情報処理学会論文誌　Vol. 50　No. 9　2274–2283 (Sep. 2009)

セキュリティ評価認証を効率化する開発プロセスと証拠資料作成支援システム

斯　波　万　恵[†1]　　佐々木　尚一[†1]

ISO/IEC15408（CC: Common Criteria for Information Technology Security Evaluation）に基づく IT 製品や情報システムのセキュリティ認証の取得が普及してきた．国内では，IC カードやデジタル複合機といった一部の IT 製品での認証取得が特に顕著である．しかし，CC 評価認証は製品開発に加え，評価のための証拠資料作成や開発期間と開発コストがかさむこともあり，新規に認証取得を行うベンダや IT 製品の裾野が広がらないといった問題もかかえている．本稿では，このような背景から製品開発のプロセスと認証取得プロセスを統合し効率化するための開発プロセスと証拠資料作成支援システムを提案する．

Development Process and Evidence Document Creation Supporting System for Security Evaluation

Masue Shiba[†1] and Naokazu Sasaki[†1]

The number of IT products and the information system that have security evaluation certification of based on ISO/IEC15408 (CC: Common Criteria for Information Technology Security Evaluation) is increased. The certification of IC cards and the digital compound machines are remarkable in Japan. However, the CC evaluation has the problem that there are few venders and IT products newly get the certification, because consume the development period and the cost. In this paper, we suggest the development process where a usual development process and the evaluation ceertification process were integrated, and an evidence document creation support system.

†1 東芝ソリューション株式会社
TOSHIBA SOLUTIONS CORPORATION

1. はじめに

IT 製品や情報システムに対する IT セキュリティ評価・認証制度 ISO/IEC15408（CC: Common Criteria for Information Technology Security Evaluation）が，国内で 2001 年 4 月から運用されており，認証取得した IT 製品や情報システム（プロダクト）は**図 1** に示すように毎年増加している[⋆1]．

国内では，IC カードやデジタル複合機といった一部の IT 製品での CC 認証取得が特に顕著である．しかし，CC 認証は製品開発に加え，認証取得のための証拠資料作成や評価認証の対応のために開発期間と開発コストがかさむこともあり，新規に認証取得を行うベンダや IT 製品の裾野が広がらないといった問題もかかえている．

本稿では，一般的なプロダクトの開発のプロセスと認証取得プロセスを統合したセキュリティを向上させるための開発プロセスと，評価認証で必要となる証拠資料を半自動で作成する証拠資料作成支援システムを提案する．本稿で提案する開発プロセスと証拠資料作成支援システムは，民生用のプロダクトで一般的に用いられる評価保証レベル（EAL: Evaluation Assurance Level）1 から 4 を対象とする．

2 章で，CC 評価認証制度の概要，3 章で日本の CC 評価認証制度と取り組む開発者の課題を示し，4 章で提案する開発プロセス，5 章で提案する証拠資料作成支援システムについ

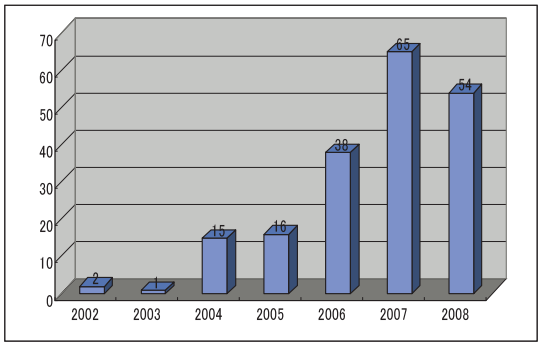

図 1　認証取得プロダクトの動向
Fig. 1　Trend of certification products.

⋆1 2008 年 11 月までの実績．

て述べ，6 章でまとめる．

2. CC の概要

CC は，プロダクトのセキュリティを開発者の主張に基づいて第三者機関が評価し，国が定めた認証機関が認証するための世界共通の評価基準である．

CC の基準は，セキュリティ評価の背景，考え方，開発/評価モデルを示したパート 1「概要と一般モデル」[1]，セキュリティ機能の要件集であるパート 2「セキュリティ機能コンポーネント」[2]，開発プロセスの設計，開発，テストといった作業フェーズにおいて，セキュリティ機能が正しく実装されていることを確認するための検査項目集であるパート 3「セキュリティ保証コンポーネント」[3] の 3 部から構成される．

CC パート 3 のセキュリティ保証要件は，**図 2** に示すように階層構造になっており，8 クラス，38 ファミリ，各ファミリに幾つかのコンポーネントがある．

表 1 にセキュリティ保証要件クラスと各クラスのファミリ数を示す．

また，これら保証要件への適合評価においても IT セキュリティ評価のための共通方法論 CEM（Common Methodology for IT Security Evaluation）[4] が標準化されている．

CC の認証取得を行う開発者は，**表 2** に示す 7 段階の評価保証レベル（EAL: Evaluation Assurance Level）の中から適合主張するレベルを選択する．

EAL はセキュリティの強度ではなく，どれだけ厳密にプロダクトのセキュリティをチェックするかというレベルである．そのため，レベルの数字が大きくなるほど，厳密な評価が行われ，多くの証拠資料が要求される．EAL は，それぞれのレベルで CC パート 3 のセキュリティ保証要件から満たさなければならない要件が提示されており，プロダクトの企画，設計開発，実装，テスト，納入に至るまでセキュアな環境で開発が行われていることが評価される．

