

# My Book

published by ReVIEW

# **別冊 詳解 Binder**

**有野和真 著**

**2017-03-31 版 発行**

## 第1章

# {intro} Binder とシステムサービス

別のプロセスに処理を依頼する場合には、何かしらのプロセス間通信 (IPC: Inter Process Communication) の仕組みが必要です。Unix ではパイプやシグナル、Unix ドメインソケットなどが良く使われますが、Android ではこれにプラスして Binder という独自の IPC も使われています。

本章では Binder について詳細に扱っていきます。Binder は通常のプロセス間通信の仕組みよりも用途が限定されています。システムプログラミングで使う、というターゲットの元に設計されています。その為プロセスを超えて送る事が出来る物も通常の IPC よりも多く、単純な値以外にも、ファイルディスクリプタやある種のオブジェクトなどを送る事が出来ます。Android はこの機能をフル活用していて、例えば 7 章の内容の裏側では、ActivityThread の内部クラスである ApplicationThread のプロキシを Binder で送ったり、Bundle や ActivityRecord なども Binder で送ったりされていました。そういう意味では Binder というのは Android にとって重要な技術と言えます。

一方で本章は他の章よりも読者に要求する前提知識が多く、本書の中では少し特殊な章となっています。そこで最初に 8.1 で、あまり前提知識が無い読者を想定して、本書の他の章を理解するのに必要な最低限の事、ひいては Android という物を理解するのに必要な Binder の最低限の所を説明する事から始める事にしました。

あまりこの分野に馴染みのない人がどこまで本章を読むのかは、8.1 を読んで、自分で判断してもらいたい、と思っています。8.1 の内容さえ理解しておけば、他の章を読むのには差し支えありません。本章が難しいと思ったら 8.1 だけ読んだ上で次の章に進んでもらえたら、と思います。

ですが、もし分散オブジェクトにある程度の理解があるなら、本章を最後まで読めば Binder についての全てを理解する事が出来るでしょう。

### 1.1 8.1 最低限の Binder 基礎知識 - 分散オブジェクトを知らない人向け

Binder は、使うのは簡単だけれど実装が複雑、という物です。使い方を覚えるのは比較的簡単で、それだけ分かっていれば他の章を理解するのには十分です。

そこで本節では、難解な実現方法は気にせずに、利用者の視点に限定して必要最低限な話をして

いきたいと思います。使う側に関して言えば、以下の三つを抑えておけば十分だと思います。

- Binder の特徴
- Binder で送れるもの
- IBinder とは何か、Stub.Proxy と Stub.asInterface

そこで本節では、なるべく専門用語などを出さずに、上記の事を説明してみたいと思います。逆に分散オブジェクトに詳しくて Binder の詳細に興味がある人は、本節の内容はあとでより詳細に扱うので、流し読みで十分です。8.2 から真面目に読み始めていただけたら、と思います。

### 8.1.1 Binder の特徴

Binder とはプロセス間通信の仕組みと、その上に構築された分散オブジェクトの仕組みです。この時点で「プロセス間通信」とか「分散オブジェクト」と言った専門用語が出てきてしまいますが、この節ではなるべくそういう言葉を使わないで説明してみます。

#### コラム: 分散オブジェクトシステムと IPC、RPC

分散オブジェクトとは、別のプロセスのオブジェクトを自分のプロセスのオブジェクトのように呼べる技術の事です。これに関連のある言葉として、IPC(Inter Process Communication、プロセス間通信)、RPC (Remote Procedure Call) があります。

IPC はプロセスの間で何かしら情報をやり取りするもの全般を指します。この時点ではオブジェクトや関数と言った概念を前提とはしません。Unix のパイプなども IPC の仕組みと言えるでしょう。

RPC は単なる IPC を越えてプロシージャ、つまり関数を呼び出す、という構造を持っています。関数を呼び出す場合、相手の関数を識別する方法があって、それを通常の関数呼び出しのように呼べる、という事を意味します。さらに RPC の場合は関数の引数をシリアル化して送信し、受け取る側でデシrializeする仕組みが含まれるのが普通です。多くの場合 RPC はプロキシの関数を呼び出すと、相手側の実体の関数が呼ばれる、という振る舞いをします。そして間の部分は何らかの方法の自動生成になることが多いと思います。古くは IDL という言語でインターフェースを書いて、そこからコードを自動生成していました。最近はインターフェースなどの型からリフレクションを用いて実行時に生成する物も多くなっています。

RPC と分散オブジェクトは昨今ではほとんど同じ意味に使われる事が多いですが、分散オブジェクトの場合はオブジェクトのインスタンスが存在する前提となります。オブジェクトのインスタンスがあると、一意性の識別と寿命の管理という問題が発生し、マシンをまたがる前提だといろいろと難しい問題が発生します。乱暴に言ってしまえば、分散オブジェクトでは RPC では必要無かった、規約に従ったリファレンスカウント処理が必要となる、という事です。

また、オブジェクトが複数存在する結果として、オブジェクトを探す、というのも重要な機能となる事が多いと思います。マシンを超えてネットワークからオブジェクトを探す、となると、なかなか複雑な仕組みとなります。

Binder の構成要素に照らし合わせると、Binder で IPC の仕組みをつかさどるのが binder ドライバとなります。その上の BpBinder と BBinder の仕組みでだいたい分散オブジェクトの仕

組みは構成されている、と言ってしまって良いと思いますが、普通は IInterface や AIDL のレイヤまでを含めて分散オブジェクトシステム、と言うと思います。binder ドライバは最初から上に載る分散オブジェクトの為に作られているため、IPC の時点で寿命管理の仕組み (リファレンスカウント) や相手を識別するための仕組み (binder\_node) が入っているのが特徴と言えます。またオブジェクトを探す仕組みとして servicemanager があります。

Binder は別のプロセスのオブジェクトを、自分のプロセス内の通常のオブジェクトと同じように見せかける技術です。同じような技術はたくさんあるのですが、Binder が少し変わっているのは、最初からシステムプログラミングの用途だけを念頭に作られている事です。これは一番下の、よそのプロセスとの通信の部分から、一番上の、ユーザーが使うようなライブラリまで一貫しています。通信部分だけを別の用途で使えるようにもしよう、という配慮も無いですし、上のライブラリを通信部分を差し替えて使えるようにもしよう、とも考えていません。スタックを上から下まで抱え持つて全体を最適化する、というのは Google らしいですね。

Binder はシステムプログラミングを前提にして、それ以外には必要のない抽象化は一切行わず、なるべくシンプルな実装となっています。それを踏まえた Binder のカタログ的な特徴としては、以下のようない物になるでしょう。

- 同一マシン内だけしか使えない
  - シンプルなインターフェース
  - コンパクトな実装
  - 高パフォーマンスで省メモリ
- ドライバとしてカーネルにアクセスする事前提
  - 通信のレイヤでスレッドを認識出来る
  - 相手のタスク構造体を直接操作出来る
    - \* ファイルディスクリプタが送れる

カーネルのドライバでの実装を前提とするので、相手のタスク構造体<sup>\*1</sup>を直接触れる、というのは珍しい部分に思います。

個々の項目の妥当性などを詳細に検証していくと複雑な実装に踏み込まなくてはいけませんが、この位の印象をそのまま持っていたら、そう大きく実態とは乖離していないと思います。

### 1.2 8.1.2 Binder の通常の使われ方 - `getSystemService()` メソッド

Binder を一般的なユーザーが使うのは、9割くらいはシステムサービスを使う時だと思います。

0章で見たように、Android はシステムサービスから構成されたシステムです。システムサービスはアプリのプロセスとは別のプロセスで動いているので、システムサービスの呼び出しは全て

<sup>\*1</sup> Linux カーネルの用語。プロセスを表すカーネルのデータ構造。

Binder を使った呼び出しとなります。

システムサービスを使う具体例を見てみましょう。例えば現在 Activity が表示されているディスプレイのサイズを取りたい場合、Activity や Context に対して

リスト 1.1: WindowManager サービスの取得

```
WindowManager wm = (WindowManager) getSystemService(WINDOW_SERVICE);
Display disp = wm.getDefaultDisplay();
...
```

などというコードを書くとディスプレイのサイズが取得出来ます。ディスプレイのサイズに限らず、アカウントマネージャでもオーディオでも、別のプロセスで実現されてしまう機能は、この getSystemService() というメソッドで何かを取得して、それをキャストして作業するのが Android の基本となっています。

上記のコードのうち、wm.getDefaultDisplay() の呼び出しが Binder によるメソッド呼び出しとなります。見て分かる通り、通常のオブジェクトに対するメソッド呼び出しとコードの上では区別できません。

getSystemService() を使って取得したオブジェクトに対してメソッドを呼び出すのが Binder を使っている例なんだな、とだけ覚えておいてもらえば十分だと思います。

### コラム: 分散オブジェクトに関わりある物達

分散オブジェクトはなかなか複雑なシステムでありながら 90 年代末期には流行っていた為、割と多くの中年プログラマは良く学んでいます。一方で web の時代が来た後にはあまり流行らなくなり、最近のエンジニアだとちょっと使われている事はあるけれど大して知らない、という人も多くなってきた印象です。

90 年代の終わりには複合ドキュメント、というのがこれからは流行る、と言われていました。ようするに Word ファイルの中に Excel のグラフを貼って、ワープロソフトの中で表計算ソフトを動かす事でグラフも編集出来るようにする、という奴です。結局はあまり使いやすく無い上にワープロに貼りたい物は限られているので、アプリケーションごとに対応してしまう方が良い、という結論になったように思います。

Windows で複合ドキュメントを実現するために使われていた分散オブジェクト技術が COM です。COM は Word や Excel のアプリケーション、Internet Explorer などのブラウザを Ruby や JScript といったスクリプト言語から触る為に良く使われている技術に思います。巨大なアプリケーションを外部のスクリプト言語から操作する、というのは分散オブジェクトの使われ方のうち、現在に至るまで最も成功している使われ方に思います。

また、分散オブジェクトはサーバーサイドの開発でアプリケーションのロジックを作る単位として使う、という使い方が提案された事もありました。アプリケーションのロジックをマシンを分散させる事で負荷分散をしたり出来るんじゃないかな、と。でも結局はコンポーネント単位では無くてアプリケーションサーバー全体を複製しておく方がてつりばやく、効率も良いという結論になり、この目的で分散オブジェクトが使われる事もほとんど無くなりました。

### 1.3 8.1.3 Binder で送信できるもの

Android のソースを読んでいて、Binder に付きあつた時に周辺のコードを理解する上で重要なのは、Binder で何を送信出来るか、という事です。送信出来るものさえ把握しておけば、それが内部でどのように送信されているかはあまり知らなくても、ソースを読む上では問題ありません。

Binder で送信できる主な物は以下の 3 つです。

1. 数値、文字列などの値
2. ファイルディスクリプタ
3. サービスオブジェクト (BBinder のサブクラス)<sup>\*2</sup>

1 はそのままなので良いでしょう。

2 は Binder の一つの特徴となっています。Linux では、ファイルを open すると、カーネル内にそのファイルを表すファイルオブジェクトが出来て、各ユーザープロセスにはこのファイルオブジェクトを表すテーブルが作られます。この各テーブルに対応するファイルオブジェクトが入り、テーブルのインデックスがファイルディスクリプタと呼ばれる物になります。

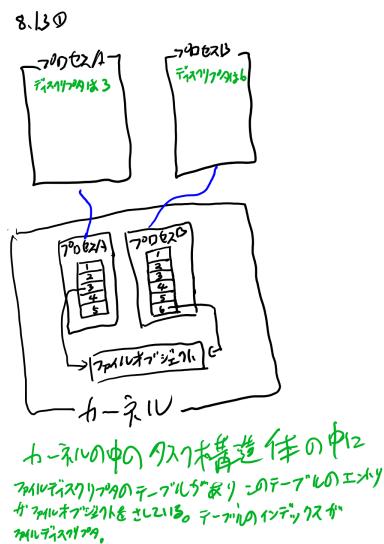
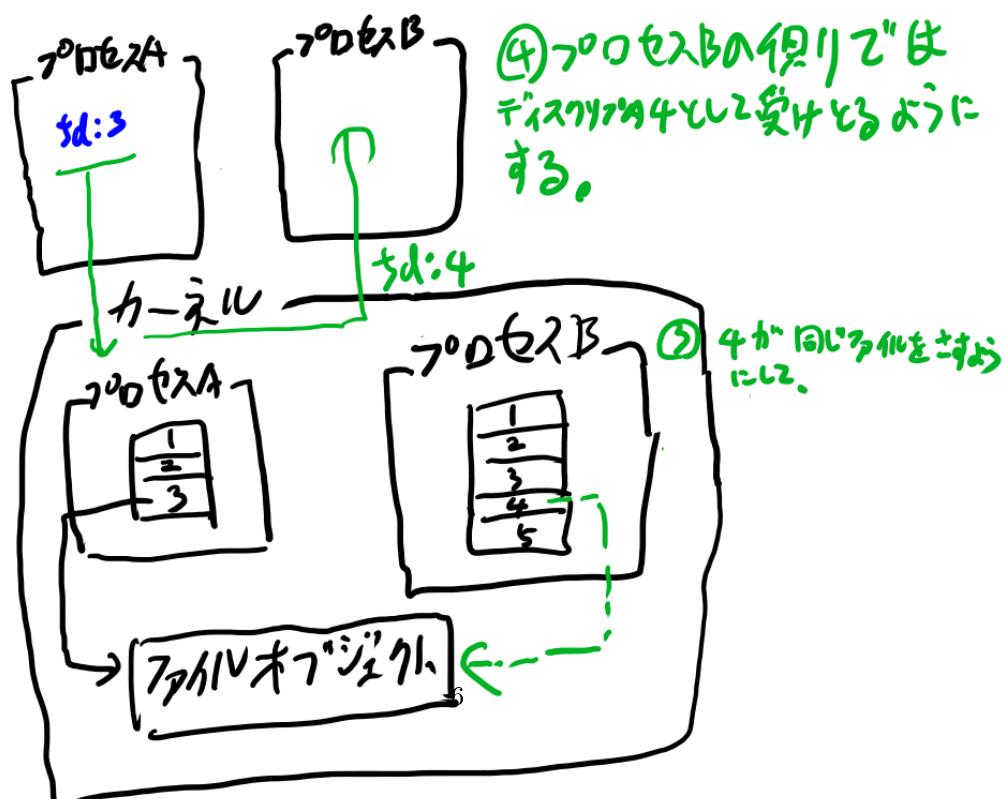
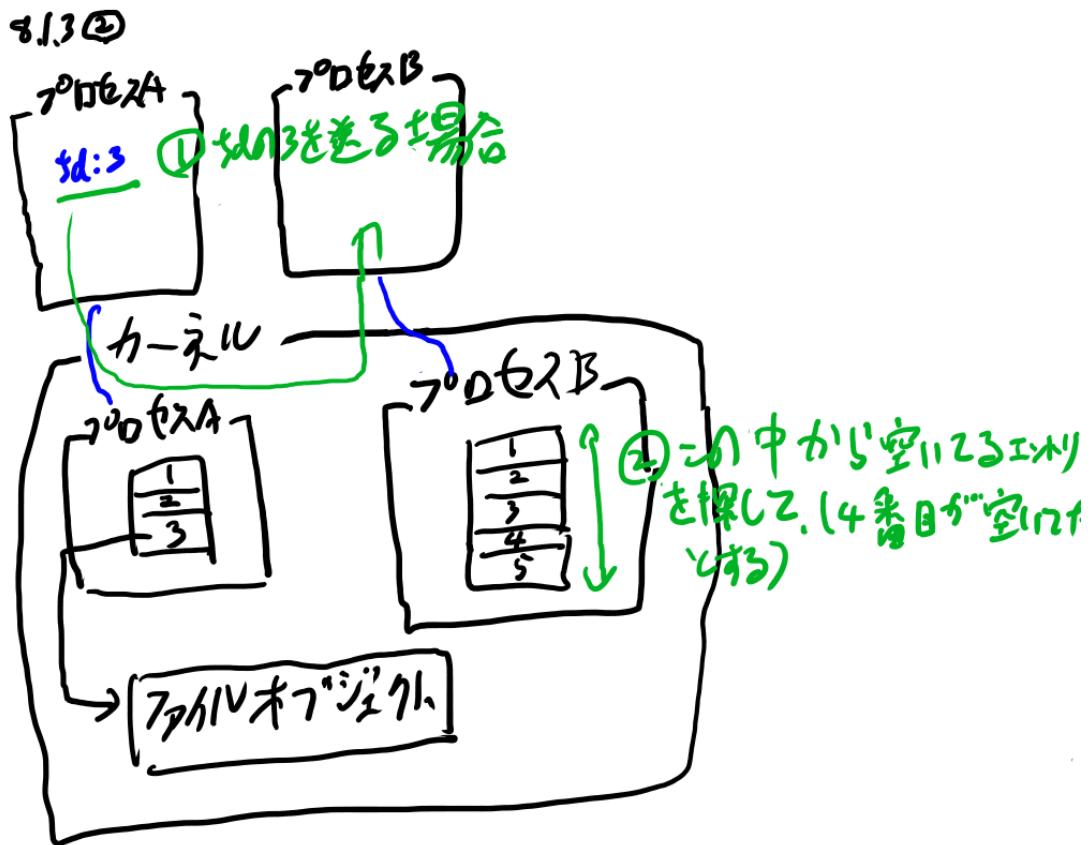


図 1.1 ファイルディスクリプタとファイルディスクリプタテーブル

binder ドライバはプロセス A からプロセス B にファイルディスクリプタを送信している事に気づいたら、プロセス A のファイルディスクリプタテーブルを見て、その参照先のファイルオブジェクトを探し出し、それをプロセス B のファイルディスクリプタテーブルに追加し、そのテーブルのインデックスに変換します。これは双方のタスク構造体というプロセスを表すデータ構造を直接触れるデバイスドライバだからこそ出来る芸当です。

<sup>\*2</sup> 実際はサービスプロキシも送る事が出来ます。つまり IBinder のサブクラスを送る事が出来ます。



3のサービスオブジェクトというのがBinderの中心となる物です。技術的にはC++のBBinderのサブクラスという事になります。BBinderのサブクラスをプロセスをまたいで送受信出来る、というのがBinderという物の中心的な機能です。6章のActivityManagerServiceも、7.2.3で登場したApplicationThreadも、BBinderのサブクラスです。

サービスオブジェクトを送信して、相手のプロセスからこのサービスオブジェクトのメソッドを呼ぶ事が出来る、これがBinderです。

### コラム: 分散オブジェクトいろいろ

世の中には様々な分散オブジェクトの仕組みがあります。私は私が関わった物以外はあまり知らないので、ここで全ての一覧を提示する事は出来ませんが、幾つか名前を挙げてみましょう。

まず本書のコラムでもたまに言及される、分散オブジェクトの代表としてはCOMが挙げられます。COMはWindowsで使われている分散オブジェクトのシステムで、トップクラスに使われている物の一つと言えます。IEとOfficeがCOMから操れる、というのがこの技術がここまで使われた直接の理由だと思います。このシステムではIDLの方言であるMIDLというインターフェース定義言語をコンパイルして、間のコードを自動生成していました。COMは使う側から見るとシンプルなため、互換なシステムも良く作られました。モバイルプラットフォームだとBREWやEMPといったシステムでは、インターフェースはCOMとなっています。

同じMicrosoftでも、より最近の.NETでは、WCFという分散オブジェクト技術があります。これは分散オブジェクト技術を含んだより幅広い物で、オブジェクト呼び出し以外のweb APIのような呼び出しもオブジェクトの呼び出しのように呼び出す事が出来ます。これはインターフェースから実行時にコードを自動生成します。型情報がネイティブよりも多く動的コード生成が容易な仮想マシンではこのスタイルが主流となっていると思います。

Microsoft以外で一番有名な分散オブジェクトシステムと言えばCORBAでしょう。昔はWindows以外で分散オブジェクトと言えばCORBAだった、と言っても過言では無いくらい、CORBA一色でした。オープンな規格で言語非依存でその他様々な物に非依存な分散オブジェクトシステムです。最近見かける所では、Linuxなどで良く使われるGnomeで採用されました。

JavaのRMIなども典型的な分散オブジェクト技術です。またEJBなどはトランザクションなど多くの付加機能がついていますが、これも分散オブジェクト技術の一つと言えます。HORBというJavaのCORBA実装(少し厳密な言い方では無いですが)も有名です。Javaはその他にもDynamic Proxyを用いたより軽量な分散オブジェクトのシステムをたまに見かける気がしますが、EJB以降は分散オブジェクト自体があまり流行っていない印象を受けます。

OS XなどにもNSConnectionという分散オブジェクトの仕組みがあります。Macもかつては複合ドキュメントを推していた時代があったと思いますが、最近ではあまり聞かなくなりました。

こうしてみると分かるように、だいたい分散オブジェクト自身は流行りが終わった技術、という印象を受けています。一方でシステムを構築するには何かしらこの手の技術が無いと不便でもあり、Androidがいまさら独自に必要最低限の物を作った、というのは、長くこの業界に居

た人間としてはなかなか感慨深いものがあり、何がサポートされていないかを見ると「ああ、分散オブジェクト」という複雑になりがちだけど、結局必要なのはこの辺だったんだな」と10年越しに答えを見せてもらったような気持ちになります。

## 1.4 8.1.4 サービスを実行する側のスレッド

Binder はよそのプロセスのオブジェクトを通常のオブジェクトのように呼ぶ事が出来る、という仕組みなので、普段は深くいろいろ考えずに、よそのプロセスのオブジェクトのメソッドを呼んでいる、と考えるだけで良いようになっています。

ですが、少し細かい事を考え出すと事はそう簡単ではありません。まず、スレッドがどうなっているのか、という問題があります。プロセス A がプロセス B のメソッドを呼んでいるとしましょう。プロセス B のメソッドを実行する時にはプロセス B の中にこのメソッドを実行しているスレッドが無くてはいけません。

通常スレッドはプロセス内で作られます。外部から勝手にスレッドを作って走らせる、という事は、普通はしません。ですから、プロセス B でメソッドを実行しているスレッドは、プロセス B が作ったものであるはずです。そこで通常、プロセス B は、あらかじめ Binder のメソッド実行専用のスレッドを作つておいて、ずっと外部のプロセスからの呼び出しを待ち構えておきます。この待ち構えているスレッドが、メソッドを実行するのです。これはメインスレッドとは異なるスレッドです。

Android では Java のプロセスが起動した時に、このスレッドを開始して待ち続けます。詳細は [zzz](#) で扱います。

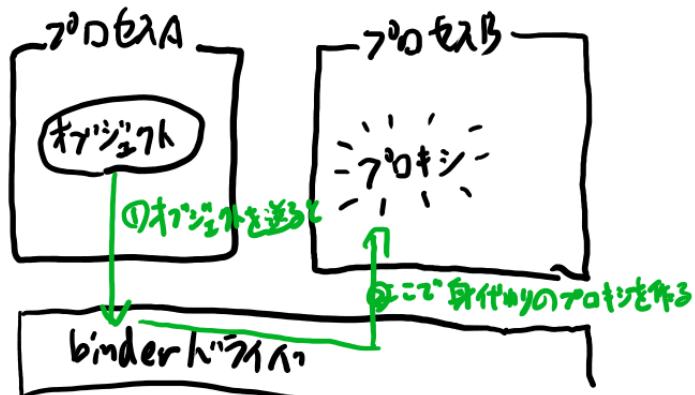
重要なポイントとしては、この Binder 越しに呼び出された側のスレッドは、いつも GUI スレッドとは別の Binder 処理用のスレッドだ、という事です。他の章を読む時には、ここは意識しておく必要があります。

## 1.5 8.1.5 サービス実装とサービスプロキシ

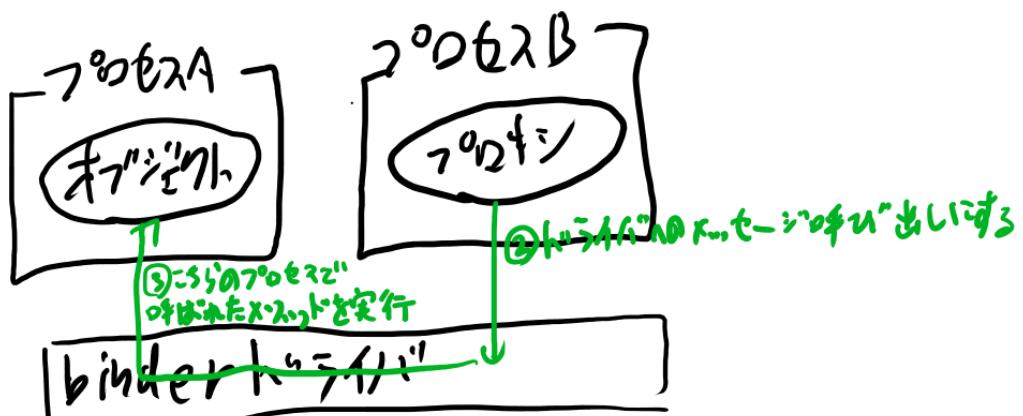
Binder でサービスオブジェクトを送る事が出来る、という話をしました。

実際には送った先はプロキシオブジェクトという物に変換されています。これはメソッド呼び出しを、そのメソッド呼び出しを表すメッセージに変換して、サービス実装側のプロセスに送信する、というオブジェクトです。

9.1.5①



オブジェクトを送る様に見ながら、本当はプロセスBで「身代り」のオブジェクトを作成する。この「身代り」を「プロキシ」と呼ぶ。



プロキシは「メソッドの中での引数などの呼び出された条件をメッセージにして送信。実際の実行はプロセスAで行う。」

図 1.3 プロキシのメソッドを呼ぶとメッセージが送信される

多くの場所ではその事を意識せずにただよそのプロセスのオブジェクトのメソッドを呼んでいる、と思っておけば良いのですが、たまにその幻想が綻びていて、実際はプロキシである、という事を意識しないといけない事があります。

そこで実装している側と、それを呼ぶプロキシ側に分かれている、という事は知っておく必要があります。その現実が一番深刻に表れていますのが次の IBinder です。

### 1.6 8.1.6 IBinder と XX.Stub.asInterface と XX.Stub.Proxy

アプリを開発していると、Binder という事を意識しないといけない事はほとんどないのですが、たまに出てくるのがこの IBinder という奴です。ソースコードを調べていても出てくると思います。同じ名前の C++ のクラスもありますが、ここでは Java の IBinder の話です。

この IBinder とは何なのか？ とソースコードを読んでもなんだか何もしてないように見える。そしてそれがなんだかごちゃごちゃしたコードの XX.Stub.asInterface() とかの引数に渡されている。なんだか良く分からないので、見様見真似でコピペで済ます、というのが良くある IBinder を前にした光景に思います。

これを全部ちゃんと理解しようとすると本章の内容をちゃんと追っていく必要が出てきてしまいますが、概念的な事はそこまで深く理解してなくても理解は出来るので、ここで簡単に説明しておきます（それでもやや難しいですが…）。

IBinder とは、サービスの実装とプロキシの両方を区別なく扱うためのクラスです。イメージとしては C 言語の union のようなもので、実態としてはサービス実装とサービスプロキシのどちらかが入っています。このどちらかが入っているがどちらが入っているかが分からない、というのがコードを読みにくくしています。

IBinder はサービスのオブジェクトがそのまま入っている場合はただキャストすれば良い訳です。少し読みにくいのがプロキシ側だった場合です。

プロキシのクラスは、通信用のオブジェクトをラップして作られています。そして IBinder はプロキシの時は通信用のオブジェクトが入っています。だからプロキシオブジェクトを得るために、この通信用オブジェクトをプロキシのクラスのコンストラクタに渡してやる必要があります。このラップするプロキシオブジェクトのクラス名は「インターフェース名.Stub.Proxy」という名前にする事になっています。例えば IHelloWorld というインターフェースなら、プロキシクラスは IHelloWorld.Stub.Proxy となります。おかしな名前ですが、これは Java の言語の制約上から来ていて、間の Stub に大した意味はありません。

