Vol.2015-SE-187 No.17
2015/3/12

セキュリティターゲットを活用したセキュリティ機能要求獲得支援法

阿部 達也[1,a)]　林 晋平[1,b)]　佐伯 元司[1,c)]

概要：システム設計段階において，あらかじめシステムに存在するセキュリティ脅威を検出し対策を講じることによって，より安全で高信頼度のシステムを開発することができる．しかし，脅威の検出と対策にはセキュリティに関する知識が必要であったり，見落としを極力減らす必要があったりすることから，コストや時間がかかる．そこで本稿では，入力されたシナリオシーケンスに対し，あらかじめ知識として保持している検出と対策のためのパターンとの比較によって，対象システムに発生しうる脅威を検出し，ミスシナリオと脅威が対策されたシナリオ，それを実現するためのセキュリティ機能を提示する手法を提案する．シナリオ記述及びパターンの記述において，セキュリティドメインに基づくプロファイルに従ったUML シーケンス図を利用し，パターン作成のための知識として，コモンクライテリアで定められているセキュリティターゲットを用いる．本稿では適用事例を用いて手法の有用性を確認した．

Eliciting Security Functional Requirements Using Security Targets

Tatsuya Abe[1,a)]　Shinpei Hayashi[1,b)]　Motoshi Saeki[1,c)]

Abstract: Detecting and mitigating security threats of information systems in design phase helps to make them secure. However, the more threats we try to detect and mitigate, the more cost and knowledge of security threats are required. In this paper, we present a technique to detect security threats, show negative scenarios, mitigated scenarios and their security functions with comparing normal scenarios of a business process and the patterns created from knowledge of security. The scenarios of a business process are described with sequence diagrams. The knowledge is extracted from the documents called Security Target compliant to the international standard Common Criteria. We show the usefulness of our approach with several case studies.

1. はじめに

情報システムにおける情報の安全性を確保し，低コストで高品質なシステムを開発するためには，ソフトウェア開発の早期である要求獲得段階においてセキュリティ機能要求を獲得することが重要である．

しかし，セキュリティ機能要求獲得において脅威の発見，対策案の導出を行う上では，(1) 人手のみによる脅威の検出，対策案の導出は非常にコストが掛かり，脅威や対策の見落としが発生する可能性がある，(2) セキュリティ機能要求獲得を行う開発者が所持するセキュリティ知識が不十分である可能性がある，という大きく 2 つの問題がある．これらの問題を解決するには，セキュリティ知識を内包した手法による脅威検出，対策案の提示の支援が必要である．

提案手法では，脅威を検出するための知識に加えて，脅威の対策案を導出し対策を埋め込むための知識をパターンとして保持する．入力されたシナリオ記述とのパターンマッチングやグラフ変換を利用することで脅威の検出と脅威が発生した際のシナリオ (ミスシナリオ) の出力を行い，同様に検出された脅威に対して，パターンを利用することで対策シナリオの導出と提示を行う．セキュリティターゲットと呼ばれる文書を知識源としてパターンを作成する．提

[1] 東京工業大学 大学院情報理工学研究科 計算工学専攻
Department of Computer Science, Tokyo Institute of Technology
[a)] abe@se.cs.titech.ac.jp
[b)] hayashi@se.cs.titech.ac.jp
[c)] saeki@se.cs.titech.ac.jp

案手法について，AGG と呼ばれる属性付きグラフ文法によって自動化を行うとともに，9 種類の脅威についての検出，対策用のパターンを作成した．自動化した提案手法を 2 ドメインの 6 つのシナリオ事例に適用して評価を行い，脅威の検出と対策の埋め込みが行えた．

我々は過去に同様の手法 [1] を提案しているが，脅威の発見のみにとどまり，対策案の導出をサポートすることは出来なかった．本手法では，[2] のアイディアを元に，対策案の導出と対策の埋め込みを実現し，より完成されたセキュリティ機能要求獲得支援手法を提案する．

本稿の構成を以下に示す．2 章において我々のアプローチを示すとともに，知識源として利用するセキュリティターゲットの説明を行う．3 章で提案手法について説明する．4 章では, 提案手法の自動化と実装したパターンを示し，5 章で適用事例を用いた評価について述べる．6 章において関連するセキュリティ機能要求獲得支援手法について述べ，最後に，7 章で本稿をまとめ, 今後の課題について述べる．

2. アプローチ

2.1 概要

提案手法では，システムのビジネスプロセスにおける利用シナリオを入力として，利用シナリオからの脅威検出と対策案の導出を行う．

手法を実現するにあたり，パターン及び入力するシナリオの適切な記述法が必要となる．記述法の要件として，(1) セキュリティ脅威を検出する上で重要となる，システム利用シナリオ内の要素の相互関係と，データのやり取りの時間的順序とを明確に記述できること，(2) セキュリティの専門家でなくともシステム利用シナリオを記述できること，がある．

そこで，本手法では，UML シーケンス図を入力シナリオ及び脅威検出と対策用のパターンの記述に使用する．この時，シーケンス図におけるライフライン，メッセージ，データの要素に，手法で定めたステレオタイプやタグ付き値を付加することによって，個々のシナリオで一致しない要素について汎用的なパターン作成を行うことができる．