開発者は，選択したレベルに適合した設計開発，実装，テストを行い，ユーザが利用開始するまでのライフサイクルを対象に，設計ドキュメントや運用記録を作成する．さらにセキュリティ設計仕様書（ST: Security Target）を公開して，プロダクトのセキュリティへの取り組みをユーザに正しく説明する必要がある．ST は，プロダクトの脅威分析を行い，脅威分析に基づいた対策方針とセキュリティ機能を実現するために必要かつ十分な方法，機能をまとめた文書である．ST はプロダクトの最上流に位置づけられる設計仕様であり，その他の評価に必要なドキュメント（証拠資料）は ST に書かれていることに一貫しているか，という観点で評価される．

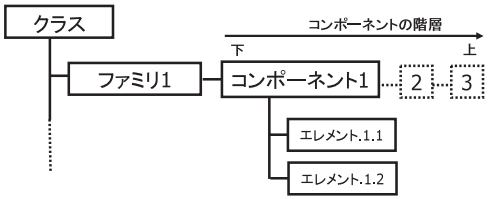

図 2　階層構造
Fig. 2　Layered structure.

表 1　セキュリティ保証要件のクラス
Table 1　Assurance class.

保証要件クラス	ファミリ
APE プロテクションプロファイル評価	6
ASE セキュリティターゲット評価	7
ADV 開発	6
AGD ガイダンス文書	2
ALC ライフサイクルサポート	7
ATE テスト	4
AVA 脆弱性評定	1
ACO 結合	5

表 2　評価保証レベル
Table 2　Evaluation assurance level.

EAL	概要
EAL7	形式的検証済み設計，及びテスト
EAL6	準形式的検証済み設計，及びテスト
EAL5	準形式設計，及びテスト
EAL4	方式設計，テスト，及びレビュー
EAL3	方式テスト，及びチェック
EAL2	構造テスト
EAL1	機能テスト

3. セキュリティ製品開発の課題

3.1 日本における評価保証制度の課題

政府は，国内での評価・認証制度の普及を目的に，中央省庁向けに「政府機関の情報セキュリティ対策のための統一基準」[5] を定め「情報システムのセキュリティ要件」および「ソフト

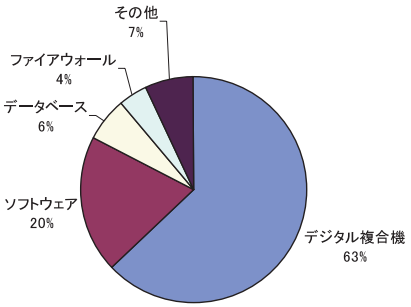

図 3　認証取得製品の内訳
Fig. 3　Breakdown of certification product.

ウェア開発」における基本遵守事項として，重要なセキュリティ要件が求められるものについては，セキュリティ設計内容が基準に適合していることを評価する ST 確認[6] を要求するといった日本独自の取り組みが行われ，政府の情報システム最適化計画の案件に適用されている．民間向けには，「産業競争力のための情報基盤強化税制」[7] が制定され，ISO/IEC15408 に基づいて評価・認証された製品の活用により，税制優遇措置を受けられることをメリットとして，サーバや DBMS 製品のメーカやベンダを中心に，認証取得が行われている．

これらの動向とは別に，セキュリティの確保が重要な IC カードや米国や中央省庁で調達要件として認証取得が必須となるデジタル複合機といった一部の IT 製品での認証取得も顕著である．

一方で，CC 認証取得は，製品開発に加え認証取得のための証拠資料の作成や開発期間の延長，開発コストがかさむこともあり，費用対効果の面でも開発者にとってまだ敷居が高いという声も大きく，新規に認証取得を行うベンダやプロダクトの裾野が広がらないといった問題もかかえている．

図 3 に制度開始から 2008 年 11 月までに国内で認証取得を行ったプロダクトごとの内訳を示す．認証取得製品の 6 割以上をデジタル複合機が占めている．実際に認証取得したベンダも**図 4** に示すように上位 7 社が認証取得件数全体の約 7 割を占めている．

このような問題に鑑み，日本の CC 認証機関である情報処理推進機構（IPA）は，CC V3.1 において，評価保証レベルが最も低い 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，特定のセキュリティ機能要件のみをセキュリティ機能として搭載する 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」という制度を 2007 年 5 月に導入した[8]．この制度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．

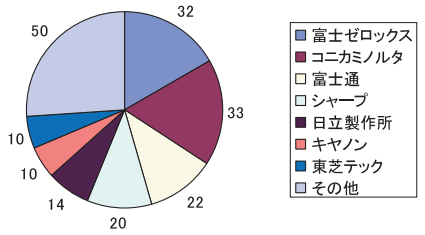

図 4　ベンダ別認証取得件数
Fig. 4　Certification number according to vender.

- ガイドラインとテンプレートにより，開発者に CC の専門的な知識は不要である．
- 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 カ月（目標）．

しかし，制度開始から 2008 年 11 月時点でこの制度による CC V3.1 の認証取得製品は，機能特定保証 3 件，プロトタイプ型機能特定保証 2 件と低調である．認知度の低さとともに，開発者側の支持が得られていないのではないかと思われる．こういった背景から，我々は CC の普及展開には開発者の視点に立った抜本的な改革が必要であると考え，開発者の課題を整理することから始め，開発者の課題に対する解決策を提示する．

3.2　開発者の課題

CC 評価認証を取得している開発者や評価・認証機関が，開発者側の問題として指摘しているのは，プロダクトの開発途中や開発終了後に認証取得のための取り組みを始める場合に，開発工程の上流に遡って証拠資料を作らなければならないという点と，開発終了後に評価コメントに対応することで仕様変更が発生することがあり，製品開発の後戻りになるためスケジュールへのインパクトが大きいという点である．また，開発者にとっては，評価認証に時間がかかりすぎるため，プロダクトのリリース時に認証取得ができなくなることがあり，プロダクトの付加価値や差異化要素がアピールできないだけでなく，調達要件を満たせなくなるかもしれないというリスクがある．

