Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

システムモデルによる機密性評価手法の提案

伊豆倉さやか† 榊啓† 矢野尾一男†

IT 技術の発展に伴い，機密情報の漏洩などのセキュリティ事故が多発している．このような事態を未然に防ぐためには，システムの設計段階で機密性を検証する必要がある．しかし，システムの大規模化・複雑化に伴い，IT システムの開発工数は増大しているため，できるだけ効率的な検証を行うことが望まれる．このような課題を解決するためには，あらかじめシステムをモデル化して，そのモデルを評価しておくことが有効であると考えられる．本稿では，統一モデリング言語（UML）をベースにしたシステムの設計図に対して，機密性に関する情報を表す属性を付与することで，機密性を評価するためのモデルを構築する手法を提案する．このモデルを用いることにより，システムの設計段階において，機密性を見積もることが可能となる．

Security Evaluation Method using the System Model

Sayaka Izukura† Hiroshi Sakaki† Kazuo Yanoo†

With the developments in Information Technology, there happen many security accidents such as information leak. To prevent such cases, it is necessary to verify the security level of the systems at the design phase. However, since IT systems are becoming larger scale and getting complex, efficient validation methods are demanded. To solve this problem, it is effective to model the systems and evaluate the model in advance. We propose a security evaluation method by annotating security semantics to the "System Model" written in Unified Modeling Language (UML). By applying this method, it becomes possible to estimate security level of systems at the design phase.

† NEC サービスプラットフォーム研究所

1. はじめに

インターネット技術の発展に伴い，情報資産の価値が高まると共に，企業の内部情報や顧客の個人情報などの漏洩事故が多発している．セキュリティ事故を未然に防ぐためには，設計段階でシステムの機密性を検証できるようなシステム開発を行う必要がある．さらに，システムの大規模化・複雑化に伴い，システム開発に要する工数は増大しており，工数を大幅に増やすことなく効率的に検証できる方式が求められている．

このような課題を解決するためには，あらかじめシステムをモデル化しておき，設計段階において機密性を見積もることが有効であると考えられる．このようなモデルベースのシステム開発の手法はいくつか提案されているが，複雑なモデルを事前に用意する必要があるため，一般の IT システムの機密性の評価に適用されている例は少ない．

そこで我々は，UML で記述されたシステムの設計情報（システムモデル）に対して，機密性に関するアノテーションを付与していくことで，資産に対する攻撃の流れを表すモデルを生成し，機密性を評価する手法を提案する．これにより，評価対象のシステムで，設計時点でのリスク対策が適切に行われていることを示すことができる．

本稿は次のように構成される．まず第 2 節で，この種の従来技術とその課題についてまとめる．次に第 3 節で，機密性評価モデルの生成に用いる「システムモデル」について紹介する．第 4 節では，このシステムモデルから機密性評価モデルを生成し，機密性の評価を行う方法を説明し，簡単なシステムに対して本手法を適用した例を示す．最後に第 5 節で，まとめと今後の課題について述べる．

2. 従来技術

システムの機密性を評価する方法としては，国際標準である ISO/IEC 15408 などで指定されたフレームワークに基づいて，システムが満たすべき様々な要件をリストアップし，チェックしていくという分析方法が一般的である．このような分析によって，定められた機密性要求を満たしているかをチェックすることができる．しかし，社内の運用ポリシーなどを反映させた独自のチェックリストを作成するのは，手間がかかるという問題がある．また，システムの構成や動作，攻撃と対策との対応関係などについて詳しく理解している専門家が，その知識に基づいてチェック項目を作成する必要があるため，構成や動作などに関する情報は，リスト作成者によってチェック項目の中に落とし込まれている．そのため，客観的な分析が難しく，また，実際にチェックを行う評価者には，システムの構成や動作などに関する知識がないため，対策の必要性がわかりにくいという問題がある．

Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

客観的に機密性を評価するためには，モデルベースの検証が有効である．すなわち，システムの構成や通信の様子などをあらかじめモデル化しておき，それを用いてシステムの設計段階で機密性を評価するという方法である．システムの構成情報や，攻撃知識を基に検証する方式として，アタックグラフ[1)2)]や，LPAS[3)]などがある．アタックグラフは，ある脆弱性とそれに起因する脅威の関連性から，最終的な脅威に繋がるような攻撃が可能であるかを分析するものである．また LPAS は，設定されているポリシーとシステムの設定情報から，機密データが漏洩する経路を分析している．しかし，これらの技術では，システムの物理的な構成情報などをあらかじめ考慮した上で評価用のモデルを構築しているため，評価者にとって，そのモデルが構築された背景がわかりづらい．このような構成情報は，システムの設計時に，システムエンジニア（SE）によって記述されるものである．記述方法としては，UML（Unified Modeling Language）[4)]などのモデリング言語が用いられることが多い．

UML は，OMG（Object Management Group）によって標準化されているモデルの統一表記法である．主にソフトウェアの設計時に利用するために作られたモデリング言語であるが，その他の様々なシステムのモデル化に用いようとする試みも行われている．例えば，UML を拡張して，システムエンジニアリング向けの汎用モデリング言語として特化させた SysML（System Modeling Language）[5)]や，Quality of Service（QoS）というコンセプトなどもモデル化の対象に含めた MARTE（Modeling and Analysis of Real Time and Embedded Systems）[6)]というプロファイルなどが提案されている．このようなモデリング手法をセキュリティ分野に適用したものとして，UMLsec[7)]や SecureUML[8)]などがある．これらの技術では，セキュリティ分野に特化した独自プロファイルを用いてセキュリティ要件をモデル化しており，状態遷移を含むような認証パターンの検証も可能である．しかし，認証パターンなどをモデル化するためには，製品そのものの動作を分かっている必要がある．また，モデル自体が複雑なものとなることが多いため，本方法を一般的な SE が実施することは難しい．文献 9)では，UML を用いてプロテクションプロファイルをモデル化している．これにより，国際的なセキュリティ基準である ISO/IEC15408 を満たすシステム設計を支援し，システムに施されているセキュリティ対策を利用者が理解しやすい形で具体的に示すことが可能となる．しかしこれは，セキュリティ要求を満たすための認証機構をモデル化したもので，それらの認証機構が適用されている機器同士の接続関係や通信プロセスなどは考慮されていない．一方，一般的な SE は，様々なセキュリティ機能が正しく実装されている製品を組み合わせてシステムを設計するため，個々の製品ではなく，複数の製品の組み合わせが，必要なセキュリティ要件を満たしているかを検証する必要がある．

以上のように，従来技術においては，分析に必要となるモデルの作成に手間がかかる上に，客観的な評価を行うことが難しい．また，セキュリティ機能が導入されている機器がどのような構成で接続されているかを考慮しなければ，実際のシステム開発の現場で利用するには不十分である．

そこで本稿では，これらの課題を解決するために，システム開発の際に記述されるシステムの設計情報（システムモデル）を利用し，それとは独立に用意されているセキュリティに関する知識をシステムモデルに与えていくことで，そのシステムに対する攻撃の流れを表すモデルを生成することを提案する．このモデルを用いることで，効率的かつ一般の SE にも理解しやすい機密性の評価を行うことができる．

3. システムモデル

本節では，機密性評価モデルの生成に用いられるシステムモデルについて紹介する．我々が提案しているシステムモデルとは，SysML を IT 分野に特化させた拡張記法によって，IT システムを記述した設計図である．プラットフォームの処理形態ごとに，ハードウェア／ソフトウェアレベルの構成，処理の流れなどが記述されており，個別案件のシステム設計を行う際の雛形として利用される．システムモデルは，様々な側面からシステムを記述した，レイヤの異なる複数のモデルから構成されるが，ここでは，機密性評価モデル生成のために必要となるモデルのみを紹介する．

