情報処理学会論文誌 Vol.58 No.12 1875–1889 (Dec. 2017)

共有アカウント利用時における不正行為の誘発要因

新原 功一[1,a)] 山田 道洋[1] 菊池 浩明[1,b)]

受付日 2017年3月12日, 採録日 2017年9月5日

概要：昨今，組織に深刻な影響を与える内部不正への対策は非常に大きな課題である．人的な要因は情報セキュリティにおける一番弱い鎖といわれている．内部不正は様々な要因によって引き起こされるが，最近の研究によると，特にシステムにログインするためのアカウントの共有が最も大きな負の振舞いといわれている．しかし，アカウントを共有することで内部不正のリスクがどれくらい増加するかは，今まで明らかになっていなかった．そこで本研究は，内部不正を誘発する際の最大の要因であるアカウントを共有することに注目する．被験者が不正事象を実行しようとする振舞いを観測するため，我々はランサーズ社のクラウドソーシングサービスにより集めた 198 名の被験者による実験を行った．アカウントを共有するグループと非共有グループについて，不正事象を計測した．不正事象を分析した結果，30 代の被験者はアカウントを共有すると個別アカウントを使う場合と比べて，不正行為が発生するリスクが高まることが分かった．

キーワード：内部不正，不正行為，共有アカウント，情報漏えい

Hypothesized Causes of Malicious Activities when Credential is Shared in Group

Koichi Niihara[1,a)] Michihiro Yamada[1] Hiroaki Kikuchi[1,b)]

Received: March 12, 2017, Accepted: September 5, 2017

Abstract: One of the biggest challenges faced by organizations is system misuse by insiders, whose actions could give a serious impact to the organization. It has been told that the weakest link in information security is the human element. Various hypothesized causes of insider threat exist. According to recent study, the most negative behavior is sharing credentials. However, it is not clear how much risk of the insider threat is increased by sharing credentials. In this paper, we focus on the most significant factor: *sharing credential*. We conduct an experiment involving 198 subjects on crowd-sourcing service, Lancers, Inc., in order to examine the behaviors that real human subjects follow when attempting to perform malicious activities. The numbers of malicious activities for some groups with/without sharing credentials are observed. To clarify the effects, we performed logistic regression analyses. Our statistical analysis shows that the risk of malicious activities for subjects who share credentials is 3 times greater than that for subjects with individual credentials.

Keywords: insider threat, malicious activities, sharing credentials, information breach

1. はじめに

2014 年に大手教育会社の業務委託先従業員が内部の情報を取得した大規模情報漏えい事案が大きな社会問題となった [3]．2017 年 1 月には，東京都中野区の元臨時職員が個人情報を盗み見たとして，同区個人情報保護条例違反の疑いで逮捕された [4]．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 [5], [6]．内部の人間が悪意を持つと，正当な権限を用いて情報を取得することができ

[1] 明治大学大学院先端数理科学研究科
Graduate School of Advanced Mathematical Sciences, Meiji University, Nakano, Tokyo 164–8525, Japan
[a)] niihara@meiji.ac.jp
[b)] kikn@meiji.ac.jp

本論文は「コンピュータセキュリティシンポジウム 2016」[1] と「2017 年暗号と情報セキュリティシンポジウム」[2] での発表を基にまとめたものである．

表 1 予備実験と本実験の比較（概要）
Table 1 Comparison between preliminary experiment and this experiment (Overview).

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
口頭発表	コンピュータセキュリティシンポジウム 2016 [1]	2017 年暗号と情報セキュリティシンポジウム [2]

るため，組織は適切な対策を継続的に行う必要がある．

我々は内部不正を誘発する要因を識別するため，疑似環境で被験者に軽微なタスクを与え，実際の行動を分析する実験を行った [7], [8]．想定した要因のうち，催促や管理者による暴言と比べて従業員に対する監視が緩い環境のほうが内部不正が発生しやすいことを明らかにした．しかしながら，どのような監視手法がより内部不正を抑制することができるかについては課題となっていた．

