データ処理に関する追加条件

本データ処理に関する追加条件（その別紙を含め、「**DPA**」といいます）は、契約当事者であるClarivateの企業体（その関係会社とあわせて「Clarivate」といいます）と、同じく契約当事者であるお客様（「お客様」といいます）間の合意（以下に定義します）に組み込まれます。

本DPAは、Clarivateが本合意に基づいて本サービスを提供する際にお客様の個人データ（以下に定義します）を処理する条件及び要件を定めています。Clarivateは、随時本DPAをアップデートする権利を留保します。そのようなアップデートがある場合、Clarivateは、その旨をお客様に通知します。本DPA、本合意及びClarivateとお客様の間のその他の適用される契約との間に矛盾又は不一致がある場合、本DPAの条件が優先されます。

本DPAに定義のない用語は、本合意で定められた意味を有するものとします。

1. 定義

a) **「関係会社」**とは、直接、間接を問わず、ある企業体を支配するか、支配されるか、又は共通の支配下にある企業体をいいます。

b) **「本合意」**とは、Clarivateとお客様間の契約であって、Clarivateはこれに基づいてお客様に本サービスを提供し、本DPAを組み込むものです。

c) **「お客様の個人データ」**とは、Clarivateが本合意に基づいてお客様にサービスを提供する際に処理する個人データを意味します。

d) **「支配」**とは、対象となる企業体の全体の50%以上の所有権、議決権持分又は同様の株式持分を持つことをいいます。**「支配される」**という用語は、これに応じて解釈されるものとします。

e) **「データ保護法」**とは、いずれかの当事者が本合意に基づいて行うお客様の個人データの処理に適用される全てのデータ保護及び個人情報保護に関する法規をいいます。これには、EU一般データ保護規則（「**GDPR**」）、カリフォルニア州プライバシー権法により修正されたカリフォルニア州消費者プライバシー法（「**CCPA**」）、児童オンラインプライバシー保護法（「**COPPA**」）、カナダの個人情報保護及び電子文書法（「**PIPEDA**」）、ブラジルの一般データ保護法（「**LGPD**」）、オーストラリアの1988年プライバシー法（「**オーストラリアプライバシー法**」）、スイス連邦データ保護法（「**FADP**」）、及び英国が採択したGDPR（「**英国GDPR**」）（それぞれ随時修正されます）などが含まれます。

f) **「EU SCC」**とは、欧州委員会が採択したGDPRに基づき個人データを第三国に移転するための標準契約条項（随時更新されます）をいい、特にモジュール1（管理者から管理者への移転）（該当する場合）及びモジュール2（管理者から処理者への移転）を含みます。

g) **「欧州」**とは、本DPAにおいては、欧州連合、欧州経済領域、これらの加盟国をいいます。

h) **「個人データの侵害」**とは、Clarivateが管理又は制御するシステム上の、お客様の個人データの偶発的又は違法な破壊、損失、改ざんや、不正な開示又はアクセスにつながる不正又は違法なセキュリティ侵害をいいます。

i) **「本サービス」**とは、本合意に規定された関連するサービスをいいます。

j) **「特別なカテゴリーの個人データ」**とは、個人データのうち以下に該当するものをいいます。(i) 人種・民族的出自、政治的見解、宗教や哲学的信条、又は労働組合への加入状況を明らかにするもの、及び遺伝子データ、自然人を一意に識別するための生体データ、健康に関するデータ又は自然人の性生活若しくは性的指向に関するデータを処理するもの、並びに (ii) 犯罪歴及び犯罪行為に関する個人データ。

k) **「代理処理者」**とは、Clarivateやその関係会社が使用する第三者又は関係会社（該当する方）であって、本合意に基づく本サービスの提供に関する義務の履行を支援する者をいいます。

l) **「UKアデンダム」**とは、英国情報コミッショナー事務所（「**英国ICO**」）が発行する欧州委員会標準契約条項（2022年3月21日発効のバージョンB1.0）の国際データ移転に関するアデンダムをいいます。

「**適切な保護措置**」、「**管理者**」、「**販売**」、「**共有**」、「**データ主体**」、「**個人情報**」、「**個人データ**」、「**処理者**」及び「**処理**」という用語は、「処理（processing）」の語の他の形態も含め、データ保護法に基づき定められる意味を有します。これらの用語がデータ保護法に基づき同じ又は類似の意味を有する範囲で、当該同じ又は類似の用語が適用されます。

2. 役割と責任

(a) 両当事者の役割　いずれかの当事者が行うお客様の個人データの処理にデータ保護法が適用される場合、両当事者は、お客様の個人データの処理に関して、お客様が管理者であり、Clarivateが処理者であることを了解し、これに合意します。詳細については、本DPAのAppendix A（「**データ処理の詳細**」）に記載されています。このような当事者の役割全般の割当とは別に、Clarivateは、別個の独立した管理者として、お客様の個人データを処理することができます。ただし、Clarivateが、運営上の目的（請求、口座管理、財務報告、ビジネスモデリング、社内報告など）で統計解析のためにお客様の個人データを処理する範囲とします。詳細については、Clarivateのプライバシーポリシー（https://clarivate.com/legal/privacy-statement/）で確認することができます。

(b) 目的の制限　Clarivateは、お客様が書面で行った適法な指示に従い、また適用法を遵守する必要に応じてお客様の個人データを処理するものとします。後者の場合、重要な公共の利益に基づく関連法に基づき禁止されていない範囲で、Clarivateは、関連する法的要件をお客様に通知します。両当事者は、お客様の個人データの処理に関するお客様の完全且つ最終的なClarivateへの指示が本DPA及び本合意に定められていることに合意し、こうした指示の範囲外の処理（該当する場合）については、当事者間の書面に定めるものとします（「**許可された目的**」といいます）。

(c) 禁止されたデータ　本DPAのAppendix Aに別段の定めがある場合を除き、お客様はClarivateに対していかなる特別なカテゴリーの個人データも提供（他者を介する提供を含みます）してはなりません。Clarivateは、個人データの侵害その他の有無にかかわらず、そのようなデータの処理に関するいかなる責任も負いません。これは、本合意又はデータ保護法により禁止されている他のカテゴリーの個人データにも適用されます。

