PTC サイバーセキュリティ及びデータプライバシー追加契約 (DPA)

本DPA は、お客様と PTC（本契約で定義するところによる。）との間の本契約の一部を構成する。お客様は、自己を代表して並びに適用法令上要求される範囲で自己の関連会社の名義及び代理により、本 DPA を締結する。専ら本 DPA の目的上、別段の表示がない限り、「お客様」とは、お客様及びその関連会社を含むものとする。本 DPA において定義していないすべての定義語は、本契約に基づく意味を有するものとする。

1. 目的及び範囲

当事者は、本 DPA が、お客様を代理してPTC が行う個人情報を含む顧客データのすべての処理について適用され、本契約の条件を補足することを合意する。本契約と本 DPA の条件との間に抵触がある場合には、本 DPA の条件が優先するものとする。

2. 解釈

2.1. 「**本契約**」とは、PTC とお客様との間の契約であって、その条件に基づき PTC がお客様に本件サービスを提供するものをいい、SaaS基本契約、PTCのお客様との契約（ライセンス契約）、グローバル・サービス契約などを含むがこれらに限られない。

2.2. 「**適用法令**」とは、GDPR、UK GDPR、CCPA、LGDP、その他、個人情報の取扱い及び／又は個人のプライバシー権の保護又は個人情報の取扱いに関するあらゆる法令をいう。

2.3. 「**CCPA**」とは、カリフォルニア州消費者プライバシー法（2020 年カリフォルニア州プライバシー権法による改正を含む。）[Ca. Civ. Code 1798.100 以下参照] をいい、カリフォルニア州の法務長官により提供される関連規制及びガイドラインをいう。

2.4. 「**管理者**」とは、個人情報の取扱いの目的及び手段を判断する事業体をいう。

2.5. 「**顧客データ**」とは、非PTCアプリケーションを除く、本件サービスに対してお客様から提出される電子データ及び情報、又は、顧客アカウントデータ及び顧客利用データを除く、その他お客様のためにPTC が処理する電子データ及び情報をいう。

2.6. 「**顧客アカウントデータ**」とは、お客様と PTC との関係に関連した個人データをいい、お客様のアカウントにアクセスすることを PTC が許諾する個人の氏名又は連絡先情報（電子メールアドレス、電話番号、役職など）及びお客様が自己のアカウントと関連付けた請求情報（請求先住所を含む。）を含むお客様。顧客アカウントデータには、PTC とお客様との関係の管理若しくは身元確認を目的として又はその他該当する法令上要求されるところに従い、PTC が収集することが必要となり得るデータも含まれる。

2.7. 「**顧客利用データ**」とは、本件サービスの提供に関連してPTCが収集し及び処理する本件サービスの利用データをいい、お客様及びそのユーザーが利用する種別の本件サービスに関するユーザーのアクティビティ、ユーザーのコンピュータ構成、並びにユーザーによる本件サービスの利用に関連した性能測定基準、通信の発信元及び発信先を特定するために使用されるデータ、アクティビティログ、並びに本件サービスの性能を最適化し及び維持するため並びにシステム乱用を調査し及び防止するために使用されるデータを含む。

2.8. 「**データ侵害**」とは、顧客データのセキュリティ、機密性、可用性又は完全性の侵害から生じた顧客データに対する不法な破壊、損失、改ざん、無許諾の開示又はアクセスを生じさせたインシデントをいう。

2.9. 「**GDPR**」とは、EU一般データ保護規則 (EU) 2016/679 及びその規則の国別実施をいう。

2.10. 「**個人**」とは、識別された又は識別可能な自然人をいう。識別可能な自然人とは、特に当該自然人に関連する識別子又はその他の情報を参照することにより、直接的又は間接的に識別しうる者をいう。

2.11. 「**LGPD**」とは、ブラジルの 2018 年 8 月 14 日法律第 13.709 号、一般個人データ保護法（2019 年 7 月 8 日 法律第 13.853 号による改正を含む。）をいう。

2.12. 「**個人情報**」とは、顧客データのうち、特定の個人に関する若しくは関連付けられるもの、又は特定の個人に関連付けることが合理的に可能である又は直接的若しくは間接的に合理的に関連付け得るものをいう。

2.13. 「**処理**」とは、アクセス、収集、記録、編成、構造化、保存、修正又は変更、検索、参照、利用、送信・発信その他の提示方法による開示、配置又は結合、制限、消去又は破壊など、自動化手段によるかどうかを問わず、顧客データに対して実施される単独の又は一連の作業をいう。

