



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

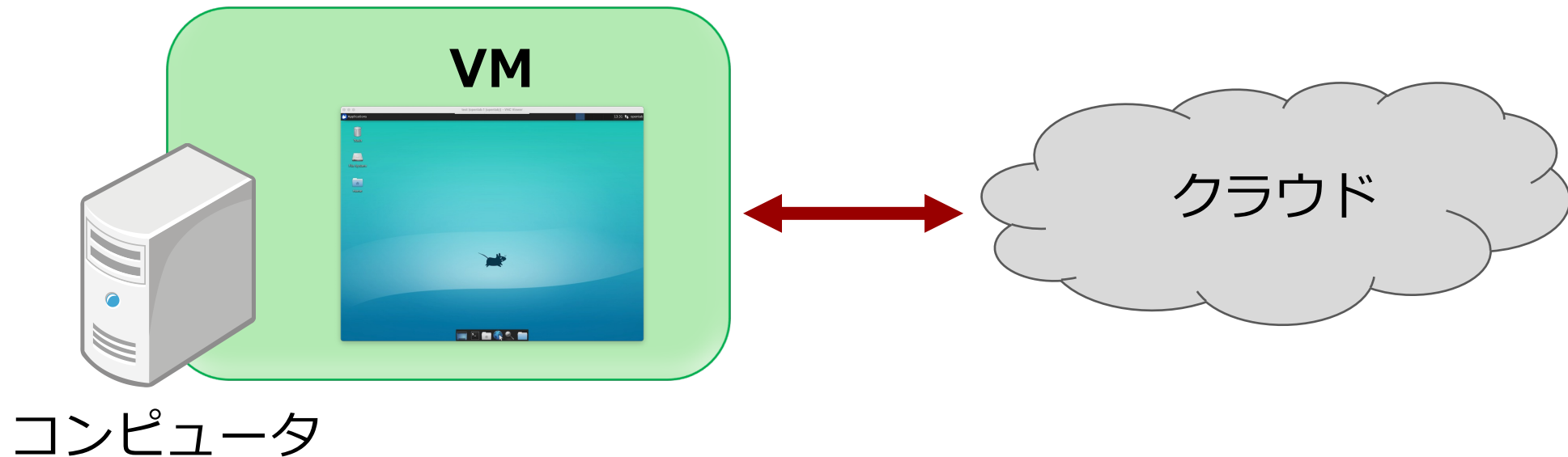
研究の目標

- 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



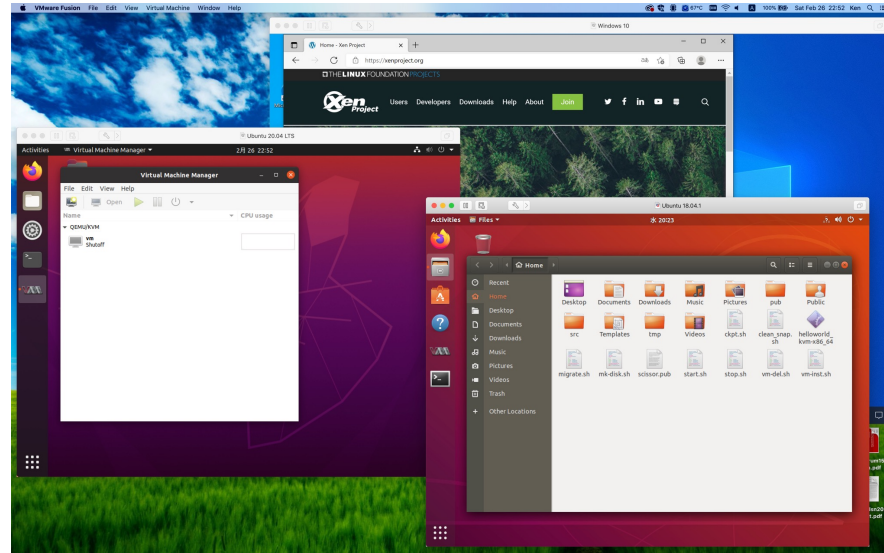
バーチャルマシン (VM) とは？

