情報処理学会論文誌 Vol.57 No.9 2064–2076 (Sep. 2016)

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

新原 功一[1,a)] 菊池 浩明[1]

受付日 2015年12月3日, 採録日 2016年6月2日

概要：昨今，認可された権限を用いて大量の個人情報を抽出し，外部に流出させる事故が世間の注目を集めている．この事件を契機として組織は，内部犯行を想定した対策を求められつつある．本研究は想定される内部犯行誘発要因と不正事象の関係を明らかにするため，疑似環境としてeラーニング形式のwebサイトを構築した．クラウドソーシングにより集めた100名の被験者を用いて，webサイトでは被験者ごとに異なる内部犯行誘発要因を発生させ，不正事象の発生数を測定した．測定結果を統計解析の手法を用いて分析し，誘発要因，個人属性（年代等），成績と不正事象の相関関係を明らかにした．

キーワード：内部犯行，情報漏えい，eラーニング，クラウドソーシング

Identification of Factors as Predictors of Insider Threat in e-learning Model

Koichi Niihara[1,a)] Hiroaki Kikuchi[1]

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: Recently, there were some incidents in which large amounts of personal information were leaked via malicious insider. Since then, organizations are required to prepare countermeasures to deal with insider threat. To reveal the connection between the hypothesized causes of insider threat and malicious activities, this study conducts an experiment using an e-learning website as a pseudo environment for insiders. The total of 100 subjects, collected via crowd-sourcing are divided into several groups with a different cause of insider threat. The numbers of malicious activities for each group are observed. The experimental results show the statistical analysis that reveals the correlation between the hypothesized causes (e.g., personal attributes, environment, and record) of insider threat and malicious activities.

Keywords: Insider threat, Information leakage, E-learning, Crowd-sourcing

1. はじめに

昨今，悪意のある従業員により大量の個人情報を漏えいさせる事故が生じている [1]．この事件を契機に，内部犯行のリスクは広く認識され，組織は十分な配慮を行うことを求められている．この従業員は比較的容易に個人情報を大量に取得できる端末，監視が薄い環境等に誘発されて犯行に及んでいる．したがって，従業員が組織等の環境要因により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] 明治大学大学院
Meiji University Graduate School, Nakano, Tokyo 164–8525, Japan
[a)] niihara@gmail.com

情報漏えいに関する内部犯行の関連研究は，主に3つに分類することができる．まず，内部犯が利用するPCやシステムの操作履歴に基づき，その振舞いから不正事象を検知する研究である．Azariaらによる疑似タスクを用いて被験者の振舞いを観察した研究 [2] があげられる．次に，悪意のある内部犯をおびき寄せるために，おとりの機密情報等を用いる研究である．Spitznerによる Honeypot の研究 [3] があげられる．最後は，既存の内部犯行事象をもとに内部犯行を誘発する要因の分析や対策を検討する研究である．社会安全研究財団によるサイバー犯罪の事例分析 [4] 等が該当する．本研究は，既存の内部犯行ではなく，疑似的な内部犯行事象を分析対象としているが，内部犯行の誘発要因を探る点で最後の分類に該当する．関連研究の詳細

は 2 章に記す．

関連研究により，内部犯行を誘発する潜在的な要因が存在することは分かってきた．しかしながら，数多くの誘発要因のうち，どの要因が本質的であるのかは不明確であった．様々な要因が複合的に情報漏えい事故を引き起こしているからである．

そこで本研究は，内部犯行を誘発させる要因の特定を目的とする．組織は，業務を遂行するうえで従業員に対して厳しい対応を行わざるをえない場合がある．社会安全研究財団 [4] の事例分析では，内部犯行を誘発する要因として，社員に対する暴言や人遣いの荒さに起因した強い不満・怒り等をあげている．一方，仮に，業務上の指摘や催促を行えないと，組織は従業員のマネジメント手法を制限されて生産性の低下等につながる可能性がある．内部犯行の誘発要因のうち，本質的な要因を識別することができれば，組織は生産性を損なうことなく効果的に内部犯行の発生確率を低減させることを期待できる．

