複数のステークホルダ観点に基づく脅威分析手法

大久保 隆夫 †

概 要

ソフトウェアシステムの要求分析における十分な脅威分析は必須であり，そのためには，単視点でのセキュリティ脅威の識別だけでは不十分で，エンドユーザのプライバシー保護など，システムに関わるステークホルダ全員の観点に立った脅威分析が必要である．本稿では，STRIDE など既存の脅威分類にはない，セキュリティ，プライバシー双方の要素を持つ，資産ベースの脅威モデル SPTM について述べる．また，SPTM モデルに基づき，複数のステークホルダ観点から脅威分析を行なう手法 TAMSA について説明する．また，SPTM および TAMSA によって，脅威分析の網羅性を高めることができることを現実のセキュリティ，プライバシー事例に対する分析によって示す．

1 はじめに

ソフトウェア開発におけるセキュリティは，開発の早期段階での対処が最もコストが少ないため，特に最上流である要求分析段階での脅威分析が重要とされている．セキュリティ要求分析手法については，現在までにいくつかの手法が提案されているが，具体的な脅威分析手法については，設計段階における脅威分析手法と比べて，充実しているとは言えず，設計段階の手法を流用しているのが現状である．近年起きているセキュリティ事故では，既存の脅威分類の問題や網羅性の欠除が原因になっていると考えられるものがある．

一方ビッグデータ分析の隆盛にともない，プライバシーの問題も顕在化している．2013 年に米政府が Google や Yahoo などのユーザの情報を収集していた PRISM 計画が明らかになり，大きな問題となった [1]．また，2013 年 6 月には JR 東日本が Suica 利用者の乗降履歴を同意なしに他社に販売していたことが発覚した [2]．プライバシーの問題は，脅威分析において，１アクター（システム提供者）視点での脅威しか識別されていないことが原因と考えられる．

本稿では，上述の問題を解決するため，次の２つの提案を行なう．

- セキュリティ，プライバシー双方の概念を持つ脅威モデル
- 複数のステークホルダ観点による脅威分析

†情報セキュリティ研究科 教授

[1] http://japan.cnet.com/news/service/35033099/

[2] http://internet.watch.impress.co.jp/docs/news/20130725_609129.html

提案する脅威モデルと脅威分析手法を用いることにより，利用者はセキュリティ，プライバシー双方を考慮した脅威分析を要求分析段階において行なうことが可能となる．また，システムに関わるすべてのステークホルダの観点での脅威を識別できるため，対策の網羅性が向上することが期待される．本稿では，現実の事例を用いて，提案モデル，手法の有効性の評価を行った．

提案モデルおよび手法はアーキテクチャとは分離可能な概念のため，ソフトウェア開発以外にも，セキュリティマネジメントやセキュリティポリシーの構築，検証，ソフトウェア運用にも応用が可能と考えられる．また，典型的なモデルをパターン化することで，分析作業の効率化が期待できる．

2　背景と研究のねらい

ソフトウェア開発において要求の変更が後工程になるほど高いため，開発の最上流，すなわちにおいて潜在する脅威を認識し，必要なセキュリティの導入を決定するセキュリティ要求分析は重要である．しかし，特に競争入札などで期間を設定された日本のシステム開発案件の要求分析課程においては，セキュリティ要求策定のための脅威分析は，手法の不足，知識（人材）の不足，時間的制約などの理由で，十分には行われていないのが現状である．我々は，上述のような制約の中でも，網羅性の高い要求レベルの脅威分析手法が必要と考える．要求レベルとは，要求分析段階で明確になっているアーキテクチャ仕様を前提とした抽象度の要求を指す．要求分析の手順は文献 [1] に提示されている下記の手順がよく用いられる．

1. 資産の識別
2. セキュリティゴール (目標) の設定
3. 脅威の識別
4. 脅威の評価
5. 対策の策定

本稿ではこのうち，3. の脅威の識別を対象とし，それ以外の手法 (資産の識別や脅威の評価) については対象としない．網羅性を向上させるためには，潜在する脅威を見落さないことが最も重要であると筆者らは考えるためである．また，セキュリティゴールは脅威が明確にならないと網羅的に設定することは困難と筆者らは考える．また，脅威とセキュリティゴールは一般に反対の関係にある (脅威を防ぐ/緩和する目的としてセキュリティゴールがある) ため，脅威の識別によって，セキュリティゴールは補完することができると考える．

3　関連研究

設計段階における脅威分析手法として知られているのが，脅威モデリング [2][3] である．脅威モデリングでは，分析者はまずソフトウェアをコンポーネントに分解し，コンポーネ

ント間のデータの流れをデータフローダイアグラム (DFD) を用いて記述する．次に DFD の中で，攻撃の対象になりうる箇所を抽出し，脅威の識別を行う．次に識別された脅威を脅威ツリーを用いて具体的に実現する手段に分解し，実現可能性の分析と影響評価を行う．

脅威モデリング手法自体は，DFD を必要とするように，ある程度設計段階が進みアーキテクチャ仕様が明確にならない要求分析段階には適用が困難である．

要求分析段階におけるセキュリティ要求分析については，様々な手法が提案されている [1] [4] [5] [6] [7] [8] [9] が，脅威を識別するための手法そのものについてはいずれの手法でも提示されていない．

ゴール指向やエージェント指向による手法 [6] [7] [8] [9] では，対策としてのゴールをいかに導出するかが問題となるが，脅威を先に識別し，そこからゴールを識別する場合は脅威の網羅性が，ゴールから脅威を導出する場合はセキュリティゴールの網羅性が問題となってしまう．

UML を拡張した手法にはミスユースケースを用いた分析 [1]，ミスユースアクティビティ [10] やマルアクティティビティ [11] などがある．ミスユースケースは UML のユースケース図に，意図しない挙動 (ミスユース=脅威) や関係するアクタ (ミスユーザ) の要素を追加し，脅威分析に用いるものである．ミスユースケースではその記法と，前述の分析手順を示しているが，脅威をどのように識別するかの手法は提供していない．大久保らは，ミスユースケースを拡張して資産とセキュリティゴールの要素を追加し，資産を基にした脅威分析手法 MASG を提案している [4] が，各資産に対する具体的な脅威識別には，例として脅威モデリングの脅威分類 (S:なりすまし，T:改ざん，R:否認，I:情報漏洩，D:DoS 攻撃，E:権限昇格）[3] を用いている．しかし，STRIDE は脅威が目的であるもの（T や I) と手段 (S や E) が区別されていないため，分析者は S(なりすまし）が具体的にステークホルダにどのような影響をおよぼすのか，直観的に理解しにくい．また，昨今のセキュリティ事件にも鑑みて，STRIDE は起きうる脅威を網羅できているとは言いがたい．たとえば，遠隔操作事件やメールの踏台による spam 攻撃などのように，ある機能が悪用されたり，踏み台になるような脅威を表現できていない．

また，ミスユースケースをはじめ，従来のセキュリティ要求分析手法は，単一的なステークホルダ（システムの提供者とほぼ同一）の観点からの脅威識別にとどまっている．このため，例えばエンドユーザに対する脅威（プライバシー侵害や，前述のエンドユーザのカード情報の漏洩) などの分析には適していない．

プライバシー保護の観点に立った研究は，上記のセキュリティ関係のものとは別に行なわれている．Deng らは，STRIDE に対応するプライバシー保護に基づいた脅威分類を提案している [12].