- 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



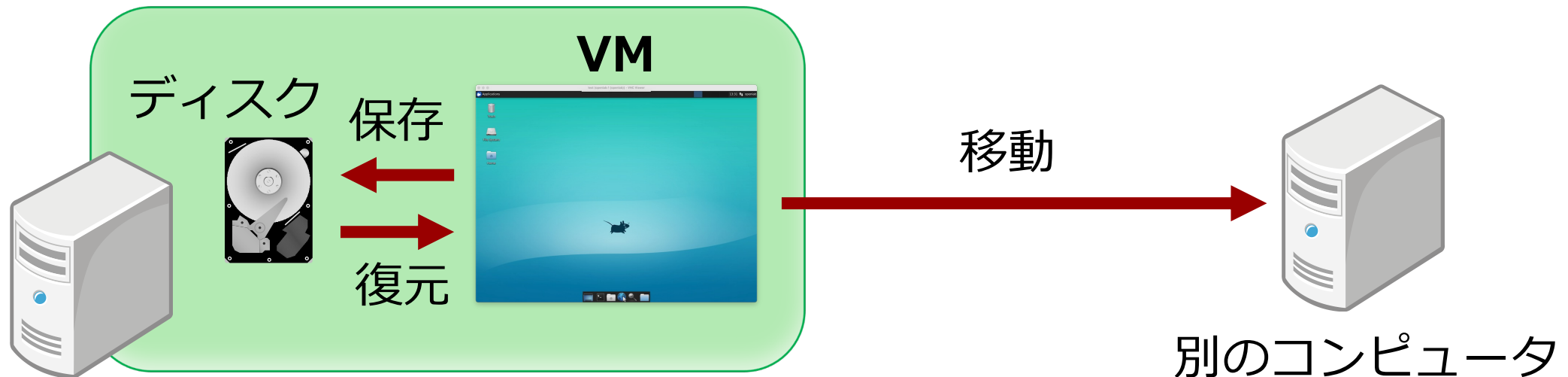
バーチャルマシンの特徴 (1)

- 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



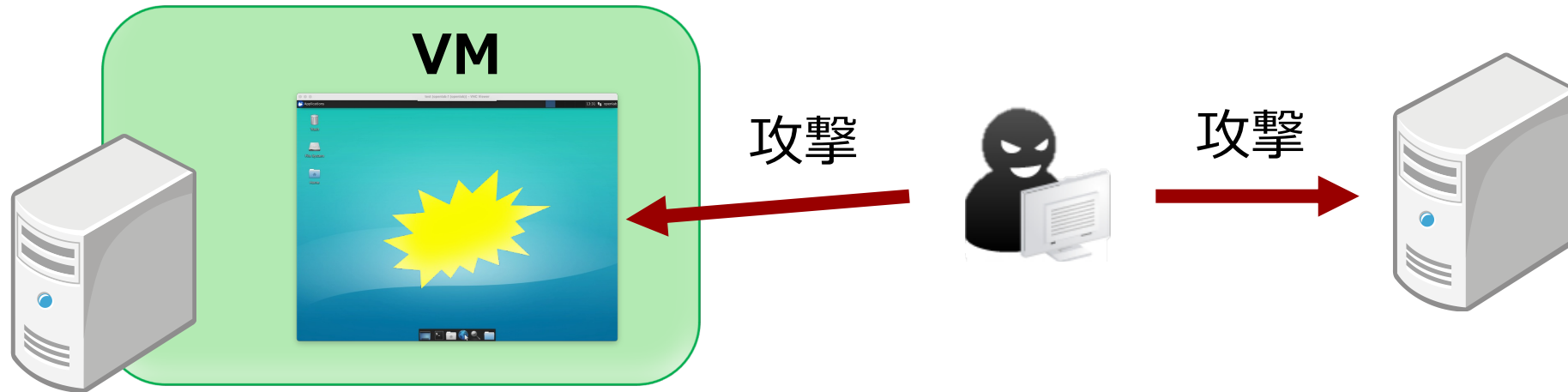
バーチャルマシンの特徴 (2)

