Development Reports

902i搭載 アプリケーション機能

FOMA902iシリーズに搭載する新規アプリケーションとして，トルカ機能，SD-Binding機能，Javaによるディジタル署名機能および個別課金機能を開発した．

大井 達郎　上田 誠
矢野 英司　為近 智行

1. まえがき

移動端末上のアプリケーション機能の飛躍的な高度化に伴い，さらなる利便性の向上を要求するユーザからの声が日増しに高まっている．

これらの要求を満たすため，FOMA902iシリーズにて既存のFeliCa®＊1機能，SD（Secure Digital）カードへのコンテンツ保存機能，移動端末セキュリティ機能に対して機能拡充を図った．FeliCa機能については，電子化されたクーポン券などの取得，表示，流通を可能とする機能を開発した．SDカードへのコンテンツ保存機能については，特定の条件でのみコンテンツを利用できる仕組みを開発することで，保存コンテンツの多様化を可能とした．移動端末セキュリティ機能については，移動端末上でディジタル署名を生成することを可能とした．

また，課金体系の多様化に対応するために，コンテンツごとの課金を可能とする機能も新規に開発した．

本稿では，これらの4つの開発機能の概要を解説する．

2. トルカ機能

2.1 サービスコンセプト

おサイフケータイの利用促進，および生活インフラとのさらなる連携強化を行うことを目的として，トルカ機能を搭載した．

トルカとは，既存の生活インフラにおいて紙ベースで流通されている店のクーポン券や会員証などを電子化したデータ（以下，トルカデータ）であり，またトルカデータを流通させ，移動端末上で表示させるサービスの総称でもある．トルカデータは，FeliCa，ブラウザ，メーラ，外部イ

＊1　FeliCa®：ソニー㈱が開発した非接触型ICカードの技術方式で，同社の登録商標．

ンタフェースなどにより移動端末内に保存，表示される．以下に，移動端末におけるトルカ機能の概要を述べる．

2.2 トルカデータの取得

トルカデータは，FeliCa機能を搭載したリーダ／ライタ（以下，R/W）に移動端末をかざしたり，ブラウザ起動中に着メロやデコメールテンプレートなどと同様にダウンロードすることで取得する．トルカデータは，使用する回線の転送レートなどにより種類が分かれ，トルカデータとして必要最低限の情報要素にサブセット化したデータ（以下，トルカスニップ）と，すべての情報要素を持つデータ（以下，トルカカード本体）の2つに大別される．

(1) FeliCaによる取得

R/Wに移動端末をかざすと，R/Wと移動端末のFeliCaチップ間で通信を開始し，自動的にトルカデータの取得，保存を行う．データの取得が完了すると移動端末はLED（Light Emitting Diode）の点滅や音の鳴動などでユーザへ通知する．FeliCaチップ間の通信方式は，フェリカネットワークス社が規定する通信プロトコルである三者間通信を利用しており，トルカデータは本通信のオペレータ固有情報領域に格納される．また，三者間通信はその性質上，送信データサイズが制限されるため，トルカスニップのみを送信対象としている．さらに，トルカスニップのデータサイズを低減するため，バイナリ形式のデータフォーマットとして送信される．ただし移動端末には，取得経路にかかわらず単一のデータフォーマットで保存するため，バイナリ形式のトルカスニップは取得後，移動端末内部でテキスト形式のフォーマットに変換される．

(2) ブラウザによる取得

ブラウザ上でトルカデータをダウンロードする場合，取得データの内容をユーザに確認させるため，トルカデータのプレビュー表示を行ったうえで保存を促す．ブラウザによる取得においては，前述した三者間通信と異なりデータサイズ制限を考慮する必要がないため，トルカスニップおよびトルカカード本体双方の取得が可能である．また，移動端末に具備された表示能力を最大限活用するために，HTML（Hyper Text Markup Language）をベースとしたテキスト形式のデータフォーマットを採用した．フォーマットの概要を**図1**に示す．

