情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-SE-164 No.8
Vol.2009-EMB-13 No.8
Vol.2009-CSEC-45 No.8
2009/5/28

コモンクライテリアのためのモデリング手法の提案

吉岡信和[†1]　田口研治[†1]
飛田孝幸[†2]　金子浩之[†2]

コモンクライテリアは，システムの設計者が主張するセキュリティの信頼性を保証するための枠組みであり，近年，産業界では重要な位置づけになりつつある．しかしながら，コモンクライテリアが求めるセキュリティの対象，その脅威と対策の明確化は，それ自体困難な活動であることに加え，従来の開発法にはない考え方であり，既存の開発に統合して行うことが難しかった．そこで，本稿では，これらの情報の分析，整理，明確化を助けるためのミスユースケースを拡張した方法を提案し，既存の開発に取り込みやすいプロセスを規定する．

A Modeling Method for Common Criteria

Nobukazu Yoshioka,[†1] Kenji Taguchi,[†1]
Takayuki Tobita[†2] and Hiroyuki Kaneko[†2]

Common Criteria, CC, is a framework to guarantee the security level of a system, which the developers argue. Although CC becomes to play an important role in industry in recent years, it is difficult to clearly define a security target, threats and the counter-measures required for CC. In addition, it is hard to integrate such security artifacts into traditional system development process because of the lack of such activities in the process.

In this paper, we have proposed a new method to help the definition of security concerns in CC with extension to a misuse-case diagram, including a process to allow us to integrate it into traditional one.

†1 国立情報学研究所 ＧＲＡＣＥセンター
GRACE Center, National Institute of Informatics
†2 みずほ情報総研株式会社 情報セキュリティ評価室
Center for Evaluation of Information Security, Mizuho Information & Research Institute, Inc.

1. はじめに

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，特に，セキュリティに関しては，企業における損害のリスクが大きい場合が多く，重要な特性である．

そのため，例えば，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がセキュリティに関する要求として規定される．さらに，その要求が破壊され，情報システムを意図した目的で運用できなり，企業が被害を受ける場合のリスクを考慮し，それを低減もしくは除去するための対策が，セキュリティ要求として検討される．

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コモンクライテリア[1)]（以下，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．

近年，セキュリティの重要性が高まるにつれ，CCに基づくセキュリティの保証が注目されているが，それに基づき安全なシステムを作る際には，次の２つの課題がある．すなわち，セキュリティに関する関心事が多く，それら間の整合性を合わせながら整理するのは難しいという課題と，この整理を従来の開発の一環として行うのが難しいという課題である．本研究では，この二つを解決するために，セキュリティに関する関心事を整理するための新しいモデルと，それを従来の開発に活かすためのプロセスを提案している．特に，本稿ではセキュリティ要求に絞って提案する．

2. コモンクライテリア（ＣＣ）によるセキュリティ保証

CCに関する規格文書は，３つのパート（パート１：概説と一般モデル，パート２：セキュリティ機能コンポーネント，パート３：セキュリティ保証コンポーネント）と，CCに基づ

Vol.2009-SE-164 No.8
Vol.2009-EMB-13 No.8
Vol.2009-CSEC-45 No.8
2009/5/28

く評価方法論を示す CEM があり，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，自然言語でセキュリティターゲット（ST：Security Target）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．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，評価対象の範囲と評価保証レベル（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

ST の記述として定義すべき情報（章立て）を図 2 に示す．

3. セキュリティ保証の課題

2 節で説明したようなＣＣに基づいてシステムの安全性（特にセキュリティ）を保証する際には，現状下記の課題が存在する．

（課題１）セキュリティの関心事の整理の難しさ： セキュリティには，図 2 にあるように，資産，脅威，対抗策，機能要件，根拠などシステムの内部のみならず，外部や利用形態などさまざまな関心事がある．また，これらの妥当性のほか，これらの間の関係も含めたセキュリティ構造の妥当性（開発側が想定する妥当な脅威，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について各々の相互関係の完全性及び正当性）をもれなく整理する必要がある．この整理は困難で，何らかのサポートが必要である．ミスユースケース[2] や UMLsec[3] など，既存の開発手法を拡張したモデリング手法はいくつか提案されているが，ＣＣにあるすべての情報は適切にモデル化できない．そのため，システムとセキュリティ要件の対応の不整合が発生し，脆弱性が残される可能性がある．

