Development Reports

故障時における移動端末内のコンテンツファイル移行機能

故障修理時に限定して再配布不可コンテンツを暗号化し，ALADINを経由して故障移動端末から修理済みもしくは交換移動端末へ移行する機能を開発した．これにより，移動端末の故障による取替え修理において，修理完了後も再配布不可コンテンツの継続利用が可能となった．

内田 基之　山崎 雄一
三村 淳　有満 妃登美

1. まえがき

移動端末の多機能化に伴い，移動端末内部に保存できるコンテンツファイルの量・項目共に増加している．そのため，お客様にとってこれらのコンテンツファイルの重要性が増してきており，移動端末間のデータ移し替えの要望も増加している．

従来は，自然故障や移動端末の不具合などといった，お客様に起因しない故障があった場合でもコンテンツファイルの移し替え，特に再配布不可*コンテンツの移し替えができない状況にあった．これは顧客満足度（CS：Customer Satisfaction）を低下させる要因となるため，深刻な問題であった．しかし，この問題を解決し，さらに店頭にて即時にコンテンツファイルを移し替えることで，即時修理（販売品取替・預託品取替）が可能となり利便性の向上を図ることができる．そこで，これらを目的とした機能の開発を行った．

2. 開発の背景

i-modeでは，コンテンツ提供事業者（CP：Contents Provider）がユーザに対し安全に有料コンテンツを提供するために，i-modeコンテンツに著作権フラグ（以下，再配布不可識別子）を設定可能としている[1]．再配布不可識別子により移動端末外への出力が許可されていないコンテンツ（以下，再配布不可コンテンツ）の場合は，移動端末故障時でさえお客様が取得したi-modeコンテンツを移

＊　再配布とは，移動端末内に保存されているコンテンツファイルを，メール添付などを利用して移動端末外に取り出すことである．

行することができず，CSを向上させる上での課題の1つであった．

そこで，自然故障や不具合による故障受付時の移動端末交換において，再配布不可コンテンツの継続利用を可能とするため，CPから故障修理時に限定して外部出力を許容され，かつ暗号化された再配布不可コンテンツを顧客管理システム（ALADIN：ALl Around DoCoMo INformation systems）を経由して，故障移動端末から修理済み交換移動端末へ移行する機能[2]をFOMA（Freedom Of Mobile multimedia Access）の901iシリーズから搭載した．FOMA 901iシリーズでは静止画像および着信メロディが移行対象コンテンツである．

このシステムのポイントは，以下のとおりである．

①故障時に限り外部出力を許容された再配布不可コンテンツの管理機能

②移動端末における暗号化／復号化エンジンの実装

③故障時におけるコンテンツに対する移行可否の付与

本稿では，故障時における移動端末内のコンテンツファイル移行システムの概要，ALADINでのコンテンツ管理機能，システムを構成する移動端末機能，故障時移行可否の付与について解説する．

3. システム概要

故障時コンテンツファイル移行システムの概要を**図1**に示す．本システムは，お客様が移動端末に保存していた各種データのうち，CPから“移動端末の故障時に限り外部出力を許容された再配布不可コンテンツ（以下，故障時移行可コンテンツ）”を，ユーザおよび機種の特定が可能な情報を用いて暗号化した後，ALADINを経由して“修理済みの移動端末”もしくは“交換された同一機種の新しい移動端末”（以下，合わせて「修理済み交換移動端末」）へ移行可能とする機能である．

なお，即時修理が必要な場合には移動端末を取り替えることから，製造番号は故障移動端末と修理済み交換移動端末で同一とは限らない．

(1) コンテンツ取得

CPサーバからi-modeコンテンツを取得する際に，i-modeコンテンツ本体と合わせて故障時移行可否を示すHTTP（HyperText Transfer Protocol）ヘッダ（以下，故

