「Winnyの技術」をもとに当時の到達点を明らかにする

講演：**金子 勇**（かねこ・いさむ）
Winny開発者
報告：**濱野智史**（はまの・さとし）
国際大学GLOCOM研究員

「Winnyの技術と倫理」シンポジウムで最初に講演のマイクを取ったのは，Winny開発者の金子勇氏である．Winnyは，音楽や映画のファイルや個人情報データなどが流通する「ファイル共有ソフトウェア」として紹介されることが多いが，金子氏によればWinnyには明確に異なる二つのヴァージョンが存在しており，後発のヴァージョン2は，ファイル交換の仕組みを土台にした「匿名BBSシステム」を備えている．ただ，これについては2005年夏に出版された『Winnyの技術』（アスキー）でも多くは言及されていない．

講演はWinnyの二つのヴァージョンに沿って行なわれた．まずは「Winny ヴァージョン1（以下，Winny 1）」というP2Pファイル共有ソフトウェアについての解説，次に「Winny ヴァージョン2（以下，Winny 2）」というBBS（掲示板）システムについての解説が行なわれ，最後に次世代P2Pシステムの展望と課題について言及した．金子氏の講演は，以上の三部構成となっている．

ちなみに，Winny 1のベータ1が公開されたのは2002年の5月であり，正式版が公開された1年後の2003年4月に，Winny 1の開発はいったん終了されている．その後Winny 2が2003年の5月に公開されたが，2004年，金子氏が京都府警に著作権幇助の罪で逮捕されて以降，Winnyの開発は一切停止されている．

以下は，金子氏の講演をもとに濱野智史が作成した報告である．

1. ファイル共有ソフトウェアとしてのWinny 1

1-1. Freenetに見る匿名性

金子氏は冒頭で，Winny 1を開発するきっかけについて，「Freenet（フリーネット）」というP2Pソフトウェアの「匿名性」に感銘を受けたからだと述べた．Freenetとは，開発者のイアン・クラーク（Ian Clarke）氏がインターネット上の言論の自由を実現する目的で考案した仕組みである．Freenetの用途はファイル共有だけではなく，このソフトウェアを経由することでメールやBBSを匿名で送受信できるように設計されている．

この匿名性のアイディアについては注釈が必要だろう．しばしば「インターネットは匿名性が高い」と言われるが，それはあくまで普段利用しているときの印象論でしかなく，技術的見地からすれば誤りである．実際は，ユーザーはブラウザでウェブページを見るたびに，自分が使用しているソフトウェアやIPアドレスといった個人情報を必ず通信先に提供している．テレビの視聴は一方的に電波を受信するだけあり，これは文字通り匿名であると言えるが，インターネットは自分の情報を送信しなければ情報を受信できないという双方向性を持つため，原理的には匿名性を持たない．そこでFreenetでは，すべてのファイルを暗号化し，ばらばらにネットワーク上に拡散させるという方法を取ることで，匿名性を実現している．この仕組みによって，ネットワーク上に誰がどのようなコンテンツを流通させようとしているのか，誰がどのハードディスクを提供しているのかを，誰も把握できない状況をつくることができるようになった．

しかし，Freenetには他のP2Pソフトウェアと比較して劣る点があった，と金子氏は指摘する．それはファイルの検索や転送に関わる効率性である．Freenetはファイルをばらばらに拡散させてしまうため，ファイルを復元する際にほうぼうからファイルの断片を探し回る必要があるが，Freenetのユーザーが常にソフトウェアを起動しているわけではないので，断片が行方不明になってしまう可能性も高い．そこでFreenet以前のP2Pソフトウェアでは，各ユーザーが所持しているファイル情報をサーバに集約することで，検索の効率性を上げていた．Napsterをはじめとする多数のサービスがこの方法を取っていたため，金子氏はこれらを「第一世代」のP2Pと呼んでいる．

しかし，そもそもP2Pとは「中央にサーバを置かずに，ピアーとピアー

(Peer-to-Peer) で通信する」という意味であるから，厳密には，第一世代の手法を純粋なP2Pネットワークと呼ぶことはできない．そのため，これは「ハイブリッド型」とも呼ばれている．また，第一世代ではサーバに情報が集中してしまうため，匿名性を守ることは困難になる．