3.1 物理モデル

システムの物理的な構成要素（機器）と，その接続関係を表すモデルである．SysML の内部ブロック図で記述する．以下に物理モデルの例を示す．

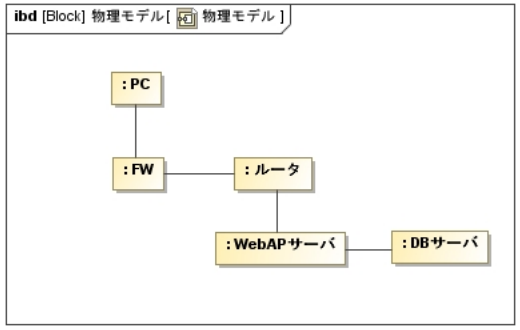

図 1：物理モデルの例

Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

3.2 プロセスモデル

物理モデルに記述された構成要素の上で実行される処理の流れを表すモデルである．物理モデルと同様，内部ブロック図を用いて記述する．以下に，プロセスモデルの例を示す．

図 2：プロセスモデルの例（検索，サーバ管理）

プロセスモデルでは，システムの上で実行されるプロセス間の関係を記述し，各プロセスには，認証方式などのセキュリティ対策に関する属性を定義する．例えば，“シェル”というプロセスには，”認証強度”という属性を定義し，そのプロセスで行われる認証の強度などを表す情報を記述する．また，それらを結ぶコネクタには，プロセス間の通信に用いられるプロトコルを表す属性を付与する．また，別のプロセスモデルとして，以下のようなシーケンス図によって，具体的な処理の流れを表すことができる．

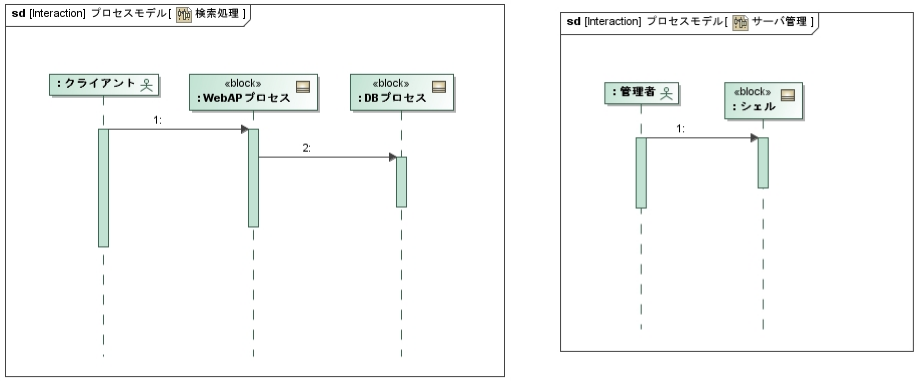

図 3：処理の流れを表すプロセスモデルの例

3.3 割当モデル

物理モデルの要素と，プロセスモデルの要素の対応関係を表すモデルである．SysMLの Allocation によって記述される．以下に，割当モデルの例を示す．

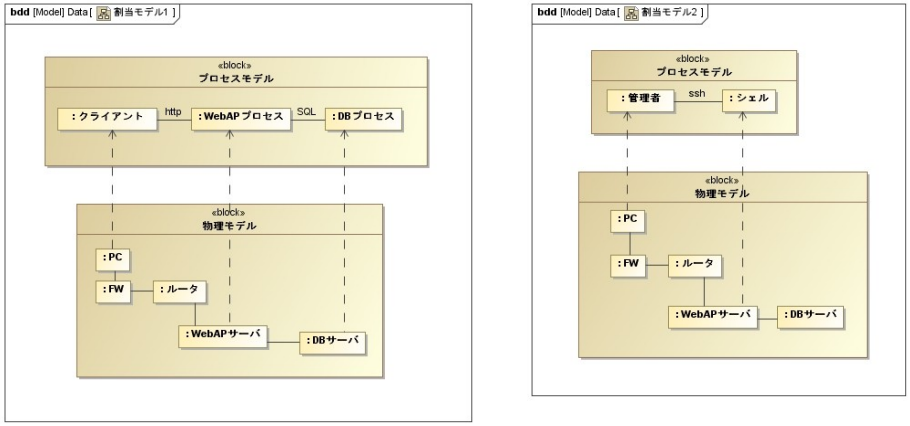

図 4：割当モデルの例

割当モデルによって，各プロセスがどの機器の上で実行されるか，という階層の異なるモデルの要素間の対応関係を記述することができる．

4. 機密性評価手法と適用例

4.1 提案手法の概要

本節では，提案手法の流れを説明する．本手法では，システムモデルと，システムモデルに依らない，システムの構成要素に対して行われる操作パターン（脅威）に関する知識を利用して，評価者によって指定された場所から，ある特定の攻撃が成功する確率をリスクとして算出することで，機密性の評価を行う．図 5 に，本手法における処理の概要を示す．

Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

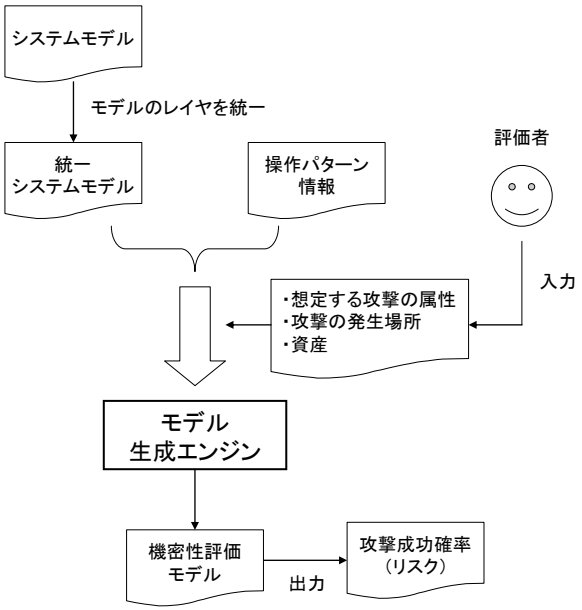

図 5：提案手法の概要

統一システムモデルは，システムモデルで記述されている，評価対象システムの物理的な構成とその上で実行されるプロセスを一つの図にまとめたものである．統一システムモデルの具体的な作成手順は以下の通りである．

- プロセスモデルから，このシステムにおいて実行されるプロセスを順に取り出し，処理の流れに沿って並べる．
- 割当モデルを参照して，各プロセスが実行される物理モデル上の機器の間に含まれるセキュリティ機器がある場合には，その機器取り出し，プロセス間に挿入する．
- プロセスと機器を繋ぐコネクタには，プロセスモデルに書かれた通信プロトコルの属性を引き継いで与える．

これにより，異なるレイヤで記述された複数の図（システムモデル）を，一つにまとめることができる．このようにして共通のレイヤに取り出されたプロセスと機器をあわせて，システムノードと呼ぶ．

また，システムモデルとは別に，システムノードにおいて可能な操作のパターンを定義しておく．これは，あるシステムノードに対してある操作が行われた場合に，その後どのような操作を行うことができるか，という脅威の依存関係を表す知識である．例えば，図 6 は，システムノード A に対して a’という操作が行われた場合には，次のシステムノードに対して b，b’という操作を行うことができ，B に b’という操作が行われた場合には，c’という操作を行うことができることを表している．

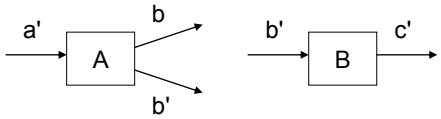

図 6：可能な操作パターン

これらの情報から，評価対象のシステムで起こり得る攻撃の流れを表す機密性評価モデルを作成する．機密性評価モデルは有向グラフで表され，攻撃は，ノード間を繋ぐエッジによって表す．エッジは，各ノード間での攻撃方法を表す属性を持ち，その攻撃の成功確率は，エッジの重みによって表される．機密性評価モデルの具体的な生成手順は以下の通りである．

- 統一システムモデルに書かれたシステムノードを順に取り出し，これらをノードとして記述する．ここで，各ノードには，システムモデルの中で書かれたセキュリティ対策とその有効度に関する情報が引き継がれている．
- 評価者によって指定された最初のノードに向けてエッジを記述する．ここで，エッジに付与された属性によって，ノードに対する不正な操作（攻撃）を表す．
- 操作パターン情報から，そのノードが受信したエッジの属性に対応する可能な操作を決定し，その属性を持つエッジを次のノードに向けて記述する．

