クラウドサービスの開発と運用においてセキュリティとプライバシを扱うためのメタモデル

鷲崎 弘宜[1] 福本 創太[1] 山本 美聡[1] 芳澤 正敏[1] 大久保 隆夫[2]
小形 真平[3] 海谷 治彦[4] 加藤 岳久[5] 櫨山 淳雄[6] 吉岡 信和[7]

[1]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
169-8555 東京都新宿区大久保 3-4-1
washizaki@waseda.jp

[2]情報セキュリティ大学院大学 [3]信州大学

[4] 神奈川大学 [5]東芝 インダストリアルICTソリューション社

[6]東京学芸大学 [7]国立情報学研究所

あらまし 我々は、クラウドサービスにおけるセキュリティやプライバシを扱うメタモデルを定義する。同メタモデルを参照することで、一貫した形で効率的に事例やパターン、プラクティスといった事実や実証済みの知識を記述整理できる。記述整理した結果を知識ベースとして参照することにより、クラウドサービスの要求定義、設計、実装、運用、保守のあらゆるフェーズにおいて事実や実証済みの知識に基づいたセキュリティとプライバシの組み入れ、確認、改善を支援できる。さらにそれらを、同一のメタモデルに基づき、実装の詳細に立ち入らない参照アーキテクチャ上で一貫かつ追跡可能な形で実現することを支援できる。

A Metamodel for Handling Security and Privacy in Cloud Service Developments and Operations

Hironori Washizak[1] Sota Fukumoto[1] Misato Yamamoto[1] Masatoshi Yoshizawa[1]
Takao Okubo[2] Shinpei Ogata[3] Haruhiko Kaiya[4] Takehisa Kato[5] Atsuo Hazeyama[6]
Nobukazu Yoshioka[7]

[1]Waseda University, Global Software Engineering Laboratory
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, JAPAN
washizaki@waseda.jp
[2]Institute of Information Security [3]Shinshu University
[4]Kanagawa University [5]Toshiba Industrial ICT Solutions Company
[6]Tokyo Gakugei University [7]National Institute of Informatics

Abstract In this paper, we propose a metamodel for handling security and privacy in cloud service developments and operations. The metamodel is expected to be utilized for

forming a knowledge-base to accumulate, classify and reuse existing cloud security and privacy patterns and practices in a consistent and uniform way. Moreover the metamodel and knowledge-base are expected to be utilized for designing and maintaining reference architecture for each secure and privacy-incorporated cloud service developments.

1　はじめに

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、クラウドサービス事業者（プロバイダ）におけるサービスやデータの集中管理に伴い、セキュリティおよびプライバシの確保が社会的急務となっている。

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。

そこで我々は、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（実装の詳細に立ち入らない抽象アーキテクチャ）に共通なメタモデルの案を定義する。全体の構想を図 1 に示す。

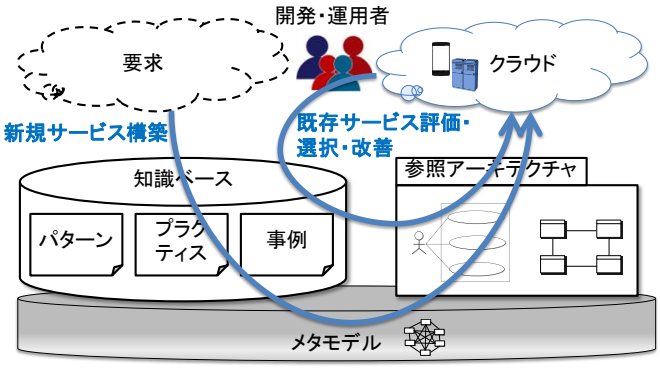

図 1: クラウドサービスにおけるメタモデルと応用の全体構想

本稿の以降においては、2 章においてクラウドサービスのセキュリティおよびプライバシを扱う上での課題をまとめ、その課題を受けて 3 章においてメタモデルの要求を整理し、要求に基づくメタモデルの案を説明する。4 章では、メタモデルの応用可能性を議論し、5 章では関連研究について言及する。最後に 6 章で本稿の内容をまとめ、将来の展望を述べる。

