「数理科学」は語る

30年前から現代へのメッセージ

今井　秀樹

1980年12月号

1980年12月号の符号理論特集号に「計算機のための誤り訂正符号」という記事を書いたとき，筆者は30年後の符号理論について，深く考えてはいなかった．ただこの理論の究極の目標「シャノンによって与えられた通信・記録における信頼性向上の限界を達成する実用的符号の構成」は30年程度で実現されることはなく，符号理論は坦々と進展すると思っていた．しかし，その後，符号理論が辿った道は筆者の予想をはるかに超え，波乱に満ちたものであった．

第一の波は実用化の大波である．誤り訂正符号の計算機への応用やコンパクトディスク（CD）への応用が契機となり，1980年前後から符号理論の通信・記録システムへの応用が急速に拡大していった．この新たな応用を探る過程の中で，新しい研究分野もいくつか生まれた．最も成功したのは，信号の変調と誤り訂正符号化を一体化し最適化を図る符号化変調の分野である．

応用が進展する一方で，CDに用いられたリード・ソロモン符号などの代数的符号を高度化した代数幾何符号の理論も多くの研究者の関心を集めた．符号理論の主役であった「代数的符号理論」は幾何学の助けも借りて，より深く豊かなものとなったのである．

しかし，1993年に第2の大波が襲ってきた．ターボ符号の提案である．これはシャノンの限界に迫る実用的な符号として初めてのものであった．それまで長い間「人が実用化できる符号はシャノンの限界に達しない」という俗説が流布していただけに，ターボ符号発明のインパクトは極めて大きかった．これはまた，符号理論の主役を代数的符号理論から，確率論を基盤とする「確率的符号理論」へ変えていくことにもなった．

ターボ符号は繰り返し復号を行うことによって，その高い性能を達成する．この考え方は実は，1963年に低密度パリティ検査符号（LDPC符号）の復号のためにギャラガーによって既に提案されていたが，その当時のコンピュータではこのような復号は実際上不可能であったため，それが注目されることはなかった．しかし，ターボ符号の出現によりLDPC符号も再評価され，シャノンの限界に迫る符号として現在の符号理論の最も重要な研究対象となり，実用化も進んでいる．

この30年間，符号理論は大きく変わり，その主役が交代し，シャノンの限界に迫る符号も見出された．しかし，これで終わりではない．実際の通信・記録システムは極めて多様で複雑ある．そのようなシステムに対し，高信頼性ばかりではなく様々な機能を持つ符号が要求されるようになってきた．それに対処し得る符号を探る中から，符号化変調がそうであったように，新たな研究分野が生まれてくるであろう．そして，第3の大波となるような新しい原理に基づく符号が現れることを期待したい．

（いまい・ひでき，中央大学理工学部，
産業技術総合研究所情報セキュリティ研究センター）