ですから、IBinder がプロキシの場合には、これをコンストラクタに渡してプロキシクラスを作るのです。

リスト 1.2: IBinder からプロキシクラスを作る例

```
// もしこの引数の token がプロキシなら
void someMethod(IBinder token) {

    // プロキシクラスのコンストラクタに渡して、ラップするプロキシオブジェクトを作る
    IHelloWorld proxy = new IHelloWorld.Stub.Proxy(token);
```

```
// 以下この proxy のメソッドを呼び出す  
}
```

この、

1. サービス実装のオブジェクトならただキャストするだけ
2. プロキシの通信用オブジェクトならラップしたオブジェクトを返す

の二つをやってくれるのが XX.Stub.asInterface() です。IHelloWorld というインターフェースなら、IHelloWorld.Stub.asInterface(token) と呼ぶと、とにかくこの IHelloWorld のインターフェースとして使えるオブジェクトが返ってくるので、実装者はこの IBinder がどちらだったのか、という事を気にする必要は無い訳です。

まとめると以下のようになります。

1. IBinder にはサービス実装のオブジェクトがそのまま入っている場合と、プロキシに使う通信オブジェクトが入っている場合がある
2. 「インターフェース名.Stub.Proxy」という名前がプロキシクラスで、これは通信オブジェクトをラップして機能する
3. 「インターフェース名.Stub.asInterface()」というメソッドが IBinder のそれぞれの場合を適切に処理してくれる

この三つが、Binder になるべく関わらないようにしている人でもたまに必要となる知識です。

## 1.7 8.1.6 Binder の基礎知識、まとめ

本節では、難しい話題を理解していくなくともこれだけ知っていれば他の部分のソースを読む時に困らない、という事をまとめてみました。

1. Binder のカタログスペック的な特徴を知っている
2. getSystemService() を使ったオブジェクトに対する操作は Binder を使っている事を知っている
3. 何が送信できるか知っている
4. サービスを実行しているスレッドが GUI スレッドで無い事を知っている
5. IBinder と「インターフェース名.Stub.Proxy」と「インターフェース名.Stub.asInterface()」を知っている

くらいを抑えておけば、内部の詳細に立ち入らなくても他の部分を理解する事は出来ると思います。内部の詳細を理解せずにこれらの事を理解しようとすると、どうしてもぼやっとした部分が残ってしまうと思いますし、たまにここでは扱っていない事もちょっとはあると思いますが、それはそういうものだ、と飲み込んでしまって、詳細を学ぶ時間を他の事に充てるのも一つの選択でしょう。

ここより先は、もっと細かい事を知りたい、という人の為の内容となります。

## 第2章

# {main-intro} Binder の本格的な入門

ここからはある程度この分野に慣れている人を対象に、Binder とその主たる応用例となるシステムサービスの詳細をしっかりと理解していくという内容となります。本節では以降の節全体をまとめた全体像の提示や、以後の節を読んで行く為の導入として、Binder の詳細を理解する意義や想定する前提知識の話をていきます。

なお、本書ではドライバ名としては小文字の binder を、Binder という仕組み全体を表す時は大文字始まりの Binder を使っていきます。

### 2.1 8.2.1 Binder とシステムサービスを詳細に理解する意義

8.1 の内容で、他の章を読んだりソースコードを読んでいく分には十分と言いました。それでは以後の長い本章の内容は何故あるのか？ という話を最初にしたいと思います。

Binder を詳細に理解していく意義としては、以下のような物があると思っています。

1. ソースコードを読んでいて Binder が登場しても、全てを正確に理解出来る
2. システムサービスのメソッド呼び出しをカーネルのコンテキストスイッチのレベルで理解出来る
3. 全てのコードが公開されている、世界中で日々使われている分散オブジェクトのシステムを学習出来る
4. Android の Android らしさを知る手がかりとなる

(1) 1 が一番大きな所だと思います。Android というシステムのソースコードを調べていく時に、「ここから先は分からない…」と毎回壁となってしまうのが、この Binder 周辺だと思います。それは本章がこれだけ長い事からも分かる通り、やろうとしている事が単純な割にはソースコードで知らないくてはいけない事が多いからです。調べたい本題が別にある状態でこの Binder のソースの深い森に遭遇してしまうと、どうしてもそれを最後まで読み切るのは難しく、いつもこの森の前まででソース読みを終える事になってしまいます。

実際のプロダクションの現場において、この森の手前までの調査で困る事はおそらくほとんど無いと思います。ですから仕事で飯を食べるだけなら、多くのプログラマはこの手前までも十分でしょう。

でも Android がこれまでの携帯電話のシステムと比較して最も新しかった点は、携帯電話のシス

テムとしては信じられないくらいオープンだった事です。せっかく全てのソースコードが公開されているのですから、Android を楽しみ尽くす為には、ソースは全て理解出来る方が絶対に良いと思います。

全てを理解しよう、と思った時に大きな壁として立ちはだかる Binder 周辺の全構造がちゃんと解説されている本章は、Android を楽しもう、と思う読者には、大きな助けとなると思います。

(2) システムサービスの呼び出しなどに代表される Binder 越しの呼び出しで、実際に何が起こっているのかをカーネルのコンテキストスイッチのレベルで理解出来る、というのは、システムを深く理解する立場からすると重要になります。コンテキストスイッチのレベルから分かる事で、汚されるキャッシュや TLB エントリなど、既にベテランのデベロッパが知っている多くの周辺知識が使えるようになります。

最終的なパフォーマンスは計測の必要がありますが、Android のシステム構成がどの位重そうか、という感覚が分かるようになります。

(3) この 3 だけはちょっと変わった視点で、分散オブジェクトのシステムの勉強としての視点となります。複雑になりがちな分散オブジェクトシステムですが、Binder は他のシステムと比べるとローカルだけを前提としていて、使われる環境も Android だけをターゲットにしているので非常にコンパクトなシステムです。そうでありながらおもちゃの分散オブジェクトシステムとは違いプロダクションで最も良く使われている分散オブジェクトシステムの一つと言えるくらい使われていて、しかも現在でも使われ続けている現代のシステムとして、十分な実績があります。

実績のある分散オブジェクトシステムを学ぼうとすると間の抽象化レイヤが多すぎてなんだかぼやっとした理解にとどまってしまう事が多いと思いますが、Binder は抽象化を極限までしない実装となっているため、一人の人間が隅から隅まで理解出来るシステムとなっています。分散オブジェクトを本格的に学ぶ最初のシステムとしては、最も良い教材だと思います。

(4) 最後は上三つと比べると少し抽象的な話となりますが、Binder は Android というシステムのプロセス構成という、モバイル OS としての立ち位置を考える時にキーとなる部分をつかさどる技術となっています。

モバイルの OS としては全て単一のプロセス内で構築する原始的な RTOS のような物から、全てプロセスを分けるマイクロカーネル的な物までいろいろと考えられます。そして多くのシステムで全てを別プロセスにするのは重すぎるため、アプリは dll にしたりと言った工夫が見られます。

Android では Binder という物を導入する事でモバイル OS としては旧来と同程度に貧弱なリソース（か少しリッチな程度）のデバイスでも動きつつ、将来的にはプロセスを分けていきよりリッチなデバイスで高パフォーマンスなシステムしていく、という進化の道筋を最初につけておいたのが特徴的です。

Binder を詳細に理解しておくと、この辺のバランス感覚を知る事が出来て、ひいては Android の Android らしさ、のような物を知る事が出来ます。こうした哲学や「らしさ」という要素は、一段深い Android という物の理解を生むと同時に、何故いろいろある中で Android だったのか？ と言ったより難しい問への答えを自分の中で探す時の手掛かりとなります。

### コラム：分散オブジェクトとマイクロカーネルの夢

私的な話となりますますが、著者の私は COM などの分散オブジェクト技術が好きな方です。

COM には若いころ結構な時間をかけて学んだ思い出があります。

カーネルを小さく保って最初からオブジェクト指向ベースの OS を作る、というのは結構多くの人が夢見た所で、私も若いころは MSR の MMLite などのような同コンセプトのシステム資料を見て胸躍らせた時代があります。

Binder の起源となった BeOS については、私はあまり詳しくありませんが、同様にマイクロカーネルでオブジェクト指向ベースなシステムだったと理解しています。その BeOS の Binder を元に Linux というマイクロカーネルと正反対のカーネルが組み合わさって、分散オブジェクトベースのシステムでありながら現実の数々の問題を解決している、というバランス感覚は、夢見る青二才とは格の違う真の OS アーキテクトの凄みを感じさせる部分だと思っています。

Honeycomb の頃などにその設計思想を活かして現代的な GUI システムへと変貌していくさまをリアルタイムで見ていた私は、久しぶりに若いころの興奮を思い出しました。

====[/column]

## 2.2 8.2.2 Binder を詳細に理解するのに必要な前提知識

本章の以降の内容では、分散オブジェクトシステムの開発の経験を前提とさせてもらいます。具体的には

1. IDL を書いてコンパイルし、スタブの実装を書いてプロキシを使った事がある（またはその意味が分かる）
2. スタブ、プロキシという言葉を理解している
3. IPC、RPC、分散オブジェクト、シリアル化といった用語が分かる
4. C 言語などの低レベルの通信層のコードに慣れている（オブジェクトのシリアル化等）

という位をイメージしています。昔書いた事はあるが忘れかかっている、という人や、完全に上記条件は満たさないが似たようなシステムを使っている（例：インターフェースからの動的コード生成系のフレームワーク利用者など）人などに向けて、多少は説明も行いますが、まったく知らない人が上記の事を学ぶには本書は適切では無いと思います。

上記の事を学びたい人は、分散オブジェクトの入門書などを学ぶのが良いと思います<sup>\*1</sup>

## 2.3 8.2.3 Binder を構成するレイヤ

分散オブジェクトのシステムは一般に複数のレイヤで実現されていて、各レイヤでプロキシと実装側のクラスが出てくる事から、毎回同じようなクラスが出てきて同じような説明をする事になります。

そんな説明を読み続けて行くと、そこで言っている事は理解する事は出来ても、そもそもなんで今こんな話をしているのか、という事が良く分からなくなっていく事になりがちです。

<sup>\*1</sup> 今なら gRPC や Thrift などでしょうか。私の頃は COM で学びました。

そこでまずは全体の構成を見てみたいと思います。以下の各節で何の話か分からなくなった時にはここに戻ってきてみてください。

## 8.2.3 ① Binderを構成するレイヤ。

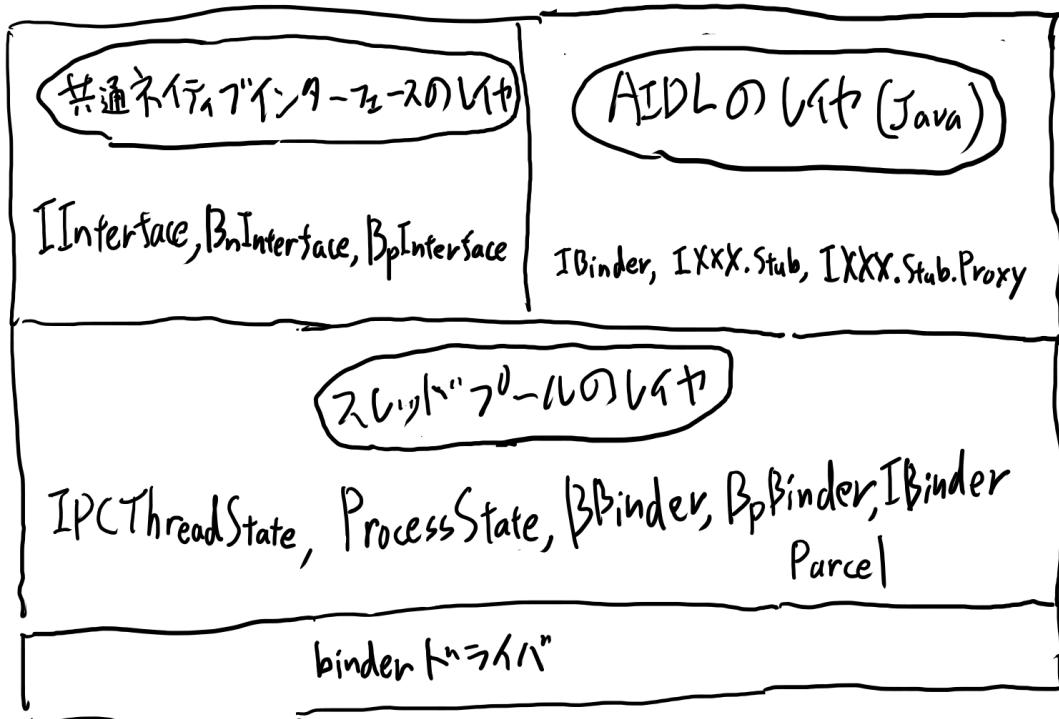


図 2.1 Binder を構成するレイヤ達

まず一番下から見ていくと、一番下は binder ドライバとなります。binder ドライバが二つのプロセスの間の通信を担当します。

その上にはスレッドプールを実現するレイヤがあります。<sup>\*2</sup> クラスとしては `ProcessState`、`IPCThreadState`、`BBinder`、`BpBinder`、`IBinder` です。

このレイヤで単純な `ioctl` によるプロセス間通信が、スレッドプールと C++ のオブジェクトに対するメッセージ送信、という形へと発展します。スレッドプールは、その実現で `BBinder` というオブジェクトの基底クラスと `BpBinder` というプロキシの基底クラスがやりとりされる、という前提

<sup>\*2</sup> なお、このレイヤ分けの図も名前も私がソースを読んで決めたもので、公式から発表されている物ではありません。そもそもこの周辺はあまり公式の情報はありません。

に基づいる為、これらは合わせて使う必要があります。この基底クラスで、全てのサービスで共通となるメッセージの処理を行います。

ここまでオブジェクトという対象をやりとりするのですが、呼び出し側はサービスが自分のプロセスに居るのか別のプロセスに居るのかに応じてコードを変えなくてはいけません。

このスレッドプールのレイヤの上には、それぞれ並行して二つのレイヤが存在しています。ネイティブと Java で、呼び出し側コードをサービスがどこのプロセスに居るかを意識せずに使えるようになる為のレイヤです。共通ネイティブインターフェースのレイヤと AIDL のレイヤはお互い依存していない、独立したレイヤです。どちらも下のスレッドプールのレイヤを使用しています。

共通ネイティブインターフェースのレイヤは、クラスとしては IInterface、BnInterface、BpInterface の三つのクラスとなります。

AIDL のレイヤは Java によるサービス実装のレイヤとなります。AIDL からコードを自動生成する仕組みを用いるレイヤで、主なクラスは生成するインターフェースに応じた名前となる為、図では IXXX と表記しました。通常は IAudioService などのような名前となります。

ネイティブでサービスを実装する時は IInterface の方を使い、Java でサービスを実装する場合は AIDL を使う事になります。

この二つのレイヤが実際にサービスを実装する人が直接用いるレイヤの為、なるべく実装者が不要なコードを書かなくても済むように自動生成やマクロなどのいろいろなトリックが使われています。また、実装にはいろいろと慣例があり、その慣例に何も考えずに従って実装すると、下の方の仕組みがどうなっているか、という事はあまり意識せずに、分散オブジェクトとしてのシステムサービスが実装出来るようになっています。開発者があまり良く理解していなくてもとりあえず見様見真似で動くコードが書ける、という訳です。

仕組みとして重要なのはドライバと、その上のスレッドプールのレイヤ、つまり IPCThreadState や BBinder のレイヤとなります。そこより上の層は開発者が実際に目にする事は多くとも、実装的には複雑な事はありません。Binder の全体像をしっかりと把握するためには binder ドライバとスレッドプールのレイヤをしっかり学ぶ事がポイントとなります。

## 2.4 8.2.4 本章の以後の構成

分散オブジェクトの解説をする時に、上からするか下からするかは難しい選択です。

上から解説すると各コードの使われ方が分かるので目的は理解しやすい反面、毎回依存する下のレイヤーはまだ解説されていない状態で現在のレイヤーのコードを理解しないといけない為、読み手のコードリーディングの慣れを要求します。一方下から解説すると依存する物は既に説明されたものだけなので説明は全て理解出来る反面、現在説明している事が何に使われるかが分からぬまま説明が続く事になります。

本書では下から順番に解説する事を選びました。その為説明はそこまでに全て出てきた要素で閉じるため読みやすい反面、そのコードがどう使われるかは先を読まないと分からない、という構成になっています。読んでいて何のために今説明しているコードがあるのか、という事が良く分からなくなったら、少し先を読んでみてから戻ってくると言っている事が分かる、という事があると思いますので、そういう読み方をしてみて下さい。

まず 8.3、8.4、8.5 の三つの節で binder ドライバのレイヤの話をします。その後 8.6 でスレッド

プールのレイヤを、8.7で共通ネイティブインターフェースのレイヤを扱い、8.8で AIDL のレイヤ、つまり Java によるシステムサービス実装を扱います。

最後に 8.9 で Binder の仕組みを実際に使っている側に視点を移して、システムサービス関連のプロセスがどのように動いているか、他の章で Binder が絡む所を Binder 側から見るとどうなるか、などの他のコンポーネントから見た Binder という位置づけを見ていきます。

なお、本章ではかなり低レベルなコードがたくさん出てきます。その為、少し他の章よりはプログラムを読みなれている人向けになっています。コードは説明の為に使っているのであって、動く事は意図していません。たとえば実際には 0 クリアをしないといけない重要なフィールドを無視したりしている為、完全に動くコードではありません。

それでは順番に見ていきましょう。まずは binder ドライバです。

## 第3章

# {syscall} binder ドライバを扱う 三つのシステムコール - open, mmap, ioctl

Binder の仕組みのうち、一番下のレイヤとなるのが binder ドライバです。binder ドライバ自体はとても単純な物で、提供している機能もかなり原始的です。

この節から続く三つの節で、binder ドライバについて解説していきます。この節では binder ドライバを扱う基本的なシステムコールである、open(), mmap(), ioctl() について、使い方の例を見ていきます。次の 8.4 ではこれらのシステムコールを使ってどのようにメッセージを送受信するか、その内容と使い方についてみていきます。8.5 ではこれらのメッセージで送信できるものについて、ドライバの内部実装と合わせて見ていきます。

なお、本章でサービスと言った場合はシステムサービスの事だとします。

### 3.1 8.3.1 binder ドライバの特徴

binder ドライバはプロセス間通信の仕組みです。サービスというプログラミングモデルでシステムを組む為に、それ専用のプロセス間通信の仕組みを作った、それが binder ドライバです。

以下のような特徴があります。

1. ローカルに特化している
2. ドライバとして実装されている為、Linux カーネルの内部データ構造を用いる事が出来る
3. サービスというプログラミングモデルを前提としていて、スレッドプールやリファレンスカウントのサポートが最初から入っている
4. 呼び出し元のプロセスの uid を正確に把握している
5. ファイルディスクリプタを送信出来る

以上を 8.1.1 と比較すると、Binder の特徴の多くはそのドライバで実現されている事に気づきます。

世の中にはたくさんのプロセス間通信の仕組みやその上の分散オブジェクトの仕組みがありますが、分散オブジェクトシステムの為だけに作られたプロセス間通信と、そのプロセス間通信だけで

動く分散オブジェクトシステム、というのは珍しいのではないでしょうか。少なくとも私は Binder しか知りません。

binder ドライバはプロセス間通信の仕組みとしては、TCP/IP や UDP のような本格的なプロトコルスタックを持つ物と比較すると、かなりシンプルな物と言えます。一方で相手のスレッドやリファレンスカウントといったものをサポートしているという点で、パイプなどの原始的な仕組みに比べるとやや複雑と言えます。多くの分散オブジェクトでは IPC のレベルではスレッドやリファレンスカウントの概念を持たない物が多いので、その上の分散オブジェクトのシステムでその仕組みを持つ事になります。一方 Binder は IPC のレベルでそのサポートを持つので、上のオブジェクトシステムが複雑になるのを防いでいます。

また、デバイスドライバとして直接カーネルモードで動くように実装されているのも特徴的です。相手のスレッドを起こすのも、カーネルのタスク構造体に直接アクセスして、まるで通常のプロック型デバイスのファイル read と同じように起こす為、単純明快です。カーネルのデータ構造に直接アクセスできるため、相手の uid を直接参照したり、ファイルディスクリプタテーブルを書き換えたり、と言った事も簡単に出来ます。

uid を正確に把握している、というのは、地味ですがリモートにも送る事が出来るメッセージング機構だと素直には作りづらい所があります。uid というのはシステムローカルな物だからです。ですがシステム内でしか使われない事を前提としている Binder では変に抽象化せずに直接 uid を使う事が出来ます。

4 章でも触れた通り、Android はアプリのプロセスを別々の uid に設定する事でセキュリティを確保している為、uid を調べる事は頻繁に発生します。カーネルモジュールは current という参照を通じて呼び元のプロセスの情報にアクセス出来るので、カーネルモジュールのドライバとしてプロセス間通信を実装するなら、呼び元のプロセスの uid を調べる、という機能は、ストレートに実装出来ます。

## 3.2 8.3.2 binder ドライバの使い方

binder ドライバの実装の細かい話に入る前に、実際に binder ドライバを使用するコードの全体像がどうなるかを見てみましょう。binder ドライバは /dev/binder というファイルとして存在していて、binder ドライバを使うプロセスはこれを open したり ioctl したりします。

binder ドライバはプロセス間通信の仕組みです。何かしらのデータをプロセスを越えて送る物、と言えます。送る物の詳細は後に回して、ここでは data というデータで長さが len の物を送る、という前提でのコードを見てみましょう。データ送信の単純化したコードの全体像を示すと以下のようになります。

リスト 3.1: binder ドライバを用いた呼び出し全体

```
// 1. binder ドライバをオープン
fd = open("/dev/binder", O_RDWR);

// 2. binder ドライバをメモリ領域に mmap。サイズは 128K Bytes
mmap(NULL, 128*1024, PROT_READ, MAP_PRIVATE, fd, 0);
```

```
// 3. read と write に使う引数の初期化。read と write は同時に使える
struct binder_write_read bwr;

// write 関連初期化
bwr.write_size = len;
bwr.write_consumed = 0;
bwr.write_buffer = (uintptr_t) data;

// read 関連初期化、今回は read はしないので 0 を入れておく。
bwr.read_size = 0;
bwr.read_consumed = 0;
bwr.read_buffer = 0;

// 4. binder ドライバの ioctl 呼び出し
res = ioctl(fd, BINDER_WRITE_READ, &bwr);
```

上記のコードはデータを送信するのに必要な全コードを最初から最後まで書いています。個々のブロックの意味についてはこれから説明していきますが、まずは全体がこんな感じになる、ということを見てください。

上記のコードにもあるように、binder ドライバを使用する典型的な手続きとしては以下のようになります。

1. `open("/dev/binder", O_RDWR)` を呼び出す
2. 1 で得られた `fd` を `mmap` する
3. `binder_write_read` という構造体に送りたいデータを指定して `BINDER_WRITE_READ` で `ioctl`

実用の場面では、`open` と `mmap` はプロセスの初期化で一回行い、以後は `ioctl` の所だけを繰り返し呼び出して通信を行います。上記コードのコメントで言う所の 1 と 2 はプロセスの初期化の所で一回行うだけ、3 と 4 はメッセージの呼び出しの都度行うという事です。

`ioctl` は送信と通信をどちらも担当します。この `ioctl` を呼び出したあとに、`bwr` の `write_consumed` や `read_consumed` の値を見て、書き込み、読み込みのどちらが処理されたかを判断します。

以下では上記のそれぞれのコードについての詳細を説明していきたいと思います。

### 3.3 8.3.3 binder ドライバの open と mmap

zzz このパラグラフはボツ

ユーザープロセスのメモリ空間はそれぞれ異なる為、通常の方法で他人のプロセスのデータを触つたりコードを呼んだりは出来ません。そこでカーネルの力を借りる必要が出てきます。プロセスが切り替わってもカーネルのメモリ空間はそのままの為、カーネル空間にデータを書けば、それを別のプロセス空間でもアクセスする事が出来ます。ですがユーザープロセスは直接はカーネルのメモリはアクセス出来ない為、何らかのシステムコールが必要となります。

binder ドライバを使うプロセスは、まずデバイスファイルである `/dev/binder` ファイルを `open` します。

リスト 3.2: binder ドライバのオープン

```
// 1. binder ドライバをオープン  
fd = open("/dev/binder", O_RDWR);
```

open はファイルディスクリプタを返します。以後の操作はこの open で返ってくるファイルディスクリプタに対して行います。

binder ドライバを使う時には、open した後にこのデバイスファイルを mmap する事になります。

リスト 3.3: binder ドライバを mmap

```
// 2. binder ドライバをメモリ領域に mmap  
mmap(NULL, 128*1024, PROT_READ, MAP_PRIVATE, fd, 0);
```

mmap はフラグが多いので全てを説明はしませんが、ポイントとなる一番目と二番目の引数だけ簡単に説明しておきます。

先頭の引数はユーザーのアドレス空間のどこにマップするかを指定します。NULL を指定するとカーネルが勝手に選びます。

二番目の引数はマップするサイズです。ここでは 128K Bytes の範囲を mmap するように指示しています。

普通 mmap はファイルの中身をメモリ空間にマップする為の API です。ですが mmap の呼び出しは内部ではドライバに処理が委譲されていて、ドライバごとに違う処理を行う事も出来ます。実際 binder ドライバはただファイルの中身をメモリにマップしている、というのとは、だいぶ異なる挙動をしています。

binder ドライバファイルを mmap すると、内部でドライバはカーネル空間に指定されたサイズくらいの送受信用のバッファを確保します。そしてそのカーネル空間に割り当てたメモリと同じ物理メモリを、ユーザー空間にもマップします。

そしてこのカーネル空間にマップされたメモリは、以後ドライバ側で送受信に使われます。ユーザー空間にマップされている領域は、ioctl の戻りなどで使われていますが、直接コードの中でそのアドレスをあらわに参照する事はありません。

何故こういう事が必要か、というのは、少しカーネルのコンテキストスイッチに慣れていないと想像しにくいかもしれません。仮想メモリから実メモリへの参照、というのは、基本的にはハードウェアで自動的に行われています。カーネルはハードウェアに仮想メモリと実メモリの対応表をセットしたり、といった操作はしますが、実際にカーネルなどのソフトウェアが仮想メモリのアドレスから実メモリをたどって値を読んだりはしません。

ドライバにとっても、アクセス出来るメモリは現在のプロセスのメモリ空間とカーネルのメモリ空間だけなのです。そのどちらでも無い、例えば送信先のプロセスのメモリを参照する方法はありません。

そこで送信先プロセスにどのようにデータを渡すか、というと、送信先プロセスが「現在のプロ

### 第3章 {systemcall} binder ドライバを扱う三つのシステムコール

セス」の時に、送信先プロセスのメモリ空間とカーネルのメモリ空間で同じ物理メモリを指すようにマップするのです。この時は送信先プロセスがまだ現在のプロセスなので、こういう操作がドライバから可能です。

そして送信元のプロセスにコンテキストスイッチしてしまっても、このカーネル空間のメモリに書きこんでおけば、後で送信先のプロセスにコンテキストスイッチした時も、ユーザー空間にコピーする事無くそのまま参照出来ます。コンテキストスイッチした時にマップされる場所をカーネル側にも置いておく事で、コンテキストスイッチせずにコンテキストスイッチした後のメモリ空間にデータを置いて置ける訳です。