2.14. 「**本件サービス**」とは、本契約に定義したサービスをいう。

2.15. 「**標準契約条項**」とは、欧州議会及び欧州理事会の規則 (EU) 2016/679 による第三国への個人データの移転に関する標準契約条項に関する 2021 年 6 月 4 日欧州委員会実施決定 2021/914、並びにスイスからの個人データの移転を対象とするための該当する承認済み改正をいう。

2.16. 「**英国追加契約**」とは、2022 年 3 月 21 日施行の第 B1.0 版である、英国情報コミッショナーが発行する EU 委員会標準契約条項の国際データ移転追加契約をいう。

2.17. 「**UK GDPR**」とは、2018の英国の欧州連合（離脱）法第3条により英国法に保存されたGDPRを意味します。

本 DPA は、適用法令で規定される権利及び義務に抵触し又は個人の基本的権利若しくは自由を損なうような形で解釈されてはならないものとする。

3. 目的の制限

PTC は、本件サービスの提供に必要な場合にのみ、及び本DPA及び本契約に定めるところに従って、顧客データを取扱うものとする。PTC は、(i) 顧客データを販売せず、(ii) 本件サービスの提供又は本 DPA に定める以外の商業目的で、顧客データの保持、利用若しくは開示を行わず、又は (iii) 本契約外で顧客データの保持、利用若しくは開示を行わないものとする。PTC は、顧客データに対する留置権、先取特権、担保権その他の権益を保有又は主張しないものとし、第三者にもこれらを認めないものとする。

4. 処理の期間

PTC による顧客データの処理は、本契約（本 DPA を含む。）の期間のみ、行われるものとする。

5. 処理のセキュリティ

5.1 PTC は、顧客データのセキュリティを確保し、顧客データをデータ侵害から保護するために、付属書 II に定める技術的及び組織的措置を確立し、本契約の期間中これを維持するものとする。適切なセキュリティの水準を評価するにあたっては、最新技術、実施費用、処理作業の性質、範囲、背景及び目的、並びに関連するリスクについて考慮済みである。

5.2 PTC は、本件サービスの提供上厳格に必要となる範囲において、自己の人員及びサブプロセッ

サーのメンバーに対してのみ、顧客データへのアクセス権を付与するものとする。PTC は、顧客データの処理権限を有する者が、秘密保持を確約し又は適切な法定の秘密保持義務を負うよう、確保するものとする。PTC は、顧客データへのアクセス権を有する人員に対し、該当するサイバーセキュリティ及びデータプライバシーの対策に関するトレーニングを定期的に行う。

5.3 契約当事者間のいかなる既存の契約上の取決めも損なうことなく、PTC は、すべての顧客データを厳秘扱いするものとし、顧客データの処理に従事する自己のすべての従業員、代理人又は承認済みサブプロセッサーに対し、その機密性を告知するものとする。

6. 監査

6.1 PTC は、サイバーセキュリティ及びプライバシーの技術的及び組織的対策について十分性を検証するために、独立第三者監査人又は内部監査人により定期的に監査を受けることとする。要請に応じて、PTC は、i) 監査報告書の概要書面をお客様に提供するものとし、ii) PTC による本 DPA 及び適用法令の遵守を確認するために必要となる、顧客データの処理に関連してお客様から行われる合理的なすべての情報請求（情報セキュリティ及び監査の質問表に対する回答を含む。）に対し、回答書面を交付するものとする。ただし、お客様は、一暦年につき一回を超えて当該権利を行使しないものとする。PTC が、ドキュメンテーションに記載されるところに従い特定の本件サービスに関して ISO 27001 認証及び SSAE 18 Service Organization Control (SOC) 2 報告書を取得済みである場合、PTC は、本契約の継続期間、それらの認証若しくは規格又はそれらの適切かつ同等の後継版を維持することに同意する。

6.2 適用法令上要求される場合、かつお客様の合理的な見解において、上記第 6.1 条に基づく権利の行使によって本 DPA 及び適用法令の遵守が実証されていないと思われる範囲に限り、お客様及びその授権代表者は、PTC による本 DPA の条件の遵守を確認するために、本契約の期間中、監査（検査を含む）を実施することができ、その監査（又は検査）については、合理的な通知後、PTC の通常営業時間中に実施されなければならない。PTC 及びお客様は、監査の時期及び継続期間を含む監査の範囲並びにお客様が責任を負うべき償還費用に合意するものとする。すべての償還費用は、PTC 又はその代理人により消費されたリソースを考慮の上、合理的なものでなければならない。

