端末管理　遠隔制御　OMA-DM

Technology Reports

端末管理に対する多様なニーズに対応した端末管理制御基盤システムの開発

近年，情報流出リスクの回避や法人向け利用ニーズへの対応などが求められている．法人利用，コンシューマ利用，通信オペレータ利用などの多様な形態に応じ，オープンプラットフォーム端末も含めた多様な移動端末に対し，遠隔初期化，遠隔カスタマイズなどの端末管理機能を一元的に提供可能とする端末管理制御基盤システムを開発した．

ネットワーク開発部　涌井 道子　竹内 伸夫
プロダクト部　一瀬 晃弘　小野木 雅

1. まえがき

近年，移動端末（以下，端末）の紛失などに伴う情報流出リスクへの適切な対応や，法人契約における社員による端末の適切な利用のための監視などが求められている．一方で通信オペレータとしても，機能が複雑化する端末における正常動作の診断チェック，機能の利用頻度の把握やネットワーク品質に関するユーザ満足度向上のために端末から取得できるネットワーク品質情報の遠隔収集といった機能が求められており，総じて端末に対して遠隔でさまざまな制御を行う機能が求められている．

ドコモは，セキュリティ機能を重要視する法人ユーザ向けに遠隔データ初期化や遠隔機能制御を強化した端末を提供しているが，一般ユーザのセキュリティへの関心も高まっており，これに応えるために端末紛失時に遠隔から端末ロックを可能とする機能[1]を搭載したFOMA端末を提供して，さまざまなサービス展開を行っている．加えて，今後市場成長が期待されるスマートフォンをはじめとするオープンプラットフォーム（OPF）端末[*1]にも，同様のニーズが想定される．

これらのことから，端末のプラットフォーム種別を問わず，多様な端末管理にかかわるサービスを包括的に管理すると同時に，ニーズに応じた機能追加を即座に行い，ユーザの要望に瞬時に応えられる端末管理制御基盤システム（以下，基盤システム）開発が求められる．

本稿では，端末を一元的に管理するとともに，OPF端末も含めた端末管理／制御方式として広く採用されている国際標準方式であるOMA（Open Mobile Alliance）-DM（Device Management）[*2]にも対応し，端末管理に対する多様なニーズに迅速に応えるべく開発した基盤システムについて解説する．

2. 基盤システム

基盤システムは，端末内データの初期化など，遠隔からの各種制御を実行する処理を一元的に管理・実行している機能群から構成される．

2.1 システム設計コンセプト

基盤システムにおけるシステム設計コンセプトを次に示す．

・機能ごとにモジュール化することで，ユーザニーズ，国際標準化における新たな仕様規定に合わせた機能拡張時の影響範囲を極力抑え，短期間でのサービス追加を実現．

・複数サービスを横断的に管理する端末制御管理部を設け，端末における優先度判定などの競合

＊1　**オープンプラットフォーム（OPF）端末**：アプリケーションを自由に追加することで，機能強化やカスタマイズが可能であり，ハードウェアに依存するネイティブアプリケーションも自由度高く利用することができる，携帯電話型の情報端末．

＊2　**OMA-DM**：OMAはモバイル関連のアプリケーションの標準化を進める団体であり，DMはデバイス管理機能．

処理に伴う負担を軽減.

・コアネットワークで保持する各種ユーザ情報と連携し，端末にSIM（Subscriber Identity Module）が挿入されたタイミングで，端末製造番号（IMEI：International Mobile Equipment Identity）と加入者番号（MSISDN：Mobile Subscriber ISDN Number）が制御対象端末か否かを判定したうえで，端末制御要求を再送するなどの付加価値を提供.

・対象端末に対し，機種／OS／アプリなどには制約を設けずにFOMA端末からOPF端末まで制御を可能とするため，制御対象端末の機種を特定した最適なプロトコルによる端末制御を実現.

2.2 システムの構成

基盤システムの構成を**図1**に示す.

①制御受付・応答部

法人が社員に貸与する端末の制御や，個人ユーザからの申告に合わせたドコモサポートシステムからのユーザ端末への制御など，さまざまなサービスの制御要求に対する受付，応答を実行している．制御要求システムはサービスの数に応じて複数存在するため，制御要求を一元的に受け付ける制御受付・応答部を設け，複数の制御要求システムからの要求プロトコルの差分を吸収すると同時に，複数システムから一度に要求される制御要求の受信制御を行っている.

