Vol.2017-EIP-77 No.4
2017/9/6

多面的信頼評価とオークションに基づいた fake news の自動推定

金子 格†

東京工芸大学†

概要：最先端の情報システムの応用において利用者が伝達される言説の信頼性に強い疑いを持つという事態が生じている。一方情報理論はノイズやエラーを含む構成要素から、システム鄭にはほぼ 100%エラーのない計算と通信を可能とする。本報告では、多面的信頼性評価に基づいて、直截な方法で信頼できる情報交換システムを構築する方法について考察する

On the estimation of fake hypothesis based on auction system and multi-lateral confidence evaluation.

ITARU KANEKO†

1. はじめに

最新のインターネットメディア，Twitter，Instagram, Facebook などの利用が急速に広がる中で fakenews, すなわちほぼ意図的な虚偽, 誤りとされる事実が広く拡散され信じられてしまう，という現象がおきていることは皮肉な状況である．情報システムの基盤である情報理論はもともと情報を誤りなく伝送することを可能とする理論的基盤であるからだ．これはやむを得ないことなのだろうか，あるいは情報の信頼度を上げる工夫を求めれば実現可能だろうか?本報告ではそうした試みの一つとして，多面的信頼性評価に基づいて、直截な方法で信頼できる情報交換システムを構築する方法について考察する

2. 動機

2010 年代以後, いわゆるソーシャルメディアの利用が急速に広がった．現時点においては Twitter，Instagram，Facebook などがその代表とされる．これらは最新のインターネット技術を活かしてきわめて大規模な情報交換を可能とし，現代の強力な情報基盤となった．たとえば大規模ストレージ，データベース，高速通信，高性能な端末，メモリやプロセッサの高性能化，映像符号化，ハイパーメディア技術，検索技術など，無数の技術の発達がこれらのメディアを支えている．

こうした最先端の情報システムにおいて，fakenews, すなわち「一般的にほぼ意図的な虚偽，誤りとされる事実が広く拡散され信じられてしまう」という現象がおきていることは，皮肉な状況である．なぜ皮肉かといえば，情報システムの基盤である情報理論はもともと情報を誤りなく伝送することを可能とする理論的基盤であるからだ．

情報理論はもともとノイズやエラーを含む構成要素からシステムが伝達しうる通信容量を求め，通信容量以内の情報は 100%誤りなく伝送できることを理論的に保障する．すなわち構成要素のエラーを全体としては波及させないだけでなく，完全にコントロールすることを可能とした理論である．だからこそ我々は 1 ペタ回の演算結果や膨大なデジタル通信に絶対的な信頼を持つことができる．

そのような理論に立脚するシステムが(複雑な階層構造を介しているとはいえ)アプリケーション層、すなわち最終的にそこから得られるメッセージの真偽が信頼できないのは皮肉な状況ではないだろうか．

そこで，それははたしてやむを得ないことなのだろうか?情報システムにユーザー層におけるメッセージの信頼度を高める機能を付加できるだろうか?こうした疑問について本報告では議論する．そして方法の一例として多面的信頼性評価に基づいて、直截な方法で信頼できる情報交換システムを構築する方法について考察する

3. 信号・ノイズ・情報

シャノンは”Mathematical Theory of Communication”で「信号」に「ノイズ」が加わり伝達されるとして「情報」の伝達をモデル化した．

† 東京工芸大学
Tokyo Polytechnic University

いうまでもなく今日の情報システムの根幹をなす理論的枠組みである．

あらためて指摘する必要はないと思われるが，情報理論では「信号」には「ノイズ」が加わるが「情報」は無劣化で伝送しうることが示される．つまりこのモデルにおいて[式 1]で与えられる帯域幅に収容可能な情報量であれば，情報を全く誤りなく伝達することが可能なのである．我々が情報システムに用いる構成要素はすべて，誤動作やノイズを含むものであり，この理論に基づいてノイズや誤作動の影響を取り除くことにより我々はペタ回の演算やペタバイトの伝送を全く誤りなく(1bit の誤りもなく)実行できる．

