平成２６年度
ものづくり中小企業・小規模事業者等連携事業創造促進事業
戦略的基盤技術高度化支援事業

「ネットワーク連携が進む次世代自動車・サービスロボット等の利用者安全を保証するセキュリティ基盤ソフトウェアの研究開発」

研究開発成果等報告書概要版

平成２７年　３月

委託者　中部経済産業局
委託先　株式会社ヴィッツ

第１章　研究究開発の概要

１－１　研究開発の背景・研究目的及び目標

【背景】

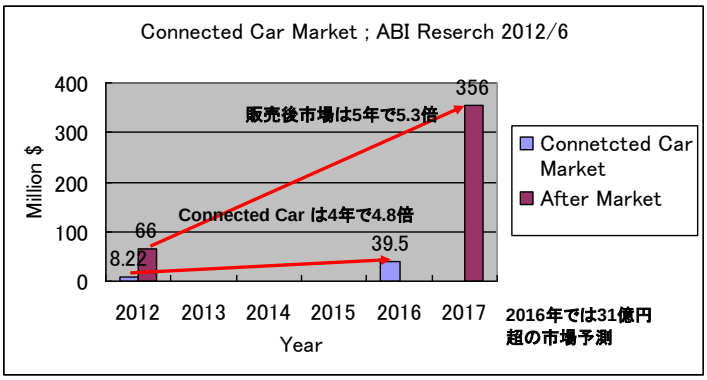


Fig-1 Connected Car 市場予測

我が国の自動車産業は、世界に先駆けた事故防止機能、優れた安全・安心性能、故障が極めて少ない信頼性、高級感がありながらも比較的低価格な車両作りを強みとして、世界市場の大部分を獲得する産業に成長し、自動車大国としての我が国経済を牽引している。我が国で行われている自動車のものづくりは、自動車の**各機能欠陥による事故をなくす設計**と、製品本来の**性能や品質を高める設計の摺合せ開発**を基盤としており、我が国の自動車製品に対する信頼は高い（2010 年の米国における日本車アクセル問題も最終的には**安全性が確認**[1]されている）。

一方、地球温暖化防止に向け、省**エネルギー・再生可能エネルギー活用・エネルギー効果的利用**が、今日の人類に課せられた**大きな課題**となっている。その対策として、あらゆる機器を接続することにより、**エネルギーの需要と供給を管理する統合システム社会**の早期実現が肝要である。とりわけ次世代自動車（Connected Car）は、外部ネットワークと繋がり、統合システムに繋がる機器と連携することにより、省エネルギーおよび利便性向上を実現することが期待され、その市場規模も大きいと予想されている(Fig-1)。例えば、EV/PHV 等の内蔵バッテリ有効活用による**電力消費の平準化**、走行連携・渋滞緩和による**省エネの実現**、暖気・エアコン・ドアロック等の遠隔制御による**快適性や防犯性、メンテナンス性の向上**などが実現しつつある。

しかしながら、次世代自動車を既存技術で構築した場合、外部ネットワークとの接続を想定していない既存自動車では外部ネットワークからの**悪意のある攻撃を防衛することができず**、外部からの制御部位へ危険指令が到達する可能性があり、**事故誘発を謀るテロ行為にも悪用される懸念**がある。さらには**悪意のある ECU 書換え**が行われる恐れがあり、**自動車の武器化**に悪用される懸念がある（既存の自動車は外部ネットワークと接続されていないため、このような脅威はいまのところ存在しない。可能性があるとすれば開発者または整備作業者

[1] www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf Toyota unintended Acceleration Investigation

による内部犯行に限られる)。

実際、米 Washington 大学 Kohno 博士らの実証実験論文では、車両通信である CAN のセキュリティ脆弱性を攻撃することにより、**エンジン動作中の CAN 通信停止**や **ECU 書換えモード移行に成功**したという報告がなされている。同様に Rutgers 大学からはタイヤ監視無線ネットワークの脆弱性が、Zurich 大学からは無線電波信号の遠隔操作に関する脆弱性が指摘されている。いずれも上述の新たな脅威の原因となるセキュリティ問題であり、**現代社会における重大なリスク要因**である。

このような現状から、次世代自動車の実現には以下の 2 つの課題(課題Ⅰ、Ⅱ)が存在する。

課題Ⅰ：ネットワークに繋がることで発生する新たな自動車のセキュリティ脆弱性に対処する必要がある。

課題Ⅱ：悪意のある ECU 書換えを防止し、制御の“のっとり”（自動車の武器化）を防止する必要がある。

他方、2010 年 米国における日本車アクセル問題では、製品の実品質は高いものの、それを裏付けるエビデンス文書の不足などから十分な説明ができず、全ての日本製品の品質が疑われ一部に不買運動が起こるなどした。このように国際社会に対する**品質説明力を備えておくことは、もはや必須**のこととなっている。さらに今後は、統合システム化の進展に伴い接続連携している各システムの問題が相互に影響を及ぼすため、製品の品質を第三者に明瞭に説明する必要性が増大すると考えられる。よって、この品質説明において以下の課題(課題Ⅲ)が存在する

課題Ⅲ：国内品質説明力を強化し、ソフトウェア品質監査制度を早期に制定・定着させる必要がある。

また、経済産業省による技術指針において、早急に対処が必要な技術に位置づけられる「**統合システム**」に関連する研究であり、また、応用分野も「**ロボット**」「**自動車**」など重点的分野への利活用が期待できる。さらに、我が国が比較的弱いとされる「品質説明力」の強化を目的とした IPA の「**ソフトウェア品質監査制度(仮称)**」の審査および監査を予定しており、我が国が**早急かつ重点をおくべき政策と一致**している。

【課題への対策】

セキュリティ脆弱性に対する攻撃パターンは、攻撃者や攻撃技術の進化により常に変化す

る（Moving threats）。そこで対策としては、**多様な攻撃を柔軟に対処**できることと、**攻撃の影響を他部位に広めないこと**が重要となる。

これを実現して上記【課題Ⅰ】および【課題Ⅱ】に対処するために、我々が現在開発中のパーティション OS が有効である。パーティション OS は、故障や不具合によるソフトウェア誤動作の影響が他部位に伝播することを防ぐ防衛機能を有しており、これまでは主として安全性の確保を目的として開発を行ってきた。これに機能を追加することで、セキュリティの確保にも応用する。