このように，P2Pの匿名性と効率性はトレードオフの関係にあった．

1-2. 匿名性と効率性を両立するという目的

金子氏の目的は，Freenetのアイディアを継承しつつ，Freenetが解決できなかった匿名性と効率性のジレンマを解決することにあった．つまり，ファイル検索や転送の効率性を確保しつつも，情報発信者の出処を秘匿する――これが当初の技術的課題であった．金子氏は，たしかにFreenetに大きな影響を受けたが，それはあくまで匿名性を実現するという「思想」の部分であり，それを実現するシステムは一から開発したという．

暗号化したファイルを拡散させるFreenetの手法には無駄が多い．前述したように，ファイルを断片化すればするほど匿名性は高まるが，ばらばらになったファイルを再び収集するのは困難になる．そこで金子氏は，匿名性の本質は情報の「拡散」にではなく，「多段中継」にあると考えた．ファイルの流れる経路が複数段に及んでしまえば，オリジナルの出処はトレースしにくくなる．金子氏は，このように匿名性概念の読み替えを行ない，Winnyを設計した．

この多段中継を実現するために，金子氏は「プロクシーサーバ (proxy server)」と呼ばれる技術をP2Pシステムに導入した．プロクシーサーバとは文字通り「代理サーバ」を意味する技術で，その用途はさまざまである．例えば，匿名性を保つために，ウェブブラウザにプロクシーサーバを中継させる．こうすることで，向こう側のウェブサーバにはプロクシーサーバのIPアドレスのみが残り，手元のマシンのIPアドレスが開示されるのを防ぐことができる．もちろんプロクシーサーバ内にもIPアドレスは残るため，実際には完全に匿名性が守られるわけではない．しかし，プロクシーサーバを「多段中継」してしまえば，オリジナルの発信元へトレースするのは，事実上困難になる．

またプロクシー技術は，効率性の上昇のためにも用いられる．通信速度が遅かった時代には，例えば，米国のウェブサイトと毎回通信するのは無駄が

多いため，LAN内にプロクシーサーバを設置することで，ネットワーク負荷を分散させていた．各ユーザーが外部のウェブサーバから取得したデータをプロクシーサーバに一時的に保存（キャッシュ）し，同じページを閲覧しようとする人が現われた場合，わざわざ直接外部のサーバにデータを取りに行かずに，このキャッシュを表示することで，米国にあるデータをその都度取りにいく手間を省いていたのだ．

金子氏は，このプロクシーサーバの持つ二点を活かして，匿名性と効率性を両立させようと考えた．通信を多段中継すればオリジナルの発信元をトレースすることは難しくなるため，匿名性は上昇する．さらにファイルを多段中継する際，そのファイルを各ノードにキャッシュしておけば，ファイルの第一次発信者と通信する手間が省けるため，転送の効率性も上昇する．このように，Winnyネットワークに接続している各ノードがプロクシーサーバの役目を果たすことによって，匿名性と効率性を両立させるというのが，Winnyの基本的なアイディアである．


金子 勇氏

1-3. Winnyのキャッシュ機構

Winnyでは，この金子氏のアイディアは「キャッシュ機構」という仕組みで実現されている．Winny上に流通するデータは，ファイルのインデックス情報となる「キー（鍵）」と，ファイルそのものである「ボディ（本体）」とに区別される．キーとは，ファイル名，ファイルサイズ，ファイル本体を所持するIPアドレス，「ハッシュ値」★1といった情報を格納した，いわゆるメタデータのことである．他方，ボディとは，ファイルの中身を暗号化したもので，別名「キャッシュ」と呼ばれている．キーのほうがファイルサイズは小さいため，ネットワーク上で大量にやりとりできる．そしてボディ（キャッシュ）は各ノードに蓄積され，転送の際の資源として活用されるという性質を持つ．

