サポートベクターマシンによるスワイプデータからの個人認証手法の確立

阿部 僚馬*　黒岩 丈介**　小高 知宏**　諏訪 いずみ***　白井 治彦****

Support Vector Machines for Swipe Data Establishment of Personal Authentication Method

Ryoma ABE*,　Jousuke KUROIWA**, Tomohiro ODAKA**
Izumi SUWA*** and Haruhiko SHIRAI****

(Received September 30, 2022)

In recent years, smartphones have not only functioned as cell phones, but have also a variety of other functions, such as electronic payment and Internet banking. Then, they contain a lot of personal information. Android OS smartphones, which have a high market share worldwide, still use pattern lock authentication, but it is poor secure. Therefore, the purpose of this study is to investigate a more secure lock by exploiting the potential features of pattern locks during swiping with support vector machine. In computer experiment, we trained a support vector machine with personal features obtained from five subjects and evaluated the false reject rate and false accept rate. From the results, we have succeeded to provide a robust and practical authentication method based on the swiping actions with support vector machine.

Key words :*pattern lock authentication*, *a support vector machine*

1. はじめに

スマートフォンの普及は進み，老若男女関係なく，1人1台持つことが当たり前の時代となってきた．スマートフォンの高性能化により，電話番号や電話帳のデータだけでなく，銀行の口座番号，ID，パスワード，GPSなどによる位置情報が記憶されている．そのため，スマートフォンの紛失は個人情報の漏洩となりかねない．これを未然に防ぐために，パスコードや生体認証を用いた個人認証方法を用いてロックをかける．

モバイル端末のOSは現在，Google社が提供するAndroid OSとApple社が提供するiOSの2つが99％を占めている．その中でもAndroid OSのシェア率が最も高い．Android OSの端末にはパスワード，PIN，パターンロック，生体認証を用いたロック方法が搭載されている．パターンロック認証は3 x 3の目印点をスワイプする指の軌跡情報から本人を認証する手法であり，簡便ではあるが，認証動作を覗き見されることにより第3者でも容易に不正侵入することができてしまう．[1]

また，実験例として，ディスプレイに付着した油脂を撮影し，解読した結果，68%の精度でパターンの解読が可能であった報告もある．[2] さらに，覗き見による認証率は高く，1回の覗き見で解読可能な確率が64.2%，システムがオートロックされる5回までに解読可能な確率は95%という実験結果も挙げられる．[3]

*大学院工学研究科 知識社会基礎工学専攻
*Fundamental Engineering for Knowledge-Based Society, Graduate School of Engineering
**知能システム工学講座
**Department of Human and Artificial Intelligent Systems
***仁愛女子短期大学 生活科学学科
***Jin-ai Women's College
****工学部 技術部
****Technical Division

そのため，様々な個人情報を守る上でも，より強固かつ容易な操作で行える認証手法が求められている．パターンロック認証には，座標データ以外に，スワイプ操作の速度，ディスプレイに対する指の接触面積または圧力など情報も存在する．これらの情報は意識的にスワイプする座標データとは異なり，人が無意識的に発するデータと言える．本研究ではこのようなデータを無意識的特徴と呼ぶ．この無意識的特徴は身体的特徴に近く，模倣が困難であるため，覗き見に対する耐性があると考えられる． そこで先行研究では，スワイプ動作の指の位置情報だけでなく，時間情報や，指の移動速度及び指の接触面積などの情報を個人特徴として注目し，より強固なパターンロック認証手法を確立することを可能とした. [4]

まず，軌跡情報取得システムからユーザーのスワイプ動作の時系列データを取得する．取得したデータから x 軸方向及び y 軸方向の速度，指の接触面積及び時間データを算出し，個人特徴の抽出をした．その際，ノイズを除去するために単純移動平均法を施した．

個人認証実験では被験者 6 名に対して計測を行い，各被験者の特徴量を抽出して独立認証を行う．そして，被験者分類には標準化ユークリッド距離を用いた認証が一番精度が良く，FRR が 18.6% ，FAR が 1.6% だった. [5] しかし，スマートフォンに実用化することを考えたときに，FAR を 0% とすることが理想である．そのため，標準化ユークリッド距離を用いた手法では，実用化には不十分である．

そこで，本研究では分類精度の高いサポートベクターマシンを用いて，認証精度のさらなる向上を目指す.

