# エクスターナルグリッドを対象とした処理目的の隠蔽法

合田 卓矢　樋上 喜信　小林 真也
愛媛大学大学院理工学研究科

## 1. 背景

ネットワーク上に散在する複数の計算機を利用し、大規模処理を効率的に処理する方法として、グリッドコンピューティングが注目されている。インターネットを介して、世界中のコンピュータを利用するエクスターナルグリッドは、より多くのコンピュータを使って構成することができるため、利用できる処理能力は大きい。しかし、悪意のある解析者がエクスターナルグリッドの中に紛れ込む可能性がある。もし、悪意のある解析者が存在すると、ネットワーク上のコンピュータにある個人情報や機密情報が覗き見されるなど、多大な損失を伴う可能性がある。このようなエクスターナルグリッド内の悪意のある解析者によってもたらされる危険性を回避するための方法は、今のところない。

そこで、我々の研究室では、エクスターナルグリッドを安全に利用できるように、処理目的の隠蔽法を提案している。

## 2. 処理目的の隠蔽法

データの隠蔽を実現するものとして、従来から暗号化技術がある。しかし、暗号化は、データ転送時等の第三者への漏洩防止が目的であり、送信先には、内容を隠蔽する必要がないということを前提としている。一方、難読化と呼ばれる耐タンパー技術は、プログラムの読み取りや改ざんへの対処技術であるが、十分な時間をかければ、処理内容を解読されてしまう。それに対して、この研究で行う処理目的の隠蔽法は処理の依頼を行う相手に処理の「意味」、「目的」、「処理手順」を知られることなく、処理の実行を依頼できる技術である。提案するアルゴリズムは解析者が得ることのできる情報から解読にかかる計算量を莫大にすることを目的としている。具体的には次のように合成断片を生成する（図１）。

- ネットワーク上に繋がれた複数台のコンピュータから信頼性が保障されたコンピュータを１台以上用意する。
- 信頼できるコンピュータで１つもしくは、複数のプログラムを分割し、それらを細かくインタリーブすることで合成断片を生成する。
- 合成断片の中にダミーコードを挿入する。

生成した合成断片は以下のように各コンピュータが実行する（図２）。

- 各合成断片は信頼できるコンピュータによって複数のコンピュータに送付され、送付された合成断片は順次、処理を行う。
- 合成断片の入出力データの受け渡しは、信頼できるコンピュータが行う。
- 信頼できるコンピュータが配布する合成断片と一緒にダミー断片も配布する。
- 合成断片を信頼できるコンピュータでも実行させる。

信頼できるコンピュータ以外のノード所有者が共謀したと考えた場合であっても、プログラムの分割とインタリーブ、またダミーコード、ダミー断片の挿入により、解析者グループが持つ部分プログラムの経路パターンが莫大になる。そして、合成断片の入出力データの受け渡しは信頼できるコンピュータが行うため、解析者はデータの流れが分からない。その上、信頼できるコン

