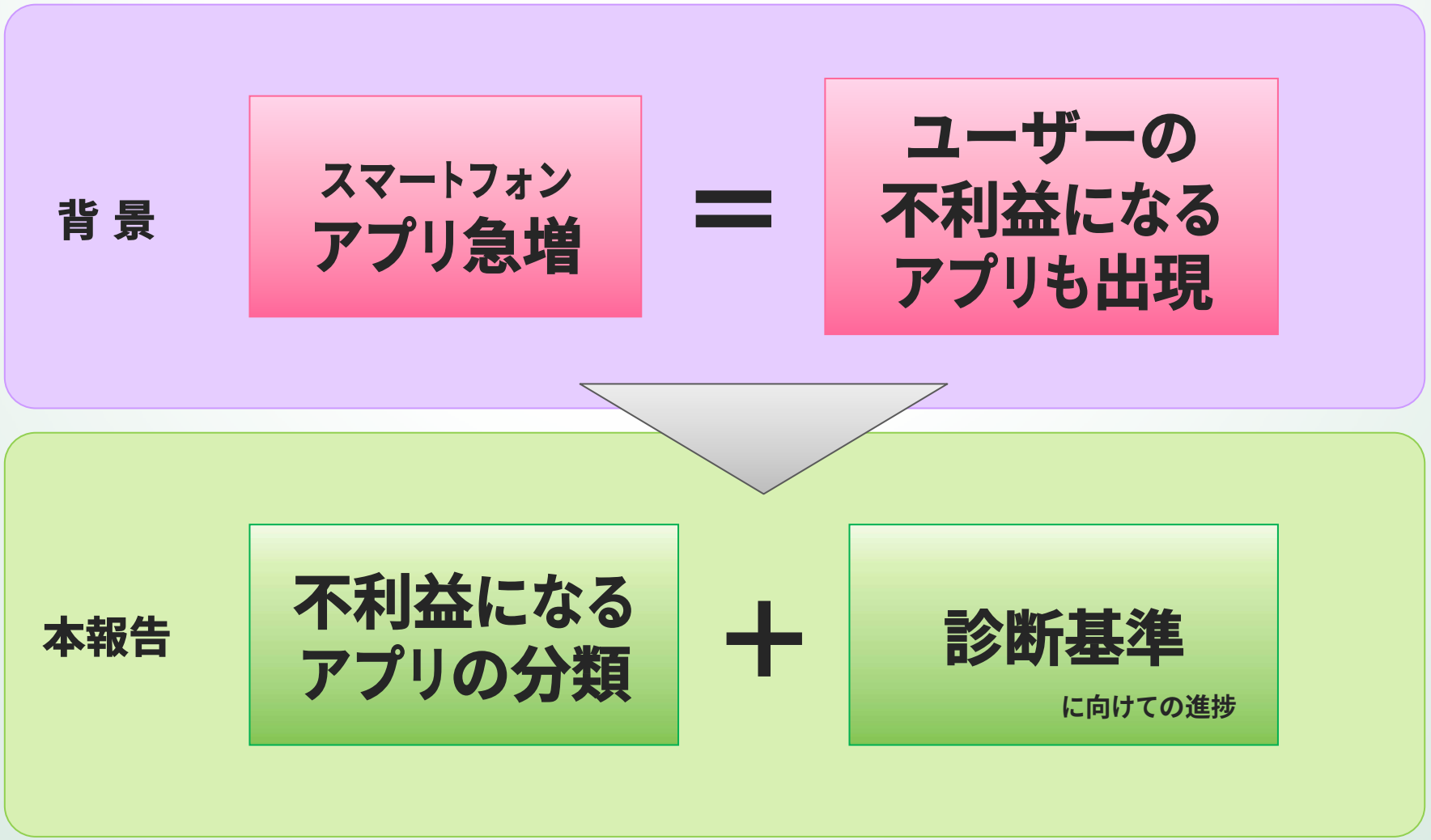
リスクウェアの分析と解析技術

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
藤村　聡　<Satoshi.Fujimura@jp.sony.com>

概要



目次

- 本タスクフォースの概要紹介
- ユーザーの不利益になるアプリの分類
- アプリ検査からの考察
- まとめと今後について
- 参加企業による座談会

本タスクフォースの概要紹介

背景 (1)

スマートフォンのマルウェア増加を示す統計

漠然とした不安の高まり

スマートフォンのマルウェア数 推移

(ABI Research社調べ)

