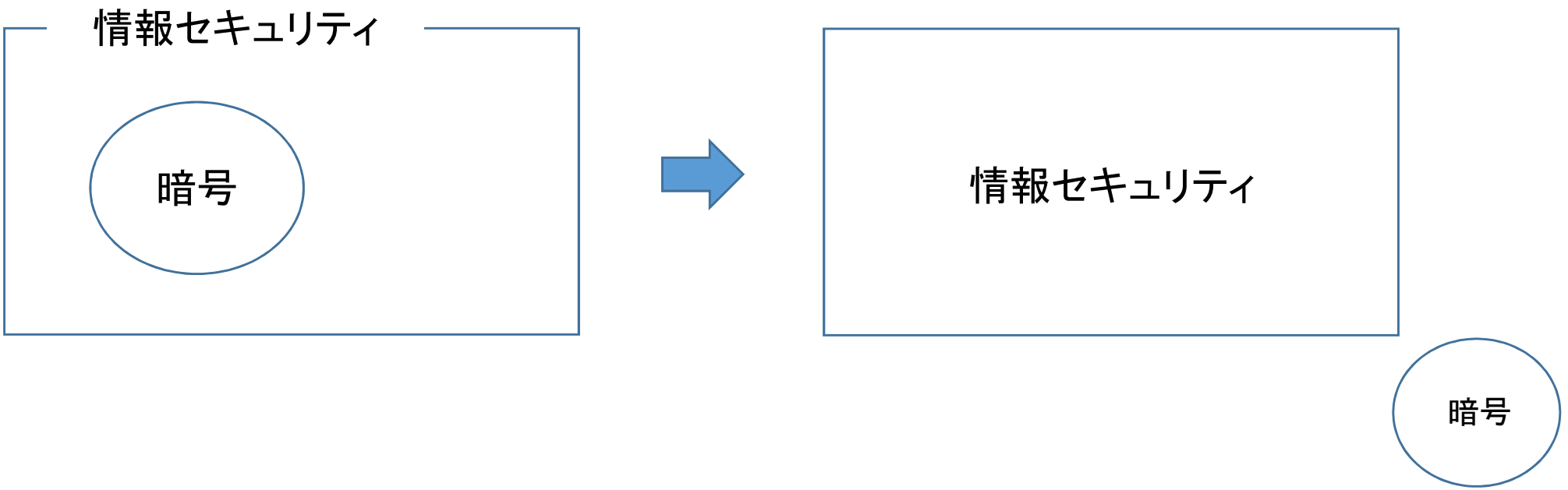
暗号・認証分科会活動報告

内容

1　活動背景
2　成果目標
3　分科会活動
4　悩み
5　成果報告
6　今後について

活動背景

・近年,「暗号などの理論的な分野」と「情報セキュリティ分野」の乖離が起きている



・また, セキュリティ自体は広がり続け, 人口も増えているが, 暗号の専門家はむしろ減っているように思われる.