(d) お客様のコンプライアンス　お客様は、お客様の個人データのお客様自身による処理及びClarivateに対する当該データの処理の全ての指示に関連して、データ保護法を含む全ての適用法を遵守しており、今後も遵守することを表明し、保証します。お客様の個人データの正確性、品質、適法性、並びにお客様によるお客様の個人データの収集方法については、お客様が単独で責任を負うものとします。お客様は、Clarivateがお客様の指示及び本DPA並びに本合意の条件に従って処理者として行為する限り、データ保護法の不遵守につき、Clarivateを免責します。

(e) お客様の指示の適法性　お客様は、Clarivateがお客様の指示に従って行うお客様の個人データの処理により、Clarivateがいかなる適用法、規制又は規則（データ保護法を含みますがこれに限りません）にも違反しないことを保証するものとします。Clarivateは、お客様からのデータ処理指示が、適用法（データ保護法を含みます）に違反していることに気付いた場合、関連するお客様の個人データの処理を停止することができます。その場合、Clarivateは、合理的な期間内に書面でお客様に通知します。お客様が適用法の違反につながる指示を修正しない場合、Clarivateは、本合意及び本DPAを直ちに解除することができます。

3. 代理処理

(a) 適格な代理処理者　お客様はClarivateに対し、本サービスの提供を目的としてお客様の代理で行うお客様の個人データの処理を代理処理者に委託することについて、全面的な許可を書面で与えるものとします。代理処理者のリストについては、Clarivateのプライバシーセンターからアクセスする（「Transparency and choice」の項目をご参照ください）か、又は**data.privacy@clarivate.com**宛にClarivateに直接お問い合わせください。さらに、お客様は、代理処理者のリストに含まれている書式を用いて、自らの代理処理者の交代及び追加の予定がある際に通知を受けるために登録することができます。登録時に、Clarivateは、代理処理者のかかる追加又は交代による変更の意図がある旨をお客様に通知するものとし、お客様が新規の代理処理者の使用について10日以内に正当な理由をもって通知により異議を唱えた場合、Clarivateは、その代理処理者による処理を避けるために、本サービスを変更するための又は商業上合理的な変更を提案するための合理的な努力を

行うものとします。Clarivateが合理的な期間内に当該代替策を提供できない場合、お客様は、30日以内にClarivateに書面で解約通知を提供することにより、いずれの当事者に対しても罰則又は責任を課すことなく、影響を受けた本サービスのうち、異議が唱えられた新しい代理処理者を使用しなければ提供することのできない部分のみを解約することができ、お客様は、解約された本サービスに対して前払いした料金につき案分した額の払い戻しを受ける権利を有します。

(b) 代理処理者の義務 Clarivateは、(i) 各代理処理者との間で、本DPAに記載されているお客様の個人データに対する保護と同等かそれ以上のデータ保護義務を含む契約を書面で締結するものとし、且つ (ii) 代理処理者が本DPAに基づく義務を遵守することについて引き続き責任を負うものとします（データ保護法により義務付けられる場合）。

4. セキュリティ

(a) セキュリティ対策 Clarivateは、Appendix B（「**技術的及び組織的セキュリティ対策**」）に記載されているClarivateのセキュリティ基準に従い、お客様の個人データのリスクに適したセキュリティレベルを徹底するために、適切な技術的及び組織的なセキュリティ対策を実施し、これを維持するものとします。

(b) 処理の秘密保持 Clarivateは、お客様の個人データを処理することをClarivateから許可された者に対して、適切な秘密保持義務を課すものとします。

(c) セキュリティ対策の更新 お客様は、データセキュリティに関してClarivateから提供された情報を確認し、本サービスがデータ保護法に基づくお客様の要件及び法的義務を満たすか単独で判断する責任を負います。お客様は、技術の進歩や発展に伴いセキュリティ対策が変更されること、及びClarivateがセキュリティ対策のアップデートや変更を適宜行うことを認めるものとします。ただし、当該アップデート及び変更は、お客様に提供される本サービスの全体的なセキュリティの低下を生じさせないことを条件とします。

(d) 個人データの侵害への対処 個人データの侵害の発生を知った場合、Clarivateは、(i) 遅滞なく、個人データの侵害が発生したと判断した時点から合理的に可能な限り、ただしいかなる場合においても48時間以内にお客様に通知するものとし、(ii) 個人データ侵害に関する時宜を得た情報をわかり次第又はお客様の合理的な要請により提供し、また (iii) 個人データ侵害の阻止及び調査を行うための妥当な措置を速やかに講じるものとします。Clarivateが本4(d)項に基づき行った個人データの侵害の通知や対応は、当該個人データの侵害についてClarivateが自己の過失又は責任を認めたとは解釈されないものとします。

5. 監査

(a) お客様の監査権 お客様からの60日以上前の書面での通知により、Clarivateは、本DPAの遵守を証明するために合理的に必要な全ての情報をお客様が入手できるようにし、（合理的であれば）本DPAの遵守を評価するためにお客様が行う調査など、お客様がその費用負担で行う監査を許可し、これに協力します。Clarivateが本サービスを対象として、独立した第三者によるシステム及び組織統制（SOC）2報告書、システム及び組織統制（SOC）3報告書又はISO 27001認証を保有している場合、お客様は、最新の報告書又は認証の写しを提出するよう書面でClarivateに指示することにより、自らの監査の実施権を行使することに同意します。なお、かかる報告書又は認証の写しはClarivateの秘密情報とみなされます。Clarivateが当該報告書又は認証を提供しない場合、お客様は、（委任された監査人による場合を含め）年に1回を限度として自らの費用負担で自らの監査を実施することができます。ただし、Clarivateが個人データの侵害の対象となった場合、又は当社のプライバシー及びセキュリティ慣行に関する正式な苦情を受けた場合はこの限りではありません。

