セキュアプロセッシングにおける処理多重化へ共謀が与える影響に関する数値的調査

稲元 勉[1]　島本 将成[2]　樋上 喜信[1]　小林 真也[1]

概要：本稿は，インターネット上の必ずしも信頼できない計算機を用いて行う分散処理のための処理多重化において，意図的に不正を行う計算機の共謀が処理結果へ与える影響の数値的調査を目的とする．ここで，処理多重化とは，ある同一の処理内容を複数の計算機に分配し，その結果を集約することで計算結果の信頼性向上を企図する手法である．処理多重化により，少数派であることとして，不正な処理結果を正しい処理結果と区別することが可能となる．しかしこの際，不正な処理結果を返す計算機が共謀すると，不正な結果が多数派となり，処理結果の正・不正を誤って判定してしまう恐れがある．本稿では，このような誤りの生じる確率を，いくつかのパラメータ設定のもと数値的に算出・調査する．

Numerical Examination on Collusive Influence over Multiplex Operations in Secure Processing

Tsutomu Inamoto[1]　Masanari Shimamoto[2]　Yoshinobu Higami[1]　Shin-ya Kobayashi[1]

1. はじめに

インターネットで提供されるサービスは増え続け，国内の人口普及率も 79%に達している [1]．インターネットの利便性向上の背景には，科学技術の発展による，安定的に稼働するネットワーク機器の入手性の向上，およびそのような機器を接続した高速なネットワーク構築の容易化があるといえる．それらの資源を活用することで，ネットワーク上に分散している多様な計算機を用いる処理手法であるグリッドコンピューティング [2] に，より高い性能を与えることが可能になると期待される．

グリッドコンピューティングは，信頼できる主体が管理する計算機だけを用いるインターナルグリッドと，そうでない計算機も用いるエクスターナルグリッドに分けられる．一つの企業や研究室といったイントラネット内に計算資源を限定すれば，前者を実現できる．一方，インターネット内の計算資源を使用するグリッドコンピューティングは，エクスターナルグリッドとして実現されることになる．これら使用するネットワークの特徴から，二つの手法は利用可能な計算資源と計算結果の信頼性についてトレードオフ関係をもつことになる．すなわち，インターナルグリッドは，利用可能な計算機数が少ないものの計算機およびネットワークの信頼性が高く計算結果も信頼できる一方，エクスターナルグリッドは，潜在的に利用できる計算機が膨大であるものの，処理内容や処理データの秘匿可能性および計算結果の信頼性が低い．このようなエクスターナルグリッドの欠点を補うために，著者らは，処理内容の秘匿 [3] や不正な結果を返す計算機（以降，不正ノード）の検出 [4] などを目指して “セキュアプロセッシング” と名付けた取り組みを進めている．本稿は，この取り組みの中で，とくに不正な結果の検出 [5] を取り上げたものである．

ある計算機から返された処理結果の正しさを判定する典型的手法として，同じ計算をほかの計算機で処理して得られた結果と比較することが挙げられる．本稿ではこの手法を “多重処理” と呼ぶ．多重処理の有効性は，不正ノードの割合が高い状況下で不正ノード同士が結託した場合，低下すると考えられる．この低下の度合いを調査することは，

[1] 愛媛大学大学院理工学研究科
Graduate School of Science and Engineering, Ehime University, Bunkyo-cho 3, Matsuyama, Ehime, 791–8577, Japan
[2] 愛媛大学工学部
Faculty of Engineering, Ehime University, Bunkyo-cho 3, Matsuyama, Ehime, 791–8577, Japan
（*2013 年 4 月より徳島銀行）

エクスターナルグリッドの有効性向上に資すると考える．

以上の背景のもと，本稿では，不正ノードの割合，不正ノード同士の共謀の有無といったパラメータが，不正な処理結果の得られる割合に与える影響を調査することを目的とする．この割合は，閉じた数式として表すことが困難であるため，擬似乱数に基づく数値計算を用いて算出する．

2. 多重処理と共謀

2.1 多重処理

何らかの計算を複数の計算機で分散処理することを考える．ここで，分散処理を行う計算機を “ノード” と呼ぶ．このとき，分散処理では，ノードから返されてきた計算結果が，正しく機能している計算機を用いた場合とは異なるという意味で不正である恐れがある．この不正は，ノードやネットワークの不調などがその原因である自然発生的なものと，当該ノードにより意図的に作成された人為的なものとに大別できる．自然発生的不正は再現性が低く，同じ処理結果が複数回得られる確率はきわめて低い．このため，同一の処理内容を多数の（三つ以上の）ノードで計算し，処理結果を照合することにより，自然発生的不正を正しい結果として受け入れてしまう確率を低下させることができる．本稿では，そのような処理の仕方を “多重処理”，その際に用いるノード数を “多重度”，ある処理結果を正しいものとして受け入れることを “受理”，不正な結果を受理してしまうことを “誤受理” と呼ぶ．多重度を増すことにより，自然発生的不正の誤受理確率を低く抑えることができる．

