「マルチメディア，分散，協調とモバイル
(DICOMO2021)シンポジウム」 令和3年6月-7月

テレワークにおけるセキュリティ等への不安に関する分析*
～ニューノーマルに向けた示唆～

森淳子[1] 小山明美[1] 小川隆一[1] 竹村敏彦[2]

概要： 新型コロナウイルス感染症拡大防止のため，テレワークやオンラインツールなどを活用する企業の数が急増し，現在もテレワークを継続している企業は多数存在している．しかしながら，本来であればこれらの導入前に十分に検討すべきセキュリティ対策やルールの策定が後回しになったケースも少なくなく，テレワーク環境を狙ったセキュリティ・インシデントも報告されている．本研究では，2020 年 11 月に独立行政法人情報処理推進機構が 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」の一環として実施した個人を対象としたウェブアンケート調査の結果から，テレワークを実施する上で個人が感じるセキュリティに関する不安（インシデントが発生した場合にどのような問題が発生するか）と回答者属性（個人属性及びその個人が所属している企業属性）の関係についての多重コレスポンデンス分析を行った．その結果、セキュリティ・インシデント発生時の対応に不安を感じているのは「勤務地が首都圏以外」および「テレワークの実績が浅く実施頻度が低い場合」であることなどを明らかにした．

An Analysis on Anxiety toward Security in Telework: Suggests for the New Normal Era

JUNKO MORI[1] AKEMI KOYAMA[1] RYUICHI OGAWA[1]
TOSHIHIKO TAKEMURA[2]

1. はじめに

新型コロナウイルス感染症拡大防止のため，2020 年 4 月，特別措置法に基づき我が国史上初の緊急事態宣言が出され，約 2 か月間に及ぶ外出自粛が余儀なくされた．その中で，政府は出勤者数の 7 割削減を目指すとの考えを示し，また長期間の外出自粛の中でも事業を継続させるため，職場以外の環境での「テレワーク（在宅勤務，モバイル勤務，サテライトオフィス勤務）」やインターネットを介してのコミュニケーション（オンライン会議，オンライン面接）に取り組む組織が急増した．このような新しいワークスタイルや IT の活用方法は，ニューノーマルと言われ，緊急事態宣言の解除後も新型コロナウイルス感染リスクだけでなく，働き方改革等の以前から求められてきた課題の対策としても有効となると考えられている．2021 年 1 月には第 2 回目の緊急事態宣言が出され，コロナ禍の収束が見通せない状況であることからも，今後このような新しいワークスタイルや IT の活用方法は継続する可能性が高い．一方，これらの対策実施のために行われた急速な ICT 環境の整備は，業務継続を優先したため，セキュリティ対策については利用者個人にまかされてしまっている（本来であればこれらの導入前に十分に検討すべきセキュリティ対策やルールの策定が後回しになっている）ことも多く，十分とは言えない．また，緊急事態宣言解除後に，これらについて企業が検証・再検討を行ったかについては明らかではない．

ニューノーマルでも安全に事業を継続するためにはルール作り，端末・ネットワークのセキュリティ対策等を利用と並行して進めざるを得ない．

独立行政法人情報処理推進機構（IPA）が 2021 年 1 月に公開した「情報セキュリティ 10 大脅威 2021」[1]では，「テレワーク等のニューノーマルな働き方を狙った攻撃」が組織への脅威として初登場し，3 位にランクインしている．実際に，組織内部ネットワークにリモートアクセスを行うために利用される VPN 製品の既知の脆弱性を突き，取得した認証情報がインターネット上に流出[2]，在宅勤務中に社用 PC から SNS に接続したことにより PC がウイルス感染し，その PC を社内ネットワーク接続したことで社内にウイルス感染被害が拡大[3]，ウェブ会議ツールの脆弱性により，非公開の会議に不正アクセスが発生[4]などのセキュリティ・インシデントも報告されている．これらの原因としては，急激なワークスタイルの変化に対する企業・組織

* 本研究の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

1 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

2 城西大学
Josai University

ならびに個人の対応・対策が十分なものでなかったことが考えられる．

テレワーク業務においては，緊急事態宣言以前からテレワークを導入していた組織と，緊急事態宣言を受けて急遽テレワークを導入した組織があり，さらに，テレワークを行う際に利用する PC やスマートフォンなどの端末が組織から貸与されているケースと，個人が所有する端末を使用（Bring Your Own Device）するケースがあり、テレワークといえどもも様々なタイプがある．

