# スマートフォンのセキュリティ技術

## Security Technologies for Smartphones

● 阿部保彦　● 池田　仁　● 江村真史

**あらまし**

スマートフォンはサービス機能実現のため，個人情報，ネットワーク事業者情報，企業情報などが格納されている。これらスマートフォンの多くはオープンOSを採用しており，誰でもソースコードなどの情報を入手可能であり，悪意を持った人々による不正情報取得の脅威にさらされている。このような脅威に対し，富士通はSecure Boot，Linux Security Module，TrustZone™などの複数技術を用いて情報の保護を行い，安全なスマートフォンを提供する。

Secure Bootはスマートフォン起動プログラムの書換えを検出し，第三者による改造プログラムの起動を不可能にして事業者情報の保護を行う技術である。Linux Security Moduleは，工場出荷後にインストールされたプログラムによる情報アクセスを制御し，不正な情報アクセスを禁止して個人情報漏えいを防止する技術である。TrustZoneはハードウェアでプログラム動作環境を分離し，オープンOS上のプログラムからの不正情報アクセスを防止してバンキングサービスの安全性を担保する技術である。

本稿では，Secure Boot，Linux Security Module，TrustZoneのそれぞれの技術を紹介する。

**Abstract**

Smartphones contain personal information, network operator information, and often contain company information. Most smartphones adopt an open-source OS and anyone can refer to its source codes, so it may be possible to maliciously and illegally acquire such information. Fujitsu protects this information with multiple technologies such as Secure Boot, Linux Security Module, and TrustZone™ to ensure smartphones are safe. Secure Boot is a technology to detect whether a boot program of a smartphone has been changed and make it impossible for a boot program that a third party has changed to start up. It also protects network operator information. Linux Security Module controls access to information by any program installed after factory shipment, stops unauthorized access to information and prevents personal information leaks. TrustZone separates program operating environments with hardware and is a technology to prevent unauthorized access to information by any program on open-source OS. It also ensures online banking services carried out on a smartphone are safe. This paper introduces each of the technologies of Secure Boot, Linux Security Module, TrustZone.

## ま え が き

スマートフォンのセキュリティ技術という言葉からどのようなことが連想されるだろうか。暗証番号を用いた端末ロック，あるいは，指紋認証などの生体認証技術，それともアンチウイルス技術だろうか。セキュリティ技術を考えるため，スマートフォンがどう使われているか考えることにする。

まず，目覚まし代わりのアラームで目覚め，新着メールの確認，週末旅行のチケットをクレジット決済，出勤時電車利用でモバイルSuica，車内では電子版新聞を携帯アプリケーションで読み，もしくはゲームをしているうちに会社に到着する。外出時，ナビアプリケーションを使って効率良く移動し，昼に弁当をおサイフケータイで購入する。外出先から社内メールサーバに接続，上司に報告し指示を確認する。帰宅後，欲しかった商品をネットで購入する。こんな使われ方がされているのではないだろうか。

これらができるのは，端末内の個人情報（アドレス帳，アプリケーション購入情報，位置情報，クレジット情報など），事業者情報（電話番号など），企業情報（社内サーバアクセス情報）を利用しているからである。もし，これらの情報を他人が利用したらどうなるだろうか。経済的損失，社会的信用消失を被るかもしれない。紛失しても端末ロックを設定しているから大丈夫と判断していないだろうか。富士通をはじめとする多くのメーカのスマートフォンは従来の携帯電話とは違い技術情報が公開されているオープンOSを採用しており，端末プログラムを書き換えたり，ロック解除アプリケーションを入れたりすることが可能で，これらの情報が利用できてしまう。更に，ユーザが認識できずに情報が流出する可能性もある。

