マルチメディア通信と分散処理　97－18
コンピュータセキュリティ　8－18
（2000．3．22）

コンテンツ流通における自律管理を目的としたカプセル化コンテンツ Matryoshka

加賀美 千春，森賀 邦広，塩野入 理，櫻井 紀彦
NTTサイバースペース研究所

情報のデジタル化は様々な分野において進展し，利便の向上，効率化が期待されている．今後，経済価値のあるもの，秘匿すべきものなど様々なタイプの情報がネットワーク上を流通する環境になると予想される．その一方で，デジタル化のもたらす情報の操作性は，不正利用をも容易にし，コンテンツ流通の発展を阻害している．筆者らは，様々な種類のコンテンツ流通を促進するために，利用/加工といった操作をコンテンツ提供者の指定する利用条件に従い自律的に制御し，ライフサイクル管理を実現するカプセル化コンテンツMatryoshkaを検討している．本稿では，利用条件の構成用件を具体化し，医療分野における適用を提案する．

Matryoshka - An Autonomous Capsule for Content Usage Management

Chiharu Kagami, Kunihiro Moriga, Osamu Shionoiri, Norihiko Sakurai
NTT Cyber Space Laboratories

Information digitization has been promoted in various fields so that we can get more convenient and efficient surroundings. In the years ahead, it can be foreseen that there will be much more different types of information over a network, such as costly or confidential information. Information operability brought about by digitization, however, has led to the problem of illegal usage, which hinders the progress with the distribution of digital information. To solve the problem, Matryoshka is intended to be a content capsule which can manage autonomously the operation executed by the user upon the content. This management of content usage is under the control of the restrictions set by content provider. In this paper, we describe a specific form of the restriction and try to apply it to patient's medical records which include confidential information.

1. はじめに

インターネットの普及やデジタル化技術の進展により，ネットワークを経由してデジタル化されたコンテンツが流通する環境が整いつつある．コンテンツには様々な分野における情報が含まれ，それらの流通にあたっては，コンテンツ作成者または提供者の著作権やプライバシーなどを保護するために，コンテンツを管理する仕組みが必要である．

また,デジタルコンテンツは，完全な複製や加工などの処理が容易で，多数者間でのネットワークを使った送受信が可能であるといった特性を持ち，利用者にとって非常に扱いやすい．その反面，利用者が利益を害する不正利用を行うことや，無意識のうちに提供者の望まない行為を行うことも容易にしている．このことは，コンテンツ流通の発展を阻害する原因になっている．

本稿では，デジタルコンテンツの流通を促進させるために必要となるコンテンツ管理機構およびMatryoshka（マトリョーシカ）による実装とその適応例を提案する．

2. コンテンツ管理

2.1. コンテンツ管理の現状

デジタルコンテンツの管理について，法的規制が検討されているが，世界中に広がるネットワークでの規制の実施には限界がある．一方で，技術的な解決策として，多くのコンテンツ管理システムが提案されている．それらの多くは，提供者からのコンテンツで構成されるデータベースを有し,サーバーによる中央集約的な管理，運営を行う形式である．利用者によるコンテンツ不正利用に関しては，コンテンツに電子透かしを埋め込むことで対処しようとする場合が多い．しかし電子透かしは，不正利用があった後，著作権侵害を追及する際の証拠となり得ても，不正利用を不可能にする手段ではない．

コンテンツに利用条件を付ける方式が提案されている．コピーマート[1][2]に代表される著作権管理システムでは，コンテンツのデータベースとは独立に，利用条件等著作権データからなるデータベースを持っている．利用条件等の記述等については，XMLベースの方式が提案されている．[3][4] このようなシステムでは，利用者は利用したいコンテンツの利用

に関して契約を結び，料金を支払った後コンテンツを入手することができる仕組みになっている．また，コンテンツに利用条件や管理情報などを組み込んだカプセル化コンテンツがある．この場合，配信されるコンテンツは暗号化されていて，許諾を得た利用者だけがコンテンツ本体にアクセスする仕組を備えている．(デジタル署名，認証，鍵配信など)このようなシステムの場合，コンテンツデータとその管理手法は分離されており，ダウンロード後のコンテンツに関する管理は不十分である．つまり，特定の流通経路で特定の利用者についてのコンテンツ配信は確保されるが，配信後のコンテンツの利用について積極的に管理していない．

