仕　様　書

１．件名　　移転申請書のコード付与及び登録記事抽出作業等データ作成

２．作業目的

本作業は磁気原簿へ移転登録事項を記録するために、データ作成を実施するものである。

なお、移転登録における実施庁目標[1]を達成するためは、特許庁の指定する期間[2]（原則２開庁日）までにデータを納入することが必須である。

また、特許庁が指定する仕様に基づき、昭和 50 年代に作成された古いプログラミング言語（ＣＯＢＯＬ）により作成された特許庁の登録システムで処理可能な各種コードでの電子化作業を実施する必要がある。

３．作業内容

３．１．通常発注分

本作業について、以下の点に留意し（１）～（５）の作業を実施すること。

・１日の発注予定件数は、申請書１７５件程度（最大申請書件数は４００件程度を想定）、発注回数２４０回（令和８年４月１日から令和９年３月３０日の開庁日）について、日々滞りなく受注を行うこと。
・納入データは、（２）を除き、発注日の翌々開庁日までに本書で指定する方法で、納入回数２４０回（令和８年４月２日から令和９年３月３１日の開庁日）について、日々滞りなく納品を行うこと。（２）については、翌開庁日に納品すること。

（１）移転申請書コード付与・登録記事抽出作業及びデータ作成

移転コード及び項目コードの付与、原簿更正記事情報の抽出及びデータ作成を、「移転申請書　移転コード付与及び原簿更正記事情報抽出基準書」（以下「基準書」という。）に従い、以下のとおり作業を行う。Ｉ．～ＩＶ．の作業で付与された情報は、ＶＩ．の作業を行うため、及び納入後の庁担当者からの問い合わせに対応するため、定められた

[1] 実施庁目標とは、中央省庁等改革基本法 第 16 条第 6 項第 2 号に基づき、各年度に特許庁が達成すべき目標を 経済産業大臣が設定し、特許庁長官に通知した目標である。移転登録は不備のない手続又は不備が受付から 12 営業日以内に解消した手続について、受付から登録原簿への登録までの期間を 15 営業日以内」と定めている。

[2] 早期受付情報に関しては、原則「翌開庁日」に納品すること。

廃棄期日（発注日の翌月最終開庁日（契約最終月は、当月最終開庁日）までの間は事業者側にて保持すること。

＊別紙「参考資料１」を参照。

Ⅰ．移転コードの付与

『基準書３．移転コード付与基準』に従い、移転申請書（写し）（以下「申請書」という。）に記載されている「表題」、「権利の表示」、「登録の目的」、「一般承継か特定承継の別」から判断し、適切な移転コードを付与する。

なお、移転コードは、５桁の数字又は英数字で構成され、『基準書３．２．３移転コード付与条件』に示されている。

＊別紙「参考資料２」を参照。

ＩＩ．固定部の付与

上記（１）で付与した移転コードのほか、申請書に記載されている「受付日」、「受付番号」、「併合の有無」、「出直識別」（郵送、窓口またはオンラインの別）、「移転申請形態」（単独申請か双方申請の別）を付与する。

ＩＩＩ．項目コードの付与

『基準書４．項目コード付与基準』に従い、申請書に記載されている「特許番号」、「登録免許税」、「住所」、「氏名」、「持分」等に、適切な項目コードを付与する。

項目コードは、３桁の英数字（例外あり）で構成され、移転コードに基づき『基準書４．２．１様式：本権にかかる移転申請書【一般承継】』以降に示されている。

＊別紙「参考資料３（一部、抜粋）」を参照。

ＩＶ．原簿更正記事情報の抽出

『基準書４．項目コード付与基準』の申請書様式例を参照し、入力指示の内容に従い、申請書から原簿に記載するための更正記事情報を抽出する。

なお、『基準書５．２　氏名・住所に関する原簿更正記事情報抽出仕様書』に従い、抽出を行うこと。

＊別紙「参考資料３（一部、抜粋）」を参照。

Ⅴ．確認

上記Ⅰ．～ＩＶ．について、基準書に記載されている内容に基づき適正に行われているか確認する。

ＶＩ．データ作成

データはＭＱヘッダ部、固定部、可変部で構成される可変長データである。

『基準書６．原簿更正記事情報作成基準』に従い、移転コード、項目コード、原簿更正記事等のデータを作成する。

また、特許庁が指定するコードに対応しない文字等が発生した場合は、一文字ずつ置換記号を付して「ひらがな」に置き換えること。置換処理をしたデータについては、置換処理報告書を作成し提出すること。

