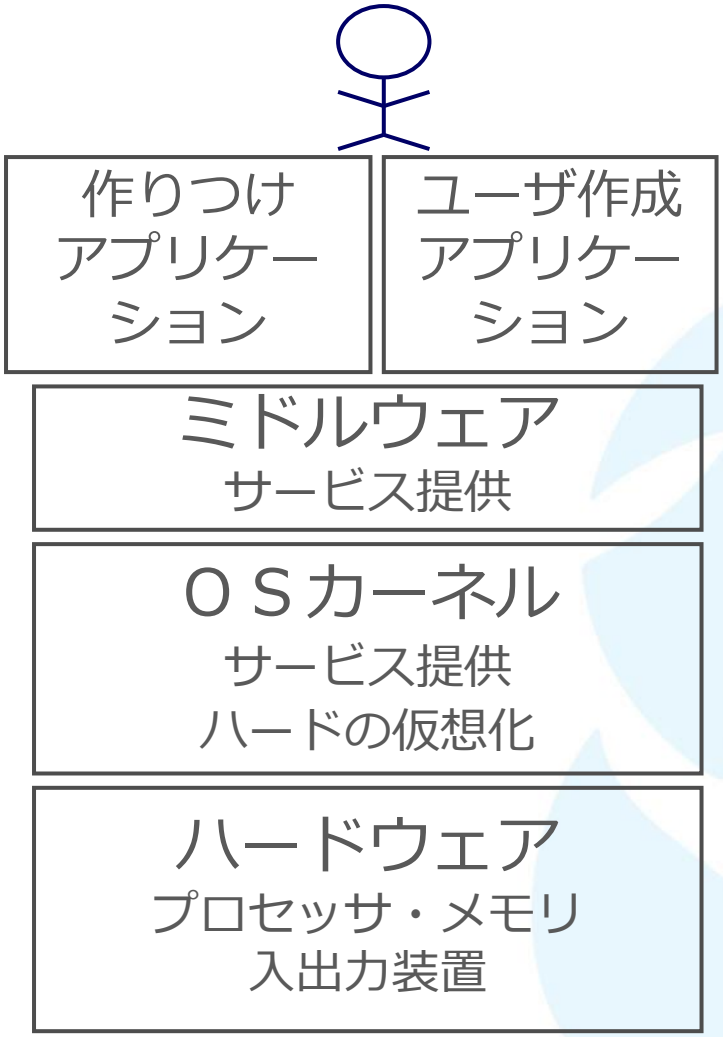
おまけ
OSの構造の境界線の理由

OSの構造の絵を思い出してください

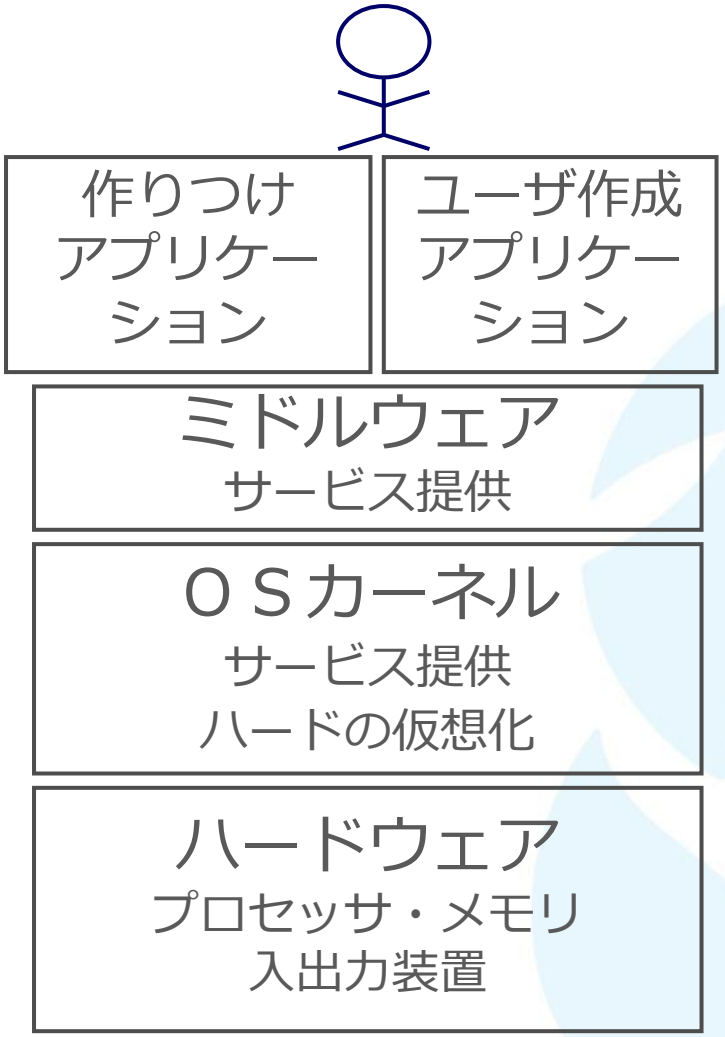
東邦大学

箱の境界線の理由は？



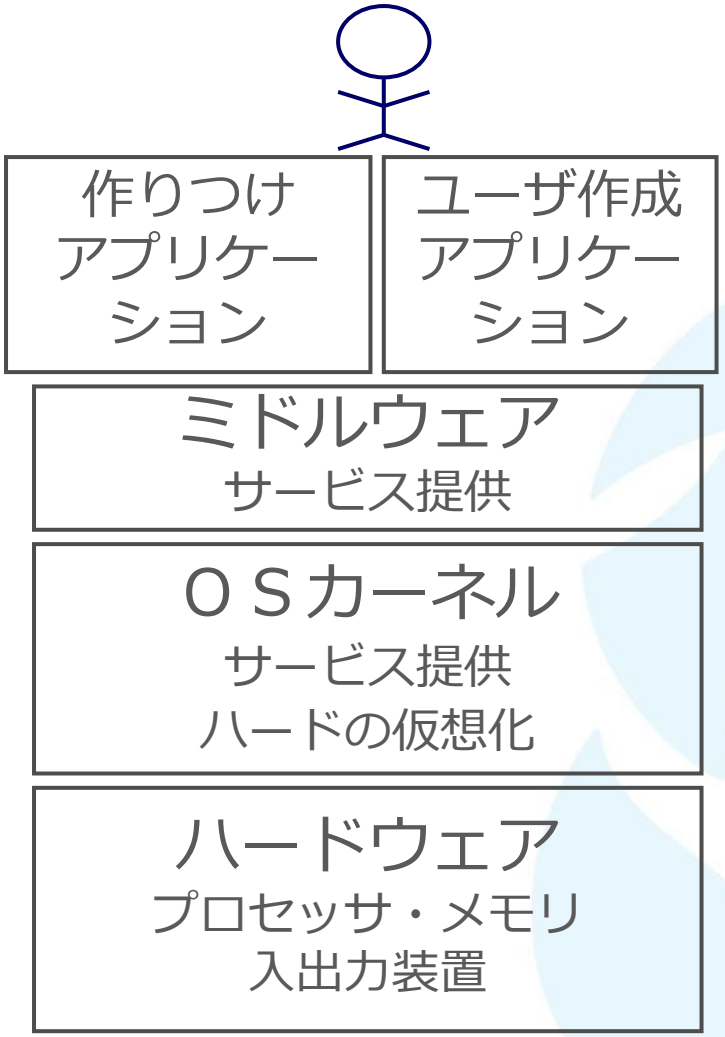
- 階層構造になっていて
  階層の間の線引きが
  されています

箱の境界線の理由は？



- 階層構造になっていて
  階層の間の線引きが
  されています
- どこに線を引くべきか？
- どの機能をどの層に
  入れるべきか

