DICOMO 2012

Androidアプリケーション動作時に安全性を高める動的制御に関する検討

A Study on Android Security Improvement at Application Runtime

情報セキュリティ大学院大学
林　里香，後藤　厚宏

2012/7/6

昨今話題のAndroid

♣ アプリが豊富

6/29時点Google Playに公開されているアプリ数: **472762**

出展：http://www.appbrain.com/stats/　（2012.6.30アクセス）

便利で楽しい！でも，中には怪しいアプリも・・・

♣ 動画を見たくてインストールしたら，電話帳の情報を抜き取られた！

ex.『～ the Movie』 (2012.4)

♣ 知らない間に位置情報が送信されてる？！

⇒アプリに組み込まれた広告機能の動作

本日のテーマ

気付いて！

これ怪しいアプリかも

安全性を確保するために

♣ その１

“権限”が怪しいアプリは，
ダウンロードしないようにしましょう．

♣ その２

“動作”が怪しいアプリは，
アンインストールしましょう．

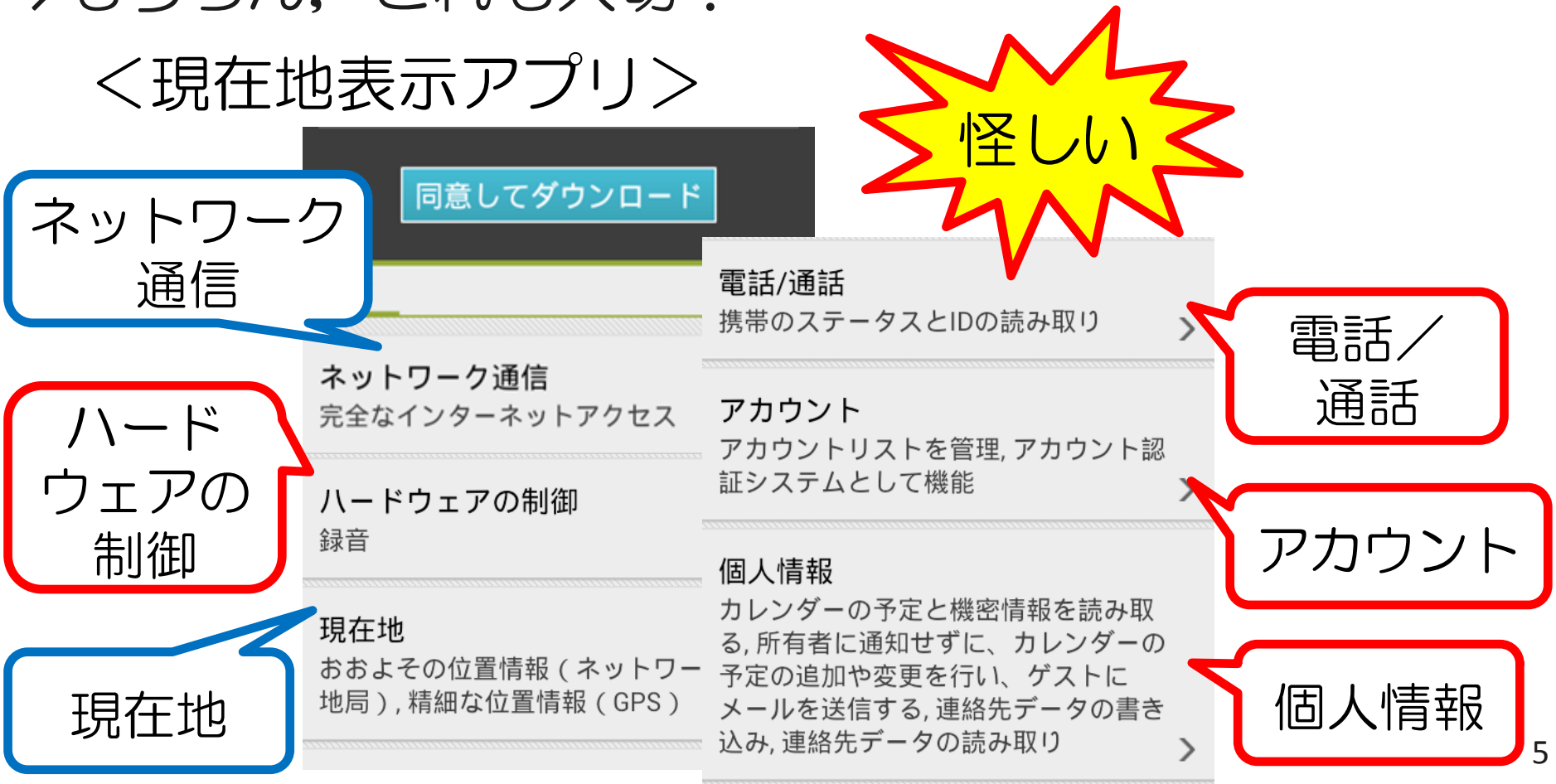
- 現状，ユーザができるのは「その１」．
- 「その２」“動作の怪しさ”に気付く材料がない．

