様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 5 月 31 日現在

機関番号：３４３１５
研究種目：若手研究（Ｂ）
研究期間：2009～2011
課題番号：２１７００００４３
研究課題名（和文）　シナリオからのプロトタイプ生成によるセキュリティ要求の妥当性確認に関する研究
研究課題名（英文）　Validation method for security requirements with prototype generation from scenarios
研究代表者
糸賀　裕弥（ITOGA HIROYA）
立命館大学・情報理工学部・准教授
研究者番号：00373100

研究成果の概要（和文）：
本研究では，ソフトウェアの利用者が記述した正常シナリオに対して，セキュリティの専門家が記述したシナリオを組み合わせて，セキュリティを考慮したソフトウェアのふるまいを明らかにするとともに，実際にセキュリティを考慮したふるまいを示すシナリオのプロトタイプを生成することで，安全・安心かつ使いやすいソフトウェアであるかを，利用者が実際に確認する方法を明らかにした．

研究成果の概要（英文）：
In this research, I defined a method to analyze the behavior of software considering security requirements by integration of the normal scenario by user and the security scenarios by professionals. And I defined a method to validate whether the software is secure, safe, and easy to use by generation of prototype from scenarios expresses the actual software behavior which considers security.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,300,000	390,000	1,690,000
2010 年度	1,100,000	330,000	1,430,000
2011 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：総合領域
科研費の分科・細目：情報学、ソフトウエア
キーワード：ソフトウエア工学

１．研究開始当初の背景

(1) アプリケーションソフトウェアにおけるセキュリティ問題は，技術的な課題というだけでなく，大きな社会問題となっており，早急な対策が求められている．

このようなセキュリティ問題に対しては，ソフトウェアテストによる実践的な欠陥除去や，数学的な設計仕様による論理的な構築などの解決方法が提案されている．

しかし，アプリケーションソフトウェアにおいては，ユーザの操作や思い違いによって重大なセキュリティ問題が生じる一方で，セキュリティの確保と使いやすさは背反するものであるという考え方のために，これらの両立をはかる解決方法が見出されてこなかった．

(2) 先行研究として，アプリケーションソフトを利用する立場から記述されたふるまい（正常シナリオ）に対して，セキュリティ確保のためのふるまい（シナリオ断片）をアスペクト指向技術によって織り込み，シナリオにおいてセキュリティを確保する方法を提案した．この手法によって，セキュリティ確保と使いやすさの双方を考慮したソフトウェアのための，セキュリティ要求の獲得と分析の手法が確立された．

(3) 先行研究により，新たに 2 つの課題が明らかとなった．

① 正常シナリオは利用者が記述したふるまいであるから，十分に理解しやすい．しかし，セキュリティを確保するためのシナリオ断片が織り込まれたシナリオは，読解性が低下する場合がある．読解性の低下は，妥当性の確認を難しくし，セキュリティの確保と使いやすさの保証を困難にする．

② 正常シナリオは利用者が実際のソフトウェアを想像しながら記述したふるまいであるから，完成したソフトウェアが要求通りであるか確認しやすい．しかしセキュリティを確保するためのシナリオ断片が織り込まれたソフトウェアのふるまいは，利用者が想像したソフトウェアと異なる場合がある．ふるまいの相違は，要求通りのソフトウェアであるかの確認を難しくし，やはり，セキュリティの確保と使いやすさの保証を困難にする．

２．研究の目的

(1) 本研究の目的は，アプリケーションソフトウェアにおけるセキュリティ要求を，利用者が記述したシナリオと，セキュリティ確保のためのシナリオ断片を用いて分析し，分析された要求の妥当性の確認方法を確立することである．

具体的には，ソフトウェアのふるまいを記述したシナリオに対して，セキュリティ確保のためのシナリオ断片を織り込んだ上で，利用者とのインタラクションに関わる部分を抽出し，より詳しい操作方法を含めたシナリオとして利用者に提供する．利用者は自身の操作を想像しながらシナリオを読めるため，妥当性確認において理解性の向上がのぞめる．

