Vol.2018-SE-199 No.18
2018/7/19

ブロックチェーン技術適用システムにおける要求獲得プロセスの一考察

山内貴弘[†1]

概要：本論文では,ブロックチェーン技術を適用しようとするソフトウェア開発プロフィールを対象として，要求獲得プロセスを検討するものである.要求獲得の技法として，i *によるゴール指向分析等を手がかりに,考慮すべき要求獲得のプロセスを検討する．またブロックチェーン技術適用の特性から，当技術の適合性の有無についても検討できるものとして提案する．

キーワード：ブロックチェーン，要件獲得，ゴール指向モデル，i* [**]

A Study on Requirement Elicitation Process in Blockchain Technology Application System

TAKAHIRO YAMAUCHI[†1]

Abstract: In this paper, we consider the request acquisition process for software development profiles to which block chain technology is applied. It is a technique to acquire requirements, using the goal-oriented analysis by i * etc. as a clue, I also propose the possibility of considering the suitability of this technology from the characteristics of block chain technology application. [**]

Keywords: Blockchain, Requirement elicitation, Goal -oriented analysis, i*[**]

1. はじめに

ブロックチェーンは 2008 年の Satoshi Nakamoto によるビットコインの論文[1]を端緒とし，その後の様々な仮想通貨発行や，各種アプリケーションへの実証実験などによって高い社会的な関心を集めている分散台帳技術である．2016 年の経済産業省による「ブロックチェーン技術を利用したサービスに関する国内外動向調査」[2]の中では，ブロックチェーン技術は，その構造上，従来の集中管理型のシステムに比べ,『改ざんが極めて困難』であり,『実質ゼロ・ダウンタイム』なシステムを『安価』に構築可能という特性を持つともいわれ，IoT を含む非常に幅広い分野への応用が期待されているという．

こうした革新的な技術とされるブロックチェーン技術はその話題性から，企業においても多くの実証実験が行われている．ガートナーによるブロックチェーンへの取り組みに関する調査結果[3]によると，11.8%の企業が実証実験を実施するとともに，これら企業を含め，40%以上の日本企業(従業員 500 名以上)は既に何らかの取り組みを開始しているという．ビットコインと同様な仮想通貨としての応用的な利用から，改ざん困難であり,取引の一貫性という観点から,スマートコントラクトといった既存システムの更新を迫るものまで多岐にわたる.しかしながら，実際のソフトウェア開発プロジェクトの現場では少なからず混乱がある.すなわち，何かしらブロックチェーンというキーワードを使うことの話題性以上の当該技術適応の意義や必要性についての確認がおろそかになっていないかという懸念である．企業や社会の課題解決の技術としてブロックチェーンを位置づけ，その中で具体的な技術課題を明らかにして， 効果的な活用の道を開くことが望まれる．そのためにはソフトウェア開発プロジェクトの最上流で，本来の要求を獲得し，その手段としてのブロックチェーンの技術適用を見極めておく必要がある．

本論文では,ブロックチェーン技術を適用しようとするソフトウェア開発プロフィールを対象として，要求獲得プロセスを検討するものである.このため，まずブロックチェーン技術の適用におけるドメイン知識の整理を行った上で，要求獲得の技法として，i *によるゴール指向分析を手がかりに,考慮すべき要求獲得のプロセスを提案する．i *ではゴールを分析するための SD モデルとそのゴールを達成するための手段を分析するための SR モデルがある．これらモデルを援用し，必要なプロセスを仮定した上で,実際のケースに当てはめて検証する．

†1 (株)クレスコ
CRESCO LTD.

