Vol.2010-MBL-52 No.11
2010/1/29

携帯電話の操作履歴活用のための プライバシ保護ミドルウェアの設計

吉川 貴[†] 太田 賢[†] 中川 智尋[†] 土井 千章[†]
野田 千恵[‡] 稲村 浩[†]

携帯電話の操作履歴を用いた，メニューのパーソナライズ機能や操作予測機能，ユーザデータの時系列表示など，履歴を活用して携帯電話の使い方をサポートする機能やサービスが提案されている．本稿では携帯電話機上で操作履歴を取得し，様々なアプリケーションから利用可能とする端末操作履歴活用プラットフォーム(操作履歴 PF)と，操作履歴 PF における操作履歴の安心・安全を確保するためのプライバシ保護ミドルウェアを提案し，そのアーキテクチャ設計を示す．プライバシ保護ミドルウェアは，操作履歴に関する脅威分析から導いたセキュリティ機能として，設定等の暗証番号保護，操作履歴の UIM 紐付け機能，抽象化機能，Java アプリに対するアクセス制御機能を備える．さらに操作履歴 PF の応用として，「ケータイ利用みまもり」アプリケーションを実装し，プラットフォームの実用性を確認した．

A Design of Privacy-aware Middleware for Leveraging Usage History of Mobile Handset

Takashi YOSHIKAWA[†] Tomohiro NAKAGAWA[†] Chiaki DOI[†] Ken OHTA[†] Chie NODA[‡] and Hiroshi INAMURA[†]

Recently usage history data have been utilized by various functions to support mobile handset usage such as personalized menu, usage prediction, timeline indication, and so on. This paper presents a design of usage history platform which enables various applications to utilize usage history data securely and reliably. After setting security requirements of usage history, we propose privacy-aware middleware for the usage history platform, which provides security functions such as PIN protection of setting and operation, UIM-based management of history data, data abstraction and access control for Java applications. We implemented an application that enhances children's cell phone literacy by feed-back of their daily usage, on top of the privacy-aware middleware and usage history platform on the cell phone for feasibility study.

1. はじめに

昨今，携帯電話の操作履歴を用いたメニューのカスタマイズ機能[1]や，操作予測機能[2]，検索候補表示機能[3]等，履歴データを活用して携帯電話の使い方をサポートする機能が提案されている．また，送受信メールやカメラ画像などのユーザデータを，それぞれ送受信時刻や撮影時刻等の操作履歴の観点で，時系列やカレンダー形式で表示する機能を備えた端末もある[4]．さらに，携帯電話からアップロードされた位置情報や写真を履歴データとして記録し，日記形式での表示や検索，他者との情報交換の機能を備えたライフログサービスも提案されている[5] [6]．

携帯電話の操作履歴はユーザの行動を示すデータである．端末上のプラットフォームとして様々なアプリケーションから利用可能とすることで，パーソナライズや使い勝手向上などの使い方サポートが期待できる．一方で操作履歴には個人情報が含まれることから，利便性を維持しつついかに安全なプライバシ保護機能を備えるかが課題となる[7]．

上記背景を元に本稿では，端末操作履歴活用のためのプラットフォーム(操作履歴 PF)を提案する．また，携帯電話上で取得した操作履歴を安心安全に取得・活用するための，操作履歴 PF 向けのプライバシ保護ミドルウェアを提案する．さらに，操作履歴 PF とプライバシ保護ミドルウェア，及び操作履歴を活用するユーザアプリケーションをプロトタイプ実装し，評価した結果についてまとめる．

2. 関連技術

操作履歴による携帯電話の使い方の分析やサポートとして，上坂ら[2]は携帯電話上でユーザの操作履歴を取得する操作履歴ロガーを提案している．履歴データを元にした機械学習により，操作予測がある程度可能であることを示している．また，Karlsonら[8]はデスクトップPCと携帯電話で操作ログを取得し，これらを併用するオフィスワーカーがどのようなパターンで日々の業務を行っているかを明らかにしている．

次に，操作履歴やその他ログに関して，プライバシ保護やフォレンジック等のセキュリティの観点からの関連研究について述べる．

- プライバシ保護：Pinkas[9]はプライバシ情報を含む各種データを暗号化したまま，各種計算を行う手法について紹介している．また，Aggarwalらはログデータをサーバにアップロードした際に，いかにプライバシ情報の漏えいを防止しつつデー

† 株式会社 NTT ドコモ 先進技術研究所
NTT DoCoMo, Inc. Research Laboratories.
‡ 株式会社 NTT ドコモ 移動機開発部
NTT DoCoMo, Inc. Consumer Device Development Department.