2. サポートベクターマシン

サポートベクターマシンはニューロンのモデルとして最も単純な線形しきい素子を用いて，2 クラスののパターン識別器を構成する手法である.

2 クラスのパターン分類問題を考えるとき, 特徴ベクトルを $\boldsymbol{x}^T = (x_0, x_1, \cdots, x_d)^T$，パラメータを $\boldsymbol{w}^T = (w_0, w_1, \cdots, w_d)^T$, しきい値を h とすると，線形識別関数は

$$y = \text{sign}(\boldsymbol{w}^T\boldsymbol{x} - h) \tag{1}$$

と表現され，2 値の出力値を計算する．関数 sign(u) は $u > 1$ のとき 1 をとり，$u \leq 0$ のとき -1 をとる符号関数である．訓練サンプル集合が線形分離可能なら

$$t_i(\boldsymbol{w}^T\boldsymbol{x} - h) \geq 1, (i = 1, ..., N) \tag{2}$$

を満たすようなパラメータが存在する．これは 2 枚の超平面で訓練サンプルが分離されていることを表している．このとき，識別平面と超平面のマージンの大きさは $\frac{1}{||\boldsymbol{w}||}$ となる．サポートベクターマシンでは訓練サンプルをなるべく余裕を持って分けるような平面が求められる．そのため，マージンを最大とするパラメータ $\boldsymbol{w}$ と h を求める問題は，制約条件

$$t_i(\boldsymbol{w}^T\boldsymbol{x} - h) \geq 1, (i = 1, ..., N) \tag{3}$$

のもとで，目的関数

$$L(\boldsymbol{w}) = \frac{1}{2}||\boldsymbol{w}||^2 \tag{4}$$

を最小とするパラメータを求める問題と等価になる.

2.1 ソフトマージン

実際，パターン認識の分野において線形分離可能な場合は稀である．そのため，非線形のものを分離するには，多少の誤りを許容する必要がある．これはソフトマージンと呼ばれる．ソフトマージンでは，誤ったサンプルと境界平面の距離をパラメータ $\xi_i(\geq 0)$ を用いて $\frac{\xi_i}{||\boldsymbol{w}||}$ と表すと，その和は

$$\sum_{i=1}^{N} \frac{\xi_i}{||\boldsymbol{w}||} \tag{5}$$

なるべく小さいことが望ましい．これからの条件から，最適な識別面を求める問題は，制約条件

$$\xi_i(\geq 0), t_i(\boldsymbol{w}^T\boldsymbol{x} - h) \geq 1 - \xi_i, (i = 1, ..., N) \tag{6}$$

の下で，目的関数

$$L(\boldsymbol{w}, \boldsymbol{\xi}) = \frac{1}{2}||\boldsymbol{w}||^2 \tag{7}$$

を最小とするパラメータを求める問題に帰着する．パラメータ γ は第 1 項のマージンの大きさと第 2 項のはみ出しの程度とのバランスを決める定数である.

2.2 カーネルトリック

ソフトマージン法を用いることで，非線形の場合でも素子のパラメータを求めることができるようになった．しかし, これによって全ての非線形の複雑な問題に対して，良い性能の識別器を構成できるとは限らない．複雑な非線形の問題に対応する方法として，特徴ベクトルを非線形変換して，その空間で線形の識別を行う方法をカーネルトリックと呼ぶ.

今，元の特徴ベクトル $\boldsymbol{x}$ を非線形の写像 $\phi(\boldsymbol{x})$ によって変換し，その空間で線形識別を行うことを考え

てみる．例えば，写像 ϕ として，入力特徴を 2 次の多項式に変換する写像を用いるとすると，写像した先で線形識別を行うことは，元の空間で 2 次の識別関数を構成することに対応する．一般に，こうした非線形の写像によって変換した特徴空間の次元は非常に大きくなりがちであるが，サポートベクターマシンの場合には，目的関数や識別関数が入力パターンの内積のみに依存した形になっており，内積が計算できれば最適な識別関数を構成することが可能である．もし，非線形に写像した空間での二つの要素 $\phi(\boldsymbol{x}_1)^T$ と $\phi(\boldsymbol{x}_2)$ の内積が

$$\phi(\boldsymbol{x}_1)^T\phi(\boldsymbol{x}_2) = \boldsymbol{K}(\boldsymbol{x}_1, \boldsymbol{x}_2) \tag{8}$$

