Androidの仕組みと
安全なスマフォの可能性

iPhone（iOS）は対象外です

iPhoneが対象外の理由

- iPhoneにはiOS以外のOSが入れられません
- Apple以外を使うことができません

スマフォ監視の恐ろしさ

- 何をどれだけ監視されているのかわからない
- 「監視していますよ」とは伝えてくれない
- しかし、「監視している」事実が時々ニュース記事にも出てきている

CIAのような第三者の監視の事実

- 2017のWikileaksの暴露「Vault 7」
- CIAがあらゆる機器やOSのバグを見つけ、そこから侵入し、大衆監視を行っていた
- 例えば、Samsungのカメラ付き・ネット接続テレビに侵入し、お茶の間を監視することも可能

Google Mapでの私の経験

- Google Map画面を見て「この店を評価しろ」と出ているのに気がついた
- しかし、その店は、Google Mapの目的地として設定していなかった。高速道路のサービスエリア（SA）だったから。
- そのSAに長時間留まったことを、Google Mapは知っていたのだ。

そもそもAndroidとは？

そもそもAndroidとは？

- パソコンと同じで、機械は「ソフトなければただの箱」
- スマートフォン機械に載せるOS（オペレーティングシステム）
- OSの上で各アプリが動作している

アプリレベルでの監視

IT企業の監視ポイント1～スマフォアプリ

- facebookやTwitterなどのスマフォ用「専用アプリ」で監視する
- 基本的にその上で行うことはすべて記録されていると思ってよい
- これらのアプリに録画・録音を許可していると、いつ行われているかわからない
- その機能が必要であれば、スマフォアプリはできる限り排除し、ブラウザベースの機能に切り替える

悪質な例

- facebookのmesseger
  - パソコン上ではブラウザで使用できるのに
  - スマフォ上では必ずアプリを要求される
- どうしてもアプリを使わせたい

IT企業の監視ポイント2～ブラウザでの利用

- 当然だが、ブラウザで利用しても監視はされている
- ログインし、その個人だと特定されているから
  二段階認証なる理由で電話番号も要求する

当然だが。。。

- このようなサービスを可能な限り減らすこと
- Facebook、Twitter、Google、Instagram。。。
- ログインして何かしらすれば、それはすべて監視され、記録され、個人が特定される。

「安全なスマフォ」に変えても。。。

- たとえ「安全なスマフォ」に変えても、これらのサービスを使う限り、監視はされ続けることに注意が必要
- しかし、現在のところ必要不可欠。可能な限り安全にするには？あるいは、代替の「サービス」はあるのか？

OSレベルの監視

GoogleはOSレベルで監視している

- Googleの監視装置が、OS(Android)に組み込まれており、常に好き放題監視している（と思ってよい）。

Androidの中身を良く見てみると。。。

- Androidのベースはオープンソース（AOSP）
- 悪さをするのは、その上に乗っているプロプライエタリ「Google Play」
- もしかして「各社プログラム」も悪さを？
- 各社スマフォは、Google Playを組み込んだ形で出荷されている（何をしてるかわからない）

オープンソースとプロプライエタリの違い

- オープンソースは、その設計図が公開されており、誰でも見ることができる。おかしな機能があれば、すぐに誰かが見つけてしまう。
- プロプライエタリは、私有ソフト。ノウハウを守るために設計図は公開されていない。が、逆に「どんな悪さをしているのか、わかったものではない」。

AOSP

- オープンソース、つまり設計図がすべて公開されているので、監視するようなプログラムを入れるとすぐにバレるため、監視機能は入っていない
- しかし、AOSPだけではOSとして機能しない

Google Play

- アプリストア(Play Store)や各種APIが提供される
- 一部アプリ(例えば、Google Map機能を利用するもの)では、Google Playが必須になる(実際にはAPI)。