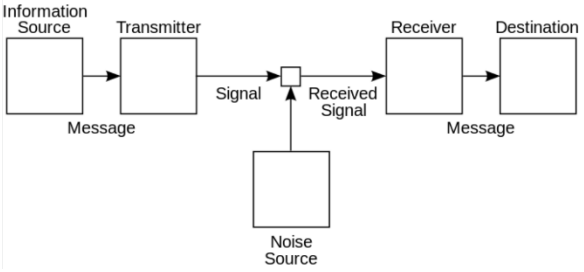


図 1 シャノンによる一般化された通信システムのダイヤグラム．「信号」に「ノイズ」が加わって受信されるが「情報」は保存伝達されることを示した．

$$C = \lim_{T \to \infty} \frac{\log N(T)}{T} \qquad [式\ 1]$$

そこで同様に SNS などで事実が伝搬によって歪められる状況も図 2 に示すようにノイズの付加によるものであるという自然な発想によってモデル化してみよう．ここで S は発信者であり Fact(事実)を持っている．これが送信 T、受信 R というプロセスの間でノイズ N の妨害をうけるから R で受け取る信号はノイズを含んでいる．しかし適切な T と R の処理を施せば S で送信した Message(情報)は D に誤りなく伝わるはずである．

4. ソーシャルネットワークへの拡張

同様のモデルをソーシャルネットワークに拡張することを試みる．ソーシャルネットワークのように多くの情報仲介者が関与し中継地点でノイズが加わるから図 3 のようなネットワーク構造になると考えられる．ここで S は送信者で T は送信処理である．途中 N はノイズが加わることを現し M はノイズが加わってひずんだ signal を再送信する仲介者を現す．最終的に signal は D で受信して S にメッセージとして伝えられる．

T と R の目的は S から D に Fact(Message)を無歪(誤りゼロ)で伝送することである．このとき信号の伝搬経路全体がノイズの加わった信号路とみなせる．したがって Message が経路の伝送容量を下回っていれば S から D に無歪伝送が可能である．

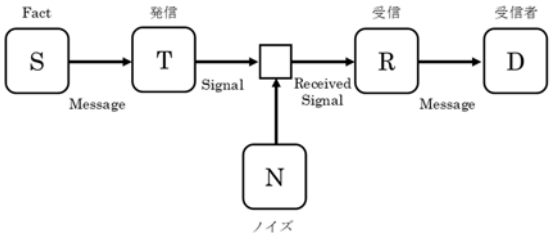


図 2 情報源を Fact とし，伝聞による損失をノイズとしてモデル化したダイヤグラム..

