スマートフォン上のアプリケーションにおける利用者情報の
取扱いに係る技術的検証等の諸問題に係る実証調査研究

# 静的解析システム仕様書

平成 29 年 2 月 1 日

## 改訂履歴

| 版数 | 日付 | 変更理由 | 変更内容 | 変更者 |
|---|---|---|---|---|
| 1.0 | H29/2/1 | 新規作成 | 1.0 版作成 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

目次

## 用語の定義

| 用語 | 内容 |
|---|---|
| apk ファイル | Android 専用ソフトウェアパッケージであり、拡張子が“.apk”のファイル |
| CAPTCHA 認証 | 画像に含まれる文字を読み取り、入力することで人間と機械を判別する認証 |
| cron | Unix 系 OS において、コマンドを定期的に実行するために用いられる。 |
| XML | Extensible Markup Language の略。インターネット上で様々なデータを扱う場合に有効で、多様な情報を「情報の意味」と「情報の内容」に分けてテキストで記述する方法（言語）のこと |
| Permission | Android プラットフォームのセキュリティ機能であり、アプリケーションが必要とする権限を開発者があらかじめ明示し、インストール時にユーザーがそれを確認することで、インストールの可否を判断できる仕組み |
| SMS | 相手先の電話番号だけで約 70 文字前後のメッセージが手軽に送受信できる、ショートメッセージサービス |
| SQL インジェクション | アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しない SQL 文を実行させることにより、データベースシステムを不正に操作する攻撃方法 |
| クロスサイトスクリプト | Web アプリケーションの不適切な入力確認による脆弱性、あるいはそれを利用した攻撃 |
| クロスサイトフォージェリー | Web アプリケーションが、本来拒否すべき他サイトからのリクエストを受信し処理する脆弱性、あるいはその脆弱性を利用した攻撃 |
| 契約者固有 ID(ICCID) | Integrated Circuit Card ID の略。SIM カードについている固有の ID である。 |
| 契約者固有 ID(IMSI) | International Mobile Subscriber Identity の略。契約者を一意に識別するもの |
| 静的解析 | Android アプリケーションの解析手法で、アプリケーションを実行せずに得られる情報（API:利用するアプリケーションインターフェース・バイトコード等）を基に利用者情報の送信有無・ |

| | |
|---|---|
| | 内容の解析を行うもの |
| 端末固有 ID(IMEI) | International Mobile Equipment Identity の略。端末を一意に識別するもの |
| デバイス固定 ID(MAC アドレス) | Media Access Control address の略。ネットワーク機器を識別するための装置固有のアドレス |

# 1　はじめに

本書は、平成 28 年度の総務省施策である「スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る実証調査研究の請負」の静的解析システムのシステム仕様書である。

# 2　システム構成

## 2.1　システム構成について

静的解析情報システム（以下、本システム）は、利用者に対して静的解析の依頼画面及び、統計情報画面を提供する「公開サーバー」と、Android アプリの静的解析を行い、解析結果を利用者にフィードバックする「バックエンドサーバー」で構成されている。

## 2.2　システム構成図

本システムの構成図を「図 2.2-1 システム構成図」に示す。

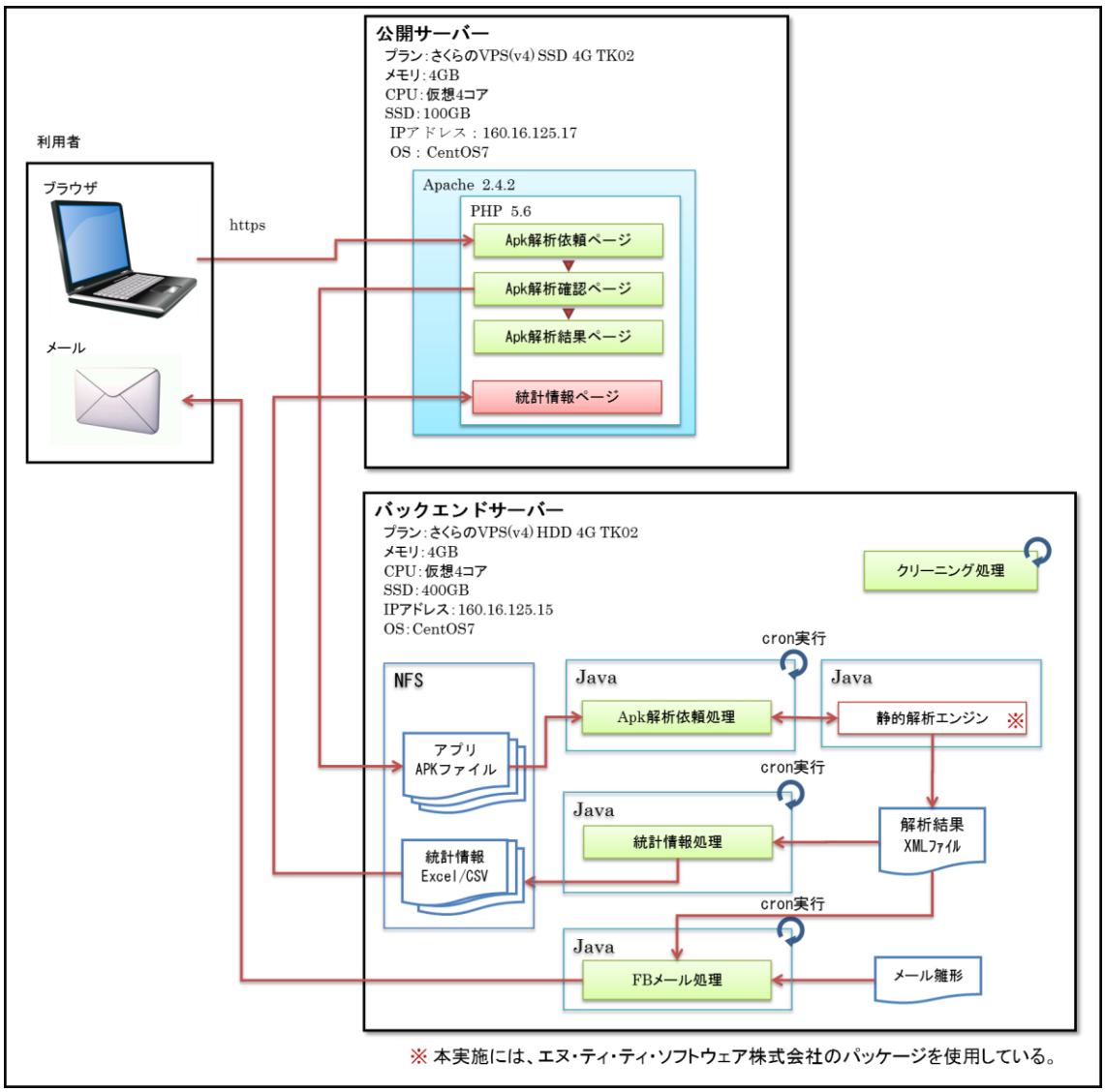



図 2.2-1 システム構成図

## 2.3 サービス一覧

公開サーバーと、バックエンドサーバーで利用するサービス・パッケージを「表 2.3-1 サービス・パッケージ一覧」に示す。

表 2.3-1 サービス・パッケージ一覧

| No. | サービス名 | 説明 | 公開※ | バック※ |
|---|---|---|---|---|
| 1 | yum-cron | パッケージ管理 yum の自動アップデート | ○ | ○ |
| 2 | tripwire | ファイル改ざん検知システム | ○ | ○ |
| 3 | rootkit | rootkit 検知ツール | ○ | ○ |
| 4 | clamav | アンチウィルスソフト（Clam AntiVirus） | ○ | ○ |
| 5 | firewalld | ファイヤーウォール | ○ | ○ |
| 6 | sshd | SSH サーバー。秘密鍵のログインのみ有効 | ○ | ○ |
| 7 | httpd | Web サーバー（Apache）+ PHP | ○ | |
| 8 | postfix | メールサーバー | ○ | ○ |
| 9 | postgresql | RDBMS(PostgreSQL) | | ○ |
| 10 | JDK | JavaSE | | ○ |
| 11 | nfs | NFS（ファイル共有） | | ○ |
| 12 | apk_analyze | apk 静的解析モジュール | | ○ |

※公開：公開サーバー、バック：バックエンドサーバーで当該サービスの利用有無を示す。

## 2.4 セキュリティ対策

### 2.4.1　ファイヤーウォール

CentOS7 にて必要なポートのみ開放をしている。

### 2.4.2　ファイル改ざんチェック

公開サーバー、バックエンドサーバーともに、ファイル改ざん検知システム Tripwire を導入し、定期的にファイル改ざんのチェックを行う。

### 2.4.3　ウィルス対策

公開サーバー、バックエンドサーバーともに、アンチウィルスソフトとして ClamAntiVirus を導入する。定義ファイルのアップデートを毎日行う。

### 2.4.4　SQL インジェクションへの対策

データベース（以下 DB）への接続に対しては、ユーザーからの入力パラメーターはすべて静的プレースホルダを利用することで SQL インジェクションへの対策としている。