本稿では，重要な情報の流出・不正使用を防ぐため，富士通製スマートフォンが実装しているセキュリティ技術を紹介する。

## セキュリティ技術の概要

（1）Secure Boot

オープンOSを採用する機器は，ユーザがそのOSを入手し改造プログラムを作成，機器に書き込むことも可能であり，悪意を持ったユーザが不正取得したスマートフォンに改造プログラムを書いて各種情報を取り出すことも考えられる。富士通はこの脅威に対し後述するSecure Boot技術を用いてOSおよびファームウェアのIntegrity（正当性）を担保する。端末起動時，プログラムの正当性を検証する技術であり，改造プログラムによる起動を停止させ情報を保護する。

（2）Linux Security Module

スマートフォンはユーザがアプリケーションを購入しインストールして使うことができる。従来の携帯電話とは違い一般ユーザがアプリケーションを作成し，厳正な審査を受けることなくアプリケーションマーケットへ登録し，ほかのユーザがそれを購入しインストールすることも可能である。富士通は，これらアプリケーションが不正にデータ取得をできないよう，アプリケーションが使用するAPI（Application Programming Interface）の動作を制限するLinux Security Module（以下，LSM）技術を用いて情報を保護する。LSM技術はAPIアクセスプログラムを判断し，API動作を制御する。

（3）TrustZone™(注)

更に，オープンOS動作環境とハード的に分離された環境で処理を行うTrustZone技術を実装し，不正プログラムなどから情報を保護する。

富士通製スマートフォンは上記以外にもセキュアストレージ，改ざん検出などいろいろな技術を実装し重要な情報を保護するが，本稿では上記セキュリティ技術について紹介する。

## Secure Boot

スマートフォンでは，端末出荷時のソフトウェアが改変されていないことが要求される。アンチウイルスソフトによるマルウェアからの防御や，LSMによる不正アクセスの防御をいくら施したとしても，ソフトウェアを改変することによって，これら実行時のセキュリティ機能を無効化し，端末を無防備な状態にされる可能性があるからである。Secure Bootは，デジタル署名の仕組みを用いてソフトウェアが改変されていないことを検証し，不正なソフトウェアが実行されることを防ぐ技術

（注）　TrustZoneは，ARM Ltd.の商標です。

である。

デジタル署名は，デジタルデータの作成者と利用者との間でやり取りするデータが改ざんされていないことを確認するために利用されており，公開鍵暗号方式とハッシュの技術を組み合わせて実現されている。

Secure Bootでは一般的に，開発によって生成されたソフトウェア（プログラムイメージ）に対するデジタル署名データを生成し，その署名データも端末に書き込む。また，起動時に実行されるプログラム（ブートローダ）に，署名を検証する処理を実装する。ブートローダがプログラムイメージを読み込む際，デジタル署名を検証する処理が実行されることで，プログラムイメージの正当性を保証する。

Androidを搭載するスマートフォンでは，OSとしてLinuxカーネルが用いられており，電源投入後，複数のブートローダを経てAndroidシステムが起動される構成となっていることが多い（**図-1**）。第1ブートローダのイメージはROM内に存在し，書き換えられないプログラムとなっている。第2ブートローダとLinuxカーネルに対して署名を生成し，第2ブートローダのイメージ検証を第1ブートローダが実行し，Linuxカーネルイメージの検証を第2ブートローダが実行する。

### ● 署名作成の手順

署名の作成者は，あらかじめ秘密鍵と公開鍵を生成しておく。

対象とするプログラムイメージからハッシュ関数を使って，ハッシュ値（メッセージダイジェスト）を生成する。

次に，署名の作成者は，秘密鍵を使ってメッセージダイジェストを暗号化する。この暗号化されたメッセージダイジェストが電子署名となる。そして，プログラムイメージと電子署名を端末の内部メモリに書き込む（**図-2**）。

なお，公開鍵は，書換えが不可能な領域にあらかじめ搭載しておく必要がある。公開鍵自体が書き換えられてしまうと，署名検証の信頼性が無効になってしまうためである。各データが端末の内部メモリに配置された例を**図-3**に示す。

