R-1

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　　118I121　坂田 海

1.はじめに

要求仕様書とは，システム依頼者からの要求を受けて開発側が実装する機能などを記述した文書である．この文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．

そこで，著者らは OWASP JAPAN の Web Application Security Requirements[1](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た．その結果を図 1 に示す．予備調査によって項目 1.4 のユーザのロックアウトや項目 1.5 のパスワードリセット等の認証に関する記載がない要求仕様書が存在することが明らかになった．

このような記載不備がスマホ決済の不正利用等の要因となる可能性がある．

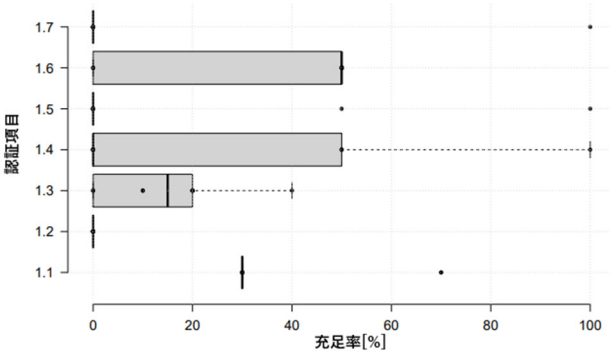


図 1.要求仕様書 10 個の認証項目充足率

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[1]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. 抽出内容が顧客の機能要件を満たすか
3. 要求に矛盾が生じていないか

3.提案手法

要求抽出では，主にインタビュー手法が用いられる．記載不備がある要求仕様書が生じる原因として，開発者の聞き漏らしが考えられる．セキュリティ要求は非機能要件であり，未実装でもシステムが動作するため，見落としが生じる可能性がある．問題が生じる箇所の例を図 2 に示す．

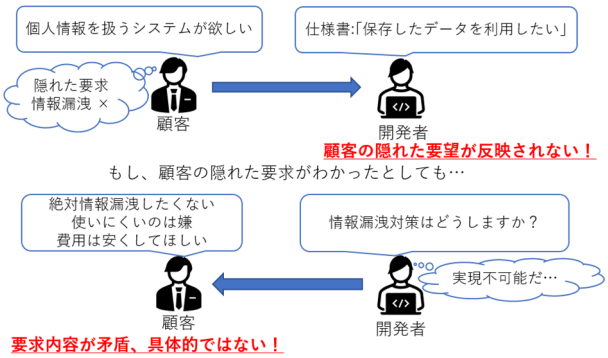


図 2.要求抽出において問題が生じる箇所の例

また，Haley ら[2]の提案手法では，保護対象の情報資産特定後，リスクを洗い出す作業がある．Riaz ら[3]の提案手法では,要求仕様書から機械学習を用いて対策するセキュリティ対策を作成する．しかし，先ほど述べた予備調査から記載内容の不備がある要求仕様書が存在する．

本研究では，このような問題を解消するために以下の手法を提案する．

1) 顧客への質問を事前に用意する
2) 質問に関する補足説明の導入
3) 質問の回答に選択肢を採用する

1) によって，開発者はツールに沿って質問をすることで聞き洩らしを防止することができる．2) によって，要求抽出に不慣れな開発者や顧客が質問内容を理解し，回答できるようにする．3) によって，開発者は顧客の回答に一番近い選択肢を選ぶだけで要求抽出ができる．

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．

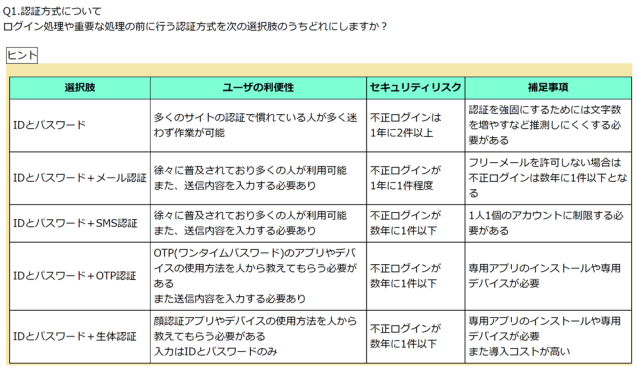
i. 質問機能
ii. 選択肢機能
iii. ヒント機能
iv. Authenticator Assurance Level

