2C2-2

複数論点交渉問題における スケーラブルでセキュアな交渉手法の提案

A Preliminary Result on Secure and Scalable Protocols for Multiple Issue Negotiation Problems

藤田 桂英*1　伊藤 孝行*1　マーク クライン*2
Katsuhide Fujita　Takayuki Ito　Mark Klein

*1名古屋工業大学大学院　産業戦略工学専攻
Techno-Business Administration, Nagoya Institute of Technology

*2マサチューセッツ工科大学　スローン経営大学院
Sloan School of Management, Massachusetts Institute of Technology

Multi-issue negotiation protocols represent a promising field since most negotiation problems in the real world involve multiple issues. Our work focuses on negotiation with multiple interdependent issues, in which agent utility functions are nonlinear. The existing works have not yet concerned about agents' private information. Such private information should be hidden for the others in the negotiation. In this paper, we propose "Negotiation Protocol using Distributed Mediator" and "Take it or leave it Protocol". These protocols can make agreement with agents' private information hidden. Moreover, we propose "Hybrid Secure Negotiation Protocol" that is combined "Negotiation Protocol using Distributed Mediator" and "Take it or leave it Protocol". Hybrid Secure Negotiation Protocol can make agreements with using less memory with agent's utility information hidden.

1. はじめに

マルチエージェント研究分野において複数論点交渉問題が重要な研究課題となってきている．既存の研究では論点の独立性が仮定することで，エージェントの効用を線形の効用関数として表現せざるえなかった．実世界の問題では複数の論点が全て独立していることは稀であり，複数の論点が相互依存関係にある場合が多い．そこで筆者らは，複数の論点が相互依存関係にある複雑な交渉問題に注目している ([Ito 07],[Fujita 08])．

また，既存の研究においてエージェントのプライバシー情報の公開については議論されていなかった．例えば，あるエージェントの効用情報が他のエージェントに知られた場合，以降の交渉で不利な状況となり，本来得られるはずの効用が減少してしまう．以上から本論文は自分の効用情報をメディエータをはじめとした他者に知られることなく，最適性の高い解を求めることを目的としている．

本問題に対する手法として，オークションに基づく交渉プロトコル [Ito 07] が提案されている．しかし，オークションに基づく交渉プロトコルは全ての効用情報を公開することなく合意形成が可能だがエージェント数の増加に伴い計算量が増大するという問題があった．そこで筆者らは代表者選択に基づく交渉手法 [Fujita 08] を提案した．代表者選択に基づく交渉手法はエージェント数に対してスケーラブルでありエージェントの効用情報の公開を最低限に抑えられる．しかし，既存の手法を用いた場合，何らかの効用情報をメディエータ等に公開する必要があり，エージェントの効用情報を他者に完全に隠すことは不可能であった．さらに，効用空間の複雑さに対するスケーラビリティ性が低い．以上から，メディエータを含めた他者にエージェント効用情報を全く知られることなく合意形成が可能な新たな交渉プロトコルを提案する必要がある．

本論文では各エージェントの効用値を他者に全く知られることなく交渉を行う**分散メディエータに基づく交渉手法**と **Take it or Leave it (TOL) 交渉プロトコル**を提案する．分散メディエータに基づく交渉手法はメディエータを分散させ，マルチパーティプロトコル [Lindell 03] を利用して個々の効用値を明かすことなく，効用値の和を求めながら合意形成を行う手法をである．本手法は効用空間を各メディエータに分散させ並列に探索させることで計算時間の削減と効用空間の複雑さに関するスケーラビリティの向上を実現する．また， TOL は次状態のへ変化を受け入れるかどうかのエージェントの返答を基にして，状態を更新しながら合意形成を行う手法である．

さらに，本論文で提案する分散メディエータに基づく交渉手法と TOL を組み合わせて**ハイブリッド型セキュア交渉プロトコル**を提案する．ハイブリッド型セキュア交渉プロトコルは最初に TOL を用いてある程度最適性の高い解にしておいてから，さらに分散メディエータに基づく交渉手法で局所的最適解を保証する手法である．ハイブリッド型セキュア交渉プロトコルは分散メディエータに基づく交渉手法で最大の問題であったメモリ量の増大を軽減しながら，最適性の高い合意案が得られる．本論文ではハイブリッド型セキュア交渉プロトコルについてシミュレーション実験を行い，様々な探索手法を組み合わせた場合の最適率とメモリ量の比較を行う．