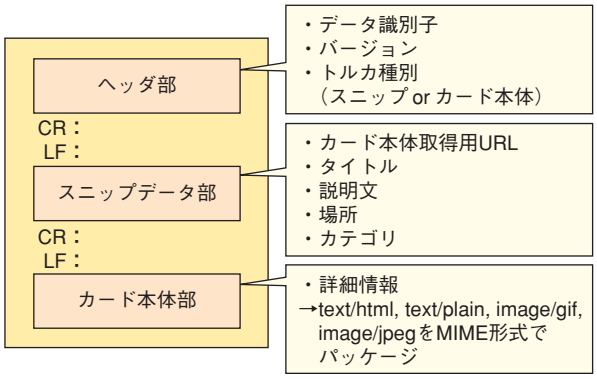

図1　トルカデータフォーマットの概要

2.3 トルカデータの表示

トルカデータはクーポン券などのカード類を電子化したものであるため，カードのように表示されることが望ましい．また，同一のトルカデータが異なる機種でも同様に表示される必要があるため，902i全機種に同一のトルカビューワを実装した．ビューワを**図2**に示す．

トルカスニップの表示は，プレーンテキストしか行えない．そのため，トルカスニップの情報要素として含まれるURL（Uniform Resource Locator）からトルカカード本体を取得し，情報更新する機能（以下，実体化）をビューワに設けた．また，ユーザが容易に実体化を行えるよう，トルカスニップ表示時には画面上に実体化ボタンを設置した．

トルカカード本体の表示においては，画像およびHTML形式のテキストが利用でき，トルカスニップと比較し豊かな表現が可能となる．また，HTMLタグにより，PhoneTo，WebTo，MailToなどの他機能との連携も実現した．

図2　トルカビューワの表示

2.4 トルカデータのエクスポート

トルカデータを移動端末同士で交換するために，メールへの添付や赤外線および外部メモリへのエクスポートを可能とした．ただし，902i移動端末のエクスポートはトルカスニップ形式のみを許容しており，トルカカード本体においては，その情報要素からトルカスニップを抽出しエクスポートを行う．そのため，インポート側の移動端末ではトルカカード本体に復元するために，前述した実体化を行う必要がある．

3. SD-Binding機能

3.1 サービスコンセプト

SD-Binding機能は，コンテンツなどの特定ファイルを暗号化しSDメモリに格納する際，暗号化に用いる鍵を取り出すのに必要な条件を併せて埋め込むことにより，ある特定の条件（FOMAカード，機種，iアプリなど）に適合している場合のみ，ファイルの復号化を可能とする技術である．

この機能を用いることで，さまざまな条件でSDカード内のコンテンツが読み書き可能な各種アプリケーションを提供することができる．具体的には，現在のi-modeのコンテンツプロバイダ（CP：Contents Provider）の意図に従ったコンテンツの著作権管理機能として提供することで，移動端末上のメモリ制約にとらわれず，必要なデータを削除することなくコンテンツのダウンロードが実現できる．また，ユーザが移動端末を変更する（あるいは故障時などに取り替える）際のスムーズなコンテンツ移行が可能となる．さらに条件の指定方法に「同一CPが作成したiアプリ」などといった概念を適用することにより，異なる複数のiアプリ間でのファイル共有など，新たなサービスの実現にもつながることが期待できる．

また，iアプリのデータをSDメモリに暗号化して格納することでSDカードの特徴である大容量を活かし，地図データ，i-motion，効果音／画像／セーブデータといった各種データを最大限に活用したゲームなどの大容量なiアプリを利用することも可能となる．

以下に，バインド種類について解説する．

3.2 バインド種類

SD-Binding機能でコンテンツを暗号化する際に用いる条件として，5種類の定義を行った．まず，i-modeコンテンツを保存する際の情報として，FOMAカード内にあるユーザ固有情報を用いる「UIM（User Identity Module）バインド」，機種情報とUIM固有情報をセットで用いる「機種バインド」の2種類を定義した（**図3**）．CPは，コンテンツダウンロード時のレスポンスに付与するHTTP（Hyper Text Transfer Protocol）ヘッダによって，これらの条件をコンテンツごとに指定することが可能であり，「UIMバインド」では異なる機種間のコンテンツ移動を，「機種バインド」では移動端末の保存容量拡大，あるいは故障時に代替機へと変更した際のコンテンツ消失リスクの低減をそれ

