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

2006－DPS－126（35）
2006－CSEC－32（35）
2006／3／17

不審な挙動の検知による内部犯対策(その 2)

丸岡 弘和*　杉浦 敏文**　西垣 正勝***
*静岡大学大学院情報学研究科，**静岡大学電子工学研究所，***静岡大学情報学部

あらまし　近年，内部不正者による情報漏洩が社会問題となっている．我々は，ユーザが不正を行う際に不審な挙動が現れることに着目し，内部不正者のリアルタイム検知を実現する方式を検討している．これまでに「横目で周囲を確認する(チラ見)」という行動の検出による内部犯検知の可能性を探ったところ，被験者は実験を重ねる内に徐々に自分の体の制御の仕方を覚え，チラ見を発生させずに不正を行うことができるようになることが判明した．そこで本稿では，不正を行う際のユーザの心理状態の変化をダイレクトに検出できる心拍数の変化を内部犯検知に利用する手法を導入する．心拍数を自分で制御することは基本的には難しいため，訓練を重ねた内部不正者であっても不正の検知を回避することはより困難になると考えられる．本手法について，新たに基礎実験を行うことによりその有効性を確かめる．

A countermeasure against insider with detection of suspicious behavior (part2)

Hirokazu Maruoka*,　Toshifumi Sugiura**,　Masakatsu Nishigaki***
*Graduate School of Informatics,　Shizuoka University
**Research Institute of Electronics,　Shizuoka University
***Faculty of Informatics,　Shizuoka University

Abstract We proposed a real-time detection of internal fraud by sensing insider's suspicious behavior in our previous work, but in which we found that experimented insiders could be able to control their behavior and avoid detection of their fraud. Therefore, in this paper, we introduce to detect heartbeat interval of insiders. It is well known that when human being gets nervous, his/her heartbeat interval will immediately change. Since it is impossible for human being to control heartbeat, it is expected that using heartbeat interval as a suspicious behavior makes it more difficult for even experienced insiders to avoid detection. By conducting some experiments, we evaluate its effectiveness.

1.　はじめに

近年問題となっている，情報漏洩をはじめとする内部不正[1]の対策としては，機密ファイルの暗号化やアクセス制御，アクセスログの保存といった方法が採用されている[2]．しかし，機密ファイルの暗号化やアクセス制御は，正規ユーザである内部不正者が復号鍵やアクセス権限を有しているために有効でない．また，ログの保存は犯行の追跡や証明には有効であり犯罪抑止力として働く[3]が，犯行をリアルタイムに検知できないため，対処が遅れてしまう可能性がある．

そこで，我々はこれまでに，ユーザが不正を行う際に生じる緊張や罪悪感といった心理状態の変化と，それに伴うユーザの挙動の変化に着目し，普段とは異なる不審な挙動を検出することによって内部不正をリアルタイムに検知する方式を提案してきた[4]．文献[4]では，不審な挙動として「横目で周囲を確認する行動(チラ見)」を検出することで内部不正を検知する手法について基礎実験を実施した．その結果，不正行為に不慣れな被験者に対しては，不正実行時にチラ見が検出され，ある程度の内部犯検知への適用可能性を示すことができた．しかし，実験を繰り返していくと，次第に自分の挙動(目や顔の動き)を制御する仕方を覚え，最初はつい目や顔を動かして周囲を確認していた被験者が，周辺視を用いたり監視者の足音を聞いたりすることによってチラ見を発生させずに不正を行うことができるようになるという問題が顕在化してきた．

よって，本稿ではユーザが制御できないレベルの心理状態の変化を検出することにより，熟練した内部不正者であっても不正を検知できる手法の実現を目指す．

2. 不審な挙動の検知による内部犯対策

内部不正者は組織の正規ユーザであるため，機密ファイルに正規にアクセスし，読み出しや書き換えを行う権限を有しており，その操作が正規業務か不正操作かを単純に判断することは難しい．このように表面的には区別が付かない正規ユーザによる正規業務と不正操作を見極めるために，我々は，ユーザの心理状態や挙動に注目する．ユーザが不正を行う際には，不正を犯すという緊張や罪悪感から，日常の正規の業務を行う際とは異なる心理状態にあると考えられる．そして，それが普段とは異なる不審な挙動や生理的な変化となって現れる可能性が高い．

