JSSEC アプリ解析技術タスクフォース 活動のご紹介

日本 スマートフォン セキュリティ協会
技術部会 アプリケーション解析技術TF

概要

- JSSEC(日本スマートフォンセキュリティ協会)技術部会アプリケーション解析技術タスクフォースにおいて、この連絡協議会と関連する内容を扱っておりますので、ご紹介させていただきます。

- 本日ご紹介させていただく内容の大部分は、先日「スマートフォンセキュリティシンポジウム 2012」での講演内容から抜粋しております。

概要

背 景

スマートフォン
アプリ急増

＝

ユーザーの
不利益になる
アプリも出現

本報告

不利益になる
アプリの分類

＋

診断基準
に向けての進捗

タスクフォースの目的

不利益になるアプリの分類

⇨ ユーザーと事業者の間で共通理解を得る

診断基準・検査項目の検討

⇨ 事業者間での情報共有、技術力向上

タスクフォース参加企業・団体

株式会社アンラボ
株式会社Empress Software Japan
株式会社カスペルスキー
KDDI株式会社
神戸デジタル・ラボ
独立行政法人情報処理推進機構（IPA）
ソニーデジタルネットワークアプリケーションズ
タオソフトウェア株式会社
デジタルアーツ株式会社
東京システムハウス
トレンドマイクロ株式会社
一般社団法人日本オンラインゲーム協会
日本ヒューレット・パッカード株式会社
ネットエージェント株式会社
株式会社ProVision
モバイル・コンテンツ・フォーラム（MCF)
日本ユニシス株式会社
株式会社ラック

