人工知能学会
第13回知識流通ネットワーク研究会
SIG-KSN-014-01

安全フレームに基づくシステム安全情報共有システムの提案

山本 修一郎

名古屋大学
愛知県名古屋市千種区不老町

A Proposal for Safety Information Sharing System based on the Safety Frame

Shuichiro YAMAMOTO

Nagoya University
Furo-cho, Chikusa-ku, Nagoya Aichi Japan

概要

システムの安全性を組織全体で保障するためには，システム開発運用活動について、適切に安全情報を共有する必要がある．本稿では，システムの安全情報を記録し共有するための安全フレームに基づいて、組織全体で安全情報を共有する方法を提案する．また、安全フレームに基づく安全情報システムの構成と活用プロセスについて述べる。

Abstract

To assure system safety in the organization, it is necessary to share safety information on system development and operation activities appropriately. In this paper, a method is proposed to record and share system safety information based on safety frame. We also explain that the system configuration and use scenarios of the proposed safety information sharing system.

1 はじめに

システムの安全性を保障するためには、安全にソフトウェアを開発するとともに、システムを安全に運用する必要がある．

このためにはシステム開発・運用活動を通じて、システム安全に対するリスクを識別して適切な安全対策を講じる必要がある。この場合、システム開発・運用活動におけるシステム障害事例についての問題票などの報告を再利用する方法が考えられる。

しかし、従来の問題票の記述は、統一されておらず、個別的な問題への対処結果が記述されているだけであり、安全情報を再利用するためには十分ではなかった。

本稿では，安全情報の記述項目を統一的に定義しておき、システム開発・運用過程で登録して再利用する方法を提案する．

以下では，2 節で関連研究について述べる．3 節で安全フレームについて述べ、4 節で安全フレームに基づく安全情報システムを提案する．5 節で提案手法の具体例を説明する．6 節で考察を述べ，最後に 7 節でまとめと今後の課題を明らかにする．

2 関連研究

以下では，安全情報システム[1]と問題フレーム[3]についての研究動向を紹介する．

2.1 安全情報システム

システムの安全情報を収集、分析、流通するために用いられている航空分野における安全情報システムの例として米国の ASRS(Aviation Safety Reporting System)[2]がある。

このような安全情報システムは、ハザードとその対策を文書化し、追跡することにより、組織的な安全プログラムの重要な構成要素となっている。

安全情報システムの留意点としては、すべてのハザードを記録すること、決定の内容と、その理由、問題の優先順位などである。安全情報システムの内容として、システム安全プログラム、安全活動状態、ハザード分析結果、ハザードの追跡情報、ハザード状態、インシデント情報、傾向分析情報、構成管理情報などが管理される。

安全情報システムの用途として、事故の前兆となる傾向と逸脱の検出、安全制御と規格の有効性評価、実際の動作とリスク分析結果との比較、ハザードの識別と制御、事故の警告、未然防止などが挙げられている。

2.2 問題フレーム

問題フレームは問題を識別し構造化するための分析手法である[3]。問題フレームでは、外部要求 R、現実の世界を構成する問題領域の性質 K、ソフトウェア開発の対象となる機械の仕様 S を考える。

R は問題世界の望ましい振る舞いや性質に関する明示的な要求である。K は世界に関する現象についての記述である。S は世界とのインタフェースに関して機械が実現すべき振る舞いや性質についての記述である。S を実現する機械が問題領域 K に対して動作するとき、外部要求 R が成立する必要がある。

このように問題フレームでは、要求を R,K,S の３つの部分に分けて記述することで、ソリューションに関する内部要求と、ソリューションを取り巻く環境としての現実世界の振る舞いや性質に関する外部要求とを明確に区別することができる。

ソフトウェアを開発することは、問題を解くための機械を作成することであり、顧客の要求に合わせないといけない。しかし顧客の要求は外部要求であり、機械に対する要求とは異なることが多い。問題フレームでは外部要求と内部要求としての仕様との関係を記述できるので、顧客と開発者とのソフトウェアに対する認識のギャップを埋める手段として有効である。

3 問題フレームに基づく安全フレーム

以下では，問題フレームをシステムの安全情報分析に適用することにより、システム安全情報を共有するためのフレームワークである「安全フレーム」について述べる.

