# 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† 菊池 浩明†

†明治大学大学院
164-8525 東京都中野区中野 4-21-1

**あらまし** 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サイトでは被験者毎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，誘発要因と不正事象の相関関係を明らかにした．

# Identification of factors as predictors of insider threat in e-learning model

Koichi Niihara† Hiroaki Kikuchi†
†Meiji University Graduate School
4-21-1, Nakano, Nakano-ku, Tokyo 164-8525, JAPAN

**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 of insider threat and malicious activities.

## 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が漏えいする事故が生じた[1]．当該事故により悪意の内部犯行のリスクが広く認識されており，組織は内部犯行のリスクに対して十分な配慮を求められている．組織は，悪意のある従業員 1 名の内部犯行によって，残りの全従業員にルールを順守させるコストより大きな損害を被る．当該事故は，従業員が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[1]．従って，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することで変容を抑える必要がある．

組織は業務遂行上，従業員に対してやむを得ず厳しい対応を行わざるを得ない場合も存在する．仮に従業員の顔色を窺ってばかりいると，組織は従業員のマネジメント手法を制限され生産性の低下等に繋がる可能性がある．内部犯行誘発要因と不正事象の相関関係の識別が出来れば，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が出来る可能性がある．

情報漏洩事故に関する先行研究は，被験者の振舞いから内部犯と正常者を識別したり[2]，犯罪記録

から内部犯の傾向を分析している[3]. しかしながら, 内部犯行を誘発する潜在的な要因があることは分かってきたが, 数多くの誘発要因の中でどの要因が本質的であるのかは不明確であった. 多様な要因が複合して情報漏洩事故を引き起こしているからである.

本研究では内部犯行を誘発させる要因の特定を目的とする. しかし, 内部犯行の頻度は低く, 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クラウドソーシングにより集めた被験者を対象とし, 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る. 被験者グループ毎に異なる誘発要因を与え, 誘発要因毎に不正事象の発生に差があるかを観察した. 不正事象を発生させたユーザ数にグループ毎の差があるかどうかをカイ2乗検定し, 不正事象と誘発要因の間の独立性を確認する. 更に, 不公平な評価方法や監視性の低さ等の要因が不正を引き起こしているかを明らかにするため, ロジスティック回帰分析により検定し, 考察を行う.

# 2 関連研究

Azariaら[2]は, Amazon Mechanical Turk[1]にて集めた 795 名の被験者の振舞いを元に悪意のある内部犯と正常者を識別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. 彼らの行動を全て記録し, SVM(Support vector machine)により学習し, 内部犯の識別が可能かどうかを検討している.

社会安全研究財団[3]は, 国内にて 2007 年から 2009 年 6 月に検挙したサイバー犯罪[4]のうち, 内部犯行を対象として事例分析を行った. 当該分析では内部犯行をシステム悪用, システム破壊, 情報流出に分類し, 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. 当該分析は従業員に対するコミュニケーションが良好でない場合, 不正事象が発生する確率が高くなると示唆している.

# 3 実験計画

## 3.1 目的

本研究は不正事象を誘発する要因を識別することを目的とする. その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
・ユーザ毎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

実組織にて誘発要因を発生させ, 内部犯による情報漏洩事象の発生を観測することが望ましいが, 実験自体が組織のセキュリティポリシーに抵触する可能性があり実現が難しい. 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

2 章で示した事例分析[3]では, 内部犯行を誘発するいくつかの要因が報告されている. それらに基づき本研究では次の 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

本実験ではランサーズ社[2]のクラウドソーシングサービスを採用した. 被験者は当該サービスにて募集した. 被験者の質を確保するため, ランサーズ社にて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. 被験者数は 100 名, 実施期間は 2015 年 7 月 16 日～22 日の 11 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

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

[2] http://www.lancers.jp/

する)を受講する. 受講完了後, 本サイトは受講完了パスコードを発行し, 正規受講者を承認する. 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.

