頭がしびれるテレビ
あなたを守る暗号の秘密

対象校種　高校
対象教科　情報　総合

放送日：2012年5月14日　放送時間：29分

この番組の良さ

● 暗号は通信に欠かせない技術

インターネットはその仕組み上、バケツリレーのようにデータが送られどこを通っていくかは送信者にはわかりません。また、無線LANやスマートフォンの普及により、データは電波として至る所に飛んでおり、悪意のある人がデータを盗み見ていることに気づきにくい環境といえます。データの盗聴を防ぐ暗号は、現代に欠かせない技術となっており、その仕組みの基礎に触れることができます。

● 暗号通信の仕組み

インターネット通信に限らず、これまでも重要な情報のやりとりには暗号が利用されてきました。古くは文字を一定数ずらして表記する古代ローマのシーザー暗号（カエサル式暗号）が有名です。以後、暗号技術は軍事・政治の世界を中心に進歩が繰り返されてきました。インターネットの登場によって、一部の人だけでなく誰もが通信の安全について留意しなければならない時代となっています。

執筆者
千葉県総合教育センター
研究指導主事　永野　直

番組活用のポイント

● 生活に密着している暗号技術

インターネットを利用する際、情報を受信するだけでなく利用者側からも様々な情報が送られていきます。例えば買い物サイトを利用する際には、氏名や住所の他、クレジットカード情報などの重要な情報を送信しなければなりません。本番組を通して、日常的に通信の安全性について意識しなければならない事に気づくでしょう。

● 公開鍵方式とは

暗号の弱点は、「鍵」が漏れてしまうと、簡単に復号化されてしまうことにありました。その弱点を克服したのが公開鍵方式です。暗号化と複合化の鍵が異なり、暗号化に使う公開鍵（数値）は秘密にする必要がないのです。この公開鍵は受信者が知っている秘密鍵を元に計算で作ります。つまり、公開鍵は秘密鍵から計算で簡単に作れ、逆に公開鍵から秘密鍵を求める計算が難しければ暗号鍵として使える事になります。これを実現しているのが、「素因数分解には時間がかかる」という特性です。例えば19×31=589という計算は簡単にできますが、589の素因数分解は時間がかかります。（実際のRSA暗号の仕組みはもう少し複雑です。）スーパーコンピュータでも、数百桁の素因数分解には1億年かかると言われています。

● 今後の情報社会と暗号

現在の技術では、コンピュータを使って暗号を破ろうとしても膨大な時間がかかるため実質的に解読できません。ただし、技術の進歩によってコンピュータの性能も飛躍的に上がります。量子コンピュータが実用化されれば、秘密鍵もすぐに解読されてしまうと言われています。進歩し続ける情報技術とともに、情報セキュリティも進歩し続けなければならないことに気づく素材になるでしょう。

対象校種 高校　対象教科 情報　総合

AIと「命・人生」の関係を考える

［授業時間 50分］　部分視聴

生徒の思考の流れと活動の流れ	教師の支援と評価
怖い・嫌だ・気持ち悪い、など そもそも盗聴なんてされることがあるの？ ウイルス対策ソフトを入れれば大丈夫？ 住所や名前、個人情報 ネットショッピングのクレジットカード情報 どんなデータも盗聴されたくない	・インターネットを使うとき、データが盗聴されているとしたらどう思うか聞く。 ・もし盗聴されたら困るというデータにはどんなものがあるが聞く
インターネット通信のデータはどうやって守られているのだろうか？	・インターネットの仕組みに簡単に触れ、通信経路は一定ではないことを確認する。
暗号が使われているのかな でも暗号の仕組みって実際どうなっているのだろう	・可能であればネットワーク内に流れているデータを見せると良い。（パケットキャプチャのデータ）
番組部分視聴①　（10分25秒～14分38秒）  最も基本的な暗号（シーザー暗号） 共通鍵の仕組み 歴史と暗号（エニグマとその解読など）	・番組の前半部分を視聴する。 ・視聴後に、シーザー暗号を使って、簡単な言葉をやりとりさせてみても良い。
暗号は政治や戦争の場面で重要だった インターネットによって個人も暗号化が必要になった	・視聴後に暗号と自分たちとの関わりについて考える場を設定する。 （暗号の必要性は国家レベルから個人レベルに変化している。）
番組部分視聴②　（15分12秒～27分29秒）  RSA暗号の誕生 公開鍵と秘密鍵の仕組み 暗号解読とその将来	・番組の後半部分を視聴する。 ・番組では実際のRSA暗号の仕組みを簡略化して説明している。より詳しく補足しても良い。
実際にWebサイトの証明書（公開鍵）について調べてみよう	・視聴後に簡単な素数同士のかけ算と素因数分解をしてみると実感しやすい。
ブラウザのアドレス欄に鍵のマークがついている 公開キーは2048ビットで、16進数表記だ 通信するサイト毎に証明書が発行されている 証明書を導入していないサイトもあるね いつかはRSA暗号も解読されてしまうの？	・PC教室のブラウザを操作して、SSL/TLSの証明書について調べ、わかったことを発表する。 ・SSL/TLS通信ではないサイトの今後の扱いや今後の暗号技術についてグループで調べる時間を設定し、発表してもよい。
インターネット通信のデータは、暗号技術によって守られ、その技術は進歩し続けている。自分たちもセキュリティ意識をもって通信をしなければいけない。	
最新の暗号技術、今後の暗号はどうなっていくのか知りたい	【主体的に学習に取り組む態度】 情報社会におけるセキュリティ、データ通信のあり方について考え、情報社会に主体的に参画しようとする態度で取り組むことができたか。