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

動的解析手順書

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
Burp Suite Free Edition	PortSwigger 社が公開しているプロキシツールで、これを利用して iOS/Android 端末の通信内容を補足する。
SSL	Secure Sockets Layer の略。インターネットなどの TCP/IP ネットワークでデータを暗号化して送受信するプロトコルの一つ
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
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
動的解析	アプリケーション実行時の挙動から得られる情報を基に、利用者情報の送信有無・内容の解析を行うもの
プライバシーポリシー	プライバシーに関する情報の取り扱いについて定めた規範のこと
プラポリ調査シート	別途配布されるプライバシーポリシー調査シートのこと。 解析するアプリのプライバシーポリシーに記載されている内容の調査を行う。動的解析結果とプライバシーポリシーの記載状況について突合解析を行う場合に利用する。

1　はじめに

本手順書は、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」として、平成 27 年度に総務省が実施した「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の請負」において実施したパケットキャプチャの動的解析手順についてまとめたものである。

なお、設定値などは本手順書の執筆時に実施したときのもので記載しており、手順上の整合性がとれていれば、必ずしもその値である必要がないものも含んでいる。

2　構成

2.1　機器構成

本手順書の執筆時の機器構成を「図 2.1-1 機器構成」および、「表 2.1-1 機器」に示す。

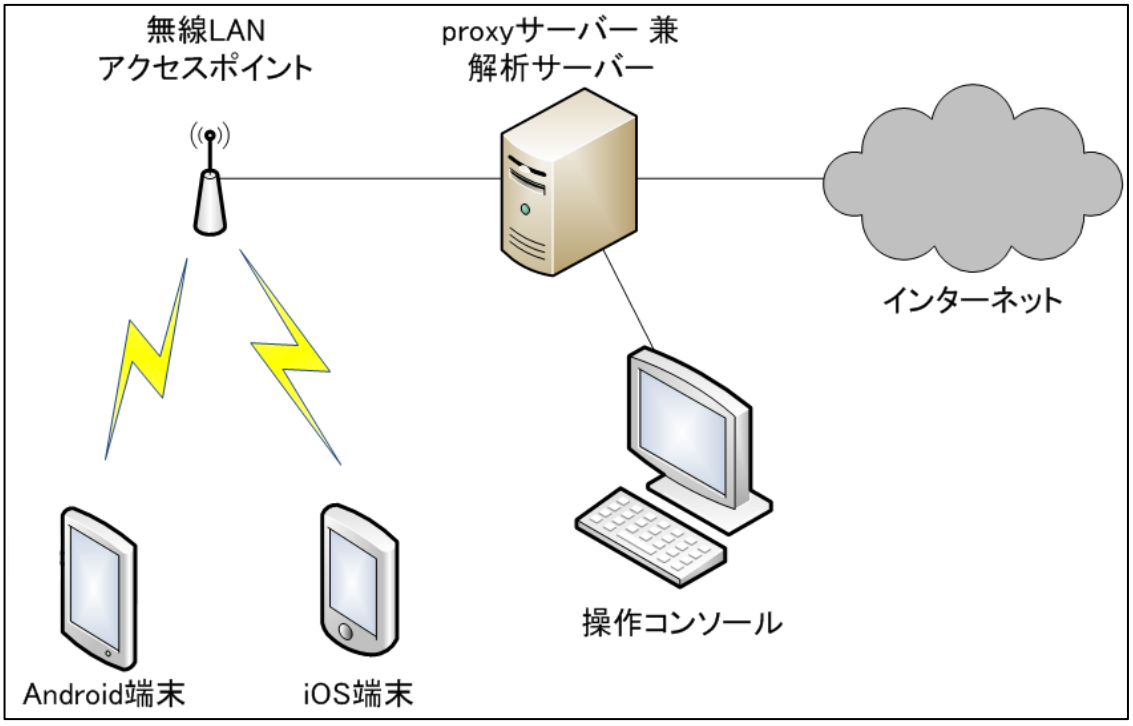

図 2.1-1 機器構成

表 2.1-1 機器

機器	役　割
Android 端末	解析を行うアプリを動作させる Android 端末
iOS 端末	解析を行うアプリを動作させる iOS 端末
proxy サーバー兼解析サーバー	proxy サーバーと動的解析を行うサーバーを兼ねたサーバー
操作コンソール	proxy サーバー兼解析サーバーを操作するコンソール
無線 LAN アクセスポイント	解析に利用する Android 端末や iOS 端末を proxy サーバーに接続するためのアクセスポイント
インターネット	解析するアプリを動作させるために利用する

