マルチメディア通信と分散処理　106－37
コンピュータセキュリティ　16－37
（２００２．２．１５）

プライバシー保護を考慮した個人情報管理システムに適した暗号プロトコル

橋川　善之　　溝入　優一　　松尾　真一郎　　坂本　弘章
（株）ＮＴＴデータ　ＩＴセキュリティ推進センター

概要
個人の属性を利用した認証などの個人情報を必要とするサービスにおいて、情報の真正性を保ちつつ、利用者の許可した相手に対して許可した情報のみの開示を可能とする方式としては、当該情報を個別に暗号化して、選択して開示する方式が提案されている[1]。本方式においては、暗号化に利用される鍵自身が情報の属する利用者に関する識別情報となるため、事業者の結託により、復号に用いられる鍵をキーとして同一人物に属する個人情報の関連性を解析可能であるという問題点が存在する。本稿では、事業者へ渡す復号用の鍵を毎回異なるものにすることにより、上記の問題点を改善した暗号プロトコルを新規に提案する。

An Encryption Protocol For Privacy Protected Personal Information Management System

Yoshiyuki Hashikawa　Yuichi Mizoiri　Shin'ichiro Matsuo　Hiroaki Sakamoto
NTT DATA CORPORATION　IT Security Center

Abstract
The method was proposed that separately encrypted personal information is registered at the center and selected to inform to realize to both keep genuineness of information and inform an only entity the user permit only information the user permit at the services which need personal information like an authorization using personal attribute[1]. In this method, because the key which is used for encryption itself become an identity of the user whom the information belong to, there a problem that it is possible to analyze the relation of information which belong to same user by matching of decryption keys by the colluding service providers. In this paper, we propose an encryption protocol which avoids this problem by changing decryption keys for service providers each time.

1. はじめに

現在、ネットワーク化の進展により様々なサービスの電子化が進んでいる。多くのサービスにおいては、ネットワークを介し電子化された場合もリアルなサービスと同様に、サービスを提供する事業者とサービスを利用する利用者という両者の立場からは、それぞれ次のような要請がある。まず事業者の立場からは、利用者の本人性及び資格の認証や市場分析、個人の特性に応じたサービス提供をするため、真正性の保証された個人情報を得たいという要請がある。一方、利用者の立場からは、プライバシーの侵害を防ぐため、自分が許可した相手に対して許可した情報のみを開示したいという要請がある。

現在、リアルなサービスや一部のネットワークを介した電子的なサービスにおいては、運転免許や保険証、パスポート、住民票といった様々な証明書がサービス登録時に確認され、その中の個人情報が真正性を持った情報として参照される。将来的に電子的なサービスが進展した状況においても、このようにサービスの外部で仕様が決められており、形態やフォーマットが多種多様で、かつ紙媒体と電子媒体が混在するような各種証明書を、情報の真正性の拠り所として利用されることが予想され、プライバシー保護を実現しつつ、既存証明書内の個々の情報を真正性を持った情報として、選択して開示できる仕組が必要になると考えられる。

このようなプライバシー保護を考慮しつつ許可された個人情報を開示する方式に関しては、いくつかの方式が研究されている[2][3][4]。また、ブラインド署名や確率的暗号などの暗号技術を応用し、匿名性を持った証明書を利用し、プライバシーの保護を実現しながら利用者のもつ権利の認証を可能にする方式[5][6][7]やSPKI 権限証明書を応用した、シンプルで効率的な、プライバシー保護を重視した権限管理方式[8]、属性証明書においてグループ署名を利用することにより、公開鍵を毎回廃止する必要なく、効率的に匿名性を保証した認証を実現する方式[9]など、プライバシー保護と認証を両立するための方式がいくつか提案されている。

これらの方式においては、個人情報の真正性は保証しないか、あるいは真正性を保証するため、システム内部に無条件に個人情報を参照できる認証主体が含まれているが、本研究では、認証主体はシステムの外部と考え、利用者以外には無条件に個人情報を参照できる主体を設定せず、かつ既存の証明書を拠り所として開示される個人情報の真正性が保証されるシステムを研究対象とする。

このようなシステムは、個人情報を個別に暗号化して、選択して開示する方式[1]を適用し、証明書により真正性が保証された個人情報を個別に暗号化してセンターに登録し、選択して事業者に開示することによる実現が有効である。しかしながら、この方式においては、暗号化に利用される鍵自身が情報の属する利用者に関する識別情報となるため、事業者が結託した場合には、復号に用いられる鍵をキーとして、同一人物に属する個人情報の関連性を解析可能であるという問題点が存在する。