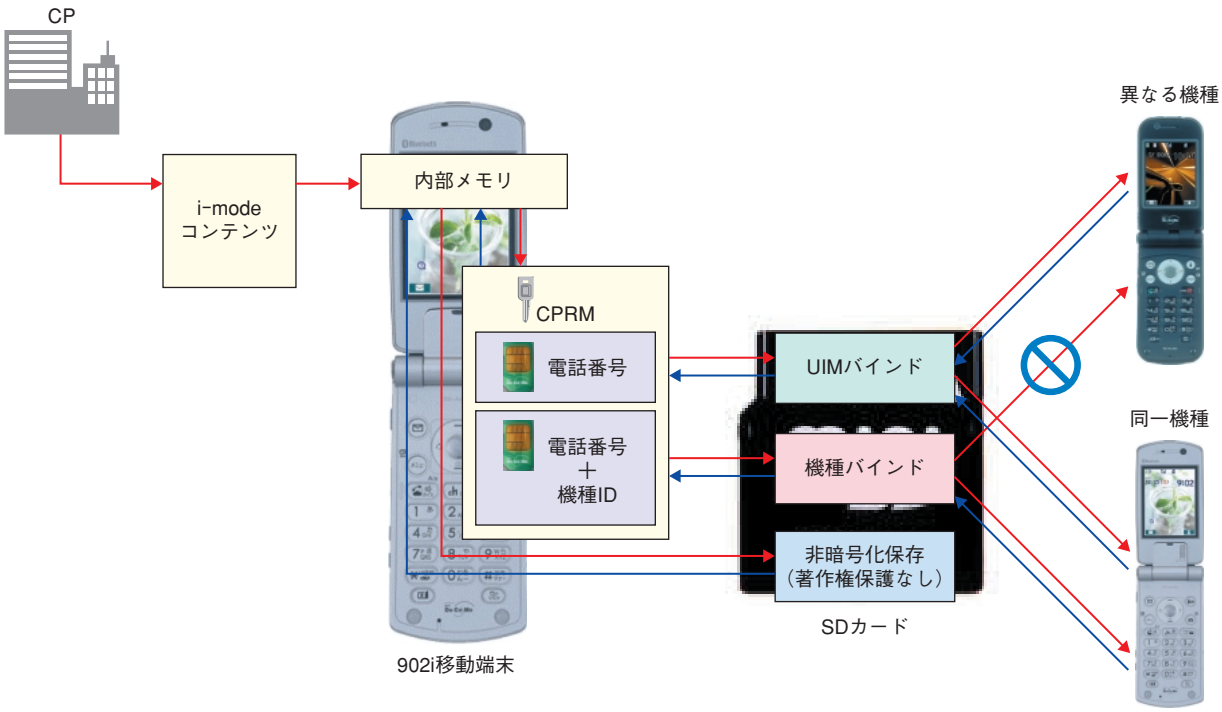

図3　SD-Bindingのバインド種別

ぞれ実現している．

また，iアプリが利用するデータへのアクセス条件として，i-modeコンテンツで用いている2種類のほかに，902iというような移動端末のシリーズ情報を暗号化に用いる「シリーズバインド」，そのデータを保存したiアプリのみにアクセス権限を与える「アプリバインド」，iアプリの提供者が同一であることを条件とする「CPバインド」の3種類を定義し，これらの条件を組み合わせて用いることを可能とした．これにより，単なるiアプリデータの大容量化だけでなく，複数のiアプリで同一のデータへアクセス可能となる．例えば，電話帳アプリのデータへメールアプリがアクセスするなど，小規模なアプリケーションの組み合わせにより大規模なアプリケーションが実現できる．

