安全な BYOD 機能提供のための Android アプリケーションの提案と開発

山本恵理[†1]　佐々木良一[†2]

近年，会社にスマートフォンなどの私物端末を持ち込み，仕事に使用するという BYOD(Bring Your Own Device)の考え方が注目を集めている．しかし，マルウェアなどによる情報漏洩の危険性が日本では危惧されているため，現段階で企業での導入例は少ない．そこで本稿ではアンドロイド端末で BYOD 機能を安全に利用するため，ホワイトリストを複数用意し，ホワイトリストごとにアプリケーションの立ち上げ制御を行うアプリケーションの提案及び開発をする．他の BYOD 機能よりも安全性，利便性を提供するためホワイトリストを自動的に切り替える仕組みや，アプリケーションの改竄検知機能を付加し，このアプリケーションを利用することで，私物端末からの情報漏洩のリスクを減らし、安全かつ便利にスマートデバイスを利用できる機能を提供する．

The proposal and development of Android application for safe BYOD functional offer

ERI YAMAMOTO[†1]　RYOICHI SASAKI[†2]

1. はじめに

近年，スマートフォン・タブレットが注目を集めている．これらは，小型のパソコンともいえるほど充実した機能を提供し，世界的に利用者が増加している．

このように，スマートフォン・タブレット端末の普及により，パソコンと同じように業務での使用を考えたBYODへの関心が急速に高まっている． Trusted Mobility Index[1]の調査によると約4000人を対象に行ったアンケートの内74%のユーザは、会社が個人のモバイル端末の業務利用を認め、必要なセキュリティ対策を取ってほしいと考えていることが判明している．

しかしその一方で，日本でのBYODの普及率は低く留まっている．その理由として考えられるのが，近年増加しているスマートフォンのマルウェアによる情報漏洩事故である．マルウェアとは，悪意をもったソフトウェアのことである．実際にあったマルウェアによる情報端末からの情報漏洩事故として記憶に新しいのが，スマートフォンの電話帳に登録されている連絡先を抜き取り，インターネットに送信するというマルウェアによる情報漏洩事故である．そして，こうしたマルウェアのターゲットとして割合が最も高いプラットフォームがアンドロイドOSである[3]．図1からも分かるように，カスペルスキーラボの調査によると，モバイル系OS全体を狙ったマルウェアのうち約9割がアンドロイドOSを標的としていることが判明している[4].

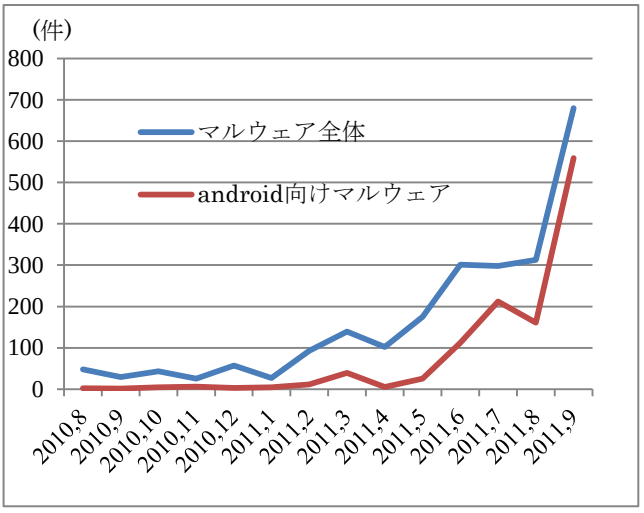

図 1　Android マルウェアの増加

Figure 1　The increase of malware in android devices

そこで本研究では，最も標的とされているアンドロイド OS の端末を BYOD で使用する際，端末をマルウェアによる情報漏洩の危険性から保護するために，複数のホワイトリストを利用してアプリケーションの立ち上げを制御する，安心かつ利便性のあるアプリケーションの提案及び開発を行う．

†1 東京電機大学大学院
†2 東京電機大学 教授

2. BYODについて

BYODとは，Bring Your Own Deviceの略語であり，企業などで従業員が私物の情報端末を利用し，業務を行うことを示す．私物として普段から使っているスマートフォン･タブレットなどから企業の情報システムにアクセスし，必要な情報を閲覧したり書き込みを行なったりすることを意味する．このBYODであるが，スマートフォン・タブレットの急速な普及とともに注目が集まっている．