のように，入力特徴 $\boldsymbol{x}_1$ と $\boldsymbol{x}_2$ のみから計算できるなら，非線形写像によって変換された特徴空間での特徴 $\phi(\boldsymbol{x}_1)$ や $\phi(\boldsymbol{x}_2)$ を計算する代わりに，$\boldsymbol{K}(\boldsymbol{x}_1, \boldsymbol{x}_2)$ から最適な非線形写像を構成できる．

3. スワイプデータとその特徴

3.1 実験に用いる個人データ

本実験には先行研究で用いられたデータを用いる．右利きの男性 5 名の被験者（ user A, user B, user C, user D, user E ）に動作が安定するまで十分なスワイプ操作を行った後にデータの取得を行い，被験者全員が同様の室内環境，体調，姿勢でデータ取得を行った．実験経路を図 1 に示す．青が目印点を表し，赤色は経路を表す．経路は ABCDACBDCABD の順であり，「Z」→「∞」→「四角」の順にスワイプする．1 人あたり，1 つの経路に対して 20 回分データの取得を行う．

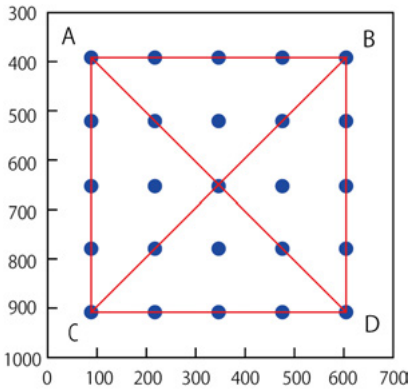

図 1 実験経路

3.2 ノイズ除去

取得した 20 回分のデータから x 軸速度，y 軸速度，接触面積のデータに分ける．取り出した x 軸速度，y 軸速度にはノイズが載っているため，平滑化を行うことでノイズを除去する．ノイズの除去には移動平均法を用いるが，移動平均法の計算には主に 3 種類存在し，単純移動平均法 (SMA)，加重移動平均法 (WMA)，指数移動平均法 (EMA) が挙げられる．先行研究より単純移動平均を用いた平滑化がほかの移動平均法よりも優れていることが分かっているため，今回の実験では単純移動平均法を用いた．ここで，単純移動平均法について説明する．は時系列データにおいてある時刻 k ステップ目を中心とし，その前後 n 個のデータの平均値を求め，その結果を k ステップ目の結果とする．すなわち $2n+1$ 個のデータの平均値が単純移動平均での結果となる．ここで単純移動平均法を以下の式で定義する．k ステップ目のデータを $A(k)$, k ステップ目の演算結果を $S(k)$ とする．ただし，データの先頭 n 個，末尾 n 個のデータに対してこの処理は行わない．この式を数回繰り返すことによってノイズを除去し，平滑化された波形を得る．