箱の境界線の理由は？



- 階層構造になっていて
  階層の間の線引きが
  されています
- どこに線を引くべきか？
- どの機能をどの層に
  入れるべきか

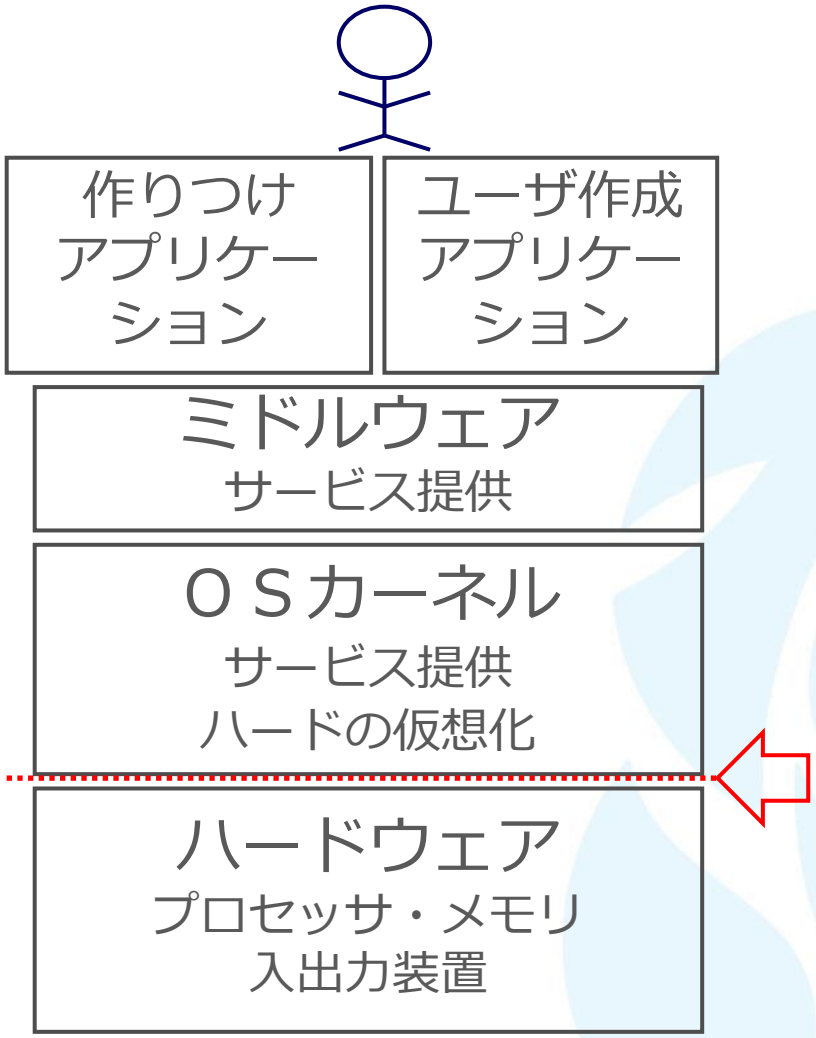
理由があるのか？

それなりに理由はあります

それなりに理由はあります

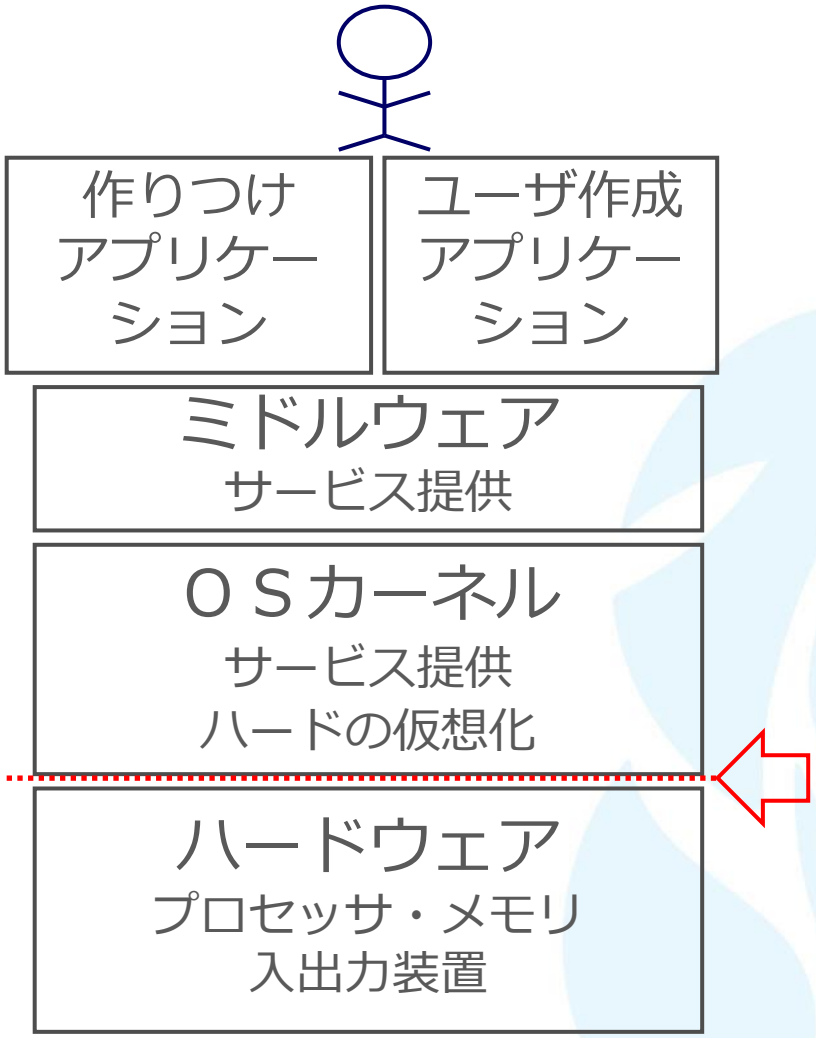
- ややこしいのでさぼりましたが、
  それなりに理由があります

ハードウェアの境界



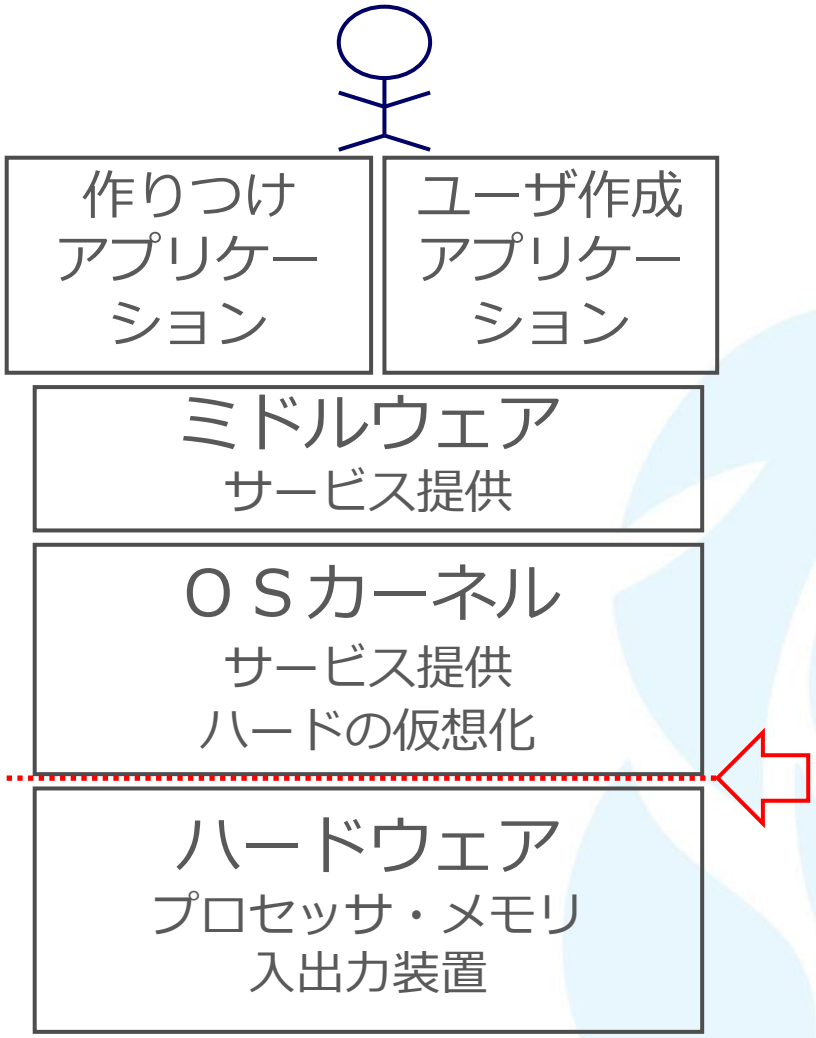
- ハードとソフトの境界は、

