端末 アーキテクチャ OSTI

Collaboration Projects

オープンで安全な移動端末を目指すOSTI技術

オープンで安全な移動端末を実現するために端末アーキテクチャ仕様書であるOSTI仕様書を策定した．これにより，企業やシステムインテグレータが自由にアプリケーションを選び，移動端末にインストールできることを目指す．なお，本研究はIntel Corporationとの共同研究により実施した．

中山 雄大（なかやま たけひろ） 太田 賢（おおた けん）
竹下 敦（たけした あつし）

1. まえがき

既存のアプリケーションソフトウェアを移動端末で自由に利用したいというニーズにこたえるために，ドコモは，DoCoMo Communications Laboratories USAおよびIntel Corporationと共同でOSTI（Open & Secure Terminal Initiative）仕様書[1]を策定した．従来，企業や個人が自由に開発したネイティブアプリケーション*1などの任意のソフトウェアを移動端末で利用する場合，従来の移動端末と同等の信頼性や安全性を確保することが困難であった．しかし，筆者らは移動端末上のソフトウェアを実行する環境（以下，ドメイン）を複数に分離させるマルチドメインアーキテクチャを採用することにより，この課題の解決を図った．マルチドメインアーキテクチャを検討するにあたり，ハードウェアに関する深い知識を持った，Intel Corporationと共同研究を行うこととした．

サーバやPCを対象とするマルチドメインアーキテクチャはすでに技術的に成熟しつつあるが，移動端末を対象とする場合は，どのドメインを使用中であっても電話として一貫性のあるサービスを維持させるために移動端末特有の考慮が必要となる．OSTI仕様書では，各ドメインに割り当てられる周辺デバイス（キーパッド，ディスプレイ，スピーカ，マイクなど）を適切に切り替える機構，ドメイン間の通信機構および着呼などのイベントに応じた割込み機構を規定することにより，移動端末として一貫性のあるサービス維持を可能にした．

本稿では，まず，OSTIのマルチドメインアーキテクチャ概要とその特徴を述べる．次に，OSTI仕様でマルチドメインアーキテクチャを実現するための下位層の実装技術として例示されている2つの方式，OSスイッチ方式と仮想マシンモニタ方式について，それぞれOSTI仕様書の規定を概説し，最後に，今後の方向性について述べる．

2. マルチドメインアーキテクチャ

2.1 マルチドメインアーキテクチャ概要

OSTIアーキテクチャは図1に示すように，アプリケーションユニット*2において，既存の法人アプリケーションやブラウザなどを自由に利用することができるエンタープライズドメインと，従来の通話やメールなどのオペレータサービスを提供するオペレータドメインの2つのドメインをサポートしている．各ドメインはそれぞれ異なるOS，GUI（Graphical User Interface），セキュリティポリシーを持つことができる．

OSTI仕様は，エンタープライズドメインと端末プラットフォーム本体との間のインタフェースをドメイン抽象化レイヤとして規定している．ドメイン抽象化レイヤについて，OSTI仕様では実装の柔軟性を持たせるため，特定の実装技術を規定していない．OSスイッチ方式と仮想マシンモニタ方式の2つを下位の実装技術例として，抽象化されたインタフェースを規定している．OSスイッチ方式は，多くのOSが備えるサスペンド・レジューム機能を利用して2つのOSを排他的に切り替えて動作させるのに対し，仮想マシンモニタ方式はCPU，メモリ，周辺デバイスなどを仮想化して2つのOSを並行して動作させるという違いがあ

＊1 **ネイティブアプリケーション**：汎用OS上で直接実行されるアプリケーションソフトウェア．iアプリは，Java™仮想マシン上で実行されるのでネイティブアプリケーションではない（Javaは米国Sun Microsystems, Inc.の商標）．

＊2 **アプリケーションユニット**：多くの移動端末において通信部分の制御を行うC-CPU（Communication CPU）とアプリケーション部分の制御を行うA-CPU（Application CPU）の2つのCPUを搭載するアーキテクチャが採用されている．アプリケーションユニットはこのうちA-CPUが制御する部分を指す．

