ネットワークソフトウェア対象のセキュリティ・プライバシ・トラストのエコシステム

Ecosystem for Security, Privacy, and Trust in Network Software Systems

鷲崎　弘宜（Hironori WASHIZAKI, Ph. D.）

早稲田大学　理工学術院　教授

(Professor, Waseda University)

IEEE Computer Society Vice President for Professional and Educational Activities, 情報処理学会ソフトウェア工学研究会主査　他

受賞：科学技術分野の文部科学大臣表彰 科学技術賞（理解増進部門）（2021年），情報処理学会ソフトウェア工学研究会功績賞（2021 年），IWESEP Best Paper Award（2019年），IMS Japan 賞 特別賞（2019年），日本 e-Learning 大賞 2019 IT 人財育成部門賞（2019年），情報処理学会ソフトウェア工学研究会卓越研究賞（2019 年），日本工学教育協会 工学教育賞（2017年）他

著書：ソフトウェア品質知識体系ガイド（第3版）－SQuBOK Guide V3－, オーム社（2020年）　Scratch でたのしく学ぶプログラミング的思考, マイナビ出版（2019年）　初級ソフトウェア品質技術者資格試験(JCSQE) 問題と解説 第2版, 日科技連出版社（2015年）　ソフトウェアパターン：パターン指向の実践ソフトウェア開発, 近代科学社（2007年）　AspectJ によるアスペクト指向プログラミング入門, ソフトバンククリエイティブ,（2004年）他

研究専門分野：ソフトウェア工学　情報システム　情報教育

あらまし

本研究ではネットワークソフトウェアシステムを対象とした共存・循環・進化型のセキュリティ・プライバシ・トラストのエコシステム（生態系）の基盤を実現する。エコシステムでは、企画から開発、運用に到るライフサイクル中のセキュリティ、プライバシ、トラストに関わる様々な成果物や知識等をメタモデル上で整理体系化・統合・再利用し、新たなソフトウェアシステムを進化的に生み出し、またその運用における新たなリスクや攻撃・対策を、当該および他のソフトウェアシステムの企画・開発・運用へ役立てる。加えて本研究では、エコシステムにおける主要な再利用対象であるセキュリティパターンの扱いに関する研究を網羅的に分類調査及び整理する。

１．研究の目的

複雑なネットワークソフトウェアシステムへのセキュリティやプライバシの作り込みは通常、過去のインシデントにおける脆弱性の識別および対策を積み重ねて達成される。本研究では、セキュリティ・プライバシ・トラストをネットワークソフトウェアシステムへ組み入れるために必要な設計上の要素と要素間の関係を整理したメタモデルを実現する。メタモデルに基づき、ネットワークソフトウェアシステムを対象とした共存・循環・進化型の「セキュリティ・プライバシ・トラストのエコシステム（生態系）」の基盤を実現する。

エコシステムでは、企画から開発、運用に到るライフサイクル中のセキュリティ、プライバシ、トラストに関わる様々な成果物や知識等をメタモデル上で整理体系化・統合・再利用し、新たなソフトウェアシステムを進化的に生み出し、またその運用における新たなリスクや攻撃・対策を、当該および他のソフトウェアシステムの企画・開発・運用へ役立てる。

加えて本研究では、エコシステムにおける主要な再利用対象であるセキュリティパターンの扱いに関する研究を網羅的に分類調査及び整理する。

２．研究の背景

IoT やクラウドに代表される複雑なネットワークソフトウェアシステムでは、多種多様多量なデータをリアルタイムに扱い業務の飛躍的な効率化や新たなサービス・価値の創造に寄与することが期待される。一方で、サービスやデータの集中管理、自然災害や侵入者といった外的要因の変化や増大、さらには設計思想やセキュリティの異なる多様な機器の接続に伴い、攻撃やデータ漏洩のリスクは増大し、他の品質を維持したまま必要なセキュリティおよびプライバシを確保することが社会的急務である。

本研究の代表者らはクラウドサービスを対象にセキュリティ知識を扱う初期的なメタモデルを実現しており [1][2]、そのプライバシの扱いを含む形での拡張を通じて本研究の基礎とした。

また本研究の代表者らは、セキュリティパターンや関連技術について国際的に研究領域をリードする立場にある。具体的には、各種セキュリティパターンの調

査分類 [3] やセキュリティパターンの適用 [4]、および適用の検証 [5][6] 等を実現している。これらを応用することで総合的に、トラストおよびプライバシも含めて事例やパターンを扱う知識ベースおよびその周辺の基礎を実現する。

