ソーシャルメディアでの災害情報共有における登録ボランティアを活用したクラウドソーシング型信頼性検証

北川 沢水[†,*] 大木 哲史[†] 小泉 佑揮[‡] 河辺 義信[‡‡] 長谷川 亨[‡] 西垣 正勝[††]

概要：近年，ソーシャルメディアが災害時情報伝達に有用であることが認識されつつある．一方で，ソーシャルメディア上に氾濫する情報は玉石混交であり，雑多な情報の中から信頼性の高い必要な情報を取捨選択することは容易ではない．災害時には，いち早く正確な情報を収集し，迅速な対応をしなければならない．そこで，情報の信頼性を確保する方法として，我々は，メッセージの中から内容が一貫している情報のみを自動抽出する「ソーシャルメディエンジン（SME)」を開発するとともに，ボランティアにメッセージの真偽の確認を依頼する「クラウドソーシング型信頼性検証」の基盤を運用する方式を提案している．これにより，ソーシャルメディアから信頼のおけるメッセージのみを抽出可能になると期待される．本論文では，クラウドソーシング型信頼性検証について，信頼のおけるボランティアが担う役割とクラウドソーシングの仕組みに着目し，効果的な構成方法を明らかにしていく．これにあたり，嘘の報告を行った者に罰を与える懲罰型抑止力方式，コミュニティ全体に働く暗黙的なムードを活用した意識型抑止力方式，対面作業者間に働く同調圧力を活用した圧力型抑止力方式の 3 つの方式を取り上げ，アンケートとシミュレーションを通じて分析を行う．

キーワード： 災害時通信，トラスト，クラウドソーシング，ソーシャルメディア，プライバシー

Reliability Verification for Disaster Information Sharing on Social Media Using Crowd-Sourcing with Registered Volunteers

Takumi KITAGAWA[†,*] Tetsushi OHKI[†] Yuki KOIZUMI[‡]
Yoshinobu KAWABE[‡‡] Toru HASEGAWA[‡] Masakatsu NISHIGAKI[††]

Abstract: In recent years, it has been recognized that social media is useful for dissemination of disaster information. On the other hand, the information flooded on social media is all mixed up, and it is not easy to select the reliable and necessary information from the miscellaneous information. In the event of a disaster, we must collect accurate information and respond quickly. As a way to ensure the reliability of information, we develop a Social Medi-Engine (SME) that automatically extracts only consistent information from the messages, and propose a method of "crowdsourcing reliability verification" that asks volunteers to verify the authenticity of the messages. This is expected to make it possible to extract only trustworthy messages from social media. This study focuses on the second stage of crowdsourcing, focusing on the role played by trusted volunteers and the mechanism of crowdsourcing to identify how to structure it effectively. We take up three methods: Punishment method to punish those who report lies; direct deterrence method, which utilizes the eyes of someone in a neighboring group; and indirect deterrence method, which utilizes peer pressure in a positive direction, and analyze them through questionnaires and simulations.

Keywords: emergency communication, trust, crowdsourcing, social media, privacy

1. はじめに

近年，自然災害の甚大化にともない，人々の災害に対する意識が向上しつつある．災害時においては，「黄金の 72 時間」と呼ばれる災害初期に，消防，警察などの救助隊員が被災者や被災状況に関する最新の情報を収集し，被災者を迅速に救出することが重要である．しかし，災害現場における複数のレスキュー組織間での情報共有の難しさ，災害時における電話網（119 番通報などの高信頼な通信インフラ）の輻輳や障害による機能不全などが原因で，迅速で最適な救助活動の実現は非常に困難な課題となっている．

一方で，電話網と比較してインターネットは耐障害性が高いことが知られており，Twitter などのソーシャルメディアを用いた被災情報の伝達が有用である事が認識されつつある．ソーシャルメディアは全ての参加者から各個のリアルタイムな情報を集約できるという利点もあるため，地方公共団体においても災害時対応のためのソーシャルメディア活用率は年々増加している[1]．2019 年 10 月に発生した台風 19 号による豪雨によって被害を受けた長野県は，Twitter を活用し独自に救助要請を収集することで約 50 件の救助に繋げることができた[2].