具体的には、アプリケーションプログラムの制御をつかさどる部位（制御パーティション）を、外部ネットワークとの通信をつかさどる部位（通信パーティション）から、**パーティション OS によって隔離**し、仮に通信パーティションが外部から攻撃を受けたとしても、制御パーティションに**影響が伝播しない技術**を確立する。そのために、通信パーティションの外部からの入り口、および、パーティション間の通信部位の 2 か所に**ファイアウォール（通信遮断機構**）を設ける。さらに、これら 2 か所のファイアウォールの間に、**ハニーポット（囮**）をしかける。攻撃者は外部ファイアウォールを突破した後、内部だと誤認してハニーポットを攻撃するが、これを悪意攻撃として特定して、攻撃者の他パーティションへの通信をパーティション間通信部位に設置したファイアフォールで**遮断**する。これにより【課題Ⅰ】の悪意指令などを防ぐと共に、【課題Ⅱ】の ECU ソフトウェア書換えも信頼できる場合のみに制限することが可能である。また、いずれの場合も攻撃者に対しては**攻撃が成功したと見せかける機能**を備えて、新たな攻撃を避ける工夫もする。

【課題Ⅲ】への対策として、これらの開発を機能安全規格 IEC 61508 および ISO 26262 に準拠して[2]実施した上で、IPA が策定中の**「ソフトウェア品質監査制度(仮称)」の審査を実施**して、第三者に対する品質説明が可能な資料（エビデンス）を備え、品質説明力向上に対処する。

なお、【課題Ⅰ】および【課題Ⅱ】の対策として、【1. 基盤ソフトウェアのセキュリティ要件導出】、【2. 基盤ソフトウェアのセキュリティコンセプトおよび仕様開発】、【3. セキュリティ基盤ソフトウェアの開発】をサブテーマとして実施し、【課題Ⅲ】の対策として【4. ソフトウェア品質監査制度に基づく適合監査】をサブテーマとして実施する。

[2] 機能安全規格 IEC 61508 および ISO 26262 のプロセス認証をドイツ TUV SUD から取得しているのは、日本で唯一本研究メンバである株式会社ヴィッツのみである。

本研究の対象は次世代自動車であるが、**統合システムの要素となる制御系システムは、すべて同様のセキュリティ課題を内包**している。本研究で開発するセキュリティ課題解決のための技術は、これら製品に共通で利用できる**メタ技術**であるため、**サービスロボット、産業用ロボット、家庭内デジタル家電など多くの分野で利用**でき、対象となる**市場の裾野は広い**。

【目標】

自動車と交通システムに関する、川下製造業者等の特有の課題及びニーズを踏まえた高度化目標

・自動車の知能化・情報端末化機能の向上

・EV/PHV 等の大量導入に対応できるインフラ構築

現在の自動車の制御 ECU は、外部ネットワークからソフトウェアをローディング及び実行するものは無い。従って、信頼できるサプライヤ企業の製品を利用している限り、渋滞緩和や省エネ・エネルギー利用効率向上等を目的とする連携走行のための遠隔制御において、**重篤な危害に至り得るセキュリティ問題の可能性は小さい**と言える。

しかしながら、**外部ネットワークに接続される場合には**、ECU ソフトウェアを悪意のあるソフトウェアに変更される恐れがあり、**サプライヤ企業の信頼性だけでは対処できな**い。本研究では、信頼できない ECU ソフトウェア**書換えを防止**することにより、自動車の知能化・情報端末化およびインフラ構築を**安全に実現**する。

ロボットに関する、川下製造業者等の特有の課題及びニーズを踏まえた高度化目標

・ネットワーク対応型ロボット用プラットフォーム・OS の構築

サービスロボットは他の組込み製品とは異なり、保護すべき個人情報（**個人識別情報、行動情報、発話情報**など）を多く有する場合があり、**情報漏えい**に対するセキュリティも重要である。これについても、本研究で開発するセキュリティ基盤ソフトウェアによって**対処可能**である。

川下分野横断的な共通の課題及びニーズを踏まえた高度化目標

・組込みソフトウェア開発技術の創出

ⅰ）更なる安全性・信頼性確保に向けた技術の高度化

ⅱ）システムの統合化に向けた技術の高度化

システム統合化に向けた中核技術開発として、組込み機器の**安全性・信頼性技術の高度化**が必要となる。すなわち、組込み機器が**システム統合した場合**のセキュリティおよび**利用者安全を強固に維持**しなければならない。本研究では、組込みシステムの基盤ソフトウェアを開発し、セキュリティ対策として、**外部からの攻撃を防**ぐための二重ファイアウォールおよびハニーポット機能を実装する。同時に、利用者安全を脅かす可能性がある、組込みソフトウェアの**悪意ある書換えを防止**する。

・他分野横展開に伴う技術的障壁の解決

ⅰ）品質説明力の強化に向けた技術の高度化

日本の組込みソフトウェア開発技術は、高安全・高品質な製品開発能力があるにもかかわらず、**品質説明力の低さが不利益**となっている。今後の統合システムでは、連携する個々の機器が安全性・信頼性などの**品質説明力を備えることが重要**となると考えられる。本研究では、開発成果物であるセキュリティ基盤ソフトウェアに高い品質説明力を持たせることによって、それを組込んだ機器自体が、外部からの攻撃に対抗できることの**説明が可能**となる。すなわち、**品質説明力の高い製品開発を推進**することとなる。

【1. 基盤ソフトウェアのセキュリティ要件導出】

次世代自動車とサービスロボットを対象に、セキュリティ脅威による**利用者安全の侵害**、**ソフトウェア書換えモードへの移行**、ネットワークおよび**プロセッサの動作モード変更**、**内部データの参照および書換え**等の脅威の**抽出と分析**を行い、基盤ソフトウェアに対する**セキュリティ要件を導出**する。