内部不正を防ぐための管理策は労働環境や待遇の改善，従業員に対する教育など様々なものが存在する [9]．なかでも，システムにログインするためのアカウントを利用者が共有すると内部不正が生じやすくなるといわれている [10]．Hausawi がセキュリティ専門家に対して行ったインタビューによると，エンドユーザが行うセキュリティにおける最も悪質な行動は認証情報の共有（Sharing credential）であった [11]．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際に 1 つの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．しかし，個別アカウントの管理は利用者の退職時の迅速な削除や定期的な棚卸しなどの対応を確実に運用する必要があり，組織にとって負荷が高い．個別アカウントの利用はインシデント発生時などに対する事象の記録としては重要であるが，どこまで内部不正を防ぐ効果があるのかは明らかにされていない．

そこで，本研究は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明らかにすることを目的とする．内部不正の発生に抑制効果が高い手法を識別できれば，組織は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させることができる．

しかしながら，実在する組織などの従業員を対象にして内部不正を観測するのは，当該組織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，長期間にわたってその過程を詳細に観察することは困難である．

この問題に対して，我々は疑似環境において，被験者が行った作業で生じる不正事象の発生数を観測する実験（以下，予備実験とする）を行った [1]．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**表 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，不正行為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った．また，ロジスティック回帰分析を行い，不正行為を誘発する主な要因を分析した．

本論文の構成は次のとおりである．2 章では，関連研究の調査について述べる．3 章では実験の評価方式，4 章で実験結果，評価を記す．5 章で考察を与え，最後に 6 章でまとめる．

2. 関連研究

本章は，内部不正の定義，予防的対策，共有アカウントの利用と不正との関係などにおける関連研究を述べる．

2.1 内部不正の定義と本研究の対象範囲

Cappli らは，内部不正を 3 つに分類した [9]．Insider IT Sabotage（情報破壊・システム破壊）は，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．Insider theft of intellectual property（知的財産窃盗）は，従業員が新しい

*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

会社への転職など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．Insider fraud（内部詐欺）は，ヘルプデスクやカスタマーサービスなどの従業員が主に金銭目的で不正を行うものである．

文献 [3] の大手教育会社の事案は，会社への復讐や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ったため，「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ともない「内部詐欺」の脅威への対策が急務になっていることから，本研究における内部不正の対象範囲は「内部詐欺」とする．

従業員らの内部不正に対して，組織が実施できる対策は 3 種類に分類できる [9]．1 つ目は Prevent（予防）である．これは環境を変えたり，職場，待遇をかえたりすることで内部不正の発生を防止する対策である．次は，Detect（検知）である．悪意のある内部犯を Honeypots でおびき寄せる Spitzner の研究 [12] や内部犯が利用する PC やシステムの操作履歴を疑似的に再現して不正を検知する Azaria らの研究 [13] などがある．また，Legg らによる個人ごと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 [14] も該当する．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．さらに 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 [15]．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．また，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 [16], [17]．これらの挙動は心理的状態に起因することから，内部不正者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．最後が，Respond（事後対応）である．情報自体を暗号化することで被害を極小化したり，適切なインシデントレスポンスを実施したりすることが該当する．

検知や事後対応に関する研究は内部不正の発生状況を把握するためには有用であるが，これらの段階ではすでに情報漏えいの被害が発生している可能性がある．そこで，本研究は内部不正の発生を予防することに焦点を当てる．

2.2 内部不正の予防

環境犯罪学では，犯罪者自身は犯罪事象の 1 つの要因にすぎず，犯罪行動はその行動が直面する環境の性質に著しく影響を受ける [18]．本研究はこの環境を内部不正の誘発要因としてとらえ，誘発要因を抑制することで内部不正の発生を予防する方策を明らかにする．

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，監視性の緩い場所の 3 つの要因が重なった場合に内部不正が生じることを主張している [19]．Cressey は，動機・プレッシャをかかえ，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」，「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ている [20]．これらの研究では，複合的な要因の重なりが内部不正を誘発する要因としている．内部不正の発生を抑制するには，いくつかの誘発要因を低減，消失させる必要がある．しかし，本質的にどの要因が内部不正の抑制に効果的であるかどうかは不明瞭な部分が多い．