３．研究の方法

高いセキュリティやプライバシをソフトウェアシステムの分析や設計の段階から作りこむためのセキュリティ・プライバシパターンやパターン以外の知識は豊富に得られつつあるが、問題に応じて適切なものを選択することや、適切な組み合わせを特定することが困難になっている。この問題はセキュリティ・プライバシパターン全般に関連するものであるが、クラウドに代表されるネットワークソフトウェアシステムにおいては特に重大である。

クラウドに代表されるソフトウェアサービスとその基礎となる仕組みは、スタック上の複数の層にわたって統合され実現される。そこで本研究では、層状のスタックにおけるセキュリティとプライバシおよびトラストに関連する本質的な概念を捉えて層別にカプセル化し、参照アーキテクチャとして機能するメタモデルを実現した [7][8][9]。同メタモデルにおいて、セキュリティとプライバシおよびトラスト関連の知識を複数の層に分けて記述し知識ベースを構成可能とする。同メタモデルは、セキュリティとプライバシおよびトラストの問題に対処するために適切なパターンやプラクティスに代表される知識や過去の事例を選択して組み合わせるのみならず、一定の抽象度におけるアーキテクチャを効果的かつ効率的に設計することにも利用できる（図 1）。

同メタモデルでは、層別の整理と共に、層を超えた整合性をもって再利用する仕組みを実現した。加えて、複雑なネットワークソフトウェアシステムはしばしば多数のデバイスと関係し、各デバイスは独自のモデルとサービスを持つため、絡み合ったシステムの全体におけるセキュリティとプライバシおよびトラストの実現にあたり、一定の抽象度で共通概念を整理し、かつ個別に各プラットフォーム固有の概念を扱うことを実現した。

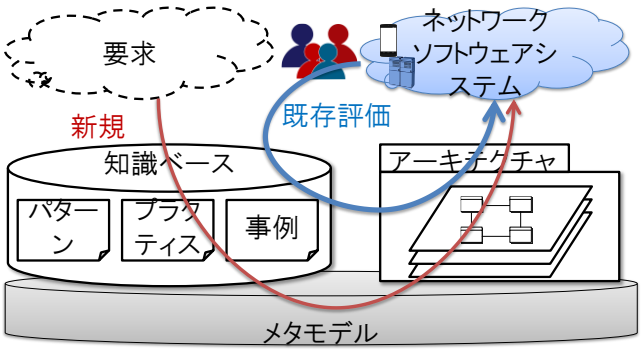

図 1. メタモデルに基づく再利用の概要

メタモデルは、セキュリティやプライバシのパターンが扱う問題と解決策のモデル化や、CVE（Common Vulnerabilities and Exposures）などのデータベースから脆弱性をモデル化する際の基礎となる。例えば、クロスサイトスクリプティング（XSS）の脆弱性は、図 2 のようにモデル化できる。問題の特定と対策の実施を容易にするために、図のモデルは、脆弱性のある要素の可視化に役立つ。

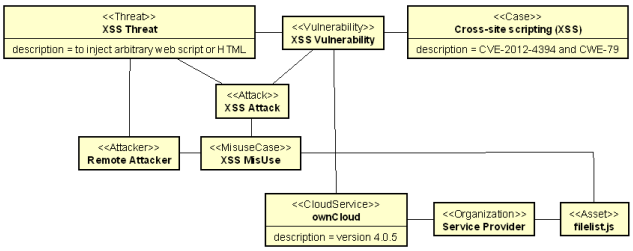

図 2. クロスサイトスクリプティングのモデル

本研究では、企画から開発、運用にいたるライフサイクル中のセキュリティ、プライバシ、トラストに関わる成果物や知識等について、メタモデル上で整理体系化・統合・再利用することで新たなシステムを生み出すエコシステムを構成可能なことを確認した（図 3）。

