スマート モバイルデバイスのビジネス活用を促進するデバイス保護管理技術

Device Protection and Management Technology Promoting Use of Smart Mobile Devices in Business Environments

池田　竜朗　■IKEDA Tatsuro
森尻　智昭　■MORIJIRI Tomoaki
阿部　真吾　■ABE Shingo

近年，スマートフォンやタブレットに代表されるスマート モバイルデバイスの普及に伴い，ビジネス目的でのこれらの利用が進んでいる。

東芝は，セキュアなAndroid™ (注1) プラットフォームを開発し，ビジネス用途で要求される強固なセキュリティ対策を実現した。東芝ソリューション(株)は，このセキュアなAndroidプラットフォームと連携したデバイス保護管理技術を開発した。この技術により，一般的なモバイルワークに限らず，売場専用デバイスなど様々なビジネスシーンで利用されるタブレットのセキュリティを確保できる。

With the widespread diffusion of smart mobile devices including smartphones and tablets in recent years, the use of such devices in business environments has been rapidly increasing.

To provide enterprise-level security for smart mobile devices, Toshiba has developed a secure Android™ platform. Applying this secure platform, Toshiba Solutions Corporation has developed a device protection and management technology for these mobile devices in order to achieve security not only in normal usages, but also in various business environments including the use of tablets as point-of-sales (POS) terminals.

1　まえがき

近年，スマートフォンやタブレットに代表されるスマート モバイルデバイスの普及が著しく，一般消費者によるそれらの利用に限らず，多くの企業がビジネスでの活用に興味を示している。

特に，米国のGoogle社が開発したAndroidプラットフォームは，アプリケーションを開発するうえでの制約が少なく，開発環境が整備されていることから，スマート モバイルデバイスのビジネス活用における有力なプラットフォームとして期待されている。しかし，Androidプラットフォームは，セキュリティ上の様々な課題が指摘されており，これが本格的なビジネス活用を阻害する要因となっている。

東芝は，このようなセキュリティ上の課題を解決するため，ビジネス用途向けのセキュアなAndroidプラットフォームを開発した[(1), (2)]。このプラットフォームは，Androidの機能を拡張してセキュリティ機能を強化したものであり，ビジネス用途で要求される強固なデバイス制御を実現した。

東芝ソリューション(株)は，このセキュアなAndroidプラットフォームと連携したデバイス保護管理技術を開発した。

ここでは，それぞれの技術の概要と，スマート モバイルデバイスの安全なビジネス活用を実現するセキュリティ ソリューションについて述べる。

(注1)　Androidは，Google Inc.の商標又は登録商標。

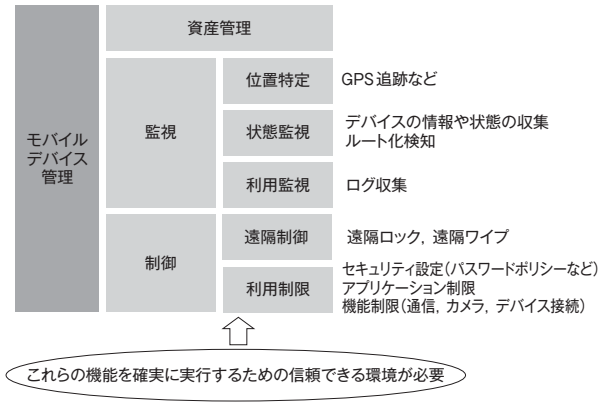


図1. MDMの機能 ― 大きく分けて，資産管理，監視，及び制御の三つの機能がある。
Mobile device management (MDM) functions

2　スマート モバイルデバイスのセキュリティ

スマート モバイルデバイスは，基本的に持ち歩いて利用するものであり，デバイスの紛失や盗難といったリスクをはらんでいる。このため，スマート モバイルデバイスのセキュリティ対策として，モバイルデバイス管理（MDM：Mobile Device Management）が注目されている。一般的なMDMの機能としては，デバイスの情報や状態の収集，紛失・盗難時の遠隔ロックや遠隔ワイプ（データの削除やデバイス初期化），及びGPS（全地球測位システム）追跡などが挙げられる（**図1**）。

