BOJ Reports & Research Papers

金融システムレポート別冊シリーズ

Financial System Report – Annex

金融機関における在宅勤務の拡がりと システム・セキュリティ面の課題 ―アンケート調査結果から―

日本銀行
金融機構局

2020年10月

本レポートの内容について、商用目的で転載・複製を行う場合は、予め日本銀行金融機構局までご相談ください。転載・複製を行う場合は、出所を明記してください。

【本レポートに関する照会先】
日本銀行金融機構局考査企画課（csrbcm@boj.or.jp）

（金融システムレポート別冊シリーズについて）

日本銀行は、マクロ・プルーデンスの視点からわが国金融システムの安定性を評価するとともに、安定確保に向けた課題について関係者とのコミュニケーションを深めることを目的として、『金融システムレポート』を年 2 回公表している。同レポートは、金融システムの包括的な定点観測である。

『金融システムレポート別冊シリーズ』は、特定のテーマや課題に関する掘り下げた分析、追加的な調査等を不定期に行い、『金融システムレポート』を補完するものである。本別冊では、2020 年 7 月から 8 月にかけて実施した「在宅勤務に関するアンケート」の結果を紹介する。

（本別冊の要旨）

新型コロナウイルスの感染拡大を受け、感染拡大を防止する観点から政府よりテレワーク等の推進が呼びかけられ、これに伴い在宅勤務の利用は急速に拡がっている。

日本銀行は、今般、当座預金取引先金融機関等のうち 239 先を対象に、新型コロナウイルスの感染拡大前後における在宅勤務の実施状況やシステム・セキュリティ面の対策・課題等について調査するため、アンケートを実施した。

アンケート結果をみると、今回の感染拡大を受けて、金融機関においても在宅勤務の導入が大きく進展したことが確認された。また、システム面では、在宅勤務用の会社貸与端末の追加調達やシステムの能力増強など、様々な対策が実施されていたほか、今後も在宅勤務関連のシステム能力増強を図る先が少なからずみられた。一方、セキュリティ面では、会社貸与端末のセキュリティ対策は概ね適切に実施されていたが、在宅勤務での利用が認められた私用端末のセキュリティ対策に改善の余地がみられたほか、Web 会議サービスの利用に当たって、運用ルールの策定など体制整備が必要な点がみられた。

在宅勤務の活用が今後も進んでいくと考えられる中、金融機関業務を安定的に運営していくためには、こうした動きに合わせてセキュリティ対策も適切に行う必要がある。日本銀行としては、金融機関が在宅勤務環境の整備やシステム・セキュリティ面の取り組みを進めていくうえで、本アンケート結果が活用されることを期待するとともに、考査・モニタリング、各種セミナー等を通じて、そうした取り組みを後押ししていく方針である。

【目　次】

Ⅰ．はじめに

在宅勤務はこれまで、わが国が直面する「少子高齢化に伴う生産年齢人口の減少」や、「働く方々のニーズの多様化」などの課題に対応するための働き方改革推進の一つの手段として注目されてきたが、新型コロナウイルスの感染拡大を受け 2020 年 2 月に政府が策定した「新型コロナウイルス感染症対策の基本方針[1]」において、感染拡大を防止する観点から、企業に対しテレワーク等の推進が強力に呼びかけられ、これに伴い在宅勤務の利用は急速に拡がることとなった。

在宅勤務は、企業が従業員や顧客の安全を確保しつつ、生産性を高めるための手段となり得る一方で、社外からの社内システムへの接続等に伴う、セキュリティ対策や情報管理体制などのリスク管理に関しても注目が集まっている。

こうした状況を踏まえ、日本銀行では、取引先金融機関等のうち 239 先[2]（以下、「調査先」という）を対象に、「新型コロナウイルス感染症対策の基本方針」の発表（以下、「方針発表」という）前後における在宅勤務の実施状況、在宅勤務にかかるシステムの整備・利用状況およびセキュリティ対策の実施状況、在宅勤務の活用に当たっての課題等を把握することを目的としてアンケート調査を実施した[3]。

以下では、アンケート調査結果を概観しつつ、今後の課題等について整理する。

---

[1] 新型コロナウイルス感染症対策本部決定（令和 2 年 2 月 25 日）。

[2] 内訳は、銀行 184 先、信用金庫 20 先（しんきん共同センターに加盟していない信用金庫）、系統中央機関 4 先、金融商品取引業者 22 先、証券金融会社 1 先、短資会社 3 先、資金清算機関 1 先、金融商品取引清算機関 2 先、その他 2 先。

[3] アンケート実施期間は 2020 年 7 月 6 日から 8 月 7 日まで。回収率は 100%。

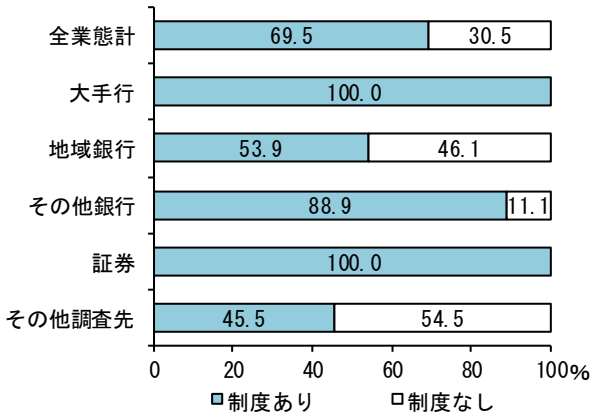
Ⅱ．在宅勤務に関するアンケートの結果

１．在宅勤務の実施状況

（１）在宅勤務制度

調査先における在宅勤務制度の有無をみると、７ 割程度の先に在宅勤務制度があるという結果となった（図表 1）。これを業態別[4]でみると、大手行や証券では全先に在宅勤務制度がある一方、地域銀行やその他調査先で制度がある先は約半数という結果となっており、業態によってばらつきがあることが確認された。

図表 1 在宅勤務制度の有無

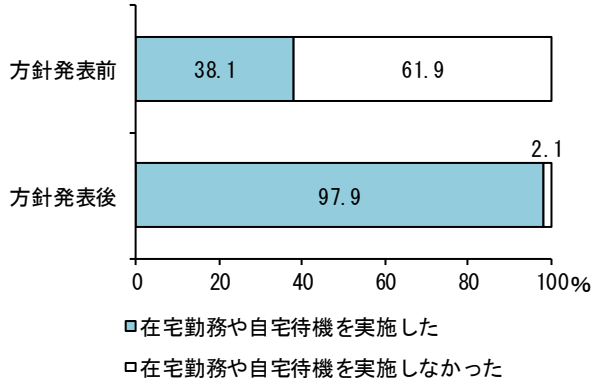


（２）在宅勤務・自宅待機の実施状況

在宅勤務や自宅待機の実施状況を方針発表前後で比較すると、方針発表前は６割が未実施であったが、方針発表後はほぼ全先が実施しているとの結果となった（図表 2）。調査先の中には、新型コロナウイルスの感染拡大に急遽対応しなければならなかったという状況から、制度はないものの、緊急対応として在宅勤務を実施したという先もみられた。