(以下 AAL とする)判定機能

v. 選択肢制限機能

vi. 矛盾検知機能

開発者は質問機能や選択肢機能を利用することで抽出すべき内容の聞き洩らしや欠落をすることなく抽出が可能になる．また，質問及び選択肢の内容は OWASP[1]の項目が基になっているため，これらを利用することで OWASP[1]を満たす要求仕様書の作成に寄与できる．次にヒント機能を利用することで開発者や顧客の知識を補いながら要求抽出ができる．図 3 に実装したツールの質問とヒントの例を示す．


Q1.認証方式について
ログイン処理や重要な処理の前に行う認証方式を次の選択肢のうちどれにしますか？

ヒント

選択肢	ユーザの利便性	セキュリティリスク	補足事項
IDとパスワード	多くのサイトの認証で慣れている人が多く迷わず作業が可能	不正ログインは1年に2件以上	認証を強固にするためには文字数を増やすなど推測しにくくする必要がある
IDとパスワード＋メール認証	徐々に普及されており多くの人が利用可能 また、送信内容を入力する必要あり	不正ログインが1年に1件程度	フリーメールを許可しない場合は不正ログインは数年に1件以下となる
IDとパスワード＋SMS認証	徐々に普及されており多くの人が利用可能 また、送信内容を入力する必要あり	不正ログインが数年に1件以下	1人1個のアカウントに制限する必要がある
IDとパスワード＋OTP認証	OTP(ワンタイムパスワード)のアプリやデバイスの使用方法を人から教えてもらう必要がある また送信内容を入力する必要あり	不正ログインが数年に1件以下	専用アプリのインストールや専用デバイスが必要
IDとパスワード＋生体認証	顔認証アプリやデバイスの使用方法を人から教えてもらう必要がある 入力はIDとパスワードのみ	不正ログインが数年に1件以下	専用アプリのインストールや専用デバイスが必要 また導入コストが高い

図 3.ツール内の質問とヒントの例

AAL 判定機能では，要求されたシステムのセキュリティリスクと対策内容を結びつけるために実装する．ツールには NIST SP800-63-3[3]に記載されている 6 個の質問からセキュリティ強度のレベルを 3 段階に分類する．この結果によって，不適切な選択肢を制限する機能を実装した．

矛盾検知機能では，不適切な組み合わせが選ばれている際に機能する．例えば，通常の認証では ID とパスワードのみ，パスワード変更では二段階認証の設定がされている場合，赤文字の警告文が表示される．

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 9 名の計 12 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，被験者は顧客役の回答を参考に AAL 判定に関する 6 問，セキュリティ要求に関する 9 問の全 15 問に答えた．

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. AAL の判定

d. セキュリティ要求の抽出

e. 選択した内容に誤りがないか確認する

f. 誤りがないと判断した場合，実験終了

手順 b の説明前に顧客が要求するシステムについて記載された用紙を配布する．この用紙は実験終了時まで見ることができる．手順 c，d では，開発者役は顧客役の回答とツールのヒントを参考に抽出作業を行い，選択肢の中で一番適切だと思う選択肢を選択することで AAL の判定，セキュリティ要求の抽出を行う．手順 e では，手順 d で選択した内容が一覧表示される．被験者は選択した内容に間違いがないか再確認をする．問題がなければ本実験を終了する．