緊急事態宣言以前からテレワークを導入しており端末を組織が貸与しているケースでは，ウイルス感染防止や情報漏洩防止などの対策の実施やルールの策定に加え，従業員がテレワークの経験があることから，通常と変わらずセキュリティ対策も意識した上で業務を行えていたことが考えられる．しかしながら，緊急事態宣言以前にテレワークの導入をしていなかった組織は業務継続を優先するため急遽テレワーク可能な ICT 環境を整備する必要が生じて，BYOD でのテレワークを実施せざるを得なかったケースも少なからずあると思われる．このケースでは，ルールの取り決めが無い状況で BYOD の機器のセキュリティ対策が従業員個人に任されてしまっている場合も多い．

また，物理的なオフィスに出社しての業務の場合，不明点や不安に思った事などを相談しやすい環境にあるが，テレワークの場合，電話やメール，チャット等の手段を用いる必要があり，気軽に聞く事が難しく孤立した状況で業務を実施せざるを得ない場合が多い．

テレワーク環境におけるセキュリティ対策は，セキュリティ・インシデントを発生させないようにするための対策を十分に行うことも重要であるが，セキュリティ・インシデントが発生した場合，迅速に適切な対応を実施しないと被害が拡大してしまう恐れがある．セキュリティ・インシデントが発生した場合，どのように対処する必要があるのか，誰にどのように連絡すべきなのかなどについて，個人が都度確認しながら対応するのではなく，誰でも同じ対応がとれる対策や，（テレワーク中で周囲に確認や相談ができる人が居ない場合でも）何をすれば良いか迷わないように準備しておき，個人がセキュリティ・インシデント発生時の対処を理解した上で作業を実施することが重要である．

一般的に、テレワークにおけるセキュリティ対策は組織が十分に行うことに加えて，個人としても適切なセキュリティ行動をとるとともに，平時よりもより高いセキュリティ意識を持つことが求められる．しかしながら，このことは容易ではないことが簡単に想像できる．

本研究では，IPA が 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」[5]の一環として実施した個人を対象としたウェブアンケート調査[6]を用いて，テレワークを実施する上で個人が感じるセキュリティに関する不安（インシデントが発生した場合にどのような問題が発生するか）とアンケートの回答者の属性（個人属性や所属企業の属性等）の関係についてのデータ分析を行う．また，このデータ分析結果を踏まえて，ニューノーマルでセキュアな働き方などについての示唆を与えたい．

本研究の構成は以下の通りである．第 2 節で，本研究で用いるアンケート調査の内容を説明するとともに，本アンケート調査結果の概要を説明する．第 3 節で多重コレスポンデンス分析の結果と考察を行う．最後に，第 4 節で本研究のまとめを行う．

2. アンケート調査

2.1 調査概要

IPA では 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」[5]を実施した．この調査の目的は，ICT 環境をはじめとしたニューノーマルへの対応に伴う変化により，IT サプライチェーンの情報セキュリティ対策にどのような影響が生じているのかを確認するとともに，新たな情報セキュリティ上のリスクについての認識や対応の実態から，ニューノーマルにより生じた課題の整理と対策の方向性を示すことである．この調査では，2020 年 11 月 2 日から 11 月 13 日にかけて個人を対象としたウェブアンケート調査，2020 年 11 月 18 日から 12 月 11 日にかけて企業・組織を対象とした郵送調査とウェブアンケート調査を併用したもの，2020 年 10 月 6 日から 2021 年 2 月 16 日にかけてインタビュー調査をそれぞれ実施している．本研究では，この中で，個人を対象としたウェブアンケート調査（以下，「テレワーク調査（個人編）」と称す）を取り上げた分析を行っていく．「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」の概要など（単純集計などを含む）については文献[5]を参照されたい．

「テレワーク調査（個人編）」の対象者は国内に居住する 18 歳以上の IT 企業・組織の従業員，IT 企業・組織以外の IT 担当者である．これらの個人を調査対象とした理由は，IT 環境や働き方の変化，セキュリティの意識や脅威の変化，今後想定される情報セキュリティリスク等についてどのように考えているかの実態把握を行うためである．このため，「個人調査」では，個人属性や所属する企業属性に加えて，企業の IT 環境や働き方に関する状況，セキュリティの意識や脅威に対する心理的状況について質問を行っている（スクリーニング設問が 5 問，本調査設問が 42 問である）．「テレワーク調査（個人編）」の最終的な回答者（有効回答者）数は，2,372 人である．なお，「テレワーク調査（個人編）」は 2020 年 11 月時点の状況を表しているものであり，現在では状況が大きく変わっている可能性があることを断っておく．

