平成20年度 卒業論文

論文題目

著作権管理のための匿名通信

神奈川大学 工学部 電気電子情報工学科

学籍番号　200402898

遠山　真一朗

指導担当者　木下宏揚　教授

目 次

第 1 章　序論　5

第 2 章　基礎知識　7

2.1 DRM（ディジタル著作権管理）. 7
2.2 既存の匿名通信方法 9
2.2.1 匿名 proxy サーバ 9
2.2.2 オニオンルーティング 10
2.2.3 Mix-net 11
2.3 カプセル化 13
2.4 エージェント 14
2.4.1 エージェントとは 14
2.4.2 エージェントの分類 15
2.4.3 モバイルエージェント 16

第 3 章　提案ネットワーク　17

3.1 情報カプセル 17
3.2 エージェント間の交渉 18
3.2.1 情報カプセルエージェント 18
3.2.2 アクセス制御エージェント 19
3.3 Dublin Core 20
3.3.1 拡張 Dublin Core モデル 22
3.4 提案するネットワーク 23
3.4.1 コンテンツの二次利用 24
3.4.2 コンテンツの二次配布 25

第 4 章　　結論 **28**

謝辞 **29**

参 考 文 献 **30**

質疑応答 **32**

図 目 次

2.1 オニオンルーティング 10
2.2 Mix-net 11
2.3 カプセル化コンテンツ 13
2.4 エージェントの分類 15

3.1 情報カプセル 17
3.2 Dublin Core モデル 26
3.3 提案するネットワーク 27

表 目 次

第1章

序論

近年,PC の高機能化やネットワークの高速化により, 音楽, 動画, 画像などのディジタルコンテンツの流通が盛んになってきている.[8] ディジタルコンテンツの最大の特徴として, 無劣化で複製が容易であるということがあげられる.[9] 一方, P2P ネットワークなどを介し, 無断送信が禁止されている映像や音楽ファイルの不正流通が社会問題となっており, DRM（ディジタル著作権管理）といったコピー制御機構の確立が緊急課題となってきている. DRM に関しても恒久的な再生が保障されていない、消費者の権利に対する不当な制限など改善すべき点が多い. また著作権だけではなく個人情報に関する権利の保護を求める声も高まっており情報セキュリティの対策が必要不可欠なものとなっている.[5] また一方でオープンソース等の配布や改変を認めているという流れもある. 従って著作権の所有者とそれを利用するユーザの間には様々な権限に対する要求に柔軟に対応可能なシステムが求められる.[3] そこでディジタルコンテンツの流通に暗号化されたディジタルコンテンツとそれに対する暗号鍵, 著作権情報, 管理エージェントなどをパッケージ化した情報カプセルを導入しこのカプセル内の情報カプセルエージェントとアクセス制御エージェントが交渉を行うことによりコンテンツを管理するという考えもある [4] しかしエージェント間で通信を行う際に流通後のコンテンツの位置の把握が困難ということや利用者などのプライバシーを保護する必要が出てくる．そこで著作物をデータベース側で管理するツールとして Dublin Core に着目する.

Dublin Coreは,簡潔なメタデータを定義してネットワークを介した情報源へのアクセスを促進する事を目的に作られたものである．メタデータはデータに関する構造化されたデータであり，それを使う事によってデータベースへのアクセスの相互操作性，柔軟性，拡張性を向上させる効果がある．また，Dublin Core はメタデータのコア要素の１つとして「権利管理」が定義されている．そこでこの要素を著作権，利用の権限のために拡張する．本稿が着目するシステム構成は,“ 拡張Dublin Core とアクセス制御リストによりデータベースを管理するエージェント ”,“ 著作権や利用の権限を制御するエージェントを伴うコンテンツのカプセル ”,“ ユーザ側のエージェント ”である．データベースには著作者が作成した著作物が格納される．データベースの管理エージェントは，データベース内部のデータの読み書きに関しては従来のアクセス制御技術が適用される．[10] しかし，一度データベース内部のコンテンツがネット上に流通すると，一般には制御不能になってしまう．本稿では既存の情報カプセルにTake-Grant と情報フィルタ，エージェントを導入し，コンテンツ利用の利便性を向上する方法を提案する．このシステムにより，コンテンツの利用の利便性の向上が期待される．本稿ではプライバシーを保護しつつ流通後のコンテンツのエージェントと権利者のエージェントが通信可能な匿名経路制御を提案する.

