2007年度修士論文

分散メタP2Pストレージによるコンテンツ配信システムの実現

早稲田大学理工学研究科

情報・ネットワーク専攻

岡本 雄太

学籍番号：3606U022-9

提出：2008年2月4日

指導：山名早人教授

概 要

本論文では、P2P ファイル共有ネットワーク上でファイルへの一意なアクセスと流通コンテンツのコントロールを可能にする新たなシステム「分散メタ P2P ストレージ (**Di**stributed **M**eta-**P**2P **S**torage; DiMPS)」を実装し、その有用性について評価を行う。従来の P2P ファイル共有ネットワークは、アクセスの一意性、アクセスコントロール、セキュリティの 3 つの面で課題を持つ。本論文ではこれらの課題を解決するため、ファイルをデータ・プロパティ・ポインタの 3 つに分割する形で構成する新たなデータ構造を導入した。その上で、本データ構造を用いて既存の P2P ファイル共有ネットワークの上位レイヤで動作する新たなシステムを提案した。第一に、データに固有 ID を付与する形で既存の P2P ファイル共有ネットワーク上で流通させることで、コンテンツへの一意なアクセスを保証し、取得と検証の自動化を可能にする。第二に、データを暗号化した上で、データ暗号鍵をデータと分離してポインタに格納することで、ファイルへのアクセスコントロールを可能にする。第三に、プロパティにレーティング情報を付与することで、ファイルに対するユーザによる評価システムを実現する。よって、提案システムを用いることで、従来の P2P ファイル共有ネットワークを、非集中的・匿名的な性質を尊重しつつ、コンテンツ配信の公共的な基盤として簡便かつ安全に利用できる。本論文では、提案システムを具体化する API ライブラリを実装し、実際の P2P ファイル共有ネットワーク上で動作させた。また、本実装を用いて評価実験を行った結果、提案システムによって P2P ファイル共有ネットワークを用いたコンテンツの配信と取得・検証の自動化が可能であり、サーバを用いたコンテンツ配信と同等の利便性を実現していることを明らかにした。

目 次

第1章　序論

Gnutella[8] や Winny[9] に代表される P2P ファイル共有ネットワークは、「自律協調型の情報流通システム」という性質から、大規模かつ自由な情報交換を実現する手段として大きく期待されてきた。一方で、ネットワーク上で起きる著作権侵害や個人情報流出が社会的な問題となるにつれ、P2P ファイル共有ネットワークを開発・運用していくことが困難になりつつある。

こうした開発・運用上の問題点を解決し、「P2P ファイル共有ネットワーク」という非集中的・匿名的アーキテクチャを維持・発展させるには、その運用に伴う弊害を抑えながら、コンテンツ配信の公共的な基盤として簡便かつ安全に利用できる仕組みへと改良する必要がある。しかし、これを実現するにあたって、従来の P2P ファイル共有システムには、アクセスの一意性・アクセスコントロール・セキュリティの 3 つの点で課題があると考えられる。

第一に、従来の P2P ファイル共有ネットワークでは、特定のコンテンツを一意に取得できない点が挙げられる。P2P ファイル共有ネットワークを、簡便かつ安全に利用できるコンテンツ配信基盤として利用するには、利用者が必要とするコンテンツをネットワークから一意に取得し、また取得したコンテンツの正当性を自動的に検証する仕組みが必要である。しかし、従来のシステムは、ネットワーク内のファイルを一意に特定する仕組みを持たず、また、取得したコンテンツの正当性をシステム的に保証する手段も存在しない。このため、コンテンツ配信基盤としての利用には問題がある。

第二に、一度ネットワーク上に流通したコンテンツへのアクセスをコントロールすることが難しい点が挙げられる。P2P ファイル共有ネットワークでは、コンテンツの実体をネットワークに参加している複数のノード上に分散して保持する。この特徴は、コンテンツ配信基盤としてスケーラビリティや可用性の面で大きなメリットがあるが、反面、ネットワーク上で流通するコンテンツを統一的に管理することは困難になる。

第三に、ネットワーク上で流通するコンピュータウィルスによる被害が深刻なものとなっているが、ユーザが事前にこうした危険なコンテンツを判別できない点が挙げられる。特に、P2P ファ

イル共有ネットワークにおいては、ネットワークを通じてコンピュータウィルスを含むコンテンツが広まりやすいため、より被害が深刻になる傾向がある。

よって、P2P ファイル共有ネットワークをコンテンツ配信基盤として利用するには、上記の 3 つの問題点を解決する必要がある。具体的には、P2P ファイル共有ネットワーク上において、各問題点にそれぞれ対応する 3 つの機能を実現することが課題となる。

1. ファイルへの一意なアクセスの保証
2. ファイルへのアクセスコントロール
3. ユーザによる評価システムの導入

以上の課題を解決するため、本論文では、ファイルをデータ・プロパティ・ポインタの 3 つに分割する形で構成する新たなデータ構造を導入する。その上で、本データ構造を用いて、既存の P2P ファイル共有ネットワークの上位レイヤで動作する新たなシステムを提案する [1][2]。

提案システムは、既存の P2P ファイル共有ネットワークをベースとして利用することで、スケーラビリティや可用性といった、P2P 型ネットワークの長所を生かしたコンテンツ配信を実現する。その上で、既存のシステム上に、以上に挙げた 3 つの機能を実現することで課題を解決し、P2P ファイル共有ネットワークを簡便かつ安全に利用できるコンテンツ配信基盤とすることを目指す。

第一に、一意な識別子を持つ「ポインタ」を介することで、コンテンツへの一意なアクセスを保証する。まず、各コンテンツファイルの実データとメタデータを分離すると共に、実データとメタデータの 2 つを同時に参照するデータ形式であるポインタを導入する。次に、実データを暗号化した上で固有 ID を付与し、固有 ID とファイルのダイジェスト値、そして暗号化に用いた暗号鍵をポインタに格納する。このポインタは、サーバ上で公開する。また、暗号化した実データを、ファイル名に代えてポインタをキーとして、既存の P2P ファイル共有ネットワーク上で流通させる。これにより、ポインタを通じて P2P ファイル共有ネットワーク上で流通するコンテンツへの一意なアクセスが保証されるため、常に同一の内容を持つデータを取得し、その正当性を自動的に検証することが可能になる。

第二に、ポインタへのアクセスを管理する仕組みを導入することで、P2P ファイル共有ネットワーク上で流通するコンテンツへのアクセスコントロールを可能にする。提案システムでは、コンテンツファイルを実データとプロパティに分離する際にデータを暗号化し、暗号鍵をポインタに格

納する。このため、実データがP2Pファイル共有ネットワーク上で流通しても、コンテンツの利用にはポインタが必要なため、ネットワークから実データのみを取得しても意味を成さない。よって、必要な場合はポインタへのアクセスを管理することで、コンテンツの流通をコントロールできる。

第三に、分離したメタデータに対して、ユーザがコンテンツに対する評価情報を付与する。これにより、ユーザはP2Pファイル共有ネットワーク上で流通するコンテンツの内容に対して価値判断を加え、それを他のユーザと共有することができる。例えば、ウィルス感染についてのレーティングをメタデータに付与することで、ユーザ間での自主的なセキュリティの確保が可能になる。

以上のように、提案システムによって課題となる三つの機能を実現する。これにより、従来のP2Pファイル共有ネットワークの問題点を解決し、簡便かつ安全に利用できるコンテンツ配信の基盤へと改良することができる。

本論文では、提案システム「分散メタP2Pストレージ」を具体化するAPIライブラリ「**DiMPS** (**Di**stributed **M**eta-**P**2P **S**torage)」を実装し、実際のP2Pファイル共有ネットワーク上で動作させる。また、本実装を用いて評価実験を行い、提案システムによってP2Pファイル共有ネットワークを用いたコンテンツの配信と取得・検証の自動化が可能であり、サーバを用いたコンテンツ配信と同等の利便性を実現していることを明らかにする。

