ファイル暗号化実習

－公開鍵暗号方式によるファイルの暗号化と復号－

１　ねらい

情報セキュリティの確保のため，ウェブサイトを閲覧するときなど，日常的に公開鍵暗号方式の技術が利用されている。この実習を通して，公開鍵暗号方式を体験し，その仕組みを理解する。

２　内容及び教材

(1) 指導内容

情報Ⅰ　情報社会の問題解決（情報セキュリティ）

情報Ⅰ　情報通信ネットワークとデータの活用（情報セキュリティ）

(2) 使用教材（配付資料等）

ア　授業プリント

イ　授業説明ファイル１，授業説明ファイル２

ウ　使用ツール

公開鍵暗号方式に対応した暗号化ソフトウェア

３　指導の流れ

(1) 基本的な指導の流れ

時限	学習内容・学習活動	指導上の留意点
1	○ＲＳＡ暗号についての学習 ・暗号化，公開鍵，秘密鍵について学習する。 ○公開鍵・暗号鍵の作成	・授業プリント及び説明用ファイルを利用する。
2	○ファイルの暗号化 ・ペアワークの相手へ，自分の公開鍵を送信する。 ・相手の公開鍵を取得する。 ・相手の公開鍵でファイルを暗号化する。 ・暗号化したファイルを相手へ送信する。 ・相手から受信したファイルを自分の	・鍵や暗号文の送受信には，ファイルサーバや電子メールを活用する。 ・暗号化，復号する際に使用する鍵の種類に注意するように声掛けをする。

	秘密鍵で復号する。 ○報告書の作成・提出 ・授業プリントを記入する。	・ペアワークの相手以外の暗号文は自分の秘密鍵では復号できないことを確認するよう促す。

(2) 発展課題

電子署名の作成と，それを付加したメールの送信及びメールが改変されていないことを確認する。

4　評価の例

評価の例として，次のようなものが考えられる。

時限	学習内容・学習活動	評価規準	評価方法・評価の観点
1	○ＲＳＡ暗号についての学習	ＲＳＡ暗号の仕組みについて，自分の言葉で説明している。	プリント ［知識・技能］
	○公開鍵・暗号鍵の作成	公開鍵・暗号鍵を作成している。	提出物 ［知識・技能］
2	○ファイルの暗号化	公開鍵によるファイルの暗号化及び秘密鍵によるファイルの復号をしている。	提出物 ［知識・技能］
	○報告書の作成・提出	各種暗号方式や電子署名について自分の言葉で説明している。	プリント ［思考・判断・表現］