### ● 署名検証の手順

端末の電源が投入されるとROMに格納された第1ブートローダが実行される。第1ブートローダはFlashストレージから第2ブートローダのイメージをメモリ上に読み込み，更に，電子署名と公開鍵を取得する。

第1ブートローダは，第2ブートローダイメージのハッシュ値を計算し，公開鍵で復号化した電子

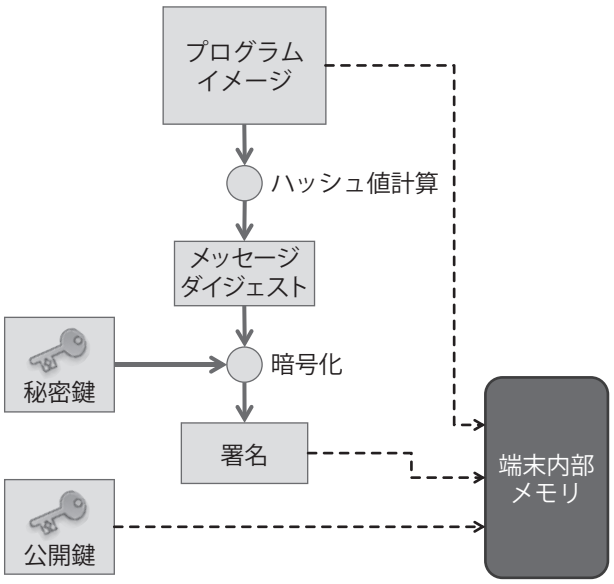



図-2　署名作成処理

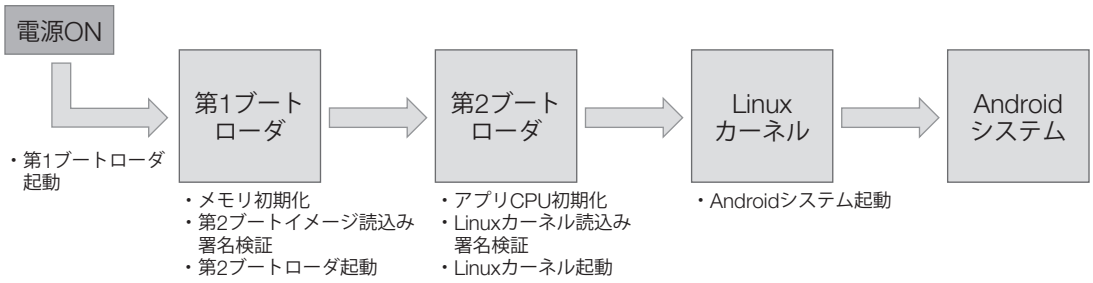
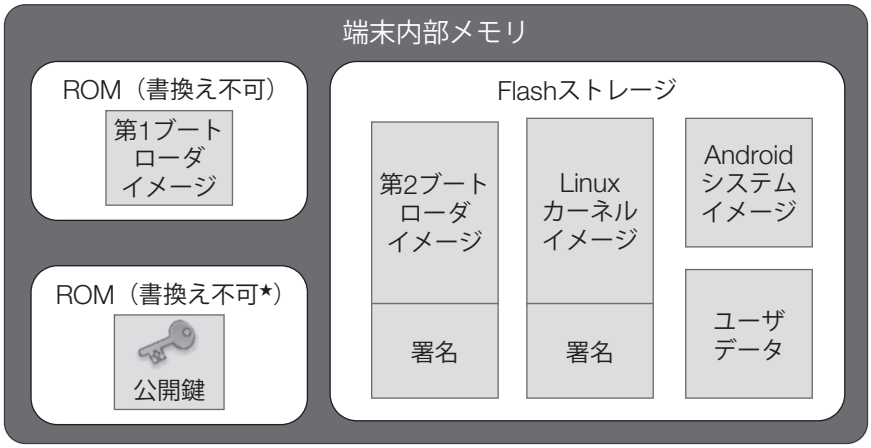



