4ZE-8

災害時対応に用いるプライバシー情報共有の一方式

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

大規模な地震や津波，世界的に多発する集中豪雨，ゼロメートル地帯における高潮により，これまでにない多様で激甚な災害のリスクの増加や災害の広域化・複合化・長期化が懸念されている．減災のためには，災害発生時に迅速な防災情報の伝達，避難勧告の発出を行う事中システムが必要である[1].

例えば，次のような災害時情報伝達手順が考えられる（図1）．（1）災害発生時，被災地の**防災関係機関**は近隣地域の防災関係機関に災害発生の連絡をする，（2）連絡を受けた近隣の防災関係機関は，個人の通勤・通学先，自宅からの経路，時間帯，家族の連絡先といった**避難支援情報**をもとに被災地にいると推測される個人の家族に連絡する，（3）連絡を受けた家族が本人に連絡する．以上のような手順により，被災情報を届けると同時に安否を確認することができる．

そのような災害時対応のための情報共有を**避難支援情報管理サーバ**の導入により実現する方法を考える．避難支援情報保管サーバを介して避難支援情報を開示することで，紙媒体で保管する場合に比べ避難支援情報へのアクセスの可用性を高めることができる．

このような手順を実現し，個人のプライバシー情報を保護する最も単純な方法は，個人が共通鍵暗号方式で避難支援情報を暗号化し，避難支援情報の復号に必要な鍵を公開鍵暗号方式で防災関係機関に渡して共有する方法である．しかし，公開鍵暗号方式の秘密鍵を防災関係機関に渡すと，（1）開示先の変更時に公開鍵・秘密鍵ペアの再生成，再配布が必要になる，（2）防災関係機関の鍵管理の負担が大きくなることが考えられる．

本稿では，避難支援情報の開示先の変更が容易で，防災関係機関が管理する鍵の値を制御することにより，1 つの鍵だけで各個人の避難支援情報を復号可能な秘密分散技術と閾

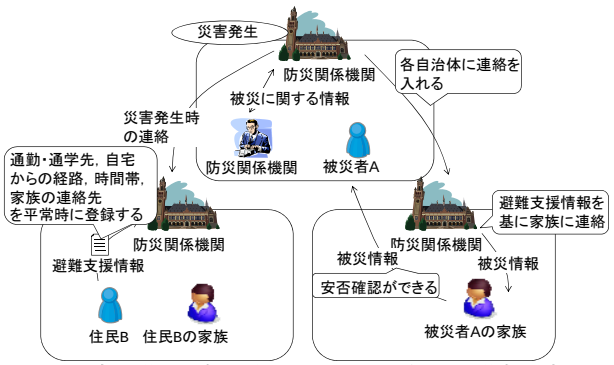

図 1：迅速な災害情報の家族に対する提供と被災者の安否を確認する情報伝達手順

値復号を組み合わせた情報提供方式を提案する．

2. 避難支援情報保管サーバを介した避難支援情報提供方式の要件

避難支援情報がネットワーク上に存在する場合，不特定多数の組織に閲覧される可能性がある．このとき，具体的には以下の点が懸念事項として挙げられる．

(1)．避難支援情報保管サーバが避難支援情報を閲覧する
(2)．個人の意図しない避難支援情報の閲覧がある

これらを踏まえると，プライバシー保護のためには次の要件が満たされなければならない．

要件（1）． 避難支援情報管理サーバは避難支援情報を閲覧できない
要件（2）． 個人の意図しない避難支援情報の閲覧がない

これらの要件を満たすことはすなわち，各個人が自身で避難支援情報を暗号化し，自身で避難支援情報の開示先を制御できるということである．

個人が避難支援情報の開示先を制御する単純な方法は次のような考え方になる．（1）避難支援情報を保管する際，個人が暗号化してから避難情報保管サーバに預ける，（2）各個人の避難支援情報の復号に必要な鍵を異なるものにし，その鍵は防災関係機関で構成されるグループと共有する．

具体的には，個人毎に用意した**グループ公開鍵**，**グループ秘密鍵**ペアを用いるとする．避難支援情報の共通鍵暗号化とその復号に用いる**避難支援情報復号鍵**をグループ公開鍵で暗号化し，避難支援情報復号鍵の復号に用いるグループ秘密鍵を防災関係機関に渡し，そのグループで共有するという方法である．

グループ秘密鍵を渡した防災関係機関から避難支援情報の復号権限をはく奪するためには，グループ公開鍵・秘密鍵のペアを再生成しなければならず，その再配布や避難支援情報復号鍵を再暗号化する等のコストが生じる．

