緊急災害時に有用な家族間の個人情報共有システム

長谷川　友香[†1]　　小　口　正　人[†1]

緊急災害時に家族間で個人情報を共有できれば，安否の確認や捜索などの面で大いに助けになる．しかし，平常時から当人の許可なしに個人情報を閲覧できるのはプライバシの観点から問題がある．そこで本研究では，緊急時判断を行い，緊急時と判断された場合に家族間で個人情報の共有を可能とするシステムを構築することを目指す．緊急時の判断をする指標としてはユーザの操作と外部情報の二種類があると考えられる．そこでまずユーザ操作を緊急時判断に用いる仕組みとして階層型相互認証を説明し，実装例を示す．一方，外部情報としては緊急地震速報や Twitter の情報が利用できると考えられ，それらを用いたシステムの展望を示す．

A Domastic Personal Information Sharing System useful in case of Emergency

Yuka HASEGAWA[†1] and Masato OGUCHI[†1]

It's useful to share personal information between each family member in case of emergency. The information let us know where to search the lost family. However it causes privacy problems that personal information can be read without a permission in usual time. Therefore this research aims to construct a system that judge whether it's an emergency or not now and enables to share personal information between family members. To judge it's an emergensy,user operations and information from outer of the system can be used. A hierarchical mutual authentication is illustrated as a user operations factor. Eathquake Early Warning and Twitter and others can be used as external information.

†1 お茶の水女子大学
Ochanomizu University

1. はじめに

東日本大震災のような災害発生時に，真っ先に心配するのは家族の安否であろう．しかし，そのような状況では電話回線の混雑などにより家族と直接連絡を取ることは困難である．その場合，災害発生時に家族がどこで何をしていたかということを知ることができれば最適な安否の確認方法の決定や，捜索する場所の特定の上で役立つ．

近年はスマートフォンを始めとした携帯型情報機器の進歩が目覚ましく，ネットワークとストレージ技術の発展も相まって，個人の日常生活の情報，いわゆるライフログを取得し記録することは容易になってきている．例えばそのような機器のほとんどには GPS 機能が備えられており，特にスマートフォンでは比較的簡単なプログラミングにより移動履歴をログとして端末自身やサーバに記録することが可能である．

災害発生時に移動履歴情報を得ることができれば大変有用であるといえる．このような移動履歴に加え，スケジュールやメールなどの情報も家族がどこで何をしていたかを知る重要な手がかりとなる．

しかしながらこのような個人情報を平常時から許可なしに見られる状態にあるということには，家族間とはいえ抵抗があると思われる．さらに，大規模な災害時ではなくても，例えば家族と連絡が取れない場合などにスケジュールだけ閲覧したいというように緊急の度合いに合わせた情報の開示制御が実現できると望ましい．

そこで緊急時であるという判断を行い，その判断がなされた場合に特別なアクセス制御を行うシステムが必要であるといえる．緊急時の判断をする指標としてはユーザの操作と外部情報の二種類があると考えられる．ここで，ユーザの操作による緊急時の判断として階層型相互認証を取り上げる．この認証方式は，相手の情報を閲覧するためには自分も同じ情報を公開することとし，相手に自分が情報を閲覧したという通知がなされることにより平常時にむやみに相手の情報を閲覧することを抑制するという考え方の認証方式である．つまり，自分の情報を見られても構わず，さらにそれを相手に通知されてもよいとユーザが考える状況ならば緊急時であろうとシステムが判断するということである．

加えて，外部情報による緊急時判断も可能である．本研究では外部情報には大きく分けて二種類あると考える．まず，緊急地震速報やニュースサイトなどのオフィシャルな情報である．これらは信憑性が高いが，地域に根差した情報ではなく，場合によっては速報性が低いという欠点が見られる．二つ目に考えられるのが Twitter といった SNS から得られるソーシャルな情報である．これらはだれでも発信できるため信憑性は比較的低いが，地域に根差

したきめ細やかな情報を迅速に取得できるという利点がある．そこで本研究ではこれらの情報を複数組み合わせて緊急時判断を行うことを検討し，欠点を補いあってより正確な判断を目指す．