よく言われるのが

♣ インストール時にアプリが要求する“権限”をよく確認して・・・

→もちろん，これも大切！

＜現在地表示アプリ＞



でも，インストール時だけでは・

- 先ほどのアプリは，インストール時の“権限”が明らかに怪しかった．では，これらはどうか？

＜現在地表示アプリ＞

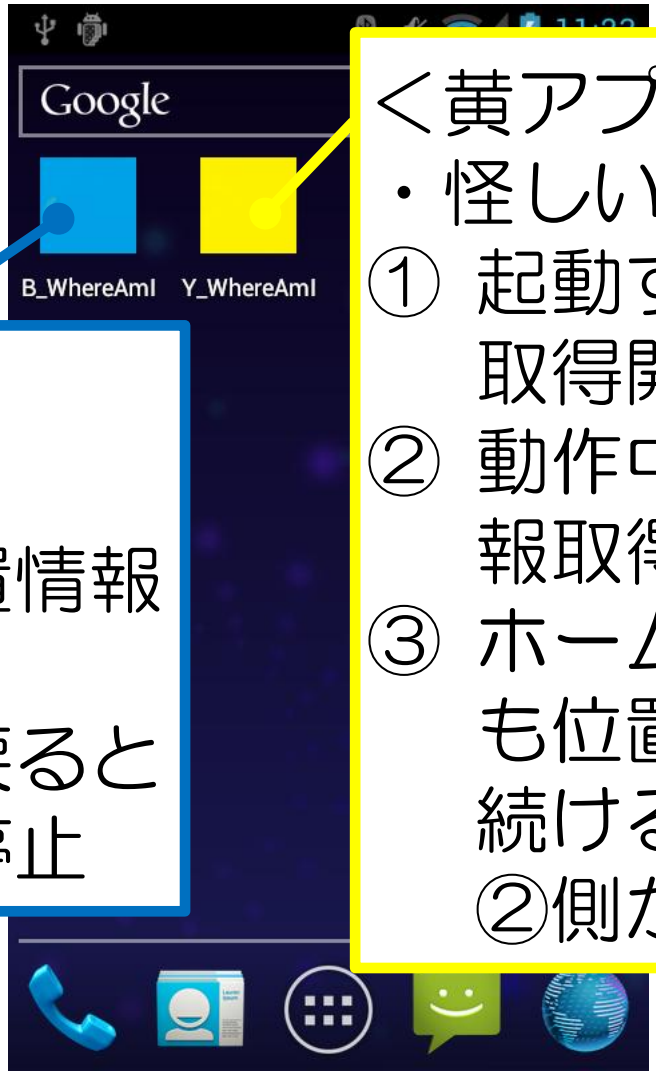
デモ１

＜現在地表示アプリ＞

- どちらも起動すると「現在地を表示する」アプリです.

