3V-5

災害時対応に用いるプライバシー情報共有支援のための開示先制御が容易なデータ共有方式

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

自然現象による被害を完全に防ぐことは難しく，被害を未然に防ぐ“防災”への取り組みだけでなく，被害を軽減する“減災”への取り組みが注目されている[1]．例えば，住民が通勤・通学先，その経路，時間帯，家族の連絡先といった日頃の行動範囲に関する情報（避難支援情報）を登録しておく．災害時は，防災関係機関が被災地区に該当する住民の家族に交通情報等を伝えることで，家族はそこから適切な避難行動を指示できれば，住民が誤った判断によって更なる被害に遭うことを回避できる（図1：(0)～(4)）．

我々はすでに，このような災害時の情報伝達を支援する方式と，住民の意志で避難支援情報の開示先を容易に制御できる暗号方式を提案している[2]．その暗号方式は，(1)“避難支援情報保管サーバ”を介して住民の登録情報を(2,2)閾値復号で共有する，(2) B市防災関係機関を追加する際，直近に追加されたA市防災関係機関がB市防災関係機関の“部分復号鍵”の初期値を生成する，という特徴を持つ．

災害が発生し，A市防災関係機関の情報システムが停止した状況を考える．交通機関の麻痺が理由で，A市方面に住む住民が帰宅を諦め，別方面の親戚等が住む，あるいは待機する施設のあるB市に向かう場合がある．この住民は，B市の交通情報等を得るために，B市防災関係機関を開示先に追加したい．しかしながら，文献[2]の提案方式では，B市防災関係機関を開示先に追加するには，A市防災関係機関がプロトコルに参加する必要がある．A市防災関係機関が被災により参加できない場合，住民はB市の交通情報等を得られず，B市方面で二次災害や別の災害が発生した際の情報伝達が困難になる（図1：(I)～(III)）．

本稿では，ある防災関係機関が情報システムを利用できない場合でも，円滑な情報伝達の支援を実現できるように，文献[2]の暗号方式を拡張する．

2. 災害時対応に用いる情報伝達支援のためのプライバシー情報の開示先制御が容易なデータ共有の拡張

文献[2]で，我々は避難支援情報の開示先を制御するために，“開示先の設定”，“開示先の追加”，“開示先の削除”及び“定期的な鍵更新”の4つの機能を提案している．このうち，開示先の設定，開示先の削除及び鍵更新の機能は，災害時に利用することを考えなくて良い．しかし，開示先の追加において，直近に追加された防災関係機関 i の情報システムが停止している場合，新たに防災関係機関 i+1 を追加できない．そこで，開示先追加プロトコルを拡張し，防災関係機関 i の情報システムが停止している場合は，(1) 防災関係機関 i+1 を開示先に仮追加する，(2) 住民が防災関係機関 i+1 に復号権限を委譲する，(3) 情報システムの起動後に，防災関係機関 i が処理を完了させる．なお，復号権限の委譲方法は文献[3]を参考にする．

住民，防災関係機関 i ($1 \le i \le n, n$ は住民が開示先に指定する防災関係機関の数)，避難支援情報保管サーバは x_1, x_i, x_S を識別子に持つ．住民及び防災関係機関 i は部分復号鍵 w_1, w_i を持ち，避難支援情報保管サーバは部分復号鍵 $w_S^{(1)}, \ldots, w_S^{(i)}$ を持つ．避難支援情報は住民が共通鍵 K で暗号化し，共通鍵 K を ElGamal 暗号で $(c_1, c_2) = (g^r, K \cdot e), r \in_R Z_q^*$ と暗号化する．なお，住民の公開鍵 e を用いたメッセージ m の ElGamal 暗号化は $E(e,m)$ と示す．p,q は $q \mid p-1$ を満たす安全な2素数とし，g は Z_q^* に含まれる位数が q の元である．以降のべき乗剰余演算はすべて p，指数に関する演算は q を法とする．