不正を行うユーザに共通する生理的な変化や挙動が存在するのならば，これを検出することにより，内部不正を効率よく検知することが可能となることが期待される．ユーザの心理状態の変化や，それに伴う挙動や生理的な変化について，検出が可能であると考えられるものの例を次に示す．

(1) 心拍数の変化
(2) 発汗量の変化
(3) 体温の変化
(4) 周囲の様子を確認する行動

本研究は，上記のような内部不正者の心理状態の変化に起因する不審な挙動や生理的な変化を検出することによって，内部不正をリアルタイムに検知することを目指すものである．

我々はこれまでに，(4)の「周囲の様子を確認する行動(チラ見)」を検出することで内部不正を検知することを試みた[4]が，被験者は実験を重ねる内に徐々に自分の体の制御の仕方を覚え，チラ見を発生させずに不正行為を行うことができるようになることが判明した．そこで本稿では，新たに(1)の「心拍数の変化」の検出を導入する．人間は平常時と緊張時において心拍数に変化が生じることが知られており，かつ，心理状態の変化は比較的速やかに心拍数の変化として現れる[5，6]．一般的に，ユーザは平常の業務を行っているときと比較して，不正を行っている際には少なからず心理的に緊張状態にあるため，これが心拍数の変化として検出されると考えられる．心拍数を自分で制御することは基本的には困難であるため，不正者が本方式の詳細を知っていたとしても本方式による検知を回避することは難しいだろう．

図 1 と図 2 は，平常時と緊張時の典型的な心拍の状態を示したものである．図は，縦軸が心拍の間隔を表す R-R 間隔[5]，横軸が時間(プロット数)である．人間は，気持ちが落ち着いてリラックスした状態にあると，図 1 のように，心拍の間隔が平均的に長くなり，ばらつきも大きくなる．逆に緊張状態にあるときは，図 2 のように，リラックスした状態よりも心拍の間隔が平均的に短くなり，狭い範囲に収まるという特徴がある[5][1]．

本稿では，この内部不正時の心拍数の変化を検出することができるかどうかを基礎実験により確認する．具体的には，平常状態と不正を行っている状態における心拍データを取得し，平常状態と不正を行っている状態を比較した場合に，図 1 の心拍の状態から図 2 のような心拍の状態への変化が観測されるかどうかを調査する．

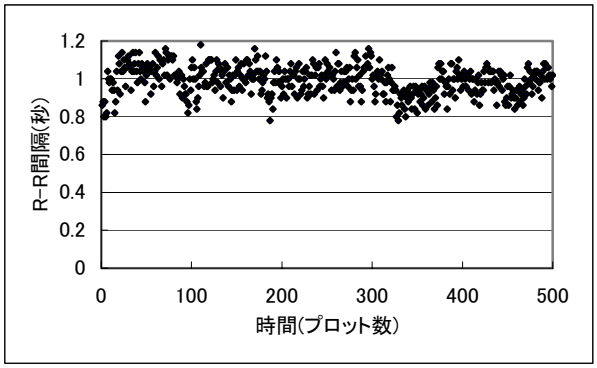

図 1：平常状態の心拍数

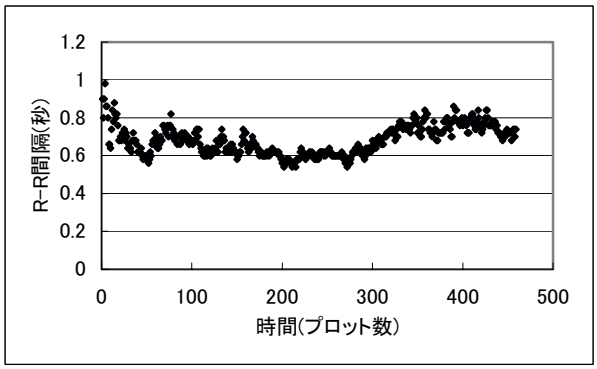

図 2：緊張状態の心拍数

3. 基礎実験

本節では，ユーザが不正を行う際に，平常時と比べ実際に心拍数が変化するかどうかを実験によって確かめる．また，これまでどおり，周囲を確認する行動(チラ見)についても，内部不正を検出するトリガ

[1]実際，図 1，図 2 のグラフは 3 章の実験にて得られた結果の中から典型的なデータを掲載したものである．

の 1 つとして合わせて観察する．内部不正者役の被験者には，事前に本方式の詳細(心拍数の変化およびチラ見を検出することによって不正行為を検知するものであること)を説明し，それでも不正行為を検知できるかどうかを調査する．

