社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－DD－69（13）
2008 / 11 / 28

アドホックネットワークによる監視カメラシステムの提案

植村　渉†　村田　正†

† 龍谷大学理工学部　〒520–2194 滋賀県大津市瀬田大江町横谷 1–5
E-mail: †{wataru,murata}@rins.ryukoku.ac.jp

あらまし　基地局を介さず端末のみでネットワークを構築するアドホックネットワークが近年注目されている．このネットワークでは，管理者となるサーバが存在しないため，ネットワークに流れる情報の管理が難しい．本研究では，アドホックネットワークの技術を監視カメラシステムに適用し，新しいシステムを提案する．撮影したカメラ画像をネットワーク内の端末で共有することで，犯罪証拠画像の完全破壊を困難にする．

キーワード　アドホックネットワーク，監視カメラシステム

A Novel Surveillance Cameras System by Ad Hoc Network

Wataru UEMURA† and Masashi MURATA†

† Faculty of Science and Technology, Ryukoku University　Seta 1–5, Otsu City, Shiga, 520–2194 Japan
E-mail: †{wataru,murata}@rins.ryukoku.ac.jp

Abstract　In ad-hoc network, we can build a network infrastructure easily. In addition, it is easy to add nodes to the network and to remove them from it. So the ad-hoc network technology lends itself to applications such as the environment where a lot of nodes go in and out frequently. In this paper, we propose a novel surveillance camera system at a car park in ad-hoc network. A node mounted on a vehicle has a camera and sends a picture to neighbor nodes. Even if the node is damaged or removed by a vehicle thief, we can know the thief information from the other nodes which received its picture. Each node has own random strings data, and the picture information is calculated by XOR operation from its original picture data, so the picture information can not be decoded into the original picture without the same strings data. We can not know its strings data even if using a lot of picture information because the length of the strings data is more longer than one of the picture data. Then a node cannot get the neighbor original picture. The strings data can be kept at only both the own node and the administrator of its car parking lot. If the node is stolen or broken down, then the administrator can decode the picture information at the neighbor node into the original picture data. We propose a novel surveillance ad-hoc network system at a car park in this paper.

Key words　ad-hoc network, surveillance cameras system

1. まえがき

近年，基地局を用いず端末のみで無線ネットワークを構築するアドホックネットワークが注目されている．ネットワークを管理する基地局がいないため，端末同士でネットワーク情報を交換し合うことで，経路設定を可能としている．ネットワークへの端末の動的な追加や離脱を考慮しているため，インフラの構築が簡単である．そのため，局所的なネットワークが新たに必要な場所や，既存のネットワークが破損した場所への適用が研究されている．例えば従来の研究として，インフラが破壊された災害現場への利用や，車車間通信への利用が挙げられる．本研究では日常生活への応用として，駐車場における監視カメラシステムを提案する．

平成 17 年の警察白書によると，車上ねらいの発生件数は 256,594 件 [1] である．また車内の物品を盗むだけでなく，自動車そのものを盗む犯罪も多発しており，同資料によると 46,728 件が認知されている(注1)．これら車における窃盗に対して，さまざまな防犯システムが提案されているが，ここでは監視カメラシステムに注目する．

監視カメラシステムに期待される役割は，大きく分けて 2 つある．犯罪証拠の記録と犯罪の抑止効果である．

(注1)：平成 18 年は車上ねらいの発生件数は 205,744 件，自動車盗は 36,058 件に減少している [2].

犯罪証拠の記録は，カメラによる機能である．記録方法としてカメラ自身で記録する方法と，離れた監視センタに情報を送ってリアルタイムで監視する方法がある．犯罪発生時に警備員を派遣するためにはリアルタイムで監視する方法が望ましく，個人のプライバシを確保するためにはカメラ自身に記録し後から確認する方法が望ましい．いずれにしても，犯罪者にカメラの場所を知られると，死角をうまく利用されたりカメラや監視センタへのネットワークを破壊されたりする危険があるため，カメラはできる限り目立たない場所に設置する必要性がある．

車上荒らしが発生するのは人目のつかない場所が多いため，カメラで撮影や監視されていると犯罪者に感じさせることで犯罪の抑止効果が生じる．しかし，そのためにはカメラを人目のつく場所に設置する必要があり，先ほどの犯罪証拠の記録のための設置方法と相反する．一般には，目立つ場所にわざと設置して抑止効果を期待するカメラと，死角をなくして現場の情報を確保するためのカメラという2種類のカメラを，役割に応じて複数設置することが多い．また，カメラの設置場所は，いたずらされないよう一般の人の手の届かない場所におく必要がある．