2　クラウドサービスの課題

クラウドサービスの開発と運用においてセキュリティとプライバシを扱うにあたり開発者や運用・保守者が直面する課題や重大性を以下に整理する。

2.1 セキュリティとプライバシの重大性

導入する個人や組織から独立したクラウドサービス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は導入上の重要な課題として認識されている[1]。例えば[2]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。

この重要性の高まりを受けて、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取り組みが動機づけられ、その取り組みにおいて以降に述べる課題の扱いを必要とする。

2.2 階層構造と横断: メタモデルの必要性へ

クラウドサービスの形態は、提供資源の種別に応じてソフトウェアアプリケーション提供の SaaS(Software as a Service)、プラットフォーム提供の PaaS(Platform as a Service)、ハードウェアや基盤提供の IaaS(Infrastructure as a Service)に大別でき、階層を構成する[3]。

これらの層はそれぞれの利用者の立場からは独立し他の層が隠ぺいされているように見えるが、実際には以下の点から階層を超えたセキュリティ・プライバシの考慮、追跡、対応付けが必要となる。

- 階層スタックにおけるセキュリティ・プライバシの扱い: クラウドサービスが管理、加工、提供するデータは階層スタック中のあらゆる階層で関係するため、階層を超えてセキュリティ(およびプライバシ)の要求の明確化および注意深い対策が必要である[4]。
- 階層の異なるクラウドサービス連携におけるセキュリティ・プライバシの扱い: クラウドサービスはしばしば、階層を超えて連携させられる。このとき、個々の階層に閉じずに超えたセキュリティ・プライバシの要求の明確化および対策が必要である。例えば[5]において階層を超えたクラウドサービス連携時のアクセス制御のポリシーの記述と処理を扱うアーキテクチャが提案されているが、その実装は今後の課題とされている。

階層を超えたセキュリティ・プライバシの要求と対策の扱いには、それらを階層を超えて一貫して表現、参照、処理することの基盤となるメタモデルが必要である。

2.3 動的な構成と共有: 実証済み知識の必要性へ

クラウドサービスの主要な特性として、動的な構成が挙げられる。費用を抑えつつ性能要求の変更(例えばユーザ数の増大)に対応するために、クラウドサービスはしばしば、運用を停止することなく、インフラ側の利用サーバ数の変更といった動的な構成変更が行われる。

また、マルチテナント方式と仮想化を通じた資源共有もクラウドサービス特有の性質である。

これらの性質は、従来のサービスおよびサービス提供ソフトウェアとは異なった(あるいはより大きな)セキュリティおよびプライバシ上のリスクを顕在化させ、従って独自あるいはより強固なセキュリティ・プライバシ要求や対策を必要とする。例えば[5]において、資源共有に伴うクラウドサービス特有のセキュリティリスクの課題が指摘されている。

クラウドサービス特有のセキュリティの要求や対策を、クラウドサービスの開発や運用に詳しくない開発者や運用者が一から扱うことは困難であり、過去の実証済みの知識の一貫した形での参照が望ましい。また専門家であっても、過去の実証済みの知識群を矛盾なく組み合わせて構成するためには、それらをメタモデル上で一貫した形で参照および再利用可能なことが望ましい。

クラウドサービスやシステムの開発や運用におけるセキュリティの効率的かつ効果的な扱いを目的として、セキュリティに関するメタモデル[6][7]や抽象的な共通参照アーキテクチャ[8]が提案されているが、プライバシは扱われていない。またセキュリティとプライバシの両者の扱いを試みるメタモデルや概念モデルの提案はあるが[9][10][11]、クラウドサービスにおけるメタモデルは明らかとなっていない。

これらの既存の成果は、妥当性が一定程度検証されたものであり、互いに密接に関わり同時の考慮が重要なセキュリティとプライバシの

両者の扱いにあたり、本稿におけるメタモデルの基礎となりえる。

3　メタモデル

上述のクラウドサービスの課題整理を受けて、本稿ではクラウドサービスにおいて明示的、一貫、かつ、階層横断的にセキュリティおよびプライバシの要求、ポリシー、対策、それらを統合した実証済み知識を扱うためのメタモデルを提案する。

