人はなぜ情報セキュリティ事故を起こすのか

Why do people cause information security incidents?

奥原 雅之 [1*]
Masayuki Okuhara[1*]

[1] 東京都立産業技術大学院大学　Advanced Institute of Industrial Technology
*Corresponding author: Masayuki Okuhara, okuhara-m@aiit.ac.jp

Abstract　Most information security incidents are caused by information technology users' actions that violate procedures and rules. This can be attributed to the risk-taking behavior of information technology users who "dare to act after recognizing the risks" in information technology usage situations. In risk-taking, decisions are made by comparing and contrasting both the utility or disutility of the action and the risk it entails. In order to clarify this mechanism, this paper surveys the extent to which general users evaluate information security-related risks sensibly, and finds that many information security-related risks are evaluated as risks that are almost equivalent to real-world risks.

Keywords　security risk; information security governance; risk-taking; security risk analysis

1　はじめに

情報技術 (IT) が一般社会のインフラとなっている今日において，情報セキュリティ事故の発生もまた日常的に発生している．これらの事故の多くは，IT 利用者のエラー，すなわち失敗によって起きている．情報セキュリティ事故を減少させるためには，このような失敗がどのようにして起こるかを知る必要がある．

我が国の個人情報保護に関しては，一般財団法人日本情報経済社会推進協会 (JIPDEC) プライバシーマーク推進センターが，日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に準拠した「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に基づいて，個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して，その旨を示すプライバシーマークを付与する，プライバシーマーク制度を 1998 年より運用している[1]．プライバシーマークを付与された事業者等は，個人情報の扱いに関する事故が発生した場合は，同センターへの報告が義務付けられている．同センターによれば，プライバシーマーク付与事業者からの個人情報の扱いに関する事故として，2022 年度は 1,460 社から 7,009 件の報告を受けている[2]．このうち，「要配慮個人情報」「財産的被害」「不正の目的」「1,000 人超」のいずれかに該当する「速報」の報告件数は 1,878 件である．

このような事故はなぜ発生するのか．同調査によれば，事故の事象分類ごとの件数は，1 位が「誤配達・誤交付」(43.0%)，2 位が「誤送信」(24.7%)，3 位が「紛失・滅失・既存」(11.2%) となっており，いずれも IT 利用者の人為的なミスやエラーに起因するものである．これは，不正アクセス（6.2%）やマルウェア・ウイルス（1.8%）による事故よりもはるかに多く，これらの上位 3 分類だけで全体の 78.9%を占める．その他，「誤表示」(5.8%) や「誤登録」(4.7%)，「誤廃棄」(1.6%) も含めると，実に全体の 90%以上が何らかの人為的なミスやエラーに起因している．情報セキュリティ事故というと，我々は外部からの攻撃者によるサイバー攻撃やマルウェア感染によるものを連想しがちであるが，実はその大部分が，普段情報を扱う IT 利用者側の失敗に起因しているのである．

さらに，同調査ではこれらの事故の原因についても集計を行っている．一つの発生事象に対して複数の原因が報告される場合があるため，原因別集計の合計は報告件数を上回る 9,663 件となっているが，ここで 1 位となっているのは「手順・ルール違反作業，操作」の 2,803 件であり，全体の 29%を占めている．以下，「作業・操作ミス」2,445 件，「確認不足」1,979 件と続いており，IT 利用者である担当者の人為的な原因によるものが上位 3 位までを占めている．

本稿では，IT 利用者がなぜ情報セキュリティの事故を起こすのかについて，失敗発生のメカニズムに着目して考察し，その判断基準となる要素として，IT 利用者が情報セキュリティに関するリスクをどの程度重要視しているかを明らかにする．

2　失敗が発生するメカニズム

芳賀繁は人間が失敗を犯し事故を起こすメカニズムについて言及している（芳賀，2003）[3]．まず芳賀はヒューマンエラーを「人間の決定または行動のうち，本人の意図に反して人，動物，物，システム，環境の，機能，安全，効率，快適性，利益，意図，感情を傷つけたり壊したり妨げたもの」と定義している[4]．また，エラーの類型として，オミッション・エラー（「やり忘れる」失敗）を「ボケ型」，コミッション・エラー（「やってしまう」失敗）を「ドジ型」と呼んでいる[5]．情報セキュリティ事故の観点で見ると，原因の大部分に「誤」の字がついている．これは事故の原因となった人間が「やらなくてよいことを誤ってやってしまっている」ことを示唆している．事故の原因となる失敗は，ここでいう「ドジ型」が大きく関与していることを伺わせる．