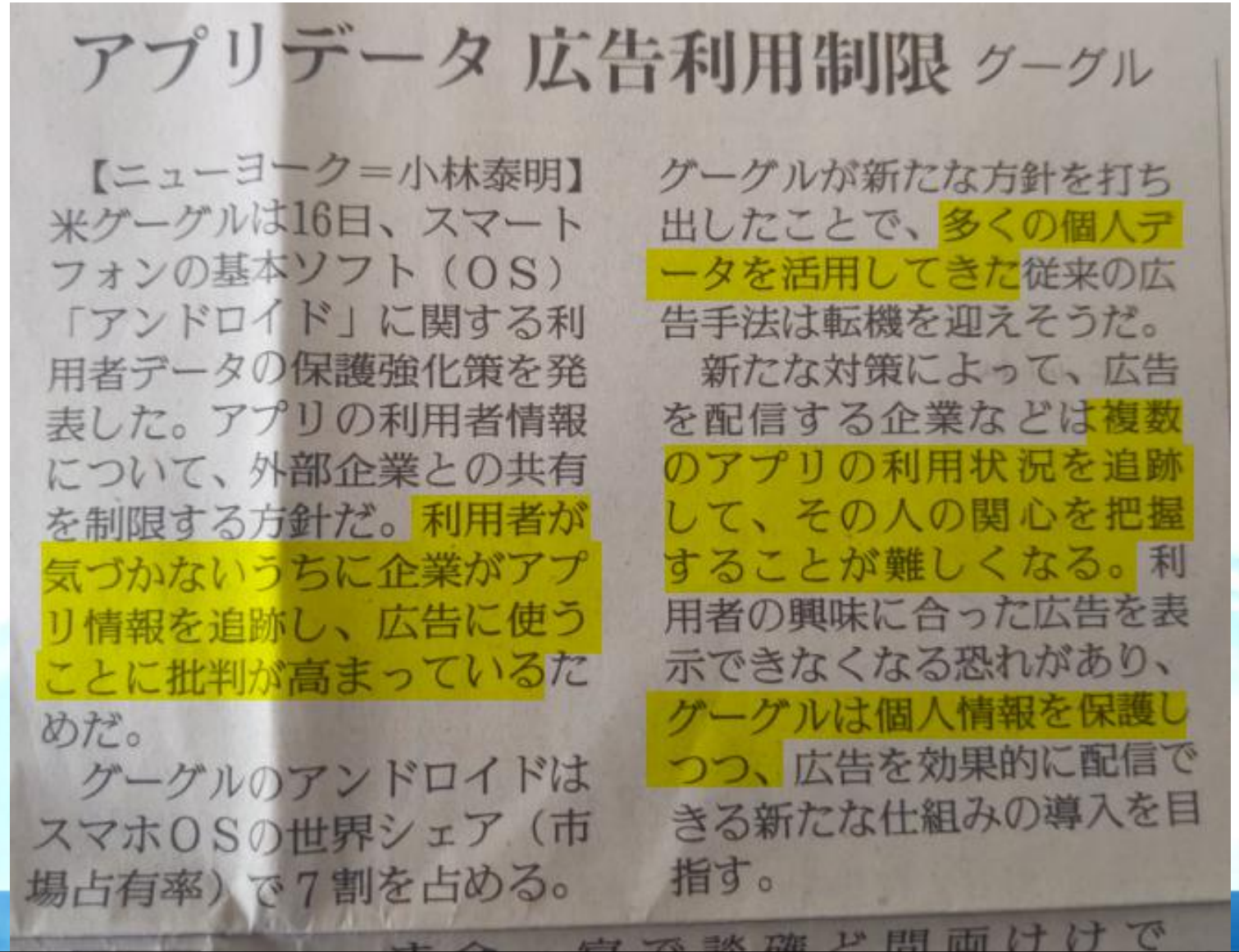
- Google Playの中身は一切わからない(設計図非公開)
- GoogleがAndroidスマフォを監視するための主要な手段
- つまり、Googleのサービスを一切使わなくても監視される

Google Playが必要なアプリの例

- 自転車レンタルアプリ
  GoogleのAPIに頼って地図を表示

2022/2の読売記事

- 個人情報保護を報道しているもののGoogleの個人情報取得を是認



アプリデータ 広告利用制限 グーグル

【ニューヨーク＝小林泰明】米グーグルは16日、スマートフォンの基本ソフト（ＯＳ）「アンドロイド」に関する利用者データの保護強化策を発表した。アプリの利用者情報について、外部企業との共有を制限する方針だ。利用者が気づかないうちに企業がアプリ情報を追跡し、広告に使うことに批判が高まっているためだ。

