データ処理に関する付属書 - GDPR
DATA PROCESSING ADDENDUM - GDPR

日本 CA 株式会社（「CA」）
〒102-0093 東京都千代田区平河町二丁目 7 番 9 号 JA 共済ビル

本データ処理に関する付属書（以下「**DPA**」または「本付属書」といいます）は、データ保護法の要件に従ってお客様の個人データを処理することに関する両当事者の合意を反映するため、お客様と CA との間で締結された既存契約、および／または CA とお客様との間で CA が提供するサービスの購入に関して締結されるその他の書面契約もしくは電子契約（以下「**原契約**」といいます）の一部を構成するものです。本 DPA の発効日は、下記の記名押印または署名欄の遅い方の日付とします。本書に定義されていない用語は、原契約に定められる意味を持つものとします。

This Data Processing Addendum ("**DPA**" or "Addendum") forms part of the existing agreement(s) between Customer and CA, and/or other written or electronic agreement between CA and Customer for the purchase of Services provided by CA (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data of Customer, in accordance with the requirements of Data Protection Laws. The Effective Date of this DPA is the date of the last signature of a party below. All capitalized terms not defined herein shall have the meaning set out in the Agreement.

1. 雑則
GENERAL TERMS

本 DPA は、（第 11 条に定義される）EU 一般データ保護規則 2016/679（以下「GDPR」といいます）の適用範囲において、お客様に代わって CA が個人データを処理する場合に適用されます。2018 年 5 月 25 日より、CA は自身のサービス提供に直接適用される GDPR の要件に従って個人データを処理します。本 DPA は、原契約（原契約のデータ処理に関する既存の付属書を含みます）において以前にお客様が交渉した顧客データの処理に関するデータ保護の約束を制限あるいは軽減するものではありません。
This DPA applies to the Processing of Personal Data, within the scope of the EU General Data Protection Regulation 2016/679 (as further defined in Section 11, and hereinafter "GDPR"), by CA on behalf of Customer. Effective May 25, 2018, CA will Process Personal Data in accordance with the GDPR requirements directly applicable to CA's provision of its Services. This DPA does not limit or reduce any data protection commitments relating to Processing of Customer Data previously negotiated by Customer in the Agreement (including any existing data processing addendum to the Agreement).

本付属書に記名押印または署名することにより、お客様は、自身を代表して DPA を締結し、また、お客様の認定関連会社がデータ管理者とされる個人データを CA が処理する場合、適用されるデータ保護法の求める範囲で、かかる認定関連会社の名義でその代理として DPA を締結します。本 DPA においてのみ、本書に別途の記載がない限り、「お客様」にはお客様と認定関連会社が含まれるものとします。
By signing this Addendum, Customer enters into the DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent CA Processes Personal Data for which such Authorized Affiliates qualify as the Data Controller. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein.

原契約に基づいてお客様にサービスを提供するうえで、CAはお客様に代わって個人データを処理することができます。CAは、サービスの提供に関連してお客様のために処理される個人データについて、以下の規定に準拠することに同意します。関連条項に別途定義がない限り、本DPAに適用される定義はすべて第11条「定義」にまとめられています。
In the course of providing the Services to Customer pursuant to the Agreement, CA may Process Personal Data on behalf of Customer. CA agrees to comply with the following provisions with respect to any Personal Data Processed for Customer in connection with the provision of the Services. If not otherwise defined in the relevant section, all definitions applicable to this DPA have been consolidated into Section 11, titled "Definitions."

2. 個人データの処理
PROCESSING OF PERSONAL DATA

2.1 両当事者は、個人データの処理に関してはお客様がデータ管理者でCAがデータ処理者であること、また、CAまたはCAグループ会社が以下の第5条「複処理者」に定められる要件に従って複処理者を業務に従事させることに同意します。
The parties agree that with regard to the Processing of Personal Data, Customer is the Data Controller, CA is a Data Processor and that CA or members of the CA Group will engage Subprocessors pursuant to the requirements set forth in Section 5 "Subprocessors" below.

2.2 お客様は、サービスを使用または受領する際にはデータ保護法の要件に従って個人データを処理するものとし、個人データの処理に関する指示がデータ保護法に準拠するようにします。お客様は、個人データおよびお客様が個人データを収集する手段の正確性、品質、適法性について、単独で責任を持つものとします。
Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 CAは、自身のサービス提供に直接適用されるデータ保護法、GDPRの要件に従って個人データを処理します。CAは、お客様の文面による指示によってのみ個人データを処理し、個人データを秘密情報と同等の注意を払って扱うものとします。お客様は、以下を目的として個人データを処理するようCAに指示するものです。(i)原契約および適用される注文書に従うための処理。(ii) 原契約の条件と矛盾しない、お客様からのその他合理的な指示（サポート・チケットによるものなど）に従うための処理。 (iii) CA またはCA関連会社に適用される適用法（該当するデータ保護法などが含まれます）で求められる個人データの処理。この処理を行う場合、適用法によって認められる限り、CAまたは該当するCA関連会社は、法の求めによる個人データの処理をお客様に通知するものとします。
CA will Process Personal Data in accordance with applicable Data Protection Laws, the GDPR requirements, directly applicable to CA's provision of its Services. CA shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions and shall treat Personal Data with the same care as Confidential Information. Customer instructs CA to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable orders; (ii) Processing to comply with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement, and (iii) Processing of Personal Data that is required under applicable law to which CA or CA Affiliate is subject, including but not limited to applicable Data Protection Laws, in which case CA or the relevant CA Affiliate shall to the extent permitted by applicable law, inform the Customer of such legally required Processing of Personal Data.

2.4. GDPR第28（3）条が要求するとおり、処理の主題と期間、処理の性質と目的、個人データの種類、データ主体の区分は、本DPA付属書の別紙1（「別紙1: お客様の個人データ処理の詳細」）に定められています。CAによる個人データ処理の主題は、原契約に基づいて提供されるサービスの履行です。お客様は、事前の書面による通知により、GDPR第28（3）条の要求を満たすために必要であると自身が合理的に判断する別紙1への合理的修正を要求することができ、CAは要求された変更をレビューします。別紙1の記載内容は、この付属書のいずれの当事者に対しても権利の付与および義務の付加を行うものではありません。
As required under Article 28(3) of the GDPR, the subject matter and duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Annex I to this DPA Addendum (titled "Annex 1: Details of Processing Customer Personal Data"). The subject matter of Processing of Personal Data by CA is the performance of the Services provided under the Agreement. Upon prior written notice, Customer may request reasonable amendments to Annex 1 as Customer reasonably considers necessary to meet the requirements of Article 28(3) of the GDPR and CA will review such requested changes. Nothing in Annex 1 confers any right or imposes any obligation on any party to this Addendum.

3. データ主体の権利
RIGHTS OF DATA SUBJECTS

3.1. CAは、適用法によって認められる限り、データ主体から本人のアクセスの権利、訂正の権利、処理の制限、消去（「忘れられる権利」）、データ・ポータビリティ、処理に対する異議、あるいは個人に対する自動化された意思決定の対象とならない権利を行使する要求を受けた場合（以下「**データ主体の要求**」といいます）、速やかにお客様に通知するものとします。処理の性質を考慮し、CAは、GDPR第3章に基づくデータ主体の要求に応じるお客様の義務を履行できるよう、適切な技術的および組織的対策によって、可能な範囲でお客様を支援するものとします。適用法の要件でなければ、要求がお客様に関係すると確認できる場合を除き、CAは事前の書面によるお客様の同意なく、かかるデータ主体の要求に対応しないものとします。
CA shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Taking into account the nature of the Processing, CA shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Chapter III of the GDPR. Except to the extent required by applicable law, CA shall not respond to any such Data Subject Request without Customer's prior written consent except to confirm that the request relates to Customer.

