安全性要求獲得方法の提案と評価

2012SE101　河合 亜実　2012SE145　松原 百映
指導教員：青山 幹雄

1　研究背景

近年，自動車の安全性への注目が高まっており，今後も自動車社会が発展していく状況においては，自動車が交通事故を起こさないという安全性を満たすことが求められている．

2　研究課題

交通事故を減らすには安全性を満たすことが求められている．本研究では，自動車の安全性を脅かすリスクの緩和に必要な要求を安全性要求と定義し，その獲得方法を提案する．

3　関連研究

(1)　ミスユースケース分析

ミスユースケース図とは，ユースケース図の拡張である．脅威を与えるネガティブな要素を追加し，脅威と緩和の関係を明確化する [1].

(2)　セキュリティパターン

セキュリティパターンは，特定の状況に関した問題に対する解決法をパターン化したものである．パターンには，名前などの他に，状況，問題，解法，解法の構造や振舞い，結果などが含まれる [2].

(3)　ETA(Event Tree Analysis)

システムの故障を初期事象とし，対策やその成否を分析し，到達する事象の生起確率を各事象の生起確率の積として表す[3].

4　アプローチ

自動車の安全性要求において，安全性の脅威は外部だけでなく内部にも存在し，自動車に関する全てのアクタはミスアクタになり得るという特徴を持つ．

本研究では，自動車に搭載されているシステムやソフトウェアが故障したことが原因で起こる交通事故を対象として，自動車の安全性要求獲得方法を提案する．

5　提案方法

本研究における安全性要求獲得方法を，提案プロセスとして図 1 に示す．

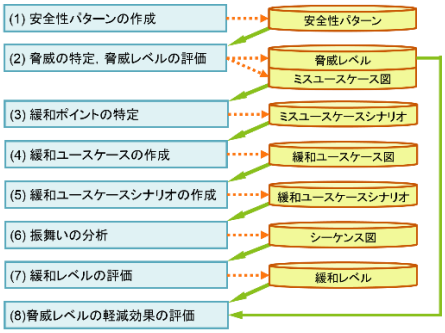

図 1　提案プロセス

5.1　安全性要求メタモデル

安全性要求のメタモデルを図 2 に示す．

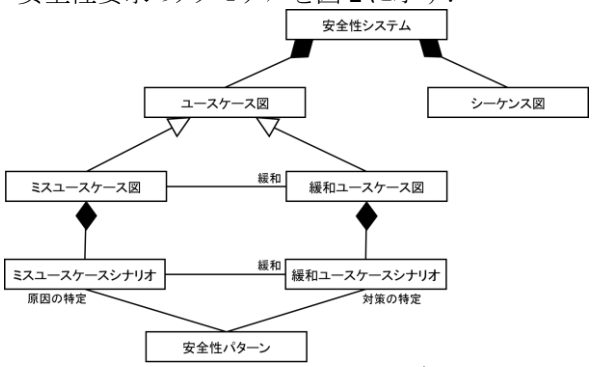

図 2　安全性要求メタモデル

5.2　詳細プロセス

(1)　安全性パターンの作成

要求獲得を行うシステムに対して，安全性パターンを作成する．

(2)　脅威の特定，脅威レベルの評価

システムについてミスユースケース分析を行い，システムに対する脅威を特定する．ここで，安全性のミスユースケース分析では，同じ名前でアクタとミスアクタが存在するという特徴がある．そのことをマルチアクタと呼ぶ．また，特定された脅威によって引き起こされる交通事故について，脅威緩和前の交通事故発生確率を脅威レベルとして，ETA を用いて算出する．

(3)　緩和ポイントの特定

ミスユースケースシナリオを記述する．脅威に対する緩和ポイントを特定して，緩和策のユースケースを追加する．

(4)　緩和ユースケースの作成

緩和策を追加したミスユースケースのことを緩和ユースケースと呼ぶ．

(5)　緩和ユースケースシナリオの作成

緩和ユースケースをもとに，緩和ユースケースシナリオを作成する．ここでは，緩和ポイントや安全性パターンを用いることに注意する．

(6)　振舞いの分析

緩和ユースケースシナリオから，システムの振る舞いの順序や時系列を，シーケンス図を用いて分析する．このとき，マルチアクタや，ユースケース，ミスユースケースを一目見てわかるように，ミスユースケースの場合は活性区間を黒塗りにし，マルチアクタはアクタの周りを太い黒枠で囲って表現する．

