SSR 平成 27 年度 調査研究プロポーザル

平成 27 年 4 月 23 日

申請者: 早稲田大学グローバルソフトウェアエンジニアリング研究所所長 鷲崎 弘宜

1. 調査研究テーマ名

クラウドサービスの開発運用におけるセキュリティとプライバシの確保のためのメタモデルに基づく知識ベースと参照アーキテクチャの調査研究

2. テーマの戦略的意義／位置付け

背景: 管理の省力化や、機能および性能要求変更への適応を意図し、各種クラウドサービスが導入されつつある。結果として業務の効率化に寄与することが期待される一方で、導入する個人や組織から独立したクラウドサービス事業者(プロバイダ)においてサービスおよびデータを集中管理するため、他の品質を維持したままで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となっている。例えば[Andriole15]においては、クラウドコンピューティングおよびサービスの普及が一般参加型の仕組みを推し進める要因となり、セキュリティの確保の重要性が指摘されている。

問題: セキュリティやプライバシ上の既知のリスクについては、過去のリスクや事例、問題とそれに対する解決策としての対策をまとめた各種のパターンといった知識を参照し、対策を最初から組み入れておくことが必要である。未知のリスクについては、要求との対応関係を維持したうえで設計および実装を可変な形とし、新たなリスクが顕在化した場合に迅速に対応することが必要である。しかし、事例やパターンといった各種の知識はあるものの個別に提案記述され、関係や組み合わせが未整理である。従って、一貫した形で効率的に知識を選択、適用および組み合わせることが難しく、設計や実装において適用した結果について要求との対応関係を追跡することも難しい。

解決: クラウドサービスのシステムおよびソフトウェアのセキュリティとプライバシの両方を扱う知識および参照アーキテクチャのメタモデルを定義し、そのうえでクラウドサービスのセキュリティおよびプライバシの要求定義や分析、リスク対策の設計や実装・運用を扱うパターンおよびパターン化されていないプラクティス・事例を整理体系化し、知識ベースとして構築する。さらに、知識ベースを参照することで開発あるいは運用・選択・修正するクラウドサービスやシステム全体の参照アーキテクチャ(実装の詳細に立ち入らない抽象アーキテクチャ)をメタモデルに従った形で導出する手法を実現する。研究の全体像を図 1 に示す。

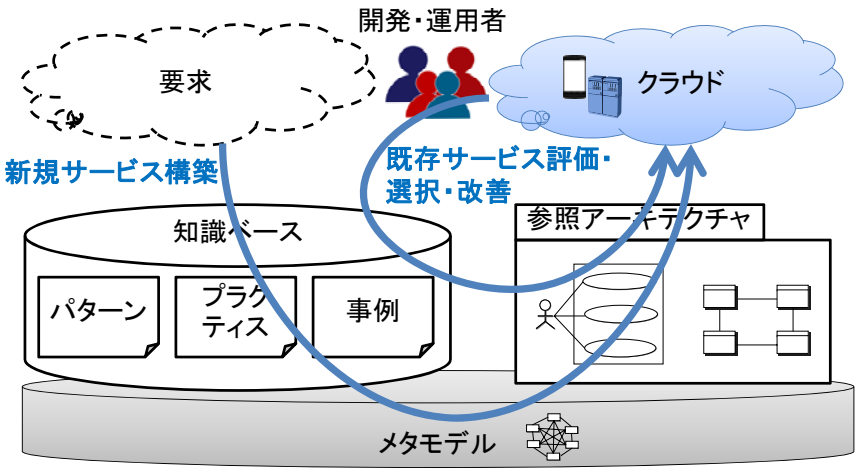

図1: 調査研究成果の全体像

クラウドサービスの開発者およ

び運用者は、知識ベースを参照することで効率的かつ効果的にセキュリティおよびプライバシ要求を獲得・分析し、さらに要求と対応するリスク対策を用いてメタモデル上で参照アーキテクチャを一貫かつ効率的に導出できる。参照アーキテクチャ上で要求とその実現方法・箇所の対応関係を容易に追跡できるため、以降の実装および保守においてセキュリティおよびプライバシ上の既知のリスク対策の確保を一貫かつ効率的に進められると同時に、新たなリスクへの対策も容易となる。