2. ブロックチェーン技術の特徴

先の経済産業省の調査で示された特性のみならず，ブロックチェーンの特性として議論がされている．高木は 1) データの連結による偽造防止，2) 主体と情報資産の紐づけ，3) 不特定多数のコンピュータによる情報管理とした．[4] 青木は，ビットコインの中核技術であり，中央管理者を置かないことが特徴の一つとした．[5] さらに山崎は中核技術であるビットコインをもとに，信頼できる第三者を不要としたものであるとしている．[6] 様々な議論がなされる中， Seebacker and Schuritz はブロックチェーン技術の文献レビューをし，特徴を図 1(著者一部省略) のように示している．[7]

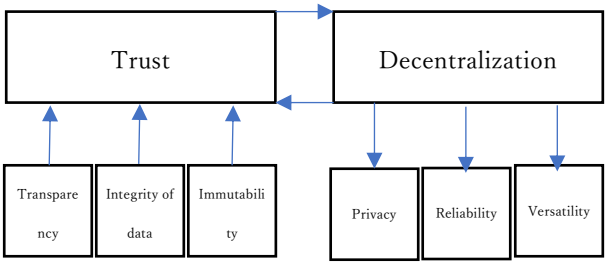

図 1．ブロックチェーン技術の特徴
Figure1. Characteristics of blockchain technology

Trust(信頼)と Decentralization(非中央集権)の 2 つの要件の相互の関係性とともに、Trust(信頼)を支える要件として,Transparency(透明性), Integrity of data(データの一貫性), Immutability(不変性) を定義し，Decentralization(非中央集権)から関連する要件としては，Privacy(プライバシー), Reliability(信頼性), Versatility(多様性)をあげている．本稿では，この Seebacker and Schuritz のモデルをブロックチェーン技術の必要要件として分析する．

3. ゴール指向モデルによる分析枠組み

本稿は，ブロックチェーン技術適用のシステムに対して適切な要求獲得を目指すものであるが，要求獲得における分析枠組みとしてはゴール指向モデルを活用する．これは Tsumaki and Tamai の要求工学技術マップ[8]で示すところの静的かつ開いている対象と認識したことによるものである．これはブロックチェーン技術の要求抽出方法として今回，静的な抽出を試みるとともに，分析対象領域としてはブロックチェーンの適用先が社会一般に開いていると判断したためである．なおゴール指向モデルの中ではゴールを分析するとともに，ゴール達成の手段を導出するため i*を用いる．

(1) i*によるブロックチェーン技術適用システム分析

Eric Yu[9]によって開発された i*は，戦略依存モデル (Strategic Dependency Model: SD モデル)と戦略依存モデル (Strategic Rationale Model: SR モデル)から構成され, SD モデルはゴールを抽出するためのモデルであり, SR モデルは，ゴールを達成するための手段を抽出するためのモデルとされる.[10]

(2)ブロックチェーン要求獲得プロセスの分析枠組み

ブロックチェーン技術の適用にあたってアクターが根本的に何を望んでいるのかについて不明確になる場合があると考えられる．例えばブロックチェーンによる課題解決を根本的なゴールと考えるのか，それともをブロックチェーンの技術を適用したプロジェクトの実施自体をゴールとするのかによって異なってくる．このように適切なゴールの抽出が欠かせないため，まずアクターが達成すべきゴールの明確化に向け SD モデルを元に分析する．そしてそこで抽出されたゴールを構造化し分析するため，ゴールマップを用いる．そこで得られたゴールの構造をもとにして SR モデルでゴール達成の手段を定義し，ブロックチェーン技術の特徴と比較し，本来的にブロックチェーン技術の適用が望ましいのか分析することとする．本稿における分析の枠組みの流れは表 1 の通りである．

表 1. ブロックチェーン要求獲得プロセスの分析枠組み
Table 1 Analysis Framework of Blockchain Request Elicitation Process

#	要件獲得プロセス
1	SD モデルによるゴール抽出
2	ゴールマップでの構造化分析
3	SR モデルによる手段の抽出
4	ブロックチェーン技術の特徴との比較分析

(3)分析対象ケース

本稿では 2 つのブロックチェーン技術の適用システムについて分析枠組みを使って検討した．一つは生命保険の保険金支払いにあたって，診断書改ざんの問題に対してブロックチェーン技術を適用しようというものである．もう一つは職場の活性化を目指し，社内通貨としてブロックチェーン技術の適用をするものである．これら 2 つのケースは実際の検討例をもとに本稿で検討した．

4. 生命保険の診断書改ざん問題への適用

生命保険のある保険のケースでは死亡もしくは重度障害にあたって，保険金が支払われる．しかしながら重度障害ではないにも関わらず，医師の診断書を改ざんし，重度障害として保険金をだまし取る例が過去に発生している．こうしたケースへの対応としてブロックチェーン技術の適用を検討した．以下，本稿での要件獲得プロセスに従って検