(2) 本研究のもう一つの目的は，上記の目的を達成するための手法を支援するシステムを作成することである．

具体的には，シナリオにおける利用者とのインタラクションに対して特定のソフトウェア部品をあらかじめ関連づけておくことで，アプリケーションソフトウェアにおけるユーザインタフェースのプロトタイプを生成することである．利用者は自身が想像したソフトウェアのふるまいを，実際のソフトウェアの動きとして見ることができる．さらに，セキュリティ確保のために変更されたふるまいを確認し，利用者が求めるソフトウェアであるかという妥当性の確認を行える．

３．研究の方法

(1) 研究の目的を達成するために，本研究では解決すべき点を図 1 に示す 3 点とし，それぞれについて解決を図った．

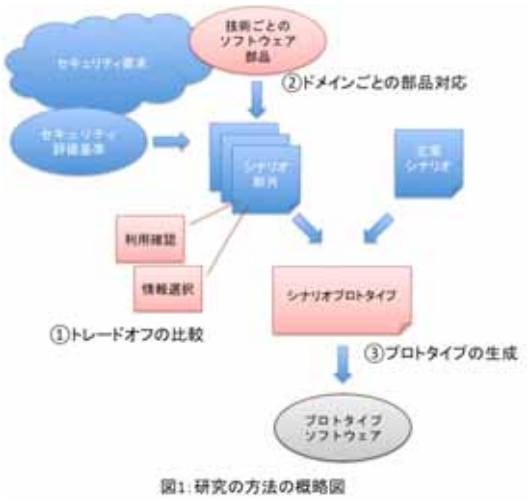

図1: 研究の方法の概略図

① 本研究では，セキュリティ要求とユーザインタフェース要求のトレードオフについて検討し，これらを記述し妥当性の確認を行う必要がある．そのためにセキュリティ要求とユーザインタフェース要求を記述できるシナリオ言語と，シナリオからのふるまいの抽出技術について研究を行った．

セキュリティ要求とユーザインタフェース要求を共通のシナリオ言語で記述するためには，ユーザインタフェース要求に該当するふるまいの語彙をシナリオ言語に導入する必要がある．そのために，グラフィカルユーザインタフェースに関するユーザインタフェースガイドラインおよびその要求獲得について調査を行った．一般的なグラフィカルユーザインタフェースにおいては，WIMP（Window, Icon, Menu, Pointer）といった要素に対する操作がガイドラインとして示されている．しかし，セキュリティ要求が必要となる認証，秘匿・匿名データの扱い等に関して一般的なガイドラインは存在せず，セキュリティに関するそれぞれの技術的な面から具体的な操作を定義しているアプローチが多数を占めていた．このため，既存のシナ

リオ言語における語彙，例えば「データの移動」の概念に対して，「ボタンをクリックする」などの具体的な操作と対応づけることで，語彙の導入に関する問題を解決した．

一方，一般的なセキュリティ要求に対する一般的なユーザインタフェースガイドラインが存在しないことから，セキュリティに関する要求や技術ごとに，使いやすさとのトレードオフを考慮してソフトウェア要求とするためには，セキュリティ要求に関する語彙の一般化・抽象化では対応できないことが判明した．そこで，それぞれの要求や技術の採用・不採用によって保証されるセキュリティの特性の変化と，採用・不採用による使いやすさの変化の両方を何らかの基準によって比較し検討することとした．

② セキュリティ要求に関して具体的なドメインを想定して分析し，シナリオ記述とする必要があることから，高機能携帯電話（スマートフォン）およびタブレット端末を対象として，ふるまいの詳細化方法およびふるまいとユーザインタフェースフレームワークとの対応について検討を行った．

具体的なドメインを高機能携帯電話およびタブレット端末としたのは，対象の機器が画面の設計や情報の入出力方法において自由度が高く，先行研究のシナリオ言語で対象としたウェブ技術への親和性も高かったためである．さらにこれらの機器には，利用者および関連の人物の個人情報，利用者および機器自体の位置情報，そして利用者および機器自体の認証情報などが多数含まれており，セキュリティ要求において対象となる情報が，簡単な操作によってやりとりされるという特性がある．このため，ソフトウェアの設計次点でのセキュリティ要求と使いやすさに関する分析と妥当性確認が特に重要だからである．

