システムズエンジニアリングを活用したITSのセキュリティ機能設計の取り組み

三菱重工業株式会社 ICTソリューション本部 制御技術部 ソフトウェア設計課 原 健太

近年の技術進歩に伴い増加するセキュリティリスクに対応するため、三菱重工機械システム株式会社ではシステムズエンジニアリングの考え方を活用し、システム開発のプロセス面からセキュリティ機能向上とその設計根拠の明確化に取り組んでいる。その一部を紹介し、おのおのの取り組み効果について述べる。

1 概要

MHI-MS（三菱重工機械システム株式会社）は、国内外の高速道路などの有料道路料金収受システム及びITS（高度道路情報システム）において、その黎明期から携わる長い歴史を持つ。この事業は、道路利用者から徴収する料金や、各種センサから収集する位置情報や画像を含んだ個人情報などを扱うといった性質上、セキュリティ機能に対する要求が非常に高い。

従来、料金収受システムは、クローズド環境というセキュリティ性の高いシステムであった。その一方で、近年は様々な業界で技術のオープン化・汎用製品の利用・クラウドサービスの利用などが進んでいる。これらは高度な技術を安価かつ容易に導入できるという利点があるが、使い方によってはセキュリティ性が低下する可能性がある。このような動向を踏まえて当社のITS事業においても、これまで以上にセキュリティ対策に注力した取り組みが必要となる。

ただし、一口にセキュリティと言っても「どの程度まで対策すれば十分なのか」を明らかにすることは難しい。あらゆるリスクを考慮すると必要なセキュリティ対策には際限がないが、すべてを実施することは不可能である。将来的に変わる可能性のある要素を考慮しながら、予算や期間を含めた限りあるリソースの範囲内で実現可能であり、ビジネスにとって適切な対策範囲を明確にしてステークホルダへと提示・実現することが求められる。

我々は、システムの特性に合わせた、かつ妥当性の高いセキュリティ対策の実現に向けた取り組みの一つとして、システムズエンジニアリングの考え方を取り入れた検討活動を実施している。前述した近年の技術動向を踏まえ、あらためてITSのセキュリティ対策を見直すにあたり、システムの立ち上げに至る企画段階からライフサイクル全体を通した観点で検討・開発を進めるシステムズエンジニアリングの考え方が有用であると考えたためである。

本記事では、プロトタイプシステムの開発を通してビジネスレベルの目的展開やプロジェクト分析といった超上流工程での活動、及びその結果を基に実施したセキュリティ要件定義と、開発の各工程で実施する妥当性確認と課題管理といった活動を実施した例を紹介し、各取り組みの目的や効果について解説する。

2 取り組み対象・項目

2.1 取り組み対象

ITSのモデルの一つとして、主に野外などに設置した各種センサ・機器と車両が無線通信するなどして課金や違反取り締まりを行う「路側システム」と、その路側システムや様々な機器とネットワーク経由で通信して情報を収集し、総合的な管理を行う「上位系システム」の構成がある。

本記事では、路側システムからネットワーク経由で情報を収集・管理してサービスを提供する上位系システムのプロトタイプ開発とセキュリティ機能検討を対象として紹介する。

2.2 取り組み項目

本記事では、超上流工程における検討項目として実施した「プロジェクト要素分析」、セキュリティ機能の検討結果を記録した「セキュリティ要件定義」、各開発工程で実施した「妥当性確認」と「課題管理」について紹介する。

プロジェクト要素分析は、設計プロセスと言うよりは経営としての企画・営業活動の段階という印象が強いが、設計プロセスの最上流工程であるということを意識して実施することによる効果について述べる。

セキュリティ要件定義は、システムのセキュリティ方針を定義する重要な工程である。プロジェクト要素分析の結果を加味し、ステークホルダにとってリーズナブルな提案を実現するための検討手法について述べる。

妥当性確認と課題管理は、全工程を通して実施する活動である。定義した開発範囲と目的に基づいた開発活動推進の監視や、次回以降の開発サイクルに向けた申し送り事項の管理について述べる。

なお、従来の開発においてもこれらと同等の作業は実施していたが、企画段階での検討結果を設計情報として捉え、かつシステム開発プロセス全体で参照し設計内容に反映する取り組みは、経験あるエンジニアの知見に依存した作業になっていることが多かっ

