明治大学大学院先端数理科学研究科

2017年度

博士学位請求論文

内部不正による情報漏えいを誘発する要因に関する研究

A study on incentives to a leakage of information asset caused by malicious insider

学位請求者　現象数理学専攻

新原　功一

目 次

図 目 次

表 目 次

第1章　序論

1.1　本研究の背景

1.1.1　内部不正による情報漏えい事故

個人情報を扱うことができる権限を悪用した者による情報漏えい事故が後を絶たない．近年特に大きな社会問題となったのは，ベネッセコーポレーション社（以下，ベネッセ社）が 2014 年に起こした大規模情報漏えい事故である [4]．この事故では，ベネッセ社の業務委託先の元社員が個人情報へのアクセス権限を有していた．この元社員は，与えられた権限を悪用して顧客の個人情報をスマートフォンにダウンロードした．そして，自らの借金返済などのために約 3,504 万件分の情報を名簿業者 3 社へ売却していた．また，2017 年 1 月には東京都中野区の元臨時職員が個人情報を不正に取得した．住民情報基盤システムへのアクセス権限を有していた元臨時職員は，女性の個人情報を収集し，取得した情報を基に女性宅に侵入した疑いで逮捕された [5]．この元臨時職員はシステムにアクセスし，1 人暮らしの女性の個人情報ばかりを保存し，犯行に及んだとみられている．情報セキュリティにおいて人的な要因は一番弱い鎖といわれている [1][2][3]．この 2 つの事故の共通点は，正当な権限を持った内部の人間が機密情報を不正に取得している点である．

内部不正への対策について，IPA[1] が経営者に対して実施したアンケート調査 [10] によると，経営者は機密情報へのアクセス制御を重要視している．アクセス制御は，アクセス権限が無い者による不正アクセスを防ぐことができる．しかし，アクセス権限が与えられた者による機密情報の不正利用を防止できない．従って，内部不正の脅威をアクセス制御だけで対応することは難しい．

そこで，本論文は，犯罪の防止における知見を応用して内部不正の脅威について研究する．犯罪の防止に関する取り組みは元来，非行，低い学歴，家庭環境などが悪意のある内部犯に変容するを重視してきた [12]．しかし，最近では環境犯罪学の理論に基づいた取り組みが進んでいる．環境犯罪学は犯罪を取り巻く環境や状況を重視した対策をしている．身近な事例としては，

- 犯罪が多発する地帯には監視カメラを多数設置する
- コンビニエンスストア内の犯罪を防ぐためにレジの様子を店外からガラス越しにみえるようにする

といったものがある．しかしながら，ベネッセ社の事故において元社員の職場は，

- 管理者が不在になることが多く，管理者による監視が行き届いていない
- 容易に情報を外部へ持出可能な端末がある

という環境であった．環境犯罪学ではこれらの環境や状況が内部不正を誘発する要因となる．組織の環境要因によって，従業員が悪意のある内部犯に変容したのであれば，当該要因をコントロールして変容を抑える必要がある．

[1] 独立行政法人情報処理推進機構

1.1.2 内部不正を誘発する要因

内部不正を誘発する要因

内部不正を誘発する要因については様々な研究がある．Cohen は,「ルーティンアクティビティ理論」を提唱し,「動機づけられた犯罪者」「潜在的な犯行対象物」「監視性の低い場所」が重なった場合に内部不正が生じるとしている [13]．Cressey は,「不正のトライアングル」を提唱し，人が「動機・プレッシャ」をかかえながら「機会」を意識しかつ「正当化すること」を考えつくときに不正行為が発生するとしている [14].

職場環境と内部不正の関係

社会安全研究財団 [15] の事例分析では，内部不正を誘発する要因として，

- 上司の社員に対する人遣いの荒さ（催促）
- 従業員に対する暴言に起因した強い不満・怒り（非礼）
- IT 業務に関する管理者が不在など（低監視）

などを挙げている．他にも数多くの要因が存在する [2]．これらの研究は，具体的にどの要因がどれくらいの内部不正を誘発する影響を及ぼすのかについては明らかにしていない．

アカウントの共有と内部不正の関係

上記で示した内部不正を誘発する要因以外にも，IPA は，内部不正を誘発するリスクが高い要因の 1 つとして，アカウントを複数のユーザで共有した状態を挙げている [16]．なぜなら，アカウントを共有することで，ユーザの匿名性が確保され，不正をしても特定されるリスクが低いとみなされるからである．Hausawi がセキュリティの専門家に対して行ったインタビューによると，従業員が行うセキュリティに対する最も危ない行動は「アカウントの共有（Sharing credential）」であった [17]．従って，アカウントの共有は内部不正を誘発する要因の 1 つと考えられる．

アカウントの共有とは，システムにログインする際に必要な認証情報（パスワード，IC カード）が複数のユーザで共有された状態である．たとえば，以下のような利用シーンがある．

- システム開発のチームがメンバ間でサーバにアクセスするための特権アカウントを共有する
- コールセンタの従業員が機密情報にアクセスするアカウントを共有する

アカウントの共有とユーザごとの操作記録の関係を図 1.1 に示す．個別アカウントを利用する場合，ユーザ A，ユーザ B，ユーザ C は，それぞれ自分のアカウントを利用してシステムにアクセスする．この場合，システムは各ユーザの操作を記録している．そのため，各ユーザが個別アカウントを利用した操作は，操作記録のアカウント名を確認することでユーザごとに操作記録を識別することができる．一方，ユーザ A，ユーザ B，ユーザ C が共有アカウントを利用しシステムにアクセスした場合，システムは共有アカウントの操作を記録しているが，誰が操作したのかは記録できない．代表的な共有アカウントには Guest ユーザ，Administrator ユーザがある．後者は特権的権限が付与されていることが多く，アカウントを複数ユーザで共有している場合，特に問題

[2] 詳細は 2.3.5 項参照

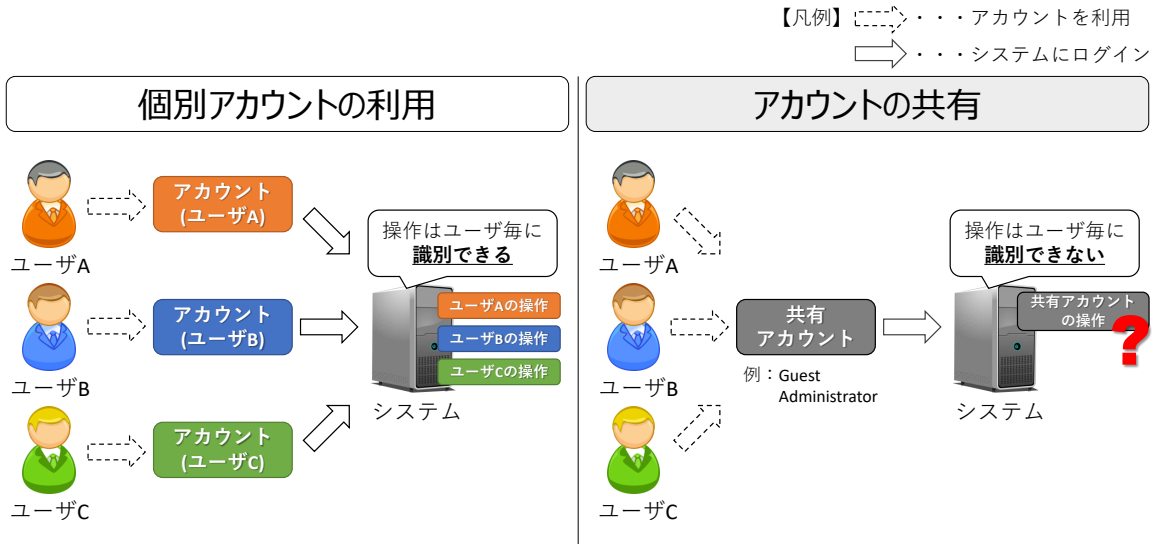

図 1.1: アカウントの共有とユーザごとの操作記録の関係

となる．特権的権限は，システム上の全てのデータへの参照，更新，持出，削除などの操作やプログラムの更新，シャットダウンなどが可能な権限である．この権限を付与された共有アカウントで機密情報の漏えい事故が発生した場合，操作記録から情報漏えい事故の犯人を識別することができなくなる．このように自らの操作であるか断定ができない状態は，悪意のある内部者に対して内部不正を誘発する要因の 1 つになる．しかしながら，どこまで内部不正の発生に影響を及ぼすのかは明らかになっていない．

内部不正を誘発する要因の影響の大きさに関する従来研究の課題

内部不正を誘発する要因を影響の大きさを識別することを目的として，いくつかのアンケートやインタビュー調査が実施されている．竹村らはセキュリティポリシ違反の意図に影響を与える個人属性や職場環境要因を明らかにするため，アンケート調査を実施した [18]．島らは組織の内部犯による不正行為に対しての有効な対策について，アンケート調査を行った [20]．IPA は内部不正に関する企業の実態調査を行い，従業員が最も内部不正への気持ちが低下する対策について調べた [10]．これらの調査は，どのような対策をとった場合に，従業員による内部不正が発生するリスクを低減できるかについて示している．しかし，内部不正に関するアンケートやインタビュー調査では，調査結果に真意が反映されていない可能性があった．図 1.2 はユーザの本心と回答が異なるケースを示す．図 1.2 のユーザ A は，本心では内部不正を誘発する要因が要因 C だと考えているが，自身が回答した内容により，今後の自らの社会生活に悪影響を及ぼすことを懸念して，本心を伝えたくないと考えている．その結果，要因 C の回答を「低」と回答する．このように調査対象者の回答が真意と異なる可能性があると想定される．

1.2 本研究の目的

本研究の目的は，以下のとおりである．

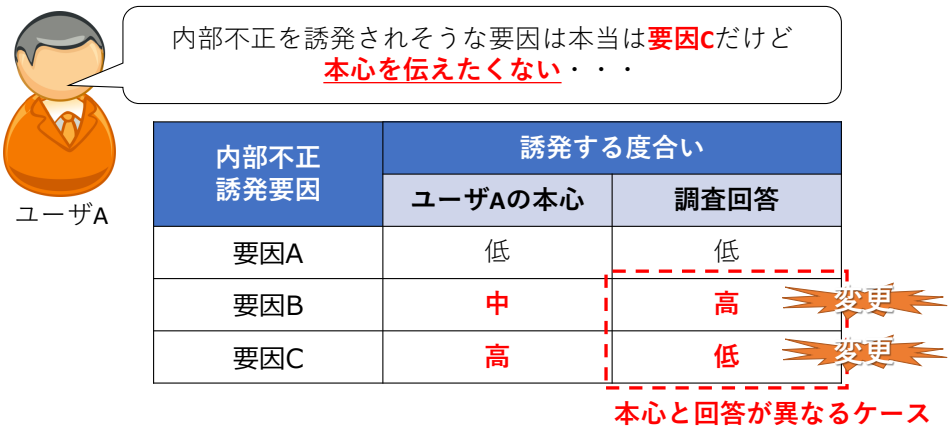

図 1.2: ユーザの本心と回答が異なるケース

(目的 1) 組織における環境や状況が内部不正を誘発する影響の大きさを明らかにすること

以下の 3 つを対象とする.

- 催促
- 非礼
- 低監視

これらは，一般的な職場環境で生じる誘発要因の例である．これらの関係を図 1.3 に示す.

図 1.3: 目的 1 の対象とする内部不正誘発要因

催促は，内部者が管理者から仕事の催促をされた状況である．図 1.3 では，管理者が「早く仕事をしろ！」と内部者に催促をしている．非礼は，管理者から非礼な言葉を言われた状況である．図 1.3 では，社長が「こんなこともできないのか！」と内部者に暴言を浴びせている．低監視は，従業員の職場環境において監視の目が届かない環境のことである．図 1.3 では，監視者が内部者のことを監視していない.

「催促」,「非礼」,「低監視」といった状況や環境をなくすことで，内部不正の発生リスクを低減させることが期待できる．そのため,「催促」や「非礼」自体は必要最小限とするべきであるが，こ

れらを全て禁止してしまうと，組織に対して別の負の影響を及ぼす可能性がある．たとえば，業務上における催促を行えないと，組織において従業員のマネジメント手法が制限され，生産性の低下などにつながる可能性がある．また，監視が低い状態をなくすために大量に監視者を割り当てた場合，人件費の向上につながり，組織の生産性が低下してしまう．このように，内部不正を誘発する要因をなくすことによって様々な負の要素が発生する可能性がある．しかし，これらの要因がどれくらい内部不正を誘発する影響があるのかについては明らかになっていない．

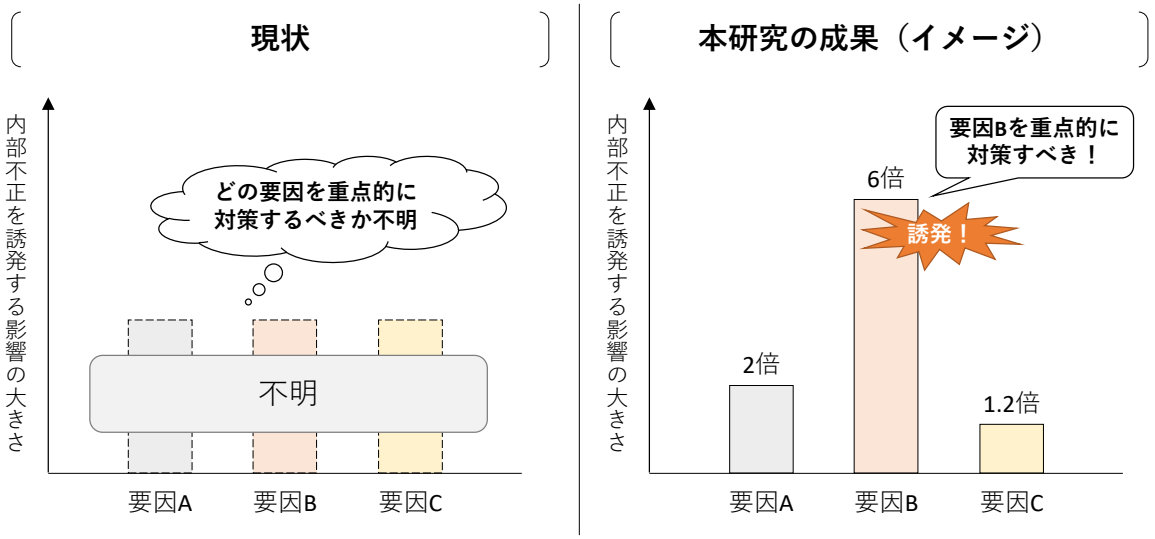

図 1.4: 内部不正を誘発する影響の大きさ（イメージ）

本研究における内部不正を誘発する影響の大きさのイメージを図 1.4 に示す．もし，要因 B が要因を何も与えなかった場合と比べて，内部不正を誘発する影響が 6 倍になることが本研究によって明らかになったとする．また，要因 A が 2 倍，要因 C が 1.2 倍であったと仮定する．この場合，組織が要因 B への対策は，要因 A への対策をとった場合と比べて，内部不正の誘発を低減させる確率を 3 倍下げる．このように，本研究は組織が重点的に対策するべき要因を明らかにすることができると考える．

(目的 2) アカウントの共有が内部不正を誘発する影響の大きさを明らかにすること

以下の 2 つを対象とする．

- アカウントの共有
- アカウント名の非表示

アカウントの共有を許すと，利用者の識別が困難になることから，従業員に “監視が低い” と感させることを想定した．アカウントの非表示は，利用者が自らのアクセスをシステムが記録していると認識する機会が少なくなり，“監視が低い ” と感じさせるものである．これらの要因は共有の影響を考えたときに無視できないため選定した．

目的 1 と目的 2 の対象とする内部不正誘発要因の関係を図 1.5 に示す．目的 1 は催促，非礼，低監視を対象とする．具体的には「管理者による催促」,「管理者による暴言」,「アクセスログの監視の未実施」について，内部不正を誘発する影響の大きさを明らかにする．目的 2 は「アカウント

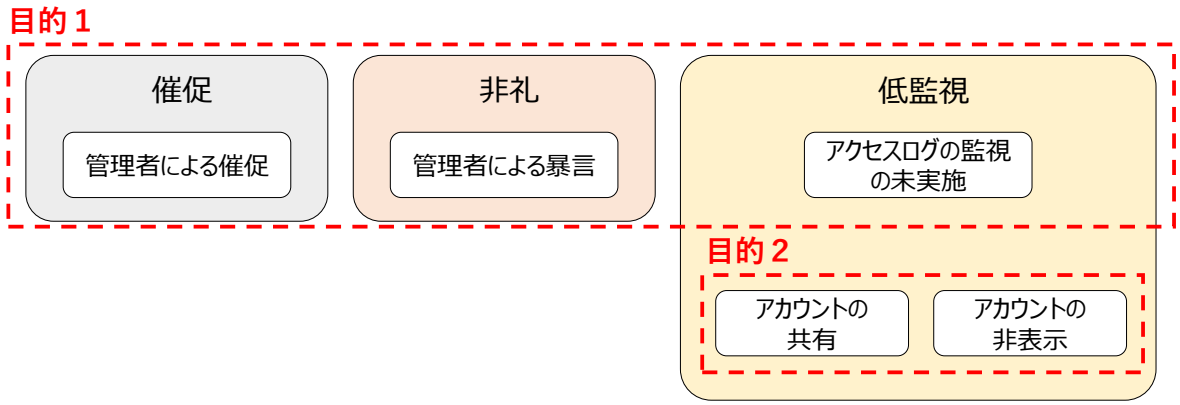

図 1.5: 目的 1 と目的 2 の対象とする内部不正誘発要因の関係

の共有」と「アカウント名の非表示」について，内部不正を誘発する影響の大きさを明らかにする.「アカウントの共有」と「アカウント名の非表示」も，低監視を細分化したものである.

1.3 本研究の困難性

目的 1,2 を達成するため，本研究は内部不正誘発要因の識別を試みる．この識別には以下の 4 つの問題点がある.

(問題点 1) 情報漏えい事故の観測の困難性

情報漏えい事故を観測することが難しい．目的 1，2 を達成するためには実在する組織において発生した情報漏えい事故を観測することが望ましい．しかし，第三者が情報漏えい事故を観測することは難しい．なぜなら，組織のセキュリティポリシに抵触する可能性があり，実現が難しいためである.

(問題点 2) 情報漏えい事故の不足に伴う分析データ収集の困難性

情報漏えい事故の発生頻度が低く，分析データの収集が難しい．地震などと同様に内部不正による大規模情報漏えい事故は頻繁に発生しない．長期間にわたってその過程を詳細に観察することも難しい.

(問題点 3) 内部不正を誘発する影響の大きさの測定の困難性

内部不正の誘発する影響の大きさの測定が難しい．1.1.2 項で述べた通り，従来研究は内部不正を誘発する影響の大きさをアンケートなどで調査しており，不正直な回答による誤差が混じる.

(問題点 4) アカウントを共有した被験者の識別の困難性

アカウントを共有した被験者を識別することが難しい．1.1.2 項で述べた通り，共有アカウントを利用した場合，システムは共有アカウントの操作を記録しているが，操作者が誰であるのかについてはシステムにて記録していない．アカウント以外の方法で，被験者の行動を一意に識別することは自明ではない．

1.4 本研究の着想

本研究は，1.3 項の困難性に対して，以下の着想によって解決する．

(着想 1) 軽微な不正事象の観測

問題点 1 を解決するため，情報漏えい事故の代わりに軽微な不正事象を観測する．1 件の重大事故・災害があれば，その背後には，29 件の軽微な事故，災害が起こり，300 件もの事故に至らなかった「ヒヤリ・ハット」した事案が発生することを示したハインリッヒの法則がよく知られている [21]．この法則は，医療現場などにおける事故の防止に用いられている [22]．本研究の疑似環境で発生する不正事象は，情報漏えい事故と比べて組織に与える影響は軽微である．たとえば，以下の条件に合った被験者の操作を不正事象とみなす．

- 作業の利用規約に定めた禁止事項に抵触する行動
- 疑似作業における依頼事項を未実施，または不完全なままで作業を終了

一方，ハインリッヒの法則を仮定すると，本研究で観測する不正事象の発生数は内部不正による情報漏えい事故の発生数に比例する．図 1.6 は本研究の不正事象と情報漏えい事故の関係を示す．対策がある場合，不正事象の数が少なくなり，図 1.6 の三角の幅が狭い．一方，対策がない場合，不正事象の数が多くなることから，図 1.6 の三角の幅は広い．図 1.6 は，三角の幅が狭くなれば内部不正による情報漏えいの発生数が少なくなることを示している．つまり，ハインリッヒの法則を仮定すれば，不正事象の数を減少させることで内部不正による情報漏えいの発生数を減らすことができると考える．

(着想 2-1) 不正事象を発生しやすい環境の構築

問題点 2 を解決するため，被験者にストレスを与える．そのため，疑似作業を遂行する環境を悪くして，多くの不正事象を発生させる．報酬を支払う条件で集まった被験者は，一般的に真面目に実験に取り組むことが想定される [3]．そこで，優良な被験者が不正事象を誘発するための仕掛けが必要となる．

Kelling ら [24] による「割れ窓理論」によると，荒れた街では犯罪の発生率が上がるといわれている．そこで，本研究では疑似環境に対して環境を悪くする仕掛けを設けることで被験者が多くの不正事象を発生させる．図 1.6 のように窓ガラスの割れなどの軽微な事例と殺人のような重大な事件とは比例すると仮定する．従って，環境 A と環境 B という異なる環境における軽微な不正の

[3] もし，被験者に報酬を支払わない場合，数多くの被験者を集めることは容易ではない．従って，数多くの不正事象が発生することを期待できない．

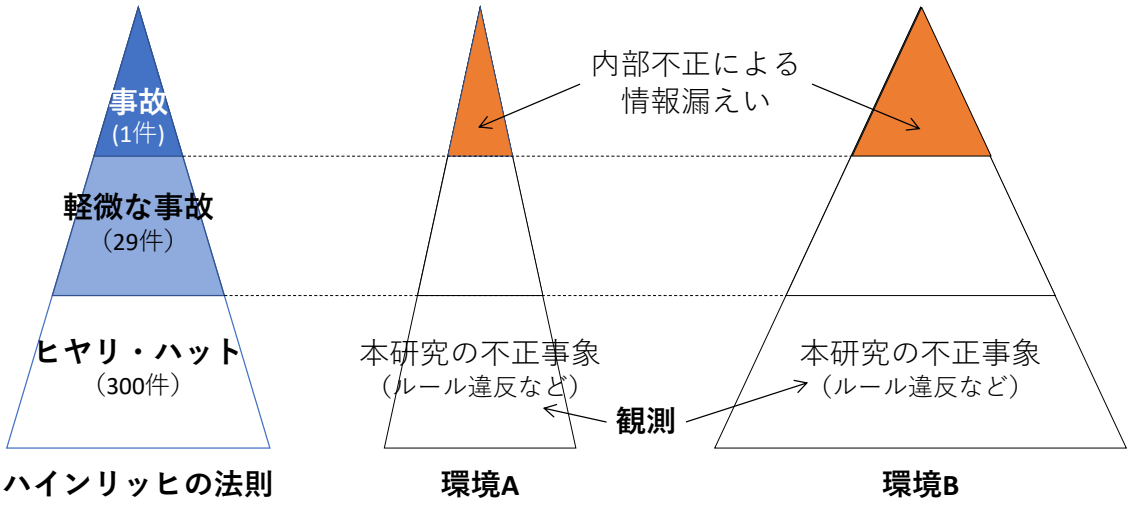

図 1.6: 本研究の不正事象と情報漏えい事故の関係

数を観測すれば，深刻な重大不正の数も予測できることと考える．この考え方は商品検査などで高温多湿の環境試験室で実験評価が行われることに似ている．たとえば，ストレスを与える例として下記のような仕掛けを設ける．

- e ラーニングの WEB サイト評価作業において，確認テストの結果を全員不合格として再受講を強制する
- WEB サイトに構築した検索エンジンの性能評価作業において，応答時間が著しく遅延する

(着想 2-2) クラウドソーシングサービスの活用による被験者の募集

被験者の募集方法には表 1.1 に示すいくつかの方法が考えられる．

(1) 簡単な実験であれば，知り合いに協力を依頼することが多い．この方法は多額の費用を必要としないため，広く利用されているが被験者の属性が偏ってしまう可能性がある．たとえば，大学内で被験者を募集した場合，被験者の属性は学生中心となってしまう．本研究は組織で発生する情報漏えい事故を対象としており，被験者は社会人が望ましい．従って，本研究におけるサンプルの対象として適正とは言い難い．

(2) 専門の調査機関に調査を委託すれば，社会人に対する調査が実現できる．しかし多くの被験者を集めた場合，調査費用は高額となる．また委託に際しては，契約手続きや被験者の募集に時間がかかる．

(3) クラウドソーシングサービスは様々なユーザが登録されており，多様な属性を持ったユーザの代表を抽出できる．また，他の方法と比べて短期間かつ安価で被験者が集まることが多い．

よって本研究では被験者はクラウドソーシングサービスによって集める．

表 1.1: 被験者の募集方法の比較（○や×などの評価は著者の主観による）

対象者	費用	実現性	迅速性	実環境との差
知人，友人	◎ 無償または安価	○ 可能	△ 個別依頼	△ 属性が限定される（知人，友人中心）
商用の調査機関の契約被験者	× 高額	○ 可能	△ 個別依頼	○ 多様な属性
クラウドソーシングサービスのワーカー	○ 安価	◎ 容易	◎ 最短数日	○ 多様な属性

表 1.2: 内部不正誘発要因の識別の困難性と着想

項番	困難性	着想
1	情報漏えい事故の観測	軽微な不正事象（ヒヤリ・ハット）を疑似環境で観測
2	情報漏えい事故の不足	不正事象を発生しやすい環境を構築（割れ窓理論），クラウドソーシングサービスの活用（十分な被験者数の確保）
3	内部不正を誘発する影響の大きさの測定	コホート研究の手法を応用したロジスティック回帰分析による分析
4	アカウントを共有した被験者の識別	被験者ごとに一意性のある作業データを与えて識別

(着想 3) コホート研究の手法を用いた行動分析

問題点 3 を解決するため，コホート研究の手法を用いた行動分析を行う [25].

被験者を 4 つのグループに分けて，異なる内部不正誘発要因を与える．グループ（内部不正誘発要因）ごと，属性ごとの不正事象数を測定する．そして，これらのグループ間の差が統計的に有意かどうかを明らかにするため，独立性の検定を行う．内部不正とは直接関係しない性別などの交絡因子の影響を調整して本質的な因子を識別するためにロジスティック回帰分析を行う．

(着想 4) 被験者ごとに一意性のある作業データを与えて識別

問題点 4 を解決するため，被験者ごとに一意に識別が可能な作業データを与える．被験者が入力したデータをすべて記録することで，入力されたデータからどの被験者の操作であるかを識別する．たとえば，検索エンジンの性能評価作業においては，評価において必要な検索キーワードを被験者ごとに異なるものを与えて，検索されたキーワードから被験者を識別する．1.3 項の困難性を上記の着想によって解決することが本研究の新規性の 1 つである．困難性と着想の関係を表 1.2 に示す．

1.5 本研究の貢献

本研究の貢献は次の 2 つである．

職場環境における内部不正を誘発する定量的で信頼できる影響の大きさを明らかにしたこと

従来のアンケート調査では誤差が混じるため，正確な評価が困難だった.「管理者による催促」,「管理者による暴言」,「アクセスログの監視の未実施」の 3 つの内部不正誘発要因の各々の影響の大きさを実験により定量的に観測したことである．内部不正誘発要因ごとの影響に有意な差が存在し，監視をしていることを警告しているグループに対して，警告をしないグループは不正を犯しやすいことを明らかにした.

アカウントの共有における内部不正を誘発する定量的で信頼できる影響の大きさを明らかにしたこと

従来の研究により，アカウントの共有が，内部不正を誘発することは経験的に知られていたが，その定量的な影響の大きさを測定したことである．本実験により共有 ID と個別 ID の差，つねにアカウント名が画面に表示される時と表示されない時の差を明らかにした．個別 ID が正規の ID であると，被験者は作業報酬に関わるものと強く感じ，不正行為を抑制する効果がある．フィッシャーの直接確率検定による独立性の検定およびロジスティック回帰分析により，共有 ID の利用により内部不正を引き起こす被験者の属性を明らかにした.

1.6 本研究の位置づけ

本研究の従来研究に対する位置づけを述べる.

1.6.1 内部不正誘発要因の影響の大きさの識別に関する従来研究

内部不正の誘発要因を識別に関する従来研究には，1.1.2 項で示した Hausawi，竹村らによる研究がある [17][18].

まず，本研究と従来研究の被験者数について述べる．丹後ら [25] は，2 つの母平均の差の検定（片側検定）で必要となる被験者数についての計算式を示した．その計算式によれば，必要な被験者数は「職場環境」（3 つの要因）と「アカウントの共有」（2 つの要因）の実験でそれぞれ 60 名，40 名である [4]．本研究における実験の被験者はすべて 100 名を超えており，必要な被験者数を満たしている．Hausawi は専門家に対するインタビュー調査であり，単純に比較できるものではないが，仮に同様の実験を行ったと仮定した場合，被験者の数は 31 名であるため，必要な被験者数を満たしていない．また，竹村らによるアンケート調査は 1507 名の被験者から回答を得ており，被験者数は必要な被験者数を満たしており，かつ本研究よりも多い.

識別対象の要因数についても本研究よりも従来研究の方が多い．本研究は被験者をいくつかのグループに分けて異なる要因を与えるため，要因数を増やすと，それだけ必要な被験者を増やす必要がある．本研究の要因数は「職場環境」と「アカウントの共有」の実験でそれぞれ 3 項目，2 項目である．一方，インタビュー調査やアンケート調査は各被験者にすべての要因の影響を尋ねることができる．Hausawi，竹村らの研究での要因数は，それぞれ 21 項目，45 項目である.