第2章

基礎知識

2.1　DRM（ディジタル著作権管理）

デジタルデータとして表現されたコンテンツの著作権を保護しその利用や複製を制御・制限する技術．主な技術としては音楽・映像ファイルにかけられる複製の制限や電子透かし,itunes における FairPlay,Adobe LifeCycle などがあげられる．デジタル化されたコンテンツは何回でもコピーしても品質が劣化しないため P2P など違法な配布・交換が増えているこれに対抗するためにコンテンツの流通・再生に制限を加える DRM 技術が注目を集めている．[1] DRM はコンテンツ利用者の利便性を損なうことなく著作権および所有者に適切な対価を還元することを目標としている. DRM を実現する仕組みにはさまざまなものがあり, その機構はコンテンツの形式や利用形態によって異なるが, ユーザが特定の再生ソフトウェア（iTunes や Windows Media Player など）を使い, 暗号化されたコンテンツを復号しながら再生する方式が一般的である. 暗号化に使われる鍵（キー）は再生ソフトウェア内に隠されているか、あるいはネットワーク上からダウンロードされることが多い. この再生ソフトウェアがユーザのコンテンツ用を管理するため, 利用期間の切れた後には再生不能にするなどの処置が可能になる.

DRMシステム（ディジタル著作権管理）の必要条件としては以下に示す

１・著作権の所有者は処理情報の条件を設定可能

２・分配された情報の完全性は保障されなければならない

３・所有者は使用者側での処理情報の妥当性をチェック可能

４・所有者は情報を使用するための条件を変更することが可能

５・所有者は分配された情報を最新のものにすることが可能

しかしDRMにも欠点がある [5]

- **恒久的な再生が保障されていない**

  DRM技術のほとんどが特定のメーカーによって定められ,その技術的詳細が一般に公開されていないことから,そのメーカーやサービスが活動を停止した際に,購入したコンテンツが将来にわたっても利用可能なのかが必ずしも担保されていない.

- **消費者の権利に対する不当な制限**

  DRMはその技術的特性により,通常,複製以外の利用 (著作権法によって認められている範囲での抜粋や,他人への譲渡など) も制限することが多い.このため,DRMは購入した製品を自由に使う消費者の権利を奪っているとの主張もある.

2.2 既存の匿名通信方法

2.2.1 匿名 proxy サーバ

proxy サーバを使用しないでホームページにアクセスした場合は，ユーザのコンピュータが接続先に直接アクセスするため，ユーザの個人情報がWWWサーバと接続先ページに残る. 一方で proxy サーバという仕組みがあり,proxy サーバを介してＷｅｂページを閲覧する場合は,proxy サーバがユーザの代わりにアクセスしてくれるので, アクセスされたWWWサーバには proxy サーバの IP アドレスしか残らないので、クライアントマシンの IP アドレスは知られない．しかし，proxy サーバにはクライアントの情報が残っているので proxy サーバの記録を調べられるとアクセスした個人の情報が漏れてしまう

2.2.2 オニオンルーティング

AnonymousProxy（匿名プロキシ）の一種で仮想回線接続により,通信を複数のノードを経由させることにより,匿名性を高めている. 暗号化が,あたかもタマネギの皮のように1ホップごとに積み重ねられることが名前の由来である. 現実装においてはTCPでの通信を行うことができるがUDPやICMPなどのプロトコルは使用することができない.[5]

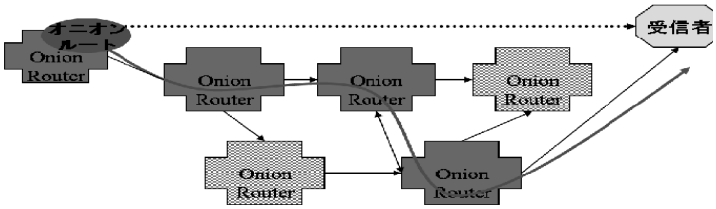

図 2.1 オニオンルーティング

2.2.3 Mix-net

接続元端末はまず各ＭＩＸサーバから公開鍵をもらう.ＭＩＸサーバ毎に公開鍵は異なり,また接続先サーバからも公開鍵をもらう.まず,端末は通信したい内容を次のように暗号化

