システム利用シナリオからのセキュリティ脅威の検出と対策シナリオの導出に向けて

阿部 達也[1,a)]　林 晋平[1,b)]　佐伯 元司[1,c)]

概要：本稿では，システム利用シナリオからセキュリティ脅威を検出しミスシナリオを出力する手法と，Security Target の記述から脅威の対策を抽出する手法を組み合わせることで，ミスシナリオに対応する脅威の対策がなされたシナリオを出力し，セキュリティ要求獲得を支援する手法について述べる．

1. はじめに

ソフトウェア開発においてセキュリティ対策，特にコスト削減や高品質な開発のためには要求獲得段階でのセキュリティ要求獲得が重要である．しかし，セキュリティ要求獲得には専門知識が必要であり，人による脅威発見や対策では見落としが発生する可能性がある．そのため，セキュリティ知識を内包したセキュリティ要求獲得の支援手法が必要である．

そこで，筆者らは既存手法として，Security Target（ST）をセキュリティ知識源として，システム利用シナリオからセキュリティ脅威を発見する手法を提案している [1]．しかし，この手法では対策案の提示は行えていない．本稿では既存手法を拡張し，対策シナリオの導出，提示までを行う手法について述べる．

2. 提案手法

2.1 提案プロセス

提案手法のプロセスを**図 1** に示す．プロセスの番号は図 1 の矢印の番号と対応している．

(1) 要求分析者は，対象のシステム利用シナリオを既存手法で定めたフォーマットのシーケンス図によって記述する．
(2) 脅威検出パターンと利用シナリオのパターンマッチングにより，脅威の検出を行う．
(3) 脅威検出パターンと利用シナリオのマッチした部分について，グラフ変換を用いて，脅威に対応するミスシナリオパターンに置き換える．これによってミスシナリオが利用シナリオに埋め込まれ，脅威に対応するミスシナリオが作成される．
(4) 同様に，脅威検出パターンと利用シナリオのマッチした部分について，グラフ変換を用いて，対策が埋めこまれたパターンに置き換える．これによって対策が埋め込まれた利用シナリオが作成される．

変換用のパターンの作成，グラフ変換を利用した埋め込みについては既存手法 [1] に基づき行う．

2.2 対策のための知識源

知識源として，Common Criteria（CC）[2] によって定められたセキュリティ評価用文書である Security Target（ST）を利用する．ST を利用する理由として，高信頼であること，複数の ST を利用することで幅広いドメインに適用できる知識を抽出できることに加え，佐伯らの手法 [3] を用いることで，それぞれの脅威について，その対策及び対策に必要なセキュリティ機能コンポーネント (SFC) 単位までのトレースを行うことができることが挙げられる．セキュリティ機能コンポーネント（SFC）とは，CC のガイドラインで定められている対策のための機能コンポーネントであり，これを組み合わせることによって ST に記述されたすべての対策が実現されている．

プロセスにおいて利用される脅威検出パターン，ミスシナリオ埋め込みパターンは ST の 3 章の記述から抽出した知識を利用して作成することができる（図 1(a),(b)）．

対策埋め込みパターンを作成するためには，脅威と対策の関係性，対策の内部で行われる動作の知識が必要である．ST の 3 章の脅威記述，ST の 4 章と 8.1 章の対策方針記述と脅威と対策方針の対応表，そして 8.2 章の対策方針と SFC の対応表をたどることによって，ある脅威に対す

[1] 東京工業大学
Tokyo Institute of Technology
[a)] abe@se.cs.titech.jp
[b)] hayashi@se.cs.titech.jp
[c)] saeki@se.cs.titech.jp

