携帯電話におけるコンテンツ退避保護方式の実装と評価

内田基之[†] 鈴木利始[†] 小島久和[†] 水口武尚[‡] 秋山康智[§] 神戸英利[§]
[†]株式会社NTTドコモ移動機開発, [‡]三菱電機株式会社情報技術総合研究所
[§]三菱電機株式会社モバイルターミナル製作所

近年、CPUの高性能化、メモリ容量増大化に伴い、携帯電話が制御できるコンテンツの種類および量が飛躍的に拡大したことにより、i-モード等のインターネットサービスによるコンテンツ（静止画、動画、Javaアプリケーション、着信メロディ等）の販売ビジネスが急速に発展してきた。また個人情報保護法の施行により、個人データのセキュアな管理の必要性が高まっている。本稿では、個人データを携帯電話内の電話帳やメールのような個人情報を含むデータと個人購入コンテンツの総称として定義し、携帯電話の機種交換や障害発生時における、個人データのセキュアな管理方法について考察し、携帯電話上での実装および性能評価を実施した。

Implementation and Evaluation of a Personal data Transfer and Protection Method for cellular phones

Motoyuki UCHIDA[†], Toshiharu SUZUKI[†], Hisakazu KOJIMA[†],
Takehisa MIZUGUCHI[‡], Hidetoshi KAMBE[§], Koji AKIYAMA[§]
[†]NTT DoCoMo, Inc. Customer Equipment Development Dept.
[‡]Mitsubishi Electric Corp. Information Technology R&D Center
[§]Mitsubishi Electric Corp. Mobile Terminal Center

The recent increases in CPU performance and memory size have enabled cellular phones to handle more varieties and larger sizes of content in a considerable manner. These expansions have triggered rapid development of the business for Internet sales of content (such as images, movies clips, Java applications, ring tones, etc.) from services like i-mode. Furthermore, the need for secure management of personal data has been increasing since the Personal Information Protection Law was enforced.. In this report, we first define personal data as data containing personal information (such as those found in phone book or emails stored in cellular phones) and/or content purchased by an individual. We then examine a method for secure management of personal data during exchange of cellular phones or other abnormal circumstances. Finally, the details of the implementation on an actual phone and performance evaluation results are described.

1. はじめに

近年、CPU の小型化高性能化、メモリ容量増大化に伴い、携帯電話が扱うコンテンツの種類および量が飛躍的に拡大したことにより、i-モード等のインターネットサービスによるコンテンツ（静止画、動画、Java アプリケーション、着信メロディ等）の販売ビジネスが急速に発展してきた。また個人情報保護法の施行により、個人データのセキュアな管理の必要性が高まっている。本稿では、携帯電話内の電話帳やメールのような個人情報を含むデータと個人購入コンテンツの総称を個人データとして定義し、携帯電話の機種交換や障害発生時における、個人データのセキュアな管理方法について考察し、携帯電話上での実装および性能評価を実施した。

2. 背景、目的

今回我々が目指したのは、「携帯電話における機種交換時、移動機障害時における安全な個人データの退避および復元方式」である。従来、機種変更時は有料コンテンツ（i アプリ、着信メロディ、画像データ）をはじめ、メモリダイヤルを除く個人データが交換後の携帯電話で継続して使用ができないという問題があった。また上記個人データの漏洩を明確に防止する方式が確立していなかった。そこで今回、我々は、個人データのセキュアな管理方式について注目し、検討をすすめた。特に移動機外への持ち出しを禁止されているコンテンツを移動機外に持ち出す場合、コンテンツの 2 次利用、改竄を防止する必要があるため、以下のセキュリティ要件を満たすものとした。

