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

2008－IOT－1（15）
2008 / 5 / 9

Privacy Grid: 私的な情報を安全に利用する分散問題解決

小野 智司† 岩川 建彦† 中山 茂†

† 鹿児島大学 工学部 情報工学科
〒890-0065 鹿児島市郡元 1-21-40
E-mail: †{ono,sc100007,shignaka}@ics.kagoshima-u.ac.jp

あらまし 通信履歴，行動履歴・予定，メディアコンテンツ，嗜好情報など，携帯電話などの情報端末に蓄積された私的な情報を安全に用いて，分散問題解決方式「プライバシ・グリッド」を提案する．本モデルは，利用者の私的な情報を情報端末外に送信しないため，情報漏洩の危険性が低く，利用者の安心感も高い．提案するプライバシ・グリッドをミドルウェアとして実装することで，私的な行動予定を考慮したスケジューリング，操作履歴に基づくユーザインタフェースの最適化など，利便性と安全性を両立した様々なシステムの実用化に寄与することができる．
キーワード プライバシグリッド，分散問題解決，最適化，遺伝的アルゴリズム，携帯電話

Privacy Grid: Distributed Problem Solving with Safe Use of Private Information

Satoshi ONO†, Takehiko IWAKAWA†, and Shigeru NAKAYAMA†

† Department of Information and Computer Science, Faculty of Engineering, Kagoshima University
1-21-40 Korimoto, Kagoshima, 890-0065 Japan
E-mail: †{ono,sc100007,shignaka}@ics.kagoshima-u.ac.jp

Abstract This paper proposes a model "Privacy grid" for distributed problem solving with the safe use of private information like communication history, action history and plans, and users' favorite contents stored on hte users mobile phones. The proposed model prevents leaks of private information and makes users feel secure because the model does not send private information outside of mobile phones. The porposed Privacy Grid can be implemented as a middleware, and contributes to develop distributed scheduling with considering private plans, optimization of a user interface based on operation history of a device, and so on.
Key words Privacy grid, distributed problem solving, optimization, genetic algorithm, mobile phone

1. はじめに

近年の携帯電話は，電子メール送受信，Web ページ閲覧などの情報端末としての機能が進化するとともに，電話やメールの送受信履歴，電話帳，ブックマーク，スケジュール，搭載されたカメラで撮影した画像など，ユーザの嗜好や私的な情報をより多く含むようになった．本稿ではこれらの情報をプライバシと呼ぶ．各個人のプライバシを利用した利便性の高いサービスの実現や取り組みが国内外で広く行われている．NTT ドコモは，携帯電話のスケジュールに登録されている予定を利用することで，利用者の行動を推定し，その行動に即した情報を自動的に配信するシステムを開発した．このシステムは，利用者の属性，興味，行動の推定を行うことで利用者の生活全般に関わる情報サポートを実現するものである．また，Google は Web ブラウザ上で動作するメーラ Gmail において，ユーザのメールの内容に応じて広告の表示を行っている．マイクロソフトは，パーソナルコンピュータや携帯電話に蓄積された個人プロファイル，すなわち，興味や趣味，性別，年齢，住所，職業，サービスや団体への加入状況，配偶者や子供の有無などの情報，使用しているソフトウェアやサービスから取得したアドレス帳，カレンダー，メール等の履歴をもとに広告を配信する特許を出願している．

上記の NTT ドコモやマイクロソフトの技術のように，個人のプライバシを利用するサービスは今後ますます普及していくものと考えられる．しかし，上記の技術は 1 人のユーザのプライバシのみを参照するものであり，プライバシを保護したままサービスを提供することは比較的容易である．すなわち，ユーザの情報端末上で広告や情報を選択的に取得するプログラムを

表 1　プライバシを参照する技術，サービスの例

技術名（開発企業名等）	行動支援型レコメンドシステム（NTT ドコモ）	広告配信技術（マイクロソフト）	広告配信技術（Google）	商品提案サービス（Amazon）	プライバシ・グリッド（本研究）
参照するプライバシの量	個人			複数人	
プライバシの保存場所	情報端末		サーバ		情報端末
参照するプライバシの種類	スケジュール	性別，年齢，住所，職業，電話帳，カレンダー，メールなど	メール，Web ページコンテンツ	商品の閲覧履歴，購買履歴	携帯電話等に蓄積された様々なプライバシ