以降においてメタモデルに対する要求を明確とし、続いて、その要求を満足するメタモデルを示す。

3.1 メタモデルへの要求

要求を以下に整理する。

- R1. 階層の一貫した扱い: メタモデルにおいて階層を超えて一貫した形でセキュリティ・プライバシの要求、ポリシー、対策、実証済みの知識を扱える必要がある。
- R2. 既存メタモデルとの整合: クラウドサービスやシステムにおけるセキュリティの扱いのメタモデル（[6][7]など）や、クラウドに限らない汎用のセキュリティ・クラウドメタモデル（[9][10]など）は、妥当性が一定程度検証された形で主要な概念と概念間の関係を整理したものであり、新たに提案するメタモデルはそれらと整合することが望ましい。
- R3. パターン・プラクティスへの容易なアクセス: クラウドサービスの開発や運用においてセキュリティやプライバシを効果的に組み入れるための仕組みや要求、ポリシー定義に関する実証済みの知識がパターンおよびプラクティスの形で様々に公開されている（例えば[12]）。さらにクラウドサービスに特化していないソフトウェアやサービス全般に対するセキュリティやプライバシのパターンも様々に公開されている（例えば[13][14]）。それらをメタモデル上で共通に分類整理することで、共通の問題に対する対策の検索や比較検討、さらには関連する知識の参照といったアクセスを容易とすることが望ましい。