†静岡大学大学院総合科学技術研究科，Graduate School of Integrated Science and Technology，Shizuoka University
‡ 大阪大学大学院情報科学研究科，Graduate School of Information Science and Technology，Osaka University
‡‡愛知工業大学情報科学部，Department of Information Science，Aichi Institute of Technology
†† 静岡大学創造科学技術大学院，Graduate School of Science and Technology，Shizuoka University
* kitagawa.takumi.15@shizuoka.ac.jp

しかし，ソーシャルメディアを災害時通信インフラとして用いるには，ソーシャルメディア上の情報の信頼性の問題が存在する．一般に，他のメディアと比べてインターネット上の情報の信頼度は低いといわれている[3]．とりわけソーシャルメディアにおいては雑多なユーザと情報が氾濫しており，その中から信頼性の高い情報のみを選択することは困難である．この課題に対し，本研究では，登録ボランティアとクラウドソーシングを活用して，災害時にソーシャルメディア上の情報の信頼性を検証する仕組みについて議論する．

2. ソーシャルメディアを用いた災害時通信の信頼性確保に向けての課題

高信頼な災害時通信を実現するためには，信頼できる発信者やメッセージを特定することが重要である．これに対し，ボランティア（現地にて物理的な支援を行うオンサイトボランティア，情報発信を通じて支援を行うオンラインボランティア）や被災者が発するメッセージは，不正確性や不確定性をはらんでいる．たとえば，ボランティアや被災者は，時として利己的な判断により嘘のメッセージや，いたずらのメッセージを意図的に送信する可能性がある．また，時々刻々と変化する災害状況下においては，ある時点で事実であると確認された状態が長期間にわたって続く保証はない．こうした状況下においては，いかにメッセージの真偽を評価・確認するかが問題となる．さらに，災害により電話網やインターネットの分断が発生する可能性がある．Peer-to-Peer 通信あるいは遅延耐性通信によって限定エリア内でのメッセージの送受信は可能であったとしても，SIP サーバや PKI 認証局との通信は困難であり，SIM 情報や公開鍵証明書に基づくメッセージ送信者の身元確認は不可能であることが想定される．こうした状況下においては，事前登録されていないボランティア，被災者に対する一時的な信頼を管理することも必要になる．

従って，災害時に信頼の確保と管理をするためには，以下のような課題を解決しなければならない．

① 災害現場に流れる雑多なメッセージの中から信頼性の高いメッセージをどのように抽出するか
② ネットワーク分断時，認証手段が利用できない状況下において，メッセージ発信者の信頼性をどのように確保するか
③ 時間的に変動する信頼度をどのようにモデル化するか

課題①は，ソーシャルメディアに流れる「メッセージに対する信頼性」をいかに確保するかという課題である．メッセージの一貫性（複数の発信源からの異なるメッセージが矛盾していない）を確認するという方法が課題①の解決に対する一助となるが，フェイクニュースが多数のユーザにリツイートされるような状況にも対処するためには，目視（真偽を人間の目で確認する）の仕組みを併用できることが望ましい．オンラインショップで販売されている商品に対しては，当該商品を購入したユーザからのレピュテーションを集約するという形で，目視の仕組みが運用されている．しかし，レピュテーションの集約には時間がかかるため，状況の変化が速い災害情報の信頼性を確認するための手段として利用するには，何らかの工夫が必要である．

課題②は，ソーシャルメディアに情報を発信する「人に対する信頼性」をいかに確保するかという課題である．情報発信者の信頼性を確認することができれば，ソーシャルメディアに虚偽のメッセージが発信されること自体を予防することが可能であり，かつ，発信者の結託やシビル攻撃などの周到な虚偽情報発信にも対抗できる．しかし，被災の渦中において被災者やボランティアの全員にユーザ登録を求めるようなことは不可能に近い．また，たとえ被災者やボランティアが事前に認証用情報を入手していたとしても，災害時には携帯電話網や PKI 認証局との通信が保障されないため，メッセージの受信者が送信者の認証用情報を取得することができず，送信者ならびにメッセージの検証が不能となる可能性がある．