【2. 基盤ソフトウェアのセキュリティコンセプトおよび仕様開発】

利用者安全のための**セキュリティ基盤ソフトウェアのコンセプト**を開発し、その妥当性を確認するために、**国際認証機関**よる第三者レビューを受けて**コンセプトレポートを取得**する。確認できたセキュリティコンセプトに基づいて、セキュリティ基盤ソフトウェア仕様を完成する。

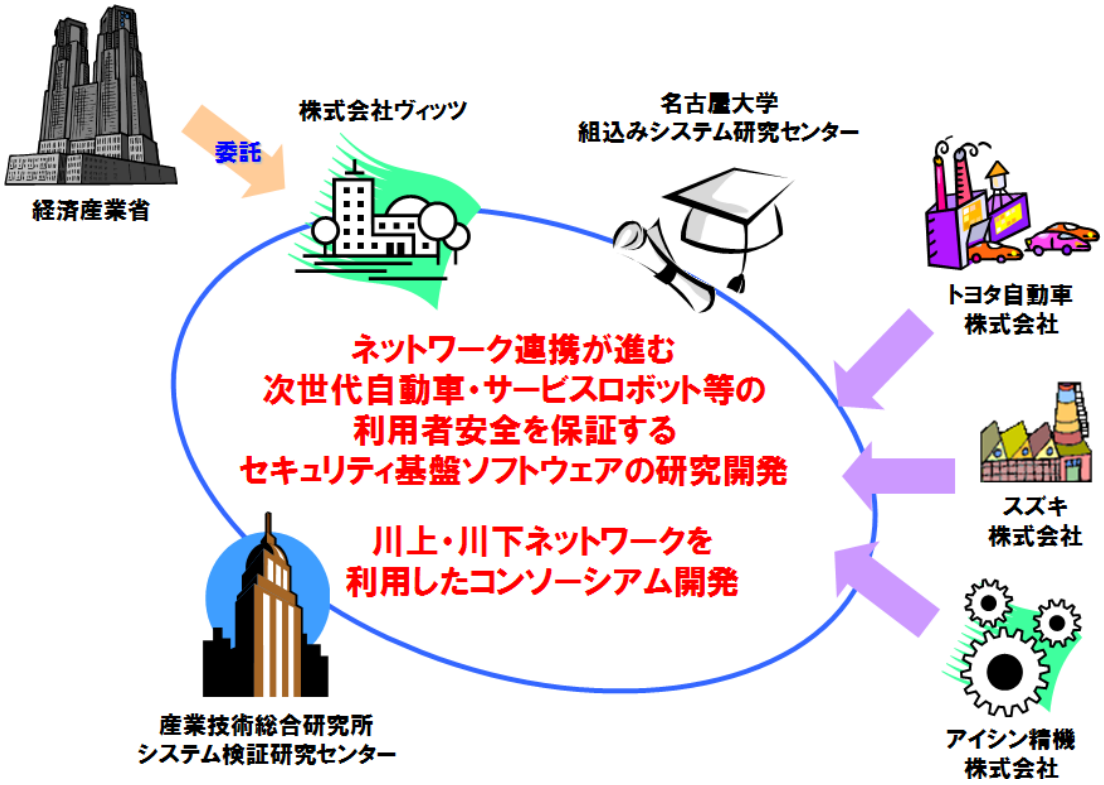
なお技術的な目標値は、想定脅威モデルにおいて、**セキュリティ脅威を 90%以上検出**し、考えられる**安全リスクを 10%以下に低減**することとする。この数値は国際的な有識者（国

際認証機関を想定）と協議し、**妥当性を確認**する。

【3. セキュリティ基盤ソフトウェアの開発】

セキュリティ基盤ソフトウェアを、**機能安全規格 IEC 61508 および ISO 26262 に準拠して開**発する。開発する基盤ソフトウェアは組込み向けであるため、非機能要件も目標値に設定することとし、装置内で利用可能なリソース性能（動作速度、ROM/RAM 使用量）を満足させる。具体的数値として、リスク低減処理による**通信処理時間の増加は 15%以下**、**ROM/RAM 使用量増加は 20%以下**を目標とする。