また，芳賀は，ヒューマンエラーにつながる要因である不安全行動に言及している．芳賀は不安全行動を「本人または他人の安全を阻害する意図をもたずに，本人または他人の安全を阻害する可能性のある行動が意図的に行われたもの」と定義している．また，不安全行動とヒューマンエラーとの関係を，「作業者が棚の上の段に置いてある重い部品をおろすときに，作業標準に定められた脚立を設置するのを面倒くさいと思い，背伸びして取ろうとしたところ，部品が落下し足の指を骨折したとする．脚立をつかわず上段のものをおろす行為は，それが成功しようとしまいと『不安全行動』である．しかし，落とすことは意図したものではない．こちらは『ヒューマンエラー』である．」と説明している（芳賀，2003）[6]．前章で見た通り，情報セキュリティに関連する事故の原因の 1 位は「手順・ルール違反作

Received: 2023-10-29; Published online: 2024-02-29

業，操作」であった．これは情報セキュリティにおける「不安全行動」とみるべきであろう．

心理学では，危険を認識したうえであえて行動することをリスクテイキングという．リスクテイキングのプロセスは，「リスクの知覚」「リスクの評価」「意思決定」の 3 つの段階からなる．このうちリスクの評価については，「主観的リスクの大きさは「事故・災害の確率×事故・災害が起きた場合に予想される損失の大きさ」の主観的見積もりである．一般的に男性はリスクを過少視し，女性は過大視する傾向があると言われている」と芳賀は述べている．

さらに，リスクテイキングの意思決定には，リスクの評価以外に，「危険をおかしてでも得られる目標の価値」（効用）と，「リスクを回避するための行動が手間がかかったり，コストがかかったり，できれば避けたいものであったりする」（不効用）が作用することも同時に芳賀は指摘している[7].

情報セキュリティの場面でも，決められた規則やルールを守らないことの動機として，これらの効用と不効用が作用していることが想定できる．例えばメールを誤送信する場合，送信先を慎重に確認しないことは，確認することによるコストを避けるため（不効用）であろうし，ファイルを暗号化せずに送付することは，単純にファイルを相手方と共有するというメリットを優先した（効用），あるいは安全な暗号化のプロセスを踏むためのコストを回避した（不効用）によるものと見ることができる．このようなアプローチにより，「なぜ IT 利用者は情報セキュリティルールを守らないのか」についてを理解することも可能かもしれない．

では，IT 利用者は，これらの効用あるいは不効用と比較較量するべき情報セキュリティに関するリスクをどのように見ているのであろうか．本稿では，主な情報セキュリティに関連するリスクと，それ以外の実世界に関連するリスクについて，それぞれどの程度の大きさを持っているかについてアンケート調査し，「世間が情報セキュリティリスクをどの程度深刻に考えているか」を明らかにする．

3 アプローチ

情報セキュリティに関するリスクを定量的に扱うための手法として，事故の発生頻度や情報資産の価値を対数スケールで扱うことがよく行われる．例えば発生頻度を「1 年に 1 回」「10 年に 1 回」「100 年に 1 回」というように，10 倍ごとのスケールで類別する方法である．いわゆるコートニーの方法[8]がこの手法を採用している．これは，正確な定量化が難しいセキュリティ事故の発生確率や事故による被害金額の算定について，その大きさを対数スケールで捉えることにより，一般的に使いやすい形でリスク分析を可能にするための工夫である．今回の調査でも，この考え方に従い，質問の選択肢は 10 倍ごとの対数スケールとなるように設計した．また，リスクの発生頻度は比較的簡単に表現できるが，リスクによる被害の大きさ（情報セキュリティの文脈では情報の資産価値に相当する）は，回答者がイメージすることは難しい．そこで，本調査では，「そのリスクを回避する手段がもしあればいくら払うか」という，リスク回避のコストを問うことで，被害の大きさを代用することとした．

