小特集「ゼロ知識証明とその応用」の編集にあたって

太　田　和　夫†

ゼロ知識対話証明（以下，ゼロ知識証明と略す）は，1985年に概念が提案されて以来，計算量理論，暗号理論の発展において重要な役割を担っている．ゼロ知識証明とは，証明者が秘密の情報を明かすことなく，検証者と対話を行いながらその秘密を知っていることを検証者に対して証明する方法である．ゼロ知識証明は計算機科学と情報セキュリティ技術におおきなインパクトを与えた．しかし，その研究と応用の現状と動向は広く知られているとは言いがたい．

ゼロ知識証明は，ゼロ知識証明を構成できる問題のクラスを特徴づける方向で理論的な研究が進展し，最近，多項式の領域で表現できる問題は対話証明で証明できるという最終的な結果が示された．一方，応用面では，ゼロ知識証明を用いると，パスワード（秘密）を示さずにパスワードを知っていることを証明でき，安全に本人確認できるので，注目されている．

本小特集では，ゼロ知識証明の研究の現状と動向について，理論とその応用の観点から解説する．本小特集によって，ゼロ知識証明のインパクトとその応用を情報処理学会の会員に幅広く理解していただけたら幸いである．また，本号には，本小特集のほかに，計算量理論・暗号理論と密接に関連した解説記事も2件掲載されているので，あわせてご一読いただきたい．

本小特集は，次の4編から構成されている．概略は，以下のとおりである．

「ゼロ知識対話証明の原理と課題」

小山謙二（NTT）による「ゼロ知識対話証明の原理と課題」では，本小特集の導入として，ゼロ知識証明の概念を，幅広い読者が理解できるように，対話形式で平易に解説している．

「ゼロ知識証明の応用」

太田和夫，藤岡淳（NTT）による「ゼロ知識証明の応用」では，ゼロ知識証明の応用として，重要なセキュリティ技術である，公開鍵暗号，利用者認証，ディジタル署名などへの適用について解説している．

「ゼロ知識証明とマルチパーティプロトコル」

黒沢馨(東工大)，岡本龍明（NTT）による「ゼロ知識証明とマルチパーティプロトコル」では，理論と応用の観点から，ゼロ知識証明のゲーム（コイン投げ，選挙，契約など，マルチパーティプロトコルと呼ぶ）への応用について解説している．本号に掲載されている解説「ビザンティン合意問題—信頼性の低い分散ネットワーク上での合意問題」（山下雅史(広島大)）と密接に関連するので，あわせてご一読いただきたい．

「ゼロ知識証明モデルと計算量理論」

静谷啓樹(東北大)，伊東利哉(東工大)，桜井幸一（三菱）による「ゼロ知識証明モデルと計算量理論」では，計算量理論の観点から，ゼロ知識証明の研究の位置づけを明らかにしている．

なお，本号に掲載されている解説「一方向関数のお話し」（渡辺治（東工大））にも計算量理論と暗号理論の関係が紹介されている．

ご多忙にもかかわらず，執筆を快諾し多大な時間をさいていただいた執筆者の方々，ならびに編集，査読にご協力いただいた方々に深く感謝いたします．最後に，本特集が読者にとってゼロ知識に終わらないことを切望して，編集にあたっての挨拶とします．（平成3年5月7日）

† NTT 情報通信処理研究所