2.2　ソフトウェア構成

本手順書の執筆時のソフトウェア構成を「図 2.2-1 ソフトウェア構成」および、「表 2.2-1

ソフトウェアのバージョン」に示す。

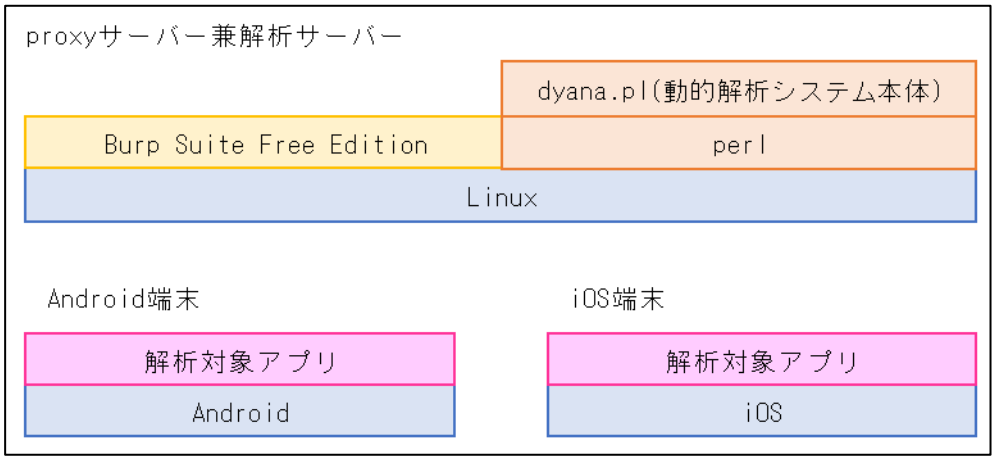

図 2.2-1 ソフトウェア構成

表 2.2-1 ソフトウェアのバージョン

ソフトウェア	バージョン	備考
Linux	CentOS7.2	
Burp Suite Free Edition	1.7.13	解析するアプリの動作ログを取得するために利用する
perl	5.16.3	動的解析システム（dyana.pl）を動作させるために利用する。 「/usr/bin/perl」にあることを前提としている
Android	5.0	
iOS	10.0	
dyana.pl	1.0	動的解析システム本体

2.3 前提条件

動的解析を行うにあたり本手順における前提条件を以下に示す。

- CentOS7.2 のインストールにおいて、インストールタイプは「desktop」を選択する。
- 解析対象のログファイルは、Burp Suite Free Edition の proxy 機能により取得したものを利用する。

3　環境構築

3.1　環境準備

環境構築を行うにあたり、「2 構成」に従い動的解析を行うための端末やインストールするソフトウェアなどを準備する。

3.2　proxy サーバー兼解析サーバーの環境構築

Linux をインストールした proxy サーバー兼解析サーバー（以下、proxy サーバーという）の環境構築を行う。

① 8080 番ポートの開放

Android 端末や iOS 端末からアクセスできるようにするために 8080 番ポートを解放する

・ 設定手順

- Firewall 設定で 8080 番ポートの解放
- 8080 番ポートが開いたことの確認

「参考」として、本手順書の執筆時に行った設定例を「図 3.2-1 8080 番ポートの開放」に示す。

```
$ sudo firewall-cmd --add-port=8080/tcp --permanent
[sudo] password for ****:
success

$ sudo firewall-cmd --reload
success

$ firewall-cmd --list-all
public (default, active)
  interfaces: eno16777736
  sources:
  services: dhcpv6-client ssh
  ports: 8080/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
```

```
  rich rules:
```

図 3.2-1 8080 番ポートの開放

② whois と perl module のインストール

動的解析システムで利用する whois と perl module をインストールする。

「参考」として、本手順書の執筆時に行ったインストール例を「図 3.2-2 ツールインストール例」に示す。

```
$ sudo yum -y install whois perl-Digest-MD5 perl-Digest-SHA
```

