生体情報を用いた抑止力型トラスト：災害時通信の信頼性向上のための仕組みの検討

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[††]

概要：現在，緊急時通信には 119 番通報などの IP 電話網が利用されているが，大規模災害時には，通信経路の渋滞や分断による不通によって迅速な情報共有が困難となっている．こうした中で，IP 電話網と比べ耐障害性が高いことから，IP 電話網に代わり，ソーシャルメディアが災害時情報伝達に有用であると認識されつつある．一方で，ソーシャルメディアに流れ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が困難であることも問題視されている．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．この問題の解決には，様々な手法を組み合わせる必要があるが，その一助として，悪意ある情報の発信を抑制する方法に焦点を当て，「生体情報を用いた抑止力型トラスト」を提案する．本論文では，災害時の情報伝達において生体情報が不正に対する抑止力として機能するか否か，アンケートを用いて調査を行う．また，調査の結果から分析を行い，本提案の有用性を検討していく．

キーワード： 災害時通信，トラスト，生体情報

Deterrence-Based Trust Provided by Biometrics : A Study for Improving Reliability of Emergency Communication

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

Abstract: Social media have been recognized as useful for emergency communication in place of the IP communication networks because of its higher tolerance for disasters than the IP communication networks. On the other hand, the information flowing through social media is a mix of lies, and it is also regarded as a problem that is difficulty in selecting necessary information with high reliability. In the disasters, you must quickly collect accurate information and respond promptly. In order to solve this problem, it is necessary to combine various methods, but as a help, focusing on the method of suppressing the transmission of malicious information, we propose the "deterrence-based trust provided by biometrics". In this paper, we use a questionnaire to investigate whether biometric information functions as a deterrent against fraud in emergency communication. In addition, we analyze from the result of the survey and examine the usefulness of this proposal.

Keywords: emergency communication, trust, biological information

1. はじめに

近年，自然災害の甚大化にともない，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，警察などのレスキュー組織や救急隊員が，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，複数のレスキュー組織間での情報共有の難しさ，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り，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人のリアルタイムな情報を集約できるため，地方公共団体においても災害時対応のための SNS 活用率は年々増加している[1]．しかし，ソーシャルメディアを 119 番通報の代替として用いるには様々な課題が存在する．その 1 つに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[2]．ソーシャルメディアにおいても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．

以上のことから，災害時にソーシャルメディア上の情報

†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

の信頼性を保証する仕組みが必要となる．本研究では，ソーシャルメディアにおける情報信頼性向上に向けた取り組みの 1 つとして，生体情報の活用について検討を行う．

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．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．また，災害によりネットワークの分断が発生する可能性がある．そうした状況で，認証局に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．さらに，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わけではない．

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，認証局が利用できない状況下において，公開鍵証明書を有していないボランティアや被災者に対し，どのように信頼性を付与するか
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

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と望ましい．オンラインショップで販売されている商品に対しては，当該諸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，ソーシャルメディア上に次々に流れるメッセージに対する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．

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，不正な発信者による結託攻撃やシビル攻撃にも対抗できる．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公開鍵証明書を入手していたとしても，災害時には PKI 認証局とのアクセスが保障されないため，メッセージの受信者が送信者の公開鍵を取得することができず，メッセージに付されている署名が検証不能となる可能性がある．

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．

本論文では，上記の 3 つの課題の内，①および②に関して検討する．

3. クラウドソーシングによるメッセージの相互確認

課題①の解決に向けてのアプローチとして，本研究では，ソーシャルメディアに流れる情報に対する信頼性を，被災地に集まったボランティアに目視確認してもらう方法を検討する．

災害現場には，志を持つ多くのボランティアが集結するが，「何を手伝えば良いのか」が分からない状況にある．そこで，ソーシャルメディアに流れるメッセージから「目視を要するイベント」を抽出し，これらのタスクの実行をクラウドソーシングのジョブとしてボランティアに依頼する．

具体的なシナリオは以下の通りである．

1. 災害現場においてローカルコインを発行する．
2. 災害現場においてクラウドソーシングシステムを稼働させる．
3. ソーシャルメディアに流れるすべてのメッセージをパースし，その災害現場に関するメッセージを自動抽出するパーサシステムを運用する．
4. パーサシステムは，メッセージを時間，場所，内容等によってカテゴライズすることによってアイテマイズする．
5. パーサシステムは，各アイテムから「そのメッセージの内容の真偽を確かめなさい」というジョブを生成してクラウドソーシングシステムに投入する．それぞれのジョブには，そのジョブに応じた報酬金額が設定されている．
6. 災害現場に到着したボランティアは，クラウドソーシングシステムにアクセスする．