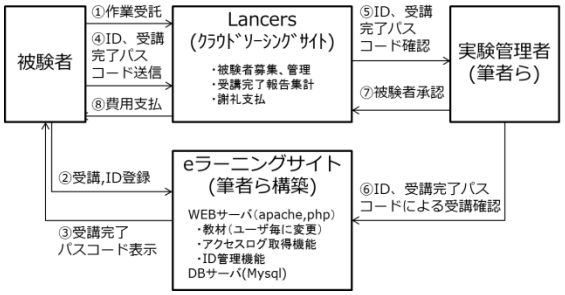


図 1 実験の流れ

### 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)を元にグループ(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グループ

| 内部犯行誘発要因名 | 一般的な事象 | 本実験での擬似事象 | 対象グループ | | | |
|---|---|---|---|---|---|---|
| | | | A | B | C | D |
| 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 | ○ | － | － | － |
| 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 | － | ○ | － | － |
| 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』[5], IPA の情報セキュリティ対策のしおり[6-8]を加工して作成した. 確認テストは各章にて 5 問ずつ出題し, 計 20 問とした. 満点は 1 問毎に 5 点, 章毎に 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)

・回答方法を都度変更する

- 選択肢のうち, 正しいもの,
- 選択肢のうち, 間違っているもの
- 選択肢のうち, 最も相応しいもの
- 選択肢のうち, 最も相応しくないもの
- 選択肢のうち, 相応しいもの全て
- 選択肢のうち, 相応しくないもの全て

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, 設問毎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.

### 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貼り付ける.

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以上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, 各画面のソースに php にてアクセス毎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

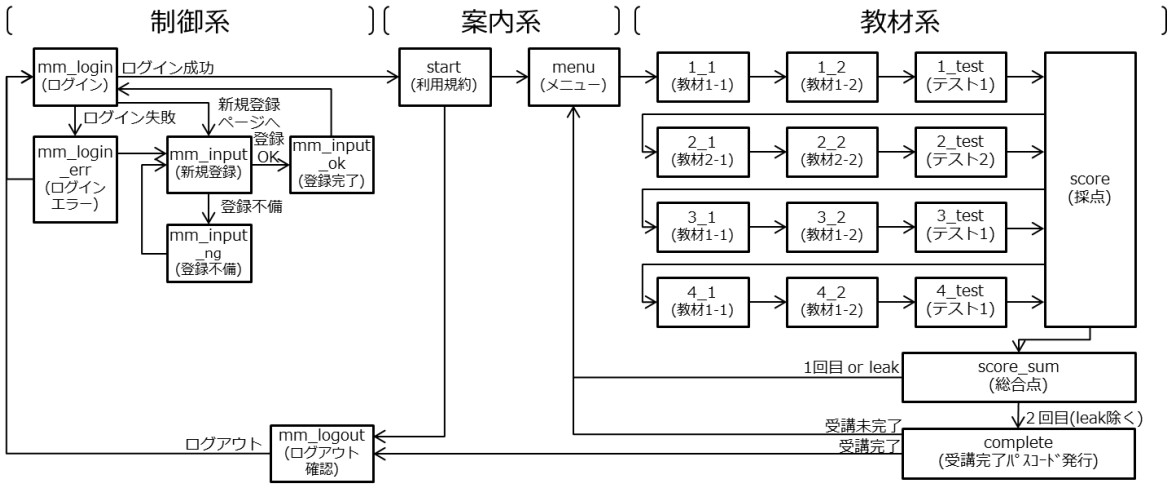


図 2 画面遷移図

「1.教材を必ず熟読した上で回答する」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，4.4 節に定めた閾値で判定する．

(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予め記載しておき，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．

表 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) |

## 3.4 内部犯行誘発要因

調査報告書[3]を元に想定される内部犯行誘発要因を本実験にて擬似的に再現した．

### 3.4.1 グループ毎誘発要因

本サイトでは，グループ毎に異なる内部犯行誘発要因を発生させた．

a)催促文言

「頑張っているのに正当な評価がされない」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、アクセス時間等を全て取得している」「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識別するため，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 共通誘発要因

被験者の不正を通常よりも誘発させるため，3.4.1 節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．

a)無条件で再試験

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 節に定める不正行為「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．

### 3.4.3 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全く発生させず，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 のように要因毎に異なる．