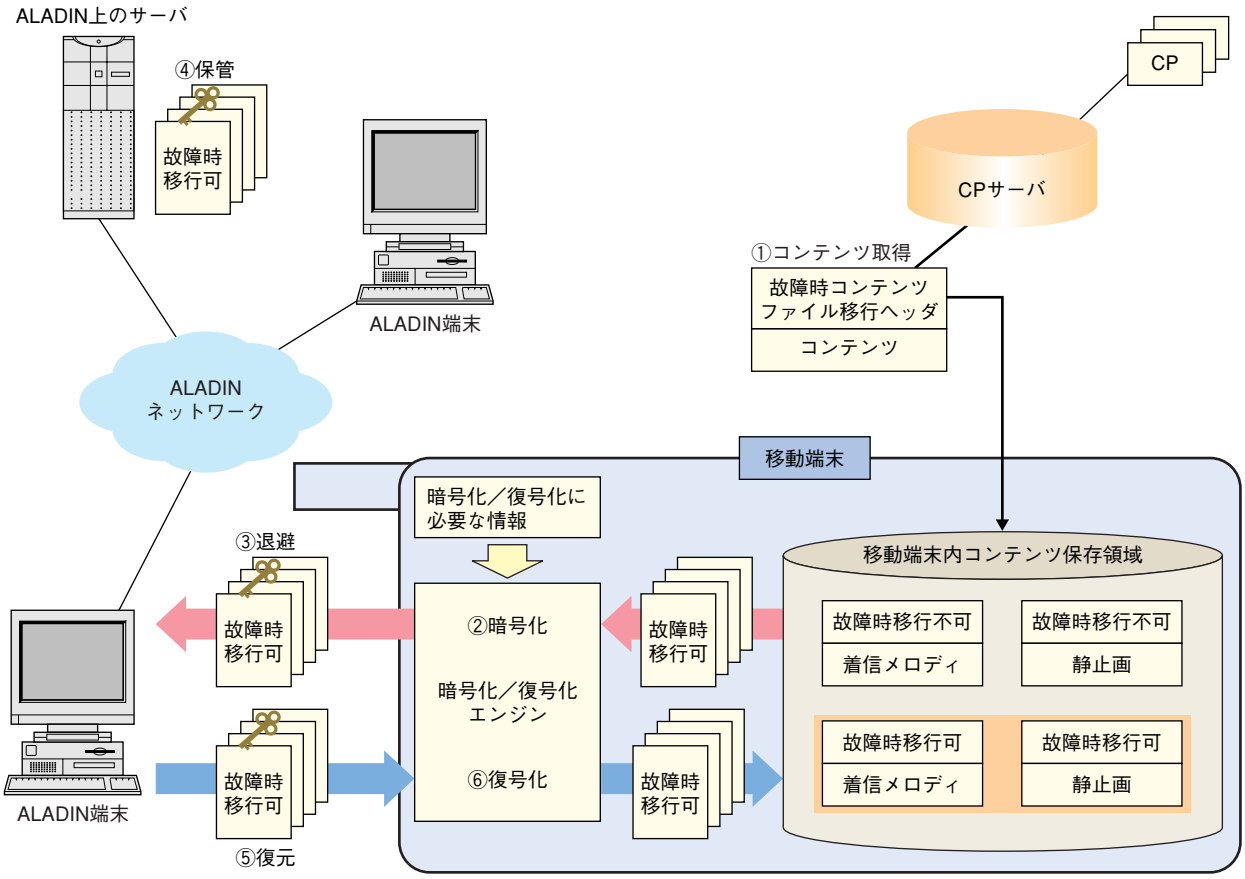


図1　故障時コンテンツファイル移行システム概要

障時コンテンツファイル移行ヘッダ）を合わせて取得し（図1①），移動端末内では，故障時コンテンツファイル移行ヘッダの値とi-modeコンテンツをセットで管理する．なお，故障時コンテンツファイル移行ヘッダの値が設定されていない場合は，故障時においてもコンテンツファイル移行機能は適用されない．

