論文の内容の要旨

論文題目　Theories of Information Hiding in Lambda-Calculus:
Logical Relations and Bisimulations for Encryption and Type Abstraction

ラムダ計算における情報隠蔽の理論：
暗号化と型抽象のための論理関係と双模倣

氏名　　住井 英二郎

二つの情報隠蔽形式に関わるプログラムの等価性に対する、二つの証明方式について研究する。その証明方式とは論理関係と双模倣であり、情報隠蔽形式とは型抽象と完全な暗号化（動的封印としても知られる）のことである。我々は、これらの理論が情報隠蔽に関わるプログラムについて論ずるために有用である、と主張する。健全性および完全性の定理と、抽象データ構造や暗号プロトコルを含む例を通じて、この主張を証明する。

型抽象はプログラミング言語において、もっとも基本的な情報隠蔽形式である。論理関係は型抽象について論じる主要な方式であり、関係パラメタ性あるいは表現独立性と呼ばれる。暗号化はもう一つの基本的な情報隠蔽形式であり、通信システムにおいて支配的である。実は、暗号化に似た操作はプログラミング言語においても有用であり、動的封印と呼ばれている。このようなコンピュータソフトウェアにおける二つの情報隠蔽形式の関連に鑑みれば、それらの間にもっと形式的な関連を確立し、一方の理論を他方へ応用できないか考えることは自然である。我々はこの疑問に肯定的な解答を与える。

まず、関係パラメタ性の理論を型抽象から動的封印に適用する。そのために、動的封印のためのプリミティブにより拡張された単純型つきラムダ計算と、その論理関係を定義する。理論の応用の実例として、この計算体系にいくつかのセキュリティプロトコルを注意してエンコードし、それらの安全性を証明する。

次に、動的封印のための双模倣の理論を構築する。論理関係と異なり、この理論は再帰関数や再帰型のある、あるいはまったく型のない、より豊かな言語へ容易に拡張できる。我々は動的封印のある型なしラムダ計算を定義し、様々な抽象データ構造の実装の等価性や、複雑な暗号プロトコルの正しさを証明することにより、この理論の強力さを

示す。

さらに、この双模倣の理論を動的封印から型抽象へ「フィードバック」し、総称型・存在型および再帰型のあるラムダ計算における、健全・完全なおかつ初等的な型抽象の理論を初めて得る。例として、抽象データ型、生成的関手、オブジェクトのエンコーディングについて論じる。

最後に、型抽象から動的封印への型誘導変換の完全抽象の予想と、抽象性を損なわずに静的検査・動的検査・無検査のコードを同時にサポートする、言語環境への応用の方向の可能性について述べる。