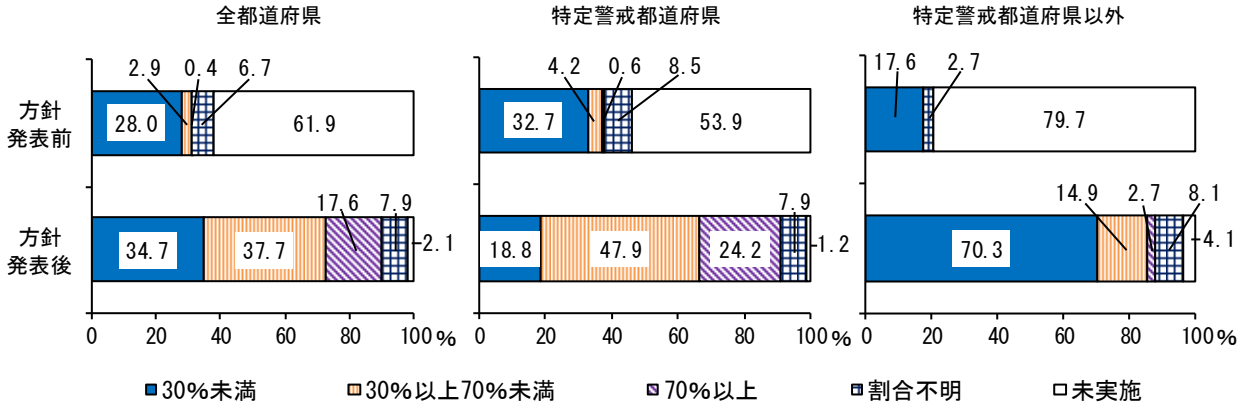
[4] 「大手行」：みずほ、三菱 UFJ、三井住友、りそな、埼玉りそな、三菱 UFJ 信託、みずほ信託、三井住友信託、新生、あおぞら（10 行）、「地域銀行」：地方銀行 64 行と第二地方銀行 38 行、「その他銀行」：大手行および地域銀行を除く銀行（72 行）、「証券」：金融商品取引業者 22 先、その他調査先：信用金庫 20 庫を含む 33 先。

図表 2 在宅勤務・自宅待機の実施状況



また、方針発表後に在宅勤務や自宅待機を実施した職員の比率をみると、全体では、一部の職員のみが実施した先から、大半の職員が実施した先まで、調査先によって様々な状況がみられており、特段の傾向は確認できなかった。もっとも、これを本店等の所在地をもとに、政府が緊急事態宣言下で指定した特定警戒都道府県[5]とそれ以外の県で比較すると、特定警戒都道府県の方が在宅勤務・自宅待機の実施比率が高くなっており、地域の感染状況や自治体の要請等に応じ、在宅勤務や自宅待機を実施したことが窺われる結果となった（図表 3）。

図表 3 在宅勤務・自宅待機を実施した職員の比率[6]



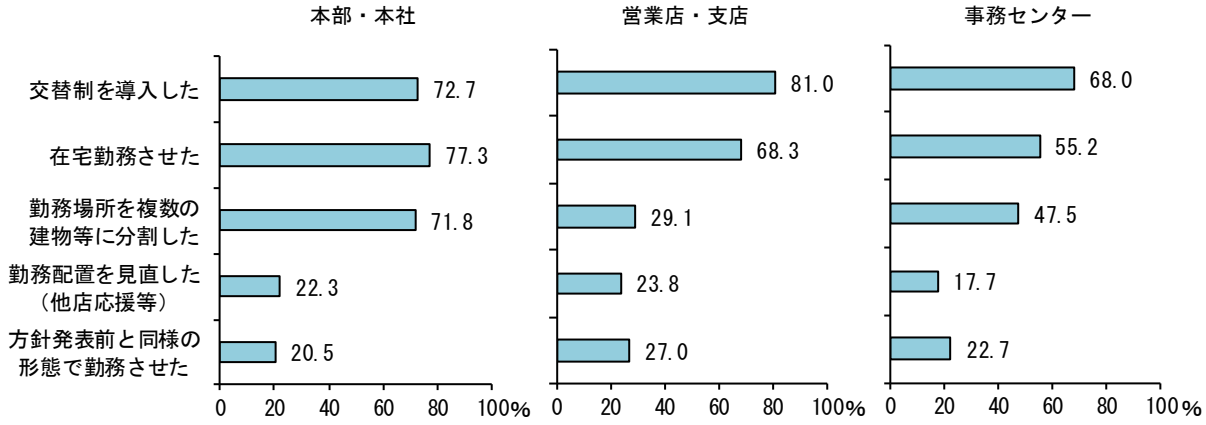
方針発表後の具体的な勤務形態を本部・本社、営業店・支店、事務センターといった事業所別にみると、いずれの事業所においても交替制や在宅勤務を実施している割合が高かった。また、本部・本社および事務センターでは勤務場所を分割して対応した先も相応にみられる結果となった（図表 4）。

---

[5] 東京都、大阪府、北海道、茨城県、埼玉県、千葉県、神奈川県、石川県、岐阜県、愛知県、京都府、兵庫県、福岡県。

[6] 内訳の数字は小数点以下第 2 位を四捨五入しているため、合計しても必ずしも 100 とはならない（以降の図表において同じ）。

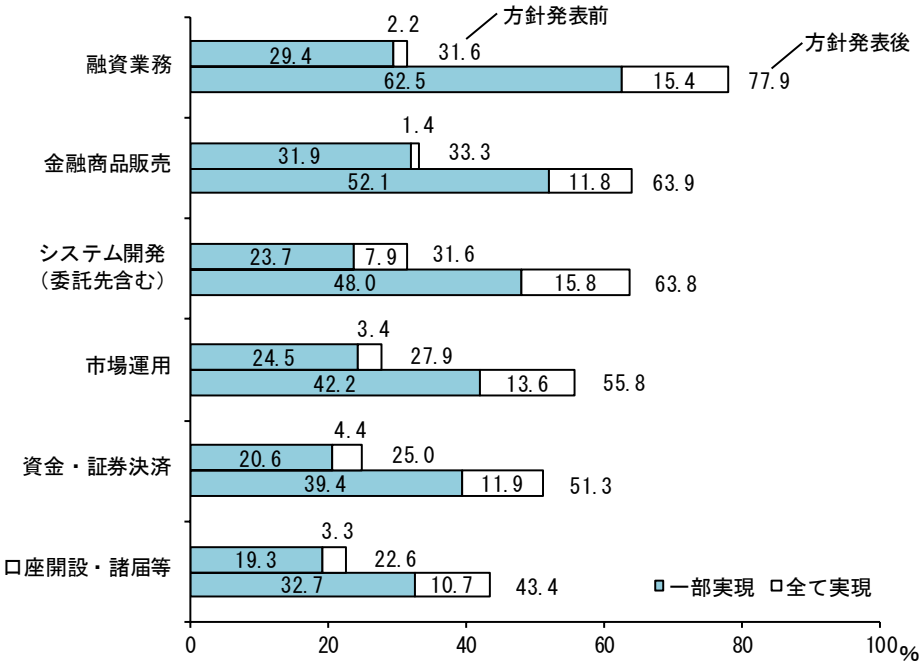
図表 4 方針発表後の主な勤務形態（複数回答可）



（注）分母は、上記 5 つの勤務形態のいずれかに相当する回答があった先。

主要な金融機関業務について、在宅勤務の実現状況をみると、方針発表前はいずれの業務も在宅勤務に対応している先は２～３割程度であったが、方針発表後はその割合が高まっている。在宅勤務を実現している割合の高い業務は融資業務、金融商品販売、システム開発業務で、6～7 割程度まで増加した。一方、口座開設・諸届等は 4 割程度にとどまっており、業務内容によって差がみられる結果となった（図表 5）。