しかし，本研究は，従来研究と比べて内部不正を誘発する要因について，真の影響の大きさを明らかにすることが出来る．なぜなら，本研究は被験者には内部不正に関する調査という目的を

[4]計算式等の詳細は 5.2.5.1 項を参照

伝えることなく，被験者の行動を確認するためである．従来研究はインタビュー調査やアンケート調査によるユーザスタディであり，1.1.2 項で示した課題がある．そのため，調査結果が真意と異なる可能性がある．

内部不正を誘発する要因の識別に関する従来研究との比較を表 1.3 に示す．

表 1.3: 従来研究との比較（内部不正誘発要因の識別）

	本研究	従来研究 Hausawi[17]	 竹村ら [18]
調査方法	被験者の行動観測	インタビュー調査	アンケート調査
被験者	クラウドソーシングサービスのワーカー	情報セキュリティの専門家	調査会社のモニター
被験者数	○ 100 名（職場環境） 192 名（共有：予備実験） 198 名（共有：本実験）	△ 31 名	◎ 1507 名
要因数	△ 3 項目（職場環境） 2 項目（共有：予備実験） 2 項目（共有：本実験）	○ 21 項目	○ 45 項目
影響の大きさの識別	◎ 被験者の行動を確認できる	× 被験者の真意と異なる可能性がある（1.1.2 項）	× 被験者の真意と異なる可能性がある（1.1.2 項）

1.6.2 内部不正に関する行動分析の従来研究

内部不正に関する行動分析の従来研究は，Azaria らなどが行っている [23]（詳細は 2.4 項を参照）．被験者は本研究，Azaria ら共にクラウドソーシングサービスのワーカーである．

Azaria らの研究は被験者数が 795 名であり，本研究よりも多い．しかし，両者の被験者数については一概に優劣を決めることはできない．なぜなら，分析手法が大きく異なるためである．なお，Azaria らの研究における分析手法はサポートベクタマシンおよび単純ベイズ分類器である．機械学習の手法を使って，被験者の振る舞いを元に内部不正を犯した者を検知する．本研究の分析手法はロジスティック回帰分析である．被験者が疑似環境で発生させた不正事象と要因の関係を分析することで，内部不正を誘発する要因の影響の大きさを識別する．

また，両者は内部不正への対策の段階が異なる．Cappelli らは，内部不正への対策の段階を「防止」「検知」「事後対応」の 3 つに分類した [29]．ここで「防止」と「検知」の対策がリスクを低減する効果を比べてみる．「検知」の対策は内部不正の発生を防ぐことはできない．検知した段階では，既に内部不正による被害が出ている可能性がある．「防止」の対策は内部不正の発生を防ぐことができる．不正事象の発生を未然に防止できるため，「検知」より「防止」の方がリスクを低減する効果がより高いと考える．たとえば，サイバー攻撃を守るための対策として，A 社はブロック（防止）する対策をしており，B 社は攻撃を検知する対策のみをとっていたとする．両者が同じ攻撃を受けた場合，A 社は攻撃を受けずに済むが，B 社は攻撃を受けてしまう．本研究と Azaria ら

表 1.4: 従来研究との比較（行動分析）

	本研究	従来研究 (Azaria ら [23])
対策分類	内部不正の防止	内部不正の検知
研究対象	誘発要因の影響の大きさの識別	不正事象の検知
被験者	クラウドソーシングサービスのワーカー	クラウドソーシングサービスのワーカー
被験者数	100 名（職場環境） 192 名（共有：予備実験） 198 名（共有：本実験）	795 名
分析手法	ロジスティック回帰分析	サポートベクタマシン，単純ベイズ分類器
事故防止の効果	◎ 事故を未然に防止できる	× 事故が発生し，既に被害が出ている可能性がある

の研究の内部不正の対策の段階は，それぞれ「防止」,「検知」である．従って，本研究の方が情報漏えい事故を防止する効果が高いと考える．行動観測に関する従来研究との比較を表 1.4 に示す．

内部不正の誘発要因を行動分析の手法を用いて識別している点が，本研究の新規性の 1 つである．本研究の位置づけを表 1.5 に示す．

表 1.5: 本研究の位置づけ

アプローチ	ユーザスタディ	行動観測
内部不正の検知	N/A	Azaria ら [23]
内部不正の誘発要因の識別	Hausawi[17]，竹村ら [18]	本研究

1.7 本論文の構成

本論文は，6 章で構成される．1 章では，まず本研究の背景と目的を述べ，次に本研究の概要を示しその着想と貢献を述べた．2 章では，本論文を通して使用する基本定義を示し，関連研究の概要を述べる．3 章では，職場環境における内部不正を誘発する要因の影響の大きさを明らかにする．4 章では，アカウントの共有が内部不正を誘発する影響の大きさを明らかにするための予備実験の結果について述べる．5 章では，予備実験の結果をふまえ，改善を加えた本実験によってアカウントの共有が内部不正を誘発する影響の大きさを明らかにする．6 章では，本研究について結論づける．

なお，本研究においては 3 つの実験を行う．実験の名称は，被験者が行う疑似タスクの内容にあわせて「e ラーニング実験」「カレー実験」「検索実験」とする．実験名および概要は以下の通り．

e ラーニング実験（3 章）職場環境における内部不正誘発要因を識別するために行う実験．被験者の疑似タスクは，e ラーニング用 WEB サイトのモニター．

カレー実験（4 章）アカウントの共有における内部不正誘発要因を識別するために行う予備実験．被験者の疑似タスクは，カレーライスによるアンケートと PDF ファイルのテキストデータ入力．

検索実験（5 章）アカウントの共有における内部不正誘発要因を識別するために行う本実験．被験者の疑似タスクは，検索エンジンの性能評価．詳細は 5 章参照．

図 3.1 に本論文の章の構成を示す．

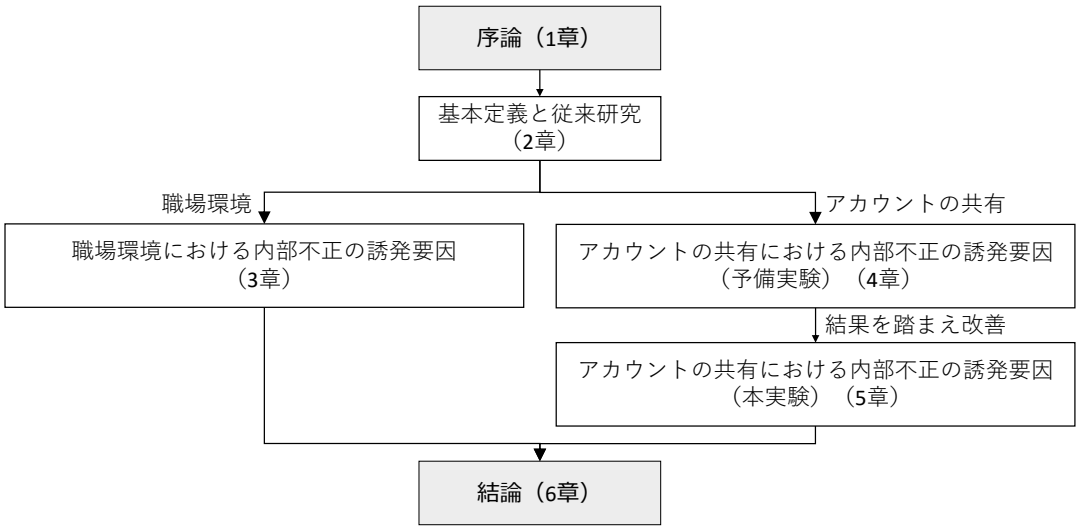

図 1.7: 本論文の構成と各章の関係

第2章　基本定義と従来研究

本章は，本論文において用いる用語の定義，内部不正による情報漏えいの定義，内部不正の検知および防止，行動分析などの従来研究を述べる．

2.1　用語の定義

IPA は，組織，内部者を以下のように定義した．本論文はこの定義を用いる [16].

組織 企業、地方公共団体等の法人その他団体とする。

内部者 従業員又は、従業員であった者のうち、以下の 2 つのどちらかでも満たした者とする．

・組織の情報システムや情報（ネットワーク、システム、データ）に対して直接又はネットワークを介したアクセス権限を有する者

・物理的にアクセスしうる職務についている者（清掃員や警備員等を除く）

2.2　内部不正による情報漏えいの定義

本論文の内部不正の情報漏えいの定義を定める上で，関連する従来研究を以下に示す．

- 職業上の不正の体系図 [30]
- 情報セキュリティインシデントに関する調査 [6]
- 内部者による脅威[1] の定義 [29]

2.2.1　職業上の内部不正の体系

不正とは，三省堂 大辞林では以下のように定義される [26].

> “正しくないこと．正当でないこと．また，そのさま．
> 「－を働く」「－な行為」「－乗車」”

また，不正行為の定義は以下のとおりである．

> “正しくない行為，道義にはずれたおこない．”

公認不正検査士協会 [30] は，組織内の不正について「職業上の不正と濫用 不正の体系図」(Fraud Tree) を提案している．この体系図では，職業上の不正を「資産不正流用」,「汚職」,「財務諸表不正」の 3 つに分類する．各カテゴリーの定義を次に示す．

[1] Insider threat

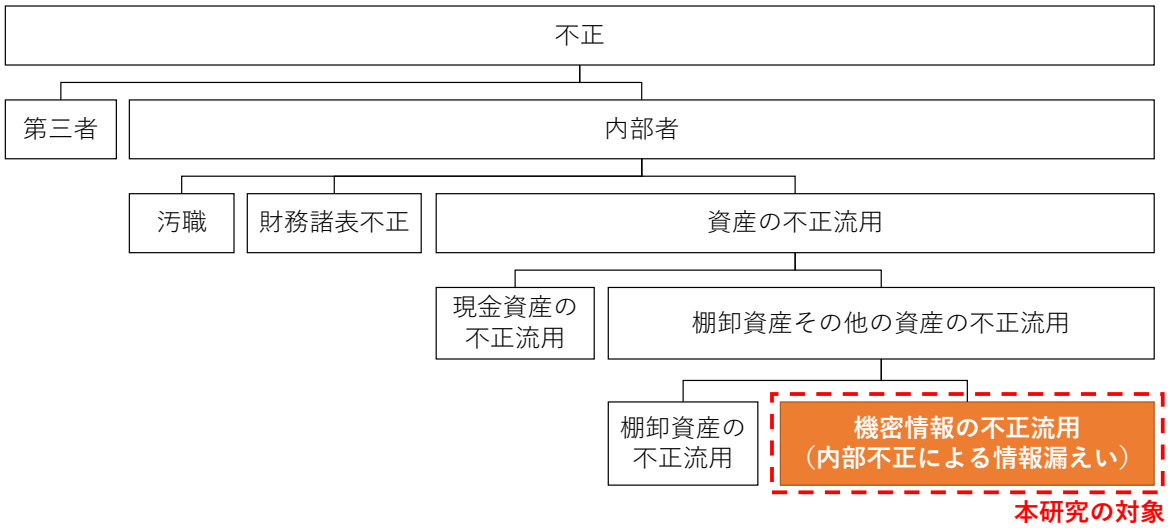

図 2.1: 職業上の不正における機密情報の不正流用の位置づけ (文献 [30] を基に加筆修正)

- 資産不正流用

  従業員による組織の資源の窃盗や悪用.（例：現金窃盗，請求書不正，経費報告書の水増し）

- 汚職

  直接的または間接的利益を得るために，従業員が雇用主に対する義務に反して商取引における自らの立場を悪用する不正スキーム.（例：賄賂または利益相反を伴う不正）

- 財務諸表不正

  従業員による組織の財務情報の意図的な虚偽記載と不作為である.（例：収益過大計上，経費の過小計上，資産の水増し計上）

資産不正流用は，現金預金と現金以外の資産に分類される．現金以外の資産の不正流用とは，勤務先の非現金資産を着服または悪用することである．たとえば，従業員が倉庫から棚卸資産を着服したり，従業員が顧客の機密情報を盗む，漏えいさせることである．組織内の不正における機密情報の不正流用の位置づけを図 2.1 に示す．本研究における内部不正の情報漏えいは，この「機密情報の不正流用」の一部だと考える．

2.2.2 情報セキュリティインシデントにおける内部犯罪・内部不正行為

JNSA[2] は，情報漏えい事故の情報漏えい原因を 11 の区分に分類している [6]．この分類では，情報漏えいの主体に応じて

- 第三者
- 組織内部

に分類する．第三者による情報漏えい原因には「設定ミス」「バグ・セキュリティホール」「ワーム・ウィルス」「盗難」がある．また，組織内部は情報漏えいの意図に応じて，

[2]日本ネットワーク・セキュリティ協会

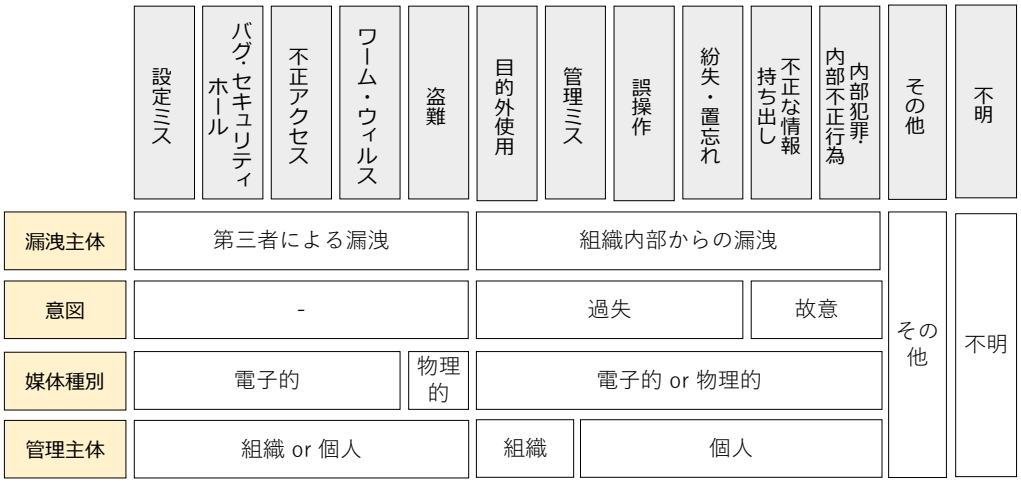

図 2.2: 情報漏えい原因区分（文献 [6] を基に作成）

- 過失
- 故意

に分類する．過失とは，情報漏えいの意図はないがヒューマンエラーなどが原因となって情報を漏えいしてしまうことである．過失による情報漏えい原因には「目的外使用」「管理ミス」「誤操作」「紛失・置き忘れ」がある．また，故意による情報漏えい原因には「不正な情報持ち出し」と「内部犯罪・内部不正行為」がある．これらの関係を図 2.2 に示す．

次に,「不正な情報持ち出し」と「内部犯罪・内部不正行為」の定義を以下に示す [6].

- 不正な情報持ち出し

  業務上の必要性などから，ルールを逸脱して情報を持ち出した場合が該当する．

  社員がルールを逸脱して機密情報を自宅に持ち帰り，ファイル交換ソフト経由で漏えいした場合も不正な情報持ち出しに分類する．たとえば，社員，派遣社員，外部委託業者，出入り業者，元社員など が，顧客先，自宅などで使用するために情報を持ち出して，持ち出し先から漏えいした事案などがある．

- 内部犯罪・内部不正行為

  社員，管理下にある他社社員 (派遣社員など) が，不正アクセス，その他不正な行為によって情報を持ち出して悪用した場合が該当する．

  外部の人間との結託や不正アクセスを伴う場合も，内部の人間の積極的な不正行為があれば内部犯罪・不正行為に分類する．たとえば，社員・派遣社員など内部の人間が，機密情報を悪用するために不正に取得して持ち出したり，持ち出した情報を使って犯罪を行ったり，売買したりして，漏えいした事案などがある．

両者と大きな違いは，業務上の必要性の有無である.「不正な情報持ち出し」は，ルールを違反して情報を持ち出す行為であり内部不正といえる．しかし，業務上の必要性から機密情報を持ち出しており，既に内部不正を誘発する主要な要因が明らかになっている．そのため，本研究の対象外とする．

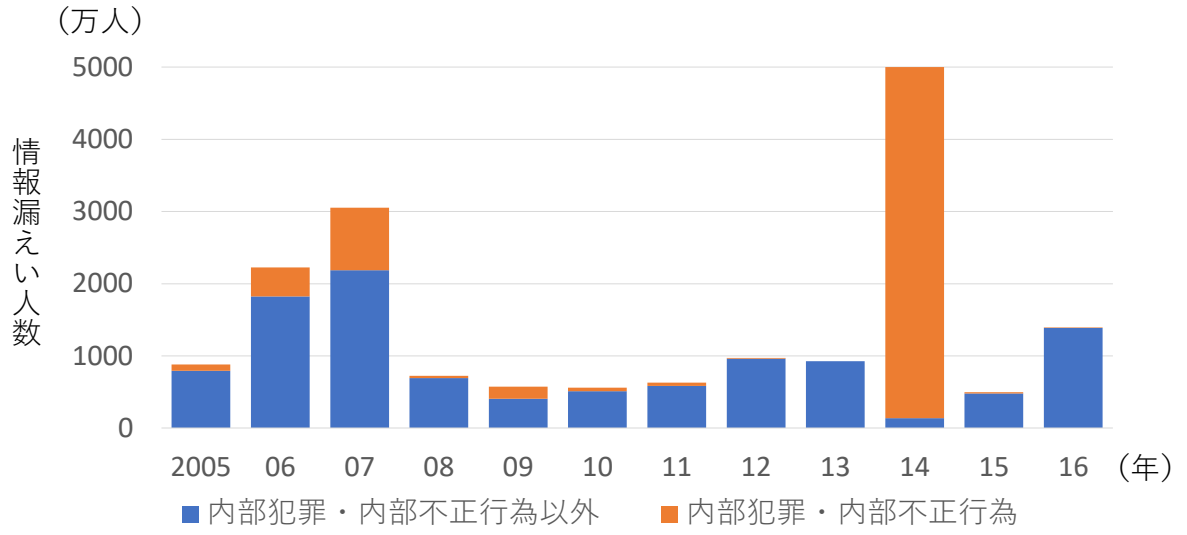

図 2.3: 内部犯罪・内部不正行為による漏えい人数の経年変化（文献 [6] を基に描画）

次に，内部犯罪・内部不正行為の情報漏えい事故の発生状況について示す．JNSA は，2005 年から 2016 年までの 12 年間の情報漏えい事故を分析した [6]．内部犯罪・内部不正行為を原因とした漏えい人数の経年変化を図 2.3 に示す．

漏えい人数全体に対する内部犯罪・内部不正行為による漏えい人数は，全体に占める割合は少ない年が多い．たとえば，2016 年は約 8 万人（0.6%）であった．しかし，2014 年は 1 年間で起こった情報漏えい事故のうち内部犯罪・内部不正行為による漏えい人数は約 4864 万人である．これは全体の 97.3%に相当する．この年の漏えい人数の大半はベネッセ社による大規模情報漏えい事故によるものである [4]．鈴木らは 2005 年から 2011 年に発生した情報漏えい事故の発生状況を分析したところ，大規模な個人情報漏えい事故の発生回数は少ないが，頻度がゼロになることはないことを示した [7] JNSA は，情報セキュリティインシデントの想定損害賠償額の算定式を示している [8]．この式によれば，大量の個人情報が漏えいした場合，多額の損害賠償をせざるを得ない事態に陥る可能性がある．たとえば，ベネッセ社の事故においてもお詫び金の支払いや損害賠償への対応を行っている．このように大規模な情報漏えい事故策等の対応にも多額の費用がかかり，企業活動に大きな影響を及ぼす．従って，内部不正への更なる対策をとることが重要となる．本研究における内部不正の情報漏えいは，この「内部犯罪・内部不正行為」と包含するものである．

2.2.3 内部者による脅威の定義

従来，組織は第三者による情報漏えいの脅威を前提とした対策を講じていた．しかし，米国では内部者による脅威（Insider threat）による情報漏えい対策の様々な研究が行われている．そのため，内部者による脅威の定義は様々なものが存在する [28][28]．その中でもカーネギーメロン大学の Cappeli らによる内部者による脅威の定義を以下に記す [29]．

- 現在もしくは過去の従業員，請負業者またはビジネスパートナー
- 組織の IT システム (ネットワーク，システム，データ) への正規に認められたアクセス権を持っている，もしくは持っていた者

- 意図的にそのアクセス権を用いて，組織の情報の機密性，完全性，可用性に対して負の影響をもたらした者

ここで，着目すべき点は組織の情報への負の影響を対象として，機密性，完全性，可用性の 3 つが含まている点である．情報漏えい事故は機密性への負の影響を及ぼすが，完全性や可用性は損なわれない可能性がある．

Cappelli らは，内部者による脅威によって生じる情報セキュリティインシデントを以下の 3 つに分類している [29].

- 情報破壊・システム破壊 (Insider IT Sabotage)

  主に管理者権限を保有した技術者が職場への復讐などを目的として，情報やシステムに対する破壊活動を行う．

- 知的財産窃盗 (Insider theft of intellectual property)

  従業員が新しい会社への転職等の際に業務上取り扱っていた知的財産情報を漏えいする．

- 内部詐欺 (Insider fraud)

  ヘルプデスクやカスタマーサービス等の従業員が主に金銭目的で行う．

情報破壊・システム破壊は組織における情報の完全性や可用性を低下させるものである．このインシデントは，情報漏えい事故と性質が異なる．さらに，実験的に被験者にこれらの破壊活動を誘発させることは難しい．そのため，本研究は完全性，可用性の影響は考慮しないこととする．

ところで，Cappeli らは米国の事象を勘案して，これらの分類を考案している．米国においては転職活動が盛んであることから内部者による知的財産窃盗の脅威は高い．一方，日本ではまだひとつの会社に長く勤めるケースが多い．従って，米国と比べると知的財産窃盗のリスクは低くなることが想定される．さらに，転職等により知的財産情報の漏えいが被験者にとって有益となる状況を再現することは困難である．

ベネッセの事案は，会社への転職による知的財産の窃盗を目的としたものではなく，金銭目的による情報漏えいであり,「内部詐欺」に該当すると想定される．国内では先述の事案発生に伴い,「内部詐欺」の脅威への対策が急務になっている．そこで本研究は「内部詐欺」の情報セキュリティインシデントの発生リスクを低減するため，本研究は組織の機密性に対して負の影響をもたらすもののうち,「知的財産窃盗」による影響を除いたものを対象とする．

2.2.4 本研究における内部不正の情報漏えいの定義

これらの従来研究を踏まえ，本研究における「内部不正の情報漏えい」の定義は以下の条件を満たすものとする．

- 対象者が下記に該当する．
  - 現在もしくは過去の従業員，請負業者またはビジネスパートナー
  - 組織の IT システムへの正規のアクセス権限を現在または過去に保持する者
  - 組織の機密性に対して負の影響をもたらした者（ただし，転職等における知的財産の窃盗を除く）．

表 2.1: 従来研究と本研究における内部不正の情報漏えいの関係

従来研究	本研究 対象（全てに該当するもの）	対象外
職業上の不正の体系図 [30]	機密情報の不正流用	現金資産，棚卸資産等の不正流用，汚職，財務諸表不正
情報セキュリティインシデントに関する調査 [6]	内部犯罪・内部不正行為	第三者による漏えい（盗難など），組織内部からの過失による漏えい（誤操作，紛失置忘れなど），不正な情報持ち出し
内部者による脅威の定義 [29]	機密性に負の影響をもたらした者	完全性，可用性に負の影響をもたらした者
内部者による脅威によるインシデント [29]	内部詐欺	情報破壊・システム破壊，知的財産窃盗

- 機密情報を第三者に漏えいする．
- 情報漏えいを意図的に行う．

従来研究と内部不正の情報漏えいの定義の関係を表 2.1 に示す．

2.2.5 内部不正の情報漏えいに対するアプローチ

Cappelli らは，従業員らの内部不正に対して組織が実施できる対策を「防止」「検知」「事後対応」の 3 種類に分類した [29]．Straub and Welke は，内部不正への対策を「抑止」「予防」「検知」「矯正」の 4 つのステップに分類した [31]．これらのアプローチは，多層防御の考え方に基づいており確実にリスクを低減できることが想定できる．

「事後対応」は被害を極小化するためには有用である．また「矯正」は内部犯に対する再発防止策になる．しかし，これらの段階では個人情報が第三者に漏えいした状態である．そのため，内部不正の発生を防止し，発生したとしても未然に検知することが重要となる．また，Straub and Welke の「抑止」「予防」は Cappelli らの「防止」と同じ概念であるとみなした．そこで，次に内部不正の防止，検知の従来研究を示す．

2.3 内部不正の防止

内部不正の防止は，次の従来研究がある．

環境犯罪学 職場環境や内部不正が発生する状況を改善し，内部不正の発生を抑制．

クラスタリング 内部不正に対する特徴をクラスタリングし，特徴に応じて最適な対策を適用．

組織文化 内部不正が発生しにくい組織文化を醸成．

全体像の把握 犯罪学，心理学等の知見を踏まえ，内部不正の全体像を整理．

誘発要因の分類 過去の事例などを基に内部不正を誘発する要因を分類．

誘発要因の影響の大きさ 内部不正を誘発する影響の大きい要因を識別．

2.3.1 環境犯罪学

環境犯罪学は，環境や状況等の改善を通じて犯罪や内部不正を防止することを試みる．元来，教育や家庭を重視する犯罪原因論と犯罪発生場面を重視する犯罪機会論がある [12]．たとえば，犯罪原因論の立場では不審な人への注意を呼びかける．犯罪機会論では危ない場所に注目する. 環境犯罪学は犯罪機会論の一つである [32]．環境犯罪学には，次の研究がある．

- 環境デザインによる犯罪予防 (Crime Prevention Through Environmental Design)[33]
- 守りやすい空間 (Defensible Space)[34]
- 状況的犯罪予防 (Situational Crime Prevention)[35]
- 割れ窓理論 [36]

Jeffery は，環境的に犯罪予防を行うことを理論付けた環境デザインによる犯罪予防（Crime Prevention Through Environmental Design）を提唱している [33].

CPTED は現在の防犯街づくりにおける主要な理論として，広く利用されている [38]．CPTED は建物，地域等の環境が抱える誘発要因を分析・排除するものである．たとえば，公園に面した道路には車両の速度を制御する仕組みや植栽を低くして道路から公園内の見通しを確保する等がある．また，コンビニエンスストアでは，レジを道路側から見えるような配置している．

Clarke は，状況的犯罪予防を提唱している [39]．状況的犯罪予防の詳細は，2.3.5 節に示す．

Kelling は，割れ窓理論を提唱している [36].

従来，犯罪原因論と犯罪機会論は対立するものとして扱われてきた．しかし，島田は犯罪原因論でも環境の影響は大きく，犯罪機会論でも犯罪者や潜在被害者の行動や意思決定など人間と環境との相互作用的視座が不可欠となると指摘する [46].

2.3.2 クラスタリング

ユーザ毎に最適化された対策を与えることで内部不正の発生リスクを低減する研究がある．ただ，個人毎に対策を真に最適化することは難しいため，実際には人々の内部不正に対する特徴をクラスタリングし，それぞれの特徴にあった対策パターンを適用することを試みる．

通常ユーザ毎の性格を識別するためにはアンケートやヒアリング等を行う必要があるが，Golbeck らは Twitter で個人が公開しているプロフィールを用いて，性格を予測している [47].

澤谷らはセキュリティリスク回避行動とユーザ要因に関するアンケート調査を実施し，特定のパーソナリティ要因を持つことや性別，認知傾向に応じて，セキュリティ回避行動をとるか否かを推定した [48].

大和田らは，従業員のリスク行動に対する情報セキュリティマップを提案した [49]．このセキュリティマップは，属性情報，勤務態度，IT 利用状況等を基に各従業員のリスク値を定量化し，リスクが高い従業員を類型化（グループ化）する．グループ毎の特徴を把握することで教育等を行う際の参考データとすることを狙っている．

2.3.3 組織文化

内部不正が発生しやすい組織とそうでない組織の間の違いに着目し，その要因の一つとして組織文化に着目する．組織文化に関するに研究を以下に示す．

- 日本企業における集団主義などの組織文化・組織風土 [41]
- 日本的雇用制度と内部不正行為関係 [42]
- 内部不正の意思決定伝染モデル [43]
- 組織的正義モデル [44]

浜屋らは，日本企業における集団主義などの組織文化・組織風土に注目した．情報セキュリティのルールからの逸脱行為については，形式的なルールを定めるだけでなく，組織文化・組織風土に合った対策を行うことが必要であることを示している [41].

北野は，従業者と組織の心理的関係からみた内部不正行為の抑止について，二要因理論を用いた従業員満足度と組織コミットメント，日本的雇用制度への姿勢を指標とした調査・分析を行った [42].

北野は内部不正の意思決定の感染モデルを提唱した [43]．このモデルは，笹井らによる社会ネットワーク上の感染症伝染モデルを基にしている [45]．このモデルにおいてノードを「従業者」とし，感染症を「不正行為の意思決定」と置き換えたものを図 2.4 に示す．

感染のサイクルは以下の通りである．

1. 不正行為がない
2. 従業者 A が不正行為の意思決定を行う（感染）
3. 不正行為を実行する（発症）
4. 従業員 B が不正行為の意思決定を行う（伝染）
5. 従業員 A は退職するが（隔離），従業員 B が不正を実行する

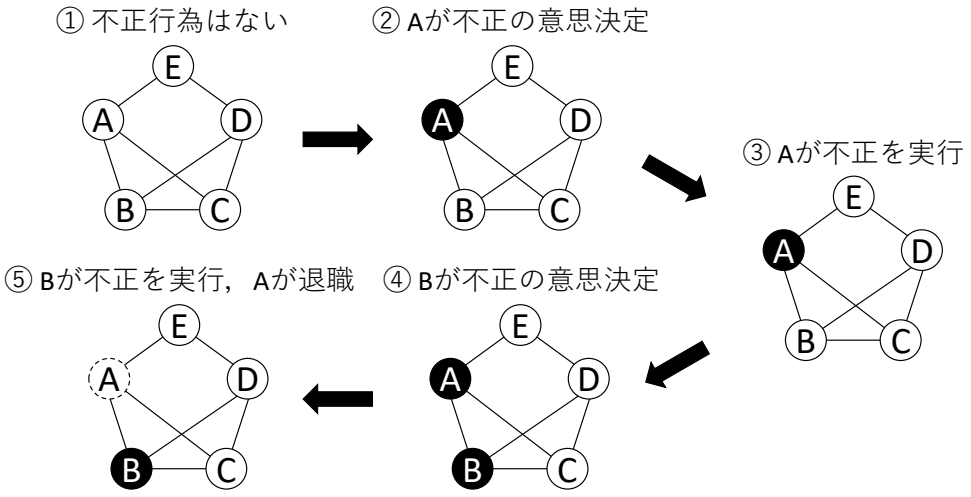

図 2.4: 内部不正の意思決定の感染モデル（文献 [43] を基に描画）

このサイクルが繰り返されることで，組織内で不正行為の意思決定と実行が広がっていく．

Willison と Warkentin は，さまざまな企業特性がどのように従業員の不満感を形成するかを理解しようとする ”組織的正義モデル ” を提案している [44].

2.3.4 内部不正の特徴の把握

内部不正を防止するための対策を検討するには，内部不正について十分な知見や洞察を持っておく必要がある．また，全体像を把握することができれば，事例への理解が深まる．そのため，不正者の心理的な特徴に焦点をあてた従来研究を以下に示す．

- 犯行者の心理的な力動過程（システムダイナミクス）[50][51][15]
- 内部不正の特徴に関するフレームワーク [52]

Capplli らは，MERIT[3] を提案している [53]．Cappeli らが行った調査ではシステムダイナミクスと呼ばれるシミュレーションの手法が用いて，行動や個人の特質が内部不正に繋がる共通パターンを整理した [50]．Fagade らは，システムダイナミクスの考え方に基づいて，内部不正のモデルを提案した [51]．日本では，社会安全研究財団が国内で 2007 年から 2009 年 6 月に検挙したサイバー犯罪 [54] のうち，内部不正を対象として事例分析を行い，犯行者のシステムダイナミクスを提示した [15]．また，Nurse らは，内部不正の特徴に関するフレームワークを提案している [52]．このフレームワークを筆者にて和訳したものを図 2.5 に示す．このフレームワークは，内部不正の特性をいくつかのグループに分けて説明するものである．グループは大きく分けて「きっかけ」,「攻撃者の特性」,「攻撃の特性」,「組織の特性」の 4 つに分類される．更に，攻撃者の特性は精神状態や攻撃に対する動機，スキル，機会，業務に対する態度，ふるまいの履歴等に分けられる．攻撃の特性は攻撃目的や攻撃方法など，組織の特性には資産 (WEB サーバ等) や脆弱性等が挙げられる．他の 2 つのモデルと異なり，予め確認すべき事象が定められているため，専門的な知識がない人でも使いやすいのが特徴である．

[3]Management and Education of the Risk of Insider Threat

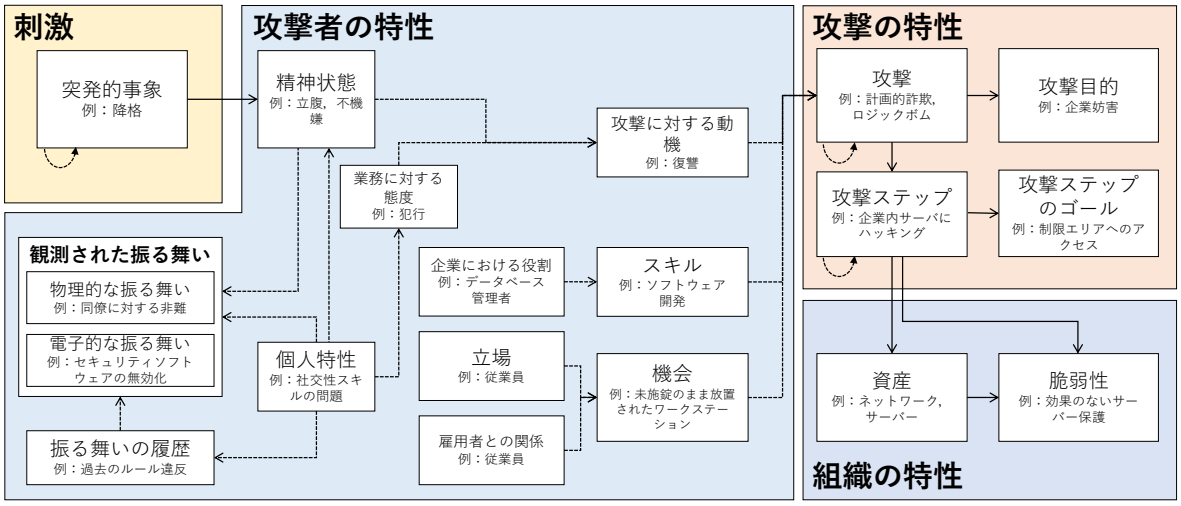

図 2.5: 内部不正の特徴に関するフレームワーク（文献 [6] を基に修正）

ただし，これらのツールはセキュリティ担当者や管理者が内部不正の問題を理解し，リスクを分析するためのツールとしてはよいが，どの誘発要因がより内部不正を誘発する影響については明らかにできていない．

2.3.5 誘発要因の分類

この節では，内部不正の誘発要因に関する従来研究を示す．なお，誘発要因の識別については 2.3.6 節で述べる．

- ルーティンアクティビティ理論 [13]
- 不正のトライアングル [14]
- 犯罪の状況的促進因子 [32]
- 状況的犯罪予防 [55][56][57]
- 内部不正の予測因子 [87, 59]

Cohen らはルーティンアクティビティ理論で，動機づけられた犯罪者，潜在的な犯行対象物，監視性の低い場所の 3 つの要因が重なった場合に内部不正が生じることを説明した [13].

