様式 C-19

科学研究費補助金研究成果報告書

平成２３年 ５月 ２６日現在

機関番号：１２６０８
研究種目：基盤研究（C）
研究期間：２００８ ～ ２０１０
課題番号：２０５００００２７
研究課題名（和文） 法令や規則に適合したソフトウェア要求の獲得技術の研究

研究課題名(英文) Study on the Techniques for Eliciting Software Requirements Compliant with Regulations

研究代表者
佐伯 元司 （SAEKI MOTOSHI）
東京工業大学・大学院情報理工学研究科・教授
研究者番号：８０１６２２５４

研究成果の概要（和文）：本研究では，法令や規則に遵守したビジネスプロセスや情報システムを開発するために，その要求獲得段階において，法令や規則に合致した要求を獲得するようにコンピュータでガイドする手法，完成した要求仕様書が法令や規則を遵守しているかどうかをチェックし，違反している場合はどの箇所が違反の原因となっているかを開発者に提示する手法を開発した．これらの手法に基づいて，開発者を支援するためのコンピュータツールを開発した．

研究成果の概要（英文）：In this research project, in order to develop efficiently business processes and information systems of high quality compliant with regulations, we have developed the technique to guide requirements analysts to elicit requirements compliant with regulations by computer and the technique to find regulatory violations of requirements specifications if any and show them. Furthermore we have developed computerized tools to support requirements analysts based on the above techniques.

交付決定額

（金額単位：円）

	直接経費	間接経費	合 計
２００８年度	1,700,000	510,000	2,210,000
２００９年度	1,000,000	300,000	1,300,000
２０１０年度	700,000	210,000	910,000
年度			
年度			
総 計	3,400,000	1,020,000	4,420,000

研究分野：要求工学
科研費の分科・細目：情報学・ソフトウェア
キーワード：仕様記述・仕様検証，要求獲得，ゴール指向分析法，格フレーム，コモンクライテリア

１．研究開始当初の背景

インターネットを用いてビジネスプロセスを支援する情報システムが普及している．情報システムの悪用を防ぐために，個人情報保護法に代表されるように関連法令や規則が整備され，法令に準拠した情報システムを開発することが必要である．特に，要求獲得段階で法律や規則を遵守していないような要求を獲得してしまうと，開発のやり直しを行わなければならず，開発期間が長期化し，開発コストが多大になってしまう問題がある．また，開発対象も大規模，多様化しており，いかに法令や規則を遵守した要求を早い段階で獲得するかは大きな問題となっている．

２．研究の目的

本研究では，１であげた問題点を解決するために，ビジネスプロセスや情報システムへの

要求獲得段階で法令や規則を遵守するような要求獲得を行う手法，および獲得したビジネスプロセスや情報システムの要求仕様が法令や規則を遵守しているかどうかをチェックする手法，違反している場合はどの箇所が違反の原因となっているかを開発者に提示する手法を開発する．また，これらの手法は，開発対象の複雑さやその要求の多さから，コンピュータでできる限り自動化できるように，支援ツールもあわせて開発する．

３．研究の方法

獲得した要求と法令文の意味処理を行うための意味モデルの開発，要求の法令や規則への適合性判定および不適の場合の修正規則の収集とコンピュータ化，既存のゴール指向要求分析法との融合を行っていった．さらに，ビジネスプロセスや情報システムの振る舞い要求の記述の形式的検査法の開発を行った．個人情報保護法といった比較的小規模の法令を例として用いて基盤技術を開発していき，より幅の広いセキュリティ分野へ適用していった．謝金を用いて研究室の大学院生にツールの開発を行わせ，評価を行いながら，確立した基盤技術の改良を進めていった．

４．研究成果

(1) 法律や規則を表現するための格フレームによる意味表現手法の開発：個人情報保護法を例にとり，その意味表現となる格フレーム化を行った．格フレームに基づく法令文の記述を拡張し，他の法令文への参照，適用順序の規定，例外や適用除外規定などのメタレベルの表現を扱えるようにした．個人情報保護法の記述を行い，手法の有用性の評価を行った．図１にこの手法で開発した法令文のメタモデルを表す．ここでは，１つの法令文は条項(Article)の集合からなっており，条項は階層的に木構造となっていることがある．構造中で最下位レベルの文(Basic Article)は，法が適用される状況(Situation)と，その状況で生じる適用対象者の行為(Act)の義務(Obligation)，禁止(Prohibition)，許可(Permission)，免除(Exemption)の記述からなっている．図２は個人情報保護法の１つの条文とその意味表現である．格フレームは動詞を述語名，格スロットはその述語の引数で表現されている．