データ入力の方法が不明な事項が発生した場合は、提出物の付箋リストを作成

すること。

＊別紙「参考資料４」を参照。

ＶＩＩ．データチェック

作成した電子データは、『基準書６．５データチェック基準』に従い、申請書単位でデータチェックを行う。

＊別紙「参考資料４」を参照。

（２）早期受付情報データの作成

早期受付情報データは８０バイト固定長である。

『基準書６．６早期受付情報データ』に従い、早期受付情報データ（特許（登録）番号データ）を作成（※）し、パスワードを付与して特許庁の指定するアドレスに電子メールで送付する。指定するアドレスは契約後に担当者が指示する。

※一発注の申請書内に同一登録番号が複数回出てくる場合も、全て（複数回分）作成する。

なお、暗号化については「14.納品する電子データについて」に記載の方法に従うこと。

＊別紙「参考資料５」を参照。

（３）手続補正書データの作成

手続補正書データは８０バイト固定長である。

特許庁から貸与された手続補正書（写し）について、『基準書６．８手続補正書データ』に従い、補正種別、四法、起案番号、受付日、受付番号を入力したデータを作成する。作成したデータは移転申請書の作成データ・移転送付先情報データとは別ファイルとして納品する。

なお、手続補正書（写し）の貸与がない場合は、０バイトデータを作成すること。

＊別紙「参考資料５」を参照。

（４）移転送付先情報データの作成

特許庁から貸与された申請書（手続補正書（写し）を除く）について、『基準書６．７移転送付先情報データ』に従い、四法、受付日、受付番号、送付先種別、送付先申請人ＩＤ等を入力したデータを作成する。作成したデータは移転申請書の作成データ・手続補正書データとは別ファイルとして納品する。

＊別紙「参考資料５」を参照。

３．２．職権訂正データ発注分

本作業について、以下に留意し、作業を実施すること。

・移転申請書（職権訂正）の電子化作業が発生した場合は、庁担当者が連絡するものとし、発注日および納入日を調整し、確実に納入すること。

・契約期間内における発注予定のファイル数は年間１２ファイル程度（１ファイル当た

りに包含される登録番号数は平均３６０件、最大８，１００件程度を想定)。なお、年間３～５回程度の発注を見込んでいる。

移転申請書（職権訂正）データの作成

発注ファイルを元に以下、Ｉ．およびＩＩ．に基づき、データ作成を行うこと。なお、１回の発注で同一の登録番号が複数存在する場合には、全件について作成すること。

Ｉ．ＭＱヘッダ部

『基準書７．移転申請書（職権訂正）データ』に記載された内容をもとにデータを作成すること。

ＭＱヘッダ部の後に実データ部が続くが、移転受付番号が変わるときは、再度ＭＱヘッダ部からデータを作成すること。

ＩＩ．実データ部

固定部・可変部ともに発注ファイルの発注シートと発注内訳シートに記載された内容に従い、データを作成すること。

なお、実データ部は、固定部の後に可変部が続くが、可変部は必要な項目コードの数だけ繰り返すため、発注内訳シートに記載された登録番号は、その数だけ可変部内で項目コードと登録番号を繰り返してデータを作成すること。

＊別紙「参考資料６」を参照。

４．発注予定件数

３．１．通常発注分

種　　別	予定件数
特　　許	１１，５００件
実用新案	４３０件
意　　匠	１，３６０件
商標（国際商標を含む）	２５，１００件 （うち、国際商標５０件）
手続補正書	３，３９０件
合　　計	４１，７８０件

