウェイとセンターサーバ間の認証データの盗聴を防止する.		IT	認証データを暗号化する. 通信データをメッセージ認証する.

最後にサイバーセキュリティ機能要件とサイバーセキュリティ保証要件を定義する. 機能要件は，ISO15408 Common Criteria Part2 で定義されるサイバーセキュリティ機能コンポーネントを要件として書き換えたものである. また保証要件は，Evaluation Assurance Level(EAL) で指定する. ISO15408 Common Criteria Part3 の EAL と評価クラスの対応表に従い，設定したリスクスコアに相当する保証要件を確認検証する (表 2.8).

表 2.8　サイバーセキュリティ対策と機能要件

脅威	方針	対応
偽センサーデータを流される.	認証データの暗号化	FTP.ITC.1(高信頼チャネル) FCS_CKM(暗号鍵管理) FCS_COP(暗号操作)
	通信データのメッセージ認証	FTP.ITC.1(高信頼チャネル) FCS_CKM(暗号鍵管理) FCS_COP(暗号操作)

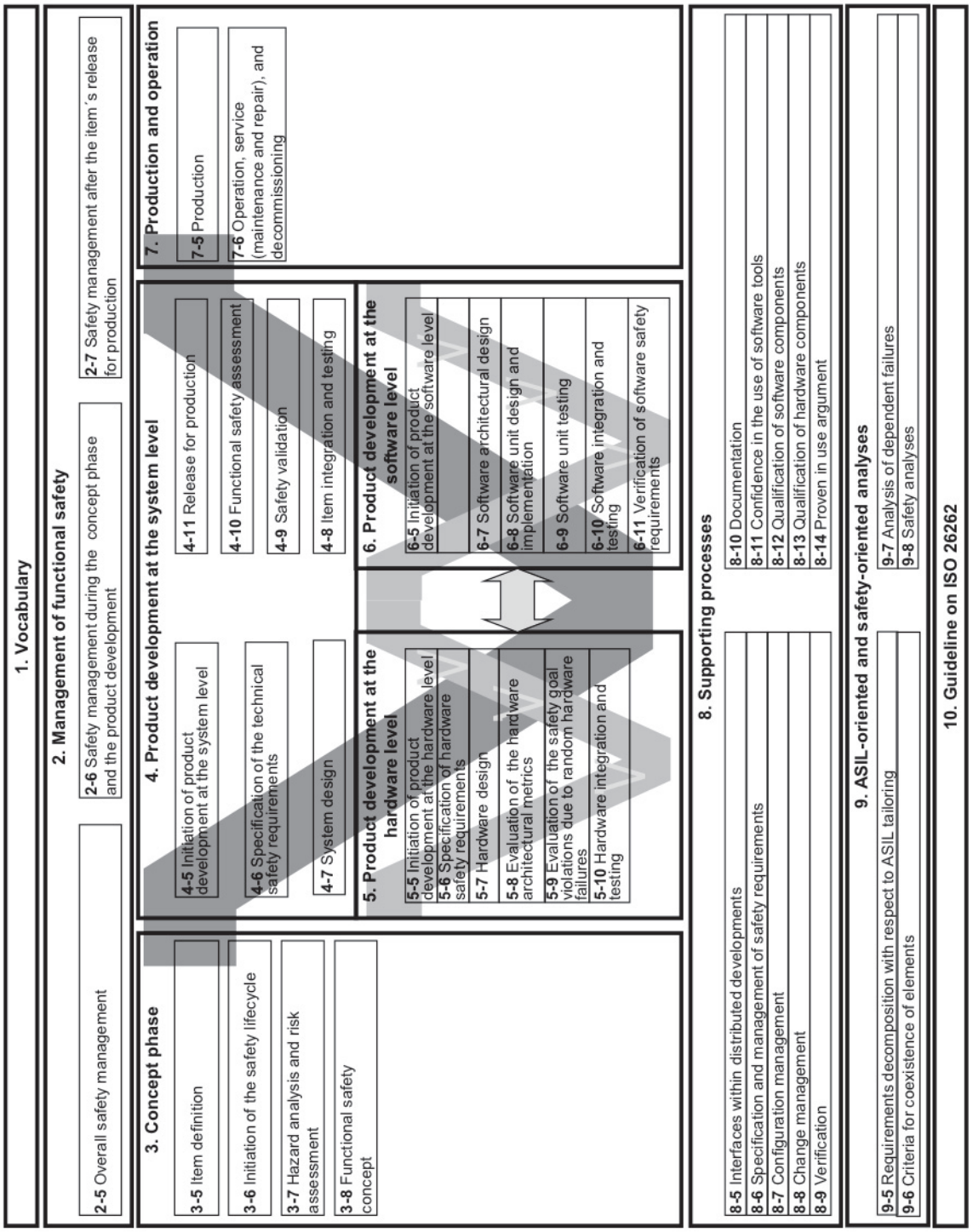


図 2.1　ISO26262 全体構成 (ISO 26262 part-1:2011 より引用

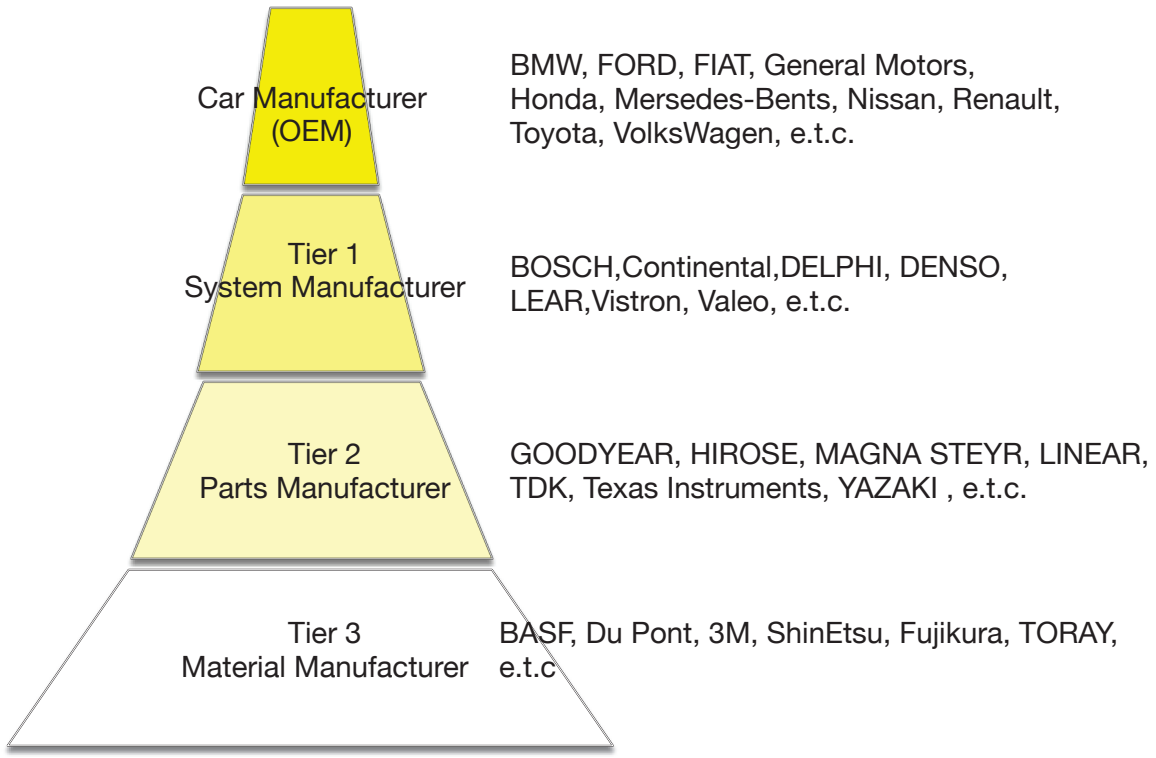


図 2.2　車載 E&E システム開発にかかる業界構造

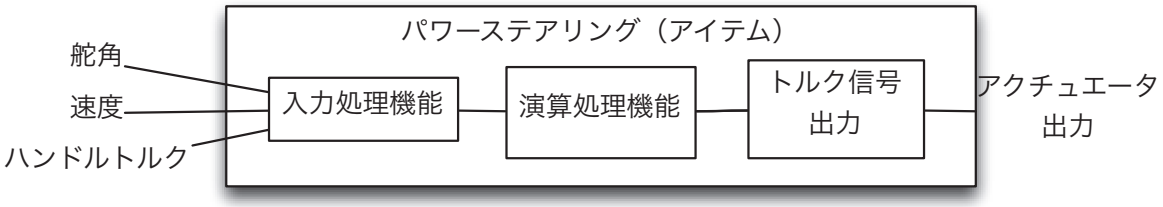


図 2.3　パワーステアリングアイテム構成図

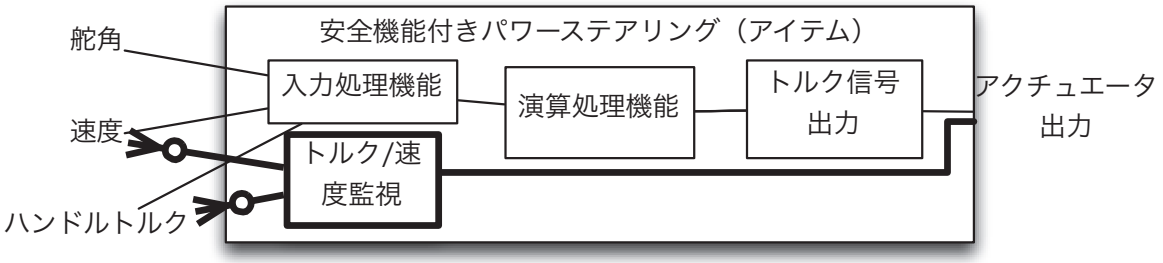


図 2.4　安全機能付きパワーステアリングアイテム構成

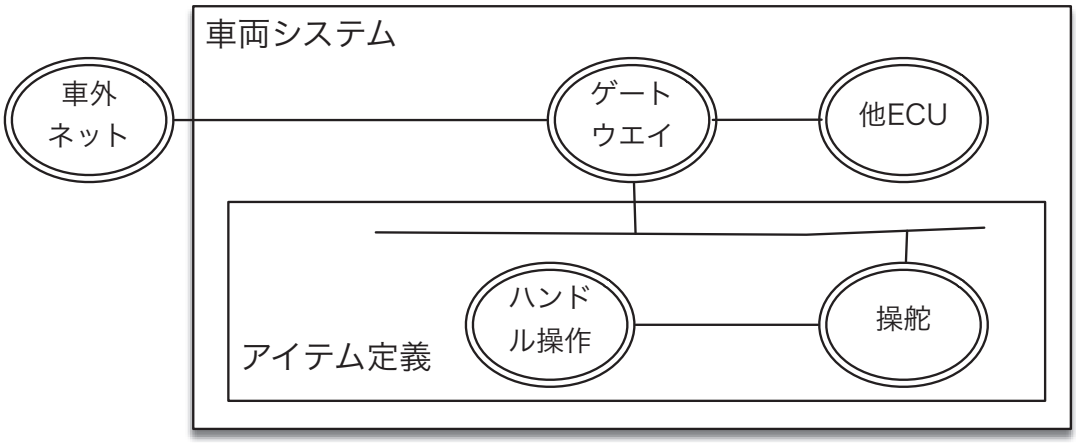


図 2.5　評価対象モデル例

2.2 目的

本章では、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 各々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．両者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の詳細化し，要件を定義する過程で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．すなわち，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．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．

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を阻止すること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 は自動車に対する機能安全規格である [3].

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撃の発表や，プラントに対する攻撃よると 2009 年以降，インシデント報告は増え続け，2013 年は 250 件超の報告がされている [6]．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，IEC　62443[7] 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 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 [8].

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．たとえば，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 [9] などでも同様である． 本章では，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曝される点とそこで発生しう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およ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．

2.3 関連研究

自動車におけるセキュリティ機能開発に関連する標準の提案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[8] 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が幾つか検討されている [10][11][12]．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 [13] がある．Macher らは，[14] 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，さら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 とよ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イス (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出来ない．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，それら作業および出力と各プロセスの入力情報が関連づけられていない．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舞の検討は行われていない．

2.4 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．たとえば，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，断線等による 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，さらに対処決定の際，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．たとえば，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．

2.5 提案手法

本章では，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なる．

2.5.1 機能安全・セキュリティ動作モデル

本章で提案する機能安全・セキュリティ機能の動作モデルを図 2.6 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) と車両のセンサー類や他の ECU，運転車が相互に情報を交換して機能している．
2. セキュリティ機能 (予防・検知)：車両本体機能およ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の移行させる．対処困難な場合には，他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もつ．もし安全機能で対処出来ない場合には，他の手段，たと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とる．

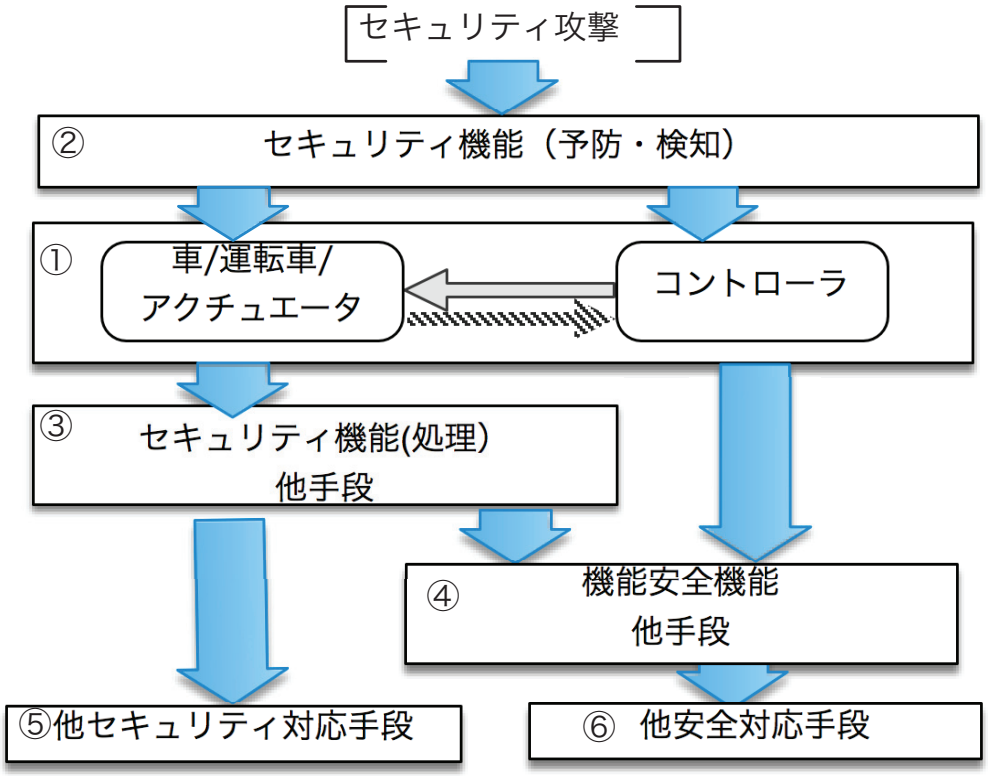


図 2.6　機能安全・セキュリティ動作モデル

5. 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出来ない事象への別手段による対応を行う．
6. 同上

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，必要な対象を行う．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，そうで無いものに分割し，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．この動作モデルは次の利点をもつ．

(a) 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づけており，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．

(b) 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 (1.5 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．

(c) 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．(1.5 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 2.7)．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なる．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とりあつかう必要上，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，その詳細化にあわせて脅威を記述する．即ち，脅威は，脅威種別，対象およ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，対処すべき脅威に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成らない．そのために ASIL レベルが導入される．

d) 実装要求になるあた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．この時に b) での脅威を利用する．

2.5.2 セキュリティ要件定義プロセス

次に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．

(1) 拡張アイテム定義 (図 2.7 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 2.7 S.1) で定義されたアイテムを入力とする．このプロセスの出力は，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．たとえば，車載ネットワーク上の機能上関係無

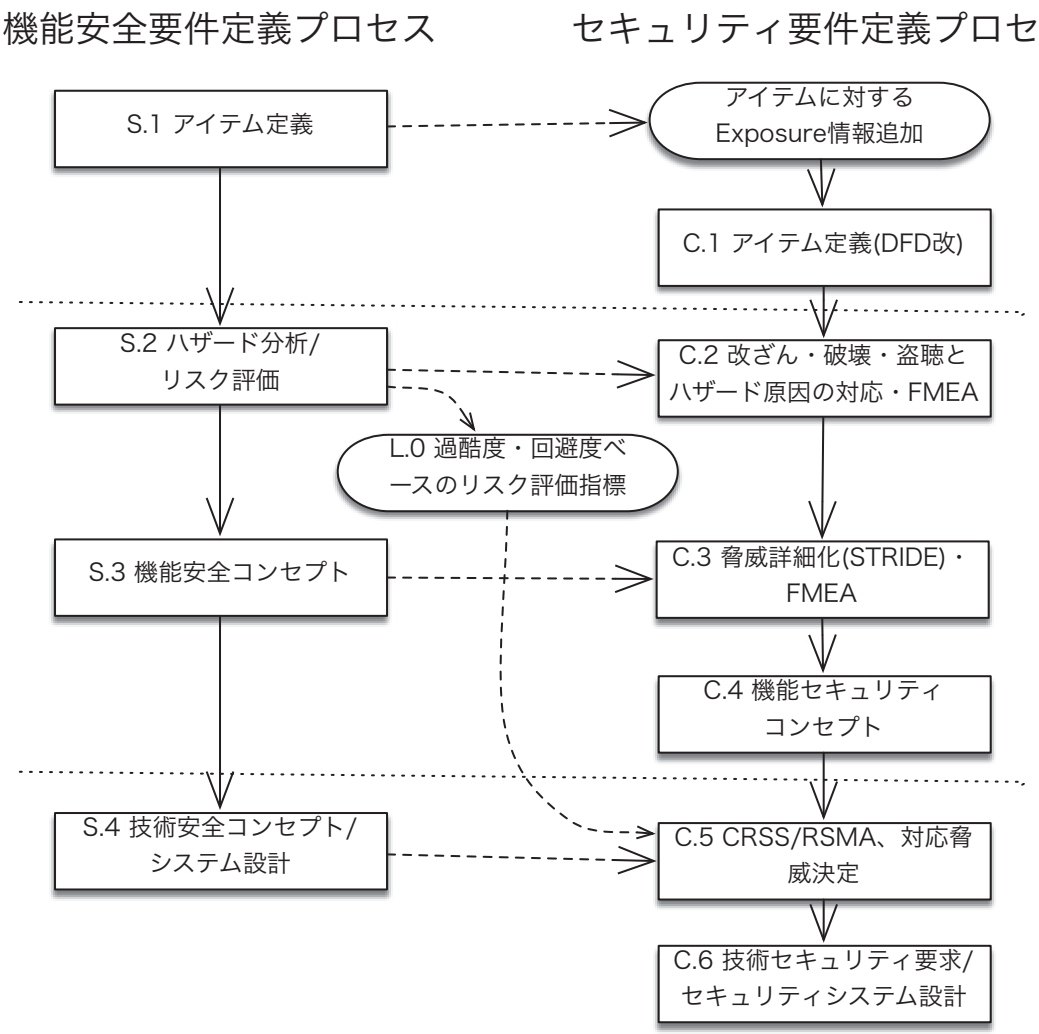


図 2.7　機能安全・セキュリティ統合プロセス

い ECU からの攻撃が相当する．この様な場合を含めでも脅威を明示的に表記するために Exposure Control Point(以下 ECP と略す) を導入する (図 2.8).

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[15] 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曝される点とそこで発生する脅威の組み合わせである．図 2.8 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出来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

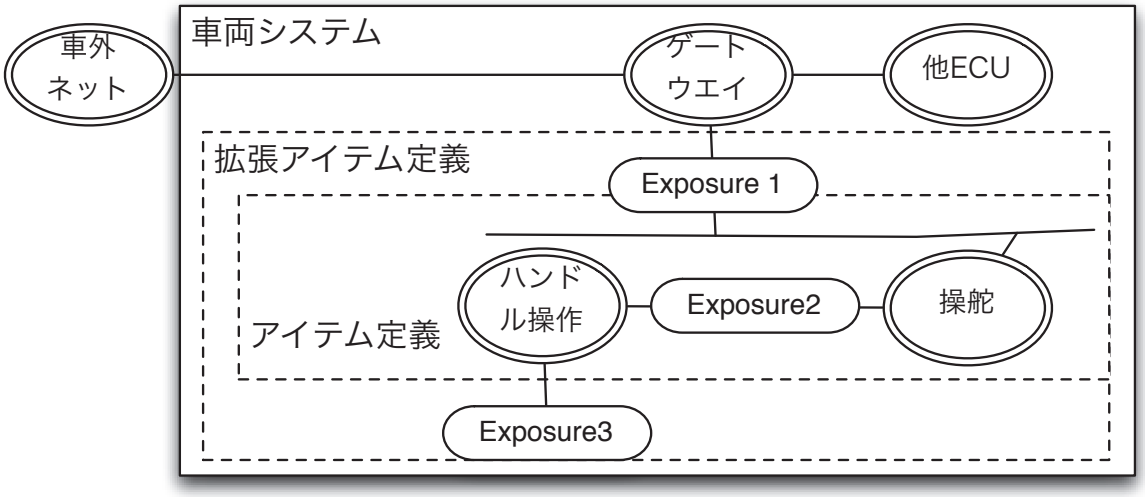


図 2.8　拡張アイテム定義 (丸四角が ECP)

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．

(2) ハザードと脅威対応 (図 2.7 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 2.7 S.2)．一方，本提案では，1.6.1 の拡張アイテム定義と機能安全でのハザードおよ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．さらに，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およ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およ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 2.7 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および安全指標である．

(3) 脅威詳細化・機能セキュリティコンセプト (図 2.7 C.3,C.4)

ここでは，機能安全コンセプト（図 2.7 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および拡張ア

イテム定義を入力とし，STRIDE 手法 [16] 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 2.7 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づける．さら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 2.7 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．

(4) リスク評価と対応，技術セキュリティ要求導出 (図 2.7 C.5, C.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さら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，(3) で定められた値 (図 2.7 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) および攻撃検知，セキュリティ機能の通知と内部の安全機能と関連づ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づけが完了する．

2.6 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 2.8)．

(1) 拡張アイテム定義 (図 2.7 S.1, C.1)

図 2.9 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，速度はセンサー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

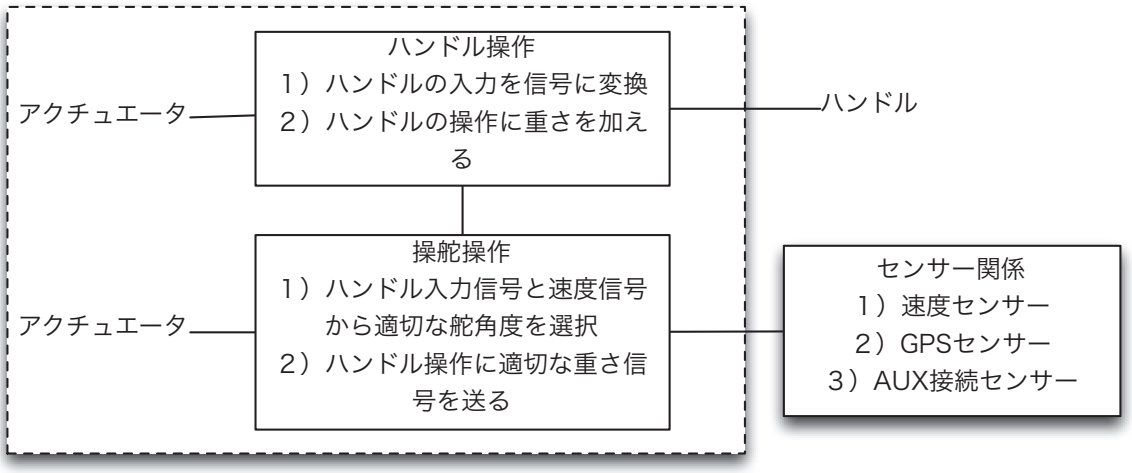


図 2.9　対象アイテム定義 (破線内)

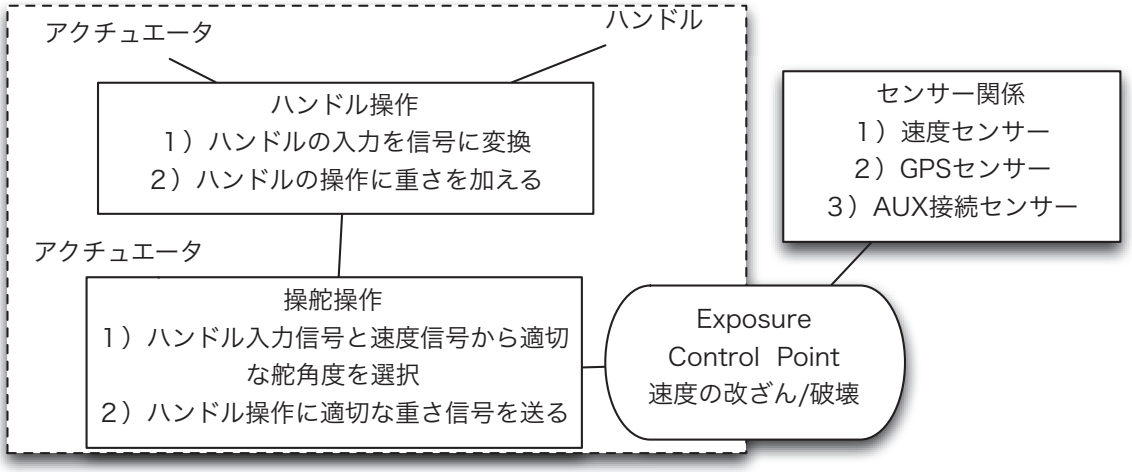


図 2.10　拡張アイテム定義 (破線内)

ローダイヤグラムに ECP を追加する（図 2.10）．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 はセンサー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．

(2) ハザードと脅威対応 (図 2.7 S.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

表 2.9　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

表 2.10　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	STRIDE 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等.	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

ECP としてデータ破壊および改ざんの脅威が想定できる (表 2.9)．このハザードに対する過酷度および回避可能性は機能安全側での HAZOP 等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.

