研究ノート

ディジタル署名を用いたSNS発信者判別手法

早稲田篤志*・高橋樹宙*・鈴木英男*・花田真樹*

要旨：スマートフォンの普及によりSNS上に災害関連情報を発信する人が増えている．これにより，多くの人が迅速な情報の収集が可能となった．その一方で，自治体や企業が一部のSNS発信者により発信されたデマ情報の対応に追われてしまい，災害への対処や業務に遅れが生じるという問題も散見される．そこで本研究では，ディジタル署名を利用して投稿者の所属する自治体を検証するシステムを提案する．これにより投稿者のプライバシーを守りつつ，問題が生じた際には投稿者を特定が可能とするシステムを提案する．

キーワード：SNS，ディジタル署名

Method to Distinguish a Sender of SNS Using a Digital Signature

Atsushi WASEDA*, Naoki TAKAHASHI*
Hideo SUZUKI* and Masaki HANADA*

Abstract: With the proliferation of smartphones, many people post and acquire information related to a disaster on the social networking service（SNS). However, because of the many rumors that were posted on the SNSs, the response to disasters can be delayed. In this paper, we have proposed a method to verify the municipality of the sender using a digital signature. Our system usually protects the privacy of the sender, but if a problem arises, it can identify the sender by the local government.

Keywords: SNS, Digital Signature

* 東京情報大学
Tokyo University of Information Sciences

2021年10月15日受付
2022年２月18日受理

1．はじめに

近年自然災害の発生に伴いSNS（Social Networking Service）に災害関連情報を投稿する人が増えており[1], [2], [3], [4], [5]，SNSの情報を収集して活用する自治体も増えている[6], [7], [8], [9]．一方で，SNSには有益な情報と同時に不正確な情報や誤情報といったデマ情報も多数投稿される[10], [11]．このようなデマ情報の中には，誤った情報を正しいと信じ，善意でリツイートすることで広まる情報もあるが，災害とは関係ない人が愉快犯的な目的で発信するデマ情報もある．ある程度落ち着いた状況であれば，Federal Emergency Management Agency（FEMA）が開設しているCoronavirus Rumor Controlのページのような，真偽について確認するサイトを参照することにより確認ができる．しかしながら，被災時のような緊急事態においては，情報が集積されるのを待ち，真偽の確認をするような余裕はなく，その場での判断が必要になるなど，平時とは異なる問題がある．そのため，デマの拡散や誤報を抑制するための方法の提案[12], [13]や自動判別を行う方法[14], [15]が提案されている．また，藤代らは情報トリアージとして有益な情報を効率的に峻別・整理する方法を議論しているが，トリアージの担当者のITリテラシーに依存するなど，多くの問題点が存在している[16]．

そこで本研究ではSNSの発信情報に疑義が生じた際にその発信者を特定するシステムを提案する．デマ情報というのは，匿名性を隠れ蓑にしていて，１次情報となるデマを流し，その記事を読んだ人が２次情報を流し，続けて３次情報の発信が連鎖したり，ネットニュースに取り上げられたりすることで，デマとして拡散していくものである．そこで，１次情報の発信者について誰であるかを確認することができるようにすることで，情報の発信に責任を持たせ，デマとなる１次情報が減ることで，結果として，デマ情報を発信するツイートの総数も削減されることが期待できる．しかしながら，任意の人や機関が発信者の個人情報にアクセスできるようにすることは，発信者のプライバシーを侵害することにつながってしまう．

