

(オンライン) ISSN 2432-1036

(冊子版) ISSN 0286-116X

都城工業高等専門学校

研究報告

第55号

令和3年1月

目 次

研究論文編

- 日本国憲法及び改憲案の定量テキスト分析による指向分析……………吉井千周……………1

資料・紹介論文編

- 暗号技術のしくみのデモンストレーション例
—小学校の剰余計算の学習のみを前提とするRSA暗号での例—……………中村博文……………12

- Microsoft Teams を活用した遠隔授業の成果
……………臼井昇太・藤川俊秀・米満忍・岡元隆洋・山下敏明……………24

研 究 論 文 編

日本国憲法及び改憲案の定量テキスト分析による指向分析

吉井 千周¹

A Quantitative Text Analysis Study of the Japanese Constitution and Proposed Constitutional Amendments

Senshu YOSHII¹

(Accepted October 1, 2020)

Abstract Seventy-five years have passed since the end of World War II. In this context, there has been much debate on constitutional change in Japan, including the Liberal Democratic Party's "Draft for Revision of the Constitution of Japan," released in 2012. Other drafts and opinions on constitutional revision have been published and discussed. A bill on the procedures for constitutional revision has been enacted, which provides for a referendum and deliberation procedures in the Diet for constitutional revision, and the movement for constitutional revision is progressing. However, even in this atmosphere of constitutional change, the content of the argument for constitutional change is surprisingly little known. Besides, the Japanese Constitution is surrounded by the GHQ-occupation theory of "imposed constitutionalism," which the public has not recognized as a legitimate argument by constitutional scholars.

Therefore, this thesis analyzes the Japanese Constitution and the proposed constitutional amendments from an objective point of view based on a quantitative text analysis of the Japanese Constitution and the proposed constitutional amendments.

Keywords [Japanese Constitution, Constitutional Amendments, Quantitative Text Analysis]

1 はじめに

日本国憲法は、大日本帝国憲法第 73 条等の憲法改正手続きに従い帝国議会での審議を経て成立した。だが、連合国軍最高司令官総司令部（以下 GHQ）占領下で、マッカーサー草案が政府に示された後に制定されたという経緯から、日本国憲法の正当性を疑問視する人々から「押しつけ憲法」として長年改憲が主張されてきた。しかし、これまでの憲法学者の議論では、帝国議会での審議過程で多くの修正が加

えられ、また 25 条 1 項の生存権規定、17 条の国家賠償規定、40 条刑事補償規定といったマッカーサー草案に記されていない条文も見られる。そのため憲法学においては、自主性が認められた上での憲法改正であったと捉えるのが定説である。このような理由からか 1990 年代までは、結党当初から現行憲法の自主的改正を党是に掲げていた自由民主党（以下自民党）ですら、改憲について公の場で語ることは少なかった。

ところが、第二次世界大戦後 75 年がすぎた 2020

¹ 都城工業高等専門学校一般科目文科 General Education Division, National Institute of Technology(KOSEN), Miyakonojo College

年の今日、帝国議会において行われた議論が無視され、GHQ 占領下で作成されたということだけから「押しつけ憲法」として、改憲を求める人々の声は大きくなっている。自民党も 2012 年に発行したパンフレット『憲法改正草案 Q&A』において、「現行憲法は連合国軍の占領下において、同司令部が指示した草案を基に、その了解の範囲において制定されたものです」と述べ、押しつけ憲法論にのっとった改憲を主張する¹⁾。

2020 年の憲法記念日にあわせた各社の世論調査を見てみると、読売新聞調査では 49% の人々が「憲法を改正する方がよい」と回答し、朝日新聞調査では 43% の人々が「憲法を変える必要がある」と回答した^{注1)}。各社の世論調査のうちでも最も低い数値である毎日新聞調査でも 36% の人々が「憲法改正に賛成」と回答している^{注2)}。こうした世論を反映してか 2004 年以降を見ても、[表 1] のとおり幾多の改憲案が様々な団体より発表されている。

表 1 2004 年以降の憲法改正試案

改正案発表団体	改憲案名	発表年
読売新聞	読売憲法改正試案	2004 ^{注3)}
公益財団法人中曽根康弘世界平和研究所	平和憲法試案	2005
新しい憲法をつくる国民会議（自主憲法制定国民会議）	日本国憲法	2006
自由民主党	日本国憲法改正草案	2012
公益社団法人日本青年会議所	日本国憲法草案	2012
ゲンロン	新日本国憲法ゲンロン草案	2012
産経新聞	国民の憲法	2013
公益財団法人松下政経塾 第 34 期生共同研究 「憲法フォーラム」	日本国憲法改正草案	2015
憲法改正発議研究会	日本国憲法改正試案	2017

(著者作成)

これらの改憲案について、特に自民党による「日本国憲法改正草案」には多くの批判の声があがっている^{注4)}。しかし、改憲を巡る議論は、改憲派と護憲

派の両派が互いの陣営の内部で議論が行い、なかなかその溝が埋まらない状態になっている。例年 5 月 3 日に行われる憲法記念日の集会にしても、改憲派と護憲派がそれぞれに集会を開き、コメントを発表するという状態が続いており、そこには建設的な対話が見られるとは言いがたい。

本論文では、そうした状況を踏まえ、定量テキスト分析の手法を用い、現行の日本国憲法と各改憲案をなるべく客観的に比較する手法を提示し、今後の日本における憲法の在り方、対話をめぐる一つの材料の提案を試みる。

2 自民党改憲をめぐる経緯

以後の議論を進めるにあたり、本論文における解析の主流となった自民党の改憲論がどのような流れで出てきたのか確認しておきたい。

長年タブー視されていた改憲をめぐる状況が一変するのは、2000 年 1 月に召集された第 147 回通常国会において、衆参両議院での憲法調査会が設置されたことによる。国会議員 30 人以内、学識経験者 20 人以内からなるこの調査会は、日本国憲法に関する調査・研究・審議等を行うために委員会組織として設置された。こうした改憲をめぐる流れの中で自民党は 2000 年 6 月に実施された第 42 回衆議院総選挙において、24 の総選挙政策のなかの 23 番目に改憲論を記載した。翌 2001 年 4 月の自民党総裁選に小泉純一郎が出馬し、「聖域なき構造改革」を掲げて総理大臣に就任すると、この傾向がさらに加速する。小泉旋風と呼ばれた厚い支持層を背景に 2003 年 11 月に実施された第 43 回衆議院議員総選挙では、自民党結党 50 周年の 2005 年秋までに改憲草案をつくることを公約する。

2005 年 4 月、両院の憲法調査会は、それぞれの報告書を各議院の議長に提出した。報告書では、現在日本国内における改憲議論の主要トピックになっている第 9 条の改正だけにとどまらず、地方自治や外国人の人権についても活発な議論が行われ、同年 8 月に開催された第 167 回国会では、憲法調査会に代わり憲法審査会が設置され、日本国憲法および日本国憲法に密接に関連する基本法制について調査を行い、日本国憲法改憲案の原案の発議も行うことができるようになった。

こうした流れをうけ、2005 年 10 月 28 日に開催された自民党結党 50 周年党大会で「新憲法草案」が発表となる²⁾。「新憲法草案」は、「新憲法起草委員会・要綱第一次素案」及びこれに基づいた「新憲法第一次案」さらに 10 月公表の「新憲法第二次案」

に修正を加えて完成する。その内容は、現行憲法第 11 章の「補則」の削除、第 2 章「戦争の放棄」を「安全保障」へと改称、自衛軍設置の記載（第 9 条 2）を行い、軍事裁判所（第 76 条）、環境権（第 25 条の 2）、犯罪被害者権利（第 25 条の 3）などの明記を行った。

各地の平和団体、いわば護憲派の新憲法草案への反発は大きく、各地で護憲派団体の活動が活発化した。また、2007 年の日本国憲法の改正手続に関する法律案をめぐる与野党協議の決裂で自民党と民主党の協力関係が崩れ、2007 年 7 月に行われた第 21 回参議院選挙において改憲を公約に掲げた自民党が参院選で大敗し、改憲の動きは沈静化するかに見えた。

だが改憲の動きは再度復活する。2011 年に発生した東日本大震災の対応などで、民主党政権への批判がおこったことなどから、自民党への再評価が生まれた。世論をうけ、2012 年 4 月 28 日のサンフランシスコ講和条約発効 60 周年に合わせ自民党は「憲法改正草案」を発表する³⁾。この改憲草案は、2005 年の新憲法草案では現実可能性に配慮し控えられていた復古的な要素が全面的に取り入れられている。天皇の元首化（第 1 条）、国防軍の設置（第 9 条の 2）、日章旗の国旗・君が代の国歌設定（第 3 条）などが記されている。

自民党は、2012 年 12 月に行われた第 46 回衆議院選挙において、被災地の復興に改憲をマニフェストに加え、議席数を大きく伸ばし与党に返り咲く。歴代最長の就任期間となった安倍首相は、積極的に改憲を唱える。また、それに対応する形で、[表 1] に示した他にも複数の改憲案が生まれることになる^{注 5)}。

3 計量テキスト分析による日本国憲法及び各改憲案の分析

3.1 計量テキスト分析による改憲案分析の利点

前章に記したような改憲をめぐる言説は、先に記した「押しつけ憲法論」をめぐる憲法学の学説はもちろん、法学をめぐる基本的な学説が顧みられないまま、特に SNS 等においては勝手な解釈が流布されかねない状況を生み出している。

通常、法律学においては条文の解釈・適用について主として以下の二つの立場がある。一つは、法律制定当時の立法者の主観的意思を探求し、その意思を法の解釈に再現するという「立法者意思説」である。もう一つは、立法者が立法当時に有していた意思ではなく、法律それ自体の意思を探求し解釈するという「法律意思説」である。現在日本では、法解

釈の主流は「立法者意思説」であるが、法律意思説も含め、科学的な知見から、法理論として確立しようとするには大きな意味がある。

しかしながら、こうした法学者の思索は人々には考慮されないまま、自説に有利になるように勝手に解釈されて流通されがちである。そこで、なるべく各人が勝手に解釈する余地を減らし、統計的な処理を用いて日本国憲法と自民党改憲案を分析してみたい。

今回は、「日本国憲法」「自民党憲法改正草案（以下「自民党案」）」に加え、多くの読者を有し国民の目に多く触れることになった「読売新聞憲法改正案（以下「読売案」）」「国民の憲法（以下「産経案」）」の 4 つの憲法及び改憲案を分析対象にする^{注 6)}。

3.2 計量テキスト分析の手法

今回の調査に使用する計量テキスト分析の手法を簡単に説明しよう。計量テキスト分析とは、文章中に登場する一つ一つの単語の登場頻度を計量し、さらに他の単語と一つの文章内での登場組み合わせをカウントしていく、という手法で文章の傾向を探る調査方法である。

もちろん、一つ一つの言葉には、複数の解釈が存在しうるため、こうした手段で憲法や改憲案の全てを分析的に捉えることは不可能である。上述した法律意思説や立法者意思説などに基づき、条文への批判的考察を行わなければならない。だが、その一方で計量テキスト分析には、一つ一つの条文中の単語に過剰に意味や意義を付け加えることがないため、文章の大まかな傾向を捉えることは可能になる。

また、計量テキスト分析では、手作業で行うことも可能ではある。だが莫大な時間がかかるため、専用のソフトウェアを利用するのが常道となっている。

今回使用するソフトウェアは、立命館大学の樋口耕一氏によって開発された KH Coder である^{注 7)}。KH Coder はテキスト型（文章型）データを統計的に分析するためのソフトウェアであり、アンケートの自由記述・インタビュー記録・新聞記事など、さまざまな文字データを分析することが可能となっている。

3.3 クレンジング作業の実施

今回の日本国憲法及び改憲案の分析には、まずクレンジング (cleansing) とよばれるテキストの修正作業が必要となる。文章化された日本語は、同じ事物を示す言葉であっても例えば「国際連合」、「国連」、「UN」(全角表記)、「UN」(半角表記)と複数の表記がある。これらを考慮せずに定量分析を行ってし

まうと、それぞれが別個の単語としてカウントされてしまう。

そのため、特に SNS などのように書き手が複数いる文章の定量テキスト分析では、各人が自由な表記を統一するクレンジング作業は必須である。その際には論文、各種辞典などを利用し、登場する地名や用語の表記をどれか一冊の書籍に準拠するようにしておく必要がある。しかし、それはクレンジング作業によって文章の細かいニュアンスを消し去りかねないため、通常のクレンジング作業では細心の注意が必要となる。

しかし、今回の日本国憲法及び各改憲案のテキスト分析においては、いずれのテキストも法律用語が使用されているため、必要最低限度のクレンジング作業を行えばよく、不必要にテキスト原文を修正しなくても分析が可能となる。今回の分析において唯一行ったクレンジング作業は、日本国憲法の旧かなづかいによる原文を現代仮名遣いに改めることのみであった。具体的には 1986 年 7 月 1 日告示、訓令された「現代仮名遣い」に関する内閣告示第一号に基づき、現代仮名遣いにあらためた。

3.4 前処理の実施

クレンジングの後に KH Coder を利用して行うのが「前処理」と呼ばれる作業になる。前処理とは、これから単語の頻度や結びつきを考えるにあたり、登場する文章を単語ごとに切り出す作業のことを差す。

例えば、日本語の「思う」という動詞には、「思わない」「思った」といった動詞変化がある。これをそのまま分析にかけてしまうとそれぞれが別の単語として扱われてしまう。単語の登場頻度をカウントする計量テキスト分析では、これらの活用変化が行われた動詞全てを同じ動詞として扱わなければならないが、手作業で全ての動詞を終止形に戻し、カウントを行うのは手間がかかる。

そこで KH Coder では、形態素解析ソフト「ChaSen」と「MeCab」を用いて日本語における動詞変化を考慮し、これらを一つの動詞「思う」と基本形に変化しカウントする。これらの形態要素解析ソフトは KH Coder と同時にインストールされる。なお、日本語同様、英語などの動詞の変化や各種短縮形を基本形に変化させる（例えば「isn't (=is not)」「I'd (=I would)」など）ソフトウェアも KH Coder には同梱されており、外国語の文章解析にも使用できる。

また複数の言葉が合成されてできた単語の取り扱いも調整が可能である。例えば、「国会議員」とい

う単語は、「国会」という言葉の使用と捉えるよりも「議員」という単語と結合した「国会議員」という一つの単語として捉えるほうが理にかなっている。そのため、言葉を取扱う際に不用意に単語を切り刻まないように調整（チューニング）を行ったほうがよい場合もある。

今回の分析では、「国会議員」「地方公共団体」「国務大臣」「日本国民」の単語を分割せず、一つの単語として捉えるよう処理を行った。これらのソフトを用いて各テキストの前処理作業を行うと、それぞれのテキストの文章数・単語数の分析結果が出る [表 2]。

表 2 日本国憲法及び各改憲案の文書数・単語数

	日本国憲法	自民党案	読売案	産経案
文章数	224	269	272	259
総抽出語	5,808	7,084	6,966	5,692
使用数	2,468	3,121	3,055	2,559