グーグルのアンドロイドはスマホＯＳの世界シェア（市場占有率）で７割を占める。グーグルが新たな方針を打ち出したことで、多くの個人データを活用してきた従来の広告手法は転機を迎えそうだ。

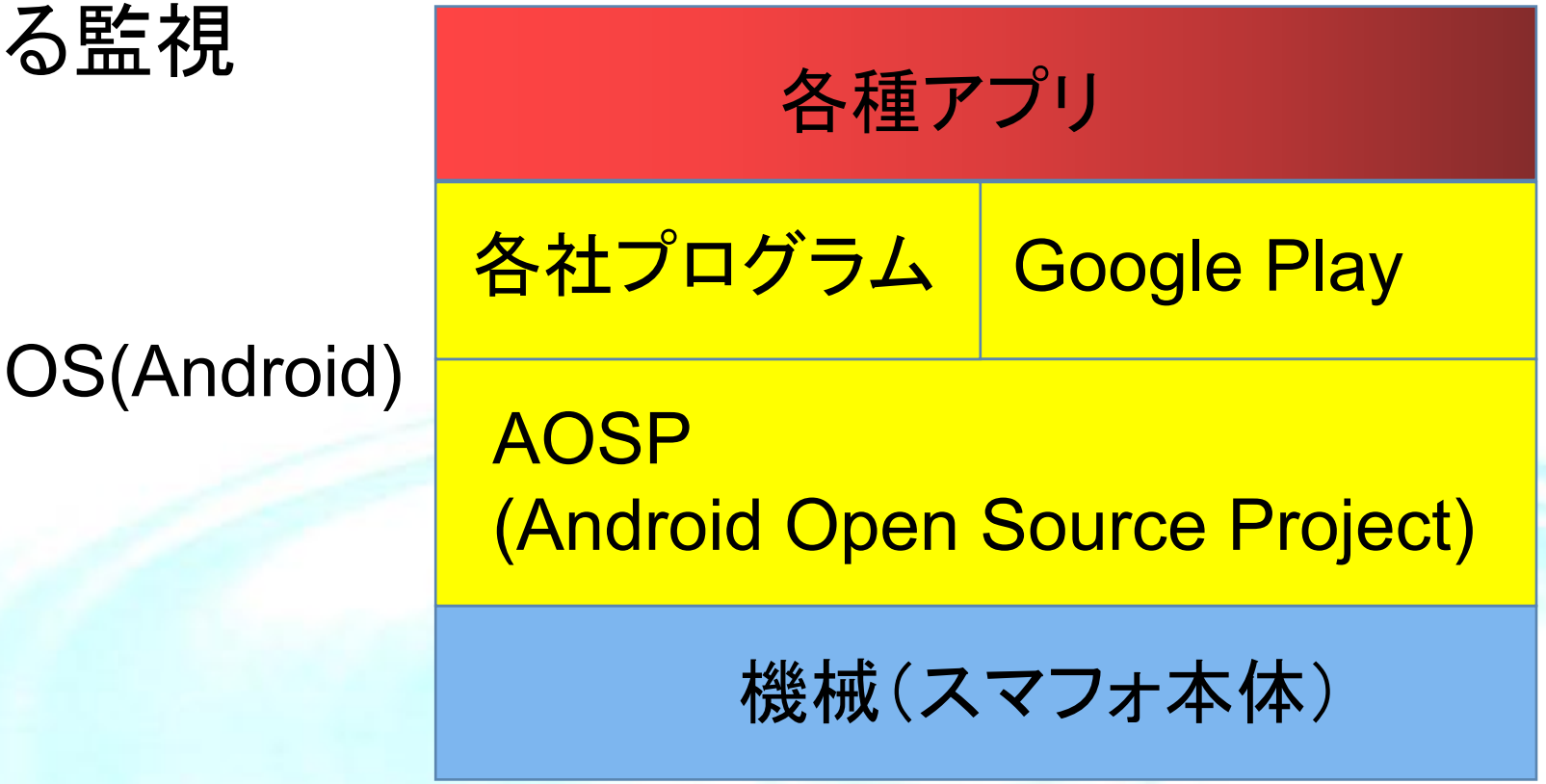
新たな対策によって、広告を配信する企業などは複数のアプリの利用状況を追跡して、その人の関心を把握することが難しくなる。利用者の興味に合った広告を表示できなくなる恐れがあり、グーグルは個人情報を保護しつつ、広告を効果的に配信できる新たな仕組みの導入を目指す。

