バーチャルマシン内の盗聴プログラムの安全な検知

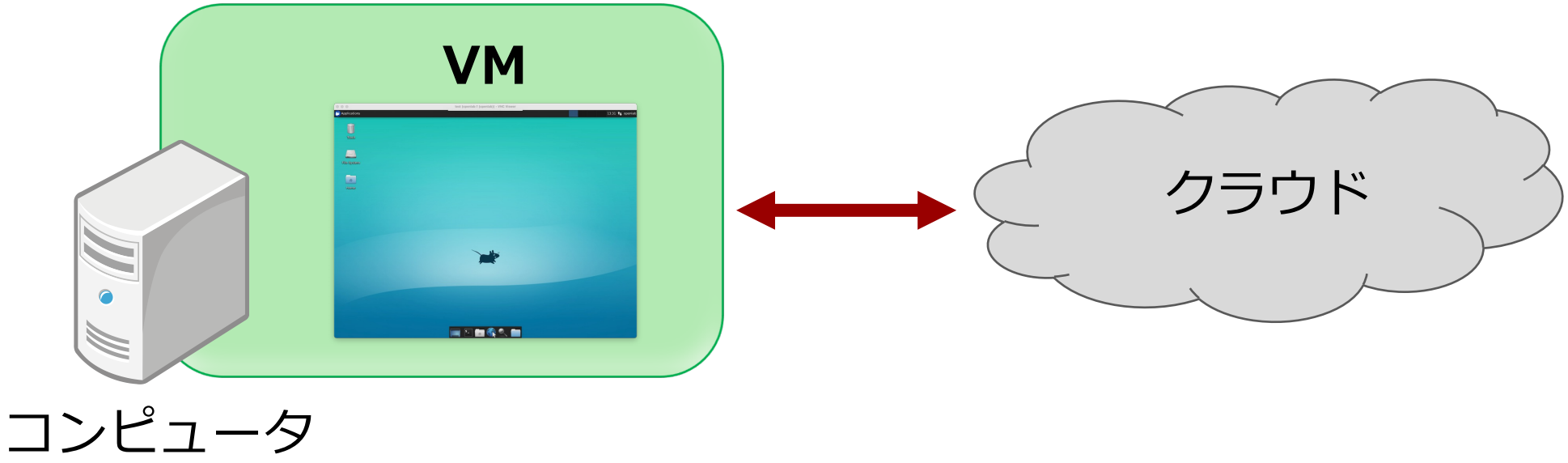
九州工業大学 情報工学部
情報・通信工学科
光来研究室

研究の目標

- バーチャルマシンを使って安全安心な情報システムを作る
  - **セキュリティ**の高いシステム
  - 信頼性の高いシステム
  - 従来の制限をとりはらったシステム

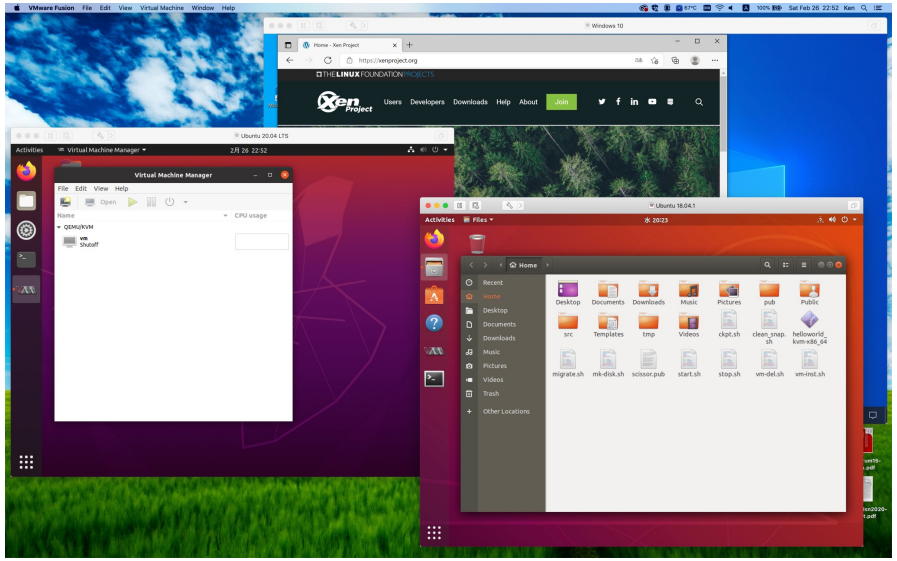
バーチャルマシン (VM) とは？

- コンピュータの中に作り出される**仮想的な**コンピュータ
  - ソフトウェア（プログラム）で作られている
- 近年の情報システムの多くで使われている
  - 例：クラウドコンピューティング