6.3 本第6条は、本 DPA 及び適用法令の遵守を実証する過程で開示及び提供が行われるすべての情報について機密を保護するためにお客様及びその独立検査人が NDA を適宜締結することを条件とする。

7. データ侵害の通知

7.1 PTC では、データ侵害を構成するおそれのあるインシデントを検出し、速やかに対応するために設計された管理及び方針を実施している。PTC は、当該インシデントを調査してデータ侵害が実際に発生したかどうかを確認し、データ侵害の根本原因を特定し、起こり得る悪影響を軽減して再発を防止するように設計された合理的な対策を講じるために、速やかにエスカレーション経路を定義する。データ侵害が生じた場合には、処理の性質及び取得可能な情報を考慮の上、PTC は、お客様が適用法令に基づく義務を遵守できるよう協力及び支援を行うものとする。

7.2 データ侵害が生じた場合には、PTC は、いかなる場合もそのデータ侵害を PTC が認識した後 72 時間以内で、不当な遅滞なく、お客様に通知するものとする。可能な場合、この通知には、少なくとも、次の事項を含めるものとする。

(a) 「何が起こったか」。データ侵害の性質、それが最初に特定された日時及び判明している範囲で起こる可能性の高い結果についての説明。

(b) 「どのような情報が関わっているか」。可能な場合には、影響を受けた顧客データの性質、個人の区分及び概数、並びに判明している場合には関係したデータ記録。

(c) 「PTCが講じている対策」。起こり得る悪影響を軽減するためなど、データ侵害に対処するために講じた又は講じようとしている対策。

(d) 「顧客が講じることができる対策」。データ侵害の影響を軽減するためにお客様側で講じるよう PTC が推奨する対策。

(e) 「詳しい情報について」。データ侵害に関する詳しい情報を取得することができる連絡窓口の詳細。

7.3 こうした情報をすべて同時に提供することが可能でない場合にはその限りにおいて、提供可能となり次第、不当な遅滞なく追加的な情報を提供するものとする。

7.4 適用法令上要求されない限り、PTC は、お客様の書面による同意（不当に拒否してはならないものとする。）を事前に照会し取得しなければ、データ侵害に関連して、いかなる個人に対しても又は法執行機関、科学捜査官、保険提供者若しくは法律顧問以外のいかなる第三者に対しても、お客様の名称又は身元を通知しないものとする。データ侵害により PTC のその他の顧客に影響が及ぶ範囲において、一般的な公式声明は、お客様の身元が開示されない限り行うことができる。

8. 個人情報の処理

8.1 当事者は、個人情報の取り扱いそれ自体が本件サービスの主題ではないことを明示的に合意する。ただし、当事者らは、PTC が個人情報の提供をある程度受ける可能性があることを完全に排除できないことを確認する。したがって、本 DPA の条件は、そうした個人情報の開示を理由として、お客様の代理で PTC が行う個人情報の取り扱いを規制するものでなければならない。個人情報に関して、お客様は、次に掲げる事項の責任を有する：i) 処理の法的根拠を確認すること、ii) 該当するすべてのプライバシー通知が個人に対し提供されるよう確保すること、並びにiii)適用法令上要求される場合には、同意を取得すること。お客様は、健康データ、政府 ID、クレジットカード情報、支払カード情報又は適用法令上定義される特別区分データなど、機密性のある情報が個人情報に含まれないように確保するために、合理的な手順を講じるものとする。処理の作業の詳細、特に個人情報の区分及びお客様の代理で個人情報の取り扱いが行われる処理の目的は、付属書Iで定められる。

8.2 PTC は、お客様からの指示書面に基づいてのみ、個人情報の処理を行うものとする。本契約（本 DPA を含む。）は、その最初の指示書面を構成する。PTC は、お客様のその他の指示については、適用法令上要求され、技術的に実現可能であり、本件サービスの履行に対する変更を必要としないものである限り、遵守するよう合理的な努力をする。前述のいずれかの例外に該当する場合又はその他 PTC が指示を遵守することができない場合若しくは適用法令に抵触する指示であると判断した場合には、PTC は、直ちにお客様に通知（電子メールが認められる。）する。

8.3 PTC は、適用法令上個人情報の取り扱いを要求される場合についても、その処理を行うことができる。その場合において、PTC は、取り扱い前にその法的要件をお客様に告知するものとするが、公益上の重要な事由に基づき法律上その告知が禁止されるときは、この限りでない。