１－２　研究体制



株式会社ヴィッツ

再委託 → 独立行政法人産業技術総合研究所

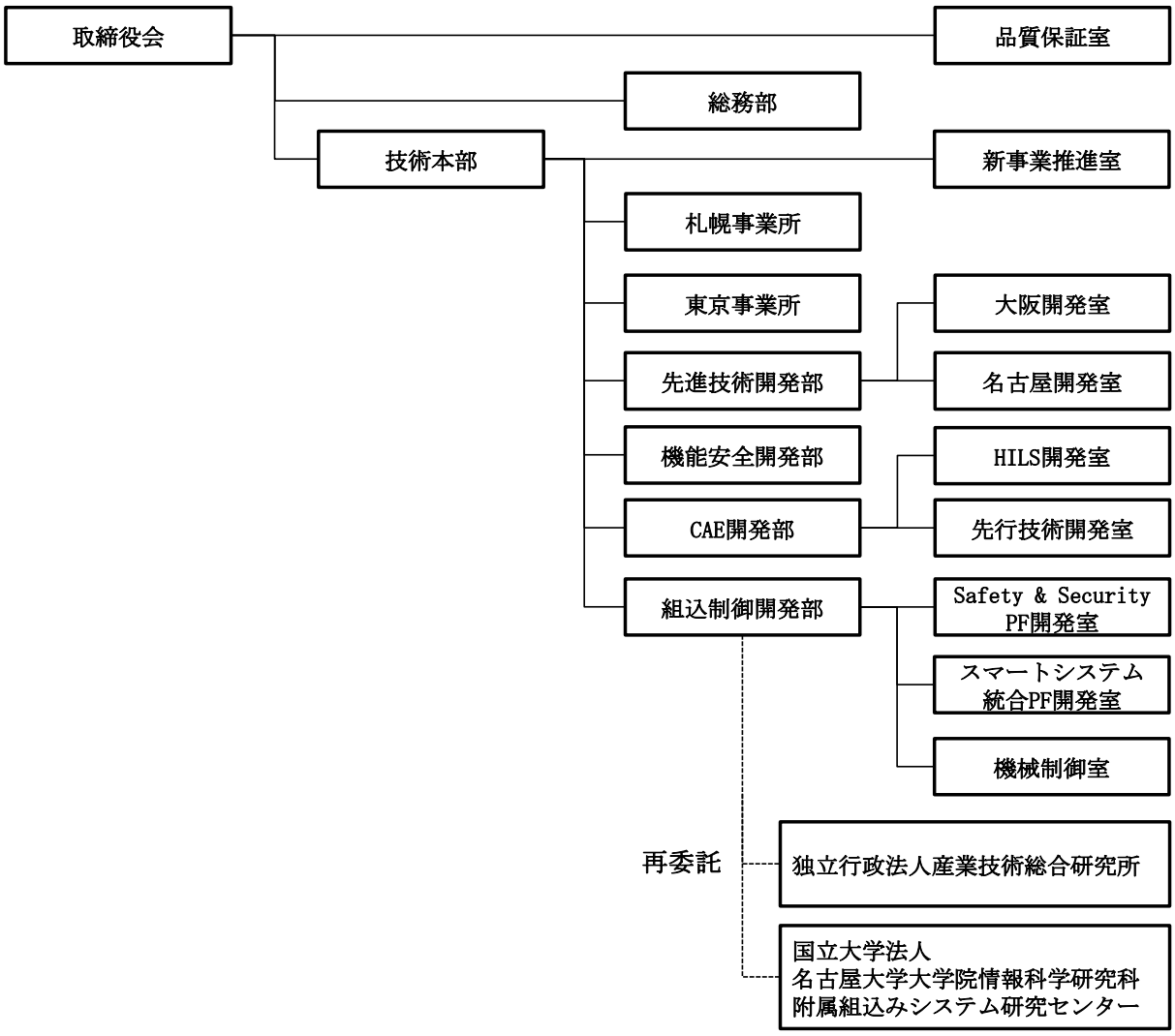
再委託 → 国立大学法人　名古屋大学
大学院情報科学研究科
附属組込みシステム研究センター