ただし、App Storeや Google Play をはじめとして、一定のマルウェア対策を行っているマーケットが増えてきている。

悪意のある者はチェックの甘いアプリマーケットを選んで投稿･配する傾向にある*。

* F-Secure Mobile Threat Report Q3 2012

背景(2)

「マルウェア以外にもユーザーに不利益をもたらす可能性のある事例が増加しつつある」と言う指摘がある

様々なアプリケーションがスマートフォンの中の情報へアクセスを行い、利用者がそれぞれの情報がどのように共有され利用される可能性があるか十分に理解することが難しくなり、不安を覚える場合もある。

(総務省「スマートフォン プライバシー イニシアティブ」より)

Androidアプリの多くに深刻なSSL脆弱性――中間者攻撃のおそれ
研究者チーム、「Google Play」人気無料アプリ100本のうち41本に脆弱性を指摘

(COMPUTERWORLD 2012年10月23日)

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

対象プラットフォーム

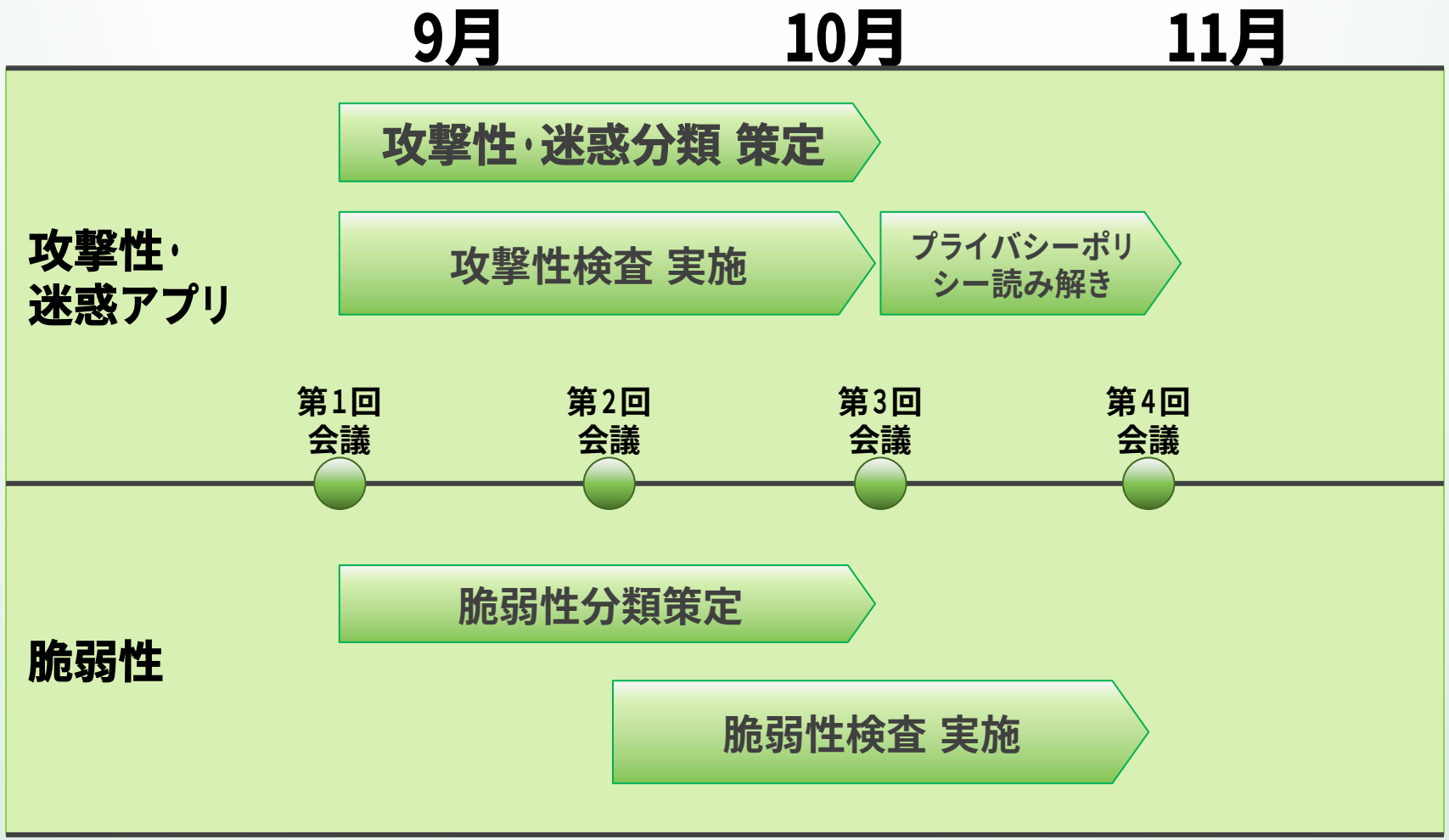
今回は Android アプリを対象

- 各社の限られたリソースの中で条件を揃えるため
- 脆弱性については「セキュアコーディングガイド」の知見を生かす
- 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

