一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2024-240(2025-03)

動的クラスタリングによるPBFTのビザンチン障害の耐性向上

岡田　鉄平†　　上山　憲昭††　　藤原　明広†††

† 立命館大学 大学院 情報理工学研究科
〒567-0870 大阪府茨木市岩倉町 2–150
†† 立命館大学 情報理工学部
〒567-0870 大阪府茨木市岩倉町 2–150
††† 千葉工業大学 工学部
〒275-0016 千葉県習志野市津田沼 2–17–1
E-mail: †is0498ex@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp, †††akihiro.fujihara@p.chibakoudai.jp

あらまし　近年，取引を改ざん困難な状態で複数のコンピュータ間で共有し，管理するブロックチェーン技術が注目を集めている．ブロックチェーンでは，新たなブロックを追加する際に台帳情報を参加者全員で共有するための合意形成が行われる．この中でも，PBFT（Practical Byzantine Fault Tolerance）は，主に一部の組織内で使用されるハイブリッド型ブロックチェーンに採用されている．PBFTは，故障や攻撃を受けたノード（ビザンチンノード）に対して耐性を持つアルゴリズムであり，ビザンチンノード数が全体の3分の1未満であれば正しく合意に達することができる．一方，PBFTは，正常なノードが全体の3分の2以上であることが前提となるため，攻撃者が一定数以上存在すると合意形成が困難となる．既存の研究では，クラスタリングを用いてPBFTのスループットを向上させる手法が提案されているが，これらの方法は静的であり，動的な環境に対応できないという課題がある．さらに，ビザンチン耐性の向上を目的としたクラスタ構成法については，未だ十分に検討されていない．そこで本稿では，PBFTにクラスタリングを適用し，攻撃者の位置を推定することにより，ビザンチンノードに対する耐性を持つクラスタを構成する新たな手法を提案する．
キーワード　ブロックチェーン, PBFT, クラスタリング

Enhancing Byzantine Fault Tolerance in PBFT through Dynamic Clustering

Teppei OKADA†, Noriaki KAMIYAMA††, and Akihiro FUJIHARA†††

† Graduate School of Information Science and Engineering, Ritsumeikan University
2–150 Iwakura-cho, Ibaraki, Osaka 567–0870
†† College of Information Science and Engineering, Ritsumeikan University
2–150 Iwakura-cho, Ibaraki, Osaka 567–0870
††† Faculty of Engineering, Chiba Institute of Technology
2–17–1 Tsudanuma, Narashino, Chiba 275–0016
E-mail: †is0498ex@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp, †††akihiro.fujihara@p.chibakoudai.jp

Abstract　In recent years, blockchain technology, which enables transactions to be distributed across multiple computers and managed in an immutable and secure manner, has garnered significant attention. Within blockchain networks, consensus mechanisms ensure the consistent sharing of ledger information when new blocks are added. In hybrid blockchains, typically employed by a limited number of organizations, the Practical Byzantine Fault Tolerance (PBFT) protocol is widely used. PBFT is designed to tolerate Byzantine nodes—nodes that may be compromised or malfunctioning—by achieving consensus as long as fewer than one-third of the total nodes are Byzantine. However, PBFT relies on the assumption that at least two-thirds of the nodes behave correctly, making consensus challenging when the number of malicious nodes exceeds this threshold. Previous research has explored the use of clustering to enhance throughput, but these methods are static and unsuited to dynamic environments. Moreover, clustering techniques aimed at bolstering Byzantine resistance remain underexplored. This paper presents a novel method for constructing clusters within a blockchain network to resist Byzantine nodes. By employing clustering, we estimate the locations of potential attackers, thereby enhancing the system's resilience to Byzantine faults.
Key words　blockchain, PBFT, clustering

1. はじめに

ブロックチェーンは，取引を改ざん困難な状態で，複数のコンピュータ間で台帳を共有して管理する技術である．ブロックチェーンは主に許可型，自由参加型，ハイブリッド型に分類される．許可型は管理者が不在で透明性の高いというメリットがある一方，参加者数や取引量が増加すると送金処理や承認処理に時間がかかるデメリットがある．自由参加型では，単独の管理者によって参加者が制限されるブロックチェーンであり，データを完全に公開する必要がなく，承認時間も短い．しかし管理者に権利が集中するため，データの分散性は許可型よりも劣る．