今回のアンケート調査では，回答者が出会う可能性がある各種のリスク 18 種について，「どの程度そのリスクに遭う可能性があるか」（頻度），「そのリスクを回避できる手段があるとすればどの程度まで出費できるか」（価値）の 2 点について尋ねる．質問したリスクは表 1 の通りである．ここで ID の 1 から 7 までは情報セキュリティ分野とは直接関係しない実生活のリスク，8 から 18 は情報分野に関係するリスクを挙げている．

表 1　調査対象のリスク

ID	ラベル	質問文
1	財布紛失	外出中に大事なもの（財布など）をなくす
2	交通事故	道を歩いていて交通事故に遭う
3	火災	自宅や普段いる場所（職場・学校など）で火災に遭う
4	大地震	自分が住んでいる土地で大地震が起こる
5	自然災害	自宅に被害が出るレベルの自然災害（台風など）に遭遇する
6	戦争	住んでいる国（日本）が武力紛争（戦争など）に巻き込まれる
7	実世界詐欺	実世界での詐欺（対面，電話などによるもの）に遭う
8	ネット詐欺	ネット上の詐欺（メール，SNS などによるもの）に遭う
9	個人情報漏えい	自分が利用している製品・サービスの提供企業から自分の個人情報が漏えいする
10	個人情報盗難	自分の個人情報がネット上で盗まれる
11	個人情報被害	盗まれた自分の個人情報で金銭的被害が発生する
12	ウイルス感染	自分が使っている情報デバイス（PC やスマホ）がコンピュータウイルスに感染する
13	アカウント乗っ取り	自分のインターネットサービスのアカウントが他人に乗っ取られる
14	データ消失	自分が使っている情報デバイス（PC やスマホ）が壊れてデータが消失する
15	ランサムウェア	自宅や職場などの PC にランサムウェア（身代金を要求するウイルス）が侵入する
16	サイバー攻撃	自分の PC やネットワークが高度な技術を持つサイバー攻撃者に直接攻撃される
17	パスワード推測	自分のパスワードを他人に当てられる
18	メール誤送信	大事な情報を記載したメールを間違って他人に送る

これら 18 個のリスクについて，「頻度」「価値」ごとに大きさを回答するように回答者に依頼する．「頻度」の質問項目は表 2,「価値」の質問項目は表 3 である．

表 2　頻度に関する質問．質問文：「以下の出来事について，あなた自身はどの程度の確率で遭遇すると思いますか．もっとも近いものを一つ選んでください．」

質問種別	選択肢
頻度	1: よく起こる（年に数回）
	2: たまに起こる（3 年に 1 回ぐらい）
	3: めったに起こらない（一生に 1 度か 2 度）
	4: ほぼ確実に起こらない（多分自分の人生では出会わない
	5: 無回答（答えたくない・質問の意味がわからないなど）

表 3　価値に関する質問．質問文：「前の質問の出来事を防ぐことができたり，その危険性を回避することができる商品（製品・サービス）がもしあったとしたら，あなたはいくらぐらいなら購入を考えますか．」

質問種別	選択肢
価値	1: 千円ぐらい
	2: 一万円ぐらい
	3: 十万円ぐらい
	4: 百万円ぐらい
	5: 一千万円ぐらい
	6: あてはまるものはない

この他，回答者の属性として職業と，性別，年齢（20 歳から 70 歳まで 5 歳刻み）を質問項目として設定している．なお，今回利用したアンケート調査サービスの仕様上，回答者の住所（都道府県単位）と，回答に使用したデバイス（PC かスマホか）も情報として取得しているが，本分析ではこれらの情報は使用していない．

調査はインターネット調査サービス「Questant」を利用し，回答者募集は同サービスのオプションである「Japan Cloud Panel」による回答者募集サービスを利用した．調査期間は 2023 年 8 月 19 日から 8 月 23 日，有効回答数は 447 名である．