8.4 お客様は、個人情報の正確性、品質及び合法性並びにお客様が個人情報を取得した方法については、単独で責任を負うものとする。したがって、適用法令に準拠して個人情報が収集され PTC に送信されるよう確保すること、特に、処理の法的根拠を有すること並びに個人に対しその個人

情報の収集及び取り扱いを適切に告知することは、お客様の責任となる。

9. サブプロセッサーの利用

9.1 PTC は、本件サービスの履行上厳格に必要となる場合には、個人情報を取扱うためのサブプロセッサーを起用することに関して、お客様の一般的許諾を受けている。お客様は、https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions に掲載されるサブプロセッサーを承認する。PTC は、当該リストの変更予定については、30 日以上前にサブプロセッサーを追加し又は差し替えて、そのサブプロセッサーの起用前に当該変更に異議申立てできる十分な時間をお客様に与えることにより、お客様に書面をもって告知するものとする。PTC は、お客様が異議申立権を行使できるよう必要な情報を、お客様に提供するものとする。

9.2 PTC は、サブプロセッサーを起用する場合には、本 DPA に基づく PTC の義務と内容的に同一の処理及びサイバーセキュリティの義務をサブプロセッサーに課す契約を通じて、これを行うものとする。

9.3 PTC は、本 DPA に従いサブプロセッサーの義務の履行について引き続きお客様に対し完全な責任を負うものとする。

10. 個人情報の国際間移転

10.1 グローバル企業として、PTC は、お客様又は個人が所在する国以外で個人情報を取扱うことが必要な場合がある。そうしたすべての個人情報の移転は、適用法令に従うものとし、PTC は、適切な保護策が維持され、個人の権利が実行可能なものとなり、及び有効な法的救済手段が利用可能となるよう、確保するものとする。

10.2 **EEA 及びスイスの個人情報：**当事者は、お客様がEEA 又はスイスからPTCに、直接的に又は転送により、個人情報を移転する場合において、十分な水準の個人データ保護の提供が欧州委員会（又はスイスからの移転の場合には、該当する管轄当局） により認定されていない EEA 又はスイス外の国又は受取人への移転に関しては、標準契約条項が適用されることに合意する。EU 標準契約条項の対象となる EEA からの個人情報の移転に関して、EU 標準契約条項は、付属書 III に従って締結され（この参照により本 DPA に組み込まれ） 完成されたものとみなされる。

10.3 PTC の拘束的企業準則：処理者方針（Binding Corporate Rules: Processor Policy） が適用される場合、拘束的企業準則：処理者方針のすべての規定は、参照により本 DPA に組み込まれ、その全部が本 DPA 内で定められている場合と同様に拘束力を有しお客様が行使できるものとする。本 DPA と拘束的企業準則：処理者方針との間に抵触又は不一致がある場合には、拘束的企業準則：処理者方針が優先するものとする。

優先順位. お客様とPTC との間において複数の移転メカニズムが適用される場合、個人情報の移転は、次に掲げる優先順位に従って単一の移転メカニズムに従う：(i) 拘束的企業準則：処理者方針、及び (ii) 標準契約条項。

10.4 **英国追加契約.** 当事者は、お客様が英国からPTCに、直接的に又は転送により、に個人情報を移転する場合において、十分な水準の個人データ保護の提供が英国の管轄規制当局又は政府機関により認定されていない英国外の国又は受取人への移転に関しては、英国追加契約が適用されることに合意し、及び付属書 III に従って締結され（この参照により本 DPA に組み込まれ）

完成されたものとみなされる。

10.5 **その他の国際移転：**非 EEA 国、スイス又は英国で設立されたお客様の代理で、PTC が個人情報を取扱う場合、PTC は、適用法令に従って移転が行われるよう確保するものとする。これには、適用法令に従って拘束的企業準則を実現している受取人に対し、又は該当するデータ保護当局により採用され若しくは承認される標準的な契約条項を締結している受取人に対し、個人情報を移転する場合が含まれる。

11. データプライバシー義務に関する顧客支援

11.1 PTC は、個人から受領した適用法令に基づく権利行使の申し出があれば、速やかにお客様に通知するものとする。PTC は、対応を行うことがお客様から許諾されない限り、その申し出に対して対応を行わないものとする。

11.2 処理作業の性質及び自己が保有する利用可能な情報を考慮の上、PTC は、a) 個人からの権利行使の申し出に対応するためにお客様が義務を果たすことができるよう支援するものとし、b) お客様による下記義務の適用法令に基づく遵守を支援するものとする。