サンプルアプリの説明

♣ どちらも起動すると「現在地を表示する」アプリ

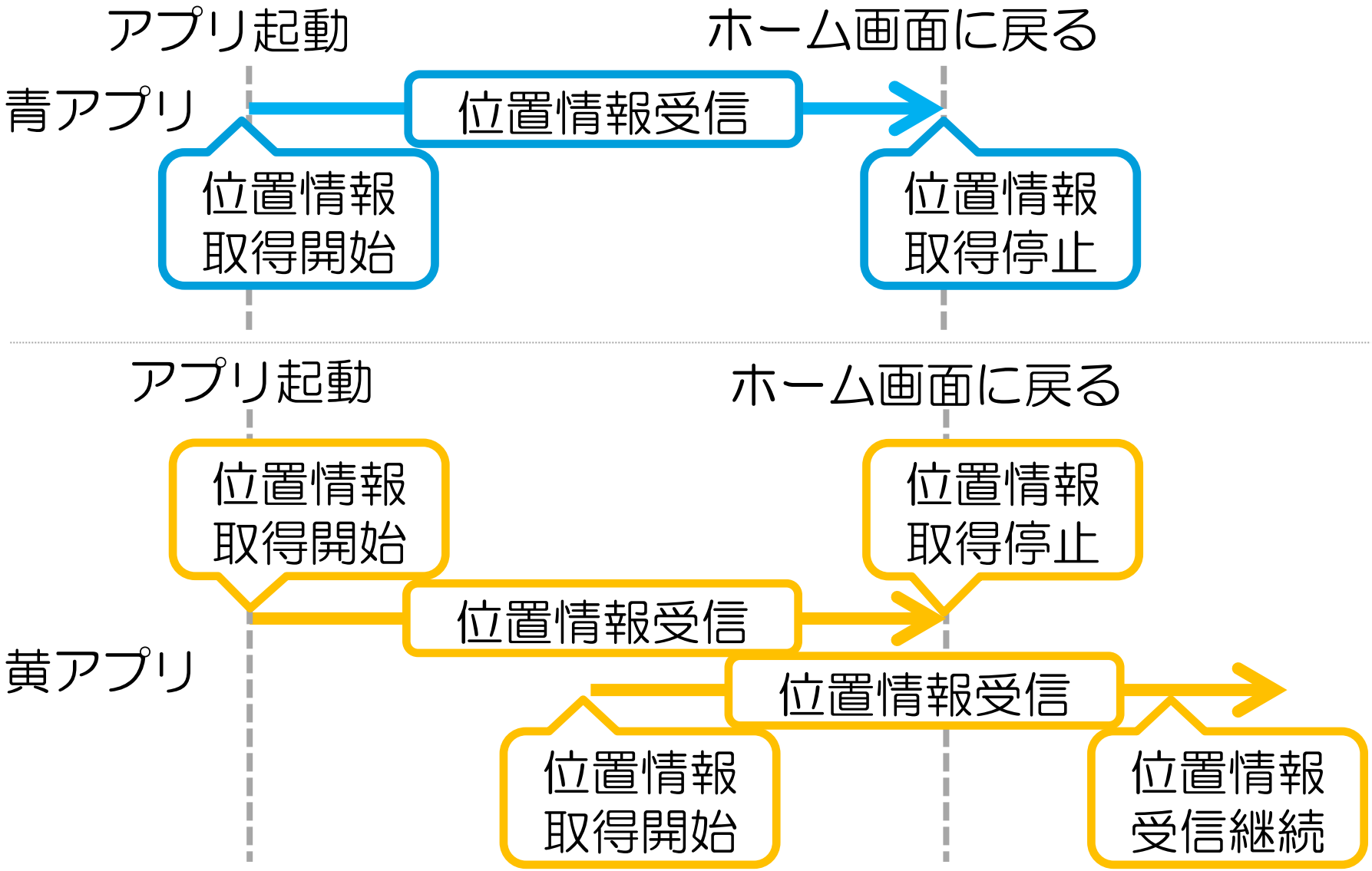


＜青アプリ＞
・普通のアプリ
① 起動すると位置情報取得開始
② ホーム画面に戻ると位置情報取得停止

＜黄アプリ＞
・怪しいアプリ
① 起動すると位置情報取得開始
② 動作中に再度位置情報取得開始
③ ホーム画面に戻っても位置情報を受信し続ける（①側は停止.②側が継続）

サンプルアプリの説明

＜現在地表示アプリ＞



（再掲）安全性を確保するために

♣ その１

“権限”が怪しいアプリは，
ダウンロードしないようにしましょう．

♣ その２

“動作”が怪しいアプリは，
アンインストールしましょう．

➢ 現状，ユーザができるのは「その１」．

➢ 「その２」“動作の怪しさ”に気付く材料がない．

提案

“動作の怪しさ”の判断材料を提供するための２つの機能

の追加を提案.

＜機能１＞　動作時の通知

♣ 注意すべき動作が生じたときに，リアルタイムでユーザに知らせる

+α … 動作の許可／拒否を可能に

＜機能２＞　動作履歴の提示

♣ 注意すべき動作について，動作履歴を提示する

提案

“動作の怪しさ”の判断材料を提供するための２つの機能

＜機能１＞　動作時の通知

♣ 注意すべき動作が生じたときに，リアルタイムでユーザに知らせる

+α … 動作の許可／拒否を可能に

＜機能２＞　動作履歴の提示

♣ 注意すべき動作について，動作履歴を提示する

動作時の通知

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

～例えばこのような感じで～

① アプリが位置情報の取得を開始するときに，ステータスバーに警告を出す

動作時の通知

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

～例えばこのような感じで～

② 無視（何もしない）⇒位置情報の取得拒否
通知領域をタップ⇒位置情報の取得許可

デモ２：動作時の通知
～例えばこのような感じで～

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 注意すべき動作が生じたときに，リアルタイムでユーザに知らせる　+α … 動作の許可／拒否を可能に

もし，動作時の通知機能があれば

- インストール時の“権限”が明らかに怪しいと判断できない場合でも，動作時に怪しさに気付くことができる.