$$S(k) = \frac{1}{2n+1}\sum_{i=-n}^{n} A(k+i) \tag{9}$$

user A の x 軸速度のデータの一部を図 2 に示す．青色はスワイプデータから取得した元データを指し，橙色は青色の元データに対して平滑化した結果を表す．

3.3 特徴抽出

次に平滑化を行った x 軸速度，y 軸速度，接触面積から特徴量を抽出する．今回の実験では x 軸速度，y 軸速度に対しては極値，指の接触面積の変化に対し

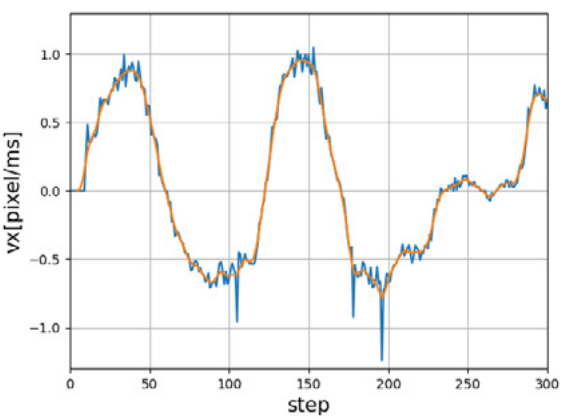

図 2 user A の平滑化後の x 方向速度

ては目印点通過時のデータを特徴量とする．速度の例として，AB 間のスワイプを考える．現在 A の座標（100，400），B の座標（600，400）である．A から B にスワイプする時，x 軸速度は正の方向に加速し，y 軸速度は変化しないため 0 であることが分かる．また，スワイプ開始点 A と目印点 B でともに速度は 0 になるため，速度の極大値が AB 間に存在していることが分かる．本実験ではこのような極値を速度の特徴点として抽出する．続いて接触面積の特徴量について説明する．図 1 から 1 回のスワイプで通過する目印点は 12 であることが分かる．また，x 軸速度，y 軸速度のデータと接触面積のデータの性質は異なり極値を取り出すことが困難なことが分かっている．そこで本実験では目印点を通過した瞬間のデータ値を取得する．

図 3 に user A の x 軸速度，図 4 に user A の 接触面積のデータを示す．どちらも赤点が抽出する特徴点の位置を表す．

4. サポートベクターマシンを用いた個人認証実験

4.1 実験方法

- 独立認証

  平滑化された x 軸速度，y 軸速度のデータからは特徴量を 7 点抽出し，接触面積のデータからは特徴量を 12 点抽出する．そして抽出した特徴量を用いて被験者ごとに x 軸速度，y 軸速度，接触面積の分類器を作成して分類を行う．

- 多数決認証

  そして，x 軸速度，y 軸速度，接触面積の独立認証の結果に対して多数決を取る．以下に多数決認証の定義式を示す．

表 1 既知 user 認証実験の user の組み合わせ

分類器	学習データ	テストデータ
A	A，B，C	A，B，C
B	B，C，D	B，C，D
C	C，D，E	C，D，E
D	D，E，A	D，E，A
E	E，A，B	E，A，B

表 2 未知 user 認証実験の user の組み合わせ

分類器	テストデータ
A	D，E
B	E，A
C	A，B
D	B，C
E	C，D

$$ANDi(S_i, X_i, Y_i) = \begin{cases} 1 & (Vote(S_i, X_i, Y_i) \geq 0.5) \\ 0 & (Vote(S_i, X_i, Y_i) < 0.5) \end{cases} \tag{10}$$

$ANDi$ は i 回目のスワイプの多数決認証の結果である．

多数決認証は，1 つの特徴で異常な結果を返した場合でも，正常な結果を返すことができ，独立認証よりも高精度な認証精度が得られることが期待できる．

今回の実験には 2 種類のテストデータを用いて，多数決認証実験を行っていく．既知 user 認証実験では，学習データとテストデータが同じ user である．これ

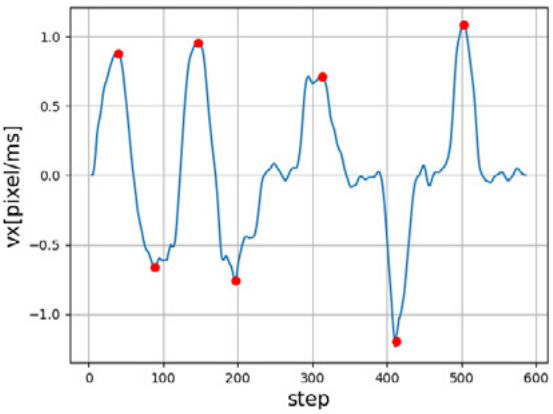

図 3 user A の x 軸速度の特徴点

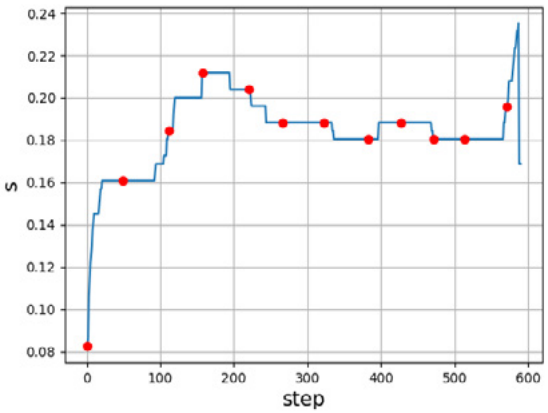

図 4 user A の接触面積の特徴点

表 3 既知 user 認証の結果

2*	x 軸速度		y 軸速度		接触面積		多数決認証	
	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)
user A	10	0	20	0	0	0	0	0
user B	60	0	40	5	0	5	30	0
user C	20	0	10	0	0	0	10	0
user D	10	5	0	5	10	0	0	0
user E	0	15	10	0	0	0	0	0
平均	20	4	16	2	2	1	8	0