2. 緊急時に有用なシステムの要件と位置づけ

緊急時に有用な個人情報共有システムの要件としては，一つには緊急時のみ情報の閲覧が可能であるという点，もう一つには緊急度に合わせた制御を行えるという点が挙げられる．これらの条件を満たすためには，外部情報とユーザ操作からの情報を組み合わせて緊急時判断を行う必要がある．外部情報からは緊急時と判断されない，例えば家族が行方不明になったというような状況ではユーザ操作の情報から緊急時判断を行う必要がある．この場合はプライバシを考慮すると，比較的プライバシレベルの低い情報のみ閲覧可能にするほうが良いと考えられる．逆に大震災といった生死にかかわるような緊急事態ならユーザ操作なしにすべての情報を公開することが有用であると考えられる．

このように，緊急時かどうかは家族の状況によって異なり，さらにどのような場合にどの情報まで公開するかという基準も家族の方針によると考えられる．そのため，本研究で構築するシステムは家族単位で制御を行うものと考え，あらかじめ家族内でセキュリティポリシを定めることとしている．そのため，通常の認証とは異なり，緊急時には自分の情報を見せることに同意しているものとして情報を取り扱うこととする．また，このシステムを使用する目的は緊急時に家族を捜すため，もしくは自分を捜してもらうためであり，悪意のない利用を想定している．悪意のある利用とは，例えば自分の個人情報としては見られても問題のないダミーの情報を登録しておき，相手の情報を取得しようとするといった利用である．このシステムを不特定多数のユーザがアクセスする情報共有システムとして用いる場合はこのような悪意のある利用が頻発することが考えられるが，家族間のシステムではこのようなことを行うと緊急時に自分の正しい居場所を家族に伝えられなくなり，自分にとっても相手にとっても非常にデメリットが大きいため，ダミーの情報を登録するということは考えないものとしている．緊急時判断の性質上，完全に正確な判断というのは不可能であると考えられるが，このような家族間という特別なグループ内では有効に機能するシステムとして提案する．

3. ユーザ操作により緊急時判断を行うシステム

本章では，ユーザ操作により緊急時判断を行い，情報閲覧を可能にするシステムについて説明する．ユーザ操作により緊急時判断を行うために階層型相互認証を用いる．

3.1 階層型相互認証

本研究における階層型相互認証とは，ユーザ各々が認証レベルを保持し，その認証レベルが同じユーザどうしは互いに相手の情報を閲覧可能なものとし，認証レベルが異なる場合には互いに閲覧不可とする認証方法である．本研究では認証レベルを一人のユーザが一つ保持するものではなく，各ユーザが他のユーザに対して一つずつ保持するものとした．例えば，ユーザ A〜C の 3 名間の認証において，ユーザ A はユーザ B に対して認証レベルを一つ保持し，ユーザ C に対しても認証レベルを一つ保持する．さらにユーザ B はユーザ A と C に対して保持し，ユーザ C はユーザ A とユーザ B に対して保持するという具合である．これらの認証レベルは互いに独立しており，例えばユーザ A がユーザ B に対する認証レベルを変更したとしてもユーザ C に対する認証レベルには影響しない．

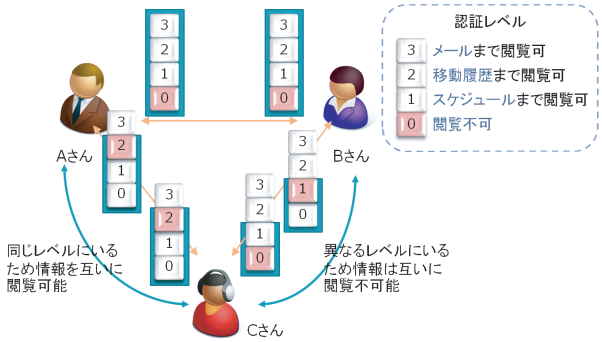

図 1 階層型相互認証の概要図

この認証レベルに個人情報を割り当てる．本研究の実装では一例として，図 1 にあるようにレベル 0 は閲覧不可，レベル 1，2，3 はそれぞれスケジュール，移動履歴，メールまで閲覧可能という割り当てを行った．

自分の認証レベルは基本的に自由に設定可能であり，それによって相手に対して公開する自分の情報を制御することができる．例えばユーザ A がユーザ B に対する認証レベルを 1 としており，ユーザ B がユーザ A に対する認証レベルを 1 としたならユーザ A と B は互いに相手のスケジュール情報を閲覧できる．ユーザ B がユーザ A にスケジュールを公開したくない場合にはユーザ A に対する認証レベルを 0 とすることで互いに何の情報も閲覧で

