内部犯行を誘発する環境の機械学習による分析

山田 道洋 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1　はじめに

情報セキュリティマネージメントにおいて，内部犯行は最も防止が困難な大きな脅威である．事例も少なく，どのような要因が内部犯行を誘発しているのか観測することは困難である．

そこで，本研究では，内部犯行を誘発または，抑制する要因を明らかにして，マネージメントに活用することを目的とする．共有ゲストアカウントの利用など異なる誘発条件を与えた合計 198 名の被験者に単純なタスクを行わせ，内部犯行の有無を調査した．この実験結果について，（1）内部犯行を行う条件を表す決定木，（2）不正を表す連関規則の抽出，（3）各属性の不正に対するオッズ比を求めるロジスティック回帰の分析を行う．

2　関連研究

新原らは，第三者による監視が低い場合に不正事象が発生する確率が高くなるという実験結果を報告している [1]．Hausawi は，専門家にヒアリングを行い，最も否定的な行為は認証情報（パスワード等）の共有であることを報告している [2].

3　提案方式

3.1　目的

本研究は，共有アカウントの利用環境にて内部犯行を誘発，抑制する要因を特定することを目的とする．

3.2　実験概要

2016 年 10 月 31 日〜11 月 2 日にクラウドソーシングサイトで募集した 198 名を被験者とし，被験者を共有ゲストアカウント（ID: guest）と個別アカウントの 2 つのグループに自動的に振り分けて，筆者らが作成した WEB サイトにて検索エンジンを評価する単純作業を行ってもらい，不正の有無を観測する．

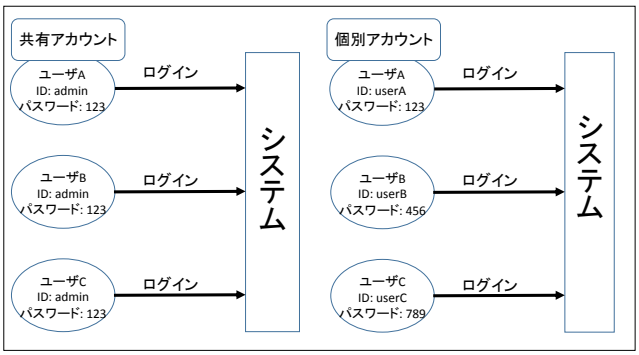

図 1　共有アカウントと個別アカウントの違いの例

3.3　共有アカウントの利用

共有アカウントと個別アカウントの違いの例を図 1 に示す共有アカウントには個別アカウントよりも管理コストが低く済むという利点がある．これは利用者が増えた場合などでも新たに ID やパスワードを発行する必要がないからである．しかし，共有アカウントは個別アカウントと比べて内部犯行を誘発しやすいと言われている．例えば，図 1 の共有アカウントの A が不正を犯しても B や C と区別がつかず，作業者の特定が困難で，不正がばれないという心情にさせてしまうからである．

3.4　作業の流れ

共有アカウント利用者と個別アカウント利用者の検索サイトまでの流れを図 2 に示す．まず，被験者はクラウドソーシングサイト「Lancers」で仕事を受注した後，筆者が用意した登録サイトへアクセスする本実験では，共有アカウントグループの検索サイトでのログイン行程を完全になくし，作業者が管理者にもわからないと被験者に思わせるために，登録サイトと検索サイトを別サイトに分割した．登録サイトには Lancers ID でログインし，別に用意された検索サイトにはログインせず，70 語のワードリストを用いて評価をする．図 3，図 4 に疑似検索サイトの実行例を示す．

†Michihiro Yamada, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University, Kikuchi Laboratory.

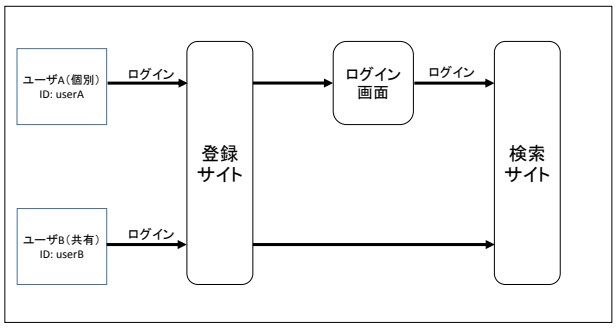

図 2　各アカウントの検索サイトまでの流れ

図 3　登録サイトの実行画面

図 4　検索サイトの実行画面

3.5　被験者の識別

本実験の検索サイトでは，共有アカウントグループはログイン行程を経ずに作業を開始する．そのためどの被験者がどんな検索を行ったかの観測が不可能である．そこで，被験者にそれぞれ異なる一意なワードリストを提示し，実際に検索されたワードを照合することで被験者の識別を行う．