### 2.4.5　クロスサイトスクリプトへの対策

公開サーバーにおいて、ユーザーからの入力パラメーターを、すべてエスケープ処理を行い出力する。

### 2.4.6　クロスサイトリクエストフォージェリーへの対策

公開サーバーでは、「図 2.4-1 キーの受信・埋め込みと送信」 のようにサーバーから受け取ったキーを利用する。

サーバーから返されたキーと送信確認画面から送られてきたキーが一致した場合に、apk ファイルの解析受付を行う。

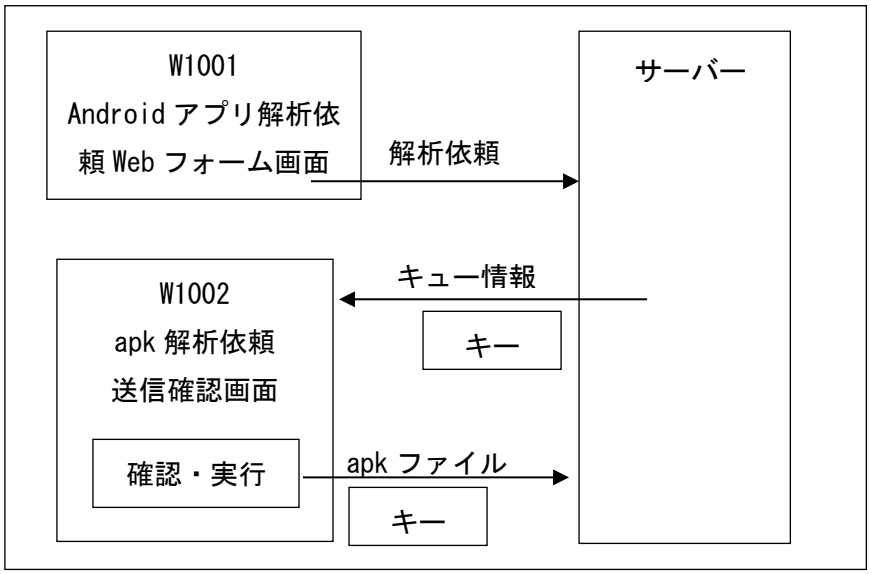



図 2.4-1 キーの受信・埋め込みと送信

### 2.4.7　連続アクセス・連投への対策

解析依頼を機械的に連投されないように、CAPTCHA 画像認証による対策を行う。

Android アプリ解析依頼画面 から解析依頼受付内容確認ダイアログを表示後に Android アプリ解析依頼画面に戻った場合、CAPTCHA 画像は更新される。

# 3 画面

## 3.1 画面一覧

本システムで提供する画面を、「表 3.1-1 画面一覧」に示す。

表 3.1-1 画面一覧

| 画面 ID | 画面名 | タイプ | 説明 |
|---|---|---|---|
| W0001 | タイトル | 画面 | タイトル画面 |
| W1001 | Android アプリ解析依頼 | 画面 | 解析依頼の必要事項を入力する画面 |
| W1002 | Android アプリ解析依頼内容確認 | ダイアログ | 解析依頼の入力内容を確認し、送信する画面 |
| W1003 | Android アプリ解析依頼受付拒否 | ダイアログ | 解析依頼を受付できなかったときの画面 |
| W1004 | Android アプリ解析受付完了 | 画面 | 依頼の受付が完了したときの画面 |
| W2001 | 統計情報 | 画面 | 統計情報をダウンロードする画面 |

## 3.2　画面遷移

本システムで提供する画面の遷移を、「図 3.2-1 画面遷移」に示す。

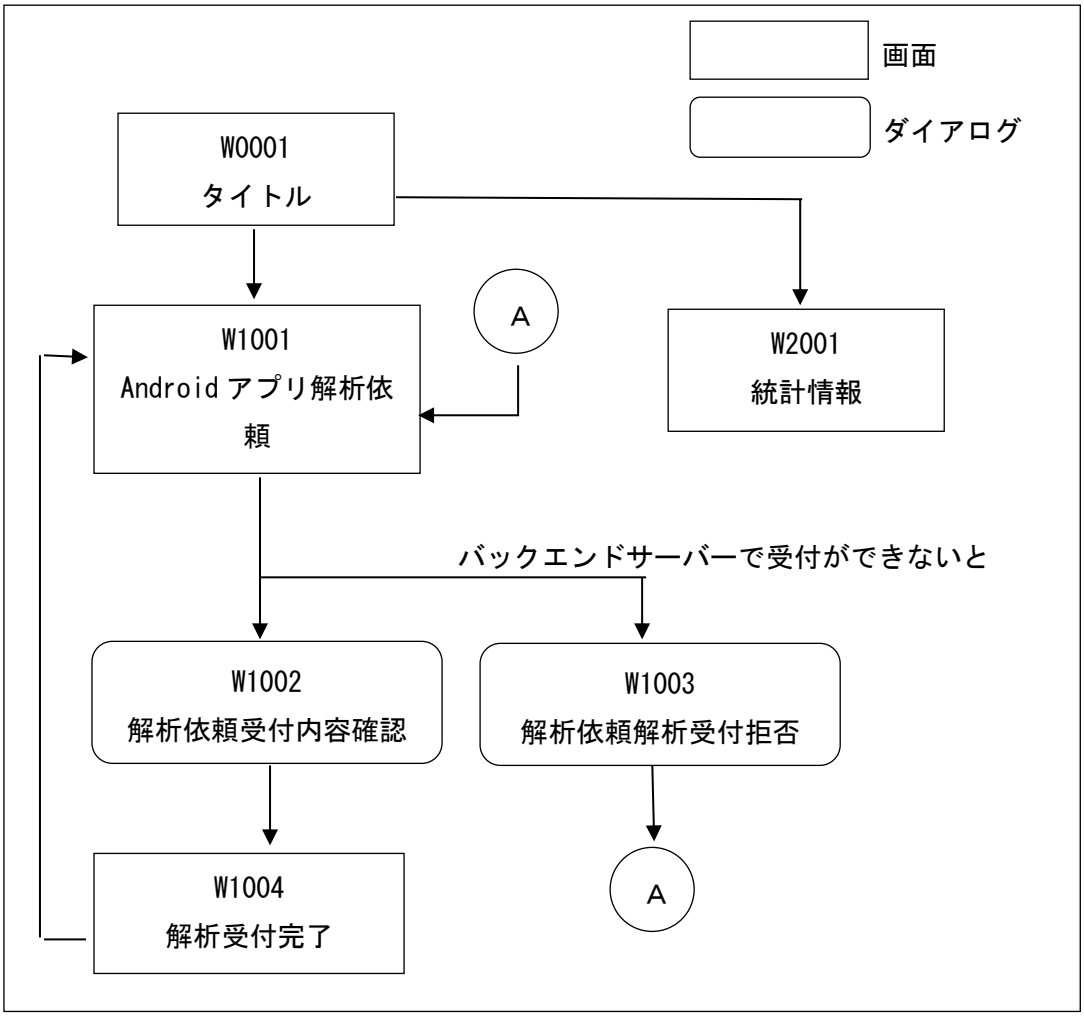
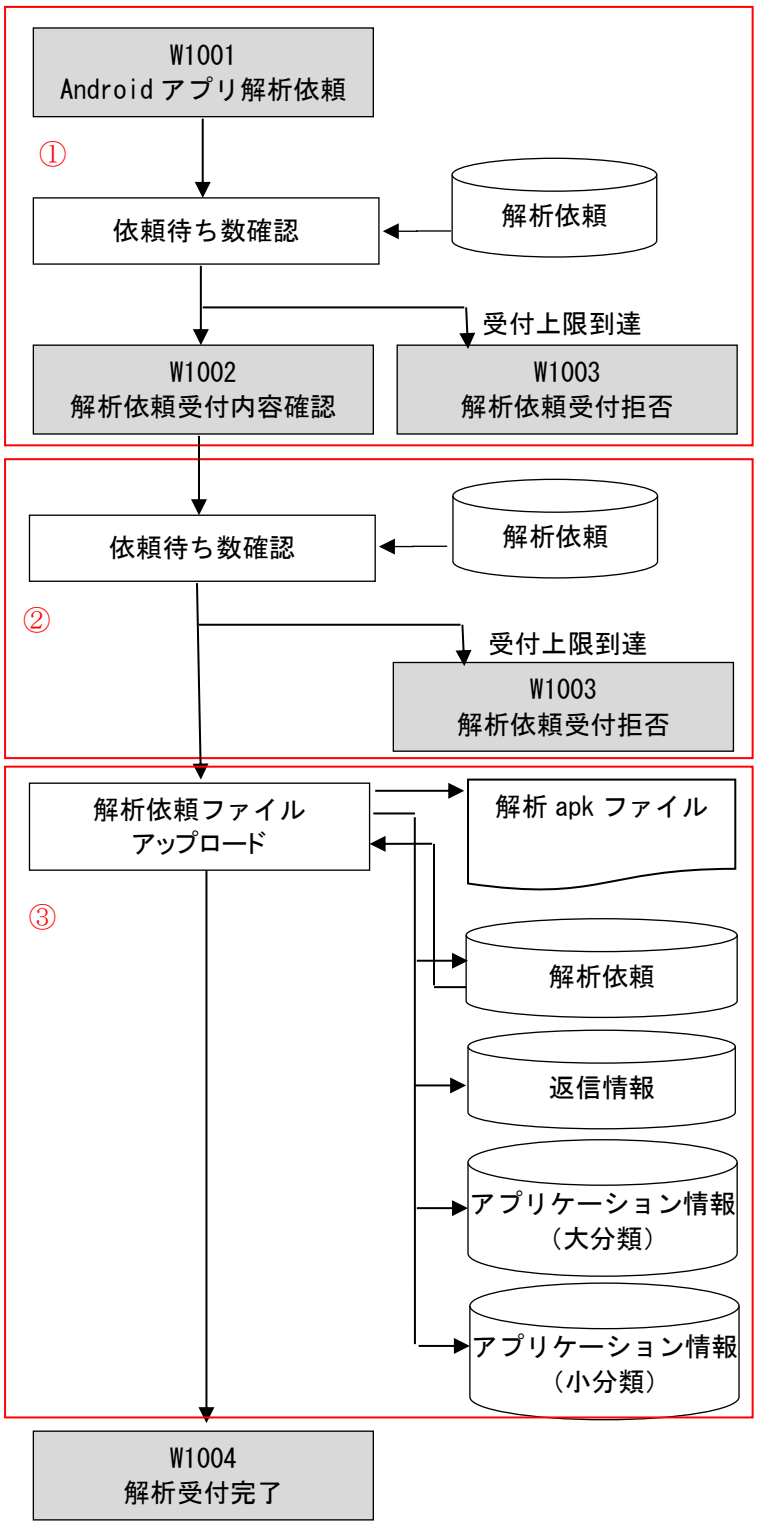



図 3.2-1 画面遷移

## 3.3 処理フロー

解析依頼処理のフローを、「図 3.3-1 処理フロー」に示す




①

- 解析処理待ち件数を「解析依頼」テーブルより取得する。
- 最大値（設定値）より多ければ解析依頼受付拒否ダイアログ表示。

②

- 確認中に受付上限に達したか確認のため、解析処理待ち件数再取得する。
- 最大値（設定値）より多ければ解析依頼受付拒否ダイアログ表示。

③

- apk ファイルをサーバーにアップロード。
- 「解析依頼」テーブルに新規レコードで「未解析」を登録し、連番となる受付番号を取得。
- 「返信情報」テーブルにメールアドレスと apk ファイル名を登録。
- 「アプリケーション情報（大分類）」テーブルに、カテゴリと利用回数を登録。
- 「アプリケーション情報（大分類）」テーブルに小カテゴリを登録。