BYODが注目される理由として，BYODを取り入れることで以下のような利点があげられるためだと考えられる．

(1) 普段使い慣れている端末で作業を行うことが出来るため，使い慣れない端末よりもスムーズに業務を行うことができ，仕事効率が改善される
(2) 会社以外の場所にいるときに業務を行いたい場合などでも利用場所を限定されずに，社内と同じような業務を行うことができるため利便性が高い
(3) 企業が従業員に個々の情報端末を用意する必要がなくなり，企業の大幅なコスト削減が期待される

これまで業務で利用する情報端末は，会社側から提供されることがほとんどであり，自分で使用しやすい端末を選択することができなかった．そのため，会社のコスト面の負担が大きく，社員も使い慣れない端末で業務を行うことになるため，仕事の効率が著しく低下していた．また，従来の携帯電話だと仕事で使用できる機能がメールほどだったが，スマートフォン･タブレットが普及したことにより，インターネットにどこからでも繋がる環境ができたため，BYODへの企業の関心が高まっている．

以上のように，BYODによって享受できるメリットは大きく，その必要性も高まってはいるが，情報端末をターゲットにしたマルウェアからの情報漏洩が懸念されている．そのため，欧米・ヨーロッパでは6割以上，同じアジア圏でも中国・韓国では9割以上の普及率のBYODだが，情報漏洩問題に対して敏感な日本での普及率は3割程度と，あまり普及していないのが現状である．

2.1 安全なBYOD導入へ向けての課題

BYODを導入する目的としてコストや利便性など様々なものが考えられる．実際にBYODを社内導入している企業では7割以上の使用者が仕事の効率やスピードが上がったなど，その効果を実感している[5]．BYODを導入するメリットであるコスト削減についてはBYODの利便性を考えた企業側が導入を進めると後から付いてくるものと考えられる．よって企業のBYOD導入に先立ち，利便性に着目して研究を進めていくべきだと考えられる．利便性に着目をすると，企業の重役など信頼できる人物が利用場所を限定されずに，業務に関わる情報を便利かつ安全に利用したいという場合が考えられる．企業の重役などは，会社に留まり仕事をしているよりも，出張業務など社外で仕事をしていることが多いためである．

その場合，企業の利益を最も意識し重要視している企業の重役が故意に情報漏洩を起こすことは考えにくいため，端末利用者による不正は考慮する必要性がないが，マルウェアや不正侵入による情報漏洩に対しての対策が必要となる．こういった問題に対する既存の対策手法として代表的なのは，MDMでスマートフォン・タブレット端末を強制的に制御する技術があるが[6]，これはいったん適用された制御内容を利用者が任意に変更することが出来ないため，情報端末の業務利用と私的利用の状態に応じて動的に制御を切り替えることが出来ないという問題がある．また，その他のBYODに関する技術も，時間帯でモードを切り替える方法などがあるが，柔軟性に欠けている．このような問題点から，ユーザが制御内容を任意に変更でき，動的に制御の切り替えをできる手法が求められている．

そのため、上記のような利用目的でBYODを導入する際には，情報端末に登録されているアプリケーションごとに使用できる場所を指定できるようにホワイトリストを作り，管理する対策方法が考えられる．このホワイトリストによる外部通信制御や立ち上げ制御を行い，マルウェアや不正侵入による情報漏洩の被害を防止する必要がある．このように情報端末を利用する場所に対応したホワイトリストを用意し，利用環境に対応したホワイトリストに自動的に切り替わる動的変更により安全性と利便性を両立させ，柔軟に対応できる仕組みが必要だと考えられる．

3. 提案内容

本研究では，安全なBYODの提供を目的とし2章で述べたような利用目的で安全性と利便性を満たすために，情報端末にインストール済みのアプリケーションの立ち上げ制御を，情報端末を利用する環境に応じて使い分けする事ができるアンドロイドアプリケーションを開発する．

