5H-4

大学教育のための電子教材の試作 ～ 情報数理教育向けインタラクティブコンテンツ ～

小林　学† 石田　崇‡ 梅澤克之†† 平澤茂一‡
†湘南工科大学 ‡早稲田大学 ††日立製作所

1　はじめに

近年 iPad や Android タブレットの爆発的普及により，電子書籍の急速な拡大が進んでいる．アメリカにおける電子書籍の普及率は 20%を越え，日本でも Amazon.com の電子書籍配信サイト Kindle ストアのオープンにより電子書籍拡大が続くものと見込まれる．また韓国では 2015 年までに小中高校でのデジタル教科書導入が決定しており，教育現場における世界的な電子教材の普及は今後急速に進むことが予想される．

本稿では大学教育における電子教材に焦点を当て，特に数式表現が必要となる情報数理向けのインタラクティブコンテンツの試作を行う．具体的には RSA 暗号を例題として用い，教育コンテンツとして試作及び評価を行う．これにより PC のみならず，iPad や Android タブレットなどマルチプラットフォームにおける情報数理教育について検討を行うことが目的である．

2　HTML における数式表現

本研究ではマルチプラットフォームを目指すことを考え，HTML 及び JavaScript により情報数理用電子教材の試作を試みる．そのため電子教材において数式を表現する必要がある．HTML において数式を表現する方法はいくつかあるが，インタラクティブに数式を表現する必要性から本研究では MathJax[4] を選択した．MathJax は JavaScript による数式表記エンジンであり，HTML 内において LaTeX あるいは MathML を用いた数式表記を可能とする．もしインターネット環境を前提とできるのであれば，MathJax を用いて数式を表記する場合，HTML の <head> と </head> の中に以下のように記述する．

```
<script type=”text/x-mathjax-config”>
MathJax.Hub.Config( tex2jax:  inlineMath: [[’$’,’$’],
[”¥¥(”,”¥¥)”]] );</script>
<script type=”text/javascript” src=”http://cdn.mathjax.
org/mathjax/latest/MathJax.js?config=
TeX-AMS_HTML”> </script>
```

あとは HTML の本文中に LaTeX の命令を挿入すると，数式として表現される．なお MathJax はオフライン環境で利用することも可能である．その場合 MathJax サイト [4] より JavaScript エンジンをダウンロードし，適宜必要なファイルを指定する．

3　RSA 暗号教育用コンテンツの試作

本節では試作を行った情報数理教育向けコンテンツについて解説を行う．情報数理全体は大変広範な分野であるため，第一著者の講義（情報セキュリティ）の中から RSA 暗号を例題として教育用コンテンツの試作を行った [5]．試作を行ったコンテンツの目次は以下である．(1) MathJax テスト，(2) 指数剰余の計算，(3) べき乗法，(4) エラトステネスのふるい，(5) フェルマーの小定理，(6) 確率的素数判定法，(7) ユークリッド互除法，(8) 拡張ユークリッド互除法，(9) オイラーの定理，(10) オイラーの定理の修正，(11) RSA 暗号化・復号，(12) 画像の RSA 暗号化・復号．

数式の表現には前節で述べた MathJax を用いた．これらのコンテンツは補助教材であり，基本的には講義で行った内容をこのコンテンツで確認し，理解をさらに深めるために用いることを前提とした．具体的には HTML の form から数値の入力を行い，アルゴリズムに従って計算される計算過程を画面に表示する．図 1 に拡張ユークリッド互除法のコンテンツを示す．


