# コモンクライテリアにおけるセキュリティ要求の規定の現状と課題

金子 浩之
みずほ情報総研(株) 情報セキュリティ評価室

IT セキュリティ評価の国際標準であるコモンクライテリア（CC：Common Criteria．ISO/IEC15408 と同義）は，開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定したものであり，主にエビデンス評価とテスト評価を実施する際の視点でまとめられている．一方，セキュリティ保証を製品やシステムのライフサイクル上で継続して実現するためには，脅威事象や個別要求の変化に応じて対策を講じていく必要がある．本稿では，CC に基づく評価を実施する立場から，製品やシステムの開発・保守におけるセキュリティ保証の現状課題を概説し，CC に準拠した保証活動のなかで，開発現場において要求分析を効果的に適用するための方向性について述べる．

## コモンクライテリアとは

今日の情報システムは，従来では達成できない業務課題をも解決する手段として大いに期待されている．その一方で，情報システムにかける投資の費用対効果は，企業経営においても，行政運営にとっても重要な関心事である．そのため，標準化されたオープンなネットワークや IT コンポーネントをできるだけ有効活用することで，許容されるコスト，期間内で情報システムを構築し，これを効果的に運用することが求められる．情報システムを複数のコンポーネントの統合により実現する際には，システム化を求める機能性以外にも，品質特性，性能特性，運用性などの非機能的な特性が求められ，その分析，設計が重要となる．セキュリティ要求は，これらの非機能要求の一部と考えられる．たとえば，システムで扱う重要な情報を資産と捉え，その特性に合わせて秘匿性，完全性，プライバシーなどを求める要求や，いつでもそのシステムサービスを提供し続ける可用性の要求など，情報システムを意図した目的で運用する際の妨げとなるリスクを低減もしくは除去するために，セキュリティ要求が規定される．これらのセキュリティ要求のうち，IT を使って実現する部分（セキュリティ機能を含む）を開発する場合，その開発した部分の信頼性が保証されていることを評価するための国際標準が CC である．特に，技術面でのセキュリティ要求とその責任所在が明確な部分が存在し，ここにターゲットを絞ってセキュリティ要求が満たされることを，その責任主体が保証したい場合に，CC の適用効果が高まる．

CC の規格文書[☆1]は 3 つのパートで構成されている．

- パート 1：概説と一般モデル
  評価対象（TOE：Target of Evaluation）と運用環境を正確にモデル化し，資産（Asset），脅威（Threat）および対抗策（Objective）によるセキュリティの概念と関係に基づいて，TOE のセキュリティ機能要件（SFR：Security Functional Requirement）とセキュリティ保証要件（SAR：Security Assurance Requirement）に関する評価の枠組みをセキュリティターゲット（ST：Security Target）として定義すること，および ST に基づく TOE 評価の一般モデル
- パート 2：セキュリティ機能コンポーネント
  セキュリティ機能要件の全体像（パラダイム），11 のクラスからなる機能要件のカタログ情報
- パート 3：セキュリティ保証コンポーネント
  セキュリティ保証のアプローチに関する全体像（パラダイム），評価保証レベル（EAL：Evaluation Assurance Level）の定義，ST やプロテクションプロファイル（PP：Protection Profile．特定の製品種別に対するセキュリティニーズについて，実装に依存せず，ST の雛形として用いることができる構成でまとめた文書）を含む 8 クラスからなる保証要件のカタログ情報

また，CC に基づく評価方法論を示す CEM[☆2]と呼ばれる規格文書があり，評価者は，ST で定義された評価保証レベルの保証コンポーネントに対し，CEM に定義さ

☆1「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」．現在のバージョンは CC Ver3.1 Revision2.
☆2「情報技術セキュリティ評価のための共通方法」 現在のバージョンは CEM Ver3.1 Revision2．ISO/IEC18045 と同義．

れるより詳細な評価単位であるワークユニットごとに評価を行う．

## コモンクライテリアに基づく保証と評価

情報システムが要求する重要なセキュリティ機能性を実装するためには，この機能性を持つ汎用製品をコンポーネントとして活用してシステムを組むことが多い．そこで，これらの製品の開発者に対し，所定の要求を満たすセキュリティ機能性やセキュリティ保証に関する信頼性の確保を求めるために，各国でITセキュリティに関する第三者による評価・認証制度の整備が進んでいる．日本では「ITセキュリティ評価及び認証制度」（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）が運用される．また，各国評価・認証制度の認証結果を認め合うCC相互承認協定（CCRA：CC Recognition Arrangement）により，自国認証以外の幅広いCC認証済み製品の国際相互流通を可能としている．CC認証済み製品としては，OS，DBMS，ファイアウォール，ネットワーク関連コンポーネント，データ保護メカニズムを持つコンポーネント，アクセス制御ミドルウェア，認証コンポーネント，スマートカード，セキュリティを重視するLSIなど，多くの分野の1000を超える製品が各国認証制度のWebサイト等でリストされている．これらの分野の主要製品の多くは，すでに一度はCC評価・認証を経験している．なお，評価者は，セキュリティ保証の実務に関する豊富な経験と評価ノウハウを有し，かつ制度から認められた組織（認定された評価機関）に属し，中立公平な第三者の立場から，設計評価，試験評価，侵入検査などを含むセキュリティの評価を実施する．

