ゴール指向を用いたセキュリティ要件の定義手法の提案

府川　真理子†　　松浦　佐江子‡

芝浦工業大学　システム工学部　電子情報システム学科†‡

1　はじめに

要求には利用者がシステムに機能として求める機能要求と「速く」等の明確な定義方法は確立していない非機能要求が存在する．セキュリティは非機能要求として定義される．

セキュリティを満たすシステム開発の大半はセキュリティに関わる知識に依存する．その為，セキュリティをシステムに組み込む際，国際標準規格 ISO/IEC 15408 として Common Criteria (CC) [1] に定義されたセキュリティ要件を熟知したシステム開発者が必要である．しかし，セキュリティ要件を作業者に依存せずに設計品質を一様にする事は困難である．

本研究ではゴール木[2]を用いたカタログとしてのセキュリティ要件の内容定義の定義により，セキュリティ要件の品質の一様化を図る．つまり，ゴール木より非機能要求であったセキュリティを機能要求にする．そして，カタログ化より開発者による設計品質の差異を減らし，更に再利用可能とする．

本稿では CC に定義された「識別と認証」の要件である「認証失敗」をカタログ化する．これをアプリケーションとしての「パスワード認証」へ適用により妥当なセキュリティ要件が抽出可能か検証する．

2　セキュリティ要件

セキュリティ要件とはセキュリティシステム開発時に満たすべき条件や要件間の依存性の定義で CC に定義されている．CC とは評価基準として定義されたもので，一般法則，セキュリティ機能要件，セキュリティ保証要件の 3 パートから成る．今回使用した要件はセキュリティ機能要件である．セキュリティ機能要件とはセキュリティ対策方針から標準言語へ書き換えられた文書で，意味的な関連から構造的に定義されている．具体的にはクラス「識別と認証」においてファミリ「認証失敗」が定義され，ファミリにコンポーネント「認証失敗時の取り扱い」が定義されている．また，各要件には定義・管理・監査等の様々な側面や依存関係も定義されている．しかし要件はクラス間で依存しているため CC から必要な要件を抽出する事は困難である．また，要件は対象システムに特化しない抽象的な自然言語で記載されているため，開発者の解釈毎に品質に差異が生じるという問題もある．

CC の利用方法として開発者が CC に定義された要件間の依存関係から対象システムに合う要件を選択する．その後，内容定義に記された文章を参照したテーラニングの実行により要件を満足させる．抽象的な自然言語の具体的化をテーラニングと呼ぶ．認証失敗のテーラニング例を以下に示す．

> TSF は[割付:認証事象のリスト]に関して，[割付:回数]回の不成功認証試行が生じたときを検出しなければならない
>
> ↓
>
> TSF は使用者のパスワードに関して，4回の不成功認証試行が生じたときを検出しなければならない

＊TSF：TOE (Target Of Evaluation) Security Function

Goal Oriented Analysis Method for Sequrity Requirements

†Mariko Fukawa　　‡Saeko Matsuura

†‡Shibaura Institute of Technology Department of Electronic and Information Systems

3　ゴール指向

ゴール指向とは、幹（目的）から枝（手段）へ関連に基づいて階層的に枝を伸ばすゴール木を用いて目的（ゴール）を曖昧な要求から明確な要求にする分析手法である．ゴールの種類として，ゴールの成立条件を明確に定義できないソフトゴールと明確に定義できるハードゴールがある．代表的なゴール指向の例として組織（アクター）毎の依存関係を分析できる i*フレームワークと一般的な非機能要求の階層構造をパターン化できる Non Functional Requirement (NFR) フレームワークがある．

ゴール指向の利用により要求変更時の影響範囲の分析，要求間の矛盾や対立の検出や解消，要求の根拠と要求漏れの確認が可能となる．つまりゴール指向を用いて要件定義の際に開発者毎の解釈の差異の減少と必要なセキュリティ要件の抽出が可能と考えた．今回は CC をゴール木で表すためパターン化可能なためカタログとして利用される NFR フレームワークを用いる．

4　NFR フレームワーク

NFR フレームワークとは非機能要求の満足化関係を階層化することにより機能要求を抽出する定義手法で、上位ソフトゴールの満足化のために下位ソフトゴールがあると読むことができる．