図-1　システムの構成例




★：公開鍵は，ROM製造時に書込みを行わず，一度だけ書換え可能なROMに保存されることもある。

図-3　端末内部メモリのデータ配置(例)

署名内のメッセージダイジェストと比較する。両者が一致すれば，内部メモリから読み込まれたイメージは書き換えられていないことが確認でき，第2ブートローダに制御を移す。もし一致しなければイメージが書き換えられたと判断し，起動処理を中断する。Linuxカーネルの検証も同様に実行される。この起動処理を**図-4**に示す。

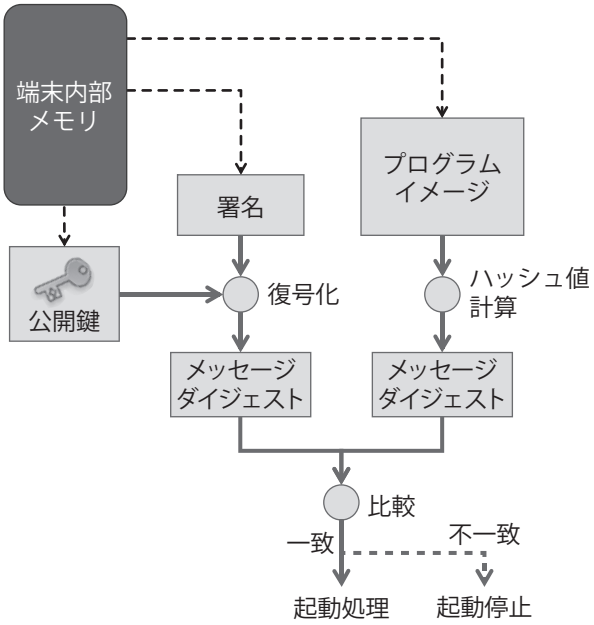



図-4　署名検証処理

### ●　署名作業の運用ルール

秘密鍵が漏えいしてしまった場合，第三者による署名データの作成が可能となってしまう。漏えいのリスクを軽減させるため，開発者と署名作成の担当者を分け，署名作成作業を隔離された部屋や設備で実施するなどの運用ルールが必要である。富士通では，署名作業の運用ルールを取り決めることによって，安全な端末の開発に取り組んでいる。

## Linux Security Module（LSM）

LSMは，Linuxカーネルバージョン2.6から導入されたカーネルに対するセキュリティ機能を拡張するためのフレームワークである。LSMはカーネル内の様々なシステムコールに対し，開発者が登録したセキュリティモジュールへのコールバック関数の呼出しを行うことができる。開発者が登録するセキュリティモジュールでは，開発者のセキュリティポリシーに従いセキュリティチェック機能を実装し，復帰値を設定することで，システムコール実行のアクセス制御をユーザ独自に行うことを可能としている。LSMの機能構成を**図-5**に示す。

富士通のスマートフォンにおいては，root権限が取得された場合でも，LSMによりシステムの改ざんができないようにすることを目的として，セキュリティモジュールを組み込んでいる。

ここでは，そのいくつかについて紹介する。

### ●　メインディスクの改ざん抑止

メインディスクのデバイスファイルに対して，write，pwriteなどの書込みを行うシステムコールをリストで管理することで，io_submit，fallocate，link，renameなどのシステムコールによるアクセスを禁止する。ただし，システムイメージファイ