ハイブリッド型は，許可型と自由参加型の中間に位置するブロックチェーンであり，複数の管理者が存在する．ブライベートチェーンより処理時間は遅いものの，権利が分散しているためデータ改ざんの耐性は高い．また，ブロックチェーンでは，新たなブロックやトランザクションが作成された際に参加者全員で検証を行う合意形成が採られており，これにより改ざん可能性のあるトランザクションを検知，排除することが可能となる．特にハイブリッド型では，PBFT (practical byzantine fault tolerance) [1] が主に採用されている．PBFT では，ビザンチンノード数が全体の 3 分の 1 未満であれば正しく合意に達することができる．一方，PBFT は 3 分の 2 以上の正常ノードが存在することが前提であるため，図 1 のように，攻撃者が一定数以上存在すると合意形成が困難となる．

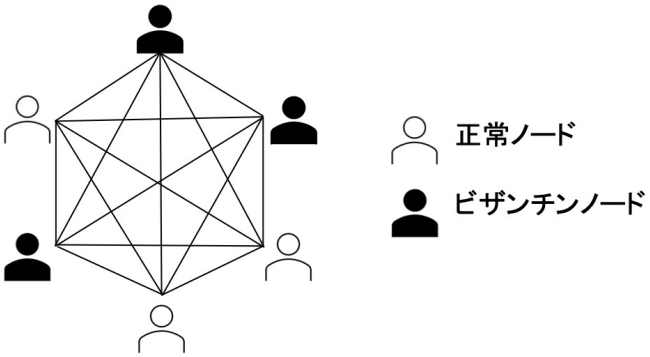

図 1　PBFT

このように，PBFT はビザンチンノードに合意が左右される．そこで本稿では，クラスタリングによりトポロジを分割し，攻撃者の場所を推定して特定のクラスタに集中させることで，ビザンチン攻撃に対する耐性を向上させる方式を提案する．一方で提案方式ではクラスタリングに伴い通信トラフィック量が増加することが懸念される．そこで提案手法を用いた場合の合意形成確率および通信トラフィック量を比較する．本研究の主な貢献を以下に示す．

- 合意を形成するために，参加者のうち 3 分の 2 以上の正常ノードを必要とする PBFT において，提案方式を用いることで正常ノードが 3 分の 2 以下でも正しく合意に達することが可能となる．
- 合意形成確率の上限値を理論解析し，シミュレーション結果が理論値と一致していることを示す．
- 通信トラフィック量の上限値を理論解析し，クラスタ数とトラフィック量の関係を明らかにする．

2. 節では関連研究について述べ，そして 3. 節で提案方式を述べる．4. 節では性能評価について述べ，最後に 5. 節でまとめを述べる．

2. 関連研究

PBFT [1] はクライアント，レプリカノード，プライマリノードにより構成される．クライアントはトランザクションを生成してネットワークに送信し，レプリカノードはネットワーク内の各ノードを指す．プライマリノードは特定のレプリカノードであり，クライアントからトランザクションを受け取り，他のレプリカノードに転送する役割がある．また，正確な合意を取るため，図 2 のように，クライアントがプライマリノードにトランザクションを送信した後，pre-prepare フェーズ，prepare フェーズ，commit フェーズの三つの段階を通じて合意を達成する．

- **pre-prepare フェーズ**:
プライマリノードが他のレプリカノードにトランザクションを転送し，それを受け取った各ノードはトランザクションの正当性を検証した後，他ノードに検証結果をブロードキャスト
- **prepare フェーズ**:
レプリカノードが検証した結果が，プライマリノードの検証結果と一致していることを確認し，他のノードに結果をブロードキャスト
- **commit フェーズ**:
prepare フェーズで受け取ったメッセージに同意する場合，commit メッセージを他ノードに送信

最終的に，全体の 3 分の 2 以上のノードから commit メッセージを受信することで，正しく合意に達した旨を reply メッセージとしてクライアントに送信する．

プライマリノードが障害を起こす，または悪意のある振る舞いをした場合，PBFT では，ビュー変更 (View Change) プロセスを開始し，新たなプライマリノードを選出する．このプロセスは以下の手順で行われる．

- 各レプリカノードは，現在のプライマリが信頼できないことを示すビュー変更メッセージを他の全ノードに送信
- 各ノードは，事前に定義された基準に基づいて新たなプライマリノードに合意
- 合意が得られた後，新しいプライマリが責務を引き継ぎ，コンセンサスプロセスを再開

ビュー変更は，プライマリノードの障害からネットワークを復旧させる際に，safety と liveness を損なうことなく実現するものである．また，PBFT では，与えられたデータについてコンセンサスを達成するよう設計されているため，フォークが発生することはないが，コンセンサスが達成されない場合がある．