(3) 脅威詳細化・機能セキュリティコンセプト (図 2.7 S3, C.3,C.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 2.10)．このとき，ECP を STRIDE 手法で詳細化する．表 2.10 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.

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

表 2.11　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	STRIDE 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
正規と区別出来ない ⇒ 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

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) およ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．ここではこの二つを確認出来るメッセージ認証機能 (MAC 認証) をもちいて対策機能とすることを想定する (表 2.11).

(4) リスク評価と対応，技術セキュリティ要求導出 (図 2.7 C.5,6)

(3) 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たいして，その実装要求 (技術安全要求) が導出される．システム設計情報等を利用してセキュリティ脅威をさらに詳細化し，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 2.12).

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 2.7 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 2.13 では，表 2.12 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 2.11 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 2.11 の対処方法である重さ信号送出 (対処 2) を実施

表 2.12　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替.	データ改ざん	6(要)

する.

これらの対策を図 2.6 のモデル図にマッピングしたものが図 2.11 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．安全機能で対処出来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.

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.

2.7　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，脅威および，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・演劇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 手法および 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

表 2.13　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	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

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関係する作業を規格化したガイドラインで ISO/IEC 27005[17] 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，さらに検討が必要と考える.

次に、本研究の関連研究である [13] との比較を行う．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，さらにシステム設計情報と併せて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二つに分類する．これにより，対処しない詳細度脅威を管理出来る一方，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．さらに，ステアリングシステムに対する適用結果を比較する． [13] のセキュリティ対策は Trustzone の境界面の HSI に対する, ハザー

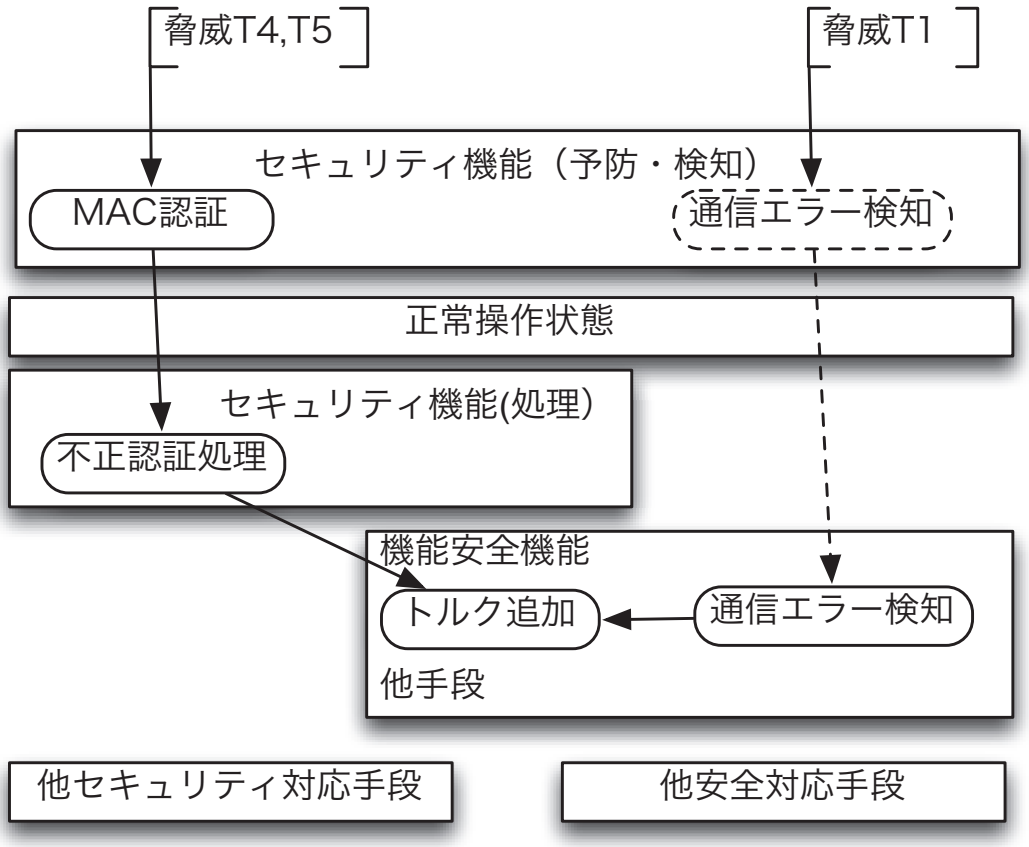


図 2.11　セキュリティ対応対象システム

表 2.14　関連研究での対策例

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，デバイス検証

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 2.14 にしめす．

表 2.13 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 2.11) 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．

2.8　まとめ

本章では，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．本章の内容が，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．

ISO 26262 に対応するサイバーセキュリティ開発の標準は，2018 年 6 月現在，ISO と Society of Automotive Engineers International (SAE International, 以下 SAE) が共同で ISO/SAE 21434 の標準の制定を進めている．しかし，現時点では，ISO の標準ライフサイクルでの Preparatory 段階である．一般的な ISO の標準化に要するタイムスパンからみて公開までにはなお数年を要する．

一方，SAE は独自に車載 E&E システム開発でのサイバーセキュリティ開発におけるガイドブックである SAE J3061 を 2016 年 1 月に発行した．このガイドラインでは，安全とサイバーセキュリティをそれぞれ，生命や財産，周辺環境に危害を与えることのないシステムの状態および，金銭，プライバシーや安全などを損なうことにつながる脆弱性を利用した攻撃を許さないシステムの状態と定義している．また，それぞれのリスクを分析するにあたり，安全では FTA を，またサイバーセキュリティでは脅威分析手法の一つである Attack Tree Analysis(ATA) を用いてリスクの発生要因を分析する．開発プロセスの観点では，SAE J3061 もコンセプトフェイズ，システムフェイズ，HW/SW 開発フェイズに相当するフェイズを定義している．

SAE J3061 では，機能安全機能とサイバーセキュリティ機能の統合については，双方の開発が相互に情報を交換することにより解消すると記載している．しかし具体的に交換すべき情報の種類やその結果，双方の開発者が行うべき作業についての指針は記されていない．本研究では，車両開発であることを重視し，かつ，サイバー攻撃が発生した場合の対処は機能安全的なアプローチが妥当性が高いとして，安全とサイバーセキュリティの統合モデルを開発している．その点において，本章の手法は安全とセキュリティの統合コンセプトについて提言していると考える．

また，Bosch も ESCAR 2014 で Bosch Security Engineering Process を発表した．このプロセスは三段階のプロセスからなる．第一フェイズは，製品コンセプトやシステムのアーキテクチャにサイバーセキュリティで実現すべき目標を決定する．第二フェイズでは，脅威分析とリスクアセスメントを実施する．第三フェイズで脅威とリスク，さらにセキュリティ対策の必要性からサイバーセキュリティの要求仕様書をつくるコンセプトフェイズ相当のプロセスである．汎用的な考え方であり，安全機能との統合に特化した本研究とはアプローチが異なる．

また，本章では，リスク評価手法として TP15002 を利用している．他に，車載システムに向けたリスク評価手法して，EVITA，HEAVENS などで提唱されている手法が存在する．本研究では，リスク対応を定めるリスク評価は実装詳細が判定可能なシステムフェイズで行い，コンセプトフェイズではリスク評価に用いるパラメータの決定にとどめている．そのため，コンセプトフェイズで EVITA，HEAVENS などのリスク評価手法で用いるパラメータを定義できれば，これらの手法を問題なく適用することができると考える．特定の評価手法に依存することは，標準プロセスとして望ましくない．この検知からも，本章で開発した安全とサイバーセキュリティの統合プロセスは好ましい性質を備えていると言える．

本研究において，サイバーセキュリティ機能の開発は機能安全設計の開発対象であるアイテムを対象として実施する．その際，アイテムに対するセキュリティ侵害を ECP とした拡張アイテム定義を導入した．この ECP を適切に定義し，セキュリティ侵害を網羅するためには，アイテム定義において，アイテムととその外部とのインタラクションが網羅されていることが必要である．この ECP の定義作業において，(1) 車載機能の高度化，複雑化にともなうインターフェースや相互作用の複雑化，および　(2) 同じ複雑化に起因する機能のデータフローの複雑化にともなうサイバーセキュリティ対策検討や脆弱性分析の複雑化に起因する問題が懸念される．

本研究では，パワーステアリングシステムを事例として，提案開発手法の妥当性を検討した．一方，現在では車載 E&E システムの機能は，高度化，複雑化する傾向がある．たとえば，先進運転支援システム (Advanced Driver Assistance System: ADAS) では，従来から存在する車両レベル機能と新たに追加されたユーザーインターフェイス，通信機能やセンサ類とを統合して，運転者による安全な運転を補助する機能を実現する．このようなシステムの例として，自動駐車システムや車線逸脱防止システムがある．自動駐車システムでは，周辺監視用のセンサ機能とブレーキシステム・ステアリングシステム・スロットルシステムの機能を利用している．

一般にこのように複雑化した開発対象では，構成要素間の相互作用が複雑化するとともに，開発対象とその外部との境界も拡大かつ複雑化する．また，機能を実装する対象である ECU に複数のアイテムが利用する機能，もしくはアイテムごとの機能を実装する．この場合，たとえ，アイテム間での依存関係や相互作用がなくても，同じハードウエアや OS

表 2.15　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

などの基本ソフトウエアを共有している．この共有資源を介した相互作用が存在する．拡張アイテム定義では，これらのインターフェースを網羅的に抽出しなければならない．また，従来機能を統合して，新たな機能を定義する際に，必ずしも従来機能で定義されているインターフェースやそれを構成する機能間の相互作用と同じ詳細さで新たな機能のそれが定義されているわけではない．そのため，設計が詳細になるに従って，インターフェースや相互作用が，もれなく詳細化され，各要件定義段階や設計段階に適切な粒度で記述できる手法が必要である．

(2) の問題は，セキュリティ対策を検討する場合，一般的には各機能間のデータフローに対して脅威の存在検証やその実現可能性，対象となる脆弱性分析を実施し，必要なサイバーセキュリティ対策を立てる．しかし，複雑な拡張アイテムではデータフローそのものが複雑化する結果，対策検討作業が膨大なものとなる．

3 章，4 章では，これらの問題点を分析し，その対応方法に関する研究結果を示す．

表 2.16　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	STRIDE 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等.	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

表 2.17　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	STRIDE 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
正規と区別出来ない ⇒ 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

表 2.18　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替.	データ改ざん	6(要)

表 2.19　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	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

表 2.20　関連研究での対策例

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，デバイス検証

第 3 章

機能安全・サイバーセキュリティ統合開発のための車両機能インターフェースの抽出手法の検討

3.1 はじめに

車には，その一部に故障や不具合が発生しても，運転者や周辺に損害を与えるような事故が発生させない，もしくは回避可能とすることが望まれる．このような，故障や不具合に対する安全性能を実現するために，本質安全と機能安全の２つの考え方がある．本質安全とは，損害や事故が発生する原因をなくすことによる安全の実現である．機能安全とは，損害や事故にいたる兆候を検知し，それに対応する安全機能により，重大な損害の発生を阻止可能な安全状態に移行することによる安全の実現である．車の安全性能の実現は，機能安全の考え方を採用している．この機能安全を実現する安全機能は，車に組み込まれている電気または電子 (E&E) システムに実装する．ISO 26262[3] は，機能安全を実現するための車載 E&E システム開発プロセスに広く採用されている国際標準である．

ISO 26262 に準拠した車載 E&E システム開発は，コンセプトフェイズ，システムデザインフェイズ，ハードソフトウエアレベルの順で進められる．コンセプトフェイズでは，開発対象において故障や不具合によって発生するリスクを評価し，それらのリスクが実現しないように機能安全を実現するための機能要件を定める．システムデザインフェイズではコンセプトフェイズで定めた機能をシステム仕様に詳細化する．その詳細化されたシステム仕様を元に具体的な実装を実現する．

ISO 26262 での開発対象は，車両レベル機能にたいして，その機能を実現する単数もし

くは複数の構成要素からなるアイテムとよぶ単位で定義される．車両レベル機能とは，車両としての機能であり，例としてパワーステアリング機能，ブレーキ機能，スロットル機能など基本的なものから，自動駐車システムや車線維持システムなどの先進運転支援システム (ADAS) などがある．アイテムの定義は，アイテムの機能定義と，それを構成する機能ブロックおよび機能ブロック間の相互作用，アイテム外部との相互作用などから構成される．しかし，現在の先進的な車両機能では，機能の統合利用や，実装時の構成の制限などから，機能間の関係が複雑化する，一般にシステムの構成要素が複雑化するにつれ，その記述の複雑さは急速に増大するため，アイテムを定義することの難易度が高くなる傾向がある．

さらに，車載 E&E システムの場合，構造の複雑化以外にも，複雑化の要因がある．たとえば，車両レベルの機能は，複数の車載電子制御ユニット (ECU) を使用して実現される．しかし，複数のアイテムで利用される機能を単一の ECU 上で実装した場合，たとえ，機能間の直接の相互作用はなくても，その ECU そのものが，アイテム間で排他制御必要な共有資源となり，それによってアイテム間の相互作用が生じる可能性がある．また，自動駐車システムや車線維持システムなどに代表される先進安全機能などの高度な車両レベル機能では，ハンドル制御，ブレーキ制御，スロットル制御など複数の車両レベル機能を密接に統合して機能を実現している．そのアイテムは，自動駐車システムを制御する機能だけでなく，それを構成する車両レベル機能，および追加された機能により発生する車両レベル機能間の相互作用をふくめて記述しなければならない．

また，品質保証面および開発コスト面から，アイテムに含まれる既存の機能な再利用することが望ましい．しかし，機能間の相互作用が複雑化した場合，新たな相互作用による影響分析が複雑化し設計の難易度が高くなることに加えて開発コストの増加が懸念される．

これらの事実を反映して，最新の国際標準ドラフト [18] のアイテム定義には複雑なシステムの記述に関する記載が追加された．すなわち，現在，車両における安全な高度機能の開発のためには，対象アイテムに関連する全ての相互作用を記述するための洗練された方法が必要である．

さらに，近年では車載 E&E システムへの可能性が学会や国際会議などで議論され，実際の攻撃可能な例が発表やデモンストレーションがおこなわれている．今後，開発される

車載 E&E システムにはサイバーセキュリティ対策の開発が不可欠と考えられており，新たな国際標準規格の開発や，様々なガイドラインの開発も進められている．車両の安全機能を攻撃目標とするサイバー攻撃に対抗する場合，対抗策は，機能安全開発の対象であるアイテムについてのサイバー攻撃リスク分析にもとづいて設計開発することが妥当と考えられる．安全機能に対する攻撃は，アイテムやその中に含まれる機能間のインターフェースをアタックエントリーポイントとして開始される．また，対抗策の設計開発は，それらエントリーポイントを経由して行われる攻撃に対抗して設計する．つまり，サイバー攻撃のセキュリティ対策を網羅的に実施するには，アイテムに関連する相互作用の網羅的な記述が必要である．この観点から，網羅的なアイテム記述における相互作用の記述を可能にする手法の開発が必要である．

車載システムは，制御機能を実装した ECU とそれを接続するネットワークからなる分散システムである．そこでの相互作用の記述は相互のインターフェースを呼び出す密結合プロセスとなる．従来，車両機能を構成する機能のインターフェースの定義は，機能間の相互作用に基づいて記述される．一般に分散システムでは，このような記述方法は機能が複雑化するにつれ，加速度的に記述量が増す．その結果，結合されたアイテムの設計が複雑になる．本章では，アイテム定義を記述するために，機能間の相互作用に対してインターフェーサ (influencer) と呼ぶ新しいオブジェクトを導入する．

インターフェーサは，機能間の共有資源と管理機能で構成される．インターフェーサの導入により，従来提案されているアイテム定義の粒度を維持しつつ，新たに追加される高機能の影響とサイバーセキュリティの考慮事項をインターフェース要件としてアイテム定義に組み込む方法を提案する．本章は以下のように構成されている．3.2 節では，自動車の安全とサイバーセキュリティのための複合品の設計の難しさについて説明する．次に，インターフェーサの基本的な考え方を 3.3 節，インターフェーサを用いた設計手順のユースケース 3.4 節で述べる．

3.2 車載 E&E システムの機能安全設計における開発対象定義の問題点

車載 E&E システムの機能安全設計は，自動車の安全設計の根幹である．機能安全とは，「E&E システムに部品故障や動作不良による危険性を防止する機能により危険を回避する

こと」を意味する [19]．ISO 26262 におけるアイテムの定義は，「ISO 26262 が適用される車両レベルで機能を実現するシステムまたはシステムの配列」と定義される [19]．アイテムは a) アイテムの構成要素，b) アイテムが置かれる周辺環境，c) アイテムの他のアイテムまたは構成要素との相互作用，d) 他のアイテムによって要求される機能，e) 他のアイテムから要求される機能，f) 機能の割り当ておよび分配，g) 運用シナリオの情報からなる [3]．

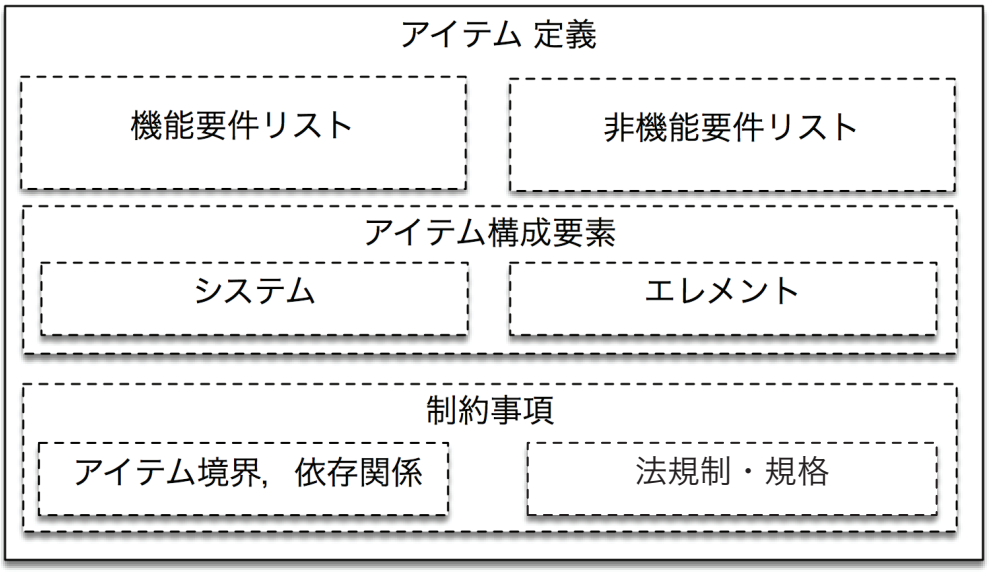


図 3.1　Abstract structure of Item

しかし，一般に，非常に複雑なシステムを，それを構成するサブシステムに分割し，サブシステム間およびサブシステムとシステム外部との相互作用で記述することは困難である．理由は，一般に，複雑なシステムでは，システム自体の複雑さに加えて，サブシステム間の相互通信の複雑さが非常に高くなるからである．複雑なシステムである自動車の E&E システムにおいて，この困難は 3 つのタイプに分類できる．

第 1 の困難は，潜在的な共有に関連する境界の定義および記述，特に，機能間の呼び出し関係や依存関係で明示的に現れされない相互作用を抽出することである．たとえば，複数のサブシステムで構成されるアイテムを考える．このとき，さらに，別のアイテムが，サブシステムの一部を共有しているとする．この場合，共有されたサブシステムを介して 2 つのアイテム間に相互作用が存在する．典型的な例は，車線維持システムとパワーステアリングシステムで，車輪の舵角を制御する装置を共有している場合である．この場合，

この制御装置をどちらのシステムが制御するかを定めるためのシステム間での制御手順が必要となる．また，複数のアイテムでECUを共有した場合，メモリ，CPU使用量，入出力(IO)，または基本ソフトウェア資源などの資源の共有によるいくつかの相互作用が存在する．しかし，機能的に独立している場合，インターフェースの観点ではECU資源の共有による相互作用は明示的には表現されない．このように，アイテム定義を組み込むためには，機能的な観点にくわえて，共有の観点を導入しなければ，すべての相互作用を抽出することは困難である．

第2の困難は，複雑な機能を従来機能を流用した差分開発によって開発する際のアイテム定義において，差分開発による従来機能の変更を最小にする事である．単純な例は[20]に示されている．しかし，現状開発されている機能はさらに複雑な物となっている．自動駐車システムやアクティブセーフティ関連の高度な車両機能は，複数の従来機能を実現しているアイテムを強調させて機能を実現する．例えば，LKAS(Lane Keeping Assist System)およびPAS(Parking Assist System)ではステアリング，スロットル制御，制動，およびそれらを制御する機能のようないくつかの車両レベル機能を統合することによって機能が実現される．しかし，安全に関わる機能がすでに実証されているシステムを再利用し，信頼性の維持と開発コストの削減を実現するという観点から，差分開発の開発者は，既存の製品から新しい機能の副作用を最小限に抑え，分離することが望ましい．また，アイテム定義に基づく開発では，できるだけ明確なアイテム間の境界線によりアイテムを分離する必要がある．これら両方の目的を満たすために，合理的な方法の1つは，事前定義されたアイテムを共有される機能資源として扱い，アイテムの管理を定義し，最後に新しく定義された共有資源とその管理機能を導入することである．しかし，インターフェースを介した相互作用による記述方法では，規模の増大による複雑さの増大が発生するため，要求される副作用の最小化と分離を実現するコストが増大する．

第3の困難は，サイバーセキュリティを考慮したアイテム定義方法の開発である．車のサイバー攻撃に対する深刻な脅威シナリオとして，サイバー攻撃によって車両の安全機能が損なわれるケースがある．悪意のある攻撃者は，車両の安全機能を侵害するためには，車両機能への攻撃経路の発見と当該機能への攻撃手法の検討を行う．攻撃者が攻撃経路を特定した上で，攻撃者は初めて，車両機能に対する攻撃を開始できる．ところで，ISO 26262では，車両の安全機能がアイテムとその境界に基づいて検討されている．したがっ

て，アイテムとその境界を車のサイバーセキュリティ分析の対象とすることは合理的である．この場合，車両機能への攻撃経路は，アイテムの境界線上で定義する必要がある．しかし，サイバー攻撃は，アイテムに定義されている機能に対する直接的な攻撃だけでなく，機能で使用される資源への攻撃などの間接攻撃が存在する．間接攻撃の例としては，ある機能をが実装されている ECU に対し Denial of Service 攻撃を行い，当該 ECU の処理能力を消費させることで，攻撃対象機能にたいして障害を発生させることなどが挙げられる．また，コントローラエリアネットワーク (CAN) ネットワークを共有する 2 つの独立したシステムのものである．これら 2 つのシステムには，相互にインターフェースは存在しない．ただし，システムの 1 つが侵害され，ネットワーク上で Denial of Service Flooding 攻撃が開始されると，他のシステムも影響を受ける．しかし，このような，直接の相互作用をもたない機能を攻撃することによる間接攻撃の攻撃経路は，ISO 26262 のアイテム定義には含まれず，したがって対応の検討範囲には入らない．さらに，アイテムに含まれていない攻撃点からのサイバー攻撃がある．例えば，車載ネットワークでは，アイテムに含まれていない妥協された ECU からサイバー攻撃が発生する可能性がある．そのような攻撃をも検討対象とするため，[8] ではアイテムではなく，「feature」がサイバーセキュリティの分析対象として導入されている．しかし，feature に含まれる範囲を特定する手法は定義されていない．したがって，機能安全開発のアイテムにおいても，サイバーセキュリティの攻撃経路となりうるアイテム関連の相互作用を網羅的に記述する方法が必要とされている．

3.3 提案方法

ここでは，先の章で提示した問題を解決するため，相互作用をインターフェースを介した相互作用として記述する方式に変わって，共有資源とその管理で相互作用を記述する方式を提案する．先の章でのべた第 1 および第 3 の困難は，ECU ハードウェア，基本ソフトウェア，またはアーキテクチャーなどの共有されている情報およびシステムを介した間接的な相互作用が考慮されていないことに起因する．第 2 のカテゴリーの問題は，既存の製品に属するシステムの相互作用を変更を最小限とする条件を満たしつつ，それらを統合した高度な機能を実現するアイテムおよびアイテム間の相互作用記述は，システム規模の増大に伴い複雑さが増大する事に起因する．言い換えれば，これらの困難は，いずれもア

イテムおよびアイテムの間で，機能によって直接定義されている相互作用以外の潜在的な相互作用が存在すること．さらに，そのような潜在的な相互作用は，インターフェースを介したコミュニケーションで網羅的に抽出し，分析検討することが困難であることに起因している．そのため，複雑化したアイテムや機能間の関係をインターフェースを介した相互作用として記述し，その上で分析検討を実施するに起因する．複雑な機能でなおかつサイバーセキュリティの分析対象とすることができるアイテムの定義を実現するために，共有資源とその管理との相互作用に基づいてアイテムとその境界を定義する方法を提案する．この共有構造を明示的に記述することにより，アイテム間の潜在的な関係を機能追加や資源として追加し，アイテムに追加してアイテム定義後の開発に反映させることを目指す．この新しく導入された構造はインターフェーサと呼ばれている．第 1 に，アイテム間の資源共有は資源によって分類され，その管理方法は 4 つの単純なカテゴリ，すなわちインターフェーサのカテゴリによって分類される．資源の種類は，論理資源 (情報) と物理資源 (ハードウェア，物理資源など) である．資源管理には，資源の移転と共有が含まれる (表 3.1).