通信内容⇒サーバ公開鍵で暗号⇒公開鍵２で暗号化⇒公開鍵１で暗号化⇒暗号化通信内容

まず,暗号化通信内容をＭＩＸサーバ１に渡す.ＭＩＸサーバ１は公開鍵１のペアである秘密鍵１で復号化.（復号化した内容を暗号化通信内容１と呼ぶ.次にＭＩＸサーバ１は暗号化通信内容をＭＩＸサーバ２に渡す.ＭＩＸサーバ２はＭＩＸサーバ１と同様,秘密鍵２で復号化.（暗号化通信内容２と呼ぶ）ＭＩＸサーバ２は暗号化通信内容２を接続先サーバに渡す.接続先サーバは秘密鍵で復号化して通信内容を把握できる.MIX サーバ１,MIX サーバ２は通信内容を知る事はできない.

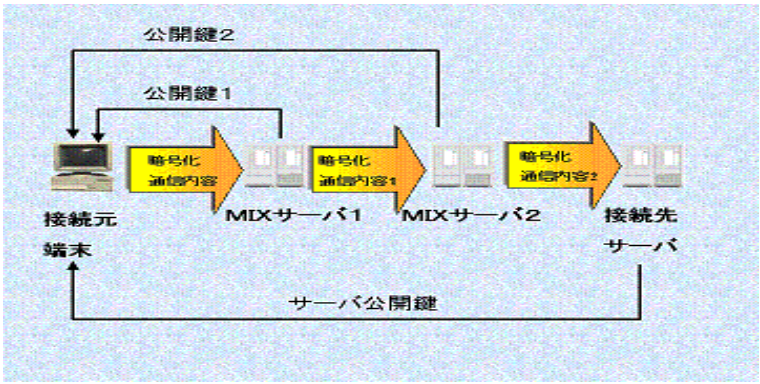

図 2.2 Mix-net

MIX サーバではまず,多くの人から来た通信内容を一旦蓄積する.ある程度溜まると,それをランダムに次の MIX サーバに渡す.また,通信内容の長さを揃えるために,わざと情報内容に「詰め物」をする.このようにすれば,MIX サーバの前後で通信を盗聴されても「だれの通信がいつ MIX サーバから送出されたか」わからなくなる.

欠点としては

・通信をサーバで一旦蓄積するために即時性にかける・端末側が複数回通信内容を暗号化するためにかなりのスペックが必要・サーバを全て調べ上げると接続元が判明してしまう

2.3 カプセル化

カプセル化とは, オブジェクト指向プログラミングが持つ特徴の一つであり, データとそれを操作する手続きを一体化して「オブジェクト」として定義し, オブジェクト内の細かい仕様や構造を外部から隠蔽することである. [1] 外部からは公開された手続きを利用することでしかデータを操作できないようにすることで, 個々のオブジェクトの独立性が高まる. カプセル化の利点としては以下のようなものが挙げられる.[2]

- 不正な操作からの保護
- 複雑さの隠蔽
- 部品化/再利用性の向上
- 修正/変更に対する影響範囲の極小化
- バグの影響範囲の極小化

P2P ネットワークの普及などによるコンテンツの不正流通が社会問題となっている中, カプセル化はコンテンツを保護する手段として非常に有効である. カプセル化コンテンツ自体は超流通的に自由にコピー・転送され, 電子鍵と組み合わせることによって, コンテンツの閲覧・再生が可能となるという仕組みにすることで, 実質的にコンテンツの権利を保護することが可能となる.

