

一般情報教育でのCSアンプラグドによる 大学生の意識と知識の変化 —公開鍵暗号に関わる教材を通して—

布施泉^{†1} 西田知博^{†2}

概要: 本稿では、公開鍵暗号に関わるCSアンプラグドの実践による学習者の意識と知識の変化について報告する。北海道大学の一般情報教育の授業の中の取り組みとして、事前調査、事後調査、および学習者の実践時における意識調査等を行った。これらの調査結果を踏まえ、大学におけるCSアンプラグドを用いた効果的な学習構成について考察する。

キーワード: CSアンプラグド, 公開鍵暗号, 一般情報教育, 意識変化

Changes in Awareness and Knowledge of University Students by CS Unplugged in General Information Education - Through a practice on Public Key Encryption -

IZUMI FUSE^{†1} TOMOHIRO NISHIDA^{†2}

1. はじめに

情報化に関わる技術は、私たちの生活に大きな変化を及ぼすものであるが、技術が複雑に組み合わせられ、また詳細化されていく中で、利用者は、その成果である機器やツールの利用が主となり、ブラックボックス化された技術には、意識が及ばないように思われる。

近年、個人のニーズに合わせたスマートなサービスの提供が進められている[1]が、当該のサービスには、一般に、多種多量の利用者データが用いられることが多い。例えば、位置情報や各種履歴情報等のデータは、どのような場合、どのような方法と対象であれば、利用が可能であるか等、社会として様々なリスクと便宜等を考慮して、運用に関する検討を進めねばならず、法の改正等も進められている[2]。

大学における一般情報教育では、情報技術が情報社会に及ぼす影響を踏まえ、情報技術の基礎となる情報科学の教育を含め、総合的に情報学の授業を設計する必要がある。現実に使われている技術の詳細は分からなくとも、その基礎となる情報科学の基本原則や仕組みの理解は必須であり、大学の一般情報教育では、より良い社会の構築をめざし、

情報化の可能性と限界を検討させることが欠かせないと考える。

本稿では、情報をネットワーク上でやり取りする際の、最も基本的かつ重要な仕組みの一つである、暗号化通信の仕組みについて習得させることを目指して行った実践について報告する。北海道大学での実践事例を報告するが、これまでは、暗号化通信の仕組みを習得させる方法として、大きく以下の実践を行ってきた。

- ・情報倫理デジタルビデオ小品集（公開鍵暗号は縁の下
の力持ち）によるビデオ視聴[3]
- ・ビデオと同じシナリオを持つ漫画教材の確認
- ・Excel等を用いた関連の実習と公開鍵暗号に関するレ
ポート提出等

上記は、特にRSA暗号による公開鍵暗号の仕組みと電子署名について理解させるための実践であるが、RSA暗号では、素数の積とべき乗・剰余を用いた数学的な関係性による性質を用いており、文系を含む学習者に、その本質をそのまま理解させることは一般には難しい。また、結果として得られた知識の習得状況はもとより、学習者への技術に対する好奇心といった意識面への働きかけについても、現在、十分な確認がなされていない。そこで本稿では、体験的な活動により、学習内容の理解促進を図るCSアンプラグドを、公開鍵暗号の原理を理解することを目的に取り上げることとする。CSアンプラグドの実践が、大学における

^{†1} 北海道大学
Hokkaido University.

^{†2} 大阪学院大学
Osaka Gakuin University

学習者にどの程度の興味・関心を与えることができるのか、また結果としての知識習得状況とその持続性等について焦点を当てて報告を行うこととする。

2. 学習の前提

北海道大学では、一般情報教育の授業が2科目用意されており、前期2単位（情報学Ⅰ）は必修、後期2単位（情報学Ⅱ）は選択の科目である。本報告のCSアンプラグドの実践は、2015年度の後期（2単位）15回の中の1回を用いて行ったものである。本章では、その学習の前提として、2015年度前期の情報学Ⅰで行った公開鍵暗号についての学習の流れについて紹介する。

(1) 情報学Ⅰでの公開鍵暗号に関わる授業内容

情報学Ⅰでは、公開鍵暗号を2015年度に初めて取り上げた。それ以前は、主に情報学Ⅱで扱う対象であった[4]。情報学Ⅰは、コンピュータ教室で行う実習中心の授業である。各教室には20名程度の学生が割り付けられており、TA等が各教室にて学習者に対応し、担当教員が全体統括する形で、6-10の複数教室で並列に授業が進行する。授業は、必修で、統一のカリキュラムで行われる。公開鍵暗号は、第14週で取り上げた。学習の流れは以下の通りである。