3.2 さらに、サービスを使用するお客様がデータ主体の要求に対応することができない場合、お客様の要求を受けたCAは、法的に認められる範囲で、データ主体の要求が適用されるデータ保護法に基づく要件であるならば、データ主体の要求に対応するうえでお客様を支援するために商業的に合理的な努力をします。法に認められる範囲に限り、かかる支援から発生する費用はお客様の負担とします。
Further, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, CA shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent CA is legally permitted to do so and provided that such Data Subject Request is required under applicable Data Protection Laws. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

4. 人員
PERSONNEL

4.1 CAは、個人データの処理に従事するCAの人員が個人データの秘密性を通知され、自らの責任について適切なトレーニングを受け、秘密保持に関する義務が適用されてCAとの契約が解除された後も義務が存続するようにします。
CA shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with CA.

4.2 CAは、個人データの処理に従事するCAの人員の信頼性を確保するために商業的に合理的な措置を講じるものとします。
CA shall take commercially reasonable steps to ensure the reliability of any CA personnel engaged in the Processing of Personal Data.

4.3 CAは、CAグループによる個人データへのアクセスが、原契約を履行するためにかかるアクセスを必要とする者に限定されるようにします。
CA shall ensure that CA Group's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4 **データ保護担当者** CAグループ会社は、データ保護法が要求するとおりにデータ保護担当者を任命しました。任命された担当者とは、datatransfers@ca.comで連絡を取ることができます。
Data Protection Officer. Members of the CA Group have appointed a data protection officer where such appointment is required by Data Protection Laws. The appointed person may be reached at datatransfers@ca.com.

5. 複処理者
SUBPROCESSORS

5.1 お客様は、(a) CAの関連会社が複処理者として委任されること、および(b) サービスの提供に関連して、CAとCAの関連会社それぞれが第三者の複処理者を業務に従事させることがあることを認め、これに同意します。かかる複処理者は、CAが複処理者を委任した目的であるサービスを提供することのみを目的として個人データを取得することを許可され、これ以外の目的のために個人データを使用することは禁じられます。
Customer acknowledges and agrees that (a) CA's Affiliates may be retained as Subprocessors; and (b) CA and CA's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Any such Subprocessors will be permitted to obtain Personal Data only to deliver the services CA has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

5.2 原契約に別途定められていない限り、CAは、各複処理者によるサービスを自身が本DPAに基づいて直接実施する場合に負うのと同じ責任を、かかる複処理者の作為と不作為について担うものとします。
CA shall be liable for the acts and omissions of its Subprocessors to the same extent CA would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.3 CAまたはCA関連会社は、各複処理者と書面による契約を締結しました。この契約には、かかる複処理者が提供するサービスの性質に該当する範囲で、個人データの保護に関して本付属書に定められた条件の保護レベルを下回らず、GDPR第28(3)条の要件またはその他のデータ保護法における同等の規定を満たす条件が含まれています。
CA or CA Affiliate has entered into a written agreement with each Subprocessor containing data protection obligations that are no less protective than the terms set forth in this Addendum with respect to the protection of Personal Data and meet the requirements of Article 28(3) of the GDPR or equivalent provisions of any other Data Protection Law, to the extent applicable to the nature of the Services provided by such Subprocessor.

5.4 お客様は、本第5条に従い、CAおよび各CA関連会社が複処理者を任命する権限を与えます。サービスの提供に関連してCAが使用するCA複処理者のリストは別紙2に記載されているとおりであり、かかるリストにはすべての複処理者の身元および所在国が含まれています(以下「**複処理者リスト**」といいます)。かかるリストにCAが変更を加える場合、最新の複処理者リストはhttps://support.ca.com/us/product-content/admin-content/subprocessor-list.htmlにてお客様に公開され (以下第5.5項に定められるとおりに)お客様が変更への異議を表明する機会が与えられます。
Customer authorizes CA and each CA Affiliate to appoint Subprocessors in accordance with this Section 5. The list of CA Subprocessors used by CA in connection with its provision of the Services is set forth in Annex 2, and such list includes all Subprocessors' identities and country of location ("**Subprocessors List**"). In the event CA makes any changes or additions to such list, the current Subprocessor List is made available to Customer at: https://support.ca.com/us/product-content/admin-content/subprocessor-list.html, thereby giving Customer the opportunity to object to such changes (as set further set forth in section 5.5 below) .

5.5 お客様は、CAが複処理者のリストを更新してから10営業日以内に速やかに書面にてCAに通知することにより、CAによる新しい複処理者の使用に対して異議を唱えることができます。お客様から異議があった場合、CAは、お客様の異議に対応するために商業的に合理的な努力し、かかる異議の対応について合理的な書面による説明を提供します。
Customer may object to CA's use of a new Subprocessor by notifying CA promptly in writing within ten (10) business days after any updates are made by CA to the Subprocessor list. In the event of such objection by Customer, CA will take commercially reasonable steps to address the objections raised by Customer and provide Customer with reasonable written explanation of the steps taken to address such objection.

5.6 **データ転送** CAは、適用されるデータ保護法に従って合法的の場合を除き、お客様の個人データを転送しないものとします。個人データがhttps://www.ca.com/jp/legal/privacy/data-transfers.htmlに記載された CA の表明および諸条件に従って転送されます。本第5.6項に従って、原契約に基づくお客様にサービスを提供することを唯一の目的として、お客様は本書にて、個人データを現地のCAグループ会社および/またはCAの認定された複処理者に日常的に転送する権限をCAに与えます。上記にかかわらず、お客様の個人データが欧州連合、欧州経済域および/またはその加盟国、スイス、イギリスから、それら地域のデータ保護法が意味する

十分なレベルのデータ保護を確保していない国に転送される場合（以下「**限定的転送**」といいます）、CAはかかる限定的転送に関して第5.6(a)項の条件を遵守します。
Data Transfers. CA shall not transfer Personal Data of Customer except lawfully, in compliance with applicable Data Protection Laws. Personal Data will be transferred in accordance with CA's statement and terms set out at https://www.ca.com/us/legal/privacy/data-transfers.html . Solely for the provision of Services to Customer under the Agreement and subject to this Section 5.6, Customer hereby authorizes CA to make routine transfers of Personal Data to the local CA Group entity and/or approved Sub-processors of CA. Notwithstanding, in the event that Personal Data of Customer is transferred from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of the foregoing territories ("**Restricted Transfers**"), CA complies with the provisions of Section 5.6(a), with respect to such Restricted Transfers.

(a) **限定的転送に関する転送方法** CAは以下の転送方法を提供します。これらの方法は、転送がデータ保護法の対象となる範囲において、本DPAに基づく限定的転送に適用されます。
Transfer mechanisms for Restricted Transfers. CA makes available the transfer mechanisms listed below which shall apply, with respect to any Restricted Transfers under this DPA, to the extent such transfers are subject to such Data Protection Laws:

(1) **プライバシー・シールド自己認証** CA は、EU-US プライバシー・シールド・プログラムの適合性認証を受けています。CA は、EEA 個人データを維持する限りプライバシー・シールドの認証を維持するものとします。EU 当局や裁判所がプライバシー・シールドが適切な転送基盤ではないと判断した場合、両当事者は承認された EU 標準契約条項（処理者）を速やかに締結するものとし、締結された時点で同条項は本書に組み込まれます。
Privacy Shield self-certifications. CA has certified its compliance to the EU-US Privacy Shield Program. CA shall maintain its certification to the Privacy Shield for so long as it maintains any EEA Personal Data. In the event that EU authorities or courts determine that the Privacy Shield is not an appropriate basis for transfers, the parties shall promptly execute an approved EU Standard Contractual Clauses (Processors), which shall be incorporated herein upon execution.