Winnyがファイルを転送する仕組みは，次のような流れである．Winny

は，作動中にキーファイルを自動的にばら撒くように設計されているため，ユーザーはつねにキーファイルをやり取りしあう状態にある．こうすることで，Winnyはファイルの検索効率を上げている．次に目的のキーファイルが検索にヒットすると，Winnyはそのキーに含まれている「ボディ（本体）を所持しているIPアドレス」――ファイル本体の「位置情報」に相当する――を参照する．この位置情報を通じてボディを所持するマシンが割り出され，Winnyは転送を開始する．つまり，ボディはつねに流通しているわけではなく，他のユーザーからの要求があってはじめて転送される仕組みをとっているのだ．こうした設計の特徴について，金子氏は，キーをプッシュ型，ボディをプル型と表現している．

この「位置情報」は，一定のアルゴリズムで書き換わるように設計されている．この仕組みを筆者なりに表現すると，Winnyは手紙の差出人をランダムに書き換え，あえて誤配を起こすよう設計されている，と言えるだろう．Winnyは，キーの位置情報を書き換える際に，実際にはファイル本体を持っていないノードもボディの所有者として指定する．これは一見すると，匿名性を実現するために効率性を犠牲にしているように見える．しかし，この設計こそが，先述した匿名性と効率性のジレンマを解決するのである．

どういうことか．この誤指定されてしまったWinnyノードは，自分の手元に所持しているキーファイルを照合し，真にボディを持つであろうノードをたどっていく．そして真にボディを所有するノードを発見すると，Winnyはそこから転送を開始する．このとき，Winnyはダウンロード途中のファイルをそのままアップロードすることが可能になっているため，元々そのファイルを要求していたノードに対してファイル転送の「橋渡し（中継）」を行なうことになる．さらに橋渡しをしたWinnyノードは，このファイルを消すことなく，そのままキャッシュとしてハードディスクに蓄積する．このキャッシュは，次に発生する中継のための資源として用いられる．

このようにWinnyは，誤配をきっかけに橋渡しの機会を生み出し，橋渡しのたびにキャッシュを蓄積するというサイクルを繰り返す．このような方法をとることで，キャッシュはほうぼうに分散されることになる．つまり，エラーのようにも見える設計は，むしろWinnyにおいては効率性上昇の源泉であると言えるのだ．

また，金子氏によれば，Winnyは人気の高いファイルほどその位置情報が書き換えられるように設計されている．人気の高いファイルはやり取りが多く発生するため，ネットワーク帯域を圧迫しやすい．そこでWinnyは「誤配→橋渡し→キャッシュ」のサイクルをより多く発生させることで，ファイル転送の効率性を向上させた．また，このサイクルが繰り返されることで，ファイルの第一次発信者はますます区別できなくなるため，同時に匿名性も上昇する．

このWinnyの仕組みについて，「中継はトラフィック（帯域の混雑度）を上昇させるだけの無駄なシステムだ」という指摘があるという．しかし金子氏は，これは誤解であると強調している．たしかにWinnyは帯域を大量に消費する．インターネットのトラフィック量の大半は，WinnyなどのP2Pが占めているといったデータもある．しかし，金子氏の考えでは，Winnyの中継システムはネットワーク資源の有効活用が目的なのである．

以上に見られるように，Winnyは，意図的に誤配を生じさせることによって，コミュニケーションの効率性と匿名性を両立させる仕組みであると要約できるだろう．

1-4.「第三世代」としてのWinny 1

次に金子氏は，Winny 1について三点のことを述べた．

第一に，Winny 1が普及した要因についてである．「たしかにWinnyは匿名性と効率性の両立に成功しているが，Winnyが普及した要因は必ずしもこの点にはない」と金子氏は留保しつつ，次のように指摘している．P2Pソフトウェアの技術的な課題は，検索の効率性だとされてきた．しかし，この課題は金子氏からすれば他のソフトで「検証済み」だと考えており，むしろ金子氏が重要視した課題は「ノードの維持率」だった．つまり，Winnyのユーザーがなるべくプログラムを終了させずに，Winnyのノードとして存在しつづけるような状態をどう実現するか．金子氏の検証したかったもう一つの課題はここにあった．

そこで金子氏の出した解答は，Winnyの「自動ダウンロード機能」である．この機能によって，Winnyのユーザーは，目的のファイル名を検索し，あとはプログラムを放置しておくだけで，自動的にファイルをダウンロードすることができる．金子氏によれば，当初この機能は存在せず，むしろあまり

