新規ファイルシステムの開発における ＯＳの多段階保護機構の必要性

光来 健一*　　千葉 滋**　　益田 隆司*

* 東京大学大学院 理学系研究科 情報科学専攻

** 筑波大学 電子・情報工学系

拡張しやすいOS

- OSを拡張するためのモジュールをOSに追加できる
  - 拡張可能なOS (SPIN、Exokernel)
- 拡張によって不安定にならない
  - モジュールのバグからOSを守る

保護機構が必要

マイクロカーネルの保護機構

- マイクロカーネルでＯＳの安定性を保つのは比較的容易である
  - 拡張モジュールをユーザプロセスにする
- 保護機構のオーバヘッドが大きく実行効率が悪い
  - システムコールが増える

保護機構 ＶＳ 実行効率

多段階保護機構の提案

- 拡張モジュールの安定度に合わせて段階的に保護の強さを変える
  - 安定していれば実行効率を優先する
  - 不安定ならば保護を優先する
  - 保護の強さが一種類では不十分である
- 各段階で同じインタフェースを提供
  - ソースコードの変更は不要である

なぜ多段階保護機構か？

- ＯＳを拡張するモジュールには完全な保護機構は必要ない
  - 拡張モジュールに悪意はない
  - モジュールのバグからＯＳを守ればよい
- 保護の完全性を緩めた弱い保護を使い、実行効率を優先させたいこともある
  - 安定しているモジュールでは保護を弱くしたい