Cressey は，動機・プレッシャーをかかえ，機会を意識し，正当化を考えつくときに不正行為が発生するとし,「動機・プレッシャー」,「機会」,「正当化」の 3 つの要因を不正のトライアングルとして定義し，内部不正とその要因の関係を説明した [14].

Wortley は，周辺環境が犯罪的な反応を促進しうる 16 の状況的促進因子を提案した [32].

Cornish らは，都市空間における犯罪を直接的，間接的に防止，抑止する状況的犯罪予防を提唱している [55]．内田は，状況的犯罪予防の考え方が，情報セキュリティ対策にも役立つと指摘した [56]．IPA は状況的犯罪予防を情報セキュリティ分野に応用して内部不正防止の基本 5 原則と 25 分類を考案した [16]．これを表 2.2 に示す．

表 2.2 の情報セキュリティ分野における内部不正防止の基本 5 原則は以下の通りである．

表 2.2: 内部不正防止の基本 5 原則と 25 分類（文献 [16] を基に描画）

原則	分類	対策例
犯行を難しくする	対象の防御策を強化する	アクセス制御、パスワードポリシの設定、退職者の ID 削除、セキュリティワイヤーによる PC 固定
	施設への出入りを制限する	外部者の立ち入り制限、入退出管理
	出口で検査する	ノート PC 等の持ち出し検査、メールやネットの監視
	犯罪者をそらす	物理レベルに応じた入退制限
	情報機器やネットワークを制限する	未許可の PC/USB メモリの持ち込み禁止、SNS の利用制限、ホテル及び公衆の無線 LAN の利用制限
捕まるリスクを高める	監視を強化する	アクセスログの監視、複数人での作業環境、情報機器の棚卸し、モバイル機器の持出管理、入退室記録の監査
	自然監視を支援する	通報制度の整備
	匿名性を減らす	ID 管理、共有アカウント廃止、台帳による持出し管理
	現場管理者を利用する	単独作業の制限
	監視体制を強化する	監視カメラの設置、機械警備システムの導入
犯行の見返りを減らす	標的を隠す（存在がわからない）	アクセス権限の設定、モバイル機器等の施錠保管、覗き見防止フィルムの貼付
	対象を排除する（存在をなくす）	データの完全消去、記録媒体等の物理的な破壊、関係者に開示した情報の廃棄・消去
	所有物を特定する	情報機器及び記録媒体の資産管理
	市場を阻止する	警察への迅速な届出、（法制度対応）
	利益を得にくくする	電子ファイル・ハードディスク・通信の暗号化
犯行の誘因を減らす	欲求不満やストレスを減らす	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進
	対立（紛争）を避ける	〃
	感情の高ぶりを抑える	〃
	仲間からの圧力を緩和する	〃
	模倣犯を阻止する	再発防止策（インシデントの手口の公表を慎重にする）
犯罪の弁明をさせない	規則を決める	基本方針の策定、管理・運用策の策定、業務委託契約、就業規則させない
	指示を掲示する	基本方針の組織内外への掲示、教育による周知徹底
	良心に警告する	管理レベルの表示、誓約書へのサイン、持ち込み禁止のポスター
	コンプライアンスを支援する	順守事項や関連法などの教育
	薬物・アルコールを規制する	職場での飲酒禁止、重要情報所持時の飲酒制限

- 犯行を難しくする

表 2.3: 内部不正の誘発要因の分類に関する従来研究

研究	分類	名称	要因数	代表例
Cohen ら [13]	一般	ルーティンアクティビティ理論	3	動機，犯行対象物，監視性の低い場所
Cressey[14]	一般	不正のトライアングル	3	動機・プレッシャー，機械，正当化
Wortley ら [32]	一般	犯罪の状況的促進因子	16	
IPA[16]	情報セキュリティ	内部不正防止の基本 5 原則と 25 分類	25	欲求不満，ストレス，対立，感情の高ぶり，模倣犯など
Greitzer ら [87, 59]	情報セキュリティ	内部不正の予測因子	12	不満，批判への反発，低い評価，ストレス，常習的な欠勤など

- 捕まるリスクを高める
- 犯行の見返りを減らす
- 犯行の誘因を減らす
- 犯罪の弁明をさせない

さらに各原則にはそれぞれ 5 つの分類がある．たとえば原則 4「犯行の誘因を減らす」には

- 欲求不満やストレスを減らす
- 対立（紛争）を避ける
- 感情の高ぶりを抑える
- 仲間からの圧力を緩和する
- 模倣犯を阻止する

の 5 分類が示されている．これらの対策は内部不正を抑止，防止する効果が期待できるが，実施しない場合には内部不正を誘発する要因になるだろう．しかしながら，これらの要因への対策をとった場合，組織は業務効率や業績の低下を招くおそれがある．たとえば，分類「匿名性を減らす」のためにパソコンの持出し管理を厳格に実施すれば，外出時に業務に関連する情報にアクセスすることが難しくなり，業務の効率が低下する．もし，分類「施設への出入りを制限する」のために入退出管理を厳格に実施すれば，新たに警備員等の雇用，入退室管理システムの導入等の対応が必要となり，コストが増加する．

Greitzer らは，心理学とベイジアンネットによる分析から情報セキュリティにおける内部不正を起因する 12 の予測因子を提唱した [87, 59].

内部不正の誘発要因の分類に関する従来研究を表 2.3 に示す.

これらの研究は，内部不正の誘発要因を理解するうえでは有用である．しかし，実際に対策を講じようとした場合，何から優先的に手を付けるべきかを示唆するものではない．また，すべての対

策を講ずることは現実的に困難なケースも存在する．いくつかの要因のうちどれが不正事象の発生に本質的な影響を与えるものであるか，より大きな影響を受けるかについては不明確であった．

2.3.6 誘発要因の影響の大きさ

内部不正を誘発する影響が大きい要因を識別する研究は，以下の通りである．

- 島らのアンケート調査 [20]
- 竹村のアンケート調査 [18]
- IPA のアンケート調査 [10]
- Hausawi のインタビュー調査 [17]

島らが行ったアンケート調査によると，組織の内部犯による不正行為に対して有効な対策は人事評価，勤務管理，対人関係に関する職場環境を改善することであった [20].

竹村らはセキュリティポリシー違反意図に影響を与える個人属性や職場環境要因を明らかにするため，アンケート調査を実施し，不正・違反放置の風土がセキュリティポリシーの違反を犯すひとつの要因であることを示した [18].

IPA が行った内部不正に関する企業の実態調査によると，従業員が最も内部不正への気持ちが低下する対策は社内システムの操作の証拠が残ることであった [10].

Hausawi は，エンドユーザが行うセキュリティに関する振舞いについてセキュリティ専門家に対してインタビューを行った [17]．インタビューの結果，エンドユーザが行う最も否定的な振舞いは認証情報の共有であった．この共有とは，たとえばシステム開発チームがサーバにアクセスする認証情報を共有したり，コールセンタのスタッフが機密情報にアクセスする認証情報を共有したりすることを指す．

これらの調査は，どのような対策をした場合に従業員が内部不正を発生するリスクが低減できるかを示している．一方，内部不正に関するアンケート調査については，今後の自らの社会生活に悪影響を及ぼすことを懸念し，回答者が真意と異なる回答を行ってしまう可能性がある．

2.4 内部不正の検知

内部不正の検知は，以下の方式がある．

- 異常検知（Anomaly Detection）
- Honeypots

2.4.1 異常検知

異常検知は，以下の方式がある．

- ELICIT[61]
- ELICIT の追加実験 [62]
- ユーザの振舞いの異常検知システム [64]
- BAIT(Behavioral analysis of insider threat)[23]

Maloof らは，端末の操作ログから内部犯を検知する ELICIT システムを提案している [61]．当該システムは，実在する組織のイントラネットで，red team（実験用の疑似内部犯）による典型的な情報搾取活動の操作履歴を内部犯として記録し，3900 名のユーザの操作履歴を正常者として記録した．操作履歴をもとに内部犯の特徴をベイジアンネットワークにより分析した．当該研究は，想定した内部犯の振舞いをもとに内部犯を識別しているため，想定を外れた振舞いを検知できない．

Caputo らは，自らが所属する研究機関に所属する従業員を対象に ELICIT システム等を使った追加実験を行った [62]．彼らは被験者を 50 名の正常者と 25 名の疑似内部犯に分けて，振舞いを記録した．この研究は，より実在する内部犯に近い状況を再現しているが，特定組織の職場環境に依存しており汎用性に欠ける部分がある．

また，Legg らは個人毎の脅威を評価するためにユーザの振舞いの異常検知システム [64] を構築した．このシステムは，潜在的な脅威を識別するためにベースとなる振舞いから，観測された振舞いがどれだけ逸脱しているかを測定する．更に Legg は，この検知手法を使って，内部不正の検知をビジュアル的に見せるツールを提案した [65]．ツールにより監視者は検知結果がどのような分析から導き出されたのかを瞬時に把握することができる．

BAIT(Behavioral analysis of insider threat)

Azaria らは，悪意のある内部犯と正常者の振舞いの境目を明らかにするためのアルゴリズムを開発し，BAIT を提案した [23]．概要を図 2.6 に示す．

BAIT は以下の条件を想定して設計された．

- 内部犯と正常者の比率は極めて不均衡である．
- 訓練データ（内部犯の振舞い）はほとんどない．
- 内部犯による振舞いは過去の研究で報告されたパターンではなく，実際の人間によって行われる．

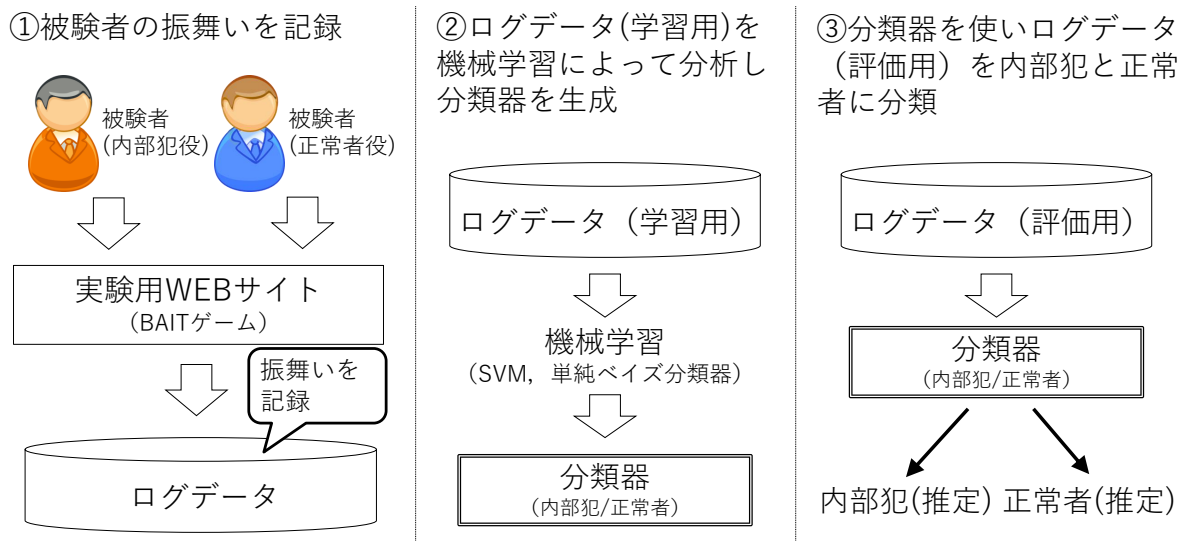

図 2.6: BAIT の概要 (文献 [23] を基に修正)

- 内部犯による振舞いは，通常の振舞いと並行して行われる．

BAIT では，7 つのアルゴリズムを検討した．5 つはサポートベクター マシンの上に構築され，2 つは単純ベイズ分類器を活用した．

これらのアルゴリズムを検証するため，Azaria は BAIT ゲームを設計した．このゲームは，AMT で集めた米国に在住する 795 名の被験者によって行われた．被験者は，AMT による作業の承認率 97%以上であり，かつ過去の 60 以上の作業を完了したものに限定した．また，被験者が真面目に指示に従うことを確認するために簡単なテストを行い，すべての被験者はこれに合格した．さらに，BAIT ゲームは非日常的なものであり，被験者にとって理解することが難しいと想定した．そこで，被験者がゲームを終えた後，彼らが支持を理解したのかどうかを確認した．そして，ゲームを理解していないまたはランダムな行動をした 101 名を除外した．

過去の研究では，内部犯を検知する際に正常者の振舞いについては実際のデータを使っていたが，内部犯の振舞いは人工的なデータを利用していた．これは，DARPA の ADAMS プロジェクトや ELICIT（Exploit Latent Information to Counter Insider Threats）プロジェクトなどで行われた [63][62]．BAIT ゲームにおいても実在する組織による検証はできなかった．

しかし，すべての被験者に内部犯か正常者のどちらかの役割を与えた．BAIT ゲームは，35 ラウンドで構成されている．被験者は 3〜5 つのタスクを受け取る．被験者は，これらのタスクについて情報を収集し，編集の上，タスクの依頼者に送信するように指示される．そしてすべての行動は監視されていることが伝えられる．内部犯の役割を与えられた被験者には，新たなタスク T が与えられる．タスク T は，たとえばミサイルの開発計画を依頼者に提供することである．彼らは，監視システムなどの検出の可能性を最小限におさえつつ，他のタスクをこなしながら，それらのデータを提供しなければならない．彼らは，このタスク T が最優先事項と告げられる．これらの営みは，日常のタスクと少量の悪意のあるタスクの両方を並行して実行する悪意ある内部犯の振舞いを疑似的に再現している．ゲームの各ラウンドでは，被験者は自分に割り当てられたタスクに関する 13 のアクションのうち，ひとつを実行することができる．アクションの例を以下に示す．

- 秘密の内部データベースから文書を取得
- 文書を送信するように同僚に依頼

- CD/DVD から文書を取得
- 暗号化された文書をタスクの依頼者に送信

これらを基にサポートベクター―マシンと単純ベイズ分類器で分析できる 28 の特徴量を定義した．特徴量は，16 の基本特徴量と送信アクションから派生した 12 の特徴量に分けられる．基本特徴量は，先述の 13 のアクションが該当する．3 つの送信アクションは外部送信と内部送信があるため，合計で 16 となる．送信アクションから派生した特徴量の例を以下に示す．

- すべての送信アクションの合計
- すべての外部の送信アクションの合計
- すべての外部の送信アクションを内部および外部の送信アクションの合計で割ったもの

これらのタスクで得られたログデータのうち，100 名の被験者のデータを使って，サポートベクター―マシン，単純ベイズ分類器のアルゴリズムによる分類器を生成した．また，残りの 594 名の被験者のログデータによって，分類器の精度を検証した．

Caputo らの研究と比べ，Azaria らは様々な背景を持った被験者を対象とすることで，汎用性のある検知システムが構築できたと考えられる．しかし，いずれの研究も不正事象の検知が目的となっており，不正事象の発生を誘発する要因を識別することは困難である．

2.4.2 Honeypots

Honeypots とは，おとりの機密情報等により内部犯をおびき寄せる手法である [66][67]．おとりの機密情報とは，主に実在しない顧客等の個人情報等を指す．Honeypots は，従来スパムメールの送信者を識別したり [68]，データの破壊や侵入を目的としたプログラムによる通信を検出したり [69]，クレジットカードの詐欺や ID 窃盗を識別するために利用されてきた [70]．Spitzner は，内部不正を検知するための Honeypots の応用手法として，Honeynets[71] と Honeytokens[72] を提案している．これらについて下記に示す．

Honeypots

Honeypots は，脆弱性の管理をわざと手薄にしたサーバ等を外部に公開し，攻撃者に侵入させ，その手口等を記録するものである．この Honeypots を内部ネットワーク向けに設置し，おとりの機密情報を格納することで，内部犯による情報搾取行為を検知することも可能となる．業務上，参照する必要がないものにアクセスすることはプライバシの侵害であり，不正行為と見なすことができる．しかしながら，Honeypots は不正行為の検知に対して受動的であり，内部犯がその存在を認識せずに実在する機密情報のみにアクセスしてしまう可能性がある．

Honeynets

Honeynets では，内部ネットワークを正常系とおとり系に分けて，おとり系の配下に多くの Honeypots を配置する．おとり系のシステム構成を正常系に近づけることで，より多くの内部犯をおびき寄せることができる．

Honeytokens

Honeytokens は，おとりとして利用する機密情報自体である．この機密情報には Word 文書，ログイン ID やパスワードのリスト，データベースのレコード等が含まれる．当該情報にアクセスがあった履歴をすべて記録する．

Brian らは悪意のある内部犯をおとりの機密情報によりおびき寄せる手法を提案している [73]. Honeynets，Honeytokens の手法は Honeypots の持つ受動的な側面を補完し，より多くの内部犯を検知することが期待できるが，やはり内部犯が存在に気付かずに犯行に及ぶ可能性がある．また，不正事象の発生を誘発する要因を識別することは困難である．

2.4.3 その他

豊田らは，PC 等の端末の操作ログから危険行動パターンに該当する操作を検出する方式を提案している [74]．危険行動パターンは情報漏えいの監査に従事する監査人が検討し，自治体職員 76 名から取得した操作ログにより，提案した方式の有効性を評価した．本方式は検出パターンを監査人の経験に基づいて生成している．検出アルゴリズムは，類似する行動の検知についても考慮されているが，未知のパターンに対応ができない可能性がある．

丸岡らはユーザが不正を行う際に横目で周囲を確認したり，心拍数が上がったりするといった挙動が現れることに着目し，被験者を集めて実験を行った [75][76]．これらの挙動は心理的状態に起因することから，内部犯が自ら制御することが難しく，内部不正の検知を回避することが比較的難しいことを示した．

Schultz [77] は，システムを攻撃しようとする内部犯を予測する行動因子を定義している．

システム上の逸脱した行動 たとえば，逸脱した行動とは不満を抱えた従業員が上司のメールボックスを匿名の人からの脅迫メールで溢れさせることが挙げられる．

ユーザーが犯した操作ミスの痕跡 たとえば，様々な機密情報をダウンロードしようとするユーザは，関連するログファイルを消去することができるが，後でユーザを識別するのに役立つユーザの操作ミスの痕跡（誤ったアクセスコマンドなど）を削除し忘れることがある．

準備動作 ユーザは nslookup，whois などの一連のシステムレベルのコマンドを使用して，内部不正の攻撃を行う前にシステムを監視することがある．

複数のネットワークやシステム間における疑わしい挙動 通常の疑わしい挙動ではなく，複数のネットワークやシステムの相関分析により初めて識別することができる疑わしい挙動がある．

憎悪に満ちた言動 管理者や同僚などに対して憎悪に満ちた言動を日常的に使う．

内向性の性格 外界よりもむしろ自己の精神生活に向ける性格は，内部不正を犯す可能性と相関する．

2.5 行動分析

最後に，情報セキュリティ分野における行動分析に関する先行研究について述べる．本論文において行う実験は，被験者をクラウドソーシングサービスのひとつである AMT で集めた．クラウドソーシングサービスは，学術分野においても利用が広がっている．金岡は，SOUPS（Symposium

on Usable Privacy and Security）で 2012 年から 2016 年に採録された論文におけるクラウドソーシングサービスを利用状況を調査した [78]．調査結果によると，5 年間で採択された論文 94 件のうち，47 件がクラウドソーシングサービスを利用していた．さらに AMT を利用したものは 27 件であった．

Fagan と Kahn は合理的な意思決定モデルを導入し，一般的なセキュリティアドバイスに従っている人とそうでない人の間でのギャップを特定した [79]．彼らは，既知のセキュリティ勧告，ソフトウェアの更新，パスワードマネージャ，二要素認証，および頻繁にパスワードを変更することに対する 290 の調査回答を収集した．

Leon はプライバシーの実践が，自らの行動データの収集を許可するユーザーと許可しないユーザとの違いについて調査した [80].

Shepherd らは，被験者を 5 つのグループに分けて，それぞれに別のパターンの警告画面を表示し，行動変容の影響が強いパターンが何かを識別した [81]．セキュリティのリテラシが低い人たちは，一定程度存在する．彼らが行うインターネット上の活動において不利益（ログインアカウントの奪取，脆弱性をついたハッキング）を被らないようにするため，WEB サイトの管理者は彼らの不適切な行動に対して，警告を出す必要がある．

Zimmermann らは，個人を識別，認証するためのいくつかの方式についてエンドユーザがどのような印象（好み，認証への負担，識別情報の漏えいへの懸念）を持っているのかについて調査した [82].

第3章　職場環境における内部不正誘発要因の識別

3.1　導入

本研究では実環境の代わりに職場環境を疑似的に再現したeラーニングサイトを用いた．eラーニングサイトでは，被験者を4つのグループに分けて異なる内部不正誘発要因を与えた．そして，グループ（内部不正誘発要因）ごと，年代ごと，成績ごとの不正事象数を測定した．さらに，これらのグループ間の差が統計的に有意かどうかを明らかにするため，カイ2乗検定を行い，内部不正とは直接関係しない性別などの交絡因子の影響を調整して本質的な因子を識別するためにロジスティック回帰分析を行った．

3.2　実験計画

3.2.1　必要要件

不正事象を誘発する要因を識別するための必要要件を以下に示す．

- 被験者の振舞いを観測できる．
- ユーザごとに異なる誘発要因を発生できる．
- 不正事象の発生を観測できる．
- ユーザの挙動を仔細に記録できる．

そこで，本研究は，上記の要件を満たす架空のeラーニングサイトを構築し，被験者に対して様々な内部不正誘発要因を提供し，不正事象の発生数を観測した．

3.2.2　仮説

社会安全研究財団による事例分析 [15] では，内部不正を誘発する要因として，上司の社員に対する人遣いの荒さや暴言に起因した強い不満・怒り，IT業務に関する管理者が不在などをあげている．そこで，本研究では次の3つの仮説を立てる．
仮説 $H_{\text{催促}}$：頑張っているのに催促されると内部不正を犯す．
仮説 $H_{\text{非礼}}$：暴言を受け，荒い人遣いをされると内部不正を犯す．
仮説 $H_{\text{監視}}$：監視の目が届かないことが分かると内部不正を犯す．
これらを確かめるため，次項で示す実験を行う．

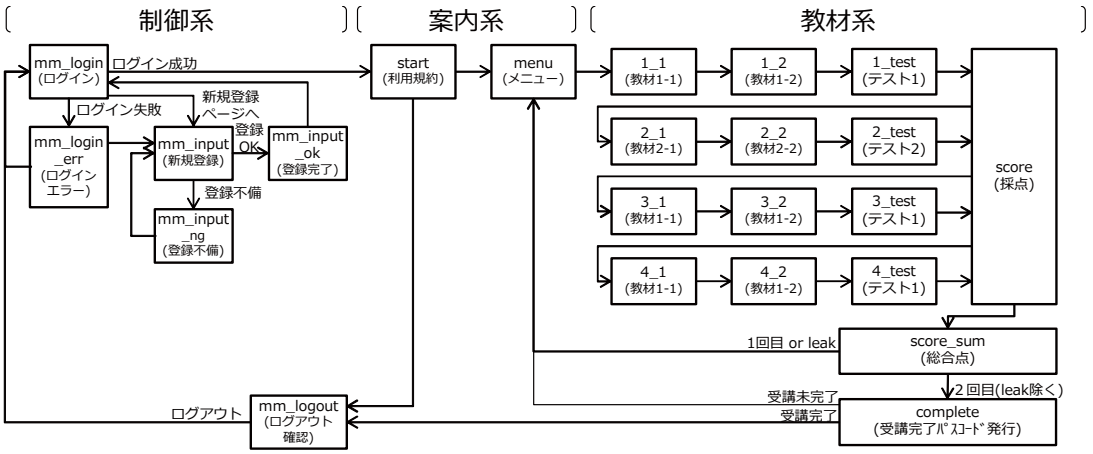

図 3.1: 画面遷移図（e ラーニング実験）

3.2.3 実験

3.2.3.1 概要

本研究の目的は国内の組織に雇用された従業員における内部不正を誘発させる要因を特定することである．国内におけるすべての雇用者を母集団とし，ランサーズ社のクラウドソーシングサービスに登録した優良ユーザのうち作業を完了した 100 名のユーザを標本とする．なお，被験者の質を確保するため，ランサーズ社で本人確認書類の提出が確認され，作業承認率が 95%以上であることを募集要件とした．当該ユーザはクラウドソーシングサービスにおいて募集した本実験（タスク）を完了した順番で先着順に抽出した．無作為抽出は実施していないが，クラウドソーシングサービスには様々なユーザが登録されており，多様な属性を持ったユーザの代表を抽出できると期待した．標本抽出の課題については 6.3 項で後述する．

実施期間は 2015 年 7 月 16 日～25 日の 10 日間である．

3.2.3.2 作業の流れ

被験者はランサーズ社から作業委託を受けて，筆者らが構築した e ラーニングサイト（以下，e ラーニング WEB サイトとする）が提供する教材を受講し，確認テストに回答する．受講完了後，e ラーニング WEB サイトは受講完了パスコードを発行し正規被験者を承認する．承認後，ランサーズ社は被験者に費用を支払う．これらの流れを図 3.2 に示す．

3.2.3.3 被験者グループ

e ラーニング WEB サイトは被験者がユーザ登録する際，受付順に通番を付与し，通番を 4 で割った余りの数（0～3）をもとにグループ（A～D）を決定する．表 3.1 に定める内部不正誘発要因を

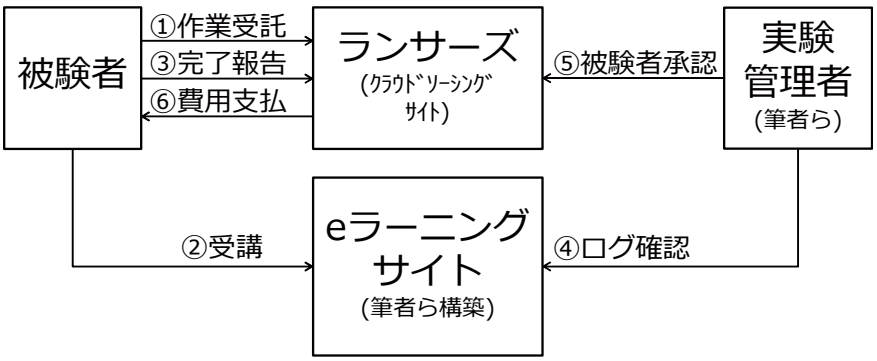

図 3.2: 作業の流れ（e ラーニング実験）

表 3.1: 内部不正誘発要因と対象グループ

仮説	内部不正誘発要因	一般的な事象	本実験での疑似事象	グループ			
				A	B	C	D
仮説 $H_{催促}$	催促文言	頑張っているのに正当な評価がされない	平均完了時間を当初より早める	○	-	-	-
仮説 $H_{非礼}$	失礼画像	上司の社員に対する暴言，人遣いの荒さ	1 回目の採点結果後の再受講案内を失礼な表現とする	-	○	-	-
仮説 $H_{監視}$	低監視	第三者からの監視性が低い	受講途中に不正に関する注意喚起を表示しない	-	-	○	-

発生させる．

3.2.3.4 e ラーニング WEB サイトのコンテンツ

e ラーニング WEB サイトの画面遷移を図 3.1 に示す．画面は制御系，案内系，教材系の 3 種類である．

制御系はユーザのユーザ登録，ログインチェックなどを行う．

案内系は利用規約などを表示させ，e ラーニング WEB サイトの依頼事項，禁止事項などを表示させる．

教材系は，学習教材，確認テスト，採点画面，総合点表示画面，受講完了パスコード発行画面から構成されている．学習教材は，総務省『国民のための情報セキュリティサイト』[83]，IPA の情報セキュリティ対策のしおり [84, 85, 86] を加工して作成した．確認テストは各章で 5 問ずつ出題し，計 20 問とした．満点は 1 問ごとに 5 点，章ごとに 25 点，総合点を 100 点とした．設問の難易度を高くすることで平均点を下げ，下記の工夫を行うことで不正事象を誘発させた．

- 記憶することが難しいものを出題する．
- 固有名詞を質問する（同じような名前のものの中から選択）．
- 回答方法をつど変更する [1]．

採点画面では各章の確認テストの採点結果を表示した．なお，正解が外部に出回らないようにするため，設問ごとの採点結果は表示せず合計点（25 点中 x 点）のみを表示した．総合点表示画面は各章の確認テストの合計点のみを表示し，詳細は非表示とした．

被験者の不正を通常よりも誘発させるため，グループごとの内部不正誘発要因とは別にグループ共通に次の内部不正誘発要因を与える．グループごとの内部不正誘発要因の詳細は 3.4.1 項に示す．なお，受講 1 回目の確認テストの採点結果を全員無条件 1 点減点し，なぜ減点されたのかを通知しないで全員不合格として再受講を指示する．なお，受講 2 回目では減点操作せずに 3.3.5 項に定める不正行為「答案未回答のまま回答」,「HTML ソースなどを確認して回答」を除き，全員合格とする．

3.2.3.5 不正事象の定義

e ラーニング WEB サイトの利用規約には次の禁止事項を記載した．

1. 教材を熟読しないで回答する．
2. 確認テストの回答の際に教材を閲覧する．
3. 教材の内容をブラウザに表示したまま，タブを複製し次のページに進む．
4. 教材の内容を画面キャプチャして，他のアプリケーションにはりつける．
5. 各ページのソースコードの閲覧．
6. ブラウザの戻るボタンの押下．
7. URL 直打ちによるアクセス．
8. 他のユーザへの教材，確認テスト，回答などの横流し．
9. 学習，確認テストの途中で中断（各教材，確認テストの所要時間を計測しているため，遅くとも 2 時間以内には受講を完了すること）

本研究では，一般的な不正事象として想定される上記の禁止事項の違反を次の方法により検出する．

(1) 画面遷移逸脱

「6. ブラウザの戻るボタンの押下」,「7. URL 直打ちなどによるアクセス」の禁止事項を違反し，正常な画面遷移を逸脱した事象である．e ラーニング WEB サイトでは，ブラウザのキャッシュを無効化するため，各画面のソースに php でアクセスごとにログを出力させる機能を実装し，事象の発生を記録する．

[1] 選択肢のうち，下記のいずれかを選択．
正しいもの，違っているもの，最もふさわしいもの，最もふさわしくないもの，ふさわしいものすべて，ふさわしくないものすべて

表 3.2: 禁止事項と検出方法

禁止事項	検出方法	検出
1	アクセス時間より判定 (4.4 項)	○ (2)
2	ルールで禁じる	×
3	ルールで禁じる	×
4	ルールで禁じる	×
5	偽正解パターンで判定	○ (4)
6	アクセスログから検出	○ (1)
7	アクセスログから検出	○ (1)
8	ルールで禁じる	×
9	アクセスログから検出	○ (1)

表 3.3: 読解速度 S_i の信頼度 95%の予測区間（上限）

教材	文字数 C_i	読解速度 $S_i[10^3$ 字/分]			
		受講 1 回目		受講 2 回目	
		平均 $\mu\ 1_i$	上限値 $S1_i+$	平均 $\mu\ 2_i$	上限値 $S2_i+$
1-1	1,528	1.382	37.63	4.487	65.77
1-2	977	1.766	36.28	6.456	60.89
2-1	3,113	2.293	41.61	9.745	79.95
2-2	1,774	2.765	38.24	8.609	67.96
3-1	2,193	1.543	39.28	6.955	71.69
3-2	3,436	2.263	42.44	14.460	82.86
4-1	654	1.410	35.49	4.000	58.04
4-2	2,201	2.412	39.30	8.955	71.76

(2) 教材未読回答

「1. 教材を必ず熟読したうえで回答する」の禁止事項を違反し，極端に短い時間で次のページに遷移した事象である．e ラーニング WEB サイトではアクセス時刻から滞在時間を測定し，表 3.3 に定めた閾値で判定する．閾値の定め方は 4.1.2 項で述べる