ここでは，CCに基づいた評価を受ける製品開発者から見た典型的なCCの適用例を示す．

CCやCEMの規格文書は，評価を行う側の視点で記述されている．また，パート2セキュリティ機能要件やパート3セキュリティ保証要件の文脈は，開発者の通常の理解よりも抽象的な表現で示されている．そこで，製品開発者は，CCやCEMの規定を開発者側への要求事項として読み替え，対象製品へのCC適用を行う場合の具体的な実施事項を検討し，CCに基づく保証の対応方針を明らかにする．その上で，以下に示すアプローチで，製品セキュリティの特性と構造の記述を，自然言語でSTとして作成することから開始する．

(1) 利用者視点で製品に求められるセキュリティ要求を収集整理する．適用すべきPPがあれば，その内容を分析する．そのほか，製品戦略上，重要と位置付けたセキュリティ要求についても検討する．これらを踏まえ，製品セキュリティのコンセプトを定義する．

(2) 評価の効果と保証の実施可能性を踏まえ，評価対象の範囲とEALを定める．

(3) 保護対象とする資産に関する脅威モデルを定義・分析し，想定する特定の運用環境における対抗策を定義する．定義した脅威と対抗策の関係は，この製品を採用する利用者が納得できる論理構造となっていることを確認する．

(4) 評価対象にてITメカニズムとして対抗策を実現するための機能要件を，パート2からの機能要件の選択，拡張により定義する．

(5) 機能要件を評価対象においてどのような機能として実現するかの要約を仕様化する．

(6) これらの検討結果を踏まえ，**図-1**にあるST文書の構造通りに記述する．

STを作成したのち，EALの定義にしたがった個々の保証コンポーネント（開発，ガイダンス文書，ライフサイクルサポート，テストの各クラスのうち，設定されたEALで満たすべき保証コンポーネント．**図-2**にCCパート3で定義する保証コンポーネントの構成を示す）が要求する評価エビデンスや，評価者がセキュリティ機能のテストや侵入検査を実施するためのテスト環境を準備する．脆弱性評定クラスに対しては，開発者が準備するエビデンスはテスト環境以外に存在しない．ただし，EALのすべての保証コンポーネントを満たすことを主張するためには，評価を受ける前に，顕在化する脆弱性が存在しないことを確認しておく必要がある．具体的には，最初に評価対象の動作に影響を与える公知の脆弱性情報を収集する．次に，評価対象の仕様や設計・開発の過程で脆弱性が組み込まれる可能性がある部分を洗い出し，これらの脆弱性が評価対象において対策済みであることを確認する．また，必要に応じて脆弱性の残存有無を確認するために，開発者自身による侵入検査を実施することが望ましい．

このように，STをはじめ，評価エビデンスの最終内容は，ライフサイクルサポートの一部のエビデンスを除き，開発が完了し出荷対象となるTOEを対象とした，完成されたものである必要がある．CCの評価においては，セキュリティの要求獲得・記述・分析フェーズのエビデンスは求められない．一方，製品の導入を検討する利用者は，その利用者のニーズに合った製品構成であり，意図する使い方が可能かどうかの確認のみでなく，ある特定の脅威への対抗策を具備しているかなど，個別のセキュリティ要求についても確認するかもしれない．また，利用者の想定する運用環境において，その製品がこれらのセキュリティ要求を満たすことが検証済みであることを期待するかもしれない．これらの確認は，STを拠り

