L-017

BYOD(Bring Your Own Device) に対応した個人情報保護手法の提案
Proposal of Personal Information Protection Method for BYOD(Bring Your Own Device)

城ヶ崎 寛 †　　中村嘉隆‡　　高橋　修‡
Hiroshi Jogasaki　Yoshitaka Nakamura　Osamu Takahashi

1. はじめに

BYOD(Bring Your Own Device)とは，会社・団体等の組織構成員が個人所有するスマートデバイスを私用ではなく，組織での活動目的で活用することをいう．iPhone, Android, Windows Phone 端末のようなスマートデバイスは，PC 同様個人所有を前提として普及してきた機器である．利便性が評価されて現在，組織での採用が相次いでいる．しかし，デバイスを生かし切る使い方として BYOD は今後の普及が望まれている．その理由は以下の３点に集約される．（１）満足度，生産性の向上（２）ワークスタイルの変革（３）端末コストの削減　である．[1]しかし現実的には，個人所有の端末を組織仕様で使用する場合，使用制限が入ったり，個人情報を組織側が意図せずに入手できたりするケースが想定される．一般にデバイスの運用管理を簡便にする，MDM (Mobile Device Management)などの仕様は，次のような目的および期待する効果のために導入されるため，主として組織側に都合のよい仕様となりがちである．

表１　一般的な MDM の導入目的と期待する効果[2]

項番	導入目的と期待する効果
1	端末に対する新規および変更設定を簡便かつ迅速に実施し，大量の端末を一元管理する
2	組織の情報資産の漏えい・持ち出しを防ぐため，端末に機能制限を施す
3	資産管理の観点から，端末種別，ＯＳ種別，利用アプリケーション種別等を管理する
4	組織のセキュリティポリシーに基づき管理する
5	端末の紛失・盗難時に組織の情報資産の漏えいを防止する
6	マルウエアへの感染による情報漏えいを防止する
7	端末のデータ資産を適切に保護・保全する
8	端末の法人所有・個人所有の区別を明確にする

ただし，BYOD においては，以下にあげるような個人情報の取り扱いに，注意を要する．（１）個人情報を含む電話帳（２）GPS 等で補足可能なデバイスの位置情報（３）通信内容・履歴・メールの内容，送受信履歴等（４）デバイス内の個人利用目的のアプリケーション一覧およびアプリケーション利用履歴　等

本稿は，端末の所有者に都合の良い仕様，すなわち不必要に個人情報を漏洩せず保護する実装方式を提案する．本稿では，実装対象を Android 端末とする．

† タタコンサルタンシーサービシズジャパン株式会社
TATA Consultancy Services Japan Limited
‡ 公立はこだて未来大学
FUTURE UNIVERCITY HAKODATE

2. 既存方式の概要

本章では，既存方式とその課題について記述する．BYOD での個人情報保護の方式としては，現在，主として以下の４方式が提案されている．

2.1 業務用の専用環境構築

仮想化技術を利用して，端末内部に業務専用環境（仮想ＯＳ環境等）を構築する方式である．デュアル・ペルソナ方式 [1] とも言われ，個人用と法人用に環境を分離する．業務で使用するメールやアプリケーション，文書や画像などの業務データは個人用の環境からはアクセス不可とすることが可能．さらに細分すると，次の２つのタイプに分けられる．（１）業務用のアプリケーションやデータを一つの「コンテナ」に入れて利用する形式．（２）BIOS およびファームウエアレベルで独自のセキュリティ領域を設け，業務用の領域を安全な形で利用する形式.

2.2 業務アプリケーション毎に制御

MAM(Mobile Application Management)とも呼ばれ，業務アプリケーション毎にアクセス権限を設定し，組織内アプリストアで配信を実現する方式である．

2.3 端末にデータを残さない

業務で使用するアプリケーションデータに関しては，一切端末側にデータを残さない形で利用する方式である．メールも WEB メール方式となり，添付ファイルの閲覧も限定されるため，利便性に欠ける．

2.4 業務用の環境設定を登録

MDM 等の管理ツールで，BYOD 専用のポリシーを設け，個別に運用していく方式．実装負荷が軽く，BYOD の導入には，ハードルが低いが，個人の完全分離が困難.

2.5 既存方式の課題

既存方式は，すべて提供者側の仕様での比較となり，本稿が提案する個人側が設定する仕様とは異なる．

比較すると下記のとおりである．

表２　既存方式の概要と課題[3]

項番	方式	課題
1	業務用専用の環境構築する方式	専用端末となるため，高性能・高価格
2	業務用アプリケーション毎に制御する方式	自社向けアプリストアの構築要で高価格
3	端末にデータを保存しない方式	オフライン利用不可で，利便性に欠く
4	業務用の環境設定を登録する方式	個人の完全分離困難プライバシーの配慮

3. 提案手法の概要

本章では，前章でふれた実装負荷の軽い，2.4 の方式で，個人情報の完全分離とプライバシーの配慮をする為に，本稿の提案する自己情報コントロールの明示的設定手法につき説明する．

3.1 個人情報保護に関する国際動向

EU の「データ保護規則案」や，米国の「消費者プライバシー権利章典」では，個人情報に関する議論が盛んであり，個人情報の活用が，新産業創出に，重要な役割を果たすとされている．[4]