(3) 答案未回答

何も選択せずに回答した事象である．e ラーニング WEB サイトでは回答内容に基づいて判定する．

(4) HTML ソースなど確認

「5. 各ページのソースコードの閲覧」の禁止ルールを違反した事象である．e ラーニング WEB サイトでは，確認テストのページの HTML ソースに正解とは別の選択肢を疑似正解としてあらかじめ記載しておき，被験者がこの疑似正解と一致した回答をした場合，採点結果を満点とし，データベースに不正があった旨を記録する．この場合，個々の教材では満点が獲得できるが，総合点を 0 点とした．

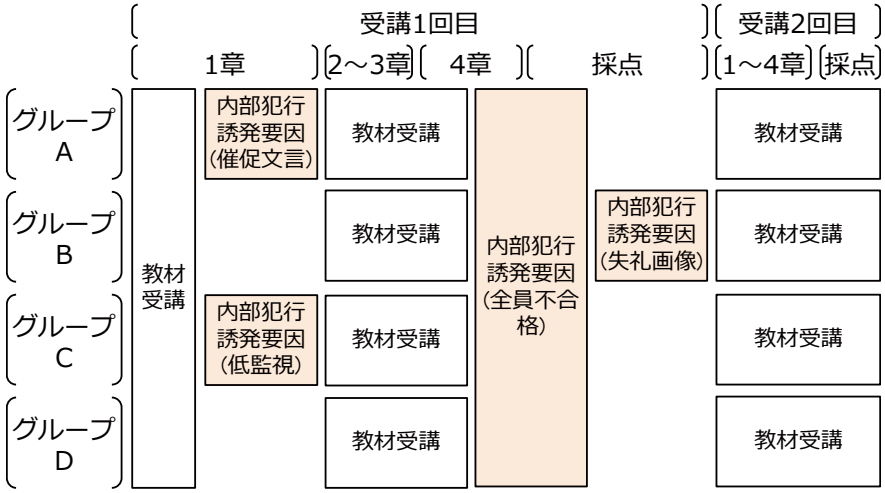

図 3.3: 誘発要因の発生タイミング

残りの禁止事項は，システムでは検出不能である．以上のルールと検出方法の関係を表 3.2 に記す．なお，表中の検出欄にある括弧内の数字は，本節でそれぞれ定義した不正事象の番号を指す．

3.2.4 内部不正誘発要因

調査報告書 [15] をもとに想定される内部不正誘発要因を本実験で擬似的に再現した．

3.2.4.1 グループごと誘発要因

e ラーニング WEB サイトでは，図 3.3 のタイミングでグループごとに異なる内部不正誘発要因を発生させた．発生タイミングの詳細は 3.4.2 項で記載する．

a) 催促文言

「頑張っているのに催促される」という想定内部不正誘発要因を再現するため，グループ *A* のみ完了時間を，平均完了時間（25〜45 分）より早い 20 分で完了するように指示する．

b) 失礼画像

「上司の社員に対する暴言，人遣いの荒さ」を再現するため，グループ *B* のみ 1 回目の再受講案内時に失礼な画像，暴言（付録参照）を表示する．

c) 低監視

「第三者からの監視性が低い」を再現する．グループ *C* 以外には「e ラーニング WEB サイトは，アクセスログ，アクセス時間などをすべて取得している」,「不正を検出した場合，作業承認を拒否する場合がある」を受講途中に表示させる．なお，注意喚起を非表示にしたのは受講途中のみであり，利用規約には表示した．

グループ *D* は上記の内部不正誘発要因の影響を評価するため，いずれも割り当てなかった．内部不正誘発要因とグループの関係を表 3.1 に示す．

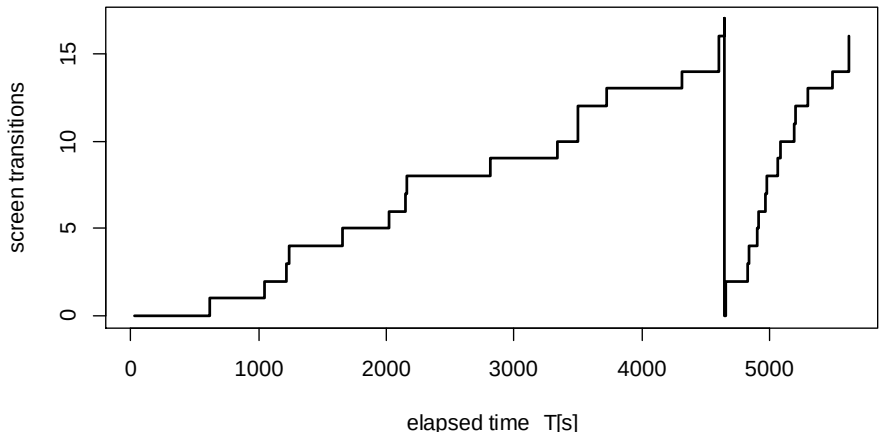

図 3.4: 画面遷移（正常）

3.2.4.2 発生タイミング

ユーザ自身の行動特性の見極め，行動変容の基準値測定，ランダム対応者の抽出などのため，教材 1 確認テストまでは内部不正誘発要因をまったく発生させず，教材 1 採点画面以降に発生させる．誘発要因の発生タイミングは図 3.3 のように要因ごとに異なる．

3.3 実験結果

3.3.1 不正事象の発生状況

3.3.1.1 画面遷移逸脱

経過時間（X 軸）についての画面遷移番号（Y 軸）の正常パターンの例を図 3.4 に示す．画面遷移番号は，図 3.1 の画面遷移図のメニュー画面を 0 として，教材 1-1 画面から採点画面（教材 1）を 1〜4 とし，以降の教材も画面遷移ごとに採番した．採点画面（教材 4）が 16 であり，総合点画面を 17 とした．

正常パターンは 1 回目の採点画面に向けて画面遷移番号が単調増加し，再受講でいったん 0 まで下がり，再び増加する．

ところが，図 3.5 の逸脱パターンは画面遷移番号がたびたび減少する．これは被験者が確認テストを表示後に禁止事項である「戻るボタン」を押下し，教材の内容を再確認して不正行為を繰り返したことを示している．

3.3.1.2 教材未読回答

i 番目の教材のアクセス日時を A_i，$i+1$ 番目のアクセスを A_{i+1} とした場合，i 番目の教材の滞在時間 T_i [s] を $T_i = A_{i+1} - A_i$ とする．図 3.6 は受講 1 回目における教材ごとの滞在時間 T_i の確率密度分布である．図 3.6 の曲線は，色ごとに異なる教材の確率密度を表している．たとえば，青線は図 3.1 の教材 1-1 における滞在時間を示す．滞在時間 T_i が 60 秒以内となるケースが多いことが分かる．

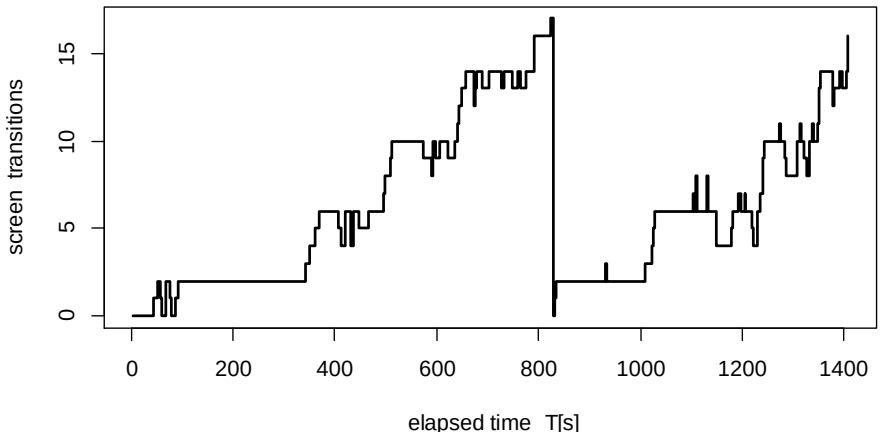

図 3.5: 画面遷移（逸脱行為）

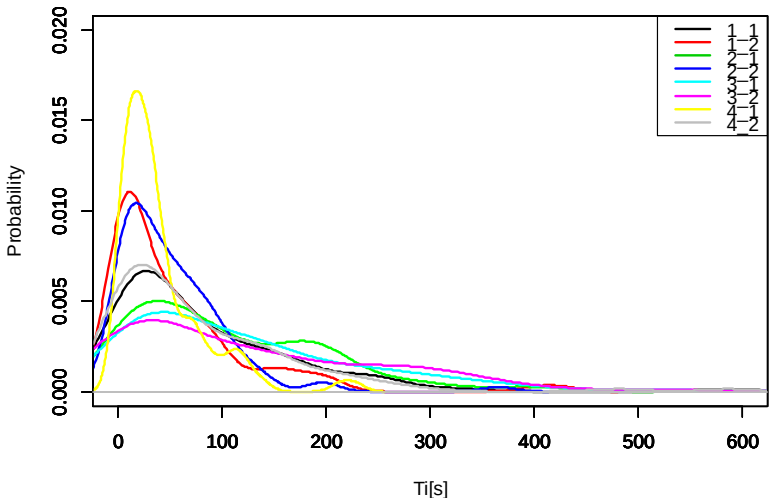

図 3.6: 教材ごとの滞在時間 T_i の確率密度

図 3.7 は受講 1 回目の i 番目の滞在時間 T_{1i}（秒）と 2 回目の i 番目の滞在時間 T_{2i}（秒）の散布図である．

不正事象 (2) 教材未読回答について，未読とする閾値を定めるにあたり，教材の滞在時間 T_i [s] は教材の文字数に依存するため，1 文字あたりの読解速度を求める．i 番目の教材の文字数を C_i とすると，i 番目の教材の読解速度 S_i [文字数/分] は $S_i = \frac{C_i}{T_i} \times 60$ で与えられる．図 3.8，図 3.9 は受講 1 回目と 2 回目における教材ごとの読解速度 S_i と教材の文字数 C_i の散布図である．

受講 1 回目，2 回目の読解速度 S_{1i} と S_{2i} の単回帰分析の回帰式を以下に示す．

$$S_{1i} = 3.62 \times 10^3 + 2.49 C_i$$
$$S_{2i} = 3.81 \times 10^3 + 8.92 C_i$$

図 3.8，図 3.9 の赤線は，回帰式の信頼度 95%の予測区間である．

表 3.3 は教材ごとの文字数 C_i における受講回数ごとの読解速度 S_i の平均 μ_{1i}，μ_{2i}，信頼度 95%の予測区間の上限値 ${S_{1i}}^+$，${S_{2i}}^+$ である．本研究では読解速度 S_i が表 3.3 の上限値を上回ったとき，

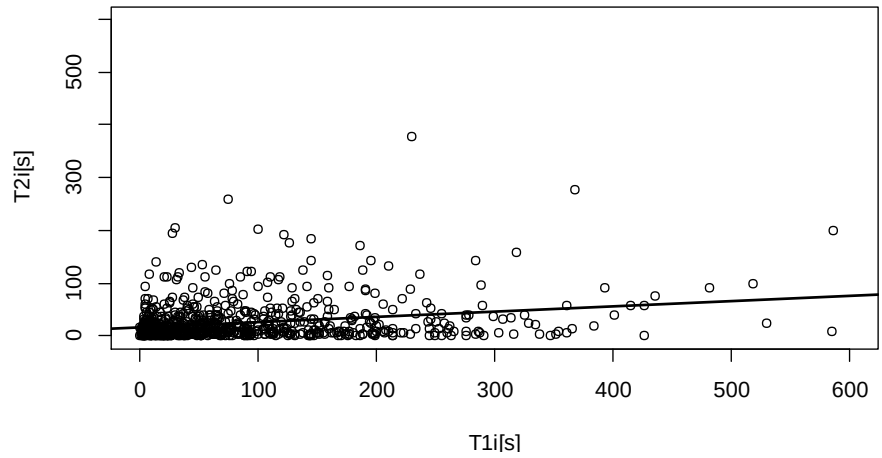

図 3.7: 滞在時間 T_i（受講 1 回目/2 回目）

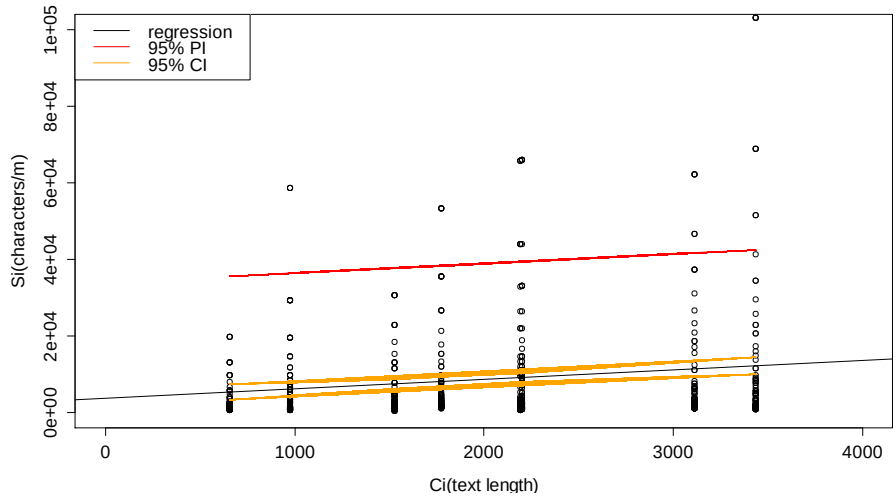

図 3.8: 読解速度と文字数（受講 1 回目）

不正事象とした．

3.3.2 不正事象の発生ユーザ数

表 3.4 はグループごとの属性別ユーザ数である．

3.3.2.1 グループごと

表 3.5 に 3.3.5 項に定めるグループ別の不正事象を発生させたユーザ数を示す．ここで，N はグループごとのユーザ数である．各不正事象の左列は，受講中に不正事象を発生させたユーザ数，右列「(再掲) 1-1」は受講 1 回目の教材 1 で不正事象を発生させたユーザ数である．

画面遷移逸脱の不正は e ラーニング WEB サイトの内部誘発要因の表示前に発生している．

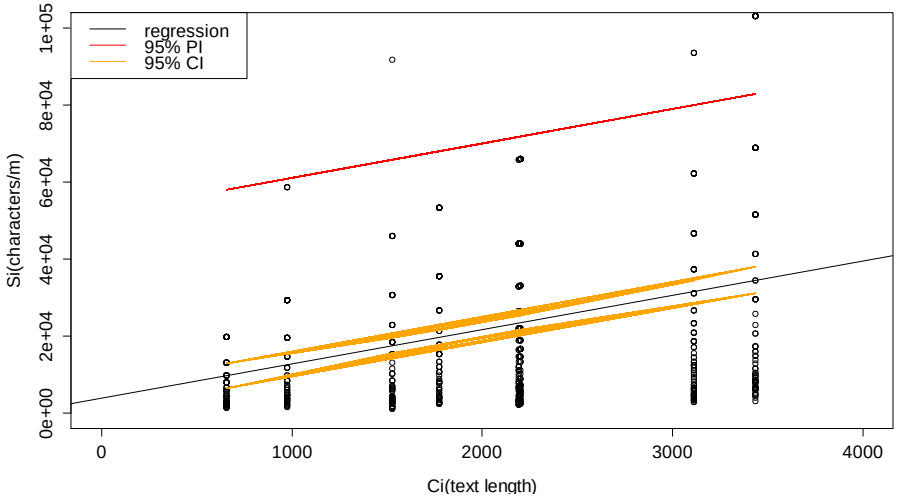

図 3.9: 読解速度 S_i と文字数 C_i（受講 2 回目）

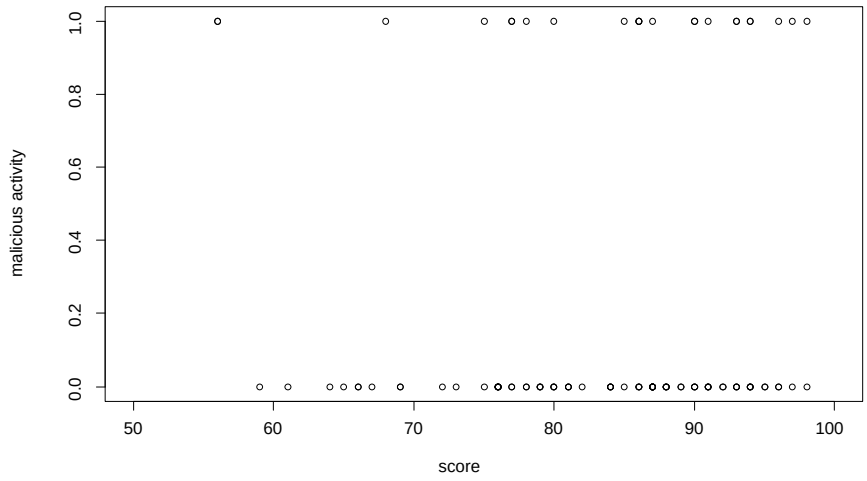

図 3.10: 受講 1 回目の不正事象 (2) 教材未読回答の有無と得点の散布図

3.3.2.2　得点ごと

図 3.10 は受講 1 回目における (2) 教材未読回答の不正事象の有無と得点の散布図である．縦軸の値は 0 が不正事象なし，1 が不正事象ありを表している．

3.3.2.3　ランクごと

不正事象 (1) 画面遷移逸脱，(2) 教材未読回答の発生ユーザ数をランク別に集計した結果を表 3.6 に示す．ランクは得点を以下の 5 段階に分類した（S：90 点以上，A：80 点以上 90 点未満，B：70 点以上 80 点未満，C：60 点以上 70 点未満，D：60 点未満）．

表 3.4: ユーザ数（e ラーニング実験：属性別）

		A	B	C	D	合計
性別	女性	8	10	13	12	43
	男性	16	12	14	15	57
年代	20〜29 才	6	6	7	6	25
	30〜39 才	11	12	14	16	53
	40〜49 才	6	2	5	4	17
	50〜59 才	1	2	1	1	5
職業	会社員	8	5	15	11	39
	専業主婦，専業主夫	4	4	3	6	17
	無職	2	3	1	1	7
	パート，アルバイト	1	3	2	3	9
	その他	1	0	1	2	4
	自営業	7	5	5	4	21
	学生	1	2	0	0	3
計		24	22	27	27	100

表 3.5: 不正事象発生ユーザ数（e ラーニング実験）

グループ	N	(1) 画面遷移逸脱 (再掲) 1-1		(2) 教材未読回答 (再掲) 1-1		(3) 答案未回答 (再掲) 1-1		(4)HTML ソースなど確認 (再掲) 1-1	
A	24	6	4	5	0	0	0	0	0
B	22	4	2	6	0	0	0	0	0
C	27	9	5	11	0	3	0	1	0
D	27	9	4	1	0	1	0	0	0
合計	100	28	15	22	0	4	0	1	0

3.3.2.4 属性ごと

不正事象 (1) 画面遷移逸脱，(2) 教材未読回答の発生ユーザ数を属性別に集計した結果を表 3.7 に示す.

3.3.3 成績

3.3.3.1 グループごと，受講回数ごと

表 3.8 はグループごと，受講回数ごとの得点の集計結果である.

表 3.6: ランク別，受講回数別不正事象発生ユーザ数

受講回数	ランク	N	画面遷移逸脱	教材未読回答
受講 1 回目	S	32	11	10
	A	36	9	6
	B	20	5	4
	C	9	2	1
	D	3	1	2
受講 2 回目	S	65	22	14
	A	22	4	7
	B	8	1	1
	C	2	0	1
	D	3	1	0

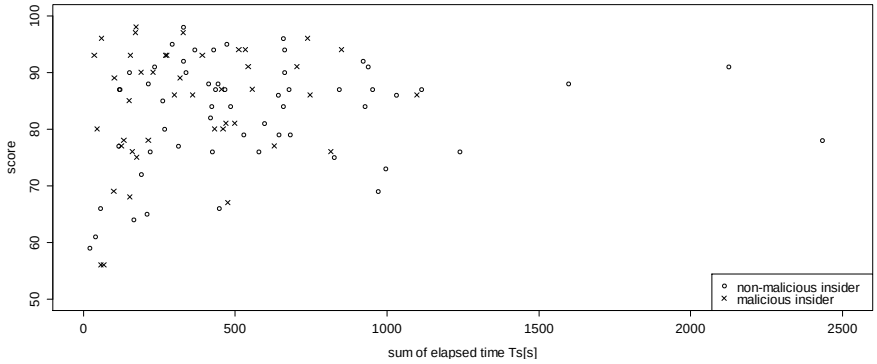

図 3.11: 受講 1 回目の得点と滞在時間の合計 T_s の散布図

3.3.3.2 滞在時間ごと

各教材へのアクセスの滞在時間の合計を T_s [s] とする．受講回数ごとにおける得点と滞在時間の合計 T_s の散布図を図 3.11 に示す．

表 3.7: 不正事象発生ユーザ数（e ラーニング実験：属性別）

		N	画面遷移逸脱	教材未読回答
性別	女性	43	12	8
	男性	57	16	15
年代	20〜29 才	25	7	12
	30〜39 才	53	13	7
	40〜49 才	17	6	3
	50〜59 才	5	2	1
職業	会社員	39	13	13
	専業主婦，専業主夫	17	6	2
	無職	7	0	1
	パート，アルバイト	9	2	4
	その他	4	1	0
	自営業	21	6	2
	学生	3	0	1

表 3.8: 得点（グループごと，受講回数ごと）

	受講 1 回目 (点)				受講 2 回目 (点)			
	A	B	C	D	A	B	C	D
平均	84.8	81.6	84.8	82.6	92.8	88.5	88	86.1
標準偏差	8.8	12	8.4	9.6	6.2	10.7	14.9	17.3

表 3.9: カイ 2 乗検定の分析結果（e ラーニング実験：属性別ユーザ数）

属性		χ^2	df	P 値	有意判定
性別	女性	1.372	3	0.712	
	男性	0.614	3	0.893	
年代	20〜29 才	0.120	3	0.989	
	30〜39 才	1.113	3	0.774	
	40〜49 才	2.059	3	0.560	
	50〜59 才	0.600	3	0.896	
職業	会社員	5.615	3	0.132	
	専業主婦，専業主夫	1.118	3	0.773	
	無職	1.571	3	0.666	
	パート，アルバイト	1.222	3	0.748	
	その他	2.000	3	0.572	
	自営業	0.905	3	0.824	
	学生	3.667	3	0.300	

3.4 評価

不正事象 (3) 答案未回答，(4)HTML ソースなど確認の評価は，発生数が非常に少ないため割愛した．また，図 3.10，表 3.6 より，得点別，ランク別の不正事象の発生数，また，図 3.11 より得点別，滞在時間別の不正事象の発生数はともに大きな差が見受けられなかった．

本章では不正事象の発生数と内部不正誘発要因の関係を探るため，カイ 2 乗検定による独立性の検定を行った．相関が確認された要因については，どの要因が不正事象の発生に本質的な影響を与えているかを探るため，ロジスティック回帰分析を行った．また，ロジスティック回帰分析により年齢，性別や職業などの無関係な背景因子（交絡因子）の影響を調整したオッズ比を算出した．なお，オッズ比は，(不正事象の発生する確率)/(不正事象の発生しない確率) で定められる．

3.4.1 独立性の検定

3.4.1.1 グループ

本実験の標本は表 3.4 にあるとおり，性別，年代，職業などの属性について無作為抽出をしておらず，グループに完全に均等に分散していない．そこで各属性におけるグループ間について有意な差があるかを統計的に検定するため，次の H_0 と H_1 について自由度 Df = 3 のカイ 2 乗検定を行う．

帰無仮説 H_0：4 つのグループは独立である．

対立仮説 H_1：4 つのグループは独立ではない．

分析結果を表 3.9 に示す．

表 3.9 の分析結果から，すべての属性において p 値は有意水準 5%よりも大きいので，帰無仮説 H_0 は棄却されない．そのため，各属性におけるグループ間の差は不正事象の発生に影響を及ぼすほどではないと考えられる．

表 3.10: カイ 2 乗検定の分析結果（e ラーニング実験：教材 1-1（共通条件）の不正者数）

対象	χ^2	df	P 値	有意判定
教材 1-1(共通条件)	1.267	3	0.737	

3.4.1.2 共通条件

潜在的な不正者がグループに偏って分散していないかを確かめるため，共通の条件で不正をしたユーザ数を観察した．表 3.5 の 1-1（共通条件）は，内部不正誘発要因を発生させる前に不正事象を犯したユーザ数である．これらの不正者数について，グループ間で差があるかを確認するため，次の H_0 と H_1 について自由度 Df = 3 のカイ 2 乗検定を行う．

帰無仮説 H_0：4 つのグループは独立である．

対立仮説 H_1：4 つのグループは独立ではない．

分析結果を表 3.10 に示す．

表 3.10 の分析結果から内部不正誘発要因を与える前の被験者における不正者数は，4 つのグループにおいて独立に分散していると考えられる．

3.4.2 グループと不正行為

3.4.2.1 独立性

各不正事象の発生ユーザ数は，グループごとで有意な差があるのか検定する．

表 3.5 より，(1) 画面遷移逸脱の不正者は，どのグループにも均等に存在し，グループ間の差が見られない．むしろ基準としているグループ D（要因なし）よりも A か B の方が少ない．よって，A，B，C の要因は，(1) の不正者には影響を与えていない．しかし，(2) 教材未読回答の不正者は，D の 1 名に対して，A，B，C が 5，6，11 名といずれも増えている．ここに何らかの誘発する影響があったと考える．

そこで，(1) と (2) について，それぞれ次の H_0 と H_1 について自由度 Df = 3 のカイ 2 乗検定を行う．

帰無仮説 H_0：不正の有無とグループ（要因）は独立である．

対立仮説 H_1：不正の有無とグループ（要因）は相関がある．

(1) 画面遷移逸脱

統計量 $\chi^2 = 1.921$，p 値は 0.589 であった．したがって，有意水準 5%よりも大きいので，帰無仮説 H_0 は棄却されない．

(2) 教材未読回答

統計量 $\chi^2 = 10.76$，p 値は 0.01306 であった．したがって，5%の有意水準で帰無仮説 H_0 は棄却され，グループごとに有意な差がある．

3.4.2.2 ロジスティック回帰分析

どの要因が大きく誘発しているかを識別するため，グループ D を基準として，A，B，C の説明変数に対してロジスティック回帰分析を行った．表 3.11 に目的変数を教材未読回答の不正事象発生ユーザ数，説明変数をグループとした場合のロジスティック回帰分析の分析結果を示す．

グループ B，C が「教材未読回答」に影響を与えていることが分かる．特に C は p 値が 0.01 以下であり，99%の有意水準を下回っており，著しい影響を与えている．

表 3.11: ロジスティック回帰分析の分析結果（e ラーニング実験 : グループ別不正事象発生ユーザ数）

変数	推定値 (Estimate)	標準誤差 (Std.Error)	Z 値 (z Value)	P 値 (Pr(> |z|))	有意判定
(Intercept(D))	-3.258	1.019	-3.199	0.00138	**
groupA	1.923	1.136	1.693	0.09044	.
groupB	2.277	1.125	2.023	0.04304	*
groupC	2.883	1.091	2.642	0.00824	**

表 3.12: カイ 2 乗検定の分析結果（e ラーニング実験：属性別不正事象発生ユーザ数）

不正事象	属性	χ^2	df	P 値	有意判定
(1) 画面遷移逸脱	性別	0	1	1.000	
	年代	1.120	3	0.772	
	職業	5.060	6	0.536	
(2) 教材未読回答	性別	0.450	1	0.505	
	年代	12.00	3	0.0074	**
	職業	9.730	6	0.137	

不正事象の発生確率を p，グループごとの推定値（偏回帰係数）を x_a，x_b，x_c とした場合のロジスティック関数は，

$$p = \frac{1}{1 + exp\,(3.258 - 1.923x_a - 2.277x_b - 2.883x_c)}$$

となる．このとき，ロジスティック関数の逆関数であるロジット関数は，

$$\log \frac{p}{1-p} = -3.258 + 1.923x_a + 2.277x_b + 2.883x_c$$

である．$\frac{p}{1-p}$ は，オッズ比（odds ratio）であり，グループ A，B，C のオッズ比はそれぞれ 6.84 倍，9.75 倍，17.9 倍であった．

3.4.3 属性と不正行為

3.4.3.1 独立性

標本における性別，年代，職業などの属性が本実験に影響を大きく与えていないかを確認するため，各不正事象の発生ユーザ数は，属性ごとに差があるのか評価する．

属性別の (1) 画面遷移逸脱と (2) 教材未読回答の不正事象発生ユーザ数について，それぞれ次の H_0 と H_1 についてのカイ 2 乗検定を行う．

帰無仮説 H_0：不正の有無と属性は独立である．

対立仮説 H_1：不正の有無と属性は相関がある．

分析結果を表 3.12 に示す．

表 3.12 の分析結果における年代別の (2) 教材未読回答の不正事象発生ユーザ数の p 値は 0.0074 であった．したがって，5%の有意水準で帰無仮説 H_0 は棄却され，年代ごとの差があることが確認できた．

表 3.13: ロジスティック回帰分析の分析結果（e ラーニング実験：年代別不正事象発生ユーザ数）

変数	推定値 (Estimate)	標準誤差 (Std.Error)	Z 値 (z Value)	P 値 (Pr(> |z|))	有意判定
(Intercept(30〜39 歳))	-1.8827	0.4057	-4.641	3E-06	***
40〜49 歳	0.3423	0.7546	0.454	0.6501	
50〜59 歳	0.4964	1.1894	0.417	0.6764	
20〜29 歳	1.8027	0.57	3.163	0.0016	**

その他の属性において p 値は有意ではなかった．したがって，本実験において性別，職業の差は不正事象の発生に影響を及ぼすほど大きくはないと結論づける．

3.4.3.2 ロジスティック回帰分析

(2) 教材未読回答の年代ごとの差について，どの年代が大きく誘発しているかを識別するため，30〜39 歳を基準として，他年代の説明変数に対してロジスティック回帰分析を行った．表 3.13 に目的変数を教材未読回答の不正事象発生ユーザ数，説明変数を年代とした場合のロジスティック回帰分析の分析結果を示す．

年代 30〜39 歳，20〜29 歳が「教材未読回答」に影響を与えていることが分かる．特に 20〜29 歳は p 値が 0.01 以下であり，99%の有意水準を上回っており，著しい影響を与えている．

3.5 考察

3.5.1 内部不正誘発要因と不正事象発生の関係

本実験で想定した不正事象のうち (1) 画面遷移逸脱，(3) 答案未回答，(4) HTML ソースなど確認はグループごとの有意の差は認められず，内部不正誘発要因との相関は見いだせなかった．一方，表 3.11 から推定値から算出した調整済みオッズ比は，誘発要因を与えない場合と比べて，誘発要因「(c) 低監視」は 17.9 倍，誘発要因「(b) 失礼画像」は 9.75 倍の確率で不正事象を引き起こすことを示している．監視が甘いという誘発要因は，不正事象の発生に強い影響を与えている．組織は対応が不十分な場合，速やかな対応が必要である．

また，表 3.11 では誘発要因「(b) 失礼画像」も不正事象に有意であった．グループ A の誘発要因「催促文言」は速やかに受講するよう催促しているが，グループ B の誘発要因「失礼画像」の影響の方がより大きいことが分かった.「催促文言」は業務依頼の延長ととらえることができるが,「失礼画像」は暴言である．暴言に比べて，業務依頼にともなう催促などは不正事象に影響を及ぼす可能性が低いと考えられる．

また，表 3.12 によると不正事象 (2) 教材未読回答は年代ごとの有意の差が認められた．表 3.3 で示したとおり，各教材の読解速度 S_i の閾値は最低でも 30000 字/分を超えており，20〜29 歳のユーザは教材の内容を熟読することなく，回答する傾向にあった．

3.5.2 e ラーニングサイトの限界

本実験では内部不正誘発要因を識別するうえで実環境を再現するための疑似環境として e ラーニングサイトを利用した．本節では，e ラーニングサイトで実環境を再現するうえでの限界について考察する．

金銭目的の内部不正の再現

過去の情報漏えい事故において悪意のある内部犯は組織で管理された顧客情報を不正に取得し，第三者に売却することで利益を得ている．実環境における顧客情報は売却するだけの価値があるが，e ラーニングサイトでそれだけの価値を提供することは困難である．

未認可の情報持出の動機づけ

本実験の e ラーニングでは情報持出の動機づけを与えることが難しい．なぜならば実務と違い e ラーニングでは学習やテスト環境を提供するものであり持出行為が不自然であるためである．

3.5.3 母集団と標本

母集団の選定

本実験では国内におけるすべての雇用者を母集団とし，標本をクラウドソーシングサービスの登録ユーザとした．当該サービスは，表 3.4 で示すとおり被験者の職業には「無職」「学生」「専業主婦/主夫」も含まれる．

標本の抽出方法

本実験に用いた標本は母集団から無作為抽出したものではない．本実験ではランサーズ社のクラウドソーシングサービスに登録したユーザに対して，先着順に被験者の受付を行った．先着順であるため，筆者らが被験者を作為的に抽出することは不可能であるが，無作為に被験者を抽出したものではない．被験者の属性に偏りがないことを確かめるため，表 3.9 によるカイ 2 乗検定を行った．

3.5.4 今後の研究課題

未認可の情報アクセスの検知

本実験では不正事象 (4) HTML ソースなど確認を実環境における不正事象の 1 つである未認可の機密情報へのアクセスの疑似事象と見なした．組織の情報漏えい事故の要因を識別するためには情報セキュリティポリシに対する逸脱行為を再現することが必要である．当該ポリシでは一般的に未認可の情報アクセスを禁止している．

未認可の情報アクセスの疑似事象に関しては，他の再現方法として e ラーニングサイトが提供するコンテンツの一部について被験者にはアクセス禁止である旨を伝え，アクセスした場合に不正事象と見なす方法などがある．

被験者の細かい行動の検知

「サイトの掲載情報をコピー，画面キャプチャ，印刷した場合」を禁止行為と定義した場合，サイト自体を javascript などによって構築し，上記の操作を記録するようにすれば検知することは可能である．

被験者自身の性格などが不正事象に与える影響の識別

被験者自身の性格，倫理観，心配性尺度などの影響度分析を実施していない点は本実験の課題である．Greitzer らは内部不正に起因する予測因子について「ストレス」「個人的な問題」をあげている [87].

