情報処理学会論文誌 Vol.57 No.9 2058–2063 (Sep. 2016)

テクニカルノート

利用者による個人情報保護手法の決定を可能とするフレームワークの提案

松永 崇秀[1,a)] 山口 哲敬[2] 高橋 健一[1] 川村 尚生[1] 菅原 一孔[1]

受付日 2015年12月3日, 採録日 2016年3月4日

概要：近年，インターネットの普及にともない，オンラインショップや施設の予約など様々なネットワークサービスが利用されている．これらのサービスのいくつかは利用者に対して個人情報の提供を要求する．しかし，利用者は提供した個人情報が実際にどのように利用されるか知ることができないため，サービス提供者に個人情報を提供することに不安を感じる．そこで，利用者が個人情報の利用方法を指定することができる仕組みを提案する．サービス提供者は自身の持つプログラムで個人情報を処理する．このプログラムに利用者が指定した処理方法を反映させることで，利用者が安心してネットワークサービスを利用できるフレームワークを実現する．

キーワード：個人情報保護，プログラム変換，セキュリティ，プライバシ

A Framework which Enables Users to Select Privacy Protection Method

Takahide Matsunaga[1,a)] Akihiro Yamaguchi[2] Kenichi Takahashi[1] Takao Kawamura[1] Kazunori Sugahara[1]

Received: December 3, 2015, Accepted: March 4, 2016

Abstract: Nowadays, various network services, such as online shops and reservation of facilities, have been used with the spread of the Internet. Some of these services request to offer personal information to users. However, we cannot know how offered personal information is used. Thus, we feel uneasy to offer personal information to service providers. In this paper, we propose a framework that an user can designate usage procedures of his/her personal information. Here, a service provider is processing user's personal information in its own program. Therefore, we realize a framework that enables to apply usage procedures designated from the user to the program of the service provider.

Keywords: personal information protection, program conversion, security, privacy

1. はじめに

近年，インターネットの普及にともない様々なネットワークサービスが利用されている．たとえば，Amazon や楽天などのオンラインショップやホテルの予約，オンラインバンキングなどがあげられる．これらのサービスは，利用者に対して名前や住所，電話番号やクレジットカード番号などの個人情報の提供を求める．利用者はサービス提供者の定める方法に従って個人情報を提供することで，サービスを利用することができる．しかし，個人情報の利用方法はサービス提供者に委ねられている．すなわち，利用者は提供する個人情報がどのように扱われているか知ることができず，1 度提供した個人情報を保護することもできない．このため，サービス提供者が個人情報を不正利用しないと利用者が信頼していることが前提として必要となる．しかし，近年では情報漏洩事件 [1] やフィッシングサイトなどによる被害 [2]，サービス提供者による情報の不正利用などが多発している．

[1] 鳥取大学大学院工学研究科
Graduate School of Engineering, Tottori University, Tottori 680–8550, Japan
[2] 鳥取大学工学部
Faculty of Engineering, Tottori University, Tottori 680–8550, Japan
[a)] s112052@ike.tottori-u.ac.jp

一方で，共通鍵暗号方式や公開鍵暗号方式などの暗号化技術や電子証明書，SSL や TLS のようなプロトコルなど，様々なセキュリティ技術が開発されている．これらの技術を利用するか否かはサービス提供者に決定権がある．すなわち，利用者は提供する個人情報の保護方法を決めることができない．このため，利用者はサービス提供者に不安を感じた（たとえば，暗号化なしで個人情報を送信することが求められたなど）としても，個人情報を提供してサービスを利用するか，個人情報を提供せずにサービスを利用しないかという選択肢しか持たない．

この問題を解決する手法として，利用者自身が個人情報の処理方法を決めることができる仕組みが提案されている [3]．一般的に，利用者が提供した個人情報はサービス提供者の持つプログラムで処理される．そこで，このプログラムの処理方法を利用者が指定した方法に書き換える．これにより，利用者が指定した方法でサービス提供者に個人情報の処理を行わせる．このことで，個人情報を提供する利用者自身が個人情報の利用方法を決定するため，利用者は安心して個人情報を提供できるようになる．本稿では，この仕組みを具体化するとともにプログラム変換の評価を行う．

