解集合モデルを用いたセキュリティポリシー等の解釈発見手法

金井　貴

1 はじめに

PCとインターネットの普及に伴い、企業内における情報共有が飛躍的に進んでいる。現在多くの企業において、内部的には顧客情報の共有化による顧客マネジメントシステムの利用や流通・在庫管理情報の共有化による生産性向上を図り、また外部的にはメールやWWW等による顧客等への情報提供や、財務情報等経営に関する情報をWWWを通じて公開することによる投資家への情報提供(IR)、さらにインターネットを通じた電子商取引等、多岐に渡る情報の流通・管理等が行なわれている。

一般に企業内および企業外との情報共有におけるメリットは非常に大きいが、一方で電子商取引により取得したクレジットカード番号の流出による被害や顧客の個人情報を流出させるなどの問題が頻発している。このような意図しない情報流出は顧客情報を扱う従業員の単純ミスから起きることが多かったが、近年ウィルスをP2Pを介してウィルスをばらまき、感染してPCに保存してある個人情報や機密情報等をP2Pネットワーク上で公開してしまうという悪質な事例も起きており、社会的な問題となっている[1]。こうした問題は民間企業だけでなく政府や地方自治体等においても機密情報流出やホームページ改竄等の問

題が起きており、政府においても対応をせまられることになった。

近年問題となっている情報漏洩問題の一例としては、ADSL 接続事業を運営する事業者の元契約社員らによる個人情報の不正取得に対して損害賠償請求が行われたことがあげられる[2]。この事件では、ADSL 接続事業者の元契約社員らが共謀してインターネットカフェから ADSL 接続業者内の顧客情報が格納されているサーバへ侵入し、個人情報の不正取得を行っている。サーバへの不正アクセスの方法としては、外部からメンテナンス業務を行うために使っていた Windows のリモートデスクトップ機能を悪用し、職場内で共用していたユーザおよびパスワードを用いて同社サーバー内への侵入に成功している。つまり元契約社員らは在籍時共同利用していたメンテナンス用のアカウントとパスワードを使い、個人情報の不正取得を行うためにリモートアクセスを利用してインターネットカフェからアクセスを行っていたのである。

この事件においては、顧客が起こした裁判において、リモートアクセスを許可したことおよび個人情報に対するアクセス管理に関して ADSL 接続事業者側に一般注意義務があると判断され、リモートアクセスのためのアカウントとパスワードについて、不正アクセスを行った者が退職した後にパスワードの変更もしくはアカウントの削除を行わなかったことが注意義務違反であると判決内で指摘されている。特に裁判ではリモートアクセスのユーザ管理について、メンテナンス業務も行う契約社員らに対して１つのアカウントとパスワードを共有させ使用させていたことやサーバの管理者権限を知っている契約社員の退職に伴うパスワードの変更等のユーザ管理が十分に行われていなかったことが問題とされている。しかし管理者権限を持つ従業員等の異動や退職に伴うパスワード変更等のユーザ管理は定期的に起きるわけではなく、また誰がどのような権限を持っているかはケースバイケースであるため、このような管理業務は必然的に非定型業務となり、ユーザ管理を担当する従業員が継続的かつ意識的にユーザの動向を管理しなければ十分管理される可能性は低いと考えられる。加えて前述の個人情報持ち出しの主犯が元契約社員であることからわかるように、昨今の流動的な雇用形態におけるパスワード管理等のユーザ管理業務は従来に増して困難になりつつある。この事例からわかるように、現状において企業等においてデータ、特に個人データへのアクセスに関する十分な管理が非常に重要かつ困難な業務であるにもかかわらず、その管理プロセスにおいて十分な対策がなされていないことが推測される。