⑵退避処理

故障移動端末をALADIN端末へ接続したのち，ALADIN端末からの指示により移動端末内のコンテンツ保存領域に格納されている故障時移行可コンテンツを暗号化し（図1②），暗号化した故障時移行可コンテンツをALADIN端末へ退避させる（図1③）．即時修理の場合は故障時移行可コンテンツをALADIN端末内に一時保存するが，預かり修理など，修理済み交換移動端末への復元作業まで数日を要する場合は，ALADINネットワーク上にあるサーバで保管する（図1④）．

⑶復元処理

修理済み交換移動端末をALADIN端末へ接続したのちALADIN端末からの指示により，暗号化した故障時移行可コンテンツを修理済み交換移動端末へ復元する（図1⑤）．ALADIN上のサーバに暗号化された故障時移行可コンテンツが保管されている場合は，一度ALADIN端末内へダウンロードし，その後修理済み交換移動端末へ転送する．修理済み交換移動端末は，暗号化された故障時移行可コンテンツを受信・復号化し（図1⑥），移動端末内のコンテンツ保存領域へ格納する．

なお，故障時コンテンツファイルの移行作業を行うのは，故障受付窓口の特定担当者に限定しており，移動元から移動先へ移動されたデータは，コピーファイルが残らないよう退避／復元処理の完了時に移動元から完全に削除される．

4. コンテンツ管理機能

お預かりしたコンテンツは改ざん，喪失，盗難の危険から守られ，確実にお客様に返却されることが重要である．したがって，ALADINのデータセンタにコンテンツを転送し，信頼性，可用性の高いサーバで保存することとした．

⑴データセンタにおける信頼性の確保

ALADIN端末を介して移動端末から移行したコンテンツは，ALADINのデータセンタへ転送され，保管される．ALADINは閉域網で構成され，かつ端末からデータセンタへのメッセージは厳しく規制・管理されているため，保管されているコンテンツへのアクセスは困難である．また，コンテンツを格納するサーバおよびストレージは冗長構成をとり，万一故障が発生してもデータの喪失を防いでサービスの継続を保証する．

⑵データ転送におけるシーケンス制御と状態管理

お預りしたコンテンツは複製を持つことを禁じられている．したがって，移行元から移行先へコンテンツの移動が確認でき次第，元のデータを確実に消去しなければならない．このため，コンテンツの移動状況をシーケンス制御し，移動状態を管理する．その概要は次のとおりである．

①故障移動端末からコンテンツを移行する場合，まずALADIN端末に一時的にデータを格納し，格納完了が確認できると故障移動端末内のコンテンツを削除する．

②ALADIN端末からデータセンタにコンテンツを移行する際も，格納完了後にALADIN端末内のコンテンツを削除する．

③データセンタに保管されるコンテンツは，故障修理完了時に暫時ALADIN端末に移行され，さらに修理が完了した移動端末に移行される．移動端末への移行が確認されると，ALADIN端末とデータセンタのコンテンツを削除する．

④不要になったコンテンツをALADINに残さないため，故障受付から一定期間経過したコンテンツは自動的に削除する．

故障移動端末から故障時移行可コンテンツをALADINへ移行する処理フローを**図2**に，故障完了・移動端末取替時にALADINから移動端末へデータを復元する処理フローを**図3**に示す．

5. 故障時コンテンツファイル移行機能対応移動端末

5.1 暗号化／復号化エンジンの実装

故障時にコンテンツファイルを移行する際，移動端末とALADIN端末間で暗号化された故障時移行可コンテンツを送受信している．これは，再配布不可コンテンツを外部出力した際，移動端末外部で不正使用されることを防止するために搭載した機能である．また，同一機種，同一のお客様の移動端末にのみ故障時移行可コンテンツを移行可能とするため，機種特定情報ならびにユーザ特定情報を暗号化／復号化処理に使用することとした．