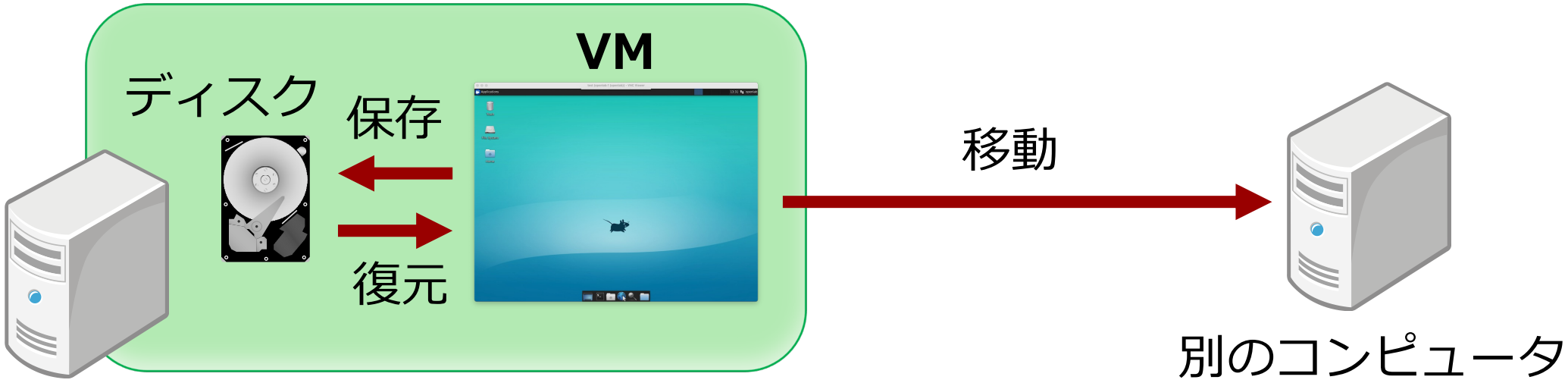
バーチャルマシンの特徴 (1)

- 必要な時に**すぐに**作ることができる
  - パソコンのように買ってくる必要がない
- １台のコンピュータの中で**多くの**VMを動かせる
  - コンピュータの余っている能力を最大限に活かせる



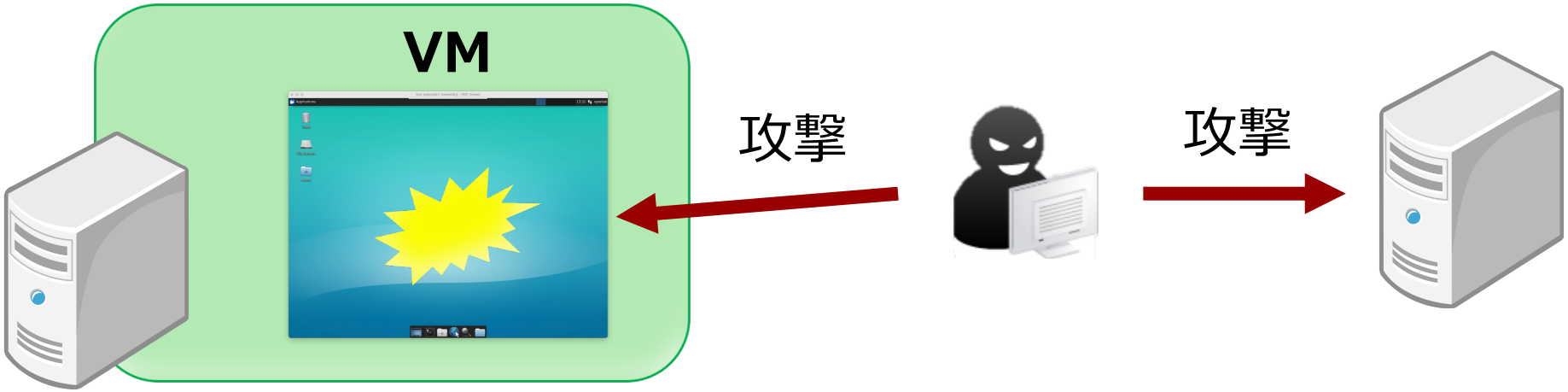
バーチャルマシンの特徴 (2)