図 3.3-1 処理フロー

# 4　画面レイアウト

## 4.1　W0001 タイトル

起点となるタイトル画面のレイアウトを、「図 4.1-1 タイトル画面」に示す。

この画面にある各項目については、「表 4.1-1 タイトル画面 詳細説明」、「表 4.1-2 タイトル画面 動作説明」 の通りである。

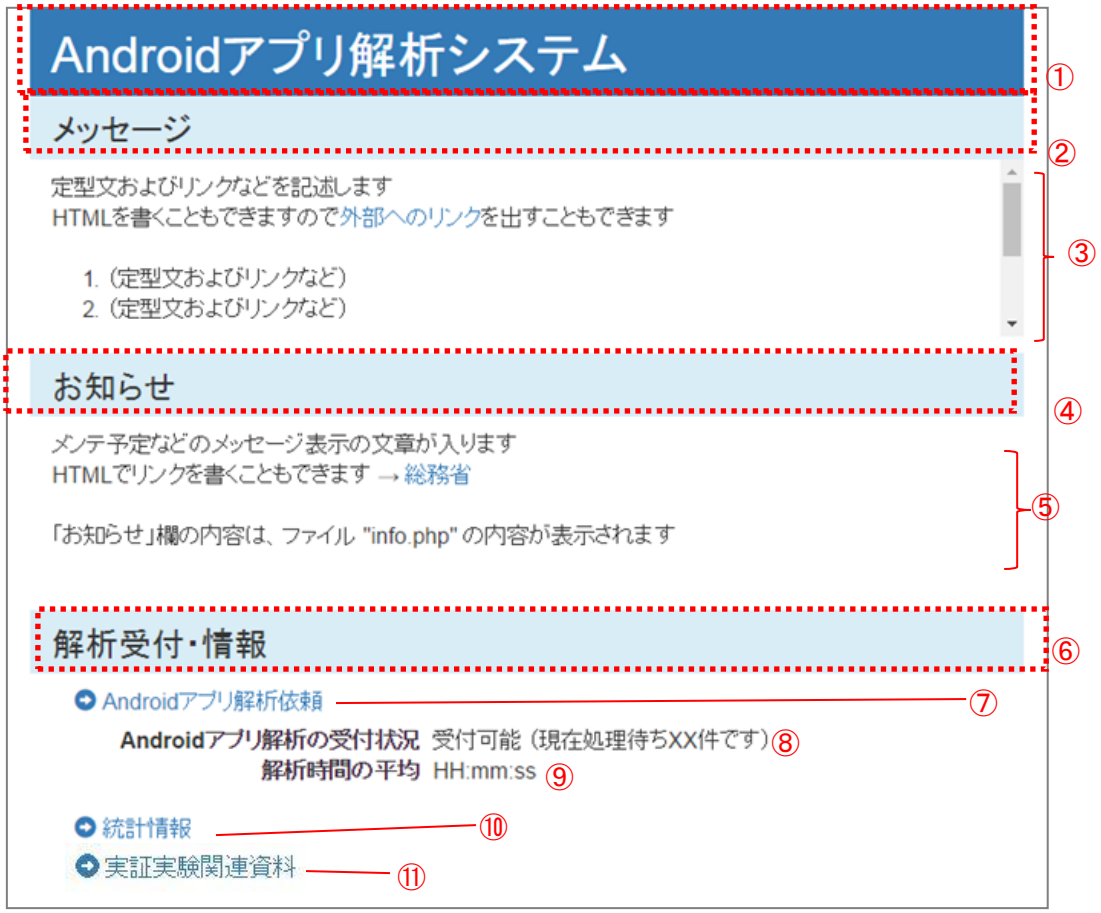



図 4.1-1 タイトル画面

表 4.1-1 タイトル画面 詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | Android アプリ解析システム | 表題 | テキスト |
| ② | 見出し 1 | メッセージ | メッセージ欄の見出し | テキスト |
| ③ | テキスト 1 | | メッセージ文 | 任意の文章 |
| ④ | 見出し 2 | お知らせ | お知らせ欄の見出し | テキスト |

| | | | | |
|---|---|---|---|---|
| ⑤ | テキスト 2 | | お知らせ文章 | 任意の文章 |
| ⑥ | 見出し 3 | 解析受付・情報 | 解析受付・統計情報へのリンク欄の見出し | テキスト |
| ⑦ | リンク 1 | Android アプリ解析依頼 | Android アプリ解析依頼へのリンク | リンク |
| ⑧ | テキスト 3 | Android アプリ解析の受付状況 | 現在の処理待ち件数を表示 | テキスト |
| ⑨ | テキスト 4 | 解析時間の平均 | 平均解析時間を表示 | テキスト |
| ⑩ | リンク 2 | 統計情報 | 統計情報へのリンク | リンク |
| ⑪ | リンク 3 | 実証実験関連資料 | ダウンロードサイトへのリンク | リンク |

表 4.1-2 タイトル画面 動作説明

| 項目 ID | 動作説明 |
|---|---|
| ③ | 任意に作成したメッセージ文章（定型文・リンクなど）を表示する。<br>外部ファイルの取り込み表示や HTML 形式ファイルの表示も可能。<br>5 行以上のときはスクロールバーが表示される。 |
| ④ | 任意に作成したお知らせ文章（メンテ予定など）を表示する。<br>外部ファイルの取り込み表示や HTML 形式ファイルの表示も可能。<br>5 行以上のときはスクロールバーが表示される。 |
| ⑦ | W1001 Android アプリ解析依頼 へ遷移するリンク。<br>「Android アプリ解析の受付状況」が受付不可の場合には、リンクとして表れずにただのテキストとなる<br>※実証実験ではこのリンクの前に説明文章を挿入した。 |
| ⑧ | Android アプリ解析の解析処理待ち件数を表示する。<br>解析待ち件数は、「解析依頼」テーブルの解析状況が「未解析」「処理中」のものの件数を取得する。 |
| ⑨ | Android アプリ解析平均時間情報を表示する。<br>解析時間の平均は、「解析依頼」テーブルの解析状況が「解析済」のもので最近 10 件分の解析時間の平均時間とする。 |
| ⑩ | W2001 統計情報 へ遷移するリンク<br>※実証実験ではこのリンクの前に説明文章を挿入した。 |
| ⑪ | 実証実験関連のダウンロードサイトへ遷移するリンク<br>※実証実験ではこのリンクの前に説明文章を挿入した。 |

## 4.2　W1001 Android アプリ解析依頼

Android アプリの解析を依頼する画面のレイアウトを、「図 4.2-1 Android アプリ解析依頼」に示す。また、アプリケーション分野の小分類を指定する場合のレイアウトを「図 4.2-2 Android アプリ解析依頼 小カテゴリ選択メニュー」に示す。

この画面にある各項目については、「表 4.2-1 Android アプリ解析依頼 」、「表 4.2-2 Android アプリ解析依頼 動作説明」 の通りである。


図 4.2-1 Android アプリ解析依頼画面


図 4.2-2 Android アプリ解析依頼 小カテゴリ選択メニュー

表 4.2-1 Androidアプリ解析依頼 詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | Android アプリ解析依頼 | 表題 | テキスト |
| ② | リンク | タイトルへ戻る | W0001 タイトルへのリンク | リンク |
| ③ | 入力フォーム1 | apkファイル指定 | apkファイル指定 | ファイル指定フォーム |
| | | ファイル選択 | apk ファイル指定ボタン | ボタン |
| ④ | 入力フォーム2 | 本システム利用者 | 利用者の種別を指定 | プルダウンメニュー |
| ⑤ | 入力フォーム3 | 本システムの利用回数 | 利用回数を指定 | プルダウンメニュー |
| ⑥ | 入力フォーム4 | アプリケーション分野 | 検査アプリケーションをカテゴリ指定 | プルダウンメニュー |
| ⑦ | 入力フォーム5 | メールアドレス入力欄 | メールアドレス入力（1つは確認用） | テキストボックス |
| ⑧ | テキスト | 利用規約 | 利用規約 | テキスト |
| ⑨ | 入力フォーム6 | 本システムの利用規約に同意する | 利用規約確認時にチェックを入れる | チェックボックス |
| ⑩ | 認証用画像 | | CAPTCHA画像 | 画像 |
| ⑪ | 入力フォーム7 | 左の数字を入力してください | CAPTCHA 画像の数値入力 | テキストボックス |
| ⑫ | ボタン | 解析依頼 | 解析依頼ボタン | ボタン |
| ⑬ | テキストラベル | 必須 | 必須入力項目ラベル | テキスト |
| ⑭ | 入力フォーム8 | 小カテゴリ | ⑥で指定したアプリケーション分野の下の小カテゴリリスト | チェックボックス |

表 4.2-2 Androidアプリ解析依頼 動作説明

| 項目ID | 動作説明 |
|---|---|
| ② | W0001 タイトル へ遷移する |
| ③ | Webブラウザのファイル指定ダイアログを開きファイルを指定する。指定したファイル名がテキストボックスに表示される。<br>必須入力項目 |
| ④ | 利用者種別を選択する。<br>利用者種別の選択項目は、「利用者マスター」テーブルの削除フラグが立っていないものを表示順に従い表示する。<br>必須入力項目 |
| ⑤ | 「初回」「二回目」～「四回目」「五回以上」から選択する<br>必須入力項目 |
| ⑥ | アプリケーションのカテゴリを選択する。<br>カテゴリの選択項目は、「大カテゴリマスター」テーブルの削除フラグが立っていないものを表示順に従い表示する。<br>必須入力項目 |
| ⑦ | メールアドレス入力欄、および、確認入力欄<br>・　ふたつのテキストボックスに入力されたメールアドレスが一致<br>・　メールアドレスとして正しい<br>上記二点が等しいことのチェックを行う<br>必須入力項目 |
| ⑧⑨ | ⑧の利用規約に同意するか否かを⑨にチェックする（同意のときチェック）<br>⑧の利用規約欄は縦方向へのスクロールバーを表示する<br>⑨は必須入力項目 |
| ⑩⑪ | ⑩に表示された数字を⑪に入力し、認証を行う<br>⑪は必須入力項目 |
| ⑫ | W1002 解析依頼受付内容確認 を表示する。<br>必須入力項目への入力がすべて正しく行われた場合にボタンを押すことが可能になる |
| ⑫ | 必須入力項目に対して「必須」の文字をラベル横に表示する。<br>必須入力項目を入力した場合、表示が消える。 |
| ⑭ | ⑥で選択された大カテゴリ配下の小カテゴリー覧を、「小カテゴリマスター」テーブルから削除フラグが立っていないものを取得し、表示順に従い表示する。<br>チェックボックスによる複数選択が可能 |

