巻頭言

それ、本当に開いても大丈夫ですか？

伊藤 和人
情報メディア基盤センター長

標的型攻撃が増えている。警視庁の分析によれば、2016 年には 4,046 件、2017 年には 6,027 件と急増している。情報セキュリティにおける標的型攻撃とは、特定の組織や人物を標的として狙いを定めて、個人情報などの重要情報を盗み取る、重要情報を人質にして身代金を要求する、不正アクセスに悪用するために情報機器を乗っ取る、といった攻撃を指す。

メールを用いた標的型攻撃の代表的な手法の 1 つはメールに添付されたファイルをメール受信者に開かせるもの、もう 1 つはメール本文中に示されたウェブサイトをメール受信者に訪問させるものである。添付ファイルを開くと PC がウィルスなどの不正ソフトウェア（マルウェアという）に感染し、マルウェアが PC 内の重要情報を外部に送信する。重要情報を暗号化して利用不可にし、重要情報を人質にして暗号解除するための金銭を要求するのがランサムウェアだ。感染直後は目に見える症状が出ず、ひそかに PC に不正侵入の裏口を作るマルウェアもある。不正なウェブサイトは、訪問するだけでマルウェアが勝手に PC に取り込まれ、感染する。あるいは、訪問したウェブサイトで言われるままにパスワードを入力するとパスワードが盗み取られる。一般利用者 1 名のパスワードが盗まれたことをきっかけにシステム管理者のパスワードが破られ、大量の重要情報が漏えいした例もある。

攻撃メールに書かれた内容が自分に関係ないと思えば不正な攻撃メールと判断して無視するが、例えば自分が使っているメールシステムの警告メッセージに似せたものは、一瞬本物と信じてしまうこともあるだろう。実は標的型攻撃も、うそを本当と信じ込ませる、という手口は従来の攻撃と変わりない。標的型攻撃では、標的の個人情報や関係するキーワードをメール本文にちりばめて、言葉巧みに標的を信じ込ませる。マルウェアとその感染経路が高度化しているのも事実だが、それよりもだましの手口が悪い意味で洗練されてきている。それゆえ標的型攻撃は「高度化している」とは言わず「巧妙化している」と表現される。標的型攻撃とは、プロの詐欺師が狙いを定めてだまそうとしているのだと認識すべきだ。だまされないために細心の注意が求められる。

メールによる攻撃の最近の傾向では、オフィスソフトのデータファイルが添付される事例が増えている。攻撃添付ファイルにはマクロと呼ばれる自動操作手順が書き込まれており、オフィスソフトでファイルを開くとマクロが実行され、マルウェアをダウンロードして PC が感染する。初期設定ではマクロ実行は禁止あるいは利用者による許可が必要なのだが、無条件にマクロを実行する設定にしていないか確認して頂きたい。

さて、あなたは埼玉大学の教員だとしよう。知らない人物からメールが届いた。「○○先生へ。埼玉大学大学院に入学して、あなたの指導の下で研究して学位が取りたい。私の経歴と研究計画は添付ファイルに書いてある。」あなたは添付ファイルを開くだろうか。

コグニティブ無線でのスペクトラムセンシングのための くし形フィルタリング

島村　徹也

1　はじめに

第 5 世代の無線通信技術においては、枯渇する周波数資源の問題解決が重要視されている。その一つの解決方法に、コグニティブ無線がある。コグニティブ無線では、利用されていない周波数帯を有効利用するために、スペクトラムセンシングにより、周波数帯の活用状況を把握する。スペクトラムセンシングには、協調型スペクトラムセンシングと非協調型スペクトラムセンシングが考えられる。本稿では計算効率的な後者を主として取り上げることにする。

通信信号の検出を行うために、これまで受信信号の巡回定常特性を利用する方法、マッチドフィルタを利用する方法や、エネルギー検出の方法など、種々の方法が検討されてきている。しかしながら、いずれも信号対雑音比が低下するにつれて、検出精度が劣化してしまう。そこで、本稿では、本来付加雑音に耐性を有する自己相関関数を利用し、さらに受信信号にくし形フィルタリングを施すことで、信号対雑音比を改善しつつ通信信号の検出精度を向上させる方法について述べる。

2　無線通信信号

無線通信システムにおいては、マルチパスフェージング特性に耐性を有する通信方式が望まれ、現在では OFDM(Orthogonal Frequency Division Multiplex:直行周波数多重分割)が主流となっている。 OFDM は次世代方式としても有力視されていることから、本稿では OFDM 信号を対象信号と考えることにする。そして、OFDM の中でも特に、Cyclic Prefix(CP)を導入した CP-OFDM を取り上げることにする。CP-OFDM 信号は、図 1 に示されるように、OFDM シンボルの後ろ部分を複写し、そのシンボルの前部分に置くことで構成される。

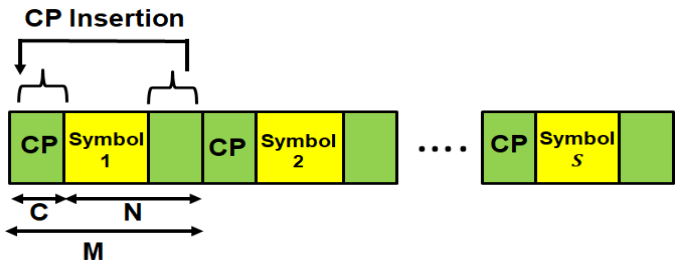


図 1　CP-OFDM 信号

3　システムモデル

図 2 は、本稿で取り上げるスペクトルラムセンシング方法のブロック図を示している。

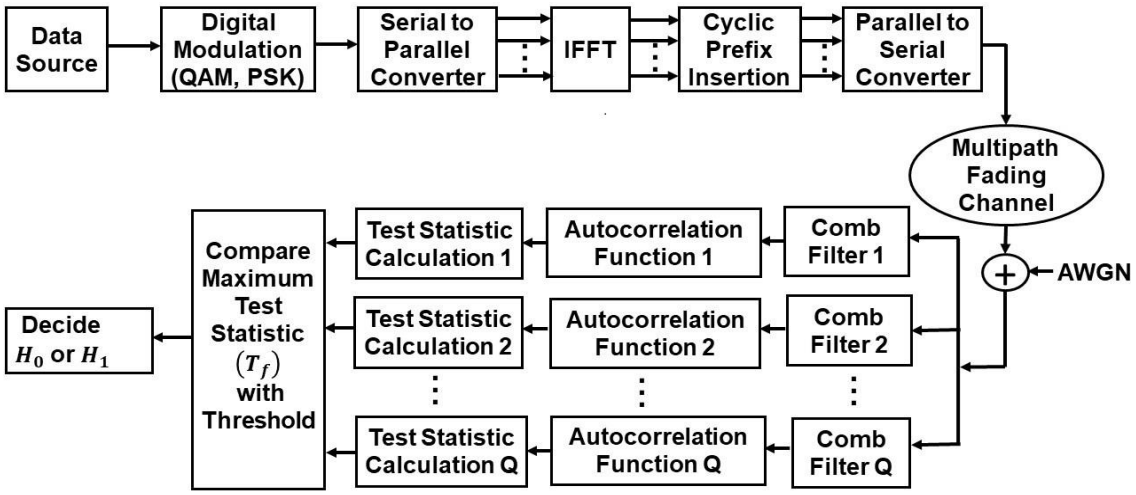


図 2　スペクトラムセンシングを実行するブロック図

送信側では、データソースが QAM または PSK 方式で変調されることを仮定する。シリアル･パラレル変換の後、IFFT(Inverse Fast Fourier Transform: 逆高速フーリエ変換)アルゴリズムによりマルチキャリア計算がなされる。ここで、CP が挿入される。そして、パラレル･シリアル変換により、CP-OFDM 信号が形成される。

通信路は、マルチパスフェージング通信路を仮定する。白色性の付加雑音も加わる。

スペクトラムセンシングは受信側で行われる。基本的には自己相関関数を計算し、OFDM シンボルの周期信号に着目し検出を行うが、くし形フィルタを前処理に利用することを考える。さらに、複数の並列構成を利用することで、統計的な意味において検出精度を向上させる。最終的には、対象信号が潜在する仮定H_1、あるいは対象信号が存在しない仮定H_0、が判定されることになる。

4　実験

ディジタル変調 16-QAM、FFT サイズ 1024、OFDM シンボル数 140、CP 長の OFDM シンボル長に対する比が 1/4、通信路はレイリーフェージング、受信側での並列処理数 3、反復回数 1500 において計算機シミュレーション実験を行った。