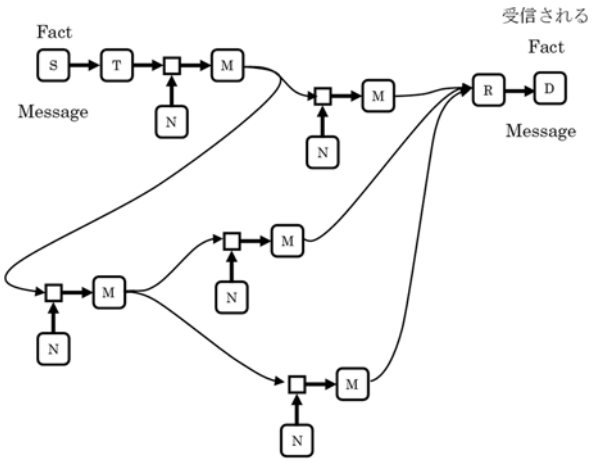


図 3 ノイズの付加を伴いつつ複雑に伝搬する信号の伝達を現すダイヤグラム．

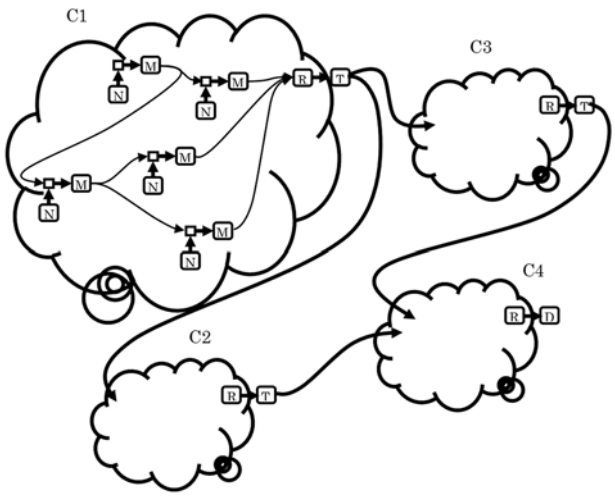


図 4 ネットワーク中に ECM＝エラー訂正機能を持つ中継点を持つネットワーク．

SNS ではさらにネットワーク中に複数の情報源などによってエラー訂正をしてから再発進する中継者が存在する．このような中継者を CIC(Confidence Implementation Component)と呼ぶことにする．

無歪伝送が可能でありその条件もわかっているので，一見問題は解決したようだがむろんそうではない．具体的に無歪伝送を実現するには以下 3 つの事項を明らかにしなければならない．

(1) Fact(Message)の定義

(2) T と R に用いる技術

(3) CIC の信頼性評価

5. 無歪伝送の条件

5.1. 何を Fact(Message)とする

まず S が伝送する Fact(Message)が何であるかを明確にする必要がある．Fact 自体があいまいなものであれば無歪伝送はあまり意味がない．

すべての人がその気になれば確認できる完全に安定した情報であれば Fact となりえる．一方でたとえば東京地方の気温は，観測方法が確定していないので，伝送歪と測定誤差の切り分けが困難であろう．定義のはっきりした年間平均気温であれば多数の観測によって真値に近づくことが保証できるから Fact として扱うことが可能と考えられる．

5.2. T(送信)と R(受信)に用いる技術

T と R には通常使われているエラー検出，エラー訂正手法が利用できる．この場合単一事象のエラーは訂正不可能である．エラー検出，エラー訂正には多数の伝送チャネルや，ある程度長いデータ列を用いる必要がある．

たとえば単一企業の株価をノイズのある経路で正確に伝送することはできないが，平均株価であればより信頼度の高い伝送が可能である．あるいは毎日の株価が不正確であっても 4 半期毎の平均価格はより正確に伝送できる．

ターボ符号など高性能な符号化を用いれば保障された伝送容量に近い情報量の Message を無歪で伝送することができる．

5.3. CIC(中継者)の信頼性評価

CIC は複数の信号を総合して一旦誤り訂正をしてから情報を再送信する．したがって本来 CIC は無歪の情報を発信することが望ましい．

CIC はそれ自身が様々な独自の手法で情報の信頼性を確認することが可能である．ネットワークの分散管理的な特性を維持するためには CIC の信頼性はここの CIC が独自の手法で行った方が望ましい．各 CIC が独自の方法で情報の信頼性を確認することで，ネットワーク全体としては fake news の様々な手法に対する頑健性が担保できるからである．

さらに分散された CIC 自体の信頼性を評価する手法が必要である．CIC は相互の結果を利用し，かつ誤りを発生することがある．CIC がお互いの情報を利用して効果的に誤り訂正を行うには相互の誤り率の推定が必要である．

以上で，無歪伝送のための 3 つの要素を説明したがこのうち 5.3 CIC の信頼性評価が最も大きな課題であると考えられる．そこで本報告の後半では CIC の信頼性評価の実現方法を検討する．