- 簡単にVM**丸ごと**のバックアップを取れる
  - 必要に応じてその時の状態に**瞬時に**戻すことができる
- 通信ネットワークを使ってデータとして転送できる
  - 別のコンピュータに**瞬間的に**移動させることができる



バーチャルマシンへの攻撃

- 通常とコンピュータと同じく攻撃を受ける恐れがある
  - VMは通常のコンピュータそっくりに作られているため
  - 同じOS（Windowsなど）、同じアプリが動作する
- 動いているソフトウェアの不具合を狙われる



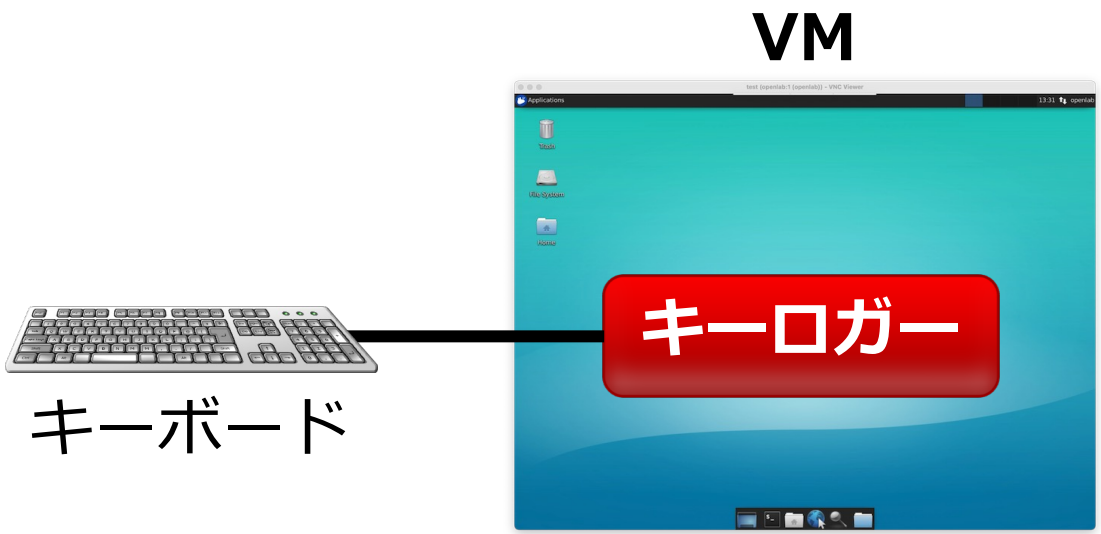
攻撃例

- VM内に侵入され、不正アクセスを行われる
  - 個人情報の盗聴、データの改ざん・削除
- VMを遠隔操作され、他のVMへの攻撃に使われる
  - 不正アクセスの中継点として悪用