2. 関連研究

個人情報の利用目的や利用方法などを記したプライバシポリシ [4] を多くのサイトが策定している．しかし，多くの利用者がプライバシポリシを閲覧しないという問題がある．そこで，収集する個人情報の利用方法を利用者に提示するフォーマットとして P3P（Platform for Privacy Preferences）[5] が提案されている．P3P は利用者があらかじめ定めた個人情報の利用基準と各サイトのプライバシポリシを比較し，自動的に情報提供の可否を判断する．しかし，P3P ではサービス提供者がプライバシポリシどおりに情報を利用することを保証しない．

また，個人情報を送信しないことにより，悪意のあるアプリケーションから個人情報を守ること [6] が提案されている．この研究では，個人情報の代わりにアプリケーションルールにより生成された制御コマンドを送信することで情報を保護する．しかし，アプリケーションルールはサービス提供者が作成しており，利用者が制御方法を指定することはできない．

利用者が安心してサービスを利用するための仕組みとして，PPM（Privacy Policy Manager）[7] が提案されている．PPM では，パーソナルデータの取扱いに関するユーザプリファレンスを管理することによってデータの流通を制御する．また，開示する情報の粒度を制御することでプライバシを保護する研究 [8], [9] が行われている．これらにより，利用者の要望にあった情報のみを送信し，その情報のみで利用できる範囲のサービスを利用することが可能となる．しかし，その情報単体で利用者の特定につながる情報は守ることができない．また，サービス提供者が必要とする情報を遮断すると，サービスの利用に支障を来す可能性がある．

3. 個人情報保護フレームワーク

利用者にはサービス提供者による個人情報の利用方法が分からないため，個人情報を提供することに不安を感じる．そこで，個人情報の処理を利用者が制御するためのフレームワークを提案する．

利用者が提供した個人情報はサービス提供者の持つプログラム（個人情報処理プログラム）によって処理される．本フレームワークでは，サービス提供者の持つ個人情報処理プログラムを変換し，利用者が指定した保護方法を適用することで，利用者が個人情報の利用方法を制御する．このことを実現するためには，

要件 1 利用者が指定する処理方法が個人情報処理プログラムに適用可能であること

要件 2 利用者が個人情報の保護方法をサービス提供者に伝えられること

が必要となる．そこで，個人情報処理プログラム中での情報の処理方法を示した利用ポリシと，個人情報の保護方法とプログラムの変換方法を記述した保護ポリシを定義する．

利用ポリシにより，利用者はサービス提供者による個人情報の利用方法を知ることができる．また，利用者は利用ポリシを参照することでプログラムに適用可能である保護ポリシを選択し，自身の希望する保護方法をサービス提供者に伝える．サービス提供者は保護ポリシに従ってプログラムを変換し，変換後のプログラムで個人情報を処理する．これにより，利用者が個人情報の保護方法を決定する．個人情報保護フレームワークの動作の流れを**図 1** に示す．

(1) サービス提供者は利用者に個人情報の提供を要求する．このとき，サービス提供者は利用者に利用ポリシを送信する．

(2) 利用者は利用ポリシを参照することで，個人情報処理プログラムに適用可能な保護ポリシを選択し，そのポリシに従って自身の個人情報を変換する．

(3) 利用者は保護ポリシと変換後の個人情報をサービス提供者に送信する．

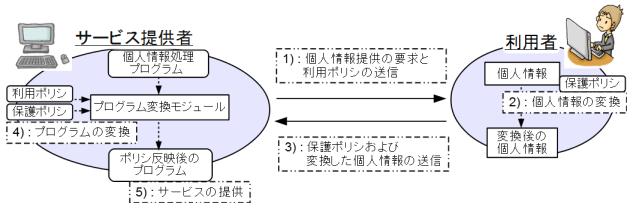

図 1 個人情報保護フレームワーク
Fig. 1 A framework for privacy protection.

