悪意のあるデバイスBadUSBによる攻撃のリスク調査

山本拓巳　菊池浩明

明治大学　総合数理学部

BadUSBとは

- Black Hat 2014にてKarsten Nohlにより提案
- 一見すると普通のUSBメモリだがPCに挿入するとUSB入力デバイス(キーボード)と認識され攻撃が行われる
- 2009年にはイランの核燃料施設へのStuxnetによる攻撃で使用された

BadUSBの脅威

1. 気づきにくい
   - ファームウェアを書き換えることで攻撃を行うので，通常のウイルス対策ソフトでは検知できない場合が多い
   - デバイスドライバのインストールも多くの場合自動で行われ，短時間で終了するので見落とすケースが多い

2. 多様な攻撃の可能性
   - キーボードの操作を自由に行うことで様々な攻撃が可能
   - マウスの操作も可能

研究

■研究目的

① 本当に気づかれないか？セキュリティ知識があれば気づくことが出来るか？

② どういった攻撃が最も気づかれにくいか？

⇒BadUSBによる攻撃のリスクを明らかにする

■研究手法

BadUSBの検知度を測る実験とセキュリティ指向度調査(SeBIS)を行い，セキュリティ意識の高さがBadUSBによる攻撃のリスクと関連性があるのかを調べる

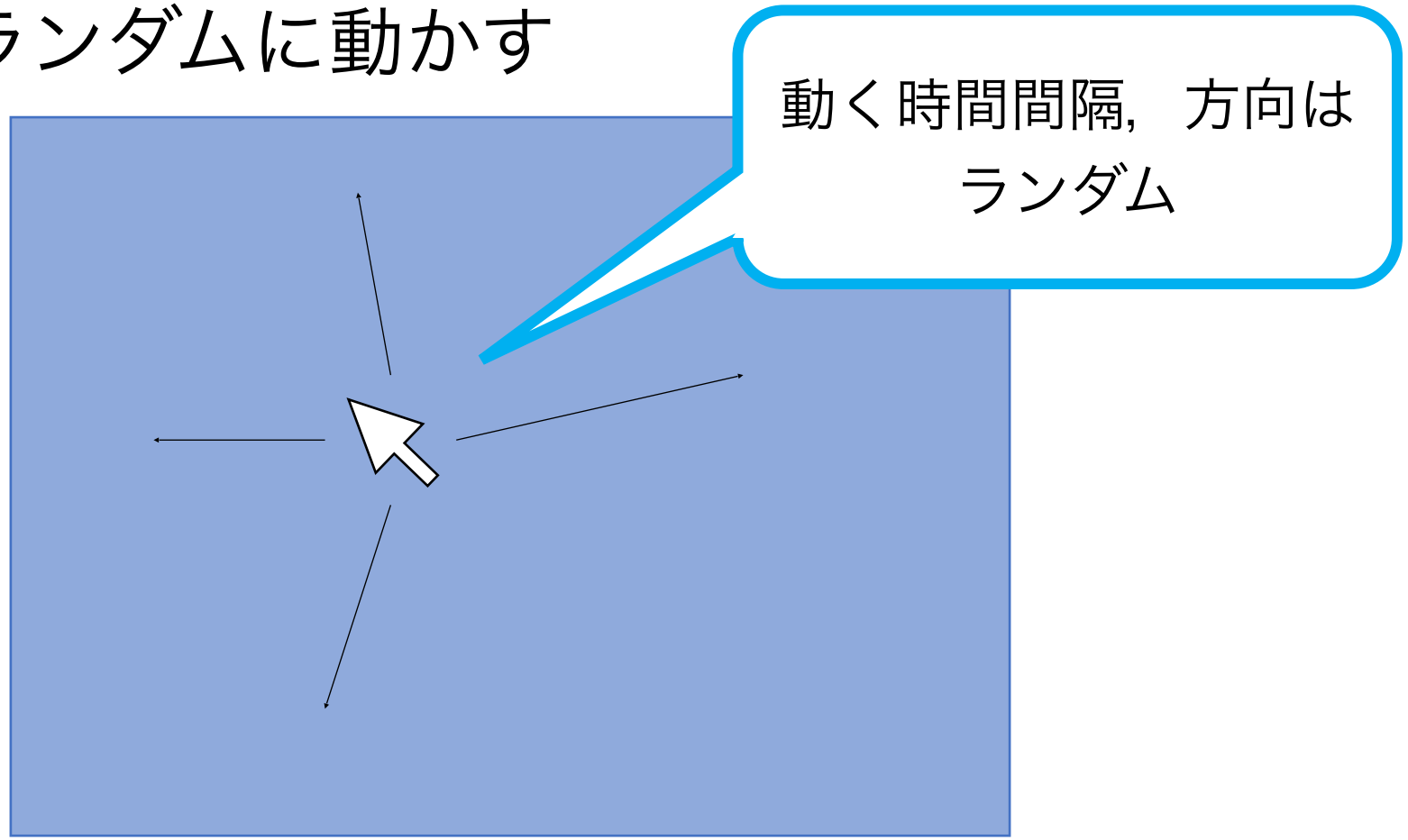
実験用BadUSBデバイスの開発

Arduinoのキーボードやマウスを操作するライブラリを使って
5つのBadUSBを実装し，これらのBadUSBを実験に使用した

1. マウスをランダムに動かす
2. カメラアプリを起動し写真を撮る
3. 何もなし（比較用）
4. テキストファイルを作成し，
   編集してから拡張子を変更
5. PCを再起動させる