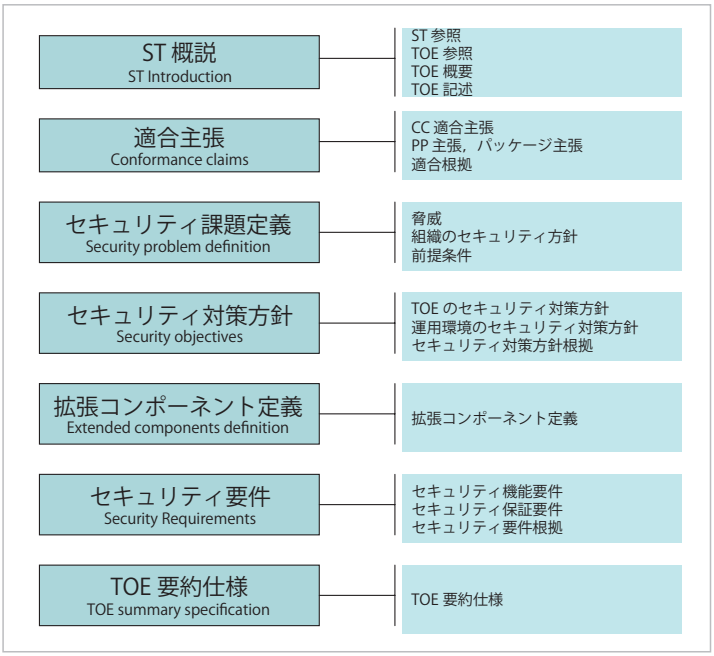


図 -1　ST の構造（CC パート 1 より）

| 保証クラス | 保証ファミリ | 省略名 | 評価保証レベル（EAL）／保証コンポーネント | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| ASEクラス | ST概説 | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| セキュリティターゲット評価 | 適合主張 | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | セキュリティ課題定義 | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 |
| | セキュリティ対策方針 | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | 拡張コンポーネント定義 | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | セキュリティ要件 | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | TOE要約仕様 | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ADVクラス | セキュリティアーキテクチャ | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 |
| 開発 | 機能仕様 | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 |
| | 実装表現 | ADV_IMP | | | | 1 | 1 | 2 | 2 |
| | TSF内部構造 | ADV_INT | | | | | 2 | 3 | 3 |
| | セキュリティ方針モデル化 | ADV_SPM | | | | | | 1 | 1 |
| | TOE設計 | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 |
| AGDクラス | 利用者操作ガイダンス | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ガイダンス | 準備手続 | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ALCクラス | CM能力 | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| ライフサイクルサポート | CM範囲 | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 |
| | 配付 | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 |
| | 開発セキュリティ | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | 欠陥修正 | ALC_FLR | | | | | | | |
| | ライフサイクル定義 | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 |
| | ツールと技法 | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| ATEクラス | カバレージ | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| テスト | 深さ | ATE_DPT | | | 1 | 2 | 3 | 3 | 4 |
| | 機能テスト | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | 独立テスト | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| AVAクラス　脆弱性評定 | 脆弱性分析 | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 |

図 -2　EAL と保証コンポーネントの相互参照（CC パート 3 より）

所として行われることから，ST を作成する際には，利用者の検討候補となり得る評価対象の構成や，想定する運用環境に合致した検証環境を特定することが不可欠である．CC 評価では，ST に定義された内容が，その製品の導入を検討する利用者からみて，評価範囲や評価したセキュリティ機能について誤解を生じることがない記述かどうかの観点からも検査する．

## セキュリティ保証における課題

CC に基づく評価では，最初に ST を検査し，ターゲットとする TOE の範囲の確認，および主張するセキュリ

ティ構造の妥当性（開発者側が想定した妥当な脅威，この脅威に対抗するための対策，対策のために必要となるセキュリティ機能要件，機能要件を実現するための仕様の要約，について各々の相互関係の完全性および正当性）を評価する．その後，EAL で指定された範囲の開発（ADV）クラスを始めとするその他保証コンポーネントの評価を行う．これまでの CC の評価実務の経験から，開発者の多くは，セキュリティ要件定義に至るセキュリティ構造分析を，要求獲得・記述・分析のフェーズで実施する例は少ない．多くの場合，仕様設計の段階もしくは実装設計の段階において ST を作成し，必要な設計フィードバックをかける方針で進める例が多い．このこと自体が，CC の要求を満たしていないということではないが，セキュリティの要求分析や要求管理が適正なタイミング，方法で行われないことで，本来，上流工程で対応されるべき問題（要求との不一致や仕様バグ等）が残留するおそれがある．以下では，製品の開発現場において，セキュリティ要求の規定に関連した CC 対応の現状の課題とその要因を示す．

### ◆ CC 導入段階

CC の導入段階では，開発者は初めて ST を作成することが多く，ST の定義内容の内部一貫性の欠如や，開発エビデンスとの対応の不整合が起こりやすい．CC は図 -1 の ST の構造と記述内容を規定しており，TOE で扱う脅威，対策，セキュリティ要件について，論理矛盾のない識別単位で構成し，それぞれの構成要素の簡潔明快な説明（CC ではステートメントと呼ぶ），および完全性，正当性に関する根拠を自然言語で記述することを求めている．ただし，CC は ST を作成するための元となる要求分析や脅威分析の手法を定めていない．また，評価すべき対象とするセキュリティ要件について，PP や市場要求を踏まえ，要件の取捨選択等の現実的な調整が必要となる．しかしながら，実際には，開発者は，製品の仕様要求，セキュリティ要求，および CC で評価するセキュリティ要求間の対応関係や論理構造を分析・管理・共有する手段を持たないケースが多い．これが ST 定義の不整合や，ST 作者以外の設計者が担当する開発エビデンスの対応不整合の原因となる．

