人間の動作に対するアノマリ型異常検知システムの実装

藤原大輔[†1] 菊地誠[†1] 阿部洋丈[†1]
岡部正幸[†2] 梅村恭司[†1]

センサを用いたセキュリティシステムは一般的に，すべての動作を検知するモードと，その動作が不審かどうかを人間が判別するモードがあり，モードの切り替えが生じる．システムが不審者の動作と正常な動作とを判別できれば，モードの切り替えを必要としない自動検知が実現できる．本研究では上記のような自動検知の実現の準備段階として，実際に焦電型センサ群を構築し，あらかじめ与える正常な動作のデータからその動作発生時のセンサ状態などを学習した．そして，正常動作の確率的モデルを定義し出現確率を推定することで，正常動作とそれ以外の動作とを判別するアノマリ型異常検知システムを実装した．

Implementation of Anomaly Detection System for Human Behavior

FUJIHARA Daisuke,[†1] KIKUCHI Makoto,[†1] ABE Hirotake,[†1]
OKABE Masayuki[†2] and UMEMURA Kyoji[†1]

Generically, a security system has two modes. One mode is to detect all behavior and the other mode is to discriminate that the behavior is anomaly by humans. Therefore, these modes must be toggled if required. If computer is able to discriminate normal behavior from anomaly automatically, we can construct automatic detection system without toggling the modes. Our study is a preliminary stage of an automatic detection that is mode free. We construct pyroelectric sensor set and provide our detection system with sensor data of normal behaviors Then our system discriminate normal behavior from others with estimations of probability of occurrence based on probabilistic models our system defined.

1. はじめに

セキュリティシステムにおいて，不審な動作を検知する方法は重要である．センサを用いたセキュリティシステムは一般的に，すべての動作を機械が検知するモードと，その動作が不審かどうかを人間が判断するモードがあり，モードの切り替えが生じる．ここで，モードの切り替えを無くしたいという要求がある．機械が不審な動作を判断できれば，モードの切り替えを必要としない自動検知が実現できることとなる．これにより人手のコストの削減が期待できる．したがって，モードの切り替えを無くすためには，不審者の動作と正常な動作との判別を実装しなければならないが，具体的にどのような方法で実現できるかは検討課題である．

†1 豊橋技術科学大学 情報工学系
Depertment of Information and Computer Sciences, Toyohashi University of Technology
†2 豊橋技術科学大学 情報メディア基盤センター
Information and Media Center, Toyohashi University of Technology

本研究ではその準備段階としてのアノマリ型異常検知のシステムを実装する．基本方針は先行研究[1),2)] を参考とする．別の領域では先行研究[3)] で同様のアプローチがある．

まず，研究室内に構築したセンサ群によって，あらかじめ定義した正常な動作に対するセンサ状態を取得する．そのセンサ状態のデータを学習データとして，正常動作の確率モデルを得る．そして未知のデータに対して正常動作の推定確率を計算することで，正常動作と異常動作との判別を試みる．本稿では，このアプローチでシステムを実装し得ることを示す．

2. ベイジアンネットワーク[4)5)]

ベイジアンネットワークとは，確率分布の図式的表現である確率的グラフィカルモデルのひとつである．グラフィカルモデルには以下のような特徴がある．

- 確率モデルの構造を視覚化する簡単な方法を提供し，新しいモデルの設計方針を決めるの

に役立つ
- グラフの構造を調べることにより，条件付独立性などのモデルの性質に関する知見が得られる
- 精巧なモデルにおいて推論や学習を実行するためには複雑な計算が必要となるが，これを数学的な表現を暗に伴うグラフ上の操作として表現できる

今回実装するシステムについては，設計の方針を確立したいという目的から，ベイジアンネットワークを使用することにする．

3. 異常検出システムの実装

正常なモデルをあらかじめ定義し，その定義に当てはまらないものを異常と判断する方法をアノマリ型の異常検知と呼ぶ．

実装したアノマリ型異常検知システムには，あらかじめ正常な動作（以降，定義イベントと呼ぶ）のときのセンサ時系列データを学習データとして与える．この学習データから，各イベントの確率的モデルを得る．そして，未知のセンサ時系列データに対して，どの定義イベントでもないと判断した場合に異常と出力する．