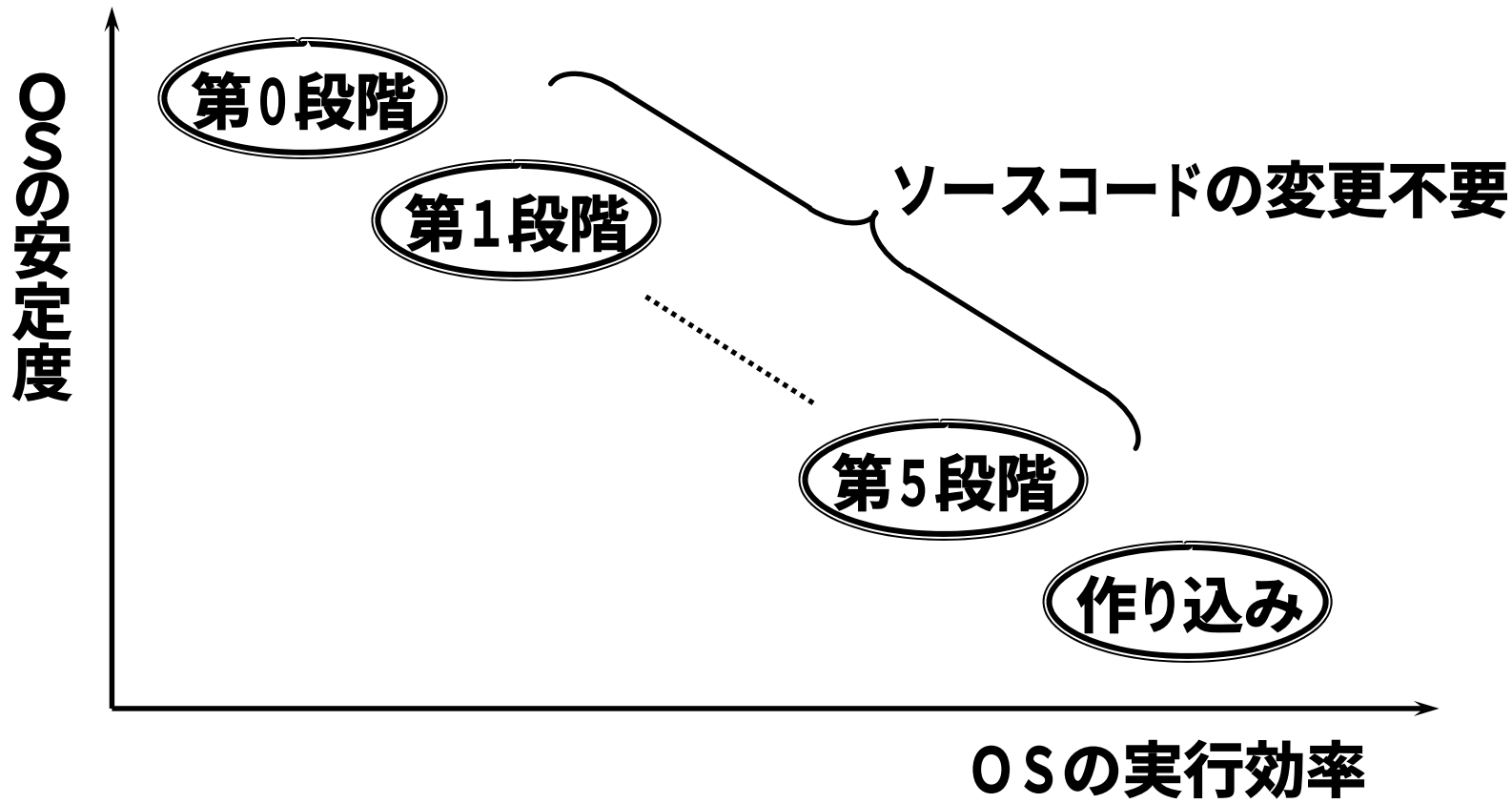
多段階保護機構の設計

- ファイルシステムのための多段階保護機構を設計した
  - 5段階の強さの保護を用意した
  - ソースコードの変更なしで保護の強さを変えられる
  - 保護の強さの変更は再コンパイルまたは再リンクで行なう

ファイルシステムでの応用例

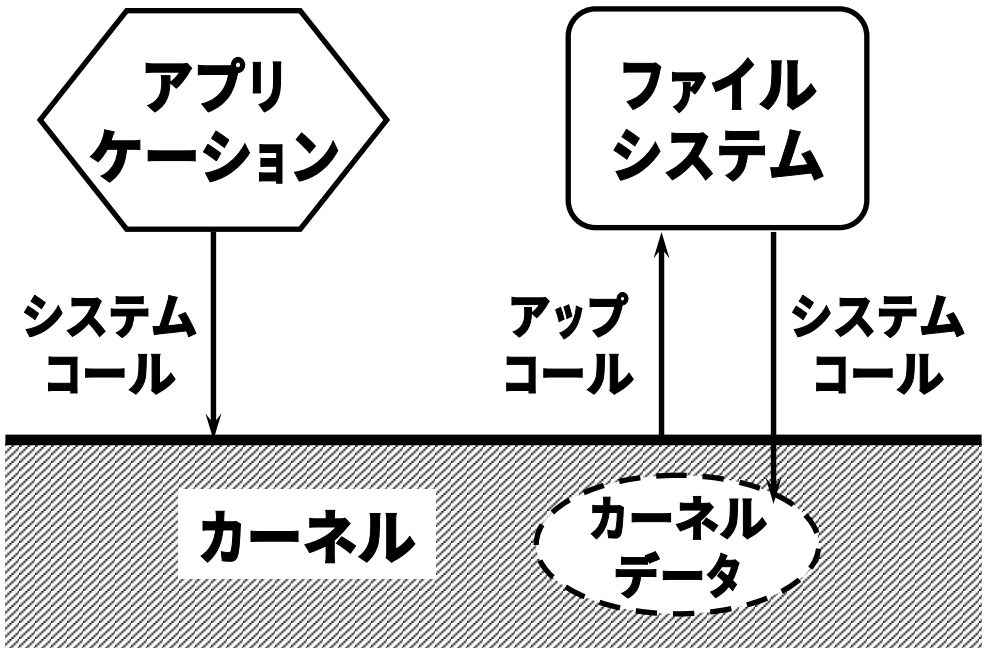
- ファイルシステムの開発の進み具合に応じて保護の強さを変える
  - 開発者が性能のよいファイルシステムを簡単に作ることができる
- 提供された不安定かもしれないファイルシステムを使う
  - ユーザが安全に新しいファイルシステムを使うことができる

