6S-05

エクスターナルグリッドにおける信頼できる計算機による処理間依存関係の隠蔽効果の最大化

砂田 俊平 *　　遠藤 慶一 †　　樋上 喜信 †　　小林 真也 †

愛媛大学工学部情報工学科 *　愛媛大学大学院理工学研究科 †

1　はじめに

分散処理技術の一つであるグリッドコンピューティングとは，複数の計算機に処理の委託をすることで高い処理能力を獲得する技術のことである．特に，インターネット上にある不特定多数の計算機を利用する技術はエクスターナルグリッドと呼ばれ，使用可能な計算機の台数にほとんど制限がないという利点を備えている．一方で，使用する計算機の中に悪人の所有する計算機が混入し，処理内容の解析や誤った処理結果の出力を行われるリスクがあるため，現在はこれらを問題視しないような限られた目的でしか使用されていない．これらの問題点の解決策の一つとして，信頼できる計算機に処理の一部を委託し，悪人から保護する『断片の保護』と呼ばれる技術がある．しかし，保護量の増加は，隠蔽できる情報量の増加と引き換えに，グリッド全体の処理速度の低下を引き起こしてしまう [1].

本稿では，保護する処理の選定方法を 2 つ提案し，それぞれの方法によってどれだけの情報を隠蔽できるのか検証を行う．

2　セキュアプロセッシング

エクスターナルグリッドでは，委託された処理を実行する計算機群の中に，悪人の所有する計算機が混入する可能性が存在する．混入した悪人の行う行動として，委託された処理内容について無許可で解析をする『不正な解析』や，意図的に誤った処理結果を返す『改竄』がある．このような悪人の混入によって発生するリスクを防止・抑制する技術群のことを，セキュアプロセッシングと呼ぶ．不正な解析によるリスクの低減に用いられる技術の一例としては，プログラム分割や断片の保護がある．

2.1　プログラム分割

プログラム分割とは，処理の委託前にプログラムを分割することでプログラム断片 (以降は単に断片と呼ぶ) とし，各断片を別々の計算機へ委託する技術である．これにより，計算機 1 台あたりに委託する処理の量を減らし，悪人が一度に取得できる情報量を抑える効果を持つ．

2.2　断片の保護

断片の保護とは，断片の一部を信頼できる計算機のみへ委託することで，悪人から保護する技術である．これにより，保護した断片が持つ情報を悪人から隠蔽できる効果を持つ．しかし，保護した断片の処理には，エクスターナルグリッド特有の膨大な計算機資源を使用できなくなる．そのため，保護量が増加すると，グリッド全体の処理速度を低下させることになる．

3　依存関係

悪人が不正な解析に利用する情報として，処理間の依存関係がある．処理間の依存関係とは，プログラムを正しく実行していくために守らなくてはならない実行順序である．悪人の取得した断片群中にある依存関係の量が多いほど，各変数や命令文が持つ役割を把握されるため，不正な解析によるリスクを上げることになる．また，断片が依存関係によって連続している長さを連続長と呼ぶ．悪人の取得した断片群が持つ連続長が長いほど，値の変化の様子を連続して観察されるため，不正な解析によるリスクを上げることになる．

4　保護する断片の選定方法

悪人が取得する依存関係の量と連続長は，不正な解析によるリスクに大きく関わると考えられる．そこで，それらを基準として保護する断片の選定を行い，効率良く不正な解析のリスクを抑える方法を，以下に提案する．

4.1　依存関係の量を選定基準とする場合

断片間の依存関係は，互いに依存関係を持つ 2 断片の内，どちらか一方でも保護することで隠蔽が可能となる．そこで，悪人が取得可能な依存関係の量を効率良く抑えていくため，他断片との依存関係の数が最も多い断片を保護していく方法を提案する．

この方法をとることで，少ない保護量でも多くの依存関係の隠蔽が行えると期待できる．

4.2　連続長を選定基準とする場合

連続長は，元プログラムの記述上において隣接する断片同士により，一続きになることが多いと考えられる．そこで，悪人が取得可能な連続長を効率良く抑えていくため，最大連続長を構成する断片群の内，中央に位置する断片を保護していく方法を提案する．なお，最大連続長を構成する断片群の総数が偶数個だった場合は，中央に値する 2 つの断片の内，元プログラム上の記述順序がより早い断片を保護することとする．

この方法をとることで，少ない保護量でも悪人が取得な最大連続長を大幅に抑えられることが期待できる．

5　隠蔽効果の検証

10 個の数値計算プログラムをサンプルプログラム (以降は単にサンプルと呼ぶ) とし，提案した 2 つの選定方法のそれぞれに従って断片の保護を行うことで，どれだけの依存関係を隠蔽できるのか検証を行う．

5.1　断片の保護を行う準備

全てのサンプルは断片の保護を行うために，以下の処理を施した後，プログラム分割によって断片化する．

- ソースファイルの取り込み

Maximizing the effect of concealing code dependence on processing flow by reliable computers in an external grid

*Syunpei Sunada, Department of Computer Science, Faculty of Engineering, Ehime University

†Keiichi Endo, †Yoshinobu Higami, †Shinya Kobayashi, Graduate School of Science and Engineering, Ehime University