図表 5 在宅勤務の実現状況

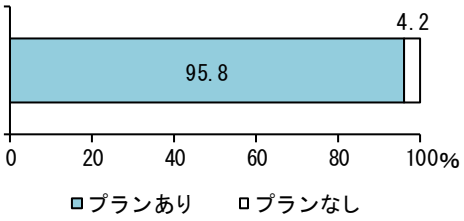


（注）分母は、各業務について、実現状況の回答があった先。

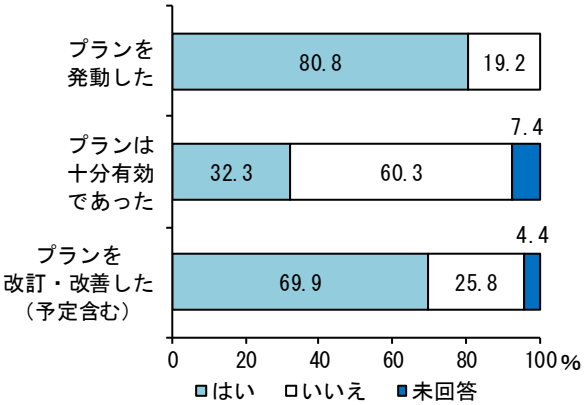
（３）業務継続計画・コンティンジェンシープランの整備・実施状況

感染症に対する業務継続計画・コンティンジェンシープラン（以下、「プラン」という）の整備状況をみると、殆どの先で整備されており（図表 6）、８割の先で新型コロナウイルスの感染拡大を受けて実際にプランを発動したとの結果となった。もっとも、同プランの評価をみると、今回の新型コロナウイルス対応のような大幅な出勤の制限を想定していなかったなど、6 割の先が、既存のプランが十分有効ではなかったと評価しており、7 割の先が改訂・改善を行う（行った）と回答した（図表 7）。改訂・改善内容として、在宅勤務を既存のプランに組み込むとした先も多く、業務継続の観点からも、在宅勤務の活用拡大を図る動きが窺えた。

図表 6 方針発表前のプランの策定状況



図表 7 プランの発動状況・評価



（注）分母は、方針発表前にプランを策定済みの先。

２．在宅勤務にかかるシステムの整備・利用状況[7]

（１）社内システムへ接続する仕組み

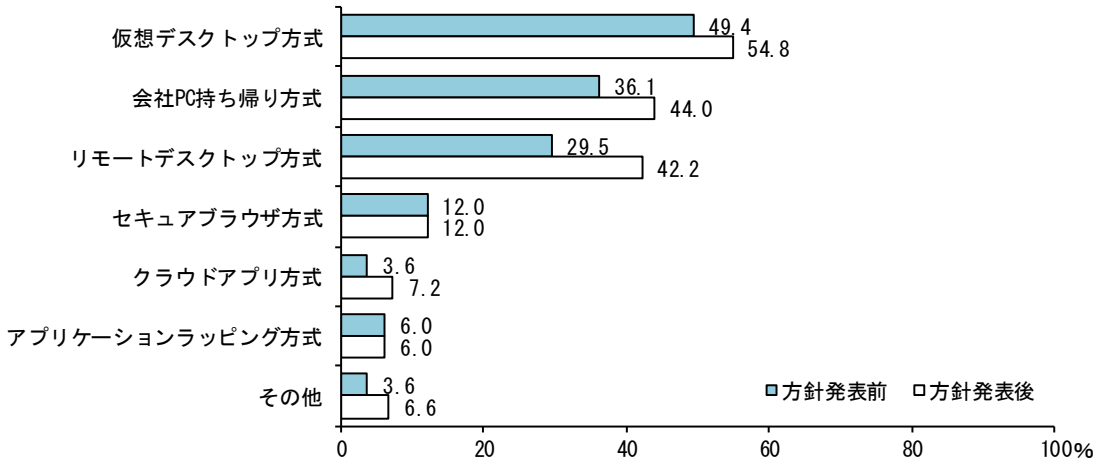
在宅勤務において、自宅から社内システムへの接続方式には様々なものがあり、選択する方式により、構築にかかる費用やセキュリティ上の留意点などが異なる。本アンケート調査では、総務省の「テレワークセキュリティガイドライン」におけるテレワークの類型（別紙を参照）ごとに、調査先における採用状況および方針発表前後の変化を確認した[8]。アンケート結果をみると、方針発表前は、上記類型のうち「仮想デスクトップ方式」がもっとも多く、「会社 PC 持ち帰り方式」と「リモートデスクトップ方式」がそれに次ぐという回答となった。方針発表後においても、こうした傾向は変わらなかったが、方針発表前後の変化幅をみると、リモートデスクトップ方式が最も大きかったことが確認された（図表 8）。同方式は、