ソフトウェアを応用したセキュリティパターンは，セキュリティ要求や設計の典型的なカタログを提供するもので，セキュリティ知識に乏しい分析者でも，セキュリティ品質の高い要求や設計仕様を提供することが可能になることが期待される．脅威識別に関して，Web の機能や資産に着目して，典型的な脅威や対策をパターン化した Web セキュリティパターン [13] や，クラウドのパターン [14] などが提案されている．たたしこれらは Web やクラウドなど特定のアーキテクチャを対象としたものである．

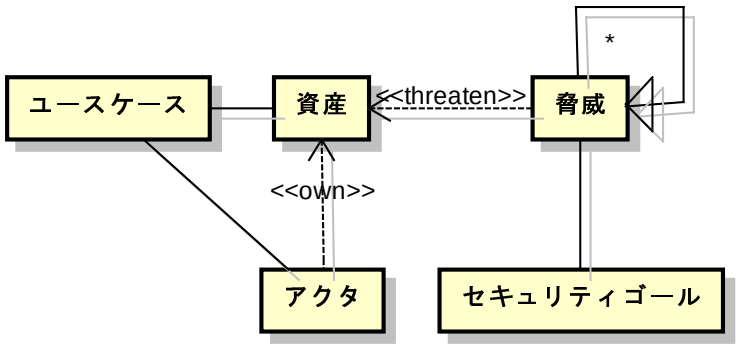

図 1: SPTM のメタモデル

4　脅威モデルおよび分析手法

本稿では，筆者が提案するセキュリティ，プライバシー双方の概念を含み，網羅性の高い脅威分類を含む脅威モデル SPTM(Security and Pricacy Threat Model)，および複数のステークホルダ観点に基づいて脅威分析する手法 TAMSA(Threat Analysis with Multiple Stakeholder Aspects) について詳細に述べる．

4.1　セキュリティ，プライバシー脅威モデル SPTM

提案するモデル SPTM のメタモデルを図 1 に示す．

このモデルは，大久保らの MASG[4] を拡張したものである．まず，文献 [1] などの，資産の識別から始まる脅威分析手順にならい，分析者が資産を識別することから脅威を分析しやすくするように，資産と，資産に基づく脅威を定義し，それらを関連づけた．なお，本稿では，SPTM の視覚的表現のために MASG の拡張記法を利用しているが，便宜上用いているのみで，本稿ではその視覚的効果による分析の効率性については提案の対象としない．本稿では，あくまでも SPTM のモデル構造のみを対象とする．

資産　文献 [1] などにあるように，資産の識別から始まる脅威分析手順にならい，分析者が保護すべき資産を識別することから脅威を分析しやすくするように，資産を定義している．

ユースケース　MASG では，ユースケースに資産を関連づけている．これは，分析者が先にユースケース分析を行った際に，ユースケースに関係する資産を導出しやすくすることを意図している．

アクタ　アクタは UML ユースケースに基づき，元々ユースケースに関連づけられているが，同時に資産についても資産の所有者である場合「own」という関連づけを SPTM では追加している．これは，ある資産に対する被害がどのアクタ（ステークホルダ）に対するものなのかを明確にするためである．

脅威　脅威は，MASG の記法に基づき，資産をおびやかす (threaten) ものとして，資産と関連づけられる．脅威は，脅威モデリング [3] の脅威ツリーの関係のように，根元と

なる脅威 (ルートの脅威) と，ルートの脅威を可能にする脅威とのツリーの関係 (メタモデルでは汎化の記法で表現) で構成される．SPTM においては，分析者の直観的の脅威認識を可能にするため，ルートの脅威は，特別にアクタへの直接的な被害に直結する脅威であるものと定義する．

セキュリティゴール MASG においては，セキュリティゴールは資産に関連づけられているが，MASG の適用実験をいくつか行った結果，セキュリティゴールと脅威が相反の関係にあり，より密接であることが分かってきた．例えば，情報漏洩という脅威と，情報の機密性 (confidentiality) を保持するというセキュリティゴールは相反の関係にある．また，文献 [1] では，セキュリティゴールを脅威より前に定義することになっているが，実験では脅威が明確になっていないと，セキュリティゴールを網羅的に定義することが困難であることも分かった．このため，SPTM では，脅威とセキュリティゴールを直接関連づけることにより，両者を相補的に導出することを可能とする．

4.2 SPTM による分析効率化のためのカタログ化，パターン化

セキュリティ知識に乏しい分析者でも，容易に脅威分析が行えるようにするため，資産や脅威のカタログ化，パターン化を進めることが必要になる．本稿では，システムを対象としたものに限らず，過去のセキュリティ事故の情報から，下記のカタログ，パターンを提案する．パターンはこれですべてではなく，下記に紹介するものを拡張して，多くの一般的な，あるいはドメインに特化したパターンを作成することが可能と考えられる．

資産のカタログ 資産のカタログの例を図 2 に示す．このカタログは，ソフトウェアシステムが内包する資産に限らず，一般的な社会活動において，セキュリティ被害にあう可能性のある資産を過去のセキュリティ事故事例に基づき列挙したものである．このように資産カタログを提供することで，分析者による資産の識別を容易にすることが可能となる．

また，このうち情報資産については，資産ごとに脅威が異なるため，より詳細化することがのぞましい．図 3 に，情報資産のカタログを示す．

資産単位の脅威分類 上記の資産カタログの資産（情報以外）ごとに，想定される脅威分類

および，対応するセキュリティゴールを列挙したものを図 4 に，また，情報資産について列挙したものを図 5 に示す．図中で，クラスは資産を，楕円のミスユースケースは脅威を表す．また，脅威は灰色で示しているが、赤色になっているものは被害に直結するルートの脅威を表す．

分析者は，資産を識別した時，図 4，5 を利用して，その資産に対応する脅威を導出することが可能になる．

ユースケースごとの脅威パターン システムの機能，あるいは人の活動の定義をユースケースとすると，様々なシステムや活動に共通のユースケースには，典型的に資産となり得る候補が存在する．したがって，あらかじめユースケースに想定される被害を