ハードウェアの境界



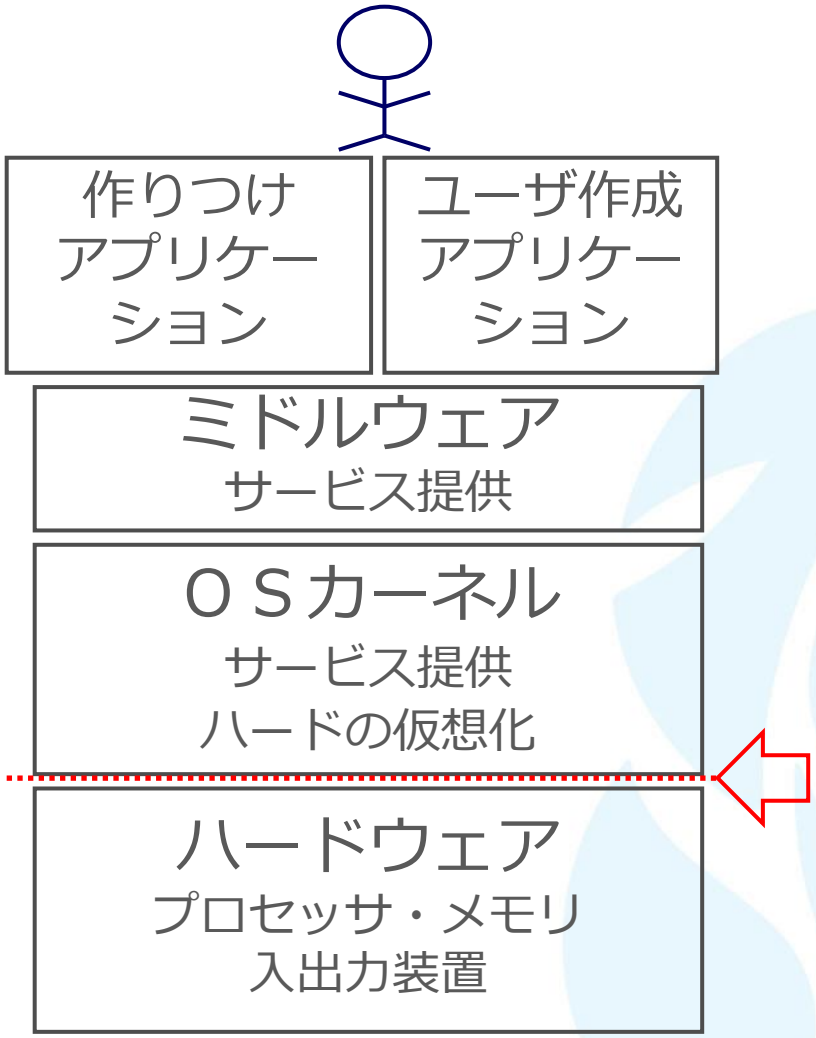
- ハードとソフトの境界は、命令にあります

ハードウェアの境界



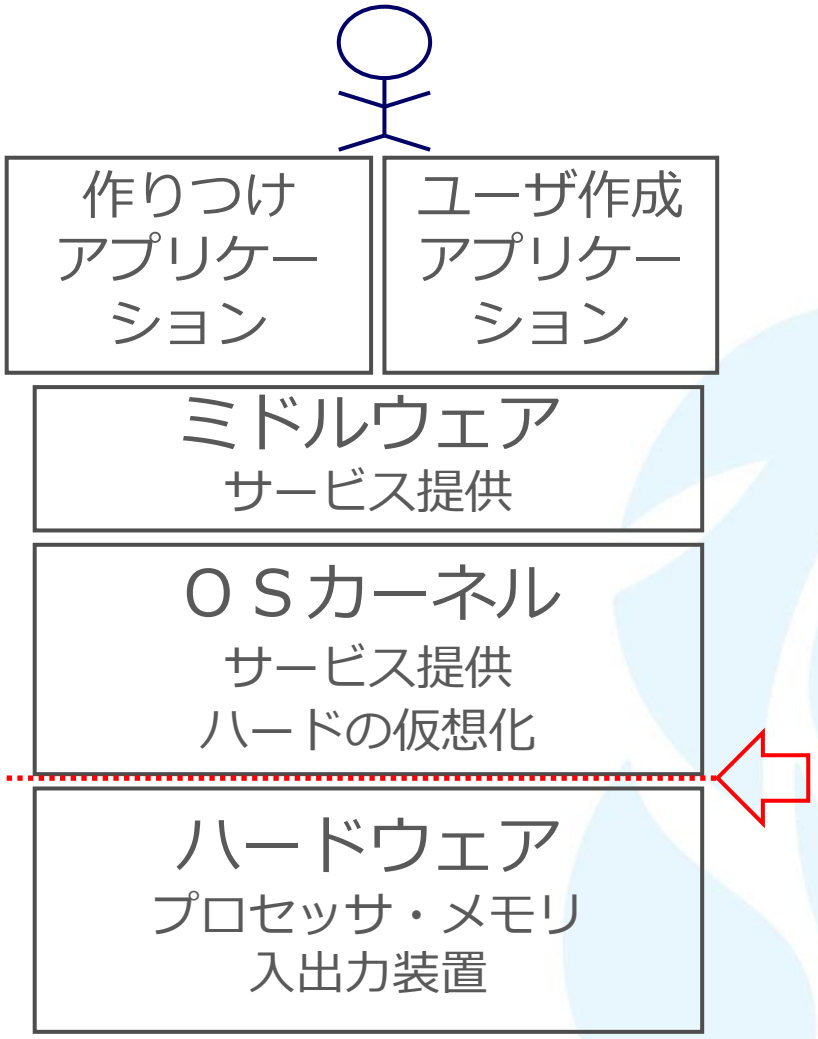
- ハードとソフトの境界は、命令にあります
- 命令で書かれたのがソフトウェア

ハードウェアの境界



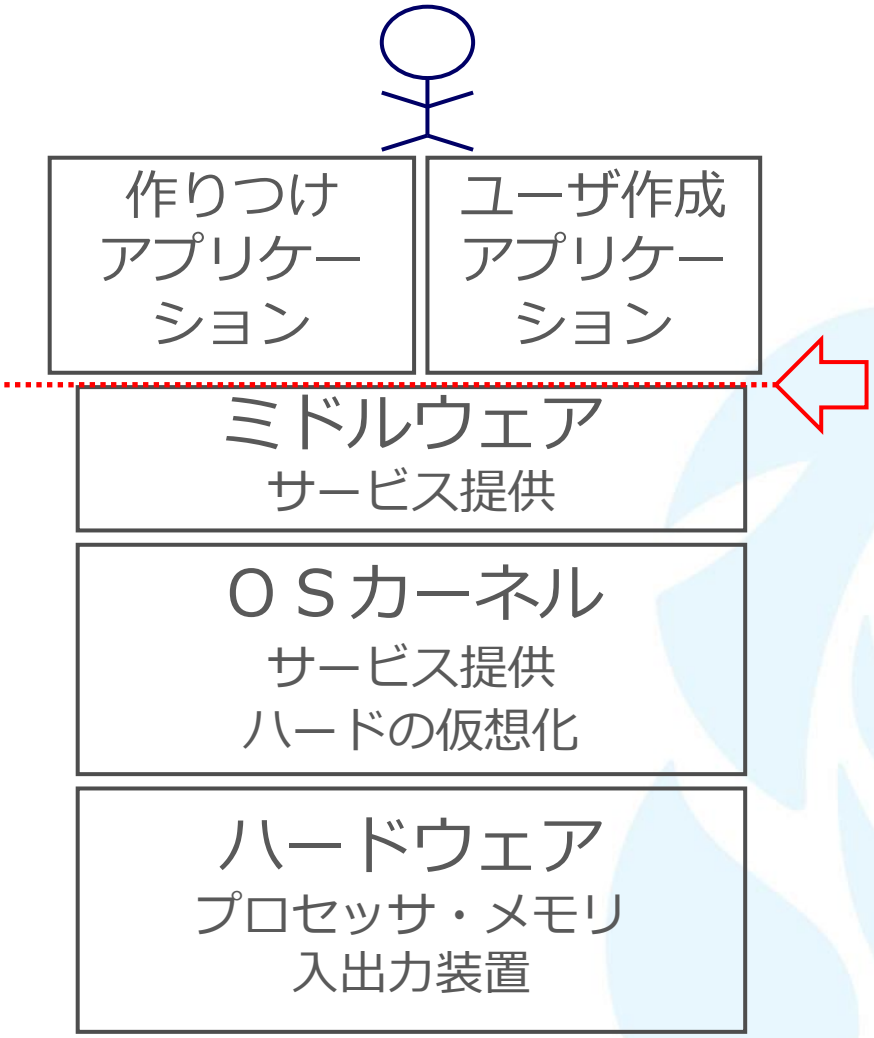
- ハードとソフトの境界は、命令にあります
- 命令で書かれたのが
  ソフトウェア
  その命令を解釈実行するのがハードウェア

