社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＩＳ－96（５）
2006／5／15

電子タグプライバシー保護ガイドラインのゴール分析

山本 修一郎　神戸 雅一

株式会社NTTデータ　技術開発本部　〒104-0033 東京都中央区新川1-21-2 茅場町タワー
E-mail: {yamamotosui, kanbems}@nttdata.co.jp

あらまし　本稿では、総務省と経済産業省が示している電子タグプライバシー保護ガイドラインを対象として具体的にゴールを分析することにより、ゴール分析を進める上での考え方を抽出する。この結果に基づいて企業情報システムに関するゴール分析の９つの視点を明らかにする。また企業情報システムへの法制度面の要求に関するゴール分析手法の可能性と課題について議論する。

キーワード　GORE, RFID, プライバシー保護, NFR, 要求工学、法制度、企業情報システム

A Goal Analysis on the RFID Privacy Protection Guideline

Shuichiro YAMAMOTO　and　Masakazu KANBE

† NTT Data Corporation R&D Headquarters,
Kayabacho Tower Bldg., 21-2, Shinkawa 1-chome, Chuo-ku, Tokyo Japan
E-mail: {yamamotosui, kanbems}@nttdata.co.jp

Abstract This paper proposes the 9 points of views to decompose the non functional goals for business information systems based on the experiment to analyze RFID privacy protection guidelines published by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry. We also discuss the possibilities and issues about the proposed goal decomposition method based on the view points for analyzing regulatory requirements for business information systems.

Keyword　GORE, RFID, Privacy Protection, NFR, Requirements Engineering, Regulation, Business Information System

1. はじめに

ゴール分析の代表的な手法には、KAOS, i*, NFRフレームワークの３つがある[1][2][3]。これらの手法の共通点は、ゴールを非機能要求、機能要求とそれらの関係に影響を与える外部環境の条件という３種に分類して、ゴール間の依存関係を明確化していることである。環境条件を示すゴールについては、それぞれ、主張、判断条件、仮説などと称しており、手法間で扱い方に差がある。ゴール間の依存関係については、次の４つの関係がある。

・AND関係：ゴールA、Bがともに成立するときゴールGが成立するか、ゴールA,Bのどちらか一方でも成立しなければゴールGも成立しないとき、ゴールAとBは、ゴールGに関してAND関係にある。

・OR関係：ゴールA、Bのどちらか一方が成立するときゴールGが成立するか、ゴールA,Bのすべてが成立しなければゴールGも成立しないとき、ゴールAとBは、ゴールGに関してOR関係にある。

・＋関係：ゴールAが成立するとき、ゴールBが成立するとき、ゴールAはBに対して＋関係にある。

・－関係：ゴールAが成立するとき、ゴールBが成立しないとき、ゴールAはBに対して－関係にある。

これらのゴール関係は論理的で明快ではある。しかし実務的に見ると、ゴールに対してサブゴールが持つ意味的な関係については必ずしも明確ではないため、具体的な局面で、どのようにゴールを分解すればいいのかという指針がなかった。

たとえば、「AならばBである」というゴールがあったとき、サブゴールとして「Aでない」と「Bである」とがOR関係で分解されることは、論理的な帰結としては理解できる。しかし、このような一般論だけで現実の問題を分析できるとはいえないだろう。

このため、筆者らは総務省と経済産業省が示している電子タグプライバシー保護ガイドライン[4]を対象として具体的にゴールを分析することにより、ゴール分析を進める上での考え方を抽出す

る。また、この結果に基づいて企業情報システムに関するゴール分析の９つの視点を明らかにする。さらに企業情報システムへの法制度面の要求に関するゴール分析手法の可能性と課題について議論する。

2. 法制度のゴール分析実験

2.1. 電子タグプライバシー保護ガイドライン

電子タグプライバシー保護ガイドラインは 10 項目の規約から構成されている[4]。このガイドラインを簡単のため RPPG(RFID Privacy Protection Guideline の略)と呼ぶことにする。RPPG の概要を以下に示す。