事例紹介：キーロガー検知システム

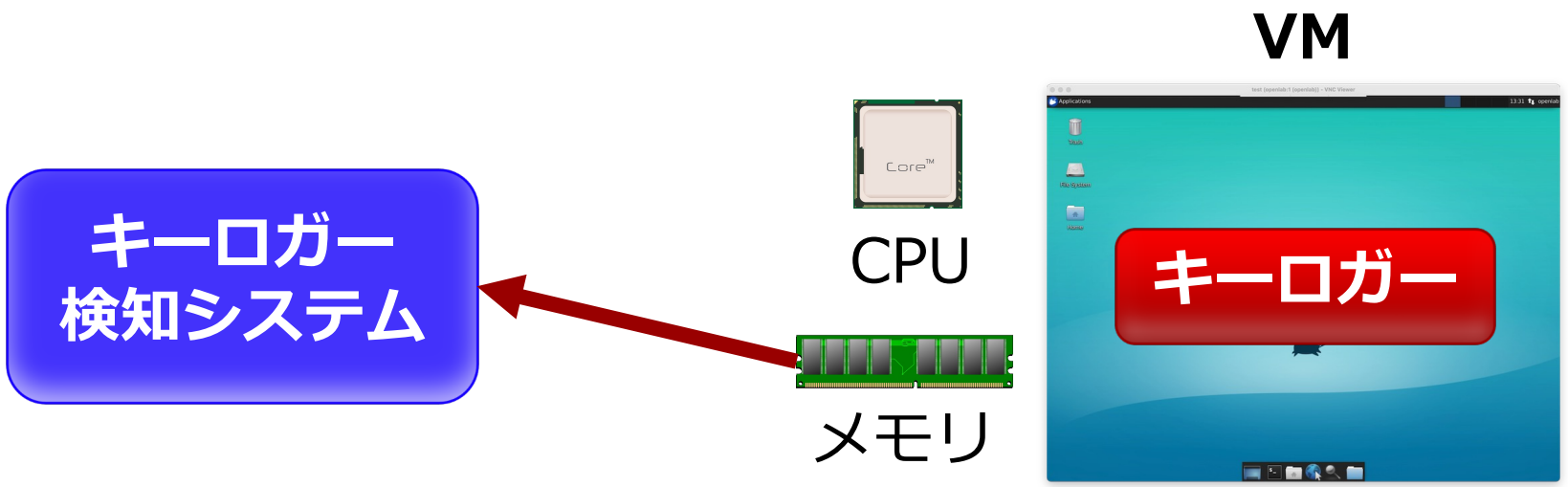
- VM内に仕掛けられたキーロガーを**安全に**検知
  - アメリカのニューヨーク市立大学と共同で研究
- キーロガーとは？
  - 利用者のキーボード入力を**盗聴**する不正プログラム

ニューヨーク市立大学にて



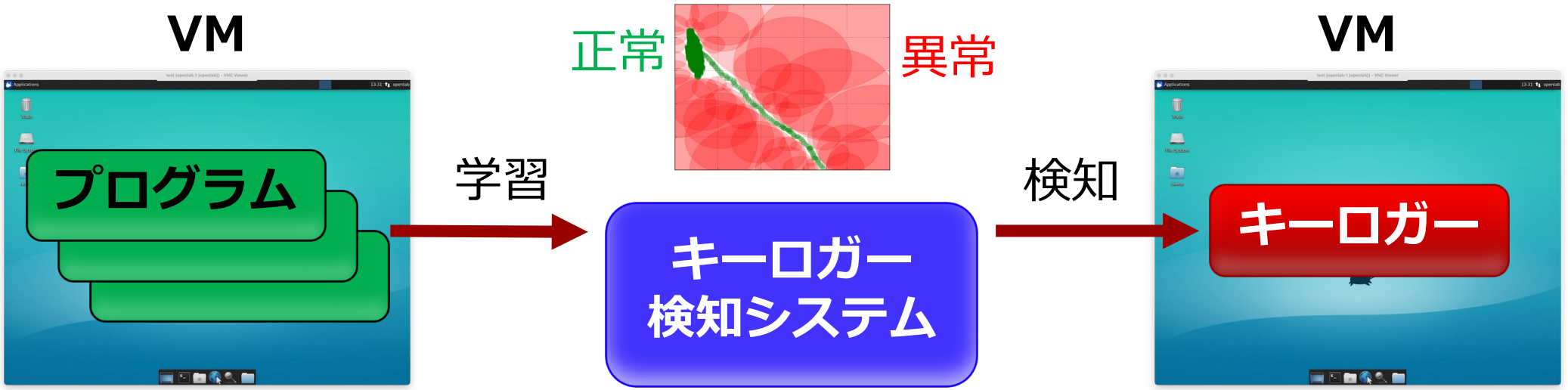
VM内の情報の解析

- キーロガー検知システムを**VMの外部で**安全に動かす
  - VM内の不正プログラムからの攻撃を防ぐ
- VMの**メモリをのぞき見て**VM内部の情報を取得
  - 例：ファイル等を読み書きしたデータ量