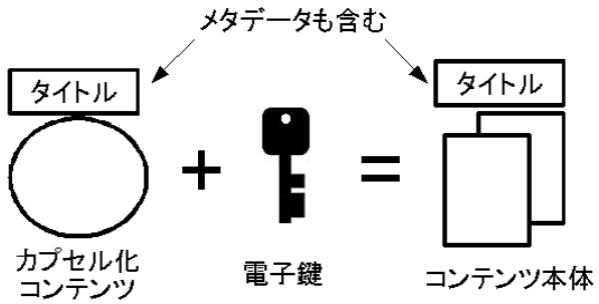

図 2.3 カプセル化コンテンツ

2.4 エージェント

2.4.1 エージェントとは

エージェントはユーザの代理人として機能するシステムである. 「エージェント」という用語はソフトウェアの抽象化/アイデア/概念を説明するものであり, その意味でオブジェクト指向プログラミングの各種用語 (メソッド, クラス, オブジェクトなど) と同類である. また, 様々な人々がそれぞれにエージェントの定義を提案しているが, それらには以下のような概念が共通して含まれている.[5]

- **永続性**
  そのコードは要求されて実行されるのではなく, 常に起動された状態で, 何らかの行動を起こす時期を自身で判断する
- **自律性**
  エージェントは, 実行すべきタスクの選択優先順位付け, 目標に向けた行動, 意思決定を人間の手助けなしで行う機能を持つ
- **社会性**
  エージェントは他のコンポーネントと何らかの通信や協調をする機能を持ち,1 つのタスクを共同で処理する
- **反応性**
  エージェントは周囲の環境を把握し, その変化に適切に反応する

2.4.2 エージェントの分類

多くの場合, 一つのエージェントがすべての機能を実現するのは難しい. また, エージェントという名称を使う場合には, ある要素機能に着目して, いろいろな形容詞を付けて呼ばれることが多い.

1. **自律エージェント**
   自己充足的であり, 観測された環境に基づいて内部目標を達成するための行動を独自の判断で決定する

2. **知的エージェント**
   一種の人工知能的機能を有するエージェントで, ユーザーを補助し、繰り返し行うべきコンピュータ関連のタスクをユーザーに代わって行う

3. **マルチエージェント**
   単体では目的を達成できず, 複数のエージェントが相互作用を及ぼしながら動作する

4. **モバイルエージェント**
   ネットワークに接続されたコンピュータ間をプログラムが移動しながら処理を行う

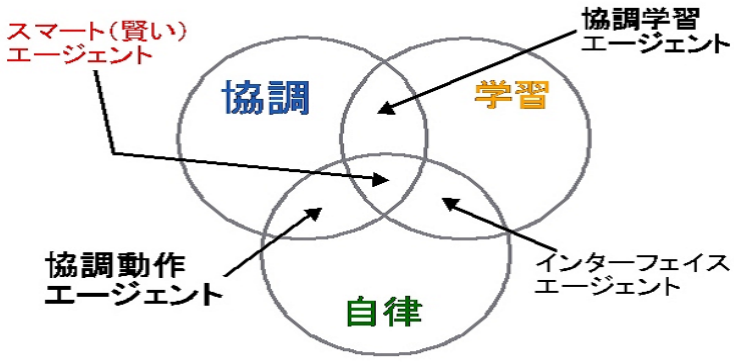

図 2.4 エージェントの分類

2.4.3 モバイルエージェント

エージェントのどのような機能に着目するかによって,エージェントが分類されることは2.4.2において述べた. ここでは,その一つであり,本研究においても重要となるモバイルエージェントについて,さらに詳しく説明する.

モバイルエージェントはネットワークを介した分散処理技術の一種であり,状態を保持したまま自律的にネットワーク上を移動し,到着したPC上で処理を継続するプログラムである.モバイルエージェントの利点としては以下のようなものが挙げられる.[6]

- **ネットワーク負荷の削減**
  タスクを局所化することで転送データを減らすことが可能
- **非同期実行**
  移動先と移動元は独立,時間節約につながる
- **通信切断への対応**
  移動後は通信切断しても処理可能
- **動的経路変更**
  移動先と移動タイミングを自律的に決定・移動
- **並列実行・負荷分散**
  複製を生成して並列処理可能
- **通信回数・遅延の低減化**
  通信相手側コンピュータに移動・処理

一方,モバイルエージェントを使用するということは,外部からやってきた信頼できないエージェントを自分のPC上で実行することも意味するため,セキュリティの問題が非常に重要となってくる.また,ネットワーク上を移動するという観点から,盗聴や改ざんといった問題への対策も必要である.