本稿では，多重処理を用いた処理結果の受理手法として，つぎの二つを考える．

- 過半数決: 多重処理で得られた結果のうち，同一のものが過半数以上を占めた場合，その結果を受理する．
- 多数決: 多重処理で得られた結果を計数し，ある結果が単独最多数となった場合，その結果を受理する．

なお，どの結果も受理されなかった場合は，票割れと判定し，いかなる結果も受理しない．

先述した二つの受理方法の違いを，図 1 を用いて説明する．この例では，多重度は 13 であり，多重処理により a, b, c という 3 種類の結果が得られ，それらを返したノード数はそれぞれ 5, 4, 4 である．過半数決を用いた場合，ノード数が 7 以上である結果がないため，票割れとなる．一方，多数決を用いた場合には結果 a が受理される．

2.2 共謀

人為的不正の受理確率も，再現性が自然発生的な場合と同様に低ければ，多重度を増すことで抑えることができる．ここで，人為的不正を意図的に返すという意味で不正なノードが知己関係にあると仮定する．それらのノードは，結託して同一の処理結果を返すことができると考えられる．本稿では，そのような結託を “共謀”，直接的あるいは間接的な知己関係を “共謀関係” と呼ぶ．不正ノード数がある程度多く，かつ不正ノードの共謀が頻発しているならば，いくら多重度を増やそうが誤受理確率を低くすることはできないと考えられる．このような定性的推測は容易であるものの，誤受理確率を定量的に見積もることは，著者らの知る限り行われていない．

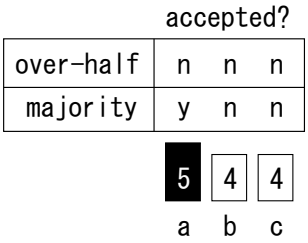


図 1 多重度 13 での多重処理の一例
Fig. 1 A result of a multiplex operation with degree of 13.

3. 誤受理確率の算出

3.1 前提

誤受理確率を算出するにあたり，以下を前提する．

- ノードを区別することはできず，あるノードが結果の正／不正を偽ったことがあるか否かは不明である．
- 多重処理時に使用するノードを指定できない．
- 不正ノード同士は，ノードによらない一定の確率で知己関係にある．
- 知己関係は双方向的である．
- 知己関係にある不正ノードは必ず共謀する．

このような前提から，本稿で考慮するエクスターナルグリッドは，知己関係を隣接行列，共謀関係を可到達行列とするランダムグラフ [6] としてモデル化できる．ただし，このモデルは数値計算の際に用いるのみで，数理的取り扱いは今後の課題である．

3.2 記号の定義

- 多重処理を行うエクスターナルグリッドの性質を規定するパラメータ．
  - N: 分散処理に用いるノード数．
  - M $(\leq N)$: 人為的不正を返す不正ノードの数．
  - p $(0 \leq \cdot \leq 1)$: 不正ノード同士が知己関係にある確率．
  - v (≥ 1): 多重度．
- 知己関係，共謀関係を表す記号．
  - $A \in \mathcal{B}^{M \times M}$: 二つの不正ノードが知己関係にあるか否かを表す隣接行列．ただし，$\mathcal{B} := \{0, 1\}$．便宜的に，各不正ノードは自分自身とも知己関係にあるとする．
  - $C \in \mathcal{B}^{M \times M}$: 二つの不正ノードが共謀関係にあるか否かを表す可到達行列．A に基づいて算出される．

3.3 共謀関係の算出

擬似乱数を用いた知己関係の設定は，つぎの手続きにより行う．

(1) A を $M \times M$ の零行列とする．
(2) A の上三角行列要素を，確率 p で 1 とする．
(3) A が対称行列となるように，A の下三角行列要素を設定する．
(4) A の対角要素を 1 とする．

知己関係 A が所与のとき，バイナリ法を組み合わせた ISM 法 [7] を用いるつぎの手続きにより，共謀関係を算出する．

(1) $B \leftarrow A$, $C' \leftarrow A$ とする．
(2) $B' \leftarrow B \cdot B^{\top}$ とする．ここで，$\top$ は行列の転置を表す．
(3) $B'' \leftarrow f^{\mathrm{b}}(B')$ とする．ここで，$f^{\mathrm{b}}(\cdot)$ は，$M \times M$ 行列の各要素を，それが 0 より大きければ 1 とすることで $\mathcal{B}$ へ落とし込む関数を表す．
(4) $C' = B''$ なら，$C \leftarrow B''$ として手続きを終了する．そうでなければ，$C' \leftarrow B''$, $B \leftarrow B''$ として手順 (2) を実行する．