本質的要因を特定するためには異なる誘発要因を発生させ，内部犯による情報漏えい事象の発生を観測することが望ましい．しかし，実験自体が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．加えて，内部犯行の発生頻度は低く，たとえ生じても組織内の機密情報を守るため，その過程を詳細に観察することは困難である．そこで，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犯行誘発要因を与えた．そして，グループ（内部犯行誘発要因）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，内部犯行とは直接関係しない性別等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．

本研究の新規性は，e ラーニングサイトの検証環境での実験結果に基づいて，内部犯行誘発要因の影響を識別したことである．不正事象「教材未読回答」において，内部犯行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 17.9 倍不正を犯しやすいこと，および年代ごとにも有意な差があることを明らかにした．

以下，2 章では，関連研究の調査に基づいて，解決したい問題を設定する．3 章では実験計画，4 章で実験結果を記す．7 章では実験結果に対する評価，6 章で考察を行い，最後に 7 章でまとめを述べる．

2. 関連研究

本研究では，内部犯行の関連研究を以下の 3 つに分類した．

まず，1 つ目は被験者の振舞いから内部犯と正常者を検知する研究である．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 [5]．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．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 [6]．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 [7]．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．Azaria らは，Amazon Mechanical Turk[*1] で集めた 795 名の被験者の振舞いをもとに内部犯を検知する実証実験を行った．本実験では，通常のタスクと悪意の内部犯行タスクを実行する被験者の振舞いを模擬したシミュレーションを行った．彼らの行動をすべて記録し，SVM（Support vector machine）により学習し，内部犯の検知が可能かどうかを検討している [2]．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 つ目は，おとりのサーバ，ネットワーク，機密情報等により内部犯をおびき寄せる手法である [3]．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．従来の 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った．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．Spitzner は，内部犯行を

[*1] https://www.mturk.com/

検知するためのHoneypotsの応用手法として，HoneynetsとHoneytokensを提案している[3]．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[8]．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．

最後は，実際の犯罪記録をもとに特徴を類推し，傾向を把握するとともに対策を検討する研究である．本研究はこの分野に該当する．環境犯罪学では，犯罪者は犯罪事象の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[9]．本研究はこの環境を内部犯行誘発要因としてとらえる．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，監視性の低い場所の3つの要因が重なった場合に内部犯行が生じることを主張している[10]．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，内部犯行とその要因の関係を説明している[11]．Cohenらや Cressyらの研究では，複合的な要因の重なりが内部犯行を誘発する要因としている．内部犯行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犯行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[12]のうち，内部犯行を対象として事例分析を行った[4]．当該分析ではMooreらによる内部犯行の分類[13]をもとにシステム悪用，システム破壊，情報流出に整理し，犯行者の心理的な力動過程（ダイナミクス）を提示した．(1) 個人の資質，(2) 企業風土・文化，(3) リストラで解雇，離職（喧嘩別れ），社長の社員に対する暴言や人遣いの荒さに起因した強い不満・怒り等から内部犯行に及ぶとしている．当該研究では，内部犯行の要因が分析されているが，内部犯行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犯行に起因する12の予測因子を提唱している[14], [15]．Cornishらは，当該対策は都市空間における犯罪予防の理論として，直接的に犯罪を防止する対策，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[16]．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[17]を提案している．Greitzerら，Cornishら，IPAの研究は，内部犯行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．

そこで，本研究では被験者ごとに異なる内部犯行誘発要因を与え，不正事象の発生数を観測することで要因ごとの影響の大きさを識別する．

3. 実験計画

3.1 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犯行誘発要因を提供し，不正事象の発生数を観測した．

3.2 仮説

社会安全研究財団による事例分析[4]では，内部犯行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等をあげている．そこで，本研究では次の3つの仮説を立てる．

仮説H_1（催促）：頑張っているのに催促されると内部犯行を犯す．

仮説H_2（非礼）：暴言を受け，荒い人遣いをされると内部犯行を犯す．

仮説H_3（監視）：監視の目が届かないことが分かると内部犯行を犯す．

これらを確かめるため，次節で示す実験を行う．

3.3 実験

3.3.1 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犯行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

