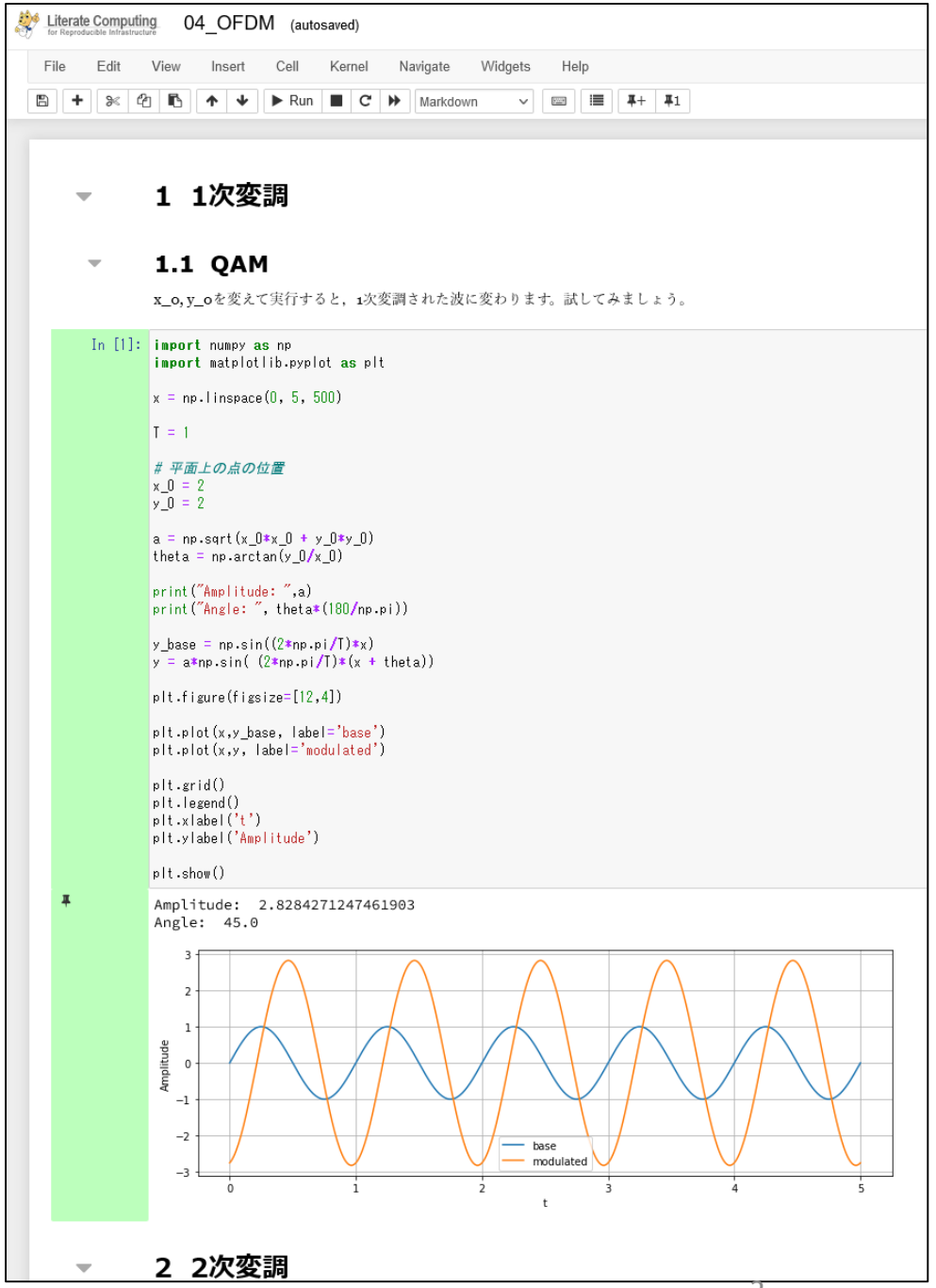
大学初年次向けの情報系講義へのCoursewareHub環境の導入

浜元信州

はじめに

- Jupyter Notebook
  - データサイエンスや機械学習等のデータ処理を行うためのPythonプログラム等の実行環境として利用されている
  - 様々なプログラミング言語によるプログラムを記述し，実行できる対話的なWebインタフェース
  - グラフ等のGUI出力も可能



はじめに

- Jupyter Notebookを使った演習の可能性
  - (Pythonの）プログラミング演習
  - 「アクティブラーニング」への適用
  - 遠隔授業：Webインタフェースなので，学外でPCを利用して演習できる環境が構築可能.

Jupyter Notebookを利用する環境準備

1．学生の個人PCにAnacondaをインストール
- 学生がインストールさせるのは，難しいケースがある

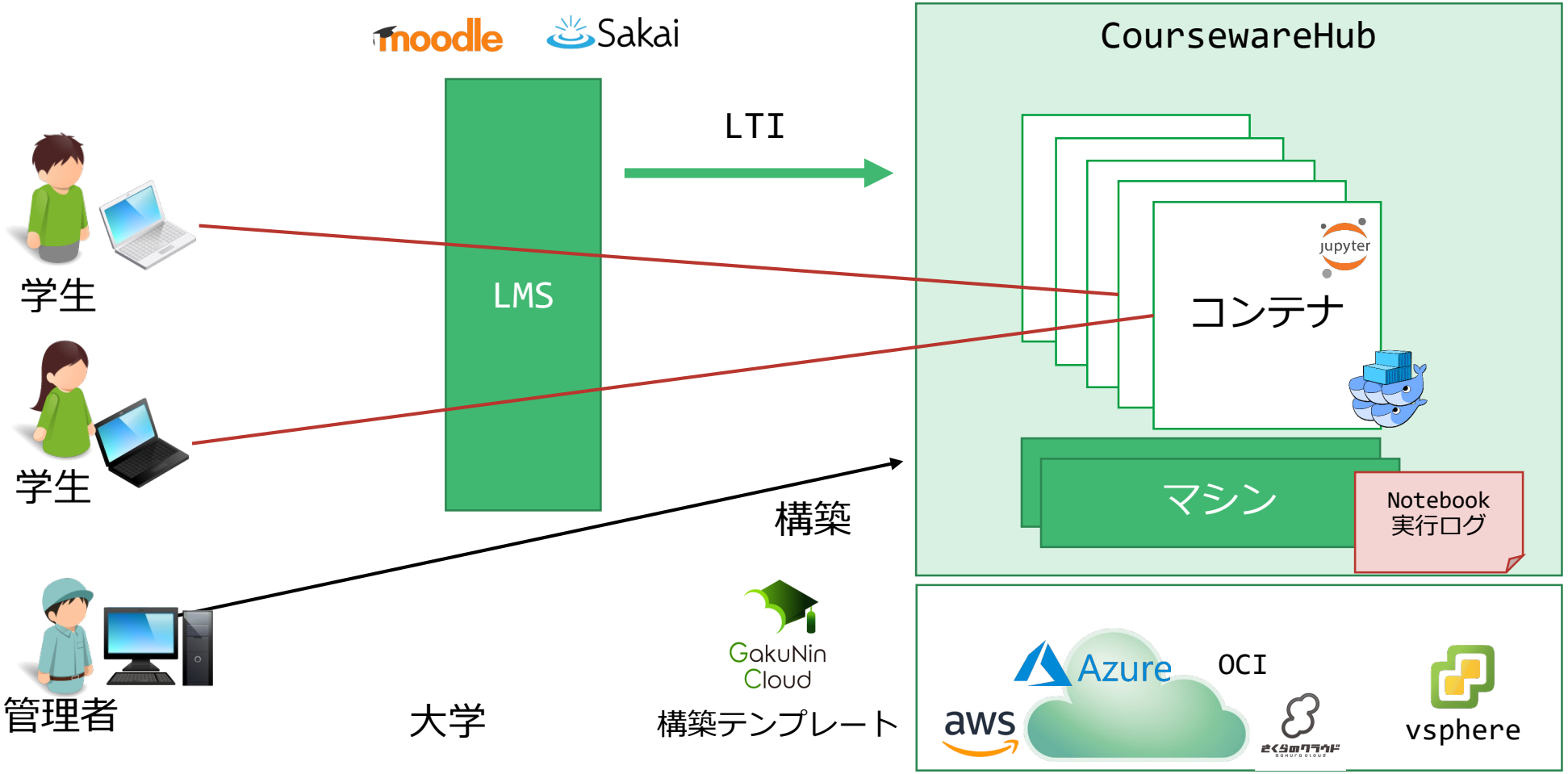
2．Google Colaboratory
- GoogleのSaaS：Googleアカウントさえあれば利用できる
- 学生のログをみれないので，遠隔授業では学生の様子が分からない