そこで本研究では，閲覧者が投稿内容を見た際に，どこに住んでいる者が投稿した情報なのかを検証可能にすることを考える．しかしながら，自宅のような情報は投稿者のプライバシーに関わるため，SNSに情報を発信する際に位置情報そのものを付与することには問題がある．また，ハッシュタグを使うことで情報を収集する方法[6], [7], [8], [9]もあるが，これは円滑な情報収集を目的としたもので，デマ情報排除を目的としたものではない．実際にハッシュタグは誰でも使うことができるため，市の名前のハッシュタグが付されたとしても，その市の居住者や現在地が市内である投稿者から投稿されたことは保証できない．そこで，投稿者が居住地について自治体レベルでまとめることで閲覧者へのプライバシーを確保することを考える．具体的な方法としては，投稿者が災害情報をSNSに投稿する際に，投稿者が自身の所属する自治体のサーバ上でディジタル署名を作成し，投稿内容にディジタル署名を添付する．この署名を検証することで，投稿者がその自治体に所属する人間であることを閲覧者は確認することができる．その一方で，投稿者のより詳しい身元についての情報は閲覧者には得ることはできない．また，検証を行った閲覧者についての情報は投稿者や自治体には得ることはできないため，SNSへの投稿者，閲覧者ともにプライバシーを保護することができる．一方で署名の生成は自治体のサーバ上で行うため，サーバ上の履歴を用いることで，署名作成者に関する情報を得ることが可能であり，デマ情報や誤った情報を発信した投稿者については身元の特定も可能である．また，このシステムを利用することにより，様々な利点が挙げられる．例として，その地域の災害情報が自治体のサーバに集まるため，より迅速な情報収集と対応が行えると期待できる．また，集まった情報を使用することで，被災状況を地図上にマッピングするなどの情報提供の活用が考えられる．

本論文は以下のように構成される．第２章は提案システムのシステム構成を説明する．第３章では，提案システムを実際に動作させた実行環境とその動作結果を示す．第４章では提案システムの考察を述べ，研究の有効性を明らかにし，最後に第５章でまとめとする．

2．システム構成

本節では提案システムについて述べる．２．１で提案システムの概要を述べ，２．２で提案システム

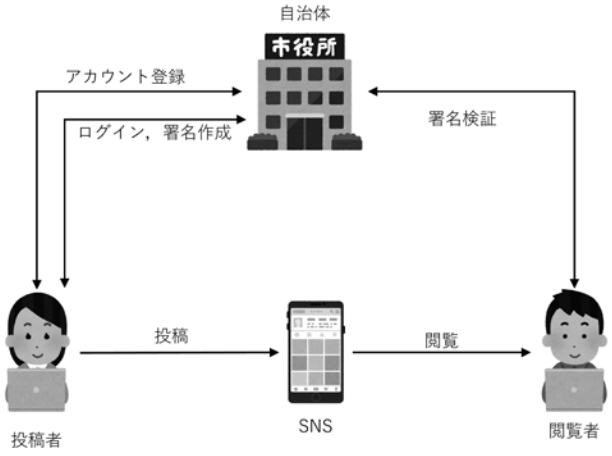

図１　システムの概要図

が実現する機能を述べる．その後２．３にて提案アルゴリズム内にて使用されているディジタル署名について簡単に紹介する．

２．１　システムの概要

提案システムの概要図を図１に示す．

提案システムでは，投稿者，閲覧者，自治体の３つのエンティティが存在し，各エンティティが以下の機能を持つ．

投稿者　SNSに対し，情報を投稿する者であり，ネットワークに接続された状態で，アカウント登録，ログイン，署名作成，署名検証，署名作成履歴閲覧を行うことができる．

閲覧者　SNSに投稿された情報を閲覧する者であり，ネットワークに接続された状態で，任意の投稿の署名検証を行うことができる．

自治体　投稿者がその自治体，ないしはコミュニティの一員であることを保証する者であり，アカウント登録の承認，ユーザ情報の管理，署名の作成者の確認，作成された署名の履歴，作成日時の確認が行うことができる．