図 3.2-2 ツールインストール例

3.2.1 動的解析システムの設定

別途ダウンロードした動的解析システムを proxy サーバーへ格納する。

- 設定手順
  - ダウンロードした動的解析システム（zip ファイル）の解凍
  - dyana.pl を proxy サーバーの適切な権限のある任意の場所へ格納する。
  - dyana.pl のアクセス権を変更する。

「参考」として、本手順書の執筆時に行った設定例を「図 3.2-3 動的解析システムの設定例」に示す。

```
$ chmod +x dyana.pl
```

図 3.2-3 動的解析システムの設定例

3.2.2 Burp Suite の取得

proxy サーバーにインストールする Burp Suite を取得する。

① Burp Suite の取得

- 取得先、格納場所

「参考」として、本手順書の執筆時にファイルを取得したダウンロード先 URL やファイル、およびダウンロードファイルの格納場所を「表 3.2-1 Burp Suite 取得の参考情報」に示す。

表 3.2-1 Burp Suite 取得の参考情報

ダウンロード先 URL	https://portswigger.net/burp/download.html
ダウンロードしたファイル	Free Edition の plain JAR file （バージョンは v1.7.15）
proxy サーバーのダウンロード	Downloads

ファイル格納先フォルダ	

・ 取得手順

- proxy サーバーにログイン
- 公式サイトより、Burp Suite を取得

3.2.3 Burp Suite の設定

proxy サーバーに格納した Burp Suite の設定を行う。

① Burp Suite の起動

「参考」として、本手順書の執筆時に行った起動例を「図 3.2-4 Burp Suite 起動例」に示す。

```
$ java -Dawt.useSystemAAFontSettings=on -jar Downloads/Burp Suite_free_v*.jar
```

図 3.2-4 Burp Suite 起動例

（本手順書の執筆時の設定では、フォントを見やすくするため以下を指定した。

「-Dawt.useSystemAAFontSettings=on」の指定をしなくても動作はするがフォントが見づらくなる。）

② Burp Suite の起動

- Welcome 画面に表示されている「Next」ボタンを押下
- 「Start Burp」ボタンを押下

③ Burp Suite の設定

・ 設定情報

表 3.2-2 Burp Suite 設定情報

タブ	設定項目	設定情報
Binding	Bind Port	8080

・ 設定の手順

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- Proxy タブをクリック
- Intercept サブタブをクリック
- 「Intercept is xxx」ボタン表記の xxx 部分が on になっている場合は、ボタンをクリックしてボタンの表記を「Intercept is off」に変更
- Options サブタブをクリック

- 「Proxy Listeners」のエリアに既存の設定がある場合は「Running」チェッククリックしてチェックをはずす
- 「Proxy Listeners」のエリアにある「Add」をクリック
- 「Add a new proxy listener」ウィンドウが開く
- Binding タブで Bind Port に「8080」を入力
- Bind to Address で「All interfaces」を選択
- 「OK」ボタン押下
- 「Add a new proxy listener」ウィンドウが閉じる
- (Confirm が出た場合は「YES」を選択)
- Options サブタブの「Proxy Listeners」に上記で作った設定(*:8080)が表示されたことを確認
- 「Running」チェックボックスをクリックしてチェックを付ける

3.2.4 Burp Suite の設定後

Burp Suite は、終了させず起動させたままとする。

4　端末の準備

4.1　端末の設定

Android 端末および iOS 端末について設定手順を示す。

4.1.1 Android 端末の設定例

① 事前準備

SSL 証明書の登録で利用する場合があるため、ファイル名の変更ができるファイル操作アプリを事前にインストールする。

② 外部接続の設定

プロキシサーバ経由で外部接続できるように設定する。

・ 設定情報

表 4.1-1 外部接続の設定情報(Android)

proxy サーバーの IP アドレス	192.168.8.101
Burp Suite の CA の証明書名	Burp proxy

・ 設定手順

proxy サーバー経由で外部接続するように設定する。

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- 「設定」→「Wi-Fi」→接続する SSID を選択
- パスワードの入力
- 「詳細設定項目」のタップ
- プロキシについて「手動」を選択
- プロキシホスト名に proxy サーバーのホスト名、もしくは IP アドレスを入力
- プロキシポートに「8080」を入力
- 「接続」をタップ

