Vol.2013-CSEC-62 No.20
Vol.2013-SPT-6 No.20
2013/7/18

細粒度の情報追跡による機密情報送信の動的制御手法

小倉 禎幸[1,a)]　山内 利宏[1]

概要：近年，Android 端末の普及に伴い，Android を標的とするマルウェアが増加し，マルウェアへの対策が重要視されている．特に，マルウェアによる端末外部への機密情報の漏洩が問題となっている．この問題に対処するために，機密情報の伝搬を追跡し，機密情報が外部に漏洩する際に利用者の判断に従って AP の動作を動的に制御する手法を提案する．具体的には，提案手法は，TaintDroid を利用し，機密情報の伝搬を変数レベルで細粒度に追跡する．端末外部に機密情報が漏洩する場合，利用者の判断に従って AP の動作を制御する．これにより，端末外部への機密情報の漏洩を防止する．また，端末外部に送信される機密情報をダミーデータに置換し，機密情報の漏洩を防止する．これにより，AP の正常な動作をできるだけ妨げることなく機密情報の漏洩を防止できる．さらに，AP 間で機密情報のやり取りがあった場合，機密情報の漏洩に関わった AP 名を取得し，機密情報の伝搬経路を把握する．これにより，利用者は機密情報の漏洩の伝搬経路とその漏洩に関わった AP を正確に把握し，漏洩要因の各 AP に対処できる．

1. はじめに

近年，個人向けの高機能な携帯端末として，スマートフォンの普及が進んでいる．スマートフォン向けのオペレーティングシステムの 1 つとして Android [1] が広く利用されている．Android のユーザは，Google Play[2] からアプリケーションプログラム（Application Program：以降，AP と略す）をスマートフォンに自由にダウンロードして，インストールできる．

しかし，配布されている AP の中にはシステムの脆弱性を攻撃して管理者権限を不正に取得するマルウェア，ネットワークや SMS 経由で外部サーバと通信して料金を発生させるマルウェア，および機密情報を外部に漏洩するマルウェアなどが発見され [3]，被害を及ぼしている．特に近年，機密情報を外部に漏洩する The Movie [4] や全国電話帳 [5] といったマルウェアによる被害が発生している．このため，端末外部に機密情報を漏洩させるマルウェアへの対策が重要視されている．この問題に対処するために，機密情報の漏洩防止に関する様々な手法が研究がされている [6]-[10]．しかし，これらの研究には，誤検知，AP の動作の妨害，および一般の利用者では理解や操作が難しいという問題のいずれかがある．

そこで，本稿ではこれらの問題をすべて解決するため，機密情報の伝搬を追跡し，機密情報が外部に漏洩する際に利用者の判断に従って AP の動作を動的に制御する手法を提案する．具体的には，提案手法は，TaintDroid [8] を利用し，機密情報の伝搬を変数レベルで細粒度に追跡する．端末外部に機密情報が漏洩する場合，利用者の判断に従って AP の動作を制御する．これにより，端末外部への機密情報の漏洩を防止する．また，端末外部に送信される機密情報をダミーデータに置換し，機密情報の漏洩を防止する．これにより，AP の正常な動作をできるだけ妨げることなく機密情報の漏洩を防止できる．さらに，AP 間で機密情報のやり取りがあった場合，機密情報の漏洩に関わった AP 名を取得し，機密情報の伝搬経路を把握する．これにより，利用者は機密情報の漏洩の伝搬経路とその漏洩に関わった AP を正確に把握し，漏洩要因の各 AP に対処できる．本稿では，提案手法の設計，実現，および評価について述べる．

2. Android における機密情報の漏洩防止手法

2.1 API に着目した手法

文献 [6] の手法は，API をフックし，利用者が API の利用の可否決定をすることで機密情報の漏洩を防止する．また，AP の動作履歴を提示することで，AP の動作の継続や反復からマルウェアか否かを利用者が判断する支援を行う．しかし，文献 [6] の手法は，API を用いて機密情報を追跡している．このため，追跡粒度が粗く，誤検知が多い問題がある．また，利用者に提示される情報の内容がパッケージ名や API 名であり，一般の利用者では表示された内容を理解しにくい問題がある．

