

# 903i 搭載 アプリケーション機能

FOMA 903iシリーズの新規アプリケーションとして、きせかえツール<sup>®\*1</sup>機能、マチキャラ機能、各社発行デジタル証明書対応機能、SMS迷惑メール対策機能を搭載し、ユーザにとってより魅力的で、より安心・安全な移動端末を開発した。

ひらいし じゅんこ	とおりやま え ま
平石 絢子	通山 恵麻
や の えいじ	にしむら よしまさ
矢野 英司	西村 佳将

## 1. まえがき

移動端末の利用シーンが広がり、ユーザが移動端末を手放せないようになってきたことから、移動端末はユーザにとってより魅力的であり、より安心・安全であることが求められている。これらの要求を満たすため、高機能・高性能な移動端末を追求するユーザをターゲットにアプリケーションとして、きせかえツール機能、マチキャラ機能、各社発行デジタル証明書対応機能、SMS (Short Message Service)<sup>\*2</sup>迷惑メール対策機能を搭載した、FOMA 903iシリーズを開発した。

きせかえツール機能、マチキャラ機能では、よりユーザの嗜好に合わせて移動端末をカスタマイズできる機能を実現した。各社発行デジタル証明書対応機能、SMS迷惑メール対策機能では、移動端末をより安心・安全に使うための機能を向上させた。

本稿では、これら4つの新規機能の概要を解説する。

## 2. きせかえツール機能

### 2.1 サービスコンセプト

移動端末の待受画面や着信音などに、ユーザが好みのコンテンツを用いてカスタマイズを行う際、より豊富なコンテンツの中から選択が行え、それを簡易な操作で設定できることが重要である。また、さまざまな領域に同じキャラクタを用いたコンテンツを設定するなど、移動端末内の世界観

\*1 きせかえツール<sup>®</sup>: (株)NTTドコモの登録商標。

\*2 SMS: 主に移動端末どうしてテキストベースの短いメッセージを送受信できるサービス。

を統一してカスタマイズしたいという要望が高まっている。

そこで、きせかえツール機能では、特にユーザの利用頻度の高い領域については、ダウンロードコンテンツを用いたカスタマイズを実現し、さまざまなコンテンツによる多彩な表現を可能とした。また、複数のカスタマイズ領域に設定するコンテンツを一括でダウンロード・設定する機能を実現し、簡易な操作で移動端末内の世界観を統一することを可能とした。

以下に、きせかえツールにおけるカスタマイズ機能の拡大および一括ダウンロード・設定機能について述べる。

## 2.2 カスタマイズ機能の拡充

きせかえツール機能では、トップメニュー画面にダウンロードしたFlash<sup>®\*3</sup>メニューコンテンツを設定可能とした。Flashメニューは、コンテンツから移動端末の機能を直接起動することが可能であり、かつ、市場に存在するFlashコンテンツを用いて誰でも作成可能であるため、いたずらコンテンツを作成される懸念が高く、既存機種ではプリインストールコンテンツとしてのみ設定可能としていた。このため、きせかえツールでは、通常のFlashコンテンツではな

く、後述のパッケージとしてのみ扱うことで、前述の懸念を解消し、ダウンロードを可能とした。これにより、プリインストールコンテンツのみならず、より豊富なコンテンツの中から、ユーザがトップメニュー画面をカスタマイズすることを可能とした。また、電池残量やアンテナ状況の表示など、ユーザがよく目にするところを中心に、新たにダウンロードコンテンツを用いたカスタマイズを可能とした。

このカスタマイズコンテンツのダウンロード化およびカスタマイズ領域の拡大により、移動端末内のより広い領域を、より多彩なコンテンツの中からユーザの趣向に即したカスタマイズが可能となった。

## 2.3 一括ダウンロード・設定機能

きせかえツール機能では、さまざまな領域を簡易にカスタマイズ可能とする機能を実現した。さまざまな領域で扱われる複数コンテンツのダウンロード・設定を一括で可能とするため、きせかえツールではコンテンツをパッケージ化する。一括ダウンロード・設定機能概要を図1に示す。