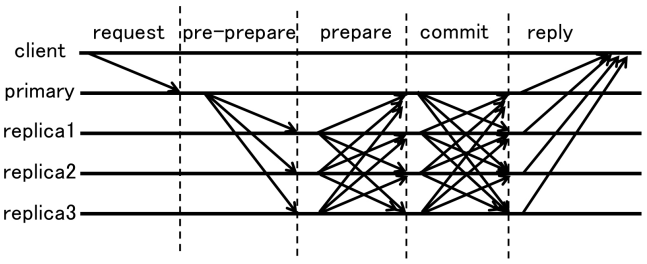

図 2　Consensus process of PBFT

[2] では，Ethereum 2 におけるバリデータノード間のブロック通信の時間的変動についての理論的分析を行っている．この研究では，ブロックを生成したノードから他のノードにブロックをブロードキャストする過程をモデル化しており，この過程は，マルコフ過程として定義され，各ノードがブロックを受信する確率が考慮される．全ノード数を N とすると，ブロックを送信する際の通信複雑性は $O(N^2)$ となり，通信遅延時間は，

$O(N \log N)$ となることを確認した．

[3] では，PBFT においてノード間のやり取りが多いため，通信オーバヘッドが大きいことに着目し，RC-PBFT (Random Cluster PBFT) を提案しその有効性を示している．クラスタリングによりクラスタを作成し，ランダムに選択されたクラスタ上で PBFT が実行され，その結果を他のクラスタにブロードキャストするというアプローチをとっており，従来の PBFT と比較してコンセンサスに要する時間の減少やスループットの向上という結果が確認された．しかし，本論文はクラスタ選択の最適化が不十分であることを主要な課題としており，ランダムなクラスタリングの使用によるビザンチンノードへの耐性が欠如している．

[4] では，PoW (Proof-of-Work) におけるトランザクション検証の遅さが課題であるとし，クラスタ内およびクラスタ間の並列マイニングを通じて検証に要する時間を短縮する手法を提案した．図 3 に示すように，ネットワークはマイニングを行うマイニングノードと他のクラスタにブロックを送信するフルノードで構成されている．全てのクラスタで同時にマイニングを開始し，ナンスを発見したマイニングノードはブロックをフルノードに送信し，そのフルノードは自身のクラスタ内のマイニングノードおよび他のフルノードに送信する．ブロックを受け取った全てのフルノードは自身のマイニングノードにブロードキャストし，検証を行う．実験の結果，コンセンサス時間を短縮し，ネットワークのスケーラビリティの向上を確認した．しかし本論文では，クラスタリングに基づくトポロジ改善がネットワークセキュリティにどのように寄与するかについての具体的な評価やシミュレーション結果は提示されていない．特に，攻撃者の数が異なる場合における耐性に関する詳細な分析が不足している．

[5] では，複数のロボットで構成されたネットワークにおいて，分散ネットワーク構造を採用することで，スケーラビリティや単一障害点の解消が期待されるが，PBFT による合意を形成するために複数回の通信が必要であることを懸念している．そこで K-means 法に基づいてロボットノードをクラスタごとにグループ化し，グループ間のコンセンサス遅延やエネルギー消費を低減する手法を提案している．また，各クラスタにおけるコンセンサスプロセス中のノードの挙動を観察およびスコア化し，スコアの高いノードをランダムにプライマリノードとして選択することで，プライマリノードの信頼性を向上させている．

[6] では，ブロックチェーンのシャーディング技術について体系的かつ包括的なレビューを提供し，シャーディングの主要な要素や課題を特定している．シャーディングは，ブロックチェーンネットワークのスケーラビリティを向上させるために，ノードを複数のグループ（シャード）に分割する技術であり，各シャードが独立してトランザクションを処理できるため，全体の処理能力が向上する．この研究では，シャーディングの実装における主要な要素や，直面する可能性のある課題について詳しく分析している．提案された方式はデータの整合性を強化する可能性を示しているものの，この問題に対する完全な解決策を提供しているわけではない．