例題として，ログインにより利用が可能になるシステムを考える．ユーザはあらかじめパスワードを知っており，システムは UI で入力を受け付ける．このシステムにおける利用シナリオとして，ユーザがシステムにパスワードを入力してログインするという利用シナリオをシーケンス図で記述すると，**図 1** のようになる．付加されたステレオタイプやタグ付き値は，3.2 章で説明する．

このシナリオについて，例えばメッセージ 2 に対して入力，送信したパスワードが盗聴される脅威が考えられる．また，この盗聴の脅威に対しては，パスワードの盗聴を防ぐために，送信時に暗号化を行うことにより対策が行える．

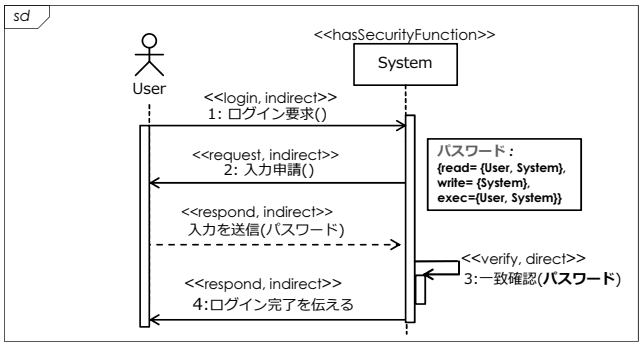

図 1 ログインシナリオ例の属性付きシーケンス図による記述

これらの検出と対策に必要なのは，“パスワードは守るべきデータである”，“守るべきデータを送受信する場合は，保護を行わなければ盗聴される危険性がある”，“盗聴を防ぐためには，暗号化を行えば良い” のようなセキュリティ知識である．このようなセキュリティ知識と利用シナリオを照らし合わせ，変換することで，脅威の検出と対策を行うことができる．具体的には，図 1 のシナリオを記述する際に，専用の記述法で検出に必要な付加情報を記述しておく．そして，脅威を見つけるための知識を内包するパターン，脅威の対策の知識を内包するパターンを作成し，手法にデータベースとして保持する．

このように，本手法ではセキュリティ知識から検出用のパターンを作成し，それと入力されたシステム利用シナリオをパターンマッチングで比較することによって脅威の検出と対策案の導出を行う．パターンマッチングを利用することによって，定義されたパターンに存在する脅威であれば，シナリオ内から網羅的に発見を行うことができる．同様に，ミスシナリオについても，埋め込みパターンによって出力できるようにすることによって，対策を行った場合と行わずに脅威が発生した際のシナリオの変化を確認し，脅威のリスク分析と照らしあわせて実際に対策を適用するか考えることができる．

2.2 知識源としてのセキュリティターゲットの利用

本手法では，脅威の対策の導出，および対策を埋め込むために必要なパターンを作成するためのセキュリティ知識源として，既存手法 [1] と同様にセキュリティターゲット (Security Target, ST) と呼ばれる脅威や対策について記述された文書を用いる．

ST は，国際基準である，コモンクライテリア（Common Criteria，CC）[3] によって記述法が定められており，既存製品についてどのような脅威が考えられ，どのような対策がされているかについて， 一貫した形式によって記述されている．ST は認証されているので高信頼であり，公開されており誰でも入手できる [*1] ため，知識源として非常

