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

Security Technology to Protect Device Platforms from Malicious Web Applications

磯崎　宏　　金井　遵　　小池　竜一
■ISOZAKI Hiroshi　■KANAI Jun　■KOIKE Ryuiti

近年，アプリケーション実行環境である端末プラットフォームとアプリケーション配布システムを含めたエコシステムとしてAndroid™(注1)プラットフォームが注目されている。Androidプラットフォームには基本的なセキュリティ機能が備わっているものの，端末メーカーの観点からは機能不足の部分もある。特に，プラグインという形で提供される端末固有の拡張機能をWebアプリケーションから利用するアーキテクチャを想定した場合，Webアプリケーションから拡張機能へのアクセスを制限する必要がある。

東芝は，この問題を解決するために，端末拡張機能へのアクセスをWebアプリケーションに応じて制限するアクセス制御技術を開発した。この技術はAndroidプラットフォームをはじめとするWebプラットフォームに容易に導入できるだけでなく，アプリケーション開発者が従来の開発環境を使ってWebアプリケーションを開発することを可能にする。

In recent software development, the Android™ platform has been increasingly attracting attention as a total ecosystem including an application execution platform and an application distribution platform. While the Android platform has basic security features, there are not enough key security features from the viewpoint of device manufacturers. In particular, it is necessary to implement an access control mechanism that restricts access from Web applications to device-specific functions, in consideration of the architecture where Web applications access device-specific functions provided as browser plug-ins.

To solve this issue, Toshiba has developed an access control technology that allows Web applications to control access to device specific functions. This access control mechanism not only makes it possible to easily and effectively introduce existing Web platforms including the Android platform, but also allows application developers to develop Web applications under their existing development environment.

1　まえがき

ユーザーの嗜好（しこう）の多様化に伴い，ユーザー自身が開発者となってアプリケーションを開発，配布し，それをダウンロードして使う利用形態が，スマートフォンやタブレット型端末で一般的になってきている。

これを実現するためのアプリケーション実行環境である端末プラットフォームとアプリケーション配布システムを含めたエコシステムとしてAndroidプラットフォームが注目されている。AndroidプラットフォームはGoogle Inc.がオープンソースとして提供する端末プラットフォームで，端末メーカーが自由に利用できる。また，Androidプラットフォーム向けアプリケーションを配布するためにAndroid Market™(注2)システムが提供されている。このような状況から，Androidプラットフォームは多くのスマートフォンやタブレット型端末に採用され，急速に普及している。しかし，Androidプラットフォームにはセキュリティ上の様々な課題が存在している。

ここでは，AndroidプラットフォームをはじめとするWebプラットフォームにおけるセキュリティ上の課題について説明し，解決策の一例として，Webアプリケーションから端末拡張機能に対してアクセス制御を実現する技術について述べる。

2　Androidプラットフォームにおけるセキュリティ上の課題

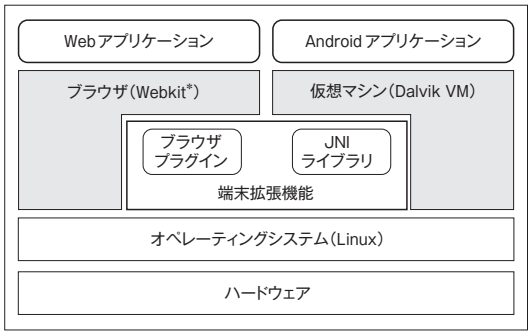
2.1　Androidプラットフォームの概要

Androidプラットフォームとはオペレーティングシステム（Linux(注3)）からミドルウェアやGUI（Graphical User Interface）などのアプリケーションを実行させる一連の実行環境である（**図1**）。

アプリケーション開発者の観点から見ると，Androidプラットフォーム上で実行されるアプリケーションには，ブラウザ上で実行されるWebアプリケーションと，仮想マシン（Dalvik™(注4) VM，VM：Virtual Machine）上で実行されるAndroidアプリケーションの2種類がある。ブラウザや仮想マシンは端末に依存しない標準的な機能をサポートしている。一方，端末固有の拡張機能はブラウザプラグインやJNI（Java™(注5) Native Interface）ライブラリという形で提供され，Webアプリケー