3．CoursewareHub
- 国立情報学研究所によるJupyterHubの改良版
- Notebook実行状況のログがわかる
- 大学で構築する必要がある。学認クラウドオンデマンド構築サービスを利用すると構築テンプレートが利用できる。

CoursewareHub

https://coursewarehub.github.io/

- ユーザ毎にNotebookコンテナ
- LTIに対応
- 構築は学認クラウドオンデマンド構築サービスを利用可能

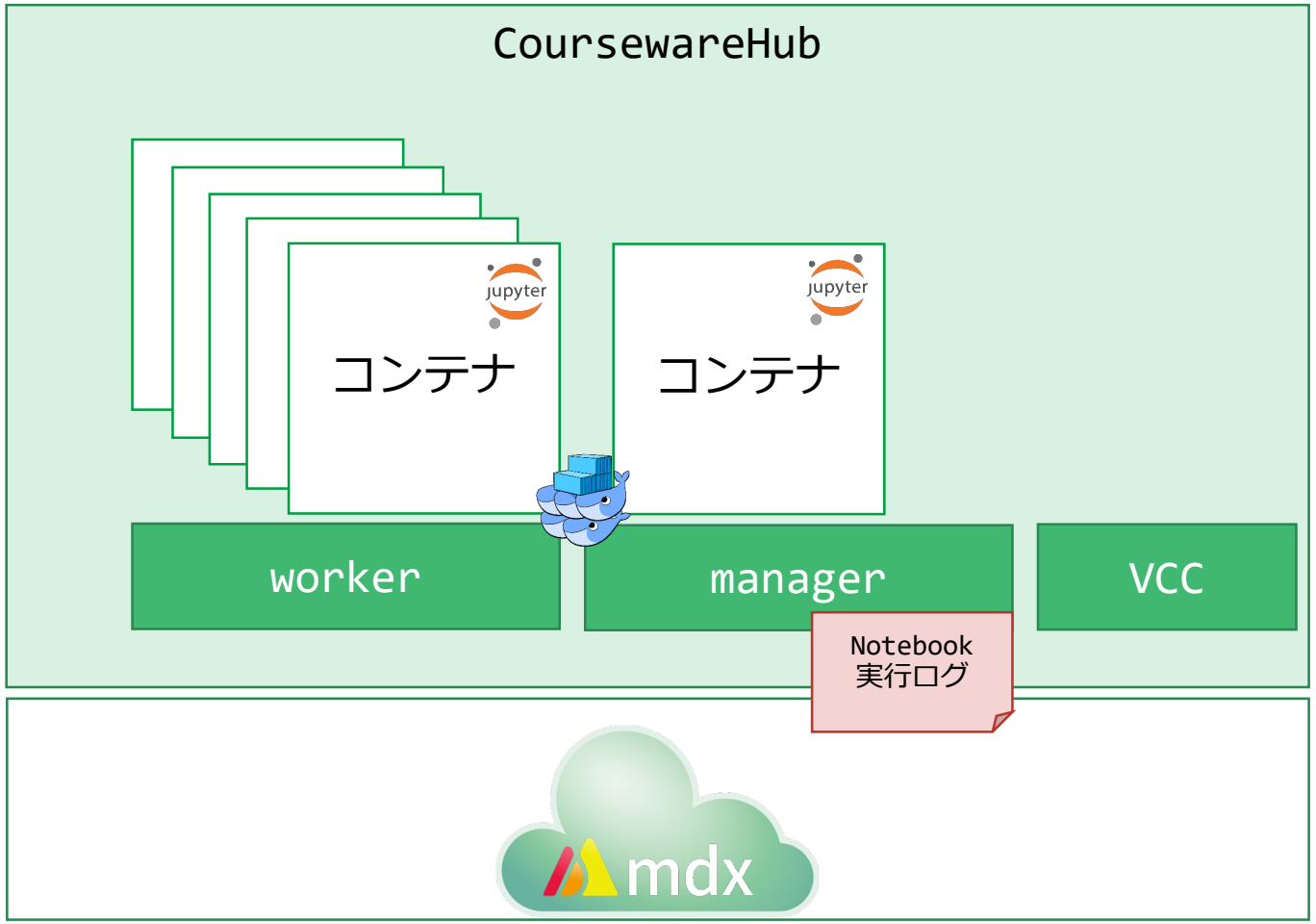


環境の比較

	PC上に構築	Google Colab	CoursewareHub
環境の構築	学生	**Google**	大学管理者 **(構築テンプレート提供あり)**
ログ取得	不可	不可	**可**
リモート接続	不要	可	可
認証	不要	Googleアカウント	**LTI連携** **学認** **ローカルアカウント**

本研究では，CoursewareHub構築テンプレートを利用し，
2022年4月現在試験運用中のmdxでCoursewareHubの構築を行なった

今回構築したCoursewareHub環境



サーバ	CPU	メモリ	ストレージ
Manager Node	10	16.02GB	336GB
Worker Node	138	221.02GB	128GB
VCC	4	6.41GB	48GB

- 受講者数は79名

GakuNin Cloud
構築テンプレート

群馬大学LMS　日本語 (ja)　n.hamamoto 浜元 信州

LB1320_コンピュータネットワークとセキュ

Home / マイコース / LB1320_コンピュータ

一般

Zoomミーティングに参加する https://gunma-u-ac-jp.zoom.us/j/83486006614?pwd=QnBqdFJkNFBxaXVUN