討することとするが，まず現状(as is)の SD モデルを示す．

(1)診断書改ざん問題の SD モデル

図 2 は，現状(as is)の SD モデルである．保険会社は事実に基づき適切に保険を支払いたいというゴールがある．ここでは改ざんの現状を表すためにアクターとして犯罪者を置き，犯罪者のゴールとそれを阻止する保険会社のチェックについて表したものである．現状，例えば医師が封書で手書きの診断書を患者に手渡しをすることを想定し，受け取った患者(犯罪者)が改ざんする流れをモデル化した．

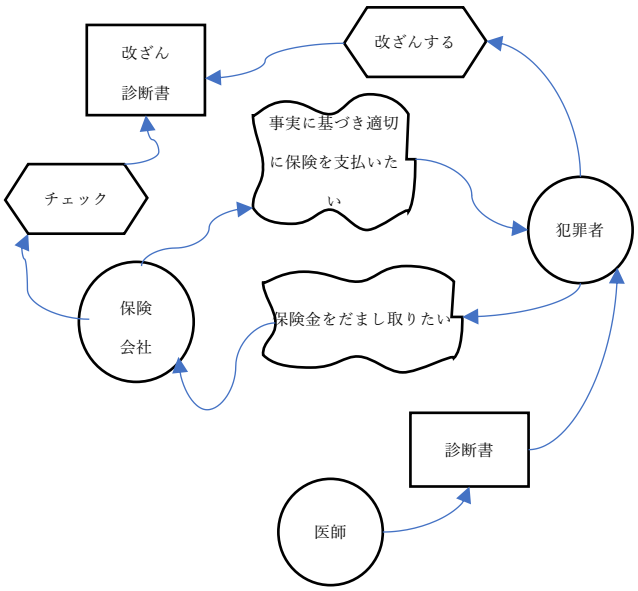

図 2. 診断書改ざん問題の SD モデル(as is)
Figure 2 Problem of alteration of medical certificate for SD model (as is)

次に図 3 として SD モデル(to be)を表した．保険の加入者をアクターとしているが，加入者には犯罪者も含まれる．

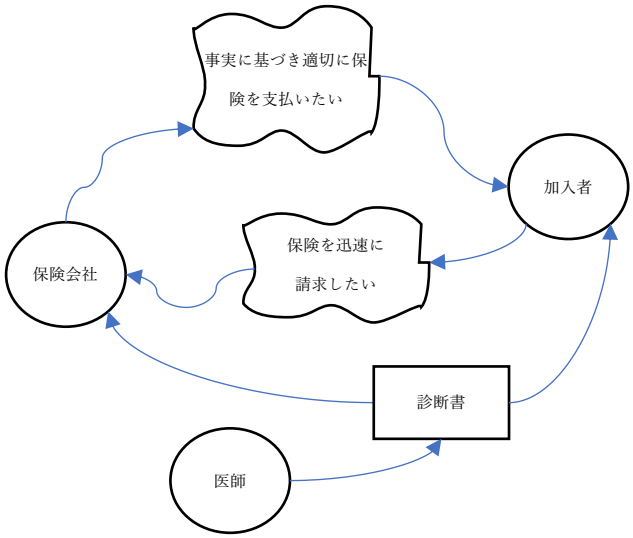

図 3. 診断書改ざん問題の SD モデル(to be)
Figure 3 Problem of alteration of medical certificate for SD model (to be)

加入者は,保険を迅速に請求したいというゴールも持つ．ここでのポイントは診断書の扱いである．改ざん問題の根本原因として診断書が加入者に渡されることにあるため，この SD モデルでは，同じ診断書が加入者とともに保険会社に共有されるようにした．

(2)診断書改ざん問題のゴールマップ

先の SD モデル(to be)の事実に基づき適切に保険を支払いたいという保険会社のゴールを分解した．ここで適切にという点に着目し，手続きに時間かけないというサブゴールも設定した．