7. ボランティアは，自身の状況に応じたジョブを請負，そのメッセージの内容の真偽を実際に確かめに行く．
8. 5 においてクラウドソーシングシステムにジョブが次々と投入されるが，それぞれジョブが多数のボランティアの中の誰かによって実行される．
9. ジョブを遂行したボランティアは，その結果をクラウドソーシングシステムに入力する．ボランティアには報奨金額分のコインが与えられる．
10. 高額のコインを獲得したボランティアには，特典（例えば災害収束後に政府から褒章）が与えられる．これがボランティアにとってのインセンティブとなる．

上記 5 において，各アイテムの報酬金額を適切に設定することにより，ボランティアに対して効果的にジョブを発行できる．例えば，隔離された状況におかれている被災者からの救難メッセージのような緊急度の高い情報や，リツイートが繰り返される拡散メッセージのような影響力の大きい情報に対しては，パーサシステムが自動的に高い報酬金額を設定してジョブを発行することによって，ボランティアが優先してそのメッセージの真偽を確かめに行くことが期待される．

上記 9 においては，不正なボランティアによる虚偽の報告を防止する工夫が必要である．これに対しては，各アイテムに対して同一のジョブを複数発行し，複数のボランティアからの報告の一貫性を確認する方法が典型的な対策となり得る．また，自身の ID（免許証等）や生体情報を登録したボランティアには，提示されている報酬金額以上のコイン（例えば報酬金額の 10 倍のコイン）を与えるような運用も考えられる．ボランティアは，高額な報酬が得られる代償として，虚偽報告をした場合には（それが発覚した時点で）登録情報から自身が特定されてペナルティ（例えばコインの没収，あるいは社会的な懲罰）が科せられる．これが不正に対する抑止力として働くと期待される．

災害現場において，上記のシステムを運用することにより，ボランティアが獲得しているローカルコインの金額によって，ボランティア各自の信頼度を測ることができる．すなわち，「メッセージに対するトラスト」を「人に対するトラスト」へと演繹できる．また，災害によってネットワークの切断が発覚した際には，「通信パケットのフォワーダとしてそのエリアに滞在する」というジョブをボランティアに発行することもできる．これらも本方式のメリットである．

本方式の今後の課題としては，自作自演攻撃の防止が挙げられる．ID あるいは生体情報を登録したボランティア（以降，登録ボランティア）は，異なるユーザ名で架空のボランティア（以降，匿名ボランティア）としてジョブを行うこともできてしまう．すなわち不正者は，「登録ボランティアとしてコインを精力的に獲得しながら，匿名ボランティアとして不正を行うことができる．自作自演攻撃とは，不正者がこの運用の隙間を悪用して，匿名ボランティアとして虚偽情報をソーシャルメディアに発信した上で，登録ボランティアとして当該情報の真偽確認のジョブを請負，その情報は偽りであったという報告を行う」ことによって，コインを不正に獲得するという攻撃である．この問題は，課題②（人に対する信頼性）にも大きく関係する．

4. 生体情報を用いた抑止力型トラスト

4.1 概要

課題②の解決に向けてのアプローチとして，本研究では，生体情報を本人確認および虚偽抑止のための手段として活用する方法を検討する．

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，救急隊員）が参加している．そこで，これら救急隊員をトラストアンカとして機能させることによって，救急隊員がボランティアの存在を目視によって確認した場合に，救急隊員からボランティアに PKI 秘密鍵と PKI 公開鍵が発行される仕組みを運用する．ボランティアの生体情報は，救急隊員の公開鍵によって暗号化された形で登録されており，プライバシに関する懸念が最小となるように配慮されている．