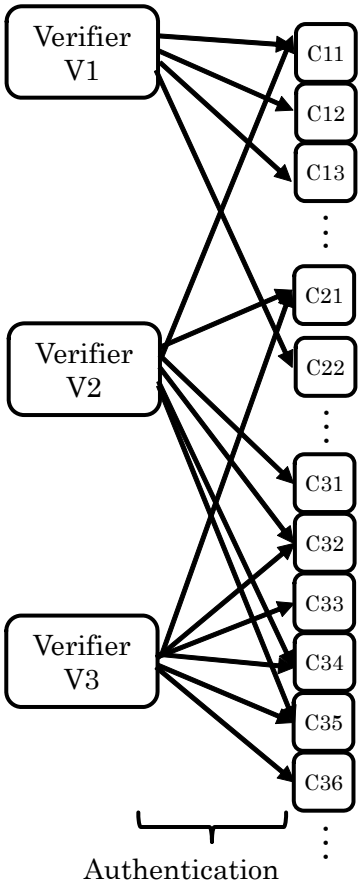


図 5 多面的信頼性評価のシステム構造の一例

6. 多面的信頼性評価

以下では前章までにその必要性を論じた，ネットワーク中で誤り検出訂正機能を担う CIC(中継者)の信頼性評価の実現手法を検討する．その実現方法には様々な可能性があるが，実現方法の一例として多面的信頼性評価と呼ぶ手法を提案し，実行方法を論ずる．ここで示す手法はすでに先行研

究として IoT(Internet of Things)のセキュリティ評価に提案した手法[3]を CIC の信頼性評価に応用している．IoT においても分散管理環境の中で軽量で信頼性が高く自立分散的な信頼性評価が必要である点が，CIC の信頼性評価と似ている．

また同手法は近年多くの分野で応用が検討されているブロックチェーン技術[4]を，従来から著者が提案している多面的安全性モデル[5]に導入して拡張したものである．

6.1. フレームワークの構成要素

多面的信頼性評価におけるシステム構造の一例を図 5 に示す．図の左半分は Verifier を示す．Verifier V1～V3 は各 CIC の信頼性を評価する．

Verifier が評価する対象が CIC C11～C13…，C21～C22…，C31～C36…であり，図に示すように複数の Verifier がさらに多数の CIC を評価するという構造を持つ．

6.2. 信頼性の評価モデル

次に信頼性評価をモデル化する．本稿では CIC C11～C36…に信頼性の問題が発生した場合，それは問題を有する CIC を評価した Verifier の問題であるとして議論を進める．いい方を変えれば Verifier の信頼性のみを仮定し，CIC の信頼性は Verifier に起因するものとしてモデルの挙動を論じる．

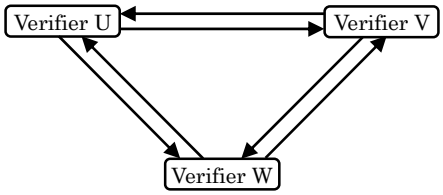


図 6 多面的相互評価.

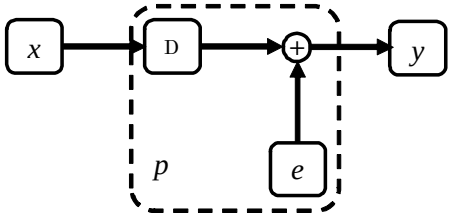


図 7 Verifier の実験用エラーモデル

7. 提案システム

次に，提案システムを示す．提案システムは PMLSM と相互評価，そしてブロックチェーンにより交換される相互評価情報からなる．

7.1. PMLSM

提案システムの第一の要素は確率的多面的安全性モデル(以下 PMLSM)である．PMLSM は安全性の高い信頼性の実現のため筆者等が提唱している信頼性管理方法である．PMLSM の構成とその特徴を図 8 に示す．