(著者作成)

こうして出された分析結果を元に KH Coder を用いた本格的な計量テキスト分析を進める。こうして抽出された憲法及び各改憲案の頻出語上位 20 のリストが [表 3] のとおりになる。一覧してわかるとおり、いずれも「法律」「定める」という言葉が頻出しており、このままでは特に互いのテキストの違いを見いだすことは難しい。

3.5 共起ネットワークの作成

前節でとりあげた前処理の実施や頻出語のリストアップだけではそれぞれの条文を分析対象とするのは難しい。そこで、このようにして取り出された登場頻度の高い単語が、他の単語とどのような形で使用されているか文中の同時使用回数別にカウントし、二次元空間にプロットするという作業を行う。こうしてできあがった図を「共起ネットワーク」と呼ぶ。

共起ネットワークは、一つ一つの文書で出現する単語（抽出語と呼ぶ）のそれぞれについて、距離（Edge）を計算し、図示することで得られる。

集合同士の類似度をはかる Edge の算出方法として、KH Coder では、Jaccard 係数、コサイン類似度、Euclid 距離を用いて算出することが可能であるが、今回は単語の関連性のみを端的に捉えることに適した Jaccard 係数を用いた方法を用いる。Jaccard 係数の算出は以下の通りとなる。

表 3 日本国憲法・改憲案頻出語上位 20 語リスト

日本国憲法		自民党案		読売案		産経案	
抽出語	出現回数	抽出語	出現回数	抽出語	出現回数	抽出語	出現回数
法律	55	法律	79	法律	68	法律	62
定める	44	定める	71	定める	54	定める	52
国会	39	国会	43	議員	42	国	37
議員	36	場合	38	国民	41	国会	37
国民	32	国民	35	国会	40	国民	33
議院	28	議員	34	憲法	31	憲法	30
憲法	28	国	32	衆議院	31	議員	28
衆議院	27	議院	30	内閣	30	衆議院	26
すべて	23	行う	30	議院	28	内閣	23
議決	23	衆議院	28	場合	28	権利	22
内閣	22	権利	24	国	26	行う	22
権利	21	内閣	24	裁判官	26	議院	21
行う	21	内閣総理大臣	24	議決	25	裁判官	18
裁判官	20	議決	23	裁判所	24	保障	18
場合	19	全て	23	参議院	23	地方自治体	17
選挙	19	地方自治体	23	内閣総理大臣	23	議決	16
有する	17	裁判官	20	すべて	22	参議院	16
受ける	16	有する	20	権利	22	裁判	15
国	15	規定	18	行う	19	天皇	15
参議院	14	必要	17	有する	19	内閣総理大臣	15

(著者作成)

まず、ある集合 A と別の集合 B の Jaccard 係数 $J(A, B)$ は、以下の式で定義される。

$$J(A, B) = \frac{|A \cap B|}{|A \cup B|}$$

例えば「法律」の単語が含まれる 55 の条文を集合 A、「定める」(B) の単語が含まれる 44 の条文を集合 B と定義し、うち両者の単語が 38 の条文に同時に登場したとする。この場合 Jaccard 係数 $J(A, B)$ は以下のとおり計算できる。

$$\begin{aligned} J(A, B) &= \frac{|A \cap B|}{|A \cup B|} \\ &= \frac{|A \cap B|}{|A| + |B| - |A \cap B|} \\ &= \frac{38}{55 + 44 - 38} \cong 0.622 \end{aligned}$$

Jaccard 係数が大きいほど、同時に登場した文が多いと判断できる。なお、どちらの語も登場しなかった、すなわち集合 A と集合 B がどちらも空集合 ϕ の場合、 $J(A, B)=1$ とする。

このようにして算出された日本国憲法及び各改憲案のテキストに登場する各単語 Jaccard 係数上位 60 を取り出しマッピングしたものが [図 1] [図 2] [図 3] [図 4] になる。記載してある数値が Jaccard 係数を示す。

こうしたテキスト分析手法によってそれぞれの憲法案がどのような傾向を持っているかを調べることができる。

3.6 対応分析の実施

前節でとりあげたそれぞれのテキストにおける共起ネットワークは、日本国憲法とそれぞれの改憲案の傾向を分析するには適しているが、憲法及び各改憲案の相対的な特徴を捉えるには適さない。そこで憲法及び改憲案を分析対象として、他の憲法及び改憲案に出てこない、いわゆる差異が顕著な単語を取り出し、二次元空間にマッピングする。このことによって、日本国憲法と憲法草案の全てのテキストが形成する憲法及び改憲案の条文が生み出す言語空間の中で、他のテキストと比較した上で、日本国憲法と各改憲案を特徴付ける語を算出することができる。

具体的な手法を確認してみよう。まず、Jaccard 係

表 4 日本国憲法及び各改憲案における特徴的な単語

日本国憲法		自民党案		読売案		産経案	
国会	0.108	法律	0.169	国民	0.099	国	0.103
議員	0.097	定める	0.163	議員	0.093	国民	0.091
すべて	0.091	場合	0.110	憲法	0.086	憲法	0.077
議院	0.084	国会	0.107	内閣	0.085	権利	0.065
憲法	0.082	国	0.090	場合	0.079	保障	0.058
内閣	0.071	行う	0.088	すべて	0.076	地方自治体	0.052
行う	0.068	全て	0.086	衆議院	0.073	天皇	0.052
権利	0.066	議院	0.083	内閣総理大臣	0.068	参議院	0.047
衆議院	0.063	内閣総理大臣	0.072	裁判官	0.062	裁判	0.045
受ける	0.060	権利	0.067	裁判所	0.061	最高裁判所	0.045

(著者作成)

数を用いて、文書と各単語の間の対応度を調べる。そのうち、他の文書に出てこない特徴的な単語を抽出する [表 4]。さらに KH Coder の対応分析機能を用い、日本国憲法及び各改憲案での差異が顕著な語上位 60 語をマッピングするという条件対応分析を行う。その結果として現れたのが [図 5] である。こうした手法を対応分析、またはコレスポンデンス分析と呼ぶ。

図中に現れるバブル (円) の大きさは登場頻度の度合いを示し、スクエア (四角形) は日本国憲法及び各改憲案を特徴付ける語から、それぞれの改憲案の位置づけを行ったものである。

4 分析結果の解釈

4.1 共起ネットワークの解釈

第 1 の特徴は、日本国憲法及び各改憲案に共通して見られる特徴として、「法律」と「定める」の用語がいずれのテキストにおいても強い結びつきである。例えば日本国憲法では、「天皇は、法律の定めるところにより」(日本国憲法第 2 条 2) といった形で現れる。

第 2 の特徴は、日本国憲法では「日本国民」の言葉が「平和」との結びつきの強固さである (前文、9 条)。他の改憲案にはみられない使われ方として現れている。

第 3 の特徴は、日本国憲法と他の改憲案との間に見られる「天皇」に関する他の言葉の結びつきの差である。日本国憲法のみが「天皇」の言葉に複数の特徴的な言葉が結びついている。特に天皇と結びつきの強い言葉として「承認」が日本国憲法では登場していることに注目したい。

第 4 の特徴は、地方自治体 (地方公共団体) に繋がる単語が他の改憲案と比して、日本国憲法に多く

現れている点である。そのため、例えば、自民党案第 20 条 3 項「国及び地方自治体その他の公共団体は、特定の宗教のための教育その他の宗教的活動をしてはならない。ただし、社会的儀礼又は習俗的行為の範囲を超えないものについては、この限りでない。」といった、日本国憲法で明確に禁止された政教分離について、各改憲案では地方自治体の活動が緩やかに認められている。

第 5 の特徴は、「緊急」「事態」という言葉と「内閣総理大臣」の言葉の結びつきが、日本国憲法以外の改憲案に存在する点である。緊急時における内閣総理大臣の権限が他の改憲案では強いといえる。

第 6 の特徴は、日本国憲法は、他の改憲案と異なり、「憲法」を含む 20 の単語によるネットワーク、「天皇」を含む 14 の単語によるネットワークを作っている点である。他の改憲案では産経案が唯一 15 の単語によるネットワークを有している。[表 2] で示したとおり、それぞれのテキストを構成する文章数・単語数ともに自民党案はどの改憲案よりも多いことがあきらかである。別の視点から捉えれば自民党改憲案では、テキストの中に単語が単発で多く利用されており、その条文の中でしか登場しない単語も多々あると考えられる。典型的には自民党改憲案 9 条に登場する「防衛軍」「軍人」のほか、前文に登場する「大災害」などである。新しい制度の創出を目指すものである以上この結果は当然であるが、その反面、日本国憲法において登場する単語の解釈が統一しやすい反面、自民党改憲案では、各条文において単語の定義や解釈を行わなければ運用できないと考えられる。

4.2 対応分析の解釈

つづけて、作成した対応分析 [図 5] 及びその作成に使用された [表 4] から以下の特徴を挙げるこ

とができる。

第 1 の特徴は、日本国憲法及び各改憲案において、日本国憲法と読売案は近い位相にあるという点である。この両者は傾向としては近いものであると考えられる。しかし、自民党案と産経案においては、それぞれが特徴的な単語の使用によって大きく位相が異なっている。

第 2 の特徴は、自民党案に特徴的な単語として人物では「内閣総理大臣」の単語が使用されている転移ある。[表 3] に示したとおり、自民党案では 24 回、読売案でも 23 回登場する。特に自民党案では [表 4] に示したとおり、各改憲案から相対的に見た場合 Jaccard 係数の値が 0.072 と高く、自民党案を特徴付ける単語であることがわかる。同様に産経案においては、「天皇」の単語が Jaccard 係数の値が 0.052 と特徴的なものとして使用されている。

第 3 の特徴は、さらに日本国憲法及び各憲法案において、[表 3] で示したとおり、「法律」「定める」という単語のこの二つの単語はそれぞれのテキストにおいて頻出の単語であるという点にある。自民党案では特に [表 4] に示したとおり、日本国憲法及び憲法改正案全体のテキストにおいて「法律」が 0.169、「定める」が 0.163 と Jaccard 係数の値が高い。つまり憲法内で様々な規定を行うのではなく、憲法外の「法律」を「定める」ことによって、規定を加えようとする傾向が見られる。例えば自民党改憲案 9 条 2 項では「国防軍は、第一項に規定する任務を遂行するための活動のほか、法律の定めるところにより、国際社会の平和と安全を確保するために国際的に協調して行われる活動及び公の秩序を維持し、又は国民の生命若しくは自由を守るための活動を行うことができる。」という具合に。

第 4 の特徴は、日本国憲法及び読売案では、「国民」、「内閣」、「衆議院」、「参議院」、「裁判所」といった統治機構に関する単語が特徴付けられる言葉である点である。これらの言葉は日本国憲法を学んだことのある学生なら誰でも耳なじみの言葉であるが、これらが自民党案及び産経案では、日本国憲法及び読売案ほどには特徴のある言葉として使用されていないということになる。

5 おわりに

本論文では、憲法及び各改憲案の条文について、一つ一つ言及することは避けてきた。しかし、これまで発表された各憲法学者の指摘を強化するデータになったと考えられる。もちろん、こうした定量テキスト分析には限界もある。例えば改憲論議に

おいて中心的トピックになる自衛隊の規定については、改憲案の条文に言及される条文数が少ないことから、この定量テキスト分析ではデータとして現れない。わずかしかな言及されない条文であっても、重要なトピックとして議論されなくてはならないテーマに定量テキスト分析で関わることは難しい。

「改憲」という国の大きなルールを変更するという議論は、国民一人一人に熟考が求められる。一つ一つの条文、そして単語に込められた意味を考えながら各憲法と改憲案に接するとき、本来ならば日本国憲法の条文の一つ一つの成立過程、誕生した背景、憲法学者の声に耳を傾けてもらうことが肝要である。SNS などの台頭により、そのような法学者や専門家の声も届かない時代となったのであれば、こうした定量テキスト分析による客観的な手法による憲法及び改憲案の分析にも多少なりとも貢献する余地があるのではないかと。

謝辞

本論文の構想は、本校赴任後から学内外でデータベースシステムの構築と運用、学生や後輩への指導に預かることができたことで生まれた。データベースシステム設計に長年携わらせて頂いたキング鉄道広告株式会社各位、宮崎県中小企業会の各位、立命館アジア太平洋大学でのデータベース論受講者各位に御礼申し上げたい。また同僚の友安一夫先生には、Jaccard 係数の算出方法について多くのご教示を頂いた。何よりも本論文の定量テキスト分析は、樋口耕一先生作成による KH Coder という素晴らしいソフトウェアと書籍がなければ実現しなかった。深く感謝申し上げます。

注

- 1) 読売新聞 2020 年 5 月 3 日付全国版、朝日新聞 2020 年 5 月 3 日付全国版世論調査結果より。
- 2) 毎日新聞社 2020 年 5 月 3 日付全国版による世論調査結果より。
- 3) 読売新聞社による「読売憲法改正試案」は、1994、2000、2004 年にわたって発表されている。
- 4) 伊藤真(2018)では、逐条的に自民党憲法案の一つ一つの条文を解説し、その不備を指摘しているほか、横田耕一(2014)は、憲法学者の手によって日本国憲法と自民党憲法改正草案の理念の違いから問いただされている。
伊藤真：増補版赤ペンチェック自民党憲法改正草

案, 大月書店, 2018

横田耕一: 自民党改憲草案を読む, 新教出版社,
2014

- 5) 日本国憲法の改憲案については、国立国会図書館が詳細にデータをまとめている。次の分権は、網羅的に憲法改正に関する文章をまとめている。元尾竜一: 最近の主な日本国憲法改正提言, 調査と情報 856号, 2015
- 6) 解析に使用した原文となるテキストは以下のとおりである。
自由民主党: 日本国憲法改正草案, 自由民主党, 2012
読売新聞: 読売憲法改正試案全文, 読売新聞全国版 2004年5月3日付、2004
産経新聞社: 国民の憲法, 国民の憲法, 産経新聞社, 214-265、2013
- 7) 2020年現在、KH Coder は公式ホームページから Windows、Mac OS、Linux 用に無料ダウンロードできる。 <https://kncoder.net/>

参考文献

- 1) 自由民主党憲法改正推進本部: 憲法改正草案 Q & A, 2012
- 2) 自由民主党: 新憲法草案, 自由民主党, 2005
- 3) 自由民主党: 日本国憲法改正草案, 自由民主党、2012

