卒業論文に向けて(3)

学部4年生
島本 大輔
2004年11月11日

概要

- 進捗
- API hooking
- 今後の予定

進捗

- Windows版IDS or Sandbox
- **調査内容**
  - API hooking **について調査**
  - PE File **についても調査**
  - **ウィルスやハッキング手法について調査**

Windows版IDS or Sandbox

- API の Hooking を用いる予定
  - 似た研究あり
- 基本的にNT系列で動作

API hooking

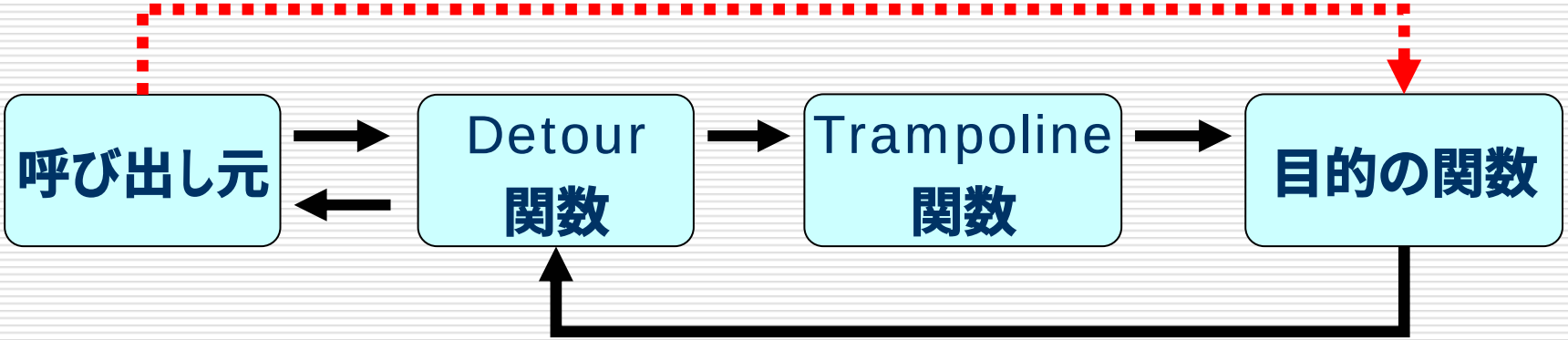
- User-mode
  - Win32 の API を Hooking
    - 演習3の研究内容 (Detours)
- Kernel-mode
  - Native API を Hooking

User-mode Hooking

- Proxy DLL [3]
  - DLL を置き換える
- API Patching [4]
  - API の中身を書き換える
  - Detours
- IAT Patching [4][5]
  - Import Address Table の値を書き換える
  - Detours にもこの機能あり

Detours(API Patching)

- **自分のコード(Detour)を実行後、本当の API を呼び出す**



Detours の適用例

Before

```
;; Target Function
Sleep:
  push  ebp              [1 byte]
  mov   ebp,esp          [2 bytes]
  push  ebx              [1 bytes]
  push  esi              [1 byte]
  push  edi
  ....

;; Trampoline Function
UntimedSleep:
  jmp   Sleep

;; Detour Function
TimedSleep:
  ....
```

After

```
;; Target Function
Sleep:
  jmp   TimedSleep       [5 bytes]
  push  edi    ; Sleep+5
  ....

;; Trampoline Function
UntimedSleep:
  push  ebp
  mov   ebp,esp
  push  ebx
  push  esi
  jmp   Sleep+5

;; Detour Function
TimedSleep:
  ....
  jmp   UntimedSleep
```

Detours

- **利点**
  - **ユーザー定義の** API **を** Hook **できる**
- **欠点**
  - API **内に「**jmp ***関数***」=5 byte **分の容量が必要**
    ⇒ 5 byte **未満の** API **は置き換えられない**
  - Win32 **の** API **は難しい**
    ⇒ DLL **側で可能かもしれない**

