コンテンツ配布システムにおける鍵管理方式の一提案

鴨志田 昭輝　中嶋 春光　宮崎 一哉　中川路 哲男

{kamosida, haru, kazu, nakawaji}@iss.isl.melco.co.jp

三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部

〒247-8501 神奈川県鎌倉市大船5-1-1

あらまし：デジタルコンテンツを暗号化し安全に配布･販売するコンテンツ配布システムにおいて，扱うコンテンツの数が増大すると，管理する必要のあるコンテンツ鍵が膨大な数になるという問題がある．本稿では,この問題を解決するため，キーリカバリの原理をコンテンツ配布システムの鍵管理に応用することを提案する．これにより，コンテンツ鍵管理のための負荷を大幅に軽減できる等のメリットがある．

A Key Management Scheme for Secure Digital Contents Distribution

Akiteru KAMOSHIDA　Harumitsu NAKAJIMA
Kazuya MIYAZAKI　Tetsuo NAKAKAWAJI

{kamosida, haru, kazu, nakawaji}@iss.isl.melco.co.jp

Information Technology R&D Center
Mitsubishi Electric Corporation

5-1-1 Ohuna, Kamakura, Kanagawa, 247-8501 Japan

Abstract: We have researched on secure contents distribution system, but there is a problem that the server must manage a lot of keys if the system deals a lot of contents. This paper proposes a key management scheme for secure contents distribution system that uses principle of key recovery. This proposal has some advantages such as reduction of loads owing to content keys management.

1 はじめに

インターネットに代表されるオープンネットワークの急速な普及にともない，ネットワーク上でのデジタルコンテンツ販売等，コンテンツの機密や著作権を保護しながらコンテンツの配布を促進するシステムの必要性が急浮上している．このような背景から，著者らはセキュアコンテンツ配布システムDIGICAPSULEの開発を行っている．

本稿では，コンテンツ配布システムにおける鍵管理方式の提案を行う．まず，2章において本研究の背景を述べる．3章では，著者らが開発を行っているセキュアコンテンツ配布システムDIGICAPSULEを紹介する．そして，4章において提案する鍵管理方式を説明し，5章において提案する鍵管理方式の拡張について述べる．最後に，6章において机上での評価を行い，7章において結論を述べる．

2 背景

著者らはセキュアデジタルコンテンツ配布システムDIGICAPSULEを開発中である（以前のバージョンではDigiGuardあるいはDIGITEXと呼ばれていた）[1][2]．本章では，セキュアコンテンツ配布システムDIGICAPSULEを開発するに至った背景について述べる．

2.1 デジタルコンテンツ配布の意義と現状

以下に示す理由から，インターネット上でのデジタルコンテンツ配布に対する需要が急増すると予測される．

1. オープンネットワークの普及
2. ネットワーク上の公共社会インフラ整備の必要性
   - ・機密文書のやりとり（企業間，企業-モバイル端末間，本社-支社間等）
   - ・電子商取引（企業間，個人）
3. デジタルコンテンツ制作環境の普及
   - ・デジタル機器，高性能ソフトウェア等

デジタル画像や電子文書といったデジタルコンテンツをインターネット上で配布・販売することは，流通コストの安さや配布範囲の広さ等多くのメリットがある．

2.2 デジタルコンテンツ配布の問題点

インターネット上でのデジタルコンテンツ配布・販売には以下のような問題がある．

1. 正当な課金が困難
   デジタルコンテンツは完全な複製を作成することが容易であるという特徴がある．このため不正なコピーが数多く流通し，正当な課金の妨げになっている．
2. 著作権保護が困難
   デジタルコンテンツは，加工・改竄が容易であるという特徴がある．このため，他人の著作物を加工して別の著作物（またはその一部）にしてしまうといった問題がある．このため，デジタルコンテンツ制作者の著作権を保護することが困難である．
3. 機密漏洩の危険性が高い
   機密文書を複製して持ち出すことによる機密の漏洩が危惧されている．また，インターネット上での盗聴・改竄・なりすましによっても機密が漏洩する危険性がある．

