卒業論文に向けて(4)

学部4年生
島本 大輔
2004年11月24日

概要

- 進捗
- System Service Hooking
- 今後の予定

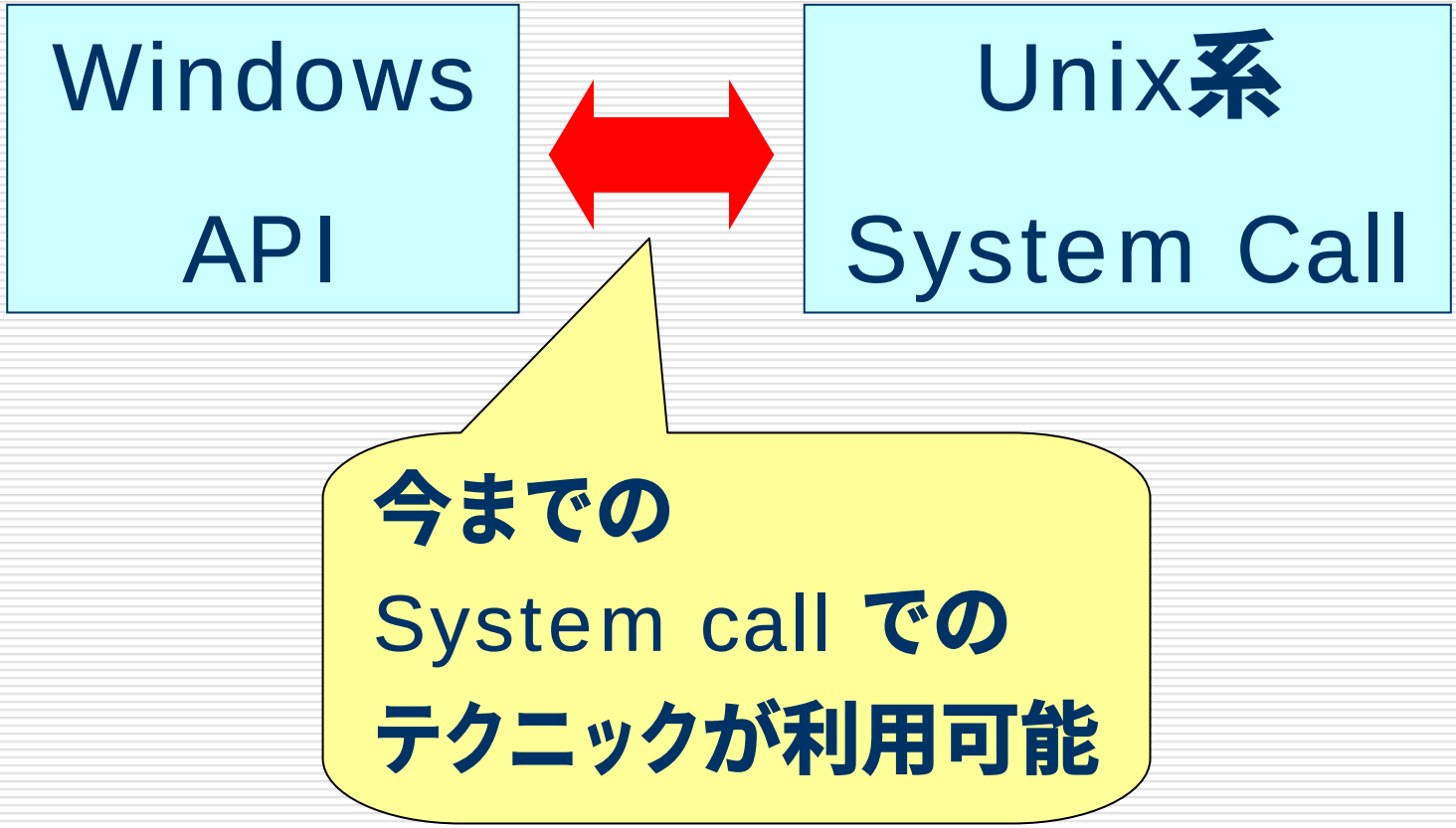
進捗

- Windows版IDS or Sandbox
- **調査内容**
  - API hooking **について調査**
    - **主に** System Service **にたいするもの**
  - Device Driver **の作り方**

Windows版IDS or Sandbox

- System Service を Hooking
- 今のところ、CreateFile のみ
- strace らしきものができれば、UNIX系列の研究を利用できるはず