タマイニング処理を行うかという点に着目し，各種アルゴリズムや通信プロトコルをその著書[7]にまとめている．

- ITフォレンジック： 加藤ら[10]は，管理者による操作履歴の改ざんを防止するため，履歴データを複数のユーザで分散保持しつつ，署名検証によって改ざんを検知する手法を提案している．また，高田ら[11]は定期的にログのバックアップを作成することでログの改ざんと消去を検出し，復元する手法を提案している．Arastehら[12]はOSやアーキテクチャ等が異なる多様な機器から収集した様々な形式のログに対して事実を解析する手法を提案している．また，Turner[13]は携帯電話等様々な機器から収集したログを構造化し，解析する手法を提案している．

これらの関連研究は主にサーバ側での履歴データのセキュリティを扱っている．本研究の貢献は，標準的な携帯電話を対象として，携帯電話上で操作履歴を扱うユースケースに沿って網羅的に脅威分析を行い，セキュリティ要件を規定する点と，そのアーキテクチャ設計を示すことの 2 点である．

3. 端末操作履歴活用プラットフォーム

操作履歴を活用するユースケースを示した後，操作履歴 PF の備えるべき基本機能を述べる．

3.1 ユースケース

携帯電話の操作履歴はユーザの行動を示す汎用データであり，様々なサービスへの応用が考えられる．操作履歴を活用するアプリケーションを，操作履歴データそのものを利用するか，解析して用いるのか(解析の有無)と，ユーザ自身が利用するのか他人と共有して利用するのか(共有の有無)のユースケースで分類し，表 1に示す．

表 1 操作履歴を用いるユースケース

	操作履歴そのものを利用	解析して利用
本人利用	・ケータイ利用みまもり[14] ・UIカスタマイズ[1]	・操作支援[2] ・レコメンド[15]
他者共有	・子ども，高齢者みまもり[16] ・社員利用管理(法人)[17]	・コミュニケーション支援[18] ・レコメンド[19]

操作履歴をそのまま本人が利用するユースケース(左上)では，子どもが自身の使い方を振り返ることで使いすぎに気付かせる「ケータイ利用みまもり」や，よく使う機能のショートカットを自動生成するUIカスタマイズなど[1]がある．操作履歴を解析した結果を本人が利用するユースケース(右上)では，未来の操作を予測して入力を支援する操作支援[2]等が挙げられる．また，コンテンツの再生履歴を解析した結果を元にコンテンツのレコメンドを行うといったユースケースがあり，一部の録画機器等で類似機能が実現されている[15].

操作履歴を他者と共有するケース(左下)において，操作履歴をそのまま送信することで子どもや高齢者の安否確認や，社員の適正な携帯電話利用のための管理に用いることが考えられる[16][17]. 操作履歴として電話の発着信やメール送受信の解析結果を共有する(右下)ことで，友人関係の可視化などのコミュニケーション支援サービス[18]が考えられる．またコンテンツ利用履歴を共有し，レコメンドサービスにつなげることも考えられる[19].

3.2 操作履歴 PF の基本機能

前述の多様なアプリケーションに対応するための，プラットフォームとしての共通機能を抽出する．

3.2.1 操作履歴の入力

- **操作履歴記録機能 :** 端末の各機能の操作履歴を記録するのに加えて，ユースケース上，操作履歴を活用するアプリケーション自身の操作履歴を記録する機能も必要である．アプリケーションをまたがって操作履歴の活用を可能とするため，共通の API とデータ構造で記録する必要がある．

3.2.2 操作履歴の出力

- **操作履歴取得機能 :** アプリケーションが，操作履歴の解析や表示を行うため，操作履歴を取得するための API を提供する
- **累積計算機能 :** 操作履歴の解析では多くの場合，累積利用回数や累積利用時間が使われるため，共通機能として累積計算機能を備える．より高度な統計や分析の機能については，アプリケーション毎に解析アルゴリズムが異なると思われるため，基本機能としては提供しない．また，携帯電話のリソース制約のため，操作履歴 PF の設計方針として，計算負荷の高いデータ処理は端末ではなく，サーバ側で対処することを考える．
- **外部出力機能 :** 操作履歴を他者と共有するユースケースや大量の操作履歴を保持するためには，サーバへの送信や外部ストレージへの出力機能が必要となる．

4. 操作履歴 PF のセキュリティ要件

操作履歴データに関して，Microsoft社の提唱する脅威分析手法[20]を用いて以下の順序で，脅威を抽出し，セキュリティ要件を導出した．

1. 前提条件の整理
2. 保護資産の規定
3. データフローの検討
4. 脅威の洗い出しと対策の検討

4.1 前提条件

- ターゲット端末：以下の条件を満たす携帯電話を対象とする
  1. ユーザによる，非信頼のネイティブアプリの入れ替えが不可能
  2. ユーザによる，非信頼の Java ベースのアプリケーションの入れ替えが可能

  ここで非信頼のソフトウェアとは，携帯電話のオペレータや端末メーカが安全性を検証済みでない，信頼できないサードパーティ製のソフトウェアを指す．現状の国内の多くの携帯電話が上記条件を満たす．例えば，NTT ドコモの携帯電話では，i アプリと呼ばれる Java アプリの入れ替えは可能であるが，サードパーティ製のネイティブアプリを工場出荷後にユーザが入れ替えることはできない．一方，iPhone や WindowsMobile，Android 等のスマートフォンはユーザによる非信頼のサードパーティ製ネイティブアプリの入れ替えが可能である．
- 信頼モデル

  非信頼の Java アプリ以外のネイティブアプリ，ミドルウェア，OS，ブートローダは，端末メーカや OS ベンダが提供するソフトウェアコンポーネントであり，信頼できるものとする．また，携帯電話のユーザとして，悪意のある信頼できないユーザも存在するものと仮定する．また，JTAG/ICE ツール等のハードウェア攻撃は想定せず，非信頼のソフトによるソフトウェア攻撃のみを前提とする．
- 脅威分析のスコープ