- 移動機の所有者は同一であることを保障
- 移動機外部に取り出したデータは、移動機外部では使用できないことを保障
- データの唯一性の保障

3. 個人データ退避システム

3.1. システム概要

図 1 に本システムの構成を示す。本システムは、移動機端末とその個人データを退避するための PC で構成され、その機器間を USB で接続する。

個人データを退避する場合、まず移動機内で格納された個人データに対して OBEX(OBject EXchange Protocol)ベースに共通フォーマット化を行い、さらに暗号化（カプセル化）を行い、退避用パッケージを作成する。この退避用パッケージのフォーマットで PC へ転送し、退避を行う。本プロトコルは、携帯電話端末に共通に実装されており、他機種交換時の退避・復元を可能にするため採用した。なお、個人データの唯一性確保の観点から、PC へ転送した個人データは移動機から削除することとした。

また、PC へ退避した個人データの復元を行う場合、退避用パッケージを退避先 PC から移動機端末に転送する。退避用パッケージを受信した移動機端末は、復号化（脱カプセル化）を行い、共通フォーマットデータを得る。このデータから個人データを取り出し、適切な保存領域に格納する。この際、機種端末情報等を用いて、データの互換性を確認することにより、不適切な移動機端末上への復元を抑制する。退避時と同様に移動機へ格納した個人データは PC 上から削除される。

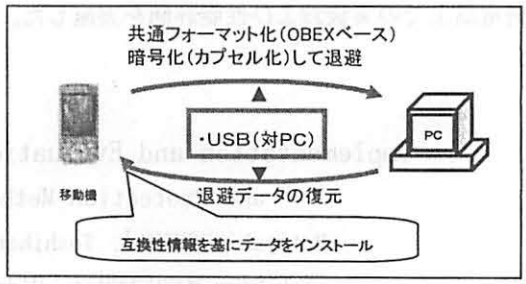

図 1 システム概要

3.2. 個人データ管理方式

移動機端末から PC へ退避する個人データは、改竄、盗難から確実に保護する必要がある。よって退避する個人データを以下の様に扱うこととした。

- 移動機端末上で暗号化を行う。
- カプセルヘッダに個人データ所有者特定用の ID を付与し、個人データと移動機端末の関係付けを行う。

3.2.1. 個人データのフォーマット変換

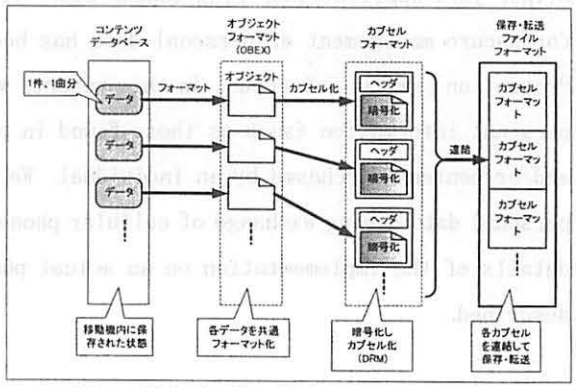

図 2 個人データの退避パッケージ変換

図 2 に個人データの退避パッケージ変換について記す。退避パッケージ変換は、以下の段階で行う。

(1) 移動機内個人データの共通フォーマット化

移動機内データベースに格納されている個人データを、携帯端末での標準転送プロトコルであるOBEXに準拠したフォーマットに変換する。これにより移動機端末上で個人データ復元の際、このフォーマットをベースに適切な保存領域に格納することができる。本機能は移動機端末の標準機能として組み込まれており、今回、その機能を利用するため、本フォーマットを採用した。

(2) 共通フォーマットデータの暗号化(カプセル化)

共通フォーマット化した個人データを暗号化し、付加情報を格納したヘッダを付与したカプセルフォーマットに変換する。これにより第三者による改竄の防止、情報漏洩の防止が図れる。

