情報セキュリティ行動モデル
- サウジアラビアの労働者の調査 -

アルスライマン　ハワーゼン[1]　小松　文子[1]

概要：情報セキュリティインシデントの多くが人的要因を原因としていることが報告されており，情報セキュリティ対策においては人的対策の重要性が指摘されている．本稿では，組織における情報セキュリティ行動を推進するために個人のセキュリティ行動への動機付けをいかにするかを目的に，情報セキュリティ行動モデルの構築を試みている．組織における情報セキュリティ行動は，組織のセキュリティポリシーへの意識や理解が必要である．情報システムの利用者が，新たな技術を受容する際の技術受容モデル（Technology Acceptance Model）を基盤として，情報セキュリティ技術と情報セキュリティポリシーへの意識と，情報セキュリティに関連した要因を加え，サウジアラビアの労働者を対象としたアンケートを実施した．モデル検証のための準備段階の分析を行ったので報告する．

キーワード：　情報セキュリティポリシー，情報セキュリティ行動，技術受容モデル

A Study on Information Security Behavioral Model
- Case of Labors in Saudi Arabia -

AL-Sulaiman Hawazen[1]　Ayako Komatsu[1]

Abstract: It has been reported that most of the information security incidents are caused by human factors, and the importance of human measures has been pointed out in the information security measures. In this paper, we attempt to construct an information security behavior model for the purpose of how to motivate individuals to take security actions in order to promote information security behaviors in organizations. Information security behavior in an organization requires awareness and understanding of the security policy of the organization. Based on the Technology Acceptance Model (TAM), which is based on the acceptance of new technology by users of information systems, we added the awareness of information security technology and information security policy, and factors related to information security. A questionnaire survey was conducted. This paper reports on the analysis of the preparatory stage for the model validation.

Keywords: Information Security Policy, Information Security behavior, Technology Acceptance Model

1. はじめに

組織が情報の保護に失敗する主な理由は，組織が主に技術的ソリューションに依存することにある．多くの組織のセキュリティ対策の中で最も弱い部分である人的要因を無視しているためだ．意識，対人スキル，組織文化などの人的要因が情報セキュリティ行動に影響を与える可能性がある． 2018 年 JNSA による調査では，発生した個人情報のインシデントの約 70%の原因が人間だと報告している[1]. また，Ingham の英国でのデータ侵害の 88%は人為的ミスが原因であり，最も一般的な間違いは機密データを間違った受信者に送信することだった．これは多くの場合，電子メールやファックスなどで発生した[2]. Ernst and Young's：2018-2019 Global Information Security Survey[3]によると，組織の 34%が，セキュリティを意識していない従業員が最大の弱点であると感じている．

サウジアラビアのセキュリティの状況について紹介する．各省には独自のセキュリティシステムがあったが, 2017 年に国家のサイバーセキュリティを担当する政府機関である国家サイバーセキュリティ機関（NCA: National Cybersecurity Agency）を設立し，その業務に関する国家機関としての役割を果たしている. NCA には，サイバーセキュリティに関する国家戦略の立案とその実施の監督を含み包括的に国家レベルで取り組みを開始した. 2020 年の第 4 四半期のレポートにおけるサウジアラビアでの 5 つの最も顕著な脅威は，第一は不正行為，二番目はマルウェア，三番目は不正アクセス，四番目は情報漏えい，最後はドメイン名のなりすましであった[4].

これらの調査結果から，人間は情報セキュリティの最も弱い部分であるということが分かる．そのため，個人の行動の原理を対象とした研究領域である行動理論を援用することが必要と考える． 本論文は，組織における個人の情報セキュリティ対策推進のための行動モデルを構築するための準備段階として，サウジアラビアの労働者に対する調査

1 長崎県立大学　地方創生研究科　情報工学専攻
University of Nagasaki

と，その分析について述べる．本論文の構成は，2 章で関連研究について述べ，3 章で研究課題と仮説，4 章で調査内容，5 章で調査結果を述べる．6 章で調査結果に対する分析と考察を述べ，7 章でまとめる．