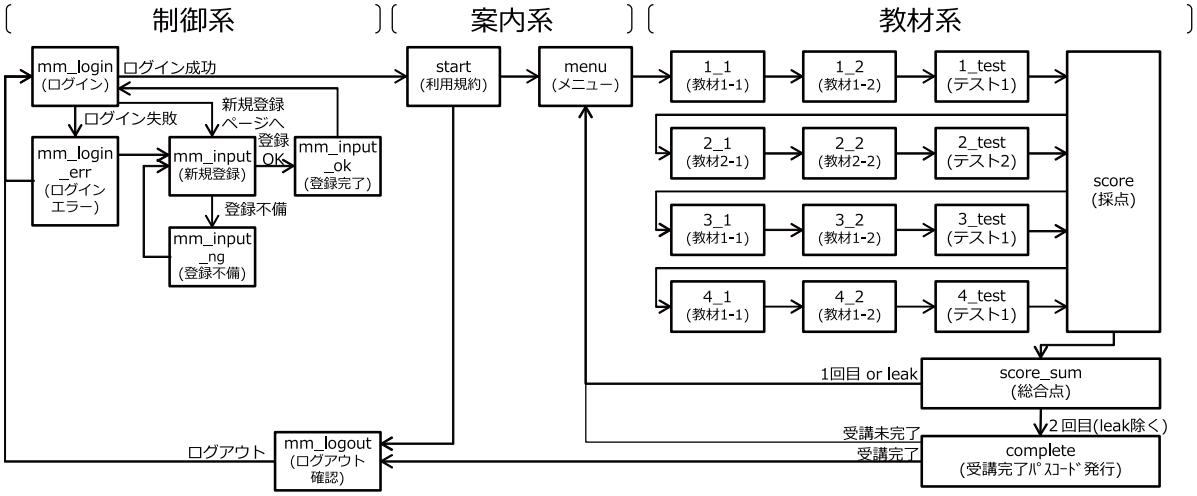

図 2 画面遷移図
Fig. 2 Screen transition diagram.

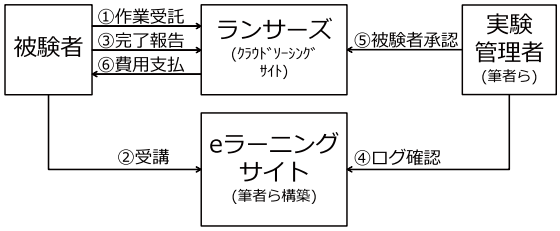

図 1 実験の流れ
Fig. 1 Processes of experiment.

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 節で後述する．

実施期間は 2015 年 7 月 16 日～25 日の 10 日間である．

3.3.2 実験の流れ

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，本サイトとする）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，本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 1** に示す．

3.3.3 被験者グループ

本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 1** に定める内部犯行誘発要因を発生させる．

表 1 内部犯行誘発要因と対象グループ
Table 1 Relationship between hypothesized causes of insider threat and groups.

仮説	内部犯行誘発要因	一般的な事象	本実験での擬似事象	対象ｸﾞﾙｰﾌﾟ A	B	C	D
H_1 (催促)	催促文言	頑張っているのに正答な評価がされない	・平均完了時間を当初より早める	○	—	—	—
H_2 (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	—	○	—	—
H_3 (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	—	—	○	—

3.3.4 本サイトのコンテンツ

本サイトの画面遷移を**図 2** 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，ログインチェック等を行う．

案内系は利用規約等を表示させ，本サイトの依頼事項，禁止事項等を表示させる．

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』[18]，IPA の情報セキュリティ対策のしおり [19], [20], [21] 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[*2].

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犯行誘発要因とは別にグループ共通に次の内部犯行誘発要因を与える．グループごとの内部犯行誘発要因の詳細は 3.4.1 項に示す．なお，受講 1 回目の 4 章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 ソース等を確認して回答」を除き，全員合格とする．

3.3.5 不正事象の定義

本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，回答等の横流し．
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 直打ち等によるアクセス」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．本サイトでは，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．

(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．本サイトではアクセス時刻から滞在時間を測定し，**表 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

[*2] 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 2 禁止事項と検出方法

Table 2 Relationship between prohibited matters and methods of detection.