(a) 個人情報の処理作業に関するリスクの評価又は予想される処理作業により個人情報の保護に生じる影響の評価（「データ保護影響評価」） を行う義務
(b) お客様が講じるリスク軽減策がなければ処理作業によって高いリスクが生じることになるとデータ保護影響評価により示される場合において、個人情報の処理作業前に管轄監督当局に相談する義務
(c) 取扱う個人情報が不正確である又は古くなったことを PTC が認識した場合には、遅滞なくお客様に連絡することにより、個人情報が正確かつ最新のものとなるよう確保する義務
(d) 個人情報処理のセキュリティに関する義務の遵守をお客様が確保することができるよう支援する義務

12. 管理者としての PTC：

お客様は、顧客アカウントデータ及び顧客利用データに関して、PTC がお客様との共同の管理者ではなく独立した管理者であることについて確認し及び同意する。PTC は、(i) お客様との関係を管理するため、(ii) 会計目的及びコンプライアンス目的など本会社の中核的業務を実施するため並びにお客様との関係管理のため、(iii) 本件サービスの詐欺、セキュリティインシデントその他の誤った利用について監視、調査、防止及び検出を行うため並びにお客様及び顧客データへの被害を防止するため、(iv) 身元確認目的のため、(v) PTC が従う、個人情報の処理及び保持に適用される法令上の義務を遵守するため、並びに(vi)その他適用法令上認められるところ並びに本 DPA 及び本契約に従い、管理者として顧客アカウントデータ及び顧客利用データを取扱う。PTC はまた、適用法令上認められる範囲において、トラブルシューティング事項を行うこと並びに新たな製品及び機能を開発し並びにそれらの開発の参考とすることを含め、本件サービスの提供、最適化、強化及び維持を行うために、管理者として顧客利用データを取扱う。管理者として PTC が行う処理作業は、https://www.ptc.com/en/documents/policies/privacy より入手可能な PTC のプライバシー方針に従うものとする。

13. CCPA規定

お客様と PTC との間において、CCPA の目的上、お客様は、「事業体」であり、PTC は、「サービ

ス提供者」であり、事業目的で個人情報を受領するものである。PTC は、「第三者」に対し個人情報を「販売」又は「共有」せず、また、本契約に従いお客様への本件サービスを履行する具体的目的のために必要となる場合その他本契約に定められる又は CCPA により認められる場合を除き、個人情報の保持、利用又は開示を行わないものとする。これらの目的上、「事業体」、「サービス提供者」、「第三者」、「販売」及び「共有」とは、CCPA 第 1798.140 条においてそれらに定められた意味を有する。PTC は、本第 13 条の各制限を理解していること及びそれらを遵守することを保証する。

14. 本 DPA の不遵守、及び契約終了

本 DPA に基づく各当事者及び各当事者の関連会社の責任は、本契約で規定される責任の排除及び制限に従うものとする。本 DPA に基づく PTC 又はその関連会社に対する請求は、本契約の当事者であるお客様の事業体が提起するものとする。いかなる場合においても、本 DPA 又はいずれの当事者も、個人又は管轄監督当局の権利を制限せず又は限定しないものとする。

15. 顧客データの検索及び削除

本契約の終了又は満了に伴い、お客様は、本契約に記載されるところに従い顧客データを書き出すことができ、又は顧客データが書き出すことができない場合には、PTC は、お客様に顧客データを返還するものとする。PTC は、適用される法令により顧客データの継続的保存が要求されない限り、本契約の条件に従い、終了の約 30 日後にすべての顧客データを削除するものとする。顧客データが削除され又は返還されるまで、PTC は、本 DPA の遵守を確保し続けるものとする。

16. 雑則

16.1 当事者らは、本件サービスに関連して当事者らが従前に締結していた既存の DPA があれば本 DPA がそれに取って代わることを合意する。

16.2 本 DPA は、適用法令により別段の要求がない限り、本契約の準拠法・管轄権規定に準拠し、それに従って解釈する。

16.3 本 DPA 及び標準契約条項は、本 DPA 第 15 条に従い PTC が行う顧客データの削除に伴い、同時かつ自動的に終了する。

[以下余白]

付属書I

取扱う個人情報のデータ主体の区分

お客様は、本件サービスに対して個人情報を提出することができ、その範囲は、お客様が単独の裁量により判断し及び管理するものであり、これには、下記区分の個人に関する個人情報などが含まれる場合がある。

- お客様の（自然人である） 従業員、代理人、顧問、フリーランス
- お客様の顧客、見込み客、業務提携者及び業者における従業員又は連絡担当者
- お客様が本件サービスの利用を許諾したお客様のユーザー

