Vol.2013-SE-180 No.7
Vol.2013-EMB-29 No.7
2013/5/28

セキュリティターゲットの作成と保守を支援するツールST-Editorの開発

三浦 潤一[1,a)]　後藤 祐一[1,b)]　程 京徳[1,c)]

概要：情報セキュリティの観点から，情報システム・製品が適切に設計され，その設計が正しく実装されていることを評価するための国際標準規格として，ISO/IEC15408（Common Criteria，CC）が策定され利用されている．CC の認証を取得するためには，情報システムのセキュリティ設計仕様書であるセキュリティターゲット（Security Target，ST）を作成しなければならない．一方で，毎日のように，情報システム・製品に対する新たな脆弱性や，攻撃方法が発見されており，脆弱性の修正や対策機能の追加のために情報システム・製品の保守作業が必要不可欠である．その際には，情報システム・製品そのものの保守作業だけでなく，セキュリティ設計仕様書である ST の保守作業もあわせて行う必要がある．
しかし，ST の作成・保守作業は，人的・金銭的・時間的コストがかかり，人為的ミスも発生しやすいため，ST の作成・保守作業を支援するためのツールが必要とされている．
本研究では，ST の作成と保守を支援するツール ST-Editor を開発した．ST-Editor は，ST の構造を視覚的に表示し，その構造をもとに ST の作成や編集が行える．また，ST の作成において，難しい点，時間のかかる点，ミスを起こしやすい点を支援する機能を備えており，ST-Editor を利用することで，ST 作成・保守時の労力の軽減，ミスの低減が期待できる．

1. はじめに

情報セキュリティの観点から，情報システム・製品が適切に設計され，その設計が正しく実装されていることを評価するための国際標準規格として，ISO/IEC15408 [5][6][7]（Common Criteria [4]，CC）が策定され利用されている．CC の認証を取得するためには，情報システムのセキュリティ設計仕様書であるセキュリティターゲット（Security Target，ST）を作成しなければならない．

一方で，毎日のように，情報システム・製品に対する新たな脆弱性や，攻撃方法が発見されており，脆弱性の修正や対策機能の追加のために情報システム・製品の保守作業が必要不可欠である．その際には，情報システム・製品そのものの保守作業だけでなく，セキュリティ設計仕様書である ST の保守作業もあわせて行う必要がある．

しかし，ST の作成・保守作業は，人的・金銭的・時間的コストがかかり，人為的ミスも発生しやすいため，ST の作成・保守作業を支援するためのツールが必要とされている．

これまでに，ST の作成を支援するツールとして，ST のひな型を生成するツール GEST が提案，実装された [1]．このツールが支援するのは，ST のひな型の生成であるため，ST の作成支援の初期段階として利用できるが，ST の編集や保守には利用できない．そこで，ST の作成から保守までを一貫して支援するツール ST-Editor が提案され [2]，そのプロトタイプが実装された [3]．

ST-Editor は，ST の構造を視覚的に表示し，その構造をもとに ST の作成や編集が行える．また，ST の作成において，難しい点，時間のかかる点，ミスを起こしやすい点を支援する機能を備えており，ST-Editor を利用することで，ST 作成・保守時の労力の軽減，ミスの低減が期待できる．

提案され，実装された ST-Editor のプロトタイプは，ST の作成・保守における一部の作業を支援しているにすぎないため，実用的とは言い難かった．そこで本研究では，プロトタイプの開発で得られた知見をもとに，実用的な ST-Editor の開発をめざし，ST の作成・保守における全ての作業を支援できる ST-Editor の開発を行った．

2. セキュリティターゲット

2.1 ISO/IEC 15408 とコモンクライテリア

CC が発行された後に，国際規格化されたものが ISO/IEC 15408 であり，ISO/IEC 15408 と CC は規格としては同じものを指している．CC は数年おきにバージョンアップを繰り

[1] 埼玉大学
Saitama Uniersity
[a)] miura@aise.ics.saitama-u.ac.jp
[b)] gotoh@aise.ics.saitama-u.ac.jp
[c)] cheng@aise.ics.saitama-u.ac.jp

返しており，2013 年 4 月時点では，CC としては Version3.1 Release4 [4]，ISO/IEC 15408 としては ISO/IEC 15408-1:2009 [5]，ISO/IEC 15408-2:2008 [6]，ISO/IEC 15408-3:2008 [7] が発行されている．

政府の調達要件として CC の認証取得が必須とされていたり，推奨とされることが増えており，日本においても，「政府機関の情報セキュリティ対策のための統一基準群」[8] により，政府が情報システム・製品の調達をする場合，CC の認証を取得した製品が推奨されている．

2.2 セキュリティターゲットとプロテクションプロファイル

ST とは，情報システムのセキュリティ設計仕様書に相当する文書であり，CC の認証取得においては，ST をベースに評価を進めるため，CC の認証取得において必要不可欠な文書である．ST は従来の情報システム・製品の開発工程には存在しない文書であり，CC の認証取得の為に，新規に作る必要がある．