(R1)目的：タグの有用性と消費者の利益・プライバシー保護の共通事項を示す

(R2)対象範囲：電子タグ装着物品手交後に事業者が対応する規則を示す

(R3)電子タグが装着されていることの表示等：装着の事実・装着箇所・の性質・情報を表示する

(R4)電子タグの読み取りに関する消費者の最終的な選択権の留保：電子タグ読み取りができないようにする方法について説明・掲示・表示をする

(R5)電子タグの社会的利益等に関する情報提供：読み取りできないようにした場合、消費者利益・社会的利益が損失することについて、表示・情報提供をする

(R6)電子計算機に保存された個人情報データベース等と電子タグの情報を連係して用いる場合における取扱い：電子タグに記録された情報を用いて個人を識別できるときは、個人情報保護法としての取り扱いを受ける

(R7)電子タグ内に個人情報を記録する場合における情報収集及び利用の制限：利用目的の本人通知・公表ならびに目的外利用する場合の本人同意を得る

(R8)電子タグ内に個人情報を記録する場合における情報の正確性の確保：正確・最新の内容、電子タグから紐付けされる個人情報を消費者に開示・訂正、情報の消失・き損・改竄・漏えいの防止を実施する

(R9)情報管理者の設置：プライバシー保護情報の適正管理・苦情処理、連絡先の公表を行う

(R10)消費者に対する説明及び情報提供：消費者が意思決定できるように、電子タグの理解を助ける

2.2. ゴール分析の進め方

本稿では、以下に示すように、RPPG の規約ごとに、ゴール分析のポイントと、作成したゴール図の説明を明確にすることによりゴール図を記述した[5][6]。この理由は、各規約に対するゴール分析が終了した時点で、これらのポイントをすべての規約にわたって系統的に分類・整理することで、ゴール分析の視点を具体的に抽出することができると考えたからである。

ゴール分析のポイントでは、RPPG の記述文をどのように解釈し、サブゴールを抽出するかという考え方を具体的に記録した。このようなやり方は文章記述からゴールを逆に導いているので、ゴールのリバースエンジニアリングと考えることもできる。

ゴール図の説明では、作成したゴール図を構成するゴールとサブゴールの関係を記述する。

2.3. ゴール分析の具体例

(R1)ガイドラインの目的に対する分析例を以下に示した。他の分析結果については[4][5]で示している。

【記述】本ガイドラインは、電子タグの有用性を利活用しつつ、消費者の利益を確保し、電子タグが円滑に社会に受け入れられるようにするため、電子タグに関する消費者のプライバシー保護について業種間に共通する基本的事項を明らかにすることを目的とする。

【分析のポイント】

まず、「目的」という単語に着目する。その前にある「業種間に共通する基本的事項を明らかにすること」までが、RPPG 全体の目的であることが分かる。注意するのは、「目的」という用語があるからといって、この節が R1 の親ゴールにはならないことだ。この理由は、中ほどに「するため」というが言葉があるからだ。つまり「前半に記述してあること」を実現するために、「後半に記述してあること」が手段として必要になるということだ。したがって、真の親ゴールは「電子タグが円滑に社会に受け入れられるようにする」ことである。また、この記述の前にある「電子タグの有用性を利活用しつつ、消費者の利益を確保し」という記述については、「しつつ」と「し」の解釈が重要だ。ここでは、「し」を「することにより」と考える。そうすると、実はこれらの記述はやはり「電子タグが円滑に社会に受け入れられるようにする」を実現するための手段ということになる。

「電子タグに関する消費者のプライバシー保護について業種間に共通する基本的事項を明らかにする」のところはどうなるだろうか？これをまとめてひとつのサブゴールにすることもできる。ここでは「について」の前半と後半に分けて、「電子タグに関する消費者のプライバシーを保護する」と「業種間に共通する基本的事項を明らかにする」との２つのサブゴールに分けて、後者を前者のサブゴールとした。この理由は、業種ごとの約束事としてのサブゴールがあるかもしれないと考えたからである。

【ゴール図】

ガイドラインの目的に対するゴール図を図１に示

す。親ゴールは「電子タグが円滑に社会に受け入れられるようにする」とした。そのサブゴールは「電子タグの有用性を利活用する」ことと「消者の利益を確保する」ことである。これらは「電子タグに関する消費者のプライバシーを保護する」ことによって実現される。そのためには「業種間に共通する基本的事項を明らかにする」ことが必要である。