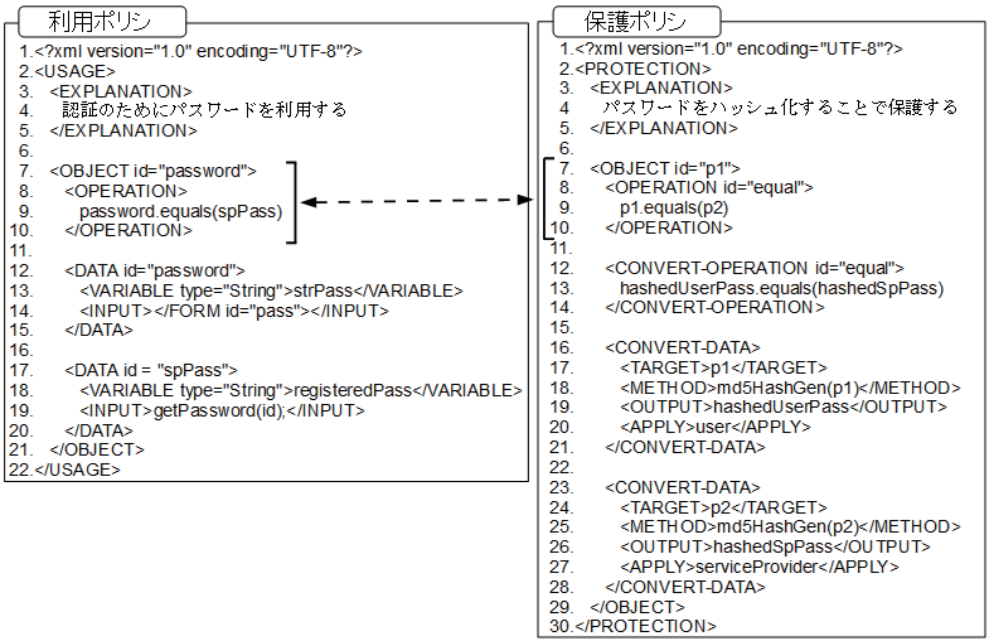

図 2 利用ポリシと保護ポリシの例
Fig. 2 Examples of an use policy and protection policy.

(4) サービス提供者は保護ポリシに従って個人情報処理プログラムを変換する．
(5) サービス提供者は，変換後の個人情報処理プログラムを用いて個人情報を処理し，サービスを提供する．

これにより，利用者は自身の指定した方法で個人情報を保護することができるため，サービス提供者による情報の不正利用や悪意のある第三者からの攻撃に対して対策することができる．

3.1 利用ポリシと保護ポリシ

本フレームワークでは，個人情報処理プログラムを保護ポリシに従って変換することで，利用者が個人情報の保護方法を決定する．ここで，プログラムを変換するためにはプログラム中での個人情報の処理方法を知る必要がある．そこで，サービス提供者は個人情報処理プログラム中での個人情報の利用方法を定義した利用ポリシを準備する．**図 2** 左に利用ポリシの例を示す．

利用ポリシは各個人情報について準備され，個人情報処理プログラム中で個人情報がどの変数に格納され，どのように処理されるかが定義される．図 2 の例はパスワードに関する利用ポリシを示している．7 行目にはパスワードが利用ポリシ中で “password” という識別子で表現されていることが示されている．また，9 行目はパスワードを password.equals(spPass) で利用することを示している．12〜15 行目では，“pass” という名前がついた入力フォームに入力されたデータがパスワードを表し，プログラム中で strPass という変数で利用されていることが分かる．同様に，17〜20 行目を見ると spPass はプログラム中で registeredPass 変数で利用され，getPassword(id) によって初期化されていることが分かる．