以下，本研究と関連する質問項目（テレワークを実施す

る上で個人が感じるセキュリティに関する不安など）に関する回答結果の概況を紹介する．これらの質問項目以外については文献[5,6]を参照されたい．

2.2 質問項目と概況

(1) 企業のテレワークの導入状況

「テレワーク調査（個人編）」では，2020 年 10 月 31 日時点の（所属している）企業のテレワーク導入・実施状況について質問している．その結果，全体の約 59%の回答者（1,396 人）が会社として実施中と回答している．また，この時点ではテレワークが行われていなかったが，過去にテレワークが導入されていたことがあると回答した割合は全体の約 17%であり，これらを含めるとテレワーク導入・実施状況（テレワークを一度でも導入したことのある企業の割合）は全体の約 76%に及ぶ．これらの回答者にテレワークの導入時期をあわせて質問したところ，「(1 回目の）緊急事態宣言前（2020 年 4 月 6 日以前)」と回答した割合は 42.7%，「緊急事態宣言中（2020 年 4 月 7 日～5 月 25 日)」と回答した割合は 50.5%，「緊急事態宣言解除後（2020 年 5 月 26 日以降)」と回答した割合は 6.8%であり，十分な準備ができずに業務環境の変化に対応せざるをえなかったことがわかる．この状況を鑑みると，テレワークに潜む様々なリスクに対するセキュリティ対策（技術的対策ならびにマネジメント対策（運用に向けたルール作りなど))を考慮できていないことが示唆される．

テレワークを 2020 年 10 月 31 日時点で会社として実施中と回答した回答者（1,396 人）に対して，本人のテレワークの実施頻度について質問したところ，5 割強の回答者が「週 3 回以上のテレワークを実施している」と回答しているa．また，テレワークを週 1 回以上実施している回答者にその（主たる）実施場所について質問したところ 99.4%が「自宅」と回答している．このことから自宅で十分なセキュリティ対策がなされていない場合，テレワーク環境が新

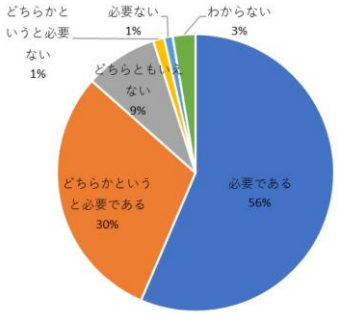

図 1：テレワークに対する社内規定，ルール等の必要性

たなリスクになりうることがわかる．さらに，テレワークを実施している回答者（1,396 人）に対して「テレワークを想定した社内規定，ルール，手順等は必要と思いますか.」といった質問を行ったところ，図 1 のようになった．

図 1 を見てわかるように，「必要である」「どちらかというと必要である」と回答している割合は合わせて全体の約 87%にまで及んでいる．この結果は，企業の新たな業務環境の変化に対する現場の声であると解釈することもできる．

(2) テレワークにおけるセキュリティ関する不安など

図 2 は，「テレワーク中にセキュリティ・インシデントが発生した場合，どのような問題が発生すると思いますか（発生しましたか).」という質問（複数回答可）に対する回答をまとめたものであるb．図 2 を見てわかるように，テレワーク中のセキュリティ・インシデント発生時の対応への不安を持っている回答者は全体の 1～2 割程度いる．

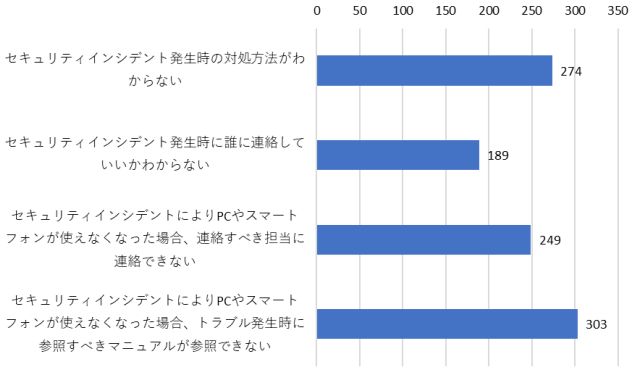

図 2：テレワーク中のセキュリティ・インシデント発生時の対応への不安

(3) 個人端末でのテレワークにおけるセキュリティ・インシデント発生時の責任への不安

「テレワーク調査（個人編）」で，テレワークで利用している（利用していた）機器（PC やスマートフォン，タブレット等の端末）は会社（企業）から支給されたものか，個人で所有するものかについて，テレワークを一度でも実施したことがある企業に属している回答者（1,800 人）に対して質問している．その結果をまとめたものが図 3 であるc．