3.1 システムと安全対策の関係

問題フレームでは、システムと要求が契機となるイベントとシステムによる応答の依存関係に基づいて対応付けられている。たとえば、問題フレームでは、①システムへの環境からのイベントが発生するとき、②「要求」に適合するように、③システムが応答する必要があるというようにして、システムの振舞と要求の関係が記述される。

この問題フレームの記述構造を参考にして、安全要求を記述することを考えると、以下のようになる。

安全フレームでは、①システムへの環境からのイベントが発生するとき、②システムで逸脱事象（ハザード）が発生した場合、③逸脱事象の原因を明らかにして、④適切に対応することにより、⑤「安全要求」に適合するように、⑥システムが応答する必要がある。

この考察から、安全情報を記述するためのメタモデルを図 2 に示すように定義できる。システムの機能要求に対して、環境への逸脱（ハザード）を識別してその原因に対処することで安全要求を満足するように、環境に対して応答する。このメタモデルでは、どのような安全対策にも限界があることから、残余リスクを定義している。また、環境をアクタとしていることを注意しておく。

3.2 安全フレームの表記法

上述した安全フレームのメタモデルに基づいて、表 1 のように、安全フレーム記述表を構成できる．表 1 では、わかりやすくするため、安全情報についての概要を記述できるようにしている。

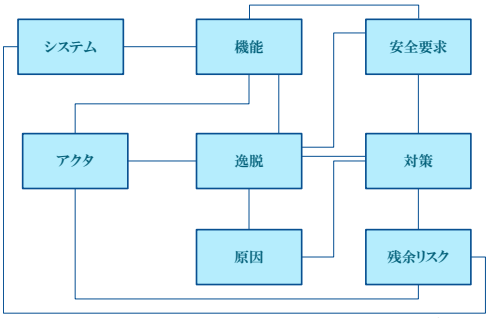

図 1　安全フレームのメタモデル

表 1　安全フレーム記述表の構成例

概要	システム	アクタ
機能要求	ハザード	ハザード原因
安全要求	対策	残余リスク

3.3 安全フレームの作成手順

安全フレームの作成手順は、以下のようになる。

【手順 1】システムの脆弱性分析

まず、システムに、どのような逸脱事象があるかを、脆弱性分析によって明らかにする必要がある。これによって、安全フレームを構成する要素間の関係構造を明らかにすることができる。もし、脆弱性がなければ安全対策の必要がないことになるので、安全フレームを記述する必要もない。

【手順 2】原因の特定

逸脱事象が識別できると、対応する原因を特定する。

【手順 3】安全対策の立案

安全要求に基づいて、逸脱状態を分析することにより、原因となる契機とそれに基づく逸脱状態から、安全対策が完了した安全状態に至るまでの重要な状態と、状態間の遷移としての一連の安全対策活動を明らかにする。

【手順 4】残余リスクの確認

安全対策によってシステムが安全状態に到達する上での制約条件を残余リスクとして明確にする。この理由は、一連の安全対策活動が正常に動作しない可能性があるからである。

【手順 5】安全情報に対する利用状況の作成

安全フレームとして作成した記述内容をシステム開発・運用過程で参考にしたことを記録する。

4 安全情報共有システムの実現方式

以下では、上述した安全フレームを用いた安全情報共有システムの概念と利用シナリオならびに、

SNS を用いた実現方式について説明する.

4.1　システム概念

安全情報システムの概念を図 2 に示す。安全情報システムでは、安全フレームによって安全情報を組織横断的に蓄積して共有することができる。また、安全情報の共有プロセスでは、安全フレームによってシステム開発・運用プロジェクトの安全性を見える化することができる。プロジェクトの安全能力を安全フレームによって分析することができる。さらに安全対策の実施結果を安全フレームと対応付けて管理できる。安全フレームによって明らかにされたシステムの脆弱性対策を教訓として蓄積することによって、安全対策知識を再利用できる。