図 3 は、スペクトラムセンシングでの False Alarm のパラメータ設定を変化させたときの、検出確率を示したものである。False Alarm のパラメータが大きく設定されるにつれて、検出精度が改善されることがわかる。

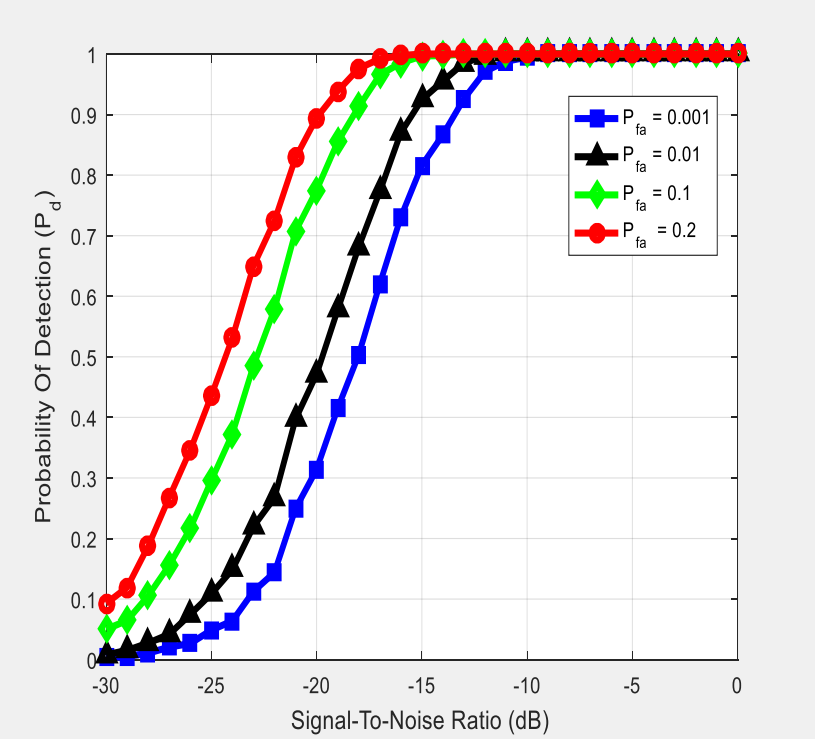


図 3　False Alarm のパラメータ設定依存性

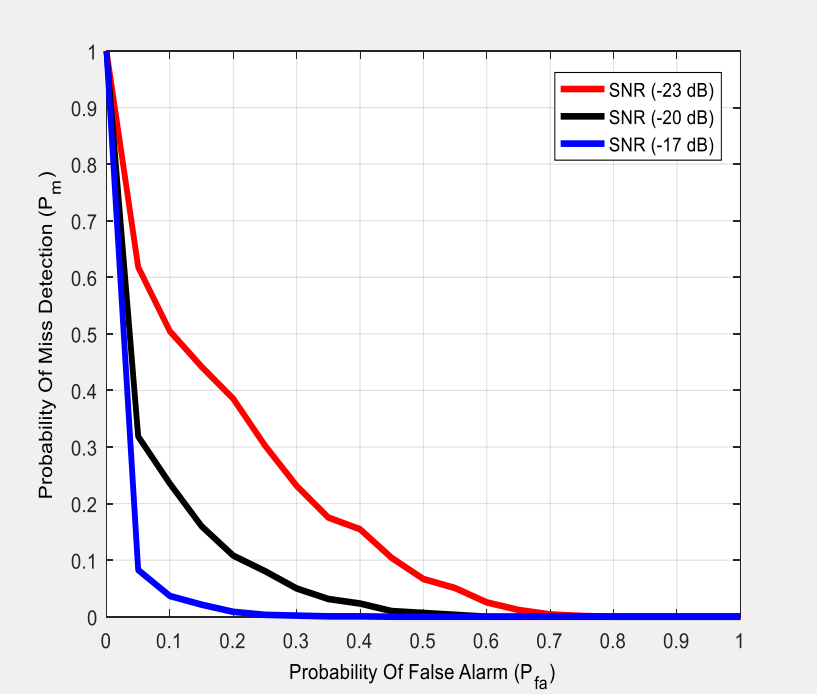


図 4　CROC 特性

図 4 は、CROC(Complementary Receiver Operating Characteristics: 補正受信処理特性)を表している。信号対雑音比が向上するにつれて、誤り検出の確率が低減していく様子が見て取れる。

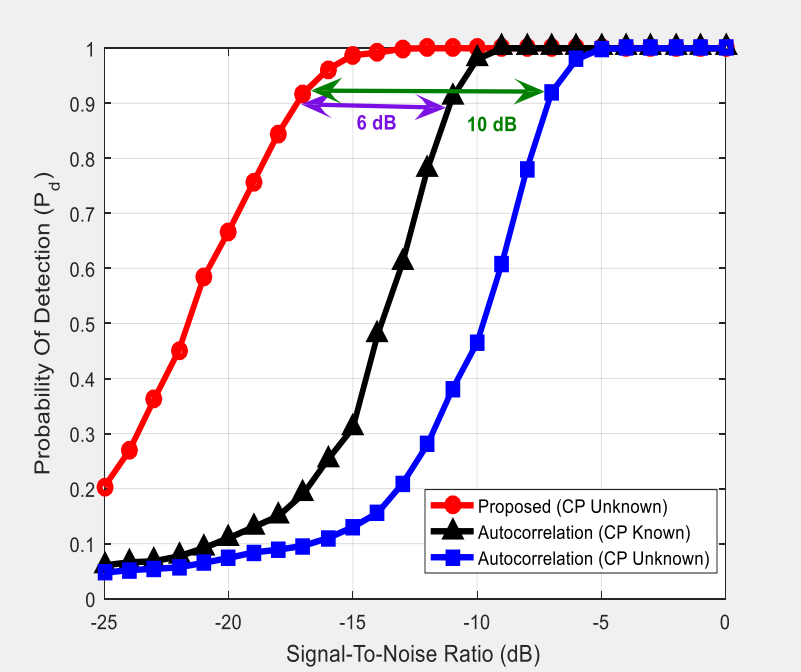


図 5　実行比較

図 5 は、False Alarm のパラメータを 0.05 に固定したときの検出確率を表している。本稿で述べている方法(Proposed)が従来法(Autocorrelation)と比較されている。従来法は、CP が既知の場合とそうでない場合をそれぞれ実行し、重ねて示している。図 5 より、本稿で記した方法は、従来法より信号対雑音比で 6dB から 10dB の改善を得ることができているのがわかる。

5　おわりに

本稿では、コグニティブ無線のためのスペクトルセンシングにおいて、効率的かつ効果的に高精度な検出結果を得ることができる方法を示している。OFDM 信号を対象信号として仮定し、CP 長が不明な場合においても、極めて低い信号対雑音比の場合まで、良好な検出結果を与える方法であることが、実験結果を介して示されている。受信側で複数の並列処理を用いるが、基本演算はくし形フィルタリングと自己相関関数計算のみであり、複雑な計算は要しない。しかしながら、従来法に比べ、信号対雑音比で 6dB から 10dB の改善を得ることができている。送信信号の情報を利用せず、必要な通信信号の検出ができる本法は、ブラインドな方法であり、今後の発展がさらに見込めると期待できる。

ビットコインにおける匿名化サービスの調査

吉浦　紀晃

1.　はじめに

メディア等ではビットコインは匿名性の高い通貨として紹介される事が多いが、実際にはビットコインそれ自体だけでは匿名性があるとは言い切れない。ビットコインではコインとその所有者との関係を直接知ることはできないが、調べる手段はある。また、店頭での支払のようにコインと所有者の関係が繋がってしまう場合ではむしろ多くの情報を与えてしまう通貨である。現金やクレジットカードで取引した場合、支払い相手は、支払った人がその前に、何を買ったかなどを知ることは無い、しかし、ビットコインでは、支払い元のビットコインアドレス(以後、アドレス)をたどることで、どこからコインを買い、どこにコインを支払ったかが推測できてしまう。これは、ビットコインが利用しているブロックチェーンを調べることで可能となる。ブロックチェーンは、公開されることでビットコインの取引の正当性を保証しているが、その一方で、ビットコインの流れが誰にでもたどることができる。

ビットコインの匿名性を高める手段(匿名化サービス)は既にあり、実際に利用されている。一方で、匿名性を高めることは、犯罪での利用に繋がる。特に、資金洗浄に利用されることが多い。ビットコインでは、匿名性と高めることと犯罪での利用がトレードオフの関係にあり、匿名性を必要に応じて無効にすることが必要となる。よって、匿名化サービスの仕組みを調べることは重要となる。