実行することで，ユーザのプライバシを情報端末外部に送信することなくサービスを提供できる．

Amazon などのインターネットショッピングサイトでは，多数のユーザの商品閲覧履歴，購買履歴をもとに，ユーザの嗜好や商品間の関連性を学習し，ユーザに商品の紹介を行うサービスを運用している．複数人の私的な情報を参照することで，各ユーザの私的な情報を利用して学習を行う認証・識別プログラムの自動生成や，各ユーザの嗜好を反映した合意形成システムの実現が期待できる．しかし，複数のユーザのプライバシをもとに問題解決を行う場合，各ユーザの情報端末上で個別にプログラムを実行するだけでは，複数のユーザのプライバシを参照することができず，Amazon のサービスのようにサーバ上にプライバシを集約する必要があった．この場合，通信内容を傍受され，暗号が解析されてしまった場合や，サーバに不正侵入を許してしまうと，ユーザのプライバシが漏洩してしまうという問題があった．また，プライバシ全てをサーバに送信することは，ユーザにとって心理的抵抗が大きい．このため，携帯電話上の情報を安全に利用し，実用的な時間内で組合せ最適化を行う方式の実現が望まれる．

本研究では，プライバシを携帯電話上に保持したまま，それらを利用した分散組合せ最適化を行うプライバシ・グリッドを提案する．プライバシ・グリッドは，複数のユーザのプライバシを携帯端末上に保持したまま問題を解決できる点で独創性が高い．NTT ドコモやマイクロソフトの技術は，各個人の情報端末におけるプライバシを参照してサービスを提供するものである．Google の広告表示技術も同様に，サーバに保存されたプライバシを参照する．これらに対し，プライバシ・グリッドは，複数人の情報端末における私的な情報を参照して問題解決を行う点が異なる．Amazon などの商品提案サービスは，サーバがプライバシを有するプライバシ集約型のシステムであるが，プライバシ・グリッドはプライバシをユーザの情報端末内に保持し，サーバに送信しない点が異なる．プライバシ・グリッドを利用することで，プライバシが漏洩する危険が低まること，およびユーザに安心感を与えることができる．

本論文では，プライバシ・グリッドの一つの実装例として，大規模な組合せ最適化問題で有効な遺伝的アルゴリズム（Genetic Algorithm: GA）を，計算機および複数の携帯電話上で分散実行するモデルを説明する．通常の計算機上で交叉，突然変異などの解候補生成の処理を行い，携帯電話上で解候補の評価を行うことにより，プライバシを解候補評価に安全に利用しつつ，携帯電話上での計算量を最小限に抑えることができる．

以下，2 章では，分散 GA の 2 つのモデル，および携帯電話を用いた従来の分散 GA について述べる．3 章ではまず，提案するプライバシ・グリッドの特徴を述べる．次に，構成，処理手順について述べ，携帯電話のプライバシを用いた解候補の評価方法について述べる．

2. 提案するプライバシ・グリッド

2.1 方針と特徴

本稿では，携帯電話上のプライバシを用いて組合せ最適化を行う方式を提案する．提案する方式の方針および特徴を以下に示す．

方針 1：携帯電話上で解候補の評価を行い，プライバシを携帯電話外に送信しない．各ユーザのプライバシを用いて最適化を行うには，セキュリティを確保した上で，携帯電話上の各ユーザのプライバシをサーバに転送する方法が考えられる．しかしながら，携帯電話に蓄積されるプライバシは，携帯電話の性能が向上するにつれて増加している．蓄積した全てのメールや電話帳などのプライバシをサーバへ送信することは，通信コストが膨大となってしまうだけでなく，近年の個人情報漏洩事件の多発により，心理的に受け入れがたいユーザもおり，現実的ではない．

提案するプライバシ・グリッドでは，プライバシを携帯電話上でのみ利用し，解候補とその評価結果のみを通信する．これにより，各ユーザの嗜好や条件を他人の携帯電話，計算機に送信せずに，全員の嗜好，条件を考慮した解を生成することが可能である．個人情報や嗜好が他の計算機に送信されないことは，携帯電話のユーザに安心感を与える．このため，より率直な嗜好の入力を促すことができ，結果として満足度の高い解を得ることができる．