ST に記述すべき内容は CC で規定されており，「CC Part1 附属書 A セキュリティターゲットの仕様 (参考)」[9] によると**図 1** のようになっている．これらの項目は全て，ST において必須の項目であり，ST 作成において必ず記述しなければならないと規定されている．ただし，その構成に関しては，変更しても良いと規定されている．

PP とは，評価対象（Target of Evaluation，TOE）の種別に応じて，TOE に依存しないように作成される ST のテンプレートである．PP を利用する場合，PP をベースとして TOE を具体化して ST を作成する．PP の利用方法として一般的なのは，政府などが調達の際に，調達基準として PP を公開する方法である．この場合，政府は，調達したい情報システム・製品に求められるセキュリティ要件を PP として公開し，開発者は，その PP を基に ST を作成し CC の認証を取得することで，調達基準を満たすことを証明する．

PP に記述すべき内容に関しても CC で規定されており，「CC Part1 附属書 B プロテクションプロファイルの仕様 (参考)」 [9] によると図 1 のようになっている．図 1 よりわかるように，PP では製品ごとに異なる部分（TOE に関する部分）が省略されている．ST は PP のスーパーセットとなっていることから，ST の作成・保守支援ツールを開発すれば，そのまま PP の作成・保守支援のためにも利用できる．

ST/PP をどのように評価すべきかに関しては，「情報技術セキュリティ評価のための共通方法（Common Methodology for Information Technology Security Evaluation，CEM）」 [4] により規定されている．

ST/PP に記述すべき内容は CC で規定されているので，CC がバージョンアップすると，ST/PP に記述すべき内容も変化する．

ST/PP
- ST 概説
  - ST 参照/PP 参照
  - TOE 参照（※ ST のみ）
  - TOE 概要
  - TOE 記述（※ ST のみ）
- 適合主張
  - CC 適合主張
  - PP 主張
  - パッケージ主張
  - 適合根拠
  - 適合ステートメント（※ PP のみ）
- セキュリティ課題定義
  - 脅威
  - 組織のセキュリティ方針（OSP）
  - 前提条件
- セキュリティ対策方針
  - TOE のセキュリティ対策方針
  - 運用環境のセキュリティ対策方針
  - セキュリティ対策方針根拠
- 拡張コンポーネント定義
- セキュリティ要件
  - セキュリティ機能要件
  - セキュリティ保証要件
  - セキュリティ要件根拠
- TOE 要約仕様（※ ST のみ）

図 1 ST/PP の構造
Fig. 1 Structure of ST/PP

3. セキュリティターゲットの作成・保守における課題

3.1 作成・保守の流れ

ST の標準的な作成の流れは，以下のとおりである．

(1) TOE を定義する
(2) TOE が対処すべきセキュリティ課題定義を定義する
(3) セキュリティ課題定義の対抗策である，セキュリティ対策方針を定義する
(4) セキュリティ対策方針を CC Part2/Part3 を用いて書き換える

3.2 作成・保守における課題

ST 作成における課題は大きく分けて以下の三つが考えられる．

課題 1 ST の作成・保守作業は人的・金銭的・時間的コストがかかる

課題 2 ST の作成・保守作業における過程で人為的ミスが発生しやすい

課題 3 ST の作成・保守未経験者にとっては ST 作成・保守作業そのものが難しい

その原因として以下が考えられる．

原因 1　ST は，従来の IT 製品の製造工程には存在しない CC 独自のドキュメントである
ST の作成・保守経験がない者が ST の作成・保守をしようとした場合，まず CC のドキュメントを読み，どのように ST を記述すればよいのか理解するところから始める必要がある．ソフトウェア開発経験が豊富な者であっても，ST の作成・保守が未経験であれば，ST の作成・保守において，何を，どこに，どう書けばよいか分からない．課題 3 に対応する．

原因 2　ST に記述すべき内容は，CC で規定されている
CC で必須と規定されている内容は，ST 内に漏れなく書かなければならず，必須の内容が記述されていない場合，不完全な ST になる．課題 1，課題 3 に対応する．

原因 3　ST の各項目の記述方法は，CC の指定通りに記述しなければならない
CC で規定されている記述方法と異なる場合，不完全な ST になる．記述方法は以下の三つに分類できる．課題 1，課題 3 に対応する．

- 規定に従った記述
- 形式的な記述
- 自由記述

原因 4　ST の各項目間の内容に一貫性のある記述が求められる
各項目間の内容に一貫性がない場合，不完全な ST となる．一貫性が求められる箇所は以下のとおりである．課題 1，課題 2 に対応する．

- EAL(Evaluation Assurance Level)/CAP(Composed Assurance Package) と SAR(Security Assurance Requirement) の一貫性
- セキュリティ課題定義とセキュリティ対策方針の一貫性
- セキュリティ対策方針と SFR(Security Functional Requirement) の一貫性
- TOE と SFR の一貫性
- TOE 概要，TOE 記述，TOE 要約仕様の一貫性