(2) **EU 標準契約条項** CA および（別紙 2 に記載の）複処理者として行動する CA 関連会社は、データ管理者とデータ処理者という関係を結ぶため、またお客様の利益のために、事前に EU 標準契約条項を締結しています。さらに本書をもって、CA は本付属書の第 9 条に詳しく定められている EU 標準契約条項（処理者）を締結し、当該条項は添付書類 1 として本書に添付されています。
EU Standard Contractual Clauses. CA and CA Affiliates acting as Subprocessor (as listed in Annex 2) have previously entered into The EU Standard Contractual Clauses for a data controller-processor relationship and for the benefit of the Customer. Further, CA hereby enters into approved EU Standard Contractual Clauses (Processors), as further set forth in Section 9 of this Addendum, and a copy of which is attached hereto in Attachment 1.

サービスに複数の転送方法が適用される場合、お客様の個人データの転送には(i) プライバシー・シールド自己認証、(ii) EU 標準契約条項の優先順位で、1つのデータ転送方法が適用されます。
In the event that Services are covered by more than one transfer mechanism, the transfer of Customer's Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) Privacy Shield self-certifications; (ii) EU Standard Contractual Clauses.

6. セキュリティ
SECURITY

6.1. 到達水準、実施の管理費用、処理の性質、範囲、文脈および目的、ならびに自然人の権利および自由に関する重大性および様々な引き起こされるリスクの可能性を考慮し、お客様およびCAは、かかるリスクに見合ったセキュリティを確保するため、適切な技術的および組織的対策を実施するものとします。CAは、別紙2「処理のセキュリティ – GDPR第32条」に定められているとおりにGDPRに基づいてデータ処理者への要件を満たす、個人データのセキュリティ、機密性、整合性を保護するための適切な技術的および組織的対策を維持します。CAは、これらの保護への準拠を定期的に監視します。CAは、適用される原契約またはそれに基づく注文書に従って提供されるサービスの提供期間中に、かかるサービスの全体的なセキュリティを大幅に低下させることはありません。
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and CA shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. CA will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data that meet the requirements for a Data Processor under the GDPR, as set forth in Annex 2 "Security of Processing – GDPR Art. 32". CA regularly monitors compliance with these safeguards. CA will not materially decrease the overall security of the Services during the term of CA's provision of such Services pursuant to the applicable Agreement or order form thereunder.

6.2 合理的な間隔でのお客様の書面による要求を受けて、CAは、お客様の個人データの処理に関連してかかる要求を受けるとCAが通常提供する、その時点で最新の第三者による監査結果または認定を適宜提供するか、そのまとめを提供します。CAは、合理的な書面による要求を受けて、本付属書への準拠を示すために必要なかかる情報をお客様に提供するものとし、CAが本付属書に準拠する合理的手順を用いていることを確認するための、個人データの処理に関連するお客様または独立系監査人による書面による監査に関する情報要求を認めるものとします（ただし、お客様が本権利を年に1回を超えて行使しないことを条件とします）。適用されるデ

ータ保護法（該当する場合はGDPR第28（3）条を含みます）の要求を満たす監査権を原契約に記載がない場合、かかる情報や監査権は本6.2項に基づいて提供されます。CAが提供する情報および／または本条に従って実施される監査には、原契約に定められた秘密保持義務が適用されます。
Upon Customer's written request at reasonable intervals, CA shall provide a copy of CA's then most recent third-party audits or certifications, as applicable, or any summaries thereof, related to the Processing of Personal Data of Customer, that CA generally makes available to its customers at the time of such request. CA shall make available to Customer, upon reasonable written request, such information necessary to demonstrate compliance with this Addendum, and shall allow for written audit requests by Customer or an independent auditor in relation to the Processing of Personal Data to verify that CA employs reasonable procedures in compliance with this Addendum, provided that Customer shall not exercise this right more than once per year. Such information and audit rights are provided under this section 6.2 to the extent the Agreement does not provide such audit rights that meet the requirements of applicable Data Protection Laws (including, where applicable, Article 28(3)(h) of the GDPR). Any information provided by CA and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in the Agreement.

6.3 CAは、お客様のサービス使用に関連して、GDPR第35条または第36条に基づいて保護影響評価を実施するお客様の義務を履行するために、お客様への合理的な支援を必要に応じて行うものとします。CAは、お客様の合理的な要求を受けて、お客様が関連する情報にその他の方法でアクセスできない限りにおいて、CAがかかる情報を入手可能である限りにおいて、かかる支援を提供します。さらに、CAは、GDPRに基づいて要求される限りにおいて、本第6.3項に関するタスクの実施における監督当局との協力または事前協議について、お客様への合理的な支援を行うものとします。
CA shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment under Article 35 or 36 of the GDPR as related to Customer's use of the Services. CA will provide such assistance upon Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to CA. Additionally, CA will provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 6.3, to the extent required under the GDPR.

7. セキュリティ違反管理と通知
SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 CAは、CAまたは複処理者によって送信、保存、またはその他の方法で処理されたお客様の個人データの偶発的または違法な破壊、喪失、改変、無権限の開示、または違法なアクセス（以下「セキュリティ違反」といいます）を認識した後、不当な遅延なくお客様に通知するものとます。CAは、かかるセキュリティ違反の原因を特定するための合理的な努力をし、速やかに、また不当な遅延なく、(a) セキュリティ違反を調査し、お客様にセキュリティ違反に関する情報（該当する場合は、かかる情報が合理的に入手可能である限りにおいて、GDPR第33(3)条に従ってデータ処理者がデータ管理者に提供しなければならない情報を含みます）を提供し、(b) 救済がCAの合理的管理の範囲内である限りにおいて、セキュリティ違反から生じる影響を軽減するとともに損害を最小化するための合理的措置を講じます。本書における義務は、お客様またはお客様の認定ユーザに起因する違反には適用されません。通知は、下記第7.3項に従ってお客様に提供されます。
CA will promptly notify Customer, without undue delay, after CA becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unlawful access to any Customer's Personal Data that is transmitted, stored or otherwise Processed by CA or its Subprocessors of which CA becomes aware ("**Security Breach**"). CA will use reasonable efforts to identify the cause of such Security Breach and shall promptly and without undue delay: (a) investigate the Security Breach and provide Customer with information about the Security Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach to the extent the remediation is within CA's reasonable control. The obligations herein shall not apply to any breach that is caused by Customer or it Authorized Users. Notification will be delivered to Customer in accordance with Section 7.3 below.

7.2 CAが本条に基づいてセキュリティ違反を報告するまたはセキュリティ違反に対応することは、セキュリティ違反に関する過失または責任をCAが認めるものではなく、そのように解釈されないものとします。
CA's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by CA of any fault or liability with respect to the Security Breach.

7.3 セキュリティ違反があった場合の通知は、CAが選択した方法（メールを含みます）を用いて、お客様のビジネス、技術、または管理側の連絡先に提供されます。CAのサポート・システム上で常に正確な連絡先情報を維持しておく責任は、お客様が単独で担うものとします。
Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means CA selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on CA's support systems at all times.