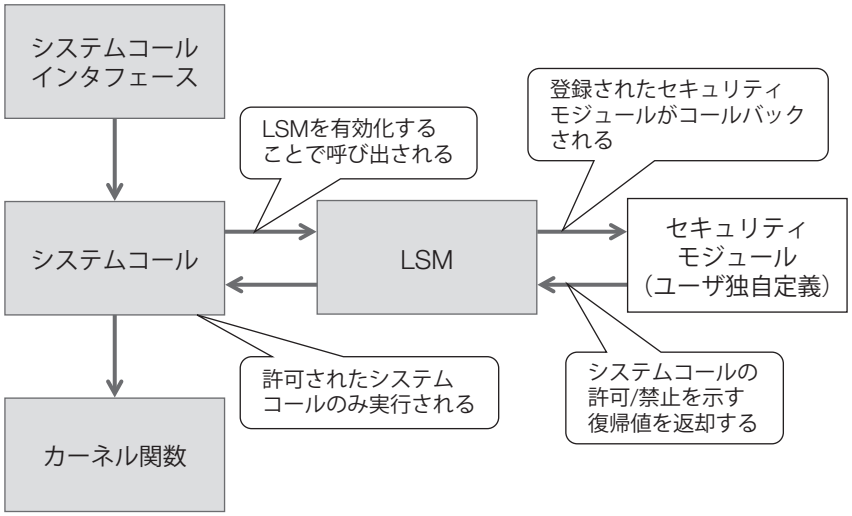



図-5　LSMの機能構成

ルの更新を行うFOTA（Firmware Over The Air）などにおいては，このメインディスクの改ざん抑止機能で書込みを抑止してしまうと不都合が生じる。よって，特定の条件を満たす場合は，メインディスクへの書込みアクセスを許可するようにしている。

● **そのほかの制御**

(1) カーネルモジュール追加の制限

インストールできるカーネルモジュールを制限し，あらかじめ決められたカーネルモジュール以外の追加を禁止する。制御方法としては，insmodコマンドから呼ばれるinit_module()システムコールのフック処理からセキュリティモジュールを呼び出す。本セキュリティモジュールは，追加を許可するカーネルモジュール名および該当カーネルモジュール改ざん検出用の情報を登録し，登録されていないもしくは改ざんされたカーネルモジュールの追加を抑止する。

(2) デバイスファイルの所有者と権限を制限

/dev配下にあるデバイスファイルごとに，あらかじめ所有者と権限を決めておき，デバイスファイルへの所有者変更および権限変更処理を禁止する。

(3) マウントの制限およびマウントポイントの固定

読み書き可能でのmount，remountとumountを禁止し，特定のマウントポイント配下での改ざんおよびアクセスを抑止する。またマウントポイントを特定のパスに固定する。

(4) ルートファイルシステムの変更を抑止

chroot，pivot，rootシステムコールによるルートファイルシステムの変更を禁止することで，ユーザランドの変更を抑止するようにしている。

(5) コピー制御

各システムコールのフック箇所で，ファイルおよびディレクトリへの読込み/書込みアクセスを禁止することで，ファイルのコピーを防止する。全てのプロセスからのアクセスを禁止すると，ファイルおよびディレクトリが通常使用できなくなるため，特定のプロセスからのみアクセスを許可するようにしている。

## TrustZone

スマートフォンで使用しているCPUは逐次処理型と呼ばれる**図-6**に示す構成をとった処理装置である。動作原理は，実行位置を示すプログラムカウンタに従い命令コードを取り込み，命令コードを制御装置に送り込み，命令に従いデータを演算レジスタ（アキュムレータ）にセットし演算装置で処理し結果をアキュムレータに出力し，それをメモリに戻す。演算結果（0，桁あふれ，マイナスなど）によりCPUの状態を示すステータスレジスタの該当bitが設定され制御装置がこれを参照し次に実行する命令を決める。この繰返しにより複雑な処理を実現する。