以降，システムの各構成要素の詳細について述べる．

3.1 実装環境と正常動作の定義

実験場所は研究室とし，**図 1** に示すように，研究室内にシステムの入力となる 6 個の焦電型センサ $(s_1, s_2, \ldots, s_6)$ を配置する．焦電型センサは，取得範囲で物が動いたときにオンとなる．今回はオンを 1，オフを 0 とする二値センサとして使用する．

定義イベントは “入口から入室し，各席に着席する” こととし，時刻 n に各席 $e_1, e_2, \ldots, e_6$ に座るイベントをそれぞれ $e_1(n) = 1, e_2(n) = 1, \ldots, e_6(n) = 1$ と表す．ここで $e = 1$ となるのは，着席した時刻のみである．この着席した時刻は，上記センサとは別の各席に設置したセンサで取得するが，この各席に設置したセンサは正解判定用であるため，異常判定時には使用しない．

3.2 取得時間間隔と可変時間圧縮

焦電型センサによるセンシングの時間間隔は 0.2 秒である．これはプログラム実装上の限界値であるが，通常の人間の動きを対象としているため，この時間間隔は妥当であると考える．

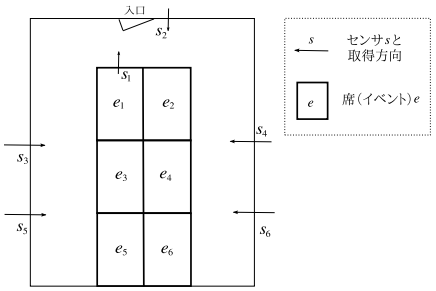

図 1 センサ配置と定義イベント

ここで，0.2 秒間隔の時系列データを圧縮することを考える．以下の 2 つの場合に，圧縮後のデータとしてセンサ値を保存する．

(1) センサ状態が変化した場合

(2) 一定時間センサ状態に変化がない場合

これは焦電型センサの性質から，何らかの動作が発生した場合はオフからオンになることが，定常状態では多くの場合センサがオフになることが想定される．(1) は動作部分の抽出に対応し，センサが連続でオンとなる状態を圧縮後の単位時間にうまく表現できる．(2) は定常状態の記録に対応しており，後に述べる動作を判定するタイミングに等しい．この時間圧縮は，(2) で定める一定時間を最大圧縮時間とする可変圧縮であり，学習データの時間的なゆれをうまく吸収できると考える．

3.3 ベイジアンネットの構成ノードの学習

学習データからベイジアンネットワークの構成ノード，すなわち，イベントの発生に反応しているセンサを求める．焦電型センサの性質から定常状態ではセンサがオフになることが多くなるので，ここでの反応とはセンサがオンになることとする．学習データとして，焦電型センサの時間圧縮後のデータを与える．このデータはセンサの二値状態に加えて，イベント発生時の時刻とそのイベント名が付与してある．時間圧縮後のイベント発生時刻を基準にして，K 時刻前までのセンサ状態を確率変数としてモデルに含める範囲とする．K はあらかじめ与えるものとする．

なおグラフ構造の学習は一般に困難であるので，今回は**図 2** に示すようにグラフを定めた．このグラフでは，センサ間の依存関係はないものとしている．したがってここでの処理は，各イベントの発生確率を因数として含む同時確率を構成する確率変数の集合を求めることに等しい．

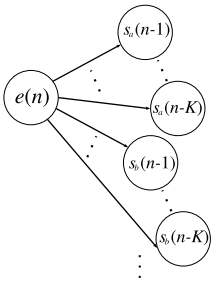

図 2 生成する確率モデルのグラフ表現

イベント e に反応するセンサ s は，式 (1) を満たすものとする．ここで閾値 0.5 は，実際のデータをもとにして定めた．

$$\exists k\ \mathrm{P}(s(n-k)=1|e(n)=1) \geq 0.5 \quad \text{for } k=1,\cdots,K \tag{1}$$

式 (1) での k に関わらず，イベント e のモデルには確率変数 $s(n-1),\cdots,s(n-K)$ のノードをすべての加える．したがって，イベント e と反応するセンサの集合 S の同時確率は式 (2) となる．

$$\mathrm{P}(e(n),S)=\mathrm{P}(e(n))\prod_{s\in S}\prod_{k=1}^{K}\mathrm{P}(s(n-k)|e(n)) \tag{2}$$