2. 関連研究

AL-Omari ら(2012)は，技術受容の理論（TAM）を使用して情報セキュリティ意識が従業員の情報セキュリティポリシーへのコンプライアンスをいかに高めるかを明らかにすることを目的に，セキュリティ受容モデル（SAM）を導入した．セキュリティ受容モデルは，「防御に対する知覚された有用性（PUOP)」と「防御に対する知覚された使い易さ（PEOU)」がインテンション（意図）を形成するが，それぞれの要素に対して，規範，自己効力，制御可能性と利用者意識（Awareness）が影響を与えるモデルを提案した．この研究ではヨルダンの銀行部門で調査を実施し PLS 回帰分析の結果，モデルの有効性と，組織のセキュリティポリシーへの従業員のコンプライアンス意図へ影響を与える要因が明らかになった［5］．図 1 に TAM を示す．

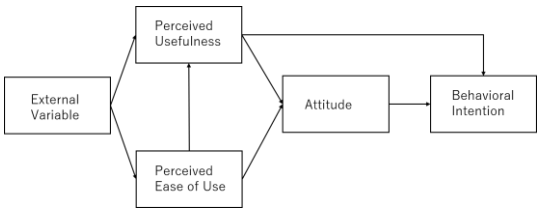

図 1　技術受容モデル（TAM）

Figure1　Technology Acceptance Model , [10]

Alanazi ら(2020)は，サウジアラビアの医療センターの労働者の情報セキュリティポリシー順守行動に影響を与える要因を明らかにするために，計画行動理論(TPB)[11],一般予防理論[12],防護動機理論（PMT）[13]，認知的モラル発達理論，イノベーション普及，合理的選択理論（RCT）などの理論から調査項目を作成し，サウジアラビアの医療センターと病院の 433 人の労働者を対象として調査を実施し，一般的なセキュリティ意識，自己効力感，宗教・道徳が影響を与えた因子であることを報告している［6］．

セキュリティ行動を測定する尺度として，Serge Egelman ら(2015)は、セキュリティ行動意図スケール(SeBIS)を開発した。SeBIS は 16 項目から構成される［7］．

Nader Sohrabi Safa ら（2015）は，防御動機理論，計画行動理論を適用し，情報セキュリティ意識，情報セキュリティポリシー，経験と関与，態度，主観的規範，脅威の評価，自己効力感がユーザーのセキュリティ行動に対して影響を与えるかを調査を通して構造方程式モデリングにより分析した．この調査では，情報セキュリティ，情報セキュリティに対する態度，脅威の評価，主観的な基準，および情報セキュリティの自己効力感，経験と情報共有が，ユーザーの行動にプラスの影響を与えることが示された．ただし，知覚される行動制御は，セキュリティを意識した行動に大きな影響を与えない［8］．

Burcu Bulgurcu ら（2010）は，合理的選択理論（合理的選択 RCT）と計画行動理論，社会的認知理論を通じて仮説モデルを構築し，情報セキュリティポリシーの遵守に対する従業員の態度に影響を与える要素を調査分析した．さまざまな組織の 464 人の従業員の調査からデータを収集した．結果は，コンプライアンス行動を強化する報酬や制裁以外の動機付け要因，特に自己効力感が大きな影響を与えることが示された［9］．

3. 研究課題　と　仮説

関連研究で述べたように，情報システム利用者が，情報セキュリティ行動を推進するには様々な要因から影響を受けていることがわかる．特に本研究では，サウジアラビアにおける組織の従業員の実際の情報セキュリティ行動に影響を及ぼす要因を明らかにすることを研究課題をする．

3.1　仮説

仮説モデル（図 2）は， AL-Omari[5]が提唱した PUOP, PEOU から意図への影響をモデル化した情報セキュリティ受容モデル(SAM)を参照したが，TAM で規定された「態度（Attitude)」と「行動」を追加している．これは，態度が意図を形成するという計画行動理論（TPB）にも沿うものである．仮説モデルにおける要素を以下に説明する．

