別紙4

登録調査機関のセキュリティに関するガイドライン

1. セキュリティ基準の策定

セキュリティに関する基本方針が策定されると共に、セキュリティの対象物が明確に規定されていること

（適切な例）

・セキュリティの対象物として、少なくとも出願書類等（出願書類、調査業務の納品物（検索報告書（作成途中のものも含む）、引用文献等）、及び、業務上入手した文献資料）及びこれらの電子データや業務上知り得た情報等が該当すること、及びそれらの保護方針が明確に記載されている。

・情報の漏洩に該当する状態（許可を得ていない書類の持ち出し、FAX・電子メールの誤送等）を明確に記載している。

・非特許文献が、特許庁から発注した特許審査に係る業務（以下「庁発注業務」）以外の目的のために使用されないよう記載している。

2. セキュリティに関する体制の整備

セキュリティに関する組織体制を構築していること

（適切な例）

・セキュリティ管理責任者が配置されている。

・セキュリティ管理責任者が明示されている。

・責任区分によって階層化された管理組織体制となっている。

3. 秘密保持義務に関する強化

調査業務従事者（調査業務実施者の他、雇用契約を結んでいない者も含む）と守秘に関する何らかの秘密保持契約を結んでいること

（適切な例）

・調査業務従事者に対し機密保持契約書等（秘密保持契約書、誓約書含む）に署名（捺印）を求める等の措置がとられている。また、機密保持契約書等の管理を行っている。

・秘密保持契約を結ぶ調査業務従事者に契約社員、アルバイト、パートタイム等も含めている。

・調査業務従事者のうち調査業務実施者には、特例法上、秘密保持義務が課され、刑法上の罰則があることを、契約時に重要事項として伝達している。

・退職後についても秘密保持規定が有効なものである。

・業務に関する書類や業務上知り得た知見・情報等を、調査業務従事者以外の者に開示・漏洩する行為に関する制限について記載されている。

・業務に関する書類や業務上知り得た情報等の開示・漏洩に対する罰則、損害賠償についても記載されている（就業規則での規定も可）。

4. 執務室の区別の明確化

庁発注業務と他の業務を行う場所とが明確に区別されていること

（適切な例）
・庁発注業務を行う執務室と他の業務を行う執務室とが明確に区別されている。
・庁発注業務用端末（以下、「業務用端末」という）が他の業務を行う端末と区別された区画に配置されている。
・調査業務従事者が庁発注業務を行う区画内で庁発注業務又は特許庁から許可を得た業務以外の業務を行っていない。
・外来者との面会（打ち合わせ）場所は庁発注業務を行う場所と隔離されている。
・庁発注業務について、会議、打ち合わせ等の会話が執務室外に漏れ聞こえることがない。

5. 入退室管理の徹底

調査業務実施者等の入退室の管理が何らかの方法で適切に行われていること

（適切な例）
・執務室内に外来者や業者等の部外者が通常立ち入らない。
・入退室時に ID カード認証や静脈認証、又は暗証番号の入力等の入退室管理が行われ、その記録が保存・管理されている。
・部外者に対しては、身分或いは用務を確認のうえ解鍵を行う等の入退室管理が行われ、その記録が保存・管理されている。
・建物の出入口又は執務室の出入口に警備員の配置や監視カメラの設置をする等、人の出入りに関する対策を講じている。
・深夜や休日には別段の入退室管理が行われている。

（望ましい例）
・同一ビル、又は同一フロアに他の会社等が入居していない。
・監視カメラを設置している場合、必要に応じてその記録を確認できる仕組みが整っている。

6. 情報システムに関する対策の徹底

調査業務従事者のうち調査業務実施者以外の者が業務用端末及びテレワーク用端末を操作しないこと（庁発注業務上必要な場合は除く）、また業務用端末及びテレワーク用端末に対するコンピュータウイルス及び外部からのアクセスに関する対策が適切になされていること

さらに、インターネット用端末、その他電磁的記録媒体については、インターネットに接続されるなど業務用端末及びテレワーク用端末とセキュリティ面での差異があることを考慮した上で、コンピュータウイルス及び外部からのアクセス等に関する対策が適切になされていること

（適切な例）
【業務用端末、テレワーク用端末、インターネット用端末に関する共通事項】
・パスワードが適切に管理されている。
・USB 機器による外部への不正な情報持ち出しをしないことを徹底している。
・ウイルス対策ソフトが導入されている。またその更新周期等を明確に規定している。