プライバシー侵害訴訟

- Googleに対する訴訟が米国では何件も起こっている

ここまでのまとめ

- アプリで監視、ブラウザ利用での監視（スマフォに関わらず）
- Google Playによる監視
  （特権がある）



機械本体での監視は可能か？

不可能

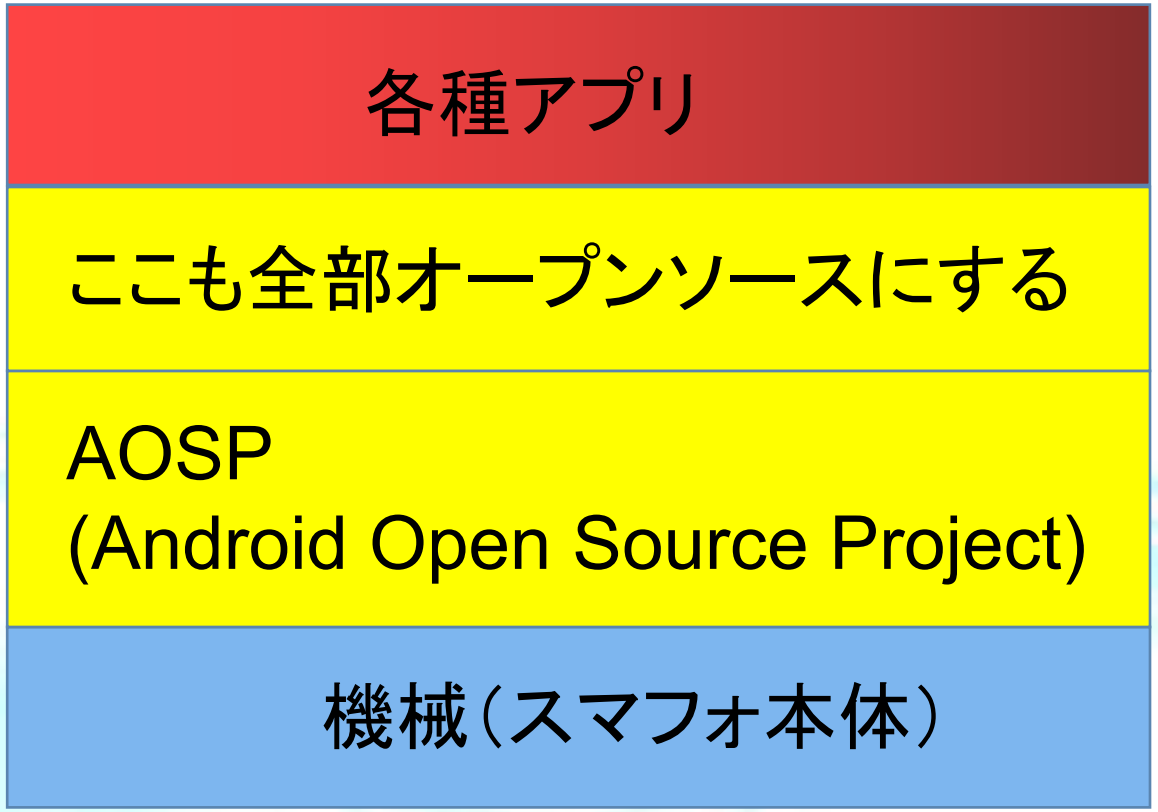
- 機械自体に監視機能を入れた場合、OS側が指示してもいない通信が勝手に発生してしまい、すぐにバレるため
- 仮に機械自体に監視機能があっても、それを送信できなければ意味がない