これを繰り返すことで，攻撃の伝播経路を作成できる．また，各ノードには，システムモデルの中で書かれたセキュリティ対策とその有効度に関する情報が引き継がれている．これを基に，この経路上を攻撃メッセージが伝播しながら変化していく様子を重み付きの有向グラフで表すことで，各攻撃の成功確率を評価することができる．

4.2 具体例

本節では，単純な Web システムを取り上げ，評価モデルを生成する具体例を示す．サンプルとするシステムでは，WebAP サーバ･DB サーバなどのサーバ機器や，ファイアウォール（FW）やルータなどのネットワーク機器が使用されており，図 1 のような構成で接続されているとする．また，このシステムでは，図 2 で表された，検索・サーバ管理という処理が実行されるものとする．

まず，図 1，図 2 に記述されている階層が異なる要素をまとめ，処理の流れに沿って並べた統一システムモデルを作成する．ここで，各システムノードには，セキュリ

Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

ティ対策の有効度を表す属性が定義されている．例えば，FW には，フィルタリング対象となるプロトコルを示す属性が与えられており，正規の通信プロトコルとして設定されている http 以外によるアクセスは，設定ミスなどが無い限りは，ほぼ遮断される．また，シェルに対しては，“認証強度＝強”という属性が与えられており，不正な ssh による攻撃は，高確率で防ぐことができる．

また，各システムノードにおいて可能な操作パターンが，以下のように定義されている．

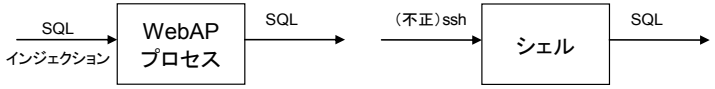

図 7 ：可能な操作パターンの例

これは，例えば WebAP プロセスが SQL インジェクション攻撃を受けた場合には，任意の SQL が実行できてしまうことや，シェルプロセスに ssh でログインできた場合には，その後，SQL を含む任意のプロセスを実行することが可能であることを表している．

上記の統一システムモデルと操作パターン情報を用いて，評価対象のシステムで起こり得る様々な攻撃の成功確率を計算する．

例えば，ssh による不正アクセス攻撃の成功確率を算出するモデルを生成する．上記の統一システムモデルからシステムノードを取り出し，最初のノードである FW に対して，ssh という属性を持つエッジを通して攻撃メッセージを送信する．前述のように，評価対象としているシステムモデルでは，FW の設定として，http 以外によるアクセスは許可されていないので，ssh による攻撃は，FW でのパケットフィルタリングによって，ほぼ防ぐことができる．ここでは，定性的なリスク評価を行うため，http 以外の属性を持つエッジの重みは 0.01 倍になるとする．この重みを掛けて，次のノードへメッセージを送信する．この際，FW から送信されるメッセージの属性は変化しない．次に，WebAP サーバ上で実行されているシェル（認証強度＝強）が，ssh 属性を持つエッジを受信する．ここでは，認証強度を強・中・弱の三段階とし，それぞれ攻撃の成功確率を 0.1・0.3・0.5 倍にする効果があるとすれば，メッセージの重みはさらに 0.1 倍となる．ここで，図 7 の操作パターン情報より，シェルにおける ssh 認証を突破した後，次のノードに対して SQL を送信することが可能となる．これは，WebAP サーバと DB サーバ間の正規の通信プロトコルとして，統一システムモデルに書かれているプロトコルと一致するので，次のノードに対する攻撃が継続する．すなわち，この攻撃が有効であることがわかる．以上の処理によって生成された機密性評価モデルの例を以下に示す．

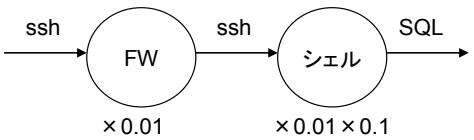

図 8：ssh 攻撃に対する機密性評価モデルの例

一方，WebAP サーバに対する SQL インジェクション攻撃の成功確率を評価する場合，FW では http に対するアクセス制限は行われないため，SQL インジェクションという属性を持つエッジの重みは変化しない．さらに，WebAP プロセスにおいても，SQL インジェクション攻撃への対策がなされていないので，メッセージの重みは変化しない．ここで，ssh による攻撃の場合と同様，統一システムモデルに書かれているプロトコルと一致する属性を持つメッセージを送信できるので，この攻撃も有効であり，ssh の場合よりも攻撃成功確率は高くなる．この場合の機密性評価モデルは以下のようになる．

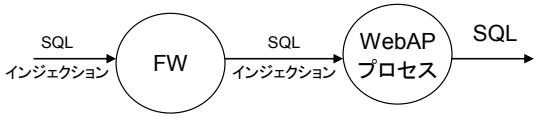

図 9：SQL インジェクション攻撃に対する機密性評価モデルの例

ここで，WebAP プロセスに対して，Web アプリケーションファイアウォール（WAF）機能など，SQL インジェクション攻撃を防ぐ何らかの対策を表す属性が与えられているようなモデルの場合には，WebAP プロセスを通過する SQL インジェクション属性を持つメッセージの重みは，その対策の有効度に応じて低減される．

このように，各ノードの属性として定義されているセキュリティ対策の強度によって，次のノードに向かうメッセージの重みを変化させていくことで，その攻撃の成功確率を評価することができる．そして，最終的に評価者によって指定された資産まで到達したメッセージの重みが，その攻撃の成功確率となる．また，この攻撃成功確率に，資産価値を乗じることで，リスクの値を算出することができる．

5. まとめと今後の課題

本稿では，システムの物理的構成状態とその上で実行されるプロセスをモデル化し，システムに対して発生すると考えられる攻撃の成功確率から，そのモデルにおける機

Vol.2010-DPS-142 No.31
Vol.2010-CSEC-48 No.31
2010/3/5

密性を評価する手法を提案した．本手法は，UML で記述されたシステムの構成と動作を表す設計情報であるシステムモデルと，モデルの構成要素に対して可能な操作のパターンに関する知識を用いて，ある資産までの攻撃の流れを明らかにする．そして，システムを構成している各要素に導入されているセキュリティ対策の有無やその強度から，ある攻撃が成功する確率（リスク）を算出するものである．このように，一般的な設計情報であるシステムモデルを利用することで，攻撃の流れを表すモデルを効率的に生成することができる．また，システムモデルと，セキュリティ脅威に関する普遍的な知識から，自動的に評価用のモデルを生成しているため，システムの構成や動作を反映させた評価の実施が可能になる．

今後の課題は，本手法を実プロジェクトに適用し，より大きなシステムモデルに対して機密性の評価を行い，本手法の有効性を検証することである．また，考えられる様々な操作パターン（脅威）と，それを防ぐ対策に関する知識を充実させ，評価対象とする攻撃や対策の種類を増やすことである．

参考文献

1) C. Phillips, L.P. Swiler, “A graph-based system for network-vulnerability analysis”, *Proceedings of the 1998 workshop on New security paradigms*, pp.71-79 (1998)
2) C.R. Ramakrishnan, R. Sekar, “Model-based Analysis of Configuration Vulnerabilities”, *Journal of Computer Security*, Vol.10, pp.189-209 (2003)
3) H.Sakaki, K.Yanoo, R.Ogawa, "A Model-Based Method for Security Configuration Verification", *Advances in Information and Computer Security*, Vol.4266, pp.60-75 (2006)
4) UML, http://www.uml.org/
5) SysML, http://www.omgsysml.org/
6) MARTE, http://www.omgmarte.org/
7) J.Jurjens, "UMLsec: Extending UML for Secure Systems Development", *Proceedings of the 5th International Conference on the Unified Modeling Language*, Vol.2460, pp.412-425 (2002)
8) T.Lodderstedt et al, "SecureUML: A UML-Based Modeling Language for Model-Driven Security", *Proceedings of the International Conference on the Unified Modeling Language*, Vol.2460, pp.426-441 (2002)
9) 森本祥一, 程京徳, "UML によるプロテクションプロファイルのモデル化とその形式的検証", 電子情報通信学会論文誌， Vol.J89-D, No.4, pp.726-742 (2006)