方針 2：オブジェクト共有空間を用いて通信を行う．プライバシ・グリッドでは，Linda モデル [1] に基づくオブジェクト共有空間を利用した分散並列環境を用いるものとし，JavaSpaces を用いて実装する [2]〜[4]．JavaSpaces を用いることにより，Java が動作可能な計算資源であれば，分散並列処理に容易に参加させることが可能となり，様々な OS を搭載した計算機，携帯情報端末，および携帯電話を利用することができる．また，インターネットなど汎用のネットワークを利用できる，計算資

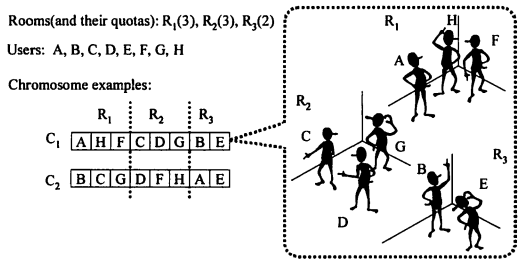

図 1　部屋割問題における染色体表現

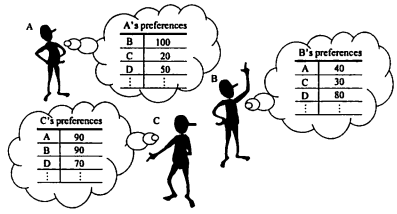

図 2　部屋割問題における嗜好情報

源の動的な参加・離脱にも容易に対応できるなどの特徴を持つため，計算機だけでなく携帯電話を計算資源とする本方式に適している．

方針 3：多点探索型最適化アルゴリズムを用いる． 本方式が対象とする問題は，各ユーザの嗜好を充足する値の集合を求める組合せ最適化問題であり，ユーザ数が増加するとその探索空間は指数関数的に増加する．このため，大規模な探索空間内において効率的に最適解を発見できる探索アルゴリズムが必要となる．また，本研究で構築する分散並列環境では，インターネットおよび携帯電話事業者のネットワークを利用するため通信コストが大きく，小さなデータを頻繁に送受信するよりも大きなデータをより低い頻度で送受信することが望ましい．よって，解候補の生成と評価を頻繁に行う必要がある山登り法 [5], [6]，焼き鈍し法 [7] などの単点探索よりも，遺伝的アルゴリズム（Genetic Algorithm: GA）[8]，Particle Swarm Optimization [9], [10] など，集団内の全解候補を一度に生成，評価できる多点探索アルゴリズム適している．

本章の以下では，実装の一例として，単一集団型の分散遺伝的アルゴリズム [11] を用いた場合をもとに説明を行う [12]．島モデル型分散遺伝的アルゴリズム [13], [14] に基づいた負荷分散や初期収束回避を目的とした柴山らの分散 GA とは異なり，ここで用いる GA は，プライバシを用いた解候補の評価を各携帯電話で行う機能分散型の GA である．

2.2　部屋割問題

提案するプライバシ・グリッドは基本的に汎用であり，組合せ最適化問題，制約充足問題などに適用することが可能である．本章では，説明を容易にするため，以下に示す部屋割問題を用いて本方式の説明を行う．

部屋割問題は，個々人の嗜好を満足するように，人を部屋へと割り当てる問題である．本問題は，人数が増加すると探索空間のサイズが指数関数的に増加し，全員の嗜好を満たす解を発見することが困難になる．

部屋割問題の解は，図 1 に示すような一次元の染色体として表現できる．各遺伝子はユーザ番号を表し，部屋 r の定員を Q_r とすると，部屋 r に割り当てられるユーザは，$\left(1+\sum_{i=1}^{r-1} Q_i\right)$ 番目の遺伝子座から $\left(\sum_{i=1}^{r} Q_i\right)$ 番目にある遺伝子座までに位置する遺伝子となる．これは，巡回セールスマン問題（Traveling Salesman Problem: TSP）[8], [14] と類似の染色体表現であり，部屋割問題においても TSP において用いられる Partially Mapped Crossover（PMX）[8] やサブツアー交換交叉など，致死遺伝子の発生を抑え，ビルディングブロックをなるべく保持する交叉方式を利用することが可能である．