上記のような問題点を解決するため，セキュアデジタルコンテンツ配布システムDIGICAPSULEの開発が行われている．

3 セキュアデジタルコンテンツ配布システムDIGICAPSULE

本章では，現在開発中のセキュアデジタルコンテンツ配布システムDIGICAPSULEについて説明する．

3.1 DIGICAPSULEの特徴

開発中のセキュアコンテンツ配布システムDIGICAPSULEは，以下のような特徴を持つ．

1. 著作権管理機能と配布･課金機能の分離
   - 制作者の配布，管理による負担を軽減
   - 制作者の著作権保護を重視
2. 購入前に試使用が可能
3. さまざまな形式のコンテンツに対応
   - PDF文書，画像，ソフトウェア，html文書など

3.2 システム構成

DIGICAPSULEは，以下のような役割を持つエントリより構成される．

制作者 ： デジタルコンテンツを制作する．
利用者 ： デジタルコンテンツを購入･使用する．
配布者 ： 制作者と利用者の間でコンテンツの配布・販売・課金を行う．
著作権管理代行機関 ： 著作権の管理を集中的に行う．

このエントリは必ずしも別人（別の機関）である必要はない．配布するコンテンツの性質や，各エントリの組織形態によって，フレキシブルに構成をかえることができる．例えば，配布者と著作権管理代行機関の機能を１つのサーバ上で実現し，コンテンツの配布･販売･課金･著作権の管理すべて行うことも可能である．

3.3 処理の流れ

DIGICAPSULEでは，暗号化コンテンツ，コンテンツ鍵，実行規則等を1つのファイルに結合(カプセル化)し，配布する．このファイルをカプセルと呼ぶ．カプセルを配布する処理の流れを表 1および図 1に示す．図 1の(1)～(8)は，表 1の番号に対応している．

表 1: 処理内容

	エントリ	処理内容
(1)	制作者	配布するコンテンツを作成する．コンテンツを暗号化する共通鍵（以下コンテンツ鍵と記す）を著作権管理代行機関に要求する．
(2)	著作権管理代行機関	コンテンツ鍵を作成する．作成したコンテンツ鍵をデータベースに登録・管理し，制作者に送信する．
(3)	制作者	コンテンツ鍵を用いてコンテンツを暗号化し，カプセルに格納する．
(4)	制作者	作成したカプセルを配布者に送信し，配布を依頼する．
(5)	配布者	カプセルをデータベースに登録し，管理する．カプセルを様々なメディアを用いて配布する．
(6)	利用者	コンテンツ鍵を配布者を通じて著作権管理代行機関から入手する．
(7)	利用者	コンテンツ鍵をカプセルに格納する．
(8)	利用者	カプセル内の暗号化されたコンテンツを，同じくカプセル内のコンテンツ鍵を用いて復号し，コンテンツ

		を利用する．復号されたコンテンツの種類に応じた利用制御を行う．

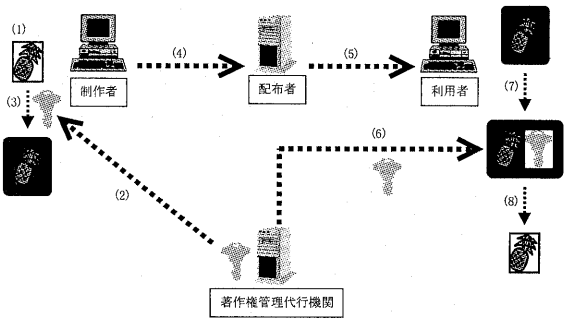

図 1: 処理の流れ

4 提案する鍵管理方式

本章では，著作権管理代行機関におけるコンテンツ鍵の管理を，キーリカバリ技術を用いて実現する手法を提案する．

4.1 目的

扱うコンテンツ数が増えたり，安全性維持のために鍵を定期的に交換するといった場合，著作権管理代行機関において管理する必要のあるコンテンツ鍵が膨大な数になり，管理のための負荷が増大する．

この問題点を解決することのできる鍵管理方式の検討を行った．

4.2 キーリカバリの目的

暗号化技術の普及にともない，データの送受信や蓄積に暗号が用いられる機会が多くなる．こうした場合，鍵を紛失してしまうと暗号化データへのアクセスが不可能になってしまう．

また，暗号技術の普及にともない，暗号を使用したハイテク犯罪の増加も予想される．こうした場合，法執行機関等の特権者による暗号化データへの合法的なアクセスが必要になる．