3.1　実験方法

3.1.1　実験環境

実験は「被験者」1 名と「監視者」1 名からなる実験ペアで行われる．実験の最初に，被験者は内部不正を行う前の平常状態について，心拍数の測定を行う．その後，被験者は内部不正者として，正規業務と不正操作(以下，「正規ジョブ」及び「不正ジョブ」と表記する)を行い，監視者は被験者の背後を歩きながら監視し，被験者が不正ジョブを行うところを発見しようとする．実験の様子を図 3 に示す．

実験に参加するのは，本学男子学生 5 名である．5 人の被験者それぞれにつき，残りの 4 名の中から「監視者」を選び，実験ペアを作る．ただし，1 回の実験において，同じ人が 2 人以上の被験者の監視者として選出されないようにした．毎回監視者を選び直しながら，各被験者について 2〜4 回の実験を行う．実験と実験の間は少なくとも一日以上の間隔をあけ，各被験者には実験の翌日に前日の実験の結果(チラ見発生の有無，心拍数変化の有無)を伝え，チラ見が観察された被験者にはそれを抑制するように，また，心拍数変化が検出された被験者にはできるだけリラックスした状態で次回の実験に望むように指示した．

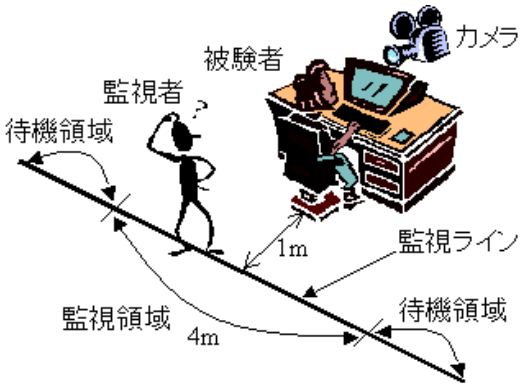

図 3：実験環境

被験者は PC の前に座って作業を行う．被験者の後方 1m には，被験者の左右の方向に「監視ライン」を設けた．監視ライン上において，被験者の位置を中心として左右 2m ずつの範囲を「監視領域」，その外を「待機領域」とする．

本実験は，内部不正の検出を目的としているため，被験者には不正ジョブが監視者に見つかることをできる限り避けてもらう必要がある．そこで，被験者に対して不正を達成する意欲を向上させるために，実験の成功回数に応じた報奨金(1000 円相当の食事券)を提供した．

3.1.2　正規ジョブと不正ジョブ

被験者の行う正規ジョブと不正ジョブは以下のように設定した．なお，両方のジョブとも，デスクトップ PC(OS：Windows2000)の GUI 上において作業を行う．

- 正規ジョブ：Web ブラウザ[2]を用いてニュースサイト[3]を閲覧した上で，そのサイトのニュースをコピーし，エディタ[4]にペーストする．1 回のコピーはニュースの一文ごとに行うよう制限し，エディタ 1 ページ分(1100 文字見当)のコピー&ペーストの作業を行う．
- 不正ジョブ：PC 内のあらかじめ決められたフォルダ内にある画像データ 1 つを，PC に接続されている USB メモリにコピーする．なお，ファイルコピーは，i) マウス操作によって画像が存在するフォルダウィンドウを開き，ii) 同様にコピー先である USB メモリのフォルダウィンドウを開き，iii) マウスのドラッグ＆ドロップ操作，または Ctrl-C ＆ Ctrl-V のキーボード入力によって画像ファイルをコピーする，という手順で行うこととする．画像データのファイルサイズは小さく，PC によるコピー処理は一瞬で終了する．

3.1.3　被験者の行動

被験者は，まず，平常状態の心拍数のデータを測定する．図 3 に示された実験環境のもと，被験者は PC の前に座り，監視者がいない状態で 10 分間の読書(本は被験者が任意に選択する)を行う．内部不正を想定するため，本来，平常状態のデータは正規ジョブのみを行っているときの心拍数を取得する方が理に適っている．しかし，基礎実験である現段階では被験者の負担を考慮して 10 分間の読書によってこれに代えた．なお，ごく少人数ではあるが，読書をした場合と正規ジョブのみを行った場合の心拍の変

[2] Microsoft Internet Explorer
[3] Yahoo! JAPAN，http://www.yahoo.co.jp/
[4] Microsoft Word 2000

化を比較する予備実験を事前に行ったところ，両者に大きな差は認められなかった. 我々はこの 10 分間の読書によって得られた被験者の心拍数のデータを，「被験者の安静時のデータ」と定義する.