原因 5　SFR/SAR コンポーネントには複雑な依存関係が存在する
SFR/SAR コンポーネントには依存関係が存在するため，あるコンポーネントを追加する場合，依存する別のコンポーネントも追加しなければならない．このコンポーネントの依存先は，複数のコンポーネントが AND/OR でつながって示されている．ST 作成者は，これを追跡して，依存先がなくなるまで，依存関係の追跡をしなければならない．このため，コンポーネントの依存関係の全列挙作業は，非常に時間がかかりミスを起こしやすい作業となる．依存関係が静的であれば，事前に依存関係の一覧を用意することも可能であるが，ST には，拡張コンポーネントが存在するため，一般的にコンポーネントの依存関係は ST ごとに異なる．課題 1，課題 2 に対応する．

原因 6　ST は，文書量が多い
ST を記述する際は，必須の内容を書かなければならず，その記述方法も規定どおりに書かなくてはならず，さらに，文書内の各項目では一貫性を保たなければならないが，ST は文書量が多い（A4 で数百ページ）ため，これらの作業をミスなく行おうとすると非常に労力がかかる．課題 1，課題 2 に対応する．

以上の課題とその原因の分析をもとに，ST の作成・保守を支援するツール ST-Editor の設計を行う．

4. 支援ツールの設計

4.1 支援方法

ST の作成・保守における課題と原因の分析結果より，ST の作成・保守においてどのような支援が必要かをまとめた．

支援 1　原因 1 に対応して，指示・ガイダンス機能を提供する
これにより，どこに，何を，どのように書けば分からない ST 作成・保守未経験者を支援する．

支援 2　原因 2 に対応して，必須内容の記述を支援する各種機能，必須内容が記述されているかチェックする機能を提供する
これにより，ST に書かなければならない内容を書き忘れるという事を防ぐことができる．

支援 3　原因 3 に対応して，ウィザード機能を提供する
これにより，CC の規定に沿って正しく ST を記述することができる．

支援 4　原因 4 に対応して，キーワード記述支援機能，対応表の生成支援機能を提供する
これにより，セキュリティ課題定義とセキュリティ対策方針の一貫性，セキュリティ対策方針と SFR の一貫性を保ちやすくなる．

支援 5　原因 5 に対応して，SFR/SAR コンポーネント間の依存関係の検索，結果の利用，検証機能を提供する
これにより，非常に時間がかかり，ミスを起こしやすいコンポーネントの依存先の全列挙作業を，素早く，ミスなく行う事ができるようになる．

支援 6　原因 4，原因 6 に対応して，ST を XML で表現した ST-XML フォーマットの導入と，ST-XML に対応した構造エディタを提供する
これにより，ST の構造を元にした ST の編集が行えるようになるため，ST の文書量の多さに関係なく，必要な個所を素早く編集できるようになる．各項目間へのアクセスも素早くできるため，各項目間の内容の一

表 1 各章ごとの支援
Table 1 Support of each chapter

章	節	ST-Editor による支援	支援割合	分類
ST 概説	ST 参照	定義，記述支援ウィザード	全て	規定準拠
	TOE 参照	定義，記述支援ウィザード	全て	規定準拠
	TOE 概要	TOE 記述支援	一部	自由記述
	TOE 記述	TOE 記述支援	一部	自由記述
適合主張	CC 適合主張	定義，記述支援ウィザード	全て	規定準拠
	PP 主張	定義，記述支援ウィザード	全て	規定準拠
	パッケージ主張	定義，記述支援ウィザード	全て	規定準拠
	適合根拠	PP と ST の一貫性検証支援	一部	自由記述
セキュリティ課題定義	脅威	キーワードラベリング支援	一部	自由記述
	組織のセキュリティ方針（OSP）	キーワードラベリング支援	一部	自由記述
	前提条件	キーワードラベリング支援	一部	自由記述
セキュリティ対策方針	TOE のセキュリティ対策方針	キーワードラベリング支援	一部	自由記述
	運用環境のセキュリティ対策方針	キーワードラベリング支援	一部	自由記述
	セキュリティ対策方針根拠	対応表の生成と検証	一部	自由記述
拡張コンポーネント定義	拡張コンポーネント定義	拡張コンポーネント定義支援	全て	CC 引用
セキュリティ要件	セキュリティ機能要件（SFR）	SFR の依存関係検索	全て	CC 引用
		SFR の入力支援	全て	CC 引用
		SFR 自動ラベリング	全て	CC 引用
	セキュリティ保証要件（SAR）	SAR の依存関係検索	全て	CC 引用
		SAR の入力支援	全て	CC 引用
		SAR 自動ラベリング	全て	CC 引用
		EAL からの自動生成	全て	CC 引用
	セキュリティ要件根拠	対応表の生成と検証	一部	自由記述
TOE 要約仕様	TOE 要約仕様	TOE 記述支援	一部	自由記述

貫性も保ちやすくなる．

ST-Editor のプロトタイプでは，支援 2，支援 3，支援 4 を考慮しておらず，支援 1，支援 5，支援 6 への対応も不十分であった．そこで，本研究では，ST の作成・保守におけるすべての工程を支援できるように，プロトタイプに足りない部分の追加，不十分な部分の強化を行い，実用的な ST-Editor を開発する．