きない状態になる．

このように平常時は情報公開の制御は当人が行えば良いが，緊急時にはこの方法は動作しない場合がある．あるユーザが無事か確認するために情報を得たいのに，そのユーザの許可がなければ情報を閲覧できないという矛盾が生じてしまう．そこで，緊急時には認証レベルに関して次のような操作を行う．まず，情報を閲覧するユーザ（以下，閲覧ユーザ）が閲覧対象のユーザ（以下，被閲覧ユーザ）の認証レベルを任意のレベルまで上げる．そうすると閲覧ユーザの被閲覧ユーザに対する認証レベルも自動的に同じレベルまで上がり，被閲覧ユーザに対して認証レベル変更を通知するメールが送られる．こうすることで閲覧ユーザと被閲覧ユーザの互いに対する認証レベルが同じになるため，情報の閲覧が可能となる．閲覧ユーザの認証レベルが自動的に上がり，被閲覧ユーザに通知が送られることで，通常時にこの操作を行うことへの抑止力になると考えられる．つまり，自分の情報を公開してまで他の人の認証レベルを上げるということは緊急時であるとみなすということである．

この認証方式の特徴として，特権ユーザが存在しないという点が挙げられる．全ての情報を閲覧できてしまう特権ユーザが家族内に存在すると，情報を閲覧されたくないという気持ちから，システム自体が使用されなくなる可能性が高いと考えられるためである．

4. 階層型認証を用いた個人情報共有システム

4.1 認証の取り決め

本提案方式では認証の基本的な取り決めとして以下のものを採用している．

基本的な取り決め
- ・相手のレベルを上げると自分も同じレベルまで上がる
- ・設定した最大値より上には上げられない
- ・自分と相手のレベルの低いほうに該当する情報まで互いに閲覧可能

さらにユーザは，相手の認証レベルを変更していない状態，相手によって自分のレベルを変更された状態，自分が相手のレベルを変更した状態の 3 状態を持ち，その状態に従って可能な操作が決まる．各ユーザから見た状態遷移の様子を図 2 に示す．

通常は「変更なし」状態におり, 自分のレベルを変更しても状態は遷移しない.「変更なし」状態から遷移が起こるのは自分が相手のレベルを上げた場合か，相手が自分のレベルを上げた場合，つまり自分以外の認証レベルの操作が行われたときである．

まず，自分が相手のレベルを上げた場合は「自分が相手のレベルを変更」状態に遷移する．

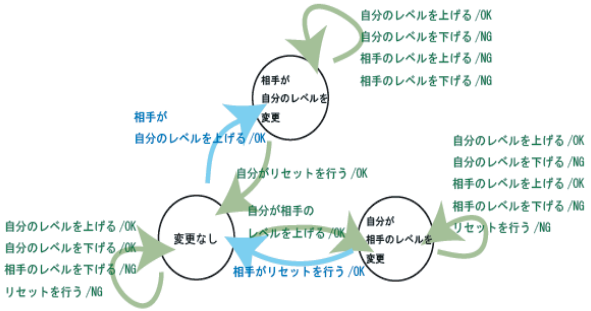

図 2 認証レベルの変更に関する状態遷移図

この状態と「変更なし」状態の相違点は，自分のレベルを下げることができない点である．これは相手のレベルを上げておいて自分のレベルを下げることができると，相手だけを高いレベルにとどまらせることになり，相手が不利な状況を作り出すことが可能になるためである．相手がリセット操作を行うことにより,「変更なし」状態に遷移し，再び自分のレベルは自分で自由に設定できるようになる．

相手が自分のレベルを上げた場合は「相手が自分のレベルを変更」状態に遷移する．この状態と「変更なし」状態の相違点は自分のレベルを下げられない点，相手のレベルを上げられない点，リセット操作を行える点である．相手にレベルを上げられた場合は自分のレベルは下げることができず，リセット操作を行うことになる．リセット動作を行うことで「変更なし」状態に遷移する．

「自分が相手のレベルを変更」状態で相手のレベルを上げられるのに,「相手が自分のレベルを変更」状態では相手のレベルは上げられない．これは,「自分が相手のレベルを変更」状態では，ある情報まで閲覧したが有用な情報が得られなかった場合にもう一段階レベルを上げたいということが考えられるが,「相手が自分のレベルを変更」状態では，それからまた相手のレベルを上げたいという状況になってもリセット操作をしてから相手のレベルを上げることが可能だからである．

このように，レベルを変更されたユーザだけがリセット操作を行うことができる．この遷移図は自分から見た場合であり，相手側の制御を考える場合には相手と自分を読みかえればよい．