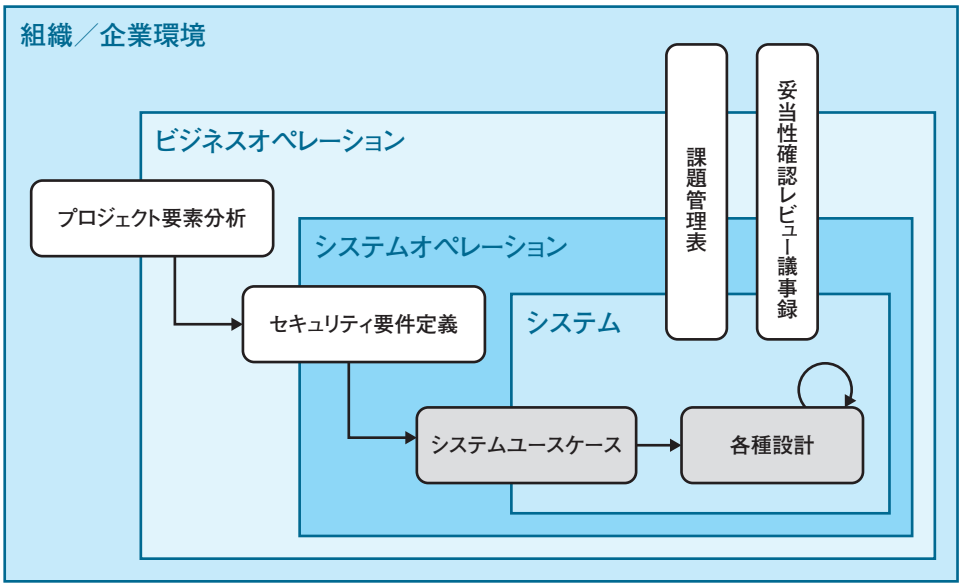

図1　プロトタイプシステム開発における各種活動

た。システムズエンジニアリングの考え方を取り入れることで、これらを誰もが設計プロセスとして明確に意識してシステム開発に取り組むことができる。

3 取り組み内容

3.1 プロジェクト要素分析

本取り組みの目的は、具体的なシステム要件検討を開始する前に、そのシステムによって解決するビジネスの課題を明らかにすることである。

前述の通り、企画・営業活動としてこれまで実施している作業であるが、設計開発部門がその内容を設計プロセスの一部として捉え、意識することで、本来の要求に即した設計を進めていく上での指針となる。

プロトタイプシステム開発に先立ち、ビジネス上の課題や、それに紐付くシステム開発の上位要求を分析し、プロジェクトそのものに求められる要件を整理した上で、プロトタイプシステム開発方針や範囲の整理をするために要素分析シートを作成した。表1に、分析内容の抜粋を示す。

導入の効果としては、開発プロジェクトに求められる要件の深掘りを実施でき、かつ設計活動の一環として取り組むことにより、その内容を設計メンバが十分に理解できるところにある。なお、本プロトタイプシステム開発では、この作業を設計メンバのみで行ったが、企画・営業・設計などを含む複数部門で実施することで、より適切な分析結果を得ることができると考える。

また、幾つかのステップを踏んで最終的に到達したいビジネスレベルの目標と、そのための最初のステップとしてまず取り組む範囲や、次回以降のステップで取り組む範囲などを明らかにすることもできる。セキュリティ機能を検討する場合は、最終的に目指すセキュリティレベルや、そこに到達するまでの段階的な開発活動と個々の達成目標などを明確にしておけば、システムが提供するセキュリティ機能の範囲に関する妥当性を主張する根拠にもなる。

3.2 セキュリティ要件定義

このプロセスではセキュリティ要件定義書を作成した。これは、開発活動の対象となるシステムに対するリスク抽出・分析・対策それぞれの検討方針、及びNIST SP800-53／82やIEC62443-3-3といった制御システムセキュリティに関する国際規格の分析内容を踏まえたリスク対策検討結果について記載したものである。

この文書では、プロジェクト要素分析で明確化したビジネスレベルの目的と、本プロトタイピングの目的を考慮して具体的な要求事項を抽出し、ニーズとの関連性が分かるようまとめている。

セキュリティ要件定義書の作成は、開発活動に対するビジネスレベルの要求の具体化につながり、結果として以降の設計作業の指針とすることができる。

図2に検討の手順を示す。リスク抽出として、システムの情報資産及びリスク発生ポイントを特定し、その組み合わせから考えられるリスクの洗い出しを行った。次に、リスク分析として、抽出したリスクの被害規模と攻撃容易性の数値化に際し、前述の「要素分析シート」で検討した内容に従ってSQuaRE品質モデルで定義される各品質特性との関連についても評価した。