表 4 未知 user 認証の結果

2*	x 軸速度	y 軸速度	接触面積	多数決認証
	FAR (%)	FAR (%)	FAR (%)	FAR (%)
user A	0	0	3	0
user B	0	0	0	0
user C	0	0	15	0
user D	20	20	50	28
user E	0	0	3	0
平均	4	4	14.2	5.6

は，先行研究と同じ実験方法である．そして，未知 user 認証実験では，学習データに用いていない user をテストデータに用いる．表 1 の user A の分類器を例に説明する．

1. A の奇数データを出力 1 で A と学習させる．
2. B, C の奇数データを出力 0 で A でないと学習させる．
3. A, B, C の偶数かつ窓数 n = 5 のデータをテストデータとして検証する．

4.2 既知 user 認証実験

学習データに, user 3 人の奇数番目を用い，テストデータには，学習データに用いた user の偶数番目のデータを用いて評価を行う．学習データとテストデータの user の組み合わせを表 1 に示す．表 1 の分類器の欄に記載されている人は，その人の分類器を作成して分類していくことを表している．

4.3 未知 user 認証実験

既知 user 認証実験と同様，学習データに，user 3 人の奇数番目を用い，テストデータには学習に用いていない user のデータを用いて評価を行う．学習データとテストデータの user の組み合わせを表 2 に示す.

4.4 評価方法

認証精度は, 本人拒否率 FRR (False Reject Rate) と他人拒否率 FAR (False Accept Rate) で評価を行う．

$$\mathrm{FRR} = \frac{\text{本人拒否回数}}{\text{試行回数}}, \mathrm{FAR} = \frac{\text{他人受け入れ回数}}{\text{試行回数}} \tag{11}$$

4.5 パラメータの決定

SVM のカーネルには rbf カーネルを用いる．ハイパーパラメータの C は 1 と固定し，γ は学習データの FRR と FAR が収束したときの値を用いて検証を行った．

$$\boldsymbol{K}(\boldsymbol{x}_1, \boldsymbol{x}_2) = \exp \frac{||\boldsymbol{x}_1 - \boldsymbol{x}_2||^2}{2\sigma^2} \tag{12}$$

4.6 実験結果

既知 user 認証実験の結果を表 3，未知 user 認証実験の結果を表 4 に示す.

表 3 を見ると，x 軸速度，y 軸速度に比べて，接触面積は本人拒否率と，他人受け入れ率の精度が高かった．x 軸速度，y 軸速度の本人拒否率はユーザー平均を取ると 20% と 16% と高いが，多数決認証をすることで，平均値が 8% と低く抑えられていることが分かる．また，各特徴量の他人受け入れ率が数%あっても多数決を取ることで 0% になった．そして，先行研究の標準化ユークリッド距離よりも高い精度を実現することができた．

表 4 を見ると，接触面積の他人受け入れ率が x 軸速度，y 軸速度と比較して，高いことが分かる．user ごとに見ると user B は各特徴量の他人受け入れ率が 0%となった．そして，多数決認証の結果では，user D 以外は 0%となり，平均を取ると，5.6%となった．

5. 考察

既知 user 認証実験の多数決認証の FAR が 0 %，未知 user 認証実験の FAR が 5.6%であったことから，学習データと未知のデータに似た特徴量を持つ user が存在すると考えられる．スマートフォンに実装するこ