関連研究: [Fer15a]は、クラウドシステムにおけるセキュリティに関するメタモデルを定義し、パターンやプラクティスを合わせて用いて参照アーキテクチャを導出する手法を提案している。また NIST は同様の支援を目的として、抽象的な共通参照アーキテクチャを定義している[NIST13]。しかしそれらはプライバシを扱っていない。さらに、メタモデルに基づいてパターンや事例等の知識を具体的に整理した知識ベースは提案されていない。

また、システムの開発運用において効率的かつ効果的にプライバシを確保する際の問題と解決策の知識が、プライバシパターンとして提案および蓄積されつつある[Lobato09]。しかしながらそれらのプライバシパターンは個別に提案記述されており、関係や組み合わせについて未整理である。また、それらに関連するプライバシの調査研究は個々に多数進められながらも、まとまった形での全体の整理は十分でないことが指摘されている[Smith11]。

本調査研究の位置づけと戦略的意義: 本調査研究では、申請者らが定義済みのセキュリティメタモデル[Haz12][Fer15a]等を応用する形でセキュリティとプライバシの両方を扱うメタモデルを定義する。さらに、申請者らが提案済みのセキュリティパターン[Fer15b]やその分類・活用手法[Fer08][Kobashi14]を応用して、プライバシも含めて事例やパターンを扱う知識ベースとその管理システムを具体的に整備し、それを一貫して活用して参照アーキテクチャを導出する手法を具体的に確立する。クラウドサービスの開発者や運用者、さらには利用者が効率的かつ適切にセキュリティとプライバシを組み入れられる点で優れている。

3. 調査研究の概要

本調査研究では、クラウドサービスの開発運用におけるセキュリティとプライバシの確保のために、SSR 賛助企業メンバーと連携の上、次の項目について調査研究を行う。また SSR フォーラムの活動方針に従い、全記録と成果を Web 上に公開すると共に、終了時に調査研究結果を作成し公開する。

(1) メタモデルの定義

クラウドサービスにおけるセキュリティとプライバシの両方を扱う知識および参照アーキテクチャのメタモデルを定義する。具体的には、共同研究者が提案済みのセキュリティを扱うメタモデル群[Fer15a][Haz12]やセキュリティパターンのモデル[Nhla10]に加え、共同研究者が検討したプライバシを統合的に扱う枠組み[吉岡 14]や外部の他の関連モデルを調査し統合する。さらにクラウドサービスの開発等におけるパターンやプラクティス群から特徴を特定し組み入れる形で拡張することでメタモデルを定義する。想定するメタモデルのイメージを、セキュリティ面を中心として図 2 に示す。

