様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月　７日現在

機関番号：16301
研究種目：基盤研究（C）
研究期間：2010～2012
課題番号：22500060
研究課題名（和文）　セキュアプロセッシングが可能なオープングリッドコンピューティングの実現
研究課題名（英文）　How to make open GRID computing reliable

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

研究成果の概要（和文）：
インターネット上のコンピュータによって構成されるエクスターナルグリッドにおける，処理内容の漏洩や誤った処理結果を返送する危険性に対する，技術的な解決方法の開発が目的である．
処理の内容の漏洩を防ぐ方法の一つあるダミーコードの挿入方法の一つを実装し，その後，それを解読する方法について検討を行った．その結果，ダミーコード挿入方法の改良の手がかりを得ることが出来た．
次いで，真正処理を実現する方法として，複数のコンピュータで同一処理を行い，その結果の多数決を行う多重処理について定量的評価を行い，有効性を示した．さらに，多数決の確定前に，最も早く結果を返すコンピュータの結果により，次の処理を始める先行処理により，高い処理性能も実現できることを示した．

研究成果の概要（英文）：
External GRID is a collection of many computers that belong to different owner respectively, we are afraid that computer’s owner is a bad guy, and he steals secret of program and return incorrect result.
Our research’s aim is to develop new technology that achieves concealing the purpose of Program, and guaranteeing exact processing.
Dummy code insertion is one of techniques against malicious analysis. There are various sorts of dummy code insertion procedures. We have implemented one sort of dummy code insertion, moreover inspected it from analyzer’s viewpoint. We got a key to improve dummy code insertion.
The second outcome is experimental result showing that multiple executions is effective for not only high reliability of execution results but also high performance. Multiple execution requires several computers to process same task. After getting the results, true result can be decided by majority. We showed that higher multiplicity achieves higher reliability. Moreover, we introduced advanced processing technique to multiple executions. Under multiple executions, each computer finished its task at different time. Majority vote may be decided when over-half of computers have finished. If there are few malicious computer, we can usually win a bet that is the first result is correct. This means that we can start the next step after getting the first result. This technique is named advance processing. We indicated advanced processing achieves high performance.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,100,000	330,000	1,430,000
2011 年度	1,100,000	330,000	1,430,000
2012 年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：サービス構築，情報システム，GRID Computing，分散処理，セキュリティ

１．研究開始当初の背景

GIRD コンピューティングの中でも，インターネットに接続されたコンピュータを利用するエクスターナル GRID は，利用可能なコンピュータが無尽蔵とも言えるほど，数多く存在するため，会社や研究機関内のコンピュータの利用に限定されるインターナル GRID に比べ，高いスループットを得られることが期待される．しかし，各コンピュータの所有者が不特定多数に渡るために，処理内容の漏洩や処理実行の確実性の確保の課題がある．このことが，エクスターナル GRID の利用が非営利目的の利用に限定される原因となっている．

エクスターナル GRID の商用目的での利用の実現には，処理内容の隠蔽と真正実行の保証を実現する技術の開発が求められる．我々は，この実現を行う方法として，セキュアプロセッシング技術を提唱し，研究開発を行ってきた．処理内容の隠蔽を達成する手法として，プログラム分割断片化，断片の再構成，ダミーコードの挿入，ダミー断片挿入などの手法の提案を行っている．また，真正実行の保証には，チェックコードの挿入，多重処理といった手法の提案を行っている．

２．研究の目的

背景で述べたように，エクスターナル GRID の商用目的での利用の実現の為に，セキュアプロセッシングを提唱し，いくつかの技法の提案を行っているが，その効果についての定量的な評価や実装が不十分であった．

そこで，これらの技法の効果について，定量的評価を行い，セキュアプロセッシング技術の実用化への道筋をつけることを目的とする．

３．研究の方法

①処理の隠蔽方法の研究，開発においては，処理を隠蔽する側（隠蔽者）の立場と隠された内容を暴く側の立場（解析者）の双方からの検証が必要となる．そこで，まず，処理隠蔽の技法の一つとされているダミーコードの挿入の具体的な方法を実装する．次いで，解析者の立場から，コード間の依存関係に注目し，各コードの特徴から，ダミーコード特有の特徴が無いかを調べる．もし，ダミーコードが他のコードと異なる特徴を持たなければ，実装したダミーコードの挿入方法は，処理内容の隠蔽を高い次元で達成できていることになる．一方，特徴的な違いを持っていれば，実装した挿入方法が不十分なものであったことになるが，今後，新たな挿入方法を検討する際の知見として大いに参考となる．