8. お客様データの返却と削除
RETURN AND DELETION OF CUSTOMER DATA

8.1 CAは、CAの手順およびデータ保護法に従って、および／または原契約の諸条件に沿って、お客様へのお客様データ返却および／またはお客様データの削除を行います。
CA shall return Customer Data to Customer and/or delete Customer Data in accordance with CA's procedures and Data Protection Laws and/or consistent with the terms of the Agreement.

8.2 適用されるデータ保護法が個人データの保存を要求しない限り、CAは、お客様の要求を受けると、処理に関連するサービスの提供が終了した後にお客様に個人データのすべてを返却または削除し、別紙2「セキュリティ処理 – GDPR第32条」に定められる手順に従って、既存コピーを削除します。
At Customer's request, CA shall delete or return all Personal Data to Customer after the end of the provision of Services relating to Processing, and delete existing copies, in accordance with the procedures set forth in Annex 2 "Security of Processing – GDPR Art. 32", unless applicable Data Protection Law requires storage of the Personal Data.

9. EU個人データについての追加条件
ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1 添付書類1の標準契約条項および本第9条の追加条件は、サービスの提供過程におけるCAによる個人データの処理に適用されます。
The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 9 will apply to the Processing of Personal Data by CA in the course of providing the Services.

9.1.1 個人データに標準契約条項が適用されるのは、欧州経済域(EEA)またはスイスから、EEAまたはスイス以外に転送される個人データで、直接的転送先または再転送先の国または取得者が(i) 個人データに十分なレベルの保護(適用されるデータ保護法に従って説明されるとおりのもの)を提供していると欧州理事会が認めていない、および(ii) 関連する当局または裁判所に個人データに十分なレベルの保護を提供していると認められる適切な枠組み(処理者に対する拘束的企業準則などが含まれます)が適用されていない場合のみです。
The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) or Switzerland to outside the EEA or Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described pursuant to applicable Data Protection Law, and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors.

9.1.2 標準契約条項は、(i) データ輸出者として標準契約条項を締結した法人、および(ii) 欧州経済域(EEA)およびスイスで設立された(原契約に定義されているとおりの)お客様の関連会社で原契約に基づく注文書によってサービスを購入したものすべてに適用されます。標準契約条項および本第9条において、お客様とその関連会社は「データ輸出者」と見なされるものとします。
The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an order under the Agreement. For the purpose of the Standard Contractual Clauses and this Section 9, the Customer and its Affiliates shall be deemed to be "Data Exporters".

9.2 本DPAおよび原契約は、個人データの処理に関してデータ輸出者が与える完全かつ最終的な指示です。指示の追加または変更がある場合は、別途の合意が必要です。標準契約条項の条項5(a)において、以下はデータ輸出者による個人データ処理方法の指示と見なされます。(a) 原契約および適用される注文書に従って処理すること。(b) お客様からのその他の合理的な指示(サポート・チケットによるものなど)で、かかる指示が原契約の条件と合致するものに準拠して処理すること。
This DPA and the Agreement are Data Exporter's complete and final instructions to Data Importer for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Data Exporter to Process Personal Data: (a) in accordance with the Agreement and applicable orders thereunder; and (b) in compliance with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement.

9.3 標準契約条項の条項5(h)に従い、データ輸出者は、CAの関連会社が複処理者として委任されることがあり、(b) サービスの提供に関連して、CAとCAの関連会社それぞれが第三者の複処理者を業務に従事させることがあることを認め、これに明示的に同意します。データ輸入者は、それぞれのサービスについて、本DPAの第5.5項に従って複処理者の身元を記した複処理者の最新リストを用意し、CAが提供する複処理者リストにさらに詳細情報を追加します。
Pursuant to Clause 5(h) of the Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that CA's Affiliates may be retained as Subprocessors; and (b) CA and CA's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Data Importer shall make available to Customer a current list of Subprocessors for the respective Services with the identities of those Subprocessors in accordance with Section 5.5 of this DPA, further detailing CA's provision of the Subprocessor List.

9.4 両当事者は、標準契約条項の条項5(j) に従ってデータ輸入者がデータ輸出者に送らなければならない複処理者契約書のコピーでは、すべての商業的情報あるいは標準契約条項またはそれと同等のものに無関係な条項は事前にデータ輸入者が削除できること、また、かかるコピーは、データ輸出者からの合理的要求があった場合のみデータ輸入者からが提供されることに同意します。
The parties agree that the copies of the Sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand; and that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

9.5 両当事者は、標準契約条項の条項5(j) 、条項11、条項12(2)に説明されている監査は、次のとおりに実施されることに同意します。データ輸出者の要求を受けて、また原契約に定められた秘密保持義務の適用を受けて、データ輸入者は、かかる要求後の合理的

な期間内に、データ輸出者（またはデータ輸出者の独立系監査人または第三者監査人でCAにとっての競合他社ではないところ）に対して、本DPAに定められた義務にCAグループが準拠していることに関する情報を提供するものとし、かかる情報は、原契約に記載されるとおりに実施される第三者による認証および監査、および／またはCAが通常お客様に提供する範囲のセキュリティ・プラクティス・ドキュメントの形態をとるものとします。お客様は、原契約の「通知」条項に従い、データ輸入者に連絡して個人データの保護に関連する手順のオンサイト監査を要求することができます。お客様は、かかるオンサイト監査に費やされた時間について、その時点で最新のCAグループのプロフェッショナル・サービス料（データ輸出者の求めに応じて提供されます）でデータ輸入者への弁済を行うものとします。かかるオンサイト監査の開始前に、データ輸出者およびデータ輸入者は、データ輸出者の責任である弁済料に加えて、範囲、時期、監査期間について相互に合意するものとします。すべての弁済料は、データ輸入者が費やしたリソースを考慮したうえで合理的であるものとします。データ輸出者は、監査中に発見された非準拠に関する情報を速やかにデータ輸入者に通知するものとします。

The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement, Data Importer shall, within a reasonable period following such request, make available to Data Exporter (or Data Exporter's independent, third-party auditor that is not a competitor of CA) information regarding CA Group's compliance with the obligations set out in this DPA in the form of the third-party certifications and audits it carries out as described in the Agreement and/or the Security Practices Document to the extent CA makes them generally available to its customers. Customer may contact Data Importer in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Data Importer for any time expended for any such on-site audit at the CA Group's then-current professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.

9.6 両当事者は、条項12(1)に記載されている個人データの削除に関する認証は、データ輸出者の要求を受けた場合のみ、データ輸入者からデータ輸出者に提供されることに同意します。

The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.

9.7 本DPAと添付書類1の標準契約条項との間に矛盾または不一致が生じた場合は、標準契約条項が優先されます。本文書がいずれかの当事者によって電子署名された場合、かかる署名は記名押印または自署と同等の法的効力を持ちます。

In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail. If this document has been electronically signed by either party such signature will have the same legal affect as a seal or hand-written signature.