カメラ自身に記録する方法は，単体で完結するため設置が簡単な反面，撮影情報の再生にはカメラから記録メディアを取り出す必要があるため手間がかかる．監視センタへ接続する場合，センタまでネットワークを構築する必要がある．有線で接続すると回路が簡単であり帯域も十分確保できるため，ビデオ信号として動画で配信することが多い．ただし，配線の取り回しのコストがかかり，特に既存の施設にあとから設置するのは大変である．また，途中で断線する危険性もある．

無線でネットワークを構築する場合，配線は楽であるが，基地局のアンテナの受信範囲内にしか設置できず，特に建物内では設置可能場所が変則的になりやすい．また，無線の周波数帯域の制限があるため，限られたチャネル数しか使うことができず，カメラの追加が難しい．

これらをまとめると，屋内では通信可能エリアが狭いので有線を用いることが多く，屋外では配線が大変なので無線を使うことが多い．最近は，有線・無線ともに帯域を有効利用するために画像の垂れ流しをやめ，IP パケット網を構築して，呼ばれたときだけ画像情報を送信する種類のものが増えてきている．TCP/IP ネットワークの規格に準ずることでインターネットへも接続可能で，外出先や携帯電話から画像を確認することもできる．

現在の監視カメラシステムでは，カメラを破壊されたり盗まれたりすると，犯罪の証拠情報が残らない危険性があり，それを補うためには死角がなくなるように設置する必要がある．しかし台数が増えると，有線の場合は配線のコストがかかり，無線の場合はチャネル数が足りなくなる．これらのことより，今後の監視カメラシステムとしては，静止画を無線で配信し，かつ端末に記録装置がついている形態へと移り行くと考えられる．ただし，無線配信を用いる場合は，屋内監視には向かない欠点が残っている．

本研究では，これらの動向を踏まえ，無線端末のみで構築する監視カメラシステムを提案する．このシステムでは，画像情報を管理するセンタをおかず，各端末がお互いの画像情報を保存しあうネットワークを構築する．データを集中管理しないため，弱点となる箇所を分散させることができる．端末を車に設置することで，常に設置場所が変化し，どこから監視されているかわからなくなる特徴がある（図1）．また，カメラのついていない無線端末を駐車場に設置することで，ネットワークの維持を助け，さらに画像の確保を助ける．この端末を人の手の届かない壁の中などに設置することで，端末の完全なる破壊をふせぎ，犯罪情報の確保が可能となる．

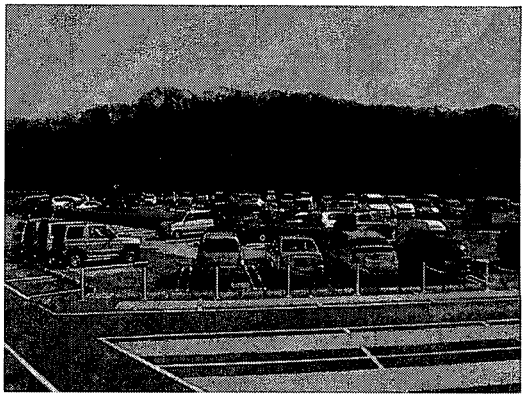

図1　自走式平面駐車場

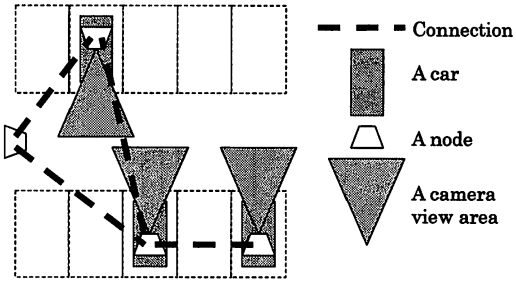

図2　駐車場における端末の配置の例

以下，2節では新しい監視カメラシステムを提案し，その特徴について議論する．そして3節にて既存のアドホックネットワークの技術と比較し，4節にてまとめる．

2. 監視カメラシステム

本節では，端末のみで構成する新しい監視カメラシステムを提案する [7].