被験者は安静時のデータを測定した直後に，内部不正者として，監視者に発見されないように正規ジョブの合間に不正ジョブを行う．あらかじめ被験者には, 本実験が「周囲を確認する行動(チラ見)」と「心拍数の変化」を検出しようとしていることを伝えている．したがって，被験者はできる限り周囲を確認せずに，かつ緊張しないように不正ジョブを行おうとすることが予測される．被験者が正規ジョブと不正ジョブの両方を完了した時点で，不正成功として実験を終了する.

3.1.4 監視者の行動

監視者は，監視ラインに沿って被験者の後ろを歩きながら，被験者のディスプレイを監視する．監視者は，片方の待機領域からもう一方の待機領域までをほぼ一定の歩速で往復しながら，監視領域内にいる間のみ被験者のディスプレイを見ることが許される. もう一方の待機領域に達したら, 監視を中断し，待機領域内で約 3 秒間停止した後，また反対側の待機領域に向けて歩き出し，監視を再開する．途中で立ち止まったり，監視領域の途中で反対方向に引き返したりすることはない．監視者は監視領域を歩いている間に散発的に被験者のディスプレイを監視する(監視領域内では常にディスプレイを凝視しているわけではない)のだが，後ろを向いている被験者はいつディスプレイを見られているのか分からないので，被験者は必然的に監視者が待機領域で停止している間に不正ジョブを試みるということになる．なお，監視者の歩く速度については監視者役の実験参加者に一任したが，通常の歩行速度の範囲内で歩くように指示した.

監視者が被験者のディスプレイ上に Web ブラウザとエディタ以外のウィンドウを発見した場合は「不正失敗」とし，その時点で実験を終了する.

本実験では，不正を犯すことに対する緊張や罪悪感から生じる挙動の変化や生理的な変化を確認したい．しかし，実験の被験者に本物の不正者と同様の緊張や罪悪感を抱かせることは難しい．そこで，監視者を置いで 監視者に Web ブラウザとエディタ以外の作業ウィンドウを発見されてはいけない” という状況を用意することにより，被験者に“ 他人に見つかってはいけない業務を行っている” という気持ちを持たせるようにし，擬似的に緊張状態を作り出している.

3.1.5 実験で取得するデータ

実験中は，カメラ[5]を用いて被験者の目や顔の動きを録画した. また, 被験者の心拍を測定するために，被験者の胸部に二箇所，右足に一箇所心電図モニタ用の電極[6]を取り付け，被験者が実験を行っている間のデータを心拍計[7]から AD 変換器[8]を通して連続的にコンピュータ内に取り込んで心電図を記録した[9]. 実験で得られた心電図から心拍の間隔を表す R-R 間隔[5]を抽出し，図 1，図 2 のようなグラフを作る.

実験終了後，取得されたデータから各被験者の周囲を確認する行動と，心拍数の変化を検出する．なお，本研究は内部不正をリアルタイムに検出することを目指すものだが，今回の実験では実験終了後に人間の目によってカメラの映像と心電図のデータを解析した.

また，正規ジョブと不正ジョブの切り替えのタイミングを見るため，実験中のアクティブウィンドウを 1ms 単位で記録した.

3.2 実験結果

事前に 5 人の被験者に，チラ見のみの検出による内部犯検知実験[4]を何度か経験してもらった．全員が不正の際にチラ見をしないようにすることができるようになった後に，チラ見と心拍の両者の検出による内部犯検知の実験を開始した．チラ見と心拍による検知実験の結果を表 1 に示す．表 1 は，各被験者の不正ジョブの成否, 周囲を確認する行動(チラ見)の有無，安静状態とジョブを行っている際の心拍数の変化の有無(心拍の間隔が平均的に短くなったか，心拍の間隔のばらつきが狭まったか)を表している.

まずは，5 人の被験者に対し，チラ見と心拍による検知実験を 2 回ずつ行った. 被験者 D と E については，はっきりとした心拍数の変化を捉えることが

---

[5] PERSONAL 社，PBC003，画素数 : 130 万画素相当，フレームレート : 30fps

[6] 日本光電工業株式会社，心電図モニタ用ディスポ電極　F ビトロード

[7] 今回は自作の装置を使用した.