にもファイルの転送効率が悪かったために追加されたものだった．しかしこの機能が，結果的にWinnyを継続的に起動しつづけるユーザーの増大に繋がり，ノードの維持率に貢献することとなった．これがWinnyの普及した要因になったのではないか，というのが金子氏の見解である．

第二に，Winnyネットワークの対障害性の強さである．純粋なP2Pは，ハイブリッド型に比べてシステム全体がダウンしにくいという特性を持つ．ハイブリッド型は中央の検索サーバを攻撃されればネットワーク全体が機能不全に陥るが，純粋なP2Pはどのノードを攻撃してもシステム全体がダウンするということはない．開発者が何も手を加えていない現在でも，Winnyネットワークが稼動しているという事実が，これを実証している．

第三に，効率性の向上のために導入された，「上流／下流」という概念と「クラスタリング」という技術についてである．前者は，回線速度の速いノードを「上流」とみなし，上流にキーファイルを集中させる仕組みのことである．後者は，同じ検索キーワードを入力しているノードに優先的に接続することで，似たような趣味を持ったユーザーをネットワークの近傍に配置する仕組みである．こうしたネットワーク形成メカニズムによって，Winnyは効率性を上昇させている．

これらの特徴から，Winnyは「第三世代」のP2Pファイル共有を実現したと言えるのではないか，と金子氏は述べている．第一世代とはNapsterなどのハイブリッド型を，第二世代とはGnutellaなどの純粋なP2Pを指す．金子氏は，2002年当時，Winnyのキャッシュ機構のシステムは，この第二世代を改良した「次世代」と呼ぶに値しただろうと語った．ただし，すでに開発から4年も経った技術であるため，もちろんいまでは限界も多い，とつけ加えた．

2. 匿名BBSシステムとしてのWinny 2

次に，金子氏は大規模匿名BBSシステムであるWinny 2についての解説を行なった．

大規模匿名BBSの原型として想定されているのは「2ちゃんねる」である．2ちゃんねるはWWWサーバ上の掲示板プログラムで運営されているため，サーバ・クライアント型の弱点である負荷集中が課題となってきた★2．その

解決のために，大規模掲示板をP2Pシステムで実現するというアイディアは，金子氏がWinnyを開発する以前の2000年頃からしばしば議論されていた．「Winny 1はファイル共有ソフトウェアの技術的実験を終えてしまった」と感じた金子氏は，Winnyの大規模ネットワークをなにか別のシステムに応用できないかと考え，匿名BBSシステムの開発に着手した．ちなみに金子氏は，Winny 1は知的好奇心が開発の動機だったが，Winny 2はソフトウェア開発者の義務感から取り組んだと述べている．

Winny 2の実装について，金子氏は次のように解説する．その基本的なアイディアは，BBSにおける「スレッド」を，Winnyにおけるボディファイルとして扱うというものだ．スレッドとは，ある一つのトピック（スレッド・タイトル）に沿った一連の書き込みのことで，例えば，2ちゃんねるでは1000の書き込みが上限となっている．Winny 2では，ファイルの中に1番目からX番目までの投稿内容が連なって記述される．

ここで課題になったのは，ファイルの「同期問題」である．そもそもP2Pシステムでは，ファイルをたらい回しにするために途中で破損や欠落が起こりやすい．そのため通信途中でファイルが変化しないよう，同一性を確保する必要がある．金子氏によれば，Winny 1はこのP2Pシステムにおける同期問題を簡潔な仕組みで解決していた．Winny 1はハッシュ値と呼ばれる仕組み（註1参照のこと）を用いており，ネットワークの途中でファイルの内容が一切書き換わらないという前提で同期を取っていた．しかし，これをBBSシステムにそのまま応用することは不可能である．なぜなら一つのスレッドファイルに書き込みを順次追加していく場合，これは「通信途中でファイル内容を書き換えていくこと」を意味するからだ．つまり，Winny 1のハッシュ値の仕組みは，Winny 2では応用できない．