【授業時】

- ・ビデオ「公開鍵暗号は緑の下の力持ち」を視聴する
- ・ビデオの内容で理解したことを評価シートに記述する
- ・関連の実習を行う

【次週までの課題】

- ・公開鍵暗号に関わる課題を提出する
- ・配布されている関連の漫画教材（ビデオと同シナリオ）を復習しておく

【次週以後の確認】

- ・公開鍵暗号に関わる漫画教材の閲覧確認と、そこで理解したことを記録シートに記述する
- ・情報倫理に関わる小テストで、公開鍵暗号に関わる設問を取り入れ、その習得度合いを確認する

(2) ビデオ「公開鍵暗号は緑の下の力持ち」の内容

参考文献[3]のビデオは、以下の流れで、公開鍵暗号についての説明を行う。本ビデオ教材は本来短編であるが、公開鍵暗号のビデオは、内容が難しく、本小品集の中で最も長い10数分の教材となっている。以下は解説でのビデオの流れである。

- ・共通鍵暗号と公開鍵暗号についての説明
 - シーザー暗号、暗号機の利用等、共通鍵暗号の概略説明と、公開鍵暗号の概念的な考え（暗号化の鍵と復号の鍵を分離して考える）の説明
- ・認証局の役割についての説明
- ・電子署名についての説明
- ・RSA暗号の概略の説明

実際に簡単な素数を用い、べき乗と剰余計算を行い暗号の数と元の数の関係性を説明する

ビデオの視聴後、「公開鍵暗号の仕組みで理解したことを具体的に記す」「電子署名の仕組みで理解したことを具体的に記す」の各設問に対する解答を授業時に提出させた。

(3) 関連実習の内容と理解した内容の記述

前述の学習の後、Excelを用いて暗号化と復号の確認を行った。図1は、Excelの練習シートの例（シーザー暗号）である。シーザー暗号、単一換字暗号、RSA暗号の順にシートで、簡単な変換を学習者に実際に行わせた。

シーザー暗号:完成形						
前からの数を知っている	暗号化でずらす文字数	2	←ここを変更し、暗号文が変			
送信者が送ろうとする文	平文	A	P	P	L	E
		↓	↓	↓	↓	↓
	平文のASCIIコード	65	80	80	76	69
	暗号化	67	82	82	78	71
		↓	↓	↓	↓	↓
実際に通信される文	暗号文	C	R	R	N	G
		↓	↓	↓	↓	↓
	暗号文のASCIIコード	67	82	82	78	71
	復号	65	80	80	76	69
		↓	↓	↓	↓	↓
言われた文から得られた文	復号文	A	P	P	L	E

図1 暗号に関する理解促進のための実習例

(4) 課題内容

次回までの課題として、「公開鍵暗号システムの長所と短所等について調査し、それが現在の情報通信において広く使われるようになったと考えられる理由を考察する」を課した。また、次の授業開始時に、公開鍵暗号に関わる漫画教材の確認によって、具体的に理解した内容を記載させ、そのファイルをその場で提出をさせた。さらに、公開鍵暗号を含む情報倫理に関わる内容の小テストを行った。

(5) 前期授業による結果の概要

上記の流れの授業で、ビデオ視聴後の学習者の理解した内容の記載例を示す。

- ・公開鍵暗号の仕組みで理解したこと：送ってもらう鍵を公開して、受け取る鍵を秘密にする／ナップザック暗号、RSA暗号など、様々な種類がある、等
- ・電子署名の仕組みで理解したこと：秘密鍵の所有者だけが作れるメッセージを用いた電子的な署名の仕組み、等

今回の小テストでは、公開鍵証明書を問う文章で、空欄を埋める設問、RSA暗号による暗号化に関する設問（公開鍵で暗号化されたデータを復号するための鍵、秘密鍵で暗号化されたデータを復号するための鍵を、公開鍵、秘密鍵、共通鍵の3択から選択）を行った。後述するCSアンプラグドの実践者の結果としては、公開鍵で暗号化されたデータを復号するための鍵として、秘密鍵を選択した割合は、91%（21名/23名）であったが、電子署名に関しては約6割の正解率、公開鍵証明書に関しては約7割の正解率であ