ミーティングID: 834 8600 6614
パスコード: 916823

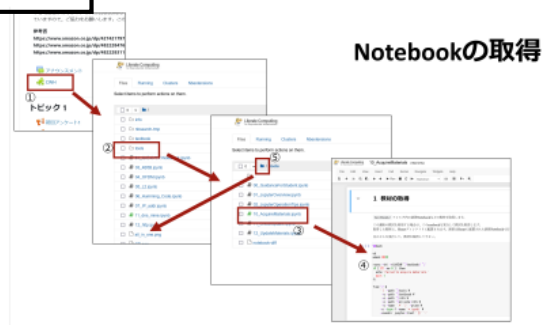
共有Googleドキュメント
https://docs.google.com/document/d/1h0urQHwKVcKY8T40WE2jEc6goGIGntagOEXUvFz0mPQ/edit?usp=sh

受講に関する注意：この授業での活動内容（CoursewareHub，LMS，Zoomなど）は，本人を特定しない形
ます。これはCoursewareHubなどの講義支援システムの利用による効果を把握し，講義支援システムや授業
ます。この点に同意いただけない場合には，浜元までご連絡お願いします。

参考書
https://www.amazon.co.jp/dp/4274217973
https://www.amazon.co.jp/dp/482228476X
https://www.amazon.co.jp/dp/4822283119

アナウンスメント

CWH



Literate Computing
for Reproducible Infrastructure

Logout　Control Panel

Files　Running　Clusters　Nbextensions

Select items to perform actions on them.　Upload　New

0 /	Name	Last Modified	File size
info		7ヶ月前	
nbsearch-tmp		7ヶ月前	
textbook		3ヶ月前	
tools		7ヶ月前	
01_はじめてのNotebook.ipynb		7ヶ月前	20.9 kB
03_4B5B.ipynb		6ヶ月前	50.9 kB
04_OFDM.ipynb	Running	1日前	205 kB
05_L2.ipynb		6ヶ月前	6.62 kB
06_Humming_Code.ipynb		5ヶ月前	12.5 kB
07_IP_addr.ipynb		5ヶ月前	27.9 kB
11_dns_mine.ipynb		4ヶ月前	84.6 kB
12_http.ipynb		4ヶ月前	55.3 kB
14_DH.ipynb	Running	4ヶ月前	23.6 kB
14_Hash.ipynb		3ヶ月前	61.7 kB
14_RSA-openssl.ipynb		4ヶ月前	25.3 kB
14_RSA.ipynb	Running	4ヶ月前	27.2 kB
all_in_one.png		6ヶ月前	13.9 kB
CD.png		4ヶ月前	12.2 kB
message		3ヶ月前	64 B
private.key		3ヶ月前	497 B
public.key		3ヶ月前	182 B

ログ内容

- user
- cell_name
- program_code
- path_logfile
- file_name
- lc_notebook_meme
- server_signature
- uid
- gid
- start_time
- output
- end_time
- results
- error
- traceback

CoursewareHubの利用例

- 室蘭工業大学でのPythonプログラミング演習（桑田ほか）
  - 学認クラウド活用事例
- 群馬大学でのPythonプログラミングの授業（井上）
  - https://coursewarehub.github.io/
- 群馬大学での教養教育科目「コンピュータネットワークとセキュリティ」（横山・浜元）

本研究では，群馬大学の教養教育科目「コンピュータネットワークとセキュリティ」の授業のログ分析の検討を行なった結果を述べる.

CoursewareHub　　CoursewareHubとは [JA]

CoursewareHub利用事例 - 群馬大学 井上先生

less than 1 minute read

CoursewareHubの利用事例を国立情報学研究所 学術基盤オープンフォーラム2021にて **群馬大学・数理データ科学教育研究センター 井上先生**にCoursewareHubの利用事例をご紹介いただきました！

資料は以下のリンクからご参照いただけます。

国立情報学研究所 学術基盤オープンフォーラム2021
2021年7月7日

CoursewareHubを利用した授業: Python入門

群馬大学・数理データ科学教育研究センター
井上　仁

Updated: August 10, 2021

Twitter　Facebook　LinkedIn

GakuNin Cloud

HOME　導入支援サービス　ゲートウェイサービス　オンデマンド構築サービス　NII 国立情報学研究所

室蘭工業大学

国立大学法人 室蘭工業大学では、情報教育の強化に向けた取り組みの一環として、クラウドとJupyter Notebookを用いたプログラミング教育を行っています。その狙いと成果について、情報教育センター長 教授 桑田 喜隆氏と、情報教育センター ひと文化領域 助教 石坂 徹氏にお話を伺いました。（インタビュー実施：2020年2月21日）

まず、室蘭工業大学の概要と情報教育センターの役割について教えていただけますか。

桑田氏： 本学では産業構造の変化や新たな社会イノベーションへの対応を果たすべく、2019年度に従来の工学部を理工学部へと改組しました。工学・科学の基礎と情報処理能力を習得し、変化する社会に対応できる人材を育成することが狙いです。これに伴い、情報教育のさらなる拡充も進めていくため、情報教育センターでも様々な形で支援を行っています。ちなみに当センターでは、2015年3月にISMS(情報セキュリティマネジメントシステム)／BCMS(事業継続マネジメントシステム)の国際認証を同時に取得しました。これは大学として世界初の事例になります。2018年に発生した北海道胆振東部地震の際には、実際にコンテンジェンシープランの発動も行いました。幸い本学に大きな被害はありませんでしたが、想定通りの対応が行えました。

国立大学法人 室蘭工業大学
情報教育センター長

授業の構成

- 「コンピュータネットワークとセキュリティ」

- 主に1年次の学生を対象とした教養教育の授業
- 基本的に講義中心
- 講義内容を補助する目的で，Jupyter Notebookを利用した演習を一部取り入れた。

- 全15回中，ほぼ毎回Jupyter Notebookへアクセスしてもらった。
- 発表は，第14回，第15回の授業が対象（提出課題とした回のみ）

授業の構成

- 公開鍵暗号やTLSに関する説明
- 授業内で説明の後，RSA暗号の具体例，電子署名の具体例，鍵交換（Diffie-Hellmann），ハッシュ関数の具体例をNotebook内で示して理解を促した。
- 各回90分授業のうち，解説がほとんどで具体例を示す時間は合計しても各回20分程度

Notebook名	内容
DH.ipynb	Diffie-Hellman 鍵共有の具体例
Hash.ipynb	さまざまなHash 関数の具体例，誕生日攻撃の解説
RSA.ipynb	オイラーの定理，RSA 暗号，電子署名の具体例

問題の例

- この例では，ユーザが入力を自由に変えてhash関数を適用することによりhash関数の変化を試せるようにしている.
- Moodle上に課題を出して，Notebookを利用して次回授業までに解答を提出してもらうこととした.

5 問題

In [1]:
```
#メッセージ
message = 'Write Message Here'
```

In [4]:
```
#SHA256でハッシュ計算

from Crypto.Hash import SHA256

hash_object = SHA256.new(data=message.encode())
print(hash_object.hexdigest())
```

```
02d021f347145d5fa38c52197fb99497bc8d6eae3053f1a51442f4fdd770ce77
```

LMSでの問題例：

次のメッセージとメッセージ認証コードが送信されてきた。メッセージの改ざんはあるか？ただし，メッセージ認証コードに利用したハッシュ関数はSHA256とする。
もし改ざんされてる場合には，正しいメッセージ認証コードも回答せよ。

メッセージ：
Stay hungry. Stay foolish.