ST の各章ごとに，ST-Editor がどのような支援を提供するかを**表 1** にまとめた．ST-Editor がどこまで支援できるかに関してを「支援割合」で，どのような記述方法が必要かに関して「分類」に表示している．分類が「規定準拠」，「CC 引用」の項目は，ほぼすべての記述を支援できるが，自由記述が求められる項目に関しては，ST の作成・保守者ごとに様々な記述方法が可能なため，原理上一部の支援までにとどまる．

4.2 要求分析

ST の作成・保守の支援方法のまとめより，ST-Editor に対する要求を定義した．R5 と R6 は，CC が様々な国で利用されており，CC のバージョンアップが頻繁に行われることから必要とされる要求である．

R1 ST-XML フォーマットに対応しなければならない
R2 ST の構造を視覚的に表示し，構造に基づいた編集ができなければならない
R3 ST の作成に慣れていない人を支援しなければならない
R4 ST の各章ごとに最適な方法で，ST の記述を支援しなければならない
R5 さまざまな CC のバージョンと言語に対応しなければならない
R6 ユーザインタフェースの多言語化に対応しなければならない

表 2 要求と機能の対応表
Table 2 Correspondence Table

	R1	R2	R3	R4	R5	R6
F1	○					
F2		○				
F3			○			
F4				○		
F5					○	
F6						○

4.3 機能定義

ST-Editor に対する要求分析をもとに，ST-Editor の機能定義を行った．要求と機能の対応は**表 2** のようになっている．

F1 ST-XML フォーマットの入力，出力，新規作成，編集，妥当性検証機能
F2 ST の構造を視覚的に表示し，編集する機能
F3 指示・ガイダンス機能
F4 各章ごとの支援機能
- **F4.1** 定義・記述支援ウィザード
- **F4.2** キーワード定義支援機能
- **F4.3** SFR/SAR コンポーネントの依存関係検索，結果の挿入，結果の検証機能
- **F4.4** EAL/CAP からの SAR リスト生成，結果の挿入，結果の検証機能
- **F4.5** 根拠表の作成支援機能

F5 CC-XML ファイルの外部からの読み込み機能
F6 ユーザインタフェースの多言語化機能

4.4 設計

ST-Editor は，ローカルアプリケーションとして動作する．

CC は様々な言語で使われていると同時に，絶えずバージョンアップを繰り返しているため，ST-Editor は，CC の言語やバージョンアップに対して柔軟でなければならない．そこで，CC の変化に依存する部分を外部ファイルとし，ST-Editor は外部ファイルを読み込むことで，適切な言語とバージョンで動作するように設計した．これにより，CC がバージョンアップしても，ST-Editor 側を変更する必要はなく，CC に関連するファイルを用意するだけでよい，また，他の言語で ST-Editor を使いたい場合も，その言語のユーザインタフェース言語ファイルを用意すればよく，ST-Editor 側を変更する必要はない．

ST-Editor のファイル構成は，以下のようになる．

- ST-Editor 本体（*.exe）
- ST-Editor 本体が利用する外部ファイル
  - UI 言語ファイル（*.dll，言語ごとに変更）
  - CC-XML ファイル（*.xml，言語・バージョンごとに

変更）
- ST-XML フォーマット定義ファイル（*.dtd/*.xsl，バージョンごとに変更）
- ST テンプレートファイル（*.stx，言語・バージョンごとに変更）

4.5 ST-XML フォーマット

ST は構造的な文章であり，その構造を扱う必要があるため，何らかのフォーマットが必要になる．文書の構造を表現するのに最適なフォーマットとして XML が良く利用されているため，XML をベースに ST-XML フォーマットを定義する．CC Portal [4] において，XML された CC が公開されているので，それをベースに ST-XML フォーマットの定義を行う．

ST-XML に対する要求は以下のとおりである．

- XML ベースでなければならない
- CC Portal で公開されている XML 化された CC と互換性を持たなければならない
- CEM での ST 評価に関する記述に対応できるタグ付けの細かさを持たなければならない
- ST-Editor 以外の ST 関連ツールで利用できる汎用性を持たなければならない
- さまざまな言語での ST の作成に対応できなければならない
- CC の 3.xx 系列にすべて対応できなければならない

ST-XML の定義は，DTD 及び XML Schema で行い，ST-XML の拡張子は「*.stx」と定義する．

ST-Editor による ST の作成・保守においては，ST-XML を意識しないで ST の編集が行え，その過程において，ST-XML フォーマットを破壊しないことが求められる．

将来，ST-XML を利用するアプリケーションを開発したい場合でも，DTD 及び XML Schema で ST-XML フォーマットが定義されているので，誰でも，ST-XML フォーマット対応アプリケーションを実装できる．

5. ST-Editor の実装

要求分析，機能定義を元に Visual Studio 2012 を用い，C#で ST-Editor を開発した．ST-Editor は.NET Framework 4.0/4.5 上で動作する．

開発した ST-Editor の主要機能を次節で紹介する．

5.1 ST-Editor の主要機能

ST-Editor を起動し，新規作成を実行した後の画面は**図 2** のようになっている．新規作成により，ST に必須の項目が自動的に生成される（ただし，中身は空）．左のツリーが ST の構造を表しており，ツリーで表現された ST の任意の項目を選択することで，その項目の内容を右側のテキストエリアに表示し，編集することができる．