[8] 株式会社コンテック，USB 対応絶縁型アナログ入力モジュール ADI12-8(USB)GY

[9] 最近では腕時計型の脈拍計[7]なども実用化されており，実際の現場では簡単に着脱できる方法で心拍を検出することも可能になると考えられる.

一回目				二回目				三回目				四回目			
実験の成否	周囲の確認行動の有無	心拍の変化		実験の成否	周囲の確認行動の有無	心拍の変化		実験の成否	周囲の確認行動の有無	心拍の変化		実験の成否	周囲の確認行動の有無	心拍の変化	
		平均	分散			平均	分散			平均	分散			平均	分散
○	○	○	×	○	×	×	×	○	×	×	×	○	×	×	×
○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
○	×	×	×	○	×	×	×	○	×	×	×	○	×	×	×
○	×	○	×	○	×	○	×	−	−	−	−	−	−	−	−
○	×	○	○	○	×	○	○	−	−	−	−	−	−	−	−

表 1：チラ見と心拍の変化を利用した内部犯検知の実験結果

できたため，この時点で実験を終了した．被験者 A と C については心拍の変化が定常的に捉えられなかったことから継続してさらに 2 回実験を行った．しかし，A の 1 回目の実験を除き，4 回の実験を通じて心拍の変化は観測されなかった．被験者 B については，1 回目，2 回目の心拍数の変化が観測されていたものの，その変化が被験者 D や E に比べ小さかったことから，やはり 3 回目，4 回目の実験を行った．4 回の実験を通じて，心拍の変化が捉えられている．

4. 考察

実験結果より，3 人の被験者においては，「不正ジョブ実行時に周囲の確認行動(チラ見)を抑える」という自分の体の制御が可能になった後でさえ，心拍数の平均または分散の変化が定常的に検出されることが確認できた．これより，不正を行うことにある程度慣れた者であっても，心拍の変化を意識的に抑制することが難しいことが分かる．特に，心拍数の平均の変化については 3 人の被験者を通じ常に観測できている(また，被験者 A の 1 回目にだけ現れた変化も心拍の平均である)．したがって，この心拍数の平均の変化は，内部不正を検知する上で有力なトリガになると考えられる．

しかし，被験者 A と被験者 C については，不正をほとんど検知できなかった．A と C に実験終了後にアンケートを実施し，実験時の心理状態について尋ねたところ，両者とも「実験中は緊張していたと思う」という回答が得られた．このことから，今回の基礎実験で A と C から，心拍数の変化が検出されなかった理由として，以下のことが考えられる．

1. 安静状態の心電図の取得時に，既に緊張状態にあった：実際，緊張しやすい体質の者はケース 1 のようなことが起こりうる．
2. 本人の感想とは異なり，被験者の身体は緊張状態に無かった：今回は内部不正という状況を“擬似的に”設けただけであったので，現実の内部不正者のような緊張状態を作り出すまでには至らなかった．また，本当に悪いことをしているわけではないが故に，被験者が実験に慣れてくるにつれて急速に緊張感が薄れてきて，心理状態に変化が生じにくくなっている可能性がある．

今回はすべての被験者の不正を検出することができなかったものの，このような簡単な実験でも 6 割程度の検知率が得られている．現実には，罪悪感や逮捕に対する恐怖から内部不正者にかかるストレスは非常に大きなものだろう．軽犯罪の場合は常習犯になると罪悪意識が希薄になると思われるが，大きな犯罪の場合は常習犯であっても緊張をすると考えられる．本方式では擬似的に緊張状態を作り出しているものの，その緊張の度合いは現実の内部犯とは比較にならない．よって，不正ジョブの種類やインセンティブの大きさなどを適切に変更し，実験における緊張度をより現実のものに近づけることができれば，被験者 A や C からも心拍の変化を検出できるのではないかと予想される．

また今回の実験では，実験中のアクティブウィンドウを記録することにより被験者がいつ不正ジョブを行っているかを捉えることができるようになっている．各被験者の心拍数の変化と不正ジョブを行っているタイミングについて調べたところ，複数の被験者から，「不正ジョブが完了すると心拍の間隔が大きくなる」という反応が見られた(図 4)．図 4 には R-R 間隔に加え，y=0.2 の線上に不正ジョブのウィ