[1] 岡山大学 大学院自然科学研究科
[a)] ogura@swlab.cs.okayama-u.ac.jp

2.2 ダミーデータを用いた手法

MockDroid [7] は，AP が機密情報の代わりにダミーデータを取得するように事前に設定する．これにより，機密情報へのアクセスを許可していない AP による機密情報の取得を防止し，機密情報の漏洩を防止する．しかし，この手法は，AP が機密情報を取得する際にダミーデータを取得するため，AP が正常に動作しない問題がある．

2.3 TaintDroid を用いた手法

TaintDroid [8] は，機密情報に Taint と呼ばれるタグ (以降，Taint タグと略す) を付与し，その機密情報が使用された場合に，機密情報の伝搬を追跡する．Taint タグは，変数同士での単項演算やコピー，配列への挿入や値の取得などが行われた際に伝搬する．また，TaintDroid は，インターネットや外部ストレージへの書き込みなどを監視している．さらに，TaintDroid は，端末外部に機密情報が漏洩した場合に，機密情報に付与された Taint タグ，端末外部に伝搬させた AP のパッケージ名，および機密情報の伝搬先をログとして記録し，利用者に提示する．利用者は，提示されたログから機密情報を端末外部に伝搬させた AP がマルウェアか否かを判断する．しかし，TaintDroid は，機密情報の伝搬を追跡することを目的としているため，機密情報の漏洩を防止できない．また，端末外部にデータを送信した AP しかログに記録しない．このため，二つ以上の AP が連携して機密情報を漏洩させるような場合，漏洩に関わった AP を正確に把握できない．

文献 [9]，[10] の手法は，TaintDroid を用いて機密情報の漏洩を防止している．文献 [9] の手法は，AP のインストール時に，AP が取得した情報を端末内でのみ使用するか端末外部への送信を許可するかを利用者が選択することにより，機密情報の漏洩を防止する．しかし，インストール時以外では，利用者は機密情報の使用範囲を変更できない．このため，利用者が任意のタイミングで設定を変更できない．

AppFence [10] は，Taint タグが付加されている機密情報が端末外部に送信される際，送信をブロックするかダミーデータを端末外部に送信することで機密情報の漏洩を防止する．しかし，利用者は AP ごとにダミーデータやポリシの設定をする必要があり，利用者の負担が大きい．また，ブロックはポリシを用いて行われている．このため，機密情報が送信される際に，その動作を利用者が動的に制御することはできない．さらに，端末上でポリシの設定を変更できない．このため，機密情報が端末外部に送信されるタイミングで利用者がポリシを変更し，AP の動作の制御方法を変更することはできない．また，ポリシを用いて AP の動作を制御するため，利用者は，機密情報の漏洩に関わった AP を正確に把握できない．

2.4 既存研究の問題点

これまでに述べた手法には，以下のいずれかの問題が存在する．

（問題 1）誤検知の多さ
（問題 2）機密情報の取得制限による AP の正常な動作の妨害
（問題 3）利用者の判断による AP の動作制御不可
（問題 4）機密情報の漏洩に関わった AP を利用者は正確に把握不可
（問題 5）利用者の負担が大きい
（問題 6）利用者に提示される情報の内容が一般の利用者では理解しにくい

3. TaintDroid の拡張による機密情報の漏洩防止手法の設計

3.1 システムへの要求

本稿では，2 章で述べたすべての問題を解決する機密情報の漏洩防止手法を提案する．（問題 1）への対処では，機密情報の細粒度な追跡ができる TaintDroid を用いる．また，（問題 2）への対処では，端末内での機密情報の利用は制限せず，端末外部に機密情報が送信される際に機密情報をダミーデータに置換する．さらに，（問題 3）への対処として，機密情報の端末外部への送信時に，利用者の判断を取得し，判断結果に従って AP の動作を制御する．次に，（問題 4）への対処として，AP 間の機密情報のやり取りがあった場合に，通信先と通信元の AP 名とやり取りされた機密情報を把握する．最後に，（問題 5）と（問題 6）への対処として，利用者への警告の提示回数の削減と警告内容を簡略化する．また，端末上での設定の変更を可能にする．