[*1] https://www.ipa.go.jp/security/jisec/certified_products/cert_list.html

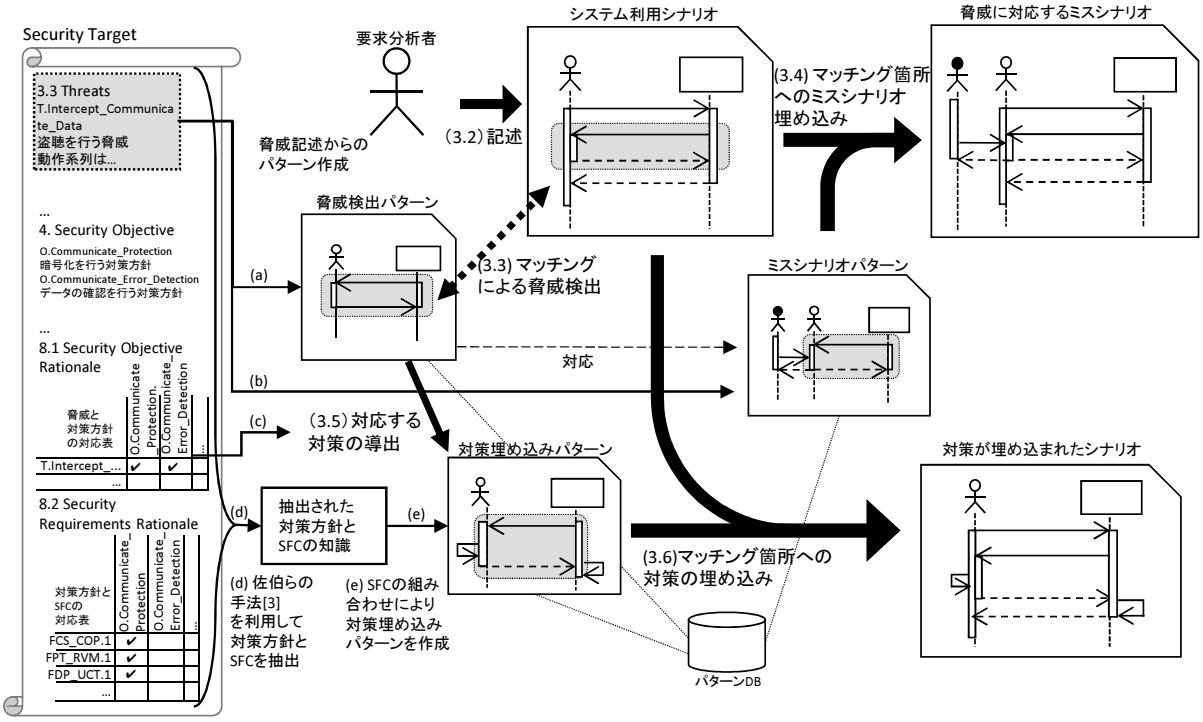

図 2 提案手法の概要

に有用である．複数の ST を利用することで，汎用的なセキュリティ知識を抽出し，それを元にパターンを作成する．作成するパターンと利用シナリオ記述に同じ記述法を利用することで，パターンマッチングによる脅威検出と対策を容易にする．ST における対策は，セキュリティ機能コンポーネント（SFC）を組み合わせることで実装されている．SFC は CC で定められているセキュリティ機能を構成するコンポーネント要素である．例えば，“FCS_COP.1” と呼ばれる SFC には，“指定されたアルゴリズムと暗号鍵長による暗号処理を行う” という内容が記述されている．この記述から，このコンポーネントを含む対策は，暗号処理を利用するという知識を得ることができる．複数の SFC を組み合わせることで，どのような対策をいつ何に行うのかが判明するので，対策をシナリオとして記述できる．

佐伯らの手法 [4] を利用することによって，ST からの脅威の対策と SFC の導出が可能である．ST 内の 3.3 章，4 章の記述と，8.1 章，8.2 章の対応表を利用することで，脅威検出の知識，脅威の対策を導出する知識，対策の実装に必要な SFC の知識を手に入れることができる．また，複数の ST についてこの手法を適用することで，パターンを記述するために必要な属性を分析し，汎用的な属性を作成する．

3. 提案手法

3.1 概要

提案手法のプロセスを**図 2** に示す．あらかじめ，ST から抽出した知識から脅威検出パターン，ミスシナリオ埋め込みパターン，対策案導出パターン，対策埋め込みパターンを作成しておく．要求分析者は，対象のシステム利用シナリオを特別なシーケンス図によって記述する．その際，各要素に対応する属性値を入れる．これに対して，脅威検出パターンとのマッチングにより，脅威の検出を行い，検出された脅威とシナリオ内の関連する要素を結びつける．また，検出された脅威に対応するミスシナリオ埋め込みパターンを適用することにより，シナリオの対象の箇所にミスシナリオを埋め込む．同様に，検出された脅威に対して，対策案導出パターンを利用することでその脅威の対策を導き，それぞれの対策について対策を関連するシナリオ中の要素と関連付ける．導出された対策について，対策埋め込みパターンを適用し，シナリオに対策を埋め込む．これによって，対象のシステム利用シナリオに対し，検出された脅威とその対策の一覧，そして脅威が発生した場合のミスシナリオと対策が実際に埋め込まれた場合の利用シナリオが出力される．ミスシナリオを導出することで，脅威が実際に発生した場合の損害を推定することが出来る．また，対策されたシナリオとの比較によって，対策を行った場合のコストとリスクの比較を行うことができる．

3.2 入力シナリオシーケンスの記述法

入力シナリオシーケンスの記述は，**表 1** の様なステレオタイプとタグ付き値を付加することで行う．脅威の検出を行うためには，動作主の種類，送受信されるデータのアクセス権限，メッセージの種類や通信方式などの情報が必要であり，手法で判別できる記述が必要である．そこで，サ

表 1　ステレオタイプとタグ付き値

Notation	Description
サブジェクトに付加 (ライフライン):	
≪hasSecurityFunction≫	セキュリティ機能を持つ
≪movable≫	持ち運び可能，動作に電源が必要
メッセージに付加:	
≪direct≫	送受信に直接接続を利用
≪indirect≫	送受信に UI や無線などを利用
≪request≫	相手に対してデータをリクエスト
≪respond≫	応答としてデータを返す
≪modify≫	データの書き込み，変更，削除を行う
≪verify≫	データの正当性を確認する
≪login≫	ログインし，セッションを開始する
≪logout≫	セッションを終了する
データに付加:	
$\{read = R \subseteq S\}$*1	R はデータの読み込み許可対象の集合
$\{write = W \subseteq S\}$*1	W はデータの書き込み許可対象の集合
$\{exec = E \subseteq S\}$*1	E はデータの実行許可対象の集合