解析作業 参加企業

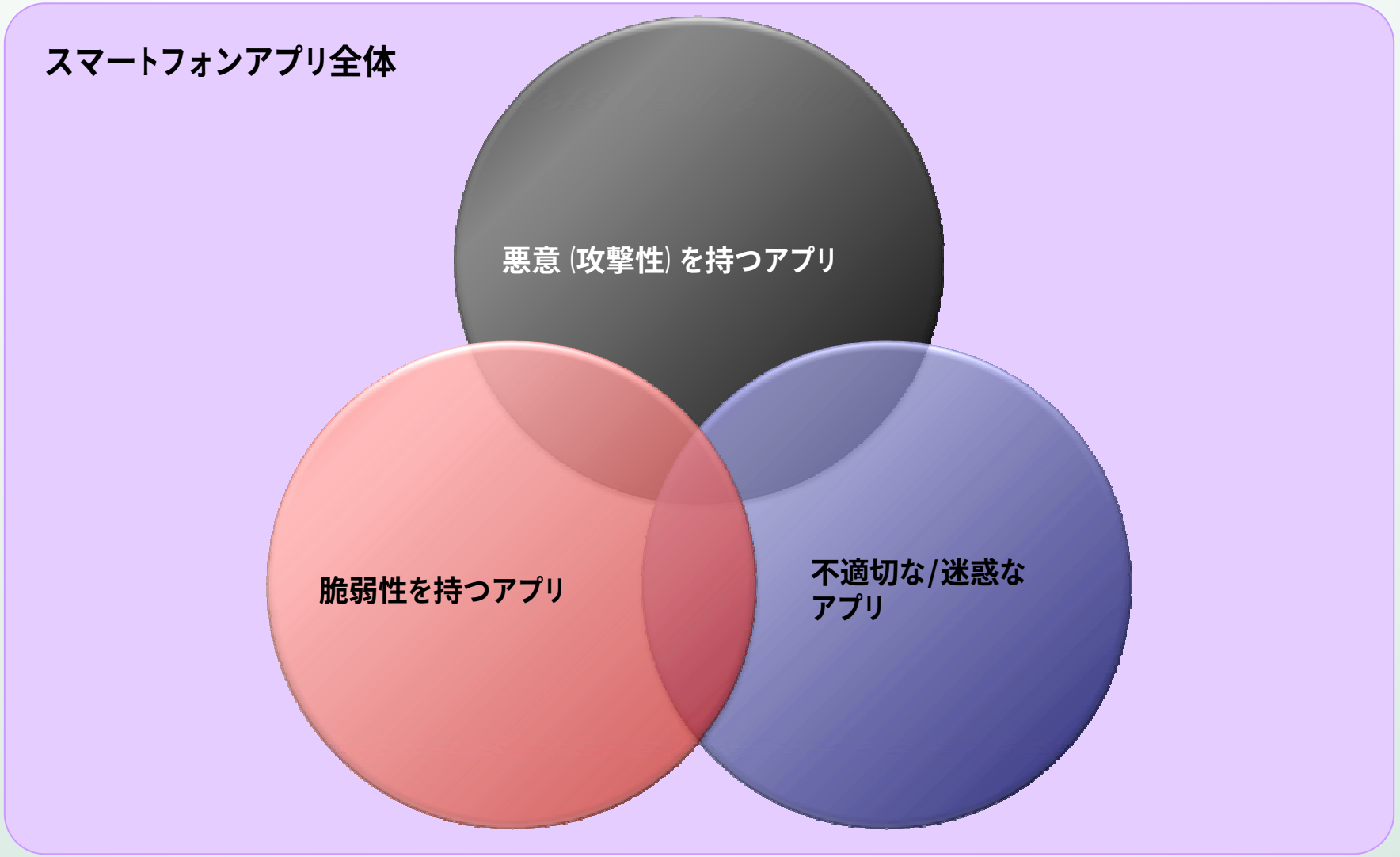
- アンラボ
- Empress Software Japan
- カスペルスキー
- KDDI
- 神戸デジタル・ラボ
- 大日本印刷
- デジタルアーツ
- トレンドマイクロ
- 日本電信電話 (NTT)
- 日本ヒューレット・パッカード
- ネットエージェント
- ProVision
- ラック
- ソニーデジタルネットワークアプリケーションズ

