ISO15408 認証取得支援の為の設計情報管理システムの提案

内田 吉宣† 平井 千秋† 藤波 武起‡ 栗田 博司‡
†(株)日立製作所 システム開発研究所 ‡同 ソフトウェア事業部

1. はじめに

情報化社会が発展した今日，社会生活の中で情報システムは必要不可欠になった．それに伴い，情報システムへの不法侵入やデータ改ざんといった被害も多くなり，情報システムのセキュリティに対する関心が高まってきている．この様な背景のもとで，1999 年 6 月に開発・製造・運用に至る過程の中でセキュリティ品質を評価・認証する評価基準として国際規格(ISO15408)が承認された[1]-[2]．日本でも，2001 年 4 月から ISO15408 の評価・認証制度の運用が開始された．

本研究では，ISO15408 認証取得の為の設計者支援という観点から，設計者がセキュリティに関する仕様記述の整合性を検証する際に、その検討経緯を容易にレビュー可能とするシステムを提案する．

2. ISO15408 評価・認証プロセス

ISO15408 の評価・認証は，以下のプロセスに沿って行われる．

(1) 申請者は，セキュリティに関する基本仕様書(Security Target:ST)と，開発に関連する全ての情報(開発の仕様，工程，環境等)，セキュリティに関する分析書等を評価機関に提出する．ここで，上記の ST 以外の情報を総称して評価対象(Target Of Evaluation:TOE)と呼ぶ．
(2) 評価機関は，評価基準書(Common Criteria)と評価方法論(Common Evaluation Methodology)に基づいて，ST で適切な計画が立てられている事を検証する．その後，TOE が ST に沿って実装されているかを検証し，評価結果を出す．
(3) 認証機関は評価機関の評価結果に基づき，最終的に認証を行う．

3. 課題とそれに対するアプローチ

3.1. 課題

設計者は，ISO15408 認証を取得する為に，開発時の作成情報以外に ST や分析書等を作成し，ST や TOE の記述間で整合性が確保されている事を検証しながら，開発を進めていく必要がある．

特に，この整合性を検証する為には，様々な種類の TOE の中から，関係する記述部分を発見・収集・理解する必要がある．しかしながら，TOE の全ての記述に対して，その作業を行うには膨大な人的・時間的コストがかかり，設計者の負担は増大する．

3.2. アプローチ

本稿では，ST と TOE の検討すべき項目(検討項目)の記述間に不整合が生じる状況として，以下の 3 つがあると考えた．

(1) 設計漏れ:最初に検討項目を設定する時
(2) 伝達漏れ:検討項目を途中で追加する時
　　設計担当者が変わった時
(3) 変更漏れ:検討項目に修正が生じた時

このうち，″設計漏れ″による不整合を防止する方法として，過去の設計事例をもとに検討項目を提示する等の方法が報告されているものの[3]，その必要十分性は保証できないことから，最終的には人手による検証が必要である．一方，″伝達漏れ″,″変更漏れ″による不整合を防止する方法としては，任意の検討項目に対して，どのような検討経緯に基づいて記述が行われたかという事を，人手により検証するのが最も効果的であると考えた．すなわち，上記の状況による不整合を防止するには、人手により検証する必要があると考えた．

ISO15408 では，整合性を検証する方法として，評価保証レベルの高いものは，形式的記述言語等を用いて演繹的に行うことを求めているものの，一般的な評価保証レベルでは，設計者の確認による検証を求めている．

本研究では，設計者による確認を支援する．設計者による確認方法としてレビューがある．レビューによる方法として，作成情報の中からセキュリティ関連記述部分の検討経緯を設計者が容易にレビュー可能とする設計情報管理システムを提案する．

本システムの概要を図 1 に示す．本システムは，以下の 2 つの機能を備えていることを特徴とする．

(1)「Extraction 機能」

ST と TOE の中からセキュリティに関して検討項目目部分のみを抽出する．検討項目部分を作成物の種類に依存しないデータ構造で一元管理する事と，検討項目間の関連付けに関する情報を管理する事により，検討項目の情報の一覧表示を可能とする．

(2)「View 機能」

セキュリティに関して検討すべき項目の内容および項目間の関連を複数の観点に基づいて表示する．″設計

「Proposal of Design Information Management System for Supporting Acquirement of ISO15408」
Yoshinobu Uchida†, Chiaki Hirai†,
Takeki Fujinami‡, Hiroshi Kurita‡
†Systems Development Laboratory, Hitachi, Ltd.
‡Software Division, Hitachi, Ltd.