そこでWinny 2に実装されたのは，「それぞれのスレッド（＝ボディファイル）は，必ず特定の一つのノード（マスター）が管理する」という仕組みである．Winny 2は，スレッドへの書き込み（ファイル内容の追加）をする際，それぞれその管理者のノードに対して行なう．こうすることで，マスターに必ず最新の投稿が集中するため，ファイルの同期問題は発生しない．しかし，この仕組みでは，書き込みをするとき必ずマスターへの接続が集中してしまう．これはつまり，Winny 1の実現した「情報の多段経由による匿名性」が成立しないことを意味する．そこでWinny 2は，書き込みは一つ隣のノー

ドから行なわれるように設計されている．

しかし金子氏は，Winny 2はまだ開発途上にあったため，決定的な欠陥が存在すると述べている．それは，この仕組みではマスターの匿名性を守ることができない点というである．例えばWinny 2では，スレッドの読み込みボタンを連打するとマスターに直接繋がってしまうという仕様になっており，連打するだけでそのスレッドを最初に立てたノードが判明してしまう．

以上が匿名BBSを目指したWinny 2の解説である．Winny 2では，分散型BBSに存在する同期問題を，マスターの一括管理という機構で解決した．しかしその代わりにマスターの匿名性が犠牲になっている．金子氏はこのトレードオフを解決するアイディアを持っていたが，Winny 2の開発中止によって実現できなかったと述べている．

3. 次世代P2Pシステムの展望と課題

最後に金子氏は，次世代P2Pシステムのための課題を二つ挙げている．第一に「Winnyはオープンシステムにならないのか」という問題，第二に「P2Pシステムは管理できないのか」という問題である．

第一点目だが，Winnyはソースコードを非公開にしたまま開発されており，いわゆるオープンソースではなかった．Winnyのプロトコルや暗号化については，書籍でその仕組みを解説しているとはいえ，ソースコードがオープンになったわけではない．金子氏はこの点について，Winnyのファイル暗号は匿名性に寄与していないため，ソースコードを公開したとしても匿名性の保持に支障が生じるわけではなかったと述べる．

それでは，なぜWinnyはオープンソースにならなかったのか．それは効率性の問題だと金子氏は言う．そもそもP2Pソフトウェアの利用者の中には，ファイルを一方的にダウンロードするだけで，一切ネットワーク上にアップロードしない「フリーライダー（タダ乗り）」が一定数存在する[★3]．ソースコードが公開されれば，彼らはファイルを一切アップロードできないように改造してしまうだろう．この事態を危惧したため，ソースコードを公開することはできなかったと金子氏は述べている．

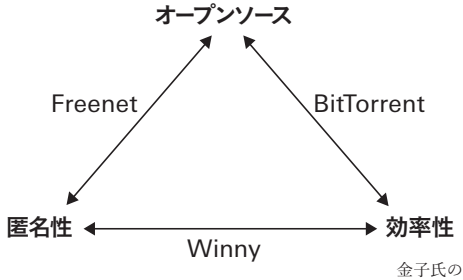
しかし金子氏は，これは2003年当時の事情だという．いまではWinnyとは別のP2Pシステムが開発されている．例えば，オープンソースの

「BitTorrent（ビットトレント）」はこの効率性とソースコードの公開性のジレンマをクリアしている．ちなみにBitTorrentとは，2001年からブラム・コーエン（Bram Cohen）氏の開発しているファイル共有システムで，人気の高いファイルほど，たくさんのノードから同時ダウンロードを行なうため，転送効率が極めて高いことで知られている．

金子氏は，このBitTorrentも第三世代P2Pシステムとみなしたうえで，第三世代P2Pには，匿名性・効率性・オープンソースの「トリレンマ（trilemma）」の構造があると指摘している（図1）．金子氏はこう説明する．Winnyは匿名性と効率性を両立させることに成功した．しかしその代わりにオープンソースにはできなかった．Freenetはオープンソースで匿名性を重視しているが，効率性の面で劣っていた．そしてBitTorrentは，オープンソースで効率性を実現しているが，匿名性は一切考慮されていない．つまり，匿名性・効率性・オープンソースの三点を同時に満たすシステムは，現在のところ存在しない．しかし金子氏によれば，いますぐこれは実現可能である．おそらく次世代のP2Pファイルソフトウェアは，匿名性・効率性・オープンソースという三つの特性を満たすものとなり，特にBitTorrentの仕組みが発展する可能性が高い．