そこで、匿名化サービスの中で、CoinJoin を取り上げ、調査した結果について簡単に報告する。なお、この報告は、埼玉大学工学部情報システム工学科 2017 年度の臼井康人君の卒業論文「CoinJoin の匿名化の調査」の内容を要約したものである。

2.　ビットコインミキサ

CoinJoin はビットコインミキサの仕組みを利用するため、最初に、匿名化サービスであるコインミキサの説明を行う。ビットコインミキサではサービス提供者のアドレスにビットコインを一旦送金する。詳細は様々であるが、送金したコインはサービス提供者のアドレスに送金された他のユーザのコインと結合される。つまり、1 人の所有となる。このコインは各ユーザが指定した別のアドレスに再配布される。ブロックチェーン上には、サービス提供者に各ユーザのアドレスから送金した履歴が残り、サービス提供者から新たな各ユ

ーザのアドレスに送金された履歴も残るが、サービス提供者のアドレスからは他の多数のユーザのアドレスへも送金されている。そのため、サービス提供者へコインを送ったどのアドレスが再配布されたどのアドレスに関連しているかを推定することは難しい。つまり新たな各ユーザのアドレスにビットコインミキサを通して送金することで過去のアドレスとのつながりをブロックチェーン上からわかりにくくすることができる。

ビットコインミキサは実際にマネーロンダリングや闇取引に利用されていたが、ビットコインミキサの大手である bitmixer が 2017 年の 7 月をもって閉鎖した。また、ビットコインミキサは、一旦、サービス提供者にコインを送金することからサービス提供者がコインを窃盗するという、犯罪もあった。

ビットコインミキサの一部ではその匿名化に脆弱性があり、トランザクションを解析することでその匿名性を破ることができた。あるサービスではトランザクションに記録されているタイムスタンプから入金のタイミングと出金のタイミングの関係性を特定し、サービス提供者へ送金したアドレスとサービス提供者から再配布されたアドレスを見抜くことができた。

3. CoinJoin

CoinJoin はビットコインミキサの次に提唱された P2P ミキサと言われているミキシング技術の 1 つである。ビットコインミキサとの大きな違いはトランザクションの段階でミキシングを行なう事である。また、サービス提供者のような中央管理者がいなくても実行可能であることも特徴の一つである。

ビットコインの 1 つのトランザクションには複数の入力と出力を指定できる。そのため、本来、トランザクションは 1 人の取引によって生成されるが、1 つのトランザクションに複数人の入力と出力をまとめることで、複数人のトランザクションを 1 つにまとめた 1 つのトランザクションを生成することができる。このように複数人の取引で構成されたトランザクションで行うミキシングを CoinJoin と呼ぶ。

具体的には次のような手順で行われる。

1. 参加者は決められたコインの値を持つ出力を作ることに合意する。
2. 参加者は決められたコインの値を持つ出力と、必要があれば、釣りの出力を持つように通常通りトランザクションを作る。
3. 以上を、1 つのトランザクションにまとめることで複数人の取引をまとめたトランザクションを作る。

こうして形成されたトランザクションは、ブロックチェーン上のトランザクションには入力と出力のアドレスが残るが、少なくとも決められた値を持つ出力アドレスは、入力ア

ドレスのどのアドレスから出力されたかを見抜くことができない。なお、おつりの出力は入力の値から一定の出力値を引くことで推測できる場合がある。

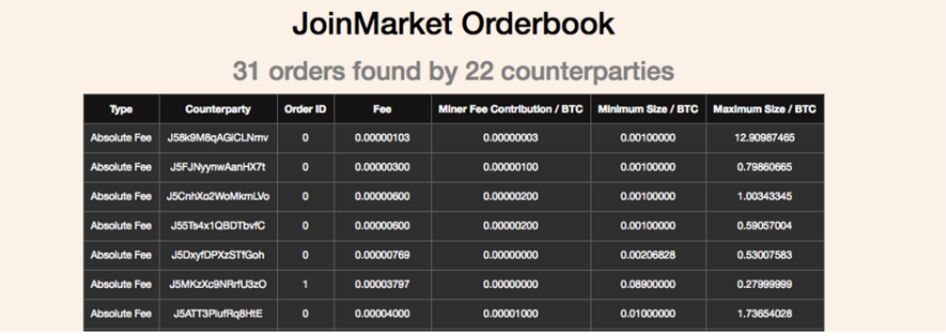
このトランザクションの構成は 1 人のユーザが複数の入力から複数のアドレスへ出力するトランザクションと変わらないので、出力の値など除けば見た目上では他のトランザクションと区別をすることは出来ない。また、CoinJoin を行う前に入力されるコインの量を調整することで、決められた値を持たないが入出力の値からトランザクション前後のアドレスの関係性を特定できない CoinJoin トランザクションを作ることが可能である。

CoinJoin では混ぜた人数と匿名性が直結している。よって、匿名性を高めるのにはより多くのユーザとミキシングを行う必要がある。しかし、1 回の CoinJoin トランザクションで人数を集めることは難しい。ビットコインミキサでは、サービス提供者のアドレスに十分な人数のコインが集まるまで待つことができたが、CoinJoin ではトランザクションを生成するタイミングで人数が揃っているという制限がある。また、CoinJoin を少人数で行う場合、スパイが参加者に含まれると十分な匿名性を確保することができない。そのため CoinJoin によって匿名性を確保する場合は、1 回ではなく複数回の CoinJoin の実行が必要であると考えられる。CoinJoin を複数回行う場合、安定した人数を集める為に、マッチングサーバやコミュニティが必要である。

4. JoinMarket

JoinMarket は CoinJoin を行うコミュニティのひとつである。安定して CoinJoin を行うための人数を確保するために参加者に報酬を与えるシステムを導入している。

JoinMarket ではユーザは 2 つに分類される。CoinJoin による匿名化を提供することで CoinJoin を安定して行うためのメーカ、CoinJoin によって匿名化を享受するテイカに分かれる。メーカは、図 1 のような取引可能な最小量、最大量、取引の際の報酬などをまとめたオーダ表と呼ばれるものを発行する。テイカはオーダ表からメーカを選択して、マッチングされたユーザと CoinJoin トランザクションを作成する。



JoinMarket Orderbook

31 orders found by 22 counterparties

Type	Counterparty	Order ID	Fee	Miner Fee Contribution / BTC	Minimum Size / BTC	Maximum Size / BTC
Absolute Fee	J58k9M8qAGiCLNmv	0	0.00000103	0.00000003	0.00100000	12.90987465
Absolute Fee	J5FJNyynwAanHX7t	0	0.00000300	0.00000100	0.00100000	0.79860665
Absolute Fee	J5CnhXo2WoMkmLVo	0	0.00000600	0.00000200	0.00100000	1.00343345
Absolute Fee	J55Tb4x1QBDTbvfC	0	0.00000600	0.00000200	0.00100000	0.59057004
Absolute Fee	J5DxyfDPXzSTfGoh	0	0.00000769	0.00000000	0.00206828	0.53007583
Absolute Fee	J5MKzXc9NRrfU3zO	1	0.00003797	0.00000000	0.08900000	0.27999999
Absolute Fee	J5ATT3PiufRq8HtE	0	0.00004000	0.00001000	0.01000000	1.73654028

図 1

JoinMarket が生成する CoinJoin トランザクションでは、テイカは一定の値を設定しその値を持つ出力 1 つと、あればお釣り用の出力を 1 つ作る。 メーカはテイカが設定した出力の値と同じ値を持つ出力を 1 つと、テイカが設定した出力の値と入力の値が同じ値でない限り、必ず 1 つのお釣り用の出力を作る。図 2 のように、トランザクションの前後で全てのアドレスは必ず更新される。