このような背景から，権限があれば鍵をもたなくとも暗号化データを復号することを可能にするシステムが必要となると考えられる．これを実現する技術がキーリカバリである．

4.3 キーリカバリの原理

文献[3]において提案されているキーリカバリシステムの原理について述べる．

1. データ暗号化時
   データを共通鍵で暗号化する際，共通鍵から鍵回復のための情報KRB(Key Recovery Block)を作成し，暗号化データに付加する(図 2). KRBを作成するためには，あらかじめ鍵回復センタに鍵回復適用条件を登録し，鍵回復ポリシー(鍵回復センタの公開鍵を含むKRB作成に必要な情報)を取得しておく必要がある．

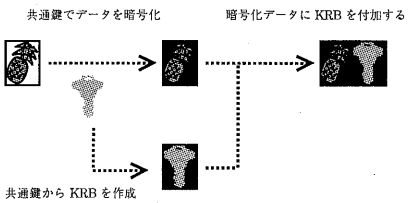

図 2: キーリカバリの原理 – データ暗号化

2. データ復号時
   データを復号する際，まず暗号化データとKRBを分離する．暗号化データを共有している鍵で暗号化し，KRBは破棄する(図 3).

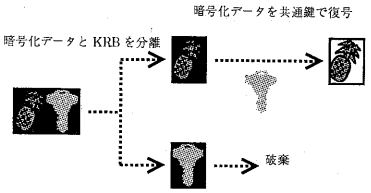

図 3: キーリカバリの原理 – データの復号

3. 鍵回復時
鍵紛失時等鍵回復が必要な場合には, KRBを鍵回復センタに送信し, 鍵回復を依頼する. 鍵回復センタは鍵回復権限を持つため, KRBから共有鍵を回復することができる. そして, 回復された鍵を用い, 暗号化データを復号する(図 4).

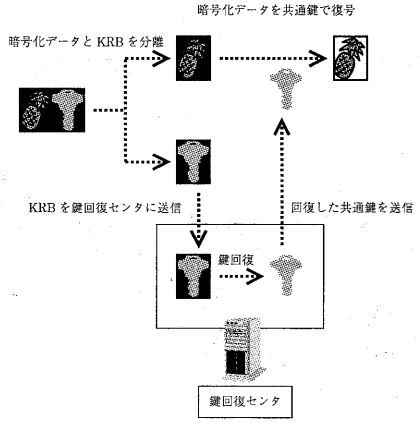

図 4: キーリカバリの原理 – 鍵回復

4.4 提案方式の原理

提案方式では, 著作権管理代行機関が鍵回復センタの役割を担う. 制作者は, あらかじめ著作権管理代行機関に対して鍵回復のための登録を行い, 鍵回復ポリシー(著作権管理代行機関の公開鍵を含むKRB作成に必要な情報)を取得しておく必要がある.

コンテンツ鍵を用いてコンテンツを暗号化した後, コンテンツ鍵よりKRBを作成する. カプセル作成時, カプセルに暗号化コンテンツとともにKRBに格納する. カプセル購入時には, 著作権管理代行機関がKRBからコンテンツ鍵を回復する.

この仕組みにより, 著作権管理代行機関でのコンテンツ鍵の管理が不要になる. この場合, 著作権管理代行機関では鍵回復権限の管理と, 鍵回復履歴 (カプセル購入履歴) の管理を行えばよいことになる.

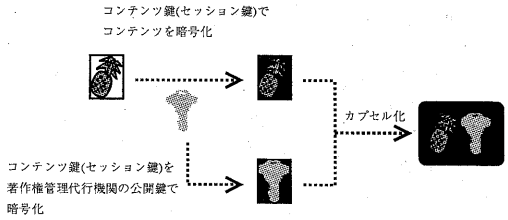

図 5: 提案方式の原理

4.5 提案方式での処理の流れ

提案する鍵管理方式を適用したDIGICAP-SULEでは, 以下の点で処理内容が大きく異なる.

1. 制作者はカプセル作成時に, 鍵回復のための情報 (以下KRBと記述) を作成し, カプセルに格納する.
2. 著作権管理代行機関はKRBからコンテンツ鍵を回復し, 利用者に送信する.

提案する鍵管理方式をDIGICAPSULEに適用した場合の処理の流れを表 2および図 6に示す. 図 6の(1)〜(10)は, 表 2の番号に対応している.