4　調査結果

集計

本アンケート調査の回答者の属性は表 4 の通りである．

表 4　回答者の属性．

設問	選択肢	回答数	比率 (%)
年令	~19	3	0.7
	20~24	6	1.3
	25~29	8	1.8
	30~34	31	6.9
	35~39	25	5.6
	40~44	45	10.1
	45~49	51	11.4
	50~54	42	9.4
	55~59	65	14.5
	60~64	56	12.6
	65~69	36	8.1
	70~	79	17.7
性別	男	281	62.9
	女	166	37.1
職業	公務員	8	1.8
	経営者・個人事業主（自営業）	53	11.9
	会社員・職員（正規雇用）	128	28.6
	会社員・職員（非正規雇用）	57	12.8
	専業主婦（主夫）	86	19.2
	学生	5	1.1
	その他	110	24.6

本アンケート調査の主な要素は，18 個のリスクに対する「頻度」と「価値」である．回答から「無回答」に相当する回答を除外して単純平均を取った結果を見てみよう．ここで，回答の選択肢が対数スケールであったことに留意する必要がある．すなわち，この結果で数値に 1 の差があるということは，回答者は 10 倍に相当する頻度または価値の差があると認識しているということを意味する．

表 5　リスクの頻度に対する回答の平均値．

順位	ID	ラベル	mean
1	9	個人情報漏えい	2.902
2	10	個人情報盗難	3.038
3	14	データ消失	3.054
4	12	ウイルス感染	3.085
5	1	財布紛失	3.133
6	5	自然災害	3.157
7	4	大地震	3.197
8	8	ネット詐欺	3.237
9	13	アカウント乗っ取り	3.262
10	17	パスワード推測	3.313
11	18	メール誤送信	3.347
12	15	ランサムウェア	3.378
13	11	個人情報被害	3.380
14	16	サイバー攻撃	3.423
15	7	実世界詐欺	3.450
16	2	交通事故	3.452
17	3	火災	3.600
18	6	戦争	3.763

表 5 は，頻度に対する回答の平均値を，昇順にソートしたものである．頻度において一番数値が低かった（つまり自分の身の回りで起こる可能性が一番高いと評価された）のが「個人情報漏えい」，２番目が「個人情報盗難」である．以降，「データ

消失」,「ウイルス感染」と続き，5 位にはじめて情報セキュリティ以外のリスクである「財布紛失」が入る．一方，数値が最も高かった（つまり自分の身の回りで起こる可能性が一番低いと評価された）ものは「戦争」で，2 番目が「火災」である．ID の 9 から 18 までが情報セキュリティに関するリスクであるが，平均値は 3.0 の周囲におおむね収束しており，「交通事故」や「実世界詐欺」とほぼ同じレンジにある．今回の調査の回答者は，情報セキュリティに関するリスクについては，ある程度「現実にありうるリスク」という評価をしていることがここからわかる．ちなみに，2022 年の交通事故発生件数は全国で 300,839 件[9]，同じく 2022 年の全国の総出火件数は 36,375 件である[10]．また，2022 年の詐欺の認知件数は 33,353 件であった[11]．これらの事案は必ずしも一案件が一被害者となるわけではないので，一般人が認知する発生頻度と一致するものではないが，それでも火災や詐欺よりも 1 桁発生件数が多い交通事故に対して，今回の回答者が同程度のリスクと考えていることは興味深い．