その他，IDによるコンテンツ管理が検討されている．コンテンツ ID フォーラム(cIDf)[5][6]では，デジタルコンテンツごとにユニークな ID(コンテンツ ID)を付与し，著作権を保護しながらコンテンツ再利用を促進する流通フレームワークを提案している．現在，ID フォーマット等の技術仕様が検討され，ID センタにより発行・管理されるコンテンツ ID に，コンテンツの管理情報，著作物属性，流通属性等の情報項目を含むことが考えられている．著作権保護のための利用制限機能については，透かし ID による対処と，不正利用の未然防止手段の併用を検討しているが，その実現手段はビジネス上，インプリメント上の判断に委ねられている．このような ID によるコンテンツ管理を目指す団体は複数存在し，The Digital Object Identifier Foundation (DOIF)[7]や，ISO の MPEG，ネットワーク音楽配信フレームワークを検討している SDMI (Secure Digital Music Initiative)[8]などがある．今後，ID を持つコンテンツの流通が予想される．

2.2. コンテンツ自律管理の必要性

コンテンツが流通する際，生成・蓄積・利用・加工といった様々な過程を経ることになる．このようなコンテンツのライフサイクルを管理しようとするマルチメディア情報ベースの研究が行われている．[9][10]その中で，コンテンツ管理のためのプログラムを内包し，カプセル化コンテンツ自身が，利用者のアクセス時に自律的に利用者の認証を行い，利用許諾を照合する仕組について研究されている．その一例として，画像ファイルの表示について，利用者の要求や支払われた対価の額によって調整できる仕組が Java アプレットにより実装されている．[11] しかし，これは Java の持つセキュリティ制限により，通信できるサーバやローカルコンピュータへのアクセスを制限されたものであり，ネットワークに接続されたコンピュータのみの利用に限られている．

今後，コンテンツの流通経路が多様化する中で，二次的な加工を含めた如何なる状態においても提供者の要求するコンテンツ管理が要求される．

こういったコンテンツの生成，流通，利用，加工などのライフサイクル全体を管理する機能を実現するためには，その中で共通に操作可能な基本単位が必要になる．[10] 筆者らは，そのような基本単位として，コンテンツ利用手段，利用条件をカプセル化して扱うことができる Matryoshka を考案，実装した．さらに，この基本単位は，コンテンツ保護の観点から，コンテンツが置かれた利用者側の環境，コンテンツ自身の状態をセンシングし，提供者の要求する利用条件に従って自律的にコンテンツを管理することを可能にしている．次章では，実現した Matryoshka について紹介する．

3. Matryoshka

3.1. Matryoshka の構造

Matryoshka の構造を以下に示す．

- ● コンテンツおよびそれ自身に関するもの
  - ・コンテンツデータ：符号化されたコンテンツ
  - ・コンテンツメタ情報：著作権情報やコンテンツの検索に使われる検索キーなどの属性情報
- ● コンテンツの表現に関するもの
  - ・コンテンツ表現情報：コンテンツのフォーマット情報，プレーヤの指定など，コンテンツを表現するための情報
  - ・コンテンツ表現プログラム：暗号復号機能のようなデータ解析手段，プレーヤなど，コンテンツデータを直接処理するプログラム
- ● コンテンツの利用に関するもの
  - ・コンテンツ管理情報：利用条件や利用状況を管理するための履歴情報など，コンテンツを管理するために必要な情報
  - ・コンテンツ管理プログラム：コンテンツ管理情報の更新，利用条件の判断など，コンテンツの利用や状態を監視，制御するプログラム
- ● Matryoshka の制御に関するもの
  - ・コンテンツ制御情報：Matryoshka 内部における処理手順

この様に Matryoshka はコンテンツ自身のほかに上記の各種情報や制御機能を内包する．

Matryoshka の実装には OLE/COM の技術を用いており，Matryoshka は OLE 複合ファイルによって実現している．OLE 複合ファイルはファイル内にファイルシステムを構成しており，そこに符号化されたコンテンツ，処理手順，利用属性に基づく利用条件，履歴情報，著作権情報，プログラムなど前述した各種情報や制御機構をそれぞれストリーム(ファイルに相当)として格納する． 構成イメージを図1に示す．