*1 S はサブジェクトの集合 ∪{public} であり，“public” は，誰でもその権限が許可されていることを明示する特殊な値である．

ブジェクト，メッセージ，やり取りされるデータにそれぞれ種類や権限，通信方式などを表すためのステレオタイプとタグ付き値を付加する．ステレオタイプは ≪≫ で囲まれた文字列，タグ付き値は {} で囲まれた文字列である．

本手法では，CC で定められている表記に合わせて，シナリオ動作主であるライフラインのオブジェクトのことをサブジェクトと呼ぶ．また，ライフラインの頭部形状により，サブジェクトが人間であるかどうかを判断する．

表 1 を利用して利用シナリオ例を記述したものが，図 1 である．それぞれ，ユーザは人間であるサブジェクト，システムはセキュリティ機能を持つサブジェクトであり，データであるパスワードは，$\{read\}$ と $\{exec\}$ の値がユーザとシステム,$\{write\}$ の値がシステムであるため，ユーザとシステムのみ読み取りと実行が可能，システムのみが書き込みが可能である，メッセージ 1,2,4 はそれぞれ UI による直接的でない通信方式によるログインの要求，パスワードのリクエストとそれに対する送信，ログイン完了の通知であり，メッセージ 3 はシステム内部における直接通信によるパスワードの正当性確認である．

3.3　脅威の検出

脅威検出パターンを利用し，入力シナリオから脅威の検出を行う．脅威検出パターンは，ST3.3 章の記述から抽出した知識から作成できる（図 2 中 a)．例として図 2 の左側に記述された，FeliCa IC カードの ST*2 の一部を利用する．ST の 3.3 章には，T.Intercept_Communicate_Data という，盗聴の脅威が発生する条件と発生した場合のミスシナリオが自然言語で記述されている．これを用いること

*2 https://www.ipa.go.jp/security/jisec/certified_products/c0251/c0251_st.pdf

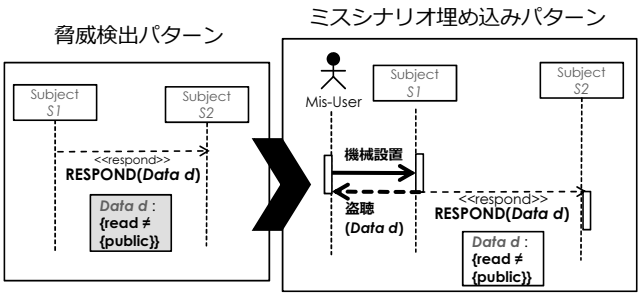

図 3　盗聴の脅威検出パターンとミスシナリオ埋め込みパターン

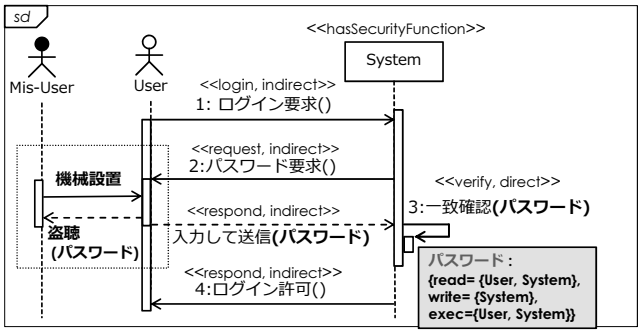

図 4　盗聴のミスシナリオが埋め込まれたシナリオ例

で，盗聴の脅威を検出するためのパターンが**図 3** 左辺のように作成できる．サブジェクト S_1 としてユーザ，サブジェクト S_2 としてシステム，対象の ≪respond≫ メッセージとしてパスワードの送信メッセージ，対象のデータ d としてパスワードがマッチするため，図 1 におけるパスワードの送信の部分に盗聴の脅威を検出することができる．

3.4　ミスシナリオの埋め込み

ST3.3 章から，脅威が発生した場合のミスシナリオを埋め込むためのパターンを同様に作成することができる (図 2 中 b)．盗聴に対応するミスシナリオ埋め込みパターン (図 3 右辺) を図 1 に適用することで，パスワードの送信メッセージに対し，ミスアクターによって通信網に機械が仕掛けられ，パスワードの盗聴がされる**図 4** のようなミスシナリオが埋め込まれる．

3.5　対策案の導出

一つの脅威に対する対策案は複数存在する．それらの関係性を導出するため，ST8.1 章から脅威に対応する対策案導出のための知識を抽出し, 対策案導出パターンとして知識を保持する．これを利用して，検出された脅威を緩和する対策を導出する（図 2 中 c)．

図 1 の例では, 検出された盗聴の脅威の対策として, 図 2 左の ST8.1 章対応表よりから，O.Communicate_Protection, O.Communicate_Error_Detection の 2 つの対策を埋め込むことで盗聴を対策できることが判明する．

