キャッシュを利用したP2Pネットワークにおける匿名性

黒宮 佑介[†]　大薮 勇輝[‡]　重近 範行[†]　湧川 隆次[†]　村井 純[†]

1. はじめに

インターネットの普及により，私たちは容易に大量の情報を転送することができるようになった．そして，情報共有をより簡単に行えるツールとして，P2P ネットワークアーキテクチャを利用した，Winny や Share が登場した．これらのソフトウェアの特徴は，P2P ネットワーク上にキャッシュ機構を持つことである．この機構では，ファイルをあるノードへ転送する際に，転送を中継するノードにファイルのコピーを保持させ，単一ノードへのネットワーク負荷を減らし，ネットワーク内での効率的なファイル共有を実現している．しかしながら，既存のキャッシュ機構は，設計上の問題により，中継ノードが自分の保持したキャッシュの情報を知ることができるため，結果として，中継ノードに対しての「転送しているファイルの匿名性」が低いという欠点がある．したがって，今回私はこのようなキャッシュ機構を利用した P2P ネットワークにおける匿名性について考察し，その解決方法を提案する．

2. 既存の問題点と目的

既存のキャッシュ機構の問題点は，本来わかってはならないはずのキャッシュの内容がわかってしまうということである．Winny や Share などのキャッシュ機構では，キャッシュの匿名性の確保に暗号化を用いている．しかし，暗号化に用いる鍵をキャッシュが保持する実装や，鍵がネットワーク全体で共通の実装であるため，暗号が解析される可能性があり，匿名性を確保できていない．また，キャッシュの内容がわかることにより，中継ノードは，どのようなファイルが，どのノードからアップロードされ，どのノードへダウンロードされているかという情報を知ることが可能である．本研究ではこの問題を解決するため，中継ノードにおいてキャッシュの内容がわからない手法の提案を行う．

3. アプローチ

キャッシュ機構を利用した P2P ソフトウェアにおいて，キャッシュの匿名性を確保するため，キャッシュ本体とキー情報（暗号鍵）を分け，それぞれを別々のネットワークで管理するアプローチを考える．キー情報は Winny や Share と同じく，一定時間ごとに各ノード間でやりとりされ，ネットワークで分散して保持される．

P2P ネットワークは，キャッシュ本体を扱うコンテンツの転送専用の P2P ネットワークと，キャッシュのキー情報やファイルの検索などの情報管理を扱う P2P ネットワークを用意し，ノード情報を相互にやりとりすることで，ファイルの転送を行うようにする．このように，キー情報とキャッシュを別々のネットワークで扱うことで，キャッシュ本体とキー情報を持つノードがファイルをダウンロードしているノードのみとなり，中継ノードへの匿名性は確保される．

似たような仕組みとして，多くの DRM では，特にキー情報の部分を，P2P ネットワークではなく，既存のサーバ・クライアントモデルで行うことで，認証を行い，コンテンツの配布を行っている．

本提案の設計を図 1 に示す．図 1 において，ファイルをアップロード（送信）している A ノードは，どのノードが自分からファイルをダウンロードしているかわかるが，意図的なものなのか，中継により行われているものなのかはわからない．また，ダウンロード（受信）を行っているノード C も，自分はノード B からダウンロードを行っているということはわかるが，ファイルを公開しているノード A からの転送なのか，中継によるキャッシュからの転送なのかはわからない．中継ノードは自分でキー情報を取りに行かない限り，キャッシュ本体を復号することはできず，どのような内容なのかわからない．

また，このとき，ファイルを受信しているノード C は，ファイル共有ネットワークとは別の，情報管理ネットワークにおいて，自分がダウンロードするファイルのためのキー情報を検索し，あらかじめキー情報を共有しておく（この例ではノード D からダウンロードする）．そして，ファイルの共有が終わると，そのキー情報を用いてキャッシュを復号し，中継ノードに転送しているファイルの内容を知られることなく，安全にファイルの転送を行うことができる．

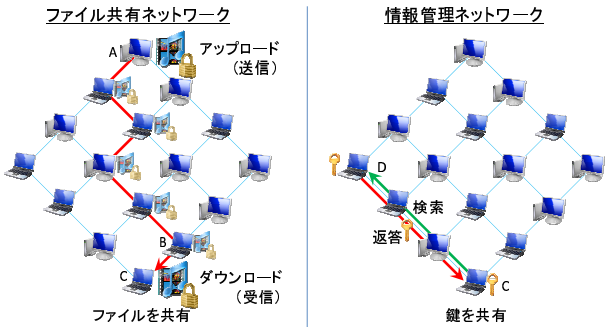

図 1: ファイル共有と鍵共有

4. これまでやったことと今後の予定

以上のことを実現するために，私は Winny クローンを開発し，その仕組みや動作について研究を行い，キャッシュ機構の問題とその解決法について考察した．

したがって今後は，その考察を活かし，キャッシュ機構などの弱点を克服し，ある程度の効率を確保しながらも，より匿名性について堅牢な仕組みを持った P2P ネットワークアーキテクチャを備えたソフトウェアを開発する．

[†]慶應義塾大学 環境情報学部 Faculty of Environment and Information Studies
[‡]慶應義塾大学 政策・メディア研究科 Graduate School of Media and Governance