SSR 平成 28 年度 調査研究プロポーザル

平成 28 年 5 月 20 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

複雑なネットワークソフトウェアシステムにおけるセキュリティ＆プライバシ・エコシステムの調査研究

2. テーマの戦略的意義／位置付け

背景: システム構成や環境、機能、要求が多様かつダイナミックに変化する IoT および大量のデータストリームを扱うクラウドコンピューティング、さらには、フォグ（クラウド＋分散処理）コンピューティングが進展しつつある。これらの複雑なネットワークソフトウェアシステムにより、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[IPA][ASC]では IoT 環境におけるセキュリティやプライバシ対策・考慮の重要性が指摘され、[And15]ではクラウド環境におけるセキュリティの確保の重要性が指摘されている。

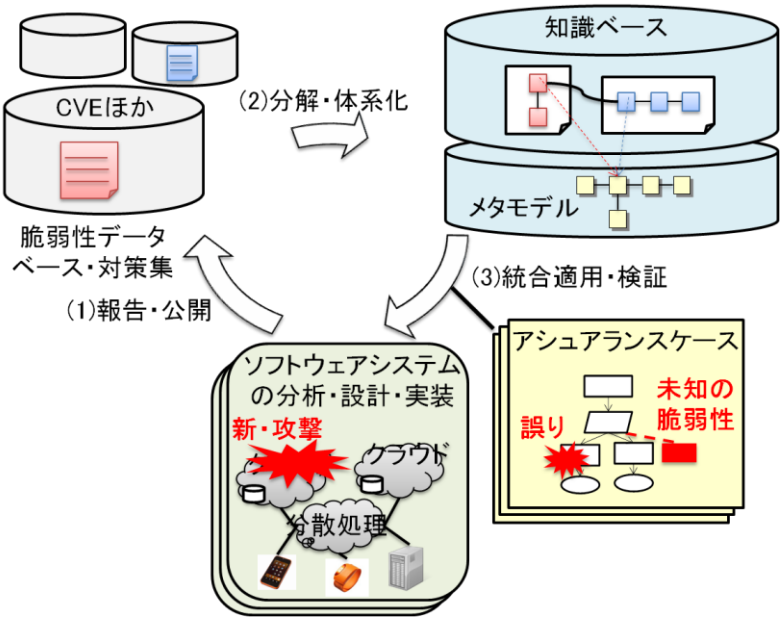
問題: 複雑なネットワークソフトウェアシステムへのセキュリティやプライバシの作り込みは通常、発生した過去のインシデントにおける脆弱性識別や実証済みの対策を積み重ねることで達成される。実証済みの対策には原則やガイドラインのような抽象度が高く多くの文脈で有効な基礎的なものから、抽象度が低く特定の文脈で有効なパターンまで様々である。

申請者らは 2015 年度 SSR において、クラウドサービスを対象に、セキュリティおよびプライバシをアーキテクチャ上で組み入れるための共通メタモデルを構築した[鷲崎 15][Was16]。同メタモデルにより、既知の脆弱性や対策、それらをまとめたパターンといった知識を体系的に整理し、一貫した形で参照し再利用することが可能となった。例えば櫨山らは同メタモデル上で各種のプライバシ技術を整理している[櫨山 16]。ただし、既存の知識をメタモデル上で整理するために一定の作業が必要であり、知識ベースの大規模化、さらには、日々新たに報告される脆弱性や対策を扱えるような最新化を実現できなかった。また、報告される問題や対策の質はまちまちであり、日々更新する仕組みの欠如や要求・問題・対策間の関係の曖昧さが知識の高信頼化の妨げとなっている。

解決: 共通の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の企画から開発、運用に到るライフサイクル中のセキュリティ＆プライバシに関わる様々な成果物や知識等を統合再利用して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・運用へ役立てる共存・循環・進化型の「ソフトウェアシステム・セキュリティ＆プライバシ・エコシステム（生態系）」を実現する（次ページ図）。

具体的には、**(1)**以降の調査研究の基礎を得るために既存のエコシステムやセキュリティ＆プライバシ技術、脆弱性・対策の公開状況を調査する。そのうえで、**(2)**脆弱性や対策の報告から共通部分

をパターン等の知識としてメタモデル上で半自動的に整理する技術を研究し、メタモデルに基づく知識ベースの大規模化と最新化を達成する。さらに(3)メタモデルに基づき整理された知識群を組み合わせた新システムの開発および既存システム拡張をモデルベースで支援する技術を研究する。その際、アシュアランスケースによりセキュリティ＆プライバシ確保の根拠として、適用知識を表明する。これにより、要求から問題、対策、知識まで追跡可能となり、リスクや攻撃発生時の問題箇所識別を容易とし、新たな脆弱性や対策の効率的な報告および知識ベース中の知識更新を支援、知識の高信頼化と最新化に寄与する。