  携帯電話内と，携帯電話からサーバや microSD といった外部デバイスへの履歴データの出力までを検討範囲とする．外部出力された後の履歴データに対する脅威は検討対象外とする．

4.2 保護資産の規定

前述の通り，携帯電話の操作履歴には電話番号やメールアドレスといった様々な個人情報が含まれるため，操作履歴データ自体が重要な保護資産となる．

4.3 データフローの検討

前述の操作履歴 PF の基本機能におけるデータフローは以下の 3 点となる．

- ユーザが携帯電話を利用することで，機能やアプリケーションが操作履歴 PF を呼び出して操作履歴を書き込む
- ユーザが利用するアプリケーションが操作履歴を利用した処理を行うため，操作履歴 PF から操作履歴を読み出す
- ユーザやアプリケーションからの要求に基づき，アプリケーションあるいは操作履歴 PF が操作履歴をサーバや他の携帯電話等の外部機器に送信する

ユースケース，前提条件，保護資産，データフローを元に作成したデータフロー図を図 1に示す．

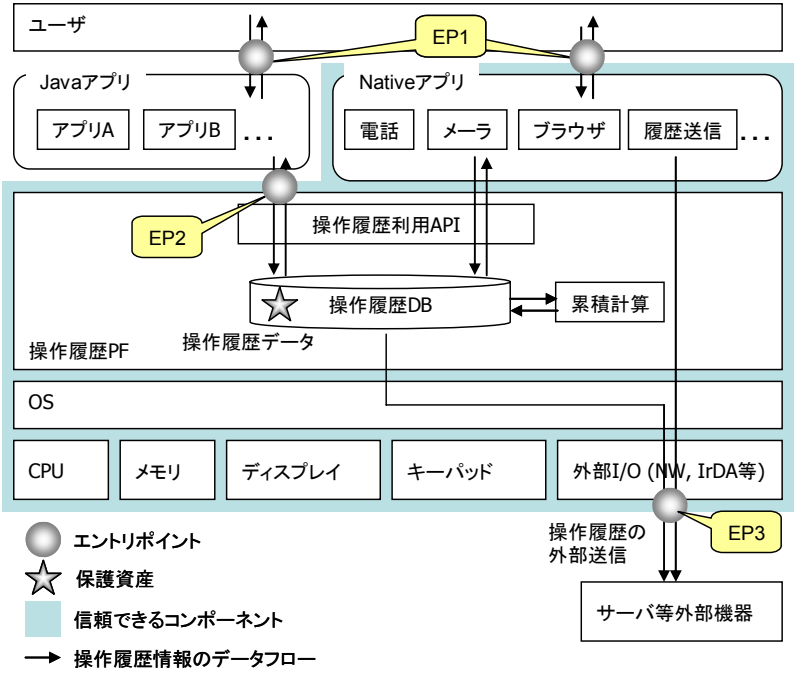

図 1 データフロー図

図中，矢印で示されるのがユースケースを元にしたデータフローである．また，網掛けで示されるのは 4.1 節で前提条件として示した信頼できるコンポーネントである．また，信頼できる領域の境界に位置する，○で示されるのがエントリポイント(EP)である．EP は脆弱性が存在する可能性のある部分であり，脅威分析の対象となる．データフロー図により，脆弱性が存在しうる EP として以下の 3 点が洗い出された．

- ユーザが各種アプリケーションを利用する場合(EP1)
- Java アプリが操作履歴 PF にアクセスする場合(EP2)
- 操作履歴が外部機器に送信される場合(EP3)

4.4 脅威分析とセキュリティ要件

表 2，表 3に，各EPに対して， STRIDEフレームワーク[20]を用いて網羅的に抽出した脅威と，そこから導いたセキュリティ要件を示す．セキュリティ要件は脅威を防止する観点と，起きた被害を抑制する点から定めた．なお，脅威において操作履歴データの改ざんについては，操作履歴の記録方法を追記のみとし，記録後の変更が不可能となるよう操作履歴PFを設計したため検討外とする．また，特権昇格については前提条件で挙げたターゲット端末ではJavaアプリが特権を取得することは困難であるため，検討外とした．特権昇格を防止するためにはJava VMの脆弱性を取り除くことが基本的な対策である．

表 2 各エントリポイントにおける脅威 (Th:脅威)

	EP1	EP2	EP3
S(成りすまし)	Th1	Th2	Th3
T(改ざん)	-	-	-
R(否認)	Th4	-	-
I(情報漏えい)	Th1, Th5	Th2	Th3, Th6
D(サービス拒否)	Th8	Th7, Th8	Th8
E(特権昇格)	-	-	-

表 3 脅威とセキュリティ要件 (R:セキュリティ要件)