2.4. ゴール図の統合

RPPGごとに10個のゴール図を作成した後で、これらを1つのゴール図に統合することを試みる。これによりRPPGを構成するそれぞれの親ゴール間の相互関係を明確にすることができる。

それでは条文ごとに作成したゴール図を統合するにはどうしたらいいだろうか？そのためには関連するゴールをまとめる必要がある。ゴールのまとまりにはどのような種類があるかを明らかにする必要がある。前述したように、AND関係とOR関係によってゴールをサブゴールに分解することは考えたが、それはゴールとサブゴール間の論理的な関係であって分解の意味を考えているわけではない。

ゴールのまとまりの意味を考えてゴール図を統合すると、たとえば図2に示すようになるだろう。この図では、まず、ゴール(R1)を達成する対象としての事業者を規定するサブゴール(R2)と、ゴールの達成手順を規定するサブゴールのまとまり(RA,RB,R9)に分解した。またサブゴールの達成手順は、準備・実施・管理というゴールのまとまりに分けた。電子タグに関するプライバシー保護の準備としては、消費者にプライバシーを保護する能力を持たせるための手段（RA）が必要で、その内容として電子タグを適切に取り扱えるようにした上で（R10）、電子タグが商品に装着されていることを認識できる（R3）という段取りが必要だ。電子タグのプライバシー保護の実施(RB)では、電子タグのシステム構成に着目して、電子タグに対してプライバシーを保護する(RC)と、電子計算機に記録される電子タグ情報についてプライバシーを保護する(R6)に分解する。

電子タグに対するプライバシー保護では、消費者が電子タグを取り外す(R4) か、電子タグを読める状態でプライバシーを保護するか(RD)かのどちらかを選択する。後者の場合には、電子多タグ内に記録された情報の利用を制限した上で(R7)、電子タグ情報の正確性を確保する(R8)という手順が必要だ。

ここで、RA,RB,RC,RDは、ゴール図を統合するために導入した中間的なサブゴールである。こうして再構成されたゴール図を振り返ってみると、逆に電子タグプライバシー保護ガイドラインを導く検討のステップが見えてくることに気づく。ということは、法律を導出するときにも、ゴール図が役に立つということだ。つまり法律をゴール指向の考え方でエンジニアリングできる可能性があるわけだ。

ゴールの意味的な関係の分類については3章で述べる。

3. ゴール関係の分類

以上述べたように、10個の個別ゴール図と1個の統合ゴール図に基づいて、以下に示すようなゴール間の関係を明らかにした。

電子タグプライバシー保護ガイドラインの文章からゴールを抽出するときのポイントの記述を整理することにより、説明、分類、手段、例示、条件、手順、構成、対象、場所という9つのゴール関係の種類を抽出した。この関係を「ゴール分解の視点」と呼ぶことにする。

3.1. ゴール分解の視点

◆説明

文章の章や節には題名がついているので、文章の題名からゴールを抽出し、文章の内容に基づいてサブゴールを作成することができる。

適用箇所：R8

◆分類

たとえば、R6では、表を用いて、個人情報取扱事業者に係る義務を、個人情報の利用目的関係、取得関係、個人データの管理関係に分類している。また具体的な義務の内容をこれらの分類項目ごとに箇条書きで述べている。このような場合、表の構造を用いてサブゴールを階層的に抽出することができる。

適用箇所：R6

◆手段

次のような文があるとき、ゴールPを実現する手段をサブゴールMが表現している。

【例1】「＜M＞により、＜P＞する」

【例2】「＜P＞するため、＜M＞する」

「により」に着目すれば、Pが目的であり、Mがそれを実現する手段を示していることがわかる。これに対して「するため」の場合、Pが目的であり、Mがそれを実現する手段を示している。