初めて CC 評価認証に取り組むメーカやベンダは，IT 製品の商品企画時に開発と並行して CC 評価認証の対応を行おうとしても，CC のセキュリティ保証要件と開発工程の関連が

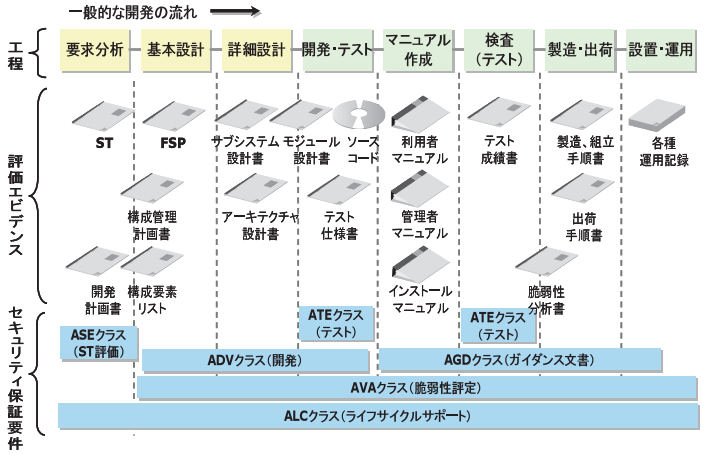

図 5　開発工程とセキュリティ保証要件
Fig. 5　Development process and security assurance requirement.

CC や CEM で明確に示されておらず，セキュリティ保証要件間の依存性も複雑なため，セキュリティ保証要件のクラスと工程を単純に対応付けただけでは，どのような手順で証拠資料の作成を進めていけばよいのか，作業イメージが分からないといった問題がある．また，CC はセキュリティ保証要件が抽象的な表現で書かれているため，証拠資料を作成するさいに既存の開発資料のどの部分と対応付ければよいのかが分からない，あるいは，証拠資料の作成そのものに時間がかかりすぎる．前述したように，評価中に仕様変更や証拠資料の見直しが発生することがあり，すべての証拠資料の一貫性を保って正確に変更することが困難といった問題もある[13),14)]．

以上の問題を整理すると，第 1 にセキュリティ保証要件とプロダクト開発工程が結び付いていない，第 2 に評価認証に必要な証拠資料を効率良く作りたい，という 2 つの課題が明らかになった．

3.3　開発者の課題の分析

第 1 の課題である「セキュリティ保証要件とプロダクト開発工程が結び付いていない」を解決するために，プロダクト開発のどの工程でセキュリティ保証要件のクラスに対応した開発を行えば十分であるかを考える必要がある．**図 5** に一般的なウォーターフォール型の工程と証拠資料，セキュリティ保証要件クラスの対応関係を示す．CC におけるセキュリティ保証要

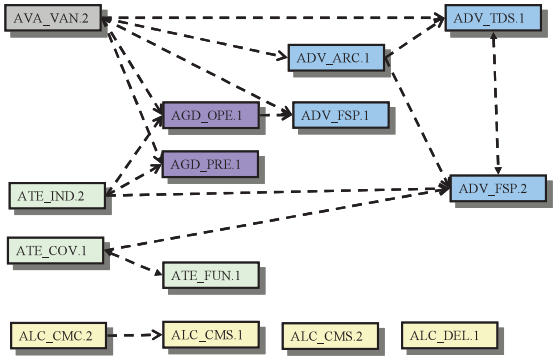

図 6　セキュリティ保証要件の依存関係
Fig. 6　Dependence of security assurance requirement.

件のクラスは，開発工程の各工程に個別に対応している要件や，商品企画から運用開始までの全体を通して適用される要件があり，どの工程でセキュリティ保証要件のどのクラスに対応した開発を行うかは，効率的なセキュリティ設計と評価を進めるうえで重要なポイントになる．図 5 の開発工程とセキュリティ保証要件，および評価エビデンス（各工程での成果物）のリンク付けができると，次にセキュリティ保証要件間の依存関係を整理する必要がある．

一例として，CC V3.1 EAL2 に対応するための開発に関係のあるセキュリティ保証要件の依存関係を**図 6** に示す．

図中の AVA_VAN.2 は，AVA（脆弱性評定）クラスの VAN（脆弱性分析）ファミリの 2 番目のコンポーネントであるという識別子であり，依存関係のある保証コンポーネントが矢印の点線でつながっている．脆弱性分析を行うためには，ADV（開発）クラスで，機能仕様の設計における保証要件を満たし，AGD（ガイダンス文書）クラスで作成されるガイダンス証拠資料を用いる必要があるということを示している．同様に，ATE（テスト）クラスと ADV（開発）クラス，AGD（ガイダンス文書）クラスは依存性が強いセキュリティ保証要件であることが分かる．

以上の分析から，次のことがいえる．

1）AVA_VAN（脆弱性分析）は多くの要件に依存しており，基本設計 → 機能設計 → 詳細設計といった設計の各フェーズで意識する必要があるため，設計終了段階で 1 度分析を行うことで，後戻り作業を減らすことができる．

2）ALC（ライフサイクルサポート）クラスは，EAL2 では，他の要件との依存関係がないた

め，たとえば開発の初期に独立して実施できる．図示しないが，EAL4 において “ALC_TAT.1 明確に定義された開発ツール” は，“ADV_IMP.1 TSF の実装表現” と相互依存関係にある．この場合も実装を行うさいの開発ツールの設定は開発の初期に計画しておくことが望ましい．3）現状の開発環境が，セキュリティ保証要件をどの程度満たしているのかを早期に確認する必要がある．