本論文の構成を以下に示す．まず，2. では本論文で扱う交渉問題の定式化と各エージェントがもつ非線形の効用空間について述べる．次に，3. では分散メディエータに基づく交渉手法と Take it or leave it 交渉プロトコルを提案する．さらに，4. ではハイブリッド型セキュア交渉手法を提案し，有効性について述べる．最後に，5. においてシミュレーション実験をもとに提案する手法の評価を行い，6. に本論文のまとめを示す．

連絡先: 藤田 桂英，名古屋工業大学産業戦略工学専攻，愛知県名古屋市昭和区御器所町，fujita@itolab.mta.nitech.ac.jp

2. 非線形効用関数に基づく交渉

本論文では，N 個のエージェントが合意形成を試みる交渉の状況を考える．論点が M 個存在し，個々の論点を $i_j \in I$ と表す．論点 i_j は $[0, X]$ の範囲の整数を値として持つ（$1 \leq j \leq M$）．交渉の結果得られる合意案は，各論点の値のベクトル $\vec{s} = (s_1, ..., s_M)$ として表現される．

エージェントの効用関数は制約を用いて表現する．l 個の制約が存在するとし，個々の制約は $c_k \in C$ と表す．制約は，単一，もしくは複数の次元（論点）に関して，制約充足条件となる値の範囲，および効用値を持つ．制約 c_k は，合意 $\vec{s}$ によって充足される場合にのみ，$w_i(c_k, \vec{s})$ を効用値として持つことができる（$1 \leq k \leq l$）．交渉に参加する全てのエージェントは，全く共有されていない独自の制約集合を持つ．

合意 $\vec{s}$ に関するエージェント i の効用を $u_i(\vec{s}) = \sum_{c_k \in C, \vec{s} \in x(c_k)} w_i(c_k, \vec{s})$ と定義する．$x(c_k)$ は，制約 c_k を充足可能な合意案の集合である．この効用表現により，凹凸のある非線形の効用空間が形成される．ここで，本論文における効用空間とは，各論点が取り得る値のあらゆる組合せについて，効用関数によって得られる効用値を空間状にプロットして得られるグラフを意味し，空間の次元数は，論点数+1 となる．この効用空間では，より多くの制約を充足可能な地点は効用が高くなり，逆に充足する制約数が少ない地点では，効用が低くなるため，空間内に効用値による高低が生じる．

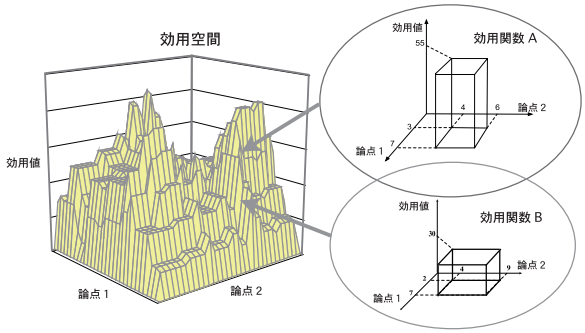

図 1: 非線形効用関数と効用空間の例

図 1 に，非線形の効用関数と効用空間の例を示す．図の効用関数 A と効用関数 B は，論点 1，および論点 2 に関連する二項制約の例を図示したものである．効用関数 A では，論点 1 に関しては $[3, 7]$，論点 2 に関しては $[4, 6]$ の範囲で合意が得られた場合に制約が充足可能であり，その場合の得られる効用は 55 であることを示している．図が示す通り，効用空間は各論点の取りうる値の全組み合わせを網羅した状態空間に，各エージェントが持つ全効用関数をプロットして得られるグラフである．実際の問題における非線形の効用空間は図が示す以上に山と谷が入り組んだ複雑な効用空間を想定している．

線形の効用関数を前提とする既存のプロトコルでは，合意案の効用は個々の論点に関する効用の加重和であるため，平坦な超平面上での単一最適化により，良質の合意（解）を得ることができる．しかし，効用空間に不規則な凹凸がある非線形の効用空間では，既存のプロトコルを適用して，良い解を得ることは難しい．従って，本論文では，エージェントは合意案の効用を正確に評価するための完全な知識（効用関数）は持っているが，最適な合意案を事前に把握することが困難であることが前提となる．本論文で提案する交渉プロトコルの目的関数は，

$$\underset{\vec{s}}{\operatorname{argmax}} \sum_{i \in Ag} u_i(\vec{s})$$

と表現できる．Ag はエージェントの集合を表す（$|Ag| = N$）．提案プロトコルは社会的効用，すなわち全てのエージェントの効用の総和を最大化する合意の発見を試みる．