活動実績

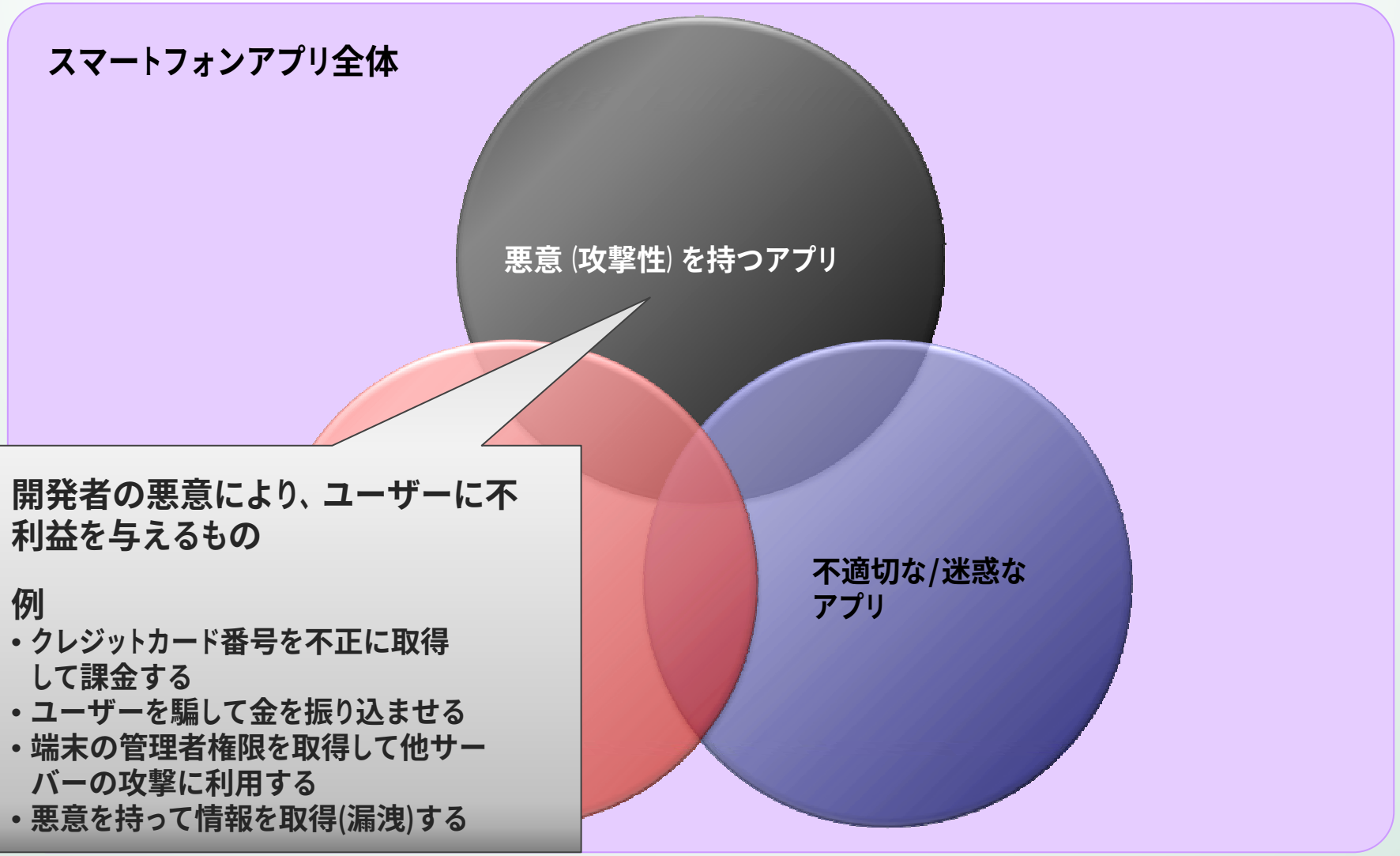


ユーザーの不利益になるアプリの分類

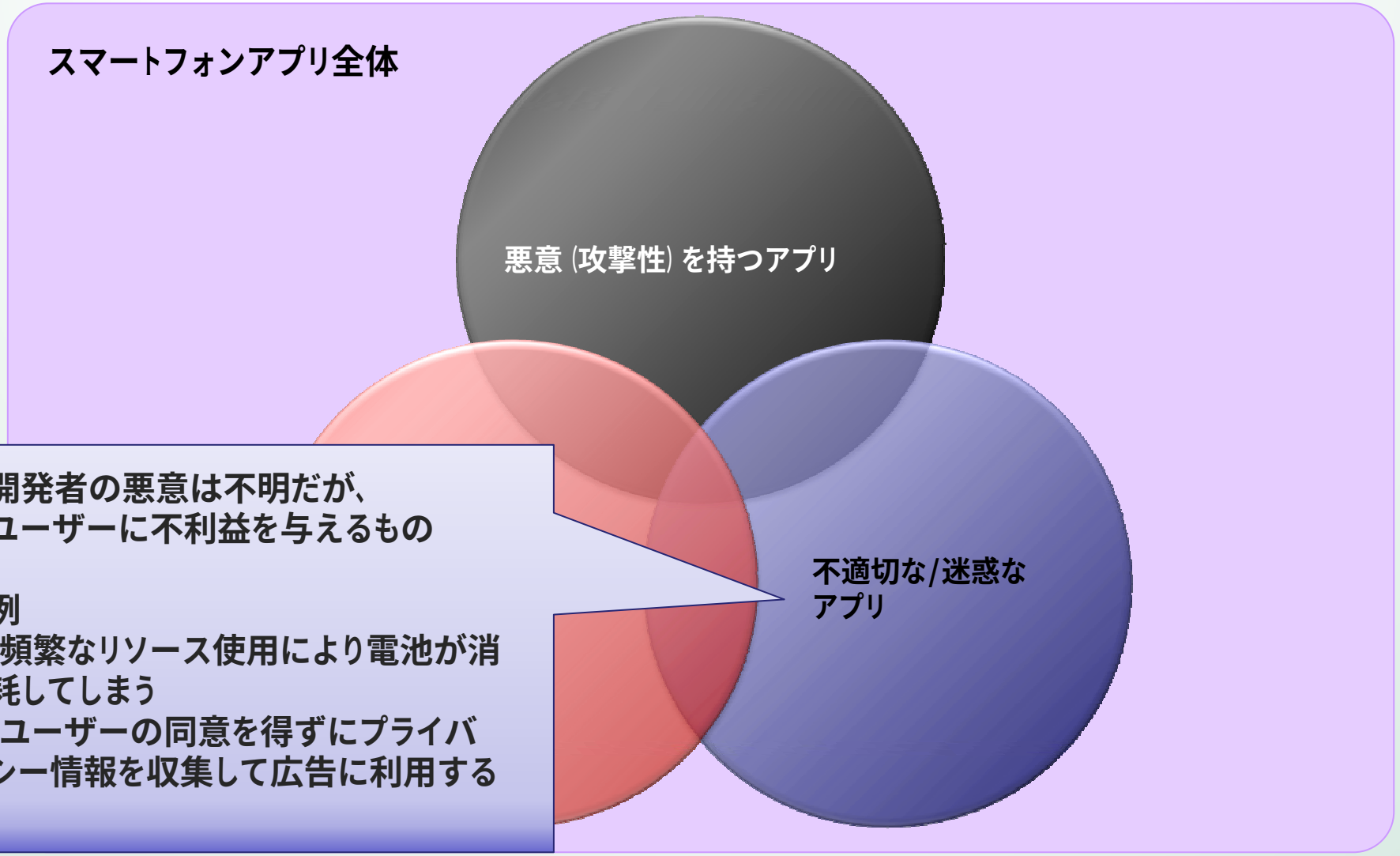
大分類



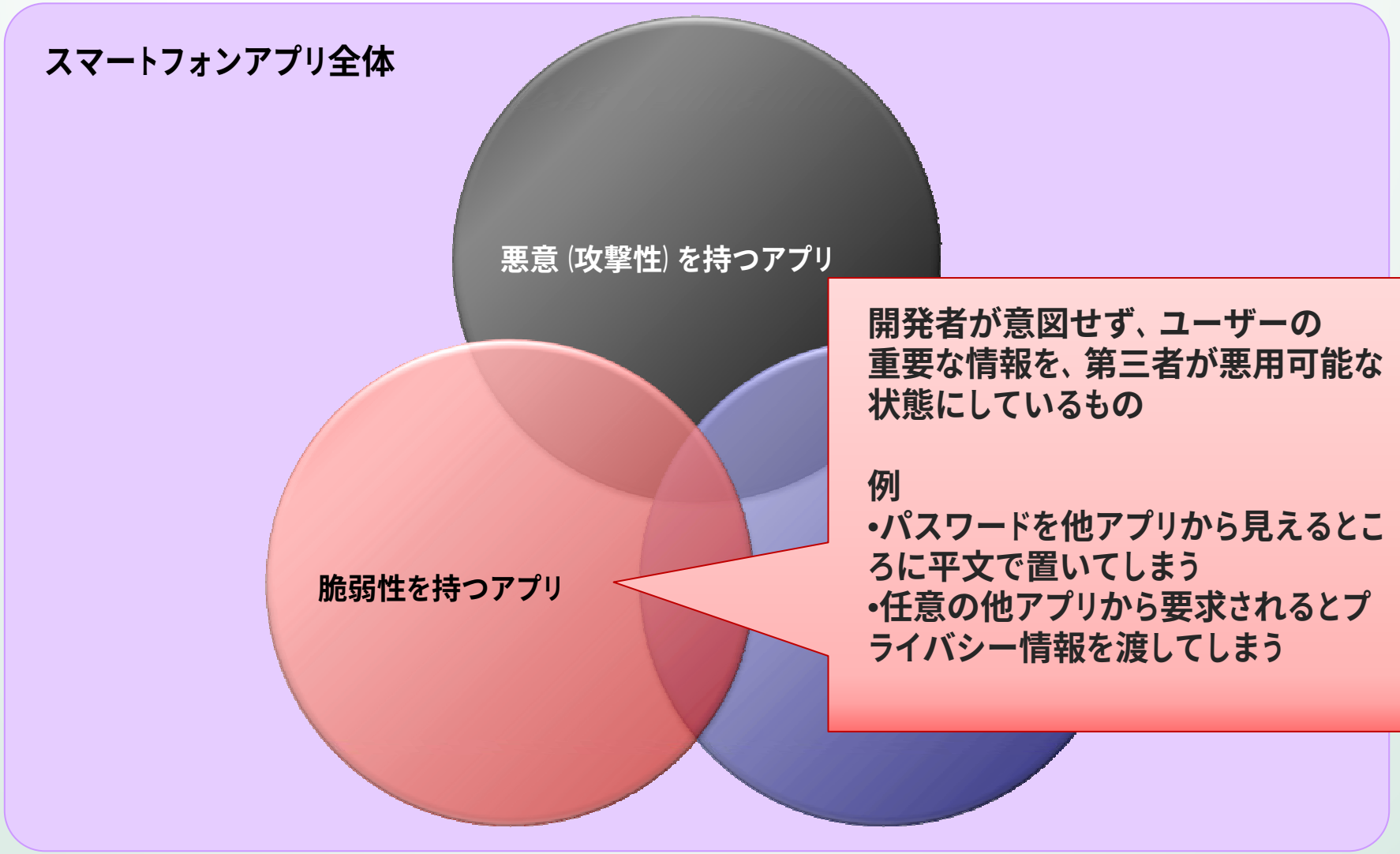
大分類



大分類



大分類



プライバシーポリシー

総務省「スマートフォン プライバシー イニシアティブ」より
プライバシーポリシー8ヶ条

①情報を取得するアプリケーション提供者等の氏名または名称：アプリケーション提供者等の名称、連絡先等を記載する。

②取得される情報の項目：取得される利用者情報の項目・内容を列挙する。

③取得方法：利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか示す

④利用目的の特定・明示
利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤通知・公表または同意取得の方法、利用者関与の方法
プライバシーポリシーの掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。利用者関与の方法については、利用者情報の利用を中止する方法等を記載する。

⑥外部送信・第三者提供・情報収集モジュールの有無
外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦問合せ窓口
問合せ窓口の連絡先等（電話番号、メールアドレス等）を記載する。

⑧プライバシーポリシーの変更を行う場合の手続
プライバシーポリシーの変更を行った場合の通知方法等を記載する（同意の範囲が変更される場合改めて同意取得）。

http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

プライバシーポリシー (つづき)