具体的なシナリオは以下の通りである．（図 1，図 2）

1. ボランティアはルート CA の公開鍵 PKroot を信頼している．
2. 救急隊員は，ルート CA から秘密鍵 SKfr，公開鍵 PKfr，公開鍵証明書 $Sig_{SKroot}(PKfr)$を発行してもらっている．ここで，$Sig_x(Y)$は，鍵 X によるデータ Y の署名を表す．
3. ボランティアは，災害現場において救急隊員に接触する．
4. 救急隊員はボランティアの生体情報 Bvo を受け取り（例えば，救急隊員が所持するスマート端末でボランティアの顔写真を撮影する），これを確認する．
5. 救急隊員はボランティアに秘密鍵 SKvo，公開鍵 PKvo，公開鍵証明書 $Sig_{SKfr}(PKvo)$を発行し，SKvo，PKvo，$Sig_{SKfr}(PKvo)$，$Sig_{SKroot}(PKfr)$をボランティアに渡す．
6. 救急隊員は Bvo を暗号化し，$\{Sig_{SKfr}(PKvo), Enc_{PKfr}(Bvo)\}$の形でアーカイブする．ここで，$Enc_x(Y)$は，鍵 X によるデータ Y の暗号化を表す．
7. 5 の後，ボランティアは前章のクラウドソーシングシステムとの連絡が可能となる．その際，ボランティアからクラウドソーシングシステムに送られる通信内容 M は，$\{M, Sig_{SKvo}(M), Sig_{SKfr}(PKvo), Sig_{SKroot}(PKfr)\}$のデータ形式で送受信される．
8. 万一，あるボランティアからの情報 M が虚偽であったことが発覚した場合，救急隊員は $Enc_{PKfr}(Bvo)$を復

号し，Bvo を警察に届け出る．警察は，Bvo を手掛かりにして，虚偽情報の発信者を捜索して特定する．

近年，生体認証が普及し，生体情報から個人を追跡・特定できるということが一般に知られるようになった．さらに，生体情報に関するプライバシ保護の重要性が強く認識されつつある．これは，多くのユーザが“生体情報が漏れてしまうと，個人を特定されるかもしれない”という危機感を有していることの表れといえる．上記の方法は，ユーザが生体情報に対して抱くこの危機感を，シビル攻撃や虚偽情報発信に対する抑止力として利用し，ソーシャルメディアに情報を投入するユーザの信頼性を高めることを狙っている．

ただし，同一のボランティアが，ある場所で vo1 と名乗って救急隊員 fr1 と接触した後に，別の場所で vo2 と名乗って救急隊員 fr2 と接触した場合，暗号化をほどくことなく $\{Sig_{SKfr1}(PKvo1)$， $Enc_{PKfr1}(Bvo1)\}$ と $\{Sig_{SKfr2}(PKvo2)$，$Enc_{PKfr2}(Bvo2)\}$の突合を検査することはできない．このため本方式は，シビル攻撃に対する耐性は不十分である．これについては今後の課題である．

本研究では，抑止力を通じて情報の信頼性が高まる仕組みを「抑止力型トラスト」と定義する．抑止力型トラストの利用によって,“嘘がばれたら発信者が自分だとばれてしまう”という心理が働き，情報発信者が嘘をつきにくくなる．この結果，生体情報が添付されたメッセージが虚偽情報である可能性が低くなることが期待され，災害時のソーシャルメディアにおける「メッセージの信頼性」を高めることにもつながると考えられる．

5. 抑止型トラストの効果に対するアンケート調査

5.1 調査項目

提案方式と抑止力型トラストの有効性を確認するため，アンケート調査を行う．本研究では，「ソーシャルメディア上に虚偽情報が流れるのを防ぐにはどうすれば良いか？」という目的に対し，「生体情報を用いた抑止力型トラストを利用することにより虚偽情報の発信を抑制できる」という仮説を立てた．この仮説を明らかにするために以下の調査項目を,アンケート調査によって明らかにする．アンケートシステムには Limesurvey[4]を利用し，被験者については，クラウドソーシングサービスである Lancers[5]を利用して募集を行った．また，被験者を募集する際に，「生体認証を利用したことがある人」を調査対象にしていることを明記した．