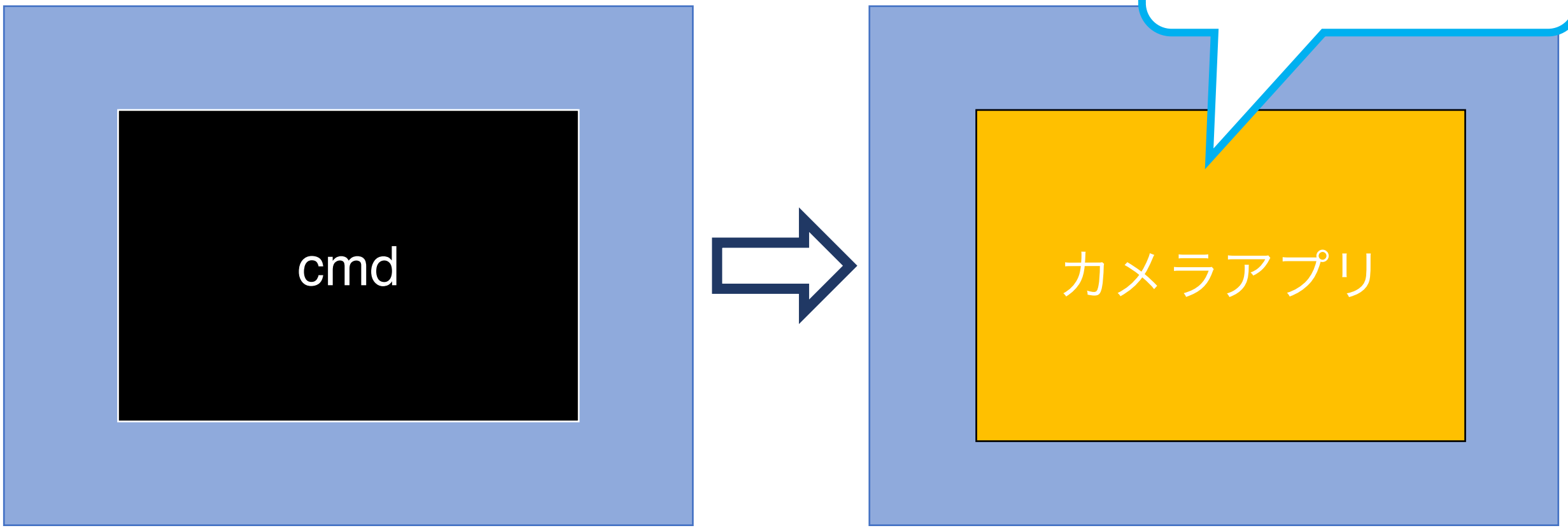
実験用BadUSBデバイス　概要

1. マウスをランダムに動かす



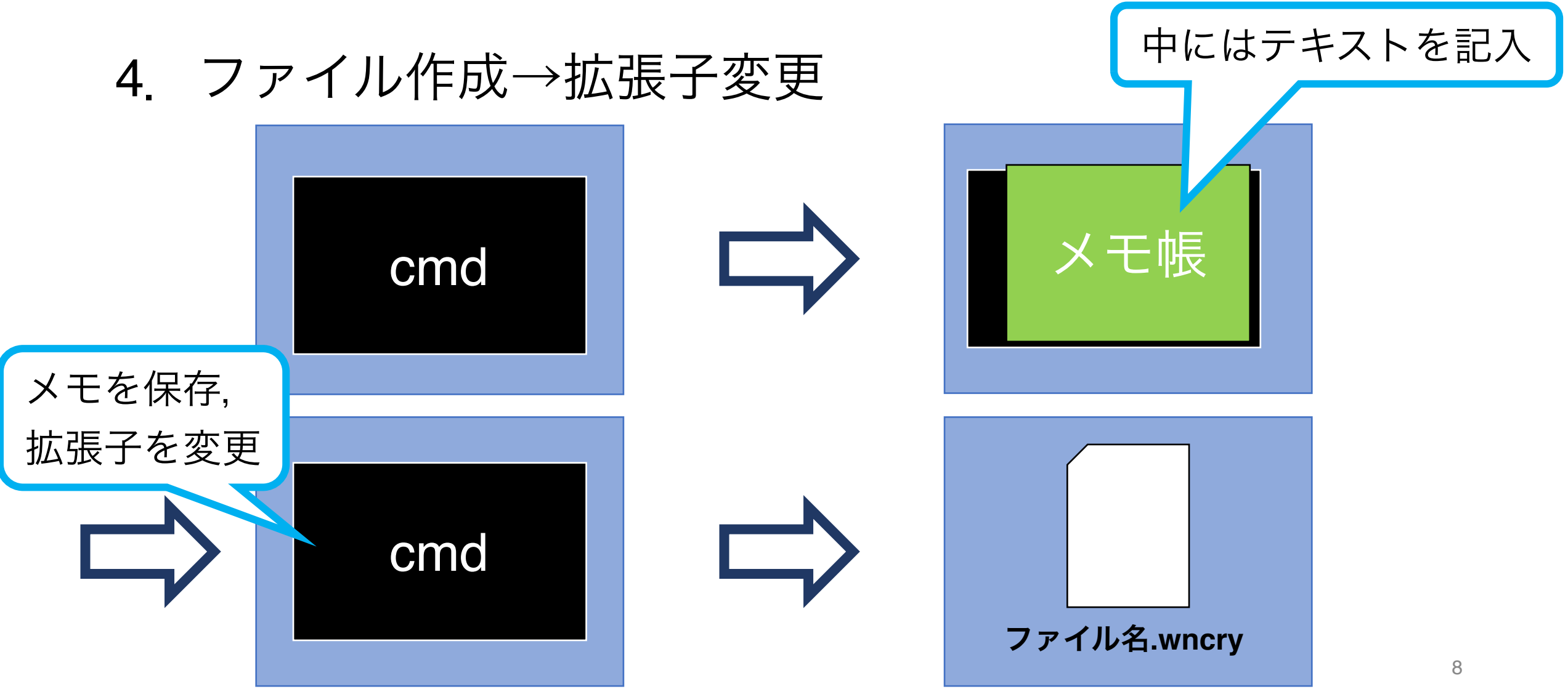
実験用BadUSBデバイス　概要

2.　カメラアプリの起動・撮影



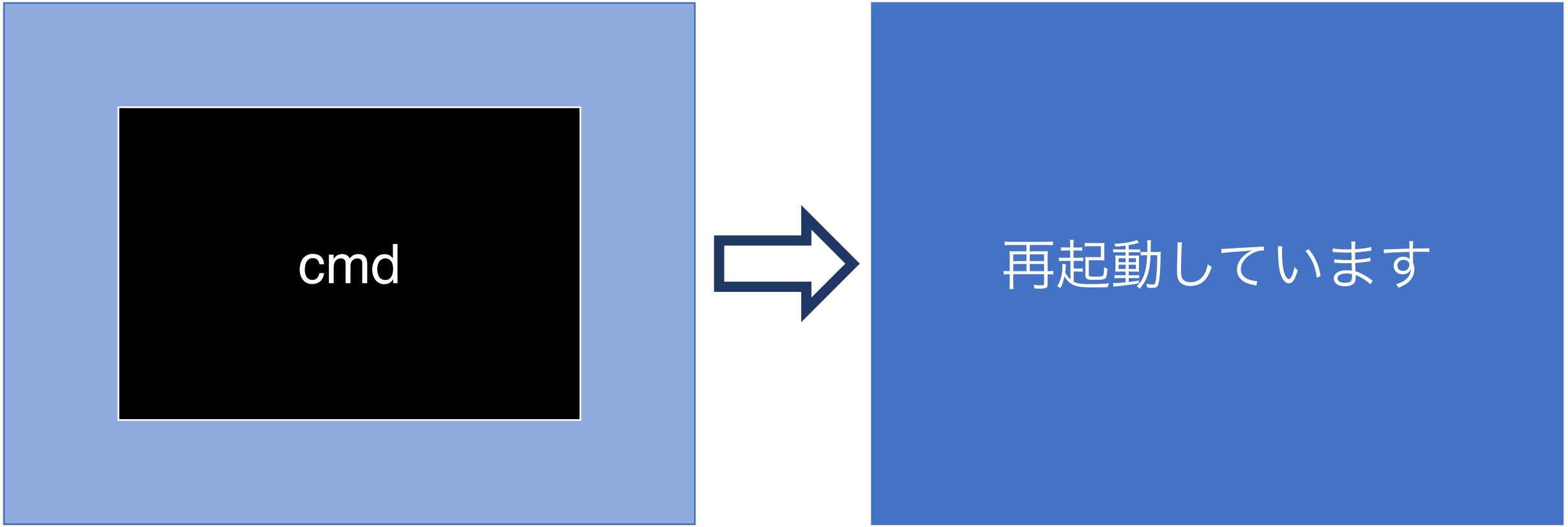
実験用BadUSBデバイス　概要

4.　ファイル作成→拡張子変更



実験用BadUSBデバイス　概要

5.　PCの再起動



評価実験方法