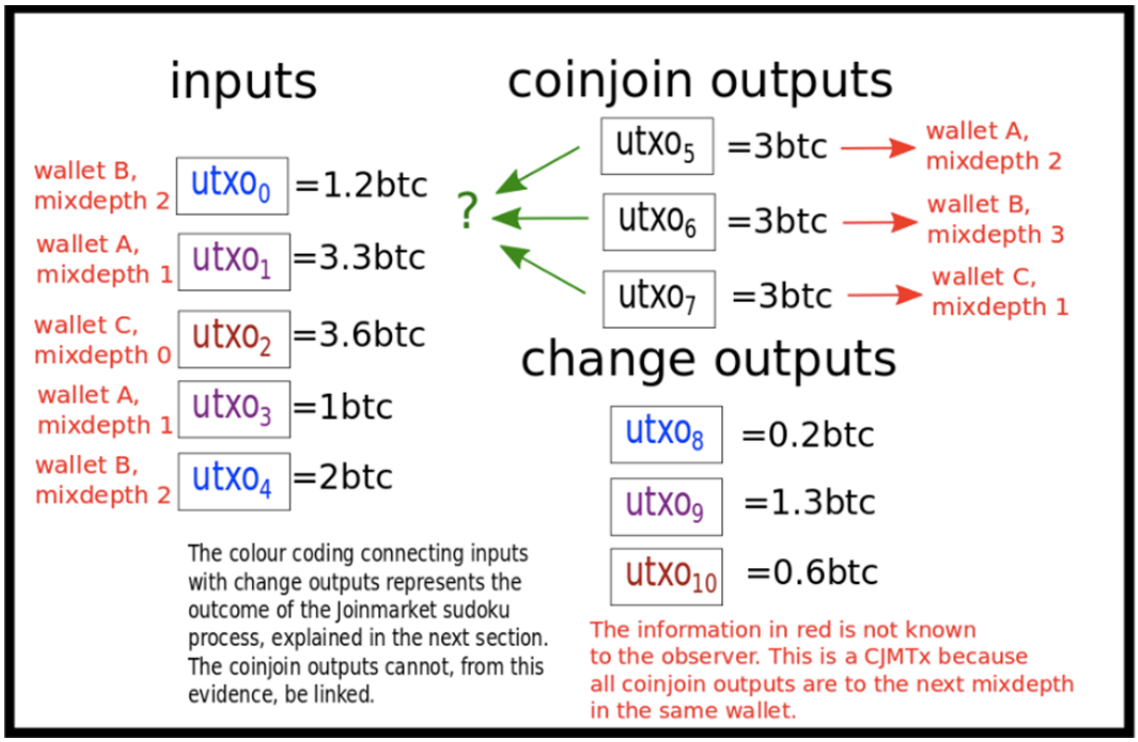


図 2

5. 調査

ブロックチェーンを分析し、JoinMarket において CoinJoin を行なっているトランザクションを調査する。具体的な調査方法は、次のとおりである。

1. CoinJoin のフォーマットに合っているトランザクションを抽出する。
2. トランザクション前後関係やアドレス情報からその精度を上げる。
3. 抽出されたトランザクションの中から JoinMarket で作られた CoinJoin トランザクションを選別しその妥当性を検証する。

まず、一度抽出を行う。具体的には、出力の値が JoinMarket で生成される CoinJoin トランザクションのフォーマットに則っているトランザクションを取りだす。コインを混ぜる以上、最低でもユーザは 2 人である。よって、最低、入力の数が 2 つ、同様に最低の出力が 2 つである。前述したように、JoinMarket の CoinJoin トランザクションはユーザの数だけ同じ値の出力をもつ。ユーザがおつり用の出力を各 1 つ持つとしても最低でも出力の半分が同じ値の出力を持つことになる。以上のことから抽出条件を

- 入力と出力の数が 2 以上である。
- 出力の半分以上が同じ値を持つ。

とする

この条件でトランザクションを抽出した結果、トランザクション数は 200 万件を超えた。この条件では多くの関係の無いトランザクションが含まれてしまった。この数のトランザクションを調べるのは難しいので、さらに、条件を加えて絞り込む。

2 回目の抽出では、CoinJoin では複数回 CoinJoin を行わなくては安定した匿名性を確保できないことを利用する。これを利用すると、CoinJoin トランザクションの出力が、次の CoinJoin トランザクションの入力になっている可能性が高いと考えられる。最初に抽出されたトランザクションの中で、入力で参照しているトランザクションの 1/2 が、最初に抽出されたトランザクションであるトランザクションを抽出する。1/2 とした理由はテイカの入力は CoinJoin を行なっていない可能性があり、メーカ 1 人と混ぜる最低人数のトランザクションでの入力は、おおよそ 1/2 となると考えられるからである。しかし、入力の数は制限されていないためテイカが非常に多くの入力を持つ可能性もあり全てのトランザクションを検出できない可能性もある。

2 回目の抽出の結果、トランザクションは 20 万件程度となった。トランザクション全体の 0.2%程度にまで絞り込めたがトランザクションの出力であるアドレスを調べたところ、

- トランザクションの前後でアドレスが変更されていないトランザクション
- カジノや取引所など、所有者が知られているアドレスが入出力に含まれているトランザクション

など、明らかに CoinJoin ではないトランザクションが含まれていた。

抽出されたトランザクションを取り出しブロックチェーン情報を検索できるサイトを用いて、さらに選別を行う。選別する方法はトランザクションにユーザが知られているアドレスが用いられているかを調べる。具体的には、使われているアドレスがユーザとして周

知されているトランザクションや、アドレスが再利用されているトランザクションを除く。残ったトランザクションの情報から JoinMarket で生成されたトランザクションかを判別する。

調査の結果、CoinJoin を行なっているか判断できないトランザクションはまだ含まれているが、CoinJoin によって生成されたと推測されるトランザクションが取り出せた。

1 回目に抽出されたトランザクションは全体の 1 %程度であり特殊なトランザクションでなければこのように条件に合うようなトランザクションが連続することは考えにくい。そのため、匿名性を確保するため複数回 CoinJoin を行なっているトランザクションである可能性が高い。このトランザクションを起点に前後に繋がっているトランザクションをたどり、1 回目の条件に合うトランザクションをリストアップし、その中に JoinMarket によって生成された CoinJoin トランザクションがあればリストアップされたトランザクションが JoinMarket によって生成された CoinJoin トランザクションであると考えられる。

選別によりトランザクションの集合が、JoinMarket によって生成されたトランザクションかを検証するために、実際に JoinMarket によって生成されたわかっているサンプルのトランザクションがリスト内にあるかを調べる。この結果、リストアップしたトランザクションの集合の中にサンプルのトランザクションがあった。よって、リストアップされたトランザクションの集合は JoinMarket によって生成されたトランザクションの少なくとも一部であるといえるだろう。

6. 考察

今回抽出した結果から JoinMarket で生成された CoinJoin のトランザクションは連続して何度も CoinJoin を行う一連のツリー状になっていることがわかった。CoinJoin を行なっているコミュニティを利用できれば、そのコミュニティでスパイとして取り引きを行い、そのコミュニティ内で行われている CoinJoin の取り引きを芋づる式に取り出すことが可能だと考えられる。

今回の調査では、CoinJoin トランザクションとして出力の値が半分以上同じであるという条件で抽出したが、前述したとおり同じ値である必要はない。しかし、入力と出力の値に一定の制限があるため、ブロックチェーンから絞り込むことは可能であると考えられる。

また、今回抽出したトランザクションは出力先がそのまま CoinJoin のトランザクションとなっていたため、簡単にリストアップする事ができた。しかし、別のアドレスに送金するトランザクションを挟むことで今回のように簡単にリストアップすることは難しくなる。CoinJoin によって匿名化する場合、一度に大量の入出金するトランザクションを作るか複数回 CoinJoin を行わなくては充分な匿名性は確保出来ない。よって、怪しいトランザ

クションの出力アドレスを追跡し、再び怪しいトランザクションの入力として使われるかを検査すれば抽出することができると考えられる。また、JoinMarket のように一定の人間がメーカの役割を持って人数を確保しているコミュニティであればそのアドレスは必要以上の CoinJoin トランザクションを生成するためその精度も上がると考えられる。

トランザクションには多くの情報が含まれているのでブロックチェーンを解析することで CoinJoin トランザクションが抽出できたことは、CoinJoin を犯罪目的で利用する場合、犯罪者にとってはリスクになると考えられる。

7. おわりに

今回の実験結果から CoinJoin が持つトランザクションの情報を用いてブロックチェーン上から JoinMarket によって作られた CoinJoin によるトランザクションを抽出することが可能であった。さらに、そのトランザクションの前後関係を追跡することで、類似の方法で作られた CoinJoin トランザクションを抽出することも可能であることが分かった。また、今回検出した CoinJoin トランザクションはかなり限定されたものである。出力の値の制限やトランザクションの連続性を隠している CoinJoin トランザクションを抽出することが今後必要になる。

ヒューズの性能向上のためのシミュレーション ソフトウェアの適用　～その 1～

山納　康

1. まえがき

回路には、短絡事故などの過電流通電による機器の故障を防止するために保護素子が取り付けられる。保護素子の一種であるヒューズは、ヒューズ自身の可溶体と呼ばれる箇所が溶断して電流を遮断するものであり、古くから利用されている。近年においては、比較的高電圧で大容量の直流電力系統がデータセンターや大規模太陽光発電所、電気自動車内部の回路など多く利用されるようになっており、ヒューズも直流タイプのものが用いられている。直流は交流と異なり、電流零点が存在しないため、電流遮断が困難と言われている。直流ヒューズが事故電流を遮断する場合は、電路であり且つ可溶体でもあるヒューズエレメントが溶断して、アーク放電を発弧させ、電源電圧以上の電圧を発生させることで、電流を限流し遮断する。従って、電流遮断時のアーク電圧の大きさは重要であり、電源電圧より低いと十分に限流ができず、遮断性能が悪化し、最悪の場合遮断失敗となることがある。

アーク電圧を高めるには、ヒューズエレメントに複数の狭小部を直列に持たせて、事故電流が流れた時にこれら狭小部を一斉に溶断・発弧させる。これにより複数のアーク放電が直列に発生することで、アーク放電の極降下電圧が現れる箇所が増え、ヒューズ全体のアーク電圧を高くすることができる。しかし、比較的立ち上がりが遅くピーク値が低い電流の遮断においては、複数設けた狭小部の全てが溶断せずにアーク電圧が低くなることある。これは、ヒューズの可溶体であるヒューズエレメント内の伝熱や周囲への放熱のために、温度分布に偏りが生じて、直列にある狭小部が同時発弧しないためと考えられている。

この温度分布の偏りをなくすには、ヒューズエレメントに過電流が流れたとき、全ての狭小部の温度が均一になるように発熱と伝熱を考慮したエレメントの設計が必要となる。本論文では、ヒューズ内部の温度分布の様子を把握するためにシミュレーションソフトの適用を試みた。これにより遮断時直前のヒューズエレメントの温度分布を知ることができ、狭小部の抵抗値を適切にすることで電流遮断直前のヒューズエレメントの温度分布を制御できる。そして、溶断・発弧のタイミングを合わせることが可能となり、比較的立ち上がりが遅くピーク値が低い電流に対する遮断性能を向上できると考えられる。今回はヒューズエレメントの一部の狭小部の長さや形状を変えることで、発熱や伝熱を定量的に制御し、狭小部全体の温度分布を均一にしたヒューズエレメントを設計した。さらに、設計したヒューズエレメントを試作し、遮断試験を実施して本手法の有効性を確認した。

2. 実験試料・装置・方法

2.1 伝熱シミュレーションによる解析方法

熱分布を制御するヒューズの設計において、電流―伝熱の連成計算は非常に有用な手段である。そこで、本研究ではシミュレーションソフト COMSOL Multiphysics® (以下、COMSOL と称する)による電熱シミュレーションを利用した。COMSOL は、有限要素法による電流―伝熱の連成計算ができ、ヒューズエレメントの温度分布を調べることができる。シミュレーションでは、以下のように設定して行い、その結果に基づいてヒューズの設計を行った。

シミュレーションは、実際の寸法に合わせて作製したヒューズエレメント(図 1 参照)及びヒューズボックス(図 2 参照)のモデルを作製し、それに電流を流した際の発熱及び伝熱を計算するという方式で行った。

これらのシミュレーションモデルを構成する材料については、ヒューズエレメントは銅製であり、ヒューズボックスはアクリル製の容器と銅端子、消弧砂(SiO_2)、アーク観察用のガラス板からなる。これらの材料の物性値はシミュレーションにおいても忠実に設定した。しかし、ヒューズボックスによる遮断試験において、アーク観察用のガラス板の有無は遮断特性にあまり影響しないことが著者らの研究で示されており [1]、シミュレーションの簡単化のために省略している。物性値は消弧砂以外はシミュレーションソフトに設定されているものをそのまま使用している。消弧砂の物性値は Adrian Plesca 氏による速断ヒューズの 3D 熱解 [2]で用いられた物性値をもとに決定した。砂は SiO_2 と空気の多孔質媒体で模擬し、SiO_2 の体積分率を 0.9 とした。表 1 に使用した材料の計算上用いた物性値を示す。

表 1　シミュレーションに用いた物性値

物質	熱伝導率 [W/(m・K)]	比熱容量 [J/kg・K]	密度 [kg/m^3]	参照抵抗率 [Ω･m]	抵抗温度計数 [1/K]
PMMA（ヒューズボックス器）	0.19	1420	1190	―	―
純銅（エレメント，端子部）	400	385	8960	1.72×10^{-8}	0.0039
SiO_2（消弧砂）	0.2	460	1100	―	―

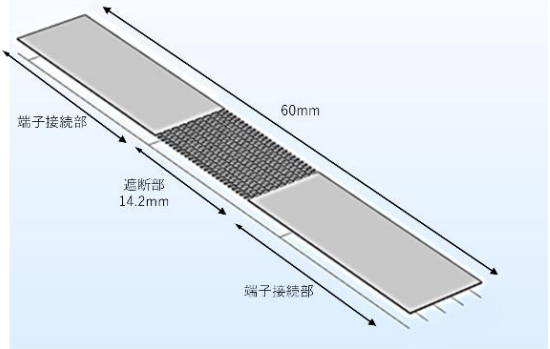


図 1　ヒューズエレメントモデル例

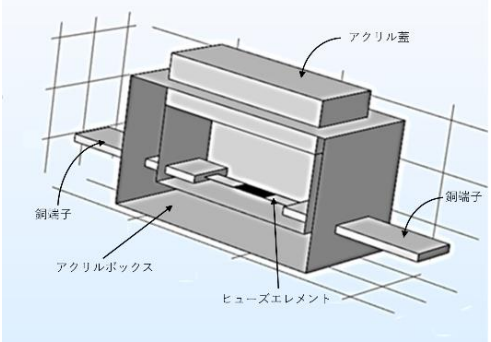


図 2　ヒューズボックスモデル例

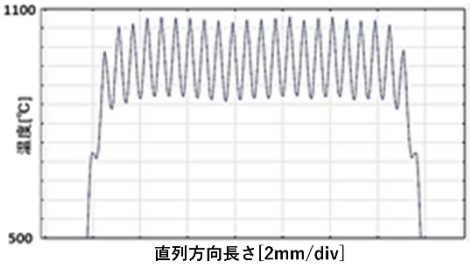


図 3　温度分布グラフ例

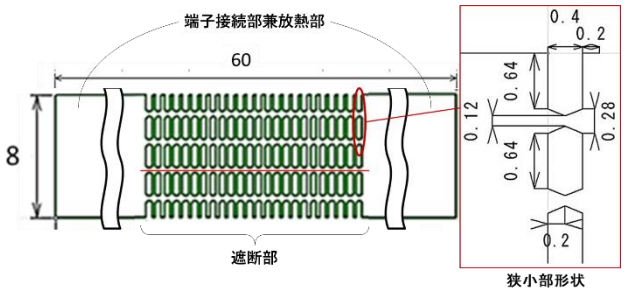


図 4　I 型エレメントの形状

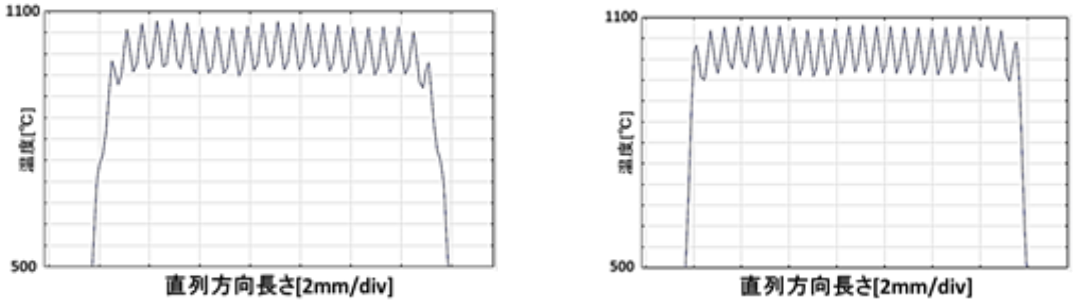
計算結果の表示方法については、エレメントの温度が銅の融点(1085 ℃)に達した時点の温度分布を、図 3 のような温度分布で評価し、これに基づいて設計を行った。温度分布は縦軸が温度で、横軸は狭小部の中心を通る線分上の場所を表している。また、温度グラフにおいて温度が高く上がっている「山」の部分が狭小部の最高温度である。