禁止事項	検出方法	検出
1	アクセス時間より判定(4.4節)	○(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 読解速度 S_i の信頼度 95%の予測区間（上限）

Table 3 95% prediction interval of reading speed S_i.

教材	文字数 Ci	読解速度S_i[10^3字/分]			
		受講1回目		受講2回目	
		平均μ_{1i}	上限値S_{1i}^+	平均μ_{2i}	上限値S_{2i}^+
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	14.46	82.86
4 1	654	1.410	35.49	4.000	58.04
4 2	2,201	2.412	39.3	8.955	71.76

(3) 答案未回答

何も選択せずに回答した事象である．本サイトでは回答内容に基づいて判定する．

(4) HTML ソース等確認

「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．本サイトでは，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．

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 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．

3.4 内部犯行誘発要因

調査報告書 [4] をもとに想定される内部犯行誘発要因を本実験で擬似的に再現した．

3.4.1 グループごと誘発要因

本サイトでは，**図 3** のタイミングでグループごとに異なる内部犯行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」という想定内部犯行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

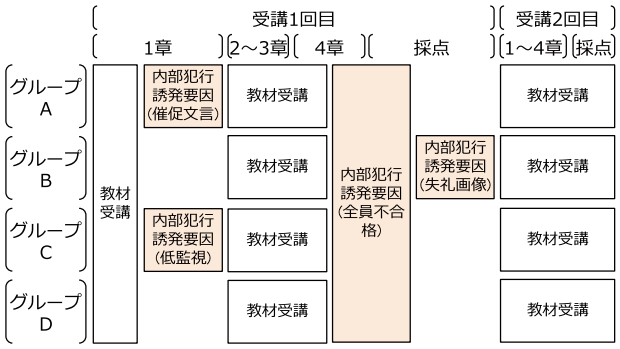

図 3 誘発要因の発生タイミング
Fig. 3 Timing of hypothesized causes of insider threat.

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「本サイトは，アクセスログ，アクセス時間等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 は上記の内部犯行誘発要因の効果を評価するため，いずれも割り当てなかった．内部犯行誘発要因とグループの関係を表 1 に示す．

3.4.2 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等のため，教材 1 確認テストまでは内部犯行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 のように要因ごとに異なる．

4. 実験結果

4.1 不正事象の発生状況

4.1.1 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 4** に示す．画面遷移番号は，図 2 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 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．

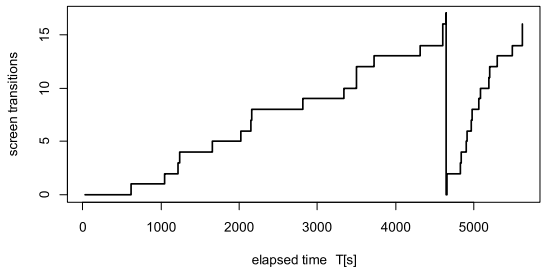

図 4 画面遷移（正常）
Fig. 4 Screen transition (normal).

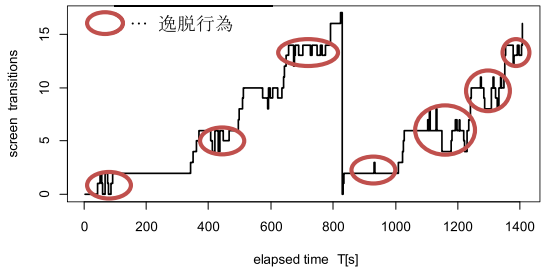

図 5 画面遷移（逸脱行為）
Fig. 5 Screen transition (abnormal).

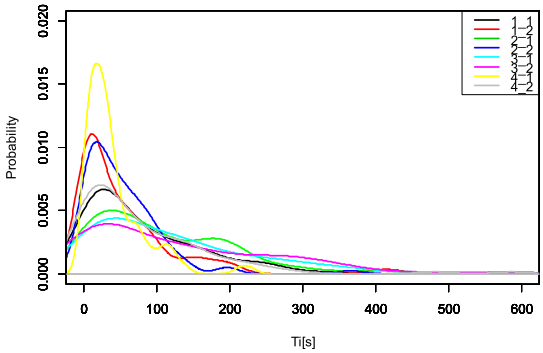

図 6 教材ごとの滞在時間 T_i の確率密度
Fig. 6 Probability density function of elapsed time T_i for each material.