本稿においては、上記の問題点を改善した暗号プロトコルについて、新規に提案する。

2. 対象モデル

2.1. システム構成

本研究においては、利用者のプライバシー保護を実現しつつ、真正性の保証された個人情報の開示を実現するため、既存の証明書内の個人情報を暗号化してセンターに登録し、利用者が許可した相手に対して許可した個人情報のみを開示するシステムを、対象モデルとする。

このシステムの概要を、図１に示す。

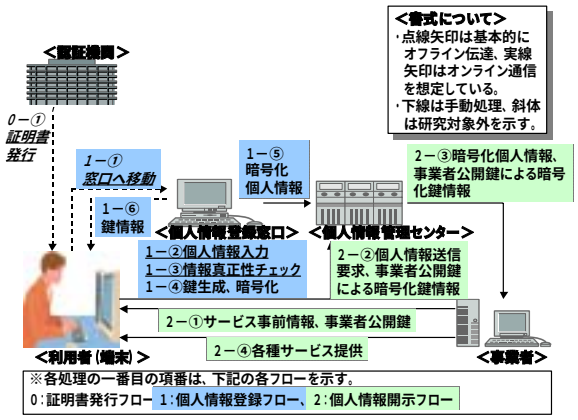

図１　システム概要

本研究で対象とするモデルは、以下の主体から構成される。

（１） 個人情報管理センター

利用者の暗号化された個人情報を保管し、利用者から開示を許可された項目に関して、暗号化された個人情報を事業者へ送る。

（２） 個人情報登録窓口

利用者が登録する個人情報と既存の証明書内の記載内容との一致を確認し、暗号化された個人情報の登録を行う。

（３） 事業者

サービス提供に必要な個人情報の開示を条件に、各種サービスを提供する。

（４） 利用者

サービスの享受に必要でありかつ自らが許可した個人情報を開示し、各種サービスを享受する。

（５） 認証機関

利用者を認証し、個人情報を含んだ各種証明書を発行する。認証機関自体はシステムの外部に存在するものとし、証明書の形態は各認証機関が独自に規定する。

2.2. 要求条件

本研究においては、プライバシー保護と情報の真正性保証の観点から、以下の要求条件を設定する。

- **情報の秘匿**：個人情報管理センターも含めて、利用者と利用者の許可した事業者、及び個人情報登録窓口における登録時以外においては、個人情報の参照はできない。
- **関連性の秘匿**：事業者に対しては、利用者が開示を許可した情報自身以外、情報と利用者の関連性に関わる情報は、渡されない。
- **限定開示の保証**：利用者は、許可した事業者

に対して、許可した個人情報のみを開示できることが保証される。
・**真正性の保証**：利用者は、既存の証明書に記載された情報とは異なる虚偽の情報を、自分の情報と偽って開示することはできない。

3. 既存方式と問題点

3.1. 既存方式

情報の真正性を保ちつつ、プライバシーの保護を考慮して、利用者が許可した事業者に対して許可した個人情報を開示するため、既存方式を適用したシステムの流れに関して、個人情報の登録と個人情報の参照に分けて、以下に述べる。

3.1.1. 個人情報登録

・**Step1-1**：個人情報登録窓口において、まず既存証明書の内容と登録内容の一致を確認する。そして、登録するそれぞれの個人情報 M_i に対して、暗号化用鍵 KE_i 及び復号用鍵 KD_i を生成する。
・**Step1-2**：式（１）に従って暗号化個人情報 C_i をそれぞれ生成し、個人情報管理センターに登録する。ここで、E は暗号化関数とする。

$$C_i = E(M_i, KE_i) \qquad (1)$$

・**Step1-3**： 各 KD_i を利用者へ出力する。

3.1.2. 個人情報開示

・**Step2-1**：利用者が開示を許可した情報項目に関して、個人情報管理センターから利用者が指定した事業者に対して、各 C_i を送付する。
・**Step2-2**：利用者が開示を許可した情報項目に関して、利用者から事業者に対して、各 KD_i が送付され、事業者において式（２）に従って M_i が求められる。ここで、D は復号関数とする。

$$M_i = D(C_i, KD_i) \qquad (2)$$

3.2. 既存プロトコルの問題点

前述した既存プロトコルにおいては、前述した要求条件の内、関連性の秘匿が満たされていない。なぜならば、個人情報の復号用の鍵は各利用者の各個人情報に対して固定的に設定されるため、事業者へ渡される復号用の鍵データ自身が対応する個人情報の属する利用者に関する識別情報となるためである。