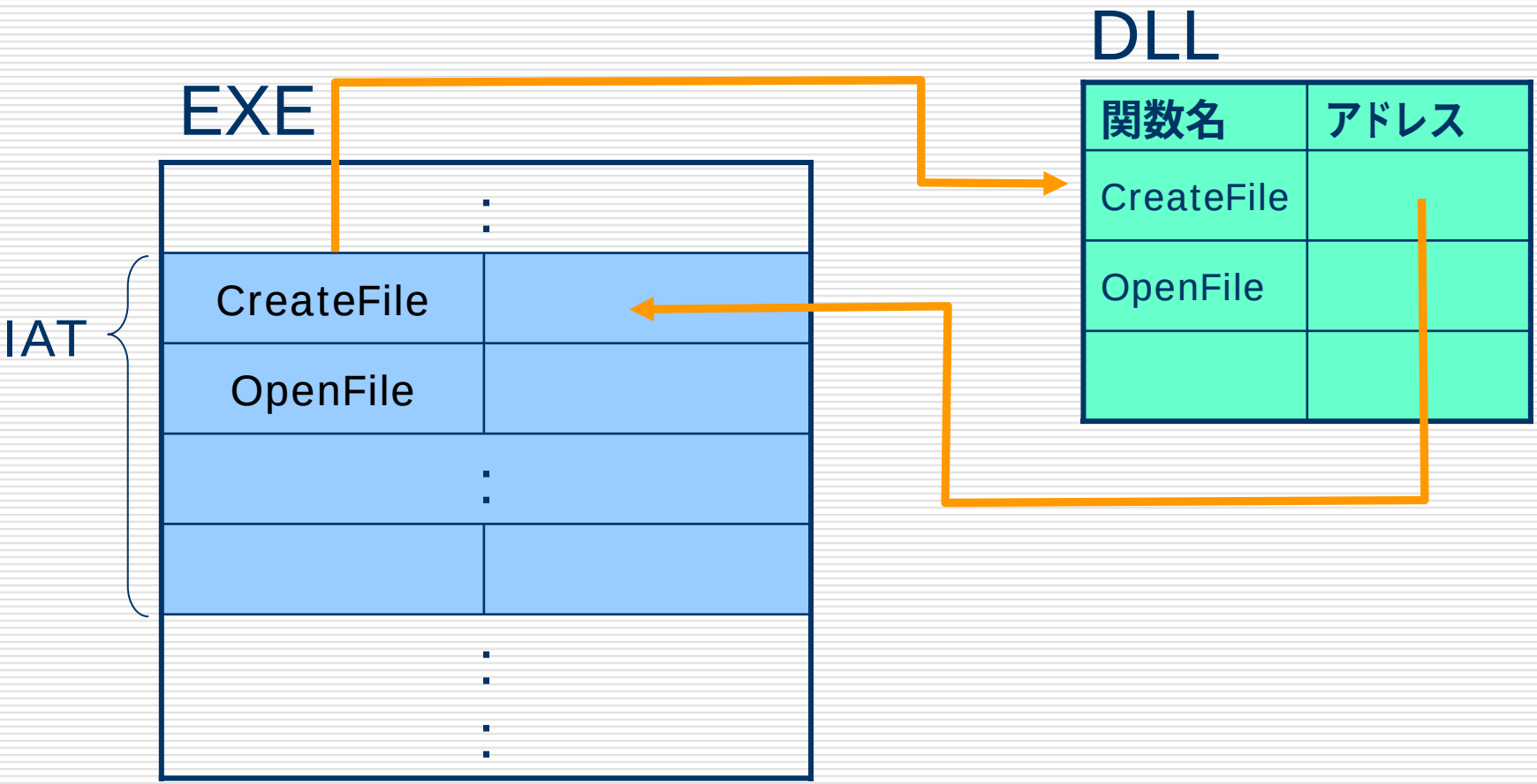
IAT Patching

- Import Address Table **を書き換える**
- Detours **にもこの機能あり**
- **この手法の文献は多い**

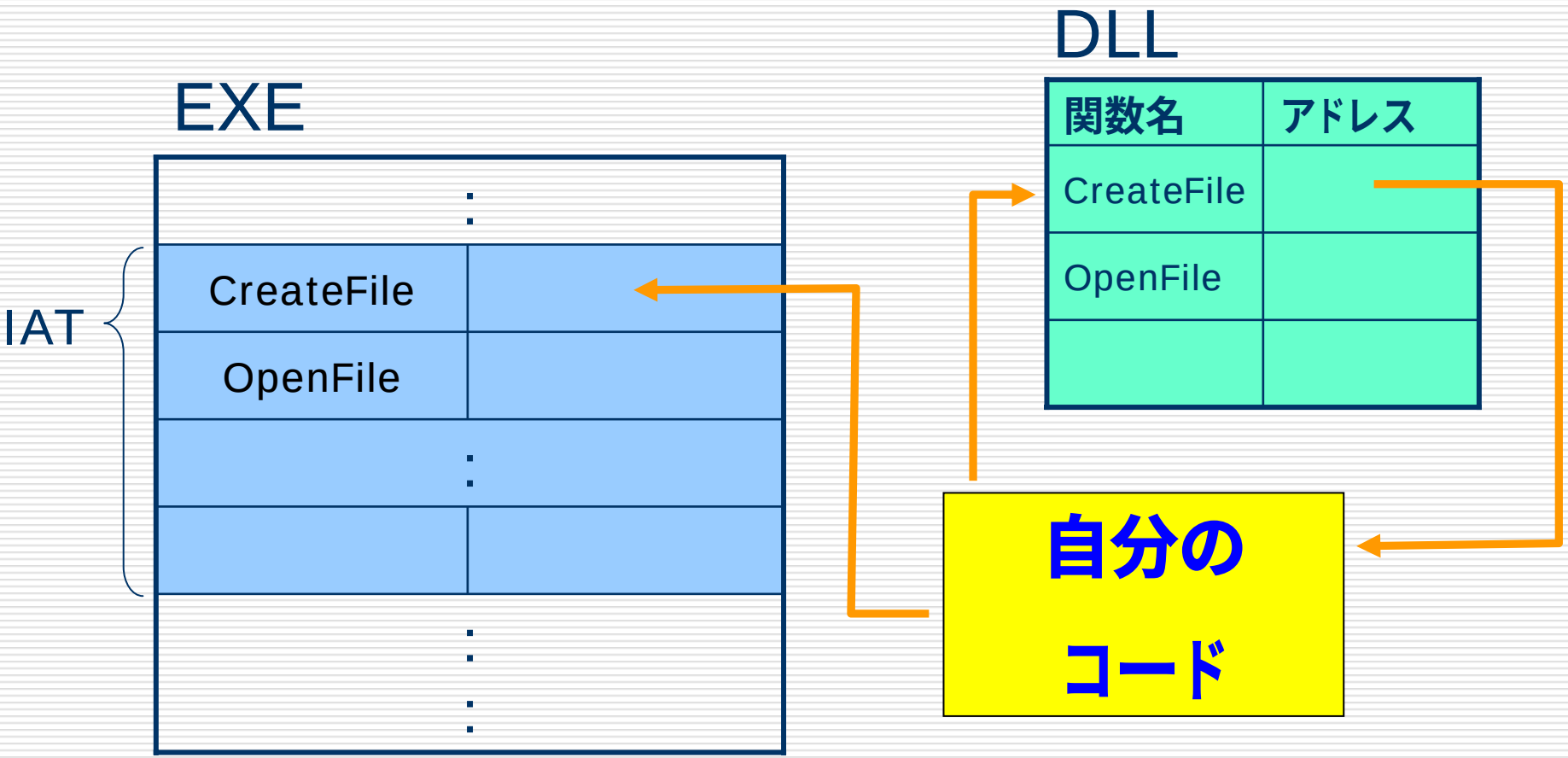
Import Address Table (IAT)

- 外部ライブラリ(主に DLL)で呼び出す関数アドレスのテーブル
  - 当然、一定値ではない
- Windows loader が DLL のアドレスをテーブルに書き込む
- 1つのバイナリに必ず1つある
  - もちろんエントリ数が0もあり(例 ntdll.dll)
- 逆の機能は Export Address Table