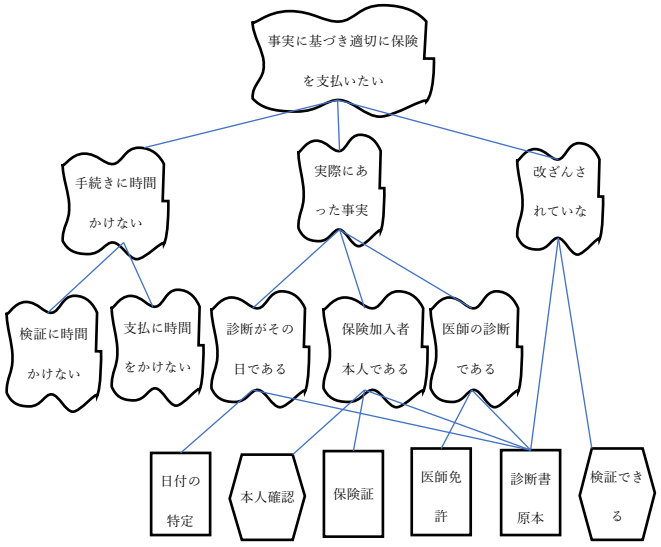

図 4. 診断書改ざん問題のゴールマップ
Figure 4 Problem of alteration of medical certificate for Goal map

(3)診断書改ざん問題の SR モデル

ゴールマップモデルで抽出されたゴールの構造および実現させるための手段をもとに、SR モデルを図 5 のように作成した．

この SR モデルでは加入者本人の診断であることを医師が確認した上で診断書を書き，その内容を加入者本人および診断書の確認を許可された生命保険会社が確認することができる流れとした．また診断書は改ざんがなされていないか検証可能としている．さらにこれらの一連の手続きに対して時間をかけないで行えることとしている．

この SR モデルで想定しているブロックチェーンの適用箇所は診断書である．すなわち，医師が診察した患者の診断書を書き，その原本を極めて改ざんされないように保持した上で，加入者，保険会社で確認可能とするための仕組みとしてのブロックチェーン技術の適用である．

これらの SR モデルがブロックチェーンの要件に適合するものか否かをブロックチェーン技術の特徴と比較して検討する．

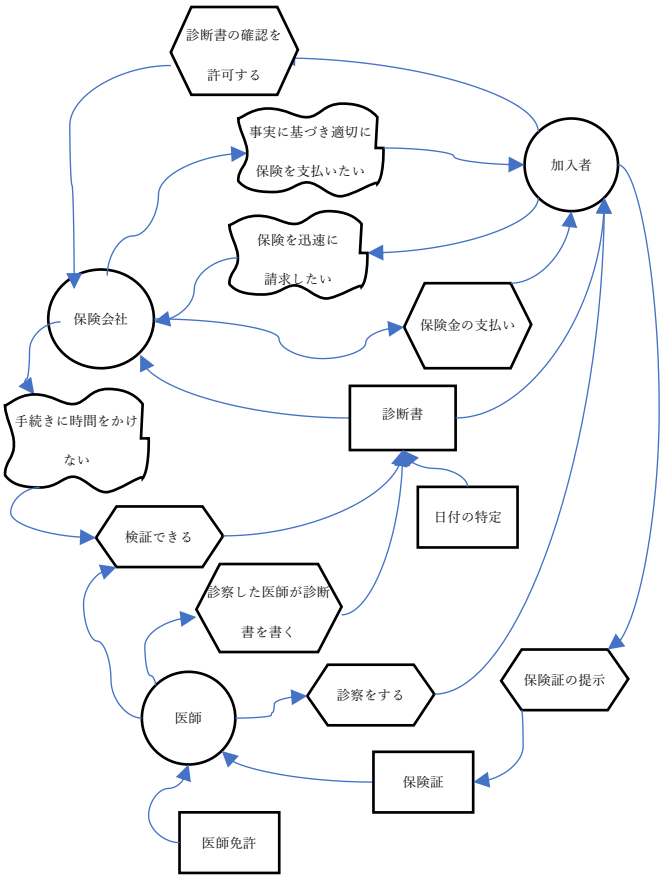

図 5. 診断書改ざん問題の SR モデル
Figure 5 Problem of alteration of medical certificate for SR model

