Vol.2020-SPT-36 No.41
2020/3/2

フェイク情報の信じやすさと対策の基本検討

佐藤 直[1]　辻井 重男[1,2]　白鳥 則郎[1]　山口 浩[1]　才所 敏明[1,2]
趙 晋輝[3]　五太子 政史[1,2]　近藤 健[2]　山澤 昌夫[1,2]　山本 博資[1]

概要：フェイクニュースなど，フェイク情報を SNS などで流布するケースが増えており，サイバーセキュリティ上の重要課題となっている．本文では，最初に，情報の真正性とフェイクについて定義する．次に，虚偽情報と信じやすさの関係を考察し，情報のサイズが大きいほど，情報が希少でエントロピーが大きいほど，信じやすいことを示す．そのあと，フェイクニュースやフェイク動画の動向を概観する．さらに，SNS の普及によって，ニュースの発信・受信が変容したことを示す．次に，ファクトチェックの現状や技術的取り組みを概説し，報道機関や中立機関によるファクトチェックが活発化していること，技術的取り組みとして，ブロックチェーンや人工知能の応用が検討されていることを示す．そのあと，ファクトチェックの課題として，チェックの自動化，チェック対象を個人に向けられたフェイク情報にまで拡大する必要があることを示す．最後に，これらの課題の解決策として２つの情報真正性保証システムを提案する．最初に，SNS に“マジで？”ボタンや“マジで！”ボタンを追加して，ファクトチェックを実施する仕組みを提案する．この提案により，SNS におけるフェイクニュースやデマの拡散を利用者自身で抑制することが可能になる．次に，デジタルフォレンジック技術を用いて，専門家がコンテンツのメタ情報をチェックし，コンテンツ作成の信ぴょう性を保証するシステム／サービスを提案する．この提案により，個人に向けられたフェイクを個々にあばくことが可能になる．

キーワード：フェイクニュース，真正性，SNS，保証，AI，デジタルフォレンジック

Basic Consideration on Credulity and Countermeasures of Fake Information

NAOSHI SATO[†1]　SHIGEO TSUJII[†1,2]　NORIO SHIRATORI[†1]
HIROSHI YAMAGUCHI[†1]　TOSHIAKI SAISHO[†1,2]　JINHUI CHAO[†3]
MASAHITO GOTAISHI[†1,2]　TAKESHI KONDO[†2]　MASAO YAMASAWA[†1,2]
HIROSUKE YAMAMOTO[†1]

Abstract: Increasingly, fake news and other fake information are distributed on SNS, etc., and this has become an important issue in cybersecurity. The paper first defines the authenticity and fakeness of information. Next, the relationship between false information and credulity is considered, and it is shown that the larger the information size, the rarer the information and the larger the entropy, the easier it is to be fooled. After that, we will look at trends in fake information and show that the spread of SNS has transformed the sending and receiving of news. Next, it outlines the current status of fact checking and technical approaches, and shows that fact checking by news organizations and neutral organizations is becoming active, and that the application of blockchain and artificial intelligence is being considered as a technical approach. After that, we show that it is necessary to automate the check and expand the check target to the fake information directed to the individual as an issue of the fact check. Finally, we propose two information authenticity assurance systems as solutions to these problems. First, we propose a mechanism for performing a fact check by adding a "seriously?" or "seriously!" button to SNS. With this proposal, users will be able to control the spread of fake news and hoaxes on SNS by themselves. Next, using digital forensic technology, an expert checks the meta information of the content and proposes a system / service that guarantees the credibility of the information making. This proposal allows individualized fake to be exposed individually.

