様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１４　日現在

機関番号：　１６３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１０５

研究課題名（和文）セキュアプロセッシング可能な開放型GRIDにおける信頼性確保と処理性能の両立

研究課題名（英文）Realization of compatibility between reliability securing and processing performance in external GRID computing system capable of secure processing

研究代表者

小林　真也（KOBAYASHI, SHINYA）

愛媛大学・理工学研究科（工学系）・教授

研究者番号：１０２３４８２４

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：同一の処理を複数の計算機に実行させる「処理の多重化」において，多重度と共謀に対する耐性の関係を定量的に評価・検討した．多重度を上げることは，望ましい結果をもたらす一方で，悪意のある計算機が複数で共謀謀議をする可能性を高める．このトレードオフ関係を定量的に明らかにした．「処理の多重化」と組み合わせることで，処理時間性能の改善を実現できる「先行処理」において，暫定結果の誤りは，改善を抑制することにつながる．これに対して，先行処理開始となる結果数の閾値設定と異なる結果の出現毎に先行処理を行う方法がある．処理時間の改善効果への影響と処理の隠蔽への阻害的影響について定量的に検討・評価した．

研究成果の概要（英文）：I quantitatively evaluated and examined the relationship between multiplicity and tolerance against collusion in "Duplicate Execution" that allows multiple computers to execute the same process. Increasing the multiplicity increases the likelihood that a malicious computer will conspire to conspire with multiple, while attaining the desired result. We quantitatively clarified this trade - off relationship. In combination with "multiplexing of processing", in the "advance processing" which can realize improvement in processing time performance, an error in the provisional result leads to suppression of improvement. On the other hand, there is a method of performing a preceding process for every appearance of a result different from the threshold setting of the number of results that is the start of the preceding process. I quantitatively examined and evaluated the influence on processing time improvement effect and the inhibitory effect on processing hiding.

研究分野：　情報工学

キーワード：　分散処理　グリッドコンピューティング　セキュリティ

１．研究開始当初の背景

グリッドコンピューティングは，ネットワークに接続されたコンピュータの処理能力を集積することで，インストラクションレベルでのスループット性能の点で，高い性能を獲ることができる．

特に，インターネット上で実現されている開放型グリッド（エクスターナルグリッド）は，インターネット上のコンピュータのアイドル時間を利用するもので，世界中に存在する無限と見なすことができるほどの数のコンピュータを利用することができること，また，インターネット空間は世界規模で広がっており時差があるため，常に，低負荷であるコンピュータが存在することから，高いスループット性能をえる方法として注目されている．しかしながら，エクスターナルグリッドの課題は，コンピュータの持ち主に悪意を持った者が紛れ込むことにある．つまり，悪意のある人物が，自らの所有するコンピュータに依頼された処理の内容を盗み取ったり，故意に正しくない結果を返すなど，不正な行為を行う危険性がある．そのため，これまで，エクスターナルグリッドは，営利目的や，機密性が必要とされる処理に用いる事ができない．

これらの課題を定量的な保証を持って，対処できる技術を実現する事ができれば，これまで，非営利目的でしか用いられなかった，エクスターナルグリッドの利用範囲が爆発的に増え，多大な計算リソースを要求する科学技術領域や産業領域に多大な貢献が期待できる．

２．研究の目的

インターネット上のコンピュータの処理能力を利用することで，インストラクションレベルでの高いスループット性能を実現するエクスターナルグリッドのもつ課題である，ノードコンピュータによる不正な解析と，故意に正しくない結果を返す不正実行に対して，数理的な裏付けを伴う定量的な保証を与える技術の確立を目指している．

不正解析や不正実行に対する対策は，エクスターナルグリッドの性能を損なうという負の効果も伴っている．従って，正の効果と，負の効果のバランスを，より望ましい状態でとることが求められている．

この取り組みでは，依頼先において正しく処理が行われる事を保証する「処理の多重化」と，複数の処理結果の照合を経ずに，暫定的な結果を用いて，後続する処理の開始を始める「先行処理手法」を組み合わせることで，不正解析や不正実行に対する対策と，高い処理性能の両立の実現を目指す．

この取り組みの成果は，エクスターナルグリッドの商用利用や機密性が求められる利用を可能とし，安価な高性能計算環境として，エクスターナルグリッドの新たな利用分野を切り開く突破口となる．

３．研究の方法

エクスターナルグリッドにおける「処理の委託に対する信頼性を確保」する方法として，同一の処理を複数の計算機に実行させる「処理の多重化」がある．処理の多重化では，同一の処理を行う計算機の結果で多数決を行い，多数を獲得した結果を正しい結果と見なして，次の処理を行う．処理の多重化は，任意の計算機が正しい結果を返す確率が，0.5 を上回るという条件下では，同一処理を行う計算機数（多重度）が増えるほど，正しい結果を得られる確率が増す．一方で，多重度の増加は，処理に関わる計算機数の増加であり，このことは，より多くの計算機に処理内容を開示する事を意味する．処理に関わる計算機の増加は，その中に悪意のある人物が所有する計算機が混入する確率を増やすことになり，処理の不正な解析に対する脆弱性を高めてしまう．特に，悪意のある人物が，複数の計算機を所有したり，あるいは，悪意のある人物同士が情報を交換するという共謀を行った場合，より多くの情報を彼らが入手する危険性がある．