ハードウェアの境界



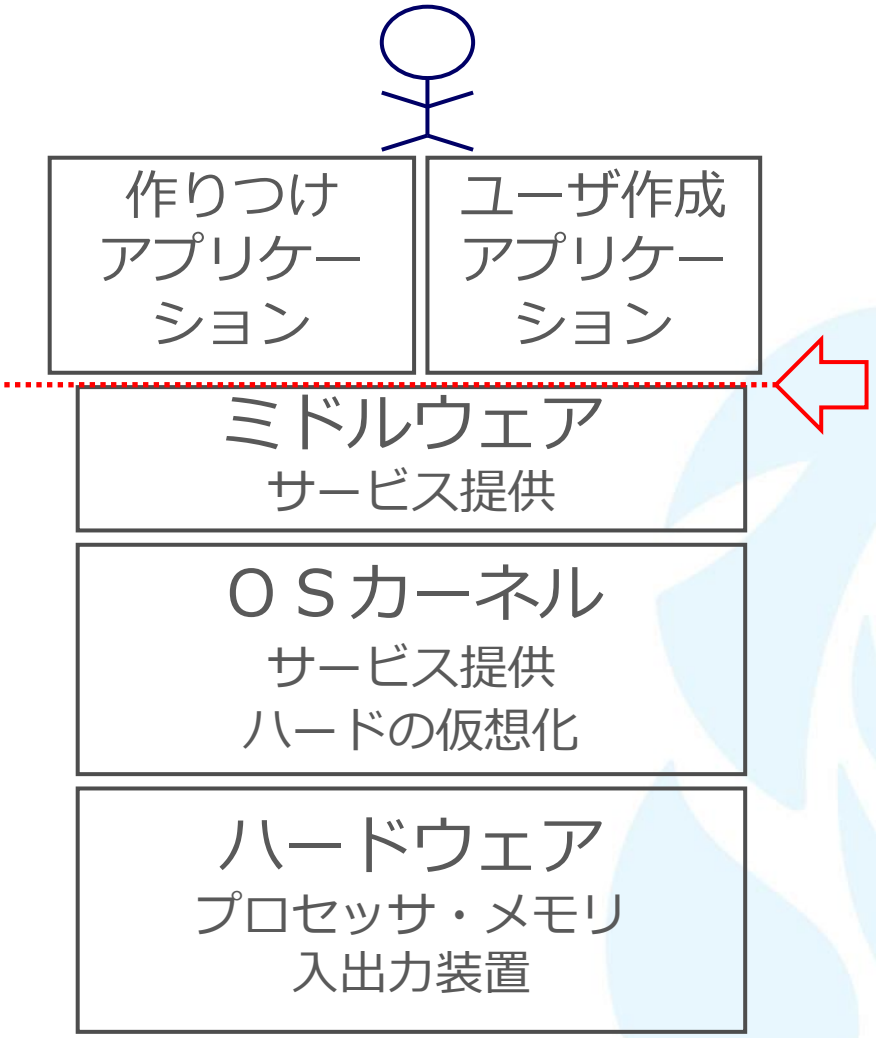
- ハードとソフトの境界は、命令にあります
- 命令で書かれたのが
  ソフトウェア
  その命令を解釈実行するのがハードウェア
- CPUのカナモノが決まれば境界は決まります