各ユーザの嗜好は，図 2 に示すように，それぞれの人と相部屋になりたい度合い（好悪度）の集合から構成される．

染色体 C_i の適応度 $F(C_i)$ は，以下の式に従って計算する．

$$F(C_i) = \frac{1}{R}\sum_{r=1}^{R}\left\{\frac{1}{Q_r(Q_r-1)}\sum_{j=1}^{Q_r}\sum_{\substack{k=1\\(k\neq j)}}^{Q_r} P_{x_{rj}}(x_{rk})\right\} \quad (1)$$

ここで，R は部屋の総数を，x_{rj} は部屋 r に割り当てられた j 番目の人を，$P_a(b)$ は人 a の人 b に対する好悪度を表す．

2.3　構成と処理手順

本研究で試作したプライバシ・グリッドの実装は，HTTP サーバと JavaSpaces サーバを兼ねた計算機（サーバ），遺伝的操作を行うクライアントプログラム（マスタ）を実行する計算機，および，携帯電話上で解候補の評価を行うクライアントプログラム（ワーカ）からなる．マスタをサーバ上で動作させることや，ワーカをパーソナルコンピュータや携帯情報端末上で動作させることも可能である．携帯電話は JavaSpaces に直接アクセスすることができないため，本方式では，サーバ上のサーブレットを介して携帯電話と JavaSpaces の通信を行う．

本方式の処理手順を図 3 および以下に示す．以下の各項目の番号は，図 3 の番号に対応している．

① マスタにおいて，ランダムに個体を生成し，初期集団とする．

②〜⑤ 各ワーカにおいて，各携帯電話上のプライバシを用いて各個体をを評価する（2.4 節）．

⑥ マスタにおいて，通常の GA と同様に，選択，交叉，突然変異などの遺伝的操作を行い，新しい個体群を作成する．

⑦ ②から⑥の処理を 1 世代とし，閾値以上の適応度を持つ解を発見するか，一定世代数 T_G の間適応度が向上しない場合に探索を終了する．得られた最終解は，オブジェクト共有空間を介して各携帯電話に送信する．上記の終了条件を満たさない場合は②に戻る．

2.4　プライバシを用いた個体の評価

本方式では，各携帯電話上のワーカが染色体の評価を行うが，マスタに，既に一度評価を行った染色体の適応度を記憶させることで，通信コストの削減を図る．マスタが保持する染色体の適応度の記憶領域をキャッシュと呼ぶ．キャッシュへのデータの読み書きは，ハッシュ法を用いて効率化を図る．