図 3 から，企業から支給されている PC を業務に用いている回答者の割合は 82.3%（1,483 人）と高いが，企業から支給されているスマートフォン等の端末を業務に用いている回答者の割合は 45.5%（819 人）とそれほど高くないことがわかる．一方で，個人所有の PC（スマートフォン等の端末）を業務に用いている回答者の割合は 20%（26%）とそ

a 22%程度の回答者が「ほとんどテレワークをしていない（社内で業務をしている)」と回答している．これらの回答者については，社内で十分な新型コロナウイルス対策を施し，また時差通勤等を推進している可能性もあることを指摘しておく．

b この質問は，テレワークを一度でも導入した企業に所属する回答者（1,800 人）を対象としたものである．

c 会社から支給される PC だけでなく，個人所有の PC も利用している回答者がいる（「業務での利用なし」は排他項目である）．

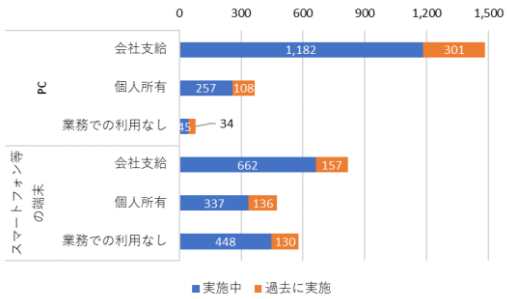

図 3：テレワークに利用している（利用していた）機器

れほど高くない．さらに，業務に企業から支給されている PC のみを業務に利用している回答者の割合は 75%（1,094 人）と高く，個人所有の PC のみを業務に利用している回答者の割合は 13%（169 人）にとどまっている[d]．企業から支給されているスマートフォン等の端末のみを業務に利用している回答者の割合は 42%（611 人），個人所有のスマートフォン等の端末のみを業務に利用している回答者の割合は 22%（286 人）となっている．

ここで，個人所有の PC もしくはスマートフォン等の端末を利用している回答者（631 人）に対して，個人端末でのテレワークにおけるセキュリティ・インシデント発生時の責任への不安について質問を行っている．631 人のうち 215 人（約 34.1%）は「不安に思うことはない」と回答しているが，残りの回答者は図 4 にある通り，何らかの不安を抱えていることがわかる．個人端末でのテレワーク実施における不安のトップ 3 はウイルス感染（39.1%，247 人），情報漏えい（34.7%，219 人），端末の紛失（27.3%，172 人）である．なお，個人所有の PC は社外だけでなく，社内でも利用されていることもわかっている[YY]．このことから，社外からのウイルス等の持ち込み，移動時の盗難防止などに注意する必要がある．