活動背景

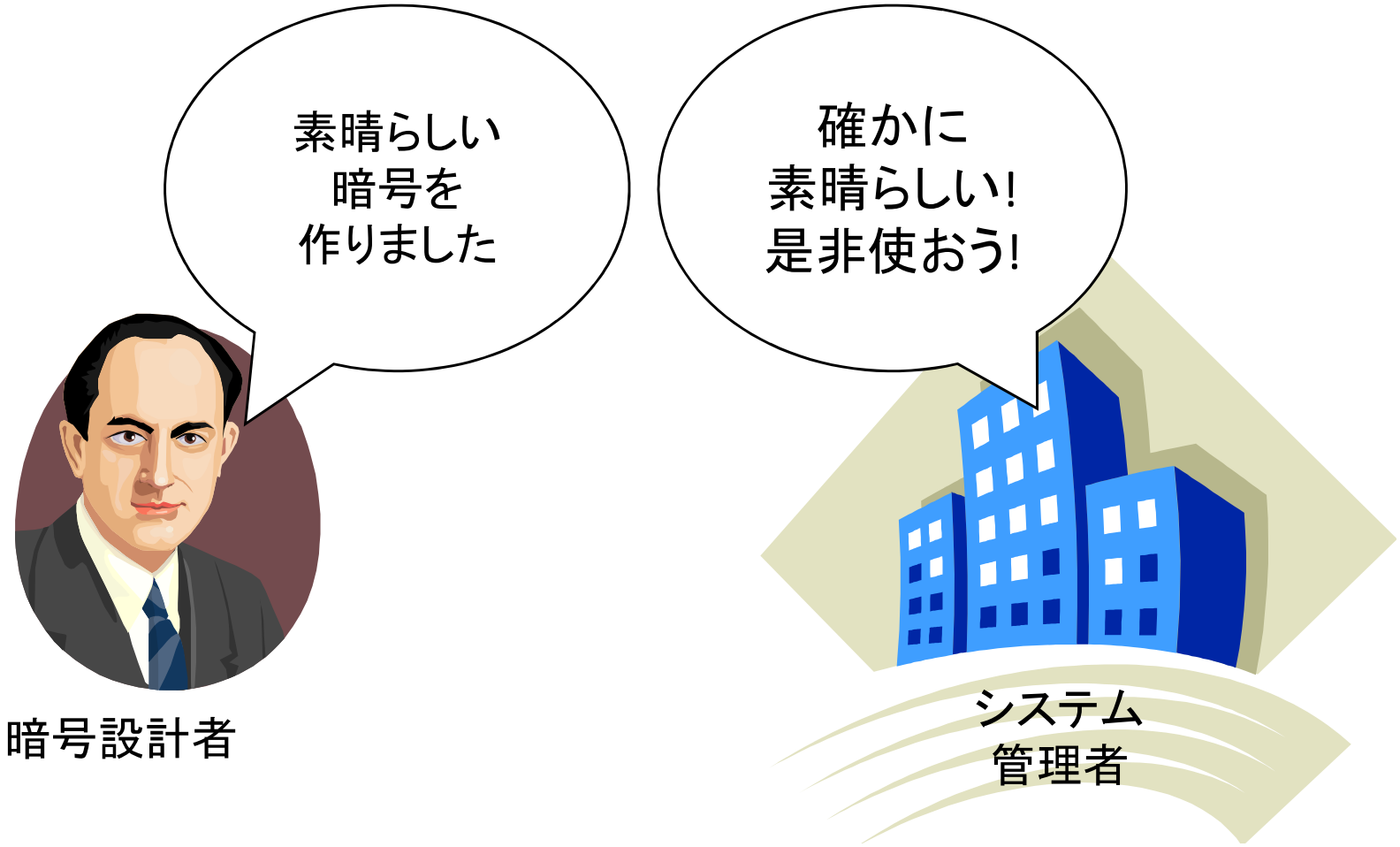
・その原因として,
暗号理論自体が独特な手法があり, 他分野の人には難しいと思われる事などが挙げられる.

・しかし, 暗号理論を理解することで
(1) 暗号理論の考え方は情報セキュリティに関して本質的な部分が多い. ⇒ それを理解することはセキュリティ技術の理解には大いに役立つ
(2) 他の分野との組み合わせることで更なるセキュリティ分野の発展も起きるのでは