以下、2章では、既存のP2Pファイル共有システムについて考察し、その問題点を述べる。3章では、2章で挙げた問題点に対する既存研究について考察する。4章では、提案システム「DiMPS」の概要を述べる。5章では、DiMPSを実装し、既存のP2Pファイル共有ネットワーク上で動作させる方法を述べる。6章では、DiMPSの実装を用いて評価実験を行う。7章では、結論と今後の課題を述べる。

第2章　P2P ファイル共有ネットワーク

本章では、まず、ディスクファイルシステムを例として、任意のシステムからファイルを取得する際に前提となる条件について考察する。次に、この考察を元に、既存の P2P ファイル共有ネットワークでのコンテンツの取得について考察し、問題点を明らかにする。最後に、P2P ファイル共有ネットワークにおけるアクセスコントロールとセキュリティ上の問題点について議論する。

2.1　「ファイルの取得」のプロセス

S. Joseph[3] によれば、ネットワーク上でファイルを取得する際に使用されるシステムは、その過程によって「WHAT（何を）」「WHERE（どこに）」「HOW（どのように）」の三つの段階に分類できる。これに倣って、「ファイルの取得」という一連のプロセスは、以下の三段階に分けて考えることができる。

1. 発見 (find): ユーザが目的とする、ある一つのファイルの存在を見つけ特定する。
2. 探索 (lookup): 発見したファイルが格納されている物理的位置を求める。
3. 取得 (get): 探索の結果を元にファイルへアクセスし、実データをローカルに複製する。

このような「ファイルの取得」を行う最も代表的なシステムとして、ディスクファイルシステムが挙げられる。最初に、ディスクファイルシステムのユーザは、対象のファイルシステム内に取得したいファイルが存在することを**発見** (find) する必要がある。多くの場合、ユーザはディレクトリ構造やキーワード検索を用いて、インデックスから必要とするファイルの存在を発見する。次に、ユーザは発見したファイルの実データが格納されている位置を知る必要がある。一般的なディスクファイルシステムにおいて、ディレクトリ名を付加したファイル名は、システム内で**一意な識別子**であることが保証されている。したがって、ユーザはファイル名をキーとして物理的な格納位置を**探索** (lookup) できる。最後に、ユーザは探索の結果を元にディスクにアクセスし、ファイルの複製を**取得** (get) することができる（図 2.1）。

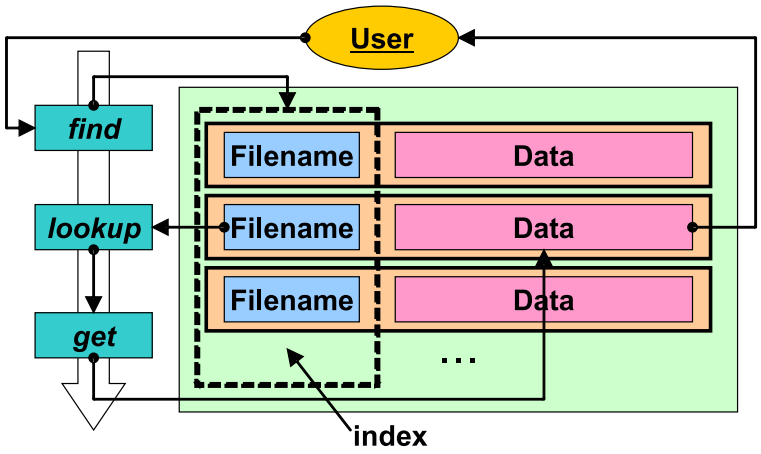

図 2.1: ディスクファイルシステムにおけるファイルの取得

すなわち、ディスクファイルシステムにおけるファイルの取得は、「システム内のファイル空間において任意のファイル名が一意である」ことを前提としている。このように、ファイル名はファイルのメタデータであると同時に、「探索」を行う際に用いる一意な識別子としての役割を持つ。このため、ディスクファイルシステムのユーザは、ファイル名を指定することで常に同じ内容のファイルを自動的に取得できる。

2.2 P2P ファイル共有ネットワークにおけるコンテンツの取得

P2P ファイル共有ネットワークは、ファイルを共有する際に、複数のノード上にあるファイル空間を、オーバーレイネットワーク上の単一ファイル空間へと仮想的に結合する。よって、多くの場合、ファイル名の一意性は保証されない。このため、多くの P2P ファイル共有ネットワークにおいて「一意な識別子による探索」という概念は存在せず、クエリ (query) として一致度の高いファイルの候補を取得し、一つを手動で選択する手法を取る。

この手法では、特定のファイルを取得したい場合でも、その要求はファイル名に対するキーワード検索として処理される。すなわち、N. Daswani ら [4] が述べているように、似た名前で異なる内容のファイルや、該当のファイルであっても版や細部の異なるファイルなど、クエリの結果として複数の異なるファイルが返される可能性がある（図 2.2)。

したがってユーザは、クエリの結果として返された候補の中から、いずれが要求したコンテンツを含むファイルであるかを、その度に手動で検証し選択しなければならない。これは、コンテン

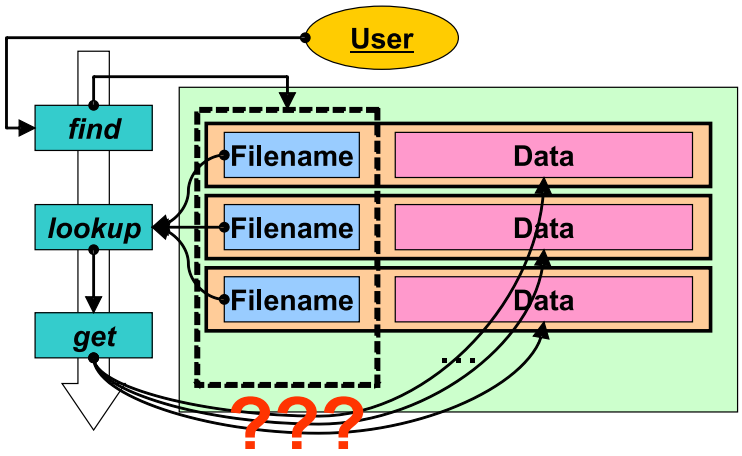

図 2.2: P2P ファイル共有ネットワークにおけるファイルの取得

ツの取得を自動化できないという点で問題がある。これに対して Daswani らは、「古さ」「エキスパート」「投票」「評判」を基準に判断する手法を提案しているが、いずれも推定による選択法であり、確実な方法とは言えない。加えて、実際に取得したコンテンツの内容が正当であることを自動的に検証できない点でも問題がある。このため、既存の P2P ファイル共有ネットワークは、コンテンツ配信基盤として簡便に利用することが困難である。

2.3 コンテンツ分散の利点と問題点

P2P ファイル共有ネットワークの特徴の一つとして、ネットワーク上の複数のノードがコンテンツを分散して保持する点が挙げられる。よって、一箇所の中央サーバでコンテンツを保持する方式と比べてスケーラビリティや可用性の面で優れており、コンテンツ配信基盤に適した方式であると言える。

一方で、配信の際にコンテンツの実体が複数のノードに分散されるため、ネットワーク上に流通するコンテンツを統一的に管理することができない。このため、中央サーバで全てのコンテンツを管理する方式と異なり、一度ネットワーク上で流通したコンテンツへのアクセスをコントロールすることが難しい。

また、P2P ファイル共有ネットワーク上で、コンピュータウィルスなどのセキュリティ上の脅威を招く要素を含むコンテンツが流通した結果、誤って利用してしまったユーザのシステム破壊や個人情報の流出などの被害が発生している。また、被害者がコンピュータウィルスの新たな感染源と