1. PCはあらかじめ用意したものを使用し，被験者は実装した5つのBadUSBを順番に挿し，それぞれがどのような挙動をするかを回答する(被験者がUSBを挿してから回答し終わるまでの時間を計測する)
2. 実験後にアンケートを実施し，各BadUSBの脅威度を5段階で評価する
3. その後IT・セキュリティ指向度を測るアンケートを実施し，被験者のIT指向度とセキュリティ指向度を測る

IT指向度・セキュリティ指向度調査

- IT指向度

  以下の3つの事項の内，経験があるがあるものの数（最大3点）

  i. 自身のコンピュータでOSのインストールまたは再インストールを行った
  ii. 家のネットワーク設定をした
  iii. ウェブページを作成した

- セキュリティ指向度（SeBIS）

  18問の質問について，しない(1)，まれに(2)，時々(3)，頻繁に(4)，常に(5) の5つの選択肢の合計値（最大90点）

  - 席を離れる際にPCのスクリーンをロックする
  - 自身が使っているプログラムが常に最新であることを確認している

  等

実験概要

- 実施期間

  2017年11月27日~12月1日

- 実施場所

  明治大学中野キャンパス　1005実験室

- 被験者

  明治大学及び大学院に所属する学生31名

- 実験状況

  PCはThinkPadを使用　OSはWindows10

  実験は一人ずつ(一人15分程度)