課題③は，ソーシャルメディアに流れたメッセージに関する「信頼性の時間的推移」をどう扱うかという課題である．災害地では状況が刻々と変化する．このため，発信された時点では正しい情報であったメッセージであっても，数時間後には間違った情報になってしまう可能性がある．このような情報の「鮮度」を，情報の信頼度の中に組み込んでいく必要がある．

現在，我々は，上記の 3 つの課題のうち，課題①および課題②を解決する仕組みを検討している段階である[4]．課題①は，ソーシャルメディアに流れる複数のメッセージの中から内容が一貫している情報のみを自動抽出する「ソーシャルメディエンジン（SME）」を開発するとともに，ボランティア（現地にて物理的な支援を行うオンサイトボランティア）にメッセージの真偽の確認を依頼する「クラウドソーシング型信頼性検証」の基盤を運用することで，これに対応する．課題②は，身元確認に応じてくれるボランティアに対しては，自身を特定できる情報（以降，本人情報）を現地の救助隊員に一時的に登録する制度を導入するとともに，少数の登録ボランティアが多数の匿名ボランティアの行動変容を促すことによって，クラウドソーシング型信頼性検証の精度を効果的に高めることで，これに対応する．

本稿では，このうち，クラウドソーシング型信頼性検証基盤における「少数の登録ボランティアが多数の匿名ボランティアの行動変容を促進させる方法」に関して検討を行った．具体的には，虚偽報告者に罰を与える「懲罰型抑止力方式」，コミュニティ全体に共有される同調意識を利用した「意識型抑止力方式」，対面作業者間に働く同調圧力を利

用した「圧力型抑止力方式」について取り上げ，今後の比較分析方法を論じる．

3. 信頼性検証システム

3.1 概要

災害時，いち早く正確な情報を収集し迅速な対応を行うための手段として，我々は，ソーシャルメディエンジン（SME）とクラウドソーシング型検査による 2 層式の情報クレンジングを提案している[4]．SME は，ソーシャルメディアに流れる複数のメッセージの中から内容が一巻している情報のみを自動抽出する．災害現場に集まったボランティアは，クラウドワーカとして，SME から出力された情報の真偽を目視により確認する．

このようなクラウドソーシング型の情報クレンジングが効果的に機能するためには，虚偽報告を行うボランティアは居ないという前提が必要である．しかし，ボランティアが匿名である場合などには，この前提が常に満たされるとは限らない．ボランティアの身元確認を徹底することができれば，身元が割れていることが虚偽報告を行うにあたっての抑止力になり得る．しかし，災害時に全ボランティアに身元確認を強制するようなことは，確認する側にとってもされる側にとっても手間や心的負担が過大となるため非現実的である．

そこで，身元確認に応じた一部のボランティア（登録ボランティア）が，他の身元確認をしていないボランティア（匿名ボランティア）の作業内容を確認する仕組みを取り入れる．登録ボランティアは，身元が割れていることが虚偽報告を行うことに対しての抑止力となる．匿名ボランティアに対しては，匿名ボランティアに見られていることが虚偽報告を行うことに対しての抑止力となる．この結果，身元確認が課せられるボランティアの人数を抑えつつ，確度の高い情報クレンジングが達成されることが期待できる．我々が提案する信頼性検証基盤のイメージを図 1 に示す．