### ◆ CC 認証製品の維持・機能拡張段階

CC 認証を得た製品に対し，ユーザからの機能拡張や変更の要求などに対応する場合，CC 評価・認証制度では，更新された製品は CC 認証済みの TOE とは異なるものとして識別しなければならない．ただし，ST のセキュリティ構造に変更がなく，TOE の構成も変更がない場合は，開発者による影響分析結果を認証機関が精査し，保証の継続（認証済みと同等であることの証明）を認める措置が可能である．一方，セキュリティ要求の変更を伴う場合，その変更要求に伴う新たなセキュリティ要求の獲得や関連要求への影響を把握し，対応に漏れのないことの保証が必要となるが，自然言語で書かれた ST の更新ワークのみでは，分析ツールとしての能力は低く，不完全な修正となる可能性が高い．また，その不備を ST やエビデンスのレビューにより発見することは場合によっては困難である．保守フェーズを含めた製品ライフサイクル全体に対する一貫した要求管理の手段が不十分であり，脅威事象や個別要求の変化への対応に関する分析が不完全となるおそれがある．

### ◆ CC 認証製品のモデル展開段階

CC 認証を得た製品の開発ドキュメント・ソースコードなどの中間生成物をコンポーネントとして活用して，類似製品等の新製品を企画検討する場合，新製品のセキュリティ要求の検討において，この活用するコンポーネントで実現するセキュリティの効果，影響を分析する必要がある．既存製品において，それを構成する特定のコンポーネントが CC により評価済みであっても，新製品でどのようにこのコンポーネントを適用しているのか，この適用方法を含むアーキテクチャとしての漏れや問題はないかどうかを注意深く確認する必要がある．このようなケースにおいては，要求の整合をモデル上で確認することが望ましい．過去の ST を流用し，その書き換えのみでセキュリティ要求の確認を行う場合，十分な検討が行われず，脅威や脆弱性を残してしまう可能性がある．

### ◆要求工学の実務適用の状況

文献 1）では，ソフトウェア製品の開発にかかわる実務者の意見などが分析され，要求工学の実務適用上の課題が挙げられているが，ここには，CC 対応時の要求工学手法の取組みにおいても有効と考えられる点が指摘されている．要求工学的なアプローチを実務で活かすためには，実効性のある手法やツールを整備するとともに，実プロジェクトとして適用可能なドメインを見極めるための効果測定方法を含む実証研究が望まれる．また，要求工学の適用範囲について要求定義局面の領域にとどまらず，開発プロセス全体へ展開するための具体的かつ実践的な手法が求められている．現時点では，CC の要求記述・分析に対して最適化した方法論やサポートツールは整備されているとはいえない状況であるが，CC 認証を取得した製品において，モデル検査や形式手法を用いた仕様検証を行って効果を得た事例も出ている [2]．