②真正実行の保証には，予め結果の分かっているチェックコードの挿入と，同一の処理を複数のコンピュータにさせる多重処理の２つの技法がある．このうち，多重処理手法を対象に，悪意のあるコンピュータノードが共謀して，同一の誤った結果を回答する場合に対して，ノード中の悪意あるノードの割合，また，悪意あるノードそれぞれの知己ノード数をパラメータとし，誤った結果がもたらされる確率を求め，定量的な検証を行う．

③多重処理手法において，同一処理を行うコンピュータノードの終了を待たずに，最初に送られてきた結果を基に，次の処理を開始すれば，処理性能にバラツキのあるエクスターナル GRID において，処理性能の高いノードの性能を有効に活用し，より早く処理ができる．これを先行処理と名付けた．先行処理を行った場合，最初に送られてきた結果が正しいとの保証はないため，多数決の結果，正しくない事が判明した場合には，再処理を行う事になるが，それとて，先行処理を行わない場合に比べ，処理時間が長くなくことは無い．先行処理を行った場合と行わなかった倍を比較し、先行処理の効果を定量的に検証する．

④これまでの成果を実プログラムに適用す

ることを目指し，実プログラムを対象とした隠蔽方法の適用を自動的に行うプログラムの実装に取り組む．

４．研究成果

①処理内容の隠蔽方法の一つに，異なるプログラムに由来する複数のプログラム断片を互いに連結するダミーコードの挿入がある．ダミーコードは，本来存在しなかったコード間の依存関係をもたらし，解析者に対して，異なるプログラムに由来する複数のプログラム断片があたかも，一つのプログラムから得られた断片であるかのように誤解させる効果がある．

本事業においては，ダミーコードの具体的な挿入方法として，ダミーコード毎に，依存するコード数を乱数で決定し，さらに，依存するコードをランダムに選ぶ方法を対象に，解析者の立場から，コードの特性について調査・考察を行った．

その結果，依存関係グラフにおいて後続のコードを持たない最終コード（グラフにおける終了ノード）のうち，そのコードをダミーコードと仮定した場合に，ダミーコードと演繹できる他のコードが存在するコード（このようなコードを単独コードと呼ぶ）のほとんどがダミーコードであることが分かった．つまり，単独コードでない，最終コードを，ダミーコードと判断することは，その誤り率が低い．このことは，解析側にとっては大いに成果を上げたと言えるが，隠蔽側に取っては，不十分であることを意味する．これにより，今後，ダミーコード挿入技法の改良の方向性が明確になった．

表１ ダミーコード 30%挿入時の
最終コードの内訳

	単独コードでない最終コード	単独コードである最終コード
ダミーコード	0	55
ダミーコード以外	11	45

②ノード中の悪意あるノードの割合，また，悪意あるノードそれぞれの知己ノード数をパラメータとし，誤った結果がもたらされる確率を求めた

図１は，参加ノード数 1000，そのうち，誤った結果を返すノード（悪人）間で繋がりのある確率を 30%とした場合に，悪人の数に対する誤った結果を導いてしまう確率（誤りを返す確率）である．

図より，多重度が大きいほど，誤った結果を導く確率が低くなることが分かる．ただし，悪人の数が，全体の半数になると，その差は無くなることが分かる．

図２は，悪人数 300 の時に，多重度を変化させた場合の，誤りを変化する確率への栄養である．図より分かるように，多重度の増加に伴い，誤りを返す確率が減少することが分かる．この次に示す．多重度の増加に伴う，処理時間の改善とあわせ，エクスターナル GRID において，多重度を増やすことが，有効であることが分かる．