⑴暗号化処理

暗号化処理手順概要を**図4**に示す．故障時移行可コンテンツ（以下Cntと表記）を暗号化するための鍵（コン

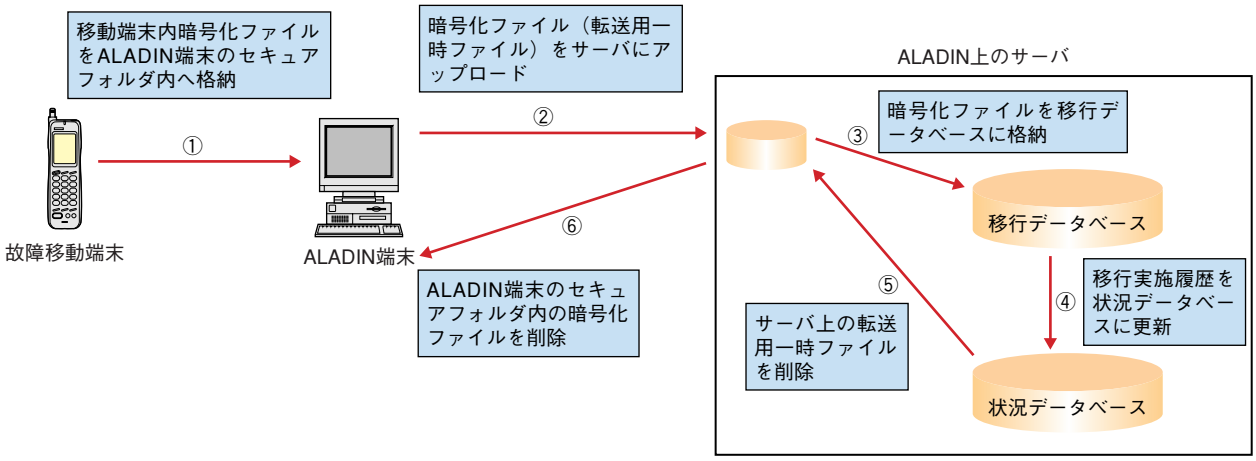


図2　コンテンツファイル移行時処理フロー

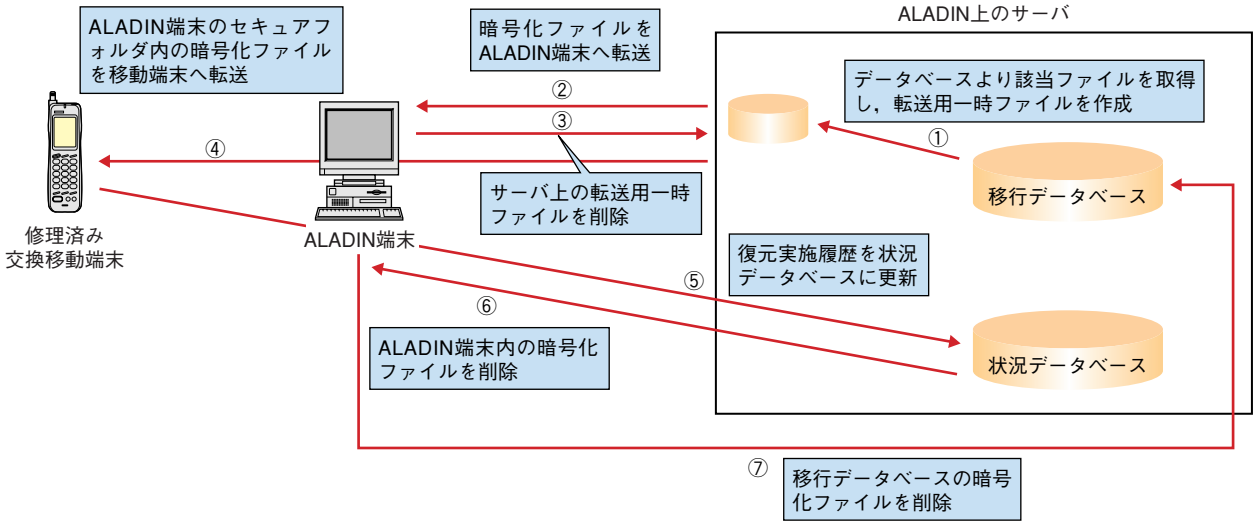


図3　コンテンツファイル復元時処理フロー

テンツ鍵Kc）を，移動端末内部の情報を用いて生成（図4①）した後，故障時移行可コンテンツを暗号化し，暗号化コンテンツE(Kc, Cnt）を生成する（図4②）．なお，故障時移行可コンテンツを暗号化するためのアルゴリズムは，任意のアルゴリズムを使用することが可能であり，端末実装メモリ容量を多く必要としないものを選定している．