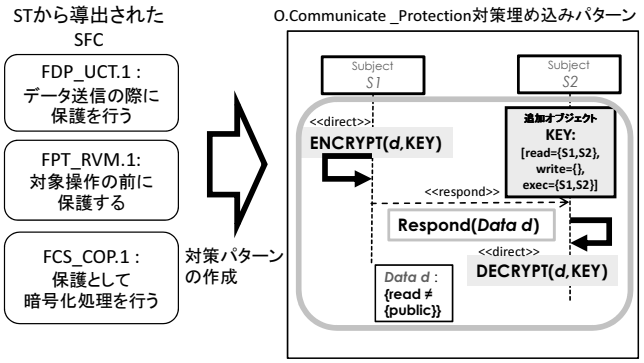

図 5 暗号化の対策を埋め込むパターン

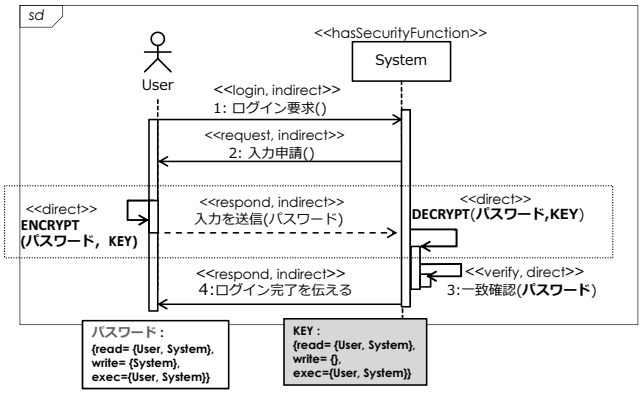

図 6 盗聴に対して暗号化の対策が埋め込まれたシナリオ例

3.6 対策案の埋め込み

脅威が検出された箇所に対して，導出された対策に対応する対策埋め込みパターンを利用し、対策が埋め込まれたシナリオに置き換える．対策埋め込みパターン例として，O.Communicate_Protection を埋め込むパターンを**図 5** に示す．

図 2 左下の 8.2 章対応表より O.Communicate_Protection を実装する SFC を組み合わせが判明する．O.Communicate_Protection は, FCS_COP.1, FDP_UCT.1, FPT_RVM.1 の 3 つの SFC で実装される事がわかる．（図 2 中 d）FCS_COP.1 は，暗号鍵を利用した暗号化保護を行う SFC である．FDP_UCT.1 は，保護すべきデータを通信する時に指定の保護を行う SFC である．FPT_RVM.1 は，各セキュリティ機能の迂回を防ぐために，他の機能を呼び出す前に必ず指定の機能を呼びだすことを指定する SFC である．この 3 つを組み合わせることで，“保護すべきデータを送信する前に必ず暗号化の処理を行う” という図 5 右のような利用シナリオシーケンスパターンを記述することができる．これをシナリオ中の検出要素に適用し，暗号化の対策を埋め込む．（図 2 中 e）

例として，図 1 にパスワードの暗号化を実際に埋め込む．先ほどのミスシナリオの埋め込みと同様に，対象となるサブジェクト S1 から S2 へのデータ d の ≪respond≫ メッセージとマッチする，ユーザからシステムへのパスワード送信メッセージの前後に，暗号化処理を表す ENCRYPT メッセージと，復号化を表す DECRYPT メッセージが埋め込まれる．また，暗号化用の鍵である KEY オブジェクトが追加される．これで，**図 6** のように暗号化の対策が埋め込まれた．これを，導出された対策すべてについて行い，対策されたシナリオを出力する．

4. 実装

パターンを網羅的に比較する必要が有るため，AGG（attributed graph grammar）と呼ばれる属性グラフ変換文法及びツール [5] を用いて，手法におけるパターンマッチングとグラフ変換を自動化した．また，手法の知識として，実際に ST からパターンを作成した．

4.1 AGG による記述

利用シナリオシーケンスの各要素及びメッセージ順序を AGG 対応の属性グラフ形式に書き直すとともに，それぞれのパターンを属性グラフ変換ルールとして作成する．

AGG では有向グラフを扱い，それに対してグラフ変換を適用できる．利用シナリオを属性グラフ形式に書き直し，それぞれのパターンに対応するグラフ変換ルールを作成，適用することによってパターンの比較と変換を行う．AGG による記述法については，過去研究 [1] を利用しているため，ここでは省略する．

AGG による変換では，検出された脅威や対策の情報を保持する専用のノードを利用する．入力シナリオに脅威検出パターンによるグラフ変換を行うことで、マッチした脅威に対応する脅威ノードがグラフに埋め込まれる．これを参照し、ミスシナリオを埋め込む．また，対策案導出パターンによってまだ対策が導出されていない脅威ノードを含む部分シナリオを検出し，その脅威を緩和する対策ノードを追加するグラフ変換を行う．ユーザーは AGG によって脅威の検出が行われたシナリオに対して，対応する対策案導出パターンを選択し，適用することで，脅威に対応する対策ノードを埋め込む．その後，対策ノードが付加されたシナリオに対し，対応する対策埋め込みパターンを用いたグラフ変換によって，対策ノードを SFC の組み合わせによる実装に展開し，シナリオに埋め込む．AGG で記述した対策埋め込みパターン例として図 5 を AGG で記述したものを**図 7** に示す．シーケンス図におけるメッセージは，message ノードと 2 つの Subject ノード，それをつなぐ from,to エッジによって表現されている．データ d に対応するのが ObjectAsset であり，それを送信対象とする Respond メッセージや他の送受信メッセージを検出している．左側のパターンが検出された場合，右辺のように対応する message ノードの前後に，encrypt メッセージに対応するノードと decrypt メッセージに対応するノードが “nextInsertion” エッジで接続される．それぞれのノー