こうした問題を受け、企業等では個人情報等へのアクセス権限の管理プロセスが十分になされていないという問題に対して、個人情報保護法や不正アクセス防止法等に対する法令遵守を企業内へ浸透させるため情報セキュリティポリシーやコンプライアンス規程を定め、これらの規程を遵守させることで情報漏洩等を防止しようと試みている[3]。こうした法令遵守を含むコンプライアンスを実行するにあたっては、内部規程を定めただけでは十分でなく、従業員への教育や指導等の継続的な活動が必要となってくる。特に従業員が内部規定を正しく解釈し、業務を行うにあって内部規程を逸脱しない行動を行えるようにすることが重要である[4]。第19次 国民生活審議会 個人情報保護部会 第14回資料１「個人情報保護法の施行状況等について」によれば、平成16年度に事業者および委託先の従業員が不注意で個人情報を漏洩した事案は全体の65%となっており、従業員が不注意により問題を起こさないよう教育する必要がある。また多くの公になった個人情報漏洩事件では、顧客情報管理に関する内部規程があることを(契約社員や派遣社員を含む)従業員等が知っていたとしても、不注意や理解不足により個人情報を流出させてしまっており、内部規程だけでなく、その規程を従業員がどのように解釈する可能性があるかということを知っておかなければ十分な内部統制が行えないということになりかねない。

そこで本論文では、従業員等がセキュリティポリシー等の内部規程を、思い込みや不注意等のバイアス要因によりどのように解釈する可能性があるのかを発見するため、従業員等が持つ可能性がある信念モデルとして解集合モデルを想定し、解集合モデルにより内部規程の解釈にどのような多様性が生まれる可能性があるかについて論ずる。また従業員等の信念モデルとして解集合モデルを用いるだけでなく、解釈の信念バイアスを新たに知識として追加することで、内部規程の解釈モデルをより実際の解釈バイアスへ近づけることで、より人間に近い内部規程の解釈の多様性を発見することを目的とする。

2　関連研究

一般に情報を不正アクセスや情報漏洩から守る手法は多様である[5]。本論文では、まずデータアクセス権に関連する研究について述べる。

データアクセスへのアクセスをアクセス権限を設けることで制限する手法については、データベース研究の初期から行なわれており、現在一般的に利用されている情報セキュリティ対策としてのデータへのアクセス制限もこのデータベースへのアクセス制限に基づくものが多い。企業が管理するデータの多くはデータベースに格納されており、ユーザから提供された個人情報や商品の情報を収集しデータベースへ自動ないしは手動で追加・変更することでデータベースを更新することで情報の有用性を保持しようとする。この情報更新プロセスにおいてアクセス制限が設定されていなければデータの格納されているサーバが特定できれば誰でもアクセス可能となるため、データベースへのアクセス制限は情報セキュリティの基本であるともいえる。

データベース上のデータに対するアクセス制御としては、役割に基づくアクセス制御（Role Based Access Control）が一般的であり、現在も多くのアクセス制御はこの方式で行われている。役割に基づくアクセス制御とは、データベースへアクセスするユーザに対しIDおよびIDの属する役割（Role）とよばれる属性を設定することにより、データベース管理者がデータの取得・変更・削除等に関して特定のユーザへ許可や禁止を行うことができる。この手法ではデータアクセスに関してIDや役割に従ってデータベース管理者のみがアクセス制限を行うことができる。

役割に基づくアクセス制限は単純で有用性の高いアクセス管理手法であるが、個人情報保護の観点から見ると機能として十分でないことが指摘されている。例えば個人情報を含むデータベースではOECD理事会勧告[6]など様々な規程やガイドラインを尊守する必要があるが、個人情報のある目的への利用に関して許可ないしは禁止を行なえるのは個人情報を提供するユーザ側であり、データベース管理者が従業員へ一括でアクセス制限を行う方式では利用目的に即した個人情報の利用のみにアクセスを制限しているとは一般的には言えないと考えられる。