情報端末の利用環境を，会社，自宅，その他の3パターンに分け，それぞれの環境で利用しても良いアプリケーションのリストであるホワイトリストを作成する．その3パターンのホワイトリストを利用環境が変わるごとに自動的に切り替え，柔軟な対応を実現する．

また，マルウェアによるアプリケーションの改竄の危険性を考慮し，アプリケーションの証明書を登録し，そのハッシュ値の照合・検証により改竄を検知する機能を搭載する．

3.1 証明書による改竄検知

開発者がアンドロイド用アプリケーションを一般に配

布する際には，マーケットにアプリケーションを登録し，それをユーザがインストールする形が主流となっている．

このように，開発者がマーケットにアプリケーションを登録する際は，アプリケーションの作成者を識別し，アプリケーション間の信頼関係を確立する手段として証明書を使用するため，APKファイルに署名する必要がある．

一般ユーザがアプリケーションをアンドロイド端末にインストールする際，証明書がアプリケーション情報に付加されるため(図2)，その端末にインストールされている全てのアプリケーションの証明書のハッシュ値をホワイトリストとして登録し，管理する．

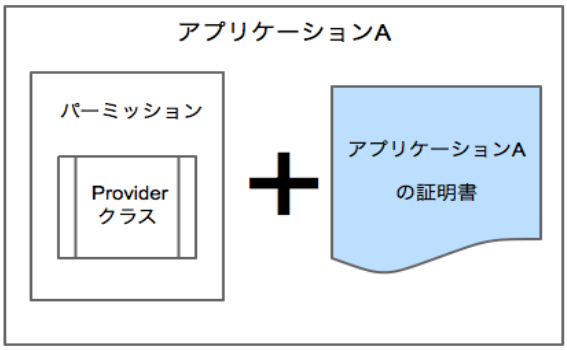

図2 アプリケーションの情報
Figure 2 Information on application

アプリケーションの初期起動の際に，このアプリケーションの証明書がホワイトリストとして登録される．初期起動の際に登録されたホワイトリストの証明書のハッシュ値と，動作しているアプリケーションの証明書のハッシュ値との相違が生じた場合，アプリケーションの改竄を検知する仕組みである．改竄を検知するとユーザに改竄を知らせるダイアログが表示される．

この仕組みにより，マルウェアによるアプリケーション間のパーミッションの改竄やデータの書き換えなどの情報改竄を検知することができる．

3.2 利用環境による複数のホワイトリスト

利用環境によるアプリケーションの使い分け方法として，アンドロイド端末にインストール済みのアプリケーション一覧から，利用環境によって使用できるアプリケーションの選別を行い，ホワイトリストに登録し，自動的に複数のホワイトリストを切り替える方法を提案する．

利用場所に応じたホワイトリストの例として想定しているのは3パターンである．ホワイトリストを3パターン用意する利点としては，ホワイトリストを3パターン用意し，考えうる端末使用場所をすべてカバーすることで，様々な環境で柔軟な対応をすることができる点にある．

以下に，想定される3パターンのホワイトリストとその内容を示す(図3)．

図3 想定する3パターンのホワイトリスト
Figure 3 The white lists for assumed three patterns

(1) 自宅のホワイトリスト

自宅のホワイトリストとは，自宅で私物の端末を使用するときのアプリケーションのリストを示す．

自宅でスマートフォンを利用する際には，ゲームやSNSなどのアプリケーションを利用することが考えられる．このとき何の対策も講じていない場合，個人情報を収集する悪意のあるアプリケーションを社員がインストールし，使用してしまうなどの危険性が考えられる．そのため端末の持ち主が自宅で使用したいアプリケーションの選別を行い，その正当性を会社の管理者がチェックしたうえで，ホワイトリストとして登録する．

(2) 会社のホワイトリスト

会社のホワイトリストとは，会社で業務を行う際に使用するアプリケーションのリストを示す．

会社でスマートフォンを利用する際には，ゲームやのアプリケーションを使用すると，仕事効率が下がる他，会社の機密情報が外部に漏れてしまうという，情報漏洩の危険性が考えられる．そのため，会社の管理者により，業務中に使用できるアプリケーションの選別を行い，ホワイトリストとして登録する．