本論文では全エージェントがすべての効用情報を公開して，非線形最適化手法を利用する手法を採用しない．本問題におけるエージェントは実世界におけるユーザの代行者として交渉を行う主体として考える．交渉の場で，効用に関する情報の公開は，実世界のユーザにとって好ましくない．例えば，エージェント A とメディエータが共謀しており，エージェント B の効用情報をエージェント A に漏洩したとする．すると，効用情報が漏洩してしまったエージェント B は以降の交渉で極端に不利な状況となり，エージェント B の本来得られるはずの効用が減少してしまう．さらに，セキュリティの面からみても効用情報を全て公開することは危険である．以上から，本論文では交渉プロトコルの目的関数を達成するとともにメディエータ（中間者）も含めた他者に全く効用情報を知られないことを重要な条件の一つとしている．

3. セキュアな交渉プロトコルの提案

3.1 分散メディエータに基づいた交渉手法

分散メディエータに基づいた交渉手法では，通常交渉では単一の存在であったメディエータを分散させる（**分散メディエータ**）．最適解の探索は山登り法に代表される反復改良探索アルゴリズム [Russell 02] 用いてを行う．さらに，マルチパーティプロトコル [Lindell 03] を分散メディエータに導入する．マルチパーティプロトコルを導入することでメディエータに各エージェントの効用情報を知られることなく合意形成が可能である．

n 個のメディエータ $(M_0, \ldots, M_j, \ldots, M_n)$ が存在し，任意の k 個以上のメディエータが集まると効用値の和が分かる場合を想定する．あらかじめマルチパーティプロトコルに必要な素数 q は共有してある．また，m 個のエージェント $(Ag_0, \ldots, Ag_i, \ldots, Ag_m)$ が存在する．

(1) まず，n 個のメディエータは探索空間を分割し，決められた空間の探索を行う．各メディエータが分割して探索を行うことで，並列処理が可能であり，計算時間を削減可能である．

(2) 各メディエータは探索を行う．もしメディエータが初めての状態を探索する場合，全メディエータのうち k 個のメディエータを選択し，全エージェントに v(シェア) の作成を行うように依頼を出す．その後，エージェント i は $f_i(0) = x_i$ をみたす高々k 次の多項式 f_i をランダムに選び，$v_{i,j} = f_i(j)$ を計算し $v_{i,j}$ を M_j へ秘密で送信する．

(3) M_j は全エージェントから $v_{1,j}, \ldots, v_{m,j}$ を受け取り，$v_j = v_{1,j} + \cdots + v_{n,j} \ mod\ q$ を計算する．その後，他のメディエータに v_j 公開する．

(4) 全ての v_j から $f(j) = v_j$ を満たす高々k 次の多項式をラグランジュの補完法を用いて求める．最終的に $f(0) = s$ が全エージェントの効用値の和となる．

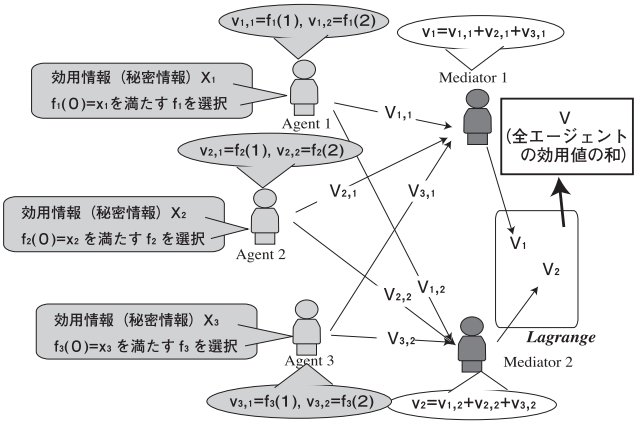

図 2: 分散メディエータに基づく交渉プロトコル

図 2 はエージェント数 3，メディエータ数 2，k=n と設定した場合の分散メディエータに基づく交渉プロトコルの一連の流れを示したものである．灰色部分はエージェントが非公開で行うステップを示す．図が示すように，分散メディエータに基づく交渉手法は多項式の選択，シェアの作成，シェアの和の計算，そして，ラグランジュの補間法という一連の流れを実行することで他者に各エージェントの効用情報を知られることなく全エージェントの和を求めることができる．

