様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

令和　　元 年　　９ 月　　５ 日現在

機関番号：６２６１５
研究種目：国際共同研究加速基金（国際共同研究強化）
研究期間：2016～2018
課題番号：１５ＫＫ００１８

研究課題名（和文）プライバシーとセキュリティを統合した要求分析フレームワーク（国際共同研究強化）

研究課題名（英文）Integrated Framework of Security and Privacy Requirements Engineering(Fostering Joint International Research)

研究代表者
吉岡　信和（YOSHIOKA, NOBUKAZU）

国立情報学研究所・アーキテクチャ科学研究系・准教授

研究者番号：２０３９０６０１

交付決定額（研究期間全体）：（直接経費）　　4,900,000円
渡航期間：　11ヶ月

研究成果の概要（和文）：プライバシーやセキュリティーの要求は、個々の利用者が自分に関する情報を誰にどこまで知られてもよいか、またリスクをどう取られるかという主観に基づいて決定される。そのため、どのような情報をプライバシー情報やセキュリティリスクとして扱うかは、利用者毎に考慮する必要があり、かつ、それは不明確で変化しやすい。
本研究では、セキュリティリスクをどこまでユーザに感知させるかにより、セキュリティやプライバシーのリスクを軽減できることを示した。さらに、トランスペアレンシをコンプライアンスの遵守に応用することにより、第三者が参加するコンプライアンスのチェックや、システム全体のリスク軽減に貢献することを発見した。

研究成果の学術的意義や社会的意義
ソフトウェアシステムが社会のあらゆる活動に入り込み、重要インフラの一つになってきている。そのため、システムのライフサイクルを通じたセキュリティとプライバシーの担が、超スマート社会の実現に必須である。

研究成果の概要（英文）：Privacy and security requirements are specified based on the subjective viewpoint in which each user feels risk individually. Therefore, privacy information and security risk should be dealt with an individual user, which is unstable.
We illustrated that security and privacy risk can be mitigated by showing security risk to users. In other works, transparency of security risk can mitigate security risk of a system in a while.In addition, we showed that we can apply transparency to the compliance of systems.

研究分野：ソフトウェア工学

キーワード：ソフトウェア開発効率化・安定化　ソフトウェア学　セキュリティ要求　プライバシー要求　トランスペアレンシー要求

様　式　Ｆ－１９－２

１．研究開始当初の背景

システムの構築時におけるセキュリティとプライバシーの担保のための研究は多数あるが、従来の研究は主に攻撃者の攻撃に対する防御に備えることを目的としており、利用者に関する脆弱性への対応が不十分である。例えば、内部犯や誤認識等の人に関するセキュリティやプライバシーの脆弱性への対応が十分考慮されておらず、この対処は運用時のセキュリティポリシーの策定や教育等に委ねられていた。

しかしながら、セキュリティ・インシデントの半数は内部者が関与しているという報告があり、セキュリティやプライバシーのリスクを人も含むシステム全体として軽減するためには教育や運用時の対応だけでは不十分であり、システムのライフサイクル全般に渡る対応が必須である。すなわち、システムの構築時に人に関する脆弱性に対処する手法の研究は今後益々重要になってくる。

２．研究の目的

透明性(トランスペアレンシ)は従来、信頼できる政府・組織のための情報公開の文脈で、組織の統制､民主主義の促進､汚職の防止に有効な手段として研究されてきた｡本研究はこの考え方を、ソフトウェアのセキュリティやプライバシーの人に関するリスクの軽減に応用した。

透明性の制御し、ユーザに対して適切にセキュリティやプライバシーの関心事を気づかせることにより、そのユーザの適切な判断を促し、結果的にリスクを軽減することが出来る。