誤受理が生じるか否かは，つぎの手続きにより算出する．

(1) N ノードから v ノードをサンプルし，それらの中に含まれている不正ノードを選択する．
(2) 共謀関係を表す可到達行列のうち，不正ノードに対応する行および列を抽出する．
(3) この抽出された行列の行ごとに列にわたって総和をとり，その行にわたる最大値が，
- 過半数決の場合: 多重度の半分より大きければ不正な結果の受理とする．v 個のノードの中で不正でないノード数が過半数（$v/2+1$ 以上）を占めていれば正しい結果の受理とする．そうでなければ票割れとする．
- 多数決の場合: 不正でないノード数より小さければ正しい結果の受理，大きければ不正な結果の受理とする．どちらでもなければ票割れとする．

4. 計算結果

4.1 過半数決の場合

誤受理確率は，あるパラメータ設定のもとでの 1,000 回の試行において誤受理が生じた割合として算出した．多重処理の具体的手法として過半数決を用いた場合の誤受理確率を表 1 に示す．なお，票割れとなった場合は，その試行の結果をたんに廃棄する．よって，1,000 回連続して票割れとなった場合，どのような結果も受理されない．

本稿では，不正ノード同士が知己関係である確率が 2%の場合を，そのような確率が十分大きいケースとして想定する．表 1 におけるパラメータ設定 2, 4, 6 の結果から，不正ノードの割合が 10%ほどならば，不正ノード同士が知己関係である確率が高くても，誤受理確率は低い．ただし，

表 1　過半数決を用いた場合の誤受理確率
Table 1　Prob. on accepting false results by using the over-half scheme.

#	N	M	p	v	False accept. rate
1	100	10	0.001	5	0
2	100	10	0.02	5	0
3	1000	100	0.001	5	0
4	1000	100	0.02	5	0.006012
5	1000	100	0.001	101	0
6	1000	100	0.02	101	0
7	1000	500	0.001	5	0
8	1000	500	0.01	5	0.51259
9	1000	500	0.001	101	0
10	1000	500	0.01	101	0.49635
11	1000	500	0.001	201	0
12	1000	500	0.01	201	0.45992
13	1000	600	0.001	201	-
14	1000	600	0.005	201	1
15	1000	600	0.01	201	0.999

パラメータ設定 7–12 の結果から，不正ノードの割合が高くなると，知己関係である確率が誤受理確率へ強い影響を与えるようである．また，パラメータ設定 8, 10, 12 の結果を比較することにより，多重度を増すことで誤受理確率が低減されることを確認できる．しかし，パラメータ設定 14 の結果から，多重度をいくら増しても，不正ノードの割合が過半数を超えると誤受理確率は 100% に近づくことが確認される．なお，パラメータ設定 13 の結果における “–” は，すべての試行が票割れとなったことを表す．

4.2 多数決の場合

表 1 と同様の数値を，多重処理の具体的手法として多数決を用いた場合について集計した結果を表 2 に示す．

表 2 から，多数決処理を用いた場合に，不正ノードの割合・知己確率・多重度が誤受理確率へ及ぼす影響は，表 1 に示した多数決処理を用いる場合と同様の傾向を有することを確認できる．また，たとえばパラメータ設定 2 と 17 の結果を比較することで，多数決処理は過半数決処理よりも誤受理確率について基本的には劣っているといえる．しかし，パラメータ設定 13 と 28 の結果の比較から，不正ノードが過半数を占めておりかつ知己確率が低い場合には，多数決処理のほうが過半数決よりも優れている可能性を見て取れる．

4.3 誤受理確率が大幅に増加する状況について

表 1, 2 のどちらでも，ノード数が 1,000 かつ不正ノード数が 600 の場合，知己確率が 0.001 から 0.005 に変化すると，誤受理確率は 1 に肉薄している．この詳細を調べるために，多重処理として過半数決を用い，ノード数を 1,000，不正ノード数を 600 と固定して，知己確率を 0.001

表 2　多数決を用いた場合の誤受理確率

Table 2　Prob. on accepting false results by using the majority scheme.