以上の (1)〜(4) のステップを探索が終了するまで繰り返し，割り当てられた空間の探索を終えたメディエータは割り振られた部分での最大値（合意案候補）を報告する．最終的に全メディエータの報告された合意案候補の中での最大値を合意点とする．以下に提案した手法の特徴を挙げる．

[セキュリティ面]　本プロトコルでは探索の際に必要なある状態における全エージェントの効用値の和をメディエータを含めた他者に知られることなく求められる．本手法が全エージェントの効用値の和を他者に知られることなく正しく求められている証明はマルチパーティプロトコル [Lindell 03] の場合と同様である．また，マルチパーティプロトコルにおいて一定数以上の参加者が不正に結託しない限りは，個人の秘密情報を解析できないことが保証されている．

本プロトコルにおいてマルチパーティプロトコルを行うメディエータの人数 k は，セキュリティの安全性と計算時間のトレードオフとなる．本プロトコルにおいてもし k 個のメディエータが共謀して各エージェントから集められたシェア v を交換し合うと各エージェントの効用値が暴かれてしまう．そのため，k の値を大きくし，メディエータ同士が共謀するのが非現実である数値にする方がセキュリティの安全性の面からみると望ましい．しかし，k が多くなるにつれて，探索を停止するメディエータが多くなり計算時間がかかる．

[スケーラビリティの面]　メディエータを分散させ，探索空間を分割させることで大きく計算時間を削減することができる．さらに，効用空間の複雑度が増した場合，計算量が莫大になり現実時間で求解不可能になる場合がある．しかし，本プロトコルでは探索空間を分割して行うため，大幅に効用空間の複雑度に対するスケーラビリティが向上する．

本プロトコルは探索した状態全てに対してシェアを作成するため，メモリ量を多く必要とするという欠点がある．また，通常の探索以上に多くの操作を必要とするため出来る限りシェアの作成を行うべきではない．以上から分散メディエータに基づいた交渉手法は出来る限りシェアを作成することなく最適性の高い解を求める必要がある．

3.2　Take it or Leave it (TOL) 交渉プロトコル

メディエータに各エージェントの効用値を知られることなく最適性の高い解を求めるもう一つの手法として TOL を提案する．本プロトコルでは，評価関数の値が増える方向に連続的に動くことを繰り返す山登り法 [Russell 02] を基に探索を行う．ただし，メディエータにエージェントの効用値を知られないために，評価関数はエージェントが現状態から次状態への変化を受け入れるかどうかの返答を基に決められる．以下に TOL のステップを示す．

(1) ランダムに初期探索地点を決定する．
(2) メディエータは各エージェントに，現在の状態と近傍の状態を比較して状態の更新を行いたいかの問いかけを行う．
(3) 各エージェントは現在の状態と問われた近傍状態の効用値を比較し，近傍状態の方が効用値が高ければ “take it” を低ければ “leave it” と返答する．
(4) メディエータは近傍状態のうち “take it” と答えたエージェント数が最大の状態へと進む．ただし，“take it” と答えたエージェント数が最大の状態が多数存在する場合はランダムで選択を行う．このようなランダム選択により山登り法の欠点の一つである局所的最大に陥ることを防ぐ．

(1)〜(4) の操作を，全エージェントが “leave it” と返答するか，“take it” と答えるエージェント数に変化がない高原に陥ったと判断した場合に合意を生成する．

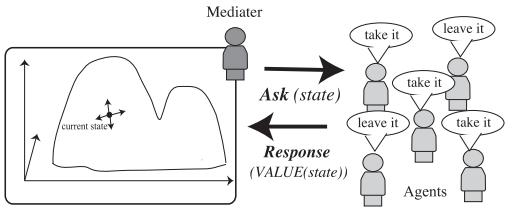

図 3: Take It or Leave it 交渉プロトコル

図 3 は TOL の概念を示している．メディエータは評価関数を知りたい状態 ($state$) をエージェントに送信する．その後，エージェントは自分の効用空間を調べ，state の状態の方が現在状態より好ましい判断すれば “take it” 現在状態に留まりたければ “leave it” を宣言し，“take it” と返答したエージェント数を送信する ($VALUE(state)$)．以上の操作を山登り法を行いながら終了条件まで続ける．

本プロトコルの長所として，探索の際の評価関数が単純であるためエージェント数が増加しても非常に高速であることが挙げられる．ただし，エージェント数が少ない場合，すぐに高原に陥ってしまい高い最適性を期待できないという問題がある．