表 3.1　抽象化された資源とその管理方法

	転送	共有
情報	通信 (メッセージ転送 RPC)	データ共有 (共有メモリ, 共有オブジェクト) or コード (機能)
物理 資源	物理的移動 (充電)	物理的共有 (通信バス, 電池)

表 3.1 に抽象化された資源とその管理方法の 4 つのカテゴリを示す．これらがインターフェーサを定義する出発点となる．

1. 情報資源の移動は，アイテムや機能間のデータ移動に対応する．データの内容は，コマンドまたはメッセージまたは一般的データのいずれか，または複合物である．管理機構の一例は，通信プロトコルである．

2. 情報資源の共有は，複数のアイテムや機能から同じデータを参照することに相当する．共有メモリの管理機能の例としては，排他制御，分散共有メモリ管理プロトコル，OS 資源制御などがある．

3. 物理的な資源の移動は，物理的な物体の移動，例えば，充電中の電力転送を伴う場合の電力などである．管理メカニズムの一例は，電力供給制御である．

4. 物理資源の共有は，メモリ，通信メディア，バス，電源などのメディアと資源の共有を意味する．管理方法にはバスアービトレーションや時分割制御がある．

この提案では，アイテムの境界は以下のように定義される．

1) 共有資源を定義する．予め，アイテムが実現される対象となる前提システムの情報が入手可能な場合は，それを使用して共用資源を定義する．

2) 共有資源の管理方法を表 3.1 に示すカテゴリの 1 つに適合するように定義する．これはインターフェーサの初期定義となる．

3) インターフェーサの初期定義を絞り込み，各アイテムに割り当てる．この手順では，インターフェーサを複数のサブインターフェーサに分け，それらの間の相互作用を定義することができる．

4) 定義された (サブ) インターフェーサを各アイテムに割り当てる．換言すれば，インターフェーサは，アイテム間の情報，データ，物理量，およびそれらの管理メカニズムの共有および管理を記述する要素として定義される．次の章では，アイテムとインターフェーサとの境界を記述する方法の例を解説する．

3.4 ユースケース

この節では，3 種類のユースケースを検討する．

1) 潜在的な共有に関連する境界の定義と記述の場合

この場合，潜在的に存在するインターフェースを特定する必要がある．例として，1 つの ECU に 2 つのアイテムを実装することを想定する (図 3.2)． ECU，すなわちハードウェアを共有することは，CPU，利用可能なメモリ，IO システムなどのハードウェア資源を共有することを意味する (図 3.2a)．次に，これらの資源の管理を定義する．ほとんどの ECU では，CPU は時分割アプローチを使用して管理され，メモリはあらかじめ割り当てられた修正領域と動的に割り当てられた領域によって管理される．すなわち，2 つのアイテム間の共有 IO は排他的に管理される (図 3.2b)．したがって，この時点で，インターフェーサの共有の対象には CPU，メモリ，IO の 3 つの候補が存在するが，ここでは IO システムに焦点を当てる． IO 資源は排他的に管理されなければならない．したがっ

て，インターフェーサは物理資源：IO，管理：排他制御である．次にインターフェーサの分割を行う．排他制御の実現のためには，IO 資源の要求側 (この場合はアイテム) と供給側 (この場合はインターフェーサ) との間に定められた手順，すなわちプロトコルが必要となる．この時点で，2 つのインターフェーサの組み合わせとしてインターフェーサを決定できる． 1 つは IO 自体の管理であり，もう 1 つはデータとその管理プロトコルへのアクセスである (図 3.2c).

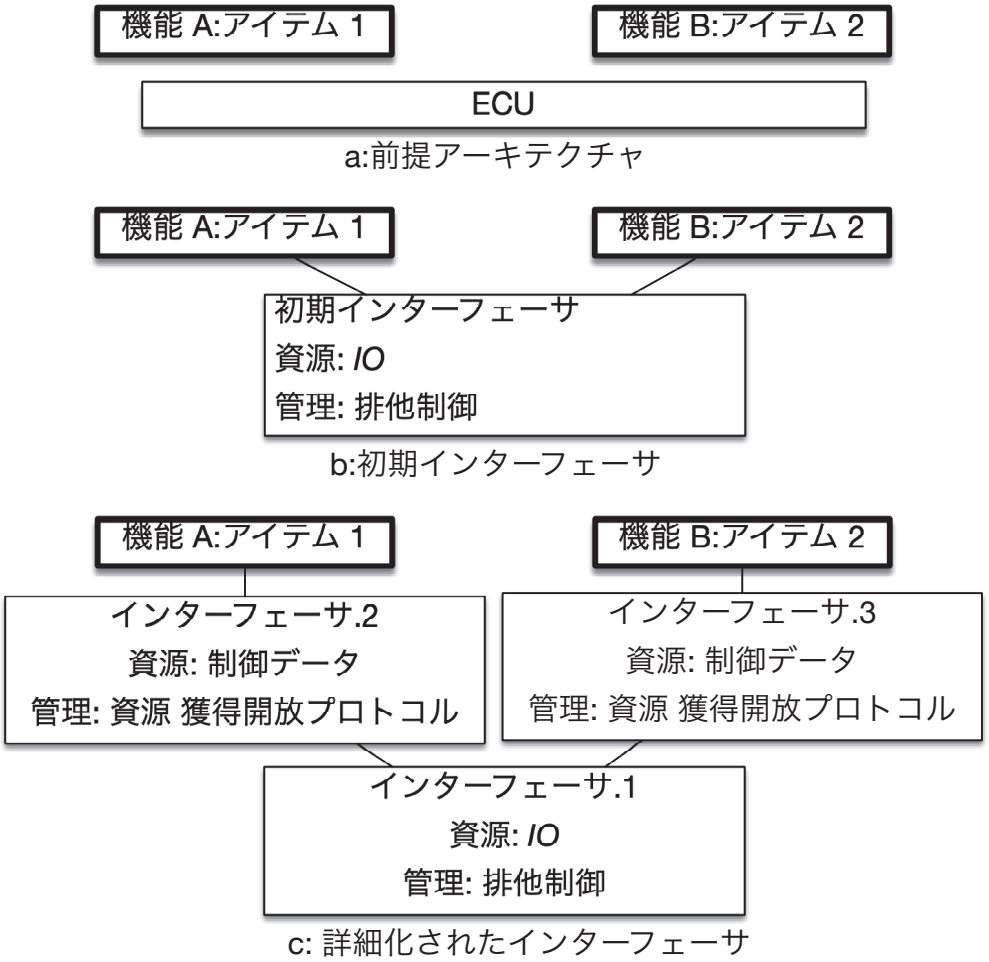


図 3.2　複数のアイテムに共有された ECU の場合

2) 差分開発における製品定義とその境界の場合

この場合，すでに開発されている機能の変更を最小限に抑えるようにアイテム定義を実施する必要がある．本研究では，ステアリングシステム，ブレーキシステム，スロットルシステム，および PAS コントローラシステムからなる PAS を想定している (図 3.3)．最

初の 3 つのシステムはすでに既存の機能として定義されており，ユーザインターフェースシステムと制御対象の制御システムで構成されていると仮定する．言い換えれば，既存の製品は，ユーザインタフェースとコントローラ機能から構成される (図 3.3 a)．また，自動駐車システムは，ユーザインターフェースまたはコントローラー機能をもち，ステアリング，ブレーキ，およびスロットルシステムの制御を共有する．次に，アイテム間で共有されている PAS の状態データと排他制御の管理を定義する．これらは，インターフェーサの最初の説明に必要な資源とコントロールである (図 3.3 b)．次に，インターフェーサを詳細化するために，最初のインターフェーサを 2 つの部分，すなわち，共有状態と一貫性制御に分割する．これらの部品は，事前に定義された製品と新しく定義された PAS コントローラシステムの各アイテムに割り当てる (図 3.3 c)．このようにして，すでに開発された機能と新規機能の境界を明確にすると同時に，従来機能にたいして新たに追加される機能を定義する．

3) サイバーセキュリティを考慮したアイテム定義方法の場合

この場合，直接的なものに加えて，潜在的なサイバー攻撃を特定できるようにアイテムとその境界を定義する必要がある．例として，ネットワークとして接続されたいくつかのアイテムを例として考える (図 3.4)．ネットワークには，CAN ネットワークを想定する (図 3.4 a)．ネットワーク自体は物理的に共有されている．さらに，ネットワーク上のデータフレームは，優先順位および仲裁規則に従って論理的に共有され，管理される．これに基づき，物理：ネットワーク，管理：排他制御というインターフェーサの最初の定義を行う (図 3.4 b)．悪意のある攻撃者は，ネットワークに接続されている別の機能 (たとえば TCU 機能）を侵害して，標的アイテム（たとえば ECU2）を攻撃する可能性がある．この攻撃を考慮するため，最初のインターフェーサを 2 つのカテゴリに分解する． 1 つはネットワークインターフェーサで，その資源はネットワークとバス調停である．もう 1 つは，ネットワークインターフェーサから情報を送受信するインターフェーサである．ここでは，この新しいインターフェーサをノードインターフェーサと呼ぶ．ノードインターフェーサは，先に定めたインターフェーサおよび ECU2 との間の情報を共有資源とし，管理機構をメッセージ通信とする．ノードインターフェーサは ECU2 の境界として取り扱える．すなわち，ECU2 の実現している機能をアイテムとして定義サれているとすると，ノードインターフェーサはアイテム境界である．悪意のある攻撃は，このノードインター

フェーサの攻撃とすることができる．言い換えれば，アイテムの定義にノードインターフェーサを追加することで，他のアイテムからのサイバー攻撃を分析できるアイテムが定義できる．これは，第 2 章で導入した拡張アイテムの Exposure Control Point (ECP) に相当する (図 3.4 c)．さらに，ネットワークインターフェーサの管理を変更すると，ノードインターフェーサの攻撃条件が変更される可能性がある．たとえば，ネットワークを 2 つのサブネットワークに分割し，それらをゲートウェイ ECU などの新しいアイテムで接続すると，他のサブネットワークからの攻撃が制限される可能性がある (図 3.4 d)．

3.5 まとめ

本研究では，インターフェーサを導入して新しいアイテム定義方法を提案した． 特に，アイテム境界とその管理で共有される論理的および物理的資源に焦点を当て，4 つの簡単なカテゴリを使用してインターフェーサの構成要素を抽出する方法を提案した． 資源を共有することで，従来のアイテムの細かいサイズによって遠隔のサイバー攻撃も捕捉されると公式化している． 複数のアイテムを統合する洗練された機能の定義において，提案された方法はアイテムの分解を容易にする．また，第 2 章で提案した各区帳アイテム定義においても，インターフェーサーの導入により定義できる．このような共有による記述は，高度化，複雑化の傾向がある車載 E&E システム開発において，網羅性の確保や，拡張アイテムの定義などによりサイバーセキュリティ対策にも有効であると考える．今後，継続してインターフェーサをキーとした車載 E&E システムの複雑性低減の有効性と応用としてのサイバーセキュリティ設計手法を検討したい．

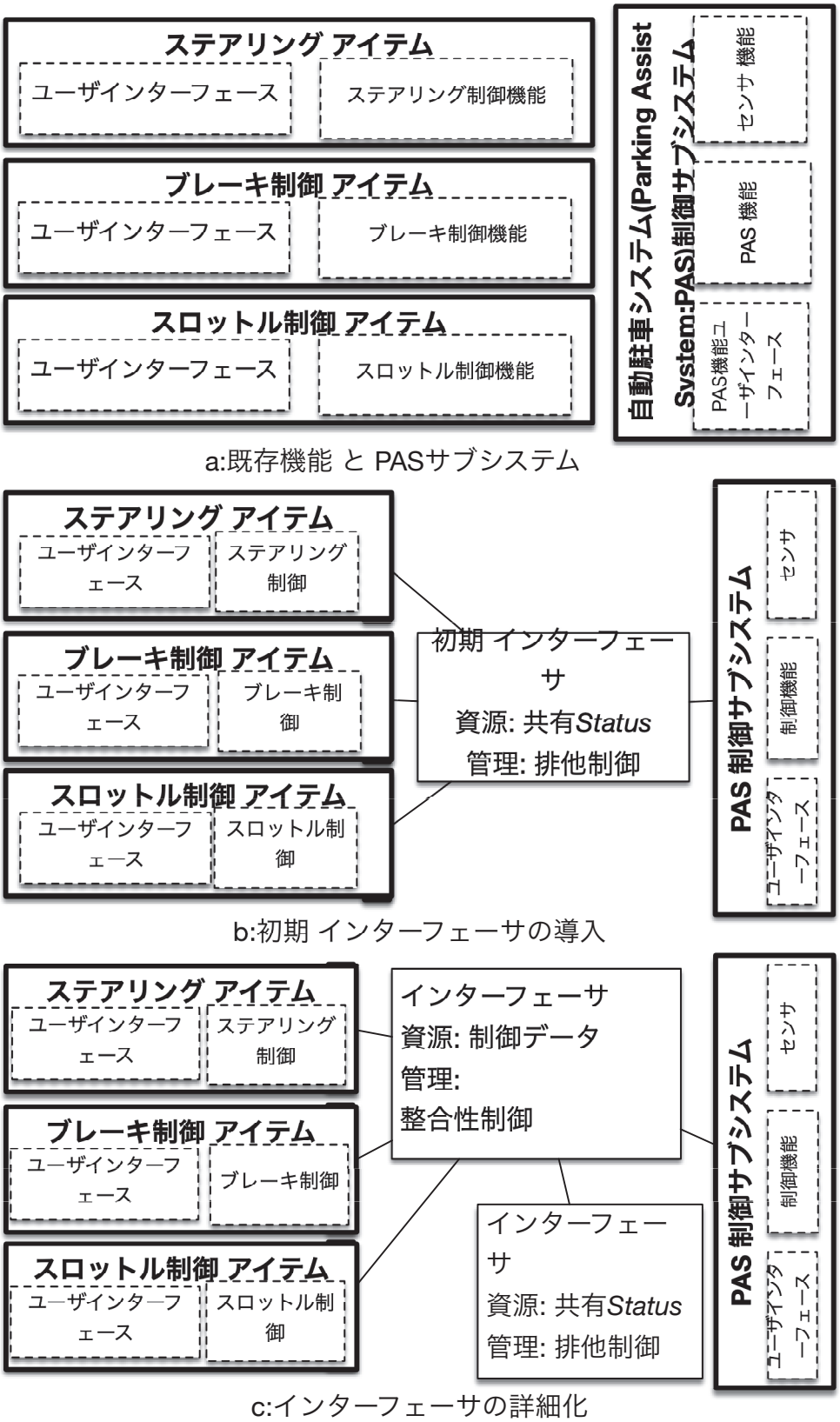
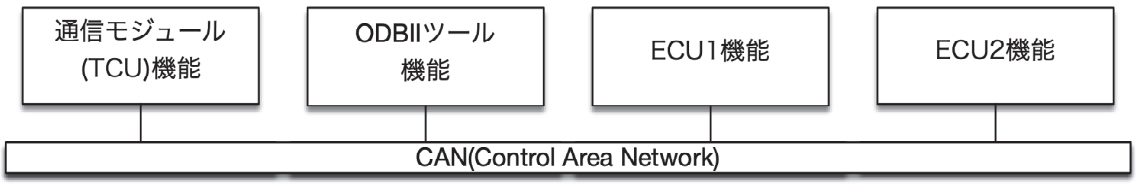
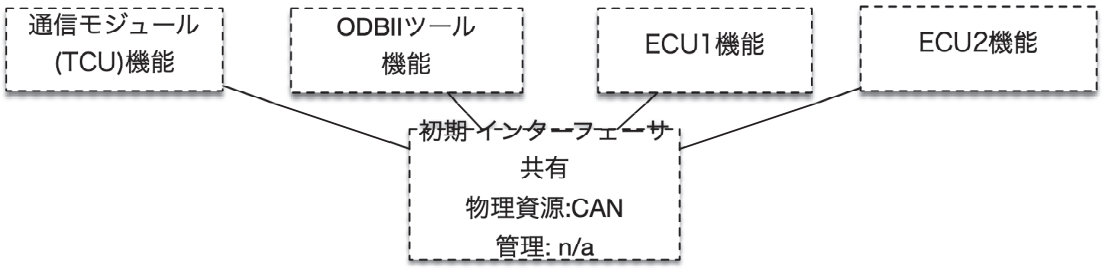


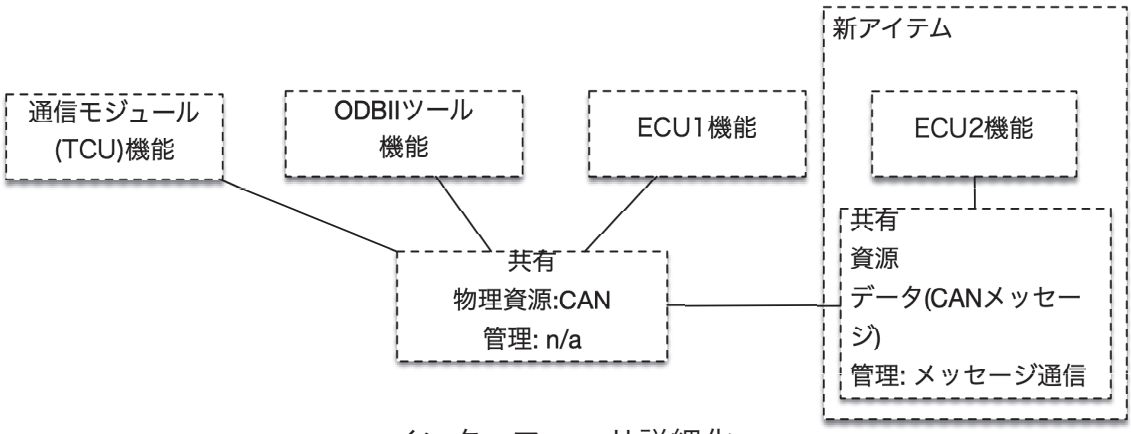
図 3.3　差分開発における製品定義とその境界の場合



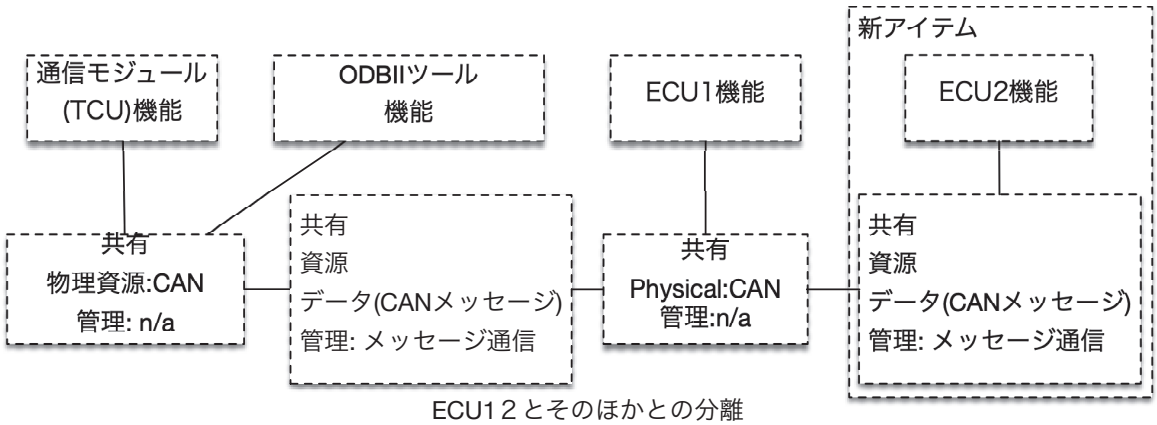
a. ECUネットワークの前提アーキテクチャ



b. 初期 インターフェーサ導入



c. インターフェーサ詳細化



ECU1 2 とそのほかとの分離

d. ECU1,2とのインターフェーサによる分離

図 3.4　車載ネットワークシステムでのサイバーセキュリティを考慮したアイテム定義

第 4 章

構造化ポリシーに基づく車載 E&E システムのサイバーセキュリティのデザイン手法の検討

4.1 はじめに

今日の自動車に搭載されている機能の多くは，車載 E&E システムで実現されている．たとえば，パワーステアリングシステムは，車速などのセンサー情報を入力とし，運転者の操作するハンドル操作を補助するアシストトルクを与えるアクチュエータとそれを制御する電子制御ユニット (ECU) で構成されている．また，近年，市販車に導入されつつある先進運転支援システム (ADAS) では，複数の車載 E&E システムを協調させて機能を実現している．さらに，車両自体の機能に加え，車両外部との通信を介して提供されるサービスの企画・検討・開発および法制度の整備や標準化が進められている．たとえば，ソフトウエアの不具合や新たな機能を追加するための車載 E&E システムのソフトウエアの無線通信を経由した更新機能．車両の状態をモニタリングし，異常動作や故障の兆候などを検知する遠隔診断や遠隔車検，車車間通信 (V2V) または路車間通信 (V2I) 通信による車同士での道路状況の共有や，インフラからの周辺状況の情報提供などによる安全運転のサポートが挙げられる．近い将来，これらのサービスはネットワーク接続された車両であるコネクティッド・カーの中核機能になることが期待されている．

しかし，通信機能を利用したサービスの実用化により，外部ネットワークからの車載 E&E システムに対するサイバー攻撃のリスクが懸念されている．実際に，いくつかの論文やワークショップで，このような実際の攻撃が実証されている [21][22]．また，自動運

転や先進運転支援システムなどの普及により，事故や障害が発生した場合，それらのシステムの動作記録が改ざんを受けていないことの保証も要請されている．さらには，ソフトウエアを含めた車両自体が製造時および保守実施時に対応した状態であることを担保するための対策の必要性も懸念されている [23]．これらの対策や保護を実現する技術として，設計製造段階では，検証のための手法や製造プロセスの管理が検討されている．また自動車の出荷後の運用から廃棄に至るまでの対策や保護技術として設計製造および運用に対してサイバーセキュリティ技術の適用が検討されている [24]．