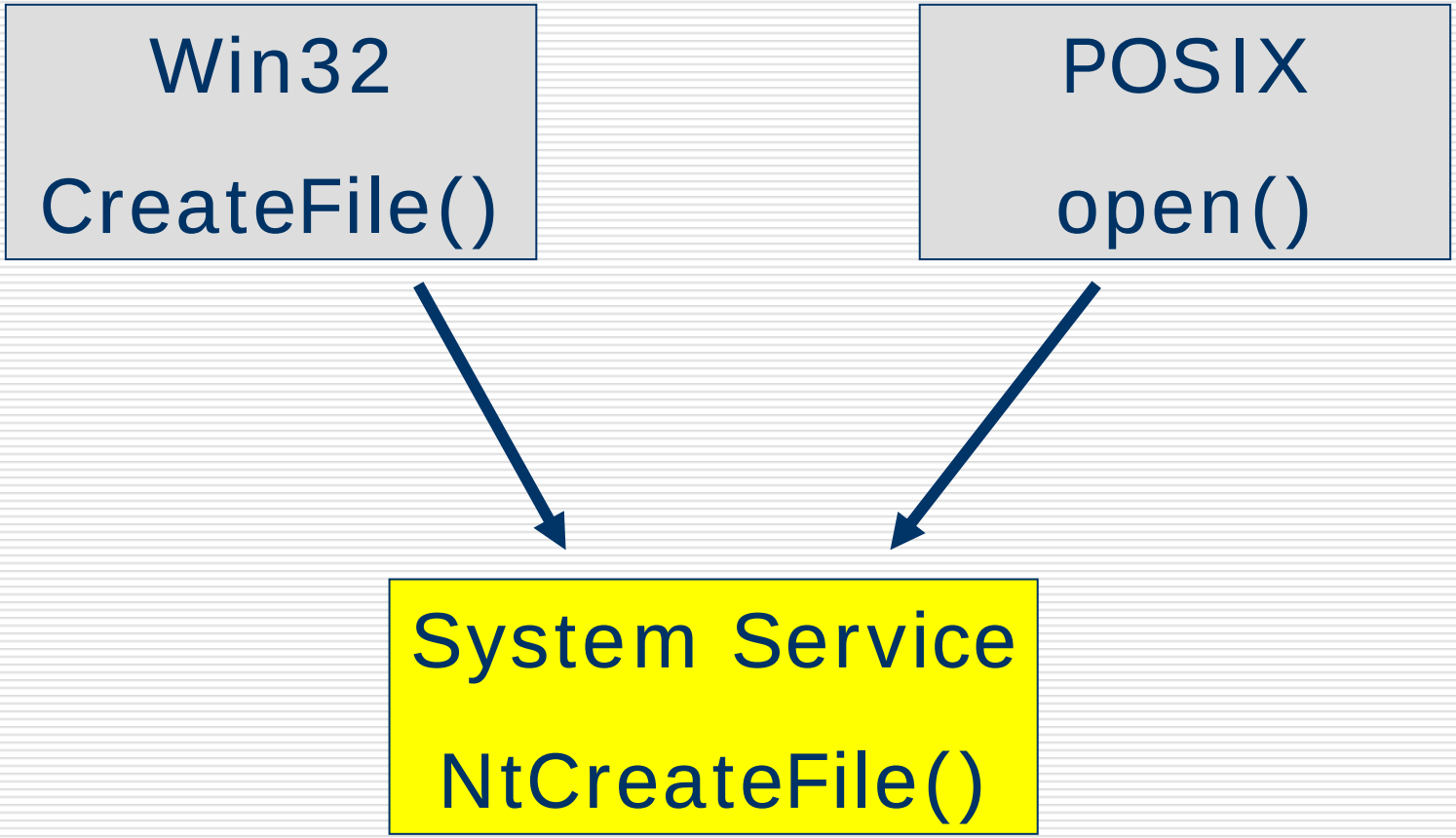
API & System Call



System Service

- Linux の System Call みたいなもの
- NT executive（ntoskrnl.exe の一部）により提供される
- まさしく、Windows の核をなす
  - 例：Win32 CreateFile() と POSIX open() は NTCreateFile() を呼ぶ
- 一部、ドキュメント化されていない！