[7] は，データを効率的に伝送するための手法であるネットワークコーディングを PBFT に活用する研究である．提案手法は最大帯域幅の要求を削減することにより，スケーラビリティを向上させることを目的としており，従来手法と比較して通信効率が向上し，スケーラビリティが改善されることを示した．[8] では，ブロックチェーンのスケーラビリティを向上させるためのソリューションを三層アーキテクチャに基づいて説明している．特にシャーディングや異なるレイヤで処理を分担することで，全体の効率を高めることを目的としている．[9] では，既存のシャーディングスキームをブロックチェーンの種類やシャーディング技術に基づいて分類し，それぞれの利点と欠点を分析している．さらに，シャーディング技術の適用性に関

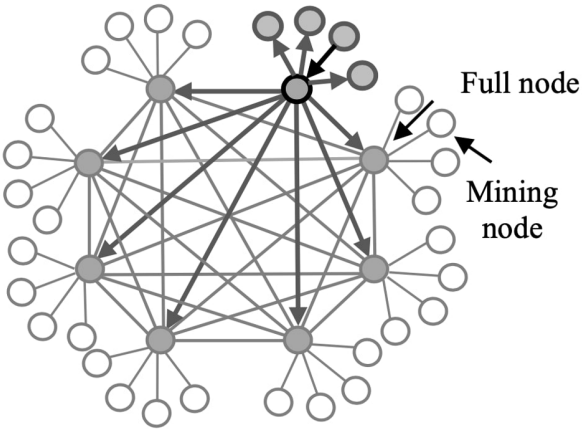

図 3　Parallel mining

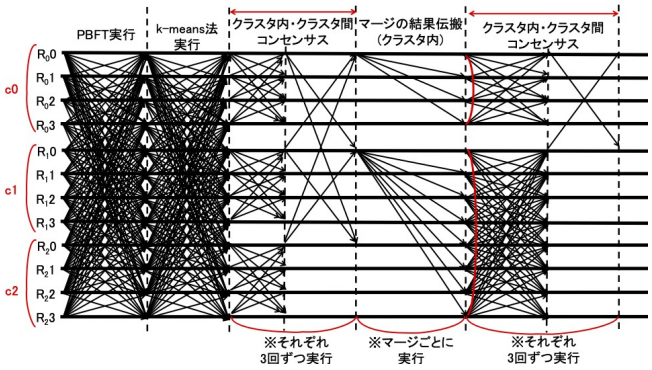

図 4　Flow of proposed method

する基準も設定している．

3. 提 案 方 式

3.1 概　　要

提案方式の流れを図 4 を用いて説明する．

（1） 全体で PBFT を実行

（2） 合意が形成できなければ，ネットワークに k-means 法を適用

（3） それぞれのクラスタ内で PBFT を実行

（4） 各クラスタ内の結果を基に，クラスタ間で PBFT を実行

（5） 合意が取れなかった場合，少数派の意見を送信したクラスタ内に攻撃者が多いと判断し，これら少数派のクラスタを 1 つにマージ

（6） コンセンサスの形成に成功した場合，その旨をネットワーク全体に共有し，終了

このように提案方式では，クラスタリングを用いることで攻撃者の多いクラスタを推定し，それらをマージすることで全体に占める攻撃者クラスタの割合を減少させることで，正しく合意に達する可能性を増加させる．また，k-means 法によるクラスタリングやマージ処理は，各ノードが自律的に実行し，その結果をそれぞれ共有する必要があるため，位置情報などをブロードキャストするためのフェーズが存在する．

具体的な流れを，図 5 を用いて説明する．白丸はブロックチェーンネットワークにおける正常ノードを，黒丸はビザンチンノードを表している．20 ノードのうち 6 ノードがビザンチンノードであり，ビザンチンノードが全体の 3 分の 1 を超えて

