

## 20兆年かけても破られないー



県立大院・五十部准教授ら

# 6G向け暗号技術初開発

暗号技術について説明する、兵庫県立大大学院の五十部孝典准教授＝神戸市中央区港島南町7

2030年ごろの実用化が見込まれる次世代の移動通信システム「6G」の実現に不可欠な高速・大容量の暗号技術を開発すること、兵庫県立大大学院情報科学研究科の五十部孝典准教授らとKDDI総合研究所のグループが世界で初めて成功した。スパコンをはるかに上回る性能の量子コンピュータが実現しても解読に20兆年以上かかる安全性と、毎秒100ギガ以上のデータを暗号化できる高速性を兼ね備えるという。

現在、通信エリアの拡大が進む5Gでは、主要技術で日本勢は後れをとっており、政府は巻き返しに力を入れている。五十部准教授によると、安全性と高速性を両立させた6G用の暗号技術は、ほかに開発されておらず、今後数年かけて第三者の検証を受け「国際標準を目指したい」として

## 日本勢巻き返しへ国際標準目指す

5G<sup>1</sup>ではデータを暗号化する鍵として「128ビット」の情報を使用する。1か0の数字が128個並んだもので、組み合わせのパターンは2の128乗(約1800京の2乗)。1秒間に44京回計算できる世界最速のスパコン「富岳」でも、解読には約24兆年かかる。ところが量子コンピュータが実現した場合、40秒程度で解読される恐れがあり、通信の安全性を現在と同程度確保するには「256ビット」の鍵が求められていた。加えて、6Gの通信速度は毎秒100ギガ<sup>2</sup>超と5Gの10倍以上が想定され、暗号化にも高速性が要求された。

五十部准教授らは、データを8分割して並列で処理する暗号方式を開発。現在のパソコンの性能でも毎秒138ギガ<sup>3</sup>の速さで暗号化することに成功した。開発を支援した総務省は「暗号は通信の安全性を支える根幹技術。6Gで先行する上で世界初の成果は評価できる」としている。(古根川淳也)

名前【 】

①兵庫県立大大学院の五十部准教授らとKDDI総合研究所のグループが世界で初めて開発に成功した技術は何ですか。

②その技術は安全性と高速性でどのような能力がありますか。

安全性

高速性

③現在、通信エリアの拡大が進む5Gのデータの暗号の解読には世界最速のスパコン「富岳」でどれだけかかりますか。また、量子コンピューターが実現した場合、どれぐらいと考えられているのでしょうか。

富岳

量子コンピューター

④五十部准教授らは、どのような暗号方式を開発し、どのような速さで暗号化することに成功しましたか。

⑤現在主流の4Gと5Gの違いや、6Gが目指していることを調べてみましょう。