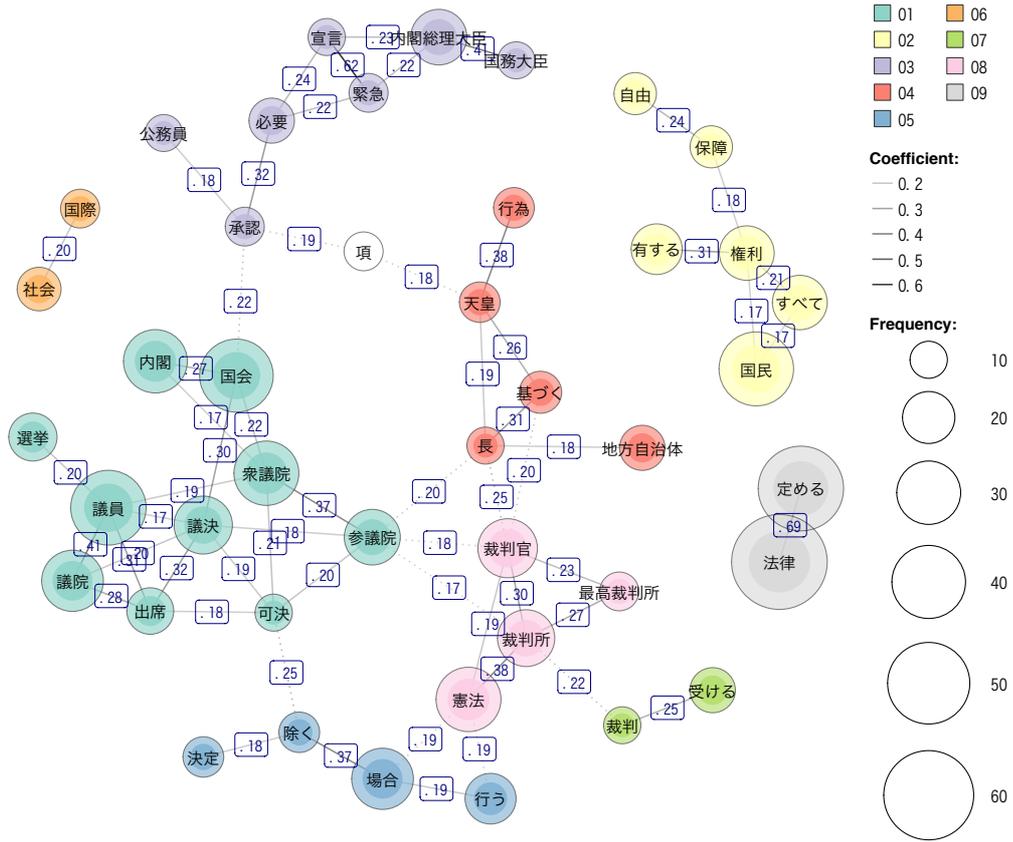


図3 読売案共起ネットワーク

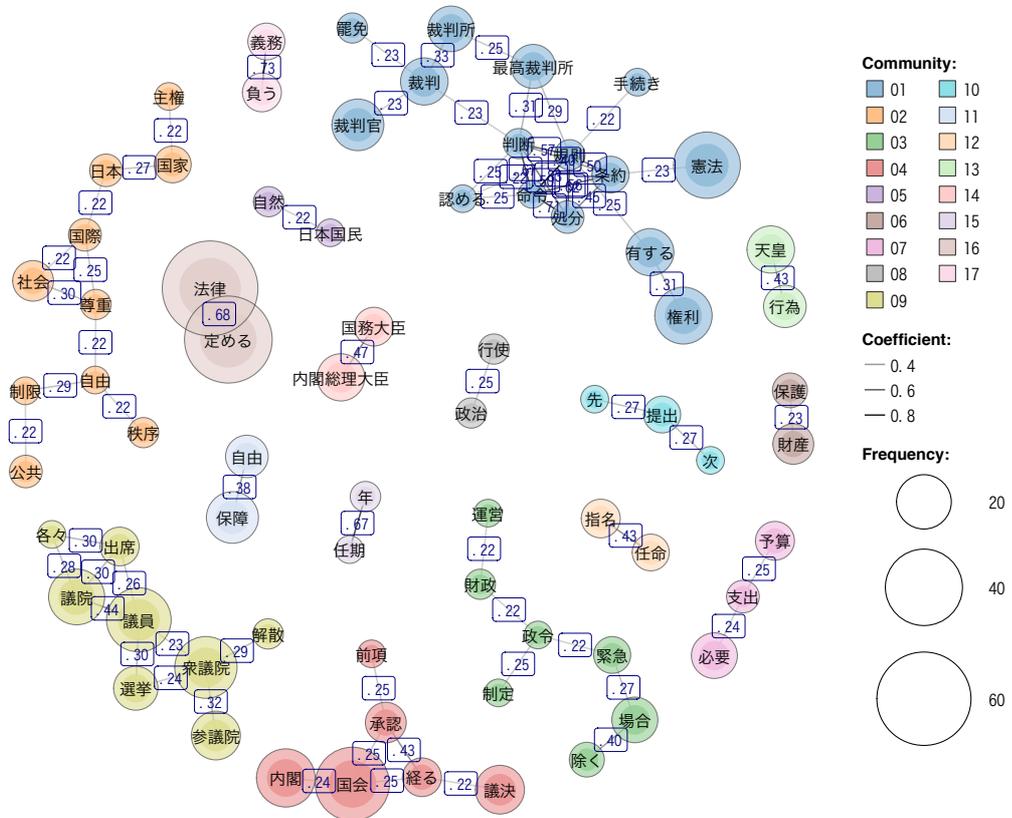


図4 産経案共起ネットワーク

資料・紹介論文編

暗号技術のしくみのデモンストレーション例 —小学校の剰余計算の学習のみを前提とする RSA 暗号での例—

中村博文¹

A Demonstration Example of Mechanism of Encryption Technology —An Example with RSA Encryption Assuming Only Learning of Remainder Calculation at Elementary School—

Hirofumi NAKAMURA¹

(令和 2 年 10 月 1 日受理)

あらまし データを秘密にして通信や記録をする暗号技術が、実際には計算でなされていることについて、小学校で習う剰余計算の学習のみを前提として、23 分程度でデモンストレーションする例を報告する。具体的には、RSA 暗号の暗号化と復号のアイデアを、比較的小さい数で確かめながら、小学 4 年生以上の多くが理解する内容になっている。その中で、0~32 についての 0 乗から 32 乗までの数を 33 で割った余りの一覧表で見える余りの性質 (33 で割った余りの世界では 0~32 のどれでも 21 乗すると元と同じという性質を、デモンストレーションでは『おもしろい性質』と呼んでいる) と、この 21 が 2 数の積であるため暗号に応用できること (デモンストレーションでは RSA 暗号の『キモ』と呼んでいる) に触れている。また、このような内容だけで提示物を作成すると数と文字だけになり無味乾燥げみであるものの、児童・生徒から大人まで比較的多くが視聴している映画『サマーウォーズ』に関連する事柄を織り交ぜて並行させることで、ある程度の興味と期待と集中の中での実施をねらっている。暗号解読に関連した計算の実演も含むものの提示中心であるが、余り計算が暗号として使用できる理由を参加者の多くが理解するデモンストレーションである。本校の毎年 1 回の科学イベントとなっている『おもしろ科学フェスティバル』において、剰余計算を学習済みの小学生から大人までを対象に実施した状況も報告する。

キーワード [出前授業, 科学イベント, 小学生, RSA 暗号, サマーウォーズ]

1 はじめに

本稿は、科学イベント等や授業で児童・生徒・学生の数理への興味を助長するものとなるように考えた一取り組み例の報告である。具体的には、通信や記録において、もし情報が盗まれても、情報の機密性保持が可能で、それが計算でなされていることについて、小学校で習う剰余計算の学習のみを前提

として、RSA暗号の暗号化と復号を具体例にした 23 分程度でのデモンストレーション例の報告である。

小中学生が主対象の本校おもしろ科学フェスティバル (年に 1 回、校内で 1 日で開催) で、家族や高大生も対象に誤り訂正を題材に出展¹⁾して以来、RSA 暗号²⁾などの暗号を扱いたいと思案していた中、関連情報^{3~5)}との遭遇や、先述の出展¹⁾での余り計算の利用経験などが繋がり、実施に至った。

1 都城工業高等専門学校一般科目

General Education Division, National Institute of Technology(KOSEN), Miyakonojo College

本稿で暗号技術やそのひとつである RSA 暗号を改めて解説することは略す。おもしろ科学フェスティバルについてや、それへの筆者の出展の動機に関しては、文献 1) に多少記載している。

2 本デモンストレーションにおける方針等

概ね以下の方針のもと、内容を構成した。

- ・関連証明と鍵作成関係は全く省くが、RSA 暗号の符号化から復号までの流れと、暗号として使える理由にはきちんと触れる。
- ・余りの計算に慣れてきた小学 4 年生から大人までが対象で、中でも小学 4 年生が確実に理解すること(わり算を既知という小学 3 年生もなるべく)。
- ・タイトルを「余り計算で分かる映画『サマーウォーズ』の暗号」とし、関連出版物^{2,6~9)}からの引用で済む範囲で、全参加者の期待に違わぬよう、作品との関連^{3,4)}も示す。(出展タイトルは、的確で短く、しかし、勘違いされにくいことを心がけた。イベントの来場者が張り紙に書いている出展タイトルの「計算」の字句を気にして敬遠する姿も見かけるが、一方でこの出展への参加者には若干の覚悟を期待できると感じている。)
- ・参加者の演習は時間的に設けられないが、計算例は、その場でパソコンで計算して提示する。
- ・用語はかけ算、わり算、余り、暗号、解説、RSA 暗号までとし、積、何乗、剰余、暗号化、鍵、素数、素因数分解、アルゴリズムは用いない(都度の若干の補足や後述の「おまけ」で一部例外あり)。
- ・画像は使用しない。(使用すると面白くはなるが、肝心の数字に対する集中をそぐ懸念がある。)
- ・所要時間は出展場所への出入りの時間以外に 23 分以内とする。多少の時間調整用の省ける内容を、「おまけ」として区別して内包しておく。
- ・おもしろ科学フェスティバルでは、小中学生と年齢の近い本校学生に可能なら協力者を募り、学生がデモンストレーションできるようスライドとシナリオ例を予め作成しておく。多少のアドリブは可とする。(令和元年の出展では、途中の確認用で後述するスライド 19、20 の 2 枚を足した。)
- ・おもしろ科学フェスティバルで協力者が得られた場合、1 日計 10 回の 30 分毎の繰り返しを学生 3 人(役割をプレゼン役、案内役と呼ぶことにする。各回各ひとり。更にもうひとは、立ち合いまたは補助で、非番の時間帯も設ける。)で交替して分担する。主として話す学生ひとり(プレゼン役)は、他の学生に補助を頼んでも構わないことにする。案内役は出入りや着席等を把握する。

- ・初歩的な用語の解説や暗号化及び復号の概念図も載せた配布資料を、持ち帰り用に用意する。その中に、その資料のカラー版とスライドを Web 掲載している URL の QR コードも載せておく。

3 デモンストレーションの内容

表 1 にデモンストレーションの内容の概要を示す。スライドのページ(頁)番号も記載している。その 13 と 15 は、スライドではなく、計算の実演例の内容である。

本稿の後ろ側に、付録として、デモンストレーションで用いるスライド等の例と、その提示の際のシナリオ例を含むイベント出展での進行例と、配布資料の例を掲載している。

なお、これらには次の実施を想定した修正を含む。デモンストレーションの中で用いている、2 を 21 個かける例は、小学生等にとって理解に十分でかつ容易な例として、全ての可能性の中から選択した。

表 1 スライド等の順序と触れる事柄

頁	触れる事柄 (この表中では言い回しの初出を太字)
1	タイトル
2, 3	映画『サマーウォーズ』も引き合いに 暗号 、 解説 の説明と、以降のあらましの説明(以下のほぼ全スライドで上部に同じ形式の目次を挿入)
4	例を用いて余り計算を復習(大人にも有効)
5	2 をかける個数を増やしながら 33 の剰余を例示
6	更にかけていきながら、余りが途中で元の数に戻ることを確認と、次ページで多量の数で驚かないようにとの断り
7	『実に面白い』(ドラマ『ガリレオ』、東野圭吾原作)を引き合いに『 おもしろい性質 』として印象付けながら、0~32 全てで 21 個かけると元に戻ることを、予め計算した表で確認
8	2 を 21 個かける例、 $2 \times 2 \times 2 = 8$ を 7 個かける例のあと、7 を知る人だけが元に戻せることを『 キモ 』として印象付け、 RSA 暗号 という名前も紹介(適宜、一言だけ、33 が 2 つの数をかけたものだからと)
9	RSA 暗号の暗号化と復号のまとめ: 2 を 3 回かけた 8 があるとき、8 を 7 回かけた人だけが 2 が分かる
10, 11	ガードナーの暗号クイズ⁶⁾ を紹介
12	RSA 暗号の解説の例示(素因数分解ができたあとをとということ提示)

13	小さい数の場合でデータとプログラムをテキストファイルから切り貼りして数式処理系(Maxima)で実際に解読の計算を実演(名前だけ、拡張ユークリッドの互除法を紹介)
14	アトキンスらの素因数分解の使用資源と結果 ⁷⁾ を提示
15	アトキンスらの素因数分解結果を用いデータとプログラムをテキストファイルから切り貼りして数式処理系で実際に解読の計算を実演(名前だけ、バイナリ法を紹介)
16	ガードナーの暗号クイズの内容と解読結果をまず数で表示 ⁷⁾
17	ガードナーの暗号クイズの答(英文) ⁷⁾ を導出
18	映画『サマーウォーズ』ではどのように表れているかについて、OZ(オズ)のパスワードや桁数 ^{8,9)} 及び暗号文の字面 ⁹⁾ の一部を挙げ比較、これらから、映画で使われている暗号はRSA暗号との推測を提示
19, 20	『おもしろい性質』と『キモ』が分かったかそれぞれ挙手で確認
21	(21~25は「おまけ」として)モジュロ演算という言葉が出てくること、余り繋がりであること、曜日が計算で分かること、紹介程度に公式の存在
22	名前だけ、ショア(Shor)の方法と量子コンピュータを紹介
23	実用化がまだのためRSA暗号は大丈夫と言及
24	映画にShorという字 ⁹⁾ が出てくるのを探してはと参加者に勧める、また、主人公は積を元の2数に分ける計算をしたかも知れないとの推測を提示
25	時間によって適宜(時間がないなら飛ばす):使用した例と用語の入った暗号化と復号の概念図で、用語を流れと共に紹介
26	最後に、映画と暗号クイズとの関連、映画の暗号がRSA暗号との推測、RSA暗号が現役など言及
27	タイトルを再表示(終了を表す意味と、次の入室者にとっての確認用で)
28, 29	参考文献(文献を掲載している資料を配布する場合には提示を省く)

4 実施状況

平成30年と令和元年の第6回と第7回おもしろ科学フェスティバルと授業での実施に関して述べる。KOSEN まちなか科学フェスティバル(校外で実施)の出展においては筆者のみでデモンストレーションしたが記録不十分のため割愛する。

おもしろ科学フェスティバルとして来場者にアンケートが実施されており、以下、両年度の集計情報の使用許可を得て記す(都城工業高等専門学校学

生課教務係及び小中学校教育支援グループ提供)。

平成30年と令和元年で(以下で、列記はこの順序)、来場者数は1540人と1620人で、アンケートへの回答者数は230[120]人と180[120]人であった(この段落の人数は概数、角かっこ内は以下も小学4年生から大人までと分かる回答者の人数)。