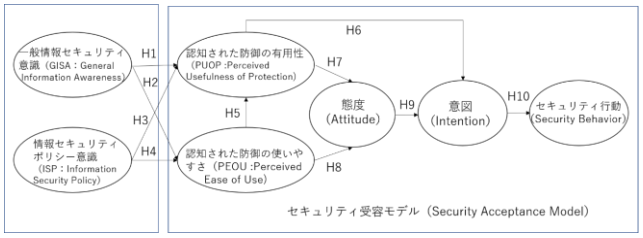

図 2　仮説モデル

Figure.2　hypothetical model

- 一般情報セキュリティ意識（GISA）：情報セキュリティ全般に対する知識や興味など
- 情報セキュリティポリシー意識（ISP）：組織の情報セキュリティポリシーへの
- 認知された防御の有用性(PUOP)：ISP が自身の業務にとって有用であること
- 認知された防御の使いやすさ(PEOU)：IPS を組織に適用することの容易さ
- 態度（ATT）：ISP を順守することへの態度
- 意図（BI）：ISP を順守する意図
- セキュリティ行動（SB）：SeBIS を利用したセキュリティ行動

これらの要素における各仮説を以下に説明する.

H1: 一般情報セキュリティ意識は，セキュリティ行動に対する認知された防御の有用性にプラスの効果をもたらす.

H2: 一般情報セキュリティ意識は，セキュリティ行動に対する認知された防御の使いやすさにプラスの効果をもたらす.

H3: 情報セキュリティポリシー意識は，セキュリティ行動に対する認知された防御の有用性にプラスの効果をもたらす.

H4: 情報セキュリティポリシー意識は，セキュリティ行動に対する認知された防御の使いやすさにプラスの効果をもたらす.

H5: 認知された防御の使いやすさは，セキュリティ行動に対する認知された防御の有用性にプラスの効果をもたらす.

H6: 認知された防御の有用性は，セキュリティ行動に対する意図にプラスの効果をもたらす.

H7: 認知された防御の有用性は，セキュリティ行動に対する態度にプラスの効果をもたらす.

H8: 認知された防御の使いやすさは，セキュリティ行動に対する態度にプラスの効果をもたらす.

H9: 態度は，セキュリティ行動に対する意図にプラスの効果をもたらす.

H10: 意図は,セキュリティ行動にプラスの効果をもたらす.

4. 調査

仮説モデルを検証するために,サウジアラビアの労働者に対してアンケートによる調査を実施する．具体的には，サウジアラビアの公的機関の協力を得ることができた．サウ当該機関には，サイバーセキュリティ部門が存在し，組織の情報と技術資産の保護に取り組んでいる．

調査項目は表 1 に示すように，それぞれの参考文献より抽出した. 詳細な項目は, 付録 A.1 に示した. 各項目には，プレフィックスを付けている（例：一般セキュリティ意識は，GISA01 から GISA05）

5. 調査結果

調査は，3 回の予備調査と 1 回の本調査を実施した．1 回目の予備調査は，6 人に対し 56 項目を英語で実施し，2 回目は 33 人に対し 56 項目をアラビア語で実施した．2 回の予備調査とも項目が多い，類似項目があるという意見があった．このため，3 回目は，信頼性係数が低い項目と類似項目を削減し 60 人に対して実施した. 本調査では，さらに信頼性係数が低い項目と類似項目を減らし, 44 項目としアラビア語で実施した．調査機関は，2021 年 6 月 7 日から 6 月 27 日の 20 日間である.

表 1　調査項目の分類と，項目数

Table 1 Classification of survey items and number of items

調査項目	項目数	参照
一般セキュリティ意識（GISA）	5	[5,6]
情報セキュリティポリシー意識（ISP）	5	[5]
認知された防御の有用性（PUOP）	5	[5]
認知された防御の使いやすさ（PEOU）	5	[5]
態度（Attitude）	5	[8,9]
意図（Intention）	5	[5,6]
セキュリティ行動（Behavior）	14	[7]

本調査の対象者数の年齢別，割合を表 2 に示す.

表 2　調査回答者

Table2 Survey Respondents

年齢	男性	女性	計
21-30	10	14	24
31-40	49	80	129
41-50	74	89	163
51-60	29	14	43
	162	197	359

6. 分析と考察

本研究では，最終的には図 1 に示す仮説モデルを検証することを目的としているが，本稿においては，仮説モデルを検証する準備段階として，因子分析による質問項目の検証と，各項目と情報セキュリティ行動への影響を重回帰分析により検証した．分析には IBM SPSS Statistics v26 を使用した.