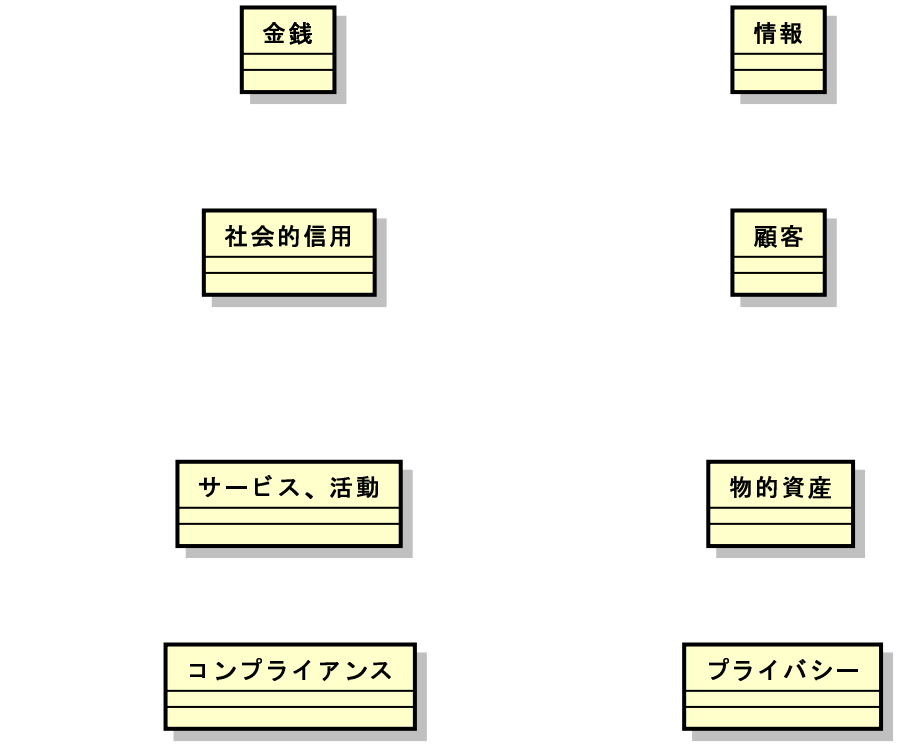

図 2: 資産のカタログ

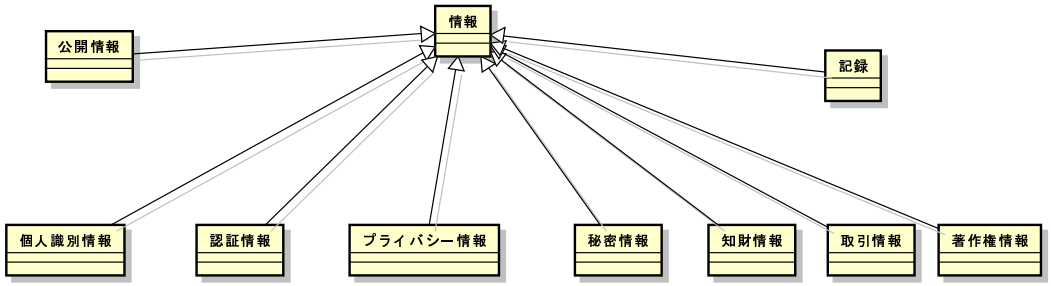

図 3: 情報資産のカタログ

資産を経由して関連づけたモデルをパターンとして用意しておくことで，あるユースケースに特徴的な脅威の候補を分析者が取得することができる．
また，更に，脅威の相反関係であるセキュリティゴールを脅威から導出し，モデルに追加しておくことで，分析者のセキュリティゴールの定義や検証を補助することが可能となる．情報提供者が自己の情報を誰かに提供するユースケースを例に，典型的な脅威を SPTM モデルを用いてパターン化した例を図 6 に示す．

脅威ツリーのパターン 脅威どうしの因果関係もまた，典型的なものはパターン化できる．なりすましの脅威ツリーパターンの例を図 7 に示す．STRIDE 脅威分類の S であるなりすましは，容易に想定はできるものの，具体的にどのような被害があるかが直観的に把握しにくい．