った。

学習者は、この段階では、公開鍵で暗号化したものは秘密鍵で復号するといった RSA 暗号の基礎的知識は、概ね身につけているように思われる。

3. CS アンプラグドの実践と各種評価結果

本章では、2015 年度後期の情報学 II の授業で行った CS アンプラグド[5]の実践を報告する。一部、情報学 I を行っていない学習者がいるが、殆どは、前期で情報学 I を履修している。

3.1 対象者と実施日

本実践における対象者とスケジュールを表 1 に示す。

表 1 本稿での CS アンプラグドの実践の流れ

対象者	2015 年度の一般情報教育科目「情報学 II」の中で、第一著者が担当する一コマを履修している者 24 名（うち 22 名は 2015 年度の情報学 I の履修者）
11 月 18 日	事前知識の調査 CS アンプラグドの実践 実践に関する意見・感想
11 月 25 日	小テストの実施
12 月 16 日～1 月 5 日	小テスト返却、冬休み中に内容を復習して再提出するよう指示
2 月 3 日	確認テストの実施

3.2 事前調査

11 月 18 日、CS アンプラグドの実践を行う前に、公開鍵暗号に関する学習者の知識の程度を確認した。2 章で述べた通り、殆どの学習者は、7 月下旬に同内容を学習している。前期授業履修者における公開鍵暗号の仕組みの理解の程度について 4 択で聞いた結果を図 2 に示す。

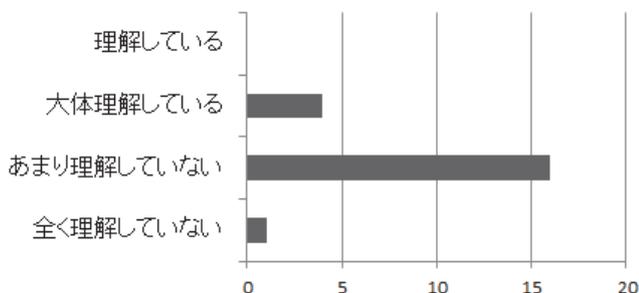


図 2 公開鍵暗号の仕組みについての理解度合い (4 択)

また、公開鍵暗号の特徴を箇条書きであげさせた。下記のような記載があった。

「大体理解している」回答者の例：暗号化と復号化で二つの対になっているカギを用いて一方を公開する方式

「あまり理解していない」回答者の例：公開されている鍵で暗号化をして、秘密にしている鍵で解読する。鍵の管理をしている機関がある。／暗号に暗号をつけることでしたっけ？学んだのですが、覚えていません。

「全く理解していない」回答者の例：便利な暗号

学習の定着という点においては、うろ覚えになっている学習者が多い印象を受ける。

3.3 CS アンプラグドの実践

授業は CS アンプラグドの教材[5]のうち、“The Peruvian coin flip—Cryptographic protocols”と“Kid Krypto—Public-key encryption”（日本語版[6]では「ペルーのコイン投げ」「子ども暗号」）を題材として行った。授業は第二著者が主となって行い、第一著者と一名の TA が補助した。

授業の前半では、[5]のコイン投げワークシート（図 3）を用いて、サッカーの試合地を決めるコイントスを遠隔地間で電話を使ってズルができないように実施する「ペルーのコイン投げ」を行った。このアクティビティでは、コインをトスする側が 6 桁の 2 進の数を図 3 の最上段に入力として書き込み、AND/OR の演算を行って求められた最下段の出力を相手に伝える。相手側は入力 1 の数が偶数ならば 0(裏)、奇数ならば 1(表)として裏表をあてる。このアクティビティを 2 人一組でコイントスする役割を交代して実施する。その後、「本当にズルはできないのか？」ということを考えさせた後、入力と出力の一覧を使って 1 対 1 に対応していないことを示し、一方関数について説明した。