6.1 相関分析

まず各要素の項目のうち，逆転項目を変換し，要素ごとに値を加算したデータを用いて，スピアマンの順位相関分析を実施した．表 3 に結果を示す.

表 3　スピアマンの順位相関分析

Table 3　Spearman's rank correlation analysis

	GISA	ISPA	PUOP	PEOU	ATT	BI
GISA	1.000					
ISPA	.422**	1.000				
PUOP	.286**	.464**	1.000			
PEOU	.444**	.369**	.384**	1.000		
ATT	.244**	.378**	.484**	.375**	1.000	
BI	.206**	.410**	.425**	.231**	.496**	1.000
SB	.387**	.282**	.260**	.326**	.265**	.190**
** 相関係数は 1%水準で有意						

結果は，以下の通りである．BI と SB 間にほとんど相関がない（≦0.2）以外は，低い相関（0.2＜r≦0.4）または，相関があり（0.4<r≦0.7），となった．高い相関のある組み合わせはなかった．

6.2 因子分析と信頼性係数

調査項目のうち，GISA から BI の 30 項目と，SB の 14 項目についてそれぞれ因子分析を実施した．また，各要素について信頼性係数クロンバックのα係数を算出した．その結果，GISA は 0.763，ISPA は 0.777，PUOP は 0.863，PEOU は 0.775，ATT が 0.738，BI は 0.876，SB は 0.737 であった．次に既存研究の因子との差異を確認した．その結果質問項目と因子に違いが生じていることが分かり，それらの質問項目をはずして，再度信頼性係数を算出したものを表４に示す．一般に信頼性係数は，0.8 以上が望ましいとされているが，ATT， BI, PUOP は 0.8 以上であり，その他の因子も 0.8 に達してはいないが一定の信頼性はある，と考える．これらの質問項目を使い，主因子法，バリマックス回転で因子分析を行い，6 つの因子（GISA， ISPA, PUOP, PEOU, ATT, BI）をそれぞれ確認できた．因子行列を表 5 に示す．

表４　クロンバックのα係数

Table４.　Cronbach's　alpha

	GISA	ISPA	PUOP	PEOU	ATT	BI	SB
数	4	5	4	3	4	5	14
α	0.784	0.777	0.867	0.760	0.847	0.876	0.737

表 5　調査項目の因子パターン行列

Table5　Factor　Analysis matrix

	因子					
	1	2	3	4	5	6
BI03	.818	.108	.115	.194	.074	.058
BI04	.763	.138	.091	.194	.018	-.008
BI01	.750	.185	.304	.148	.120	.053
BI02	.704	.095	.211	.196	-.020	.044
BI05	.593	.181	.224	.087	.107	.012
PUOP03	.153	.838	.179	.098	.074	.126
PUOP02	.192	.781	.205	.185	.105	.085
PUOP01	.159	.638	.150	.162	.030	.125
PUOP04	.175	.582	.328	.218	.124	.120
ATT02	.301	.224	.792	.235	.013	.031
ATT03	.337	.248	.660	.198	.100	.065
ATT01	.201	.257	.632	.146	.044	.020
ATT04	.349	.232	.466	.246	.112	.073
ISPA03	.194	.111	.117	.687	-.001	.075
ISPA01	.140	.083	.109	.540	.078	.023
ISPA04	.086	.160	.250	.528	.333	.111
ISPA02	.226	.208	.155	.517	.083	-.008
ISPA05	.251	.281	.285	.485	.210	.050
GISA04	.013	.108	.092	.050	.792	.125
GISA03	.068	.044	.046	-.018	.760	.143
GISA02	.069	.049	.015	.305	.552	.193
GISA01	.110	.060	.015	.416	.508	.082
PEOU02	.059	.067	.015	.168	.121	.787
PEOU03	.059	.126	.107	.025	.173	.769
PEOU01	-.011	.096	-.002	-.011	.115	.550