Th1: 他人がユーザに成りすまして操作履歴を生成，閲覧，外部保存・送信する	
	R1-1: 操作履歴関連操作時は本人性確認を要求する
	R1-2: アクセス可能な操作履歴データを限定する
Th2: 悪意のある Java アプリが操作履歴を生成，閲覧，外部保存・送信する	
	R2-1: 信頼できる Java アプリからのアクセスのみを許可する
	R2-2: Java アプリが扱える操作履歴データを必要最小限に限定する
Th3: 履歴データの外部送信時にサーバの成りすましにより情報漏えいが発生する	
	R3-1: サーバ認証を行う
	R3-2: 外部送信される履歴データを必要最小限に限定する
Th4: ユーザが操作履歴データを否定する	
	R4-1: 他ユーザによる携帯電話操作を防止すること(R1-1)
	R4-2: 履歴データの改ざんを不可能とする
Th5: 機種変更や貸与時に元ユーザの履歴データが情報漏えいする	
	R5-1: 他者に元ユーザの履歴データを利用させない
	R5-2: アクセス可能な操作履歴データを限定する(R1-2)
Th6: ユーザの設定ミスにより，間違った送信先に履歴データが送信される	
	R6-1: 送信先の設定ミスを事前に防止する
	R6-2: 外部送信される履歴データを最小限に限定し，被害を抑制する(R3-2)
Th7: 悪意のある Java アプリが多数の API 呼び出しを行う	
	R7-1: 信頼できる Java アプリからのアクセスのみを許可する(R2-1)
	R7-2: API 呼び出しにかかるリソース消費を低減する
Th8: リソース不足により操作履歴関連の処理が失敗する	
	R8-1: リソース不足状態が発生しないように事前対処する
	R8-2: リソース不足状態に陥る前に操作履歴関連処理を実行する
	R8-3: 復帰時に操作履歴データを復活させる

Th1：他人が，端末を奪取し，正規ユーザに成りすまして操作履歴にアクセスする脅威が事考えられる．この脅威を防止するため，本人性確認が要件(R1-1)となる．指紋や虹彩などを用いた生体認証や物理的なドングルキー(USB キーやカード)を用いる方法，暗証番号等があるが，本稿の設計では，多くの携帯電話においてメールや電話帳などの個人情報の保護に使われている暗証番号保護を採用し，操作履歴関連の各種設定や閲覧操作を行う際には暗証番号の確認を必須とする．一方，被害の抑制のため，アクセス可能な履歴データを限定すること（R1-2）が必要となる．本研究では，操作履歴種別個別の記録可否設定を可能とし，不必要な操作履歴を記録しないようにする．

Th2：悪意のあるJavaアプリが正しいアプリになりすまして，操作履歴にアクセスする脅威が考えられる．脅威の防止，抑制のため，それぞれ信頼できるJavaアプリにのみアクセスを許可するアクセス制御要件(R2-1)，アクセス可能な履歴データを限定する要件(R2-2)が考えられる．R2-1 の対策として，オペレータやメーカの審査を通ったJavaアプリを信頼できるアプリとしてアクセスを許可したり，ユーザが許可したJavaアプリにアクセスを許可するアクセス制御が考えられる．本設計では審査を通ったJavaアプリに操作履歴へのアクセスを許可するアクセス制御を導入する．R2-2 については，本設計ではR1-2 と同様の対策をとる．他にも，操作履歴の表示等，限定的な機能であればX-OBJECT[21]のように生の操作履歴データをアプリに与えずに，処理する対策も考えられる．

Th3：悪意のあるサーバが操作履歴を取得する脅威についてはサーバの成りすましの防止としてサーバ認証(R3-1)や，被害の抑制として外部送信される履歴データの限定 (R3-2)が要件として挙げられる．本設計ではサーバ認証として既存機能の流用性の面から SSL によるサーバ認証を用いる．被害抑制の要件に対しては，送信するデータ項目を減らす手法やノイズを混入させる手法，履歴データの抽象化（数値を一定の規則に従って近似値に丸める等）や暗号化の対策が考えられるが，項目削除やノイズ混入はデータ復旧処理が必要となる．また，暗号化は，データを暗号化したまま解析す

る特殊な解析アルゴリズム設計が必要となり,扱いやすさに課題がある.本設計では,外部送信時の履歴データ抽象化機能を用意する.

Th4 : ユーザが操作履歴を否定する脅威については， Th1 と同様に他ユーザによる成りすましの防止(R4-1)と，履歴データの改ざんの防止(R4-2)が要件となる．他ユーザによる成りすましは Th1 で検討済みである．改ざん防止については前述の通り，操作履歴 PF として改ざんが起きない設計をとっている．

Th5 : ユーザを EP とした情報漏洩として，端末の貸与や譲渡の際に，新しいユーザに，端末内に残っている履歴データが漏洩することが考えられ，他者に元ユーザの履歴データを利用させないこと(R5-1)や，被害の抑制のためアクセス可能な履歴データを限定すること(R5-2)が要件として導かれる．この対策としては，貸与や譲渡の際の UIM が差し替えられるタイミングで履歴データを削除するか,他者に履歴データを利用させないためのアクセス制御が考えられるが，前者は貸与した端末を返却されるケースにおいて履歴データが失われるという問題がある．本稿の設計では履歴データを UIM カードと紐付けて管理し，他の UIM カード挿入時には履歴データにアクセスできないよう，UIM ベースのアクセス制御方式を導入する．

