アクタ関係表に基づくセキュリティ要求分析手法（ＳＡＲＭ）の改良提案

†金子　朋子　　‡山本　修一郎　†田中　英彦
所　属† 情報セキュリティ大学院大学　所　属‡ 名古屋大学

１．　はじめに

攻撃シーンごとにセキュリティ要求を網羅的に表形式で分析できるアクタ関係表に基づくセキュリティ要求分析手法（ＳＡＲＭ）[1]を提案した。本稿では次に示すＳＡＲＭの課題について考察する。

① 適用対象・使用方法と成果物の明確化
② 要求定義工程での利用例の具体化
③ 一般者と攻撃者のゴールとソフトゴール、タスク、資源に対する表現の構造化
④ 設計工程の抽出対象の具体化

２．適用対象者・使用方法

適用対象者はユーザとセキュリティ設計者とシステム開発担当者である。

ＳＡＲＭの使用方法はシステム開発の上流工程において、一般の要求分析をシステム開発担当者が作成する。次にセキュリティ設計者がＳＡＲＭとして攻撃内容を付加する。ユーザとセキュリティ設計内容について合意する。但し、セキュリティ機能要件のみの記述も利用可能としている。

３．　成果物の明確化

文献[1]ではＡＡ表とＳＡＲＭ__Ａ表のみを提案した。本稿では、ＳＡＲＭ__Ｂ情報、ＳＡＲＭ__Ｃ表、ＳＡＲＭ__Ｄ表を追加提案する。

3-1　ＡＡ（Asset×Attack）表

ＡＡ表は攻撃シーンごとに守るべきアセットを特定することを目的として、守るべきアセットと攻撃の組み合わせを整理した表である。

要求定義工程で利用するレベルに絞り込むため、ＡＡ表を用いてSTRIDE単位で攻撃と守るべきアセットを特定できる表に改良する。攻撃とアセットの組み合わせに応じて、よりセキュアなシステムを実現できる。マイクロソフトが定義するSTRIDEモデルとは、Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information disclosure（情報の漏えい）、Denial of service（サービス拒否）、Elevation of privilege（特権の昇格）の６種に脅威分類したものである。STRIDE単位でＳＡＲＭ__Ａ表を作成することにより、要求定義工程レベルで、抜け漏れのなくかつ細かすぎないセキュリティ要求分析ができる。

表3-1　ＡＡ（Asset×Attack）表の事例

攻撃方法	種別	COOKIE情報	セッションID	パスワード	個人情報	SARM_A	SARM_B	SARM_C	SARM_D
なりすましによる不正注文	S	○	○	○	○	A_S	B_S	C_S	D_S
注文情報の改竄	T		○	○	○	A_T	B_T	C_T	D_T
商品注文への否認	R				○	A_R	B_R	C_R	D_R
情報の漏えい	I	○	○	○	○	A_I	B_I	C_I	D_I
システムへのDos攻撃等	D	○	○			A_D	B_D	C_D	D_D
管理人への権限昇格	E	○				A_E	B_E	C_E	D_E

→SARM作成単位

3-2　ＳＡＲＭ__Ａ(Attack)表

ＳＡＲＭ__Ａ表は攻撃者、悪意、攻撃方法、脆弱性の特定を行うことを目的として、ＡＡ表で抽出した攻撃シーン単位で作成し一般アクタに、攻撃者を追加したアクタ関係行列[1]である。ＳＡＲＭ__Ａ表、ＳＡＲＭ__Ｃ表、ＳＡＲＭ__Ｄ表の３つのアクタ関係行列では、一般者と攻撃者のゴールとソフトゴール、タスク、資源に対する表現の構造化を実施している。

表現の構造化は、①各マークを○ゴール、☆ソフトゴール、◇タスク、□資源のように前置すること。②一般者は白抜きのマーク、攻撃者は黒塗りのマークを使用すること。③タスク間の関係は＆：論理積（and）か｜：論理和(or)を前置し、構造化することで表現される。又、攻撃者の目標・意図・タスクを明確にするため、攻撃者欄を灰色に塗りつぶすことにした。