各段階の位置づけ



第0段階

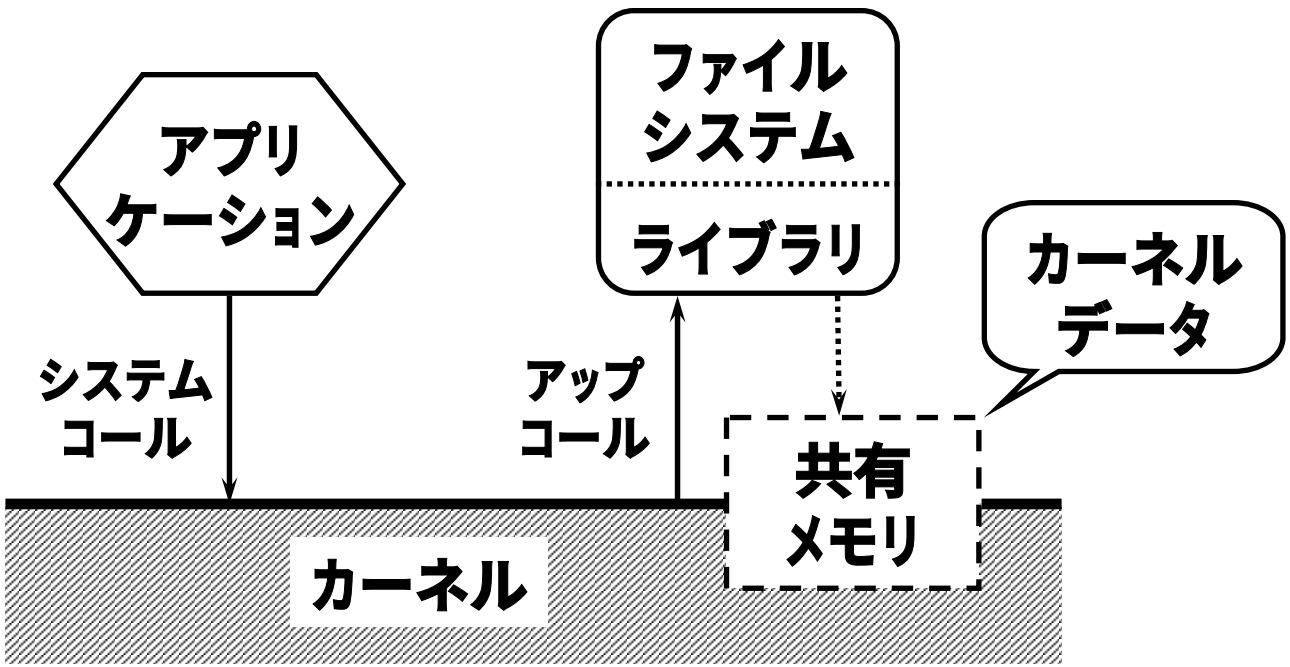
- 実行効率が悪いので実装していない
- 第1段階～第4段階の基本



マイクロカーネル
アーキテクチャと
同等

第1段階（1）

- カーネルデータを共有メモリ上に置く
  - 実行効率が良くなり、ポインタも扱いやすい



第1段階(2)