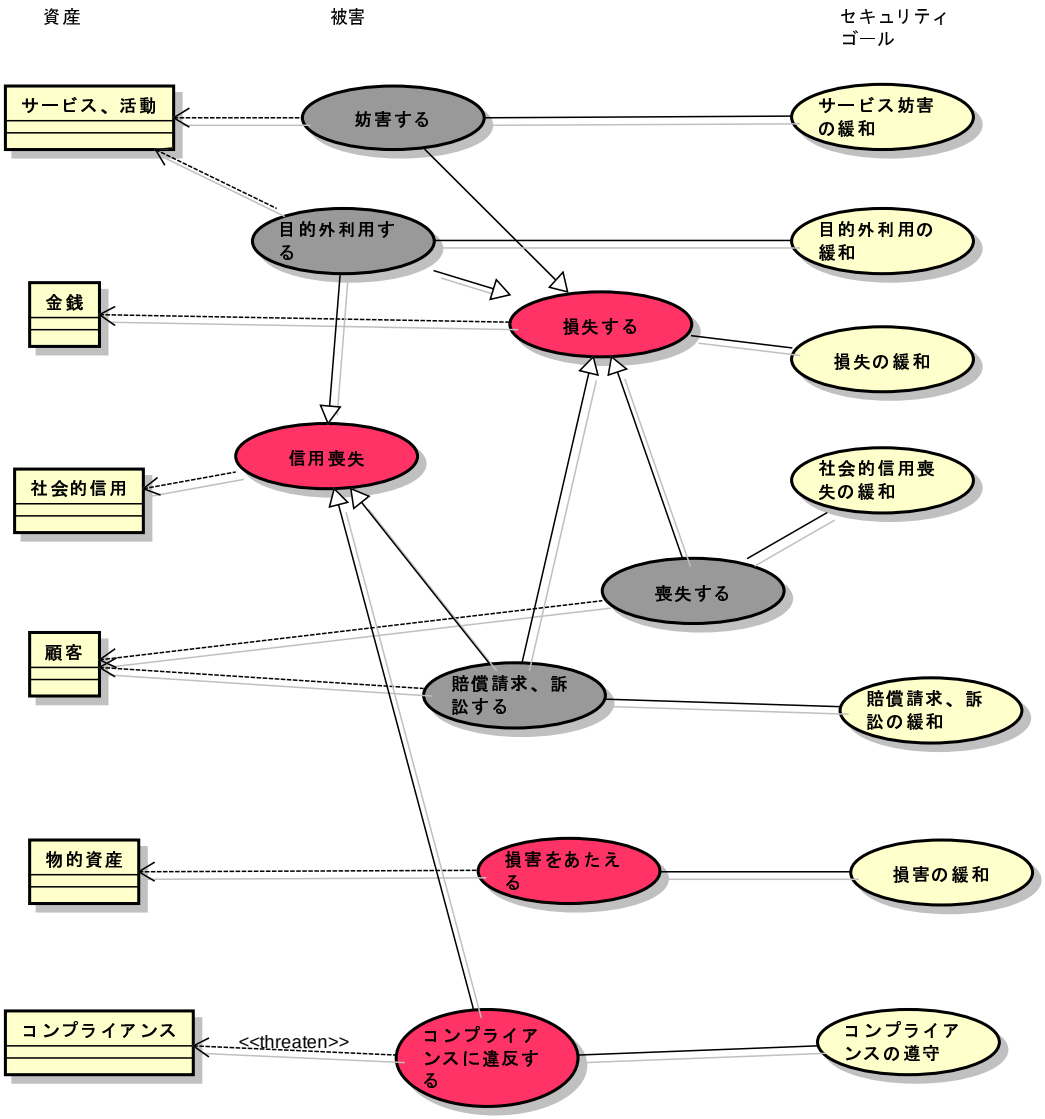

図 4: 脅威分類

Alice，Bob があるユースケースにかかわっている場合，第三者である Mallory が，Alice になりすますという脅威が想定される．このばあい ，なりすましによって，Alice と Bob がかかわっているユースケースが悪用される，あるいはユースケースに附随する資産が窃取，改ざんされる脅威が考えられる．したがってこの構造を図 7 のようにモデル化しておけば，分析者が先に「なりすまし」を識別した時には，その根元となる被害（「悪用，窃取，改ざん」）を導出できるし，逆に「悪用，窃取，改ざん」を先に識別した場合，その手段として「なりすまし」を導出できる．

4.3 複数のステークホルダ観点による分析 TAMSA

図 6 の脅威モデルは,「情報提供者」アクタにとっての,「第三者アクタ」による脅威を表

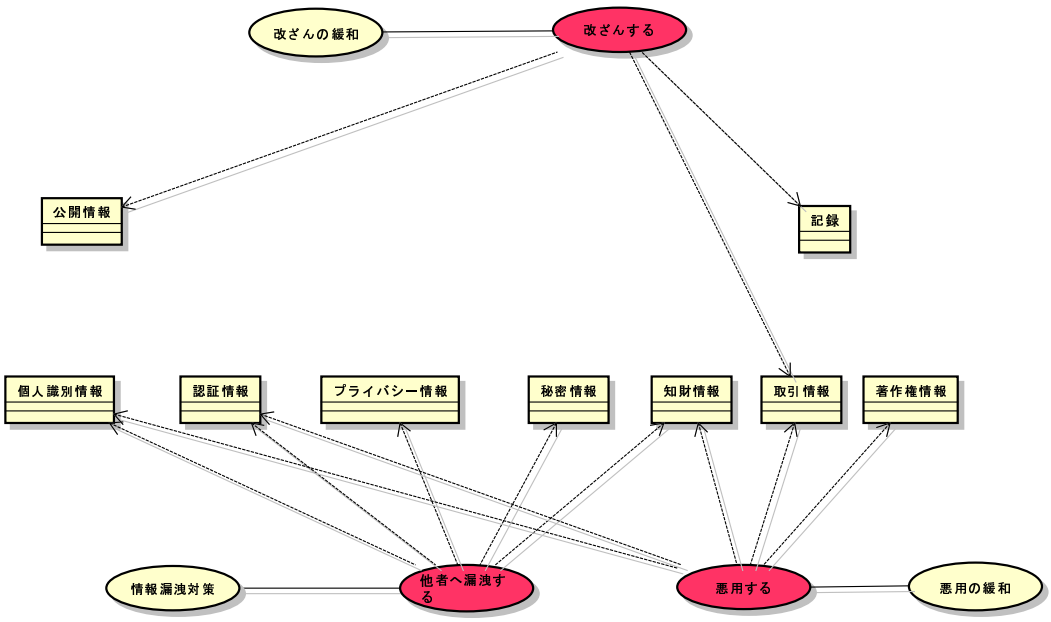

図 5: 脅威分類 (情報資産)

表 1: 脅威識別するアクタの組み合わせ (情報提供の例)

	被害対象アクタ	脅威を与えるアクタ
(1)	情報提供者	情報提供者
(2)	情報提供者	情報受信者
(3)	情報提供者	第三者
(4)	情報受信者	情報提供者
(5)	情報受信者	情報受信者
(6)	情報受信者	第三者

しているが，実際には脅威によって被害を受けるステークホルダはこの他にも「情報受信者」が該当する．また，脅威を与えるアクタも,「情報受信者」が与えるかもしれないし，別の「情報提供者」が脅威になる場合もある．提案手法 TAMSA は，まず最初にシステムや活動に関係するステークホルダをすべて識別したのち,「被害を受けるアクタ」「脅威を与えるアクタ」について識別したステークホルダのすべての組み合わせを作成し，すべての組み合わせについて脅威の識別を行なう．情報提供の例の場合，脅威識別を行なう組み合わせは表 1 の 6 通りとなる．なお，ステークホルダの組み合せにおいて，第三者が被害対象となる組み合わせは除外している．

図 6 の脅威モデルは，表 1 のうち，(3) の組み合わせで脅威識別した場合を示している．(2) の組み合わせで脅威識別した場合を図 8 に示す．図 6 とは異なる脅威 (「目的外利用する」および関連脅威) が現れていることがわかる．