また，個人情報の保護方法およびプログラムの変換方法は保護ポリシとして定義する．パスワードをハッシュ化することで保護するポリシの例を図 2 右に示す．7〜10 行目には，パスワードが保護ポリシ中で “p1” という識別子で表現され，p1.equals(p2) という形式で利用されるときに適用可能であることが示されている．12〜14 行目には，p1.equals(p2) でのパスワードの利用を，hashedUserPass.equals(hashedSpPass) に変換しなければならないことが示されている．さらに，hashedUserPass は p1 を md5HashGen メソッドによって変換して生成すること（16〜21 行目）や，hashedSpPass は p2 を md5HashGen メソッドによって変換して生成すること（23〜28 行目）が示されている．

これらのポリシを結び付けることで，プログラムに適用可能な変換ルールを導出する．保護ポリシは利用ポリシをもとに利用者が選択したものであるため，2 つのポリシの `<OBJECT>` を参照し，それぞれのポリシ中のパスワードの識別子を結び付ける．図 2 右の保護ポリシが図 2 左の利用ポリシに適用するものとして選択されたとすると，利用ポリシ中の password は保護ポリシ中の p1 に対応することが分かる．同様に，利用ポリシ中の spPass は保護ポリシ中の p2 に対応することが分かる．さらに，password はプログラム中で strPass 変数として，spPass は registeredPass 変数として利用されていることが分かるため，保護ポリシ中の p1.equals(p2) は strPass.equals(registeredPass) で実現されていることが分かる．これにより，strPass.equals(registeredPass) を

hashedUserPass.equals(hashedSpPass) に変換するための変換ルールを導出する．また，strPass は入力フォームに入力されたデータであることから，このデータに対して md5HashGen メソッドを適用し，hashedUserPass を生成する変換ルールを導出する．同様に，hashedSpPass は getPassword(id) で得られる値に対して md5HashGen メソッドを適用し生成する．これにより，保護ポリシが保護対象とする情報が，プログラム中でどの変数に格納され，どのような操作で処理されるか知ることができる．

3.2 プログラムの変換

前節で述べたポリシの結び付けにより，変換ルールを生成することができる．これらの変換ルールを適用すべき場所を特定するためにプログラムの解析を行う．ここでは，Java 言語で記述されたプログラムを対象とし，Java 言語のソースコードを解析することができる ASTParser [10] を利用する．ASTParser は EclipseJDT が提供する API の 1 つで，Java 言語のソースコードを解析し，抽象構文木を生成する．抽象構文木とは，ソースコードからコメント文や空行などの実行する際に不要な情報を取り除いたデータ構造のことである．ASTParser により構文解析され，プログラムの各行は変数の宣言文や代入文，ループ文などのように意味付けされる．またその行はさらに字句へと分解され，変数名やメソッド名などのように意味付けされる．これにより，プログラム中でどの変数にどの情報を格納するか，どのメソッドでどの変数を使用するかなどが解析できる．

