NFR フレームワークを用いたセキュリティに関する要求定義支援ツールの提案

櫛部 健汰　伊藤 恵

本研究はセキュリティ知識が不足している開発者に対してセキュリティに関する要求定義を支援するツールを提案する．要求定義ではステークホルダのニーズを的確に把握し，下流工程に向けてどのようなシステムを構築するのかを明確にする必要がある．特にセキュリティに関する要求は工程の手戻りなどを防ぐために，適切に定義されなければならない．要求を定義・分析する手法の一つとして NFR フレームワークという手法がある．この手法は，非機能要求に焦点を当てたゴール指向要求定義法である．しかし，この手法はセキュリティ知識が十分でない場合，適切な要求定義を行うのは難しい．本研究では，開発者がセキュリティ要求定義を行う際の NFR フレームワークに着目し，ゴール分解する際に自然言語処理とルールベースを用いてゴール分解を支援する拡張 NFR フレームワークを考案し，それを用いて要求定義を支援することを目指す．

This research proposes a tool to support security requirements definition for developers who lack security knowledge. In the requirements definition, it is necessary to accurately understand the needs of stakeholders and to clarify what kind of system to construct for the downstream process. In particular, security requirements must be properly defined in order to prevent reworking of the process.The NFR framework, which is one of the methods for defining and analyzing requirements, is a goal-oriented requirements definition method focusing on non-functional requirements. Focusing on the NFR framework in defining security requirements, devising an extended NFR framework that supports goal decomposition using natural language processing and rule-based approach. By the framework ,we aim to support security requirements definition.

1　はじめに

近年，スマートフォンの普及や IoT システムの流行などによって個人から企業まで情報サービスが普及し暮らしが便利になっている．情報サービスの普及に伴い，効率よく情報サービスに関するシステムを開発するためにシステム開発工程が重要とされている．システム開発工程の一つである要求定義では，顧客の要求を適切に理解し，後工程にシステムの最終開発物を定義する重要な工程である．[7] 要求定義が不十分であると，後工程のシステム開発に重大な影響を及ぼすことは多い．要求定義がうまくいかない理由の一つとして，顧客側の要望を開発側が具体化する際に生じるギャップがある．顧客側の早く，安く，いいものを使いたいと言った要望に対して，開発側は具体的な IT 技術や開発者側の開発規模などから折り合いをつけて最終的な要求定義を行う．開発側が顧客側の要望に対して折り合いをつけた際にギャップが生じてしまう．

特にセキュリティに関する要求 (以下セキュリティ要求) はシステムの機能とは関係ない要求，非機能要求として扱われ，要求定義においてはギャップが生じやすい．セキュリティ要求を要求定義時点から定義することで，早期に脅威を意識した開発ができたり，後工程からの手戻りのリスクを軽減することができる [4]．セキュリティ要求定義は，常日頃から増える脅威や新しく増える要求などに適切に対処する必要があるので通常の機能要求に関する要求定義よりも複雑に

A Proposal of Security Requirements Definition Support Tool Using NFR Framework

Kenta Kushinobe, 公立はこだて未来大学　システム情報学部　情報アーキテクチャ学科, School of Systems Information Science, Future University Hakodate.

Kei Ito, 公立はこだて未来大学, Future University Hakodate.

なってしまうことが多い．しかし複雑であるにも関わらず，システム開発を行う際に，顧客側はセキュリティに関する漠然とした要求はあるもののセキュリティの知識が乏しいので開発側にセキュリティに関する要求を任せるというのが一般的である．しかし，開発側もセキュリティの専門家ではないことが多い．

経済産業省の調査[5]によると2016年時点でセキュリティに関する人材が13.2万人不足となっており，2020年には不足数が19.3万人に増加すると見込まれている．この傾向は中小企業では特に深刻である．開発側がセキュリティの知識が不足していると，セキュリティ関係の用語の理解不足などから適切なセキュリティ要求定義を行うことは難しいといえる．セキュリティ要求定義が適切にできずに顧客とのギャップを生じさせてしまうと，脅威に対応できていなかったり，システムの脆弱性に気づかずに後々に莫大なコストがかかってしまうなどの問題が考えられる．そのような問題を発生させないためにも，セキュリティ要求定義は適切に行われるべきである．

セキュリティ要求定義を明示的に表現する枠組みとして，NFRフレームワークが挙げられる．NFRフレームワークは非機能要求を組織的に表現するゴール指向要求定義手法[2]である．そこで本研究では，セキュリティ知識が不足している開発者がセキュリティ要求定義をNFRフレームワークを用いて行う際にルールベースと自然言語処理を用いてゴール分解を支援する．それにより要求定義を支援する手法を提案する．

本稿では2章でセキュリティ要求に関する研究について述べる．3章では本研究で用いたNFRフレームワークについて述べる．4章では本研究で開発する要求定義支援ツールについて述べる．5章ではツール開発の前に行なった事前調査について述べる．6章では本稿のまとめと今後の展望について述べる．