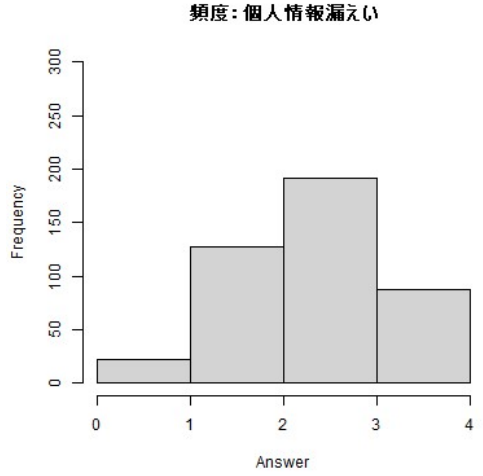

図 1　　個人情報漏えい（ID=9）のヒストグラム

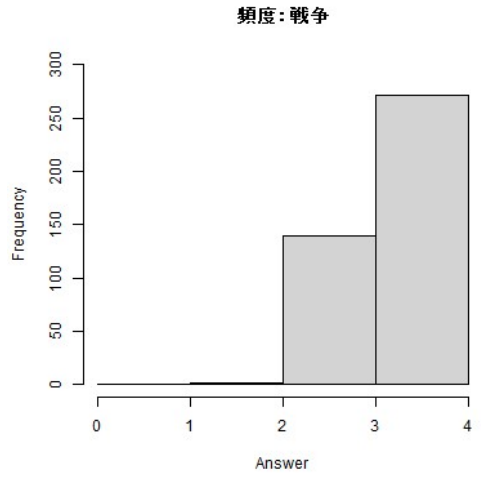

図 2　　戦争（ID=6）のヒストグラム

各回答の分布は，おおむね正規分布に近い，なだらかな分布を示した．ここでは，平均値が最も低かった「個人情報漏えい」と，最も高かった「戦争」についての回答のヒストグラムを参考として図 1 および図 2 に示す．なお，選択肢 5 の「無回答」は図から除外している．

表 6 は，価値に対する回答の平均値を，降順にソートしたものである．一番数値が高かった（つまり回避できるならば高いコストを払ってもよい）のは「戦争」であり，以下「メール誤送信」「大地震」「自然災害」と続く．「戦争」「大地震」「自然災害」などは，回答者自身の努力で回避できる余地がほとんどなく，またその被害が自分だけではなく社会全体に及ぶことなどから，高いコストを払っても回避できるならば回避したいという意思からの結果と推定できる．これらの中に「メール誤送信」が入っていることは興味深い．メールの誤送信は身近なリスクでありながら，効果的な回避手段がないことを反映しているのかも知れない．一番数値が低かった（つまり回避のために高いコストを払えないとした）のは順に「ウイルス感染」「個人情報被害」「データ消失」であった．これらは例えばウイルス対策ソフトなど，すでに確立した対策ソリューションが市場にあるため，それらと同等のコスト感覚が一般に定着していることが要因として考えることができる．

表 6　　リスクの価値に対する回答の平均値．

Rank	ID	label	mean
1	6	戦争	4.060
2	18	メール誤送信	3.557
3	4	大地震	3.539
4	5	自然災害	3.461
5	17	パスワード推測	3.391
6	1	財布紛失	3.365
7	3	火災	3.365
8	7	実世界詐欺	3.362
9	2	交通事故	3.351
10	16	サイバー攻撃	3.349
11	15	ランサムウェア	3.313
12	9	個人情報漏えい	3.302
13	8	ネット詐欺	3.273
14	10	個人情報盗難	3.262
15	13	アカウント乗っ取り	3.233
16	14	データ消失	3.168
17	11	個人情報被害	3.154
18	12	ウイルス感染	3.114

今回の調査では，「頻度」と「価値」の二つの指標を対数スケールに基づく選択肢で調査している．このため，二つの指標を算術的に加算することは，実際の評価値の積を求めることと同じ意味を持つ．そして，コートニーの方法がそうであったよう

に，一般に事象が発生する場合のリスクの大きさは頻度と価値の積で示されることが多い．これらの点を踏まえれば，「頻度」と「価値」の和は，回答者が考えているリスクの大きさを示す指標となることが期待できる．今回の調査では，頻度と価値のスケールが逆向き（頻度は数値が小さい方がリスクが高く，価値は数値が大きい方がリスクが高い）ので，便宜上頻度の符号を逆転し，「価値 - 頻度」の数値を計算することで，回答者が考えるリスクの大きさを評価する．この値（表中 score で示す）を降順にソートした結果を表 7 に示す．

表 7　頻度と価値に基づくリスクの大きさの評価．

Rank	ID	label	score
1	9	個人情報漏えい	0.400
2	4	大地震	0.342
3	5	自然災害	0.304
4	6	戦争	0.297
5	1	財布紛失	0.232
6	10	個人情報盗難	0.224
7	18	メール誤送信	0.210
8	14	データ消失	0.114
9	17	パスワード推測	0.078
10	8	ネット詐欺	0.036
11	12	ウイルス感染	0.029
12	13	アカウント乗っ取り	-0.029
13	15	ランサムウェア	-0.065
14	16	サイバー攻撃	-0.074
15	7	実世界詐欺	-0.088
16	2	交通事故	-0.101
17	11	個人情報被害	-0.226
18	3	火災	-0.235