4.　ハイブリッド型セキュア交渉プロトコル

前章で提案した分散メディエータに基づいた交渉手法と TOL はそれぞれシェア作成によるメモリ量と最適性において欠点があった．本章では前章で提案した 2 手法を順に用いて探索を行う新たな手法を提案する．本論文では本章において提案する手法をハイブリッド型セキュア交渉プロトコルと呼ぶ．以下にハイブリッド型セキュア交渉プロトコルを示す．

(1) 複数のメディエータに対して探索空間を分割し，各メディエータに割り当てる．
(2) 各メディエータは与えられた探索範囲に対してランダムに決められた値を初期値として，3.2 において提案した TOL を用いて交渉を行う．TOL を用いることで，シェアを作成せず，ある程度の最適性を持った解を求められる．
(3) TOL で求めた解を初期値として，3.1 において提案した，分散メディエータに基づく交渉手法を用いて交渉を行う．分散メディエータに基づく交渉手法により，他のエージェントやメディエータに効用情報を知られずに局所最適解を保証できる．
(1)〜(3) 操作を初期地点をランダムに変えながら繰り返し行う．

本章で提案しているハイブリッド型セキュア交渉プロトコルは分散メディエータに基づく交渉手法と比較して少ないメモリ量で高い最適性が期待できる．本プロトコルは，TOL を最初に実行することで，分散メディエータに基づく交渉プロトコルにおける探索初期値を高い値になる．また，TOL はシェアをを全く作成しない．さらに，分散メディエータを用いる探索手法が山登り法などの場合，性質上 TOL で探索した状態を再探索することはない．以上から，初めに TOL 交渉手法を実行することでメモリ量が減らせる．一方，最適性においても TOL は高原と判断され終了することが多い．その結果，分散メディエータに基づく交渉プロトコルで探索する際に最適性を下げる

原因であった局所的最大に陥ることを，分散メディエータの初期値が異なる地点から探索することで防ぐことができる．

5. 実験結果

5.1 実験設定

本実験では，ランダムに生成された効用関数をもつエージェント間の交渉を 100 回試行し平均値を取る．全エージェント数は 6 である．また，分散メディエータにおける交渉手法における全メディエータ数は $2^{(\text{論点数})}$ でそのうち 4 メディエータ集まると全エージェントの効用値の和が求められる．

[効用関数の設定] 論点の値域は [0,9] で，制約数は 10(単項制約)，5(単項制約を除く各次元) である．制約の最大効用は 100 *(論点数) で，制約の最大範囲は 7 である．

[シミュレーテッドアニーリング (SA) の設定] 分散メディエータに基づく交渉手法では SA[Russell 02] の初期の温度を 10 度として，500 回の繰り返し処理を経て温度を 0 まで下げることとする．一方，ハイブリッド型セキュア交渉プロトコルは初期の温度を 5 とし，処理を 50 回繰り返す．ハイブリッド型セキュア交渉プロトコルにおける SA の目的は TOL で最適性を高くした値を初期値として局所的最適解を保証させることである．そのため，探索範囲が拡大しすぎないように初期の温度設定を低めにし，処理回数も少なく抑えてある．

実験は JAVA2(1.5) で記述し，Mac OS 10.5 が動作している iMac (Core2Duo 2.33GHz メモリ 1.5GB) で行った．

5.2 実験結果

図 4 と図 5 は本論文で提案した複数の手法を比較した実験結果を示す．“(A) 分散メディエータ (SA)” は分散メディエータに基づく交渉手法を行った場合に探索手法としてシミュレーテッドアニーリング (SA) を適用させた手法を示す．同様に “(B) 分散メディエータ (HC)” は分散メディエータに基づく交渉手法を行った場合に探索手法として山登り法 (HC) を用いた手法を示す．“(C) ハイブリッド型 SA” は分散メディエータに基づく交渉手法を行うステップにおいて探索手法として SA を適用させた手法を示す．“(D) ハイブリッド型 HC” は分散メディエータに基づく交渉手法を行うステップにおいて探索手法として HC を適用させた手法を示す．“(E)TOL” は TOL のみを用いた手法を示す．