この欠陥を用いた具体的な問題点としては、以下が考えられる。

＜前提＞
・事業者１と事業者２が結託しているとする。
・双方の事業者に対して、同一の利用者から個人情報 M_i を含み、異なる情報項目群が、開示される。
・個人情報 M_i 自身は、不特定多数に属する情報であり、それのみで個人を特定できない情報とする。

＜事業者へ渡される情報＞
・利用者 A が、M_i を含む個人情報群 MG1 を事業者１へ開示するため、個人情報群 MG1 を各々暗号化したデータ群 CG1 と KD_i を含む鍵データ群 KDG1 が事業者１へ渡される。
・利用者 A が、M_i を含む個人情報群 MG2 を事業者２へ開示するため、個人情報群 MG2 を各々暗号化したデータ群 CG2 と KD_i を含む鍵データ群 KDG2 が事業者２へ渡される。

＜事業者の不正＞
・事業者１と事業者２へ開示された個人情報群自身の比較を行った場合、個人情報群 MG1 と MG2 に共通の情報 M_i が含まれることが判明したとしても、前提から MG1 と MG2 が同一の利用者に属することはわからないが、渡された鍵データのマッチングを調べ、鍵データ群 KDG1 と KDG2 に同一の鍵データ KD_i が含まれることが判明すると、個人情報群 MG1 と MG2 は同一の利用者に属する情報であることが判明してしまう。

上記の問題点の具体的な例としては、例えば、利用者 A が事業者１に対して名前と住所と性別を開示し、事業者２に対して性別と生年月日を開示したような場合、性別の復号に用いる鍵が同一であることから、鍵の一致を調べることによりこれらの個人情報群が同一の個人に属する情報であることが判明してしまう。

また、結託する事業者に個人情報の開示を行えば行うほど、同一の利用者に属すると判明す

る個人情報の範囲が広がるとともに、その利用者のサービスの履歴も判明する。

そこで、この問題点を回避するため、前述した要求条件を全て満たし、この問題点を解決した暗号プロトコルについて、次章で提案する。

4. 提案する暗号プロトコル

4.1. 基本プロトコル

4.1.1. 方針

暗号化された個人情報の復号用の鍵の一致による関連性の解析を防止するため、同一の情報に関して事業者における復号用の鍵が毎回異なる方式を考える。既存プロトコルにおいては、情報の秘匿と真正性の保証を両立するために暗号化された個人情報が個人情報管理センターで保管されているが、ここで提案するプロトコルにおいても同様に暗号化保管される必要があり、情報の開示時には平文の個人情報を利用できないため、利用者側で単純に毎回異なる鍵を生成して暗号化することはできない。そこで、個人情報管理センターから事業者へ渡される暗号化された個人情報に対して、毎回何らかの処理を加えることにより、復号用の鍵を異なるものにする。

上記を実現するため、ここで使用する暗号アルゴリズムは、復号用の鍵が合成可能であるとし、暗号化用鍵と復号用鍵の対(KE1,KD1)及び(KE2,KD2)に対して、鍵の合成関数 Comp により式（3）に従って合成復号用鍵 KD12 を求めたとき、

$$KD12 = Comp(KD1, KD2) \qquad (3)$$

任意のデータ M に対して、式（4）の関係が満たされるものとする。

$$D(E(E(M, KE1), KE2), KD12) = M \qquad (4)$$

ここで、E は暗号化関数、D は復号関数とする。

そして、個人情報管理サーバにおいては毎回異なる鍵で再度個人情報を暗号化し、事業者へは合成された復号用の鍵を渡すことにより、毎回復号用の鍵を異なるものにする。

4.1.2. 個人情報登録

・**Step1-1**：個人情報登録窓口において、まず既存証明書の内容と登録内容の一致を確認する。そして、登録するそれぞれの個人情報 M_i に対して、初期暗号化用鍵 $KEini_i$ 及び初期復号用鍵 $KDini_i$ を生成する。