上記の考え方に基づいてセキュリティ要件定義書を作成することの効果は以下の通りである。

- 上位概念であるビジネスレベルの目的を確実に反映して、かつ要素分析時に定義した範囲のセキュリティ機能に関する要件定

表1　要件分析シート

ビジネスレベルの課題	具体的な機能と比べて設計根拠が希薄であったセキュリティについて、ITSとして必要な機能を向上させたシステム構築を進めたい。
原因	• 従来は「固定された」「閉じた」環境の中にシステムを構築するという前提があり、オープンな情報システムと比較してセキュリティリスクが低かった。ただし、近年急速に進む技術のオープン化やクラウド利用に伴い、ITS事業もこれまで以上に高いセキュリティレベルが求められるようになる。 • セキュリティリスクは技術の発展と共に常に形を変え、それに合わせてセキュリティ対策も常に変化し続けることが必要な状況の中で、システムにとって必要なセキュリティ機能の根拠を明確にしてステークホルダへ提供することが難しい。
対策	• これまでは経験を積んだ技術者が独自に実施していたセキュリティ機能に対する設計範囲・根拠の明確化プロセスを設計活動として明示的に取り入れる。 • 既存の設計プロセスを定めたセキュリティ標準や設計標準と照らし合わせ、今後ITSとして必要になるセキュリティ機能を満たすシステム設計／開発手法の確立を目指す。 • 同様の手法を今後のITS開発に展開し、課題解決につなげる。
対策を決定・実施するための手段	• ITSのプロトタイプ開発を通し、検討範囲を限定して実施する。 • セキュリティ機能については、SQuaRE品質（＊1）のうち検討対象範囲に影響すると考えられる「機密性」「完全性」「真正性」「責任追跡性」「否認防止性」の観点から分析し、必要となる機能検討を進める。

＊1：Systems and software Quality Requirements and Evaluation；システム及びソフトウェア製品の品質要求及び評価に関する国際規格ISO/IEC 25000シリーズ、国内規格JIS X 25000シリーズの総称。

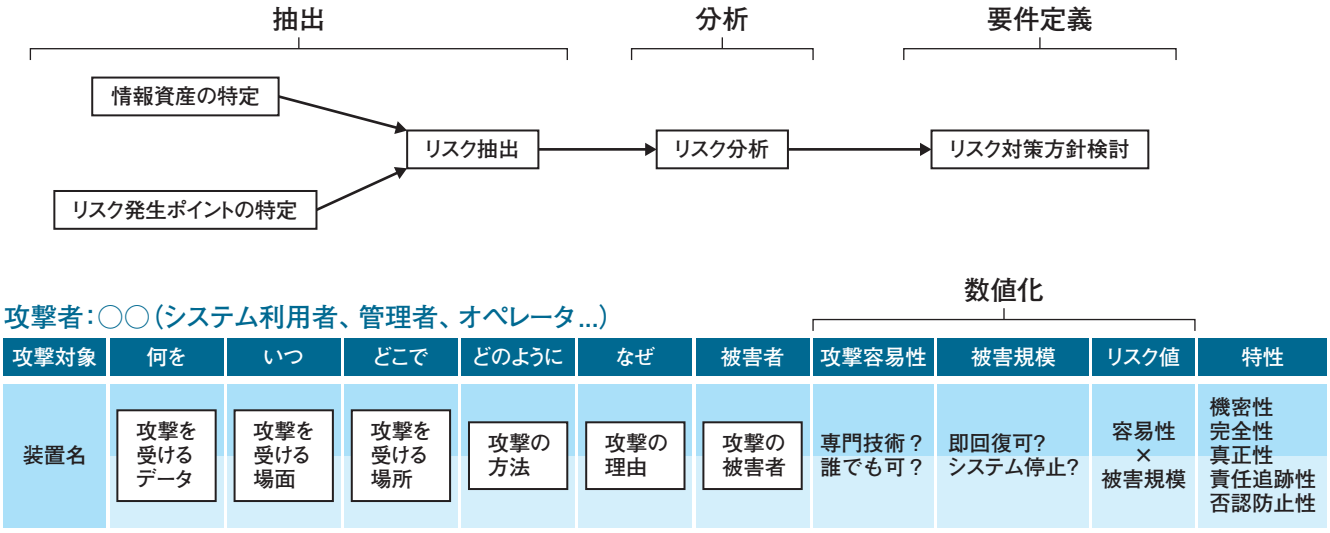

図2　セキュリティ要件定義書作成手順

義を行うことで、開発活動で必要とするセキュリティ機能の要件を漏れなく検討することができる。

● 検討結果は設計の妥当性を示すエビデンスとして利用することができる。

3.3　妥当性確認と課題管理

このプロセスは、開発活動全体を通して実施する取り組みである。超上流工程において、ビジネスレベルの背景とで達成すべき「セキュリティ機能の向上」と今回の開発活動で実現すべき範囲を明確化し、その内容について具体的なシステムとして定義したセキュリティ要件の設計・実装・テストの各設計プロセスで実施するレビューにおいて、「本来の目的に対する達成度」「次回以降の開発まで保留すること」を確実に管理するための取り組みを実施した。