→アンインストールへ

提案

“動作の怪しさ”の判断材料を提供するための２つの機能

＜機能１＞　動作時の通知

♣ 注意すべき動作が生じたときに，リアルタイムでユーザに知らせる

+α … 動作の許可／拒否を可能に

＜機能２＞　動作履歴の提示

♣ 注意すべき動作について，動作履歴を提示する

動作履歴の提示
～例えばこのような感じで～

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

① 注意すべき動作が起こった時に，提案システム側で動作日時を記録する

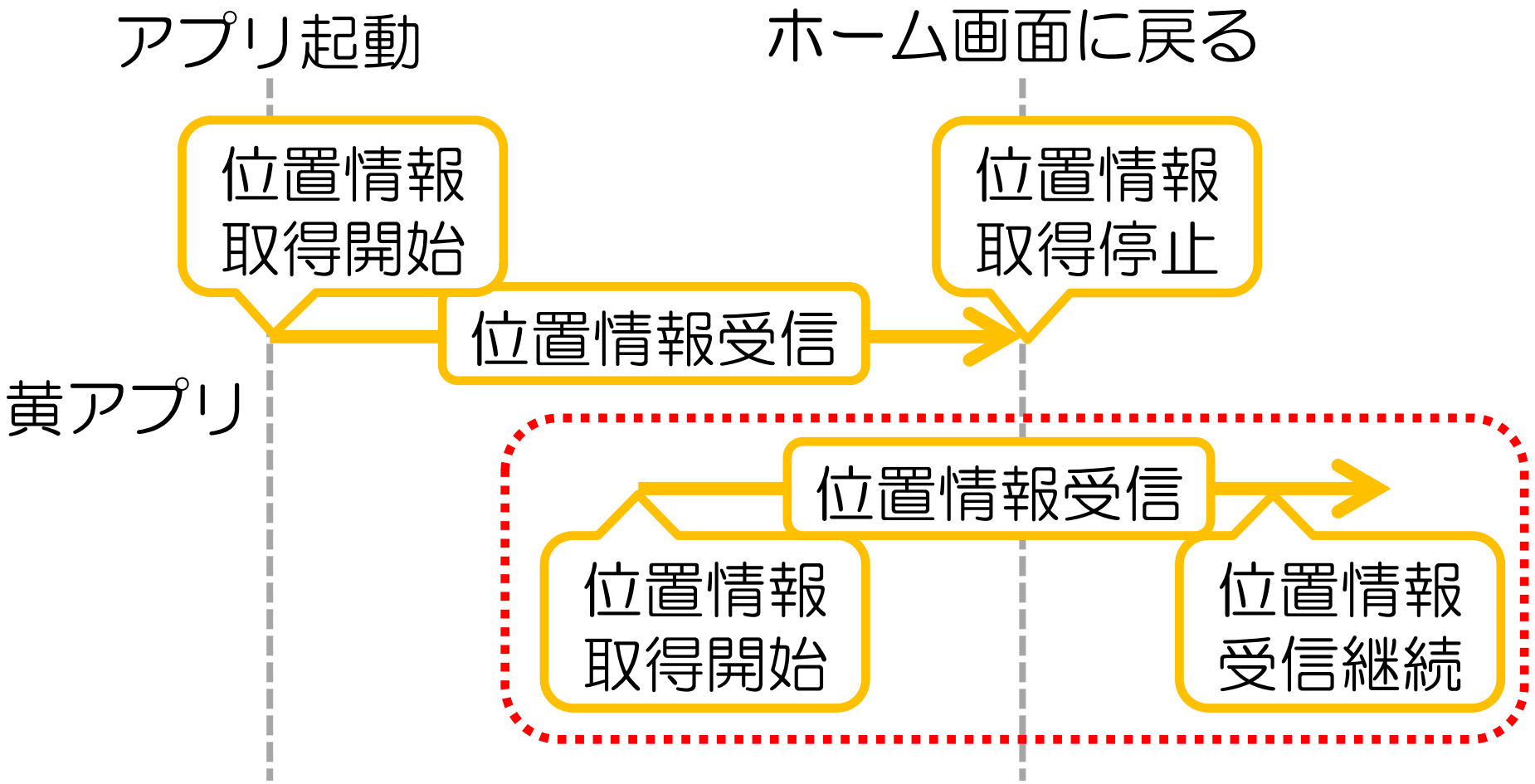
⇔現状，怪しいかもしれないアプリ自身は，使えるログを出力しない

② ①をわかりやすくユーザに提示する

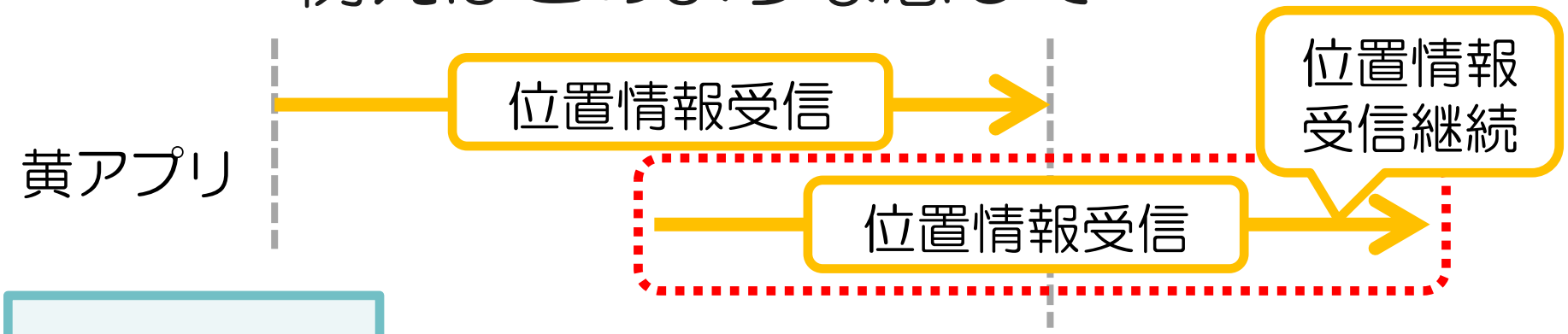
動作履歴の提示
～例えばこのような感じで～

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

＜現在地表示アプリ＞



動作履歴の提示
～例えばこのような感じで～

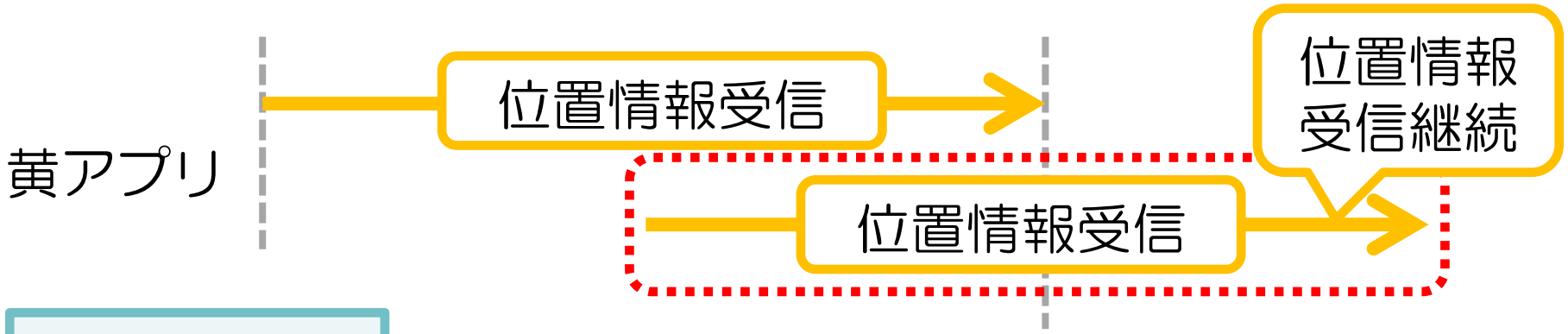


黄アプリの
動作履歴

動作	日時
位置情報取得開始	2012/06/29 09:30
位置情報取得開始	2012/06/29 09:30
位置情報取得停止	2012/06/29 09:33
位置情報取得開始	2012/06/29 20:13
位置情報取得開始	2012/06/29 20:1
位置情報取得停止	2012/06/29 20:15

ん？開始
2回に停
止1回？

動作履歴の提示
～例えばこのような感じで～



黄アプリの
動作履歴

動作	日時	継続時間
位置情報取得	2012/06/29 09:30	00:03:24
位置情報取得	2012/06/29 09:30	continue
位置情報取得	2012/06/29 20:13	00:05:10
位置情報取得	2012/06/29 20:13	continue

ん？
continue？

もし，アプリの動作履歴がわかれば

- インストール時の“権限”が明らかに怪しいと判断できない場合でも，動作の怪しさに気付くことができる.

→アンインストールへ

安全性を確保するために

♣ その１

“権限”が怪しいアプリは，
ダウンロードしないようにしましょう．

♣ その２

“動作”が怪しいアプリは，
アンインストールしましょう．

- 現状，ユーザができるのは「その１」．
- 提案システムでは，「その２」の判断材料をユーザに提供する．

安全性を確保するために（提案）

提案システムでは

“動作の怪しさ”の判断材料を提供するための２つの機能

の追加を提案.