などメリットも考えられる

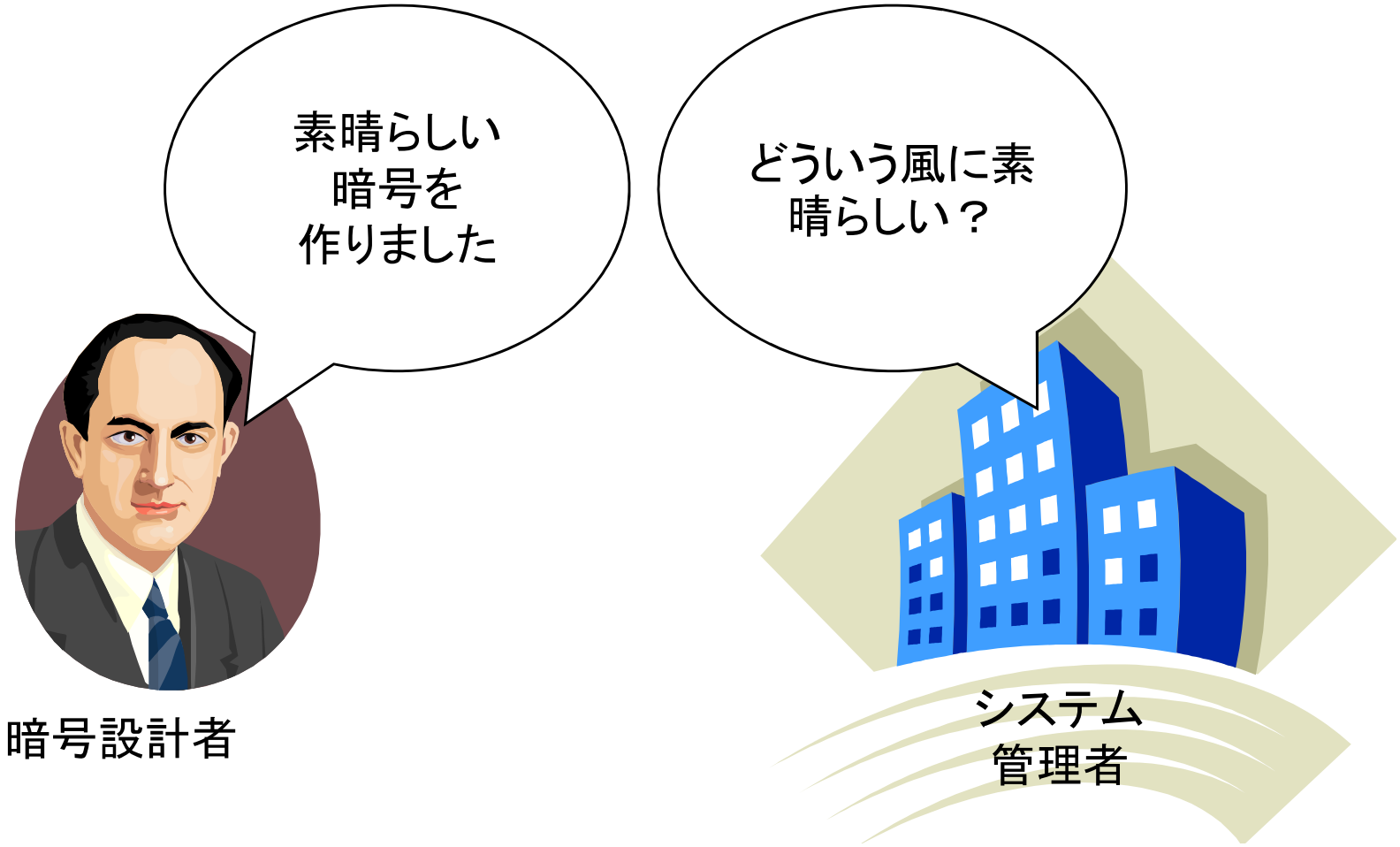
活動背景

理想



活動背景

現実(1)

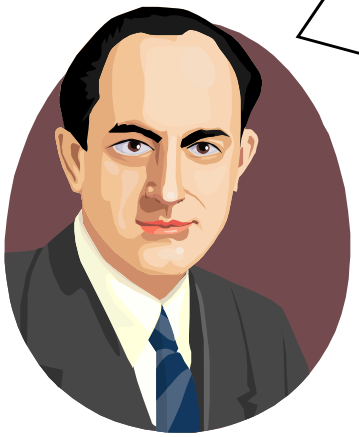


活動背景

現実(1)