6.実験結果と考察

実験結果と予備調査の OWASP の必須項目の充足率を図 4 に示す．

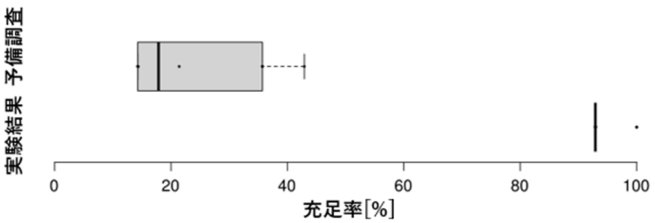


図 4.OWASP における必須項目の充足率

図 4 から実験結果では OWASP における必須項目を多く満たすことがわかる．

また，上記の実験結果の独立性を確認するため，分散が等しくないと仮定した 2 標本による t 検定を行った．検定結果は表 1 の通りである．

表 1.t 検定(分散が等しくないと仮定)結果

#		本研究
1	t	18.3
2	P(T<=t) 片側	2.51×10^{-9}

本検定では，帰無仮説H_0を「予備調査とツールの実験結果に母平均の差はない」，対立仮説H_1を「予備調査とツールの実験結果に母平均の差はある」，有意水準αを 0.05 とした．表 1 からH_0を棄却しH_1を採択する．よって，上記の結果から本研究のツールによって OWASP[1]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ことが確認できた.

次に，本実験で選ばれた選択肢によって，顧客の機能要件を満たす充足率を図 5 で示す.

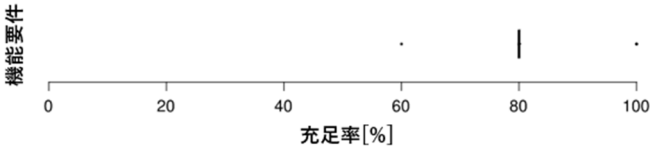


図 5.顧客の機能要件を満たす充足率

図 5 からツールによって，顧客の機能要件を高い充足率で満たすことが確認でき，80%に集中していることがわかる．これは顧客役が一部の要求抽出作業において，利便性に関する要望を意図的に伝えなかったことが原因である.

一方で，顧客の機能要件を 100%満たす被験者が存在する．この被験者は，顧客役が伝え忘れた利便性に関する要望を抽出する質問を自力で補い，顧客役の要望を聞き出すことができたため，充足率が 100%となった．また，60%になった被験者は，顧客役の要望を抽出できたが，顧客の要望より自身の価値観を優先したことで顧客の機能要件を満たす充足率が低くなった.

前述したことを基に，RQ について回答する．RQ1 について，実験結果から本研究のツールは OWASP[1]の必須項目を満たす要求仕様書の作成に寄与できることを確認した．RQ2 について，実験結果から顧客の機能要件を高い充足率で満たす要求仕様書作成に寄与できることが確認できた．RQ3 について，選択肢制限機能と矛盾検知機能によって，選ばれた選択肢に矛盾が生じないことが実験結果から確認できた．以上 3 点から本研究のツールは，認証対策が明記された要求仕様書の作成に寄与できる.

7.関連研究

本研究の関連研究として，セキュリティ要求の抽出，分析に関するフレームワークを提案した Haley ら[2]の研究，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[3]の研究を挙げる．上記 2 つの研究と本研究の比較は表 2 の通りである.

Haley ら[2]の研究では，要求の決定方法は顧客と開発者の話し合いによって決定する．しかし，本研究の手法では，選択肢による決定を採用している．これによって，要求抽出に不慣れな開発者であっても要求抽出ができる.

Riaz ら[3]の研究では，要求抽出をする対象は要求仕様書である．しかし，本研究の手法では，要求抽出の対象は顧客としている．これは，予備調査で要求仕様書の記載不備が確認できたため，記載不備のある要求仕様書から作成された内容は，顧客が要望する内容と異なる可能性がある.

表 2.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	しない
2	Charles ら[2]	顧客	話し合い	する
3	Riaz ら[3]	仕様書	機械学習	しない

8.まとめと今後の課題

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った．実験結果から本研究のツールは OWASP[1]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，顧客の機能要件を高い充足率で満たすことも確認できた．最後に，選ばれた選択肢に矛盾が生じていないことも確認できた.

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] 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).

[2] Charles B. Haley, Jonathan D. Moffett, Robin Laney, Bashar Nuseibeh,“A framework for securety requirements engineering,” Proceedings of the 2006 international workshop on Software engineering for secure systems(SESS’06),pp.35‐42, May 2006.

[3] 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.

[4] 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).