(3) その他のホワイトリスト

その他のホワイトリストとは，会社以外の，図書館やカフェなどから業務を行いたいときに登録するホワイトリストのことを示している．

この，その他の場所でスマートフォンを利用する際には，ゲームなどのアプリケーションを使用すると仕事効率が下がってしまうが，会社と連絡を取る

ためにSNSなどのアプリケーションを使用したいという場合が考えられる．その際，会社のホワイトリストよりも柔軟ではあるが，自宅のホワイトリストと比べると制限を厳しくしたホワイトリストが必要であると考えられる．また，その他のホワイトリストは，あくまで業務を行う場合を想定しているため，アプリケーションの選別は会社の管理者が行うことになる．

図4にホワイトリスト登録までの流れを示す．

図5 ホワイトリスト登録までの画面遷移

Figure 5 Screen transfers for white list registration

この3パターンのいずれかにアプリケーション振り分けを行いホワイトリストとして登録する．

しかし，この3パターンのリストを任意の人物が作成できてしまうと，第三者によるリストの書き換えが容易に行われる可能性がある．そこで，会社で使用できるアプリケーションのリストと，会社以外の出先等で使用できるアプリケーションのリストは，あくまで仕事を行う環境であると考え会社の管理者のみがリストの作成を行えるようにするためパスワードの設定機能を付加する．自宅で使用するアプリケーションのリストについては，端末の所有者のみがリストの作成を行なえるようにするためパスワードの設定機能を付加する．これにより，パスワードを設定した者のみがホワイトリストの作成を行なえるようになり，私物端末をプライベートで利用するときと仕事で利用するときの設定が安全かつ明確におこなわれるようになる．

この3パターンの何れかにアプリケーションを登録し利用環境が切り替わると，その利用環境のホワイトリストで許可されていないアプリケーションは，その立ち上げを停止する．これにより，端末にマルウェアが潜んでいたとしても，使用できるアプリケーションが最小限に抑えられているホワイトリストを使用中の場合，マルウェアによる情報漏洩を防ぐことが可能である．

また，これらのホワイトリストを登録する際は，同時に，3パターンのどのホワイトリストであるかを選択し，登録する．図5に，ホワイトリストの作成から登録までの流れをフローチャートで示す．

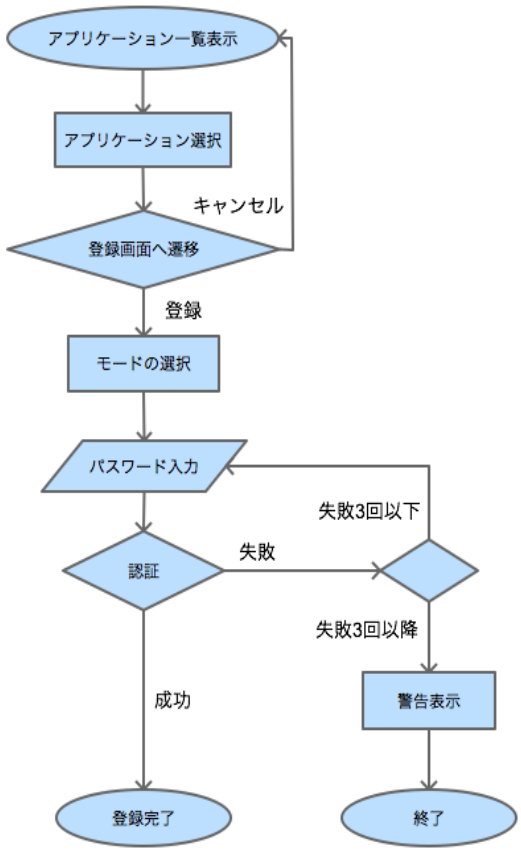

図6 ホワイトリスト登録までの流れ

Figure 6 The flow for white list registration

3.3 ホワイトリストの動的切り替え

適用するホワイトリストを動的に切り替えるトリガとして，各ホワイトリストの利用環境ごとのSSIDの検知とGPSの情報を組み合わせる方法を提案する(図6)．SSIDとは，IEEE 802.11シリーズの無線LANにおけるアクセスポイントの識別子のことである．混信を避けるために付けられる名前で，最大32文字までの英数字を任意に設定できる．また，GPSとはGlobal Positioning Systemの略称で，人工衛星を利用して端末が地球上のどこにいるのかを正確に割り出すシステムのことである．これにより，スマートデバイス