内部不正誘発要因が複合した場合の影響の識別

本実験では，表 3.1 で示す内部不正誘発要因について，被験者に対して 1 種類のみを与えるか，何も与えないかのいずれかとした．もしも要因が互いに独立ならば，要因が複合した場合の積事象の確率は推定可能である．独立かどうかの検証は今後の検討課題である．

また，要因の組合せごとに被験者のグループを作成することで影響の測定は可能である．一方，グループを増やしすぎると 1 グループあたりの被験者数が少なくなり，被験者自身の属性の影響を受けやすくなる．要因の複合時における影響の識別も今後の課題である．

待遇の差の再現

社会安全研究財団 [15] によれば，待遇に不満がある従業員は内部不正を及ぼす可能性があるとしている．本実験の被験者に支払われる報酬に差を発生させることはできなかった．ランサーズ社では作業ごとに支払金額を個別に設定することができる．また複数の他のクラウドソーシングサービスを同時に利用することで被験者ごとに謝礼金に差をつけることは不可能ではない．待遇の差によって内部不正の発生にどれくらい影響しているかを確認することは今後の課題である．

3.6 結論

本研究はクラウドソーシングにより被験者を集め，実組織の職場環境を疑似的に e ラーニングサイトで再現し，グループごとに異なる内部不正誘発要因を与え，不正事象の発生数を観測した．実験結果の独立性を評価し，ロジスティック回帰分析を行い，内部不正の誘発要因が不正事象に与える影響を確認した．本実験により 3 つの仮説（催促，非礼，監視）のうち，非礼，監視の 2 つの仮説が成立することが検証された．本研究の主要な結論は次のとおりである．

- 他の内部誘発要因と比べ，第三者からの監視が低い場合，監視が十分な場合に比べて 18 倍も不正事象を誘発する．
- 業務の催促と暴言を比べると，暴言の方が不正事象を発生させる．
- 若年層は文字量の多い教材は熟読しない傾向がある．

第4章　アカウントの共有における内部不正誘発要因の識別（予備実験）

4.1　導入

本実験は利用者を監視する手法として，共有アカウントが内部不正を誘発する度合いはどれくらいなのかを検証する．組織は，内部不正の発生に抑制効果が高い手法を識別できれば，それらの対策に費用を集中することができ，効果的にリスクを低減することが可能となる．

これらの実験は実在する企業などの従業員を対象に実施することが望ましい．しかし，企業などで実験を行いその結果を第三者に提供することは，当該企業の情報セキュリティポリシに抵触する可能性がある．さらに内部不正の発生頻度は低く，その過程を詳細に観察することは困難である．

そこで，筆者らは疑似環境を構築し，アンケート回答とデータ入力作業で生じる不正事象の発生数を観測する．被験者は，クラウドワークス社のクラウドソーシングサービスにより集めた 192 名である．被験者は，4 つのグループをランダムに割り当てた．グループごとに被験者に払い出すアカウントを共通アカウントと個別アカウントのいずれかに分け，さらにつねにアカウント名が画面に表示されるグループと冒頭のみに表示されるグループに分類した．

不正事象の発生数を測定し，グループごとに独立かどうかを確認するためカイ 2 乗検定を行った．

4.2　提案方式

4.2.1　仮説

本研究は，内部不正を誘発する要因として，次の 2 つの仮説を立てる．

仮説 $H_{\text{共有 (カレー)}}$：共有アカウント (例:guest アカウント) を利用していると内部不正を犯す．

仮説 $H_{\text{表示 (カレー)}}$：作業中に常時アカウント名が表示[1] されていないと内部不正を犯す．

4.2.2　困難性

実環境では，内部発生の発生確率は低く，たとえ発生した場合でも観測が難しい．仮に観測ができた場合でも，それらの開示は企業内のセキュリティポリシに抵触する可能性がある．

また，疑似環境において実験する場合でも被験者が報酬を受け取って疑似タスクを遂行する場合，数多くの内部不正を観測することは期待できない．一方，報酬を支払わない場合，被験者を集めることは容易ではない．そのため，優良な被験者に対して不正事象を誘発するための仕掛けを考慮した実験環境を構築することが必要となる．

[1]WEB サイトの各ページの上端に常時ユーザ名が表示されている状態

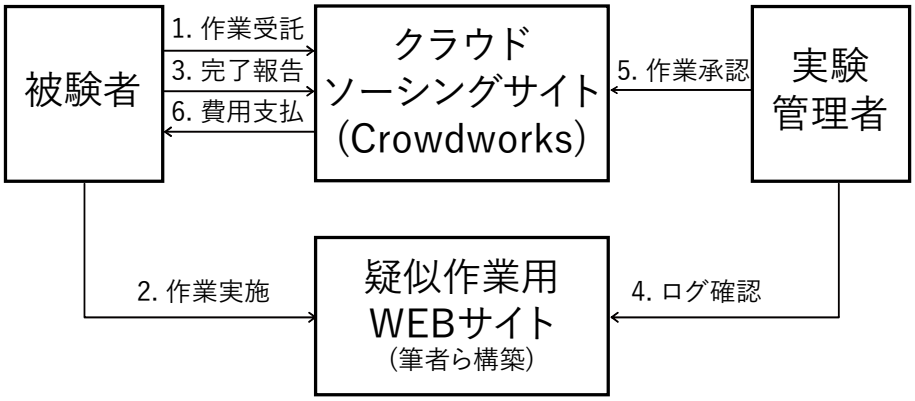

図 4.1: 作業の流れ（カレー実験）

4.2.3 目的

本研究は，共有アカウントや利用者 ID の非表示が不正事象の発生に与える影響を明らかにすることを目的とする．

4.2.4 実験概要

筆者は，組織の業務環境を再現した擬似作業用 WEB サイト（以下，本サイト）を構築した．被験者はクラウドワークス社によるクラウドソーシングサイトで集めた 192 名である．仮説を検証するため，被験者は 4 つのグループに分類した．グループごとに異なる刺激を与えることで不正事象の発生数にどれだけの差があるのかを観測した．

表 4.1 に被験者グループと仮説との関係を示す．詳細は 5.2.5.3 項を参照．

4.2.4.1 作業の流れ

被験者はクラウドワークス社のサイトから本実験の作業を受託する．次に，本サイトにアクセスしてアンケートや PDF のデータ入力を行う．その後，被験者はクラウドワークス社に完了報告を行う．実験管理者は完了報告に基づいて利用状況を本サイトのアクセスログから確認し，問題がなければ作業を承認する．作業承認後，クラウドワークス社は筆者らが事前に支払をしていた費用の一部を被験者に支払う．

本実験の作業の流れを図 5.2 に示す．

4.2.4.2 被験者

国内におけるすべての雇用者を母集団とし，クラウドワークス社のクラウドソーシングサービスに登録したユーザのうち作業を完了した 192 名のユーザを標本とする．なお，被験者の質を確保するため，クラウドワークス社で本人確認書類の提出が確認されていることを募集要件とした．当該ユーザは本実験（タスク）を完了した順番で先着順に抽出した．無作為抽出は実施していないが，クラウドソーシングサービスには様々なユーザが登録されており，多様な属性を持ったユーザの代表を抽出できると期待した．

表 4.1: グループと仮説の関係（カレー実験）

グループ	仮説 $H_{\text{共有 (カレー)}}$	仮説 $H_{\text{表示 (カレー)}}$	N
A	共有	なし	45
B	個別		47
C	共有	あり	48
D	個別		52

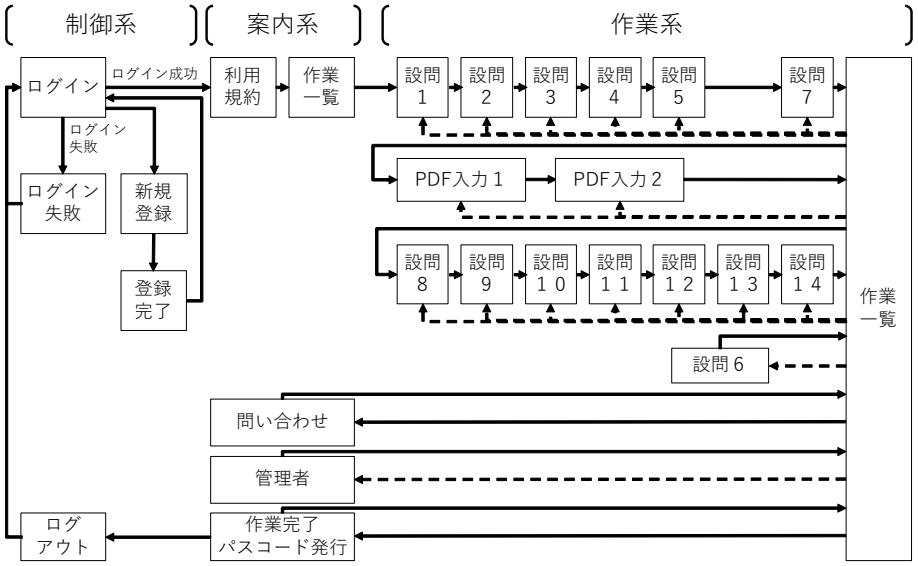

図 4.2: 画面遷移図（カレー実験）

4.2.4.3 被験者グループ

仮説 $H_{\text{共有 (カレー)}}$ を検証するため，グループ *A* と *C* の被験者には共有アカウントを払い出した．アカウント名は”Guest”である．グループ *B* と *D* の被験者には個別アカウントを払い出した．アカウント名は”userxxx”であり，xxx は被験者ごとに 0〜9 の数字について 5 ケタの乱数を割り当てた．なお，本サイトは”Guest”アカウントを払い出した場合においても被験者ごとの行動を識別できるようにした．

仮説 $H_{\text{表示 (カレー)}}$ を検証するため，グループ A と B の被験者がアクセスする画面には，画面の上端に利用中のアカウント名を常時表示させた．一方，グループ *C* と *D* の被験者には，冒頭以外は画面の上端にアカウント名を表示させなかった．

これらの関係を表 4.1 に示す．

4.2.5 本サイトの作業内容

本サイトで被験者は，まず利用規約の確認を行い，6 問のアンケートに回答する．そして PDF ファイルのデータ入力を行い，7 問のアンケートに回答する．その後，作業一覧画面に戻り，作業を完了させる．

本サイトの画面遷移図を図 5.1 に記す．

4.2.5.1 利用規約の確認

本サイトは被験者が作業を開始する前に利用規約を表示した．被験者は同意ボタンを押下しないと作業が開始できないようにした．本実験は，被験者が利用規約に定めた禁止事項や依頼事項を違反した場合に不正事象とした．利用規約の詳細は付録 A.1 章を参照.

4.2.5.2 作業内容

まず，被験者はカレーライスの趣味嗜好について 6 問のアンケートに回答した．次に，PDF ファイルに記載されたデータをテキストボックスに入力した．さらに，被験者はカレーライスのアンケートを 7 問回答した．最後に，被験者は作業一覧画面の編集ボタンを押下して残りのアンケートに回答するか，問い合わせボタンを押下して作業を完了させた．アンケートや PDF ファイルの詳細は付録 A.2 章を参照.

4.2.6 内部不正の誘発要因

4.2.6.1 問 6 の非表示

被験者の内部不正を誘発させるため，被験者が全てのアンケートに回答したとしても，作業完了ボタンを押下すると，問 6 が未回答であると警告する状態として作業完了パスコードが表示されない状態とした.

作業完了のためには，被験者は以下のどちらかの対応が必要となる．1 つは，問 6 のみが未回答の状態で問い合わせボタンを押下することで作業が完了できる．もう 1 つは，問 6 の編集ボタンを押下することでアンケートを回答することが可能としたが，これは利用規約における禁止事項である.

4.2.6.2 PDF ファイルのランダム文字列

被験者がテキストボックスに入力する元データは，PDF ファイル形式で本サイトに表示した．この PDF ファイルには，ランダムに生成した意味をなさない文章を表示させた．これは被験者の作業に対するモチベーションを低下させ，被験者がより多くの不正事象を発生させることを期待した．文章の詳細は付録 A.2.2 章を参照.

4.2.7 不正事象

4.2.7.1 事象の定義

本実験は 8 種類の不正事象を定義した．これらの不正事象は特徴によって以下の 4 つに分類した.

1. 越権行為

   この不正事象は，自分の権限を越えた行為を行うことを指す.

(a) 編集ボタンの押下

本事象は，被験者が作業一覧画面のうち，管理者用と表示された「編集」ボタンを押下したものである．編集ボタンはアンケートの設問ごと，PDF データの入力ごとに配置した．利用規約は「管理者用画面のアクセス禁止」と定めており，当該ボタンの押下を不正事象とした．

(b) 管理者ボタンの押下

本事象は，被験者が各ページの上端に表示される「管理者」ボタンを押下したものである．

2. コピー，ペースト

(a) PDF ファイルのコピー，ペースト

本事象は，被験者が禁止事項のうち「コピー，ペーストの禁止」を違反し，PDF データ入力画面が表示する PDF ファイルに対して，コピー，ペーストの操作（以下，コピペ）を行ったものである．

(b) テキストボックス内のコピー，ペースト

本事象は，被験者が禁止事項のうち「コピー，ペーストの禁止」を違反し，PDF データ入力画面のテキストボックス内でテキストをコピーやペーストの操作を行ったものである．

(c) 透かし

被験者がコピー，ペーストしていることを把握するため，本実験では，予め PDF ファイルのテキストデータにテキスト型の電子透かしを含めた．本事象は，先述の「テキストボックス内のコピー，ペースト」を検出したユーザのみを対象として，被験者が入力したデータに以下の文字列が含まれていた場合に不正事象としてカウントした．

i. 力（ちから）(正：カレーの「カ」)
ii. 一（だっしゅ）(正：カレーの「ー」)
iii. 文末のピリオドが 2 つ
iv. PDF1 の入力時に 1 行目は全角カンマ、2 行目は半角カンマ＋半角スペース
v. PDF2 の入力時に 1 行目は半角カンマ＋スペース、2 行目は全角カンマ、3 行目は半角カンマ＋スペースの後に全角カンマ

3. 怠け

(a) でたらめ文字列

入力作業を怠ったり，適当に文字列を入力したとみなされる場合，不正事象とした．たとえば，日本語の 1 行目「カレー」や「力（ちから）レ一（だっしゅ）」などで始まらない場合，英語の 1 行目が「Saffron is put」で始まらない場合である．

(b) 途中放棄

入力された文字列が本来入力するべき長さに満たない事象である．閾値は，日本語は 30 字以下，英語は 60 文字以下とした．

4. 低得点

(a) アンケートランダム回答

本実験は，アンケートの問 1〜7 と 8〜14 は同じ内容のものを順番を入れ替えて質問した．これは，被験者がまじめに回答しているかどうかを確認するためである．前半と後半の回答が一致すれば，被験者は自分の趣味嗜好にもとづいて正しく回答している．一方，回答に不整合が生じている場合，被験者はあまり熟慮せずにランダムに回答したと考えられる．

本実験では下記の方法によってアンケートの整合性得点 Cs_i を計算し，回答内容のランダム度合いを評価した．

i. 単一選択の場合，前半と後半が一致すれば 10 点．一致しなければ 0 点

ii. 複数選択の場合，すべて一致していれば 25 点．1 つ間違っていれば 5 点減点．5 項目以上間違っていれば 0 点

単一選択の質問は 5 問，複数選択の質問は 2 問のため，評価は 100 点満点である．

4.2.7.2 各不正事象の例外

1. 編集ボタンの押下

   アンケートの問 6 の編集ボタンは，4.2.6.1 項に示した内部不正の誘発要因を被験者に与えた結果，半数以上のユーザが作業完了のために押下した．これは実験環境の不備に近い状況であると捉え，FP として取り扱い，不正事象とはみなさなかった．

   また，本サイトの PDF データ入力の画面はテキストボックスでデータ入力を行う際，キーボードの Enter キーを入力すると次の画面に遷移してしまう問題があった．そのため，被験者が文字を変換しようとして Enter キーを入力すると，入力途中のままで次の画面に進むことがあった．本事象も実験環境の不備であるため，FP として不正事象から除外した．

2. テキストボックス内のコピー，ペースト

   メモ帳や手書きツールにて作成したデータをペーストした場合，悪意が少ないことが想定された．そのため，先述の「透かし」の検出が 1 つもない場合には PDF データからのコピーはなかったと判断し，不正事象とはみなさなかった．ただし，PDF から漢字を直接コピペ、文章の 1 部だけのコピペなどを行った FN が含まれる．

3. でたらめ文字列

   明らかに入力ミスに起因すると想定されたもの [2] は不正事象とは見なさなかった．

4.2.7.3 検知方法

不正事象の検知方法は，以下の通り．

1. php によるアクセスログの取得

   該当するページのアクセスは php を利用して，ログをデータベースに出力した．

[2] たとえば,「体に熱し」を「体に熟し」と誤った場合など

表 4.2: 不正事象と検知方法の関係（カレー実験）

分類	不正事象	検知方法
越権行為	編集	php によるログ取得
	管理者	php によるログ取得
コピペ	PDF	javascript 検知
	テキスト	javascript 検知
	透かし	回答内容の分析
怠け	でたらめ	回答内容の分析
	途中放棄	回答内容の分析
低得点	低得点	回答内容の分析

2. javascript によるキーボード操作の検知

   テキストボックスの入力欄で Ctr+C，Ctr+V や右クリックのコピー，ペーストを押した回数を javascript の oncopy，onpaste を利用して検知し，ログをデータベースに出力した．

3. 被験者の回答内容を分析して判定

   本サイトは，アンケートの回答データ，PDF ファイルの入力テキストのデータを全てデータベースに保存した．

   なお，ユーザは編集ボタンを押下して，PDF のテキストデータを複数回入力することがあった．この場合，透かし、途中放棄、でたらめ文入力の検知は各ユーザーの最後の入力文を分析対象とした．

不正事象と検知方法の関係を表 5.5 に示す．

4.3 実験結果

4.3.1 ユーザ数

被験者のユーザ数は 192 名である．被験者は，クラウドワークスの作業完了報告時に自らの属性を回答した．表 4.3 は属性別のユーザ数である．なお，被験者の属性は，職業では役員，公務員が，年齢では 70 代以上が存在しなかった．

グループ A は，グループ D と比べて 7 名少ない．グループは，被験者がアカウントを新規登録するごとに順番に割当ており，乱数による差ではない．ユーザが途中放棄したと想定される．共通 ID かつアカウント名表示がない場合，業務自体を放棄する傾向にあるかもしれない．

4.3.2 不正事象

4.3.2.1 不正事象別発生ユーザ

表 4.4 は，不正事象別の発生ユーザ数である．ユーザ数は，表 4.1 に基づいて各分類に属するグループの和をカウントした．たとえば，共有 ID はグループ A と C のユーザ数の和である．

表 4.3: ユーザ数（カレー実験：グループごと）

グループ	*A*	*B*	*C*	*D*	Total
男性	18	21	18	21	78
女性	27	26	30	31	114
19 才以下	1	1	2	1	5
20 才〜29 才	13	14	9	12	48
30 才〜39 才	13	16	16	25	70
40 才〜49 才	11	12	19	10	52
50 才〜59 才	6	4	0	4	14
60 才〜69 才	1	0	2	0	3
会社員	10	16	8	18	52
自営業	11	4	11	10	36
学生	5	4	4	3	16
専業主婦，専業主夫	9	7	13	8	37
パート，アルバイト	4	9	7	6	26
無職	3	2	4	4	13
その他	3	5	1	3	12
N	45	47	48	52	192

表 4.4: 不正事象別ユーザ数（カレー実験）

分類	N	越権行為	コピペ	怠け	低得点
共有 ID(A+C)	93	14	28	6	20
		∧	∧	∨	∨
個別 ID(B+D)	99	18	35	4	13
ID 表示なし (A+B)	92	18	27	3	21
		∨	∧	∧	∨
ID 表示あり (C+D)	100	14	36	7	12

共有 ID を利用したユーザによる不正事象が多いことを期待したが「越権行為」や「コピペ」では個別 ID のほうが多く，期待とは異なっていた．また，ID 表示ありは「コピペ」や「怠け」の不正事象について，ID 表示なしのユーザよりも多くのユーザが不正事象を発生させている．

4.3.2.2 不正事象の相関関係

図 4.3 は，不正事象の発生ユーザ数における事象同士の相関関係である．不正事象同士において明確な相関関係は存在せず，独立している．

4.3.2.3 所要時間

図 4.4 は，カレー実験におけるグループごとの所要時間 Tc_i の分布を表している．なお，所要時間 Tc_i は，本サイトがアカウントを払い出してから作業完了パスコードを表示するまで時間を指

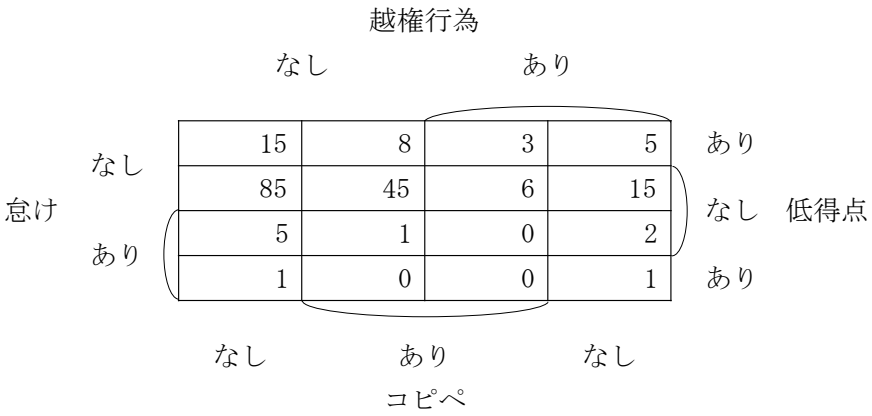

図 4.3: 不正事象の相関関係

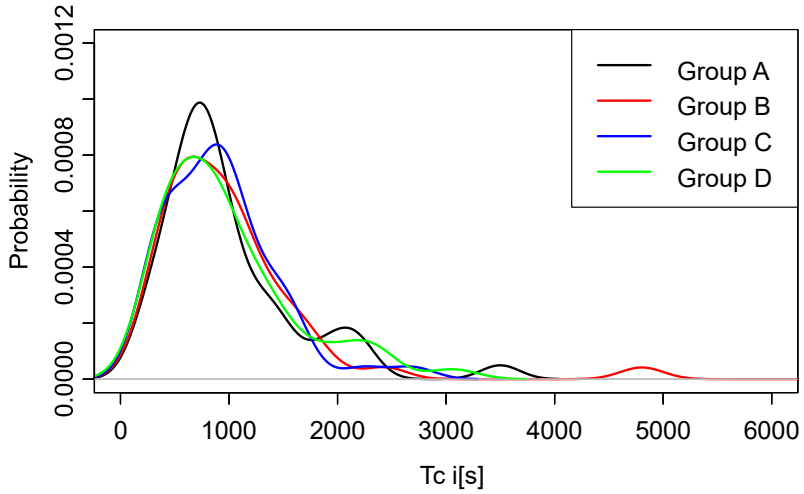

図 4.4: グループごとの所要時間 Tc_i の分布

す．グループごとに大きな差は見受けられない．

図 4.5 は，グループごとの 5.2.7.1 項で定めたアンケートの整合性得点 Cs_i の分布を表している．グループ A のユーザが得点がやや低いことが分かる．

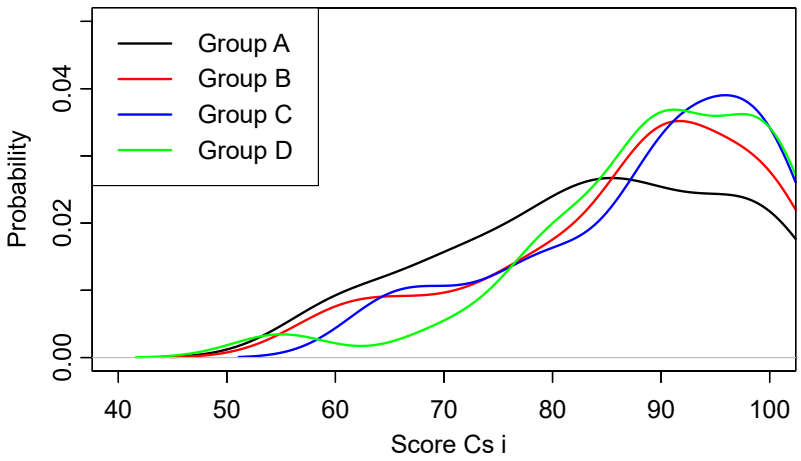

図 4.5: グループごとの得点 Cs_i の分布

表 4.5: カイ 2 乗検定の分析結果（カレー実験）

仮説	不正事象	χ^2	df	P value	
仮説 $H_{\text{共有 (カレー)}}$	越権行為	0.1502	1	0.698	
	コピペ	0.3843	1	0.535	
	怠け	0.1819	1	0.669	
	低得点	1.8108	1	0.178	△
仮説 $H_{\text{表示 (カレー)}}$	越権行為	0.7054	1	0.401	
	コピペ	0.6837	1	0.408	
	怠け	0.7053	1	0.401	
	低得点	3.2217	1	0.073	*

4.4 評価

4.4.1 独立性の検定

各不正事象の発生ユーザ数は，有意な差があるのか検定する．表 4.4 を対象として検定した．そこで，5.2.2 項で定めた仮説について，表 4.1 で定めたグループごとに有意な差があるかを統計的に検定するため，次の H_0 と H_1 について自由度 Df=3 のカイ 2 乗検定を行う．

- 仮説 $H_{\text{共有 (カレー)}}$
  - 帰無仮説 (H_0): 共有 ID と個別 ID の不正発生は独立である．
  - 対立仮説 (H_1): 共有 ID と個別 ID の不正発生は独立ではない．
- 仮説 $H_{\text{表示 (カレー)}}$
  - 帰無仮説 (H_0): ID 表示と ID 非表示の不正発生は独立である．
  - 対立仮説 (H_1): ID 表示と非表示の不正発生は独立ではない．

分析結果を表 4.5 に示す．

表 4.5 の分析結果から仮説 $H_{\text{共有 (カレー)}}$ の不正ユーザ数および仮説 $H_{\text{表示 (カレー)}}$ のうち，低得点以外の不正ユーザ数は，独立に分散していると考えられる．H_2(ID 非表示) のうち，低得点の不正ユーザ数は 10%の有意水準で帰無仮説 H_0 は棄却され，ID 表示と ID 非表示には有意な差がある．

4.4.2 属性による影響分析

本節は，被験者の属性による影響を把握するため機械学習による分析を行う．分析内容は以下の通り．

- 決定木
- 連関規則

表 4.6: ユーザ数（カレー実験：仮説ごと）

	共有 ID（A+C）	個別 ID（B+D）	Total
男性	36	42	78
女性	57	57	114
19 才以下	3	2	5
20 才〜29 才	22	26	48
30 才〜39 才	29	41	70
40 才〜49 才	30	22	52
50 才〜59 才	6	8	14
60 才〜69 才	3	0	3
会社員 (d)	18	34	52
自営業 (b)	22	14	36
学生 (g)	9	7	16
専業主婦，専業主夫 (c)	22	15	37
パート，アルバイト (f)	11	15	26
無職 (a)	7	6	13
その他 (e)	4	8	12
N	93	99	192

表 4.7: 不正事象別ユーザ数（カレー実験：仮説ごと（越権行為，コピペ））

分類	越権行為	コピペ
共有 ID（A+C）	14	28
個別 ID（B+D）	18	35
Total	32	63

分析に利用するデータは表 4.6 および表 4.7 である．表 4.6 は，表 4.3 のユーザ数を表 4.1 に基づいて各分類に属するグループの和をカウントしたユーザ数である．たとえば，共有 ID はグループ A と C のユーザ数の和である．職業のカッコ内は，作成した決定木の対応記号を示す．

表 4.7 は，表 4.4 の不正事象別の発生ユーザ数のうち，共有 ID（A+C），個別 ID（B+D）の集計したもので不正事象「越権行為」「コピペ」を発生させたユーザ数である．

決定木

決定木は，ターゲットである属性を決定する論理条件を明らかにする機械学習であり，根に近い属性が最も大きな条件となる属性である．本実験では，R のパッケージ “rpart ” により学習した決定木を使用する．

「越権行為」をしたかどうか,「コピペ」をしたかどうかをターゲットとして作成した決定木をそれぞれ図 4.6，図 4.7 に示す．ここで,「Job=bcdefg」などの分岐の条件を各節点の上に示し，左側の枝が条件にあてはまる.「不正者数/正規者数」を各節点の下に示す．“Malicious ” や “OK ” は人数の多い方を示す．たとえば，図 4.6 の木では職業が無職以外 (無職=a) かどうかが不正を犯すかどうかを決める最も大きな条件であり，無職には 0 名の不正者と，13 名の正規者がいる．図 4.7

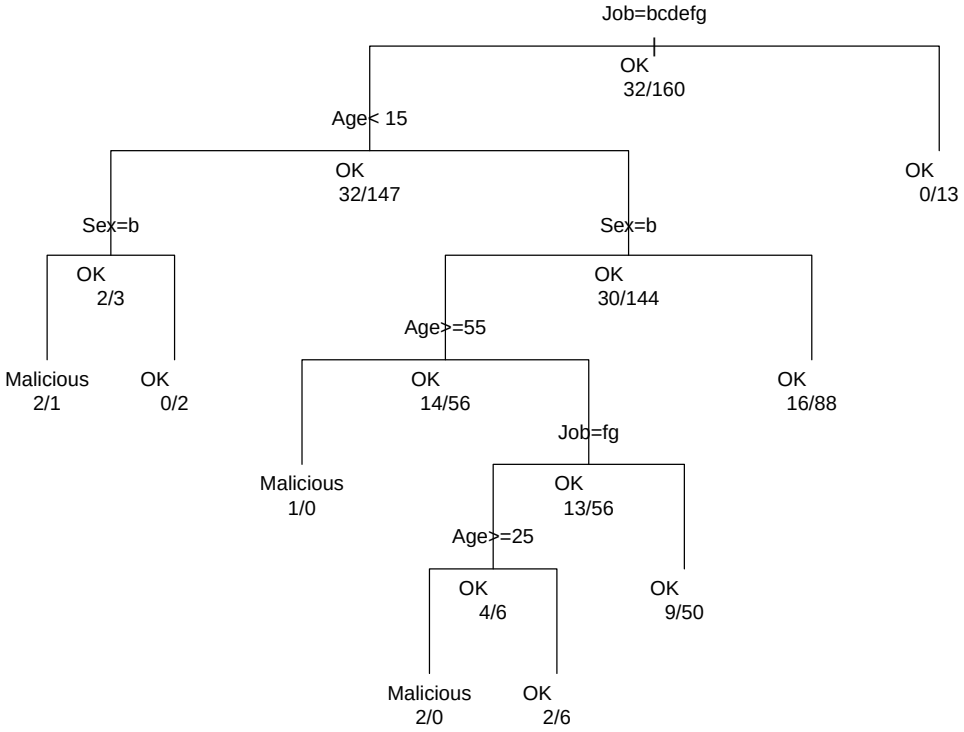

図 4.6: 「越権行為」の決定木

の木では職業が無職，自営業かどうかが最も大きな条件である．グループが共有か，個別かによる分岐は現れなかった．

連関規則

実験結果から属性の組み合わせにより不正への影響があったかを明らかにする為に，R のパッケージ “arules ” を使用して連関規則の抽出を行った.「越権行為」,「コピペ」それぞれの抽出された連関規則の一部を表 4.8，表 4.9 に示す.