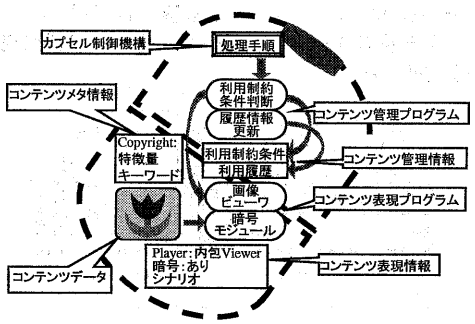


図1. Matryoshka の構造

3.2. Matryoshka 動作機構

Matryoshka は最初に Matryoshka 参照プログラムによってロードされる. 参照プログラムでは, 内包されたコンテンツ制御情報を解析し, 必要時に応じて各ストリームに改竄チェックを行いながら処理手順に基づき, 内包されたコンテンツ管理プログラムやコンテンツ表現プログラムを実行し, あとは実行された各プログラムに処理を委ねることとなる.

利用条件判断は, コンテンツ管理プログラムがコンテンツ管理情報に従い実行されることにより, コンテンツ自身の自律管理を実現している. コンテンツ管理情報／プログラムを入れかえることにより多様なコンテンツ管理が可能となる.

各プログラムはActiveXコントロールで実装されており Matryoshka 参照プログラムはそのコンテナとなっている. また Matryoshka 参照プログラム自身もコントロール化されているので Matryoshka 内にさらに Matryoshka をコンテンツとして内包するような入れ子構造にも対応している. 動作イメージを図2に示す.

各プログラムは必ずしも Matryoshka 内に内包する必要はなく, その場合は事前に動作環境で登録されていればよい.

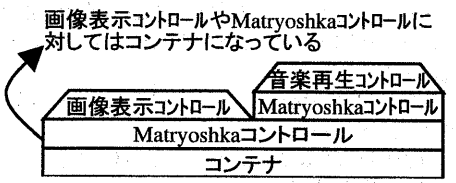


図２. Matryoshka の動作

3.3. Matryoshka 配信システム

ここでは WWW サーバを用いて Matryoshka を配信するシステムを実装したので紹介する. この実現例では, ダウンロードした端末だけにコンテンツの利用を制限することを可能にした. これを実現するにはコンテンツ管理情報に

・ ダウンロード時の端末情報を内部に埋め込む.
・ 保存したコンテンツを参照時, 既に埋め込まれた端末情報と動的に所得したものとのチェック.

を行うように記述する. これにより他の環境に再配布してもそのコンテンツを利用不可能とすることができる. このシステムの概要を図3に示す.

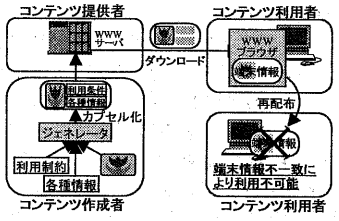


図3. Matryoshka 配信システム

コンテンツ管理情報の記述を変えることで期間や回数の利用条件を設定することができる.

4. コンテンツの利用条件

3 章で紹介したシステムの利用条件では, コンテンツ利用の回数, 期間, 期限, 利用者端末の制限を行っている. コンテンツの全ライフサイクルに対する利用条件は, 二次的な加工などを含む利用者の様々な操作について考慮したものである必要がある. この章では, 全ライフサイクル管理を可能にする利用条件について考察する.

4.1. 利用条件の構成

全ライフサイクルを通してコンテンツに及ぶ利用者の操作には以下のものがある.

・参照
・カプセル内の変更(追加, 削除, 改変等)
・他のコンテンツとの組み合わせ

また, これらの操作を制御する方法として, 回数, 期間, 期限, 利用者端末の制限, ユーザ属性, 利用目的, 利用範囲などがある. そこで, コンテンツ提供者が利用者に許可する操作(以下, 利用形態)とその制御(以下, 利用制御)の項目から, 以下のように利用条件を構成する.

利用条件＝利用形態＋利用制御

従って, 提供者が利用者に許可する操作が複数ある場合は,そのすべてについての利用条件を用意する.