Th6 : サーバを EP とした情報漏洩として，履歴データの外部送信先をユーザが携帯電話で設定する際，設定ミスにより間違った送信先に履歴データが送信される脅威が考えられる．送信先の設定ミスの防止の要件（R6-1）に対して，送信先設定に入力欄と確認を用意したり，テスト送信を行って送信先が正しいかを確認する対策が考えられる.これらのミス防止対策は一般によくなされており,本稿の設計にも反映する．また，送信されてしまった場合に被害を抑制する要件(R6-2)については，R3-2 と同様であり，外部送信時の履歴データ抽象化機能で対応する．

Th7 : 悪意のある Java アプリが多数の API 呼び出しを行いサービス拒否攻撃を行う脅威に対しては,防止策として信頼できる Java アプリを選別してアクセス制御すること(R7-1)や，被害の抑制として，API 呼び出しにかかるリソース消費を低減すること（R7-2）が要件となる．本研究では Th2 で議論したように，審査を通った Java アプリに限定して操作履歴へのアクセスを許可するアクセス制御を導入する．

最後に，リソース不足により操作履歴関連の処理が失敗する可能性がある(Th8).例えば CPU やメモリに高負荷が生じてハングアップしたり，電池切れを起こしたり，メモリ制約により履歴データがあふれたりといった脅威が考えられる．電池切れやハングアップについては発生前に対処すること(R8-2)が要件となる．この場合，リソース不足発生前に不揮発メモリにデータを書き込むことが重要であり，本研究では操作履歴処理中に書込み状態を管理する保持フラグを不揮発メモリ上に保存する対策を行う．一方，履歴データ量の問題については通常のデータベースと同様に記録可能容量を制限することでリソース不足を回避できる(R8-1)．可能な限りデータを残すためサイクリックに保存し,上限到達時には古い履歴データから消去していくよう設計した.

5. アーキテクチャ設計/実装

図 2に，3.2節の基本機能を備える操作履歴PFのアーキテクチャを示す．また，セキュリティ要件を満たすため，前章の各対策をプライバシ保護ミドルウェアとして上位に設計した．また，その他携帯電話特有の要件についても検討のうえ，全体のアーキテクチャを設計し，プロトタイプの実装を行った.

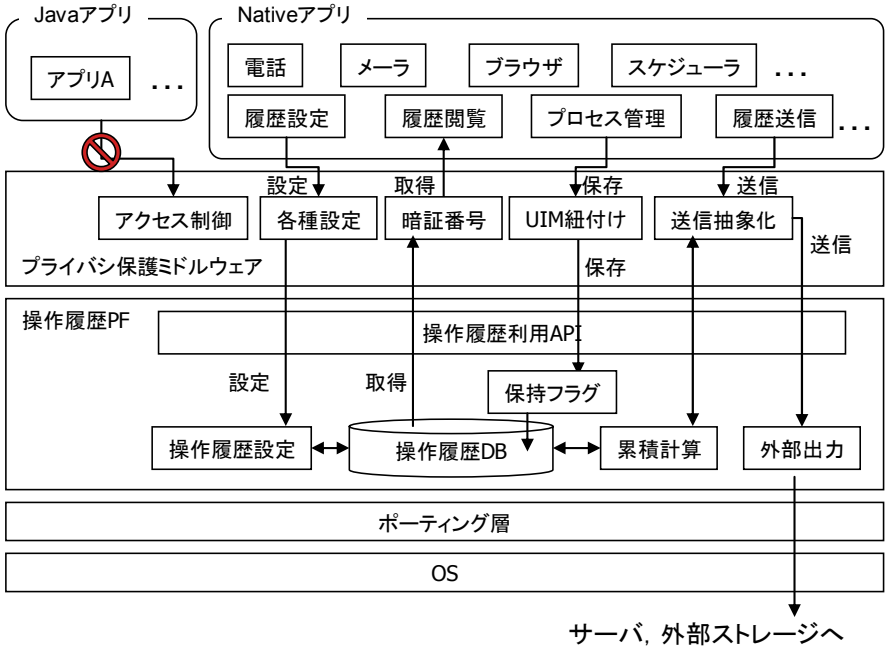

図 2 アーキテクチャ

5.1 携帯電話特有の要件と対策

携帯電話特有の課題に対する設計上の特徴は以下のとおりである.

- **操作履歴関連処理の軽量化：**
  RAM や CPU の制約上，操作履歴の記録や取得処理が操作の応答性に影響を与えないように，軽量化が必要である．そのため，設計上，操作履歴に記録するデータサイズを各フィールド 100 バイトまでに制限した.
- **操作履歴保存容量の固定化：**

内蔵ストレージ（NAND フラッシュメモリ）の容量制約上，サイクリックに操作履歴を保存し，利用容量を固定化した．

- **リソース不足時の記録漏れ対策(R8-2)：**
  バッテリ駆動であるため，バッテリ切れや電池の取り外し等による突然の低電圧状態になり，操作履歴の記録漏れを起こす可能性がある．そこで，操作履歴の記録開始時に，不揮発メモリ上の保持フラグをセットし，書込完了後にリセットする機能を加えた．再起動の際，保持フラグを参照することで，操作履歴の記録漏れの有無が確認でき，操作履歴データの信頼性を確認できる．