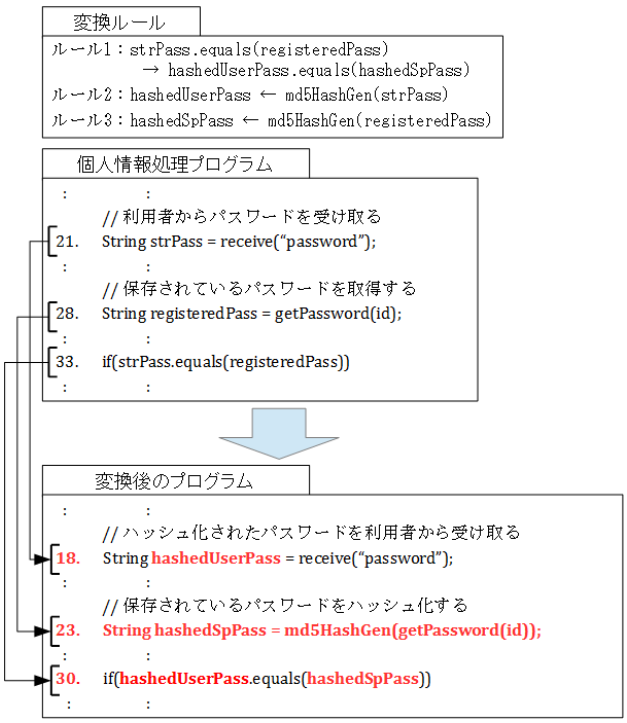

図 3 変換ルールとプログラムの変換例
Fig. 3 Conversion rules and an example of program conversion.

解析後，変換ルールを変換対象のプログラムに適用し，プログラムを変換する．すべての変換ルールを適用することで，利用者が選択した保護方法を適用した個人情報処理プログラムを生成する．プログラムの変換例を**図 3** に示す．

図 3 では図 2 のポリシにより生成した変換ルールを適用した例を示している．プログラムの解析により，strPass.equals(registeredPass) は個人情報処理プログラム中の 33 行目で使用されていることが分かる．このため，この箇所を変換ルールに従って hashedUserPass.equals(hashedSpPass) に書き換える（30 行目）．また，利用者のパスワードは md5HashGen(strPass) によってハッシュ化されるため，利用者からパスワードを受信する部分は hashedUserPass を受信するように変換する（18 行目）．同様に，registeredPass も md5HashGen メソッドによりハッシュ変換する（23 行目）．これにより，ハッシュ化したパスワードで認証するようにプログラムを変換することができる．

4. 実験

4.1 動作実験

Web の入力フォームから入力を要求されている情報を抽出し，各個人情報に対して保護ポリシを選択することができる機能を Google Chrome [11] のアドオンとして実装した．また，生のパスワードを要求し，パスワード認証に成功したか否かを表示するだけのサービスを準備した．**図 4** に保護ポリシ選択前と，パスワードをハッシュ化する保護ポリシ選択後の認証結果を示す．変換前では生のパスワード（java_password）を受け取り認証していたが，変換後ではハッシュ化されたパスワード（54cbc・・・）で認証に成功していることが確認できる．

4.2 プログラム変換率の評価

利用ポリシと保護ポリシによりプログラムが想定どおりに変換できるかを評価した．変換対象のプログラムとして，GitHub [12] で “server chat” や “server password” と検索した結果の上位から Java 言語で記述されているもの 10 個

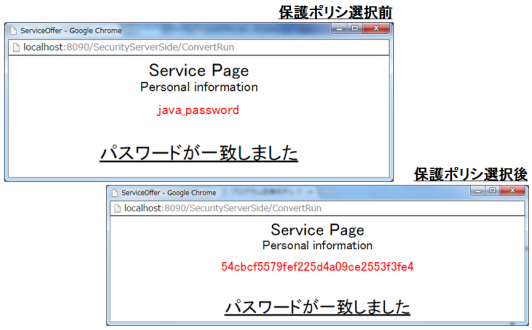

図 4 パスワードの認証結果
Fig. 4 A result of password authentication.

表 1 実験結果
Table 1 Experimental result.

変換成功	79 通り
変換失敗	7 通り

を利用した．また，それぞれのプログラムが扱う個人情報ごとに利用ポリシを準備した．2 つ以上の個人情報を扱うプログラムが存在するため，準備した利用ポリシの合計は 13 個となった．保護ポリシとしては，ハッシュ化した情報で認証を行うためのポリシや通信路の暗号化を行うためのポリシなどの 7 個を準備した．

利用ポリシと保護ポリシの組合せ 91（=13*7）組のうち，利用ポリシと保護ポリシの組合せとして不適切なもの 5 組を除いた 86 組について変換が成功するかどうか実験した．実験結果を**表 1** に示す．