## 4.3　Android アプリ解析依頼確認画面

Android アプリ解析依頼確認画面は、W1001 Android アプリ解析依頼 上にダイアログとして表示される。

このとき、解析処理待ち件数が受付最大値（設定値）以下の場合は W1002 解析依頼受付内容確認 を表示し、受付最大値を超えている場合は W1003 解析依頼受付拒否 を表示する。

### 4.3.1　W1002 解析依頼受付内容確認

解析依頼受付内容確認ダイアログのレイアウトを、「図 4.3-1 解析依頼内容確認ダイアログ」 に示す。このダイアログは、解析依頼のための apk ファイルアップロードが始まると「図 4.3-2 アップロード中ダイアログ」 に示す表示に変わる。この画面にある各項目については、「表 4.3-1 解析依頼内容確認ダイアログ 詳細説明」、「表 4.3-2 解析依頼内容確認ダイアログ 動作説明」 の通りである。


図 4.3-1 解析依頼内容確認ダイアログ


図 4.3-2 アップロード中ダイアログ

表 4.3-1 解析依頼内容確認ダイアログ 詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | 送信内容確認 | ダイアログタイトル | テキスト |
| ② | ボタン 1 | ×（閉じる） | ダイアログを閉じる（動作は⑨キャンセルボタンと同じ） | ボタン |
| ③ | テキスト 1 | apk ファイル指定 | W1001 で選択したファイル名 | テキスト |
| ④ | テキスト 2 | 本システム利用者 | W1001 で選択したシステム利用者種別 | テキスト |
| ⑤ | テキスト 3 | 本システムの利用回数 | W1001 で選択したシステム利用回数 | テキスト |
| ⑥ | テキスト 4 | アプリケーション分野 | W1001 で選択したアプリケーション分野と、チェックした小カテゴリを括弧内に表示 | テキスト |
| ⑦ | テキスト 5 | メールアドレス | W1001 で入力したメールアドレス | テキスト |
| ⑧ | テキスト 6 | 以上の内容で解析を依頼します | | テキスト |
| ⑨ | ボタン 2 | キャンセル | キャンセルボタン | ボタン |
| ⑩ | ボタン 3 | 依頼 | 依頼ボタン | ボタン |
| ⑪ | テキスト 7 | apk ファイルのアップロードをしています | | テキスト |
| ⑫ | プログレスバー | | プログレスバー | プログレスバー |

表 4.3-2 解析依頼内容確認ダイアログ 動作説明

| 項目 ID | 動作説明 |
|---|---|
| ③④⑤⑥⑦ | W1001 Android アプリ解析依頼 で入力した内容を表示する |
| ②⑨ | ダイアログを閉じ、W1001 Android アプリ解析依頼 に戻る |
| ⑩ | apk ファイルを送信する。⑧のテキストを⑪の表示に変更し、⑨⑩のボタ |

| | |
|---|---|
| | ンが表示されていた場所に⑫のプログレスバーを表示 |
| ⑪⑫ | 送信完了後に W1004 解析受付完了 へと遷移 |

### 4.3.2　W1003 解析依頼受付拒否

解析依頼受付拒否ダイアログのレイアウトを、「図 4.3-3　解析依頼受付拒否ダイアログ」に示す。

この画面で利用する部品とその項目概要については、「表 4.3-3 解析依頼受付拒否ダイアログ詳細説明」、「表 4.3-4 解析依頼受付拒否ダイアログ 動作説明」 の通りである。

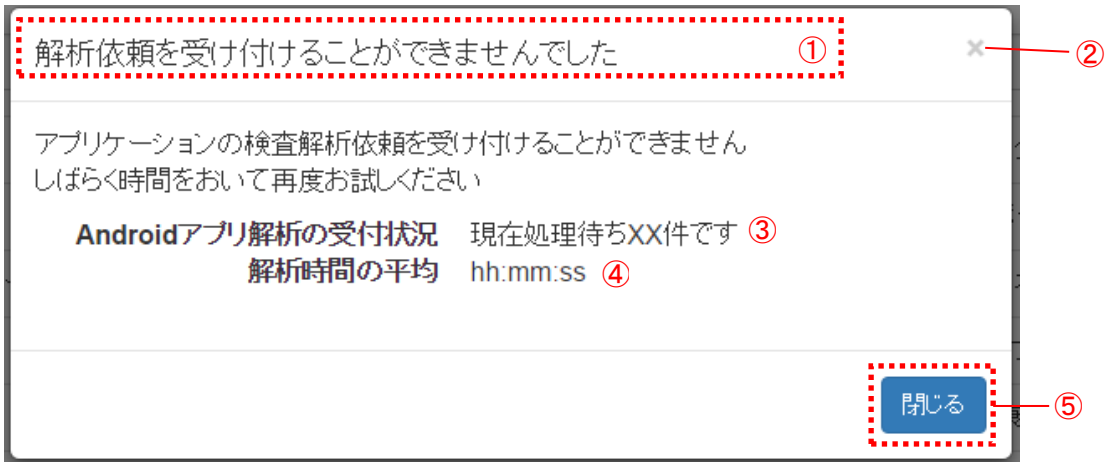



図 4.3-3　解析依頼受付拒否ダイアログ

表 4.3-3 解析依頼受付拒否ダイアログ詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | 解析を受け付けることができませんでした | ダイアログタイトル | テキスト |
| ② | ボタン 1 | ×（閉じる） | ダイアログを閉じる（動作は⑤閉じるボタンと同じ） | ボタン |
| ③ | テキスト 1 | Android アプリ解析の受付状況 | 現在の処理待ち件数を表示 | テキスト |
| ④ | テキスト 2 | 解析時間の平均 | 平均解析時間を表示 | テキスト |
| ⑤ | ボタン 2 | 閉じる | 閉じるボタン | ボタン |

表 4.3-4 解析依頼受付拒否ダイアログ 動作説明

| 項目 ID | 動作説明 |
|---|---|
| ③ | Android アプリ解析の解析処理待ち件数を表示する。<br>解析待ち件数は、「解析依頼」テーブルの解析状況が「未解析」「処理中」のものの件数を取得する。 |
| ④ | Android アプリ解析平均時間情報を表示する。<br>解析時間の平均は、「解析依頼」テーブルの解析状況が「解析済」のもので最近 10 件分の解析時間の平均時間とする。 |
| ②⑤ | ダイアログを閉じ、W1001 Android アプリ解析依頼 に戻る |

## 4.4　W1004 解析受付完了

解析受付完了画面を、「図 4.4-1 解析受付完了画面」に示す。

この画面で利用する部品とその項目概要については、「表 4.4-1 解析受付完了 詳細説明」、「表 4.4-2 解析受付完了 動作説明」 の通りである。

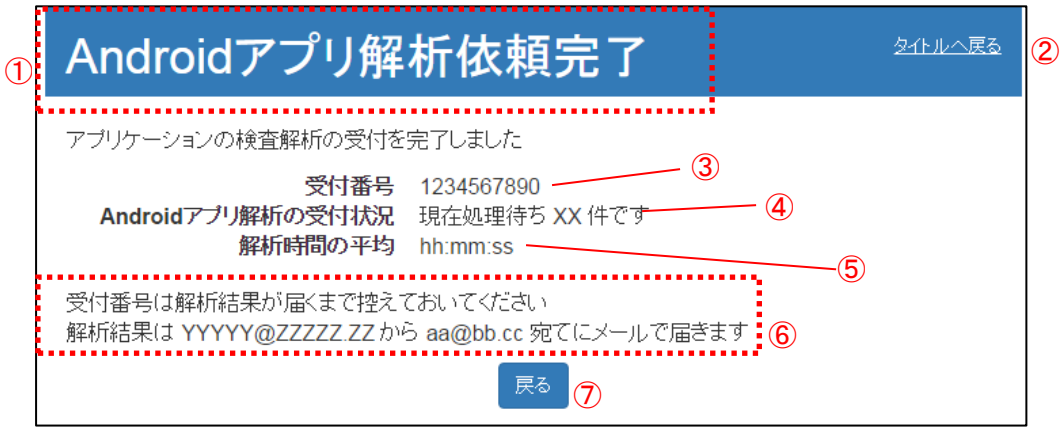



図 4.4-1 解析受付完了画面

表 4.4-1 解析受付完了 詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | Android アプリ解析依頼完了 | 表題 | テキスト |
| ② | リンク | タイトルへ戻る | W0001 タイトルへのリンク | リンク |
| ③ | テキスト 1 | 受付番号 | 受付番号 | テキスト |
| ④ | テキスト 2 | Android アプリ解析の受付状況 | 現在の処理待ち件数を表示 | テキスト |
| ⑤ | テキスト 3 | 解析時間の平均 | 平均解析時間を表示 | テキスト |
| ⑥ | テキスト 4 | 解析結果は【送信メールアドレス】から【メールアドレス】宛てにメールで届きます | 解析結果連絡方法通知などメッセージ欄 | テキスト |
| ⑥ | ボタン | 戻る | 戻るボタン | ボタン |