10. 本DPAの当事者
PARTIES TO THIS DPA

10.1 責任の制限 CA, Inc.は添付書類1の標準契約条項の当事者です。CA, Inc.が原契約の当事者でない場合でも、原契約の「責任の制限」条項がお客様とCA, Inc.の間で適用され、その意味において、「CA」という場合は、CA, Inc.と原契約の当事者であるCAのグループ会社の両方を含むものとします。各当事者およびその関連会社すべての責任には、本DPAおよび認定関連会社とCAの間のすべてのDPAに基づくかそれらに関連して発生するものすべてを累積して、契約違反、不法行為、その他のいかなる法的理論に基づくか否かを問わず、該当サービスの基礎となる原契約の「責任の制限」条項が適用され、かかる条項において当事者の責任という場合は、原契約および全DPAのすべてに基づく当該当事者およびその関連会社すべての累積責任を意味します。本DPAにおいてDPAという場合は、別紙、スケジュール、および／または付録を含む本DPAを意味します。

Limitation of Liability. CA, Inc. is a party to the Standard Contractual Clauses in Attachment 1. If CA, Inc. is not a party to the Agreement, the Section of the Agreement 'Limitation of Liability' shall apply as between Customer and CA, Inc., and in such respect any reference to 'CA' shall include both CA, Inc. and the CA entity who is a party to the Agreement. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and CA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement governing the applicable Services, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes, Schedules and/or Appendices.

10.2 認定関連会社と契約関係 本DPAを締結することにより、お客様は、自身を代表してDPAを締結し、また、お客様の認定関連会社がデータ管理者とされる個人データをCAが処理する場合、適用されるデータ保護法の求める範囲で、かかる認定関連会社の名義でその代理としてDPAを締結します。各認定関連会社は、本DPAおよび該当する限りにおいて原契約に基づく義務に拘束されることに同意します。認定関連会社は、原契約の当事者ではなく、当事者になることもなく、DPAの当事者でしかありません。認定関連会社によるサービスへのアクセスおよびサービスの使用はすべて、原契約の諸条件に準拠しなければならず、認定関連会社が原契約の条件に違反すれば、それはお客様による違反と見なされます。本書において別途の記載がない限り、本DPAにおいてのみ、「お客様」にはお客様と認定関連会社が含まれるものとします。

Authorized Affiliates & Contractual Relationship. By executing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates if and to the extent CA Processes Personal Data for which such Authorized Affiliates qualify as the Data Controller. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For

the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and such Authorized Affiliate is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein.

10.2.1 通知 原契約の契約当事者であるお客様は、本DPAに基づいて、CAとのあらゆる通知を取りまとめることに対して依然として責任を負い、認定関連会社を代表して本DPAに関連する通知を行い、受領する権利があります。

Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with CA under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.2.2 認定関連会社の権利 認定関連会社は、CAと締結するDPAの当事者となる場合、適用されるデータ保護法に要求される限りにおいて、本DPAに基づく権利を行使し救済を求める権利があります。その際には、以下の条件が適用されます。
Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with CA, it shall to the extent required under applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.2.2.1 適用されるデータ保護法により、認定関連会社が直接CAに対して権利行使または救済請求するよう求められない限り、両当事者は、(i) 原契約の契約当事者であるお客様が単独で認定関連会社の代理として、かかる権利行使または救済請求を行い、(ii) 原契約の契約当事者であるお客様は、本DPAに基づくかかる権利を各認定関連会社個別にではなく、すべての認定関連会社をまとめた形で行使するものとします。

Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against CA directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually, but in a combined manner for all of its Authorized Affiliates together.

11. 定義
DEFINITIONS

「**CA関連会社**」とは、CAによって支配されている会社、CAを支配する会社、またはCAと共同支配されている会社をいいます。
"CA Affiliates" means any entity which is controlled by, controls or is in common control with CA.

「**CA**」とは、適宜、本DPAの当事者であるCAグループ会社をいいます。
"CA" means the CA Group entity that is a party to this DPA, as applicable.

「**CAグループ**」とは、個人データの処理に関わるCAおよびCA関連会社をいいます。
"CA Group" means CA and its Affiliates engaged in the Processing of Personal Data.

「**認定関連会社**」とは、お客様の関連会社のなかで(a)欧州連合、欧州経済域および／またはそれらの加盟国、スイスおよび／またはイギリスのデータ保護法が適用されるもの、(b)お客様と CA との間で締結された契約に従ってサービスを利用することが許可されているが、CA との注文書に記名押印または署名しておらず、原契約の定める「お客様」ではないものをいいます。本 DPA においてのみ、本書に別途の記載がない限り、「お客様」にはお客様と認定関連会社が含まれるものとします。特に「**お客様認定関連会社**」とは、お客様が直接的または間接的に過半数所有するか過半数所有により支配する会社をいいます。
"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and CA, but has not signed its own Order Form with CA and is not a "Customer" as defined under the Agreement. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein. For the avoidance of doubt, "**Customer Affiliate**" means a legal entity that Customer directly or indirectly majority owns or controls through a majority interest.

「**データ管理者**」、「**データ処理者**」、「**データ主体**」、「**欧州理事会**」、「**加盟国**」、「**監督当局**」は、GDPR第1章第4条に定められる意味を持ち、それらに類する用語もその定義に従うものとします。
"Data Controller", "Data Processor", "Data Subject", "Commission", "Member State", and "Supervisory Authority" shall have the meaning given to them in Chapter 1, Article 4 of the GDPR and their cognate terms shall be construed accordingly.

「**データ保護法**」とは、原契約に基づいて個人データを処理する際に適用されるすべての法律および規制をいい、それには(以下に定義されている)GDPRをはじめとする欧州連合、欧州経済域、それらの加盟国の法律および規制が含まれます。
"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR (as defined below), applicable to the Processing of Personal Data under the Agreement.

「**GDPR**」とは、個人データの取扱いと関連する自然人の保護に関する、および、そのデータの自由な移転に関する、ならびに EU 指令 95/46/EC を廃止する EU 一般データ保護規則 2016/679（欧州議会および理事会の 2016 年 4 月 27 日の規則（EU）2016/679）をいいます。
"**GDPR**" means EU General Data Protection Regulation 2016/679 (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*) on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing EU Directive 95/46/EC.

「**個人データ**」とは、(i) 識別された人または識別可能な人に関する情報、(ii) 識別された法人または識別可能な法人に関する情報（かかる情報は、適用されるデータ保護法に従って、個人データまたは個人を識別できる情報と同様に保護されている場合）をいい、(i)と(ii)のそれぞれについて、かかるデータは原契約に関連して提供される（適用される原契約に定義されているとおりの）お客様データです。
"Personal Data" means any information relating to (i) an identified or identifiable person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), where for each (i) or (ii), such data is Customer Data (as defined in the applicable Agreement) provided in connection with the Agreement.

「**処理**」とは、自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正もしくは変更、検索、参照、使用、送信による開示、配布、または、それら以外に利用可能なものとすること、整列もしくは結合、制限、消去もしくは破壊のような、個人データに実施される業務遂行または一群の業務遂行をいいます。
"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

「**セキュリティ違反**」とは、本付属書の第7条に記載されている意味です。
"Security Breach" has the meaning given in Section 7 of this Addendum.

「**セキュリティ・プラクティス・ドキュメント**」とは、情報セキュリティ・プラクティス・ドキュメント（または、お客様がCAから購入するサービスに依存する該当部分）をいいます。この文書は随時更新され、https://www.ca.com/jp/legal/privacy/information-security-practices.htmlから提供されるか、（該当する場合）CAとお客様との間で締結された原契約に含まれます。
"Security Practices Document" means the Information Security Practices Document (or the applicable part dependent on what Services Customer purchases from CA), as updated from time to time, accessible at https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf, or as otherwise incorporated in the Agreement between CA and Customer.

