別紙３

調査業務発注先及び発注件数の決定方法
並びに請負金額の決め方について

令和６年１２月
特許庁　審査第一部
調整課　審査推進室

１．はじめに

登録調査機関が行う先行技術文献調査は、審査官が効率的に特許審査を進めていく上で大変重要なものです。また、登録調査機関が請け負った調査業務については、特許庁からの発注に対し、必ず遅滞なく納入することが、特許庁が迅速な審査を滞りなく進める上で不可欠です。

これらを踏まえ、特許庁が調査業務を発注する際には、品質の高い調査業務を行うことができる能力、及び、特許庁からの発注に対する過去の納入実績や検索者等の働きやすい環境整備も重視しつつ、調査業務のより一層の効率化を図るために請負価格要素も考慮した上で、調査業務の発注先及び発注件数を決定します。

２．発注先等の決定方法の概要

発注先となる登録調査機関には、より品質の高い調査業務を行うことができ、かつ、発注に対して遅滞なく調査業務結果を納入できること、秘密情報を扱うための適格なセキュリティを保持していることに加え、継続的に業務を遂行できる財務的な安定性を備えていることや、特許庁からの連絡に対して迅速に対応する体制及び調査業務実施者を適切に指導する体制（以下、両者を「指導連絡体制」という）を備えていること等が求められます。

このため、調査業務を実施する登録調査機関は、調査業務の品質評価結果（審査官が各登録調査機関の調査業務の品質を評価した各区分における品質評価結果）が一定水準を超えていることに加え、適格な管理体制・セキュリティを保持していること、財務状況に安定性を有していること、及び適格な業務体制・連絡体制を保持していることが必須要件となります。各区分に新たに参入を希望する登録調査機関は、品質評価結果を得るために、事前に一定量の調査業務（以下「事前調査（トライアル）」という）を行い、その結果を審査官が評価することとします。事前調査を行わず、品質評価結果が得られない場合、新規参入は認められません。

同一区分で複数の登録調査機関から応募があった場合、上記に加え、各登録調査機関の当該区分における過去の納入実績、検索者等の働きやすい環境構築

並びに、請負価格要素としての、応募時に提示された当該区分における単価等に基づいて、登録調査機関の順位付けを行い、順位の高い登録調査機関から、受注希望換算件数（内国対話型換算）に応じて件数の割当てを行います。なお、技術点の高い機関が受注できない場合などには、特別換算件数が配分されます。また、発注先が１区分１機関のみとなった場合などは、補充換算件数が２機関目に配分されます。

発注件数のうち、オプション検索を実施する件数は、区分ごとに所定の割合で割り当てられますが、当該所定の割合は、令和７年度予算、審査請求件数、応募状況に応じて変動します。

第１次募集の結果、予算状況に余裕がある場合には、件数に残余がある区分について第２次募集を行うことがあります。第２次募集については、第１次募集において同区分に応募した登録調査機関のみ応募可能です。

３．選定会議について

発注先の登録調査機関の選定及び発注件数の割り当てを、適正かつ公正に行うため、特許庁外の弁理士、弁護士等の有識者の会議員からなる調査業務外注先選定会議を開催し、各登録調査機関の応募区分ごとの調査業務の品質、過去の納入実績、指導連絡体制、単価、さらに各登録調査機関のセキュリティの保持状況、財務状況の安定性等を評価していただきます。

〇 財務状況については、信用調査会社が調査を請け負います。
〇 セキュリティの保持については、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」をご参照ください。

４．請負金額の決め方について

請負金額は、登録調査機関ごとに見積書を提出していただき、特許庁が作成した予定価格の範囲内で決定されます。

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。

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】
（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。

（紙）

・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（PDF：289KB）又は別添2（PDF：79KB）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。

注：別添1（PDF：289KB）又は別添2（PDF：79KB）には、PDF ファイルが埋め込まれています。クリックすることでアクセスすることができます。

令和6年12月13日　改訂