改良 KT 法を用いたインタビューによるセキュリティ要求抽出手法

橋浦研究室　　118I176　高橋 侑希

1.はじめに

要求仕様書は，システム開発における最初の工程（要件定義）にて作成され，後の工程の基盤となる．このため，記載内容に不備がある場合，深刻な問題になる．

先行研究として坂田[1]の研究がある．坂田[1]の研究では OWASP JAPAN の Web Application Security Requirements[2](以下 OWASP とする)をベンチマークとし，インターネット上で公開されている要求仕様書 10 個の認証項目に着目して予備調査を実施し充足率が低いことを明らかにした．そこで，NIST SP800-63-3[3] の Authenticator Assurance Level(以下 AAL とする)とインタビュー手法を用いたアプローチを提案し，充足率の改善を試みた．坂田[1]の手法では充足率を向上させることに成功したが取り入れている AAL は認証方式の決定に利用するものであるため，認証以外の要求抽出への妥当性を保証できないという側面もある．

2.研究目的

本研究の目的は，認証対策が明記された要求仕様書の作成ができるようにすることである．そのために坂田[1]の手法を改良したうえで，セキュリティの要求抽出において必要な情報が欠落しないような要求抽出の支援を目指す．

本研究で検証する RQ は以下の 3 つである．

1. OWASP[2]における必須項目を満たす要求仕様書作成に寄与できるか
2. 先行研究の手法を改良したことによる悪影響はないか
3. リスクをどれだけ洗い出せるか

3.提案手法

目的を達成するために以下の手法を提案する．

1) リスクの洗い出しを支援する
2) 譲歩資産の特定とリスクの評価をする
3) 顧客への質問を事前に用意する
4) 質問に関する補足説明の導入
5) 質問の回答に選択肢を採用する

4.ツールの実装

本ツールは，開発者がインタビュー手法にて要求を抽出する際に併用することを想定する．実装する機能は以下の通りである．

i. 質問機能
ii. 選択肢機能
iii. ヒント機能
iv. リスク洗い出し補助機能
v. CommonVulnerabilityScoring System[4](以下 CVSS とする)機能
vi. 矛盾検知機能

5.実験

本実験では，RQ を確認するため日本工業大学大学院電子情報メディア工学専攻に所属する学生 3 名，並びに先進工学部情報メディア工学科に所属する学生 5 名の計 8 名を被験者とする実験を行った．

開発者役を被験者，顧客役を著者が行い，被験者は顧客役の求めるシステムの要件を参考にリスクを洗い出し，情報資産の特定とリスクの評価を行い，それぞれの情報資産毎に必要なセキュリティ要求の抽出を行った．

5.1 実験の流れ

実験の流れは以下の通りである．

a. 実験の概要･ツールの説明
b. 顧客が要求するシステムの説明
c. リスクの洗い出し
d. 情報資産の特定とリスクの評価
e. 各情報資産毎にセキュリティ要求の抽出
f. 選択した内容に誤りがないか確認する
g. 誤りがないと判断した場合，実験終了