2 関連研究

関連研究としてセキュリティ要求に関する研究やNFRフレームワークをシステム連携に用いた研究がある．

2.1 セキュリティ要求策定の研究

大久保らの研究[6]ではソフトウェア開発プロジェクトが以下のような2つのグループで構成されることを前提としたセキュリティ要求分析手法（AORSE）を提案した．

(A) ソフトウェア開発において想定される脅威，およびその対策について十分な知識を有するが開発対象のドメイン知識は不十分な者

(B) 開発対象のドメイン知識は十分であるがセキュリティ知識は不十分な可能性がある者

AORSEではセキュリティ知識，ドメイン知識が上記(A),(B)のように分かれていることを前提としセキュリティ要求分析・策定作業をそれぞれの知識において明確化できるように責任範囲を明確化する．最初に(B)の知識を用いてソフトウェアの機能の定義を行なう．次に機能のデータでセキュリティ保護が必要であるというデータを「保護資産」として抽出する．どのデータが保護資産なのかを判断するためには(A)の知識を必要とする．次に対象となるソフトウェアに対する脅威を(A)，(B)の双方の知識を用いて抽出する．最後に抽出された脅威に対して想定される対策案を(A)の知識を用いて考案する．

それらのような要求分析作業を終了した後に，設計仕様を考案する．このようにセキュリティ知識を要する作業を分離することで，少数のセキュリティ有識者が全ての要求策定作業に参加せずに済み，効率的な作業を実現できる．この研究はセキュリティ有識者がいることを前提として提案しているが，セキュリティ知識が不足している開発者を支援するという面では本研究の目指す形と一致している．

2.2 システム連携におけるNFRフレームワークのNFR型カタログの提案

矢嶋らの研究[9]ではNFRフレームワークと組み合わせて用いるシステム連携に特化したNFR型カタログを定義して要求定義工程の問題解決方法を提案した．NFRフレームワークはNFR型カタログという階層構造を用いてゴール分解を行う．NFR型カタログとは主にシステム要求の分析において分析者を支援するために性能やセキュリティといった一般的

な非機能要求の型をあらかじめ型としてパターン化したものである [8]．パターン化することでゴール分解を容易にすることができる．図 1 にそのカタログの例を示す．例をとると，時間という NFR 型にはスループットとレスポンスタイムなどが構成要素としてある．このように非機能要求に関する基本的構造をゴール階層を用いて記述することができる．しかし，このカタログのままではシステム連携を行う際に差異が生じてしまう．そこで矢嶋らは発展性や柔軟性といったシステム連携に必要な特性を NFR 型カタログに組み込んだ．システム連携に必要な特性を NFR 型カタログに組み込んで拡張することで，システム連携先の機能要求と非機能要求の関係を表現し，連携する機能要求の関連性や制約条件を明らかにすることを目指した．

本研究は，セキュリティ要求定義を行う際に NFR フレームワークを用いて支援することを目的としており，システム連携であるという面をセキュリティ分野に変更すれば本研究と方向性は一致している．NFR フレームワークの本研究での使用方法に関しては第 3 章にて述べる．

3 NFR フレームワーク

本節では NFR フレームワークについて述べる．図 2 が NFR フレームワークの全体図である．

3.1 NFR フレームワーク

ソフトウェア要求を定義する方法は様々なものが提案されている．ゴール指向分析もソフトウェア要求を定義する手法の 1 つである．ゴールを用いて要求の抽出，分解化，分析などを行うことでシステムが達成すべき目的を達成できると報告されている．[1] NFR フレームワークはトロント大学の Lawrence Chung らによって考案された [2] ゴール指向分析の 1 種である．満足化するべき非機能要求をいくつものソフトゴールごとに分解することによってソフトゴールツリー（以下，SIG 図）を作成し，SIG 図に操作ソフトゴールを対応づけることによって対象システムの機能を明らかにする．表 1 が NFR フレームワークで用いる構成要素である．