車載 E&E システムへのサイバーセキュリティ技術の適用では，IT システムと同じくリスクベースのアプローチが取られる．リスクベースのアプローチとは，保護すべき資産を特定し，それが侵害されたリスクの大きさを評価し，対策の要否を判断の上，対策を策定，実施する一連のプロセスである．自動車における保護資産である最も重要な機能とは，安全に関連した機能である．現在，自動車の開発における安全設計は，機能安全の考え方で行われており，特に車両内の電気および&または電子 (E&E) システムは，国際規格 ISO 26262 に規定されている機能安全機能開発プロセスに準拠して実施されている．リスクを評価する上で重要な情報である攻撃分析などは，システムの分析粒度と整合性を取るべきである．

ISO 26262 に準拠した車載 E&E システム開発では，開発対象を，アイテムとよばれる，車両レベルでの機能によって定義記述する [19]．アイテムで定義される主な内容は，(1) アイテム外部との相互作用，(2) アイテムを構成する機能と機能間のおよびアイテム外とのインターフェースである．これらは機能間でのデータフローと考えて良い．また ISO 26262 では，アイテムで定義された機能を，前提アーキテクチャと呼ばれるシステム・アーキテクチャの各要素に割り当てる．一方，一般にサイバーセキュリティにおけるサイバー攻撃の分析はデータフローに対する攻撃の分析が基礎となる．したがって，アーキテクチャの各要素へ割り付けられた機能間のデータフローをサイバー攻撃分析することは，車両レベル機能に対するサイバーセキュリティ対策の基礎となる．したがって，サイバーセキュリティ設計においても，アイテム定義を分析対象とすることの妥当性は高いと考える．

また，ISO 26262 では，アイテム定義に割り付けられた機能要件を，さらに実装を前提とし構成要素に分割し，基本設計を構成する個別の要素に割り付けてゆく．アイテムをサ

イバーセキュリティ対策の対象とした場合，ISO26262 の要件の詳細化に相応して，サイバー分析およびサイバーセキュリティ対策の粒度を上げてゆくことができる利点がある．

アイテムは車両レベルの機能であるが，個々のアイテムにおいて，他のアイテムとの間には，直接の機能的な相互作用に加えて，アイテム間での機能，それらを実現する OS などの基本ソフトウエアや CPU，バス，IO，ネットワークなど物理的リソースなど，さらには，アイテムそのものの共有など，様々な形の共有によるものが存在する．特に，先進運転支援システムのように複数の車両機能を統合する機能では，機能を統合し，かつ競合する制御を調整するための機能が，それぞれ個別の車両機能にも必要となる．そのため，個々のアイテムにおいても統合機能を考慮した分析，設計を考慮する必要がある．

この統合機能の追加は，結果として新たなサイバー攻撃の対象となり，サイバーセキュリティリスクの再評価が必要となる．たとえば，スロットルシステムに対して，動作状態の同期インターフェイスから，動作モードをアダプティブオートクルーズ機能とするようななりすまし攻撃が実施された場合を考える．この場合，スロットル制御のみがオートクルーズモードとなるために運転者による速度の調節ができなくなるリスク事象がある．このように，従来機能を統合して高度な制御機能を追加した場合，追加された制御機能だけでなく，追加された統合機能を攻撃することにより，従来からある機能にも新たな攻撃が可能となる．自動車の開発では，差分開発を中心とした機能の再利用が中心であるが，このような再評価の発生は，差分開発のベースとなる機能の再評価および開発修正が必要となり開発コストの増大を生む懸念がある．

また，一般に，このような複合システムでは，規模の増大にしたがい，加速度的にシステム間の相互作用が複雑化する．高度な車両機能を実現するために複数のアイテムを統合し，機能間の連携が密接になった場合も同様の状況が発生すると考えられる．このような場合，複合システムに含まれる機能間，機能と機能外部の相互作用が複雑化し，その結果，機能を記述するデータフローを網羅的に抽出，分析することが困難になる．サイバー攻撃への対抗策は，サイバー攻撃の対象となる処理のデータフローを分析し，一部もしくは複数の地点で実施される．したがって，データフローの網羅性が確保と分析が困難となる場合，結果としてセキュリティ対策の検討の網羅性も同時に保証困難となる．また，データフローの網羅性が確保された場合でも，分析対象の量の増大は当然として，新たな攻撃手法が見つかった場合の影響範囲の分析や新規対策の実施の検討の実施には，データフロー

に対する再分析が必要となる．したがって，機能の高度化に伴う，急速な開発コストの増大は避けられない．

これらの問題を解決するために，本章では，車両システムのためのポリシーベースのアプローチをサイバーセキュリティに適用することを提案する．サイバーリスクアセスメントの標準的なアプローチでは，保護される資産が定義され，これらの資産に対する脅威が各機能ごとに導出され，評価される．本章で提案するアプローチは，相互に密接に関連している機能のグループにサイバーセキュリティポリシーを適用する．各機能セットのポリシーは，そこに属するすべての機能が従わなければならない一連のルールを決定する．IT システムにおける Defense in Depth アプローチと同様，全体のサイバーセキュリティポリシーにはその部分であるサブセットのサブポリシーが含まれている．ポリシー内部に配置された機能および機能間通信はすべて当該ポリシーに準拠しなければならない．この場合，いかなる攻撃においても，攻撃の最初の段階でポリシーに従わないと実施できない．このことにより，網羅的な相互作用の抽出条件が緩和されると同時に，対象とすべき攻撃の範囲が狭められ，脆弱性評価のコストが削減されることが期待される．

本章は以下のように構成されている．4.2 節では，自動車の安全とサイバーセキュリティのための E&E システム設計と，自動車サイバーセキュリティの設計の難しさについて説明する．4.3 節では，サイバーセキュリティ要素の基本的な考え方と構造化されたポリシー設計を記述する．4.4 節では実施シナリオを示す．

4.2 自動車 E&E システム開発におけるサイバーセキュリティリスク対応の問題

一般に，IT システムのサイバーセキュリティ対策では，リスクアセスメントベースの手法が取られる．これは，自動車などの制御システムのサイバーセキュリティ対策においても有効な手法であると考えられており，現在提案されているガイドラインやベストプラクティスはこの手法をベースにしている．制御システムのサイバーセキュリティに関しては，監視制御とデータ収集 (SCADA) システムに関する先行研究がいくつか存在する [25]．さらに，IEC62443[7] による標準化が進められている．SCADA システムでは，システムの要素である，センサ，コントローラ，制御プロセス，ネットワークおよびデータベースなどによってシステムが構成される．これは，一般的な IT システムと共通してお

り，また，これら間の相互作用も IT システムで利用されている技術と共通性が高い．また，処理を行うハードウエアやソフトウエアは，情報システムと共通性が高い実装アーキテクチャを基盤としている．そのため，IT システムにおける脅威の分析やシステムや実装の持つ脆弱性の保護，脅威を軽減・阻止する手法などが適用可能である．

一方，車載 E&E システムは，車両レベルの機能で定義されたアイテムとよばれる開発対象の結合で定義される．一般に，アイテム定義の作業は難しいと言われている．これは，アイテム自体の複雑さに加えて，他のアイテムからくる影響や相互作用をアイテム境界として明確に定義することが難しさに起因する．この簡単な例は [20] で与えられている．このようなシステム記述の複雑さを，簡単な要素に分解して記述する手法として，従来の研究では，システムの機能分割を検討し，車両の機能ごとに階層分解を行っている [26]．しかし，このような階層分割の手法を用いても，複雑な車両機能のためのアイテムを定義することは，依然として難しい．さらに，アイテムは車両レベルの機能実現に特化したシステムの結合で構成されている． IT システムのように汎用的なものではない場合が多い．さらに，これらのシステムの実現は，リアルタイム性に加えて，適切なコストと信頼性を実現するために，機能および利用条件に特化した要件分析，設計実装が行われる．また，近年では自動ブレーキや車間維持，車線維持など，複数のアイテムの機能を統合して一つの高機能なシステムを定義しており，構成要素であるサブシステム同士の関連性が密となり，システム全体の複雑さが高いものがある．そのため，構成要素の結合が疎であり，かつ汎用技術を用いている IT システムのサイバーセキュリティ分析や対策の有効性は，車載システムのそれに対しては限定されており，対象とするシステムもしくは複数のシステムが組み合わされる車両タイプごとの個別に詳細な分析が必要とされる，また，脆弱性や脅威に対する対策も，車両システムや車両タイプごとに個別に対策を検討する必要がある．要素技術としては共通性があった場合でも，その適用に際しては同様である．また，IT システムでのセキュリティ対策では保守管理部門による運用技術による対策も重要とされる．一方，車載 E&E システムは，車載 E&E システムの非専門家である一般ユーザが使用するため，専門家を要する運用技術による対策は困難である．また，開発に際しては，IT システムにおける分業体制ではなく，車メーカを頂点とする垂直分業による分散開発体制を取る場合が一般的である．この体制では，開発システムに関する知識は各分業のレイヤー固有の情報として保持される．このことも，汎用的な技術を用いて

構築されている一般的な IT システムの構築とは異なる点である (表 4.1).

表 4.1　車載 E&E システム開発と IT システム開発の相違点の概略

	車載 E&E システム	IT システム
サブシステム間の結合	密結合が存在する	基本的に疎結合
構成要素のアーキテクチャ	機能最適で共通性が少ない	共通技術を利用
開発体制および開発対象に対する知識	OEM からソフト／ハード開発まで階層化された分散開発. 階層間で開発対象に対する知識の共有が少ない	各開発者間で, 階層は存在するものの, 共通技術を利用している部分の知識を共有する開発

以下，本節では，これらの相違の内容を解説したうえで，車載 E&E システムのサイバーセキュリティ設計／開発での，分析・評価・対策検討，脆弱性分析，および実装に関して，IT システムにおけるそれとの相違を記載する.

4.2.1　サブシステム間の結合

まず，車載 E&E システムの開発プロセスである ISO 26262 における開発成果物を IT のそれと比較する．以下，開発成果物は ISO 26262 における開発成果物を検討の対象とする．車載 E&E システムでは車両レベルでの機能をアイテムとよぶ開発対象として分割する．車両システム全体からみるとアイテムはサブシステムである．例として，パワーステアリング，電子車体姿勢制御，エンジン制御がある．これらのアイテムはそれぞれ単独に存在しているのではなく，機能レベルで相互に関連をもつ場合が多い．たとえば，電子車体姿勢制御は，車両がカーブを曲がる際などに車が不安定な挙動を起こした場合に車両の状態に対応して，４つの車輪に装着されたブレーキを制御して車体の挙動を安定に戻す機能である．この機能は，車体にかかっている加速度やタイヤの回転数などを入力として，左右のブレーキの制御を行うとともに，エンジンの回転数も制御することでより高い安定性を実現する．車体制御機能の動作中は，エンジン制御機能は，アクセルペダルからの指示と，電子車体姿勢制御からの指示を調停してエンジンの制御を実施しなければならない．また，姿勢が安定し，車体制御機能の動作が不必要となった後には，アクセルペダルからの指示による制御に戻さなければならない．また，ブレーキシステムは，車体制御機能の動作中は，ブレーキベダルからのブレーキ操作に加えて，電子車体姿勢制御からの制御指示も調停してブレーキの制御を実施しなければならない (図 4.1)．現状の車載

E&E システムではさらに複雑な配線となっている．

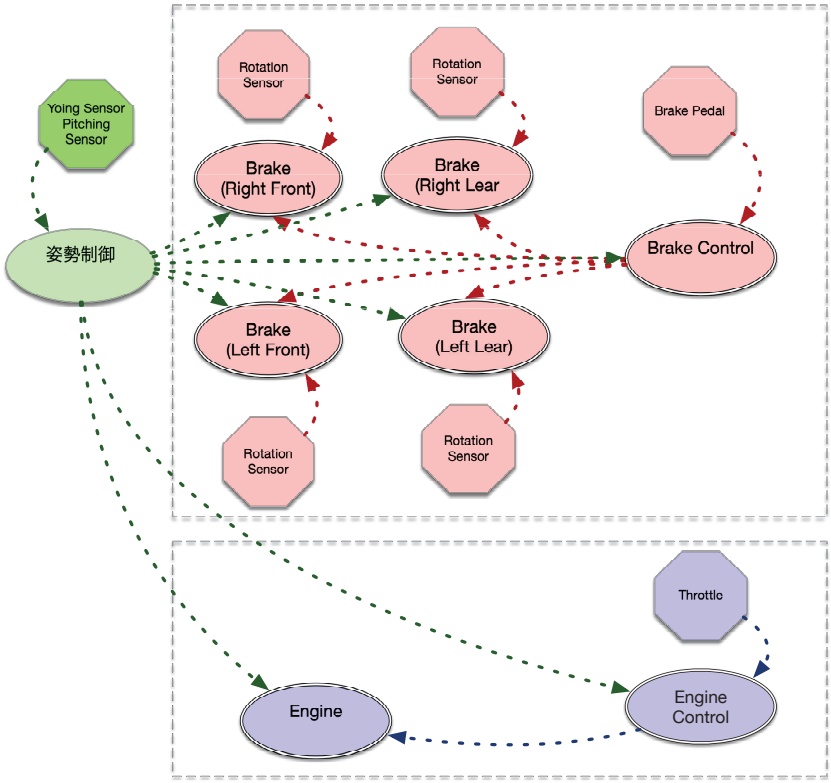


図 4.1　車載 E&E システムでの機能制御の例（点線部分は，単独機能（ブレーキ，エンジン制御）二重線部分は機能調停が必要な部分）

このように，現代の車載 E&E システムでは，複数のアイテムが，単独での機能を持つ一方，それらの機能を関連，協調させることにより実現する機能がある．そのため，複数のアイテムの協調により実現させる機能では，サブシステム間の動作の同期が必要となる．例えば，LKAS もパワーステアリングも操舵に関わる機能であるが，ユーザが操作を開始した場合には LKAS はユーザの操作に委ねるために，その操作を停止しなければならない．しかし，一方で，この様な調停の仕組みそのものが攻撃の対象となる．しかも，調停のような２つの機能の同期に関る機能は，必ずしも無効化や偽装する必要はなく，遅延などのタイミングのズレを誘発することで十分な脅威となり得る．たとえば，先の例であげたハンドル操作では，操作の切り替わりのタイミングをずらすことは，操作者に違和感を与え，それによってハンドル操作のミスを引き起こす要因となりえる．ハンドル操作のような単一の機能ではなく，これらは，高度に関連し合う機能では更に状況は複雑になる．例えばアクセル制御とブレーキ制御では，エンジンブレーキの効果とあわせてブレーキを

調整しなければならない．さらに，左右のブレーキの調整により車体の横滑りを制御する機能が働いた場合，この機能から，左右のブレーキの制御機能に干渉が入る．この様な場合では，システムの同期に加えて，量的な指標を含めた協調動作が必要となる．サブシステムでの制御が複雑になるにつれ，状態の確認や調停に利用されるパラメータや同期に必要な情報が個別の場合と比較して増大する，一方で脅威となる事象も，攻撃対象となる資産が増加するため増加し，それら増大した資産が侵害された場合に発生する事象も分析が必要とあるため，必然的に分析のコストが高くなる．また，ADAS などの先進システムに限らず，自動車に搭載される機能は，部品故障時の重大事故の誘発を軽減，阻止するために実施される機能安全設計が実施される．これは，故障時のハザード分析とリスクアセスメントの結果から導出される安全目標に対して，それを実現するための機能要件が定義され，その機能要件を，システム上の構成要素に配置することで要件が定義される．たとえば，故障を検知し，検知した結果の動作要件が定められ，それらがサブシステムに配置される．さらに配置された要件は，現実に実装可能な機能として要件が詳細化される．例えば，故障の結果，異常な入力が発生した場合，入力値をモニタして，それが異常値とは判定されるための機構を必要ならば追加する．この機能安全機能も，一種の保護すべき機能と考えると，セキュリティ攻撃の対象と見ることができるため，サイバーセキュリティ分析が必要である．

4.2.2 構成要素のアーキテクチャ

このように，機能的なレベルでのサイバーセキュリティ対策が設定できても，対策の実装において汎用技術が利用できる IT システムの場合と異なり，システムや ECU 個別の分析が必要となる．車載 E&E システムでは，機能をコストや利用環境などの制約下で実現するために適切なハードウエア選択を行う．この場合，コンピュータとしてのアーキテクチャの統一性は次に置かれる．例えば，カーナビゲーションシステムでは，大量のデータを扱ったり，標準的な通信プロトコルを用いる必要から Microsoft Windows や Linux などの汎用高機能 OS が利用される．また，TCU/V2X 機器などでは，I-TRON などの組込み OS から汎用組み込み OS が利用される一方，ゲートウエイなどの車載ネットワークを制御する ECU では，極めて早い起動速度と，接続されている複数のネットワーク間のフレーム転送を極めて小さな遅延で行う必要性などから，受信割り込みの処理を最優先

した，OS の無いのシステムを使用する場合がある．また，実時間制御の制約が厳しい一方で，複雑な演算処理を必要とするエンジン制御においては，複数コアを搭載したマイクロコントローラを利用し，コアのそれぞれに特定の機能を割り付けて動作させる場合も存在する．このように実現方式が，個々の ECU によって大きく異なる場合が多いため，想定可能な脅威に対して，現実に可能な攻撃を抽出するには，実装に関する情報が必要である．これらは，車両における脅威を評価する要件の定義フェイズでは得にくい情報である．また，同様に，実装に関する情報が必要な，対策を実装する際のコストについても，評価時には正確には把握することが困難である．

4.2.3 車載 E&E システムのサイバーセキュリティ設計／開発プロセス

サイバーセキュリティシステムの開発は，対象定義，リスク評価および対応とその実装，および評価としての脆弱性評価の一連の手続きで行われる．ここでは，車両の開発プロセス，及びそのマネジメントに起因する困難も含めて分析する．

車載 E&E システムの開発では，分散開発体制で行われることがほとんどである．これは，車両レベル，システムレベル，部品 (ECU) レベルごとに異なる開発者が開発するスタイルである．この分散開発のスタイルでは，各開発者が持つ情報が本質に異なる．すなわち，車載 E&E システムのサイバーセキュリティを実現する開発者間の知識が偏在しており，かつ制約下での性能実現が優先されるため，共通基盤を利用するよりも部分最適化が優先されることに起因する問題である．IEC62443 では，開発に関係するステークホルダーを，オペレータ，システムインテグレータ，およびシステム開発者の 3 つのカテゴリに分類している．システムインテグレータは，システム全体のサイバーセキュリティを設計するのだが，サブシステム間の相互通信は，IT システム設計と類似もしくは同一の基盤を利用しており，ネットワーク，サーバ，データベースなどのシステムの各コンポーネントは，基盤となるアーキテクチャが IT システムのそれと同様もしくは類似したものに基づいている．共通のアーキテクチャの理解に基づいて，システムインテグレータと，システム開発者は相互に脆弱性についての情報を共有することができる．たとえば，システムインテグレータは，サーバが内部に置かれるのか外部に置かれるのかによって必要な脆弱性検査の手法を指定することなどが可能である．したがって，システムインテグレータは，IT サイバーセキュリティの知識と方法を利用することが可能である．一方，車

載 E&E システムの開発では分散開発が広く採用されている．この開発体制には，OEM，Tier-1，Tier-2 または Tier-3 の 3 つのカテゴリのステークホルダが存在する．また，それぞれに異なる設計対象の枠の中で，上流開発から与えられた要件に従って適切な設計／開発を行う．しかし，ECU は制約上，目的の実現に対して最適化されたハードウエアやソフトウエアを使う．さらに問題を複雑にするのは，ECU などの内容は企業の秘密情報，特許や保有するノウハウにあたるものが含まれている場合が多い．そのため，情報の共有はつねに制約を受け，部分的なものとなる．

そのため，機能間の相互関係が複雑化かつ増大し，かつ開発者ごとに情報が分割されている場合，システム全体や個別の機能に対するサイバーセキュリティ脅威を詳細化することは一般に極めて困難である．これは，サイバーセキュリティリスクの分析，特に脅威と関連する脆弱性の分析と，それに基づく対策の実施に際して多大なコストの発生を意味する

知識の偏在が及ぼす最大の影響を受けるものがリスク・アセスメントである．また，現在の主流の脅威分析手法はデータフローをその分析の基本データとするものが多い．たとえば，車両用のリスク分析手法である JASO-TP15002 もその一例である．そのような，リスク・アセスメントは，データフローに基づく脅威源の抽出と脅威事象の特定，脅威事象の発生可能性の特定，影響度の特定を行い，最終的に発生可能性と影響度からサイバーセキュリティリスクのスコアリングの一連の作業で行われる．そのために，まず，データフローに基づいて脅威源の抽出と脅威事象の特定作業を検討する．複雑なシステムに対する脅威を抽出する場合，一般にはその複雑さに比例して脅威事象の量も増大する．また，脅威導出においても，たとえば STRIDE 手法を用いた場合，現行の脅威種別のみならず機能相関が損なわれた結果発生する脅威などの種別を追加する必要がある．[27]．たとえば，複数サブシステム間の同期が必要である場合，それらの機能の時間的なズレを発生させる事も脅威となりうる．このような事例では，単に脅威抽出のためのキーワードが増加するだけでなく，時間的なズレのような，システムとその外部との相互作用およびシステム内部のデータフローを念頭において脅威事象を抽出しなければならず，分析における脅威導出の難易度が高くなる．

また，開発対象に対する要件の分析や，設計が進むに連れて進行する開発対象の設計粒度の詳細化に適合した，脅威事象の詳細化と修正を行うためには，OEM とサプライヤの

間で脅威に関して共通の情報を持ち，車両レベルから ECU やそれを構成するソフトウエア・ハードウエアに至るまで一貫した脅威に関する情報を構築しなければならない．しかし，自動車開発の主流プロセスである分散開発において知識の偏在がこれを困難にしている．OEM は，車両レベルの影響度を考慮したリスクアセスメントを行うことが可能である．一方，ECU を製造するサプライヤは，製品である ECU において脅威事象の対象となる脆弱性の詳細について評価しうる情報を持っている．一方では，車両全体もしくは車載システムの全体における ECU がどの様な攻撃経路で攻撃されうるか，また ECU に侵入された場合の影響範囲についての情報は持ち合わせていない．サプライヤが持つシステム境界に関する情報は，OEM の実行した機能レベルの分析に基づく重要度判定に従った，ECU の機能に対する脅威への対抗機能の要求である．したがって，サプライヤで，ECU 開発におけるリスク評価や対策決定において必要とされる脅威事象の実現可能性の詳細化を行うことは困難である．また，これらの情報を欠いているために，サプライヤは，ECU に対する脅威事象の実現可能性に関する情報を特定または詳細化することも困難である．そのため，脆弱性評価において，脅威に対するの対処優先度を想定することが出来ない．これらの理由により，サプライヤが脆弱性の評価を行う場合，脅威想定をサプライヤ視点で作成して対応するか，すべての想定されうる脅威に対して対応するかのいずれか行わねばならない．一方では，脆弱性評価の対象となるインターフェースは ECU 機能の増大に従い加速度的に増加している．したがって，サプライヤにおいて脅威想定を内部で行った場合でも，網羅的な対策を行った場合でもまた，脆弱性対応に費やすコストは増大する恐れがある．

4.3 車載 E&E システムサイバーセキュリティのための構造化セキュリティモデル

前節にあげた問題点をまとめると，1）車載 E&E システムは機能が高度化するにつれ，機能間の協調動作が増大し，かつ，これを構成する要素間のデータフローが複雑化する一方，2）車載特有の理由により，個別最適設計された実装アーキテクチャが使われており，脅威や脆弱性の分析はシステムや構成要素個別に行う必要がある．さらに，3) 複雑化したデータフローが分析対象となっているにもかかわらず，開発対象に関する情報は，分散開発により知識が分散しており，2）とも相まってサイバーセキュリティに必須のリスクア

セスメントや，脅威／脆弱性分析の実施に際して制約事項となっている，システムを構成するの３点にまとめられる．すなわち，開発の参加者が，データフロー上に脅威や脆弱性を分析するために必要な情報を共通で情報として持っていないにもかかわらず，データフローを唯一の分析手法としていることによると考えられる．そこで，ここでは，データフローに対する分析を単一アプローチとすることによるサイバーセキュリティ設計／開発上での問題点に対して，構造化したセキュリティポリシーの導入により，データフローをセキュリティポリシーが適用される境界毎に分割することにより緩和・解決する手法を提案する．

セキュリティポリシーとはある特定のグループや範囲に対して適用されるセキュリティ上の規則のセットである．セキュリティポリシーによる情報セキュリティ対策は IT システムでは一般に行われる．例えば，企業内部に入り情報システムを利用するにあたって IC カードによる入退出管理が行われ，情報機器の利用に際しては，常時 IC カードによる確認が行われるポリシーで情報システムが管理されている場合を考える．この場合，社内，社外という区分け（ゾーニング）と IC カードによる出入り管理および情報機器の利用により，不正侵入や，他人へのなりすましを，ポリシーに準拠した監視方法で，確認することが可能となる．さらに，重要な情報を取り扱う部分を区別する必要がある場合には，同じ構造を入れ子にすればよい．このようなポリシーによる管理構造は，他にも，ファイルシステムへのアクセス制御などで利用されている．

一方，車載 E&E システムでは車両レベルの機能を実現するサブシステムから構成されている．一般にサブシステムは，さらにそれを構成する複数のサブシステムから構成される．その構成上，ポリシーとはサブシステムである ECU やその更に詳細な機能，また逆に複数の ECU からなるサブシステムの間の機能の利用や情報の伝達に関する規則となる．すなわち，同一のセキュリティポリシーが適用される範囲内では，それに含まれる要素間での機能や情報交換が可能であり，それ以外のポリシー適用部分からの機能利用や情報交換を制限するという構成をポリシー間で持つことにより車載 E&E システムとの整合性が高くなると考えられる．そこで，システムのセキュリティポリシーの実現手段としてセキュリティポリシー要素 (SPE) を導入する．システム全体のセキュリティポリシーは，SPE の組み合わせとして表現される．上位 SPE に属する SPE はサブ SPE と呼ぶ．サブ SPE は，開発対象内のサブシステムのグループに適用される．サブシステムに含ま

れる要素は互いに密接に関連しており，同一のセキュリティポリシーで管理する．つまり，SPE は，SPE に含まれているサブシステムにたいし，SPE で存在するためのセキュリティ要件を設定する．具体的には，SPE は 2 つのポリシーで構成される．1 つは SPE の境界にあるポリシーを，もう一つは，SPE の 内部ポリシーで構成される (図 4.2).