ピュータでも合成断片を実行するため、解析者は全ての合成断片を獲得することは不可能である。これにより処理が第三者にあからさまになる危険性を回避できる期待がある。

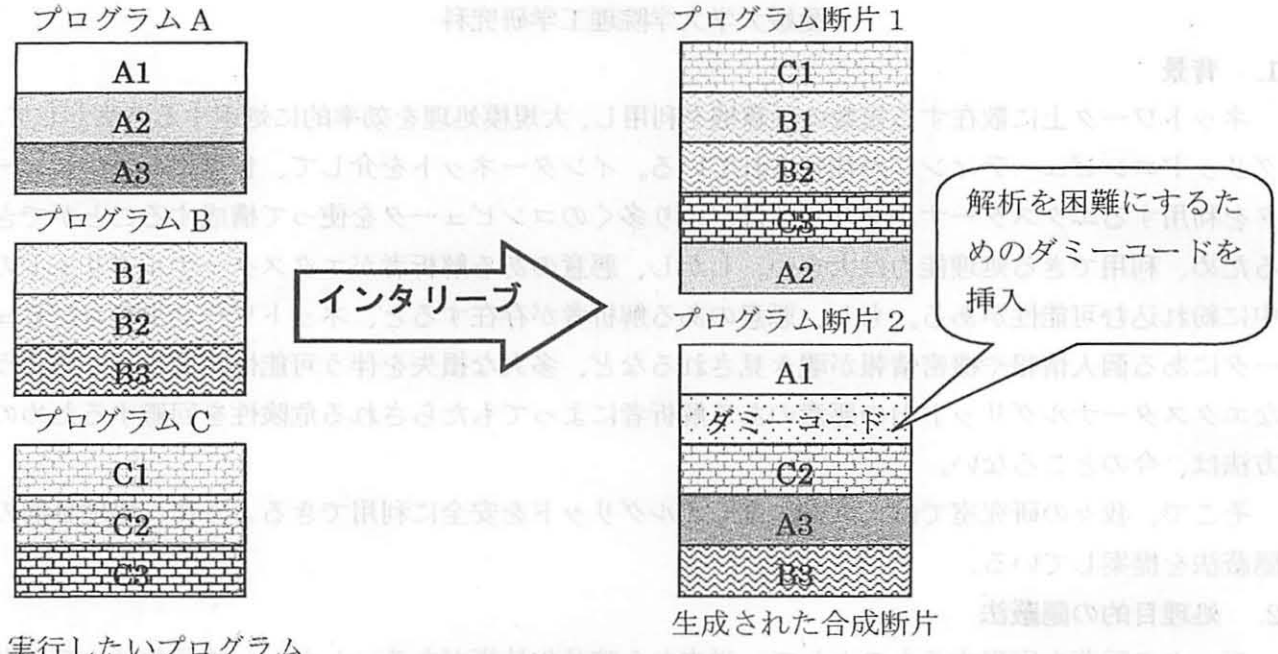


図1：プログラム断片の生成例

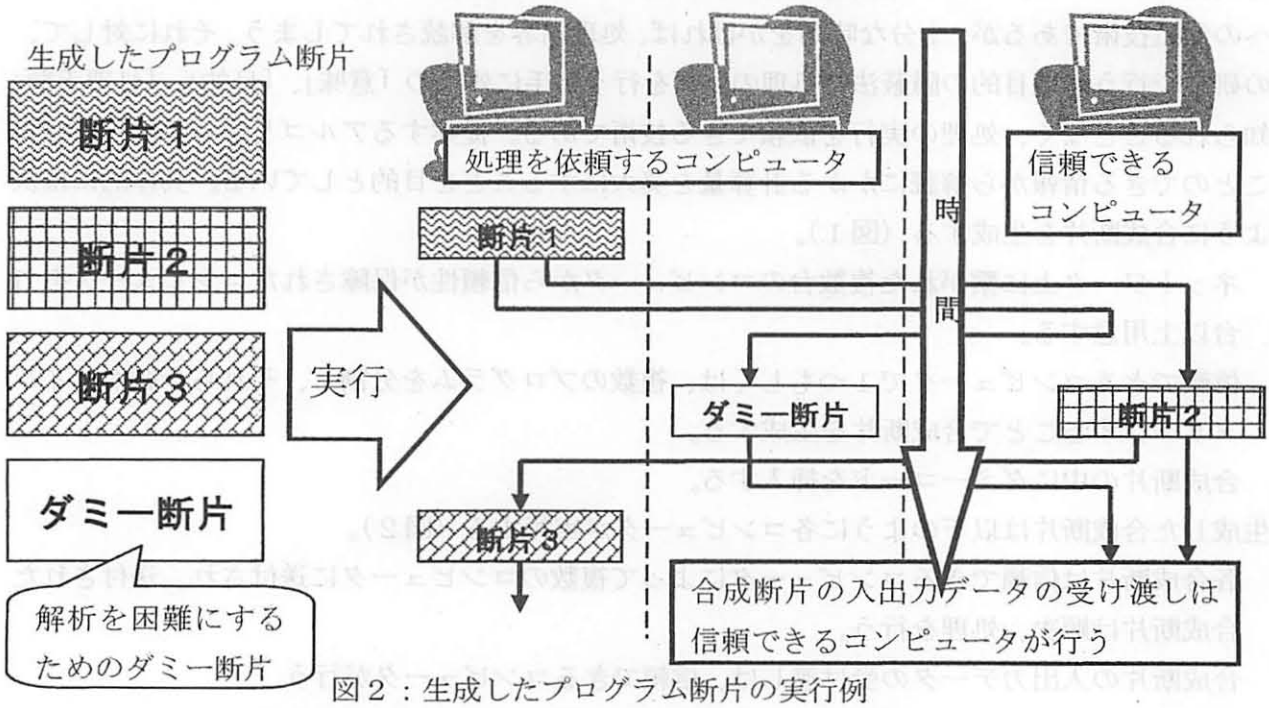


図2：生成したプログラム断片の実行例

## 3. 結論

我々の研究では、エクスターナルグリッドを対象とした処理目的の隠蔽を提案している。従来からある暗号化や難読化とは違い、第三者のみならず処理の実行を行う相手にも処理目的を知られないようにする方式であり、開放型グリッドコンピューティングの新たな応用を切り開くものである。