そこで，本研究取り組みでは，多重度と共謀に対する耐性の関係を定量的に評価・検討する．多重度を上げることは，不正な結果の混入という点については，望ましい結果をもたらす一方で，悪意のある計算機が複数で共謀謀議をする可能性を高める．このトレードオフ関係を数学的手法を中心に定量的に明らかにする．

また，「処理の多重化」と組み合わせることで，処理時間性能の改善を実現できる「先行処理」における，改善を抑制することにつながる，暫定結果の誤りに対する対策法である，先行処理開始となる結果数の閾値設定と異なる結果の出現毎に先行処理を行う方法について，処理時間の改善効果への影響と処理の隠蔽への阻害的影響について定量的に検討・評価する．

４．研究成果

・「処理の多重化」における多重度と共謀に対する耐性の関係の検討

プログラム分割と処理多重化は，エクスターナルグリッドにおける不正解析や改竄の対策である．プログラム分割では，エクスターナルグリッドに投入されたプログラムを複数断片に分割し，各プログラム断片を異なる計算機に処理の依頼をする．このようにすると，各計算機が得ることができるプログラムが全体の一部に限定されるとなり，結果として悪人が得ることができる部分がプログラム全体の一部に限定すことができ，不正な解析の対策として有効である．

一方，処理の多重化は，複数のノードに同一の処理を依頼し，得られた複数の処理

結果から多数決によって，信頼性の高い結果を採用することができ，不正な実行に対する改善対策となる．

しかし，処理の多重化は，複数のノードに断片を配布するため，同一の処理を行うノード数の増加は，その中に，悪人が入り込む確率を増やすことになる．従って，悪人がプログラムを得る可能性が増し，不正解析の危険性が増す．

解析には，依存関係を把握する必要があり，悪人が得る断片の連続している量が少ないほど，依存関係の把握が困難になり，不正解析も困難となる．

平成 26 年度は，悪人が得ることができるプログラム連続部の最大長に対する確率と，任意の分割数と多重度の時に悪人グループが得ることができるプログラムが連続している量の期待値で示した．この確率と期待値は，最適な分割数を見つける際の定量的な指標として用いることができる．

平成 27 年度は，先行処理において，最初に返された結果に基づいて先行処理を行う方式と処理結果の違いに応じて網羅的に先行処理を行う方式に対して，最大連続長がどのように変化するかを定量的に示した．先行処理は，処理の多重化において，最も早く返された結果に基づいて，次の処理を行う方式である．最も早く返された結果は，結果が返信された時点では，必ずしも正しい結果とは限らない．しかし，不正実行を行うノードの存在確率が 0.5 未満であれば，最初に返された結果を暫定的に正しいと見なして次の処理を開始しても，いずれその結果型正しかったと判定される可能性が高い．従って，暫定結果に基づいて処理を始めることは，高速なノードを有効に活用し，プログラム全体の完了時間の短縮をもたらすことができる．

さらに，平成 28 年度には，信頼できるコンピュータで実行する割合と，悪意のある計算機集団の共謀謀議に対する耐性との関係を定量的に評価した．これにより，エクスターナルグリッド利用の際の，安全性，コスト，利用可能範囲を判断する定量的な指標を示すことが出来た．

・「先行処理」における暫定結果決定条件と利用計算機数の検討

プログラム分割と多重化を用いた依頼処理の高速化を目的とした先行処理手法では，ロールバックによって処理高速化の効果が減少する問題があった．

平成 26 年度には，これを解決・改善するために，暫定処理開始に条件を設ける手法と，新出の処理結果が返される度に新しく処理するノードを確保し，同時並行して残影処理を進める暫定処理を網羅する手法を提案した．

暫定処理の開始に条件を設ける方式では，同一の処理結果が一定数以上あつまらないと，先行処理を行わない．このようにすることで，先行処理開始時の暫定処理結果が真正である確率が高まることとなる．

一方，網羅的に実行する方式では，新たな処理結果が送られる度に，その結果に基づき，先行処理を開始する．このようにすることで，先行処理に関わるノード数は増えるものの，全ての可能性を網羅しているため，かならず，正しい結果に基づく処理が行われていることになり，正しいことが保証される状態まで後戻りするロールバックが発生しない．従って，最も短い時間で，正しい結果を返した計算機の性能を活かすことができ，グリッドの高速性を最大限に引き出すことができる．