  実験時の画面は周りに見えないようにし，静かな状態で行った

実験結果1（平均正解度・脅威度）

- 正解度(Accuracy) は

$$\frac{\text{○の人数} + \text{△の人数} \times 0.5}{\text{被験者数}} \times 100$$

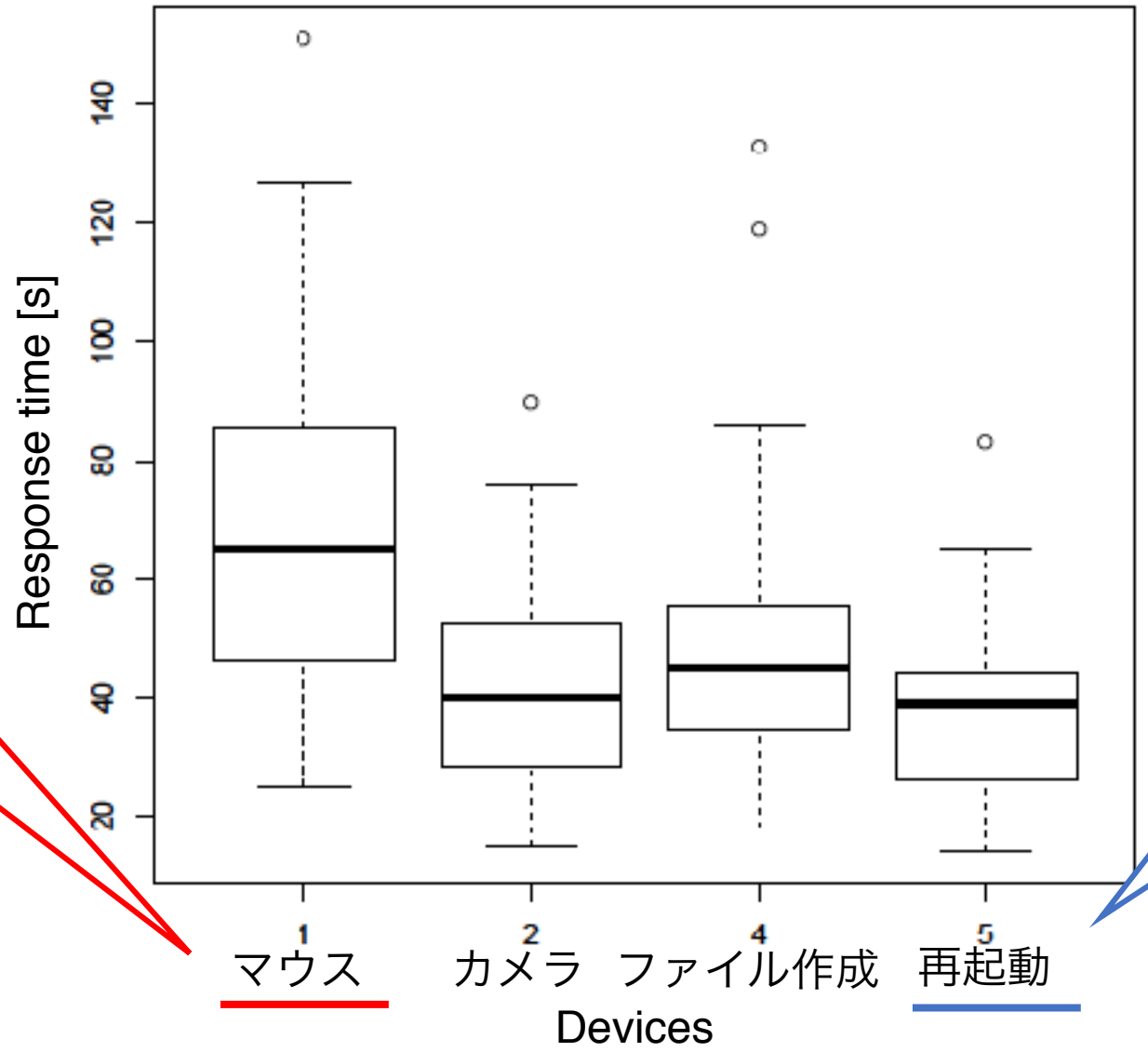
と定義する

- ○は完全正解，△は一部正解とする

マウス　　カメラ　ファイル作成　再起動

	(1)	(2)	(4)	(5)	平均
平均正解度	66.1	71.0	51.6	100	72.2
平均脅威度	2.2	4.5	3.4	3.3	3.3

実験結果2（回答時間）



カーソルの移動方向や時間もランダムなため，目立たない

