平成28年11月30日　長崎新聞　ふるさと総合面掲載

県立大・連続セミナー　4

# 暗号技術の実際

情報システム学部
情報セキュリティ学科教授
松崎　なつめ

## コストと利便性を考慮

暗号は近寄り難く自分とは無縁と考える人が多いですが、実は、とても身近なところで社会の仕組みや皆さんの生活を守っています。

例えば、インターネットで買い物をする際のクレジット決済では、ＳＳＬ／ＴＬＳといった暗号を応用した仕組みで相手の正当性を確かめ、決済情報を秘匿化しています。サイトでＳＳＬ／ＴＬＳが使われているかは、アドレスバーの鍵マークで確認できます。

また、ＤＶＤやＢｌｕ－ｒａｙではコンテンツを暗号化することで、不正コピーを防止しています。さらに最近話題の暗号通貨においても、そのキーテクノロジーのブロックチェーンで、取引の不正な変更を防止するために暗号が使われています。暗号を用いてネット上のデータや著作権者の権利を保護しているからこそ、安心して便利に買い物をし、映画コンテンツを自宅で楽しむことができるのです。

さて、こういった暗号を組み込んだ暗号システムを設計する際、どんなことに気を付けて設計するのでしょう。技術的には、暗号強度を上げることは可能ですが、それに伴いコストが上がり、処理時間がかかってユーザーの利便性を損なうことがあります。

このため、セキュリティーは、コストと利便性とのバランスを考慮し、どんな能力を持つ攻撃者のどんな攻撃を防ぐのかを定め、どこまで技術で対応し、ほかは法律などで対処するといった方針を関連するステークホルダ間で決めます。

そして、こうした過程を経て作られた暗号システムは、新たな攻撃や周りの環境などの変化を考慮して定期的に見直すことが重要です。

**（次回掲載は12月14日です）**