メッセージ認証コード：
160191b09603044b6599a237cc2c458dd348bc37c4fae7f1674764dac45d7feb

問題の例

1 RSA暗号

- 平文をM，暗号文をC，復号文をM'
- 暗号文CはM^eをnで割った余り：$C \equiv M^e \pmod{n}$
- 復号文M'はC^dをnで割った余り：
  $M' \equiv C^d \pmod{n} \equiv M^{ed} \pmod{n}$

- 平文と復号文が一致しないと「復号できた」とは言えない。
- M^{ed}をnで割った余りが必ずMになるようなn, e, dが存在することが証明されている。（オイラーの定理）

  $M \equiv M^{ed} \pmod{n}$
- ただし，$pq = n, k(p-1)(q-1)+1 = ed$, pとqは異なる素数

1.1 秘密鍵と公開鍵の生成

大きな素数を２個選ぶ．仮にこれをp, qとする

```
In [ ]: p=
In [ ]: q=
```

合成数$n = pq$を計算する。 (e,n)は公開鍵になる

```
In [ ]: n=p*q
        print(n)
```

$(p-1)(q-1)$と互いに素な正整数eを選ぶ

```
In [ ]: (p-1)*(q-1)
```

```
In [ ]: # dは秘密鍵になる
        d=818945
In [ ]: #確認
        e*d % ((p-1)*(q-1))
```

$M^{ed} \equiv M \pmod{n}$,

$n = pq, ed = k(p-1)(q-1)+1$

1.2 オイラーの定理を確認

- M^{ed}をnで割った余りが必ずMになるようなn, e, dが存在することが証明されている。（オイラーの定理）

  $M \equiv M^{ed} \pmod{n}$
- ただし，$pq = n, k(p-1)(q-1)+1 = ed$, pとqは異なる素数

```
In [ ]: # 平文Mを指定（nより小さい数）
        M=10
In [ ]: M%n
In [ ]: M**(e*d) % n
```

1.3 RSA暗号と復号を試す

- 平文をM，暗号文をC，復号文をM'
- 暗号文CはM^eをnで割った余り：$C \equiv M^e \pmod{n}$
- 復号文M'はC^dをnで割った余り：
  $M' \equiv C^d \pmod{n} \equiv M^{ed} \pmod{n}$

```
In [ ]: # 平文Mを指定（nより小さい数）
        M=15
In [ ]: #暗号文
        C = M**e % n
        print(C)
In [ ]: #復号
        C**d % n
```