※一発注の平均申請書件数：約１７５件（特許：４８件、実用：２件、意匠：６件、商標：１０５件、補正書：１４件）

※一発注における最大申請書件数は４００件を想定している。

※※発注予定件数は変動することがあり得るため、年間調達件数を保障するものではない。

３．２．職権訂正データ発注分

移転申請書(職権訂正)	１２回

※移転申請書（職権訂正）１回当たりの登録番号数は、平均３６０件、最大８，１００件程度を想定している。

※発注予定件数及び回数は、変動することがあり得るため、年間調達件数を保障するものではない。

５．契約期間

令和８年４月１日から令和９年３月３１日（２４１開庁日）とする。

６．発注物件及び発注方法

以下の物件を引き渡す。

６．１．通常発注分

（１）～（３）はＰＤＦファイルにパスワードを付与してＺＩＰ化し特許庁より電子メールで送付する。

（１）移転申請書等送付表・・・別紙「参考資料７」

（２）発注依頼書・移転送付票・・・別紙「参考資料７」

（３）発注書類（移転申請書（写し）、手続補正書（写し））・・・別紙「参考資料２，５」

※（１）～（３）は、作業終了後、提出した月の翌月にすみやかに廃棄すること。契約年度の最終月の分は、最終月末に廃棄すること。

６．２．職権訂正データ分

以下について、Ｅｘｃｅｌファイルにパスワードを付与してＺＩＰ化し特許庁より電子メールで送付する。

・発注ファイル・・・「参考資料１４」

※作業終了後、提出した月の翌月にすみやかに廃棄すること。契約年度の最終月の分は、最終月末に廃棄すること。

７．発注日時

・特許庁から、電子メールで毎日１６時３０分までに送付する。なお、送付後に移転申請書等に修正が発生した場合は、発注日の翌日１０時３０分までに修正が発生した分の移転申請書等のみ電子メールで送付する。

※発注件数が多い場合や連続した休日後に発注遅延が生じる場合は、当日の発注分については１３時００分まで、翌日の修正分については１０時００分までに連絡する。

※移転申請書（職権訂正）のデータ作成は、庁担当者からの連絡後、発注日時について、別途、調整すること。

８．貸与物

移転コード付与及び原簿更正記事情報抽出基準書
※作業終了後返却すること。

９．納入物件

以下の物件を提出および納入する。

（１）３．１．（１）移転申請書コード付与・登録記事抽出作業及びデータ、（３）手続補正書データ、（４）移転送付先情報データ、３．２．移転申請書（職権訂正）データ

※３．２．移転申請書（職権訂正）データは、発注があった時のみ納品すること。

（２）３．１．（２）早期受付情報データの作成で作成した電子データ

（３）移転データ納品リスト

ａ　移転データ案件リスト・・・・・・別紙「参考資料８」参照。

ｂ　移転データ合計件数リスト・・・・別紙「参考資料９」参照。

ｃ　移転データ合計文字数リスト・・・別紙「参考資料１０」参照。

（４）置換処理報告書・・・・・・・・・・・・別紙「参考資料１１」参照。

（５）付箋リスト・・・・・・・・・・・・・・別紙「参考資料１２」参照。

（６）移転データチェックリスト・・・・・・別紙「参考資料１３」参照。

（７）機密情報借用書、機密情報返却・廃棄報告書

（８）納品書

１０．納入方法

（１）９．提出物件および納入物件（１）、（２）については、以下、提出期日までに電子データにパスワードを付与してメールにて担当者に送付する。アドレスは契約後に担当者が指示する。

なお、データサイズが大きく、１通のメールによる送付が実施できない際は、庁担当者と協議すること。

（２）９．提出物件および納入物件（３）～（８）については、以下の期日までに電子データにパスワードを付与してメールにて担当者に送付する。アドレスは契約後に担当者が指示する。

納入期日　　９．納入物件（１）、（３）～（６）

原則、発注日の翌々日１３時００分まで

※移転申請書（職権訂正）データに関しては、提出期日を庁担当者と別途調整すること。

９．納入物件（２）

原則、発注日の翌日１３時００分まで

９．納入物件（７）、（８）

１ヶ月分をまとめて毎月月末開庁日に納入すること。

１１．発注・提出スケジュールについて

（１）提出物件は、原則発注日より２開庁日後の提出とする。（３．１．（２）早期受付情報データの作成で作成した電子データを除く）

ただし、令和８年４月１日に貸与する、３月３０日受付分・３月３１日受付分のうち、３月３０日分は提出を翌開庁日とすること。

また、令和９年３月３０日に貸与する、３月２９日受付分の発注物については、提出を翌開庁日とする。

（２）事前に、発注・提出スケジュール表（以下、発注・納品スケジュールという。）を渡す。

（３）災害等（政府の規制を含む）のやむを得ない事情がある場合は、発注・納品スケジュールの変更を協議して決定する。

１２．納品する電子データについて

形式：ＯｐｅｎＳＳＬ によるＡＥＳ２５６ＣＢＣ を使用し、ＯｐｅｎＳＳＬバージョン１．０．２ｒによる復号化が可能なよう暗号化を行った上で、以下に沿って納品すること。

ただし、令和９年１月４日以降の納入物件については、ＯｐｅｎＳＳＬによる暗号化を行わず納品すること。

（移転申請書データ）

ファイル名　　ＲＢＩ１１０

使用コード　　ＳＪＩＳ

（手続補正書データ）

ファイル名　　ＲＢＩ３Ａ０

使用コード　　ＳＪＩＳ

（移転送付先情報データ）

ファイル名　　ＲＢＩ１Ｊ０

使用コード　　ＳＪＩＳ

１３．情報セキュリティに関する事項

業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、仕様書別紙１「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