関連研究: セキュリティやプライバシを扱うメタモデルは様々に提案されているが[Fer15][Haz12][Kal08][Tes11][Arj14]、同一概念間についてしばしば異なる関係が与えられており、また、扱う問題領域に依存する部分と非依存な部分が必ずしも明確ではない。

セキュリティのエコシステムとして、クラウドサービスに特化したもの[Fer16][Ko15]やネットワークシステム全般を扱うもの[VAR]が提案されている。これらは、種々のセキュリティ技術やツール群、利害関係者を共存・発展させる点で共通するが、抽象的な枠組みの提案に留まり、実際のインシデントから脆弱性や対策を機械的に導出し、体系化整理するという一連の流れを具体的に支援するものではない。またプライバシを扱わない。

本調査研究の位置づけと戦略的意義: 申請者らは 2015 年度に SSR フォーラムの助成を受けて、代表的な既存メタモデル群を統合し、かつ、クラウドサービスに依存する部分と非依存な部分を明確とした[鷲崎 15][Was16]。得られたメタモデルを改訂の上、本申請研究の基礎として用いる。

本調査研究が実現する具体的なセキュリティ＆プライバシ・エコシステムは、既存の抽象的なエコシステムの枠組みの一つのインスタンスと捉えられる。ただし本調査研究は、脆弱性や対策の再利用・検証、更なるインシデント発生時の脆弱性や対策の抽出と体系化という一連の流れを具体的に支援する点、および、プライバシもあわせてメタモデル上で一貫して扱う点で優れている。

3. 調査研究の概要

本調査研究では、複雑なネットワークソフトウェアの開発運用におけるセキュリティとプライバシの効率的・効果的・持続的な確保のために、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) エコシステムの枠組みと脆弱性・対策の報告調査

研究の基礎を得るために、(1a) ネットワークソフトウェア全般に有効な既存のエコシステム、(1b) 既存のセキュリティ＆プライバシ対策技術研究、(1c) 既存のセキュリティ＆プライバシの脆弱性・対策の報告リポジトリを調査し、サーベイ論文としてまとめる。(1b)について本申請研究メンバーを中心として予備的な調査結果を発表済みであり[Ito15][櫨山 16]、2016 年度に調査範囲を拡大する。

(2) 報告からのメタモデル上での知識整理と体系化

日々アップデートされる Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD), Japan Vulnerability Notes (JVN)等の代表的な脆弱性データベースやそれらからリンクされた個々の対策報告から、共通部分をパターン等の知識として抽出し、他との関連付けによる体系化を経てグラフベースの知識ベースを構築および更新する。各データベースや報告集の記述様式はまちまちであり、メタモデル中の語彙へとマッピングして一貫して扱うことを実現する。また、各データベースや報告集の中では、例えば下図は CVE [CVE]における異なる脆弱性の記述であるが、to に続いた脅威（破線）の指定、via に続いた攻撃手法（下線）の指定など、暗黙の記述規則を見て取れる。その手動あるいは機械的な学習と明示的な規則化によりメタモデルへの展開を実現する。関連付けには、セキュリティ＆プライバシ特有の特徴を手掛かりとした自然言語処理の適用を検討する。

CVE-2016-2000

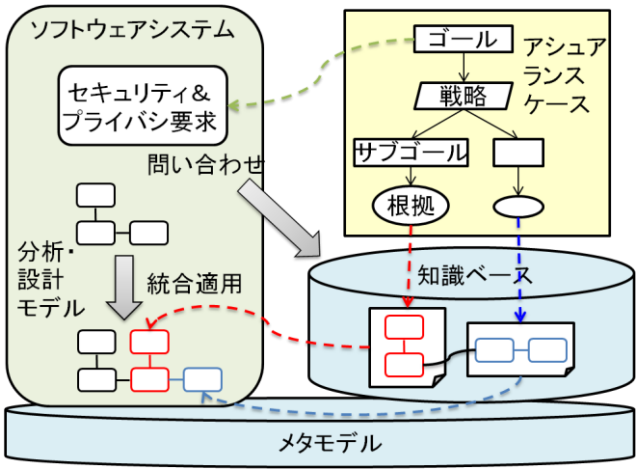
HPE Asset Manager 9.40, 9.41, and 9.50 and Asset Manager CloudSystem Chargeback 9.40 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, *related to the Apache Commons Collections (ACC) library.*

CVE-2016-0790

CloudBees Jenkins before 1.650 and LTS before 1.642.2 *do not use a constant-time algorithm to verify API tokens*, which makes it easier for remote attackers to determine API tokens via a brute-force approach.