第3章

提案ネットワーク

3.1　情報カプセル

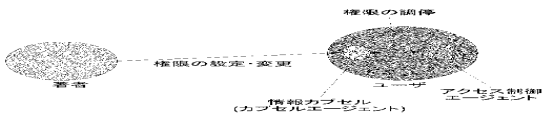

図 3.1　情報カプセル

暗号化されたコンテンツは, 情報カプセルエージェントにより管理されているため, 利用条件が満たされない限り, コンテンツを復号し, 再生することはできない. ただし, カプセル化コンテンツ自体はコンテンツ管理者のサーバ, P2P ネットワークなどを介し, 自由に流通できるものとする

3.2 エージェント間の交渉

コンテンツの管理はアクセス制御エージェント, 情報カプセルエージェントと称する2つの制御プログラムにより行われる. 2つのエージェントは, それぞれ様々な役割を果たすが, 主にアクセス制御エージェントはコンテンツを取得する権利 (Take), 情報カプセルエージェントはコンテンツを提供する権利 (Grant) が与えられている. この情報カプセルエージェントとアクセス制御エージェントの間でコンテンツの利用に関する交渉が行われ, 契約が成立すれば, ユーザは許諾範囲内でのコンテンツの利用が可能となる. 以下に各エージェントのそれぞれの役割を説明する.

3.2.1 情報カプセルエージェント

- コンテンツ管理者 (権利者) もしくは, サイト運営者が使用するエージェントで Grant 権をもつ
- 情報カプセルエージェントはカプセル化コンテンツの中に組み込まれておりコンテンツ流通における不正流通の監視, アクセス制御等を行う
- 不正流通が行われた場合にはすぐに管理者に連絡する
- XrML により記述された著作権情報・利用条件を参照することで, コンテンツの利用の可否を判別する
- 情報カプセルエージェントはカプセル化コンテンツと共にネットワーク上を自由に流通しており, 各ユーザのアクセス制御エージェントと交渉を行う必要があるため, モバイルエージェントとする.

3.2.2 アクセス制御エージェント

- ユーザからのアクセス権の要求を受けて, コンテンツ管理者からユーザへ送信され, ユーザ側で使用されるエージェントで Take 権をもつ
- アクセス制御エージェントの秘密鍵により暗号化されたセッション鍵を復号できる
- ユーザ毎にコンテンツ管理を行う必要があるため, 複製が不可能でなければならない
- アクセス制御エージェントはプレーヤやブラウザなどのソフトウェア上で動作する

3.3 Dublin Core

メタデータはデータについてのデータであり，インターネットに分散配置されたデータベースの中にどの様なデータがあるかを記述し，検索効率を上げる目的がある．Dublin Core Metadata Element Set は，この様に多種多様なメタデータを効率的に参照，交換する必要最小限のメタデータの組み合わせ（メタデータセット）として開発された．以下はDublin Core の 15 個のエレメントである・タイトル (情報資源に与えられた名前)

・作成者 (情報資源の内容の作成に主たる責任を持つ者)

・主題及びキーワード (情報資源の内容の主題)

・内容記述 (情報資源の内容の説明)

・公開者 (情報資源を提供している主体)

・寄与者 (情報資源の内容に貢献している者)

・日付 (情報資源のライフサイクルにおけるイベントに関連する日)

・資源タイプ (情報資源の内容の種類またはジャンル)

・形式 (情報資源の物理的または電子的形式)

・資源識別子 (与えられた環境において，情報資源の一意に定まる参照)

・出処 (現在の情報資源が作り出される源となった情報資源の参照)

・言語 (情報資源の内容を記述する言語)

・関係 (関連情報資源への参照)

・時間的，空間的対象範囲 (情報資源の範囲または領域)

・権利管理 (情報資源に含まれる，ないしは関わる権利に関する情報)

その中で，著作権に関する要素に rights がある．これは，リソースが保持する，あるいはリソースに適用される権利に関する情報で，通常，リソースの権利管理宣言やそのような情報を提供するサービスについて言明されて，知的所有権，著作権などのさまざまな財産権などの情報を含むことが多い．この要素がない場合は, リソースの権利に関していかなる憶測もたてない事になっている．また，right の拡張要素として，accessRights がある．これは，誰がリソースにアクセスできるかについての情報もしくはセキュリティステータスの提示で，アクセス権は，プライバシー，セキュリティ又はその他の規

則に基づいたアクセスあるいは制限に関する情報を含んでいる場合がある．しかしながら，権利管理における要素における拡張がなされておらず，また，利用目的が明白でないなど，Dublin Core の表現が不足している．

3.3.1 拡張Dublin Coreモデル

著作権を保護するために必要な機能は以下のとおりである.