③ SSL 証明書の登録

Burp Suite でログ取得するときに端末側の SSL の通信を確認するために SSL 証明書を登録する。

・ 設定情報

表 4.1-2 BurpSuite の設定情報(Android)

proxy サーバーの IP アドレス	192.168.8.101

・ 設定手順

proxy サーバーの SSL 証明書を Android 端末へ登録する。

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- ブラウザを起動
- http://<proxy サーバーの IP アドレス>:8080 にアクセス
- 画面の上部右隅に表示される「CA Certificate」をタップ
- ダウンロードを開く
- ファイル操作アプリを利用しファイル名 cacert.der を cacert.crt に変更
- ファイル操作アプリより、cacert.crt をタップ
- Burp Suite の CA の証明書名として任意の文字列を入力
- OK をタップ

④ 位置情報を設定できるアプリのインストール

位置情報を含めて解析する場合、位置情報を動的に変化させないために、解析対象となるアプリとは別に、位置情報を固定できるアプリをインストールし、端末上で疑似ロケーションの許可を行う。

位置情報を設定できるアプリを「疑似ロケーション」「位置情報固定」などの文字列で検索する。

・ 設定手順

疑似ロケーションの設定をできるようにする。

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- 「設定」→「タブレット情報」をタップ
- 「ビルド番号」を「開発者向けオプション」が有効になるまで連続タップ
- 「設定」に戻り、「開発者向けオプション」をタップ
- 「疑似ロケーションを許可」をタップして許可

⑤ アプリのインストール

解析対象となるアプリをマーケットなどから取得しインストールする。

4.1.2 iOS 端末の設定例

iOS 端末の設定について、設定手順を以下に示す。

① 外部接続の設定

proxy サーバー経由で外部接続できるように設定する。

・ 設定情報

表 4.1-3 外部接続の設定情報(iOS)

proxy サーバーの IP アドレス	192.168.8.101
Burp Suite の CA の証明書名	Burp proxy

・ 設定手順

proxy サーバー経由で外部接続するように設定する。

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- 「設定」→「Wi-Fi」→接続する SSID を選択
- パスワードの入力
- 「接続」ボタンのタップ
- 接続後、SSID 名の右端にある「〇印に i」のボタンをタップ
- スクロールすると「HTTP プロキシ」の設定があるため「手動」をタップ
- 「サーバ」に proxy サーバーのホスト名、もしくは IP アドレスを入力
- 「ポート」に「8080」を入力

- 「< Wi-Fi」をタップ

② SSL 証明書の登録

Burp Suite でログ取得するときに端末側の SSL の通信を確認するために SSL 証明書を登録する。

・ 設定情報

表 4.1-4 Burp Suite の設定情報(iOS)

proxy サーバーの IP アドレス	192.168.8.101

・ 設定手順

proxy サーバーの SSL 証明書を登録する。

「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

- ブラウザを起動
- http://192.168.8.101:8080 にアクセス
- 画面の上部右隅に表示される「CA Certificate」をタップ
  「どのデバイスにこのプロファイルをインストールしますか?」と聞かれた場合は iPhone を選択
- インストール画面でプロファイルが「PortSwigger CA」の証明書である事を確認
- 右側の「インストール」ボタンをタップ
- パスコードを入力
- 警告画面より「インストール」をタップ
- 「インストール」をタップ
- 「完了」をタップ

③ アプリのインストール

解析対象となるアプリをマーケットなどから解析するアプリをインストールする。

5　ログ取得

5.1　事前準備

「参考」として、本手順書の執筆時において、ログ取得をスムーズに進めるために事前準備として行った作業を以下に示す。これらを実施しなくてもログ取得を行うことは可能である。

- 利用する端末において、ログ取得前に一度アプリを操作し、感触をつかんだ。
- ログ取得のための操作では全てのボタンをタップするが、外部アプリが起動するボタンは対象外とするため、誤って操作しないよう、タップするボタンを手順としてメモで記録した。
- 一連の操作を行った後は、ログ取得に向けてアプリを削除し、再インストールを行った。