アプリごとに作成する

≠ 事業者単位のプライバシーポリシー

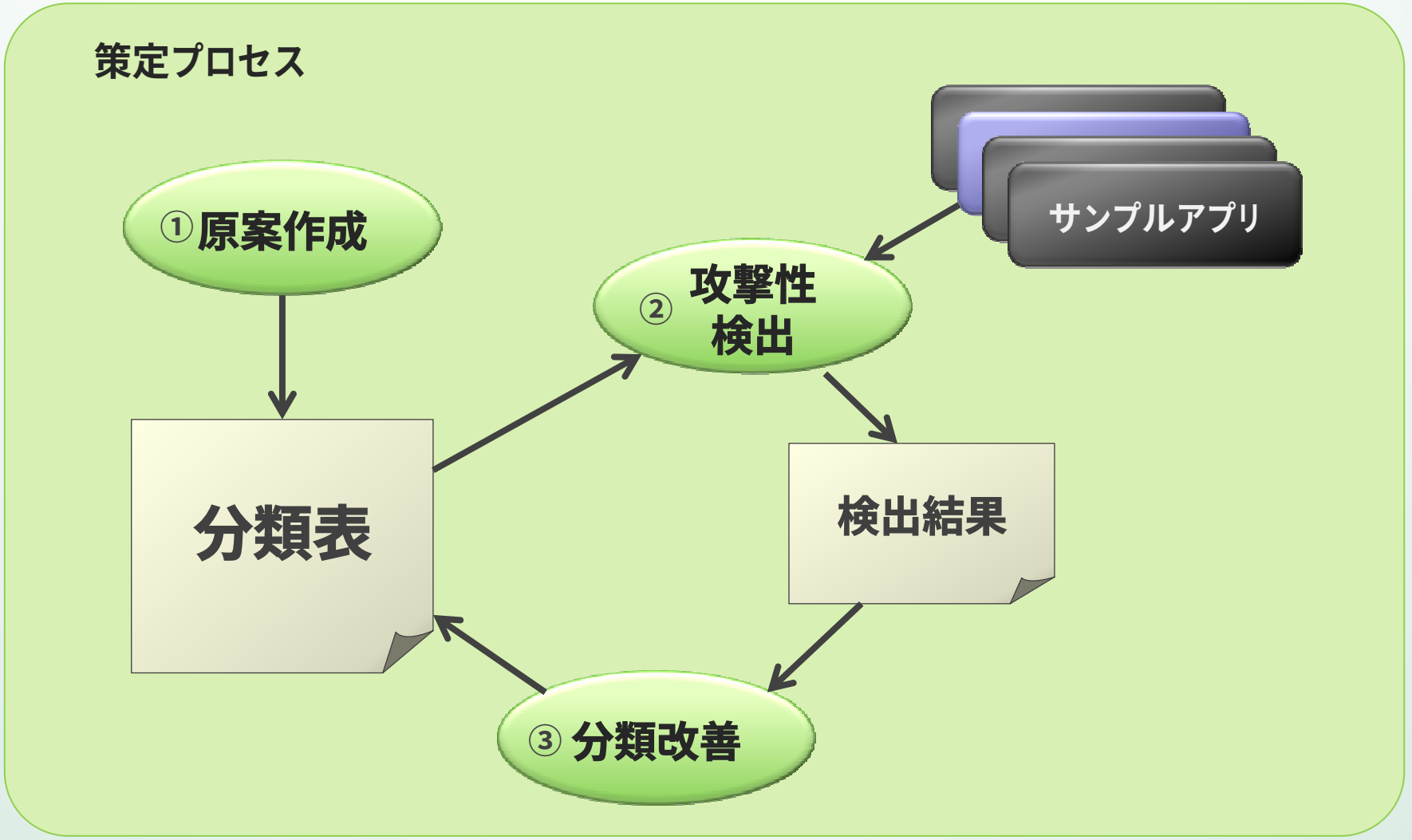
プライバシー性の高い情報は
ユーザーの同意を取る(オプトイン)

電話帳、位置情報、通信履歴等

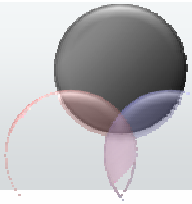
プライバシーポリシー (つづき)

8ヶ条	内容の例
1. 情報取得者	●▲株式会社
2. 取得する情報	端末のID (IMEI)
3. 取得方法	アプリが自動で取得
4. 利用目的	アプリの使用頻度計測のため
5. 利用者関与の方法	設定画面で拒否可能(オプトアウト)
6. 第三者提供の有無	無し
7. 問い合わせ窓口	(メールアドレスなど)
8. ポリシー変更方法	アプリ更新情報に記載