アンケートの中には「楽しかったイベント」という尋ね方で35件と34件の出展の中から複数回答で選択する設問がある。それによると、本稿のデモンストレーションの出展への選択は7[7]人(内小学生が4年生1人)と16[11]人(内小学生が、3、4年生2人ずつと6年生の計5人)であった(出展あたりの平均は33[18]人と20[12]人であった)。本稿の出展への参加者は両年とも10回で少なくとも80人程度以上であった。これらの比率からは、本稿のデモンストレーションは地味で敬遠されがちな題材の割には協力学生の頑張りもあって健闘したと思われる。なお、本稿で参加者という言葉を用いているが、他の出展の殆どが何かしらのいわゆる参加型であるのに対して、本稿のデモンストレーションの出展は視聴のみであったことは、大きな相違点である。

両年度で、シナリオ例とスライドに大きな差異はなかったが、参加者にとっての印象の違いに関わりそうな思いあたる事柄を挙げておく。

平成30年はパソコン演習室で実施した。教卓画面のスライド等の表示が画面転送で全席のパソコンに提示できる。参加者は最初と最後以外では殆どパソコン画面を見る状況であった。(パソコン演習室は来場者の動線からそれるため多少呼び込みもした。)

令和元年は、むやみに省くと参加者に伝わらないことを協力学生により念押しした。また、普通教室でプロジェクタスクリーンに投影した。プレゼン役はその横にいてパソコン操作もする。途中で2つ質問をする機会もあった。姿や身振りも見える位置であり、毎回ではなかったがアドリブ的にドラマや映画の特徴的なセリフを真似る回数がより多かった。

平成30年は、参加者に尋ねておらず理解度は不明であるが、低年齢の参加者を除き、数字の多いスライドでも殆どが注視していた。令和元年は途中で挙手で尋ねた(スライド19、20)。中には参加者が少なく挙手がない場合もあった。遠慮もあったと思われる。多いとき、児童・生徒6人中の5人以上が挙手した。釣られての挙手はないように思われた。

授業では令和元年夏に1年生の情報基礎Iで10分程度に縮めて提示した。映画のテレビ放映が夏にあることを知り、暗号の話題の先取りとして扱った(使用検定教科書にRSA暗号の説明はない)。最後に唐突に確認用のスライドなしで面白い性質とキモ

の理解を尋ねて、多いクラスで半数程度が挙手した。挙手を遠慮した学生もいた。現在、専攻科の担当科目も含め、事前提示課題を伴う活用を模索中である。

5 おわりに

暗号技術のひとつである RSA 暗号の原理を 23 程度でデモンストレーションする例を報告した。

余り計算が暗号として使用できる RSA 暗号のアイデアを小学 4 年生以上の多くの参加者が理解する。

今後、一層の時間短縮や、参加部分の創出や、理解に繋がる確認の方法やタイミングも検討したい。

本稿は 2019 年電子情報通信学会総合大会における発表¹⁰⁾をもとにまとめたものである。

謝辞

本校おもしろ科学フェスティバル等において支援頂いた方々や、工夫もしつつ小中学生等来場者に事前準備の上終日一生懸命にデモンストレーション等を行ったボランティアの支援学生各位に感謝します。

参考文献

- 1)中村博文: 誤り訂正技術のしくみのデモンストレーション例, 一小学校の剰余計算の学習のみを前提とするリード・ソロモン符号の変形例-, 都城高専研究報告, 第 52 号, pp.69-80, 2018
- 2)R. L. Rivest, A. Shamir, L. Adelman: A Method for Obtaining Digital Signature and Public-key Cryptosystems, MIT-LCS-TM-082(MIT Laboratory for Computer Science), 1977
- 3)いぶき: 映画サマーウォーズの暗号を京大生が解いてみた結果, <https://reienza.com/entame/summer-wars.html>
- 4)HKNEET: 【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方 2056 桁の暗号は解けるのか?, <http://win32programmer.seesaa.net/article/421790350.html>
- 5)まいとう情報通信研究会: サルにも分かる RSA 暗号, <http://www.maitou.gr.jp/rsa/rsa10.php> (以上 3 件の参照は 2017/12)
- 6)M. Gardner: A new kind of cipher that would take millions of years to break, *Mathematical Games*, *Scientific American*, 237(2), 120-124, 1977
- 7)D. Atkins, M. Graff, A. K. Lenstra, P. Leyland: The magic words are squeamish ossifrage, *Procs. of Asiacrypt '94*, pp.263-277, 1994
- 8)岩井恭著, 原作細田守: サマーウォーズ, 角川書店, 2009
- 9)アニメスタイル編集部編: サマーウォーズ絵コンテ細田守, スタイル, 2009
- 10)中村博文: RSA 暗号の小学 4 年生から大人までへの実演例 ー都城高専おもしろ科学フェスティバルにおいてー, 2019 年電子情報通信学会総合大会基礎・境界/NOLTA 講演論文集, A-2-1, p.21, 2019

付録

デモンストレーションで用いるスライド等の例を付図 1 に、その提示の際のシナリオ例を含むイベント出展での進行例を付表 1 に、配布資料の例を付図 2 に示す。

本報告では、説明の便宜上、スライド等に一贯した番号を付けているが、協力学生に配布しているシナリオ例においては、スライドは順に並んでいるという前提だけにして、通し番号は掲載していない。それは、シナリオ例配布後から当日までの判断でスライドの追加削除や移動があると無用になるためである。また、次の実施に向けた改善のための修正において、番号の対比の取り直しが必要なくなる。

進行例には、打ち合わせ等の際の記載箇所の特定の容易さから、項番ではなく行番号を付記している。協力学生への配布の際は、1 段組で空行を増やしている。それには、必要な設営に関する事柄も含めている。

おもしろ科学フェスティバルでは予め全出展のあらまし (Web ページではテーマ詳細と称している。出展毎に 1 ページである。本稿の出展において、内容は、付図 2 で示した配布資料例から QR コードを除いた内容と殆ど同じである。) を本校の Web ページで公開している。この行事においては、小学生向けに使用漢字に配慮することになっている。本稿の出展に関するものは、小学 4 年生以上で習う漢字をルビ付き若しくはひらがな表記としている (筆者はオレンジ工房 “小学校で習う漢字チェックツール” <http://orange-factory.com/tool/kanjicheck.html> で確認した)。

参加者への配布資料は、準備の都合から、これまでのところはモノクロである。おもしろ科学フェスティバル終了後でもスライドや配布資料のカラー版 (付図 2 はその例を 93% に縮小したものである) を見て頂き易いよう Web 上に掲載し、配布資料にはその QR コードを印刷している。

付表1 出展等での進行例 (1) その1/5

1 ※進行例(プレゼンのシナリオ例を含む)	63
2	64 以下、30分毎(計10回)の1回分の内容。
3 留意事項	65
4 ・余りの計算(小学3年で学習)が分かる4年生なら、わり算	66 (ここから。始まりの5分前位に、前の担当者と交代。)
5 の余りの面白い性質と、RSA暗号のキモと、映画との関連	67 (始まる前、適宜案内：前側から詰めてください。)
6 (わりと有名な暗号クイズと、その解説も)が分かること。	68 (案内役(余裕があればプレゼン役やフリーな人も手伝う。)
7 ・入室した人は聞く気である。導くつもりで、「難しい	69 が、着席を促しながら、各席にもれなく、プリントを裏返し
8 ですね」などというやる気をそぐ言葉を絶対に安易に挟ま	70 で置く。配布中に参加者が手を出されたときは、手渡しする。
9 ないこと。	71 参加者が読んでものがめない。白紙等は取り替える。)
10 ・プレゼンで、「暗号」と「解説」、途中から「RSA暗号」	72 (プレゼン役は、PC画面がスクリーンに表示されている
11 も、という用語を使うが、これら以外の「積」、「剰余」、「素	73 ことを確認。wxMaxima が起動中であることと、テキストエ
12 数」、「素因数分解」、「アルゴリズム」、「鍵」、「暗号化」、「復	74 ディタでプログラムを開いていることも確認。wxMaxima に
13 号」、その他の、用語は一切使わないこと。スライドや後述	75 前の回でのプログラムが残っていたら、エンターキーを2
14 の進行例に含めたものだけは、例外的に用いる。	76 0回位押し画面を流しておく。毎回新規画面でも可。)
15 ・参加者のために、0分か30分丁度での開始、23分以内	77 (参考：テキストエディタから最初のプログラムを切り貼
16 のプレゼン、25分以内で部屋の外まで、を厳守。	78 りするとき、前回のプログラムが見えない方が良いので、文
17 ・参加者はネット上の記事や当日の配布物などを全く読ん	79 字サイズや空行挿入等で調整しておく方が良い。)
18 でないという前提で、参加者が迷わないよう進める。	80
19 例：多いなら教室外で整列、入室～着席、席へのプリント	81 ■1 (プレゼン役がスライド1ページ目を表示。)
20 配布、プレゼン、退室アナウンス～教室外へ。	82 (プレゼン役は、pptのスライド表示が最初のページで
21 整理券は使わない(以前は発行した)。入口(教室後ろや廊	83 あることを確認。違ったら最初のページにする。出展中ではな
22 下)に3分前以降、来られていた順に、席の分だけ入室を。	84 いなどと勘違いされないよう表示しておく。)
23 ・この資料(及び、スライド等の資料)は書き込み可。当日	85 //開始直後前方に注目が行くようタイトルのみ表示。
24 終了後、要らなければ回収。今後の差し替え分も同様。	86 (30分毎の開始時刻までには、着席を終えているように
25 ・サマーウォーズは、映画の他に小説複数とコミックス等が	87 する。教室の内外で適切に入室や着席の案内を。)
26 ある。OZ(オズ)の管理センターの認証パスワードの後部	88
27 の具体的な文章と、その暗号文全体の具体的な数字と、Sh	89 (0分と30分に開始するために。)
28 orの方法の記事を見ているシーンは、印刷媒体にもある。	90 (プレゼン役は、原則、時間通りに開始。万が一、大勢の入
29 スライドでの提示は、文字情報に留め、出典を(配布資料等	91 室が遅れている場合でも1分以上遅らせない。でない、時
30 に)記して引用で済む範囲だけにする。	92 間が決まっている別の予約がある人に迷惑。必要なら、途中
31 //画像は安易に使うと集中の妨げになるため用いない。	93 で、おまけの3つ目を飛ばして時間調整。)
32	94 (案内役は、開始時間直前に、適宜、教室前後のドアを閉め
33 ・予め、各回のプレゼン役と案内役を決めておくことにする	95 る。遅刻者へは、次の回に来れない事情があるか尋ね、待て
34 (表を用意するので、それに記入)。	96 ないときは、空き席、または立ち見の、場所を案内する。着
35 ・小学4年生が、余りのおもしろい性質と、RSA暗号のキ	97 席または移動を見届ける。)
36 モを、理解するという趣旨が変わらなければ、細かい表現や	98
37 細かい例示はアドリブで変えて構わない。	99 ★適宜挨拶(皆さん、こんにちは)★この辺りで、学科や
38 但し、下記の進行例の、順序だった説明の互いの関連性や、	100 学年や名前等の一部を名乗るかどうかは任意。
39 小学4年生以上が対象だということを忘れないように。	101 これから、外に出るまで、25分くらい、時間を頂きます。
40 ・勝手に内容を省かないこと。文を抜かないこと。省略は、	102 席にプリントを配っていますが、今は裏返しにしてい
41 思考が繋がらなくなるので不可。言い換えは可。	103 ださい。
42 (過去にはそういう大小の失敗例があった。)	104 では、始めます。
43 ・無理しなくてよいが、小さいながらも、いくつか山場や笑	105 //ターゲットをひとり程度決めて、その子供には分か
44 いを取ってもよい所がある。または、作れる。	106 ってもらつつもりで話すのもよい。でも、他の人から嫉妬さ
45 ・以下で指示した以外にも、間を入れるとよい。間は大事。	107 れないように。
46 但し、退室開始まで23分以内を厳守。	108 ■2 (このスライドは、雰囲気のためのもので、中身の直
47 ・以下は、基本的な流れである。頭に入れれば見なくても良い	109 接の解説を今はしない。)
48 し、抜けるよりは、読みながらの方がよい。	110 『暗号』というのは、ほかの人に分からないように、デー
49 ・以下で、■はスライド進行(切り替え)、◆はアニメーシ	111 を作り変えることです。
50 ャン機能でのスライド内進行、●は別ソフト操作、★は各自	112 そして、それをあばくことを、『暗号解説』とか『解説』と
51 が考えて適宜行動。()は追加指示。丸かっちは、重要では	113 いいます。
52 ない、という意味ではないので、注意。	114 ここでは、短く、『解説』ということにします。
53 スライドは、例えばエンターキーで次ページへ。動きを出す	115 映画とか小説などの『サマーウォーズ』では、暗号や、解説
54 機能は、不注意や環境によるコマ飛びの懸念から、使わない。	116 のシーンが、当たり前に出てきます。
55 :☞はマウス(または、レーザーポインタ)での指示。これ	117 ★必須ではないが、時間的余裕が確かなら映画を観た人が
56 が無い所でも、参加者はほぼスクリーンしか見ていないの	118 どれくらいか、挙手で尋ねてもよい。
57 で、マウスポインタ(または、レーザーポインタ)の活用は必	119 (必須ではないが、次の3項目は、指を伸ばしながら数える
58 須。その際、操作が速すぎると、伝わらないので注意。	120 ようにするしぐさを交えるのも一手。)
59 「//」の右側はメモなので、読まないこと。不用意に話題に	121 サマーウォーズは空想の話ですが、シーンのいくつかは、
60 混ぜると時間オーバーになる。	122 『実際の暗号』や、『わりと有名な暗号クイズ』や、『その解
61 ・全体の所要時間の不確定度が特に高くなるのは、入退室、	123 読』と関連している所があります。
62 操作ミス、そしてアドリブ部分である。	124 今日は、この三つを、確かめます。