リアルタイム性を要求されるシステムでは割込みなどの発生時，それまで実行していた逐次処理

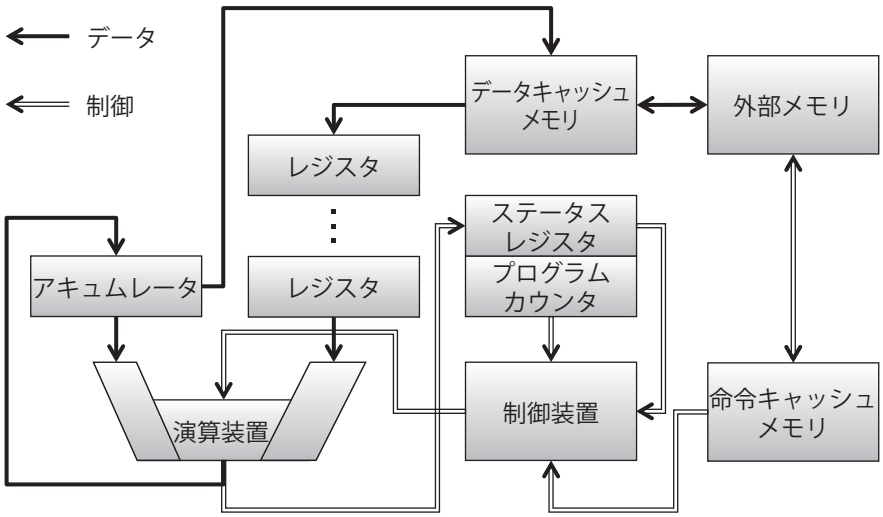



図-6　CPU内論理構成

を停止し割込み要因ごとに決められた処理を即時に実行する。このとき，図-6に示すレジスタ群を待避して割込み発生前の状態を保持し，割込み先頭へJumpし処理を行う。割込み処理終了時，待避していたレジスタ群を復旧させ割込み前実行中の処理に復帰する。TrustZoneは，この割込み動作に相当する動作をソフトウェア的に発生させ，割込みとは違う新たな動作空間を作り出す技術である。TrustZoneはARM Ltd.のv6アーキテクチャから実装されたハードウェア技術であり，MMU（Memory Management Unit）などでハードウェアリソースアクセス制御を行いメモリ，各種ハードウェアリソースに対して，TrustZone，非TrustZone上の処理のアクセスを制御し，リソースの分離，保護を行う。この技術を用いてオープンOSを非TrustZoneに，重要なデータにアクセスする信頼された処理をTrustZoneに配置し，オープンOS上の処理から重要なデータ，ハードウェアリソースへのアクセスを禁止し情報の保護を行う。例えば，暗復号処理ハードウェアアクセラレータなどをTrustZoneエリアからのみ使用可能とすることで復号処理を制限し，不正なアプリケーションが復号できないようにすることでコンテンツ保護を行うDRM（Digital Rights Management）を実現する。

## む　す　び

スマートフォンは個人情報，企業情報やPCにはないネットワーク事業社情報が入っている。オープンOSは多くの人の努力により日々品質向上が図られる一方，悪意を持った人にもソフトウェアが公開されており，これを採用するスマートフォンには情報流出，不正使用などのリスクが存在する。このため，情報を守る技術が必要になり，いろいろな技術が開発されてきた。富士通は，今回紹介した不正ソフト混入防止技術「Secure Boot」，不正アプリケーションによる情報取得防止技術「LSM」，および動作空間の分離技術「TrustZone」による情報の保護を行って，ユーザに安全なスマートフォンを提供する。しかし，悪意のある人々が情報不正入手方法を進化させており，セキュリティ技術の更なる進化が必須である。また，オープンOSのぜい弱性も相次いで発見されており，不正技術に対抗するためぜい弱性の改善も重要である。富士通は，オープンOSのぜい弱性に対処しつつ，セキュリティ技術を発展させ，それを実装し，安全なスマートフォンを開発し今後も継続的に社会に貢献していく。

## 著者紹介


**阿部保彦**（あべ　やすひこ）
モバイルフォン事業本部スマートフォンコア開発統括部 所属
現在，スマートフォン開発に従事。

**江村真史**（えむら　まさふみ）
モバイルフォン事業本部スマートフォンコア開発統括部 所属
現在，スマートフォン開発に従事。

**池田　仁**（いけだ　ひとし）
モバイルフォン事業本部スマートフォンコア開発統括部 所属
現在，スマートフォン開発に従事。