3.3 その他の機能

コンテンツを暗号化しSDメモリに保存する際，標準技術であるCPRM（Content Protection for Recordable Media）仕様およびSD-Binding仕様を利用することで，異なるメーカ間でも，SDカードを媒体としたコンテンツ移動あるいは共有が実現できる．

また，前述以外の工夫として，暗号化する際に各コンテンツのファイル種別やタイトルなどを示す情報をヘッダとして付与することにより，なんらかの条件によって利用できないコンテンツについても，ある程度の情報をユーザへ伝えることを可能とし，不要なファイルの識別の簡易化などSDカード上での検索効率化を図った．

さらに，単なる暗号化にとどまらず，着信音設定可否情報など各コンテンツが持つさまざまな属性情報を，PCなどでアクセスできないSDカード上の保護領域に保持することで，コンテンツ自体には含まれていない情報についても常に識別／処理可能とし，再生制限があるコンテンツの暗号化後における再生制限管理を可能としている．

4. Javaによるディジタル署名

4.1 サービスコンセプト

移動端末とCPなどとの通信において，相互間でやり取りを行うトランザクションデータ（HTML，画像など）に対するディジタル署名検証機能と，ディジタル署名生成機能を提供した．本機能により従来の電子認証サービスにおける，SSL（Secure Sockets Layer）通信による通信の暗号化，あるいは本人性認証のサービス提供に加えて，トランザクションデータの改ざん検知が可能となる．

4.2 機能条件

FOMA端末で展開されている電子認証サービスであるFirstPassの秘密鍵を用いることでディジタル署名生成機能を実現している．また，Java™*2アプリケーションをインストールすることでや法人の意思に沿った通信サービスを提供できることから，本機能においてもユーザの利用の自由度を向上させるため，Java（iアプリ）での機能提供を実現した．

4.3 ディジタル署名の機能

(1) ディジタル署名検証機能

CPなどから送信されたトランザクションデータに，CPからのディジタル署名が付与されている場合，移動端末にてCPの本人性認証およびトランザクションデータの改ざんの有無を検証可能とした．

本人性認証には，信頼性の基点となるトラストアンカとして移動端末の販売時にプリインストールされているRootCA（Root Certificate Authority）証明書を用いている．このRootCA証明書の所有者情報と，トランザクションデータに付与されたディジタル署名に含まれているCP証明書および中間CA証明書の各所有者情報と発行者情報を比較する．これにより，各証明書が上位証明書から適切に発行されているかを検証し，CP証明書の本人性，実在性確認を可能としている（**図4**①～③）．

トランザクションデータの改ざん検知については，ディジタル署名内に含まれるCP証明書の公開鍵を用いて，署名値の復号処理を行い得られた値と，移動端末側で同ハッシュ関数*3を用いてトランザクションデータから得られたハッシュ値を比較し，同一値であるかを確認することにより実現している．

署名検証可能なディジタル署名フォーマットは，一般的に普及されているPKCS#7SignedDataフォーマットに対応しており，また署名検証可能な署名アルゴリズムはsha-1withRSA，md5withRSA，md2withRSAに対応している．

(2) ディジタル署名生成機能

CPなどから送信されたトランザクションデータに対して，移動端末にてディジタル署名を生成し，トランザクションデータに付与することを可能とした（図4④）．

＊2　Java™：Java およびすべての Java 関連の商標およびロゴは，米国およびその他の国における米国 Sun Microsystems, Inc. の商標または登録商標．

＊3　ハッシュ関数：原文から固定長の擬似乱数を生成する演算手法．一般的に一方向関数が利用されるため，演算後のハッシュ値から原文を算出することができず，また同じハッシュ値を持つ異なるデータを作成することは極めて困難である．