(7)　緩和レベルの評価

脅威緩和後の交通事故発生確率を緩和レベルとし，脅威レベルと同様に ETA を用いて評価する．

(8)　脅威レベルの軽減効果の評価

(2)で評価した脅威レベルと(7)で評価した緩和レベルを比較し，安全性が向上しているかどうかを評価する．ここで，「安全性が向上している」とは，脅威レベルより緩和レベルが低下している状態とする．

6　例題への適用

6.1　概要

実際の自動車の制御システムの仕様に本提案を適用し，妥当性を確認する．プリクラッシュセーフティシステムを対象とする．2004 年モデル[4]，2009 年モデル[5]のミリ波レーダセンサが故障した場合に，カメラセンサを追加した 2009 年モデルで安全性が向上したことを比較，検証する．

6.2　適用

(1)　安全性パターンの作成

プリクラッシュセーフティシステムについて，安全性パターンを作成した．

＜安全性パターン 1＞	
名前	ブレーキが作動しない
原因	運転手の前方不注意
問題	運転手がわき見や居眠りをした際，障害物に気が付かず，適切にブレーキを作動させないため，障害物と衝突する恐れがある．
対策	ミリ波警報器により，運転手に警告をする．
結果	警報器が作動し，運転手の注意を促すため，障害物を発見し，適切なブレーキの作動が行える．よって障害物との衝突を回避できるようになる．

＜安全性パターン 2＞	
名前	プリクラッシュセーフティコンピュータが作動要求を送信しない
原因	ミリ波レーダセンサの故障
問題	(1)　ミリ波レーダセンサによる前方の障害物の検知ができず，プリクラッシュセーフティコンピュータが障害物との衝突回避の可否を判断できなくなり，衝突を避けられない恐れがある． (2)　ミリ波レーダセンサによる前方の障害物の検知ができず，警報器が作動しない．これにより，運転手は前方の障害物に気づかないまま走行を続け，衝突する恐れがある．
対策	ミリ波レーダセンサとは別に，カメラセンサを設置する．また，カメラセンサからの情報を解析して障害物についての情報を得られるコンピュータを設置する．
結果	カメラセンサで車両前方の風景をデジタル映像として取り込み，その映像データをコンピュータで解析することで，障害物を検知するだけでなく，車両から障害物までの距離や，障害物の高さや幅といった具体的な情報を得ることができ，障害物との衝突を回避できるようになる．

(2)　脅威の特定，脅威レベルの評価

2004 年のプリクラッシュセーフティシステムのミスユースケース図を作成し，脅威を明確にした(図 3)．また，脅威緩和前の交通事故発生確率を脅威レベルとして，ETA を用いて算出した．脅威レベルは，初期事象の発生確率をλ_0，対策 i の失敗確率をλ_iとして，交通事故発生確率の積となる(図 4)．