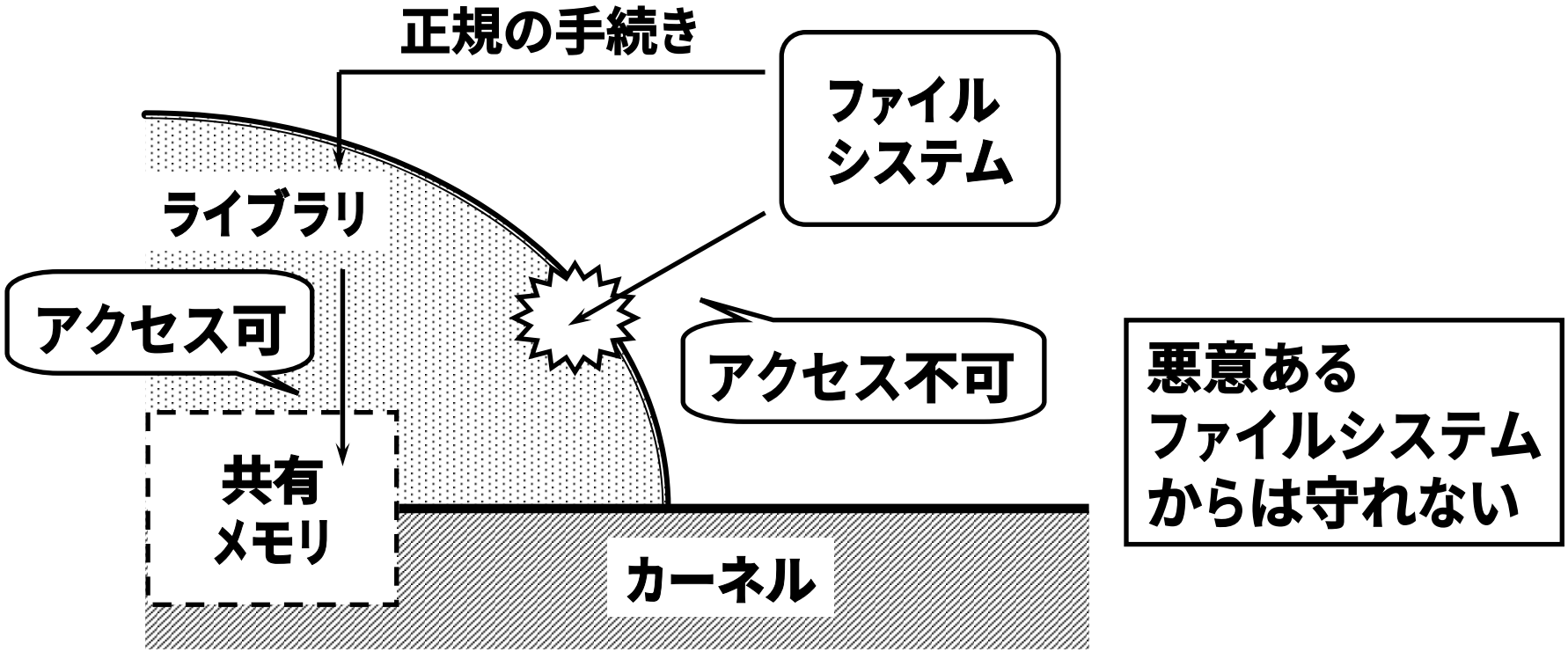
- 共有メモリに直接アクセスするのは危険
  - カーネルデータを破壊するかも

共有メモリへのアクセスはライブラリが隠蔽

- ライブラリはどのようにカーネルデータを保護するか？
  - 共有メモリを保護する
  - カーネルデータをコピーする

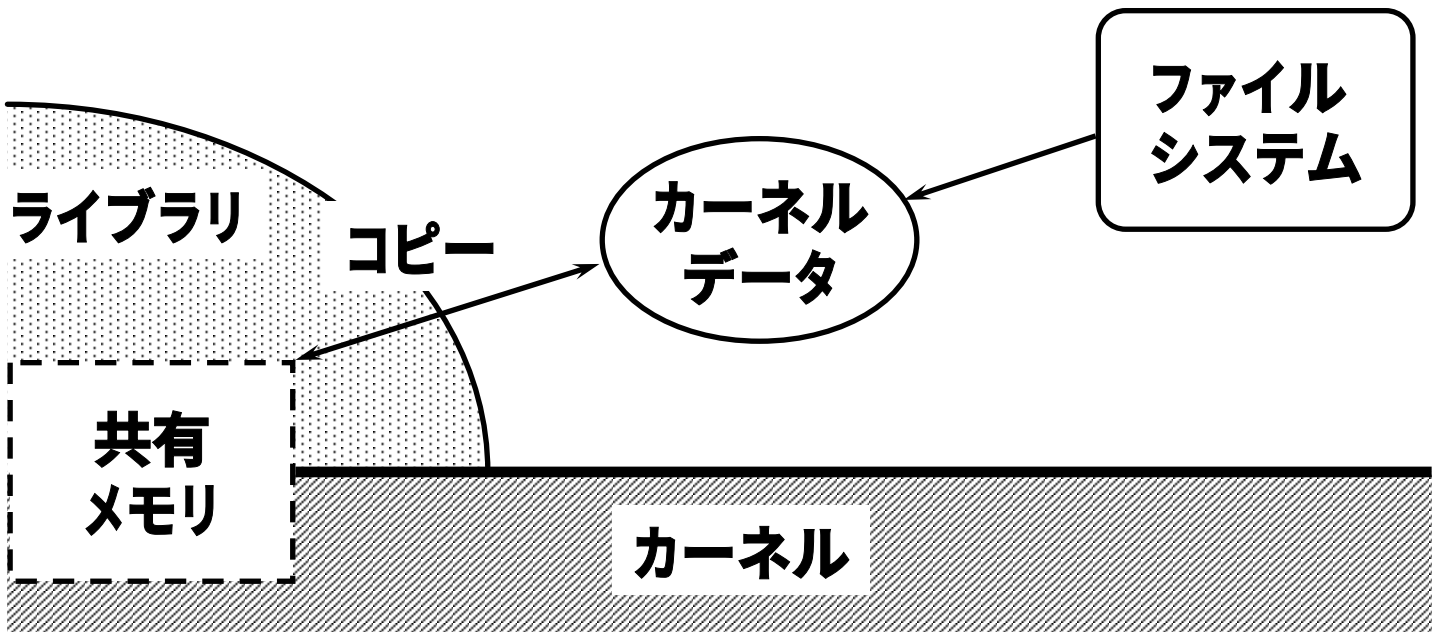