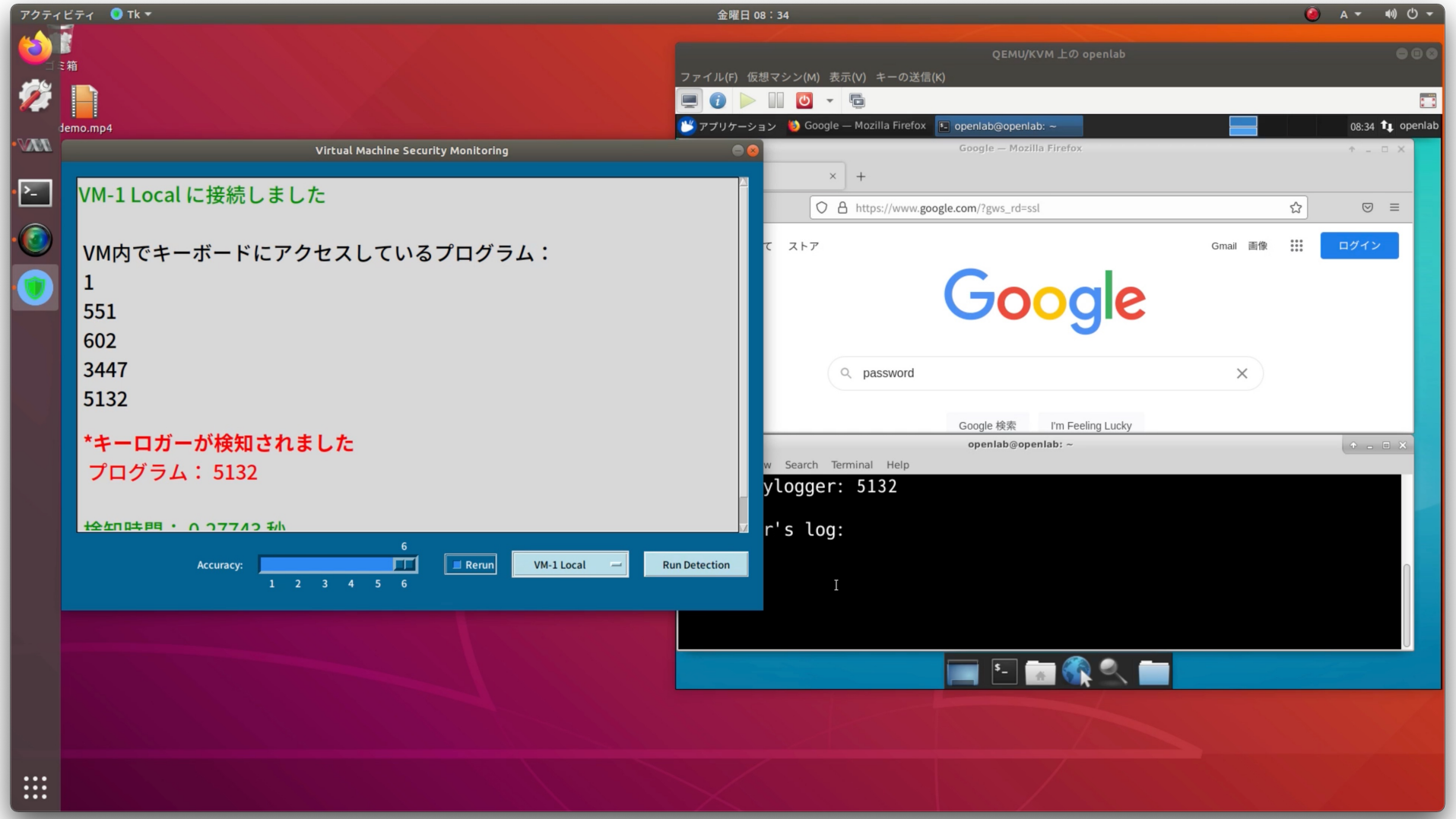


人工免疫システムを用いた検知

- 人間の免疫システムがウイルスを発見する仕組みを応用
  - 自己を**学習**することで非自己を検知
- 事前にVM内のプログラムの**正常な**挙動を学習
  - キーロガーに特有の**異常な**挙動をしているプログラムを発見



デモ


アクティビティ
Tk
金曜日 08：34
demo.mp4
Virtual Machine Security Monitoring
VM-1 Local に接続しました
VM内でキーボードにアクセスしているプログラム：
1
551
602
3447
5132
*キーロガーが検知されました
プログラム： 5132
Accuracy:
Rerun
VM-1 Local
Run Detection
QEMU/KVM 上の openlab
ファイル(F) 仮想マシン(M) 表示(V) キーの送信(K)
アプリケーション
Google — Mozilla Firefox
openlab@openlab: ~
08:34
openlab
https://www.google.com/?gws_rd=ssl
Gmail
画像
ログイン
Google
password
Google 検索
I'm Feeling Lucky
Search
Terminal
Help
ylogger: 5132
r's log: