B-025

セキュリティ要求分析を容易にする
システム機能ベースセキュリティパターンの研究
A function-based security pattern for easy security requirements analysis

宇野 健二† 田中 英彦†
Kenji Uno Hidehiko Tanaka

1. はじめに

セキュリティパターンは，セキュリティ専門家の知識を広く活用するための手法である．セキュリティ要求分析に対しても，守るべき資産の価値と，それに対する脅威・脆弱性を評価するプロセスがセキュリティパターンとして提案されているが，現状では，それらのプロセスの実行や，その結果からセキュリティ要求を導出する際に，セキュリティに関する知識が必要とされるため，実際の開発現場ではほとんど採用されていない．

本研究では，脆弱性や解決策などが明らかになっている Web アプリケーションを対象に，通常の機能要求分析に対応付けることで，セキュリティに関する知識のない開発者でも，容易に利用可能なセキュリティ要求分析に対するセキュリティパターンの検討を行う．

2. 関連研究

本章では，セキュリティパターンの関連研究を紹介し，その問題点を述べる．

2.1 セキュリティパターン

セキュリティパターンに関してまとまっている文献として Schumacher らの[1]がある．[1]でまとめられているセキュリティ要求分析に関するセキュリティパターンでは，資産の識別，資産価値の設定，脅威評価，脆弱性評価，リスクの決定など８つのプロセスパターンが提示されており，８つのプロセスを実施することでセキュリティ要求が導出される．

例えば，脅威評価のセキュリティパターンでは，企業の資産に対する脅威を識別し，それらの脅威の起こる可能性や頻度を評価するためのプロセスが示されている．具体的には，最初に企業の資産に対する脅威（脅威源・脅威行動・脅威の結果）の識別を行い，資産タイプや脅威源による脅威のグループ化を行った脅威テーブルを作成する．それと並行して脅威の試行頻度や発生する可能性を評価するための指標を作成し，可能性指標により各々の脅威を評価して，脅威テーブルに反映させる．本パターンにより，脅威の存在と発生頻度の両方を増加させる要因の理解が助けられ，既知の脅威により被る損害を確認することが可能となる．一方で，脅威評価のセキュリティパターンでは，脅威の識別精度が分析担当者のセキュリティ知識に大きく依存するため，セキュリティ知識のない開発者ではパターンの適用が難しいという課題がある．

また，セキュリティ要求分析を行うためには，８つのセキュリティパターンを実施する必要があるが，その実施にはかなりの時間が必要となる点も課題である．

2.2 Web セキュリティ要求パターン

大久保らは，ミスユースケース記法を拡張し，資産の概念を導入することで脅威抽出を容易にした，資産ベースミスユースケース（Asset-based Misuse case: AsseMis）記法を提案し[2]，AsseMis を Web 領域に適用することで，脅威や対策のパターン化が可能と考え，８つの Web セキュリティ要求パターンを提案している[3]．

Web セキュリティ要求パターンは，資産の形態（データの流れ，セキュリティプロパティ）ごとに起こりうる脅威，対策をパターン化している．AsseMis による分析において，ユースケース図の作図，資産情報の付与を行った結果から，資産の形態の条件に該当するセキュリティパターンがあれば，そのパターンを適用することで，脅威や対策を自動的に抽出することが可能となり，セキュリティ有識者による脅威分析の作業を省力化することが可能となる．

一方で，同じパターンを適用する場合であっても，それぞれのユースケースについて，パターン内の脅威や対策を適用するかどうかの検討が必要である．そのため，AsseMis の作成などほとんどの作業は省略することはできず，作業が煩雑になるという課題がある．また，ユースケースごとにパターンを適用するため，同じパターンを適用するユースケースが複数存在する．そのため，セキュリティ要求が重複して導出され煩雑になるという点も課題である．

3. 提案パターンについて

セキュリティ対策をできる限り抜け漏れなく実施するには，開発の出来るだけ早期段階からセキュリティについて認識し対応することが必要である．

しかし，[1]のセキュリティパターンをアプリケーション開発工程に適用する場合，機能要求分析とセキュリティ要求分析の工程の間に関係性は無く別々の工程となっている．そのため，予算や時間的な制約，あるいはセキュリティ要求を検討できる担当者がいないなどの要因により，セキュリティ要求分析の工程が軽視され，セキュリティ要求分析が実施されない可能性も考えられる．

本研究では，要求分析の工程でセキュリティ要求分析を実施することを目的として，機能要求分析とセキュリティ要求分析の工程をできる限り関連性のある工程とすることで，要求分析の工程で機能要求分析の一連の工程としてセキュリティ要求分析が実施されるように，セキュリティに関する知識のない開発者でも，容易に利用可

†情報セキュリティ大学院大学, Institute of Information Security

能な，システムの要求機能からセキュリティ要求を導出できるセキュリティパターンの検討を行う．

3.1 Web アプリケーション機能モデル

機能に対応するセキュリティパターンを作成するために，Web アプリケーションの機能のモデル化について検討を行う．[4]では，Web アプリケーションにおける典型的な脆弱性や攻撃について，その機構や解決策も含めて，知識として整理され公開されている．それを参考に，脆弱性と機能を対応付けて Web アプリケーション機能モデルの作成を行った．図１に Web アプリケーションの機能モデルを示す．一例として，「SQL インジェクション」の脆弱性であれば，注意が必要なウェブサイトとして，DB を利用するウェブアプリケーションが挙げられているため，「DB／SQL」機能を抽出した．