対象とした高機能携帯電話およびタブレットのアプリケーションフレームワークについて調査した結果，Android においては，個人情報・位置情報・認証情報についてアプリケーションのインストール時に利用者に対して確認を行い，その後の利用時においては再度の確認が行われないことが判明した．一方で iOS においては個人情報・位置情報・認証情報はアプリケーションの利用時にダイアログ等によって確認する必要があると判明した．同時に，インストール時の確認が理解性に乏しい場合が多数を占めていることや利用時の確認を行わない悪意あるアプリケーションが存在することが明らかとなった．これらの問題はソフトウェア開発者によるセキュリティ要求の分析が不十分なだけでなく，利用者に対してセキュリティ要求を適切に開示する方法の不足を示している．

前者の問題に対しては，本研究におけるシナリオ言語において，セキュリティ要求に関する事前条件を記述することが可能であることを利用し解決を図った．あらかじめ情報の利用の承認が行われている場合には，利用時の確認を行わない，利用の承認が行われていない場合には，利用時の確認を行うというシナリオを記述することで対応した．

後者の問題に対しては，個人情報・位置情報・認証情報において具体的な利用方法をシナリオに記述し，利用時に確認を行う方法を提案したが，これらをセキュリティ要求として要求仕様書に含めるべきかについては要求獲得者の判断に依存する部分がある．このため，利用する情報の重要性に対して数値を対応させ，数値が大きい場合には確認の操作を用いるガイドラインとすることとした．また，これらの情報の具体的な利用については，未確認のまま情報が移動することのないように，ダイアログ等を用いて確認をする必要があり，使いやすさが大幅に低下することが考えられた．そこで，使いやすさの変化を利用者や要求獲得者に知らせるために，セキュリティに関するふるまいを記述したシナリオ断片ごとに，使いやすさを示す数値を対応させ，数値の変化を示す方法とした．数値はダイアログ等，利用者による入力や確認といった操作の回数を用いることとした．扱う情報の重要性の数値と，情報を扱う操作の回数を示す数値を比較し検討することで，セキュリティ要求を明らかにする方法とすることで，トレードオフを解決した．

ただし，この方法は対象ドメインの個人情報・位置情報・認証情報に対する解決方法であり，より一般的なアプリケーションや，ダイアログ以外のより自由度の高いインタラクションで利用できるように拡張する必要がある．

③ 具体的なドメインを想定したシナリオ記述に対して，詳細なふるまいと対応したソフトウェア部品を組み合わせることでプロトタイプを生成し，セキュリティ要求の分析及び妥当性の確認を行う必要があることから，このシステムの作成を試みた．

セキュリティ要求は，個々のセキュリティ技術と密接に結びついているため，ふるまいを抽出するためには，セキュリティ技術に対応するシナリオ断片を準備する必要がある．実際のアプリケーションソフトウェアを想定したシナリオを準備し，先行研究において取り組んだ情報技術セキュリティ評価のためのコモンクライテリアで利用される語彙を用いる方法で抽象的な表現とし，さらに対象ドメイン向けに具体化するケースを用いた．この際，対象ドメインに含まれる個人情報・位置情報・認証情報ごとの重要性を分け，

対象ドメイン向けの具体化・詳細化を行う方法とした．

利用者が記述する正常シナリオに対して，シナリオ断片を織り込むことでセキュリティが確保されたシナリオが生成される．まず，セキュリティが確保されたシナリオに対して，シナリオ断片ごとに対応するソフトウェア部品を用意し，シナリオ同様にプログラムの状態で織り込み（weave）を行うことでプロトタイプソフトウェアを直接生成する方法を検討した．しかし，具体的な対象ドメインごと，セキュリティの機能ごとのソフトウェア部品を，シナリオ断片に対応する抽象化した表現とすることが困難であることが判明した．その理由は，シナリオ言語が「データの移動」といった概念を集めてふるまいを表現しているのに対して，ソフトウェア部品は概念に対する操作がドメインごと，セキュリティ技術ごとに多岐にわたっており，具体化の方法を対象のドメインおよび技術ごとに準備する必要があったためである．この問題を適切に解決できなければ，既存のソフトウェア開発者による作り込みと変わらない手法となる．