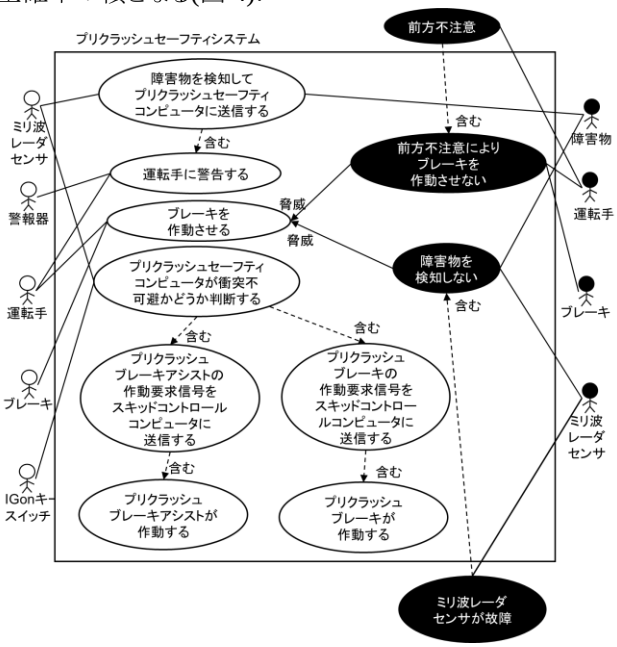

図 3　2004 年モデルのミスユースケース図

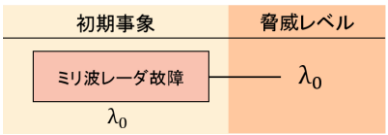

図 4　2004 年モデルの脅威レベル

(3)　緩和ポイントの特定

ミスユースケースシナリオを記述し，シナリオの基本パスに安全性パターンを対応させて，緩和ポイントを特定した．

＜ミスユースケースシナリオ 1＞	
(1)　ミスユースケース名	前方不注意によりブレーキが作動しない
(2)　アクタ／ミスアクタ	運転手が前方の障害物に気づかず，障害物と衝突する
(3)　概要	運転手，ブレーキ
(4)　トリガ	前方不注意
(5)　事前条件	運転手はブレーキを作動させていない
(6)　基本パス	1)　運転手は，前方の障害物に気づかず，自動車の走行を続ける 2)　運転手は，ブレーキを作動させず，ブレーキが作動しない
(7)　結果	自動車と障害物が衝突する
(8)　ステークホルダリスク	運転手のリスク　⇒　軽傷
(9)　ミスアクタプロフィール	1)　運転手に悪意はない 2)　ブレーキは正常に機能している
(10)　緩和ポイント	ブレーキが作動しない

＜ミスユースケースシナリオ 2＞	
(1) ミスユースケース名	障害物を検知しない
(2) アクタ／ミスアクタ	障害物，ミリ波レーダセンサ
(3) 概要	ミリ波レーダセンサが故障したことにより，前方の障害物を検知できず，障害物と衝突する
(4) トリガ	ミリ波レーダセンサの故障
(5) 事前条件	ミリ波レーダセンサが故障している
(6) 基本パス	1) ミリ波レーダセンサの故障により，プリクラッシュセーフティコンピュータは，前方の障害物の検知情報を取得しない 2) プリクラッシュセーフティコンピュータは，スキッドコントロールコンピュータに作動要求を送信しない
(7) 結果	運転手は，前方の障害物に気づかない
(8) ステークホルダリスク	運転手のリスク ⇒ 障害物と衝突
(9) ミスアクタプロフィール	1) 障害物は，移動できる物でも移動できない物でもあり得る 2) ミリ波レーダセンサは機能していない
(10) 緩和ポイント	ミリ波レーダセンサの故障

(4) 緩和ユースケースの作成

ミスユースケース図とミスユースケースシナリオをもとに，脅威を緩和するユースケース図を作成する(図 5).

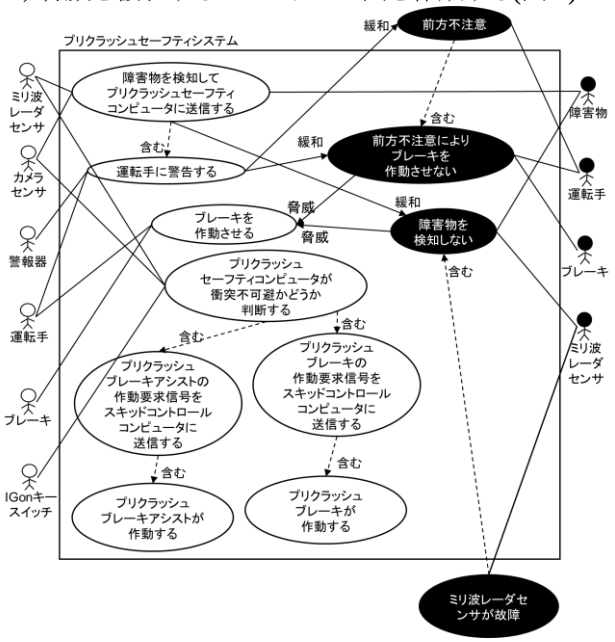

図 5 2009 年モデルの緩和ユースケース図

(5) 緩和ユースケースシナリオの作成

緩和ユースケースのシナリオを記述した.

