# 感染症の流行シミュレーション

## The simulation of epidemic of infectious diseases

赤堀涼太郎　冨岡直毅　中川彰文

指導者：橋村泰司　太田伸一

**要旨**

近年,毎年のように冬になると感染症の流行が起こっている。私たちはMicrosoft Excel(以下「Excel」と記す）を用いて感染症の流行の様子をシミュレーションした。その結果，私たちは感染症がどのように広がっていくかを視覚的に確認することが出来た。

In these days, infectious disease is epidemic every year in winter. We tried to simulate infection of the disease by using Excel spreadsheets. As a result, we were able to check visually how infectious disease spread.

キーワード:SIRモデル，コンピュータシミュレーション，Excel

## １．序論

販売店の売り上げをシミュレートするような簡単なものから，地球シミュレーターのような地球全体の環境変動の様子をシミュレートするという複雑なものまで，現在，様々な事象をシミュレートによって予測できる。本研究では，私たちの身近にある表計算ソフトウェアであるExcelを用いて,シミュレーションの研究を行うことにした。Excelの機能を最大限に活用できるシミュレーション方法を考えた場合，汎用性も考慮すると，セルオートマトン方式が最も適していると考えられる。そこで私たちはセルオートマトン方式でシミュレーション研究をするにあたり，感染症の流行を示すモデルが最も適していると考え，本研究を行った。

## ２．研究内容

〈研究目的〉

感染症がどのくらいの早さで，どのようにひろがっていくかを，視覚的にわかりやすく捉えられるように感染症流行シミュレーターを作成する。

〈本研究における感染症について〉

本研究における感染症とは，以下，次の条件を満たすものとする。

① 接触感染，飛沫感染によって感染が拡大する。
② 潜伏期間を持たず，感染したものはすぐに他のものを感染させる。
③ 一度感染したことのあるものは，免疫を持ち，再感染をしない。

実験１：感染症の流行をグラフに示す

〈目的〉

Excelの表計算機能を用いて感染症の流行の様子をグラフに表す。

[感染拡大の数学モデル]

このモデルは，ケルマックとマッケンドリックによって開発されたモデルであり，感受性人口，感染人口，隔離された人口によって構成される。感受性人口とは，まだ免疫を持たず感染の可能性のある人口で，感染人口とはその時点で感染している人口を表し，隔離された人口は感染後に回復し免疫を取得した，もしくは感染が原因で死亡した人口である。それぞれを数理モデルでは感受性人口をS，感染人口をI，隔離された人口をRで表す。時刻ｔから$\Delta t$経過したときのそれぞれの増加

方程式は

$$S(t+\Delta t) = S(t) - \lambda S(t)I(t)\Delta t \qquad (1)$$

$$I(t+\Delta t) = I(t) + \lambda S(t)I(t)\Delta t - \gamma I(t)\Delta t \qquad (2)$$

$$R(t+\Delta t) = R(t) + \gamma I(t)\Delta t \qquad (3)$$

と表される。(1)(2)(3)式においてλは感染率と一日の接触回数の積を表す比例定数，γは回復率を表す比例定数を表す。
本実験では(1)(2)(3)式に関係する数値を表１のように定義する。

| | |
|---|---|
| 初期感受性人口(人) | 35 |
| 初期感染人口(人) | 5 |
| 初期隔離人口(人) | 0 |
| 1回の接触あたりの感染率(%) | 0.1 |
| 1日あたりの接触回数(回) | 10 |
| 1日あたりの回復率(%) | 20 |
| 時間の間隔(日) | 0.25 |
| 期間(日) | 90 |

表１　本実験における各数値の定義

〈方法〉
① 図１の様に t,S(t),I(t),R(t)の値を入力する。
② それぞれ(1)(2)(3)式に基づいて単位時間を 0.25[日]とし，t=90[日]まで計算させる。
③ 計算によって出た値を基にグラフを作成する。