1. 利用目的が明白である

2. 著者の名前とコンテンツが対応していること

3. 著者が流通しているコンテンツの権限を更新，削除することが可能

著作権に拡張したDublin Coreモデルを図3.2に示す．Dublin Coreの表現を，著作物に関する権利関係や利用目的などについてさらに拡張したもので，著作権情報の詳細が既存のものよりも明白になっている．図3.8において，著作物の権利が何なのかを確認する．著作権とは狭義の著作権である複製権，上演・演奏権，上映権，公衆送信権，口述権等に対応する．利用条件とは，その中の一つの権利の有無あるいは金銭との関連の組合せである．RDFではこのような各権利に対応して書き下す.

権利ごとに3つに分類される.

・利用目的1　著作者の権利がないときで，例えば，著作権法での著作物の著作権の期間が終了したときである.

・利用目的2　著作者の権利がある状態で，ユーザの利用における課金が発生しない場合である.

・利用目的3 著作者の権利があり，かつユーザが利用する際に課金が発生する場合である.

それぞれの権利において利用目的が何なのかをコンテンツのダウンロードと複製，改変の3つにに分類できる．利用目的2と3では複製において，配布する際に配布後のコンテンツが残って使える状態なのか残ってても使えないまたは再配布後にコンテンツ自体削除されるかの2つに分類される．利用目的2において，それぞれの目的において著作権の使用における許可するかどうかに承認が必要なのか，承認なしでも利用できるのかに分類される．利用目的3において，許可するかどうかについては課金によって制御される．また，二次的，三次的に利用または配布においてこのモデルを適用すれば，著作権情報の権限が保持され，安全に流通できるようになる．提案法においては，権限の設定に利用する.

3.4 提案するネットワーク

ネットワークが図3.3に示すノードで構成されるよう仮定. カプセルはコンテンツ, アクセス制御とルーティング確認を管理するエージェントを持つ. これらのノードの機能はカプセルを作成, 使用, 転送.

ネットワークの構造は以下の通り

- distributor（配布者）は著作権を所有しているか配布されたコンテンツの所有者. 所有者はコンテンツのアクセス権と目的を変更可能
- ユーザはコンテンツを使用し二次コンテンツを作成. したがってユーザは配布者ともなりえる
- エージェントはコンテンツに同伴してユーザのノードでのコンテンツの使用を管理
- ルータはコンテンツをメタ情報と共に転送. この情報はエージェントとルーティングに使用されたトレースセットからなる
- カプセルはコンテンツ, エージェント, トレースセットでできている.
- アップリンクメッセージは配布者からエージェントまで転送されたデータもしくはメッセージ. このメッセージはコンテンツを更新するかアクセス権を制御するのに使用.
- ダウンリンクメッセージはエージェントから配布者まで転送されたデータもしくはメッセージ. このメッセージはエージェントがコンテンツの証明を確認できないときそれをチェックするのに使用.

3.4.1 コンテンツの二次利用

エージェントによる制御によって行う手順

1. ユーザが著作者(または配布者)に欲しい情報を要求し，利用目的を伝える．

2. 著作者側のアクセス制御エージェントが著作物を著作権モデルに適用し，カプセル化してカプセルエージェントを生成する．

3. カプセル化コンテンツをユーザに配布する．

4. カプセルエージェントがユーザ側のアクセス制御エージェントと権限が一致しているかどうか確認する．

5. ユーザがコンテンツの中の欲しいデータを抽出し，それを元に編集し，二次著作者となる．

6. アクセス制御エージェントが他のユーザの欲しい情報の要求と利用目的を受け取り，カプセル化して，著作者のカプセルエージェントに加えて新たなカプセルエージェントを生成する．

7. 新たに作られたカプセル化コンテンツを他のユーザに配布する．

3.4.2 コンテンツの二次配布

二次配布では以下のような流通を行う.

1. ユーザが著作者 (または配布者) に欲しい情報を要求し，利用目的を伝える.