こうした問題に対処するため、個人情報保護を目的としたいわゆるヒポクラティックデータベース（Hippocratic database）が提案され[7]、個人情報保護を意識したアクセス管理の拡張として注目されている。個人情報保護を意識したデータベースでは、プライバシーポリシーおよびプライバシー認証から構成されるメタデータをデータベースへ付加し、データ利用者のデータへのアクセス認証等を行う手法を主に用いている。従来の役割に基づくアクセス制御では、データベースを利用するユーザごとアクセスの禁止や許可を与えていたが、ヒポクラティックデータベースでは顧客等データの提供者が企業内におけるデータの利用に対し許可や禁止を行うことで個人情報提供者自身がアクセス制限を行うことが可能である。また役割に基づくアクセス制御の別の拡張としては、アクセス制御に目的（purpose）を導入するByunらの研究がある[8]。Byunらの研究では、役割によるアクセス制御に加えて、どのような業務のためにデータへアクセスするのかという目的という概念をデータアクセス制御に組み入れることで、より柔軟性のあるアクセス制御や安全性を高めるデータベース保護を行うための枠組みを提案している。

これらデータベースのアクセス管理機能を用いた手法は、システム内に情報アクセスに関する権限を付加することでセキュアな環境を構築することを目的として行なわれる。しかし実際の個人情報漏洩事件では、個人情報等に関する規制があり、かつ技術的にも個人情報漏洩を防ぐ手段が存在するにもかかわらず従業員のミスにより個人情報を漏洩してしまうという事例が多い。先に挙げた情報漏洩事件の判決においてもリモートアクセスの制限のための手段には代替手段が存在するにもかかわらず管理体制について著しい不備があったとの指摘がなされている。このように個人情報漏洩の未然防止が技術的に可能であるにもかかわらず情報漏洩が起きる現状から考えると、アクセス制御のみに頼った手法では限界があると考えられる。

次に個人と社会における規制等に関連する研究について述べる。個人等が社会において与えられた規範や規制を遵守するか否かに関する研究としては、マルチエージェントにおける規程の遵守に関する研究があげられる[9][10]。マル

チエージェント環境と規程の遵守に関する研究では、エージェントの目的とエージェントの属する社会に存在する規制との間に矛盾がないか、もしくは与えられた規制をエージェントが遵守することが可能であるかどうかを判断することにより、社会の規制を遵守する環境を保つことを主眼においている。具体的には、一般社会に存在する法律や社会ルール、内部規程等、社会規範や倫理規定等をモデル化し、エージェント環境内に導入した上、エージェント間のインタラクションに関して規制を遵守できるかどうかについて判定する方法に関し研究されている。このような社会ルール等があるマルチエージェント研究の一例としては、個々のエージェントの振る舞いが、そのエージェントが属する社会全体の規制と適合するかどうか、またエージェント自身が持つ目的と社会規制との整合性を検証する研究等があげられる。またHeckmanらはエージェントシステムが個人の権利を侵害する可能性について主に法的側面から論じており、権利侵害を行いにくいエージェントデザインについての助言を行っている[11]。

上記で述べた研究ではエージェントが社会規制に適合するかどうかを判定することを主目的としているため、社会内部に存在するエージェントが故意や解釈の相違等により規程を遵守しないといった可能性を考慮していない。また実社会では法律等を含む規制の多くには解釈に幅があり、個人の立場により好ましいと思われる規程の解釈が異なる可能性があるというケースを想定していない。そのため社会に存在する規制が解釈の余地のないほど厳密に定義されているというケースを除き、実社会におけるコンプライアンスのプロセスが十分モデル化されているとは言い難いと考えられる。

3　解集合モデルを用いた解釈発見手法

本章では、従業員等が不注意や偏った理解により、セキュリティポリシー等の内部規程をどのように解釈する可能性があるのかを発見するための手法について述べる。まず初めに解集合を用いた内部規程の解釈モデルのフレームワークについて述べ、内部規程に関する知識や組織が内部規程を置く目的等をどのように表現するかについて説明する。次にフレームワークを用いて実際にデータベースアクセスに関するセキュリティ規程を記述し、従業員等が持つ可能性のある内部規程の解釈に関するバイアスにより内部規程のみでは表現できない様々な解釈の可能性が存在することを示す。