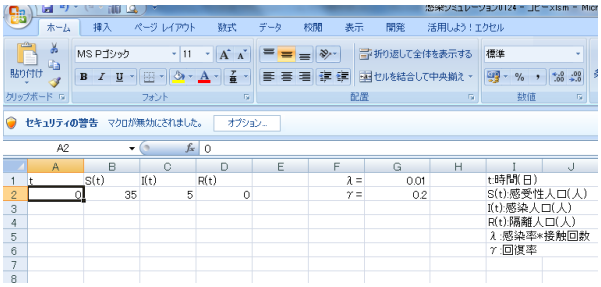



図１　それぞれの値を入力する様子

〈結果〉
図２の様に感染症の流行による各人口の変化の様子をグラフで示すことが出来た。以下，このグラフを理論値のグラフと呼ぶことにする。

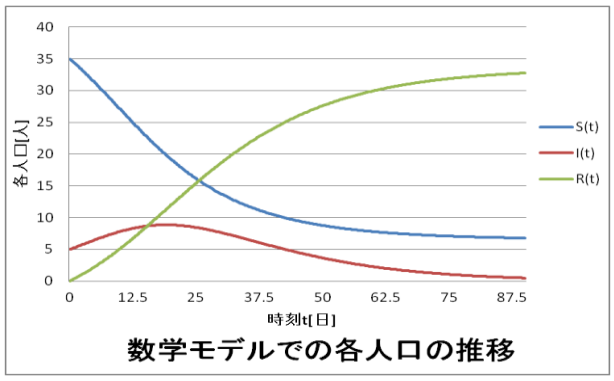



図２　感染症流行時の各人口の推移の様子

〈考察〉
図２の I(t)に注目すると，t=20 付近で極大値を取っている。よってこのときが感染症の流行のピークであると考えられる。
このように，感染症の流行は，一度流行のピークを向かえ，経過時間とともに自然に流行が衰退していくと考えられる。

実験２：セルオートマトン方式で感染症の流行の様子をシミュレーションする。

〈目的〉
Excel のマクロ機能を用いて，セルオートマトン方式により，学校の教室内で感染症の感染が拡大した場合をシミュレーションする。

[セルオートマトン方式]
ある事象において，それが何か外部の指令によって引き起こされるのではなく，全体を構成するメンバーまたは要素のそれぞれが周囲の状況を判断して一定のルールを振る舞うことである秩序が形成され事象が起こるとき，この局所的なルールに基づく相互作用を調べるために使用される計算モデル。分割された均一なセル同士の相互作用によって自動的に動作が行われる。

[感染拡大の決定]
本研究では，式(4)に基づいてシミュレーションを行った。
=IF(OR(注目セル<=0,注目セル>1,注目セル=""),IF(OR(注目セル>1,注目セル=""),IF(OR(AND(0<近傍セル,近傍セル<1),RANDBETWEEN(1,100/感染係数),IF(注目セル="","",注目セル)),注目セル),注目セル-回復係数)…(4)

また，感染係数，回復係数は次の様に設定する。
感染係数　（病原菌の感染率×接触回数）
（ただし，本研究ではシミュレーターの整合性を示すため，この値は $10^n$ とする）
回復係数　$(感染期間)^{-1}$

［感染拡大の範囲］
本研究では，実際に我々が学校内で生活する教室での感染拡大の様子を示す。

〈方法〉
①感染症の教室内での感染拡大を式（４）に基づいてシミュレーションを行う。この時初期条件を表１と同じにする。
②単位時間 t を 0.25［日］として，感染の流行が終了するまでシミュレーションする。
③更新ボタンを押すごとに，感受性人口，感染人口，隔離人口を測定する。
④測定値から，グラフを書く。