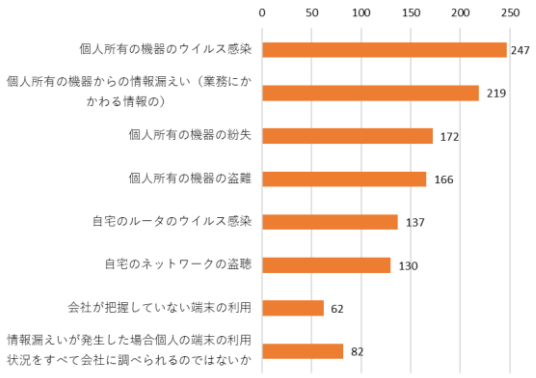

図 4：個人端末でのテレワークにおけるセキュリティ・インシデント発生時の責任への不安

(4) テレワークで使用するネットワーク環境におけるセキュリティ対策

「テレワーク調査（個人編）」では，テレワークを一度でも導入した企業に所属する回答者（1,800 人）に対して，テレワークで使用するネットワーク環境について質問を行っている．その結果，個人が所有している機器（個人購入のルータやスマートフォンでのデザリング，住宅に設置済みの WiFi 等を利用）でネットワークに接続している回答者数は 1,162 人（65%），企業から支給された機器（企業から支給されているモバイルルータやスマートフォンでのデザリングを利用）でネットワークに接続している回答者数は 638 人（35%）である．後者に関してある程度の水準のセキュリティ対策が期待されるが，前者に関しては回答者のセキュリティに対する意識などに依存したセキュリティ対策の水準になってしまうことが予想される．そこで，続いて，個人が所有している機器でネットワークに接続している回答者（1,162 人）に対して，自宅のホームネットワークにおけるセキュリティ対策として気を付けていることについて質問している（図 5）．「ID/パスワードは初期設定から変更している」「ファームウェアを最新の状態に更新している」「強度の高い暗号化方式（WPA2 等）を設定している」については約 70%の回答者が実施していることがわかる．一方で，それ以外に項目についてはいずれも 50%を下回っていることが見てとれる．

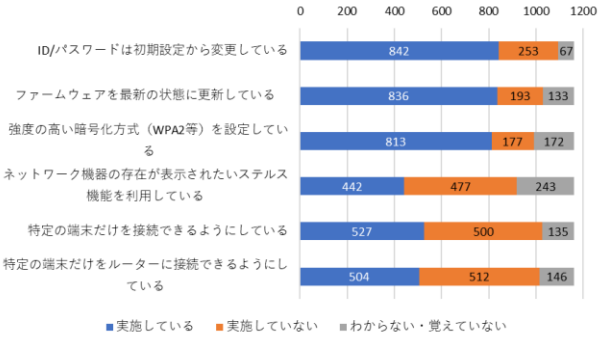

図 5：自宅のホームネットワークにおけるセキュリティ対策として気を付けていること

(5) 回答者属性

表 1 は回答者の属性をまとめたものである．「テレワーク調査（個人編）」では，IT 企業か否か，また企業規模（従業員数）が大きいか否か，といった基準で分類を行ってサンプルを収集している[e]．

表 1 の回答者属性としては回答者の個人属性（年齢や性別，雇用形態，所属部署）と回答者の所属する企業属性（業

d これをテレワーク実施中の企業と過去にテレワークを実施していた企業に分けて見てみると，個人所有の PC のみを業務に利用している前者に所属する回答者の割合は 12.1%であるのに対して，後者に所属する回答者の割合は 17.1%となっている．

e IT 企業かどうかによって，企業規模の基準が異なる．「テレワーク調査（個人編）」では IT 企業の場合，従業員数が 101 人以上で大規模，IT 企業以外の企業・組織の場合，従業員数が 301 人で大規模としている．

表 1：回答者属性

		#			#
性別	男性	2,078	所属企業の売上高	5千万円未満	110
	女性	294		5千万円以上～1億円未満	92
年齢	20代	80		1億円以上～3億円未満	166
	30代	317		3億円以上～10億円未満	213
	40代	747		10億円以上～100億円未満	442
	50代	886		100億円以上～1千億円未満	346
	60歳以上	342		1千億円以上～1兆円未満	238
雇用形態	経営者・役員	161		1兆円以上	198
	会社員・公務員・職員	1,981		わからない	567
	専門職	40	所属企業の勤務地	北海道・東北	176
	契約社員・派遣社員	190		関東（東京除く）	342
所属部署	営業	241		東京	863
	販売	32		中部	322
	総務	96		近畿	436
	経理	36		中国・四国	117
	財務	11		九州・沖縄	116
	人事	30	所属企業の従業員数	～19人	297
	情報システム	1,028		20人～49人	263
	企画	134		50人～100人	320
	販促・マーケティング	31		101人～300人	381
	製造	134		301人～500人	150
	商品・サービス開発	235		501人～1,000人	187
	研究	114		1,001人～5,000人	344
	その他	250		5,001人～10,000人	134
所属企業の業種	製造業	618		10,001人以上	296
	情報通信業	616	分類	IT 企業・大規模	717
	卸売業・小売業	201		IT 企業・中小規模	610
	金融業・保険業	139		IT企業以外・大規模	526
	その他の業種	798		IT企業以外・中小規模	519

種，売上高，勤務地域，従業員数）を取り上げている．

3. 分析

本研究では，多重コレスポンデンス分析を行い，テレワークにおけるセキュリティ等への不安の一つである個人端末でのテレワークにおけるセキュリティ・インシデント発生時の責任への不安と回答者属性との関係性について検討する．

3.1 多重コレスポンデンス分析

2 つのカテゴリ（質的）変数間の関係について調べる方法はコレスポンデンス（対応）分析と呼ばれる．2 つのカテゴリ変数は行項目と列項目に分けられ，その関連性についてはクロス集計表を用いて表の形で示すことができるが，行と列の項目数が多くなれば，表の解釈が難しくなるといった難点がある．コレスポンデンス分析は，それぞれの項目を散布図で視覚化するだけではなく，2 つの項目を組み合わせた散布図で項目間の関係を視覚的に捉えることができるといった特徴を持つ. コレスポンデンス分析を拡張し，3 つ以上のカテゴリ変数間の関連性・類似性を，平面的な（もしくは，立体的な）図で示す分析方法が多重コレスポンデンス分析（multiple correspondence analysis）である[7].