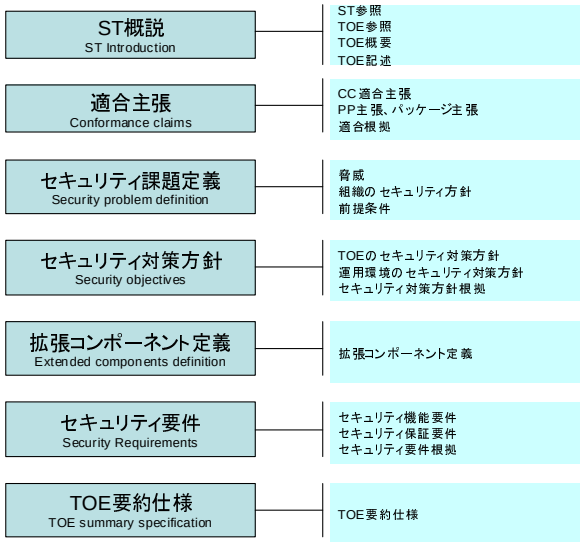

図 1 ST の構造
Fig. 1 Structure of ST

（課題２）既存の開発手法とのギャップ： secureTropos[4] や KAOS[5] などセキュリティ要求を分析するための手法はいくつか提案されているが，産業界でもっとも多く用いられている UML ベースの既存の開発手法とのギャップが大きく，導入にコストがかかる．そのため，ＣＣによる認証を行うために，システムの設計が進んだ段階で，セキュリティ要件を整理，定義している現状がある．しかしながら，セキュリティ要件は，設計方法に影響を及ぼすためセキュリティ要件を満たすために，設計を大幅に変更するなど作り直しのコストが非常に高くなるリスクが存在する．すなわち，セキュリティ要件を他の要件と同様，既存の開発の上流工程で行い，それを踏まえた設計ができるようにする手法が必要である．

4. ＳＴに基づくセキュリティ分析のためのモデル

本稿では，3 節で説明した課題１を解決するためにミスユースケースを拡張し，2 節で説明したセキュリティの要件定義に重要な資産（Asset），対抗策・方針（Objective），前提 (Assumption) 等を表現し，脅威やセキュリティ機能性（Security functionality）とともに，

Vol.2009-SE-164 No.8
Vol.2009-EMB-13 No.8
Vol.2009-CSEC-45 No.8
2009/5/28

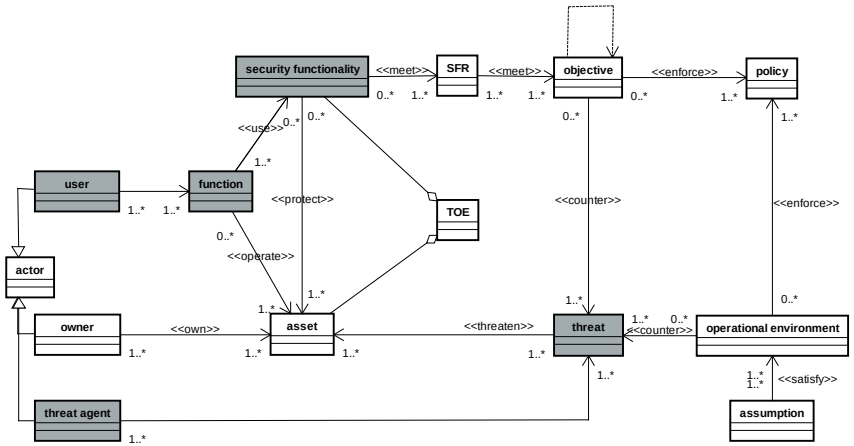

図 2 ST に基づくセキュリティ分析のためのメタモデル
Fig. 2 Metamodel for security analysis based on ST

それらの関係を明確化するモデルを提案する．また，そのモデルでは，ＣＣによる評価の範囲を明確にするために，評価対象（TOE：Target of Evaluation）が明示できる．図 2 が，ST に基づいてセキュリティの要件を分析するためのモデルのメタモデルである．この図の中の，グレーの要素は，従来のミスユースケースで表現されている要素である*1 このメタモデルをＵＭＬのユースケースを拡張して実体化することにより課題２の従来の開発とのギャップをモデルの観点で埋めることができる．