＜緩和ユースケースシナリオ 1＞	
(1) 緩和ユースケース名	運転手に警告する
(2) アクタ	警報器，運転手
(3) 概要	警報器は，プリクラッシュセーフティコンピュータから警告要求を受信し，警報器を作動させる
(4) 事前条件	プリクラッシュコンピュータから警告要求を受信している
(5) 基本パス	警報器を作動する
(6) 結果	警報器の作動により，運転手は注意喚起を促され，前方の障害物に気づく

＜緩和ユースケースシナリオ 2＞	
(1) 緩和ユースケース名	障害物を検知してプリクラッシュセーフティコンピュータに送信する
(2) アクタ	カメラセンサ，障害物
(3) 概要	ミリ波レーダセンサとは別にカメラセンサを設置したことで，ミリ波レーダセンサが故障しても，前方の障害物を検知できるようになる
(4) 事前条件	カメラセンサが正常に機能している
(5) 基本パス	1) カメラセンサからの車両前方の映像データの解析情報をもとに，前方の障害物を検知する 2) 障害物の検知情報をプリクラッシュセーフティコンピュータに送信する
(6) 結果	プリクラッシュセーフティコンピュータは，警報器に警告要求を送信する

(6) 振舞いの分析

緩和ユースケース図とシナリオをもとに，脅威緩和済のプリクラッシュセーフティシステムの振舞いをシーケンス図で示し，振舞いの順序や対策の場合分けを明確にした(図 6).

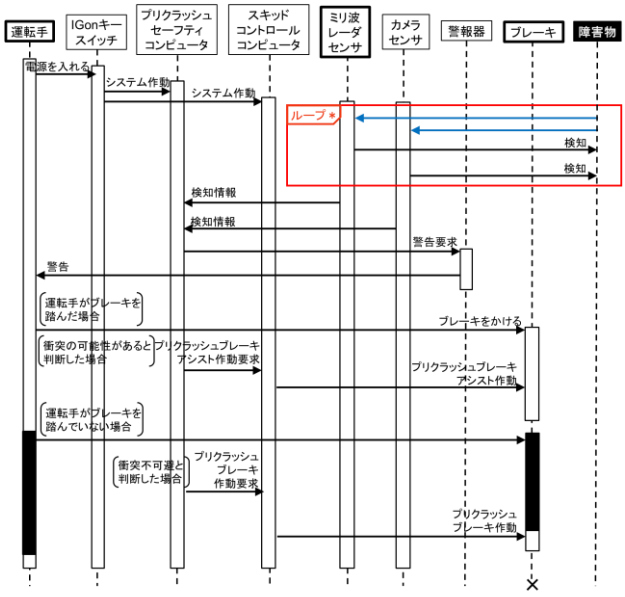

図 6 2009 年モデルのシーケンス図

(7) 緩和レベルの評価

脅威緩和後の交通事故発生確率を緩和レベルとし，脅威レベルと同様にETAで評価した(図 7).

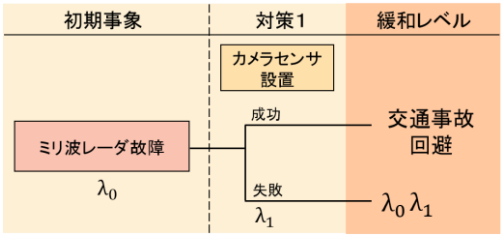

図 7 2009 年モデルの緩和レベル

(8) 脅威レベルの軽減効果の評価

脅威レベルと緩和レベルを比較すると，次の式(1)が得られる.

$$\lambda_0 > \lambda_0\lambda_1 (0<\lambda_0<1,\ 0<\lambda_1<1) \qquad (1)$$

式(1)より，脅威レベルより緩和レベルが低下したため，2009 年モデルでは，安全性が向上していることが分かった.