8.3.3 ①

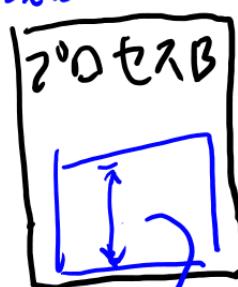
現在のプロセス



カーネル

現在のプロセスのメモリとカーネルのメモリに触る事は出来ない。  
プロセスAがプロセスBにデータを送る時、この状態で、プロセスBのメモリには触れない。

現在のプロセス



ここで「現在のプロセスがBの時に、同じ物理Xモリのブロックをカーネル空間とプロセスBのメモリにマップしておきます。(この時はプロセスBのメモリに触れる)

物理Xモリ

カーネル

現在のプロセス



左側のメモリは触れないが、

<sup>23</sup>  
物理Xモリ

カーネル

左側から書き

### 3.4 8.3.4 binder ドライバの ioctl と読み書き

Binder を用いたメッセージの送受信には、ioctl システムコールを使います。ioctl については「[ioctl システムコール](#)」を参照ください。

メッセージの送受信に使うリクエスト ID は BINDER\_WRITE\_READ です。呼び出しは以下のようないコードとなります。

リスト 3.4: binder ドライバの ioctl

```
// 4. binder ドライバの ioctl 呼び出し
res = ioctl(fd, BINDER_WRITE_READ, &bwr);
```

三番目の引数の**&bwr** というのは、送受信に使う構造体、binder\_write\_read のポインタです。BINDER\_WRITE\_READ は送信と受信を一度に出来る API となっている為、

binder\_write\_read には読み取り関連の設定と書き込み関連の設定を行う事になっています。書き込み関連は以下のようにバッファと長さ、そして現在どこまで書いたかを表す consumed を初期化します。

リスト 3.5: binder\_write\_read の write 側の初期化

```
struct binder_write_read bwr;

// write 関連初期化
bwr.write_size = len;
bwr.write_consumed = 0;
bwr.write_buffer = (uintptr_t) data;
```

ここで data はドライバに送りたいデータの入ったポインタ、len はそのデータの長さです。読み込み関連は読み込みに使うバッファとそのサイズですが、読み込みをしない場合は read\_size に 0 を入れておきます。

リスト 3.6: binder\_write\_read の read 側初期化

```
// read 関連初期化、今回は read はしないので 0 を入れておく。
bwr.read_size = 0;
bwr.read_consumed = 0;
bwr.read_buffer = 0;
```

このように初期化した bwr を ioctl に渡します。再掲すると以下のコードです。

リスト 3.7: binder ドライバの ioctl 再掲

```
// 4. binder ドライバの ioctl 呼び出し  
res = ioctl(fd, BINDER_WRITE_READ, &bwr);
```

このように ioctl を呼ぶ事で、ドライバにデータを送ったり、逆にドライバからデータを受け取ったり出来ます。

以上で 8.3.1 で示した、binder ドライバを使った API 呼び出しの標準的なコードについて、一通りの説明を行いました。

しかし、ここまで説明では、bwr の read\_buffer の中身や write\_buffer の中身、つまりドライバにどういう種類のデータを書き込んで、ドライバからはどういう種類のデータが読み取れるのか、という話は一切していません。

binder ドライバと送受信するデータの中身は、bwr の write\_buffer や read\_buffer の中でさらに決まりがあります。今回の例で言うと bwr.write\_buffer に渡しているデータの中で、さらに決まりがあるのです。

以後ではこの送受信のデータの詳細から、binder ドライバという物の動きを具体的に見ていきましょう。

## 第4章

# {driver\_message} 8.4 binder ドライバによるメッセージの送受信 - servicemanager とサービス

前節では、binder ドライバを扱う基本的なシステムコールとなる、open, mmap, ioctl について簡単に見ました。このうち、ioctl については実際に何を送受信するのか、という所の話はしていません。本節ではこの ioctl でやり取りするメッセージの内容について見てきます。

メッセージを見ていく時には、そのメッセージのやり取りの相手、という物が登場します。この相手がサービスです。

そこで本節ではメッセージの内容とサービスの呼び出しについて見てきます。その過程で重要な特別なサービスである、servicemanager についても扱います。

### 4.1 8.4.1 ドライバに書きこむデータの入れ子構造

ドライバに書きこむデータは binder\_write\_read 構造体のデータだ、と言いました。この構造体の中にさらに BC\_TRANSACTION の時には binder\_transaction\_data 型のデータが入り、その中にさらに flat\_binder\_object が入ります。このようにデータは入れ子になっていて、しかも構造は全て似ています。そのデータの種類があって、さらにバッファのポインタとその長さ、というのがパターンです。

通信にまつわる説明ではありがちな構造ですが、この手の説明を読むのに慣れてないと、毎回同じような事を言っている別の型が乱立していて、何の話をしているのか良く分からなくなる、という問題が発生します。

そこで個々のデータ型の説明をする前に、まずは全体の入れ子構造をここでしめしておきたいと思います。binder\_write\_read、binder\_transaction\_data、flat\_binder\_object は、以下のようないくつかの関係にあります。

8.4.1 ①

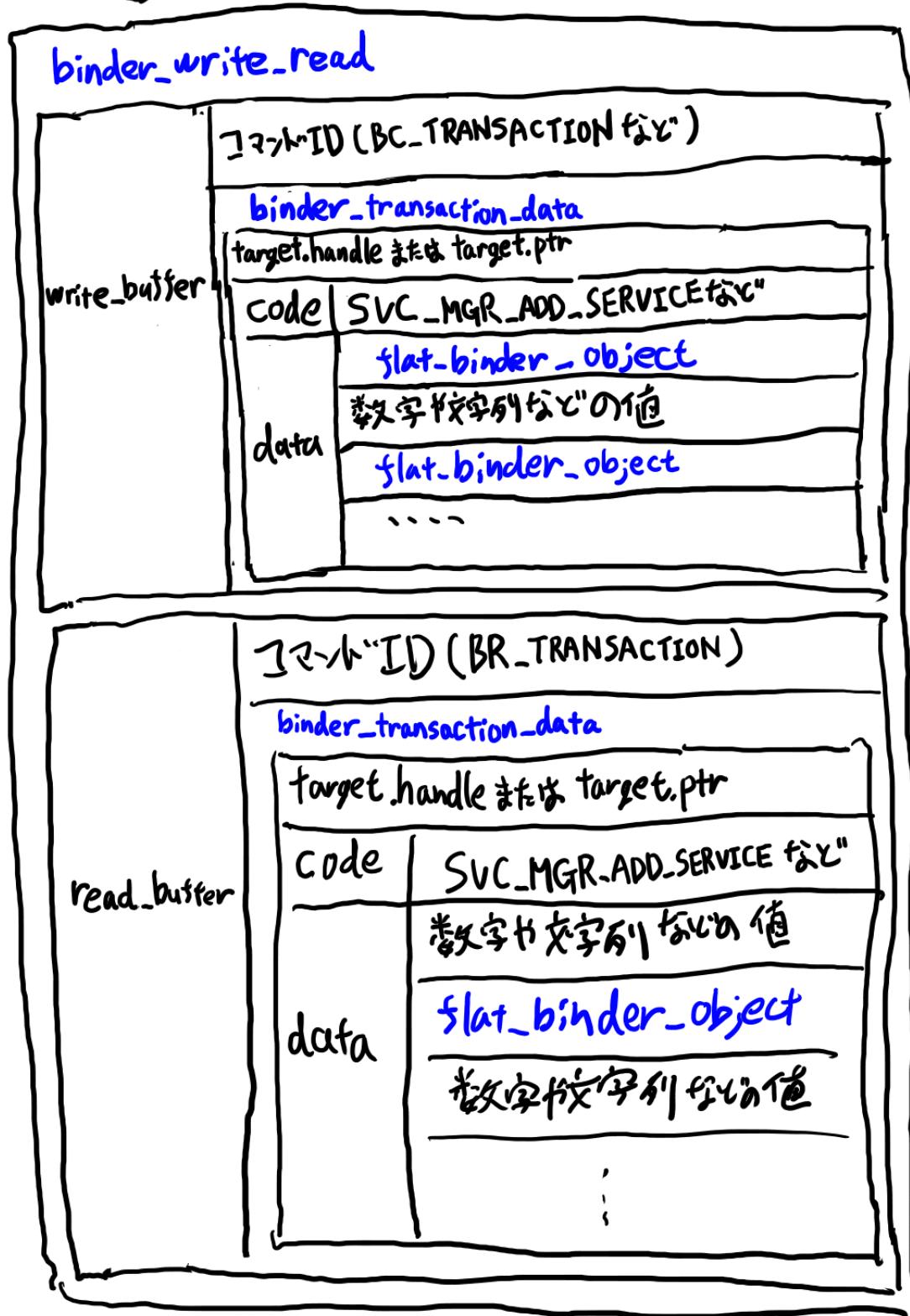


図 4.1 binder\_write\_read、binder\_transaction\_data、flat\_binder\_object の包含関係

以下の節でそれぞれの関係が良く分からなくなってきた時には、この図に戻ってきてみてください。

## 4.2 8.4.2 ドライバに書き込むデータのフォーマットとコマンド ID

ioctl を使って読み書きするデータは binder\_write\_read 構造体だと言いました。(8.3.4) 例えば以下のようなコードで初期化していました。

リスト 4.1: binder\_write\_read の write 側初期化、再掲

```
struct binder_write_read bwr;  
  
// write 関連初期化  
bwr.write_size = len;  
bwr.write_consumed = 0;  
// /* 1 */  
bwr.write_buffer = (uintptr_t) data;
```

ここで /\* 1 \*/ で data という変数のデータを詰めています。このデータの中身についての話をします。

このデータの先頭は、コマンド ID となっています。そして各コマンド ID に応じてその後に続くデータが決まります。

良く使うコマンド ID には以下の物があります。

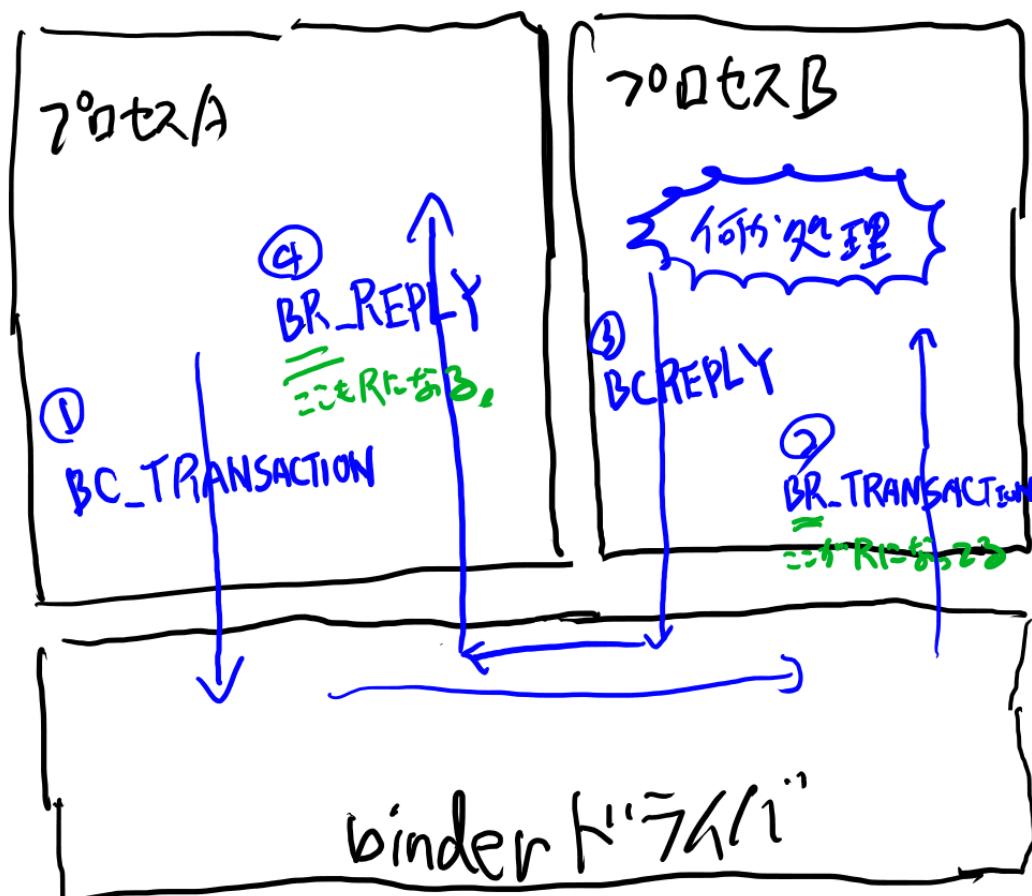
1. BC\_TRANSACTION
2. BC\_REPLY
3. BC\_ACQUIRE
4. BC\_RELEASE

一番大切なのが 1 の BC\_TRANSACTION です。これはよそのプロセスのメソッド呼び出しを行う時に使用するコマンドです。2 は上記のメソッド呼び出しに対する返信のコマンドです。

また、書き込む時と、書き込んだデータを読み込む時でコマンド ID の接頭辞が変わります。具体的には BC\_TRANSACTION を書き込むと、サービス側で読みだす時には BR\_TRANSACTION という ID になりますし、BC\_REPLY は BR\_REPLY に、BC\_ACQUIRE は BR\_ACQUIRE になります。

BC\_TRANSACTION して BC\_REPLY が返る様子を図にすると、以下のようになります。これが一つのメソッド呼び出しに対応します。

8.4.2①



トライバに送る時はいつも「BC-」で  
始まる。トライバから読む時はいつも「BR-」で  
始まる。またBC\_TRANSACTIONに対する返答はBC\_REPLY

図 4.2 BC が BR になり、TRANSACTION に REPLY が返る

コマンドの下二つに話を戻すと、BC\_ACQUIRE と BC\_RELEASE はハンドルのリファレンスカウントを上げたり下げたりする時に使います。ハンドルとは、メソッドを呼び出す相手や呼び手を表す物です。サービスのインスタンスの ID と言えます。ハンドルさえあれば、binder ドライバは対応するサービスのポインタを探す事が出来ます。

Binder の特徴の一つとして、最初から C++ やオブジェクト指向を前提としている、という物があります。そこでリファレンスカウントによるオーナーシップやメソッドという物が最初からある程度下のレイヤにも組み込まれています。具体的に言うとハンドルというインスタンスを指示するものがあったり、そのリファレンスカウントが、binder ドライバのレベルで存在している、という事です。

それでは以下、BC\_TRANSACTION について詳しく見ていきましょう。

### 4.3 8.4.3. BC\_TRANSACTION コマンドと binder\_transaction\_data

BINDER\_WRITE\_READ で ioctl を呼び出す時に書き込むデータのうち、先頭が BC\_TRANSACTION コマンド ID の場合、

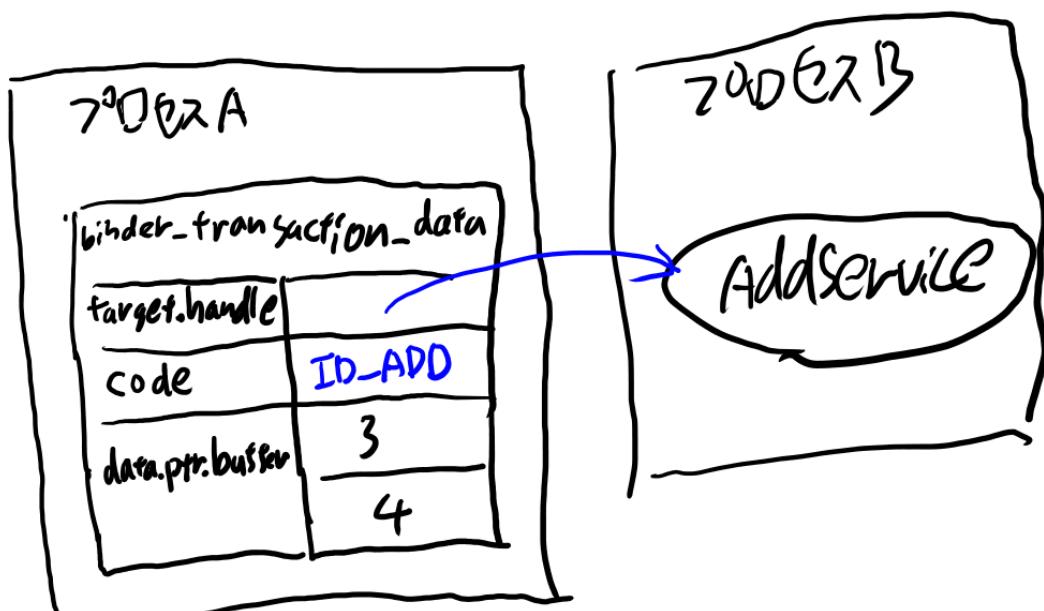
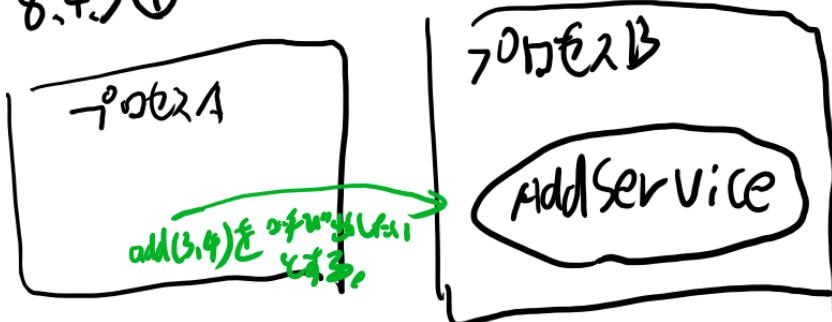
送るデータの中身は、コマンド ID の後に binder\_transaction\_data が続く事になっています。長さは sizeof(struct binder\_transaction\_data) です。

binder\_transaction\_data はメンバの多い構造体で全部説明するのは大変ですが主要な物だけ抜き出すと以下になります。

表 4.1 binder\_transaction\_data のフィールド

target.handle	やりとりをする相手を表すハンドル
code	どのメソッドかを表す ID
data.ptr.buffer	メソッドの引数のデータ領域をさすポインタ
data_size	メソッドの引数のデータの長さ

8.4.3 ①



`binder_transaction_data` はこうなる。

`target.handle`: 呼び出し元サービスのハンドル

`code` : 呼び出すドリ、トを表す int 値。サービスが決まる。

`data.ptr.buffer`: 引数が入る。`add(3,4)`を呼び出したいなら 3 と 4 がバイト配列に入る。

図 4.3 binder\_transaction\_data とメソッド呼び出し

メソッドを呼び出す相手、どのメソッドかを表す ID、そして引数のデータ（`data.ptr.buffer` と `data._size` はセットでデータ）という事で、これだけあると相手のメソッドを呼ぶ事が出来るのが分かると思います。

8.4.3 ②

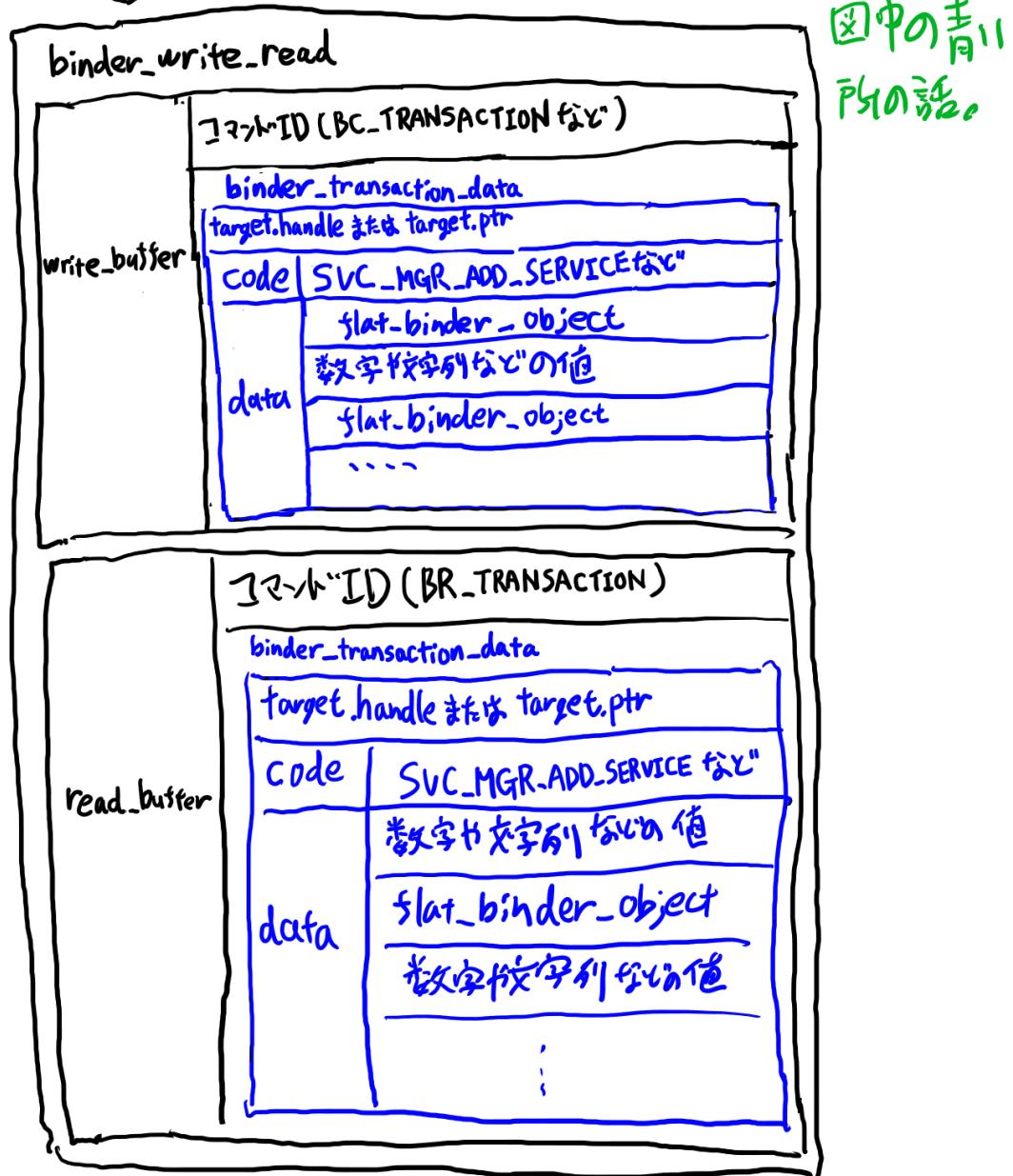


図 4.4 binder\_write\_read と binder\_transaction\_data の関係

引数のデータは先頭からベタにバイナリ値が書かれています。

書いた方と読んだ方で対応がとれていれば正しい値が取れる、という形式です。Parcel という utility クラスがシリализとデシリализに使えますが、ただ生のデータを読み書きするだけ

です。

code はメソッドを表す ID で、各サービスが勝手に決めます。

さて、あと表 4.1「binder\_transaction\_data のフィールド」の中で残っているのは target.handle だけです。この target.handle さえ分かればメソッドを呼び出す事が出来ます。そこで登場するのが servicemanager です。

#### 4.4 8.4.4 servicemanager によるサービスハンドルの取得

分散オブジェクトのシステムではオブジェクトを表す何らかの名前から、そのリファレンスを取る所が重要となります。一般にはそれをネーミングサービスと言いますが、Android の場合そのネーミングサービスに相当するのが servicemanager です。

servicemanager は特別なサービスです。サービスなので、上記の BC\_TRANSACT を送る事によって servicemanager のメソッドを呼び出す事が出来ます。ここまででは通常のサービスと変わりません。servicemanager が特別なのは、ハンドルが 0 番である事が最初から決まっている事です。

ですから、全てのクライアントは、最初から servicemanager のハンドルは知っている事になります。target.handle に 0 を代入すれば、それは servicemanager へのメソッド呼び出しだ、と解釈されます。こうして、どこからかハンドルを取得しなくとも、servicemanager へだけは BC\_TRANSACT を送る事が出来ます。

servicemanager のメソッドのうち、良く呼び出す物のメソッド ID の一覧を以下に載せます。

1. SVC\_MGR\_ADD\_SERVICE
2. SVC\_MGR\_CHECK\_SERVICE

1 がサービスとして登録するメッセージです。詳細は後述します。

2 の SVC\_MGR\_CHECK\_SERVICE で、サービスを名前で検索出来ます。SVC\_MGR\_GET\_SERVICE というメッセージもあって同じ処理をしていますが、SVC\_MGR\_CHECK\_SERVICE を使っているようです。

SVC\_MGR\_CHECK\_SERVICE の引数としては、"android.os.IServiceManager"という文字列と検索したいサービス名の二つです。

例えば SurfaceFlinger サービスのハンドルを検索したい場合の binder\_transaction\_data の作り方は以下のようになります。(重要な所だけ抜き出しています) 簡単のため Parcel というシリアルライザを使いますが、特に説明しなくともコードから何をやってるかは想像出来るでしょう(詳細は 8.6.2 でも扱います)。

リスト 4.2: Parcel を用いた binder\_transaction\_data の作り方

```
// binder_transaction_data のうち引数の所のデータを作る。  
// 作りたいのはベタのデータを書き込んだバイナリ配列だが、Parcel ユーティリティクラスを使って作る。  
Parcel writeData;  
  
// servicemanager のインターフェース名。ハードコードされた文字列  
writeData.writeString16(String16("android.os.IServiceManager"));  
  
// 探したいサービスの名前
```

```
writeData.writeString16(String16("SurfaceFlinger"));

// writeData が完成したので、次は binder_transaction_data を作る。
// BC_TRANSACTION で送るデータ。
struct binder_transaction_data tr;

// servicemanager のハンドルは 0 にハードコード
tr.target.handle = 0;

// 呼び出すメソッドの ID。
tr.code = SVC_MGR_CHECK_SERVICE;

// 引数には上で作った writeData を設定
tr.data_size = writeData.dataSize();
tr.data.ptr.buffer = writeData.data();
```

この binder\_transaction\_data 構造体のデータを binder ドライバに送りつけて、結果を取得すると、SurfaceFlinger サービスのハンドルが得られます。

このように、servicemanager という特別なサービスはハンドルが 0 と固定の値になっているので、クライアントのコードは最初から servicemanager に対してだけはメソッドを呼び出せます。そしてその servicemanager が全サービスの一覧を持っていて、その servicemanager にハンドルの検索を頼む訳です。

## 4.5 8.4.5 SVC\_MGR\_CHECK\_SERVICE を例に、ioctl呼び出しを復習する

以上で一通り servicemanager のメソッド呼び出しの解説を終えたのですが、復習も兼ねてこの binder\_transaction\_data を実際に送信するまでのコードも見てみましょう。内容としては 8.3.4 と同じ内容となります。以下、重要なコードだけを抜粋していきます。

まずは binder\_transaction\_data は BC\_TRANSACTION コマンドで送信するでした。BC\_TRANSACTION コマンドの送受信には binder\_write\_read 構造体を使い、これを ioctl に渡すでした。

そこで binder\_write\_read 構造体を用意します。まずは送信用のデータから。これはコマンド ID BC\_TRANSACTION と、先ほどの binder\_transaction\_data をバイト列に書き込んだ物になります。

リスト 4.3: binder\_transaction\_data を binder\_write\_read にセットする

```
// 送信用のデータのバッファ
byte writebuf[1024];
*((int*)writebuf) = BC_TRANSACTION
memcpy(&writebuf[4], &tr, sizeof(struct binder_transaction_data));
```