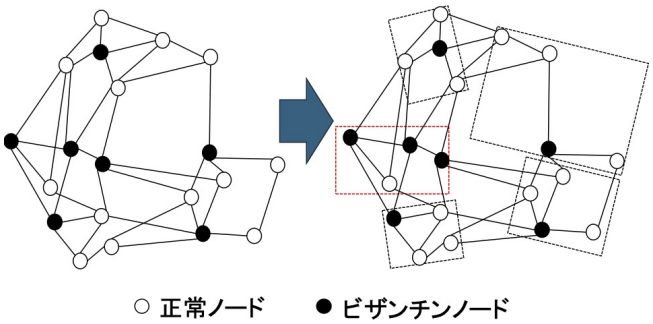

図 5　Clustering

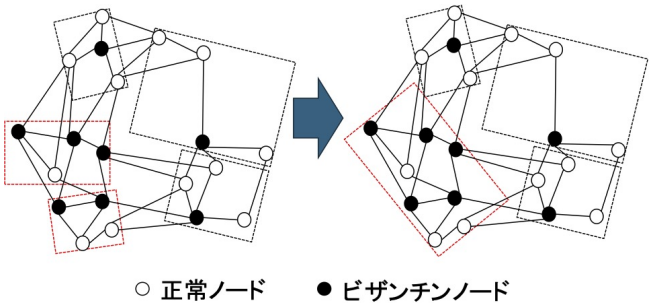

図 6　Merging clusters

いるため，この状態で PBFT を実行しても合意を形成することは不可能である．そこでクラスタリングを行った結果，赤の点線で囲った部分のような，ビザンチンノードがクラスタ内の 3 分の 1 以上存在するクラスタが 1 つ発生した．それぞれのクラスタ内で PBFT を実行し，またクラスタ間でも PBFT を実行すると，5 つのクラスタのうち，合意に達したクラスタは 4 つであるため，正しく合意を形成することができる．

一方，図 6 の左図のように，クラスタリングを実行しても，ビザンチンノードが多数を占めるクラスタが 2 つ発生し，3 分の 1 以上の賛成を得ることができず，合意形成することができない場合がある．そこで少数派のクラスタ (赤点線) を合成することにより，4 つのクラスタのうち正常なクラスタは 3 つとなり，正常に合意を形成することが可能となる．

また，提案方式ではクラスタのマージを行う際，クラスタ内の平均ノード数の小さいクラスタ同士を結合し，PBFT の最小構成数である 4 つのクラスタになるまでマージを実行する．表 1 に，クラスタ内の平均ノード数を n，初期クラスタ数を m としたときのクラスタ内のノード数の変化の例を示す．

表 1　Example of changes of node count in each cluster

マージ回数	クラスタ内のノード数	クラスタ数
0	$n, n, n, n, n, \ldots$	m
1	$2n, n, n, n, \ldots$	$m-1$
2	$2n, 2n, n \ldots$	$m-2$
$\ldots$	$\ldots$	$\ldots$

3.2　Liveness と Safety

PBFT は，全体の n 個のレプリカのうち $\lfloor (n-1)/3 \rfloor$ 個までが同時に障害を起こしても，liveness と safety の両方を保証する．liveness は，リーダノードの障害や悪意のあるノードが存在しても，システムが進行可能であることを保証し，safety は，システムが誤った結果や矛盾した結果を生成しないことを保証する．

同様に，提案方式ではリーダノードがビザンチン障害ノードとなった場合にビュー変更を行うことで liveness を維持することが可能である．また，複数のクラスタが同時にビュー変更を実行する場合，すべてのクラスタでビュー変更が完了していることを検証する必要がある場合がある．この検証が行われない場合，一部のクラスタがビュー変更の完了を待たずにコンセンサスを試みる可能性があり，これにより潜在的な矛盾が生じるリスクがある．そのため，すべてのクラスタがビュー変更を完了し，安定した状態に戻ったことを確認する仕組みを含めることで，ビュー変更が安全に完了した後にのみクラスタ間の合意形成を進めることが可能となる．

3.3　性 能 限 界

提案方式の合意形成確率および通信トラフィック量の上限値を理論解析する．

表 2　Variables

変数名	説明
N	総ノード数
m	クラスタ数
n	クラスタ内のノード数
f	ビザンチンノード数

3.3.1　合意形成確率

合意形成確率の性能限界を分析する．ここでは簡単のためクラスタは等しいノード数で分割される場合を仮定し，表 2 の変数を用いると，総ノード数は，$N = mn$ と表せる．通常の PBFT におけるビザンチンノード数の上限値は，$N = mn = 3f + 1$ より，

$$f = \frac{mn-1}{3} \tag{1}$$

となる．また m 等分割した 2 段階 PBFT におけるビザンチンノード数 f^m の上限値は，

（1）　$m = 3f' + 1$ より，f' 個のクラスタでは，全ノードがビザンチンノードでも可能であるため次式が得られる．

$$f' = \frac{m-1}{3} \tag{2}$$

（2）　残りの $(2f'+1)$ 個のクラスタでは，$n = 3f'' + 1$ より，

$$f'' = \frac{m-1}{3} \tag{3}$$

個のノードがビザンチンノードでも可能である．

そのため (2)(3) 式より次式が得られる．

$$\begin{aligned} f^m &= f' \times n + (2f'+1) \times f'' \\ &= \frac{mn-1}{3} + \frac{2}{9}(m-1)(n-1) \\ &= f + \frac{2}{9}(m-1)(n-1) \end{aligned} \tag{4}$$