防災関係機関は個人の数だけグループ秘密鍵を管理するので鍵管理の負担がかかる．この負担が大きくなると，鍵の紛失・盗難のリスクが高まり，別の鍵で再暗号化する手間や避難支援情報の漏えいに繋がると考えられる．防災関係機関が 1 つの鍵で全ての個人の避難支援情報を復元できれば鍵管理の負担は軽減できる．

次章では避難支援情報の開示先変更が容易，かつ，防災関係機関が管理する鍵が複数ある場合は単一化することで鍵管理の負担を軽減できる避難支援情報の開示方法と開示先の管理方法を提案する．

3. 避難支援情報の開示先変更が容易で防災関係機関の鍵管理の負担が少ない避難支援情報開示方式

3.1. 秘密分散によるグループ秘密鍵の管理

防災関係機関がグループ秘密鍵を復元せずに避難支援情報を復号する方法に，グループ秘密鍵を秘密分散[2]で個人と防災関係機関間に分散管理し，閾値復号によって避難支援情報を直接復号する方法が考えられる．また，シェアの再分散[3]を利用することでグループ秘密鍵を復元することなく，開示先変更に伴う分散情報の変更が実現できる．

秘密分散によるグループ秘密鍵の分散管理は，防災関係機

A Privacy Information Sharing System For Rescuing Sufferers
† Yuuki NAGASAWA and Yoshiaki SHIRAISHI・Nagoya Institute of Technology
‡ Masami MOHRI・Gifu University
§ Youji FUKUTA・Aichi University of Education

関と避難支援情報保管サーバの二者で閾値復号ができるようにする．これは，防災関係機関が避難支援情報の復号に他の防災関係機関と協調計算する必要がなく，アクセスの可用性を高めることができるためである．

まず，(2,n)秘密分散を単純に適用した場合を考える．このとき，開示先を変更するためには全ての分散情報保持者が協調して新しい分散情報を計算する必要があり，オフラインの分散情報保持者がいる場合に実行できない．

次に，協調計算の参加人数を少なくするために(2,n')秘密分散を繰り返し適用して多分木状に分散すると，秘密鍵の分散構造の維持が困難になるため効率は良くない．

そこで，図 2 のように(2,2)秘密分散を繰り返し適用し，二分木状に管理することを考える．このようにすることで，他の防災関係機関と協調することなく避難支援情報が復元できるだけでなく，開示先変更時の分散構造維持が容易になると考えられる．このとき，分散した一方を避難支援情報保管サーバに，他方を個人が開示先として指定する防災関係機関に渡す．それぞれを**サーバ部分復号鍵**，**メンバ部分復号鍵**と呼ぶ．

次節では，避難支援情報の開示先の変更方法，開示方法を提案する．

3.2. (2,2)秘密分散を繰り返し適用したグループ秘密鍵の分散管理によるメンバ部分復号鍵を単一化できる避難支援情報提供方式

グループ秘密鍵を前節で述べた方法で分散管理し，各防災関係機関と避難支援情報保管サーバはその分散情報である部分復号鍵を保持する場合，(2,2)閾値復号を用いれば防災関係機関はグループ秘密鍵を復元することなく避難支援情報を復号することができる．

閾値復号は次の 3 ステップで行う．

Step1. 避難支援情報保管サーバは，防災関係機関から避難支援情報の入手リクエストを受け取ると，避難支援情報保管サーバ上に保管されている暗号化された避難支援情報と避難支援情報復号鍵のうち，避難支援情報復号鍵をサーバ部分復号鍵を用いて**部分復号**する．

Step2. 部分復号された避難支援情報復号鍵を防災関係機関のメンバ部分復号鍵を使って**完全復号**する．

Step3. 復号された避難支援情報復号鍵を使って避難支援情報を復号する．

この復号処理では，グループ秘密鍵が現れず，復号対象である避難支援情報復号鍵が防災関係機関のところで直接出力されるため，各防災関係間機関と避難支援情報保管サーバはグループ秘密鍵を知ることなく避難支援情報を復号可能である．つまり，グループ公開鍵・秘密鍵ペアの再生成，避難支援情報の再暗号化のコストが生じない．

【開示先制御を実現するプロトコル】

避難支援情報の開示先を制御するためには，開示先の設定，開示先の追加，開示先の削除および定期的な鍵の更新の 4 つが必要と考える．ここでは，開示先の設定について説明する．