(S,m)-BDHE Sum判定問題が困難であり、疑似ランダム関数が存在すれば、適応的攻撃者にも安全。

…

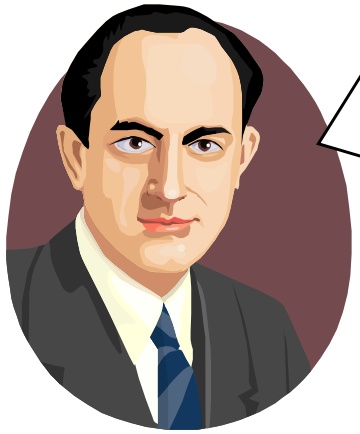


暗号設計者

システム管理者

活動背景

現実(2)



真に安全な
暗号設計者

(S,m)-BDHE Sum判定問題が困難であり、疑似ランダム関数が存在すれば、適応的攻撃者にも安全。

真に安全でない
暗号設計者

?????????
?????????
?????????
?????????
?????????
???????

識別できない…

システム
管理者

活動背景

・どんなに素晴らしい成果であっても、それが他の人に伝わらなければ、何もしていないのと大差がない

・暗号や認証など理論的な分野を一般人, (専門でない)技術者に理解させられるようにならなければならない.

人に情報を「正確に」「分かりやすく」
伝えられるようにならなければならない

人に情報を伝えるステップ

(1) 我々を取り巻く状況を正確に伝える
(2) その状況において不足しているものが何かを伝える
(3) それが不足していることでどのような問題が起こっているのか伝える

(4) その不足を解消させる実物を見せる
(5) その実物を得た事でどのような利益があるのか伝える

論文の構成(1)

・はじめに

- 研究対象を取り巻く状況を広い視点で説明する
- 何が不足しているのかを説明する
- それが不足しているためにどんな問題が生じているのか説明する
- その不足を解消する提案手法の概要を説明する
- 提案手法の校歌を説明する
- 類似した別の手法(関連研究)との違いを説明する

論文の構成(2)

- 提案手法の詳細
  - 問題を解決するための大雑把なアイデアを説明する
  - そのアイデアで上手くいきそうな理由を説明する
  - そのアイデアに基づく具体的な提案手法を記述する
  - 提案手法が上記アイデアで正しく具現化している根拠を説明する

論文の構成(3)

・提案手法の評価

- 提案手法が「はじめに」で提示した問題を解決していることの根拠を伴った説明をする
- 性能評価を行う
- 他の関連する手法との比較を行う

・まとめ

- 論文全体の主張を簡潔にまとめる
- どのような問題がどのように解決されたかを説明する

成果目標

一般的な論文の構成(1)～(3)に沿って,
第三者にそのものの「凄さ」「素晴らしさを」を正確に伝えられるようになる.

分科会活動

- 産総研 花岡悟一郎先生指導の下,
  - スライド作成, 発表
  - 論文執筆

  の練習を行い,「人に伝える技術」の向上を図った.

- 「情報セキュリティ特別演習」にて実地

前期

4/13　4/20　5/11　6/1　6/15　6/22　7/6

後期

9/21　10/5　11/9　11/16　12/14　12/21　1/18

重要視された点

(1) 我々を取り巻く状況を正確に伝える
(2) その状況において不足しているものが何かを伝える
(3) それが不足していることでどのような問題が起こっているのか伝える