社会安全研究財団は，国内で 2007 年から 2009 年 6 月に検挙したサイバー犯罪 [21] のうち，内部不正を対象として事例分析を行った [22]．当該分析では犯行者の心理的な力動過程（ダイナミクス）を提示した．そこでは，内部不正の要因が分析されているが，内部不正の発生に関する本質的な要因は定かではなかった．Greitzer らは心理学とベイジアンネットによる分析から内部不正に起因する 12 の予測因子を提唱している [23], [24]．Cornish らは，都市空間における犯罪予防の理論として，直接的，間接的に犯罪を防止，抑止する対策を状況的犯罪予防と名付け 25 種類の対策を提唱している [25]．IPA はセキュリティ対策に特化した状況的犯罪予防の対策を提案している [10]．Greitzer ら，Cornish ら，IPA 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．

いくつかの研究では，実際の犯罪記録をもとにして内部不正の誘発要因の特徴を類推し，傾向をモデル化している．Capplli らは，MERIT [*2] を提案している [26]．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 [27]．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良いが，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．

島らが内部不正の経験がある人とない人を比較したアンケート調査によると，組織の内部不正者による不正行為が発生しない対策は，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 [28]．竹村らはセキュリティポリシ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た [29]．その結果，不正・違反放置の風土がセキュリティポリシの違反を犯す 1 つの要因であった．不正・違反放置の風土とは，星野らによれば，日常的に基本的なルールが破られた

[*2] Management and Education of the Risk of Insider Threat

表 2 内部不正の誘発要因に関する研究の比較
Table 2 Comparison of studies for hypothesized causes of insider threat.

	調査方法	想定する内部不正の誘発要因
島ら [28]	アンケート調査	職場環境
竹村ら [29]		個人属性や職場環境要因
IPA [31]		内部不正に関する対策の実施状況
筆者ら [8]	被験者の行動観測	職場環境（催促・非礼・緩い監視）
筆者ら（本研究）		緩い監視（共有アカウントの利用・ID 非表示）

り，管理者が不正や違反を知りながらそれを放置したりといった組織の体質のことを指す [30]．職場環境や風土を改善することが内部不正の防止につながることは明らかとなったが，限られた経営資源の中でこれらを大きく改善することは容易ではない．IPA による内部不正に関する企業の実態調査では，従業員の内部不正への気持ちを最も低下させ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 [31]．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，アンケートの回答は，回答者が自分の過去に実施した内部不正を追及されたり，今後の社会生活に悪影響を及ぼしたりすることを懸念した結果，実態と乖離してしまう可能性がある．

そこで，我々は内部不正を誘発する要因を識別するため，疑似環境で被験者に軽微なタスクを与え，実際の行動を分析する実験を行った．被験者には異なる要因を与え，不正事象の発生数を比較した．要因は催促，暴言，監視が緩い環境の 3 種類を与えたところ，監視が緩い環境の方が不正事象が発生しやすいことを明らかにした [8]．一方，監視方法には，監視カメラの設置，警告メッセージの表示，警備員の配備やアクセスログによる監査など様々なものが存在する．これらの方法の中でも，内部不正の発生リスクに強く起因している方法を識別することができれば，組織は当該監視を強化することで効果的に内部不正の発生を抑制することができる．

先行研究と本研究を比較した結果を**表 2** に示す．

2.3 共有アカウントの利用と内部不正

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 [11]．インタビューの結果，エンドユーザにおける最も悪質な行動は認証情報の共有（17%）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．また，IPA は内部不正発生時に利用者の識別が困難なため，心理的に共有 ID の利用は重要情報を持ち出しやすい環境となると指摘している [10]．Hausawi や IPA は，共有アカウントと内部不正の関係をしているにとどまり，その影響の大きさについては明らかにしていない．

3. 実験のデザイン

3.1 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．

3.2 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 $H_{\text{共有}}$：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 $H_{\text{表示}}$：作業中に常時アカウント名が明示[*3]されていないと不正行為を犯す．

3.3 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．

[*3] 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 3 実験デザインの概要
Table 3 Overview of experiment design.