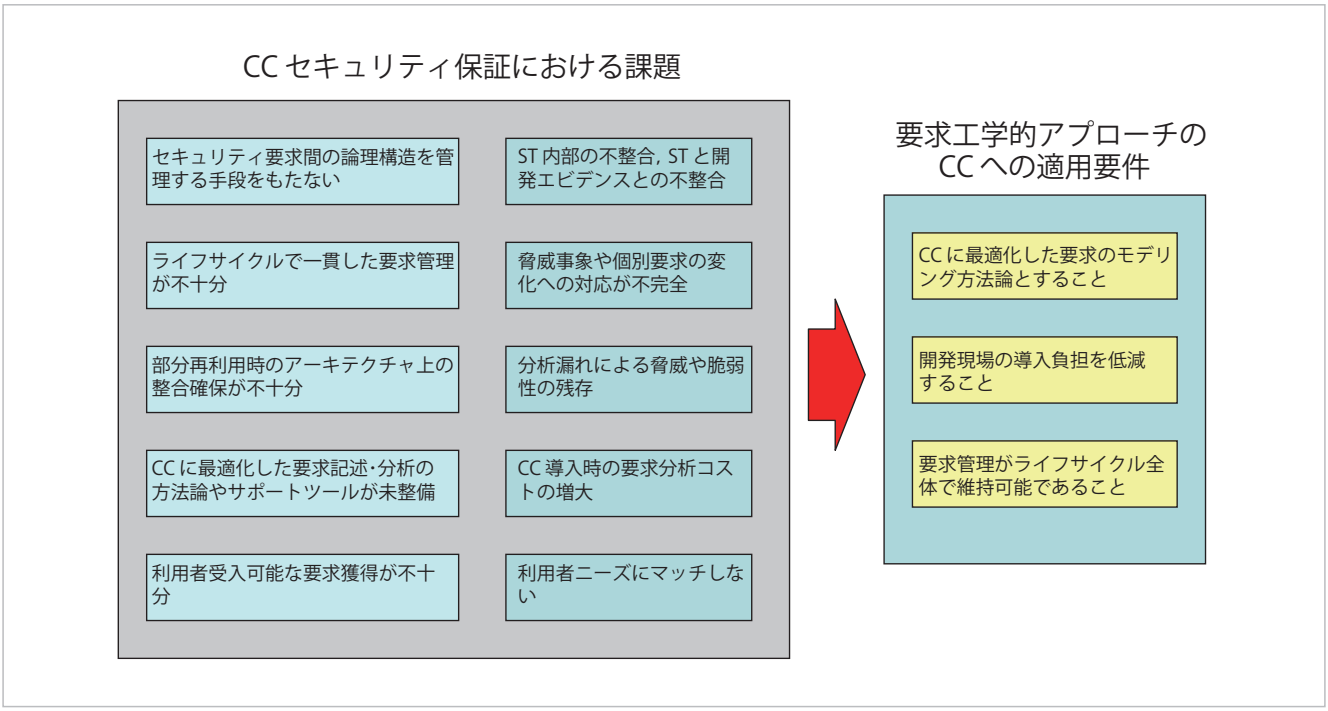


図 -3　CC によるセキュリティ保証の課題と要求工学的アプローチの適用要件

### ◆利用者視点を考慮した要求獲得・分析

CC に基づき第三者評価を行う評価機関では，対象製品のセキュリティ保証状況を評価する際，客観性や評価の再現性を意識した評価プロセスを導入している．ここでの CC 評価実務において，製品の導入を検討する利用者（消費者）の受け入れ条件・要求について，開発者側の理解が不十分なケースが見受けられる．CC は，ST に対して，消費者が確認する際に TOE の範囲，運用環境をはじめ，評価が行われたセキュリティ機能について誤解を与えない正確な記述を要求している．昨今の製品開発は高度に専門分化され，要求獲得・記述が開発者視点で行われる傾向があり，利用者視点での非機能要件の検討が ST 作成に必ずしも反映されていない．そのため，要求の獲得に漏れが生じ，利用者ニーズの取り込みが不十分なケースが存在する．

## 要求工学的アプローチのセキュリティ保証への適用の方向性

このような CC の保証とセキュリティ要求分析に関する現状の課題，および CC に基づいたセキュリティ保証活動の実効性を高めるためにセキュリティ要求分析がどのように適用されるべきかについての方向性を以下に示す（**図 -3**）．

**(1) CC に最適化した要求のモデリング方法論とすること**

CC では ST に基づいて保証を主張することが原則であることから，CC のセキュリティ構造とモデルの構造との対応関係，および表現における親和性は必須要件である．TOE が満たすべきセキュリティ要件は，保護すべき資産と脅威の関係をベースとしたモデル化が必要である．ただし，ST は設計書ではなく評価のための定義書である．CC に基づいて評価できることが重要であり，セキュリティ要求仕様の全体と完全に一致する必要はない．一方，利用者が自身の要求を満たすことが確認できるレベルの正確なステートメント表現が求められ，ST 上の識別ラベルを使って表現できると分析の効率性が高まる．また，モデリング方法論は，開発エビデンスとの対応関係を維持するために，製品仕様の分析モデルと相互参照可能であると開発エビデンスとの対応がとりやすく CC の適用のトータルコストが削減できる．

**(2) 製品開発現場での導入に負担が少ないこと**

要求分析の方法論は，過度なコストをかけることなく製品開発現場に導入できる必要がある．ここでのコストとは，方法論の理解・習得にかかる教育コスト，方法論を実現するサポートツールの操作性，コミュニケーションやネゴシエーションに要する総時間，製品設計・開発に対するインパクト（効果または負担）に伴うコスト，知識移転に要するコストなどを想定する．

**(3) 要求管理が製品ライフサイクル全体で維持可能であること**

製造者の責務範囲で行う実際のセキュリティ保証は，製品ライフサイクル全体が対象となる．初期の製品化範囲のみでなく，脅威事象の変化に対応する TOE の修正，機能拡張などの製品仕様の変更などに伴うセキュリティ