各問題への対処から，提案手法への要求は以下のようになる．

（要件 1）AP による端末外部への機密情報の送信を動的に制御できること
（要件 2）AP が機密情報を端末外部に送信した結果を使用しない限り，AP の動作を妨害しない
（要件 3）機密情報毎に漏洩に関わったすべての AP 名と伝搬経路を取得できること
（要望 1）利用者の負担を少なくすること
（要望 2）利用者の判断を支援すること

（要望 1）と（要望 2）は，機密情報の漏洩防止の観点から要件とはならないが，重要な課題である．

また，提案手法は，AP による利用者の意図しない機密情報の漏洩を防止することを目的としている．

3.2 提案手法の全体像

提案手法の全体像を**図 1** に示す．提案手法は，一部に TaintDroid の機能を利用し，5 つの機能からなる．提案手法は，AP が機密情報を取得する際（(1) 〜 (2)），機密情

Vol.2013-CSEC-62 No.20
Vol.2013-SPT-6 No.20
2013/7/18

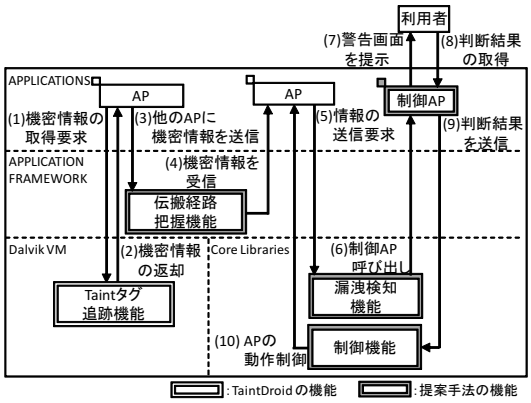

図 1 提案システムの全体図

報を取得した変数に Taint タグを付加し機密情報を追跡する（Taint タグ追跡機能）．また，AP 間で機密情報が伝搬した場合（(3) ～ (4)），その伝搬経路を把握する（伝搬経路把握機能）．さらに，機密情報に付加された Taint タグを利用して，AP がデータを端末外部に送信する際（5），送信されるデータに機密情報が含まれているかどうか判断する（漏洩検知機能）．機密情報が含まれていた場合（(6) ～ (8)），機密情報の端末外部への送信を許可するか否か利用者に尋ね，利用者の判断結果を取得する（制御 AP）．利用者の判断結果に従って，機密情報を端末外部に送信する動作を制御する（(9) ～ (10)）（制御機能）．

（要件 1）への対処では，機密情報の伝搬を細粒度で追跡し，機密情報が端末外部に送信される際に，その動作を検知し，利用者の判断に従って制御する必要がある．このため，提案手法では，Taint タグ追跡機能において，TaintDroid を利用して機密情報を追跡し，漏洩検知機能において，端末外部への機密情報の送信を検知する．その後，制御 AP を用いて，利用者に警告画面を提示し，AP の動作の可否を尋ねる．制御機能において，利用者の判断結果に従って AP の動作を制御することで実現する．

（要件 2）への対処では，AP による機密情報の取得を制限せず，端末外部に機密情報を送信しない限り，AP の動作を妨害しない必要がある．このため，提案手法では，制御 AP において利用者がダミーデータの送信を選択した場合，制御機能により，端末外部に送信される機密情報をダミーデータに置換することで実現する．端末外部に送信される機密情報のみをダミーデータに置換するため，端末外部に機密情報を送信した結果を AP が利用しない限り，AP の動作を妨害しない．

（要件 3）への対処では，機密情報を漏洩させた AP が，どういった経路で機密情報を取得したのかを判断する必要がある．このため，提案手法では，AP 間で機密情報がやり取りされた際，伝搬経路把握機能において，通信先と通信元の AP 名とやり取りされた機密情報を把握し，機密情報の伝搬経路を把握する．これにより，機密情報の漏洩に関わった AP 名を取得できる．利用者は，機密情報の漏洩に関わった AP を正確に把握し，それぞれの AP に対して対処することができる．