[7] ２．以降の設問については、Web 会議および委託先による社内システムへの接続に関するものを除き、在宅勤務制度を有する先を調査対象とした。

[8]「テレワークセキュリティガイドライン第４版」（総務省、平成 30 年４月 13 日）。

他の方式と比べると、自社のシステム構成を大きく変更することなく、短期間での導入が可能であるため、選好された可能性がある。

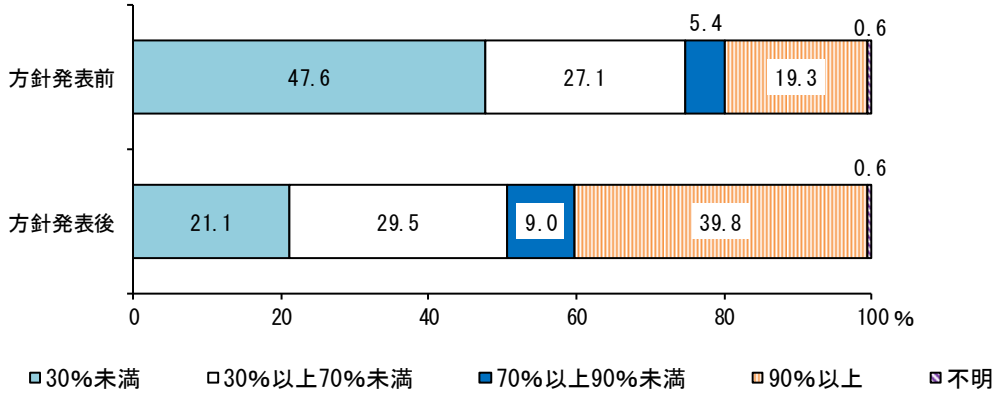
図表 8 在宅勤務に使用する端末と社内システムの接続方式（複数回答可）



（２）在宅勤務用端末・回線

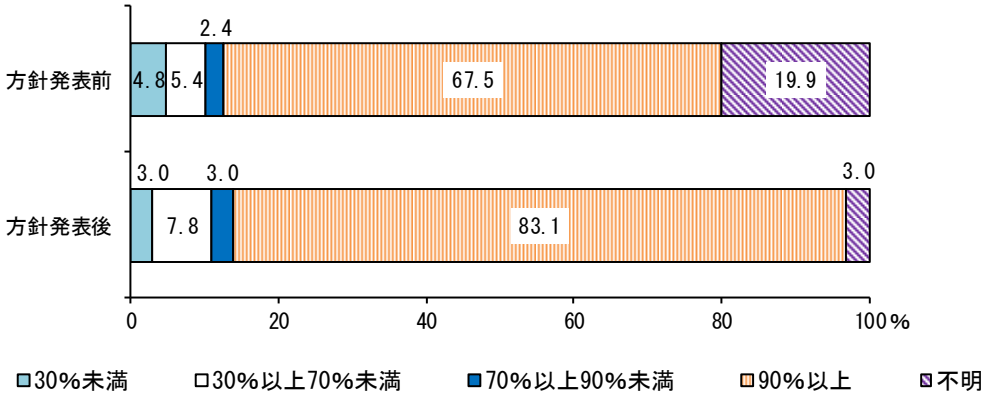
在宅勤務用端末がどの程度整備されているかを確認する観点から、全職員数に対する同端末台数（パソコン、スマートフォン、タブレット等を合算した台数）の割合をみると、方針発表前は 30%未満の先が約半数を占め、70%以上の先は 2 割強にとどまった一方、方針発表後は外国金融機関を中心に半数の先が 70%以上となるなど、大幅に増加していることが確認された（図表 9）。

図表 9 全職員数に対する端末台数の割合



在宅勤務環境を整備するうえでは、在宅勤務用端末の台数だけではなく、外部から社内システムに対し、同時にどれだけの台数を接続可能とするかも留意すべき要素となる。端末台数に対し同時にアクセスできる台数が少ない場合、社内システムに接続できない端末が発生し、在宅勤務の円滑な実施に支障が生じるおそれがある。アンケート結果では、多くの先で端末台数の 90%以上が同時に接続可能な環境を用意していることが確認された（図表 10）。

図表 10 端末台数に対する同時接続数の割合

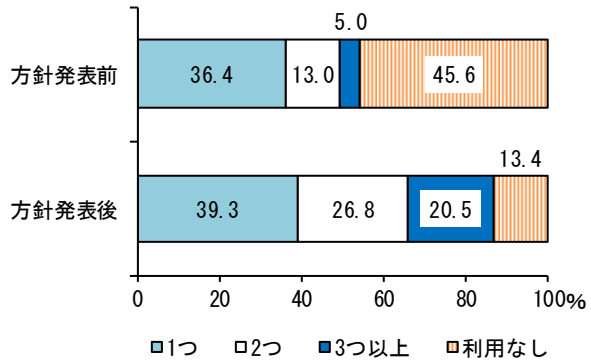


（注）「不明」は在宅勤務用端末がゼロの先を含む。

（３）Web 会議

新型コロナウイルスの感染拡大に伴い、非接触でのコミュニケーション手段として、Web 会議[9]が注目を集めている。本アンケート調査では、社外とのコミュニケーションに利用する Web 会議サービスの利用状況等について確認した[10]。アンケート結果をみると、方針発表前は半数強であったが、方針発表後には９割近い先が何らかのサービスを利用するようになっており、金融機関においても利用が拡がっていることが確認された。また、利用しているサービスの数をみると、方針発表前は複数のサービスを利用している先は２割程度にとどまっていたが、方針発表後は半数近くまで増加した（図表 11）。利用する Web 会議サービス数が増えることは、用途に応じた使い分けなど利便性の向上につながる一方で、サービス毎の脆弱性情報の把握等、リスク管理の重要性も高まっているといえる。

図表 11 利用している Web 会議サービスの数

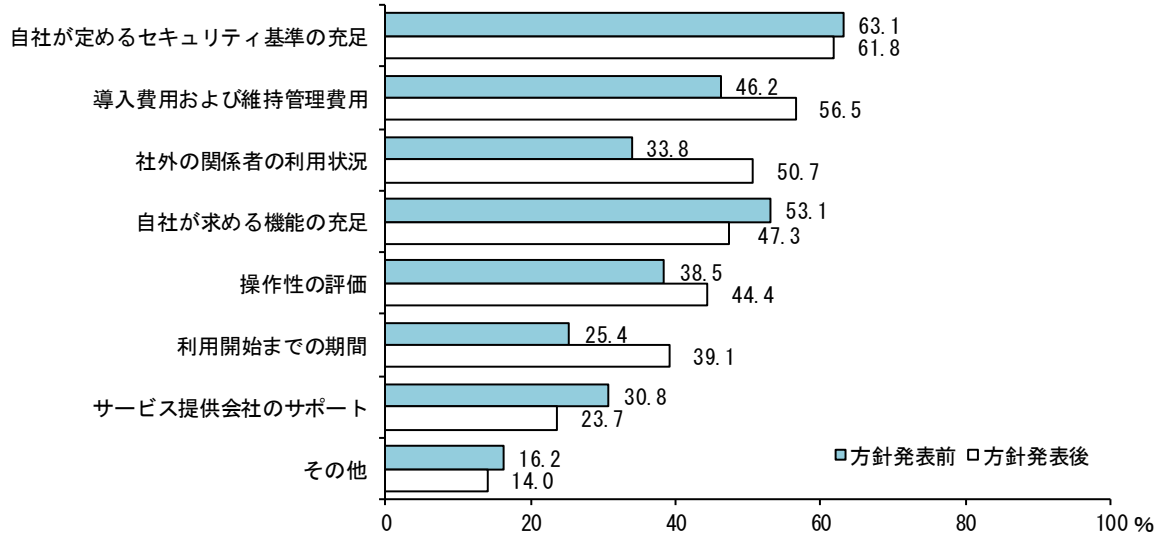


[9] インターネットを通じて遠隔地と、音声や映像のやり取り、資料の共有などを行うことができるコミュニケーションツール。

[10] 回答対象は自社が主催者として利用する場合のみ。

なお、Web 会議サービスを選定した際に重視したポイントをみると、方針発表前後ともセキュリティが最も重視されているが、方針発表後は社外の利用状況や費用を重視する先も増えている。方針発表に伴い Web 会議サービスの利用が急速に拡大する中で、サービスの選定にも様々な要素が加味されたことが窺えた（図表 12）。