多重コレスポンデンス分析は，コレスポンデンス分析と同様に, 多重クロス集計表の関連性を分析することになる．

3.2 質問項目の加工

多重コレスポンデンス分析を行うためには，アンケート調査によって収集された回答データを加工する必要がある．その簡単な手順などについて説明する．

アンケート調査では，図 6(a)にあるような形式でデータが保存されているが，これでは多重コレスポンデンス分析

ID	Q1
1	A
2	B
3	C
4	D
5	E

(a) カテゴリカルデータ

ID	Q1.A	Q1.B	Q1.C	Q1.D	Q1.E
1	1	0	0	0	0
2	0	1	0	0	0
3	0	0	1	0	0
4	0	0	0	1	0
5	0	0	0	0	1

(b) ダミーデータ

図 6: アンケート調査データの変換

を行うことはできず，図 6(b)のような 0 か 1 を付与するデータ形式に変換する必要がある．

第 2.2 節で示した「テレワークにおけるセキュリティ関する不安」(「セキュリティ・インシデント発生時の対処方法がわからない」「セキュリティ・インシデント発生時に誰に連絡していいかわからない」「セキュリティ・インシデントにより PC やスマートフォンが使えなくなった場合，トラブル発生時に参照すべきマニュアルが参照できない」)の回答はもともと 2 値をとっているので特に変換作業の必要はない．しかしながら，回答者属性（「年齢層」「テレワークの実施頻度」「テレワーク導入時期」「業種」「勤務地域」「従業員数」)に対してはこれらの変換作業を行う必要がある．そのため，実際の分析では回答者数は 1,396 人（テレワークを実施している回答者数）になる．

「年齢層」は 5 カテゴリ（20 代，30 代，40 代，50 代，60 歳以上)，「テレワークの実施頻度」は 4 カテゴリ，「テレワーク導入時期」は 3 カテゴリ，「業種」は 5 カテゴリ（製造業，情報通信業，卸売業・小売業，金融業・保険業，その他の業種)，「勤務地域」は 7 カテゴリ（北海道・東北，関東（東京を除く)，東京，中部，近畿，中国・四国，九州・沖縄)，「従業員数」は 9 カテゴリである．

3.3 分析結果

本研究では，R version 4.0.3 を用いて，「テレワークにおけるセキュリティ関する不安」と回答者属性の多重コレスポンデンス分析を行った[8]．その分析結果を図示したものが図 7 である．

この分析に用いられているサンプルサイズは 1,396 人，カテゴリ総数は 30 であり，多重コレスポンデンス分析における最大次元数は 29 である．紙面の都合上，省略するが，多重コレスポンデンス分析を実行して得られる固有値に関する結果に関して，累積寄与率が第 2 軸までで 11.2% であり, 低い水準になっている. 第 3 軸までを見ると 15.5% となり，必ずしも大きな改善は見られない．また，多次元空間でプロットを解釈することは非常に困難であるため，本研究では平面の結果を採択することにする．固有値の累積寄与率が低くなっている理由の一つとして，分析に用いているカテゴリ数が多いことが考えられる．