例文：電子タグが円滑に社会に受け入れられるようにするため、電子タグに関する消費者のプライバシー保護について業種間に共通する基本的事項を明らかにする。

適用箇所：R1,R3,R4,R6,R9,R10

◆例示

次のような文があるとき、ゴールAを実現する事例

をサブゴールXが表現している。

【例3】「<X>するなど、<A>する」

【例4】「<A>する例は<X>である」

例文：情報提供を行う等、消費者の電子タグの理解を助けるよう努める。

適用箇所：R3,R4,R10

◆条件

次のような文があるとき、ゴールAを実現するための条件をサブゴールCが表現している。

【例5】<A>する条件は<C>である

【例6】<A>するには<C>する必要がある

適用箇所：R3,R4,R5,R7,R8

◆手順

次のような文があるとき、ゴールAを実現するための条件をサブゴールCが表現している。

【例7】<A>するための手順は<P>である

ゴールAを実現するシナリオを一連の手順や段取りをPで記述された内容が与えている。

Pの内容では、通常、「～し、～する」というように、接続詞でつなぐことで、順序を表現する。

例文：電子タグに関する消費者のプライバシーを保護するためには、そのための準備として消費者にプライバシーを保護する能力を与え、プライバシーの保護を実施し、個人情報を責任者が管理するという手順が必要である。

注意：手段と手順の違いは、手順の場合だとサブゴール間の順序関係が付けられているが、手段の場合にはサブゴール間の順序関係までは規定しないことにある。

適用箇所：R8

◆構成

次のような文があるとき、ゴールAの構成要素をサブゴールEが表現している。

【例8】<A>の構成要素は<E>である

【例9】<A>は、<E1>・・・<En>からなる

適用箇所：R8

◆対象

次のような文があるとき、ゴールAの構成要素をサブゴールOが表現している。

【例10】<A>する対象は<O>である

【例11】<O>が<A>に対応する

例文：当該電子タグ及び当該電子タグが装着された物品を取り扱う事業者が対応することが望ましい規則について定めるものである。

適用箇所：R2

◆場所

次のような文があるとき、ゴールAを実現する場所や物体をサブゴールWが表現している。

【例12】<動作>は<場所>において行う

【例13】<場所>に<動作>する

例文：商品に電子タグが添付されていることを表示する

適用箇所：R3,R4

3.2. ゴール関係の参照モデル

ゴール分解の視点を考慮したゴール関係をクラス図で整理すると図3のようになる。図3の階層関係には、視点に対する9個の関係と、接続関係がある。接続関係は、階層関係の種別がAND関係かOR関係のいずれであるかを表現するものである。したがって階層関係の属性としてもいいが、ここでは図のわかり易さを考慮してクラスとして記述した。

4. 考察

本稿では、法制度の例として「電子タグプライバシー保護ガイドライン」を対象としてゴール分析をした。個人情報保護法や日本版SOX法を見てもわかるように、ITがビジネスの基盤要素になるにつれて、ITコンプライアンスが重要な課題になっている。法制度は企業が遵守する必要のある社会的なルールであって、法制度に対するゴール分析ができればすべての企業が共通的に利用できる可能性が高いと考えられる。基本的には、企業ごとに個別に同じ法律を分析しなおさなくてもいいと思われる。

たとえば、片山らは、情報科学による安心な電子社会の実現を目指して「検証進化可能電子社会」の研究を推進している[7]。電子社会を形式的に記述する上でも、法制度文書をゴール分析しておくことで形式的な記述を容易化できると考えられる。

また、経営からみるとITをいかに適切に活用して経営目標を実現するかが重要になってきており、ITケイパビリティが注目されている。したがって、ITに対するゴール分析では、図3に示したように経営目標と法令順守の両面を考慮する必要がある。経営目標とそれに対する非機能ゴールは企業ごとに異なるかもしれないが、法制度に対する非機能ゴールは各企業で共通的に必要となるはずだ。ITへの機能要求はこれらの非機能要求を実現する必要がある。このように系統的に法制度と経営目標から機能要求を抽出することができればビジネスとITが首尾一貫することになり、ITアラインメントが達成されるだろう。