(2) 法令文と要求文のマッチングによる適合性判定技術の開発：法令文と要求文を格フレーム表現の上でマッチングを行い，要求文に関連する法令文の抽出を行い，適合性を判定するためのアルゴリズムを開発し，ツールとして実装した．マッチングには，同義語などの処理を行う必要があるため，オントロジや辞書を介して行う手法となっている．

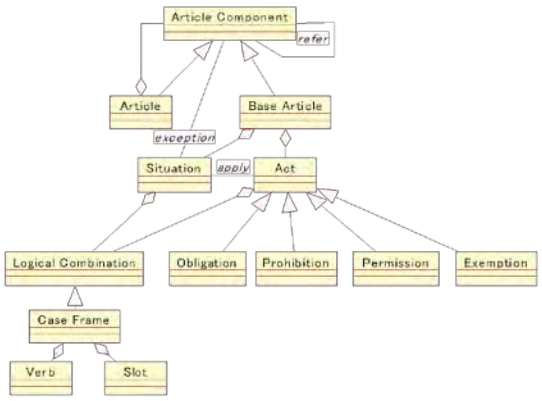

図１　法令文のメタモデル

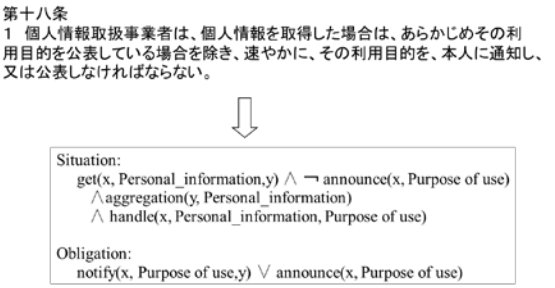

図２　法令文の意味表現

図３に本手法を用いて，要求に個人情報保護法１８条１項が適用された簡単な例を示す．インターネットを用いた電子ショップの例で，電子ショップ側は，利用者を登録する際に個人情報を収集する．その際，個人情報保護法では，集めた個人情報の使用目的を公知するか(announce)，本人に知らせる(notify)しなければならないという義務(Obligation)を規定している．分析者が最初に書いた要求文「... 加入申し込み時に個人情報をもらう」だけでは，この法令に違反している．本手法では，この文の格構造を抽出し，その主動詞「もらう」と同義の動詞の格フレームを持つ法令文を検索する．１８条１項の意味表現の状況部分(Situation)の格フレーム get(x, Personal_information, y)がマッチしたため，分析者は本当にこの法令が適用される状況になっているかどうかをチェックする．例えば，状況部分に含まれている格フレーム¬ announce(x, Purpose of use)（使用目的が告知されていない）が成り立っているかどうかを調べる．その結果，この法令が適用される状況であることが判明し，義務(Obligation)である行為を要求文に追加するという作業を行う．図では，分析者は義務の中から announce(x, Purpose of use)を選択し，マッチングの際に得られた情報を

用いてスロット部分を埋め，要求文の改訂を行っている．結果としては，動作主格スロット x に電子ショップを代入し，「電子ショップは，個人情報の使用目的を告知」という要求が追加される．図４に開発したツールの画面の一部を示す．ツールのマッチングと推論部分は Prolog を用いて実現されている．この図は，図３での作業を支援している．電子ショップの要求文「電子ショップは，加入希望者から，加入申し込み時に，個人情報をもらう」に対し，個人情報保護法１８条ではその使用目的を知らせないといけないと規定しており，知らせる行為が入っていないため，法令に適合していない可能性があることを示唆している．Verb のエリアに要求文と法令文マッチングのための語彙の統一を，case frame のエリアに使用した格フレームが表示されており，guide の部分に，notify か announce 動作を追加する必要があることが格フレーム表現で表示されている．