Keywords: fake news, authenticity, SNS, assurance, digital forensics

1. はじめに

暗号・認証技術の普及に伴い，情報社会の信頼性が高まってきている一方，SNS などにより，個人レベルで発信される情報の真正性が社会問題化しつつある．いわゆる，フェイクニュースやフェイク動画が飛び交う中で，情報が真実であるかどうかを見極め，保証するシステムの確立が喫緊の課題となっている．

本文は，上記のような視点から，情報の真正性の保証について考察したものである．以下，最初に，対象とする真正性とフェイクの定義を行う．次に，虚偽情報と信じやすさの関係やフェイク情報の動向を概観する．また，ファクトチェックの現状や技術的取り組みを整理する．最後に，情報の真正性を保証する２つのシステム提案を行う．すなわち，SNS において，マジで？”ボタンや“マジで！”ボタンを追加して，投稿の真正性を利用者自身がチェックし

1 中央大学 研究開発機構
Research and Development Initiative, Chuo University
2 セキュア IoT プラットフォーム協議会
Secure IoT Platform Consortium
3 中央大学　理工学部
Faculty of Science and Engineering, Chuo University

保証する仕組み，デジタルフォレンジック技術で専門家がコンテンツのメタ情報を検証し，コンテンツ作成に関わる信ぴょう性を保証するシステム／サービスを提案する．

2. 真正性とフェイクの定義

情報技術セキュリティ管理指針を定めた ISO/IEC TR13335 によれば，真正性（Authenticity）は，情報セキュリティの要素の一つであり，「エンティティ（ユーザ，システム）による振る舞いが明確であること．なりすましや偽の情報でないことが証明できること」とされている[1].

情報セキュリティにおける認証（Authentication／Certification）は，「相手が本人であることを確認すること，あるいは，人に紐づけられた固有の情報で人の真正性を判断すること」といった意味合いで用いられることが多い．この認証により，情報の発信者の真正性は確認できても，発信されたコンテンツの真正性までは確認できない．以下，本文では，情報コンテンツの真正性を単に真正性と呼び，検討対象とする．

次に，本文におけるフェイクを定義する．偽物や虚偽を表現するのにフェイクという表現がよく使用される．実際，フェイクは，なりすました人（例：詐欺師）やニセ物（例：贋作）として，情報以外の虚偽を表すことが多いように見受けられる．しかし，なりすましやニセ物も情報を偽って相手をだますことに違いはない．言い換えれば，虚偽の対象は異なるものの，虚偽情報が手段となっていることに変わりはない．このことから，本文では特に断らない限り，フェイクは虚偽情報を意味することとする．

3. 虚偽情報と信じやすさ

3.1 虚偽情報のサイズと信じやすさ

最初に，虚偽情報のサイズが大きくなるほど，信じやすくなると仮定する．情報（メディア）は文字情報，音情報，画像情報に分類されることが多い．虚偽情報もこれら３種類の情報で構成できる．通常，我々が日常生活で扱う情報のサイズ（バイト数）は，文字情報，音情報，画像情報の順に大きいので，単一メディアの場合，虚偽情報もこの順に大きく，フェイクに成功しやすいのではないかと考えられる．これは，俗に，百聞は一見に如かず，あるいは，Seeing is believing といわれることからも分かる．昨今，実際に発生しているフェイクの代表例３つ（フィッシングメール，振り込め詐欺，フェイク動画）について，メディアの組み合わせ，ならびにフェイクの特性（情報作成の困難性，信じやすさ，件数）を比較し表１に示す．

3.2 虚偽情報のサイズと信じやすさ

情報の希少性（新規性）は情報エントロピーとも呼ばれ，希少な情報ほどエントロピーが大きくなる．一般に，情報が希少であるほど，そのインパクト（価値）は大きく，関心を呼ぶ傾向がある．例えば，ニュースは，新規性の高い報道情報を意味するが，誰も想定しなかった事象が報道された場合，スクープと呼ばれ，受信者の関心も高くなる．逆に，同じような情報が度々伝えられると，希少性（新規性，エントロピー）が小さくなり，関心度合いも低下する．虚偽情報も同様であり，希少性（新規性）が大きいほど，信じやすくなるという仮説をたてる．ただし，この情報の希少性は，前節の情報のサイズと異なり，受信者の経験（過去の学習の有無や回数）に大きく依存する．すなわち，経験（学習）したことのない情報ほど，受信者にとってインパクトが大きいため，その情報が虚偽であった場合は，信じやすくなると仮定する．