最近では，デバイスの監視や制御だけではなく，デバイス及びデバイス上のアプリケーションやコンテンツを資産管理する機能を提供する製品も見られるようになってきた。MDMのこれらの機能は，スマート モバイルデバイスのビジネス活用において重要な役割を担うため，今後も様々な企業で導入が進むことが予想される。一方で，MDMの機能が正しく実行できるかについては，プラットフォームの信頼性に大きく依存するため，MDMの動作環境であるプラットフォームには高い信頼性が求められる。

3　ビジネス用途向けAndroidのセキュリティ技術

Androidプラットフォームでは，端末を管理するためのデバイス管理API（Application Programming Interface）[3]を標準で提供しており，一般的なMDM製品は，このAPIを利用してデバイスの制御を行っている。このAPIは，スクリーンロックのパスワードポリシーや，ストレージの暗号化ポリシー，及び遠隔操作によるデータ削除といったデバイス管理に関する共通的な機能を提供している。しかし，USB（Universal Serial Bus）接続や外部ストレージ接続，アプリケーションのインストール，アンインストール，及び起動や，システムのアップデートなど，オペレーティングシステム（OS）やハードウェア（HW）に関連する制御までは提供されていない。特にUSB接続には，開発者向けオプション機能のUSBデバッグを用いて，多くの情報を抜き出されるリスクがある。このように，ビジネスでの活用を考えたとき，セキュリティ対策としてAndroid標準のデバイス管理APIで提供される管理機能だけでは不十分である。

東芝は，このような課題に対して，ビジネス用途を想定したセキュアなAndroidプラットフォームを開発した。Androidプラットフォームの機能を拡張し，許可しないアプリケーションのインストール，アンインストール，及び起動，SDカードやUSBメモリの接続，Bluetooth®（注2）やWi-Fi®（注3）の利用，並びにアプリケーションごとのTCP/IP（Transmission Control Protocol/Internet Protocol）接続などを，強制的に制御するためのセキュリティ機能を実現している。これにより，ビジネス用途で要求される，より強固なセキュリティ対策が可能になっている。