「**セキュリティの別紙**」とは、個人データの保護についてCAが導入する技術的および組織的セキュリティ対策で、別紙2「処理のセキュリティ – GDPR第32条」に記載されているものをいいます。CAセキュリティ・プラクティス・ドキュメントの条件とセキュリティの別紙の条件が矛盾する場合、GDPRの要件によるセキュリティ対策と個人データ保護に関しては、セキュリティの別紙2に記載された条件が優先します。
"Security Annex" means the technical and organizational security measures implemented by CA for the protection of Personal Data, set forth in Annex 2 "Security of Processing – GDPR Art. 32". To the extent that the terms of the CA Security Practices Document and the terms of the Security Annex conflict, the terms of the Security Annex 2 shall govern with respect to the security measures and protection of Personal Data in accordance with the requirements of the GDPR.

「**サービス**」とは、保守サービスおよびサポート・サービス、および／またはコンサルティング・サービスあるいはプロフェッショナル・サービスを提供すること、および／またはSaaSおよび／または原契約に基づいて提供されるその他のサービス（その中でCAによってお客様の個人データが処理されるもの）を提供することをいいます。
"Services" means the provision of maintenance and support services and/or consultancy or professional services and/or the provision of software as a service and/or any other services provided under the Agreement where CA Processes Personal Data of Customer.

「**標準契約条項**」とは、十分なレベルのデータ保護を確保していない第三国で設立された処理者への個人データ転送に関する2010年2月5日の欧州理事会の決議に従ってお客様とCA, Inc.との間で締結され、添付書類1として添付される契約をいいます。
"Standard Contractual Clauses" means the agreement executed by and between Customer and CA, Inc. and attached as Attachment 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

「**複処理者**」とは、CAまたはCAグループ会社が業務に従事させるデータ処理者をいいます。
"Subprocessor" means any Data Processor engaged by CA or a member of the CA Group.

別紙および添付書類のリスト
List of Annexes & Attachments

- 別紙1: お客様の個人データ処理の詳細
  Annex 1: Details of Processing Customer Personal Data
- 別紙2: 処理のセキュリティ– GDPR第32条
  Annex 2: Security of Processing – Art. 32 GDPR

- 添付書類1: 標準契約条項
  Attachment 1: Standard Contractual Clauses

本DPAは、発効日をもってお客様とCAの間で締結された原契約の一部として拘束力を持ちます。本文書がいずれかの当事者によって電子署名された場合、かかる署名は記名押印または自署と同等の法的効力を持ちます。両当事者は本DPAを2通作成し、それぞれ正当な権限を有する代表者が以下のとおり記名押印または署名して締結するものとし、各1通を保有するものとします。
IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement(s) between Customer and CA, as of the Effective Date. If this document has been electronically signed by either party such signature will have the same legal affect as a seal or hand-written signature.

お客様	**CA**
住所:	住所:
会社名:	会社名:
役職:	役職:
氏名:	氏名:
押印日: _____年_____月_____日	押印日: _____年_____月_____日

別紙 1: お客様の個人データ処理の詳細
ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

別紙 1 には、GDPR 第 28 条(3)号(または、適宜その他のデータ保護法の同等の条項)が要求するお客様の個人データの処理に関する詳細が含まれています。
This Annex 1 includes certain details of the Processing of Customer's Personal Data as required by Article 28(3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

お客様の個人データ処理の主題と期間
Subject matter and duration of the Processing of Customer Personal Data

お客様の個人データの処理の主題および期間は、主契約および本付属書に記載されます。
The subject matter and duration of the Processing of the Customer Personal Data are set out in the Principal Agreement and this Addendum.

お客様の個人データ処理の性質と目的
The nature and purpose of the Processing of Customer Personal Data

性質
Nature:

- ☒ 収集 Collection
- ☒ 記録 Recording
- ☐ 公開 Disclosure
- ☒ 削除 Deletion
- ☐ 変更 Alteration
- ☐ 制限 Restriction
- ☒ 使用 Use

目的: お客様の個人データは、主契約に定められるサポートまたはSaaSを提供するために使用されます。
Purpose: Customer Personal Data is used to provide Support or SaaS as set out in the Principal Agreement.

処理対象となるお客様の個人データの種類
The types of Customer Personal Data to be Processed

自然人のお客様のデータ Customer Data of natural persons	☒
企業のお客様のデータ Customer Data of companies	☒
従業員のデータ Employee Data	☒
その他の個人データ Other Personal Data	☐

お客様の個人データが関係するデータ主体の区分
The categories of Data Subject to whom the Customer Personal Data relates

要配慮個人データまたは個人データの特別カテゴリ(GDPR 第9条)
Special Categories of Personal Data (Art. 9 GDPR)

健康状態／性生活 Health/sex Life	☐	政治的指向 Political Opinions	☐
労働組合への加入 Trade Union Membership	☐	人種／民族的出自 Racial/Ethnic Origin	☐
宗教または信条 Religious or Philosophical Beliefs	☐		

お客様およびお客様関連会社の権利義務
The obligations and rights of Customer and Customer Affiliates

お客様およびお客様関連会社の権利義務は、原契約および DPA(DPA の別紙、添付書類、またはスケジュールを含みます)に定められています。
The obligations and rights of Customer and Customer Affiliates are set out in the Agreement and the DPA, including any Annex, Attachment or Schedule to the DPA.

別紙 2 - 処理のセキュリティ – GDPR 第 32 条
ANNEX 2 - SECURITY OF PROCESSING – ART. 32 GDPR

前文
Preamble

到達水準、実施の管理費用、処理の性質、範囲、文脈および目的、ならびに自然人の権利および自由に関する重大性および様々な引き起こされる可能性のリスクを考慮し、管理者および処理者は、かかるリスクに見合った適切なセキュリティレベルを確保するため、下表記載を含む技術的および組織的対策を実施するものとます。
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

§ 1 適切なセキュリティレベルを確保するための技術的および組織的な対策（SaaS およびオンプレミス）
Technical and organisational measures implemented to ensure an appropriate level of security (SaaS and On Premise)

(1a) 個人データの**仮名化／匿名化**の対策 Measures on **pseudonymisation /anonymisation** of personal data:
本製品に保存されるデータは、一般に、仮名化または匿名化を必要とする性質のものではありません。仮名化または匿名化が必要となるときは、お客様が CA にエスカレーションするものとします。 Data stored in this product is not generally of a nature that requires pseudonymisation or anonymisation. If required, Company should escalate to CA. **オンプレミス** **On Premise:** 対象外 Not applicable

(1b) 個人データ**暗号化**の対策 Measures on the **encryption** of personal data:
暗号化 ENCRYPTION すべてのデータは暗号化して送られ、現在は TLS 1.0、1.1（廃止予定）および 1.2 がサポートされます。さらに、お客様のデータは、バックアップまたはオフサイト保存（該当すれば）のために CA の施設から移動される場合には暗号化されます。暗号鍵マテリアルの機密性、整合性、可用性を確保するため、鍵管理手順が採用されます。暗号化製品の使用は、該当する管轄内での暗号化の使用に関する現地の規制および法令に準拠します。 All data is encrypted in-transit. using TLS, with 1.0, 1.1 (will be deprecated), and 1.2 currently supported. In addition, Company Data is encrypted on any server or device that is removed from CA's premises for backup or off-site storage (where applicable). Key management procedures are employed that assure the confidentiality, integrity and availability of cryptographic key material. Use of encryption products comply with local restrictions and regulations on the use of encryption in a relevant jurisdiction. 暗号化ポリシー Encryption Policy 暗号化の使用について定めるデータ・セキュリティのポリシーは文書化されます。お客様のデータを送信する際の暗号の強度が定義されます。 Data security policy that dictates encryption use is documented. The encryption strength of Company Data in transmission is defined. 暗号鍵管理 Encryption Key Management 暗号鍵管理の手順は文書化され自動化されます。様々な製品やソリューションを導入することで、データ暗号鍵を暗号化し続けることができるようにしています（ソフトウェア・ベースのソリューション、ハードウェア・セキュリティ・モジュール（HSM）など）。 Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted (e.g., software based solution, Hardware Security Module (HSM)). 暗号化の使用 Encryption Uses 公共のインターネットでお客様のデータを送信する場合は、常に暗号化されたチャネルが用いられます。送信が自動化さている場合、暗号化の詳細は文書化されます。マニュアルで送信する場合は、許可された専任スタッフがデータの暗号化／解読を行います。いずれのネットワークで送信される場合でも、お客様のデータは必ず暗号化されます。VPN 送信は、暗号化されたチャネルで実施されます。

Company Data transmission over the public internet always utilizes encrypted channel. Encryption details are documented if transmission is automated. Approved and dedicated staff is responsible for encrypting/ decrypting the data, if manual. Company Data must also be encrypted while in transit over any network. VPN transmissions are performed over an encrypted channel.