（18社・団体：50音順）

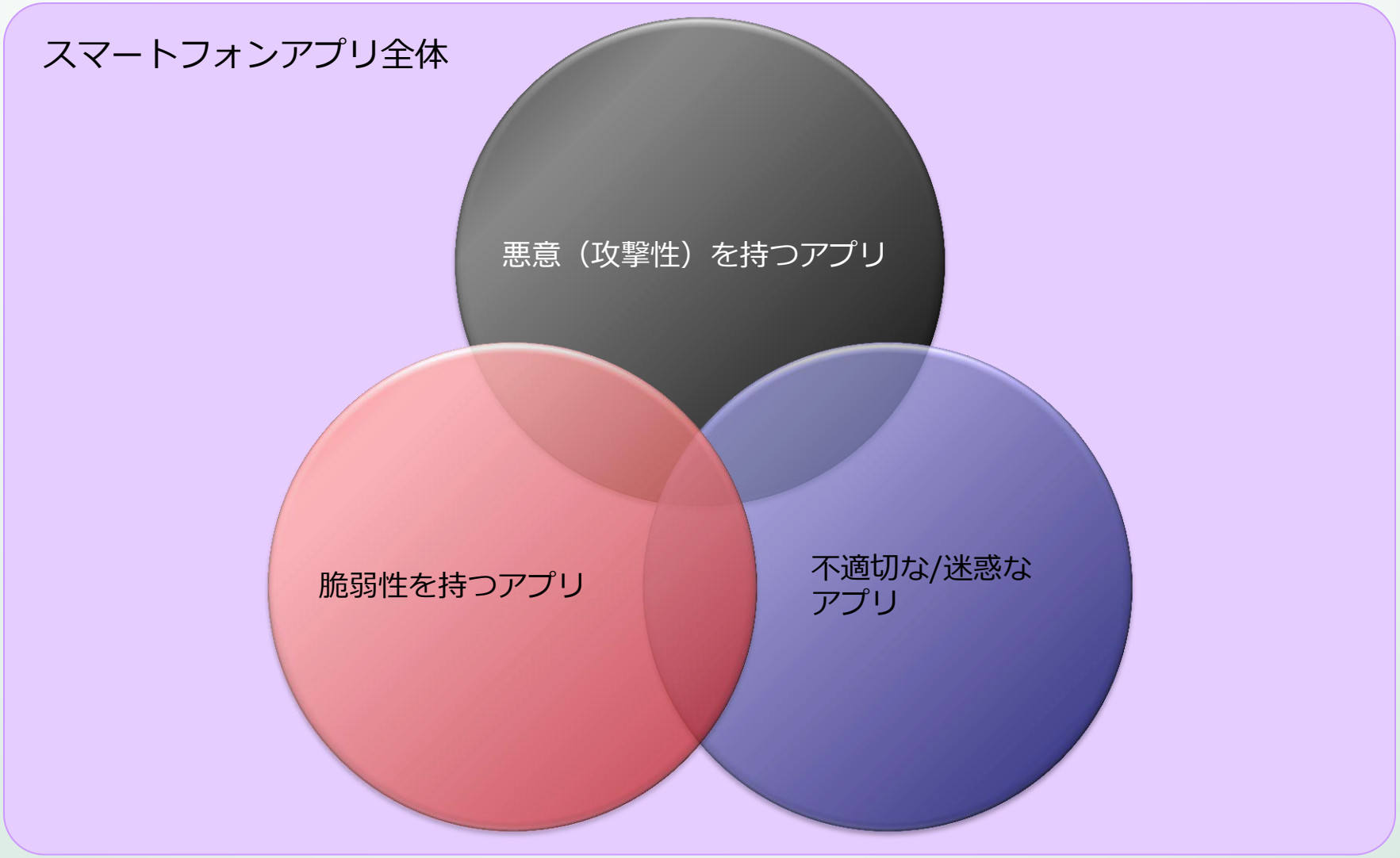
※解析用のアプリ提供企業及びオブザーバー含む

対象プラットフォーム

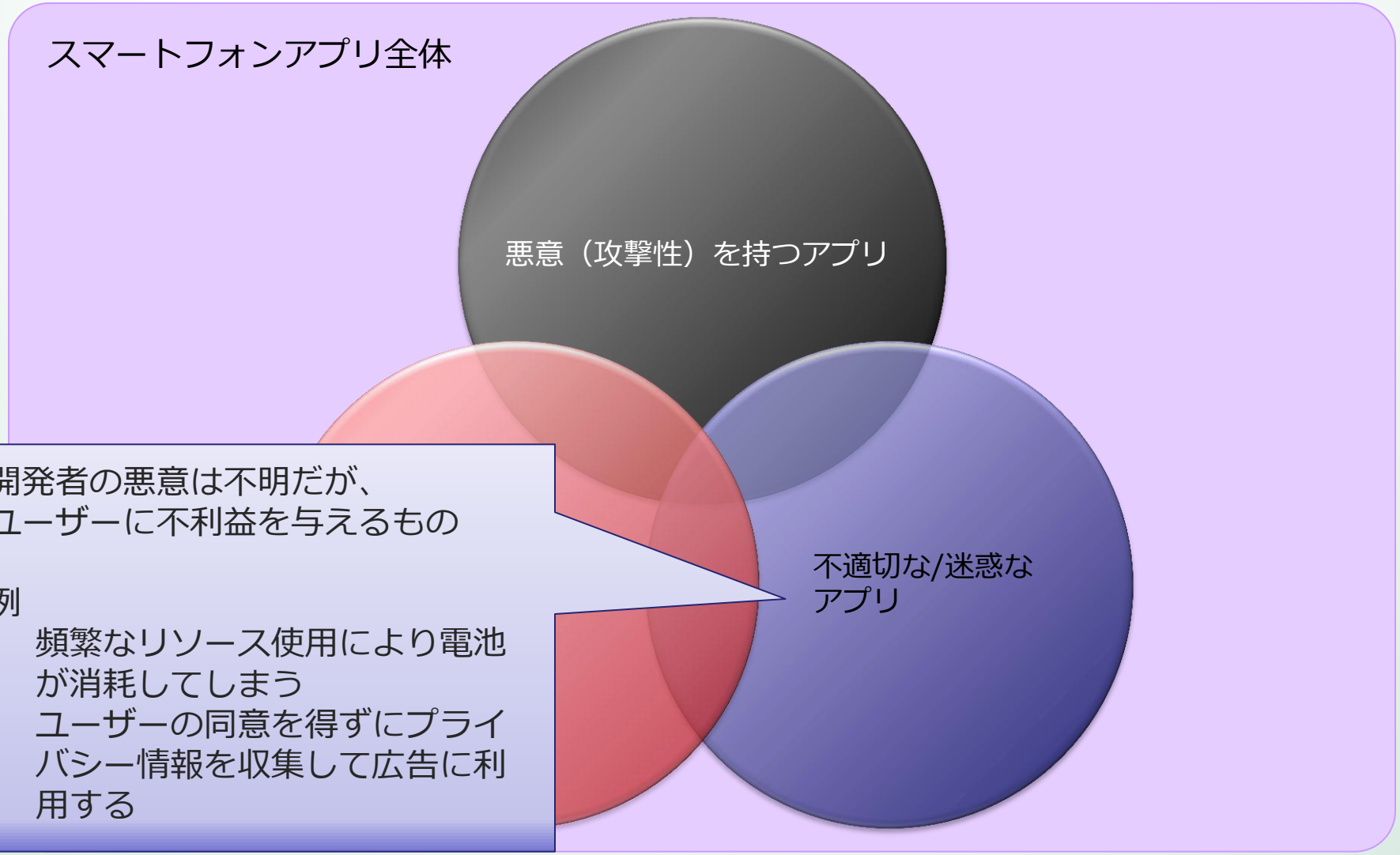
今回は Android アプリを対象

- 各社の限られたリソースの中で条件を揃えるため
- Android アプリだけにリスクがあるわけではなく、本タスクフォースの結果の大部分は他OSにも当てはまると考える

ユーザーに不利益となるアプリの大分類



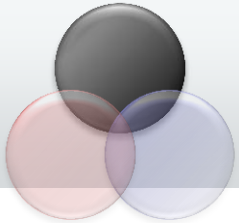
大分類



開発者の悪意は不明だが、
ユーザーに不利益を与えるもの

例
- 頻繁なリソース使用により電池が消耗してしまう
- ユーザーの同意を得ずにプライバシー情報を収集して広告に利用する

不利益になるアプリの分類 (つづき)
分類表 (1) 攻撃性を持つもの



情報漏洩 （スパイウェア）	キー操作、位置情報、利用者情報などを、悪用のために外部に漏洩するアプリ
詐欺 （振り込め／ワンクリック）	利用者を騙して、不正に料金を請求するアプリ