(4) その不足を解消させる実物を見せる
(5) その実物を得た事でどのような利益があるのか伝える

前期の活動

- 「自分の好きなものの」をテーマに,
  (1) スライドを用いたプレゼンテーション
  (2) 論文執筆
  を行い, 互いにそれをレビューし合った

- テーマの例

  Xperia ear duo (イヤホン)
  PCゲーム

  など

後期の活動

- 「情報セキュリティ技術」をテーマに,
  (1) スライドを用いたプレゼンテーション
  (2) 論文執筆
  を行い, 互いにそれをレビューし合った

- テーマの例

  AES暗号

  Physically Unclonable Function

  など

悩み

・暗号認証分科会最大の悩み

「成果報告がしづらい」

・去年度までは調べた情報セキュリティ技術の紹介
→ 反応は微妙. 批判があった事も

・「技術が向上した」事を伝える事は難しい
→「効果のある活動をしている」事を伝えよう

成果報告

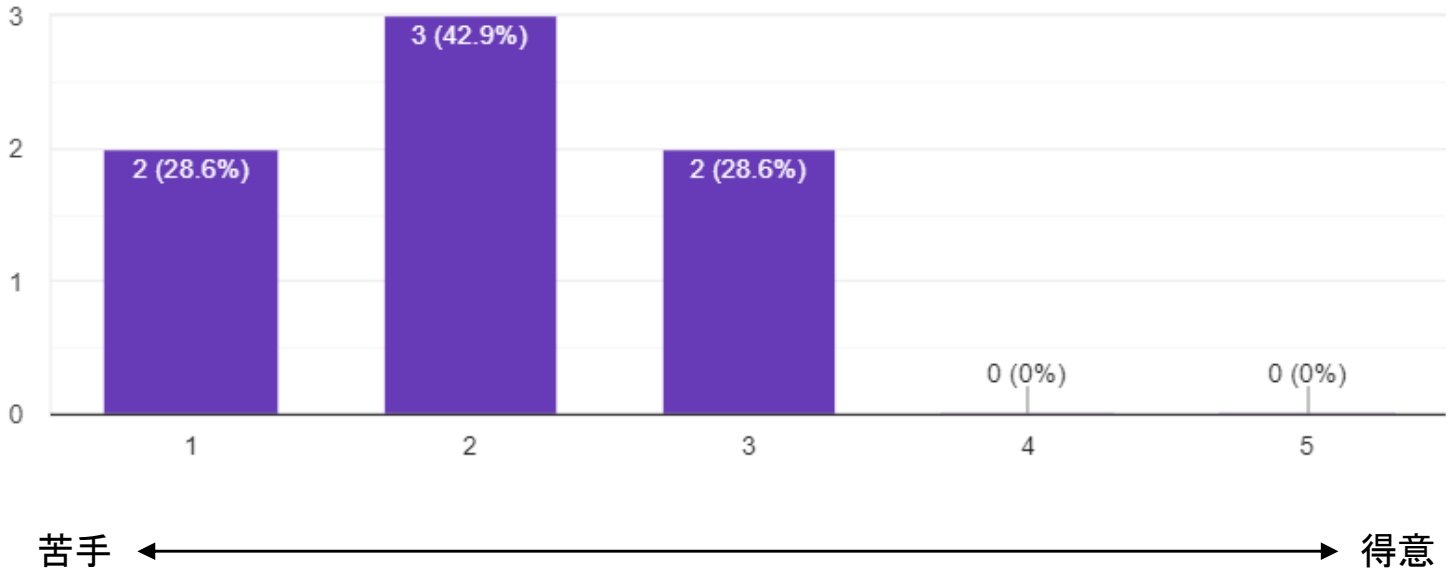
・この活動内容(プレゼン, 論文執筆練習)についてのアンケートを行った

・回答者は7名
　暗号認証分科会に所属している人
+ 情報セキュリティ特別演習履修者

・「技術は向上したか」「学んだ事は今後役に立ちそうか」などこの活動の意義などを問うた.