- 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**戻ることができる
- 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

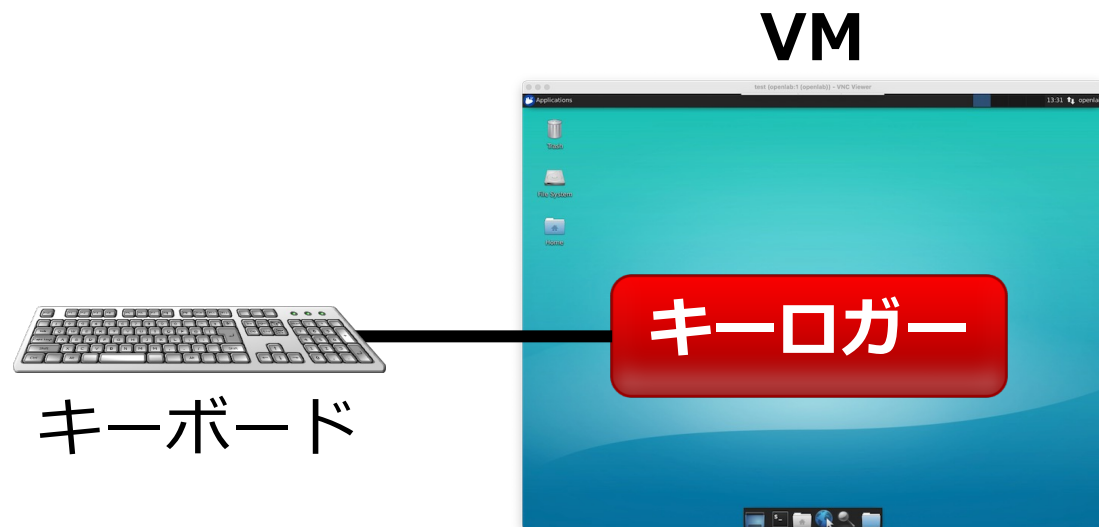


事例紹介：キーロガー検知システム

- 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

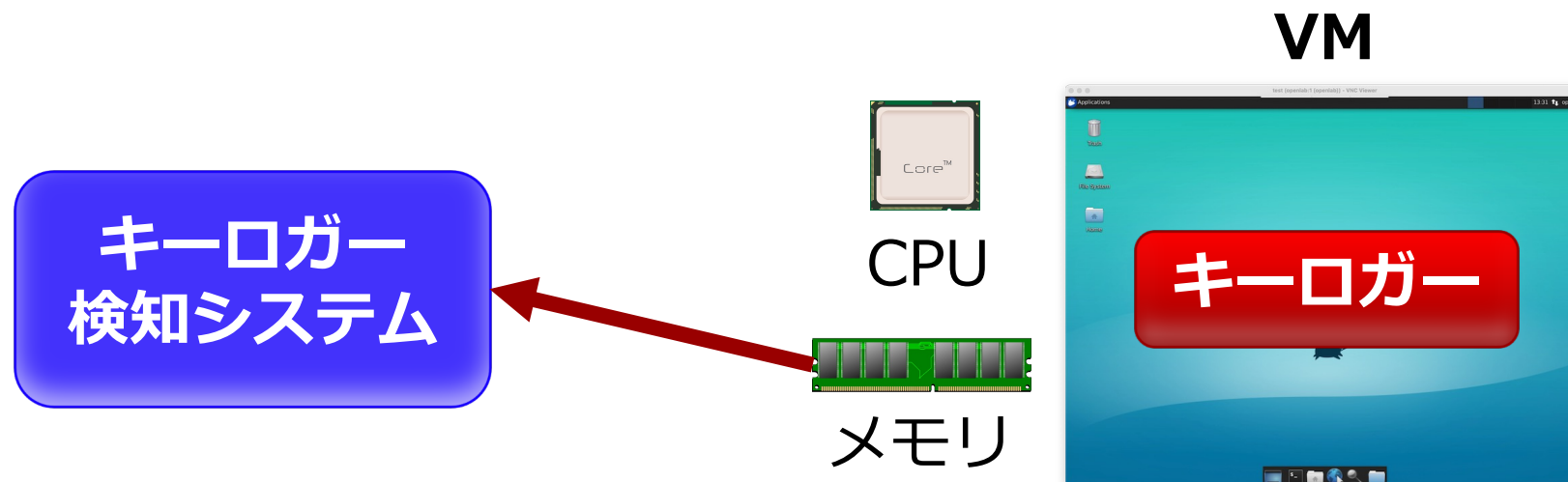


ニューヨーク市立大学にて



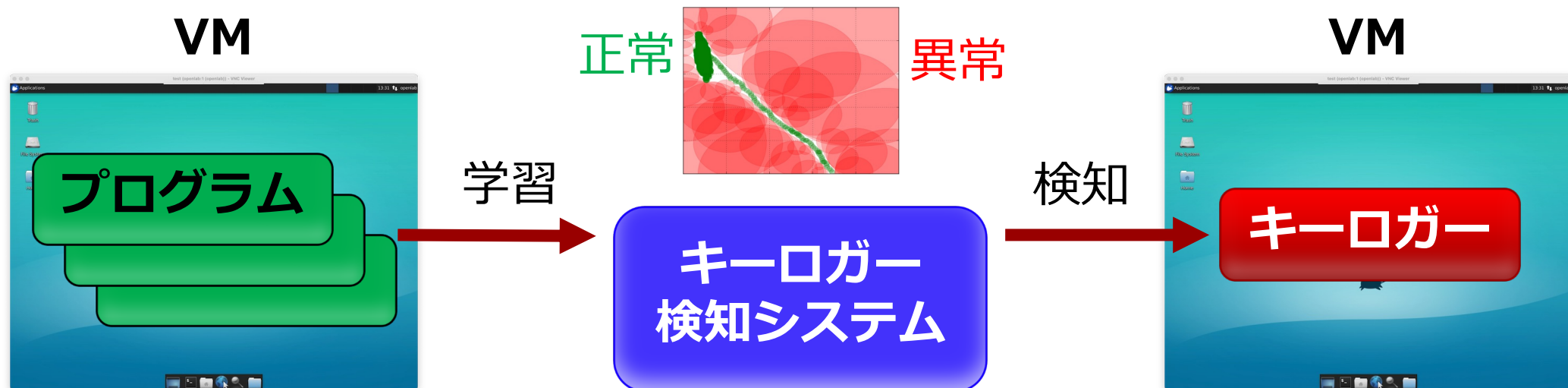
VM内の情報の解析

- 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

The screenshot displays a virtual machine environment with a security monitoring tool. The tool's main window, titled "Virtual Machine Security Monitoring", shows a notification: "VM-1 Local に接続しました" (Connected to VM-1 Local). Below this, it lists programs accessing the keyboard: "VM内でキーボードにアクセスしているプログラム:" followed by a list: "1", "551", "602", "3447", and "5132". A red alert message states: "*キーロガーが検知されました" (Keylogger detected) and "プログラム: 5132" (Program: 5132). The detection time is noted as "検知時間: 0.27712 秒". At the bottom, there is an "Accuracy" bar (0-6), a "Rerun" button, a "VM-1 Local" dropdown, and a "Run Detection" button.

In the background, a Mozilla Firefox browser window shows the Google homepage with the search bar containing the text "password". Below the browser, a terminal window displays the command "ylogger: 5132" and the output "r's log:". The desktop environment includes a taskbar with icons for applications, a terminal, and a file manager. The system tray shows the date and time as "金曜日 08:34".