2.2 実験試料

本研究では、計算による狭小部の温度分布が均一になるよう設計したエレメントと比較対象として従来通りに全ての狭小部の形状や寸法が等しいエレメントを設計した。本論文中では、従来通りのものを CS タイプ、狭小部の温度分布を均一にしたものを OPT タイプと称する。ヒューズエレメントの主な仕様としては、狭小部の直列数は 24 個(24S と記す)とし、並列数は 4 個(4P と記す)で、エレメントの厚さは 100 μm 、エレメントの抵抗値は 2.4 ±0.05 mΩ とした。

エレメントの形状を図 4 に示す。温度分布の調整は狭小部の長さを変えることで抵抗値を変化させ、発熱と伝熱を繰り返し計算して調整をした。温度分布を調整する方法としては最端の狭小部の形状を変えることで発熱・伝熱を調節している。COMSOL によるシミュレーションによって、それぞれのエレメントに特定の電流を流した時の、狭小部の温度が融点(1085 ℃)に達した時点での温度分布を図 5 に示す。

以上の温度分布より、従来の形状(CS タイプ)では端側の狭小部の温度が中央付近の狭小部と比べて大きく下がっているのがわかる。これは、図 4 のヒューズエレメントの構造から分かるように、エレメントの両端部に広い端子接続部が存在しており、ヒューズエレメントの狭小部の端付近で発生する熱が端子接続部に伝わるためである。そこで、OPT タイプではヒューズエレメントの端の狭小部の長さや形状を変えることで、発熱量を増やし、さらに伝熱させにくくすることで、端の温度の低下を防ぎ、温度分布を均一に近づけている。



(a) CS タイプ　　(b) OPT タイプ

図 5　ヒューズエレメントの温度分布

2.3 遮断試験装置・方法

図 6 に示すようなアクリル製の透明なヒューズボックス内にヒューズエレメントを設置し、内部を消弧砂で充填した。また、ヒューズボックス底面にはガラス板が敷かれており、下からエレメントを撮影することができ、アーク発生時の発光の様子も確認することができる。実際のヒューズに近い状態に保つために油圧ポンプによりヒューズボックスの蓋を 3.0 MPa で加圧する。遮断試験は図 7 に示す遮断試験回路を用いて行った。合成コンデンサ C_0(合成容量 0.44 F)を 300 V に充電し、投入器を動作させて試験ヒューズに電流を通電する。試験時の電流は、固有電流が 1,045 A で通電から電流のピークまでの時間が 5 ms の電流が流れるように設定した。試験時はヒューズ間の電圧と電流をオシロスコープで測定した。電圧電流波形データからパソコンでヒューズの遮断の諸特性の解析を行った。

遮断試験時のアーク観察の条件を表 2 に示す。フレームレートは 73000 fps で、13.7 μs ごとに撮影している。シャッタースピードは 1.52 μs である。ND フィルタとレンズの絞りによりアークによる発光を減光している。解像度は 128×32 である。

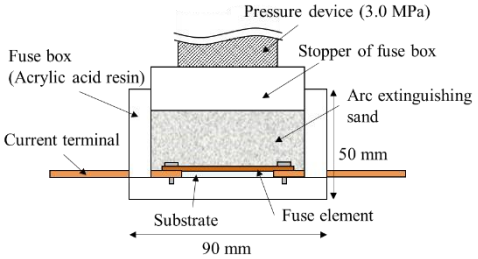


図 6　ヒューズボックスの断面図

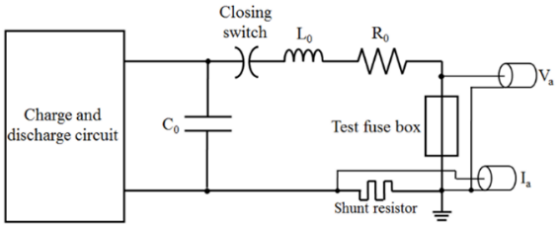


図 7　遮断試験回路図

表 2　アーク観察の条件

Flame rate [fps]	Shutter speed [s]	F 値	ND フィルタ
73000	1/657000	4	ND4 × 1

3. 試験結果および検討・考察

3.1 遮断性能の比較

遮断性能の比較は、遮断時の電流電圧波形および波形から得られた諸特性値で行った。波形の例として、電流電圧波形を図 8 に示す。図中の発弧開始時は、アーク電圧の立ち上がりから決定した。また、遮断波形から得られた諸特性の比較を表 3 にまとめる。

動作過電圧は発生したアーク電圧の最大値、dV/dt はアーク電圧の立ち上がりの速さであり、値が大きい方が限流作用によく働く。アーク I^2t 値はアークの発生から遮断完了までの間にヒューズを通過したエネルギーを表し、少ないほど遮断性能が良いことを示す指標となる。基本的にはアーク I^2t 値での比較が望ましいが、データの取得において、急変する電流の値を正確に捉えられない場合があるため、3 つの値で総合的に判断を行う。

表 3 の遮断特性の比較により CS タイプよりも OPT タイプの方が遮断性能が高くなった。これは、シミュレーションによるヒューズエレメントの設計通り、温度分布を制御することで従来の形状では溶断しにくかった端が溶断し、その分アーク電圧が高く発生したことによると考えられる。今回のエレメントではないが、同じように COMSOL により温度分布を制御したエレメントに対して遮断試験を実施したときのアーク画像を図 9 に示す。比較すると、同じ時間において OPT タイプの方がアークが大きく、より多くの狭小部が溶断し、発弧していることがわかる。

一方、別のヒューズエレメントではあるが電流立ち上がりが極端に早い条件において CS タイプよりも OPT タイプの遮断性能が劣る結果となった。OPT タイプは端でしかアークが発弧しておらず、このため遮断性能が低くなった。これは、エレメントの温度分布を均一に計算した電流条件と比べて立ち上がり速度やピーク値が異なり、di/dt でみると計算条件の 20 倍以上の速さで電流が流れたため、溶断時間が短くなった結果、考慮していた端への熱伝導が起こらず、比較的抵抗値が高い端の狭小部の温度が大きく上昇したためと考えられる。

以上の結果から、ヒューズエレメントの温度分布を制御することで遮断性能が向上できたことから、ヒューズエレメントの伝熱計算による設計は遮断性能の向上に効果を発揮できることを明らかにした。さらに別の実験では、計算条件以外の広い範囲の電流条件に対しても遮断性能を向上できている。しかし一方では、極端に電流の立ち上がりが早い条件では特性が CS タイプより劣ることもあり、全ての電流条件で向上させることは難しいと考えられる。

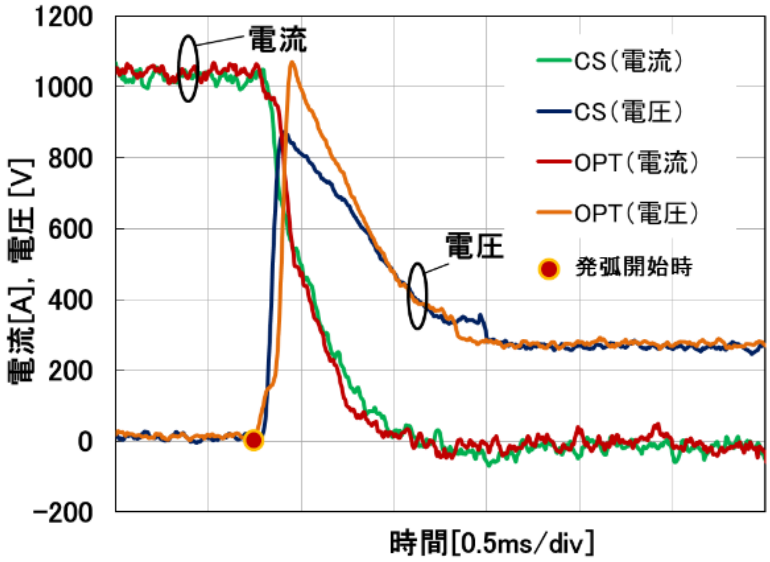


図 8　Ⅰ型エレメントの遮断波形比較(条件 2)