パッケージ化されたコンテンツ（以下、パッケージ）は、パッケージタイトルなどの基本情報および各コンテンツがどの

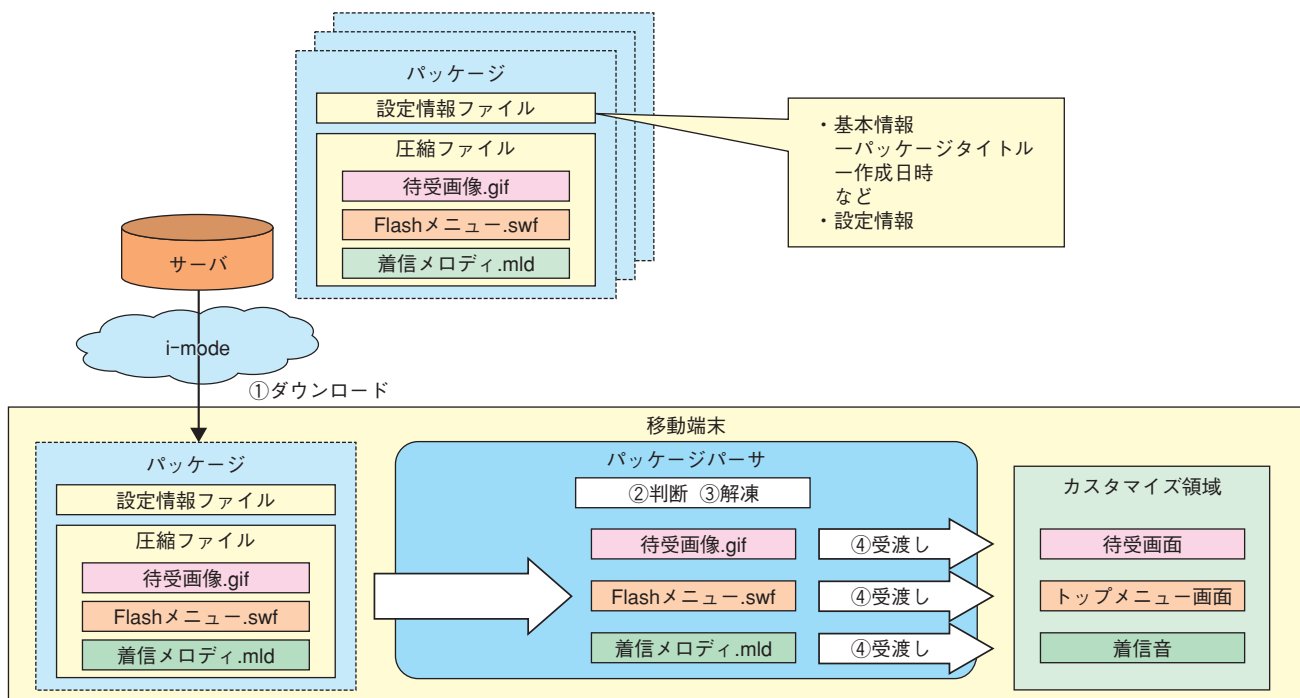


図1 一括ダウンロード・設定機能概要

\*3 Flash<sup>®</sup>: 音声やベクタグラフィックスのアニメーションを組み合わせたコンテンツを作成するソフト、または作成されたコンテンツのこと。Flashは、Adobe Systems Inc.の米国およびその他の国における商標または登録商標。

カスタマイズ領域に設定されるかを指定する設定情報ファイル、実コンテンツを圧縮した圧縮ファイルから構成される。

パッケージは、i-modeブラウザよりダウンロードすることで取得される(図1①)。取得されたパッケージの設定には、移動端末に搭載されたパッケージパーサを利用する。パッケージパーサは、設定情報ファイルの判断および圧縮ファイルの解凍を行うモジュールである。パッケージ設定時、パッケージパーサは設定情報ファイルから各コンテンツがどのカスタマイズ領域に設定されるべきかを判断し(図1②)、解凍したコンテンツ(図1③)を該当のカスタマイズ領域へ受け渡す(図1④)。該当のカスタマイズ領域では、受け取ったコンテンツを設定に反映する。これにより、複数コンテンツの一括ダウンロード・設定が実現される。

### 3. マチキャラ機能

#### 3.1 サービスコンセプト

待受画面などを変更し、ユーザ好みの移動端末にカスタマイズする機能が普及している。しかし、ユーザのカスタマイズ領域を拡張するうえで、待受画面やメニュー画面などの複数の機能画面に同一のコンテンツを継続して表示する機能は、これまで提供されていない。また、ユーザが感情移入しやすいことと、コンテンツプロバイダ(CP: Contents Provider)のビジネス領域開拓につながることで、提供されるコンテンツの増加が期待されることから、キャラクタコンテンツの活用が検討された。そこで、待受画面やメニュー画面などの異なる機能画面を背景画像として、そこにキャラクタ画像を継続して重畳表示する機能を、マチキャラ機能として実現した。