不利益になるアプリの分類



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	

アプリ検査からの考察

悪意（攻撃性）アプリの検出

JSSEC 会員企業から提供された 10 のサンプルアプリを各社で解析

- 解析方法は問わない (各社独自の方法による)
  情報漏洩（スパイウェア）、詐欺（振り込め／ワンクリック）、
  踏み台（ボット／バックドア）、脱獄（権限奪取／ジェイルブレイク）
- プライバシー情報の送信を検知した場合は、情報の内容と送信先を報告
- 広告モジュールを発見した場合は、広告事業者名を報告

(参考) 解析方法の分類

動的検査

- アプリを実際に動かし、その挙動を検査する
- 自動で大量のアプリを検査しやすい
- 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
- ユーザー登録しないと使えないアプリなど、手作業が必要なことも

静的検査

- アプリの構成ファイルを分析し、問題を見つける
  - Android アプリの場合は、APKファイルの構成要素からある程度の分析が可能
- 問題発見の網羅性が高い
- 問題の可能性が多く見つかるので、本当に問題であるかどうかの吟味が必要

悪意（攻撃性）検査からの考察 (1)

情報送信が悪意によるものかどうかを判断することが難しいケース

海外の広告事業者と思しきサーバーに端末情報などを送信しているが、広告事業の正当業務なのか、広告事業のふりをした情報収集なのかが判断しづらい

検査者が正当性 / 違法性を判断できないことがあり得る

判断しづらい場合は、検出結果をユーザーに報告するにとどまらざるを得ない可能性がある

悪意（攻撃性）検査からの考察 (2)

「詐欺」の分類について意見が割れた

- 電話を勝手に掛けるだけで不正課金と判断したメンバー
- 悪意のある者から高額請求されるケースに限定したメンバー

本タスクフォースでは高額請求のみを「詐欺」に分類し、不適切な通信は「エゴ」に分類した

プライバシー情報取扱検査

JSSEC 会員企業から提供されたアプリ数件
(該当企業の提供)と、その他アプリ数件を対象

各アプリが送信している情報の検出と、提示される
プライバシーポリシーの読み解き＆比較を行った

プライバシー取扱検査の考察(1)

ポリシーの読み解きは困難な作業

- ポリシーの置き場にバラつきがある
  マーケットのアプリ説明画面からリンクされている webページ
  → apkファイル単体を対象とする検査では難しい
  アプリ起動時に表示される画面
  アプリの設定 UI の奥深くで表示できる画面
- 利用規約とプライバシーポリシーが混ざっている事例多数
- アプリのポリシーではなく事業者のポリシーを出している事例多数
- 書式が各社各様なので、「8ヶ条」の各要素を探すのが大変

効率よく確実に検査できる工夫が必要

プライバシー取扱検査の考察(2)

ユーザーが認識しやすく、かつ検査しやすいプライバシーポリシーの必要性

- 利用規約と分離した、アプリのプライバシーポリシーとする
- 重要な情報を取得するアプリは明確にユーザー同意を得る
- 「8ヶ条」を明確にした共通書式を用い、これを機械的にチェックできるようにする

今後も引き続き検討が必要

既にガイドラインを公開している企業･団体もあり、これらとの連携も視野に。

- モバイル･コンテンツ･フォーラム(MCF)
  「スマートフォンのアプリケーション･プライバシーポリシーに関するガイドライン」
- タオソフトウェア
  「アンドロイドスマートフォンプライバシーガイドライン」

脆弱性を持つアプリの検出

**参加企業2社の検査項目、
および「セキュアコーディングガイド」の
章立てを参考に、共通の検査項目表を作成**

JSSEC 会員企業が市場に出しているアプリ数件(該当企業の提供)と、著名なアプリを対象に、各社で検査を実施

脆弱性検査からの考察

参加企業によって検査手法は異なる

動的解析、静的解析
自動検査、手動検査

自動解析と手動解析の結果に大きな差がある

自動解析の結果をヒントに手動解析するなど組み合わせると
精度が上がる

発見された脆弱性の深刻度を判定するには、関連する資産(守りたい情報)などの手動レビューが必要

参加企業が少なく、作業時間も不十分なので、もっと実験を重ねる必要がある

まとめと今後について

まとめ

スマートフォンアプリのうち、ユーザーにとって
不利益になるアプリを分類した

この分類にしたがって実際に幾つかのアプリを
検査することにより、検査にまつわる課題が
洗い出されてきた

今後

以下の内容を報告書として公開予定

- ユーザーと事業者との間の共通用語として、今回策定した分類の利用を提案する
- 業界の検査技術を底上げするため、判定基準や検査方法について事業者間でさらに意見交換した結果を明らかにする

参加企業による座談会

以上