5.2　ログの取得

5.2.1 位置情報の固定

Android 端末において、「4.1.1 ⑤アプリのインストール」でインストールしたアプリを利用して、位置を固定する。この時の位置情報(緯度と経度)は、「6.3.1 個別の情報の確認方法(Android)」で利用する。本手順書の執筆時には、この時の位置情報をメモにより残した。

5.2.2 サーバーによるログ取得の開始

proxy サーバーに Burp Suite でログ保存を開始する。

- 設定情報

表 5.2-1 ログ保存の設定情報

Burp Suite により取得したログを保存するファイル名	burplog

- 設定手順

  「参考」として、本手順書の執筆時に利用した設定手順を以下に示す。

  - 「3.2.4 Burp Suite の設定後」に開いているウィンドウを確認
  - User options タブをクリック
  - Misc サブタブをクリック
  - 「Logging」エリアにある Proxy: Requests のチェックボックスをオン
  - ファイル名(N)に、ログを保存する任意のファイル名を入力し「保存」ボタンを押下

    （ファイル名はアプリごとに変える）

この状態で「5.2.3 端末によるログ取得」を実施する。

proxy サーバーにおいて、ログ取得中の動作を確認することもできる。

「参考」として、本手順書の執筆時に利用した確認方法を「図 5.2-1 取得ログの確認方法」に示す。

```
$ tail -f burplog
```

図 5.2-1 取得ログの確認方法

5.2.3 端末によるログ取得

① ログの取得

各端末において、以下の手順でログを取得する。

・ 操作手順

- アプリの起動
- 全てのボタンを押下

設定した時間までに全てのボタン操作が終了しなかった場合、もしくはそれ以上操作を続けていても変化がないと思われる場合は、操作を終了する。

実証実験では、最大 1 時間を設定して操作を行った。

ゲームなど継続利用が前提となっているアプリは、しばらく継続操作した先のイベントにおいて外部送信が行われる事も考えられるため、継続可能であれば、設定した時間まで操作を継続する。

5.2.4 ログ取得の終了

解析を行うアプリの終了後、Burp Suite によるログの記録取得を終了する。

「参考」として、本手順書の執筆時に実施した手順を以下に示す。

- 「5.2.3 端末によるログ取得」でチェックを入れた Proxy: Requests のチェックボックスのチェックをはずす
- Burp Suite の終了

6　動的解析システムの実行

6.1　動的解析システムの概要

動的解析システムは、「5 ログ取得」において、Burp Suite により取得したログを利用して、Android端末もしくはiOS端末に格納されている個別の情報を外部へ送信していないか確認するためのものである。

解析の準備として、利用者は『デバイス情報ファイル』を作成する。『デバイス情報ファイル』には、Android 端末もしくは iOS 端末に格納されている個別の情報のうち、外部への送信有無を確認したい情報を指定する。

動的解析システムは、Burp Suit で取得したログに対して、この「デバイス情報ファイル」で指定した情報の外部送信有無を解析し結果を返す。

具体的には、対象ログファイル内で、デバイス情報ファイルに「検索用の値」として記載されたデータが外部へ送信されていないかを検索する。

検索にあたっては、「検索用の値」 と、英文字を全て小文字化した値、英文字を全て大文字化した値、またそれらを、md5,sha1,sha256,sha512 でハッシュした値を用いる。

対象ログファイル内で、これらの値のいずれかにマッチした場合、その値が送信された IP アドレスを解析結果として出力する。(結果出力ファイルが指定されていた場合、該当ファイルに格納する)

6.2　デバイス情報ファイルの作成

デバイス情報ファイルは、テキストエディタを利用して作成する。

デバイス情報ファイルには、「6.3 端末情報の取得」で確認した個別の情報のうち、外部送信の有無を確認したい情報を以下のフォーマットで指定する。

・ 設定情報：

「参考」として、本手順書の執筆時に利用した設定情報を「表 6.2-1 デバイス情報ファイルの設定情報」に示す。

表 6.2-1 デバイス情報ファイルの設定情報

デバイス情報ファイルのファイル名	devinfo
結果表示用のタイトル	プラポリ調査シートの「②-記載状況詳細」に「個別」として記載されている横軸の項目名で設定、項目名に（ ）で記載されている内容は省略した。 例：OS 生成 ID（Android ID）は、OS 生成 ID と設定