なることで、ネットワークを通じて被害が拡大しやすい。

しかし、既存の P2P ファイル共有ネットワークにおいては、ユーザは事前にセキュリティ上危険なコンテンツを判別できない。このため、被害の抑制が困難なものとなっている。

2.4 まとめ

本章では、既存の P2P ファイル共有ネットワークについて考察し、簡便かつ安全なコンテンツ配信基盤として利用する際に、アクセスの一意性・アクセスコントロール・セキュリティの 3 つの点で問題があることを示した。

まず、システムからファイルを取得する際に要する処理を発見・探索・取得の三段階に分類した。次に、本分類をディスクファイルシステムを例として適用し、ファイル名がファイルのメタデータであると同時に、探索の際に用いる一意な識別子としての役割を持つことを示した。

続いて、P2P ファイル共有ネットワークにおけるファイルの取得について考察した。その結果、既存の P2P ファイル共有ネットワークでは、ファイル名の一意性が保証されないため一意な識別子による探索が行えず、ネットワークからのコンテンツの取得・検証を自動化できないことを示した。

最後に、既存の P2P ファイル共有ネットワークでは、一度ネットワーク上に流通したコンテンツをコントロールできないことに加え、コンピュータウィルスなどセキュリティ上脅威となるコンテンツによる被害が問題となることを述べた。

3 章では、以上に述べた既存の P2P ファイル共有ネットワークの抱える課題を踏まえ、これらの 3 つの課題に対する関連研究の考察を行う。

第3章　関連研究

本章では、2 章で挙げた既存の P2P ファイル共有ネットワークの解決すべき 3 つの課題について、関連研究を挙げ考察を行う。

3.1　アクセスの一意性

Cogny[6] は、P2P ネットワークの中に中央サーバを置き、コンテンツごとにユニークな ID を付与することで一意性を保証しつつ、コンテンツの発見と管理を行う。Cogny は、コンテンツに対して ID の他に、更新ごとに版を付与して管理する。すなわち、中央サーバに対して ID を用いて問い合わせると、流通しているコンテンツのうち最新版を発見し取得することができる。また、コンテンツの全文検索を行うために、コンテンツを解析して得たメタデータを中央サーバに登録し、要求に応じて検索を行う。

BitTorrent[10] は、安コストかつ効率的にコンテンツの配信を行うことを目的として開発された P2P 型コンテンツ配信システムである。特に、公開初期の大容量コンテンツへのアクセスの集中によるスケーラビリティの問題を解決することを主眼としている。BitTorrent は、サーバ上に「.torrent」メタファイルを置き、このメタファイルの情報を用いてネットワークからコンテンツの探索と取得を行う。

どちらの手法においても、ユーザは ID あるいはメタファイルといった一意な識別子を利用してコンテンツを取得する。これによりユーザは、システムから必要とするコンテンツを一意に特定し自動的に取得できる。

また、これらの既存手法の特徴として、P2P ネットワークを用いてコンテンツの配信する際に、中央サーバを用いてコンテンツの探索と取得を行う点が挙げられる。Cogny は、コンテンツの実体を保持するノードを中央サーバが常に把握し、個々のノードからの要求に応じてノード間のコンテンツの取得を仲介・記録する。また、BitTorrent は、配信するファイル毎に専用の P2P ネットワークを生成し、その維持のために、ネットワーク上の全てのノードとファイル断片の所在をリア

ルタイムに管理する専用のサーバ（トラッカー）を必要とする。

このように両手法では、P2P ネットワーク上のノードとコンテンツの実体の状態を中央サーバで一元的に管理することで、コンテンツの一意な配信を実現している。このため、コンテンツ配信における中央サーバへの依存が大きく、P2P ネットワークの状態をリアルタイムに把握するために多数のノードと交信し続ける必要がある。このため、サーバへの負荷やスケーラビリティが問題になりやすい。

3.2 アクセスコントロールとセキュリティ

既存の P2P ファイル共有ネットワークの課題として、アクセスコントロールとセキュリティの確保が挙げられる。これに対して、コンテンツホルダが承認しないコンテンツの流通を阻止し、配信するコンテンツの正当性と安全性を保証することを目的として、中央サーバを用いた DRM(Digital Rights Management) 技術を P2P ネットワークに組み込むことで、P2P ネットワーク上で流通するコンテンツのコントロールを行う手法が多数提案されている [5] [7]。

しかし、これらの手法においては、中央サーバがコンテンツのノード間の移動やローカルでの利用状況を逐一把握することを目的としている。このため、各ノードは常に中央サーバと通信する必要があり、中央サーバの負荷やスケーラビリティに問題があると言える。

3.3 まとめ

本章では、既存の P2P ファイル共有ネットワークの 3 つの問題点、すなわちアクセスの一意性・アクセスコントロール・セキュリティの確保について、関連研究を挙げてそれぞれの手法について考察を行った。また、中央サーバを用いて問題点の解決を図る既存手法は、中央サーバの負荷とスケーラビリティの点で課題があることを示した。

4 章では、以上に述べた関連研究を踏まえ、これを解決する提案システム「DiMPS」の概要を述べる。

第4章　DiMPSの概要

本論文では、1 章および 2 章で述べた 3 つの課題を解決するために、既存の P2P ファイル共有ネットワーク上に、一意なアクセスの保証・アクセスコントロール・ユーザによる評価システムの 3 つの機能を導入する (表 4.1)。また、これを実現するため、従来の P2P ファイル共有ネットワークをベースとして、その上位レイヤで動作する新たなシステムを提案する [1][2]。

具体的には、P2P ファイル共有ネットワーク上で流通するファイルを機能ごとに分割し、**データ・プロパティ・ポインタ**の 3 つの要素からなる新たなデータ構造を定義する。提案システムは、個々のファイルからこれら 3 つのデータ構造を生成する。そして、分割した各データをそれぞれ異なる媒体上で流通させ、総体として一つのシステムを構成する。これにより、既存の P2P ファイル共有ネットワークをコンテンツ配信基盤として機能させる（図 4.1)。

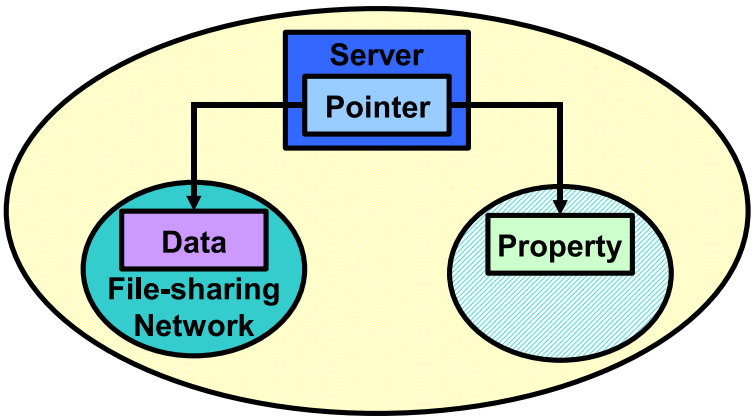

図 4.1: 提案システムの概念図

本章では、まず、提案システムである分散メタ P2P ストレージ「DiMPS (Distributed Meta-P2P Storage)」の構成と実現する機能について概要を述べる。本章で述べる次に、提案システムを既存手法と比較し、その優位性を明らかにする（表 4.1)。

表 4.1: 課題に対して提案システムで実現する機能

課題	機能	参照
簡便・安全なコンテンツ配信基盤の実現	コンテンツへの一意なアクセスの保証	(4.1.1)
流通コンテンツの管理	コンテンツに対するアクセスコントロール	(4.1.2)
セキュリティ上の脅威の回避	ユーザによる評価システムの導入	(4.1.3)

