

セキュリティパターンのモデル化と応用に向けて

鷲 崎 弘 宜[†]

セキュリティパターンとパターン活用技術研究の現状を概観した上で、その基盤を与える様々なモデル化の方法、および、応用の可能性を検討する。

Modeling Security Patterns and Application

HIRONORI WASHIZAKI[†]

We overview the current state of security patterns and researches on patterns utilization technology. Moreover, we discuss the way of modeling security patterns and the possibility of application regarding the modeling results.

1. はじめに

計算機やサービス間の相互運用性や接続性が高まると同時に、情報システムの広範あるいは双方向の利用が広まる中で、ソフトウェアシステムの開発および運用においてセキュリティを確保することの重要性が増している。しかしながら、セキュリティは他の品質特性と異なる側面が多く（例えば脆弱性や攻撃への対策が主であること、開発やシステムの全体にわたって考慮する必要があることなど）、セキュリティの専門家や過去の対策経験者でなければその確保は難しい。

そこで、熟練者のノウハウや過去の成功事例を習得し再利用する方法としてセキュリティパターンが注目されている。セキュリティパターンとは、特定の文脈において頻出するセキュリティ上の問題に対するよく知られた解決策をまとめあげた記述である^{?)}。これまでに、分析や設計、実装などのさまざまな工程について多数のセキュリティパターンが抽出され、その報告数は近年増加の傾向にある²⁾。

2. セキュリティパターン研究

セキュリティパターンの蓄積と利用機会の増大に呼応して、セキュリティパターンの活用技術に関する研究が世界的に取り組み始められている³⁾。例えば筆者らは、セキュリティパターンの分類や適用について研究を進めている^{4),5)}。セキュリティパターン研究の多くは計算機を用いたパターンの自動処理を扱うため、も

とものセキュリティパターンについて注目する側面を何らかの形でモデル化している。

ここで、要求やソフトウェアシステムの分析、設計、実装、開発にあたってセキュリティ上の共通の言語は存在しないのが現状であるため、扱うセキュリティパターンをどのようにモデル化するかが、セキュリティパターン研究・技術の性質に大きく影響を与える。

3. セキュリティパターンのモデル化

セキュリティパターンの活用にあたり、そのモデル化の方法の適切さ・特性が基盤となるとの考えに基づき、筆者らは複数のモデリング言語を同一のセキュリティパターンの表現に適用してその特性を比較する研究を進めている（詳細は文献⁶⁾に掲載予定である）。具体的には、代表的なセキュリティパターンとして Role-Based Access Control (RBAC) パターン¹⁾を取り上げて、同パターンの注目する側面のモデル化にあたり UML・ミヌースケース、UMLのセキュリティ拡張である UMLsec や SecureUML, i*/Tropos/Secure Tropos 等のゴール指向モデル、さらには Problem Frames 等をそれぞれ別個に適用し、その結果を主に表現力や応用の観点から比較考察している。

例えば、RBAC そのものは様々なバリエーションを含めて文献⁷⁾にまとめられており、ここでは、RBAC が適用されている場合にユーザやロール、パーミッション設定およびセッションの間で満たされるべき性質が述語論理によりモデル化されている。同様に文献⁸⁾では、形式言語により性質を厳密に規定している。これらの規定やモデル化は特定の性質・制約の記述にとど

[†] 早稲田大学 Waseda University

まり、周囲の環境やソフトウェアシステム、それらの構造や振る舞いとの関係をモデル化したものではない。一方、ソフトウェアシステムのモデル化について代表的なUML(さらにはSysML)をRBACパターンの与える解決構造のモデル化に適用できるが、その表現力は限定的であり、性質・制約の表現に他の記述言語(例えばOCLなど)を必要とする。このように、セキュリティパターンのモデル表現とソフトウェア・システムモデルの融合が重要な課題となる。

4. 議 論

上述のような現状の比較を概観した上で、ワークショップにおいては次のような未整理な点を議論したい。

- 適用や検出、検証といった特定用途の観点からのモデリング言語の適性: 例えば筆者らは、アクタ間の依存関係が複雑な場合のモデリングに特に有効なゴール指向モデル^{i*)9)}を用いて、RBACパターンをモデル化し、さらにはモデル変換言語を用いて変換により部分的に適用が可能であることを確認しつつある⁵⁾。
また、セキュリティはアーキテクチャの設計にあたり効率性や使用性といった他の品質としばしばトレードオフの関係にあり、モデリング言語はその関係を表現できると同時に、解消に向けた応用へと役立てられることも望まれる。この点で、ゴール指向モデルは有効に機能する可能性がある。さらに既存のアーキテクチャ設計・評価手法との接続も検討すべき事項である。
- セキュリティパターンそのものの種別や特性に応じたモデリング言語の適性: セキュリティパターンはProblem Pattern(問題・ドメインより)とSolution Pattern(解決より)に大別できる。このとき、その種別に応じて最適なモデリング言語・表現は異なる可能性がある。例えば、ゴール指向モデルはSolution Patternには不向きな可能性がある。
- プロセスとの関係: Secure Tropos等の一部の方法論は特定のモデリング言語に加えて、プロセスを内包しているが、他のモデリング言語の適用・併用可能性も含めて検討の余地がある。

参 考 文 献

- 1) M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, "Security Patterns: Integrating security and systems engineering," Wiley 2006.
- 2) T. Heyman, et al., "An Analysis of the Security Patterns Landscape," Proc. 29th International Conference on Software Engineering Workshops (ICSEW), 2007.
- 3) N. Yoshioka, H. Washizaki and K. Maruyama, "A survey on security patterns," Progress in Informatics, No.5, pp.35-47, 2008.
- 4) E.B. Fernandez, H. Washizaki, N. Yoshioka, A. Kubo, Y. Fukazawa, "Classifying Security Patterns," Proc. Asia-Pacific Web Conference (APWeb), 2008.
- 5) Y. Yu, H. Kaiya, H. Washizaki, Y. Xiong, Z. Hu, N. Yoshioka, "Enforcing a security pattern in stakeholder goal models," Proc. 4th ACM Workshop on Quality of Protection (QoP), 2008.
- 6) T. Tun, et al.: "Modelling Security Patterns: A Survey," Chapter in ed. H. Mouratidis, "Software Engineering for Secure Systems: Industrial and Research Perspectives," IGI Global, 2009. (to be published)
- 7) R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman "Role-Based Access Control Models," IEEE Computer, Vol.29, No.2, pp.38-47, 1996.
- 8) D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, R. Chandramouli. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), Vol. 4, No. 3, pp. 224 - 274, Aug. 2001.
- 9) E.S.K. Yu. Modelling strategic relationships for process reengineering, University of Toronto, 1996.

1) M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, "Security Patterns: Integrating security and systems