4.1.2 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 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 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 2 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 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

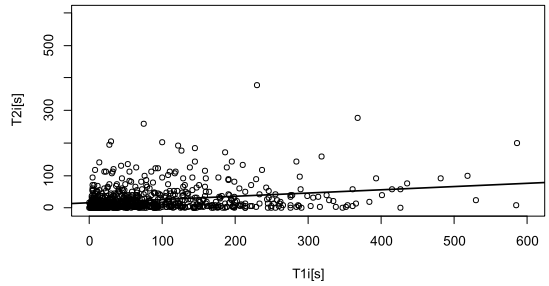

図 7 滞在時間 T_i（受講 1 回目/2 回目）

Fig. 7 Scatter plot between elapsed time T_i of the 1st lecture and 2nd lecture.

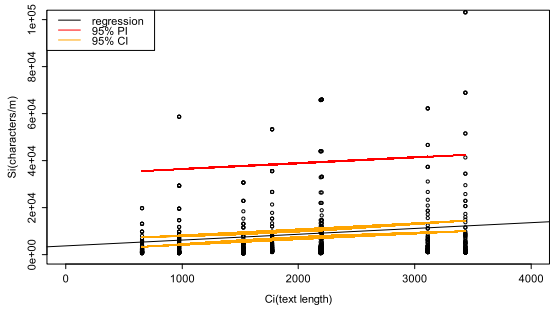

図 8 読解速度と文字数（受講 1 回目）

Fig. 8 Scatter plot between reading speed S_i and number of characters C_i (the 1st lecture).

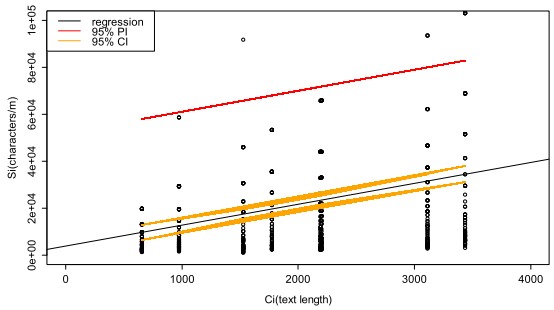

図 9 読解速度 S_i と文字数 C_i（受講 2 回目）

Fig. 9 Scatter plot between reading S_i and number of characters C_i (the 2nd lecture).

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 8**，**図 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 8，図 9 の赤線は，回帰式の信頼度 95%の予測区間である．

表 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 の上限値を上回ったとき，不正事象とした．

表 4 属性別ユーザ数

Table 4 Number of users for each attribute.

		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歳	6	6	7	6	25
	30〜39歳	11	12	14	16	53
	40〜49歳	6	2	5	4	17
	50〜59歳	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 5 不正事象発生ユーザ数

Table 5 Number of users who performed malicious activities for each group.

		N	(1)画面遷移逸脱		(2)教材未読回答		(3)答案未回答		(4)HTMLソース等確認	
				(再掲) 1-1		(再掲) 1-1		(再掲) 1-1		(再掲) 1-1
グループ	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

4.2 不正事象の発生ユーザ数

表 4 はグループごとの属性別ユーザ数である．

4.2.1 グループごと

表 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本サイトの内部誘発要因の表示前に発生している．

4.2.2 得点ごと

図 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．

4.2.3 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 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）．

4.2.4 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 7** に示す．

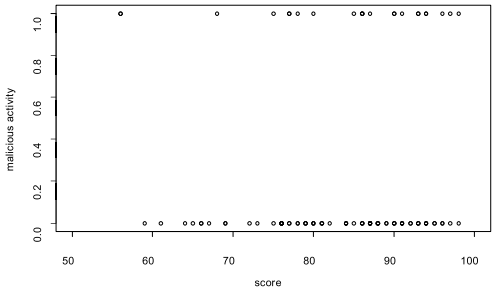

図 10 受講 1 回目の不正事象 (2) 教材未読回答の有無と得点の散布図

Fig. 10 Scatter plot between malicious activities of 1st lecture and score.