	(例) 利用者の電話番号／メールアドレス／アドレス帳／位置情報などを勝手に収集し、これらを画面上に表示して利用者を脅迫する 海外では勝手に高額なプレミアムSMSに接続させるものも
踏み台 （ボット／バックドア）	端末を乗っ取って、外部から不正に操作するアプリ
	(例) 迷惑メールや多量パケットの送信
脱獄 （ジェイルブレイク、権限奪取）	OS / ライブラリ / アプリケーションの脆弱性を突くアプリ
	(例) スマートフォン向けOSが持つ制限機構を解除する (ジェイルブレイク)

不利益になるアプリの分類 (つづき)
分類表 (2) 不適切な/迷惑なもの

不適切な情報送信	利用者情報を外部に送信する際に、利用者への適切なアプリケーションに関するプライバシーポリシーの提示と承諾を伴わないもの
本来利用できない機能や権限	自身で脱獄（ジェイルブレイクや管理者権限奪取）しないものの、他のアプリケーションが奪ったシステム・管理者権限の利用を想定したアプリケーション OSが提供する安全性を考慮したAPIがあるにも関わらず、これを回避して安全対策を外した独自のAPIを利用するアプリケーション
	(例)端末をWiFiアクセスポイント化するアプリ
エゴ	必要以上の電池浪費、通信設備負荷、利用者にとって迷惑な強制通知、など
	(例)GPSを頻繁に利用して電池を消費する、頻繁に通信を発生させる、OSの通知領域に広告を表示する