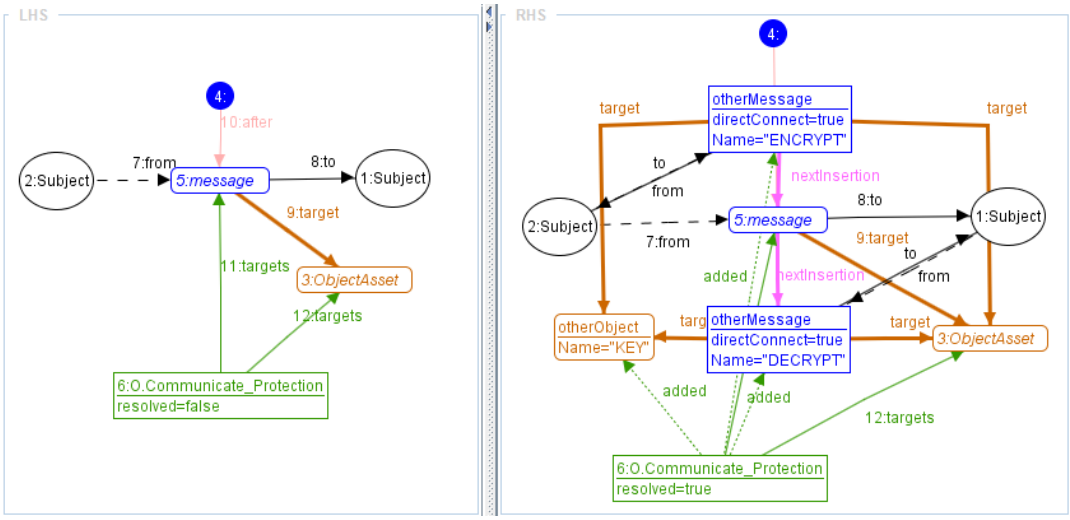

図 7 AGG による暗号化対策埋め込みパターン

ドは，データ d と KEY という名前のオブジェクトを対象として持つ．この変換が行われたあとの後処理によって，“nextInsertion” エッジが解消され，正しく AGG グラフのメッセージの流れの中に対策が埋め込まれる．

4.2 作成したパターン

今回，手法で利用できるパターンとして，9 種類の検出用パターンと，それから導出される 12 種類の対策パターンを作成した．

作成には，3.3 節で利用した “FeliCa IC カードシステム”(C251)，“e-passport system”(C229)[*3]，“IC 住民基本台帳カード”（C191）[*4] の 3 種類の ST およびサーバークライアント型のシステムドメインとして，“Intel SOA Expressway v2.7.0.4 and Intel SOA Expressway v2.7.0.4 for Healthcare”（1627）[*5] の ST を利用した．複数のドメインの ST から知識を抽出し，より汎用的なパターンの作成をできるようにする．**表 2** に作成した脅威検出パターンと，抽出元になった ST を示す．元になった ST に対応する数字が太字になっている．例えば，アクセス侵害の脅威検出パターンは，1627 の ST に 2 種類の該当脅威が存在したため，それらを元に検出パターンを作成し，脅威に対して 3 つの対策案が導出される．

提案手法では，ST に記述されている脅威のうち，利用シナリオ中の動作から検出できるもののみをパターンとして記述しており，前提条件や運用環境，システム構成等が原因となって発生するハードウェアへの物理的攻撃などの脅威については，シナリオ記述からは検出できないため対象の脅威から除外している．

[*3] http://www.ipa.go.jp/security/jisec/certified_products/c0229/c0229_st.pdf
[*4] https://www.ipa.go.jp/security/jisec/certified_products/c0191/c0191_st.pdf
[*5] https://www.commoncriteriaportal.org/files/epfiles/1627_ST-Version_1_9%20(2).pdf

表 2 作成した脅威検出パターンと抽出元の ST

脅威名	IC カード C251	IC カード C191	IC カード C229	Server 1627	合計	対策案数
アクセス侵害				**2**	2	3
コマンド悪用	**1**		1	1	3	4
盗聴	**2**	1	1	3	7	2
電源断	**1**	1			2	2
なりすまし	**1**	1			2	1
スキミング			**1**		1	1
覗き見			**1**		1	1
認証偽造			1	**2**	3	2
ハイジャック				**1**	1	2
対応脅威数	5	3	5	9	22	
ST 総脅威数	9	6	8	25	48	
カバー率	0.56	0.50	0.63	0.36	0.46	

5. 評価

提案手法が脅威検出及び対策手法として有用であるか，正しく機能するかを適用事例を用いて確認した．以下の 2 つの観点から評価する．

評価 1 提案手法によって，実際のシナリオから精度の高い検出と対策ができたか

評価 2 入力シナリオのドメインの差で検出性能に差が生じるか

適用事例として，対策がされていない利用シナリオを準備し，手法で定めた属性によってシーケンスを記述する．正解セットとして，対象シナリオに対し，セキュリティのエキスパートの手によって脅威の検出と対策の導出を行い，脅威の一覧と想定される対策を作成した．その後，対象シナリオに対して提案手法を適用し，脅威の検出と対策案の埋め込みを行う．そして，正解セットと出力された検出結果を比較する．

