情報処理 講義録	コース・講義等	情報処理安全確保支援士	科目	専門知識対策講義	回数	1

配布物	★テスト類：[ ]	講師	根岸 先生
	★その他の配布物1：[ ]		
	★その他の配布物2：[ ]		

黒板内容

暗号技術

- Ⓒ … 守秘
- Ⓘ … 改ざん検証，認証 ← 本人確認 / 本物のデータかの確認
- Ⓐ … 可用性を損なう攻撃
  - マルウェア
  - DoS攻撃

プリント

③ 暗号技術の基本用語

鍵：数値（128bit ～ 4096bit）（2進数）← 鍵ファイルで扱う（目安）

パスワード：単語 英数字，記号，8～16文字

パスフレーズ：文（スペースもOKなことが多い）20～40字（スペース）

↓

〈人の頭で覚える〉

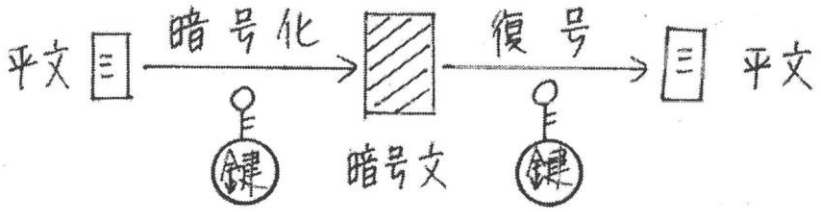
・鍵ファイル [数値] → ファイルにロックをかけておく

= パスワード / パスフレーズ を利用してロックする

この講義録の著作権は、TAC株式会社または権利者に帰属しており、当社に無断で複製、改変、転載、転用、インターネット上にアップロードする等の著作権を侵害する行為は法律によって禁止されております。

TAC Wセミナー

③暗号技術の基本用語



・平文(plain text)：誰でも内容を判読できるデータ
・暗号文(cipher text)：特定の人だけが内容を判読できる
・暗号化(encrypt)：鍵を利用して平文を暗号文に変換する
・復号(decrypt)：鍵を利用して暗号文を平文に変換する
・鍵(key)：暗号化，復号に利用する数値
・鍵の危殆化：鍵が第三者に漏洩するなどして，意味のない物になってしまうこと
　→ミス：本人のミスでばらしてしまった
　→攻撃：フィッシング，推測された，解析された

【鍵を推定する攻撃例】
・選択平文攻撃：
　攻撃者が指定した平文を暗号化させて，暗号文と平文の関係から鍵を推定する
・既知平文攻撃：
　http:// などのよく使われる文字列がどのような暗号文になっているのかから鍵を推定する
・**サイドチャネル攻撃**：動作を観測して鍵を推定する
　→電力解析攻撃，タイミング攻撃，故障利用攻撃