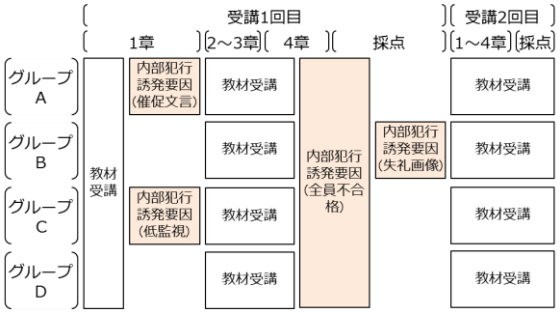


図 3 誘発要因の発生タイミング

## 4 実験結果

### 4.1 属性別ユーザ数

表 3 はグループ毎の属性別ユーザ数である．

表 3 属性別ユーザ数

| | | 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才～29才 | 6 | 6 | 7 | 6 | 25 |
| | 30才～39才 | 11 | 12 | 14 | 16 | 53 |
| | 40才～49才 | 6 | 2 | 5 | 4 | 17 |
| | 50才～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 |

### 4.2 不正事象発生ユーザ数

表 4 に 3.3.5 節に定める不正事象を発生させたユーザ数をグループ別，集計した結果を示す．表 4 の N はグループ毎のユーザ数である．各不正事象の左側の値は，受講中に不正事象を発生させたユーザ数，右側「(再掲)1-1」は受講 1 回目の教材 1 にて不正事象を発生させたユーザ数である．

表 4 不正事象発生ユーザ数

| | | 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ソース等確認 | (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 |

画面遷移逸脱は本サイトの内部誘発要因の表示前に不正事象が発生している．

### 4.3 画面遷移逸脱

経過時間と画面遷移の正常パターンを図 4 に示す．

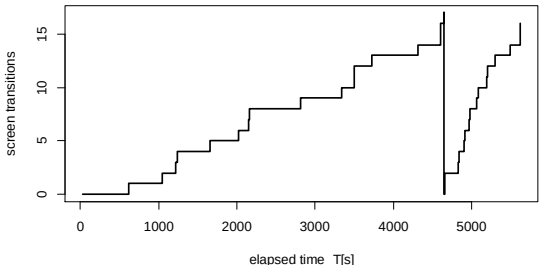


図 4 正常な画面遷移

正常パターンは1回目の採点画面に向けて画面遷移数が単調増加し，再受講にて一旦 0 まで下がり，再び増加する．

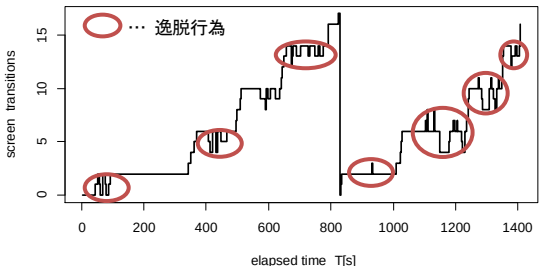


図 5 逸脱行為を含む画面遷移

ところが，図 5 の逸脱パターンは画面遷移数が度々減少する．これは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が繰返し行われたことを示している．

### 4.4 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 番目のアクセスの滞在時間 $T_i$[s]を

$$T_i = A_{i+1} - A_i$$

とする．i 番目の教材の文字数を $C_i$ とする．

図6，図7は受講1回目，2回目における滞在時間

$T_i$と教材の文字数 $C_i$(文字)の散布図である.

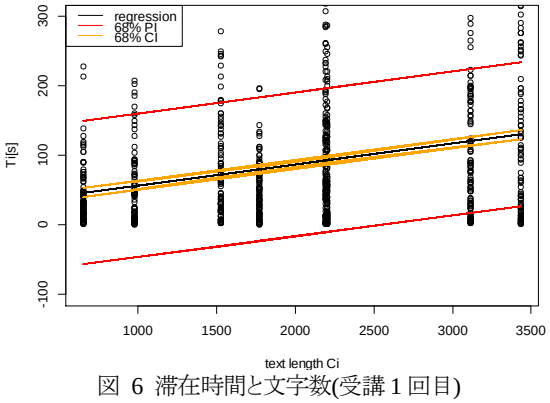


図 6 滞在時間と文字数(受講 1 回目)