評価 1 のために，検出結果のうち，検出が上手く出来た脅威の数，人手で見落としていた脅威の数，検出できな

表 3 シナリオに想定された脅威種別と検出結果

ドメイン/シナリオ	説明	規模	検出結果			検出失敗	対策失敗
			想定内（正解）	想定外	誤検出		
IC カード/改札:入	駅に入るとき，カードの残高を確認し乗車駅を書き込む	9	盗聴 2, 電源断	スキミング		なりすまし	
IC カード/改札:出	駅から出るとき，カードの残高の引き落としを行う	15	盗聴 2, 電源断 2, スキミング 2			なりすまし 2	
IC カード/書類	ユーザーを PIN で認証し，カードのデータを用いて書類発行	14	盗聴 3, 覗き見	なりすまし, スキミング		コマンド悪用	
ショップ/入会	3 つの部分からなる．新規ユーザーが，サイトを開き，入会処理を行い，サイトを閉じる	18	盗聴, 覗き見	スキミング			スキミング
ショップ/注文	6 つの部分からなる．ユーザーがログインし，商品をカートに入れ，カートを確認し注文，配送を依頼し，ログアウト	32	盗聴 9, 覗き見 8, アクセス侵害 3	スキミング	なりすまし	コマンド悪用, なりすまし 2, アクセス侵害	
ショップ/管理者	2 つの部分からなる．管理者が専用サイトを開き，商品を追加	13	盗聴 2, 覗き見 2, ハイジャック			なりすまし, スキミング	ハイジャック

かった脅威をそれぞれ確認するとともに，人手による正解と見落としていた正解を合わせた真の正解の数を利用し，適合率，再現率，F 値を計算し，検出手法としての精度を確認する．また，手法で埋め込まれた対策が，想定された対策と同様であるかを確認する．

評価 2 のために，複数のドメインのシステムについて記述したシナリオを入力することで，手法の検出対策能力が対象ドメインによらない汎用的なものであることを確認する．

5.1 対象シナリオ

適用事例では知識源の ST と同様のドメインの IC カードを利用シナリオ及び知識源に利用した ST とは異なるドメインである，オンラインショッピングシステムのシナリオへの適用を行い，手法の検出能力の汎用性を確かめる．

IC カードドメインにおける例題として，過去研究 [1] で利用した 3 種類のシナリオを利用する．2 種類の IC カード改札システムのシナリオと，1 種類の自動書類発行システムのシナリオが存在する．

オンラインショッピングシステムのドメインにおける例題として，鈴木によって作成されたシステムのユースケース記述を利用する [6]．14 種類のユースケース記述を組み合わせ，入会，注文，管理者の商品追加の 3 シナリオを作成した．**表 3** に，利用したシナリオと規模 (メッセージ数，オブジェクト数) を記述する．

5.2 適用結果

表 3 に，実験で利用したシナリオと説明，検出結果を示す．脅威名の後ろの数字は検出数を示す．例えば，IC カードの改札入シナリオでは，想定されていた 2 つの盗聴と電源断の脅威が検出され，想定されていなかった妥当であるスキミングの脅威が検出された．また，想定されていたなりすましの脅威は検出されなかった，という結果になる．

表 4 検出の適合率と再現率

ドメイン	正解	検出	誤検出	適合率	再現率	F 値
IC カード	20	16	0	1.00	0.80	0.89
ショップ	35	30	1	0.97	0.83	0.89
合計	55	46	1	0.98	0.83	0.89

表 5 失敗とその原因

失敗	対象	原因
検出ミス	なりすまし	パターンとシナリオ記述のズレ
検出ミス	コマンド悪用	パターンとシナリオ記述のズレ
検出ミス	アクセス侵害	パターンのバグ
検出なし	認証偽造	対象シナリオに存在せず
誤検出	なりすまし	ログインの検出に失敗
対策失敗	ハイジャック	パターンのバグ
対策失敗	スキミング	対策挿入箇所のミス

5.3 分析

想定されていなかったが妥当な脅威が正解であったと仮定した場合，それぞれ適合率，再現率，F 値を計測した結果は**表 4** のようになった．

評価 1 結果として，想定されていなかったが妥当な脅威を正解に加えた場合，6 シナリオ合計の適合率が 0.98 と非常に高い値になった．再現率についても，0.83 と，高い値であるといえる．更に，2 つの値の調和平均である F 値は 0.89 となり，これも検出手法としては高い値であるといえる．

9 種類の脅威のうち盗聴，覗き見，ハイジャック，電源断は誤りなく検出された．残りはうまく検出が出来ないものがあった．検出や対策が失敗した原因について分析した結果，**表 5** に示す理由が判明した．原因は手法のプロセスではなく，検出パターンの問題，メッセージ属性の問題，シナリオの問題にあったと考えられる．