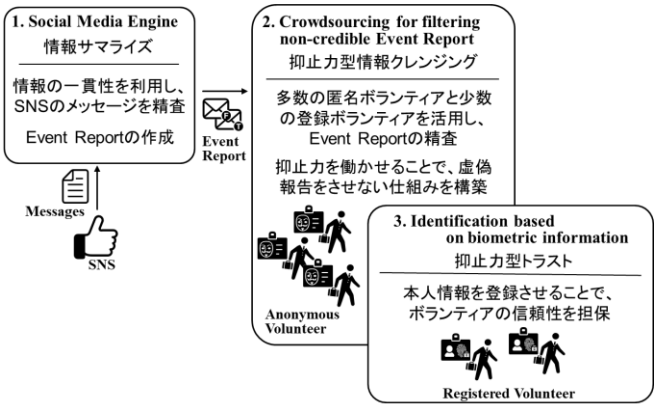

図 1　信頼性検証システム

3.2 情報サマライズ：SME による一貫性を有するソーシャルメディアメッセージの抽出

ソーシャルメディアエンジン（SME）は，ソーシャルメディアメッセージをパースし，テキストマイニング技術によって，ソーシャルメディア上の被災地に関する情報を抽出した上で，時間，場所，内容に応じて分類してアイテム化する．Twitter のリツイートによって拡散した情報など，同一内容のメッセージについては縮約され，独立したアイテムごとに個々の「Event Report」としてまとめられる．ソーシャルメディアに流れる情報は玉石混合であるため，この段階の Event Report には誤った情報も含まれている．そこで, 次の段階で 匿名ボランティアと登録ボランティアによって，Event Report の真偽の確認を行う．

3.3 抑止力型情報クレンジング：クラウドソーシングによる Event Report の真偽確認

ソーシャルメディアエンジン（SME）から出力された Event Report は, クラウドソーシングシステムに投入され，個々の Event Report に関する「真偽の確認」がジョブとして公開される．被災地に到着したボランティア（匿名ボランティアおよび登録ボランティア）は，クラウドソーシングシステムにアクセスすることによってジョブ（Event Report）の一覧を確認する．その中から，自分の状況あるいは目的に合致した Event Report（例えば，現在の自分の所在地近辺の Event Report や，報奨金額が高い Event Report）を選び，その真偽確認を自らのジョブとして受注する．ボランティアは Event 発生地点に直接赴き，Report 内容の真偽を目視によって確認し，その結果をクラウドソーシングシステムに報告する．

一般的にソーシャルメディアに流れるメッセージは多量のため，ソーシャルメディアエンジンから出力される Event Report も相応の数となることが予想される．莫大な量の Event Report の真偽を判断していくには，ボランティア（クラウドワーカ）を十分に確保する必要がある．そこで，ボランティアには匿名での参加を許し，正しい報告を行った際に報酬（以降，コイン）を授与する．ボランティアのインセンティブを更に高めるために，コインを現金通貨と換金可能にすることも一案であろう．

ただし，匿名ボランティアに関しては，その匿名性から，Event 発生地点に赴かずに報告だけを行い，不正にコインを獲得しようとする者が現れる可能性がある．匿名性はまた，結託あるいはシビル攻撃などのボランティアによる周到な不正に対してもその温床となる．そこで我々は，登録ボランティアを「匿名ボランティアの不正に対する抑止力」として活用する．本研究ではこれを「抑止力型情報クレンジング」と呼称する．具体的には，登録ボランティアが匿名ボランティアの作業内容を確認する仕組み（その具体的な方法については次章で詳述する）を取り入る．虚偽報告

が発覚した匿名ボランティアに対しては，4 章に記載する方式ごとに違いはあるものの，その時点で当該ボランティアの ID とコインを抹消・没収するといった懲罰，もしくは信頼性の低下や報酬の減額などペナルティが課せられる．災害活動中に虚偽報告を行わなかった匿名ボランティアのみが，災害終息後にコインを現金通貨に換金することができる．

3.4 抑止力型トラスト：登録ボランティアの信頼性の担保

登録ボランティアは本方式における信頼の砦であり，虚偽の報告を行うことがないということが大前提となる．そこで我々は，身元確認に応じたボランティアのみを登録ボランティとして採用する．身元が割れているため不正が発覚した場合には自分が特定されてしまうことが，虚偽報告を行うことに対しての抑止力となる.本研究ではこれを「抑止力型トラスト」と呼称している[5].