希少性の大きい虚偽情報が，社会問題化した事例は古今東西を問わず多く伝えられているが，イソップ寓話の「オオカミ少年」は，少年に村人が騙され続けた結果，すなわち，虚偽情報を学習した結果，虚偽情報の希少性が低下し，悲劇の結末を迎える．この寓話は，情報の真正性保証を検討する上でヒントになる．そこで，後の **6.** では，「オオカミ少年」を題材として，情報エントロピーと信じやすさについて考察を深めることにする．

表１　フェイクの特性

フェイクの種類		フィッシングメール	振り込め詐欺	フェイク動画
メディアの組合わせ		文字	音	音＋映像
フェイクの特性	情報作成の困難性	易 → 難		
	信じやすさ	難 → 易		
	件数	多 → 少		

4. SNS におけるフェイクの動向

現在，SNS におけるフェイクとして社会問題になっているのは，フェイクニュースとフェイク動画（ディープフェイク）である．以下では両者の動向を概観する．

4.1 フェイクニュースの動向

Facebook や Twitter などの交流系 SNS で流布される偽情報をフェイクニュースと呼ぶことが多い．報道機関が提供しているニュースと交流系 SNS のニュースを表２で比較する．表２において，交流系 SNS ニュースの特徴として，内容が社会的なもののみならず個人的なものへと拡大したこと，ファクトチェック機能がないためにニュースの信頼

性が低下したこと，受信者がニュースを拡散できるようになったこと，があげられる．このような，ニュースとしての変容は，デマの拡散をうみ，ネット炎上などの他者攻撃につながっていると考えられる．

表２　報道機関のニュースと SNS のニュース

	報道機関のニュース	SNS のニュース
発信者	ジャーナリスト	個人
報道の権利・資格	制限あり（報道倫理）	制限なし
発信者のなりすまし	難（少ない）	易（多い）
発信者の匿名性	小	大
受信者の行動	受信のみ	受信情報を拡散
内容の公共性	高い（政治的，社会的）	低い（個人的）
内容に対する責任	あり	なし
ファクトチェック	あり（専門機関，専従者）	なし

デマ拡散の事例として，表３に我が国における自然災害後のデマ拡散を示した．自然災害後のデマ拡散は，被災者をさらに追い込む悪質なものが多いが，現行の法制下では取り締まりが難しく，これまで，偽計業務妨害で逮捕された事案が１件あるのみである．また，SNS によるデマ拡散が人命を奪った例もある．2018 年 9 月 14 日に駐日台湾外交官が自殺した，という事件が報道された．この背景は以下のようであったと推定されている．すなわち，同月 4 日の台風 21 号により，大型タンカーが関西国際空港の連絡橋に激突し，多くの中国系観光客が空港に孤立した．その後，空港が手配したバスで救出されたのであるが，その際，「中国大使館が専用バスを手配して人々を救出した．台湾駐日事務所はなにもしてくれなかった」というデマが SNS 上で拡散した．このデマによって，台湾駐日事務所が多くの抗議にさらされ続け，責任者が自殺に追い込まれた，というものである．

文献[2]は 2016 年から 2017 年にかけて，Twitter で流れた約 126,000 件の投稿を対象に，デマ拡散の実態を調査し，統計的に分析した報告である．報道記事などに基づき事実確認を行い，投稿を真／偽（デマ）に分類して，延べ約 300 万人に約 450 万回 Tweet される過程を観測している．得られた主な結果は以下のようである．

・デマ投稿の上位 1%は，ほぼ常に 1000〜10 万人に到達した．一方，真の投稿は 1000 人以上に到達することは殆どない．
・デマ投稿は真の投稿よりも 6 倍ほど拡散速度が速い．