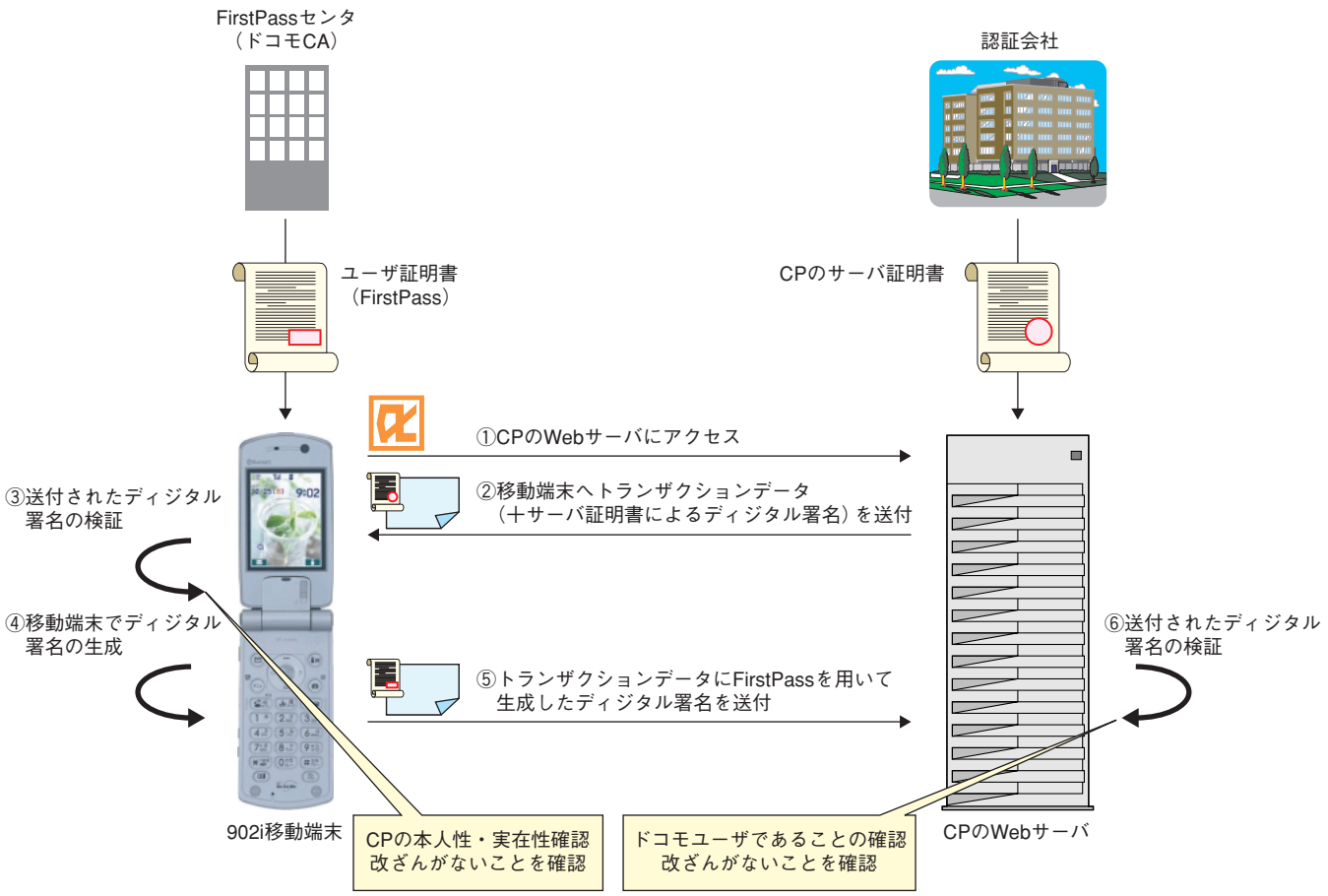

図4　ディジタル署名検証・生成イメージ

ディジタル署名生成にはFirstPassのユーザ証明書と対になる秘密鍵を用いている．この秘密鍵は耐タンパ性に優れたUIMに格納されており，また秘密鍵の読み出し処理はドコモ提供のアプリケーションからのみ可能とする設計としているため，iアプリからは扱えず機密情報の漏洩防止を実現している．また，不正に大量の署名生成処理が行われることによって秘密鍵による演算結果が取得され，大量の演算結果から秘密鍵値の予測が容易になるという脅威を防ぐために，署名生成時には移動端末のユーザに対してPIN2コード入力を必須とする仕組みとしている．