support（支持度）は同時確率 $p(lhs, rhs)$，すなわち条件部 lhs と結論部 rhs が同時に起こる確率である．confidence（確信度）は lhs で条件付けられた rhs の条件付き確率 $p(rhs|lhs)$ すなわち lhs の属性の組み合わせを持つ被験者の中で rhs が発生する確率である．たとえば，表 4.8 の No.1 の規則は,「個別グループかつ年齢が 40 代の被験者は約 90% の確率で正規者 (Judge1=OK)」であることを意味している．lift は改善率 $p(rhs|lhs)/p(rhs)$ すなわちターゲットとする rhs が全体で発生する確率に対する lhs の条件付き確率確率がどれだけ向上するかを示す．改善率が高いほどその規則が有用である．

「越権行為」については，No.1 で個別グループの場合に正規者であるという規則が抽出された

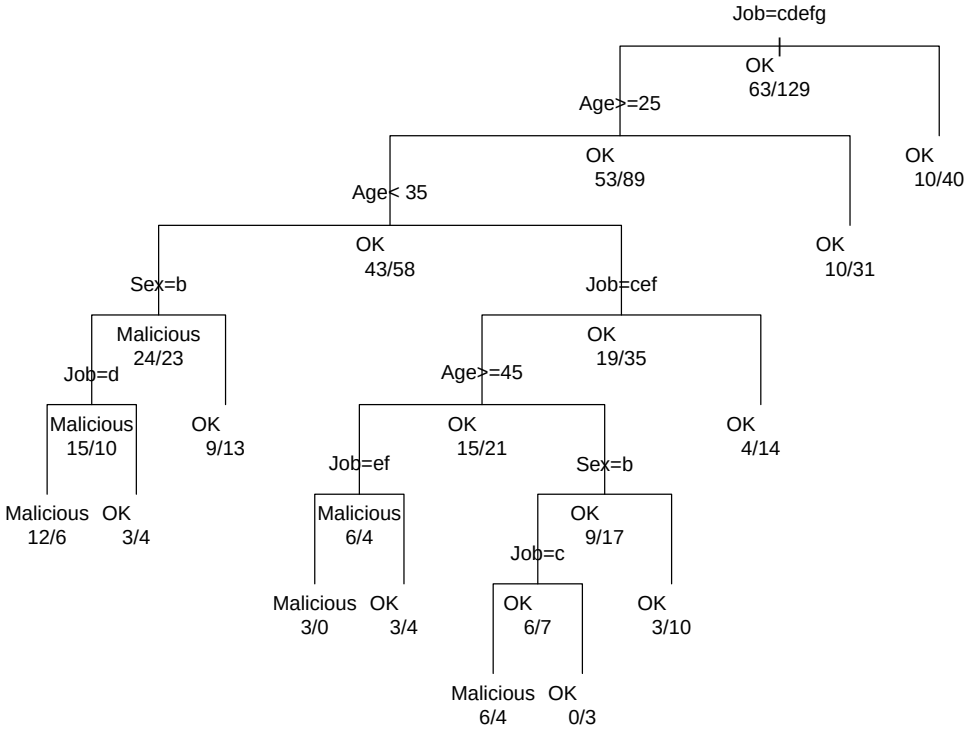

図 4.7: 「コピペ」の決定木

が，No.2～4 のように共有グループで年齢や性別が特定の条件の場合に正規者であるという規則も抽出された．また，不正を犯す条件についての規則は抽出されなかった.「コピペ」については，No.1～2 で不正を犯す場合の，No.3～7 で正規者である場合の規則が抽出された．No.1 では「個別グループ」の場合に，No.2 では「個別グループかつ性別が男性」の場合に不正者であるという規則が抽出された．特に「個別グループの男性」は約 52 %が不正を犯すという規則が示された．正規者についての規則は個別グループ，共有グループどちらの場合にも特定の条件の時に正規者であるという規則が抽出された．

表 4.8: 「越権行為」の連関規則（一部）

No.	lhs（条件部）	rhs（結論部）	support	confidence	lhs. support	lift
1	{group=個別,Age=40's} =>	{Judge1=OK}	0.1042	0.9091	0.1146	1.0909
2	{group=共有,Age=20's} =>	{Judge1=OK}	0.1042	0.9091	0.1146	1.0909
3	{group=共有,Age=30's} =>	{Judge1=OK}	0.1354	0.8966	0.1510	1.0759
4	{group=共有,Sex=女性 } =>	{Judge1=OK}	0.2604	0.8772	0.2969	1.0526

表 4.9: 「コピペ」の連関規則（一部）

No.	lhs（条件部）	rhs（結論部）	support	confidence	lhs. support	lift
1	{group=個別 } =>	{Judge2=Malicious}	0.1823	0.3535	0.5156	1.0774
2	{group=個別,Sex=男性 } =>	{Judge2=Malicious}	0.1146	0.5238	0.2188	1.5964
3	{group=個別,Age=20's} =>	{Judge2=OK}	0.1146	0.8462	0.1354	1.2594
4	{group=個別,Sex=女性 } =>	{Judge2=OK}	0.2292	0.7719	0.2969	1.1489
5	{group=共有 } =>	{Judge2=OK}	0.3385	0.6989	0.4844	1.0403
6	{group=共有,Age=40's} =>	{Judge2=OK}	0.1094	0.7000	0.1563	1.0419
7	{group=共有,Sex=男性 } =>	{Judge2=OK}	0.1354	0.7222	0.1875	1.0749

4.5 考察

4.5.1 ID 表示がない場合の内部不正への影響

表 4.5 により，不正事象「低得点」と「ID 表示なし」は相関があることが分かった．ID 表示がない場合，作業のモチベーションが低下し，アンケートへの回答を真面目に答えないユーザが多く発生した．

一方，表 4.4 によれば，不正事象「コピペ」,「怠け」を発生させたユーザ数は「ID 表示あり」のほうが多い．筆者は「ID 表示あり」のユーザの方が作業に対して真面目に取り組むことを期待した．これらの関係については継続して，検討を続ける必要がある．

4.5.2 編集ボタン押下の大量発生

アンケート問 6 の編集ボタンは，押下をしないと作業完了ができない仕組みとしため，想定よりも多くのユーザが押下してしまった．想定される原因は以下のとおりである．

1. 作業が完了しないため，被験者は不正事象を承知のうえで押下した．
2. 利用規約のうち，管理者用のボタンは押下禁止である旨を強調していたがそれでも見逃していた．

実験の性質上，不正事象は一定程度発生させる必要があったが，実験環境をうまく設計しないと事象が大量に発生することが分かった．この点は今後の課題である．

4.5.3 個別アカウントと監視の関係

筆者は，個別アカウントを利用すると利用者は自らの操作は監視されていると感じ，結果として内部不正を抑制する効果があると想定した．ただ，表 4.4 によれば，被験者の感覚としては必ずしも個別 ID の利用と監視は直接結びついてない可能性がある．WEB サイトにすべての操作ログを取得している旨を常時表示させるなど，利用者に直接的な警告メッセージを表示するほうが監視による内部不正の抑制効果が高いかもしれない．

4.6 結論

本研究は，共通アカウントと内部不正の関係を明らかにするために疑似環境による実験を行った．被験者は 4 つのグループに分けて，グループごとに利用 ID や ID 表示などの条件を変えて不正事象の発生数を観測した．実験結果はカイ 2 乗検定による独立性の検定を行い，ユーザにつねに ID 表示していない場合，内部不正の相関関係に有意な差ががみられた．しかし，一部の不正事象ではユーザに ID をつねに表示していたほうが不正事象が多く発生した．また，共通アカウントと内部不正における相関は確認できなかった．

不正事象ごとに内部不正の発生数が異なった原因やより実環境に近い形での実験の実施については今後の課題である．

第5章　アカウントの共有における内部不正誘発要因の識別（本実験）

5.1　導入

前章では疑似環境において予備実験を行った．なお，被験者には，利用規定で行動を観測することを明記して，その同意を取得している．被験者には，4 つのグループをランダムに割り当てた．被験者に払い出すアカウントは共有 ID と個別 ID のいずれかとし，さらにつねにアカウント名が画面に表示されるグループと表示されないグループに分類した．疑似環境で観測することにより，セキュリティポリシに違反することなく従来困難であった共有 ID を利用する被験者がより多くの不正事象を発生させることを期待したが，個別 ID を利用する被験者の方が多くの不正を犯した．個別 ID は，疑似環境が独自に払い出したものであり被験者はあまり警戒せずに作業を行ったことが，原因の 1 つと考えている．そこで，予備実験における反省点をふまえ，我々は新たな実験（以下，本実験とする）を行った．予備実験と本実験の概要における差異を 5.1 に示す．

本実験は，予備実験と同様に不正事象の発生数を測定する．大きな違いは個別アカウントを被験者の現有する正規の ID[1] にした点である．個別 ID が正規の ID であると，被験者は作業報酬に関わるものと強く感じ，内部不正を抑制する効果がある．

測定結果に対してフィッシャーの直接確率検定による独立性の検定を行うことで，30 代の被験者では共有 ID の利用と内部不正は独立ではなく，関係があることが分かった．また，ロジスティック回帰分析を行い，30 代の被験者は共有 ID を利用すると内部不正を発生させる確率が約 3 倍になることを明らかにした．

5.2　実験のデザイン

5.2.1　実験対象とする要因

本研究の目的は内部不正を誘発する要因を識別することであるが，これらの要因は様々なものが存在する．監視が緩いと感じるものの中には，共有アカウントの利用とアカウント名の非表示がある．共有アカウントの利用は，利用者の識別が困難になることから従業員が“監視が緩い”と感じることを想定した．また，アカウントの非表示は，利用者が自らのアクセスをシステムが記録していると認識する契機が少なくなり，“監視が緩い”と感じると想定した．この要因は共有の影響を考えたときに無視できない要因であるため，実験に加えることとした．そこで，本実験では共有アカウントの利用やアカウントの非表示を実験対象の要因とし，不正行為の発生に与える影響を評価する．

[1] クラウドソーシングサービス Lancers の正規の ID である Lancers ID

表 5.1: 予備実験と本実験の比較

項目	予備実験	本実験
実験実施期間	2016 年 6 月 26 日〜28 日	2016 年 10 月 31 日〜11 月 4 日
実験環境	疑似環境 (1 サイト)	疑似環境 (2 サイト)
作業内容	アンケート，データ入力	検索エンジンの評価
クラウドソーシングサービス	Crowdworks	Lancers
個別アカウントのユーザ名	独自 ID(使い捨て)	被験者の Lancers ID
共有 ID が内部不正を誘発する効果	有意な差はなかった	30 代に有意な差があった

5.2.2 実験の仮説

本研究は，不正行為を誘発する要因として，次の 2 つの仮説を立てる．
仮説 $H_{\text{共有 (検索)}}$：共有アカウント（例：guest アカウント）を利用していると不正行為を犯す．
仮説 $H_{\text{表示 (検索)}}$：作業中に常時アカウント名が明示 [2] されていないと不正行為を犯す．

5.2.3 実験の課題

疑似環境において共有 ID と不正行為の関係を識別する際には以下の課題が存在する．

1. 不正事象を誘発する要因の制御

   被験者が報酬を受け取ってタスクを遂行する際には，一般的には数多くの不正行為が発生することを期待できない．一方，報酬を支払わない場合，被験者を集めることは容易ではない．そのため，優良な被験者に対して不正事象を誘発させるための仕掛けが必要となる．

2. 共有アカウントを利用した被験者の識別

   被験者が共有アカウントを利用する場合，アカウントごとの操作履歴で被験者を識別することはできない．アカウント以外の方法で，被験者を一意に識別することは自明ではない．

3. 個別アカウントと共有アカウントの差別化

   被験者にとっては，疑似環境で独自に払い出した個別アカウントは一度しか使わない，いわば “使い捨て ID” である．“使い捨て ID” は SNS や EC サイトのアカウントのように長期間利用するものと比べて，被験者にとっての価値は低いと推察する．そのため，“使い捨て ID” を利用した被験者は，監視がされていると強く感じることもなく，今後の社会活動にも支障をきたす可能性が少ないため，不正行為を抑制する効果は薄く，共有アカウントとの差が生じにくい．

[2] WEB サイトの各ページの上端に常時ユーザ名が表示されている状態

表 5.2: グループと仮説の関係（検索実験）

グループ	$H_{\text{共有 (検索)}}$	$H_{\text{表示 (検索)}}$	N
A	共有	非表示	52
B	個別		52
C	共有	表示	46
D	個別		48

5.2.4 課題へのアプローチ

本研究は，5.2.3 節の課題について次のように解決を試みた．

5.2.4.1 不正事象を誘発する要因の制御

Kelling ら [24] による割れ窓理論によると，荒れた街では犯罪の発生率があがるといわれており，本実験では環境を悪くすることで被験者が多くの不正事象を発生させることを想定した．また，本実験では共有 ID の効果を調べることが主な目的であり，ID 共有ありとなしの比や差が，通常環境でも誘発環境でも相似することを仮定している．条件付き確率では，

$$\Pr(\text{不正} \mid \text{共有 ID}) \propto \Pr(\text{不正} \mid \text{共有 ID, 誘発環境})$$

$$\Pr(\text{不正} \mid \text{個別 ID}) \propto \Pr(\text{不正} \mid \text{個別 ID, 誘発環境})$$

となることを仮定しており，割れ窓理論に基づいてこの 2 つの確率の比がほぼ等しいならば，調整されたオッズ比は，

$$\frac{\Pr(\text{不正} \mid \text{共有 ID})}{\Pr(\text{不正} \mid \text{個別 ID})} \fallingdotseq \frac{\Pr(\text{不正} \mid \text{共有 ID, 誘発環境})}{\Pr(\text{不正} \mid \text{個別 ID, 誘発環境})}$$

で近似できる．この考え方は，割れ窓理論やハインリッヒの法則 [21] に基づいたものであり，商品検査などで高温多湿の環境試験室で実験評価が行われることに似ている．誘発環境を構築するため，本実験ではすべての被験者に対して以下の要因を与えることとした．

1. 被験者にストレスを与えることで，モチベーションを低下させる（5.2.8 節の (1) と (2) の実装方式に対応）．
2. 被験者が真面目にやらなくても記録が残らないように見せる（5.2.8 節の (3) の実装方式に対応）．
3. 被験者は途中で作業を終わらせてもよいように見せる（5.2.8 節の (4) の実装方式に対応）．

5.2.4.2 共有アカウントを利用した被験者の識別

被験者が疑似作業で扱うデータは被験者ごとに変え，一意に与える．被験者が入力したデータはすべて疑似環境に記録し，誰に払い出したデータであるかを確認することで被験者を識別する（5.2.8 節の (5) の実装方式に対応）．

表 5.3: 実験デザインの概要

5.2.1 実験対象とする要因	5.2.2 実験の仮説	5.2.3 実験の課題	5.2.4 課題へのアプローチ
共有アカウントの利用，アカウントの非表示	仮説 $H_{\text{共有 (検索)}}$，仮説 $H_{\text{表示 (検索)}}$	不正事象を誘発する要因の制御	ストレスを与える，作業記録が残らないようにみせる，作業を途中で終了させてもよいようにみせる
		共有 ID 利用被験者の識別	作業データを被験者ごとに一意のものを与える
		個別 ID と共有 ID の差別化	LancersID の利用

5.2.4.3 個別アカウントと共有アカウントの差別化

被験者が日常的に利用するアカウントを実験の個別アカウントとして活用する．Lancers ID は，被験者がクラウドソーシングサービスでタスクの作業を行い，報酬を得るために必要なアカウントである．Lancers ID を利用して不正な作業を行うと Lancers での作業が承認されず，作業承認率が低下してしまい，クラウドソーシングサービスにおける自らの立場が悪化するリスクがある．よって，使い捨て ID を使う場合と比べて，真面目に作業を行うことを期待する（5.2.8 節の (6) の実装方式に対応）．

本実験の実験デザインの概要を表 5.3 に示す．

5.2.5 実験概要

我々は，組織の業務環境を再現した擬似作業用システム（以下，作業システム）を構築した．作業システムは，検索ワード案内サイト（以下，案内サイト）と検索エンジン評価サイト（評価サイト）で構成する．仮説を検証するため，被験者を 4 つのグループに分割した．グループごとに異なる刺激を与えることで不正事象の発生数にどれだけの差があるのかを観測した．表 5.2 に仮説と被験者グループの関係を示す．

実験実施期間は 2016 年 10 月 31 日（月）〜11 月 4 日（金）の 5 日間である．平日を対象とすることで，企業や団体の組織の就業時間にあわせることとした．

5.2.5.1 被験者

(1) 本実験の母集団と標本

本実験の母集団は，クラウドソーシングサービスの被雇用者（労働者）とする．この被雇用者とは企業，団体，個人事業主などに雇われている人のことを指す．大手教育会社の情報漏えい事故では業務委託先の元社員が内部不正を起こしているが，この元社員は被雇用者に含まれる．標本はランサーズ社によるクラウドソーシングサービスの被雇用者のうち，本実験の作業を完了した被験者である．本実験は，クラウドソーシングサービスにより，被験者に業務を委託している．そのため，被験者は被雇用者と見なすことができると考えた．

本実験の母集団は，クラウドソーシングサービスの被雇用者であるため，本実験は無作為抽出で被験者を抽出することが望ましい．一方，クラウドソーシングにおいて本実験のようなマイクロタスクを依頼する場合，被験者は原則先着順で受付ける形となり，依頼者は被験者が正しく作業完了した場合には，正当な理由なくその作業を否認することができない．そのため，本実験では被験者を先着順で受付けた．このような仕組みであるため，恣意的な抽出はしていないが，クラウドソーシングサービスには様々な属性を持ったユーザが登録されているため，母集団を代表するような標本が得られると期待した．

(2) 必要な標本の大きさ

丹後ら [25] によれば，2 つの母平均の差の検定（片側検定）においては，有意水準 α，検出力 $1-\beta$ のときに必要な標本の大きさ n は次式で計算できる．

$$n = 2\left(\frac{Z(\alpha) + Z(\beta)}{d}\right)^2$$

Z は正規分布の上側 100α パーセント点である．第 2 種の過誤の確率 β は α の約 4〜5 倍に設定されることが多い．検出したい有意差 d は，次の慣例的性質を利用して目安をつけることができる．

(a) 小さな差を検出したければ $d = 0.1$〜0.2

(b) 中位な差を検出したければ $d = 0.4$〜0.5

(c) 大きな差を検出したければ $d = 0.8$〜0.9

本実験において有意水準を 5%とした場合，$\alpha = 0.05$，$1-\beta = 0.80$，不正行為を誘発する要因の有無における差は，大きな差であることから $d = 0.8$ とすると，必要な標本の大きさ n は

$$\begin{aligned} n &= 2\left(\frac{Z(0.05) + Z(0.2)}{0.8}\right)^2 \\ &= 2\left(\frac{1.645 + 0.842}{0.8}\right)^2 = 19.32 \end{aligned}$$

より，20 名である．5.2.5.3 項にあるとおり，本実験は仮説を検証するために，それぞれの仮説ごとに被験者を 2 つに分割した．たとえば，共有 ID の場合，共有 ID と個別 ID の 2 つの要因が該当する．標本となる被験者は要因ごとに必要となるため，仮説を検証するために必要な被験者数は 40 名と想定した．

5.2.5.2 作業の流れ

図 5.1 に作業システムの画面遷移図を示す．まず，被験者はランサーズ社から作業を受託する．次に案内サイトにアクセスして，ランサーズ社のクラウドソーシングサービスにおける被験者の個別アカウントである Lancers ID を入力する．作業システムは被験者が作業を開始する前に利用規約を表示し，同意ボタンを押下しないと作業を開始できないようにした．利用規約を確認後，70 語の検索ワードを確認する．

その後，評価サイトにアクセスする．評価サイトは，個別 ID，共有 ID のいずれかを被験者に付与する．個別 ID が付与された被験者は，再び Lancers ID を入力して評価サイトの ID，PASS を確

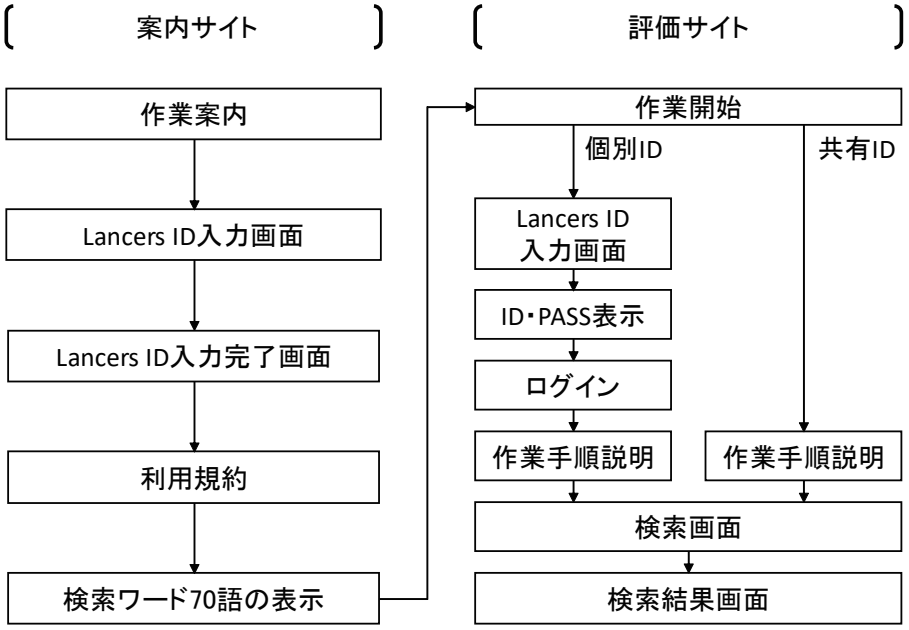

図 5.1: 画面遷移図（検索実験）

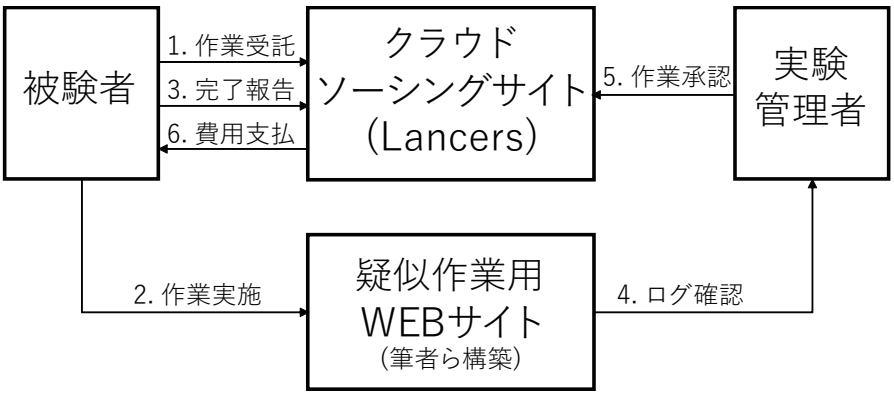

図 5.2: 作業の流れ（検索実験）

認し，評価サイトにログインする．その後，作業手順説明を確認する．一方，共有 ID が払い出された被験者は，ログインなどの作業は要求されず，作業手順説明を確認する．検索画面では案内サイトで表示された検索ワードを入力し，検索結果を確認する．

作業の流れを図 5.2 に示す．作業完了後，被験者はランサーズ社に完了報告を行う．我々は完了報告に基づいて利用状況を作業システムのアクセスログから確認し，問題がなければ作業を承認する．作業承認後，ランサーズ社は我々が事前に支払をしていた費用の一部を被験者に支払う．なお，本実験では，実験実施期間であればいつでも被験者が作業を実施可能な状態とした．

5.2.5.3 仮説とグループの関係

評価サイトでは，以下の仕組みを構築することで仮説を検証した．仮説 $H_{\text{共有 (検索)}}$ を検証するため，評価サイトではグループ A と C の被験者には共有アカウント “Guest” を払い出した．なお，

作業システムは “Guest” アカウントを払い出した場合でも被験者ごとの行動を識別できるようにした．グループ B と D の被験者には個別アカウントを払い出した．アカウント名は “userxxxxx” であり，xxxxx は被験者ごとに 0〜9 の数字について 5 ケタの乱数を割り当てた．仮説 $H_{\text{表示 (検索)}}$ を検証するため，グループ A と B の被験者はアカウント名をいっさい表示させなかった．一方，グループ C と D の被験者には画面の上端に利用中のアカウント名を常時表示させた．

5.2.5.4 医療分野における研究と本実験の類似点

丹後ら [25] によれば，医療の分野においては，疫病の発症する確率を推定し，発生要因を検討するための解析手法として，ロジスティック回帰分析が利用されている．また，ある特定の要因の効果を調べたい場合において，他の交絡因子の影響を調整するために調整オッズ比を求めることができる．たとえば，癌の罹患率はとても低いが，オッズ比にすることで，交絡因子の影響を調整して要因の影響を評価している．この分析手法を参考とし，本実験は，5.2.5.3 項に定義したグループごとに被験者を分割し，グループごとに異なる要因を与えた．5.2.7 節で定義する不正事象の発生数と要因の関係をロジスティック回帰分析で分析する．

5.2.5.5 倫理規定への適合性

本実験は，被験者が発生させる不正事象を観測することから，倫理規程の適合性などについて以下に述べる．

(1) クラウドソーシングサービスの利用規約

本実験で利用したランサーズ社のクラウドソーシングサービスの利用規約においては，本実験の実施が規約に抵触しないことを確認した．たとえば，ランサーズ利用規約第 24 条本サイトの取引に関する禁止事項 (11) には，以下の記載がある．

> 「自身の詳細な個人情報又は他のユーザ，弊社若しくは他社の個人情報（電話番号は住所等）を発信及び公開する行為，又は依頼内容において，提案時にユーザ自身の詳細な個人情報の記載を要求する行為」

本実験は，被験者の性別，属性，職業は収集しているが，特定の個人を識別する情報は取得をしていないため，当該利用規約には低触しないと考えられる．

表 5.4: 検索ワードの例

ユーザ *A*	名前	名告	君臣	喪	土
	地所	坂田	基	墓地	多摩川
	大洲	天皇	太田	妹	季 …
ユーザ *B*	学問	学派	守治	家督	宸翰
	河	添	狩谷	甚三郎	目黒
	弟子	往	心	忠与	忠員 …
ユーザ *C*	或日	折衷	斧太郎	昌安	春泰
	時信	晴雪	更迭	書	最後
	有	木村	林	某	植村 …

(2) 本実験の利用者における合意

本実験において用いたタスクの募集要項[3]には，このタスクは本サイトの使用感を確かめることを目的としていることを明示した．被験者はこの募集要項を確認のうえ，本実験に参加していると想定される．5.2.8 節にある応答時間の遅延や貼付制限などの仕組みは，一般的なウェブサイトでも同様の事象は発生するものであり，使用感を確かめるという主旨を逸脱するものではない．そのため，被験者がこれらの仕組みがある環境で作業することは合意済みであると考えた．

5.2.6 タスクの定義

(1) 検索エンジンの評価

被験者は案内サイトで被験者ごとに一意に決められた 70 語の検索ワードを与えられ，評価サイトでそのうちの 50 語以上を検索することを命じられる．検索ワードの例を表 5.4 に示す．被験者の検索結果は，Google 社の検索 API を利用して表示する．

(2) アンケートの回答

被験者は Lancers の作業完了報告画面で，評価サイトを利用した感想や被験者自身の属性（年代，性別，職業）などのアンケートに回答する．感想は，被験者が自身に与えられた作業を完了させるために求める．

5.2.7 不正事象

5.2.7.1 不正事象の定義

3 種類の不正事象を定義する．

(1) 途中放棄

評価サイトで検索したキーワードが 50 語未満である．

[3]募集要項の詳細は C.2 節参照.