7 評価

本提案方法では，ミスユースケース分析を行う際に，セキュリティパターンを応用した安全性パターンを対応させることで，ミスユースケースシナリオから，脅威に対する緩和ポイントと緩和策を明確にすることが可能になった. また，全ての振舞いの時系列を分析することで，脅威ごとに緩和策の有効性を定量的に分析可能になった.

(1) 安全性パターンの有効性

セキュリティパターンを応用して安全性パターンを定義することで，システムやソフトウェアの故障の原因と対策をパターン化できる. これにより，脅威の原因を明確にすることで，適切な対策を体系的に特定できるようになった.

(2) マルチアクタの有効性

安全性に関する全てのアクタがミスアクタになり得るという特徴を，マルチアクタとして表現可能とした. マルチアクタを導入したことにより，ミスユースケース図やシーケンス図から，マルチアクタがどのような条件で脅威になるかを評価できるようになった.

(3) 安全性の定量的な評価の有効性

ETA を用いることで，脅威レベルや緩和レベルのように，安全性を定量的に表現可能になった. また，脅威レベルと緩和レベルを評価，比較することで，安全性の向上を体系的に，かつ定量的に評価可能とした.

8 考察

(1) ミスユースケース分析の拡張の有効性

1) 従来のミスユースケース分析との比較

従来のミスユースケース分析にマルチアクタを導入することで，システムに対する脅威について，外部要因による脅威だけでなく，内部要因による脅威も明確にすることが可能になった. これにより，自動車の安全性の特徴に対応したミスユースケース分析を行うことが可能になった.

2) セキュリティへの応用

セキュリティにおける従来のミスユースケース分析では，外部要因による脅威が分析されていたが，本提案方法を応用すると，システムのユーザなどによる情報漏洩などの，内部要因によるシステムのセキュリティ要求獲得が可能になる.

(2) ETA の適用

従来のミスユースケース分析では機能の分析を行うため，定性的な要求獲得であったが，ETA を適用することで，脅威緩和後の安全性の向上を定量的に評価可能になった. このように，従来のミスユースケース分析に ETA を組み合わせることで，定性的であった安全性要求に加え，定量的な安全性要求も獲得可能となった.

9 今後の課題

(1) システムの対策の優先順位の決定

実際のシステムの故障時における安全性を考慮した際には，対策の実行順序に加えて，対策の優先順位が重要になる. 安全性を満たすシステムの設計では，対策の実行順序だけでなく，優先順位を考慮した設計が求められる.

(2) 要求獲得の範囲の拡大

本研究はシステムやソフトウェアの故障が原因となる交通事故を対象としたが，実際には，システムやソフトウェア以外にも原因となり得るため，ステークホルダによる要因や環境要因も対象に含める要求獲得方法の実現が求められる.

10 まとめ

本研究では，自動車の安全性を脅かすリスクの緩和に必要な要求を安全性要求と定義し，自動車に搭載されているシステムやソフトウェアが故障したことが原因で起こる交通事故を対象として，自動車の安全性要求獲得方法を提案した. 本提案方法をプリクラッシュセーフティシステムに適用して，安全性が向上していることを定量的に評価した. 本提案方法により，自動車の安全性を満たすシステムやソフトウェアの設計や開発が期待できる.

参考文献

[1] I. Alexander, Misuse Cases, IEEE Software, Vol. 20, No. 1, pp. 58-66.

[2] 吉岡 信和 他，セキュリティソフトウェア工学の研究動向，コンピュータソフトウェア，Vol. 28，No. 3，2011，pp. 43-47.

[3] J. X. Wang, etc.，日本技術士会(訳)，リスク分析工学，丸善，2003, pp. 71-79.

[4] TOYOTA CROWN MAJESTA 新型車解説書 2004 年 7 月，第 9 章 pp. 45-88.

[5] TOYOTA CROWN MAJESTA 新型車解説書 2009 年 3 月，第 9 章 pp. 28-37.