非機能要求を表現する基本単位として．非機能要求の満足化を表現する NFR ソフトゴール(☁)，満足化を助ける技術を表現する操作ソフトゴール(☁)，意思決定の根拠を表現する理由ソフトゴール(☁)がある．ソフトゴール間の関係を表すものとして貢献関係を用いる．上位ソフトゴールの満足化のために下位ソフトゴールが必要不可欠の場合は AND(†)，下位ソフトゴールでなくても良い場合は OR(‡)，ただ貢献しているのであれば Satisficing(↑)と表す．

NFR フレームワークの要求分析手法を説明する．①まず，満足化するべき非機能要求を顧客に文章などで表現する．②次に最初に分かる非機能要求を列挙し複数のゴール木を作成する．③その後，複数のゴール木間の相互干渉の明確化する．④最後にゴール木の終端を評価・抽出し満足化を確認する．という手順でゴール木を作成し分析する．

5　認証失敗についての NFR ゴール木の作成例

4 で述べた要求分析手法を基に考えていく．手順①では CC という仕様書を用いるためこの作業を行う必要はないと判断した．手順②では「識別と認証」の「認証失敗」の非機能要求のみをゴール木として表したが，「識別と認証」に定義されている他の要求についてもゴール木を作成する必要がある．手順③では構造化を意図した CC を用いたので既に明確化されている．しかし，依存関係等の把握は困難なために各要件間の相互干渉を明確化する必要はある．手順④作成したゴール木では，ソフトゴール間の枝について重み付けをし，評価・抽出が可能である．本稿では手順②について説明する．

文献[3]では電子タグ保護ガイドラインから表 1 の分解方法のルールを用いてゴール木の作成を行っている。CC もガイドラインと同じく規約文書であることから、各記述文の分解にはこのルールを適用することとした．

表　1　分解方法のルール

	着眼点	文例	上位ゴール
1	説明	文章の題名と内容	題名
2	手段	・<手段>により<目的>する　・<目的>するため<手段>する	目的
3	例示	・<X>するなど<A>する　・<A>する例は<X>である	A
4	条件	・<A>する条件は<C>である　・<A>するには<C>する必要が	A
5	手順	<A>するための手順は<P>である	A
6	構成	・<A>の構成要素は<E>である　・<A>は<E1>…<En>からなる	A
7	対象	・<A>する対象は<O>である　・<O>が<A>に対応する	A
8	場所	・<動作>は<場所>において行う　・<場所>に<動作>する	動作

ルールにより一意に分解可能となり，設計品質の差異が減少する．例えばCCの本文の「パラメタは、失敗した認証試行回数及び時間の閾値を含むがそれに限定されない」を分解する際にルール6の構成を用いると「パラメタを決定する」は上位ゴール他の要件は下位ゴールに貢献関係ＯＲで繋がる．

同様に作成した内容定義・管理・監査におけるゴール木を図1，図2，図3に示す．CCを忠実にゴール木で表現するため，作成時に定義とは別に付録として記された例等も要件名の前に（例）と記す形で操作ゴールとして定義した．更にCCは構造化されて記されているのでその構造を意識した．具体的には要件の貢献関係やセキュリティ要件を内容定義・管理・監査と分けた．管理とはシステムの属性やアクション等の管理で，監査とはシステムの動作の監査（ログをとる等）である．これにより各側面から要求を把握できる．

6　ゴール木の利用例

認証失敗のセキュリティ要件の使用例を説明する．

まず図1より「不成功認証試行回数に関する値を定義する」の手段として「失敗した認証試行の回数の閾値を決定する」がある．これは2の“[割付:回数]回”と同様に捉える事が出来る．つまりゴール木による部分木として把握できる．

次に図1の①「不成功認証試行回数が定義した回数に達するときに検出する」から②「セション確率プロセス終了後のアクションを定義する」へ満足化を表す矢印がある．これは①の要件満足化後②を行うと捉える事が出来る．つまり，認証失敗の動作として不成功認証試行回数が定義回数に達する→セション確立プロセス終了後のアクションを決定する→利用者アカウントを管理者定義の条件になるまでTSFを無効にする→（管理者定義の条件を満足する）→再確立するとなる．

管理・監査は定義に付加すると考える．例えば図1の「失敗した認証試行の回数の閾値」について図2の「不成功認証試行回数の定義ができる役割を決定する」ではセキュリティ定義者かシステム開発者か許可利用者が不成功認証試行回数を定義可能と記されている．つまり開発段階で回数を定数として定義するか，利用者（管理者等）が回数を定義するか選択可能としている．このとき管理者等が回数を定義する際はシステムに新たに「入力する」というサービスが必要となる．