画面の変化が最も大きい

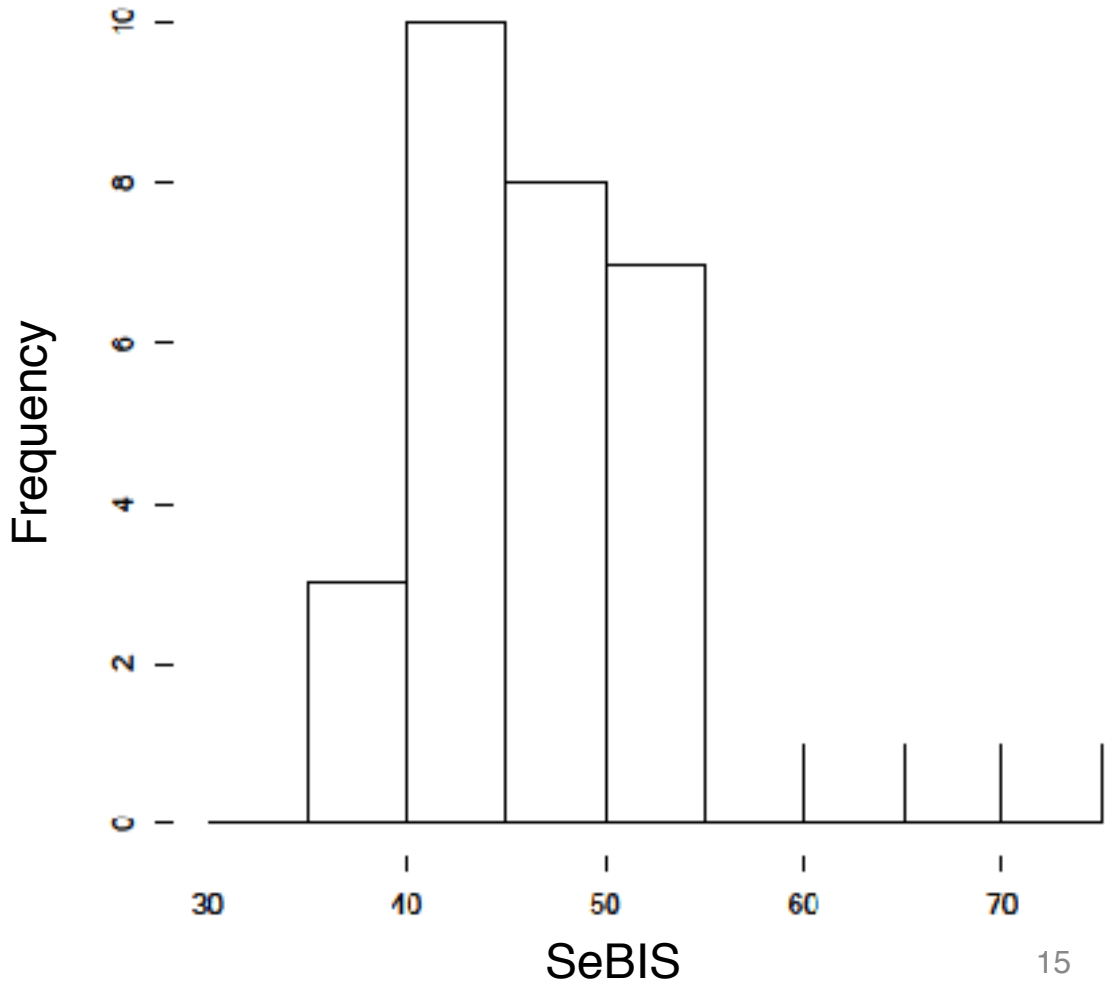
実験結果3（IT指向度・SeBIS）

IT指向度平均：1.5

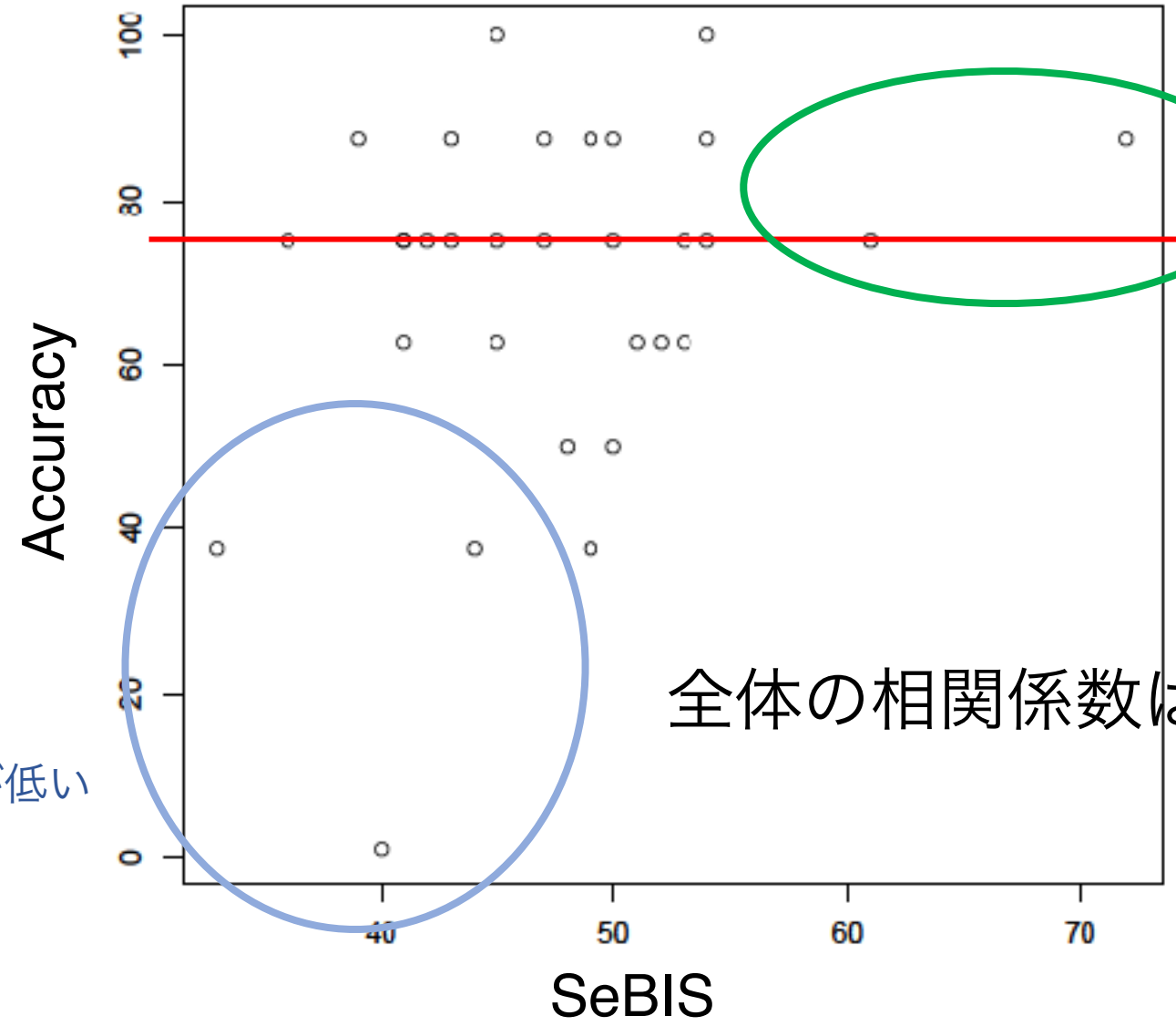
SeBIS平均得点：47点

IT 指向度	0	1	2	3
人数	4	12	10	5

相関係数は0.3



正解度とSeBISの関連性



セキュリティ意識が高い

正解度 75

全体の相関係数は0.2

セキュリティ意識が低い

正解度とSeBISの確率検定

S…各被験者ごとのSeBIS

A…各被験者ごとの平均正解度

T…各被験者ごとの脅威度平均

μ()はそれぞれの被験者全体での平均

有意水準は0.05

	正解度			脅威度		
	$A < \mu(A)$	$A \geq \mu(A)$	p 値	$T < \mu(T)$	$T \geq \mu(T)$	p 値
$S < \mu(S)$	4	10	0.6	8	6	0.9
$S \geq \mu(S)$	6	11	＞ 0.05	7	10	＞ 0.05

結論

- BadUSBを用いた評価実験を行った
  - 再起動を行うものが最も検知率が高かった(ファイル作成の2倍)
  - カメラで撮影するものが最も脅威度平均が高かった(マウスの2倍)
- セキュリティ指向度とBadUSBへの認知には，統計的な相関はなかった
- セキュリティ指向度だけでなくPCに関するより専門的な知識が必要？（ファームウェアに関する知識等）

  ー企業ではThin clientを導入し対策を行っているところもある