3.1 実験対象とする要因	3.2 実験の仮説	3.3 実験の課題	3.4 課題へのアプローチ
共有アカウントの利用	仮説 $H_{共有}$	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
アカウントの非表示	仮説 $H_{表示}$	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

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．

3.4 課題へのアプローチ

本研究は，3.3 節の課題について次のように解決を試みた．

3.4.1 不正事象を誘発する要因の制御

Kelling ら [32] 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 [33] 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（3.8 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（3.8 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（3.8 節の (4) の実装方式に対応）．

表 4 仮説とグループの関係
Table 4 Study groups and conditions.

グループ	$H_{共有}$	$H_{表示}$	N
A	共有	非表示	52
B	個別		52
C	共有	表示	46
D	個別		48

3.4.2 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（3.8 節の (5) の実装方式に対応）．

3.4.3 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（3.8 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 3** に示す．

3.5 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 4** 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．

3.5.1 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 [34] 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

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

より，20 名である．3.5.3 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．

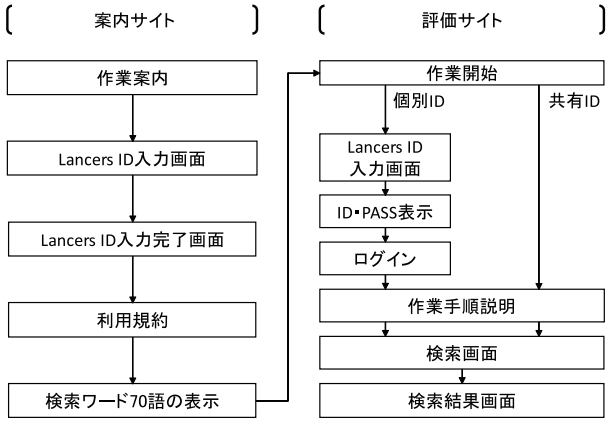

図 1 画面遷移図

Fig. 1 Screen transition diagram.

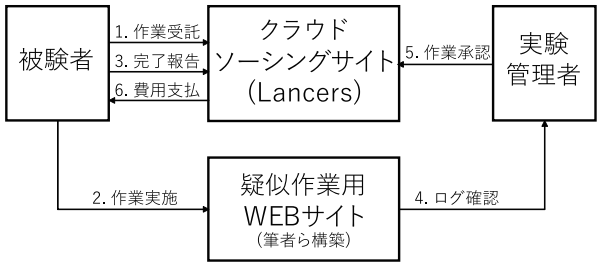

図 2 作業の流れ

Fig. 2 Flow diagram of the experiment.

3.5.2 作業の流れ

図 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 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．

3.5.3 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 $H_{\text{共有}}$ 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 $H_{\text{表示}}$ 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．

3.5.4 医療分野における研究と本実験の類似点

丹後ら [34] 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，3.5.3 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．3.7 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．

3.5.5 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 検索ワードの例
Table 5 Examples of a search word.

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[*4]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．3.8 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．

3.6 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** 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．

3.7 不正事象

3.7.1 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．

(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

[*4] 募集要項の詳細は A.1 節参照．

表 6 不正事象と検知方法の関係
Table 6 Relationship between malicious activities and methods of detection.

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 7 被験者の検索回数 s と遅延時間，貼付制限の関係
Table 7 Relationship between search count and delay time, the restriction of pasting text.

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	○

にアクセスすること」に該当する．

3.7.2 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 6** 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．

3.8 課題に対する実装方式

3.4 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 7** 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[*5]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 7 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 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．

4. 実験結果

4.1 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 の紐付けができなかった．そのため，被験者は 198 名である[*6]．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 8** 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．

*5 例：宸翰（表 5 のユーザ B の 5 番目）
*6 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．

表 8 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）

Table 8 Number of users (A: sharing / non-indicated, B: individual / non-indicated, C: sharing / indicated, D: individual / indicated).

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

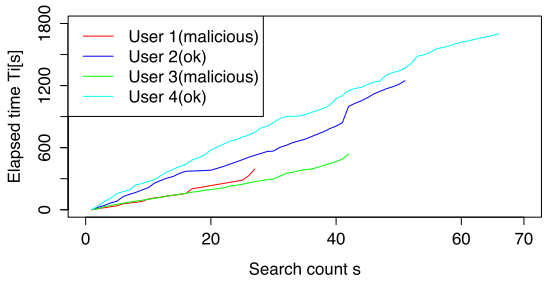

図 3 所要時間と検索回数（代表的な 4 つのパターン）

Fig. 3 Elapsed time with regards to query counts.