取扱う個人情報の区分

お客様は、本件サービスに個人情報を提出することができ、その範囲は、お客様が単独の裁量により判断し及び管理するものであり、これには、下記区分の個人情報などが含まれる場合がある。

- 氏名
- 肩書
- 役職
- 雇用者
- 連絡先情報 (会社、電子メール、電話、仕事先住所)
- ID データ

データ及び関係リスクについての性質を十分に考慮した、機密性あるデータの処理（該当する場合） 及び制限又は保護策の適用、たとえば、厳格な目的制限、アクセス制限（特別なトレーニングを終えたスタッフにアクセスを限定することを含む。）、データへのアクセス記録の保持、転送の制限又は追加的なセキュリティ対策など。

- なし

処理作業の性質

- 本件サービスの提供上必要となる、収集、記録、編成、構造化、保存、翻案・改変、検索、参照、送信・発信その他の提供方法による開示、制限、消去又は破壊

お客様の代理で個人情報の処理が行われる目的

- 本契約で具体的に定義される本件サービスの提供

処理作業の継続期間

- 本契約に基づき PTC が本件サービスを提供する期間、及びその期間の延長又は更新

付属書 II

顧客データのセキュリティを確保するための技術的及び組織的対策

「ネットワーク」とは、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）を用いて互いに接続されたデータの共有を可能にするために相互接続される、コンピュータ、サーバー、メインフレーム、ネットワークデバイス、周辺機器その他のデバイスの集合体をいう。

「セキュリティ管理」とは、情報技術システム及び関連物理施設におけるセキュリティリスクに対処し又は関連方針を実施するための方法として、本契約の条件に準拠した、NIST 800-53 を実施するために必要となる特定のハードウェア、ソフトウェア又は管理メカニズムをいう。セキュリティ管理では、特定の集団、個人又は技術に関連したセキュリティ方針上の要素を実施するために用いられるべき、技術、方法、実施手順その他の具体的要素又はその他のプロセスが指定される。

「セキュリティ方針」とは、セキュリティに関係する会社情報を確保するため及び該当する法令の遵守を義務付けるための指針をいう。

「セキュリティ手順」とは、NIST 800-53 の遵守又は ISO27001 の認証を達成し及び維持するために行われる段階的な措置をいう。

「システム等」とは、コンピュータソフトウェア、ファームウェア、コンピュータハードウェア（一般的な目的又は特定の目的の別を問わない。）、電気通信能力（音声、データ及び映像の全ネットワークを含む。）その他類似する又は関連する自動化、コンピュータ化又はソフトウェアの項目をいう。

本契約及び DPA に基づきセキュリティ義務を遵守するために、PTC は、常に、(i) ISO27001 認証など業界最高基準に即したセキュリティプロセスを備えるか、又は国立標準技術研究所 (NIST) 800-53 セキュリティ要件の「中位レベル」の影響管理を実施済みでなければならず、(ii) 本 DPA に定めるセキュリティ上の要件、義務、仕様及びイベント報告手順を備える。

1. セキュリティプログラム及びガバナンス

PTC は、常に、下記を含むセキュリティプログラムを維持する。

(a) 下記要件を管理する、CISO（最高情報セキュリティ責任者）又はセキュリティ担当被指名者
(b) セキュリティ方針、セキュリティ手順及びセキュリティ管理
(c) セキュリティインシデント管理プログラム
(d) 本件の業務委託を支援する全従業員に向けた、セキュリティ周知・トレーニングプログラム
(e) セキュリティ変更プロセス中、PTC のセキュリティ環境の安定性及び信頼性を促進するための、セキュリティ変更管理プログラム
(f) 事業継続計画及び災害復旧計画（定期的な検査を含む）
(g) リスクアセスメントについて特定、評価、対応及び実施を行うための、セキュリティリスク評価プロセス
(h) 本件の業務委託の一環としてプロバイダがソフトウェアを開発し提供する場合、プロバイダは、OWASP OPEN SAMM など業界基準に即した安全なソフトウェア開発ライフサイクルを維持する。

(i) 本件の業務委託の一環としてプロバイダがクラウドサービス（LaaS、PaaS、SaaS） を提供している場合、プロバイダは、CSA CCM 及び SOC2 の規格に即して諸慣行を調整する。

