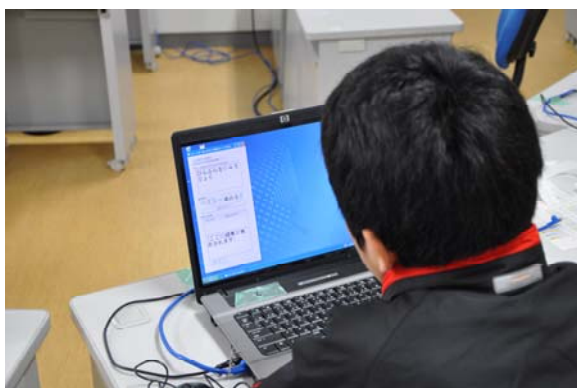
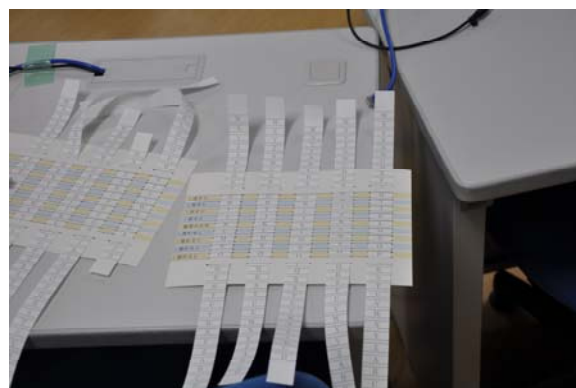


事業名	代表者所属	徳山工業高等専門学校
11KJ-020	代表者	技術職員 藤本 竜也
通信・情報を守る仕組みを知ろう － 暗号の基礎 －	開催地	山口県
	助成金額	10 万円
活動概要		
<p>日時： 2011 年 12 月 23 日 (金) 13:00～16:40</p> <p>場所： 徳山工業高等専門学校 (周南市)</p> <p>対象： 中学生</p> <p>参加者(人)： 6 人</p> <p style="padding-left: 40px;">内訳(小中高の先生； 0 人)(生徒； 6 人)</p> <p>内容： 暗号および情報セキュリティの基本事項について、座学および演習を通じて学習する。また、さまざまなデモ実験を行ない、暗号化の必要性を感じてもらう。</p>		



パソコンを用いたシーザー暗号の演習



シーザー暗号の補助シート



デモ実験の様子

事業の目的・ねらい

近年のめざましい情報通信技術(ICT)の発展により、日常生活のあらゆる場面に情報端末が存在し、気軽に情報のやりとりができる環境が整いつつある。これは小中学生においても同様であり、パソコン等を用いたインターネット通信、携帯電話の所持などさまざまな情報に触れ、またこれを発信する機会が増えている。その

一方で、情報セキュリティに関する教育は十分行われておらず、情報盗聴のリスクを知らないまま使用している事が多い。

本事業では、情報の暗号化の基礎に焦点を絞り、暗号の必要性などをデモ実験や演習を通じて体験する講座を行なう。この講座を通じて、セキュリティに関心をもつきっかけを提供する。

事業の概要

本講座では、内容を 1. 情報・通信とは何か、2. 暗号の基礎、3. シーザー暗号 の3つに分けて進めた。各内容でははじめに座学を行ない、基本的な事項の解説を行なった。その後、関連したデモ実験や演習を行ない、座学で解説した事項に関する理解を深めてもらった。

1. 情報・通信とは何か

本講座の主テーマである暗号に先立ち、情報や通信に関して、携帯電話やノートパソコンといった身近なデバイスを例示しながら解説を行なった。また同時に、通信を行なうときは情報が盗まれる危険性があることを説明した。

このテーマのまとめとして、メールの本文や件名、ユーザのパスワードなどを読み取るデモ実験を行なった（実際に受講者にも体験してもらった）。

2. 暗号の基礎

暗号に関する基本事項として、暗号方式(アルゴリズム)や暗号鍵などの説明をし、さらに、暗号の目的や効果についても説明を行った。また、無線 LAN(WEP, AES など)やインターネットショッピング(SSL/TLS)、DVD(CSS など)を例としてあげ、意識はしない様々な場面で暗号が使用されていることを解説した。

このテーマのまとめとして、簡単な暗号を解読する演習を行なった。また、スキュタレー暗号などを実際に見せた。

3. シーザー暗号

具体的な暗号方式として、仕組みが単純で暗号化・復号の処理を容易に行なうことができるシーザー暗号を取り上げ、その原理について説明を行った。

演習では、シーザー暗号の補助ツール(事前作成)や専用アプリケーション(事前開発)を使用して、暗号化や復号を実際に体験してもらった。また、ペアになり、暗号文のみを相手に伝えて元の文章を当ててことに挑戦してもらい、情報が守られていることを確認した(このとき、いろいろな鍵を試してみると正解が得られることも確認してもらった)。

最後に、暗号を用いることで情報・通信の秘密を守れるが、あらゆる場面で有効であるとは限らないことを説明し、本講座のまとめとした。

成果・効果

本講座の対象である中学生にとって、暗号や情報セキュリティは馴染みがないであろうテーマであったため、内容は極力シンプルにし、また、身近な例や演習・デモ実験を多くしてイメージを掴んでもらえるような構成を心がけた。受講者の反応を見るかぎり、少し難しい点もあったようであるが、概ね理解してもらえたと思う。

講座の目的としていた、日頃何気なく使用しているデバイスの危険性を知らうことや、情報セキュリティに関心を持つきっかけ作りという点では、十分とは言えないものの成功したと思う。