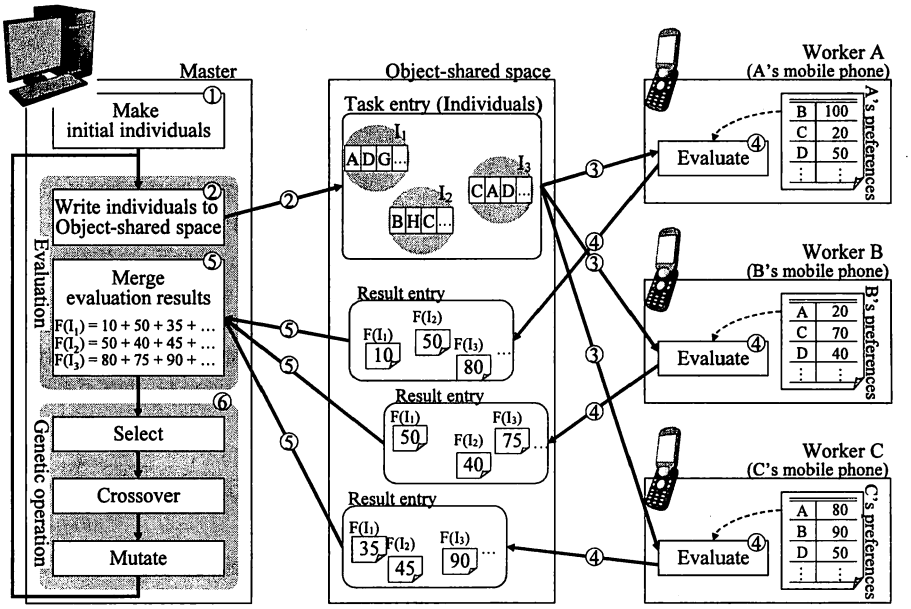

図3 処理手順

本方式における，解候補評価の手順を以下に示す．以下の各項目の番号は，図3の番号に対応している．

② 集団内の各個体に対し，キャッシュ内に登録されていない全ての個体を1つの仕事エントリに格納し，オブジェクト共有空間に書き込む．キャッシュ内に登録されている個体は，キャッシュ内に登録されている適応度を評価結果として用いる．

③ 各ワーカは，オブジェクト共有空間を監視し，個体群の遺伝子情報が書き込まれた場合には，その情報をワーカ内に取り込む．このとき，全てのワーカが同じ個体を取り込む必要があるため，オブジェクト共有空間上に残しておく．

④ ワーカは，携帯電話上に保持されたプライバシを用いて取り込んだ個体群を評価し，その結果を結果エントリとしてオブジェクト共有空間に書き戻す．

⑤ マスタは，ワーカから書き込まれた仕事エントリをオブジェクト共有空間から回収し，各ワーカによる適応度を平均することで各個体の適応度を得る．全てのワーカからの仕事エントリを回収した時点で，仕事エントリをオブジェクト共有空間から削除する．全ての個体とその評価結果をキャッシュに登録する．

なお，個々の結果エントリには，送信元のワーカ（およびワーカを実行している携帯電話）を識別する情報は含まない．また，ワーカと JavaSpaces 間での通信，またはワーカが動作している携帯電話で何らかの問題が発生し，結果エントリが一定の時間を越えても JavaSpaces に書き戻されない場合，マスタ側は得られた結果エントリのみを用いて染色体の評価を行う．

本方式の現段階において，プライバシは，探索実行前にユーザが専用のインタフェースを通じて各自の携帯電話に入力する．これは，EZ アプリの開発用ライブラリ KDDI-P や，i アプリの開発用ライブラリ DoJa3.0 以降など，携帯電話上のプライバシを参照可能な Java ライブラリの利用が，携帯電話事業者に認定された企業などに限られるためである．本方式においても上記のライブラリを利用することで将来的に，電話帳の登録情報，音声通話や電子メールの送受信履歴をもとに解候補の評価を行える．

3. 応用例

提案するプライバシ・グリッドは，複数人のプライバシを参照する最適化問題や組合せ探索問題に広く応用が可能である．以下では，典型的な応用として，分散スケジューリング，メールフィルタ分散学習，ユーザインタフェース分散最適化への応用について述べる．

3.1 分散スケジューリング

提案するプライバシ・グリッドの応用例として，勤務パターンが不規則な労働者のスケジューリングシステムが考えられる（図4）．労働者が，私的なスケジュールを自身の情報端末に入力しておき，ワーカプログラムを実行しておくと，マスタ計算機と各ワーカが分散問題解決を行う．すなわち，マスタ計算機が解候補の生成を行い，ワーカ計算機が私的なスケジュールをもとに送信された解候補の評価を行う．評価結果をもとに，マスタ計算機は勤務シフト案を修正し，上記の処理を繰り返す．労働者からみると，私的なスケジュールを自身の携帯端末に入力するだけでよく，他人に私的なスケジュールを知らせなくともよいという利点がある．また，携帯端末上で，仕事と私的な