キャラクタ画像の形式は、2D/3D形式ともに対応している。また、不在着信などの移動端末の状態遷移に応じて、重畳表示されたキャラクタ画像を変更することが可能である。マチキャラ機能に対応した待受画面を写真1に示す。例えば、通常の状態(写真1(a))時に不在着信が生じると不在着信状態へと状態遷移が行われ、不在着信用のキャラクタ画像(写真1(b))が表示される。

マチキャラ機能用キャラクタデータは、i-modeコンテンツとしてCPが自由に作成/提供することができる。

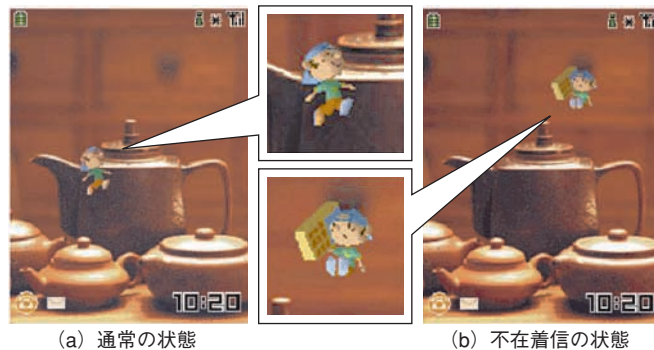


写真1 マチキャラが表示された待受画面

#### 3.2 構成技術の概要

マチキャラ機能は、「キャラクタの表示座標管理」、「キャラクタ画像を切り替える状態遷移管理」、「時間情報によるキャラクタの外見変更」の3つの機能から構成される。

##### (1) キャラクタの表示座標管理

キャラクタの表示位置を制御することで、移動端末画面上をキャラクタ画像が移動する表現を実現する。表示位置の制御では、行動パターンや移動速度を変えることでキャラクタらしさを表現できることと、用意されたルートでの移動のみを繰り返し単調な表示としないことを考慮し、以下の2種類の移動方法を用意し、CPが自由に組み合わせられるようにした。

- ・定型移動：キャラクタが移動するルートをCPが設定することで、CPの意図を重視する移動方法
- ・自動移動：キャラクタが移動するルートを移動端末内で生成することで、同一の移動ルートの繰返しを避けることを重視する移動方法

##### (2) キャラクタ画像を切り替える状態遷移管理

不在着信やメール受信などの移動端末の状態遷移によるキャラクタ画像の変更と各状態の優先順位管理を行う。

CPは、移動端末の不在着信などの各状態に対して、状態遷移発生時のキャラクタ画像や移動時のキャラクタ画像などを用意できる。

##### (3) 時間情報によるキャラクタの外見変更

現在時刻やマチキャラコンテンツ使用時間により、キャラクタの外見変更を行う。キャラクタの外見変更を行う方法として、キャラクタデータで利用されるテクスチャ\*4を変更することにより実現する方法と、キャラクタデータ全

\*4 テクスチャ：3D形式のデータにおいて、物体表面の質感を表現するために物体表面に貼り付ける画像のこと。

体を差し替えることにより実現する方法がある。テキストチャ変更では、昼間はスーツを着て夜になるとパジャマを着るなど、見た目の変化の小さな表現が可能である。外見変更に必要な追加データ量も小さい。テキストチャ変更は、3D形式のキャラクタデータでのみ適用可能である。キャラクタデータ全体差替では、子供から大人に変わるなど、見た目の変化の大きな表現が可能である反面、外見変更に必要な追加データ量も大きい。キャラクタデータ全体差替は、2D/3D形式いずれのキャラクタデータでも適用可能である。

## 4. 各社発行デジタル証明書対応機能

### 4.1 サービスコンセプト

移動端末で展開されているセキュア通信サービスでは、ドコモが発行するデジタル証明書（FirstPass）を利用していたが、一般の証明書発行局（CA（Certificate Authority）局）や各法人独自にて発行するデジタル証明書の増加に伴い、各CA局が独自のポリシーでFOMAユーザを認証しセキュアサービスを提供する、というニーズが顕在化している。

そこで、移動端末でのセキュリティ機能の高度化と法人市場の拡大を目的として、本機能にて、移動端末から一般のCA局や各法人が発行するデジタル証明書を取得し保存することを実現し、これらのデジタル証明書をセキュア通信やデジタル署名に利用可能とした。

### 4.2 各社発行デジタル証明書の取得・保存

デジタル証明書は、標準的な発行データフォーマットであるPKCS#12（Public Key Cryptography Standards#12）<sup>\*5</sup> デ