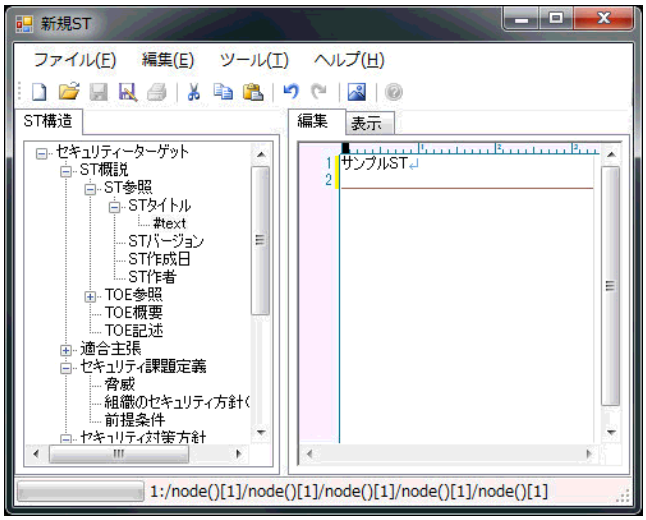

図 2 起動し新規作成を実行した画面
Fig. 2 Start and New

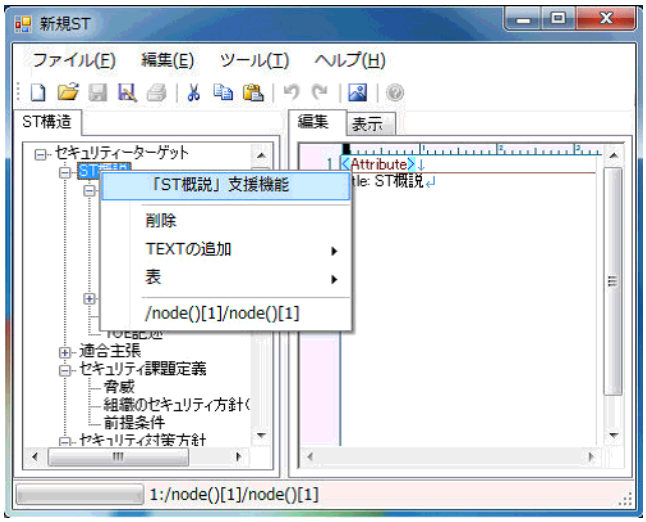

図 3 コンテキストメニュー 1
Fig. 3 Context Menu 1

テキストの編集機能としては，コピー/切り取り/貼り付け/削除，UNDO/REDO，検索/置換などの，エディタとしての基本機能を全て備えている．左側のツリーの各項目は，必要に応じて，項目の追加・削除などが行える．

任意の章を選択し，コンテキストメニューを呼び出すことで，その章に最適な支援機能を呼び出すことができる（**図 3**）．これにより，利用者は各章を順に選択していき，用意されている支援機能を利用することで，ST に必要な内容をすべて作成・編集することができる．

利用者は，編集したい項目をツリーから直接選び編集を行うこともできるし，各項目に用意された支援機能を用いて編集を行うことができる．また，各種機能は上部のメニューバーから呼び出すことも可能である．