【業務用端末に関する事項】

・全調査業務従事者に対して、業務用端末の利用が以下に限られていることを周知徹底している。

1）調査業務実施者が、庁発注業務を行う場合。

2）調査業務実施者が、調査業務能力の向上のための研修を行う場合。

3）調査業務実施者育成研修受講中の者が、研修を行う場合。

4）調査業務実施者が、調査業務外注事業公募への応募にあたり、事前調査を行う場合。

5）調査業務従事者が、調査業務実施者の命により、庁発注業務を行う際の下準備（注）を行う場合。

（注）業務用端末の電源ON／OFF、調査業務対象出願明細書中に先行技術として記載された文献のプリントアウト、といった調査業務実施者としての能力・判断を要しないもの。

・ICカードについて破損・紛失・盗難を防止するような適切な管理がされている。特定登録調査機関用のICカード（庁からの貸与物）は別に管理されている。

・業務用端末を他のネットワークへ接続していない。

【テレワーク用端末に関する事項】

・全調査業務従事者に対して、テレワーク用端末の利用が以下に限られていることを周知徹底している。

1） 調査業務実施者が、庁発注業務を行う場合。

2） 調査業務実施者が、調査業務能力の向上のための研修を行う場合。

3） 調査業務実施者育成研修受講中の者が、研修を行う場合。

4）調査業務実施者が、調査業務外注事業公募への応募にあたり、事前調査を行う場合。

・ICカードについて破損・紛失・盗難を防止するような適切な管理がされている。

・テレワーク用端末を他のネットワークへ接続していない。

・テレワーク用端末を紛失しない安全確実な方法がとられている。

【インターネット用端末に関する事項】

・安全性が疑われるアプリは導入・利用しない。

・OS やアプリ等は常に最新のものに更新し、改造を行わない。

・ウイルス対策ソフトの導入・自動スキャンが可能なものは、これを実施する。

・無線 LAN を利用する場合は、適切な暗号化方式を利用し、信頼できるアクセスポイントに接続する。その際、暗号化方式として WPA2 又は WPA3 の利用を調査業務従事者に推奨すること。

【クラウドサービスに関する事項】

・調査業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、別途規程等で定め

る不正アクセス対策を実施するなど規程等を遵守すること。
・本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」のISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とすること。
・クラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

7. 出願書類等及び電子データの管理に関する対策の徹底

出願書類等（出願書類、調査業務の納品物（検索報告書（作成途中のものも含む）、引用文献等）、及び、業務上入手した文献資料）及びこれらの電子データの管理（保管、廃棄等）を厳重に行っていること

（適切な例）

【保存に関する事項】

（電子データ）
・電子データを保存する場合は、アクセス制限を設定する、パスワードを用いて保護する、暗号化を行う等、適切に管理している。
・電子データを保存した機器等について、盗難及び不正な持ち出し等を防ぐ対策をしている。
・電子データについて、どの出願に対応した電子データであるか分かるように管理（例えば、出願番号をフォルダ名とするフォルダ内に当該出願番号の案件に対応する全ての電子データ格納する）している。

（紙）
・出願書類等の保管には、専用の鍵付き書庫が使用されている。
・終業時には在宅勤務のために持ち出したものを除く全ての出願書類等が専用の書庫に格納され、必ず施錠されている。鍵についても適切に管理されている。

【持出し等に関する事項】

（紙・電子データ共通）
・少なくとも特許庁への納入または返却あるいは在宅勤務を目的とした場合以外においては、出願書類等及び電子データの持ち出しを禁止している。また、持ち出しを行う場合は、1件ごとに管理者の許可を得ている。
・特許庁への納入または返却あるいは在宅勤務を目的として出願書類等、電子データまたは IC カードを運搬する場合は、紛失や盗難を防ぐ安全確実な方法で行う。調査業務実施者自身が運搬する場合の注意事項が定められている。

（電子データ）
・電子データを保存した電磁的記録媒体を運搬する場合には、情報の暗号化を行う、パスワード機能を備える電磁的記録媒体を利用する等の情報漏えいを防ぐための対策をしている。

【廃棄に関する事項】

（紙・電子データ共通）

・出願書類等及び電子データの廃棄について、どの出願に対応した出願書類等及び電子データを廃棄したのかを管理し、廃棄の有無を随時確認できる状況にある。

（電子データ）

・電子データを記録した電磁的記録媒体を廃棄する場合には、記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消している。