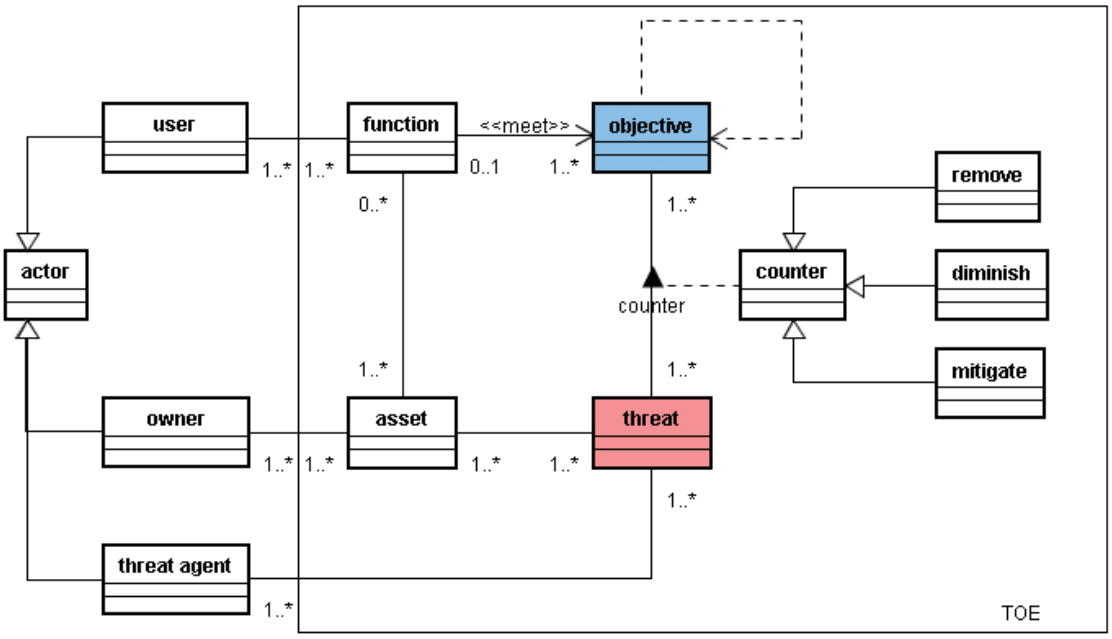


図 -4　ST の概念を用いたメタモデル（一部分）のクラス図

要求の更新情報を維持し，対応すべき保証の影響個所を正確に把握するために，要求モデル記述の修正と分析を繰り返し実行でき，開発フェーズ間のモデルのトレーサビリティを保つ必要がある．そのため，製品の企画・開発・保守・廃棄のプロセス全般において，モデルの一貫性が維持できるように管理する必要がある．

## UML 拡張適用の方向性

CC との親和性を意識したモデリング手法として，UML（Unified Modeling Language）を拡張する場合の例を示す．UML を用いる利点としては，開発現場においてすでに広く利用されているため，導入コストがかからないこと，拡張に対して柔軟性を持ち，かつ視覚的にも理解しやすく，分析におけるコミュニケーションが容易であることが挙げられる．このモデリング手法により製品の持つセキュリティ機能（function）と資産（asset）の観点からそれに対する脅威と対策を分析し，明示的にモデル化することが可能となる．

**図 -4** のメタモデルはミスユースケース図[4] を拡張して CC との親和性を考慮した分析手法の一部分である．また，**図 -5** は，CC 認証実績の多い複合型プリンタ（MFP：Multi Function Peripheral）の一般的な機能に対してこの分析手法を適用した簡単なミスユースケース図の例である．ここでは，CC 認証の申請者が，セキュアな印刷機能を function として主張したい場合を例に説明する．セキュアな印刷機能とは，利用者が印刷等の目的で MFP に格納した文書を他の利用者の不正な閲覧から保護できることと仮定する．この仮定に従い，保護したい asset は MFP に格納される「機密性のある文書」となる．またここでは説明のため，ユーザ A を正当な利用者（user）とし，ユーザ B をユーザ A の文書を不正に閲覧しようとする攻撃者（threat agent）と仮定する．

このとき，ユーザ B による「機密性のある文書」に対する脅威（threat）を考えると，ユーザ A になりすましての不正な文書へのアクセスが考えられる．次にその脅威に関する機能的な対策（objective）として利用時のユーザ認証を行うこととし，対応する脅威に結びつけ，さらに脅威に対してどういった効果があるのかを実線のステレオタイプとして記載する．この対策により脅威は軽減されるが，新たにユーザ認証に用いるユーザ ID，パスワード等の機密情報の不正入手が懸念される．それにより新たな Asset として「ユーザ情報」が分析対象となり，同様に asset に対する脅威，脅威に対する対策を考察する．今回は説明を省略するが，次の分析段階では objective を満たすために function へ実装すべきセキュリティ機能の要件（SFR）を，CC パート 2 に照らし合わせて分析する（**図 -6**）．