表 1　NFR フレームワークの構成要素

No.	ソフトゴールの名称	図形
1	非機能（NFR）ソフトゴール	
2	操作ソフトゴール	
3	理由ソフトゴール	

主に 3 種類のソフトゴールを用いて SIG 図を記述する．ゴール分解などで主に用いられるのが，表 1 の No.1 の NFR ソフトゴールである．NFR ソフトゴールは満足化の対象となる非機能要求を表現する．NFR ソフトゴールに対して AND 分解と OR 分解という 2 種類のゴール分解を繰り返しながら最終的に操作ソフトゴールを求める．表 1 の No.2 の操作ソフトゴールである．操作ソフトゴールは上位のゴールを満足化するために必要な技術を表現する．操作ソフトゴールを定義する際には意思決定や相互依存関係を明確にするために表 1 の No.3 の理由ソフトゴールを記述する．表 1 らの構成要素を用いた SIG 図が図 2 である．AND 分解は図 2 の一番上の分解である．システムにはネットワークとサーバというもの両方が必要である，つまりどれもが欠けてはならないという分解である AND 分解を行なった．AND 分解を行う際に SIG 図には分解した枝をまとめるように線を引く．その線で，AND 分解を行なっていることを示す．それ以外の図 2 の分解は OR 分解である．OR 分解は複数の要素があった場合にどれかが達成できればいいという分解である．SIG 図には AND 分解とは異なり，枝をまとめる線は引かない．操作ソフトゴールと NFR ソフトゴールを記述する際には，NFR 型と話題名の 2 つを記述する．図 2 の一番上位の NFR ソフトゴール (セキュリティ [システム]) を例に挙げると，セキュリティが NFR 型でシステムが話題名である．NFR 型とは非機能要求の種類を指す．具体例としては安全性，可用性などが挙げられる．話題名とは，その非機能要求が満たされる対象である．具体例としては，営業情報システム，ATM システムのよ

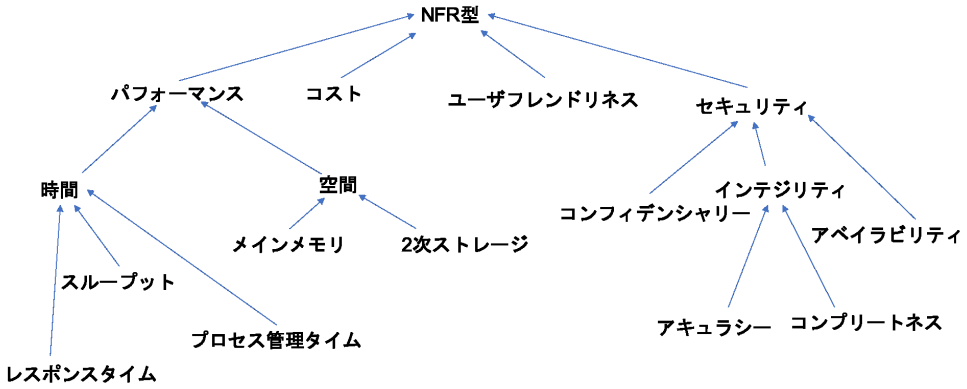

図 1　NFR 型カタログ

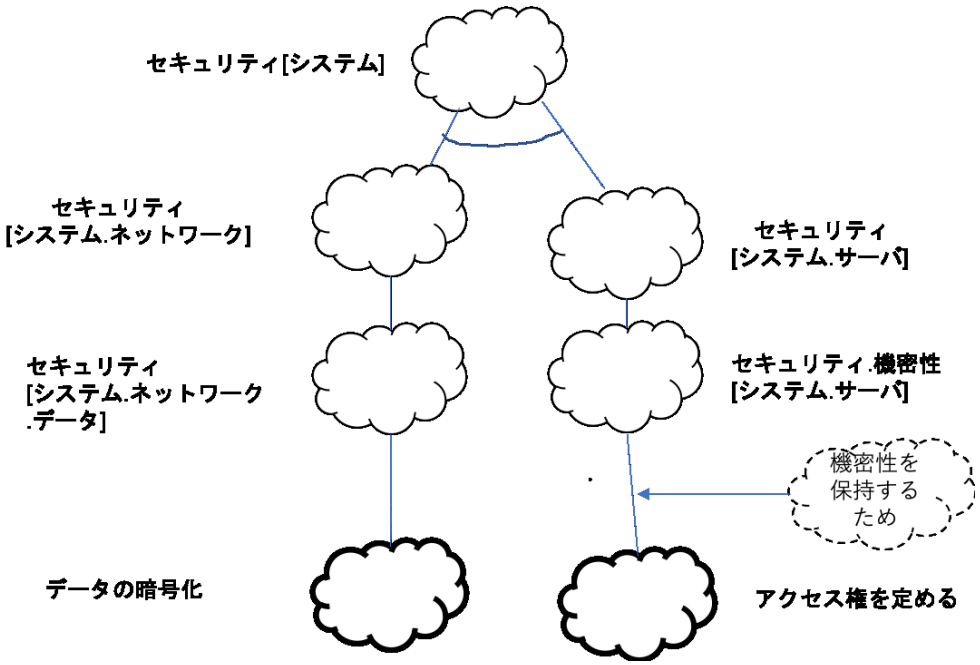

図 2　NFR フレームワークの SIG 図の一例

うな具体的な開発物を指す．ゴール分解する際には，NFR 型に基づいて分解する方法（以下，NFR 型分解），話題の構造化による分解（以下，話題分解）の 2 つの分解方法がある．NFR 型分解に関しては一般的な非機能要求の階層構造を NFR 型カタログとして定義しておくことができる．これらの 2 つの分解方法を使用して最終的な操作ソフトゴールを定義する．NFR フレームワークを用いて非機能要求を分析・定義することで機能要求との整合性を保つ効果や，他の非機能要求との衝突を回避する効果が期待できる．