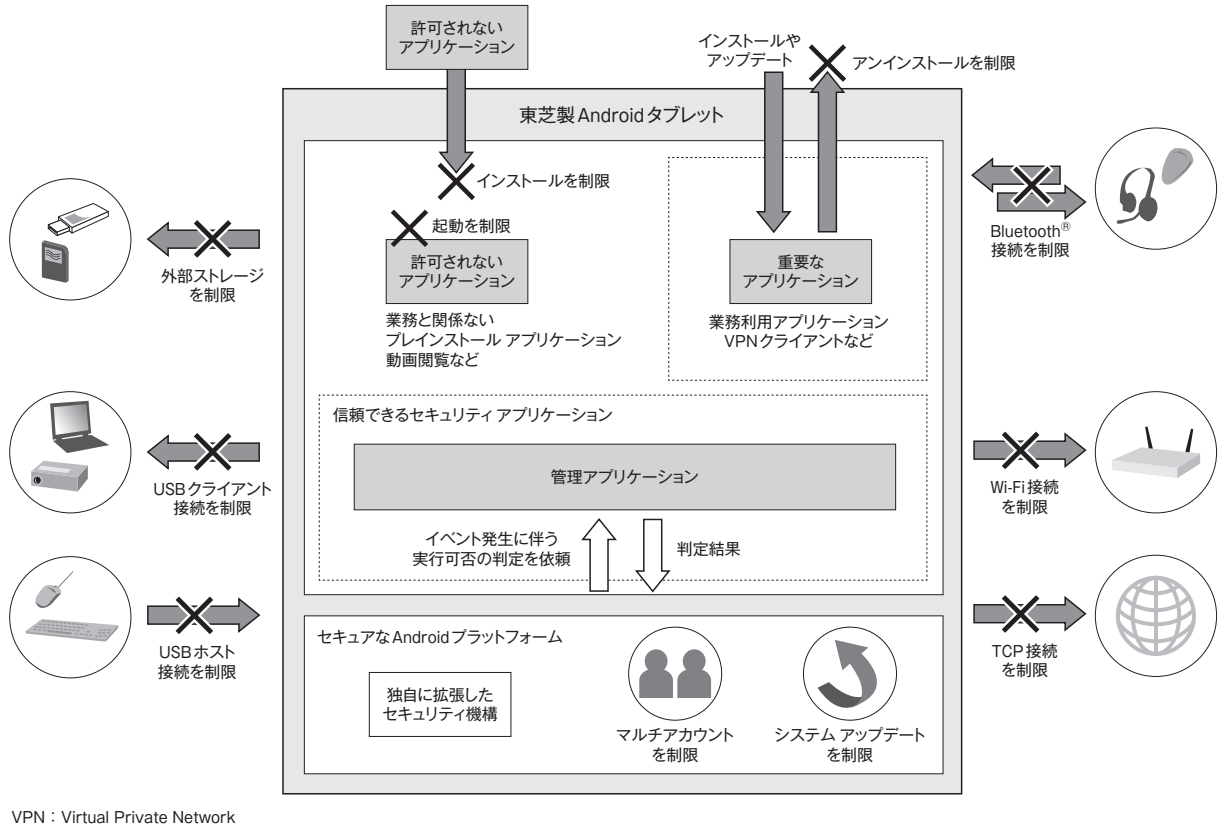


図2．セキュアなAndroidプラットフォームと連携したデバイス保護管理技術 ― セキュアなAndroidプラットフォームをデバイスの保護管理における信頼環境と位置づけ，そこで提供されるセキュリティ機能を制御するための管理アプリケーションである。

Device protection technology cooperating with secure Android platform

（注2）　Bluetooth®ワードマーク及びロゴは，Bluetooth SIG, Inc.の登録商標。
（注3）　Wi-Fiは，Wi-Fi Allianceの登録商標。

4　ビジネス用途向けデバイス保護管理技術

4.1　セキュアなAndroidプラットフォームと連携したデバイス保護管理技術

東芝ソリューション(株)は，3章で述べたセキュアなAndroidプラットフォームと連携し，ビジネス用途のタブレットをターゲットにしたデバイス保護管理技術を開発した(**図2**)。具体的には，セキュアなAndroidプラットフォームを，デバイスの保護管理における信頼環境(Trusted Environment)として位置づけ，そこで提供されるセキュリティ機能を制御するための管理アプリケーションである。

管理アプリケーションの主な役割は，プラットフォーム内で生じる様々なイベント(アプリケーションを起動しようとしているなど)を許可するか否かの判断を行うことにあり，様々なビジネスシーンに応じた複雑な条件を即座に判定することが求められる。そこで，4.2節で述べる，軽量(低い処理コスト)で柔軟なアクセス制御機構が必要になる。

4.2　軽量で柔軟なアクセス制御機構

一概にタブレットをビジネスで活用するといっても，様々な用途や形態が考えられる。例えば，パソコン(PC)の延長としての利用や，特殊な専用デバイスとしての利用などが挙げられる。それぞれのケースで制御したい内容も異なり，また，その判定条件も様々である。より厳密な管理を望むのであれば，「社内で開発した業務アプリケーションは，任意に起動してよい。ただし，重要な承認を行う特定の業務アプリケーションは，業務時間中かつ社内でだけ起動すること」といった，複雑な規則で判定することが求められる。

その反面，複雑な規則で判定しようとすると，頻繁に発生する様々なイベントに対してそのつど判定しなければならず，端末リソースに大きな負荷を生じさせ，イベント実行の遅延を引き起こすおそれがある。

そのため，ビジネスでの活用で求められる複雑な条件で即座に判定するための，軽量で柔軟なアクセス制御機構が必要になる。アクセス制御機構の基本的な考え方には，属性ベースアクセス制御(ABAC：Attribute Based Access Control)モデルを採用した[4](**図3**)。

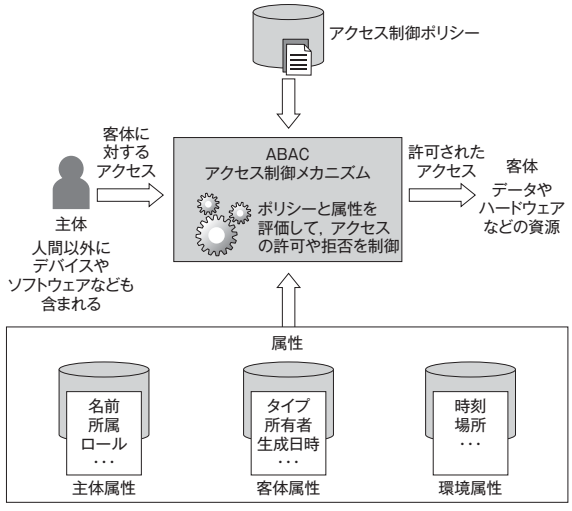


図3．ABACモデルの概念 ― 様々な属性に基づいてアクセスの可否判定を行う。
Basic concept of attribute-based access control (ABAC) model