３．研究の方法

適切な透明度を実現するためには、(1)不確実な人の行動、(2)透明度の決定、(3)他との競合、(4)個人の特性への適合を考慮する必要がある。

人の行動は本質的に非決定的である。例えば、重要ファイルが USB にあることを知った場合、それを机の鍵のかかる引き出しに保存して十分な対策をとる人もいれば、ポケットに不用意に入れてしまう人もいるだろう。また、同じ人が同じ情報を知ったとしてもいつも同じ行動を起こすとは限らない。透明性の要求を規定する際には、開発者はこのような不確実な人の行動をどのようにモデル化し、人に関するリスクを軽減できる透明度をどのように分析、導出できるのかの問いに応える必要がある。

透明度は、特定の情報の公開とみなすことができる。これは、情報秘匿に関する要求と相反する可能性があることを意味する。例えば、あるサービスでプライバシーに関する情報が適切に扱われているかを監視する場合、監視者には個人のプライバシーに関する情報が漏洩してしまうかもしれない。また、極秘情報の存在をその情報を知りえない人に認知させようとするとその情報の機密性と競合する。さらに、特定の情報をユーザに認知させることにより、セキュリティやプライバシーの観点以外の品質に悪影響を及ぼすことがある。例えば、正規ユーザを犯罪者のように扱う情報の提示は､そのユーザのやる気を損ない､活動の生産性を下げることになりかねない。そのため他の要求・品質と多面的に競合を発見し解決する方法を考える必要がある。

本研究は、セキュリティに関する行動心理学（Behavioral Information Security）と要求工学を融合することでこれらに対処する。

４．研究成果

セキュリティやプライバシーに関する人の行動は、セキュリティ行動学の分野で分析され、傾向が明らかになっている。人の行動モデルは、次ページの図１のように、要因間のグラフで表し、関係には仮説の確からしさの確率が付与される。

例えば、この例では、罰(sanction)の大きさは悪用(Misuse)の意図に負の影響を与えている(悪用を抑制している要因である)事がわかる。このように確率的に与えられた人の行動モデルに対して、影響度を加味した行動パターンを構築し、システムの構築時に利用可能にした。

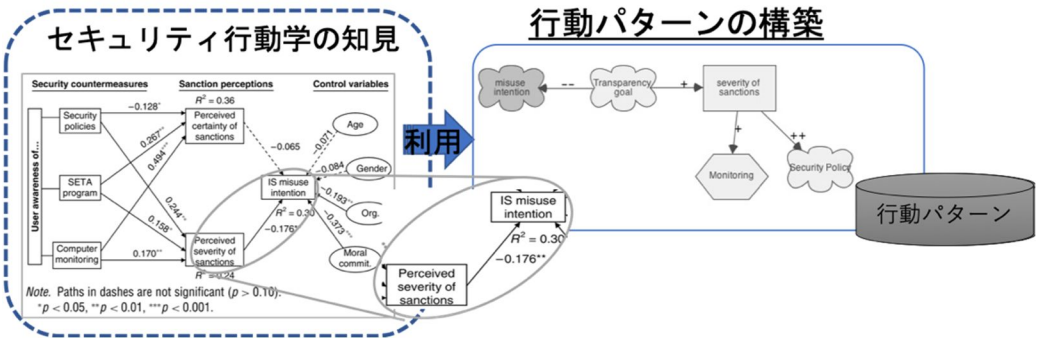

図１：行動パターンの構築

さらに、この行動パターンを使って、要求分析手法である i*を使って要求を分析することで適切なトランスペアレンシ要求を導出することができた。下の図２がその分析例である。