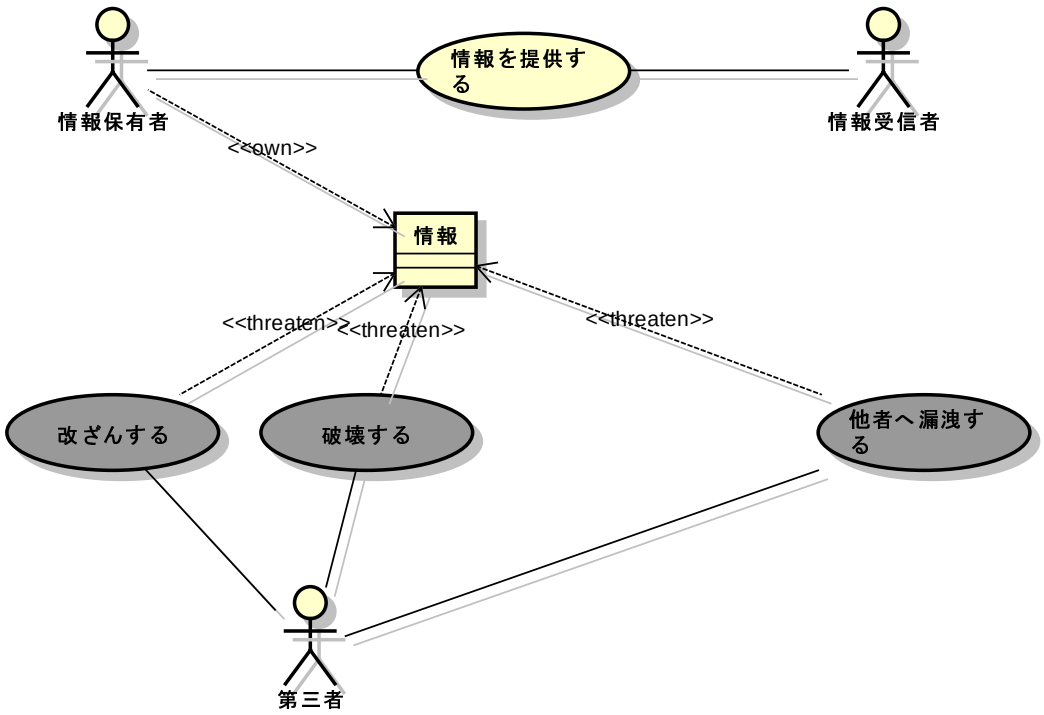

図 6: 情報提供の脅威パターン

4.4 アーキテクチャ情報を利用した脅威分析の詳細化

前項までは，アーキテクチャに依存しない形での脅威分析手法について述べた．しかし，要求分析においてもある程度のアーキテクチャ仕様 (システム構成，プラットフォーム，ネットワーク構成等) を想定することができる場合があり，その場合にはアーキテクチャ仕様を加味して，TAMSA による分析を進め，分析を詳細化することが可能になる．

- ステークホルダの追加
  アーキテクチャ仕様を追加することにより，アーキテクチャに依存するステークホルダを追加できる場合がある．例として，システムとしてクラウドを用いる場合を示す．クラウドを用いる場合では，クラウドアーキテクチャに依存して，図 9 に示すようなステークホルダが識別される．したがって，脅威識別を行なうステークホルダの組み合わせは最大で 30 通りとなる．

- アーキテクチャに依存するアタックサーフェスの発見
  アーキテクチャ仕様が明確になると，アーキテクチャをどのように情報などが流れるのかが明確になり，脅威モデリング [3] の DFD を用いた分析のように，攻撃のポイントとなるアタックサーフェスが識別可能になる．アタックサーフェスが識別されることで，そのポイントにおいてどのような具体的攻撃や脅威が可能になるか，詳細化が可能になる．この詳細化には，脅威モデリングの DFD や，ミスユースアクティビティ図 [10] の記述を用いることができる．ミスユースアクティビティによる

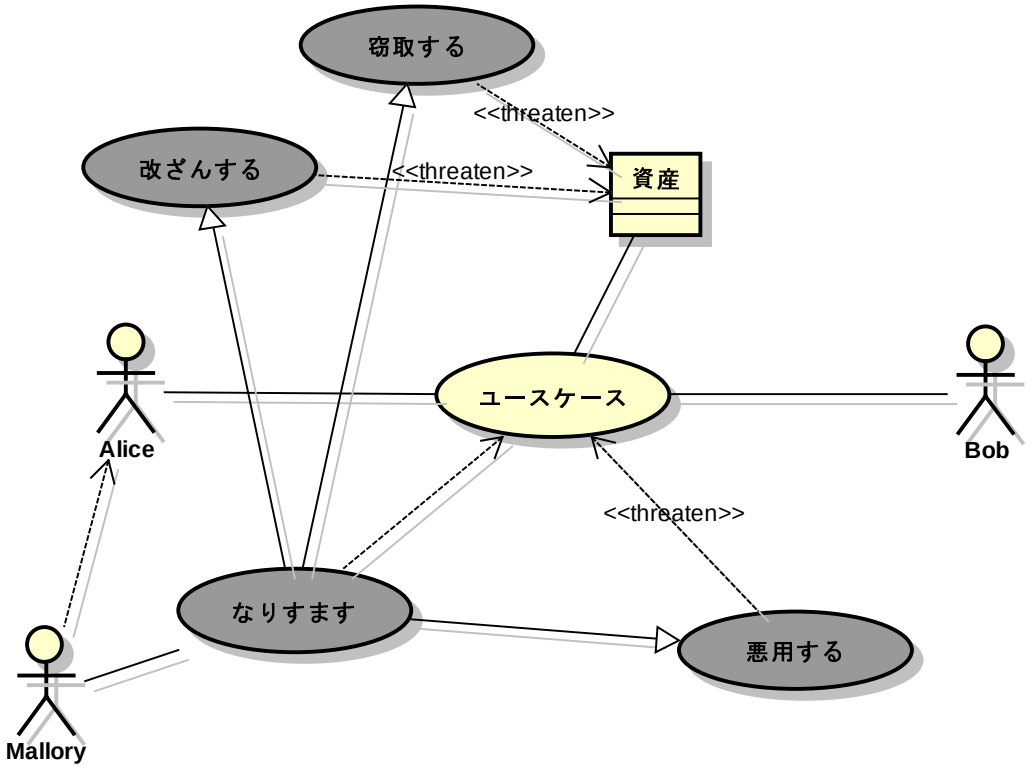

図 7: なりすましの脅威ツリーパターン

記述の例を図 10 に示す．例えば，クライアントからサーバにデータが送信される場合，その径路はアタックサーフェスとなり，盗聴される脅威が存在する．また，サーバ上ではデータストアにデータを格納しているが，データストアが狙われ，データが窃取される脅威も存在する．このように，アークテクチャと情報の流れを記述することで，脅威の詳細化が可能になる．

5　事例に基づく評価

提案する SPTM および TAMSA を 2 つの事例に適用し，以下について確認を行った．

- SPTM でプライバシーに対する脅威がセキュリティと統一的に表現できるか
- SPTM を用いて，典型的なセキュリティ問題を解決するパターンを記述できるか
- SPTM および TAMSA を用いた分析により，過去に起きたセキュリティ事故事例の脅威を要求レベルで識別できるか