5.2 操作履歴 PF

操作履歴の記録や取得のために，履歴を保持するためのデータベースを備える．
また，各種ユースケースを実現するため，操作履歴の記録，取得，操作履歴記録の可否設定，利用回数/時間の積算などの抽象化を行う累積計算といった各機能を操作履歴利用APIとして公開している．例えば，ネイティブアプリはプライバシ保護ミドルウェア越しに本APIを呼び出すことで操作履歴を保存したり，取得したりすることが可能である．アプリケーション個別の操作履歴の記録には，アプリケーション自身を修正する必要がある一方で，アプリケーションの起動など，アプリケーションに依存しない操作履歴はプロセス管理モジュールのようなミドルウェアを修正することで記録できる．本APIの一例を表 4に示す．

表 4 操作履歴利用 API の一例

記録機能	LogpfErr LogpfDbInterface::Print(LogpfInfo& Info) アプリケーションからコールされることで操作履歴を記録する． 引数：日時、ログデータ種別、アプリ ID、アプリ名
取得機能	LogpfErr LogpfDbInterface::GetCyclic(LogpfInt ID, LogpfInfo& Info) レコード ID を引数に、操作履歴データを取得する． 引数：レコード ID、ログデータ本体へのポインタ
累積計算機能	LogpfInt Count(LogpfKind kind, LogpfInt appUID) 指定された履歴種別の前日 1 日の合計回数を取得する。 引数：ログ種別、アプリ ID，返り値：合計回数

5.3 プライバシ保護ミドルウェア

4章の各対策をプライバシ保護ミドルウェアとして設計した．

1. **操作履歴 PF の各種設定(R1-1,R1-2,R4-1)：**操作履歴種別個別の記録可否設定や操作履歴の外部送信先等，操作履歴 PF の各種設定を携帯電話上から行えるようにした．また設定画面を暗証番号で保護し，他人による不正な設定を防止した．
2. **操作履歴取得時の UIM 紐付け，暗証番号による保護(R1-1,R1-2, R4-1, R5-2)：**操作履歴データは全て UIM 情報と関連付けて管理され，他の UIM 挿入時には操作履歴データを取得不可能とした．また，操作履歴データをアプリケーションが取得する場合は暗証番号の入力を必須とし，他人による操作履歴の閲覧を防止した．
3. **別領域への保存とアクセス制御(R2-1,R7-1)：**リダイヤルやメールの受信箱とは別の領域に操作履歴データを保存し，審査を通過した一部の信頼できる Java アプリからのアクセスのみを許可するように設計した．
4. **外部送信時の抽象化(R3-2,R6-2)：**操作履歴データを外部機器に送信する際に，生データが送信されないように抽象化して送信する機能を備えた．操作履歴 PF の累積計算機能を利用して各アプリケーションの利用回数や利用時間の合計をアプリケーションに提供する．

5.4 ユーザアプリケーション「ケータイ利用みまもり」

昨今，小学生や中学生の携帯電話普及率が上昇しており，小学 6 年生では 31.6%，中学 3 年生では 55.2%となっている[22]．それに伴い，携帯電話への依存や，掲示板/メールによる誹謗中傷を発端とするトラブルが問題となっている[23]．また，教育再生懇談会においても，有害情報からの保護，携帯電話の利用ルールの教育の必要性が報告されており，社会問題として広く認知されてきている[24]．
本研究では，こういった課題の中の携帯電話依存について，操作履歴を用いて日々の使い方を自ら振り返り，適切な使い方を身につけられるアプリケーションを検討した．図 3に本アプリケーション「ケータイ利用みまもり」のユースケースシナリオを示す．

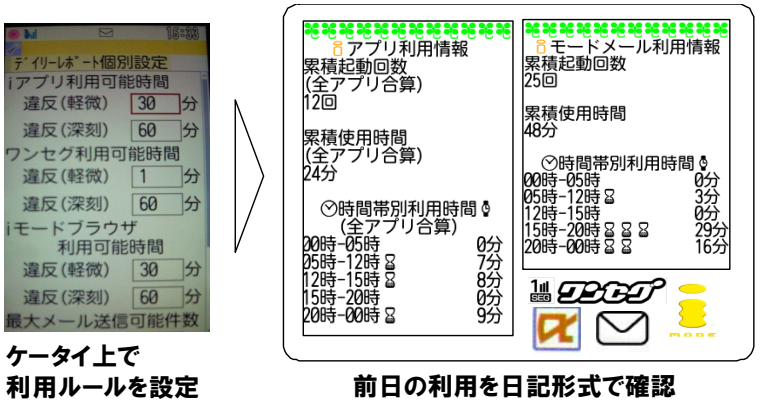

図 3 「子どもみまもり」のシナリオ

1. 親と子が話し合い，利用ルールを決めるためのチュートリアルサイト[25]などを活用して，子どもの携帯電話上で利用ルールを決める．本プロトタイプでは，Javaアプリ，ワンセグ，iモードブラウザ，メール送信のそれぞれについて一日の使用時間や一日の送信件数の上限を，利用ルールとして設定する．
2. 子どもが携帯電話を使用する．
3. 1 日 1 回，前の日の各アプリケーションの起動回数や使用時間，利用ルールを守れたかどうかが日記形式で自身にメール送信され，前の日の使い方を振り返ることができる．携帯電話上で設定すれば親の携帯電話等に送信することも可能．