第二に，P2Pの管理可能性の問題である．先述したように，純粋なP2P（ピュアP2P）では任意のノードがダウンしてもネットワーク全体に影響を及ぼさないため，耐障害性は強いとされている．しかしこれは裏を返せば，管理可能性が弱いとも言えるのだ．例えば，個人情報を含む名簿ファイルなどがWinny上に流出した場合，これを管理者が一挙に削除するような仕組

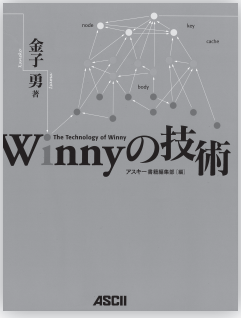
図1：第三世代P2Pにみられる「トリレンマ（trilemma）」の構造



金子氏の講演資料をもとに作成

みは存在せず，永遠にファイルが流通し続けてしまう．実際，海外のP2Pファイル共有ソフトウェアをめぐる裁判では，純粋なP2Pのサービスは管理者不在であるため，開発者や運用会社の責任は追及できず，ユーザーへの裁判が集中している．

しかし金子氏は，この問題は技術的な欠陥に過ぎないと強調する．金子氏は，ピュアP2Pでも管理可能性を実現するアイディアがあるが，現在刑事裁判で係争中のためWinnyの改良に手をつけることができないと述べ，講演を締めくくった★4．



『Winnyの技術』
金子勇 著，アスキー書籍編集部 編
アスキー
2005年10月28日刊
B5変形判，204頁，本体2400円

★1――ハッシュ値とは，辞書的には「原文から固定長の疑似乱数を生成したもの」である．例えば「議事録.doc」という40キロバイトのファイルがあった場合，ハッシュ関数によって「fb3a0ec36」といった一定の桁数の乱数値へと変換される．このハッシュ値は，ファイル名が変わっても，ファイルの中身が変わらなければ書き換わることはない．しかしファイル名が同じであっても，1バイトでもその中身が変化していればハッシュ値は書き換わる．この性質を使って，データが通信途中に改竄されていないことを確認することができる．

★2――2002年8月に，2ちゃんねるはサーバ負担が大きすぎるため掲示板閉鎖の危機に直面した．しかし，2ちゃんねるユーザーの有志が掲示板プログラムの改良を行なうことで，閉鎖は回避された．この事件については，例えば鈴木謙介『暴走するインターネット』（イーストプレス，2002年）を参照のこと．

★3――P2Pファイル共有ソフトウェザで著作権侵害を行なう場合，これは日本の法の下では，著作権法の「ダウンロード送信可能化権」の侵害にあたる．これは「ファイルをアップロード可能な状態にする」という状態を咎めるものであるため，P2Pのユーザーにとって，アップロードはダウンロードに比べてリスクが高い．そのため，ダウンロードだけを選好する「タダ乗り」的なユーザーが多くなる．

★4――「Winnyの技術と倫理」シンポジウム後，Winny上で個人情報データの流出が相次いだ．金子氏はこの問題について，3月11日に大阪で行なわれたLSEのイベントで，「ウィニーネットワークが健全であることを望む．プログラムを数行書き換えることで漏えい対策はできるが，警察や検察との関係で動けない．求められれば協力する」と述べたという．「ウィニー開発者：『流出は想定外で残念』講演会で主張」MSN毎日インタラクティブ，3月11日，<http://www.mainichi-msn.co.jp/keizai/it/24hour/news/20060312k0000m040085000c.html>.

また3月20日の第21回公判で，弁護側は，金子氏がWinnyの技術を応用したP2Pソフトウェア「オズテック」をIT関連企業と共同開発していると明らかにした．このソフトでは，アップロードする側の管理可能性を実現しているという．「ウィニー：開発者，今度は安全に流通させる新ソフト」MSN毎日インタラクティブ，3月20日，<http://www.mainichi-msn.co.jp/today/news/20060321k0000m020066000c.html>.