4.1 DiMPS の構成と機能

提案システムは、各ファイルが持つ実データとメタデータを分離し、前者を**データ** (Data)、後者を**プロパティ**(Property) と呼ぶデータ形式で扱う。また、提案システムは、データとプロパティのそれぞれに、システム全体で一意な識別子となる**固有 ID**(UID; Unique IDentifier) を与える。このうち、データはこれを暗号化した上で、データに付与した固有 ID をファイル名に代えて探索キーとして、P2P ファイル共有ネットワーク上で流通させる（図 4.2)。

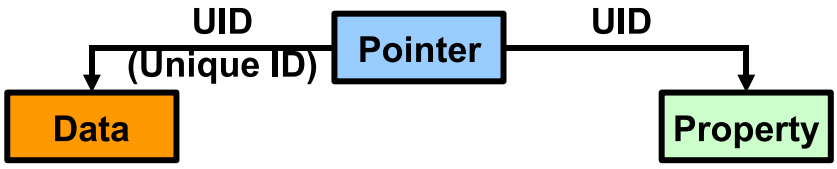

図 4.2: 本システムで定義する新たなデータ構造

4.1.1 一意なアクセスの保証

第一に、一意な識別子を保持する**ポインタ**を介して、P2P ファイル共有ネットワークからのコンテンツの一意な取得を保証する。ポインタは、データとプロパティという 2 つの要素への固有 ID を同時に保持するデータ形式である。またポインタは、データとプロパティのダイジェスト値と、データの暗号化に用いた**暗号鍵**を固有 ID と共に格納する。コンテンツから生成したポインタは、ポインタ生成者の電子署名を付与してポインタ自身の真正性を検証可能にした上で、任意のサーバ上で公開する。

これにより、システムの利用者は、ポインタに格納された固有 ID をキーとして、P2P ファイル共有ネットワークから常に同一の内容を持つデータを取得できる。また、ネットワーク取得した

データは、ポインタに格納されたダイジェスト値と比較することで、内容の正当性を自動的に検証することができる（図 4.3）。

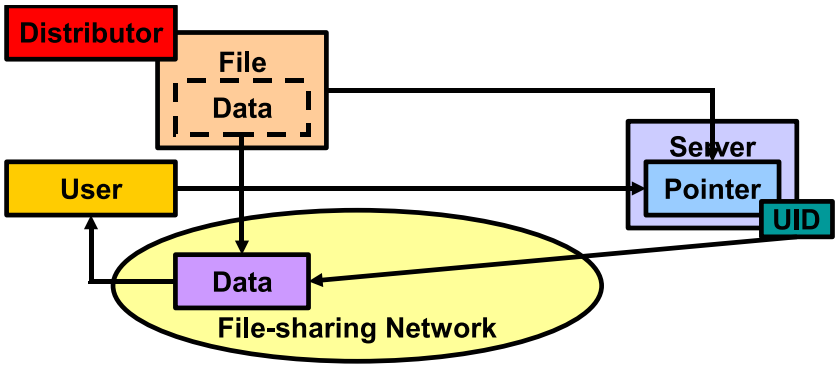

図 4.3: ポインタを介したコンテンツの流通と取得

4.1.2 アクセスコントロール

第二に、ポインタへのアクセスを管理する仕組みを導入することで、P2P ファイル共有ネットワーク上で流通するコンテンツのコントロールを実現する。提案システムでは、ファイルをデータとプロパティに分離する際にデータを任意のアルゴリズムで暗号化し、使用した暗号鍵をポインタに格納する。

このため、データが P2P ファイル共有ネットワーク上で流通しても、データの利用にはポインタが必要なため、ネットワークからデータのみを取得しても意味を成さない。よって、ポインタを管理することで、コンテンツの利用をコントロールすることが可能になる（図 4.4）。

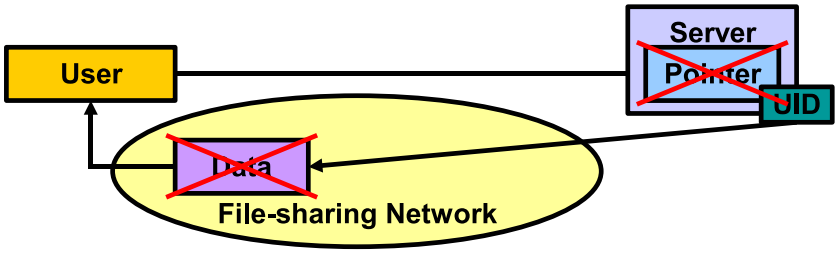

図 4.4: ポインタによる流通コンテンツのコントロール

4.1.3 ユーザによる評価システム

第三に、プロパティに対して、システム利用者が流通コンテンツへのレーティング情報を付与する。プロパティは、コンテンツに対する様々な形式のメタデータを格納する汎用のデータ形式である。プロパティを利用することで、従来のファイル名でキーワードを表現する単純な方式に比べ、より多様な形式でメタデータを表現できる。また、プロパティは、コンテンツの配布者だけでなく、システムの利用者が後から自由にメタデータを追記し共有することができる。

このため、システムの利用者は、コンテンツのメタデータ情報と共に、セキュリティ上の脅威となるコンテンツのプロパティにレーティング情報を付与することができる。他の利用者は、プロパティのレーティング情報を参照することで、事前に危険なコンテンツを判別することができる（図4.5)。

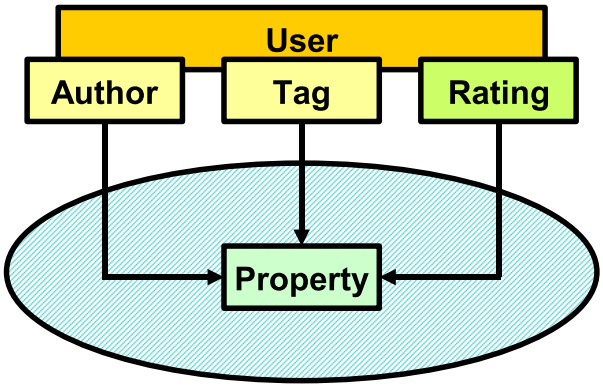

図 4.5: プロパティが格納する様々なメタデータ

4.1.4 機能の分散と協調

提案システムは、図 4.1 に示したように、個々のファイルを機能ごとに分割した 3 つの要素をそれぞれ異なるサブシステムが扱うことで、総体として一つのシステムを構成する。

例えば、提案システムを利用することで、ユーザはサーバから入手したポインタを用いて、P2P ファイル共有ネットワークから探索・取得すべきコンテンツを一意に特定できる。このときユーザは、ポインタに格納された一意な識別子を用いて、P2P ファイル共有ネットワーク上でのコンテンツの探索・取得を効率的に行える。一方で、ポインタを配信するサーバは、P2P ファイル共有ネットワーク上のコンテンツの実体の位置や状態を把握する必要がなく、中央サーバを利用するこ

表 4.2: 既存手法と提案システムの比較

	Unique Access	Controlabillity	Rating System	Server Independency
Existing File-sharing	×	×	△	○
Cogny	○	○	×	×
BitTorrent	○	○	×	×
DRM-embedded File-sharing	○	○	×	×
Proposed System	○	○	○	△

とによる負荷やスケーラビリティの問題を軽減できる。

このように提案システムでは、一つの機能を異なるサブシステムが協調して実現するため、結果としてシステムを運用する上での個々のサブシステムの負担を分担し、軽減することができる。