表 2: 提案方式適用後の処理内容

	エントリ	処理内容
(1)	制作者	配布するコンテンツを作成する．また，コンテンツ鍵を作成する．
(2)	制作者	コンテンツ鍵を用いてコンテンツを暗号化し，カプセルに格納する．コンテンツ鍵よりKRBを作成し，カプセルに格納する．
(3)	制作者	作成したカプセルを配布者に送信し，配布を依頼する．
(4)	配布者	カプセルをデータベースに登録し，管理する．カプセルを様々なメディアを用いて配布する．
(5)	利用者	KRBを配布者を通して著作権管理代行機関に送信し，コンテンツ鍵を要求する．
(6)	著作権管理代行機関	KRBからコンテンツ鍵を回復し，配布者を通して利用者に送信する．
(7)	利用者	コンテンツ鍵をカプセルに格納する．
(8)	利用者	カプセル内の暗号化されたコンテンツを，同じくカプセル内のコンテンツ鍵を用いて復号し，コンテンツを利用する．復号されたコンテンツが流出しないよう，コンテンツの種類に応た利用制御を行う．

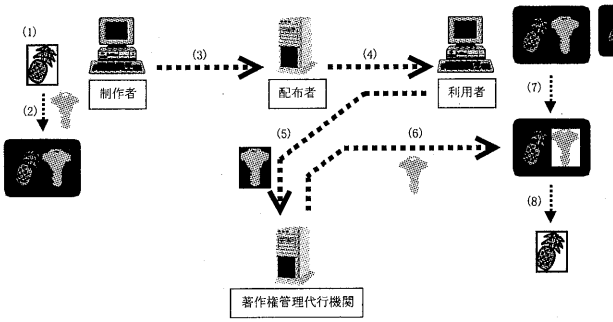

図 6: 提案方式適用後の処理の流れ

5 提案方式の拡張

提案する鍵管理方式は，キーリカバリの原理を利用している．このため，本来のキーリカバリの目的を果たすコンテンツ配布システムを構築することが比較的容易である．

キーリカバリに対応したDIGICAPSULEの概要を図 7に示す．この場合，制作者はカプセルにKRBを2つ格納する．1つめのKRBは，著作権管理機関がコンテンツ鍵を復号するために用いられる．もう1つのKRBは，鍵回復センタがコンテンツ鍵を回復するために用いられる．

図 7に示すようなシステムは，主に法執行機関による合法アクセスの仕組みに用いられると考えられる．例えば，違法なコンテンツ（他者の著作物を不正に販売しようとする等）を販売していないかどうかを特権者が検査するといったケースが考えられる．

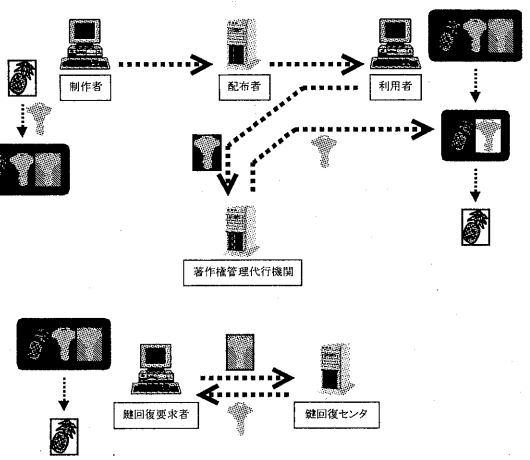

図 7: キーリカバリに対応した場合の処理の流れ

6 評価

提案した鍵管理方式の評価を行う.

6.1 有効性

提案する鍵管理方式を適用することにより, 以下のような利点がある.

1. 鍵管理による負荷の低減
   ・著作権管理代行機関においてコンテンツ鍵をデータベースで管理する必要がない.
   ・著作権管理代行機関は, KRBからコンテンツ鍵を回復することが可能である. このため, コンテンツ鍵をもたなくても, 販売実績の把握等DIGICAPSULE本来の機能を果たすことができる.
   ・コンテンツ鍵をデータベースで管理しないため, コンテンツ鍵の定期的なバックアップが不要となる. このため, サーバ上のデータのバックアップ作業を大幅に簡素化できる.
2. カプセル生成時の手間の低減
   ・著作権管理代行機関においてコンテンツ鍵をデータベースで管理する必要がないため, カプセル作成時に著作権管理代行機関と通信する必要がない.
   ・上記理由から, カプセル生成時の通信回数や手間を削減できる.
   ・コンテンツ鍵が各制作者端末上で生成されるので, 鍵生成に使用される乱数が十分安全であることが前提となる.
3. 特権者による監査機能の実現
   ・KRBを2つカプセルに格納することにより, キーリカバリの目的の1つである法執行機関による合法アクセスの仕組みを提供することが可能になる.
   ・米国では一定の鍵長以上の強度をもつ暗号輸出製品にはキーリカバリ機能のサポートが義務づけられており, 日本でも同様に暗号製品輸出に際してキーリカバリ機能のサポートが義務づけられる可能性がある. このため, 上記のようなキーリカバリ機能のサポートが望まれる.