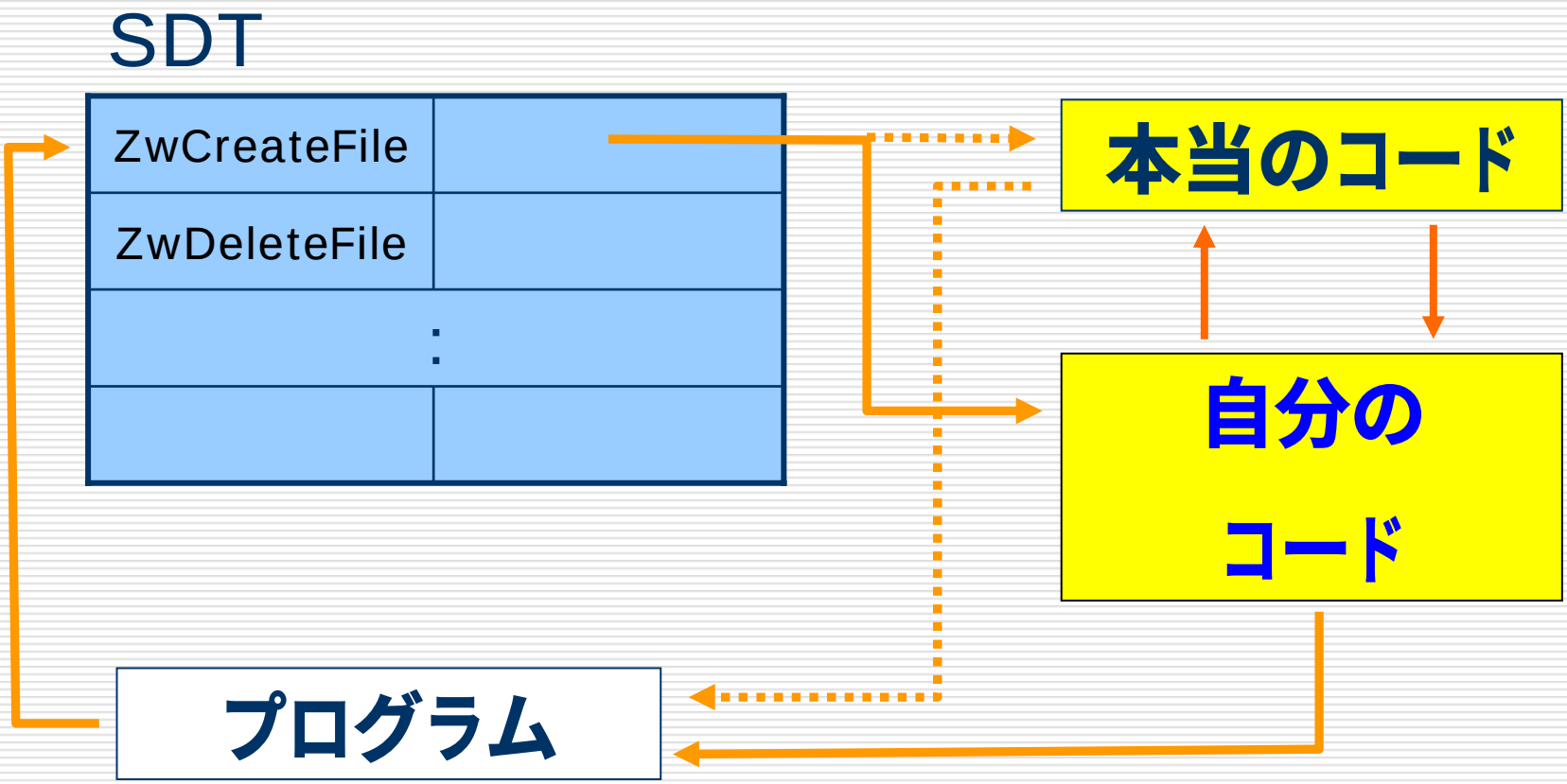
System Service



System Service Hooking

- System Service **はリスト**(System Service Descriptor Table(SSDT))**で管理**
- SSDT **は** Service **へのポインタを持つ**
- **このリストの値を変えれば良い**
  ⇒ 自分の関数に書き換える
- **当然、**Kernel mode**で動作**
  ⇒ Device Driver **として組み込む**

System Service Hooking



問題点

- 先に hooking されている可能性
- OS のバージョンにより、ntokrnl.exe が微妙に異なる
  ⇒ 各OSに対応させるのが面倒
- 有効性が未知数
  - 特定の動作を検出したい場合には有効だが……

Implementation

- **出力**
  - **今は** DbgPrint **で出力**
    ⇒ DebugView **で確認**
  - **将来的にはファイル出力**
- **実演**

関連研究

- System Service Hooking は Rootkit とかに多く使われている [1, 4, 5]
  - 主にプロセス等のリソースを隠すため
- この hooking を検出するツールもある [4]

今後の予定

- Kernel-mode hooking の実装を続ける
  - API を増やす
  - 出力方法の改良
- 回避策がないか、さらに詳しく調査
- UNIX系の System call の技術の調査

参考文献

1. Greg Hoglund and Gray McGraw (2004)
   ”EXPLOITING SOFTWARE”, Addison-Wesley
2. Art Baker and Jerry Lozano (2001)
   “The Windows 2000 Device Driver Book：A Guide For Programmers”, Prentice Hall PTR
3. Undocumented Windows NT
   http://www.windowsitlibrary.com/Documents/Book.cfm?DocumentID=356
4. Rootkit.com
   http://www.rootkit.com/
5. Phrack.org
   http://www.phrack.org/