8.4.5 ①

writebuf

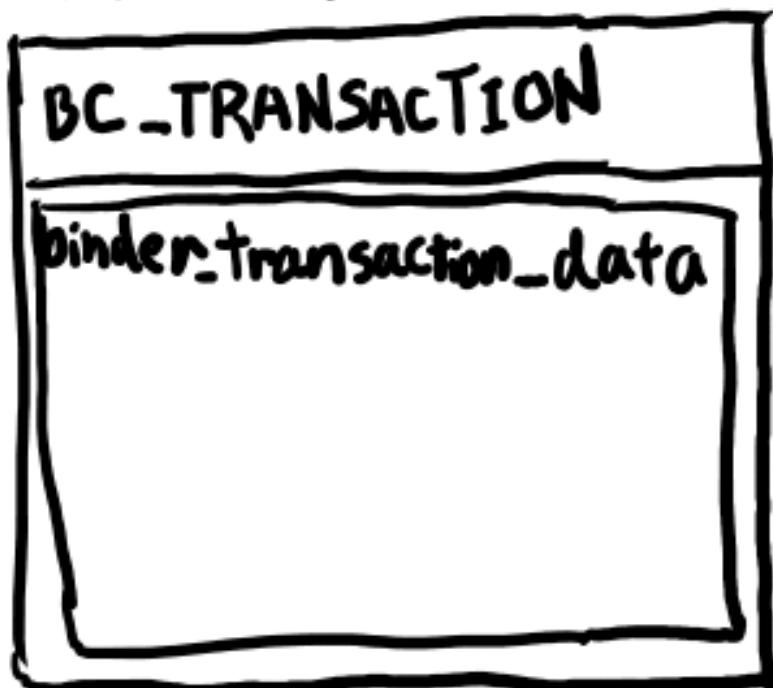


図 4.5 writebuf の中身

binder\_transaction\_data にはユーザー領域のデータへのポインタ、data.ptr.buffer が含まれるのですが、これはドライバ内で allocate してコピーしてくれます。

あとはこの送信用のデータを binder\_write\_read に設定して、受信用にはデータを受け取るバッファを設定し、ioctl を呼びます。

リスト 4.4: ioctl で結果を受け取る

```
// 結果受け取りのバッファ
byte readbuf[1024];

struct binder_write_read bwr;

// 送信用データ。長さはコマンド ID のサイズ +binder_transaction_data のサイズ
bwr.write_size = writebuf;
bwr.write_buffer = sizeof(int)+sizeof(struct binder_transaction_data);

// 受信用バッファ
bwr.read_size = 1024;
bwr.read_buffer = readbuf;

// ioctlでservicemanagerのSVC_MGR_CHECK_SERVICEを呼び出す
res = ioctl(fd, BINDER_WRITE_READ, &bwr);
```

### 8.4.5②

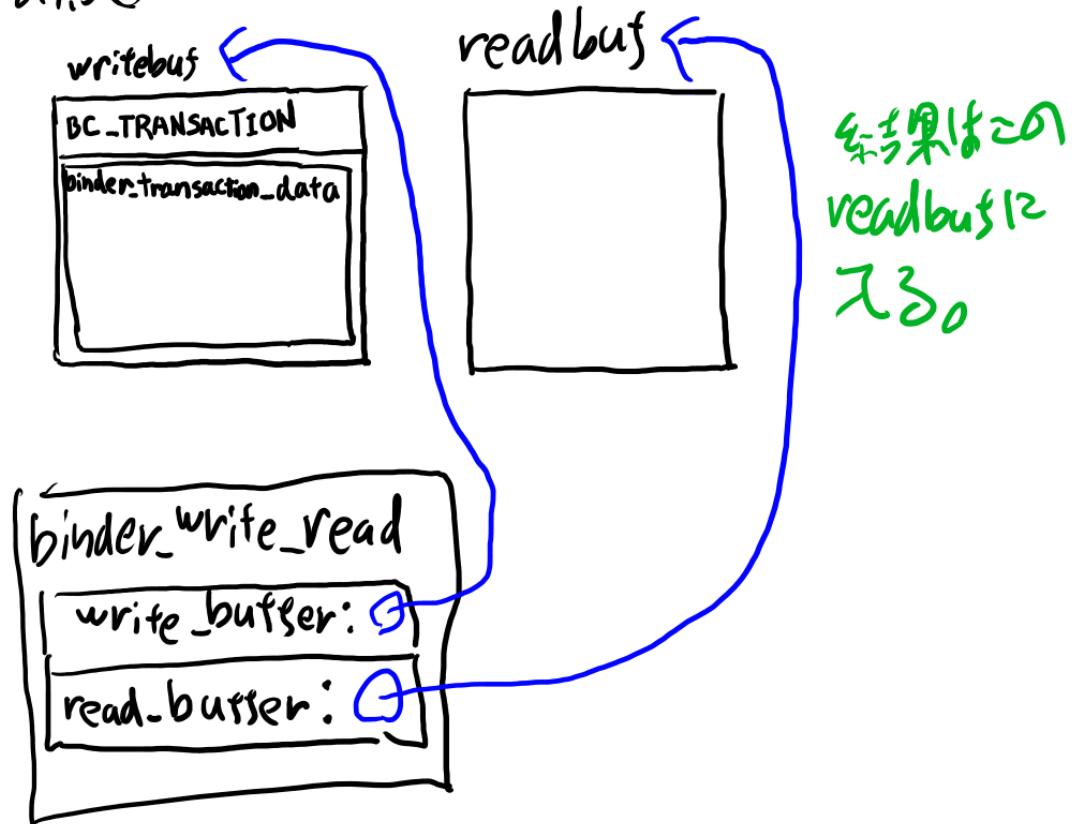


図 4.6 binder\_write\_read の writebuf と readbuf

最初の writeData が `binder_transaction_data` に入り、それが `writebuf` に入って

buffer\_write\_read 構造体に入る、という 4 段階の入れ子になっているのでややこしいですが、一つ一つの処理はかなり単純です。

このコードを実行すると、binder ドライバはこのスレッドを一旦止めて、servicemanager のスレッドを起こしてこの binder\_transaction\_data を渡して処理させ、その結果を受け取ってから元の呼び出しのスレッドを起こして ioctl から返ります。

結果は bwr.read\_buffer に入ります。

では次にこの結果がどういう物か、典型的な処理を見る事で見ていきましょう。

## 4.6 8.4.6 サービスハンドルの取得の結果 - メッセージ受信

ioctl を用いたメソッド呼び出しの結果は、binder\_write\_read 構造体の read\_buffer に書かれます。書かれたデータの長さは bwr.read\_consumed に入れます。

read\_buffer には先頭の 4 バイトに戻りのコマンド ID が、それ以後にそのコマンドの付随データが入ります。送信の側と同じですね。

BC\_TRANSACTION の結果が正常に返る場合のコマンドは、BR\_REPLY と決まっています。その後に付随するデータは binder\_transaction\_data で、送信時と同じです。

そしてその binder\_transaction\_data の data.ptr.buffer の中には flat\_binder\_object 構造体というのが入っています。

この構造体はサービスのハンドルやサービスのプロセスの場合はサービス自身のポインタ、そしてファイルディスクリプタなどを保持できるオブジェクトです。

今回のケースでは、この構造体の中にハンドルが入っています。

8.4.6 ①

readbuf

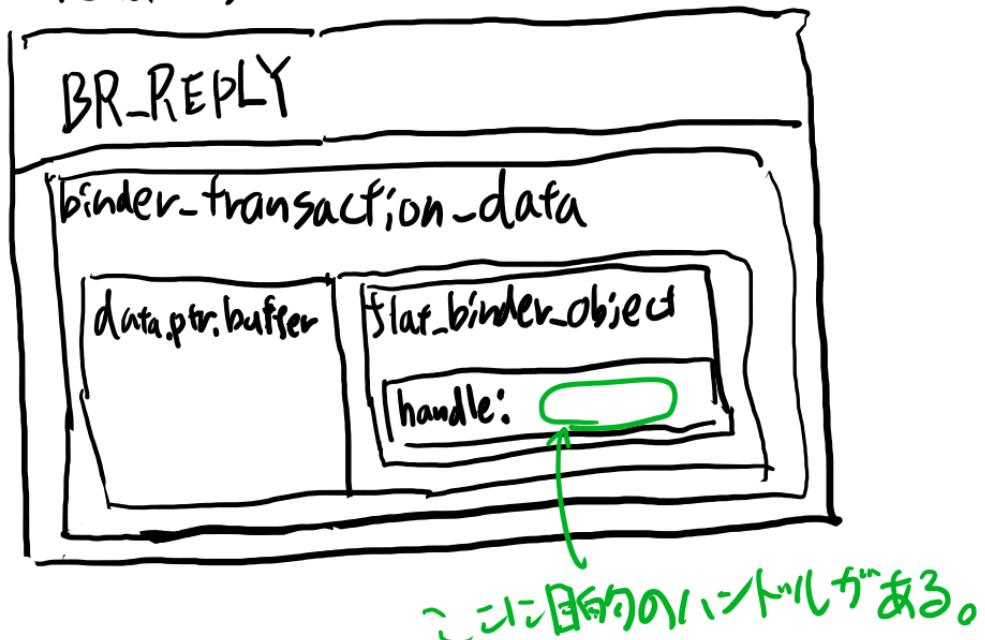


図 4.7 読み出したバッファの構造

8.4.5 のコードの続きとしては以下のようなコードでこのハンドルが取れます。

リスト 4.5: 読みだしたバッファから binder\_transaction\_data を取り出す

```
// /* 1 */ 先頭 4 バイトはコマンド ID
int cmd = *((int*)readbuf);

// BC_TRANSACTION のリプライは正常時は BR_REPLY
assert(cmd == BR_REPLY);

// /* 2 */ BR_REPLY の後続データも binder_transaction_data 型
struct binder_transaction_data tr_res;
memcpy(&tr_res, &reabuf[4], sizeof(struct binder_transaction_data));

// /* 3 */ binder_transaction_data 型には flat_binder_object のデータが入っている
struct flat_binder_object *obj;
obj = (struct flat_binder_object*)tr_res.data.ptr.buffer;

// /* 4 */ handle は flat_binder_object の中の handle フィールドに入っている
int handle = obj->handle;
```

少し細かいコードになりますが、このように

1. コマンドを取る（今回のケースでは使いませんが）
2. binder\_transaction\_data を取り出す
3. その中から flat\_binder\_object を取り出す
4. その中の handle フィールドに目的のサービスハンドルが入っている

という手順になります。なお、/\* 3 \*/で flat\_binder\_object という物が登場しましたが、これについては次節で詳細に扱います。

こうして目的のサービスのハンドルを取得したら、以後はこのようにして得たハンドルに対して 8.4.4 で説明したのと同様なコードで、指定したサービスのメソッドが呼び出せます。

ここで解説したコードはサービスのハンドルの取得時の受信した後のコードですが、メッセージ受信全般でほとんど同じ構造のコードとなります。

ioctl は binder\_write\_read 構造体の write\_size を 0 にして呼び出すと、呼び出し時点でブロックしてメッセージが来るのを待ちます。

サービスの実装側では、この受信としての ioctl 呼び出しでブロックしてメッセージが来るのを待ち、メッセージがやってくるとこの ioctl から帰ってくるので binder\_write\_read の read\_buffer から、先ほど解説したサービスハンドルの取得と同じような手順でコマンド ID を読み出し、コマンド ID に応じた処理を行います。

さて、ioctl を使うコードとしては以上でだいたいの説明が終わりです。以下では実装側に目をうつし、ioctl の内で何が起こっているのかをもう少し詳しく見ていきましょう。

## 第5章

# {flat\_binderobj} 8.5 binder ドライバ の内側とオブジェクトの送信 - `flat_binder_object`

前節では、servicemanager でサービスを検索する例を通じて、binder ドライバを利用して引数が文字列のみの簡単なメソッドを呼び出す手順を見てきました。

さて、サービスを検索するには、サービスが既に登録されていないといけません。そこで次の話題としては当然、このサービスをどう登録するか、という事に移る訳ですが、サービスを登録するのは、サービスを検索するよりも、一つだけ難しい所があります。それは引数にサービスというオブジェクトが含まれてしまう、という事です。

サービスというオブジェクトを含んだ引数をどのように扱うか、というのが本節の主要なテーマとなります。その為には binder ドライバ内部で様々なデータをどう管理しているのか、という事を知る必要があります。

binder ドライバ内部のデータ管理は、カーネルのメモリ空間で行われるカーネルモードでの話となります。

### 5.1 8.5.1 オブジェクトを送信すると何が起こるか？

詳細に入る前に、オブジェクトを送信すると何が起こるのか？ という事の概要から始めたいと思います。

オブジェクトというのはメソッドという処理が含まれるので、転送する事が出来ません（少なくとも Binder では転送されません）。ここで例示の為に、オブジェクトの存在しているプロセスをプロセス A と呼び、それを送りつける先をプロセス B とします。

プロセス A からオブジェクトをドライバに渡すと、ドライバがこのオブジェクトのポインタを覚えておきます。そしてプロセス B には、このポインタを表すハンドルを渡します。B にはオブジェクトを転送される訳では無くハンドルが渡されるのですが、ここでプロセス A 内のポインタがドライバに保持される、というのが工夫です。

## 第5章 {flat\_binderobj} 8.5 binder ドライバの内部とオブジェクトを送信するとき何が起こるか

---

ポインタという物は概念的にはそのプロセスのアドレス空間内のアドレスです<sup>\*1</sup>ですからプロセス A のポインタはプロセス A のアドレス空間上でないと有効ではありません。ですがアドレスをドライバが記憶する事は出来ます（そのアドレスの中身を参照するのはちょっと大変ですが）。

そしてプロセス B がハンドルに対してメソッド呼び出しをしたら、それをプロセス A に転送するのですが、この時は記憶したポインタのアドレスも戻してやる訳です。プロセス A の ioctl から戻った時というのは、アドレス空間はプロセス A の物となっているので、このポインタはそのまま有効で、以前送信の時に引数で渡したポインタとなっている訳です。

---

<sup>\*1</sup> ARM の場合厳密にはそれを参照するためのディスクリプタですが、この場合の議論は等しく有効です。

8.5.1 ①

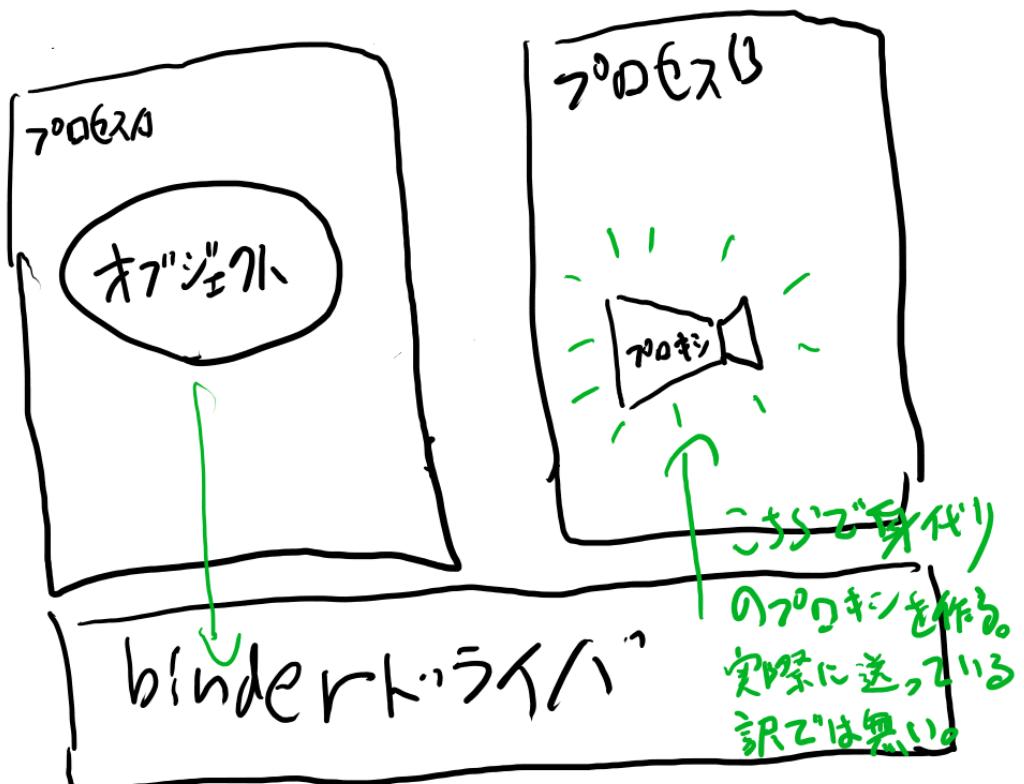
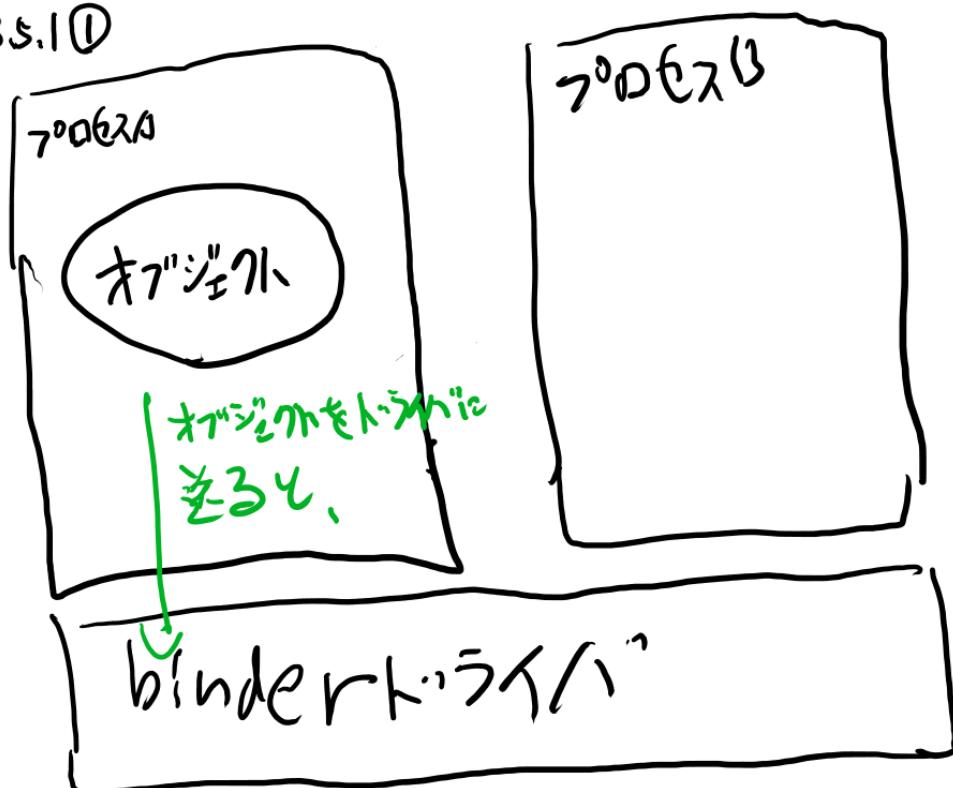


図 5.1 オブジェクトを送ると、プロキシが作られる

### 8.5.1②

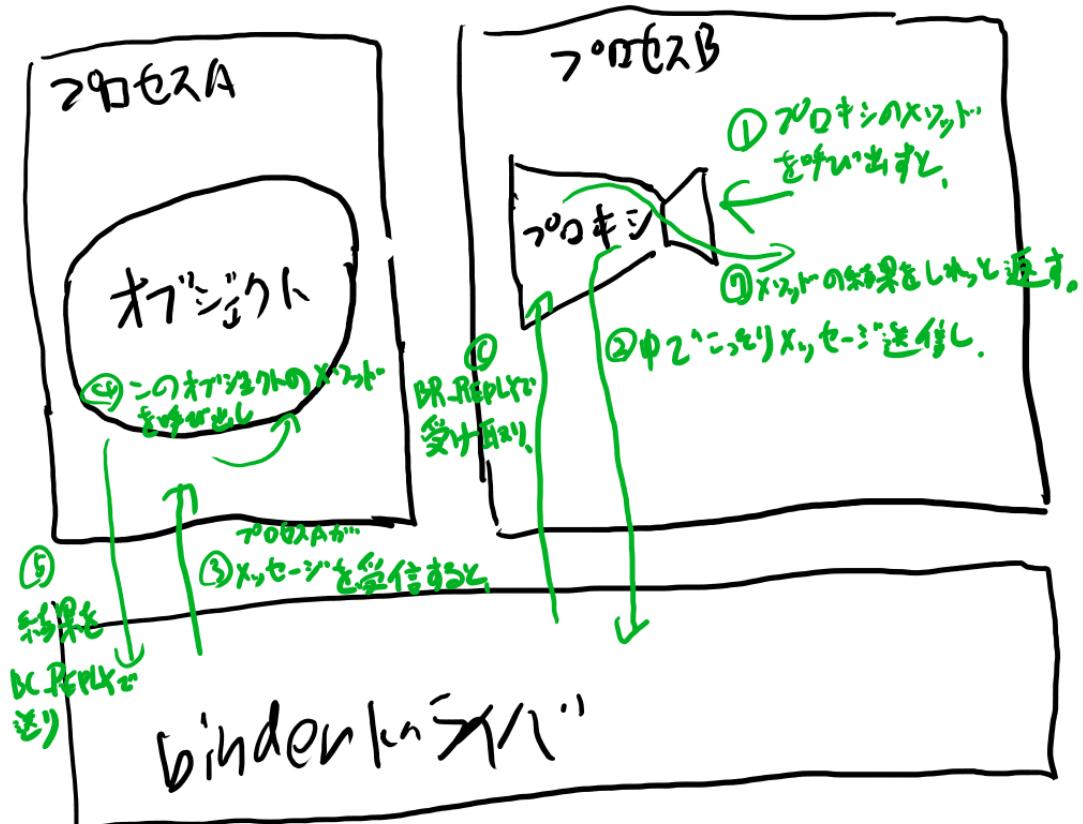


図 5.2 プロキシのメソッドを呼ぶとオブジェクトが呼ばれるメカニズム

つまり、オブジェクトは転送されません。プロセス A からオブジェクトを転送しようとしてもドライバの所で記憶されるだけで、実体はプロセス B には行かないのです。でも身代わりとしてハンドルというのが代わりに届く事になります。

これがオブジェクトを送信する時に起こる事のイメージです。

## 5.2 8.5.2 スレッドとプロセスのデータ構造 - binder\_proc と binder\_thread

binder ドライバは、binder ドライバを使用するプロセスに関する情報を、binder\_proc というデータ構造で管理しています。これはドライバを open した時にカーネルによって作られる file 構造体のフィールドに格納されます。ユーザープロセスの側から見れば、binder ドライバを open した時に返るファイルディスクリプタに格納されています。ファイルディスクリプタは ioctl 呼び出しの

第一引数で渡し続けるので、この binder\_proc もプロセス内で同じインスタンスが毎回ドライバに渡されます。@##@ TODO: 図と説明でファイルオブジェクトが open の都度作られる前提で書いているが後で本当にそうか確認。

また、スレッドを表すデータ構造もあります。binder はメソッド呼び出しを前提としたプロセス間通信です。メソッド呼び出しが単なるメッセージングと違うのは、結果が返る、という所です。

メソッド呼び出しを成立させるためには、BC\_TRANSACTION と BC\_REPLY の二つの ioctl 呼び出しが必要です。そして BC\_REPLY を送る時には対応する BC\_TRANSACTION を送ってきたスレッドに送信しないと、結果が呼び出したスレッドに返りません。つまり、BC\_TRANSACTION を受け取る側が処理をしている間、送信元のスレッドを覚えておく必要があります。<sup>\*2</sup>

そこで binder ドライバは、ioctl を呼び出される都度、呼び出しスレッドに対応するデータ構造を作成して管理します。このスレッドを表す構造体は binder\_thread という名前です。binder\_thread は binder\_proc にツリーとして保持されます。<sup>\*3</sup>

---

<sup>\*2</sup> BC\_REPLY の時には target の指定は必要ありません。binder ドライバが自動的に探してくれます。

<sup>\*3</sup> Linux カーネルが提供している赤黒木で保持されます。

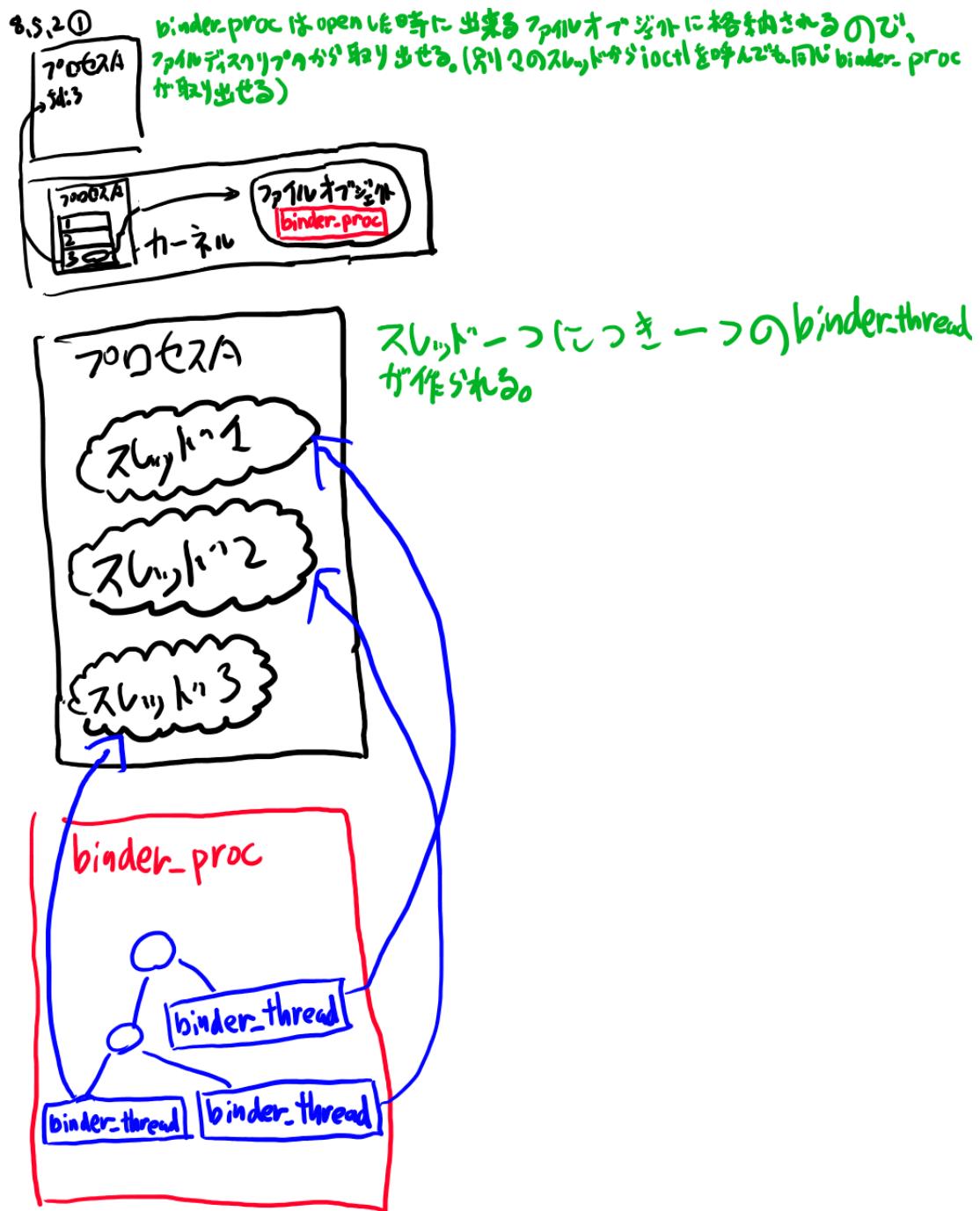


図 5.3 binder\_proc と binder\_thread

ioctl が呼ばれる都度、呼び出し元のスレッド ID を見て、そのスレッド ID に対応するスレッド構造体が、プロセス構造体に既に入っているかを検索します。無ければ新たに生成してツリーに追加します。このように、スレッド構造体は ioctl を呼び出す都度 lazy に、しかも暗黙に作られます。