表 3　遮断特性の比較

タイプ	動作過電圧 [V]	dV/dt [V/□s]	アーク I^2t 値 [A^2s]
CS	885	10.5	118
OPT	1095	11.2	90

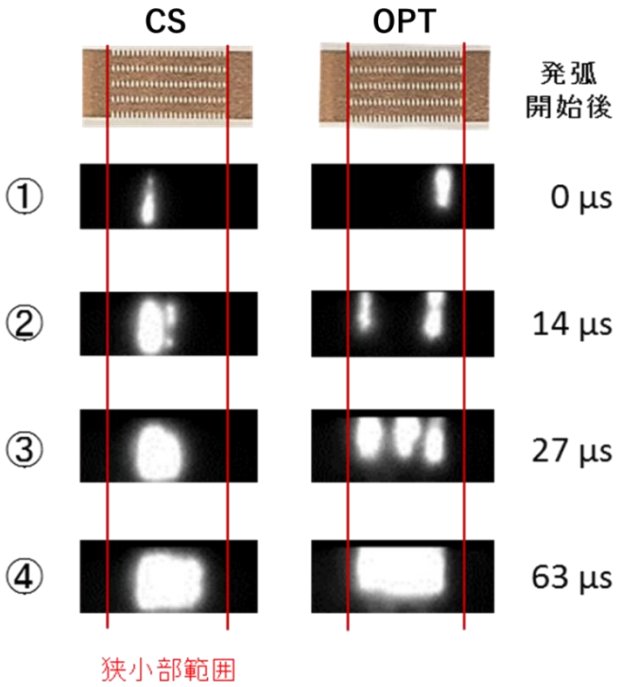


図 9　Ⅱ型のアーク画像(条件 2)

4. まとめ・今後の展望

本論文では、電流遮断時のヒューズエレメントの温度分布を、電流と伝熱の連成計算を用いて、ヒューズエレメント狭小部の温度を定量的に制御することで、遮断性能を従来のものより向上させることを試みた。得られた結果を以下にまとめる。

(1) ヒューズエレメントの端子側への伝熱が強く温度が下がりやすいエレメント端側の狭小部の発熱量を増やし、伝熱をさせにくくすることで、通常では溶断しにくい狭小部が溶断・発弧するようになり、遮断性能を向上させることに成功した。

(2) 温度分布の制御による遮断性能の向上は、計算条件以外の広い範囲の電流においても遮断性能を向上できたが、極端に異なる電流条件において遮断性能が悪くなる場合も存在した。

今回の結果から、狭小部の形状のみを変えて制御しても、全ての電流条件で従来以上の遮断性能を発揮するエレメントを作製することは難しいが、狭小部以外の放熱部と呼ばれる部分の幅や長さや厚みを変えて、さらに多角的な点で伝熱を操作することで、より広い電流条件に対応できるヒューズエレメントを作製することが可能であると期待できる。また、今回の試験結果と電熱計算結果の相関性は十分にみられ、エッチドヒューズのような微細な構造のエレメントの設計における電熱計算の利用は十分に有用であると言える。

参考文献

1) 石川 夕貴 他：ヒューズリンク内部のアーク観測とアーク電圧特性の調査，電気学会研究会資料放電・開閉保護・高電圧合同研究会, ED-15-135 SP-15-059 HV-15-101, pp. 29-34 (2015).

2) Adrian Plesca: Dependence of current interruption performance on the element patterns of etched fuses, *8th International Conference on Electric Fuses and their Applications*, pp.79-85 (2007).

3D-Modeling for the Developments of Polyhedra [1]

Takashi Horiyama

A development of a polyhedron is a simple polygon obtained by cutting edges or faces of the polyhedron and unfolding it into a plane. While we can realize a development by a paper (i.e., we can draw it on a paper), we may have troubles when we fold it into a polyhedron. Since it has no thickness, the folded polyhedron is fragile. More precisely, the hinge is flexible enough to be bend with at most 180 degrees, and thus we cannot fix the dihedral angles between adjacent faces.

To avoid such trouble, we use the technique of rigid-foldable thick origami [1]. By this technique, as shown in Figure 1, zero-thickness ideal facets (denoted by red lines) are realized by thick panels: First offset the ideal facets by constant distance in two directions, and then trim facets by the bisecting planes of dihedral angles between adjacent facets. Figure 1(a) and (b), respectively, illustrate the flat and folded states.

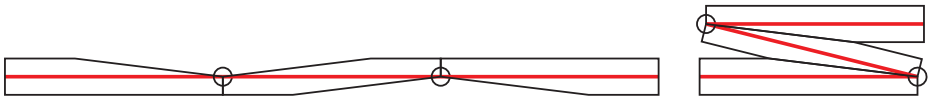


Figure 1: Thick panel origami [1].

If we trim the facets in the same side, all facets are folded in that side. If two polyhedra have a common development of the same shape (see e.g., [2], [3]), we can realize it so that it can be folded into the two polyhedra: We prepare hinges on the place where at least one polyhedron has a folding line. One side of the hinges is trimmed if they correspond to a polyhedron, and the other side is trimmed if they correspond to another polyhedron.

References

[1] T. Tachi, Rigid-Foldable Thick Origami, Origami 5 (Fifth International Meeting of Origami Science, Mathematics, and Education), pp. 253-263, 2011.

[2] Y. Araki, T. Horiyama, R. Uehara, Common Unfolding of Regular Tetrahedron and JZ Solid, Journal of Graph Algorithms and Applications, vol. 20, no. 1, pp. 101-114, 2016.

[3] T. Biedl, T. Chan, E. Demaine, M. Demaine, A. Lubiw, J. I. Munro, and J. Shallit, Notes from the University of Waterloo Algorithmic Problem Session, September 8, 1999.

[1] This article is a technical report without peer review.

小型コンピュータと移動ロボットを活用したネットワーク監視手法

小川　康一、吉浦　紀晃

1. はじめに

大学のネットワークは、企業に比べて自由に利用できる環境にある。そのため、利用者はネットワーク機器を用意し、自身の判断でネットワークに接続している。このような環境では、利用者の不注意によりネットワーク障害を頻発させていることが多い。利用者が使用するネットワーク機器は管理機能が乏しく、SNMP(Simple Network Management Protocol)などの監視プロトコルが利用できないため、Nagios や Cacti といった通常のネットワーク監視システムは利用できない。また、利用者は IT に必ずしも詳しくないため、ネットワーク管理者が障害の発生した部屋に出向き、障害の解決を余儀なくされている。この課題に対し、ネットワーク管理者が障害対応時に行う「目視」による切り分け作業に着目した。Web カメラと小型コンピュータの Raspberry Pi を用い、画像処理により LED インジケータ(以下、LED)を認識する監視装置を開発している [1)]。しかし、この方法では、監視装置ごとに 3G/LTE の移動体通信回線(以下、移動体通信回線)が必要で、監視対象が多い場合はコストが高くなる。そこで、本研究では、移動ロボットを利用した監視情報を収集する手法を着想するに至った。

2. 本研究の目的

我々は、先行研究 [1)]で、Web カメラと Raspberry Pi により監視装置を開発している。監視装置の Web カメラにより監視対象のネットワーク機器の LED の点滅状態を取得する。このことにより定常的な監視を実現している。本手法はネットワーク管理者が障害解決時に行う「目視」にヒントを得たものである。

本手法には、静止画と動画を用いた場合があるが、簡単のため静止画の方法を説明する。静止画の方法では、機器の LED の状態を画像で比較する。カメラで LED の情報を収集する。これを画像処理により切り出し、2 値化処理を行う。そのため現状では、色の状態変化には対応できない。白くまとまった範囲をブロブという単位で識別する。正しい状態と異常時の状態でブロブの状態が異なるので、この情報を利用してネットワーク機器の状態変化を認識する。メディアコンバータの例を図 1 に示す。

図 1.　LED の点灯位置による状態認識の例

この場合、LED の状態を撮影するカメラはそのままネットワーク機器に取り付けるとズレが生じて正しく認識ができない。このため、ネットワーク機器に取り付け可能なアタッチメントを開発している(図 2)。

図 2. 監視装置のアタッチメントの装着例

本提案手法をもとに実装したシステムは、埼玉大学で利用しているメディアコンバータを監視対象として実験を行い、移動体通信回線を利用して情報収集できることを確認した。監視装置は小型化のため Raspberry Pi を採用している(図 3)。

図 3. メディアコンバータ監視システムの設置例

ネットワーク障害時には監視対象のネットワーク機器が管理するネットワークは利用できない。そのため、本手法では、移動体通信回線を利用している。しかし、多数の監視装置が必要となる場合には移動体通信回線をその分用意するため、莫大なコストがかかる。また、セキュリティを考慮した場合、内部ネットワークに閉じた監視システムを構成できないという問題点があった。

3. 提案手法

本研究では、先行研究における問題点の解決策のひとつとして、移動ロボットによる監視情報の収集を提案する。今回、家庭用のお掃除ロボットであるルンバをベースとした移動ロボ

ット(図 4)を開発した。この移動ロボットは、著者が携わったクラウドロボットサービスの先行研究 [2]において開発したものをベースに発展させ、独自の改良を加えたものである。