コンテンツの種類や利用分野によっては, cIDf などの第三者機関の発行する ID 毎に, 利用条件を設定

する場合が考えられる．そのような場合，以下のように利用条件を記述する．

利用条件 ＝

利用形態＋利用目的(ID)＋ユーザー属性等

（利用目的をIDとして取得する場合）

そして第三者機関への問い合わせ機能をコンテンツ管理プログラムに追加することで，このような外部の規定にも適応した，コンテンツの利用制御が可能となる．

4.2. 利用条件の付与

ここでは，コンテンツのライフサイクルの中での流通過程をモデル化する．一つは，カプセルに内包されたコンテンツの表現機構に従いコンテンツを単純利用する場合，他方は，編集アプリケーション等によってカプセルを再構築(編集)する場合である．前者は利用者，後者は編集者によって行われるとすると，コンテンツ提供者からのコンテンツ流通の過程を以下のように表す．

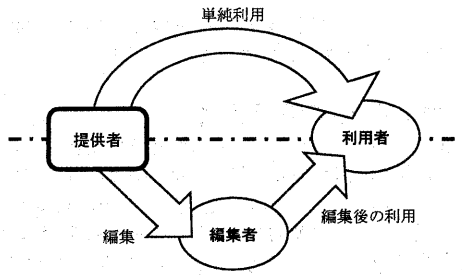


図4. 流通モデル

このモデルから3つの利用場面(単純利用，編集，編集後の利用)が考えられ，それらに対し利用条件を付与できるようにすることが必要である．コンテンツに対する利用条件の例を図5に示す．

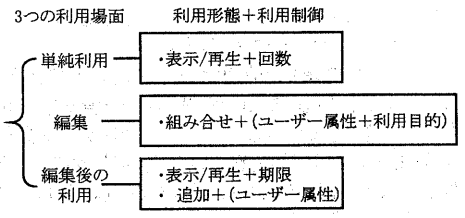


図5. 提供者がコンテンツに付与する利用条件の例

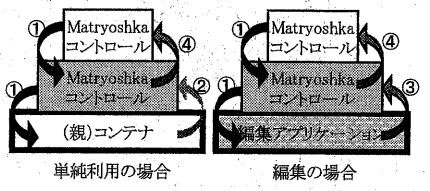
4.3. 利用条件判断機構

コンテンツには，上記のように複数の利用場面に対する利用条件が付与されている．利用条件判断の基本は，これらを適切に発動させ，利用者の操作の可否を判断することである．その結果に基づいてMatryoshkaは動作する．

●利用場面，利用形態の判断

図6に判断機構のイメージを示す．

Matryoshka コントロールは基盤となる(親)コンテナが編集機能を持っているか問い合わせて利用場面を判断する．



①: Matryoshkaコントロールからの問い合わせ
②:編集機能を持たない(親)コンテナからの応答
③:編集アプリケーションからの応答
④: MatryoshkaコントロールからMatryoshkaコントロールへの応答

図6. 判断機構

Matryoshka コントロールは自分の親となるコンテナに問い合わせコンテナからの応答を受ける．コンテナがMatryoshkaコントロールであれば再帰的に問い合わせを行う．このとき，Matryoshka コントロールから子供のMatryoshka コントロールへの応答(④)には，(親)コンテナの編集機能の有無と自身がMatryoshkaコントロールであるという情報を伝える．このようにして，編集アプリケーションによる処理であるかどうか，及び自身が編集物であるかどうかを判断する．また，自身が編集物であることは，履歴情報からも分かり，編集後の利用条件を発動する判断材料となる．編集機能の無いコンテナ上にある場合，内包されているコンテンツ表現プログラムによる処理であると判断し，単純利用に対する利用条件を発動させる．単純利用における利用形態は内包されている表現プログラムから判断でき，編集における利用形態の判断は編集前後のデータの差分から判断し，適切な利用条件を発動する．

●利用制御の判断

コンテンツ管理プログラムは，利用場面と利用形態を判断し利用条件を特定した後， Matryoshka内，システム内，第三者機関などから識別情報を取得し設定された利用制御と比較判断する．以下，取得情報の例を挙げる．

・時間制限の場合，システムの時間情報．正確な時間を外部サーバーから得る．

・回数制限の場合，Matryoshka内に記録した操作に関する履歴情報．

・ユーザー属性の場合，利用者のネットワークやマシンの限定には，IPアドレス，MACアドレスを用いる．ユーザーが任意に属性を入力する形をとることも可能だが，認証サーバーなどの第三者機関またはICカードによる認証機能により，ユーザーのなりすましを防止する．