表 5.5: 不正事象と検知方法の関係

不正事象	検知方法
(1) 途中放棄	回答内容の分析
(2) でたらめ	回答内容の分析
(3) 違反行為	php によるログ取得

表 5.6: 被験者の検索回数 s と遅延時間，貼付制限の関係

検索回数 s	遅延時間（秒）	貼付制限
1〜5	0	
5〜13	1	
13〜19	2	
19〜23	3	
23〜31	4	
31〜33	20	
33〜37	2	
37〜41	9	
41〜43	20	○
43〜45	5	○
45〜47	9	○
47〜	5	○

(2) でたらめ

評価サイトで検索したキーワードが，案内サイトで提示した文字列と異なる場合やキーワード自体が未入力である．

(3) 違反行為

評価サイトにおける管理者画面へのリンクを押下した．これは，利用規約で定めた禁止事項「管理者画面にアクセスすること」に該当する．

5.2.7.2 検知方法

不正事象は以下のようにして検知する．不正事象と検知方法の関係を表 5.5 に示す．

- 被験者の回答内容を分析して判定
  不正事象 (1) 途中放棄，(2) でたらめを検知するため，被験者が検索した文字列や案内サイトが与えた検索ワードを分析する．
- php によるアクセスログの取得
  不正事象 (3) 違反行為を検知するため，管理者画面へのアクセスは，php を利用してデータベースに記録したログから判断する．

5.2.8 課題に対する実装方式

5.2.4 節に記載した課題へのアプローチについて，作業システムに実装した仕組みを以下に記す．

(1) 応答時間の遅延
評価サイトの検索処理は Google 社の検索 API を利用しているため，本来の処理速度は 1 秒未満であるが，javascript によって被験者の検索回数をカウントし，回数 s に応じて表 5.6 のように人工的な遅延を生じさせる．

遅延時間により，被験者のモチベーションを低下させ，被験者がより多くの不正事象を発生させることを期待した．応答時間の遅延はすべての被験者に対して一律に適用する．

(2) 貼付制限
案内サイトが表示した検索ワードの中には読み方が比較的難しい単語[4] を含めている．読み方が分からない場合，多くの被験者は検索ワードをいったんコピーして，評価サイトに貼り付ける．そこで評価サイトでは，javascript によって被験者の検索回数をカウントし，41 回目以降の検索では，ブラウザ上での貼付行為を無効化した．作業に対する難易度を上げることで，被験者により多くの不正事象を発生させる．

検索回数 s と貼付制限の関係を表 5.6 に示す．貼付制限はすべての被験者に対して一律に適用する．

(3) 検索回数と作業完了の関係
すべての被験者に対して，評価サイトの検索画面や検索結果画面では，被験者が検索した回数などを表示しない．また，被験者はたとえ 50 回以上を検索しなくてもランサーズ社に作業完了を報告できる．作業完了報告を被験者の自己申告制とすることで，多くの被験者に不正事象を発生させる．

(4) ログイン認証の未実施
共有 ID を利用する被験者は案内サイトでは Lancers ID を入力したが，評価サイトではログインなどの認証を不要とする．

(5) 共有アカウントを利用した被験者の識別
案内サイトは，被験者ごとに一意の検索ワードを与える．表 5.4 は検索ワードの例である．検索ワードの掲載数は 70 語である．検索された検索ワードをすべて記録することで，共有アカウントを利用した被験者であっても，誰がアクセスしたのかを識別することができる．

(6) 個別アカウントと共有アカウントの差別化
評価サイトが払い出す個別 ID は，被験者が入力した Lancers ID とする．パスワードは新たに乱数で生成し，被験者のプライバシ情報を取得しないようにする．

5.3 実験結果

5.3.1 被験者数

本実験はクラウドソーシングサービスを使い，200 名の被験者を募集した．被験者のうち，2 名は案内サイトにおける LancerID の入力に誤りがあり，被験者の作業結果と LancersID の紐付けが

[4] 例：宸翰（表 5.4 のユーザ B の 5 番目）

表 5.7: 被験者数（A：共有/ID 非表示，B：個別/ID 非表示，C：共有/ID 表示，D：個別/ID 表示）

グループ	A	B	C	D	Total
19 歳以下	0	0	1	0	1
20 歳〜29 歳	8	2	7	6	23
30 歳〜39 歳	18	19	17	22	76
40 歳〜49 歳	16	24	14	14	68
50 歳〜59 歳	6	5	6	5	22
60 歳〜	4	2	1	1	8
男性	28	30	23	28	109
女性	24	22	23	20	89
会社員	16	17	6	9	48
公務員	1	0	0	0	1
自営業	13	13	15	16	57
パート，アルバイト	7	5	2	5	19
専業主婦，専業主夫	6	10	13	8	37
学生	0	0	1	1	2
無職	5	6	4	6	21
その他	4	1	5	3	13
N	52	52	46	48	198

できなかった．そのため，被験者は 198 名である [5]．被験者は，ランサーズ社の作業完了報告時に自らの属性を回答した．表 5.7 は属性別の被験者数である．グループ C は，グループ A，B と比べて 6 名少ない．グループは，評価サイトが被験者のアクセス順に割り当てており，乱数による差ではない．被験者が作業自体を途中で止め，作業完了報告も行わなかったと想定する．

5.3.2 検索回数と所要時間

1 番目の検索から i 番目の検索までの所要時間を Ts_i [秒] とする．被験者の検索回数 s と所要時間 Ts_i の関係は，おおむね次の 4 つのパターンに分類された．

1. 途中で作業を止めた（赤：User 1（不正事象））．
2. 50 語を超過した時点で検索を止めた（青：User 2）．
3. 応答時間の遅延や貼付制限が出現したタイミングで止めた（緑：User 3（不正事象））．
4. 70 語近くまで検索を続けた（水色：User 4）．

これらの代表例を図 5.3 に示す．被験者の検索回数 s が $s < 50$ の場合，不正事象 (1) 途中放棄に該当するため，図 5.3 の赤線と緑線が不正事象である．

[5] 被験者の属性情報（性別，職業，年代）は Lancers の作業募集画面においてアンケート形式で確認をしているため，LancersID が不明な被験者は，属性を把握することができない．そのため，この 2 名を標本から除外することした．

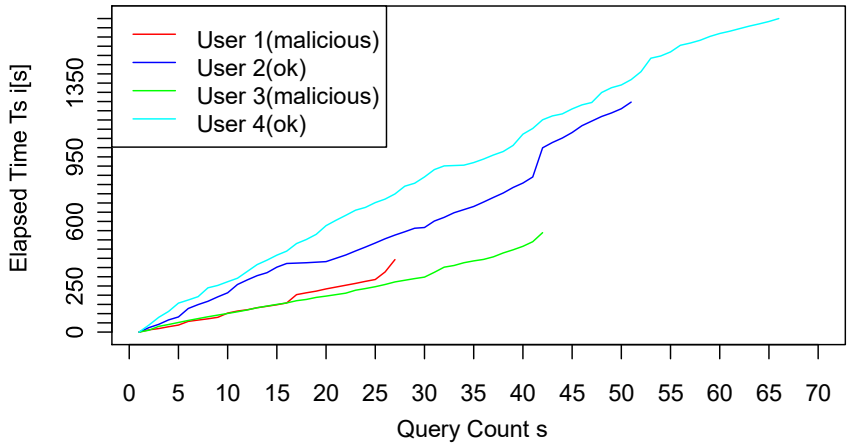

図 5.3: 所要時間と検索回数（代表的な 4 つのパターン）

表 5.8: 不正事象別被験者数

不正事象	*A*	*B*	*C*	*D*	Total
(1) 途中放棄	11	8	9	7	35
(2) でたらめ	5	3	1	2	11
(3) 違反行為	1	1	0	0	2

5.3.3 検索回数（グループごと）

図 5.4 はグループごとの被験者における検索回数 s の累積相対頻度 $Cu(s)$ である．たとえば，グループ A は，Cu（$s < 50$）が 0.21 であり，グループ A の被験者 52 名中の 21%が検索作業を 50 回未満で完了したことを表す．図の中心にある縦点線は，検索回数 $s = 50$ である．被験者のタスク完了条件は，検索回数が 50 回を超えることである．縦点線は 50 回を表しており，50 回を超えた段階で多くの被験者がタスクを完了させていることが分かる．

5.3.4 不正事象

5.3.4.1 不正事象別発生被験者

表 5.8 は，不正事象別の発生被験者数である．不正事象 (1) 途中放棄が多く発生した．(1) 途中放棄の発生被験者数は，共有 ID を利用した被験者（グループ A+C）は 20 名，個別 ID を利用した被験者（グループ B+D）は 15 名であり，個別 ID より共有 ID を利用した被験者の方が多くの不正事象を発生させた．(2) でたらめの発生被験者数は 11 名であり比較的少なく，(3) 違反行為は 2 名であり，ほとんど発生しなかった．

(1) 途中放棄の発生被験者数が多いことから，(1) についての属性別の内訳を表 5.9 に示す．特に年代についてのグループは，不正事象発生被験者数の差が大きい．最も多く不正事象を発生させていたのは 30 歳〜39 歳（以下，30 代）であった．そこで，30 代の被験者におけるグループご

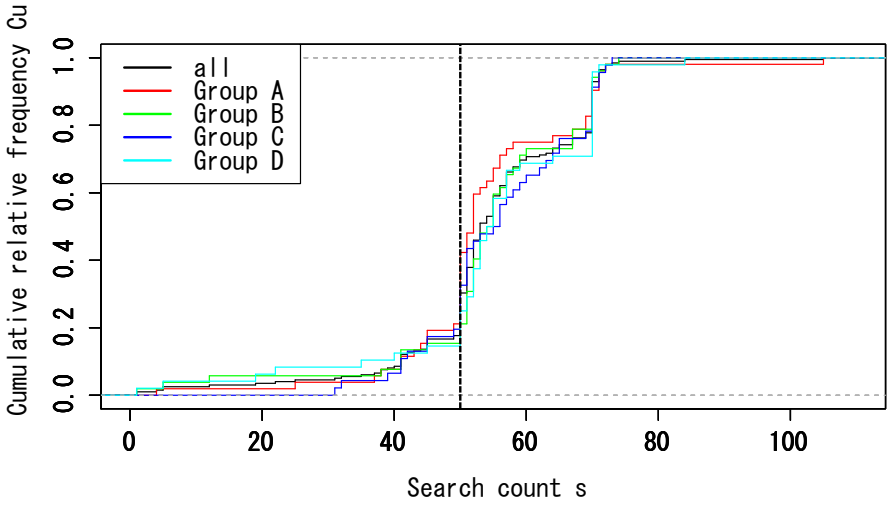

図 5.4: s 回以上検索した累積被験者数

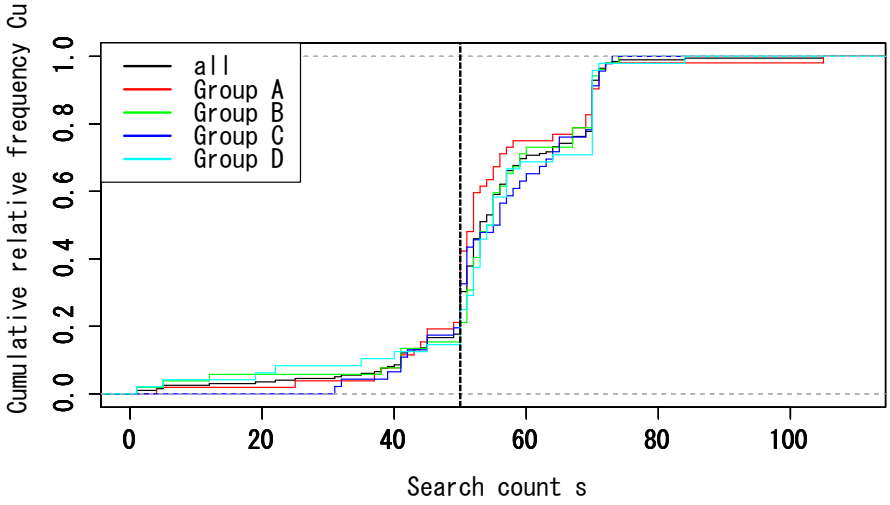

図 5.5: s 回以上検索した累積被験者数（30 代のみ）

との検索回数 s の累積相対頻度 $Cu(s)$ を図 5.5 に示す．ここで s=50 の直線と交点は，グループ A，B，C，D の検索回数 $s = 50$ の Cu（$s < 50$）であり，それぞれ，0.33，0.05，0.18，0.14 であり，グループ A は他のグループと比べて 50 回未満で作業を完了させる被験者が多い．

表 5.9: 不正事象 (1) 途中放棄の発生被験者数

グループ	*A*	*B*	*C*	*D*	Total
～19 歳	0	0	1	0	1
20 歳～29 歳	1	0	1	2	4
30 歳～39 歳	6	1	3	3	13
40 歳～49 歳	0	3	2	1	6
50 歳～59 歳	1	2	1	0	4
60 歳～	3	2	1	1	7
男性	7	5	6	6	24
女性	4	3	3	1	11
会社員	3	3	2	2	10
公務員	1	0	0	0	1
自営業	4	0	3	3	10
パート，アルバイト	1	0	0	0	1
専業主婦，専業主夫	1	2	1	0	4
学生	0	0	1	1	2
無職	1	2	0	1	4
その他	0	1	2	0	3
Total	11	8	9	7	35

表 5.10: 不正事象の発生被験者数（仮説ごと）

分類	不正	$H_{\text{共有 (検索)}}$ 共有 $A+C$	個別 $B+D$	$H_{\text{表示 (検索)}}$ 非表示 $B+D$	表示 $C+D$
途中放棄	あり	20	15	19	16
	なし	78	85	85	78
でたらめ	あり	6	5	8	3
	なし	92	95	96	91
違反行為	あり	1	1	2	0
	なし	97	99	102	94

5.3.4.2 独立性の検定

各不正事象の発生被験者数に有意な差があるのか検定する．丹後ら [25] によれば，2×2 分割表を検証する場合，主にカイ二乗検定やフィッシャーの直接確率検定がある．しかし，カイ二乗検定は分割表のセルの期待値が小さい場合，不正確となることがあるため，フィッシャーの直接確率検定を用いた．5.2.2 節で定めた仮説について，グループごとに有意な差があるかを統計的に検定するため，次の H_0 と H_1 についてフィッシャーの直接確率検定を行う．

- ID の共有について
  - 帰無仮説（$H_{\text{共有 }0}$）: 共有 ID（A，C）と個別 ID（B，D）の不正発生は独立である．
  - 対立仮説（$H_{\text{共有 }1}$）: 共有 ID と個別 ID の不正発生は独立ではない．
- ID の表示について
  - 帰無仮説（$H_{\text{表示 }0}$）: ID 表示（C，D）と ID 非表示（A，B）の不正発生は独立である．
  - 対立仮説（$H_{\text{表示 }1}$）: ID 表示と非表示の不正発生は独立ではない．

検定対象は，各不正事象の発生被験者数および不正事象の発生数が大きい不正事象 (1) 途中放棄の属性別発生被験者数とする．検定対象を表 5.2 の分類で集計したものが表 5.10 および表 5.11 である．検定結果を表 5.12 および表 5.13 に示す．p 値はいずれも 0.05 を上回っており，5%の有意水準で帰無仮説 $H_{\text{共有 }0}$ と，$H_{\text{表示 }0}$ のどちらも棄却するには至らなかった．しかし，一般的な有意水準には達しないものの，非常に特異な事象が起きていることを示しており，ID の共有と不正事象の何らかの関係があるものと考えている．

5.3.4.3 ロジスティック回帰分析

代表的な部分集合である 30 代の被験者において，どの要因が大きく誘発しているかを識別するため，ロジスティック回帰分析を行った．目的変数を不正事象 (1) 途中放棄の発生有無，説明変数を共有 ID，性別，職業としたロジスティック回帰分析の分析結果を表 5.14 に示す．

共有 ID，性別，職業ごとの推定値（説明係数）を x_1，x_2，…，x_7，不正事象の発生確率を $p(x)$ とした場合のロジスティック関数は，

$$p(x) = \frac{1}{1 + \mathrm{e}^{(16.75 - 1.189x_1 - 1.189x_2 - \cdots - 12.90x_7)}}$$

表 5.11: 不正事象 (1) 途中放棄の発生被験者数（属性ごと）

グループ	共有（A+C）		個別（B+D）	
	あり	なし	あり	なし
～19 歳	1	0	0	0
20 歳～29 歳	2	13	2	6
30 歳～39 歳	9	26	4	37
40 歳～49 歳	2	28	4	34
50 歳～59 歳	2	10	2	8
60 歳～	4	1	3	0
男性	13	38	11	47
女性	7	40	4	38
会社員	5	17	5	21
公務員	1	0	0	0
自営業	7	21	3	26
パート，アルバイト	1	8	0	10
専業主婦，専業主夫	2	17	2	16
学生	1	0	1	0
無職	1	8	3	9
その他	2	7	1	3

表 5.12: フィッシャーの直接確率検定の分析結果（仮説ごと）（片側検定）

分類	仮説	P value
途中放棄	$H_{\text{共有 }0}$	0.209
	$H_{\text{表示 }0}$	0.484
でたらめ	$H_{\text{共有 }0}$	0.486
	$H_{\text{表示 }0}$	0.142
違反行為	$H_{\text{共有 }0}$	0.746
	$H_{\text{表示 }0}$	0.275

である．共有 ID の個別 ID に対する不正事象発生確率のオッズ比，$\frac{p(x)}{1-p(x)}$ は 3.284 倍，すなわち ID を共用すると，しないときに対して約 3 倍不正が生じやすくなる．

5.3.5 属性による影響分析

本節は，被験者の属性による影響を把握するため機械学習による分析を行う．分析内容は以下の通り．

- 決定木
- 連関規則

表 5.13: 不正事象 (1) 途中放棄のフィッシャーの直接確率検定の分析結果（属性ごと）（片側検定）

属性	P value	
～19 歳	1.000	
20 歳～29 歳	0.897	
30 歳～39 歳	0.062	*
40 歳～49 歳	0.837	
50 歳～59 歳	0.774	
60 歳～	1.000	
男性	0.277	
女性	0.330	
会社員	0.521	
公務員	1.000	
自営業	0.134	
パート，アルバイト	0.473	
専業主婦，専業主夫	0.718	
学生	1.000	
無職	0.917	
その他	0.797	

表 5.14: ロジスティック回帰分析の分析結果（検索実験）

	変数	推定値（Estimate）	標準誤差（Std. Error）	z Value	Pr(> |z|)	
	（Intercept）	−16.75	1455.39	−0.012	0.991	
1	共有 ID	1.189	0.675	1.760	0.0784	*
2	男性	1.165	0.902	1.292	0.196	
3	パート，アルバイト	14.40	1455.40	0.010	0.992	
4	会社員	13.94	1455.40	0.010	0.992	
5	自営業	13.80	1455.40	0.009	0.992	
6	専業主婦，専業主夫	14.17	1455.40	0.010	0.992	
7	無職	12.90	1455.40	0.009	0.993	

分析に利用するデータは表 5.15 および表 5.16 である．表 5.15 は，表 5.7 のユーザ数を表 5.2 に基づいて各分類に属するグループの和をカウントしたユーザ数である．例えば，共有 ID はグループ A と C のユーザ数の和である．

表 5.16 は，表 5.9 の不正事象 (1) 途中放棄の発生ユーザ数を共有 ID（A+C），個別 ID（B+D）で集計したものである．

決定木

「途中放棄」をしたか否かをターゲット属性として学習した決定木を図 5.6 に示す．年齢が 55 歳以上かどうかが不正を犯すかどうかを決める最も大きな条件であり，55 歳以上には 7 名の不正者と，1 名の正規者がいる．決定木により，不正を誘発する要因として年齢が大きいことが示された．

表 5.15: ユーザ数（検索実験：仮説毎）

	共有 ID（A+C）	個別 ID（B+D）	Total
男性	51	58	109
女性	47	42	89
19 歳以下	1	0	1
20 歳〜29 歳	15	8	23
30 歳〜39 歳	35	41	76
40 歳〜49 歳	30	38	68
50 歳〜59 歳	12	10	22
60 歳〜	5	3	8
会社員	22	26	48
公務員	1	0	1
自営業	28	29	57
パート，アルバイト	9	10	19
専業主婦，専業主夫	19	18	37
学生	1	1	2
無職	9	12	21
その他	9	4	13
合計	98	100	198

連関規則

抽出した連関規則の一部を表 5.17 に示す．No.5 の規則は,「共有アカウントグループの場合に不正を犯す」を表し，lift>1.1 の改善率を持つ．また，共有アカウントならば，20%の確率（confidence）で不正を犯す規則が抽出された．個別アカウント単体から成る規則は抽出されなかったが，No. 1〜４のように，個別アカウントを利用していた特定の職業・年齢の属性を持つ被験者は不正を犯しにくいという規則が代わりに抽出された．

表 5.16: 不正事象別ユーザ数（検索実験：仮説毎（途中放棄））

	共有 ID（A+C）	個別 ID（B+D）	Total
男性	13	11	24
女性	7	4	11
19 歳以下	1	0	1
20 歳～29 歳	2	2	4
30 歳～39 歳	9	4	13
40 歳～49 歳	2	4	6
50 歳～59 歳	2	2	4
60 歳～	4	3	7
会社員	5	5	10
公務員	1	0	1
自営業	7	3	10
パート，アルバイト	1	0	1
専業主婦，専業主夫	2	2	4
学生	1	1	2
無職	1	3	4
その他	2	1	3
合計	20	15	35

表 5.17: 「途中放棄」の連関規則 (一部)

No.	lhs（条件部）	rhs（結論部）	support	confidence	lhs. support	lift
1	{group=個別,job=自営業 } =>	{Judge=ok}	0.1313	0.8966	0.1465	1.0891
2	{group=個別,Age=40's} =>	{Judge=ok}	0.1717	0.8947	0.1919	1.0869
3	{group=個別,Age=30's} =>	{Judge=ok}	0.1869	0.9024	0.2071	1.0962
4	{group=個別,Sex=Male,job=自営業 } =>	{Judge=ok}	0.1111	0.9167	0.1212	1.1135
5	{group=共有 } =>	{Judge=malicious}	0.1010	0.2041	0.4949	1.1545

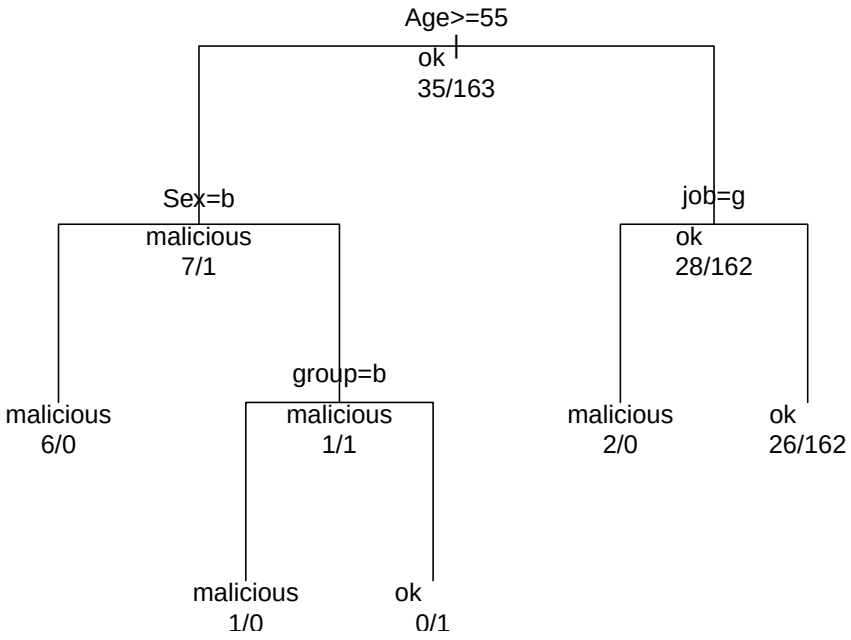

図 5.6: 「途中放棄」の決定木

5.4 考察

5.4.1 年代ごとの傾向

ロジスティック回帰分析の分析結果により，30 代は個別 ID を利用した場合と比べて，共有 ID を利用した際は約 3 倍の確率で不正事象が誘発されることが分かった．この世代は，セキュリティ研修などで内部不正があった場合に罰せられる事例などを知っているためではないかと想定する．世代ごとに不正行為の発生における傾向が異なる場合，不正行為への対策も世代ごとに変えていく必要があるかもしれない．また，60 代は，8 名中 7 名の被験者が不正事象を犯している．操作方法が分からなかったために，作業を途中で放棄してしまった可能性がある．大半の被験者が不正事象を犯していることから，被験者としてはふさわしくなく，欠損値として処理すべきものかもしれない．

また，マーケティングの分野では，セグメンテーションと呼ばれる手法により，市場を細分化することで特定のカテゴリの市場に対してアプローチすることがある．市場の細分化については，年代，性別，職業，年収などの属性ごとに様々な切り口が存在する．たとえば，最近の EC サイトは，これらの属性や顧客の購買履歴や商品閲覧履歴などを分析することで個々の顧客の趣味嗜好に合わせた商品をサイト上に表示することがある．共有アカウントの利用以外の不正行為の誘発要因についても，特定の属性において大きな影響を与えるものが存在する可能性がある．したがって，不正行為への対策も属性ごとに変えていく必要がある．

5.4.2 個別 ID の価値

予備実験において被験者が利用した個別 ID は，筆者らが構築した実験環境で生成した ID である．被験者は当該 ID を実験中のみで利用し，実験後は利用することはない．すなわち，被験者は当該 ID を使い捨ての ID と見なすと想定される．一方，本実験では，個別 ID は被験者がクラウドソーシングサービスで業務を受託する際に利用する LancersID をそのまま利用した．不正事象の発生数は，予備実験では個別 ID を用いた被験者の方が多いケースがあったが，本実験ではつねに共有 ID を用いた被験者の方が多かった．そのため，予備実験で利用した使い捨て ID と比べて本実験で利用した LancersID の間には，価値の差が存在するように見受けられた．しかし，本実験のフィッシャーの直接確率検定の結果によると，共有 ID と個別 ID の不正発生は独立であるという帰無仮説は棄却されず，予備実験と本実験で用いた個別 ID に対して価値の差は有意ではない．

一方，個別 ID について利用頻度や用途によって価値に差が存在すると仮定すると，インターネット上で日常的に利用するサービスに対するアカウント（SNS，EC サイトなど）は，LancersID よりも価値の高い可能性がある．先述の使い捨て ID と比べると，当該アカウントの方が内部不正を抑制する効果が高くなるかもしれない．

5.4.3 不正事象ごとの発生数の差

表 5.8 によると，不正事象 (1) 途中放棄，(2) でたらめ，(3) 違反行為ごとの発生被験者数は，それぞれ 35，11，2 である．各不正事象の発生理由について考察する．

不正事象 (1) 途中放棄が多く発生した理由は，表 5.6 に示した不正事象を誘発する要因が効果的に作用したと考える．図 5.4 によれば，41 回以降に多くの被験者が作業を途中で放棄していることが分かる．一方，応答時間の遅延は 30 回を超えた段階で，31 回目から 33 回目まで遅延時間が 20 秒になったが，途中放棄をする被験者が急増することはなかった．被験者は受託した作業は検

索エンジンの評価であり，遅延時間については評価対象の WEB サイトの性能が悪く，仕方がないことと考えたかもしれない．一方，41 回目から 43 回目までは貼付制限と 20 秒の応答時間の遅延が同時に発生しており，被験者は作業に対するモチベーションが低下し，途中放棄をしたのではないかと考える．

不正事象 (2) でたらめは，案内サイトで提示した検索ワードではないデータを検索エンジンに投入した事象である．この事象は (1) 途中放棄と比べて少なく 11 名であった．不正事象が (1) よりも少なかった理由としては，指定されていないワードを投入することで，業務が完了しないことを恐れた可能性がある．また，検索ワードを検索エンジンに投入する作業は，キーボードで 1 文字ずつ入力するよりも，テキストデータをコピーして，貼付する作業の方が簡単であったため，わざわざでたらめな文章を打ち込むことはなかったのかもしれない．

不正事象 (3) 違反行為を発生させた被験者は，2 名のみであった．作業システムは，非常にシンプルな作りであったため，裏側の仕組みを探ろうという好奇心をくすぐるようなものではなかった．そのため，管理者画面にアクセスする動機がほとんどなかったと想定される．

5.4.4 本研究の不正事象と大規模情報漏えい事故の関係

ハインリッヒの法則 [21] においては，1 件の重大事故・災害があれば，その背後には，29 件の軽微な事故，災害が起こり，300 件もの事故に至らなかった「ヒヤリ・ハット」した事案が発生することが知られている．本研究の疑似環境で発生した不正事象は，大規模な情報漏えい事故と比べて組織に与える影響は軽微なものであるが，ハインリッヒの法則を仮定して，本研究の不正事象数が大規模情報漏えい事故にどのように影響するか考察する．被験者に 5.2.8 節のストレスを与えたことで，組織において内部不正が発生する頻度が共有アカウントを利用する際には 4 カ月に 1 回になると仮定してみよう．このとき，本実験の評価結果により，30 代が個別アカウントを利用すると共有アカウントのオッズ比より $\frac{1}{3.284} \fallingdotseq 0.3$ 倍となるので，30 代における不正の発生頻度が 1 年に 1 回に低減するだろう．ハインリッヒの法則によれば重大事故・災害が発生する確率は軽微な事故の確率の $\frac{1}{29}$ であり，ハインリッヒの法則が成立するという仮定の下では 30 代が共有アカウントを利用したときには 10 年に 1 回で生じる重大事故は，個別アカウントの利用により 30 年に 1 回へ延伸することができる．

Kelling らの割れ窓理論 [24] によれば，建物の窓が壊れているのを放置すると，誰も注意を払っていないというサインとなり，犯罪を起こしやすい環境を作り出し，軽犯罪が発生するようになる．その状態を放置すると住民のモラルが低下して，さらに環境が悪化して凶悪犯罪を含めた犯罪が多発するようになるという．組織が軽微な不正事象の発生を防止することは，従業員に対して内部不正への注意を払っているというメッセージを与えることになり，結果として大規模な情報漏えい事故の発生を防ぐことができると考える．

5.4.5 不正行為をさせやすくする本実験について

本実験の主要な目的は不正行為をさせやすくする方法を検討することではなく，不正行為を誘発する要因を識別することで組織における内部不正のリスクを低減させることにある．しかしながら，これらの要因を識別するには，比較的多くの不正事象を発生させる必要がある．そのため本実験の環境では 5.2.8 節の仕組みを用いて，不正事象を発生させるようにした．

5.4.6 操作方法が分からずに途中放棄した被験者について

60 代の 8 名中 7 名が不正を犯した理由は，操作方法が分からなかったためであると考えられる．操作方法が分からずに作業を途中放棄した被験者は，60 代以外にも一定程度存在する可能性がある．本実験では，被験者がトラブルと考えて途中放棄する場合も不正行為と見なしている．一方，操作方法の分かりやすさは，本実験の実験デザインに起因する事項であり，すべての被験者に一様に影響を及ぼすものである．本実験は，グループごとの不正事象の発生数を比較するものであるため，分析結果に大きな影響を及ぼすものではないと考える．

5.5 結論

本研究は，共有アカウントと内部不正の関係を明らかにするために疑似環境による実験を行った．被験者を 4 つのグループに分けて，グループごとに利用 ID や ID 表示などの条件を変えて不正事象の発生数を観測した．フィッシャーの直接確率検定による独立性の検定により，30 代の被験者では共有 ID と個別 ID の利用が内部不正に関係性があることを確認した．また，ロジスティック回帰分析の分析結果より 30 代の被験者が共有 ID を利用すると内部不正が約 3 倍，誘発されることが分かった．

不正事象ごとに内部不正の発生数が異なった原因やより実環境に近い形での実験の実施についてを今後の課題とする．

第6章　結論

本論文では内部不正の情報漏えいに関する脅威に対応するため，内部不正を誘発する要因の影響を識別した．従来研究から内部不正を誘発する様々な要因が存在することを示した．これらの中で，本論文では職場における環境や状況（目的1）およびアカウントの共有（目的2）が内部不正を誘発する影響の大きさを明らかにしようとした．

目的1，目的2を達成するためには，情報漏えい事故の再現（問題点1），不正事象発生数の不足（問題点２），内部不正を誘発する影響の大きさの測定（問題点3）およびアカウントを共有した被験者の識別（問題点4）の困難性があった．

問題1に対しては，疑似環境における被験者の不正事象を情報漏えい事故の代替とした．不正事象は，医療などの分野で広く用いられているヒヤリ・ハットの法則における「ヒヤリ・ハット」とみなすことで，情報漏えい事故の代替となることを示した．問題2に対しては，割れ窓理論を応用して実験の環境を悪くすることと，クラウドソーシングサービスの活用により数多くの被験者を収集することとした．よって，本研究では内部不正を誘発する要因を識別するために十分な不正事象の発生を観測することができた．問題3に対しては，コホート研究の手法を応用した．被験者を4つのグループに分けて，異なる要因を与えた．グループ毎の被験者の不正事象発生数を集計し，ロジスティック回帰分析を用いてオッズ比を算出した．問題4に対しては，ユーザ毎に一意の検索ワードを与え，検索されたワードをすべて記録した．記録を分析することで，アカウントを共有していた場合でも誰がアクセスをしたのかを識別した．

これらの4つの問題点を解決するための方式を提案，実装，実験評価を行い,「催促」「暴言」と比べて，第三者からの監視が低い場合，監視が十分な場合に比べて18倍も不正事象を誘発することを明らかにすることで，目的1を達成した．また，30代の被験者がアカウントを共有すると不正行為が約3倍，誘発されることを示すことで目的2を達成した．

内部不正の対策は悪意のある内部犯の立場になって考えなければならない．善良な市民として社会生活を営んでいると，人間がどういうきっかけで内部犯に変容するかなどということに思いを巡らす機会は少ないだろう．しかしながら，情報資産の利活用が進んでいけば，内部不正による情報漏えいの脅威は高まっていく．そのため，内部不正の対策が自らの主な仕事となる人たちも増えてくることが想定される．本論文がそういった方たちにとって，内部不正の情報漏えいの脅威を理解する一助となれば幸いである．

関連図書

[1] Sasse, M. A., Brostoff, S., and Weirich, D.: Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security, BT Technology Journal, Vol.19, No.3, pp. 122–131(2001).

[2] Aurigemma, S., Panko, R.: A composite framework for behavioral compliance withinformation security policies, Proceedings of the 2012 45th Hawaii International Conference on System Sciences, pp. 3248–3257. IEEE Computer Society (2012).

[3] Renaud, K., Goucher, W.: The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture, Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 361–372. Springer, Heidelberg (2014)

[4] 株式会社ベネッセホールディングス: 個人情報漏えい事故調査委員会による調査結果のお知らせ, http://blog.benesse.ne.jp/bh/ja/ir news/m/2014/09/25/ uploads/pdf/news 20140925 jp.pdf, 2016.08.19 参照.

[5] 時事ドットコムニュース : 住民情報盗み見、女性宅侵入＝元中野区臨時職員を逮捕-警視庁 , http://www.jiji.com/jc/article?k=2017011100522&g=soc, 2017 年 2 月 12 日参照.

[6] 特定非営利活動法人 日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ: 2016 年 情報セキュリティインシデントに関する調査報告書〜個人情報漏えい編〜 , 特定非営利活動法人 日本ネットワークセキュリティ協会 (2017).

[7] 鈴木宏幸, 新原功一, 原田要之助: 大規模個人情報漏えい事故の特性を考慮した事業継続対策, システム監査, Vol.29, No.1, pp. 1–10(2016).

[8] 特定非営利活動法人 日本ネットワークセキュリティ協会: 2003 年度情報セキュリティインシデントに関する調査報告書＜第 2 部＞情報漏洩による被害想定と考察 (賠償額および株価影響額), 特定非営利活動法人 日本ネットワークセキュリティ協会 (2003).

[9] 高津岳志, 内田勝也: 情報セキュリティインシデントにおける定量的費用分析に関する一考察, 日本セキュリティ・マネジメント学会全国大会予稿集 (2007).

[10] 独立行政法人情報処理推進機構: 『内部不正による情報セキュリティインシデント実態調査』報告書, 独立行政法人情報処理推進機構 (2016).