表３　災害発生後のデマ拡散の例

年月	災害	SNS 上のデマ拡散
2011 年 3 月	東日本大震災の千葉製油所火災	Twitter「有害物質が雨と一緒に降る」
2016 年 4 月	熊本地震	Twitter「熊本の動物園からライオンが逃げた」・・・偽計業務妨害で逮捕
2018 年 6 月	大阪府北部地震	Twitter「外国人は地震に慣れていないので犯罪をする」
2018 年 7 月	西日本豪雨	Twitter「レスキュー隊を装った窃盗グループが被災地に入っている」
2018 年 9 月	北海道胆振東部地震	LINE「○○市で地響きがしているので数時間後，再び大地震がくる」

4.2 フェイク動画の動向

フェイク動画は YouTube など動画系 SNS サイトにアップされ，閲覧されることが多い．ディープラーニング（深層学習）技術により，複数の動画から虚偽動画を合成するのが特徴で，ディープフェイクとも呼ばれる．2018 年前半に作成ツールが公開されて以来，急速に利用者が増大した．

現状，フェイク動画はある動画に写されている人の顔を他人の顔にすり替えたものが多く，殆どがポルノ動画であると言われている[3]. このようなフェイク動画を SNS にアップする目的は，アップサイトへのアクセス数をあげることによる広告収入獲得，リベンジポルノによる嫌がらせ，スキャンダル映像による政敵のイメージダウン，などが考えられる．

フェイク動画はフェイクニュースと同じ悪意のある偽情報であるが，デマ拡散という観点からみるとあまり有効な手段とはなっていない．この理由として，フェイク動画を作成するには，GPU（Graphics Processing Unit）を搭載した高性能コンピュータが必要で，多くの時間を要するなど，コストが大きいことがあげられる．また，技術的レベルも

まだ不十分で，全く違和感のない顔にすり替えできるまでにはいたっていない．また，フェイク動画には，映像に連携した音声（スピーチ）も必要となるが，標的者と見極めがつかないような音声を合成するのはまだ難しい．

以上から，現状，フェイク動画を見破るのは，それほど難しくはなく，デマ拡散リスクはフェイクニュースに比べ小さい．しかし，技術やコスト面の課題は日進月歩で克服されつつあるため，近い将来，手軽にフェイク動画が作成でき，交流系 SNS で処理されるようになると，デマ拡散リスクも大きくなると推定される．

5. ファクトチェックの現状

前章で示したように，交流系 SNS におけるフェイクニュース（デマ）の拡散の影響は大きく，その対策が急がれている．ここでは，対策の現状として，フェイクニュースのファクトチェックの動向と技術的な取り組みを概観する．

5.1 ファクトチェックの動向

4.1 で述べたように，従来，報道機関は専門家（専門組織や専従者）を配置し，自身が発信するニュース・記事の事実確認（ファクトチェック）を実施してきた．このファクトチェックは現在，SNS などの投稿にまで拡大されている．報道の自由度が高いとされる米国では 2000 年代前半から大学や新聞社がニュースのファクトチェックを実施しており，著名なものとして，ペンシルバニア大学の FactCheck.org[4]，ワシントンポストの Fact Checker[5]，などがあげられる．Fact Checker は虚偽のグレードをピノキオの数（4 段階）で表している．以上のように，報道機関が中心になって，ファクトチェックが実施されているが，近年は中立機関による取り組みも行われている．例えば，日本では，2014 年に日本報道検証機構がファクトチェックサイト Gohoo[6]をたちあげ，政治・社会・経済など幅広い分野のニュースを対象に，有志によるファクトチェックの結果を公開している．また，2017 年には，ジャーナリスト，大学研究者による，ファクトチェックの啓発・支援組織ファクトチェック・イニシアティブ・ジャパン（FIJ）が活動を開始した[7].

なお，SNS などインターネットサービス事業者側の取り組みは比較的遅れているが，Google は，他機関の協力も得て，2017 年より，同社検索サイトの内容をファクトチェックするサービスを提供している[8](ただし，日本語の場合は未実施).