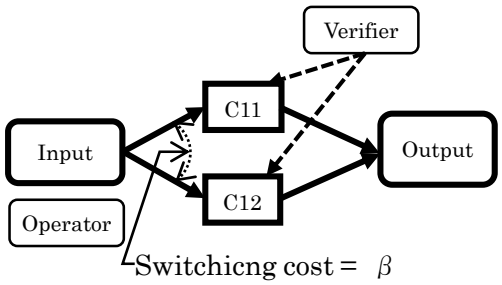


図 8 多面的信頼性評価モデル

本図の C11, C12 は図 5 の C11，C12 とは別の一般的な任意の 2 つの CIC である．C11 と C12 は交換可能な(同一機能を果たし得る)で，β はこれらの切り替えコスト(Switching Cost)であるとする．評価を行うのは Verifier であり切り替えを行うのは Operator である．

金子等は PMLSM においてゲーム理論により Verifier と Operator のとりえる選択の利得行列を分析した[2]．その結果切り替えコストβが高いと Verifier が Operator に信頼性不良を報告しない戦略が「ナッシュ均衡」として成立し Verifier が欠陥を報告しないと利得が上がることが示された．このように PMLSM を利用すると Verifier と Operator の相互関係，交換コストが Verifier の信頼性にあたえる影響を推定することができる．一方具体的にどのような機構でどういう計算方法で評価を得るかは示されていなかった．

表 1 Mutual Evaluation of Verifier

	V1	V2		V3	V4	V5	Avg
c01	0.123	0.101		0.091	0.123	0.100	0.108
c02	0.125	0.172		0.129	0.159	0.110	0.139
c03	0.099	0.120		0.060	0.082	0.073	0.087
c04	0.135	0.085		0.079	0.053	0.075	0.085
c05	0.106	0.095		0.139	0.103	0.086	0.106
c06	0.063	0.137		0.115	0.120	0.102	0.107
c07	0.103	0.091		0.053	0.095	0.054	0.079
c08	0.039	0.046		0.033	0.058	0.130	0.061
c09	0.019	0.065		0.081	0.045	0.028	0.048
c10	0.151	0.115		0.079	0.089	0.162	0.119
RMS error	0.028	0.018		0.024	0.017	0.030	

表 2 Mutual Evaluation Experiments

	Nv	Np	P(D)	$\bar{ev}$		$\bar{e}$	$\bar{y}$
Experiment1	10	100	0.2	0.1		0.1	0.1
Experiment 2	10	50	0.1	0.1		0.1	0.1
Experiment 3	10	50	0.1	0.2		0.2	0.2

そこで提案システムでは各種の推定を複数の Verifier が行い，その評価の信頼性を相互に評価させることを提案する．図 6 に Verifier の相互評価を示す．Verifier が相互の情報を信頼できる形で参照できればこのように Verifier が相互に信頼性を評価することが可能になる．

7.2. ブロックチェーン

第二の要素はブロックチェーンである．ブロックチェーンは相互評価に必要な信頼できる情報共有に利用できる

ビットコインで注目されたブロックチェーンの本質的機能は分散処理可能な台帳管理である．電子署名により改ざんを防止した「ハッシュチェーン」を拡張すると，だれでもがハッシュチェーンに記入可能かつ検証可能とすることができる．ブロックチェーンを利用すると基本的に，特定の管理者を設置することなく自由に記入が可能で整合性のとれた台帳を共有することができる．

