2ZF-9

災害時対応に用いるプライバシー情報共有支援システムの設計と試作

齋藤　永司† 長澤　悠貴† 毛利　公美‡ 福田　洋治†† 白石　善明†

名古屋工業大学† 岐阜大学‡ 愛知教育大学††

1. はじめに

自然現象による被害を完全に防ぐことは難しく，防災だけでなく被害の軽減に取り組む減災も重要である[1]．我々は既に，図 1 に示した減災を支援することを目的とした情報伝達方式[2]を提案している．この方式は平常時に住民は通勤・通学先，その経路・時間帯といった日頃の行動範囲に関する情報をサービスに登録しておき，非常時には防災関係機関（例：自治体）がサービスに登録されている住民の情報のうち，被災地にいる可能性のある住民の情報を探し，住民が指定した非常時連絡先に交通情報等の避難を促す情報を連絡することで減災を支援するというものである．

日頃の行動範囲や非常時連絡先といった情報はプライバシー情報であり，情報共有サービスを提供するサービス管理者に閲覧されること，サービス管理者から第三者に漏えいすることといった懸念がある．プライバシー情報の保護は基本的には暗号化して保存することで一般には対応される．我々は図 1 の手順を支援するシステムのための暗号方式を提案しており[2]，暗号処理を行うライブラリを開発している．本稿では，その暗号方式のライブラリを用いたプライバシー情報共有システムの設計と試作，その評価について述べる．

2. 機能要件

各利用者（住民，防災関係機関，サービス管理者）の立場からシステムの機能要件は次のようになる．

[**住民**]プライバシー情報の保護がなされること

日頃の行動範囲や連絡先といったプライバシー情報をシステムに登録するため，サービス管理者や第三者に自身の情報は漏えいして欲しくないと住民は考える．

[**防災関係機関**]プライバシー情報の管理コストが低いこと

非常時には住民のプライバシー情報をもとに被災地にいる可能性のある住民への情報伝達を迅速に行いたい．しかし，情報を蓄積保管しておくには情報漏えい対策などのコストがかかる．

[**サービス管理者**]住民と防災関係機関から信頼されるサービスを提供すること

住民のプライバシー情報を管理するので安全性対策をするが，もしも情報漏えい事故が起こったときにも第三者にプライバシー情報が閲覧されないような情報保管をしたい．

3. システムで使用する暗号方式

機能要件を満たすプライバシー情報共有システムを構築するために文献[2]の暗号方式を用いる．図 2 に示すように，共通鍵暗号と公開鍵暗号を組み合わせてプライバシー情報を住民が暗号化し，サービス管理者と協力して防災関係機関が復号する．

住民はプライバシー情報を共通鍵で暗号化し，その共通鍵を公開鍵で暗号化する．サービス管理者のサーバでは暗号化されたプライバシー情報と共通鍵を保管する．

住民は防災関係機関と暗号化された共通鍵を復号する秘密鍵を共有することで第三者に漏えいすることなくプライバシー情報を開示することができる．(2, 2) 閾値秘密分散を繰り返し適用して秘密鍵を分散共有し，(2, 2) 閾値秘密復号でサーバに情報を閲覧されることなく復号する．