この結果，「個人情報漏えい」が最も大きなリスク評価となった．その後，「大地震」「自然災害」「戦争」などの，実世界の特に人命に係わるリスクが続いている．全体的には情報セキュリティ関連のリスクは下位に集中していることが見て取れる．

分析

ここからは，回答者の属性によるグループごとに，回答の平均値に差があるかどうかを検証する．表 8 に，各回答に対する性別ごとの平均値と，その差に対する t 検定の結果を示す．なお，これ以降の検定においては，分析を簡便とするため，すべてデータ分布の正規性を前提としないノンパラメトリック検定を使用する．t 検定の算出には R 言語（version 4.3.1）に組み込みの t.test 関数および pairweise.t.test 関数を使用した．

頻度に対する設問のうち，「データ消失」「ランサムウェア」の 2 問について，平均値の差が 1%有意となった．また，「ウイルス感染」「サイバー攻撃」の 2 問については，平均値の差が 5%有意となった．これらはすべて女性の方が，男性よりもより高い平均値となっている．それ以外の設問でも一般に女性の方が男性よりも高い平均値となっており，男性の方が高かったものは「実世界詐欺」のみであった．前出の芳賀の著作では男性の方がリスクを過少視する傾向があると述べていたが，ここでは男性の方が一般的にリスクの発生頻度を高く評価していることになる．ただし，有意差が観測された設問はいずれも情報技術に関連するリスクであることから，男性と女性では情報技術に対する意識や理解の差が影響している可能性もある．

また価値に対する設問のうち，「財布紛失」「個人情報漏えい」「ウイルス感染」「メール誤送信」の 4 問について，平均値の差が 5%有意となった．これらを含め，価値に関する設問ではすべての設問で女性の平均値が男性を上回っていた．「お金で解決できるならリスクを回避したい」という指向性は，男性よりも女性の方が高いのかも知れない．

次に，職業グループごとの各質問の平均値に有意な差があるかを調べてみる．職業グループは「その他」を含め 7 グループあるため，各グループ間の平均値の差についてボンフェローニ補正を用いた多重 t 検定を行った．この結果，ほとんどすべての組み合わせで平均値に有意な差はなかった．この中で，比較的 p 値が低かった（0.1 以下であった）設問と職業グループの組み合わせを表 9 に列挙する．職業グループ 6（学生）が他のグループと有意差を生じやすい傾向は見て取れるが，このグループはそもそも絶対数が少ない（全回答者の 1.1%）ので，そのことが結果に影響していると考える方が自然であろう．これを踏まえれば，各種リスクの評価について，回答者の職業はほとんど影響を与えていないと評価してよいであろう．

表 9　各回答の平均値の差が大きかった職業グループの組み合わせと多重 t 検定の結果．p 値のうち，0.05 以下のものには「*」，0.01 以下のものには「**」を付している（以降の表も同様）．

ID	ラベル	職業グループ	p 値
P1	頻度：財布紛失	1, 6	0.0341*
		2, 6	0.0162*
		3, 6	0.0050**
		4, 6	0.0077**
		5, 6	0.0014*
		6, 7	0.0261*
P4	頻度：大地震	5, 6	0.043*
		6, 7	0.093
P15	頻度：ランサムウェア	3, 5	0.081

最後に，年齢と各質問の平均値に有意な差があるかどうかを調べてみる．年齢は 5 歳間隔で細かく層別されているが，この粒度で有意な差があることは期待できないため，表 10 に示す 15 歳ごとの間隔で 4 個のグループに再編成して分析することとした．なお，世代名はマーケティングに関する世代を参考に便宜上付与したもので，公式なものではない．

これらの 4 グループに対して，職業グループの分析と同様に，各グループ間の平均値の差についてボンフェローニ補正を用いた多重 t 検定を行った．この結果，すべての組み合わせで平均値に有意な差はなかった．本調査においては，年齢によるリスクの大きさの評価の違いは観測されなかったと言ってよい．

表 8　リスクの頻度に対する回答の平均値の男女の比較と，平均値の差に対する Welch の t 検定の結果.