(b) お客様の監査の範囲と適用される条件 お客様によって委任された監査人は、Clarivateの競合相手であってはならず、Clarivateの秘密情報及び全ての監査結果の秘密性を保持することを監査人に義務付ける秘密保持契約であってClarivateが適切と判断するものを締結しているものとします。お客様とClarivateは、監査を実施するにあたり、前もって、その監査の範囲、時期及び期間について相互に合意するものとします。お客様は、監査のためにClarivateが要した時間に応じてClarivateの費用を支払うものとします。Clarivateの代理処理者に対する監査が要請された場合、お客様は、当該監査が追加の又は異なる監査条件の対象となる場合があることを了解します。全ての支払いレート及び費用は、Clarivate又は第三者代理処理者が費やしたリソースを考慮し、Clarivateの時間給が適用されます。監査及び調査にはClarivateの適切なデータ保護及び情報セキュリティのポリシーが適用されます。監査の範囲は、Clarivateの情報システム、又はお客様の個人データ

の保護に適用されるポリシー及び手順に限られます。お客様は、Clarivateのローデータ、プライベート、センシティブ、秘密又は専有のビジネス情報（従業員の給与や人事記録、お客様の個人データとは関係がないClarivateの拠点、帳簿、文書、記録、その他の情報のいかなる部分、又はその他の秘密情報、法律上の特権がある情報も含みます）を閲覧しないことに同意します。お客様は、Clarivateのセキュリティ情報又は資料をコピーし、又はClarivateの施設若しくはシステムから持ち出してはなりません。
お客様は、Clarivateに対して無償で、監査結果の写しを提供するものとします。監査中にClarivateが本DPAに基づくセキュリティ、秘密保持又はデータ保護義務を遵守していないことが判明した場合、お客様は監査の完了後直ちに、その旨を詳細にClarivateに通知するものとします。監査や調査で得られた情報及び監査や調査の結果は、Clarivateの秘密情報とみなされます。

6. 国際的なデータ移転

(a) Clarivateから第三者へのデータ移転　第3条及び本第6条の条件に従い、Clarivateは、データ保護法に基づく国境を越えたデータ移転に関する規定の遵守を徹底することを前提として、データ保護法の意味における第三国に拠点を置くデータ受領者にお客様の個人データを移転することがあります。

(b) GDPRに基づくデータ移転　ClarivateがEU/EEA外に拠点を置き、GDPRに基づき保護されるお客様の個人データを受け取る場合において、GDPR第45条第3項の意味における十分性認定が移転に適用されない範囲で、両当事者は、本DPAに署名することによりEU SCCを締結することに合意します。したがって、EU SCCは、本DPAに組み込まれるものとみなされ、Clarivateは、「データ輸入者」となり、お客様は、「データ輸出者」となります。特に、両当事者は、以下のとおり合意します。(i) EU SCCの第7条は適用されないこと、(ii) モジュール2について、第9条(a) のオプション2（一般的な書面による承認）が適用され、期間は、10日間以上とすること、(iii) 紛争解決機関は存在しないこと（第11条）、(iv) Clause 17のオプション2が適用され、本合意で特定された加盟国の法が適用されること、また加盟国の法について合意に至らない場合は、アイルランドの法律が適用されること、(v) 第18条の裁判所の選択は、本合意において合意されるとおりとし、加盟国の裁判所について合意に至らない場合は、アイルランドの裁判所とすることに合意するものとします。EU SCCのAnnex 1に基づき必要とされる情報は、本DPAのAppendix Aに記載されており、管轄の監督当局は、EU SCCの第13条で特定されたデータ輸出者を担当する監督当局とします。EU SCCのAnnex 2に基づき必要とされる情報は、本DPAのAppendix Bに記載されています。

(c) UKデータ移転　Clarivateが英国外に拠点を置き、英国GDPRに基づき保護されるお客様の個人データを受け取る場合で、英国の十分性認定に関する規則に基づき十分性認定が適用されない範囲で、両当事者は、第6条(b)に定められ、UKアデンダムにより修正された書式にてEU SCC（この言及により本DPAに組み込まれたとみなされます）を締結することに合意します。

(d) FADPに基づくデータ移転　Clarivateがスイス外に拠点を置き、FADPに基づき保護されるお客様の個人データを受領する場合において、FADPに基づく十分性認定が適用されない範囲で、両当事者は、第6条(b)に定める書式にてEU SCCを締結することに合意します。これは、以下のとおり修正されるものとします。(i) GDPRへの言及は、FADPの対応する規定を指すものと解釈されます。(ii) 「EU」、「連合」、「加盟国」及び「加盟国の法」への言及は、場合により、スイス及びスイス法を指すものと解釈されます。(iii) Annex Bに記載されている管轄の監督当局は、Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragterとします。(iv) スイス法が適用されます（第17条）。(v) 第18条の裁判所及び管轄の選択は、スイスとします。(vi) 第18条(c)の「加盟国」という語は、いかなる形であれ、スイスに居住地を置くデータ主体が補償を請求することを禁止するものと解釈してはなりません。

(e) 代替移転メカニズム　Clarivateが、データ保護法に準拠したお客様の個人データの移転に関して、データ保護法に定める代替データ移転メカニズム（EU SCCの新版や後継版を含み、以下「**代替移転メカニズム**」と総称します）を実施又は採用した場合、当該代替移転メカニズムは、本DPAに記載された移転メカニズムに代わり適用されます。管轄裁判所又は監督機関の命令により、本DPAに記載されている手段では、お客様の個人データをデータ保護法に従って正しく移転することができなくなった場合（理由の如何を問いません）、Clarivateは、お客様の個人データの適法な移転を可能にするために合理的に必要な追加の手段や保護手段を実施することができます。