Updating IAT



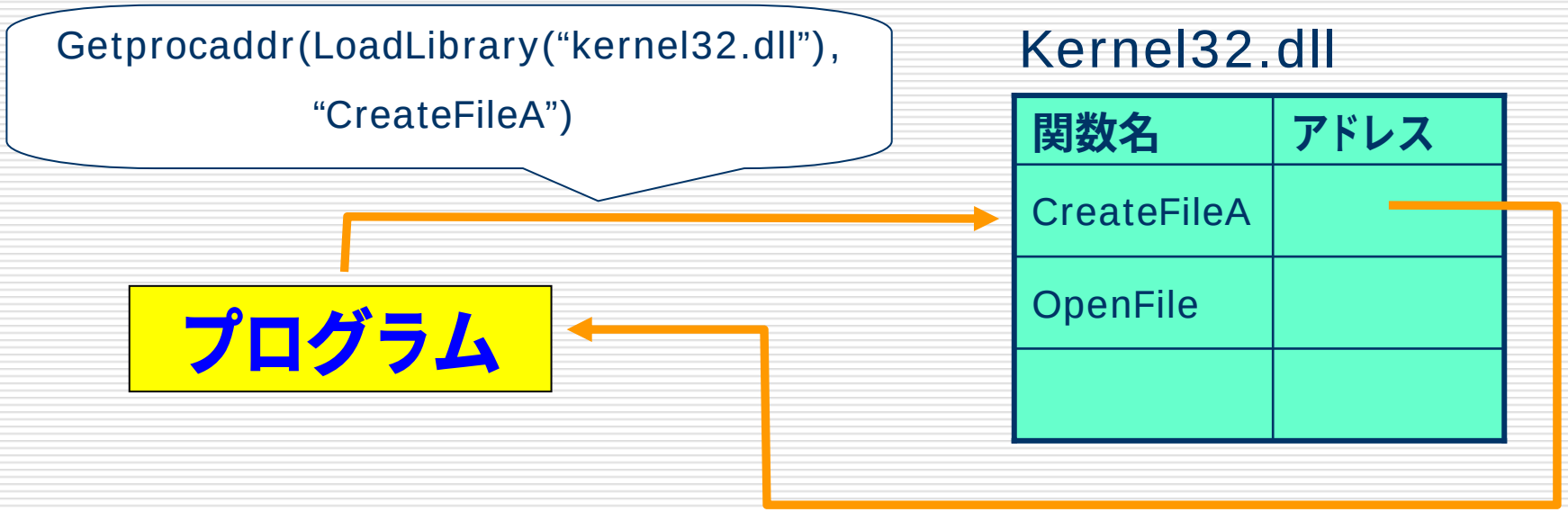
Using IAT for Hooking



IAT Patching

- **回避策がある**
  - Getprocaddress **で動的にライブラリの関数アドレスを引ける**
- **実際、ウィルスとかはそうしている**
  - OS **のバージョンによって、関数アドレスが異なるため**

