要 旨

難読言語 Malbolge の逆コンパイル困難性に関する研究

菅 優也

プログラム中のアルゴリズムやデータ構造を秘密に保つために，実行結果を保ったままプログラムを解析しにくいように書き直す難読化と呼ばれる技術がある．

難読化の研究の一つにプログラムを難読言語に変換するというものがある．難読言語とは，いかにプログラミング言語上でプログラムの作成を困難にするかを目標とした言語である．飯澤は,「この世で一番分かり辛くする事」を目標とした Malbolge にプログラムを変換することで難読化を行っている．

この手法では，プログラムを機械的に Malbolge プログラムへ変換しているため，作成された Malbolge プログラムから機械的に元のプログラムへ復元できる可能性がある．飯澤も逆コンパイルの可能性について触れているものの，実際に逆コンパイルを行うなどの検証を行っておらず，難読効果の検証が不十分である．そこで本論文では飯澤の手法に対し，実際に逆コンパイラを作成することで難読効果の検証を行った．

結論として，作成した逆コンパイラにより元のプログラムと同等のものを出力することができたため，飯澤の難読化方法は難読効果が弱いといえる．一方，Malbolge の仕様を利用し，変換した Malbolge プログラムの前後にダミーコードを追加することで難読効果を向上させることができるという考察も得られた．

キーワード　難読化，難読言語，Malbolge，逆コンパイル

Abstract

A study on the difficulty of the decompilation of an esoteric programming language Malbolge

Yuya KAN

Obfuscation is a technique to rewrite a program without changing execution results in order to make it difficult to analyze and to keep its algorithm and data structure secret.

Izawa proposed an obfuscation method in which a program is converted into an esoteric programming language Malbolge. An esoteric programming language is a language that aims at making it difficult to construct or understand a program. Malbolge is one of esoteric programming lanuages and aims at being the most difficult in the world to understand the construction of a program. However, Izawa's obfuscation is mechanical convertion and has possibility that we can reconstruct the original program from a Malbolge program. Though Izawa has mentioned the possibility of decompilation, sufficient investigation of the effectiveness of the obfuscation has never been given. Therefore this thesis investigate the effectiveness of Izawa's obfuscation by constructing a decompiler.

As a result, Izawa's obfuscation is vulnerable to decompile because the decompiler reconstruct the original program from a Malbolge program. However, it is also found that the obfuscation can be improved by adding some dummy code at the top and bottom of a program.

key words obfuscation, esoteric programming languages, Malbolge, decompilation