付表1 出展等での進行例 (2) その2/5

125 //「自分で調べたい方は、これからの話を聴いてはいけ	187 でも、本当は難しさは変わっていないということを、皆さん
126 ません。」というのは、言わないでよい。省略。	188 は見抜いてください。(←省略不可)
127 暗号以外では、ネタバレがないようにします。(うまく言っ	189 では…。
128 て笑ってもらってもいい所ではある。)	190 //次のスライドは、コントロールキーとスクロールボ
129 用語を、ほとんど使わずに進めますが、暗号の基本は、押さ	191 タン等で、適宜拡大縮小をしてもよい。
130 えるつもりです。	192 ■7 この表は、ひとつ一つ、きまじめに計算した結果です。
131 わり算の余りを習っていれば、分かりますので、頭フル回転	193 (これを見た人が量でびっくりするプレゼンはダメ。)
132 で、しっかりついてきてください。	194 さっきの、『2』をかけていったのが、この表では、黄色の
133 大人の方(かた)も、ぜひ一緒に聴いてください。	195 行です。
134 //お子さんと後で話されるために。とか、油断すると大	196 1つ:☒:で2、2つ:☒:で4、ずっと行って、11個:
135 人でも分からなくなります。も省いてよい。	197 ☒:で元と同じ2、21個:☒:でも同じ2でしたね。
136 ★このあとは、小学生の方(かた)向けの言葉遣いで話しま	198 11個の所:☒:から後ろは、繰り返しになっています。
137 す。目上の方(かた)は、ご了承ください。	199 今日は、『21個かけた余り』に注目します。緑の列です。
138 ここからは、前のスクリーンを見ながら聴いてください。	200 もしも、かける回数が1回でも違うと、殆どが、元に戻りま
139 ■3 この順番で進めます。	201 せん。
140 余り:☒:、余りのおもしろい性質、余りの暗号への応用、	202 例えば、2:☒:を20個なら1:☒:ですし、22個なら
141 科学雑誌の暗号クイズと解説、サマーウォーズでの扱い、お	203 4:☒:です。2にはなりません。
142 まけ、です。	204 ほかに、例えば、3:☒:を21個かけて33で割った余
143 //あまり せいしつ あんごうへ クイズ かいどく え	205 りは3:☒:になっています。
144 いがで おまけ 共通見出し行をずっと表示	206 4:☒:なら4:☒:になっています。
145 『サマーウォーズ』に出てくる暗号は、割り算の余りのおも	207 ひとことで言うと、この列:☒:と緑の列:☒:が同じです
146 しろい性質を使っています。	208 ので、21個かけると元と同じ数になると言えます。
147 ここで、割り算の授業はしませんが、軽一く、おさらいをし	209 ★次行は単に読むだけでなく、決して必須ではないが、可能
148 ておきます。	210 なら、セリフはドラマに似せて言ってみる。
149 (以下では、「2の3乗」や「2を3回かける」(←×算は2	211 『ガリレオ』というドラマのセリフで、『実に、おもしろい』
150 個)ではなく、「2を3回かける」のように言うこと。)	212 というのがありますが、まさにそれです。
151 ■4 例えば、64÷33なら、33がひとつと、引いて、	213 このおもしろい性質がサマーウォーズの暗号の種だという
152 余りが31です。	214 ことが、すぐ後で分かります。
153 16÷33なら、余りは16です。	215 //そのときには、今のが実におもしろい性質なんだと
154 このあとは、余りだけ注目します。	216 いうことが改めて分かるはずですよ。
155 ですので、矢印を使って、この:☒:ように余りだけを書く	217 おさらいですが、かけ算した余りには、11個とか、21個
156 場合があります。	218 という、かけ算の特別な回数るときには、元と同じ数になる
157 今度は、2を、どんどん繰り返しかけてみます。	219 という、おもしろい性質が確かにありますね。:☒:
158 ■5 どんどんかけながら、33で割った余りを次々と書	220 //ここに後ろの内容理解の確認を持ってくるのも一手。
159 くと、こんな風になります。	221 ★少し間を置く。
160 ★計算はやってあります。★それを使います。★33で割っ	222 2のかけ算で、もう少し続けます。
161 た余りだけ注目します。	223 ■8 21という値は、3×7ですので、21個かけるのは、
162 2だけなら余りは2、2×2は4で、割った余りは4、2が	224 3つ分ずつを、7つまとめても同じです。
163 3つなら8で、余りは8という具合です。	225 3つ分かけたら8ですので、8を7つかけても、余りは元と
164 2が6個なら64で、余りは、さっきのスライドと同じで、	226 同じ、2になっています。
165 31です。	227 ★少し間を置く。
166 2が7個のときは、計算してあります。29です。	228 ここには書いていませんが、6つ分なら25です。8つ分な
167 このあとは、かける個数で表します。	229 ら16です。元の2には戻りません。
168 //かけ算記号ではなくて、数字の個数に注目します。	230 ★少し間を置く。そして、ゆっくり言う。
169 すると、こんな、:☒:風に、短く書けます。2を7つかけ	231 言い換えると、7つ分ということを知らない人は、元の数に
170 て33で割った余りは29、という具合です。	232 は戻せないということが言えます。
171 //かけて、33で割ることを、…	233 //言っていることが分かりますか?//時間の余裕がな
172 もっと続けます。	234 いので念押しはし難いが、分からなさそうなら念押しを。
173 ■6 こんな具合です。8つかけた256での余りは、25	235 ◆つまり、3つ分ということと8は誰に教えてもいいので
174 です。	236 すが、7つ分ということを知っている人だけが元に戻せる
175 ずっと続けることができます。33で割った余りですので、	237 という事なので、2を秘密にして送るための、暗号として
176 余りは0から32までの33通りしかなくて、2を何度も	238 使えるわけです。
177 かけていくと、いつかは必ず繰り返しになります。	239 ★少し間を置く。
178 例えば、2を11個かけたら2048で、余りを計算すると	240 2だけではなくて、3でも4でも5でも、3つかけたのは、
179 2です、21個かけても余りが2です。	241 7を知る人だけが元に戻せます。
180 //こんな風に繰り返しになります。	242 これが今日のキモです。//おもしろい性質も、キモも、個
181 2だけではなくて、ほかの数でも、何度もかけるのをやって	243 数はそれぞれ、全体でひとつだけになっている。
182 みました。次のスライドで見せます。	244 繰り返しですが、3つかけたデータは、7を知る人だけが元
183 先に言っておきますが、ひとつの表にまとめましたので、デ	245 に戻せるというのが、今日のキモです。
184 ータが沢山あります。	246 これはさっきのおもしろい性質の応用です。//時間の余
185 今日の話だけでなく、かすが増えたり、数(すう)が大き	247 裕がないので念押しはし難いが、必要そうなら念補足を。
186 くなっただけで、難しいという人がいますが、	248 ★少し間を置く。

付表1 出展等での進行例 (3) その3/5

249	7を知らなくても、数が小さいときは、かけ算を2回、3回、	311	算してみます。
250	4回と順に試して、すぐに7つを試せますが、普通はとても	312	(切り貼りする。) //手間だが計算を感じてもらいため。
251	大きな数にして、単純に試すだけなら世界中のコンピュー	313	●(wxMaximaの画面を表示して。)(wxMaximaでの実行は、
252	タを使っても何百年とか、何億年とか、もつととか、かかる	314	シフトキーを押しながらエンターキーを押すこと。)
253	ようにしています。	315	この:☞:ように7が計算できました。ついでに、8を、7
254	この暗号には名前がついています。(これは、いきなり感を	316	つけた余りも計算していて、元の2が得られています。
255	なるべく出さないようにするための一言である。)	317	(実行結果は、前の表示を流用ではなくて、その都度実行さ
256	◆3人の発明者の頭文字をとって『RSA暗号』です。	318	せない臨場感がない。)
257	サマーウォーズにでてくる暗号は、実は、このRSA暗号で	319	今のように計算できたので、『RSA暗号は、暗号として
258	です。理由は、後で分かります。	320	うだめ』かという、そうではありません。
259	//そういう切れる理由は、今日の話最後まで聴いた	321	33のように小さい数ですと簡単に3と11をかけたと分
260	ら分かります。	322	かりますが、暗号クイズのように100桁くらいとか、更に、
261	★ところで、このようなうまいことができるのは、実は、3	323	サマーウォーズのように1000桁以上とかに増やすと、
262	3が、3×11のように、2つの数をかけた数だからなん	324	かける前の2つの数を求めるのに必要な時間が、どんど
263	です。このことは、今日は深入りしません。ご了承ください。	325	増えます。
264	おさらいをしておきます。	326	速い方法を、人類はまだ見つけていません。
265	■9 2を3つかけて、33で割った8を送ります。	327	もし、ここにいる誰かが発明したら、きっと名前が残ります。
266	7というのを知っている人だけが、7つかけて余りを求め	328	でも、悪い奴から見て、この子は暗号やぶりに役立つと思わ
267	て、元の2に戻せます。	329	れたら、誘拐されるかも知れません。(この辺りは、うまく
268	7つでなくて、近い回数、8つでも、6つでも元の2には	330	笑いを取ってもよい所。)
269	戻せません。	331	//殆ど冗談です。が、可能性はゼロではありません。//
270	//ここに後ろの内容理解の確認を持ってくるのも一手。	332	今は、ブラックユーモアです。//半分だけ冗談です。
271	このRSA暗号を使って、暗号クイズが出されました。	333	半分冗談です。(この辺りも、うまく笑いを取ってもよい所。)
272	■10 サイエントフィック・アメリカンという有名な	334	さて、さっきのクイズは129桁でしたので、なかなか2つ
273	一般向け科学雑誌で、マーチン・ガードナーという人が、1	335	の数に分けられなかったのですが…。
274	977年に出した、暗号クイズです。	336	■14 アトキンスという人や仲間が、ネットで呼びかけ
275	//RSA-129という言い方もされます。//上記	337	て、大勢の協力をもらって成功しました。
276	雑誌和訳本は日経サイエンス。近年のは本校図書館にも。	338	★約20か国の、約600人の協力をもらって、
277	暗号を解いたら100ドルもらえるという懸賞問題でした。	339	★約1600台のコンピュータを使って、8か月かかった
278	当時の2万円くらいです。桁数が多いです。びっくりしな	340	そうです。
279	いでください。(難解と思われたいよう前もって言うておく。)	341	1994年に結果が発表されています。
280	これです。	342	千年以上解読はできないという予想もありましたが、クイ
281	■11 さっきの例も、左側に載せています。	343	ズが出されてから17年で解読されました。
282	位(くらい)が多いです。一行で書き切れないので2行で書	344	それで、約1600台のコンピュータで、8か月かけるま
283	いています。ひとつの数です。	345	では持ちこたえたわけです。
284	ここ:☞:は129桁です。1万を32回かけたくらいの数	346	//★皆さんは、この解読にかかった期間を、短いと思
285	です。	347	ますか、長いと思えますか。//少し間をとる。
286	左側に書いたさっきの例と比べると、これ:☞:やこれ:☞:	348	サマーウォーズはSFですので、もっとけた数の多いのを、
287	が分かっている、これ:☞:やこれ:☞:分からないわけ	349	健二君が紙と鉛筆を使って一晩で解くシーンとか、鼻血を
288	です。	350	こぼしながら暗算で解くシーンもあります。(せりふも入れ
289	クイズが出たときは、解読に、千年くらいかかるとか、もつ	351	て、取れたら、笑いを取ってもよい所。)
290	とかかかるとか、言われていました。	352	でも、実際は、RSA暗号の解読は簡単ではないので、今も
291	//例えば、4年かかるとか、言われていました。	353	世界中で使われています。買い物などでは当然ですが、最近
292	京は1万を4回かけた数です。	354	は普通のホームページでも、何を見ているか、ほかから知ら
293	映画のサマーウォーズと違って、実際の解読は楽ではあり	355	れないようにするためにも、よく使われます。
294	ません。でも、方向性はいくつか考えられています。	356	さて、暗号クイズの、解読の続きです。
295	サマーウォーズで、健二君の解読方法の説明はありません	357	●15 (テキストエディタのプログラムを表示して。)
296	が、ひとつだけ、お話しします。	358	暗号にするときにかける個数がここ:☞:、アトキンスたち
297	先ほどの例を使います。	359	が突き止めた、割る数のもとになっていた2つの数がこれ:
298	■12 まず、33は、3と11をかけたものです。	360	☞:とこれ:☞:です。プログラム:☞:はさっきと同じ
299	個数を表していたここ:☞:の3と、今の3と11とで、あ	361	ものです。//「同じ」を強調したいが、さりげなくでよい。
300	る方法、ここでは名前だけにしますが、『拡張ユークリッド	362	(切り貼りする。)
301	の互除法』というものです、それを使うと、計算で、7が分	363	●(wxMaximaの画面を表示して。)(wxMaximaの実行は、シ
302	かります。	364	フトキーを押しながらエンターキーを押すこと。)
303	今ここにあるパソコンで、計算してみます。	365	もう終わりました。かける前の数が分かっていると、こんな
304	●13 (テキストエディタのプログラムを表示して。)	366	に速いんです。
305	3と3と11というデータがここ:☞:です。ここ:☞:	367	データを元に戻すためにかける個数が、ここ:☞:に求まっ
306	は、説明は省きますが、コンピュータ・プログラムです。小	368	ていますので、解読ができます。
307	学生がローマ字の練習をするよりも、字数はざっと少ない	369	これ:☞:を、この個数だけ:☞:かければよいわけです。
308	です。//プログラムは短く作ってある。不十分な所もあ	370	今ここで気付いた人がいるかも知れませんが、もしも、この
309	る。これを読んでいるあなたは読解できるだろうか?	371	個数だけ、本当に気まじめにかけ算するのを待っていると、
310	これをマクシマ(Maxima)というフリーソフトで、今から計	372	みーんな、今日は家に帰れません。(面白くしてもよいし、