表 6 ランク別，受講回数別不正事象発生ユーザ数

Table 6 Number of users who performed malicious activities for each rank.

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

表 7 属性別不正事象発生ユーザ数

Table 7 Number of users who performed malicious activities for each attribute.

		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歳	25	7	12
	30〜39歳	53	13	7
	40〜49歳	17	6	3
	50〜59歳	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

4.3 成績

4.3.1 グループごと，受講回数ごと

表 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．

4.3.2 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 11** に示す．

表 8 得点（グループごと，受講回数ごと）

Table 8 Scores for each group in the 1st and the 2nd lecture.

	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

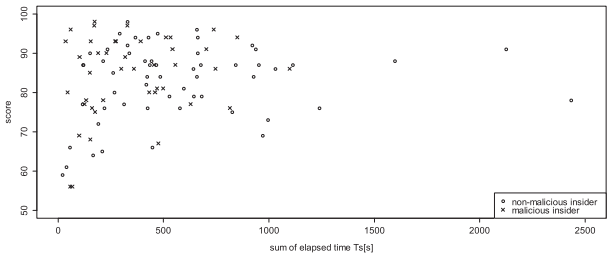

図 11 受講 1 回目の得点と滞在時間の合計 T_s の散布図

Fig. 11 Scatter plot between score of the 1st lecture and sum of elapsed time T_s.

5. 評価

不正事象 (3) 答案未回答，(4) HTML ソース等確認の評価は，発生数が非常に少ないため割愛した．また，図 10，表 6 より，得点別，ランク別の不正事象の発生数，また，図 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犯行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，性別や職業等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．

5.1 独立性の検定

5.1.1 グループ

本実験の標本は表 4 にあるとおり，性別，年代，職業等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 $\mathrm{Df} = 3$ 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 9** に示す．

表 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 9 カイ 2 乗検定の分析結果（属性別ユーザ数）
Table 9 Results of chi-square test. (Number of users for each attribute).

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歳	0.120	3	0.989	
	30〜39歳	1.113	3	0.774	
	40〜49歳	2.059	3	0.560	
	50〜59歳	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	

表 10 カイ 2 乗検定の分析結果（教材 1-1（共通条件）の不正者数）
Table 10 Results of chi-square test. (Number of users who performed malicious activities at 1st lecture's 1st chapter for each attribute).

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

5.1.2 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 5 の 1-1（共通条件）は，内部犯行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 10** に示す．

表 10 の分析結果から内部犯行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．

5.2 グループと不正行為

5.2.1 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 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効果があったと考える．

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．

表 11 ロジスティック回帰分析の分析結果（グループ別不正事象発生ユーザ数）
Table 11 Results of logistic regression analyses. (Number of users who performed malicious activities for each group).

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	**

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．

5.2.2 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 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．

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．

5.3 属性と不正行為

5.3.1 独立性

標本における性別，年代，職業等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．

表 12 カイ 2 乗検定の分析結果（属性別不正事象発生ユーザ数）
Table 12 Results of chi-square test. (Number of users who performed malicious activities for each attribute).

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	

表 13 ロジスティック回帰分析の分析結果（年代別不正事象発生ユーザ数）
Table 13 Results of logistic regression analyses. (Number of users who performed malicious activities for each generation).

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	**

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 12** に示す．

表 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．

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．

5.3.2 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 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．

6. 考察

6.1 内部犯行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 ソース等確認はグループごとの有意の差は認められず，内部犯行誘発要因との相関は見いだせなかった．一方，表 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 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等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 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 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．

6.2 e ラーニングサイトの限界

本実験では内部犯行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．

(1) 金銭目的の内部犯行の再現

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．

(2) 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．

6.3 母集団と標本

(1) 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 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．

(2) 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 9 によるカイ 2 乗検定を行った．

6.4 今後の研究課題

(1) 未認可の情報アクセスの検知

本実験では不正事象 (4) HTML ソース等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等がある．

(2) 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 等によって構築し，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．

(3) 被験者自身の性格等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，心配性尺度等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 らは内部犯行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 [14]．