また，各エンティティ間の通信は安全に行えるものを仮定する．

２．２　システムの機能

提案システムは，６つの機能を備えている．システム全体の事前準備を行うset_up機能，なりすましの投稿を行えないように投稿者を登録するregistration機能，log_in機能，投稿者が投稿時に自治体が署名を生成するsignature機能，署名の作成履歴を閲覧するhistory機能，閲覧者が署名の検証を行うためのverification機能である．それぞれの機能は以下の通りである．

set_up機能　自治体のサーバ上で，アカウント情報保存用データベースと署名履歴用データベースの二つを作成し，ディジタル署名方式の鍵生成アルゴリズムsig_key_genを実行して署名鍵sk，検証鍵vkを生成する．

registration機能　システムのアカウント作成を実現する．アカウントを作成したい投稿者は，自身の自治体のサーバにアクセスし，登録画面から身元確認情報を入力する．自治体は入力された身元確認情報を基に，住民であるかどうかの確認を行い，住民であればアカウントを発行する．住民でなければ登録申請を拒絶する．

log_in機能　投稿者のシステムへのログインを実現する．ログイン画面にて，ユーザ登録時に設定した，アカウント情報を入力しログインをする．ログインに成功したならば署名の作成（signature）と履歴閲覧（history）が行える．失敗したならば，再度ログイン画面が表示される．

signature機能　投稿者による署名生成を実現する．署名作成画面よりSNSのユーザIDと災害情報を入力すると，sig_signが実行され，入力された情報の署名が作成される．

history機能　署名の作成履歴閲覧機能である．署名作成履歴画面にてそのユーザが今までに作成した署名のメッセージと日付が表示される．

verification機能　検証者による署名の検証を実現する．トップページにて投稿内容とその署名値を入力すると，sig_veriが実行され，署名の検証が行える．署名検証では，ログイン処理を必要としない．

本システムでは自治体の住民であるかの確認プロセスは割愛するが，住民基本台帳やマイナンバーによる身元の確認や，住民票の写し等の証拠書類との照合を想定している．

２．３　ディジタル署名

ディジタル署名は文書に対して行う印鑑による捺印を電子的に実現する技術であり，３つのアルゴリズムsig_key_gen，sig_sign，sig_veriからなる．提案システムではset_up機能にてsig_key_genを，signature機能にてsig_sign，verification機能でsig_veriをそれぞれサブルーチンとして呼び出し実行する．

sig_key_gen　1^k（kはセキュリティパラメータ）

を入力とし，署名鍵*sk*，検証鍵*vk*を出力する確率的多項式時間アルゴリズムである．出力された署名鍵*sk*は署名者が秘密に保存し，検証鍵*vk*は公開することができる．

sig_sign　署名鍵*sk*と署名を施したいメッセージ*m*を入力とし，署名*s*を出力とする確率的多項式時間アルゴリズムである．

sig_veri　署名*s*，メッセージ*m*及び検証鍵*vk*を入力とし，*s*が*m*の正当な署名であればvalid，そうでなければinvalidを出力する確率的多項式時間アルゴリズムである．

代表的なディジタル署名方式として楕円曲線上の離散対数問題を安全性の根拠とするECDSA（Elliptic Curve Digital Signature Algorithm）が存在する．楕円曲線を利用した方式は素因数分解問題や有限体上の離散対数問題を用いた署名法よりも鍵長が短いという特徴があり，署名生成や検証にかかる計算量が少ないという利点がある．ECDSA署名方式はディジタル署名で最も望ましい安全性定義であるEUF-CMA（Existential Unforgeability Against Chosen Massage Attack）を満たしていることが証明されている[17]．

3．実　　装

提案方式について，実装を行った．実装の環境は表1にまとめる．実装における署名方式は384ビットECDSA方式を採用し，ECDSA中に使用されるハッシュ関数としてはSHA2を利用した．ログインのシステムとしてはメールアドレスとパスワードの組を用いたパスワード認証方式を採用している．各エンティティ間の通信は盗聴に対して保護を行うため，SSL/TLS通信を前提として行う．

提案システムは全てウェブブラウザ上で完結し，トップページからクリックや入力により，図2のように画面は遷移をしていく．

3．1　準備

まず全体のシステムのセットアップとして，set_up機能を実行し，データベースの作成，署名に使う署名鍵，検証鍵を作成する．データベースはアカウント情報を管理するデータベースと，作成した署名の履歴を管理するデータベースであり，それぞれ図3の要素を持つ．