3.4 考察

第 3.3 節の多重コレスポンデンス分析によって,「テレワークにおけるセキュリティ関する不安」と回答者属性の関係が平面に可視化された．

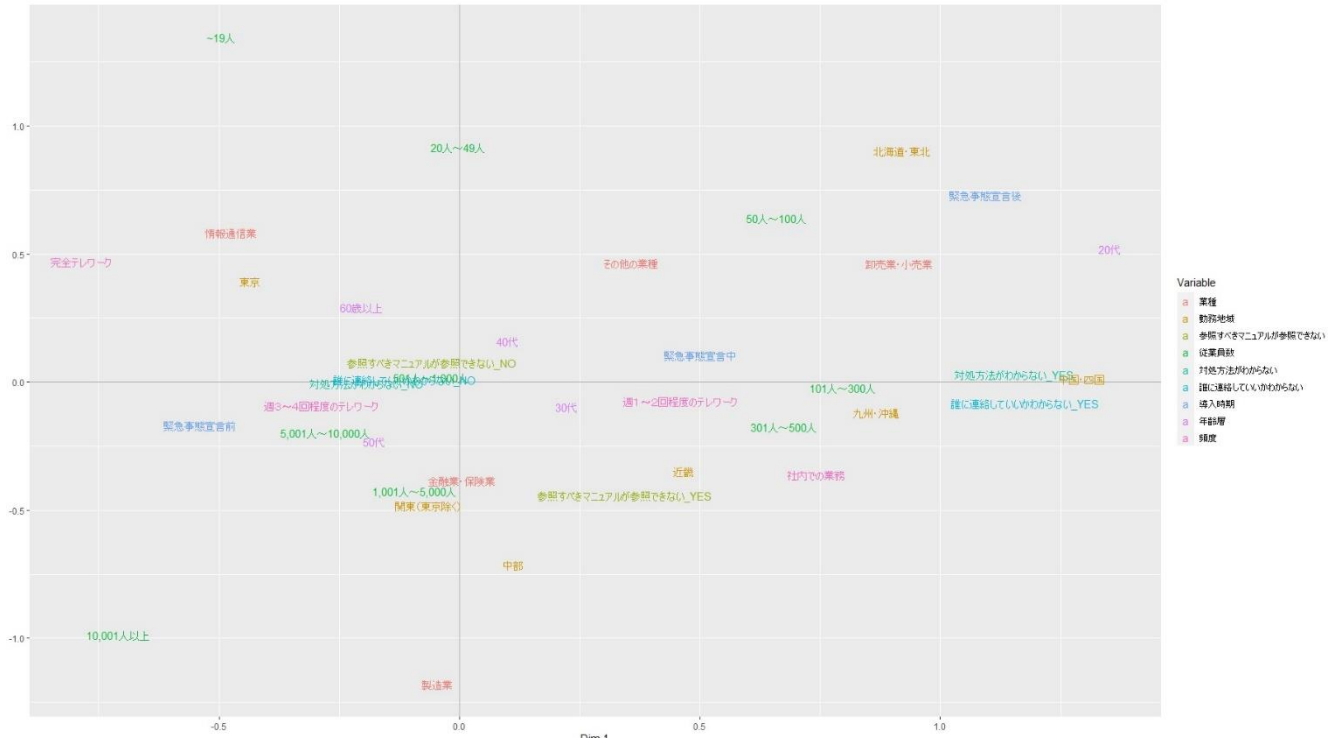

図 7：分析結果

図 7 の見方について簡単に説明する．例えば，「週 3～4 回程度のテレワーク」の近くに位置しているものとして「緊急事態宣言前」「5,001～10,000 人」「50 代」「テレワークにおけるセキュリティ関する不安」（「セキュリティ・インシデント発生時の対処方法がわからない_NO」「セキュリティ・インシデント発生時に誰に連絡していいかわからない_NO」「セキュリティ・インシデントにより PC やスマートフォンが使えなくなった場合，トラブル発生時に参照すべきマニュアルが参照できない_NO」）などがある[f]．これらの要因は，週 3～4 回程度のテレワークを実施している個人の特徴であるといえる．一方で，例えば「緊急事態宣言中」「緊急事態宣言後」とは離れているため，この要因との関係性は弱いといえる．このように，注目する要因 A があった場合，その近くにある他の要因でもってその特徴付けが可能となる．これを踏まえて，以下，これの分析結果に対する考察を行っていく．

全体的な傾向として，左側のエリア（第 2 象限・第 3 象限）では，勤務地域が首都圏（東京，関東（東京除く））の場合，セキュリティ・インシデント発生時に「マニュアルが参照できない」「対処方法がわからない」「誰に連絡していいかわからない」という不安を感じていないが，右側のエリア（第 1 象限・第 4 象限）では，勤務地が首都圏以外であり，「マニュアルが参照できない」「対処方法がわからない」「誰に連絡していいかわからない」という不安を感じている傾向があることがわかる．

また，テレワークの導入時期を見ると，緊急事態宣言前の導入の場合，いずれの不安要因とも離れているが，緊急事態宣言中の導入の場合「マニュアルが参照できない」，緊急事態宣言後の導入の場合「対処方法がわからない」「誰に連絡していいかわからない」といった不安を感じていることから，テレワーク導入の実績が浅い場合，不安を感じている傾向があることが示唆される．