2. 著作者側のアクセス制御エージェントが著作物を著作権モデルに適用し，カプセル化してカプセルエージェントを生成する.

3. カプセル化コンテンツを利用者に配布する.

4. カプセルエージェントが利用者側のアクセス制御エージェントと権限が一致しているかどうか確認する.

5. カプセルエージェントがユーザにたどり着いたときにユーザの存在を確認し，履歴としてカプセルに書き込む.

6. ユーザのアクセス制御エージェントは，カプセルを再配布する際にカプセルを複製する．そのとき，複製されたカプセルエージェントにおいてはユーザの履歴が入っているとする.

7. 他のユーザへ再配布する.

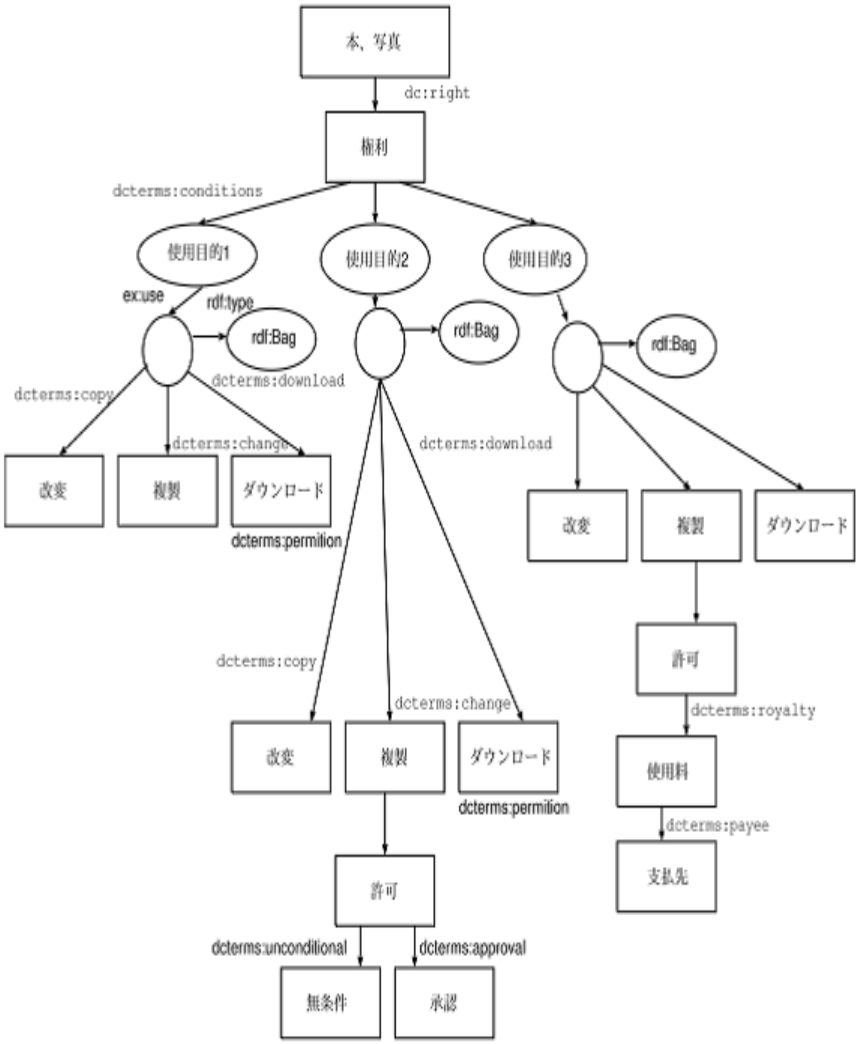

図 3.2 Dublin Core モデル

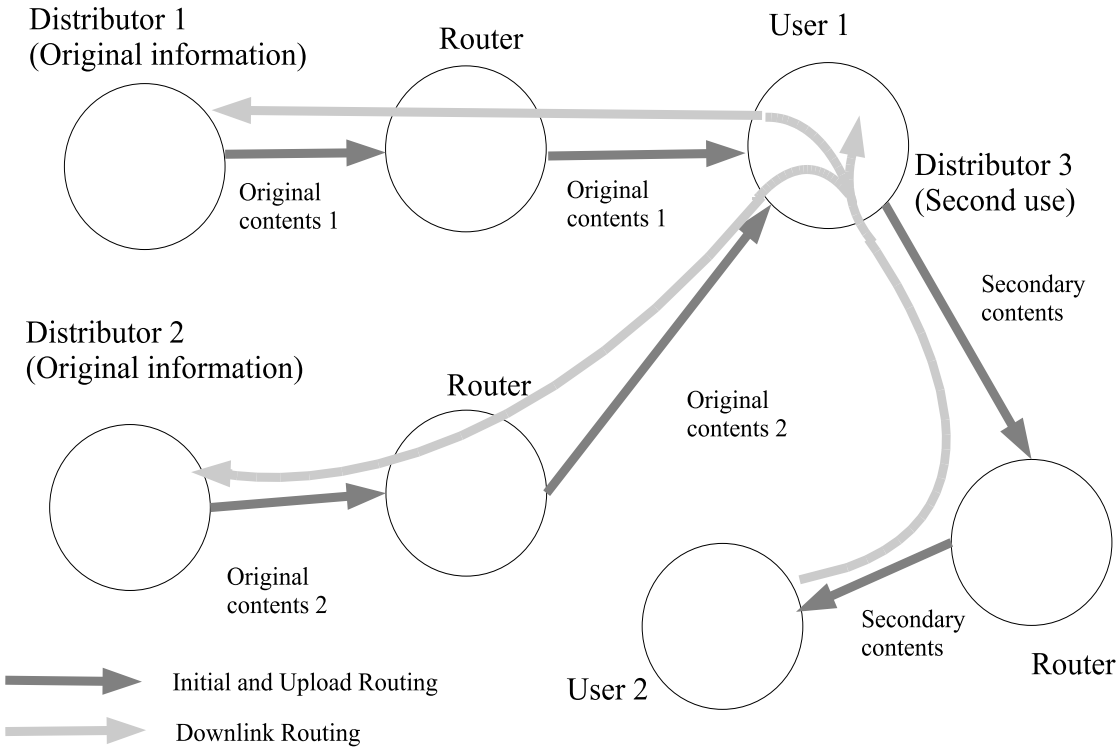

図 3.3 提案するネットワーク

第4章

結論

本研究ではプライバシーを保護しつつ流通後のコンテンツのエージェントと権利者のエージェントが通信可能な匿名経路制御を提案した. 今後の課題としては実際にシステムの構築方法を検討していきたい.

謝辞

本研究を行なうにあたり，終始熱心に御指導していただいた木下宏揚教授と鈴木一弘助手に心から感謝致します．また，公私にわたり良き研究生活を送らせていただいた木下研究室の方々に感謝致します．

2009年2月

遠山　真一朗

参考文献

[1] ”IT 用語辞典”
http://e-words.jp/