表 4.4-2 解析受付完了 動作説明

| 項目 ID | 動作説明 |
|---|---|
| ② | Android アプリ解析の受付番号を表示する。 |
| ③ | Android アプリ解析の解析処理待ち件数を表示する。<br>解析時間の平均は、「解析依頼」テーブルの解析状況が「解析済」のもので最近 10 件分の解析時間の平均時間とする。 |
| ④ | Android アプリ解析平均時間情報を表示する。<br>解析時間の平均は、「解析依頼」テーブルの解析状況が「解析済」のもので最近 10 件分の解析時間の平均時間とする。 |
| ⑦ | メールアドレスは W1001 Android アプリ解析依頼 で入力されたものを表示する。 |
| ⑧ | W1001 Android アプリ解析依頼 へ遷移する。 |

## 4.5　W2001 統計情報

統計情報画面 を、「図 4.5-1 統計情報画面」に示す。

この画面で利用する部品とその項目概要については、「表 4.5-1 統計情報詳細説明」、「表 4.5-2 統計情報詳細項目の動作説明」 の通りである。

作成された統計情報ファイルをダウンロードすることができる。


図 4.5-1 統計情報画面

表 4.5-1 統計情報詳細説明

| 項目 ID | 項目 | ラベル | 説明 | 部品種類 |
|---|---|---|---|---|
| ① | タイトル | 統計情報 | 表題 | テキスト |
| ② | リンク 1 | タイトルへ戻る | W0001 タイトルへのリンク | リンク |
| ③ | 見出し 1 | リアルタイム情報 | リアルタイム情報の見出し | テキスト |
| ④ | テキスト 1 | Android アプリ解析の受付状況 | 受付可否と、受付可のときは現在の処理待ち件数を表示 | テキスト |
| ⑤ | テキスト 2 | 解析時間の平均 | 平均解析時間を | テキスト |

| | | | | |
|---|---|---|---|---|
| | | | 表示 | |
| ⑥ | 見出し 2 | Android アプリ静的解析 統計情報ダウンロード | 統計情報ダウンロード欄の見出し | テキスト |
| ⑦ | テキスト 3 | YYYY 年 MM 月 | ダウンロード対象年月 | テキスト |
| ⑧ | リンク 2 | 統計情報ダウンロード対象ファイル名 | 統計情報ファイルへのリンク | リンク |

表 4.5-2 統計情報詳細項目の動作説明

| 項目 ID | 動作説明 |
|---|---|
| ② | クリックすると、W0001 タイトルへ遷移する |
| ④ | Android アプリ解析の解析処理待ち件数を表示する。<br>解析待ち件数は、「解析依頼」テーブルの解析状況が「未解析」「処理中」のものの件数を取得する。 |
| ⑤ | Android アプリ解析平均時間情報を表示する。<br>解析時間の平均は、「解析依頼」テーブルの解析状況が「解析済」のもので最近 10 件分の解析時間の平均時間とする。 |
| ⑦<br>⑧ | 統計情報でダウンロードできるログの年月を表示・ファイル名でリンクを作成し、クリックすることでダウンロードを行う |

# 5　バッチ処理

## 5.1 バッチ処理一覧

本システムのバッチ処理の一覧を「表 5.1-1 バッチ処理一覧」に示す。
B0009 Android アプリ静的モジュール については、別途インターフェース仕様書に示す。

表 5.1-1 バッチ処理一覧

| No. | バッチ処理名 | バッチ処理 ID | 処理概要 | 処理方式(サイクル) | 備考 |
|---|---|---|---|---|---|
| 1 | apk 解析依頼処理 | B0001 | Android アプリ静的解析依頼状況を確認し、依頼が在る場合は、「Android アプリ静的解析」を実行する。<br>Android アプリ静的解析結果を解析し、DB に蓄積。及び解析結果を依頼者にメール送信する。<br>メール送信後、apk ファイルを削除し、依頼者のメール情報、不要となったファイルを削除する。 | cron<br>(1 分毎) | |
| 2 | 統計情報処理 | B0002 | DB より月の累計データを取得し、統計情報を作成し、ファイルに出力する。 | cron<br>(月次) | |
| 3 | Android アプリ静的解析モジュール | B0009 | apk ファイルの静的解析を行う | B0001 から起動 | エヌ・ティ・ティ・ソフトウェア株式会社のパッケージを使用 |

## 5.2 バッチ構成図

本システムのバッチ処理の構成を「図 5.2-1 バッチ構成図」に示す。

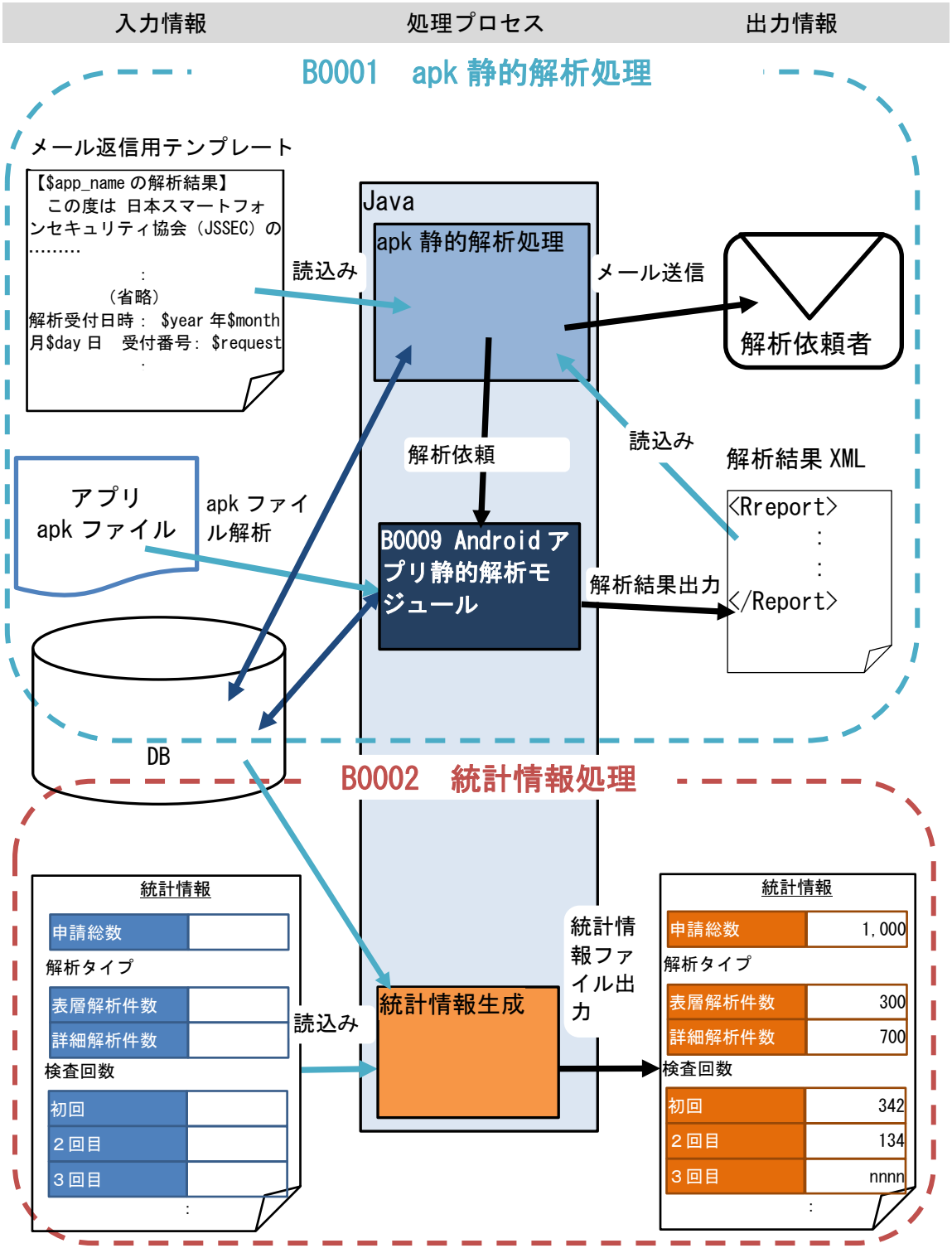


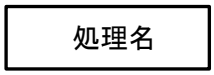
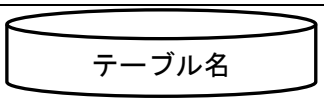
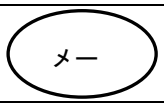
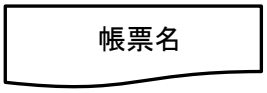

図 5.2-1 バッチ構成図

## 5.3 バッチ処理フロー

### 5.3.1　処理フローの凡例

バッチ処理フローの凡例を「表 5.3-1　バッチ処理フロー凡例」に示す。

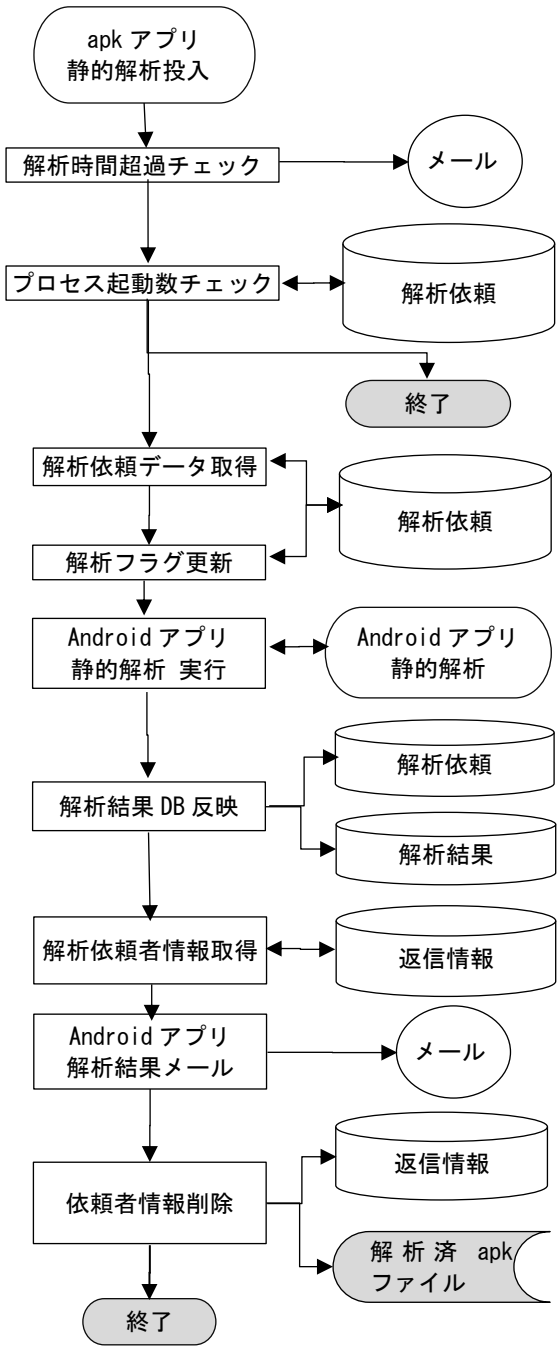
表 5.3-1　バッチ処理フロー凡例

| 用語 | 内容 |
|---|---|
|  | ジョブ（フロー開始）を表す記号 |
|  | 処理を表す記号 |
|  | ファイルを表す記号 |
|  | DB のテーブルを表す記号 |
|  | E メールを表す記号 |
|  | 帳票(Excel)を表す記号 |
|  | 処理の終了を表す記号 |
|  | ファイル削除を表す記号 |

