ワークショップ構成：RSA暗号化を体験しよう

タイトル：公開鍵と秘密鍵を用いた暗号化・復号化の体験

学習目標：

- RSA暗号の原理を理解する。
- 公開鍵と秘密鍵を用いた暗号化・復号化の過程を学ぶ。
- 実際のツールを使用して、メッセージの暗号化と復号化を行い、公開鍵暗号体系の実用性を自分で確認する。

ねらい：

- 公開鍵暗号体系の安全性と効率性について理解する。
- デジタルセキュリティの基本的な概念としての暗号化復号化の重要性を認識する。
- 実際のシナリオでRSA暗号化を適用する能力を養う。

背景と解説：

- RSA暗号は、公開鍵暗号体系の一つであり、秘密鍵と公開鍵のペアを使用している。公開鍵は誰とでも共有でき、メッセージの暗号化に使用されるが、復号化には秘密鍵が必要となる。この性質により、安全な通信が可能になる。
- RSA暗号は、インターネットセキュリティ、電子メールの暗号化、データの安全な転送など、多くの分野で広く使用されている。

ワークの構成：

Part 1: RSA暗号値の基礎（30分）

- RSA暗号とは何か？
- 公開鍵と秘密鍵の関係
- RSA暗号の数学的原理（簡易説明）
- 簡単なデモンストレーション：キーペアの生成

Part 2: 暗号化と復号化のプロセス（20分）

- 公開鍵を使用したメッセージの暗号化方法
- 秘密鍵を使用したメッセージの復号化方法
- 実例紹介：実世界でのRSA暗号の使用シナリオ

Part 3: ハンズオン実習（35分）

- 実習準備：模擬ツールの紹介と操作方法
- 実習：自分のメッセージを暗号化し、他の参加者に復号化させる
- 実習：他の参加者から受け取った暗号化メッセージを復号化
- 実習の振り返りと質疑応答

使用するツール：

- RSA暗号化によるファイルの暗号化・復号化　　file2RSAcrypt.html
- RSA暗号化によるメッセージの暗号化・復号化　　RSAcrypt2.html
- 公開鍵秘密鍵キーペア生成　　RSA_keypair.html


ja-JP