１４．情報管理体制について

（１）情報管理体制

① 受託者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体図」」及び「情報取扱者名簿」（氏名、住所、生年月日、所属部署、役職等が記載されたもの）を契約前に提出し、担当課室の同意を得ること。（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。）なお、情報取扱者名簿は、業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、特許庁が保護を要さないと確認するまでは、情報取扱者名簿に記載のあるもの以外に伝達又は漏えいされないことを保証する履行体制を有していること。

② 本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、担当課室の承認を得た場合は、この限りではない。

③ ①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め担当課室へ届出を行い、同意を得なければならない。

（２）履行完了後の情報の取扱い

特許庁から提供した資料又は特許庁が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。

１５．秘密の保持

（１）受託者は、本仕様以外にいかなる場合でも当該書類及び帳票類を使用してはならない。

（２）受託者は、当該発注及び納品に関する書類及び帳票類はその取り扱いを厳重に注意する。

（３）受託者は、契約締結後速やかに、当該業務及び情報セキュリティを確保するための体制を定めた体制図を提出すること。

（４）受託者は、貸与された紙媒体、電子媒体を、担当者の許可なく当庁外で複製してはならない。また、作業終了後には、複製した情報等が電子計算機等から消去されていることを担当者が確認できる方法で証明すること。

（５）受託者は、当庁が実施する監査を受け入れるとともに、指摘事項への対応を行うこと。

（６）受託者は、本作業を再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、契約等により再委託先に担保させること。

（７）上記のほか、個人情報の保護に関する法律（平成１５年法律第５７号）、政府機関の情報セキュリティ対策のための統一基準（内閣サイバーセキュリティセンター）、特許

庁個人情報保護管理規程及び特許庁情報セキュリティ運用細則等の関係法令及び規程を遵守しなければならない。

１６．仕様書の疑義

仕様書に疑義がある場合については、適宜担当者の指示に従い速やかに対処すること。

１７．課室情報セキュリティ責任者

特許庁審査業務部審査業務課登録室長　　伊藤　康雄

（なお、責任者に人事異動が生じた場合は、新たに配属となった者が課室情報セキュリティ責任者となるものとする。）

１８．庁担当者

特許庁審査業務部審査業務課登録室管理班管理第一係　　佐藤　萌花

（なお、庁担当者に人事異動が生じた場合は、新たに配属となった者が庁担当者となるものとする。）

１９．その他

（１）発注、納入にあたり特許庁の駐車場を使用する場合は、車両制限があるので注意すること。（特許庁庁舎は高さ制限２．８ｍ以下、２．２ｍ以下の場所有。）

（２）納入物等を作成する際、「国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）第 6 条第 1 項の規定に基づき定められた環境物品等の調達の推進に関する基本方針（令和 7 年 1 月 28 日変更閣議決定）」に定める印刷用紙の「判断の基準」を満たすこと。ただし、当該「判断の基準」を満たす製品を納入することが困難な場合には、特許庁担当者の了解を得た場合に限り、代替品の納入を認める。

○環境物品等の調達の推進に関する基本方針（令和 5 年 12 月 22 日変更閣議決定）

https://www.env.go.jp/content/000201733.pdf

○グリーン購入の調達者の手引き（令和 7 年 2 月）

https://www.env.go.jp/content/000311831.pdf

仕様書別紙１

情報セキュリティに関する事項

以下の事項について遵守すること。

【情報セキュリティ関連事項の確保体制および遵守状況の報告】

1) 受注者は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下 2)～17)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、特許庁（以下「当庁」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（別紙））を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

　なお、報告の内容について、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

【情報セキュリティ関連規程等の遵守】

2) 受注者は、「経済産業省情報セキュリティ管理規程（平成 18･03･22 シ第 1 号)」、「経済産業省情報セキュリティ対策基準（平成 18･03･24 シ第 1 号)」及び「政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版)」（以下「規程等」と総称する。)を遵守すること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

3) 受注者は、当庁又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

【情報セキュリティを確保するための体制】

4) 受注者は、本業務に従事する者を限定すること。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等)、実績及び国籍に関する情報を担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示

すること。

5）受注者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、1)から 17)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

【情報の取扱い】

6）受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当庁内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

7）受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当庁外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

8）受注者は、本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

9）受注者は、契約期間中及び契約終了後においても、本業務に関して知り得た当庁の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

なお、当庁の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

【情報セキュリティに係る対策、教育、侵害時の対処】

10）受注者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

11）受注者は、本業務の遂行において、情報セキュリティが侵害され、又はそのおそれが

ある場合の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

【クラウドサービス】

12）受注者は、本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、2)に掲げる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。