拡張ユークリッド互除法（与えられた a, c から $ab + cd = 1$ となる b, d を求める）

$a =$ 1010 ， $c =$ 1071

計算

$r_0 = c = 1071$，$r_1 = a = 1010$

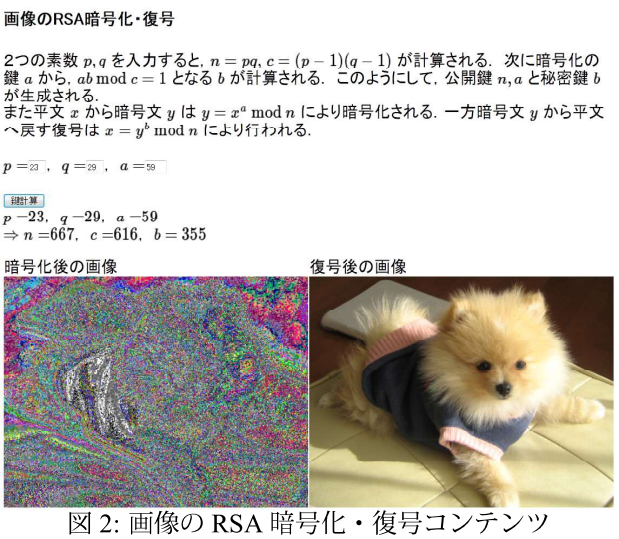
ユークリッド互除法	書き換え	変数に置き換え
$1071 \div 1010 = 1$　余り61	$1071 = 1 \times 1010 + 61$	$r_0 = 1 \times r_1 + r_2$
$1010 \div 61 = 16$　余り34	$1010 = 16 \times 61 + 34$	$r_1 = 16 \times r_2 + r_3$
$61 \div 34 = 1$　余り27	$61 = 1 \times 34 + 27$	$r_2 = 1 \times r_3 + r_4$
$34 \div 27 = 1$　余り7	$34 = 1 \times 27 + 7$	$r_3 = 1 \times r_4 + r_5$
$27 \div 7 = 3$　余り6	$27 = 3 \times 7 + 6$	$r_4 = 3 \times r_5 + r_6$
$7 \div 6 = 1$　余り1	$7 = 1 \times 6 + 1$	$r_5 = 1 \times r_6 + r_7$
$6 \div 1 = 6$　余り0	使わない	使わない

移項	代入	計算結果
$r_2 = r_0 - 1 \times r_1$	$r_2 = r_0 - 1 \times r_1$	$r_2 = 1 \times r_0 - 1 \times r_1$
$r_3 = r_1 - 16 \times r_2$	$r_3 = r_1 - 16 \times (1 \times r_0 - 1 \times r_1)$	$r_3 = -16 \times r_0 + 17 \times r_1$
$r_4 = r_2 - 1 \times r_3$	$r_4 = (1 \times r_0 - 1 \times r_1) - 1 \times (-16 \times r_0 + 17 \times r_1)$	$r_4 = 17 \times r_0 - 18 \times r_1$
$r_5 = r_3 - 1 \times r_4$	$r_5 = (-16 \times r_0 + 17 \times r_1) - 1 \times (17 \times r_0 - 18 \times r_1)$	$r_5 = -33 \times r_0 + 35 \times r_1$
$r_6 = r_4 - 3 \times r_5$	$r_6 = (17 \times r_0 - 18 \times r_1) - 3 \times (-33 \times r_0 + 35 \times r_1)$	$r_6 = 116 \times r_0 - 123 \times r_1$
$r_7 = r_5 - 1 \times r_6$	$r_7 = (-33 \times r_0 + 35 \times r_1) - 1 \times (116 \times r_0 - 123 \times r_1)$	$r_7 = -149 \times r_0 + 158 \times r_1$

以上より，$1 = r_7 = -149 \times r_0 + 158 \times r_1 = -149 \times c + 158 \times a$ であるから $b = 158$ ，$d = -149$ となる．

図 1: 拡張ユークリッド互除法コンテンツ

学生は講義中の例題の数値，あるいは適当な数値を入力し，各自で計算した内容とコンテンツの出力を比較することにより，理解度の確認を行う．


画像のRSA暗号化・復号

2つの素数 p, q を入力すると，$n = pq$，$c = (p-1)(q-1)$ が計算される．次に暗号化の鍵 a から，$ab \bmod c = 1$ となる b が計算される．このようにして，公開鍵 n, a と秘密鍵 b が生成される．
また平文 x から暗号文 y は $y = x^a \bmod n$ により暗号化される．一方暗号文 y から平文へ戻す復号は $x = y^b \bmod n$ により行われる．