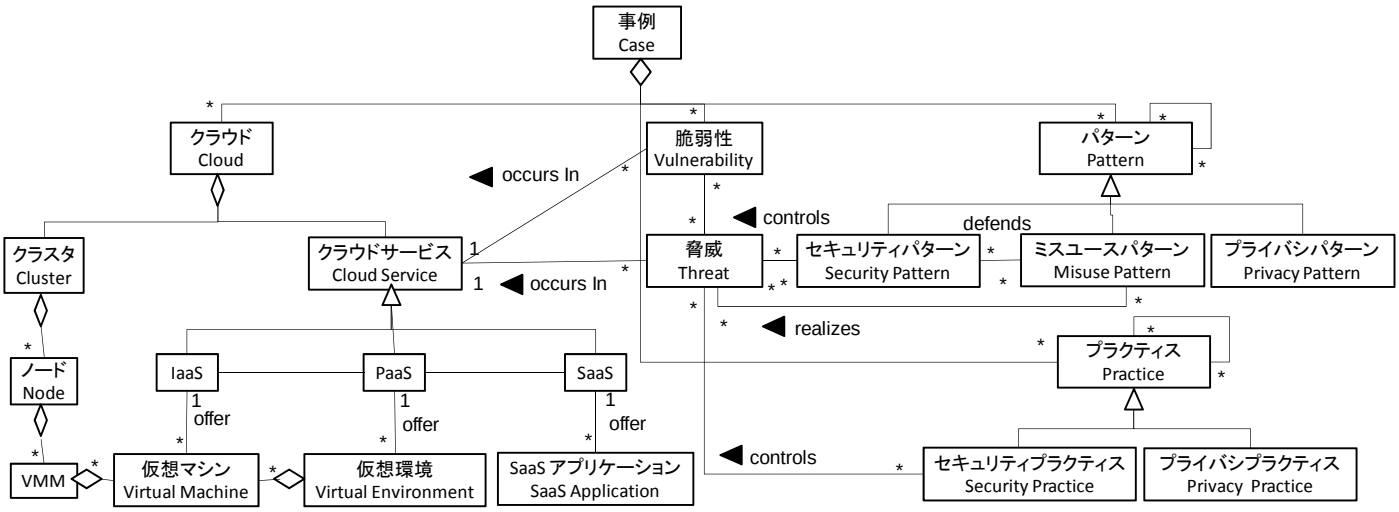

図 2: 知識および参照アーキテクチャのメタモデルのイメージ（[Fer15a]を基に拡張）

(2) 知識ベースの構築

クラウドサービスのセキュリティやプライバシ上の事例、申請者らが国際的にリードする各種のパターン（[Fer15b]他）、プラクティスを調査し、賛助企業メンバーを含む申請者らの経験に基づくパターンやプラクティスの新規記述を含めて特徴と関係をメタモデル上で整理体系化し、知識ベースとしてまとめる。まとめるにあたり、ソフトウェア品質知識体系 SQuBOK を申請者らが策定した際の体系化プロセスとセキュリティ関連の知識、申請者らが実現済みのパターン抽出手法[Nomoto11]・拡張手法[中野 13]、および、申請者らのパターン分類手法[Fer08]等を知識体系化と拡充に応用する。

(3) 知識ベース管理システムの実現

知識ベースの利便性を高めるため、申請者らのパターン検索システム[Kubo08]および知識・事例ベース管理システム[Saito15]の仕組みを応用して、知識間の関連を通じた検索、全体・詳細閲覧および管理を容易に可能とする知識ベース管理システムを実現する。

(4) 参照アーキテクチャの導出手法の実現

知識ベース管理システムを活用してセキュリティおよびプライバシ要求を獲得分析し、リスク対策を検討設計した結果を参照アーキテクチャとしてメタモデルに基づき導出する方法とプロセスを手法としてまとめる。その際、申請者らのセキュリティパターンの適用支援手法[Kobashi14]や開発方法論[Fer10]、要求獲得手法[Saeki13]等を応用する。

(5) 実証実験と改善フィードバック

SSR 賛助企業メンバーからクラウドサービスの開発や選択・運用の実問題あるいはそれに近い問題設定を受け、産学共同でメタモデル、知識ベースおよび参照アーキテクチャ導出手法を実験的に適用し、有効性を検証および検証結果に基づき改善を施す。

4. 調査研究の進め方

申請者らの実績の拡充に加えて、関連研究の調査と応用、SSR 協賛企業の研究参加者の知見やパターン等の入力および共同作業ワークショップを持って進める。下記に協賛企業メンバーの方々を加

えて十数名程度のプロジェクトとする。また、技術調査にあたり文献や学会発表をあたると同時に、国内外の研究者・実務家の招待講演を検討している。

大学側メンバー

- 鷲崎 弘宜、早稲田大学グローバルソフトウェアエンジニアリング研究所、所長・准教授（主査）
- 大久保 隆夫、情報セキュリティ大学院大学、教授
- 小形 真平、信州大学 大学院理工学系研究科情報工学専攻、助教
- 海谷 治彦、神奈川大学 理学部、教授
- 櫨山 淳雄、東京学芸大学 教育学部、教授
- 吉岡 信和、国立情報学研究所 アーキテクチャ科学研究系、准教授
- Eduardo Fernandez, Florida Atlantic University, Professor

企業側メンバー（協賛企業からメンバー追加募集予定）

- 鹿糠 秀行、(株)日立製作所 研究開発グループ システムイノベーションセンタ
- 近藤 佑樹、(株)日立製作所 研究開発グループ システムイノベーションセンタ