したがって

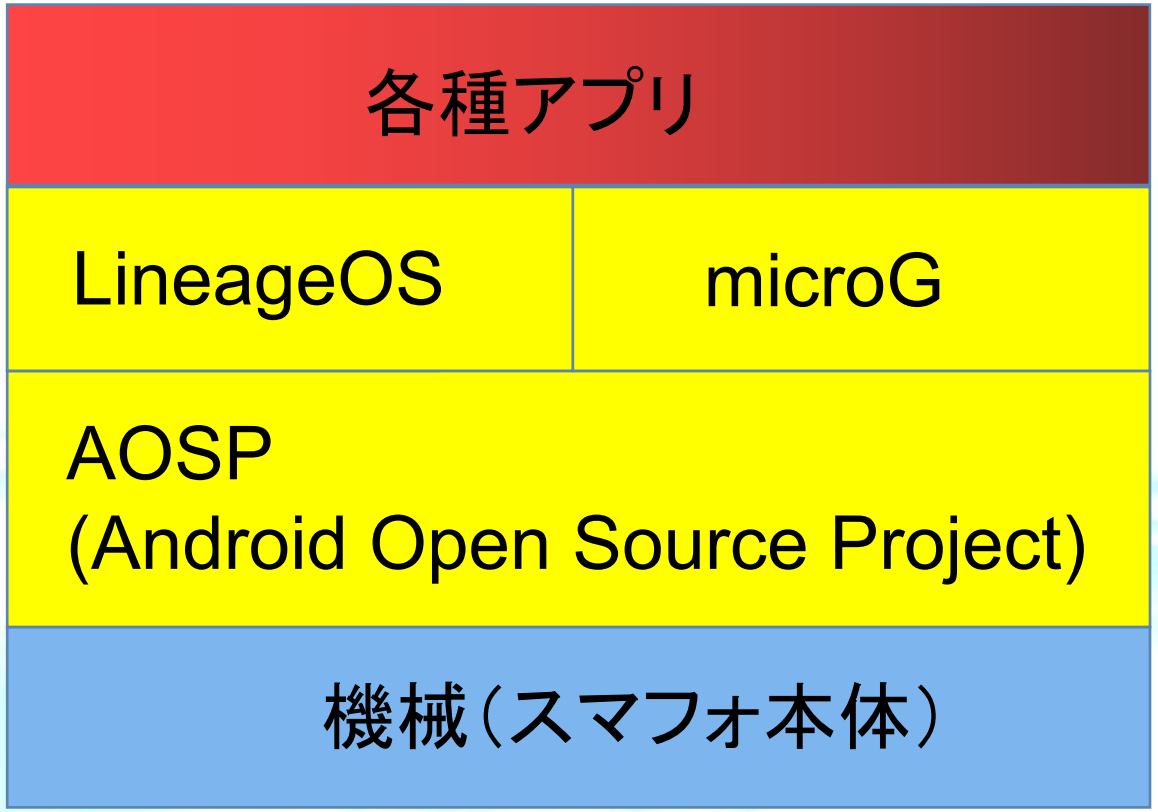
- AOSPを使うが、Google Playその他プロプライエタリなものをを使わないOSを利用する
（あるいは、使っても安全な形態のもの）
- 機械自体は、そのOSが入るならば何でもよい
- しかし、OSを変えただけではダメで、その上のアプリに気を配る必要がある