こうして、ioctl を呼び出している各スレッドをドライバが管理しているので、

`BR_TRANSACTION` を呼び出されている側のユーザープロセスが処理している間は、呼び出し元のスレッド情報をドライバが覚えておいてくれるので、その後に `BC_REPLY` をドライバに送ると、自動的に呼び出し元のスレッドを探し出してそのスレッドに返してくれます。

8.5.2(2)

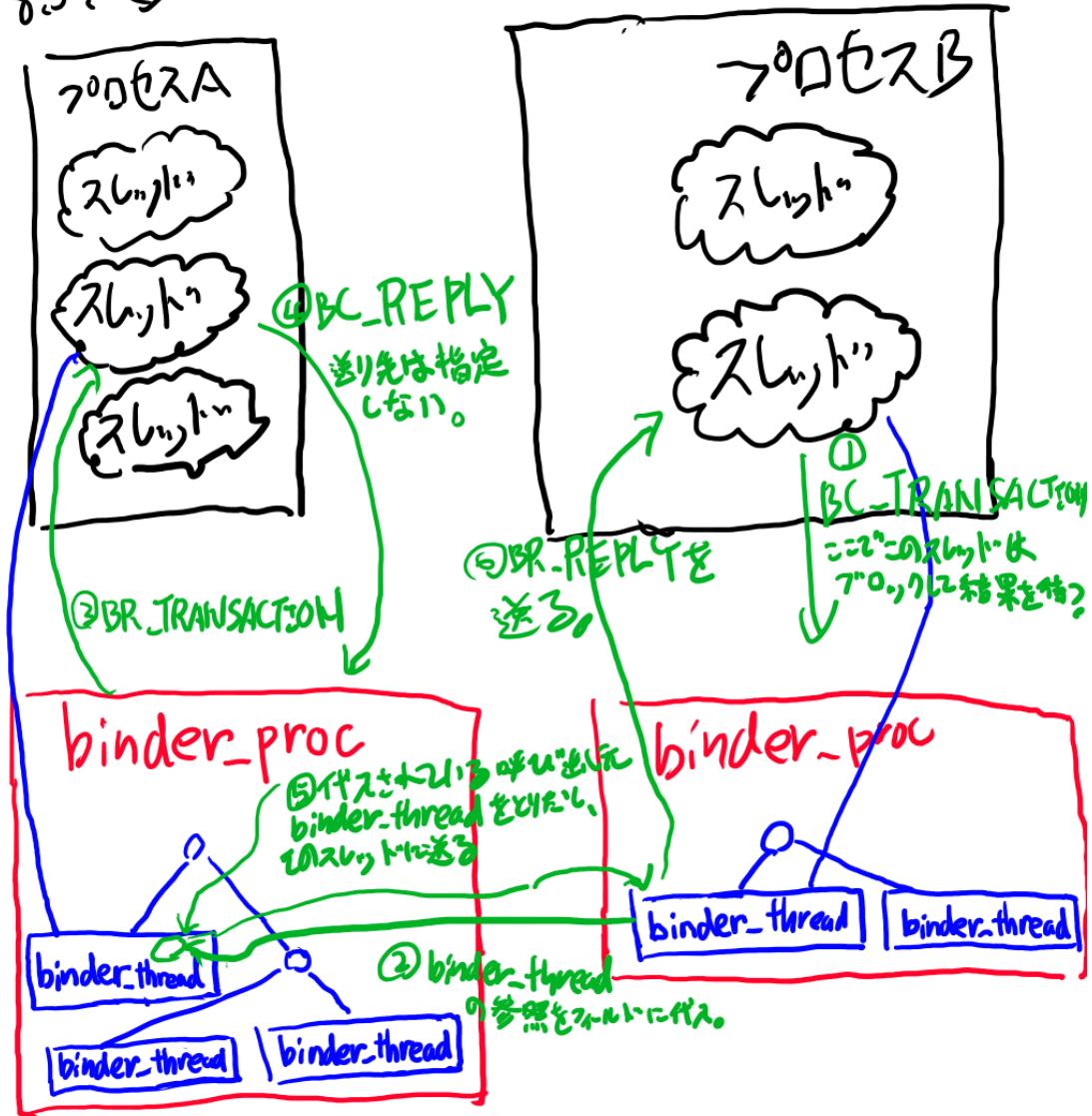


図 5.4 binder\_thread に REPLY 先を記憶する

コラム: プロセス構造体という呼び名と `binder_proc`

Linux カーネルでは、プロセス構造体と言う物があります。この本以外の本では、プロセス構造体と単に言ったら、この Linux カーネルのプロセス構造体を指すのが普通です。そ

して binder ドライバが持つプロセスのデータを表す構造体は、区別する為に構造体名である binder\_proc と呼ぶのが普通でしょう。ですが、本章ではプロセス構造体と言ったら binder\_proc を指します。これは、この binder ドライバの周辺にはプロセス構造体の他にも大量の構造体名が出てくる為、覚えなくてはならない構造体名を一つでも減らす為の工夫です。私も初めてこの周辺を読んだ時は構造体名が多すぎて、すぐにどの構造体名が何だったのかを忘れてしまい苦労しました。幸い、本章では Linux カーネルのプロセス構造体に言及する必要は無いので、どちらか分からなくなる事は無いはずです。もし Linux カーネルに詳しいが為にかえってこの工夫がややこしい、という方が居たら、心の中でこの章のプロセス構造体、という言葉を全部 binder\_proc に置き換えて読んでください。====[/column]

### 5.3 8.5.3 オブジェクトの送信と flat\_binder\_object その 1 - ユーザー プロセス 側

メソッド呼び出しの引数としてオブジェクトを渡す場合の話に入ります。

オブジェクトというのは生のポインタです。そのプロセス内のメモリ空間でだけ意味があります。この生のポインタを binder ドライバに渡すと相手側ではハンドルとして渡ってきます。

まずは生のポインタが存在しているプロセス側で、送信する時のコードを見てみましょう。

binder ドライバに生のポインタを渡す場合は、flat\_binder\_object 構造体に入れて渡します。

サービスの取得の所、つまり受け取る側でも、結果は flat\_binder\_object 構造体として返ってくる、という事を説明しました。(8.4.6) 送る側もこの flat\_binder\_object という構造体を使います。flat\_binder\_object には型を表すフィールドがあり、そこには大きく三つの値が入ります。

1. BINDER\_TYPE\_BINDER
2. BINDER\_TYPE\_HANDLE
3. BINDER\_TYPE\_FD

1 がポインタ、2 がハンドル、3 がファイルディスクリプタです。

たとえば handle という変数に入ったハンドルの値を保持する flat\_binder\_object は以下のように作れます。

リスト 5.1: flat\_binder\_object にハンドルを入れる場合

```
flat_binder_object obj;
obj.type = BINDER_TYPE_HANDLE;
obj.handle = handle;
```

ptr というポインタ変数に入ったポインタを保持する flat\_binder\_object なら以下のようになります。

リスト 5.2: flat\_binder\_object にポインタを入れる場合

```
flat_binder_object obj;
obj.type = BINDER_TYPE_BINDER;
obj.binder = ptr;
```

8.5.3 ①

flat_binder_object	
type	BINDER_TYPE_BINDER
handle	ポインタ
binder	

flat_binder_object	
type	BINDER_TYPE_HANDLE
handle	サービスのハンドル
binder	

flat_binder_object	
type	BINDER_TYPE_FD
handle	ファイルディスクライプタ
binder	

flat\_binder\_objectで送るのは、①ポインタ②ハンドル③ファイルディスクライプタの3つ

図 5.5 flat\_binder\_object で送れる物三つ

基本的にはこの flat\_binder\_object を引数を表すバッファに入れて少し補助的な設定をした上で ioctl を呼べば良い、という事になります。引数というのは binder\_transaction\_data の ptr.buffer に入る、という話を 8.4.3 で行いましたが、いろいろな場所に説明が飛ぶと読む方も大変だと思うので、一部繰り返しになりますがもう一度ここで全体像を見てみましょう。

サービスの servicemanager への登録を例として、オブジェクトの送信を見てていきます。MyService というクラスをサービスとして登録する場合を見ていきます。サービス名は"com.example.MyService"とします。

servicemanager はハンドルが 0 という固定値でした。この 0 というハンドルに BC\_TRANSACTION で SVC\_MGR\_ADD\_SERVICE というメソッドを呼び出すことで、サービスの登録を行えます。(8.4.4)

SVC\_MGR\_ADD\_SERVICE は、引数として以下の三つを受け取ります

1. String16 型の"android.os.IServiceManager"という固定文字列
2. String16 型のサービス名、この場合は"com.example.MyService"
3. サービスのポインタ

1 番目と 2 番目は適当なバイト配列に memcpy してやれば良い訳です。3 は flat\_binder\_object にオブジェクトのポインタを詰めて、それを memcpy してやれば良いのですが、flat\_binder\_object の時にはもう一つ、オフセットの指示という作業が追加で必要となります。というのは、それ以外の値は全てドライバとしてはバイト列をコピーするだけで良いので中を知っている必要は無いのですが、flat\_binder\_object だけはドライバが変換するので、中身を知っている必要があるのです。

まずはバイト配列を生成し、二つの固定文字列をバイト配列にコピーします。詳細は省略します。

リスト 5.3: バイト配列に二つの文字列をコピー

```
byte writedata[1024];
// "android.os.IServiceManager"のString16をwritedataにmemcpyする。省略
...
```

```
// "com.example.MyService"のString16をwritedataにmemcpyする。省略
```

次に flat\_binder\_object を memcpy します。まずは flat\_binder\_object の作成から。

リスト 5.4: バッファにコピーする flat\_binder\_object を生成

```
// MyService のインスタンスを生成
MyService *service = new MyService;

flat_binder_object obj;
// ポインタの時はタイプは BINDER_TYPE_BINDER
obj.type = BINDER_TYPE_BINDER;
// obj.binder にポインタを入れる
obj.binder = service;
```

このように flat\_binder\_object という物を作つて、writedata に memcpy します。なお、文字列二つを memcpy した時に used バイトまで既に使つたとします。<sup>\*4</sup>

リスト 5.5: 生成した flat\_binder\_object をバイト配列にコピー

```
// flat_binder_object を writedata の used バイトより先に書き込む。
memcpy(&writedata[used], &obj, sizeof(flat_binder_object));

// 後で使うので used を進めておく。
used += sizeof(flat_binder_object);
```

こうして出来た writedata を 8.4.4 と同様に binder\_transaction\_data に入れて、それを 8.4.5 と同様に binder\_write\_read に入れれば良い訳ですが、flat\_binder\_object を渡す時は先ほども述べた通り、さらにオフセットの指定という事もやらなくてはいけません。

<sup>\*4</sup> used の実際の値は  $4 + 2 * \text{sizeof}(\text{"android.os.IServiceManager"}) + 4 + 2 * \text{sizeof}(\text{"com.exmaple.MyService"})$  ですが、詳細を気にする必要は無いでしょう。

第5章 {flat\_binder} と {flat\_binder} の送信の内側と外側の object の送信 1. flat\_binder 内側

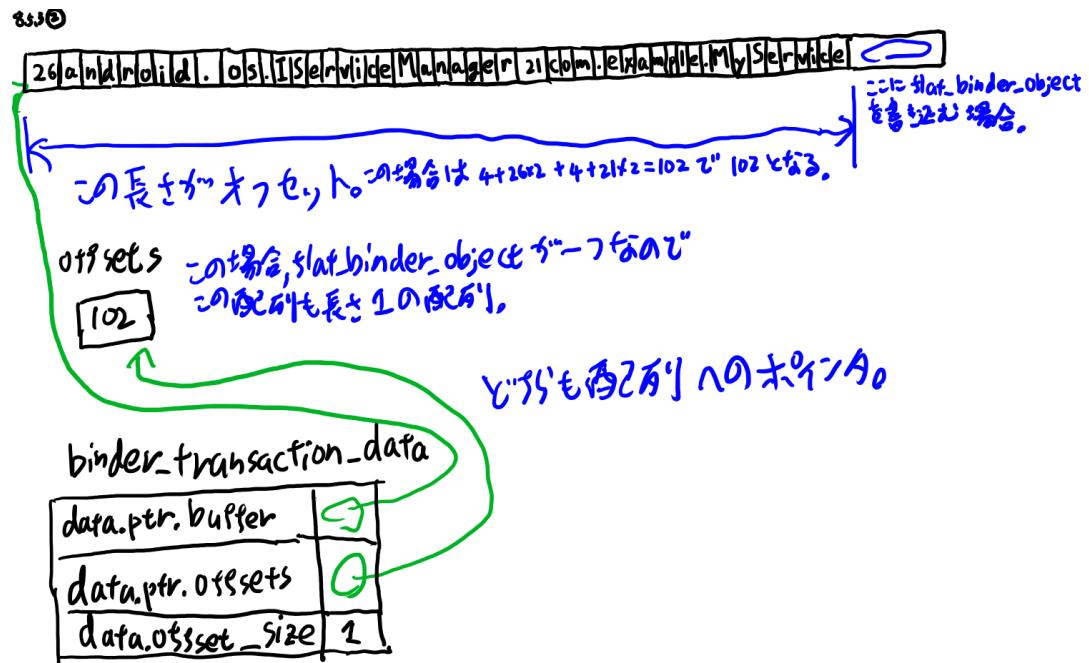


図 5.6 flat binder object とオフセットの書き方

一気に三つの事が説明に出てきたので、一つずつ見てていきましょう。

まずは `binder_transaction_data` に上で作った `writedata` やターゲットとなるハンドル等を設定します。

リスト 5.6: binder transaction data に送り先のハンドルを指定し、ここまで作ったバッファをセット

```
// binder_transaction_data の設定
struct binder_transaction_data tr;

// servicemanager のハンドルは 0 にハードコード
tr.target.handle = 0;

//呼び出すメソッドの ID。今回はサービスの登録なので ADD_SERVICE。
tr.code = SVC_MGR_ADD_SERVICE;

//引数には上で作った writedata を設定
tr.data_size = used;
tr.data.ptr.buffer = writedata;
```

送り先が0、メソッドIDがSVC\_MGR\_ADD\_SERVICE、引数がwritedata、という訳です。さらにこの引数データの中で、どこにflat\_binder\_objectがあるか、という情報も追加してやります。

リスト 5.7: `binder_transaction_data` の引数の中のうち、どこが `flat_binder_object` かを表す offset を指定

```
// offsets として、今回は送り出すデータの中には flat_binder_object は一つなのでサイズは 1
size_t offsets[1];
// flat_binder_object をどこに書いたか。最後の引数なので末尾から sizeof(flat_binder_object) だけ戻った所にあるはず。
offsets[0] = used - sizeof(flat_binder_object);

// offsets は、今回は長さ 1 の配列
tr.data.offset_size = 1;

// 上で設定した offsets を代入
tr.data.ptr.offsets = offsets;
```

binder ドライバにこの ptr.buffer の中のこことここに変換の必要のある flat\_binder\_object が入っているよ、と伝える為に、offsets というメンバと offset\_size というメンバを設定します。offsets は size\_t の配列で、各要素が flat\_binder\_object が ptr.buffer の先頭からのオフセットに対応します。offset\_size は offsets 配列の長さです。

このようにして設定した binder\_transaction\_data を buffer\_write\_read に詰めて BC\_TRANSACTION として ioctl を呼び出します。

以後は前に説明したサービス取得のコードと全く同じコードになりますが、再掲しておきます。

リスト 5.8: 再掲: サービス取得のコード

```
// 送信用のデータのバッファ。コマンド ID と先ほど作った binder_transaction_data を詰める。
byte writebuf[1024];
*((int*)writebuf) = BC_TRANSACTION
memcpy(&writebuf[4], &tr, sizeof(struct binder_transaction_data));

// 結果受け取りの為の受信用バッファ
byte readbuf[1024];

// binder_write_read に送信用と受信用のバッファを設定
struct binder_write_read bwr;

// 送信用データ。長さはコマンド ID のサイズ +binder_transaction_data のサイズ
bwr.write_size = writebuf;
bwr.write_buffer = sizeof(int)+sizeof(struct binder_transaction_data);

// 受信用バッファ
bwr.read_size = 1024;
bwr.read_buffer = readbuf;

// ioctl で servicemanager の SVC_MGR_ADD_SERVICE を呼び出す
res = ioctl(fd, BINDER_WRITE_READ, &bwr);
```

このようにすると、MyService という生のポインタを引数にして、servicemanager にサービスを登録する、というメソッドを呼び出した事になります。それではこの生のポインタが binder ドライバではどう扱われて servicemanager 側に渡るのか？ という部分を見ていきましょう。

## 5.4 8.5.4 オブジェクトの送信と flat\_binder\_object その 2 - binder ドライバと受信側

ioctl 呼び出しの時に flat\_binder\_object を渡すと、ドライバは内部で flat\_binder\_object の中身の種類に合わせて適切に変換し、送り先に送ります。

BINDER\_TYPE\_BINDER のポインタは呼び出し元のメモリ空間でしか有効で無いので、このポインタを渡されても別のプロセスは困ってしまいます。

8.5.2 で解説したように、binder ドライバを open した時のファイルディスクリプタには、そのプロセスの構造体が格納されています。

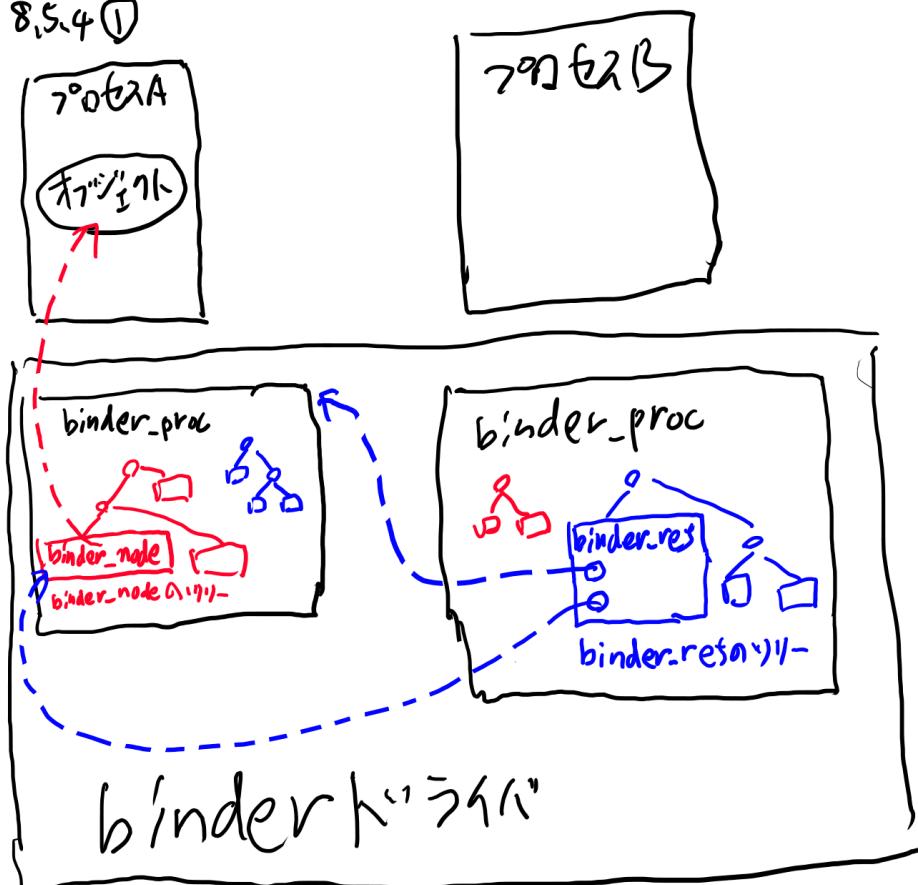
そしてこのプロセス構造体には、そのプロセスが保持する BINDER\_TYPE\_BINDER のポインタを格納するツリーがあります。このツリーのノードを、binder\_node と呼んでいます。ツリーになっているのは高速に検索する為です。<sup>\*5</sup>

あるプロセスが保持しているサービスのポインタの一覧がツリーで管理されていると言いました。さらに、そのプロセスが参照している外部のサービスの一覧もツリーで管理されています。これは binder\_ref というノードの表すツリーです。このツリーのノードで、参照しているサービスが表されます。binder\_ref のフィールドには、参照しているサービスが所属しているプロセス構造体と、そのプロセス構造体にある BINDER\_TYPE\_BINDER のポインタを参照する binder\_node が格納されます。

---

<sup>\*5</sup> これも Linux カーネルの提供する赤黒木となっています。

8.5.4 ①



binder\_nodeは自身のプロセスのポインタに対する所。  
binder\_resは参照している別のプロセスのポインタに対応。

図 5.7 binder\_ref が参照している物

別の角度から同じ事を説明してみましょう。別のプロセスに BINDER\_TYPE\_BINDER のポインタを渡す時を考えます。ポインタが所属しているプロセスを A、送り先のプロセスを B とします。

8.5.4(2)

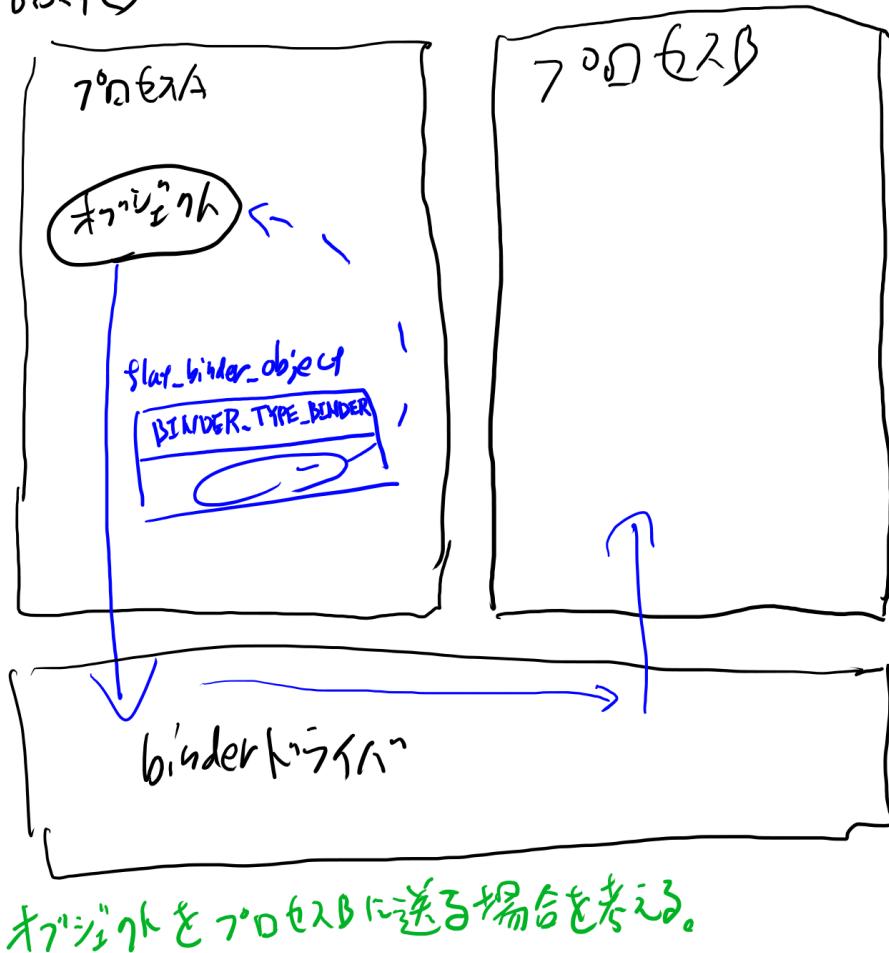


図 5.8 問題設定。オブジェクトを B に送信したい。

その時には、以下の事が起こります

1. A のプロセス構造体の binder\_node ツリーに、このポインタを表すノードを追加してポインタを格納
2. B のプロセス構造体にこのポインタへの参照を表す binder\_ref のノードを追加し、1 のノードと A のプロセス構造体を追加
3. B の binder\_ref のツリーのノードに一意の int の ID を振って、その ID をハンドルとしてプロセス B に渡す

この 3 のハンドルこそが、サービスの取得の時に得られた BINDER\_TYPE\_HANDLE の flat\_binder\_object に格納されていた、そして binder\_transaction\_data の target.handle に格納する、そして servicemanager は 0 とハードコードされているハンドルです。

binder\_ref とハンドルの関係はちょっとわかりにくいですが、binder\_ref のノードに順番に 1 から自然数の ID を振っていて、その ID がハンドルだ、というとだいたい正しい説明となります。「だいたい正しい」というのは、途中でノードを削除したりすると抜け番が出来て、新しくノードを作る時にはそれを再利用する処理がある為です。とにかく、binder\_ref のノードを一意に識別する int 値がハンドルです。

ハンドルは binder\_ref のノードを引くキーと言えます。内部実装を忘れれば、ハッシュのような物に格納されていて int のキーで lookup 出来ると思っておいて問題ありません。そしてそのキーがハンドルという訳です。<sup>\*6</sup>

B のプロセス内でのこのハンドルは、このプロセス B でのみ有効な int 値です。この値があれば、B のプロセス構造体から素早く binder\_ref を検索できます。そして binder\_ref の中を見ると、このサービスを所持しているプロセス構造体と、このサービスのポインタを所持している binder\_node が得られます。

以上が A から B を呼び出した場合です。

これを逆の順序で見ていくと、B からこのハンドルに対して BC\_TRANSACTION した時に何が起こるのかが分かります。B から A を呼び出す事を考えましょう。