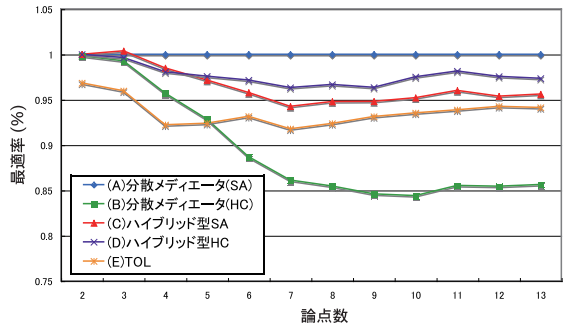

図 4: 最適率の比較

図 4 は “分散メディエータ (SA)” を基準とした場合の解の最適性の比較を行っている．(B) は論点数の増加に従って急激に減少している．(B) の減少の理由としては論点数の増加にともない効用空間の広さが急激に増加するため，山登り法の欠点である局所的最大に陥る可能性が増加するからである．分散メディエータを用いた手法における最適率は探索手法に大きく依存することになる．(E) は論点数全体において最適率は高くないが大きく減少することのない安定する数値となっている．この安定する理由は多くのエージェントが受け入れる状態を目指し，全エージェントが共通して高い部分で合意を生成するため安定的な値を得られる．一方，(C) や (D) は (E) に比べて最適率が高い値を示しており，特に (D) は (C) よりも高い最適率となっている．(D) の最適率が高くなる理由は (C) は SA の性質上，まれに TOL によって高くした探索初期値よりも低い値で探索を終了するが (D) は山登り法の性質上，必ず探索初期値より高い値で探索を終了からである．

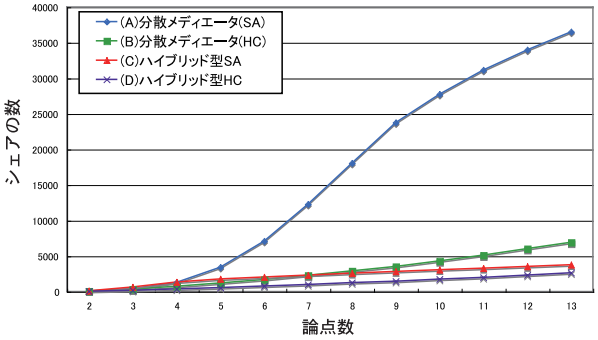

図 5: シェア数の比較

図 5 は交渉の際に各メディエータが平均してシェア (v) をどれだけ作成したかを示している．シェアの数を調べることにより各手法のメディエータのメモリ量を比較することができる．(A) はシェアの数が指数的に急増している．一方 (B) は (A) に比べてシェアの数が大幅に削減されている．分散メディエータにおけるメモリ量の特徴は山登り法と SA の探索手法の特徴に依存する．また，ハイブリッド型を用いた場合，分散メディエータのみを用いた場合に比べてシェアの数が削減されている．この理由は TOL ではシェアを作成せず，分散メディエータによる交渉手法の探索初期値を高い値にできるからである．

以上の二つの実験から，ハイブリッド型は高い最適率を保ちながらシェアの数を減らすことに成功していることが分かる．

6. まとめ

本論文ではメディエータを含めた他者にエージェントの効用情報を知られることなく合意形成を行う，“分散メディエータに基づく交渉手法” と “Take it or leave it 交渉プロトコル” を提案した．分散メディエータに基づく交渉手法はメディエータは各エージェントの効用値を知ることなく合意形成を行うことは可能である．さらに，各メディエータが効用空間を分割して探索を行うため並列処理が可能になり，効用空間の複雑さに対する高いスケーラビリティが発揮できる．また，TOL においてもエージェントの効用情報をメディエータに報告することなく，交渉を行える．さらにハイブリッド型交渉手法を提案し，シミュレーション実験により，使用するメモリ量を減らしながら最適性の高い合意を求めることが可能であることを示した．

参考文献

[Fujita 08] Fujita, K., Ito, T., and Klein, M.: A Preliminary result on a representative-based multi-round protocol for multi-issue negotiations, in *Proc. of AAMAS-2008* (2008)

[Ito 07] Ito, T., Hattori, H., and Klein, M.: Multi-issue Negotiation Protocol for Agents : Exploring Nonlinear Utility Spaces, in *Proc. of IJCAI-2007*, pp. 1347–1352 (2007)

[Lindell 03] Lindell, Y.: *Composition of Secure Multi-Party Protocols: A Comprehensive Study*, Springer (2003)

[Russell 02] Russell, S. J. and Norvig, P.: *Artificial Intelligence : A Modern Approach*, Prentice Hall (2002)