① 生体情報が虚偽情報送信の抑止力として働くか？

（ア）どのような生体情報を用いれば抑止力が高まるのか？

（イ）個人情報と生体情報の間に抑止力効果の差はあるのか？

（ウ）事前認証と生体情報の添付の間に抑止力効果の差はあるのか？

② プライバシをさらす程度と虚偽情報送信の抑止力効果は同等か？

③ 嘘の程度によって虚偽情報送信の抑止力の効果は変化するか？

ここで，③の嘘の程度についてだが，嘘には事実を偽装する嘘や誇張する嘘など様々な種類が存在する．嘘の種類によって，ユーザが嘘を発信しやすくなり，抑止力が働きにくくなることが考えられる．本来であれば，嘘を分類できる指標を用いて,それに応じた質問を作成するべきである．しかし,当該指標に関する既存研究の有無を調査した結果,今回のアンケートに適応可能なものが得られなかった．そこで,今回は,「自分が得られる利益」「他人が被る不利益」の 2 軸で嘘を分類し，嘘の分類表図 3 を作成した．図 3 の分類を基軸とし,「自分が得られる利益」と「他人が被る不利益」が等しい 3 つの嘘,「救助」「配給」「いたずら」をアンケートに用いることとした．

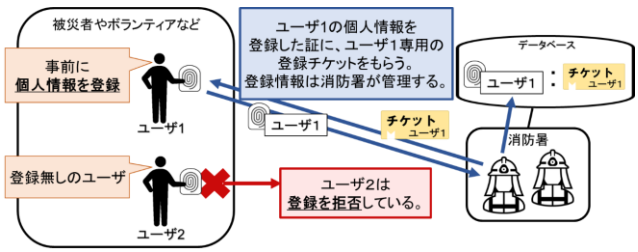

図 1 事前登録型イメージ図（登録時）

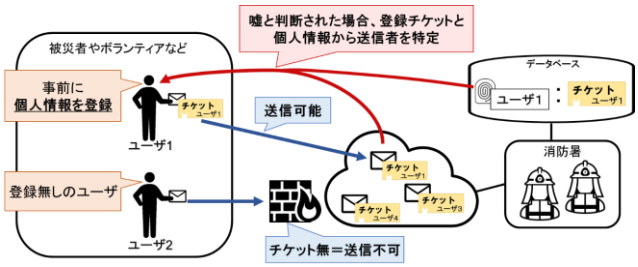

図 2 事前登録型イメージ図（送信時）

嘘の分類		他人が被る不利益		
		大	小	無し
自分が得られる利益	大	救助		
	小		配給	
	無し			いたずら

図 3 嘘の分類

5.2 アンケートの質問構成

5.1 節で述べた調査項目を明らかにするため,以下の質問を作成し，アンケートを実施した．番号は，実際に実施したアンケートでの質問順である．また，今回の調査に用いる生体情報と個人情報は「最低限個人を特定できる情報」かつ「スマートフォンで入力可能な情報」を条件に,「顔」「指紋」「声紋」「基本 4 個人情報（氏名＋住所＋生年月日＋性別)」「氏名＋住所」「携帯電話の番号」「運転免許証」の 7 つとした.

① 生体認証の利用に関する質問

生体認証をよく利用している人ほど，生体情報が個人を特定できる情報であることがを知っているため，プライバシをさらす程度や抑止力の程度に差が出るのではないか，と考えた.そこで,どのような生体認証を利用しているか，また，その生体認証を利用し始めてどれくらい経つのか，といった質問を行う.

② IMC

今回のアンケートは,心理尺度による「測定」ではなく，質問文を独自に作成する「調査」である．このような調査が適切に行われるためには，回答者が質問項目の意味を正確に理解し，回答形式と回答者の回答を合致させ回答させる必要がある．しかし，このような場合，Satisfice 問題が発生し,オンライン調査では大きな影響を与える[7]. Satisfice 問題の中でも，強い Satisfice の対策が必須とされている．強い Satisfice とは,「調査項目の内容を理解するための認知コストを払わず，誰でも選択可能な選択肢を選んだり，当てずっぽうに選んだりすること」である．この Satisfice 問題の対策として，事前にスクリーニングする方法が広く検討されている[8][9]．その 1 つが，この IMC（Instructional manipulation check）である[10]．IMC とは，リッカート尺度や複数選択式の設問に対して，回答者に「正しく答えないように」求めることで，Satisfice の有無を確認する方法である．IMC の和文での構成も提案されている[7].