（紙）

・出願書類等を情報が漏洩しない形で廃棄するための設備が備わっている。

【その他】

（インターネット検索等）

・検索報告書の判断に係る事項が第三者に漏洩することのないよう、インターネット検索を行う際の検索式・検索語等や、クラウドサービスの生成AIへ入力するプロンプト等に注意することが定められている。

（紙・電子データ共通）

・複製についての制限や複写物の管理について定められている。

（電子データ）

・電子データを電子メール等で送信する場合は、安全確保に留意して送信の手段を決定し、誤送信の防止や、添付ファイルをパスワードで暗号化する等、安全確保のための適切な対策を行っている。

（媒体一般）

・特許庁への出願書類等の宅配便業者を利用した発送時の誤配送を防止するための対策を行っている。

8．セキュリティに関する教育の実施

セキュリティ教育が全調査業務従事者に広く行われていること

（適切な例）

・調査業務従事者を対象とした研修カリキュラムの中にセキュリティに関する内容が盛り込まれている。セキュリティに関する教育を定期的に実施している。

・全調査業務従事者がセキュリティ基準を承知している。

9．セキュリティに関するリスク管理の実施（事故処理への対応）

災害や盗難等で業務に関する書類等を紛失した場合、または、システム上、ウイルス感染が発生した場合及びハッキングされた場合の具体的な対応策について検討がなされていること

（適切な例）

・想定し得る災害等に対応した対策がマニュアルに記載されている。

・バックアップやリカバリに対する規定が存在する。

10．セキュリティに関する内部監査の実施

セキュリティ管理策の実行及び効果を定期的に監査していること
（適切な例）
・監査責任者が配置されている。
・定期的に監査が行われている。
・監査記録が保存されている。

なお、調査業務実施者が在宅勤務又は Teams 対話を実施する場合のセキュリティについては、別添1又は別添2に記載のセキュリティ基準に従うこととする。また、その他事項のセキュリティについて、審査推進室が別途セキュリティ基準を定めた場合には、当該基準に従うこととする。

令和7年12月12日　改訂

調査業務実施者が在宅勤務を行う場合の情報セキュリティ対策基準

調査業務実施者が自宅等にてテレワークを実施する場合には、本基準又は本基準と同等の基準を満たす必要がある。調査業務指導者が調査業務実施者の業務を行う場合も同様とする。

I. 実施場所・環境

セキュリティ確保や業務の円滑な実施等の観点から、執務室と同等の環境として、以下の3つの点が確保された自宅または実家、登録調査機関で管理されているサテライトオフィスとする（サテライトオフィスは、事前に特許庁が業務の実施を認めたものに限る）。要件を満たさない場合は、いかなる場所であってもテレワークを実施することは認められない。

(1) 情報の機密性が守られる環境であること。PC 画面を覗かれる危険性、電話やウェブ会議に際しての音声が漏れ、紙の書類等の盗み見・紛失の危険性がないよう、十分な注意を払うこと。
(2) 業務に専念できる環境にあること。（セキュア PC を利用することができる高速のインターネット回線があること。育児や介護による業務への支障が生じないような措置が講じられていること、等）
(3) 安全が確保された環境であること。なお、実施中の安全衛生管理については、自己の責任をもって当たること。
(4) 庁発注業務と他の業務を区別される環境であること。

II. テレワークで行えない業務

調査業務実施者は、以下の事項を、テレワークにおいて実施することができない。

① テレワーク用端末とインターネット系端末との間で、データの移行を行うこと。
自宅等の環境で、データの移行はできない。出勤時に執務室で、上長の承認を得た上で、テレワーク端末とインターネット系端末との間で、データの移行を行う。
② 区分40に関する一切の業務。
③ テレワーク用端末で、自宅のプリンターにより印刷を行うこと。

III.. テレワークで行うことができる業務

調査業務実施者は、Ⅱ．の業務を除き、執務室において業務用端末を用いて行うことができる業務と同様の業務を、テレワークにおいて実施することができる。

以下の、1．～8．に実施することができる業務を示す。2．～7．の業務については、1．で充足すべき条件を満たした上で、各業務内容に応じた追加の条件を満たす必要がある。なお、機密情報に該当しない書類と該当する書類は以下の通りとする。

(1) 機密情報に該当しない書類

- 公報や公開済みの技術文献の電子データ（紙の場合も同様）

(2) 機密情報に該当する書類

- 出願関係書類、検索履歴を記載した書類、検索報告書、書き込み済み公報・技術文献、審査官向け説明資料の電子データ（紙の場合も同様）
- 検索報告書作成のためのロジックや新規性進歩性の判断等の、庁発注業務に関する文章の書き込みがされた書類の電子データ（紙の場合も同様）

