氏名	PATTIYANON, Charnon
学位の種類	博士（情報科学）
学位記番号	博情第 499 号
学位授与年月日	令和 5 年 3 月 24 日
論文題目	Security Weakness and Privacy Preservation Analysis of SSI Management Systems using Information Retrieval and System Modeling
論文審査委員	青木利晃 北陸先端科学技術大学院大学 教授
	平石邦彦 同上 教授
	ベウランラズバン 同上 准教授
	佐伯元司 南山大学 教授
	立石孝彰 日本 IBM Senior Research Scientist

論文の内容の要旨

The Self-Sovereign Identity (SSI) model is a cutting-edge approach to identity management that empowers individuals with complete control and sovereignty over their digital identities. This is achieved through the utilization of distributed ledger technology, allowing for autonomous administration without the need for central authorities. A system that implements the key architecture and features defined by the SSI model is commonly referred to as an SSI management system. As a personal information processing system, it is imperative that SSI management systems are designed with sufficient security and privacy measures to ensure the protection of personal information.

In SSI management systems, various security and privacy considerations can be evaluated and enhanced. The process of analyzing security weaknesses is an effective method for identifying the presence of common weaknesses in the target system. Similar to other domain software systems, SSI management systems may have specific weaknesses that require attention. The governance of the SSI management system serves as a framework for enforcing the principles and system properties defined by the SSI model, which are critical to protecting the operation of digital identities in various contexts. However, it has been noted that the current principles and system properties may not address necessary security and privacy aspects. Data sharing events within the SSI management system are unique situations in which data objects are made available with other actors. These events should be aligned with the SSI governance to ensure adequate protection.

This dissertation presents an approach to evaluating the security and privacy of the SSI management system by integrating domain expertise with information retrieval and system modeling techniques. The proposed approach consists of three solutions: mitigating SSI-specific weaknesses, improving SSI system properties, and modeling SSI data sharing events.

The first solution for enhancing security in the SSI management system is to mitigate the unique security weaknesses specific to this system. Currently, there has been limited research on SSI-specific weaknesses, making it challenging to identify them directly from the design of the SSI management system. This dissertation aims to overcome this challenge by utilizing language correlations between descriptions of common security weaknesses published in the well-respected Common Weakness Enumeration (CWE) database and the functional

requirements of the SSI management system. The goal is to infer the presence of SSI-specific weaknesses and initiate further analysis and mitigation efforts. To accomplish this, the SSI Weakness Identification Framework (SWIF) is proposed. This framework combines natural language processing and information retrieval techniques with the creation of a cross-domain transfer knowledge graph to identify SSI-specific weaknesses. The results of this study indicate that a recommender system implementing the SWIF is capable of accurately identifying language correlations and inferring valid SSI-specific weaknesses with optimal efficiency.

The second solution of the proposed approach is to improve the security and privacy of SSI system properties. This dissertation leverages laws, regulations, and standards as source documents to achieve this improvement. The principles and system properties of the SSI management system must adhere to these source documents in order to ensure proper governance of the system in terms of security and privacy. However, the definitions of laws, regulations, and standards differ from the SSI model concept, making it challenging to directly align source documents with SSI system properties. To address this challenge, this dissertation presents a systematic analysis method and an improved set of SSI system properties. The analysis method is used to assess the compatibility of security and privacy controls from source documents with existing SSI system properties, and to revise or introduce new properties as necessary. The improved SSI system properties are more globally consistent with source documents than the current set and are applicable to actual scenarios.

The final solution of the proposed approach involves a method for modeling SSI data-sharing events. This dissertation aims to comprehensively analyze these events by extracting the unique types and constraints from the SSI model concept. The events are modeled as a state transition system to provide a foundation for security and privacy analysis. The transformed SSI system properties serve as security and privacy specifications in the context of data sharing. The proposed method involves modeling the SSI data sharing state transition system using the Alloy specification language. The result could report a secure and privacy-preserving data sharing system within a specified scope.

Keywords: self-sovereign identity, weakness identification, compliance property, software modeling, security and privacy

論文審査の結果の要旨

本博士論文では，自己主権型 ID(Self-Sovereign Identity, 以下，SSI と略す)管理システムを対象として，そのセキュリティとプライバシーを分析する手法を提案している．SSI は，政府などの公的機関やサービス事業者が ID を提供管理するのではなく，個人が ID を宣言し管理するという，新しい ID の考え方であり，近年，急激に注目を集めている．SSI は，その特性上，公共性が高く，セキュリティとプライバシーに関して慎重に分析する必要がある．一方，それが運用されている事例はまだ少なく，潜在的なリスクは明確になっていないのが現状である．さらに，SSI の公共性から，それを扱う SSI 管理システムは各国の法令や国際標準に準拠する必要があるが，どのような要件を満たせば良いか明確になっていない．このように，SSI の新規性と特性から，セキュリティおよびプライバシーに関する実用化への問題が存在する．そこで，本博士論文では，SSI 管理システムの設計を対象として，これらの問題を解決する手法を提案している．

本博士論文は，潜在的な脆弱性の発見手法，法令および国際標準との一貫性分析手法，データ共有

の分析手法の提案から構成されている．従来システムと SSI 管理システムの関係を知識グラフとして表現し，recommendation system の基本的な技術を用いて，CWE(Common Weakness Enumeration)リストから SSI 管理システムと関係する項目を抽出することに成功している．また，各国の法令文書，国際標準文書と SSI の特性を関連づけ，それらへの準拠のために SSI 管理システムに要求される性質を抽出することにも成功している．分析対象の SSI 管理システムが決まると，これらの提案手法を用いて，潜在的な脆弱性を抽出し，それと関係する性質を特定することができる．このような性質が，SSI 管理システムで実現されていることを保証するために，データ共有に関する挙動を形式化し，自動検証する手法を提案している．一連の提案は，SSI に特化した領域知識を既存技術に導入して実現している．領域知識の定義において，既存技術と組み合わせて有効に働く領域知識の表現方法，および，系統的な領域知識の獲得方法を考案している．この点が新規であり，独創的な点である．また，SSI 自体が新規な概念であり，先行研究も少ないことを考慮すると，この点は高く評価できると考えられる．また，以上の一連の提案は，複数の実験により定量的に評価されており，それらの有効性を確認できている．

以上，本博士論文は，計算機科学における理論を領域特化して実践応用するための手法を提案しており，学術的にも応用面においても貢献するところが大きい．よって，博士(情報科学)の学位論文として十分に価値があるものと認めた．