＜機能１＞　動作時の通知

♣ 注意すべき動作が生じたときに，リアルタイムでユーザに知らせる

+α … 動作の許可／拒否を可能に

＜機能２＞　動作履歴の提示

♣ 注意すべき動作について，動作履歴を提示する

安全性を確保するために（提案）

もし，２つの機能が追加されれば，

- インストール時の“権限”が明らかに怪しいと判断できない場合でも，

↓

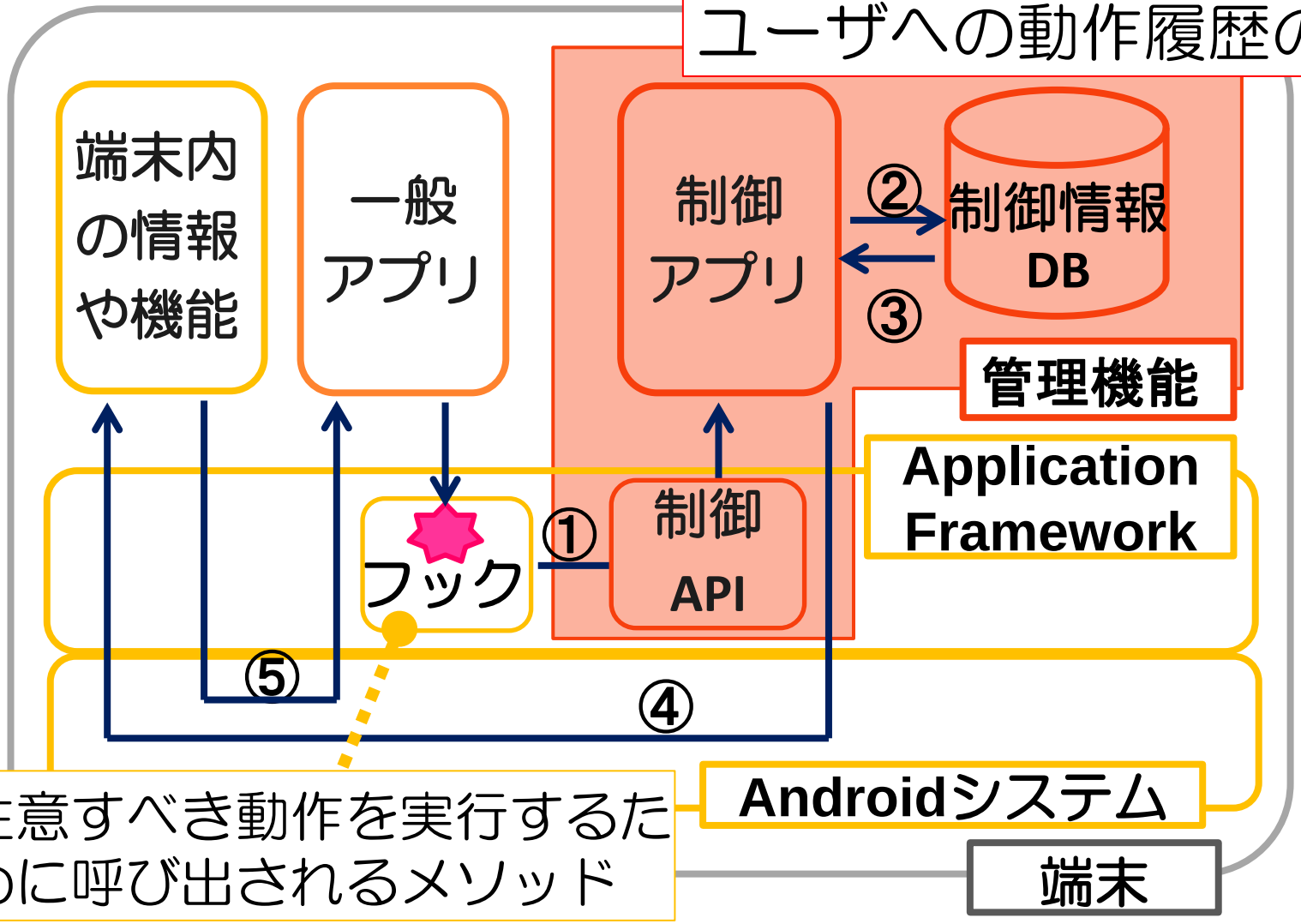
- 動作時に怪しさに気付くことができる．（機能１：動作時の通知）
- 動作の怪しさに気付くことができる．（機能２：動作履歴の提示）