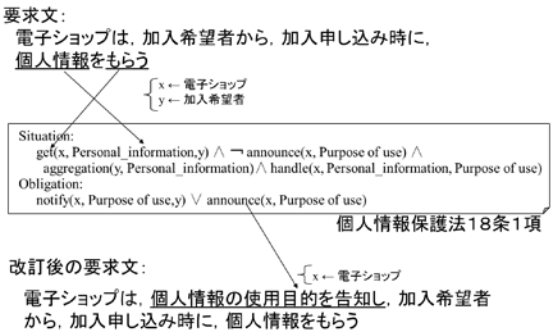

図３　個人情報保護法の例

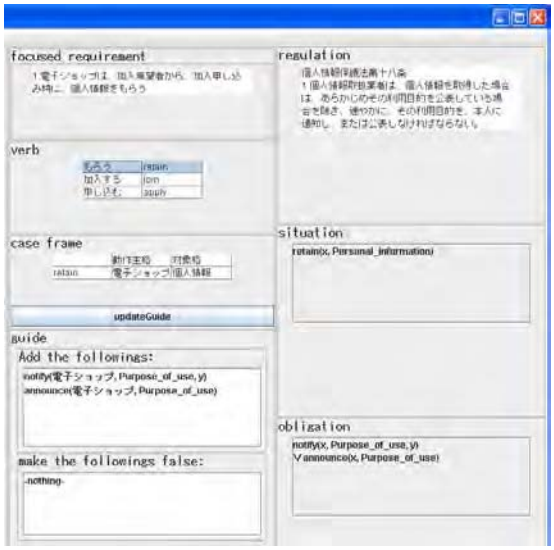

図４ 法令に適合した要求獲得の支援ツール

(3) 要求変更の支援手法：要求文が法令文に適合していない場合は要求の修正を行わなければならない．要求修正の際の波及解析を行う手法を開発した．波及解析は，各要求に属性値を振っておき，グラフで表現された要求間の論理的な関係をもとに，属性値を伝播させることにより，波及効果を推論する手法と支援ツールを開発した．図５に開発した支援ツールの画面を示す．図中の楕円で表示された部分が１つの要求を，矢印がその論理的な関係を示す．この図は，要求「トラブルコストを減らす」という要求を削除した場合，どの要求に影響が及ぶかと全体に対してどれぐらい達成度が影響を受けるかを示している．法令に違反していると判明した要求とその関連要求を単純に削除するのではなく，このツールを用いて波及効果を分析し，代替案を考えていくことが必要である．

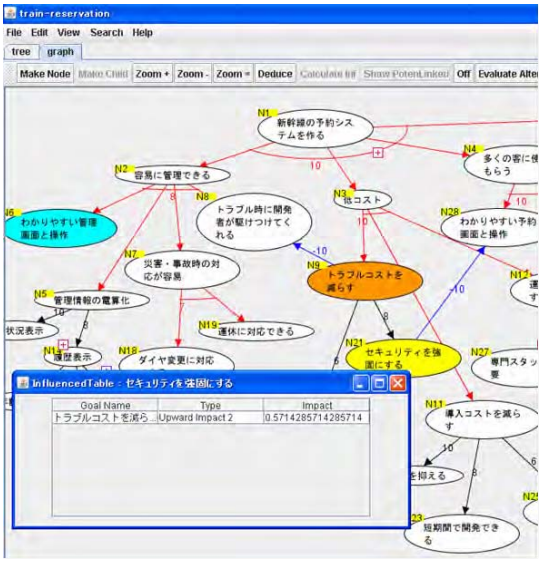

図５　変更の波及解析ツール

(4) 時相論理による法令文の表現とモデルチェッカを用いた適合性判定：(2)の手法では，動作順序などに関する性質はチェックできないため，Prolog などの述語論理ベースの手法だけではなく，時相論理とモデルチェッカを使用する手法とを併用する手法を開発した．まず，ユースケースで記述された動作仕様を状態遷移機械に変換する手法を開発し，変換ツールを開発した．ユースケース記述は自然言語で書かれているため，(1)で開発した格フレームによる意味表現法，(2)で開発した格フレームベースの法令文と要求文をマッチングする技術を用いて，語彙の統一を行いながら変換する．分岐時間時相論理で法令文の義務，禁止，許可，免除といった様相を表現する手法を開発し，法令文の時相論理式表現を検査すべき性質としてモデルチェッカへの入力とした．また，法令に適合していない場合は，モデルチェッカは反例を出力するため，(3)の技術と組みあわせ，法令に適合するようにユースケースモデルを