3.4 隣センサの学習

3.3 節では，各イベントに対してオンになるセンサを反応のあるセンサとして学習した．ここで入口に近いセンサ s_1 について考えると，イベント e_1, e_3, e_5 で s_1 がオンになることがあると想定される．イベント e_1 と e_3 を区別するためには，センサ s_3 の状態が必要となる．これより，反応のあるセンサの隣にあるセンサも有用な情報を持つと考える．

そこで，センサの位置関係を学習データから求め，式 (1) で求まるセンサ集合の隣にあるセンサをベイジアンネットワークのノードに加えることとする．センサ s_p の隣にあるセンサ s の条件は式 (3) を満たすものとする．ただし，各基準となるセンサ s_p に対して最大 2 個なので，式 (3) の左辺値が大きい順に 2 つ選ぶ．

$$\frac{\mathrm{fr}(s(n)=1,s_p(n-1)=1)}{\sum_{i\neq p}\mathrm{fr}(s_i(n)=1,s_p(n-1)=1)} > 0.2 \tag{3}$$

ここで $\mathrm{fr}(a(n)=1,b(n-1)=1)$ は，学習データ中にセンサ状態が $a(n)=1,b(n-1)=1$ となった回数である．n は任意時刻である．

3.5 判 定 方 法

式 (2) の同時確率から，ベイズの定理よりセンサ状態 S_ω が与えられたときのイベントの出現確率が求まる．

$$\mathrm{P}(e(n)=1|S_\omega)=\frac{\mathrm{P}(e(n)=1,S_\omega)}{\mathrm{P}(S_\omega)}=\frac{\mathrm{P}(e(n)=1,S_\omega)}{\sum_{v\in\{0,1\}}\mathrm{P}(e(n)=v,S_\omega)} \tag{4}$$

この事後確率を計算するタイミングは，タイムアウトの発生，または，テストデータファイルの終端とする．タイムアウトとはすべてのセンサの状態が一定時間変化がないことを表し，イベント発生後は定常状態になるという仮定のもとにこの時点で判定する．タイムアウトの閾値は 6.0 秒とする．

異常か定義イベントかの判定は，(4) に学習データを入力し，各イベントごとに最小値 $\mathrm{P}_{min}(e)$ を求め，テストデータから得られる事後確率との比をとり，1 未満かどうかで行う．すなわち，

$$\frac{\mathrm{P}(e(n)=1|S_\omega)}{\mathrm{P}_{min}(e)} \tag{5}$$

が 1 未満ならば異常であると判定する．

表 1 イベントに反応のあるセンサ集合の学習結果

行動	センサ集合	行動	センサ集合
e_1	s_1	e_2	s_2
e_3	s_1, s_3	e_4	s_2, s_4
e_5	s_3, s_5	e_6	s_4, s_5, s_6

4. 実　　験

4.1 予備実験：反応センサの学習

3.3 節に示したイベントに反応のあるセンサの学習について実験した．学習データとして，6 種の定義イベントそれぞれ 20 件のセンサ時系列データを与え，式 (1) より，K を 4 として各定義イベントに反応のあるセンサ集合を求めた．結果を**表 1** に示す．

図 1 と表 1 とを見ると，席に最も近い入口側のセンサが含まれており，$e_3 \sim e_6$ は席から 2 番目に近い入口側のセンサが含まれている．また，e_6 の結果に s_5 が含まれているが，これはセンサ s_5 の取得範囲が席 e_6 まで及んでいるためである．これらの結果は我々が実験前に想定した反応センサに近いものであり，総じて想定された結果であると言える．

4.2 予備実験：隣センサの学習

3.4 節に示した隣にあるセンサの学習について実験した．学習データとして同様に 6 種の定義イベントそれぞれ 20 件のセンサ時系列データを与え，式 (3) より，各センサの隣のセンサを求めた．結果を**表 2** に示す．