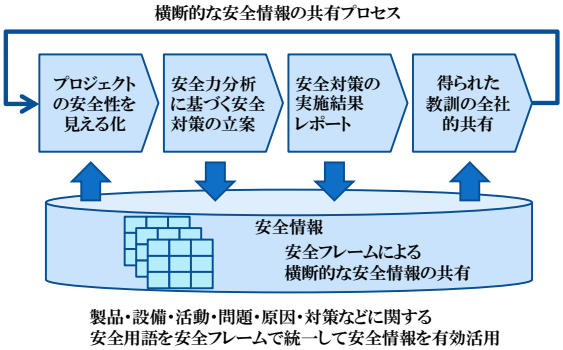

図 2 安全情報システムと情報共有プロセス

4.2　SNS による安全情報システムの実現

安全情報システムの目的は、上述したように、組織内で安全情報を共有することである。したがって、組織内で情報共有を支援する SNS[4]を活用することができる。たとえば、SNS の主な機能を安全情報活動にどのように活用できるかを整理すると、表 2 のようになる。

表 2　SNS の機能による安全情報活動

SNS の主な機能	安全情報共有活動
個人ページ	自己紹介、システム経験、専門知識などを紹介
近況・日記	現状の課題の提起と回答への協力、提案
フォルダ	安全フレームなど安全情報を登録して、共有
友人	情報交換・協働
メッセージ	友人関係の構築・特定の友人とのメッセージ交換
コミュニティ	情報共有範囲の制御、プロジェクトチームの構築
検索	安全情報の全文検索

SNS を用いることで、容易に安全情報システムを構築できる。安全フレームの情報構造については、サーバ上で XML のタグを用いて統一的に管理することができる。

同じコミュニティ構成員間で安全フレームを共有できるようにしておくことで協働編集できる。また公開されている安全フレームを検索することで、対象システムに類似する逸脱事象とその安全対策を再利用できる。

また、安全情報の検索では、安全フレームの記述項目名と、検索したい情報のキーワードを指定することで、指定したキーワードが対象記述項目に出現する安全フレームを検出できる。

このような安全情報検索では、表 2 で示した個人ページ、日記・近況、安全フレームが対象となる。しかし、フォルダ内に格納されたすべての文書を検索対象とすると、処理が複雑化する可能性があるので、安全フレームを格納するフォルダを特別に管理することを考慮する必要がある。

また、安全フレームの作成では、ハザード分析や安全対策技術の専門家による支援が必要になる。この場合、安全問題を相談することが、相談依頼者の不利益にならないように、匿名化を考慮する。また、相談内容を安全技術専門家が一般化することにより、組織内で共有できるような、一般安全フレームを格納できるフォルダが必要である。このような組織内で安全情報の共有を支援するための専門家組織を安全情報委員会として整備することが重要になる。

5 具体例

以下では安全フレームの具体例を説明する。

例 1 ：複製 DB に対する安全フレームの記述項目を列挙すると以下のようになる（表 3)。

[概要]複製 DB の物理故障に対してサービスを継続する
[システム] 複製 DB システム
[アクタ] DB 利用者。逸脱の影響：サービス全断
[機能要求] DB を複製する
[逸脱] 複製 DB 内容が破壊される
[原因] DB サーバ物理故障の手順が不明確
[安全要求] サービスが全断しない
[対策] DB サーバ物理故障対応を手順化する
[残余リスク] 故障対応手順の訓練不足

表 3　複製 DB システムの安全フレームの例

概要	システム	アクタ
複製DBの物理故障に対してサービスを継続	複製DBシステム	DB利用者 影響:サービス全断
機能要求	**ハザード**	**ハザード原因**
DBを複製	複製DB内容の逸脱	DBサーバ物理故障の手順が不明確
安全要求	**対策**	**残余リスク**
サービスが全断しない	DBサーバ物理故障対応の手順化	故障対応手順の訓練不足

例 2：データ登録機能に対する安全フレームの記述項目を列挙すると以下のようになる（表 4)。

[概要] データ項目登録に対してシステムを継続する
[システム] 情報管理システム

[アクタ] 情報登録者。逸脱の影響：情報を登録できない
[機能要求]データ項目を登録する
[逸脱] 入力データの桁数がデータ項目の定義長より大きい
[原因]桁数オーバーのため、情報を登録できない
[安全要求] データ項目を安全に登録できる
[対策] データ項目の桁数だけデータを登録して、あふれた情報を廃棄する
[残余リスク] 必要な情報を廃棄する可能性がある