(4) 内部犯行誘発要因が複合した場合の影響の識別

本実験では，表 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．

(5) 待遇の差の再現

社会安全研究財団 [4] によれば，待遇に不満がある従業員は内部犯行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犯行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．

7. おわりに

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犯行誘発要因を与え，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，内部犯行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．

(1) 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．
(2) 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．
(3) 若年層は文字量の多い教材は熟読しない傾向がある．

今後の主な研究課題は，以下のとおりである．

- 様々な第三者からの監視方法の中から内部犯行の抑制に効果の高い方法の識別
- 標本となる被験者の無作為抽出方法の検討
- 未認可の情報持ち出し，アクセスの検知
- 被験者自身の性格を考慮した内部犯行誘発要因の影響度分析
- 内部犯行誘発要因の複合時における影響の識別
- 待遇の差の再現

参考文献

[1] 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 2015 年 8 月 19 日）．
[2] 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).
[3] Spitzner, L.: Honeypots: Catching the insider threat, *Proc. 19th Annual Computer Security Applications Conference*, pp.170–179 (2003).
[4] 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).
[5] 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).
[6] Maloof, M. and Stephens, G.: *elicit: A System for Detecting Insiders Who Violate Need-to-Know*, Springer Berlin Heidelberg, pp.146–166 (2007).
[7] Caputo, D., Maloof, M. and Stephens, G.: Detecting Insider Theft of Trade Secrets, *Security & Privacy*, IEEE, pp.14–21 (2009).

[8] Brian, B. et al.: *Designing Host and Network Sensors to Mitigate the Insider Threat*, pp.22–29 (2009).
[9] Wortley, R. et al.：環境犯罪学と犯罪分析，社会安全研究財団 (2010).
[10] Cohen, L.E. and Felson, M.: Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, pp.588–608 (1979).
[11] Cressey, D.R.: *Other people's money; a study in the social psychology of embezzlement*, Free Press (1953).
[12] 警察庁：警察白書 平成 20 年版，ぎょうせい (2008).
[13] Moore, A., Cappelli, D. and Trzeciak, R.: *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*, Springer US (2008).
[14] 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).
[15] 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).
[16] 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).
[17] 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).
[18] 総務省：国民のための情報セキュリティサイト，入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/guide.html⟩（参照 2015 年 7 月 10 日）.
[19] 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).
[20] 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).
[21] 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).

付　　録

(1) 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．

(2) 内部不正誘発要因「失礼画像」の表示内容

図 A·1 に「失礼画像」を示す．

(3) 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．

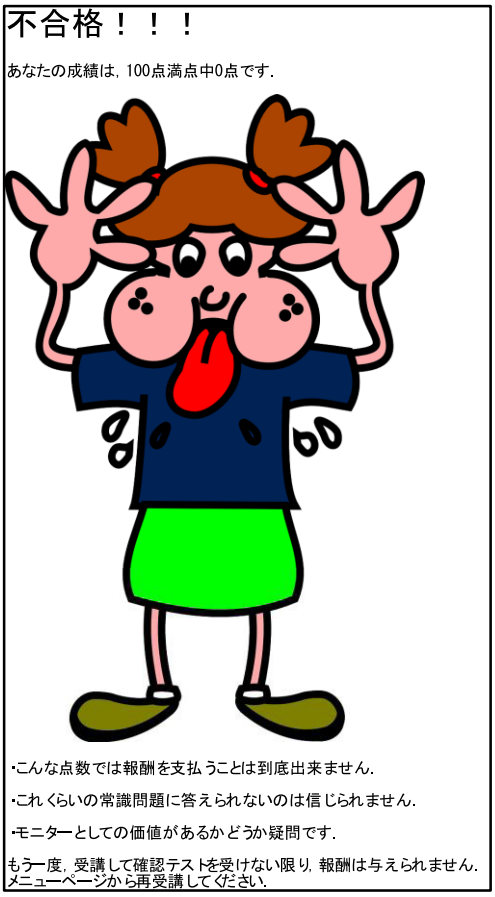

図 A·1 失礼画像
Fig. A·1 Rude picture.

新原 功一（学生会員）

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．

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．