2. 設計及び検査によるセキュリティ

PTC は、下記を維持する。

(a) NIST 800-53 の効果的なセキュリティ管理の調整及び実施を合理的に確保する、セキュリティアーキテクチャ

(b) データ保護のために必要となる、効果的なファイアーウォール・侵入検出技術のシステム

(c) データの分離を実現する、適切なネットワーク上のセキュリティ設計要素

(d) 送信時及び保存時の情報を暗号化するための手順

(e) PTC のセキュリティ上のシステム及びプロセスの定期的な検査を確立するための手順

(f) 当該システムを通じて収集、処理及び送信が行われるお客様のデータを保護するように設計されたウェブサイトアプリケーションの構築を実現するための、データベース及びアプリケーション層の設計プロセス

3. 監視及びパッチ管理

PTC は、下記を確立済みであり、本契約の期間中それらを維持する。

(a) セキュリティパッチを最新の状態に維持するためのメカニズム

(b) お客様のデータへの未遂の及び実際の攻撃又は侵入を検出するための監視システム・手順

(c) セキュリティ警報について監視、分析及び対応を行うための手順

(d) アンチウイルス及びアンチマルウェアの最新市販ソフトウェアの使用及び定期更新

(e) インストールされたソフトウェアの完全性を定期的に検証するための手順

4. PTC 許可ユーザーによるリモートアクセス管理

PTC は、下記を実施する。

(a) 「Need to Know（必要最小限の利用者への権限付与）」の原則に準拠したユーザー認証・許可の適切なメカニズム

(b) 適宜、PTC 及びサブプロセッサーの両方で、リモート許可ユーザーに関する厳格なアクセス制限を実施するための管理

(c) 許可ユーザーのアカウント・認証管理の適時かつ正確な管理

(d) すべてのパスワードを暗号化し又はハッシュ化するためのメカニズム

(e) アクティブでないアカウント／廃止／移転された許可ユーザーについてアクセス権を直ちに取り消すための手順

(f) 職務分掌を維持する手順

(g) コンピュータアクセス権を有する各許可ユーザーに対して一意に ID を割り当てるための手順

(h) パスワード及びセキュリティパラメータに関して PTC から提供された初期設定について変更及び適切な管理を確保するための手順

(i) お客様の作業明細書に関連したシステム等への多要素認証（MFA）の合理的な適用

5. 施設アクセス管理

PTC は、下記を確立済みであり、本契約の期間中それらを実施する。

(a) すべての情報資産及び情報技術に関して、適切なデータセンターでのその資産及び技術の保

存及び保護を確保するための、物理的な保護メカニズム

(b) システム等への物理的アクセスを制限するために整備された適切な施設出入管理

(c) 施設へのアクセスについて監視及び「Need to Know」に基づく制限を確保するための手順

(d) 潜在的な環境ハザード（火災・水害被害など）又は技術的故障に起因する、お客様のデータ及びお客様に従属するシステム等の破壊、損失又は損害を防止するための対策

(e) お客様のすべての機密情報を物理的に保護するため及び不必要となった時点で当該情報を適切に破棄するための管理

[PTC のサイバーセキュリティ及びプライバシー・プログラムに関する詳細は、PTC の ISO27001 及び SOC2 Type II レポートのコピーを入手できる PTC の Trust Center（https://www.ptc.com/en/about/trust-center ）をご覧ください。]

付属書III

標準契約条項

（データインポート先である）PTC Inc. と、（データエクスポート元である）「お客様」（当該移転に関連する自己の関連会社その他の管理者の代理として、お客様が管理者を務める場合を適宜含む。）との間においては、標準契約条項の下記モジュールが適用されるものとし、個々に締結され、参照により組み込まれる。

モジュール 1 –お客様が管理者であり PTC が DPA に従い独立の管理者として個人情報を取扱う場合の移転に関する、管理者から管理者への移転

モジュール 2 –処理者としての PTC への個人情報の移転に関する、管理者から処理者への移転

モジュール 3 - 処理者から処理者への移転（お客様が処理者であり PTC がサブプロセッサーである場合）

標準契約条項に関しては、下記が適用されるものとする。

- 第 9 条 – サブプロセッサーの利用.
    - モジュール 2 及びモジュール 3
        - オプション 2、書面による一般的許可
        - データインポート先は、当該リストの変更予定については、30 日以上前に PTC サブプロセッサーを追加し又は差し替えて、その PTC サブプロセッサーの起用前に当該変更に異議申立てできる十分な時間をデータエクスポート元に与えることにより、データエクスポート元に書面をもって特に告知するものとする。
- 第 17 条 – 準拠法
    - モジュール 1、2 及びモジュール 3
        - オプション 1
        - これらの条項は、第三者受益者権利を認める法律となることを条件として EU 加盟国の一国の法律に準拠するものとする。契約当事者らは、これをアイルランド共和国の法律とすることを合意する。
- 第 18 条 - 法廷地選択及び管轄権
    - モジュール 1、2 及びモジュール 3
    - 契約当事者は、それらをアイルランド共和国の裁判所とすることを合意する。