5. おわりに

本稿では、「電子タグプライバシー保護ガイドライン」を対象として具体的なゴール分析を実施し、個別的なゴール図の統合手法を示すとともに、ゴール分解

の視点を、説明、分類、手段、例示、条件、手順、構成、対象、場所という９つの関係として明確化することができた。従来はこのようなゴールを分解するときの視点は必ずしも明確ではなかったので、どのようにゴールを分解すればいいかわかりにくいという問題があった。今回明らかにした９つの視点は、ゴール分解を段取り立てて進める上で、実務面から見ても有効であると考えられる。今後も継続して適用経験を蓄積してこれらの視点の十分性や有効性を確認していく予定である。

ゴールを分解していく過程で、どの視点を適用していくかという順序によっては、作成されるゴール図が異なる場合があるかもしれない。このようなゴール図に関する等価性についても検討する必要がある。

ゴール図の統合で導入した中間ゴールは各規則に対するゴールを結合しており、RPPG 全体を理解する上での道標を与えている。この意味では、中間ゴールが統合ゴール図の核であるといえよう。逆に考えれば、RPPG のような法制度体系をゴール分析する上では、中間ゴールをどのように設定していくかが、体系の完全性や一貫性を検証する上で重要になると思われる。

もし企業情報システムが遵守すべき法制度がゴール図で定義されていれば、企業情報システムに対するゴール図との関係を明らかにすることで、企業情報システムの法制度に対する適合性の判定を容易化できる可能性がある。これらの問題についても検討していく予定である。

文　献

[1] Lawrence Chung, Brian Nixon,Eric Yu, John Mylopoulos, Non-Functional Requirements In Software Engineering, Kluwer Academic Publishers, 2000.

[2] Kotonya, G. and Sommerville,, I., Requirements Engineering – Process and Techniques, John Wiley & Sons, 2002.

[3] 山本修一郎, 要求定義・要求仕様書の作り方、ソフト・リサーチ・センター、2006.

[4] 総務省・経済産業省：http://www.soumu.go.jp/s-news/2004/pdf/040608_4_b.pdf

[5] 山本修一郎, 要求工学, 第17回ゴール分析 応用編, http://www.bcm.co.jp/site/youkyu/youkyu17.html

[6] 山本修一郎, 要求工学, 第18回ゴール分析 応用編つづき, http://www.bcm.co.jp/site/youkyu/youkyu18.html

[7] 片山卓也、検証進化可能電子社会、情報処理学会誌、vol.46, no.5, pp.515-512, 2005.