4.2 既存手法との比較

3 章で述べた既存手法と提案システムの相違点として、P2P ネットワークを用いてコンテンツの配信を行う際に、コンテンツの探索と取得に中央サーバを用いない点が挙げられる。既存の手法では、ネットワーク上の全てのノードとコンテンツの実体の所在を中央サーバでリアルタイムに管理することでコンテンツ配信を行う。このため、コンテンツ配信における中央サーバへの依存が大きく、サーバへの負荷やスケーラビリティ点で問題がある。

一方、提案システムでは、中央サーバはコンテンツの一意性を保証するポインタの配信にのみ利用し、P2P ネットワーク上のノードやコンテンツ実体の状態について一切関知しない。このため、既存手法よりも中央サーバへの依存度が低く、中央サーバの負荷やスケーラビリティの問題が相対的に小さく済む点でメリットがある。また、ポインタを配信できれば良いため、一般的なウェブサーバをそのままポインタサーバとして利用できる点も利点として挙げられる。さらに、提案システムではコンテンツのメタデータを柔軟に扱えるため、コンテンツに対してレーティング情報を付与することによってセキュリティを確保できる点も利点である（表 4.2)。

4.3 まとめ

本章では、提案システムの概要を述べ、既存手法との比較によって本提案手法の優位性を示した。

提案システムでは、ファイルをデータ・プロパティ・ポインタと呼ぶ 3 つのデータ構造に分割することで、P2P ファイル共有ネットワークをコンテンツ配信基盤として利用するために必要な 3 つの機能を実現する。第一に、ポインタに格納した固有 ID をキーとして、コンテンツの一意な取得を保証する。第二に、データを暗号化して暗号鍵をポインタに格納することで、P2P ファイル共有ネットワーク上で流通するコンテンツのアクセスコントロールを行う。第三に、プロパティにレーティング情報を付与することで、ユーザはセキュリティ上の脅威があるコンテンツを事前に回避できる。

また、提案システムを既存手法と比較し、提案システムがサーバ依存性の低さなどの点で利点を持つことを示した。

5 章では、本章で述べた提案システムを、API ライブラリ「DiMPS」として実装する。

第5章　DiMPSの実装

本論文では、4章で述べた提案システムの具体化を目的として、APIライブラリ「DiMPS(Distributed Meta-P2P Storage)」を、Java言語とXMLを用いて実装する。また、DiMPSの有用性を検証するため、代表的なP2Pファイル共有ソフトウェアの一つである「LimeWire」[11]上にDiMPSを実装し、動作させる。

5.1　Coreコンポーネント

DiMPS APIのうち、ファイルからデータ・プロパティ・ポインタからなる3つのデータ構造（三つ組）を生成・管理するコア(Core)コンポーネント群の構成を図5.1に示す。

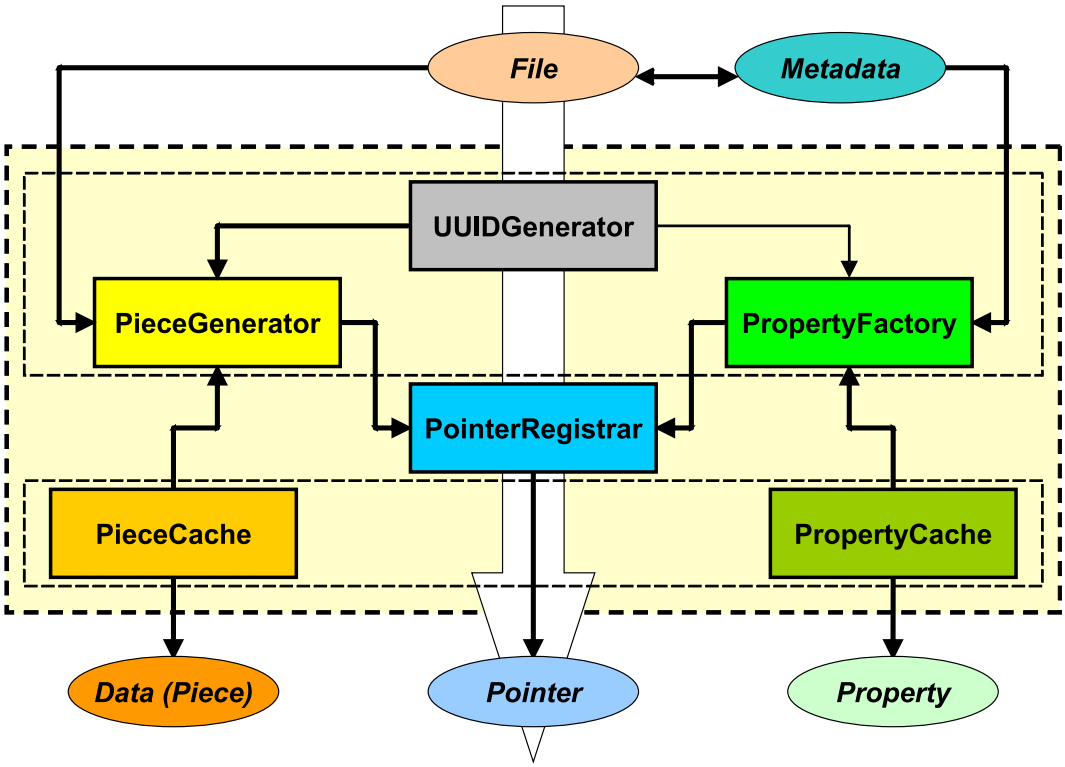

図 5.1: DiMPS API Core コンポーネント群

コア・コンポーネント群は、大まかに**生成器**（Generator）・**キャッシュ**(Cache)・**レジストラ**(Registrar) の 3 つに分類できる。まず、API への入力として、DiMPS を用いて配信するコンテンツファイルの実データとメタデータを用意する。次に、データとプロパティのそれぞれに対して、任意のアルゴリズムの UUID 生成器とキャッシュを用意する。これらのコンポーネントは、他のコンポーネントから利用される際に、必要に応じて自由に差し替えることができる。

生成器は、実データ及びメタデータ・UUID 生成器・キャッシュを入力とするコンポーネントである。まず、生成器は実データをデータに、メタデータをプロパティに変換する。次に、それぞれに対して UUID 生成器で生成した UUID を付与した後、キャッシュへ出力する。また、同時に、生成したデータとプロパティをレジストラへ入力する。

キャッシュは、データを一定サイズごとに分割した形式である**ピース** (Piece) やプロパティをローカルに保存する際に、記憶装置への入出力を抽象化するコンポーネントである。生成器は、ピースやプロパティに与えた UUID をキーとしてキャッシュに問い合わせることで、実際の保存形式を意識せずとも、環境に合わせて適切な入出力ストリームを得ることができる（図 5.2)。

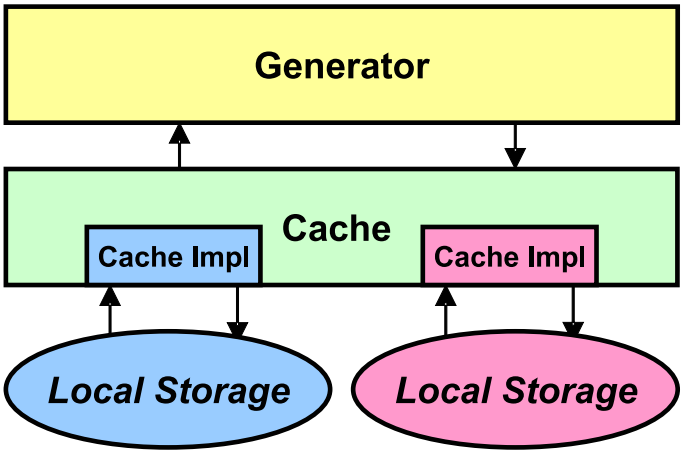

図 5.2: Cache コンポーネント

レジストラは、データとプロパティからポインタを生成するコンポーネントである。具体的には、データとプロパティからダイジェスト値と暗号鍵を取り出してポインタを構成する。次に、ポインタに対してポインタ生成者の電子署名を付与した後、XML 形式で出力する。これにより、利用者はいつでも、取得したポインタの真正性を自動的に検証できる。