【拡張した開示先追加プロトコルにおける防災関係機関 i+1 の仮追加から追加完了までの流れと仮追加中の避難支援情報の復号の流れ】

[防災関係機関 i+1 を仮追加]

step1 避難支援情報保管サーバは $f_S(x) = a_S \cdot x + t,\ a_S, t \in_R Z_q^*$ を生成し，$f_S(x_{i+1})$ を防災関係機関 i+1 に送信する．

step2 防災関係機関 i+1 は $f_{i+1}(x) = a_{i+1} \cdot x + u,\ a_{i+1}, u \in_R Z_q^*$ を生成し，$f_{i+1}(x_S)$ と $E(e,u)$ を避難支援情報保管サーバに送信する．

step3 避難支援情報保管サーバは，$w_S^{(i+1)} = f_{i+1}(x_S) + f_S(x_S)$ を計算する．

step4 防災関係機関 i+1 は $w_{i+1} = f_{i+1}(x_{i+1}) + f_S(x_{i+1})$ を計算し，部分復号鍵とする．

[住民が防災関係機関 i+1 に復号権限（委任鍵）を委譲]

step5 住民は，制約条件 ϕ（例：防災関係機関 i の情報システムが応答しない間）を設定，委任鍵

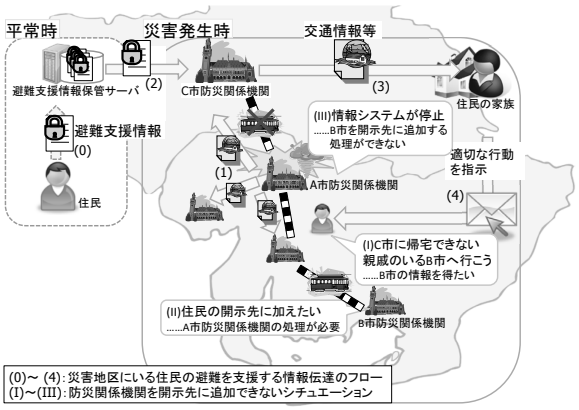

図1：被災地区にいる住民への情報伝達のフローと情報伝達ができないシチュエーション

Extension of 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

$\sigma=(\lambda_1(0)\cdot w_1-H(\phi,v),E(e,v))$ を生成し，(σ,ϕ) を避難支援情報保管サーバに送信する．ただし，$H(\cdot)$は衝突困難な一方向性ハッシュ関数，制約条件 ϕ は避難支援情報保管サーバが検証可能な記述とし，$\lambda_1(0)=-(x_S/x_1-x_S)$，$v\in_R Z_q^*$ とする．

[防災関係機関 i+1 が委任鍵で避難支援情報を復号]

step6 防災関係機関 i+1 は，避難支援情報の復号を避難支援情報保管サーバに要求する．

step7 避難支援情報保管サーバは制約条件 ϕ を検証し，成立すれば ϕ，暗号文 (c_1,c_2)，$c_1^{\lambda_1(0)\cdot w_1-H(\phi,v)}$，$c_1^{\lambda_S(0)\cdot w_S^{(1)}}$，暗号化した避難支援情報を送信する．ただし $\lambda_S(0)=-(x_1/x_S-x_1)$ とする．成立しない場合は *error* を返す．

step8 防災関係機関 i+1 は以下を計算し，避難支援情報の復号に用いる共通鍵 K を復号し，鍵 K で避難支援情報を復号する．ただし，d は e に対応する秘密鍵である．*error* を受け取った場合は終了する．

$$\frac{c_2}{c_1^{\lambda_1(0)\cdot w_1-H(\phi,v)}}\cdot\frac{1}{c_1^{\lambda_S(0)\cdot w_S^{(1)}}}\cdot\frac{1}{c_1^{H(\phi,v)}}$$

$$=\frac{c_2}{c_1^{\lambda_1(0)\cdot w_1+\lambda_S(0)\cdot w_S^{(1)}}}=\frac{c_2}{c_1^{d}}=K$$

[防災関係機関 i が防災関係機関 i+1 の追加を完了]

step9 避難支援情報保管サーバは防災関係機関 i に t と部分復号した $E(e,u)$ を送信する．

step10 防災関係機関 i は u を完全復号し，$w_{sub}=t+u$ を計算する．

step11 防災関係機関 i 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．

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

step12 避難支援情報保管サーバは $w_S'^{(i+1)}=w_S^{(i+1)}+g_{i+1}(x_S)$ を計算し，部分復号鍵とする．

3. 安全性

2 章のプロトコルの安全性について議論する．住民，防災関係機関及び避難支援情報保管サーバはプロトコル通り動作し，結託しないと仮定する．

[避難支援情報保管サーバが $t+u$, w_1,w_i,w_{i+1} を得られない]