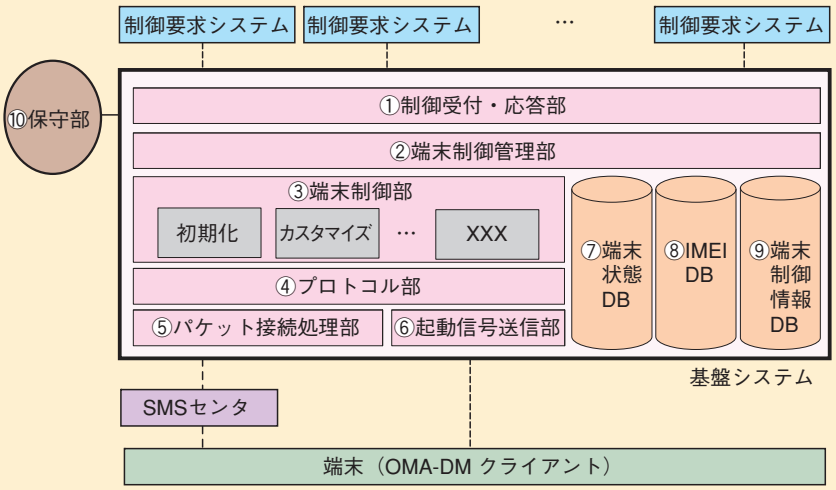


図1　基盤システム構成

②端末制御管理部

制御受付・応答部より端末へ送信される遠隔初期化，遠隔カスタマイズなどの制御要求を横断的に管理しており，1台の端末に複数の制御要求が同時に要求された場合，同時に発生した制御要求間の優先順位付け，制御中処理との優先度判定を実施している．制御要求を受け付けた端末制御管理部では，契約条件の確認，端末状態DB参照による端末状態の判定，さらには，IMEI DB参照により制御対象端末か否かの判定を行い，制御要求の正当性を検証している．また，位置登録などのコアネットワーク機能と連携した再送処理を行っている．例えば，端末制御が失敗した際に，次の位置登録や電源がONされたことを検知し，再送を行う.

③端末制御部

端末制御管理部から転送された制御要求を受けて，端末制御情報DBを参照し，機種ごとの制御可能な機能，適用制御プロトコルなどを認識し制御を実行している．端末制御部は遠隔初期化，遠隔カスタマイズなどの端末制御を行う機能単位で構成されており，OMA-DMで制御するサービスについては，OMAで規定されているLAWMO（Lock And Wipe Management Object）[*3]，DCMO（Device Capability Management Object）[*4]などの各種管理機能を適用している．また，標準化での新たな仕様規定に合わせ，随時管理機能を追加可能な仕組みとなっている.

④プロトコル部

端末制御プロトコルの処理部であり，OMA標準のDMクライアントを搭載した端末にはOMA-DM方式で制御するなど，対象の端末に応じてプロトコルの選択が可能となっている.

＊3　**LAWMO**：端末を遠隔からロック・初期化する管理機能.
＊4　**DCMO**：端末機能の使用可否を遠隔から制御する機能.

⑤パケット接続処理部

端末と基盤システム間でSSL（Secure Socket Layer）[*5]接続を行うと同時に，パケット通信の課金処理や接続可否判定を実施している．基盤システムは複数のサービスで使用される基盤であるため，サービス（機能の利用形態・契約状態）に応じて課金方法が異なることが予想される．そこで，基盤システムへ接続する際に端末が指定する接続先（APN：Access Point Name）を課金方法が異なるサービス単位に分けるとともに，パケット接続処理部ではこれら複数のAPNでの接続を許容している．

⑥起動信号送信部

OMA-DM方式にて端末制御を実施する際には，SMS（Short Message Service）にてDMN（DM Notification）[*6]を端末向けに送信し，端末から基盤システムへのパケット接続を起動する．具体的には，起動信号送信部でDMNを生成し，端末に対してSMSを送信している．