IAT Patching の回避策

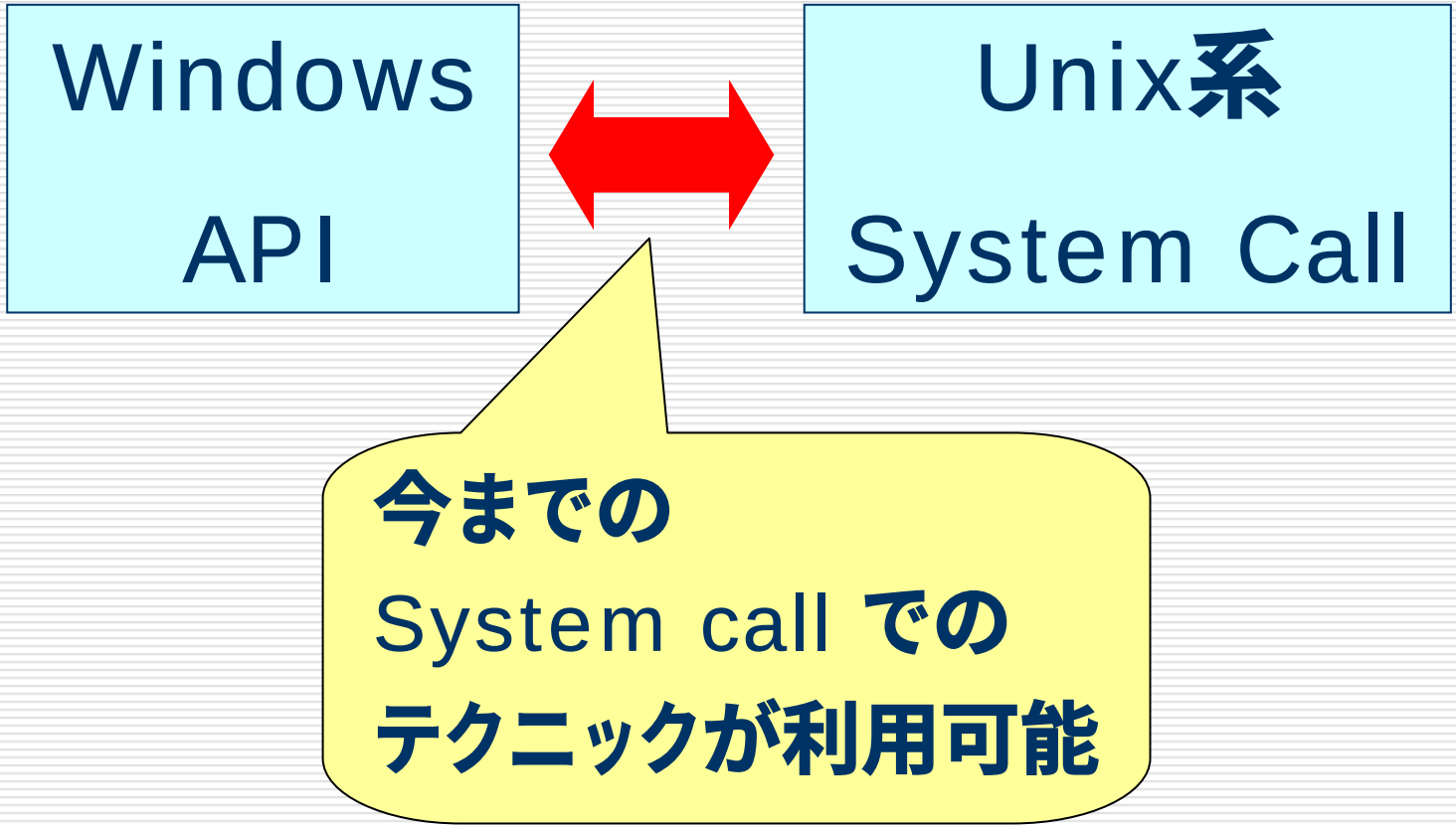


- プログラムの任意の場所で読み込める
- IAT は関係ない

Kernel-mode Hooking

- Windows NT の System service を hooking
  - Kernel-mode で動作する device driver を利用
  - 過去に例あり [6]
- 手法としてはそれほど新しくない
- セキュリティへの応用の論文は少ない (と思われる)
- Rootkit への応用あり……

API & System Call



今後の予定

- Kernel-mode hooking の実装
  - VMWare 上でテスト予定
    （バグのたびに再起動が面倒）
- さらに別の手法をプラスα
  - システムコールを利用した研究の応用
  - Hooking を組み合わせる、など

参考文献(1)

1. An In-Depth Look into the Win32 Portable Executable File Format (Part 1 & 2)
   - http://www.msdn.microsoft.com/msdnmag/issues/02/02/PE/default.aspx
   - http://www.msdn.microsoft.com/msdnmag/issues/02/03/PE2/default.aspx
2. Process-wide API spying
   - http://www.codeproject.com/system/api_spying_hack.asp
3. API Spying Techniques
   - http://www.internals.com/articles/apispy/apispy.htm

参考文献(2)

4. Detours
   - http://research.microsoft.com/sn/detours/
5. Hooking Windows NT System Services
   - http://www.windowsitlibrary.com/Content/356/06/1.html
6. A Host Intrusion Prevention System for Windows Operating Systems
   - Roberto Battistoni, Emanuele Gabrielli, Luigi V. Mancini ESORICS 2004