参考文献

[Andriole15] S.J. Andriole, “Who Owns IT?”, CACM, Vol. 58 No. 3, Pages 50-57, 2015
[Fer15a] E.B. Fernandez, et al, "Building a security reference architecture for cloud systems," REJ, Jan. 2015
[NIST13]NIST Cloud Computing Security WG, "Cloud computing security reference architecture"2013
[Lobato09] L.L. Lobato, et al., "Patterns to support the development of privacy policies", OSA 2009
[Smith11] H.J. Smith, et al., "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, Vol. 35 No. 4, pp. 989-1015, 2011.
[Haz12] A. Hazeyama, “Survey on Body of Knowledge Regarding Software Security,” SNPD 2012
[Nhla10] A. Nhlabatsi, et al., “Security Patterns: Comparing Modeling Approaches”, in “Software Engineering for Secure Systems”, IGI Global, 2010
[吉岡 14]吉岡,“プライバシとセキュリティの要求工学の統合化するフレームワーク”, SES’14 ワークショップ
[Fer15b] E.B. Fernandez, et al., “Cloud Access Security Broker (CASB),” AsianPLoP 2015
[Nomoto11] Y. Nomoto, et al., “Automated Extraction of Analysis Patterns”, AsianPLoP 2011
[中野 13] 中野, 角谷, 鈴木, 鷲崎, 深澤, 羽生田, 本橋, 三上, “パターンの構造化を利用したパターンランゲージの拡充”, 電子情報通信学会論文誌, Vol.J96-D, No.11, pp.2705-2709, 2013
[Fer08] E.B. Fernandez, et al., “Classifying security patterns,” APWeb 2008
[Kubo08] A. Kubo, H. Nakayama, H. Washizaki, Y. Fukazawa, “PatternRank: A Software-Pattern Search System Based on Mutual Reference Importance,” PLoP 2008
[Saito15] 齊藤, 櫨山, 吉岡, 小橋, 鷲崎, 海谷, 大久保, “ソフトウェアセキュリティ知識を活用したセキュアなソフトウェア開発のための事例ベース管理システムの開発”, 信学報告 KBSE2014-57, 2015
[Kobashi14] T. Kobashi, N. Yoshioka, H. Kaiya, H. Washizaki, T. Okubo, Y. Fukazawa, “Validating Security Design Pattern Applications by Testing Design Models,” IJSSE, Vol. 5, Issue 4, pp.1-30, 2014
[Fer10] E.B. Fernandez, N. Yoshioka, H. Washizaki, et al., “Using security patterns to develop secure systems”, in “Software Engineering for Secure Systems”, IGI Global, pp16-31, 2010
[Saeki13] M. Saeki, S. Hayashi, H. Kaiya, “Enhancing Goal-Oriented Security Requirements Analysis Using Common Criteria-Based Knowledge,” IJSEKE, Vol. 23, No. 05, pp. 695-720, 2013

申請者略歴

氏名: 鷲崎 弘宜（わしざき ひろのり）
学歴: 1999 年 3 月 早稲田大学理工学部情報学科卒業
2001 年 3 月 早稲田大学大学院理工学研究科修士前期課程修了
2003 年 3 月 早稲田大学大学院理工学研究科博士後期課程修了、博士（情報科学）
職歴: 2002 年 4 月～2004 年 3 月 早稲田大学理工学部 助手
2004 年 4 月～2008 年 3 月 国立情報学研究所 助手（2007 年より助教）
2008 年 4 月～現在 早稲田大学理工学術院 准教授、国立情報学研究所 客員准教授
2010 年 11 月～現在 早稲田大学グローバルソフトウェアエンジニアリング研究所所長
専門: 設計、再利用、品質保証を中心にソフトウェアエンジニアリングの研究、教育、社会展開に従事。IEEE Computer Society Japan Chapter Chair、SEMAT Japan Chapter Chair、情報規格調査会 SC7/WG20 主査、論文誌 IJSEKE、IEICE Trans、コンピュータソフトウェア誌 各編集委員ほか。
連絡先: 〒169-8555 東京都新宿区大久保 3-4-1 早稲田大学 63 号館 0503 室
Tel:03-5286-3272 E-mail: washizaki@waseda.jp Web:http://www.washi.cs.waseda.ac.jp