（要望 1）と（要望 2）への対処では，利用者が難しい操作をせず，機密情報の漏洩を防止し，利用者が機密情報の漏洩による危険性を理解する必要がある．このため，提案手法では，利用者への警告において，次回以降の提示の有無を AP ごとに設定できるようにし，警告画面において一般の利用者の理解しやすい情報を提示することにより実現する．詳細は，3.6.1 項で述べる．

3.3 Taint タグ追跡機能

Taint タグ追跡機能は，機密情報の伝搬を追跡する機能である．本機能には，TaintDroid を利用している．Taint タグ追跡機能は，AP が機密情報を取得した際に，機密情報に付加している Taint タグを伝搬させる．これにより，AP が取得した機密情報を細粒度で追跡できる．

3.4 伝搬経路把握機能

伝搬経路把握機能は，AP 間の機密情報の伝搬経路を把握する機能である．本機能は，Taint タグを利用することで実現する．

伝搬経路把握機能は，AP 間で機密情報がやり取りされた際，通信元の AP のパッケージ名，通信先の AP のパッケージ名，やり取りされるデータ，および Taint タグを取得し，取得した情報を記録する．これにより，機密情報の伝搬経路を把握できる．また，機密情報が端末外部に送信される際，記録している情報を利用して，機密情報の漏洩に関わったすべての AP のパッケージ名を取得できる．

3.5 漏洩検知機能

漏洩検知機能は，端末外部への機密情報の送信を検知し，制御 AP を呼び出す機能である．本機能は，Taint タグを利用することで実現する．

漏洩検知機能は，AP が端末外部への情報の送信を要求した際，送信を要求した情報に付加されている Taint タグを取得する．取得した Taint タグから送信を要求した情報に機密情報が含まれているか否かを識別する．含まれていた場合，機密情報の漏洩と判断し，取得した Taint タグから機密情報の種類を特定する．また，機密情報を端末外部に送信する AP のパッケージ名を取得する．取得したパッケージ名を用いて，伝搬経路把握機能が保持している情報から取得したパッケージ名に該当する情報を検索する．該当するパッケージ名が存在した場合，そのパッケージ名の AP と AP 間で機密情報のやり取りを行った AP のパッケージ名と AP 間でやり取りされたデータを取得する．これにより，伝搬経路把握機能から機密情報の漏洩に関わったすべての AP のパッケージ名と AP 間でやり取りされ

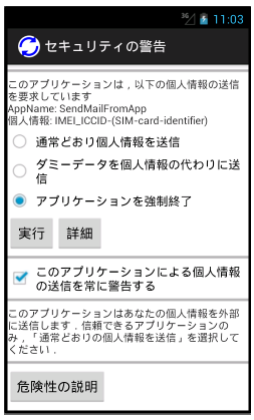

図 2 警告画面

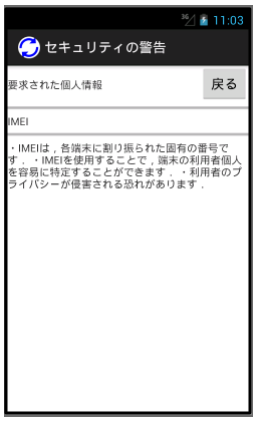

図 3 機密情報の危険性の説明

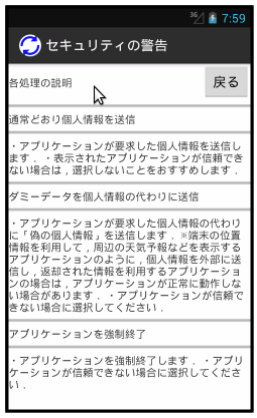

図 4 処理内容の詳細

たデータを取得できる．次に，AP が端末外部に送信するデータに AP 間でやり取りされたデータが含まれているかを確認する．含まれていた場合，そのパッケージ名の AP を機密情報の漏洩に関わった AP と判断し，機密情報の漏洩に関わったすべての AP のパッケージ名を制御 AP に送信する．

