講演番号： 100

ユーザの意思を考慮した個人情報公開制御方式

B－7　Control Method for Opening Personal Information Considering User’s Will

手塚　広太†　長谷川　靖恭†　新津　善弘†

Kota Tezuka†　Yasunori Hasegawa†　Yoshihiro Niitsu†

† 芝浦工業大学 システム理工学部

† College of System Engineering and Science, Shibaura Institute of Technology

1. はじめに

現在，インターネットを利用したサービスの一種として，ユーザから提供された個人情報を利用し，そのユーザにとって最適な情報を提供するといったサービスが存在する．

本稿では，提供される個人情報に対して選別を行い，それぞれの個人情報に適した暗号化方式を提案し，その有効性を評価する．

2. 従来研究

従来研究[1]では，ユーザが望むサービスのランクの指定とそのランクに対応した個人情報の入力を行い，その結果がサービス提供者側に送信される場面を想定している．この時，ユーザが望むサービスのランクが高いほど,要求される個人情報の項目やその粒度は高くなる．ここで，サービス提供者が事前に設定しておいた個人情報の重要度・安全度を基に個人情報の危険度のレベルが選別され，それぞれのレベルに適した暗号化方式を用いて情報が保護されている．

3. 研究概要

3.1. 目的とアプローチ

個人情報の種類による個人特定度や粒度，ユーザが希望する匿名希望度を基に個人情報の選別を行うことで，個人情報送信時の安全性向上と処理時間短縮の両立を目指す．

また，暗号化に関しては，従来研究と同様に公開鍵暗号化方式と秘密分散法を利用するものとする．

3.2. 想定環境

本稿で扱うサービスは，個人情報を公開する度合いに応じてサービスの品質が向上するという性質のものを想定する．

ユーザはサービスを受ける際，サービス提供者から送信されたユーザ項目に記載された個人情報の種類に該当する情報と個々の情報について，匿名希望度の入力を行うものとする．ユーザ項目とは，氏名や年齢，位置情報など多様な種類の個人情報とその個々の情報に対して設定された，以下に定義する匿名希望度，粒度，個人特定度をまとめたものである．

匿名希望度:ユーザがその情報に対して匿名性を求める度合いを表し，数値が大きいほどユーザがその情報に対し匿名性を望んでいるものとする．

粒度:その個人情報の詳細さを表し，数値が大きいほど情報が詳細であるものとする．

個人特定度:その情報一つでどれだけ個人が特定できるかを表し，個人情報の種類によって異なるものとする．

3.3. サービス手順

Step1：ユーザがサービス提供者にサービスを要求する

Step2：サービス提供者はサービスの内容・品質を考慮して定めたグレードの一覧(以下，サービスランク表とする)と公開鍵をユーザに送信する

Step3：ユーザはサービスランクの選択，個人情報の入力を行い，システムによりデータを暗号化する

Step4：ユーザは暗号化されたデータをサービス提供者へ送信する

Step5：サービス提供者は暗号化されたデータを収集し，秘密鍵を用いてデータを復号化する

Step6：ユーザにサービスが提供される

4. 提案方式

4.1. 暗号化手順

サービス手順の Step3 で入力された個人情報の内，個人が特定されにくい情報をデータ集合 A，個人が特定されやすい情報をデータ集合 B，ユーザの匿名希望度が大きい情報をデータ集合 C の 3 種類に選別する．本稿では，これら 3 種類のデータ集合に対して秘密分散法と RSA 暗号方式(公開鍵ビット長は 1024 ビット)による暗号化を行う．

4.2. 方式案

方式案 1

データ集合 A，B，C において，個人情報一つひとつに対して秘密分散法を適用する．

方式案 2

データ集合 B において，個人情報一つひとつに対して秘密分散法を適用する．データ集合 A，C においては，個人特定度と粒度，匿名希望度の和が閾値以上であれば個人情報一つひとつに，閾値未満であれば個人情報をまとめて秘密分散法を適用する．