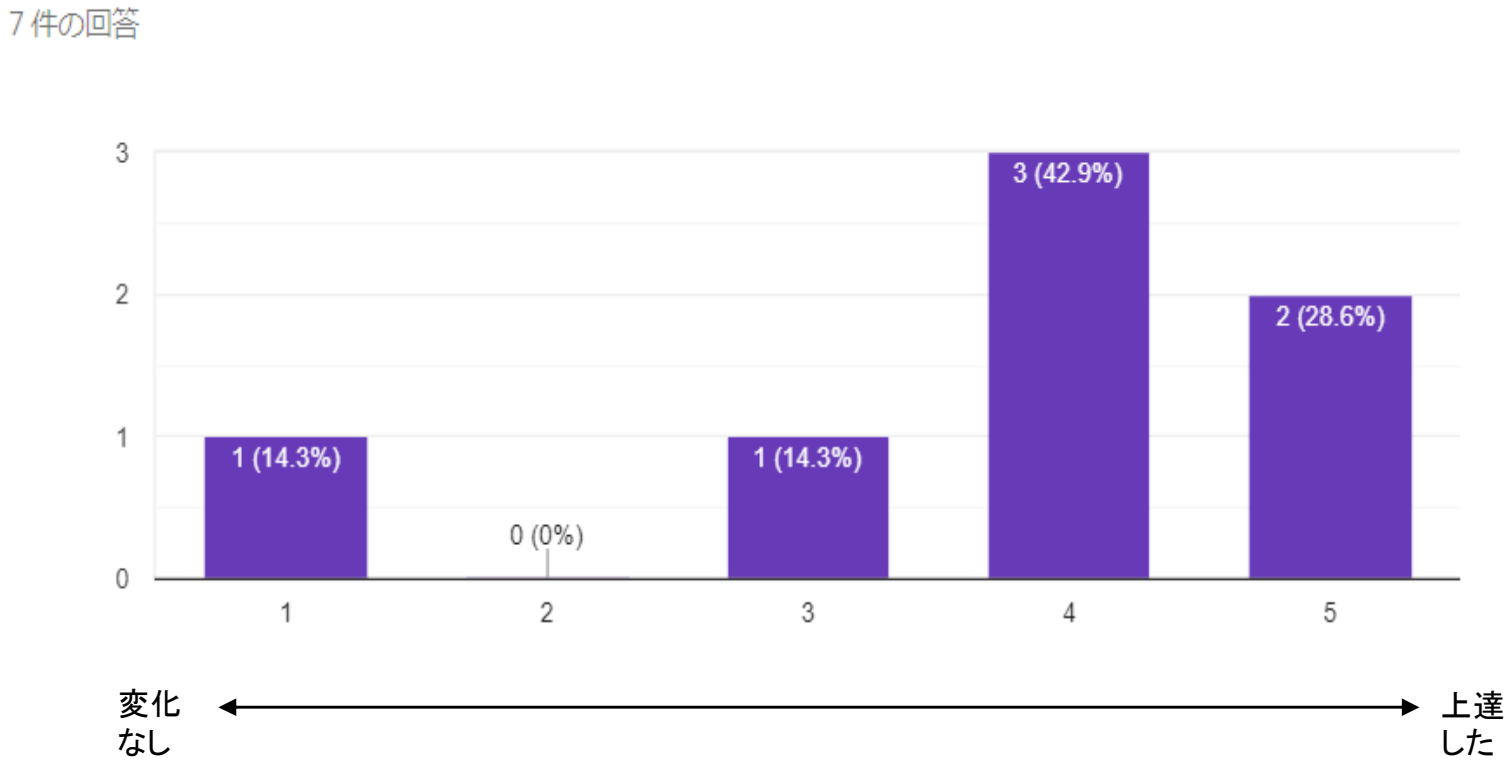
アンケート(1)