すなわち提案方式は従来の PBFT と比較して，$2(m-1)(n-1)/9$ だけビザンチンノードの上限値が増加する．

ここで，$m \approx n$ で増えると考えると，

$$\frac{f^m}{N} = \frac{5}{9} - \frac{4}{9} \times \frac{1}{n} - \frac{1}{9} \times \frac{1}{n^2} \tag{5}$$

であり，$N \to \infty$ のとき，

$$\frac{f^m}{N} \to \frac{5}{9} \tag{6}$$

となる．したがって，(6) 式よりビザンチンノード数が全体の 5/9 を下回る割合で存在する場合は，提案手法を用いることで合意が得られる可能性がある．

3.3.2 通信トラフィック量

通信トラフィック量に対しても [10] を基に通信複雑性を算出する．表 2 の変数を用いると，k-means 法による位置情報共有や，PBFT による合意形成に伴うトラフィック量は，以下のようになる．

$$N \log N + 3(m \log m + n \log n) \tag{7}$$

マージを一度実行するとクラスタ数は $m-1$ となり，各クラスタのノード数は 1 つのクラスタは $2n$ となり，残りの $m-2$ 個のクラスタは n となる．このとき発生するトラフィック量 T は，

$$T = 3\left\{(2n)\log(2n) + (m-1)\log(m-1)\right\} \tag{8}$$

となる．マージ回数が $m/2$ 回のとき，クラスタ数は $m/2$ となり，各クラスタのノード数はすべて $2n$ となる．したがって，

$$T = 3\left\{(2n)\log(2n) + \frac{m}{2}\log\frac{m}{2}\right\} \tag{9}$$

となり，(8)(9) 式より，

$$\begin{aligned} T &= N\log N + 3(m\log m + n\log n) \\ &\quad +3\times\frac{m}{2}\times 2n\log 2n + \sum_{i=\frac{m}{2}}^{m-1} i\log i \\ &= nm\log nm + 3n\log n + 3nm\log 2n + \sum_{i=\frac{m}{2}}^{m-1} i\log i \end{aligned} \tag{10}$$

となる．ここで，(10) 式において，以下となる．

$$\begin{aligned} \sum_{i=\frac{m}{2}}^{m-1} i\log i &\simeq \int_{\frac{m}{2}}^{m} x\log x\,dx \\ &= \left(\frac{m^2}{2}\log m - \frac{m^2}{4}\right) - \left(\frac{m^2}{8}\log\frac{m^2}{2} - \frac{m^2}{16}\right) \\ &= O(m^2\log m) \end{aligned} \tag{11}$$

したがって，(11) 式より，m が増加すると，通信量の上限が $m^2 \log m$ で増加する．

4. 性能評価

提案方式の有効性を計算機シミュレーションにより，合意に達した割合および発生トラフィック量を比較する．合意形成確率では，100 回の試行の中で，合意に達した確率を評価する．

4.1 評価条件

表 3 に計算機シミュレーションの条件をまとめる．提案手法 (Proposed Method (k = 7, 10, 15)) と従来の PBFT (Existing PBFT)，k-means 法を 1 度のみ適用した PBFT (Existing Method (k = 7, 10, 15)) を比較する．また，攻撃者は特定の領域に集中的に配置し，ノード間の位置関係が近いものを同一クラスタに分類できるように k-means 法を適用した．

表 3 Conditions in computer simulation

項目	条件
ノード数	90
ビザンチンノード数	0〜90
クラスタリング手法	k-means 法
クラスタ数	7, 10, 15
ネットワークトポロジ	Barabasi-Albert (BA) Erdos-Renyi (ER) Watts-Strogatz (WS)

