氏名	左近　透
学位の種類	博士（応用情報科学）
学位記番号	博情第 50 号
学位授与年月日	平成 30 年　9 月　27 日
学位授与の要件	学位規則第 4 条第 1 項該当（課程博士）
論文題目	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
論文審査委員	（主査）教授　　中本　幸一 （副査）准教授　五十部　孝典 （副査）准教授　大島　裕明

学位論文の要旨

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が試みとしてあげられる．

また，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，本研究での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られる．

論文審査の結果の要旨

自動運転をはじめとして自動車車載システムの高度化に伴い、安全に加えてセキュリティ対策が急務となってきている．車載システムにおいて，サイバーセキュリティ対策は　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)等のあらゆる角度から行う必要がある．

本研究では，上記開発プロセス，情報管理の角度から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．こ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．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．

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．

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．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，大幅に良好な結果を得た．

車載システムにおけるセキュリティ対策の必要性は今後も強まっていく．本研究のアプローチは極めて実践的であり，社会や産業での進展に貢献することが大であり，本博士論文の実用面での価値も大きいということができる．

以上を総合して本審査委員会は，本論文が博士（応用情報科学）の学位授与に値するものと全員一致で判定した.