受講前, 人前で発表するのは得意でしたか



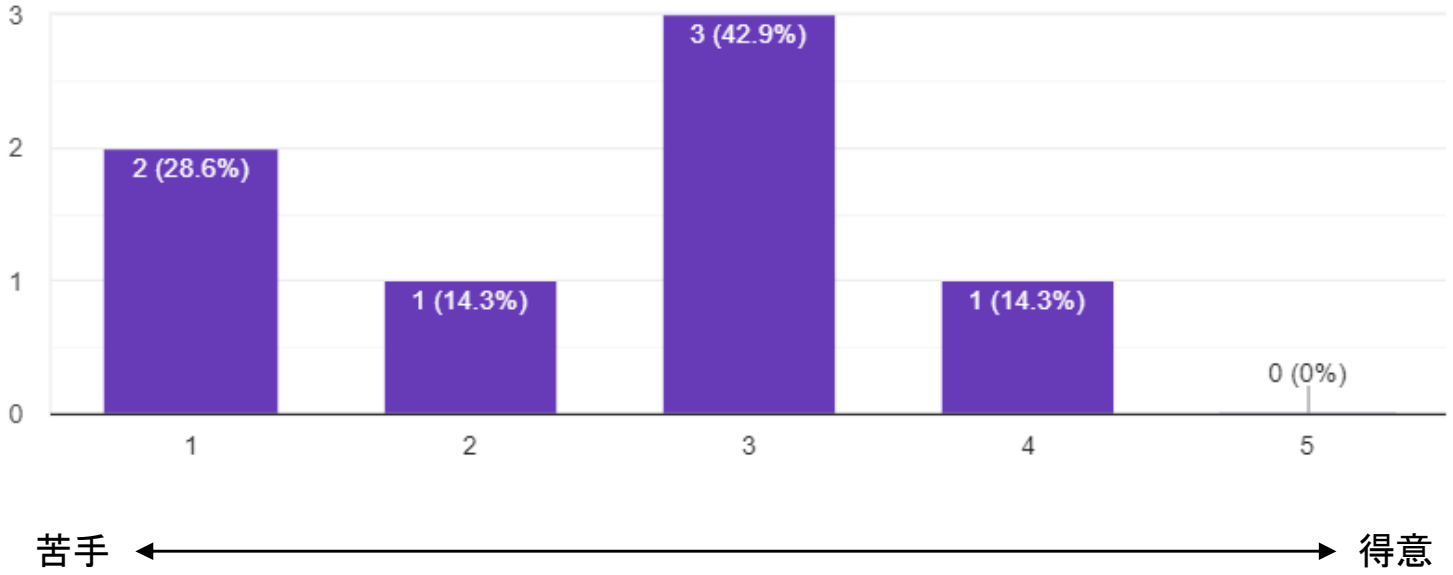
アンケート(2)