オンプレミス
On Premise:
データ管理者は、サポート・ケースのデータを暗号化してデータ処理者に提供します。ケースの解決はセキュリティが確保された環境で実施されます。30 日が経過するとケースはクローズされ、サポート・ケースのデータは削除されます。
Data Controller provides support case data in an encrypted manner to Data Processor. Case resolution is done in a secured environment. 30 days after case is closed, support case data is deleted

(1c) 個人データの**継続的機密性**を確保するための対策
Measures of ensuring the **ongoing confidentiality** of personal data:

CA 情報アクセス制御ポリシーおよび CA 職務分掌ポリシーに基づき、お客様のデータが保存されているデータセンタへのアクセスは CA の運用チームに限定されます（CA は最低限の特権原則に従い、役割とビジネス・ユースケースに基づいたアクセスのみを付与します）。アクセス権は定期的または役割の変更した際および雇用の終了した際にレビューされます。お客様のデータが保存されている環境へのアクセスは、厳密に制御および監視されます。お客様は、自らのサブスクリプション・データへのアクセス管理に対する責任を担い、それらのアカウントのライフサイクルにも責任を負います。お客様のサブスクリプション管理者は、アプリケーション内のユーザ管理および関連するパスワード・ポリシーに責任を持ちます。
お客様は、このアカウントのライフサイクルに責任を持ちます。
All access to the data centers where Company data is stored, is restricted to CA's Operations Team according to CA Information Access Control Policies and CA Segregation of Duties Policy (CA follows the principle of least privilege and only grants access based on role and business use case). Access rights are reviewed regularly or upon change of role/termination of an employee. Access to the environment where Company data is stored is strictly controlled and monitored. Company is responsible for managing access to their subscription data and are responsible for the lifecycle of those accounts. Company Subscription Administrators are responsible for user administration and related password policies within the application.
The Company is responsible for the lifecycle of this account.

オンプレミス
On Premise:
作業はセキュリティが確保された環境で実施されます。データ転送にはセキュリティが確保されます。データは、サポート・ケースがクローズされた後に削除されます。
Work is done in secure environment; data transfer is secured. Deletion of data after closing of support case.

(1d) 個人データの**継続的機密性**を確保するための対策
Measures to ensure **ongoing integrity** of personal data:

データの整合性
DATA INTEGRITY

CA Technologies のポリシーおよび手順は、保存されているデータ、受領されたデータ、制御されているデータ、もしくはそれらとは別にアクセスされるデータが不正にアクセスされることなく、元の状態を保持できるように設計されます。データの整合性を検証するための調査手順が定められます。
CA Technologies Policies and Procedures are designed to ensure that any data stored, received, controlled or otherwise accessed is not compromised and remains intact. Inspection procedures are in place to validate data integrity.

データ送信制御
Data Transmission Controls

データの整合性を確保するためのデータの送信制御プロセスおよび手順は文書化されます。送信されたデータが受領したデータと同一であることを検証するために、チェックサムとカウントが採用されます。
Data transmission control processes and procedures to ensure data integrity are documented. Check sums and counts are employed to validate that the data transmitted is the same as data received.

データ・トランザクション制御
Data Transaction Control

フィナンシャル・メッセージにおけるトランザクションの重複を防止または特定するための制御は文書化されます。送信中にデータの整合性を確保するために使用されるデジタル・サティフィケート（デジタル署名やサーバ・トゥ・サーバなど）は、文書化されたプロセスおよび手順に準拠します。
Controls to prevent or identify duplicate transactions in financial messages are documented. Digital certificates (e.g., digital signature, server to server) utilized for ensuring data integrity during transmission follow a documented process and procedure.

オンプレミス
On Premise:
対象外。データは、サポート・ケースがクローズされた後に削除されます。第 2 条 a) ～e)ご参照ください。
Not applicable; Data is deleted after closing of support case, see section 2 a) to e)

(1e) **処理システムおよびサービスの現行の可用性**を確保するための対策
Measures to ensure **ongoing availability of processing systems and services:**

可用性の制御
AVAILABILITY CONTROL

- データ処理センタでの火災に対する保護および停電の際の対策。バックアップも含まれます。
- Protection against fire and measures in case of power outages in the data processing centers including backup

物理的制御
Physical Controls

CA Technologies は、悪意のある人物または許可されていない人物に対する保護のための効果的な制御を設定しています。施設全体を対象とした物理的制御は文書化されます。一般エリアに対し、サーバ／コンピュータ／通信ルームにはさらなるアクセス規制が設定されます。
CA Technologies has effective controls in place to protect against physical penetration by malicious or unauthorized people. Physical controls covering the entire facility are documented. Additional access restrictions are enforced for servers/ computer/ telecommunications room compared to the general area.

バックアップとオフサイト保存
Backup and Offsite Storage

CA Technologies は、スケジュール通りに遅延なくデータのバックアップを実施するためのバックアップ・ポリシーと関連手順を定めています。バックアップされた（オンサイトおよびオフサイトの）データを保護するため、効果的な制御が確立されます。また、CA Technologies は、お客様のデータがバックアップ先との間で安全に転送または移動されるようにします。さらに、CA Technologies は、データがバックアップ機器から安全に復旧されるよう、定期テストを実施します。
CA Technologies has a defined backup policy and associated procedures for performing backup of data in a scheduled and timely manner. Effective controls are established to safeguard backed up data (onsite and off-site). CA Technologies also ensures that Company Data is securely transferred or transported to and from backup locations. Furthermore, CA Technologies conducts periodic tests to ensure that data can be safely recovered from backup devices.

バックアップ・プロセス
Backup Process

バックアップおよびオフサイト保存の手順は文書化されます。手順により、アプリケーションとオペレーティング・システムを完全に復元することができます。バックアップ・メディアからの復元は、定期的にテストされます。オンサイト・ステージング・エリアには文書化および実証された環境制御（湿度、温度など）があります。
Backup and offsite storage procedures are documented. Procedures encompass ability to fully restore applications and operating systems. Periodic testing of successful restoration from back-up media is demonstrated. The on-site staging area has documented and demonstrated environmental controls (e.g., humidity, temperature).

バックアップ・メディアの破壊
Backup Media Destruction

バックアップ・メディアの適切な破壊方法を担当者に指示できるよう、その手順は定義されます。第三者によるメディアの破壊には、破壊を確認するための文書化された手順（破壊証明書など）が添付されます。
Procedures are defined for instructing personnel on the proper methods of backup media destruction. Back up media destruction by a third party is accompanied by documented procedures (e.g., certificate of destruction) for destruction confirmation.