3.2 セキュリティ要求における NFR フレームワーク

セキュリティ要求は非機能要求に含まれる．セキュリティ要求を NFR フレームワークを用いて求める際には脅威を念頭に置きながらセキュリティ要求を定義することとなる．脅威とはシステムに損害や影響を発生させる可能性のことである．情報セキュリティにおいて脅威は人為的脅威と環境的脅威の 2 つに分けることができる．人為的脅威とは人間によって引き起こされる脅威のことである．人為的脅威は意図的脅威と偶発的脅威に分けることができる．意図的脅威は主に悪意のもった者によってもたらされる脅威である．システムに対して攻撃を行ったり，システムを故意的に破壊することなどが当てはまる．偶発的脅威とは人為的なミスによってもたらされる脅威である．悪意がないのにネットワークエラーが引き起こってしまったり，パスワードを誤って紛失してしまった行為などが当てはまる．人為的脅威ではない脅威は環境的脅威である．災害によって，データセンターが被災してしまったりという人間の力ではどうすることもできない脅威のことを指す．

NFR フレームワークはこれらの脅威をもとにゴール分解を行うことで，脅威が引き起こされる原因を明確にする．しかし，NFR フレームワークにおいてセキュリティ要求を定義する際にはどのような場面でどのような脅威が考えられるのかというセキュリティ知識が必要となる．脅威がわからなければ，ゴール分解を行うことも難しい．したがって，セキュリティ知識が不足していれば NFR フレームワークを用いてセキュリティ要求定義を行うことが難しい．セキュリティ知識が少ない開発でも NFR フレームワークを用いてセキュリティ要求定義を適切に行えるようにするのが本研究で考案するツールである．

4 本研究で考案するツール

本研究では拡張 NFR フレームワークという要求定義支援ツールを用いて，セキュリティ知識が少ない開発者のセキュリティ要求定義を支援することを目的としている．図 3 に本ツールの全体図を示す．ツールの概要としては，拡張 NFR フレームワークは NFR ソフトゴールの話題名と NFR 型に着目し，それらを用いてゴール分解する時にルールベースと自然言語処理を用いてゴール分解を支援することで開発者の支援を行い，適切なセキュリティ要求定義を行うことを目指す．

4.1 NFR 型を用いてゴール分解を行う際の支援手法

NFR フレームワークでゴール分解を行う際には先述のように NFR 型分解と話題分解の 2 つの分解方法があげられる．NFR 型分解を行う場合には，システムに必要なセキュリティ要素を理解している必要がある．しかし，セキュリティ知識が不足していると必要なセキュリティ要素が出せない．NFR 型分解には 3.3 節で述べたように NFR 型カタログというものが存在する．NFR 型カタログのセキュリティに関する部分は情報セキュリティの 3 要素である機密性，完全性，可用性があげられる．しかし昨今のセキュリティに対する情勢から，これらの 3 要素では足りないと考えた．そこで ISO/IEC 27001:2005 で新たに追加された要素である真正性，責任追及性，否認防止，信頼性らの 4 つの要素を追加したセキュリティ拡張 NFR 型カタログを提案する．セキュリティ拡張 NFR 型カタログをもとに NFR 型分解を行うが，NFR 型カタログのみでは分解の支援ができるとは言えない．セキュリティ知識が不足している開発者はこのカタログを使う際に用語が理解できずに使用してしまう可能性がある．そこでセキュリティ拡張 NFR 型カタログをもとにルールベースを用いてゴール分解を支援する手法を提案する，例えば機密性というセキュリティに関する NFR 型があったとしたら機密性を保つために，アクセス権の明確化が必要であることや，個人情報の漏洩を防ぐなどの具体的解決策を提案することを目指す．このようなゴール分解支援を行うことでセキュリティ知識がない人でもセキュリティ要求定義を行えるように目指す．