#	N	M	p	v	False accept. rate
16	100	10	0.001	5	0
17	100	10	0.02	5	0.001
18	1000	100	0.001	5	0
19	1000	100	0.02	5	0.0020101
20	1000	100	0.001	101	0
21	1000	100	0.02	101	0
22	1000	500	0.001	5	0.047506
23	1000	500	0.01	5	0.4995
24	1000	500	0.001	101	0
25	1000	500	0.01	101	0.49796
26	1000	500	0.001	201	0
27	1000	500	0.01	201	0.47857
28	1000	600	0.001	201	0
29	1000	600	0.005	201	0.99399
30	1000	600	0.01	201	0.999

表 3　過半数決を用いた場合の知己確率 0.001 〜 0.005 での誤受理確率

Table 3　Prob. on accepting false results over acquaintance probability by using the over-half method.

p	v			# of invalid votes with $v = 201$
	5	101	201	
0.001	0	0	0	999
0.002	0.11957	0	-	1,000
0.003	0.57562	0.89655	1	952
0.004	0.62	0.98151	1	215
0.005	0.64599	0.97084	0.99897	26

表 4　多数決を用いた場合の知己確率 0.001 〜 0.005 での誤受理確率

Table 4　Prob. on accepting false results over acquaintance probability by using the majority method.

p	v			# of invalid votes with $v = 201$
	5	101	201	
0.001	0.10349	0	0	0
0.002	0.2339	0.009009	0.001	0
0.003	0.54644	0.67782	0.73587	27
0.004	0.6103	0.92981	0.9739	4
0.005	0.66243	0.97686	0.99499	1

から 0.005 まで 0.001 刻みで変化させた場合の誤受理確率を表 3 に示す．この表の最右列は多重度 201 で票割れの生じた回数を示す．また，多数決を用いた場合の同様の数値を表 4 に示す．

表 3, 4 より，知己確率 0.002, 0.003 のあいだを境として，多重度の上昇が誤受理確率を低下，上昇させていることが確認される．ただし，多重度が 201，知己確率が 0.002 の場合には，過半数決では 1,000 回の試行がすべて票割れとなり，多数決では誤受理確率が 0.001 となっている．この結果から，ある不正ノードと知己である不正ノード数が 1.2 から 1.8 になる辺りで不正ノード群がパーコレーション [8] を起こしていることが示唆される．また，過半数決と多数決を比較したとき，後者は誤受理確率について前者よりも劣っているが，票割れが少ないためにパーコレーションが生じる閾値近傍では計算量について優れているといえそうである．

5. おわりに

本稿では，信頼できない主体が管理する計算機を用いたグリッドコンピューティングであるエクスターナルグリッドを対象とし，意図的に不正な結果を返す計算機同士の共謀が不正な結果の受理確率へ与える影響について調査した．擬似乱数系列を用いた計算の結果，不正ノード数が全体の 10%ほどであったり不正ノード同士が知己関係にある確率が低いと，不正な結果を受理する確率は低くなること，およびその確率は多重度を増すことで低減できることを確認した．また，系の規模が大きい場合の結果から，不正ノードと知己関係にある不正ノード数が 1.2 から 1.8 になる近傍で，不正ノードのほとんどが共謀関係を有するというパーコレーションの生じる可能性が示唆された．以上より，不正ノード数の割合が半数を超え，かつ共謀によりパーコレーションが生じた場合には，いくら多重度を高くした多重処理を行っても，ほぼ 100%の確率で不正な結果を受理してしまうと考えられる．

今後の課題として，より現実的な問題設定を考慮することや，ランダムグラフモデルを用いて不正な結果を受理する確率を定式化すること，不正ノードの検出手法を考案・併用することなどが挙げられる．

参考文献

[1] 総務省：平成 24 年度情報通信白書 (2012).
[2] 溝口文雄：グリッドコンピューティング—情報処理の新しい基盤技術，岩波書店 (2005).
[3] Himeda, K., Hirata, K., Higami, Y. and Kobayashi, S.: Consideration of Characteristics of Programs for Concealing Purpose of Processing in Distributed Computing Systems, *Polish Journal of Environmental Studies*, Vol. 17, No. 4C, pp. 226–229 (2008).
[4] Miyaoka, H., Hirata, K., Higami, Y. and Kobayashi, S.: The Detection of Falsification with Check Codes in External Grid, *Polish Journal of Enviromental Studies*, Vol. 17, No. 4C, pp. 294–298 (2008).
[5] 島本将成：セキュアプロセッシングの多数決処理における共謀関係に関する研究．愛媛大学卒業論文 (2013).
[6] リック・デュレット：ランダム グラフダイナミクス—確率論からみた複雑ネットワーク，産業図書 (2011).
[7] 井上雅裕，陳　新開，長谷川浩志：システム工学—問題発見・解決の方法—，オーム社 (2011).
[8] 矢久保考介：複雑ネットワークとその構造，共立出版 (2013).