卒業論文　2019 年度（平成 30 年度）

卒論

慶應義塾大学 環境情報学部

石川 達敬

徳田・村井・楠本・中村・高汐・バンミーター・植原・三次・中澤・武田
合同研究プロジェクト

2020 年 1 月

卒業論文　2019 年度（平成 30 年度）

卒論

論文要旨

アブスト

キーワード

OS

慶應義塾大学 環境情報学部

石川 達敬

Abstract Of Bachelor's Thesis　Academic Year 2019

Title

Summary

abst

Keywords

OS

Bachelor of Arts in Environment and Information Studies
Keio University

Tatsunori Ishikawa

目 次

図 目 次

表 目 次

第1章　序論

1.1　背景

コンピュータの管理者は，動作中のコンピュータの情報を監視することが必要となる場面がある．例えば top コマンドや ps コマンドを用いて，プロセスの一覧を得たり，gdb コマンドを用いてプロセスをトレースし，プロセスの状態を把握する．

その他にも，様々な手段を用いてログイン中のそのコンピュータ自身の状態を監視・解析する．

1.2　着目する課題

コンピュータの状態は，コンピュータ内部におけるレジスタの値および，内部から参照できる仮想アドレス空間上に保持されている．

例えばコンテキストスイッチでは，task$_s$*truct* 構造体から辿れる退避されたメンバから値を取り出すことでプロセス空間および状態の復元を行なっている．

task$_s$*truct* 構造体をはじめとして，*Linux* カーネルの変数や型，関数は，様々なアーキテクチャやカーネルコンフィグに対応するため，マクロによって分岐されている．この分岐が確定するのは，*Linux* カーネルをビルドするときであり，構造体のメンバへのアクセス，関数のアドレスなどはコンパイラが保証している．

実際のカーネルのバイナリは，vmlinux としてコンパイルされた後，strip され bzImage となる．ユーザーが作成したカーネルモジュールなどで関数を呼び出す際は，シンボルとアドレスの変換表である ‘/boot/System.map‘を参照し，実際の

背景で述べた RDMA NIC を用いた解析手法では，メモリの物理アドレスを指定し，逐次的に値を取得し外部から復元していくが，CPU レジスタの現在の値は直接知ることができないため，例えばプロセスの一覧を取得したい場合は，コンテキストスイッチ時に退避された値を辿っていく必要がある．しかし，上述の通り task$_s$*truct* はビルドされた際のカーネルコンフィグによって，どのメンバが先頭アドレスからどのオフセットに保持されているかは変動する．

Linux カーネルのバージョン，System.map の情報および config の情報を知らなければ，メモリのみから正しくコンテキストを復元していくことはできない．

本研究では，上記 3 つの情報のうち，System.map およびビルド時のカーネルコンフィグの値を知ることができないことを問題と定義する．

1.3　目的

以上の背景および課題から，

1.4　アプローチ

アプローチ

1.5　構成

構成