続いて機種特定情報ならびに，ユーザ特定情報を用いてコンテンツ鍵Kcを暗号化するための鍵（固有鍵Kti）を生成（図4③）した後，コンテンツ鍵を暗号化し暗号化コンテンツ鍵E(Kti, Cnt）を生成する（図4④）．

さらに復号者の正当性確認を実施するためのコンテンツ鍵Kcのハッシュ値Hc(Kc）を計算する（図4⑤）．最後に暗号化コンテンツE(Kc, Cnt)，暗号化コンテンツ鍵E(Kti, Kc)，コンテンツ鍵ハッシュ値Hc（Kc）を1つにまとめて暗号化ファイルを生成する．

上記手順にて生成した暗号化ファイルをALADIN端末へ送信する．

(2) 復号化処理

復号化処理手順概要を**図5**に示す．ALADIN上で一時保存されていた暗号化ファイルを受信した移動端末は，機種特定情報ならびにユーザ特定情報を用いて暗号化コンテンツ鍵E(Kti, Kc）を復号するための固有鍵Ktiを生成し（図5①），コンテンツ鍵Kcを復号する（図5②）．復号されたコンテンツ鍵Kcのハッシュ値Hd(Kc）を計算し（図5③），暗号化ファイルに格納されていたコンテンツ鍵ハッシュ値Hc(Kc）との比較検証を実施する（図5④）．図5①の手順にて生成した固有鍵Ktiが暗号化処理時と異なる場合は，図5④の比較検証時にハッシュ値が一致しないため，コンテンツ鍵Kcが正しい固有鍵Ktiで