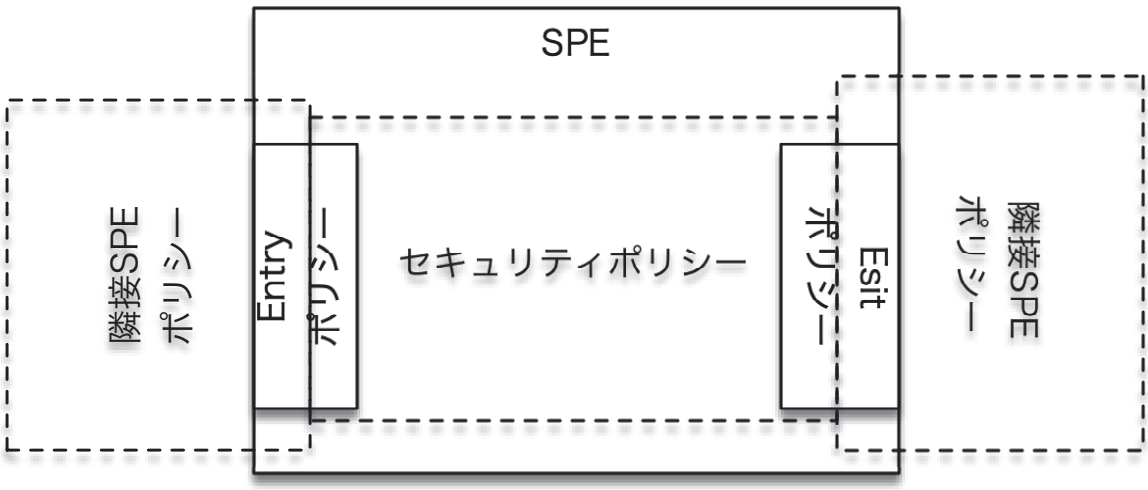


図 4.2　SPE の基本構造

境界ポリシーは，ポリシー内部に入るための規則およびポリシーから出るための規則で構成される．これらの規則をここでは，Entry ポリシー，Exit ポリシーと呼ぶ．すなわち，Entry ポリシーは外部の入力を，内側にいれ，内部のポリシーに適合させるためのポリシー，Exit ポリシーは内部から外部への出力を外部に出力し，さらにそのポリシーに適合させるための構造である．In/Out 規則の例はそれぞれセキュアコーディングにおける入力および出力 validation に相当する．内部ポリシーは，SPE の内部に含まれる機能が満たすべき条件となる．これは，ポリシー内部の処理や機能間のデータ交換において満たさなければならない規則である．Entry/Exit ポリシーに加えて内部ポリシーは，内部の状態が常にセキュアであり，かつ内外との相互作用も管理されていることの評価規則の導出の基本となる定義である．

この SPE を構造的に組み合わせることにより柔軟にシステムに対応できるセキュリティポリシーの構造化を実現する．ポリシーの組み合わせに関しては，均一，多層，分離，格子型の構造およびその組み合わせなどが提唱されている [28]，[29]，[30]．ここでは，これらの構造を基本に車載システムの機能構成に対応したポリシー構造の演算を以下の包含，独立，統合，分散の 4 つのカテゴリに要約する (図 4.3).

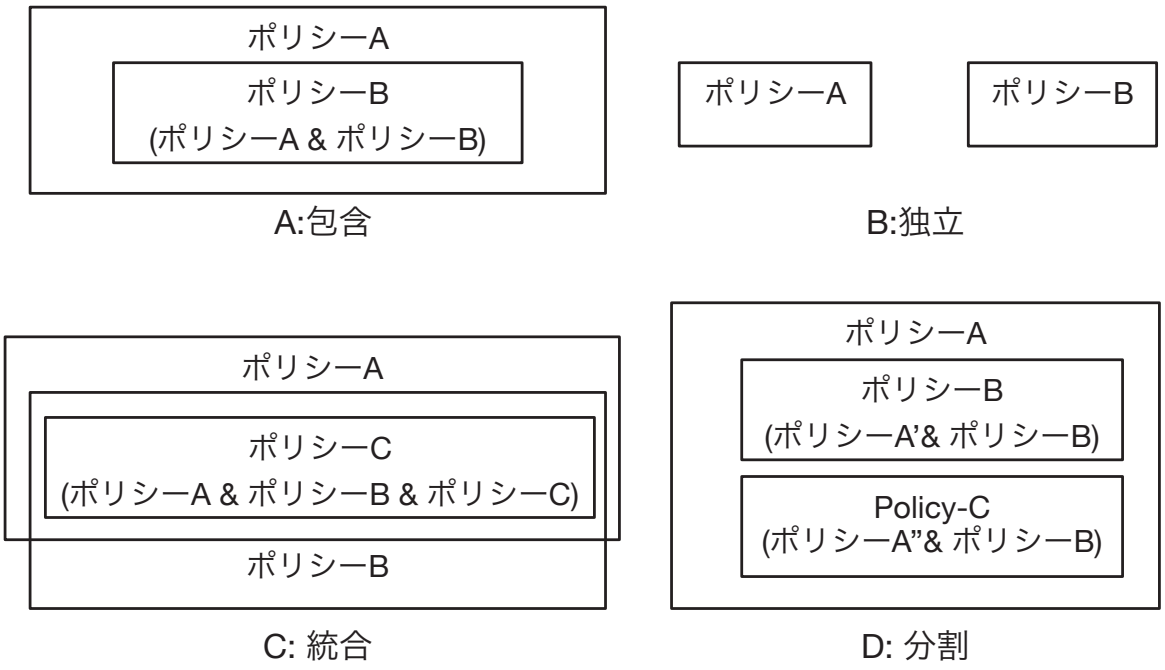


図 4.3　4 つの SPE 間関係の概略図

A. 包含 (inclusion)

包含は，SPE の内部にさらにサブ SPE が存在する構成を表す．サブ SPE 内には，SPE およびサブ SPE に対するセキュリティポリシーがある．この構成の実装では，サブ SPE に含まれるコンポーネントは，サブ SPE の内部ポリシーに従う．サブ SPE の Entry/Exit ポリシーは，サブ SPE 自体が上位 SPE のポリシーに従うための条件を満たす．この構成では，SPE の内部サブシステムが SEP ポリシーと上位の SPE のポリシーの両方によって保護されているため，悪意のある攻撃者が SPE 内のサブシステムを侵害することは困難となる．また，上位 SPE に包含される側の SPE から見れば，同じく包含されている SPE との相互作用が守るべきポリシー定義であるとみなせる．

B. 独立 (Independent)

この構成では，1 つの SPE は他の SPE とは独立している．これは，ポリシーが全く異なる 2 つのグループに相当する．

C. 統合 (Integration)

これは包含の変形である．複数の上位 SPE が共通するサブ SPE を包含している形式である．このパターンの例は，異なるセキュリティポリシーがサブシステムを共有する 2 つ

の別々の機能システムで構成されている．

D. 分割 (disparsion)

これもまた，包含の変形である． SPE は 2 つの独立したサブ SPE で構成され，共通ポリシーが両方の SPE に適用される．この実装パターンの例は，サブシステムで構成されるシステムで，各サブシステムは，共通のポリシーを共有するだけでなく，独自のポリシーを保持している．

構造化ポリシーモデルを定めるためには，その境界の選び方に加えて，ポリシー境界が現実に境界として機能することが要件として求められる．このような要件は車載 E&E システムでは，物理的な条件，論理的な要件がある．

物理的な要件とは，物理的な機構により分離されている場合である．たとえば，車両のある正式な分解手順を経ないと到達できない場所にある，同一のボックスに入っている，同一のファイアウォールやゲートウエイで保護されたネットワークセグメントに接続されている，trustzone として区別されている，同一のプロセッサの中で実現されているなど，何らかの物理的に他のグループと区別可能な要件である．これらの相違は，必ずしも絶対的なものではない．たとえば，同一の基板上に実装されている複数のシステムという区切りは，基板上の処理装置を別と考えると別のポリシーに属することになる．

また，論理的な要件は，情報的に区別されるグループである．たとえば，常時，同一グループとして通信および内部状態をモニタリングされている，同じ公開鍵鍵暗号基盤の Certificate Authority を用いている，同一の鍵生成システムにより生成された共通鍵を用いている，共通鍵などの秘密情報を共有している，認証機能により相互認証が実施済みで，認証に基づいたセッションを貼っているなどが論理的に他のグループと区別可能な条件である．厳密には，物理，論理双方に関連する境界も存在する．たとえばファイアウオールのフィルタリングルールは，ファイアウォールで物理的に区別した上で，入ってくるデータに対して論理的なフィルタリングを加えていると考えても良い．

4.4 構造化ポリシーモデルの構築手法とユースケース

本節では，前の節で解説した構造化ポリシーモデルの構築手法を，ユースケースを用いて具体的に提示し，あわせて，構造化ポリシーモデルを採用した場合の脆弱性評価の概要を示す．

構造化ポリシーモデルの構築とは，換言すれば，システムやサブシステムの関係性から構造的 SPE を抽出し，それらに対して適切かつ整合的にセキュリティポリシーを割り当てることである．保護すべき機能にたいし適切なポリシーを設定ために，階層的機能構造を前提とする．これは，システムは複数のサブシステムから構成され，サブシステムもまたシステムとして，それを構成するサブシステムを持つという構造である．車載 E&E システム全体をシステムとすると，アイテムは，車載 E&E システムを構成するサブシステムである．また，アイテムを構成する機能群は，アイテムというシステムを構成するサブシステムである．また，この様にして構成されたシステム，サブシステム間のデータフローは予め定義されているものとする．以下，車載 E&E システムからみて最上位のサブシステムをアイテムと称し，それより階層が下のシステムをサブシステムと称する．

前節で解説したように，SPE の分割は，物理的特性，機能的関連性に基づいて分割する．物理的特性とは，基盤や，筐体，配置，ネットワークのセグメントなど物理的に区別可能な特性である．これらは，逆にいえば，一定の物理的な条件を共有するグループであると考える．論理的・機能的関連性は，情報によるつながりで分別されるグループである．このグループの決め方は，データフローの付帯的情報，たとえば，脅威分析が予め行われており，機能の脆弱性に対する評価などが完了している場合には，それらの情報も参照して行う．たとえば，単にデータフローだけが判明している場合では，複数の機能に対してデータフローがある機能を SPE 候補として切り出す，データフローの数が多いものを関連性が高いとしてまとめて SPE 候補として切り出すなど，データフローの数に基づく距離空間における分割により SPE 候補を切り出す．また，逆にデータフローが資産の移動を含む場合には，当該資産が移動する範囲を SPE 候補とする．これは，データフローに資産の重みを加えた距離空間における分割問題でと考えることが出来る．

現実には，論理的特性，論理的特性だけで，SPE の分割は定まらない．たとえ情報の相互関連性が高くても，物理的位置が離れている場合にはその制約を受ける．したがって，SPE の構成は，物理的構成と論理的構成が層状に積み重なる構造となる．そして，その間の関係を前節で述べた論理的な規則で合成することによりシステム全体のポリシーの構造階層化が達成される．まず，ここでは，SPE 構築の例を，SPE 構造の導出と，ポリシーの割当とその検証，最後に各 SPE に含まれるサブシステムに対する脅威分析の段階で具体的に示す．

1. SPE 導出 1：相互に関連する複雑なアイテムを取りまとめて最上位の SPE とする．
2. SPE 導出 2：各アイテムのサブシステムを，その物理的特徴，機能的関連性，および類似性に基づいてグループに分け，各グループをサブ SPE 候補とする．次に，それらを階層的に重ね合わせる，
3. ポリシー割当 1：最上位の SPE にセキュリティポリシーを定義する．この SPE はシステム外部にたいするシステム全体のセキュリティポリシーとなると同時に，これに含まれる各サブ SPE が共通に前提とするポリシーとなる．
4. ポリシー割当 2：各サブ SPE にポリシーを導出し，割り当てる．さらに，わりあてられたサブ SPE のセキュリティポリシーに関して整合性を取る．この整合性を取る必要があるのは，独立を除く 3 つの関係である．包含や合成関係の場合，整合性のとり方には二通りのパターンがある．一つは上位の SPE のセキュリティポリシーと重複する下位 SPE ポリシーを，上位の保護があるという理由で，下位 SPE ポリシーから削除するもの，もう一つは，そのまま残すかパターンである．これには，逆に．包含される各 SPE で共通するポリシーを上位の SPE のポリシーとして，各 SPE から削除するか，そのまま残存させるかのパターンでもある．最終的に，ポリシーの割当を定めた後に，図 4.3 の関係で，ポリシーを合成し，各 SPE に対して必要なポリシーが割り当てられているかを確認する．
5. 脆弱性検証：SPE を元に，各サブシステムの脆弱性評価の対象となる脅威分析を実施する．

この手順の例として，1 つはパワーステアリングシステム (PSS)，もう 1 つは車線維持システム (LKAS) の 2 つのアイテムで構成されるシステムを検討する． 各アイテムのサブシステムを表 4.2 に示す．

表 4.2　PSS と LKAS の持つ機能

アイテム	サブシステム
PSS	1) 速度センサ,2) トルクセンサ,3) アクチュエータ, 4) ステアリングユニット,5) ステアリングアクチュエータ
LKAS	1) 速度センサ, 2) 車線検知器, 3) 制御ユニット 4) ステアリングユニット

ステップ 1 の後，すべての関連アイテムが最上位の SPE のポリシーに従う (表 4.3)．

表 4.3　アイテムと最上位 SPE

	最上位 SPE	
	PSS	LKAS
サブシステム	1) 速度センサ 2) トルクセンサ, 3) アクチュエータ 4) ステアリングユニット 5) ステアリングアクチュエータ	1) 速度センサ 2) 車線検出器, 3) 制御ユニット 4) ステアリングユニット

ステップ 2 では，すべてのアイテムが，その物理的特徴，機能的関連性，および類似性に従って分類される．この場合，アイテムの機能は，論理的にセンサシステム，決定システム，制御システムに分類される．また，車両の物理的構成も考慮し，各機能の物理的配置を用いる．この場合，速度センサは単一のユニットである．アクチュエータは単一のユニットでなければならない．ステアリングユニット，トルクセンサ，およびステアリングアクチュエータは，位置および機能において密接に関連している．したがって，これらのサブシステムは 1 つのグループを形成する必要がある． LKAS の場合，車線検出器と制御ユニットは他のサブシステムと強く結合する．したがって，これらのサブシステムは，表 4.4 に示すように，1 つのグループを形成する．

表 4.4　サブシステムのグループ化

	最上位 SPE	
	PSS	LKAS
グループ 1	1) 速度センサ,	1) 速度センサ,
グループ 2	3) アクチュエータ	
グループ 3	2) トルクセンサ 4) ステアリングユニット 5) ステアリングアクチュエータ	4) ステアリングユニット,
グループ 4		2) 車線検出器 3) 制御ユニット

さらに，グループ 3 をさらにサブカテゴリに分割する．PSS と LKAS はステアリングユニットを共有する．したがって，ステアリングユニットは，PSS および LKAS のサイバーセキュリティ要件に従う．しかし，トルクセンサとステアリングアクチュエータは

PSS のみに属する．したがって，グループ 3 をグループ 3-1(トルクセンサーとステアリングアクチュエータ) とグループ 3-2(ステアリングユニット) に分割する．そして，これらのグループが従うポリシーの構造として，この構造に従ってサブ SPE の割当および階層構造を定める (表 4.5).

表 4.5　サブレベルへの分割

		最上位 SPE
サブ SPE-1		1) 速度センサ,
サブ SPE-2		3) アクチュエータ
サブ SPE-3	サブ SPE3-1	2) トルクセンサ, 5) ステアリングアクチュエータ
	サブ SPE3-2	4) ステアリングユニット,
サブ SPE4		2) 車線検出器, 3) 制御ユニット

ステップ 3 では，セキュリティポリシーの導出を行う．ここでは，セキュリティポリシーをトップレベルの SPE に割り当て，それを分割する手法をとる．トップレベルのセキュリティポリシーを定義する前に，トップレベルのセキュリティポリシーでセキュリティ脅威からシステムを保護する必要があるため，車両レベルの脅威評価とリスク評価の結果を確認する必要がある．この場合，PSS および LKAS に適用される車両レベルのリスク評価によって扱われる脅威は，それぞれ表 4.6，および表 4.7 に示すとおりであると仮定する．

表 4.6　PAS に対する脅威

原因	1 から 4 によるデータ改ざんや詐称によるパワーステアリング システムにおける異常なハンドル操作補助トルクの発生
原因 1	速度センサからの不正な値
原因 2	ステアリングユニットからアクチュエータへの不適切な操作指示値
原因 3	トルクセンサからステアリングユニットへの不正な価
原因 4	ステアリングアクチュエータへの不正なトルク指示値

これらの脅威からシステムを保護するために，最初の段階ですべてのサブ SPE のセキュリティポリシーを含む最上位のセキュリティポリシーを定義する．表 4.6 と表 4.7 に示すように，これらの攻撃はサブシステム間の通信を改ざんまたは偽装するものである．このような通信がシステムの外部から容易に行われると，システムのセキュリティが侵害

表 4.7　LKAS に対する脅威

原因	1 から 4 によるデータの改ざんや詐称による車線からの逸脱
原因 1	車線検出器からの不正な状態情報
原因 2	制御ユニットからステアリングユニットへの不適切な操舵指示
原因 3	速度センサーからの不正値
原因 4	PAS に対する脅威と同じ原因による PAS システムの異常動作

される．したがって，最上位のセキュリティポリシー SP0 を次のように定義する．

SP0　当該システムに関係していない外部からの送信者によって送信されたデータを許可しない．

ステップ 4 では，ある SPE に割り付けられたセキュリティポリシーに対して，その直下にあるサブ SPE 内部が満たすべきポリシーを追加する．追加の結果として得られるポリシーは，図 4.3 の規則にしたがって包含，独立，合成，または，分割される．ここでは，SP0 を最上位の SPE に割り当てる．

SP0 を満たし，かつ，各 SPE が安全であることを保証するためには，SPE 内部からのデータの改ざんや挿入を防止する方針が必要となる．すなわち，システム内部のデータの正当性が保証されなければならない．したがって，トップレベルのセキュリティポリシー SP0 は，次のように追加修正される．

SP0-0　当該システムに関係していない外部からの送信者によって送信されたデータを許可しない．

SP0-1　このシステムに含まれるサブ SPE が適用されたサブシステムのデータの存在のみを許可する．

次にサブシステムが従うサブ SPE に割り当てられるセキュリティポリシーを定める．この場合，想定するサブシステム，いいかえれば，想定されるサブ SPE にしたがうサブシステムからのデータ以外は，最上位 SPE の内部に取り付けられた，なりすましのデータである可能性がある．したがって，

SP1-0　正当なサブ SPE に従っているサブシステムによって送信され，改ざんされていない適切なデータを許可する．

また，同様に，サブ SPE 内部のデータも正当性が保証されなければならない．また，サブ SPE の外部にデータを送る場合，相手側のサブ SPE に対して SP1-0 と同等のポリシーが要求される．したがって，

SP1-1　サブ SPE にふくまれる，サブシステムもしくはさらに下位のサブ SPE のデータ以外は，サブ SPE に含まれない

SP1-2　サブ SPE から他の SPE にデータを渡す場合には，他の SPE のポリシーに従っていることを保証するもの以外は，渡さない．

ここで，このシステムのデータフローを確認する必要がある．PSS と LKAS の性質から，このシステムのデータフローは図 4.4 に示すものと仮定する．

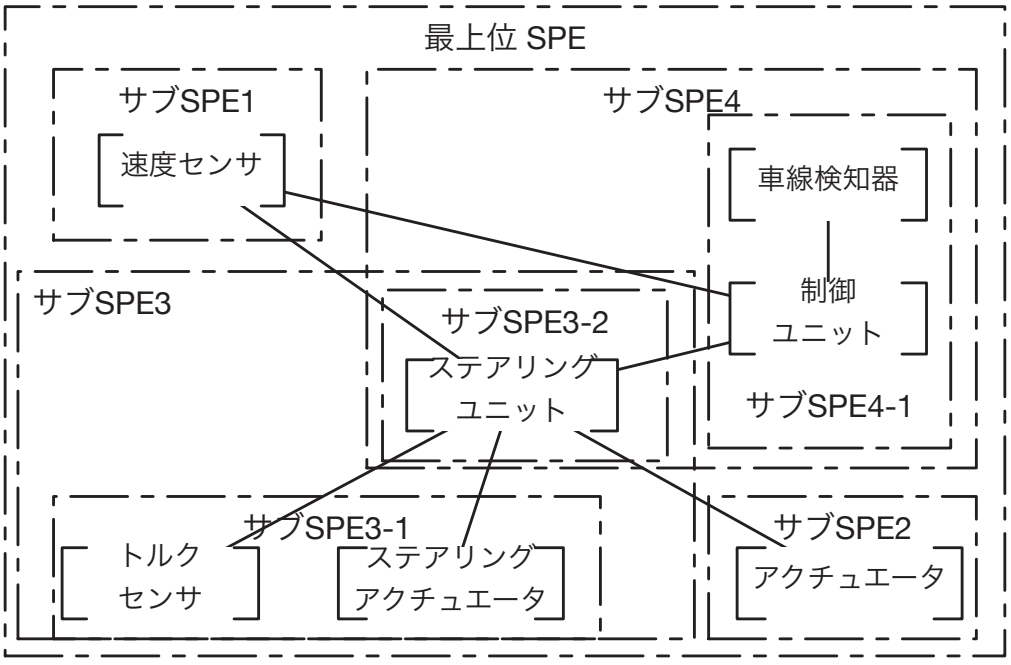


図 4.4　SPE 間のデータグロー

最後に，各 SPE に次のセキュリティポリシー (SP) が割り当てられる．ここでは，以下の通りに割り当てられる．

トップレベル SPE の SP　このアイテムの外に正しい送信者が受信した適切なデータを受け入れ，SPE2，SPE3，および SPE4 が適切なデータを送信できるようにする (SP0-1，SP0-2).

SPE2 の SP　サブ SPE3 とサブ SPE4 によって送信され，改ざんされていない適切なデータを許可する．また，送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-1，SP1-2 の個別適用).

SPE3 の SP　サブ SPE1，サブ SPE2，サブ SPE4 によって送信され，改ざんされていない適切なデータを許可する．また，送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-1，SP1-2 の個別適用).

SEP4 の SP　サブ SPE1 とサブ SPE3 によって送信され，改ざんされていない適切なデータを許可する．また，送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-1，SP1-2 の個別適用).

SPE3-1　サブ SPE 3-1 の正しいサブシステムによって送信され，改ざんされていない適切なデータを許可し，SPE3-2 が適切なデータを送信できるようにする．送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-1，SP1-2 の個別適用).

SPE3-2　サブ SPE2，サブ SPE3-2，サブ SPE4-1 の正しいサブシステムによって送信され，改ざんされていない適切なデータを許可する．送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-2 の個別適用)．送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-1，SP1-2 の個別適用).