③ プライバシに関する質問

各情報に対して，他人に提示する機会があった場合どの程度のプライバシを晒していると感じるか，調査するために質問を作成した．それぞれの個人情報について,「どのくらいプライバシを晒していると思うか」と言う質問に対して，5 件法を用いて,「1 : 全くそう思わない」「2 : あまりそう思わない」「3 : どちらとも言えない」「4 : まあそう思う」「5 : そう思う」として，回答を集めた．この回答結果をプライバシスコアとする.

④ メッセージ送信に関する質問

本論文で提案した抑止力型トラストの有効性を調査するための質問である．被験者には，抑止力型トラストが実装された緊急時通信網で，いたずら・配給・救助の 3 つの嘘を発信しようとしているユーザをそれぞれイメージしてもらい，回答をしてもらった.

また，添付型と事前登録型の 2 種類の説明文を作成し，回答時に被験者をランダムに添付型回答群と事前登録型回答群に分けるようにした．回答選択肢は，プライバシに関する質問と同様だが,「嘘のメッセージの送信時に，各情報を添付した場合でも，メッセージをそのまま送信すると思うか」と言うように質問を設定したため，値が小さいほど抑止力が高いということになる．この回答結果を抑止力スコアとする.

⑤ 生体認証に関する質問

生体認証の知識の差によって，抑止力に差が出るのではないかと考えた. そこで, 文献[11]の生体認証の脆弱性に関する記述を参考に,生体認証の知識を問う質問を作成した. その際，複数ある脆弱性のうち，今回は生体認証特有の課題に絞り，利用した．また，前述した Satisfice 問題の対策の一つとして，回答の一貫性を利用したフィルタリングを行うこととした．そのため，次の例の通り，いくつかの脆弱性に関しては，1 つの脆弱性から 2 つの質問を作成し回答の一貫性を確認できるようにした.

例）脆弱性「複製：物理的に生体情報を複製できる」
質問①：生体情報は物理的な方法で複製出来ない
質問②：生体情報の成功な偽造物を作ることができる

これらの質問に，Yes/No で回答してもらい，その脆弱性に関する知識の有無を調べる．質問①で No と答えた（つまり正解した）人は，質問②でも Yes と答える（つまり正解する）はずである．不正解のときも同様になるため，ここで回答に一貫性が持てない場合は，文章を読み飛ばしている可能性が高いと判断できる．また，具体的な質問になりすぎると，なんとなく正しい回答を悟らせる可能性もある．その 2 点に注意し，実験実施者内（著者ら 3 名以上）で推敲を重ね，質問分を作成した．最終的に，17 つの脆弱性から 31 問の質問を作成，そのうち一貫性のとれた質問は 11 ペアとなった．さらに,「この質問には必ず右（左）を選択してください」というダミー質問を 2 つ追加した.

⑥ SNS の利用に関する質問

本提案がソーシャルメディアに関するものであることから，日常的な SNS の利用に影響を受けるのではないか，と考えた．そこで，文献[12]を参考に，本研究の分析に利用できそうなものを抜粋し，アンケートの質問に組み込んだ.

⑦ 基本情報

被験者の基本情報を問う項目は「デモグラフィック項目」と呼ばれ，分析には極めて重要である一方で，プライバシや個人情報に関するデリケートな質問である[13]. そこで，今回アンケートで質問する項目については，分析に必要な情報のみに絞っている．また，警戒心を抱かせないため，アンケートの最後に聞くように配慮した.

6. 結果

被験者数は, 20〜60 代の 200 名（男性 73 名, 女性 48 名）となった．前述したとおり, 回答時に被験者をランダムに添付型回答群と事前登録型回答群に分けるようにした．その結果, 添付型回答群 86 名, 事前登録型回答群 114 名となった．この被験者から，まずは IMC でのフィルタリングを行う．IMC の設問の指示に従い回答せずに次に進んだ人たちを遵守群，指示を読まずに回答をしてしまった人たちを違反群とする．その結果，遵守群 121 名，違反群 79 名となった．次に，遵守群 121 名に対して，回答の一貫性を用いたフィルタリングを行う．0 節の⑤で記した通り，全 11 ペアの質問を利用し，一貫しなかったペアを誤答数としてカウントして集計した結果を図 4 に示す．本来であれば，誤答数 0 問の被験者を分析で利用すべきなのだが，8 名では分析には少なすぎる．今回は，0〜2 問であれば許容範囲とした．以上より, 最終的に分析で利用する被験者は 66 名となった．以降の結果では, その 66 名の結果をまとめたものを記す． 66 名のうち，添付型回答群は 25 名，登録型回答群は 41 名であった．また, ダミー質問に対して誤った回答した被験者は 3 名居たが，IMC のフィルタリングで除外できていたため，結果に影響はない．