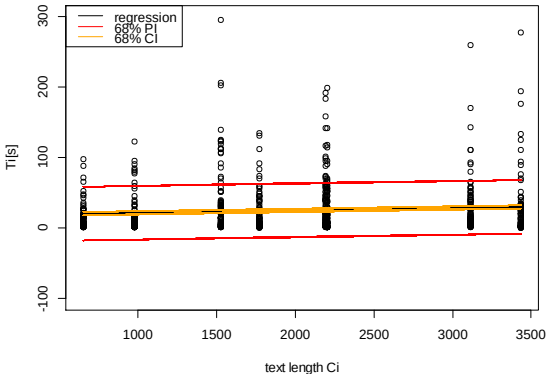


図 7 滞在時間と文字数(受講 2 回目)

受講 1 回目と 2 回目の滞在時間 $T_1$, $T_2$ の単回帰分析の回帰式を以下に示す.

$$T_{1i} = 27.0 + 3.00 \times 10^{-2} C_i$$

$$T_{2i} = 18.3 + 3.51 \times 10^{-3} C_i$$

図 8 は受講 1 回目における滞在時間 $T_i$ の確率密度分布である. 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.

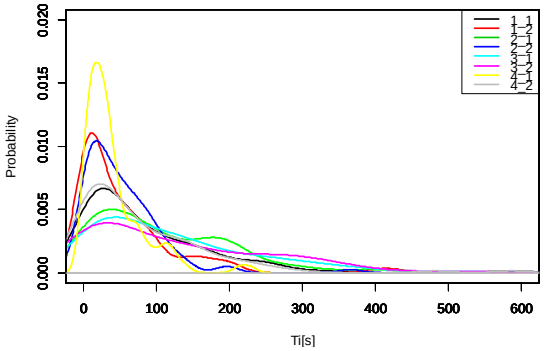


図 8 教材毎の滞在時間の確率密度

図 9 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.

i 番目の教材の読解速度 $S_i$(文字数/分)は

$$S_i = \frac{C_i}{T_i} \times 60$$

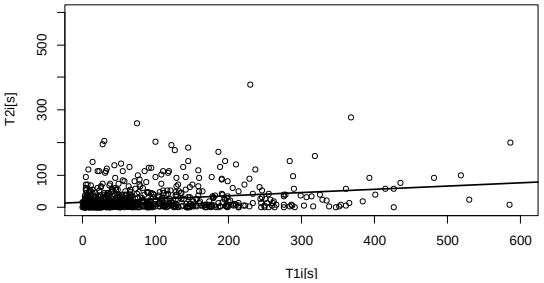


図 9 滞在時間(受講 1 回目/2 回目)

で与えられる. 図 10, 図 11 は受講 1 回目と 2 回目における教材毎の読解速度 $S_i$ と教材 $C_i$ の文字数の散布図である.

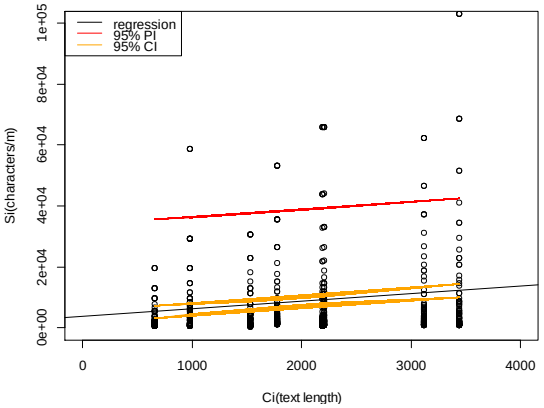


図 10 読解速度と文字数(受講 1 回目)

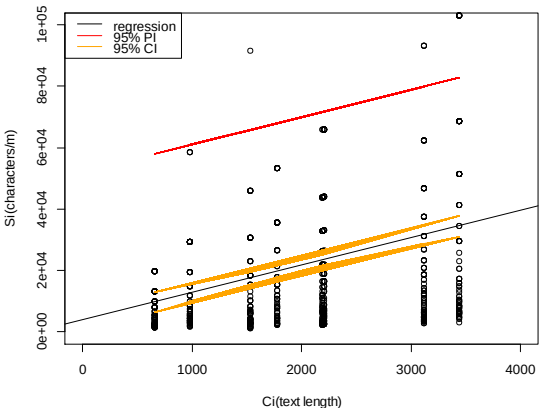


図 11 読解速度と文字数(受講 2 回目)

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 10, 図 11 の赤線は, 回帰式の信頼度 95%の予測区間である.