---

<sup>\*6</sup> 厳密には内部ではポインタによる赤黒木とハンドル値による赤黒木の二本の木を持つ事でこの構造を実現しています。

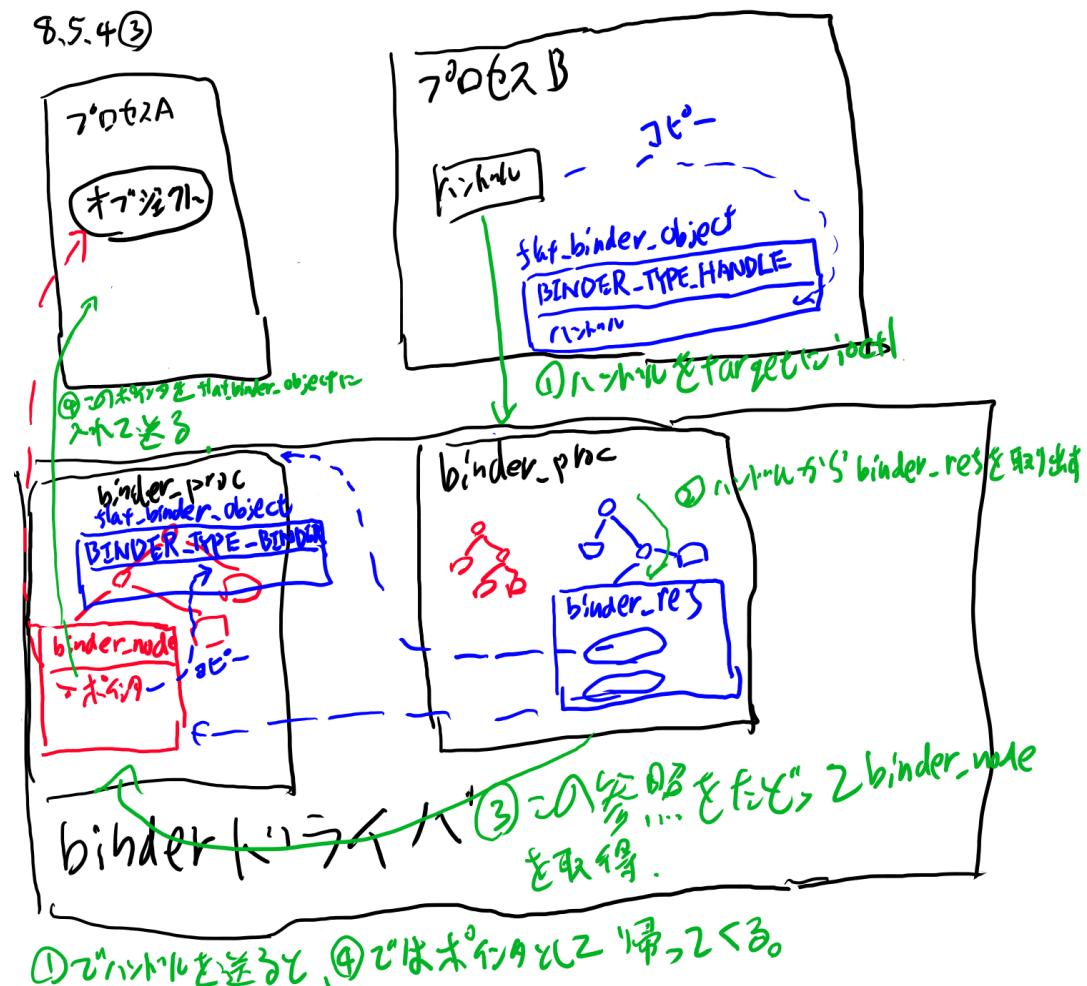


図 5.9 B からハンドルを target に A のオブジェクトを呼び出す

1. プロセス B がハンドルを target に ioctl を呼び出す
2. ドライバがプロセス B のプロセス構造体の `binder_ref` ツリーからハンドルの表すノードを高速に検索して取り出す
3. `binder_ref` のノードの中にある送り先のプロセス構造体と `binder_node` を取り出す
4. 送り先のプロセスのメモリ空間で有効なサービスへのポインタを `binder_node` から取り出す
5. `binder_transaction_data` の `target.ptr` にこのポインタを詰める
6. プロセス A の ioctl から戻る

という手順になります。1で渡したハンドルが、`binder_ref` を介して B のポインタになって B に渡る訳です。

`target` 以外の所で、引数などに `BINDER_TYPE_HANDLE` の `flat_binder_object` がある場合にも、ほぼ同じ作業が行われます。唯一の違いは、`flat_binder_object` は送り先ではタイプが

BINDER\_TYPE\_BINDER に変更される事です。

ターゲットの場合は送り先のプロセスに必ずオブジェクトが存在するので型を表すフィールドは必要ないのですが、引数の場合はそのプロセスには存在しない場合も存在するのでハンドルかポインタかを表すフィールドが必要になる訳です。

## 9.5.4④

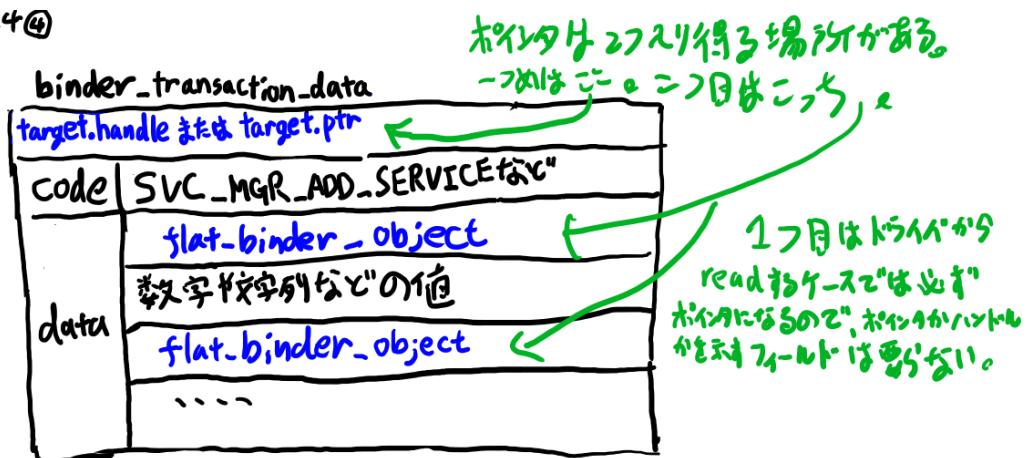


図 5.10 ポインタが入る二つの場所

ハンドルはプロセス B の中でしか有効ではありません。例えばプロセス C がまたプロセス A の同じサービスに対して呼び出しを行う時には、プロセス C にはプロセス B とは別の `binder_ref` リーがあるので、その辺りのインデックスも別物となります。

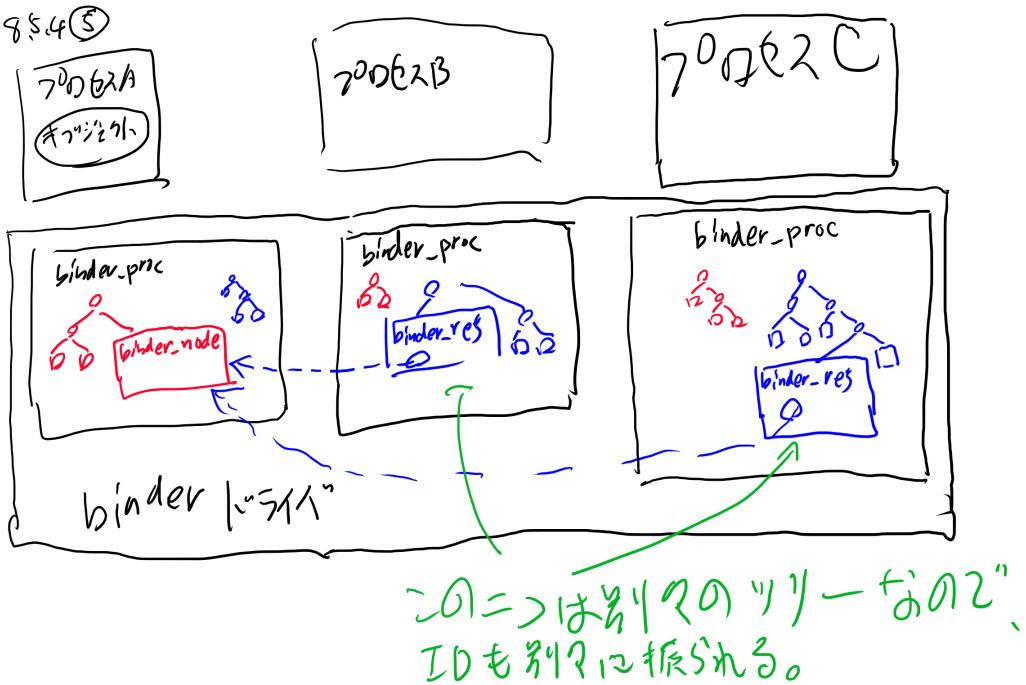


図 5.11 B と C では別のハンドルの値となる

こうして、ポインタを送るとそれを管理する binder\_node のツリーと、それを参照する binder\_ref のツリーが双方のプロセスに作られて、binder\_ref のノードを表すハンドルが ioctl からは返る事になります。そしてこのハンドルをターゲットに ioctl を呼び出すと、受け取る側では binder\_node からポインタを引いて、ポインタに戻って ioctl から返ってくる事になります。

このようにして、binder ドライバはまるでオブジェクトを送っているかのように見せかけています。

以上でオブジェクトの送信のメカニズムの説明が終わったので、任意のメソッドを呼び出す事が出来るようになります。これで binder ドライバの主要なところは一通り解説した事になりますが、おまけとしてファイルディスクリプタの送信の話もしましょう。

## 5.5 8.5.5 ファイルディスクリプタの送信と flat\_binder\_object - BINDER\_TYPE\_FD の場合

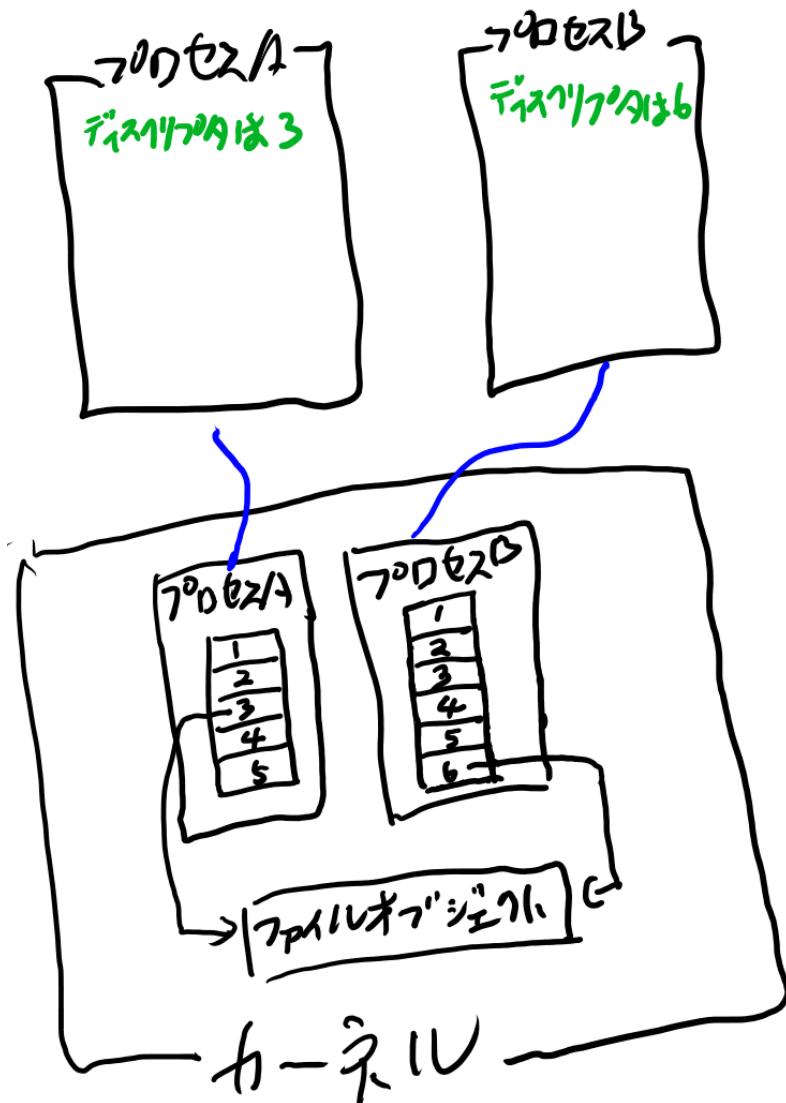
binder の特徴でファイルディスクリプタを別のプロセスに送れる、という物があります。ここで解説してしまうと大した話でも無いのですが、有名な話でもあるのでここでメカニズムを確認しておきます。

ファイルディスクリプタの話をする為には Linux のファイルの話を少しする必要があります。Linux の各プロセスには、自身のオープンしているファイルの一覧を保持するテーブルがあります。このテーブルをファイルディスクリプタテーブルと言います。このファイルディスクリプタテーブルの各エントリが、カーネルの管理するオープンしているファイルオブジェクトを指しています。ファイルディスクリプタというのは、通常はこのプロセスごとのファイルディスクリプタテーブル

## 第 55章 Has a binder object ある場合はその送信元の内側 binder object の送信元 ParentRef の場合

の先頭からのインデックスです。

8.13①



カーネルの中のタスク構造体の中には  
ファイルディスクリプタのテーブルがあり、このテーブルのエントリ  
がファイルオブジェクトを示している。テーブルのインデックスが  
ファイルディスクリプタ。

図 5.12 ファイルディスクリプタとファイルディスクリプタテーブル、再掲

## 第 55 章 flat\_binder\_object の送信と内側 binder\_object の送信と flat\_type\_fd の場合

さて、プロセス A でオープンしているファイル、fd1 があったとします。これをプロセス B に送る場合を考えます。

ファイルディスクリプタを送る場合も、BINDER\_TYPE\_BINDER でサービスを送る場合と同じく、flat\_binder\_object を使います。

リスト 5.9: ファイルディスクリプタも flat\_binder\_object で送る

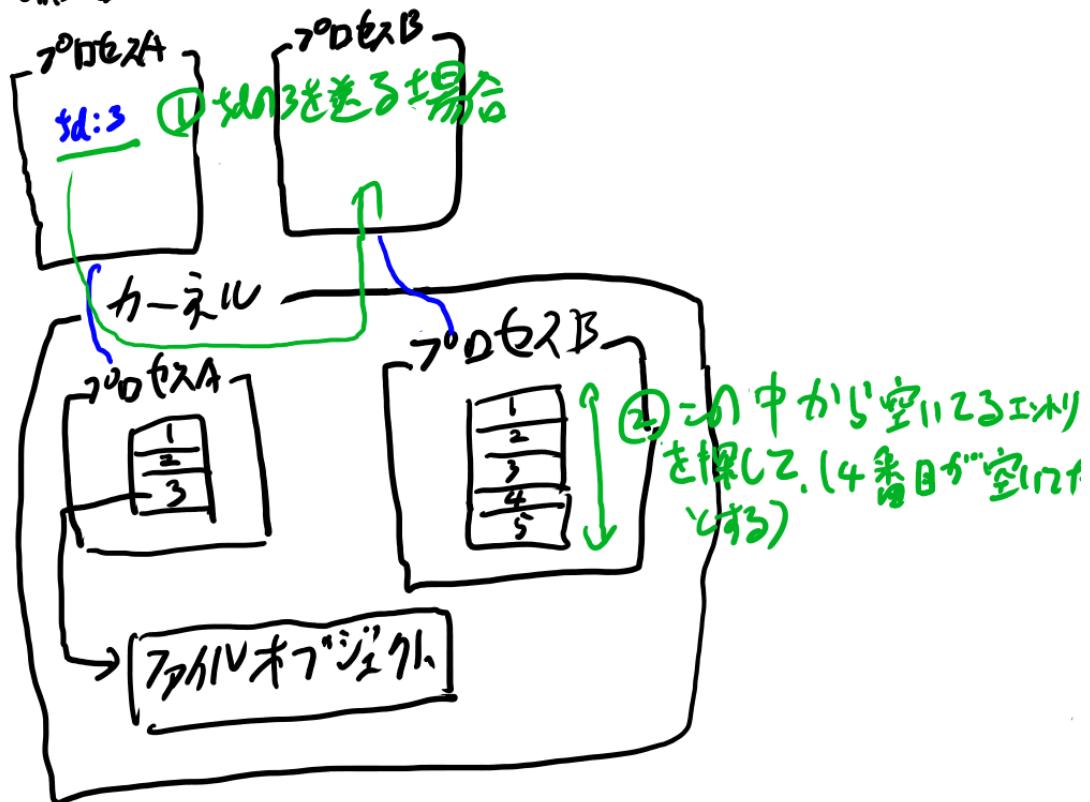
```
flat_binder_object obj;

// ファイルディスクリプタの時はタイプは BINDER_TYPE_FD
obj.type = BINDER_TYPE_FD;

// obj.handle にファイルディスクリプタを入れる
obj.handle = fd1;
```

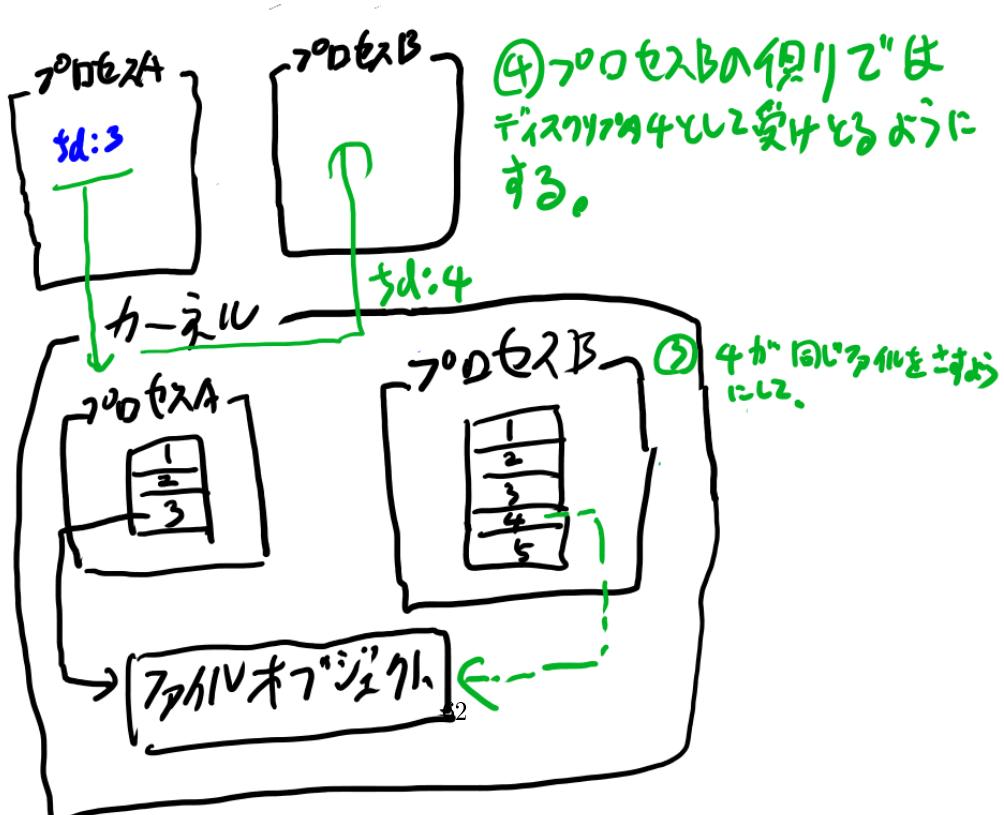
さて、こんな flat\_binder\_object を含んだデータを ioctl に渡すと、binder ドライバは送り先のプロセスのファイルディスクリプタテーブルから空きを探して、このファイルディスクリプタテーブルが指しているのと同じファイルのエントリを指すようにして、この送り先のディスクリプタテーブルに handle の値を書き換えます。

8.1.3 ②



④  $\log_B$  の復元ではディスクログを読み込むようにする。

⑤ 4が同じアレイを指向する。



## 第5章 flat\_binderが持つためのデータ送信バッファ側binderシミュレットの送信とFlatTypeFdの概念

そのコードを抜き出すと以下のようになっています。

リスト 5.10: binder ドライバ内でのファイルディスクリプタの処理

```
int target_fd;
struct file *file;

// pobj には flat_binder_object のポインタが入っているとする。
// カーネル API。オープンしているファイルオブジェクトを取ってリファレンスカウントを +1
file = fget(pobj->handle);

// target_proc で表しているプロセスのファイルディスクリプタテーブルから空いているディスクリプタを
// 取ってくる
target_fd = task_get_unused_fd_flags(target_proc, 0_CLOEXEC);

// target_proc のプロセスのファイルディスクリプタテーブルにカーネルのファイルオブジェクトを代入
task_fd_install(target_proc, target_fd, file);

// 送り先のハンドルに変換
pobj->handle = target_fd
```

task\_get\_unused\_fd\_flags() 関数と task\_fd\_install() 関数は binder ドライバで実装されている関数ですが、名前の通りの事をしているだけなのでここではこれ以上は踏み込みません。

ポイントとしては、flat\_binder\_object に BINDER\_TYPE\_FD として開いているファイルのファイルディスクリプタを入れて binder 経由でサービスに送ると、サービス側ではそのサービスの動くプロセス上のファイルディスクリプタテーブル上の同じファイルを指すエントリに自動的に変換してくれる、という事です。

この辺のコードはカーネルの内部構造をいろいろ触る割にはシンプルで読みやすいので、カーネルの勉強をしたい人などは読んでみると面白いと思います。

以上で binder ドライバの説明は全て終わりました。

サービスは全て、binder ドライバさえあれば実装出来ます。ですが皆が全部をこの ioctl で実装していくのは大変だし無駄なので、この binder ドライバを使うライブラリがこの上に提供されています。

以下ではこの binder ドライバの上に作られているライブラリについて話をしていきます。

## 第 6 章

# {threadpool-layer} 8.6 スレッドプールのレイヤ - BBinder と IPCThreadState

前節までで解説した binder ドライバさえあれば、サービスの実現に必要な事は全て出来ます。ですが、これはあまりにも低レベルな為、これだけで分散オブジェクトのシステムを実装すると、各サービスの開発者皆が同じようなコードを書く事になってしまいます。

そこで ioctl を直接呼び出して決まった処理を行う部分をスレッドプールで行うレイヤがあります。このレイヤはデータをシリализ-デシリализする Parcel、最終的に処理を受け取る BBinder、BBinder に対応するハンドルを保持してメッセージを送信する BpBinder、としてスレッドプールである IPCThreadState と ProcessState で構成されています。

//image[6\_1][スレッドプールのレイヤの位置づけ]

また、ネイティブで実装されたシステムサービスは、それを実行するプロセスの main 関数が多くの場合このレイヤのクラスを走らせて、自身のサービスを servicemanager に登録するだけ、というコードになっています。そこでこの節でシステムサービスの典型的な main 関数についても見ていきます。

なお、システムサービスは SDK のレイヤでは提供出来ません。システムイメージに含める必要があります。このレイヤを直接使うのはカスタム ROM 開発者やメーカーの人など、かなり限られた人しか作る事は出来ないと思います。

独自のハードウェアをサービスとして提供したいメーカーの方などは本節の内容はとても貴重な資料となると自負していますが、そうで無い人でも、スレッドモデルの周辺を理解しているとカーネルのレベルで何が起こるのかを正確にイメージ出来るようになるので、私は Android を深く理解するなら必須の内容と思っています。

### 6.1 8.6.1 スレッドプールのレイヤの構成要素

スレッドプールのレイヤを構成する中心となるクラスは IPCThreadState です。このクラスは各スレッドごとに一つインスタンスが出来るようなスレッドローカルなシングルトンで、IPCThreadState::self() と呼ぶと、TLS にインスタンスが無ければ生成されます。( TLS については 3.2.2 のコ

ラム参照) zzz 参照の仕方相談

ioctl でデータを送受信するには、バイト配列に値をシリアル化したり、バイト配列から値をデシリアル化する必要があります。また flat\_binder\_object のオフセットを指定したりする必要があります。そういう ioctl に渡す引数処理を行うためのユーティリティが Parcel です。前節で memcpy で行っていたような処理を代わりに行ってくれます。

IPCThreadState は Parcel を二つメンバに持ります。mIn と mOut です。mOut に書いておいたものが、binder\_write\_read の write\_buffer の方に、mIn は read\_buffer の方に使われます。binder\_write\_read については 8.3.4 などで扱いました。

IPCThreadState の joinThreadPool() というメソッドが、ioctl を呼び出して、結果を処理する、というループを回します。この時に上記の mIn と mOut を設定した binder\_write\_read を引数とします。

IPCThreadState は、servicemanager に登録するオブジェクトは BBinder である、という前提を設ける事で、ioctl の結果の処理のうち、多くの共通部分を処理してくれます。これがサービス実装の基底クラスとなります。

そしてサービスの実装が BBinder であるなら、サービスのプロキシに対応するクラスもあります。それが BpBinder です。この BpBinder は IPCThreadState を用いて、ターゲットとなるハンドルに対して ioctl 呼び出しを行います。また、共通の基底クラスとして IBinder が存在します。IBinder の役割はこの時点で述べるのは難しいので、zzz で説明します。

最後に大した事はないクラスですが良く登場するものに ProcessState という物があります。これは一プロセス一インスタンスなシングルトンオブジェクトで、IPCThreadState を立ち上げたりといった処理を行うユーティリティクラスです。

IPCThreadState, Parcel, IBinder と BBinder と BpBinder、そしておまけの ProcessState が、スレッドプールのレイヤを構成しているクラスです。

## 6.2 8.6.2 Parcel とシリアル化

Parcel はシリアル化やデシリアル化の機能を備えたバッファです。つまり内部にバイト配列を持っていて、このバイト配列に値をコピーしたり、このバイト配列から値を復元したりします。8.4.4 でちょっと登場しました。

大した事をするクラスでは無いのですが、今後良く登場するのでここで少し詳細に見ておきます。まず、String16("android.os.IServiceManager") をバッファにコピーする事を考えます。バイト配列にコピーするなら以下のようないい處になります。

リスト 6.1: バイト配列に文字列をコピーする場合

```
String16 s = String16("android.os.IServiceManager");

byte buf[1024];
memcpy(buf, s.string(), s.size());
```

これをパーセルに書く場合は以下のようになります。

リスト 6.2: Parcel に文字列をコピーする場合

```
String16 s = String16("android.os.IServiceManager");

Parcel buf;
buf.writeString16(s);
```

writeString16 の他に writeInt32 や、バイト配列を書きこむ write などもあります。書きこんだ配列を取得するのは data() メソッドです。

リスト 6.3: Parcel からバッファのポインタを取得

```
byte *ptr = buf.data();
int size = buf.dataSize();
```

また、Parcel には flat\_binder\_object のサポートがあります。writeStringBinder というメソッドに BBinder のポインタを渡すと、内部で flat\_binder\_object にラップして書き込み、書き込んだ場所を覚えておいてくれて、ipcObjects() というメソッドでオフセットの配列を取得出来ます。

8.5.3 で見たサービスの登録の時に用意するバッファと同じバッファは、以下のように用意出来ます。

リスト 6.4: サービス登録の三つの引数の書き込み

```
Parcel buf;

// 第一、第二引数の文字列を書く
buf.writeString16(String16("android.os.IServiceManager"));
buf.writeString16(String16("com.example.MyService"));

// MyService のインスタンスを生成
MyService *service = new MyService;

// 第三引数の flat_binder_object を生成して書きこみ
buf.writeStrongBinder(service);
```

Parcel に write するメソッドを呼び出していくだけで、簡単です。こうして出来たバッファを binder\_transaction\_data にセットするのでした。