3.6 制御 AP

3.6.1 表示する情報

制御 AP は，利用者に警告画面を提示し，利用者の判断結果を取得する AP である．また，取得した判断結果を制御機能に送信する．

利用者の判断を支援するために，警告画面の内容は分かりやすいものでなければならない．提案手法では，利用者が判断しやすい警告画面を以下のように設定した．

(1) 機密情報を外部に送信する AP 名
(2) 機密情報を取得した AP と機密情報を外部に送信する AP が別の場合（複数の AP が連携している場合），すべての AP 名
(3) AP が送信する機密情報の種類（電話番号など）
(4) AP が取得した機密情報の危険性の説明
(5) AP に対する警告画面の表示の有無の選択項目
(6) AP に対する処理内容の選択項目
(7) AP に対する処理内容の詳細

また，設定した内容を実現した警告画面の例を**図 2**，**図 3**，および**図 4** に示し，利用者の判断を支援する情報と利用者の負担を減らす工夫について述べる．

利用者の判断を支援する情報について，利用者に提供する情報としてパッケージ名や UID を提示する既存手法は多い．しかし，これらの情報では利用者は，AP が機密情報を端末外部に送信する動作を許可するか否かの判断が難しい．このため，提案手法では，利用者の判断を支援する情報として AP 名と送信される機密情報を提示する（(1)，(2)，(3)）．また，提示する情報量が多い場合，利用者が判断しづらくなる．このため，表示する警告画面は図 2 の様に 1 画面のみで警告の内容と処理選択ができるようにする．

さらに，機密情報が端末外部に漏洩した場合の危険性を確認できることが利用者の判断を支援するうえで重要である．このため，図 2 の「危険性の説明」ボタンから，図 3 のように AP が取得した機密情報が漏洩することによる危険性を確認できるようにする（4）．なお，機密情報が漏洩することによる危険性は，これらの情報を利用者が必要だと判断した場合に提供できるように，画面遷移を用いて提供する．

次に，利用者の負担を減らす工夫について述べる．提案手法では，機密情報が端末外部に送信されようとするたびに利用者に許可を求める．しかし，許可を求める頻度が高くなると利用者の負担が増加する．このため，利用者に許可を求める頻度を抑制する必要がある．提案手法では，図 2 のチェックボタンで表示されている項目のように，利用者が AP ごとに警告の有無を選択できるようにする（5）．これにより，警告画面の表示頻度を抑制し，利用者の負担を減らすことができる．

さらに，機密情報を漏洩させた AP に対する処理選択において，利用者が処理選択を判断しやすいことが重要である．このため，警告画面における AP に対する処理選択の際，図 2 のラジオボタンで表示されている項目のように，選択項目を三つに限定し，簡単な選択で処理内容を決定できるようにする（6）．また，AP に対する処理内容の詳細は，図 2 の「詳細」ボタンから図 4 のように確認できるようにする（7）．なお，AP に対する処理内容の詳細は，これらの情報を利用者が必要だと判断した際に提供できるよう，画面遷移を用いて提供する．

3.6.2 処理の流れ

制御 AP は，漏洩検知機能から送信された AP のパッケージ名に対応する AP 名と機密情報の種類を取得する．取得した AP 名と機密情報の種類を警告画面に提示し，AP が端末外部へ機密情報を送信する動作を許可するか否かを利用者に尋ね，利用者の判断結果を取得する．制御機能に取得した判断結果を送信する．

3.7 制御機能

制御機能は，利用者の判断結果に従って，AP の動作を制御する機能である．制御機能の処理の流れを述べる．制御機能は，制御 AP から利用者の判断結果を受け取る．受け取った判断結果に従って，AP が機密情報を端末外部に送信する動作を制御する機能である．AP の動作の制御には，AP の動作を制御しない場合と，AP を強制的に終了させる制御方法以外に，利用者の意図しない機密情報の漏洩を防止し，かつ AP を継続して利用できる制御方法が必要である．このため，提案手法では，通常処理，ダミーデータの送信，および強制終了の制御方法を実現する．通常動作は，機密情報の端末外部への送信を許可する場合に選択する．ダミーデータの送信は，機密情報の端末外部への送信を許可せず，AP の動作を継続したい場合に選択する．ダミーデータの送信では，機密情報が端末外部に送信される際，送信される機密情報の代わりに，対応するダミーデータを端末外部に送信する．これにより，AP の動作を終了せず，機密情報の漏洩を防止できる．強制終了は，機密情報の端末外部への送信を許可しない場合に選択する．強制終了は，AP の動作を強制的に終了させ，機密情報の漏洩を防止する．

