

緊急時判断機能を備えた 家族間情報共有システム

長谷川 友香[†] 小口 正人[†]
[†]お茶の水女子大学

1. はじめに

東日本大震災のような災害発生時には、多数のユーザが同時にネットワークを利用するため、回線が輻輳を起し、急激に電話やメールが繋がりにくくなるという事態が発生する。このような場合には、電話やメールなどを用いた家族の安否確認は非常に困難である場合が多い。そのような状況では家族の安否の手掛かりになる情報が少しでも得られれば精神面や搜索の観点から役立つといえる。本研究ではそのような状況を踏まえ、緊急時に有用である家族間の情報共有システムを構築した。本論文ではシステムが緊急時であると判断するために用いることのできる情報とその利用方法を中心に論じる。

2. 家族間情報共有システム

2.1 概要

家族間での緊急時における情報共有を目的としたシステムである FISS(Family Information Sharing System) を構築した。そのシステム構成を図 1 に示す。

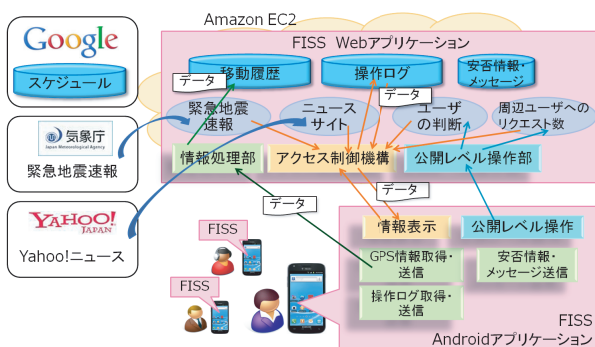


図 1: システム構成図

FISS はサーバ側とクライアント側に分かれており、サーバ側は汎用クラウドサービスである Amazon EC2 上に、クライアント側は Android 端末で動くアプリケーションとして構築している。ユーザは Android アプリケーションからシステムを利用する。

2.2 システムの機能

FISS の第一の機能は個人情報の蓄積である。この個人情報とは、家族と連絡が取れなくなった際に家族の居場所を特定したり、安否を確認したりするために有用な情報を指す。そのような情報としてさまざまなものが考えられるが、例として移動履歴、Android 端末の操作ログ、スケジュールの情報を用いることとした。各情報が、災害発生時にどこにいたか、誰と何をしていたか、いつ

まで携帯電話を操作できる状態にあったかの手掛かりになると考えられるためである。さらに、災害が起きたと判断された際にユーザに対して安否確認を行い、その際にユーザから送信される安否情報やメッセージを保存する。この安否確認にユーザが反応したかどうかとも内部情報として緊急時判断に用いる。

第二の機能は、緊急時であるという判断材料となる外部からの情報を取得することである。後述するが、緊急時であるという判断には複数の情報を用い、より信頼性の高い情報のアクセス管理を実現する。緊急時判断の材料となる情報は、これも多く考えられるが、例として緊急時になりうる状況の一つである地震に着目し、緊急地震速報とニュースサイトの記事を取り込むこととした。これらは公開されている API を用いて取得している。

第三の機能は、ユーザの Android アプリケーションの操作によって得られる、システム内部の情報を緊急時判断とアクセス制御に用いるために処理することである。ここでいう「ユーザの Android アプリケーションの操作」とは、自分の家族内のあるユーザの個人情報を見たいというリクエストを送ることである。このリクエストも緊急時判断の情報源となりうるが、リクエストがあったら常に緊急時であると判断するように用いると個人の独断で情報を見ることのできるシステムになってしまう。そのような状況を避けるために、この情報を直接ではなく何らかの処理方式に従って用いるべきであると考えられる。本論文ではその処理の方式として「階層型相互認証」と「周辺ユーザへのリクエスト数抽出」の二種類を提案する。FISS 中ではそれらを併用することとした。

第四の機能は、第二の機能で取り上げた外部情報と第一、第三の機能で取り上げた内部情報を用いて緊急時判断を行い、アクセス制御を行うことである。ここでいうアクセス制御には、情報を見せるか見せないかという制御だけでなく、どの情報を見せるかという制御も含まれる。具体的には、外部情報である緊急地震速報とニュース記事、また内部情報のうち「周辺ユーザへのリクエスト数」、「安否情報の有無」を用いて緊急時判断を行い、「階層型認証」を用いてどの情報を見せるか決めるアクセス制御を行う。

3. 緊急時判断とアクセス制御

緊急時判断とアクセス制御は図 2 の流れで行う。あるユーザの情報を見たいというリクエストがあったときにまずステップ 1 として緊急地震速報、ニュース記事あるいは周辺ユーザへの情報公開リクエスト数を用いて情報閲覧をリクエストされているユーザが危険地域にいるかを判断する。ここでいう危険地域とは災害の被害が及ぶ

Domestic Personal Information Sharing System which has a function to Detect Emergency
 Yuka Hasegawa[†] and Masato Oguchi[†]
[†]Ochanomizu University