(3) モデルベースの知識統合適用とアシュアランスケースによる表明

メタモデル上に整理された知識群を、知識ベース上で要求に基づき問い合わせて検索し、組み合わせて新ソフトウェアシステムを開発あるいは拡張することを支援する手法を実現する。ここで、申請者らの過去のセキュリティパターン適用・検証技術[Shi10][Kob14]を発展応用し、ソフトウェアシステムの分析・設計モデルに対するモデル変換を通じた知識群を組み合わせた適用を基本とする(下図)。適用にあたりセキュリティ＆プライバシ要求に対する対策の統合的適用、その実現結果としての設計、実装が有効な根拠の表明として、知識ベース中の知識を参照するアシュアランスケースの記載も支援する。これにより、以降の運用でリスクや攻撃が発生した際に、アシュアランスケース上で誤りや新たな脆弱性・問題を識別し、追跡可能な分析、設計、実装上で対策を検討すると同時に、その脆弱性・対策を報告しやくする。さらには知識ベース中の知識の更新を通じて高信頼化・最新化を支援する。



(4) 実証実験と改善フィードバック

SSR 賛助企業メンバーと産学共同でエコシステム全体の適用実験を実施し、その有効性を検証および検証結果に基づき改善を施す。適用対象として、2015 年度の SSR フォーラムの助成を受けて開発

したクラウドサービス[鷲崎 15][Was16]の発展を念頭に、2016 年度に一定の複雑さのある実用に近いネットワークソフトウェアシステムを実装して用いる。

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追加募集者を加えて十数名程度のプロジェクトとする。技術調査にあたり、国内外の研究者・実務家の招待講演も実施する。

<u>大学側メンバー</u>

- 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・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 学術研究院（工学系）、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
- Yann-Gaël Guéhéneuc, Ecole Polytechnique de Montreal, Professor
- Foutse Khomh, Ecole Polytechnique de Montreal, Assistant Professor

<u>企業側メンバー</u>（以下は承諾済み、他に協賛企業から追加募集予定）

- 鹿糠 秀行、(株)日立製作所 研究開発グループ、主任研究員
- 吉野 雅之、(株)日立製作所 研究開発グループ、主任研究員
- 山本 暖、(株)日立製作所 研究開発グループ、研究員
- 加藤 岳久、東芝インダストリアル ICT ソリューション社、研究主務

参考文献

[IPA] IPA セキュリティセンター, “IoT 開発におけるセキュリティ設計の手引き”, 2016
[ASC] 大塚昭彦／TECH.ASCII.jp, “セキュリティベンダー10 社予測まとめ”, 2016
[And15] S.J. Andriole, “Who Owns IT?”, CACM, Vol. 58 No. 3, Pages 50-57, 2015
[鷲崎 15]鷲崎ほか“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”CSS
[Was16] H. Washizaki, et al, “A Metamodel for Security and Privacy Knowledge in Cloud Services”, Services 2016
[櫨山 16] 櫨山淳雄ほか, “プライバシーを考慮したソフトウェア開発技術の文献に基づく動向調査”, SIGKSN 2016
[Fer15] E. B. Fernandez, et al, "Building a security reference architecture for cloud systems," REJ, 2015
[Haz12] A. Hazeyama, “Survey on Body of Knowledge Regarding Software Security,” SNPD 2012
[Kal08] C. Kalloniatis, et al. “Addressing privacy requirements in system design: the pris method,” REJ, 2008
[Tes11] R. Tesoriero, et al. “Model-Driven Privacy and Security in Multi-modal Social Media Uis,” MSM 2011
[Arj14] M.Arjona, et al., “Validation of a Security Metamodel for Development of Cloud applications,” OCL 2014
[Fer16] E. B. Fernandez, “Modeling and Security in Cloud Ecosystems,” Future Internet, 2016
[Ko15] Ko & Choo, "The Cloud Security Ecosystem, 1st Edition", Syngress, 6.18, 2015.
[VAR] VARACODE, "How Application Security Fits Into the SECURITY ECOSYSTEM", 2015
[Ito15] Y. Ito, H. Washizaki, et al. “Systematic Mapping of Security Patterns Research,” PLoP 2015
[CVE] The MITRE Corporation, “Common Vulnerabilities and Exposures”, https://cve.mitre.org/
[Shi10] Y. Shiroma, et al., “Model-Driven Security Patterns Application and Validation,” PLoP 2010
[Kob14] T. Kobashi et al “Validating Security Design Pattern Applications by Testing Design Models,” IJSSE2014

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～2016 年 3 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
2016 年 4 月～現在 早稲田大学理工学術院 教授、国立情報学研究所 客員教授
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。
ISO/IEC/JTC1/SC7/WG20 Convenor, IEEE Computer Society Japan Chapter Chair、SEMAT Japan Chapter Chair, 論文誌 IJSEKE, IEICE Trans, コンピュータソフトウェア各編集委員。
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