なお，ダミーデータは，以下の二つの方法のどちらかで置換する．一つ目の方法は，null 文字列のデータに置換するものである．これは，端末外部に送信される機密情報が，カメラ，マイク，およびログの場合に，使用する．このとき，ログの中身は確認せず，null 文字列のデータに置換する．これにより，ログの中身をすべて置換する場合に比べて，処理時間を短縮できる．二つ目の方法は，固定の値を返すものである．これは，端末外部に送信される機密情報が，端末の位置情報，電話番号，および，IMEI（International Mobile Equipment Identifier）などの場合に使用する．

なお，ダミーデータを送信することにより，AP が正常に動作しない場合がある．例えば，利用者の位置情報を取得し，その場所の天気予報を表示する AP が外部にダミーデータを送信したとする．このとき，AP は，利用者の正確な位置情報を取得できないため，利用者がいる場所の天気予報を表示できない．

3.8 期待される効果

提案手法の実現により，以下の効果が期待できる．

(1) 誤検知の削減
TaintDroid を利用し，細粒度で機密情報の伝搬を追跡することで，API を用いた機密情報の伝搬追跡と比較して，誤検知を削減できる．

(2) 機密情報の漏洩の防止
細粒度で機密情報の伝搬を追跡することで，AP が端末外部に機密情報を送信する動作を検知し，利用者にその動作を許可するか否かを尋ねる．これにより，機密情報の漏洩を防止できる．

(3) 機密情報の漏洩に関わったすべての AP 名の取得
AP 間の機密情報の伝搬経路を把握することで，機密情報の漏洩に関わったすべての AP 名を取得することができる．これにより，利用者は，機密情報の漏洩に関わったすべての AP に対処できる．

(4) AP の動作を妨げない機密情報の漏洩の防止
AP が端末外部に機密情報を送信する動作に対する利用者の選択項目として，ダミーデータの送信を追加した．これにより，利用者は，通常の AP の動作を妨げることなく，機密情報の漏洩を防止できる．

(5) 利用者の負担の軽減
警告画面において，利用者が AP に対する処理を容易に選択できる．また，利用者は，AP ごとに警告表示の有無を選択できる．これにより，利用者の負担を軽減できる．

4. 実現と評価

4.1 実現内容

現時点では，伝搬経路把握機能と AP ごとの警告表示の有無の設定を除くすべての機能を実現しており，機密情報の漏洩の防止とダミーデータによる端末外部に送信される機密情報の置換を実現している．しかし，伝搬経路把握機能が実現できていないため，機密情報の漏洩に関わったすべての AP の取得ができない．また，2 回目以降の警告表示の有無を AP ごとに設定することができない．このため，今回は，現時点で実現している機密情報の漏洩を防止する機能について評価する．

4.2 評価の目的と評価環境

評価の目的について以下に示す．なお，評価では，VM 上で動作する Android Emulator を用いた．ゲスト OS と Android Emulator の評価環境を**表 1** と**表 2** に示す．

(1) 機密情報の漏洩防止の確認
Android に提案手法を適用することで，AP による機密情報の漏洩を検知し，利用者が AP による情報の送信を拒否することで，AP による不正な機密情報の漏洩を防止できることを示す．

表 1 ゲスト OS の評価環境

ディストリビューション	Ubuntu 10.04.4 LTS
カーネル	Linux ubuntu 2.6.32-42-generic
仮想 CPU 数	4
メモリ	4 GB

表 2 Android Emulator の評価環境

Android バージョン	Android 4.1
TaintDroid バージョン	TaintDroid 4.1(updated Dec 6, 2012)