の緯度・経度・高度などを数cmから数十mの誤差で割り出すことができるものである．このSSIDとGPSの情報によってホワイトリストの動的切り替えを行う．SSIDとGPSの情報を併用することにより，利用場所によるホワイトリストの切り替えをより正確に行う．

また，ホワイトリスト方式を採用する理由として，ブラックリスト方式と比較して，厳密性が高く，安全性が高いため，ホワイトリストに登録されていない未知のアプリケーションの立ち上げが不可能になるという点が上げられる．

図7 トリガによるモードの切り替え

Figure 7 The change of the mode depending on triggers

4. プロトタイプの実装

3章の提案手法を元に，アンドロイドアプリケーションのプロトタイプの実装を行なった．プロトタイプの実装にあたって，現段階では，アプリケーションの立ち上げ制御の前段階として，アプリケーションのネットワーク通信制御の実装を行なった．アプリケーションの改竄検知については，3.1節で述べたものを採用している．

開発環境は以下の通りである(表1).

表1 開発環境

Table 1 Development environment

開発OS	Mac OS X Mountain Lion
開発環境	Pleiades eclipse 3.5 エミュレータ：Android4.1
開発言語	Java、xml
SDK	Android 4.1 x Platform

4.1 モード切り替えのトリガ

複数のホワイトリストを切り替える方法として，SSID と GPS 情報の併用により自動的に切り替わる方法を提案した．しかし，実際にアプリケーションを使用していると，電波障害や誤設定などにより SSDI と GPS の両方の情報が取得できない場合が考えられる．その場合の対策として，両方の情報が取得できない場合は自動的にその他のホワイトリストモードへ移行し，その後，手動でホワイトリストの切り替えが行えるようになる機能を付加した．その他のモードは 3 パターンのモードの中でも，会社と自宅の両方に連絡を取ることができ非常時にも対応することができるためである．これにより，自動的にホワイトリストが切り替わらない場合でも，端末利用者が適切なモードへ切り替えを行うことができる．

4.2 ネットワーク通信制御

今回のプロトタイプでは，立ち上げ制御の前段階として，ネットワーク通信の制御を行う機能を実装した．これにより，ネットワーク通信を必要とするホワイトリストで許可されていないアプリケーションの外部への情報流失の危険性の低減を図る．また，ネットワーク通信の制御においては，図7にあるように，その設定を3G通信とWifi通信についてそれぞれネットワーク通信の制御を行なえるように開発を行った．3Gとは，ITU(国際電気通信連合)で標準化されたディジタル携帯電話システムであり，モバイルインターネットの進化に伴い，データ通信の高速化などに対応するためのシステムである．また、WifiとはWireless Fidelityの略称であり、Wifi Allaianceによって、国際標準規格であるIEEE 802.11規格を使用したデバイス間の相互接続が認められたことを示す名称である．

このように，アンドロイド端末にデフォルトではついていない機能を付加することで通信方法を識別することにより，ネットワークの通信制御方式をより細かく行えるようになる．