### 5.3.2　apk アプリ静的解析依頼 処理フロー

apk アプリ静的解析依頼バッチ処理のフローを「図 5.3-1　Android アプリ静的解析依頼 処理フロー図」に示す。

| バッチ処理 ID | B0001 | バッチ処理名 | apk アプリ静的解析依頼 | 処理概要 |
|---|---|---|---|---|




**■プロセス起動数チェック**
・解析処理開始時刻から 3 時間以上経っているものは、システム異常のエラーとして依頼者に解析結果メールを送信する

**■プロセス起動数チェック**
・「Android アプリ静的解析」の解析中数が 1 以上の場合、処理を終了する。
但し、処理開始時刻から 3 時間以上経っている場合、処理中とカウントしない。

**■解析依頼データ取得**
・「解析依頼」テーブルより、解析状況が「未解析」で待ち時間が一番長いアプリ情報を取得。

**■解析フラグ更新**
・「解析依頼」テーブルの対象レコードを「解析中」に更新。

**■Android アプリ静的解析 実行**
・「Android アプリ静的解析」を起動し応答を待つ。

**■Android アプリ解析結果 DB 登録**
・「解析依頼」テーブルの対象レコードを「解析済」に更新。
・解析結果を「解析結果」テーブルに登録。

**■解析依頼者情報取得**
・「解析依頼」テーブルから解析した依頼者情報を取得。

**■Android アプリ解析結果メール**
・Android アプリ静的解析結果を成型して依頼者にメールを送信する。

**■依頼者情報削除**
・「返信情報」テーブルに登録している依頼者メールの情報を削除、及び解析したアプリケーションファイルを削除。

図 5.3-1　Android アプリ静的解析依頼 処理フロー図

### 5.3.3　統計情報 処理フロー

統計情報バッチ処理のフローを「図 5.3-2　統計情報 処理フロー図」に示す。

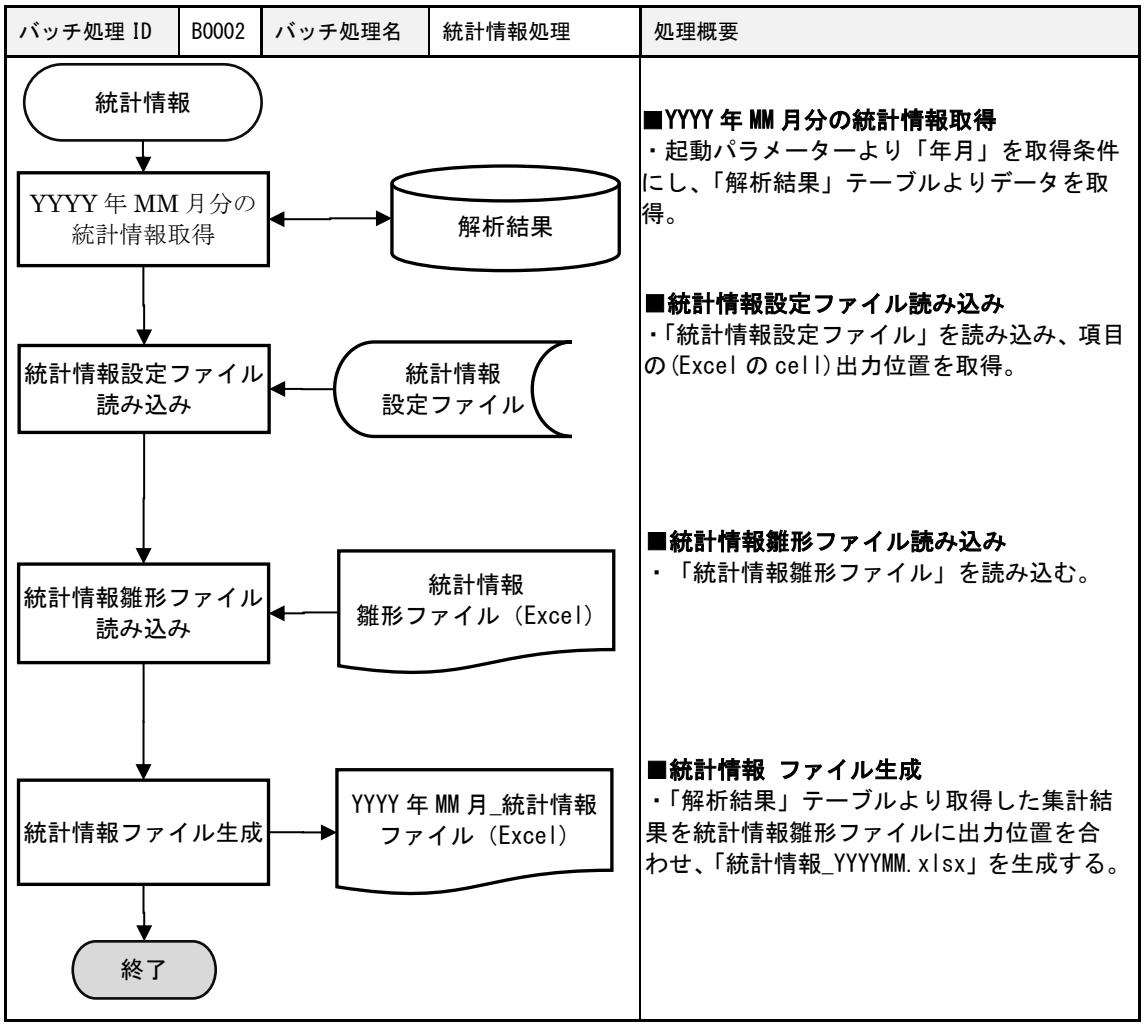



図 5.3-2　統計情報 処理フロー図

# 6 データ設計

## 6.1 スキーマー覧

DB 上のスキーマを「表 6.1-1　スキーマー覧」に示す。

表 6.1-1　スキーマー覧

| スキーマ名 | 説明 |
|---|---|
| web_analyze | 静的解析・統計情報システムで使用する DB |
| apk_analyze | 静的解析モジュールで使用する DB |

## 6.2 テーブルー覧

DB 上のテーブルを「表 6.2-1　テーブルー覧」に示す。

表 6.2-1　テーブルー覧

| スキーマ名 | テーブル名 | 説明 |
|---|---|---|
| web_analyze | application_info_category | 解析依頼 |
| | response_info | 返信情報 |
| | application_info_category | アプリケーション情報(大分類) |
| | application_info_family | アプリケーション情報(小分類) |
| | analysis_response | 解析結果 |
| | service_user | 利用者マスター |
| | category | 大カテゴリマスター |
| | family | 小カテゴリマスター |
| apk_analyze | dev | 開発者情報 |
| | lib | ライブラリー情報 |
| | module | モジュール情報 |

## 6.3 テーブル詳細

### 6.3.1　スキーマ web_analyze 上のテーブル詳細

スキーマ web_analyze 上のテーブルの詳細を 「表 6.3-1」 ～「表 6.3-7」 に示す。

表 6.3-1 解析依頼 analysis_request

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 受付番号 | request_no | integer | 4 | ○ | ○ | ○ | オートインクリメント |
| 2 | 解析状態 | analysis_status | smallint | 2 | | ○ | | 0:未実施<br>1:解析中<br>2:解析済<br>3.異常 |
| 3 | 申請日時 | request_datetime | timestamp | 8 | | ○ | | |
| 4 | 解析開始時刻 | analysis_starttime | timestamp | 8 | | | | |
| 5 | 解析終了時刻 | analysis_endtime | timestamp | 8 | | | | |
| 6 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 7 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-2 アプリケーション情報(大分類)　application_info_category

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 受付番号 | request_no | integer | 4 | ○ | ○ | ○ | |
| 2 | 本システム利用者 | service_user | smallint | 2 | ○ | ○ | | |
| 3 | 本システム利用回数 | analysis_count | smallint | 2 | ○ | ○ | | |
| 4 | 大カテゴリ | category | smallint | 2 | | ○ | | |
| 5 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 6 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-3 アプリケーション情報(小分類)　application_info_family

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 受付番号 | request_no | integer | 4 | ○ | ○ | ○ | |
| 2 | 大カテゴリ | category | smallint | 2 | ○ | ○ | | |
| 3 | 小カテゴリ | family | smallint | 2 | ○ | ○ | | |
| 4 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 5 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-4 解析結果 analysis_response

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 受付番号 | request_no | integer | 4 | ○ | ○ | ○ | |
| 2 | 解析結果状態 | analysis_response_status | char | 2 | | ○ | | 00:解析処理成功<br>01:制限時間超過<br>02:表層解析不可<br>03:フロー解析エラー<br>04:内部処理エラー |
| 3 | Permission | permission | integer | 4 | | ○ | | AndroidManifest.xml で定義された uses-permission 要素の android:name 属性 |
| 4 | 動的クラスローダー実行数 | class_loader_execute_count | integer | 4 | | | | 検出有の件数 |
| 5 | 内部 Script 実行数 | script_execcute_count | integer | 4 | | | | 検出有の件数 |
| 6 | 利用者情報の送信 | result | smallint | 2 | | ○ | | 0：送信検出無<br>1：送信検出有 |
| 7 | OS 生成 ID | os | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 8 | 端末固有 ID(IMEI) | imei | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 9 | 契約者固有 ID(IMSI) | imsi | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 10 | 契約者固有ID(ICCID) | iccid | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 11 | デバイス固定 ID(MACアドレス) | macaddress | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 12 | 電話番号 | tel | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 13 | メールアドレス | mail | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 14 | 位置 | area | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 15 | アドレス帳 | address_book | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 16 | マイク | microphone | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 17 | カメラ | camera | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 18 | 加速度センサー | sensor | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 19 | SMS | sms | smallint | 2 | | | | 0：送信検出無<br>1：送信検出有 |
| 20 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 21 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-5 利用者マスター service_user