そこで，セキュリティを確保したシナリオを，より操作に具体化したシナリオプロトタイプに一度変換し，さらに操作ごとにプロトタイプソフトウェアとして生成する方法に研究の方向を変更した．シナリオにおける操作をプロトタイプソフトウェアに変換する方法は既存の研究が存在することから，実現が可能であると思われた．一方で，シナリオプロトタイプの生成においては，シナリオ断片において抽象化した表現を当該ドメイン向けに具体化・詳細化する必要がある．抽象化の際に捨ててしまうドメインごと，セキュリティ技術ごとの具体的な情報をヒントとして保存しておき，これを利用する方法を用いることとした．しかし，対応するソフトウェア部品のプログラムにおいて，シナリオにおける抽象化・具体化との対応を行う方法を明らかにすることができず，シナリオプロトタイプの操作とセキュリティ技術における操作を一致させることができていない．そのため，シナリオプロトタイプの生成を行う手法を明らかにした段階にとどまる．

(2) 本研究の実施期間において，特に対象とした高性能携帯端末やタブレットといった機器に対して，その個人情報・位置情報・認証情報を利用したサービスが多数開始された．それにともない，これらの情報を利用者が制御する方法について広く議論が行われた．本研究においては，アプリケーションソフトウェアを発注する利用者と設計・実装する技術者による要求獲得を想定していたが，現状においては，既に実装されたアプリケーションソフトウェアを利用する利用者と再設計・保守する技術者に対するセキュリティ要求の再度の明確化と妥当性の確認が必要となった．

本研究においてもアプリケーションソフトウェアの実際の利用者による，利用時の情報の扱い方に対する妥当性確認の必要性を認めたが，妥当性確認を利用時に行うというソフトウェア要求自体を，設計時に考慮するという方法を用いて一部解決することとした．

４．研究成果

(1) 本研究の学術的な特色・独創的な点としては，具体的なドメインを想定したセキュリティ技術やセキュリティに関するふるまいをシナリオとして表現する方法を明らかにしたこと，及び，そのように表現されたシナリオを組み合わせ，具体的な操作として再構成したシナリオプロトタイプとする方法を明らかにしたことである．これにより，一般の利用者には理解しづらいセキュリティに関するソフトウェアのふるまいを，読解性の高いシナリオとして読むことができ，妥当性確認が行えるようになった．

(2) 本研究で得られた成果の位置づけとしては，現在も利用者が増え続けている高機能携帯端末やタブレットといった，個人情報・位置情報・認証情報を扱うハードウェアやソフトウェアにおいて，セキュリティ要求を明らかにすることが利用者の安全・安心につながる一方で，使いやすさとのトレードオフが存在し，対象ドメインあるいは対象のセキュリティ技術を共通に扱う方法が必要となっていることが明らかとなったことである．しかし，それぞれのドメインとセキュリティ技術ごとの対応が様々であり，共通に扱う方法に対するさらなる課題が明らかになった．

(3) 本研究の今後の展望としては，ソフトウェアの妥当性確認の方法における新たな知見を得るために，シナリオプロトタイプからのプロトタイプソフトウェアの生成システムの完成を目指す．

本研究で明らかとなった手法とプロトタイプソフトウェアの生成システムの評価実験を行い，成果を公表し社会に還元していくことが早急に求められており，喫緊の課題である．

また，ソフトウェアの制作時におけるセキュリティ要求と使いやすさの確認だけでなく，社会的な変化や環境の変化に対するセキュリティ要求の変化とソフトウェア保守において明らかになった本手法の適用方法について検討する必要がある．

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）

〔学会発表〕（計 1 件）
① 発表者名：Hiroya Itoga, 発表課題：Security Requirements Elicitation using Scenarios, 学会名等：DUT-RU 2012 Joint Workshop on Information Science and Engineering, 発表年月日：2012 年 3 月 2 日, 発表場所：大連（中国）

６．研究組織
(1)研究代表者
糸賀　裕弥（ITOGA HIROYA）
立命館大学・情報理工学部・准教授
研究者番号：00373100