3.2 具体的なメタモデル

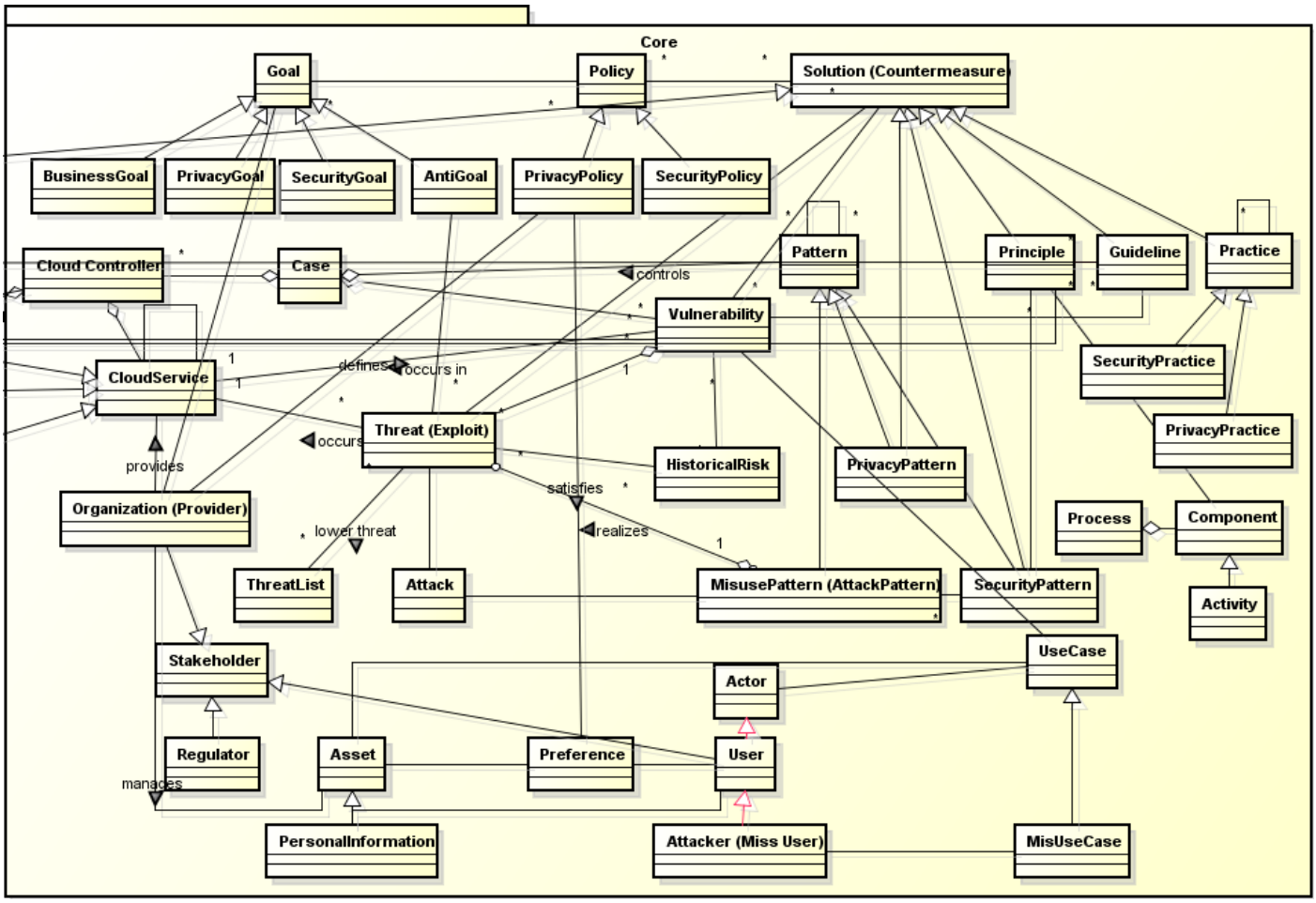

図2: コアパッケージの案（抜粋）

上述の要求 R1-R3 を受けて、我々はクラウドサービスの開発や運用においてセキュリティ・プライバシを扱うメタモデルの案を、コアパッケージ、ソフトウェアパッケージ（SaaS 相当）、プラットフォームパッケージ（PaaS 相当）、インフラパッケージの 4 部分に分けて UML クラス図を用いて定義することとした。

- コアパッケージ: クラウドサービスの階層スタックの特定階層によらない共通の主要な概念および概念間の関係を整理したモデルである。初期案を図 2 に示す。共通概念をコアパッケージに整理することで階層を超えた一貫したセキュリティ・プライバシの扱いを可能とする（要求 R1 の扱い）。またこの初期案は、既存のメタモデルと概ね整合する形を取っている（要求 R2 の扱い）。
- ソフトウェアパッケージ: SaaS を中心にソフトウェアアプリケーション階層固有の概念を扱う。例えばセキュリティ対策（プラクティスともみなすことができる）の一種であるコーディングルールは、基本的にはソフトウェアアプリケーションレベルで扱われるため、ソフトウェアパッケージ内に位置づける。初期案を図 3 に示す。
- プラットフォームパッケージ: PaaS を中心にプラットフォーム階層固有の概念を扱う。初期案を図 3 に示す。
- インフラパッケージ: IaaS を中心にインフラ階層固有の概念を扱う。初期案を図 3 に示す。