(4)診断書改ざん問題へのブロックチェーン技術適用の妥当性分析

当診断書改ざん問題へのブロックチェーン技術適用について，表 2 と通り分析した．

表 2. ブロックチェーン技術適用の妥当性分析 1
Table2. Validity analysis 1 of application of Blockchain technology

分類	BC 要件	当ケース	備考
Trust	Transparency	適合	(a)
	Integrity of data	適合	(b)
	Immutability	適合	(c)
Decentralization	Privacy	適合	(d)
	Reliability	適合	(e)
	Versatility	適合	(f)

当ケースでは，Trust(信頼)および Decentralization(非中央集権)のどちらの各ブロックチェーン要件とも適合している．

(a) Transparency(透明性)については,診断書を複数のアクターで参照可能としているとともに，改ざんされていないか検証できることを要件としているため，その点，ブロックチェーンで求める透明性と適合する．
(b) Integrity of data(データの一貫性)は診断書という唯一の原本が複数あってはならないため，この点も適合する．
(c) Immutability(不変性)は改ざんされないことを保証する必要があるため，当ケースと適合する．
(d) Privacy(プライバシー)は当ケースにおいて診断書という個人のセンシティブな情報であるため，非常に重要である．データの透明性がありながら，必要なアクターにのみ参照可能とする要件が必要になるため，当ケースと適合する．
(e) Reliability(信頼性)については,当ケースのシステムの重要性から適合する．
(f) Versatility(多様性)はアクターである保険会社,加入者,医師それぞれが複数おり,社会的なシステムとして存在することを鑑みると，多様性は必須な要件であり,当ケースと適合する．

上記の比較検討から,当診断書改ざん問題へのブロックチェーン技術適用の妥当性はあると示唆される．次に別ケースとして職場活性化のための社内通貨のケースを分析する．

5. 職場の活性化に向けた社内通貨への適用

職場では社員それぞれの貢献によって適切な評価がされ，インセンティブが得られるようなケースが有効である場合がある．こうしたケースに仮想通貨のような機能を会社内に適用しようという動きもある．その点について本稿での要件獲得プロセスに従い分析する．

(1)社内通貨の SD モデル

図 6 は社内通貨に関する SD モデルである．

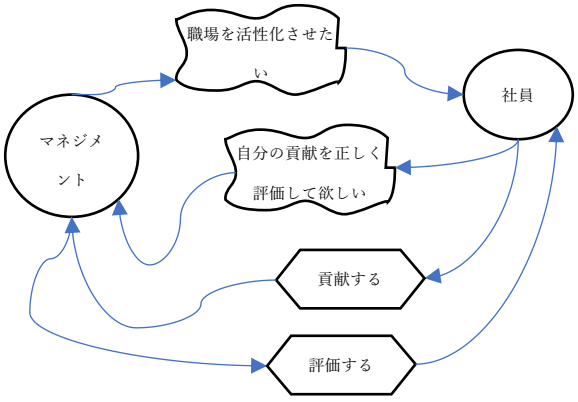

図 6. 社内通貨の SD モデル
Figure 3 Inter Company currency for SD model (to be)

このケースではアクターであるマネジメント、社員それぞれの職場を活性化させたいというゴールと自分の貢献を正しく評価して欲しいというゴールの関係を示している．次にこれをもとにゴールマップで構造を分析する．

(2)社内通貨のゴールマップ

図 7 は職場を活性化されたいというゴールをもとにゴールの構造を分析したものである． 職場の活性化のためには評価が可視化されていること，貢献に見合った評価があること，評価に見合った報酬があることをサブゴールとして以下の通り分解した．