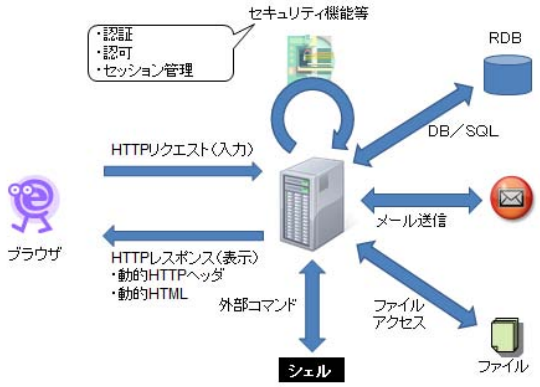

図１　Web アプリケーション機能モデル

「HTTP リクエスト（入力）」については，特定の脅威に関連する機能ではないが，さまざまな脅威の予防的見地から対策が必要となるため，追加している．

3.2 システム機能ベースセキュリティパターン

提案するシステム機能ベースセキュリティパターンとしては，図１のそれぞれの機能について，発生する可能性のある脆弱性等の問題点とその対策及びセキュリティ要求をまとめてセキュリティパターンとして提供する．

想定する適用方法としては，機能要求分析で明らかになった要求機能を元に，システムで必要となる機能を図１の Web アプリケーション機能モデルから選択することで，適用すべきセキュリティパターンが決定可能となる．

一例として，図書館情報システムを考える．要求機能としては，「検索機能」や「図書貸出予約・状況確認機能」などが考えられる．この２つの要求機能を元に，Web アプリケーション機能モデルからシステムとして必要となる機能を選択すると，「HTTP リクエスト(入力)」・「HTTP レスポンス(表示)(動的 HTML)」・「DB/SQL 機能」・「認証機能」・「認可機能」・「セッション管理機能」が選択され，これらに対応するセキュリティパターンの適用が必要となる．

4. 考察

Schumacher らの研究は，セキュリティ要求分析のプロセスを実施する上で支援となるパターンではあるが，その結果は担当者の知識に因る所が大きく，また，すべてのプロセスの実施には時間がかかるものと思われ，セキュリティを重視したアプリケーション開発以外では適用は難しいものと考える．

大久保らの研究は，条件付きではあるが機能要求分析とセキュリティ要求分析の工程が一連の工程として実施することが可能であり，さらに適用システムを Web 領域に限定すれば Web セキュリティ要求パターンが提案されているため，さらなる作業の効率化が可能である．しかし，ユースケースごとにセキュリティパターンを適用して脅威や対策を精査するため，ほとんどの作業は省略できず，また，セキュリティ要求が重複して導出されるため，作業が煩雑になるものと考えられる．

提案するセキュリティパターンでは，Web アプリケーションの機能をモデル化し，機能ごとの脅威や対策をセキュリティパターンとして提案することで，機能要求分析で得られた機能を元に，セキュリティパターンの選択が可能となり，機能要求分析とセキュリティ要求分析の工程を一連の工程としてセキュリティ知識のない担当者でも容易に実施可能となる．

また，システム全体で必要とする機能を選択し，セキュリティパターンを適用するため，セキュリティ要求の重複を少なくし，作業が分かりやすいものになっていると考える．

課題として考えられることは，システム全体の大まかな機能としてセキュリティ要求を導出するため，ユースケース単位で考えた場合には不要となるはずのセキュリティ要求も含めた過剰なセキュリティ要求になる可能性が考えられる．そのため，提案パターンによるセキュリティ要求の導出後に，ユースケース単位での検証が必要になるのではないかと考える．

また，提案する Web アプリケーションの機能モデルが，Web アプリケーションの機能を網羅しているのかの検証も必要であると考える．

5. おわりに

本稿では，セキュリティ要求分析における既存のセキュリティパターンの課題を説明し，システム機能ベースの新たなセキュリティパターンの提案を行った．

今後は，Web アプリケーションにおける脅威や対策についてまとめられた資料を参考に，Web アプリケーションの機能モデルのさらなる精査を行い，Web アプリケーション機能モデルを作成し，機能ごとのセキュリティパターンを作成する．また，セキュリティパターン作成後は，ケーススタディを行い，既存のセキュリティパターンとの優位性について検証を行う．

参考文献

[1] M. Schumacher, F. Buschmann, E. B. Fernandez, D. Hybertson, P. Sommerlad. , “Security Patterns: Integrating Security And Systems Engineering”, John Wiley & Sons Inc, 2006.
[2] Takao Okubo, Hidehiko Tanaka, “Identifying Security Aspects in Early Development Stages”, Proc. International Conference on Availability, Reliability and Security (ARES’08), Barcelona, Spain, pp.1148-1155 (2008).
[3] Takao Okubo, Hidehiko Tanaka, “Web Security Patterns for Analysis and Design”, Pattern Languages on Programs (PLoP) 2008, Oct. 2008.
[4] 情報処理推進機構(IPA), “安全なウェブサイトの作り方　改訂第５版”, http://www.ipa.go.jp/security/vuln/documents/website_security.pdf