3．1　解釈バイアスを考慮した内部規程等の知識表現フレームワーク

前章で述べたように、情報への不正アクセスや情報漏洩の防止、特にプライバシー保護規程の遵守を支援するシステムに関し活発に研究されているが、これらの研究ではコンプライアンスに関連する内部規程の解釈は一通りに定まることが前提とされており，その解釈の定まった内部規程と矛盾の無い行動を従業員やコンピュータ・エージェントが行っているかどうか（または行えるかどうか）について検証する手法の開発が進んでいる。しかし実際の情報漏洩等の事件では従業員等による内部規程の記述に関するの誤解や不注意等、内部規程そのものよりも内部規程の解釈が適切に行われていないため引き起こされることが多い。そのため法令遵守や内部規程遵守等のコンプライアンスのプロセスを適切に表現するためには、法令や内部規程等単一の知識記述から多様な解釈が行われることを前提とした知識表現モデルが必要となる。そこで本研究では複数のモデルを持ちうる知識表現形式として解集合モデルを基礎的なフレームワークとして採用することで、知識の解釈モデルを複数持つことを可能とするアプローチを取ることとした。

解集合モデルを採用することで解釈の多様性の一部を表現することはできるが、解集合モデルを用いた内部規程の解釈モデルだけでは、個々の従業員等の内部規程の解釈におけるばらつきや、個人の解釈モデルと組織から与えられる内部規程や制約との相違を明確に分離して表現することが困難である。そこで本研究では、内部規程に関する知識を組織における内部規程の目的、内部規程に関する知識、事実、および個人が持つ知識解釈のバイアスの４種類に分類することとした。以下に本論文で採用する知識表現フレームワーク[12]を示す。

定義：エージェントの知識解釈フレームワーク

エージェントの知識解釈フレームワークは〈G, R, F, B〉の４つ組で構成される。

- G：組織のコンプライアンス規程に即した目的。これらは解集合プログラミングにおける一貫性制約（integrity constraint）として記述される。
- R：コンプライアンスに関する知識を表現する一般ホーン節（general horn clause）の集合。
- F：物や人に関する事実（fact）の集合。アクセス許可や役割などが記述され，通常事実節で表現される。
- B：内部規程に関する解釈バイアスの集合。解釈バイアスとはエージェントがコンプライアンス知識を解釈する際用いられる可能性のある知識のことであり、Bに含まれる個々の解釈バイアスは一般ホーン節の集合で記述される。

エージェントがとりうる解釈バイアス Δ は、上記フレームワークを用いて構築されるリテラルの集合である。解釈バイアス Δ は下記の条件を満たすことが要請される。

$$\Delta \in \bigcup_{i \in I} B_i \text{ ただし} B_i \in B$$
$$R \cup F \cup \Delta| = G$$
$$R \cup F \cup \Delta \text{が矛盾しない}$$

ここでIは B_i のインデックス、各 $B_i \in B$ はあるエージェントの持つ可能性のある解釈バイアスの一部である。

3．2　例題

本節では前節で導入した知識表現フレームワークを用いて、あるデータベースに関するセキュリティポリシーに関する知識を記述し、エージェントが持ちうる解釈バイアスを導入した際どのような解釈がなされうるかについて、例題を用いて説明を行う。本節で用いる例題としては、組織内のプライバシー情報を含む可能性のあるデータベースとそうでないデータベース、また従業員に関する情報としてプライバシー情報へアクセス可能な役職とそうでない役職があるとして、データベースへのアクセス制限に関してどのような解釈が行いうるのかについて考察する。

例題：企業Ａでは顧客の注文に応じて商品を配送するために、メールアドレスのデータベースと代金請求のための購買情報に関するデータベースの２種類のデータベースを作成し利用している。購買情報に関するデータベースは住所や氏名等が含まれているためプライバシー情報を持つデータベースであると企業Ａ内で定められている。

顧客はＡへ情報を登録する際、自身が登録したメールアドレスに請求書を送ることを許可しており、また従業員がマーケティング分析のため（プライバシーを考慮したデータマイニング[13][14][15]等のプライバシー保護技術を用いた上での）購買情報を利用することを認めているが、マーケティング分析以外の用途のために購買情報を利用することは認めていない。