86 通りの組合せのうち，79 通りの組合せについては変換に成功した．しかし，7 通りの組合せについては変換に失敗した．変換に失敗した組合せを分析すると，シリアライズを使用しているプログラムや，変換対象の変数が複数のクラスにまたがって使用されているプログラムであった．これらはプログラムの変換機能を拡張することで解決できると考える．

4.3 考察

本フレームワークでは利用者が保護ポリシを選択し，その保護ポリシに従って個人情報処理プログラムを変換することで，利用者が選択した方法で個人情報を保護する．ここで以下の問題が発生することが考えられる．

問題 1 利用者が保護ポリシを選択できない．
問題 2 不正な動作をするプログラムに変換される．
問題 3 プログラムが解析され，変換が無効化される．

一般的な利用者はセキュリティに関する知識が乏しく，どのような保護ポリシを選択すればよいかを判断できない．このために問題 1 が発生する．このことに関しては，保護ポリシデータベースを管理する第三者信頼機関（以下，TTP）を準備し，TTP が提示した推奨保護ポリシを利用者が選択することで解決できるものと考える．利用者の多くは推奨保護ポリシを利用することになると考えられるが，この場合でもサービス提供者の技術や意図（たとえばフィッシングによるパスワード取得）に依存せず，推奨された方法で自身の個人情報を保護することができる．また，保護方法に脆弱性が見つかったとしても，推奨保護ポリシを変更することでただちに脆弱性に対応することができる．

問題 2 は利用者が不正な保護ポリシを選択したときに発生する．たとえば，マルウェアを仕込む変換を行う保護ポリシであった場合，個人情報処理プログラムにマルウェアが仕込まれてしまう危険性が存在する．これに関しても，TTP が検証を行った保護ポリシの利用のみをサービス提供者が許可することで解決できるものと考える．

問題 3 に関してはプログラムの解析を困難にすることで軽減できる．たとえば，プログラムの変換も TTP が行うこととし，TTP がプログラム難読化技術 [13], [14] を利用して変換後のプログラムを難読化する．これによりサービス提供者によるプログラムの解析が困難になる．また，時間をかけて解析したとしても，サービス提供者が得られるのはそのプログラムで利用された一個人のデータのみであるため，得られるメリットが少なくプログラム解析の動機を抑えることができると思われる．

5. おわりに

本稿では，インターネットサービスの利用時における個人情報提供への利用者の不安を軽減するための手法として，個人情報保護フレームワークを提案した．個人情報保護フレームワークでは，サービス提供者の持つ個人情報処理プログラムを利用者が選択した方法で変換し，変換後のプログラムで個人情報を処理する．これにより，利用者が選択した方法で個人情報を保護することが可能となる．

参考文献

[1] ニュースガイア株式会社：情報漏洩事件・事故一覧，Security NEXT，入手先 ⟨http://www.security-next.com/category/cat191/cat25⟩（参照 2015-11-10）．
[2] フィッシング対策協議会：報告書類，入手先 ⟨https://www.antiphishing.jp/report/⟩（参照 2015-11-10）．
[3] Takahashi, K., Matsuzaki, T., Mine, T., Kawamura, T. and Sugahara, K.: Protection of Personal Information based on User Preference, *IJNCAA*, Vol.1, No.4, pp.822–834 (2011).
[4] IBM：プライバシー・ポリシーの定義，入手先 ⟨https://publib.boulder.ibm.com/tividd/td/ITPME/SC23-1284-00/ja_JA/HTML/p12plmst22.htm⟩（参照 2015-09-16）．
[5] W3C: Platform for Privacy Preferences (P3P) Project, available from ⟨http://www.w3.org/P3P/⟩ (accessed 2015-09-16).
[6] 田丸修平，岩谷晶子，高汐一紀，徳田英幸：プライバシを考慮したパーソナライゼーションを実現するアプリケーションフレームワーク，情報処理学会研究報告，Vol.93, pp.49–56 (2003).
[7] 中村 徹，Andrew A. Adams，村田 潔，清本晋作，高崎晴夫，渡辺 龍，三宅 優：パーソナルデータ流通基盤：Privacy Policy Manager（PPM）の受容性評価，暗号と情報セキュリティシンポジウム（SCIS2014），3D3-2 (2014).
[8] 宮本崇弘，竹内 亨，奥田 剛，春本 要，有吉勇介，下條真司：プライバシとサービス品質のトレードオフを考慮した個人情報制御機構の提案，電子情報通信学会第 16 回データ工学ワークショップ（DEWS2005），6-A-01 (2005).
[9] 菊池 亮，高橋克巳：ログ情報活用におけるプライバシー保護技術の考察，情報の科学と技術，Vol.63, No.2, pp.69–73 (2013)，入手先 ⟨http://ci.nii.ac.jp/naid/110009578963⟩.
[10] Manoel Marques：Eclipse の ASTParser を試す，IBM developerWorks，入手先 ⟨https://www.ibm.com/