（注1），（注2），（注4），（注7）　Android，Android Market，Dalvik，Google Appsは，Google Inc.の商標又は登録商標。

（注3）　Linuxは，Linus Torvalds氏の米国及びその他の国における登録商標。



*Webブラウザ用のオープンソースソフトウェア

図1. Androidプラットフォームのシステム構成 — Webアプリケーションと Androidアプリケーションの2種類がある。

System architecture of Android platform

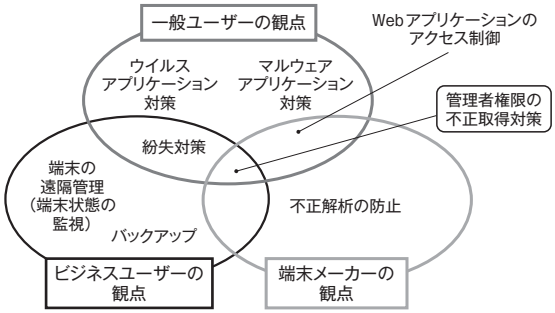


図2. Androidプラットフォームで不足しているセキュリティ機能 — モバイル端末のプラットフォームとしては，端末メーカーの観点から見たセキュリティ機能が不足している。

Security features lacking in Android platform

ションやAndroidアプリケーションは，ブラウザや仮想マシンを介してこれらの端末拡張機能を利用することができる。

また，Webアプリケーションは，HTML 4（HyperText Markup Language 4），HTML5，CSS（Cascading Style Sheets），JavaScript™ (注6)といったインターネットで用いられているWeb技術を使って，従来は端末にインストールして使うスタンドアロンアプリケーションと同等の機能を実現することができる。このため，端末拡張機能として提供される端末固有の機能とインターネットサービスを連携させたアプリケーションの作成に適しているだけでなく，従来のWebサイトの開発者を取り込める利点がある。例えば，チャンネルを選局する機能をブラウザプラグインとして実装すれば，ダウンロードしたWebアプリケーションがその端末機能を利用して放送コンテンツを表示しつつ，その横にインターネットから取得したTwitter（つぶやき）で交わされる情報を表示するようなアプリケーションを容易に記述できるようになる。他にも，他機器に録画されたコンテンツの再生機能をブラウザプラグインとして実現すれば，Webアプリケーションがコンテンツの再生制御を行いつつ，インターネットから取得した他のユーザーのコメントを同時に表示するような機能を実現できるようになると期待できる。

2.2 Androidプラットフォームにおけるセキュリティ上の課題

これまで実現できなかったアプリケーションがAndroidプラットフォームにより実現できるようになると期待される一方で，スマートフォンやタブレット型端末などモバイル端末のプラットフォームとして利用する場合，**図2**に示すようなセキュリティ機能が不足していると考えられる。

2.2.1 一般ユーザーの観点

Android Marketシステムへは開発したアプリケーションを誰でも登録することができる。したがって，悪意のある開発者がユーザーの許諾なしに個人情報などを取得するマルウェアアプリケーションを登録することも可能である。この対策の一つとしてAndroidプラットフォームでは，アプリケーションのインストール時にそのアプリケーションがどのような機能を使うかユーザーに確認を求める仕組みがある。例えば，本来，電話帳を利用する必要のないアプリケーションが電話帳の利用を求めている場合，もしかすると不正に利用者の個人情報を収集するのではないかと疑うことができる。しかし，一般ユーザーに注意深く検査を求めることは現実的ではない。そこで，ウイルス対策ベンダーを中心に，多くのAndroidプラットフォーム向けウイルス対策アプリケーションが提供されつつある。