本提案のモデルでは，考慮する必要のない不要な脅威やセキュリティの対策を要求中に含めないようにするために，守るべき資産を明確にし，脅威，資産，それに関連するセキュリティ機能付き機能の関係を表現できるようにしている．さらに，その機能のセキュリティ機能要件（SFR:Security Functional Requirements）を明確にするために，脅威，および，それに対する対抗策・方針（objective）と関連付けている．図 2 中の Policy は，組織のセキュリティ対策方針であり，運用環境（operational environment）は，システムの運用等，提供する機能以外での脅威への対策方針である．すなわち，このモデルでは，脅威に対しては，どこまで運用で対策するか，機能で対応するかを明確にあらわすことができる．さらに，運用での対策に対しては，環境における前提条件（assumption）を明確にし，その対策が前提条件のもとで成立することを確認できる．

これらの関係に基づいてモデルを分析することで，考慮すべき脅威の妥当性検証が容易になるだけでなく，すべての脅威に対する対策がセキュリティ機能要件として規定されているか，それとも運用として対策されているかを分析できるようになる．

図 3 に，本メタモデルを用いて複合機のセキュリティ機能に関する要求をモデル化した例を示す．この例は，機密文書などを安全に印刷する機能（F.PRINT）に対するセキュリティの要求を示している．この機能では，保護対象の印刷文書（secure print file）が保護資産となり，それに対して所有者以外の User B が中身を閲覧してしまう脅威（Exposure of the secure print file）を挙げている．さらに，User B のネットワーク上の盗聴という脅威に対しては，LAN 自体に盗聴検知機能を持たせるという運用上の対策がなされ，それで盗聴ができないという仮定をおいた設計であることが，運用環境，および，前提条件により明確になっている．

5. ＳＴに基づくセキュリティの分析手順

図 2 には，従来のユースケースにある要素以外に，それに関連するさまざまなセキュリティの関心事が含まれている．そのため，課題１にあるように，これらを整理することは容易ではなく，整理のための何らかの方法・方針が必要となる．そこで本稿では，次の３つのフェーズに分けて要件を整理・分析することを提案する．

フェーズ１：脅威に基づくセキュリティの認識

まず，システムが提供する機能のうちセキュリティが必要かどうかを，機能・資産・脅威の関係から洗い出す．資産を明確にすることで，脅威の存在性やリスクが明らかになり，システムの機能に関するセキュリティの重要性が認識できる．図 4 が，複合機に関するフェーズ１のモデルの例である．このモデルによって，印刷機能に関して文書漏れの脅威の可能性があり，システム内の文書ファイルがその対象となることで，被害が存在するというリスクが認識できる．

フェーズ２：対策方針の検討

フェーズ１で認識された脅威に対して，対策方針（objective）を決定する．同時に対策方針に関連する機能を明確化する．このフェーズでは，対策方針を実施するために新たな資産（二次資産）を追加する場合もある．例えば，特定の資産にアクセスするときは，認証・

*1 図 2 では，ＣＣの用語に合わせてシステムが持つべき機能を Function，ミスユーザを Threat Agent と定義している．また，暗号や認証などのセキュリティ自体の機能は，システム内部の機能であるため要求としてはモデル化しない．