7. データの返却又は削除

サービスが終了又は満了した場合、並びにかかる終了又は満了後30日以内にお客様の書面による要求及び選択が行われた場合、Clarivateは、（お客様の選択により）Clarivateが所有又は管理するお客様の個人データの全て（コピーを含みます）の削除又はお客様への返却を行うものとします。ただし、当該返却により、その時点におけるClarivateの時間給でお客様に追加手数料が発生する場合があります。当該手数料は、別個の見積書及び作業明細書に記載されます。この規定は、以下には適用されません。(i) Clarivateがお客様の個人データの全部又は一部の保持を適用法で義務付けられている範囲、又は(ii) Clarivateがバックアップシステムにアーカイブしたお客様の個人データ。 Clarivateは、Clarivateの削除に関する方針に従って削除されるまで、当該データを安全に隔離し、それ以上の処理が行われないよう保護するものとします。若しくは(iii) Clarivateが第2条に定めるとおり、独立した別個の管理者として処理するお客様の個人データ。

8. データ保護法に基づくデータ主体の権利及びその他の義務に関する支援

(a) データ主体からの要求　サービスの一環として、Clarivateは、お客様の個人データの抽出、修正、削除又は使用制限を行うことができるセルフサービス機能をお客様に提供します。お客様は、データ主体からのデータ保護法に基づく自らの権利を行使する旨の要求に対応するために、データ保護法に基づく自己の義務に役立てるため、追加費用なしに、この機能を使用することができます。処理の性質に鑑みて必要な場合、Clarivateはさらに、お客様が、データ主体からデータ保護法に基づく自らの権利を行使する旨の要求を受けた場合にこれに応じる義務を果たすために、合理的な支援を提供します。Clarivateに対して直接、そのような要求がなされた場合、Clarivateは、適切であると合理的に判断される場合（例えば、データ主体に対してお客様にコンタクトするよう案内する場合、データ主体に対してセルフサービス機能の情報とともに一般に公開されているリンクを案内する場合、又は要求の性質やClarivateのどのお客様が関係しているかを確認する場合など）を除き、又は適用法で義務付けられる場合を除き、お客様より事前の承認を得てから、当該要求への直接の対応を行うよう努めるものとします。Clarivateが当該要求に対応する場合、Clarivateはお客様に通知し、その要求の写しをお客様に提供するものとします。ただし、Clarivateがそのような行為を法的に禁止されている場合、又は当該行為が実施不可能であるか、お客様にとって利益がない若しくは利益が少ないために不当であるか、又は適用法に違反するとみなされる場合はこの限りではありません。

(b) データ保護法に基づく義務　データ保護法に基づき義務付けられる範囲で、且つ常に本サービスに関連している場合のみ、Clarivateは、（処理の性質及びClarivateに提供される情報を考慮して）お客様がデータ保護法に基づく義務（データ保護の影響評価の実施等）を遵守することができるよう合理的な水準の支援を提供します。

9. 法域別条件

Appendix Cに記載されたいずれかの法域で生じたお客様の個人データであって、かかる法域のデータ保護法により保護されているお客様の個人データをClarivateが処理する範囲においては、本DPAの条件に加えて、Appendix Cに記載された該当法域に関する条件（「**法域別条件**」といいます）が適用されます。法域別条件と本DPAのその他の条件との間に、矛盾又は不明瞭な点がある場合、法域別条件が優先します。ただし、当該法域別条件はClarivateに適用される範囲でのみ優先されるものとします。

10. 本合意との関係

(a) 契約期間　DPAは、Clarivateがお客様に代わってお客様の個人データの処理業務を実施する限り、又は本合意が終了するまで（且つ、上記7条に従い、お客様の個人データの全てが返却又は削除されるまで）、有効であるものとします。

(b) 優先性　両当事者は、本DPAが、両当事者が本サービスに関連してこれまでに締結したデータ処理に関する既存の合意や同様の文書に置き換わるものであることに合意します。お客様の個人データの処理関して本DPAと本合意の残りの部分との間に矛盾又は齟齬が生じた場合、(i) SCCs、(ii)本 DPA、(iii) 本合意の残りの部分（本合意の残りの部分は、本合意に規定される優先順位に従って解釈されるものとします）の順に優先します。

(c) 変更の効果　本DPAによって変更される部分を除き、本合意は変更されず、有効であるものとします。

(d) **第三者の権利**　本DPAの当事者、その継承者及び正当な譲受人以外の者は、本DPAの条件を執行するいかなる権利も有しないものとします。ただし、明確化のために記すと、この条項は、EU SCC（英国GDPR及びFDPAにおいて修正されたもの）に基づくデータ主体の権利を制限するものではありません。

(e) **準拠法**　本DPAは、適用されるデータ保護法に別段の定めがある場合を除き、本合意の準拠法及び裁判管轄に関する条件に従い、これにより解釈されるものとします。

Appendix A – データ処理の詳細

本Appendix Aでは、Clarivateが処理者となり、お客様が管理者となるデータ処理の具体的な詳細を記載しています。

データ管理者：
本合意で定義されるお客様

処理者：
本DPAの冒頭で定義されるClarivate

対象：
本DPAに基づくデータ処理の対象は、お客様の個人データです。

処理の期間：
Clarivateは、本DPAの第7条及び第10条 (a) の定めに従い、お客様の個人データを処理します。

処理の目的及び性質：
お客様の個人データの処理の目的及び性質には、次の必要に応じた処理を含みます。(i) 本合意に従って本サービスを提供するため、(ii) 本合意及び本DPAに基づくClarivateの義務を履行するため、(iii) データ管理者から（電子メール又はサポートチケットを介して）受領したその他の合理的な指示であって、本合意の条件と矛盾しないものに準拠するため、(iv) ユーザーの生産性、信頼性、効率性、品質及びセキュリティを向上させるため、最新且つ高性能の本サービスを維持するため、(v) 本サービスにおけるバグを修正し、問題のトラブルシューティングを行うため、及び (vi) 下記の該当サービスに記載されたもの。

データ主体のカテゴリー：
管理者は、本サービスに対してお客様の個人データを提出することができます。その範囲は管理者の裁量により決定及び管理されるものであり、以下のサービスごとに記載されたデータ主体のカテゴリーに関するお客様の個人データを含みますが、これに限定されません。

個人データのカテゴリー：
管理者は、サービスが提供される目的に従いお客様の個人データをサービスに送信することができます。なおその範囲は本書又は本合意に定める制約を受け、データ管理者の独自の裁量により決定及び管理し、以下のサービス及び提供される製品文書に記載された個人データのカテゴリーを含みますが、これに限定されません。