これらをふまえて，4 章で，セキュリティ保証要件の適合化を実施する順序・プロセスを定義した CC 評価認証のための開発プロセスについて述べる．提案する開発プロセスにより，複雑な保証要件の依存関係を意識することなく，保証要件を満たす証拠資料を作成することが可能となる．

第 2 の課題である「評価認証に必要な証拠資料を効率良く作りたい」を解決するためには，抽象的な表現で書かれている保証要件の内容を噛み砕いて，必要十分な記述を引き出すためのガイドや，要件として必要十分な項目を入力すると自動的に証拠資料を生成し，チェックしてくれるシステムが必要である．

一般的なプロダクトの開発において，要求仕様書や機能仕様書，システム（ソフトウェア，プログラム）設計書，テスト仕様書/成績書，インストールガイド，利用者操作マニュアルのようなドキュメントは通常作成されるため，これらのドキュメントから必要な部分を抽出し，CC 特有の部分を入力することにより，適合する EAL の保証要件を満たす項目の証拠資料を生成するというシステムの仕様が考えられる．

また，CC では開発の最上流工程で ST を定めることが要求されている．2 章で述べたとおり，ST は，プロダクトの種別や機能概要の説明のほかに，守るべき資産と，プロダクトに実装するセキュリティ機能を記載する必要がある．セキュリティ機能は，脅威分析を行い，分析結果の対策方針の実現方法として CC パート 2 のセキュリティ機能要件から必要な要件を選択したうえで，要件を実施する具体的な機能が定義される．ST の生成にはこのようなデータが必要であるが，セキュリティを考慮しないプロダクトでは，脅威分析が行われてないことがままある．そこで，特に ST の生成においては事前にセキュリティの骨子となるセキュリティシナリオを作成すると効率的である．

セキュリティシナリオとは，セキュリティ課題とその対策，実現方法の関係を明確に表現することを目的に作成するものである．具体的には，セキュリティ課題と呼ばれる想定脅威や前提条件に対し，対抗あるいは実現するための対策方針，それら対策方針を具体化した実現方法の 3 つの要素を対応づける．セキュリティシナリオの例を**図 7** に示す．

セキュリティシナリオの作成は，シナリオ作成のガイドラインとこれまでのプロダクト開発の経験などから得られた脅威と対策をノウハウ化した脅威対策リストを用いて，開発者が手作業で行っている．セキュリティシナリオは，以下の手順で作成する．

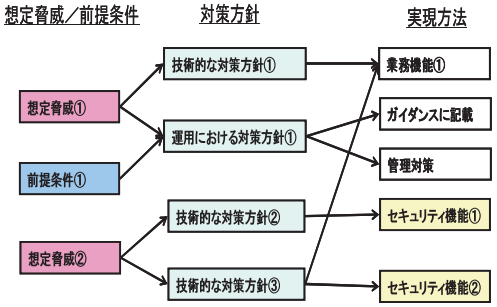

図 7　セキュリティシナリオ
Fig. 7　Security scenario.

- はじめにプロダクトの保護すべき情報資産と関与者を定め，脅威対策リストを用いてその利用環境から想定される脅威を抽出する．
- 次に，想定脅威に対抗するための技術的対策方針や前提条件や遵守すべき組織のセキュリティ方針を実現するための運用・管理的な対策方針を脅威対策リストから選定する．
- 最後に抽出したセキュリティ課題，対策方針，実現方法をそれぞれをトレースできるように図式化する．

セキュリティシナリオを作成することにより，ST に必要なデータの約半分の内容が確定する．セキュリティシナリオの今後の課題として形式知化された脅威対策リストと UML（Unified Modeling Language）の拡張ミスユースケースによる手法[15] などを応用した抽出や分析を取り入れ，証拠資料作成支援システムと連携することを検討したい．

セキュリティシナリオを入力として ST の生成を行うということも証拠資料の自動生成システムに必要な要求仕様である．これらの要求仕様を満たし，第 2 の課題を解決するための証拠資料作成支援システムについて，5 章で説明する．

4. 提案する開発プロセス

4.1 CC 評価認証のための開発プロセス

3.3 節で分析を行った第 1 の課題に対する提案開発プロセスでの対応方針を示す．

1）脆弱性分析は多くの要件に依存している，については，設計実装の工程終了時，それ

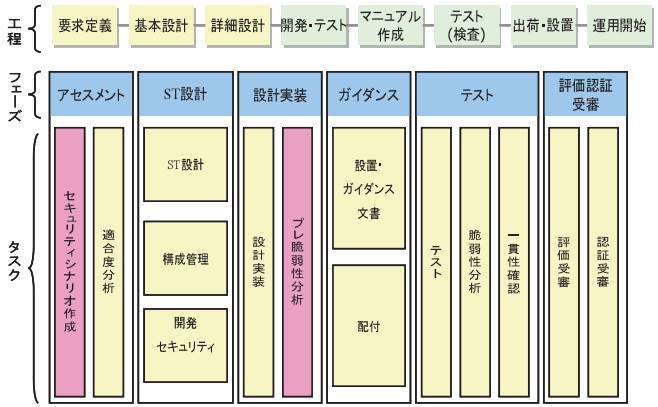

図 8　CC 開発プロセス
Fig. 8　Development process for CC Evaluation.