5.2 Adapter コンポーネント

DiMPS API と P2P ファイル共有ネットワーク、及び DiMPS から P2P クライアントを操作するアダプタ (Adapter) コンポーネントの関係を図 5.3 に示す。

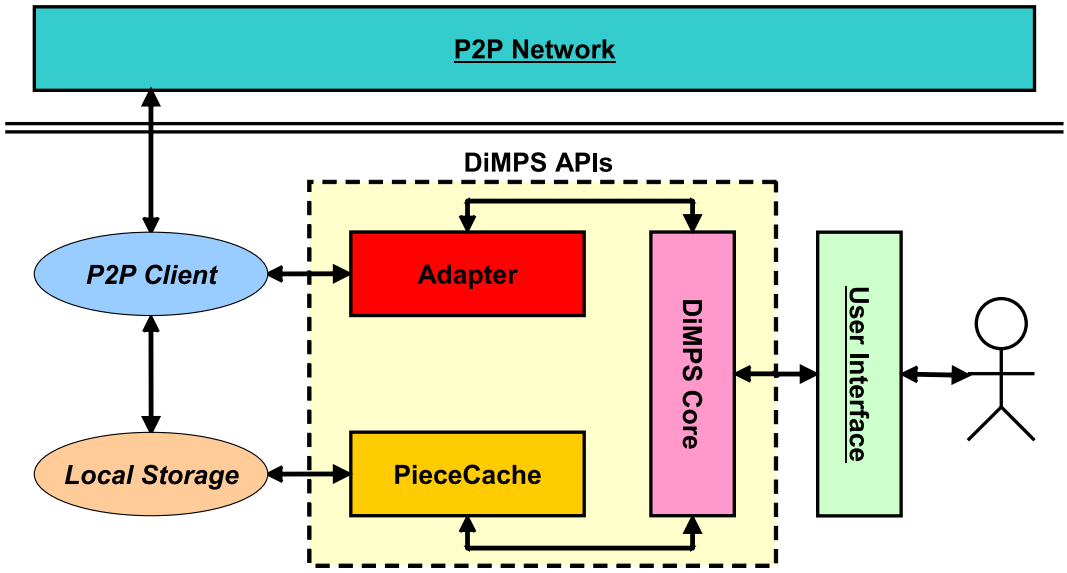

図 5.3: Adapter コンポーネント

アダプタは、P2P ファイル共有ネットワークに対するクエリの発行やピースの取得などの操作を抽象化するコンポーネントである。利用者の要求に従って、P2P クライアントに依存する具体的な操作を実行すると共に、コア・コンポーネント群に対して共通のインターフェースを提供する。加えて、P2P クライアントがネットワークから取得し、ローカルに保存したピースに対しても、5.1 節で述べたキャッシュ・コンポーネントを利用することで、P2P クライアントの実装に拠らない共通の操作を可能にする。

すなわち、DiMPS が利用する P2P ファイル共有ネットワークごとにアダプタとキャッシュを実装することで、実際に利用する P2P ファイル共有ネットワークの種類を問わず、DiMPS API による透過的な操作が可能になる。このことは、提案システムの利用者にとって、実際に利用する P2P ファイル共有ネットワークの詳細を意識せずに、コンテンツの配信や取得といった DiMPS の機能を簡便に利用できるメリットをもたらす。

5.3 DiMPS APIの利用

DiMPS を利用してコンテンツを配信するには、コンテンツファイルを DiMPS API に入力し、データ・プロパティ・ポインタをそれぞれ得る。次に、データを P2P ファイル共有ネットワーク上で流通させ、ポインタは任意のサーバ上で公開する。

コンテンツの利用者は、まずポインタをコンテンツ配信者のサーバから取得する。そして、取得したポインタを DiMPS API に入力することで、DiMPS はポインタの署名を検証した後、P2P ファイル共有ネットワークから目的のコンテンツを構成するピースを取得し、正当性の検証を行う。次に、ポインタに格納された暗号鍵を用いてピースを復号して結合し、目的のコンテンツを得る。これらの処理は、DiMPS が全て自動的に実行するため、ユーザは利用している P2P ファイル共有ネットワークの詳細を意識することなく、コンテンツを利用できる。

以上のように、DiMPS を利用することで、P2P ファイル共有ネットワークを利用して非常に簡便かつ安全にコンテンツを配信・取得できる。また、ポインタを Web サーバ上に置き、DiMPS と Web ブラウザを連携させることで、従来の Web サーバを利用したコンテンツ配信と同等の利便性を実現できる。

5.4 まとめ

本章では、DiMPS API を構成するコンポーネント群の詳細と利用方法を述べ、その有用性を示した。

まず、コンテンツファイルからデータ・プロパティ・ポインタからなる 3 つのデータ構造を生成するコア・コンポーネント群の構成を述べ、生成器・キャッシュ・レジストラを組み合わせて利用することを示した。次に、コア・コンポーネント群と P2P クライアントを仲介するアダプタ・コンポーネントについて述べ、アダプタとキャッシュを用いて P2P クライアントに対する操作を抽象化できることを示した。これにより、P2P ファイル共有ネットワークに対する透過的な操作を実現し、DiMPS を用いたコンテンツ配信を簡便に利用できることを明らかにした。

6 章では、本章で述べた DiMPS の実装を用いて P2P ファイル共有ソフトウェア「LimeWire」上で評価実験を行い、提案システムの有用性を明らかにする。

第6章　評価実験

本章では、5 章で実装した DiMPS API を用いて、提案システムの評価を行う。これにより、提案システムによって従来のコンテンツ配信方式と同等の利便性を実現しつつ、P2P ファイル共有ネットワークを用いたコンテンツ配信の利点を享受できることを示す。具体的には、代表的な P2P ファイル共有ソフトウェアの一つである LimeWire[11] 上に DiMPS を実装してローカル環境でコンテンツの取得実験を行い、条件を変化させながら取得所要時間を計測する。また、同様に HTTP プロトコルを用いたコンテンツの取得についても実験し、両者を比較することで評価を行う。

6.1　実験環境

DiMPS の評価実験を行うにあたって、仮想マシン環境ソフトウェアの VMware[12] を用いて、一台の評価用コンピュータ上に複数のノードとネットワーク環境を仮想的に構築した。また、擬似的に実環境の条件を再現するため、ノード間の通信に Dummynet[13] を用いて遅延発生器を導入した。本実験では、この仮想環境を用いて検証を行う。

実験に用いる仮想環境を構築した評価用コンピュータを表 6.1 に示す。また、仮想環境において評価用環境で用いたソフトウェアと、評価に使用したファイルの情報を表 6.2 に示す。

表 6.1: 評価用コンピュータ

CPU	Intel Core 2 Duo E6850 3.00GHz
Memory	3326 MB
HDD	294 GBytes
OS	Windows Vista Bussiness
Virtual Machine	VMware Server 1.0.2

本実験では、以上の環境を用いて、仮想環境内に評価用ネットワークを構築した。ここで、評価用ネットワークの仮想物理トポロジを図 6.1 に示す。また、本実験で使用するノード S_1, C_1, C_2, C_3

表 6.2: 評価用環境と評価用ファイル

OS	Ubuntu 7.10
Java	Java SE 6 update 4
P2P File-sharing	LimeWire 4.17.2 beta
Delay Generator	FreeBSD 5.3-RELEASE + Dummynet
Communication Delay	20 msec
Evaluation File	103,099,308 bytes
HTTP Server	Apache 2.2.4