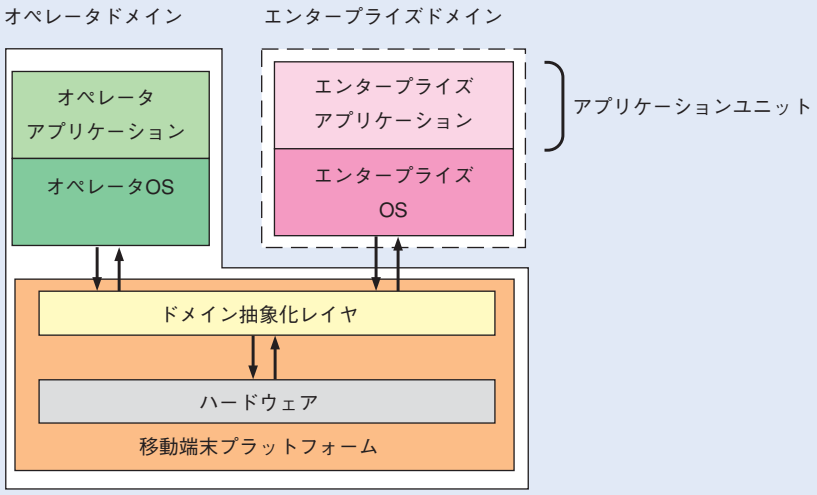

図1　OSTIアーキテクチャ

る．OSTI仕様におけるドメイン抽象化レイヤのねらいは，その差異を小さくすることである．

2.2 OSTI仕様の特徴

(1) オペレータサービスの安全性保証

OSTI仕様の最大の特徴は，万が一，エンタープライズドメインにセキュリティ上の問題が生じても，ドメイン間の分離によってオペレータドメインへの影響を遮断できるため，電話などのオペレータサービスの信頼性，安全性は従来どおり保証されるという点である．オペレータドメインは，オペレータによって従来の移動端末と同様のセキュリティポリシーで運用され，信頼性，安全性が確保される．一方，エンタープライズドメインのセキュリティポリシーは，企業の情報システム部門など，オペレータ以外が定めることができ，そのポリシーにおいて許されるソフトウェアが使用される．

(2) 新しいユーザ体験

OSTI仕様の別の特徴は，複数のドメインを1台の移動端末上に共存させることにより，新たな移動端末の使い方を可能とすることである．典型的な利用法としては，エンタープライズドメインを業務用途とし，オペレータドメインを個人用途とすることが考えられる．例えば，エンタープライズドメインのOSにWindows®[*3]を用いると，利用できる業務用アプリケーションの選択肢が広がるというメリットが得られる．

ドコモとDoCoMo Communications Laboratories USAが実装したOSTIプロトタイプシステムの外観を**写真1**に示す．オペレータドメインにLinuxが用いられ，エンタープライズドメインにWindows CE（Consumer Electronics）が用いられている．OSTIでは，ユーザが操作できるのは常に一方のドメインであり，ドメイン切替えのための専用ボタンの押下などにより瞬時に他方のドメインに切り替えることができる．ある時点において，ユーザが操作可能なドメインをフォアグラウンド・ドメインと呼び，操作不能なものをバックグラウンド・ドメインと呼ぶ．あるドメインがバックグラウンドに切り替えられた際，そのドメイン内のソフトウェアの動作を継続させるかどうかは実装に依存する．

(3) 移動端末として一貫性のあるサービス維持

マルチドメインアーキテクチャであっても従来の移動端末の機能性や利用法を維持しなければならない．例えば，フォアグラウンド・ドメインにおいてマナーモードが設定された後，ドメイン切替えによって他方のドメインがフォアグラウンドになった際，マナーモード設定がそのドメインにも反映されていなければならない．

OSTI仕様書では，このようなドメイン間の連携・協調を必要とする要求に対し，ドメイン間でメッセージを交換するための基本的な機能とプロトコルを規定している．具体的にはメッセージの一意の識別子，通常のデータメッセージと確認応答メッセージの識別，メッセージ長，次のメッセージの位置など，メッセージ交換に必要なヘッダ要素の規定や，各メッセージ交換の確認応答（成功／失敗）が通知されることを規定している．このメッセージ交換機能により，エンタープライズドメインとオペレータドメインが協調した処理を行うことが可能になる．

3. OSスイッチ方式

OSTI仕様の実現方法の1つであるOSスイッチ方式について説明する．現在，多くのOSは，消費電力節約のために一時的にスリープモードに入るサスペンド・レジューム機能を備えている．サスペンド機能によりOSがスリープ状態になる際には，システムの

＊3 **Windows®**：Windowsは米国Microsoft Corporationの登録商標．

写真1　OSTIプロトタイプシステムの外観

状態がメモリなどに保存され，大部分のハードウェアが停止する．レジューム機能によりスリープ状態から復帰する際には，メモリなどからシステム状態を取り出し，システムを復元する．このとき，サスペンドしていたアプリケーションは実行停止時点から再開する．OSスイッチ方式は，このサスペンド・レジューム機能をドメイン切替えに利用するものである．フォアグラウンドからバックグラウンドに切り替わる際はOSのサスペンド機能によりスリープ状態に遷移し，バックグラウンドからフォアグラウンドに切り替わる際はレジューム機能によりスリープ状態から復帰する．この切替えは1秒以下で完了することが求められる．