図 -5 は簡単な例ではあるが，明示的にモデル化されていて，threat に対する objective，threat がどの asset に対するものかなどが一般的な ST を参照する場合に比べ容易に認識できる．また一般的な ST では困難

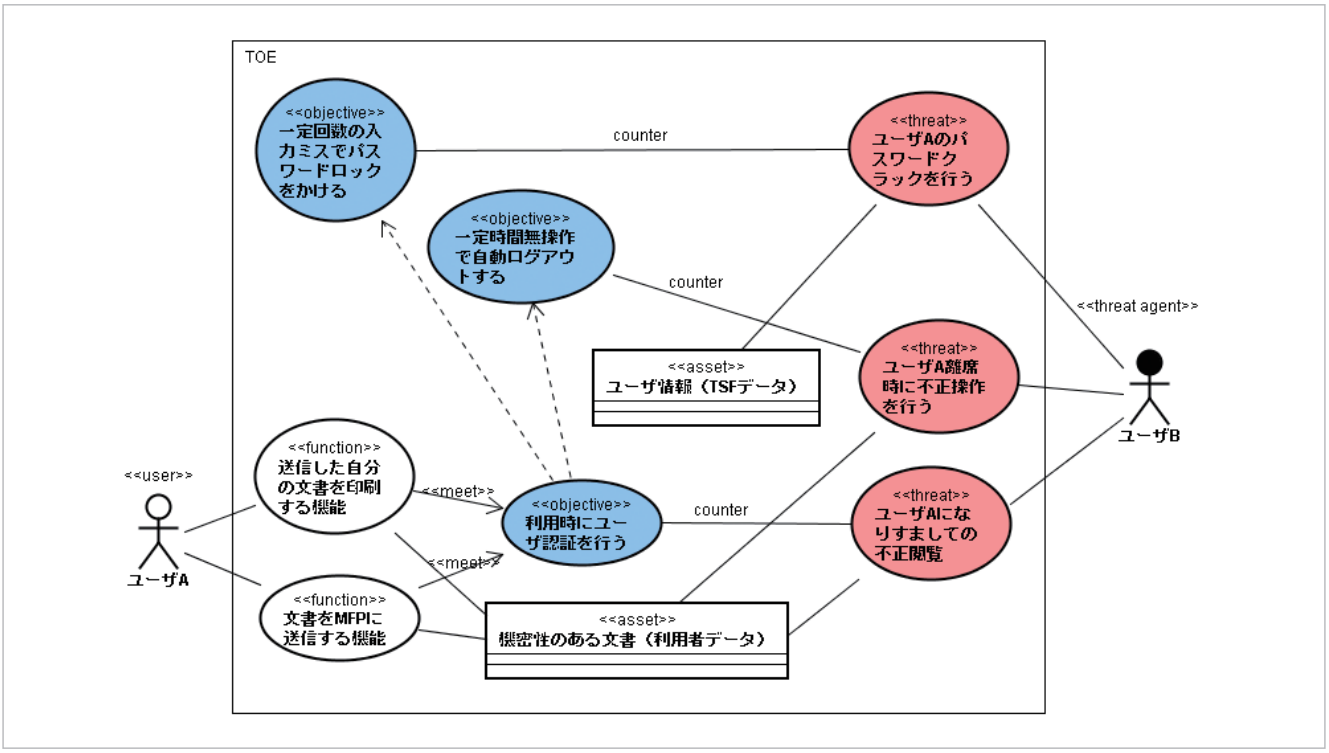


図 -5　MFP 製品を例にした脅威と対策分析（抜粋）

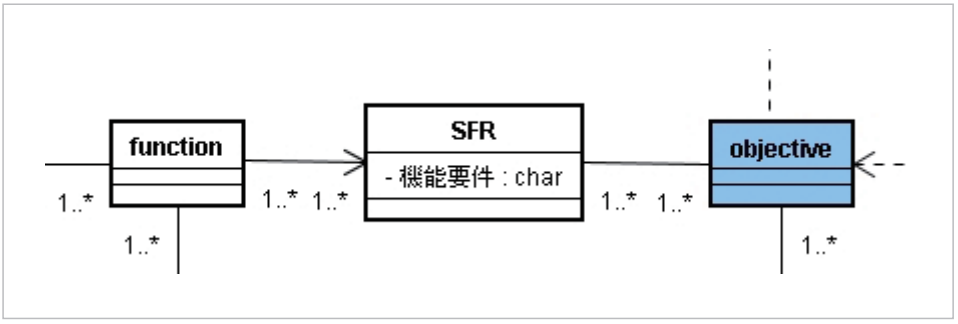


図 -6　SFR を含めたメタモデル（抜粋）

な開発者間の情報共有，類似した機能のある製品への利用等も比較的容易となる．さらにこの分析手法により一通り収束したミスユースケース図は，ST を記述する上で必要な項目が記載されており，なおかつ ST に記述が必要となるセキュリティ対策方針根拠（脅威に対する対策の対応分析）の簡潔で明確な材料となる．この分析手法は CC の取得を目指す開発者にとって，関係者間の認識統一や分析の手段として有用となると考えられる．