表 2 隣センサの学習結果

基準センサ	隣センサ
s_1	s_3
s_3	s_5
s_5	s_3, s_6

基準センサ	隣センサ
s_2	s_4
s_4	s_2, s_6
s_6	s_4, s_5

表 3 テストデータが定義イベントの場合

行動	正解	異常	誤り
e_1	10	0	0
e_3	10	0	0
e_5	7	3	0

行動	正解	異常	誤り
e_2	10	0	0
e_4	10	0	0
e_6	10	0	0

表 4 テストデータが異常行動の場合

行動	異常	誤り
$e_1 - e_3$	5	1
$e_3 - e_5$	2	4
$e_5 - e_6$	1	5

行動	異常	誤り
$e_2 - e_4$	2	4
$e_4 - e_6$	3	3
$e_1 - e_2$	5	1

図 1 と表 2 とを見ると，s_5 と s_6 は実際は対面であるが，学習結果では隣と判別された．これは，センサ s_5 および s_6 の取得範囲が対面まで及んでいるためである．また，s_1 と s_2 の隣関係が学習できていないが，これは学習データの中に s_1 と s_2 の両方を通るような動きが無かったためである．

4.3 定義イベントの判別

学習データとして同様に 6 種の定義イベントそれぞれ 20 件のセンサ時系列データを与え，テストデータとして各定義イベントそれぞれ 10 件を入力し，どのように判別されるかを実験した．式 (1) および式 (2) の K は 4 とし，各テストデータで事後確率と学習データから求めた最小値との比 (式 (5)) を求め，すべてのイベントに対して 1 未満ならば異常行動と判定し，1 以上のものがあれば，その中で最大をとるイベントと判定した．結果を**表 3** に示す．

異常を検出する前に正常なパターンを同定することは必要であるが，全体で 57/60 で正しく判別できており，これは実現できていると言える．

4.4 異常行動の判別

テストデータのイベントを，異常行動 “着席せずにセンサ間をうろつく” として，全 36 件の異常行動に対して 4.3 節と同じ設定で実験した．36 件の内訳は，2 つの隣り合う席の間を往復する (例:$e_1 - e_2$ 間の往復) のが 5 箇所それぞれ 6 件と，$e_5 - e_6$ 間の往復が 6 件である．結果を**表 4** に示す．表中の “誤り” は，定義イベントのいずれかに判別されたことを示す．

全体で 18/36 で異常と判別した．この結果だけを見れば決して良い性能とは言えない．

今回、センサデータから動作を判定するタイミングとして，タイムアウトまたはデータファイルの最後と定めた．ゆえに，途中の状態は一切見ていない．途中の状態の情報を利用することで，性能を向上させることが出来ると考えられる．

実用上はまだ改善の余地が多いが，この枠組みで動作するシステムを作成できたと考える．

5. おわりに

動作モードの切り替えが不要なシステムの実現の準備段階として，アノマリ型異常検知のシステムの実装を示した．

可変時間圧縮の妥当性やイベントの判定時期など，検討すべき点は多い．また最終的な目標として，センサ配置や定義イベント，各閾値などを事前知識なしで設定でき，どこでも動作するシステムを実現することがある．このようなシステムの実現のための問題点は多く残されており，それら問題の解決は今後の大きな課題である．

謝辞 この研究は，戦略的情報通信開発推進制度（SCOPE）の課題「実空間情報処理のためのインターユビキタスネットワークの研究」の成果です．また，平成 20 年度科学研究補助金課題番号（19500120）の研究成果を使用しました．

参考文献

1) 青木茂樹, 大西正輝, 小島篤博, 菅原康博, 福永邦雄. 人感センサによる独居高齢者の行動パターンの認識. 電子情報通信学会技術研究報告. WIT, 福祉情報工学, Vol. 101, No. 703, pp. 43–48, 2002.
2) 関弘和, 多田隈進. 全方位センサのベイジアンネットワーク表現に基づく高齢者非日常行動検出モニタリングシステム. 電気学会論文誌D（産業応用部門誌）, Vol. 128, No.8, pp. 1052–1059, 2008.
3) C. Kruegel, D. Mutz, W. Robertson, and F.Valeur. Bayesian event classification for intrusion detection. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pp. 14–23, 2003.
4) 本村陽一. ベイジアンネットワーク. 電子情報通信学会誌, Vol.83, No.8, pp. 645–646, 2000.
5) 赤穂昭太郎, 神嶌敏弘, 杉山将, 小野田崇, 池田和司, 鹿島久嗣, 賀沢秀人, 中島伸一, 竹内純一, 持橋大地, 小山聡, 井手剛, 篠田浩一, 山川宏. パターン認識と機械学習（下）: ベイズ理論による統計的 予測. シュプリンガー・ジャパン, 2007.