評価 2 IC カードドメインの 3 シナリオと，ショッピングサイトの 3 シナリオでは，それぞれ検出される脅威の種類は違っている．これは，IC カードのシナリオでは電源断の脅威が，UI を用いたやり取りの多いショッピングサイトのシナリオでは覗き見の脅威が多く発見されていることから確認できる．しかし, スキミングや盗聴のようなドメインによらない一般的な脅威については, どちらのシナリオでも検出されている．また, 精度の値では，どちらも再現率が 0.8 以上, F 値が 0.89 となっており, ドメイン差による極端な検出能力への影響はないと考えられる．なりすましの誤検出はショッピングシナリオでのみ発生したが, この誤検出はショッピングシナリオ中のログイン動作の記述方法が原因であり, 対象シナリオのドメイン差が直接の原因ではない.

5.4 結論

（評価 1）適用事例に対し適合率, 再現率共に高い値となったほか，パターンのミスを除き対策を埋め込めたため, 提案手法の検出能力の高さと有用性を示唆できる．

（評価 2）対象シナリオのドメインによらず提案手法は安定した精度で脅威検出，対策を行えたことから，提案手法の複数ドメインに対する汎用性が示唆できる．

6. 関連研究

セキュリティ機能要求獲得を支援する手法は多く存在する．例えば，ミスユースケース [7] やセキュリティユースケース [8] などのセキュリティ要求獲得のための記述法, そしてそれらを利用した SREP[9] などのセキュリティ要求獲得支援のためのプロセスが提案されている．しかし，これらはプロセスの提案であり, 人手によらない脅威の検出，対策案の導出を提案する手法ではない．Were らによる, CC の脅威を知識源として用いてユースケース図のアクターに属性を振ることで脅威を検出する支援手法 [10] や，瀧澤らによる，データフロー図や配置図の要素に属性をふることで脅威を検出する手法 [11], Beckers らによるプロブレムフレームを利用した脅威分析対策手法 [12] などが存在する．これらの手法は，図に属性を付加し，知識を用いて脅威を検出するアプローチという点では提案手法と同様であるが，対象とする図内の要素について，静的な特徴のみしか考慮していないという点が異なる．要素の静的な特徴は同じであっても，システムにおける動作の順序等の動的特徴によって脅威が発生する可能性がある．提案手法は利用シナリオとシーケンス図を用いることで，時間や動作の順序が関係した脅威を検出し，具体的なシナリオ例としてわかりやすく対策を提示できる．

7. おわりに

本稿では，システム利用シナリオから脅威を検出し，その対策案を提示する手法を提案した．提案手法では，ST から脅威の検出と対策の知識を抽出し，専用のシーケンス図で記述された利用シナリオとパターンとの比較によって脅威を検出し，ミスシナリオの形式で表示する．その後，SFC の組み合わせによって対策が埋め込まれたシナリオを表示する．提案手法を AGG ツールによって実現し，2 種類のドメインのシナリオについて汎用的かつ高精度な検出と対策が行えた．

今後の課題は，シーケンス図の記述，変換を一連で支援するツールを作成し，被験者実験によるさらなる手法の有用性と汎用性の確認，また，現在検出できない, システムの前提条件や構成から発生する脅威を検出するための，新たな情報の付加方法の考察である．

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] 阿部達也，林　晋平，佐伯元司：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，ソフトウェアエンジニアリングシンポジウム 2014 予稿集，pp. 206–207 (2014).
[3] Common Criteria : New CC Portal, `http://www.commoncriteriaportal.org/`
[4] 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).
[5] Taentzer, G.: AGG: A Graph Transformation Environment for Modeling and Validation of Software, *Proc. AGTIVE*, LNCS, Vol. 3062, pp. 446–453 (2004).
[6] 鈴木啓史：ユースケース記述の検査を目的とした状態遷移モデル生成の研究，東京工業大学工学部情報工学科学士論文 (2012).
[7] Sindre, G. and Opdahl, A.: Eliciting Security Requirements with Misuse Cases, *Require. Eng.*, Vol. 10, No. 1, pp. 34–44 (2005).
[8] Firesmith, D.: Security Use Cases, *J. Object Technology*, Vol. 2, No. 3, pp. 53–64 (2003).
[9] Mellado, D., Fernández-Medina, E. and Piattini, M.: Applying a Security Requirements Engineering Process, *Proc. ESORICS*, LNCS, Vol. 4189, pp. 192–206, (2006).
[10] Ware, M., Bowles, J. and Eastman, C.: Using the Common Criteria to Elicit Security Requirements with Use Cases, *Proc. IEEE Southeast Conference*, pp. 273–278 (2005).
[11] 瀧澤悠介，阪井隼也，海谷治彦，小形真平，海尻賢二：アセットフロー図と配置図を用いた情報システムのセキュリティ要求分析支援ツール，電子情報通信学会技術研究報告，Vol. 112, No. 496, pp. 31–36 (2013).
[12] Beckers, K., Heisel, M. and Hatebur, D.: Supporting Common Criteria Security Analysis with Problem Frames, *JoWUA*, Vol. 5, No. 1, pp. 37–63 (2014).