状態に対応する取り決めをまとめると以下のようになる．

全状態で共通の取り決め
・自分のレベルを上げられる
・相手のレベルを下げられない
「変更なし」状態での取り決め
・自分のレベルを下げられる
・相手のレベルを上げられる
・リセット操作が行えない
「自分が相手のレベルを変更」状態での取り決め
・自分のレベルを下げられない
・相手のレベルを上げられる
・リセット操作が行えない
「相手が自分のレベルを変更」状態での取り決め
・自分のレベルを下げられない
・相手のレベルを上げられない
・リセット操作が行える

4.2 システム構成

システムの構成を図 3 に示す．

Google App Engine 上に個人情報共有システムを作成し，この上でユーザ認証と個人情報へのアクセス制御，個人情報の蓄積などを行っている．ユーザからデータのリクエストがあると，アクセス制御部はユーザのアカウント情報と認証レベルを参照し，そのユーザがそのデータに対してアクセスの権限があるかの認証を行う．アクセス可能と判断されると，該当するデータを取得し，ユーザに提示する．ユーザにアクセスする権限がない場合にユーザは他のユーザの認証レベルを変更してアクセスできるようにする必要がある．この処理もアクセス制御部が行い，レベルが変更されたユーザに対してその旨のメールを送信する．

情報の閲覧と後述する移動履歴の取得には Android 端末を用いている．

4.3 個人情報へのアクセス

本システムで扱う個人情報はスケジュール，移動履歴，メールの 3 種類である．通常の利用であればこれらの情報にアクセスするのは本人だけであるが，情報共有のためにはシステムからアクセスする手法が必要になる．それぞれの情報へのアクセスの実装方法を以下に

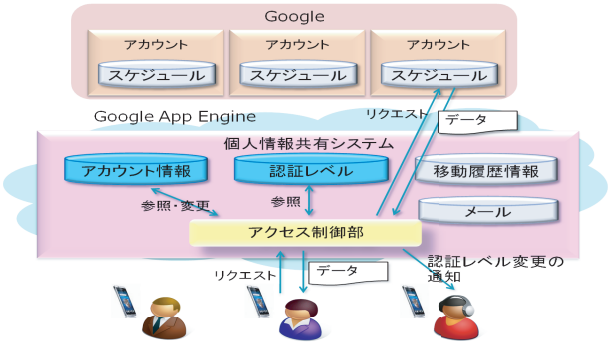

図 3 システム構成図

示す．システムから各ユーザの個人情報へのアクセスを可能にした上で，認証を行ってそれらの情報へのアクセスを制御する．家族内に特権ユーザは存在せず，システムが認めたレベルまでの情報を互いに閲覧可能となる．

4.3.1 スケジュール

スケジュール情報としては，Google Data API を用いて Google カレンダーの情報を取得する．Google Data API とは REST 形式でカレンダーやマップなどの Google のリソースを操作できる API である．本システムでは，この API を用いるに当たり OAuth 認証を行う．OAuth 認証とは，あらかじめ信頼関係を構築したサービス間でユーザの同意のもとにセキュアにユーザの権限を受け渡しする「認可情報の委譲」のための仕様である．本システムの初回利用時にユーザがシステムに対して Google カレンダーへのアクセス権限を委譲し，システムはそれ以降その権限使って個人のカレンダー情報を取得することができる．

4.3.2 移 動 履 歴

移動履歴は Android 端末で GPS を使って取得する．具体的には，Android 端末で動くアプリケーションを作成し，一定時間ごとに現在地の緯度と経度を取得してサーバに送信させる．サーバはその情報を蓄積し，閲覧のリクエストがあった場合には Google Map 上に位置を線でつないで表示する．

4.3.3 メ ー ル

メールは転送設定を行い，クラウド上のアプリケーションで受信して蓄積する．本システムでは Gmail からの転送を想定して実装している．

4.4 使 用 例

図 4 に情報の閲覧画面を示す．

左から，ユーザ一覧画面，メール閲覧画面，移動履歴閲覧画面，スケジュール閲覧画面である．ユーザ一覧画面から認証レベルの変更操作を行う．閲覧できると判断された情報はリンクが表示され，そこから閲覧画面に遷移するようになっている．