このシステムでは2種類の無線端末を用いる．カメラのついている端末と，カメラのついていない端末である．カメラあり端末は車に設置し，カメラなし端末は駐車場の敷地に設置する（図2）．カメラの有無の違いだけで，それ以外の無線通信機能や画像保管能力などは同等である．

カメラあり端末は，あるタイミングで画像を撮影すると，それを自端末に保管すると共に隣接端末へも配信する．隣接端末は画像を受信すると，自端末に保管し，その後あるタイミング

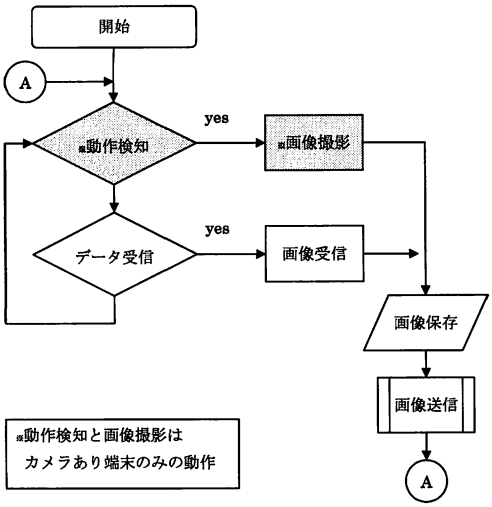

図 3 監視カメラシステムの端末フローチャート

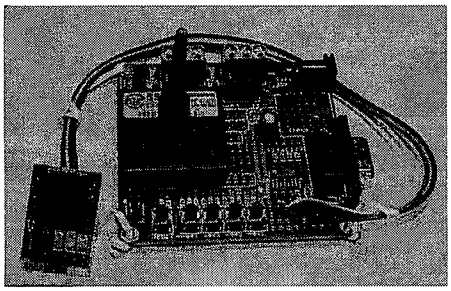

図 4 JPEG カメラを接続したカメラモジュール

でさらに隣接端末へと配信する．これを繰り返すことで，ネットワーク上の各端末で，撮影画像を共有するシステムである（図 3）．カメラなし端末は，画像の撮影を行わないだけで，それ以外はカメラあり端末と同じ動作をする．

この節では，この提案する監視カメラシステムの特徴について議論する．

2.1 無線モジュール

監視カメラシステムには，8 ビットのマイコンつき無線モジュール SS-1（表 1）を用い，シリアルカメラを接続する（図 4）．ただし，このマイコンの記憶容量は小さいため，もう 1 つのシリアル接続でさらに外部マイコンと接続する．

センサーネットワークでよく用いられる ZigBee の物理層は IEEE 802.15.4 に準じているが，この無線モジュールも同様に IEEE 802.15.4 に準じている．しかし，ZigBee の通信プロトコルは積んでいないため，中継機能などは持っていない．本提案手法では，隣接端末への画像情報の送信を繰り返すことでネットワークに情報を分散させるため，中継機能がなくても問題ない．

2.2 撮影画像の暗号化

今回使用するモジュールには加速度センサーがついているため，車の揺れを検知するセキュリティシステム同様に，外部からの攻撃を検知できる [9]．揺れ検知にあわせた写真撮影が可能であり，さらに異常事態を隣接端末に伝えることで，周りの端末に撮影のきっかけを与えることができる．それ以外には，モジュールに接続している外部マイコンを利用して，撮影画像の差分情報などから動体検知を行うことも考えられる．

これらの情報を用いて写真を自動撮影できるが，その写真を他端末に転送するにはプライバシの問題を考慮しないといけない．そこで，撮影画像を暗号化し，他の端末で撮影した画像は再生できないようにする．ここでは鍵を用いた XOR による暗号化を考えるが，それ以外の暗号化を用いても問題ない．マイコンの計算能力との兼ね合いで，実用的な方法を用いれば十分である．

カメラあり端末は，撮影画像と同等の長さのランダム文字列を保持しておき，撮影した画像と XOR を取ったものを画像情報として保存する（図 5）．この暗号化された画像情報を隣接端末に送信する．鍵となるランダム文字列は，自端末以外には管理者のみが保管するものとする．管理者は，この監視カメラネットワークとは物理的に異なる場所に鍵を保管し，有事の際にのみ取り出すこととする．これにより，もし端末を盗まれても，その端末のカメラが撮影した画像しか見ることができず，他の端末が撮影した画像のプライバシを守ることができる．また無線通信をする上では，通信を傍受される可能性は十分あるが，送信している情報自身が暗号化されているため問題にはならない．

これ以外にも，画像を転送する際に情報を分割したり冗長性を付加することで，1 枚の画像情報から元の情報を復元できなくすることも考えられるが，これらの方法に関しては今後の課題とする．

2.3 画像の中継について

画像情報は，隣接端末への転送を繰り返すことで，ネットワーク内の端末で情報を共有する．無線通信を用いるため，配送方法はブロードキャストとなり，基本的に範囲内の端末に同時に届けることが可能である．

表 1 The Specification of Wireless Module(SS-1).

