2007－ＣＳＥＣ－38（７）
2007／7／19

CC V3.1 EAL1 機能特定保証 ST の有効性に関する考察

斯波 万恵[†] 佐々木 尚一[†] 石田 貴久[†] 井口 寛[‡] 島田 毅[†]

東芝ソリューション株式会社 IT 技術研究所[†]
東芝ソリューション株式会社 プラットフォームソリューション事業部[‡]
E-mail:{Shiba.Masue, Sasaki.Naokazu, Ishida.Takahisa, Iguchi.Hiroshi,
Shimada.Tsuyoshi }@toshiba-sol.co.jp

あらまし Common Criteria Version3.1(CC V3.1) Evaluation Assurance Level 1(EAL1)において、機能特定保証、プロトタイプ型機能特定保証といった新しい仕組みが制定された。本稿は、CC 作業でもとくに高コスト・高難度とされるセキュリティターゲット(ST)設計に焦点をあて、この仕組みがどの程度有効か実証実験を行った。

キーワード ISO15408、CC V3.1、機能特定保証、プロトタイプ型機能特定保証

Consideration on effectiveness of CC V3.1 Function Specific Assurance ST

Masue SHIBA[†] Naokazu SASAKI[†] Takahisa ISHIDA[†] Hiroshi IGUCHI[‡]
Tsuyoshi SHIMADA[†]

Advanced IT Laboratory, Toshiba Solutions Corporation[†]
Platform Solutions Division, Toshiba Solutions Corporation[‡]
E-mail:{Shiba.Masue, Sasaki.Naokazu, Ishida.Takahisa, Iguchi.Hiroshi,
Shimada.Tsuyoshi }@toshiba-sol.co.jp

Abstract Function Specific Assurance and Prototyping Function Specific Assurance are new concepts of Common Criteria Version3.1. We did proving experiments to learn how effective these concepts are, especially focusing on the ST design, which is claimed to be of high cost and difficulty.

Keyword ISO15408, CC V3.1, Function Specific Assurance, Prototyping Function Specific Assurance

１．はじめに

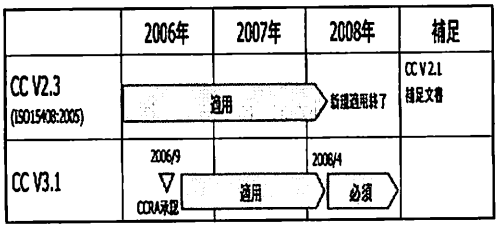
Common Criteria Version 3.1(CC V3.1)[1][2][3]の使用が、2006 年 9 月から開始した。2008 年 4 月からは、旧バージョンである CC V2.3 ではなく、CC V3.1 が必須となるため、今後 V3.1 による認証取得が加速してい

くと思われる。CC V3.1 移行措置の流れを図１に示す。

CC V3.1 と CC V2.3 との主な相違点は、セキュリティ機能の基本設計を記す、セキュリティターゲット(ST)と呼ばれるセキュリティ設計仕様書に記述すべき内容あるいは保証すべき要件が、Evaluation Assurance Level 1(EAL1)の場合と EAL2 以上で異なることである。

日本の CC 認証機関である情報処理推進機構(IPA)は、CC V3.1 EAL1 を「機能特定保証」と名付け、開発コスト削減により短期間での認証取得が可能として、機能特定保証による認証取得を推奨している。さらに、機能特定保証に IPA が指定したガイドラインとテンプレートを用いて ST を作成した IT 製品に対して評価認証を行う「プロトタイプ型機能特定保証」(プロトタイプ型)も 2007 年 3 月に提案され、「CC V3 プロトタイプ型機能特定保証ガイダンス」[4]が 2007 年 5 月に公開された。

本稿では、IPA が推奨している機能特定保証およびプロトタイプ型の有効性について、開発者の立場で ST 設計に着目して考察する。２章で CC V3.1 EAL1 の ST と機能特定保証の概念を示し、３章で本研究の目的、４章で目的に対する有効性の検証として今回我々が試行した ST 設計の方法、結果および考察について述べ、５章でまとめる。