例えば，適合主張の章でコンテキストメニューを呼び出した場合，適合主張の定義・支援ウィザードが呼び出され

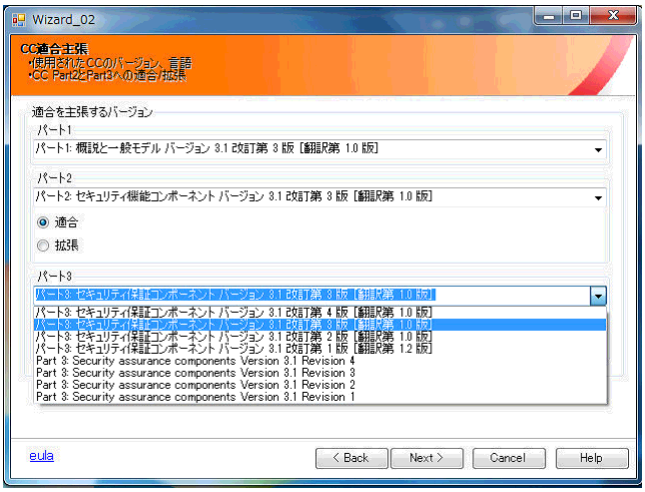

図 4 定義・支援ウィザード画面
Fig. 4 Definition and Support Wizard

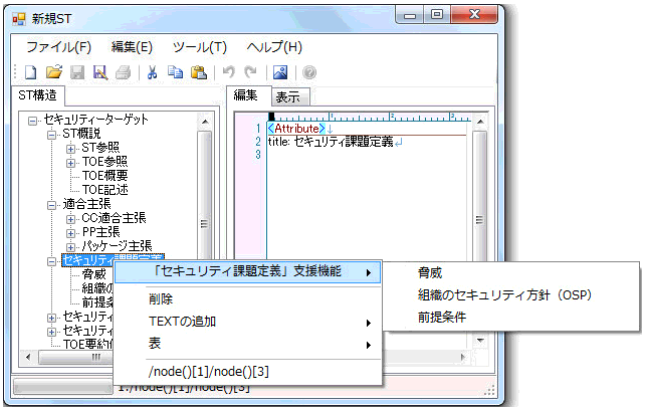

図 5 コンテキストメニュー 2
Fig. 5 Context Menu 2

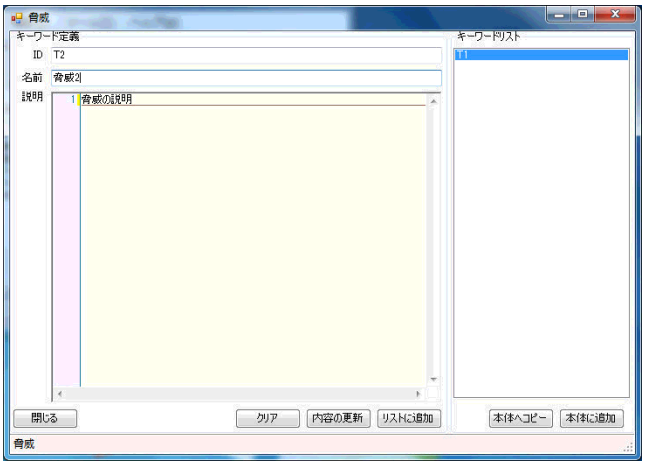

図 6 キーワード定義支援機能
Fig. 6 Keyword Definition Support

る（**図 4**）.

コンテキストメニューで呼び出される支援機能は各章ごとに異なり（**図 5**），例えば，セキュリティ課題定義の章ではキーワード定義支援機能が呼び出される（**図 6**）.

上部のメニューバーからも同じ機能の呼び出しを行う事

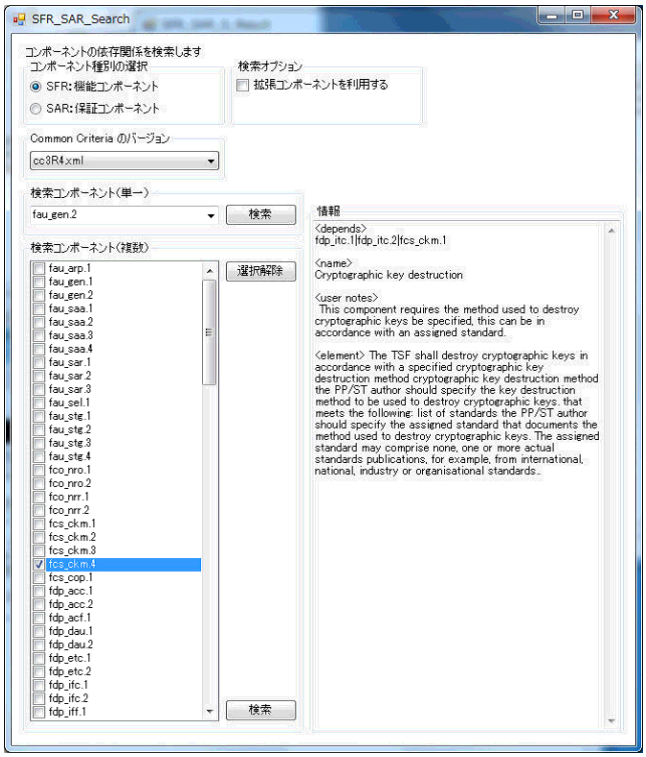

図 7 依存関係検索機能（コンポーネント選択）
Fig. 7 Dependency Search (Component Select)

ができるため，利用者は，自分のやりやすい方法で機能を呼び出し，利用することができる．もちろん，支援機能を使わないで必要な項目を直接編集することも可能である（図 2）.

次に，コンポーネントの依存関係検索について説明する．セキュリティ要件の章のコンテキストメニュー（または，上部メニューバー）から，SFR/SAR コンポーネントの依存関係検索機能が呼び出せる（**図 7**，**図 8**）．依存関係検索機能を呼び出したら，まず検索したいコンポーネントを選択（複数選択可能）する（図 7），その後，検索の実行をすることで，選択されたコンポーネントの依存関係の検索が行われ，その結果が表示される（図 8）.

検索結果（図 8）の画面構成は，左側に依存関係をツリーで表現した結果，真ん中に選択したノードにおける追加すべきコンポーネントの一覧，右側に選択したコンポーネントの内容が表示される．追加すべきコンポーネントの一覧から，必要なコンポーネントを ST に追加することできるため，検索結果を直接 ST 反映させることができる．また，左側の検索結果ツリーは，利用者が依存先のコンポーネントを選択しやすいように，ツリー表示からコンポーネント数表示に切り替えることもできる（**図 9**）.