・**Step1-2**：式（5）に従って初期暗号化個人情報 $Cini_i$ をそれぞれ生成し、個人情報管理センターに登録する。

$$Cini_i = E(M_i, KEini_i) \qquad (5)$$

・**Step1-3**： 各 $KDini_i$ を利用者へ出力する。

4.1.3. 個人情報開示

・**Step2-1**：利用者は、開示するそれぞれの個人情報 M_i に対して、再暗号化用鍵 $KEre_i$ 及び再復号用鍵 $KDre_i$ を生成する。

・**Step2-2**：各復号用鍵に関して、式（6）に従い一時復号用鍵 $KDtmp_i$ を求める。

$$KDtmp_i = Comp(KDini_i, KDre_i) \qquad (6)$$

・**Step2-3**：各 $KEre_i$ を個人情報管理センターへ送付し、個人情報管理センターにおいて式（7）に従って各 $Cini_i$ を再暗号化して $Ctmp_i$ を求め、

$$Ctmp_i = E(Cini_i, KEre_i) \qquad (7)$$

各 $Ctmp_i$ を事業者へ送信する。

・**Step2-4**：式（5）、（6）、（7）から式（8）が成り立つため、利用者から各 $KDtmp_i$ を事業者へ送付し、事業者においては式（8）に従って M_i が求められる。

$$M_i = D(Ctmp_i, KDtmp_i) \qquad (8)$$

4.2. 提案するプロトコルの評価

要求条件に対する提案プロトコルの評価を以下に示す。

・情報の秘匿に関しては、個人情報管理センターには利用者の保持する初期暗号化用鍵により暗号化された個人情報が登録されるため、開示が許可された事業者と個人情報登録窓口における登録時以外は個人情報管理センターも含めて個人情報が参照できない。

・関連性の秘匿に関しては、復号用の鍵を毎回変化させることにより、開示が許可された個人情報自身以外には、情報と利用者の関連性に関わる情報は渡されない。

・限定開示の保証に関しては、個人情報の参照

に必要な復号用の鍵を利用者が選択して事業者に渡すため、許可した事業者に対して許可した個人情報のみが開示されることが保証される。
・真正性の保証に関しては、既存の証明書で真正性が保証された個人情報が個人情報管理センターに保管され、そこから事業者へ渡されるため、利用者が虚偽の情報を偽って開示することはできない。

4.3. RSA 暗号を利用したプロトコル

4.3.1. 概要

前述した暗号プロトコルに関しては、暗号化用の鍵と復号用の鍵が異なる必要性はないため、共通鍵系の暗号アルゴリズムにより実現しても問題ないが、一般的に利用されている共通鍵系の暗号アルゴリズムにおいて復号鍵が合成可能という性質を持ったものはない。一方、公開鍵系の暗号アルゴリズムにおいては、この性質を持ったものがいくつか存在する。そのため本研究においては、その中でも代表的な RSA 暗号を利用して、具体的なプロトコルを設計した。

RSA 暗号においては、法 n と互いに素で任意の情報 M に対して式（9）を満たす e と d の組合せで、(e,n)と(d,n)が暗号化用の鍵と復号用の鍵として使用されるが、

$$\{(M \wedge e) \wedge d\} \bmod n = M \qquad (9)$$

復号鍵の合成は、法 n が固定されている鍵群において、2つの d を乗算することにより実現可能であるが、利用者毎に n を変化させた場合には、n が個人情報の関連性を解析するためのキーとなってしまう。そのため、n は規定された情報項目毎に一律に設定し、全ての利用者が同じ n を利用する必要がある。

4.3.2. 個人情報登録

・**Step1-1**：個人情報登録窓口において、まず既存証明書の内容と登録内容の一致を確認する。そして、登録するそれぞれの個人情報 M_i に対して、情報項目毎に一律に設定された n_i、p_i、q_i から、互いに素でランダムな e_{ini_i} 及び d_{ini_i} を式（１０）を満たすように生成する。

$$\{e_{ini_i} * d_{ini_i}\} \bmod \phi(n_i) = 1 \qquad (10)$$

ここで、p_i、q_i は素数とし、n_i、p_i、q_i は式（１１）を満たすものとする。

$$n_i = p_i * q_i \qquad (11)$$

また、$\phi(n_i)$は式（１２）から求められる値とする。

$$\phi(n_i) = (p_i - 1) * (q_i - 1) \qquad (12)$$

・**Step1-2**：式（１３）に従って初期暗号化個人情報 $Cini_i$ をそれぞれ生成し、個人情報管理センターに登録する。

$$Cini_i = \{M_i \wedge e_{ini_i}\} \bmod n_i \qquad (13)$$

・**Step1-3**： n_i、p_i、q_i 及び d_{ini_i} を利用者へ出力する。

4.3.3. 個人情報開示

・**Step2-1**：利用者は、開示するそれぞれの個人情報 M_i に対して、n_i、p_i、q_i から、互いに素でランダムな e_{re_i} 及び d_{re_i} を式（１４）を満たすように生成する。