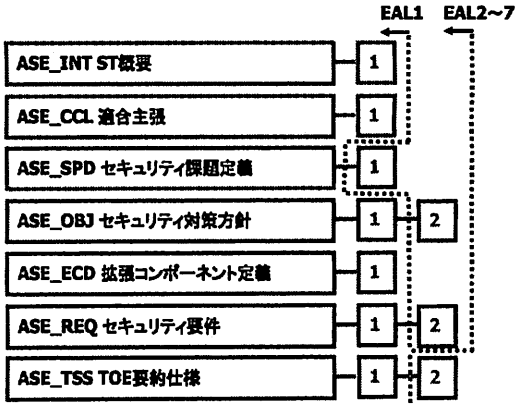


【図１】CC V3.1 移行措置の流れ

２．機能特定保証の概念

２．１．CC V3.1 EAL1 の ST

CC V3.1 EAL1 の ST に求められるセキュリティ保証要件では、図２に示すように、「セキュリティ課題定義」が不要である。これは、評価対象 Target Of Evaluation(TOE)の種別、概要、運用環境から TOE のセキュリティ機能を導き出すことに重点が置かれ、TOE の脅威と前提条件、セキュリティ対策方針の妥当性は問わないという考え方に基づいている。



【図２】CC V3.1 EAL1 セキュリティ保証要件

CC V3.1 EAL1 の ST 構成を表１に示す。３章「セキュリティ対策方針」には運用環境の対策方針のみを記述すればよく、６章「TOE 要約仕様」では根拠を記述しなくてもよい。

【表１】CC V3.1 EAL1 ST 構成

１章　ST 概要	1.1 ST 参照
	1.2 TOE 参照
	1.3 TOE 概要
	1.4 TOE 記述
２章　適合主張	2.1 CC 適合
	2.2 PP 適合
	2.3 パッケージ適合
	2.4 適合根拠
３章　セキュリティ対策方針	3.1 運用環境のセキュリティ対策方針
４章　拡張コンポーネント定義	

5章　セキュリティ要件	5.1 セキュリティ機能要件
	5.2 セキュリティ保証要件
	5.3 セキュリティ要件根拠
6章　TOE 要約仕様	

2．2．機能特定保証の概念

機能特定保証とは、CC V3.1 EAL1 での CC 評価認証の別称である。EAL1 では、ST で特定したセキュリティ機能に対して評価認証を行うため、認証マークは IT 製品全体ではなく、評価を行ったセキュリティ機能に対してのみ付与される。

2．3．プロトタイプ型機能特定保証の概念

プロトタイプ型は、初めて CC 評価認証を取得するベンダ向けに、CC の内容を深く理解しなくても証拠資料が作成できるように IPA が開発したものであり、「機能特定保証」のうち IPA が定めた「CC V3 プロトタイプ型機能特定保証ガイダンス」に忠実に従い、CC 評価認証を行う仕組みである。

開発者は、「開発証拠資料作成ガイダンス」に従って、開発証拠資料である ST、機能仕様書、ガイダンス文書（導入マニュアル・運用マニュアル）、構成リストを作成する。

プロトタイプに基づいた証拠資料作成と評価には、次の３つの利点があると IPA は述べている。

- 開発者に CC の知識は不要
- 開発者の作業工数は１～２週間（目標）
- 評価開始から認証書取得まで１～２ヶ月程度（目標）

とくにプロトタイプ型では、ST 設計の作業を簡略化するために、評価の対象とするセキュリティ機能を識別認証、アクセス制御、暗号、セキュリティ管理の４つに大きく分類し、これらのセキュリティ機能を実現するために必要なセキュリティ機能要件(SFR)を 17 コンポーネントに制限している。CC Part2 にリストアップされている SFR は 11 クラス、133 コンポーネントであるが、プロトタイプ型で使用できるコンポーネントは、国内で評価認証実績のある SFR の代表的なものに限定される。

3．本研究の目的

このように、CC V3.1 で EAL1 対応の簡略化した ST と、日本独自のプロトタイプ型機能特定保証という概念が生まれた背景には、以下の事情がある。

- CC の認証取得には専門的な知識が必要であり、政府統一基準[5]や産業競争力のための情報基盤強化税制[6]といった制度を導入しても、一部のパワーベンダを除き、利用者の裾野が広がらない。
- 証拠資料作成および評価に、多くの時間とマンパワー（コスト）がかかる。とくに ST 設計と評価には、認証取得までに必要な作業全体の約３割の作業時間が必要といわれている。

CC V2.3 における我々の評価認証取得コンサルテーション経験から、はじめて認証取得を行うベンダの新規開発製品では、開発者一人で ST 設計を行った場合、平均で 1.5 人月、約 250 時間を要している。

機能特定保証とプロトタイプ型といった新しい仕組みの有効性を、以下の視点で検証することが、本研究の目的である。

1. CC V2.3 に比べて ST 設計期間は短縮するか
2. ガイダンスに従えば、CC の知識がない開発者も容易に正確な ST が作れるのか
3. どのような場合に機能特定保証やプロトタイプ型の ST が有効となるのか

4．有効性の検証

4．1．方法

3章で示した3つの視点を検証するために、我々は実際のIT製品を題材としてST設計を試行した。題材には、東芝ソリューション(株)の FlexClient/Mobile™[7] を用いた。FlexClient/Mobile™は、PC持ち出しによる情報漏えいの脅威から社内の情報資産を守るセキュリティ機能を備えたシンクライアント対応のミドルウェアである。