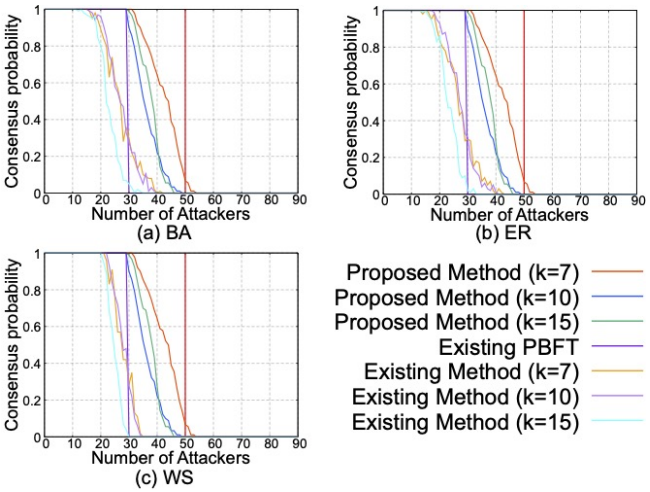

図 7 Consensus probability against number of attackers

4.2 合意形成確率

図 7 に，ネットワークトポロジを BA モデル，ER モデル，WS モデルで各々生成し，攻撃者数を 0 から 90 まで変化させた場合の合意形成確率を示す．いずれのモデルにおいても，提案方式では攻撃者数が全体の 1/3 を超えても合意に達することが可能となり，合意形成確率は従来方式よりも提案方式の方が高いことが確認できる．これは攻撃者が多いクラスタが集約され，正しい結果を得るクラスタの比率が増加するためである．また攻撃者数が最大約 50，つまり全体の 5/9 以上の攻撃者がシステムに存在していても正しく合意を形成することができるため，理論解析にて導出した性能限界値と一致しており，理論値とシミュレーション結果が矛盾しないことがわかる．一方，クラスタ数が小さい ($k = 7$) 時に，この性能限界値を超えている．これは，3.3.1 節では，1 度のみクラスタリングを実行した時の理論値であるのに対し，シミュレーションではクラスタリングとマージを複数回実行したことが起因し，性能限界を超えたと考えられる．

4.3 トラフィック量

図 8 に，発生した通信トラフィック量を攻撃者数に対して示す．提案手法では，クラスタリング後の PBFT によるトラフィックが発生し，また k-means 法を実行するために各ノード間でデータをブロードキャストする必要があるため，従来手法と比較してトラフィック量が増加する．また，攻撃者数が全体の 1/3 を超えると，クラスタリングやマージ，クラスタ内およびクラスタ間での PBFT によるトラフィックが発生するため，トラフィック量は急激に増加する．さらにクラスタ数が多くなるほど，合意に達しなかった場合にマージする回数が増えるため，攻撃者の増加に伴いトラフィック量が増加する．

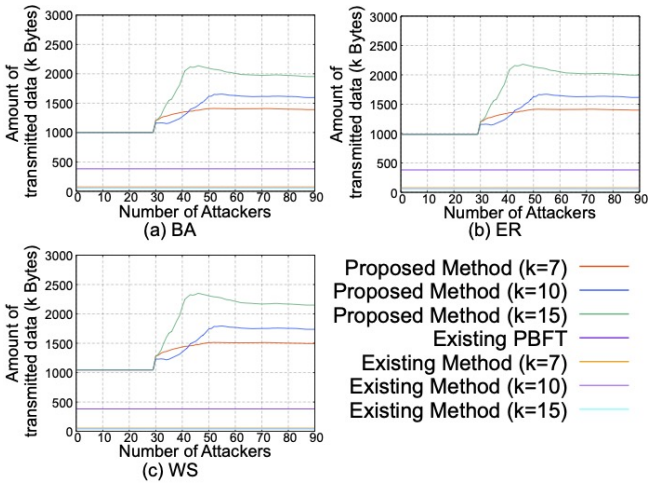

図 8　Amount of traffic against number of attackers

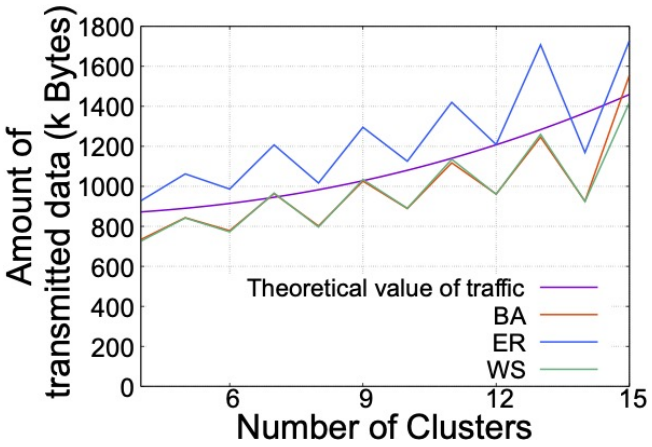

図 9　Amount of traffic against number of clusters

図 9 に，ノード数を 90，攻撃者数は 40 と設定したときの，クラスタ数を変化させたときの BA モデル，ER モデル，WS モデルのトラフィック量，および 3.3.2 節で導出した通信量の理論値 $O(m^2 \log m)$ を示す．なお，シミュレーション値と理論値の傾向を比較するため，理論値に固定値を加算したものをプロットする．また，BA モデルと ER モデルの線が重なって描画されている．さらに，曲線が不規則に変動しているのは，クラスタ数が偶数の場合は，賛成クラスタと反対クラスタが同数になることがあり，コンセンサスに達しないことがあるため，奇数の場合と比べて合意形成確率が下がるためである．