修正する作業を支援する手法を開発した．この流れを図６に示す．

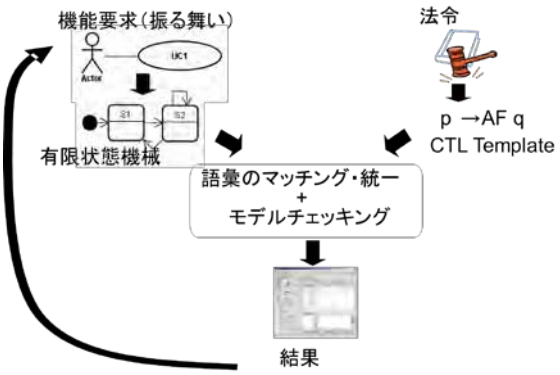

図６　モデルチェッカでの適合性判定

(5) コモンクライテリアに準拠したセキュリティ要求獲得法：セキュリティ要求記述の規則でもあるコモンクライテリアに準拠したセキュリティターゲット文書から，脅威，セキュリティ対策，セキュリティ機能要求とそれらの間の関係を抽出し，オントロジとして表現し，知識ベース化する手法の開発を行った．これらの知識はビジネスプロセスや情報システムが高いセキュリティ機能を持つためには守らなければならないセキュリティ規則とみなせる．さらにセキュリティターゲット文書から構築した知識をゴール指向要求分析法に組み込み，セキュリティ規則に準拠したセキュリティ機能要求を獲得する手法を開発し，支援ツールを開発した．ツール中では，Prolog で表現された知識を用いてゴール分解の推論を行い，分析者にそれを示唆することにより，作業の支援を行う．図７にツールの使用画面を示す．図中の楕円がゴールを，矢印がゴール分解を表わしている．ここでは「データの機密性を確保」というゴールに対し，右下のエリアで表示されているように，「暗号鍵管理」などの１３の機能を追加するように示唆されており，そのうちの「利用者認証」機能の追加を選択しようとしているところである．この手法を評価するために，e-Passport，Felica カード，住基カードのセキュリティターゲット文書から，脅威，対策，セキュリティ機能の知識と規則を抽出し，オントロジ化し，これを用いて，身分証明書，公共交通の料金のプリペイドカードなどの多様な機能を持つスマートカード管理システムの要求獲得実験を行った．その結果，２４の機能を表すゴールに対し，７のセキュリティ対策のゴール，５１のセキュリティ機能関係のゴールが追加され，いずれも抽出した知識と規則によって獲得されたものであった．これにより，本手法が有用であることとともに，特に類似分野の複数のセキュリティターゲットから知識や規則を抽出することの優位性が確認できた．

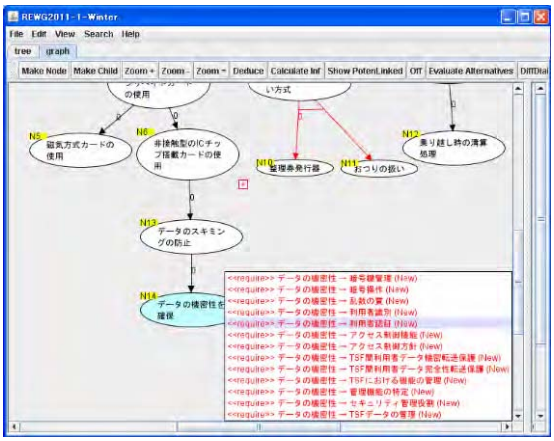

図７　セキュリティ要求獲得支援

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 13 件）

①Motoshi Saeki, Haruhiko Kaiya, Satoshi Hattori, Checking Regulatory Compliance of Business Processes and Information Systems, Communications in Computer and Information Science, Vol.50, 71-84, 2011, 査読有

② Motoshi Saeki, Semantic Requirements Engineering, Intentional Perspectives on Information Systems Engineering, 67-82, 2010, 査読無（招待論文）

③ Haruhiko Kaiya, Yuutarou Shimizu, Hirotaka Yasui, Kenji Kaijiri, Motoshi Saeki, Enhancing Domain Knowledge for Requirements Elicitation with Web Mining, Proc. of 17th Asia-Pacific Engineering Conference (APSEC2010), 3-12, 2010, 査読有

④ Motoshi Saeki, Shinpei Hayashi, Haruhiko Kaiya, An Integrated Support for Attributed Goal-Oriented Requirements Analysis Method and Its Implementation, Proc. of 10th International Conference on Quality Software, 357-360, 2010, 査読有