図 5 作成した AP の起動画面

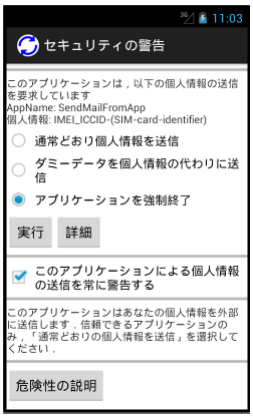

図 6 制御 AP の警告画面

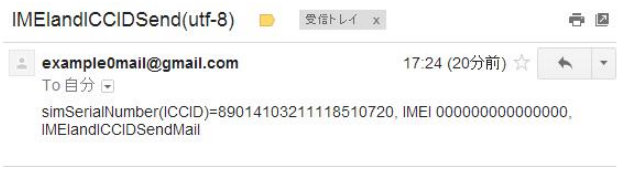

図 7 AP を通常動作させた場合の送信内容

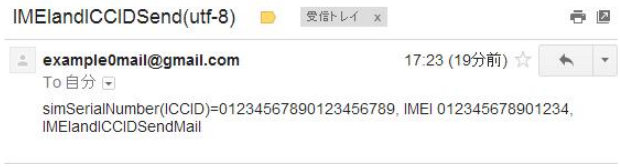

図 8 AP にダミーデータを送信した場合の送信内容

(2) 外部に漏洩する機密情報の置換結果の確認
AP によって端末外部に送信される機密情報をダミーデータに置換できることを示す．

4.3 機密情報の漏洩防止

4.3.1 評価に使用する AP

本評価では，ダミーデータを送信することで，通常の AP の動作を妨げることなく，機密情報の漏洩を防止できることを示すために，IMEI と ICCID（Integrated Circuit Card ID）を取得し，Gmail を用いて端末外部に IMEI と ICCID を送信する AP を作成し使用する．

4.3.2 評価結果

作成した AP を提案手法で動作させた場合の動作結果を以下に示す．

(1) 作成した AP は，起動すると**図 5** の画面を表示
(2) ボタンを押下すると，AP は IMEI と ICCID を取得し，Gmail の SMTP サーバを用いて，指定した Gmail アドレスへ取得した情報を送信
(3) 機密情報の送信を検知し，制御 AP が呼び出され**図 6** の画面を表示
  (A) 「アプリケーションを強制終了」を選択し，「実行」ボタンをを押下した場合，AP はエラーにより強制終了
  (B) 「通常どおり個人情報を送信」を選択し，「実行」ボタンを押下した場合，**図 7** のように端末外部に機密情報を送信
  (C) 「ダミーデータを個人情報の代わりに送信」選択し，「実行」ボタンを押下した場合，**図 8** のように機密情報をダミーデータに置換した内容を送信

(3) のように，利用者は，AP が端末外部に機密情報を送信する動作を動的に制御できる．また，送信される機密情報をダミーデータに置換することで，機密情報を端末外部に送信した結果を使用しない限り AP の動作を妨げることなく，機密情報の漏洩を防止できる．

5. 関連研究

API を用いた機密情報の漏洩を防止する研究として，文献 [6] がある．文献 [6] 手法では，機密情報にアクセスする API と機密情報を外部に漏洩する API をフックし，ユーザが API の利用の可否決定をすることで機密情報の漏洩を防止する．なお，文献 [6] の手法では，利用者に動作履歴を提示する．一方，提案手法は，TaintDroid を利用し，変数レベルでの機密情報の伝搬追跡を行う．このため，文献 [6] の手法に比べて，追跡精度が高く，誤検知の少ない機密情報の漏洩防止手法を実現している．

機密情報をダミーデータに置換することにより機密情報の漏洩を防止する研究として，文献 [7] がある．利用者が，AP からアクセスできる機密情報を正規の機密情報かダミーデータかあらかじめ AP ごとに設定する．これにより，正規の機密情報へのアクセスを許可していない AP による機密情報の漏洩を防止する．しかし，文献 [7] の手法では，AP が機密情報を取得する際にダミーデータに置換する．このため，AP が正常に動作しない問題がある．例えば，AP が正規の機密情報を取得することで動作を継続する場合，AP がダミーデータを取得することで，AP が強制終了することがある．一方，提案手法では，端末外部に機密情報が送信される際に機密情報をダミーデータに置換する．このため，AP による機密情報の取得を制限しない．これにより，提案手法では，端末外部へ機密情報を送信しない限り，AP の動作を妨げない．