被災地では電話網やインターネットの断絶が予想されるため，ボランティアの本人情報の登録は近距離通信を用いて行われる．災害現場には，警察署や消防署などからも多くの署員や隊員（以降，救助隊員）が参加している．登録を希望するボランティアは，自身の本人情報を被災地にて救助隊員に受け渡す．救助隊員はボランティアを目視で確認した上で，ボランティアに PKI 秘密鍵と PKI 公開鍵証明書を発行する．登録ボランティアは，PKI 秘密鍵によって署名を付した形でメッセージを発信する．かつ，署名付メッセージには必ず PKI 公開鍵証明書が同封される．これにより，受信者は PKI 認証局に問い合せることなく，登録ボランティアからのメッセージの正当性を確認することができる[5].

本人情報は登録ボランティアの身元を確認するための情報であり,生体情報や個人情報などが候補として存在する．どういう情報を本人情報として用いるかによって，登録ボランティアが感じる抑止力の大きさは変化する．また，本人情報の登録は，プライバシーに関する懸念をはらむ．どういう情報を本人情報として用いるかによって，登録ボランティアが感じる心的負担の大きさも変化する．著者らは既に，本人情報の種類と抑止力・心的負担の大きさの関係を調査している．詳しくは文献[5]を参照されたい．

4. 抑止力型情報クレンジングにおける登録ボランティアの活用形態

4.1 匿名ボランティアに働く抑止力の種類

本章では，登録ボランティアが匿名ボランティアの作業内容を確認する具体的な仕組みについて検討する．具体的には，虚偽報告者に罰を与える「懲罰型抑止力方式」，コミュニティ全体に共有される同調意識を利用した「意識型抑止力方式」，対面作業者間に働く同調圧力を利用した「圧力型抑止力方式」に着目した．

4.2 懲罰型抑止力方式

懲罰型抑止力方式は，登録ボランティアに絶対的な権限と特別な役割を与え，匿名ボランティアからの報告に対して真偽の検査を依頼する方式である．登録ボランティアによって検査虚偽報告を暴かれた匿名ボランティアは，その時点で ID とコインが抹消される．この懲罰が，匿名ボランティアの不正に対する抑止力となる．

懲罰型抑止力方式のイメージを図 2 に示す．VA はクラウドソーシングやボランティアの報酬の管理を行う Volunteer Authority，IC は災害現場の統括を行う災害対策本部，FR は救助隊員（First Responder）である．懲罰型抑止力方式の流れは以下の通りである．

① SME がソーシャルメディアメッセージから Event Report を作成.
② VA は，匿名ボランティア用クラウドソーシングシステムを通じて，Event Report の真偽の確認を匿名ボランティアに依頼.
③ ジョブを受注した匿名ボランティアは，単独で Event Report の真偽確認を行い，匿名ボランティア用クラウドソーシングシステムを通じて結果を VA に報告.
④ VA は当該匿名ボランティアに報償．真と判断された Event Report については IC に送信.
⑤ IC は，登録ボランティア用クラウドソーシングシステムを通じて，VA から受領した Event Report の真偽の再確認を登録ボランティアに依頼.
⑥ ジョブを受注した登録ボランティアは，単独で Event Report の真偽確認を行い，登録ボランティア用クラウドソーシングシステムを通じて結果を IC に報告.
⑦ IC は当該登録ボランティアに報償．真であった場合は，救助要請を FR に送信．偽であった場合は，懲罰要請を IC に送信.
⑧ VA が IC から懲罰要請を受け取った場合，虚偽を報告した当該匿名ボランティアの ID とコインを抹消.