不安要因の顕著な傾向としては，インシデント発生時の「対処方法がわからない」と感じる人は「誰に連絡していいかわからない」という不安も感じており，インシデント発生時の具体的な振る舞いについて関連性があることが指摘できる．

さらに，テレワークの実施頻度で見ると，週 3～4 回程度実施している人より週 1～2 回程度実施している人の方が「マニュアルが参照できない」「対処方法がわからない」「誰に連絡していいかわからない」といった不安を感じていることから，テレワークの実施頻度が低い場合，不安を感じている傾向があることが読みとれる．

加えて，「30 代～60 歳以上」は中央に寄っており，「20 代」とは離れているが，いずれも不安要因とは離れており，年齢と不安要因との関連性は低いことが読み取れる．さらに，情報通信業で東京都内に勤務しており完全テレワークの場合いずれの不安要因とも離れており，関連性が低いことが読み取れる．

f 「テレワークにおけるセキュリティ関する不安_NO」はテレワークにおけるセキュリティ関する不安が特にないことを表している．一方で，「テレワークにおけるセキュリティ関する不安_YES」はテレワークにおけるセキュリティ関する不安があることを意味する．

4. おわりに

本研究では，IPA が 2020 年度に「ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査」[5]の一環として実施した個人を対象としたウェブアンケート調査[6]の調査結果を紹介するとともに，テレワークを実施する上で個人が感じるセキュリティに関する不安と回答者等の関係についてコレスポンデンス分析により検証を行った．分析の結果から，セキュリティ・インシデント発生時の対応に不安を感じているのは「勤務地が首都圏以外」および「テレワークの実績が浅く実施頻度が低い場合」であること，セキュリティ・インシデント発生時の対処方法がわからないという不安を感じている人はインシデント発生時の連絡先もわからないといった不安を感じていることなどがわかった．

テレワークは今後も定着することが想定されるため，インシデント発生の対処方法や連絡先が取り決められ，どのような環境でも対応ができるよう事前に準備しておくことで，安心してテレワークを実施できる状況を整えておく必要がある．

特に，緊急事態宣言中および緊急事態宣言以降にテレワークを導入している場合，セキュリティ・インシデント発生時の対応方法や連絡先の取り決めや周知の不足が無いか，テレワーク環境でインシデントが発生してもマニュアルが参照できる状態になっているかについて，見直しを実施することを推奨する．今回分析で用いたデータは 2020 年 10 月 31 日時点の状態であるが，2021 年 5 月の時点で 3 度目の緊急事態宣言，まん延防止等重点措置により，ニューノーマルの考え方も変化を迎えていることが考えられる．そのため，更なる調査も必要と考える．また，これらの分析結果が，ニューノーマルでセキュアな働き方などについての対策のための一助となることを期待したい．

参考文献

[1] 情報処理推進機構「情報セキュリティ 10 大脅威 2021」<https://www.ipa.go.jp/security/vuln/10threats2021.html>(参 照 2021-05-09)

[2] Security NEXT「VPN 認証情報漏洩に見る脆弱性対策を浸透させる難しさ」 https://www.security-next.com/117811

[3] ScanNetSecurity「在宅勤務時 SNS 経由で社用 PC が感染，社内ネットワーク接続で被害拡大（三菱重工業）」https://scan.netsecurity.ne.jp/article/2020/08/14/44439.html

[4] Gigazine「オンライン会議ツールの Zoom に「攻撃者がわずか数分で非公開の会議にアクセスできる脆弱性」があったとの報告」https://gigazine.net/news/20200730-zoom-cracking-private-meeting-passwords/

[5] 情報処理推進機構，ニューノーマルにおけるテレワークと IT サプライチェーンのセキュリティ実態調査，2021 年＜https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html＞(参照 2021-05-09)

[6] 情報処理推進機構，テレワークの実施における不安に関する調査結果（個人編 中間報告），2021 年＜https://www.ipa.go.jp/security/fy2020/reports/scrm/index.html＞(参照 2021-05-09)

[7] Le Roux, B., Rouanet, H.: Multiple Correspondence Analysis, SAGE Publications, 2010

[8] 川端一光・岩間徳兼・鈴木雅之，R による多変量解析入門: データ分析の実践と理論，オーム社，2018 年