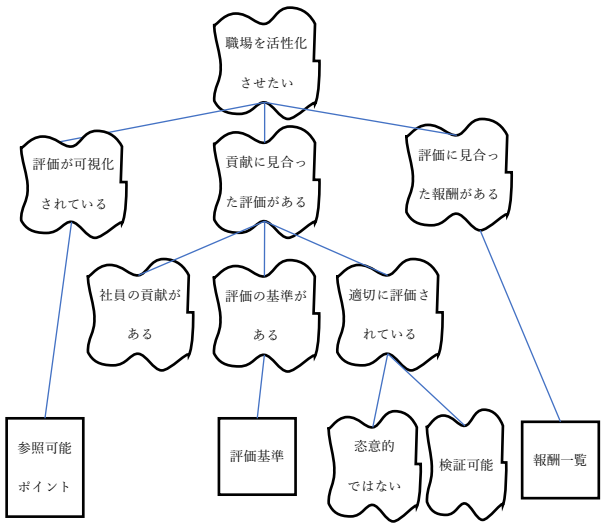

図 7. 社内通貨のゴールマップ
Figure 7 Inter Company currency for Goal map

(3)社内通貨の SR モデル

ゴールマップモデルで抽出されたゴールの構造および実現させるための手段をもとに、SR モデルを図 8 のように作成した．

ゴールマップで作成したサブゴールを達成させるための手段として参照可能なポイントを設けてある．この部分が社内通貨となる想定である．すなわち，社員の貢献に対して，マネジメントが評価するがその際の報酬として社内通貨を媒介とする仕組みとした．

またこれらの評価にあたっては評価基準を設け，恣意的なものとしないこと，さらに社内通貨のシステム自体でずるができないように検証可能なものとした．

(4)社内通貨へのブロックチェーン技術適用の妥当性分析

当社内通貨へのブロックチェーン技術適用について，表 3 と通り分析した．

当ケースでは，Trust(信頼)の部分は通貨としての信頼性から必要性はあるが，Decentralization(非中央集権)の各要件についての適合性は限定的である．詳細は次の各備考に示した通りである．

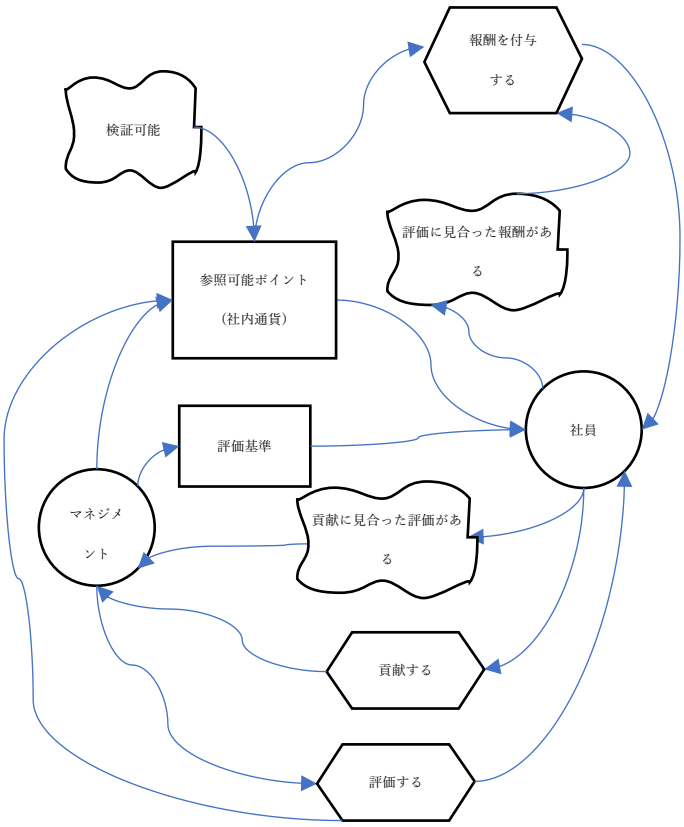

図 8. 社内通貨の SR モデル
Figure 8 Inter Company currency for SR model

表 3. ブロックチェーン技術適用の妥当性分析 2
Table3. Validity analysis 2 of application of Blockchain technology

分類	BC 要件	当ケース	備考
Trust	Transparency	適合	(a)
	Integrity of data	適合	(b)
	Immutability	適合	(c)
Decentralization	Privacy	不適合	(d)
	Reliability	一部不適合	(e)
	Versatility	不適合	(f)

(a) Transparency(透明性)については,ポイントの可視化を目的としているため,ブロックチェーンで求める透明性と適合する．

(b) Integrity of data(データの一貫性)は通貨というものの特性上，二重使用があってはならないため，この点も適合する．

(c) Immutability(不変性)は改ざんされないことを保証する必要があるため，当ケースと適合する．

(d) Privacy(プライバシー)は当ケースにおいてはそれほど必要性がない.逆に社内で獲得した通貨を可視化し競わせたい動機の方が強いと考えられるため，当ケース

は不適合である.