OSとアプリの境界



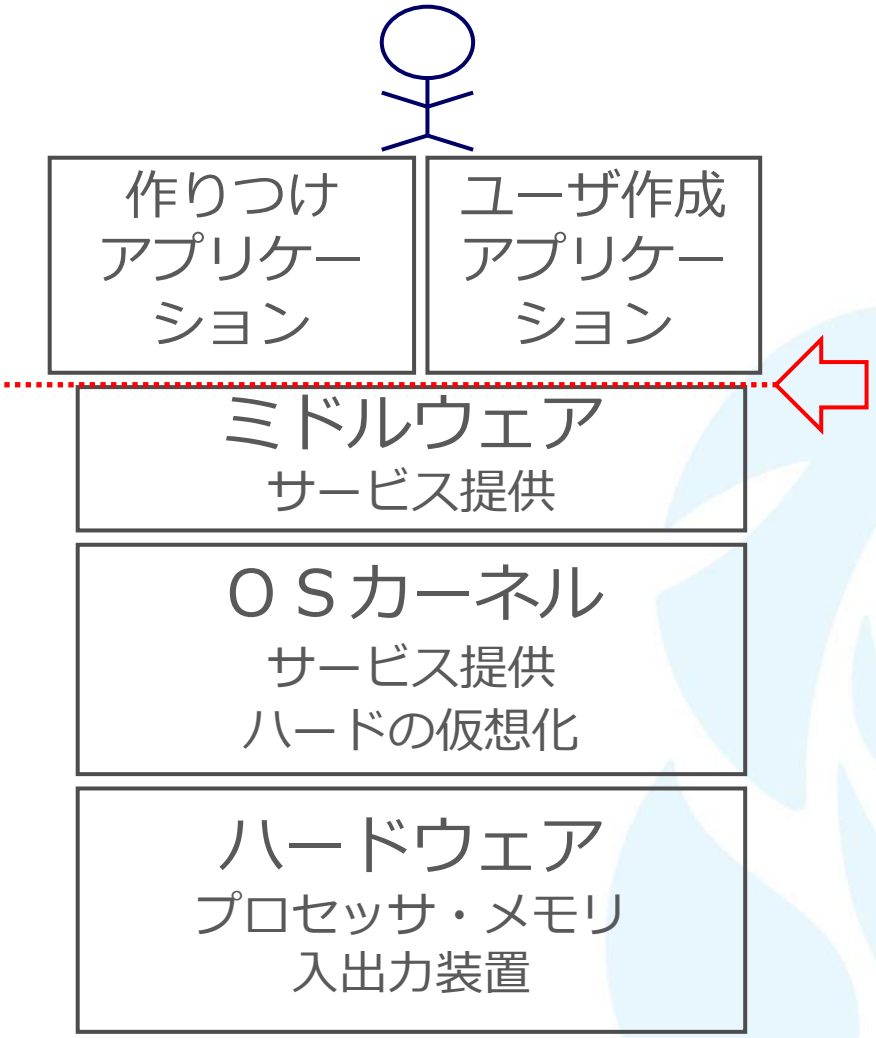
- OSとアプリの境界は、

OSとアプリの境界



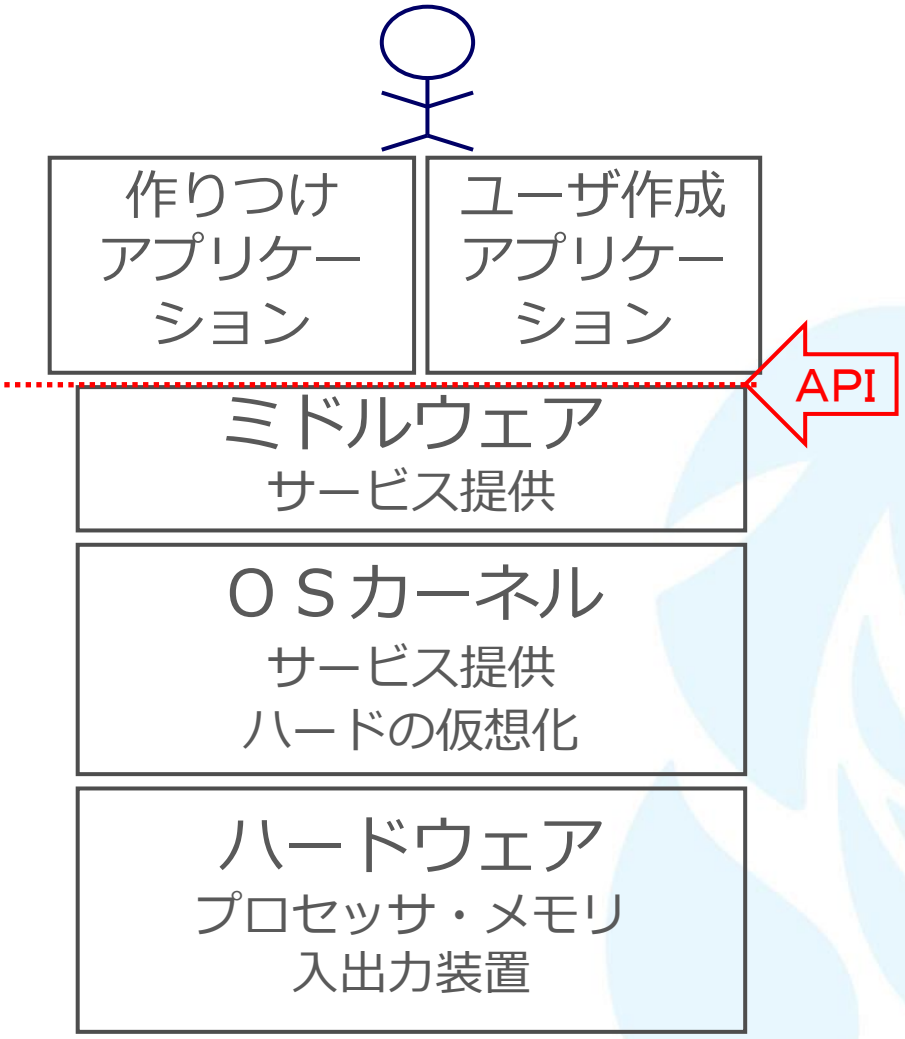
- OSとアプリの境界は、OSのサービスで決まります

OSとアプリの境界



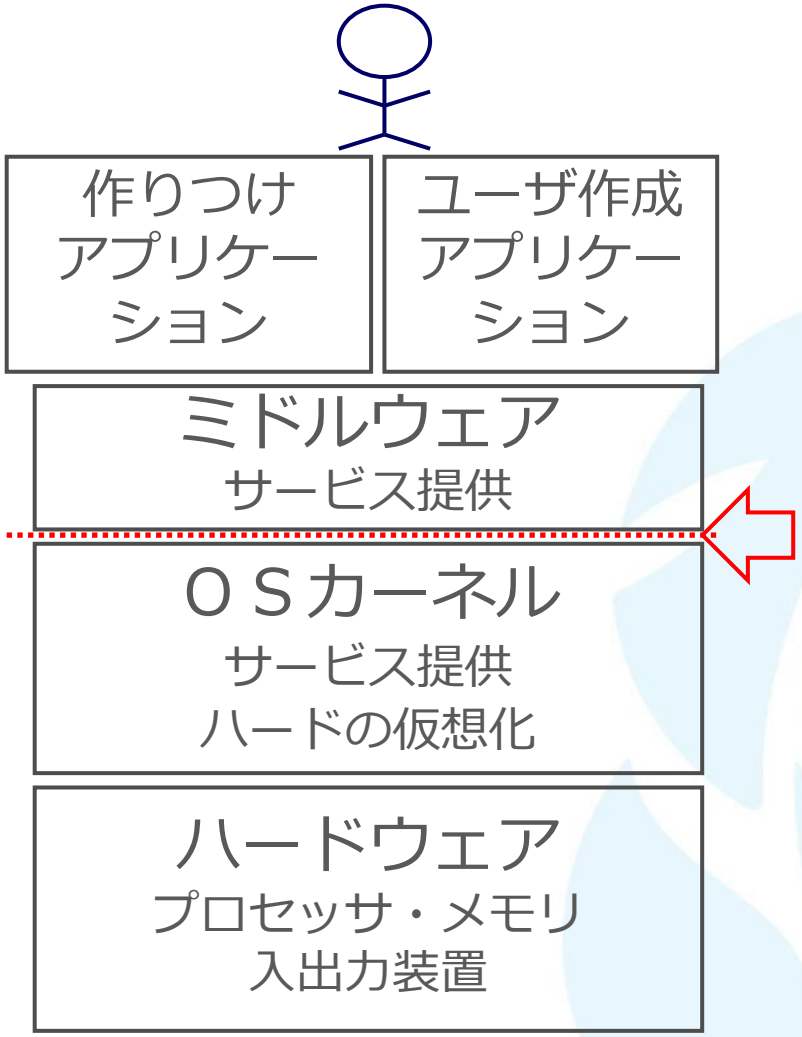
- OSとアプリの境界は、OSのサービスで決まります
- どんなサービスを提供するか、です

OSとアプリの境界



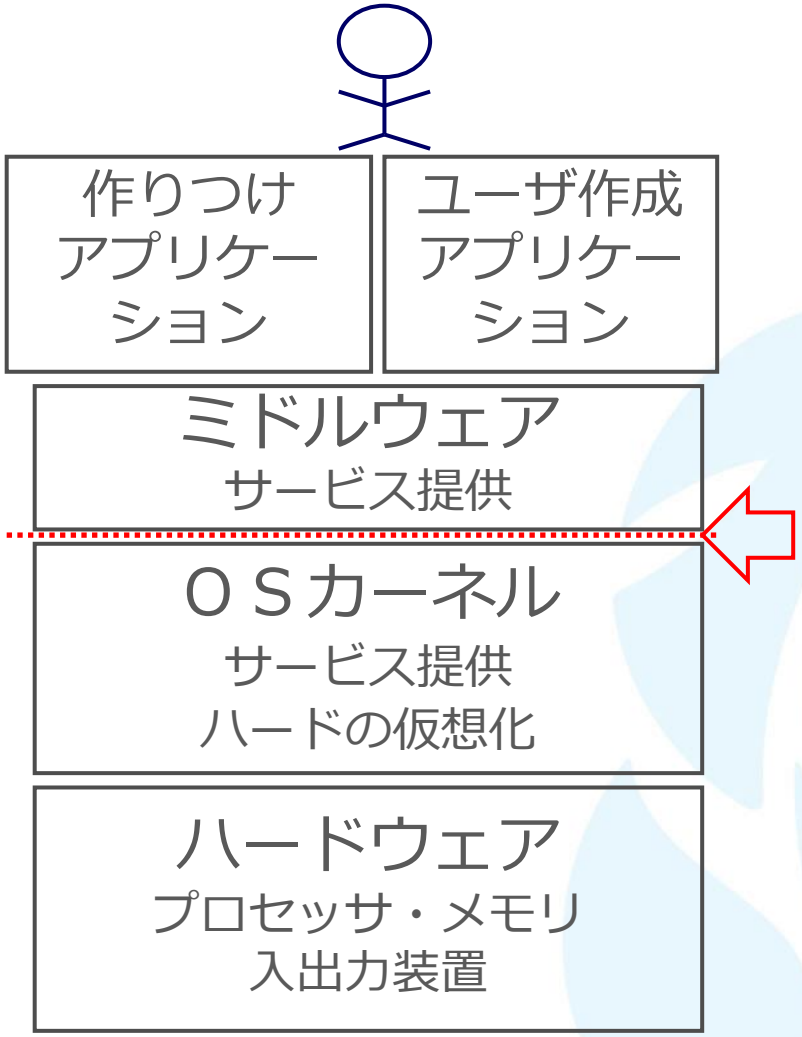
- OSとアプリの境界は、OSのサービスで決まります
- どんなサービスを提供するか、です
- アプリはAPIを介してサービスを利用します (Application Interface)