図表 12 Web 会議サービスの選定ポイント（複数回答可）

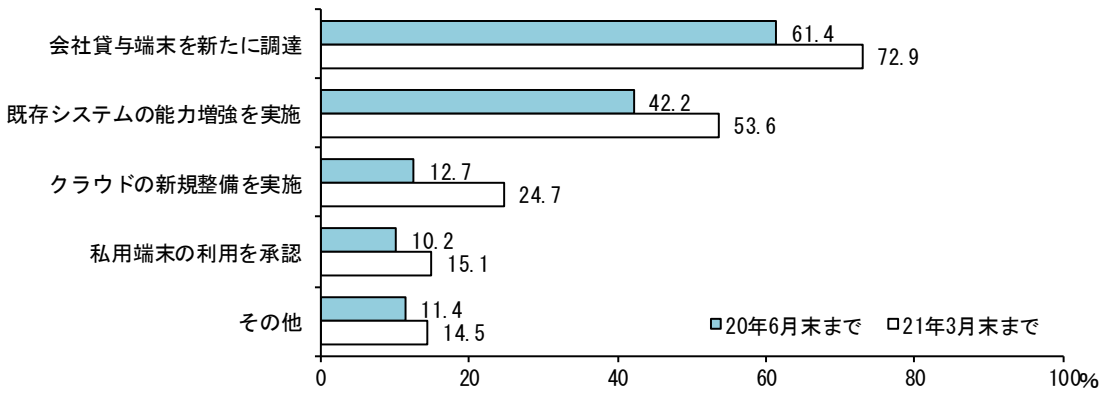


（注）分母は、Web 会議サービスを利用している先。

（４）方針発表後に実施したシステム対応および今後の方針

方針発表後に在宅勤務体制の整備のために実施したシステム対応をみると、会社貸与端末の新規調達（６割程度）や既存システムの能力増強（4 割程度）を行った先が多いという結果となった。2021 年 3 月末までに予定している対応も含めてみると、それぞれ７割程度、５割程度まで増えているほか、クラウドの新規整備を行う先も２割強となっているなど、多くの先が在宅勤務のための対応を進めていく様子が窺えた（図表 13）。

図表 13 在宅勤務のために行ったシステム対応（複数回答可）

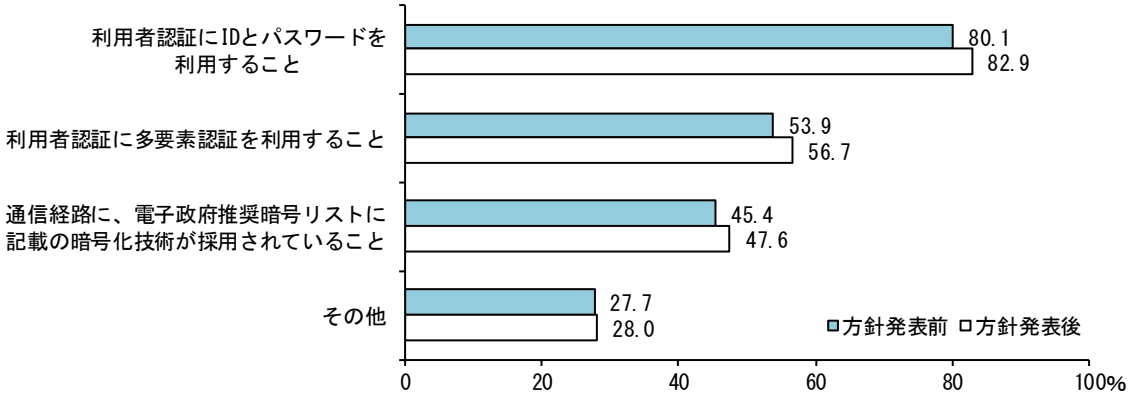


３．在宅勤務にかかるセキュリティ対策

（１）社内システムへの接続に用いるセキュリティ対策

社内システムへの接続時のセキュリティ対策をみると、８割程度の先で ID・パスワードによる認証、半数程度の先で多要素認証[11]を実施しているほか、その他では閉域モバイル網[12]などインターネットを経由しない接続経路を利用するといった回答がみられた（図表 14）。社内システムへの接続に当たっては、第三者による不正アクセスや通信内容の窃取を防ぐ観点から、ID・パスワードのみならず、多要素認証や通信の暗号化等複数の対策を組み合わせるなど、リスクに応じた適切なセキュリティ対策を実施することが重要である[13]。

図表 14 社内システム接続の際のセキュリティ対策（複数回答可）



（注）分母は、社内システムに接続する仕組みを有する先。

（２）委託先による社内システムへの接続

在宅勤務については、自社の職員だけではなく、委託先の職員も行うケースがある。在宅勤務中の委託先職員からの社内システム接続に関する認否をみると、接続を認めていた先は方針発表前で１割程度であったのに対し、方針発表後では２割程度まで高まっており、自社の職員だけではなく、委託先の職員が自宅から社内システムに接続するケースも増えたことが確認された（図表 15）。接続を認めている先におけるセキュリティ対策については、９割程度の先で接続状況を把握しており、７割程度の先で自社のセキュリティポリシーの充足状況の確認や接続に関する注意喚起を行っているという結果となったほか、その他では委託先

---

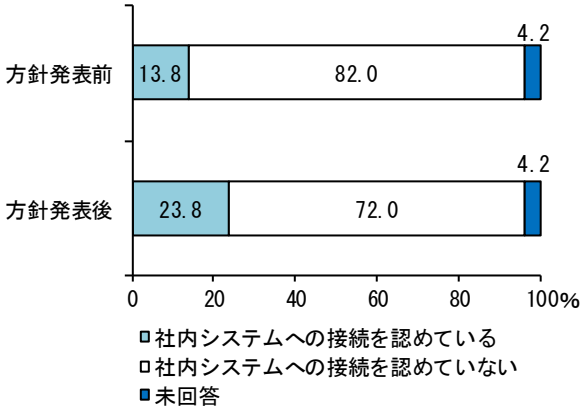
[11] 「知識情報（パスワード等）」、「所持情報（ハードウェアトークン、IC カード等）」、「生体情報（指紋等）」のうち、２つ以上を組み合わせて行う認証。

[12] 携帯電話やスマートフォン等のモバイルネットワーク上で、限られた利用者や拠点間のみを接続するネットワーク。

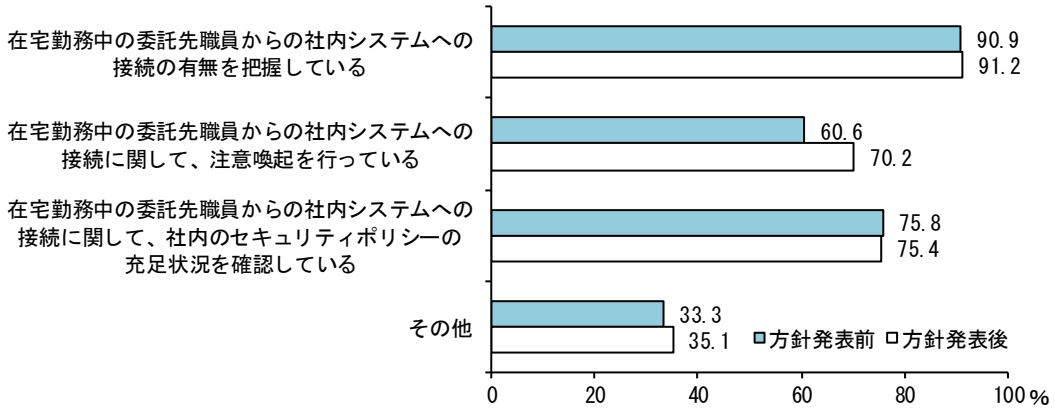
[13] 社内システムへの接続では、近年、ネットワーク機器の脆弱性を悪用したサイバー攻撃がみられていることから、本稿で採り上げた対策に加え、サイバー攻撃やネットワーク関連製品の脆弱性に関する情報を収集し、セキュリティパッチの適用や各種設定の見直し等の対策を適時適切に行うことも求められる。

が接続できるシステム環境を制限しているという回答がみられた（図表 16）。委託先職員の自宅からの社内システム接続は、自社の場合と比べセキュリティレベルが十分にコントロールできない可能性もあるため、重要な業務を委託している場合などは、セキュリティポリシーの充足状況の確認などを通じ、自社のセキュリティレベルを満たしているかを確認することが必要である。