(e) Reliability(信頼性)については, 耐障害性は確保する必要はあるが, クリティカルなものではない.

(f) Versatility(多様性)はアクターであるマネジメント,社員に限定されているため, 多様なアクターを想定する必要はないため, 当ケースにおける適合性はない.

上記の比較検討から, 社内通貨におけるブロックチェーン技術適用の妥当性は通貨としての信頼の点のみであり, その他のブロックチェーンの持つ要件上は必要のない適用領域であると示唆される.

6. 考察

ブロックチェーン技術の適用システムとして保険会社に向けた診断書の改ざん問題の対処と社内通貨について確認した. 今回設定した SD モデル, ゴールマップ, SR モデルそしてブロックチェーン技術要件からの比較検討というプロセスにおいて, 次の点が示唆された.

- 同様なブロックチェーン技術を適用したシステムであっても, 要求を詳細に確認するプロセスにおいてブロックチェーン技術を適用する必要性のないものを発見することができる.
- 特に Decentralization(非中央集権)の各要件については, その必要性を検証することがブロックチェーン技術適用の核となると考えられる. すなわち, 社内通貨のような場合は, 一社の中に閉じており, 非中央集権である必要がないケースがあるためである.
- 当ケースは要件獲得における検討段階でのプロセス適用であり, この内容で要件の抽出し切れるものではない. しかし, 検討当初でブロックチェーン技術を適用するにあたってのスクリーニングに使用できる可能性はある.

7. おわりに

本稿では, ブロックチェーン技術を適用しようとするソフトウェア開発プロフィールを対象として, 要求獲得プロセスを検討した. 要求獲得の技法として, i *によるゴール指向分析を手がかりに, 診断書の改ざん問題と社内通貨を例に, 考慮すべき要求獲得のプロセスを提案した. 現在, 数多くのブロックチェーン技術適用の実証実験が行われており, 様々なケースがあるため, 今回の 2 ケースでの説明では限界がある. 一方, i*等を利用した要件獲得のプロセスが, ブロックチェーン技術適用についても正しい要件の整理上有効であることが示された. 今後はより詳細化した分析, 他の要件獲得での手法も検討し, 効果的な分析をしていきたい.

謝辞 当ケースの検討にあたり, 協力頂いた皆様に, 謹んで感謝の意を表する.

参考文献

[1] “Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf (2018/05/20)
[2] ブロックチェーン技術を利用したサービスに関する国内外動向調査, 経済産業省 http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html(2018/05/20)
[3] ガートナーによるブロックチェーンへの取り組みに関する調査結果, ガートナー, https://gartner.co.jp/press/html/pr20180405-01.html (2018/05/20)
[4] 高木聡一郎, “ブロックチェーンの基本と発展”, 情報処理 Vol.57, No.12, Dec2016 情報処理学会, pp1188
[5] 青木崇, “ブロックチェーン(分散型台帳)最新事情” 第 4 次産業革命を牽引する革新的な技術への期待と課題, 情報管理 Vol.60, No.3, 2017.6 科学技術振興機構, pp167
[6] 山崎重一郎, “ブロックチェー・エコノミーのコンセンサスとガバナンス”, 情報管理 Vol.60, No.6, 2017.9 科学技術振興機構, pp412-419
[7] Seebacker and Schuritz, Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review, IESS 2017, LNBIP 279, pp.12-23, 2017
[8] Tsumaki and Tamai, A Framework for Matching Requirements Engineering Techniques to Project Characteristics, Software Process; Improvement and Practice, Vol11 No5, 505-519
[9] Eric Yu, Towards modeling and reasoning support for early-phase requirements engineering, Proc. Of the Third IEEE. Pp226-235, 1997
[10] 玉井哲雄・中谷多哉子 ソフトウェア工学, 放送大学教育振興会, pp70-91