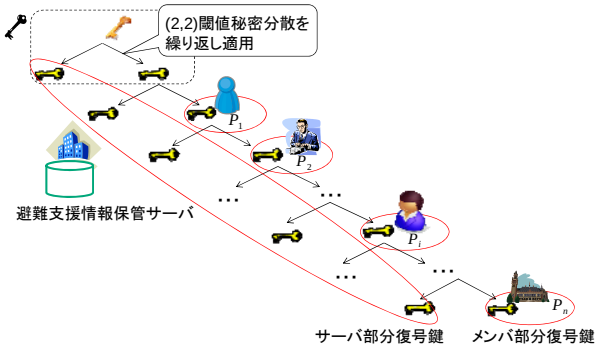

図 2：(2,2)秘密分散によるグループ秘密鍵の管理方法

なお，以下で行う演算は全て $\bmod p$ 上で行われるものとし，防災関係機関 $P_1,\ldots,P_n$ に $x_1,\ldots,x_n$，避難支援情報保管サーバに x_S が識別子として割り当てられているとする． p は十分に大きな素数を表し，防災関係機関 P_i のメンバ部分復号鍵を w_i，サーバ部分復号鍵を $w_S^{(i)}$ と表す．

[防災関係機関 P_1 と避難支援情報保管サーバでグループ公開鍵 pk_G を生成]

Step1. 防災関係機関 P_1 と避難支援情報保管サーバは，分散情報生成プロトコル[4]を用いてそれぞれの部分復号鍵 $w_1, w_S^{(1)}$ を生成する．

Step2. 防災関係機関 P_1 は $g^{a_{10}}, g^{a_{11}}$ を，避難支援情報保管サーバは $g^{a_{S0}}, g^{a_{S1}}$ を公開する．ただし，a_{10}, a_{S0} と a_{11}, a_{S1} は，Step1で各々が生成した一次分散多項式の定数項と係数である．

Step3. 避難支援情報保管サーバは乱数 sk_1 を生成し，Step2 で公開された $g^{a_{10}}, g^{a_{S0}}$ を使ってグループ公開鍵 $pk_G = g^{a_{10}} \cdot g^{a_{S0}} \cdot g^{sk_1}$ を計算し公開する．

[防災関係機関 P_i が防災関係機関 P_{i+1} の部分復号鍵を生成]

Step5. 防災関係機関 P_i は一次分散多項式 $f_i(x) = a_{i0} \cdot x + w_i$ を生成し，$f_i(x_{i+1})$ を防災関係機関 P_{i+1} に，$f_i(x_S)$ を避難支援情報保管サーバに送信する．

Step6. 防災関係機関 P_{i+1} は自身の部分復号鍵の初期値を $w_{sub} := f_i(x_{i+1})$ とする．避難支援情報保管サーバは部分復号鍵の初期値を $w_{Ssub} := f_i(x_S)$ とする．

Step7. 防災関係機関 P_{i+1} は自身の部分復号鍵 w_{i+1} をランダムに生成する．防災関係機関が既に別のグループの部分復号鍵を持つ場合，既に保持している部分復号鍵 w_{i+1} を用いる．

Step8. 防災関係機関 P_{i+1} は以下の式で $g_{i+1}(x_S)$ を計算し，避難支援情報保管サーバに送信する．

$$g_{i+1}(x) = \frac{w_{i+1} - w_{sub}}{x_{i+1}} x \bmod p$$

Step9. $g_{i+1}(x_S)$ を受信した避難支援情報保管サーバは部分復号鍵 $w_S^{(i+1)} = w_{Ssub} + g_{i+1}(x_S)$ を計算し，使用する．

防災関係機関 P_i がすでにメンバ部分復号鍵を保持する場合，Step6～Step9 の手続きを行うことにより，既に所持している部分復号鍵との単一化が可能になる．

なお，これらのプロトコルはシミュレーション評価により，現実的な時間で避難支援情報の開示と開示先の制御ができることを確認している．

4. おわりに

本稿では，暗号化された避難支援情報の復号に必要な鍵を単一化することで，防災関係機関にかかる鍵管理に関する負担を軽減するグループ秘密鍵の管理方法を提案した．

本稿で提案した方式は，迅速性が求められる従来の災害時要援護者支援システムにも適用可能と考える．

参考文献

[1] 国土交通省，国土形成計画，平成 20 年 1 月

[2] Shamir, A.: How to share a secret, Communications of the ACM, vol.22, no.11, pp.612-613, Nov. 1979.

[3] Desmedt, Y. and Jajodia, S.: Redistributing secret shares to access structures and its applications, George Mason Univ., Tech. Rep., 1997.

[4] T. Pedersen, A threshold cryptosystem without a trusted party, Proc. of Eurocrypt'91, LNCS No.547.