実験データについて，紙面の都合上，結果の全てを掲載することが困難なため，本論文で分析を行うものに焦点をあてて掲載をしていることに注意されたい．また，調査に利用したプライバシ情報に関して,「なにもなし : non, 顔 : face, 指紋 : fing, 声紋 : voice, 氏名+住所+生年月日+性別 : PI4, 氏名+住所 : PI2, 運転免許証 : DL, 携帯電話番号 : PN」と表記する．

プライバシスコアの平均と分散を表 1 に示す．また，事前登録型の抑止力スコアの平均と分散を表 2 に示す．表中の値については「平均値（分散）」となっている．また，有効数字は 3 桁とする．

7. 分析

実験データを元に統計的な分析を行い, 5.1 節で述べた調査項目を明らかにしていく．本研究では，リッカート尺度で回答してもらったため，分析では，プライバシスコア，及び抑止力スコアを順序尺度として扱うこととした．はじめに，プライバシを晒す程度に差があるのかを検証する．ノンパラメトリックな対応のある 3 群以上の比較として，Friedman 検定を行ったのちに，ウィルコクソンの符号付順位検定で Holm 法を用いた多重比較を行った．有意水準は 5%とする．Friedman 検定の結果，$p < .05$ となり，群間で何らかの差があることが確認された． どの群の間に差があったのかを示した，多重比較の結果を表 3 に示す．表中の値は, 少数第 3 位以下を切り捨て表示する。表 1, 表 3 より，プライバシを晒す程度は,「運転免許証，氏名＋住所＋生年月日＋性別，氏名＋住所」が最も高く，その次に「顔，指紋，携帯電話番号」，最も低いのが「声紋」となった．同様に，抑止力の差についても検定を行った．“事前登録型・いたずら”の多重比較の結果を表 4 に示す．Friedman 検定の結果は $p < .05$ であり，群間で何らかの差があることが確認できた．表 2，表 4 より，生体情報や個人情報を登録することで，嘘の情報発信の抑止力になることが確認できた．同様の傾向が，事前登録型の他の嘘や，添付型でも確認できた．最も抑止力の低いと考えられる voice に対して有意差が出ている部分もあるが，voice と face の間には有意差はみられなかった．この結果は，他の場合と共通していなかった．被験者が少ないことや，多重比較による有意水準の調整による影響が考えられる．

次に，嘘の程度によって，抑止力に差が出るのかを検証した．何を添付（登録）するかは考慮せず，被験者毎に何かしら登録した際の抑止力スコアの平均を出し，それをデータとして，比較を行った．ただし，登録をしない「なにもなし」は抑止力が働かないとして除いている．検定の方法は, 同様である. Friedman 検定の結果は, $p < .05$ となり，群間で何らかの差があることが確認できた．多重比較の結果を表 5 に示す. 表 5 より，事前登録型は嘘の程度が大きくなるにつれて, 抑止力が働きにくくなることが分かった.

最後に，プライバシを晒す程度と虚偽情報発信の抑止力が同等なのか，分析を行う．まず，ノンパラメトリックな指標であるスピアマンの順位相関分析を用いる．事前登録型の嘘の程度毎に，有意水準 5%で分析を行った結果が表 6 である．プライバシスコアは値が大きいほどプライバシを晒していると感じる度合いが高く，抑止力スコアは値が小さいほど抑止力効果が高いため，負の相関が出るほど，プライバシを晒す程度と虚偽情報発信の抑止力が同等と言える．表 6 より，いたずらと配給に，低い負の相関があることが分かった. 視覚的に確認するため, 散布図を用いて，プライバシスコアを縦軸，抑止力スコアを横軸とし，嘘の程度毎にプロットした．その結果を図 5 に示す．図中の楕円は，30%の確率楕円である．図 5 より，嘘の程度が大きくなるにつれて, 抑止力効果が低下していることが分かる．実装に向けて，どのような情報を用いるのが良いか，検討を行う．