依存先が複雑な SFR コンポーネントを例に，依存関係の検索から結果の利用までを説明する．図 8 は複雑な依存先を持つ「fcs_ckm.4」を検索した結果である．検索結果を利用しやすくするために，検索結果をツリーでなく，追加

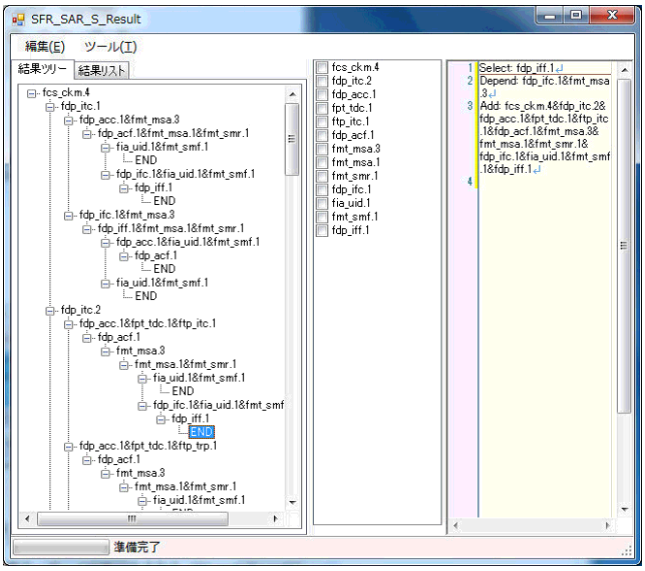

図 8 依存関係検索機能（検索結果 1）
Fig. 8 Dependency Search (Search Result 1)

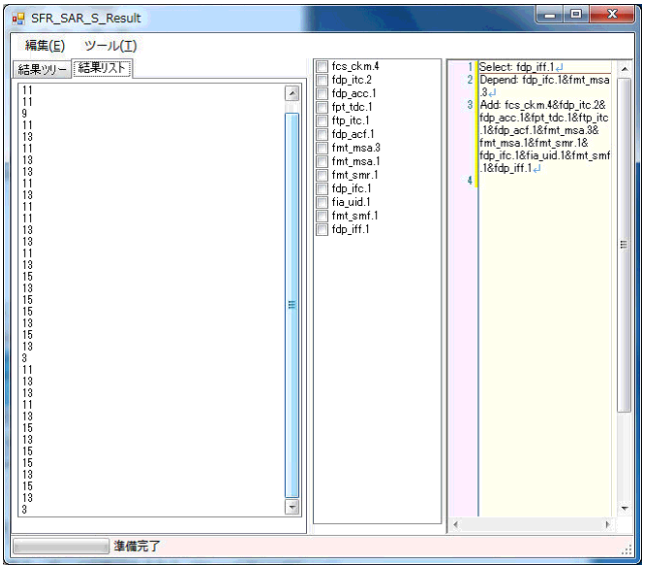

図 9 依存関係検索機能（検索結果 2）
Fig. 9 Dependency Search (Search Result 2)

するコンポーネント数で表示したのが図 9 である．図 9 より「fcs_ckm.4」を追加したい場合，38 通りの検索結果が得られることがわかる．利用者は，この 38 通りの中から必要に応じて適切なコンポーネントの組み合わせを選択し ST に反映させる．追加するコンポーネントが最も多い場合で 15 個，最も少ない場合で 3 個コンポーネントが必要なことから，単純に追加するコンポーネントが少ない組み合わせを選ぶのであれば，3 つの結果を利用すればよいことがわかる．

この結果からわかる通り，依存関係が複雑な場合，SFR の依存関係検索を人間の手で行おうとすると，非常に時間がかかりミスも発生しやすく，検索結果が複数の場合，どれを選べばよいか分かりにくい．しかし，ST-Editor を使

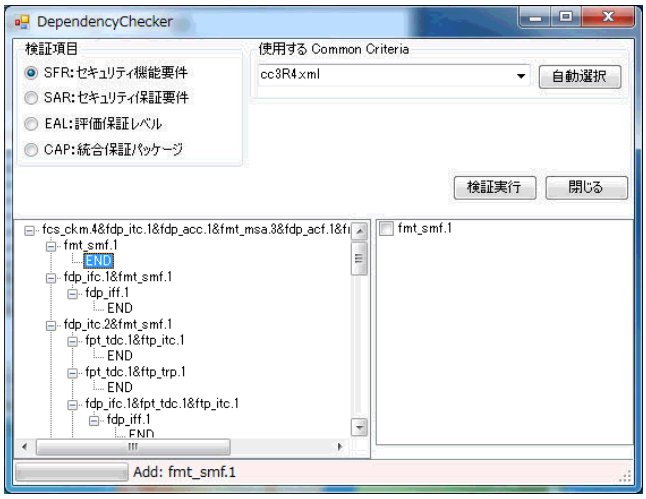

図 10 依存関係検証機能
Fig. 10 Dependency Verification

うことで，瞬時に正確に依存関係の検索を行うことができ，検索結果から適切なものを選ぶ作業も行いやすい．

図 10 は，SFR/SAR の依存関係検証機能，及び EAL/CAP の検証機能の画面である．

SFR/SAR の依存関係検証機能は，ST 内に記述された SFR/SAR がお互いに依存関係を満足し，不足コンポーネントが存在しないかどうかを検証する機能である．検証に成功した場合は，成功の表示が出て，検証に失敗した場合は，どのコンポーネントを追加すれば依存関係を満足できるのかという検索結果を表示する．不足コンポーネントが存在する場合，この画面から ST への追加が可能である．