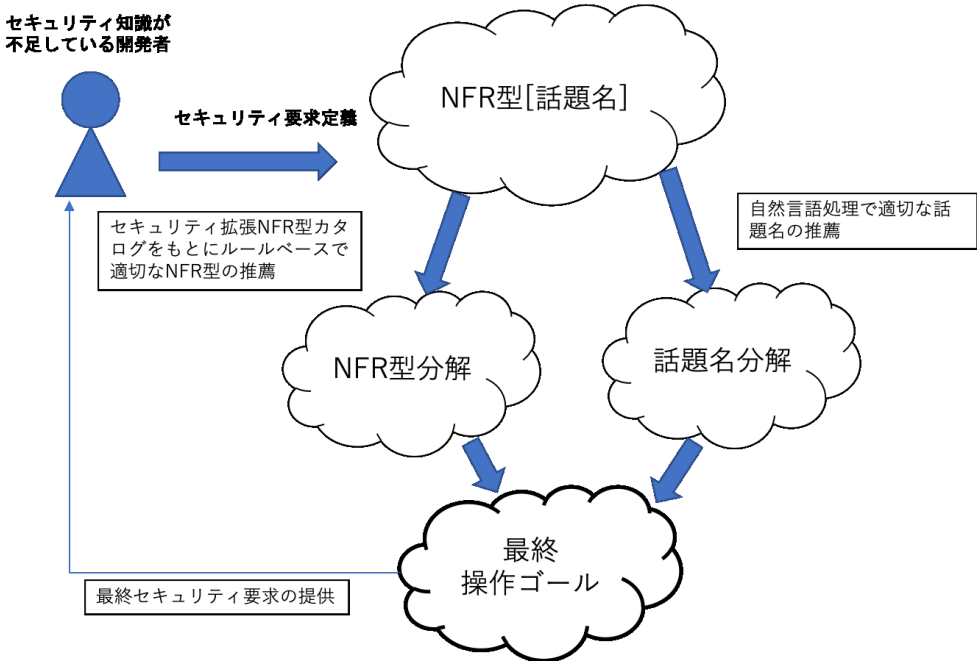

図 3　提案ツール

4.2　話題名を用いてゴール分解を行う際の支援手法

NFR フレームワークは話題名を用いてゴール分解を行う．しかし，セキュリティ知識が少ない開発者の場合，話題名を用いて分解する際に適切な用語を用いることが難しい．例えば，営業情報システムという話題名でゴール分解を行う際には，営業情報システムのネットワークに関連するセキュリティを考えるのかという問題や，営業情報システムのファイアーウォールを考えなければならないなどの問題など，次にどのようなセキュリティ面での用語でゴール分解すればいいのか判断するのが難しい．そこで自然言語処理を用いてシステムに関連する用語を推薦する手法を提案する．具体的には営業情報システムという話題名があったならば，「営業」「情報」「システム」に分けて単語を識別し，「営業」ならば「顧客」や「商談」のように単語に必要なキーワードを抽出することを目指す．

5　調査

要求定義支援ツールの開発に向けて「開発者が違う場合のセキュリティ要求の違い」,「セキュリティ知識が不足している場合に満足なセキュリティ要求を定義できない」などの背景と目的を明確化するために事前調査を行なった．調査は最初にセキュリティ知識を測るような問題を解いてセキュリティ知識のレベルを判断し，その後に用意した要求定義シナリオを読んでセキュリティ要求を抽出してもらうというように行なった．

5.1　調査協力者

調査の協力者は公立はこだて未来大学システム情報科学部学部生 30 名及び同学科を卒業し，同大学院に所属している大学院生 1 名の合計 31 名であった．

5.2　調査方法

大きく分けてセキュリティ試験とセキュリティ要求書き出しの 2 つの調査を行なった．

5.2.1　セキュリティ試験

最初に，協力者のセキュリティの知識を測るためにセキュリティ試験を行なった．4 択式の問題を全 10 問用意し解答させた．セキュリティ試験の問題は，IPA が行なっている IT パスポート，基本情報技術者試験，応用情報技術者試験の問題のセキュリティ分野の問題から抜粋した．テスト問題の難易度は基本情報技術者試験の問題が 4 問，IT パスポートの問題が 3 問，応用情報技術者試験の問題が 3 問という構成にした．このセキュリティ試験を行うことで協力者のセキュリティ知識に対する理解度を確かめ，のちに行われるセキュティ要求書き出しの際にセキュリティ知識の理解度とセキュリティ要求の的確さの関係を調べる．使用した試験問題は付録 A に載せる．

5.2.2　セキュリティ要求書き出し

セキュリティ試験を行なった後に，セキュリティ要求シナリオ（以下，シナリオ）を読んでもらいシナリオのセキュリティ要求を抽出してもらった．協力者には自分が開発会社の担当者になったつもりで考えられる脅威と，その脅威をなくすためのセキュリティ要求を書き出してもらった．制限時間は上限は設けなかったが，最低でも 20 分は書き出してもらった．セキュリティ要求を書き出すためのコツとしてシナリオはセキュリティ関係の部分をかなり甘く設定しているので，それらの脆弱性をつくようなイメージで書き出すと良いという指示を出した．シナリオは付録 B に載せる．

5.3　調査結果

調査結果として以下のようなデータが得られた．

5.3.1　セキュリティ試験

図 4 がテストの点数一覧である．横がテストの点数，縦が人数を表している． テストの平均点は 4.7 点であった．協力者のセキュリティ知識を測るためにこの試験を行なった．最低点が 2 点，最高点が 8 点と協力者のセキュリティ知識にばらつきがある結果となった．