2.2.2 ビジネスユーザーの観点

スマートフォンやタブレット端末は徐々にビジネスシーンで利用されつつあるが，そのほとんどはWebブラウザとして利用されているにすぎない。Androidプラットフォームを搭載した端末をパソコン（PC）のようにビジネスシーンで本格的に運用していくためには，盗難・紛失対策や，端末に適切なセキュリティポリシーが設定されているかどうかを監視する機能，データのバックアップ機能などが求められると考えられる。

この対策としてウイルス対策ベンダーが中心となって，セキュリティソリューションを提供している。また，Google Inc.も管理者がリモートで端末を操作するためのAPI（Application Programming Interface）やアプリケーションのGoogle Apps™ (注7) Device Policyを提供している。しかし現状では，それらのAPIを利用したアプリケーションが本格的に普及しているわけではない。

2.2.3 端末メーカーの観点

Androidプラットフォームで映画などの有料コンテンツを再生するアプリケーションを実現する場合，コンテンツの著作権を保護する目的で，そのアプリケーションにDRM（Digital Right Management）の機能を実装する必要がある。一般的にDRMでは，コンテンツに暗号を施し，正当なアプリケーションだけが復号できるような仕

(注5)，(注6) Java，JavaScriptは，Oracle又は関連会社の米国及びその他の国における商標又は登録商標。

組みを提供しているため，コンテンツを復号するための暗号ロジックや鍵が不正に解析されたり改変されたりすることを防ぐ必要がある。

また，一般ユーザーと端末メーカー共通の観点として，Webアプリケーションから端末拡張機能へのアクセス制御を行う必要がある。2.1節で述べたように，Webアプリケーションは比較的容易に機器の機能とインターネットサービスを連携させたアプリケーションを記述することができる。このような利点がある一方で，機器に録画した放送コンテンツを勝手に削除するような，不正なWebアプリケーションが配布，実行されるおそれがある。Androidアプリケーションの場合には，インテントと呼ばれるプロセス間通信の仕組みによりアプリケーション間の呼出しを制限することが可能であるが，Webアプリケーションの場合には同等の機能がない。したがって，Webアプリケーションに応じて端末拡張機能へのアクセスを制限するアクセス制御技術が求められる。

このように，Androidプラットフォームでは，特に端末メーカーの観点から見た場合に不足しているセキュリティ機能がある。3章では，当社が開発したWebアプリケーションから端末拡張機能に対してアクセス制御を実現する技術について述べる。

3　端末拡張機能へのアクセス制御技術

3.1　要求事項

端末拡張機能へのアクセス制御を実現するには，特定のWebアプリケーションだけに端末拡張機能へのアクセスを許可するシステムを実現する必要がある。しかし，Webアプリケーションの開発を一般に公開することを考えると，Webアプリケーション開発者と端末拡張機能の開発者は異なるため，Webアプリケーションや端末拡張機能の開発ライフサイクルまでを含めた，以下に述べる要求条件を満たす必要がある。

(1)　端末拡張機能の開発者が認めたWebアプリケーションに限り拡張機能の利用を許可できるようにする。
(2)　Webアプリケーション単位で端末拡張機能へのアクセス制御ができる。
(3)　端末拡張機能を呼び出すWebアプリケーションを開発する場合，通常のプラグイン呼出しと同様の手続きでWebアプリケーションを構築できる。
(4)　端末拡張機能の呼出しを行わない一般のWebアプリケーションを開発する場合，その開発者に追加的な負担をかけない。
(5)　端末拡張機能の開発者は一般の開発と同様のスタイルで拡張機能を開発できる。

3.2　全体アーキテクチャ

端末拡張機能へのアクセス制御は端末内で実行されるが，その機能を説明する前に，まず，Webアプリケーション開発者がWebアプリケーションの開発をスタートしてから端末上でWebアプリケーションが実行されるまでの流れについて，**図3**を用いて説明する。