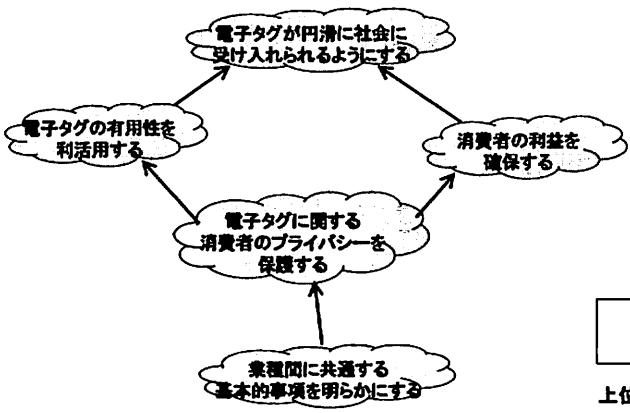

図1 RPPG-1 ガイドラインの目的

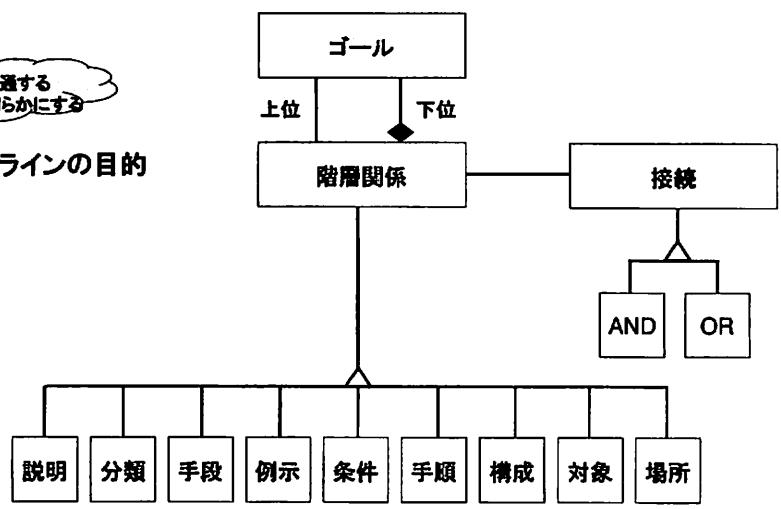

図3 ゴール図の関係

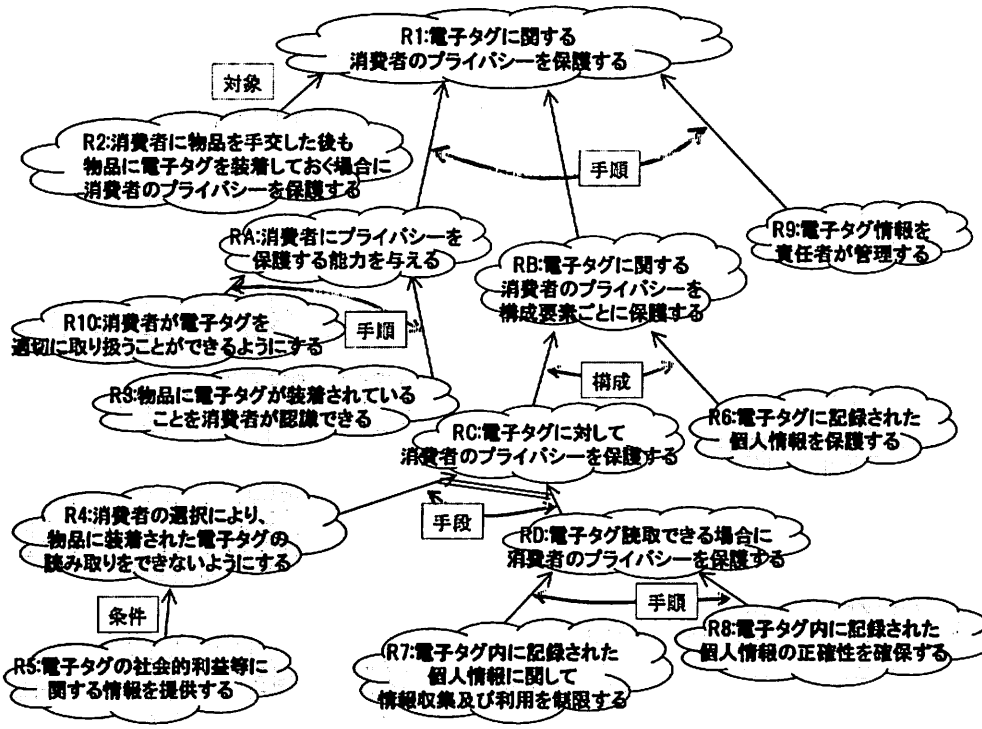

図2 ガイドラインに対するゴールの全体構成

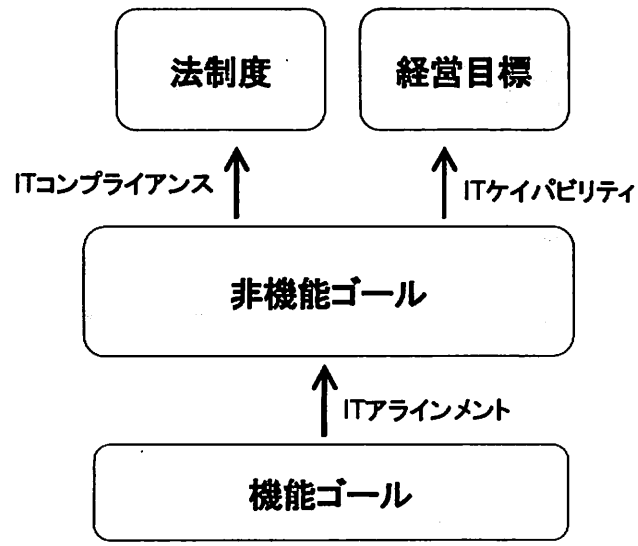

図4 経営目標、法制度とゴール