M-137

ユビキタスサービス基盤 (6)
～ユビキタス情報の分散管理～

A Ubiquitous Service Platform (6)
- A Cooperative Distributed Management of the Ubiquitous Resources -

田口 大悟† Daigo TAGUCHI　野田 潤† Jun NODA　楫 勇一‡ Yuichi KAJI　山田 敬嗣† Keiji YAMADA

1. はじめに

ネットワークで接続された多様な情報機器によって，生活に密着した情報サービスが提供されるユビキタス環境が社会に浸透しつつある．我々は，このユビキタス環境において，人に優しく安全で便利なサービスを容易に実現できるユビキタスサービス基盤の構築を目指している．

モバイル機器はその携帯性に起因して紛失／盗難／故障の確率が高い．このためモバイル機器に保持される情報は喪失／漏洩の危機にさらされている．これら危機への対策にはバックアップや暗号化が有効であるが，一般にセキュリティ強化と利便性向上とは相反し，多くの場合，利便性が犠牲となっている．

ユビキタス環境で取り扱われる情報を統一的に管理する情報管理基盤(ユビキタス情報管理基盤[1])では，利便性を損なうことなく，情報の喪失防止／漏洩防止を実現することを目指している．我々は，モバイル機器に保持される情報(携帯情報)に着目し，情報特性と機器特性に応じた情報分散管理とアクセス制御の検討を行った．本報告では，携帯情報の分類，分散管理のための要件，及び携帯電話に保持される情報のバックアップの課題と解決策を概説する．

2. 背景と課題

ユビキタス社会では，情報機器を携帯すればより多くの情報サービスをいつでもどこでも享受することが可能となる．例えば，Suica®サービス[2]ではICカード，公衆無線LANサービスではノートPC，i-mode®サービス[3]では携帯電話を携帯してサービスを享受する．一方で，これらモバイル機器の紛失／盗難／故障による，情報の喪失／漏洩が社会問題化している．モバイル機器の紛失経験者の割合は15%を超え，特に機密性の高い情報を扱う会社経営陣クラスで20%を超えている[4]．

情報機器紛失による情報の漏洩防止には，暗号化が有効である．また情報喪失対策として有効な手段はバックアップである．こまめなバックアップにより，情報機器の紛失／故障による情報喪失を最小にすることができる．しかし，これらの運用における問題が残る．ハードディスク暗号化で利用する暗号鍵は，パスワードあるいはパスフレーズの形で利用者の記憶に留められている．しかし，管理するパスワードの数が多くなると記憶困難となり，忘却防止のため手帳や付箋に記載することも少なくない(図 1-左)．

バックアップには，不正リストアの問題がある．例えば，携帯電話にダウンロードした著作権のある着信メロディをPCにバックアップする．このデータを友人の携帯電話へリストアできれば，不正コピーとなり，著作者の利益を損なう(図 1-右)．実際のサービスでは，携帯電話の転送禁止機能を利用して，著作権のあるコンテンツはPCへバックアップできないように制御されている．この制御は不正コピーの防止に有効であるが，正当な目的によるバックアップを不可能にしており，利用者の利便性を一部損なっている．

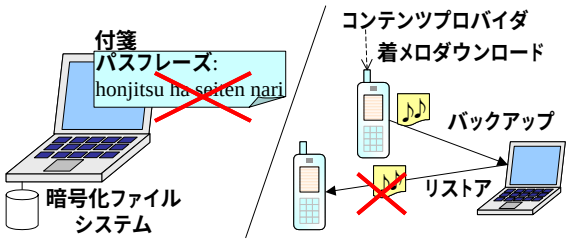

図 1 暗号化とバックアップの問題点

3. ユビキタス情報の分散管理

ユビキタス情報管理基盤では，セキュリティ強化や不正利用防止のため犠牲となりやすい利便性の課題を，ユビキタス情報の分散管理によって解決する．

3.1. 携帯情報

本報告では，ユビキタス環境を流通する情報のうち，喪失／漏洩の危険性の高い，モバイル機器に保持される情報(携帯情報)に着目して議論する．表 1は携帯情報を利用時の価値変化，喪失時／復元データ利用時損益者の観点で分類した表である．これによれば，携帯情報を喪失した場合の損益者は常に利用者本人であるのに対し，バックアップ・リストアで得た復元情報，複製情報が利用された場合の損益者は，情報価値変化の有無と増減方向，システム機能(同一情報の複数回利用チェック機能など)に依存して，利用者あるいはサービス提供者と替わることがわかる．

3.2. ユビキタス情報分散管理の要件

ユビキタス情報管理基盤における情報分散管理・アクセス制御では以下を実現する必要がある．

(1)冗長性を持たせた情報分散格納

機器の紛失／盗難／故障による情報喪失を防ぐため，複数の機器に冗長性を持たせて情報を分散して格納する．

(2)冗長情報への排他的アクセス制御

不正に入手・作成された情報を元にしたサービスの不正享受を防止するため，冗長的に格納した情報へのアクセスを排他的に制御する．

(3)機器特性／情報特性に応じた管理

分散されたユビキタス機器は異なる環境に置かれた性能や使用目的の違う機器である．このため分散格納では機器特性に応じて格納方法を決定する．例えば，携帯電話には

† NEC インターネットシステム研究所，Internet Systems Research laboratories, NEC Corporation
‡ 奈良先端科学技術大学院大学 情報科学研究科，Graduate School of Information Science, Nara Institute of Science and Technology