Vol.2009-SE-164 No.8
Vol.2009-EMB-13 No.8
Vol.2009-CSEC-45 No.8
2009/5/28

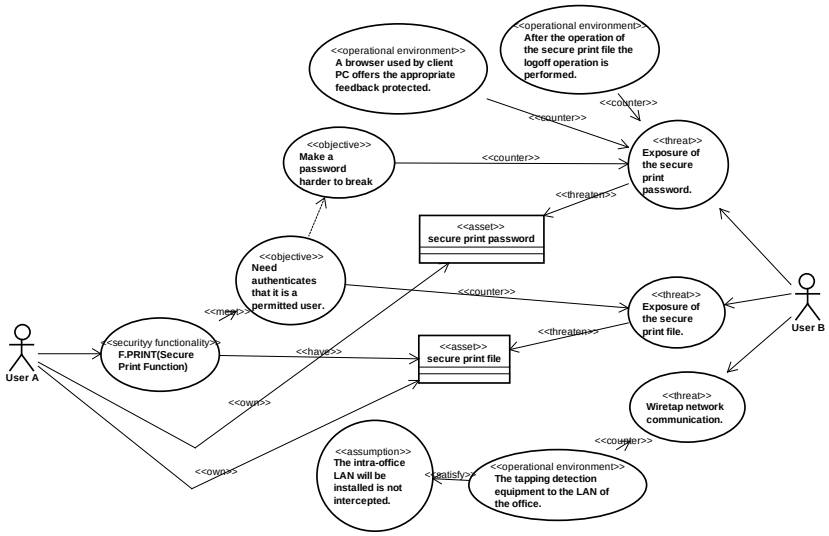

図 3 複合機のセキュリティ要求モデルの例
Fig. 3 An Example of A Security Requirements Model for A Multi-Function Printer

許可を必要とするという対策方針を立てた場合，認証のための鍵が必要になり，それがシステムの新たな資産となる．さらに，新たな資産に関しては鍵が盗まれるなどの新たな脅威が考えられる．そのために，このフェーズでは，脅威・対策方針・機能・資産，そして新たな脅威と，繰り返し，考慮すべき脅威，および，対策を洗い出す必要がある．また，脅威に対しては，システム内での対策の他に，運用環境による対策も検討する．

フェーズ３：セキュリティ機能仕様の決定

最終的には，フェーズ２までに洗い出された対策方針を，どのように機能として実現すべきかをセキュリティ機能要件として整理する．セキュリティの対策方針は，システムの機能を実現する際の制約になる．例えば，機密性が必要な文書ファイルを印刷する際,「認証によって許可されているかどうかを確認する」というセキュリティの対策方針を決めた場合，その方針は，印刷機能に対して,「認証を行い，かつ，認証に連続して失敗したときには，機能を無効にする」という制約を規定する．

これらのプロセスは，従来のユースケースを用いた機能要求の洗い出しを入力とし，それに対するセキュリティの要件獲得に用いることができ，従来の開発に容易に取り込むことができる．

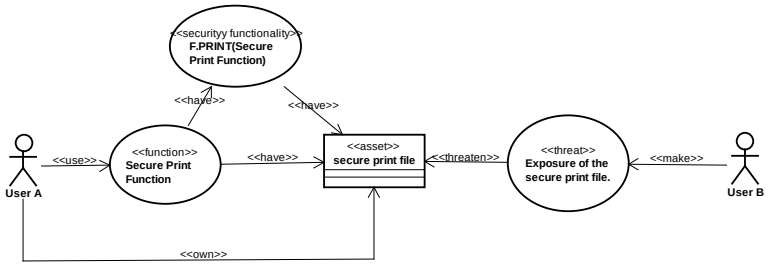

図 4 複合機のセキュリティ要求モデルの例 (フェーズ１)
Fig. 4 An example of A Security Requirements Model for A Multi-Function Printer (Phase 1)

6. おわりに

本稿では，コモンクライテリアに基づいてシステムの安全性を保証する際に，適切なセキュリティ要件を整理するためのモデリング手法を提案した．具体的には，ミスユースケースを拡張し，資産，対抗策・方針，前提等を表現し，脅威やセキュリティ付き機能との関係を明確化した．さらに，セキュリティ要件の分析の難しさを解決するために，このモデルの構築方法を示した．これらにより，従来の開発と親和性が高い手法が提案できた．今後は，ＣＣの認証を受けた実例題に対して，本手法を適用し，その有効性を評価する．さらに，本手法をサポートする開発環境を構築する．

参 考 文 献

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　バージョン 3.1 *http://www.ipa.go.jp/security/jisec/cc/index.html*.
2) Sindre, G., Opdahl, A.L.: *Eliciting security requirements with misuse cases*, Requir. Eng.,Vol. 10, No. 1, pp. 34–44 (2005).
3) Jan Juïjens: *Developing Safety-Critical Systems with UML*, UML 2003, Springer, LNCS 2863, pp 360–372 (2003).
4) Mouratidis, H. and Giorgini, P. : *Secure Tropos : Dealing Effectively with Security Requirements in the Development of Multiagent Systems*, in Safety and Security in Multiagent Systems, LNCS, Springer-Verlag (2006).
5) Letier, E. : *Reasoning about Agents in Goal-Oriented Requirements Engineering*, Ph.D. thesis, Universite catholique de Louvain (2001).