上述のように階層に共通概念と固有の概念

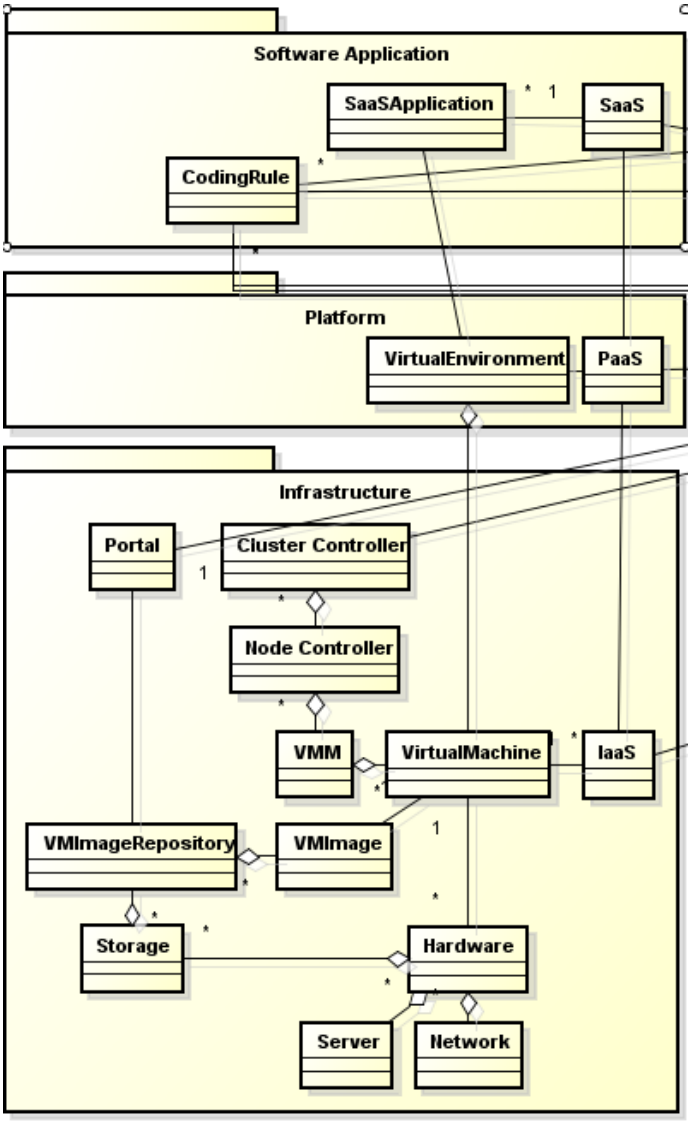

図3: 階層固有のパッケージの案（抜粋）

をパッケージに分けて整理することで、知識ベースを将来構築するに当たり各種のパターンやプラクティスを整理しやすくすることを意図している（要求 R3 の扱い）。

4　メタモデルの活用

メタモデルの活用として、知識ベースの構築、および、参照アーキテクチャの導出・活用を検討している。

4.1 知識ベースの構築

メタモデルは、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ことに用いることができる。

4.2 参照アーキテクチャの導出と活用

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を導出および保守するにあたり、同じメタモデルを参照することで、効率的かつ一貫した参照アーキテクチャの導出と保守を支援する。

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ことが期待できる。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ことが期待できる。

5　関連研究

[6]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[8]。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[14]。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[15]。

6　おわりに

本稿では、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に共通なメタモデルの案を定義し、その将来的な応用可能性について言及した。

今後の展望として、具体例を用いたメタモデルの検証と洗練、具体的な知識ベースの構築、ならびに、それらを用いた参照アーキテクチャの導出と保守を通じたセキュリティ・プライバシの効率的かつ効果的な扱いの検証が挙げられる。

謝辞

本研究は情報科学国際交流財団 2015 年度 SSR 産学戦略的研究フォーラムの助成を受けて実施した。

参考文献

[1] Rania Fahim El-Gazzar, “A Literature Review on Cloud Computing Adoption Issues in Enterprises,” IFIP Advances in Information and Communication Technology, Volume 429, 2014, pp 214-242.

[2] S.J. Andriole, “Who Owns IT?”, CACM, Vol. 58 No. 3, Pages 50-57, 2015.

[3] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, “On Technical Security Issues in Cloud Computing,” Proceedings of the IEEE International Conference on Cloud Computing (CLOUD 2009), Bangalore, India, 21-25 September, 2009.

[4] S. Subashini, , V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, Vol.34, No.1, pp.1–11, 2011.

[5] Abdulrahman A. Almutairi, Muhammad I. Sarfraz, Saleh Basalamah, Walid G. Aref, Arif Ghafoor, “A Distributed Access Control Architecture for Cloud Computing,” IEEE Software, Vol. 29, No. 2, pp.36-44, 2012.

[6] E.B. Fernandez, et al, "Building a security reference architecture for cloud systems," REJ, Jan. 2015

[7] A. Hazeyama, “Survey on Body of Knowledge Regarding Software Security,” SNPD 2012

[8] NIST Cloud Computing Security WG, "Cloud computing security reference architecture"2013

[9] C. Kalloniatis, E. Kavakli, S. Gritzalis, “Addressing privacy requirements in system design: the pris method,” Requirements Engineering, Vol.13, No.3, pp.241–255, 2008.

[10] Ricardo Tesoriero, et al. “Model-Driven Privacy and Security in Multi-modal Social Media Uis,” International Workshops MSM 2011.

[11] 吉岡信和, “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

[12] E.B. Fernandez, et al., “Cloud Access Security Broker (CASB),” AsianPLoP 2015

[13] 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

[14] L.L. Lobato, et al., "Patterns to support the development of privacy policies", OSA 2009

[15] H.J. Smith, et al., "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, Vol. 35 No. 4, pp. 989-1015, 2011.