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．

4.2 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 T_i [秒] とする．被験者の検索回数 s と所要時間 T_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 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 3 の赤線と緑線が不正事象である．

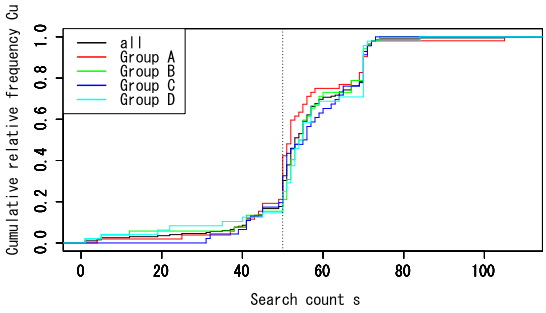

図 4 s 回以上検索した累積被験者数

Fig. 4 Cumulative relative frequency of users with query counts s.

表 9 不正事象別被験者数

Table 9 Number of users who performed malicious activities.

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

4.3 検索回数（グループごと）

図 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．

4.4 不正事象

4.4.1 不正事象別発生被験者

表 9 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 10** 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との検索回数 s の累積相対頻度 $Cu(s)$ を**図 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 10 不正事象 (1) 途中放棄の発生被験者数
Table 10 Number of users who performed Sabotage (1).

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

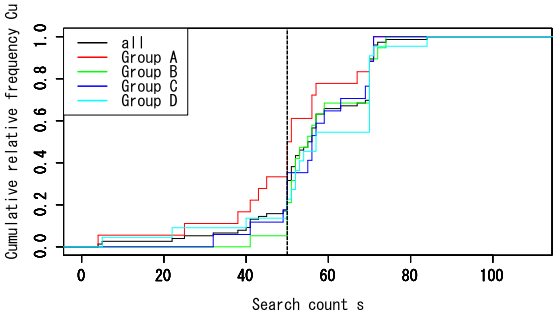

図 5 s 回以上検索した累積被験者数（30 代のみ）
Fig. 5 Cumulative relative frequency of users with query counts s (only 30s).

4.4.2 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 [34] 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．3.2 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．

表 11 不正事象の発生被験者数（仮説ごと）
Table 11 Number of users who performed malicious activities for each hypotheses.

分類	不正	$H_{\text{共有}}$ 共有 $A+C$	$H_{\text{共有}}$ 個別 $B+D$	$H_{\text{表示}}$ 非表示 $B+D$	$H_{\text{表示}}$ 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

表 12 不正事象 (1) 途中放棄の発生被験者数（属性ごと）
Table 12 Number of users who performed malicious activities of Sabotage (1) for each attribute.

グループ	共有（A+C） あり	共有（A+C） なし	個別（B+D） あり	個別（B+D） 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

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 4 の分類で集計したものが**表 11** および**表 12** である．検定結果を**表 13** および**表 14** 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．

4.4.3 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 15** 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 13 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）

Table 13 Result of fisher's exact test for each hypotheses (one-sided test).

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

表 14 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）

Table 14 Result of fisher's exact test on the number of malicious activities of Sabotage (1) for each attribute (one-sided test).

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	

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. 考察

5.1 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．

5.2 個別 ID の価値

予備実験 [1] 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

表 15 ロジスティック回帰分析の分析結果

Table 15 Logistic regression analyses results.