共有メモリの保護

- ライブラリの外では共有メモリをアンマップ



カーネルデータのコピー

- ライブラリの外では共有メモリ上のカーネルデータをコピーしたものにアクセス



第1段階～第4段階

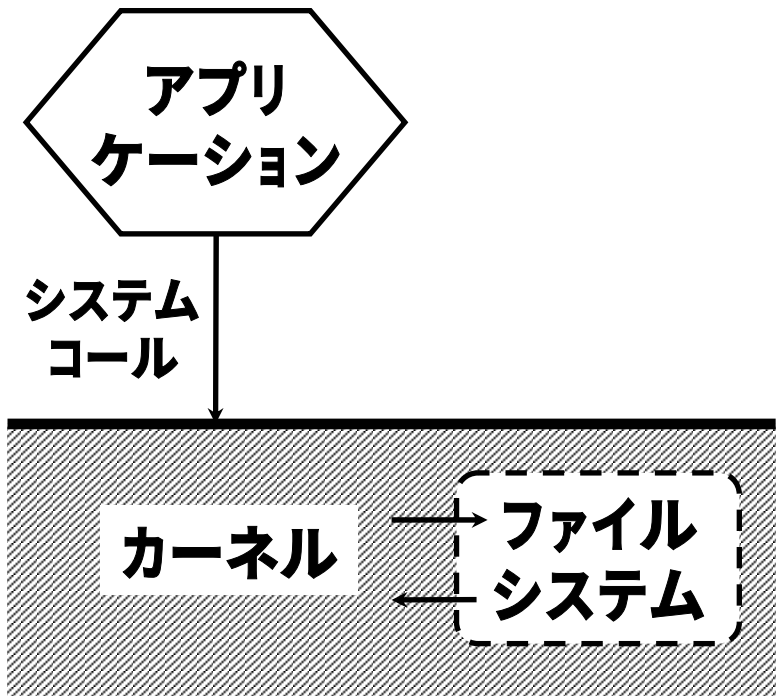
- 第1段階～第4段階の違いは以下の通り

段階	共有メモリの保護	カーネルデータのコピー
1	読み書き不可	する