--- 一部省略 ---

LMS上での問題

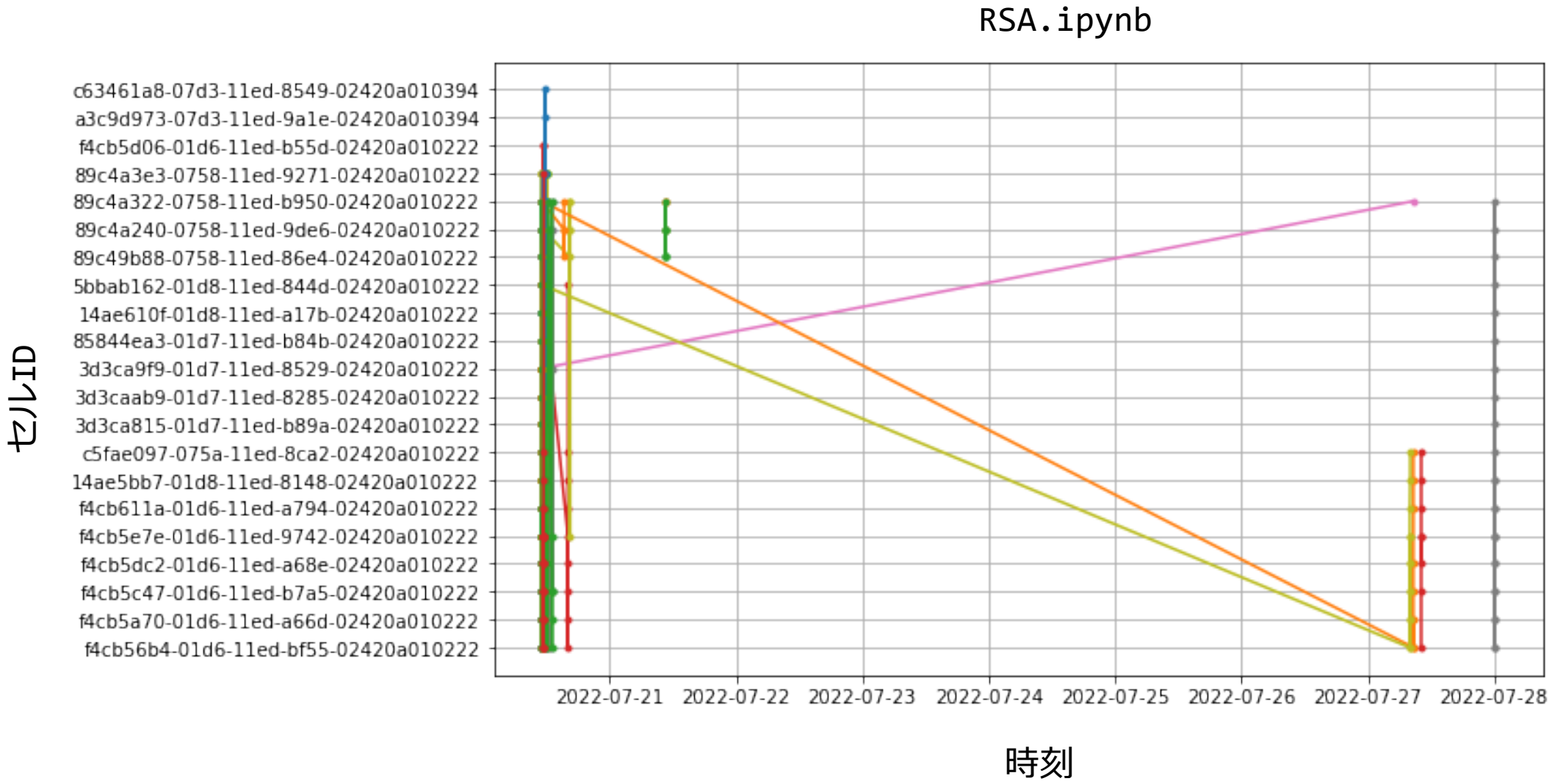
RSA暗号

- p=3，q=11としてn，e，dを選んでみよ

- 選んだe，d，nでM=17を暗号化／復号してみよ

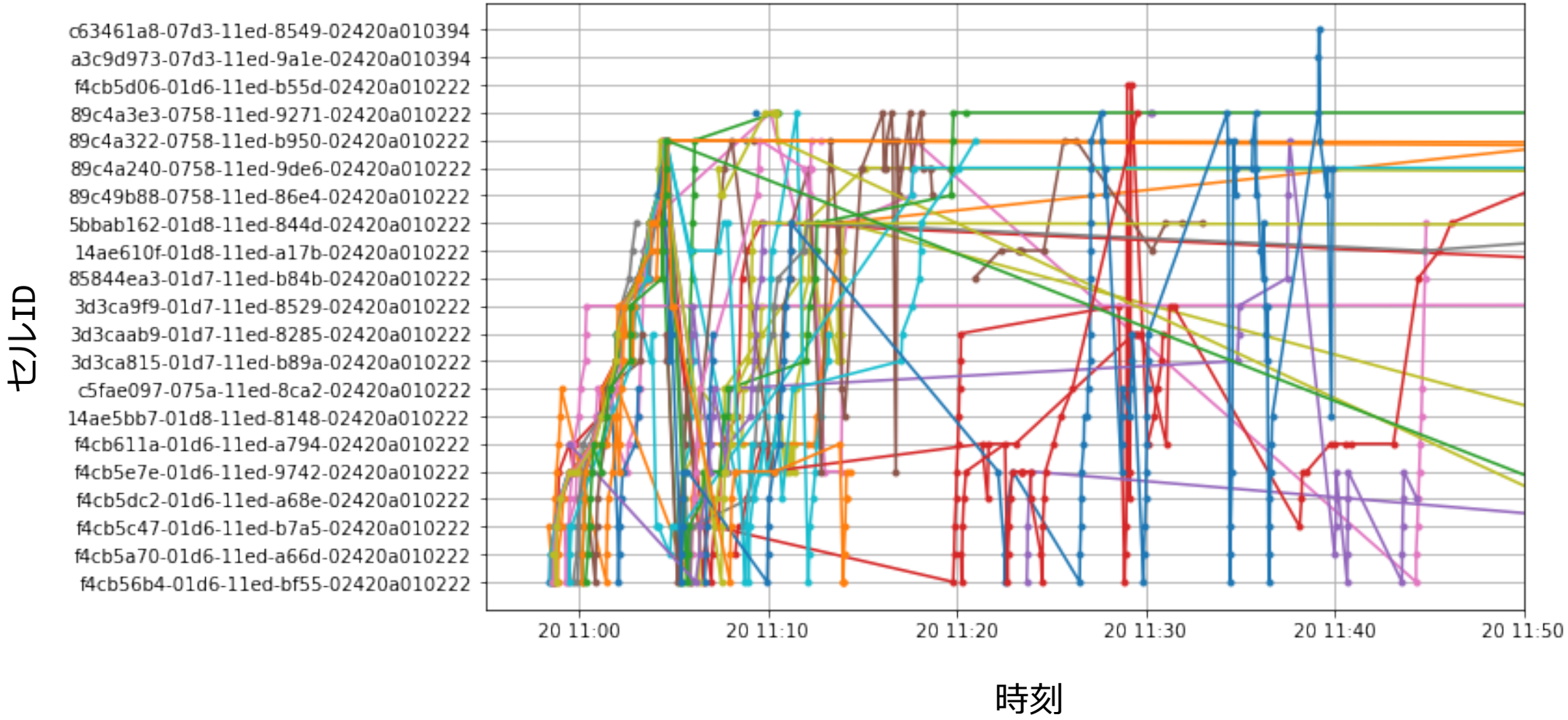
実行結果

セル実行の分布

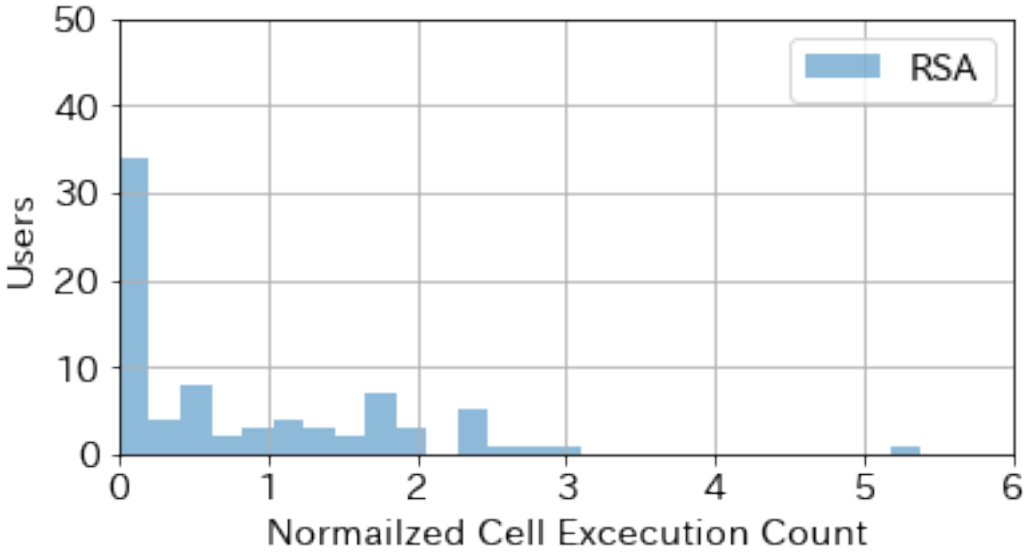

RSA.ipynb
セルID
c63461a8-07d3-11ed-8549-02420a010394
a3c9d973-07d3-11ed-9a1e-02420a010394
f4cb5d06-01d6-11ed-b55d-02420a010222
89c4a3e3-0758-11ed-9271-02420a010222
89c4a322-0758-11ed-b950-02420a010222
89c4a240-0758-11ed-9de6-02420a010222
89c49b88-0758-11ed-86e4-02420a010222
5bbab162-01d8-11ed-844d-02420a010222
14ae610f-01d8-11ed-a17b-02420a010222
85844ea3-01d7-11ed-b84b-02420a010222
3d3ca9f9-01d7-11ed-8529-02420a010222
3d3caab9-01d7-11ed-8285-02420a010222
3d3ca815-01d7-11ed-b89a-02420a010222
c5fae097-075a-11ed-8ca2-02420a010222
14ae5bb7-01d8-11ed-8148-02420a010222
f4cb611a-01d6-11ed-a794-02420a010222
f4cb5e7e-01d6-11ed-9742-02420a010222
f4cb5dc2-01d6-11ed-a68e-02420a010222
f4cb5c47-01d6-11ed-b7a5-02420a010222
f4cb5a70-01d6-11ed-a66d-02420a010222
f4cb56b4-01d6-11ed-bf55-02420a010222
2022-07-21
2022-07-22
2022-07-23
2022-07-24
2022-07-25
2022-07-26
2022-07-27
2022-07-28
時刻