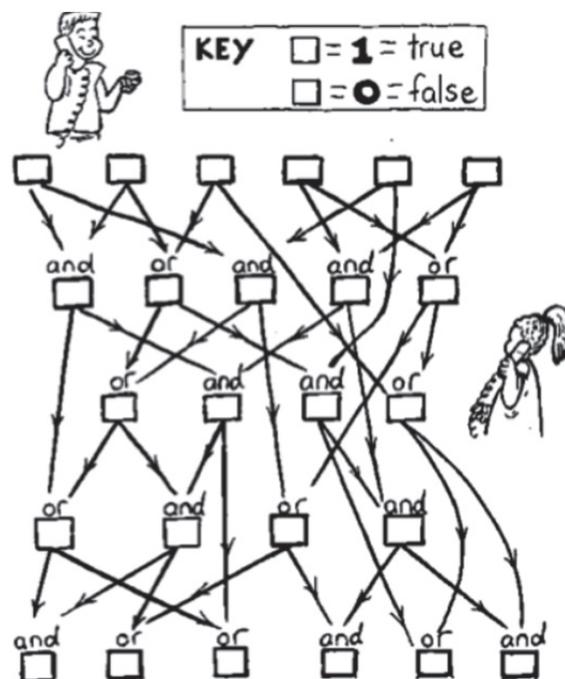


図 3 コイン投げのワークシート

授業の後半ではまず、[5]のアイスクリームワゴンのワークシート（図 4）を用いてワゴンの配置問題を考えさせ

た。図4は観光都市の地図という設定で、線は通り、点は交差点を表す。ここで、ワゴンが交差点でアイスクリームを販売するとしたとき、どの交差点に居ても隣の交差点まで歩けばアイスクリームを買え、かつ、台数が最小となるようなワゴン配置を考えさせた。これは、支配集合を求める問題であり、NP 困難であることを説明した後、図5左のようにワゴンの配置(支配集合)を決めた上で右のような地図を作成するのは、ワゴンを置いていない交差点を結ぶことによって簡単に作成できることを説明し、実際に作ってもらった。その上で、元の値から結果を計算することは容易でも、結果から元の値を求めることは非常に困難な一方関数があることを説明した。