受講後, 発表は上達しましたか



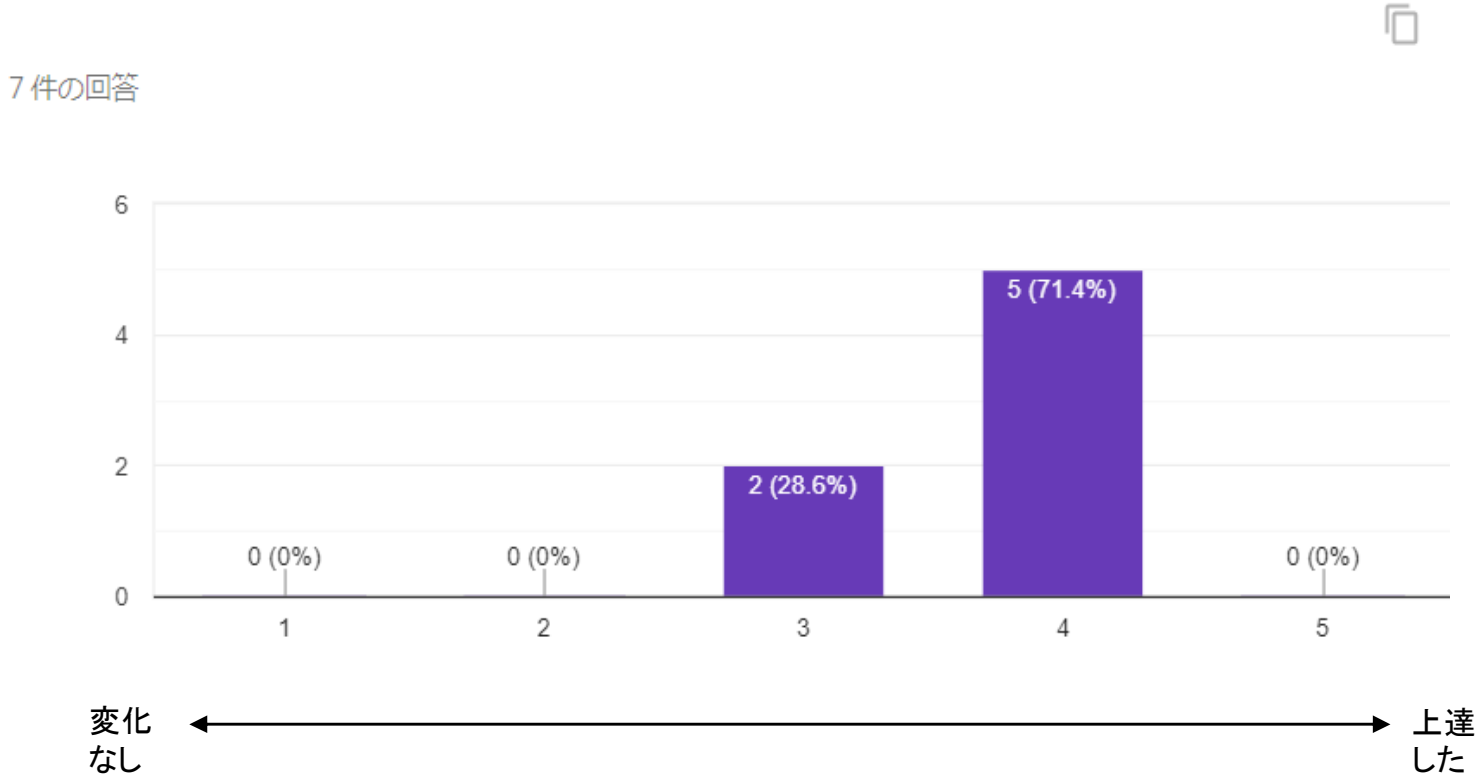
アンケート(3)

受講前, 論文の執筆は得意でしたか



アンケート(4)

受講後, 論文の執筆は上達しましたか



アンケート(5)

・発表, 論文執筆共に過半数以上が この活動で上達した事を実感 → 効果のある活動

講義を通して得られたもの

論文執筆のコツ・プレゼン資料作成のコツ
論文やプレゼン資料の構成力
自分には発表が不可能であることを理解した
聞き手に必要な情報が伝わりやすいプレゼン、論文の作り方。発表者に対して質問するポイント。
図表を用いると初めての人にでも伝わりやすいが、文書のみの場合は工夫が必要である。また、結論を最初に書く、問題提起と解決の対応をしっかりとるなど論文を書く上でのテクニックを身につけられた。
情報セキュリティに関する知識
資料作りで気を付けるべき点を学べた

アンケート(6)

・学んだ事を研究室やインターンでの資料作りに活かせた, などのコメントも

この講義を受ける事の最大のメリットは何だと思いますか
伝わりやすい論文執筆のノウハウを学べること。
他人の発表を指摘し，また他人に指摘されることで自分になかった視点が得られた
発表の練習になる
問題→提案→評価の発表の大まかな流れを掴めること。
発表のフィードバックをその場で複数の人たちから貰え、回を重ねるごとに改良する体験ができること。
情報セキュリティに関する知識を身につけられること
資料作りや発表の技術を学べる

来年度の活動について

・活動内容, 成果目標は現状のまま
→ 就職してからも使うであろう技術. 訓練をしていて損はない.

・成果報告会での発表方法は工夫が必要

・発表, 論文執筆の苦手なM1の方は是非来年は暗号認証分科会に

余談

「最も良問を用意した分科会はドコ？ 研究分科会〇×クイズオンラインチャレンジ」1位

暗号・認証分科会

（獲得票率 37%）