OSカーネルとカーネル外との境界



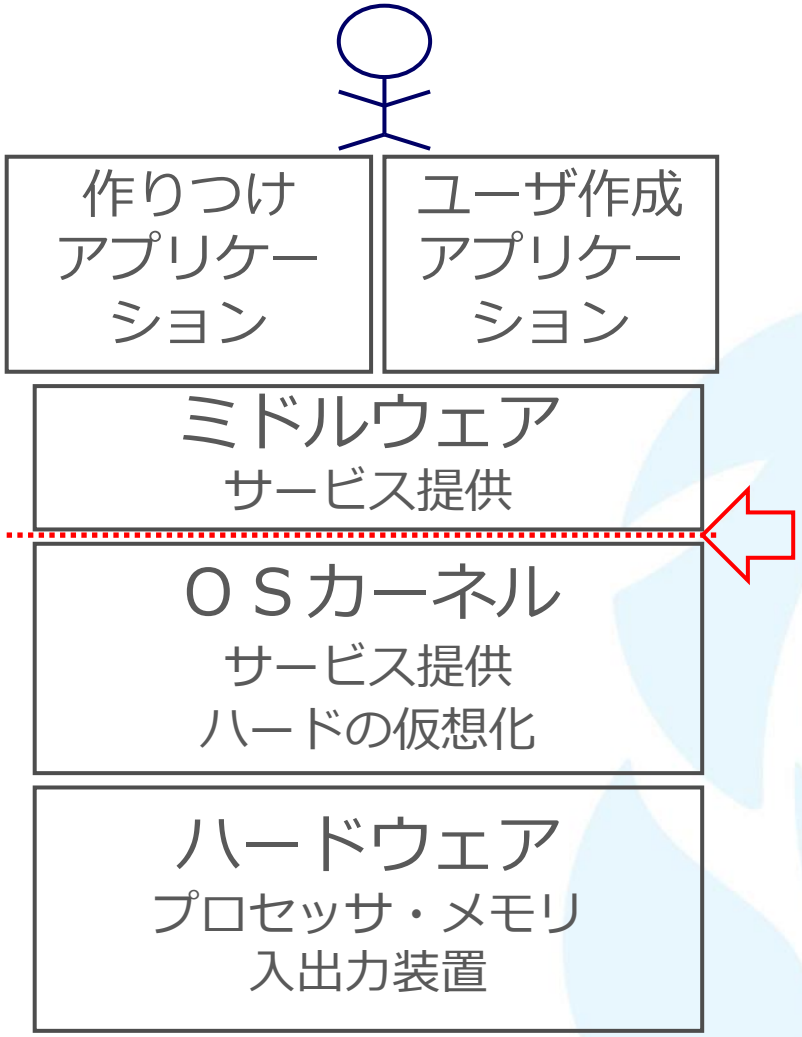
- カーネルの境界は

OSカーネルとカーネル外との境界



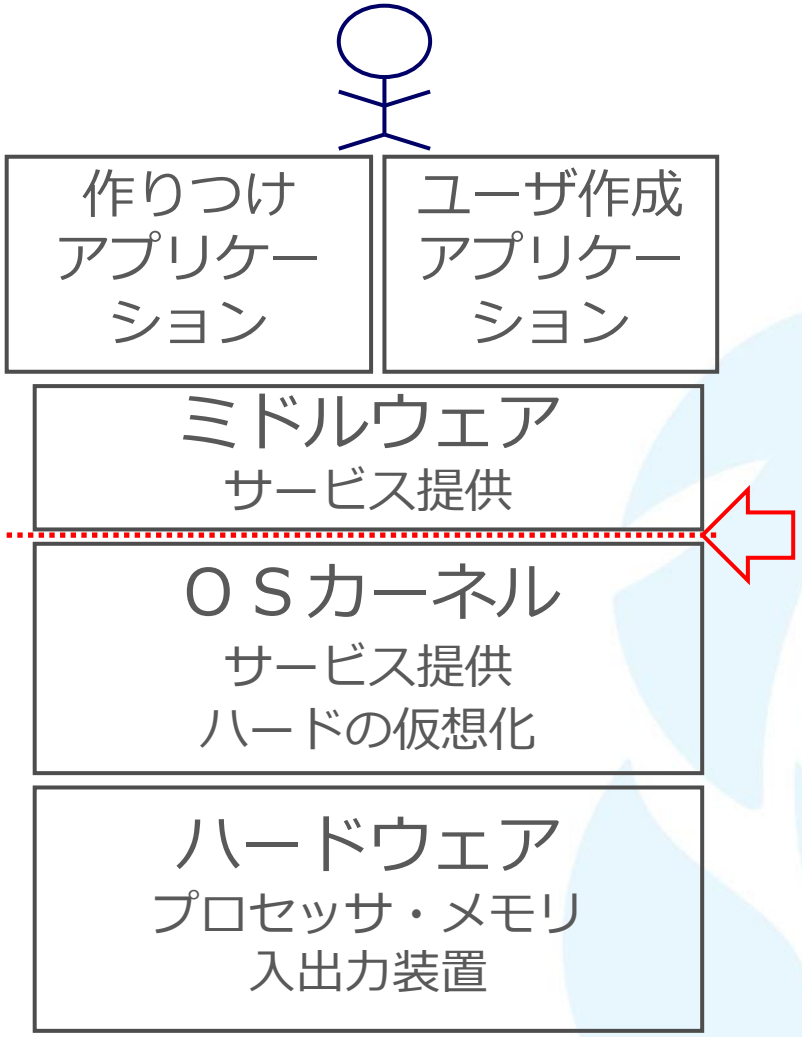
- カーネルの境界は
  実は保護の境界です

OSカーネルとカーネル外との境界



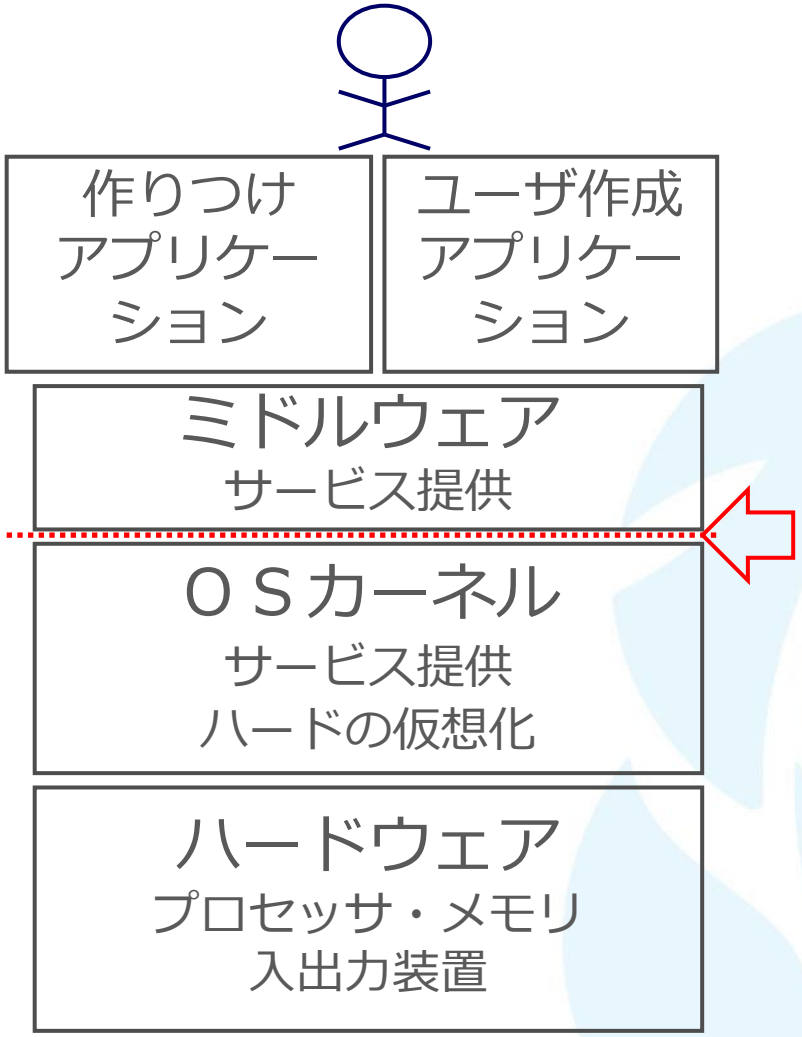
- カーネルの境界は
  実は保護の境界です
- カーネルは

OSカーネルとカーネル外との境界



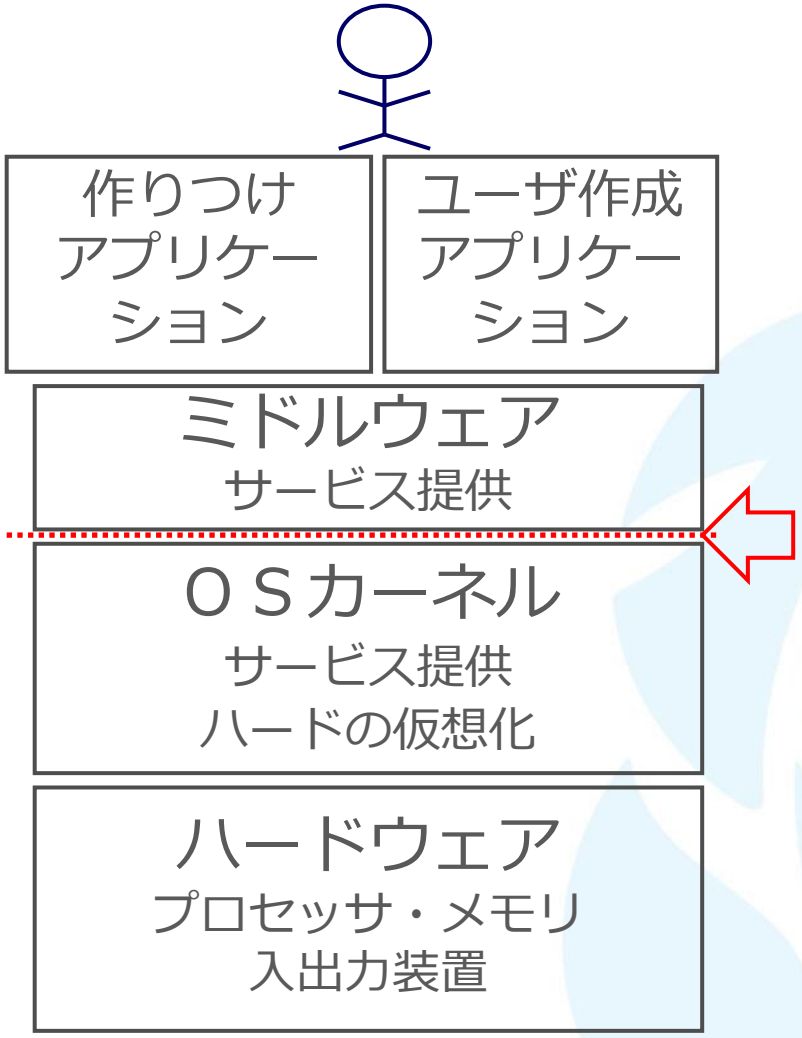
- カーネルの境界は
  実は保護の境界です
- カーネルは