不利益になるアプリの分類 (つづき)
分類表 (3) 脆弱性があるもの

「セキュアコーディングガイド」の分類に沿って以下の分類とする

Activityの不適切なIntent送信	ファイルの不適切な扱い
Activityの不適切なIntent受信	Browsable Intent の不適切な扱い
Broadcastの不適切な送信	Log への不適切な情報出力
Broadcastの不適切な受信	UI への不適切な情報出力
Content Providerの不適切な利用	Permission の不適切な扱い
Content Providerの不適切な公開	AccountManager の不適切な扱い
Serviceの不適切な利用	Clipboard の不適切な扱い
Serviceの不適切な公開	その他の問題
SQLiteの不適切な扱い	

アプリ検査；　プライバシー編

・プライバシーポリシーの読み解きトライアル
・送信情報の検知トライアル

プライバシー観点から達成すべきこと

(「イニシアティブ」の8項目)

(1) 各アプリのプライバシーポリシーが**必要項目**を満たしているか検証し、その内容をユーザーが確認できること

→複数のサンプルについてポリシーの読み解きを実施

(2) プライバシー情報の実際の取り扱いが、プライバシーポリシーと合致しているかどうかを確認すること

→複数のサンプルについて各社の技法で検査を実施

プライバシーポリシー読み解きトライアルの結果

- ポリシーの置き場がバラバラで探すのに苦労
  - マーケットのアプリ説明画面からリンクされた webページ
  - アプリ起動時の画面、アプリの設定 UI の奥深く
- 日本語以外の言語で書かれたものがある
- 様式がバラバラで要素の読み解きに苦労
- 内包している情報収集モジュールを考慮していない
- アプリではなく企業のポリシーしか無い場合がある
- 利用規約と混在している場合がある

- 手動で丁寧に読み解けばほぼ正確な検査が可能だが、
  現状では手間がかかりすぎて費用に見合わない

プライバシーポリシー読み解きの結果

- ポリシーの置き場がバラバラで探すのに苦労
  - マーケットのアプリ説明画面からリンクされた webページ
  - アプリ起動時の画面、アプリの設定 UI の奥深く
- 日本語以外の言語で書かれたもの
- 様式がバラバラで要素の読み解き
- 内包している情報収集モジュール
- アプリではなく企業のポリシーし
- 利用規約と混在している場合がある

まずは「イニシアティブ」の8項目を各業界団体のガイドなどに従って提示することの促進が必要

- 手動で丁寧に読み解けばほぼ正
  現状では手間がかかりすぎて費

検査を確実＆効率良く実施するのに適した実装が望ましい (後述)

