複数の活動にまたがるシステムのためのセキュリティ要求分析手法

海　谷　治　彦[†1]

今日の情報システムは単独で動作するわけでは無く，システムの構成要素であるソフトウェア，利用者，実行プラットフォーム等が時間的・空間的に他の複数のシステム群の活動に共用される．このような観点を考慮したセキュアな要求分析法の紹介を通して，共通問題および既存のセキュア開発手法の比較検討を行うため方向性の一つを示す．

A Method for analyzing security requirements for a system used in several different activities

HARUHIKO KAIYA [†1]

An information system today is never used alone, but other systems shares its components such as software, users and platforms over time and space. We introduce a method for analyzing security requirements taking this point into account so that we can discuss a new direction for a benchmark problem and existing methods for secure software development.

1. はじめに

今日の情報システムは全く単独の環境化において利用されることはほとんど無く，複数の活動にまたがって利用される．例えば，ウエブブラウザという単一のプラットフォームにおいて，多数の異なるソフトウェアが動作するのが当たり前である．場合によっては，私的活動と業務活動の双方がプラットフォームの資源を時間的もしくは空間的に共有する場合もある．逆に，単一のソフトウェアが異なるプラットフォームで共通利用されることで，多数の異なるプラットフォームが連結されることもある．dropbox 等のネットワークストレージによって，PC, スマートフォン，タブレット等が連結されるのが，その典型例である．

ソフトウェアもしくはプラットフォームが複数の異なる活動において共通利用される場合，予期しない情報の流れや，更新を行うことが可能となる場合がある．結果として，個々の活動で情報資産保護が徹底されていても，全体として資産保護に抜けができてしまう場合がある．既存のセキュリティ要求分析手法では，このような視点が欠けている．

本稿では，上記の問題意識に基づくセキュリティ要求分析法を考察する．提案手法は BYOD (Bring Your Own Devices) 下におけるセキュリティ要求分析手法[1)]に基づいている．

†1 神奈川大学 理学部
Kanagawa University

2. 手法の概要

図 1 に手法の概要を示す．本手法では i*モデリング言語[3)] を用いる．i*では，ある単一活動におけるシステムとシステム関係者 (図中では actor と表記) 間のゴール達成のための依存関係をモデル化する言語である．i*ではゴールとゴールを達成するための手段 (タスクと呼ばれる具体的な処理) との関係もモデル化する．以下に本手法の手順を示す．

(1) i*を用いて開発対象のシステムとシステムの関係者 (actors) をモデル化する．
(2) (1) のモデルに出現する関係者およびシステムが関係している既存の他の活動についても，同様に i*でモデル化する．
(3) 上記でモデル化した複数の i*モデルを統合する．図に示すように，同一の actor およびシステムは一つに併合する．
(4) 統合したモデル上において，予め意図しているゴール以外のゴールが達成可能か否か分析する．
(5) 意図していないゴールが達成可能であり，かつ，それが資産の保護を脅かす場合，意図していないゴールを達成不能なようにモデルを変更する．

3. 事　　例

我々は本手法を用いて生命保険の勧誘業務の IT 化について分析を行った．この業務においては，BYOD に基づき，保険勧誘員が私物の端末を用いることを想

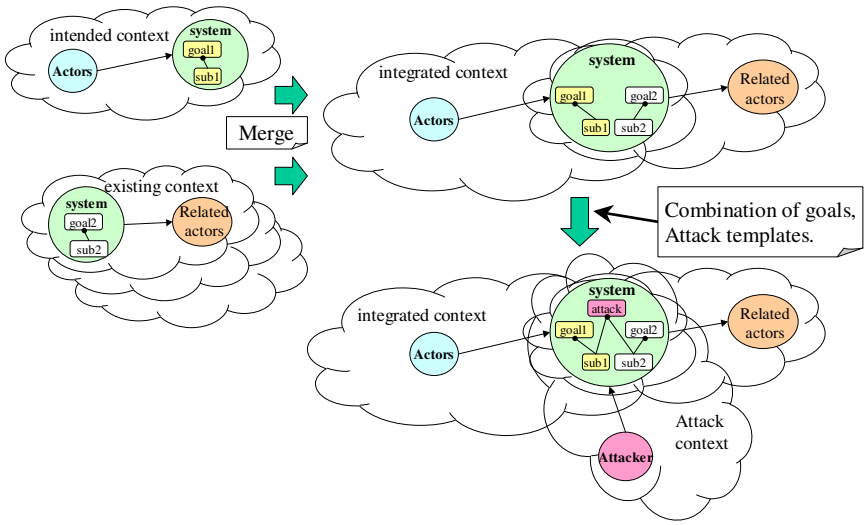

図 1 手法の概要

定した．その結果，以下のような脅威の可能性を分析することができた．

- 顧客リストの漏えい
- 位置情報の漏えいによる顧客の住居や巡回経路の情報漏えい
- 端末上の契約締結機能の改竄による意図しない契約の追加締結

最初の二つの脅威については，i*モデルにおいて，ゴール達成に別手段を用いることで，脅威を回避することができた．しかし，最後の脅威については，一部のゴール達成を諦める以外，脅威の回避をすることが不可能であることが分析できた．

4. おわりに

本手法およびワークショップテーマを鑑みて，以下のような点について今後検討してゆきたい．

- 本稿冒頭で述べたように，セキュリティは単独の活動やシステムのみに注目するのではなく，あるシステムや人物が同時に関わる活動，共用される情報や設備に注目しなければならない．こうした観点から共通問題の再検討したい．
- 本稿での提案手法では，新たな情報システム開発を行う場合，そのシステムに関わる既存の活動も考慮してモデル化を行う．実際には既存の活動も日々刻々と変化する場合がある．本手法で用いているモデリング言語 i* は時間軸上の変化に対する分析手法を提供していないため，現状の手法は，このような変化に適用はできない．この点の改善点を検討したい．
- 本稿での手法では，脅威を回避できたか否かという判定のみしかできない．これに対して，脅威をどの程度回避できたか，回避するために，どの程度，既存の活動や既存の開発プランに対して影響があるかという定量的な評価を行うことができない．この点についても，既存の手法[2] を吟味することで検討してゆきたい．
- 既存のセキュアな開発手法が，本稿で注目するようなシステムが複数の活動に同時に関係する点や，(2) で述べた活動自体が時間的に変化する点を，どの程度，考慮しているかを調査したい．

参 考 文 献

1) Kaiya, H., Okubo, T., Kanaya, N., Suzuki, Y., Ogata, S., Kaijiri, K. and Yoshioka, N.: Goal-Oriented Security Requirements Analysis for a System Used in Several Different Activities, *Advanced Information Systems Engineering Workshops*, Lecture Notes in Business Information Processing, Vol.148, Springer, pp.478–489 (2013).

2) Okubo, T., Kaiya, H. and Yoshioka, N.: Analyzing Impacts on Software Enhancement Caused by Security Design Alternatives with Patterns, *International Journal of Secure Software Engineering (IJSSE)*, Vol. 3, No. 1, pp. 37–61 (2012). http://www.igi-global.com/ijsse/.

3) Yu, E., Giorgini, P., Maiden, N. and Mylopoulos, J.: *Social Modeling for Requirements Engineering*, The MIT Press (2010). ISBN 0262240556.