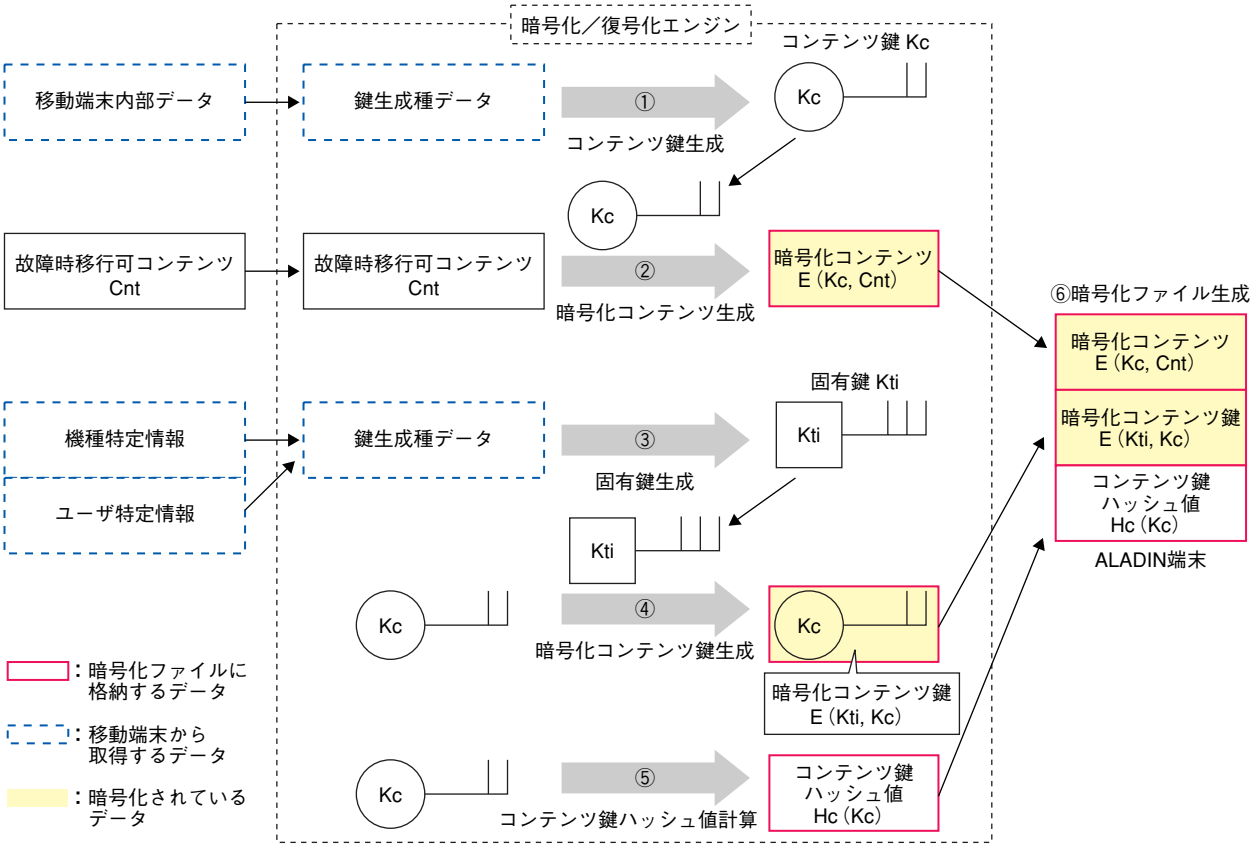


図4　暗号化処理手順概要

復号されていないことが分かる．つまり，機種特定情報もしくはユーザ特定情報のうち，少なくとも1つが暗号化時に使用したものと異なっていることが分かる．

このように，暗号化されている故障時移行可コンテンツを復号する前に，復号に使用するコンテンツ鍵Kcの検証を実施することにより復号者の正当性を確保している．

検証の結果，問題ないことが判明した場合は暗号化コンテンツを復号し，移動端末へ格納する（図5⑤）．

5.2 故障時移行可否確認機能

移動端末内に保存されているコンテンツに対して，故障時コンテンツファイル移行機能での移行対象かどうかを確認できるようにするため，ALADIN端末で故障時移行可コンテンツ一覧を取得する機能ならびに，お客様自身が端末操作によりコンテンツ詳細情報表示にて故障時移行可否を表示させる機能を実装している．これにより，故障受付来訪前に故障時移行可否を確認することが可能となっている．

6. 故障時移行可否の付与

再配布不可識別子はDRM（Digital Rights Management）機能の1つである．DRM機能を実装することは，CPがユーザに対し安価にかつ安全に有料コンテンツを提供するために重要なものであり，i-modeビジネスを実現する上で必須となる機能である．しかしながら，2章で記載したように移動端末故障の場合でさえ，修理済み交換移動端末にお客様が取得したi-modeコンテンツを移行することができず（**図6**①），CSを向上させる上での1つの課題であった．そこで，故障時に再配布不可コンテンツを修理済み交換移動端末に移行可能な新たな仕組みを設けることとした．

故障移動端末内の再配布不可コンテンツを修理済み交換移動端末に合法に移行させるためには，故障時であり同一機種であることに限定して移行することをCPに許容してもらう必要がある．また，既存のi-modeコンテンツもあるため，故障時移行可否の付与方法は，運用面と技術面の両面からみて最適な方法が望まれる．

具体的な故障時コンテンツファイル移行可否付与方法は，コンテンツ配信時にHTTPレスポンスヘッダに**表1**のような故障時コンテンツファイル移行ヘッダを指定する方法である（図6②）．本仕組みを採用することは，移動端末およびサーバの両方にとって望ましい方法である．サーバ側に関していえば，CGI（Common Gateway Interface）の変更やサーバの設定変更による一括付与が可能となるため，