検証の方法として、以下の試行を行った。

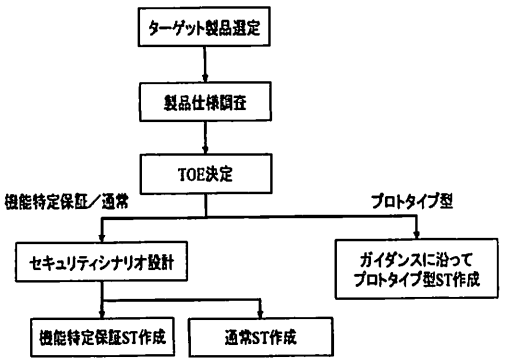
試行1：「開発者証拠資料作成ガイダンス」を参照して、ST設計経験のない開発者とST設計経験者がそれぞれプロトタイプ型STを作成する。但し、それぞれの開発者の題材となるIT製品のセキュリティ機能に関する知識は同等である。

試行2：CC V2.3でST設計の経験がある開発者が、CC V2.3と同じST設計プロセスに従って、以下の2種類のST設計を行う。

(1)機能特定保証ST

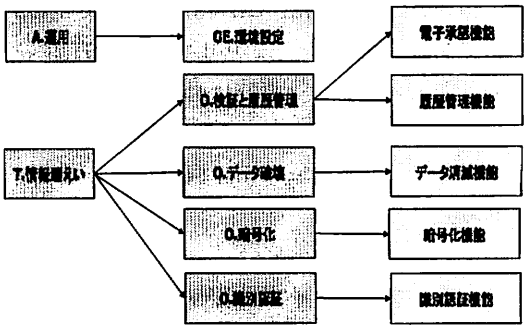
(2) EAL2以上で使用するST(通常ST)

今回の試行におけるST設計の作業フローを図3に示す。



【図3】ST設計の作業フロー

図3の「セキュリティシナリオ設計」とは、セキュリティ課題定義（脅威、前提条件）とセキュリティ対策方針を策定し、実装するセキュリティ機能とリンク付けることであり、それぞれをトレースできるように図式化したものを「セキュリティシナリオ」とよぶ。試行2で試作したSTのセキュリティシナリオ例を図4に示す。



【図4】セキュリティシナリオ

4．2．結果

試行1の結果として、ST設計経験の有無によるプロトタイプ型STの作業時間とST頁数の違いを表2に、それぞれの作業工数内訳を表3に、STに記述したSFRとセキュリティ機能の数の差を表4に示す。

【表2】プロトタイプ型STの作業時間とST頁数

	経験者	未経験者
時間(H)	22	78.5
ST頁数	14	61

【表3】作業工数内訳(H)

	経験者	未経験者
製品仕様調査	12.5	14
用語・1章	3.5	6.6
2章	0	0.4
3章	1	0.5
4章	0	0

5 章	1	23
6 章	1	28
確認・レビュー	3	6

【表４】プロトタイプ型 ST の SFR とセキュリティ機能数

	経験者	未経験者
SFR　　クラス	2	4
コンポーネント	6	16
セキュリティ機能	2	5

試行２の結果を表５から表７に示す。表 5 に試行１で作成したプロトタイプ型 ST、および試行２で作成した２種類の ST の作業時間と ST 頁数、表６にプロトタイプ型 ST と機能特定保証／通常 ST でそれぞれ選択した SFR、表７にプロトタイプ型 ST と機能特定保証／通常 ST に記述したセキュリティ機能を示す。

【表５】作業時間数と ST 頁数

	プロトタイプ型 ST	機能特定保証 ST	通常 ST
時間(H)	22	42	50
ST 頁数	14	21	26

【表６】選択した SFR

プロトタイプ型 ST	機能特定保証／通常 ST
FIA_UID.1	FAU_GEN.1
FIA_UAU.2[1]	FCS_CKM.1
FIA_UID.2	FCS_COP.1
FIA_UAU.2[2]	FDP_DAU.1
FIA_UAU.7	FDP_RIP.1
FCS_CKM.1	FIA_UID.2
FCS_COP.1	FIA_UAU.2
	FIA_UAU.7

【表７】セキュリティ機能

プロトタイプ型 ST	機能特定保証／通常 ST
・ 識別認証機能 ・ 暗号機能	・ 電子承認機能 ・ 履歴管理機能 ・ データ消滅機能 ・ 暗号化機能 ・ 識別認証機能