〈結果〉
図３～図８に示すように感染症の感染拡大をシミュレーションすることができた。

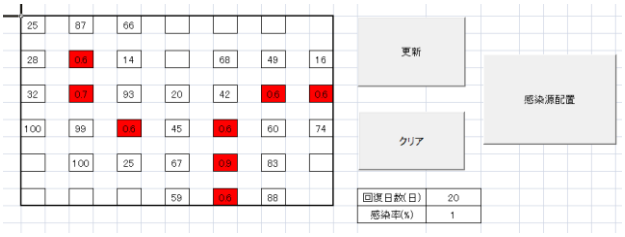


図３　t=10 の様子

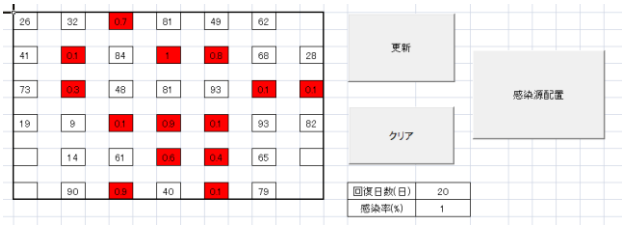


図４　t=20 の様子

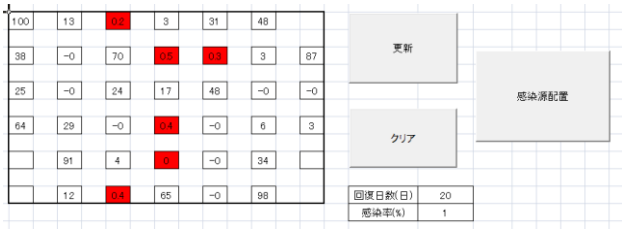


図５　t=30 の様子

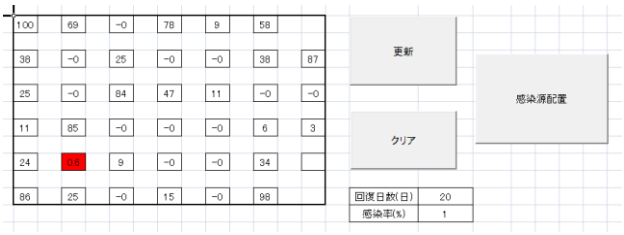


図６　t=40 の様子

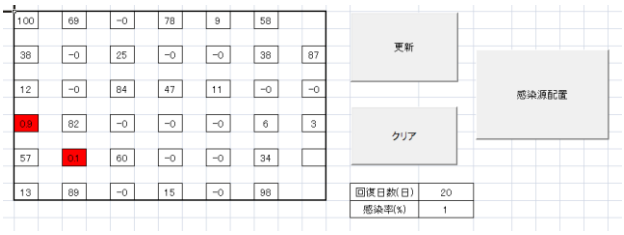


図７　t=50 の様子

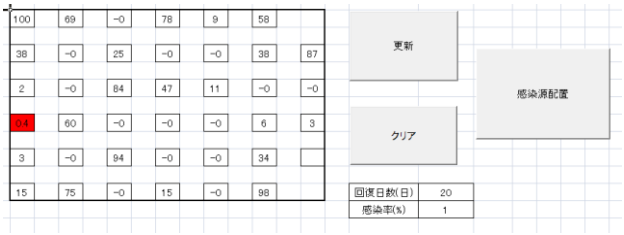


図８　t=60 の様子

さらに，この時の各時刻の人口をグラフにすると，図９のようなグラフが得られた。

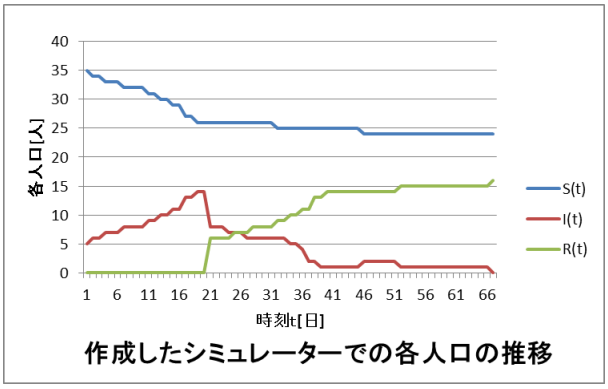


図９　シミュレーターでの各人口の推移

〈考察〉
我々が作成したシミュレーターによる感染症の流行の様子でも理論値のようなグラフを描くことができた。
理論値のグラフと比較すると，グラフの概形は理論値のグラフと近い。しかし，数値にはずれが見られる。この原因は，理論値のグラフは計算式から導き出した普遍のものであるが，シミュレーションでは，各時刻ごとの感染者の配置により異なるためと考えられる。

## 3.結論

Excel の表計算機能およびマクロ機能を用いて，感染症の流行拡大の様子をシミュレーションすることができた。実験１，実験２のグラフの比較により，我々が作成したシミュレーターの整合性も示すことができた。今後は，潜伏期間のある感染症，感染症予防による流行の衰退がある場合も考慮して研究したい。