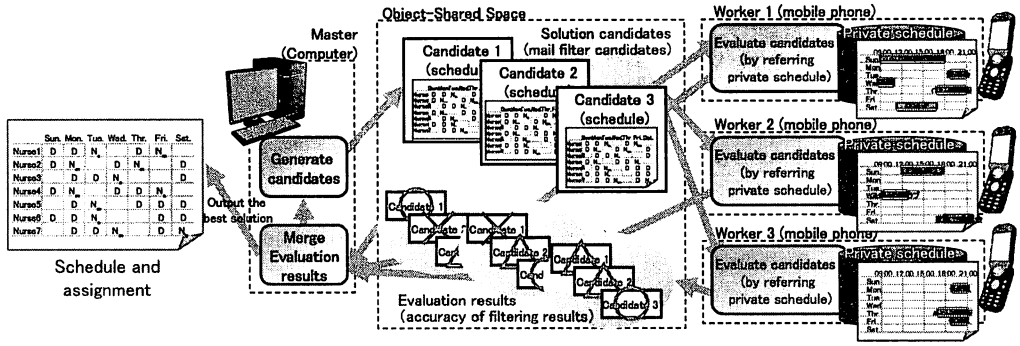

図 4　分散スケジューリングへの応用

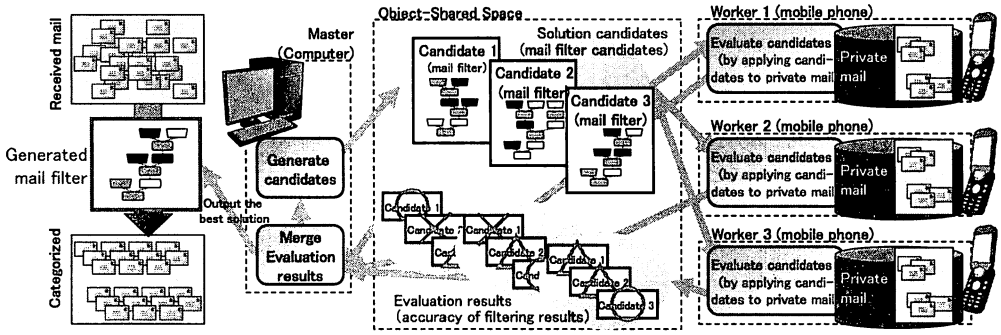

図 5　メールフィルタ分散学習への応用

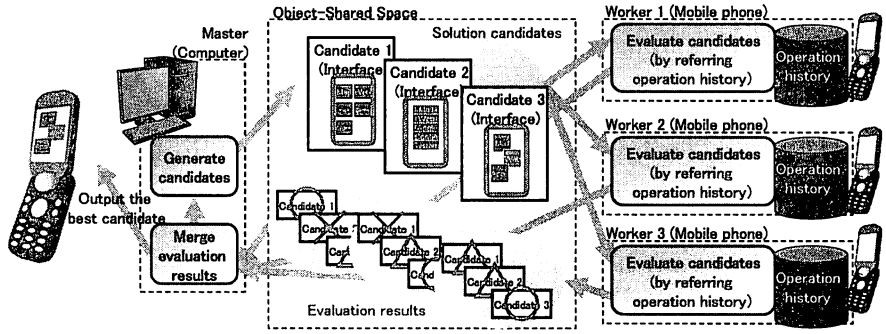

図 6　ユーザインタフェース最適化への応用

スケジュールとを一元的に管理することができる．雇用者（管理者）からみると，各労働者の私的な都合を考慮した勤務シフトを自動的に生成でき，労働者の私的なスケジュールを保持する必要がないため個人情報の漏洩の危険が低い．また，ある労働者の都合が悪く，勤務できない状況になった場合にも動的に再スケジューリングを行うことができる．

3.2　メールフィルタ分散学習

迷惑メールを自動的に識別・分類するメールフィルタは，メールを日常的な通信インフラとして使用するユーザにとって不可欠なツールである．過去の迷惑メールのみを用いてフィルタの学習を行うと，重要なメールが迷惑メールと判別されてしまうなど，不十分な精度のフィルタが生成されてしまう．迷惑メール以外の通常のメールを学習に利用することでフィルタの精度を改善することができるが，業務や私用のメールを他者に提供することは難しく，各ユーザが個別に学習を行う必要があった．

提案するプライバシ・グリッドを用いてメールフィルタを分散学習すると，業務や私用のメールを他者に見せることなく，学習データとして提供することができる（図 5）．すなわち，マスタ計算機が生成したフィルタ候補をワーカ（計算機や携帯電話）に配信し，各ユーザが保持するメールアーカイブを用いてフィルタの評価を行うことができる．マスタ側で，迷惑メールのみを用いた学習を行うことで初期解を生成し，ワーカからの評価結果をもとに反復改善を行うことで，クラス境界を正確に学習した高品質なメールフィルタを生成することができる．