ID	ラベル	Means:男性	Means:女性	t	df	p 値	
P1	頻度：財布紛失	3.10989	3.17284	-0.89485	328.56	0.37150	
P2	頻度：交通事故	3.423488	3.5	-1.3067	356.02	0.19220	
P3	頻度：火災	3.587189	3.620482	-0.57904	345.21	0.56290	
P4	頻度：大地震	3.160142	3.259036	-1.5466	317.2	0.12300	
P5	頻度：自然災害	3.124555	3.210843	-1.2439	333.75	0.21440	
P6	頻度：戦争	3.75089	3.783133	-0.55121	325.41	0.58190	
P7	頻度：実世界詐欺	3.451957	3.445783	0.083614	294.23	0.93340	
P8	頻度：ネット詐欺	3.213523	3.277108	-0.71092	304.18	0.47770	
P9	頻度：個人情報漏えい	2.839858	3.006024	-1.7776	305.16	0.07646	
P10	頻度：個人情報盗難	2.992883	3.114458	-1.3595	310.59	0.17500	
P11	頻度：個人情報被害	3.338078	3.451807	-1.4967	309.78	0.13550	
P12	頻度：ウイルス感染	3.007117	3.216867	-2.5122	327.02	0.01248	*
P13	頻度：アカウント乗っ取り	3.220641	3.331325	-1.4141	313.27	0.15830	
P14	頻度：データ消失	2.960854	3.210843	-2.9923	323.05	0.00298	**
P15	頻度：ランサムウェア	3.295374	3.518072	-2.7891	313.25	0.00561	**
P16	頻度：サイバー攻撃	3.359431	3.53012	-2.2803	358.37	0.02318	*
P17	頻度：パスワード推測	3.27758	3.373494	-1.1937	327.13	0.23350	
P18	頻度：メール誤送信	3.291815	3.439759	-1.8561	320.54	0.06436	
V1	価値：財布紛失	3.156584	3.716867	-2.4911	328.75	0.01323	*
V2	価値：交通事故	3.217082	3.578313	-1.7111	328.16	0.08801	
V3	価値：火災	3.241993	3.572289	-1.5609	329.9	0.11950	
V4	価値：大地震	3.455516	3.680723	-1.1006	330.05	0.27190	
V5	価値：自然災害	3.380783	3.596386	-1.0458	333.89	0.29640	
V6	価値：戦争	3.932384	4.277108	-1.7108	355.84	0.08800	
V7	価値：実世界詐欺	3.227758	3.590361	-1.6322	331.13	0.10360	
V8	価値：ネット詐欺	3.185053	3.421687	-1.0536	331.63	0.29280	
V9	価値：個人情報漏えい	3.24911	3.391566	-0.62956	331.85	0.52940	
V10	価値：個人情報盗難	3.177936	3.403614	-1.0017	332.55	0.31720	
V11	価値：個人情報被害	2.967972	3.46988	-2.2793	328.12	0.02329	*
V12	価値：ウイルス感染	2.950178	3.391566	-2.0008	324.97	0.04625	*
V13	価値：アカウント乗っ取り	3.096085	3.463855	-1.6389	327.15	0.10220	
V14	価値：データ消失	3.042705	3.379518	-1.5313	330.92	0.12660	
V15	価値：ランサムウェア	3.174377	3.548193	-1.6738	333.07	0.09511	
V16	価値：サイバー攻撃	3.199288	3.60241	-1.804	333.21	0.07213	
V17	価値：パスワード推測	3.245552	3.638554	-1.7434	335.44	0.08218	
V18	価値：メール誤送信	3.377224	3.861446	-2.0955	336.33	0.03687	*

参考までに，比較的平均値の差が大きかった（p 値が低かった）年齢グループの組み合わせを表 11 に示す.

表 10　年齢グループの定義.

ID	年齢層	世代名	回答者数
1	~39	ゆとり世代	73
2	40~54	ロスジェネ世代	138
3	55~69	バブル世代	157
4	70~	ブーマー世代	79

表 11　各回答の平均値の差が大きかった年齢グループの組み合わせと多重 t 検定の結果.