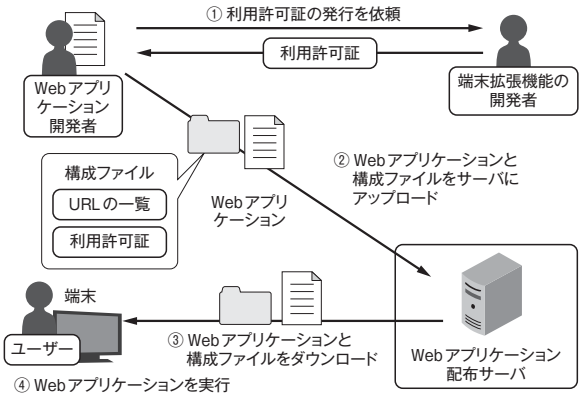


図3．Webアプリケーション配布までの流れ ― Webアプリケーションと構成ファイルが端末にダウンロードされる。
Information flow from application development to application distribution

(1)　Webアプリケーション開発者はWebアプリケーションの配布に先立ち，端末拡張機能の開発者から端末拡張機能の利用許可証を取得する。利用許可証には，Webアプリケーション固有のID（Identification），及びどの端末拡張機能の利用が許可されているかを示すポリシー情報が含まれる。
(2)　Webアプリケーション開発者は開発したWebアプリケーションに構成ファイルを添付してWebサーバにアップロードする。構成ファイルには，Webアプリケーションに含まれるURL（ファイル位置）の一覧，及び端末拡張機能の開発者から取得した利用許可証が含まれる。
(3)　端末のユーザーがWebアプリケーションと構成ファイルをダウンロードする。
(4)　端末内でWebアプリケーションを実行する。端末内の動作については次節で述べる。

3.3　端末内のアクセス制御機構

端末は，Webアプリケーション配布サーバからWebアプリケーションと構成ファイルをダウンロード（3.2節(3)）して，**図4**に示すように，構成ファイルに含まれる利用許可証の内容に従ってアクセス制御を行う。

まず，Webアプリケーションと構成ファイルがダウンロードされると，端末内のアクセス制御機構はWebアプリケーションが起動したことを検出し，そのWebアプリケーションに対応した構成ファイルの中から利用許可証を読み込む（①）。Webアプリケーションが実行される過程で端末拡張機能が呼び出されると，アクセス制御機構はその呼出しを検出してアプリケーションを特定し（②，③），利用許可証で許可された呼出しかどうかを判定する（④）。利用許可証に記載された呼出しであ

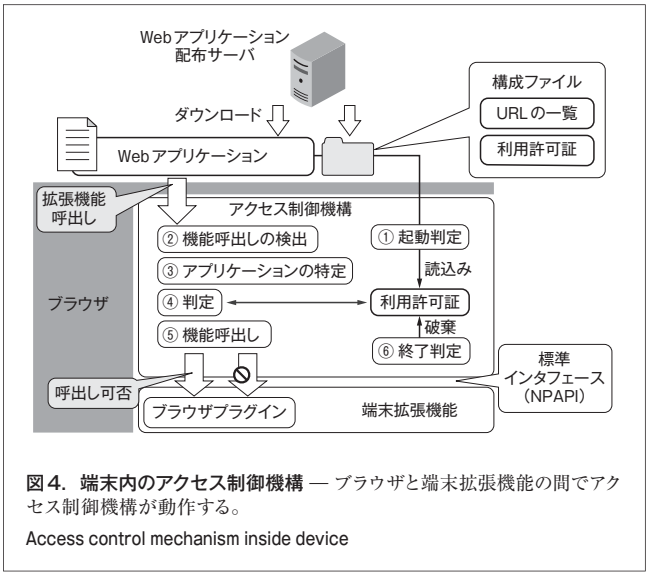


図4．端末内のアクセス制御機構 ― ブラウザと端末拡張機能の間でアクセス制御機構が動作する。
Access control mechanism inside device