Size	32 mm × 32 mm × 9 mm
Voltage	3.3 v
Electric Current	2 μA for waiting
	40 mA for sending
Modulation	2.4 GHz spread spectrum
	(IEEE 802.15.4)
Speed	250 kbps
Sensor	Acceleration sensor
	Temperature sensor
g-Range = 1.5g	800 mV/g
g-Range = 2g	600 mV/g
g-Range = 4g	300 mV/g
g-Range = 6g	200 mV/g
Acceleration Modes	Dynamic Acceleration
	Static Acceleration
Supply Voltage(V_{DD})	-0.3 to +3.6

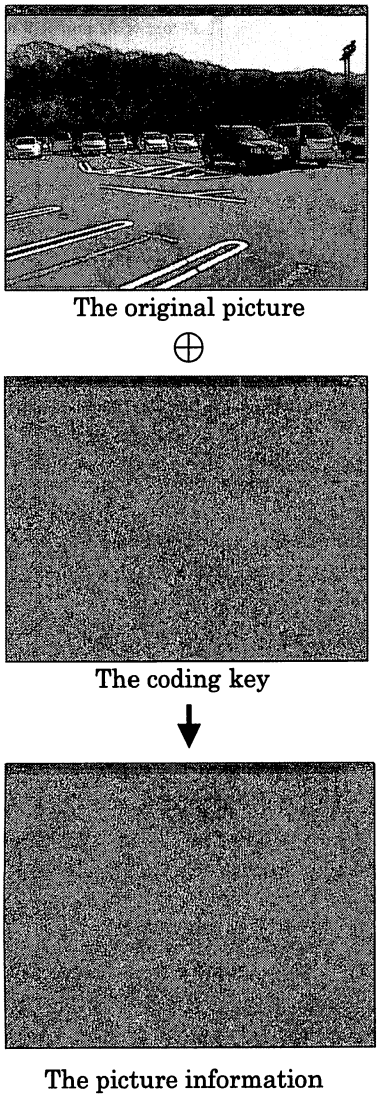

図 5　各端末の持つ鍵と，それによる画像の暗号化の例

同じ画像を重複して受信したときは，そこで転送を終了すれば良い．もし，画像情報の転送回数を 1 回に制限すると，端末はブロードキャストにより隣接端末に画像情報を送るだけで十分である．もし，2 回以上の場合は，各画像情報に転送回数の情報を付加して管理する必要がある．そして，転送するごとに 1 減らし，0 になると転送を終了する．全端末で画像情報を共有するためには転送回数の制限をなくすのが良いが，その分保存媒体の容量を圧迫するため，駐車場の規模に応じて転送回数の制限を行う必要がある．これらの関連に関しては今後の課題とする．

端末が画像情報を送信するのは次のときである．1) 加速度センサーの感知などにより写真を撮影したとき，2) まだ転送回数の残っている画像を持っているとき．これらのとき，端末は隣接端末に画像情報を転送する．通常 1 対 1 通信の場合，受信確認（ACK）を送ることで通信を進めるが，1 対多のため，多数の端末から ACK を返すわけにはいかない．そこで，正常受信の時には何も返さず，受信失敗の場合に NAK を送る方法を採用する．もし，複数端末が受信失敗して多数の NAK が競合しても，電波の強い 1 つの NAK が送信端末に届けば再送が実現できる．これらの成功率に関しては，現在研究中である [10].