表 4　データ項目の安全フレームの例

概要	システム	アクタ
データ項目登録に対するシステムの継続	情報管理システム	情報登録者 影響:情報を登録できない
機能要求	ハザード	ハザード原因
データ項目を登録する	入力データ項目の桁数オーバー	桁数オーバーのためシステムが中断
安全要求	対策	残余リスク
データ項目を安全に登録できる	データ項目の桁数だけデータを登録して、あふれた情報を廃棄する	必要な情報を廃棄する可能性がある

6 考察

以下では，上述した安全フレームに基づく安全情報共有システムの有効性について考察する．

6.1　安全フレーム記述表

安全フレーム記述表を用いることにより，安全情報を，多面的な観点から網羅的に共有できる．これによって，安全情報の一貫性のある管理とそれに基づく効率的な共有が実現できる．

安全フレーム記述表により，従来の文書では統一的に整理されていなかった安全情報を系統的に記述し共有できることを明らかにした．

提案した記述表では，ハザードの影響をアクタ項目で記述している。影響の重大性なども含めて安全対策を選択するための記述として、現状の記述項目で充分であるかどうかについては、より多くの例に適用して評価する必要がある。

6.2　安全情報コミュニティ

前節で示したように，本提案によって，自然言語で記述された安全情報に基づいて，安全フレームの記述項目を網羅的に抽出できることから、組織内で安全情報を過不足なく共有できることは明らかである．

本手法では、安全フレームに基づいて系統的に安全情報項目を明確化できるだけでなく，登録した安全情報項目を SNS で共有できる．たとえば、必要な安全情報項目が、どのようなシステムの安全フレームのどこで記述されていたかを検索できる。したがって，選択した安全対策が十分であることを、安全情報システムに蓄積された安全フレームに基づいて客観的に説明できる．

また，自然言語による安全フレームの記述から対話的に安全情報項目を抽出できるだけでなく、必要があれば、対応する安全フレームの作成者と SNS で意見交換できることから、実際のプロジェクトに適応することは容易であると考えられる．したがって，今後，本手法を実際のプロジェクト活動に適用する研究についても進めていく予定である．

6.3 適用範囲

本稿で対象とした安全フレームの構成は一般的であり，本手法が 5 章で示した例だけでなく、他の安全情報の記述にも適用できることは明らかである。

6.4　限界

本稿では，提案手法がシステムの安全情報の共有に対して適用できることを示した。しかし、どのような能力の要員がどれくらいの工数で安全情報を作成・共有できるかなどの生産性や品質に関する有効性については、定量的に評価していない．このため，本手法の有効性について、安全情報システムを試作して定量的な効果を明らかにしていく必要がある．

7 まとめと今後の課題

本稿では，安全フレームに基づく安全情報を共有する手法とシステムについて提案した．安全フレームを記述した事例は 2 件だけであるが，手法としての一般性は高いので、他の事例についても適用できると考えている．

また，本稿の内容は手法の実行可能性を評価するための試行評価の段階にとどまっているため，定量評価までは至っていない．今後，実際のソフトウェア開発・運用工程を対象とする安全情報システムの評価実験を進める予定である．

謝辞

本研究は CREST「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」研究領域（DEOS プロジェクト）の支援を受けたものである[5][6][7].

参考文献

[1] Nancy Leveson, Safeware– System Safety and Computers, Addison-Wesley, 1995, 松原友夫監訳, セーフウェア，翔泳社，2009
[2] ASRS, Aviation Safety Reporting System, http://asrs.arc.nasa.gov/index.html
[3] M. A. Jackson, Problem Frames: Analyzing and Structuring Software Development Problems (Addison-Wesley, 2001)
[4] 山本修一郎、CMCで変わる組織コミュニケーション、企業内SNSの実践から学ぶ、NTT出版、2010
[5] DEOSプロジェクト, http://www.crest-os.jst.go.jp
[6]DEOS プロジェクト，2011 科学技術振興機構 White Paper DEOS-FY2011-WP-03J, *www.dependable-os.net/ja/topics/file/**White_Paper**_V3.0J.pdf*
[7] Mario Tokoro eds., Open Systems Dependability, Dependability Engineering for Ever-Changing Systems, CRC Press, 2012