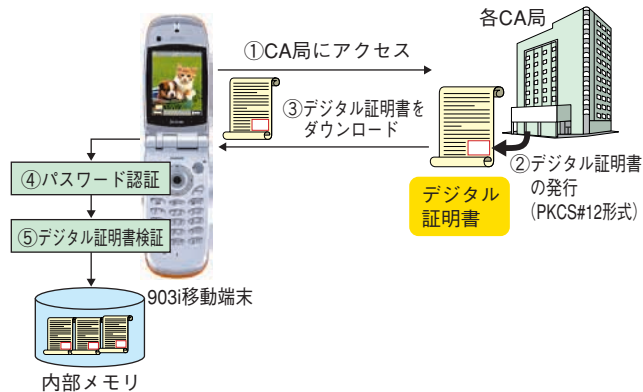


図2 各社発行デジタル証明書ダウンロードイメージ

ータとしてCA局などで生成され、移動端末ではブラウザ機能によりCA局の証明書発行サイトに接続し、PKCS#12データをダウンロードすることで取得する（図2①～③）。

このPKCS#12データにはデジタル証明書と対をなす秘密鍵も含まれており、秘密鍵は非常にセキュアな情報であることから、CA局側でパスワードによる暗号化が施されている。そのため、PKCS#12データを取得する際は、移動端末にてCA局が設定したパスワードの入力を必ず促すことで、不正なデータを取得することを防止している（図2④）。

また、従来の移動端末では、販売当初より搭載しているデジタル証明書や、ドコモが発行するデジタル証明書（FirstPass）のみを利用可能としていたために、デジタル証明書自体のデータ形式などの正当性は、移動端末でデジタル証明書をダウンロードや利用する前に、ドコモで確認することができた。しかし、本機能ではドコモ以外のCA局が発行するデジタル証明書を扱うため、事前にドコモでデジタル証明書の正当性を確認することは不可能である。また、CA局ではそれぞれの方針によりさまざまなデータ形式のデジタル証明書を発行しているため、セキュア通信サービスに利用可能なデジタル証明書だけを保存可能とし、不要・不正なデジタル証明書は保存不可とするような仕組みが必要である。このため、移動端末にデジタル証明書を保存する際に、ダウンロードされたデジタル証明書の正当性を検証する機能を搭載した。具体的には、デジタル証明書のデータ形式の検証をはじめ、PKCS#12データ内に含まれるデジタル証明書とその上位証明書（Root証明書やサブRoot証明書）間でのチェーン形成<sup>\*6</sup>可否の検証と、さらに公開鍵・秘密鍵ペアの正当性検証を実施することで、セキュア通信サービスでの利用性を保証している（図2⑤）。

### 4.3 各社発行デジタル証明書の利用

ダウンロードされたデジタル証明書はセキュア通信サービスで利用が可能である。本モデルでは既存機能である、SSL（Secure Sockets Layer）<sup>\*7</sup>/TLS（Transport Layer Security）<sup>\*8</sup>通信とデジタル署名にて利用が可能である。以下に、それらの利用方法を説明する。

#### (1) SSL/TLS通信での利用

移動端末のブラウザ機能やiアプリから、ダウンロードした他社発行のデジタル証明書を利用してSSL/TLS通信を

\*5 PKCS#12：証明書と秘密鍵を交換・伝達するために利用される標準的なデータ形式。

\*6 チェーン形成：デジタル証明書が該当のCA局から発行されたか否かを証明するための手法。

\*7 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間で通信を行う際に、通信を暗号化しデータの改ざんを発見することにより、安全に通信を行うためのプロトコル。

行うことが可能である。

利用するデジタル証明書は、SSLプロトコル上でサーバから指定されるRoot証明書一覧に対応したデジタル証明書が移動端末側で自動的に抽出される。これにより、ユーザが選択する際に利用可能なデジタル証明書だけを表示するといった、利便性向上のための動作を実現している。

また、デジタル証明書をサーバ側へ送信する際、秘密鍵による署名演算が必要となるが、秘密鍵は非常にセキュアな情報であることから、移動端末利用者の本人性確認が必要である。そのため、本機能ではすでに移動端末に実装されている端末暗証番号の入力を必須とすることで、既存機能流用によって開発量を抑えつつ、本人性確認を実現している。なお、今後はさらに本人性確認を強化するために、生体認証技術との連携を検討している。

## (2) デジタル署名での利用

既存機能であるiアプリによるデジタル署名機能にて、本機能によってダウンロードしたデジタル証明書の利用が可能である。デジタル署名とは、主に移動端末とサーバ間でやり取りされるトランザクションデータに対して、デジタル証明書と対をなす秘密鍵を用いて暗号化し、暗号化したデータをトランザクションデータに付与することで、改ざん防止および本人性確認を実現するための手法である。