2	読み出し専用	する
3	なし	する
4	なし	しない

第5段階

- ファイルシステムをカーネルに組み込む
- ソースコードを変えないためのオーバヘッドは残る

モノリシックカーネルとほぼ同等



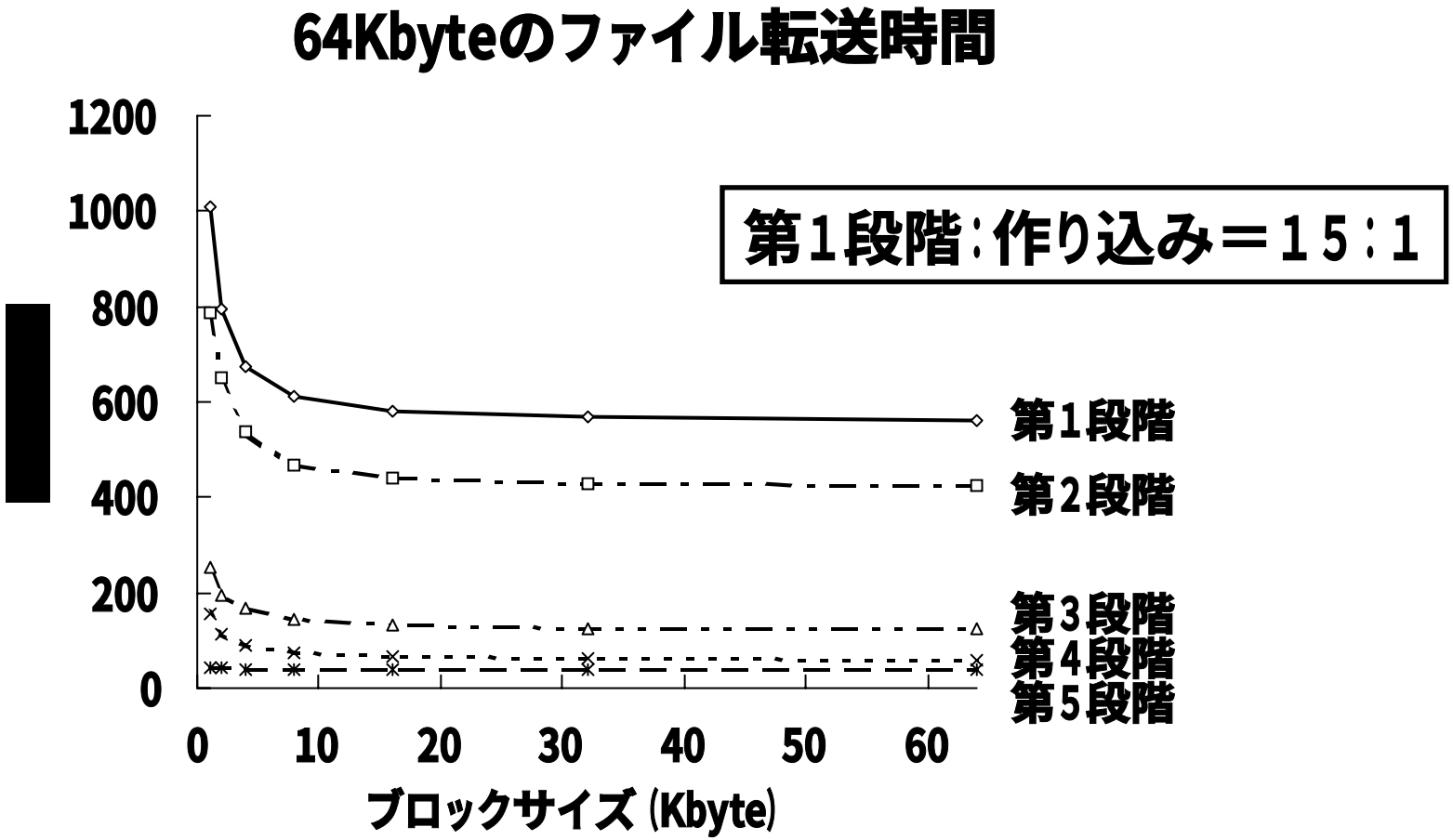
多段階保護機構の実装

- ファイルシステムのための多段階保護機構をNetBSDに実装した
- 2つのファイルシステムを作成・実験した
