## 学習指導案:情報通信ネットワークの仕組み

|  |  |  |
| --- | --- | --- |
| **単元名**  情報セキュリティ |  | **内容のまとまり**  情報通信ネットワークとデータの活用 |

### 1. 単元の目標

1. 情報セキュリティの技術的な面を理解する。
2. 自宅や学校に限らず、カフェやホテルなど外出先でも安全に情報通信を行えるようになる。

### 2. 単元の評価基準

|  |  |  |
| --- | --- | --- |
| 知識・技能 | 思考・判断・表現 | 主体的に学習に取り組む態度 |
| 1. 情報セキュリティの技術的な面を理解する。 2. 暗号化と鍵の扱いについて理解する。 | 1. 情報通信サービスを利用する際に、何が安全で何か危険か、また、どのような情報がログとして残る可能性があるかを思考できる。 | 1. 情報セキュリティの発展に目を向け、人類が行ってきた情報を暗号化したり秘匿したりする方法、または解読する方法を調べることができる。 |

### 3. 指導と評価の計画

本単元の標準時間は2時間とする。授業時間の指導のねらい、生徒の学習活動及び重点、記録の有無、評価方法については次の表のとおりである。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 時間 | ねらい・学習活動 | 重点 | 記録 | 備考 |
| 1 | ○ネットワークインタフェース層のセキュリティ   * 有線LANと無線LANを題材に、ネットワーク構築には装置や経路の安全を確保する必要があることを理解させる。   ○無線LANの暗号化方式   * また、無線のような電波は傍受が容易なため暗号化を行うが暗号化方式によっては効果がほとんどないことを伝える。 | 知 | ○ | 知①: ワークシート  思①: ワークシート |
| 2 | ○共通鍵暗号方式   * 分かりやすい鍵の例として、共通鍵暗号方式から導入を行う。また、例としてシーザー暗号も取り扱う。   ○公開鍵暗号方式   * 鍵を安全に交換することが課題であることを理解させたうえで、それを実現する方法として公開暗号方式があることを説明する。   ○安全なインターネットサービスの利用   * HTTPS通信のような方法によりインターネットサービスの安全が一定のレベルで担保されていることを伝える。 | 知 | ○ | 知①: ワークシート  思①: ワークシート |

### 4. 観点別学習状況の指導と評価

#### 本時における「知識・技能」の指導と評価

本時においては、「知識・技能」の観点について、全員の記録をとる評価を行う。

1. 知識・技能:情報セキュリティと鍵の仕組みについて理解させる。

* 無線LANを題材に、通信経路を暗号化する必要性を理解させる。
* 共通鍵暗号を題材に、鍵の交換が課題になることを理解させる。
* 安全に鍵を交換する方法として公開鍵暗号方式が利用できることを理解させる。

1. 評価基準:

* ワークシートの記載などを通じて、生徒の理解を評価する。

1. 展開:

本時では、スライドに従って生徒に情報セキュリティの考え方を理解させる。

|  |  |
| --- | --- |
| 学習活動 | 評価と配慮事項 |
| 1. ネットワークインタフェース層のセキュリティ 導入として無線LANでは電波が傍受可能な点に触れ、経路を暗号化する必要があることを示す。次に、暗号化の話に触れ、鍵の重要性を示す。 2. 暗号化と鍵   シーザー暗号を題材に共通鍵暗号方式の特徴と課題を解説する。その後、公開鍵暗号方式について解説する。   1. 安全なインターネットサービスの利用   インターネットサービスを利用する際に、情報がどのように守られているかを、TCP/IPレイヤーモデルの考え方も参考にしながら、解説する。 | * 試験ではWEP暗号方式の脆弱性に触れることになると考えられるが、まずは、無線LANの傍受の行いやすさや経路を暗号化する必要があることを伝える。 * 暗号化にはアルゴリズムと鍵の両方が必要なこと、また、共通鍵暗号方式では通常、鍵を秘匿すればよく、アルゴリズムは公開されていても構わないことを理解させる。公開鍵暗号方式の理解は時間がかかるため、1コマで完璧に覚えさせるのではなく、複数回説明したほうが良いかもしれない。 * 下の層である経路だけが暗号化されていても上位層で生のデータが流れていた場合にはプロバイダーや機器の管理者には情報が閲覧される可能性がある。また、それらのスタッフが悪意を持っている場合や、そもそも攻撃者に設備を乗っ取られている可能性があるため、注意が必要となる。 |

1. 本時における「知識・技能」の指導と評価の方法:

|  |  |
| --- | --- |
| 評価 | 評価の視点 |
| 「おおむね満足できる」状況（B） | * 暗号化を行うためには鍵と暗号化のためのアルゴリズムが必要である。また、簡単な暗号化アルゴリズムは脆弱なのでセキュリティのために用いてはならない。 |
| 「十分満足できる」状況（A) | * 公開鍵暗号方式は公開鍵と秘密鍵のペアを用いた暗号化方式で、この方式を採用することで情報を安全に受け渡すことができる。また、この仕組みを応用することで電子署名も実現することもできる。 |