<u>○書類作成等の業務</u>

1．機密情報を扱わず、テレワーク用端末を持ち出すことなく行うことができる補助業務

【業務内容例】

- 本願情報を確認したり、本願明細書、公報や技術文献に下線を引く、色分けをしたりすること。
- 検索報告書作成のためのロジックを検討すること。
- インターネット用端末にて、J-PlatPat での検索及びインターネットを用いた一般的な検索を行うこと。
- メールで審査官や調査業務指導者等と事務連絡を行うこと。

【充足すべき条件】

（情報機器端末）

制限なし

（登録調査機関による管理）

- 調査業務実施者に在宅で行う調査業務の対象案件を事前登録させること。
- 調査業務実施者の在宅勤務の状況を管理簿等により管理すること。

（持出可能な電子データ又は書類）

- 書き込みがされていない公報（本願の公報も含む）や技術文献。ただし、調査業務の対象出願が特定されないこと、及び、検索報告書で提示文献として提示することが特定されないことを要する。

2．検索報告書以外の機密情報を扱う業務（テレワーク用端末を持ち出して行う業務も該当）

【業務内容例】

- 機密情報に該当する書類を持ち出して、業務をすること。

- 公報（本願の公報も含む）や技術文献に文章の書き込み（検索報告書作成のためのロジックの記載、新規性進歩性の判断の記載等）をすること。（下線、色分けは１．）
- 審査官向け説明資料（引用例との対比表など）を作成すること。
- テレワーク用端末を用いて業務を行うこと。

【充足すべき条件として追加する条件】
（登録調査機関による管理）
- 調査業務実施者が機密情報及びテレワーク端末を持ち出す場合は事前登録させること。
- 機密情報及びテレワーク端末を運搬する場合には、紛失や盗難を防ぐ安全確実な方法で行うこと。
- 調査業務実施者が機密情報に該当する書類を登録調査機関に持ち帰った際に、紛失書類の有無について確認すること。
- 上記の事項を管理簿等により管理すること。

（持出可能な電子データ又は書類）
- 制限なし

３．検索報告書を扱う業務
【業務内容】
- クラスタ検索システムでの検索結果に基づいて検索報告書を作成すること。
- 商用データベースを利用した検索結果に基づいて検索報告書を作成すること。この場合、審査推進室長が在宅での使用を認めた商用データベースについては、在宅での検索結果に基づいて検索報告書を作成することができる。ただし、手順書で検索履歴の記録や提出について規定されている場合は、当該規定にも従うこと。また、７．に記載の「IP アドレス認証方式による商用データベースを利用する業務」を行うことが認められている場合には、検索履歴の記録や提出を求めている商用データベースについても、在宅での検索結果に基づいて検索報告書を作成することができる。

【充足すべき条件として追加する条件】
以下の①から③の内、該当する事項を充足すること。
① 登録調査機関が用意した情報機器端末（テレワーク用端末以外）を用いる場合
（情報機器端末）
- 登録調査機関が用意したセキュアな情報機器端末（端末の利用に当たり認証を要し、端末内に暗号化されない状態で情報が残らない機器）を用いること。調査業務実施者が所有する情報機器端末を使用することはできない。

（登録調査機関による管理）
- 調査業務実施者が、出願関係書類及び検索履歴、審査官向け説明資料、検索報告書の電子データを持ち出す場合は事前登録させること。

- 要機密情報（出願関係書類、検索履歴、書き込み済み公報・技術文献、審査官向け説明資料、検索報告書）の電子データを扱う場合は、以下のいずれかの方法とすること。また、情報機器端末や外部電磁的記録媒体を運搬する場合は、情報の暗号化を行い、紛失や盗難を防ぐ安全確実な方法で行う。
  （1）セキュアな情報機器端末内の記録装置に暗号化した状態で格納して移送するか、暗号化した状態で外部電磁的記録媒体に格納して移送する。
  （2）情報機器端末からオフィスネットワークに VPN 接続を行い、オフィスネットワーク内のファイルサーバに接続して移送する。
  （3）情報機器端末から登録調査機関に設置されたセキュアな情報機器端末に TLS（SSL）接続、IPsec 接続、SSH 接続等による通信の暗号化を実施して接続し、在宅勤務先の情報機器端末からセキュアな情報機器端末をリモートアクセスにより操作する。
  （4）7. に記載の「IP アドレス認証方式による商用データベースを利用する業務」を行うことが認められている場合に、これを用いて移送する。
  （5）審査推進室による利用承認を得たクラウドサービスを利用して、電子データの移送や編集を行う。
- 上記の各事項を管理簿等により管理すること。
- 情報機器端末及び外部電磁的記録媒体の調査業務実施者への貸し出しについて管理簿等で管理すること。