図表 15 委託先による社内システムへの接続



図表 16 接続に関するセキュリティ対策（複数回答可）



（注）分母は、社内システムへの接続を認めている先。

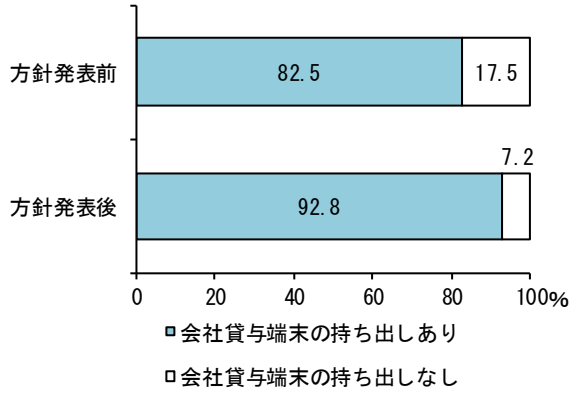
（3）端末等のセキュリティ対策

在宅勤務で使用する端末のセキュリティ対策も、在宅勤務を適切に実施していくうえで重要な要素である。本アンケート調査では、在宅勤務用端末を会社貸与端末と、私用端末に分けて、利用状況およびセキュリティ対策を確認した。アンケート結果をみると、9 割強の先が在宅勤務に際して会社貸与端末を利用していた（図表 17）。方針発表後のセキュリティ対策をみると、マルウェア[14]対策ソフトの利用（8 割程度）が最も多く、最新のセキュリティパッ

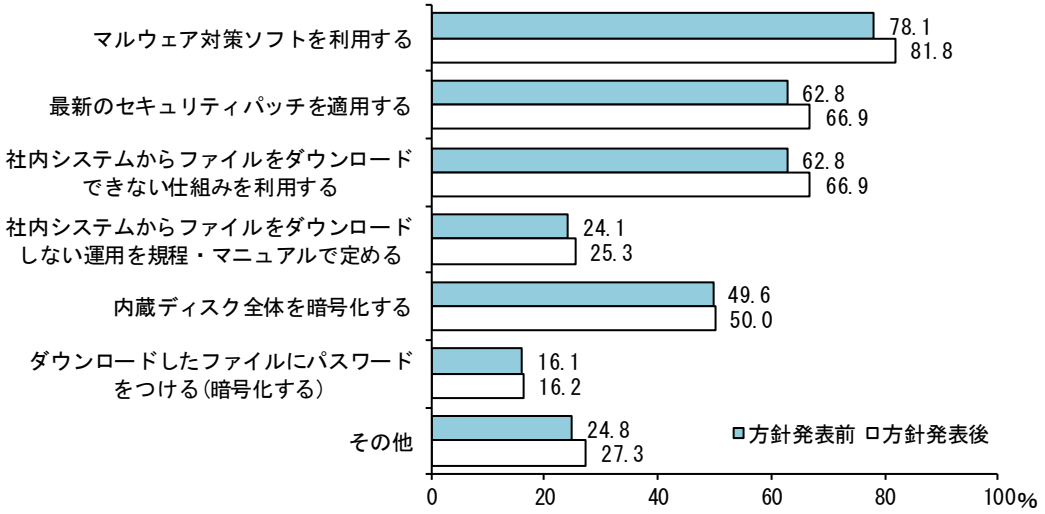
[14] 不正かつ有害な動作を行う意図で作成された悪意あるソフトウェアやコード（コンピュータプログラム）の総称。ウィルス、ワーム、トロイの木馬、スパイウェア、キーロガー、バックドア、ランサムウェアなどが含まれる。

チの適用および社内システムからファイルをダウンロードできない仕組みの利用（６～７割）が次いで多かった（図表 18）。会社貸与端末については、端末にデータを残さず、マルウェア感染リスクが限定的なシンクライアント端末を利用する先も相応にみられており、殆どの先で様々なセキュリティ対策を組み合わせながら必要なセキュリティを確保しようとしている様子が確認された。

図表 17 会社貸与端末の利用状況



図表 18 会社貸与端末のセキュリティ対策（複数回答可）

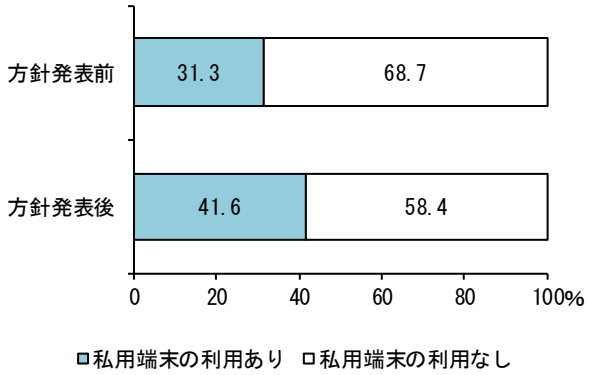


（注）分母は、会社貸与端末の持ち出しありの先。

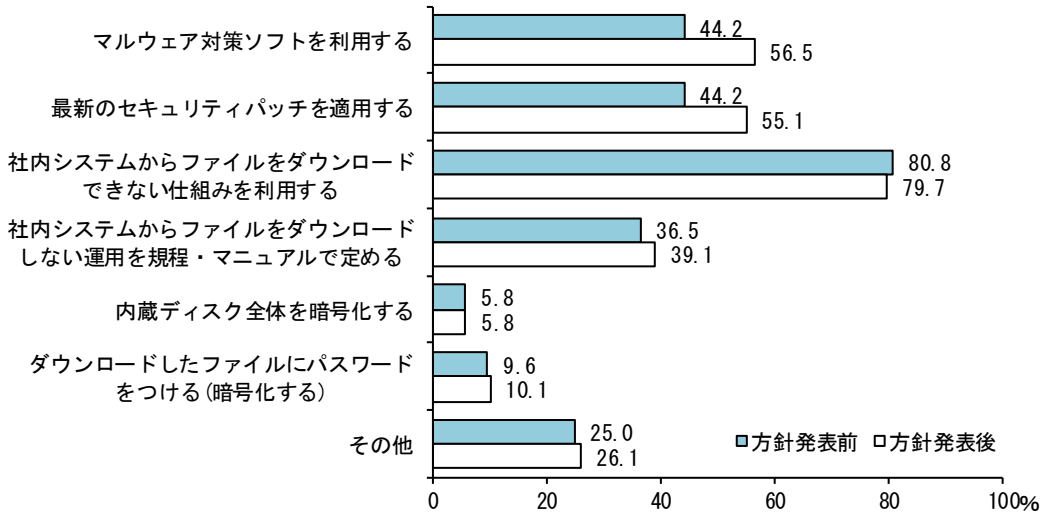
次に私用端末については、方針発表前は３割、方針発表後は４割程度の先が利用を認めているという結果となった（図表 19）。方針発表後のセキュリティ対策をみると、社内システムからファイルをダウンロードできない仕組みを利用している先がもっとも多かった（８割程度）。次いでマルウェア対策ソフトの利用や最新のセキュリティパッチの適用（５～６割程度）が多かったが、いずれも会社貸与端末と比較すると実施割合は低い結果となった（図表 20）。私用端末については、会社貸与端末と比較しセキュリティの統制がとりづらく、例えば