2.4　画像情報の容量

本研究では，320 × 200 ピクセルの画像サイズを対象と考えている．ファイル形式として JPEG を用いるため，圧縮の結果画像ファイルサイズは一定にならないが，平均して 5kB であった．

1GB の容量を持つ CF カードや SD カードを使うと，約 20 万枚の画像情報を記録できることになる．適度な人の出入りがある研究室を撮影した場合，1 日 1 万枚の情報必要であったため，単純に考えると 10 端末 2 日の画像情報が保管できる計算となる．実際に駐車場にて測定する必要があり，その結果に応じて画像サイズの調整も検討する必要がある．

2.5　セキュリティ

提案手法のセキュリティに対する頑強性について検討する．セキュリティに対してこのシステムには 2 つの項目がある．1 つ目は，それぞれの端末が独自の鍵を持っており，各撮影画像を暗号化していることである．これは，2.2 節にて議論している．2 つ目は，端末が撮影した画像情報を隣接端末で共有していることである．この要素について検討する．

車載端末は破壊や盗まれる直前まで撮影を続ける．従来のセキュリティシステムでは，端末が破壊されたり盗まれると情報は残らない．一方，提案システムでは，隣接端末に画像情報を送り続けるため，犯罪者の写っている情報が残っている可能性が高い．もし，犯罪者が撮影された画像を削除しようとするならば，情報が中継された隣接端末全てを破壊しなければならない．しかし，その隣接端末もさらに画像を転送しているため，結局犯罪者は全ての端末を破壊しないと安心できない．

ここで，カメラなし端末が重要となる．カメラなし端末は無線でつながる範囲であればどこにでも設置できるため，壁の中など犯罪者の手の届かない場所に設置できる．そのため，犯罪者は全ての端末を破壊が不可能である．結果として，端末を破壊することは自分の画像を残すことにつながるため，車上荒らし自身の抑止力として期待できる．

3.　アドホックネットワークについて

端末のみでネットワークを構築するアドホックネットワークでは各端末が対等の立場であるため，ネットワークを一元管理できない．各端末でネットワークの状況を把握する必要がある．特に重要となるのは，端末の追加と離脱により，ネットワーク形態が変化する場合である．この節では，アドホックネットワークにおける従来の研究を紹介し，ルーティングプロトコルについて説明する．

3.1　ルーティングプロトコル

管理者の存在しないアドホックネットワークでは，ネットワークの維持のためにルーティングテーブルの更新が重要とな

る．各端末が自由に移動するため，パケットを送信したいときにルーティングテーブルが古く現状と異なると，適切にパケットを送信できない．

ルーティングテーブルを最新にするために，大きく分けて2種類のルーティングプロトコルの提案がされている．1つ目は常にルーティングテーブルを交換し合うことで最新情報を維持する方法である．プロアクティブ型のルーティングプロトコルと呼ばれ，OLSR(the Optimized Link State Routing protocol) [6]などが該当する．ルーティングテーブルが常に最新なので，パケットを送りたい時にいつでもすぐに送ることができる．しかし，ルーティングのための情報を交換し合うため常に通信する必要があり，電力の消費が多い．それに対してリアクティブ型のルーティングプロトコルでは，経路要求が発生してから経路構築を行う．AODV(the Ad-hoc On-Demand Distance Vector routing) [3]，DSR(the Dynamic Source Routing Protocol for Mobile Ad Hoc Networks) [4]，そして DYMO(Dynamic MANET On-demand Routing) [5] などが該当する．経路要求のないときは情報を交換しないため電力効率が良いが，経路を作るのに時間がかかるため実際にパケットを送信するまでに時間がかかる．これら両方を組み合わせて使うハイブリッド型なども提案されている．

ルーティングテーブルの維持が必要なのは，以下の2点の理由である．まず端末が自由に動くため，接続状況が動的に変化し，過去の情報が意味を持たないからである．次に離れた端末と1対1通信を行うためである．

今回使用する無線モジュールには，加速度センサーが内蔵されている．そのため，端末の移動を検知でき，端末の移動時にルーティングテーブルを交換し合えば，ネットワークの維持が可能である [8]．運転時の揺れに対する対策などが必要であるが，従来のアドホックネットワークのルーティングプロトコルとは異なる問題点を持つ．

また，提案する監視カメラシステムでは，離れた端末と通信する必要がなく，隣接端末にさえデータを送信できれば十分である．離れた端末へは，その隣接端末が後ほど送信すればよく，急いで遠くの端末に送らなくても十分である．これらより，ルーティングテーブルの維持はさほど問題ではない．