5.1　プライバシー問題

ただしプライバシー保護に関しては，単純な情報漏洩だけでなく，文献 [12] が挙げている

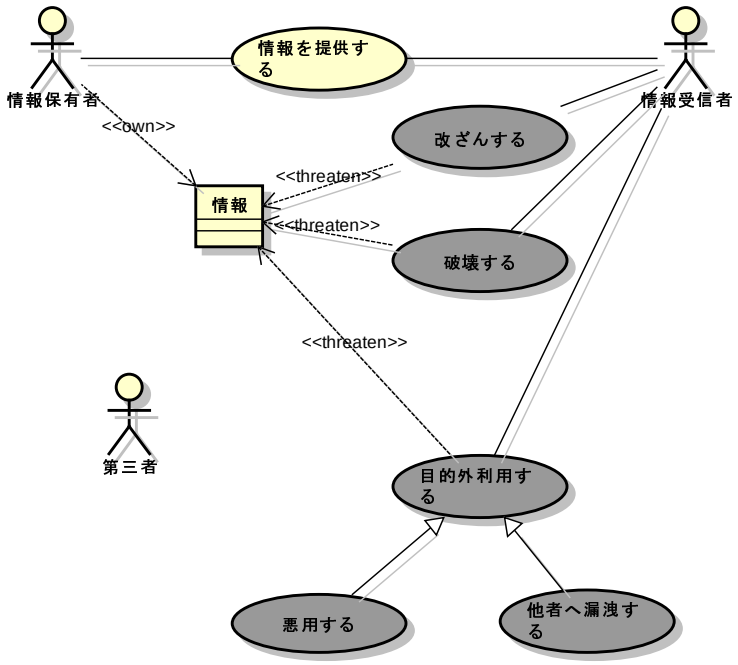

図 8: 情報提供の脅威パターン ((2) の組み合わせ)

ような匿名性 (anonimity)，仮名性 (pseudonymity) の確保，リンクされない (unlinkability)，行動を監視、追跡されない (undetectability，unobserbability，plausible deniability) といった概念がある．そこで，SPTM を用いて，これらの保護を抽象的な「プライバシー」という資産として図 2 の資産カタログに追加した．次に，名寄せやリンクなどの脅威をこの「プライバシー」資産への脅威として記述し，根元の脅威として「プライバシー侵害」を追加した．プライバシーにおける，資産と脅威，セキュリティゴールの関係を示した脅威分類を SPTM で記述したものを図 11 に示す．プライバシー保護には，コンプライアンス遵守の概念が不可欠である．日本であれば個人情報保護法などの法律やガイドライン，内規が存在する．そのため資産カタログに「コンプライアンス」を追加し，プライバシーの侵害がコンプライアンス違反の原因となることを関係性で示し，相反するセキュリティゴールとして「コンプライアンス遵守」を追加している．コンプライアンス遵守意識の高いステークホルダに対しては，この関係性を用いてプライバシー保護の重要性を認識させることができる．図 8 の情報提供の例で，情報がプライバシー情報であった場合のパターンを，図 11 のパターンを利用して記述したものを図 12 に示す．TAMSA 分析により，プライバシーの問題は主に情報提供者側を被害対象とした場合で検討されるものに包含できる．これらのパターンを用いることにより，プライバシーを含む脅威分析を，通常のセキュリティ脅威分析の一環として行なうことが可能になる．

5.2 グローバルデータのカード情報流出の事例

2013 年 5 月，エクスコムグローバル社の海外用データ通信レンタルサービス「GLOBAL DATA」，海外用レンタル携帯電話サービス「Global Cellular」（グローバルセルラー）の

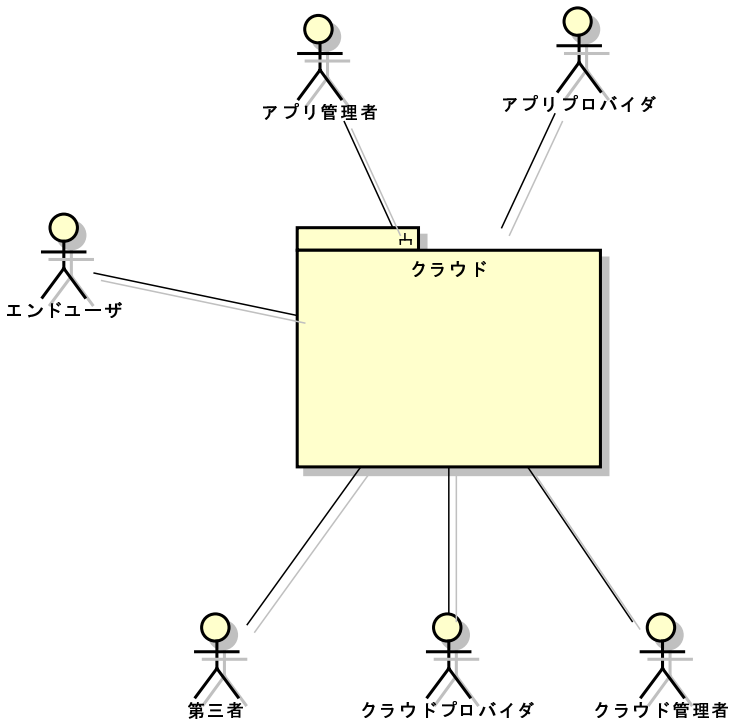

図 9: クラウドアーキテクチャにおけるステークホルダ

顧客情報（約 11 万件のクレジットカード情報およびセキュリティコード）を流出させるセキュリティ事故が発生した[3]．原因は Web サーバに対する SQL インジェクション攻撃であると発表された．

一般に，クレジットカード決済におけるクレジットカード情報やセキュリティコードの漏洩は，対策するアプリケーション提供者にとっての脅威が見えにくいという問題がある．カード情報などは顧客の所有物であるし，決済を承認するのは信販会社である．アプリケーション提供者は，データを信販会社に中継し，承認結果をもってサービスや商品の販売を行なうという構造になっている．従って，PCIDSS のように業界のセキュリティ標準の準拠の必要性がない場合を除き，データの流出そのものは，直接アプリケーション提供者の利害に影響しない．従来の単一視点による脅威分析を行っている限り，今後も対策が不十分になるおそれがある．

SPTM および TAMSA による多視点的な脅威分析を行えば，このような対策観点の漏れを防ぐことができる可能性がある．決済代行業者を用いたクレジットカード決済を SPTM で表現したモデルを図 13 に示す．このようにアプリケーション自身が決済を行わず，決済代行サーバにカード情報を転送して決済代行してもらう構成は，エクスコムグローバルの例に限らず，一般的によく行われている．

ここでは，アーキテクチャ仕様が Web と決まっているため，ステークホルダ「アプリケーション提供者」を追加している．TAMSA による分析により，エンドユーザを被害対