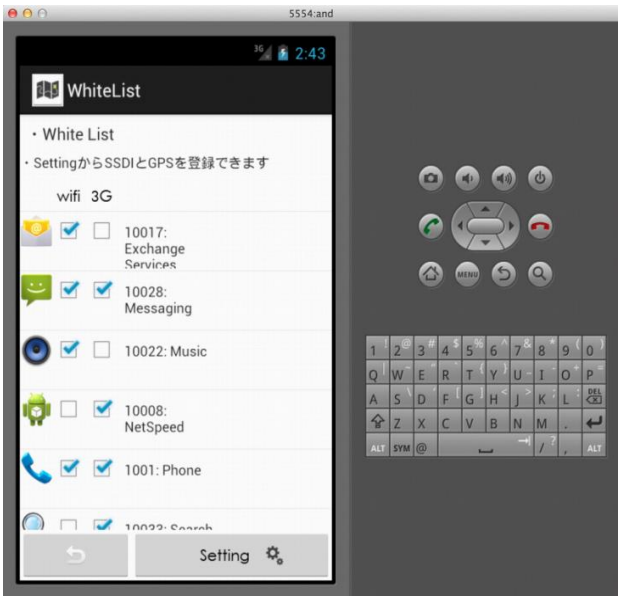

図8 ネットワーク通信設定画面

Figure 8 Network communication setting screen

4.3 端末の root 化

今回開発したアプリケーションを使用するには，アンドロイド端末を root 化する必要がある．通常，一般ユーザが端末を使用する場合，ユーザ権限という一部の機能しか使用できないモードでシステムを使用している．よって一部のファイルにアクセスが禁じられており，機能に制限が設けられている．root 化とは，アンドロイドをプラットフォームとするスマートフォン・タブレットにおいて，root 権限でシステムを操作できるように改造することである．root 化を行うことで、あらかじめ設けられた機能の制限を取り外し，端末をより自由に使用することができ，開発側の自由度も高くなる．本研究で提案しているアプリケーションの立ち上げ制御は，root 権限を必要とするため端末の root 化を行う必要がある．

5. 考察

5.1 機能の比較

本研究にて実装したアプリケーションを, 他の BYOD の運用を目的としたアプリケーションの主な機能と比較することにより考察を行った．表 2 にその機能を表として示す.

表 2 各アプリケーション機能の比較
Table 2　Comparison of each application function

	機能
本研究	ホワイトリストを複数用意することにより, 利用環境に応じたアプリケーションの使い分けが可能となっている. 利用環境ごとの切り替えが SSID と GPS の情報により自動的に行われる. アプリケーションごとのハッシュ値を管理することで, 改竄の検知を行うことができる.
MDM [9]	情報端末内のアプリケーションを利用不可に設定できる. リモートワイプやリモートロックにより，情報端末を紛失した際の情報の漏洩を防ぐ.
NTT データ [10]	時間帯，GPS，SSID の情報により，業務モードと私用モードを切り替えることが出来る. MDM との連携により，リモートワイプやリモートロックを行うことが出来る.
DME [11]	一つの管理コンソールで，社内の情報端末，アプリケーション，ユーザを管理することができる. 組み込み型の MDM を使用して，リモートワイプを行うことが出来る.

次に、本研究で想定している利用環境とそのとき必要とされる機能を示し、それらに対し上記で上げた BYOD の運用を目的としたアプリケーションがどの程度有用かを示す (表 3). なお，表 3 において，有用性を 3 段階で示し，〇は有用性が十分にあると考えられる場合，×は有用性があるとは考えにくい場合, △はどちらともいえない場合を示す.

表 3 想定状況におけるアプリケーションの有用性の検討
Table 3　Examination of the usefulness of the application in an assumption situation

想定している状況					
企業の重役など信頼できる人物が利用場所を限定されずに，業務に関わる情報を便利かつ安全に利用したい場合.					
		NTT Data	DME	MDM	本研究
利便性	端末の利用環境に応じて適切なアプリケーションをリストアップしたホワイトリストを複数作成することが出来き，端末を使用する場所に応じて使用できるホワイトリストを切り替える.	△	×	×	〇
安全性	端末がマルウェア等に感染してしまった場合の情報漏洩対策.	×	×	×	〇
	端末を紛失してしまった場合の情報漏洩対策.	〇	〇	〇	△

表 2 に示したように，本研究以外は最大 2 つまでのモードしか設定することができず，NTT のアプリケーションに関しても今回想定している状況の場合だと柔軟性に欠けていると考えられるため，表 3 においての有用性評価を△としている．また安全性において，本研究はマルウェアによる情報漏洩対策を行なっているため，安全性が高い．端末を紛失した際の対策に関しても，他人が閲覧できる情報はその他モードの限られたものとなっている．今後，他の BYOD アプリケーションのようにリモートワイプやリモートロック機能と組み合わせることで，より安全性を高めることが出来ると考えられる.