サービス	目的と性質	データ主体のカテゴリー	個人データのカテゴリー
Converis	ホスティング、サービスの実装、技術サポート	• 従業員、代理人、アドバイザー及び管理者の契約者 • 管理者から本サービスの使用を許可された個人 • 参加ジャーナルのピアレビュー実施者、編集者など学会メンバー • 管理者が決定するその他のデータ主体	• 氏名及び機微性のないその他の識別情報（従業員ID番号、ResercherID、ユーザー名など） • 人口統計情報 • ビジネス連絡先情報 • 専門家情報 • 本合意により認められ本サービスに追加された、サービスにより生成された、その他サービスに保存されるその他の個人データのカテゴリー

Discovery, Research and Library Workflow Solutions:
360 Core
360 LINK
360 MARC Updates
360 Resource Manager
360 Search
Intota™ Assessment
Pivot/Pivot-RP
RefWorks
Summon
Ulrichsweb
Ulrich's™ Serials Analysis System
Intota™
	ホスティング、サービスの実装、技術サポート	• 図書館利用者、図書館スタッフ、教員、学生、管理者、従業員、訪問者、同窓生	• 基本的な図書館利用者及び使用者の情報（以下を含む）
			  • 氏名
			  • 郵送先住所
			  • 電子メールアドレス
			  • 電話番号及びその他の連絡先情報
			  • 機関識別番号
			  • 部署と職務
			• スタッフの基本情報及びスタッフの連絡先情報
			• スタッフの業務及び活動の記録を含む、スタッフ関連の使用状況情報
			• 研究活動
			• 一般的な使用情報（IPアドレスなどの接続データを含む）
			  • サプライヤー／ベンダー情報

EndNote	ホスティング、技術的サポート、及び関連サービス	• 管理者の従業員、代理人、アドバイザー、及び契約社員（自然人） • 出版物の著者や査読者など、学術コミュニティのメンバー • お客様 • 潜在的なお客様 • 管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別子（電子メールアドレス、ResearcherID、ユーザー名など） 本サービスにおいて追加、生成又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの
First to File	ユーザーアカウントの事前登録、ホスティング、実装、技術サポート、プロフェッショナルサービス（該当する場合）	• 管理者の従業員、代理人、アドバイザー、フリーランサー（自然人） • 管理者から本サービスの使用を許可された個人 • 管理者の見込み顧客、顧客、ビジネスパートナー、及びベンダー（自然人） • 管理者の見込み顧客、顧客、ビジネスパートナー及びベンダーの従業員又はコンタクト • 発明者、特許出願人及び譲受人、商標権者、弁護士（該当する場合、弁理士を含みます）を含む、管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別情報（署名など） • 業務上の連絡先情報 • 人口統計学的情報 • 職業的情報 • 本サービスにおいて追加、生成又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの
Integrated Library Systems: **Millennium** **Polaris Sierra** **Vega** **Virtua** **及び関連モジュール**	ホスティング（管理者又は承認済み外部ホスティングプロバイダーがホストする場合を除く）、実施、技術サポート	• 管理者の従業員、代理人、アドバイザー、フリーランサー（自然人） • 管理者から本サービスの利用を許可された者（図書館利用者を含む）	• 図書館利用者のデータ（図書館カード番号又その他の識別番号など。データ主体の図書館カードの画像、年齢又は生年月日、連絡先情報、居住証明書等が含まれるほか、政府発行の身分証明書やデータ主体がお客様に提供したその他の文書のコピーが含まれる場合がある） • 本サービスの利用に関する情報（図書館利用者の場合は、図書館のリソースの使用など（訪問した場所や支所、要請したか、保持しているか、返却したか、又はアクセスした資料の履歴を含む）） • 図書館スタッフとのやり取り • その他の図書館サービスの利用、支払いを容易にするために提供された情報、延滞料金又は罰金

			• 氏名及び機微性のないその他の識別子（職員ID番号、ユーザー名など） • 業務上の連絡先情報 • 人口統計学的情報 • 職業的情報 • 本サービスにおいて追加、生成又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの
IP management systems **FoundationIP** **IPfolio Ipendo** **Inprotech** **Memotech** **Patrawin** **The IP Management System** **Unycom**	ホスティング（管理者又はSalesforceなどの承認済み外部ホスティングプロバイダーがホストする場合を除く）、実施、技術サポート	• 管理者の従業員、代理人、アドバイザー、フリーランサー（自然人） • 管理者から本サービスの使用を許可された個人 • 管理者の見込み顧客、顧客、ビジネスパートナー、及びベンダー（自然人） • 管理者の見込み顧客、顧客、ビジネスパートナー及びベンダーの従業員又はコンタクト • 発明者、特許出願人及び譲受人、商標権者、弁護士（該当する場合、弁理士を含みます）を含む、管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別子（職員ID番号、ユーザー名など） • 業務上の連絡先情報 • 人口統計学的情報 • 職業的情報 • 本サービスにおいて追加、生成又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの
IPプロフェッショナルサービス	IPに関連するプロフェッショナルサービスの提供（更新、ドケッティング及び出願に関わるサービスを含みますがこれらに限定されません）	• 管理者の従業員、代理人、アドバイザー、フリーランサー（自然人） • 管理者から本サービスの使用を許可された個人 • 管理者の見込み顧客、顧客、ビジネスパートナー、及びベンダー（自然人） • 管理者の見込み顧客、顧客、ビジネスパートナー及びベンダーの従業員又はコンタクト • 発明者、特許出願人及び譲受人、商標権者、弁護士（該当する場合、弁理士を含みます）を含む、管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別子（職員ID番号、ユーザー名など） • 業務上の連絡先情報 • 人口統計学的情報 • 職業的情報 • 本サービスにおいて追加、生成又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの
市場調査 - 市場調査活動の一環として行われる契約上必要な安全性及び品質に関する報告	本合意に規定されたお客様又は製造販売承認取得者に対する安全性及び品質に関する事象の報告	• 市場調査参加者	• 氏名 • 人口統計学的情報 • 職業的情報 • 連絡先情報 • 謝礼金の処理に必要な情報
市場調査 - 一次市場調査プロジェクトのためのリストベースの募集活動	一次市場調査のための特定の人物の募集を目的としてお客様から提供されたリストの取扱い	• 潜在的市場調査参加者	• 氏名 • 人口統計学的情報 • 連絡先情報 • 職業的情報 • 謝礼金の処理に必要な情報
My Organization (InCites Benchmarking and Analytics Module)	ClarivateのInCitesにおけるMy Organizationモジュール上で、お客様が自己の研究者データベースをアップロード、分析、及び管理できるようにすること	• 管理者の従業員、代理人、アドバイザー、及び契約社員（自然人） • 管理者から本サービスの使用を許可された個人 • 管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別情報（従業員ID番号、ResearcherID、ユーザー名など） • 人口統計学的情報 • 業務上の連絡先情報 • 職業的情報 • 本サービスにおいて追加、生成、又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの

クラウドベースの library management, discovery, research, reading list and mobile/web app (Ex Libris SaaS services):
 	
Alma
 	
Esploro
 	
CampusM
 	
Leganto
 	
Primo SaaS/Primo VE
Rapido
	ホスティング、
	
	サービスの実装、技術サポート及び／又はその他の関連サービス
		• 図書館利用者、図書館スタッフ、教員、学生、管理者、従業員、研究者、訪問者、同窓生	• 図書館利用者及び使用者の情報（以下を含む）
			  • 氏名
			  • 郵送先住所
			  • 電子メールアドレス
			  • 電話番号及びその他の連絡先情報
			  • 機関識別番号
			• 図書館／カタログ関連の図書館利用者及び使用者の情報（以下を含む）
			  • 図書館の活動、貸出及び罰金に関する情報
			• スタッフの基本情報（連絡先情報を含む）
			• スタッフの業務及び活動の記録を含む、スタッフ関連の使用状況情報
			• 研究活動
			• 一般的な使用情報（IPアドレスなどの接続データを含む）
			• サプライヤー／ベンダー情報
			• 該当する場合、モバイルプラットフォーム情報
			  • デバイス情報（識別子やプラットフォームなど）
			• 該当する場合、出勤及び位置データ

以下を含む、ローカルにインストールされたEx Librisソフトウェアのソフトウェアサポート及びメンテナンスサービス： **Aleph Local** **Primo Local** **Rosetta Local** **Voyager Local** **SFX**	リストされた製品のローカルインストールバージョンへのリモートアクセスによるサポートとメンテナンスのパフォーマンス	• お客様が選択し、Clarivateが一時的にアクセスできるローカルインストールシステムに保存される、データ主体のカテゴリー	• ソフトウェアメンテナンス及びサポートサービスの提供に関連してClarivateがアクセス権を有するプログラムを実行するローカルシステム上にお客様が保存するか、ソフトウェアメンテナンス及びサポートサービスの提供の過程でお客様がClarivateに提供する個人データの種類 • 処理は非常に限定的であり、主にサポートサービスのコールを解決するために、システムのアクティブ、且つ一時的なリモートアクセス中の個人データへの偶発的なアクセスに関与します。
Web of Science Reviewer Recognition; **Web of Science Author Connect** **Web of Science Reviewer Locator**	該当するサービスへのサインアップを招待された個人リスト（お客様から提供されたもの）を処理する場合のみ	• 研究者や査読者など、学術コミュニティのメンバー	• 氏名及び機微性のないその他の識別子（研究者IDなど） • 人口統計学的情報 • 業務上の連絡先情報 • 職業的情報 • データ主体の査読活動に関連するその他の情報
ScholarOne	ホスティング、技術的サポート、及び関連サービス	• 管理者の従業員、代理人、アドバイザー、及び契約社員（自然人） • 出版物の著者や査読者など、学術コミュニティのメンバー • 管理者が決定したその他のデータ主体	• 氏名及び機微性のないその他の識別情報（従業員ID番号、ResearcherID、ユーザー名など） • 人口統計学的情報 • 業務上の連絡先情報 • 職業的情報 • 本サービスにおいて追加、生成、又は保存されるその他のカテゴリーの個人データであって、本合意に基づき許可されたもの

特別なカテゴリーの個人データ：

市場調査活動の一環として契約で要求された報告義務がある安全性又は品質に関する事象のために処理される健康関連の詳細情報を除き、本サービスの提供に関連して、Clarivateが特別なカテゴリーの個人データの収集や処理を希望したり、そうしたデータを意図的に収集又は処理したりすることはありません。

処理業務：

お客様の個人データは、本合意（本DPA及び作業明細書又は注文書を含みます）に基づき処理され、また、お客様に提供される本サービスの提供、維持及び改善のために必要な場合に、本合意に従って又は適用法によって求められる通りに処理されます。お客様の個人データには、次のような処理業務が行われる場合があります。

業務又は一連の業務とは、それが自動化されているかどうかに関わらず、収集、記録、組織化、構造化、保存、翻案や改変、検索、参照、使用、送信による開示、頒布若しくはその他の方法により入手可能とすること、調整若しくは結合、制限、消去若しくは破壊をいいます。

個人データ移転の頻度：

お客様の個人データは、開始時、及び期間中必要に応じて移転されます。

保持期間：

データは、本DPAの第7条に記載された通り、本合意の期間、保持されるものとします。

上の規定は、Clarivateから代理処理者への移転についても適用されるものとします。

Appendix B – 技術的及び組織的対策

本サービスには、以下に記載された技術的及び組織的対策が適用されます（本DPAの第4条(c)に準拠して随時更新されます）。

情報セキュリティプログラム

Clarivateは、情報セキュリティに関するよく知られた業界標準に沿って、必要な技術的及び組織的対策を網羅する明確に定義された情報セキュリティプログラムを設け、自社の情報資産の機密性、完全性及び可用性を保護しています。

人員

当社の全スタッフは、当社のバリューとミッションを網羅した行動規範を遵守しなければなりません。当社の全スタッフは、自己の責任及び当社のポリシーと基準を把握しており、また、当社の情報セキュリティチームから、適切なガイダンスとサポートを定期的に受けています。