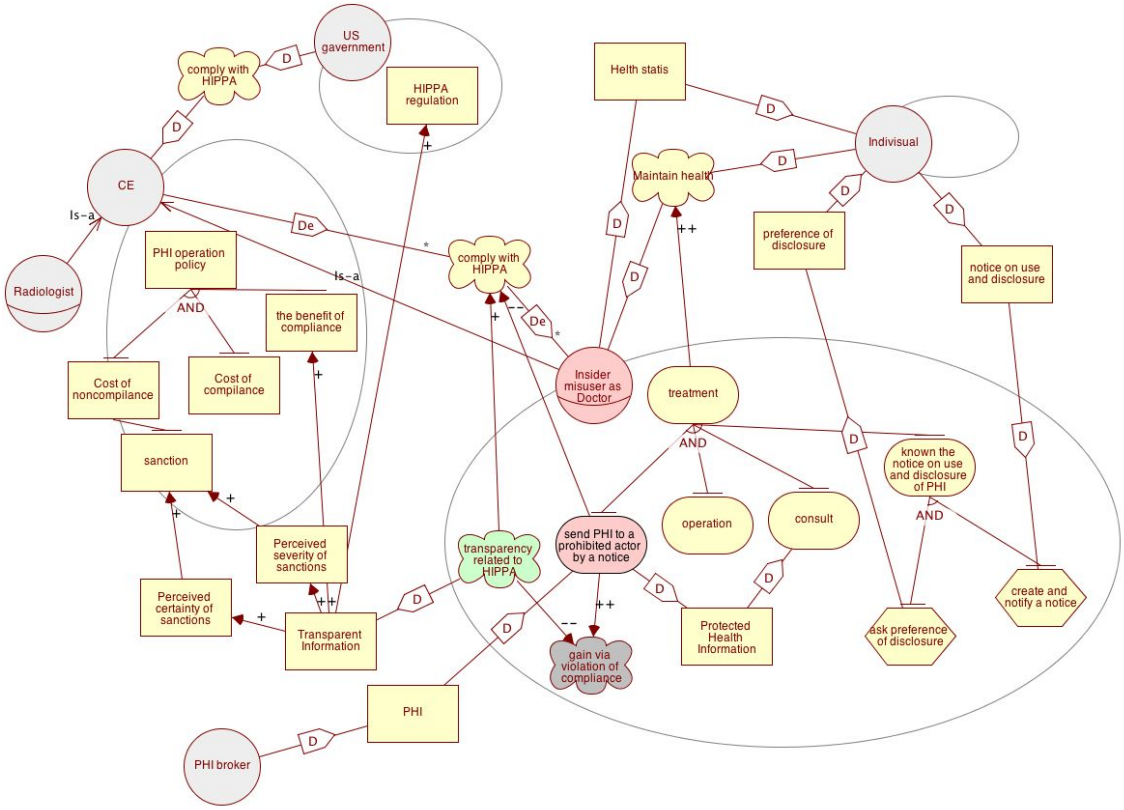

図２：トランスペアレンシ要求の分析例

５．主な発表論文等

〔雑誌論文〕（計　１件）

1. Haruhiko Kaiya, Nobukazu Yoshioka, Hironori Washizaki, Takao Okubo, Atsuo Hazeyama, Shinpei Ogata and Takafumi Tanaka, Eliciting requirements for improving users' behavior using transparency, The 4th Asia Pacific Requirements Engineering Symposium (APRES 2017), pp 41-56, Communications in Computer and Information Science, vol. 809, Springer, 2017.
2. Yijun Yu, Haruhiko Kaiya, Nobukazu Yoshioka, Zhenjiang Hu, Hironori Washizaki, Yingfei Xiong, Amin Hosseinian-Far, Goal Modeling for Security Problem Matching and Pattern Enforcement,International Journal of Secure Software Engineering (IJSSE), IGI Global, Vol.8, No.3, pages 42-57, 2017.7(invited paper)

〔学会発表〕（計　1件）

1. 河本 高文,二木 厚吉,吉岡 信和:業務プロセスの信頼性のアセスメントツール,コンピュータセキュリティシンポジウム 2017 論文集, 情報処理学会, No.2, pp.1280-1287, 山形県, 10 月 25 日 (2017).

６．研究組織

研究協力者
研究協力者氏名：Yijun Yu
ローマ字氏名：Yijun Yu

研究協力者氏名：Bashar Nuseibeh
ローマ字氏名：Bashar Nuseibeh