従来アドホックネットワークではルーティングプロトコルの研究が中心であったが，今回提案するシステムではあまり重要でない．

3.2 ネットワークの形態

端末のみでネットワークを構築する方法として，P2P 技術がある．P2P 技術を用いたファイル交換ソフトとして Winny [11] などが有名であるが，これらは，既存の物理ネットワークの上に仮想的なネットワークを構築し，そこでの通信に着目している．つまり，通信インフラは安定している．それに対してアドホックネットワークは，通信インフラにおいて基地局が存在しないため，ネットワークの維持が困難である．しかし，通信インフラを安定させることができれば，概念的には似ている．そのため，Winny における情報流失事件と同様に，アドホックネットワーク上で端末による情報共有を行えば，情報の完全消去は難しいものとなる．本研究で提案する監視カメラシステムは，この特徴を利用している．

4. おわりに

本研究にて，アドホックネットワークを用いた駐車場における新しい監視カメラシステムを提案した．このシステムには，2つのセキュリティの考えが含まれている．1つ目は暗号化のための鍵であり，2つ目はネットワーク全体で画像情報を共有することである．

各端末は独自の暗号鍵を持ち，全ての撮影した写真を暗号化する．例えば鍵との XOR である．それゆえ，他の端末からは画像情報を復元できず，一定のプライバシが確保される．

撮影した画像は，ネットワークに属するほかの端末にも転送される．そのため，ある端末が破壊されたり盗まれたりしても，その端末が撮影した情報は取り出せる．撮影された情報を完全消去するためには，全ての端末を破壊する必要があるが，見えない場所にも端末を設置可能なため，完全消去は不可能である．

現在，無線モジュール SS-1 を用いてシステムを構築中である．今後は実際に設置し，運用上での問題点を検討する必要がある．

謝　辞

本研究は文部科学省のハイテク・リサーチ・センター整備事業（平成18年度-）による私学助成を得て行われた．

文　献

[1] Keisatsu Hakusyo(Police White Paper) 2006, Section 2.1.3, Figure. 2–11, the number of street crimes(1996 – 2005), http://www.npa.go.jp/hakusyo/h18/honbun/hakusho/h18/html/i2130000.html#i2011000

[2] Keisatsu Hakusyo(Police White Paper) 2007, Section 1.3.1, Figure. 1–9, the number of street crimes(1997 – 2006), pp.66 – 68, http://www.npa.go.jp/hakusyo/h19/honbun/pdf/19p01000.pdf

[3] C.Perkins, E.Belding-Royer, and S.Das: Ad hoc on-demand distance vector(AODV) routing, Internet Engineering Task Force(IETF), Internet-Draft: draft-ietf-manet-aodv-13.txt (July, 2004).

[4] D.B.Johnson, D.A.Maltz, and Y.Hu: The dynamic source routing protocol for mobile ad hoc networks(DSR), Internet Engineering Task Force(IETF), Internet-Draft: draft-ietf-manet-dsr-10.txt (July, 2004).

[5] I.Chakeres, Boeing, C.Perkins, and Nokia: Dynamic MANET On-demand (DYMO) Routing, Internet Engineering Task Force(IETF), Internet-Draft: draft-ietf-manet-dymo-05.txt (June, 2006).

[6] T. Clausen, P. Jacquet: Optimized Link State Routing Protocol (OLSR), Internet Engineering Task Force(IETF), RFC3626: http://www.ietf.org/rfc/rfc3626.txt (October, 2003).

[7] W. Uemura and M. Murata: A Proposal of a Novel Surveillance Ad-hoc Network System at a Car Park, In 2007 Hawaii and SITA Joint Conference on Information Theory, pp. 172–176, (2007).

[8] W. Uemura and M. Murata: A Novel Ad-hoc Network Routing Protocol with an Acceleration Sensor, In 5th International Conference on Information Technology and Applications, pp. 211 – 213, (2008).

[9] W. Uemura and M. Murata: Classification of Car Motion Detection using Neural Networks based on Accelera-

tion Sensor, In Joint 4th International Conference on Soft Computing and Intelligent Systems and 9th International Symposium on advanced Intelligent Systems (SCIS & ISIS 2008), pp. 1944 – 1946, (2008).
[10] W. Uemura and M. Murata: A Proposal of Pictures Sharing Network Using Multicast with NAK, In International Conference on Control, Automation and Systems 2008 (ICCAS2008), pp. 1540 – 1543, (2008).
[11] 金子 勇: Winny の技術, アスキー書籍編集部, (2005).