付表1 出展等での進行例 (4) その4/5

373	無理して笑いを取らなくてもよい) //富岳で頑張っても。	435	したからプレゼンがまずいということではないので、気に
374	//太陽が燃え尽きるまで待っても、終わりません。	436	しないように。
375	でも、うまい方法があって、今日は深入りしませんが、『バ	437	(上記について補足:当日ではなくて事前に、3つ目のおま
376	イナリ法』という方法で高速化しています。	438	け1枚にかかる時間を計っておいて、正確に何分以降なら、
377	それで計算して解説したデータが、これ:☹:です。	439	全体が23分以内で終わらなくなり1枚スキップすべきか、
378	これを、さっきの表にまとめてみます。	440	時間把握をしておくことが望ましい。)
379	■16 解説して、これ:☹:が分かったわけです。(着	441	
380	色してあるので、色を言うのと分かりやすい。)	442	// (おまけの1つ目)
381	次に、この数:☹:の意味の取り方を説明します。	443	■21 サマーウォーズでは、健二君が『モジュロ演算』と
382	暗号クイズでは、もともと、数字が2つずつ:☹:,文字と	444	いう言葉を、1回だけ使います。
383	対応させてありました。	445	意味が分からなくても、映画を観るのに困りませんが、
384	ですの…。	446	モジュロ演算は、『余りを求める計算』という意味です。今
385	■17 さっきの:☹:を、ふた桁ずつで区切ると、こう:	447	日、何回も出てきた計算のことです。
386	☹:になります。	448	サマーウォーズでは、西暦の年と月(つき)と日の数字から
387	最初の20はT:☹:と対応します。次の08はHと対応し	449	『曜日』を求める話が出てきます。
388	ます。次の05はE、次の00は空白です。	450	それは、暗号とは無関係です。でも、余りを使います。言わ
389	//最後の05は、Eと対応していて、最後のここ:☹:	451	ば、『余りつながり』の話題です。
390	のEです。	452	//数を数えたときに、7で割った余りに注目すると、0
391	このような:☹:文字の並びが得られて、これで暗号クイズ	453	~6の繰り返しです。
392	の解説が完了です。 //パチパチ。	454	『日曜日から土曜日』を、順に数字の『0から6』で表すと、
393	//メッセージは「魔法の言葉は squeamish	455	曜日が、数で扱えます。
394	ossifrage(気難しいヒゲワシ) //ossifrage (骨折り)	456	年と月(つき)と日の数字から、正しく0~6が出てくるよ
395	//最後の単語:☹:に、「骨の折れる仕事」の意味があ	457	うにうまく調整した数式が、いくつかあります。
396	るのを利用した、ジョークだそうです。	458	『ツェラーの公式』というのが有名です。
397	最後の単語が、お疲れ様のような意味があって、出題したガ	459	//本題の暗号の印象が薄まるので公式は表示しない。
398	ードナーからの解説者へのジョークだそうです。 //うま	460	//どちらも、割った答えの、1より小さい部分は捨てる
399	く笑いを取ってもよい。少し間を置いてよい。	461	ようなわり算を何回か使います。
400	さて、肝心の、サマーウォーズで、どうだったかという…。	462	3000より大きい数は出てきませんので、皆さんも、頑張
401	■18 このように:☹:読みやすいように小文字も使って	463	れば、時間はかかっても、暗算でできます。
402	あって、更に文が追加されていました。これが、『オズの管	464	//サマーウォーズの健二君は、速かったですね。 //2
403	理センターの認証パスワード』だったということでした。	465	1世紀だけならもっと簡単になります。
404	それから、サマーウォーズでは、『2056桁の暗号』とい	466	★飛ばして可:ちなみに、僕/私が初めて暗算したとき、自分
405	う言い方になっていました。	467	の誕生日の曜日を求めるのに★秒かかりました。
406	その中に、暗号クイズにあった、緑のこのあたり:☹:の数	468	//世の中には計算しないで曜日が分かる人が少しいま
407	字は、大部分がそのまま使われています。	469	すが、その話は、ここでは深入りしません。
408	このことから、サマーウォーズに出てくる暗号はRSA暗	470	これは、ここまでの紹介にしておきます。
409	号だろう、と推測できます。	471	//7で割った余りで曜日が決まります。//式解説は省
410	//オズ(OZ) //今度映画で確認してみてください。	472	く。 //公式を使いMaximaか何かで参加者の年月日で計
411	//2056桁に何を含まかは実際は明確ではない?	473	算してみせるのもとりあえず省く。個人情報保護をどうク
412	//この緑の数:::は、皆さんがあとで調べなくてい	474	リア?
413	いように、配布プリントに載せておきました。	475	//今日の日付で計算すると、ゼロで、日曜と分かります。
414	★少し間を置く。	476	
415	ちょっと、振り返りの質問をします。(聞き方はアレンジし	477	次のおまけです。
416	ても差し支えない。) //そもそもだが、プレゼンの初めで、	478	■22 // (おまけの2つ目)
417	確認することを、何らか断っておくかどうかは任意。	479	RSA暗号は、3や11のようなかける前の元の数が、もし
418	(中村がいなくて、プレゼン役は、次の2問の挙手者数を	480	分かると、すぐ解説できる、ということ、を、さっき確認しま
419	記録。退室前までに全人数や小3以下人数も記録。)	481	した。
420	■19 サマーウォーズの暗号は、21個かけて33で割	482	かける前の数を求めるに、『ミクロの世界』でだけできるこ
421	った余りが、元に戻る、というような、余りのおもしろい性	483	とを、利用した方法が、発明されています。
422	質を使っていました。余りにこのようなおもしろい性質が	484	『ショア』という人の発明です。(ここでもできるだけいき
423	あることは分かっている、という人は、手を挙げて知らせて	485	なり感を減らすためこんな言い方をしている。)
424	ください。	486	//アルゴリズムというのは計算手順とか処理手順とい
425	■20 サマーウォーズの暗号のキモは、◆同じ数を3つ	487	う意味です。//今はアプローチが量子ゲート型だけでない
426	かけた8という値は、更に7つかけることを知っている人	488	//注意:ショアが発明したのは量子コンピュータでは
427	だけが元に戻せるということでした。これが分かっている、	489	なくて、それを使った素因数分解アルゴリズム。
428	という人は手を挙げて知らせてください。	490	でも、その方法を使うには、特別なコンピュータが必要です。
429	(少し間をおいて) ありがとうございます。	491	今、覚えなくてもいいですが、『量子コンピュータ』:☹:と
430	サマーウォーズの暗号については、ここまでですが、この後、	492	いいです。
431	すこしおまけを追加します。	493	//最近、ニュースになったりしています。
432		494	これ:☹:が、もしも実用化されると、RSA暗号は使いも
433	★ここで判断。もし例えば約18分以上経過していたら、3	495	のにならなくなります
434	つめのおまけとその説明は飛ばす。おまけの3つ目を飛ば	496	でも…。

付表 1 出展等での進行例 (5) その 5/5

497	■ 2 3 //可能ならよりおもしろいスライドを置きたい。	559	で、外に出さないのは、この 7 だけです。
498	安心してください。	560	復号をすると、元と同じひらぶんが得られます。今日の例で
499	なぜ安心かという、世界中で研究していますが、と一っ	561	は『2』: ☹: のことです。
500	も難しく、本格的な実用化はまだ先だ、と言われていま	562	
501	// RSA 暗号はコンピュータの処理速度の進歩に合わ	563	さて、今日(きょう)は…。
502	せて桁数を増やしていけば大丈夫と言われていま	564	■ 2 6 これらを確認しました。(時間がないので、原則、
503	//量子コンピュータの扱える桁数は、2 0 2 0 / 9 1	565	スライドの字を読みあげないこと。)
504	BM公表 6 5 ビット; 2 0 2 3 に 1 1 2 1 ビット公表予定	566	★以下の 6 行は、時間があるなら言う。ゆっくりと。
505	■ 2 4 映画では、誰かがショアの方法の記事を見ている	567	サマーウォーズに出てくる暗号は、今も使われている R S
506	シーンが、ちらっと、最初から最後までどこかで、出てき	568	A 暗号のようでした。映画で最初に出てくる解読結果には、
507	ます。このつづり: ☹: も出てきます。まだ気が付いていな	569	科学雑誌の暗号クイズと同じ部分がありました。
508	い人は、今度映画を観るときに気を付けて探してみてください。	570	R S A 暗号が、今も暗号として使える理由は、余りを求める
509		571	ための 3 3 のような数を大きくしたとき、かける前の 3 や
510	//健二君は量子コンピュータではありませんが、	572	1 1 のような数を求める速い方法が、まだないからでした。
511	そのようなシーンがあることも、映画の暗号は R S A 暗号	573	
512	だろうとか、健二君は数をふたつに分ける計算をしたのだ	574	パソコン画面はここまでです。
513	らうと、推測できる根拠です。	575	■ 2 7 //最後の表示スライドはタイトルのみのもの。
514	//先のことですが、もしかしたら、今の小中学生や高校	576	入退室後入ってきた次の人が、見てもよい内容である。
515	生の皆さんの子供の世代は、高校で、量子コンピュータにつ	577	計算で機能を持たせる技術は沢山使われています。データ
516	いて教わるような時代になっているかもしれません。	578	を守る暗号以外では、例えば、印鑑やサインと同じことをデ
517		579	ータだけでする技術や、2 次元コードのように少しデータ
518	(おまけの 3 つ目は、残り時間によっては、「配布物にある	580	が消えても壊れても直す技術や、データの量を減らす技術
519	ことですので」などと言って、飛ばしても可。)	581	や、電波や電気一度に沢山のデータを送る技術です。
520	★最後のおまけです。	582	//今日は、データを守る暗号技術について、一部だけ、
521	// (おまけの 3 つ目)	583	お話ししました。)
522	暗号について、いろいろ調べたい人も、いるかも知れませ	584	
523	でも、暗号関係の本やホームページは、基本的な用語でも、	585	机の上に配っているプリントには、もう少し、追加して書い
524	説明なしに使われていることが多いです。	586	てあります。家で読んでください。//今読まないでという
525	特によく出てくる用語を、いくつか紹介したいと思います。	587	意味。
526	すこーしだけ、お勉強をします。これから 2 分間くらいは、	588	大人の方(かた)も、持って帰ってください。(もし複数枚
527	寝ててもいいです。(笑いを取っても良い所。)	589	持って帰る人がいても、大目に見る。)
528	//高専の学生にもたまに寝ている人がいます。とかは	590	この部屋は、前から、出られます。//部屋によって適宜
529	言わない。失望する人がいてもいけないため。	591	退室の際は、忘れ物がないようにお願いします。
530	後で見られるように配布プリントに書いてありますが、今	592	
531	は、パソコン画面を見てみてください。	593	以上で終わりです。
532	//ここまでで暗号のひとつである R S A 暗号のしくみ	594	★適宜お礼 (ありがとうございました。)
533	が分かりましたので、それになぞらえて紹介します。	595	では、退室してください。
534	さっきの例になぞらえて紹介します。	596	(プレゼン役は、教室前側のドアがあるなら開ける。)
535	■ 2 5 まず、暗号を使う前の、もとのデータのことを『ひ	597	(プレゼン役は、次のために、スライドを 1 ページ目にして
536	らぶん』: ☹: といいいます。専門家はこの字をひらぶんと読	598	おく。また、wxMaxima は、エンターキーを 2 0 回押して
537	みます。今日の最初の例では『2』: ☹: のことです。	599	画面を流しておく。別画面を作ってもよい。)
538	それを分からなくしたデータを、『暗号文』: ☹: といいいます。	600	(案内役は、後部入口のドアを開ける。混み合うとき、退室
539	今日の例では『8』: ☹: のことです。	601	優先や、次のグループに待って頂くことや、入室のタイミン
540	//ひらぶんから、暗号文を作ることを…	602	グを、適宜アナウンス。)
541	暗号文を作ることを『暗号化』: ☹: といいいます。	603	(プレゼン役と案内役は、忘れ物が無いか、もし有ってもで
542	暗号化はデータを作り変えているのですが、どう作り変え	604	きるだけ早く発見してあげられるように留意。)
543	るかを指示するデータを、『暗号鍵』: ☹: といいいます。ちょ	605	(プレゼン役、案内役とも、次の担当者に引きつぐ。)
544	っとカッコいい響きの言葉です。	606	
545	今日の例では『3 と 3 3』: ☹: のことです。初めての人は、	607	その他
546	鍵という言い方が、少し変に聞こえるかもしれませんが、分	608	ここからは中村用のメモ。読まなくてもよい。
547	からないように『封印するための鍵の役割』と思ったらいい	609	シナリオ例その他を予め読んでおくことを念押し。
548	です。	610	可能ならスライドを電子データで見られるように(また
549	暗号文を元に戻すことを『復号』: ☹: といいいます。復号に	611	は、Web 掲載。)
550	は『化ける』という漢字を付けられないのが普通です。	612	この出展の協力者は昼食時以外に後学のために 4 0 分程
551	復号もデータを作り変えているのですが、それを指示する	613	度離れられる時間を設けることを伝達(連続する 1 時間の
552	データを、『復号鍵』: ☹: といいいます。	614	始まりと終わり以外か、3 0 分の始まりと終わり以外を 2
553	今日の例では『7 と 3 3』: ☹: のことで、『封印を解くため	615	回、但し、朝から 2 回目までは仮に非番でも抜けずに互いに
554	の鍵の役割』だと思ったらいいです。	616	他の学生の動きを見ておくこと。)
555	復号鍵がばれると、暗号になりませんので、この復号鍵を、	617	当日の服装は任意(状況にもよる。)
556	部外者には教えないようにします。	618	できるだけ事前に飲み物代プラスアルファ位までは、
557	//今日の例で復号鍵は 7 と 3 3 のことですが、	619	用意: ローテーション記入用の表、張り紙を全て。
558	3 3 : ☹: は、暗号鍵: ☹: にもありますので、R S A 暗号	620	整理券を用いる場合には印刷して用意、整理用の箱も。

Microsoft Teams を活用した遠隔授業の成果

臼井昇太¹・藤川俊秀²・米満忍³・岡元隆洋³・山下敏明⁴

The Accomplishment of Distance Education Utilized by Microsoft Teams

Shota USUI¹, Toshihide FUJIKAWA², Shinobu YONEMITSU³,
Takahiro OKAMOTO³ and Toshiaki YAMASHITA⁴

(Accepted September 30th, 2020)

Abstract COVID-19 occurred in China, its infection spreading in the world wide even now. The infection spread of COVID-19 brought about many changes in Japanese education. That influence extended to the National Institute of Technology(KOSEN). One of KOSEN, Miyakonojo College, employed remote teaching to prevent infection spread of COVID-19 from May 2020. Moreover, we organized "The remote teaching construct and operation team" to construct and operate the remote teaching. This team is constructed with the remote teaching system by Microsoft Teams and operated from May to September 2020. This paper deals with the contents of activities and outcomes for our college's remote teaching from the remote teaching build and operation team's perspective. In the following text, we explain the background to implementation in section 2. In sections 3 and 4, we focused on the movement after the operating and the remote teaching system's achievements and problems. In section 5, the results obtained are summarized.