② テレワーク用端末を用いる場合

（情報機器端末）

- テレワーク用端末を用いること。

（登録調査機関による管理）

- テレワーク用端末の調査業務実施者への貸し出しについて管理簿等で管理すること。
- テレワーク端末を運搬する場合には、紛失や盗難を防ぐ安全確実な方法で行うこと。

③ 調査業務実施者が所有する情報機器端末を用いる場合

1. 及び6. の条件に加えて、以下の条件を充足した場合に、調査業務実施者が所有する情報機器端末を用いることができる。

（情報機器端末）

- 在宅勤務先の情報機器端末から登録調査機関に設置されたセキュアな情報機器端末に TLS（SSL）接続、IPsec 接続、SSH 接続等による通信の暗号化を実施して接続し、在宅勤務先の情報機器端末からセキュアな情報機器端末をリモートアクセスにより操作して、セキュアな情報機器端末内で検索報告書を作成すること。

（登録調査機関による管理）

- 在宅勤務先の情報機器端末とセキュアな情報機器端末の間でファイルの転送、ク

リップボードの共有、デバイスの共有を禁止する設定とし、その設定方法について特許庁に報告すること。

なお、手順書に従って本事業で利用できる商用データベースを用いて調査業務を実施した場合を除き、クラスタ検索システムで検索及びスクリーニングをした履歴のない検索結果に基づいて検索報告書を作成することは認めない。

４．電話やメール等で、審査官や調査業務指導者等と連絡を行う業務
【業務内容例】
- 審査官と、対話の日程調整や案件に対する相談を行うこと。
- 調査業務指導者と事務連絡を行うこと。

【充足すべき条件として追加する条件】
（登録調査機関による管理）
- 調査業務実施者が、電話やメール等で、案件に関する相談を行う場合は、情報漏洩が起きないように、安全確実な方法で行うこと。

<u>○検索関連の業務</u>

５．スクリーニング業務
【業務内容】
- テレワーク用端末を用いて、クラスタ検索システムでのスクリーニングを行うこと。（充足すべき条件として追加する条件①を参照）
- 登録調査機関が用意したスクリーニングツールを用いてスクリーニングを行うこと。（充足すべき条件として追加する条件②を参照）

【充足すべき条件として追加する条件①】
（情報機器端末）
テレワーク用端末を用いること。

（登録調査機関による管理）
- テレワーク用端末の調査業務実施者への貸し出しについて管理簿等で管理すること。
- テレワーク端末を運搬する場合には、紛失や盗難を防ぐ安全確実な方法で行うこと。

【充足すべき条件として追加する条件②】
１．及び６．の条件に加えて、以下の条件を充足した場合に、在宅でのスクリーニングによりクラスタ検索システムでのスクリーニングを補完することができる。
（スクリーニングツールとその利用方法）
- 登録調査機関において以下の要件を満たすスクリーニングツールを用意し、調査業務実施者は当該スクリーニングツールを用いてスクリーニングを実施すること。

・実際にスクリーニングを行った特許文献の履歴（以下「スクリーニング履歴」という。）を生成するものであること。
・スクリーニング履歴の改ざんを防ぐ措置が取られていること。

- 当該スクリーニングツールを用いてスクリーニングを実施した後、クラスタ検索システムにおいて、対象案件を「審査対象案件」に登録した上で、スクリーニング履歴から抽出される文献集合をクラスタ検索システムへファイル入力すること（ファイル入力については、特実検索システムマニュアルを参照）。
- 文献抽出に用いた検索式をクラスタ検索システムにおいて再現し、移行した文献集合との差分をクラスタ検索システムによりスクリーニングすること（文献抽出に用いたデータベースの差異により、抽出される文献にも差異が生じる可能性があるため）。

（登録調査機関による管理）

- スクリーニングツールの保守・管理を行うこと。
- 当該案件の少なくとも納品後１年はスクリーニング履歴を保管すること。
- 特許庁がスクリーニング履歴の提出を求めた場合には、電子データにて速やかに提出できるようにすること。