企業Ａ内にはマーケティング部門があり、マーケティング部門内にはデータマイニングを用いた購買情報分析を行う部署とマーケティング分析の結果に基づいてメールや手紙等により顧客に情報提供を行う部署の２種類の部署が存在する。

ある従業員はマーケティング業務全般に携わっており、購買情報分析およびメールによる顧客への情報提供の両方の業務に関連する作業を行っている。この従業員はマーケティング全般の目的でのデータベースへのアクセスが認められており、また購買情報分析のためにプライバシー情報を持つデータベースへのアクセス権については公式に認められている。

問題：この従業員がどのデータベースへのアクセスが許可されていると考えられるか。

本例題において問題となるのは、プライバシー情報およびプライバシー情報

を含むとされているデータベースとはどういうものかに関して厳密に定義されていないこと、そしてプライバシー情報へのアクセス権に関する規則が厳密に定義されていないため解釈に幅が生じていることの２点があげられる。

まずプライバシー情報とデータベースとの関係に関しては、本例題ではメールアドレスのデータベースがプライバシー情報の含まれるデータベースかどうかが記述されていないことがあげられる。一般的にはメールアドレスはプライバシー情報と考えられているため、メールアドレスのデータベースはプライバシー情報を含むデータベースであると推定されると思われるが、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」においては、メールアドレスのみから構成されるデータベースは個人情報とはならないとする見解が示されている[16]。ただし経済産業省のガイドラインにおいても他の情報を用いて容易に個人が特定できる場合はメールアドレスのデータベースであっても個人情報となるため、一概にメールアドレスが個人情報でないとは言い切れない。さらにプライバシー情報と個人情報は異なるものと解釈することも可能であり[17][18]、プライバシー情報保護のための内部規定と個人情報保護に関するガイドラインとの関係が不明確であるため、アクセス権による保護対象であるかないかについて解釈の余地があると思われる。

つぎにプライバシー情報へのアクセス権に関する規則に関しては、プライバシー情報を含むアクセス権において、アクセス許可およびアクセス禁止のどちらともいえないケースの場合、規程をどのように解釈しアクセスの可否を決定する指針が述べられていないことが問題となる。本例題においてデータベースへのアクセスを求めている従業員はマーケティング全般に関わっているため実務上禁止されていなければアクセスを許可しても良いとも考えられるが、情報セキュリティの観点から見れば明示的なアクセス許可がなければ拒否すべきであると考えることもできる。こうしたセキュリティを強化するとユーザへの利便性が低下し業務効率の低下が起き、ユーザへの利便性に配慮するとセキュリティリスクが増大するという問題は情報セキュリティの運用上多く見られる問題であるが、具体的な問題に関してセキュリティと利便性とのバランスをどのようにとっていくかは多くの場合担当者の判断にまかされていると考えられる。このことから、こうした問題に関する解釈の多様性を認識しておくことはリスク管理の観点から非常に重要なことであると考えられる。

3．3　解集合プログラミングを用いた内部規定の記述と解釈の発見例

本節では、3.1節の知識表現フレームワークを基づき3.2節の例題にある規程等がどのように記述することが可能かを示す。まず組織が満たすべき一貫性制約Ｇとして与えられるものとして、アクセス可能であることとプライバシー情報にアクセスする許可が禁止されているということが同時に起こらないという一般的な制約を与えるものとする。この制約は以下のように記述できる。

```
:- can_access (A, D, P), -privacy_permission (A, D, P).
```

上記の一貫性制約は、「あるエージェントＡがある目的Ｐを持ってデータベースＤにアクセスするためには個人情報アクセスの許可が無ければアクセスできない」ことを表している。