総括研究代表者（PL）
国立大学法人名古屋大学
大学院情報科学研究科
附属組込みシステム研究センター
教授/センター長
高田 広章

副総括研究代表者（SL）
株式会社ヴィッツ
常務取締役
技術本部
組込制御開発部 部長
服部 博行

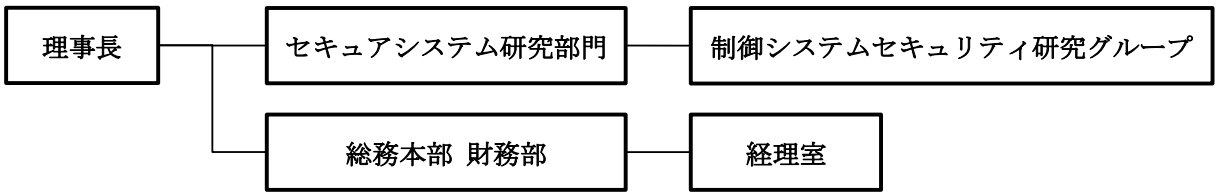
＜事業管理者＞

株式会社ヴィッツ

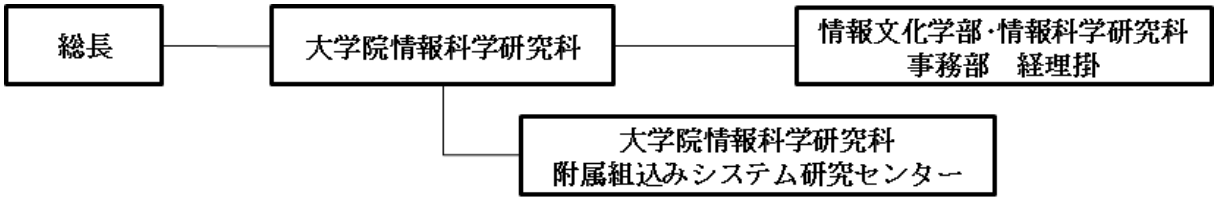


＜再委託先＞

独立行政法人産業技術総合研究所

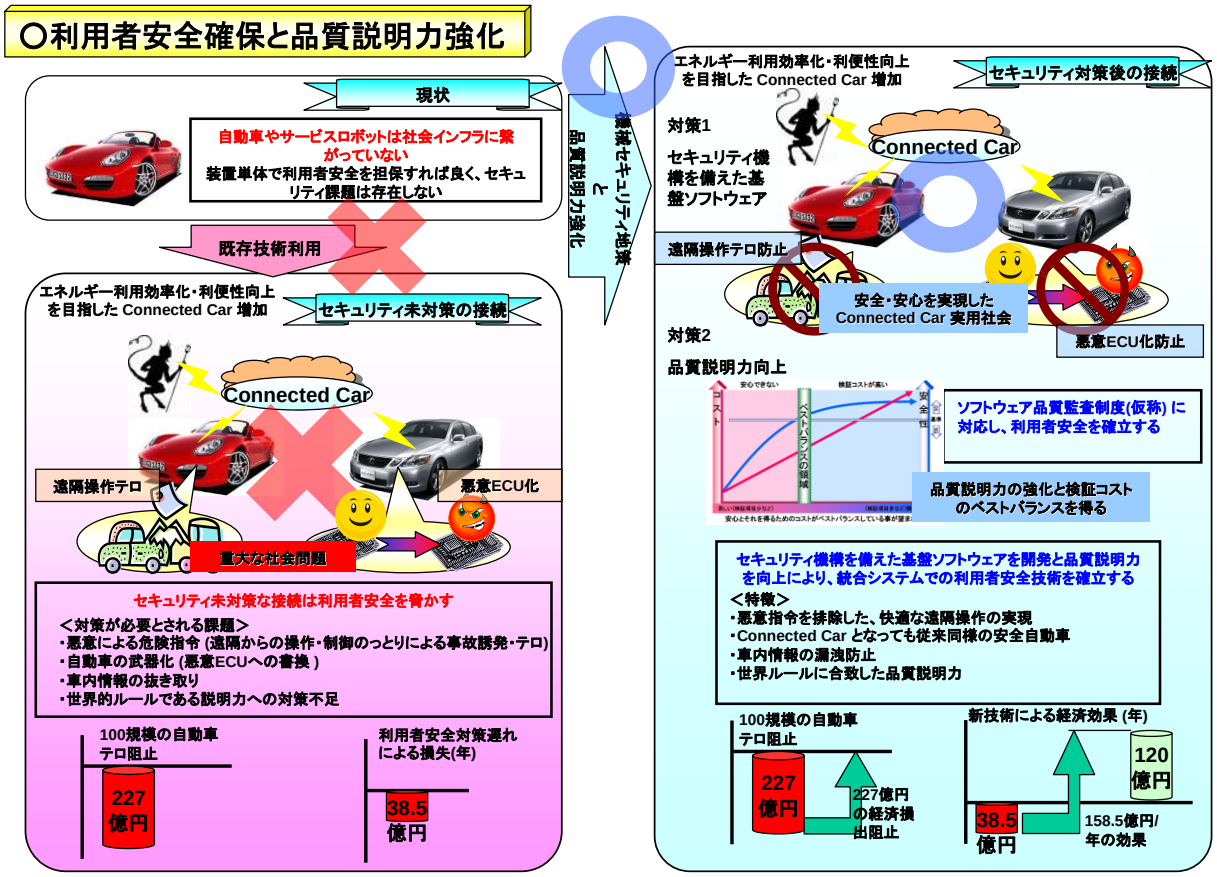


国立大学法人名古屋大学 大学院情報科学研究科　附属組込みシステム研究センター



１－３　成果概要

本研究では、蓄電池を用いたエネルギー利用の効率化や、車両間および車両-インフラ間連携による省エネルギーの手段として注目を集める次世代自動車（Connected Car）が抱えるセキュリティおよび安全性の課題を解決する。すなわち、自動車が「統合システム」の一員として外部ネットワークに繋がることにより、新たに発生するセキュリティ脅威への対策を行う研究開発である。なお本研究成果は統合システムの構成要素となるサービスロボット等にも利用できる技術である。



○ 新技術を実現するために解決すべき研究課題

エネルギー利用効率化および省エネルギー対策として、統合システム社会の早期実現が切望されている。次世代自動車は、外部ネットワークを通して統合システムの一員となることで（Connected Car）、内蔵する大容量バッテリを有効利用したエネルギー消費量の平準化や、自動車間および自動車-インフラ間連携による省エネルギーなどへの貢献が期待されている。しかしながら、セキュリティ対策がほどこされていない既存技術で単に繋げた場合、外部ネットワークと車両内部装置（例えばカーナビ）が繋がることで、外部ネットワークからの悪意ある攻撃が、車両内部装置を経由して、それに繋がる車両制御ネットワーク（例え

ば CAN 通信）に侵入し、**自動車制御装置に悪意ある指令を実行する可能性**がある。その結果、最悪の場合には**ブレーキの無効化**や**意図しないアクセル操作による急発進**など、**操作や制御がのっとられる恐れ**があり、事故誘発を謀る**テロ行為**にも悪用されかねない。こうした懸念は、外部広域ネットワークと接続していない**既存自動車ではありえない**が、次世代自動車（Connected Car）においては、**利用者および社会の安全に対する新たな脅威（セキュリティの脆弱性に起因し利用者の生命・財産や社会に損害がおよぶ危険性）**であり、早急な対策が必要となっている。実際、米国運輸省道路交通安全局（NHTSA）は GM 社の車両に搭載されている遠隔制御機能の危険性を認めており、**我が国の車両メーカーは NHTSA の要望により対策に迫られている**。

この種の脅威は、サービスロボットなど統合システムと連携するすべての**制御装置に共通する課題**であるといえる。そこで本研究では、統合システム社会における新たな脅威を分析により明確にした上で、統合システム社会での**利用者安全と社会安全を達成するセキュリティ基盤ソフトウェアを開発**する。この基盤ソフトウェアは、セキュリティ攻撃の早期発見と悪意指令の侵入防止を目的とし、パーティション機能を有する制御用 OS をベースとして開発する。これにより、制御装置に対する**セキュリティ攻撃の大部分を検出**し、**制御部位への進入を断つ**ことで利用者および社会に対する潜在的安全リスクの大幅な低減を実現する。なお車載ネットワーク等のセキュリティ脆弱性研究では第一人者の、米ワシントン大学準教授 Kohno 博士への聞き取り調査によれば、こうした**基盤ソフトウェアによる対策は、他に取組み例がない**。

さらに本研究では、開発作業を**機能安全規格（ISO 26262／IEC 61508）に準拠**して行い、かつ、IPA（独立行政法人情報処理推進機構）が策定中の**「ソフトウェア品質監査制度（仮称）」の審査および監査**を実施する。これにより、国内大手自動車メーカーの米国でのリコールで問題となった第三者に対する**品質説明力を国際レベル程度に確保**し、セキュリティおよび安全性の説明が可能な基盤ソフトウェアを実現する。以上を通じて本研究では、統合システム社会における利用者安全技術の確立を目指す。

〇研究開発の具体的内容

組込みソフトウェアにおける高度化目標達成に資する特定研究開発等の実施方法

(1) 技術要素の高度化（技術開発及びソフトウェアの開発）

・プラットフォーム

・セキュリティ部品

システム統合を構成する要素製品の開発に必要な、**セキュリティおよび利用者安全上の課題を解決**できる**基盤ソフトウェア(ソフトウェアプラットフォーム)**を、安全規格（IEC 61508／ISO 26262）に準拠して開発する。