  - ハードを直接操作し、

OSカーネルとカーネル外との境界



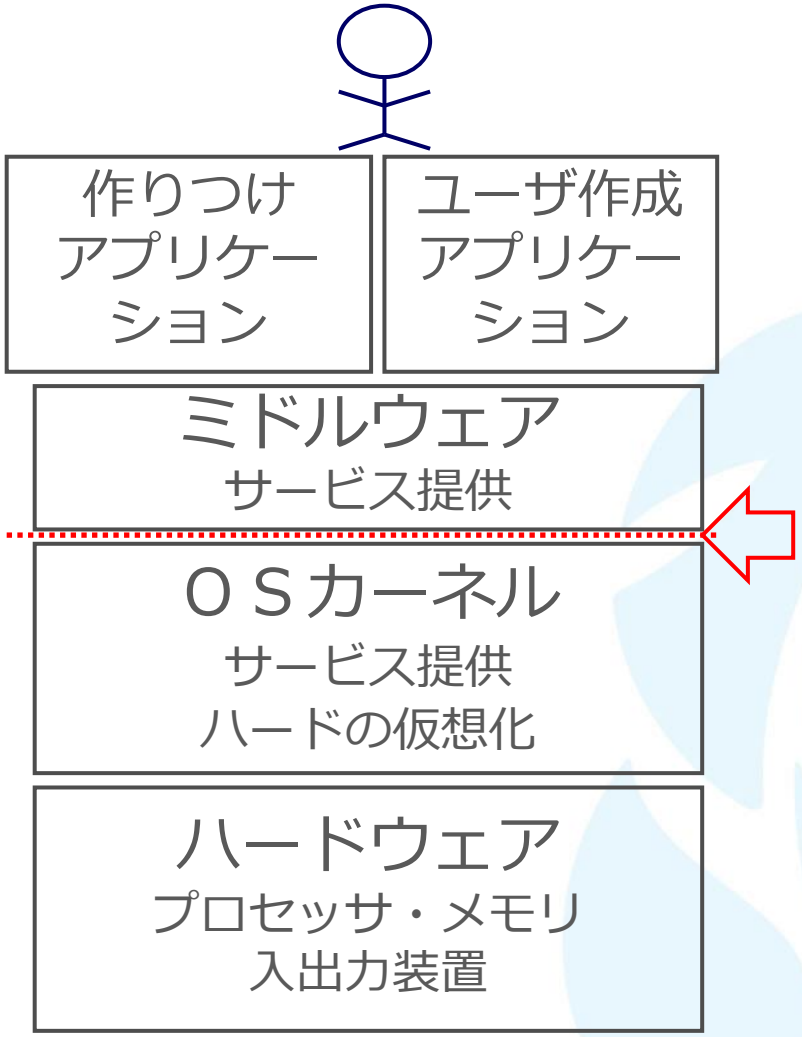
- カーネルの境界は
  実は保護の境界です
- カーネルは
  - ハードを直接操作し、
  - 外部(上位)からの勝手なアクセスを禁じ、ハードを保護する役目を持つ

OSカーネルとカーネル外との境界



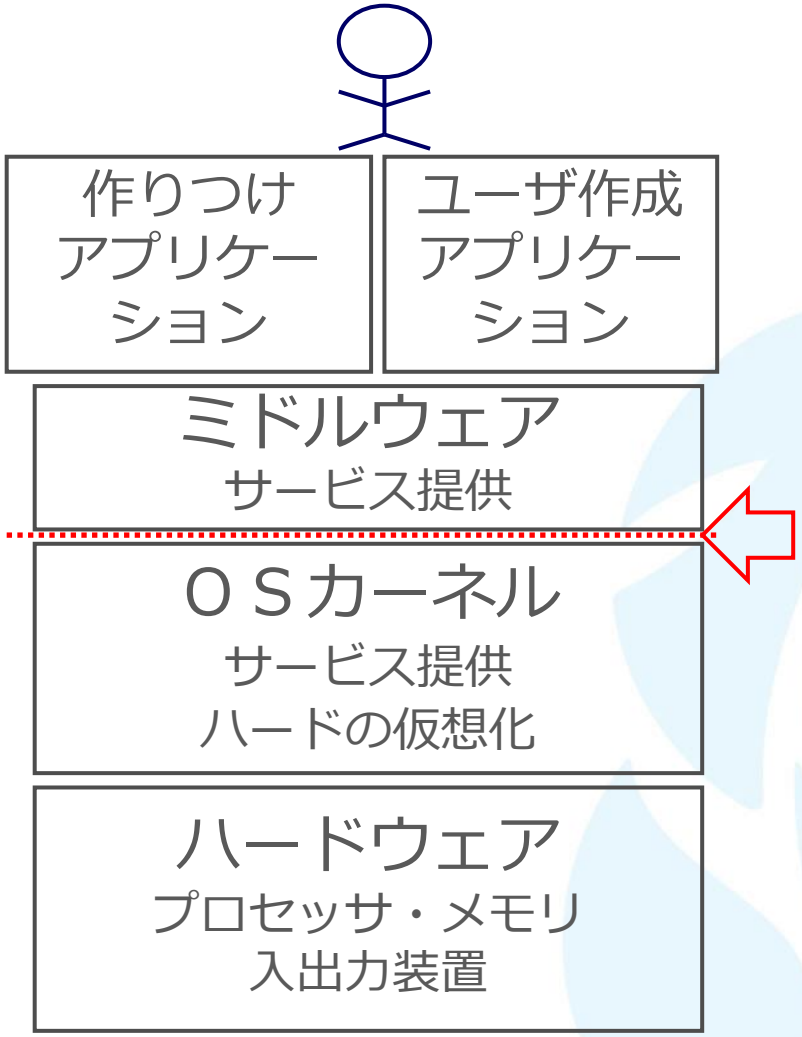
- カーネルの境界は
  実は保護の境界です
- カーネルは
  - ハードを直接操作し、
  - 外部(上位)からの勝手なアクセスを禁じ、ハードを保護する役目を持つ
- なので、 (ハードによる)
  物理的な保護の仕組がある