生成するディジタル署名フォーマットは一般的に普及しているPKCS#7SignedDataフォーマットに準拠しており，CPなどでも容易に署名検証が行えることを可能にしている．また，署名生成で利用する署名アルゴリズムは，sha-1withRSA，md5withRSAに対応している．

移動端末は，トランザクションデータに生成したディジタル署名を送付し，Webサーバ側で送付されたディジタル署名を検証する（図4⑤⑥）．

5. 個別課金

5.1 サービスコンセプト

パケット定額制の導入による現状の市場動向やユーザの利用傾向などを総合的に判断し，既存のi-modeサービスにおける有料コンテンツの課金体系である，サイトごとの月額課金に加え，コンテンツごとの課金を可能とする仕組みを提供し，i-modeサービスのさらなる利用を促進する．

5.2 個別課金の仕組み

コンテンツごとの個別課金を可能としているシーケンスおよび画面遷移を**図5**に示す．

①移動端末ブラウザを用いて対象サイトにアクセスし，対象コンテンツをダウンロードする処理（パスワード認証など）を経て，最終的にダウンロードを行う画面を取得する（図5①）．

②図5①の「ダウンロード」を行うタグには，「個別課金モード」に移行するための属性が記載されており，ユーザにより，その属性付きのボタンもしくはアンカーが押下された場合に，移動端末はその属性を判別