４．３．考察

試行結果を 3 章で示した 3 つの視点に基づいて考察する。

1. CC V2.3 に比べて ST 設計期間は短縮するか

表 2 から、未経験者の CC V 3.1 プロトタイプ型 ST 設計の作業時間は 78.5 時間という結果が得られた。対象となる IT 製品は異なるものの、同じように未経験の開発者が一人で ST 設計を行った場合の作業時間は、CC V2.3 では我々のコンサルテーション経験により平均 250 時間であることから、ST 設計期間は、CC V2.3 に比べて約 1/3 程度に短縮できるのではないかと考えられる。

2. ガイダンスに従えば、CC の知識がない開発者も容易に正確な ST が作れるのか

ST 設計の中で、とくに CC の専門知識が必要となるのは、５章「セキュリティ要件」のセキュリティ機能要件に関する記述である。今回、未経験者がプロトタイプ型のガイダンスに従い ST 設計を行った結果、表 3 の作業工数内訳に示すとおり、５章「セキュリティ要件」の作成に 23 時間、約 30%の工数を占めており、従来も ST 設計の課題であった CC の知識が必要な項目の難易度は軽減していない。従って、プロトタイプ型のガイダンスに従っても容易に ST 設計が行えるとは言い難い。

次に、正確な ST が作れるのかという点について、考察する。SFR が CC Part2 の中から自由に選択できる場合は、IT 製品の持つ特長的なセキュリティ機能を ST に記述することがで

きるが、プロトタイプ型では、17 コンポーネントの限定された SFR だけで表現しなければならない。このため、表 4 に示すように経験者は 2 つのセキュリティ機能のみを選択し、繰返しを除く 6 つのコンポーネントに対応させた。プロトタイプ型で経験者が選択した SFR を表 6 の左側に、セキュリティ機能を表 7 の左側に示す。一方、未経験者は、IT 製品の持つすべてのセキュリティ機能を ST に記述すべく、選択可能な 17 コンポーネントの SFR のうち、16 コンポーネントを用いて表現しようとした。それぞれの ST をレビューした結果、未経験者が選択した SFR は不適切であり、正確な ST とはならなかった。

これらの結果から、現在のプロトタイプ型の開発者向けガイダンスは、未経験の開発者にとっては、まだハードルが高く、誤った解釈をしてしまう可能性があり、改良が必要であるといえる。

3. *どのような場合に機能特定保証やプロトタイプ型の ST が有効となるのか*

ST に記述する内容が少ないほど設計期間も少なくなることが表 5 の結果から実証された。

とくにプロトタイプ型は、評価対象となる IT 製品のセキュリティ機能が、利用者の識別認証とアクセス制御に関わる機能や、データの暗号化に限定される既存製品であり、低コストで早期に CC 評価認証を行いたい場合に有効であるといえる。

しかし、表 6、7 に示すように機能特定保証／通常 ST では IT 製品に実装されている特長的なセキュリティ機能が網羅できているのに対し、プロトタイプ型では識別認証と暗号に関する SFR しか選択肢がなかった。調達仕様上必要な、あるいは IT 製品の特長的なセキュリティ機能をプロトタイプ型で制限されたコンポーネントで表現できないケースでは、有効とならないことに注意しなければならない。

5．まとめ

実際の IT 製品を題材にして CC V3.1 に適用できる 3 種類の ST 設計を試行することにより、新しい仕組みの有効性を考察した。

このデータから CC V3.1 の機能特定保証やプロトタイプ型の ST は、開発においてコスト削減が期待できることがわかった。

一方、プロトタイプ型を利用する上で留意すべき課題も明らかになった。

今後、さらに追試を行い、より正確な比較検討ができるデータの収集、考察とプロトタイプ型の具体的な改良点について提示したい。

参考文献

[1]CC V3.1 Part1 http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf

[2]CC V3.1 Part2 http://www.commoncriteriaportal.org/public/files/CCPART2V3.1R1.pdf

[3]CC V3.1 Part3 http://www.commoncriteriaportal.org/public/files/CCPART3V3.1R1.pdf

[4] CC V3 プロトタイプ型機能特定保証ガイダンス http://www.ipa.go.jp/security/jisec/ccv3_eal1.html

[5] 統一基準 http://www.nisc.go.jp/active/general/kijun01.html

[6] 情報基盤税制 http://www.meti.go.jp/policy/it_policy/zeisei/index.html

[7]東芝ソリューション（株） FlexClient http://pf.toshiba-sol.co.jp/prod/thinclient/index_j.htm