６．パスワード認証方式による商用データベースを利用する業務

【業務内容】

- 情報機器端末を用いて、審査推進室長が在宅での利用を認めた商用データベースをパスワード認証方式により利用して検索を行うこと。
- J-PlatPat での検索及びインターネットを用いた検索を行うこと。

【充足すべき条件として追加する条件】

（情報機器端末）

＜ソフトウェア＞

- 安全性が疑われるアプリは導入・利用しないこと。
- ＯＳやアプリ等は常に最新のものに更新し（業務利用に支障が生じるおそれがあるとして、審査推進室長や登録調査機関の情報セキュリティ責任者が指示した場合を除く。）、改造を行わないこと。
- ウイルス対策ソフトの導入・自動スキャンが可能なものは、これを実施すること。
- 無線LANを利用する場合は、適切な暗号化方式を利用し、信頼できるアクセスポイントに接続すること。その際、暗号化方式として WPA2 又は WPA3 の利用を調査業務実施者に推奨すること。

＜ハードウェア＞

- 利用する情報機器端末について、調査業務実施者は指導者等の責任ある者の許可を予め得ること。
- 家族等との共有は禁止する。ただし、サインインのアカウントを共有していない場合はこの限りでない。
- 一定時間操作しない場合に自動ロックするよう設定すること。

- パスワードを設定すること。

＜その他＞
- 業務利用の目的を完了した場合は、情報を当該情報機器端末から消去すること。

（登録調査機関による管理）
① 登録調査機関が用意した情報機器端末を用いる場合
- 情報機器端末を運搬する場合は、紛失や盗難を防ぐ安全確実な方法で行うこと。
- 情報機器端末の調査業務実施者への貸し出しについて管理簿等で管理すること。

② 調査業務実施者が所有する情報機器端末を用いる場合
- 利用可能な情報機器端末の条件について、調査業務実施者に常に参照可能な形で提示すること。
- 調査業務実施者等に利用を許可した情報機器端末の機種等について管理簿等で管理すること。

7. IP アドレス認証方式による商用データベースを利用する業務
【業務内容】
- 本事業で利用できることとされている商用データベースを IP アドレス認証により利用して検索を行うこと。

【充足すべき条件として追加する条件】
（情報機器端末）
- 6. に記載の「パスワード認証方式による商用データベースを利用する業務」ができる情報機器端末を用いること。
- 在宅勤務先の情報機器端末から登録調査機関の情報システムに TLS（SSL）接続、IPsec 接続、SSH 接続等による通信の暗号化を実施して接続すること。

<u>○対話関連の業務</u>

8. Teams を利用した対話業務
【業務内容】
- Teams を利用して対話を行うこと。

【充足すべき条件として追加する条件】
（情報機器端末）
- 6. に記載の「パスワード認証方式による商用データベースを利用する業務」ができる情報機器端末を用いること。
- 在宅勤務先の情報機器端末に、Teams アプリ/プラグインのインストールができること。

（登録調査機関による管理）

- 審査推進室において別途マニュアルに定めるオンライン対話に準じた管理を行うこと。

〇その他業務

上記１．～８．以外の業務についても、業務実施前に特許庁に確認し、特許庁が認めた業務については実施することができるものとする。

令和7年12月12日　改訂

別添2

Teams 対話におけるセキュリティ特則

Teams 対話は、以下の場所にて実施できることとする。

① 庁発注業務を行う執務室

② セキュリティガイドラインで定められる庁発注業務を行う執務室と同等のセキュリティ管理を行っている区画

③ 庁発注業務を行う執務室外であって、登録調査機関が管理する建物内の区画された部屋
ただし、以下の条件を満たすこと。
・Teams 対話を実施する時間帯には、庁発注の調査業務に従事しない者が立ち入らないようにする
・Teams 対話を実施する時間帯には、使用中である旨を出入り口に表記する
・部屋の外からは部屋内を覗うことができず、また、会話が部屋の外に漏れ聞こえることがない

④ 登録調査機関が管理していない（部屋の外側を不特定多数が出入りする）建物内の区画された部屋
ただし以下の条件を満たすこと。
・Teams 対話を実施する時間帯には、庁発注の調査業務に従事しない者が立ち入らないようにする
・入退室時にIDカードの利用、若しくは暗証番号の入力等の管理が行われている、又は内側から鍵がかけられる
・部屋の外からは部屋内を覗うことができず、また、会話が部屋の外に漏れ聞こえることがない

⑤ 調査業務実施者の自宅または実家、登録調査機関が管理しているサテライトオフィス。ただし、登録調査機関が定めた在宅勤務規程を満たすこと