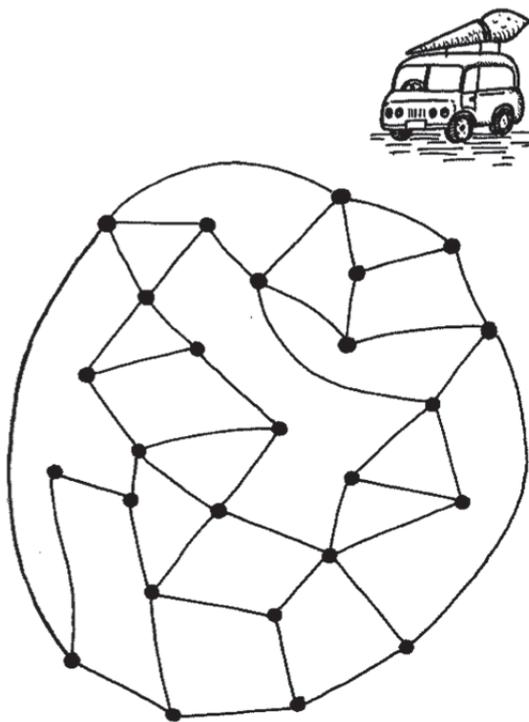


図4 アイスクリームワゴンのワークシート

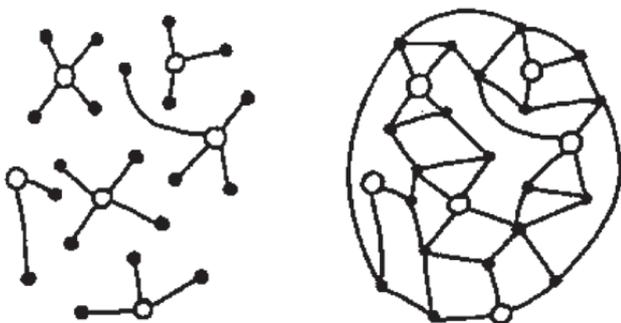


図5 地図の作成

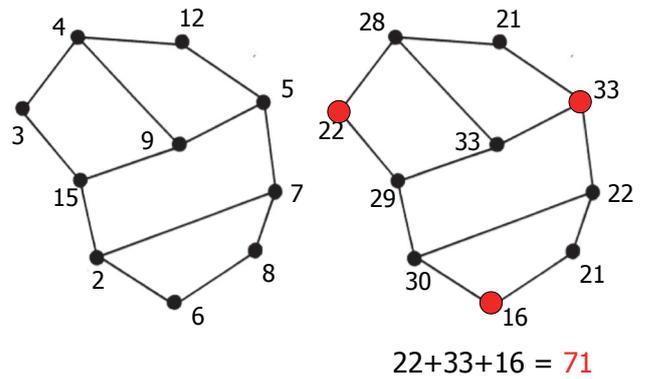


図6 秘密の数の伝達

最後に秘密の数をこの地図を使って伝達できることを説明した。秘密の数(図6の例では71)を伝達するためには、図6左のように地図の各交差点に数を、すべて合計すると伝えたい数になるように割り当てる。その後、各交差点で自分の数と線がつながっている交差点の数を足しあわせたものをそれぞれの交差点がもつ数として図6右のように割り当てた地図を相手方に伝える。この地図は、アイスクリームワゴンを置く交差点がわかっているならば、その数を足せば(図6の例では $22+33+16$)、伝わってきた秘密の数(71)を求めることができる。ここで、地図が公開鍵、ワゴンの位置が秘密鍵と考えることができることを説明する。公開鍵の地図をさらに複雑にし、秘密の数を伝達する側が各交差点に数を割り当てて伝えることによって、秘密鍵(ワゴンの位置)を知る相手先はその数を簡単に解読できると、ワゴンの位置を求めることが困難であるので、それを知らない傍受者は秘密の数を解読することが困難であることを説明した。

3.4 授業後の学習者の反応

学習者に、実践後に記載させた感想の一部を抜粋して紹介する。

- ・アイスクリームワゴンと公開鍵暗号の対応関係がちゃんと理解できなかった。でも、楽しかったです。
 - ・「逆算するのがとても難しい」ってことが暗号化で大事なことだとよくわかった。体験できたのが楽しかった。
 - ・今回の授業内容については、大体は理解できたように思う。様々な種類のゲームができて、とても面白かった。
 - ・単純にパズルを解く楽しさがあった。そればかりでなく公開鍵の例として非常にわかりやすかったので、今までよく理解できなかった公開鍵の仕組みが簡単にイメージできるようになった。
 - ・暗号化に関して、鍵がなければ復元が難しいとされているが、時間があれば破られるということも理解した。
 - ・プリントが配られて内容を見たときは一体暗号と何の関係があるか全く分からなかった。しかし解説を聞くと一つ一つが暗号とつながっていて興味深かった。
- 等、CS アンプラグドの実践については、学習者は意欲的に

取り組み、興味・関心を喚起したことが分かる。

3.5 翌週の小テストの実施と結果

3.4 の実践の翌週に小テストを行った。授業の前半部分全体が対象であり、公開鍵暗号に関わる箇所は、その一部である。公開鍵暗号については、ほぼ前期の小テストと同様の内容についての出題を行ったが、選択肢からの選択ではなく、空欄を自由記述で埋めるようにさせた。なお、本設問は、小テストの後半に配置された関係で、時間がなくて解けなかった学習者がいた可能性もある。

設問は以下の通りである『A から B へ、インターネットを利用して安全にデータの送受信を行いたい。A が送信者、B が受信者である。公開鍵のシステムを使う際、具体的にどのような手順となるか。以下の「 」に適切な語句を入れる。(1)A は B の「 」鍵を入手する。(2)A は B の「 」鍵を使って、データを暗号化し、B に送信する。(3)B は、A から送られたデータを「 」鍵で復号する。』それぞれの正答率は、(1)92%、(2)63%、(3)67%であった。

3.6 小テストの返却と振り返り

学習者に 3.5 の小テストを返却し、冬休み中に復習するように指示をした（復習内容は、当然ながら公開鍵暗号以外のものを含む）。

3.7 授業終了時の確認テスト

3.5 の小テストは、時間的な制限で解くことができなかった可能性があるため、2月3日の確認テストでは、授業の最初にそれだけの問題で確認を行った。学習者の理解の程度の詳細を確認するため、確認テストでは、A ショップ（ネットショップ）と A ショップを利用する 3 名（B, C, D）の利用者を設定し、各利用者のカード情報を A ショップに送るために、どのように鍵のやり取りを行うかを回答させた。B, C, D から A ショップに送る際に使う鍵、A ショップが利用者から送られたデータを復号する際に使う鍵をそれぞれ回答する設問であり、回答は 6 項目から構成される。全てを完璧に正解した学習者は 7 名、更に、完全正解ではないが、内容をきちんと理解していると思われる学習者は 2 名いるが、残りの学習者は何らかの間違いをしていた。

4. 考察

3 章における実践と各種の確認・評価結果を受け、本章では、これらの実践についての考察を行う。2 章では、2015 年度前期の授業終了時の小テストで、約 9 割の学習者が、公開鍵で暗号化したデータの復号には秘密鍵を使うことを選択する設問に正解したと述べた。しかしながら、その知識の定着率はさほど高くはなく、数か月後の 11 月の実践時には、内容の詳細（公開鍵と秘密鍵の関係性等）を失念している学習者が多かった。但し、その事前調査によると、2 種類の鍵（公開鍵、秘密鍵）が存在することは、概ね記憶