OSカーネルとカーネル外との境界



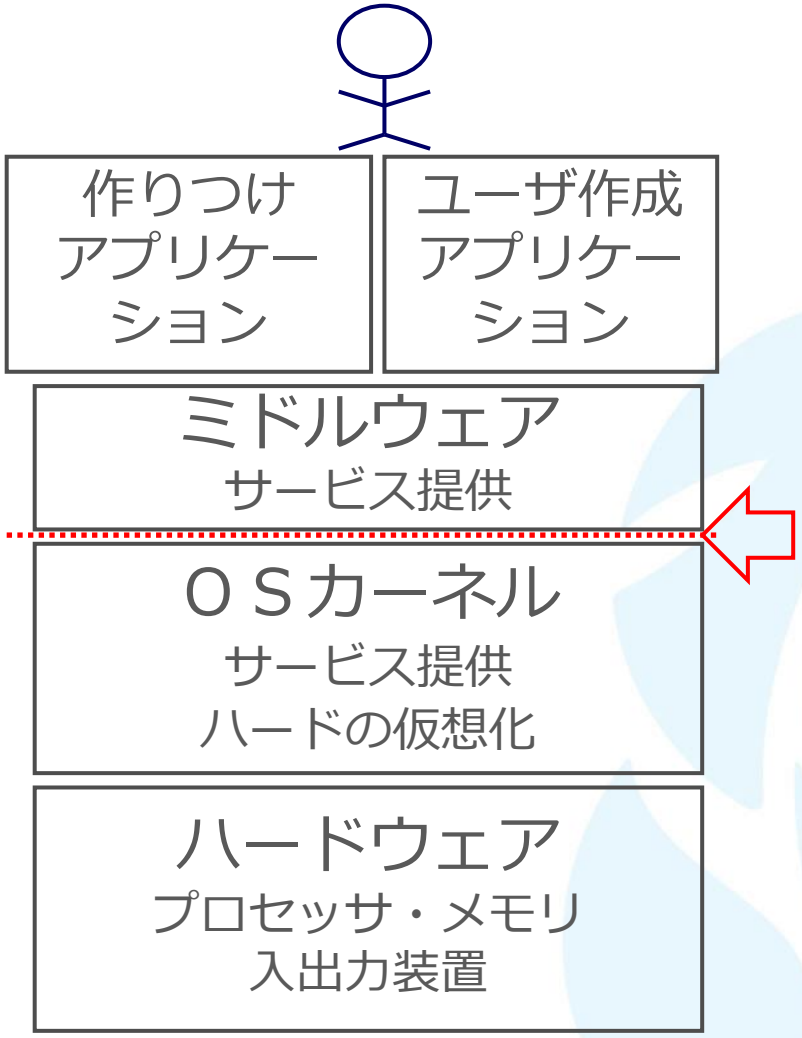
- この境界の内側か外側かの違いが、
  カーネル内と外の差

OSカーネルとカーネル外との境界



- この境界の内側か外側かの違いが、カーネル内と外の差
- 保護の基本は
  - 共有されるハードを他のプログラムから守ること

OSカーネルとカーネル外との境界



- この境界の内側か外側かの違いが、カーネル内と外の差
- 保護の基本は
  - 共有されるハードを他のプログラムから守ること
  - ハードを守る仕組みを壊されないこと

保護の細かい話は別にして
それぞれの階層の境界の
理由が分かりましたか？

さて
カーネル保護の仕組の説明です
（面倒な人は飛ばしてもOKです）

カーネル保護のやりたいこと

- システムは多くのユーザが使う (ネットからを含めて) ので悪意や自分優先の要求がある
  - 悪意・ずる・誤りで、壊してしまうかも知れない
- ハードを共有させている管理ソフト (特にカーネル) は、安全に使わせなければならない
  - ルールを守らせるためには、カーネルを自由に書き換えたり実行されたりすると困る (禁じたい)
  - (保護機構自身も壊されては困る)

カーネル保護の登場人物

- ハードウェア
  - CPUの実行モード、　モード切替機構
  - メモリのアクセス制御（実行を禁じる）
- ソフトウェア
  - 割込みの活用　～　後で詳しく触れる
  - カーネルの構造　特定の入口だけ入れる

CPUの実行モードとは

- ハードウェアで定義されたもの
  - ソフトで書き変えられない機構

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類
  - （より凝ったCPUもあるが）

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類
  - （より凝ったCPUもあるが）
  - CPU内の特権モードフラグのビットが立つ

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類（より凝ったCPUもあるが）
- 特権モードのハード制約は

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類（より凝ったCPUもあるが）
- 特権モードのハード制約
  - メモリに、特権モードのみで実行できるフラグを立てられる

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類（より凝ったCPUもあるが）
- 特権モードのハード制約
  - メモリに、特権モードのみで実行できるフラグを立てられる
    ⇒　「カーネルのプログラムは特権モードになっていないと実行できない」というようにできる

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類（より凝ったCPUもあるが）
- 特権モードのハード制約
  - メモリに、特権モードのみで実行できるフラグを立てられる
  - 特権モードに入れるのは、割込みが起こるか、SVC命令を実行した時だけ（勝手に移れない）

CPUの実行モードとは

- ハードウェアで定義されたもの
- 特権モード（カーネルモード）と
  ユーザモードの２種類（より凝ったCPUもあるが）
- 特権モードのハード制約
  - メモリに、特権モードのみで実行できるフラグを立てられる
  - 特権モードに入れるのは、割込みが起こるか、SVC命令を実行した時だけ（勝手に移れない）

スーパーバイザ・コール命令

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行

カーネルのメモリを特権モードのみ実行許可

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行
- 特権モードに移る時（割込み・SVC命令）
  必ず割込み処理プログラムを実行させる

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行
- 特権モードに移る時（割込み・SVC命令）
  必ず割込み処理プログラムを実行させる

実はSVC命令は、内部的に割込発生で実現する

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行
- 特権モードに移る時（割込み・SVC命令）
  必ず割込み処理プログラムを実行させる
- これによって
  - ユーザがカーネル内の好きな部分を実行することはできない

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行
- 特権モードに移る時（割込み・SVC命令）
  必ず割込み処理プログラムを実行させる
- これによって
  - ユーザがカーネル内の好きな部分を実行することはできない

ジャンプして飛び込んでもモード違反で実行不可

東邦大学

で、以下の設定にする

- アプリはユーザモードで実行、
  カーネルは特権モードのみで実行
- 特権モードに移る時（割込み・SVC命令）
  必ず割込み処理プログラムを実行させる
- これによって
  - ユーザがカーネル内の好きな部分を実行することはできない
  - 必ず、特定の入口 (割込み処理) を経て入るので入口で変な指定をしていないかチェックできる

更に

- 入出力命令を特権命令とし
  （特権モードでないと実行できない命令）
  ユーザモードでは入出力機器を扱えない
  ようにする

更に

- 入出力命令を特権命令とし
  （特権モードでないと実行できない命令）
  ユーザモードでは入出力機器を扱えない
  ようにする
- システムを制御するレジスタ等も
  特権モードでないと扱えないようにする

更に

- 入出力命令を特権命令とし
  （特権モードでないと実行できない命令）
  ユーザモードでは入出力機器を扱えない
  ようにする
- システムを制御するレジスタ等も
  特権モードでないと扱えないようにする

などによってユーザから保護する

カーネル保護の仕組はやっかいなので
ざっと理解しておけば良いでしょう

本当に必要になった時に
もう一度復習して下さい

カーネル保護の考え方が
分かりましたか？

次へ

東邦大学