ンドウがアクティブになっている時間を記載してある．図 4 の右側に注目すると，不正ジョブが完了した時点(最後に不正ジョブのウィンドウが非アクティブになった時点)を境に，心拍の間隔が増加している．これは，不正ジョブが無事終了した時点で被験者に安堵感が生まれ，それまでの緊張状態からリラックスした状態へと心理状態が移行したことを示していると考えられる．この反応は，内部不正者が実際に不正を行っている場合にも現れると予想される．内部不正者の心理などをより詳細に調査し，このような特徴的な反応を適切に検出していくことにより，内部犯検知をさらに向上させることが可能になると考える．

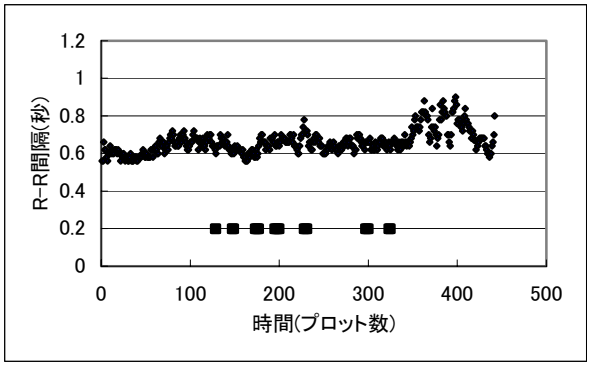

図 4：不正ジョブ終了時の心拍数の変化

5. まとめ

ユーザが内部不正を行う際には，緊張や罪悪感などから心理状態が変化することに着目し，これまでの周囲を確認する行動(チラ見)に加え，心拍数の変化を検出することによって内部犯を検知する方式を提案した．本稿では基礎実験を行い，本方式を熟知している内部不正者がある程度訓練したとしても，自分の心理状態を制御することができず，本方式による不正検知を回避することが困難であることを示した．

ただし，心拍は被験者が緊張状態にあるときだけでなく，物事に集中した際にも変化が生じることが知られている[5]．このため実際には，安静時－不正時間の心拍変化ではなく，正規ジョブに集中して取り組んでいる場合と不正ジョブを行っている場合で心拍が変化するかどうかを調査する必要がある．

また，心拍の変化を利用するにあたっては，被験者に心拍計を装着してもらわなければならないということが大きな問題となる．現在は腕時計型の心拍計なども実用化されているため，実用の現場ではそのような機器を使用する必要がある．心理状態の変化は心拍だけでなく，皮膚温にも敏感に影響を与えることが知られている[6]ため，これらの情報を利用するのもよいだろう．例えば，心拍の代わりに皮膚温の変化を検出する方法であれば，カメラ型の温度計を用いることにより，ユーザに非接触の状態でユーザの顔の表面温度の変化を捉えることが可能であると思われる．

謝辞

静岡大学電子工学研究所沖田善光先生に，心電図測定装置(心拍計)の貸与と，心拍の測定に関するご助言を頂いた．謹んで謝意を表す．

参考文献

[1] 河井保博,「情報漏洩，事件に学ぶ事後対策」，日経コンピュータ 記事，2004 年 5 月 17 日，http://itpro.nikkeibp.co.jp/free/NC/TOKU2/20040525/1/ (2006 年 2 月 確認).

[2] 「情報漏洩対策」，電子政府・電子自治体情報チャネル，http://cgs-online.hitachi.co.jp/serial/serial011/002.html (2006 年 2 月 確認) .

[3] 「ESS REC」，エンカレッジ・テクノロジ，http://www.et-x.jp/modules/tinycontent1/ (2006 年 2 月 確認).

[4] 丸岡弘和，西垣正勝,「不審な挙動の検知による内部犯対策」，情報処理学会研究報告，2005-CSEC-28, Vol2005, No.33, pp.363-368, 2005.

[5] 堺章,「新訂目で見るからだのメカニズム」, 医学書院.

[6]「職場環境診断のための人間感覚データベース」，http://www.hql.or.jp/gpd/jpn/www/hdb/work/content/topmenu.htm (2006 年 2 月 確認).

[7] 「日立 AirSense」，日立製作所，http://www.hitachi.co.jp/wirelessinfo/airsense/ (2006 年 2 月 確認).