3.3 ユーザインタフェース分散最適化

パーソナルコンピュータや携帯電話のソフトウェアにおいて，様々な習熟度のユーザ全てにとって使いやすいユーザインタフェースを設計することは重要である．本研究の分散問題解決方式を利用することで，ユーザインタフェースの評価および最適化を行うことが可能となる（図 6）．パーソナルコンピュータや携帯電話などの端末に，ユーザの操作履歴を記録しておく．ユーザインタフェースの開発者は，インタフェースの構成案をユーザの端末に送信する．ユーザの情報端末は，過去の操作履歴に基づいて，送信されたインタフェースの構成案の評価を行い，評価結果を開発者に返送する．これを繰り返すことにより，多くのユーザにとって利用しやすいインタフェース構成を得ることができる．各ユーザの操作履歴は開発者に直接送られることはなく，各ユーザのプライバシは保たれる．

4. おわりに

本稿では，携帯電話のプライバシを安全に利用して分散組合せ最適化を行う方式を提案した．本方式は，携帯電話を計算資源として分散問題解決に参加させることができ，ユーザは安心して嗜好情報を入力でき，満足度の高い解を得ることができる．また，電話やメールの送受信履歴，携帯電話に搭載されたカメラで撮影した画像などを利用できる．

今後，プライバシ・グリッドをミドルウェアとして実装する．また，タブー探索におけるタブーリストや，免疫アルゴリズムにおける記憶細胞のように，探索における集中化と多様化の制御に反映させることで，より少ない通信コストで解探索を行える最適化アルゴリズムを開発する．

謝辞

本研究の一部は，財団法人 倉田記念日立科学技術財団 倉田奨励金によるものです．ここに記して感謝の意を表します．

文　献

[1] D. Gelernter: "Generative communication in linda", ACM Trans. Program. Lang. Syst., **7**, 1, pp. 80–112 (1985).

[2] K. Takeda, S. Ono and S. Nakayama: "Jsgrid: An environment for heterogenous cluster computing", Proc. of Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies (PDCAT2005), pp. pp.507–512 (2005).

[3] 武田, 小野, 中山："異機種混合クラスタ環境 jsgrid の開発と評価", 日本計算工学会論文集, **8**, 20060005, pp. pp.211–221 (2006).

[4] 岩川, 小野, 中山："分散並列処理プログラミング言語 Espace の開発", システム制御情報学会論文誌, **19**, 7, pp. 296–298 (2006).

[5] E. Rich and K. Knight: "Artificial Intelligence", Mcgraw-Hill College (1990).

[6] S. Minton, A. B. P. M. D. Johnston and P. Laird: "Minimizing conflicts: a heuristic repair method for constraint satisfaction and scheduling problem", Artificial Intelligence, **58**, pp. 161–205 (1992).

[7] S. Kirkpatrick, C. D. Gelatt and M. P. Vecchi: "Optimization by simulated annealing", Science, Number 4598, 13 May 1983, **220, 4598**, pp. 671–680 (1983).

[8] D. E. Goldberg: "Genetic Algorithms in Search, Optimization, and Machine Learning", Addison Wesley, Reading (1989).

[9] J. Kennedy: "Small worlds and mega-minds: Effects of neighborhood topology on particle swarm performance", International Conference on Evolutionary Computation, pp. 1931–1938 (19999).

[10] F. van den Bergh: "An Analysis of Particle Swarm Optimizers", PhD thesis (2002).

[11] 廣安, 三木, 佐野, 谷村, 濱崎："2 個体分散遺伝的アルゴリズム", 計測自動制御学会論文集, **38**, 11, pp. 990–995 (2002).

[12] 小野, 中山, 片山："解探索装置、適応度評価装置、最適化システム、解探索方法、適応度評価方法及びプログラム", 特開 2006-277137 (2006).

[13] R. Tanese: "Distributed genetic algorithm", Proceedings of the Third International Conference on Genetic Algorithms, pp. 434–439 (1989).

[14] 飯村, 池端, 中山："オブジェクト共有空間を用いた並列遺伝的アルゴリズムにおけるノアの箱舟戦略の検討", 情報知識学会誌, **13**, 2, pp. 1–7 (2003).