5.2 今後の課題

本研究では，安全なBYOD機能を提供するためのアンドロイドアプリケーションを開発した．しかし，今回のプロトタイプで実装した機能であるネットワーク通信の遮断だ

けでは，すべてのマルウェアへの対策は不十分なため，今後は，アプリケーションの起動を制御することでマルウェアによる情報漏洩を防ぐ機能を追加する予定である．

また，4.2節で述べたように，root化により使用者側・開発者側共にメリットはあるものの，システムレベルでの改造が行われるため，マルウェアに対する危険性が高まる恐れがある．さらに考えられる問題点は，ホワイトリストに誤ってマルウェアを登録してしまう危険性である．これらの対策として，端末にアプリケーションをインストールする際と，本アプリケーションでホワイトリストを作成する際にパーミッションの制限を設ける機能を追加する予定である．パーミッションとは，アプリケーションをインストールする際に，ライブラリへのアクセス権限をユーザが承認する機能のことである．

アプリケーションをインストールした際のパーミッション承認画面の例を図 8 に示す．

図 8 パーミッション要求画面

Figure 8 Screen for requiring permission

パーミッションを承認することによって扱えるデータの中には個人情報に関わるようなパーミッションも存在する．そのため，これらの機能を付加することが，事前に不正なマルウェアを端末にインストールしないための対策と，安全なホワイトリストを作成するために必要だと考えられる．

6. おわりに

本研究では，最も標的とされているアンドロイド OS の端末を BYOD で使用する際，端末をマルウェアによる情報漏洩の危険性から保護するために，複数のホワイトリストを利用してアプリケーションの立ち上げを制御する，安心かつ利便性のあるアプリケーションの提案及び開発を行った．

今回実装したアプリケーションは，5 章でも述べたように，他の BYOD の運用機能を提供するアプリケーションで対策されている，端末を紛失した際の対策が不十分であると考えられる．そのため，本アプリケーションにも端末を紛失した際の対策についても考慮する必要があると考えられる．具体的には，端末を紛失した際に遠隔操作によって端末内のデータを消去する機能や，端末にロックをかける対策が考えられる．

また，さらに安全性を高めるためネットワーク通信の遮断以外にアプリケーションの起動制御起機能を実装し，実用実験を行なっていきたいと考えている．

参考文献

1) Our Mobile Planet,
<http://www.thinkwithgoogle.com/mobileplanet/ja/downloads/>
2) Trusted Mobility Index,
<http://www.juniper.net/jp/jp/company/press-center/press-releases/2012/pr_2012_05_22-15_00.html>
(2012.3) .
3) MMD 研究所，職場での私用スマートフォンの利用実態調査,
<http://mmd.up-date.ne.jp/news/detail.php?news_id=1177>
4) McaAfee，セキュリティ研究レポート,
<http://www.mcafee.com/japan/security/publication.asp>
(2012.4) .
5) IT Pro，深刻さ増す Android マルウェア,
<http://itpro.nikkeibp.co.jp/article/COLUMN/20120210/380960/>
(2012.2) .
6) (著)吉田 晋,スマートフォンの業務利用におけるセキュリティ対策
(出版社)ソフトバンククリエイティブ
(2012.3) .
7) AV-TEST，Detailed Test Reports,
<http://www.av-test.org/en/tests/mobile-devices/android/ >
(2012) .
8) Android Developers,
<http://developer.android.com/develop/index.html>
9) The What, Why, and How of Master Data Management,
<http://msdn.microsoft.com/en-us/library/bb190163.aspx>
10) NTT Data,
<http://www.nttdata.com/jp/ja/news/release/2013/041500.html>
(2013.4)
11) Soliton DME,
<http://www.soliton.co.jp/products/service/dme/>
<http://www.theregister.co.uk/2013/05/02/gartner_half_firms_demand_byod/>
12) ZDnet,
<http://www.zdnet.com/topic-byod-and-the-consumerization-of-it/>
13) BYOD Risks & Rewards
<http://www.sophos.com/en-us/security-news-trends/security-trends/byod-risks-rewards.aspx>
14) Forget choice: 50% of firms will DEMAND you BYOD by 2017,
<http://www.theregister.co.uk/2013/05/02/gartner_half_firms_demand_byod/>