

コンテンツ利用管理システム: モバイル RightsShell -コンテンツ配信方式-

5V-1

中村 暢達 仁野 裕一 谷 幹也 市山 俊治

NEC

インターネットシステム研究所

1. はじめに

近年、デジタルコンテンツが広く利用されるようになったが、コンテンツの著作権保護に関しては、様々な課題がある。我々が開発したモバイル RightsShell は、モバイル機器向けのコンテンツ配信サービスにおいて、コンテンツを不正な利用から守り、安全にコンテンツを配信するシステムである。システムの概要については、参考文献[1]において述べ、本稿においてはモバイル機器向けに開発された2つの技術: 可変暗号化方式、シュードコンパイル方式について述べる。

2. 可変暗号化方式

コンテンツを不正な利用から保護するには、暗号化は有効な手段である。暗号強度の高い暗号方式を用いることで、安全性は一般に高くなるが、一方で計算処理が増加し、メモリ量やプロセッサ能力に制限がある携帯機器においては、暗号処理に時間がかかるなどの問題点があった。

モバイル RightsShell では、暗号化の対象となるデータのフォーマットに応じて、暗号パラメータを変更する可変暗号化方式を用いている。

図1に可変暗号化方式を説明するための暗号カプセルの例を示す。この例では、コンテンツはプログラムで、プログラムの利用条件情報と共に暗号カプセル化されている。暗号カプセル化の概要についてはここでは述べない(参考文献[2])。図では、コンテンツの各領域ごとにどのように暗号化されているかが示されている。

利用条件情報がどのように暗号化されているかは、あらかじめ定められおり、この例では、トリプル DES を用いている。利用条件情報は、コンテンツの利用回数、利用秒数、有効期間や、コンテンツがどのように暗号化されているかを示すパラメータなどの重要情報を含み、安全性が高い暗号方式が適用される。利用条件情報のデータサイズは大きくないため、処理量が多い暗号方式を使っても問題とはならない。

可変暗号化方式では、コンテンツはいくつかのブロックごとに異なる暗号方式が適用されている。ここでは、プログラムコードと、GUI リソースと、キャラクタイメージでそれぞれ異なる攪拌回数のブロック暗号が適用されている。GUI リソースのように、一般的な情報で、保護する必要がない場合には、攪拌回数が少ない軽い暗号が使われている。一方、キャラクタイメージのように、著作権保護の必要性が高いデータに対しては、攪拌回数が多い十分な安全性がある暗号が使われる。

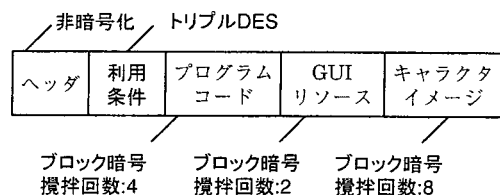


図1 暗号カプセルの例

プログラムを対象例としたが、音楽、画像、構造化文書に対しても、同様に適用可能である。

3. シュードコンパイル方式

携帯機器においては、画面サイズ、入力 IF に制限があり、PC と比べ操作性が十分でない。そのため、

暗号カプセル化されたコンテンツの復号などの操作支援として、シュードコンパイル方式を開発した。

図2にシュードコンパイル方式の例を示す。中間コードは携帯機器でそのまま実行できる実行形式であり、暗号カプセル実行形式とは、前述の中間コードに、暗号化された利用条件およびコンテンツをシュードコンパイル（強制挿入）した形式となっている。

次に、暗号カプセル実行形式の振る舞いについて述べる。暗号カプセル実行形式が起動されると、利用条件およびコンテンツの復号を行い（起動コード）、次に、復号したコンテンツを実行している機器にインストールし（インストールコード）、暗号カプセル実行形式から、インストールしたコンテンツのプレーヤーもしくはコンテンツ自身（実行プログラムであれば）に実行制御を移す（終了コード）。

機器には、クライアントソフトが予め常駐実行されている必要があり、コンテンツの利用を監視する。コンテンツの利用が終了すれば、終了イベントをトリガーにして、インストールされているコンテンツを再暗号化・バックアップし、元の暗号カプセル実行形式に格納する。そして、機器からアンインストールを行う。

シュードコンパイル方式は、元のコンテンツの形式によらず、またソースファイルの変更などの作業なしに、容易に利用管理機能を付加できる。

4. 実装

以上の機能を PalmOS 端末に実装した。中間コードは約 4K バイト、携帯端末に常駐するクライアントソフトのサイズは約 23K バイトである。処理時間は、PalmVx (DragonBall EZ 20 Mhz) で、60K バイトのコンテンツの実行まで 1 秒以内であり、十分なレス

ポンスを得られた。図3に実行例を示す。

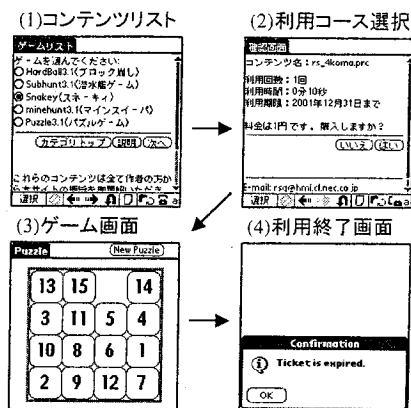


図3 PalmOS 上でのモバイル RightsShell 実行例
(Palm Computing 社提供の Puzzle.prc をカプセル化して実行)

5. おわりに

モバイル機器向けのコンテンツ利用管理システムのプロトタイプを開発した[3]。可変暗号化方式、シュードコンパイル方式を用い、処理能力やユーザインタフェースに制限のある携帯端末においても、十分使用可能であることを確認した。

参考文献

- [1] コンテンツ利用管理システム：モバイル RightsShell-システム概要、谷、仁野、中村、市山、情報処理学会 63 回全国大会 5V-02、2001.09
- [2] コンテンツのカプセル化とアクセス制御、細見、中江、市山、下 條、UNIX MAGAZINE(アスキー)、Vol.9、PP.158-166、2000.08
- [3] 日経エレクトロニクス No.790、PP.37-38、2001.02.26

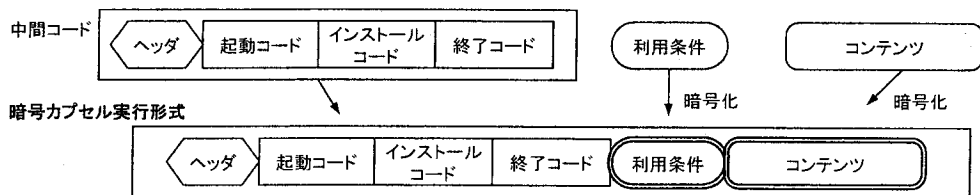


図2 シュードコンパイル方式の例