次にコンプライアンスに関する知識Ｒとして、アクセス可能かどうかを表す述語 can_access/3について記述を示す。

```
can_access (A, D, P) : -database (D), permitted_purpose (A, D, X),
  descendant_purpose (P, X), not -can_access (A, D, P).
-can_access (A, D, P) : -database (D), has_privacy_info (D),
  ancestor_or_descendant_purpose (P, X), -privacy_permission (A, D, X).
```

最初の節では、データベースへのアクセスを許可された目的の下位概念に属する目的であればアクセスを許可することを表している。次の節はアクセスが禁止されている場合について記述しており、データベースＤがプライバシー情報を持ちかつエージェントＡがプライバシーに関する許可を出せない目的を含む可能性のある目的Ｐ（より具体的には、目的Ｐの上位概念または下位概念に

プライバシーに関する許可が出せないことが明示されている目的が存在する）ならばアクセスを禁止することを表している。

3.1節の例題に関する事実の集合Ｆは、下記のように表現することができる。

person (agent_a).

purpose (marketing). purpose (analysis). purpose (advertise).

isa_purpose (analysis,marketing). isa_purpose (advertise,marketing).

has_privacy_info (billig_db).

permitted_purpose (agent_a,D,marketing) : - database (D).

privacy_permission (agent_a, D, analysis) : - database (D).
-privacy_permission (agent_a, D, advertise) : - database (D).

ここで agent_a は問題となっている従業員を表す記号で、最初の節において従業員は人間であることを表している。次の５つの節はアクセスする目的に関する定義である。まず目的（purpose）には３種類あることを定義し、それぞれマーケティング全般（marketing）、マーケティング分析業務（analysis）、メール配信などの広告業務（advertise）であることを表している。次にマーケティング分析業務と広告業務はマーケティング全般の業務の下位概念であることを isa_purpose/2 という述語を用いて表現している。

has_privasy_info/1 はプライバシー情報を持っているデータベースを定義し、購買情報データベースはプライバシー情報を持つことを表している。最後の２節は、従業員がマーケット分析に関する目的であればデータベースへのアクセスは許可され、広告業務に関する目的ではアクセス許可を得ることができないことを表している。

最後に従業員の解釈バイアスの例として、以下の５種類を考える。

B_1 : {has_privacy_info (D) : - database (D), not -has_privacy_info (D).}

B_2 : {-has_privacy_info (D) : - database (D), not has_privacy_info (D).}

B_3 : {privacy_permission (A, D, P) : - database (D), person (A), purpose (P),
not -privacy_permission (A, D, P).}

B_4 : {-privacy_permission (A, D, P) : - database (D), person (A), purpose (P),
not privacy_permission (A, D, P).}

B_5 : {privacy_permission (A, D, P) : - database (D), person (A),
permitted_purpose (A, D, P).}

解釈バイアス B_1 と B_2 はデータベースがプライバシー情報を含むかどうかに関する決定する際に用いられる解釈バイアスである。B_1 はプライバシー情報を含まないと明示されていなければプライバシー情報を含むとする解釈であり、B_2 はプライバシー情報を含むと明示されていなければプライバシー情報を含まないと考える解釈である。

B_3, B_4 および B_5 はプライバシー情報へのアクセスが許可されているかどうかを決定する際に用いられる解釈バイアスである。解釈バイアス B_3 はプライバシーに関する許可を受けていないと明示されていなければプライバシー情報へのアクセスを許可することを表し、B_4 はプライバシーに関する許可を受けていると明示されていなければアクセスを禁止することを表す．最後の解釈バイアス B_5 は、データベースへのアクセスを許可された目的であればプライバシー情報へのアクセスも許可されているという解釈である。この解釈はプライバシー情報へのアクセスの問題をデータベースへの許可された目的でのアクセスの問

題へと還元して考えていることを表している。

以下では上記のセキュリティ規程を記述した知識ベースおよび知識バイアスを用いてどのようなアクセス制限が行われていると解釈できるのかについて述べる。本稿ではすべての解釈バイアスの組み合わせについて述べることはせず、解釈バイアスの導入による解釈の際の特徴的なケースについてのみ説明することとする。