OSスイッチ方式では，バックグラウンド・ドメインのソフトウェアが動作しないという制約がある．そのため，フォアグラウンド・ドメインで作業しながら，バックグラウンド・ドメインのソフトウェアを利用して音楽の再生やバックアップなどの処理を実行するといったことはできない．また，ネットワーク接続に関する制約として，ドメイン切替え時にネットワーク接続をすべて切断するか，ネットワーク接続を維持するための特別な処理を行わなければならない．後者の場合，接続状態に関する情報をドメイン間通信によってバックグラウンド・ドメインと共有するとともに，バックグラウンド・ドメインがスリープ状態から復帰する際にネットワーク接続状態を回復する処理が必要になる．

OSTI仕様書では，OSスイッチ方式を利用する場合のエンタープライズドメインとドメイン抽象化レイヤ間のインタフェースとして，以下の3つを規定している．

・エンタープライズOSの起動・一時停止・再開
・エンタープライズOSのシステム管理インタフェース：
プラットフォーム管理，オペレータOSとエンタープライズOS間の通信，ストレージ，周辺デバイス
・OSスイッチ方式特有の考慮事項：
OSスイッチ制御，オペレータドメインの保護

本章では，これらの規定の中でもOSスイッチ方式特有の検討事項であるOSスイッチ制御とオペレータドメインの保護について解説する．

3.1 OSスイッチ制御

OSスイッチ制御は，ユーザ操作によるドメイン切替えだけではなく，特定のイベントの割込みによる切替え動作を規定している．例えば，エンタープライズドメインがフォアグラウンド状態にあって，電話の着呼があった際，オペレータドメインに切り替えたいケースがある．エンタープライズドメインは，電話の着呼イベントをドメイン間通信によってオペレータドメインに送信した後，ドメイン抽象化レイヤに対してドメイン切替え要求を発行する．オペレータドメインはレジューム後，その着呼イベントを受信して着信処理を実行できる．ただし，OSスイッチ方式は各OSが排他的に動作する方式であるため，エンタープライズOSでVoIP（Voice over IP）[*4]通話中など，切替えを抑制したい状態も考えられる．このため，OSTI仕様ではOSスイッチのロックとその解除を行うためのインタフェースを規定している．

3.2 オペレータドメインの保護

OSスイッチ方式では，エンタープライズドメインがフォアグラウンドにあるとき，そのOSカーネル[*5]は原理的に移動端末上のすべてのリソースへ

＊4　**VoIP**：IPネットワーク上で音声データを送受信する技術．
＊5　**OSカーネル**：OSの中核を成すソフトウェアであり，ディスクやメモリなどの計算機資源の管理，割込み処理，プロセス間通信などOSとしての基本機能を提供する．

のアクセスが可能である．通常は，エンタープライズOSにリソースアクセスの制約を課すことで，オペレータドメインの重要データ保存領域（例えば，ユーザのアドレス帳や有料コンテンツ利用のための秘密鍵などが保存されている領域）を保護する．ここでは，エンタープライズOSはオペレータにとって信頼できるもののみが採用されるという前提が置かれている．しかし，万が一，悪意のあるプログラムにOSカーネル権限が奪われた場合，オペレータドメインの重要データが悪用される危険がある．その対策として，OSTI仕様書では，難読化を併用するデータ暗号化とTrustZone®[*6]によるデータ保護を例示している．

難読化を併用するデータ暗号化とは，ドメイン切替えによりオペレータドメインがスリープ状態に入る際に重要データを暗号化するものであり，スリープ中にエンタープライズドメインによって悪用される危険を回避する．再度のドメイン切替えによりオペレータドメインがスリープ状態から復帰する際には，暗号化していたデータを復号する．ここで，暗号処理に用いる鍵をそのまま保存しておくとスリープ中にエンタープライズドメインによって鍵が盗まれ，重要データが解読されてしまう危険がある．そこでOSTI仕様書では，OSスイッチ方式でこれらのデータ暗号化を行う場合，リバースエンジニアリング[*7]が困難なアルゴリズムによってのみ，鍵を再現できるなどの難読化技術を併用することを必須としている．