5.2 技術的な取り組み

前節で示したファクトチェックは，ジャーナリストなど，各分野の専門家によって実施されている．これに対し，近年，ブロックチェーンや人工知能（AI）をファクトチェックに活かそうという技術的取り組みも開始されている．例えば，2018 年 5 月，スロベニアのイベンタム社は，最初にフェイクニュースを特定した人に対して，ブロックチェーンを用いて報償の支払いを保証するシステムを開発した[9]．また，米国マサチューセッツ工科大学などは，フェイクニュースを見破る AI の開発を進めている [10].

6. ファクトチェックの課題

前章までの考察を踏まえて，ファクトチェックの課題を整理する．以下，チェックの自動化，チェック対象の拡大，人工知能の利用，という 3 点から課題を整理する．

6.1 チェックの自動化

前章で示したように，現状，ファクトチェックは専門家（人間）が実施している．このため，以下が問題となる．

・チェックに公平さ・客観性を欠く可能性がある．
　ファクトチェックの担当者は否定するであろうが，社会生活を営む上で，組織や他者との利害関係のない人間はいない．また，担当者の主観がファクトチェックに反映しない，とも言いきれない．すなわち，専門家も人間である以上，不公平かつ主観的なチェックをおこなう可能性がある．
・チェックに時間を要する．
　優れたファクトチェックの専門家であっても，分を争うような事案をファクトチェックするのは困難である．さらに，ファクトチェックの専門家は少数であり，今後増大するであろうフェイクニュースに対応できなくなることが予想される．

以上から，ファクトチェックの自動化を検討すべきであろう．

6.2 チェック対象の拡大

現状，ファクトチェックの中心は SNS などのマスメディアを介したフェイクニュースやデマが対象である．このため，以下が問題である．

・公共性の高い政治的・社会的問題のみが対象である．
　一般生活者が個別に接するフェイク，例えば，振り込め詐欺やフィッシングメールなど，個人を標的にしたフェイクのファクトチェックは優先度が低く，実施されていない．
・個人の意思で個別にファクトチェックできる仕組みがない．
　SNS などにおいて，偽情報や不適切な投稿がチェックされる動向にあるが，これは SNS 事業者が一括しておこなうことが多く，専門知識やスキルのない個人が個別にチェックを希望しても実施する仕組みがない．

以上から，ファクトチェックの対象をニュース以外のフェイクにも拡大するとともに，個人の意思に基づくファクトチェックの実現を検討すべきであろう．

6.3 人工知能の利用

5.2 では，ファクトチェックを行う AI が開発されつつあることを示した．周知のごとく，AI は多方面で実用化されており，多大な導入効果を上げているが，現在広く応用さ

れている AI は，フェイクニュースのファクトチェックに向いていないと危惧している．以下，フェイクニュースのファクトチェックと AI の特徴から，この理由を概説する．

AI は文字情報，音情報，画像情報を機械学習することが前提になっている．すなわち，AI に多くの情報を与え，この学習を深めるほど能力を高めることができる．一方，**3.2** で，情報を多く学習するほど，情報エントロピーが低下し，情報が虚偽の場合は信じやすくなることを示した．フェイクニュースによってだまされるのは，その情報エントロピーが大きいからであると考えられる．しかし，AI を利用するには，この情報エントロピーは低いことが求められる．このことから，情報エントロピーの大きいフェイクニュースのファクトチェックに現在の AI は不向きといえる．

以上をイソップ寓話の「オオカミ少年」に当てはめると表４のように示すことができる．同表で，少年からの情報がニュース，村人は AI に該当する．同表は，村人は少年からの度重なるフェイクニュースを過学習し，最後にはニュースの真偽が正しく判断できなかったことを示している．