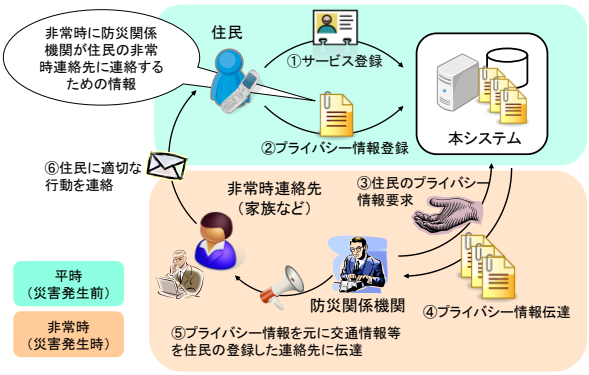

図 1 災害時の情報伝達手順

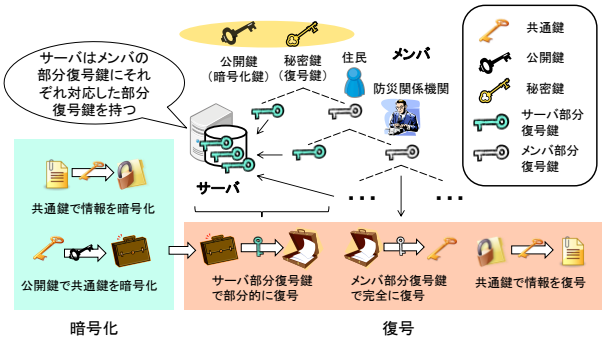

図 2 暗号化と復号の流れ

4. 試作システム

各利用者が利用できる機能は以下の通りである．

[**住民**]ログイン，新規登録（ユーザ情報登録），ユーザ情報編集，パスワード再発行，プライバシー情報登録・編集

[**防災関係機関**]ログイン，ユーザ情報編集，防災関係機関連絡情報編集・取得，（住民の）プライバシー情報取得

[**サービス管理者**]ログイン，新規登録（防災関係機関），住民・防災関係機関ユーザ情報閲覧

4.1. データの種類

次の 3 つの情報をシステムで用いる．

[**ユーザ情報**]各利用者がログインする際に必要な ID やパスワードといった情報．

[**プライバシー情報**]住民自身により登録される．非常時に防災関係機関が用いる日頃の行動範囲や時間帯，非常時連絡先といった，暗号化で保護される情報．

[**防災関係機関連絡情報**]非常時に防災関係機関同士が連絡し合う際に必要な情報．防災関係機関の間で公開される．

4.2. 動作手順

利用できる機能のうち，主な機能である住民の新規登録，プライバシー情報登録，防災関係機関のプライバシー取得時の動作手順を示す．

[**新規登録**]住民とサービス管理者が行う．防災関係機関は住民のプライバシー情報を閲覧する権限を持つため，自由に登録できないようにするためにサービス管理者が防災関係機関のサービス登録を代行する．以下のステップはユーザを住民とした場合の例である．防災関係機関の新規登録の場合，秘匿したい情報はないと思われるので，鍵生成といった暗号処理は省略できる．

Prototype Implementation of a Privacy Information Sharing System for Rescuing Sufferes

† Eiji Saito, Yuuki Nagasawa and Yoshiaki Shiraishi・Nagoya Institute of Technology

‡ Masami Mohri・Gifu University

†† Youji Fukuta・Aichi University of Education

Copyright ©2012 Information Processing Society of Japan.
All Rights Reserved.

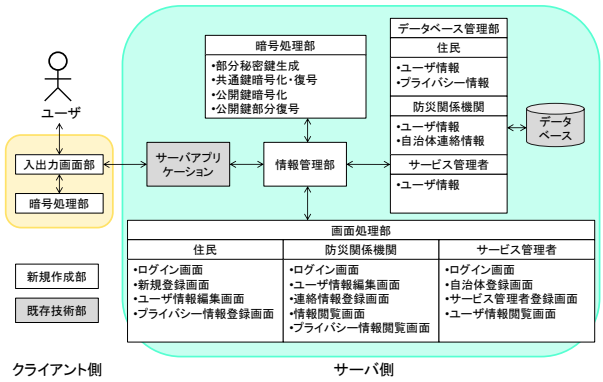

図 3 システム構成

step 1. ユーザは新規登録画面でユーザ認証に必要な情報を入力する.

step 2. 入出力画面部は入力されたユーザ認証情報を暗号処理部に渡し暗号化，およびプライバシー情報を開示するための秘密鍵の分散情報を生成する.

step 3. 入出力画面部は暗号化されたユーザ認証情報と秘密鍵の分散情報を，暗号化通信路を通じてサーバに送信する.

step 4. サーバの情報管理部は受信した秘密鍵分散情報を暗号処理部に渡し，暗号処理部はそのユーザの秘密鍵分散情報に対応した公開鍵や後のプライバシー情報取得に必要なサーバ部分復号鍵など，プライバシー情報の暗号処理に用いる情報を生成する.

step 5. 情報管理部はユーザ認証情報とプライバシー情報の暗号処理情報をデータベース管理部に渡し，データベース管理部の住民ユーザ情報管理部でデータベースに格納する.

step 6. 画面管理部で新規登録完了画面を生成し，ユーザに出力する.