私用メールで不正な添付ファイルを開いたり、不正な Web ページを閲覧したりするなどしてマルウェアに感染することにより、社内システム接続時の ID やパスワードを窃取されてしまうといったリスクもある。こうした点を踏まえると、マルウェア対策ソフトやセキュリティパッチの適用についても、会社貸与端末と同程度の注意を払うことが必要と考えられる。

図表 19 私用端末の利用状況



図表 20 私用端末のセキュリティ対策（複数回答可）



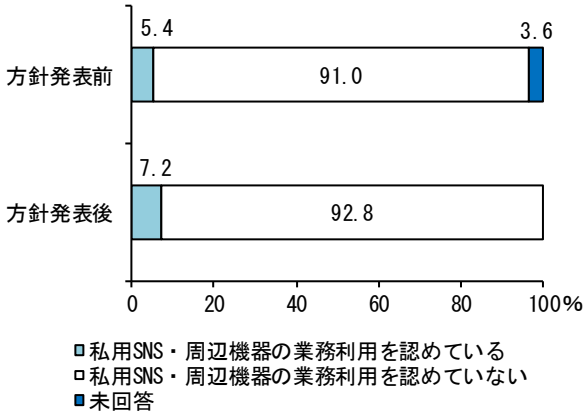
（注）分母は、私用端末の利用ありの先。

なお、在宅勤務において私用の SNS[15]・周辺機器の利用を認めているかという質問に対しては、ごく一部で私用のプリンタや記憶デバイス等の周辺機器の利用を認めている先がみられた[16]（図表 21）。利用を認めている先の多くは、利用時のルールの策定やユーザへの注意喚起といった対策を行っていたが、印刷物や記憶デバイスの紛失による情報漏えいなど、リスクは小さくないため、利用者に策定したルールを遵守させるなど、適切な運用を徹底することが求められる。

[15] Social Networking Service の略。テキストチャットや電子メール等、外部とのコミュニケーションが行えるサービス・ツール。

[16] 他方、私用の SNS の利用はほぼみられなかった。

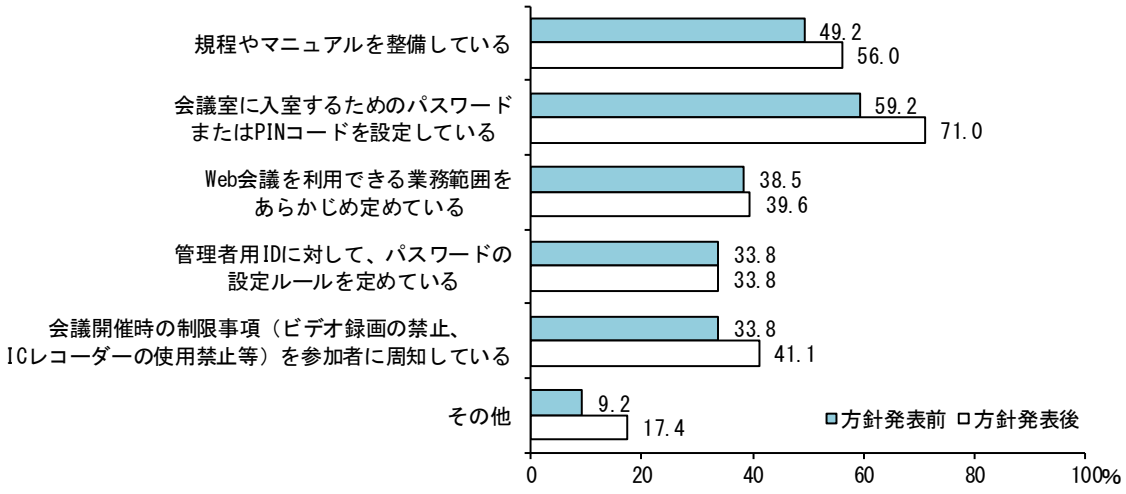
図表 21 私用 SNS・周辺機器の利用状況



（4）Web 会議サービス利用時のセキュリティ対策

Web 会議サービス利用時のセキュリティ対策をみると、会議参加時にパスワードまたは PIN コード[17]を設定している先は 7 割程度、サービスの利用にかかる規程やマニュアルを整備している先は半数程度という結果となった（図表 22）。Web 会議には、第三者が不正に会議に参加することにより機密情報が窃取されてしまうリスクもあることから、会議室への入室制限や利用できる業務範囲の設定など、サービスの機能や用途も踏まえた適切なセキュリティ対策を規程やマニュアルで定めることにより、会議が安全に行われる体制を早期に整えることが必要と考えられる。

図表 22 Web 会議のセキュリティ対策（複数回答可）



（注）分母は、Web 会議サービスを利用している先。

[17] Personal Identification Number の略。暗証番号。

４．在宅勤務の今後の活用方針と活用に向けた課題

本アンケート調査では、システム対応やセキュリティ対策に加え、在宅勤務の今後の活用方針や、活用を展望するうえでの課題についても、自由記入の形で調査した。

まず、今後の活用方針については、新型コロナウイルス感染拡大への対応など業務継続の観点だけではなく、働き方改革の観点からも活用を進めていくという先が多くみられたほか、対象業務や対象職員を拡大し、在宅勤務比率を引き上げられる体制を整備するという先もみられた。在宅勤務制度のない先では、制度や必要となるシステムインフラの整備などについて今後検討を進めるとした先が多くみられた（図表 23）。

図表 23　在宅勤務の今後の活用方針（調査先から聞かれた主な回答内容）

働き方改革	・新型コロナウイルス等感染症対策に加え、働き方改革の観点も盛り込んだ在宅勤務制度を策定予定。 ・今般、緊急対応措置として在宅勤務を実施したが、今後は、平常時での在宅勤務の活用について働き方改革の観点から検討する。
対象業務・対象職員の拡大	・現状在宅勤務ができない業務についても、ペーパーレス化の促進やシステム環境の整備等により、在宅勤務で実施可能とするよう検討を進める。 ・これまで在宅勤務の対象者を一部に限定してきたが、新型コロナウイルスの感染拡大への対応として緊急的に対象者を拡げたこともあり、全役職員を対象者とするよう制度の見直しを実施する。
制度の新設・整備	・新型コロナウイルスの感染拡大への対応のため、制度のない中で在宅勤務を実施してきたが、今後制度化するとともに、必要なシステムインフラを整備する予定。

また、さらなる活用に当たっては、押印等の紙を前提とした事務フローの見直し、在宅勤務用端末の増加や社内システムへの接続環境の改善などのシステムの整備・能力増強、個人情報の取扱い等情報管理体制の整備、システムのセキュリティ確保、コミュニケーションの円滑化、労働時間の把握や長時間労働化への対応等の労務管理や、職員の目標設定等の人事管理など様々な課題が挙げられた。また、一部の先からは、勘定系システムや日銀ネット端末等の操作のために出社の必要性が生じているとの声も聞かれた（図表 24）。