提案システムのトップページを図4に示す．トップページの中央に署名検証部があり，右上に投稿者のログイン画面，アカウント登録画面への遷移ボタンがある．署名検証については3．5にて解説する．

3．2　アカウント登録

情報の投稿を行う投稿者はまずアカウント登録を行う．トップページ右上の“REGISTER”を押すことで示されるアカウント作成ページに遷移し，registration機能が起動する．画面上の各項目を入力し，登録ボタンが押されることで，その自治体に所属しているかの確認が行われ，確認がされるとアカウントが作成される．登録されたアカウントは以後の投稿時に利用される．

3．3　投稿

投稿者が投稿を行う際はトップページ右上の“LOGIN”ボタンを押し，ログイン画面に遷移し，log_in機能が起動する．アカウント登録を行ったメールアドレスとパスワードを入力し認証に成功すると，図5のようなマイページに遷移する．

署名作成時はマイページ中央の署名作成ボタンを

表1　実装環境

自治体サーバ	名称	バージョン
OS	CentOS7	7.9.2009
Web サーバ	apache	2.4.6
データベース	MariaDB	5.5
プログラミング言語	PHP	7.4.13
フレームワーク	Laravel	7.30.1
署名作成・検証	OpenSSL	1.0.2

クライアント（PC）	名称	バージョン
OS	Windows10 Home	1909
Web ブラウザ	Google Chrome	87.0.4280.141（Official Build）

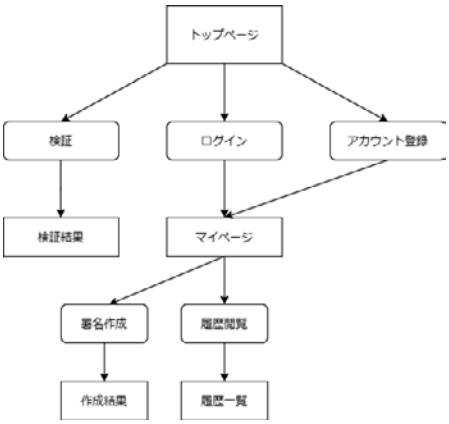

図２　システムの画面間遷移

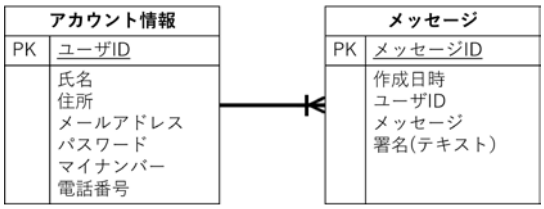

図３　データベース

図４　トップページ

図５　マイページ

図６　署名作成ページ

押すことで図６に示す署名作成ページに遷移し，signature 機能が起動する．テキスト入力欄に，投稿したい災害情報を入力し，“作成”ボタンを押す．署名が作成されると図７のような署名作成結果ページに遷移する．作成された署名はテキストとQRコードの２種類の方法で表示される．

その後SNSを起動し，テキスト入力欄に，入力した災害情報をコピーして投稿し，その後，署名作成結果ページに表示された署名情報のテキスト，またはQRコードをリプライ機能を使用して投稿を行う（図８）．

図７　署名作成結果ページ

図８　投稿

３.４　履歴閲覧

マイページから署名履歴をクリックすると，history機能が起動し，これまで署名を行ったメッセージの一覧が図９にように表示される．

３.５　閲覧

署名付きの情報を閲覧した者はトップページにメッセージと署名を入力することにより署名の検証を行うことができる．署名の入力はQRコードの場合は中央の“ファイルを選択”ボタンから選択する．テキストの場合はテキストボックスに入力する．その後検証するが押されるとverification機能が実行され，validであれば検証成功ページ（図10）に，invalidであれば検証失敗ページ（図11）に遷移する．