(3) カプセルフォーマットデータの退避パッケージ化

退避パッケージは、カプセルフォーマットデータを連結し、1つのファイルにしたものである。これにより転送時のオーバーヘッドを軽減し、転送効率の向上を図った。

4. 実装

本章では、実装したシステムの概要および動作シーケンスについて記す。

4.1. 実装システム概要

図3に実装システム概要を記す。

本システムは、移動機端末と退避先PCで構成される。

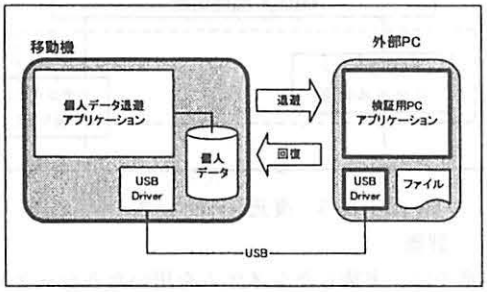

図3 実装システム概要

・移動機

FOMA D2101Vをベースとし、個人データ退避機能を追加した試作機。PCとUSBで接続し、退避・復元を行う。

・検証用PCアプリケーション(PC上)

移動機の個人データ退避機能を確認するための、PC上のアプリケーション。移動機とUSBで接続し、退避・復元を行う。

PCと移動機間は、USBで接続されOBEXプロトコルによりデータは転送される。転送データは個人データを暗号化したものであり、また、PCへ退避したデータはファイルに格納される。退避・復元処理の操作はPCより行い、移動機はPCからの要求に応じて動作する。

4.2. サポートコンテンツ

個人データとして以下のデータをターゲットにした。

データカテゴリ	フォーマット
アドレス帳	vCard2.1
Bookmark	vBookmark 1.0
着信メロディ	MFi, MFi2, MIDI
イメージ	GIF
	JPEG
スケジュール	vCalendar 1.0
iアプリ	iアプリフォーマット
iモーション	ASF
	ALS(独自フォーマット)

表1 個人データサポートコンテンツ

この他に移動機の互換性情報や個人データの転送結果を転送・保存するために以下の参照データを採用した。

・ 互換性チェック情報

互換性チェック情報は、カテゴリ毎の個人データの移動機端末への格納条件を表すものである。PCからの要求に応じ、移動機からPCへ転送され、PC側で移動機が格納できないデータをフィルタリング(互換性チェック)するために用いる。

・ 移動先移動機格納データログ

移動先移動機格納データログは、格納結果記載したログファイルであり、移動機側で作成するものと、外部PC側で作成するものがある。移動機側で作成するものは、外部PCから個人データを復元する場合に作成される。外部PCからの要求によって外部PCへ転送される。外部PC側で作成するものは、外部PCから移動機へ個人データを復元する際、互換性チェックによるフィルタリング結果が書き込まれる。

4.3. 動作シーケンス

4.3.1. データ退避シーケンス

PCへ移動機の個人データを退避(移動)する際の動作シーケンスを図4に示す。概要を以下に示す。

(1) USB上にシリアル回線を接続

(2) OBEX のコネクションを確立
(3) PC がパッケージファイルを要求
(4) 移動機はパッケージファイルを生成
(5) 移動機はパッケージファイルを送信
(6) PC はパッケージファイルを受信し、ファイルとして保存。
(7) PC が移動機へデータの削除を要求
(8) 移動機は要求されたカテゴリの全データを削除
(9) (3) ～ (8) をカテゴリ毎に繰り返し
(10) OBEX のコネクションを切断
(11) USB 上のシリアル回線を切断