⑦端末状態DB

基盤システムにより制御された端末状態（カメラロック，ブラウザロックなど）を管理し，端末状態に応じて端末制御の可否を判断する際に参照される．

⑧IMEI DB

使用中のIMEIとMSISDNの組合せ情報を管理するデータベースであり，端末制御時に制御対象端末が現在使用中かを判定する際に参照される．

⑨端末制御情報DB

端末制御に必要な端末機種情報と適用プロトコルを管理するデータベースであり，適用プロトコルがOMA-DMの場合には，OMA-DMで規定されているMO（Management Object）[*7]を保持しているため，MOを登録するのみで制御が可能となっている．

⑩保守部

基盤システムを遠隔から監視・制御し，ユーザからの問合せなどに対応すべく，端末制御のログも管理している．

3. 基盤システムを利用したサービス

ドコモでは基盤システムを利用したサービスとして，「遠隔カスタマイズ」「遠隔初期化」「遠隔ロック」「遠隔初期設定」を提供している．中でも「遠隔カスタマイズ」「遠隔初期化」は，法人ユーザ向け端末管理サービスである「ビジネスmoperaあんしんマネージャー」上のオプションサービスとして，2008年11月19日に提供を開始した[2]．

(1)遠隔カスタマイズ

「遠隔カスタマイズ」サービスは，企業の端末管理者が遠隔設定で必要最低限の機能を社員に利用させることで，業務外利用制限や情報漏洩リスクの軽減化といった，端末の利用に関する企業ごとのポリシーに，柔軟に対応することを目的として提供している．カスタマイズ設定対象機能の一覧を**表1**に示す．

(2)遠隔初期化

「遠隔初期化」サービスは，端末で保持する電話帳，メールなどのユーザデータ削除や設定リセットを遠隔から実施し，工場出荷時の状態にすることにより，紛失時の情報漏洩防止を実現している．削除の対象は端末本体のユーザデータだけではなく，メモリカード，SIMカード内のユーザデータにも対応しており，個別に選択して削除できる．

3.1 サービス処理フロー

遠隔カスタマイズサービスの処理フロー例を**図2**に示す．本サービス

表1　遠隔カスタマイズ設定対象機能一覧

遠隔カスタマイズ制御項目（2009.10.1現在）
カメラ利用
音楽・動画プレイヤー利用
ワンセグ利用
メーラ利用
ブラウザ（iモード・フルブラウザ）利用
iアプリ利用
iアプリ自動起動設定
マナーモード強制（直接制御）
ダイヤル発信制限
電話帳登録外着信拒否
電話帳利用
Bluetooth®※1・USB通信・赤外線通信・FeliCa®※2通信によるデータ送受信
データBOX利用
外部メモリ利用
FOMAカード内の電話帳・SMSの閲覧・移動
生体認証のみ有効
開閉ロック設定（ON/OFF）
ICカードロック設定（ON/OFF）
GPS位置提供設定

※1　Bluetooth®：米国Bluetooth SIG Inc.の登録商標．
※2　FeliCa®：ソニー㈱の登録商標．

＊5　**SSL**：主にインターネットを利用してクライアントとサーバとの間で安全に通信を行うためのプロトコルであり，暗号化，認証，改ざん検出の機能を提供．
＊6　**DMN**：OMA-DMにて規定されている端末制御を起動するための通知情報．
＊7　**MO**：OMA-DMにて端末を制御する際に，制御対象となる端末構造．

はOMA-DM方式により実現される．なお，遠隔初期化サービスもほぼ同様の動作である．

企業の端末管理者は法人ユーザ向け管理サイトにて，事前に登録された端末のMSISDNおよびIMEIを指定し，基盤システムへ遠隔カスタマイズの制御要求を送信する．

基盤システムでは，制御要求を受け付けると指定された端末への制御が許可されている場合，端末に対しDM制御を開始するためのメッセージとしてPackage[*8]（以下，Pkg）#0（DMN）を端末へ送信する．Pkg#0（DMN）を受信した端末はパケット接続およびSSLネゴシエーションを行う．端末はセッション確立後，IMEIなどの端末情報を含んだPkg#1を基盤システムへ送信する．Pkg#1を受信した基盤システムは，指示された制御対象端末であるかをIMEIの照合により判定する．判定後，制御コマンドを含んだPkg#2を端末へ送信する．Pkg#2を受信した端末は，制御コマンドの内容に応じた制御を実行する．端末にて制御完了後に，Pkg#3で完了報告を基盤システムへ送信する．基盤システムはPkg#4で受信確認を端末へ送信し，Pkg#3が基盤システムで正常に受信されたことを端末が認識すると，DM制御を終了する．同時に基盤システムは，制御完了報告を法人ユーザ向け管理サイトあてに通知し，制御を終了する．