[**プライバシー情報登録**]非常時に防災関係機関が利用する情報を住民がシステムに予め登録する機能である.

step 1. ユーザはプライバシー情報登録画面で災害発生時に防災関係機関が利用する情報を入力する.

step 2. プライバシー情報を入出力画面部は暗号処理部に渡し，暗号処理部は 3 章の暗号方式を用いて暗号化する.

step 3. 入出力画面部は暗号化されたプライバシー情報等をサーバに送信する.

step 4. 受信したプライバシー情報を情報管理部はデータベース管理部に渡し，データベース管理部の住民プライバシー情報管理部でデータベースに格納する.

step 5. 画面管理部でプライバシー情報登録終了画面を生成しユーザに出力する.

[**プライバシー情報取得**]非常時に防災関係機関がサービス提供サーバから住民のプライバシー情報を取得する機能である.

step 1. ユーザはプライバシー情報取得画面でユーザ情報を入力，入出力画面部はユーザ情報をサーバに送信する.

step 2. 受信したユーザ情報を情報管理部はデータベース管理部に渡し，データベース管理部の防災関係機関ユーザ情報管理部は登録されている防災関係機関かどうか検索する．登録済みであれば次のステップに進む.

step 3. 防災関係機関に情報開示を指定している住民の暗号化されたプライバシー情報を暗号処理部に渡し，3 章の暗号方式を用いて部分的に復号する.

step 4. 住民のプライバシー情報を画面管理部でユーザに出力する.

step 5. 受信した住民のプライバシー情報を受信した入出力画面部は暗号処理部に渡し，完全に復号する.

表 1 開発環境

開発言語	Java (JDK1.6.0.24)
JavaEE	JavaEE 6 Web
Webコンテナ	GlassFish3.1.1[3]
データベース	MySQL5.5
JDBC	MySQL Connector/J 5.1.13

表 2 動作性能

OS	Windows7 Professional
CPU	Intel(R) Core(TM) i5 650 3.20GHz
RAM	4.00GB

表 3 応答時間計測結果

	平均時間（ms）
新規登録	160.84
プライバシー情報登録	54.41
プライバシー情報取得	68.81

5. 評価

5.1. システムの主観評価

2 章の機能要件が満たされていることを説明する.

[**住民**]プライバシー情報の保護

サービス管理者にも情報の復号はできない暗号方式を採用しているので情報の閲覧はされない.

[**防災関係機関**]プライバシー情報の管理コスト削減

情報漏えい対策をすべきプライバシー情報を外部のサービス事業者に委託することで管理に関するコストを省くことができる.

[**サービス管理者**]信頼性の高いサービス

使用する暗号方式によりサービス管理者も情報の閲覧はできず，第三者にデータが漏えいしても復号できない.

5.2. システムの応答性能

サービスへの新規登録，プライバシー情報登録，プライバシー情報取得の 3 つの処理について応答時間を計測した．計測に使用したサーバの動作性能は表 2 のとおりである．暗号化と復号で用いるプライバシー情報のデータサイズはシステム利用時に登録する情報量を想定して 1KByte とした．各 100 回ずつ計測を行い，平均値を求めた結果を表 3 に示す．暗号処理や復号処理が入っていても現実的な応答時間である.

6. おわりに

本稿では情報伝達の支援システム[2]を Web アプリケーションとして設計し実装した．暗号技術によってプライバシー情報の保護を実現することで，住民，防災関係機関，サービス管理者のそれぞれにとって利点のあるシステムとなっている.

防災関係機関が住民のプライバシー情報から被災地区に該当する住民の非常時連絡先に情報を連絡する流れのシステム化や，住民がサービスに登録する際の適切な認証方法の検討などが今後の課題である.

参考文献

[1] 内閣府：減災への取組：災害被害を軽減する国民運動のページ（内閣府防災担当），入手先 <http://www.bousai.go.jp/km/gst/index.html>（参照 2011-12-27).

[2] 長澤悠貴，毛利公美，福田洋治，白石善明：災害時対応に用いるプライバシー情報共有の一方式，情報処理学会第 73 回全国大会講演論文集，第 4 分冊，pp. 663-664（2011）.

[3] GlassFish：GlassFish Server 3.1.1 — Java.net，入手先 <http://glassfish.java.net/downloads/3.1.1-final.html>（参照 2012-01-11）.

Copyright ©2012 Information Processing Society of Japan.
All Rights Reserved.