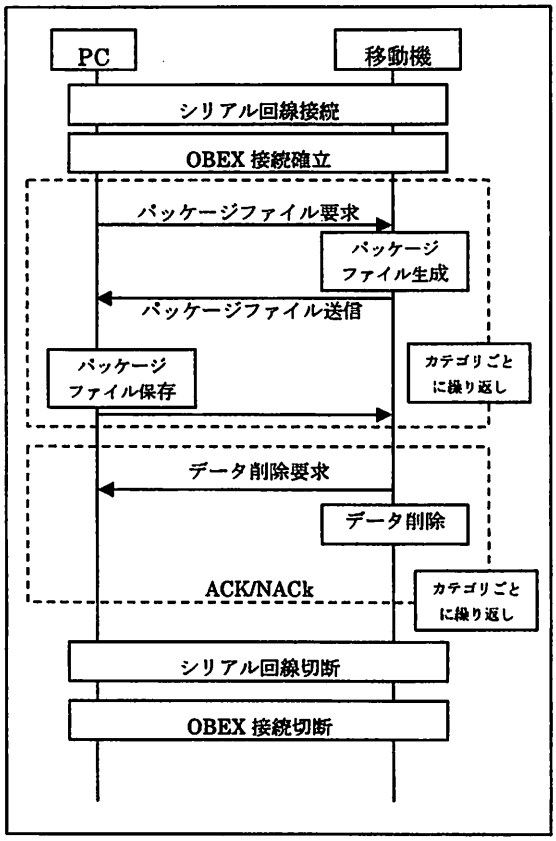

図 4 退避シーケンス

4.3.2. データ復元シーケンス

PC へ移動機の個人データを復元する際の動作シーケンスを図 5 に示す。

(1) USB 上にシリアル回線を接続
(2) OBEX のコネクションを確立
(3) 互換性チェック情報を要求と送信
(4) PC の互換性チェック
(5) PC がパッケージファイルの送信
(6) 移動機は復元するカテゴリの全データを削除
(7) 移動機は受信したパッケージファイルを解析し、各データをデータベースへ追加
(8) 格納データログ情報を要求と送信
(9) (3) ～ (8) をカテゴリ毎に繰り返し
(10) OBEX のコネクションを切断
(11) USB 上のシリアル回線を切断
(12) PC 上のパッケージファイルを削除

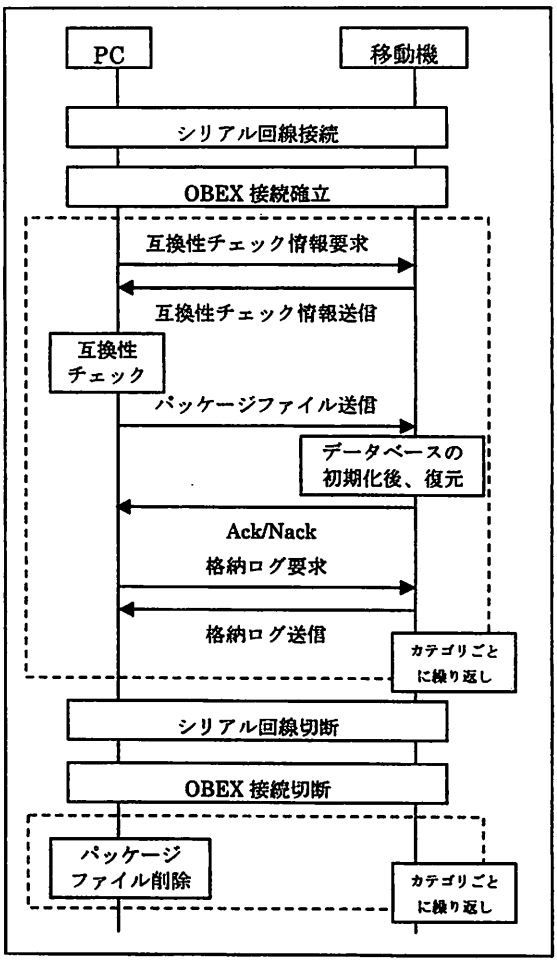

図 5 復元シーケンス

5. 評価

本章では、実装したシステムを用いた各シーケンスにおける性能評価について記す。

5.1. 評価環境

本評価は、図 3 に示す構成で行った。

PC : CPU:Pentium3.0/1GHz、メモリ 512MB
移動機端末 : D2101V (45MIPS)
USB : USB1.1

5.2. 評価項目

本評価は、実装した移動機がサポートする表 2 に

示す個人データの各カテゴリに対し、退避および復元における時間を図4、図5に示す各段階ごとに測定した。また、データ数は、実装移動機が格納できる最大数で評価を行った。