① 妥当性確認

設計プロセスで実施するレビューにおいて、上位図書の内容が確実に反映されていることを確認する（検証）だけでなく、超上流

工程で検討した今回の開発活動で達成すべき範囲とその内容、セキュリティ要件定義書で明確化した具体的なシステム要件からの乖離がないかを確認する（妥当性確認）という観点を強く意識した。

長いライフサイクルを持つシステムの場合、システムの複雑化や、機能追加・改善により開発プロセスが何度も繰り返されるが、軽微な機能追加や修正が前工程との間では整合性が取れていたとしても、本来そのシステムを導入することでステークホルダが実現したい目的の達成や、そのシステムで提供すべき機能の範囲から乖離してしまうことがあり得る。開発プロセスの最後に実施するシステムテストや、客先への導入後にその乖離による問題が発生する前に、各設計プロセスで常に上流で定義した要件に対して確実に妥当性確認を実施することで、本来の目的に即した開発活動を進めることができ、その証拠とすることもできる。

プロトタイプ開発においては、本来の目的と乖離していないかどうかをチェックする妥当性確認の観点からレビューを実施する意識付けのため、上位図書の内容を漏れなく反映しているかをチェックする検証とレビューシートを分けて妥当性確認を行った。

これにより、例えば「セキュリティ監査目的として、システムオペレータの操作履歴を取得する」というセキュリティ要件に紐付く機能の設計書に対して妥当性確認を行う場合、記録する内容は十分か、記録しない場合はどのような理由があるのか、記録した結果をどのように保存してどう活用するのか、といった内容を関係者間で調整し、考えを共有することができた。

抽象的な要件に対する機能は人によって考えに違いが生まれるため、都度本来の要件や目的と照らし合わせて妥当性確認を行うことは、セキュリティ検討の面から見ても設計根拠やシステムに適切なセキュリティ機能の提供に有力な手段であると考えている。

② 課題管理表

妥当性確認により見つかった本来目的との乖離が課題として残った場合や、プロトタイプシステムの開発時は実現する機能を制限し、次回以降の開発で追加する機能など、開発活動全体としての課題を整理するための課題管理表を運用した。

課題管理表には、課題の内容と原因、対策方針、暫定対策の実施内容、次回以降の開発に向けた申し送り事項などを記載する。プロジェクト全体を通しての課題を一覧として管理し、引き継いでいくことで、現時点の暫定対策を次回の開発で修正し、機能を追加することでプロジェクトとしての本来目的を達成することができる。

本プロトタイプシステムの開発においては、製品化時点では必要だが、プロトタイプ時点では運用でカバーできるような機能など、セキュリティ要件定義書の内容から一部簡略化して設計・実装したセキュリティ関連機能の内容（具体的機能、簡略化方針、その妥当性など）と、次回以降の開発に向けた申し送り事項などを記録した。これにより、プロトタイプシステムが提供する機能の妥当性を示す資料になると共に、次回の改修で追加設計や実装が必要な範囲を漏れなく引き継ぐことができた。

4 取り組みの成果

今回は、プロトタイプシステム構築を通したITSに必要なセキュリティ機能検討の活動例として、超上流工程でのプロジェクト分析・その結果を踏まえたセキュリティ要件定義・全工程で継続的に実施した妥当性確認と課題管理について紹介した。個々の取り組みに対する導入効果は３節で述べた通りだが、開発活動全体を通して実現できることは、下記の内容を全て明文化することでシステムの目的を意識しつつ、関係者間で考えを共有しながら開発を進められるところにあると考える。

- ビジネスレベルで最終的に目指す目的
- そのために現段階で必要なシステムとその機能範囲
- 各工程のアウトプットと現段階で必要な機能との対応
- 最終的に目指す目的に対する残課題と対策方針

セキュリティ機能の検討にシステムズエンジニアリングを活用したプロセスを適用することで、冒頭で述べた「“セキュリティ”という将来的に変わる可能性のある要素を考慮しながら、予算や期間を含めた限りあるリソースの範囲内で実現可能であり、ビジネス・システムにとって必要な対策範囲とその設計根拠を明確にしてステークホルダへと提示・実現する」という課題の改善につながっている。

今後は、今回のプロトタイプ開発で抽出した課題の解決を製品化時に実施すると共に、更に幅広い案件に対してセキュリティ機能設計を含む各種開発に、システムズエンジニアリングの考え方を導入した仕組みを検討していく。

No.	状況	課題記述文書	課題	原因	対策案	現時点の方針	対応済み文書	申し送り事項
	クローズ 対策検討中 文書反映中 …	課題提起した文書	課題内容	課題の根本的な原因	課題に対する最終的な対策	対策案に従い現時点の開発で実施する内容	現時点の対応内容を明記した設計書	次回以降の開発に向けた申し送り事項

図３　課題管理表の作成