developerworks/jp/opensource/library/os-ast/〉（参照 2015-11-10）.
[11] Google：Chrome ブラウザ，入手先 〈https://www.google.co.jp/chrome/browser/desktop/〉（参照 2015-11-10）.
[12] GitHub: Explore GitHub, available from 〈https://github.com/explore〉 (accessed 2015-11-10).
[13] 玉田春昭, 中村匡秀, 門田暁人, 松本健一：Java クラスファイル難読化ツール DonQuixote，ソフトウェア工学の基礎 XIII，日本ソフトウェア科学会 FOSE2006，pp.113–118 (2006).
[14] 福島和英，櫻井幸一：ソフトウェア透かしにおける個人識別情報埋め込み位置の難読化，暗号と情報セキュリティシンポジウム（SCIS2003），pp.1053–1058 (2003).

松永 崇秀 （学生会員）

平成 4 年生．平成 27 年鳥取大学工学部知能情報工学科卒業．現在，同大学大学院工学研究科情報エレクトロニクス専攻修士課程在学中．コンピュータセキュリティに興味を持つ．

山口 哲敬

平成 5 年生．平成 28 年鳥取大学工学部知能情報工学科卒業．同年金融系のシステム開発会社へ就職．金融業務システムに興味を持つ．

高橋 健一 （正会員）

昭和 51 年生．平成 16 年九州大学大学院システム情報科学府博士課程修了．博士（工学）．同年財団法人九州システム情報技術研究所（現，九州先端科学技術研究所）入所．平成 23 年より，鳥取大学大学院工学研究科情報エレクトロニクス専攻准教授．情報セキュリティ，エージェントシステム，ユビキタス技術等の研究に従事．電子情報通信学会，電気学会，IEEE 各会員．

川村 尚生 （正会員）

昭和 40 年生．平成 6 年神戸大学大学院自然科学研究科博士課程単位取得退学．同年鳥取大学工学部知能情報工学科助手，現在，同大学大学院工学研究科情報エレクトロニクス専攻教授．エージェントシステム，社会情報システムに関する研究に従事．博士（工学）．電子情報通信学会会員．

菅原 一孔 （正会員）

昭和 31 年生．昭和 56 年東京工業大学大学院理工学研究科電子物理工学専攻修士課程修了．同年神戸市立工業高等専門学校電気工学科講師．同校助教授を経て，平成 6 年鳥取大学工学部電気電子工学科助教授，現在，同大学大学院工学研究科情報エレクトロニクス専攻教授．計算機工学に関する研究に従事．平成 22 年日刊工業新聞社モノづくり連携大賞，平成 21 年船井ベストペーパー賞，平成 21 年総務大臣賞産学官連携功労者表彰，平成 20 年総務大臣表彰 U-Japan 大賞等受賞．平成 25，26 年度情報処理学会中国支部支部長，平成 21 年度電子情報通信学会中国支部支部長．工学博士．