## 4.参考文献

1)三井和男:新 Excel コンピュータシミュレーション　数学モデルを作って楽しく学ぼう，pp.33-44　pp.167-189
2)エクセルでシミュレーション
http://www.din.or.jp/~take_din/math/inful.htm
3)感染症流行モデル
http://dr-urashima.jp/pdf/kaneki-2.pdf

# 人間の判断を用いた本文解析による標的型メールの識別精度向上

川上幸起　小野裕之　谷村勇大　山田敬汰　吉川大智

指導者：橋村泰司　太田伸一

**要　旨**

今日，企業や行政を対象とした標的型メール攻撃の脅威が増大しており，対策は急務である。しかしながら，従来のセキュリティ対策ソフトウェアによる検知は難しい。この原因は，安全のメールと攻撃を意図したメールの識別が困難なことにあると考えられる。そこで，我々は，メールの識別においてメール本文の解析を用い，その解析に人間の判断を加えることで，より高精度な識別を行うことを目的として，ソフトウェアを作成し，実験によって有用性を検証した。

キーワード：標的型メール，標的型攻撃，セキュリティ対策ソフトウェア，メール本文

The threat of the targeted e-mail attack to the enterprise and the administration increases today. Measures of the attack are pressing needs. It is thought that one of the reasons for it is difficult to distinguish between safe e-mail and targeted e-mail. Then,  we made the software to improve the detection accuracy by adding man's judgment to the judgment of e-mail

## １．序論

標的型メール攻撃とは，主に企業や行政に対して行われる標的型攻撃の一種で，通常のメールを装い，添付ファイルやURLを開かせることによって，標的に侵入し情報の搾取やシステムの破壊などを行う攻撃であり,近年,被害が急増しており，対策は急務である。この攻撃は，情報処理推進機構が発表した“情報セキュリティ10大脅威2016“の中で組織がもっとも警戒すべき脅威とされている[1)]。2015年に発生した，日本年金機構を標的とした攻撃によって125万件の個人情報が流出したこと[3)]は，日本中に大きな衝撃をもたらした。最近になって，その手口は巧妙化しており，従来の差出人のヘッダーやアドレス，添付ファイルの検査を行うソフトウェアや使用者への教育などの対策では被害を防ぐことが難しくなってきている[1)]。現在コンピュータにおけるセキュリティの研究が盛んに行われているが，どれも良い結果を残せていない。我々は，標的型メールなどのメールの分析に従来はほとんど目を付けられていなかったメールの本文を解析することでメールの識別に新たな指標を加えることができるだろうと考えた。しかし，コンピュータによる文の解析は研究段階であり，現状ではプログラムしたソフトウェアで,文を解析することは困難である。そこで，解析の一部に人の判断を加えることで解析が可能になるのではないかと考えた。この研究では，ユーザーがメールを閲覧する直前に，人の判断を利用して解析・識別することで，これまで検知することが難しかった標的型メールを検知することを目標として，ソフトウェアを作成し，有用性を検証した。

## ２．研究内容

本研究では,メールの本文中にある語を検知し，その文脈や内容が標的型メールによく見られるものであること，文法の不自然さなどをユーザーに判断させ，その判断をもとに，メールが攻撃を目

的としたものかどうかを識別するソフトウェアを作成する。そして，そのソフトウェアを用いることで標的型メールを検知できることを検証する。

ソフトウェアの作成.