まずはじめに解釈バイアスを用いない場合（つまり$\Delta=\phi$）を考える。このときG, RおよびFのみを用いて解釈を行うが、このG∪R∪Fに関しては解集合モデルが存在しない、つまり無矛盾となる解釈ができない。これはマーケティング全般でのデータベースへのアクセスが認められているにもかかわらず広告業務におけるプライバシー情報へのアクセスは禁止されていることにより、一貫性制約Gと矛盾するからである。このケースは、企業内部でのアクセス制御と顧客のプライバシー情報へのアクセス可否の情報とが互いに対立することにより矛盾無く判断を下すことが不可能となるケースが存在することを示していると考えられる。

次にB_1のみを解釈バイアスとして用いたケースを考える。このときプライバシー情報を持たないと明示されていない場合はすべてプライバシー情報を含むデータベースと判断されるため、メールアドレスのデータベースはプライバシー情報を含むという解釈が可能となる。そのため$\Delta=B_1$の場合、マーケティング分析目的でのメールアドレスデータベースおよび購買情報データベースへのアクセスは許可されるが、広告業務でのデータベースは、両方のデータベースにおいても禁止されることになる。またB_2のみを解釈バイアスとして用いたケースではプライバシー情報を含むと明示されない限りデータベースはプライバシー情報を含まないと解釈されるため、$\Delta=\phi$のケースと同じ矛盾が生じる。このためB_2を解釈バイアスとして持つ場合、データベースへのアクセス可否についての判断は不可能ということになる。

B_1の解釈バイアスを用いることでデータベースへのアクセス許可における解釈が存在することがわかったため、次にB_1へプライバシー情報へのアクセス許可に関する解釈バイアスを追加することにより解釈がどのように変化するかについて見ていくことにする。まずB_1とB_3を組み合わせた場合（$\Delta=B_1\cup B_3$）では、$\Delta=B_1$の場合と同様にマーケティング分析目的でのメールアドレスデータベースおよび購買情報データベースへのアクセスは許可されるが、広告業務でのデータベースは、両方のデータベースにおいても禁止される。データベースへのアクセス可否の判断について$\Delta=B_1\cup B_1$と$\Delta=B_1$の間で差異はないが、$\Delta=B_1\cup B_3$の場合はプライバシー情報へのアクセスが明示的に許可されていると解釈されるため、さらなる解釈バイアスの追加によりデータベースへのアクセス許可の判断が覆る可能性は少なくなっている。

次に$\Delta=B_1\cup B_4$となるケースでは$\Delta=B_1$とは異なり、いかなるデータベースへのアクセスも不可と判断される。これはB_4が明示的にプライバシー情報へのアクセス許可があるとされないかぎりプライバシー情報へのアクセスは禁止されるという強い仮定であり、この仮定を導入することでマーケティング全般の業務におけるプライバシー情報へのアクセスは禁止されているという、通常は予期しない結論が導きだされるためである。B_4は基本的にプライバシー情報へのアクセスは許可しないという解釈であるため、フェイルセーフの観点から言えば好ましい解釈であるように思われるが、このようなセキュリティ強化のみを重視した仮定の元では業務上問題が生じる可能性があることがわかる。

$\Delta=B_1\cup B_4$という解釈バイアスは強すぎる仮定であるため、Δへ新たな解釈バイアスB_5を追加する。$\Delta=B_1\cup B_4\cup B_5$という解釈バイアスの元での解集合モデルでは、従業員はマーケティング全般の業務目的でのデータベースアクセスが認められているため、再度（マーケティング全般の下位概念である）マーケティング分析目的でのデータベースアクセスが許可されることになる。$\Delta=B_1\cup B_4\cup B_5$と$\Delta=B_1$の相違点としては、$B_4$により基本的にプライバシー情報へのアクセスは禁止されるため、事実に関する情報Fが追加されたとしてもプライバシー情報を含むデータベースへのアクセスは明示的に許可されない限り禁止される点があげられる。このため解釈バイアス$B_1\cup B_4\cup B_5$はB_1のみより好ましい仮定であると言うことができる。