  - 簡易RAMディスク
  - 簡易NFS

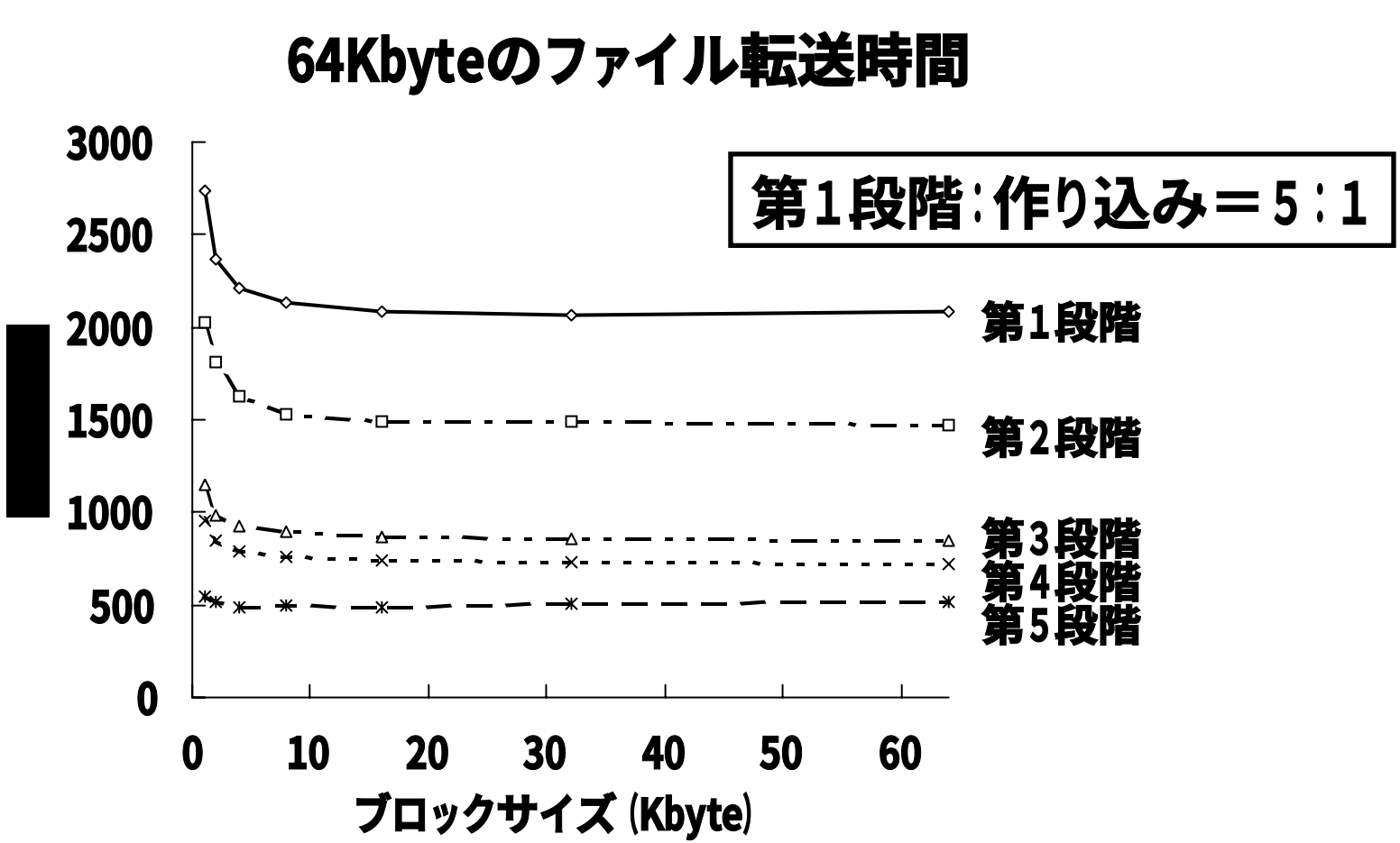
多段階保護機構のオーバヘッド測定

- ブロックサイズを変えてファイルの転送時間を測定した
- 実験対象
  - 第1段階～第5段階のファイルシステム
  - 多段階保護機構を使わず、カーネルに作り込んだファイルシステム
- 実験環境
  - SPARCstation 5