と推定される地域のことである。ステップ2として、ユーザが危険地域にいた場合はそのユーザから安否情報が通知されているかを調べる。安否情報が通知されていない場合に、そのユーザは危険地域にあり、かつ安否がわからないという可能性が高いので、家族はそのユーザの情報を見ることができるとことになる。しかし、あくまでも可能性が高いというだけであり、実際には何の被害も被っておらず、ただ携帯電話を見ていなかったということも十分にありうる。それゆえに、該当ユーザの個人情報を一気に全て公開してしまうことは適切でないと考えられる。そこでステップ3として階層型相互認証を用いる。この階層型相互認証を用いることで先に述べたような状況で情報が見られることを防ぎ、さらに段階的な情報の公開が可能となる。

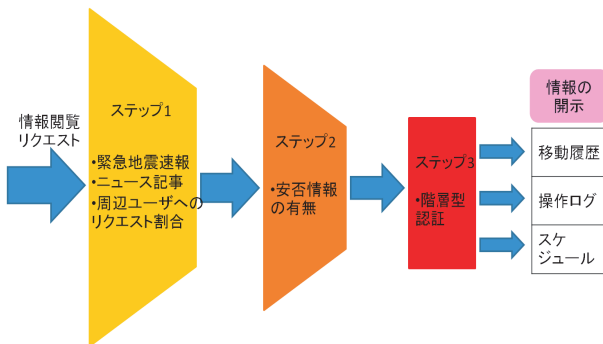


図 2: 緊急時判断とアクセス制御の流れ

4. 情報閲覧リクエストの取り扱い

2章で述べたように、あるユーザの情報を見たいというリクエストは「周辺ユーザへのリクエスト数抽出」「階層型認証」の二つの方式で処理して緊急時判断・アクセス制御に用いる。

4.1 周辺ユーザへのリクエスト数抽出

この方式は、一人のみの判断では信用度が低いが、多くの人が同様の判断をしたら信頼度は高いものとしてよいだろうという考え方に基づいている。情報を公開するようリクエストが送られたユーザ A の周りにはユーザを探し、それらのユーザにも同様にリクエストが送られているか調べる。ユーザ A の周りのユーザにもリクエストが送られている場合は、その地域は災害の被害を受ける可能性が高いとそれぞれの家族が判断しているとみなせる。そこでユーザ A は危険地域にいると判断する。

この方式のメリットは、当事者の判断ではなく第三者の判断のみを参考にするため、客観的な基準で情報の公開・非公開が決まるということである。

4.2 階層型相互認証

本論文では階層型相互認証とは、ユーザがそれぞれある階層に在るとし、同じ階層にいるユーザ同士が認証されたとして情報を互いに閲覧できる認証モデルである。各階層には個人情報が割り当てられており、同階層のユーザでその情報を互いに閲覧できる。相手を上位層に上げると、自分の階層も強制的に上位層に上がる仕様とし、これによりむやみに高い階層の情報を見ないよう抑止力

として働くと考えられる。この認証方式の詳細については [1] を参照されたい。

5. 外部情報の取得

外部情報の取得からユーザへの安否確認の送信までの流れを図 3 に示す。

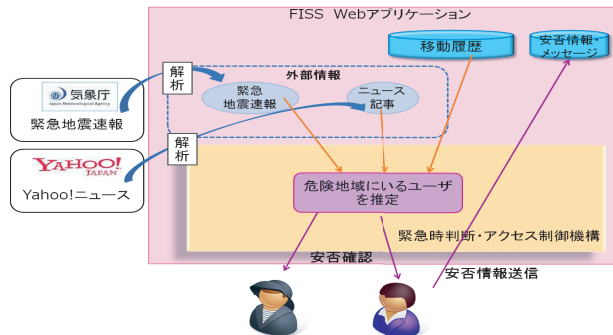


図 3: 緊急時判断とアクセス制御の流れ

5.1 緊急地震速報

気象庁から直接緊急地震速報を取得するには「予報業務許可」が必要であり、法人でなければならない。そのため Twitter 上で発表される緊急地震速報のツイートを取得することで間接的に緊急地震速報を利用した。Twitter 社の提供する「Streaming API」を利用し、緊急地震速報を流しているアカウントのツイートをリアルタイムで取得する。そのツイート内容から地震の発生位置や規模を解析し、危険地域にいると判断したユーザに対して安否確認を行う。

5.2 ニュース記事

さまざまなニュースサイトが存在するが、一例として Yahoo!ニュースを取り上げ、その記事が発行される様子を監視することとした。Yahoo!社が提供する「トピックス見出しアーカイブ API」を利用し、地震に関連するニュース記事が発行されたかどうかを一定の間隔で確認する。発行された場合はニュース記事の見出しを解析し、緊急地震速報の場合と同様にユーザに安否確認を行う。

6. まとめと今後の課題

緊急時に家族間で個人情報を共有するためのシステムを構築した。緊急時のみ情報の閲覧を可能にするための外部情報と内部情報を用いた緊急時判断手法を提案した。

今後は周辺ユーザ数の抽出に関して、どの程度のユーザがリクエストを受け取っているときに緊急状態と判断すべきかなど詳細を検討していきたい。

参考文献

[1] 長谷川友香, 小口正人, "緊急災害時に有用な家族間の個人情報共有システムの提案と実装", 情報処理学会全国大会, 2012年3月
 [2] Takeshi Sakaki, Makoto Ozaki, and Yutaka Matsuo: "Earthquake Shakes Twitter Users: Real-time Event Detection by Social Sensors", Proc.of the 19th international conference on World Wide Web 2010