[3] http://www.itmedia.co.jp/news/articles/1305/27/news131.html

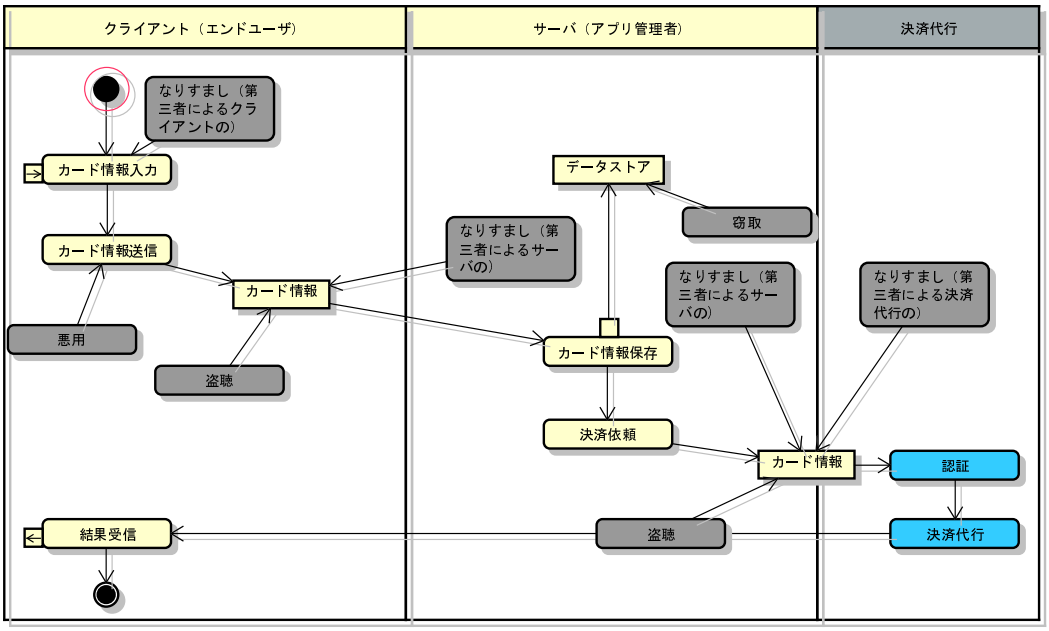

図 10: ミスユースアクティビティ図の例

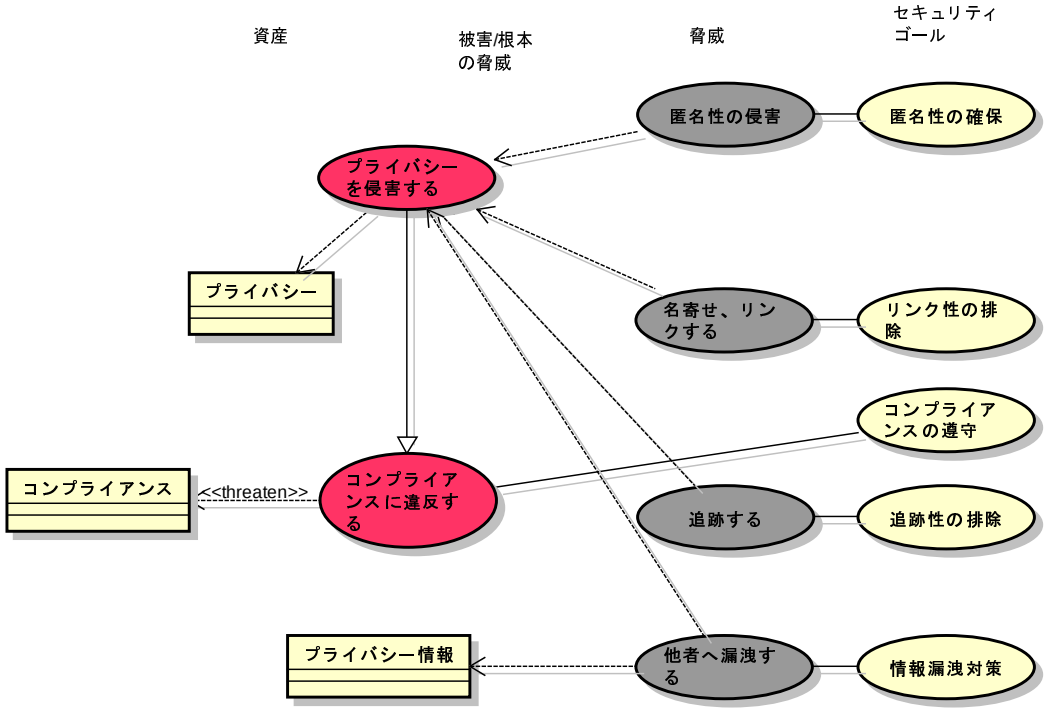

図 11: 脅威分類 (プライバシー)

象とした場合，カード情報に対し,「窃取」，決済サービスに対し,「悪用する」という脅威が識別できる．次に，脅威ツリーのパターンを利用すると，カード情報の窃取は決済サー

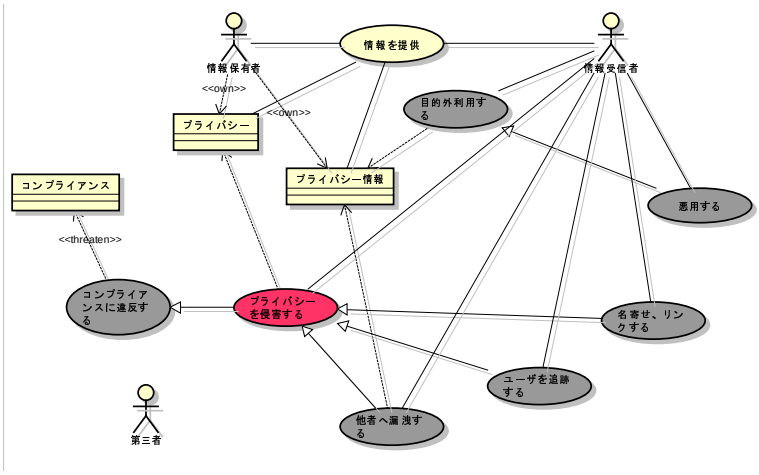

図 12: プライバシー情報提供の脅威パターン ((2) の組み合わせ)