5.3.2　セキュリティ要求書き出し

セキュリティ要求の書き出しは IPA が提供している非機能要求グレード 2018 [3] をもとに評価を行なった．非機能要求グレードとは非機能要求についてのユーザと開発者との認識の行き違いや, 互いの意図とは異なる理解を防止することを目的とし, 非機能要求項目を網羅的にリストアップして分類するとともに, それぞれの要求レベルを段階的に示したものである. 重要な項目から順に要求レベルを設定しながら, 両者で非機能要求の確認を行うことができる．事前調査では，非機能要求グレードの大項目の一つであるセキュリティをもとに評価を行なった．セキュリティに関する今回使用した中項目には以下のようなものがある．

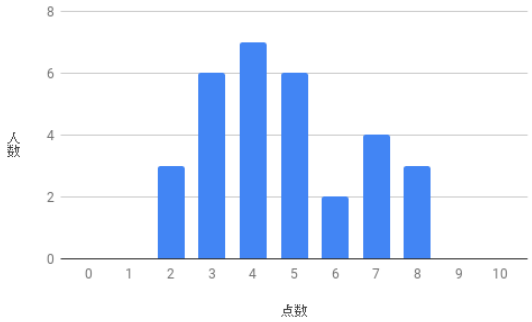

図 4　セキュリティ試験の点数分布

- セキュリティリスク管理
  システム運用後に発見された脅威や脆弱性にどう対応するかについて
- アクセス・利用制限
  開発する情報システムで取り扱う資産に対するアクセスおよび利用の制限について
- データの秘匿
  開発するシステムについて流通および蓄積する情報の秘匿について
- 不正追跡・監視
  システム運用後に発生する不正行為の追跡および監視について
- ネットワーク対策
  ネットワークのセキュリティ対策について，不正な通信を遮断するための制御やシステム内の不正行為や通信を検知する仕組みの導入などがある
- マルウェア対策
  コンピュータウイルス，ワーム等のマルウェアの

セキュリティ対策について

- web 対策
  Web アプリケーションの脆弱性へのセキュリティ対策について
- セキュリティインシデント対応/復旧
  セキュリティインシデントが発生することを前提とした対策について

セキュリティ要求書き出しは単純に書き出した要求の数と書き出された要求のうち非機能要求グレードのセキュリティ分野に当てはまるものというものの 2 つに分けた．図 5 が書き出されたセキュリティ要求の数であり，図 6 が非機能要求グレードに当てはまったセキュリティ要求の数である．両図ともに横は要求の数，縦は人数を表している．非機能要求グレードに当てはまるセキュリティ要求の具体例として「個人情報の保護のためにネットワーク通信の保護が必要である」という要求がある．この要求は非機能要求グレードのネットワーク対策に当てはまるような要求である．逆に非機能要求グレードに当てはまらない要求としては「B 社側にあるサーバは A 社に置くべきである」という要求である．この要求はセキュリティの観点から正しい要求ではあるが，セキュリティ面の具体的な用語を用いて記述を行なっていないので非機能要求グレードの要求には当てはまらない要求として数える．このように，具体的な記述がないようなセキュリティ要求は非機能要求グレードの要求として数えていない．