漏れ″に関しては，設定した検討項目を一覧表示することにより，項目の必要十分性をチェックできる．一方，″伝達漏れ″,″変更漏れ″に関しては，検討すべき項目に至るまでの過程（道筋）を一覧することにより，検討の過程を迅速に把握し、記述の整合性が確保されているかを検証する作業のコストを低減させる．

このように，「Extraction 機能」による抽出，「View 機能」による検証，不整合部分の修正，というサイクルを繰り返す事により， ST と TOE の間の記述の整合性を確保できる．

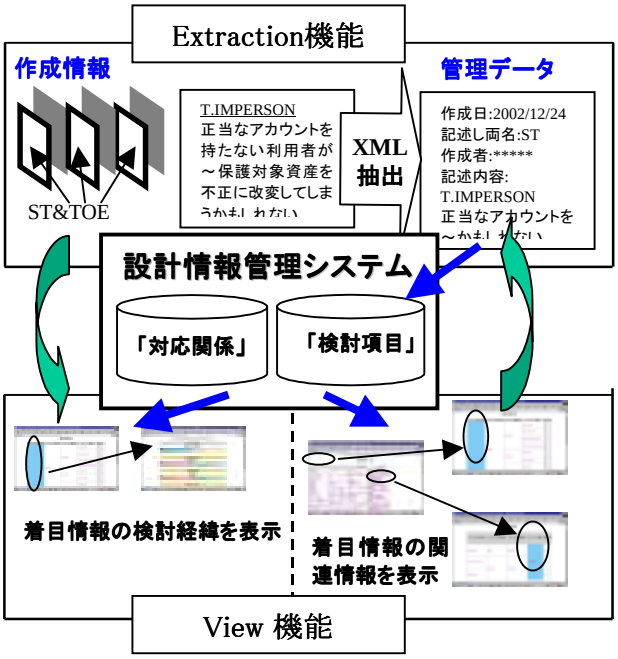

図1　設計情報管理システムの概要

4. 設計情報管理システムの実装

上記を実現するプロトタイプとして以下の機能を有するシステムを開発した．

4.1. Extraction 機能

セキュリティに関して検討項目毎に，作成情報から以下の情報を抽出する．

(1) メタ情報（作成日，記述資料名，作成者等）
(2) 本文記述内容
(3) 特定の項目（上位項目）から，直接導かれた開発工程の下位の項目（下位項目）
(4) 下位項目によって充分な対応が立てられているという証明（充足性）

抽出した上記情報のうち，(1),(2),(4)は検討すべき項目内容を記述する「検討項目」クラスの属性として，(3)については検討項目間の関連を示す「対応関係」クラスの属性として管理保持する．

4.2.View 機能

Extraction 機能により抽出保持された情報を，図 2 に示すような，「検討項目」をノード，「対応関係」を辺とする階層グラフとして表示する．

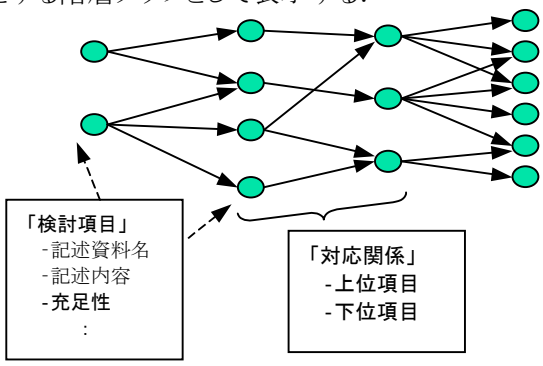

図 2　管理されるデータと階層グラフ

本機能では，以下の3つの観点による表示を実現する．

(1) 検討項目の一覧表示
検討項目に漏れがないかをチェックする．

(2) 関連部分グラフの表示
階層グラフにおいて着目する検討項目から下方（図2では右方）には有向グラフについて到達可能な検討項目を，上方（図2では左方）には有向グラフとは逆向きについて到達可能なノードと辺により構成される階層グラフの部分グラフを表示する．これにより，修正が生じた際に関連する項目をチェックする．

(3) 「検討項目」の属性の一括表示
指定した検討項目又は検討項目の関連部分グラフに含まれる検討項目の属性情報をまとめて表示．これにより，検討の過程を迅速に把握する．

5. おわりに

ISO15408 認証取得にかかる設計者の負担軽減を目的とし，作成情報の中からセキュリティに関連する記述部分を抽出する「Extraction 機能」と，抽出データを様々な観点で表示する「View 機能」から成る設計情報管理システムを提案し，プロトタイプを開発した．本システムにより，設計者が検討経緯を容易にレビューでき，記述間の整合性確保に要するコストを削減できると考える．

今後，ISO15408 を取得する情報システムの開発に適用し，開発現場での効果を定量的に評価する．

参考文献

[1]「ISO/IEC 15408『情報セキュリティ評価標準』のご紹介 Version 2.0」，情報処理振興事業協会セキュリティセンター（2000）．
[2]「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 翻訳版」，情報処理振興事業協会（2001）．
[3]永井康彦ほか:「セキュリティ対策目標の最適決定技法の提案」，情報処理学会論文誌，Vol.41，No8，pp2264-2271（2000）．