↓

- アンインストールへ

提案システムの概要

ユーザへの動作の通知
アプリ動作の記録
ユーザへの動作履歴の提示

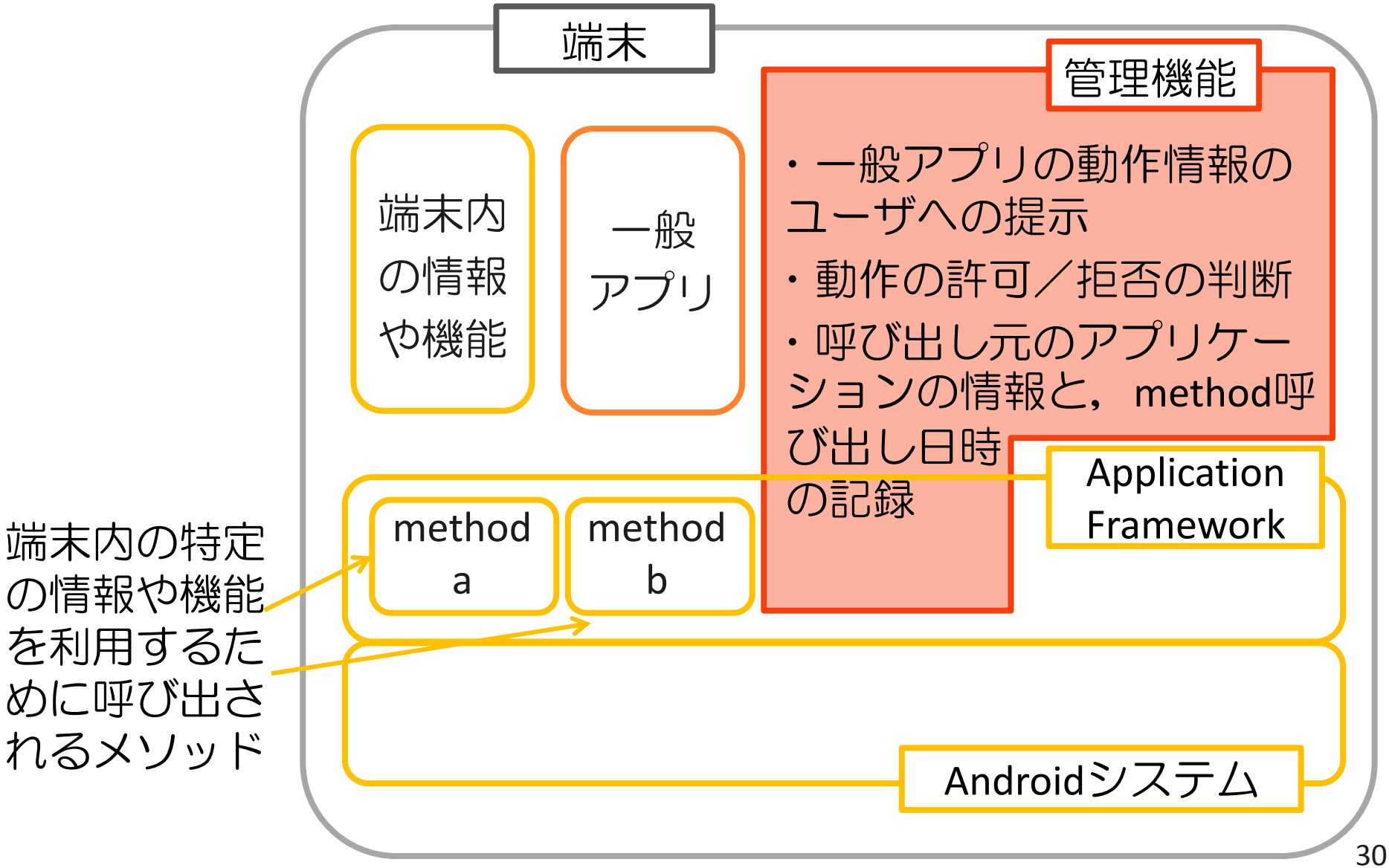


今後の予定

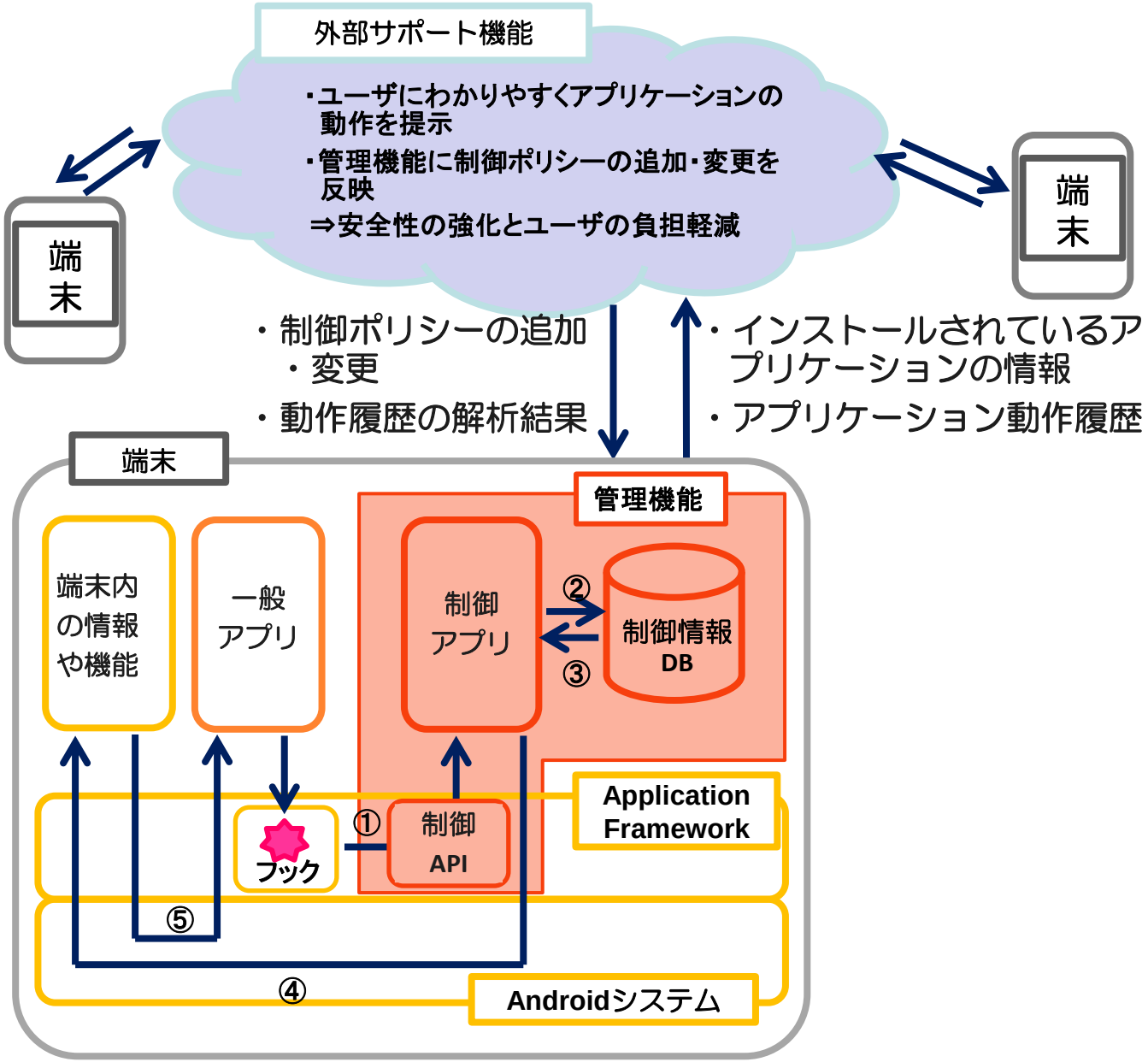
- Application Framework層に手を加えて，端末内の管理機能（動作履歴の記録，動作時の警告の表示，動作時の許可／拒否）を実装する.
- 一般に公開されているアプリケーションの動作履歴を収集する.
- ユーザ負担を軽減するための制御ポリシーの内容を検討する.
- 管理機能を充実させる（制御ポリシーの反映）.