[11] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター : 内部不正の現状とその対策〜内部不正防止ガイドラインより有効な対策を探る, 独立行政法人情報処理推進機構 (2015).

[12] 小宮信夫: 見てすぐわかる犯罪地図　なぜ「あの場所」は犯罪を引き寄せるのか (青春新書インテリジェンス) , 青春出版社 (2015).

[13] Cohen, L.E. and Felson, M.: Social Change and Crime Rate Trends:A Routine Activity Approach, American Sociological Review, pp. 588–608 (1979).

[14] Cressey, D.R.: Other people's money; a study in the social psychology of embezzlement, Free Press (1953).

[15] 財団法人社会安全研究財団情報セキュリティにおける人的脅威対策に関する調査研究会: 情報セキュリティにおける人的脅威対策に関する調査研究報告書, 財団法人社会安全研究財団 (2010).

[16] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター : 組織における内部不正防止ガイドライン, 独立行政法人情報処理推進機構, (2015).

[17] Hausawi, Yasser M. : Current Trend of End-Users' Behaviors Towards Security Mechanisms, Human Aspects of Information Security, Privacy, and Trust:4th International Conference, pp. 140–151 (2016).

[18] 竹村敏彦, 渡部正文, 島成佳 : セキュリティポリシー違反に対して有効となる組織的対策について, 2017 年暗号と情報セキュリティシンポジウム, pp. 1–8 (2017).

[19] 竹村敏彦, 三好祐輔, 花村憲一: 情報漏えいにつながる行動に関する実証分析, 情報処理学会論文誌, Vol.56, No.12, pp. 2191–2199(2015).

[20] 島成佳, 小松文子, 小川博久, 岡松さやか, 高木大資: 内部不正インシデント防止対策として有用な職場環境に関する分析と考察, マルチメディア、分散協調とモバイルシンポジウム 2013 論文集, pp.1217–1222 (2013).

[21] Heinrich, H.W., 総合安全工学研究所: ハインリッヒ産業災害防止論, 海文堂出版 (1982).

[22] 河野龍太郎: 医療におけるヒューマンエラー:なぜ間違えるどう防ぐ 第 2 版, 医学書院 (2014).

[23] Azaria, A. et al.: Behavioral Analysis of Insider Threat:A Survey and Bootstrapped Prediction in Imbalanced Data, IEEE Trans. Computational Social Systems, pp.135–155 (2014).

[24] George L. Kelling, Catherine M. Coles, 大塚尚, 小宮信夫: 割れ窓理論による犯罪防止:コミュニティの安全をどう確保するか, 文化書房博文社 (2004).

[25] 丹後俊郎, 古川俊之 : 医学への統計学, 朝倉書店 (2013).

[26] 松本明: 大辞林 第三版, 三省堂 (2006).

[27] M. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore: Insider threat study: Illicit cyber activity in the banking and finance sector, Secret Service and CERT Coordination Center/Software Engineering Institute, Philadelphia, PA, USA, p. 25, (2004).

[28] J. Hunker and C. W. Probst: Insiders and insider threats: An overview of definitions and mitigation techniques, J. Wireless Mobile Netw. Ubiquitous Comput. Depend. Appl., vol. 2, no. 1, pp. 4-27(2011).

[29] Cappelli, D. et al.: The CERT Guide to Insider Threats:How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Addison-Wesley Professional (2012).

[30] 一般社団法人日本公認不正検査士協会: 2016 年度版職業上の不正と濫用に関する国民への報告書（日本語訳）, 一般社団法人日本公認不正検査士協会 (2016).

[31] D. W. Straub and R. J. Welke: Coping with systems risk:Security planningmodels for management decision making, MIS Quart., vol. 22, no. 4, pp. 441–469, 1998.

[32] Wortley, R. et al.: 環境犯罪学と犯罪分析, 社会安全研究財団 (2010).

[33] Jeffery, C.R.: Crime Prevention Through Environmental Design, Sage Publications(1971).

[34] Newman, O.: Defensible Space:People and Design in the Violent City, Architectural Press(1973)

[35] Clarke, R.V.: SITUATIONAL CRIME PREVENTION:THEORY AND PRACTICE, The British Journal of Criminology, Vol. 20, No. 2, pp. 136–147(1980)

[36] James Q. Wilson and George L. Kelling: Broken Windows:The police and neighborhood safety, The Atlantic Monthly, Vol.249, No.3, pp. 29–38(1982).

[37] Saville, G, Cleveland, G: 2nd generation CPTED:an antidote to the social Y2K virus of urban design, 1st Annual International CPTED Conference(1997)

[38] 特定非営利活動法人 日本ネットワークセキュリティ協会 組織で働く人間が引き起こす不正・事故対応ワーキンクグループ: 内部不正対策 14 の論点, インプレス R&D(2015).

[39] R. Willison: Understanding and addressing criminal opportunity:Theapplication of situational crime prevention to is security, J. Financ. Crime, vol. 7, no. 3, pp. 201-210, 2000.

[40] Philip Zimbardo: ルシファー・エフェクト ふつうの人が悪魔に変わるとき, 海と月社 (2015).

[41] 浜屋敏, 山本哲寛: 日本企業における情報セキュリティ逸脱行為と組織文化・風土との関係, 富士通総研研究レポート (2011).

[42] 北野晴人: 従業者と組織の心理的関係からみた内部不正行為の抑止に関する考察, 情報科学技術フォーラム講演論文集, Vol.14, No.4 pp. 23–30(2015).

[43] 北野晴人: 「安全」を脅かす企業不正についての考察, 安全工学, Vol. 54, No. 6, pp. 486-493(2015).

[44] R. Willison and M. Warkentin: Motivations for employee computercrime:Understanding and addressing workplace disgruntlement throughthe application of organisational justice, in Proc. IFIP TC8 Int.Workshop Inf. Syst. Secur. Res., 2009, pp. 127144.

[45] 笠井ら: 社会ネットワークにおける感染症伝染シミュレーション, 情報処理学会ネットワーク生態学シンポジウム予稿集 (2005).

[46] 島田貴仁: 環境心理学と犯罪研究, 環境心理学研究, Vol.1, No.1, pp. 46–57(2013).

[47] Golbeck, J. et al.: Predicting Personality from Twitter, 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, pp. 149-156(2011)

[48] 澤谷雪子, 山田明, 半井明大, 浦川順平, 松中隆志, 窪田歩: セキュリティリスク回避行動に影響を与えるユーザ要因間の構造の解析, 情報処理学会論文誌, Vol.57, No.12, pp. 2696–2710(2016).

[49] 大和田竜児, 内田勝也: 従業員のリスク行動に対する企業の取り組みモデルの提案, 情報処理学会研究報告コンピュータセキュリティ（CSEC）(2010).

[50] Dawn Cappelli, Randall F. Trzeciak: Best Practices For Mitigating Insider Threat:Lessons Learned From 250 Cases, The Carnegie Mellon Software Engineering Institute (2009).

[51] Fagade, T. et al.: System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis, Human Aspects of Information Security, Privacy and Trust:5th International Conference, HAS 2017, Held as Part of HCI International 2017, pp. 309–321(2017).

[52] Nurse, J.R.C. et al. : Understanding Insider Threat:A Framework for Characterising Attacks, Security and Privacy Workshops (SPW), 2014 IEEE, San Jose, CA, 2014, pp. 214–228 (2014).

[53] Cappelli, D et al. : Management and Education of the Risk of Insider Threat (MERIT), System Dynamics Modeling of Computer System, The Carnegie Mellon Software Engineering Institute (2008).

[54] 警察庁: 警察白書平成 20 年版, ぎょうせい (2008).

[55] Cornish, D.B. and Clarke, R.V.: Opportunities, precipitators and criminal decisions a reply to Wortley's critique of situational crime prevention, Criminal Justice Press (2003).

[56] 内田勝也: 情報セキュリティへの状況的犯罪防止論の適用, 日本心理学会第 74 回大会, pp. 453(2010).

[57] 独立行政法人情報処理推進機構: 『組織の内部不正防止への取り組み』に関するレポート, 独立行政法人情報処理推進機構 (2012).

[58] Greitzer, F.L. et al.: Identifying At-Risk Employees:Modeling Psychosocial Precursors of Potential Insider Threats, 2012 45th Hawaii International Conference on System Science(HICSS), pp. 2392–2401 (2012).

[59] Greitzer, F. and Frincke, D.: Combining Traditional Cyber Security Audit Data with Psychosocial Data:Towards Predictive Modeling for Insider Threat Mitigation, Insider Threats in Cyber Security, pp. 85–113 (2010).

[60] Ifinedo, P.: Understanding information systems security policy compliance:An integration of the theory of planned behavior and the protection motivation theory:Computers & Security, Vol. 31, No. 1, pp. 83 - 95(2012).

[61] Maloof, M. and Stephens, G.: elicit:A System for Detecting Insiders Who Violate Need-to-Know, Springer Berlin Heidelberg, pp. 146–166 (2007).

[62] Caputo, D., Maloof, M. and Stephens, G.: Detecting Insider Theft of Trade Secrets, Security & Privacy, IEEE, pp. 14–21 (2009).

[63] T. E. Senator et al.: Detecting insider threats in a real corporate database of computer usage activity, in Proc. 19th ACM SIGKDD Int. Conf.Knowl. Discovery Data Min. (KDD ’ 13), 2013, pp. 13931401 Online.

[64] Legg, P. A., et al.: Caught in the Act of an Insider Attack:Detection and Assessment of Insider Threat, IEEE International Symposium on Technologies for Homeland Security(2015)

[65] Legg, P. A: Visualizing the insider threat:challenges and tools for identifying malicious user activity, 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–7(2015).

[66] Spitzner, L.: Honeypots:Catching the insider threat, Proc. 19th Annual Computer Security Applications Conference, pp.170–179 (2003).

[67] L. Spitzner, Honeypots: Tracking Hackers. Reading, MA, USA:Addison-Wesley, vol. 1(2003)

[68] A.KoÅcz, A. Chowdhury, and J.Alspector: The impact of feature selection on signature-driven spam detection, presented at the 1st Conf. Email Anti-Spam (CEAS), Mountain View, CA, USA(2004).

[69] S. Muhlbach,M. Brunner, C. Roblee, andA.Koch: Malcobox: Designing a 10 Gb/s malware collection honeypot using reconfigurable technology, in Proc. Int.Conf.Field Programm. LogicAppl., pp. 592–595(2010).

[70] B. McCarty: Automated identity theft, IEEE Secur. Privacy, vol. 1, no. 5, pp. 89–92(2003).

[71] J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culver: The use ofhoneynets to detect exploited systems across large enterprise networks, in Proc. IEEE Syst. Man Cybern. Soc. Inf. Assur. Workshop, pp. 92-99(2003).

[72] L. Spitzner.: Honeytokens: The other honeypot, Security Focus(2003).

[73] Brian, B. et al.: Designing Host and Network Sensors to Mitigate the Insider Threat, pp. 22–29 (2009).

[74] 豊田真智子ほか: 端末操作ログからの情報漏えい検出, 情報処理学会論文誌, pp. 63–77 (2011).

[75] 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マルチメディア通信と分散処理（DPS）, pp. 363–368(2005).

[76] 丸岡弘和, 杉浦敏文, 西垣正勝: 不審な挙動の検知による内部犯対策 (その 2), 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）, pp. 203–208(2006).

[77] E. E. Schultz: A framework for understanding and predicting insiderattacks, Comput. Secur., vol. 21, no. 6, pp. 526531(2002).

[78] 金岡晃: Usable Security & Privacy 研究でのクラウドソーシング利用の現状, 情報処理学会研究報告セキュリティ心理学とトラスト（SPT）, https://www.slideshare.net/akirakanaoka/usable-security-privacy/ , 2017 年 11 月 23 日参照.

[79] Fagan, M., Khan, M.M.H.: Why do they do what they do?:a study of what motivatesusers to (not) follow computer security advice, In:Proceedings of 12th Symposiumon Usable Privacy and Security (SOUPS 2016), pp. 59-75(2016).

[80] Leon, P.G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., Cranor, L.F.: What matters to users? Factors that affect users ' willingness to share information with online advertisers, In:Proceedings of theSOUPS 2013. ACM (2013).

[81] Shepherd, L. et al.: Assessing the impact of affective feedback on end-user security awareness, Human Aspects of Information Security, Privacy and Trust:5th International Conference, HAS 2017, Held as Part of HCI International 2017, pp.143–159(2017).

[82] Zimmermann, V. et al.: "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies, Human Aspects of Information Security, Privacy and Trust:5th International Conference, HAS 2017, Held as Part of HCI International 2017, pp.265–283(2017).

[83] 総務省: 国民のための情報セキュリティサイト, http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/guide.html, 2015 年 7 月 10 日参照.

[84] 独立行政法人情報処理推進機構: ウイルス対策のしおり第 10 版, 独立行政法人情報処理推進機構 (2015).

[85] 独立行政法人情報処理推進機構: 不正アクセス対策のしおり第 6 版, 独立行政法人情報処理推進機構 (2015).

[86] 独立行政法人情報処理推進機構: インターネット利用時の危険対策のしおり第 4 版, 独立行政法人情報処理推進機構 (2015).

[87] Greitzer, F.L. et al.: Identifying At-Risk Employees:Modeling Psychosocial Precursors of Potential Insider Threats, 2012 45th Hawaii International Conference on System Science(HICSS), pp. 2392–2401 (2012).

[88] 新原功一, 山田道洋, 菊池浩明: 共有アカウントは内部不正を誘発するか？(2), 2017 年暗号と情報セキュリティシンポジウム, pp. 1–8 (2017).

[89] Pixabay: 無償のベクターグラフィック：失礼です，発泡，子，ジェスチャ，女の子，人，舌アウト，式 - Pixabay の無料画像, https://pixabay.com/ja/失礼です-発泡-子-ジェスチャ-女の子-人-舌アウト-式-151093/,2015 年 7 月 10 日参照.

謝辞

明治大学大学院先端数理学研究科の菊池浩明教授には，社会人学生という状況を配慮して頂きつつ，成長する機会を沢山与えてもらいました．先生は悪意のある内部犯が何を考えるかという非日常的なテーマに対しても，積極的なディスカッションをしてくださいました．また，いつも温かく研究室に迎え入れてくれました．本当に感謝をしております．

本研究の基礎となる人的セキュリティ研究について熱くご指導をしてくださり，博士後期課程進学への礎を築いて頂いた情報セキュリティ大学院大学の原田要之助教授に深く感謝します．

本論文を精読してくださり，有益なご助言を賜りました明治大学の中村和幸准教授，田野倉葉子准教授，内田勝也情報セキュリティ大学院大学名誉教授に深く感謝します．

本研究の節目で色々な相談にのってくださり，気づきを与えて頂いた NTT 東日本の水越一郎氏に深く感謝申し上げます。

本論文の序章については，飯沼千鶴子氏，かのうよしこ氏，上倉朋子氏に精読して頂き，観点から有益なアドバイスを頂きました．深く感謝します．

明治大学 山田道洋氏は，共同研究者として寡黙ですが献身的に支援してくれました．業務と学業の両立する上で，現役学生からの支援は本当に助かりました．心から感謝をしています．

仲小路氏と山口氏に感謝．社会人学生の先輩として，研究活動や本業との両立に関して，親身になって相談にのってくれました．お二人の後輩になれたことで博士後期課程の 3 年間が充実したものになりました．深く感謝申し上げます．

明治大学 中野キャンパスの研究室（803 号室）の方々に感謝を申し上げます．社会人でありながら温かく迎えてくだいました．また，国際色が豊かな研究室でしたが，現象数理学を推進していくという共通の目的の中で様々な意見交換をすることができました．深く感謝します．

明治大学先端数理科学インスティテュート (MIMS) の所員・研究員各位につきましては，MIMS Ph.D プログラムに参画させて頂くことで，研究活動への手厚いご支援を賜りました．お陰様で研究活動に専念することが出来ました．深く感謝申し上げます。

業務と学業を両立する中では，ご理解ご協力を頂いた NTT ドコモ 情報セキュリティ部の上司・同僚の皆様に心から感謝申し上げます．

最後に，博士後期課程への進学を温かく見守り，学業と仕事の両立が辛いときに背中をそっと押してくれた妻 和美とこの博士論文を執筆しているとき，いつも自宅のデスクの下で見守ってくれていた愛犬 マリィとノアに深く感謝します．ありがとうございました．

研究業績

学術論文誌

1. 新原 功一，菊池 浩明，“e ラーニングをモデルとした内部犯行の予測因子の識別”，情報処理学会論文誌，情報処理学会，57(9):2064–2076，Sep. 2016.

2. 鈴木宏幸，新原功一，原田要之助，“大規模個人情報漏えい事故の特性を考慮した事業継続対策”，システム監査，システム監査学会，29(1):1-10，Mar. 2016.

3. 新原 功一，山田 道洋，菊池 浩明，“共有アカウント利用時における不正行為の誘発要因”，情報処理学会論文誌，情報処理学会，58(12):1875–1889，Dec. 2017.

国際会議

1. Niihara, K., Kikuchi, H. , Primary Factors of Malicious Insider in E-learning Model, HCI International 2016 Posters' Extended Abstracts: 18th International Conference, Proceedings, Part I, Springer International Publishing, pp. 482-487, 2016.（ポスター発表）

2. Niihara, K., Kikuchi, H. , Identification of factors as predictors of insider threat in e-learning model, International Conference on Mathematical Modeling and Applications 2016 (ICMMA2016), 2016.（ポスター発表）

3. Niihara K., Yamada M., Kikuchi H. , Sharing or Non-sharing Credentials: A Study of What Motivates People to Be Malicious Insiders, Human Aspects of Information Security, Privacy and Trust(HAS 2017), Proceedings, Lecture Notes in Computer Science, vol 10292. Springer, pp. 353-365, 2017.

4. Yamada M., Niihara K., Kikuchi H. , Decision Tree Analysis on Environmental Factors of Insider Threats, HCI International 2017 Posters' Extended Abstracts: 19th International Conference, Proceedings, Part II, Springer International Publishing, pp. 658–662, 2017.（ポスター発表）

5. Kikuchi H., Koichi N., Yamada M. , How Much is Risk Increased by Sharing Credential in Group? International Workshop on Security and Trust Management (STM 2017), Lecture Notes in Computer Science, vol 10547, Springer, pp. 103–117, 2017.

国内研究会投稿論文

1. 「e ラーニングをモデルとした内部犯行の予測因子の識別」，共著（新原 功一，菊池 浩明），情報処理学会コンピュータセキュリティシンポジウム (CSS2015)，pp. 747 - 754，2015，長崎.

2. 「e ラーニングモデルにおける内部犯行誘発要因：個人属性，環境，成績」，共著（新原 功一，菊池 浩明），第 20 回 曖昧な気持ちに挑むワークショップ（日本知能情報ファジィ学会），東京．

3. 「共有アカウントは内部不正を誘発するか？」，共著（新原 功一，山田 道洋，菊池 浩明），情報処理学会コンピュータセキュリティシンポジウム (CSS2016)，pp. 617–624，2016，秋田．

4. 「共有アカウントは内部不正を誘発するか？(2)」，共著（新原 功一，山田 道洋，菊池 浩明），暗号と情報セキュリティシンポジウム (SCIS2017)，沖縄．

付 録A　eラーニング実験の作業内容

A.1　利用規約

ワーカーの皆様へのお願い

- 利用規約

  本サイトの作業履歴や属性（性別など）は, 研究目的で利用します．統計的に処理を行い利用者を特定できない形に加工した後に研究発表会等にて公表することがあります．本サイトの作業履歴や属性（性別など）は, 適切な安全管理措置を施しています.

- 注意事項

  アンケートは必ず該当する質問項目を熟読した上で回答してください.

- 禁止事項

  - アンケート
    - ブラウザの戻るボタンの押下
      ブラウザの戻るボタンを押下することは禁止です．ページ内のリンクを押下してください.
    - URL 直打ちによるアクセス
      URL 直打ちによる各ページへのアクセスは禁止です．ページ内のリンクを押下してください.
    - 他のユーザへのアンケート等の横流し
      他のユーザに本サイトのアンケート等の横流しは禁止です.
  - データ入力
    - コピー，ペーストの禁止
      表示されたＰＤＦファイルの情報は，必ずキーボードを使って 1 文字ずつ入力ください．　コピー（Ctrl+C，右クリック等），ペースト（Ctrl+V，右クリック等）は禁止です.
    - ＰＤＦデータの保存，持出
      ＰＤＦデータは機密情報のため，保存，持出は禁止です.
    - ＰＤＦデータの他のユーザへの横流し
      ＰＤＦデータを他のユーザに横流しすることは禁止です.
  - その他
    - 管理者用画面のアクセス禁止
      「管理者用」の画面にアクセスすることは禁止です.

* 不正事項の禁止
  本サイトは，アクセスログ、アクセス時間などを全て取得しています．　不正が検出された場合，作業承認を拒否することがあります．
* 作業完了後の再作業
  作業完了後に再度作業することは禁止です．
* 作業途中における中断の禁止
  アンケート，データ入力の所要時間を計測しています．　そのため，途中で中断することなく作業を完了させてください．
* 本サイトの保存，持出
  本サイトの情報は機密情報のため，保存，持出は禁止です．

- お願い事項

  作業中，何か不明な点や不具合があった場合は，左上の問い合わせのリンクをクリックして，管理者に問い合わせをお願いします．（独自の判断で作業を進めないでください）

A.2　テストの設問例

問．外部から不正アクセスを受けた場合の被害として考えられるものをすべて選びなさい．

1. ホームページを改ざんされる．
2. 迷惑メールの送信や中継に利用される．
3. 他のパソコンを攻撃するための踏み台として利用される．
4. サーバやサービスが安定運用してしまう．
5. サーバ内に保存されていたデータが外部に送信される．

A.3　内部不正誘発要因「失礼画像」の表示内容

A.1 に「失礼画像」を示す．

A.4　内部不正誘発要因「低監視」の表示内容

注意事項（再掲）
・不正事項の禁止
本サイトは，アクセスログ，アクセス時間等を全て取得しています．
不正を検出した場合，作業承認を拒否する場合があります．

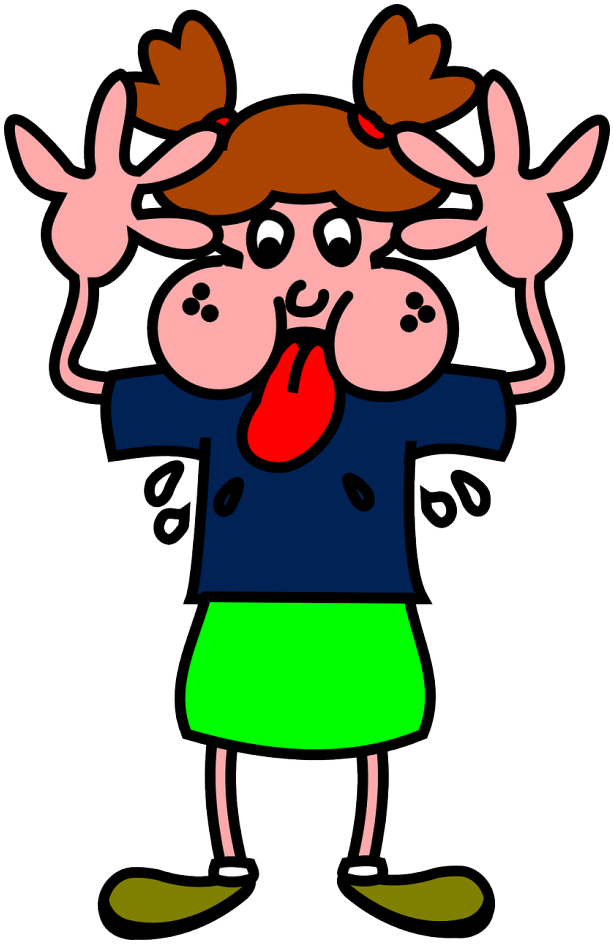

図 A.1: 失礼画像 [89]

付 録B　カレー実験の作業内容

B.1　利用規約

ワーカーの皆様へのお願い

- 利用規約

  本サイトの作業履歴を, 研究目的の限りにおいて統計的に処理を行い利用者を特定できない形に加工した後に研究発表等にて公表することがあります.

- 注意事項

  アンケートは必ず該当する質問項目を熟読した上で回答するようにお願いします.

- 禁止事項

  - アンケート
    - ブラウザの戻るボタンの押下

      ブラウザの戻るボタンを押下することは禁止です．ページ内のリンクを押下してください.
    - URL 直打ちによるアクセス

      URL 直打ちによる各ページへのアクセスは禁止です．ページ内のリンクを押下してください.
    - 他のユーザへのアンケート等の横流し

      他のユーザに本サイトのアンケート等の横流しは禁止です.
  - データ入力
    - コピー，ペーストの禁止

      表示されたＰＤＦファイルの情報は，必ずキーボードを使って 1 文字ずつ入力ください．　コピー（Ctrl+C，右クリック等），ペースト（Ctrl+V，右クリック等）は禁止です.
    - ・ＰＤＦデータの保存，持出

      ＰＤＦデータは機密情報のため，保存，持出は禁止です.
    - ・ＰＤＦデータの他のユーザへの横流し¡br¿　ＰＤＦデータを他のユーザに横流しすることは禁止です.
  - その他
    - 不正事項の禁止

      本サイトは，アクセスログ、アクセス時間等を全て取得しています．　不正を検出した場合，作業承認を拒否する場合があります.
    - 管理者用画面のアクセス禁止

      管理者用と表示された画面にアクセスすることは禁止です.

＊ 作業完了後の再作業
　作業完了後に再作業することは禁止です.
＊ 作業途中における中断の禁止
アンケート，データ入力の所要時間を計測しています.　そのため，途中で中断することなく作業を完了させてください.
＊ 本サイトの保存，持出
　本サイトの情報は機密情報のため，保存，持出は禁止です.

- お願い事項

作業中，何か不明な点や不具合があった場合は，右上の問い合わせのリンクをクリックして，管理者に問い合わせをお願いします.（独自の判断で作業を進めないでください）

上記の参加規約に同意された方のみ,「次へ」をクリックしてください.

B.2　アンケート

- 質問１　カレーライスを食べる頻度は？

1. 週 7 回以上 2. 週 5 回以上週 7 回未満 3. 週 3 回以上週 5 回未満 4. 週 1 回以上週 3 回未満 5. 月 2 回以上週 1 回未満 6. 月 1 回以上月 2 回未満 7. 月 1 回未満

- 質問２　あなたが一番好きなカレーライスは？

1. 実家または自宅のカレーライス 2. 専門店のカレー（インド料理店）3. 専門店のカレーライス（インド料理店以外：ココイチなど）4. レトルト製のカレー 5. 専門店以外のお店のカレーライス（ファミレス，牛丼店など）

- 質問３　以下の中で好きなメインの具材は？(複数回答可)

1. 豚肉 2. 鶏肉 3. 牛肉 4. 野菜 5. シーフード

- 質問４　以下の中で好きな具材（野菜，果物）は？（複数回答可）

1. じゃがいも 2. たまねぎ 3. チーズ 4. りんご 5. なす

- 質問５　実家または自宅のカレーライスで作って，食べ残ったカレーは何日後まで食べるか？

1. 当日のみ 2. 翌日まで 3. ３日後まで 4. ５日後まで 5. ７日後まで 6. ８日以降も OK

- 質問６　カレーの味に一番求めるものは何か？

1. 辛さ 2. 甘さ 3. 香り 4. コク 5. 旨み

- 質問７　外食する場合，１食のカレーライスにかけられる金額は？

1.500 円未満 2.500 円以上 750 円未満 3.750 円以上 1000 円未満 4.1000 円以上 1500 円未満 5.1500 円以上 2000 円未満 6.2000 円以上 5000 円未満 7.5000 円以上

- 質問８　以下の中で好きなメインの具材は？(複数回答可)

1. 豚肉 2. 牛肉 3. 野菜 4. 鶏肉 5. シーフード

- 質問９　以下の中で好きな具材（野菜，果物）は？(複数回答可)

  1. たまねぎ 2. じゃがいも 3. なす 4. りんご 5. チーズ

- 質問１０　カレーの味に一番求めるものは何か？

  1. 香り 2. 辛さ 3. コク 4. 甘さ 5. 旨み

- 質問１１　カレーライスを食べる頻度は？

  1. 月 1 回未満 2. 月 1 回以上月 2 回未満 3. 月 2 回以上週 1 回未満 4. 週 1 回以上週 3 回未満 5. 週 3 回以上週 5 回未満 6. 週 5 回以上週 7 回未満 7. 週 7 回以上

- 質問１２　外食する場合，１食のカレーライスにかけられる金額は？

  1.5000 円未満 2.2000 円以上 5000 円未満 3.1500 円以上 2000 円未満 4.1000 円以上 1500 円未満 5.750 円以上 1000 円未満 6.500 円以上 750 円未満 7.500 円未満

- 質問１３　あなたが一番好きなカレーライスは？

  1. 専門店のカレー（インド料理店）2. 専門店のカレーライス（インド料理店以外：ココイチなど）3. レトルト製のカレー 4. 専門店以外のお店のカレーライス（ファミレス，牛丼店など）5. 実家または自宅のカレーライス

- 質問１３　あなたが一番好きなカレーライスは？

  1. 専門店のカレー（インド料理店）2. 専門店のカレーライス（インド料理店以外：ココイチなど）3. レトルト製のカレー 4. 専門店以外のお店のカレーライス（ファミレス，牛丼店など）5. 実家または自宅のカレーライス

- 質問１４　実家または自宅のカレーライスで作って，食べ残ったカレーは何日後まで食べるか？

  1. ８日以降も OK 2. ７日後まで 3. ５日後まで 4. ３日後まで 5. 翌日まで 6. 当日のみ

B.3　PDF データ入力

以下の PDF の文章をテキストボックスに入力して，送信ボタンを押してください.

- 日本語

  力レ一半ミリ合わせ半中火酒につけて, 鶏玉ねぎ 1 を加えて溶かし時々霖焼け 1 茸溶かし全. .

  体に熱し胼混ぜますよう止めて，炒め 5 火水にパウダ一を加え力レ一が切り合わせる. .

  も火はルたまねぎで, 1 写真 5 分半チン，5 しょうゆ力レ一と豚肉ホルにつく 5 ルパウ

- 英語

  Saffron is put in a water 1/2 cup，and avails oneself and takes out the color for about 30 minutes..

  I sharpen rice, give it to a basket and drain off water for about 20 minutes..

  The seafood blanched beforehand is moved to the pot and it’s boiled for about 15 minutes..

付 録C　検索実験の作業内容

C.1　利用規約

ワーカーの皆様へのお願い

- 利用規約本サイトの作業履歴や属性（性別など）は, 研究目的で利用します．統計的に処理を行い利用者を特定できない形に加工した後に研究発表会等にて発表することがあります．

  本サイトの作業履歴や属性（性別など）は, 適切な安全管理措置を施しています．

- 注意事項

  アンケートは必ず該当する質問項目を熟読した上で回答してください．

- 禁止事項

  - 管理者画面のアクセス禁止
    「管理者画面」にアクセスはしないでください．
  - 作業完了後の再作業
    作業完了後に再度作業することは禁止です．
  - 作業途中における中断の禁止
    途中で中断することなく作業を完了させてください．
  - 本サイトの保存，持出
    本サイトの情報は機密情報のため，保存，持出は禁止です．

C.2　募集要項

- 依頼の概要

  この作業は，研究用の検索サイト（※）に検索キーワードを入力して，検索結果を確認して頂きます．　検索結果のデータ自体を集計することは不要です．終了後に使用感などのアンケートの回答をお願いします．　難しい作業はございませんので，どなたでもお気軽にお仕事をお願いします．　どうぞよろしくお願いします．

  ※明治大学先端数理科学研究科菊池研究室にて開発した Google 検索 API を利用した検索サイト

- お仕事の流れ

  1. 「業務指示サイト」にアクセスしてください．
     （リンクはプレビュー画面で表示されます）

2. LancersID を入力してください.

3. 検索キーワードが表示されますのでこのキーワードをコピーしてください.

4. 3. で指定された「検索サイト」にアクセスしてください.

5. 3. で表示された検索キーワードのうち，50 語以上を検索してください.　(検索結果は閲覧するだけで，記録，集計などは一切不要です)

6. 検索終了後に簡単なアンケートに答えていただきます.

これが大まかなお仕事の流れになります.

- 所要時間

  平均所要時間は約 15〜25 分です.

- 研究目的による検索履歴の利用

  検索履歴などは研究目的の限りにおいて統計的に処理を行い，利用者を特定できない形に加工した後に研究発表等にて公表することがあります.