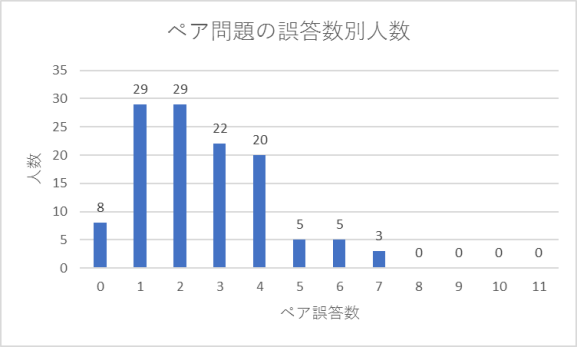

図 4　ペア問題の誤答数別人数

表 1 プライバシスコアの平均（分散）（n=66）

情報	プライバシスコア
face	4.09 (1.13)
fing	3.91 (1.19)
voice	3.26 (1.24)
PI4	4.76 (0.498)
PI2	4.64 (0.598)
DL	4.62 (0.718)
PN	4.08 (0.810)

表 2 登録型抑止力スコアの平均（分散）（n=41）

情報	いたずら	配給	救助
non	4.24 (1.14)	4.02 (1.25)	4.22 (1.21)
face	1.76 (1.02)	2.32 (1.17)	2.95 (1.40)
fing	1.90 (1.11)	2.56 (1.34)	2.93 (1.31)
voice	2.39 (1.18)	2.95 (1.22)	3.27 (1.18)
PI4	1.37 (0.662)	2.10 (1.32)	2.61 (1.38)
PI2	1.49 (0.746)	2.20 (1.21)	2.80 (1.36)
DL	1.37 (0.733)	1.90 (1.20)	2.49 (1.43)
PN	1.73 (0.922)	2.46 (1.27)	3.12 (1.47)

**: < .01, *: < .05

表 3 プライバシスコアの多重比較結果：p 値 （n=66）

	DL	face	fing	PI2	PI4	PN
face	0.00**	-	-	-	-	-
fing	0.00**	1	-	-	-	-
PI2	1	0.00**	0.00**	-	-	-
PI4	0.67	0.00**	0.00**	0.14	-	-
PN	0.00**	1	1	0.00**	0.00**	-
voice	0.00**	0.00**	0.00**	0.00**	0.00**	0.00**

**: < .01, *: < .05

表 4 事前登録型の抑止力スコアの多重比較結果：p 値（n=41）

	DL	face	fing	non	PI2	PI4	PN
face	0.07	-	-	-	-	-	-
fing	0.06	1	-	-	-	-	-
non	0.00**	0.00**	0.00**	-	-	-	-
PI2	0.6	0.22	0.09	0.00**	-	-	-
PI4	1	0.07	0.05	0.00**	0.53	-	-
PN	0.07	1	1	0.00**	0.38	0.05	-
voice	0.00**	0.07	0.02*	0.00**	0.00**	0.00**	0.01*

**: < .01, *: < .05

表 5 嘘の程度による抑止力スコアの差（n=41）

	いたずら	配給
配給	0.00017**	-
救助	0.0000093**	0.00071**

**: < .01, *: < .05

表 6 相関分析の結果（n=41）

嘘の程度	相関係数（p 値）
いたずら	-0.36 (0.00**)
配給	-0.212 (0.00**)
救助	-0.127(0.03*)