ABACモデルは，特定のオブジェクトに対するアクセスを制御するために，アクセスする主体の属性(名前や所属など)，アクセス対象となる客体の属性(種類や所有者など)，及びアクセスしている環境の属性(時間や場所など)に基づいて判定するアクセス制御モデルである。ABACモデルを実現するアクセス制御技術としては，産業標準化団体であるOASIS(Organization for the Advancement of Structured Information Standards)で標準化されているXACML(Extensible Access Control Markup Language)[5]が知られている。XACMLは，ABACベースのアクセス制御モデルに基づいたポリシー記述言語を定義しており，高いレベルの拡張性と柔軟性を備えている。このため，Webや機密性の高いデータへのアクセスにおけるアクセス制御機構など，幅広い分野で利用されている。

しかし，XACMLは，その高い拡張性と柔軟性のため，サポートするソフトウェアの処理コスト(ソフトウェアのサイズやメモリ使用量，処理速度)が高くなる傾向がある。これは，タブレットのような限定されたリソースの環境下で，高頻度にポリシーを評価するには適さない。そこで，XACMLをベースにし，タブレット上のソフトウェアで軽量に処理できるポリシー記述言語を設計した。

このポリシー記述言語の特徴は，次のとおりである。

(1)　軽量なデータ記法の採用　　ポリシーを記述するためのデータ記法として，軽量なJSON(JavaScript Object Notation)仕様を採用した。JSONは，様々なソフトウェアやプログラムで，データ交換やデータ記述の記法として広く利用されている。また，Androidプラットフォームでは，JSON処理に関する標準クラス ライブラリが提供されているため，JSONデータを容易に取り扱える。

(2)　省略表現　　XACMLでは，データのタイプや照合アルゴリズムなど，特定の値は必ず明示的に記述する必要があり，ポリシーのデータサイズを増加させる一つの要因となっている。これに対し，全ての構成要素に対してデフォルト値を設定し，省略可能とした。例えば，属性をどのように照合するかを指定する照合アルゴリズムを省略した場合は，文字列完全一致とみなすようにした。