方式案 3

データ集合 A においては個人情報をまとめて秘密分散法を適用する．データ集合 B においては個人情報一つひとつに対して秘密分散法を適用する．データ集合 C においては個人特定度と粒度，匿名希望度の和が閾値以上であれば個人情報一つひとつに，閾値未満であれば個人情報をまとめて秘密分散法を適用する．

5. 評価

5.1. 評価実験

本稿の有効性を検証するため，仮想的にユーザ項目を作成し，評価実験を行った．本稿で使用した PC のスペックを表 1 に，作成した仮想ユーザ項目を表 2 に示す．また，一般的な暗号方式である RSA 暗号方式(公開鍵のビット長は 2048 ビット)を各方式案との比較対象とした．

表 1. 使用した PC のスペック

OS	Windows 7 Home Premium
CPU	Intel® Core™ i5-2450M CPU @ 2.50GHz
メモリ	8.00GB

表 2. 作成した仮想ユーザ項目

個人情報の種類	入力した情報	個人特定度	粒度	匿名希望度
氏名	芝浦太郎	Ⅴ	Ⅴ	Ⅴ
電話番号	090-XXXX-XXX	Ⅴ	Ⅴ	Ⅴ
生年月日	199X年XX月XX日	Ⅳ	Ⅴ	Ⅳ
メールアドレス	shibaurataro@shibaura-it.ac.jp	Ⅳ	Ⅳ	Ⅳ
マイナンバー	XXXX-XXXX-XXXX	Ⅴ	Ⅴ	Ⅴ
年齢	22歳	Ⅲ	Ⅲ	Ⅲ
職業	大学生	Ⅰ	Ⅱ	Ⅲ
生体情報	175cm	Ⅱ	Ⅲ	Ⅲ
住所	埼玉県さいたま市見沼区	Ⅳ	Ⅳ	Ⅴ
性別	男	Ⅰ	Ⅰ	Ⅱ
趣味	テニス	Ⅱ	Ⅲ	Ⅱ
血液型	B型	Ⅰ	Ⅱ	Ⅲ

5.2. 評価項目

- 処理時間（ミリ秒）
  ユーザにサービスが提供されるまでの時間
- 安全向上度
  暗号化を行うことで安全性は向上するものとする．RSA 暗号方式を適用すると安全性が 1 向上し，秘密分散法を適用すると安全性が 2 向上するものとする．
- 意思反映度
  匿名希望度が 3 以上の個人情報に対し，単体で秘密分散法が適用されていれば匿名希望度が 2 向上し，まとめて適用されていたら 2 低下する．匿名希望度が 2 以下の個人情報に対しては，秘密分散法が適用されていれば 1 向上するものとする．

5.3. 実験結果

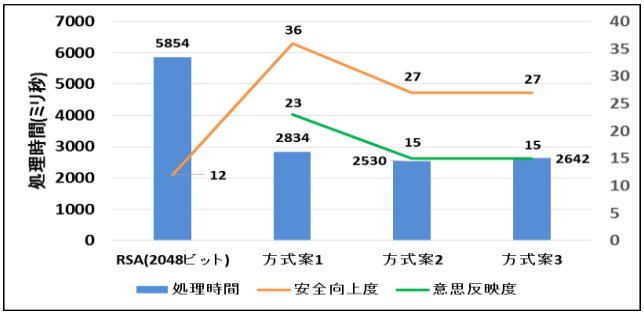

図 1. 仮想ユーザに対する処理時間，安全向上度，意志反映度

6. 考察

図 1 よりどの方式案も一般的に使用されている RSA 暗号と比べて，安全性向上度の面で優位であることが分かった．この結果は，計算量的安全性をもつ RSA 暗号に加えて，情報量的安全性をもつ秘密分散法を適用したためだと考えられる．また，RSA 暗号のビット長を大きくするよりも秘密分散法を適用する方が安全性向上度の面，処理時間の面で優位であることが分かる．

7. まとめ

本稿では，個人情報送信の際にユーザの意思を考慮したセキュリティの公開制御方式を提案し，仮想的に作成したユーザ項目を利用した評価実験を行った．

参考文献

[1]遠藤智也，澁谷優貴，新津善弘“個人情報のセキュリティを考慮した公開制御方式” 電子情報通信学会東京支部学生会 2015 MAR