表3-2の例で説明すると、攻撃者EVEの脆弱性のあるシステムBOBに対する意図は攻撃者EVEの行の脆弱性のあるシステムBOBの列に表現さ

Improvement Proposal of a Security Requirements Analysis Method based on "Actor Relationship Matrix"
Kaneko Tomoko†　Yamamoto Shuichiro‡　Tanaka Hidehiko†
† Institute of Information Security　‡Nagoya University

れる。★ALICEになりすましてBOBのシステムで商品を注文したいという意図のもとに、◆ALICEのｾｯｼｮﾝIDを盗むというタスクと◆ALICEになりすまして、商品の注文をするという２つのタスクを実施するので、&が前置される。◆ALICEのｾｯｼｮﾝIDを盗むという攻撃より守るべき資源としては■ -- COOKIE情報があり、資源が攻撃者のゴール、ソフトゴールに対してどの程度の脆弱性を持つかをｉ＊のLiu法[2]に準じて－－、－、未記入の３段階レベルで表示する。これにより脆弱性のレベルの特定をはかることができる。◆ALICEのｾｯｼｮﾝIDを盗むというタスクは、◆Script Insertionか◆HTTPレスポンス攻撃か◆XSSという３つの攻撃方法のいづれかで可能であるので｜が前置される。又、脆弱性のあるシステムBOBは自システム内に◆ALICEのCOOKIE情報をEVEに送信というＸＳＳの脆弱性をもつので、意図しないで加害者の攻撃に加担してしまうXSSの特殊状況をBOB行とBOB列の対角欄に表現でき、この部分は灰色に塗りつぶされる。

表3-2　ＳＡＲＭ__Ａ(Attack)表の事例

	利用者ALICE	脆弱性のあるシステムBOB	攻撃者EVE
利用者ALICE	☆色々なサイトを閲覧したい □COOKIE情報	☆BOBのサイトを閲覧したい &◇BOBのサイトのトップページにアクセスする &◇ログインをする	☆EVEのサイトを閲覧したい ◇BOBのサイトにログインしたままEVEのサイトをクリックする
脆弱性のあるシステムBOB	☆正当な利用者にアクセスさせる	&○利用者情報を保護する □利用者情報 &○利用者ごとの管理をする &◇許可された利用者に情報へのアクセスを許可する □認証データ &◇ALICEにセッションIDを割り当てCOOKIE情報を通知する &○COOKIE情報を管理する □ -- COOKIE情報 &○商品の販売をする ｜◆XSSの脆弱性によりALICEのCOOKIE情報をEVEに送信 ■--XSSの脆弱性	☆正当ではない利用者にはアクセスさせない ◇偽造された認証データの使用を検知または拒否する 意図しないで加害者に攻撃に加担してしまうXSSの特殊状況を表現できる
攻撃者EVE	★ALICEにEVEのサイトをクリックさせたい ◆利用者ALICEにEVEのサイトをクリックさせる	★ALICEになりすましてBOBのシステムで商品を注文したい &◆ALICEのｾｯｼｮﾝIDを盗む ■--COOKIE情報 ｜◆Script Insertion ｜◆HTTPレスポンス攻撃 ｜◆XSS &◆ALICEになりすまして、商品の注文をする	★ALICEになりすましてBOBのシステムで商品を注文し、商品を手に入れたい &◆Cookie情報窃盗スクリプトを起動 &◆Cookie情報内のｾｯｼｮﾝIDを利用する

3-3　ＳＡＲＭ__Ｂ（Base）情報

ＳＡＲＭ__Ｂ表は攻撃方法や対策案の根拠を明確にして、ユーザの理解を助けることを目的として、ＳＡＲＭ__Ａ表に示された攻撃方法の補足説明や対策の根拠を示す情報である。シーケンス図等で補足説明する。

3-4　ＳＡＲＭ__Ｃ（Countermeasure）表

ＳＡＲＭ__Ｃ表は、攻撃者に対する対策案の特定を行い、ユーザに提示することを目的としてＳＡＲＭ__Ａ表で抽出した攻撃者のタスクに対して効果レベルと共に攻撃に対する対策案を記述するアクタ関係行列である。