SPE4-1　サブ SPE1-および，サブ SPE 3-2 が送信し，改ざんされていない適切なデータを許可する．送信に際しても相手側 SP の提示するポリシーに準拠する．(SP1-0，SP1-2 の個別適用).

4.3 節で定義したルールでこれらの SP を組み合わせると，各 SPE の合成ルールされたもので各サブ SPE に準拠するサブシステムは保護されることになる．したがって，これらのポリシーの実装は，このシステムをサイバー攻撃からの多重保護を実現する．これらのポリシーの典型的な実装は，SPE 内部の悪意のあるデータフローをスキャンする小さなゲートウエイとモニタ機能を組み合わせることである．

ステップ 5 では，脅威／脆弱性分析を実施する．構造化ポリシーにおける脅威／脆弱性

分析を，形式的に説明する．まず，基本パターンとして単一の SPE で記述されたシステムを考える．この SPE ではポリシー P が定義されている．図 4.2 でしめしたように，ポリシー P は Entry ポリシー EP，内部ポリシー CP，Exit ポリシー XP から構成されている．

ここで，SPE 内部でポリシーで管理されている機能 f_x のアクセスを考える．f_x にアクセスして，そこからレスポンスを得るためには，f_x に適用されているポリシー P を満たさなければならない．攻撃者は，f_x を攻撃するためには，まず，SPE 境界で EP を回避するか迂回しなければならない．さらに EP を超えたあとも，CP を満たさなければ SPE 内部に入ったとしても f_x にアクセスすることはできない．これは，f_x を直接攻略するための最低限の要件であり，SPE 外部からの攻撃者は，この要件を満たさなければならない．さらに，SPE 内部からの情報を得るためには，EP を満たさなければ，出力が SPE から外部へ戻ることがない．

ここで，ポリシー P を攻略するための手法を MCR(P) と表す．また，機能 f_x を攻撃するための手法は，MCR(f_x) と記載できる．ポリシー P を攻略して機能 f_x を攻撃する場合は MCR(f_x,MCR(P)) と表記する．攻撃者は，攻撃に際して何らかの情報を必要とする場合がある．ポリシー P を攻略するために必要な情報を R(P) とすると，攻撃手法は，MCR(P,R(P)) と表記できる．攻撃者は，それぞれのポリシーの攻略手法を開発し，実行しなければならない．

つぎに，単一の SPE を想定して，その内部の機能 f_x への攻撃を検討する．このとき，SPE 内に入る場合にフィルタリングによる Entry ポリシーを，また内部ではブロードキャストによる通信のシリアライズによる順序制御ポリシーを想定する．

EP　フィルタリングルールにより特定の IP アドレス以外は SPE 内部に通さない

R(ER)　フィルタリングルール

CP　SPE 内部での通信はすべてシリアル番号がつけられ，順序付けられないデータは削除される

R(CP)　次に使用される SPE 内部で使われているシリアル番号

XP　フィルタリングルールにより，正しいシリアル番号は SPE 外部に出さない

この場合の攻撃は， フィルタリングルールの情報から，アドレス詐称してデータを送

り込む．このデータは，推測でシリアル番号がつけられたデータを利用する．しかし，この攻撃では，次のシリアル番号に対する情報が欠落しているがため，偶然一致するか，多くの試行の結果として一致する場合が想定されるが，それは意図したタイミングでの攻撃は困難である．したがって，有効な攻撃を行うためには，シリアル番号の入手が必要である．つまり，XP を攻略して，シリアル情報を SPE 外部に漏洩させることが必要である．つまり，XP を改ざんして，シリアル付きデータを外に漏洩させ，その情報をもとに, アドレス詐称してデータを送り込まなければならない．

構造化ポリシーモデルで SPE 内部の機能の脆弱性とは，構造化ポリシーの何れかの部分または全体が無効化される想定である．上の例では，フィルタリンクのバイパスでは，内部ポリシーを突破できない．したがって，フィルタリングルールの Spoofing により通過して，内部に正規データとして送り込まれる脅威，および統計的に送り込まれたシリアルがたまたま合致してしまう脅威，および Exit ポリシーが改ざんされシリアル情報が流出する脅威が脆弱性評価として考慮すべき脅威となる．

これにより，概念的には (図 4.5) で表されるように想定しなければならない脆弱性に対する攻撃の範囲が縮小する．

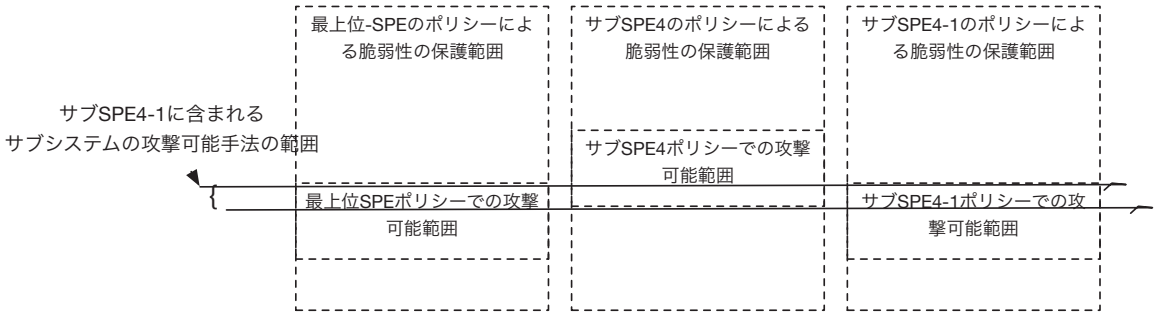


図 4.5　攻撃範囲の制限

4.5　まとめ

本章では，構造化されたセキュリティポリシーに基づいて安全な自動車システムの設計方法を提示した．ポリシー構造を構築するために，ポリシー間に 4 種類の関係を定義した．ポリシー構造を定義するために，ここでは機能要素間の関係に基づく機能分割を使用する．まず機能部門ごとにポリシーの下部構造を割り当てる．サイバーセキュリティリスクアセスメントから得られるセキュリティポリシーは，サブレベルセキュリティポリシー

に分割され，ポリシーサブ構造に割り当てられる．サイバーセキュリティのプロセスは，ポリシー実現に必要なセキュリティ機能を割り当てることによって設計される．また，セキュリティポリシーの導入により，セキュリティ要素内の機能に対する攻撃方法が制限される．したがって，脆弱性評価コストは減少すると予想される．この研究で提案された車載サイバーセキュリティシステム設計の有効性を引き続き検証する．

第 5 章

ユーザー操作の繰り返しを考慮したウィンドウログの解析によるユーザーの識別手法

5.1 はじめに

本章では，一般的なセキュリティ・アプライアンス製品で取得されるユーザの操作履歴からユーザを分別し，さらにユーザの不正操作やなりすましを検出するための解析手法を提案する．

提案手法は，実際の操作記録の特徴の分析に基づき，操作記録に残される操作中のタスクの情報にくわえて，ユーザの作業モデルを仮定し，繰り返し操作に着目した操作履歴のパターンを抽出・分析を行うこと特徴とする．分析に際しては，機械学習によるデータ学習によりナイーブベイズ分析器を生成し，データの評価を行った．評価は，企業での実オフィス業務でのユーザ操作履歴に対し，ナイーブベイズ分析器によるユーザ判別手法を実施した．

本手法の適用により，ナイーブベイズ分析器による自己同一性判定では学習データに対して 90% 程度の判別率を持つ．これは，操作記録をバイグラムにより符号化し，それに対してユーザ判別手法を適用した場合の学習データに対する判別率の数値 67% と比較して，有意な分別精度の向上を得た．

近年，組織内に保有する情報の漏洩・紛失・毀損などの情報セキュリティ・インシデント対策の重要性が高まっている．これらの情報セキュリティ・インシデントは，大別すれば，(1) クラッキングによる外部からの侵入やマルウエア感染などによる外部要因による

もの，(2) 内部のユーザやシステム管理者によるいわゆる内部要因によるもの，に大別される．特に内部要因によるインシデントは発生した場合，規模および情報の内容が，大きくかつ機微なものとなる場合が多く，組織に与える被害が大きなものとなる傾向がある [31].

そこで，近年，情報セキュリティの分野において組織内部の人間による情報漏洩のリスクが注目されている．それに対応して ISO/IEC 27001 などの情報セキュリティに関連する規約等では，情報端末の操作履歴の取得と活用を推奨している．それと軌を一にして，ユーザ操作履歴を取得するツールの開発や商品が，そして一般への普及が進展している．一方，その操作履歴の活用については，もっぱら抑止力による効果が期待されており，不正検知などの能動的な利用に対する期待度は低いのが実態である [31].

内部要因によるインシデントのうち，ユーザが関与するものとして，(1) アクセス権限の不正取得による操作 (いわゆる成りすまし)，および (2) ユーザのアクセス権限内での操作での不正操作 (サボタージュや裏切り) がある．いずれの場合でも，一般には PC 監視ソフトウェアによる操作ログの取得が有効であるとされる．

これらのユーザ操作履歴ツールは，一般に端末およびログインユーザの識別子，操作時刻，時間，使用したアプリケーション，およびこれが操作対象としているファイル名を記録する．この履歴を利用したユーザの同定，さらには不正行為の検出への適用可能性についていくつかの手法が検討されている．

不正行為の検出には，“誰が” “いつ” “どこで” “何に対して” “何を行ったか” の特定が必要である．上記のツールでは，利用が禁止されているコマンドやファイルの利用状況の確認，勤務管理と連動した操作時刻の整合性の確認，利用している PC とユーザ ID との関連確認などが確認できる．しかし，“誰が” の部分に関しては，パスワード漏洩や離席時の操作などのなりすましの可能性が残る．

なりすましに対しては，操作履歴の統計的な特徴を分析し，その特徴で各ユーザのプロファイルを作成，その特徴から本人を特定する機械学習をもちいた分析手法が効果的であると考えられている．

しかし，この操作ログの効能およびその利用に関しては，主に不正行為の証跡調査が可能になることによる心理的な不正行為に対する抑止力が期待されており，不正行為そのものの検出に対しては期待度が低い．また，操作ログをもちいて不正行為の発見を行うに

は，大量のログを個々人の利用パターンや部門毎の振る舞いを考慮した分析を行わねばならず非常にコストが高い．またデータマイニングや統計的な手法を用いた方式も提案されている [32]．これらの手法では，コマンドラインログやアプリケーションログを対象としたものが主流である．

一方，ウィンドウシステムでは，ウィンドウの操作等取得可能なデータ量が多岐にわたる一方で，不正検出については処理量の増大等により一般に適用可能な手法は未だ見いだされていない [33]．

ウィンドウプログラムを対象とした一般の操作ログ取得システム製品では，ユーザが操作しているウィンドウの履歴，いわゆるアクティブウィンドウログを取得するものが多い．このアクティブウィンドウログとは，ユーザが操作しているウィンドウのタイトルバーに表示される文字列ならびに操作時間などの付帯情報を記録したものである．Microsoft Windows や MacOS などのウィンドウシステムのユーザインターフェイスガイドラインの規定では操作対象なども文字列に含ませることと指示している．そのため，ガイドラインに準拠したアプリケーションならば，単なるアプリケーションの詳細な操作情報が得られる．このアクティブウィンドウログによりインシデントの発見等の簡便化が可能ならば，組織におけるインシデント抑止力の向上に大きく寄与するものと考える．

本章の構成は以下の通りである．5.2 節で提案する解析手法を説明し，5.4 節で実際のオフィス業務でのデータへの適用結果を述べる．5.5 で関連研究を述べる．最後に 5.6 でまとめと今後の課題を述べる．

5.2 アクティブウィンドウログ

5.2.1 アクティブウィンドウログ

アクティブウィンドウログは，ユーザが操作しているウィンドウに関するログであり，その内容は，ウィンドウタイトル，プロセス名，操作時間などからなる．ウィンドウタイトルの記載内容は，スタイルブックでアプリケーション名と操作対象，操作モードを利用することが推奨されている．さらに，実際のアクティブウィンドウログでは，付帯情報として，操作時刻および次のウィンドウに切り替わるまでの時間，端末名およびログインユーザ名を含むものが多い (図 5.1 参照)．

コマンドラインログでは，ユーザの操作情報はコマンドライン引数のみであるが，アクティブウィンドウログでは，ウィンドウタイトルに依存はするもののより詳しい操作情報が得られる．また，システムログ (Microsoft Windows のアプリケーションログも含む) と比較すると，アプリケーションログはソフトウェア作成の際にログを残す仕組みを組み込まなければならない．一方，アクティブウィンドウログはウィンドウの切り替え時に従って発生する．そのため，任意のアプリケーションに対して適用可能である．また，特にシステムコールやマウスやキー入力など，いわゆる低レベルのシステムログはユーザ側の操作の結果発生するものではあるが，一般に量が多く，また，操作しているアプリケーションとの直接の関連性がない．そのため何らかの関連付けが必要となる．

5.2.2 対象業務およびログについて

アクティブウィンドウログの対象とした操作者は，営業部門，顧客情報管理 (課金等) および管理・保守部門からなっている．これらの部門は，共通の顧客管理システムを用いている (図 5.2)．この顧客管理システムではサービス内容を含む個人情報，支払い状況ならびに課金にかかる服地的情報 (クレジットカード番号など) を取り扱っている．このシステムは，データ入力モード，検索モードなどデータを取り扱う状況に応じた操作モードを持っている．データの保護は，ID/PW およびそれに付随するアクセス権の管理で実施されている．たとえば，非課金部門では課金にかかる情報は一切アクセスできない．また，日常的な管理業務や報告書作成には Microsoft の Office Suite が，部門間および個人連絡には電子メールおよび電話が，そして顧客要求は Web ベースの管理システムで一括管理されている．また，営業部門は，情報収集の名目で，制限の下でインターネットの自由な利用が許可されている．

```
第2営業  275 PC08048 2011/6/1  7:45:54  0:00:06 ACTIVE  iexplore.exe  リンコム ネクスト2 - Microsoft Internet Explorer
第2営業  275 PC08048 2011/6/1  7:46:01  0:00:03 ACTIVE  Explorer.EXE Program Manager
第2営業  275 PC08048 2011/6/1  7:46:04  0:00:11 ACTIVE  iexplore.exe  リンコム ネクスト2 - Microsoft Internet Explorer
第2営業  275 PC08048 2011/6/1  7:46:16  0:00:02 ACTIVE  EXCEL.EXE  Microsoft Excel
第2営業  275 PC08048 2011/6/1  7:46:19  0:00:03 ACTIVE  EXCEL.EXE  パスワード
第2営業  275 PC08048 2011/6/1  7:46:23  0:01:01 ACTIVE  EXCEL.EXE  Microsoft Excel - 退社時間調査 [共有]
技術部   240 PC07026 2011/6/1  7:46:39  0:02:40 ACTIVE  iexplore.exe  リンコム ネクスト2 - Windows Internet Explorer
第2営業  275 PC08048 2011/6/1  7:47:24  0:00:03 ACTIVE  iexplore.exe  リンコム ネクスト2 - Microsoft Internet Explorer
```

図 5.1　アクティブウィンドウログの例

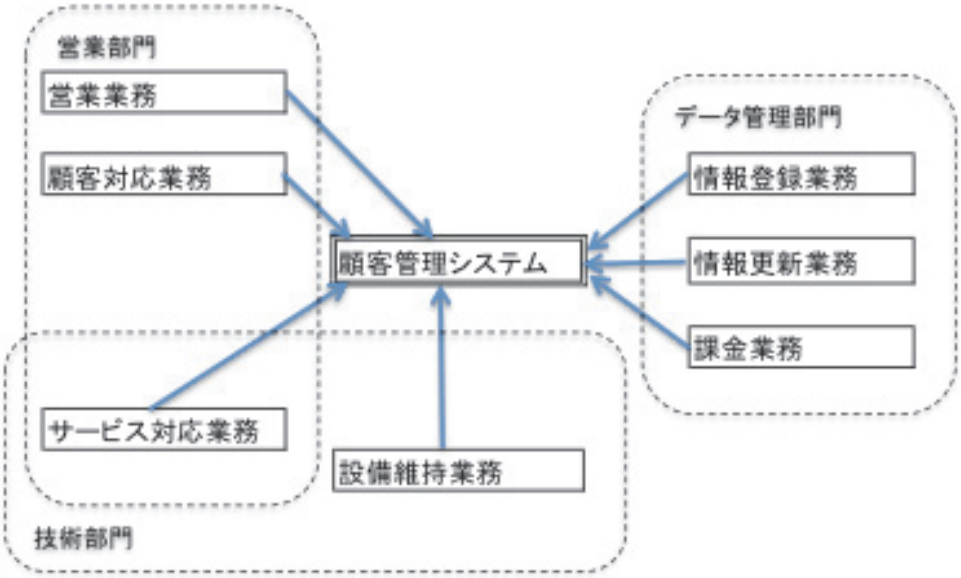


図 5.2　業務概略図

ログを取得するシステムは，Motex 社の LanScope を利用した．LanScope は PC 側エージェントにより，図 5.3 の情報を収集している．

エージェント設定情報	部署名等(手動設定)、端末名称
時間情報	日付・時刻・稼働時間
操作情報	アプリケーション、動作種別
ウインドウタイトル	ウインドウタイトル
その他	管理データ

図 5.3　LanScope のログデータ構成

5.2.3　操作パターンとログの関係

アクティブウィンドウログは，ユーザの操作の結果，発生するウィンドウの切り替えに関する記録であることから，ログの内容は次のようにカテゴリ分けされると推定される．

・カテゴリ 1：業務遂行上 (作業上) 必然的に発生するパターン．このパターンにはさらに，ある業務を遂行する上でアプリケーションやスクリプト側が強制するパターン，すな

わち業務内容とログが (誤操作などをのぞき) 一対一に対応するもの，および，(悪意の操作や) 規定された業務手順などによって操作が定められているもので，アプリケーション側などにより操作が強制されていないもの，の 2 つのサブカテゴリが存在する．いずれも規則性を持つ．

・カテゴリ 2：不随意に発生する事象に対応して発生する切り替え．たとえば，メール受信通知や電話応対に対応して割り込み的な業務を行う場合や，業務中の調査，ネットサーフィン，ウィンドウ操作のミスによる別ウィンドウ操作などが該当する．この切り替えには業務遂行上必要な切り替えと業務に関係なく，偶然切り替えられるものの 2 通りがある．これらは全ログに共通する規則性は持ちにくい．

一般に，コマンドラインシステムでは，カテゴリ 2 に属する操作は (一般ユーザの場合) 操作系列の中断→切り替えという手順を必要とするため，すべての操作系列はある意図で実施されていると仮定できる．ウィンドウシステムの場合，システムに対する操作の観点から言えば，カテゴリ 2 に属する操作は，一種の割り込み，もしくは (正規の操作からみれば) ノイズと見なす事ができる．しかし，カテゴリ 1 の様に操作が規定されておらず，デスクトップ上に表示しているアプリケーションやその配置，ユーザの操作性向など，ユーザ個々の特徴などが含まれており，コマンドラインシステムでのログと同等であると考えられる．逆にカテゴリ 1 の情報はユーザが行うべき業務内容を反映していると考えられる．

5.2.4 不正操作とログとの関係

ここでは，先の操作パターンとログの関係でのべたパターンに従って，不正があった場合のアクティブウィンドウログのパターンを考察する．ここでは，検討する不正操作パターンとして内部要因による不正を想定する．内部犯行のパターンでは，システムの悪用，情報の持ち出し，破壊行為の 3 種類に大別される．

いずれの場合も，操作者の権限の範囲内で行われるため，犯行行為そのものは，なりすまし，もしくは権限保有者 (システム上の欠陥もしくは管理上の問題で本来保有すべき権限を持たない場合も含む) のいずれかである．

なりすましに対しては，通常操作者と異なる人物が操作を行うため，ログによる個人の行動プロファイリングおよびそれに基づく個人識別する手法が有効である．一方，権限保

有者による操作は，操作頻度を判定基準とする識別方法では漏れる場合が想定される．たとえば，課金システムでクレジットカードの不正登録を行った後，再登録を行ったのか，単にカードの間違い登録を行った後，カードの再登録をおこなったのかは，コマンドの発生順序では判断できない．この場合は，逆に個人のプロファイリング情報そのものの特徴 (この場合だと再登録が多いという情報) が有効と考えられる．

アクティブウィンドウログでは，カテゴリ 1 のパターンを記録することが想定される．たとえば，先の例では，単に課金アプリケーションの操作という記録にくわえてカード登録，変更という本来データベース操作レベルの情報も残ることが想定される．そのため，プロファイリング用の情報としての有効性が期待できる．

また，カテゴリ 2 では，複数のアプリケーションの移動パターンを示している．そのため，コマンドログに近い挙動ではあるが，先の場合と同様，どの状態への移動であるかまで判定できるため，カテゴリ 2 の 2 つのパターンを分別する事が可能となる事が期待できる．

5.3 ユーザ操作モデルに基づいたループイベントによるユーザー識別

本章では，ユーザの PC のウィンドウ利用の操作履歴のうち，事務作業におけるユーザモデルを設定し，さらにウィンドウのタイトル部分の情報を含めて活用することで，ユーザを識別する方式を提案する．モデルでは，事務処理においては，ある特定の操作系列が繰り返えしに個々人の特徴が表現されると考える．それに従い，操作履歴のうち，あるウィンドウから別のウィンドウに遷移後，元のウィンドウに戻る操作系列をイベント (ループイベント) として抽出し，すべての操作履歴をこのイベントの組み合わせで記述する．このループイベントに対して統計的機械学習処理によるユーザ識別を行う手法をとる．その方法は，1) ウィンドウログデータからのイベントの抽出，2) オフィス業務モデルを用いた作業パターンの抽出，3) 作業パターンの外部影響の排除 (5.4.1 節)，4) 作成されたデータへの統計解析手法の適用 (5.4.2 節，5.4.3 節) の順で行う．

5.3.1 ウィンドウログ

一般的なセキュリティ・アプライアンス製品で取得されるユーザのウィンドウ操作履歴は，インプットフォーカスを保有するウィンドウに関する，利用者識別子，タスク名，ウィンドウタイトル名，操作開始時刻，操作時間やファイルの作成，変更，削除，移動およびデバイスの挿入・除去などが記録されている．ここでタスク名とは，当該ウィンドウを表示したプログラム，ウィンドウタイトルは，ウィンドウのタイトルバーに表示されている文字列が記録されている．本章ではこの記録をウィンドウログと呼ぶ．なお，本章では簡単化のため，ユーザの正常操作と誤操作を区別しないものとする．

5.3.2 イベントの抽出

ウィンドウログから必要なイベントを抽出する方法を述べる．ここでイベントとは，ウィンドウログに含まれるタスク名とウィンドウタイトルの組をいい，この系列をイベント系列と呼ぶ．イベントを英文字 1 字のシンボルで表記し，あるイベント (A) から別のイベント (B) への遷移 (これにはタスクが変わる場合，ウィンドウタイトルが変わる場合の両方が含まれる) をイベントの連接 (AB) で表す．ウィンドウタイトルは以下の種類がある．

- 操作対象のファイル名 (Word, Excel などのオフィスアプリケーションソフトウェアの場合)
- アクセス対象の URL(ブラウザの場合)
- 情報入力・操作指示などの操作モード (業務プログラムの場合)

5.3.3 作業パターンの抽出

オフィス業務での作業パターンの抽出を容易にするために，企業におけるオフィス作業をモデル化する．これは以下の特徴をもつ作業となる．

1. ユーザは処理すべき業務の入った入力トレイから業務を取り出し，PC で処理をし，出力トレイに処理結果を置くものとする．したがって，作業状態はもとに戻るため

に，一連の作業はループを形成している．

2. 実際に業務を続けている間は (3) を除き目的達成のために作業を継続する．
3. 処理すべき業務には優先されるもの，されないものなど優先度が付与されている．この処理中に電話がかかってくるなどの割り込み処理も発生しうる．

こうした事務作業を，優先度付入力キューをもつサーバーとしてモデル化することが可能である (図 5.4)．サーバーはスケジューラをもち，優先度に応じた業務を取り出す．割り込み作業は最高優先度入力が到着したものとみなす．

このモデルの帰結として以下が想定される．

1. 操作履歴の中で同じ手続きが存在し，それらは連続して繰り返し行われる傾向が存在する．そのため，手続きの多くは，開始と終了が同一アプリケーションと操作対象となり，一連の手順は閉じたループを形成する傾向がある．
2. 閉じたループは途中で別作業 (別ループ) に割り込まれても，割り込まれる前の状態に戻る．
3. 継続する長さは本人の属性というよりも外部 (仕事量) からの与件として定められる

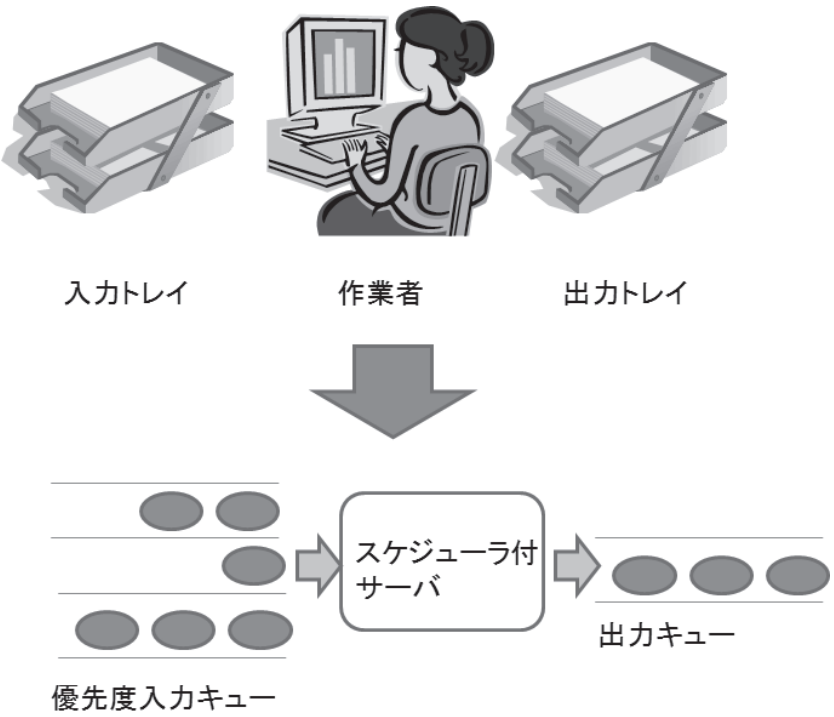


図 5.4　事務作業のモデル

ことが操作履歴の特徴として存在する.