重要な情報資産に対する脅威を軽減するため、正社員の採用活動にあたっては、関連する法令や規制に従って経歴の確認が適切に実施されます。

当社では、全員を対象とした情報セキュリティトレーニングを継続的に実施し、必要に応じて、特定の対象グループ及び個人に向けた追加トレーニングを実施しています。当社スタッフは秘密保持義務を負っており、また、当社のポリシーや自己の責任を遵守しなかった場合の結果について理解しています。

Clarivateにおける従業員の退職プロセスには、システムの許諾及びアクセス権の無効化、並びに会社資産の返却を直ちに実施することが含まれています。

個人データの暗号化

個人情報が、電子的送信中に許可なく読み取られ、複製され、改変され、削除されることを防ぎ、個人データの移転先組織をデータ送信機能により確認することができるよう、暗号化を含む対策が取られています。

ユーザーアクセスの管理

Clarivateは、情報資産へのアクセス権の付与に関して、明確に定義されたプロセスを設けています。当社は、権限のない人物がデータ処理設備（アクセス管理、ログ記録、パスワード保護を含みます）を使用することを防ぐための対策を行っています。

データ処理設備のユーザー権限は、個人データへのアクセスを制限し、不正なアクセスや開示から保護するためのそれぞれの役割や責任に沿って認められています。Clarivateのパスワードポリシーは、全ての情報資産について全社的に、パスワードの長さ、複雑さ、パスワードの有効期限、履歴、及び認証失敗時のアカウントロックに関する要件を定めています。

インフラのセキュリティ

当社のサービスは、パブリックネットワーク及びプライベートのネットワークを通じて提供されます。通信内容は安全なチャネル及び暗号化によって傍受から保護されています。Clarivateは、侵入防御システム(IPS)、ネットワークアクセスを管理し制限するファイアウォールやAWSのグループ、データセンターのVLANSを用いてネットワークとの境界を保護しています。

システム及びデータの適切な水準の保護を確実にするために設計された階層型コントロール（ネットワークセグメンテーションの使用を含みます）があります。

マルウェア対策

Clarivateが所有しサポートを行っているオペレーティングシステム（当社のデータセンターでホストされているか、クラウドに配置されています）は、当社のポリシーに従い、次世代ウイルス対策ソリューションで保護されています。

パッチ管理

当社では、内部の脆弱性管理ツール、ベンダーやその他の第三者セキュリティ組織を通じてセキュリティ脅威インテリジェンスの収集と検証を行っています。当社ではパッチ管理基準を設けており、テクノロジーチームによる適切なパッチ適用を行います。当社のセキュリティパッチは、パッチの重大度の評価と定義から開始されます。パッチ適用後、システムの安定性と可用性を検証するために、プライオリティ認証とQAテストが用いられます。場合によっては、既知の脅威を軽減するために、追加のセキュリティコントロールが実施されます。

セキュリティモニタリング

Clarivateは、カスタマーデータへのロジカルネットワークアクセスと情報資産の使用を24時間 x 週7日記録しモニターするための専門のネットワーク＆セキュリティオペレーションセンター（NOC/SOC）を設置しています。セキュリティログは、リアルタイム認識、イベント相関、インシデント対応のため、SOC（セキュリティオペレーションセンター）へ送られます。データエントリーの記録も行われ、個人データ処理システムへの個人データの入力や改変、又は個人データの削除が行われたかをチェックし、もしそのようなことが行われていた場合、誰が行ったのかを確認します。

セキュリティ及びプライバシーインシデント対応

インシデントが特定された場合に、それに対するインシデント対応プロセスが設けられています。専門のインシデント対応チームが、軽減とコミュニケーションに関する手順書に従い、インシデントを管理します。

Clarivateのインシデント対応プロセスでは、セキュリティインシデントを適時に制御及び修正するための是正措置を確実に実施できるよう、インシデントの効果的な報告、調査及びモニタリングを義務付けています。

オペレーションセキュリティ

情報システム環境のオペレーションに関する全ての変更（サーバー、ネットワーク設備、ソフトウェアへの変更を含みます）は、正式な変更管理プロセスに従って行われます。

システムクラッシュや情報の偶発的削除などの事象に備えて、データ復旧を目的として情報及びソフトウェアのバックアップコピーが安全に維持されています。

容量の管理及びモニタリング

当社のオペレーション環境の健全性を維持するため、システム、サービス、及びオペレーションのモニタリングを実施しています。適切な規模の環境のモニタリング及び維持を行う管理ツールが導入されています。

脆弱性スキャン

Clarivateは、セキュリティチェック、自動又は手動のセキュリティレビュー、アプリケーション及びインフラの脆弱性評価スキャンなど、多層にわたるセキュリティ脆弱性管理プログラムを導入しています。特定された問題を評価、検証、優先順位付け、及び修正するための措置が講じられています。

脆弱性管理に重点を置いた当社のプログラムを実施するために、当社のグローバルネットワーク上のインターネットに接続されたサイトは、定期的にスキャンされています。

リスク管理

当社のプロダクトチーム及びテクノロジーチームは、情報セキュリティ分野の専門家に対し、定期的にリスクアセスメントを委託しています。リスクアセスメントの実施内容には、アーキテクチャレビュー、脆弱性スキャン、アプリケーションセキュリティ試験、技術コンプライアンスレビューなどがあります。

リスクアセスメントに続き、情報セキュリティリスクマネジメントチームが、プロダクトチーム及びテクノロジーチームと協議を行い、コンプライアンスの隙間や、リスクが特定された領域に取り組むための是正計画とロードマップを策定します。

さらに、ITガバナンス、リスク及びコンプライアンスチームが、ポリシー、基準及び規制上の要件についての監査を実施し、評価用の監査結果及び業務の修正計画を記録します。