いずれのモデルもクラスタ数の増加に伴い，トラフィック量も増加する．また，理論値に沿ってトラフィック量が増加しており，3.3.2 節で述べた理論値の正当性が確認できる．さらに理論値はオーダ値であるため，理論値とシミュレーション値は傾向として一致していることを確認した．

今後は，シャーディングにおけるコンセンサスメカニズムの適用についても探究する必要がある．

特に，[11] によるビザンチン耐性を持つコンセンサス・ブロックチェーンにおけるブロック時間分布の理論的分析は，本研究において有用な知見を提供する．この知見をシャーディング環境に適用することで，スケールするブロックチェーンにおいても整合性と性能を維持しつつ，より効率的かつ安全なコンセンサスが可能となる．

5. ま と め

本稿では，クラスタリングおよびクラスタのマージを行うことで，PBFT のビザンチン攻撃の耐性を向上させる手法を提案した．提案方式の合意形成割合と通信トラフィック量を計算機シミュレーションにより既存方式と比較し，以下のことを確認した．

- 提案方式を用いることで，攻撃者が全体の 3 分の 1 以上存在していても正しく合意を形成することが可能である．
- 全体の最大 5/9 の攻撃者が存在していても正しく合意に達することが可能となり，この値は，理論解析により導出した合意形成確率の性能限界と一致する．
- トラフィック量は，通信回数やデータ量の増加により，従来方式と比較して大幅に増加した．また攻撃者が増加するほど，他のクラスタとやりとりする回数も増加するため，通信量が増加した．
- クラスタ数の増加に伴い，トラフィック量が増加した．提案方式により発生する通信量の理論上限値を導出し，それに固定値を加算したものとシミュレーション結果を比較すると，同じ傾向で増加することを確認した．

今後は，合意形成確率を維持したまま，トラフィック量を抑える手法を考案する予定である．

謝辞 本研究成果は JSPS 科研費 23K11086，23K21664，23K21665，23K28078 の助成を受けたものである．ここに記して謝意を表す．

文　献

[1] M. Castro, B. Liskov, Practical byzantine fault tolerance, OSDI 1999.
[2] A. Fujihara, Explaining temporal fluctuations of broadcast communications between validator nodes in a proof-of-stake blockchain, Proceedings of Blockchain Kaigi 2023 (BCK23).
[3] R. M. Othmen, et al., Simulation of Optimized Cluster Based PBFT Blockchain Validation Process, IEEE ISCC 2023.
[4] A. J. Al-Musharaf, et al., Improving Blockchain Consensus Mechanism via Network Clusters, BICITS 2021.
[5] Y. Sun, Y. Fun, Improved PBFT Algorithm Based on K-means clustering for Emergency Scenario Swarm Robotic Systems, IEEE Access, vol. 11, pp. 121753-121765, 2023.
[6] G. Wang, et al., SoK: Sharding on Blockchain, 1st ACM Conference on Advances in Financial Technologies (AFT ' 19). Association for Computing Machinery, 2019, pp. 41-61.
[7] B. Choi, et al., Scalable Network-Coded PBFT Consensus Algorithm, 2019 IEEE International Symposium on Information Theory (ISIT), IEEE, 2019, pp. 857-861.
[8] B. L. Y. Quan, et al., Recent Advances in Sharding Techniques for Scalable Blockchain Networks: A Review, IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3523256.
[9] X. Liu, et al., A survey on blockchain sharding, ISA Transactions, vol. 141, pp. 30-43, 2023.
[10] A. Fujihara, Theoretical Analysis on Block Time Distributions in Byzantine Fault-Tolerant Consensus Blockchains, IEEE International Conference on Blockchain 2024.
[11] A. Fujihara, Mathematical Modelling of Dual-Layer Byzantine Fault-Tolerant Consensus Process for Optimal Sharding and Mitigation of Blockchain Trilemma, 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Berlin, Germany, 2024, pp. 1-10, doi: 10.1109/BRAINS63024.2024.10732571.