まず，(1) のループ作業の抽出を説明する．一般の事務作業では，スプレッドシート (S) とワードプロセッサ (W)，スプレッドシートと会計ソフトなどを組み合わせて作業をおこなうなど，単独のアプリケーションで閉じず，複数のアプリケーション，またはウィンドウを組み合わせて作業を行う.

ある図や表のはいったドキュメントを作成する場合，ワードプロセッサ (W) とスプレッドシート (S) と描画ソフト (G) を互いに組み合わせて作業を行う．このとき操作のイベント系列が

WSWGSWS

となったとする.

この系列はワードプロセッサを始点として見ると，WSW，G，SWS という 3 つの手順から構成されていると見なすことができる.

この様に両端に同じシンボル (イベント) が現れる区間で分離し，操作系列をこの分割された手順の組み合わせで表現する.

ループイベントを両端が同じシンボル (イベント) であるイベント系列と定義する.

ACDCA のようにループイベントの途中で別のループイベント (CDC) が形成されることがある.

これをループイベントの呼び出しと呼ぶ.

ループイベントを両端のシンボルで置換して表し，これを縮退イベントと呼ぶ.

上の例では，WSW，SWS がループイベントであり，WSW の両端のシンボル W，SWS の両端のシンボル S が縮退イベントである.

ループイベントはスタックを用いて抽出することができる.

その手続きを図 5.5 に示す.

図 5.6 にこの動作例を示す．A,B,C,D まで順次スタックにプッシュし (1 ～ 4)，次に C をプッシュした時 (5) に既に同じイベント C がスタックにあるので，CDC をループイベントとして取り出し，縮退イベント C で置き換える (6).

次に A がプッシュされると (7)，同じイベント A があるので ABCA を縮退イベント A で置き換える (8).

一連のイベント系列は一般的には，ループイベントとその連結，およびループイベント

```
while(入力となるシンボルが存在する){
   当該シンボル X をスタックにプッシュする.
   if (同一シンボル X がスタック中に存在する
         (X'とする)) {
      シンボル X'からシンボル X までを
      スタックから取り出して
      ループイベントとして保存する.
      シンボル X をプッシュする.
      //シンボル X'からシンボル X までを X で置換
}
```

図 5.5　ループイベント抽出処理

の途中から別のループイベントの呼出しで表現されると考えられる.

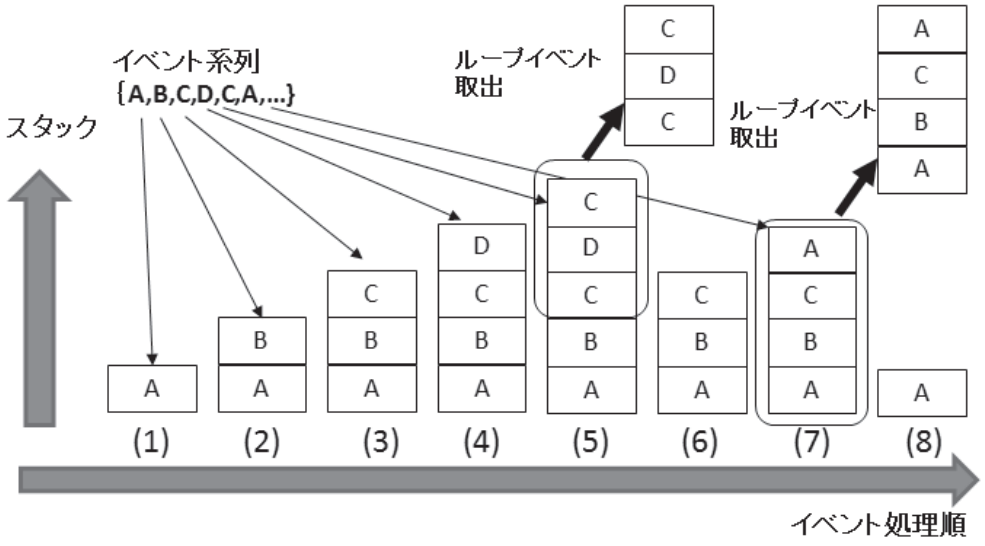


図 5.6　スタックによるループイベントの抽出

5.4　実オフィス業務データへの適用

提案手法によるウィンドウログの分析結果を示す．ウィンドウログの解析対象とした実オフィス組織は，営業部門，顧客情報管理 (課金等) およびシステム管理・保守部門からなっている．これらの部門は，共通の顧客管理システムを用いている (図 5.7)．この顧客管理システムではサービス内容を含む個人情報 (連絡先，支払い状況，サービスおよびそれらの改訂履歴) および，機微情報とされるクレジットカード番号や口座情報，未払い履歴など課金にかかる情報を取り扱っている．このシステムは，データ入力モード，検索モードなどデータを取り扱う状況に応じた操作モードを持ち，モードに応じてウィンドウタイトルが変わる．

また顧客からの要求管理はブラウザベースのシステムで行われている．また，日常的な管理業務や報告書作成には Microsoft のオフィススイーツが，部門間および個人連絡には電子メールおよび電話が使われ，顧客要求は Web ベースの管理システムで一括管理されている．また，営業部門は，情報収集の名目でインターネットの自由な利用が許可されている．当該オフィスで働くユーザは約 300 名，6 月から 8 月までの 3 か月のオフィス作業

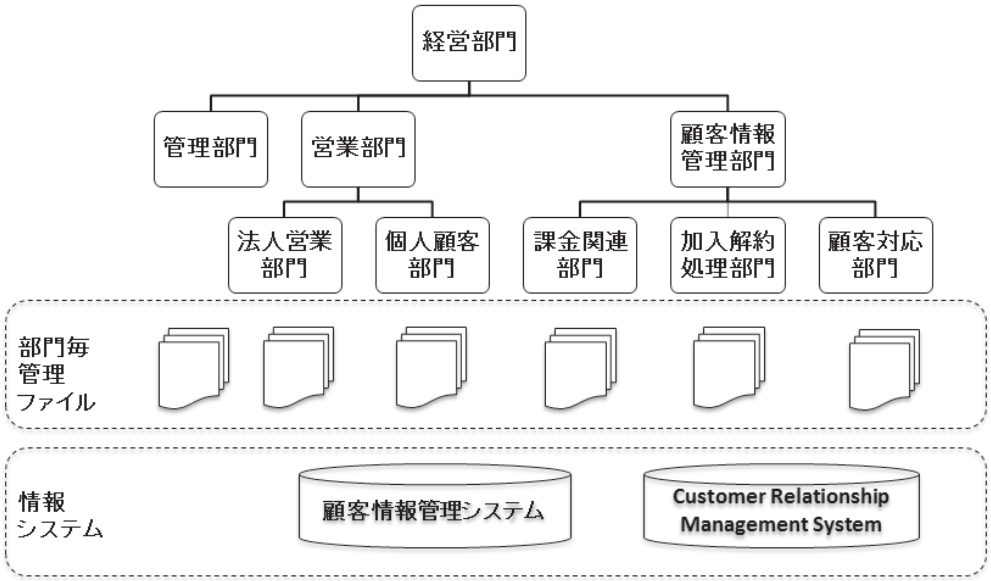


図 5.7　対象組織の構成

のログを収集し分析した．

5.4.1　作業モデルの検証

提案した作業モデルがこのデータで成立していることを検証する．作業モデルが成立している場合には，1) 特定のタイトルがよく使われており，そのほかは頻度が極めて低くなること，2) 比較的短いループイベントが生成されており，長いものや閉じていないループイベントが発生していないこと，3) 事務作業のトレイのモデルから繰り返しが発生しやすいことである．

営利組織における業務部門など，目的が明確で，かつ操作対象が限定されている環境では，一般に想定されるよりもウィンドウタイトルの数は爆発的に増えない．たとえば，ある特定のファイルが業務で利用するリストであった場合，当該ファイルの名称をふくむウィンドウログの数は目的の無いファイルよりも有意に多いと考えられる．

実際，今回の解析に使った例を図 5.8 に示す．ごく少数の操作対象のタイトルが殆どを占めていることが分かる．

この図では，一般的なタスクの代表例としてブラウザを，そして利用目的に特化したア

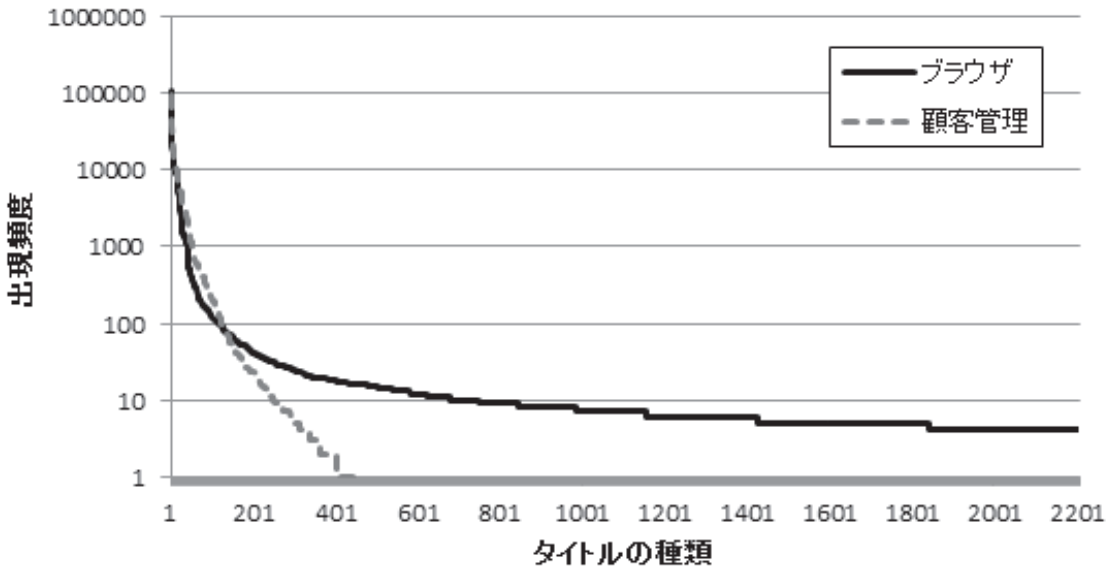


図 5.8　ブラウザと顧客管理ソフトウェアでのウィンドウタイトルの頻度分布

プリケーションとして顧客管理用のソフトウェアのウィンドウログを使用した．一般にブラウザはクエリ文字列を含む URL をタイトルに表示するため，特定のよく使われるページ，検索対象の URL などを表示するため種類が多くなりがちになる．ブラウザの部分で長くのびている部分は，関係する業者などのサイトを表示しているものが主であった．

そこで，以下では，ファイル名，URL，操作モードなど識別するウィンドウタイトルは予め指定し，これ以外のウィンドウタイトルは識別しないことにした．

つぎに，本作業環境でのループイベントについて調べる．イベント系列は以下の 4 つに分類することができた．

A1: アプリケーションや手順の制約等により，ほぼ単一の手順しかとりえないパターン: 特定アプリケーションの特性や，指定された作業手順の特性とみなしうる．事務作業は手順化されている場合が多く，また，アプリケーションの制約で手順が定められている場合もある．この場合，同一のパターンが複数ユーザにわたって見られる．これの変種として，

A1': ユーザの癖や作業パターンにより頻出手順が生成されるパターン:これは同一の作業を異なる手順で行うものやマニュアル化されていない場合でも個々人の手順として固定化しているものである．例えば，あるユーザでは ACBDBDA のように BD の作業を 1 回のループの中で終わらせる作業を，別ユーザは ACBDA と ACBDA の 2 回のループで作業を行うものである．

A2: ループイベントの途中で別のループイベントが呼び出されるパターン: 作業中の電話対応にともなう端末操作やある手順中から別の手順を呼び出して処理を行う一種の呼び出しに相当する．例えば，ループイベント ABCA の途中で，別のイベント列 XYZX が発生した場合，ABCXYZXA という系列になるものである．

A3: 複数の作業が並列して実行されており，系列がインターリーブするパターン: 例えば，ABCBA と別作業 XYZYX がある場合，ABXYCBZYAX のようにインターリーブするパターンである．この時には，本来，BCB，YZY のループが抽出されるところが，BXYB，BCZYAX (閉じていない) のループが抽出される．そのため，作業は完結しているのだが，見かけ上，ループが開かれた状態になる．このパターンが多発する場合ループによる解析は困難である．

A4: 繰り返しが発生しない，もしくは極めて長周期となるパターン: 一連の長い手続き

を順をおって実施する場合に発生する．今回対象としている事務作業では図 5.4 に示すように同一作業の繰り返しとなるため発生しにくいと考えられる．

ループイベントの抽出の観点から言えば，A3 はループの途中で別作業がはいるためループイベントの抽出を誤る場合がある．しかし，あるまとまった作業を区切りにしないで作業を変えるのは，作業の復帰が遅れるなどの作業効率が悪くなると考えられるため，A3 は発生頻度は少ないと考えられる，そこで A1 の頻度分布と A2 はユーザの特徴を示すと考えられ，本研究で使用する．

図 5.9 に本実験でのループイベントのユーザ全体の 1 か月分の平均長の頻度分布を示す．図で明らかなように，ループの長さが長くなるとともに急速に頻度が下がる．この図から，ループの長さは比較的短い距離に集中しており，同じ操作，もしくは参照してすぐに戻るという操作を続ける傾向が強いと思われる．したがって A4 は存在しないと仮定して以下の解析を進める．

あるユーザの 1 週間のループイベントの呼び出し状況を図 5.10 に示す．これも比較的浅い階層で処理がおこなわれていることが示されている．突発的に深くなっているのは，割り込み的に発生した業務と推測される．

高さが一定になっている部分では，同じ手順が繰り返されており，トレイのモデルに適

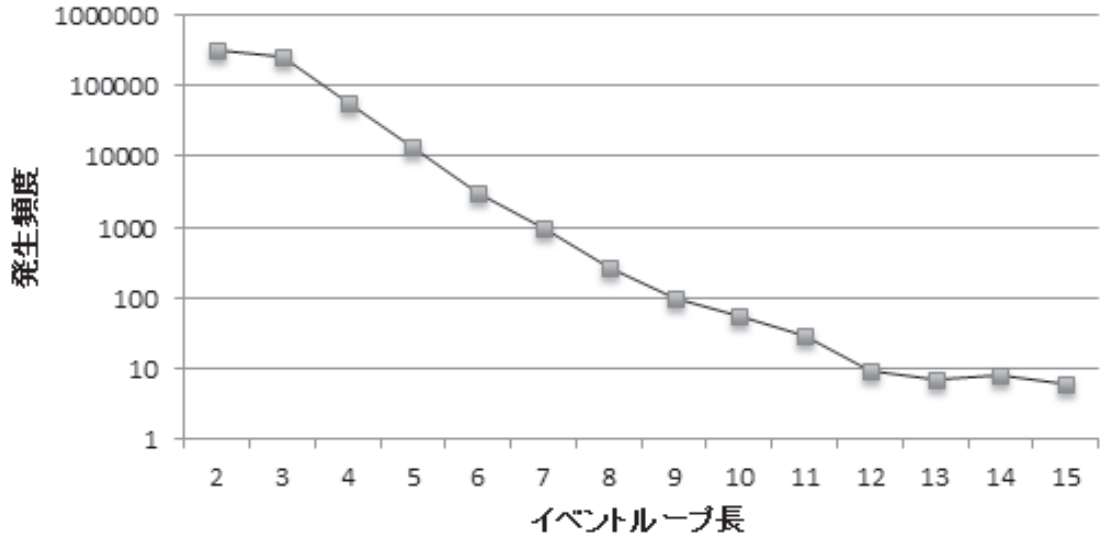


図 5.9　ループイベント長の頻度分布

合していると考えられる．

5.4.2 ループイベントによるユーザ判定

学習データのループイベントからナイーブベイズ分析器を生成し，ユーザのループイベントデータをナイーブベイズ分析器にかけて，各ユーザを正常に判定できるかを調べた．対象とした N 人の指定された期間においてユーザのログで抽出されたループイベントを $L_i(i = 1, \ldots, n)$ とするとき，各ユーザ U_i のループイベントの出現頻度は n 次元のベクトル V_i として表される．今回の学習データで n は 14289 であった．ユーザ U_i のループイベントの発生確率分布 P_i は $P_i = (\sum_{j=1}^{n} a_{i,j} / \prod_{j=1}^{n} a_{i,j}!) \prod_{j=1}^{n} p_j^{a_i}$ となる．ここで，$a_{i,j}$ は U_i の L_j の出現数，p_j は全ユーザでのループイベント L_j の発生確率である．あるユーザ U_x のループイベントを学習させ，その発生確率分布 p_x と p_i の比から U_x がユーザ U_i のいずれと判断されるかを調べる．

上記の定義に基づき，ナイーブベイズ分析器を R のパッケージ e1071 の nativeBayes を利用して実現した．具体的には以下のようになる．

```
model <- nativeBayes(V1,V2,...,VN) #(1)
result <- predict(model, Vx)       #(2)
```

(1) で学習データとしてユーザ $U_i(i = 1, \ldots, n)$ のループイベントのベクトル V_i を用いてナイーブベイズ分析器のモデルを作成し，(2) で判定対象のループイベントのベクトル V_x

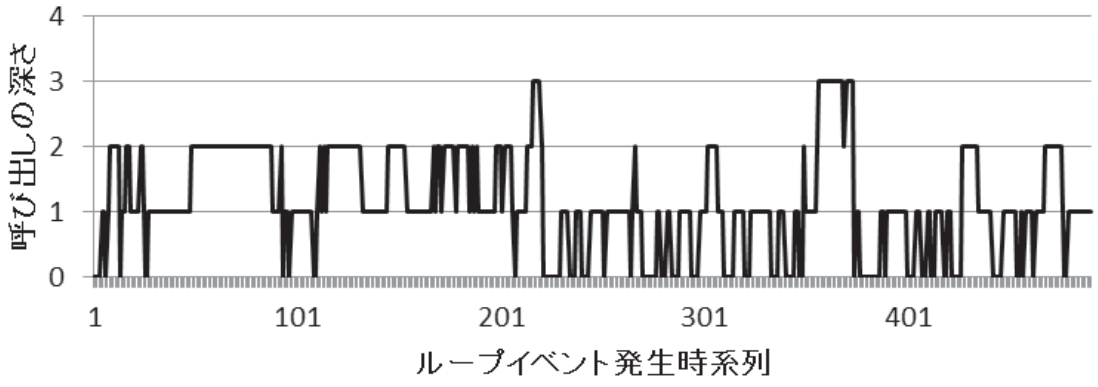


図 5.10　ユーザのループイベントの呼び出し

が，どのユーザに近いかの出現数の値で出力する．学習データ V_i に対して V_x を U_i のものとして判定した出現数の割合を正答率を呼ぶ．

ナイーブベイズ分析器は，1 日毎のユーザの作業単位を基に作成した．これは 1 日が作業としてまとまっていると同時に 1 日よりも短い単位で区切ると，絶対量が少ないため，突発的な操作による影響を大きく受けやすいことによる．また，学習区間として 1 ヶ月を単位とする．これは一般的な事務作業においては，1 か月をサイクルとした作業が繰り返されることが想定されるからである．まず，分析器としての基本的な性能を調べるために学習データ V_i を判定対象データとして再度ベース分析器にかけた．ループイベント抽出処理を行った場合と行わなかった場合のベイズ分析器において，対象データ V_i がユーザ U_i と判定されるかという実験を行った．その結果を図 5.11 に示す．この図の左の円グラフでは，ループイベント処理を行った場合に，データ V_i がユーザ U_i と正しく判定された

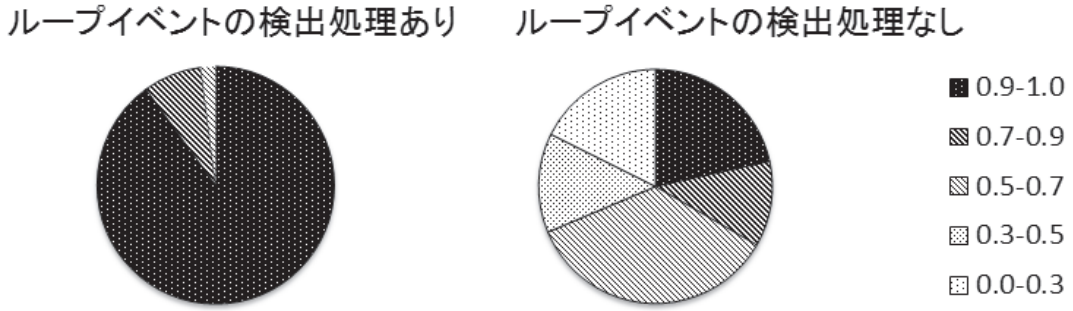


図 5.11　ユーザ判定の正答率でみたベイズ分析器の精度向上

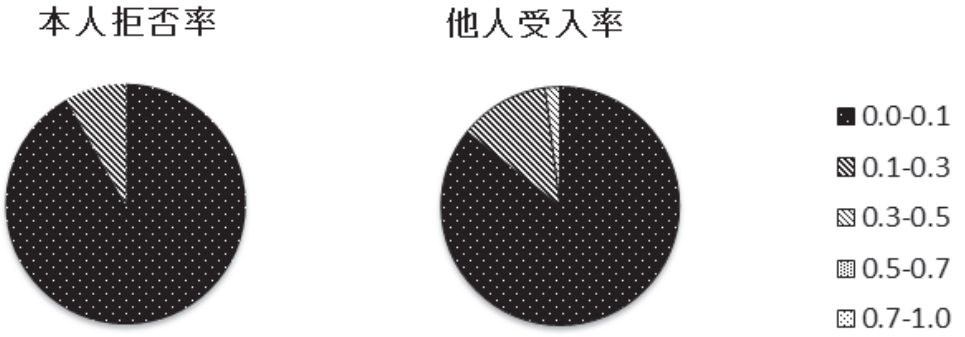


図 5.12　図 5.11 左での本人拒否率と他人受入率

正答率が 0.9∼1.0 にあるようなユーザ数は 92% 占めることを示している[*1]．全ユーザでの正答率の平均は 97% である．ループイベント処理を行わなかった場合に，同図右に示すように 0.9∼1.0 にあるようなユーザ数が 22%，正答率の平均は 74% となり，明らかに低い値となる．

ユーザ識別の精度指標として正答率以外に，本人を他人であると判定する確率 (本人拒否率，対象データ V_i がユーザ U_i と判定されなかった割合) と，他人を本人であると判定する確率 (他人受入率，対象データ $V_j(j \neq i)$ がユーザ U_i と判定された割合) を評価する．上記の実験での値を図 5.12 に示す．本人拒否率は，約 90% 以上のユーザで 0∼0.1，全ユーザでの平均値は 0.03 である．また，他人受入率は，80% から 90% のユーザで 0∼0.1，全ユーザでの平均値は 0.07 である．

このようにベイズ分析器としての基本性能はループイベントを抽出した場合に有意に高いものとなっている．提案手法では単純 N グラム手法のような機械的な結合ではなく，作業モデル上想定されるコマンドのループに基づいた構造を抽出している．すなわち，バイグラムだと別系列となるもの (例えば AB と BC，CA) が一つのコマンドのループ (ABCA) という意味がある単位として扱っており，このため本提案手法の方が単純 N グラム手法よりも基本性能が高いと考えられる．

次に，この様にして作成されたベイズ分析器を用いて，同一ユーザに対して，学習月の翌月と翌々月の 2 か月連続したループイベントベクトルを判定対象データとして使用してユーザ判定を行った．その正答率を図 5.13 に示す．この図から学習月の翌月のユーザ判定の正答率は，0.9∼1.0 にあるようなユーザ数が 58%，ユーザ全体の平均で 0.90，翌々月については，0.9∼1.0 にあるようなユーザ数が 60%，ユーザ全体の平均で 0.80 であった．学習月の翌月の本人拒否率と他人受入率を図 5.14 に示す．この図から本人拒否率は 75% のユーザで 0∼0.1，他人受入率は 62% のユーザで 0∼0.1 である．さらに，本人拒否率，他人受入率の全ユーザでの平均は各々 0.105，0.108 であり，これらの数字はオフィスでの適用では問題ない低さと考えている．

一方，比較のためループイベントを入力とするのではなく，イベントのバイグラムを入力としたナイーブベイズ判定器を作り，同様の実験を試みた．バイグラムを選んだのは，バイグラムがユーザごとにイベントの発生頻度が直前のイベントに依存するとした場合の

[*1] 他の円グラフも同様.