表 1　各サンプルプログラムが持つ特徴

プログラム名	A	B	C	D	E	F	G	H	I	J
プリプロセス前行数	23	29	26	101	26	45	38	32	31	62
繰り返し文展開後行数	409	417	409	536	405	579	511	507	408	448
総断片数	21	21	21	27	21	29	26	26	21	23
総依存関係量	1005	999	803	1272	503	4691	13552	1101	1501	920
最大連続長	20	4	16	26	20	4	13	25	20	18
依存関係にある他断片の数の平均	3.71	3.90	3.43	3.78	2.00	6.00	15.85	3.77	3.71	9.75

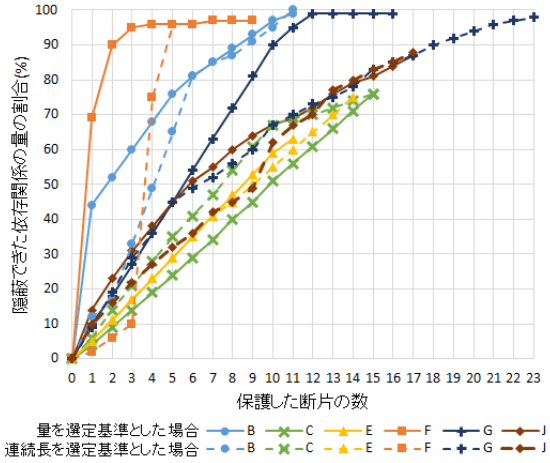

図 1　隠蔽できた依存関係の量の割合

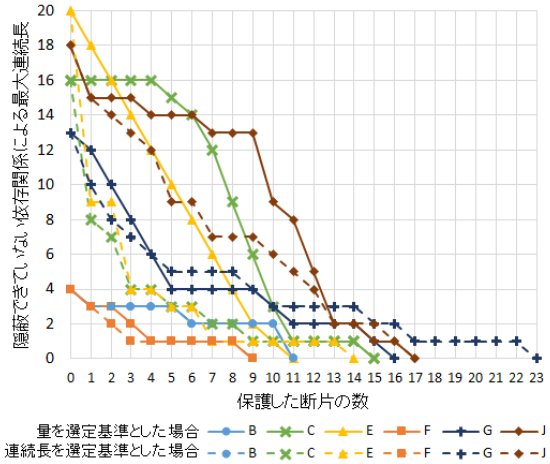

図 2　隠蔽できていない依存関係による最大連続長

- マクロの置き換え
- 空白行等の処理行わない行の削除・整理
- for 文の展開

for 文の展開時には，初期化式と継続条件式，最初期化式の全てが定数によって指定されている場合のみ，各命令式によって定められた回数分の展開を行う．

また，プログラム分割時には，断片の処理による各計算機への負担を抑えつつ，各断片が持つ依存関係の量を大きくできるとされる，20 行ずつの断片となるよう分割を行う [2]．

表 1 は，本節の処理を行う中で判明した，各サンプルが持つ特徴をまとめたものである．

5.2　評価方法

2 つの提案方法に従った場合，どれだけ目的に則した隠蔽が行えるのか，以下の基準に従って評価を行う．

- 隠蔽できた依存関係の量の割合
- 隠蔽できていない依存関係による最大連続長

なお，どちらの選定方法に従う場合も，複数の断片が選定される条件に当てはまった時は，元プログラム上での記述順序が早い断片を優先することとする．また，断片間の依存関係が全て隠蔽できた時点で，断片の保護は終了することとする．

5.3　評価結果と考察

評価の結果，期待通りに情報の隠蔽を行うことができなかったサンプルが 6 個見つかった．それらのサンプルに対して行った，断片の保護による隠蔽効果の評価結果が図 1 と図 2 である．

図 1 より，依存関係の量を選定基準とした場合に期待通りの結果となるなら，サンプル B や F のように，保護開始直後に多くの依存関係を隠蔽できるはずである．しかし，残りの 4 個のサンプルでは，各断片が持つ他断片との依存関係の量に違いがなかったため，隠蔽できた依存関係の量に大きな差が出なかった。中でもサンプル C は，連続長を選定基準とした場合のほうが多くの依存関係を隠蔽できていた．これは，元プログラムの記述上で中央付近にあたる断片が，断片内の依存関係を多く持っていたために起きたと考えられる．

図 2 より，連続長を選定基準とした場合に期待通りの結果となるなら，サンプル C や E のように，保護開始直後に最大連続長を大きく抑えられるはずである．しかし，サンプル B や F においては，断片間の依存関係が枝分かれし，最大連続長そのものが短くなってしまったため，予想した隠蔽効果が見られなかった．また，サンプル G や J においては，最大連続長が極端に短くなっている訳ではないにもかかわらず，予想した隠蔽効果が発揮されなかった．これは，for 文の展開時に依存関係にある命令文間の記述上の距離が長くなり，依存関係にある他断片の数が増えたことで，連続長の寸断が困難になったからであると考えられる．

6　結論

以上より，依存関係の量や連続長を選定基準とした場合，期待した隠蔽効果が十分に現れないプログラムが幾つか存在することがわかった．そのため今後は，ある選定基準に基づいて効果的に隠蔽が行えなかった場合，他の選定基準も考慮することができるような選定方法の考案が必要だと思われる．

謝辞

本研究は JSPS 科研費 JP26330105 の助成を受けたものです．

参考文献

[1] 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”, 情報処理学会全国大会講演論文集, Vol.78, No.3, pp.85-86, 2016

[2] 高須賀 智, 樋上 喜信, 小林 真也:“処理目的の隠蔽法における依存関係に基づくプログラム分割サイズに関する考察”,DICOMO(Multimedia, Distributed, Cooperative,and Mobile System) 2008, pp.1899-1904, 2008