までの証拠資料を対象に開発者自身で，プレ脆弱性分析を実施する．2）ライフサイクルサポートは，他の要件と独立して実施できる，については，開発の早い段階でルールと仕組みを確立する必要がある ALC クラスは ST 設計と並行して実施する．3）現状の開発環境が，保証要件をどの程度満たしているかを早急に確認する必要がある，については，ST 設計の前に適合度分析を行う．

これらをふまえて，プロダクト開発と並行して CC に適合するための開発プロセスを定義した[9]．

提案する CC 開発プロセスは，EAL1 から EAL4 のプロダクトが，新しいセキュリティコンセプトに基づいている場合や，類似の製品で CC 評価認証の実績が少ない場合に活用することを想定して設計した．提案する CC 開発プロセスは**図 8** に示すように，アセスメントフェーズ，ST 設計フェーズ，設計実装フェーズ，ガイダンスフェーズ，テストフェーズ，評価認証受審フェーズからなり，ウォーターフォール型の開発プロセスに重ね合わせて，CC 評価認証受審のための証拠資料を作成していくようにフェーズが構成されている．

文献 16) などでは，開発ドキュメントの例と評価証拠資料のイメージについて示されているが，提案する CC 開発プロセスのように，具体的に開発のどの工程で CC 開発のためのタスクを実施すればよいのかは示されていなかった．

以下，提案する CC 開発プロセスの特徴的なフェーズとタスクについて述べる．

- アセスメントフェーズ：システムの企画・要求定義の工程と並行して実施し，セキュリティシナリオ作成と適合度分析の作業タスクからなる．セキュリティシナリオ作成タスクでは，プロダクトのセキュリティ機能と利用環境の脅威分析を行い，分析によって抽出された脅威の対策方針を策定することにより，ST の骨子であるセキュリティシナリオを作成する．同時にプロダクトの範囲と評価認証に関わる ALC クラスの対象範囲を明確にする．適合度分析では，選定した EAL に関わるすべてのセキュリティ保証要件の現状とのギャップ分析を行い，分析結果から解決すべき課題へのアクションアイテムと，以降の作業フェーズ全体のボリュームを見積もる．
- ST 設計フェーズ：基本設計の工程と並行して実施し，アセスメントで作成したセキュリティシナリオに基づいて ST 設計を行う．同時に構成管理や開発者によるライフサイクルモデルの仕組み作りやルールの明文化を行い，以降のフェーズで構成管理規程に従った証拠資料の作成と開発環境のセキュリティが確保できるようにする．
- 設計実装フェーズ：詳細設計から開発・テスト工程と並行して実施する．設計実装フェーズで AVA クラスに基づくプレ脆弱性分析を行うが，これは脆弱性の混入を未然に防ぐための設計・実装とテスト仕様を早期に策定し，テストフェーズでの脆弱性分析の規模を想定するためである．
- テストフェーズ：ATE クラスに基づくテストの証拠資料作成は，一般的なプロダクトの場合，試作が完了し，市場に投入する直前の量産品のテスト（検査）段階で実施する．図 5 に示すように，テストは開発と製造時の検査の 2 工程で行われるが，テストに関する証拠資料作成は，量産品のテスト（検査）における問題発生時のゆり戻しを回避し，1 つのタスクで完結するために最終フェーズで行う．

4.2　開発者の課題の分析

提案する CC 開発プロセスを用いて CC 評価認証を実施したプロダクトと，本プロセス適用前に CC 評価認証を行ったプロダクトにおいて，開発期間の違いを比較した．比較に用いたプロダクトは同じ種類の IT 製品で，両者とも CC V2.3 の基準を用いて EAL2 で認証を取得している．比較結果を**表 3** に示す．

提案プロセスを適用したプロダクトでは，適用前の事例に比べて，開発期間が約 1/3，評価に要する期間が約 1/4 程度短縮された．適用事例では，ST 設計の前に骨子となるセキュリティシナリオを作成し，設計・実装フェーズ終了時にプレ脆弱性分析を，検査（試験）工程の後に脆弱性分析とその評価を実施した．これらのタスクは，開発全体での工数は増えるものの，後工程の負担を低減させ，セキュリティ設計の品質を高めている．このため，提案プロセス適用前

表 3　開発期間の比較
Table 3　Comparison at development period.

	適用（月数）	非適用（月数）	効果
開発期間	3.2	5	1/3 短縮
評価期間	3	4.3	1/4 短縮
認証期間	3	3.2	少し縮小

に比べて，開発の各タスクにおける不備や見落としに対する評価者からの指摘事項が少なく，前工程への後戻り作業が低減した．その結果として，開発・評価期間が縮小したと考えられる．

検証結果が示すように，提案プロセスは CC 証拠資料作成の効率向上に効果があるといえる．しかし，効率面だけを重視しているのではなく，一番最初のアセスメントフェーズ，開発時のプレ脆弱性分析といった基準では特に求められていないタスクを実施することで，セキュリティ保証要件に適合していない開発作業の明確化や早い段階での脆弱性のフィードバックを実施できるように，プロダクトと CC 証拠資料の品質の向上も考慮している．

5. 提案する証拠資料作成支援システム

5.1 証拠資料作成支援システム

これまで，証拠資料の作成を支援するシステムは，評価認証済みの ST をデータベース化して新たに作成する ST と似たものを抽出し利用するというアプローチのシステムが提案されている[10),11)]．しかし，これらの作成手法や支援システムは ST のみを対象としたものだけで，ST を基本とするその下流の開発プロセスの証拠資料までカバーする方法やシステムは提案されていない．

3.3 節で分析を行った第 2 の課題である「評価認証に必要な証拠資料を効率良く作りたい」を解決するために，提案する証拠資料作成支援システムは，ST をはじめとする機能仕様書やテスト成績書といった設計，開発での証拠資料を半自動生成する．