間の全ての通信を遅延発生器を介することで、通信に対する遅延の発生や帯域制限を実施し、より実環境に近い条件で実験を行った（図 6.2）。

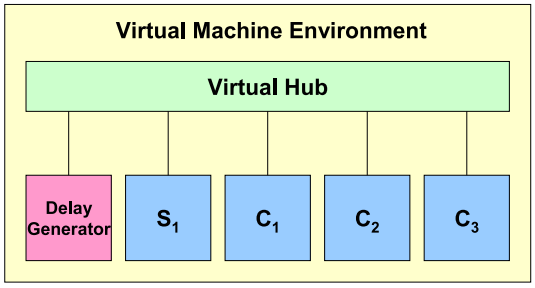

図 6.1: 仮想物理トポロジ

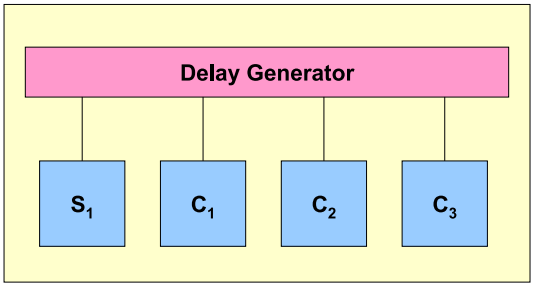

図 6.2: 仮想論理トポロジ

6.2 DiMPS によるコンテンツ取得時間の計測

本論文では、P2P ファイル共有ソフトウェアの LimeWire を用いて、DiMPS の評価実験を行った。具体的には、6.1 節で用意した実験環境上に、LimeWire を用いてオーバーレイネットワークを構築した（図 6.3）。次に、ノード S_1, C_2, C_3 上に、10,000,000 バイトごとに分割した評価用ファイルを DiMPS API に入力して得たピース (Piece)11 個を配置し、C_1 をユーザ端末としてピースの取得実験を行った。

ユーザ端末 C_1 を操作して DiMPS API にポインタを入力すると、DiMPS は、ネットワーク内でピースを保持するノードの位置を得るため、アダプタを通して LimeWire クライアントでクエリを実行する。次に、ピースの実体を保持しているノードを発見すると、LimeWire クライアント

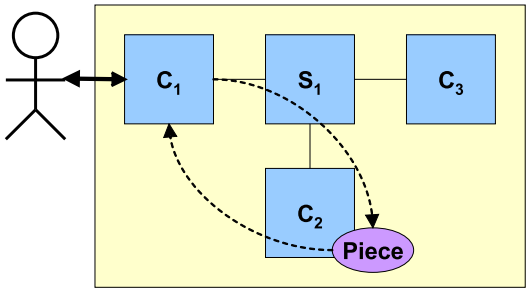

図 6.3: 評価用 P2P ファイル共有ネットワーク

に対して自動的にダウンロードの指示を出す。本実験では、DiMPS API にポインタを入力してから、LimeWire クライアントが全てのピースの取得するまでの時間を計測した。

また、提案システムの特徴を考察するため、様々な条件の下で取得実験を行った。具体的には、初期状態においてネットワーク内でピースを保持するノード数を 1 ノード、2 ノード、3 ノードと変化させ、それぞれについて全ピースの取得に要した時間を計測した。また、ノード間通信に対して、条件を変化させながら 1Mbps から 10Mbps までの間で帯域制限を実施し、計測を行った。

さらに、提案システムとの比較に用いるため、現在コンテンツ配信の手段として一般的である HTTP サーバからのコンテンツ取得実験を併せて行った。具体的には、評価用ファイルを保持する、HTTP サーバを動作させたノードをネットワークに接続した。その上で、提案システムに対する実験と同様に、帯域制限を変化させながら C_1 から wget コマンドで評価用ファイルを取得し、取得に要した時間を計測した。

以上の実験の結果を、図 6.4 に示す。

6.3 考察

まず、HTTP サーバからコンテンツを取得する場合と、DiMPS を用いて 1 ノードのみからコンテンツを取得する場合の比較を行う。図 6.4 に示すように、帯域制限が同条件の場合、両者において、コンテンツ取得にかかる所要時間に差はほとんど認められない。

しかし、一般的に HTTP サーバを用いるコンテンツ配信方式と、P2P ファイル共有ネットワークを用いる提案システムの方式を比較すると、HTTP サーバを用いる方式ではより良い通信環境を利用できる場合が多い。このため、提案システムを用いたコンテンツ配信サービスが、既存手法と同等の所要時間でコンテンツ配信サービスを提供できるかは、単純に結論できない。

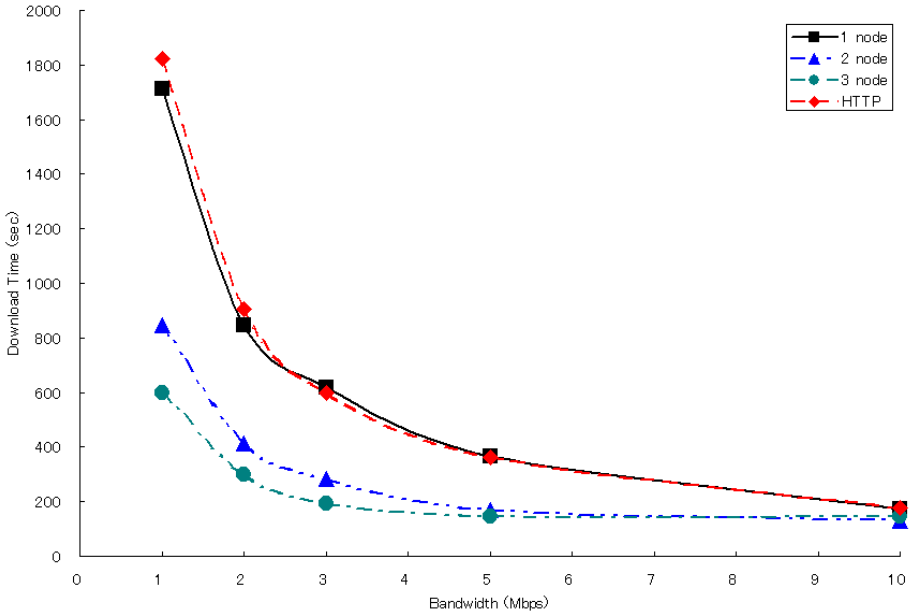

図 6.4: 評価用コンテンツの取得所要時間

次に、DiMPS を用いてネットワーク上の複数ノードから同時にコンテンツを取得する場合について考察する。帯域制限が同条件の場合、提案システムでは、初期状態でコンテンツを保持しているノードが多いほど、より少ない所要時間でコンテンツを取得できることが分かる。

2 ノード時、3 ノード時の取得所要時間を 1 ノード時と比較し、倍率として求めたものを図 6.5 に示す。この図より、利用できる帯域が少ない場合ほど、コンテンツ保持ノード数の増加による効率の改善効果が高いことが分かる。また、帯域制限が 3Mbps から 5Mbps 付近でもっとも取得効率が改善し、1Mbps 付近でもノード数にほぼ比例した効率の改善が見られる。加えて、一部の帯域では、取得時間が比例倍を超えて改善している。

よって、利用できる帯域が少ない場合、複数のノードから同時にコンテンツをダウンロードするため、ノード数に比例して効率が改善することが分かる。また、コンテンツを同時並行的に取得することで、ダウンロード前後に要する開始終了処理中も帯域を効率的に使用できるため、ノード数に対する比例倍を超えて効率が改善していることが分かる。しかし、1Mbps 付近ではダウンロード中にタイムアウトが発生する場合があり再接続が必要となるために、効率の低下が見られる。