[2] ”カプセル化と隠蔽”
http://www.nextindex.net/java/capsulate.html

[3] 山田孔太：
情報カプセルを用いた著作権管理 2006

[4] 須田大介：
エージェントによるカプセル化コンテンツの著作権管理 2008

[5] ”ウィキペディア（Wikipedia)”
http://ja.wikipedia.org/wiki/

[6] ”モバイルエージェント”
http://research.nii.ac.jp/ ichiro/download/satoh-nii010516.pdf

[7] 山田孔太, 木下宏揚, 森住哲也:
”情報フィルタと情報カプセルによる著作権所有権保護システム”

[8] 五十嵐達治, 遠藤直樹, 川森雅仁, 古原和邦, 三瓶徹, 中西康浩：
”ユビキタス時代の著作権管理技術”, 東京電機大学出版局, 2006.

[9] 山田孔太, 木下宏揚, 森住哲也, 稲積康宏：
”エージェントベースの情報カプセルを用いたコンテンツ利用の
利便性の向上”, SCIS2007

[10] 牛頭靖幸，森住哲也，稲積泰宏，木下宏揚 :
”Covert Channel 分析評価のためのアクセス制御エージェントシステムの提案 ”

質疑応答

Q：実際にシュミレーションしてみたか？

A：実際にns2を使いシュミレーションしてみようとしましたがうまくtclやC＋＋といった言語を扱うことができずコンパイルなどでエラーとなってしまいシュミレーションを行うことが出来ませんでした