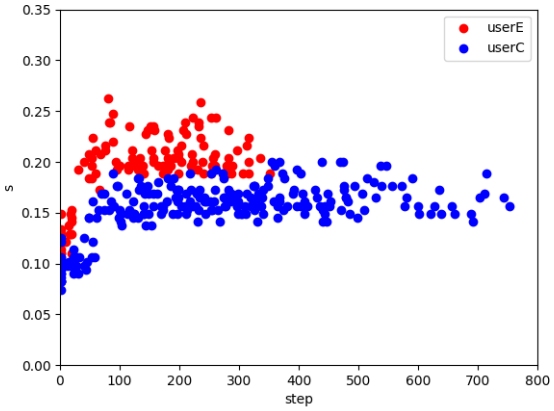

図 5 user C と user E の接触面積

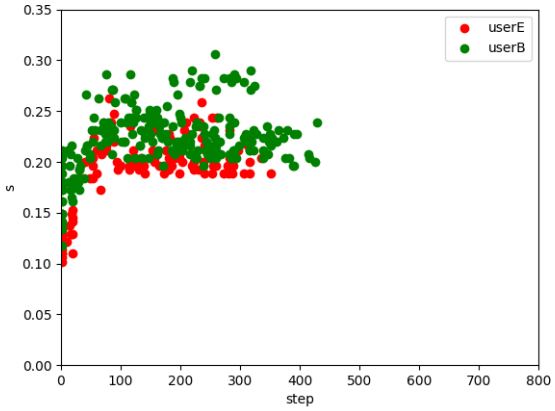

図 6 user B と user E の接触面積

とを考えたときに第 3 者による侵入を防ぐことのほうが重要であるため，本人拒否率よりも他人受け入れ率を低く抑えることのほうが重要である．今回の実験で user D 他人受け入れ率が 0%でなかった理由を明らかにしていく必要がある．

user D の分類器では，user B と user C を未知データとして用いた．多数決認証の結果では，user C より user B の方が誤認識している割合が多く，なかでも接触面積を用いた分類では，user B のすべてのデータを user D 誤認識していた．そこで，user B と user D の接触面積の特徴量の比較を行った．user C と user D の接触面積のデータを図 3 に示し，user B と user D を図 4 に示す．図 3 と図 4 を比較すると，user C と user D は点の重なっている部分が少なく，特徴量の違いが現れていることが分かる．一方で user B と user D は user C と比較して点が重なっている部分が多く，似た特徴量を持っていることが分かる．よって今回の接触面積の分類で user D の FAR が 50% と高かったのは，user B と user D の特徴量が似ていたからだと考えることができる．

6. まとめ

今回，先行研究の標準化ユークリッド距離を用いた手法よりも高い精度を出すために，サポートベクターマシン用いた実験を行った．既知 user 認証実験では，FRR が 8%，FAR が 0%となり，先行研究より高い精度を出すことができた．また，未知 user 認証実験では，FAR が 5.6%であった．未知 user 認証実験の FAR が 0%に抑えられなかった原因として，user D と user B の接触面積の特徴量が似ており，分類することが難しかったからなのではないかと考えられる．現時点での解決方法として，x 軸速度，y 軸速度のデータから特徴量として，特徴点の速度を用いているが，特徴点間の時間など特徴量を増やすことで，解決するのではないかと考えられる．以上の結果から，1 人の user を除いて，他の user の FAR は 0% に抑えることができたため，サポートベクターマシンを用いることで，強固で実用的な認証方式の実現に成功した．

参考文献

[1] 石黒司，福島和英，清本晋作，三宅優 ：“モバイル端末のロック解除向けパターン認証の安全性評価” 情報処理学会研究報告，Vol.2012-SPT-4 No.41，pp.273-278，2012

[2] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith,“Smudge Attacks on Smartphone Touch Screens.”Department of Computer and Information Science University of Pennsylvania

[3] Guixin Ye , Zhanyong Tang , Dingyi Fang , Xiaojiang Chen , Kwang In Kim , Ben Taylor , and Zheng Wang ,“Cracking Android Pattern Lock in Five Attempts.”NDSS ’17, 26 February - 1 March 2017, San Diego, CA, USA

[4] 牧野隆典，山田健一郎，納富一宏，斎藤恵一 ：“スマートフォンにおけるパターン認証の強化～軌跡情報および傾き情報に基づく生体認証～” 第 26 回バイオメディカル・ファジィ・システム学会年次大会講演論文集，pp.25-28，2013

[5] 小松哲幸 黒岩丈介 小高知宏 諏訪いずみ 白井治彦，”スワイプ操作における無意識的特徴量を用いた個人認証，”平成 28 年度電気関係学会北陸支部大会講演論文集，F2-42(2016.9)