相互に評価結果を参照可能とすれば Verifier が相互の信頼性を多面対照的に評価することが可能になる．

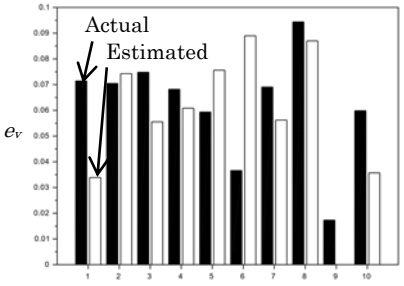
表 1 にそのような評価方法の一例を示す．ここでは各 Verifier の各 CIC の評価結果が示されている．この評価結果をブロックチェーンにより相互に電子署名しながら共有するものとする．各 Verifier の評価結果には個別の誤差と Verifier に依存する誤差がありその結果約 0～0.2 になる．表では全 Verifier の評価の平均値を最尤推定値として求め，個々の Verifier の評価値との差を error として Verifier 毎に RMS error を算出している．ここでは V4 の 0.017 が最小である．様々な相互評価の方法がとりえるが，その一つとしてこのように総平均で推定値を求め，そこからの誤差により Verifier の信頼性を推定するという単純なこの方法も可能である．

8. シミュレーション実験

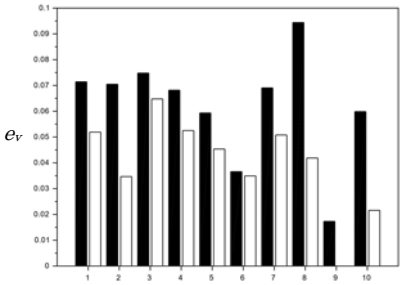
次に現実的な状況で Verifier の評価が可能かをシミュレーションにより確認する．具体的には多数の Verifier とさらに多数の CIC が存在し，Verifier は CIC の信頼性について非常に低い確率で CIC の不完全な情報を得ているような場合を想定し，提案した Verifier の相互評価により，Verifier 固有の誤差が小さい Verifier を選択できるだろうか，という疑問点を実験で確認する．

図 7 に Verifier の実験用エラーモデルを示す．観測変数 x(p)は 0～1 の値をとる p 番目の CIC の信頼度である．Verifier v は v 番目の Verifier を表す．Verifier が CIC の信頼性について情報を得る確率は小さいとし，観測確率 P(D)で x(p)を観測できるとする．たとえば観測率 P(D)=0.1 では全 Verifier が x(p)を観測するのは 10 回中 1 回だけである． Verifier の評価結果には大きなノイズが加わるとし Verifier 固有のノイズ ev と純粋なノイズ e(t)が加わり，観測結果 yv(p)を得るものとする．ここで e(t)は完全にランダム(観測のたびにでたらめなノイズ)とする．

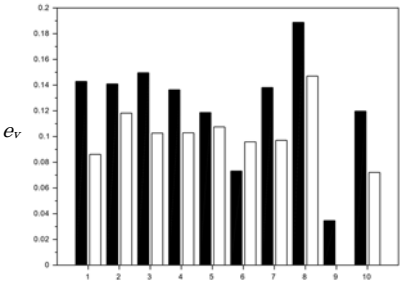
表 2 に実験条件を示す．Nv は Verifier の数，Np は CIC の数，P(D)は観測率，ev は Verifier 依存ノイズの最大値， e はランダムなノイズの最大値である．



(a) Experiment 1



(b) Experiment 2



(c) Experiment 3

図 9 実験結果.

図 9 に実験結果を示す. 横軸は Verifier を示し，black(Actual) は Verifier 依存ノイズ ev，white(Estimated)は相互評価による推定値で，いずれも値が小さいと誤差が小さいことを示す．ev

の値が大きい場合,似た傾向を示す Verifier 同士が相互に高い評価をするため Estimated の大小は ev の大 小と相関しない場合がある. しかし ev の実値(Actual)が良い 場合は Estimated も良い(低い)値が期待される.

実験結果は期待通り ev が最小である Verifier #9 が相互評 価でも最小となった.

結果はノイズに左右されるので常に最良の Verifier が選択 されることは保証されない. しかし多数の Verifier 間の相互 評価により Verifier 固有の誤差 ev が小さい Verifier を識別で きる可能性が高いことが示された.