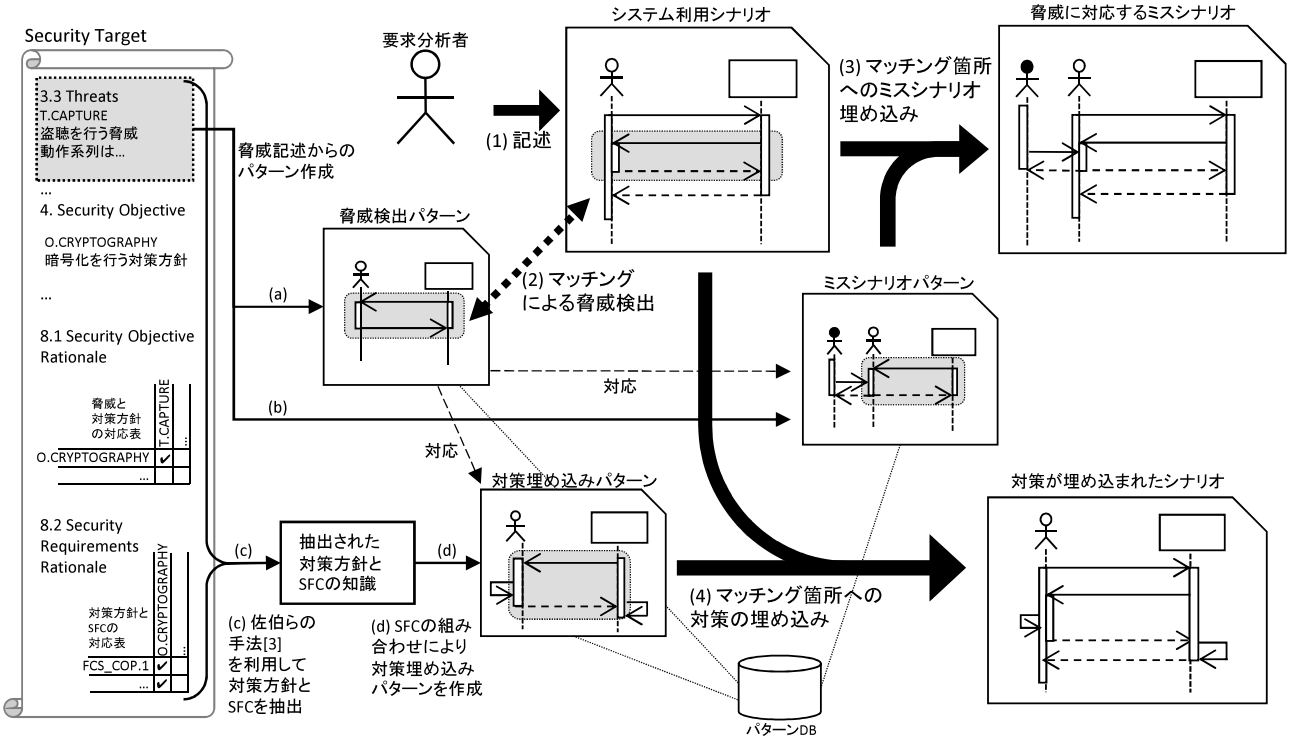

図 1 提案手法の概要

る対策とそれを構成する SFC の関係をトレースすることができる [3]（図 1(c)）．そのため，各 SFC に対応する動作系列やデータをシナリオに埋め込むパターンを記述しておき，それを関連性を元に組み合わせることによって最終的に脅威の対策を埋め込むためのパターンを得ることができる（図 1(d)）．

2.3 脅威からの対策と SFC の導出例

図 1 内の 3.3 章の記述，4 章の記述，8.1 章，8.2 章の対応表を利用する．記述された脅威 T.CAPTURE について，8.1 章の対応表より 4 章に記述された対策 O.CRYPTOGRAPHY が対応することが判明する．また，8.2 章の対応表より O.CRYPTOGRAPHY は FCS_COP.1 とその他の SFC を組み合わせることで実装できることが判明する．FCS_COP.1 に関するパターンを適用することで，対策が埋め込まれたシナリオを得る．

2.4 実装

パターンの検出と対策の埋め込みはグラフ変換によって実装する．グラフ変換には AGG [4] を利用する．作成したパターンはパターン DB に保存される．

パターンと入力シナリオは既存手法 [1] で定めた検出用の情報を付加したシーケンス図で記述する．検出用情報の例として，送受信データについてのアクセス制限情報や，メッセージがどの CRUD 動作を行うのかを表すステレオタイプなどが存在する．

既存手法では脅威の検出とミスシナリオの埋め込みに必要な検出用情報のみが実装されており，これを SFC をパターンとして記述できるように拡張する．また，対策が埋め込まれた後のシナリオを入力した場合の対策済み脅威の再検出が発生しないようにするための脅威検出パターンの改善も必要である．

3. おわりに

本稿では既存手法である利用シナリオからの脅威検出手法を，ST から脅威の対策と SFC を抽出する手法を用いることで，対策シナリオの出力を行う事ができるように拡張した．今後の課題として，拡張手法の SFC パターン及び対策埋め込みパターンの作成と実装，セキュリティ機能要求獲得支援法としての有用性の評価などが挙げられる．

参考文献

[1] Abe, T., Hayashi, S. and Saeki, M.: Modeling Security Threat Patterns to Derive Negative Scenarios, *Proc. APSEC*, pp. 58–66 (2013).
[2] Common Criteria : New CC Portal, `http://www.commoncriteriaportal.org/`.
[3] Saeki, M., Hayashi, S. and Kaiya, H.: Enhancing Goal-Oriented Security Requirements Analysis using Common Criteria-Based Knowledge, *Int'l J. Softw. Eng. Knowl. Eng.*, Vol. 23, No. 5, pp. 695–720 (2013).
[4] The Attributed Graph Grammar System: AGG 2.0.4, `http://user.cs.tu-berlin.de/~gragra/agg/`.