表 5 は教材毎の文字数 $C_i$ における受講回数毎の読解速度 $S_i$ の平均 $\mu_{1i}$, $\mu_{2i}$, 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 5 の値を上回った時, 不正事象とした.

表 5 読解速度 Si の信頼度 95%の予測区間（上限）

| 教材 | 文字数Ci | 読解速度Si[$10^3$字/分] | | | |
|---|---|---|---|---|---|
| | | 受講1回目 | | 受講2回目 | |
| | | 平均 $\mu_{1i}$ | 上限値 $S_{1i}^+$ | 平均 $\mu_{2i}$ | 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 | 39.30 | 8.955 | 71.76 |

# 5 評価

## 5.1 グループと不正行為の独立性の検定

各不正事象の発生ユーザ数は，グループ毎に差があるのか検定する．

表 3 と表 4 の 1_1(共通条件)の不正者より，4 つのグループは各属性がほぼ均等に分散していると考えられる．表 4 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，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．

帰無仮説 $H_1$：不正の有無とグループ（要因）は独立でない．

(1)画面遷移逸脱

統計量 $\chi^2$=1.921，p 値は 0.589 であった．従って，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．従って，5%の有意水準で帰無仮説 $H_0$ は棄却され，グループ毎の差があることが確認できた．

(3)答案未回答

不正事象の発生ユーザ数は 4 名のみのため，検定は割愛した．

(4)HTML ソース等確認

不正事象の発生ユーザ数は 1 名のみのため，検定は割愛した．

## 5.2 ロジスティック回帰分析

カイ 2 乗検定の結果，(2)教材未読回答はグループ毎の差が確認できた．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 6 に目的変数を教材未読回答，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．

表 6 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 | ** |

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わかる．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．

## 5.3 考察

本実験にて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毎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，不正事象(3)教材未読回答はグループ毎の有意の差が認められた．受講途中に不正に対する注意喚起の文言を表示させていないグループ C は，不正事象の発生数に著しい差があった．これは誘発要因「(c)低監視」が不正事象の発生に強い影響を与えていることを示している．

また，誘発要因「(b)失礼画像」も不正事象数に有意の差があった．グループ A の誘発要因「催促文言」は速く受講するように求めているにも関わらずグループ B の誘発要因「失礼画像」の方がより大きな差が存在した．「催促文言」は業務依頼の延長と捉えることが出来るが，「失礼画像」は暴言である．暴言に比べて，業務依頼に伴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．

本実験では注意喚起を表示しなかったユーザに不正事象が多く発生した．実組織でも情報漏洩等に関する注意喚起を従業員に伝えられていない場合，

不正事象発生のリスクが高くなっている可能性がある. 実組織にてこれらの注意喚起を職場等に掲示することは比較的容易である. 本実験は, 受講途中に注意事項の文言を数行追記しただけで不正事象の発生に著しい差があった. 注意喚起の対応が不十分である場合, 速やかな対応が必要である.

## 6　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ラーニングサイトにて再現し, グループ毎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. 実験結果にカイ 2 乗検定, ロジスティック回帰分析を行い, 内部犯行誘発要因に係る不正事象への影響を確認した. 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, 不正事象が発生する可能性が高い.

(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可能性が高い.

今後の課題は, 実組織の情報管理状況に近い環境等による本実験の拡張, 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である.

## 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",(2014) ( 2015 年 8 月 19 日参照, http://blog.benesse.ne.jp/bh/ja/ir_news/m/2014/09/25/uploads/pdf/news_20140925_jp.pdf).

[2]Azaria, A., et al., "Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data", IEEE Transactions on Computational Social Systems, pp. 135-155, (2014) .

[3]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) .

[4]警察庁, "警察白書 平成 20 年版", ぎょうせい, 12, ii, p.226, (2008) .

[5]総務省. "国民のための情報セキュリティサイト" (2015) (2015/07/10 参照, http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/guide.html) .

[6]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, "ウイルス対策のしおり（第 10 版）",(2015) .

[7]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, "不正アクセス対策のしおり（第 6 版）",(2015) .

[8]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, "インターネット利用時の危険対策のしおり（第 4 版）",(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全て選びなさい.

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


(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.