7　まとめ

ゴール木により，要件満足化には何が必要か把握可能でき，セキュリティ要件を一意に決定可能となる．またカタログ化により後の根拠や過去の事例を追跡参照，再利用可能となる．

今後の課題として保証要件を満たすようなゴール木を作成する．保証要件とは評価対象が機能要件を満たす保証を取得する方法の記述である．これによりセキュリティを熟知してない開発者でもセキュリティレベル毎に必要な要件を把握可能と考えた．セキュリティレベルとは保証尺度で，具体例として銀行と個人における暗号取り扱い方の違いがある．これらはCCのセキュリティ保証要件に記されている．また，ゴール木で各要件間の依存関係を表現することにより選択した要件の他の要件への影響範囲が把握可能となる．

8　参考文献

[1] 情報処理推進機構: “セキュリティ評価の為のコモンクライテリアパー2:セキュリティ機能コンポーネント”

[2]山本修一郎: “ゴール指向によるシステム要求管理技法”

[3]山本修一郎　神戸雅一: “電子タグプライバシー保護ガイドラインのゴール分析” 電子情報処理学会(2006.5.15)

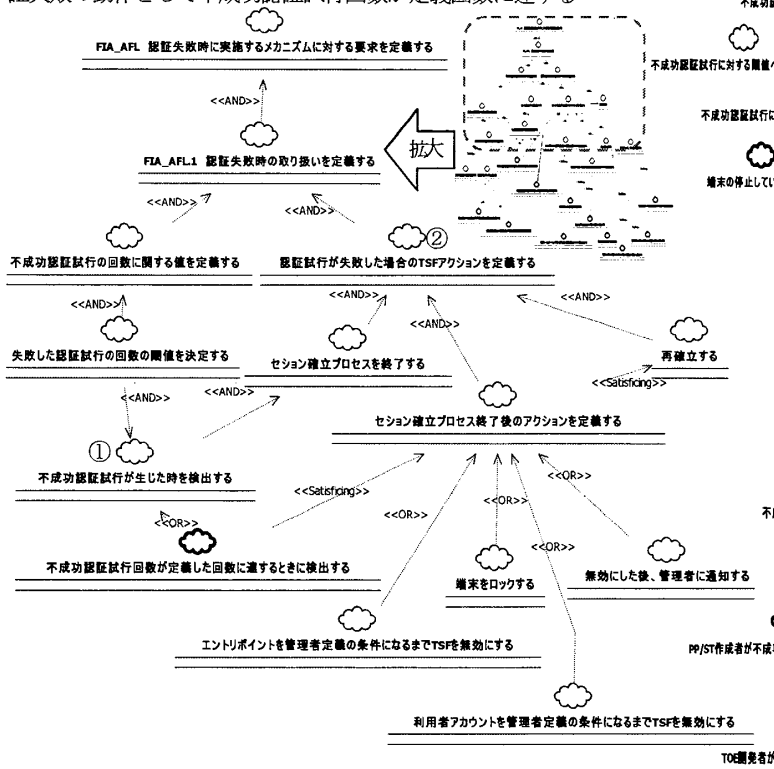

図1　内容定義におけるゴール木の一部（拡大図）

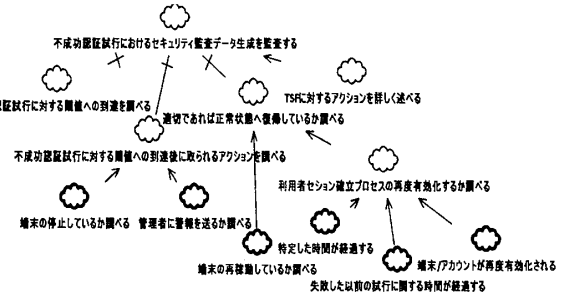

図2　管理におけるゴール木（属性）

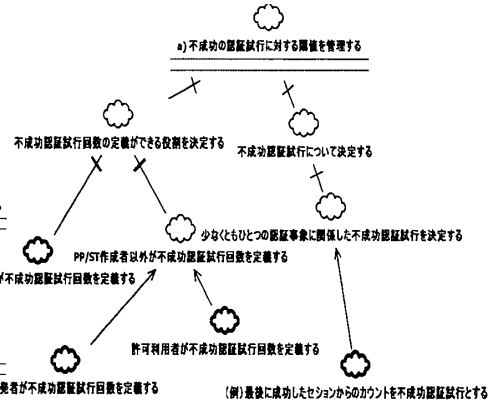

図3　監査におけるゴール木