6.実験結果と考察

本研究の実験結果と坂田[1]の予備調査及び実験結果における OWASP[2]の必須項目の充足率を図 4 に示す．

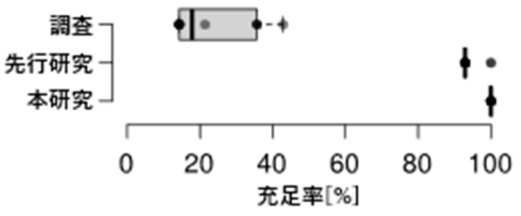

図 4.OWASP における必須項目の充足率

図 4 から実験結果では必須項目を多く満たし，

坂田[1]の実験結果を上回ることが分かる．

次に，本研究の実験結果と坂田[1]の実験結果における顧客の機能要件を満たす充足率を図 5 で示す．

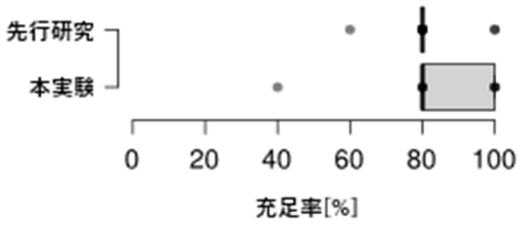

図 5.顧客の機能要件を満たす充足率

図 5 から顧客の機能要件を高い充足率で満たすことが確認できる．また，独立性を確認するため，t 検定を行った．検定結果は表 2 の通りである．

表 2.t 検定(分散が等しくないと仮定)結果

#		本研究
1	t	0.14
2	P(T<=t) 片側	0.45

検定の結果，独立性はないことが分かる．これについては，今回のツールの改良では要求抽出におけるインタビュー部分の支援を加えていないことが原因である．

次に本研究で洗い出されたリスクの種類とその数を図 6 に示す．

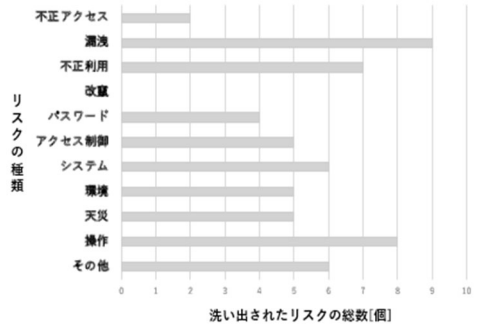

図 6.洗い出されたリスクの種類毎の総数

図 6 から幅広い種類のリスクを洗い出すことが出来たことがわかる．しかし，情報改竄が 0 であることからデータの完全性への危機意識が低いということを示している．

前述したことを基に，RQ について回答する．RQ1 について，寄与できると言える．RQ2 について，結果として坂田[1]の実験結果を下回らずかつ類似した結果を得ることが出来たため，悪影響はないと言える．RQ3 について，幅広いリスクを洗い出すことが出来ることを確認できた．

7.関連研究

本研究の関連研究として，事前に作成された要求仕様書からセキュリティ項目を作成する Riaz ら[5]の研究を挙げる．

表 3.本研究と関連研究の比較

#		対象	決定方法	リスク特定
1	本研究	顧客	選択肢	する
3	Riaz ら[5]	仕様書	機械学習	しない

8.まとめと今後の課題

実験結果から本研究のツールは OWASP[2]の必須項目を満たす要求仕様書作成に寄与できることが確認できた．また，坂田[1]のツールを改良したことによる悪影響が生じないことも確認できた．最後に，幅広いリスクの種類を把握することの補助が可能であることも確認できた．

今後の課題として，本研究では認証項目のみに焦点を当てたため，他のセキュリティ項目に関する質問，ヒント，選択肢を追加する必要がある．

謝辞

本研究を進めるにあたり，貴重な助言をいただいた橋浦 弘明准教授に感謝いたします．また，実験に協力してくださった日本工業大学の学生の皆さんに感謝いたします．

文　献

[1] 坂田 海，“インタビューによるセキュリティ要求抽出手法，”日本工業大学 卒業論文,2022-01.

[2] 上野 宣“OWASP Web Application Security Requirements，” <https://github.com/OWASP/www-chapter-japan/blob/master/secreq/OWASP_WebApplicationSecurityRequirements.pdf >(Accessed 2021/04/30).

[3] NIST，“NIST Special Publication 800-63-3，” <https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html>(accessed:2021/10/14).

[4] FIRST,”CommonVulnerabilityScoringSystem v3.0:Specification Document,” <https://www.first.org/cvss/v3.0/specification-document>, 2015-6-10, (accessed:2022-5-23).

[5] M. Riaz, J. King, J. Slankas and L. Williams, "Hidden in plain sight: Automatically identifying security requirements from natural language artifacts," Proc.of IEEE 22nd International Requirements Engineering Conference (RE 2014), pp. 183-192, Aug. 2014.