	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	

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．

5.3 不正事象ごとの発生数の差

表 9 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 7 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 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 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 [33] 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 3.8 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 [32] 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．

5.5 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 3.8 節の仕組みを用いて，不正事象を発生させるようにした．

5.6 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．

6. おわりに

本研究は，共有アカウントと不正行為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．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 を利用すると不正行為が約 3 倍，誘発されることが分かった．

謝辞 本研究の基礎となる人的セキュリティ研究について，ご指導をしてくださった情報セキュリティ大学院大学の原田要之助教授に感謝します．また，本研究への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，NTT 東日本の水越一郎氏に感謝します．

参考文献

[1] 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？，コンピュータセキュリティシンポジウム 2016 論文集，pp.617–624 (2016).
[2] 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).
[3] 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，入手先 ⟨http://blog.benesse.ne.jp/bh/ja/ir_news/m/2014/09/25/uploads/pdf/news_20140925_jp.pdf⟩（参照 2017-02-12）．
[4] 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，入手先 ⟨http://www.jiji.com/jc/article?k=2017011100522&g=soc⟩（参照 2017-02-12）．
[5] Aurigemma, S. and Panko, R.: A composite framework for behavioral compliance with information security policies, *Proc. 2012 45th Hawaii International Conference on System Sciences*, pp.3248–3257, IEEE Computer Society (2012).
[6] Renaud, K. and Goucher, W.: The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture, *Proc. 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp.361–372, Springer, Heidelberg (2014).
[7] 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，Vol.57, No.9, pp.2064–2076 (2016).
[8] Niihara, K. and Kikuchi, H.: Primary Factors of Malicious Insider in E-learning Model, *HCI International 2016 – Posters' Extended Abstracts: 18th International Conference, Proceedings*, Part I, pp.482–487, Springer International Publishing (2016).
[9] 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).
[10] 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，p.31 (2015).
[11] Hausawi, Y.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).
[12] Spitzner, L.: Honeypots: Catching the insider threat, *Proc. 19th Annual Computer Security Applications Conference*, pp.170–179 (2003).
[13] 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).
[14] 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).
[15] 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).
[16] 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).
[17] 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).
[18] Wortley, R. et al.：環境犯罪学と犯罪分析，社会安全研究財団 (2010).
[19] Cohen, L.E. and Felson, M.: Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, pp.588–608 (1979).
[20] Cressey, D.R.: *Other people's money; a study in the social psychology of embezzlement*, Free Press (1953).
[21] 警察庁：警察白書平成 20 年版，ぎょうせい (2008).
[22] 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).
[23] 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).
[24] 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).
[25] 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).
[26] 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).
[27] Nurse, J.R.C. et al.: Understanding Insider Threat: A Framework for Characterising Attacks, *2014 IEEE Security and Privacy Workshops* (*SPW*), San Jose, CA, pp.214–228 (2014).
[28] 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).
[29] 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).
[30] 星野崇宏，荒井一博，平野茂美，柳澤秀吉：組織風土と不祥事に関する実証分析，一橋経済学，Vol.2, No.2, pp.157–177 (2008).
[31] 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).
[32] Kelling, G.L., Coles, C.M., 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).
[33] 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).
[34] 丹後俊郎，古川俊之：医学への統計学，朝倉書店 (2013).

付　　録

A.1 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．

A.2 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．

新原 功一　（正会員）

2002 年青山学院大学理工学部経営工学科卒業．2010 年情報セキュリティ大学院大学修士課程情報セキュリティ専攻修了．2010 年情報セキュリティ大学院大学客員研究員．現在，明治大学大学院博士後期課程在学中．情報セキュリティインシデントの研究に従事．

山田 道洋　（学生会員）

2017 年明治大学総合数理学部先端メディアサイエンス学科卒業．現在，明治大学大学院博士前期課程在学中．

菊池 浩明 （正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学院博士前期課程修了．1994 年同博士（工学）．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，2006 年同情報理工学部情報メディア学科教授．1997 年カーネギーメロン大学計算機科学学部客員研究員．2013 年明治大学総合数理学部先端メディアサイエンス学科教授．2016 年同先端数理科学研究科長．WIDE プロジェクト暗号メールシステム FJPEM の開発，認証実用化実験協議会（ICAT），IPA 独創情報技術育成事業等に従事．暗号プロトコル，ネットワークセキュリティ，ファジィ論理，プライバシ保護データマイニング等に興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2010 年情報処理学会 JIP Outstanding Paper Award．2013 年 IEEE AINA Best Paper Award．2014 年情報セキュリティ文化賞．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM 各会員．本会フェロー．