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 利用者 ID | service_user_id | integer | 4 | ○ | ○ | ○ | |
| 2 | 利用者名称 | service_user_name | varchar | 96 | | ○ | | |
| 3 | 表示順 | display_order | integer | 4 | | ○ | ○ | |
| 4 | 削除フラグ | delete_flg | smallint | 2 | | ○ | | 1:削除 |
| 5 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 6 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-6 大カテゴリマスター category

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 大カテゴリ ID | category_id | integer | 4 | ○ | ○ | ○ | |
| 2 | 大カテゴリ名 | category_name | varchar | 64 | | ○ | | |
| 3 | 表示順 | display_order | integer | 4 | | ○ | ○ | |
| 4 | 削除フラグ | delete_flg | smallint | 2 | | ○ | | 1:削除 |
| 5 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 6 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

表 6.3-7 小カテゴリマスター family

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | 大カテゴリ ID | category_id | integer | 4 | ○ | ○ | | |
| 2 | 小カテゴリ ID | family_id | integer | 4 | ○ | ○ | | |
| 3 | 小カテゴリ名 | family_name | varchar | 64 | | ○ | | |
| 4 | 表示順 | display_order | integer | 4 | | ○ | ○ | |
| 5 | 削除フラグ | delete_flg | smallint | 2 | | ○ | | 1:削除 |
| 6 | 登録日時 | insert_datetime | timestamp | 8 | | ○ | | |
| 7 | 更新日時 | update_datetime | timestamp | 8 | | ○ | | |

### 6.3.2　スキーマ apk_analyze 上のテーブル詳細

スキーマ apk_analyze 上のテーブルの詳細を 「表 6.3-8」 ～ 「表 6.3-10」 に示す。

表 6.3-8 モジュール情報 module

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | モジュール番号 | mod_id | integer | 4 | ○ | ○ | ○ | |
| 2 | メソッド名 | method | varchar | 1024 | | ○ | | 含むクラス名 |
| 3 | ライブラリー番号 | lib_id | integer | 4 | | ○ | | |
| 4 | 作成日時 | created_at | timestamp | 8 | | ○ | | |
| 5 | 更新日時 | updated_at | timestamp | 8 | | ○ | | |
| 6 | 登録根拠の情報 | source | integer | 4 | | ○ | | 1：公開仕<br>2:静的解析（許諾有）<br>3:静的解析（許諾無） |

表 6.3-9 ライブラリー情報 lib

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | ライブラリー番号 | lib_id | integer | 4 | ○ | ○ | ○ | |
| 2 | ライブラリー名 | library | varchar | 1024 | | ○ | | |
| 3 | 事業者番号 | dev_id | integer | 4 | | ○ | | |
| 4 | 作成日時 | created_at | timestamp | 8 | | ○ | | |
| 5 | 更新日時 | updated_at | timestamp | 8 | | ○ | | |
| 6 | 収集元の情報 | source | integer | 4 | | ○ | | 1:システム検証<br>2：SPI II |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 3：JSSEC |
| 7 | ライブラリー仕様公開状態 | status | integer | 4 | | ○ | | 1：ライブラリーの仕様が公開されている<br>2：ライブラリーの仕様は非公開 |
| 8 | 法的状態 | regal | integer | 4 | | ○ | | 1:利用規約なし<br>2:利用規約はあるがリバースエンジニアリングに関する記載はない<br>3:利用規約にリバースエンジニアリングに関する記載があり、許容されている<br>4:利用規約にリバースエンジニアリングに関する記載があり、明示的に拒否されている |
| 9 | 法的状態（付加情報） | regal_op | integer | 4 | | ○ | | 1:申請書を受領しており解析に関する許諾を得ている<br>2:申請されていないが実証実験目的とし |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | て解析を実施する<br>3:明示的に断られたが、実証実験目的として解析を実施する |
| 10 | モジュールのプライバシーポリシーURL | policy | varchar | 1024 | | | | |
| 11 | 利用目的 | purpose | integer | 4 | | | | 1：広告<br>2：利用解析<br>3:仲介型広告<br>4：開発支援<br>5:認証・識別 |
| 12 | バージョン | version | varchar | 1024 | | | | |

表 6.3-10 開発者情報 dev

| No | カラム(論理) | カラム(物理) | 型 | 長さ | Primary | Not Null | Unique | 備考 |
|---|---|---|---|---|---|---|---|---|
| 1 | dev_id | ライブラリー番号 | integer | 4 | ○ | ○ | ○ | |
| 2 | dev | ライブラリー名 | varchar | 1024 | | ○ | | |
| 3 | devurl | 事業者番号 | varchar | 1024 | | ○ | | |
| 4 | created_at | 作成日時 | timestamp | 8 | | ○ | | |
| 5 | updated_at | 更新日時 | timestamp | 8 | | ○ | | |

# 7　メール本文作成

メール本文の作成は、ApacheJakarta の Velocity(http://velocity.apache.org/)モジュールを使用し、メール本文雛形ファイルと解析結果をマージし、本文を生成する。

## 7.1　メール本文作成の機能

メールの作成は、メール本文雛形にプログラム処理時に設定する値のキー項目を記述し、処理時にプログラム内で保持している値に変換する。メール本文は HTML 形式で生成する。

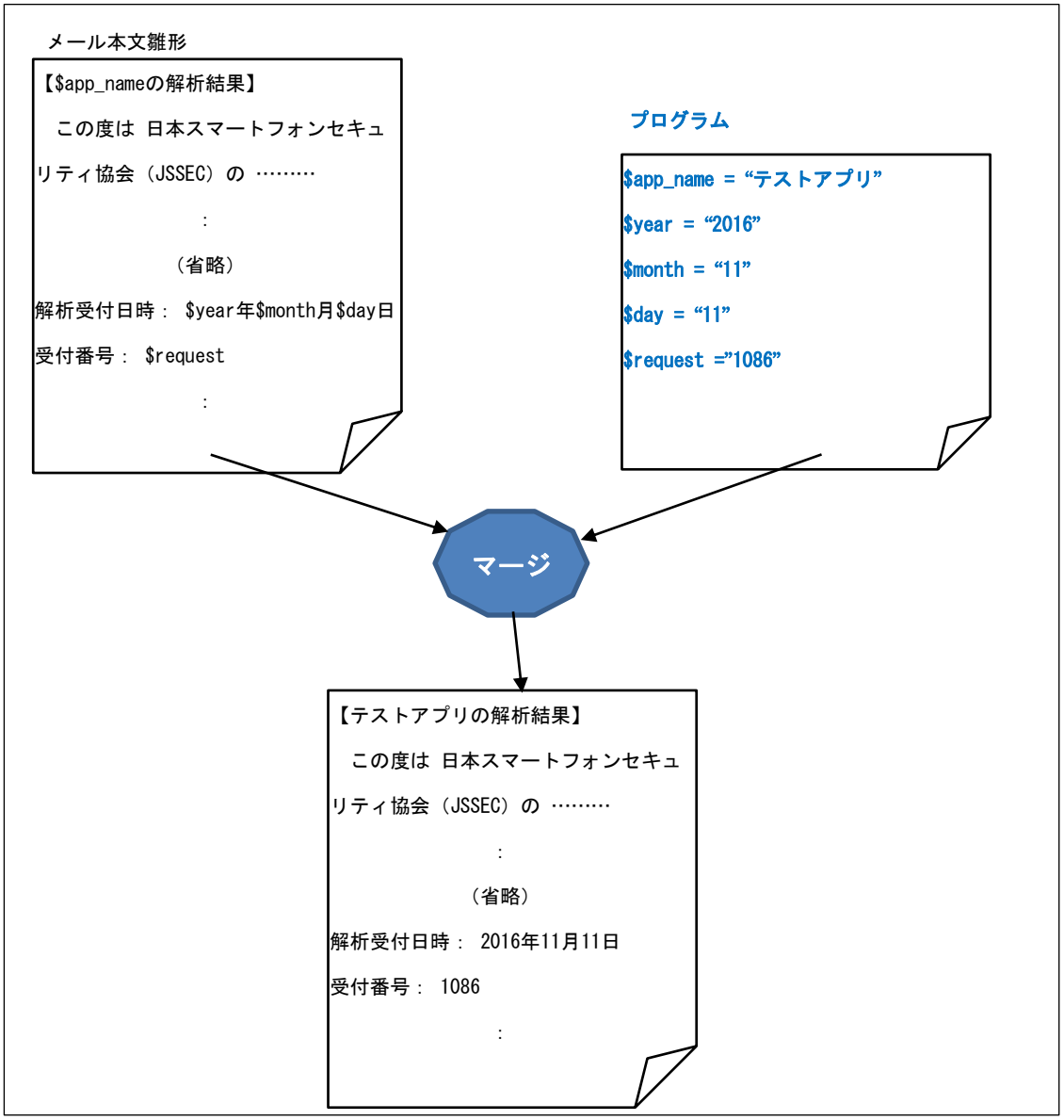



図 7.1-1 メール作成概要図

## 7.2 解析システム異常時のメール返信

解析結果が内部処理エラー、Android アプリ静的解析が中断するなどで解析結果が異常となった場合、また、解析結果のメールを依頼者に送信すると同時に、Bcc により管理者のメールアドレスへも送信する。

解析結果が異常終了とならず、解析依頼テーブルの解析状態のステータスが「解析中」のまま、制限時間（3 時間）以上経過していた場合も解析システム異常としてメールを返信する。