Keywords [Construction of a remote teaching system, Remote teaching operation, Distance education, Microsoft365 Microsoft Teams]

1 序論

2019年12月に中華人民共和国湖北省武漢市で発生した新型コロナウイルス感染症(以下、COVID-19)は、2020年9月の時点においても世界規模で広がっており、いまだ深刻な状況が続いている。我が国においても、2020年1月に初の感染者が確認されて以

降、その広がりには全都道府県にまで影響を及ぼしている。日本政府は国内での感染拡大を抑制するために、同年2月27日に全国の小中高校に対して3月2日からの臨時休校を要請し、4月7日付で7都府県に対して緊急事態宣言を発令、その後、全都道府県に対して4月16日付で緊急事態宣言を発令した。多くの高等教育機関では、文部科学省および国立高

1 都城工業高等専門学校電気情報工学科 Department of Electrical and Computer Engineering, National Institute of Technology(KOSEN), Miyakonojo College
2 都城工業高等専門学校機械工学科 Department of Mechanical Engineering, National Institute of Technology(KOSEN), Miyakonojo College
3 都城工業高等専門学校学生課教務係 Student Affairs Division, National Institute of Technology(KOSEN), Miyakonojo College
4 都城工業高等専門学校物質工学科 Department of Chemical Science and Engineering, National Institute of Technology(KOSEN), Miyakonojo College

等専門学校機構本部（以下、高専機構本部）からの通達に基づき、学生の入構を制限し、前期科目を対面型の授業から遠隔型の授業に切り替えて開講した。都城工業高等専門学校（以下、本校）においても、学生と教職員の感染を防ぎ、かつ「学びを止めない」という高専機構本部の方針に重きを置き、対面授業から遠隔授業に切り替えて前期開講科目を実施することを決定した。本報告の目的は、遠隔授業システムを導入するために立ち上げた遠隔授業構築・運営チームの視点から、本校の取組事例などを紹介し、総括することである。

2 遠隔授業導入の経緯

日本国内で2020年1月に初の感染者が確認された新型コロナウイルスは、同年2月のクルーズ船ダイヤモンド・プリンセス号による集団感染を契機に日本国内で多くの関心を集めることとなった。当初は楽観的な雰囲気もあり、学校生活に関してもそれほど大きな影響は見られなかった。しかしながら、感染の拡大はその後全国的に広がり続け、3月2日からは全国の小中高校で一斉休校措置となった。

本校においては、3月23日に実施された危機対策本部会議において、次年度の授業は予定通り行うこととしながらも、COVID-19の状況次第では、臨時休講処置の可能性もあるため、3月27日に開催する次年度授業開始にあたっての対応会議で議論することとした。この対応会議の席で、初めて遠隔授業に係る言及があり、その実現可能性について検討した。その結果、技術的に実現は可能であるが、運用的な観点から事前準備と学生・教職員へのレクチャーが必要であるとの結論に至った。

これを受けて、学内の有志4名によって遠隔授業システムの検討が開始された。検討にあたっては、まず遠隔授業の形態として、以下に示す①オンラインビデオ通話システムによるリアルタイム配信型と、②チャットや動画サイトを活用したオンデマンド配信型のいずれの方式を採用するかについて議論した。

① リアルタイム配信型

リアルタイム配信型の場合、教員と学生の映像・音声等によるやり取りができ、学生の教員に対する質問機会の確保ができるため、これまでの対面授業とそれほど変わらない授業を実施することができる。しかし、本校の学内ネットワークへの負荷およびトラブル発生時の対応人員の不足という問題だけでなく、学生の通信環境が担保されていなければならず、通信環境が整っていない学生への対応が必要である。

② オンデマンド配信型

オンデマンド配信型の場合は、学生が自分の都合に合わせて受講することができ、通信環境にそれほど左右されない点が利点であるが、リアルタイムでの質問が難しい、教員側の準備の負担が大きいという懸念がある。

上記2つの配信システムを精査・分析した結果、学校全体で取組むべき課題となる運用上の観点から、本校ではオンデマンド配信型の遠隔授業システムを採用することとした。

遠隔授業システムの基幹プラットフォームについては、googleが提供しているgoogle classroomや、株式会社朝日ネットが提供しているmanabaなどが選定対象として挙げられたが、アカウント管理やインシヤルおよびランニングコストの負担が大きく、議論の末、採用することは困難であるとの結論に至った。結果として、アカウント管理（2018年度から本校全学生に発行）や運用コストなどの観点から、高専機構本部が包括ライセンス契約を結んでいるMicrosoft365のMicrosoft Teamsを採用することとした。これらの方針が固まった上でMicrosoft Teamsによる遠隔授業システムの構築に取り掛かり、4月5日にはその基本構成が完成した。

システムの基本構成が完成した後、4月9日に開催された運営企画委員会・危機対策本部会議にて、校長より構築したシステムを本校の「遠隔授業システム」とし、全学的に取り組むよう要請があった。また、遠隔授業システムを構築・運営するために「遠隔授業構築・運営チーム」（以下、遠隔チーム）を立ち上げることが認可された。

同会議に先立つ4月7日には、本科1年生および2年生を来校させ、Microsoft365アカウントの配付およびログインの確認とメールの基本的な使い方について講義を実施した。これは、本来1年生の情報基礎Iの授業内で実施する内容であるが、この時点で4月20日まで授業を実施しないことが決定されており、学生に対して一括で連絡を取る手段が皆無であったため、メールを活用して学校との連絡を取れるようにするためである。この結果、新入生から専攻科生までがMicrosoft365アカウントを有することとなり、メールを用いた一斉連絡ができる状況を確認した。

つぎに、学生が遠隔授業を実施できる状況にあるかを把握するため、通信環境調査を実施した。その結果、本科・専攻科に所属する全学生852名のスマートフォン・タブレット・PCの所有率は100%であり、遠隔授業の実施については支障がないことが確認できた。しかしながら、自宅にWi-Fiを有してい

ない学生が、52名（全学生の約6.1%）いることが明らかになった。このような環境下において、講義動画をオンデマンドで配信する形式を採用した場合は、通信制限を超過した際、講義動画を閲覧できなくなり、自宅にWi-Fiを有している学生と有していない学生の間で、不平等が生じてしまうことが懸念された。そこで、教務委員会および遠隔チームにおいて、チャットを主とした遠隔授業にする方針を策定した。遠隔授業における出席状況の確認とエビデンスの確保も懸案事項となったが、講義終了後には必ずMicrosoft Teams上で課題を課し、1週間後に提出させ、それをもって出席とし、提出された課題をエビデンスとすることが決定した。この時点で正式な遠隔授業の実施は決まっていたが、いつでも遠隔授業を実施できるように、大まかな運用方針を4月中旬までに整えた。

国内でのCOVID-19の感染状況は拡大を続け、4月16日には緊急事態宣言が全国に拡大することとなった。この状況において、4月20日からの学校再開は難しい状況となり、またその先の収束の見通しも立たないことから、4月23日に開催された危機対策本部会議では、対面授業は実施せず、5月11日から遠隔授業システムを用いた遠隔授業を実施することを正式に決定し、その旨、学生および保護者に対して通知を行った。この時点で、遠隔授業システムは概ね完成していたが、詳細な運用方針については、まだ確定していなかった。しかしながら、学生には事前に概要を知らせておく必要があり、かつMicrosoft Teamsアプリのインストール等を準備させる必要があるため、遠隔授業の運用方法に関する動画およびMicrosoft365操作手順書を作成し、併せて学生に展開した。

遠隔授業の正式な実施にあたり、業務に係る教職員（非常勤講師を含む）への使用方法の説明が喫緊の課題となった。これまでに、本校ではMicrosoft Teamsの活用を全く行っておらず、ほぼすべての教職員が初めて使用する状況であった。また、遠隔授業に関しては、遠隔チーム内においても最適な実施方法が確立できておらず、多くの教職員はどのような授業形態で実施すれば良いのか不安を抱えている状況であった。そのため、最適な授業の実施方法よりもMicrosoft Teamsの操作の習熟度を高めることを優先して運用することを目指した。一連の第一段階として、操作手順と動作の流れを示した動画を作成し、それらを用いて、4月下旬に全教員、非常勤講師、技術職員向けにそれぞれレクチャーを実施した。また、レクチャーで不足した部分に関しては、テスト用のチーム（クラス）とチャンネル（担当科目）

を準備して習熟度を高めてもらうこととした。この結果、課題の提出方法およびチャットの使用方法についてはほとんどの教職員で理解が進み、漠然とした遠隔授業への不安の解消にも繋がった。ついで、遠隔チームはこのレクチャーで挙がってきた意見を吸い上げ、教務委員会と連携して運用方針の詳細を固めた。詳細な運用方針の策定に際し、オンデマンド方式の遠隔授業をいつ受講させるかについて議論となったが、学生の生活習慣の乱れを防ぐためにも、対面授業の場合と同様に時間割通りに受講させるのが望ましいという結論に至り、策定した運用方針の基、最終的な学生向け手順書と操作動画を5月1日に学生に展開した。また、遠隔授業開始後に操作に関する不明点、遠隔授業に関することや生活に関する悩みなどを解消し、学生がスムーズに遠隔授業を受講できるように専用の問い合わせフォームをMicrosoft365のMicrosoft Formsにより準備した。

5月9日と10日の2日間で、Microsoft Teamsのチーム（クラス）・チャンネル（科目）に対して、全教職員と全学生の紐づけ作業を行い、5月11日から遠隔授業を正式に実施する運びとなった。

3 遠隔授業開始後の動向

5月11日から遠隔授業システムを用いた遠隔授業が正式に開始された。当初はシステム操作に不慣れであることに起因するトラブルの問い合わせが集中したが、遠隔チームでは、Microsoft Teamsの操作習熟度が高まれば、操作面のトラブルは減少すると事前に予測しており、操作面に関するトラブルは5月下旬には概ね収束した。

一方で、個々の学生が遠隔授業システムの操作方法を理解し、授業に馴染めるかという懸念は払拭しきれなかった。そのため、5月12日から毎日、全クラス・全科目の課題提出率を調査し、学生の状態の経過観察を行うこととした。ここで、課題提出率は、調査時点の課題提出者数を受講者数で除して百分率で表した値を示す。表1に第1週目(5/11~5/15)の各学年の課題提出率を示す。第1週目の本科全体の課題提出率は99.4%であった。遠隔チームでは、教員、学生共にMicrosoft Teamsの操作に慣れていないため、第1週目の提出率は低いものと想定していたが、それに反し非常に高い提出率であった。これは、教職員への事前レクチャーと、学生向けに作成した手順書が有効であったと考えられる。第1週目はガイダンスのみを実施する授業がほとんどであり、本格的な講義と課題提示は第2週目から行われるため、遠隔チームではそれ以降も継続的に課題提出状

況を調査することとした。

表1 第1週目課題提出率 (単位: %)

1年	2年	3年	4年	5年
99.3	99.4	99.6	99.8	98.8

図1および図2には、それぞれ第1週目から第6週目(5/11~6/19)までの学年別の週間課題提出率の推移と、同期間の本科全体の週間課題提出率を示す。縦軸には課題提出率を、横軸は経時変化(週)を示す。本科1年生、4年生および5年生については、概ね一定の傾向を示しているが、2年生と3年生については、週を追うごとに提出率が低下し、結果として全体の課題提出率も週を追うごとに悪化していることがわかる。この要因として、1)講義内容を学生が理解できずに課題を提出ができない、2)課題量が適切ではなく学生に負担が掛かりすぎて課題を提出できない可能性などを推測した。

そこで、遠隔チームでは学生に対し、第1回目のアンケートを実施し、原因を調査し、分析することとした。第1回目の学生向けアンケートは5月22日~29日の期間で実施し、571名から回答があった。このアンケートの回収率は67.0%である。遠隔授業の状況を把握するため、遠隔授業の感想、システムの良いところ/悪いところ、遠隔授業で困っているところ、学習時間の変化、課題の量など14項目についてアンケート調査をおこなった。

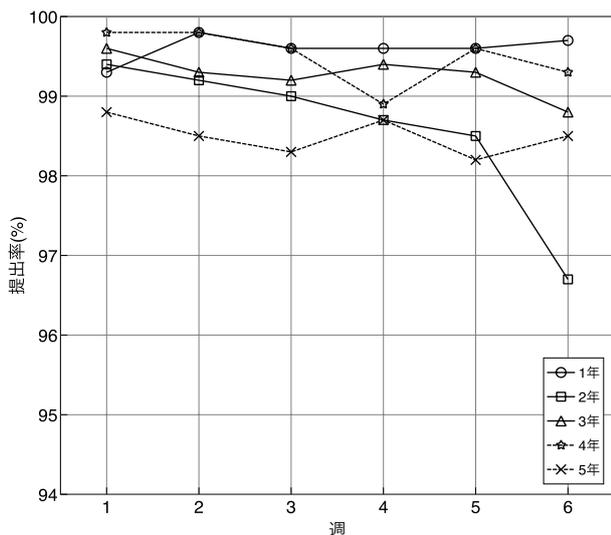


図1 週間課題提出率 (学年別: 第1~6週目)

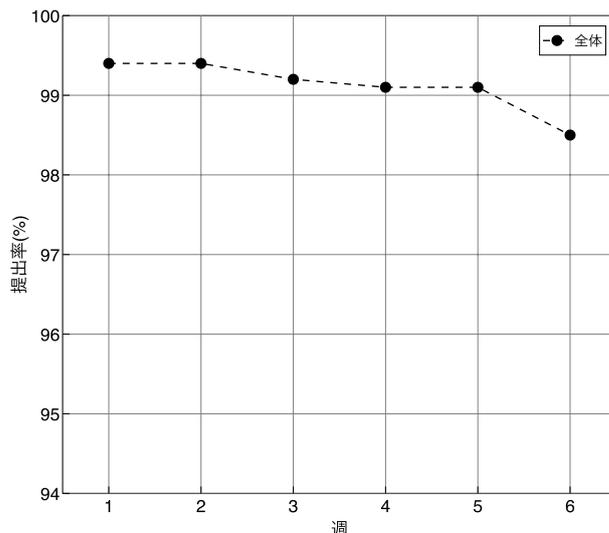


図2 週間課題提出率 (本科全体: 第1~6週目)

図3は「課題の量が適切であるか」という質問の回答結果を示す。この結果に基づくと、63%の学生が課題量は適切であると回答しており、この結果に基づくと、学生はそれほど負担を感じていないように思われる。しかしながら、学年ごとに見てみると1年生に関しては、図4に示すように8割弱の学生が課題量は適切であると答えているのに対し、5年生では図5に示すように5割以下である。この傾向は他学年でも見られ、学年が進行するほど課題量は適切でないと感じる学生が増えている。この要因としては、第3週目から実験・実習科目が入ってきたため、そのレポート等も含めて課題数が増えたことが考えられる。

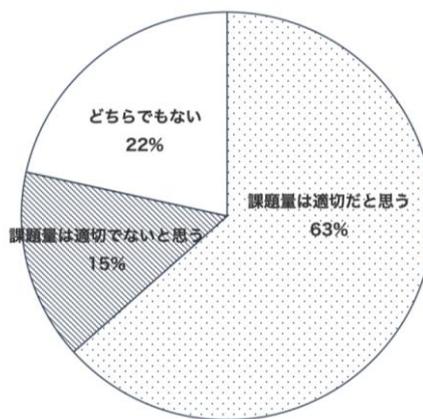


図3 課題の量について (全体: n=571)

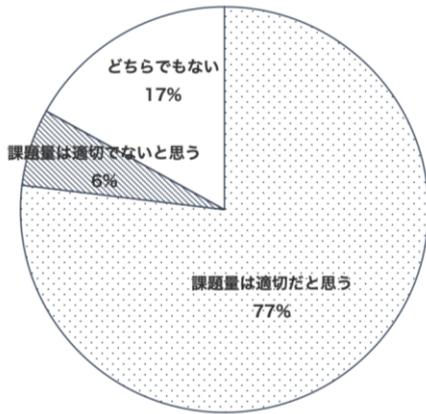


図4 課題の量について (1年生 : n=130)

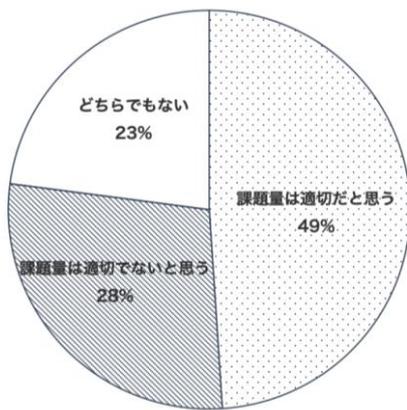


図5 課題の量について (5年生 : n=96)

遠隔授業で困っていることに係る自由記述については、「課題と授業内容をまとめるのに追われて復習や予習ができていない。」・「ただでさえすべての科目に課題が課されているのに突出して多い科目がある。どの教科も無理のないよう量を考えてほしい。」・「課題が多い。対面ならこちらの言い分次第で量を考えてくれることもあるけど、それが出来ない中、全教科課題があることをちゃんと考慮してほしい。」などの意見があり、課題量が多く、負担に感じている学生もいることがわかった。その他にも「教科ごとに課題の提出方法が異なり毎回提出方法を確認しなければならない。」・「教員によって課題の出し方(pdf、jpeg、Word等)が異なる。」・「課題のやり方を詳しく説明してくれないとわからない教科もある。」・「配布資料の説明が少なく、課題を解くための手段を理解しづらい。」など、教員の課題の提示方法に関する意見も散見された。そこで、まず課題名称の統一を図り、課題名、提示日と締め切りがわかるよう課題名称のガイドラインを策定した。課題提示方法に関しては、遠隔チームから事例を示して改