３.６　後処理

自治体は被災時における対応が終了し，平時の対応になった時点で，sig_key_genを実行し，鍵の更新を行う．

図９　履歴閲覧ページ

図10　検証成功ページ

図11　検証失敗ページ

４．考　　察

提案システムはSNSでの発信者について，ディジタル署名により検証が可能にするシステムになっている．署名の生成と検証は自治体の鍵を使用しており，個人には紐づいていない．これにより，署名の検証を行う閲覧者に対して署名から投稿者の身元が判別されることはない．一方で，自治体についてはシステムへのログインの履歴や作成した署名の履歴から，投稿者の特定は可能となっている．これにより災害時のデマの発信時の発信者の特定をSNS運営会社を介さずに行えるという利点が存在する．また，本システムはSNSのアカウントそのものとは連動していないため，通常の投稿時と災害時にシステムを使って情報発信を行うアカウントを分けておくことで，過剰な身元の特定を防ぐことも可能である．さらに，閲覧者はシステムへのログインは必要ないため，自治体や投稿者に身元が識別されることはなく，また，他自治体に居住する閲覧者による検証に制限がかかることもない．このように，投稿者及び閲覧者のプライバシーについて配慮されたシステムとなっている．

さらに，本システムでは情報の発信に一定の責任を持たせたことで，デマとなる１次情報の発信を抑制されることが期待できる．これは，デマの元となる１次情報は善意の情報，悪意の情報，意図せず間違っている情報などが存在する．そのときに，１次情報を発信した人は誰であるかを自治体が後に検証できるようにすることで，デマとなる１次情報の発信に心理的な抑止をかけることにつながる．内田らによると2018年の台風21号関連のツイートが３日間で約610万件発信され，そのうち，１次情報は最もツイートの総量が多くなった時で40％程度となっており，その時のツイート数は10分間で約32,000ツイート，リツイートが約48,000ツイートとなっている[18]．この40％の１次情報がシステムにより署名を施す対象である．提案システムにより40％のオリジナルツイートのうちx％の発信が行われなかったと仮定すると，リツイートはx％減ると見積もることができ，全体のツイート量もx％減ることになる．このように，40％の一次情報のツイートが減ることで，全体のツイート数も抑止できることが期待できる．また，この情報は閲覧者にとっても，投稿者の

署名を確認することで責任をもって投稿した内容かを確認することができ，信頼できる情報かデマかを判定する一助とすることができる．

さらに，提案システムは投稿者の所属する自治体が被災地にあるかどうかをディジタル署名にて確認するシステムとなっている．この判定については所属自治体によるディジタル署名の代わりにGPSによる位置情報を直接用いて行う方法も考えられる．しかしながら，スマートフォンの位置情報については偽装アプリが数多く存在する．そのため，例え被災地から発信されている情報であっても，位置情報の偽装がされている可能性があることになる．悪意あるデマ情報であれば，当然位置情報の偽装も行われていることが予測できるため，位置情報で悪意あるデマを防ぐことは難しい．また，正確な位置情報の発信は行動履歴から個人の特定にもつながりうるプライバシー情報の一つであり，公開に当たっては注意を要する情報となる．提案システムにおいては位置情報は自治体レベルに丸められており，個人の特定につながらないという利点が存在する．

提案システムに関する攻撃として，災害とは全く関係のない場所における情報を，被災地で起きた災害の情報であるかのように偽装する攻撃が考えられる．この攻撃を成功させるには被災地の自治体の署名鍵で作成された署名を偽造する必要がある．これはECDSAの偽造不可能性に抵触するため，提案システムではこのような攻撃が成功する確率は無視できるぐらい小さい．

正規の署名を本来のメッセージとは異なる別のメッセージに付加する攻撃も考えられるが，これはメッセージの改ざんに当たる．そのため，署名の検証アルゴリズムであるsig_veriを通過せず，高い確率で検知が可能である．