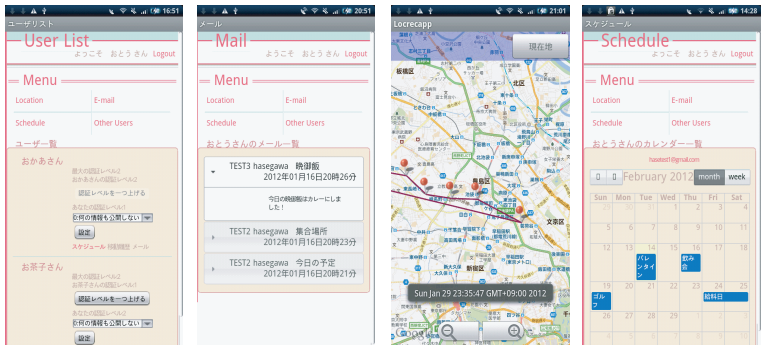

図 4 Android アプリケーション使用画面

5. FISS(Family Information Sharing System)

前章ではユーザ操作により緊急時判断を行うシステムについて説明した．ここから，ユーザ操作に加えて外部情報を緊急時判断材料として取り入れた，より実用的なシステム FISS(Family Information Sharing System) を提案する．

5.1 システム構成

システムの構成を図 5 に示す．本システムでは，外部情報として緊急地震速報やニュースサイトなど公的機関の発行する情報とマイクロブログなどの SNS 情報を取り入れて緊急時の判断材料にする．これらの情報は利用する前に解析して使いやすい形に変える必要があるので，情報解析部に情報を収集し，それを緊急時判断部に渡して緊急時かどうかの判断を行い，緊急時ならばアクセス制御部に通知を行う．アクセス制御部は緊急モードでアクセス制御を行うようにする．これにより，ユーザの操作だけで緊急時判断をする場合に比べ，平常時に個人情報を閲覧される可能性が低い，より実用的なシステムを実現できる．

さらに，プラットフォームを Google App Engine から AmazonEC2 に変更する．この

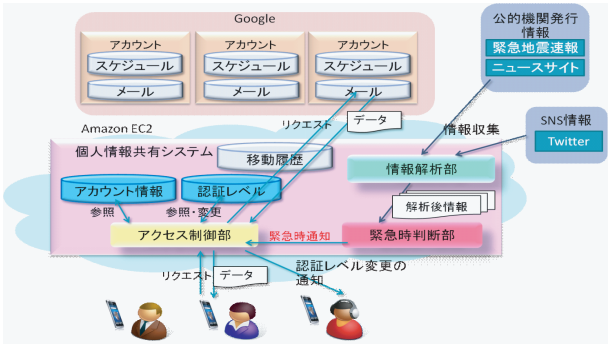

図 5 FISS のシステム構成図

変更の理由は，Google App Engine は PaaS であるのに対し，AmazonEC2 は IaaS であるというところにある．IaaS を用いることでデータを実際にどのデータセンタに保存するかやシステムの構成などをより柔軟に変化させることができると考えられる．これにより，緊急時判断をユーザ認証だけでなくデータの場所やシステムの構成にも適応させて緊急時に動的に変化するシステムを構成できると思われる．

5.2 外部情報の取得

外部情報はオフィシャルな情報とソーシャルな情報の二種類に分けて考える．オフィシャルな情報には，気象庁の発する緊急地震速報や警報・注意報，メディアの発するニュースなどが含まれる．ソーシャルな情報には Twitter や Facebook などの SNS の情報が含まれる．これらの情報の特徴を表 1 に示す．

表 1 外部情報の特徴

	信憑性	速報性	情報のきめ細かさ
オフィシャルな情報	高い	種類による（速くても正確性が低い場合あり）	比較的低い
ソーシャルな情報	低い	高い	高い

公的機関の発行する情報は信憑性が高いが，速報性に欠けるという欠点がある．緊急地震速報などは速報性があるが，情報の正確性が低いということもありうる．（東日本大震災の第一報の緊急地震速報の予測震度は 1 であった．）また，地域に根差した情報という点では SNS の情報に比べるときめ細かさが低いといえる．SNS の情報はどんな人でも情報を発信

できるために信憑性は低いが，同時にそれは速報性を高くするということを意味する．また，地域に根差したきめ細かな情報を得ることができる．

これらの点から，複数の情報源を用いて緊急時判断をすることで欠点を補いあえ，精度の高い判断ができると期待する．これらの情報それぞれに対して適切な解析を行い，実際の判断に用いることができるものに変換する必要がある．