9. オークションの導入

これまで，ソーシャルネットワークに情報伝達を拡張し，その伝達における誤り検出と誤り訂正の自律分散的な構成を論じ，自律分散的な Verifier により相互の信頼性と CIC の信頼性を評価する可能性を示した. しかし, いかなる Verifier がどのような目標と基準で作成されシステムに組み込まれるかについては論じられていない.

Verifier 自体はシステムの中で特に有用な機能を有していない．本報告が論ずる自律分散型の情報交換システムにおいて多数の Verifier を積極的に構築するインセンティブが見当たらない．Verifier は CIC の欠陥を検出することを目的とし CIC は情報の不確実さを伝えることを期待されているが，いずれも情報を受ける時点では情報の価値を下げてしまうから，そのままではそれらの機能を積極的に果たすインセンティブが CIC にも Verifier にもないことは，本システムの信頼性を大きく損ねてしまう.

一つの解決策として情報保険とオークションによって Verifier に CIC の評価のインセンティブを与えることを提案する.

Verifier の性能は先に示したように相互評価によって相互的に透明性を持って評価することができる．そこでこの性能を指標とした保障取引とオークションを併用すべきだと考える.

Verifier 保障の枠組みを表 3 に示す. 各 Verifier は目標となる CIC の性能を示し, 実績が上回る限り保障人は保障利用者から保障料を受け取る．実績を下回った場合は保障人が保証利用者に保険金を支払う．Verifier の運営開発者はその差額を活動資金とする.

この枠組みにおいて保証人を引き受ける場合に Verifier が保証金からみて高性能であることが求められるから保証人には自ら高性能な Verifier を選別するインセンティブが生じる．Verifier も実績と開発計画において保証人に魅力的であるためには，効率的でリスクの少ない信頼性評価システムの構築を目指すインセンティブが生じる．そして保障利用者はできるだけ安価で高性能な Verifier を選択するが，同時にリスク分散のため各 Verifier の保障条件や保障の原資にも考慮することになる．Verifier によって保障範囲が異なれば，利用者は目的に応じて Verifier を分散して組み合わせた方が安全であるから，保障金を確実に得るために Verifier の分散化のインセンティブも生じることになる.

表 3 Verifier 保障の枠組み

予定 e_v	実 e_v	保障人	保障利用者
e_v<A	e_v>A	保障金支払い	保障金受け取り
e_v<A	e_v<A	保障料受け取り	保障料支払い

10. まとめ

SNS の普及に伴い伝達される message の真偽がわからないという問題に着目した. SNS の特性を利用し複数の伝達経路があることなどを利用して情報の信頼性を高める方法を提案した．さらにそのために情報の誤り訂正を担う CIC : Confidence Implementation Component が元データの回復に寄与し，全体としてより高い信頼性を自動的に追及していくフレームワークを示した．最後にオークション手法により Verifier に性能向上と，相互の独立性を高めるインセンティブを与えるという方法を提案した．オークション手法については現状枠組みを示したにすぎずシミュレーション等による評価は行っていないので，オークションをとりいれたシステムの評価は今後の課題としたい.

参考文献

[1] Claude E. Shannon, Warren Weaver. The Mathematical Theory of Communication. Univ of Illinois Press, 1949. ISBN 0-252-72548-4

[2] 金子 格, 白井 克彦,「高度デジタル AV フレームワークの多面的安全性とその特性」, 情報処理学会論文誌 Vol. 41, No. 11, 3010-3018(2000)

[3] 金子格，確率的多面的セキュリティモデルとブロックチェーンを用いたメディア IoT 向け軽量セキュリティフレームワーク，電気学会論文誌C，137(6), 796-801 (2017)

[4] 佐古和恵,「透明性と公平性を実現するブロックチェーン技術」, 情報処理学会誌, vol. 57, No. 9, 864-869(2015)

[5] 金子 格, 白井 克彦,「高度デジタル AV フレームワークの多面的安全性とその特性」, 情報処理学会論文誌 Vol. 41, No. 11, 3010-3018(2000)