れば端末拡張機能を呼び出し，記載されていなければエラーを返す（⑤）。Webアプリケーションが終了すると利用許可証を破棄する（⑥）。

ここで考慮しなければならない点は，端末内で様々なWebアプリケーションが実行されることである。例えば，Webアプリケーションの中には，録画など端末固有の機能を呼び出すWebアプリケーションAを端末メーカーが作成し広告部分のWebアプリケーションBを広告主が作成して，それを一つの画面で同時に実行する場合がある。このとき，アクセス制御機構は構成ファイルの利用許可証に記載されたポリシー情報を適用してWebアプリケーションごとに端末拡張機能へのアクセス制御を行う必要がある。また，連続して異なるWebアプリケーションを実行する場合もあり，あるWebアプリケーションの終了後，別のWebアプリケーションが起動した場合には，アクセス制御に利用するポリシー情報も更新しなければならない。アクセス制御機構では，URLの遷移を自動的に検出し，Webアプリケーションの開始と終了を判定してWebアプリケーションに応じた利用許可証の読込みを行うことでこの問題を解決している（要求事項(1)，(2)の解決）。

アクセス制御機構は，図4に示すように，ブラウザと端末拡張機能の間に挿入され，Webアプリケーションがブラウザプラグインの API を呼び出す際に透過的にアクセス制御の処理を行っている。すなわち，Webアプリケーションからはあたかも端末拡張機能を直接呼び出しているように見えるため，Webアプリケーションは通常のブラウザプラグインを呼び出すのと同じ手続きで端末拡張機能を呼び出すことができる。これにより，アクセス制御機構に専用のAPIを定義することなく，開発者は通常の手続きでWebアプリケーションを開発することができる（要求事項(3)，(4)の解決）。

また，アクセス制御機構と端末拡張機能のインタフェースにNPAPI（Netscape Plugin Application Programming Interface）と呼ばれるブラウザとプラグインの標準インタフェースを用いることで，端末拡張機能の開発者がアクセス制御を意識せずに拡張機能が開発できるような仕組みを提供している。（要求事項(5)の解決）。

4　あとがき

スマートフォンやタブレット型端末では，Androidプラットフォームの採用が今後も進むと予想される。ここでは，Androidプラットフォームのセキュリティ上の課題を一般ユーザー，ビジネスユーザー，及び端末メーカーそれぞれの観点から分析した。そして，Androidプラットフォームを搭載した端末のアプリケーション実行環境としてブラウザを用いる場合，不正なWebアプリケーションの実行を防止するためには，Webアプリケーションから端末拡張機能へのアクセス制御機能が必要であることを示し，その解決策として当社が開発した端末拡張機能へのアクセス制御技術について述べた。

今後は，ユーザーが開発したアプリケーションとDRM機能など秘密情報を扱うアプリケーションが端末内で共存する場合を想定し，秘密情報を扱うアプリケーションをユーザーが不正に解析することを防止する技術が必要になると考えられる。このため，Androidプラットフォームのようなオープンプラットフォームにおいて，端末内のソフトウェアモジュールの不正解析を防止したり，プラットフォームの改変を防止したりする技術の開発を進める必要がある。

文　献

(1) ANDROID developers. "What is Android?". <http://developer.android.com/guide/basics/what-is-android.html>, (accessed 2011-09-07).
(2) スマートフォン活用セキュリティガイドライン策定WG. “スマートフォンの安全な利活用のすすめ～スマートフォン利用ガイドライン”. <http://www.jnsa.org/result/2010/smap_guideline_Beta.pdf.>,（参照2011-09-07）.


磯崎　　宏　ISOZAKI Hiroshi
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー研究主務。ホームネットワーク及びセキュリティ技術に関する研究・開発に従事。
Computer Architecture & Security Systems Lab.


金井　　遵　KANAI Jun, D.Eng.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー，博士（工学）。IPTV配信及びプラットフォームセキュリティ技術に関する研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer Architecture & Security Systems Lab.


小池　竜一　KOIKE Ryuiti, D.Eng.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー，博士（工学）。P2Pコンテンツ配信及びプラットフォームセキュリティ技術に関する研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer Architecture & Security Systems Lab.