タイトル：ファイルの改ざんの有無をハッシュ値で確認する

学習目標：

- ハッシュ関数とハッシュ値の基本的な理解を深める。
- ハッシュ値を用いてファイルの改ざん検出方法を学ぶ。
- 実際のツールを使用して、ハッシュ値の計算と確認を行い、ファイルの完全性を自分で確認する。

ねらい：

- デジタルデータのセキュリティの重要性とデータ完全性の確認方法を理解する。
- ハッシュ関数がデータの整合性確保にどのように役立つかを実感する。
- 実世界のシナリオでハッシュ値を活用する能力を養う。

背景と解説：

- インターネット上のファイルをダウンロードする際に、改ざんされていたり破損していないことを確認するために「ハッシュ値」が用いられている。
- ハッシュ値は、任意のファイルからハッシュ関数で算出される、16進数が並んだ固定長のテキスト形式の値である。ハッシュ値は、同じファイルからは同一のハッシュ値が算出される特性を持っている。つまりファイルのハッシュ値が異なるなら、ファイルの内容に変更があったということを示している。
- そこで、そうしたハッシュ値の特性を踏まえて、インターネットにファイルを公開する際にオリジナルのハッシュ値を公表することで、元のファイルに変更や改ざんが無いことを確認することができる。

使用するツール：

- 任意の文字列のハッシュ値を求める　text_hash_conv.html
- 任意のファイルを16進数に変換する　hash_conf.html
- 16進数からハッシュ値を求める　hex_hash_conv3.html
- ２個のハッシュ値を比較

ワークの構成：

Part 1: ハッシュ関数とハッシュ値の基礎（30分）

- ハッシュ関数とは何か？
- ハッシュ値の用途と特性
- 主要なハッシュ関数（SHA-1, SHA-256）とその違い
- 簡単なデモンストレーション：文字列のハッシュ値計算

Part 2: ハッシュ値とデータの完全性（20分）

- ハッシュ値がデータの完全性確認にどう役立つか
- 改ざん検出の原理
- 実例紹介：ハッシュ値を用いた改ざん検出

Part 3: ハンズオン実習（35分）

- 実習準備：7-zipやオンラインハッシュ計算ツールの紹介
- 実習：任意のファイルに対するハッシュ値の計算
- 実習：インターネット上で公開されているファイルをダウンロードし、公開されているハッシュ値と自分で計算したハッシュ値を比較して、ファイルの内容に変更や改ざんがないことを確認
- 実習の振り返りと質疑応答