(2) 開発技術の高度化（手法開発及びその支援ツールの開発）

・機能安全技術（リスク分析技術、安全設計技術等）

・ソフトウェアの実装

・独立検証・他動性確認技術（IV&V）等テスト/検証

・セキュリティシステム

・システム統合化（スマートエネルギー、サービスロボットシステム等）

・クラウド環境を前提とした組込みシステム

研究開発する基盤ソフトウェアが自動車 ECU のソフトウェアプラットフォームに活用されると仮定して、**セキュリティ分析および安全分析**を行い、自動車 ECU の**セキュリティおよび安全要件を導出**する。導出した要件を**機能安全規格（IEC 61508／ISO 26262）が要求する開発手法**を用いて基盤ソフトウェアの**開発・実装**を行なう。これらにより、機能安全技術、ソフトウェアの実装、セキュリティシステムを高度化する。

さらに、IPA（独立行政法人情報処理推進機構）が検討を進めている「**ソフトウェア品質監査制度(仮称)**」に基づく**審査・監査**を実施することで、独立検証・他動性確認技術(IV&V) 等テスト/検証を高度化する。

クラウド環境を前提とした組込みシステムに、本研究の成果である**セキュリティ基盤ソフトウェア**を用いることで、システム統合に利活用できる**セキュリティ製品を実現**することが可能となり、システム統合化、クラウド環境を前提とした組込みシステムを高度化する。

(3) 管理技術の高度化（手法開発及びその支援ツールの開発）

・トレーサビリティ管理、定量的開発管理

・技術文書の品質向上（自動生成、自動チェック等）

本研究で開発する基盤ソフトウェアは、**機能安全規格 IEC 61508／ISO 26262** に準拠して開発する。そのため、機能安全規格が要求するレベルの**トレーサビリティ管理を実施**するとともに、**技術文書品質を確保**する。IPA が検討している「ソフトウェア品質監査制度

(仮称)」の監査も実施し、本研究成果が妥当な**品質を備えていることを立証**する。

○具体的対処方法

提案者らが開発中の故障や不具合による誤動作を他部位に伝播することを防ぐ**パーティションOS**に、**多重ファイアウォール**と**ハニーポット（囮）**をしかけ、**悪意攻撃指令を検出**し、制御を行うパーティションへの**攻撃を遮断**する。これらの機能を機能安全に対応した開発をし、IPA が検討している「ソフトウェア品質監査制度(仮称)」にも同時に準拠し、**品質説明力向上**を模索する。

【1. 基盤ソフトウェアのセキュリティ要件導出】

【1.1 基盤ソフトウェアのセキュリティおよび安全分析】

セキュリティ基盤ソフトウェアを、**自動車制御 ECU** と**サービスロボット動作制御コンピュータ**に利用すると仮定し、**セキュリティ脅威の抽出と分析**を行う。セキュリティ脅威から保護するべき点として、1. セキュリティ脅威による**利用者安全の侵害**　2. 組込みソフトウェアの**書換えモード移行**　3. ネットワークおよび**プロセッサの動作モード変更**　4. 内部データへの**参照および変更指令** を対象とし、セキュリティ脅威の抽出を行う。

想定開発成果：基盤ソフトウェアのセキュリティおよび安全分析結果

【1.2　セキュリティ基盤ソフトウェア要件定義】

抽出した脅威への対策を検討し、基盤ソフトウェアの要件として定義する。

想定開発成果：セキュリティ基盤ソフトウェア要件定義書

【2. 基盤ソフトウェアのセキュリティコンセプトおよび仕様開発】

【2.1 基盤ソフトウェアのコンセプト開発】

基盤ソフトウェアのセキュリティ要件導出で抽出したセキュリティ基盤ソフトウェア要件が、提案者らが開発を終えつつあるパーティション OS と、Fig-2 に示す機構によって実現可能であることを立証して、基盤ソフトウェアのセキュリティコンセプトとて開発する。

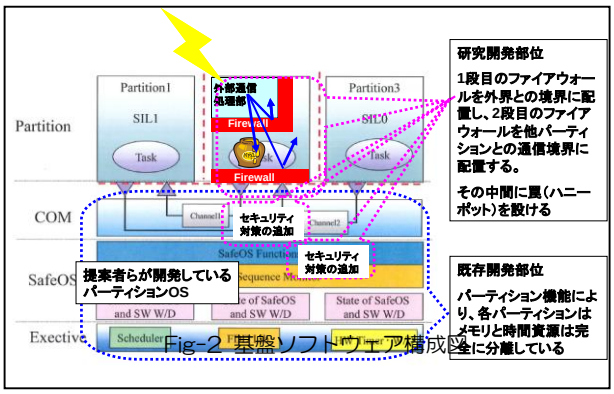


Fig-2 基盤ソフトウェア構成図

想定開発成果：基盤ソフトウェアのセキュリティコンセプト（日本文・英文）

【2.2 基盤ソフトウェアのコンセプトレポート取得】

開発したコンセプトは**国際認証機関**等からレビュー評価を受けてその妥当性を確認し、**コンセプトレポートを取得**する。

想定開発成果: 基盤ソフトウェアのコンセプトレポート（国際認証機関より取得）

【2.3 基盤ソフトウェアの仕様開発】

現在のところ、多重ファイアフォールおよびハニーポットによる機能を検討しているが、上記【1】の要件導出および本サブテーマ実施時に得られた**必要対策機能が明確となれば随時追加**する。これらの機能群をまとめて、**セキュリティ対策ライブラリ仕様**を策定し、完成間近の**パーティション OS 仕様とマージして、基盤ソフトウェアの仕様を開発**する。

想定開発成果：セキュリティおよび利用者安全への対策ライブラリと基盤ソフトウェア仕様書、セキュリティマニュアル

【3. セキュリティ基盤ソフトウェアの開発】

【3.1 セキュリティ対策ライブラリの開発】

上記【2】で開発した仕様を元に、**セキュリティ対策ライブラリを開発**する。開発には、自動車向け機能安全規格 **ISO 26262 ASIL D** および 一般機器向け機能安全規格 **IEC 61508 SIL 3** が要求する手法、管理および開発プロセスを用い、**ISO 262626 ASIL D および IEC 61508 SIL 3 のレベルに対応可能なライブラリを開発**する。