因子抽出法: 主因子法

回転法: Kaiser の正規化を伴うバリマックス法

次に，セキュリティ行動（SeBIS 項目）に対して，確認のため因子分析を実施した．[7]の通りに，4 因子が抽出された．因子 1 は，積極的意識（Proactive Awareness）,因子 2 は更新，因子 3 はパスワード生成，因子 4 はデバイスのセキュア化である．ただし，SB04 は，[7]ではパスワード生成因子を構成していたが, 本調査では, 因子負荷量は低かった．表 6 に SeBIS 行動の因子分析結果の因子行列を示す．

表 6　SeBIS の因子パターン行列

Table6 Factor Pattern matrix on SeBIS items

	因子			
	1	2	3	4
SB09	.733	.104	.106	.043
SB10	.682	.034	.103	.127
SB07	.666	.066	-.017	.105
SB14	.608	.069	.083	.042
SB08	.524	-.040	.015	-.012
SB12	.105	.888	.151	.070
SB13	.169	.691	.175	.109
SB11	-.107	.442	.160	.107
SB05	.137	.172	.719	.098
SB06	-.017	.140	.500	.077
SB04	.141	.194	.225	.057
SB02	.060	.015	-.014	.788
SB01	.095	.185	.164	.443
SB03	.065	.113	.256	.320

因子抽出法: 主因子法

回転法: Kaiser の正規化を伴うバリマックス法

6.3 情報セキュリティ行動への影響因子の確認

因子分析の結果より，各因子に対して因子得点を算出し各因子と情報セキュリティ行動（SB）への影響を調査するため， SB 得点の合計を標準化に変換した数値を従属変数とし，独立変数を 6 つの因子として，重回帰分析を実施した．結果を表 6 に示す．

表 6　情報セキュリティ行動への重回帰分析

Table6. Multiple regression analysis on information security behavior

						共線性の統計量	
	非標準化係数	標準誤差	標準化係数 β	T 値	有意確率	許容度	VIF
(定数)	1.657E-15	.048		.000	1.000		
BI	.104	.052	.097	2.019	.044	.991	1.009
PUOP	.146	.052	.134	2.814	.005	.993	1.007
ATT	.156	.054	.139	2.907	.004	.987	1.013
ISPA	.117	.057	.099	2.073	.039	.985	1.016
GISA	.341	.053	.304	6.365	.000	.992	1.008
PEOU	.193	.054	.171	3.580	.000	.994	1.006

a. 従属変数 Z スコア: セキュリティ行動

モデル	R	R2 乗	調整済み R2 乗	推定値の標準誤差
1	.450[a]	.202	.189	.90071503

1%有意であるのは，PUOP, ATT, GISA, PEOU で 5%有意は BI，ISPA であった．独立変数間の多重共線性については, VIF が 10 を超えていないため発生していないとみなせる. モデルの要約度をみると, 調整済み決定係数 R^2 が 0.189 と低い数値であり, 当てはまりは高くはないと考えらえる．

6.4 考察

仮説モデルの検証は今後の分析にゆだねるが，今回の分析の範囲に対しての考察を述べる．

相関分析において，意図（BI）と行動（SB）の相関がほとんどないことが特徴である．セキュリティ対策の実態では,「やらなければならない」と考えていても実際には,「行動」に結びつかないケースが知られている． また，今回利用した SeBIS のセキュリティ行動は，組織におけるセキュリティ行動というよりも，個人の行動を対象としていることが原因の可能性もある．今後の分析で留意が必要と考える．次に，態度（ATT）と意図（BI）間は，相関がみられた．計画的行動理論による「態度は意図」を形成する，を支持していると考えられる．意識のうち，一般的セキュリティ意識（GISA）は，セキュリティポリシー意識（ISPA）と，認知された防御対策の使いやすさ（PEOU）と相関があった．一般的セキュリティ意識がセキュリティポリシー意識と相関があるのは，自明と考えるが，態度（ATT）や意図（BI）間で低い相関となっている．態度や意図と相関があるのは，セキュリティポリシー意識（ISPA）と認知された防御の有用性（PUOP）であった．組織においては，一般的な意識ではなく，具体的な組織のポリシーや実際のセキュリティ対策の有用性のほうが影響が大きいことが推察される．