今回は，メインプログラムに Java，データベース管理に MySQL を使用し，統合開発環境 eclipse にて開発を行った。

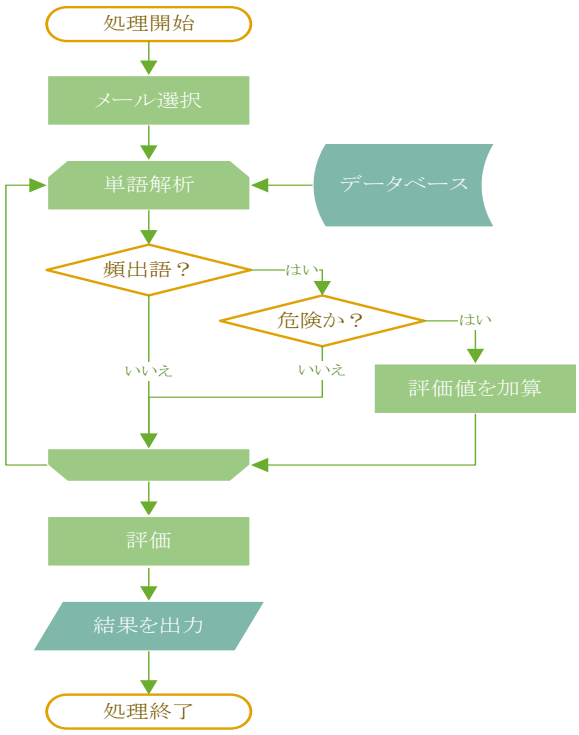



図１　ソフトウェアの挙動の概要

図１は作成したソフトウェアの挙動の概要である。単語検知は一文ごとに行い，検出された文中の単語が強調表示され，ユーザーがそれを見て判定する。ユーザーが危険であると判定した場合は，判断された語に予め与えられた評価値が加算される。安全であると判断した場合は加算されない。評価値とは出現回数に基づいて，識別のために各語に割り当てられた値である。こうして得られた評価値の合計の平均が一定の基準値を越えるかどうかで識別する。評価値と基準値については後述する。

予備実験.

〈目的〉

メール内に多く出現する語を選定する。

〈方法〉

(1)インターネット上にある多数の標的型メールと安全なメールのサンプル，それぞれ 40 通と 20 通を集める。

(2)集めたメールから出現回数の多い語を図２のように EKwords 2004 によって品詞分解と集計を行う。

(3) ワードを選定する。※選定の基準は出現回数がメール中の語の合計の内，上位１％以上のものとする。


図２　EKwords を用いた語の集計

〈結果〉

実験の結果，21 種類 46 語を検知に用いる語とした。

実験１.

〈目的〉

各語の評価値を設定する。

〈方法〉

(1)それぞれのメールに含まれる割合を求める。

(2)割合をもとに各語に評価値を付与する。

母数が違う（標的型メールは 40，安全なメールは 20）ので安全なメールの出現回数を２倍して評価値を求める。

$$\frac{\text{標的型 出現回数}}{\text{標的型メールへの出現回数} + \text{安全メールへの出現回数} \times 2} = \text{評価値}$$

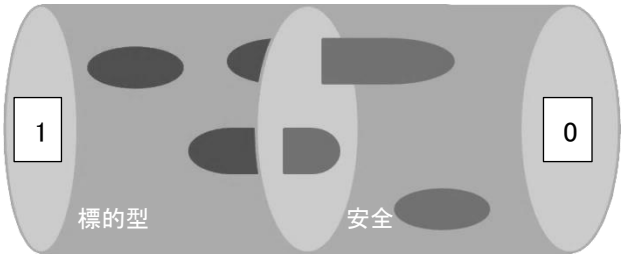



図３　評価値を付与するイメージ

〈結果〉

評価値の決定に用いたデータと，それを基に導き出した評価値の一覧を一部抜粋して示す。

**表　評価値の決定**

| 語 | 標的型（回） | 安全（回） | 評価値 |
|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ |
| 依頼 | 0 | 8 | 0 |
| 確認 | 13 | 5 | 0.565 |
| 期限 | 4 | 0 | 1 |
| 至急 | 10 | 1 | 0.833 |
| 詳細 | 6 | 6 | 0.333 |
| 資料 | 16 | 15 | 0.347 |
| ⋮ | ⋮ | ⋮ | ⋮ |

上記のデータを基に計算し評価値を求めた。

**表　語とその評価値**

| 語 | 評価値 |
|---|---|
| ⋮ | ⋮ |
| 添付 | 0.35 |
| ファイル | 0.38 |
| 確認 | 0.56 |
| 至急 | 0.83 |
| ⋮（他） | ⋮ |

〈考察〉

標的型メールは安全なメールと大差ない文面であることが特徴であるため，通常のメール対策では警戒される「添付」などの語は大きい評価値とならなかった。これらの語は，安全なメールにも多いため，評価値が小さくなったと考えられる。逆に，「至急」や「確認」など資料の確認を求める言葉は，標的型攻撃においてファイルを開く行為自体が攻撃の成功に大きく関わっているため，大きな評価値を持ったと考えられる。