TrustZoneによるデータ保護は，一部のARMプロセッサ[*8]に搭載されるTrustZone技術を利用して2つのドメインを分離するものである．TrustZoneは，プロセッサによって移動端末をセキュアドメインとノンセキュアドメインに分離し，前者はすべての移動端末リソースへのアクセスを許可し，後者は限定されたリソースへのアクセスしか許さないというアクセス制御をハードウェアレベルで強制できる．OSTI仕様では，オペレータドメインをセキュアドメインに割り当て，エンタープライズドメインをノンセキュアドメインに割り当てる．エンタープライズドメインが，オペレータドメインの重要データにアクセスできない構成とすることで，エンタープライズドメインのOSカーネル権限が奪われても，重要データへのアクセスを防止できる．TrustZoneはARMプロセッサ限定の技術であるが，他のプロセッサであっても同様のドメイン分離能力を備えていれば，同様に利用可能である．

4. 仮想マシンモニタ方式

OSTI仕様の実現方法の1つである仮想マシンモニタ方式を説明する．仮想マシンモニタ方式は，CPU，メモリや周辺デバイスなどのハードウェアを仮想化して，複数のOSにその実行環境を提供する技術である．OSTIにおける仮想マシンモニタ方式では，1つの端末上で複数のOSを並列に実行可能となり，OSスイッチ方式の同時に両方のOSを稼動できないという制約は課されない．ただし，その代償として仮想化の処理のため，CPU，メモリや消費電力などのリソース消費が増加してしまう．

OSTI仕様書では，仮想マシンモニタ方式を利用する場合のエンタープライズドメインとドメイン抽象化レイヤ間のインタフェースとして，以下の3つを規定している．

- エンタープライズOSの起動・一時停止・再開
- エンタープライズOSのシステム管理インタフェース：
  プラットフォーム管理，オペレータOSとエンタープライズOSの通信，ストレージ，周辺デバイス
- 仮想マシンモニタ方式特有の考慮事項：
  周辺デバイスの切替え機構

仮想マシンモニタ方式の特徴は，2つのOSが並行動作する環境でも電話として一貫した動作を維持するため，OS間での周辺デバイスの切替え・共有制御を規定している点である．OSTI仕様書では，周辺デバイスをコア型（ディスプレイやキーパッドなど），オンデマンド型（カメラやマイクなど），共有型（スピーカやバイブレーションなど）の3種類に分類している．コア型に属する周辺デバイスは，ドメイン切替えボタンと連動して一緒に切り替えるように制御するのに対して，オンデマンド型は，各ドメイン内のアプリケーションなどからの要求に応じて，いずれかのドメインへ割当てを切り替えるものである．電話中にドメインを切り替えて作業を可能にしつつも，一緒にマイクも切り替えられてしまうことで音声入力が途切れることがないように，ロックやその解除のインタフェースを規定している．また，共有型は両方のドメインから同時に利用可能とするものの，マナーモー

＊6 **TrustZone®**：英国ARM Limitedの登録商標．

＊7 **リバースエンジニアリング**：ソフトウェアやハードウェアの構成や動作を解析し，製造方法や動作原理などを明らかにすること．

＊8 **ARMプロセッサ**：英国ARM Limitedが開発したアーキテクチャを採用するCPU．移動端末や携帯型ゲーム機器などで広く使われている．

ドを考慮し，スピーカの場合，片方のドメインでマナーモードが設定された状態では，もう一方のドメインでも音が鳴らないように制御する．

また，OSTI仕様書では，仮想マシンモニタ方式で課題となるリソース消費削減のため，バックグラウンドのドメインを休止状態にするインタフェースや，周辺デバイスの電力管理を行うためのインタフェースも要件として規定している．

5. あとがき

本稿では，OSTI仕様書で規定したマルチドメインアーキテクチャの概要とその特徴および実現方法としてのOSスイッチ方式と仮想マシンモニタ方式を解説した．

OSTI仕様は，従来のオペレータサービスの品質や安全性を損なうことなく，企業や個人が自由に開発した既存のアプリケーションソフトウェアを利用できるようにするための移動端末向けマルチドメインアーキテクチャを，世界で初めて規定したことに意義がある．

今後は，本仕様に基づくプロトタイプを開発し，仕様の検証を行っていく．また，広く移動端末メーカやソフトウェア開発会社などからOSTI仕様書に対する技術的なフィードバックを得て，技術改良を進めていく予定である．

文　献

[1] Intel Corporation and NTT DoCoMo, Inc: “Open and Secure Terminal Initiative (OSTI) Architecture Specification Revision 1.00,” 2006.
http://www.nttdocomo.co.jp/corporate/technology/osti/index.html