モデルだからである．この学習月の翌月の正答率を図 5.15 に示す．0.9~1.0 にあるようなユーザ数が 22%，正答率の全ユーザでの平均は 0.67 となり本提案方式による結果よりは明らかに低い値となっている．なおバイグラムでの本人拒否率の平均は 0.33，他人受入率の平均は 0.32 である．これらの値から本章の手法は有意に有効であることを示している．

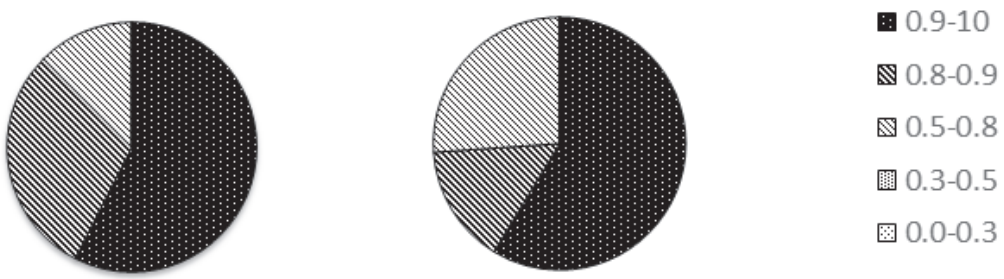


図 5.13　学習月の翌月，翌々月データでのユーザ判定の正答率

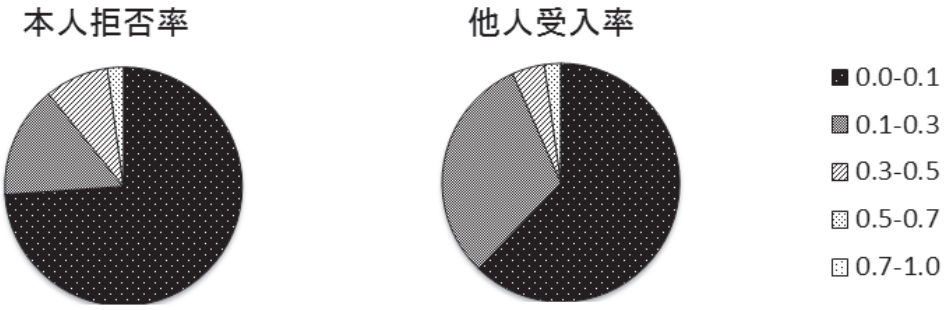


図 5.14　図 5.13 左，翌月データでの本人拒否率と他人受入率

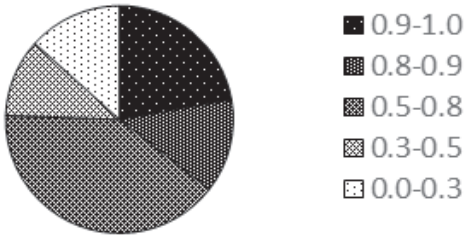


図 5.15　翌月データ (図 5.13 左) でのバイグラムによるユーザ判定の正答率

5.4.3　ループイベントによるユーザアカウントの不正使用の検出

企業内における不正な情報の取得として，他人のアカウントでのログインなどによる不正アクセスが考えられる．そのような不正アクセスは，ユーザ本人が利用していない状態での利用が想定される．そのような場合とは，C1) 本人が終日不在時，C2) 本人が帰宅後，C3) 本人の離席時に他のユーザのアカウントを利用したという状況である．C1) は自明であるので，C2)，C3) を想定して次のようなデータを作成し実験を行った．C2) では，対象ユーザ 40 人からランダムに 10 人選択し，その人のデータの 1 日のイベント系列データから後半の M% の個数のデータを除き，その最後に別のユーザの同数のデータを連結させる，C3) では同様に 1 日のイベント系列データからランダムに M% の個数のデータを除き，同じ個所に他のユーザのものをに混在させる，というデータを作成した．なお，M は 10，20，50 である．C2)，C3) の場合のユーザ判別の正答率は各々図 5.16，図 5.3 の様な結果となった．2 つの図から，C2)，C3) の場合の利用時間が長くなることに相当した，他のユーザログの割合を多くした場合に異常ユーザとして発見しやすくなることが分かる．また，2 つの図を比較すると，他人のデータ追加と他人のデータ混入でほぼ同程度に判別することができている．これは 1 日を単位に判定を行っているため，差が出にくくなっていると思われる．

ある部門において別の部門のユーザを検出できるかを調べるために同一部門で類似した作業を行っている営業部ユーザ同士 7 人のイベント系列データにおいて C3 同様に 10%,

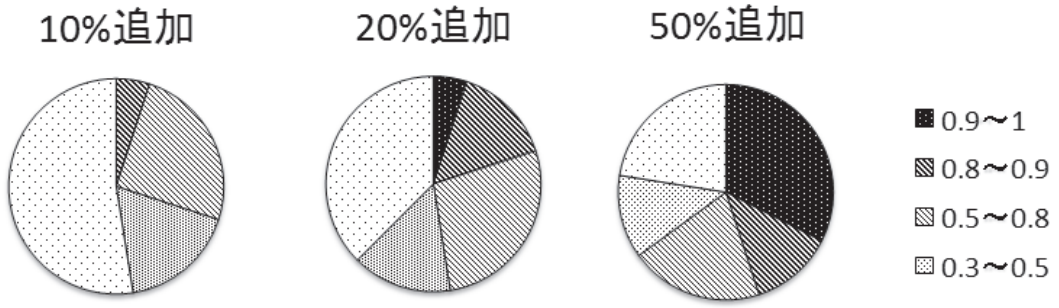


図 5.16　C2 の場合のユーザ判定の正答率

20%，50% のデータをランダムに交換した場合 (D1) のデータ，営業部ユーザと顧客管理部門のユーザ，各 7 人のデータのイベント系列データにおいて C3 同様にランダムに交換した場合 (D2) のデータを作成した．図 5.18 に，この 2 つの場合の異なる部門のユーザの検出率を示す．同図において，D2 の場合，すなわち営業部と顧客管理部門という異なる組織に属するユーザのイベント系列データを交換した場合に，これを検出する割合が極めて高いことを示している．部門が異なると操作も異なり，ウィンドウログも異なる．このため，別の部門のユーザの検出率が高くなることを意味している．すなわち，異なる部門の人間がユーザアカウントの不正使用したような場合には，その検出は容易であることを示している．この手法は重要管理部門などの操作系列が非重要部門で行われているかという検出には適用可能であると考えられる．ただし類似作業を行っている場合のユーザ混入判定には，別の手法を合わせて用いるが必要となる．

5.5 関連研究

本節では，ウィンドウシステムログを用いた不正検出に関する関連研究と，本研究で検討対象とするアクティブウィンドウログについて簡略に説明する．

ログを利用した不正検出やユーザの行動検出についてはナイーブベイズ，主成分分析，隠れマルコフを用いたものなど多くの文献が存在する．代表的なものとして [32] がある．一方，ウィンドウシステムのログ分析による不正検出はコマンドラインログ研究に比べて現状では数が少ない．Shavlik らは，200 以上の Windows2000 のパラメータを毎秒測定し，1500 以上もの評価パラメータでユーザを特定することを試みた [34]．

その結果，95% 程度の確率でユーザを判別できることを示した．しかし，この様な大量

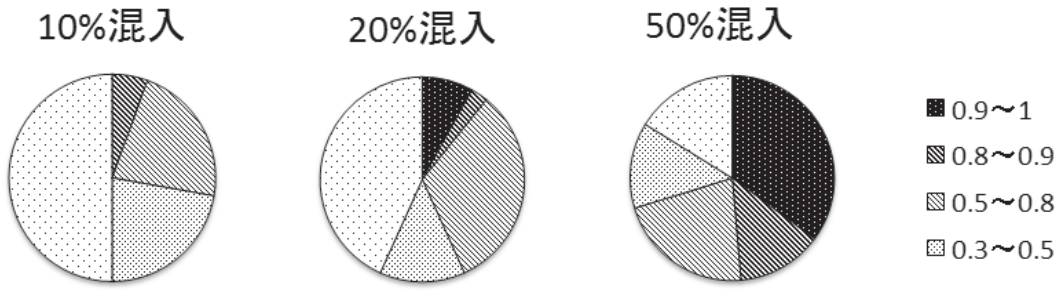


図 5.17　C3 の場合の判定の正答率

のデータを収集し続ける事は本研究が対象とするような一般の業務環境においては難しいと考えられる．

Nguyen らはシステムコールをモニタリングする方式を検討した [35]．彼らはシステムコールの履歴からユーザとファイル，ユーザとプロセス，プロセスとファイルの関係性を中心に分析した．しかし，ユーザの操作パターンがユーザ毎に一定でないために本研究が目的とする不正ユーザ検出には適切ではないと考えられる．

Li らは Windows 環境のデータを一年以上にわたって収集し，それをサポートベクターマシンのプロファイルにより分類しようとした [36]．不正アクセスの検出についてはユーザのデータを混合したデータを作成することでシミュレートした．しかし，ユーザの分離ができるものの高い誤検知率 (False Positive Rate) の解消が困難と述べており，本研究が目的とする不正アクセス検出には向かないと考えらえる．

Goldring はウィンドウのタイトルとプロセステーブルからの情報を 2 年に渡り収集した [37]．ユーザを識別するパラメータとして，ウィンドウ切り替え間隔，新しいウィンドウを開く時間間隔，ウィンドウのタイトルで利用されている語数などで分類する事を提案した．ただし，実際の分析については触れられていないため，提案方式の良否については

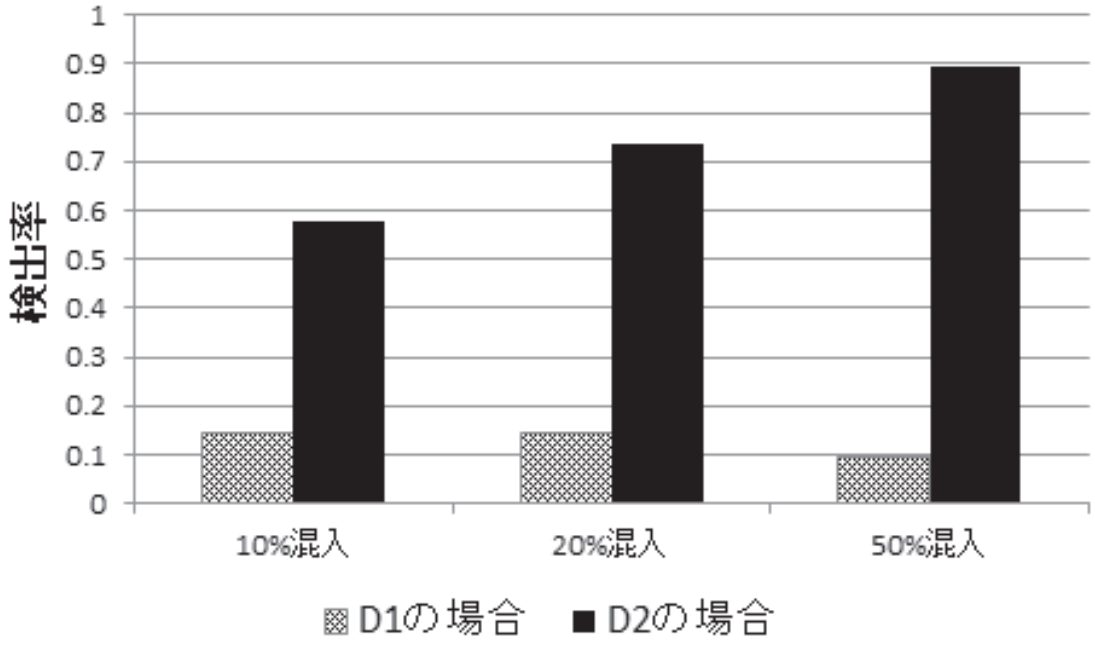


図 5.18　異なる所属部門のユーザの検出率

判定できない．

[38] ではウィンドウログを用いて，ユーザの作業の変化を判別することが可能であることが示された．これは，ユーザ履歴をカーネル PCA により分別することで，典型的な利用パターンを作成し，それの遷移でユーザの状態を示すものである．ただし，この状態遷移でユーザの分別が可能かについての詳細は明らかにされていない．また，ページランキングの手法を用いてウィンドウの使用されるコンテキストを分類し，休憩と作業のタイミングからユーザの分別を行っている．これらの手法はユーザ個別に存在するパターンを見るもので，80 %程度の確率でユーザを分別しているが，本研究が目的とするユーザの行動に不正パターンが含まれるかについての検出についての議論はなされていない．

ウィンドウ操作履歴以外にも，キーボードの打鍵長を捉える事でユーザの分別をおこなう研究もある ([32])．単なるウィンドウの操作履歴だけでなく，複数の入力ログを組み合わせる事で，より精度の高いユーザの判別が可能になると思われる．

5.6 まとめ

本章では，広くオフィスで利用されているツールによりユーザウィンドウ操作をイベントとして取得し，そこからループを形成するイベント系列を抽出して，ループを形成するイベント系列を抽出しベイズ分析により，ユーザの識別，もしくはユーザの行動の変化を簡単に検出しようとした．この場合，オンラインでの分析は難しいが，日単位での分析ではユーザの識別と不正利用の検出の可能性を示すことが出来たと考える．ただし，3.3 節で示したように解析対象の組織において構成員が大きく変化する場合や業務の内容が異なる場合は正答率が下がる．したがって，こういうことが起こらないような学習時期と判定時期が連続している状況下で利用が望ましいと考える．

今後，サーバーアプリケーションや，クラウドコンピューティングなどの手法によりサーバー側での不正検出が重要となる．しかし，サーバー側でのデータ取得は難しいため，利用者端末側でのログの取得並びに分析の重要性はむしろ高まるものと考える．

今後は，解析ターゲットとなるデータの種類を増やした有効性の検証や操作時間，時間的な特徴など他の統計情報との組み合わせによる検出の検討を行いたい．

第 6 章

結論

本論文では，自動車の電子システムの開発を対象として，サイバーセキュリティ開発プロセスの検討をおこなった．本研究では，車という安全性が極めて重視される製品において，サイバー攻撃が発生した場合の車両レベルの対応を安全機能動作と統合するモデルを提示した．このモデルに従い，従来の安全機能の開発と適合性を重視し，サイバー攻撃に対する対処の要件定義からシステムデザインをを安全機能開発のそれと統合する方式を提示した．また，車両開発における分散開発の特徴に留意し，サイバーセキュリティ対策の基礎となるリスクアセスメントについて，車両レベルでのリスク評価を，ここの部品やシステムレベルの開発に反映させるよう，指標による対応のレベル分けを提案した．このようなしくみにより，従来の車両開発体制および開発プロセスと整合性のあるセーフティ・セキュリティ開発プロセスを開発した．

また，高機能化，複雑化する車両システムにおいて，開発対象を正しく定義することは適切なセキュリティ対策を検討する上で必須の要件となる．分散システムの設計と同様，機能間のインターフェイスの定義方法では，システムが複雑化するにつれ，加速度的に設計の難易度が高くなる．そのため，機能間で共有している情報や物理的資源に着目したインターフェイスの定義方法を提案した．この手法では，直接インターフェイスをもたなくても資源を共有している隠れインターフェイスも抽出する．そのため，サイバーセキュリティ設計において網羅的な設計検討が容易となる．

さらに，開発や保守，運用における従業員や関係者が関与する組織内部の重大なセキュリティリスクに対応して，システム利用者の異常行動を検出する方式を提案した．この方式は，既存のユーザの操作ログを利用するもので，大きな導入コストを追加することなく

90% 以上の割合でユーザーの以上を検出可能にした．

今後，あらゆるものがネットワークに接続される IoT システムでは，サイバーセキュリティ技術の適用は必須となる．しかし，IoT システムで制御する対象となる、自動車、医療，産業機械、ロボットなどにおいて、すでに，ISO や IEC などの国際標準化団体が機能安全開発に関する国際標準規格を定めている．そのため、たとえ理想的なサイバーセキュリティ手法であったとしても，これらの規格が定める既存の開発手法や運用形態や安全対策との適合性が低ければ，導入や適用コストが膨大となるうえに，サイバー攻撃発生時に不適切な反応を引き起こす可能性がある．その結果，無適用状態の長期化や形骸化を生み，サイバー攻撃による損失リスクが残存する．さらに、国際標準に準拠しない限り、国際的な至上に参入できないリスクもある．このような事態を回避する面からも，セキュリティの要素技術に加えて，国際標準への準拠，適用対象の基本的な性質や既存の開発，管理運用形態および事故などの損失対策に基づくサイバーセキュリティの研究開発は，今後，重要性をましてゆくものと考える．

謝辞

本研究を行うにあたり，長年にわたり，終始ご指導頂いた兵庫県立大学中本幸一教授，ならびに本論文の副査を努めていただいた五十嵐先生，大島先生に心より感謝いたします．

また，特に車載システムに関連した開発現場からの指摘を頂いた，住友電気工業株式会社および株式会社オートネットワーク技術研究者の同僚技術者ならびに，情報システムの操作記録の利用を許可いただいた株式会社ベイ・コミュニケーションズ総務部に対して熱く御礼申し上げます．

最後に，末筆ではありますが，本研究活動および論文執筆，学会研究会発表などで陰日向なく協力いただいた我が妻子に対し感謝の意を評します．

参考文献

[1] 自動車技術会. 自動車の情報セキュリティ分析ガイド. テクニカルペーパー JASO TP-15002(JP), 2015.

[2] 日本工業標準調査会. 工業標準化と JIS. http://www.jisc.go.jp/jis-act/index.html, 参照 2018 年 8 月 16 日.

[3] Road vehicles - Functional safety - . International Standard ISO 26262:2011, 2011.

[4] Road Vehicles – Cybersecurity engineering, ISO/SAE AWI 21434. https://www.iso.org/standard/70918.html, 参照 2018 年 8 月 16 日.

[5] Functional safety of electrical/electronic/programmable electronic safety-related systems. International Standard IEC 61508：2010, 2010.

[6] Industrial Control Systems Cyber Emergency Response Team. Year in Review 2014. https://ics-cert.us-cert.gov/Year-Review-2013, 参照 2018 年 8 月 16 日.

[7] ISA. ISA99, Industrial Automation and Control Systems Security. https://www.isa.org/isa99/, 参照 2018 年 8 月 16 日.

[8] SAE. Surface Vehicle Recommended Practice. SAE Standard J3016, 2016.

[9] EVITA. E-safety vehicle intrusion protected applications. https://www.evita-project.org/, 参照 2018 年 8 月 16 日.

[10] M. Steiner and P. Liggesmeyer. Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. In *32nd International Conference on Computer Safety, Reliability and Security*, pp. 233–240, 2013.

[11] D. Ward, I. Ibarra, and A. Ruddle. Threat Analysis and Risk Assessment in

Automotive Cyber Security. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, Vol. 6, No. 2, pp. 507–513, 2013.

[12] K. Schmidt, P. Tröger, H.-M. Kroll, T. Bünger, F. Krueger, and C. Neuhaus. Adapted Development Process for Security in Networked Automotive Systems. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, Vol. 7, No. 2, pp. 516–526, 2014.

[13] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner. SAHARA: a Security-Aware Hazard and Risk Analysis Method. In *2015 Design, Automation Test in Europe Conference Exhibition*, pp. 621–624, 2015.

[14] G. Macher, R. Messnarz, E. Armengaud, A. Riel, E. Brenner, and C. Kreiner. Integrated Safety and Security Development in the Automotive Domain. SAE Technical Paper 2017-01-1661, 2017.

[15] R. Baskerville. Information systems security design methods: implications for information systems development. *ACM Computing Surveys*, Vol. 25, No. 4, pp. 375–414, 1993.

[16] A.Shostack. *Threat Modeling: Designing for Security.* Wiley, 2014.

[17] Information technology – Security techniques – Information security risk management. International Standard ISO/IEC 27005:2011, 2011.

[18] Road vehicles - Functional safety - . Under development ISO 26262:2018, 2018.

[19] Road vehicles - Functional safety - Part 3: Concept phase. International Standard ISO 26262-3:2011 (E), 2011.

[20] Road vehicles - Functional safety - Part 10: Guideline on ISO 26262. International Standard ISO 26262-10:2012 (E), 2012.

[21] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald. In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. In *10th Annual Cyber and Information Security Research Conference*, pp. 1:1–1:8, 2015.

[22] C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. `http://illmatics.com/Remote%20Car%20Hacking.pdf`, 参照 2015 年 11 月 15 日.

[23] Philip Koopman and Michael Wagner. Transportation cps safety challenges. 2014 NSF Workshop on Transportation CyberPhysical Systems.

[24] Farinaz Koushanfar, Ahmad-Reza Sadeghi, and Hervé Seudie. Eda for secure and dependable cybercars: Challenges and opportunities. In *Proceedings of the 49th Annual Design Automation Conference*, pp. 220–228, 2012.

[25] S. M. Choi, R. H. Kim, G. Y. Kim, H. K. Lee, G. Y. Gim, and J. B. Kim. A Study of Effective Defense-in-Depth Strategy of Cyber Security on ICS. *International Journal of Security and Its Applications*, Vol. 10, No. 5, pp. 235–242, 2016.

[26] W. van der Hoek, C. Witteveen, and M. Wooldridge. Decomposing Constraint Systems: Equivalences and Computational Properties. In *The 10th International Conference on Autonomous Agents and Multiagent Systems - Volume 1*, pp. 149–156, 2011.

[27] Jean-Philippe Monteuuis, Aymen Boudguiga, Jun Zhang, Houda Labiod, Alain Servel, and Pascal Urien. Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, pp. 3–14, 2018.

[28] W. H. Ware. Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. RAND Report R-609-1, RAND Corporation, 1979.

[29] D. E. R. Denning. A Lattice Model of Secure Information Flow. *Communications of the ACM*, Vol. 19, No. 5, pp. 236–243, 1976.

[30] R. Anderson. A Security Policy Model for Clinical Information Systems. In *1996 IEEE Symposium on Security and Privacy*, pp. 30–43, 1996.

[31] 情報処理推進機構. 組織内部者の不正行為によるインシデント調査. 調査報告書, 2012.

[32] 山西健二. データマイニングによる異常検知. 共立出版, 2009.

[33] M. Salem, S. Hershkop, and S. J. Stolf. A Survey of Insider Attack Detection Research. In *Insider Attack and Cyber Security: Beyond the Hacker*, pp. 69–90. 2008.

[34] J. Shavlik and M. Shavlik. Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage. In *10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 276–285, 2004.

[35] N. Nguyen, P. Reiher, and G. H. Kuenning. Detecting insider threats by monitoring system call activity. In *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop*, pp. 45–52, 2003.

[36] L. Li and C.N. Manikopoulos. Windows NT one-class masquerade detection. 2004.

[37] T. Goldring. Authenticating Users by Profiling Behavior. Invited Talk in ICDM Workshop on Data Mining for Computer Security, 2003.

[38] Kazuhiro Suzuki, Hiroshi Yasuda, Kilho Shin, and Tetsuji Kuboyama. Discriminating User Behavior though PC Operation Logs by PageRank Convergence Patterns. *International Journal of Computer and Communication Engineering*, Vol. 3, No. 1, pp. 37–40, 2014.