因子分析では，関連研究の因子を検証的に因子分析を実施した．因子を構成する調査項目はすべて同じとはならなかった．これは，調査対象が異なることも理由のひとつかもしれない．抽出した因子は，すべて関連研究と同じであったため, これらの因子を今後の統計分析に利用していく．

重回帰分析の結果について考察する．有意確率を見ると意図（BI）と情報セキュリティポリシー意識（ISPA）が 5%有意，これら以外は，1%有意となった．全ての因子が正の符号であり，これは以下のように解釈できる．

意図（BI）があるほど，認知された防御の使いやすいほど（PEOU），態度（ATT）があるほど，情報セキュリティポリシーへの意識（ISPA）が高いほど，認知された防御の有用性（PUOP）を感じるほど，そして情報セキュリティ意識（GISA）が高いほど，情報セキュリティ行動をとりやすいことがわかる．標準偏回帰係数 β をみると，最も影響を与えたのが一般的情報セキュリティ意識（GISA）で，順に使いやすさ（PEOU）有用性（PUOP），態度（ATT）であった．相関分析では，相関が弱かった一般的情報セキュリティ意識であったが，他の変数も含めた回帰分析では，有意に影響を与えており，抑制変数の可能性を示していると考えられた．

今回の分析の結果を情報セキュリティ対策推進に役立てるケースを考える．個人への外部からの影響として，まず第一に, 一般的な情報セキュリティ意識を高めるために, 情報セキュリティインシデントに関連するニュースや情報セキュリティ対策の効果などの情報を周知すること. 次に, 情報セキュリティポリシーへの意識，理解を高めることである．具体的には，情報セキュリティ研修において考慮すべきと考える．また，組織の構成員に要請するセキュリティ対策は，使いやすさと有用性を感じさせることが重要である．関連研究では，自己効力感の影響が確認されているが，使いやすさと有用性は，自己効力感に関連していると考える．

最後に調査についてその限界を考察する．調査は，サウジアラビアの公的機関の協力を得て，オンラインで Web のフォームに回答してもらう方法で実施した．しかし，組織の職員全体の年齢や男女別構成について情報を得ることができなかった．このため，サウジアラビアの一般的な労働者を対象としたとみなすことは困難と考える．ただし，395 人という回答者を得ていることから，統計分析においては一定の信頼性を得ることができる．最後に言語の違いについて述べる．本調査は英語の質問項目をアラビア語に翻訳したものを利用した．予備調査で少人数の英語での調査を実施し，アラビア語翻訳時の留意事項などの提示を依頼したが，翻訳による質問の意図の「ぶれ」がある可能性を否定できないことを留意したい．

7. おわりに

情報セキュリティ行動を利用者の技術受容の観点から調査，分析した結果を示した．サウジアラビアの組織の協力を得て，質問紙調査による調査を実施することができた．因子分析の結果から，参考とした関連研究の因子と同じ因子を抽出することができた．因子得点を利用した回帰分析では，各因子が，情報セキュリティ行動へ影響を与えていることが明らかになった．これらの結果をもとに，今後，仮説モデルの検証を予定している．本研究による調査分析が今後のサウジアラビアにおける情報セキュリティ対策推進に役立つことを期待する．

参考文献

[1] JNSA，2018 年 情報セキュリティインシデントに関する調査報告書 https://www.jnsa.org/result/incident/2018.html

[2] Ingham, L. (2018). 88% of UK data breaches caused by human error, not cyberattacks. The Verdict Magazine. https://www.verdict.co.uk/uk- data- breaches- human- error/ .

[3] Ernst, Y., 2018, 2019. Global Information Security Survey, New York. Retrieved 2020-04-25 from https: //assets.ey.com/content/dam/ey-sites/ey-com/en _ ca/topics/ advisory/ey- global- information- security- survey- 2018- 19.pdf Parsons et al:2014

[4] National Cybersecurity Authority (Q42020) Cyber Security Quarterly Bulletin， https://nca.gov.sa/files/qb2020q4_en.pdf

[5] Ahmad Al-Omari,Omar El-Gayar,Amit Deokar,"Security Policy Compliance: User Acceptance Perspective" Hawaii International Conference on System Sciences,2012