・利用目的等の場合，既存情報で判断するのが困難なメタ情報であるので，第三者機関による判断に委ねる．Matryoshkaは，コンテンツが持つID等の認証のために第三者機関にアクセスし，自律的に認証を行う．

5. 適用例：医療分野の場合

Matryoshkaは，著作権保護だけでなく，プライバシー保護を必要とする情報の管理も行う．例えば，情報提供において利用者の特定及び情報量の制限などを必要とするコンテンツの場合である．

この章では，医療従事者がMatryoshkaを使って医療情報，特に電子カルテを提供する場合を考える．利用条件を構成する項目は公開文書[12][13]を参照している．概要を図7に示す．

5.1. 利用条件の例

電子カルテは，患者個人の情報,主訴,現病歴や症状,病名,血液検査データ,心電図,X線画像やその他の画像検査,保険情報,投薬情報などを含んでいる．これら複数の情報は，同じ場所で同じ担当医によって作成されるわけではなく，担当医の診療記録をはじめ，複数の検査・測定の記録が追加されて構成されている．また，それぞれ個人のプライバシー情報を含んでおり，利用に関して，提供する情報毎に利用目的，利用者，利用範囲を限定することが重要になると考えられる．そこで，各々の医療情報毎にカプセル化し利用条件を付与する場合を考える．カルテ全体としては，複数の Matryoshka を内包する一つのMatryoshkaとする．

利用条件の項目として以下のような例を挙げる．

＜利用目的＞
・診察/治療　・薬剤の調製
・医療機関の運営管理
・医療保険　・研究　・教育　・行政上の調査

これらは，あらかじめ第三者機関に管理されたIDによって識別するものとする．

＜利用形態＞
・参照 ・追加 ・組み合せ

＜ユーザー属性＞
・患者本人 ・担当医 ・担当検査医
・薬剤師 ・担当看護婦

＜範囲＞
・全体 ・検査データ

これをもとに Matryoshka に利用条件を付与する例を示す．例えば，図7におけるMatryoshka1は，患者が専門病院で人間ドックなどの検査を受けた時のデータが内包される．Matryoshka1に設定される利用条件は表1のとおりである．

表1，Matryoshka1における利用条件の例

利用場面	利用形態	利用制御		
		利用目的	ユーザー属性	範囲
単純利用	参照	診察・治療	担当医	全体
			患者	
		病院の管理	担当者	
編集	参照	研究	研究者	検査データ
	組合せ			
編集後の利用	参照	教育	研究者	検査データ
			学生	