また、本システムは、1対1のローカル通信であり、外的影響が極めて少ないため、測定回数は4回とし、その平均値を取った。

データカテゴリ	内容
電話帳	700件
スケジュール	50件
ブックマーク	50件
着信メロディ	500件
静止画	500件
動画	156件
Javaアプリ	100件

表2　評価試験データ

5.3.　結果と考察

図6に退避時における性能評価の結果を示す。

データベース読込時間については、静止画が同じ500件の着信メロディの約30倍以上である。これは、着信メロディをデータベースから読み出す際、データベースのopenとcloseを全件読み出しの最初と最後に行うのに対し、静止画では1件毎にopenとcloseを行っていたことに起因する。これは動画も同様である。電話帳で時間を要しているのは、名前を保存するデータベースと電話番号等を保存するデータベースの2つで構成されており、このためレコードのサーチ、呼び出し回数が増えることによるものである。

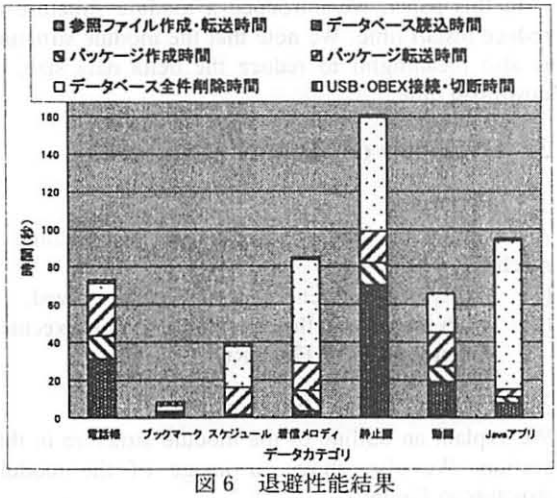

図6　退避性能結果

パッケージフォーマット時間(暗号化＋カプセル化時間)および転送時間は、データサイズにほぼ比例している。

データベース全件削除時間について、着信メロディ、静止画、動画は、管理情報をデータベースに登録し、データファイルをファイルシステムへ登録するように構成されており、その対応関係を保つために1件ずつ削除しているため、時間を要している。

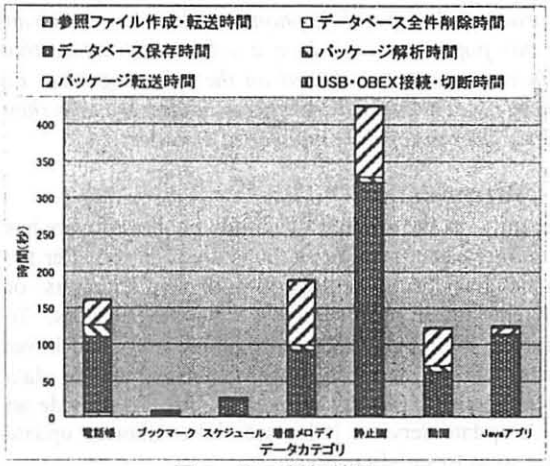

図7　復元評価結果

図7に復元時における性能評価の結果を示す。データベース保存時間について、本処理だけで全体の約7割の時間を要している。特に静止画では、レコードの追加を1件毎にデータベースのopenとcloseを行っていることに起因する。電話帳で時間を多く要しているのは、退避時の原因にも記した2つのデータベースで構成されていることに起因する。以上のように、全体性能はデータベースの性能に大きく影響される。

6.　おわりに

今回、我々は移動機端末における個人データのセキュアな退避・復元方式について実装し、評価を行った。今後は特に性能問題の原因となっているデータベースの構造を考慮した方式、および個人データの更なる大容量化や、コンテンツに依存した制約等にも対応した方式について検討して行きたい。

参照文献

[1] NTT ドコモテクニカルジャーナル Vol13 No.1 故障時における移動機端末内コンテンツファイル移行機能

[2] 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)