ID	ラベル	年齢グループ	p 値
P2	頻度：交通事故	2, 3	0.03
V2	価値：交通事故	1, 3	0.33
V3	価値：火災	1, 2	0.50
V14	価値：データ消失	3, 4	0.45
V15	価値：ランサムウェア	1, 3	0.57
		3, 4	0.31

考察

本調査の主な目的は，情報関連のリスクは，他の実世界のリスクと比べてどの程度の大きさで評価されているかを知ることであった．表 7 に示されているように，大部分の情報関連リスクは，実世界リスクの間に挟まれた中位グループを形成することがわかった．特に，多くの人が一般的なリスクとして認識している「交通事故」や「火災」よりも，情報関連のリスクの方を大きなリスクとして捉えていることは特筆するべきであろう．

また，リスクの評価については，男女の間については一部有意な差が見られたものの，職業や年齢についてはほとんど有意差は見られなかった．男女間の差については，性別による性格的な要因があるかもしれないが，男女において普段の情報システムや情報デバイスの接し方に差があることが影響している可能性もある．

ここで,「なぜ IT 利用者は情報セキュリティルールを守らないのか」について考えてみよう．IT 利用者が決められた情報セキュリティの規則やルールを守らないことの動機として，その行動による効用と不効用が作用しているとすれば，そこには効用または不効用とリスクとの比較較量があったはずである．実際に事故が起こっているとすれば，効用・不効用を過大評価したか，あるいはリスクを過小評価したかのいずれかである．ところで情報セキュリティの規則を守らないことによる効用・不効用の大きさは，多くの場面で明確である．例えばファイルの暗号化のルールを守らないで，平文のまま送信するのは，単にその手間を節約するためであり, IT 利用者にとってその効用はほぼ明らかである．従って，比較較量の判断に誤りがあったとすれば，リスクを過小評価していることが主な原因であると考えられる．

本調査の結果，IT 利用者は情報セキュリティリスクを，「交通事故」や「火災」よりも大きなリスクと捉えていることが明らかになった．利用者は決して情報セキュリティ事故を「自分の身には絶対起こらないリスク」とは捉えていないか，あるいは「自分だけは交通事故に遭うことはない」と確信しているかのいずれかである．このどちらが正しいかは今回の調査ではわからないが，「情報セキュリティ関連のルールは，交通ルールと同程度には守られる（あるいは守られない)」と考えるのがおそらく合理的なのだろう．

5　おわりに

本稿では，主な情報セキュリティに関連するリスクと，それ以外の実世界に関連するリスクについて，それぞれどの程度の大きさを持っているかについてアンケート調査を実施し，「世間は情報セキュリティリスクを現実世界とほぼ同等に深刻に考えている」ということを明らかにした．ただし，本調査において「価値」の指標とした質問項目は，実際の被害の大きさそのものではないため，結果が正確にリスクの大きさを反映しているかは議論の余地がある．

また，今回の分析ではリスクの評価値が回答者の属性によってほとんど差が出なかった．この点については，よりよい属性の定義によって，有意差が得られるような調査とするための改良の余地があると考えられる．

さらに，今回の結果に対して，なぜ回答者がそのように考えたかについては情報がまったくないため，今後の取り組みとして, IT 利用者がどのようなメカニズムでリスクの大きさを評価しているかについて調べることも必要であろう．

参考文献

1. 一般財団法人日本情報経済社会推進協会，プライバシーマーク制度. [cited 2023]. Available https://privacymark.jp/system/about/outline_and_purpose.html
2. 同, 2022 年度 個人情報の取扱いにおける事故報告集計結果. [cited 2023]. Available https://privacymark.jp/system/reference/pdf/2022JikoHoukoku_230802.pdf
3. 芳賀繁，失敗のメカニズム 忘れ物から巨大事故まで，角川ソフィア文庫, 2003
4. 同, p.43.
5. 同, p.86.
6. 同, p.148.
7. 同, p.150.
8. R. H. Courtney, JR., “Security risk assessment in electronic data processing systems”, National Computer Conference pp. 97-104, 1977.
9. 公益財団法人交通事故総合分析センター，交通事故発生状況. [cited 2023]. Available https://www.itarda.or.jp/situation_accidents
10. 総務省消防庁，消防統計（火災統計）. [cited 2023]. Available https://www.fdma.go.jp/pressrelease/statistics/
11. 法務省，犯罪白書. [cited 2023]. Available: https://hakusyo1.moj.go.jp/jp/69/nfm/n69_2_1_1_1_1.html