・ 設定例

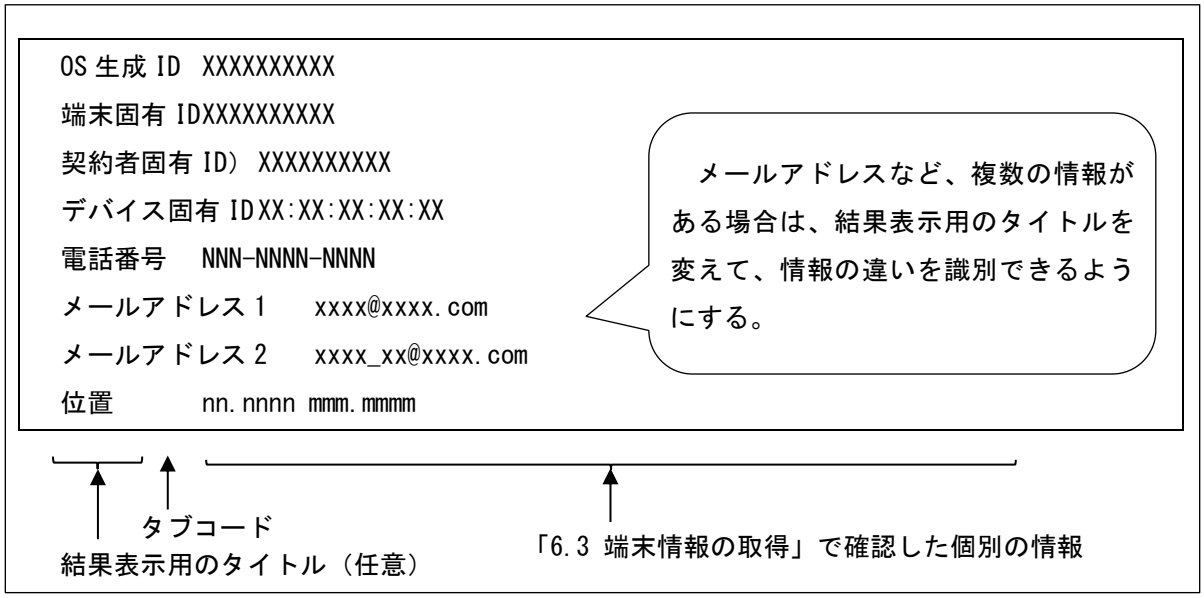

図 6.2-1 デバイス情報ファイルの設定例

「デバイス情報ファイル」には、確認したい情報として、以下の 2 つをタブコードで区切り 1 行 1 項目で指定する。

・ 送信情報として表示する任意の文字列「結果表示用のタイトル」（「図 6.2-1 デバイス情報ファイルの設定例」参照）

・ 端末に格納されていた個別の情報である「検索用の値」

位置情報は、緯度（nn.nnnn）と経度（mmm.mmmm）をタブコードで区切り 1 行として指定する。指定する緯度経度は小数点以下 4 桁までを入力する。

メールアドレスなど、アプリを実行する端末に複数の情報が登録されている場合は、確認したいアドレス 1 項目につき 1 行で複数記載することにより、各アドレスの外部送

信有無を確認することができる。

6.3　端末情報の取得

Android 端末もしくは iOS 端末に格納されている個別の情報について確認する。

確認したい情報が見つかった場合は、「6.2 デバイス情報ファイルの作成」で作成した『デバイス情報ファイル』へ記載する。

6.3.1 個別の情報の確認方法(Android)

Android 端末に格納されている個別の情報に対する確認方法として、本手順書の執筆時に利用した Nexus7 の確認方法を「参考」として以下に示す。なお、③契約者固有 ID（IMSI、ICCID）と⑤電話番号は Nexus7 にはない情報のため、スマートフォンにより確認する方法を「参考」として記載している。