実験２

〈目的〉メールを正確に識別するための判断基準値を求める。

〈方法〉

(1)標的型メールと安全なメールの中から，それぞれ無作為に複数個ずつ選ぶ。

(2)被験者にメールをソフトウェアを用いて判別させる。

(3)被験者の選択を記録し，基準値を変化させて，各基準値での挙動を再現する。

(4)各メールが正常に判断できる基準値を絞り込む。

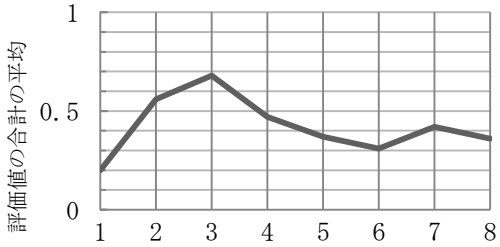



図４　絞り込みのイメージ

(5)正常に判断できる確率が高い基準値を求める。

〈結果〉

各判断基準値における識別の正誤を示す

**表**　各基準値における識別の正誤

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 0.75 | ○ | × | × | × | ○ | × |
| 0.50 | ○ | ○ | × | ○ | ○ | × |
| 0.4375 | ○ | ○ | ○ | ○ | ○ | ○ |
| 0.375 | ○ | ○ | ○ | ○ | × | ○ |
| 0.25 | ○ | ○ | ○ | ○ | × | × |

〈考察〉

基準値を求めることができた。しかし，0.25，0.50，0.75 の三点から正解率が高い方の間を取る操作を繰り返しているので，0.25 以下または 0.75

以上のデータを求めておらず，絞り込みも不十分と考えられる。求めていない部分のデータを取り，精度をより高めての検証が必要である。

実験３

〈目的〉

このソフトウェアの有用性を検証する。

〈方法〉

(1)標的型メールから 20 通，安全なメールから 10 通（それぞれ半数）を無作為に選出。

(2)被験者にソフトウェアを用いて識別させる。

(3)標的型メールを識別できるかを検証する。

〈結果〉

メールを正確に識別できた割合の平均は，標的型メールでは，71%，安全なメールでは 62%となった。

〈考察〉

正確な検知の割合は高くなかった。原因はメール内に発見できる単語が少なく，正確な識別ができるほどの母数を得られなかったからだ。

## ３．結論

今回の研究で，単語ごとの危険度を設定し，これだけでは無く，さらに人の判断を組み合わせて標的型メールを識別することができる割合は
71% 安全なメールを識別することが出来る割合は 62%であるということが分かった。
しかし，これからはより検知精度を上げる必要があり，そのためには基準値のより細かい精度での設定が必要であるということが分かった。

## ４．今後の方向性

(1)データベースの単語を充実させる。

(2)基準値の設定方法の見直し。

## ５．参考文献


1. IPA：情報セキュリティ白書 2016
2. 北條孝佳，松浦幹太：文字列類似性を考慮した標的型攻撃のグループ化手法
3. 日本年金機構：個人情報流出について http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai03/pdf/03shiryou01.pdf
4. 標的型攻撃メールの傾向と事例分析 https://www.ipa.go.jp/security/technicalwatch/20140130.html
5. 内田勝也： 情報セキュリティ心理学の提案
6. 山本幹雄，ほか３名：人間の理解手法を用いたロバストな音声対話システム

# 平成２８年度２年次生課題研究発表会について

1　課題研究成果発表会（校内）

ＳＳＨ研究開発プログラムの中で最も大きな位置付けをもつ「課題研究」において，２年次生が１年間にわたって取り組んできた研究の成果を発表する研究成果発表会を開催した。発展研究，論文研究について次の日程で３回の発表会を本校の第２生物教室及びサイエンス館にて行った。

1回　10月　5日(水) 13：50 ～ 15：30(６限～７限)
　　発展研究の研究成果を評価：９グループ全て口頭発表

2回　12月 14日(水) 13：50 ～ 15：30(６限～７限)
　　発展研究の研究成果を評価：９グループ全て口頭発表
　　※岡山県理数科理数系コース課題研究合同発表会のステージ発表選考会を兼ねて実施した。