## 8.4.1 ①

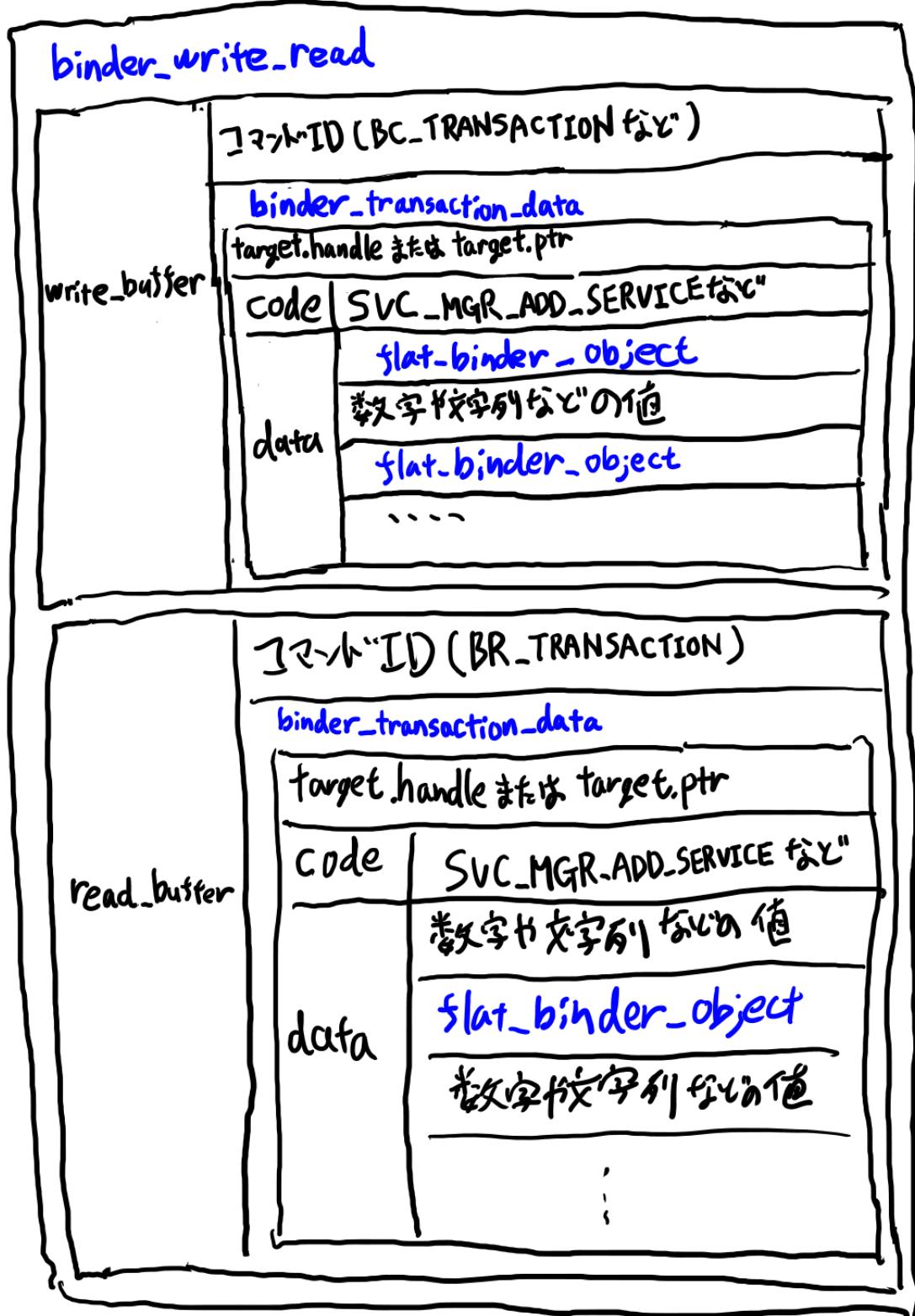


図 6.1 binder\_write\_read、binder\_transaction\_data、flat\_binder\_object の包含関係、再掲

そのコードは以下のようになります。

リスト 6.5: 引数の書きこまれたバッファを binder\_transaction\_data に設定

```
struct binder_transaction_data tr;

// servicemanager のハンドルは 0 にハードコード
tr.target.handle = 0;

// 呼び出すメソッドの ID。今回はサービスの登録なので ADD_SERVICE。
tr.code = SVC_MGR_ADD_SERVICE;

// 引数には上で作った writedata を設定
tr.data_size = buf.dataSize();
tr.data.ptr.buffer = buf.data();

// /* 1 */ offsets 配列と配列の長さの設定。
tr.data.ptr.offsets = buf.ipcObjects();
tr.data.offsets_size = buf.ipcObjectsCount();
```

8.5.3 のコードに比べると、バイト配列の扱いをほとんど気にする必要が無くなっているのが分かると思います。また、/\* 1 \*/ にあるように offsets の配列を作ってくれる所が Binder 専用のシリアルライザっぽいですね。

最後になりましたが、Parcel は binder\_transaction\_data のバッファを作る時にも、binder\_write\_read のバッファを作る時にも使えます。

### 6.3 8.6.3 IPCThreadState 概要

IPCThreadState は各スレッドごとに一つインスタンスが出来るような単位のオブジェクトです。そしてそのスレッドで、「ioctl を呼んで受信した結果を処理する」という処理をループするオブジェクトです。GUI のメッセージループに似ていますね。ioctl 周辺の処理を全て受け持つクラス、と言えます。

IPCThreadState は Parcel 型の mIn と mOut というオブジェクトを保持します。そしてスレッドプールのループで、mOut に書かれている事を write\_buffer にセットし、そして read\_buffer に mIn をセットして ioctl を呼び出します。つまり mOut を送信し、結果を mIn で受け取る訳です。

このようなループが走る事で、コードの他の部分では mOut に送りたい物を詰めておけばやがて勝手に送信される、という風に出来ます。

IPCThreadState は名前の通り、スレッドローカルなオブジェクトです。さらにスレッドローカルなシングルトンオブジェクトもあります。IPCThreadState::self() と呼び出すと、同一スレッド内ならどこでも同じインスタンスが返ります。<fn>初回呼び出しでインスタンスが作られて、7 章で紹介した TLS(スレッドローカルストレージ) にインスタンスが入ります。</fn>

だから次の ioctl ループで何か送り出してほしい、と思う事があったら、IPCThreadState とは全然関係無いクラスの中でも、IPCThreadState()::self() と現在のスレッドの IPCThreadState インスタンスを取り出して、そのインスタンスにリクエストなどを依頼する事が出来ます。

具体例は 8.6.7 の BpBinder で登場します。

IPCThreadState は、メッセージの受信対象が BBinder のサブクラスである、という前提で処理を行います。ここで少しメッセージの受信対象について補足しておきます。ioctl のメッセージ送受信には、必ず送る相手、受け取る相手がいます。この「相手」はハンドルで指定します。ハンドルが存在するためには、どこかしらで flat\_binder\_object か target にポインタを入れて binder ドライバに渡してある必要があります。(8.5.4 参照) 通常のケースではハンドルは servicemanager から取得する物ですが、幾つかのケースでは引数に渡されたオブジェクトがハンドルとして相手側に渡る事もあります。<fn>7.2.3 の ApplicationThread などがこのケースです。</fn>

どちらにせよ、何かしらの手段で binder ドライバに渡したポインタだけがメッセージを受け取る事になります。このプロセスにメッセージがやってきた、という事は、このプロセスのそれ以前の場所でポインタを binder ドライバに渡していて、そのポインタに対してメッセージがやってきている訳です。

この、現在のプロセスで以前に binder ドライバに渡したポインタ、それが BBinder のサブクラスでなくてはいけない、と IPCThreadState は要求している訳です。実際 Android で binder ドライバに渡される全ポインタが BBinder のサブクラスとなっています。

話を戻します。ioctl 呼び出しのループを実際に実行するメソッドが joinThreadPool() です。次項でこの IPCThreadState の本体とも言える、joinThreadPool() メソッドを見ていきます。

## 6.4 8.6.4 IPCThreadState の ioctl() 呼び出しループ - joinThreadPool() メソッドと BBinder

IPCThreadState の joinThreadPool() は、ioctl を呼び出して結果を処理する、というループを行うメソッドです。メソッドの名前は、このメソッドを呼ぶと以後このスレッドはスレッドプールの一員としてループを処理し続けます、というような意味合いでしょう。ループのメソッドでは普通ですが、このメソッドも一度呼び出すと終了メッセージまで戻ってきません。

ioctl で受信したメッセージの先頭はコマンド ID になっていました。(8.4.2 参照)

リスト 6.6: コマンド ID の取り出し

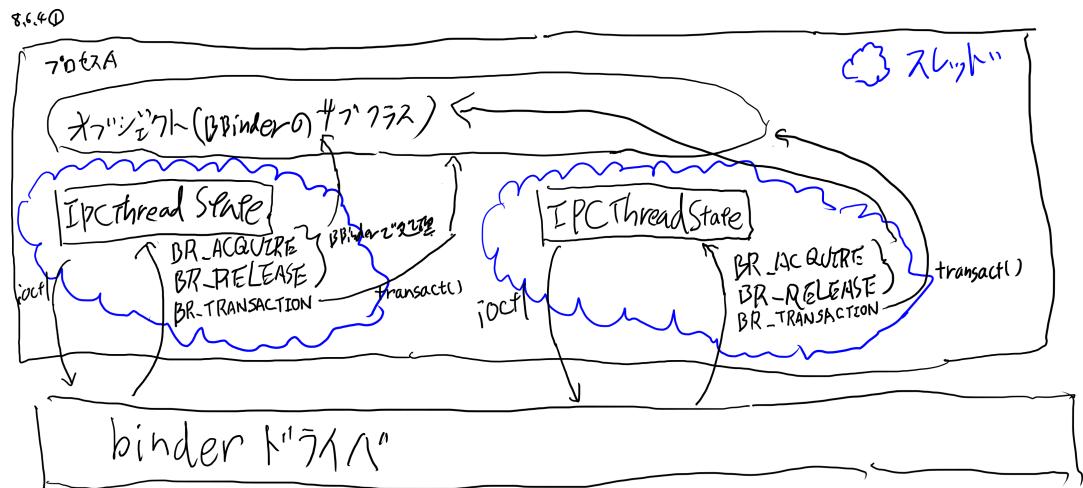
```
// ioctl 呼び出し後。結果は mIn に入っている

int32_t cmd;
cmd = mIn.readInt32();
```

コマンド ID で、重要なのは以下の物が挙げられます。

1. BR\_TRANSACTION
2. BR\_ACQUIRE
3. BR\_RELEASE

受信側なので BR で始まっています。joinThreadPool() メソッドは、ioctl を呼び出してはこれらのコマンド ID に応じた処理を行うメソッドです。

図 6.2 `joinThreadPool()` メソッドの処理概要

先頭の `BR_TRANSACTION` 以外はリファレンスカウントなどの寿命管理関連です。これらの処理は、サービスの基底クラスとなる BBinder だけで全ての処理が実行出来るので、`joinThreadPool()` メソッド内で処理が完結し、BBinder を継承するサービスの実装者は別段何もコードを書かなくても必要な処理が行われます。

さて、一番重要なのは残った `BR_TRANSACTION` コマンドです。`BR_TRANSACTION` はサービスのメソッドの処理を行う所です。これはサービス実装者にしか何をやりたいのかは分かりません。だから `IPCThreadState` は皆に共通と思われる事だけをやってくれて、後はサービスの実装者に実装を任せます。

`IPCThreadState` がやってくれる、皆に共通と思われる事は大ざっぱには以下の事となります。

1. メッセージ受信対象オブジェクトと引数のデータを取り出す
2. メッセージ受信対象オブジェクトの `transact()` メソッドに引数データを渡して呼び出す
3. 結果を `BC_REPLY` として送り返す

ようするにバイト配列からオブジェクトを取り出してメソッドを呼び、またバイト配列にして送り返す、という事をやります。`transact()` メソッドにするのに必要な事を全部やってくれる、と思っておくのが良いですね。

もう少し厳密に書くと、以下のような手続きとなります。

1. `binder_write_read` の `read_buffer` から、`binder_transaction_data` を取り出す
2. `binder_transaction_data` からメソッドを表す ID を取り出す (`code` と呼ぶ)
3. `binder_transaction_data` からメソッドの引数に相当するデータを `Parcel` に詰める (`buffer` と呼ぶ)
4. 呼び出し元の `uid` や `pid` を取り出してフィールドに保存
5. `tr.target.ptr` を `BBinder*` にキャストする  
厳密には `tr.target.cookie` だが概念的には同じ  
`</fn>`

6. 5 でキャストした BBinder の transact を呼び出す。引数は 2 のメソッドを表す ID(code)、3 の Parcel、あとは結果を入れる空の Parcel(reply と呼ぶ)
7. 6 を呼び出した結果の reply を、BC\_REPLY コマンドとして呼び出し元に返信する

それほど複雑な処理でもないのでソースコードを読んでみても良いのですが、上記の説明とそれ程変わらないコードなのでここには載せません。興味のある方は IPCThreadState.cpp の getAndExecuteCommand() メソッドの周辺を読んでみてください。

とにかく、IPCThreadState の joinThreadPool() メソッドによるループは、コマンド ID に応じて行える処理は全て行って、BR\_TRANSACTION の時には必要なデシリアライズや結果の返信は受けた上で、transact() メソッドを呼び出して後はサービス実装者に任せる、という振る舞いをします。

そこでサービスを実装する側としては、BBinder の transact() を実装すればいい訳です。そしてそのメソッドの処理の結果は reply という引数の Parcel に書き込んでやると、IPCThreadState は勝手に BC\_REPLY として結果を返信してくれます。

このように、transact() メソッド以外の部分は BBinder の基底クラスと IPCThreadState で勝手に処理してくれます。そこで次には、BBinder の transact() とはどういうメソッドか？ という話になります。

### 6.5 8.6.4 BBinder の transact() と onTransact()

BBinder はリファレンスカウントに応じた寿命処理と、transact() メソッドを持ったクラスです。  
<fn>寿命管理周辺は別段難しい事も無いコードとなっているので本書では扱いません。</fn>

IPCThreadState による ioctl のメッセージループからは、BBinder の transact() メソッドが呼ばれる、と言いました。

BBinder の transact() メソッドはサービスの transact() の共通の処理を行います。そしてサービス固有の処理に関しては、BBinder 自身の onTransact() を呼びます。onTransact() はいわゆるテンプレートメソッドのデザインパターンです。

BBinder の onTransact() メソッドの型を見てみましょう。

リスト 6.7: onTransact() メソッドの型

```
status_t BBinder::onTransact(  
    uint32_t code, const Parcel& data, Parcel* reply, uint32_t flags)
```

先頭の引数、code は binder\_transaction\_data の code に入っている、メソッドを表す ID です。これはサービスが独自に決めます。servicemanager なら SVC\_MGR\_ADD\_SERVICE や SVC\_MGR\_CHECK\_SERVICE などでした (8.4.4 参照)。

二番目の引数、Parcel の data はメソッドの引数のデータが入った Parcel です。

三番目の引数の reply は、結果を書き込む Parcel です。onTransact の中にメソッドの結果を書き込みます。これは return の値は正常に成功したかどうかのステータスコードを返す、という決まりになっているから、通常のメソッド呼び出しのように return で結果を返すという手段が使えない

為です。

四番目の flags は呼び出しが oneway、つまり結果を受け取らなくて良い前提で呼び出されたか、それとも通常の結果が返るメソッド呼び出しかを表します。

onTransact の実装者としては、第一引数の code を見て switch し、その code に応じた引数を data から取り出して、結果を reply に write していけば良い訳です。

典型的なコードとして、int a と int b の結果を足した物を返す MYSERVICE\_ADD と、引いた結果を返す MYSERVICE\_SUB を持ったサービス、MyService1 を実装すると以下のようになります。

リスト 6.8: add と sub を持つ MyService1 の実装例

```
// BBinder を継承
class MyService1 : public BBinder {
    enum {
        // メソッド ID。IBinder::FIRST_CALL_TRANSACTION より大きい値を使う約束になっている
        MYSERVICE_ADD = IBinder::FIRST_CALL_TRANSACTION,
        MYSERVICE_SUB
    };
    ...

    // onTransact をオーバーライド
    virtual status_t onTransact(
        uint32_t code, const Parcel& data, Parcel* reply, uint32_t flags = 0) {
        switch(code) {
            case MYSERVICE_ADD: {
                // data から引数を取り出し。これはサービスごとに決める。
                // 今回は呼び出し側で int32 を二つ並べて書き込んでいる、と仮定している。
                int a = data.readInt32();
                int b = data.readInt32();

                // a+b を計算して reply に書く
                reply->writeInt32(a+b);
                return NO_ERROR;
            }
            case MYSERVICE_SUB: {
                // MYSERVICE_ADD と全く同様。
                int a = data.readInt32();
                int b = data.readInt32();

                // a-b を計算して reply に書く
                reply->writeInt32(a-b);
                return NO_ERROR;
            }
        }
        return BBinder::onTransact(code, data, reply, flags);
    }
};
```

このように作った MyService1 を new して servicemanager に登録すれば、クライアントはこのサービスを呼び出す事が出来るようになります。

引数を data から readInt32() したりする、というのは少しまだ低レベルな要素が残っています

が、この MyService1 の実装くらいまで来ると、だいぶ通信回りのコードは無くなって、提供する機能に集中出来るコードとなっていましたか？

### 6.6 8.6.5 サービスの呼び出し側のコードとプロキシの必要性

さて、上記のように作ったサービスを呼び出そう、と思ったとします。まずサービスのハンドルは 8.4.4 で説明した手順で取れます。より簡単な取得の方法についてはプロキシを扱った後に触れます (8.6.9 参照)。

#### プロキシを使わないサービス呼び出しの例

さて、この handle に対して binder\_transaction\_data を用意し、binder\_write\_read に詰めて ioctl をすれば、メソッド呼び出しが出来るのでした。(8.4.5 など参照) でもそれはとても長いコードになるので、毎回サービスを呼び出す都度やるのは大変です。例えばエラー処理などを省いても、以下のようなコードになってしまいます。

リスト 6.9: プロキシ無しのサービス呼び出し

```
int handle;

// 8.4.4 にあるようなコードで MyService1 のハンドルを取得したとする。
// コードは省略。

// 3+4 を計算させる。
int a = 3;
int b = 4;

Parcel trbuf;
// /* 1 */ 引数 a, b の書き込み
trbuf.writeInt32(a);
trbuf.writeInt32(b);

// ハンドルとメソッド ID を指定
struct binder_transaction_data tr;
tr.target.handle = handle;
// /* 2 */ 呼び出したいメソッドのメソッド ID
tr.code = MYSERVICE_ADD;

// 引数を設定
tr.data_size = trbuf.dataSize();
tr.data.ptr.buffer = trbuf.data();

// binder_write_read の初期化開始。
// binder_write_read に使う送信用バッファとして bwrbuf を初期化。
Parcel bwrbuf;

bwrbuf.writeInt32(BC_TRANSACTION);
bwrbuf.write(&tr; sizeof(tr));

// binder_write_read の受信に使うバッファ。
Parcel readbuf;
```

## 第6章 {threadpool-layer} 8.6 スレッド池側のioctl呼び出し側のioctlとParcelの必要性

```
readbuf.setDataCapacity(256);

// binder_write_read に上記送信用、受信用バッファをセット。
struct binder_write_read bwr;

bwr.write_size = bwrbuf.dataSize();
bwr.write_consumed = 0;
bwr.write_buffer = bwrbuf.data();

bwr.read_size = readbuf.dataCapacity();
bwr.read_consumed = 0;
bwr.read_buffer = readbuf.data();

// ioctl 呼び出し
res = ioctl(fd, BINDER_WRITE_READ, &bwr);

// 結果は readbuf 内のバイト配列内に入っているが、長さを教えてやる必要がある。
readbuf.setDataSize(bwr.read_consumed);
readbuf.setDataPosition(0);

int32_t cmd = readbuf.readInt32();
assert(cmd == BR_REPLY);

// binder_write_read から binder_transaction_data を取り出し、その中のバイト配列を resultbuf に
// セットする。
binder_transaction_data tr2;
readbuf.read(&tr2, sizeof(tr2));

Parcel resultbuf;
resultbuf.ipcSetDataReference(tr.data.ptr.buffer, tr.data_size, NULL, 0);

// /* 3 */ a+b の結果の取り出し。つまり 7 が入ってる
int result = resbuf.readInt32();
```

こんなコードになってしまいます。binder ドライバの復習として全体のコードを見てみたい、という時ならいざ知らず、ただ  $3+4$  を計算させる為に毎回こんなコードを書くのは大変ですよね。

そこでサービスの提供者は上記と同じ事をするコードを、サービスの実装と一緒に提供する事になっています。それがサービスプロキシです。

### プロキシを使ったサービス呼び出しの例

サービスのプロキシのインターフェースは、直接呼びたいメソッドの形で定義します。上記の MyService1 のプロキシなら、以下のようになります。

リスト 6.10: プロキシのインターフェース

```
class 何かのクラス {
    int add(int a, int b);
};
```

このインスタンスを作って、このメソッドをただ呼べば良いように作ります。名前は、普通はサービスの名前の前に Bp をつけた物にする約束です。

リスト 6.11: サービスプロキシの名前は、Bp から始めるコンベンション

```
class BpMyService1 {
    int add(int a, int b);
};
```

サービスを呼び出す為にはハンドルが必要です。そこで、コンストラクタでハンドルを渡すようになります。

リスト 6.12: サービスプロキシのコンストラクタを追加

```
class BpMyService1 {
public:
    BpMyService1(int32_t handle);
    int add(int a, int b);
};
```

実装はおいといて、使う側としては、以下のように使えます。

リスト 6.13: サービスプロキシを用いてサービスを呼び出す例

```
int handle;
// 今回も handle は 8.4.4 のようなコードで習得済みとする。

sp<BpMyService1> myservice = new BpMyService1(handle);

// MYSERVICE_ADD を呼び出す
int result = myservice->add(3, 4);
```

こんな風に使える、BpMyService1 をサービスと一緒に提供します。この ByMyService1 をプロキシクラス、と呼びます。

ByMyService1 を実装するのは、原理的には先ほどのプロキシ無しのコードと同じ事をすれば良い訳です。binder\_transaction\_data と binder\_write\_read を適切に初期化して ioctl を呼び、結果を返します。

ただ、これも毎回全部書くのは大変です。これでは大変なのがサービスを呼ぶ人からサービスを実装する人に移っただけです。そこでプロキシを実装するのを支援してくれるクラスが提供されています。これが BpBinder です。

そこで以下では、この BpBinder について見ていきましょう。

## 6.7 8.6.6 サービスのプロキシと BpBinder の使い方

前項のメソッドの呼び出しの長いコード「プロキシ無しのサービス呼び出し」を見ていくと、呼び出すメソッド特有な処理は以下の三つだけである事に気づきます。

1. 引数を trbuf に詰める所
2. メソッドごとのメソッド ID
3. 結果を取り出す所

これ以外の処理は、基本的にはどのサービスのメソッド呼び出しても同じです。そこで上記の作業だけ自分でやって、それ以外は BpBinder::transact() を呼ぶ、というのが、BpBinder の使い方です。

例えば BpBinder を使うプロキシの最小限な物は、以下のようになります。

リスト 6.14: BpBinder を用いたプロキシの実装例

```
class MyService1Proxy {
public:
    MyService1Proxy(int32_t handle) : mRemote(handle) {}
    BpBinder mRemote;

    int add(int a, int b) {
        Parcel data, reply;

        // 1. 引数を data に詰める
        data.writeInt32(a);
        data.writeInt32(b);

        // 2. BpBinder の transact をメソッド ID をつけて呼び出す
        mRemote.transact(MYSERVICE_ADD, data, &reply);

        // 3. 結果の取り出し
        return reply.readInt32();
    }
};
```

add の実装はこれだけです。前項のコードに比べるとずっと短くなりましたね。そしてメソッドに特有の三つの部分だけの実装となっている事が分かります。

このようなプロキシクラスさえ提供されていれば、MyService1 を使うのは簡単です。MyService1 サービスを使う人は、handle をコンストラクタで渡して、このプロキシの add をよびだせば良いのです。

リスト 6.15: MyService1Proxy を使うコード例

```
int handle;
// handle は 8.4.4 のコードで取り出してあるとする。
```

```
// プロキシクラスのコンストラクタに handle を渡す
MyService1Proxy myservice(handle);

// プロキシのメソッド呼び出し
int result = myservice.add(3, 4);
```

サービスの使用もだいぶ簡単になりました。このように、BpBinder を用いる事で、サービスのプロキシを簡単に実装出来る事が分かりました。

## 6.8 8.6.7 BpBinder の実装 - transact() メソッドと IPCThreadState

BpBinder はハンドルを渡して初期化し、transact() メソッドを呼んでメッセージを送信する、という話をしました。

実際の実装は、実は BpBinder 自身は ioctl を呼び出しません。その代わり、現在のスレッドの TLS に入っている IPCThreadState に処理を任せます。

エラー処理を省くと以下のようなコードになっています。

リスト 6.16: BpBinder::transact() メソッド

```
status_t BpBinder::transact(
    uint32_t code, const Parcel& data, Parcel* reply, uint32_t flags)
{
    status_t status = IPCThreadState::self()->transact(
        mHandle, code, data, reply, flags);
    return status;
}
```

BpBinder は IPCThreadState の参照を受け取ったりしていないのですが、IPCThreadState はスレッドローカルなシングルトンなので、いつでもこのように IPCThreadState::self() で取得することができます。

IPCThreadState の transact は mOut に引数の処理を書いた後に joinThreadPool() メソッドとほぼ同じ処理を一回だけ行う、という振る舞いをします。

こうして、プロキシの実装者から見ると、BpBinder は transact を呼ぶと binder\_write\_read や binder\_transaction\_data を自分で設定して呼び出して結果を取り出す、という事をやってくれます。BpBinder を使えば実際の ioctl 周辺の処理を自分で書く事無く、全てこのスレッドプールのレイヤが処理してくれます。

こうしてサービスの実装者も使用者も、細かいプロセス間通信のコードを書く事無く、サービスの実装とプロキシの実装を提供出来るようになりました。

## 6.9 8.6.8 servicemanager のプロキシ - IServiceProvider

BpBinder とプロキシの説明を終えたので、servicemanager のプロキシについて見ておく事にします。servicemanager のプロキシは最初から Android のフレームワークの中に含まれています。

servicemanager はハンドル 0 番に固定されているので、プロキシとして最初からメソッド呼び出しが出来ます。具体的には 8.4.4 で行っているコードと同じ事をすれば良いのですが、これをプロキシ化したクラスに、BpServiceManager というクラスがあります。通常はその基底クラスである IServiceProvider を使う事になっています。

ハンドルを取得せずに使う事が出来るので、IServiceProvider のインスタンスはグローバル関数で簡単に取得出来るようになっています。そのグローバル関数の名は、defaultServiceManager() です。

リスト 6.17: defaultServiceManager の宣言

```
namespace android {
    sp<IServiceProvider> defaultServiceProvider();
}
```

sp は StrongPointer の略で、スマートポインタです。寿命管理をしてくれる以外は普通のポインタとして使えます。コラム リファレンスカウントとスマートポインタ - RefBase と Weak Reference と sp

### コラム: リファレンスカウントとスマートポインタ - RefBase と Weak Reference と sp

リファレンスの寿命管理として、Android では RefBase というユーティリティクラスが提供されています。これは寿命管理では良く出てくる、Weak Reference と通常のリファレンスを管理する基底クラスです。Android では Weak Reference じゃない通常の所有を、Weak Reference の反対として Strong Reference と呼びます。RefBase には、incStrong(), decStrong() のようないリファレンスカウントの上げ下げを行うメソッドと、incWeak(), decWeak() という Weak Reference のリファレンスカウントを上げ下げするメソッドがあります。

そしてこれらのリファレンスカウントのメソッドを使って寿命管理をするスマートポインタの一つが sp です。sp は Strong Pointer の略で、Weak でないリファレンス、つまりカウントが 0 になるとそのオブジェクトを削除するオーナーシップを表します。

RefBase 自身は Binder とは関係無く使える汎用のユーティリティクラスですが、Binder 関連のクラスは RefBase を継承している物がほとんどなので、Binder 関連のコードではこの sp は良く出てきます。====[/column]

こうして取得した IServiceProvider で、良く使うメソッドは以下の二つです。

リスト 6.18: IServiceProvider の addService() と checkService() メソッドの宣言

```

class IServiceManager {
public:
    // サービス登録を使うメソッド
    virtual status_t addService( const String16& name,
                                const sp<IBinder>& service,
                                bool allowIsolated = false) = 0;

    // サービス取得使うメソッド
    virtual sp<IBinder> checkService( const String16& name) const = 0;
};


```

addService() と checkService() の二つのメソッドです。これらは、8.4.4 で挙げた servicemanager の二つのメソッド ID、つまり SVC\_MGR\_ADD\_SERVICE と SVC\_MGR\_CHECK\_SERVICE に対応したプロキシメソッドです。

checkService() の結果は、ハンドルを返すのではなく、それを BpBinder にラップした物を返します。型はそのスーパークラスの IBinder を返す事になっています。何故 BpBinder でなく IBinder なのか、については 8.6.10 で扱います。

なお、何回か自動でリトライする getService() というラッパも存在します。こちらの方が便利なので通常はこちらを使いますが、本質的には checkService メソッドと同じ事を行います。