表４「オオカミ少年の話」におけるフェイクの学習と結果

少年からの情報	学習状態	ニュース性⇒判断	村人の対応・結果
最初の“オオカミが来た”（フェイク）	未学習	ニュース性大⇒判断不能	大騒ぎ（高対応）
2 回目の“オオカミが来た”（フェイク）	1 回学習	ニュース性低下⇒事実／フェイク半々	小騒ぎ（低対応）
何度も“オオカミが来た”（フェイク）	フェイクのみ多数回学習	フニュース性さらに低下⇒フェイク性増大	低対応化進展
最後の“オオカミが来た”（事実）	学習過多	ニュース性なし⇒無視	無対応による不幸な結末

7. 情報の真正性を保証するシステムの提案

前章の検討をもとに，デマ拡散の対策として，情報の真正性を保証するシステムを提案する．具体的に，SNS において“マジで？”ボタンと“マジで！”ボタンを利用してフェイクニュースやデマの拡散を防止する仕組み，および，デジタルフォレンジック技術[11]を用いてコンテンツのメタ情報をチェックするシステム／サービスを提案する．

7.1 SNS において“マジで？”ボタン・“マジで！”ボタンを利用してデマの拡散を防止する仕組み

広く普及している SNS において，投稿に対し，受信者が“いいね”，“フォロー”などのボタンを押すことで反応することが多い．これらのボタンは，概ね，受信者が投稿を肯定する（賛意や支持を示す）ものが多いため，デマを拡散させてしまう要因となっている．この問題に対して，受信者が投稿を懸念する（真正性の確認を要求する）ボタンと，投稿者が投稿の真正性を保証するボタンを追加することを提案する．具体的には，図１に示す“マジで？”ボタンと“マジで！”ボタンを付け加えた投稿画面を構成することを提案する．例えば，SNS 事業者は投稿に対する“マジで？”ボタンが押された回数を計測し，一定数に達した場合，一時的に投稿を削除して拡散を防止する．同時に，“いいね”，“フォロー”ボタンの機能を停止する．そのあと，SNS 事業者は投稿者に，“マジで！”ボタンを押して投稿の真正性確認要求に応える，よう促す．さらに，投稿者が“マジで！”ボタンを押し，確認要求に応えたことを受信者に通知する．このような，仕組みを用いて，真正性の確認が SNS 利用者自身によって多段階に実施されれば，デマのトラフィックを制限し，拡散を防げると考えられる．

なお，本提案は即時性が高いため，特に，緊急通報発生時の誤報の拡散防止と真正性保証に効果があると期待している．なお，ネットワーク的観点から，本提案は投稿者と受信者のピア・ツー・ピア型の保証システムに分類される．

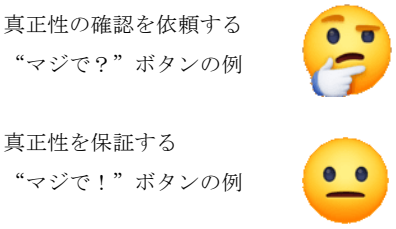

図１“マジで？”ボタンと“マジで！”ボタン

7.2 デジタルフォレンジック技術を用いてコンテンツのメタ情報をチェックするシステム／サービス

6.3 から，未学習で情報エントロピーの大きいフェイクニュースやデマを直接的（明示的）にファクトチェックすることは困難と考えられる．また，ファクトチェックが誤った場合のリスクも大きいことが分かる．ここでは，情報コンテンツの直接的なファクトチェックではなく，情報コンテンツのメタ情報をチェックし，間接的（暗示的）にファクトチェックするシステム／サービスを提案する．具体的には，フェイクニュースやデマを含むコンテンツ一般の

メタ情報（作成時刻，作成場所，作成者，作成ツール，拡散経路，情報サイズ，など）を調査・特定することを提案する．この提案は，直接的なファクトチェックの代替と位置づけられる．換言すれば，コンテンツの真正性を保証する，のではなく，コンテンツ作成に関する信ぴょう性を保証する，ということである．