していたようである。

時間の経過とともに忘却することは、ある程度は避けられないものではあるが、学習の構成や内容等を考慮することでその割合を下げることはできないだろうか。3 章の CS アンプラグドの実践に関する事前テスト、小テスト、確認テストにおける回答内容を学習者毎に確認すると、事前テストで、公開鍵暗号の仕組みを「大体理解している」と回答した 4 名のうち 3 名は、最終の確認テストでも完全に正解をしている。この 4 名に対しては、CS アンプラグドの実践は、認識の確認と強化につながっていると言える。確認テストを完全正解した 7 名のうち、残りの 4 名は、事前テスト時には「あまり理解していない」「情報学 I を履修していない」学習者であるが、CS アンプラグド実践後の小テストでも完全な正解をしている。CS アンプラグドの実践で、公開鍵暗号において、送信者と受信者が用いる鍵についての知識が定着したと考えてよいように思われる。

残りの学習者は、確認テストで、完全な正答をしていない。これらの解答にはいくつかの特徴があった。正しく理解がなされていない点は大きくは以下の 2 点と考えている。○公開鍵と秘密鍵が、ペアの鍵を構成していることに対する理解が正確になされていない。例えば、A の公開鍵で暗号化したデータを復号できるのは、A の秘密鍵であるのだが、この部分を利用者の秘密鍵としてしまう学習者が 6 名いた。

○誰の公開鍵や秘密鍵を使うかが理解できていない。例えば、B が A にデータを送信する際に、B の公開鍵を使い、B の秘密鍵で(A が)復号すると答えた学習者が 3 名いた。その他、電子署名と混乱している学習者が数名いた。

3 章の CS アンプラグドの実践においては、時間の関係で、主には、与えられた地図を用いての暗号化と復号の実践を行い、学習者自身が地図を作る（公開鍵の生成に対応する）作業は完全には行うことができなかった。この、学習者自身が各自で公開鍵を生成し、他の学習者に解説を試みさせるというステップを経ることで、誰の地図を使って、どのように情報のやり取りさせるのか、その際の秘密鍵は誰のものを使うことになるか、を確認させることができれば、前述の誤りを回避させることができる可能性がある。学習者が誤りやすい上記の 2 点に関し、関連の実践を追加して行うことで、認識の誤りを低減できるか否かを、今後、実践し評価したいと考えている。

5. まとめ

本稿では、公開鍵暗号の仕組みを理解させるために行った実践と関係する各種評価結果について報告した。CS アンプラグドの実践により、学習者は公開鍵暗号について、興味・関心を持ったことは確かであるが、知識の定着としては、あるパターンの誤解を生ずる場合があることが確認さ

れた。今後、CS アンプラグドの実践を行った学習者に対し、インタビュー調査を行い、誤解の原因や、わかりにくかった内容等を調査し、効果的な学習構成や手法について確認を進める予定である。特に、CS アンプラグドの特徴である体験型の学習内容を、全体の学習構成として、どこでどのように行うことが効果的なのかについて、調査を進める予定である。

また、公開鍵暗号についての基礎知識が習得されていることを確認するとともに、それが、私たちが日常用いている各種ツール、例えばウェブブラウザやメール等での SSL 通信において、具体的にどのように役立てられているのかを含め、順次、理解促進を図ることが必要であると考えている。

参考文献

- [1] "平成 27 年度版情報通信白書", 総務省.
<http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html>
- [2] "個人情報の保護に関する法律".
<http://law.e-gov.go.jp/htmldata/H15/H15HO057.html>
- [3] 中村純他, 情報倫理デジタルビデオ小品集 III, IV, V. 大学 ICT 推進協議会
<https://axies.jp/ja/video>
- [4] 布施泉, 岡部成玄. ビデオとマンガを用いた情報倫理教育—学習効果と教材の使用順序—. 教育システム情報学会誌, Vol.27, No.4, pp. 327-336 (2010).
- [5] Tim Bell, Ian H. Witten and Mike Fellows: CS UNPLUGGED - An enrichment and extension programme for primary-aged students (2015).
<http://csunplugged.org/books/>
- [6] コンピュータサイエンスアンプラグド (日本語サイト).
<http://www.csunplugged.jp/>