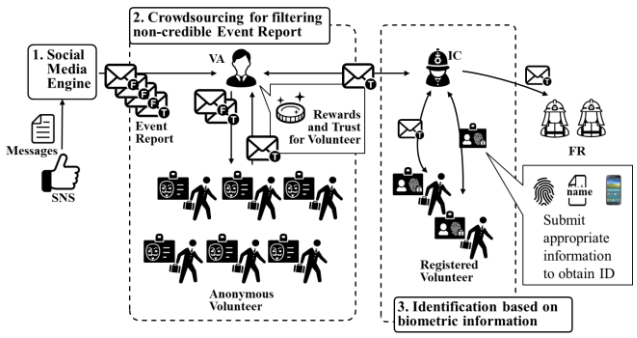

図 2　懲罰型抑止力方式

4.3 意識型抑止力方式

「長いものには巻かれろ」や「朱に交われば赤くなる」という格言に表されるように，人間の行動は，自分がどういうコミュニティに所属しているかに依って変わり得る．善人が多いコミュニティに所属している者は，善人が少ないコミュニティに所属している者よりも，自分も善人であろうとする意識が高い傾向にあると言えよう．意識型抑止力方式は，「現在，被災地に何名のボランティアが集まってきており，その中に何名が登録ボランティアであるか」を全匿名ボランティアに周知する方式である．これにより，ボランティアのコミュニティ全体に暗黙的な「善行のムード」が形成されると，匿名ボランティアが嘘をつきにくくなることが期待される．本研究ではこれを「意識型抑止力」と呼称する．

意識型抑止力方式のイメージをに図 3 示す．意識型抑止力方式の流れは以下の通りである．

① SME がソーシャルメディアメッセージから Event Report を作成．
② VA は，クラウドソーシングシステムを通じて，ボランティアに Event Report の真偽の確認を依頼．
③ ジョブを受注した匿名ボランティアあるいは登録ボランティアは，単独で Event Report の真偽確認を行い，クラウドソーシングシステムを通じて結果を VA に報告．
④ VA は当該匿名ボランティアに報償．真と判断された Event Report については IC に送信．
⑤ IC は救助要請を FR に送信．

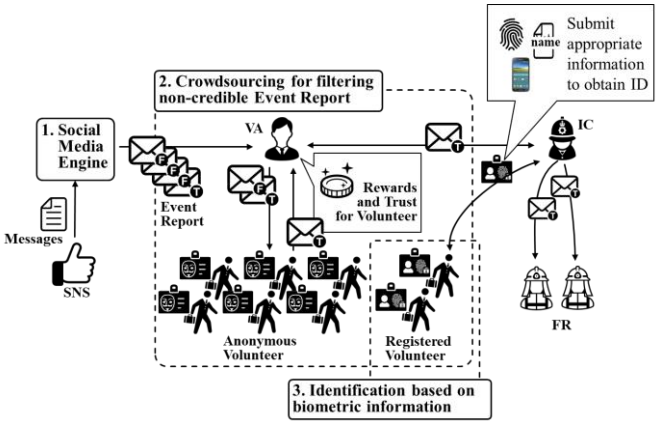

図 3　意識型抑止力方式

4.4 圧力型抑止力方式

被災地においては，数名のボランティアがチームを編成し，グループ単位で支援活動を行う場合も多い．圧力型抑止力方式は，2〜3 名のボランティアがチームを編成し，グループ単位で Event Report の真偽確認を行う方式である．匿名ボランティアと登録ボランティアがランダムに選ばれてチームが編成される．登録ボランティアと匿名ボランティアによって編成されたチームにおいては，登録ボランティアが監視役となるため，匿名ボランティアも正しく行動せざるを得ない状況となる．匿名ボランティアのみによって編成されたチーム[a]においても，常に行動を共にするチームメンバーの間に同調圧力が生まれ，匿名ボランティアが嘘をつきにくくなることが期待される．本研究ではこれを「圧力型抑止力」と呼称する．圧力型抑止力方式のイメージをに図 4 示す．圧力型抑止力方式の流れは以下の通りである．