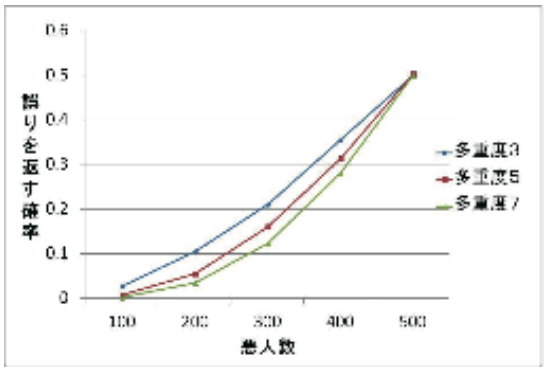

図１　悪人数 対 誤りを返す確率

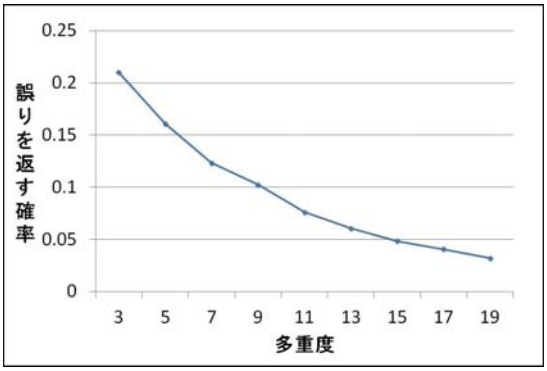

図２ 多重度 対 誤りを返す確率

③先行処理では，最初に送られてきた結果が正しいとの保証はないため，多数決の結果，正しくない事が判明した場合には，再処理を行う事になるが，それとて，先行処理を行わない場合に比べ，処理時間が長くなくことは無い．そこで，先行処理を導入された場合にどの程度の改善が見込まれるかをシミュレーションにより評価した．

表２は，多重度を変化させた場合の，従来方法と先行処理を用いた場合の処理時間，ならびに，従来方法に対する先行処理を用いた場合の改善度である．

先行処理を用いることにより，25%から，40%程度の処理時間の改善が行える事がわかる．

表 2 多重度 対 改善度

	多重度	閾値	処理時間	改善度
従来法	3	2	11.859	-
	5	3	11.156	-
	7	4	10.836	-
	9	5	10.675	-
提案法	3	2	8.804	25.76%
	5	3	7.497	32.79%
	7	4	6.936	35.99%
	9	5	6.632	37.87%

④実プログラムへの適用については，ループ回数が実行時に決定するような，事前に決定不可能な処理の取扱が課題として残っている．今後の課題として，引き続き取り組んでいく事を計画している．

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２件）

① Jun Kawano, Hiroshi Kai, Yoshinobu Higami, Shinya Kobyashi, Dummy code insertion and its efforts on concealment for Secure processing, Proceeding of 18th International Multi-Conference on Advanced Computer Systems, 査読有り, CD 出版, 2012
② Akihiko Funo、Koji Hirata, Yoshinobu Higami, Shinya Kobyashi, Optimistic Processing Protocol for Multiplexing in External PC Grids, Proceeding of 17th International Multi-Conference on Advanced Computer Systems, 査読有, CD 出版, 2010

〔学会発表〕（計３件）

① 稲元 勉, 島本 将成, 樋上 喜信, 小林 真也, 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, 分散、協調とモバイルシンポジウム, 2013 年 7 月 10 日
② 川野 純, 布野 晶彦, 甲斐 博, 樋上 喜信, 小林 真也,セキュアプロセッシングにおける ダミーコードと隠蔽効果の関係,情報処理学会マルチメディア、分散、協調とモバイルシンポジウム, 2012 年 7 月 4 日
③ 布野 晶彦, 平田 孝志, 樋上 喜信, 小林 真也, 多重化を用いた PC グリッドにおける先行処理手法, 電気関係学会四国支部連合大会, 2010 年 9 月 25 日

〔図書〕（計１件）

① Jun Kawano, Hiroshi Kai, Yoshinobu Higami, Shinya Kobyashi , SIGMA-NOT（Poland）出版, PRZEGLAD ELEKTROTECHNICZNY (Electrical Review), ISSN 0033-2097, R. 88 NR 10a/2012

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
平田　孝志（HIRATA KOUJI）
東京理科大学・工学部・助教
研究者番号：10510472

(3)連携研究者
なし