表 1　各属性とグループの人数

グループ	共有アカウント	個別アカウント	合計
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

3.6　不正事象

被験者が検索サイトにて検索したワードが，50 語未満であった場合に不正事象とみなし，「作業の途中放棄」と定義する．検索作業は 50 語以上の検索を行わなくても作業の完了報告ができる様にし，不正行為が一定数発生することを期待する．

4　実験結果

4.1　実験結果

被験者の各属性とアカウントのグループ毎の人数を表 1 に示す．不正事象を犯した人数を表 2 に示す．共有アカウント利用グループの方に，より多くの不正者が発生した．

4.2　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．「途中放棄」をしたか否かをターゲット属性として，R のパッケージ “rpart” により学習した決定木を図 5 に示す．ここで，「Age>=55」等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．例えば，図 5 の木では年齢が 55 歳以上かどうかが不正を犯すかど

表 2　各属性とグループの不正者数

グループ	共有アカウント	個別アカウント	合計
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

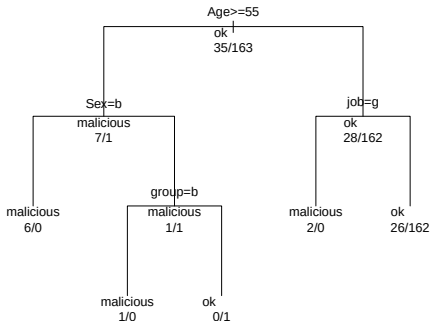

図 5　「途中放棄」の決定木

うかを決める最も大きな条件であり，55 歳以上の 7 名の不正者と，1 名の正規者がいる．

4.3　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」連関規則の抽出を行った．抽出した連関規則の一部を表 3 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．例えば，No.1 の規則は，「個別グループかつ職業が自営業の被験者は 89% の確率で正規者」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．

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，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．

4.4　ロジスティック回帰分析

各属性による影響の確率検定を行うために，R の”glm”関数を用いて目的変数を「途中放棄をした」と設定したロジスティック回帰分析を行った．分析結果とオッズ比を表 4 に示す．Intercept を基準にして対応する各属性との比較で計算しており，本分析の Intercept の持つ属性は「共有アカウント・女性・専業主婦」である．ロジスティックモデルでは，不正を犯す確率 p を，個別アカウントを表す論理変数 x_1，男である変数 x_2 などを用いて，

$$log\frac{p}{1-p} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots$$

と定める線形式で推定する．この係数 β_0，β_1 が表 4 の Estimate である．ロジスティック回帰分析では年齢 Age が不正への影響の有意差（p 値 < 0.05）が見られた．また，職業が学生，公務員の場合に有意差がみられるが母数が極端に少ないために特異なデータであると考えられる．

Odds は各属性と基準となる属性の不正を犯す確率を比較した時のオッズ比を示し，個別アカウントの利用者は共有アカウントの利用者と比べて不正を犯す確率が 0.67 倍に下がるという結果が得られた．

5　まとめ

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．また，連関規則により，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．さらに，ロジスティック回帰分析から個別アカウントの利用により共有アカウント利用時に比べて約 33 %不正を抑制できるという結果が示された．

一方，職業や年齢によって母数が極端に少ない要因も発生した．これら環境要因についても一定以上の母数を集めることは，今後の課題である．

表 3　抽出された連関規則 (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}	0.1313131	0.8965517	0.1464646	1.089063
2	{group=個別,Age=40's}	{Judge=ok}	0.1717172	0.8947368	0.1919192	1.086858
3	{group=個別,Age=30's}	{Judge=ok}	0.1868687	0.902439	0.2070707	1.096214
4	{group=個別,Sex=Male,job=自営業 }	{Judge=ok}	0.1111111	0.9166667	0.1212121	1.113497
5	{group=共有 }	{Judge=malicious}	0.1010101	0.2040816	0.4949495	1.154519

表 4　ロジスティック回帰分析とオッズ比

	Estimate	Pr(>|t|)	Odds
(Intercept)	-0.107074	0.384287	2.41E-02
Group 個別	-5.42E-02	0.306387	6.78E-01
Sex 男性	0.048906	0.465707	1.41E+00
Age	6.49E-03	0.023689 *	1.05E+00
job 自営業	0.031873	0.735564	1.38E+00
job 会社員	0.097586	0.297715	2.18E+00
job その他	0.087399	0.476033	1.86E+00
job パート，アルバイト	-0.06025	0.566693	4.41E-01
job 公務員	0.668873	0.082308 .	2.90E+07
job 学生	1.012411	0.000336 ***	3.37E+08
job 無職	0.06497	0.558746	1.74E+00

参考文献

[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，Computer Security Symposium 2015, 情報処理学会，pp. 747-754, 2015.

[2] Hausawi, et.al，Current Trend of End-Users' Behaviors Towards Security Mechanisms，HAI，HCI 2016，pp．140-151，2016.