カスタムROMとは

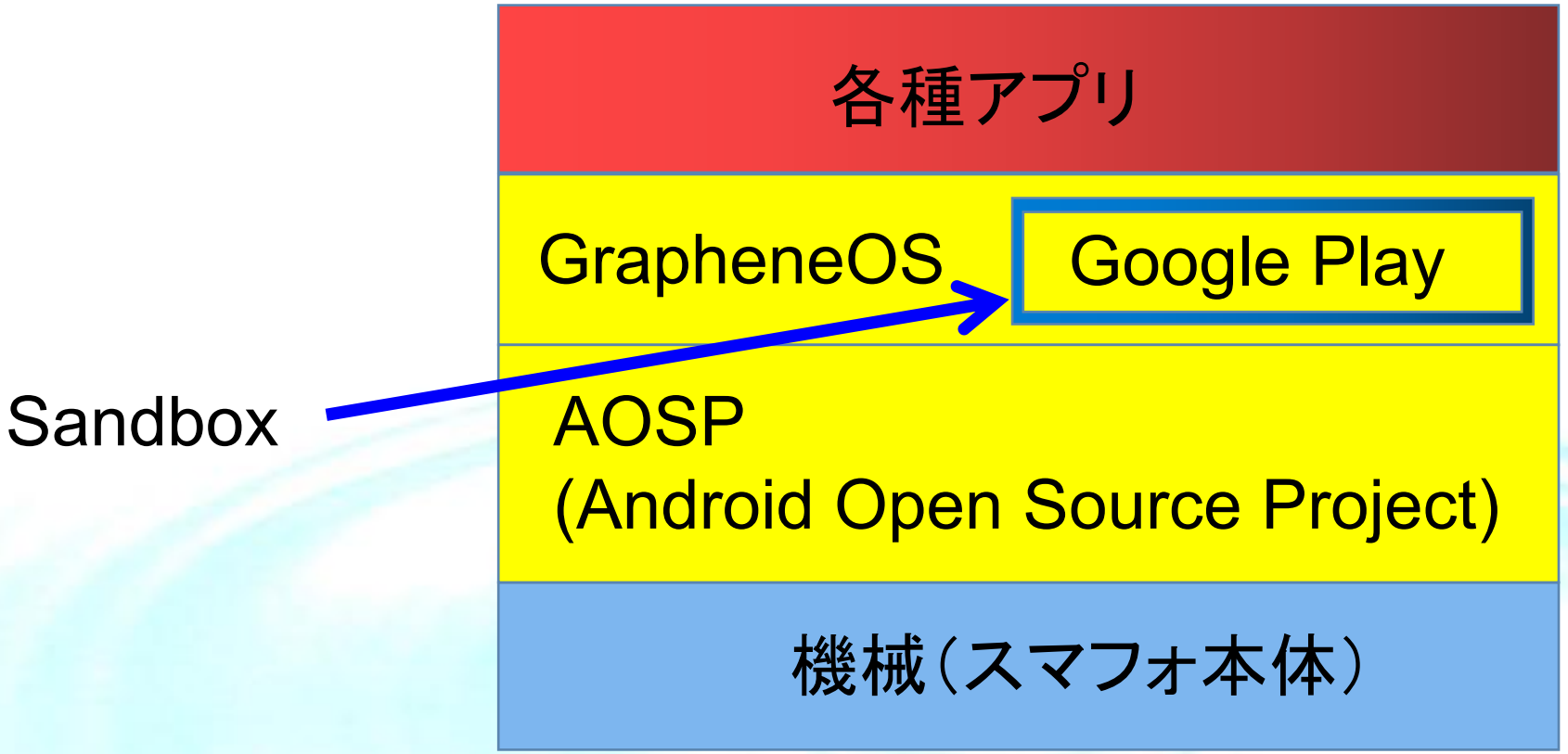
- 基本的には、OS部分をすべてオープンソースに
- ただし、Google Playを
  必要とするアプリもある



- Google Playを追い出し、独自のプログラムを使う（LineageOSの方法）



- Google Playを使っても特権を与えない
（GrapheneOSの方法）



- オープンソースのAOSPを利用した独自のOSで、これ自体もオープンソース。Google Playを完全排除するか、あるいは特権を与えない
- これで、各スマフォメーカーの提供する（監視付きプロプライエタリの）OSを置き換える
- ハードウェアはそのまま。中身を安全なものに交換。

カスタムROMの種類

GrapheneOSの特徴

- エドワード・スノーデン「スマフォ使うならGrapheneOSにする」

- 最もプライバシーに配慮したカスタムROM、らしい
- ただし、Google Pixelシリーズのみ対応
- 各Pixel機種のGrapheneOSのサポート期間は、Googleの各Pixelサポート期間に準ずる
  （Google自体がサポートをやめた機種でのGrapheneOSのそれ以上のサポートは無し）
- サンドボックスにて、Google Playを「安全に」実行することで、ほとんどのアプリが動く

LineageOSの特徴

- GrapheneOSと異なり、様々な機種をサポートしている
- Google Playに代わるmicroGという仕組みで、Google Playを必要とするアプリの実行もできる（はず）。

CalyxOSの特徴

- 使用していないのでわかりません