①攻撃者のマークが存在するｎ行ｍ列に攻撃のタスク◆に対する対策→を記入し、その対策が攻撃に対して果たす効果を→の後に++、+、未記入（+-0）として付与する。

◆タスク→効果　対策名：根拠ＩＤ

◆Ｔ→＋ＣＭ：ＩＤ

アクタに対する対策案の中で、効果を参照し、効果の大きいものから、実施できるように実施対策の検討の際に本表を用いる。更に根拠ＩＤ単位に対策一覧表を作成し、実施する対策を絞り込み、ユーザとの合意を得るために使用する。

表3-4　ＳＡＲＭ__Ｃ(countermeasure)表の事例

	利用者ALICE	脆弱性のあるシステムBOB	攻撃者EVE
利用者ALICE	☆色々なサイトを閲覧したい □COOKIE情報	☆BOBのサイトを閲覧したい &◇BOBのサイトのトップページにアクセスする &◇ログインをする	☆EVEのサイトを閲覧したい ◇BOBのサイトにログインしたままEVEのサイトをクリックする
脆弱性のあるシステムBOB	☆正当な利用者にアクセスさせる	&○利用者情報を保護する □利用者情報 &○利用者ごとの管理をする &◇許可された利用者に情報へのアクセスを許可する □認証データ &◇ALICEにセッションIDを割り当てCOOKIE情報を通知する &○COOKIE情報を管理する □ -- COOKIE情報 &○商品の販売をする ｜◆XSSの脆弱性によりALICEのCookie情報をEVEに送信 ■--XSSの脆弱性	☆正当ではない利用者にはアクセスさせない ◇偽造された認証データの使用を検知または拒否する タスクと対策と効果の記入
攻撃者EVE	★ALICEにEVEのサイトをクリックさせたい ◆利用者ALICEにEVEのサイトをクリックさせる	★ALICEになりすましてBOBのシステムにアクセスしたい &◆ALICEのｾｯｼｮﾝIDを盗む ■--COOKIE情報 ｜◆XSS ---サニタイズ：S-1｜++入力検証：S-2 ｜URI設定 ＋S-3｜+SSL利用：S-4 ｜+最新の対策：S-5 ｜◆Script Insertion+++ サニタイズ：S-6｜監視：S-7 ｜◆HTTPレスポンス攻撃 ---サニタイズ：S-8｜++セッション指定変更：S-9 &◆ALICEになりすまして、商品の注文をする	★ALICEになりすましてBOBのシステムで商品を注文し、商品を手に入れたい &◆Cookie情報窃盗スクリプトを起動 &◆Cookie情報内のｾｯｼｮﾝIDを利用する

3-5　ＳＡＲＭ__Ｄ(Design)表

ＳＡＲＭ__Ｄ表はユーザと合意した対策を記表し、設計につなげることを目的として、ユーザと合意の上、実施する対策のみを記入するアクタ関係行列である。ＳＡＲＭ__Ｄ表では、灰色に塗られていた攻撃者ＥＶＥの行で攻撃者ＥＶＥのセル以外の塗りつぶしが消える。これはＳＡＲＭ__Ｃ表で挙げられていた対策案のうち、ユーザと合意のとれた実施する対策で、実際に設計するタスクのみを記入し、設計工程の抽出対象の具体化を実施しているからである。

４．　まとめ

本手法はｉ＊のLiu法で作成するモデルを表現可能であり、更に以下の利点をもつ手法である。①表形式で作成しやすい②表形式で関係性を検証していくのでアクタ関係の完全性が向上する。③タスク間の関係をandとorの構造化で表現し、ゴール指向の特長を備えている。アクタ数は限られているので表の大きさが無意味に大きくなることはない。ｉ＊のLiu法との比較・評価について今後も研究していく予定である。

<参考文献>

[1]金子　朋子, 山本　修一郎, 田中　英彦, アクタ関係表に基づくセキュリティ要求分析手法（ＳＡＲＭ）の提案, 2009, P721, CSS2009

[2] Liu他, “Security and Privacy Requirements Analysis within a Social Setting”, RE2003