標準契約条項付属書 I

A. 当事者リスト

- 1 –データエクスポート元は、自己を代表しかつ欧州連合、英国及びスイスに所在する諸管理者を代理する、お客様とする。
- 2 – データインポート先は、121 Seaport Boulevard, Boston, MA 02021 の PTC Inc とし、本契約でのお客様及び PTC それぞれの連絡先詳細が適用されるものとする。

B. 移転についての説明

個人データの移転が行われるデータ主体の区分

- モジュール 1 – 管理者から管理者：
  - PTC の製品を使用し又は PTC のサービスにアクセスすることをお客様から許可された、お客様の従業員、コンサルタント、委託業者、供給者、業務提携者及び顧客である個人。
- モジュール 2 – 管理者から処理者
  - お客様の従業員、コンサルタント、下請業者、サプライヤー、ビジネスパートナー及び顧客。お客様が本件サービスに個人データをアップロードする可能性のあるその他の個人
- モジュール 3 – 処理者から処理者
  - お客様の従業員、コンサルタント、委託業者、供給者、業務提携者及び顧客。お客様が本件サービスに個人データをアップロードする場合があるその他の個人。

個人データの移転が行われるデータ主体の区分

移転が行われる個人データは、下記区分のデータに関係する場合がある。

- モジュール 1：
  氏名、会社、ユーザー名、ユーザー ID、組織、仕事連絡先詳細、PTC の製品・サービスに関するやり取り（ログファイル及びインシデント報告など）。IP アドレス、クッキーデータ、デバイス識別子などのデバイス関連情報。
- モジュール 2 及びモジュール 3：氏名、会社、組織、仕事連絡先詳細、PTC の製品・サービスに関するやり取り（ログファイル及びインシデント報告など）、及び PTC のサービスにアップロードされる個人データ。機密性あるデータの移転は行われない。

移転の頻度（たとえば、データの移転が 1 回限りであるか又は継続的であるかの別など）

継続的処理の性質

データインポート先は、本契約で特に具体的に記載されるところ及び本契約（DPA を含む。）の条件により許可されるところに従い、本件サービスを提供するための必要に応じて、個人データを取扱うものとし、下記が含まれるものとする。

データインポート先による本件サービスの提供上必要となる、収集、記録、編成、構造化、保存、翻案・改変、検索、参照、送信・発信その他の提供方法による開示、制限、消去又は破壊

個人データの保持が行われる期間、又はこれが可能でない場合には、その期間を判断するために用いられる基準。

個人データは、本契約の条件に従い本件サービスの終了時に本件サービスから削除される。

PTC（サブプロセッサー）への移転に関しては、処理の主題、性質及び継続期間も指定する。

参照：https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions

C. 管轄監督当局

- 第 13 条に従い管轄監督当局を特定する。
    - 管轄監督当局は、アイルランド共和国のデータ保護委員会（Data Protection Commission）とする。

標準契約条項付属書 II - 技術的及び組織的対策。

DPA 付属書 II が適用されるものとする。

英国追加契約

(a) 英国追加契約の表 1 に関して、当事者らの詳細及び主要連絡先情報は、本付属書 III のパラグラフ A に掲載される。

(b) 英国追加契約の表 2 に関して、この英国追加契約が付加される承認済み EU SCC、モジュール及び選択条項のバージョンに関する情報は、本付属書 III のパラグラフ B に掲載される。

(c) 英国追加契約の表 3 に関して、

1. 当事者のリストは、本付属書 III のパラグラフ A に掲載される。
2. 移転についての説明は、付属書 III のパラグラフ B（処理の性質）に記載される。
3. 付属書 II（技術的及び組織的セキュリティ対策）は、英国追加契約の付属書 II として適用されるものとする。
4. サブプロセッサーリストは、https://www.ptc.com/-/media/Files/PDFs/legal-agreements/fy18/PTC-Inc-List-of-Sub-processors.pdf に掲載される。

(d) 英国追加契約の表 4 に関して、データインポート先及びデータエクスポート元の両者は、英国追加契約の条件に従い英国追加契約を終了することができる。

2.5 抵触.　EU 標準契約条項又は英国追加契約と本 DPA 又は本契約の他の条件との間に抵触又は不一致がある範囲においては、適宜、EU 標準契約条項又は英国追加契約の規定を優先する。