図表 24　在宅勤務のさらなる活用に向けた課題（調査先から聞かれた主な回答内容）

事務フローの見直し	・ペーパーレス化など押印や郵送等紙による処理を前提とした事務フローの見直しが必要。
システムの整備・能力増強	・自宅から社内システムに接続するためのネットワーク機器を増強する必要がある。 ・在宅勤務用端末が不足しており、台数の確保が必要。
自社拠点のみに設置されているシステムへの対応	・社内の勘定系システムや日銀ネット等については端末等の操作のために出社が必要。
セキュリティの確保	・新型コロナウイルスの感染拡大を受け、在宅勤務用のシステム環境を整備した結果、セキュリティリスクは高まっており、セキュリティ対策の重要性は増している。
情報管理体制の整備	・個人情報等機密性の高い情報を扱う事務について、セキュリティを確保しつつどこまで行うことができるか検討が必要。
コミュニケーションの円滑化	・職員間のコミュニケーション不足による業務品質や生産性の低下への対応のため、新たなコミュニケーションのあり方の検討やツールの整備が必要。
労務管理、人事管理	・労働時間の把握や、勤務時間とプライベート時間があいまいになることによる長時間労働化への対応。 ・在宅勤務の長期化に伴う職員のメンタルヘルスケア。 ・職員の目標設定や評価。

Ⅲ．おわりに

アンケート結果から、今般の新型コロナウイルスへの対応の中で、金融機関における在宅勤務の利用が大きく拡がったことが確認されたほか、今後についても、働き方改革も含めた制度の整備や対象業務・対象職員の拡大など、多くの先で活用を推進していくという声が聞かれた。

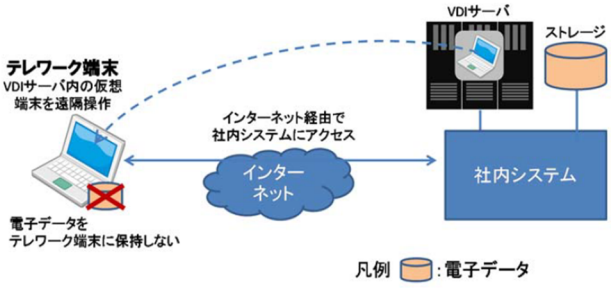
感染拡大の防止を図りつつ金融機関業務を継続するうえで、在宅勤務の有用性が確認された。一方で、在宅勤務に伴う社内システムへの不正アクセスや情報漏えいなどセキュリティ面のリスクも改めて指摘されている。金融機関においては、重要な社会インフラを提供する事業者として、セキュリティや業務継続など様々な観点からそのリスクと効果を見極めつつ、在宅勤務のさらなる活用を含めた業務継続力の向上に取り組むことが求められる。

日本銀行としても、今後も考査・モニタリングやセミナーなどを通じて、金融機関の取り組みを後押ししていく方針である。

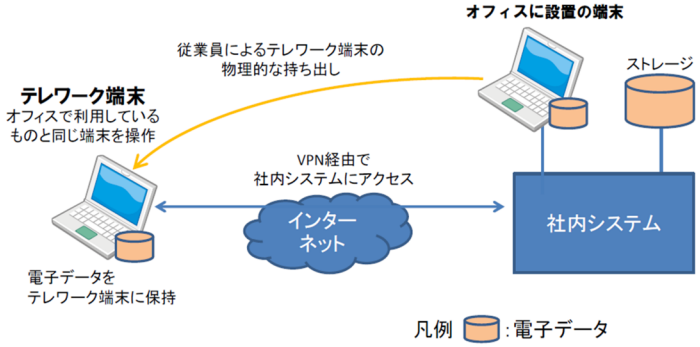
（別　　紙）

社内システムへの接続方式[18]

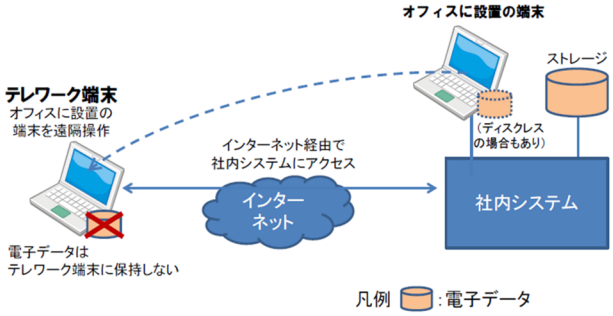
仮想デスクトップ方式
オフィスのサーバ上で提供される仮想デスクトップ基盤（VDI）に、テレワーク端末から遠隔でログインして利用する方式。



会社PC持ち帰り方式
オフィスで用いている端末をテレワーク先に持ち出し、VPNで接続して作業を行う方式。

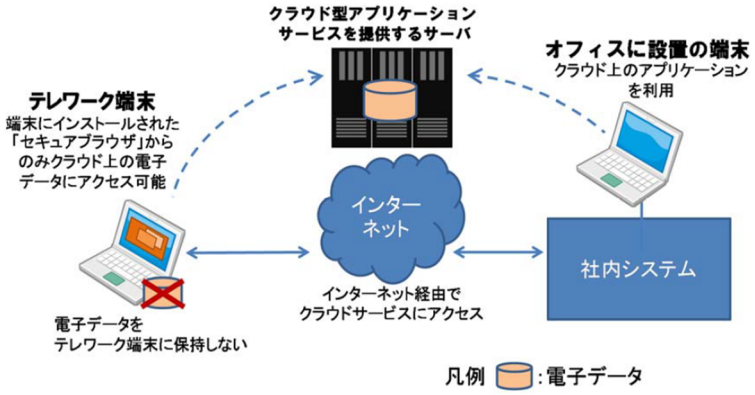


リモートデスクトップ方式
オフィスに設置された端末のデスクトップ環境を、テレワーク端末から遠隔操作したり閲覧したりする方式。

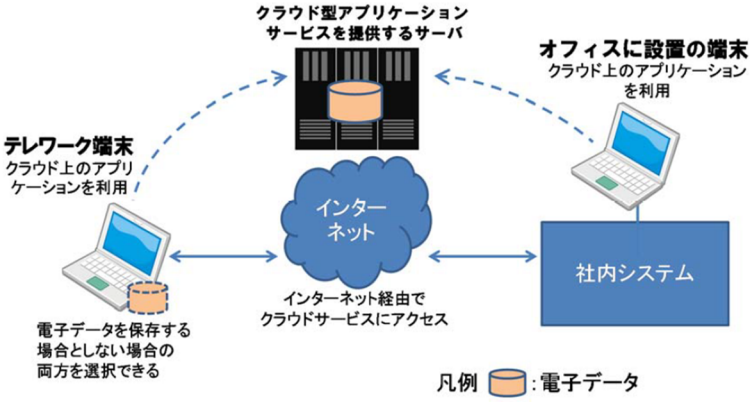


[18] 総務省「テレワークセキュリティガイドライン第４版」（https://www.soumu.go.jp/main_content/000545372.pdf）を加工して作成。

セキュアブラウザ方式
クラウド型アプリ方式の安全性を高めた方式。ドキュメントやデータをデバイス上の安全な領域で表示し、終了時に自動的に消去することでリスクを回避している。



クラウドアプリ方式
オフィスかテレワーク環境かどうかを問わず、インターネットで接続されている環境からクラウドサーバ上で提供されるアプリケーションにアクセスすることにより、作業を行う方式。



アプリケーションラッピング方式
テレワーク端末内に、ローカルの環境とは独立した仮想的な環境(コンテナ等)を設けて、その中でテレワーク業務用のアプリケーションを動作させる方式。