⑤Motoshi Saeki, Haruhiko Kaiya, Satoshi Hattori, Detecting Regulatory Vulnerability in Functional Requirements Specifications, ICSOFT, 105-114, 2009, 査読有

⑥ Ryo Hasegawa, Motohiro Kitamura, Haruhiko Kaiya, Motoshi Saeki, Extracting Conceptual Graphs from Japanese Documents for Software Requirements Modeling, Proc. of 6th Asia-Pacific Conference on Conceptual Modeling, CRPIT 96, 87-96, 2009, 査読有

⑦Motoshi Saeki, Shinpei Hayashi,Haruhiko Kaiya, A Tool for Attributed Goal-Oriented Requirements Analysis, Proc. of the 24th IEEE/ACM International Conference on Automated Software Engineering (ASE2009), 670-672, 2009, 査読有

⑧Motoshi Saeki, Haruhiko Kaiya, Security Requirements Elicitation Using Method Weaving and Common Criteria, Lecture Notes in Computer Science (Models in Software Engineering), Vol.5421, 185-196, 2009, 査読有

⑨ Motoshi Saeki, Haruhiko Kaiya, Supporting the Elicitation of Requirements Compliant with Regulations, Lecture Notes in Computer Science, Vol.5074, 228-242, 2008, 査読有

⑩Sjaak Brinkkemper, Inge van de Weerd, Motoshi Saeki, Johan Versendaal, Process Improvement in Requirements Management: A Method Engineering Approach, Lecture Notes in Computer Science, Vol. 5025, 6-22, 2008, 査読無 (招待論文)

⑪Daisuke Tanabe, Kohei Uno, Kinji Akemine, Takashi Yoshikawa, Haruhiko Kaiya, Motoshi Saeki, Supporting Requirements Change Management in Goal Oriented Analysis, Proc. of 16th IEEE Requirements Engineering Conference, 3-12, 2008,査読有

⑫ Kazuma Yamamoto, Motoshi Saeki, Attributed Goal-Oriented Analysis Method for Selecting Alternatives of Software Requirements, 電子情報通信学会英文論文誌, 91-D, 921-932, 2008, 査読有

⑬ Motohiro Kitamura, Ryo Hasegawa, Haruhiko Kaiya, Motoshi Saeki, A Supporting Tool for Requirements Elicitation Using a Domain Ontology, Software and Data Technology, Communications in Computer and Information Science, Vol.22, 128-140, 2008, 査読有

〔学会発表〕(計 12 件)
①佐伯元司, 知識ソースとしてのコモンクライテリアの活用法, 情報処理学会ソフトウェア工学研究会ウィンターワークショップ 2011・イン・修善寺, 2011 年 1 月 20 日, 修善寺

②佐伯元司, セマンティック要求工学 (招待講演), 電子情報通信学会知能ソフトウェア工学研究会, 2010 年 7 月 29 日, 釧路公立大学

③佐伯元司, 林晋平, 服部哲, コモンクライテリアをドメイン知識としたゴール指向セキュリティ要求獲得法, 電子情報通信学会知能ソフトウェア工学研究会,2010 年 3 月 5 日, 九州工業大学

④佐伯元司, 林晋平, 海谷治彦, 属性つきゴールグラフ指向要求分析法の支援のための統合ツール, 電子情報通信学会ソフトウェアサイエンス研究会, 2009 年 5 月 21 日, 秋田大学

⑤佐伯元司, 海谷治彦, 服部哲, モデルチェッカを用いた要求仕様の法令準拠性の検査, 電子情報通信学会ソフトウェアサイエンス研究会, 2008 年 12 月 18 日, 高知工科大学

〔その他〕
ホームページ等
http://www.se.cs.titech.ac.jp/research/agora/

６．研究組織
(1)研究代表者
佐伯　元司　(SAEKI MOTOSHI)
東京工業大学・大学院情報理工学研究科・教授
研究者番号：８０１６２２５４
(2)研究分担者
(3)連携研究者
(4)研究協力者
海谷　治彦　(KAIYA HARUHIKO)
信州大学・工学部・准教授
研究者番号：３０２６２５９６

林　晋平　(HAYASHI SHINPEI)
東京工業大学・大学院情報理工学研究科・助教
研究者番号：４０５４１９７５