想定開発成果：セキュリティ対策ライブラリ

【3.2 セキュリティ基盤ソフトウェアの開発】

【3.1】の成果と提案者らが開発中のパーティション OS と結合し、セキュリティ基盤ソフトウェアを完成させる。

想定開発成果：基盤ソフトウェア、開発エビデンス（IEC 61508 SIL3 用、ISO 26262 ASIL-D 用）

１－４　当該研究開発の連絡窓口

＜事業管理者＞

株式会社ヴィッツ

愛知県名古屋市中区栄2-13-1 名古屋パークプレイス

＜経理担当者＞

株式会社ヴィッツ

総務部　グループリーダー　佐藤倫子

TEL：052-220-1218　FAX：052-218-5855

E-mail：noriko@witz-inc.co.jp

＜業務管理者＞

株式会社ヴィッツ

専務取締役　技術本部　本部長　服部博行

TEL：052-223-7570　FAX：052-218-5855

E-mail：hat@witz-inc.co.jp

第2章　基盤ソフトウェアのセキュリティ要件導出

【概要】

次世代自動車とサービスロボットを対象に、セキュリティ脅威による利用者安全の侵害、ソフトウェア書換えモードへの移行、ネットワークおよびプロセッサの動作モード変更、内部データの参照および書換え等の脅威の抽出と分析を行い、基盤ソフトウェアに対するセキュリティ要件を導出する。

2−1　基盤ソフトウェアのセキュリティおよび安全分析

【目標】

本研究で開発する基盤ソフトウェアは、IT 融合システムで連携される組込み機器を対象とする。そのため、本研究成果である基盤ソフトウェアが幅広い分野で利用できるために、安全分析の対象とする機器は「自動車制御 ECU」と「サービスロボット動作制御コンピュータ」とし、セキュリティ脅威が直接安全を脅かす恐れがあるシビアな装置を選択する。

セキュリティ脅威から保護するべき点として、

1. セキュリティ脅威による利用者安全の侵害
2. 組込みソフトウェアの書換えモード移行
3. ネットワークおよびプロセッサの動作モード変更
4. 内部データへの参照および変更指令

を対象としてセキュリティ脅威の抽出を行い、基盤ソフトウェアのセキュリティおよび安全分析結果をまとめる。

【研究成果】

基盤ソフトウェアが利用される想定システムのセキュリティ分析を行い完成させることができた。その結果からセキュリティの脅威から守るべき点を導出することができた。

【課題】

基盤ソフトウェアが利用される想定システムのセキュリティ分析を行うことができたため、今後の課題はない。

2−2　セキュリティ基盤ソフトウェア要件定義

【目標】

「基盤ソフトウェアのセキュリティおよび安全分析」の分析結果から得られる脅威への対策方法を検討し、基盤ソフトウェアへの対策要件を定義する。

【研究成果】

基盤ソフトウェアの要件を定義するためにセキュリティの規格である IEC62443 の調査検討は完了した。調査内容を３－１基盤ソフトウェアのコンセプト開発、３－３基盤ソフトウェアの仕様開発を大幅に進めることが可能となった。

【課題】

IEC62443 の正式版が発行されなかったため、今後ドラフト版から正式版が発効されたらドラフト版と正規版の差分を調査する必要がある。

第３章　基盤ソフトウェアのセキュリティコンセプトおよび仕様開発

【概要】

利用者安全のためのセキュリティ基盤ソフトウェアのコンセプトを開発し、その妥当性を確認するために、国際認証機関よる第三者レビューを受けてコンセプトレポートの取得に必要な指摘事項を得る。確認できたセキュリティコンセプトに基づいて、セキュリティ基盤ソフトウェア仕様を完成する。

なお技術的な目標値は、想定脅威モデルにおいて、セキュリティ脅威を 90%以上検出し、考えられる安全リスクを 10%以下に低減することとする。この数値は国際的な有識者（国際認証機関を想定）と協議し、妥当性を確認する。

3−1　基盤ソフトウェアのコンセプト開発

【目標】

「基盤ソフトウェアのセキュリティ要件導出」にて抽出したセキュリティ基盤ソフトウェア要件が、提案者らが所持するパーティション OS とハニーポット（囮）を有する多重ファイアフォール機構によって実現可能であることを立証し、基盤ソフトウェアのセキュリティコンセプトを開発する。

セキュリティとセイフティの確保の為に、国際認証機関と技術協議を実施し世界最高水準の技術

導入をはかる。

【研究成果】

Security OS の想定システムのセキュリティ分析を完成させ、コンセプトレポート取得レベルにすることはできた。

【課題】

TUV SUD からコンセプトレポートの発行はしてもらえたが、TUV SUD から微小な指摘が出ているため、指摘事項を対応する必要がある。

3−2　基盤ソフトウェアのコンセプトレポート取得

【目標】

「基盤ソフトウェアのコンセプト開発」にて開発したコンセプトは国際認証機関等からレビュー評価を受けて妥当性を確認する。妥当性確認方法として、来年度認証機関からコンセプトレポートを取得する事を目指して作業を進める。

【研究成果】

作成したドキュメントに対して TUV SUD から意見をもらうことができレポートの発行をしてもらえた。

【課題】

レポートの発行はしてもらえたが、TUV SUD から指摘が出ているため、指摘事項を対応する必要がある。

3−3　基盤ソフトウェアの仕様開発

【目標】

研究開始時は多重ファイアフォールおよびハニーポットによるセキュリティ対策機能を検討する。また、基盤ソフトウェアのセキュリティ要件導出の結果により得られた必要対策機能が明確となれば、これらの対策機能を随時追加する。

これら機能群をまとめてセキュリティ対策ライブラリとして策定し、提案者らが保持するパー

ティション OS 仕様とマージして基盤ソフトウェア仕様として開発する。

【研究成果】

の Security OS の Security Requirement Specification の開発を行い、TUV SUD のレビューを受けることができた。