表 1 携帯情報の特性

分類	携帯情報例	利用時 価値変化	喪失時 損益者	復元情報 利用時 損益者
パーソナルデータ	アドレス帳 スケジュール	不変	利用者本人	利用者本人
デジタルコンテンツ	着信メロディ 待ち受け画像	不変	利用者本人	著作者／配信者
電子チケット	映画鑑賞券 鉄道回数券	減少	利用者本人	発券者／発行者 ※1 利用者本人 ※2
電子ポイントカード	マイレージカード 商店ポイントカード	減少[ポイント利用時]	利用者本人	
		増加[ポイント加算時]	利用者本人	利用者本人 ※1

※1 利用時にサーバ問合せによるチェックを実施しない場合
※2 利用時にサーバによるチェックが実施され，復元情報が他人により先に利用された場合

移動先で利用可能な情報を格納しておく必要があるが，その冗長情報を，別の携帯電話に格納する必要はなく，バックアップデータとしてホーム PC に格納すれば十分である．また，情報価値変化の有無，不正利用時損益者を考慮して管理方法を決定する必要がある．

4. 携帯情報のバックアップとリストア

携帯電話の紛失／故障／機種変更時に備えた携帯情報のバックアップとリストアについて説明する．ここでは，こまめなバックアップを容易に実現するため，バックアップ先機器をホーム PC とする．検討した方式の前提条件は以下である．

- 携帯電話には利用可能な情報が常に格納される．
- 携帯電話には機器／利用者識別情報が格納される．
- 携帯情報にはリストア許可条件が付与される．

また，対象とする携帯情報はとしては以下の 4 種類を考える．括弧内は情報作成者が要求するリストア可否条件の例である．

- パーソナル情報(同一ユーザならリストア許可)
- デジタルコンテンツ(同一端末ならリストア許可)
- 電子チケット(サーバ問合せがあればリストア許可)
- 電子ポイントカード[加算時](常にリストア許可)

これら条件のもと，安全で便利なバックアップ・リストアを実現する一つの手順を以下に示す(図 2).

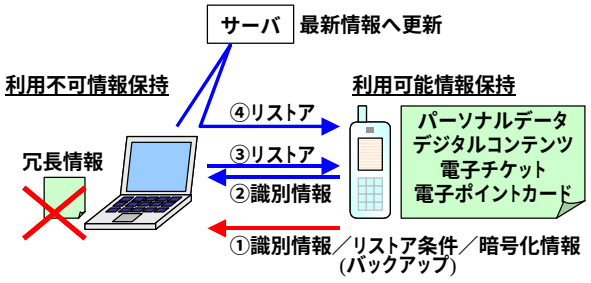

図 2 携帯情報のバックアップとリストア

バックアップ：
①機器／利用者識別情報，リストア条件，暗号化した携帯情報を転送して，ホーム PC に格納する．ホーム PC に格納した冗長情報は暗号化されているため利用できない．
リストア：
②機器／利用者識別情報を転送してリストアを要求する．
③リストア要求に含まれる機器／利用者識別情報と，バックアップデータの識別情報・リストア条件を比較／判定し，サーバ問合せが不要ならば，ホーム PC からバックアップデータを転送，携帯電話で復号して，リストアを完了する．
④サーバ問合せが必要ならば，サーバへ問合せ，最新情報へ更新した後，携帯電話へ転送，格納してリストアを完了する．またサーバでは旧情報を無効化する処理を行う．

尚，ホーム PC における改ざん，通信傍受によるなりすまし攻撃，リプレイ攻撃などを防止するにはデジタル署名技術，暗号化技術，鍵管理技術を応用する．

5. 考察

前記したバックアップ・リストア方式では，ホーム PC に暗号化した携帯情報を格納することにより，ユビキタス情報管理で必要とされる冗長性を持たせた分散格納と，冗長情報への排他的アクセス制御とを実現している．また，情報特性をリストア可否条件として携帯情報に付与することにより，情報特性に応じた管理を容易にするシステム構築が可能となる．

本報告では，モバイル機器に利用可能な情報を常に保持することを前提とし，情報価値変化，冗長情報復元による損益者を考慮した分散管理・アクセス制御方法を示したが，携帯できない大容量の情報を扱うための分散管理，利用頻度や機密度を考慮した分散管理の検討も必要である．

6. おわりに

ユビキタス環境で利用されるモバイル機器に格納される情報の喪失防止・漏洩防止を実現するため，冗長性を持たせた分散格納，冗長情報への排他的アクセス制御，情報特性と機器特性とに応じた情報管理が重要であることを示した．また携帯電話に保持される情報について，ホーム PC への安全なバックアップ・リストアの実現方法を概説した．

参考文献

[1] 谷他, “ユビキタスサービス基盤 (4) ～ユビキタス情報管理基盤～,” FIT 2003.
[2] JR 東日本, <http://www.jreast.co.jp/> (03/07/04)
[3] NTT DoCoMo, <http://www.nttdocomo.co.jp/> (03/07/04)
[4] 中野長昌, “モバイル機器の盗難・紛失に対するセキュリティ管理”, 情報システム産業分析, Vol.14 No.159(2002):2-3.