このように，情報のメタ情報をもとに事実を解明する技術として，情報セキュリティ犯罪後に適用されているデジタルフォレンジック技術がある．デジタルフォレンジック技術は専門性が高く，個人レベルで実施するのは難しいので，専門スキルや調査資格を持った，SNS 事業者やセキュリティベンダが依頼を受けて実施することになろう．なお，ネットワーク的観点から，本提案は調査の依頼者と請負者からなるクライアント・サーバ型の保証システムに分類される．

表５に，上記両提案の比較を示したので参考にされたい．

表５　提案の比較

提案	SNS における“マジで？”ボタンと“マジで！”ボタンによるフェイクニュースの拡散制御	デジタルフォレンジック技術によるフェイクニュースのメタ情報チェック
保証内容	コンテンツの真正性	コンテンツ作成の信ぴょう性
保証形態	ピア・ツー・ピア型	クライアント・サーバ型
保証主体	当事者（投稿者）	第三者（専門家）
専門知識／スキル	不要	必要
客観性	小	大

8. まとめ

本文は，SNS におけるフェイク情報問題を取り上げた．最初に，情報の真正性とフェイクについて定義したあと，虚偽情報と信じやすさの関係を考察し，情報のサイズが大きいほど，情報が希少でエントロピーが大きいほど，信じやすいことを示した．そのあと，フェイクニュースやフェイク動画の動向を概観した．さらに，現状の，フェイクニュースのファクトチェックの動向と技術的な取り組みを示した後，ファクトチェックの自動化，チェック対象の拡大が必要であることを述べた．機械学習をベースとした人工知能がファクトチェックに向かないことも指摘した．これらの考察を踏まえて，コンテンツの真正性やコンテンツ作成の信ぴょう性を保証するシステムとして，SNS において“マジで？” ボタン・“マジで？”ボタンを利用してファクトチェックする仕組み，および，デジタルフォレンジック技術を用いてコンテンツ作成のメタ情報をチェックするシステム／サービスを提案した．

今後，関連する研究者や組織と議論を深め，提案システム／サービスの具現化を図る．

謝辞　本論文発表は，総務省 SCOPE「IoT デバイス認証基盤の構築と新 AI 手法による表情認識の医療介護への応用について」の研究開発（181603006)」の一環として行ったものであり，研究委託を頂いた総務省に謝意を表する．

参考文献

[1] 情報セキュリティ・キーワード 2016 ① 情報セキュリティマネジメント編 <https://www.iseeit.jp/if-sub-160405.html>, 2020 年 1 月 26 日アクセス
[2] S. Vosoughi，D. Roy，S. Aral,‘ The spread of true and false news online’, Science, Mar. 2018, Vol. 359, Issue 6380, pp. 1146-1151
[3] ディープフェイクで狙われる K-POP のスター達 <https://www.excite.co.jp/news/article/RollingStone_32156/>，2020 年 1 月 26 日アクセス
[4] FactCheck.org<https://www.factcheck.org/>, 2020 年 1 月 26 日アクセス
[5] Fact Checker < https://www.washingtonpost.com/news/fact-checker/>, 2020 年 1 月 26 日アクセス
[6] Gohoo<http://gohoo.org/>, 2020 年 1 月 26 日アクセス
[7] ファクトチェック・イニシアティブ・ジャパン <http://fij.info/>, 2020 年 1 月 26 日アクセス
[8] Fact Check now available in Google Search and News around the world <https://blog.google/products/search/fact-check-now-available-google-search-and-news-around-world/>, 2020 年 1 月 26 日アクセス
[9] ブロックチェーンでフェイクニュースと戦う新たな「Eventum」プラットフォーム <https://japan.cnet.com/release/30250328/>, 2020 年 1 月 26 日アクセス
[10] フェイクニュースを見破る AI が開発される？ < https://www.nttdata.com/jp/ja/data-insight/2018/1206/>, 2020 年 1 月 26 日アクセス
[11] 佐々木良一，上原哲太郎，櫻庭信之，白濱直哉，野﨑周作，八槇博史，山本清子,「デジタル・フォレンジックの基礎と実践」，東京電機大学出版局，2017 年 3 月