図 4. 情報収集を行う移動ロボット

提案手法の概略を図 5 に示す。あらかじめ、移動ロボットと監視装置間で無線 LAN によるアドホックネットワークを形成する。情報収集は、監視装置が設置されている部屋の近傍の廊下を移動ロボットが走行することにより実現する。

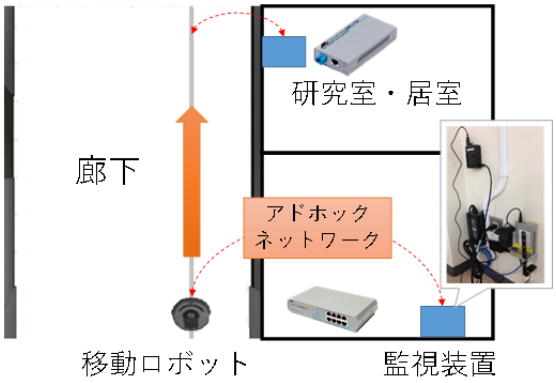


図 5.　移動ロボットによる情報収集の概要

ここで、移動ロボットを利用した監視システムの全体像について図 6 に示す。

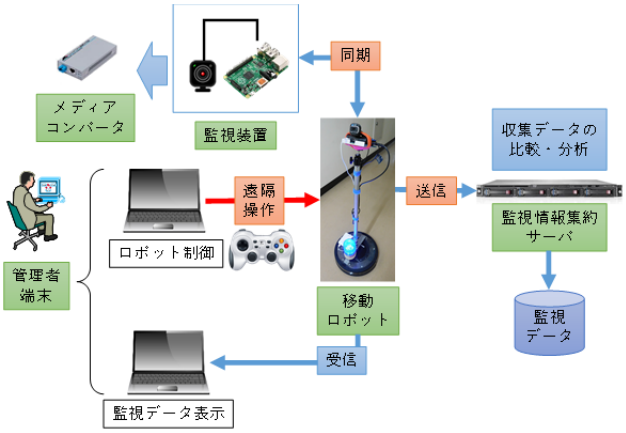


図 6.　移動ロボットを用いた監視システムの概要

本システムは、監視装置、移動ロボット、監視情報集約サーバ(以下、サーバ)、管理者端末(監視データ表示、ロボット制御の 2 台)で構成する。監視対象のネットワーク装置ごとに監視装置を設置する。監視装置は無線インターフェースを持ち、移動ロボットとアドホック接続を可能とする。移動ロボットは移動体通信回線で通信を可能とする。移動ロボットの移動制御プログラムは管理者端末のうちロボット制御を担当する端末で稼働する。

本システムは、監視装置設置箇所の近傍を通信機能のある移動ロボットが巡回する。監視装置が取得したデータは、移動ロボットが近傍に訪れる際にデータを移動ロボット経由でサーバに転送する。サーバに監視装置からのデータを集める。ネットワーク管理者は、サーバから最新の監視状況を管理者端末のブラウザで受信するとともに、必要に応じてサーバに蓄積された監視情報を閲覧できる。

移動ロボットを遠隔操作させる際、ネットワーク管理者が操作管理画面で移動ロボットに装着した Web カメラの映像を頼りに操作する。監視装置から取得した情報はサーバから WebSocket を利用して管理者画面にリアルタイムに表示できるようにしている(図 7)。

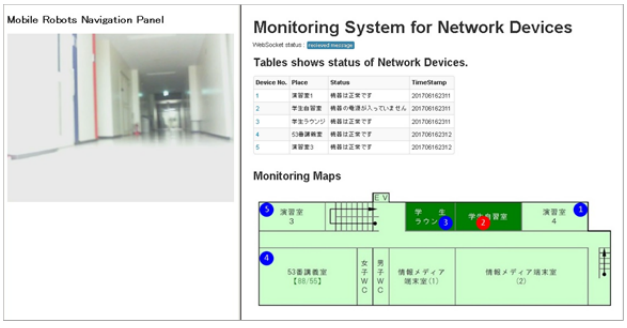


図 7.　管理者の画面表示

収集した監視情報は、サーバのデータベースに蓄積する。これにより、時系列でデータを確認できるため、利用者の利用実態から障害が発生するタイミングを予測するなど原因

追跡が可能となる。

4.発展

本研究では、前章の監視システムを基本とし、その発展として以下 2 つの追加機能の実装と、埼玉大学構内で実験を行った。

(1)SLAM を利用した自動走行による監視情報の収集 [4)]

前述の監視システムでは、管理者の遠隔操作を行う前提である。遠隔操作を実施するためには、監視装置周辺情報の知識や移動ロボットの操作経験が必要となるなど、管理者への負担が大きい。そこで、移動ロボットにレーザ測距センサー(図 8 左)を搭載し、環境地図(図 8 右)をあらかじめ作成することにより自動での情報収集を実現した。環境地図の作成と移動ロボットの自己位置推定には SLAM(Simultaneous Localization and Mapping)を利用した。

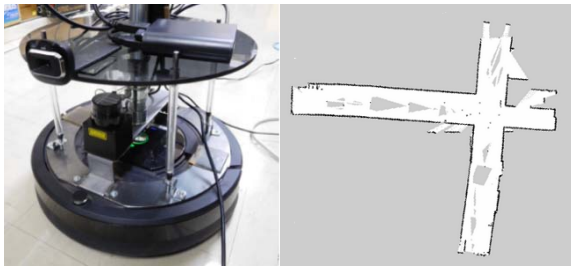


図 8.　レーザ測距センサーと環境地図

本手法では、作成した環境地図の座標をとり、手動でポイントを定義し、このポイントを巡回するウェイポイントと呼ばれる方法を採用している。この手法を採用することにより監視情報の自動収集を実現した。

(2)RSSI 値を利用した移動ロボット制御による通信の最適位置の探索 [5)]

(1)の方法により監視情報の自動収集を実現できた。しかし、データ量や条件によっては時間内に通信が完了しないことがあった。予備実験を行ったところ、移動ロボットが監視装置と通信する場合、必ずしも通信が良好であるとは限らないことがわかった。そこで、移動ロボットと監視装置間の無線の受信電波強度を示す RSSI(Received Signal Strength Indicator)に着目し、RSSI が高い箇所を移動ロボットが探索することによって、最適な通信を確保する手法を提案した。

探索は全探索が望ましいが、非効率的であるため、ウェイポイントの箇所から移動ロボットを前後左右にそれぞれ約 30cm に移動し、各地点での RSSI 値を計測し、一番高い値の地点で通信する方法をとった。実験により提案手法の有効性が確認できた。

5. おわりに

本研究では、移動ロボットを活用した新しいネットワーク機器監視手法を提案した。また、実験により、移動ロボットによる監視情報の収集が可能であることを明らかにした。実際、本研究の実用化には、移動ロボットの運用方法についての検討が必要である。現状 1 台の移動ロボットでは電源の問題があり、充電している間に監視情報の収集ができない問題がある。そこで、複数の移動ロボットを交互に走行させることを検討中である。また、移動ロボットにより監視可能な場所も限定されるため、本手法の情報収集手法はあくまでも解決方法の一つである。今後、あらゆる可能性を考慮し、他の方法による情報収集手法についても検討していきたい。

謝辞

本研究は、JSPS 科研費 17H00371 の助成を受けたものです。

参考文献

1) 小川康一，吉浦紀晃：小型コンピュータと画像処理技術を活用したネットワーク機器監視装置の開発，情報処理学会研究報告インターネットと運用技術(IOT), 2017-IOT-38(5), pp.1-7(2017).
2) 藤田正典，青柳一之，大橋修，落合瑛史，常盤嘉昭，加藤由花：仮想環境を用いた移動ロボット用遠隔操作システムの提案，情報処理学会研究報告マルチメディア通信と分散処理(DPS)，2014-DPS-158(15)，pp.1-6(2014).
3) 小川康一，吉浦紀晃：移動ロボットと小型コンピュータを活用したネットワーク機器監視手法，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム(DICOMO)，pp.1354-1361(2017).
4) 小川康一，吉浦紀晃：移動ロボットによる環境地図を用いたネットワーク機器監視情報の自動収集手法，情報処理学会研究報告インターネットと運用技術(IOT)，2017-IOT-39(1) ，pp.1-7(2017).
5) 小川康一，吉浦紀晃：利用者のネットワーク機器を監視する移動ロボットの自動情報収集のための通信制御手法，情報処理学会インターネットと運用技術シンポジウム(IOTS2017)，pp.1-10(2017).

※本論文は、第 40 回生理学技術研究会奨励研究採択課題技術シンポジウムで発表した内容に加筆修正したものです。