① SME がソーシャルメディアメッセージから Event Report を作成．
② VA は，クラウドソーシングシステムを通じて，ボランティアチームに Event Report の真偽の確認を依頼．
③ ジョブを受注したボランティアチームは，メンバー全員で Event Report の真偽確認を行い，クラウドソーシングシステムを通じて結果を VA に報告．
④ VA は当該ボランティアチーム(の各メンバー)に報償．真と判断された Event Report については IC に送信．
⑤ IC は救助要請を FR に送信．

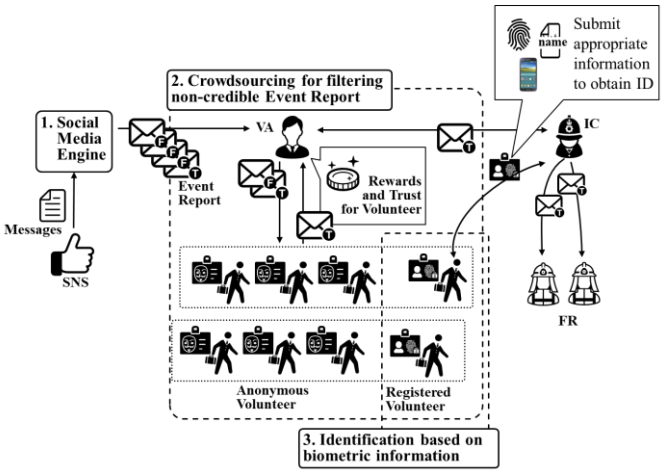

図 4　圧力型抑止力方式

a 本稿は，少数の登録ボランティアが多数の匿名ボランティアの行動変容を促す方式を検討している．このため，2〜3 名のボランティアがチームを組んだ場合，その多くは匿名ボランティアのみによって編成されたチームとなる．

4.5 考察

3 つの方式の中で最も抑止力が大きいと考えられるのが懲罰型抑止力である．一方で，ID やコインの抹消という直接的な懲罰に訴えるこの方式は，匿名ボランティアが単純な過失によって Event Report の真偽判定を誤ってしまった場合には，過度なペナルティとなり得る．また，登録ボランティアの誤判定によって匿名ボランティアの ID やコインが抹消されるようなことが発生してしまうと，問題となり得る．更に，懲罰型抑止力方式は，匿名ボランティアが真と判定した Event Report のみが登録ボランティアによる検査対象となるため,「実際には真の情報であるにも関わらず, 不正な匿名ボランティアが偽と判定した Event Report」は登録ボランティアによる検査対象からは外れてしまう．すなわち懲罰型抑止力方式には，情報クレンジングの不完全性が残る．

次に抑止力が大きいと考えられるのが，圧力型抑止力方式である．実際の災害現場において，ボランティアの単独行動は二次災害の危険を高めることから，基本的にチームでの行動がスタンダードである．そのため，圧力型抑止力方式は，現状に即しており，最も現実的であるといえる．また，各 Event Report の真偽を複数のボランティアが確認しているため，高確度の情報クレンジングが期待できることも圧力型抑止力方式の利点である．複数のボランティアが確認をするという点について，ボランティアが単独行動をとる場合に，「複数の匿名ボランティアに同じ Event Report の真偽確認を依頼し，その匿名ボランティアらからの報告を集約して Report 内容の真偽を判定する」という方式（以降，多数決方式）も考えられる．多数決方式を採用すれば，各 Event Report を複数の眼で確認することができる．しかし，単独でのボランティア活動においては，対面作業者間に働く同調圧力が働かないため，不正に対する抑止力は小さい．具体的には，不正な匿名ボランティアが結託攻撃やシビル攻撃によって多数決の結果を操作することが可能である．したがって，抑止力型情報クレンジングにおいて，多数決方式は適切ではないと考えている．

最も抑止力が小さいと考えられるのが，意識型抑止力方式である. 直接的な監視の目が存在するわけではないため，悪事を強行するような不正者がいても不思議ではない．しかし，いかなるコミュニティにおいても何かしらのムードが自然に醸成されることが通常である．このため，懲罰型抑止力方式あるいは圧力型抑止力方式による情報クレンジングを行うボランティアコミュニティの中にも，意識型抑止力を生じさせることができる可能性がある．すなわち意識型抑止力方式は，懲罰型抑止力方式あるいは圧力型抑止力方式との併用が可能であるかもしれない．