プロトタイプ上に実装した日記形式のメール画面の詳細を図 4に示す．送信されるメール文面には詳細な操作履歴が表示されず，プライバシ保護ミドルウェアの抽象化機能が提供する各アプリケーションの使用回数や使用時間帯情報に留められ，子どものプライバシを保護している．

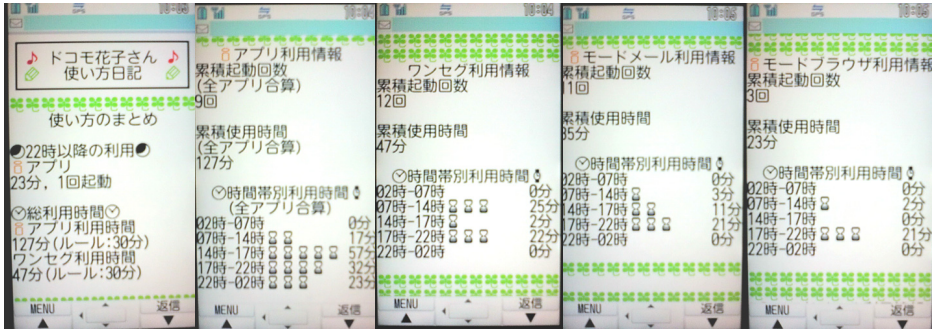

図 4 日記形式のメール画面

6. 評価

6.1 操作履歴の記録漏れ対策(R8-2)の有効性

信頼性向上を目的とした，操作履歴書込み状態を管理する保持フラグ(Cm9)の有効性について評価実験を行った．実験に際しては，フタを開閉しながら電池を脱着することで，操作履歴の記録中に意図的に異常を発生させ，保持フラグが有効に働くかどうかを確認する，という方法を取った．表 5に 100 回の試行を 3 回行った結果を示す．

表 5 保持フラグの有効性に関する実験結果 (単位：回)

項番	試行回数	開閉履歴保存成功回数	保持フラグ保存回数
1	100	99	1
2	100	99	1
3	100	98	2

実験の結果，ほとんどの場合で正しく開閉履歴を保存可能であり，異常発生による操作履歴の保存失敗が稀なケースであることがわかった．とはいえ100回に1～2回程度，操作履歴の保存失敗が発生したが，その場合にも保持フラグが不揮発メモリ上に確実に保存されたことを確認した．これにより，操作履歴の記録中に何らかの異常が発生した場合でも後からその事実を把握できることを確認した．

6.2 操作履歴のデータ量

ユースケースを実現するために必要な操作履歴DBの容量を，実データを元に机上計算した．まず，ユーザの 1 日の携帯電話の使用回数を，総務省や内閣府の調査報告書等[26][27][28][29][30][31]から抜粋した結果を表 6に示す．なお今回は様々な調査資料から使用回数を抜粋し，調査結果の最頻値を平均的ユーザ，調査結果内の最上位階級の代表値を高利用ユーザ，高利用ユーザの 5 倍の値をヘビーユーザとして設定した．

表 6 各モデルケースの携帯電話の使い方 (単位：回/1 日)

	平均的ユーザ	高利用ユーザ	ヘビーユーザ
電話発信	2	8	40
電話着信	2	8	40
メール送信	6	27	135
メール受信	8	27	135
Web 閲覧	1	7	35
Java アプリ起動/終了	1	7	35
アプリ起動/終了	13	50	250
端末開閉	22	106	530

次に，各モデルケースの使用回数や使用時間から 1 日の操作履歴データ量を計算し，目安として 5MBに達するまでの日数を机上計算した．その結果を表 7に示す．

表 7 計算結果

	1 日分の行数	1 日分のデータ量	5MB までの日数
平均的	全 127 行	58.1 KB	約 88 日
高利用	全 563 行	254 KB	約 20 日
ヘビー	全 2815 行	1.24 MB	約 4 日

検討の結果，操作履歴 DB に 5MB 程度を確保すれば，平均的なユーザで約 3 ヶ月弱の操作履歴データを保持することが可能であることがわかった.「子どもみまもり」や「高齢者安否確認」のようなユースケースであれば問題ない期間である.

7. おわりに

本稿では，携帯電話機上で操作履歴を安心安全に取得・活用するための端末アーキテクチャについて検討した．操作履歴を利用するユースケースに基づいて各種要件を規定し，特にセキュリティについてアーキテクチャレベルの脅威分析を行い，その対策を含むプライバシ保護ミドルウェアを提案した．さらに提案手法に基づいて実機上でのプロトタイプ実装を行い，提案手法の有効性を確認した．今後，操作履歴を活用した様々なアプリケーションの具体的な検討を進め，操作履歴 PF の機能拡張もはかっていく.