送信情報の検知トライアルの結果

動的検査

- アプリを実際に動かし、その挙動を検査する
- すべての挙動を起こすのは難しく、検出漏れが出る可能性がある

自動解析

短時間で大量のアプリを検査しやすい

手動解析

初期設定やユーザー登録を要するアプリは手動操作が必要→手間と時間

静的検査

- アプリの構成ファイルを分析、問題を抽出
- 可能性（能力・権限）の発見の網羅性が高い

自動解析

アプリ内への情報取得は検知可能
→送信の有無の判断は難しい

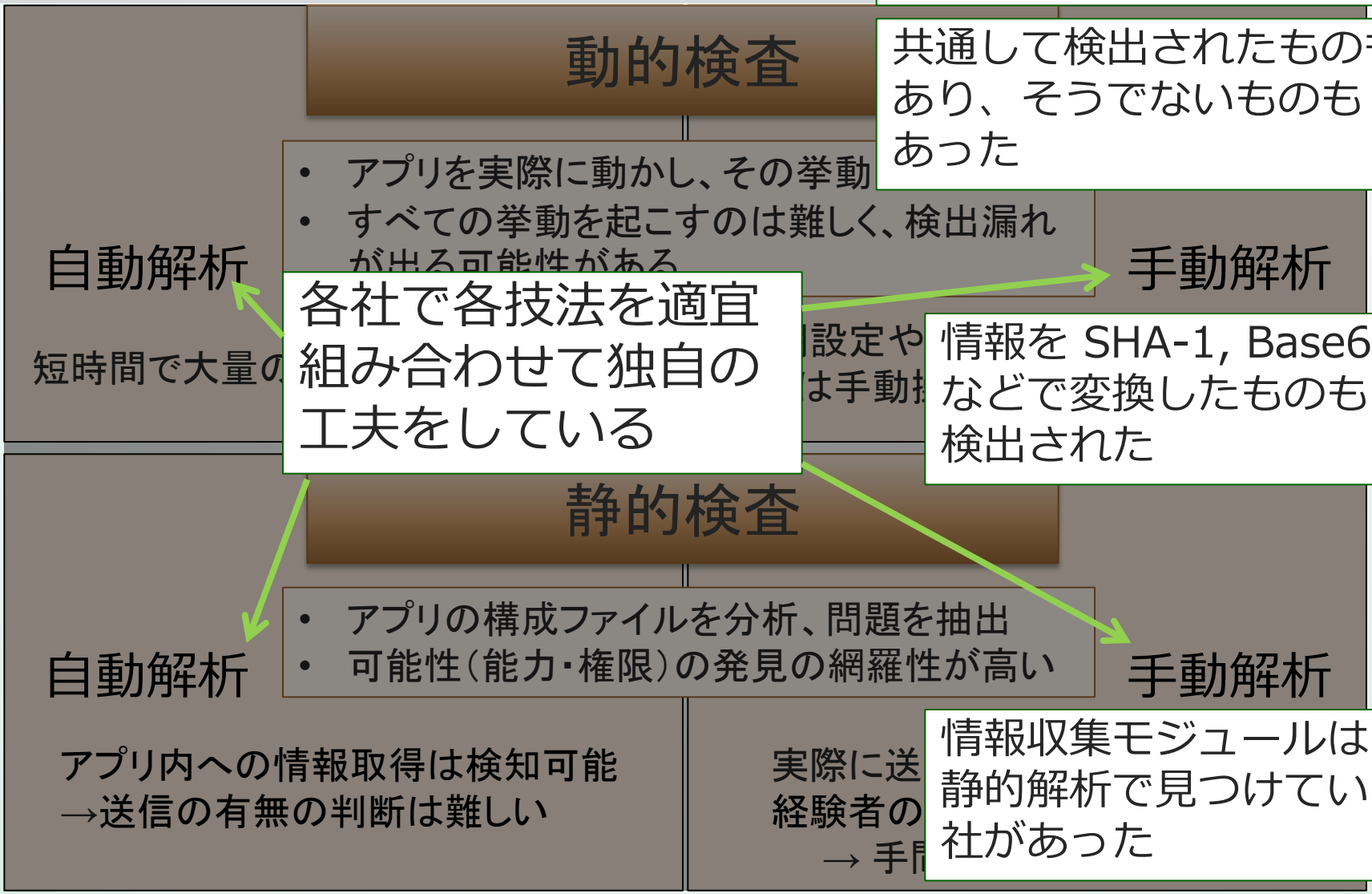
手動解析

実際に送出しているかどうかなど、
経験者の検査で送信の判断は可能
→ 手間と時間

送信情報の検知トライアルの結果

情報の送出は動的検査で見つけている社が多い

共通して検出されたものもあり、そうでないものもあった



情報を SHA-1, Base64 などで変換したものも検出された

情報収集モジュールは静的解析で見つけている社があった

まとめ

- プライバシーポリシー
  - まずは「イニシアティブ」の8項目を各業界団体のガイドなどにしたがって提示することの促進が必要
  - 検査を確実＆効率良く実施するのに適した実装が望ましい
    - 共通の名称のファイルに、共通の書式(共通のタグを持つXMLなど)で記載し、それをアプリで表示するなど
- ポリシーと挙動の合致確認
  - 各事業者(マーケット運用者、アンチウイルスベンダー、など)の目的に合わせた精度、掛けられるコストなど、種々の条件に応じた検査手法を適宜組み合わせることにより、最適な検証設計を行うことが望ましい。

以上