避難支援情報保管サーバは step1～step4 で分散情報生成プロトコル[4]を実行するため，分散情報生成プロトコルの安全性より避難支援情報保管サーバは，自身の部分復号鍵 $w_S^{(i+1)}$ の秘密にあたる $t+u$，防災関係機関 i+1 の部分復号鍵 w_{i+1} を得られない．

step2 で $E(e,u)$ を得るが，ElGamal 暗号方式の安全性より u を得られない．step9 で $E(e,u)$ を部分復号するが，閾値復号の安全性より u を得られない．step11～step12 で，避難支援情報保管サーバは $g_{i+1}(x_S)$ から w_i-u を得られるが，w_i を計算するには u が，u を計算するには w_i が必要となるため，どちらも得られない．

step5 で委任鍵 $\sigma=(\lambda_1(0)\cdot w_1-H(\phi,v),E(e,v))$ を受け取るが，委任鍵から部分復号鍵 w_1 を得るには v が必要となる．v は ElGamal 暗号化されているため，ElGamal 暗号方式の安全性より，避難支援情報保管サーバは w_1 を得られない．

[防災関係機関 i+1 が $t+u$,$w_S^{(i+1)}$ を得られない，委任鍵を利用できるのは制約条件 ϕ が成り立つ間のみ]

防災関係機関 i+1 は step1～step4 で分散情報生成プロトコルを実行しているため，分散情報生成プロトコルの安全性より防災関係機関 i+1 は，自分の部分復号鍵 w_{i+1} の秘密にあたる $t+u$，避難支援情報保管サーバの部分復号鍵 $w_S^{(i+1)}$ を得られない．

防災関係機関 i+1 は $\lambda_1(0)\cdot w_1-H(\phi,v)$ と v から w_1 を計算できるが，step7 で得る $c_1^{\lambda_1(0)\cdot w_1-H(\phi,v)}$ から $\lambda_1(0)\cdot w_1-H(\phi,v)$ を得る必要がある．離散対数仮定より $c_1^{\lambda_1(0)\cdot w_1-H(\phi,v)}$ から $\lambda_1(0)\cdot w_1-H(\phi,v)$ を求めることは計算量的に困難であるため，w_1 を得られない．同様の理由で，$c_1^{\lambda_S(0)\cdot w_S^{(1)}}$ から $w_S^{(1)}$ を得られない．

委任鍵で復号する際，step7 で避難支援情報保管サーバが制約条件 ϕ を検証する．検証を通過した場合のみ復号に必要な値を得られるため，防災関係機関 i+1 が委任鍵を使用できるのは制約条件 ϕ を満たす場合のみである．

[防災関係機関 i が w_{i+1} ,$w_S^{(i+1)}$ を得られない]

step9～step10 で防災関係機関 i は，防災関係機関 i+1 と避難支援情報保管サーバが持つ部分復号鍵の秘密である u+t を得る．防災関係機関 i は step1～step2 で生成された $a_{i+1},a_S\in_R Z_q^*$ を得られないため，防災関係機関 i+1 と避難支援情報保管サーバの部分復号鍵を計算できない．

以上より，2 章で拡張した開示先追加プロトコルと委譲した権限での復号は安全といえる．

4. おわりに

台風などの自然災害で交通機関が麻痺すると，帰宅困難者が発生する．帰宅困難者は被災状況が得られない，流言やデマに混乱することがあるため，家族から情報や指示を得ることで減災に繋がると考える．本稿では，被災地区にいる住民への情報の伝達を支援する方式において，住民が登録する情報の開示先を容易に制御できる暗号方式を拡張した．この拡張により，住民は災害発生時でも開示先を追加することができるようになった．安全性を評価し，拡張したプロトコルを実行しても，各主体の部分復号鍵が他の主体に知られないことを確認した．

参考文献

[1] 内閣府：災害被害を軽減する国民運動のページ，内閣府（オンライン），入手先 <http://www.bousai.go.jp/km/>(参照 2011-12-09).

[2] 長澤 悠貴，毛利 公美，福田 洋治，白石 善明：災害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，第 4 分冊，pp.663-664(2011).

[3] 渡邊 裕治，沼尾 雅之： P2P データ共有における暗号化データのアクセス制御，情報処理学会論文誌，Vol.44，No.10，pp.2437-2443(2003).

[4] T. Pedersen: A threshold cryptosystem without a trusted party, Proc. of Eurocrypt'91, LNCS No.547, pp.522-526(1991).