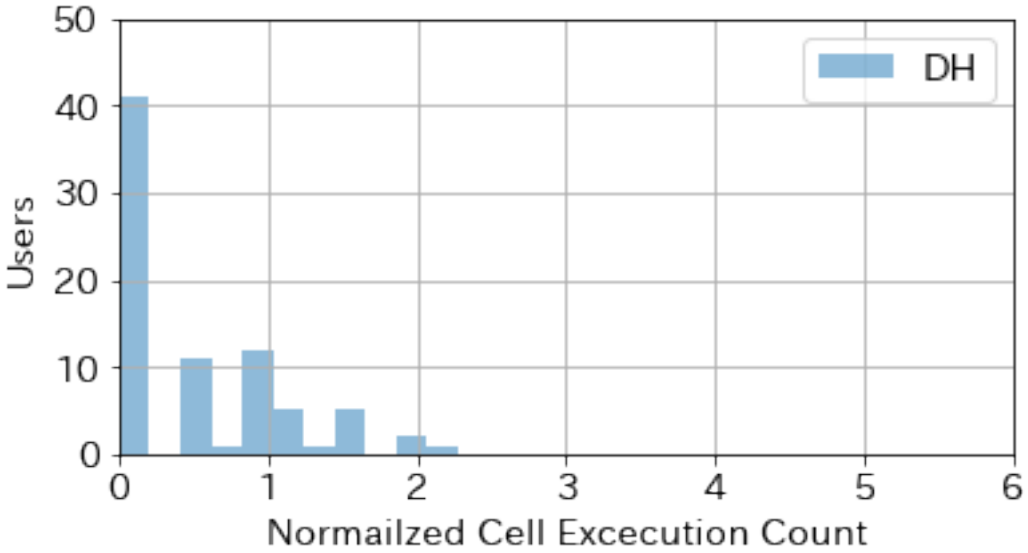
実施結果と考察

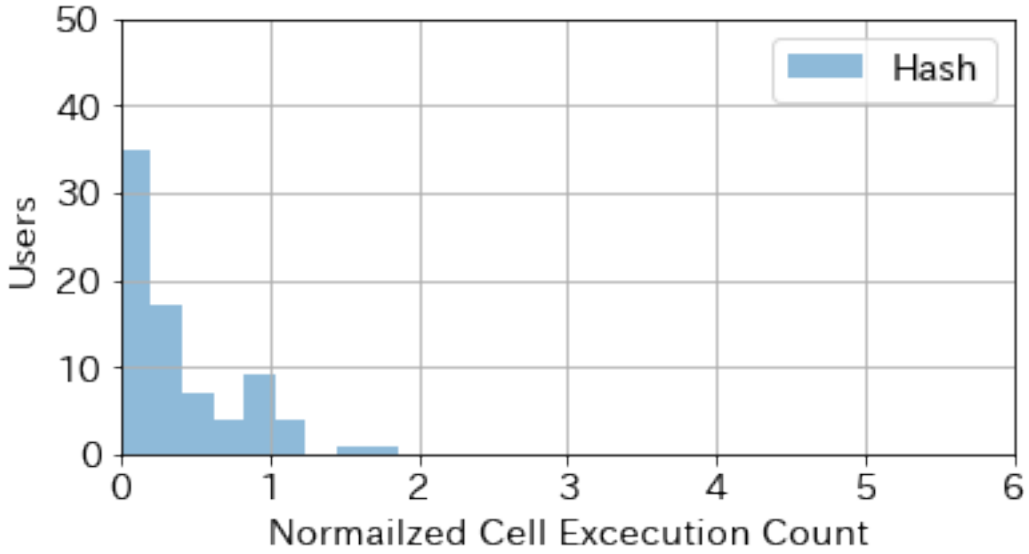
RSA.ipynb



セル実行回数分布



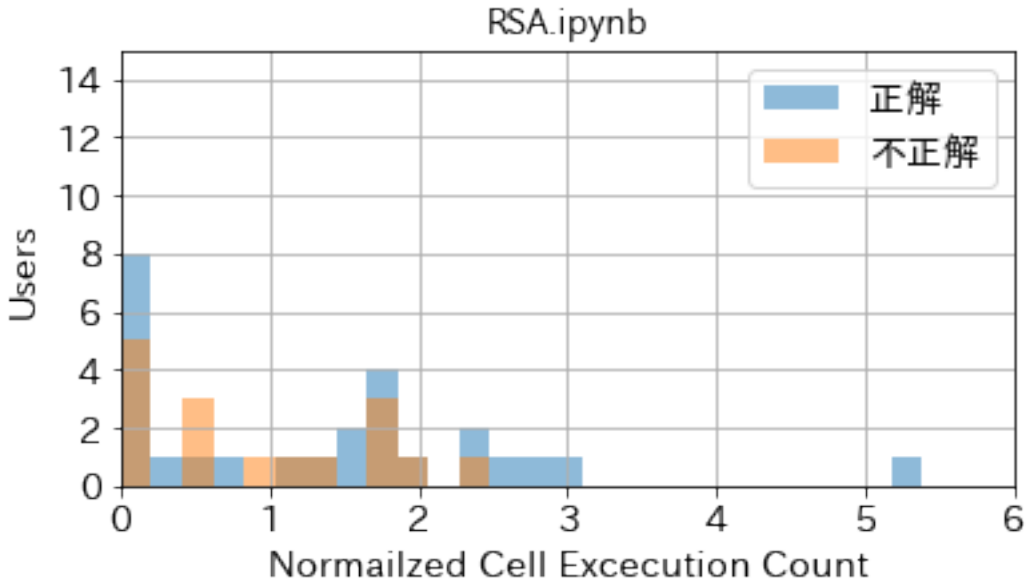


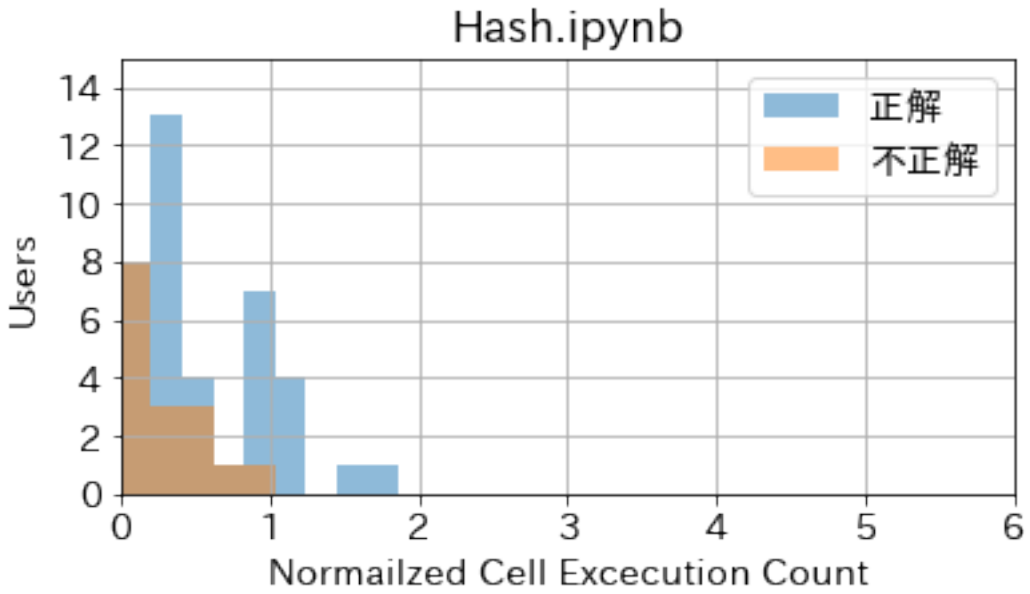


規格化したセル実行回数
＝セル実行回数/Notebookの全セル数

- 一回もセルを実行できていないユーザが少なからずいる
- Hashの実行回数が少ないのは，問題と関係ないサンプルセルが多かったため

問題正答との関連

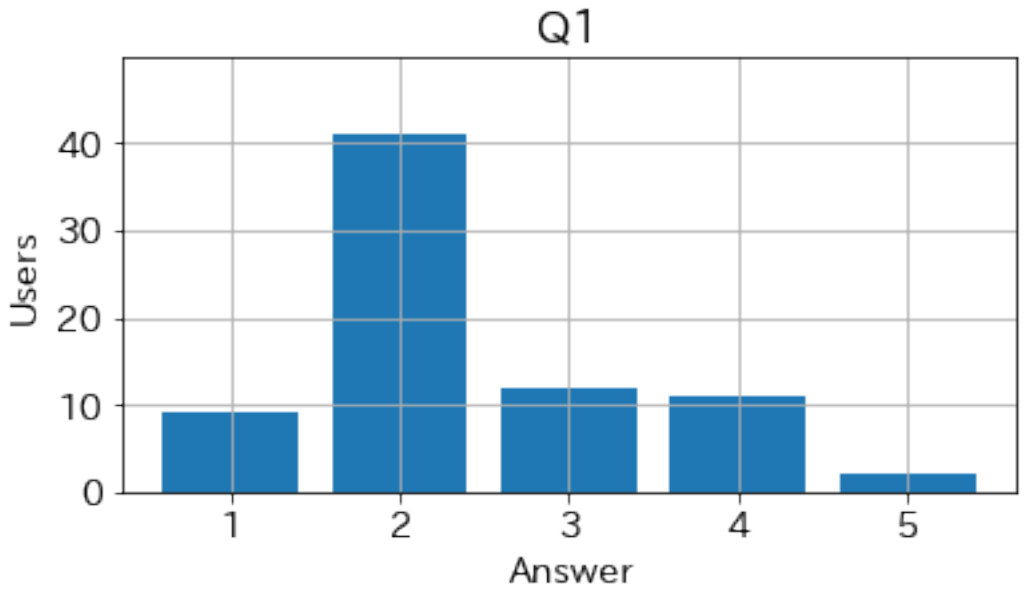