上記の点が提案方式により改善されているといえる. また, 提案方式を適用することにより, DIGICAPSULE本来の機能が損なわれることはない.

6.2 安全性

提案方式では, 暗号化されるコンテンツすべてに対してKRBが作成され, カプセルに格納される. KRBは著作権管理代行機関(鍵回復センタ)の秘密鍵で暗号化されている. このため, 秘密鍵の漏洩により, あらゆるカプセル内のコンテンツの利用が可能になる. よって, 著作権管理代行機関(鍵回復センタ)の秘密鍵を厳重に管理する必要があり, そのために耐タンパー性をもつ鍵管理装置の導入等の処置が必要となるケースもある.

6.3 運用性

提案方式では, コンテンツ鍵をデータベースで管理しないため, コンテンツ鍵の定期的なバックアップが不要となる. このため, サーバ上のデータのバックアップ作業を大幅に簡素化できる.

しかし, 提案方式はDIGICAPSULEとキーリカバリシステムを組み合わせているので, DIGICAPSULEのための設定以外にキーリカバリのための設定が必要となる.

キーリカバリのための設定は，著作権管理代行機関と制作者端末で必要となる．著作権管理代行機関では，適正な鍵回復ポリシーの管理を行い，制作者は著作権管理代行機関より鍵回復ポリシーを取得し，適切に鍵回復適用条件を設定する必要がある．

しかし，キーリカバリのための設定は，インストール時に一度だけ行えばよいため，これにより運用性が大幅に損なわれることはない．

6.4 カプセルのファイルサイズの変化

カプセルを生成する際，KRBもカプセルに格納する．KRBを格納した分だけファイルサイズは増加する．

しかし，コンテンツのファイルサイズよらずKRBのサイズは一定(条件にもよるが，2KB程度)であるため，比較的大きなコンテンツ(200KB程度以上の大きさがある)の場合にはファイルサイズに大きな影響はない．

6.5 速度性能

提案方式では，カプセルを作成する際，KRB作成に要する時間の分だけ処理時間が余分にかかることになる．しかし，コンテンツの作成に必要な情報を制作者がGUIを通してを入力する場合，入力時間に比べてKRB作成時間は非常に短い(測定条件にもよるが，200KBぐらいのコンテンツの場合0.3秒程度)．このため，提案方式適用による影響はほとんどない．

また，コンテンツ購入時に，KRBからコンテンツ鍵を回復する時間が余分にかかる．この場合も同様に，コンテンツの購入に必要情報を利用者がGUIを通して入力する場合，入力時間に比べてKRB作成時間は非常に短いため，提案方式適用による影響はほとんどない．

7 おわりに

コンテンツ配布システムにおける鍵管理方式を提案した．

この方式により，著作権管理代行機関におけるコンテンツ鍵の管理が不要となり，カプセル作成時の手間が軽減される．また，提案方式を適用することにより，監査機能の実現も同時に行うことが可能である．

しかし，コンテンツ鍵の管理が不要であるかわりに，鍵回復を行うための秘密鍵を厳重に管理する必要がある．そのために，耐タンパーな鍵管理装置の導入などが必要となるケースも考えられる．

よって，提案方式により監査機能の実現やコンテンツ鍵管理が不要であるといった運用性の向上が期待されるが，鍵回復のための秘密鍵をより厳重に管理する必要が生じる．

参考文献

[1] 宮崎 一哉，中嶋 春光，中川路 哲男，“セキュアデジタルコンテンツ配布方式の検討，” 情報処理学会第55回全国大会講演論文集 6Q-1, pp.3-246, 1997.

[2] 中嶋 春光，宮崎 一哉，中川路 哲男，“セキュアデジタルコンテンツ配布システム-DIGITEX-の開発，” 1998年電子情報通信学会講演論文集 SD-3-7, pp.408-409, 1998

[3] 中野 初美，竹原 明，松田 規，中川路 哲男，“キーリカバリシステムの試作と商用システムへの応用に関する検討，” 情報処理学会研究報告, Vol.98, No.108, pp.1-6, 1998