善を促すこととした。さらに、第8週目に課題を提示しない期間を設け、少しでも学生の負担を軽減するようにした。

図6には、第7週目から第15週目(6/22~9/4)までの学年別の週間課題提出率の推移を示し、図7には同期間の本科全体の週間課題提出率を示す。ただし、第7週目は第8週目に課題を学生に提示しない期間を設けているため、提出期限が2週間と通常とは異なることに留意されたい。図6および7の縦軸には課題提出率を、横軸は経時変化(週)を示す。第8週目において、前述の課題を提示しない期間を設けたことで、一時的に課題提出状況は改善されている。しかしながら、その後は、全体的に課題提出率が減少し、特に低学年生の提出率については著しく減少している。一方、高学年生の課題提出率については、第14週目以降、低学年生に比べて比較的高い傾向を示している。すなわち、課題を提示しない期間を設けることは、課題提出率の改善に一定の効果を得られるが、限定的な改善効果であるといえる。

なお、課題提出率の減少傾向の要因については、6月29日~7月3日の期間で実施した第2回目のアンケート結果から考察することができる。このアンケートの回収率は71.0%(605名が回答)である。

図8には、第1回目のアンケートと同じ設問である課題量に係るアンケート結果を示す。課題量が多すぎると答えた学生は32%を示し、第1回目のアンケートと比較して17%増加している。

「現時点で遠隔授業に関して困っていることがあれば書いてください」という自由回答に基づくと、「遠隔授業での学生の理解度に対して課題の量と難易度が適切ではない。それならばもう少し理解を深め

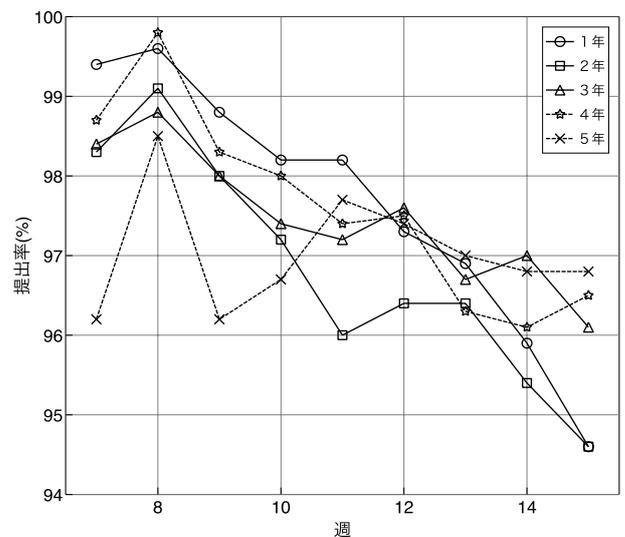


図6 週間課題提出率 (学年別 : 第7~15週目)

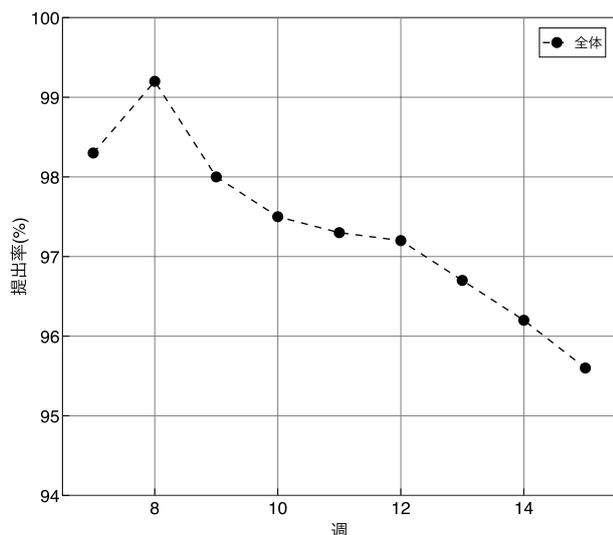


図7 週間課題提出率 (本科全体：第7～15週目)

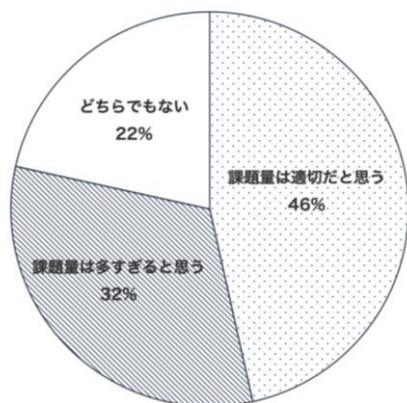


図8 課題の量について (全体：n=604)

られるよう期限を融通して欲しい。」・「課題の量が多すぎる先生がいるので、全教科課題が出ていることを考えて、課題の量を調整するようにして欲しい。」・「課題をその日に終わらせて、理解に時間がかかった場合、普通の授業より時間がかかってしまうこと。また課題をあと回しにしても、蓄積された課題が週末や次の日に響くこと(課題の量は日や授業によって変わる)」・「専門科目の課題が多すぎる。一教科につき、授業90分、課題90分の目安と聞いたが、1教科の課題に4.5時間かかっている。また、模範解答も配布されないため、提出したが、果たして合っているのかよくわからない。」などの回答があった。これらの学生の回答結果から、遠隔チームとしても、全教員に対して課題量を減らすよう要請を行い、課題提出率の悪い科目の授業担当者に対しては、直接改善を要請したが、抜本的な改善には至らなかった。すなわち、先に述べた状況が継続的に続いた結果と

して、学生の疲労の蓄積やモチベーションの低下につながり、課題提出率が低下したものと考えられる。

4 遠隔授業から得られた成果と課題

本校で実施された初の遠隔授業は、COVID-19の感染状況に左右されながらも、5月11日から9月4日までの116日間実施された。課題提出の観点からは、教員、学生が共に手探り状態からスタートしたため、双方が適切と考える課題量を見出すことができず、最終的には課題提出率が低下するという状況となった。しかしながら、全学年で94%以上の課題提出率を維持できたことは、一定の成果があったといえる。

第1回目のアンケートにおいては、対面授業と遠隔授業のどちらが受講しやすいかについての質問を行った。その結果、図9に示すように対面授業が受講しやすいとの結果が多数であった。しかしながら、遠隔授業、どちらも変わらないと答えた学生を足すと5割を超えており、遠隔授業に関しても半数以上の学生は抵抗を感じていないこともわかる。遠隔授業が受講しやすいと答えている学生は学年が進行するにつれて増加しており、専門科目が遠隔授業との親和性が高いと感じている学生が多いことを示している。図10は、第2回目のアンケートにおいて遠隔授業に慣れたかどうかについての問いの結果であるが、慣れたと回答した学生は77%を示している。すなわち、当初から半数以上の学生は、遠隔授業をある程度抵抗なく受け入れられており、また、時間が経過することで、多くの学生は遠隔授業に適応できていることを裏付けている。

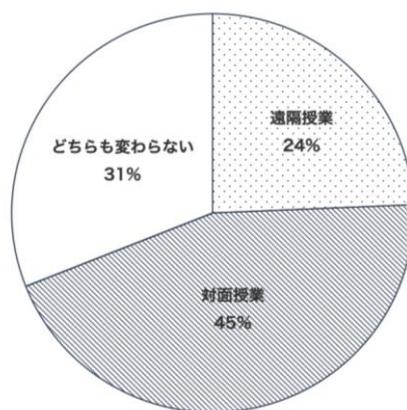


図9 授業形態による受講のしやすさについて (全体：n=571)

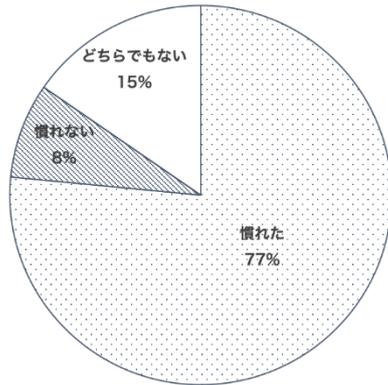


図 10 遠隔授業に慣れたかどうかについて
(全体 : n=605)

第 1 回目のアンケートにおいて、学生に遠隔授業システムの良いところを質問したところ、「授業と違い、自分のペースでできるのでいいと思う」・「理解した授業は短く、分からない授業は長く時間が使える」・「授業内容が後からでも確認しやすい為、就活に関する事を終わらせてからでも授業に遅れづらい」・「授業内容を後から見直せること、ノートを取る余裕が充分にあるのでまとめやすい」など、遠隔授業システム自体は好意的にとらえている学生も多いことがわかる。また、「パソコンの扱いに慣れる」など、これまで情報系が苦手だった学生にとっては、自ずと IT スキルを向上させる機会になったものと考えられる。遠隔授業システムの悪いところとしては、「グループワークができない」・「課題を閉じて手順等を見ないといけないのか不便だった」・「どの資料がどこに入っているのか全部まとめて見れるようにしてほしい」など、システム上で単純に解決できない問題もあり、遠隔授業システムの構成の見直しや、他のツールを導入し、それと併用するなどの改善を図ることが今後の課題である。

対面授業が始まった後に遠隔授業システムをどのように使用したいかという問いには「体調不良で欠席しなければならない場合や災害で登校できない場合に利用したい」・「課題の管理と提出が自宅からでも出来る点が便利だと思う。そのため、授業を学校で受け、課題を遠隔授業システムの活用によって提出する形での利用がしたい」・「台風やインフルエンザでの学級閉鎖などの時に家でも授業する手段として活用して欲しい」など、前向きな意見が多数あった。これらの意見は、今後の遠隔授業システムの活用方法の参考にしていきたい。

今回の遠隔授業を通しての最大の成果は、学生の学習習慣の定着であるといえる。図 11 は、第 1 回目

のアンケートにおいて、対面授業と比較した学習時間の変化について聞いた結果である。この結果に基づくと、3 割強の学生の学習時間が増加している。これまで、試験前のみ学習する学生は一定数いたが、今回の遠隔授業においては、全授業において課題を課したため、自ずと勉強する機会が増えたためと考えられる。学生にとっては数か月間、自らの力で課題に取り組まなければならない、過酷な環境であったと考えられるが、このように学習習慣が定着したのは遠隔授業システムを導入した成果である。

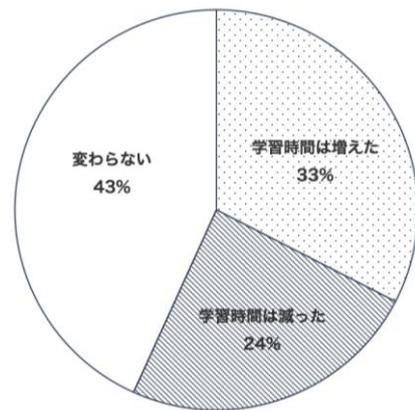


図 11 対面授業と比較した学習時間の変化
(全体 : n=571)

遠隔授業を通しての最大の課題は、適切な遠隔授業の手法と課題量の確立である。課題量に関しては、先に述べた通り教員、学生の双方が適切と考える課題量を見出すことができなかったことは運営上問題であり、その最適な量を見出すことが喫緊の課題である。また、遠隔授業の講義方法に関しては、「対面授業より分かりにくく、追いつくのが大変」・「授業内容の説明が少ない科目がある」・「音声と資料だけではなかなか分からない所が多い」・「授業は貧弱な説明だけで、しかも解けない課題を出すので時間だけが持っていられる科目がある」などの声がアンケートで挙げられた。このことから、教員の遠隔授業に対する意識の向上と、スキルアップが望まれる。なお、前期末に授業評価アンケートを実施したが、①評価が高い授業を公開授業とすること、②評価が高い授業の担当者を講師とした FD を実施するなど、遠隔授業の良い面を教員間で共有し、自らの授業方法を改善する方法を提供することで、授業の質を向上させることも今後の課題であるといえる。

5 今後の展望

本校では後期からの対面授業再開に向け、9月11日に「新型コロナウイルス感染拡大防止のための対応基準」を策定した。この総合レベルは本校の位置する都城市・三股町圏域の感染状況によって変化するが、このように感染状況の変化に柔軟に対応できるのは、遠隔授業システムが構築され、前期期間中に教員、学生共に遠隔授業システムの操作に習熟できたからであり、これは本校にとっては大きな強みである。感染に不安を感じ登校を希望しない学生に対しては、対面授業再開後も遠隔授業を選択肢として選ぶこともでき、これはハイフレックス型の授業として遠隔授業システムの新たな使い方の一つを示すものとする。また、後期からの授業に関しては、対面授業と遠隔授業を組み合わせるブレンド型の授業も実施することもできる。このように、遠隔授業システムの導入と前期期間中の遠隔授業の実施は、今後の本校の教育システムを劇的に変化させ、教育効果を飛躍的に向上させるきっかけとなった。そして、コロナ禍をきっかけに、テレワークを積極的に推進する企業も増えている。本校の遠隔授業を受けた学生は、テレワークに対しても抵抗なく受け入れることができるため、テレワークを推進する企業からの需要は今後ますます拡大すると考えられる。

教育効果を高め、学生の価値を高めることができる本校の遠隔授業システムは、今後も学校全体で取組み、教職員、学生の声をフィードバックさせながら、本校の財産としてその質の向上を図りたい。

謝辞

遠隔授業の構築と運用に際し、本校教職員ならびに学生諸君に多大なる支援とご尽力をいただいたことに、この場をお借りして感謝の意を表す。

都城工業高等専門学校
研究報告第 55 号

令和 3 年 1 月印刷
令和 3 年 1 月発行

編集兼発行者:独立行政法人国立高等専門学校機構
都城工業高等専門学校

郵便番号:885-8567

所在地:宮崎県都城市吉尾町 473 番地の 1

National Institute of Technology(KOSEN), Miyakonojo College
ADDRESS:473-1 Yoshio-cho, Miyakonojo City,
Miyazaki Prefecture, Japan 885-8567

TEL (0986) 47-1109

FAX (0986) 47-1111

Research Report
of
National Institute of Technology (KOSEN), Miyakonojo College

No.55

2021

Contents

Research Papers:

- A Quantitative Text Analysis Study of the Japanese Constitution
and Proposed Constitutional Amendments..... Senshu YOSHII.....1

Data and Introduction:

- A Demonstration Example of Mechanism of Encryption Technology
—An Example with RSA Encryption Assuming Only Learning of Remainder Calculation
at Elementary School—..... Hirofumi NAKAMURA.....12
- The Accomplishment of Distance Education Utilized by Microsoft Teams
...Shota USUI, Toshihide FUJIKAWA, Shinobu YONEMITSU, Takahiro OKAMOTO
and Toshiaki YAMASHITA.....24