近年，Twitter について多くの研究がなされている．ある話題に関するメッセージ検出[1)]やリアルタイムに要約を生成するシステムの開発[2)]などが挙げられる．Twitter はソーシャルな情報が取得可能であるというだけでなく，緊急地震速報などをリアルタイムにツイートするアカウントも存在しているため，オフィシャルな情報の取得にも Twitter が活用可能であると考えられる．Twitter のツイートの収集のために StreamingAPI が提供されており，ツイート自体は比較的容易に取得が可能である．これらの点から，Twitter を用いて外部情報を取得し利用することは現実的であるといえる．そこで，FISS に実装する外部情報の取得と解析の機構として図 6 を提案する．

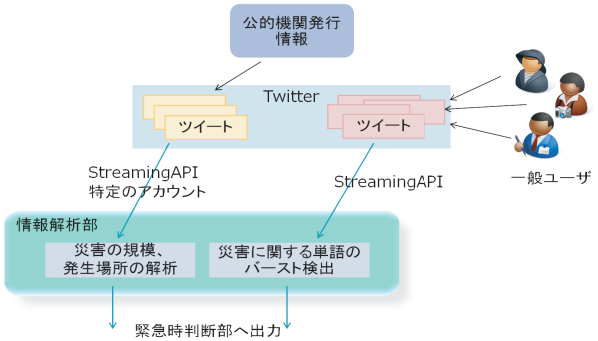

図 6　情報解析部概要図

オフィシャルな情報に関しては，その情報がツイートされているアカウントを FISS に登録しておき，StreamingAPI を用いてそのアカウントのツイートを取得する．ツイート内容を解析し，災害の規模や発生場所を抽出して，緊急時判断部に出力する．

ソーシャルな情報に関しては，一般ユーザのツイートを取得し，災害に関する語句のバースト検出を行う．バーストとは，データストリームにおけるイベントの異常な集中発生のことである．「地震」や「津波」など災害に関する単語は平常時はある程度の数のツイートでしか用いられないが，災害時にはそれらの単語を用いたツイートが急激に増えると予想される．このような特定の単語に関するリアルタイムバースト検出手法は蝦名らによってすでに提案されており，その有効性も検証されている．[3)] また，ツイートの際の GPS による位置情報から地震の発生場所を検知し，警告を発する研究[4)]もなされており，位置情報から緊急時となっている地域の検出も考えられる．

また，ソーシャルな情報には信憑性が低いという欠点があるため，情報が信頼できるものかを判断する必要もあるといえる．マイクロブログ上での流言検出の研究[5)]もなされているので，信憑性の低さにも対応できるシステムの構築を目指したい．

6. ま と め

緊急時に有用な家族間情報共有システムにおいては，緊急時判断が必要であり，その判断材料としてユーザ操作による情報と外部情報が考えられる．ユーザ操作に関しては階層型相互認証機構を実装し，相手の認証レベルを変更する場合に緊急時であるとみなすものとした．外部情報についてはオフィシャルな情報とソーシャルな情報を組み合わせて緊急時判断を行うことが正確性を高める上で望ましいと考えられ，どちらも Twitter から情報の取得が可能である．階層型相互認証機構を備えたシステムの実装を行い，これをより実用に近づけた，複数の情報から緊急時判断を行う情報共有システム FISS を提案した．

7. 今後の課題

FISS の実用化に向けて情報解析部と緊急時判断部の実装を行う．情報解析部については Twitter を用いてオフィシャルな情報とソーシャルな情報を取得して判断材料となる形で出力できるようにする．また，緊急時判断部については緊急時であるという判断を下すためにそれらの出力をどのように組み合わせていくべきなのか考察し，実装していく．

謝　　辞

本研究は一部，独立行政法人情報通信研究機構の委託研究「新世代ネットワークを支えるネットワーク仮想化基盤技術の研究開発・課題ウ　新世代ネットワークアプリケーションの研究開発」によるものである．

参 考 文 献

1) 山本祐輔，及川孝徳，山名早人: ”字幕テキストの利用によるマイクロブログからのテレビ番組に言及したメッセージ検出手法”，DEIM Forum 2011
2) 坂本翼，横山昌平，福田直樹，石川博: ”マイクロブログを対象としたリアルタイムな要約生成システムの試作”，DEIM Forum 2011
3) 蝦名亮平，中村健二　小柳滋:” リアルタイムバースト検出手法の提案”，日本データベース学会論文誌，Vol.9，No.2, pp.1-6,2010 年 11 月
4) 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
5) 藤川智英，鍛冶伸裕，吉永直樹，喜連川優: ”マイクロブログ上の話題抽出とユーザの態度の分類に基づく流言検出支援システム” ，DEIM Forum 2012