【課題】

Security Requirement Specification に対して TUV SUD から指摘が出ているため、指摘事項を対応する必要がある。

第４章　セキュリティ基盤ソフトウェアの開発

【概要】

セキュリティ基盤ソフトウェアを、機能安全規格 IEC 61508 および ISO 26262 に準拠して開発する。開発する基盤ソフトウェアは組込み向けであるため、非機能要件も目標値に設定することとし、装置内で利用可能なリソース性能（動作速度、ROM/RAM 使用量）を満足させる。具体的数値として、リスク低減処理による通信処理時間の増加は 15%以下、ROM/RAM 使用量増加は 20%以下を目標とする。

4－1　セキュリティ対策ライブラリの開発

【目標】

基盤ソフトウェアの仕様開発にて検討した、セキュリティ対策ライブラリの仕様を基に、セキュリティ対策ライブラリの開発を行う。また、開発するセキュリティ対策ライブラリは IEC62443 に準拠して開発を行う。

【研究成果】

基盤ソフトウェアの仕様開発の研究成果を活用して、セキュリティ対策ライブラリの開発には成功した

【課題】

リスク低減処理による通信処理時間の増加が 15%以下、ROM/RAM の使用量増加は 20%以下

という目標に対してソースコードの改善が必要である。

4－2　セキュリティ基盤ソフトウェアの開発

【目標】

基盤ソフトウェアの使用開発にて検討した、セキュリティ基盤ソフトウェアの仕様を基に、セキュリティ基盤ソフトウェアの開発を行う。また、開発するセキュリティ基盤ソフトウェアは IEC62443 に準拠して開発を行う。

【研究成果】

本年度は IEC62443 に準拠したセキュリティ規格ドキュメント及び IEC62443 に対応したセキュリティ基盤ソフトウェアを開発する目標が達成できた。

【課題】

通信処理時間や ROM/RAM の使用量等、性能面で課題が見つかっているため、性能面の改善を進める必要がある。

第５章　海外調査

【概要】

次世代自動車（Connected Car）を既存技術で構築した場合、外部ネットワークとの接続を想定していない既存自動車では外部ネットワークからの悪意攻撃を防衛することができず、外部からの制御部位へ危険指令が到達する可能性があり、事故誘発を謀るテロ行為にも悪用される懸念がある。さらには悪意ある ECU 書換えが行われる恐れがあり、自動車の武器化に悪用される懸念がある。

実際、米 Washington 大学 Kohno 博士らの実証実験論文では、車両通信 CAN のセキュリティ脆弱性を攻撃することにより、エンジン動作中の CAN 通信の停止や ECU 書換えモード移行に成功したという報告がなされている。同様に Rutgers 大学からはタイヤ監視無線ネットワークの脆弱性が、Zurich 大学からは無線電波信号の遠隔操作に関する脆弱性が指摘されている。いずれも上述の新たな脅威の原因となるセキュリティ問題であり、現代社会における重大なリスク要因である。

このように海外において組込みのセキュリティに関する研究が進んでおり、最先端な組込みセ

キュリティの意見を求めると同時にソフトウェアのセキュリティ規格である IEC62443 の認証取得をするために、国際認証期間である TUV SUD にセキュリティコンセプトフェーズのレポートを入手し、本研究で開発するセキュリティコンセプトが妥当であることを確認して、研究成果であるセキュリティ基盤ソフトウェアを開発する。

5−1　セキュリティコンセプトの認証機関レビュー

【目標】

セキュリティの規格では、設計初期段階でセキュリティ性を如何に確保するかのセキュリティコンセプトが定まっていることが要求されている。そのため、国際認証機関から認証を取得するためには、認証機関によるコンセプトのレビューレポートが必要となる。

本研究では、認証を取得するだけの費用の捻出が難しいことと、研究予算を認証費用として支出できないことから、認証取得は研究終了後の事業化にて検討する。

本研究では、コンセプトフェーズのコンセプトレポートを取得し、かつ、開発成果の監査レビューを取得する。

【研究成果】

国際認証機関 TUV SUD と技術ミーティングを実施し、本年度検討したコンセプトドキュメントについて意見やアドバイスを頂いた。それぞれの検討項目に対策を施し、検討したこと対して指摘をもらうことができコンセプトレポートを発行してもらうための意見やアドバイスをもらうことできた。

【課題】

なし。

最終章　全体総括

3 年間の成果を以下に記載する。

【平成 24 年度成果】

【成果 1】

Liu 手法によるセキュリティ分析手法を確立させ、国際認証機関 TUV SUD よりセキュリティ分析手法及びセキュリティ分析結果については検討したことが妥当であり、問題がないことを確

認した。

【成果 2】

セキュリティ分析結果から出た脅威への対策を検討し、基盤ソフトウェアの要件として定義を行い、セキュリティの基板ソフトウェアの仕様を決定した。

【平成 25年度成果】

【成果3】

Security OS のコンセプトドキュメントである、セキュリティコンセプトを作成した。また IEC62443 に準拠する、ドキュメントも作成し、国際認証機関 TUV SUD より我々が作成したセキュリティコンセプト及び、各種ドキュメントについてレポートを頂くことができた。

【成果4】

基盤ソフトウェアの仕様を決めていく上で EVITA プロジェクトを調査し、本プロジェクトで目指している、セキュリティ基盤ソフトウェアの仕様を明確にすることができた。また、その仕様を、国際認証機関である TUV SUD にレビューしてもらい、セキュリティ基盤ソフトウェアの仕様が妥当であり、問題がないことを確認することができた。

【平成 26年度成果】

【成果5】

基盤ソフトウェアが利用される想定システムを定義し、想定システムのセキュリティ分析を完成させ、国際認証機関である TUV SUD にレビューしてもらい、コンセプトレポート取得レベルにすることができた。

【成果6】

基盤ソフトウェアの仕様開発の研究成果を活用して、セキュリティ対策ライブラリの開発とセキュリティ基盤ソフトウェアの開発に成功した。