(3)　自動的なルール最適化　　複数のルールを記述したとき，冗長な記述表現を最適化するための機構を組み込んだ。例えば，「“文字列Aと完全一致するか”又は“文字

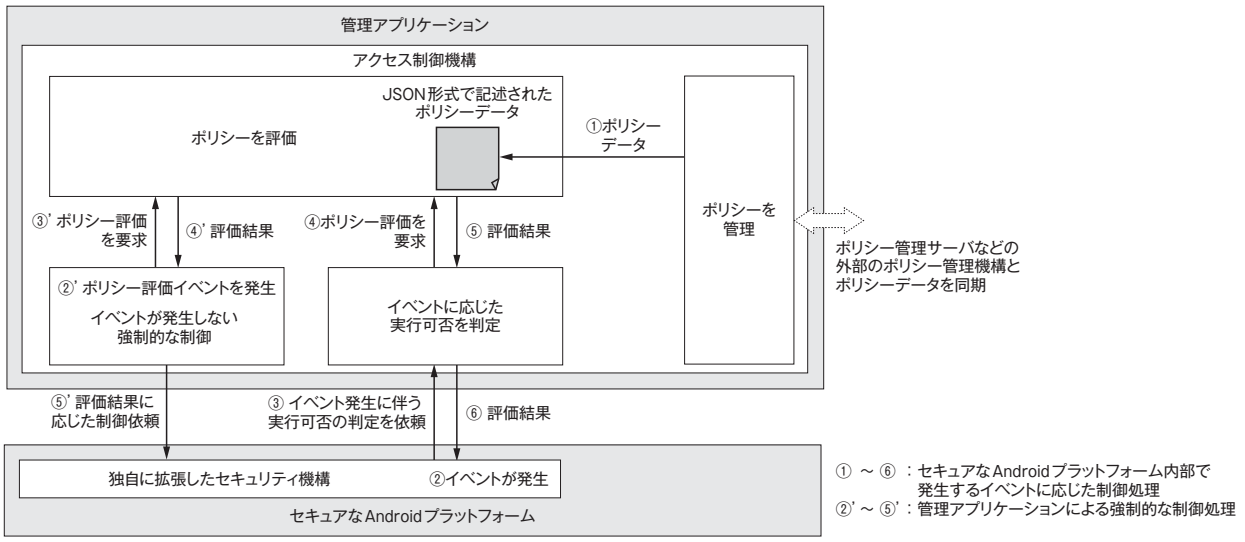


図4．管理アプリケーションのアクセス制御機構 ― ポリシーデータを評価して，セキュアなAndroidプラットフォームのイベントを制御する。
Access control mechanism in management application

列Bと完全一致するか"」という規則（規則1とする）と，「文字列A又は文字列Bと完全一致するか」という規則（規則2とする）があるとする。この二つの規則は，規則の意味としては等価であるが，規則1は二つのルールが結合した形として表現され，規則2に比べて記述が冗長である。このようなケースで，規則1の記述を，論理的に等価な規則2に変換するようにした。ただし，最適化を除外した特殊な例外規則を記述するケースもあるため，この最適化処理を回避する機構も設けている。

前述のポリシー記述言語を用いて，**図4**に示すようなアクセス制御機構を開発した。ここでは，2通りのアクセス制御を実現している。一つは，セキュアなAndroidプラットフォーム内部で発生するイベントに対する制御である。アプリケーションがインストールされたときや，USB接続があったときなど，一般的な制御に用いる。もう一つは，管理アプリケーション内部でイベントを発生させる制御である。強制的にアプリケーションをインストールしたりアンインストールする用途に用いる。

5　ビジネス用途への適用

東芝ソリューション（株）は，このデバイス保護管理技術を用いて，様々なビジネス用途で利用するタブレットのセキュリティを確保するソリューションの開発を進めている。

5.1　モバイルワークへの適用

企業において，社外で業務を行うモバイルデバイスとして，タブレットを利用するケースへの適用が考えられる。タブレットを用いて，社内のネットワークやシステムにアクセスしたり，ローカルのアプリケーションで業務を行うことを想定している。

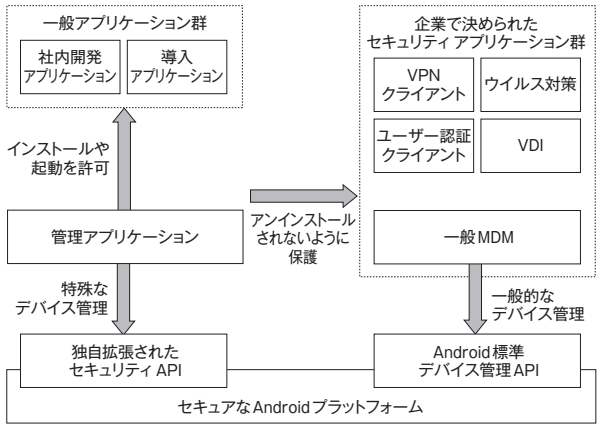
管理されるタブレットは，数十台から数千台といった規模であり，それぞれの部門や用途に応じたポリシーを適用させる必要がある。そのため，一般的なMDM製品と同様に，複数のタブレットを部門や用途に応じたグループとして管理し，管理サーバでポリシーを一元管理する形態とした。管理者は，Web GUI（Graphical User Interface）を通じて，ポリシーの設定やポリシー適用状況の確認などを行うことができる。東芝ソリューション（株）は，開発したデバイス保護管理システムとその他のセキュリティ製品を組み合わせて，モバイルワークでのタブレットの安全な活用を進めており，社内での運用を開始している（**図5**）。

タブレットには，マルウェア対策アプリケーションやVPN（Virtual Private Network）クライアント アプリケーションなど，社内で決められた様々なセキュリティ製品をインストールしている。ユーザーが勝手にこれらのセキュリティ製品をアンインストールできないように，このシステムの管理アプリケーションが制御している。また，Android標準のデバイス管理APIを利用する管理（遠隔ロックや遠隔ワイプなど）については，一般的なMDM製品を利用している。