実験結果（簡易RAMディスク）

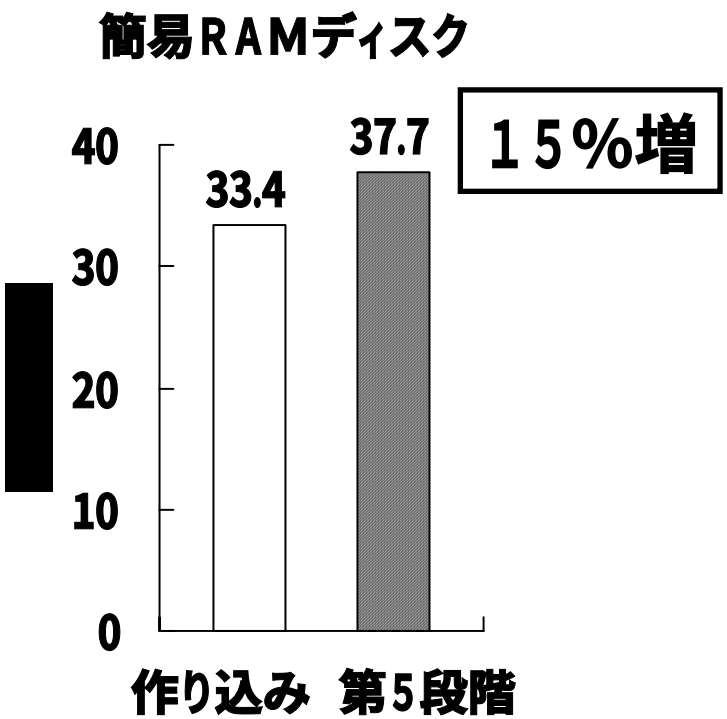


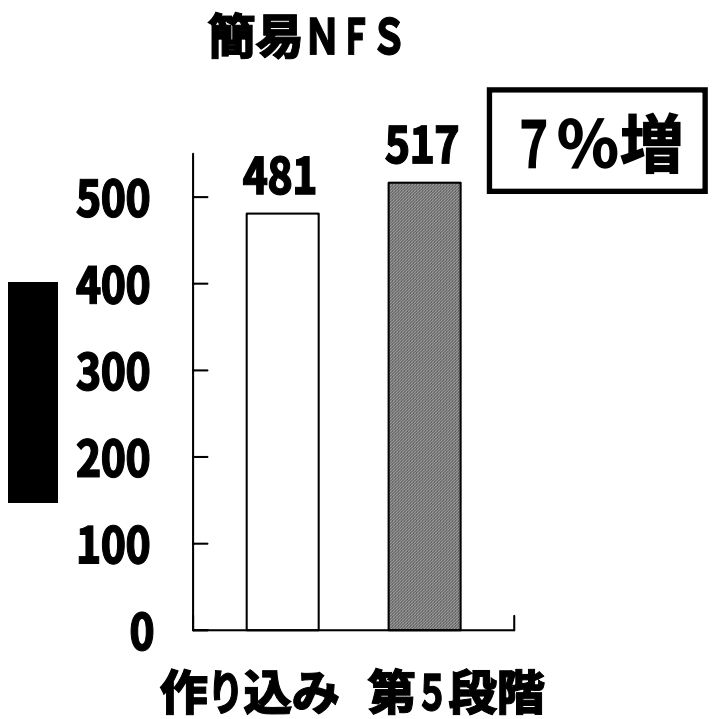
実験結果（簡易NFS）


64Kbyteのファイル転送時間
第１段階：作り込み＝５：１
3000
2500
2000
1500
1000
500
0
0
10
20
30
40
50
60
ブロックサイズ (Kbyte)
第１段階
第２段階
第３段階
第４段階
第５段階

第5段階と作り込みの性能差

64Kbyteのファイル転送時間
(ブロックサイズ 64Kbyte)





考察(1)

- 保護を弱めると実行効率が改善される
- 最も保護の弱い第5段階は作り込みに近い性能を示す

最終的に性能のよいファイルシステムを作成可能

考察(2)

- かなり強い保護をかけてもオーバヘッドはそれほど大きくない
  - カーネルとの通信が頻繁に起こるとオーバヘッドが大きくなる

ＯＳの安定性を実用的なオーバヘッドで保てる

関連研究

- **Mach** [Accetta 86]
  - **モジュールはユーザプロセスで作成**
- **SPIN** [Bershad 95]
  - **モジュールは型安全なModula-3で書かれる**
- **VINO** [Seltzer 94]
  - **Software Fault Isolationでモジュールの安全性を保つ**

最適な一種類の強さの保護のみ提供

まとめ

- 多段階保護機構を提案した
  - 拡張によってＯＳが不安定にならないように、段階的に保護の強さを変えられる
- ファイルシステムのための多段階保護機構を実装した
- 実験によって多段階保護機構の有用性を示した
  - 最終的に作り込みに近い性能が得られる

今後の課題

- 多段階保護機構は一般的な機構なので、他のサブシステムに対しても実装する
- 多段階保護機構をアプリケーションのプラグインなどに幅広く利用できるようにする