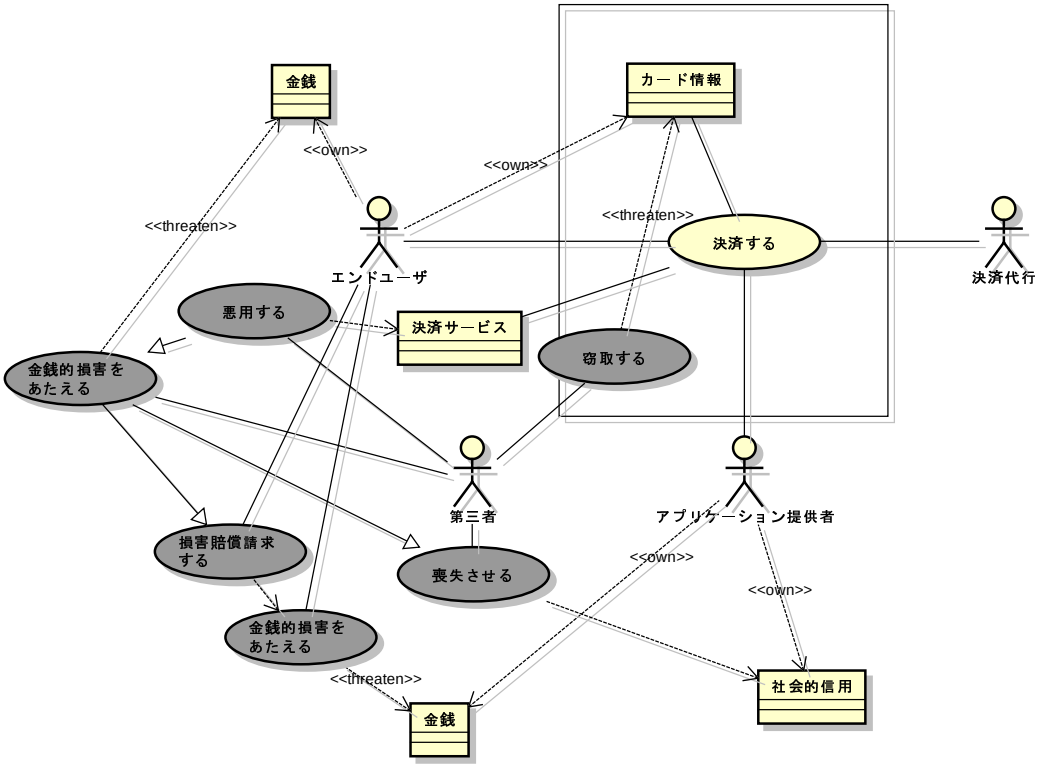

図 13: 決済の脅威モデル

ビスの悪用の原因となり，決済サービスの悪用はエンドユーザに金銭的損害をもたらす．更に脅威ツリーパターンを用いると，エンドユーザの金銭的被害は，アプリケーション提供者に対する損害賠償請求の原因となり，更に損害賠償請求がアプリケーション提供者の，社会的信用の損失および金銭的損害の原因となる．このように，単純にエンドユーザに対する脅威が識別できるだけでなく，それが他のステークホルダにも脅威になりうることもパターンを用いて示すことができる．

次に，決済のデータの流れを Web のアーキテクチャに基づいてミスユースアクティビティで記述したものが，図 10 である．ここではサーバのデータストアに一旦カード情報 (セキュリティコードを含む) を保存している．この構成では，サーバ上のデータストアにあるデータは，SQL インジェクションなどの攻撃により，窃取される脅威が存在することが分かる．実際に，エクスコムグローバルの例では，SQL インジェクションによりこのデータストアのデータが流出した．決済代行を用いる場合，カード情報は受け渡すだけで，データストアには保管しないという仕様もありうる．その場合，図 10 のミスユースアクティビティ上ではデータストアのアタックサーフェスがなくなるため，該当する脅威がなくなる．データフローの設計をする際に，ミスユースアクティビティのような脅威分析を行なうことで，識別されたアタックサーフェスを調整して，脅威の少ない仕様を設計することも可能になる．

6 おわりに

本稿では，筆者が提案する，従来のアプリ提供者以外の観点 (プライバシーや他のステークホルダ) を加えて分析を行なうことで，純粋に要求分析段階における脅威分析の網羅性を向上させる脅威モデル SPTM，および分析手法 TAMSA について述べた．また，提案モデルおよび手法を実際の事例に適用し，網羅性を向上させる可能性があることを示した．

本研究の成果は，以下の 2 分野の基盤となるものであり，今後の当該分野の研究に貢献できるものであると考える．

- 要求分析における作業を省力化し，品質を向上させるセキュリティパターンの構築
- 管理側だけでない観点を含むセキュリティマネジメント，セキュリティ運用のモデル化と検証

本稿では，資産，脅威などいくつかの観点でセキュリティパターンができる可能性を示した．しかし，これらのパターンの充分性や有効性，妥当性の検証は行っていない．分析におけう SPTM，TAMSA の有効性を確認するには，SPTM を用いたパターンの整備，評価が必要であるが，それらは今後の研究課題である．

参考文献

[1] Sindre, G. and Opdahl, A. L.: Eliciting security requirements with misuse cases, *Requir. Eng.*, Vol. 10, No. 1, pp. 34–44 (2005).
[2] Howard, M. and LeBlanc, D.: *Writing Secure Code Second Edition*, Microsoft (2003).
[3] Swiderski, F. and Snyder, W.: *Threat Modeling*, Microsoft Press (2004).
[4] Okubo, T., Taguchi, K. and Yoshioka, N.: Misuse Cases + Assets + Security Goals, *CSE (3)*, IEEE Computer Society, pp. 424–429 (2009).
[5] C.B.Haley, R.Laney, J.D.Moffett and B.Nuseibeh: Security Requirements Engineering: A Framework for Representation and Analysis, *IEEE Trans. Software Eng.*, Vol. 34, No. 1, pp. 133–153 (2008).
[6] Letier, E.: Reasoning about Agents in Goal-Oriented Requirements Engineering, PhD Thesis, Universite catholique de Louvain (2001).

[7] van Lamsweerde, A.: Elaborating Security Requirements by Construction of Intentional Anti-Models, *Proceedings of the 26th International Conference on Software Engineering*, ICSE '04, pp. 148–157 (2004).
[8] Liu, L., Yu, E. and Mylopoulos, J.: Security and Privacy Requirements Analysis within a Social Setting, *Proceedings of the 11th IEEE International Conference on Requirements Engineering*, pp. 151–161 (2003).
[9] Mouratidis, H. and Giorgini, P.: Secure Tropos: a Security-Oriented Extension of the Tropos Methodology, *International Journal of Software Engineering and Knowledge Engineering*, Vol. 17, No. 2, pp. 285–309 (2007).
[10] Braz, F., Fernandez, E. and VanHilst, M.: Eliciting Security Requirements through Misuse Activities, *Database and Expert Systems Application, 2008. DEXA '08. 19th International Workshop on*, pp. 328–333 (2008).
[11] Sindre, G.: Mal-Activity Diagrams for Capturing Attacks on Business Processes, *REFSQ*, pp. 355–366 (2007).
[12] Deng, M., Wuyts, K., Scandariato, R., Preneel, B. and Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements, *Requir. Eng.*, Vol. 16, No. 1, pp. 3–32 (2011).
[13] Okubo, T. and Tanaka, H.: Web security patterns for analysis and design, *Proceedings of the 15th Conference on Pattern Languages of Programs*, PLoP '08, pp. 25:1–25:13 (2008).
[14] Hashizume, K., Fernández, E. B. and Yoshioka, N.: Misuse Patterns for Cloud Computing, *SEKE*, Knowledge Systems Institute Graduate School, pp. 683–686 (2011).