既存手法である多重化及び先行処理手法と，これら提案手法の効果の比較，考察を行った．先行処理の開始に条件をつける手法では，真正処理率の増加に伴い高速化の効果が低下してしまうが，ロールバックによって新たに確保する処理ノード数を押さえることが可能であることを示せた．また，不正解析への対策となる．暫定処理を網羅する手法は，高速化の効果は高いが，管理ノードに対する負荷の増加や解析のリスクがあることを示した．

平成 27 年度は，暫定処理結果を決定する際の閾値の違いが，高速性，信頼性，機密性に対してもたらす影響を評価し，それらの関係性を定量的に示した．この結果は，利用者の要求に応じた，高速性，信頼性，機密性のバランスを達成する際の定量的指標となる．

平成 28 年度には，悪意や故障により正しくない結果を返す計算機の存在確率や悪意を持つ計算機が共謀謀議を行う確率と，先行処理の効果，ならびに処理の隠蔽への影響との定量的関係を明らかにした．

異なる結果が送られる度に，同一処理を行う計算機を増やす網羅的な先行処理は，処理時間の増加をもたらさないものの，正しくない結果を返す計算機の増加に伴い，同一処理を行う計算機数の増加につながり，結果として，共謀謀議が行われやすくなることを示した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

1. K. Yamaguchi, T. Inamoto, K. Endo, Y. Higami, and S. Kobayashi: “Evaluation of Influence Exerted by a Malicious Group’s Various Aims in the External Grid,” Proceedings of The 20th International Multi-Conference on Advanced Computer Systems (ACS 2016) ,査読有り，(2016.10)

〔学会発表〕（計 9 件）

1. 山口 晃右, 藤橋 卓也, 遠藤 慶一, 小林 真也, エクスターナルグリッドにおける網羅法の処理ノード数増加に対する抑制手法の提案, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2017)（2017.6.28, 北海道札幌市）
2. 山口晃右, 遠藤慶一, 樋上喜信, 小林真也, エクスターナルグリッドの処理結果を誤りに導くことを意図する悪人がもたらす影響の定量的評価, 第 79 回情報処理学会全国大会（2017.3.18, 愛知県名古屋市）
3. 田中祐生, 遠藤慶一, 樋上喜信, 小林真也, 閾値暫定法を用いたエクスターナルグリッドにおける高速性・機密性・信頼性のトレードオフ関係の定量的考察, 第 79 回情報処理学会全国大会 2017.3.18, 愛知県名古屋市）
4. 山口 晃右, 稲元 勉, 樋上 喜信, 小林 真也: “悪人集団の盗視に対抗する保護処理を用いたエクスターナルグリッドの性能評価”, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2016), pp.344-351 (2016.7.6, 三重県鳥羽市)
5. 田中 祐生, 井上 竜太郎, 稲元 勉, 遠藤 慶一, 樋上 喜信, 小林 真也: “暫定閾値に基づく先行処理を用いたエクスターナルグリッドにおける閾値と処理時間の関係”, 平成 28 年度 電気関係学会四国支部連合大会 (2016.9.17, 徳島県徳島市)
6. 廣瀬 吉隆, 稲元 勉, 樋上 喜信, 小林 真也: “セキュアプロセッシングにおける先行処理による処理時間改善に対する定量的評価”, 第 14 回情報科学技術フォーラム (FIT2015), Vol. 4, pp.241-242 (2015.9.17, 愛媛県松山市)
7. 山口晃右, 稲元 勉, 樋上喜信, 小林真也: “エクスターナルグリッドに対する依存関係を利用した不正解析のリスクを軽減する手法”, 第 78 回情報処理学会全国大会 (2016.3.11, 神奈川県横浜市)
8. 中矢 匠, 稲元 勉, 樋上 喜信, 小林 真也: “プログラム断片の連続性に基づくセキュアプロセッシングの秘匿性能に関する調査”, マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2015), pp. 287-294 (2015.7.8, 岩手県八幡平市)
9. 平田 智紀, 稲元 勉, 樋上 喜信, 小林 真也: “セキュアプロセッシングにおけるファイル分散配置による通信負荷改善の効果に関する研究”, マルチメディア, 分散, 協調とモバイル (DICOMO2014) シンポジウム, pp. 1806-1817 (2014.7.11, 新潟県新発田市)

〔図書〕（計 1 件）

1. K. Yamaguchi, T. Inamoto, K. Endo, Y. Higami, and S. Kobayashi: “Evaluation of Influence Exerted by a Malicious Group’s Various Aims in the External Grid,” Chap.10, pp.112-122, Hard and Soft Computing for Artificial Intelligence, Multimedia and Security, Springer (2017)

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
ホームページ等
なし

６．研究組織
(1)研究代表者
小林　真也（KOBAYASHI, Shinya）
愛媛大学・大学院理工学研究科・教授
研究者番号：10234824

(2)研究分担者
稲元　勉（INAMOTO, Tsutomu）
愛媛大学・大学院理工学研究科・助教
研究者番号：10379513