$$\{e_{re_i} * d_{re_i}\} \bmod \phi(n_i) = 1 \qquad (14)$$

・**Step2-2**：利用者は、各 d_{ini_i} 及び d_{re_i} に関して、式（１５）に従い d_{tmp_i} を求める。

$$d_{tmp_i} = \{d_{ini_i} * d_{re_i}\} \bmod \phi(n_i) \qquad (15)$$

・**Step2-3**：利用者は、各 n_i 及び e_{re_i} を個人情報管理センターへ送付し、個人情報管理センターにおいて式（１６）に従って各 $Cini_i$ を再暗号化して $Ctmp_i$ を求め、

$$Ctmp_i = \{Cini_i \wedge e_{re_i}\} \bmod n_i \qquad (16)$$

各 $Ctmp_i$ を事業者へ送信する。

・**Step2-4**：式（１０）、（１３）、（１４）、（１５）、（１６）から式（１７）が成り立つため、利用者は各 n_i 及び d_{tmp_i} を事業者へ送付し、事業者において式（１７）に従って M_i が求められる。

$$M_i = \{Ctmp_i \wedge d_{tmp_i}\} \bmod n_i \qquad (17)$$

5. おわりに

本稿では、利用者のプライバシー保護を実現しつつ、真正性の保証された個人情報の開示を実現するため、既存の証明書内の個人情報を暗号化してセンターに登録し、利用者が許可した相手に対して許可した個人情報のみを開示するシステムにおいて、既存の暗号プロトコルを適用した場合には、事業者の結託により、復号用の鍵をキーとして個人情報の関連性が解析可能であるという問題点が存在することを示し、復号鍵が合成可能な暗号アルゴリズムを利用して、上記の問題点を改善した暗号プロトコルを新規に提案した。

また、それとともに、RSA 暗号を利用して具体的なプロトコルが設計できることを示した。

今後の課題としては、RSA 暗号を利用した暗号プロトコルの安全性の証明や、性能面からより最適なプロトコルの実現方法の検討などが残されている。

また、本プロトコルの新規サービスへの適用も、検討していく予定である。

6. 謝辞

本研究は、通信・放送機構（TAO）の委託研究「走行支援システム実現のためのスマートゲートウェイ技術の研究開発」の一環として実施されています。この場をお借りしまして、御礼申し上げます。

参考文献

[1] An Internet Attribute Certificate Profile for Authorization
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ac509prof-09.txt

[2] 岡野智之, 菊池浩明, 岩井有, 小池範行, 後藤滋樹, 藤岡淳, 中野秀男, 松本勉, 妹尾健史, 渡邊哲夫, “インターネットにおけるプライバシ技術構築と適用に関する研究開発”, 第 15 回 IPA 技術発表会(1996.10.30～31)
http://www.ipa.go.jp/STC/IPADECS/index2.html

[3] 松本勉, 菊池浩明, 岩井有, 小池範行, 後藤滋樹, 中野秀男, 藤岡淳, 清水健介, 岡本克哉, 妹尾健史, 井口誠, 友村清, 藤井真司, 稲村誠一, 渡邊哲夫, “インターネットにおけるプライバシ技術構築と適用に関する研究開発－プライバシを考慮した視聴度調査システム”, 第 16 回 IPA 技術発表会(1997.10.30～31)
http://www.ipa.go.jp/STC/IPADECS/index2.html

[4] 相馬浩之, 田中博樹, “利用者のプライバシー保護を実現するコンテンツ流通システム”, 信学技報, p135-140, (2000.3)

[5] 佐藤直之, 鈴木英明, “匿名のままの権利行使を可能とした認証方式”, 情報処理学会論文誌, p2138-2147, (2000)

[6] 飯田恭弘, 佐藤直之, 花木三良, “ユーザを識別しない認証方式の実装と評価”, 情報処理学会第 62 回全国大会, 3-301, （平成 13 年前期）

[7] 佐藤直之, 鈴木英明, “プライバシ保護に注目した証明書を基盤とした認証システムの一方式”, コンピュータセキュリティ 5-6, p31-36 (1999.5.21)

[8] 齋藤孝道, 梅澤健太郎, 奥乃博, “個人情報の扱いを考慮したアクセス制御の一方式”, コンピュータセキュリティシンポジウム 2000, p55-60, (平成 12 年 10 月)

[9] 崔浩哲, 菊池浩明, 中西祥八郎, “効率的な匿名権限委託”, コンピュータセキュリティシンポジウム 2000, p61-66, (平成 12 年 10 月)