## 関連研究

UML のユースケース図をセキュリティに対して拡張した研究例は多い．McDermott と Fox によるアブユースケース図 [3] は，通常のユースケース図に加え，インタラクションの結果がシステムに対して害を与えるユースケースをアブユースケースと呼ぶ．Sindre と Opdahl によるミスユースケース図 [4] では，ミスユースケース（Misuse case）とミスユーザ（Misuser）という攻撃と誤操作を含むアクターを明示的に導入している．Firesmith によるセキュリティユースケース図 [5] では，Security と Misuse を使って，通常のユースケースとは区別している．UMLsec は，UML をベースに，配置図，クラス図等の図表現に対してセキュリティに関する特徴を記述するための拡張を施している．一方，セキュリティ要件の獲得と実装を含む開発プロセスの定義と各プロセスの最善の実践方法を提案するものとして，Mead らによる SQUARE [6] がある．なお，SQUARE については，本特集の記事で詳細を説明しているので参照されたい．また，ユースケースでは一般的に表現が困難である非機能要求のモデリングにおいては，ゴール指向分析手法について多くの研究が行われている．

## CC の今後の展望

コモンクライテリアに基づくセキュリティ評価は，中立的な第三者である評価者が，脆弱性の分析や侵入検査を行うことにより，開発者が保証する製品のセキュリティの信頼性が十分受入可能であることを，利用者に代わって確認するものである．したがって，本来，利用者自身が要求するセキュリティについて明確な基準を持つことが重要であり，セキュリティ保証を要求する側の立場で，しっかりとした実施可能なセキュリティの要求定義が求められる．CC の枠組みでは PP がそれに相当する．本稿では，CC 保証を行う開発者側で行われるセキュリティ要求分析を対象に解説した．CC が規定する保証と評価の手法を導入する開発者にとって，要求のモデル化手法は，対策すべきセキュリティの問題把握と対応の相互関係を定義するために有効な手段を与える．この手法を CC に最適化できれば，要求と対応の抜けやバランスのチェックの精度が高まり，CC に基づく保証・評価の効率化に向けて大いに期待される．ただし，実務適用を促進するためには，製品ライフサイクル上の各プロセスで管理可能な手法，ツールの整備が必要である．また，モデル化においては「どこまで精緻に落とし込むべきか」という課題が常に残る．実務適用の効果を上げるためには，プロダクトラインの方法論を取り入れ，かつ，設計・開発工程の各プロセスでのアクティビティとその結果が，それぞれの階層化されたモデル上の要素と関連付けられ，各々の効果が測定可能な状態であることが望まれる．モデル化の詳細化レベルは，各階層のモデル化の目的，および予測される費用対効果に基づいて設定される．また，これに応じて，評価実務における自己評価と第三者評価の位置付けや手段も変容することになろう．今後は，評価実務でも適用可能な，工学理論に基づいた体系的な検証手法に関する研究との連携も必須となるであろう．


**参考文献**

1）鎌田真由美：要求工学の現状と課題，情報処理，Vol.49, No.4, pp.347-356 (Apr. 2008).
2）栗田太郎：携帯電話組込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用，情報処理，Vol.49, No.5, pp.506-513 (May 2008).
3）McDermott, J. P. and Fox, C. : Using Abuse Case Models for Security Requirements Analysis, In ACSAC, pp.55-64, IEEE Computer Society (1999).
4）Sindre, G. and Opdahl, A. L. : Eliciting Security Requirements with Misuse Cases, Requirements Engineering Journal, 10 (1) : pp.34-44 (2005).
5）Firesmith, D. : Security Use Case, Journal of Object Technology, 2 (1) : pp.53-64 (2003).
6）Mead, N. R. and Stehney, T. : Security Quality Requirements Engineering (square) Methodology, ACM SIGSOFT Software Engineering Notes, 30 (4) : pp.1-7 (2005).


（平成 21 年 2 月 2 日受付）


**金子 浩之**　▶hiroyuki.kaneko@gene.mizuho-ir.co.jp

1962 年生まれ．富士総合研究所を経て，現在はみずほ情報総研（株）情報セキュリティ評価室 室長．経済産業省が進める IT セキュリティ評価および認証制度の認定を受けた評価機関において IT セキュリティ評価事業を主管．IT 製品やシステムのセキュリティ評価のほか，情報セキュリティをはじめとする調査，研究開発，システム監査，情報セキュリティ監査，コンサルティングに携わる．