すでに考察したように、同じ帯域制限の条件下での実験では、コンテンツ配信方式としてどちらが優れているかを結論することはできない。しかし、提案システムでは P2P ファイル共有ネットワークを利用するため、すでにコンテンツを保持している多数のノードから同時にコンテンツを取

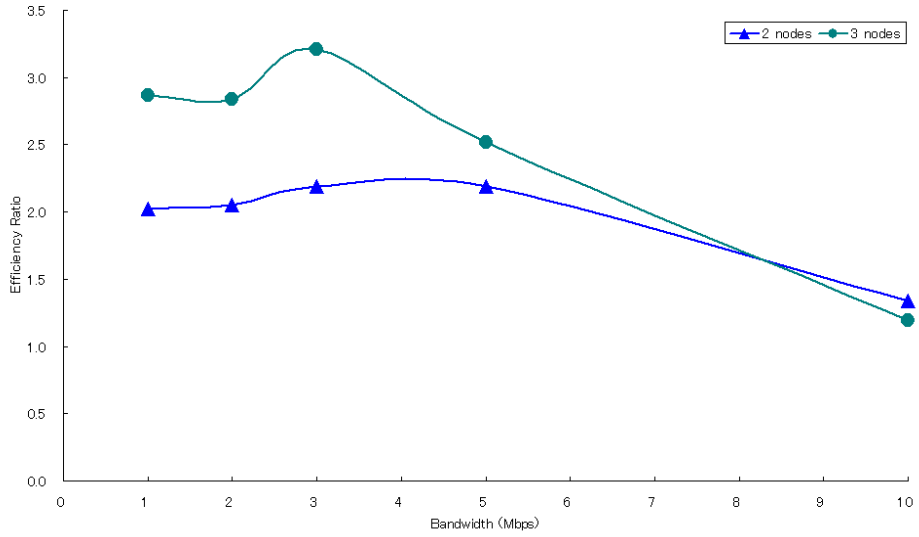

図 6.5: 複数ノード時の取得所要時間改善率

得できる。このため、ネットワーク上でコンテンツを保持するノードが増えるほど、コンテンツ取得にかかる所要時間を改善できると考えられる。

また、提案システムでは、コンテンツの探索と取得に中央サーバを利用しないため、サーバへの負荷やスケーラビリティの点において利点を持つ。加えて、コンテンツ配信基盤として HTTP サーバを利用する方式と、提案システムを利用する方式は、ともにユーザが必要とするコンテンツを一意に取得することができる。このため、提案システムにおいても、HTTP サーバを利用する方式と同等の利便性を確保できる。

このため、今後、DiMPS をウェブブラウザから利用できるインターフェースを実装すれば、提案システムを利用したコンテンツ配信サービスにより、既存の HTTP サーバを用いたコンテンツ配信方式と同等の利便性を実現できると考えられる。

6.4 まとめ

本章では、提案システムを実装した DiMPS を用いて P2P ファイル共有ネットワーク上で評価実験を行い、様々な条件の下で、ネットワークからコンテンツを取得する際の所要時間を計測した。加えて、同じ条件で HTTP サーバを用いた実験を行い、提案システムと比較した。

この結果、提案システムでは、ネットワーク上のコンテンツ保持ノード数が増えるほどコンテンツ取得にかかる所要時間が改善でき、HTTP サーバを用いる方式に対して利点を持つことを示し

た。さらに、提案システムはコンテンツの一意な取得が可能なため、既存の HTTP サーバを用いたコンテンツ配信サービスと同等の利便性を実現できることを示した。

第7章　結論

本論文では、既存の P2P ファイル共有ネットワークを利用した新しいコンテンツ配信システムと、その実装である DiMPS について述べ、その有用性を示した。

まず、これまで一意性について考慮されてこなかった P2P ファイル共有ネットワーク上のファイルに対して固有 ID を付与し、ファイルデータの一意な取得と自動的な検証を可能にする。これにより、P2P ファイル共有ネットワークをコンテンツ配信基盤として利用することができる。次に、ファイルの構成要素をデータ、プロパティ、ポインタの 3 つに分割し、それぞれを別個のシステムで管理する。ポインタにはファイルの取得に必須な情報が保存されており、ポインタへのアクセスをコントロールすることで、P2P ファイル共有ネットワーク上で流通するファイルをコントロールできる。また、プロパティに格納されたレーティング情報を参照することで、ユーザは取得するファイルの評価を判断できる。加えて、ファイルの構成要素を複数のシステムで分担して管理するため、個々のシステムの負担を軽減することができる。

提案システムの実装である DiMPS は、抽象化によって、システムが利用する P2P ファイル共有ネットワークに対する透過性を高めている。これにより、システムの利用者は、実際に利用する P2P ファイル共有ネットワークの詳細を意識せず、簡便にコンテンツの配信と取得を利用できる。また、ウェブブラウザとの連携により、既存の HTTP サーバを利用したコンテンツ配信と同等の利便性を実現できる。

今後は、DiMPS を実環境で運用していくことで、さらに提案システムの有用性の実証及び改善点の検討を進めていきたい。

参考文献

[1] 岡本雄太, 蛭田智則, 山名早人: ”P2P ファイル共有ネットワーク上で動作するメタファイルシステム”, 日本ソフトウェア科学会インターネットテクノロジワークショップ 2005(WIT2005) (2005)

[2] 岡本雄太, 蛭田智則, 山名早人: ”P2P ファイル共有ネットワークを利用した大規模分散ストレージの実現”, 第 69 回情報処理学会全国大会講演論文集, Vol.3, pp.297-298, 1W-1 (2007)

[3] Sam Joseph: ”P2P Metadata Search Layers”. Agents and Peer-to-Peer Computing 2003, LNAI, No.2872, pp.101-112 (2004)

[4] Neil Daswani, Hector Garcia-Molina, Beverly Yang: ”Open Problems in Data-Sharing Peer-to-Peer Systems”, In Proc. of the 9th International Conference on Database Theory, Siena, Italy, pp.1-15 (2003)

[5] IWATA, T., ABE, T., UEDA, Y., SUNAGA, H.: ”A DRM system suitable for P2P content delivery and the study on its implementation”, Proceedings of The 9th Asia-Pacific Conference on Communications(APCC 2003), Volume 2, pp.806-811 (2003)

[6] 竹辺靖昭, 美馬秀樹, 苫米地英人: ”P2P コンテンツ交換システムにおけるコンテンツの整合性維持および全文検索の高度化”, 情報処理学会研究報告 2003-DSP-114, pp.31-36 (2003)

[7] 仁野裕一, 加藤大志, 福岡秀幸, 谷幹也: ”P2P ネットワークにおける情報の流通監視方式の提案”, 情報処理学会第 67 回全国大会, 6K-4 (2005)

[8] Gnutella: `http://www.the-gdf.org/`

[9] Winny: `http://www.geocities.co.jp/SiliconValley/2949/`

[10] The Official BitTorrent Home Page: `http://www.bittorrent.com/`

[11] LimeWire: http://www.limewire.org/

[12] VMware: http://www.vmware.com/

[13] Dummynet: http://info.iet.unipi.it/~luigi/ip_dummynet/

外部発表リスト

1. 岡本雄太, 蛭田智則, 山名早人: ”P2P ファイル共有ネットワーク上で動作するメタファイルシステム”, 日本ソフトウェア科学会 第 7 回インターネットテクノロジーワークショップ (2005.11)

2. 岡本雄太, 蛭田智則, 山名早人: ”P2P ファイル共有ネットワークを利用した大規模分散ストレージの実現”, 情報処理学会 第 69 回全国大会 (2007.03)

3. 岡本雄太, 山名早人: ”分散メタ P2P ストレージ「DiMPS」による
コンテンツ配信システムの実現”, 電子情報通信学会 第 19 回データ工学ワークショップ (DEWS2008) (2008.03)