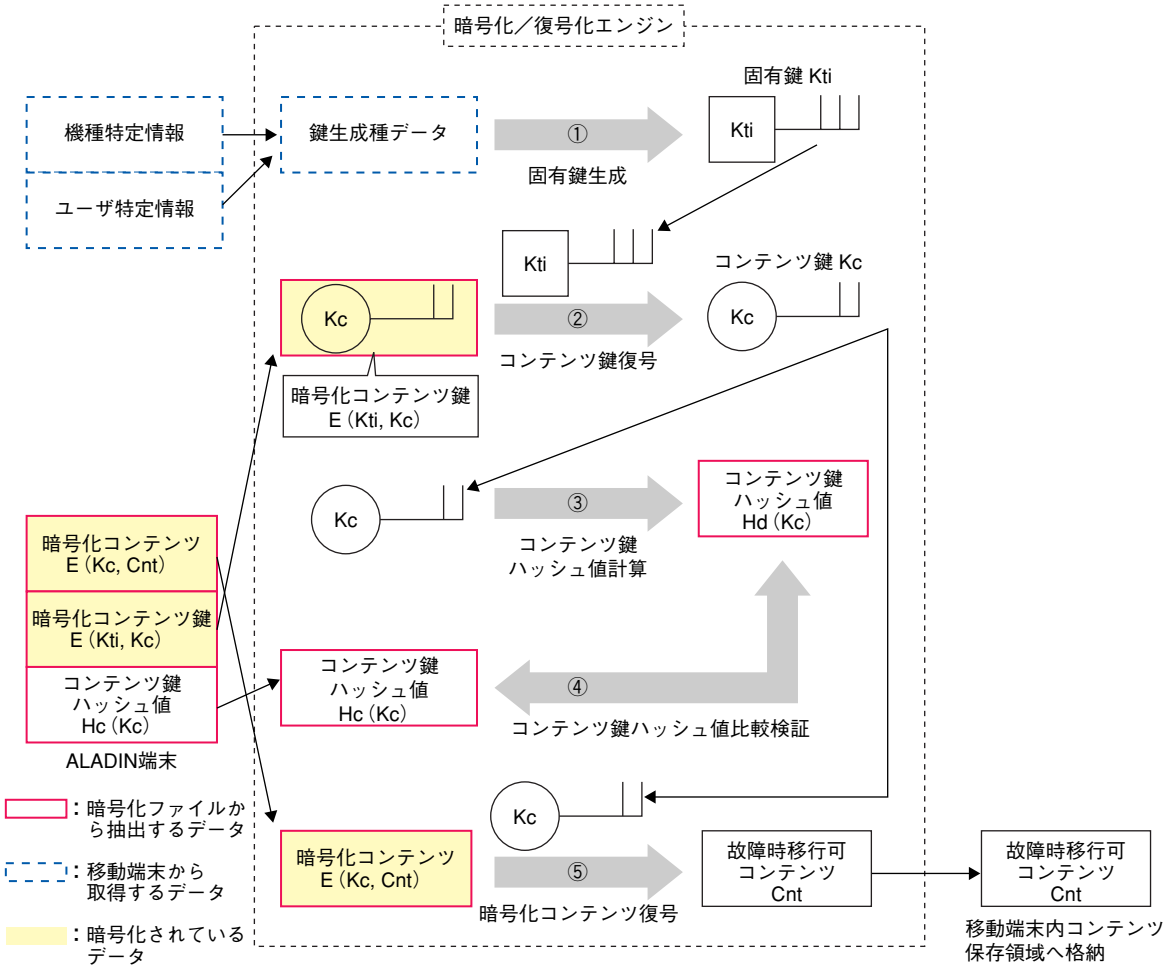
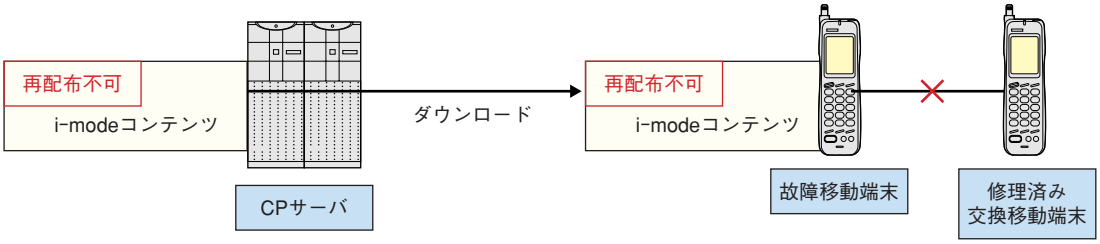
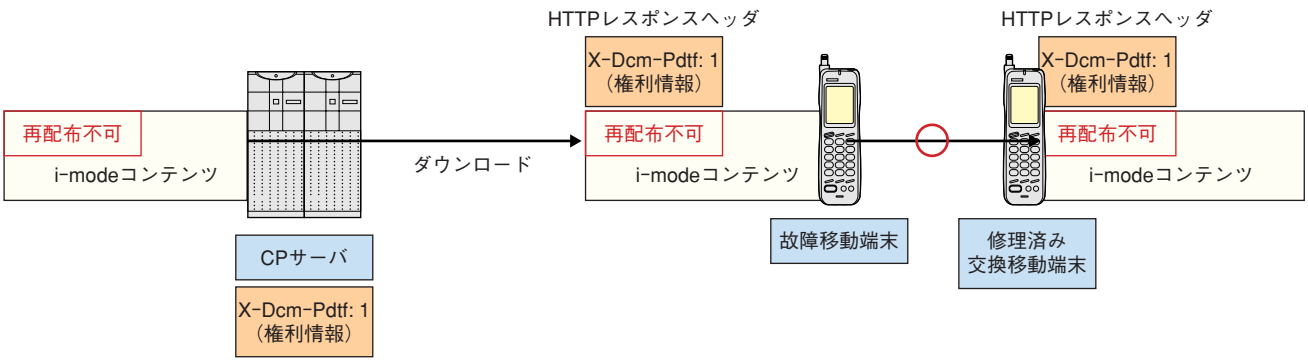