議論の中で，自己情報コントロール権という権利が登場する．まだ法的解釈の結論が出ていないが，権利としては，「自己に関する情報の流れをコントロールする権利」という解釈がなされている．今回は，自己情報コントロール権を実装し，ユーザーが自ら，自己に関する情報を許可，禁止，確認する制御を設定可能とする手法を提案する．

3.2 Android 端末に対する MDM 方式

現在，Android 端末の API として，リモート側から制御可能な MDM の機能は充実していない．このため，MDM 機能の多くの実装は，エージェント型（アプリケーションをデバイス側に導入する方式）となっている．これにより，以下のような機能を実現している．（表中の数字は、1 章でとりあげた個人情報を含む機能）

表 3　MDM で実現可能な代表的な基本的機能[5]

項番	カテゴリ	設定内容
1	設定管理	アプリケーション配信
2		パスワードポリシー
3		位置情報取得(2)
4		リモートワイプ(1)(2)(3)(4)
5		リモートロック
6	セキュリティ	Wi-Fi 機能利用制限
7		カメラ起動の制限
8	資産管理	機器情報の収集
9		アプリケーション一覧の収集(4)
10	運用	ログ管理(3)(4)
11		エージェントの削除対策

実装の状況を図 1 に示す．エージェントアプリケーションが端末制御用の API をコールし，その結果を受け取り，デバイス外部のサーバーとやり取りする．

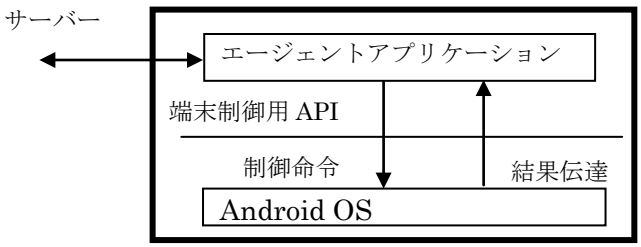

図 1 .MDM における端末制御フロー

3.3 明示的な自己情報コントロール手法

個人用の自己情報コントロールを実現するモジュールをエージェントアプリケーションの外側にライブラリとして実装する．このライブラリでは，使用する独自 API を定義する．実際に端末制御用 API を Android OS に対して実行する際には，ユーザーに対して，許可，禁止，確認の制御を自分で設定可能とする．これにより，端末の所有者である個人側に都合の良い仕様を実現する．今回の実装では，位置情報の取得に関する機能に限定することとする．

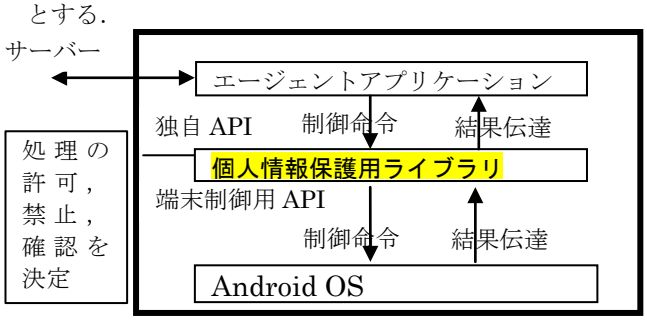

図 2 . MDM における明示的な自己情報コントロール手法の端末制御フロー

4. おわりに

本稿では，BYOD に対応した個人情報保護手法として，明示的な自己情報コントロール手法の実装を提案した．現在，BYOD に対する関心は高く，2 章で示したように数多くの実装方式が提案されている．しかしいずれも，一長一短があり．BYOD の普及には課題が残る．本稿の方式は，端末制御用 API を Android OS に対して実行する際に，ユーザーが制御を自分で設定可能とする手法である．ユーザーおよび組織運営者側ともに納得しやすく，個人情報の完全分離とプライバシーの配慮により BYOD の普及に貢献すると考える．

今後は，具体的な実装および評価を実施してゆく予定である．

参考文献

[1]スマートフォン　プライバシー　イニシアティブ　－利用者情報の適正な取り扱いとリテラシー向上による新時代イノベーション－　総務省　利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会　(2012/8)

[2]MDM 導入・運用検討ガイド　一般社団法人日本スマートフォンセキュリティ協会(JSSEC)技術部会　デバイスワーキンググループ　MDM タスクフォース (2013/1/24 発行)

[3]BYOD 時代のスマートデバイス活用　－企業クライアントの新たな選択肢がもたらす IT 活用の変化－野村総合研究所　情報技術本部　先端 IT イノベーション部　(2013/5/21)

[4]小松文子，佐藤祥太郎，宮澤泰弘，美馬正司　パーソナル情報保護と活用のための調査報告　Computer Security Symposium 2012 (2012/10/30-11/1)

[5]BYOD 時代の戦略ツール MDM 徹底解説　日経ネットワーク（2012/10/25 掲載).

デュアル・ペルソナ方式[1]: Dual persona, in a mobile management context, is the provisioning and maintenance of two separate and independent end user environments on a single mobile device. Typically, the first environment is personal and the second one is for work.