また別の攻撃としては過去に同じ自治体で起きた災害時の情報を再利用することでデマ情報を発信する攻撃も考えることができる．この攻撃についてはその情報の付された署名も再利用するかによりさらに分類ができる．署名を再利用しない場合はその時点での署名を偽造する必要がある．これは前の攻撃と同様にECDSAの偽造不可能性に抵触するため，高い確率ではじくことができる．一方で，署名も再利用する場合，過去にその自治体に住んでいたユーザによる正規の署名であるが，システムは過去の災害が鎮静後に署名鍵skと検証鍵vkの更新を行っているため，情報に付された署名は現在の検証鍵に対応する署名鍵で作成された署名ではない．したがって，現在の鍵ペアにとっては正当な署名とみなされないため，検証を通過しない．よって，検出が可能である．なお，この鍵ペアの更新については自治体のサーバ内情報の更新のみとなるため，投稿者の持つアカウント情報には影響を与えない．

情報の活用については，現状SNSに投稿された災害情報を収集し，人工知能を用いて解析することで災害状況を把握するシステムがある[14], [15]．このようなシステムではデマにより情報の矛盾が生じれば把握ができるが，それにはある程度の情報が収集されていることが必要となる．提案システムは，このような収集してから解析するシステムに比べ，投稿者が自治体のサーバ上で署名を作成してからSNSに投稿するため，自治体が災害状況を把握するのが速くなると考えられる．追跡性については，匿名でSNSに投稿した人物を特定するためには裁判等の手続きが必要であり，時間が必要となる．提案システムでは自治体のサーバ上に署名履歴とアカウント情報が保存されているため，これらを照会することで，容易に特定が可能である．これらの結果をまとめると，表２のような違いがある．

提案システムで使用する署名方式についてはECDSA方式に限定されるものではない．提案システムは災害時の利用を想定しているため，通常時より通信が混雑することが予想される．円滑な情報の発信には少ない計算資源でも利用が可能であるこ

表２　GPSとの比較

	GPS	提案システム
位置情報	遠隔で偽装可能 詳細な位置情報はプライバシーになる	登録した自治体とは別の場所にいても署名の作成が可能
情報の活用	SNSから災害情報を収集	自治体のサーバに災害情報が記録
追跡性	法的手続きが必要	自治体のサーバにあるアカウント情報に照会

と，通信の帯域を圧迫しにくい署名長の短さが求められる．そのため，提案システムの実装においてECDSAを採用した．これは楕円曲線上の離散対数問題を利用した方式は他の素因数分解問題や有限体上の離散対数問題を利用した方式に比べ，鍵長や署名長が短く，これは通信，計算の両資源の節約につながるためである．

5．まとめと今後の課題

本研究では，デマやフェイクニュースの基となる1次情報を発信したSNSの投稿者について，所属する自治体を検証可能にするシステムを提案した．署名生成を自治体の署名鍵で行うことで，投稿者の匿名性を確保し，問題のある投稿が行われた際には自治体にあるアカウント情報と照会することで，投稿者の身元の特定も可能である．また，閲覧者については特にアカウントの作成は必要としておらず，閲覧者の身元については匿名性が保たれている．さらにこのシステムでは災害情報は署名作成時に自治体のサーバに記録されるため，より迅速に災害情報の収集を行うことも実現されているなどの利点が存在する．

今後に解決すべき課題としては，投稿者や閲覧者の利便性向上のため，平常時と災害時の投稿アカウントの切り替え機能や発信する情報を入力したら自動で署名を生成して投稿する機能や閲覧時に自動で検証を行ってくれる機能を組み込んだアプリの開発などが挙げられる．また，後処理を行い署名鍵と検証鍵のペアの更新を行った結果，それまでの署名鍵で作成された署名の検証が通過しないという点が挙げられる．これにより過去の情報の再利用によるデマを防ぐという利点もあるが，後から情報の検証ができないという問題点もあるため，効率の良い改善法を提案することも今後の課題とある．署名を行う自治体は全ての投稿について投稿者の身元の確認が一機関で可能であるという問題点があるため，複数機関の協力を必要とするように改良を施すことも今後の課題である．

参考文献

［1］内閣官房情報通信技術（IT）総合戦略室防災班：災害対応におけるSNS活用に関する自治体調査（2019年度）（アクセス日 2021/10/6）（2020）．https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/pdf/2019SNSjititai_chousa.pdf.