5. 比較分析の方針

今後，以下の点に着目し，懲罰型抑止力方式，意識型抑止力，圧力型抑止力方式の効果を比較検討していく．

① 登録ボランティアと匿名ボランティアの人数比と，各方式によって達成される情報クレンジングの確度の関係
② ボランティアの人口密度（災害エリアの大きさとボランティアの総数の比率）と，各方式によって達成される情報クレンジングの確度の関係
③ Event Report の数量と，各方式によって達成される情報クレンジングの確度の関係

分析には，エージェントシミュレーションを利用する．エージェントの振る舞いを決定するにあたっては，各方式における抑止力の違いを明確にする必要がある．これについては，アンケート調査によって明らかにしていく．

6. まとめ

我々は，災害時にソーシャルメディア上の情報の信頼性を保証する方法として，ソーシャルメディアに流れる複数のメッセージの中から内容が一貫している情報のみを自動抽出する「ソーシャルメディアエンジン」を開発するとともに, ボランティアにメッセージの真偽の確認を依頼する「クラウドソーシング型信頼性検証基盤」を運用する方式を提案している．本論文では，この提案システムのうち,「クラウドソーシング型信頼性検証基盤」に焦点を当て，嘘の報告を行った者に罰を与える“懲罰型抑止力方式”, 対面作業者間に働く同調圧力を活用した“圧力型抑止力方式”, コミュニティ全体に働く同調圧力を活用した“意識型抑止力方式”の 3 つの方式を取り上げた．

懲罰型抑止力方式は，３つの方式の中で最も抑止力が大きいものの，過度なペナルティから誤判定における危険性が大きい．また，Event Report の一部のみを取り扱うことになってしまうことから，情報クレンジングとしての不完全性が残る．

意識型抑止力方式は，直接的な監視ができないため，最も抑止力は小さいと考えられるが，どのようなコミュニティにも存在するムードを活用した抑止力であるため，他の方式との併用の可能性がある．

３つの方式の中でも，最も現実的であるのが圧力型抑止力方式だと考えている．実際の災害現場において，チーム行動はスタンダードであり，チーム行動により複数のボランティアで真偽確認を行えるため，高確度での情報クレンジングが期待できる．

今後，提案している信頼性検証システムに適したクラウドソーシングの方式を明らかとするため，アンケートとシ

ミュレーションを通して，調査，分析を行っていく．

謝辞　本研究は NICT 受託研究課題 193 による．

参考文献

[1] 内官房情報通信技術（IT）総合戦略室 : 災害対応における SNS 活用ガイドブック，入手先 https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/pdf/h2903guidebook.pdf

[2] NHK NEWS WEB : 長野県台風 19 号でツイッターの救助要請収集 約 50 件救助に, 入手先 https://www3.nhk.or.jp/news/html/20191110/k10012171761000.html

[3] 総省情報通信政策研究所：平成 28 年情報通信メディアの利用時間と情報行動に関する調査報告書，入手先 http://www.soumu.go.jp/menu_news/s-news/01iicp01_02000073.html

[4] Mohammad Jahanian, Toru Hasegawa, Yoshinobu Kawabe, Yuki Koizumi, Amr Magdy, Masakatsu Nishigaki, Tetsushi Ohki, K. K. Ramakrishnan: DiReCT: Disaster Response Coordination with Trusted 匿名ボランティア s, Proceedings of 2019 International Conference on Information and Communication Technologies for Disaster Management, pp.1-8 (2019.12).

[5] 北川沢水，向平浩貴，上原航汰，大木哲史，小泉佑揮，河辺義信，長谷川亨，西垣正勝 : 抑止力型トラスト : 災害報告検証者の信頼性向上のための仕組みの検討，暗号と情報セキュリティシンポジウム 2020 予稿集，1C1-4 (2020.1)