13）受注者は、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。

14）受注者は、前 2 項における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。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用】

15）受注者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること。

①各工程において、当庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当庁と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

③不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。 また、以下を含む対策を行うこと。

(a) 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

(b) 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファ

イルが常に最新の状態となるように構成すること。

(c) 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

(d) 不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

(e) EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

④情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた、又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

⑥受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。

⑦ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。

⑧外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。

・サービス開始前および、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。

なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

⑨電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

【アプリケーション・コンテンツの情報セキュリティ対策】

16）受注者は、アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。

①提供するアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。

(a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

(b) アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。

(c) 提供するアプリケーション・コンテンツにおいて、当庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。

②提供するアプリケーション・コンテンツが脆弱性を含まないこと。

③実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

④電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・

コンテンツの提供方式を定めて開発すること。

⑥当庁外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当庁外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。

17）受注者は、外部に公開するウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

別紙

令和　　年　　月　　日

特許庁○○○課長　殿

住　　所
名　　称
代 表 者 氏 名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

情報セキュリティに関する事項１）の規定に基づき、下記のとおり報告します。

記

１．契約件名等

契約締結日	
契約件名	

２．報告事項

項目	確認事項	実施状況
情報セキュリティに関する事項２）	本業務全体における情報セキュリティの確保のため、「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年度版）、「経済産業省情報セキュリティ管理規程」（平成１８・０３・２２シ第１号）及び「経済産業省情報セキュリティ対策基準」（平成１８･０３･２４シ第１号）（以下「規程等」と総称する。）に基づく、情報セキュリティ対策を講じる。	
情報セキュリティに関する事項３）	経済産業省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行う。	
情報セキュリティに関する事項４）	本業務に従事する者を限定する。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を担当職員に提示する。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示する。	
情報セキュリティに関する事項５）	本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して情報セキュリティに関する事項１）から１７）までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。	
情報セキュリティに関する事項６）	本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、経済産業省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に経済産業省の担当職員（以下「担当職員」という。）の許可を得る。	

	なお、この場合であっても、担当職員の許可なく複製しない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項 ７）	本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく経済産業省外で複製しない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項 ８）	本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。	
情報セキュリティに関する事項 ９）	契約期間中及び契約終了後においても、本業務に関して知り得た経済産業省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。 なお、経済産業省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供する。	
情報セキュリティに関する事項 １０）	本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施する。	
情報セキュリティに関する事項 １１）	本業務の遂行において、情報セキュリティが侵害され又はそのおそれがある場合の対処方法について担当職員に提示する。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従う。	
情報セキュリティに関する事項 １２）	本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、「情報セキュリティに関する事項２)」に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。	
情報セキュリティに関する事項 １３）	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。	
情報セキュリティに関する事項 １４）	情報セキュリティに関する事項１２）及び１３）における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。	
情報セキュリティに関する事項 １５）	情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施する。 （１）各工程において、当庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。 （２）情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当庁と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。 （３）不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。また、以下を含む対策を行うこと。 ①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。 ②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。 ③不正プログラム対策ソフトウェア等の設定変更権限については、システム	

	管理者が一括管理し、システム利用者に当該権限を付与しないこと。 ④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。 ⑤EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。 （４）情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。 （５）サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。 （６）受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。 （７）ウェブサイト又は電子メール送受信機能を含むシステム等の当庁外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「．ｇｏ．ｊｐ」を使用すること。 （８）外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。 ・サービス開始前および、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。 ・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。 ・必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。 （９）電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともに SMTP によるサーバ間通信の TLS（SSL）化や S/MIME 等の電子メールにおける暗号化及び電子署名等により保護すること。	
情報セキュリティに関する事項 １６）	アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行う。 （１）提供するアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。 ①アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。 ②アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。 ③提供するアプリケーション・コンテンツにおいて、当庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。 （２）提供するアプリケーション・コンテンツが脆弱性を含まないこと。 （３）実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。	

	（４）電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。 （５）提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。 （６）当庁外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当庁外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。	
情報セキュリティに関する事項 １７）	外部公開ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に従う。また、ウェブアプリケーションの構築又は改修時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施する。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出する。 なお、チェックリストの結果に基づき、担当職員から指示があった場合には、その指示に従う。	

記載要領

１．「実施状況」は、情報セキュリティに関する事項２）から１７）までに規定した事項について、情報セキュリティに関する事項１）に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。

２．上記に記載のない項目を追加することは妨げないが、事前に経済産業省と相談すること。

（この報告書の提出時期：定期的（契約期間における半期を目処（複数年の契約においては年１回以上））。）