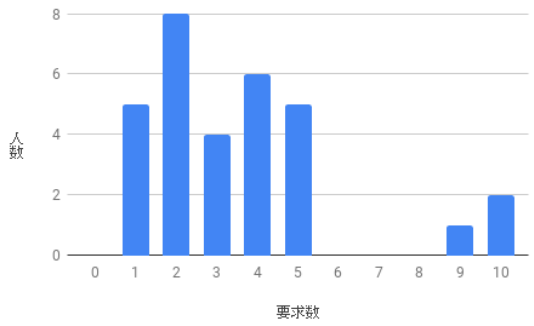

図 5　セキュリティ要求書き出しの総数

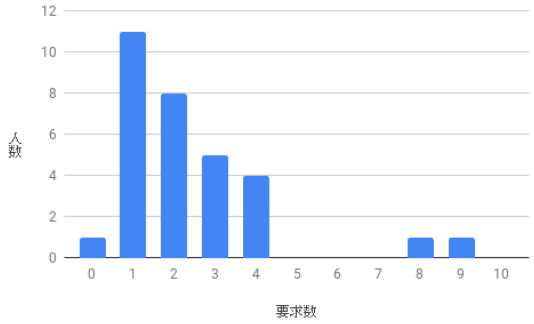

図 6　非機能要求グレードに基づいたセキュリティ要求の数

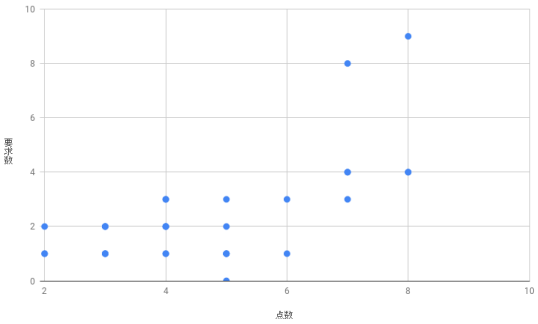

図 7　非機能要求グレードに基づいたセキュリティ要求の数とセキュリティ試験との分布図

単純なセキュリティ要求の書き出しの平均書き出し数は 3.3，非機能要求グレードに基づいたセキュリティ要求書き出し数の平均は 2.0 であった．

5.3.3　セキュリティ試験とセキュリティ要求書き出しの因果関係

セキュリティ試験の点数と非機能要求グレードに基づいたセキュリティ要求の数を分布図として表したものが図 7 である．横がセキュリティ試験の点数，縦が非機能要求グレードにもとづいたセキュリティ要求書き出しの数である．

図 7 を見ると正の相関関係が見られる．これは，セキュリティ知識とセキュリティ要求を書き出すのは正の相関関係があると考えられる．

5.4 考察

今回の事前調査よりセキュリティ知識が不足している開発者は満足なセキュリティ要求定義を行うことが困難であるということがわかった．また，同じセキュリティ要求でも，セキュリティ知識によって具体性が違うこともわかった．具体例として協力者 A と協力者 B のセキュリティ試験とセキュリティ要求書き出しを例にあげる．協力者 A はセキュリティ試験が 3 点であり，協力者 B はセキュリティ試験の点数が 8 点であった．両者とも脅威として個人情報が流出してしまうという問題があると書いた．しかし，セキュリティ要求に違いがあった．協力者 A はセキュリティーの強化という記述のみであったが，協力者 B はサーバを B 社に置いていると B 社内で悪意のある人がいると情報が盗まれてしまうということがあるので，信頼できる第三者企業にサーバをおく，もしくは自社でサーバをおく必要があるというように記述していた．このようにセキュリティ試験の点数に応じてセキュリティ要求の具体性が違っている例が多数あった．具体性の違いとして考えられたのが，セキュリティに関する用語を使用しているかという違いもあった．辞書攻撃を防ぐような強固なパスワードを設定させるのようなセキュリティ要求も上げられていた．そこで，セキュリティに関する用語を推薦できるようにツールの開発を行うとセキュリティ要求定義支援できると考えた．今後のツール開発で事前調査で得た知識をもとに開発を行う．

6 おわりに

本研究ではセキュリティ知識が不足している開発者でもセキュリティ要求定義の支援ができるように，ルールベースと自然言語処理を用いた拡張 NFR フレームワークの開発を目指している．そのため，本稿ではその開発に向けた事前調査の結果及び提案するツールについて論じた．調査結果として，セキュリティ知識とセキュリティ要求定義には関係があることがわかった．今回の調査でわかったことをもとに，今後ツールの開発・評価を行なっていく．

参 考 文 献

[1] A.Lamsweerde: Goal-Oriented Requirements Engineering: A Guided Tour, *Proceeedings RE' 01*, pp. 249–263, 2001.

[2] J.Mylopoulos, L.Chung, B.: Representing and Using Non-Functional Requirements: A Process-Oriented Approach, *IEEE Transactions on Software Engineering*, Vol. 18, No. 6, pp. 483–497, 1992.

[3] 独立行政法人情報処理推進機構 技術本部ソフトウェア高信頼化センター: 非機能要求グレード 2018, https://www.ipa.go.jp/sec/ softwareengineering/reports/20100416.html, 最終アクセス 2019/8/4.

[4] Bashar Nuseibeh, 吉岡信和: セキュリティ要求工学の実効性:1. セキュリティ要求工学の概要と展望, 情報処理, Vol. 50, No. 3, pp. 187–192, 2009.

[5] 商務情報政策局 情報処理振興課: IT 人材の最新動向と将来推計に関する調査結果 報告書概要版〜, Technical report, 経済産業省, 2016.

[6] 大久保隆夫，田中英彦: 効率的なセキュリティ要求分析手法の提案, 情報処理学会論文誌, Vol. 50, No. 10, pp. 2484–2499, 2009.

[7] 岡崎義勝, 大森久美子: ずっと受けたかった要求分析の基礎研修, 翔泳社, 2011.

[8] 山本修一郎: 〜ゴール指向による！！〜システム要求管理技法, 株式会社ソフト・リサーチ・センター, 2007.

[9] 矢嶋健一，落水浩一郎: NFR フレームワークにおけるシステム連携向け拡張 NFR 型カタログの提案, ソフトウェア工学の基礎 *XVI*, pp. 289–296, 2009.