CC 証拠資料の作成の効率化を阻む要因として，以下のような課題があった．

- 文書内または文書間での記述内容の関連が強く，1 カ所の変更で複数の記述内容に影響があり，修正漏れが発生していた．
- 複数の開発者により作成される場合，証拠資料間での用語や略語などの不統一や記載内容の抜け・漏れがあった．
- 機能仕様書やテスト成績書など，既存の開発ドキュメントに対し，CC の評価で要求される内容を追加しなければならなかった．

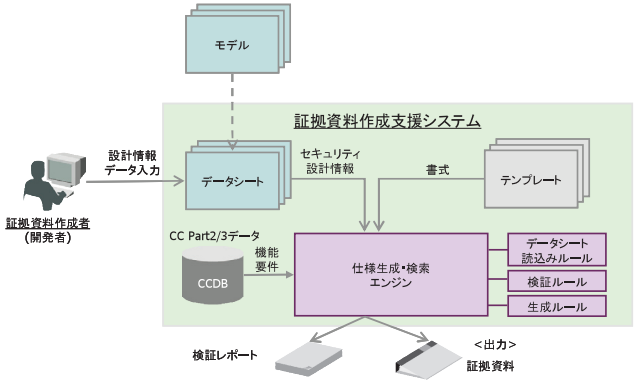

図 9　証拠資料作成支援システム
Fig. 9　Evidence document creation support system.

3 番目の課題は，3 章で分析したシステムの要求仕様の 1 つでもある．

これらの課題と要求仕様に対応するために，提案システムでは，証拠資料における記載項目をモデル化し，その設計仕様を入力する「データシート」と証拠資料の書式となる文書ファイルを「テンプレート」として分離した．提案システムは，以下の特徴を持つ．

- 開発者がデータシートへ設計情報を入力することにより，あらかじめ準備されているテンプレートの書式に従って，証拠資料を生成する．
- 単一の証拠資料内，または複数の証拠資料間の用語や仕様記述の一貫性を検証する．
- データシートにより証拠資料を一元管理する．

図 9 に証拠資料作成支援システムの概要を示す．

証拠資料作成支援システムは，証拠資料のモデルと入力フォームを示したデータシート，CC パート 2，パート 3 のデータを格納した CCDB，証拠資料のテンプレートを入力とし，次の 3 つの機能を持つ仕様生成・検索エンジンで構成する．

- データシートの入力データと CCDB の読み込み機能．
- データの整合性と一貫性を検証し，検証レポートを出力する検証機能．
- テンプレートの書式に基づき証拠資料を自動生成して文書ファイルを出力するドキュメント生成機能．

提案システムでは，CC V3.1 に対応した ST，機能仕様書（FSP: Functional

Specification），アーキテクチャ設計書，テスト仕様書/成績書などの証拠資料ごとにモデルを定義している．ST は，システムの要求仕様であるセキュリティシナリオを入力情報とするモデルとなっている．データシートとデータシート読み込みルール，検証ルールは，保証要件を満たすための項目が網羅されていることが必要であり，CEM と IPA の証拠資料作成・レビュー講座[16] を参照して開発を行った．生成ルールやテンプレートも同様に公開情報や入手可能な証拠資料の構成・目次を参考に開発した．テンプレートの構成や目次と生成ルールについては，証拠資料を作成する開発者ごとに柔軟に対応できる．提案システムのモデルとテンプレートの妥当性は，公開されている CC V3.1 で認証取得している公開 ST と，入手可能なその他の証拠資料を用いて，必要なエラーが検出できるか，手書きの証拠資料と同等の内容を生成できるか，などについて検証を行った．

提案システムの利用手順に沿って，エンジンの機能と各種ルールについて説明する．

開発者がデータシートに入力した設計情報と CCDB，テンプレートをエンジンがデータシート読み込みルールに従って取り込む．

テンプレートにデータシートから読み込む項目の識別子と箇条書きや表形式といった記述書式を示すタグ情報を埋め込むことで，データシートとテンプレートを結び付ける．また，このタグ情報は，テンプレート以外にも，既存の設計ドキュメントに追加することも可能であり，既存の設計ドキュメントに不足の CC で要求されている内容を簡単に追加できる．

テンプレートは，CC 評価で求められるセキュリティ保証要件に適合した内容と目次で構成されており，開発者が必要な設計情報をデータシートに入力するだけで，テンプレートに沿ったドキュメントが生成される．これにより，開発者によらない均質な証拠資料を生成することが期待できる．

次に，エンジンは読み込んだ設計情報を検証ルールに従ってチェックする．検証ルールは，用語や識別子の定義漏れや重複はないか，命名規則にマッチするか，定義されていない項目を引用していないか，などをチェックする．システムは検証結果を検証レポートとして示す．検証レポートの例を**図 10** に示す．

この例は，「SF. 識別認証機能」というセキュリティ機能の実現方法として，FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FMT_SMR.1 の 4 つのセキュリティ機能要件（SFR）が必要であるというセキュリティシナリオがデータとして入力されているが，「SFR の実現方法」記述欄に FIA_UAU.2 に関する記載漏れがあるということをエラーとして検出した，という内容である．

このように検証機能では，人間が気づきにくい識別子の不一致や記載洩れといった記述ミスを，機械的なチェックにより開発者に提示することで，記述ミスを自動的に排除し，レビューや評価の効率を上げることができる．