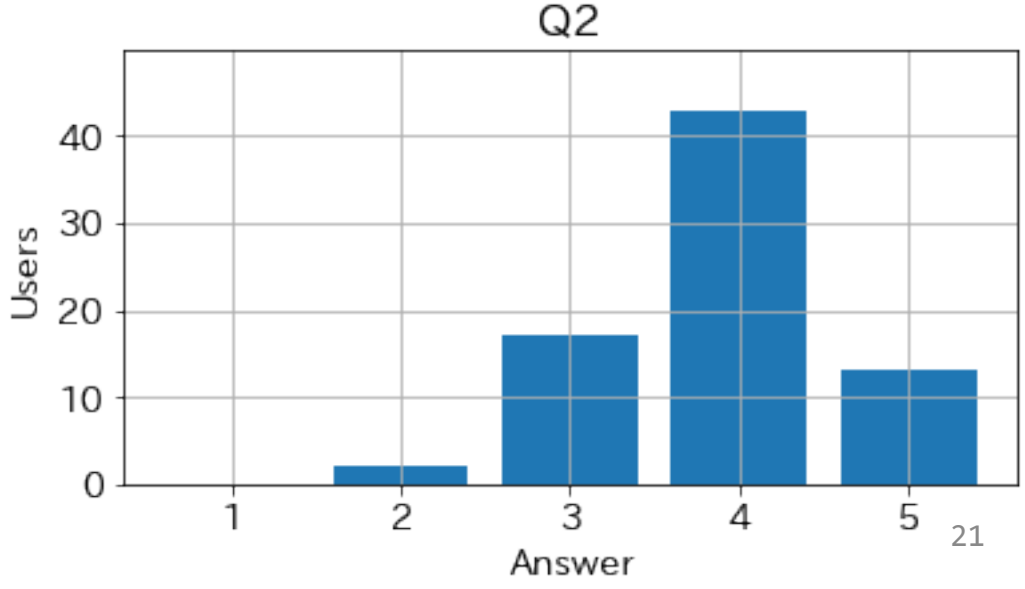
どちらの問題でも，問題正解者の方が，セル実行回数が多い傾向

アンケートとの関連

- Q1 CoursewareHubの利用は難しかったでしょうか？
  1．とても難しかった
  2．難しかった
  3．どちらともいえない
  4．簡単だった
  5．とても簡単だった

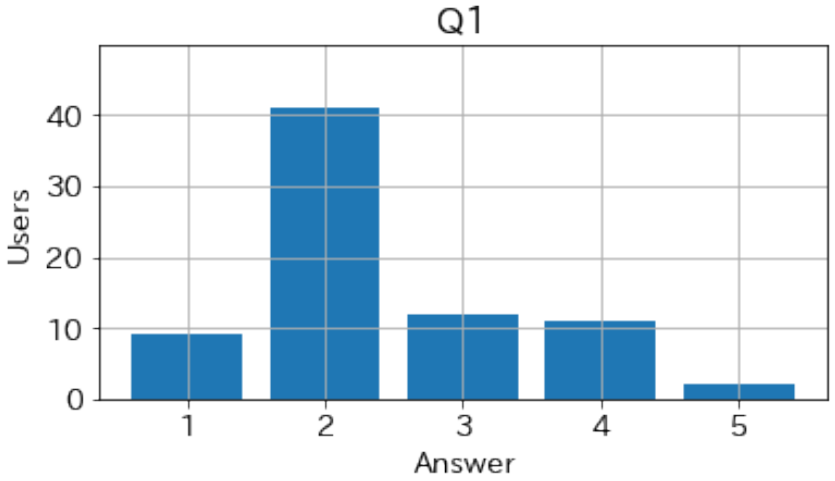


- Q2CoursewareHubの教材は授業内容の理解に役立ちましたか？
  1．全く役に立たなかった
  2．役に立たなかった
  3．どちらともいえない
  4．役に立った
  5．とても役に立った