なお、デジタル署名生成時は秘密鍵を利用することから、SSL/TLS通信時と同様に、端末暗証番号の入力を必須とすることで、移動端末側での利用者の本人性確認を実現している。

## 5. SMS 迷惑メール対策機能

### 5.1 サービスコンセプト

昨今、急増しているSMSを用いた迷惑メールへの対策として、SMS送信業者へ送信制限などを実施してきた。しかしながら、一部のSMS迷惑メールがユーザに届いてしまう可能性がある。また、SMSは電話番号をあて先とするため被害の拡大が想定され、早急な対応が必要である。そこで今回、安心・安全な移動端末への取組みとして、新たに移動端末側に、セキュリティスキャンを用いたSMS迷惑メール対策機能を搭載した。この機能は、受信したSMSの本文に電話番号やURLが含まれていた際に、ユーザに対して警告通知を行う機能である。これにより、ユーザが迷惑SMS業者へ不用意に接続することを未然に防ぐ効果を期待して

いる。以下に、本機能実現のために用いた技術の概要を説明する。

### 5.2 任意メッセージ表示機能

本文に電話番号やURLのリンクがあるSMSは、既存のセキュリティスキャン機能を用いて問題要素として検出できる。しかし、検出時に表示される警告が固定形式であるため、SMS迷惑メール対策などに柔軟に対応できない問題がある。そこで、警告メッセージの内容を自由にカスタマイズする機能を実現し、検出する問題に適したメッセージを表示する機能を実現した。問題検出時に自由にカスタマイズできるメッセージの表示を可能にするため、セキュリティスキャン機能の拡張を行った。

#### (1) パターンデータフォーマットの拡張

パターンデータに、問題要素検出時に表示するメッセージをデータの一部として格納できるようにデータフォーマットを拡張した。これによりパターンデータは、ダウンロードによる更新ができるため、問題の検出パターンだけでなく表示メッセージの追加・修正・削除を行うことも可能となった。つまり、新手の迷惑メールなどで問題検出時に新しいメッセージ表示の追加が必要となった場合に対しても柔軟に対応できることを意味している。

なお、移動端末バイリンガル設定にも対応できるよう、日本語／英語のメッセージを同時に格納できるようにした。

#### (2) 問題要素検出時のメッセージ表示方法の変更

既存のセキュリティスキャン機能は、スキャン用パターンデータに含まれる問題のレベル値に一意に対応（表1）した固定のメッセージを表示する仕組みとなっていた（図3①）。今回より、パターンデータにメッセージが格納されたタイプの問題を検出した際には、固定のメッセージは表示せず、代わりにパターンデータに格納されたメッセージを表示するよう移動端末の動作を変更した（図3②）。

### 5.3 その他の関連する機能

迷惑SMSメールの警告通知は、ユーザへ特定のSMSに対する警戒心を呼びかける機能である。そのため、本認識が浸透したユーザのために、セキュリティスキャン機能の有効／無効設定とは別に警告通知を有効／無効に設定できるメニューを用意した。なお、警告通知の設定は、セキュリ

\*8 TLS：SSLをインターネット標準技術として規定し、拡張されたプロトコル。SSLと比べ、暗号アルゴリズムやエラーメッセージ規定などが拡張されている。


表1 問題のレベル値と表示するメッセージの対応イメージ

問題のレベル値	表示メッセージ
レベル0	メッセージA
レベル1	メッセージB
レベル0	メッセージC
レベル1	メッセージD

パターンデータ		
問題要素Ⅰ	レベル0	(なし)
問題要素Ⅱ	レベル1	(なし)
問題要素Ⅲ	レベル0	メッセージG
問題要素Ⅳ	レベル1	メッセージH


拡張したエリア  
→メッセージを格納

①問題要素Ⅰ  
検出時の画面



パターンデータに  
メッセージがない場合

②問題要素Ⅲ  
検出時の画面



パターンデータに  
メッセージがある場合

図3 拡張したパターンデータおよび問題検出時の画面イメージ

ティレベルを落とさないようセキュリティスキャンの機能の設定が有効な場合にのみ、切替え可能なメニューとした。

## 6. あとがき

903iシリーズに搭載された新規アプリケーションとして、きせかえツール機能、マチキャラ機能、各社発行デジタル証明書対応機能、SMS迷惑メール対策機能について概説した。これらの機能の搭載により、移動端末のカスタマイズ機能やセキュリティ機能の向上を図った。

今後もより多彩なカスタマイズ機能や、より高度なセキュリティ機能の実現を目指し、ユーザからのさまざまな要求を満たした移動端末の開発を進めていく。