また，制御完了時に端末の設定状態が端末状態DBに登録され，企業の端末管理者は法人ユーザ向け管理サイトを通して，カスタマイズの設定状態を確認できる．

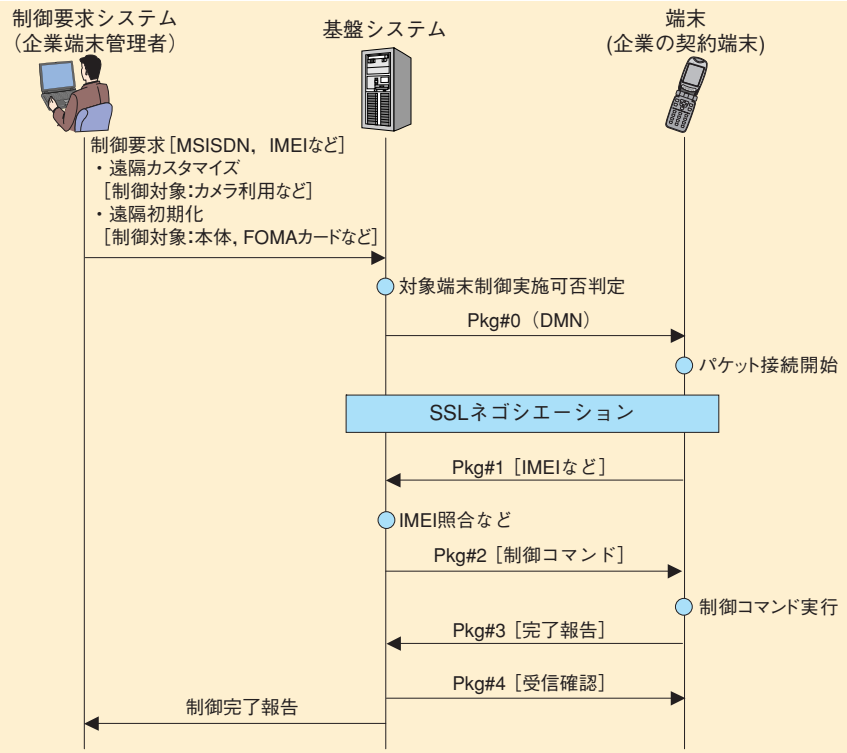


図2　遠隔カスタマイズ実行時の処理フロー例

3.2 端末のソフトウェア構成

端末のソフトウェア構成イメージを**図3**に示す．遠隔カスタマイズ，遠隔初期化サービスではOMA-DM方式を利用するため，OMA標準のDMクライアントを使用する．また，DMクライアントはPkgデータ処理のみを実行するため，カスタマイズ／初期化処理実行部，制御対象アプリケーションを起動するアプリ起動制御部を端末機能として実装している．

本サービスにおける端末内の処理概要を次に示す．

アプリ起動制御部は基盤システムからのPkg#0（SMS）受信を契機に機能起動条件を判定し，DM機能を起動する（図3①②）．DMクライアントは基盤システムと送受信するPkgデータの生成／解析を行い（図3③），基盤システムからの指示をカスタマイズ／初期化処理実行部へ通知し，カスタマイズ／初期化処理が実行される（図3④）．