ネットワークソフトウェア対象のセキュリティ・プライバシ・トラストのエコシステム

Ecosystem for Security, Privacy, and Trust in Network Software Systems

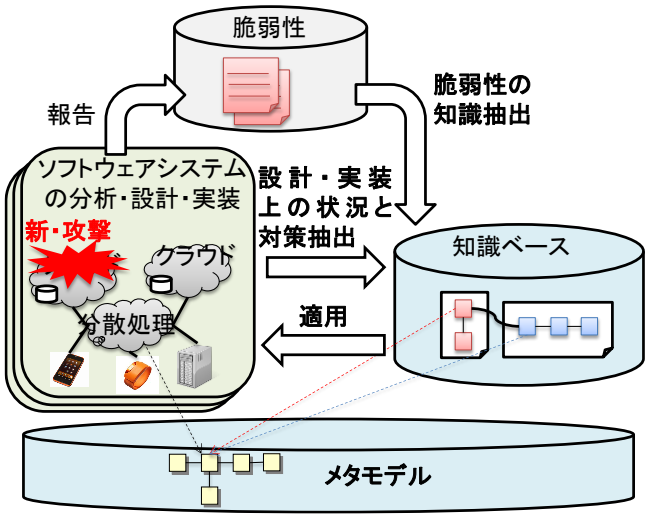

図 3. メタモデルに基づくエコシステムの概要

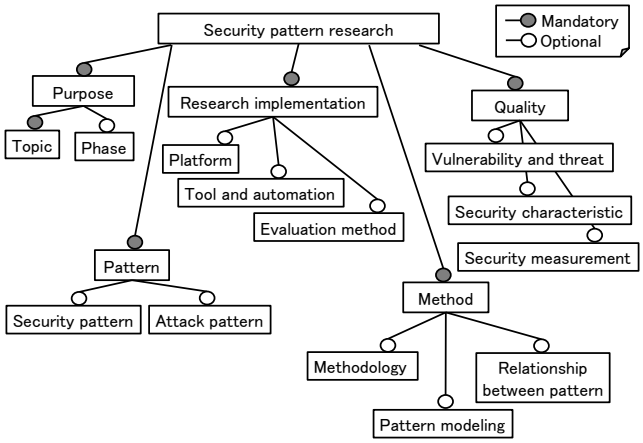

図 4. セキュリティパターン研究の分類体系

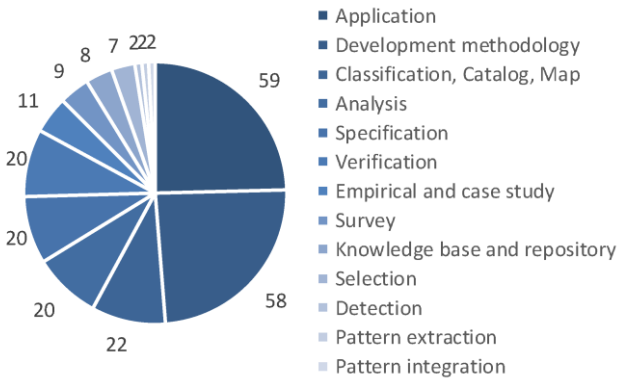

図 5. セキュリティパターン研究の内容分類

加えて本研究では、エコシステムにおける主要な再利用対象であるセキュリティパターンの適用や検証などの研究・実践手法群の分類体系を実現し、網羅的かつ体系的な文献調査を通じて全体像を明らかとした[10][11]。分類体系の一部を図 4 に示す。

セキュリティパターンは、セキュアなソフトウェアシステムの開発・運用において、ある特定の状況下でしばしば出現するセキュリティ関連の問題を網羅している。1990 年代後半以降、約 500 のセキュリティパターンが提案されている。技術的な要素はよく調べられているが、方向性や全体像、実装にあたっての課題などは十分に整理されていなかった。そこで本研究では、240 の論文を対象とした系統的な文献調査により、セキュリティパターン研究のための分類法を考案した。我々の分類法と調査結果は、実務家と研究者の間のコミュニケーションを改善し、用語を標準化し、セキュリティパターンの有効性を高め、エコシステムの構成に寄与するものである。

例えばセキュリティパターン研究が扱う内容の分類を図 5 に示す。大部分を適用および開発方法論が占め、そのほかに分類などがあることがわかる。また、各研究・実践手法が扱う具体的なセキュリティパターンとして次のものが頻出であることを明らかとした: Role-Based Access Control (RBAC), Authorization, Authentication, Authenticator, Secure logger.