A　付録：セキュリティ試験問題

問 1 生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか
ア　本人のディジタル証明書を信頼できる第三者機関に発行してもらう
イ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する
ウ　マルウェア定義ファイルの更新が頻繁な製品を利用することによって，本人を誤って拒否する確率の低下を防ぐ．
エ　容易に推測できないような知識量と本人が覚えられる知識量とのバランスが，認証に必要な知識量の設定として重要となる．

問 2 CAPTCHA の目的はどれか
ア　Web サイトなどにおいて，コンピュータではなく人間がアクセスしていることを確認する。
イ　公開鍵暗号と共通鍵暗号を組み合わせて，メッセージを効率よく暗号化する。
ウ　通信回線を流れるパケットをキャプチャして，パケットの内容の表示や解析，集計を行う。
エ　電子政府推奨暗号の安全性を評価し，暗号技術の適切な実装法，運用法を調査，検討する。

問 3 リスク共有 (リスク移転) に該当するものはどれか
ア　損失の発生率を低下させること
イ　保険への加入などで，他者との間でリスクを分散すること
ウ　リスクの原因を除去すること
エ　リスクを扱いやすい単位に分解するか集約すること

問 4 コンピュータやネットワークのセキュリティ上の脆弱性を発見するために，システムを実際に攻撃して侵入を試みる手法はどれか
ア　ウォークスルー
イ　ソフトウェアインスペクション
ウ　ペネトレーションテスト
エ　リグレッションテスト

問 5 Web サーバの認証において，同じ利用者 ID に対してパスワードの誤りがあらかじめ定められた回数連続して発生した場合に，その利用者 ID を自動的に一定期間利用停止にするセキュリティ対策を行った。この対策によって，最も防御の効果が期待できる攻撃はどれか
ア　ゼロデイ攻撃
イ　パスワードリスト攻撃
ウ　バッファオーバフロー攻撃
エ　ブルートフォース攻撃

問 6 無線 LAN において，あらかじめアクセスポイントへ登録された機器だけに接続を許可するセキュリティ対策はどれか
ア　ANY 接続拒否
イ　ESSID のステルス化
ウ　MAC アドレスフィルタリング
エ　WPA2

問 7 PDCA モデルに基づいて ISMS を運用している組織において，始業時の手順に従って業務用 PC に適用されていないセキュリティパッチの有無を確認し，必要なパッチを適用している。この活動は PDCA サイクルのうちどれに該当するか
ア　P
イ　D
ウ　C
エ　A

問 8 公開鍵暗号方式を用いて送信者が文書にディジタル署名を行う場合，文書が間違いなく送信者のものであることを受信者が確認できるものはどれか

ア　送信者は自分の公開鍵を使用して署名処理を行い，受信者は自分の秘密鍵を使用して検証処理を行う。

イ　送信者は自分の秘密鍵を使用して署名処理を行い，受信者は送信者の公開鍵を使用して検証処理を行う。

ウ　送信者は受信者の公開鍵を使用して署名処理を行い，受信者は自分の秘密鍵を使用して検証処理を行う。

エ　送信者は受信者の秘密鍵を使用して署名処理を行い，受信者は自分の公開鍵を使用して検証処理を行う。

問 9 HTTPS を用いて実現できるものはどれか

ア　Web サーバ上のファイルの改ざん検知

イ　クライアント上のウイルス検査

ウ　クライアントに対する侵入検知

エ　電子証明書によるサーバ認証

問 10 緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は，どれに分類されるか

ア　ソーシャルエンジニアリング

イ　トロイの木馬

ウ　パスワードクラック

エ　踏み台攻撃

B　付録：セキュリティ要求シナリオ

B.1　登場会社

- A 社
  売上高 10 億円，従業員数 50 名の製造業会社
- B 社
  システム開発業者

B.2　背景

社内システムに関してはシステムに詳しい人間が A 社の web サイトも作成，運用していたが長期間使われていたので外部の開発業者である B 社に外部委託し web システムを刷新するとともに自社製品の販売や紹介もできる web サイトを構築することにした．

B.3　A 社の希望システム

- 製品紹介の web サイト
  A 社で販売している製品を紹介できるような web サイト，web サイトの情報更新は B 社が A 社の更新依頼を受けて行うことになった．サーバは A 社にシステムに詳しい人がいないので B 社側に管理を依頼した．
- 製品を購入できる EC サイト
  A 社で販売している商品を購入できるようにする EC サイトである．住所，名前，電話番号，メールアドレス，支払い方法 (クレジットカードかコンビニ支払いか) という個人情報を受け取って商品を発送できるようにしたい
- EC サイトの情報を管理できるシステム
  EC サイトから受け取った個人情報をすべて管理できるようにする.A 社担当者は,EC サイトから送られてくる個人情報をもとに製品を発送したい．システムが故障した場合には EC サイトの情報取り扱いを停止できるようにする．