ありがとうございました。

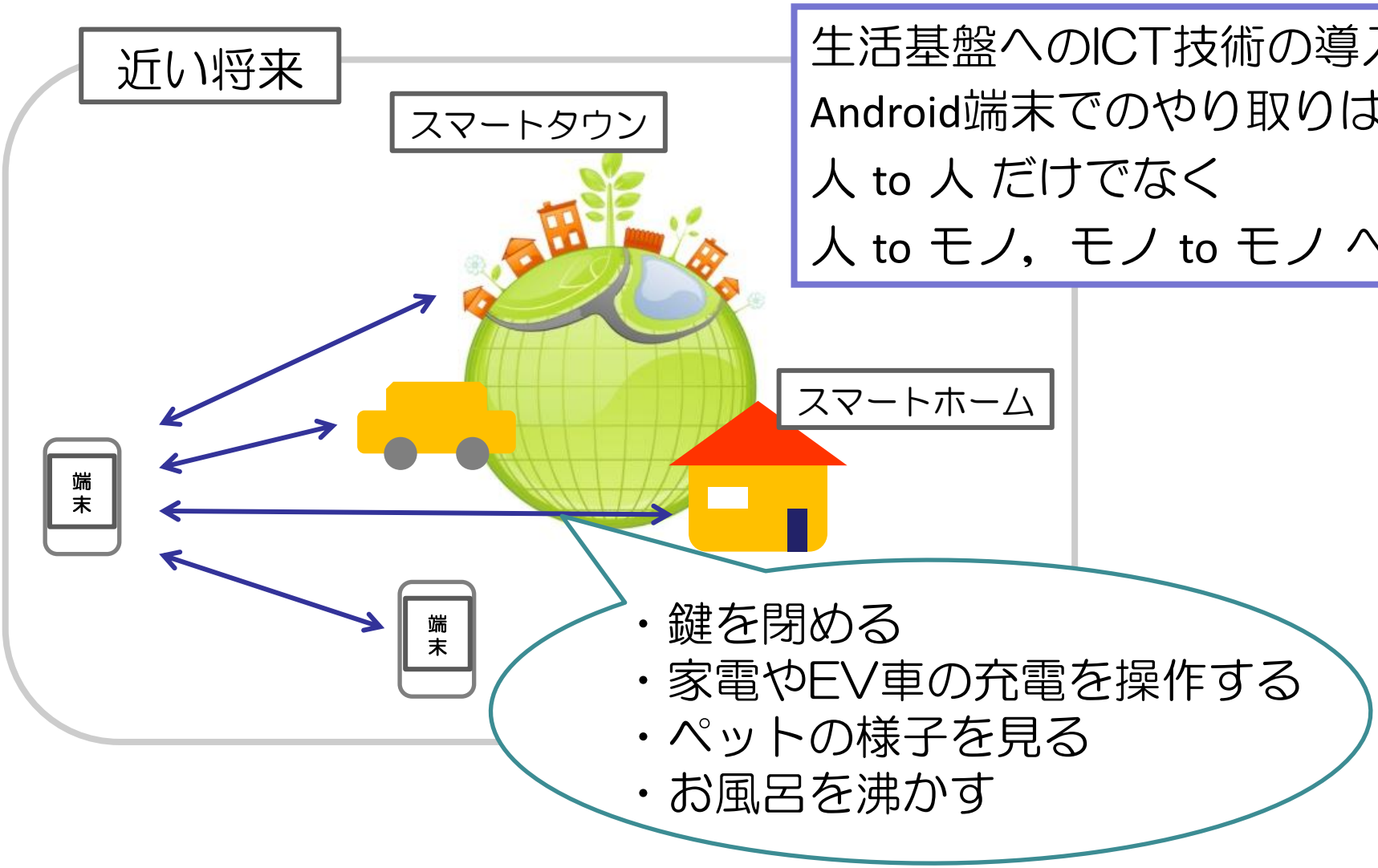
提案システムの概要


端末
管理機能
端末内の情報や機能
一般アプリ
・一般アプリの動作情報のユーザへの提示
・動作の許可／拒否の判断
・呼び出し元のアプリケーションの情報と，method呼び出し日時の記録
Application Framework
method a
method b
Androidシステム
端末内の特定の情報や機能を利用するために呼び出されるメソッド

提案システムの概要


外部サポート機能
・ユーザにわかりやすくアプリケーションの動作を提示
・管理機能に制御ポリシーの追加・変更を反映
⇒安全性の強化とユーザの負担軽減
端末
端末
・制御ポリシーの追加・変更
・動作履歴の解析結果
・インストールされているアプリケーションの情報
・アプリケーション動作履歴
端末
管理機能
端末内の情報や機能
一般アプリ
制御アプリ
制御情報DB
②
③
Application Framework
フック
①
制御API
⑤
④
Androidシステム

生活基盤へのICT技術の導入



Android端末の安全性を確保することがより重要になる