## 6.10 8.6.9 IServiceManager を用いてサービスのハンドルを簡単に取得する

比較の為、8.4.4 で述べた servicemanager 呼び出しでサービスのハンドルを取得するのと同じコードを、IServiceManager でも書いてみましょう。

defaultServiceManager() でプロキシを取得し、checkService() が getService() で取り出せば良い、という事になります。8.4.4 と同様に "SurfaceFlinger" サービスを取得する場合のコードは以下のようになります。

リスト 6.19: getService() の使用例

```

sp<IBinder> binder = defaultServiceManager()->getService(String16("SurfaceFlinger"));
int handle = binder->remoteBinder()->handle();

```

IBinder や BpBinder の詳細はここでは重要では無いので、すぐにハンドルを取り出してしまいます。普段は BpBinder を取得すれば十分なのでわざわざ handle() まで取得する事はありませんが、必要であれば上記 2 行で簡単に handle も取得出来ます。

## 6.11 8.6.10 IBinder とは何か？ - SVC\_MGR\_CHECK\_SERVICE でハンドルが返ってこない 場合

getService() メソッドの結果は BpBinder では無くて IBinder といいう基底クラスだと  
言いました。いつも BpBinder であれば最初から BpBinder を返せば良いのですが、実は  
SVC\_MGR\_CHECK\_SERVICE では、ポインタが返ってくるケースがあります。それは検索  
するサービスが自分のプロセスのサービスの場合です。この場合は BBinder がそのまま返ります。

例を挙げましょう。例えば以下のコードでは、addService() で渡したポインタがそのまま帰って  
きます。

リスト 6.20: addService() したのと同じ場所で checkService() する例

```
// /* 1 */ 登録するサービスのポインタ
MyService1* service1 = new MyService1();

sp<IServiceManager> svcmgr = defualtServiceManager();
svcmgr->addService(String16("com.example.MyService1"), service1);

// /* 2 */ checkService() で取得したオブジェクト
sp<IBinder> result = svcmgr->checkService("com.example.MyService1");
```

この場合、/\* 1 \*/ の service1 と /\* 2 \*/ の result は同じインスタンスを指します。

これくらい単純なケースだと、いちいち IServiceManager に問い合わせたりせず、最初から  
service1 を使えばいいじゃないか、という気がしてしまいますが、現実にはもっとずっと複雑なケー  
スもありうるのです。

本質的にはこれは checkService() に限らず、binder ドライバに BINDER\_TYPE\_HANDLE の  
flat\_binder\_object を送る場合にいつでも起こり得ます。BINDER\_TYPE\_HANDLE を送信し  
た先が、そのハンドルの元となるポインタの存在するプロセスの場合、BINDER\_TYPE\_BINDER  
に変換されて送信されます。

この事をもう少し詳しく見ていきましょう。プロセス A にサービスのポインタが存在し、プロセス B とやり取りする場合を考えましょう。

プロセス A から生のポインタをプロセス B に送る時は、flat\_binder\_object に  
BINDER\_TYPE\_BINDER を入れるのでした。(8.5.3, 8.5.4) すると、プロセス B の側では  
BINDER\_TYPE\_HANDLE として渡ってきます。

8.6.10 ①

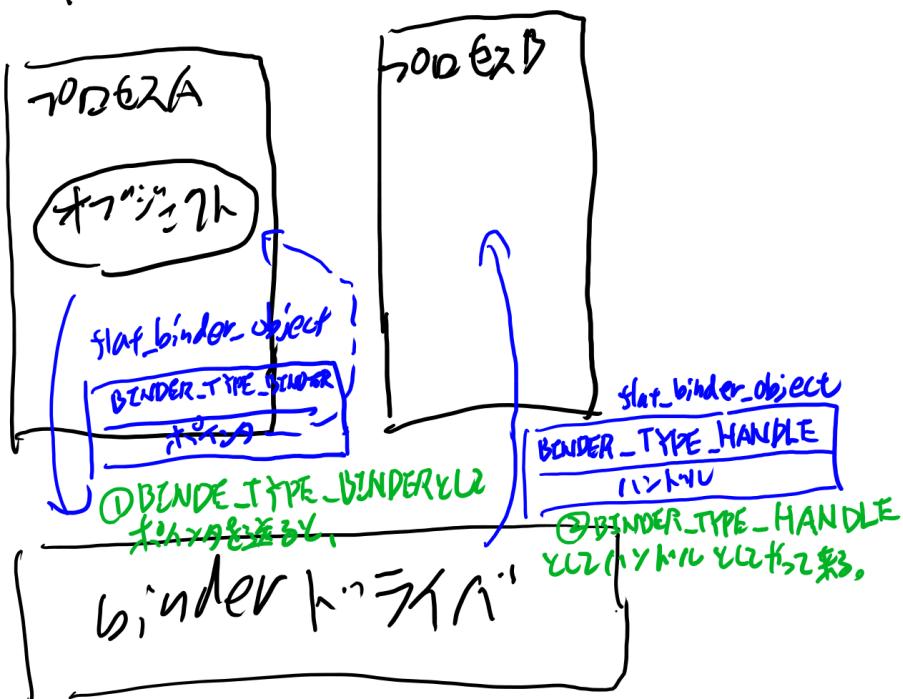


図 6.3 BINDER\_TYPE\_BINDER を送ると BINDER\_TYPE\_HANDLE として出てくる

このハンドルを今度は逆にプロセス B からプロセス A に送る場合を考えます。この場合は、逆に BINDER\_TYPE\_HANDLE が、BINDER\_TYPE\_BINDER に変換されてプロセス A の側に出てきます。

8.6.10 ②

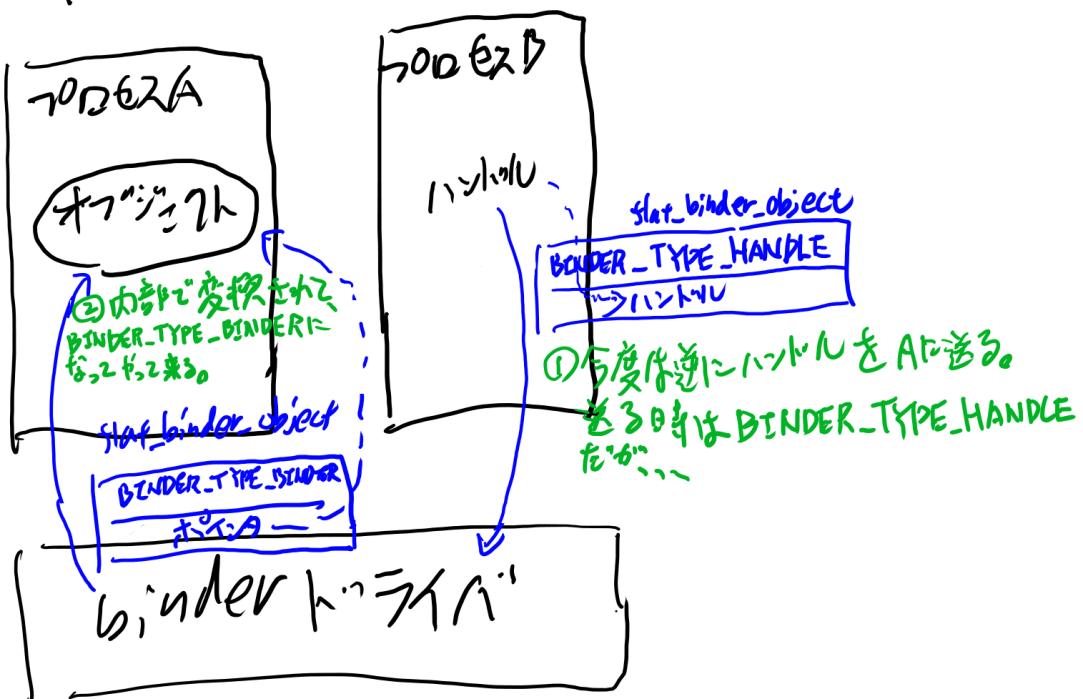


図 6.4 BINDER\_TYPE\_HANDLE を送ると BINDER\_TYPE\_BINDER として出てくる

二つのプロセスの場合では自明にも思えるかもしれないが、プロセス C を足してみます。  
 プロセス A が B に送ります。すると BINDER\_TYPE\_BINDER が  
 BINDER\_TYPE\_HANDLE となります。

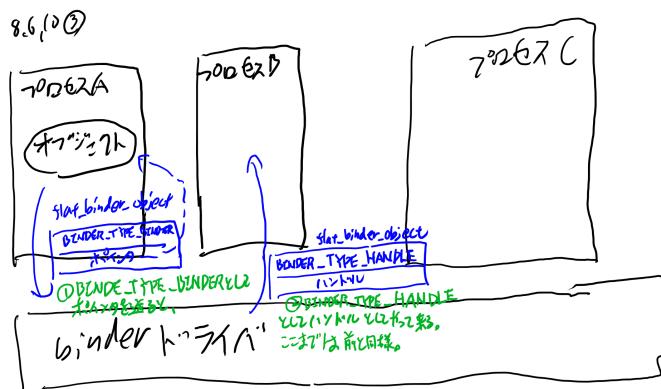


図 6.5 BINDER\_TYPE\_BINDER を送ると前回同様、BINDER\_TYPE\_HANDLE として出てくる

プロセス B がプロセス C に BINDER\_TYPE\_HANDLE を送ります。するとプロセス C でもこれは BINDER\_TYPE\_HANDLE のままです。

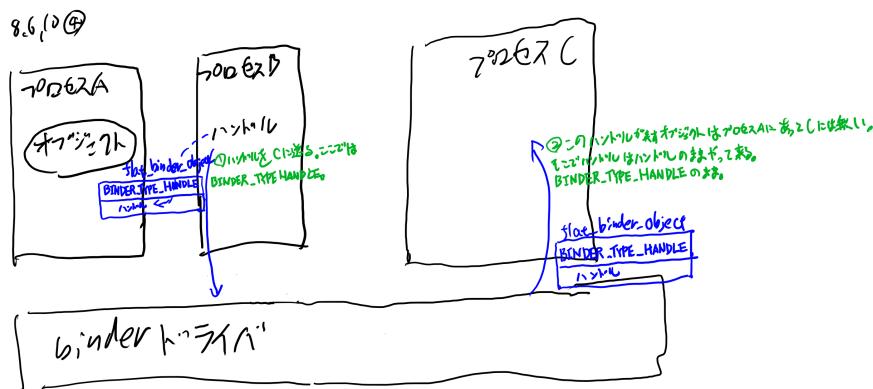


図 6.6 BINDER\_TYPE\_HANDLE を送ると、今回は BINDER\_TYPE\_HANDLE のまま出てくる

図 6.7「BINDER\_TYPE\_HANDLE を送ると、今回は BINDER\_TYPE\_HANDLE のまま出てくる」と図 6.5「BINDER\_TYPE\_HANDLE を送ると BINDER\_TYPE\_BINDER として出てくる」の違いに注目してください。どちらも BINDER\_TYPE\_HANDLE を送信していますが、受け取る側は図 6.5 が BINDER\_TYPE\_BINDER に変換されるのに対し、図 6.7 は

BINDER\_TYPE\_HANDLE のままでです。<sup>\*1</sup>

さて、ここからプロセス C からプロセス A にこのハンドルを送るとどうなるか？ というと、この場合はこのハンドルの表す生のポインタが所属するプロセスに戻ってきたという事なので、BINDER\_TYPE\_BINDER として名前のポインタが返ります。

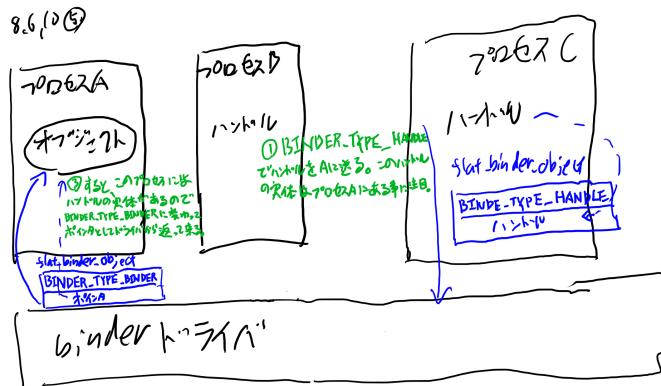


図 6.7 BINDER\_TYPE\_HANDLE を送ると、今度は BINDER\_TYPE\_BINDER として出てくる

このように、ハンドルを送信した結果がハンドルなのか BINDER\_TYPE\_BINDER に変換されるかは、相手のプロセスによります。

そこでクライアントとしてはサービスの参照に生のポインタでもハンドルでもどちらの場合でも共通に扱えるインターフェースを使う事になります。これが IBinder です。

IBinder は BBinder と BpBinder の共通の基底クラスです。

<sup>\*1</sup> なお、ハンドルの値はプロセスごとに異なります。図 5.11 を参照

8.6.10 ⑥

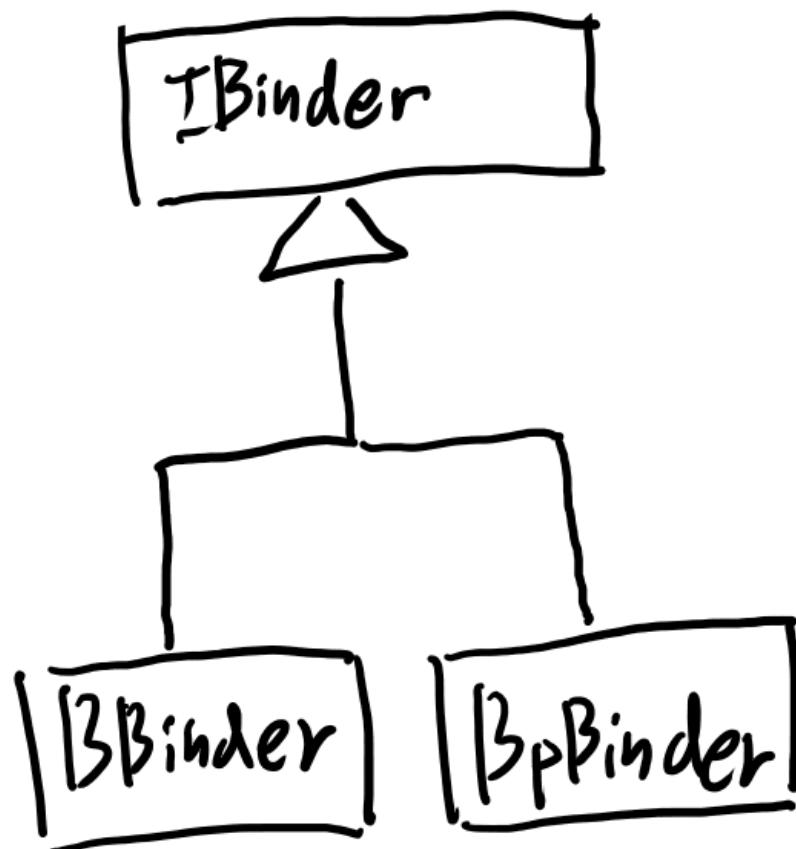


図 6.8 IBinder、BBinder、BpBinder のクラス図

IBinder が BBinder なのか BpBinder なのかを問い合わせるために、localBinder() というメソッドと remoteBinder() というメソッドが存在します。

リスト 6.21: localBinder() と remoteBinder() の型

```
class IBinder : public virtual RefBase
{
public:
    virtual BBinder*      localBinder();
    virtual BpBinder*     remoteBinder();
};
```

BBinder は localBinder で this を返し、remoteBinder で NULL を返します。BpBinder は localBinder で NULL を返し、remoteBinder で this を返します。

リスト 6.22: localBinder() と remoteBinder() の実装それぞれ

```
class BBinder : public IBinder
{
public:
    virtual BBinder*      localBinder() { return this; }
    virtual BpBinder*     remoteBinder() { return NULL; }
};

class BpBinder : public IBinder
{
public:
    virtual BBinder*      localBinder() { return NULL; }
    virtual BpBinder*     remoteBinder() { return this; }
};
```

これらのメソッドを用いる事で、どちらのインスタンスかをしる事が出来ます。

IServicemanager の checkService() などは、返ってきた flat\_binder\_object が BINDER\_TYPE\_BINDER か BINDER\_TYPE\_HANDLE かに応じて、BBinder のポインタを返すか BpBinder のインスタンスを生成して返すかを判断しています。

つまり以下のようなコードになっている訳です。

リスト 6.23: IServicemanager の checkService() の概要

```
flat_binder_object *obj;
// obj は binder_transaction_data から取り出す。詳細省略

sp<IBinder> out;
switch(obj->type) {
    case BINDER_TYPE_BINDER:
        // obj->ptr と obj->cookie は概念的には同じ物が入っている
        out = reinterpret_cast<IBinder*>(obj->cookie);
        return out;
    case BINDER_TYPE_HANDLE:
        out = new BpBinder(obj->handle);
        return out;
}
```

上記コードで obj->ptr と obj->cookie が出てきますが、概念的には同じインスタンスが入っています。実際には obj->ptr には Weak Reference が、obj->cookie には実体のポインタが入っています。

## 6.12 8.6.11 ProcessState とスレッドプール

ここまでで IPCThreadState の joinThreadPool() メソッドが ioctl を呼び出すループの処理を行っている、という話をしました。ですがこのクラスのどちらへんがスレッドプールなのか、という話はしていません。肝心のスレッドを開始するのが ProcessState クラスとなります。

ProcessState はシングルトンオブジェクトで、一プロセスにつき一インスタンスが対応し、プロセス全体のスレッドプールに関する情報を保持します。

ProcessState を取得するには、ProcessState::self() を呼び出します。するとまだインスタンスが出来ていなければ作成し、既にインスタンスがあればそのインスタンスを返します。

ProcessState クラスは、startThreadPool() というメソッドを持ちます。これが新しいスレッドを開始し、そのスレッドの中で IPCThreadState の joinThreadPool() を呼び出します。

リスト 6.24: startThreadPool() の実装

```
void ProcessState::startThreadPool()
{
    // 新しいスレッドを作つて実行。スレッドのクラスは PoolThread。
    sp<Thread> t = new PoolThread(isMain);
    t->run();
}

// PoolThread は、新しいスレッドの中で IPCThreadState の joinThreadPool を呼ぶだけのスレッド。
class PoolThread : public Thread
{
protected:
    virtual bool threadLoop()
    {
        IPCThreadState::self()->joinThreadPool();
        return false;
    }
};
```

こうして、ProcessState の startThreadPool() メソッドを呼び出すと、新しいスレッドが作られて、そのスレッドの中では IPCThreadState の joinThreadPool() メソッドが呼ばれます。この joinThreadPool() は ioctl を呼び出して処理するループでした。(8.6.4)

ProcessState の startThreadPool() を何回か呼ぶと、呼んだ回数分だけスレッドが作られて、皆が ioctl で待ち状態に入ります。そして binder ドライバからメッセージがやってきたら処理を行つて、また ioctl で待ち状態に入る訳です。これはまさにスレッドプールです。

このように、実装のほとんどは IPCThreadState の joinThreadPool() メソッドではありますが、そのループをスレッドプールとして管理するのが ProcessState です。

## 6.13 8.6.12 システムサービスの main 関数と ProcessState - 独自のシステムサービスを提供する時のコード例

ProcessState にはスレッドプールの管理の他に、もう一つ役割があります。それは binder ドライバの open と mmap です。

サービスを提供するプロセスは、まず binder ドライバを open して mmap しなくてはいけないのでした。(8.3) これら open と mmap の処理は、ProcessState のコンストラクタで行います。

リスト 6.25: ProcessState のコンストラクタで binder ドライバの open と mmap が行われる

```
// open_driver() で open() が行われる。
ProcessState::ProcessState()
    : mDriverFD(open_driver())
...
{
    if (mDriverFD >= 0) {
        // open に成功していたら mmap を行う。
        mVMStart = mmap(0, BINDER_VMSIZE, PROT_READ, MAP_PRIVATE | MAP_NORESERVE, mDriverFD, 0);
    }
}
```

このように、ProcessState を作成すれば、binder ドライバを使うのに必要な初期化は自動的に行われます。

ProcessState はシングルトンオブジェクトで、最初に static メソッドである ProcessState::self() が呼ばれた時にインスタンスが作成されます。以後の self() メソッド呼び出しはその作成した同じインスタンスが返されます。

こうして open したファイルディスクリプタはどこのスレッドからも参照出来る為、IPCThreadState から ioctl を呼ぶ時にも ProcessState から取り出して第一引数に渡す事が出来ます。具体的には ProcessState::self()->mDriverFD で参照出来ます。

この ProcessState のコンストラクタによる binder ドライバの open と mmap 処理も踏まえると、典型的な Service、例えば MyService を実装する C++ のコードを走らせる main() のコードは、簡易的に書くと以下のように書けます。

リスト 6.26: サービスを提供する exe の典型的な main() の内容

```
void main() {
    // (1) ProcessState のコンストラクタ呼び出し。
    ProcessState* ps = ProcessState::self();

    // (2) 別スレッドを立ち上げて ioctl のメッセージループ開始
    ps->startThreadPool();

    // (3) servicemanager にサービスを登録する、後述
    defaultServiceManager()->addService(String16("MyServiceName"), new MyService);
```

```

    // (4) この main のスレッドも ioctl メッセージループを回し続ける事でスレッドプールのースレッド
    // として振る舞う。
    IPCThreadState::self()->joinThreadPool();
}

```

(1) まずは先頭の ProcessState::self() の呼び出しで、ProcessState のコンストラクタが呼ばれます。ここで /dev/binder の open と mmap を行います。

(2) startThreadPool() 呼び出しで、新しいスレッドを立ち上げて、ここで ioctl をメッセージ受信の為に呼び出して、このスレッドはブロックします。

(3) その次にやるべき事は、MyService のインスタンスを new で作り、そのポインタをバインダドライバ経由で servicemanager に SVC\_MGR\_ADD\_SERVICE メソッド ID で送る事で、このサービスを servicemanager に登録する事でした。

ここでは 8.6.8 で出てきた IServiceManager を使っています。この過程で MyService ポインタに対応した binder\_node が作られ、別のプロセスからはこの binder\_node を参照する事でポインタを識別できます。

(4) サービスのポインタを servicemanager に登録したので、このメインスレッドもやる事は無くなりました。そこでこのスレッドも有効利用すべく、ioctl呼び出しを行うループを実行し、スレッドプールのースレッドとして振る舞います。

このコードでは (2) の startThreadPool() と (4) を合わせて、メッセージループは二つのスレッドとなりました。

これでサービスを提供するプロセスのやるべき事は終わりです。実際に記の main 関数とほとんど同じ内容の main 関数のプロセスは、Android のシステムサービスのプロセスでは良く見かけます。

説明の為にあえて分離しましたが、実際は (1) と (2) は 1 行で書く事が出来るため、main 関数はたったの 3 行となります。

## 6.14 8.6.13 サービスの仕組みとシステムの発展 - サービスの実装とプロセスの分離

ここまでで、Binder という仕組みのうち、スレッドプールのレイヤの解説が終わりました。先に進む前に、この時点で実現されているサービス、という物について、どういう特徴があるかを少し考えてみたいと思います。

Android ではハードウェアや新たなシステムの機能を追加する時は、システムサービス、という形で追加する事を推奨しています。システムサービスとは BBinder のサブクラスで、servicemanager に登録して使うものです。

サービス自身は何かのプロセス上で動きますが、一対一の関係では無く、一つのプロセスで複数のサービスを提供する事は可能ですし、また良く行われる事でもあります。

システムサービスの実装は BBinder のサブクラスとして onTransact を実装し、さらにそれに対応したプロキシを BpBinder を用いて実装するだけです。このコードには main 関数で作った何かを

参照する必要は一切ありません。main 関数でこのサービスへの依存が発生するのは、addService() の引数だけです。(8.6.12 の (3) に対応)。

システムサービスがそれぞれ別のプロセスに分かれている方がロバストで安全なシステムにしやすいですが、一方でプロセスはメモリや CPU などのハードウェア資源を消費する物でもあり、組み込みのシステムであまり多くのプロセスを立ち上げるのは、重くなりすぎて使いものになりません。また、プロセス間通信もプロセス内のメソッド呼び出しそれぞれ重くなります。システムサービス相互のやりとりをなるべくプロセス内のメソッド呼び出しで済ますには、同じプロセスに多くのサービスが存在する方が良いという事になります。

### コラム: サーバープロセスとサービス

システムサービスを提供しているプロセスはサーバープロセスと呼ばれます、サーバーという用語はいろいろな場所で使われていてややこしいので、特に必要が無ければ本書では「サービスを提供しているプロセス」と呼ぶ事にしています。ですが、このサーバーという呼称を知っていると、ソースを読む時に便利な事もあります。例えば SystemServer プロセスは、Androidにおいてサービスを提供している重要なプロセスですが、本コラムで述べたようなサーバーという名前の使われ方を知っていれば、SystemServer という名前を見ただけでサービスを提供しているプロセスである事が推測出来ます。===[/column]

Android のシステムサービスは、どれくらいプロセスを分けるのか、という決断を、あまり実装に影響を与えるに行う事が出来る設計となっています。次の節で扱いますが、システムサービスの仕組みは、呼び出し側はサービスがどこのプロセスに属しているかを意識せずに使えるように作る事が出来ます。プロセスを分けていっても他のパートのコードには影響を与えません。

まだ多くの端末でリソースが限られている時代の場合には一つのプロセスにたくさんのサービスを動かす事により、分散で無い通常のモノリシックなシステムのようにふるまい、少ないリソースでも動くようになります。

そして時代が進みハードウェアが発展してきて、メモリや CPU 資源が潤沢になっていくに応じて、重要なサービスを別のプロセスに分けてハードウェアスレッドを割り当てたり、障害に対してロバストにしていったりできます。

実際、Android はバージョンを重ねるごとにサービスのプロセスを分けていった歴史があり、その歴史は現在でも進行中です。

### コラム: surfaceflinger サービスにみる、システムの発展

surfaceflinger というシステムサービスがあります。詳細は 12 章で扱います。このサービスは、初期の頃はその他のシステムサービスと同様、SystemServer というプロセスに存在していました。初期の頃はほとんどのサービスがSystemService プロセス一つで実行されていました。少なくとも Android 2.3 の GB までは SystemServer プロセスにありました。

ですが、ハードウェアの進歩に伴い、おそらく Honeycomb の頃から<sup>\*2</sup> surfaceflinger は別プロセスに分かれる事になりました。ハードウェアスレッドの少ない端末ではパフォーマンスの低下がみられましたが、十分なハードウェアスレッドの存在する機種では、なめらかで引っかかるないアニメーションが実現されるようになりました。

このように、ハードウェアの進歩に合わせて柔軟にシステムのプロセス構成を変更していく、というのは、Android というシステムの大きな特徴と言えます。年々劇的な進歩を遂げてきた携帯電話というハードウェアの上で、時代の激変になんとか対応し続けて来られたのも、Android の基盤とも言えるシステムサービスの設計の段階で、このようなハードウェアの進歩に応じたシステムの発展がデザインされていたおかげである、と言えるでしょう。

また、1巻のコラムで触れる Stagefright バグとその結果の Media Framework の改善も、時代に合わせたプロセス構成の発展のまさに現在行われている例と言えると思います。

また、スレッドプールにどれだけのスレッドを用意するかもサービスの実装とは独立に決定出来ます。main 関数でたくさん startThreadPool() を呼べばスレッドプールに割り当てられるスレッドは多くなる訳です。サービスの実装側ではスレッドプールにスレッドが幾つあるかは、一切気にする必要はありません。

このように、サービスの実装は一切いじらずにプロセスやスレッド数といったリソースやシステム構成の設計を行えるのは、Android のシステムサービスという仕組みの重要な特徴と言えます。

## **別冊 詳解 Binder**

---

2017年3月31日 初版第1刷 発行

著者 有野和真

---