**: < .01, *: < .05

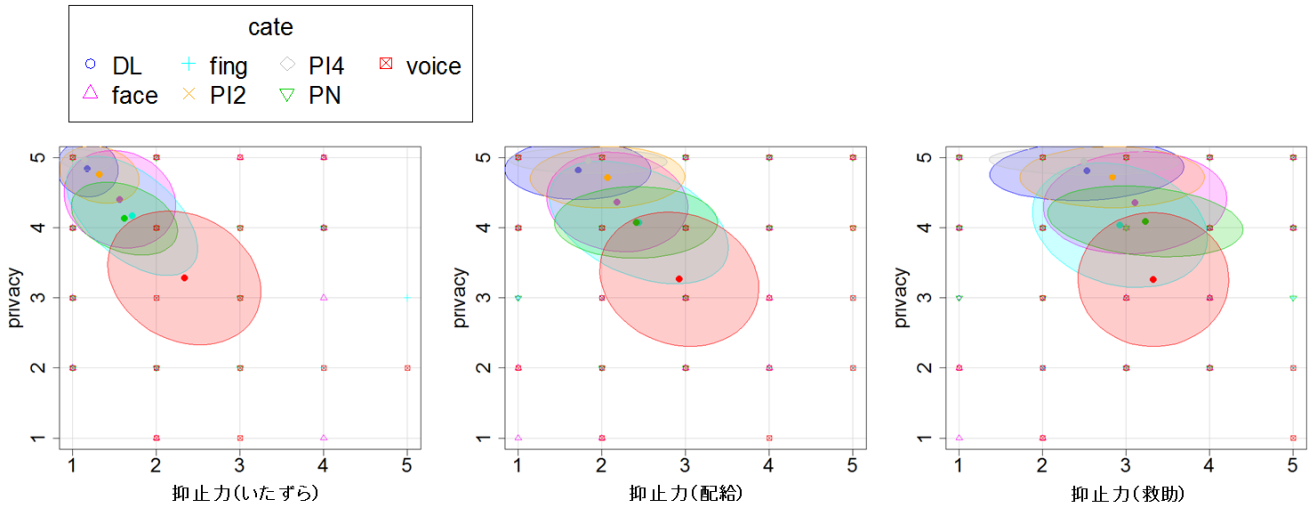

図 5 プライバシスコアと抑止力スコア 散布図

8. まとめ

本論文では，情報の信頼性を確保する手法として，「抑止力型トラスト」を提案し，アンケートにより，その有用性を検証した．生体情報，個人情報が虚偽情報発信の抑止力として働くことが分かり，その抑止力は嘘の程度によって変化することが分かった．本論文で示した分析は最低限のものであり，調査項目すべてを明らかにするものではない．個人情報や生体情報の中でも，プライバシを晒す程度が低く，抑止力効果が高いもの程抑止力型トラストの運用に向いていると考えられる．より分析を進め，プライバシと抑止力の関係を明らかにし，実装に向けて，どのような情報が抑止力型トラストに向いているのか，検証を進めたい．また，分析に用いることの出来るデータが予想以上に少なくなってしまったため，追実験も考えていく．

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〉(2018).

[2]. 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，
〈http://ww.soumu.go.jp/menu_news/s-news/01iicp01_02000073.html〉(2018).

[3]. Rousseau D. M., Sitkin, S. B., Burt, R. S., and Camerer, C.: Not so different after all: A cross-discipline view of trust, Academy of management review, Vol23, No.3, pp.393–404(1998).

[4]. LimeSurvey：LimeSurvey: the online survey tool - open source surveys（オンライン），入手先〈https://www.limesurvey.org/〉(2019).

[5]. ランサーズ株式会社：Lancers（オンライン），入手先〈https://www.lancers.jp/〉(2019).

[6]. 国立研究開発法人情報通信研究機構：「スマートコミュニティアを支える高信頼ネットワーク構成技術の研究開発」に対する提案書(2017).

[7].三浦麻子，小林哲郎：オンライン調査モニタの Satisfice に関する実験的研究，社会心理学研究，Vol.31，No.1，pp1-12(2015).

[8]. Berinsky, A. J., Margolis, M. F., and Sances, M. W.: Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys. Am5.1erican Journal of Political Science, Vol.l58, pp.739–753(2014).

[9]. Chandler, J., Mueller, P., and Paolacci, G.: .Nonnaïveté among Amazon Mechanical Turk workers: Consequences and solutions for behavioral researchers. Behavior Research Methods, Vol.46, pp.112–130(2014).

[10]. Oppenheimer, D. M., Meyvis, T., and Davidenko, N.: Instructional manipulation checks: Detectingsatiscing to increase statistical power. Journal of Experimental Social Psychology, Vol.45,pp.867–872(2009).

[11]. （株）日立製作所システム開発研究所：「バイオメトリクスセキュリティ評価基準の開発」2003 年度 報告書（抜粋），入手先〈https://www.jaisa.or.jp/action/group/bio/pdfs/0715_02.pdf〉（2018）

[12]. 消費者庁：インターネット消費者トラブルに関する総合的な調査研究 報告書「ＳＮＳに関するアンケート結果」，入手先〈http://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/adjustments_index_1_170111_0002.pdf〉(2018)

[13]**鈴木淳子：質問紙デザインの技法[第 2 版]，株式会社ナカニシヤ出版**（2016）