[6] Sultan T. Alanazi , Mohammed Anbar , Shouki A. Ebad, Shankar Karuppayah ,Hadeer A. Al-Ani : Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector, Symmetry 2020, Vol12(9), 1544; （online） available from https://doi.org/10.3390/sym12091544 - 18 Sep 2020

[7] Serge Egelman, Eyal Peer：Scaling the Security wall developing a Security Behavior Intentions Scale (SeBIS)， Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ,2015

[8] Nader Sohrabi Safa , Mehdi Sookhak , Rossouw Von Solms , Steven Furnell , Norjihan Abdul Ghani , Tutut Herawan： Information security conscious care behaviour formation in organizations，Elsever, Computers & Security Vol 53, PP 65-78, 2015（online） available from https://www.sciencedirect.com/science/article/pii/S0167404815000863?via%3Dihub

[9] Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat： INFORMATION SECURITY POLICY COMPLIANCE: ANEMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS, MIS Quarterly Vol. 34 No. 3 pp. 523-548/September 2010

[10] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models," Management science, vol. 35, pp. 982- 1003, 1989.

[11] Ajzen, I. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 1991, 50, 179–211.

[12] Gibbs, J.P. Crime, punishment, and deterrence. Southwest. Soc. Sci. Q. 1968, 48, 515–530.

[13] Rogers, R.W. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology: A sourcebook; The Guilford Press: New York, NY, USA, 1983; pp. 153–176.

付録

付録 A.1　質問項目

Id	Questionnaires
General Information Awareness (GISA 01-04) 1Disagree,5agree	
01	Overall, I am aware of the potential security threats and their negative consequences.
02	I have sufficient knowledge about the cost of potential security problems.
03	I follow news and developments about the security related technologies.
04	I read about the problems of malicious threats attacking users' computers.
Information security policy awareness(ISPA01-05) 1Disagree,5agree	
01	I am aware that my organization has a formal policy that forbids employees from installing new software on work on computers.
02	I am aware of my organization's specific guidelines that describe acceptable use of computer passwords.
03	I am aware that my organization has a formal policy that forbids employees from modifying computerized data in an unauthorized way.
04	I understand the rules and regulations prescribed by my organization's ISP.
05	I understand my responsibilities toward enhancing my organization's information system security as prescribed in the organization's ISP
Perceived Usefulness of Protection(PUOP01-04) 1Disagree,5agree	

01	Complying with my organization's ISP saves me time
02	Complying with my organization's ISP improves the quality of the work I do.
03	Complying with my organization's ISP makes it easier to do my job.
04	Overall, I find complying with my organization's ISP useful in my job.
Perceived Ease of Use(PEOU01-03), 1Disagree,5agree	
01	I find that the information security policy at my workplace is inflexible.
02	I find it hard to comply with the requirements of my organization's ISP.
03	I am encountering difficulty in performing the tasks assigned to me, when applying the information security policy in my workplace.
Attitude(ATT01-04), 1Disagree,5agree	
01	I think it is a good idea to follow the information security policy at the workplace.
02	I believe that it is necessary to follow the information security policy at the workplace.
03	I like the idea of following information security policies.
04	For me, compliance with my business' information security policy is beneficial.
Behavioral intention(BI01-05), 1Disagree,5agree	
01	I intend to continue following to the information security policy of my organization.
02	I would follow the organization's security policy whenever possible
03	I intend to protect computers and their peripherals in accordance with the requirements of the information security policy of my organization.
04	I intend to protect my work information in accordance with the requirements of its information security policy.
05	I intend to recommend that others comply with ISP.
Security Behavior(SB01-14), 1Never,2rarely,3Sometimes,4Often,5Always	
01	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
02	I use a password to unlock my computer.
03	I manually lock my computer screen when I step away from it.
04	I do not change my passwords unless I have to.
05	I use different passwords for different accounts that I have.
06	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
07	When someone sends me a link, I open it without first verifying where it goes.
08	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar
09	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)
10	If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
11	When I'm prompted about a software update, I install it right away.
12	I try to make sure that the programs I use are up to date.
13	I verify that my anti-virus software has been regularly updating itself
14	If I receive an e-mail that requires me to respond, I reply without first checking the sending e-mail address.