まえがき

昔から数理的技法に対して懐疑的な人は多かった．特にソフトウェアの検証に関しては，何百万ステップという巨大なプログラムを検証することなど絶対に不可能だと思いこんでいる人は今でも多いと思う．実はそんなことはなくて，近年のソフトウェア検証技術の進歩により，巨大なプログラムの検証も現実的になってきている．ただし，自動的に検証可能な性質は限られており，複雑な検証要件に対してソフトウェアの正しさを証明することはまだまだ難しいと言わざるをえない．

何百万ステップという巨大なプログラムと比べて，いわゆる暗号プロトコルは，簡単なものならば数ステップ，複雑なものでもせいぜい数十ステップのメッセージのやり取りによって規定される．ところが，そのようにほんの一握りのメッセージによって定義されるプロトコルの正しさを保証することは，存外に難しいのである．実際に，広く用いられているプロトコルの誤りが後になって発見される，ということがしばしば起こる．

このようなプロトコル検証の難しさはどこから生じているのであろうか．一つには，暗号プロトコルの検証要件を的確に定義すること自体が難しいからである．たとえば，匿名性や認証性などの要件を厳密に定義することは，決して自明なことではない．また，プロトコルの実行環境を適切にモデル化することも難しい．一般に，プロトコルは多くの実行主体（エージェント）が並列に動作する環境で実行される．それらのエージェントは非決定的に，しかも確率的に動作する．また，各エージェントは，計算時間やメモリなど限られた計算リソースのもとで動作することが仮定される．プロトコルに対する攻撃者もエージェントの一種であるが，これに無限の計算時間を許してしまえば，計算論的な仮定に基づくどんなプロトコルも破られてしまうからで

ある．したがって，暗号プロトコルの検証要件は，並列性，非決定性，確率性，計算リソース（特に計算時間）の制限を想定して，定義されなければならない．

そして，そのように定義された検証要件を証明する方法論も，当然ながら，自明なものではない．もちろん，数理的技法の分野においては，並列性や確率性などは従来から活発に研究されており，それらに対処するための方法論も発展してきている．しかし，暗号プロトコルの検証においては，それらの方法論のすべてを束ねた上に，暗号や署名など，暗号プロトコルに特有の演算を扱わなければならないのである．

しかし，以上のような困難さが存在するからこそ，暗号プロトコルの検証は，数理的技法の研究者たちにとって，挑戦し甲斐のある対象となったのである．数理的技法の分野で活躍してきた多くの世界的権威たちが，暗号プロトコルを対象とした研究を始め，その波が日本にも及んだ結果として，日本応用数理学会に「数理的技法による情報セキュリティ」研究部会が立ち上がったのである．

もちろん，数理的技法の研究者たちが目を付ける以前に暗号プロトコルの検証の研究が行われていなかったのかというと，決してそんなことはない．暗号学者たちが長年に亘ってプロトコルの正しさを保証する方法論を発展させてきた．特に，暗号系の強さを厳密に定義する枠組みが開発され，それにしたがってプロトコルの正しさを証明することが一般的に行われるようになった．そもそも，上述したような制限された計算リソースのもとで確率的に振る舞うエージェントを，確率的多項式時間チューリング機械としてモデル化したのは暗号学者たちである．

ところが，確率的多項式時間チューリング機械を用いた議論は，ややもすると，非常に複雑で間違いやすい．発表された時点で証明付きと銘打たれたプロトコルに，後になって誤りが発見される，ということがしばしばあった．そこで，数理的技法の研究者たちが，暗号プロトコルの検証に本格的に取り組むようになった，という次第である．その結果，暗号学者たちと数理的技法の研究者たちが一致団結して，暗号プロトコルの検証の研究を進めるようになり，ここに，1 つの境界分野が生まれた，と言っても過言ではないだろう．

本書は，そのような新しい境界分野に関する入門書である．この分野における基礎的な概念と主要な方法論について解説している．言うまでもなく，暗号分野の研究者と数理的技法の研究者に読んでいただきたい．なぜなら，暗号プロトコルの検証に関する研究は，暗号分野にとっても数理的技法にとっても，実りが多いからである．暗号分野においては，検証のための方法論が進展することにより，より煩雑なプロトコルや複雑な検証要件に取り組むことが可能となる．数理的技法にとっては，モデル化の対象が広がり，検証のための新たな方法論が展開される．どちらの分野にとってもいいことばかりなのである．

本書を執筆・編集するに当たり，多くの方々のご援助をいただいた．特に，出版に際したいへんお世話になった共立出版株式会社編集部の諸氏，本書を監修していただいた日本応用数理学会出版担当理事の西垣一朗氏，執筆・編集の機会を与えてくださった元日本応用数理学会会長の岡本龍明氏，さらに草稿に対して貴重なコメントをいただいた田辺良則氏，川本裕輔氏，久保田貴大氏に感謝の意を表したい．

2010 年 5 月

編者　萩谷 昌己
塚田 恭章