SF.識別認証機能

★エラー	SFRの実現方法に、SFR[FIA_UAU.2]が含まれていません
クラス	SF
Excel	STデータシート.xls#'TSS'!A4..D4
SFRの実現方法	FIA_vvUAU.2を実現するには、利用者を代行する顧客情報DBアプリ(サーバ)のセッションの利用を許可する前に、各利用者に認証を要求すればよい。 SF.識別認証機能は、顧客情報DBアプリ(サーバ)のセッションを生成する前に、利用者としての認証を要求している。 FIA_UAU.7を実現するには、パスワードの入力時に入力されたパスワードの文字数だけを利用者に提供すれば良い。 SF.識別認証機能は、パスワードの入力時に入力されたパスワードの文字数だけを利用者に提供する。 FIA_UID.2を実現するには、利用者を代行する顧客情報DBアプリ(サーバ)のセッションの利用を許可する前に、各利用者に識別を要求すればよい。 SF.識別認証機能は、顧客情報DBアプリ(サーバ)のセッションを生成する前に、利用者としての識別を要求している。 FMT_SMR.1を実現するには、利用者を代行する顧客情報DBアプリ(サーバ)のセッションを管理者或いは担当者に関連付け、役割を維持すればよい。 SF.識別認証機能は、OSでの識別認証成功時に利用者を代行する顧客情報DBアプリ(サーバ)のセッションを管理者或いは担当者に関連付け、役割を維持している。
識別子	SF.識別認証機能
対応SFR	• FIA_UAU.2 • FIA_UAU.7 • FIA_UID.2 • FMT_SMR.1
対応TSF	• TSF.識別認証機能

図 10　検証レポートの例
Fig. 10　Case with verification result.

ドキュメント生成機能は，生成ルールに従って，テンプレートのタグ情報の位置に仕様間の対応分析表や，仕様の一覧表を自動生成し，文書ファイルとして出力する．**図 11** に生成された ST の例を示す．

この例の記述を生成するデータシートの内容は，「保証レベル」の項目に [EAL1] と記入するだけであり，テンプレートは以下のようになっている．

```
6.2. セキュリティ保証要件

[spec:保証要件]
[spec:SAR 一覧]
```

[spec:保証要件] はタグ情報であり，生成ルールの以下の記述に従って生成される．

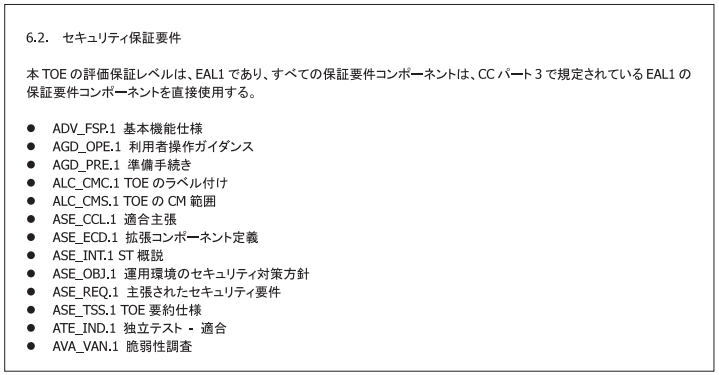

図 11　生成された ST の例
Fig. 11　Case with security target.

Doc.makeText(”本 TOE の評価保証レベルは，[spec:仕様:保証レベル:内容] であり，すべての保証要件コンポーネントは，CC パート 3 で規定されている [spec:仕様:保証レベル:内容] の保証要件コンポーネントを直接使用する．¥n”)

[spec:SAR 一覧] は，CCDB の SAR（セキュリティ保証要件）から [保証レベル:EAL1] のコンポーネントを抽出して生成する．

5.2　証拠資料作成支援システムの提要評価

ST と FSP をターゲットとして，提案する証拠資料作成支援システムの適用評価を行った．

ST に関しては，CC 証拠資料作成に関して経験の少ない開発者が，提案システムを用いて ST を作成した場合と，提案システムを用いずに設計ガイドのみで ST を作成した場合の作業工数の比較評価を行った．ST は同じプロダクトについて，EAL1 プロトタイプ型機能特定保証に適合する内容で作成した．

その結果，提案システム利用時の作業時間が設計ガイドのみに比べて約 1/3 に減少し，効率化が図れていることが分かった[12)]．

今回我々は，FSP に関して同じ保証要件レベルの 2 つのプロダクトで，提案システムを用いて FSP を作成した場合（プロダクト A）と，提案システムを用いずに FSP を作成した場合（プロダクト B）で，作成期間，FSP のボリュームの観点から効率化についての評価を行った．

FSP 作成手順は，両プロダクトとも，はじめにセキュリティ機能，その他の機能，インタフェースを抽出しそれらのつながりの分析を行い，FSP で要求される「インタフェースに関する詳細記述」を入力/作成し，レビュー・修正を行うという同じ作業ステップを踏んだ．**表 4** にそれぞれのプロダクトの FSP 作成に関する比較値を示す．

表 4　FSP 比較値
Table 4　FSP comparison value.

