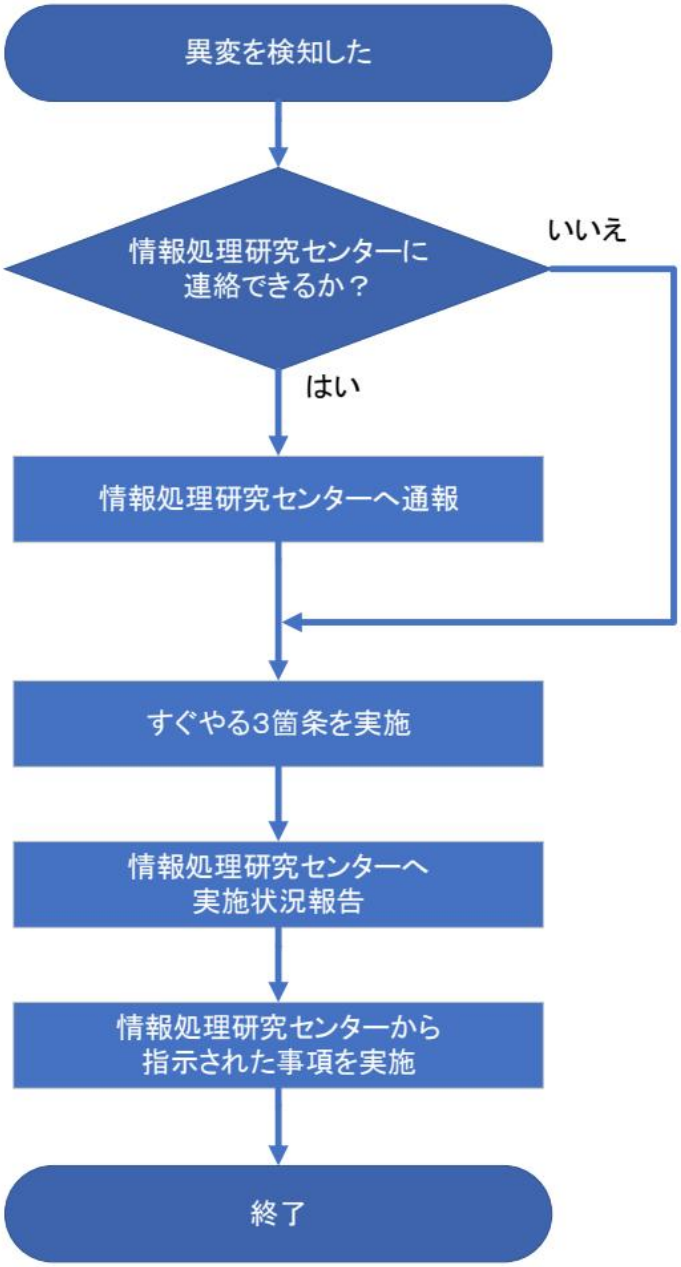
Onomichi City University
尾道市立大学

情報セキュリティインシデント発生時の対応フロー

- 情報セキュリティインシデントとは、情報セキュリティ上の望ましくない事象全般を指し、マルウェア（ウイルス）感染、不正アクセス、情報漏えい、システム障害、ヒューマンエラー、自然災害などが含まれます。
- 情報セキュリティインシデント発生時（もしくは発生の恐れがある場合）には、以下の対応フローのとおり実施してください。



- すぐやる 3 箇条とは・・・（次ページで解説）

Onomichi City University
尾道市立大学

- 重要： すぐやる 3 箇条
  1）危ない兆候や怪しいものはすべて情報処理研究センターに報告
  2）ネットワーク切断（LAN ケーブルを抜く、Wi-Fi をオフにする）
  3）シャットダウンしない（ネットワーク切断ができない場合は、物理電源ボタン 1 度押しスリープを実施）（復帰しないように監視）

- **＜2）の解説＞**ネットワークを切断する練習をしてください。「Wi-Fi をオフにする」について、マウス画面操作が封じられることがありますのでキーボード操作により Wi-Fi をオフにする方法を事前に確認・練習して緊急時に備えてください。（キーボードに飛行機や電波のマークの刻印ありますので、fn キーと組み合わせて押すとオフラインになります。）
- **＜3）の解説＞**「シャットダウンしない」は、「２） ネットワーク切断」ができた場合に「シャットダウンしない」となります。「２） ネットワーク切断」ができなかった場合には、学内で被害が広がったり学外へ情報が漏れ続けたりする可能性がありますので、物理電源ボタン 1 度押しスリープを実施、スリープできないようなら物理電源ボタン長押し強制シャットダウンを実施）