5.2　専用デバイスへの適用

5.1節で述べた管理サーバの形態では，一元管理する管理サーバの構築が必要になり，小規模な特定業務への利用には向かないケースがある。例えば，店舗における接客用デバイスやサイネージデバイス，及び複数の企業が合同で実施する建設・建築現場での情報デバイスなどが挙げられる。

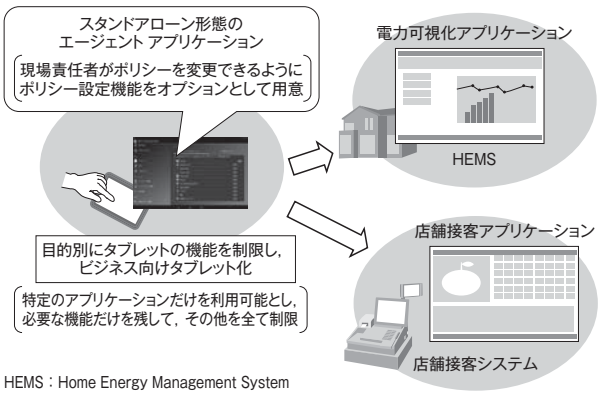
そこで，管理サーバを用いない専用デバイス向けの管理アプリケーションを開発した。この管理アプリケーションは，タブレット上でポリシーの設定を変更できるGUI画面を提供する。



VDI：Virtual Desktop Infrastructure

図5．モバイルワークへの適用 — 様々なセキュリティ製品と組み合わせて，社外でタブレットを活用する際のセキュリティを確保している。

Example of secure mobile working system using tablets



HEMS：Home Energy Management System

図6．専用デバイスへの適用例 — スタンドアローンで運用するビジネス用途で利用されるタブレットのセキュリティを確保する。

Examples of secure special-purpose terminals using tablets

この形態は，監視的な意味合いは薄く，タブレットのセキュリティ強化を目的としている。東芝ソリューション(株)は，この管理アプリケーションを，家庭内エネルギー モニタリングシステムの電力可視化端末や，小売業の店舗接客端末などへ適用することを検討している（**図6**）。

6　あとがき

東芝ソリューション(株)は，東芝が開発したセキュアなAndroidプラットフォームと連携し，様々なビジネスシーンでタブレットを安全に活用するためのデバイス保護管理技術を開発した。

また，このようなセキュリティの仕組みは，スマート モバイルデバイスに限らず，M2M (Machine to Machine) デバイスのようなスマートデバイス全般でも同様に必要になってくると考えられる。今後は，この技術の適用を様々なスマートデバイスの領域に拡大していく。

文　献

(1) 磯崎　宏 他. 不正なWebアプリケーションから端末プラットフォームを保護するセキュリティ技術. 東芝レビュー. **66**, 11, 2011, p.23－26.

(2) 東芝 研究開発センター.“企業向けAndroid™セキュリティ技術”. <http://www.toshiba.co.jp/rdc/rd/fields/12_t14.htm>,（参照 2013-09-17）.

(3) Android Developers. "Device Administration". <http://developer.android.com/intl/ja/guide/topics/admin/device-admin.html>, (accessed 2013-09-17).

(4) NIST SP800-162 (Draft). "Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)". <http://csrc.nist.gov/publications/drafts/800-162/sp800_162_draft.pdf>, (accessed 2013-09-17).

(5) OASIS XACML TC. "eXtensible Access Control Markup Language (XACML) v3.0". <https://www.oasis-open.org/standards#xacmlv3.0>, (accessed 2013-09-17).

池田　竜朗　IKEDA Tatsuro
東芝ソリューション(株) IT研究開発センター 研究開発部主務。情報セキュリティ技術の研究・開発に従事。情報処理学会会員。
Toshiba Solutions Corp.

森尻　智昭　MORIJIRI Tomoaki
東芝ソリューション(株) IT研究開発センター 研究開発部主務。情報セキュリティ技術の研究・開発に従事。情報処理学会会員。
Toshiba Solutions Corp.

阿部　真吾　ABE Shingo
東芝ソリューション(株) IT研究開発センター 研究開発部。情報セキュリティ技術の研究・開発に従事。
Toshiba Solutions Corp.