図5　復号化処理手順概要



①故障時コンテンツファイル移行機能に非対応の場合



②故障時コンテンツファイル移行機能に対応の場合

図6　再配布不可コンテンツの流れ

表1　故障時コンテンツファイル移行ヘッダ

故障時コンテンツファイル移行ヘッダ	故障時コンテンツファイル移行
X-Dcm-Pdtf: 0	―
X-Dcm-Pdtf: 1	○
上記以外	―

比較的容易にCPが既存コンテンツに対しても故障時コンテンツファイル移行ヘッダを付与することが可能となる．また，端末技術という観点では，ファイル種別に依存することなく，どのコンテンツファイルにも適用可能であり拡張性を持った手法となる．

7. あとがき

本稿では，故障修理時における移動端末内のコンテンツファイル移行機能についてシステム概要，移動端末機能，コンテンツ管理機能，故障時移行可否の付与について述べた．今後はさらなるCS向上が達成できるようサービス検討を行い，その実現に向けた技術開発を進めていく予定である．

文　献

[1] ドコモホームページ内「DRMとは」
（http://www.nttdocomo.co.jp/p_s/imode/make/drm/index.html）
[2] ドコモホームページ内「故障時コンテンツファイル移行機能」
（http://www.nttdocomo.co.jp/p_s/imode/make/drm/index.html）

用　語　一　覧

ALADIN：ALl Around DoCoMo INformation systems
（顧客管理システム）
CGI：Common Gateway Interface
CP：Contents Provider（コンテンツ提供事業者）
CS：Customer Satisfaction（顧客満足度）
DRM：Digital Rights Management
FOMA：Freedom Of Mobile multimedia Access
HTTP：HyperText Transfer Protocol