TaintDroid の利用により機密情報の漏洩を防止する研究として文献 [9] と文献 [10] がある．文献 [9] は，AP のインストール時に，AP が取得した情報を端末内でのみ使用するか端末外部への送信を許可するかを利用者が選択することにより，機密情報の漏洩を防止する手法を提案している．このため，インストール時以外には，利用者は機密情報の使用範囲を変更できない．このように，文献 [9] の手法では，利用者が任意のタイミングで設定を変更できない．一方，提案手法は，AP が端末外部に機密情報を送信する際，

利用者が機密情報の送信を許可するか否かを設定できる．また，利用者は任意のタイミングで設定を変更できる．文献 [10] は，機密情報をダミーデータに置換することにより機密情報の漏洩を防止する手法を提案している．また，文献 [10] の手法は，ポリシを用いて機密情報の漏洩を防止する．しかし，端末上でポリシの設定を変更できない．このため，利用者が任意のタイミングでポリシを変更し，AP の動作の制御方法を変更することはできない．一方，提案手法は，すべての機能を端末上で実現し，AP の動作の制御方法を変更できる機能を提供している．このため，利用者は，任意のタイミングで AP の動作の制御方法を変更できる．

6. おわりに

機密情報の伝搬を追跡し，機密情報が外部に漏洩する際に利用者の判断に従って AP の動作を動的に制御する手法を提案した．提案手法は，TaintDroid を利用し，機密情報の伝搬を追跡する．端末外部に機密情報が漏洩する場合，利用者の判断に従って AP の動作を制御する．これにより，端末外部への機密情報の漏洩を防止する．また，端末外部に送信される機密情報をダミーデータに置換することで，AP の通常の動作妨害することなく機密情報の漏洩を防止できる．さらに，AP 間で機密情報のやり取りがあった場合，機密情報の伝搬経路を把握することで，機密情報の漏洩に関わった AP 名を取得できる．

評価では，作成した AP を用いて，機密情報の漏洩を防止できること示した．また，端末外部に送信される機密情報をダミーデータに置換することで，通常の AP の動作を妨げることなく，機密情報の漏洩を防止できることを示した．

今後の課題として，伝搬経路把握機能の実現と実 AP を利用した評価がある．

謝辞 本研究の一部は，公益財団法人 栢森情報科学振興財団 平成 23 年度研究助成による．

参考文献

[1] Android, http://www.android.com/
[2] Google Play, https://play.google.com/store
[3] Zhou, Y. and Jiang, X. :Dissecting Android Malware: Characterization and Evolution, Proceedings of the 33rd IEEE Symposium on Security and Privacy (Oakland 2012), (2012).
[4] Symantec, 日本の Android ユーザーから利用者情報を盗み出す”The Movie”マルウェア http://googlemobile.blogspot.jp/2012/02/android-and-security.html
[5] 産経ニュース，スマホアプリで 76 万件分の利用者情報流出か「全国電話帳」インストールに注意 http://sankei.jp.msn.com/affairs/news/121006/crm12100617380008-n1.htm
[6] 林 里香，後藤 厚宏，: Android アプリケーション利用の安全性を高めるアプリケーション動作の「見える化」，コンピュータセキュリティシンポジウム 2012(CSS2012) 論文集，vol.2012，no.3，pp.130-137(2012).
[7] Beresford, A.R. Rice, A. Skehin, N. and Sohan, R. : MockDroid: Trading privacy for application functionality on smartphones, Proc. 12th Workshop on Mobile Computing Systems and Applications (HotMobile) (2011).
[8] Enck, W. Gilbert, P. Gon Chun, B. Cox, L.P. Jung, J. McDaniel, P. and Sheth, A.N. : TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones, Proc. 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI) (2010).
[9] 梶原 直也，堀 良彰，櫻井 幸一，: 情報フロー追跡を用いた Android 端末における情報送信制御，2013 年暗号と情報セキュリティシンポジウム (SCIS2013) 論文集，電子媒体 (2013).
[10] Hornyack, P. Han, S. Jung, J. Schechter, S. and Wetherall, D. : These aren't the droids you're looking for: retrofitting android to protect data from imperious applications, Proc. 18th ACM conference on Computer and communications security (2011).
[11] Schlegel, R. Zhang, K. Zhou, X. Intwala, M. Kapadia, A. and Wang, X. : Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones, Proc. 18th Annual Network & Distributed System Security Symposium (NDSS '11), pp. 17-33 (2011).