4 おわりに

本論文では、個人情報保護等に代表されるコンプライアンスを適切に行うため内部規程の従業員ごとの解釈の相違がどのように表現できるのかについて考察し、内部規程等の解釈多様性に関する問題に対応した知識表現フレームワークを提案した。また提案したフレームワークを用いて実際にデータベースアクセスに関するセキュリティ規程を記述し、従業員等が持つ可能性のある内部規程の解釈に関するバイアスにより内部規程のみでは把握できない様々な解釈の可能性が存在することを示した。

今後の課題としては、本論文において提案した知識表現を用いてセキュリティポリシー等に関する多様な解釈がコンプライアンスにどのような影響を及ぼすかについて分析を行うことがあげられる。具体的には本研究で提案した知識表現フレームワークを用いて推論を行い、企業等のコンプライアンスに対する取り組みに対し解釈バイアスによる解釈の多様性がどのような影響を及ぼすかについてシミュレーションを行うことが必要であると思われる。シミュレーションを行うためには、業務内容の授受、指示を遂行するための手段に関する推論、コンプライアンス規程を用いて指示の検証を行う仕組みやコンプライアンス違反が起きる可能性がある場合のネゴシエーション等のエージェント間のコミュニケーションが必要になると考えられる。

本研究の一部は平成18年度日本学術振興会科学研究費補助金若手研究(B)(コンプライアンスシミュレーションシステムの開発、課題番号18700159)の補助を受けて行われたものである。

参考文献

[1] 情報セキュリティ検討会，情報セキィリティ白書2007年版，2007
[2] 大阪地判平成18年５月19日
[3] 堀部政男監修，鈴木正朝著，個人情報保護法とコンプライアンス・プログラム，商事法務，2004
[4] 田中宏司，コンプライアンス経営（新版），生産性出版，2005
[5] 金井貴，個人情報保護法に基づくコンプライアンスに関する IT 支援の動向と今後の課題，明治学院大学法科大学院ローレビュー第２巻第５号，pp. 83-93，2006
[6] プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告，1980
[7] Rakesh Agrawal et. al., Hippocratic Databases, Proceedings of the 28th International Conference on Very Large Databases, 2002
[8] ji-Won Byun et al., Purpose Based Access Control of Complex Data for Privacy Protection, pp. 102-110, SACMAT'05, 2005
[9] Fabiola Lopez y Lopez, Michael Luck and Mark d'Inverno, Constraining Autonomy through Norms, Proceedings of AAAMAS, pp. 674-681, 2002
[10] Fabiola Lopez y Lopez, Michael Luck and Mark d'Inverno, Normative Agent Reasoning in Dynamic Societies, Proceedings of AAMAS, pp. 730-737, 2004
[11] Carey Heckman and Alex Roetter, Designing Government Agents for Constitutional Compliance, pp. 299-305, Proceedings of Autonomous Agents, 1999
[12] 金井貴，コンプライアンスに関する知識ベースにおける解釈の多様性表現のための一手法，情報処理学会 第70回全国大会，pp. 2-7 - 2-8，2007
[13] Vassilios S. Verykios et al., State-of-the -art in Privacy Preserving Data Mining, pp. 50-57, SIGMOD Record, Vol. 33, No.1, 2004
[14] Yucel Saygin and Vassilios S. Verykios and Ahmed K. Elmagarmid, Privacy Preserving Association Rule Mining, Proceedings of the 12th International Workshop on Research Issues in Data Engineering, pp.151-158, 2002
[15] Rakesh Agrawal and Ramakrishnan Srikant, Privacy-Preserving Data Mining, Proceedings of the ACM SIGMOD Conference on Management of Data, pp. 439-450, 2000
[16] 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（告示)、経済産業省、平成16年10月22日、平成19年３月30日見直し
[17] 園部逸夫編集，個人情報保護法の解説 改訂版，ぎょうせい，2005
[18] 岡村久道著，個人情報保護法，商事法務，2004