［2］Toriumi, F., Sakaki, T., Shinoda, K., Kazama, K., Kurihara, S. and Noda, I.: Information Sharing on Twitter during the 2011 Catastrophic Earthquake, *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13 Companion, pp. 1025-1028 (2013).

［3］Mendoza, M., Poblete, B. and Castillo, C.: Twitter Under Crisis: Can we trust what we RT?, *SOMA 2010 - Proceedings of the 1st Workshop on Social Media Analytics*, pp. 71-79 (2010).

［4］鳥海不二夫：ソーシャルメディアにおける災害情報，災害情報，Vol. 16，No. 2，pp. 139-142（2018）．

［5］中村　功：熊本地震にみる災害通信の進展と課題，災害情報，Vol. 15，No. 2，pp. 113-120（2017）．

［6］和光市：災害時におけるツイッターハッシュタグの利用について（アクセス日 2021/10/8）（2014）．http://www.city.wako.lg.jp/home/kurashi/bousai/_19053/_19048/_13853.html.

［7］かすみがうら市：かすみがうら市災害用ハッシュタグの運用基準（アクセス日 2021/10/8）（2016）．https://www.city.kasumigaura.lg.jp/page/page001912.html.

［8］韮崎市：災害時におけるツイッターの活用（災害用ハッシュタグの利用）について（アクセス日 2021/10/8）（2020）．https://www.city.nirasaki.lg.jp/bosai_bohanjoho/bosaijoho/1/3250.html.

［9］日向市：災害用ハッシュタグの利用について（アクセス日 2021/10/8）（2021）．https://www.hyugacity.jp/display.php?cont=190725133744.

［10］朝日新聞：地震直後「ライオン放たれた」投稿の男性，不起訴処分（アクセス日 2021/10/8）（2017）．https://www.asahi.com/articles/ASK3Q5VPQK3QTLVB019.html.

［11］朝日新聞：「シマウマ脱走」デマ拡散再び　熊本市長も注意呼びかけ（アクセス日 2021/10/8）（2018）．https://www.asahi.com/articles/ASL6L5DK8L6LPTIL05Z.html.

［12］池田圭佑，榊　剛史，鳥海不二夫，栗原　聡：口コミに着目した情報拡散モデルの提案およびデマ情報拡散抑制手法の検証，情報処理学会論文誌数理モデル化と応用（TOM），Vol. 11，No. 1，pp. 21-36（2018）．

［13］上野　史，北島瑛貴，高玉圭樹：多次元意見共有モデル上のシグモイド関数に基づく誤報防止アルゴリズム，人工知能学会論文誌，Vol. 36，No. 6，pp. B-KB2_1-12（2021）．

［14］松本慎平，川口大貴，鳥海不二夫：東日本大震災前後のTwitter利用者の投稿活動に基づく定量化と自動判別への応用，人工知能学会論文誌，Vol. 30，No. 1，

pp. 393-402（2015）.
［15］水野淳太，後藤　淳，大竹清敬，川田拓也，鳥澤健太郎，クロエツェージュリアン，田仲正弘，橋本力，奥村明俊：対災害情報分析システムDISAANA及びその質問応答モードの性能評価，研究報告コンシューマ・デバイス＆システム（CDS），Vol. 2015-CDS-14，No. 14，pp. 1-13
［16］藤代裕之，松下光範，小笠原盛浩：大規模災害時におけるソーシャルメディアの活用―情報トリアージの適用可能性，社会情報学，Vol. 6，No. 2，pp. 49-63（2018）.
［17］Fersch, M., Kiltz, E. and Poettering, B.: On the Provable Security of（EC）DSA Signatures, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, Association for Computing Machinery, pp. 1651-1662（2016）.
［18］内田　理，宇津圭祐：災害時のソーシャルメディア利活用，電子情報通信学会基礎・境界ソサイエティFundamentals Review，Vol. 13，No. 4，pp. 301-311（2020）.