$p =$ 23 ， $q =$ 29 ， $a =$ 59

暗計算

p 23，q 29，a 59
$\Rightarrow n = 667$，$c = 616$，$b = 355$

暗号化後の画像　　復号後の画像

図 2: 画像の RSA 暗号化・復号コンテンツ

一般に講義中に行うことのできる例題や演習では問題数に限りがあり，多くのパターンを提示することはできない．また書籍においてもページ数の関係で例題に費やせる紙面には限りがあり，学生の理解度に適合

Trial Development of the Electronic Teaching Materials for University Education - Interactive Contents for Mathematical Information
†Manabu KOBAYASHI ‡Takashi ISHIDA ††Katsuyuki UMEZAWA
‡Shigeichi HIRASAWA
†Shonan Institute of Technology, ‡Waseda University, ††Hitachi, Ltd.

した例題や演習課題などきめ細かい提示は困難である．以上のような場面に際し，試作したコンテンツは有効性を持つものと考える．

次に画像の RSA 暗号化・復号のコンテンツ画面を図 2 に示す．このコンテンツは RSA 暗号の鍵パラメータを正しく設定すると，鍵の生成を行った後画像の暗号化及び復号を行い，暗号化後の画像と復号後の画像を表示する．誤ったパラメータを設定すると，暗号化が不完全であったり，正しく復号できないことが確認できる．なお図 2 のコンテンツは HTML5 の規格である canvas 要素と JavaScript を用い，画像のピクセルごとに処理を行なっている．このように HTML5 を用いると画像処理も行うことができ，インタラクティブな教育用コンテンツを構築することが可能である．

4 PhoneGap Build によるマルチプラットフォーム化

本節では前節で示した電子教材をマルチプラットフォーム化する方法について検討する．インターネットが利用できる環境であれば，各端末の WEB ブラウザで上の電子教材は問題なく動作する[1]．

一方実際の教育現場でタブレット端末などを利用する場合，各端末が Wi-Fi に接続できるとは限らないため，オフラインで利用することを想定する必要がある．そこで本節では Adobe 社の PhoneGap Build サービス [6] を利用することを検討する．PhoneGap Build とは，HTML と JavaScript で記述したプログラムを各プラットフォームのアプリにクラウド上で変換する WEB サービスである．具体的には HTML と JavaScript で記述した全プログラムをフォルダに入れ，このフォルダを zip ファイルとして圧縮しておく．この zip ファイルを PhoneGap Build サービスにアップロードすると，各 OS 用のアプリに自動的に変換され，希望の OS 用アプリをダウンロードすることにより各端末で利用可能となる．

ここでの目的はタブレット端末上でのオフライン実行のため，数式表示のために 2 節で述べたオフライン用 MathJax エンジンも同様にフォルダ内に配置しておく．この環境で PhoneGap Build を利用したところ，問題なく iOS 用並びに Android OS 用のアプリに変換することができた．また Android 端末である Nexus7 でこのアプリを実行したところ[2]，数式表示及び画像処理の双方ともに問題なく実行することができた．

以上のように，HTML と JavaScript を利用してコンテンツを制作し，PhoneGap Build を利用することにより，簡便に情報数理教育向けコンテンツのマルチプラットフォーム化を行うことが可能である．

5 アンケートによる試作教材の有効性の評価

試作したコンテンツを大学の講義中に使用し，学生に対してアンケート調査を実施した．講義では試作コンテンツを以下のように使用した．(1) 口頭での解説，(2) 確認テスト（1 回目），(3) コンテンツによる学習，(4) 確認テスト（2 回目），(5) アンケート調査．1 回目の確認テスト全 4 問のうち 3 問以上に正答した学生 (A 群) とその他の学生 (B 群) に層別を行ったところ，39 名の受講者中 A 群の学生が 18 名，B 群が 21 名であった．この A 群と B 群それぞれのアンケート結果を調べたところ，コンテンツににについて満足と思う学生の比