これらのうち、動的解析システムで外部送信の有無を確認したい情報について、端末に登録されている情報を「検索用の値」として「デバイス情報ファイル」へ記載する。記載方法は、「6.2 デバイス情報ファイルの作成」を参照。

① OS 生成 ID（Android ID）の確認

設定アプリから、タブレット情報→端末の状態の順にタップ。

「シリアル番号」を確認する。

② 端末固有 ID（IMEI）

設定アプリから、タブレット情報→端末の状態→IMEI 情報の順にタップ。

「IMEI」を確認する。

③ 契約者固有 ID（IMSI、ICCID）

設定アプリから、タブレット情報→端末の状態→IMEI 情報の順にタップ。

「IMSI」「ICCID」を確認する。

④ デバイス固有 ID（MAC アドレス）

設定アプリから、タブレット情報→端末の状態の順にタップ。

「Wi-Fi MAC アドレス」を確認する。

⑤ 電話番号

設定アプリから、端末情報→機器の状態→SIM のステータスの順にタップ。

「電話番号」を確認する。

⑥ メールアドレス

設定アプリから、アカウント→Google の順にタップ。

登録されているメールアドレスを確認する。

⑦ 位置

「5.2.1 位置情報の固定」において、固定した位置情報（緯度と経度）を確認する。

⑧ 広告 ID

Google 設定アプリから、広告をタップ。

「広告 ID」を確認する。

6.3.2 端末の情報取得方法(iOS)

iOS 端末の情報の確認方法を以下に示す。

これらのうち、動的解析システムで外部送信の有無を確認したい情報について、端末に登録されている情報を「検索用の値」として「デバイス情報ファイル」へ記載する。記載方法は、「6.2 デバイス情報ファイルの作成」を参照。

① OS 生成 ID（UDID）

設定アプリから、一般→情報の順にタップ。

「シリアル番号」を確認する。

② 端末固有 ID（IMEI）

設定アプリから、一般→情報の順にタップ。

「IMEI」を確認する。

③ 契約者固有 ID（ICCID）

設定アプリから、一般→情報の順にタップ。

「ICCID」を確認する。

④ デバイス固有 ID（MAC アドレス）

iOS 端末の MAC アドレス。

設定アプリから、一般→情報の順にタップ。

「Wi-Fi アドレス」を確認する。

⑤ 電話番号

端末の電話番号。

電話アプリを起動し、「連絡先」タブを選択する。
「自分の番号」を確認する。

⑥ メールアドレス

iOS 端末には以下の 2 か所に登録されているメールアドレスを確認する。

- 設定アプリから、メール→アカウントの順にタップ。
  表示された個々のアカウントをタップして、登録されているメールアドレスを確認する。
- 設定アプリから、メッセージをタップ。
  「MMS メールアドレス」に表示されたアドレスを確認する。

⑦ 位置

iOS 端末に標準でインストールされている「マップ」アプリを利用して、位置情報を確認する。

「マップ」アプリを起動する。
矢印のボタンをタップして現在地を表示した後、現在地を表す青い丸印をタップする。
位置情報となる「緯度」と「経度」を確認する。

6.4 実行

動的解析システム（dyana.pl）により、Burp Suite で取得したログと、デバイス情報ファイルを利用して個別の情報の外部送信について解析する。

- 設定情報

表 6.4-1 解析実行の設定情報

Burp Suite により取得したログを保存するファイル名 「5.2.2 サーバーによるログ取得の開始」で指定	burplog
デバイス情報ファイルのファイル名 「6.2 デバイス情報ファイルの作成」で指定	devinfo

- 実行手順
  - proxy サーバーから、動的解析システム（dyana.pl）を「3.2.1 動的解析システムの設定」で格納したディレクトリで実行。
  - 実行結果の確認
    動的解析の実行結果として、外部へ送信されている情報が表示される。

「参考」として、本手順書の執筆時に利用した実行手順を「図 6.4-1 実行手順」に示す。

図 6.4-1 実行手順

実行結果の送信先には、送信情報の送信先 IP アドレスが表示される。

IP アドレスの横には、whois コマンドにより取得した「Organization」の項目が出力される。「Organization」に情報がない場合は、IP アドレスのみ出力される。