## 7.3 メール本文

メール本文雛形からメール本文を生成する。メール本文は、以下に示す 5 種類のうちのいずれかを解析結果により生成する。

- 解析処理成功
- 解析処理時間超過
- 表層解析不可
- フロー解析エラー
- 解析システム内部処理エラー

# 8　統計情報作成

統計情報の作成は、ApacheJakarta の POI(http://poi.apache.org/)モジュールを使用する。統計情報雛形ファイルに統計情報を書き込み、別ファイル名で保存する。

## 8.1　統計情報ファイル作成の機能

統計情報雛形ファイルを読み込み、統計情報用の設定ファイルに記述している出力位置に合わせて、各項目の値を書き込む。指定年月の統計情報をすべて書き込んだら「統計情報_YYYYMM.xlsx」のファイル名で保存する。

（※ YYYY は年 MM は月）

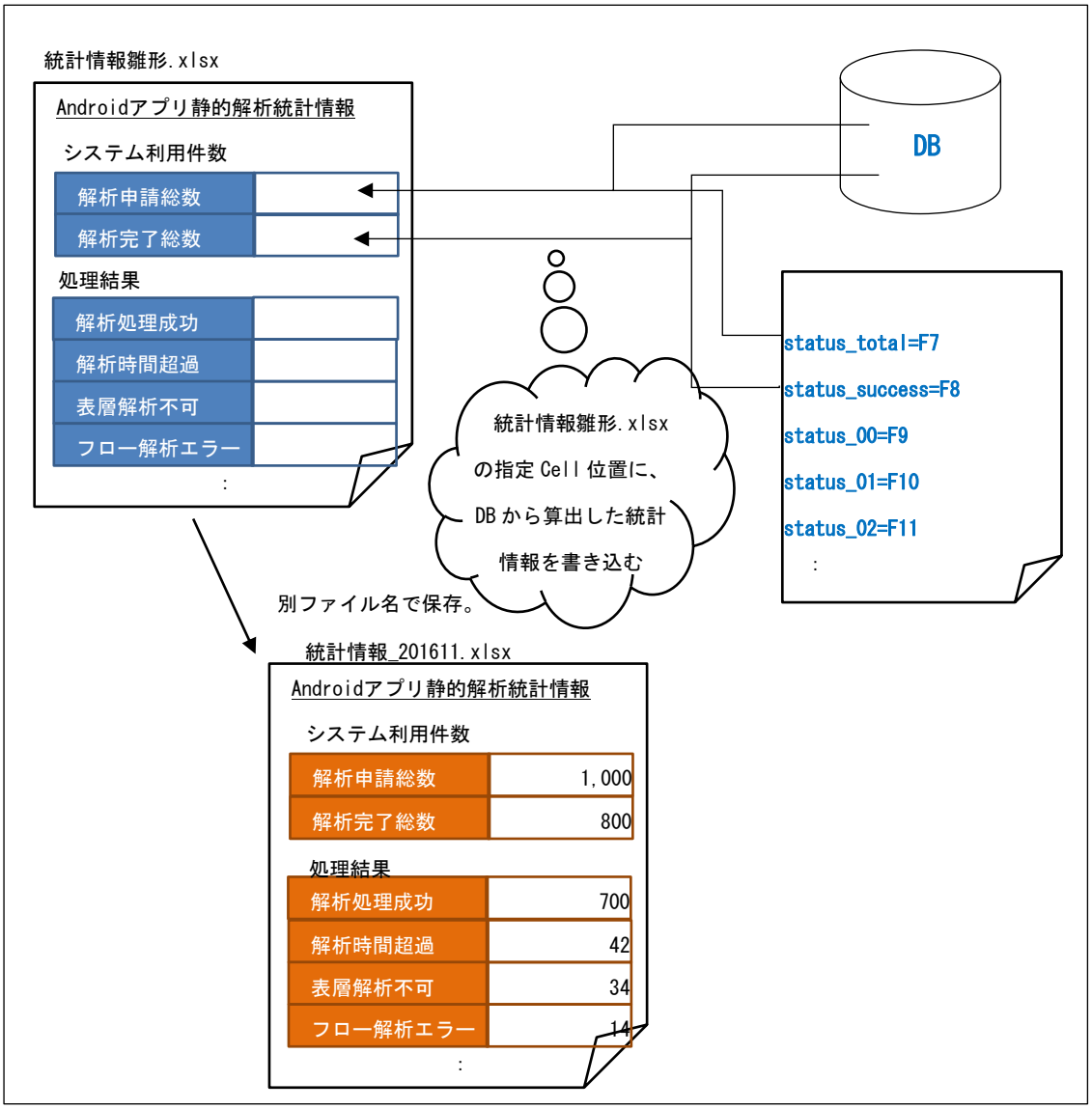



図 8.1-1 統計情報概要図

## 8.2 統計情報のイメージ

統計情報雛形ファイルに指定年月の統計情報を書き込んで生成すると「図 8.2-1 統計情報イメージ図」に示すような統計情報ファイルを作成する。

Android APK静的解析 統計情報(2016年11月)

### システム利用件数

| | | |
|---|---|---|
| 解析申請総数 | | 10,207,619 |
| 解析完了総数（制限時間超過、解析エラー含む） | | 8,976,596 |
| 処理結果 | 00:解析処理成功 | 8,123,456 |
| | 01：制限時間超過 | 654,321 |
| | 02：表層解析不可 | 1,218,678 |
| | 03:フロー解析エラー | 198,819 |
| | 04:解析システム内部処理エラー | 12,345 |

### アンケート：本システムの利用者

| | |
|---|---|
| アプリ提供者（自らアプリを開発している） | 3,123 |
| アプリ提供者（他者に委託するなどで開発は自ら行っていない） | 957 |
| アプリ開発者（受託開発など自らの名では提供していない） | 52,349 |
| スマートフォンアプリに関する研究者 | 543 |
| その他アプリ解析を必要とする事業者・個人 | 3,452 |

### アンケート：本システムの利用回数

| | |
|---|---|
| 初回 | 10,000,023 |
| 2回目 | 2,414 |
| 3回目 | 1,515 |
| 4回目 | 1 |
| 5回目以上 | 203,666 |

### アンケート：カテゴリー毎の件数

| | |
|---|---|
| 一般 | 3,457,537 |
| Android Wear | 134,549 |
| エンタメ | 527,892 |
| カスタマイズ | 791,345 |
| コミック | 539,245 |
| ショッピング | 8,932 |
| スポーツ | 527,244 |
| ツール | 23,774 |
| ニュース＆雑誌 | 91,234 |
| ソーシャルネットワーク | 633,472 |
| ビジネス | 64,527 |
| ファイナンス | 72,899 |
| メディア＆動画 | 6,745 |
| ライフスタイル | 4 |
| ライブラリ＆デモ | 58,381 |
| 医療 | 835,675 |
| 音楽＆オーディオ | 83,683 |
| 教育 | 64,564 |
| 健康＆フィットネス | 34,117 |
| 交通 | 11 |
| 仕事効率化 | 623,179 |
| 写真 | 851,458 |
| 書籍＆文献 | 2,526,428 |
| 通信 | 462,346 |
| 天気 | 321,566 |
| 旅行＆地域 | 888,852 |
| その他 | 0 |
| ゲーム | 6,234,554 |
| アーケード | 6,211 |
| アクション | 123,571 |
| アドベンチャー | 517,813 |
| カード | 543,272 |
| カジノ | 999,996 |
| カジュアル | 971,224 |
| シミュレーション | 5,235,276 |
| ストラテジー | 224,624 |
| スポーツ | 2,462,462 |
| パズル | 2,642,426 |

| | |
|---|---|
| ボード | 70,051 |
| レース | 34,234 |
| ロールプレイング | 621,242 |
| 音楽 | 124 |
| 教育 | 1,241,555 |
| 言葉 | 98,989 |
| 雑学 | 356,789 |
| その他 | 0 |
| ファミリー | 5,235 |
| 5 歳以下 | 12 |
| 6～8 歳 | 333 |
| 9 歳以上 | 914 |
| 人気キャラクター | 1,812 |
| アクション＆アドベンチャー | 1,253 |
| クリエイティビティ | 51 |
| ごっこ遊び | 534 |
| 音楽＆動画 | 543 |
| 教育 | 4,000 |
| 頭の体操 | 2,358 |
| その他 | 0 |
| 非公開（社内利用など） | 356,789 |
| 農業,林業,水産業,鉱業,建設業 | 0 |
| 総合工事,建設業 | 5,235 |
| 設備工事,製造業 | 12 |
| 一般製造業,製造業 | 333 |
| 印刷・出版,製造業 | 914 |
| その他の製造業,卸売・小売業, | 1,812 |
| 金融・保険業 | 1,253 |
| 不動産業 | 51 |
| 運輸・通信業 | 534 |
| 電気・ガス・水道・熱供給業 | 543 |
| サービス業－放送業 | 4,000 |
| サービス業－広告／デザイン | 2,358 |
| サービス業－法律／会計等 | 2,526,428 |
| サービス業－設計 | 462,346 |
| サービス業－医療 | 321,566 |
| サービス業－教育機関 | 888,852 |
| サービス業－各種団体 | 0 |
| サービス業－その他のサービス業 | 6,234,554 |
| 公務 | 6,211 |
| 利用業種は問わない | 1,253 |
| その他(個人等) | 51 |
| その他 | 510,293 |

## 解析結果

| | |
|---|---|
| AndroidManifest.xmlで定義されたuses-permission要素の総数 | 1,234,567 |
| 動的クラスローダを実行しているアプリ件数 | 4,524,281 |
| 内部でScriptを実行しているアプリ件数 | 99,754 |

## 詳細解析結果（利用者情報の送信が検出されたアプリ件数）

| | |
|---|---|
| 利用者情報の送信 | 3,123 |
| OS生成ID | 2 |
| 端末固有ID（IMEI） | 3 |
| 契約者固有ID(IMSI) | 1 |
| 契約者固有ID(ICCID) | 5 |
| デバイス固有ID(MACアドレス) | 12 |
| 電話番号 | 123 |
| メールアドレス | 14,124 |
| 位置 | 142 |
| アドレス帳 | 64 |
| マイク | 234 |
| カメラ | 2,352 |
| 加速度センサー | 821 |
| SMS | 3,413 |

図 8.2-1 統計情報イメージ図