参考文献

[1] アクロディア，プレスリリース 2009 年 10 月 21 日，
http://www.acrodea.co.jp/press/2009/20091021_01/index.html, (参照 2009/12/3)
[2] 上坂 大輔，村松 茂樹，横山 浩之：携帯電話におけるユーザ状況適応型操作支援技術の検討, 情報処理学会研究報告, Vol. 2008-UBI-20, No. 6, pp. 33-38, 2008
[3] Google，”モバイル Google マップ”， http://www.google.co.jp/mobile/gmm/，(参照 2009/12/15).
[4] N905i, “ライフヒストリビューワ”， SO903i, SO903iTV, “ライフタイムカレンダー”.
[5] KDDI 研究所,” ユビキタスネットワーク技術の研究開発～ケータイ de ライフログ”，
http://www.kddi.com/business/oyakudachi/square/labo/003/，(参照 2009/12/03)
[6] ソニー，Life-X | ライフログ・シェアリングサービス，http://life-x.jp/，(参照 2009/12/03)
[7] 3.2Charu C. Agarwal and Philip S. Yu, editors. Privacy Preserving Data Mining: Models and Algorithms. Springer, 2008.
[8] A.K.Karlson, B.R.Meyers, A Jacobs, P Johns, and S.K.Kane, “Working Overtime: Patterns of Smartphone and PC Usage in the Day of an Information Worker”, The 7th Int. Conf. on Pervasive Computing, pp.398-405, 2009, .
[9] Pinkas B.: Cryptographic Techniques for Privacy-Preserving Data Mining. ACM SIGKDD Explorations, 4(2), 2002.
[10] 加藤慧，中山心太，荒川淳平，三島久典，吉浦裕，“組織的不正を想定したログ情報の改ざん防止システム”，情報処理学会研究報告，Vol.2009-DPS-138，No.20，pp.187-192, 2009.
[11] 高田哲司，小池英樹，“逃げログ：削除まで考慮に入れたログ情報保護手法”，情報処理学会論文誌，Vol.41, No.3, pp.823-831 (2000).
[12] A.R.Arasteh, M.Debbabi, A.Sakha and M.Saleh. “Analyzing multiple logs for forensic evidence”, In the Digital Investigation Journal, Volume 4, Number 1, September 2007, pp. 82-91.
[13] P. Turner, Selective and intelligent imaging using digital evidence bags, Digital Investigation, Volume 3, Supplement 1, pp. 59-64.
[14] マイコミジャーナル, “CEATEC JAPAN 2009 レポート”,
http://journal.mycom.co.jp/articles/2009/10/06/ceatec_keitai2/001.html, (参照 2009/12/21)
[15] SONY, “x-おまかせまる録”, http://www.sony.jp/bd/omamaru2009/index.html, (参照 2009/12/17)
[16] AOS テクノロジーズ，“Net Nanny” http://oyako119.jp/，(参照 2009/12/17)
[17] インテック，“LogRevi” ，http://www.intec.co.jp/service/lp/logrevi/，(参照 2009/12/17)
[18] Skydeck，“Skydeck”，http://skydeck.com/，(参照 2009/12/17)
[19] Last.fm, “Last.FM”, http://www.lastfm.jp/, (参照 2009/12/17)
[20] Frank Swiderski and Window Snyder, ”Threat Modeling”, Microsoft Press, Redmond, USA, June 2004.
[21] NTT ドコモ，“DoJa-3.0, XObject クラス, com.nttdocomo.lang.XObject”.
[22] ベネッセ，子どもの ICT 利用実態調査，2009/4/21，
http://benesse.jp/berd/center/open/report/ict_riyou/hon/index.html，(参照 2009/12/03)
[23] 吉田 俊和，高井 次郎，元吉 忠寛，五十嵐 祐，“インターネット依存および携帯メール依存のメカニズムの検討 −認知-行動モデルの観点から-“，電気通信普及財団 研究調査報告書 No.20, pp.176-183, 2005.
[24] 教育再生懇談会,” これまでの審議のまとめ－第一次報告－”，平成 20 年 5 月 26 日.
[25] NTT ドコモ，「ルール作りの 5 つのポイント」，
http://www.nttdocomo.co.jp/corporate/csr/safety/kids/rule/point/，(参照 2009/12/16)
[26] 総務省、「電気通信サービスに係る内外価格差に関する調査」、
http://www.soumu.go.jp/s-news/2005/pdf/050809_4_2.pdf，2005/8/9，(参照 2009/12/3).
[27] 総務省、「トラヒックからみた我が国の通信利用状況（平成 19 年度）」、
http://www.soumu.go.jp/s-news/2008/pdf/081010_3_bs.pdf, 2008/10/10，(参照 2009/12/03).
[28] 内閣府、「第 4 回情報化社会と青少年に関する調査報告書」，
http://www8.cao.go.jp/youth/kenkyu/jouhou4/html/html/2-1-2.html，平成 14 年 7 月 , (参照 2009/12/03).
[29] インプレス R&D、「ケータイ白書 2009」、2008 年 12 月 11 日
[30] 東京都教育庁指導部、「子供のインターネット・携帯電話利用についての実態調査報告（概要）」、http://www.kyoiku.metro.tokyo.jp/press/pr081009s/pr081009s_chousa.pdf, 2008/10/9，(参照 2009/12/03).
[31] 財団法人吉田秀雄記念事業財団、「携帯電話利用の実態 2007」，
http://www.yhmf.jp/pdf/activity/adstudies/vol_24_04.pdf, 2008/6/18，(参照 2009/12/03).