プロダクト		A	B
インタフェース数		11	14
セキュリティ機能数		10	8
その他の機能数		11	14
FSP 頁数		28	47
作成期間（週数）		2	5
作成期間内訳 (週数)	分析	1	1
	入力／作成	0.5	1
	レビュー・修正	0.5	3

表 4 に示すように，提案システムを用いたプロダクト A の作成期間は，プロダクト B の約 1/3 であり，特に FSP のレビュー・修正期間が大幅に短縮されている．

2 つのプロダクトはインタフェース数や機能数に大きな差はなく，1 人の開発者が文章を作成するとプロダクト B のように約 1 カ月かかってしまうが，提案システムを用いたプロダクト A では約半分の期間でデータシートへの入力が行える．レビュー・修正期間の短縮は，FSP 内，および FSP と ST との用語や識別子の一貫性チェックや，定義していない項目を引用していないかなどの検証が，目視によるチェックから自動化されたことで，修正作業が効率化されたのではないかと考えられる．

プロダクト A の FSP については，ST 確認制度を適用する情報システムとして評価を受審しており，提案システムが実用に耐えうることが確認できた．

提案システムの適用評価として，ST と FSP の効率化について論じてきた．開発者が証拠資料をガイドやテンプレートに基づいて記述していく場合に比べ，データシートに設計仕様を入力するだけで，証拠資料内，複数の証拠資料間の一貫性や抜け・漏れのチェックと生成が行えるシステムを用いることで開発の効率が図れることが分かった．しかし，今回の適用評価は，ST と FSP 単独での提案システムを用いた場合とそうでない場合の比較だけであり，開発の証拠資料全体を通した検証が実施できなかった．ST からテスト成績書までの一貫性と効率化に関する検証が，今後の課題である．

また，現状の提案システムは，ASE，ADV，ATE といった設計系の保証要件クラスの証拠資料作成を支援しているが，ALC や AGD といった管理系要件クラスについては未対応

である．今後は管理系の保証要件へも対応できるように拡張を検討したい．

6. おわりに

本稿では，CC や CEM で難解とされるセキュリティ保証要件の依存性を整理し，製品開発の工程とリンクさせて評価の過程で後戻りが起きにくい効率的なセキュリティ証拠資料作成順序を CC 開発プロセスとして構築した．

また，セキュリティ保証要件で必要とされる項目を入力することで証拠資料を半自動生成する証拠資料作成支援システムを開発した．これらの開発プロセスとシステムを実際のプロダクトに適用して評価を行った結果，導入前に比べて開発期間が短縮されたという結果が得られた．

ただし，証拠資料の複雑度は TOE 規模と EAL に比例して増していくため，機械的なチェックには対応できるが，非形式記述である文章の意味に関しては開発者，評価者で対応するしかない．提案システムは，レビューの正確さ，効率化に寄与するための方法論やシステムになっていないため，これらの方式の検討も行っていきたい．また，今回適用評価を行ったプロダクトは，EAL1 と 2 であったため，EAL の違いによる問題点や課題は把握できていない．今後は，EAL3，4 での事例の収集が必要である．

本稿で提案した CC 開発プロセスと証拠資料作成支援システムをさらに検証，改良し，CC 評価認証を行うプロダクトに適用することで，セキュリティ品質を向上させ，CC 評価認証の裾野を広げることにつなげていきたい．

参考文献

1) CC v3.1 Part 1: Introduction and general model.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R2.pdf
2) CC v3.1 Part 2: Security functional requirements.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf
3) CC v3.1 Part 3: Security assurance requirements.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf
4) CEM. http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf
5) 政府機関の情報セキュリティ対策のための統一基準.
http://www.nisc.go.jp/active/general/kijun01.html
6) ST 確認制度．http://www.ipa.go.jp/security/jisec/st_confirmation/index.html
7) 産業競争力のための情報基盤強化税制.
http://www.meti.go.jp/policy/it_policy/zeisei/index.html
8) 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
9) 斯波万恵，佐々木尚一，吉井大吾，石田貴久，小田原育也，島田　毅：ISO15408 評価認証におけるセキュリティ開発プロセス支援方法，*CSS2006* (2006).
10) ラミレス・カセレス・ギジェルモ・オラシオ，勅使河原可海：国際標準に基づいたセキュリティターゲット作成のナレッジデータベース，*CSS2005* (2005).
11) 堀江大輔，後藤祐一，程　京徳：情報セキュリティ工学データベースシステム ISEDS の API の実現と応用，FIT2007 予稿集，D-023 (2007).
12) 斯波万恵，佐々木尚一，石田貴久：セキュリティ設計仕様書の課題と設計支援方法の提案，*SCIS2008* (2008).
13) IPA：セキュリティ評価の実際，IT セキュリティ評価認証及び認証セミナー.
http://www.ipa.go.jp/security/jisec/documents/sm200410_3_mhir.pdf
14) IPA：日立認証局システム Enterprise Certificate Server Set による ISO/IEC 1408 認証取得について，IT セキュリティ評価認証及び認証セミナー.
http://www.ipa.go.jp/security/jisec/documents/sm200410_5_4_hitachi.pdf
15) 前富　博，大久保隆夫，田中英彦：拡張ミスユースケース図を利用した既存システムのセキュリティ更改要件抽出/分析手法，*CSS008* (2008).
16) IPA：評価証拠資料作成・レビュー講座.
http://www.ipa.go.jp/security/jisec/apdx/documents/cc_eval_20061121.pdf

(平成 20 年 12 月 1 日受付)
(平成 21 年 6 月 4 日採録)

斯波　万恵

1962 年生．1986 年岡山理科大学理学部基礎理学科卒業．同年株式会社東芝入社．現在，東芝ソリューション株式会社 IT 技術研究所情報セキュリティラボラトリー研究主務．暗号実装技術，情報セキュリティ評価技術およびセキュリティ要求工学の研究開発に従事．電子情報通信学会員．

佐々木尚一（正会員）

1966 年生．1985 年株式会社東芝入社．現在，東芝ソリューション株式会社 IT 技術研究所情報セキュリティラボラトリー研究主務．セキュリティ構築技術，セキュリティ評価技術の研究開発に従事．ISO/IEC JTC 1/SC 27/WG 3 小委員会委員．