物理的セキュリティ及び第三者ベンダーのマネジメント

Clarivate製品をホストしているクラウドサービスプロバイダーを含む全ての戦略的データセンターは、Clarivateが採用した業界の物理的セキュリティ基準に従ってデプロイされ、管理されます。当社のガイドラインには、物理的セキュリティ、建物の維持管理、防火、空調、補助発電機付きのUPS、種々の電力及び通信へのアクセスに関する要件が含まれます。Clarivateは、ベンダーリスクマネジメントプログラムの一環として、第三者データセンターの監査保証報告書のレビューを行っています。

当社施設への出入りが、コントロールされた方法で、オペレーション上の必要性がある場合にのみ許可されるよう、当社施設への出入りをコントロールするための様々な安全策が用いられています。施設の秘密性に応じて、サービス時間外のアラーム装置やセキュリティサービス、異なるセキュリティゾーンへの場所の分割、警備員、IDカード、近接型カードリーダーを組み込んだ電子アクセス制御、物理的な施錠、PIN番号といった対策の全部又は一部を実施しています。

Appendix C - 法域別条件

欧州経済領域、英国及びスイス：

政府によるデータへのアクセスの要求　一般に、Clarivateが自主的にお客様の個人データを政府機関や政府当局（法執行機関を含む）に提供することはありません。Clarivateが、政府機関又は政府当局（法執行機関を含む）から、主たるコンタクト情報が欧州経済領域、英国、又はスイスの所在を示しているデータ主体について、そのデータ主体に帰属するお客様の個人データへのアクセスを強制的に要求（召喚令状、裁判所命令、捜索令状、その他の有効な法的手続など、方法の如何を問いません）された場合、Clarivateは、(i) Clarivateがそのデータの処理者であることを政府機関に通知し、(ii) 政府機関に対し、お客様に直接データを要求するよう働きかけ、及び (iii) お客様が保護命令やその他の適切な救済措置を求めることができるよう、お客様の主たるコンタクトのeメールアドレス宛にeメールを送信し、その要求について通知するものとします。この一環として、Clarivateは、お客様の主たるコンタクト情報及び請求先情報を関連当局に提供することができます。Clarivateは、法的に禁止される場合、又は個人、公共の安全若しくはClarivateに対する差し迫った深刻な危険を防ぐために緊急のアクセスが必要であると合理的且つ誠実に判断される場合、本項の遵守を要しないものとします。

米国カリフォルニア州：

Appendix Cの本セクション「米国カリフォルニア州」は、ClarivateがCCPAの範囲内でお客様の個人データを処理する場合にその範囲に限り適用され、両当事者を拘束します。Appendix Cの本セクション「米国カリフォルニア州」が本合意又はDPAの条件と矛盾する場合には本セクションが優先しますが、本合意又はDPAにそのほかの変更を加えるものではありません。両当事者は、以下の通り合意します。

(a) 定義　別途記載されている場合を除き、「管理者」の定義には「**ビジネス**」を含み、「処理者」の定義には「**サービスプロバイダー**」を含み、「データ主体」の定義には「**消費者**」を含み、「個人データ」の定義には「**個人情報**」を含みます（いずれの場合も、CCPAに定義された通りとします）。本Appendix Cの本セクション「米国カリフォルニア州」においてのみ、「**許可された目的**」は、適用法の遵守のために必要な場合、書面（本合意を含みますがこれに限定されません）で別途合意した場合、又はCCPAに基づき「サービスプロバイダー」が別途容認されている場合において、本DPAに記載されている限定的で特定された目的に限り、且つ本DPAに記載されたお客様の適法な指示書に従ってのみ、お客様の個人データを処理することを含むものとします。

(b) コンプライアンス　Clarivateは、CCPAの適用される条項を遵守します。これには、企業がCCPAにより義務付けられる同レベルのプライバシー保護を提供することが含まれます。Clarivateは、CCPAに基づく義務をもはや履行することができないと判断した後に、お客様に通知する場合があります。お客様は、ClarivateがCCPAに基づくお客様の義務に沿った方法でお客様の個人データを使用するよう徹底するために、合理的且つ適切な措置を講じることができます。お客様は、事前の書面通知をもって、Clarivateによるお客様の個人データの不正使用を停止し、是正するために合理的且つ適切な措置を講じることができます。

(c) 禁止されている使用　Clarivateは、以下を行いません。

- 本合意に基づいて収集されたお客様の個人データを、「販売」又は「共有」（これらの語はCCPAで定義されています）すること。
- 本合意及び本DPAに定められている事業上又は商業上の目的以外で、お客様の個人データを保持、使用又は開示すること。
- 適用されるデータ保護法規により明示的に許容される場合を除き、お客様との直接的な事業上の関係外でお客様の個人データを保持、使用又は開示すること。
- CCPAに基づき許容される場合を除き、お客様の個人データを、他の人や団体若しくはそれらの代理人から受け取った個人情報、又はClarivateと消費者とのやり取りから収集した情報と結合すること。

米国、学生データ – 家族の教育上の権利及びプライバシー権（Family Educational and Privacy Rights、FERPA）：

Appendix Cの本セクション「米国、学生データ」は、ClarivateがFERPAの範囲内でお客様の個人データ（「**FERPAデー**

タ」）を処理する場合にその範囲に限り適用され、両当事者を拘束します。この場合、お客様は、FERPAに基づく規制が適用される教育団体又は教育機関であるものとします。Appendix Cの本セクション「米国、学生データ」が本合意又はDPAの条件と矛盾する場合には本セクションが優先しますが、本合意又はDPAにそのほかの変更を加えるものではありません。両当事者は、以下の通り合意します。

(a) お客様は、ClarivateによるFERPAデータの処理に関して、適用法に基づいて必要な通知を提供し、保護者の同意を取得する責任を負います。

(b) 34 CFR § 99.31(a)(1)(i)に従い、Clarivateは、本合意若しくは本DPAにより許容される場合、別途お客様が書面にて許可する場合、又は適用法により義務付けられる場合を除き、FERPAデータを他者に開示することはありません。疑義を避けるために付言すると、お客様は、Clarivateが本サービス提供の目的でFERPAデータをその代理処理者に開示する場合があることに同意します。

最終更新：2025 年 06 月 （Version 3.0）