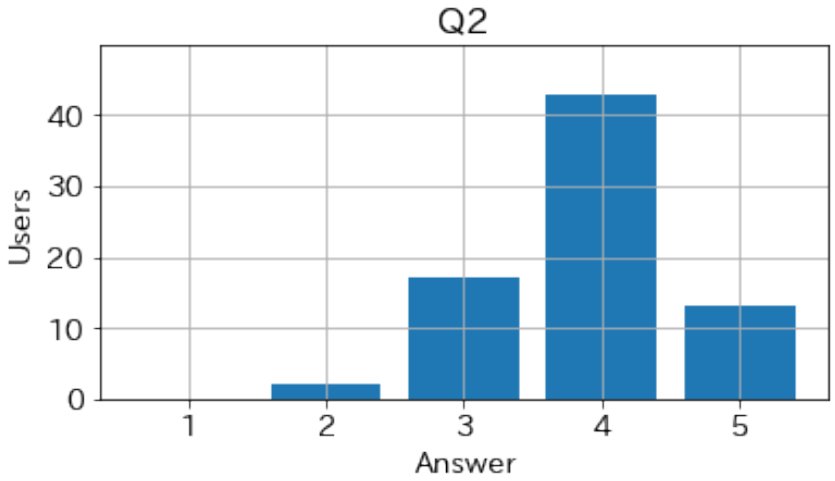


アンケートクロス集計

CoursewareHubの利用は
難しかったでしょうか？



CoursewareHubの教材は授業内
容の理解に役立ちましたか？



Q2

Q1	1	2	3	4	5
1	0	0	3	4	2
2	0	1	11	23	6
3	0	1	1	8	2
4	0	0	2	6	3
5	0	0	0	2	0

難しい方は，教材が役に立たないと回答
する傾向があるが，かなり少数

全体としては，教材が役にたたないとは
考えていないように見える

自由記述

- 学外から使用すると、VPNの影響かどうかわからないが、２～３回プログラムを実行しただけで動かなり、使いづらかった。
- 使っていくうちに少し慣れてきた。
- 接続が悪く利用できないことが何度かあった
- CoursewareHubは扱うのにpythonの知識が必要なので、初心者には難しいものだと思いました。
- ウェブ上で教科書のようなものを使うのは新鮮で面白かった。演習として用いることができたのも嬉しかった。
- 特に数式を使えるのが楽しかった。
- 実際にコマンドを実行することで、文章のみの授業よりも格段に面白く、分かりやすくなったと思います。
- ペースが速く，ついていけないことが多かった.
- 実際にコマンドを実行してみることで理解が深まった。
- 授業で学んだことを実演することでさらに理解が深まった。
- 実際に学んだことをすぐに実践することができてわかりやすかったです。
- こちらとしてはENTERを押すだけなので、扱いが難しいということはなかったが、あまり理解にはつながらなかったと思う。
- プログラミングについてはあまり詳しくないので、プログラムを理解することはできなかったが、授業内容の理解には役に立ったと思う。
- CWHでのアドレスなどの計算をするとき、セル内の数字を変えようとしたら計算ができなくなって難しかったが、コンピュータの情報を色々まあ部ことができて良かったです。
- 個人的には結構CWHを使うのは楽しかったので、来年以降も使い続けた方がいいと思います。
- 実際にやってみることで、どこにどんなことがかかれているのか、どんなことをしているのか理解がしやすかったです。

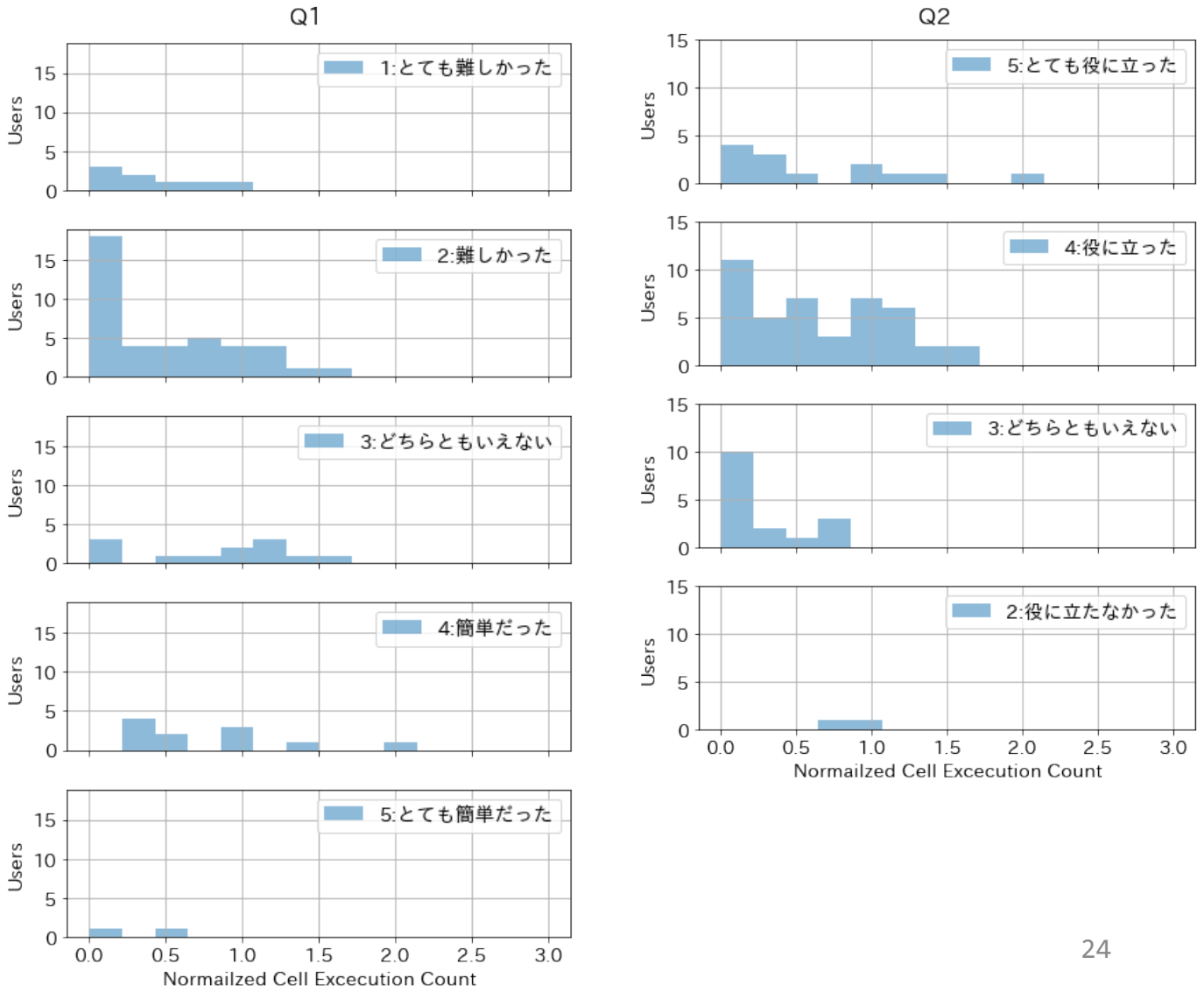
セル実行回数とアンケートの関連

難しいと感じる方は，そもそもセルが実行できてない

VPNの利用と関連している可能性がある

役に立ったとと感じるかどうかは，難しさよりも，セルの実行回数との関連は低い

一度もセル実行していない方	23名
とても難しい	3
難しい	14
どちらともいえない	3
簡単	0
とても簡単	2
無回答	2



セル実行時間間隔と正答の関係

	不正解	正解
間隔なし	5	26
間隔あり	1	1

電子署名の問題

	不正解	正解
間隔なし	15	35
間隔あり	1	4

メッセージ認証の問題

以下を区別した
　　間隔なし：セルをある時点でまとめて実行して演習を行った
　　間隔あり：何回かに分けて実行して演習をした
今回は，セルの実行間隔が1時間を超えた場合，複数回に分けてセルを実行したと判断した.

実行間隔があいているユーザ（復習）はそもそも少ない
復習したかしないかに関して，違いを議論することはできなかった

まとめと展望

- 群馬大学の1年生の情報系講義に対して，CoursewareHubを利用した演習を行った.
  - Notebook実行ログの結果
    - 課題の正答率が高いほど，セル実行回数が多い傾向がみられた.
    - 復習を行なった学生が少なく，復習の効果はわからなかった.
  - アンケートの結果
    - CoursewareHubが役に立った
    - 使用感については難しかったという傾向，原因は判断できなかった。
      - VPN/Notebookの内容/CoursewareHub自身によるもの
- 今後の展望
  - セル実行の時系列データの活用

＊本研究成果の一部は，データ活用社会創成プラットフォームmdxを利用して得られたものです。