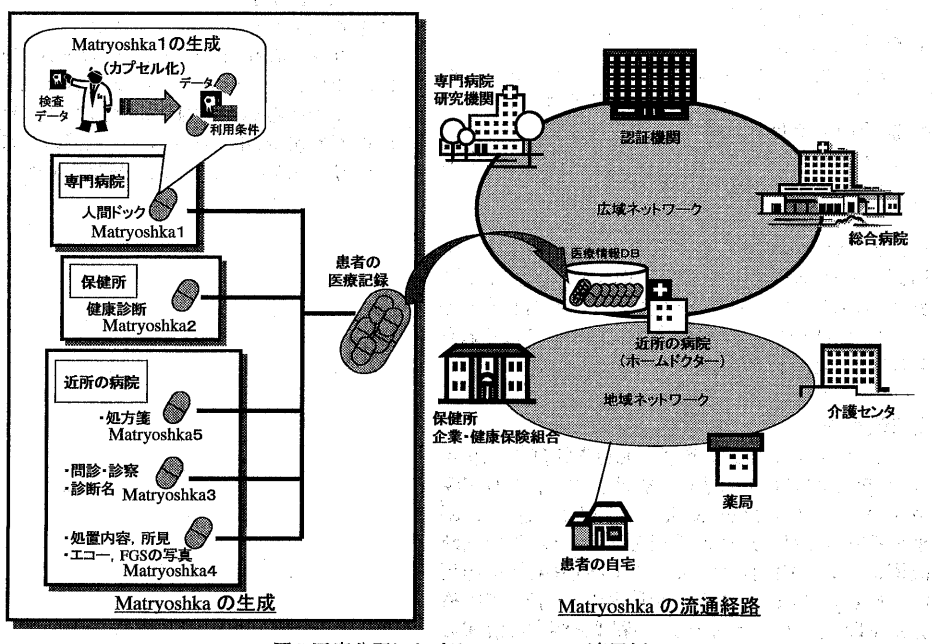


図7，医療分野におけるMatryoshkaの適用例

5.2. 流通過程

患者の医療記録についてMatryoshka1～5があり，それらを内包したMatryoshkaが一つのカルテとして，データベースに蓄積されているとする．これらが仮にネットワーク上を流通し利用される際には，利用条件に設定された利用者の属性と利用目的がID認証機関等で認証され，記述されている利用条件で利用される．

例えばMatryoshka1の利用条件(表1)の場合，患者が通院するホームドクターは内包されている人間ドックの結果を閲覧でき，診断の参考に利用することができる．また，人間ドックの検査を行った専門病院においては運営管理のために，担当者が閲覧する．研究機関では，人間ドックデータ内の内視鏡の画像などが症例の資料として編集利用される．この編集物は臨床研修を受ける学生に閲覧される．

5.3. 解決しようとする課題

Matryoshkaは，医療分野における以下の課題を解決する．

1，セキュリティ・プライバシーの保護

各情報に利用条件を付与し，認証サーバーなどの第三者機関またはICカードによる認証機能により，利用目的や利用者属性を限定したアクセス制限を行える．また，アクセスを許可した者の操作を制限して改竄を防ぎ，情報の範囲を限定して患者の特定を防ぐ．

2，利用履歴の管理

利用者および操作に関する履歴を管理でき，データ利用者を特定する．

3，データの統合

様々な場所で作られた同じ患者のデータを入れ子構造にして一つのデータとして構築する．

4，流通後の管理

カプセルが単独で流通しても，付与された利用条件に従った利用を維持する．

医療記録の電子化とその流通には，記載形式，使用語等の標準化や，医学的見地などから患者の閲覧についてのガイドライン整備など様々な課題が残されており[14][15]，実際の適応にあたってはそれらを考慮しなければならない．

6. まとめ

本稿では，コンテンツ流通における管理の現状からコンテンツの自律管理の必要性を述べ，その実現方法の一つとしてMatryoshkaを紹介した．さらに，編集を考慮した利用条件の構成を具体化し，その判断機構について検討した．また，この利用条件を適用したMatryoshkaのコンテンツ管理の一例として医療分野を取り上げ，プライバシー保護を要する情報の管理について考察した．

参考文献

[1] 北川善太郎，“電子著作権管理システムとコピー・マート”，情報処理第38巻第8号，1997，663-668

[2] http://www.copymart.gr.jp/japan/tophome.html

[3] 星野他，“コンテンツの複合的権利記述による権利保護と流通支援”，情処研報,Vol. 98, No.85, EIP-2, pp. 1-8, 1998

[4] 熊沢他，“他権利者間の権利関係及び利益分配方式の記述によるコンテンツ再利用支援”，情処研報，Vol. 99, No.11, EIP-3, pp. 65-72, 1998

[5] CIDF Specification1.0 Working Draft Ver.1.0

[6] http://www.cidf.org

[7] http://www.doi.org

[8] http://www.sdmi.org

[9] 田中克巳，“マルチメディアコンテンツのアクセスアーキテクチャ”，ADBS‘97，1997

[10] 谷口他，“マルチメディア情報ベースとその格納単位Matryoshka”，DICOMO‘99シンポジウム論文集，pp. 207-212, 1999

[11] 木俵他，“版権管理のための Java による画像データカプセル化，情処研報,97-DBS-111，1997

[12] 日本保健医療情報システム工業会
電子カルテのセキュリティ特別WG 電子カルテシステムのセキュリティ設計 厚生省事業からの報告(平成8年11月)

[13] 厚生省報道発表資料 98/06/18「カルテ等の診療情報の活用に関する検討会」報告書概要

[14] 財団法人医療情報システム開発センター医療情報処理関連の標準化動向調査 成8年度報告書

[15] 医療記録の開示をすすめる医師の会編集 金原出版「医師のための医療情報開示入門」