制御対象アプリケーションが起動される際は，アプリ起動制御部がカスタマイズ状態に従い，当該アプリの起動を実行または制限する（図3⑤）．

3.3 他機能との競合処理

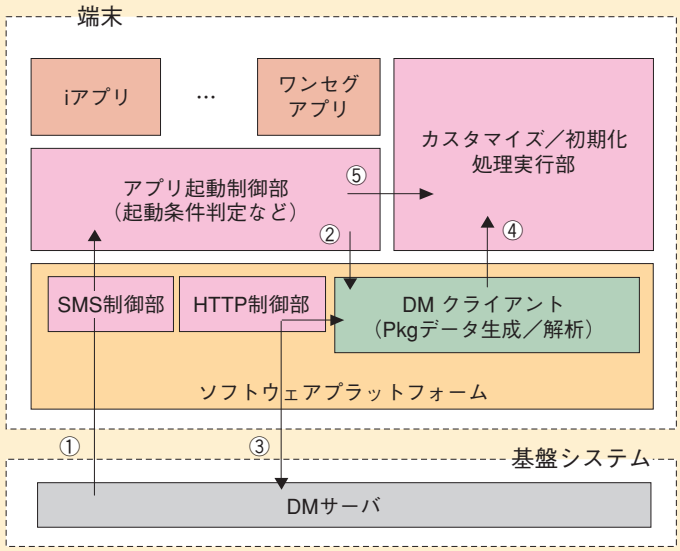
本サービスのようなサーバ起動型の基盤システムでは，Pkg#0（SMS）を契機にパケット通信による制御を

＊8 **Package#X**：OMA-DMにおける処理メッセージ．Xは処理メッセージの順番を示す値（0，1～4）．

開始する．そのため，端末を使用中に制御が開始される場合がある．この点に対しOMA-DM方式では，Pkg#0受信時に強制的にDM処理を実行または利用者が実行可否を選択して可の場合にのみ実行，のいずれかを管理者が選択できる．

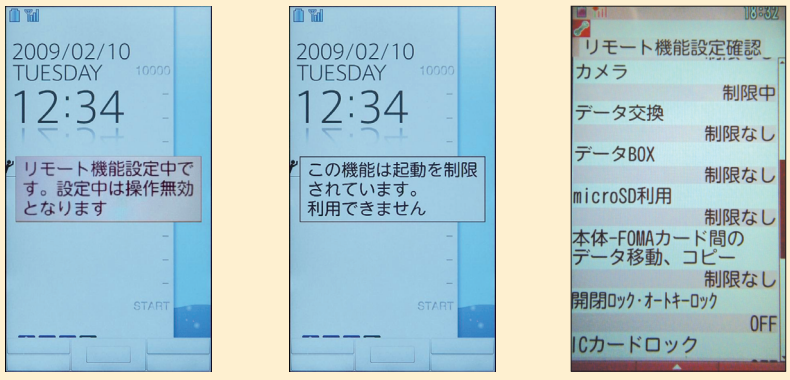
今回の遠隔初期化，遠隔カスタマイズサービスでは，リスク軽減のため管理者からの指示を最優先としており，端末利用中のユーザの意思にかかわらず実行することになる．そのため，強制的にDM処理を実行する設定としている．また，特にパケット通信中など他機能の実行により本機能の実行が阻害されないよう，音声通話や緊急性のある機能以外は原則強制的に終了し，DM処理を実行することとしている．

なお，今後追加されるサービスによっては他機能を優先するケースも考えられる．その場合は，例えばPkg#0のオペレータ拡張領域にて独自パラメータを追加するなどの対応により，サービスごとに優先度を設定することが可能となる．



HTTP：Hypertext Transfer Protocol

図3　端末ソフトウェアの構成



制御実行中画面　　機能制限中喚起表示画面　　機能設定状態確認画面

図4　遠隔カスタマイズ制御実行時の端末画面イメージ

3.4 ユーザインタフェース

遠隔カスタマイズ制御実行中の端末画面イメージを**図4**に示す．制御完了後に制限された機能を操作しようとした場合，「機能制限中喚起表示画面」のように表示され，該当機能は操作できなくなる．また，制御された機能はグレーアウトされるか，起動時に操作できない旨が表示される．また，企業管理者のPC操作により，本機能のメニューを通じて各端末の制御状態を確認できる．

4. あとがき

本稿では，端末管理に対する多様なニーズに迅速に応えるべく開発した端末管理制御基盤システム，適用サービスとして遠隔初期化および遠隔カスタマイズの機能について解説した．今後も，ユーザニーズやOMAでの仕様規定の動きに合わせ，端末管理機能の追加を実施していく予定である．

文　献

[1] 櫻井，ほか：“安心・安全な生活ケータイの利用に向けたネットワークによる端末管理基盤技術開発―ケータイ指定ロック機能のシステム開発―，”本誌，Vol.16，No.1，pp.36-40，Apr. 2008.

[2] NTTドコモ報道発表資料：“「ビジネスmoperaあんしんマネージャー」の機能を拡充，”Nov. 2008.