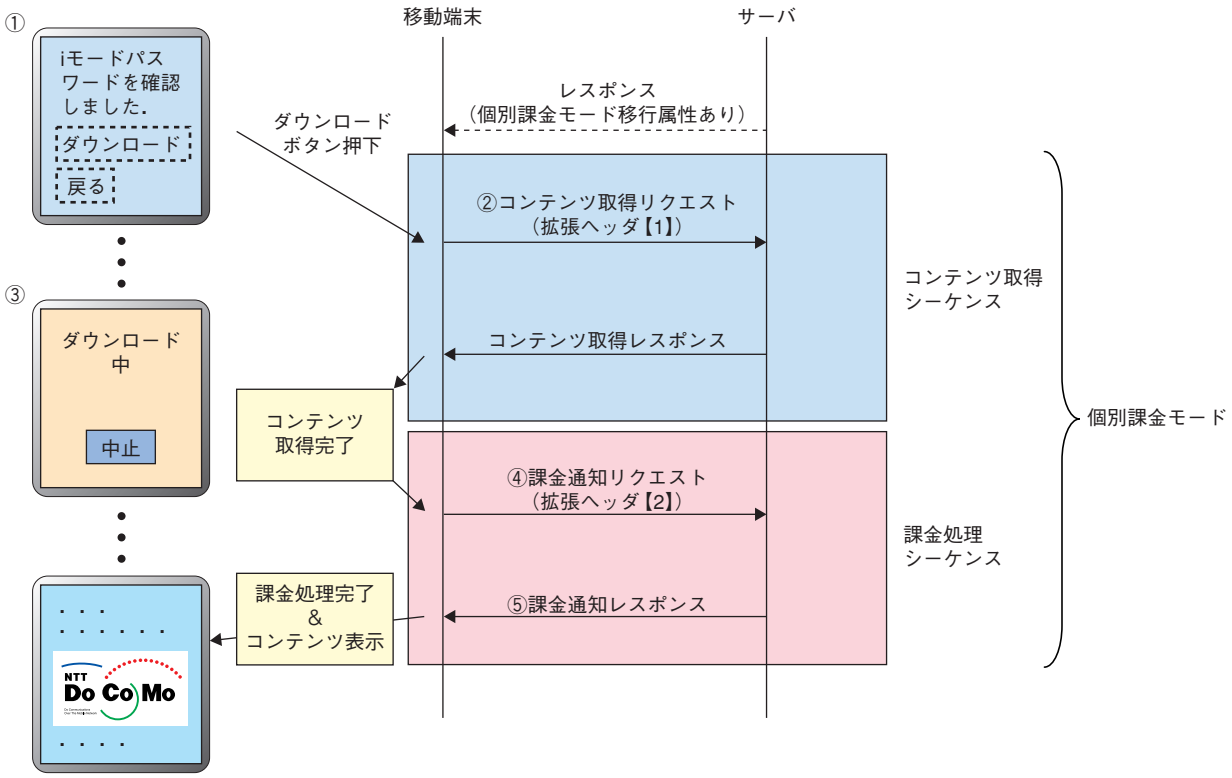

図5　個別課金基本シーケンスおよび画面遷移

し，これから個別課金モードでダウンロードすることを認識する．

③個別課金モードでダウンロードする際には，サーバ側からの指示を基にし，移動端末からのリクエスト信号に拡張ヘッダを付与する（図5②）．サーバはこの拡張ヘッダをチェックし，移動端末が正常に個別課金モードでダウンロードしているかどうかを随時確認する．また既存の機種では，ダウンロード中であってもコンテンツによっては，それまでに取得したものから随時表示することがあった．ただし，個別課金の機能としては，ダウンロード完了後に課金通知を行うため既存機種のように随時表示を行うと，課金処理がされないままに移動端末でコンテンツが閲覧できる事態が発生する．このような事態を避けるため，個別課金モードでは，ダウンロードし課金完了するまでは取得したコンテンツを表示しないこととする（図5③）．なお，コンテンツの取得については，個別課金用の拡張ヘッダが付与される以外は個別課金ではない通常のコンテンツ取得と同様である．

④コンテンツを取得完了した後，次に課金処理を行う．移動端末は，コンテンツを取得完了した時点で，自動的に内部で決められたURLにアクセスし，該当コンテンツをダウンロードしたことをサーバ側に通知する（図5④）．サーバは，移動端末からの通知を基に，移動端末側へレスポンスを返すとともに，ユーザへの課金処理を実行する．

⑤移動端末は，課金通知レスポンス（図5⑤）を受信した後，対象コンテンツの表示を行う．

5.3　通信不良に伴う課金通知の再送機能

移動端末では無線を利用した通信を行っているため，通信不良によるデータ取得の中断などが発生する可能性がある．取得が中断されると，これまで取得したデータはすべて破棄されてしまうが，通信料（パケット量）が発生し，ユーザに不利益を与えることも否めない．また，コンテンツはすべてダウンロードしており表示できる状態にはあるが，課金通知処理が完了していないために，コンテンツを表示することができないケースも存在してしまう．よって個別課金の機能として課金処理のみ失敗の場合に限り，課金通知の再送を促す機能を設けた．これにより，ユーザへの不利益を減少させた．

6.　あとがき

移動端末上に多様な機能が搭載される中で，FeliCaを利用したコンテンツの取得や課金体系の柔軟化といった，よりユーザビリティを高める機能およびコンテンツ保護・セ

キュア通信拡張といった，よりユーザセキュリティを高める機能の開発について述べた．

今後ますます，生活インフラとの連携強化の加速やセキュリティ機能要件への高まりが予想されるが，トルカ機能や移動端末上でのセキュリティ機能においても，さまざまな利用形態に対応するため，利便性の向上やビューワのさらなる改善などを実施していく予定である．

用 語 一 覧

CP：Contents Provider（コンテンツプロバイダ）
CPRM：Content Protection for Recordable Media
HTML：Hyper Text Markup Language
HTTP：Hyper Text Transfer Protocol
LED：Light Emitting Diode
RootCA：Root Certificate Authority
SD：Secure Digital
SSL：Secure Sockets Layer
UIM：User Identity Module
URL：Uniform Resource Locator