3回　１月25日(水) 12：55 ～ 15：30(５限～７限)(本校サイエンス館)
　　発展研究,論文研究の論文を評価：４グループ口頭発表，９グループ全てポスター発表
　　口頭発表テーマ　①熱音響冷却装置の製作と冷却原理の考察
　　②NaCl溶液－Cu電極濃淡電池での起電力発生の原因
　　③プラナリアの自切頻度に短期間の温度上昇が与える影響
　　④人間の判断を用いた本文解析による標的型メールの識別精度向上

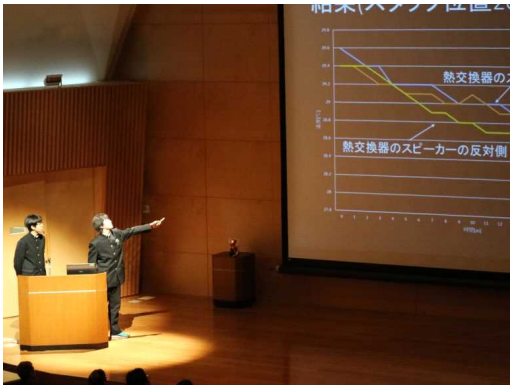
口頭発表は，スライドによるプレゼンテーションを行い，各グループ７分程度の発表を行った。

**第２回研究発表(口頭発表)**

**第３回研究発表(ポスター発表)**

2　第14回高大連携理数科教育研究会・第17回岡山県理数科理数系コース課題研究合同発表会

県内の理数科設置４校では，「課題研究」を開講し，各校が独自に実施する校内での発表会で，研究成果が報告されている。しかし，発表会を校内のみで終わらせることなく，理数系教育の共通理解と更なる充実・発展を目指して，合同の発表会が企画され，「第１回理数科課題研究合同発表会」が平成13年３月，岡山理科大学を会場に開かれた。17回目となる本年度は，平成29年２月４日(土)に岡山大学を会場に開催された。以下，この発表会の概略を示す。なお，ステージ発表では，「NaCl溶液－Cu電極濃淡電池での起電力発生の原因」が優秀賞を獲得した。




**ステージ発表**

ポスター発表

本年度は本校が当番校として，司会進行
や受付など発表会全体の運営を行った

## 平成 28 年度　第 14 回高大連携理数教育研究会
## 第 17 回岡山県理数科理数系コース課題研究合同発表会

■発表会の概要

| | | |
|---|---|---|
| 日時 | 平成 29 年 2 月 4 日(土) | |
| 会場 | 岡山大学創立五十周年記念館 | |
| 日程 | (1) 開会のあいさつ | 9:50 ～ 10:00 |
| | (2) 発表（入退場・質疑を含めて 10 分以内） | 10:10 ～ 14:50 |
| | ポスターセッション(62 組) | 13：30 ～ 14:50 |
| | (3) 指導講評 | 15:00 ～ 15:50 |
| | (4) 閉会のあいさつ | 15:50 ～ 16:00 |

■研究テーマ(ステージ)発表校

| 分野 | テーマ | 発表校 |
|---|---|---|
| 物理 | 発泡スチロール板の滑空距離の研究<br>～射出角度と重心と形状に注目して～ | 岡山一宮 |
| | 坂道を下る自転車の質量と速さ | 玉島 |
| | 静摩擦中に起こる物体接触面の変化の研究 | 津山 |
| | 熱音響冷却装置の製作と冷却原理の考察 | 倉敷天城 |
| 数学 | 暗記に適した学習アプリの開発 | 岡山一宮 |
| 化学 | 水溶液の溶質が物性に及ぼす影響について<br>の基礎的研究 | 津山 |
| | NaCl 溶液－ Cu 電極濃淡電池の陰イオンの影響 | 倉敷天城 |
| | 無機イオン吸着剤の研究<br>～第 2 報 非晶性アルミノ珪酸塩の吸着特性～ | 岡山一宮 |
| | 鉛蓄電池の自己放電に対する<br>金属イオンの影響について | 玉島 |
| 生物 | 植物由来の揮発成分による菌の増殖抑制<br>に関する研究 | 岡山一宮 |

ステージ発表表彰式

発表を終えて集合写真