平成28年11月23日　長崎新聞　ふるさと総合面掲載

県立大・連続セミナー　3

暗号技術の基礎

情報守る仕組み知ろう

情報システム学部
情報セキュリティ学科准教授
穴田　啓晃

インターネットにつながった電子機器を多くの人が利用する現在、悪賢い第三者が私たちの通信を聴こうとしていると言われています。この脅威に対し、暗号は私たちの情報を第三者に分からなくする機能を実現しています。また、個人番号カードの交付とともに電子証明書の利用が身近になりました。その暗号技術は、なりすましや改ざんを防ぐデジタル署名です。

暗号の歴史は古く、AをCに、XをZに、という具合に文字をずらしたのがその起源です。何文字ずらすという暗号化・復号の数字は「鍵」と呼ばれ、送信者・受信者が共通に持ちます。この種の「共通鍵暗号」は20世紀初めから戦争とともに高度化され、主要な方式の一つとなりました。その一方、現代の画期的な発明に「公開鍵暗号」があります。暗号化には公開リストに載っている「公開鍵」を、復号にはそれと異なる「秘密鍵」を使うのが特徴です。

公開された鍵で作った暗号文がなぜ解読されないのか？　標準的なRSA暗号の場合、実は「公開鍵」に600桁以上という非常に大きな数字が用いられています。この数字を積に分解するのに大変な手間が掛かる、というのがその根拠なのです（四桁ですら例えば1073＝29×37と分解するのはちょっとした手間です）。このRSA暗号が動く仕組みの基本は、小学生のとき親しんだ剰余算（商と余りを求める計算）です。そして、剰余算の世界で成り立つ「オイラーの定理」により、暗号文がきちんと復号されます。

暗号技術を適切に使って情報を守るため、機能する根拠や動く仕組みを押さえておくことが不可欠と考えています。