4. 将来展望

本研究では、クラウド等のネットワークソフトウェアシステムに対し過去の成果や知識をパターンやプラクティスおよび事例の形で整理し再利用することで、トラストに基づきセキュリティとプライバシを組み入れて次の開発運用へと役立てる共存・循環・進化型エコシステムの基盤を実現した。

今後は、本研究の代表者らが整理している IoT システムの設計・実装における IoT パターン [12][13] のうちでセキュリティやプライバシを扱うものを組み入れて知識ベースを拡充させることを計画している。そのうえで、有効性を評価するために複数のサービスを含むクラウドシステムの開発など、より複雑なケーススタディを実施すること、および、利用を拡大するための詳細なフレームワークの開発を計画している。

ネットワークソフトウェア対象のセキュリティ・プライバシ・トラストのエコシステム

Ecosystem for Security, Privacy, and Trust in Network Software Systems

おわりに

本研究の成果を用いることで、ネットワークソフトウェアシステムの開発者や運用者は、メタモデルに基づき整理構築および更新される知識ベース中の過去の脆弱性やパターンを参照して効率的および効果的に、一定のトラストの上でセキュリティやプライバシの要求を獲得および分析し、知識ベース中で要求に対応したリスク対策候補を識別し設計および実装できる。

今後は、IoT セキュリティパターンやプライバシパターンの組み入れを通じた知識ベースの拡充、より複雑なケーススタディの実施、および、利用を拡大するための詳細なフレームワークの開発を計画している。

参考文献

[1] H. Washizaki, et al., “A Metamodel for Security and Privacy Knowledge in Cloud Services,” 12th IEEE World Congress on Services (SERVICES), pp. 142-143, 2016.

[2] E. B. Fernandez, N. Yoshioka, H. Washizaki, Madiha H. Syed, “Modeling and Security in Cloud Ecosystems,” Future Internet, Vol.8, No.13(2), pp.1-15, 2016.

[3] N. Yoshioka, H. Washizaki, K. Maruyama, “A survey on security patterns,” Progress in Informatics, No.5, pp.35-47, 2008.

[4] Y. Yu, H. Kaiya, N. Yoshioka, Z. Hu, H. Washizaki, et al., “Goal Modelling for Security Problem Matching and Pattern Enforcement,” International Journal of Secure Software Engineering (IJSSE), Vol.8, No.3, pp.42-57, 2017.

[5] T. Kobashi, N. Yoshioka, H. Kaiya, H. Washizaki, et al., “Validating Security Design Pattern Applications by Testing Design Models,” International Journal of Secure Software Engineering (IJSSE), Vol. 5, Issue 4, pp.1-30, 2014.

[6] M. Yoshizawa, H. Washizaki, et al., “Implementation Support of Security Design Patterns Using Test Templates,” Information, Vol.7, No.2(34), pp.1-19, 2016.

[7] T. Xia, H. Washizaki, et al., “CSPM: Metamodel for Handling Security and Privacy Knowledge in Cloud Service Development,” International Journal of Systems and Software Security and Protection (IJSSSP), Vol. 12, No. 2, pp.1-18, 2021.

[8] T. Xia, H. Washizaki, et al., “Cloud Security and Privacy Metamodel: Metamodel for Security and Privacy Knowledge in Cloud Services,” 6th International Conference on Model-Driven Engineering and Software Development (MODELSWARD), pp.379-386, 2018.

[9] E. B. Fernandez, H. Washizaki, N. Yoshioka, “Using Security Patterns to Develop Secure Systems – Ten years later,” International Journal of Systems and Software Security and Protection (IJSSSP), Vol. 9, No. 4, pp. 46-56, 2019.

[10] H. Washizaki, et al., “Systematic Literature Review of Security Pattern Research,” Information, Vol. 12, No. 1:36, pp.1-27, 2021.

[11] H. Washizaki, et al., “Taxonomy and Literature Survey of Security Pattern Research,” IEEE Conference on Applications, Information and Network Security (AINS), pp. 87-92, 2018.

[12] H. Washizaki, et al., “Landscape of Architecture and Design Patterns for IoT Systems,” IEEE Internet of Things Journal, Vol. 7, No. 10, pp.10091 – 10101, 2020.

[13] H. Washizaki, et al., “Analysis of IoT Pattern Descriptions,” 2021 IEEE/ACM 3rd International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT), pp.1-6, 2021.

この研究は、平成２８年度ＳＣＡＴ研究助成の対象として採用され、平成２９～令和元年度に実施されたものです。