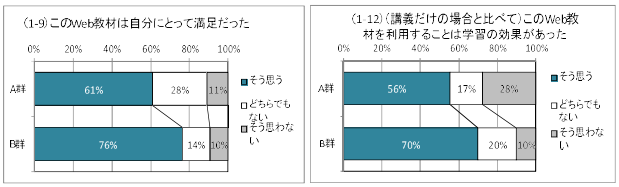


図 3: コンテンツに対する満足感

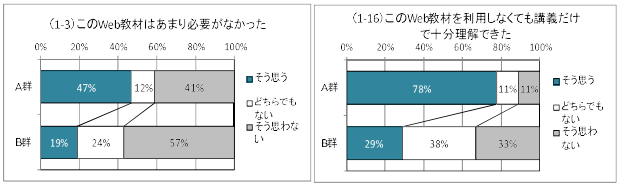


図 4: コンテンツの有効性

率は A 群が 61%，B 群で 76%となり，コンテンツを利用する段階でまだ理解度が不十分である学生の方が満足度が若干高いことが分かった．

また，A 群の学生は 8 割近い学生がコンテンツを利用しなくても理解ができ，約半数の学生がコンテンツは必要なかったと認識している一方で，B 群の学生に対してはコンテンツの必要性や理解の補助としての認識が高いことが分かった．

また自由記述回答でも,「自分の好きな値を（入力値として）設定できる」ことや「反復的にできる」ことを利点として挙げている．

情報数理の授業項目は学生の事前知識のばらつきが大きい場合が多く，理解度の低い学生に対しての補助教材として特に有用であると期待できる．

6 まとめ

本稿では RSA 暗号を例題として情報数理向けの教育コンテンツを試作し，簡単な確認テスト及びアンケートによって評価を行った．また PhoneGap Build を用いたコンテンツのマルチプラットフォーム化について検討を行った．本稿では RSA 暗号に特化して試作を行ったが，用いた技術は HTML と JavaScript であるため，情報数理の多くの分野に適用できるものと考える．

今回は試作教材による小規模評価実験であったが，今後コンテンツが充実するに従い，著作権使用料やアプリ提供サービス利用料などについても準備が必要である．

謝辞

本研究の一部は JSPS 科研費基盤研究 (C)No.23501178 の助成を受けたものです．

参考文献

[1] 西谷匠，杉山雄一郎，樋山聡，桑原恒夫，“誤答に対する教師のリアルタイムでのアドバイスを支援する e-ラーニングシステム，” 電子情報通信学会論文誌 (D) Vol.J91-D No.6, pp.1538-1549, 2008.
[2] 仲林清，細川真伸，川上太一，佐藤一夫，永岡　慶三，“SCORM 2004 を拡張したモバイルラーニング環境の設計と実装，” 電子情報通信学会論文誌 (D) Vol.J91-D No.2, pp.143-151, 2008.
[3] 舟生日出男，稲山雅史，平嶋宗，“問題解決プロセスを利用した選択問題の誤選択肢及び解説の自動生成，” 電子情報通信学会論文誌 (D) Vol.J93-D No.3 pp.292-302, 2010.
[4] http://www.mathjax.org/
[5] http://publicweb.shonan-it.ac.jp/info/RSA/
[6] https://build.phonegap.com/
[7] 塩谷隆二，中林靖，“スマートフォンアプリ開発入門–iOS vs. Android(4) ,” 日本計算工学会誌，Vol.17, No.3, pp.2817–2823, 2012.

[1]ただし HTML5 を利用したコンテンツは，対応する WEB ブラウザが必要となる点に注意されたい．
[2]利用した OS は Android4.2 である．