EAL/CAP の検証では，EAL/CAP で規定された SAR コンポーネントが ST に含まれているかを検証する．検証成功時，失敗時の動作は，SFR の検証と同じである．

図 11 は，CC で規定された内容が ST に記述されているかをチェックする機能である．CC で規定された内容が記述されていない場合，該当項目のノードが赤色で表示される．利用者は，赤色の部分を埋めることで（内容が正しいかはともかく）ST に必須の項目を埋めることができる．必須の内容が記述されている場合はノードが青く表示される．これにより書洩らしが軽減できる．

図 12 は，セキュリティ対策方針根拠表の作成支援機能である．キーワード定義支援機能により定義されたキーワードを元に表を自動生成することができるため，利用者は，生成された表を埋めるだけでセキュリティ対策方針根拠の表を作ることができる．

図 13 は，ST に含まれる SFR がすべて依存先を満足しているかどうかを主張する根拠表の自動生成機能である．この表は ST 内に含まれる情報を元に全自動で生成が可能であり，基本的には利用者が編集を行う必要はない．表は右から，ST に存在する SFR，CC の規定による依存先，ST

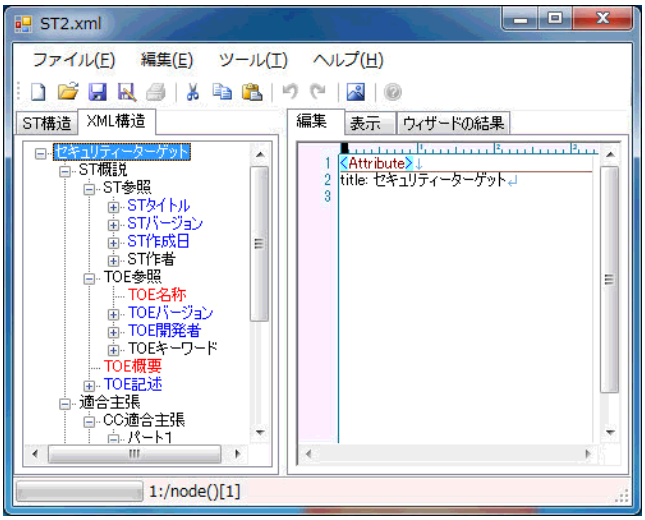

図 11 必須内容チェック機能
Fig. 11 Fill Check

図 12 セキュリティ対策方針根拠表作成機能
Fig. 12 Table Maker (Security Objectives)

が満足している SFR，ST が満足していない SFR となっている．図 13 の場合「fau_gen.1」において「fpt_stm.1」が足りてないことがわかる．

SFR の依存関係検証機能と類似しているが，依存関係検証機能は足りない SFR が存在するかどうかを検証し，足りない SFR が存在した場合に SFR を追加することができるのに対して，こちらは ST に記述すべき根拠表を生成する．

6. おわりに

本研究では，ST-Editor のプロトタイプ開発で得られた知見をもとに，実用的な ST-Editor に必要とされる機能を全て備えた ST-Editor を開発した．ST-Editor を利用することで，少ない労力で，ミスを起こすことなく ST の作成・保守が行えるようになると期待できる．

今後，開発した ST-Editor の有効性を評価する．

図 13 SFR 依存性の根拠表作成機能
Fig. 13 Table Maker (SFR Dependency)

参考文献

[1] Horie, D., Yajima, K., Azimah, N., Goto, Y. and Cheng, J.: GEST: A Generator of ISO/IEC 15408 Security Target Templates, in Lee, R., Hu, G. and Miao, H. (Eds.), *Computer and Information Science 2009*, Studies in Computational Intelligence, Vol. 208, pp. 149-158, Springer-Verlag (2009).

[2] Cheng, J., Goto, Y., Horie, D., Miura, J., Kasahara, T. and Iqbal, A.: Development of ISEE: An Information Security Engineering Environment, Proceedings of the 7th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA '09), pp. 505-510, IEEE Computer Society Press (2009).

[3] Sun, G., Yajima, K., Miura, J., Shi, K., Goto, Y. and Cheng, J.: A Supporting Tool for Creating and Maintaining Security Targets According to ISO/IEC 15408, Proceedings of the 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS 2012), pp. 745-749, IEEE (2012).

[4] Common Criteria Project: Common Criteria, available from ⟨http://www.commoncriteriaportal.org/cc/⟩ (accessed 2013-04-10)

[5] ISO: ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

[6] ISO: ISO/IEC 15408-2:2008, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

[7] ISO: ISO/IEC 15408-3:2008, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

[8] 内閣官房情報セキュリティセンター: 政府機関の情報セキュリティ対策のための統一基準群（平成 24 年度版）．入手先 ⟨http://www.nisc.go.jp/active/general/kijun24.html⟩（参照 2013-04-10）．

[9] IPA/JISEC: セキュリティ評価基準（CC/CEM）．入手先 ⟨http://www.ipa.go.jp/security/jisec/index.html⟩（参照 2013-04-10）．