オフサイト保存
Offsite Storage

オフサイト施設の物理的セキュリティ計画は文書化されます。エントリ・ポイントとストレージ・ルームでは、アクセス制御が実施されます。オフサイト施設へのアクセスは制御され、アクセスを得るための承認プロセスが設定されます。オフサイトへのデータの電子的送信は、暗号化されたチャネルを介して行われます。
Physical security plan for the offsite facility is documented. Access controls is enforced at entry points and in storage rooms. Access to the off-site facility is restricted and there is an approval process to obtain access. Electronic transmission of data to off-site location is performed over encrypted channel.

オンプレミス
On Premise:
「クローズド・ショップ」環境。対象外。データはデータ管理者のもとに保持されます。
Closed-Shop-Environment; not applicable. Data remains with Data Controller in existence.

(1f) **処理システムおよびサービスの継続的復旧力**を確保するための対策
Measures to ensure **ongoing resilience of processing systems and services:**

脆弱性の監視
VULNERABILITY MONITORING

CA Technologies は、新規および既存の脅威および脆弱性に関する情報、実際の機関またはその他の攻撃、および既存のセキュリティ制御の有効性に関する情報を継続的に収集および分析します。監視制御には、関連するポリシーと手順、ウイルスと悪質なコード、侵入検知、イベントと状態の監視が含まれます。関連するログ処理は、セキュリティ・イベントを強調表示し調査する効果的な制御を提供します。
CA Technologies continuously gather and analyze information regarding new and existing threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code, intrusion detection, and event and state monitoring. Related logging process provides an effective control to highlight and investigate security events.

脆弱性のポリシーと手順
Vulnerability Policy and Procedure

内部または外部ネットワークおよび／または特定のホストの侵入／脆弱性テストが実行されます。テストは、通常、評判の高い外部組織によって外部で実行されます。お客様の環境は、テスト範囲に含まれます。高リスクと評価されたすべての問題は、適切なスケジュールで修正されます。
Penetration/ vulnerability testing of the internal/ external networks and/ or specific hosts is performed. The tests are usually performed externally by a reputed external organization. Company environments are covered as part of the scope of the tests. All issues rated as high risk are remediated with appropriate timelines.

アンチウイルスと悪質なコード
Anti-virus and Malicious Code

サーバ、ワークステーション、およびインターネット・ゲートウェイ機器は、最新のアンチウイルス定義で定期的に更新されます。定義された手順は、すべてのアンチウイルス・アップデートに対応します。アンチウィルス・ツールは、週次スキャン、ウイルス検出、リアルタイムのファイル書き込みアクティビティ、シグネチャ・ファイルの更新を実行するように設定されます。ラップトップとリモート・ユーザもウイルス対策の対象です。無許可または非サポート(フリーウェアなど)のアプリケーションを検出および削除する手順は文書化されます。
Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g., freeware) applications are documented.

アラー・トイベントには、以下が含まれます。
Alert events include the following attributes:

固有の識別子
Unique identifier
日付
Date
時間 Time
優先順位レベルの識別子
Priority level identifier
送信元 IP アドレス
Source IP address
送信先 IP アドレス
Destination IP address
イベントの詳細
Event description
セキュリティ・チームに送信された通知
Notification sent to security team
イベント・ステータス
Event status

セキュリティ・イベントの監視
Security Event Monitoring

セキュリティ・イベントはログに記録され（ログファイル）、監視され（適切な人物）、対処されます（タイムリーなアクションが文書化され、実行されます）。ネットワーク・コンポーネント、ワークステーション、アプリケーション、監視ツールを使用してユーザのアクティビティを監視します。イベントに対応するための組織的な責任が定義されます。重要なシステム構成の変更を記録する構成チェックツールが利用されます（または他のログが利用されます）。管理者による変更はログ・パーミッションに制限されます。さまざまなログの保持スケジュールの定義および遵守がなされます。
Security events are logged (log files), monitored (appropriate individuals) and addressed (timely action documented and performed). Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined. Configuration checking tools are utilized (or other logs are utilized), that record critical system configuration changes. The log permission restricts alteration by administrators. Retention schedule for various logs are defined and adhered.

(1g) **技術的または物理的事故の場合に個人データの可用性および個人データへのアクセス**を復元するための対策
Measures to restore **availability and access to personal data in the event of a technical of physical incident:**

上記の可用性の制御をご参照ください。
See above AVAILABILITY CONTROL

事故対応
INCIDENT RESPONSE

CA Technologies は、情報セキュリティ事故があった場合に備え、計画および関連手順を文書化します。事故対応計画には担当者の責任が明記され、関連する通知当事者が特定されます。事故には、訓練を受けた担当者が対応します。事故対応計画の実行については、定期テストが実施されます。
CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant notification parties. Incident response personnel are trained. Execution of the incident response plan is tested periodically.

事故対応プロセス
Incident Response Process

情報セキュリティ事故管理ポリシーと手順は文書化されます。事故管理ポリシーおよび／または手順には、以下が含まれます。
Information security incident management policy and procedures are documented. The incident management policy and/or procedures include the following attributes:

- 組織構成が定義される。
  Organizational structure is defined
- 対応チームが決まる。
  Response team is identified
- 対応チームの可用性が文書化される。
  Response team availability is documented
- 事故の検出と開示のスケジュールが文書化される。
  Timelines for incident detection and disclosure are documented
- 事故プロセス・ライフサイクルは以下の通りであり、下記の個々のステップを含む。
  Incident process lifecycle is defined including the following discrete steps:
  - 特定
    Identification
  - 各事故への重大度の指定
    Assignment of severity to each incident
  - 通知
    Communication
  - 解決
    Resolution
  - トレーニング
    Training
  - テスト（チェック頻度）
    Testing (check frequency)
  - 報告
    Reporting
- 事故は分類し、優先順位を付ける必要がある。
  incidents must be classified and prioritized
- 事故対応手順には、リレーションシップ（デリバリ）マネージャまたは契約書に記載されている他の連絡先へのお客様による通知が含まれていなければならない。
incident response procedures must include Company notification to the relationship (delivery) manager or another contact listed in the contract

エスカレーション／通知

Escalation/Notification
事故対応プロセスは、CA Technologies がインシデントを認識したら速やかに（何時であるかを問わず）実施されます。
Incident response process is executed as soon as CA Technologies is aware of the incident (irrespective of time of day).

オンプレミス
On Premise:
一部にのみ適用。データは、サポート・ケースがクローズされた後に削除されます。
Only partially applicable; Data is deleted after support case is closed.

(1h) **技術的および組織的対策の効果を定期的にテスト、審査、評価**するための対策
Measures for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures:**

組織的制御
ORGANIZATIONAL CONTROL

運用
OPERATIONS

CA Technologies は、自らの IT 資産が正確かつ安全に運用されるよう IT 運用手順を文書化します。
CA Technologies has documented IT operational procedures to ensure correct and secure operation of its IT assets.

運用手順と責任
Operational Procedures and Responsibilities.

運用手順は運用マニュアルとして文書化され、正常に実行されます。操作マニュアルには、以下のコンポーネントが含まれます。
Operational procedures are documented in an operations manual and successfully executed.
The operations manual includes the following components:

スケジュール要件
Scheduling requirements
エラー対応（データの移動、印刷、コピーなど）
Handling errors (e.g., transport of data, printing, copies)
特別な出力の生成と取り扱い
Generating and handling special output
システムの保守とトラブルシューティング
Maintenance and troubleshooting of systems
SLA / KPI およびエスカレーションのレポート構造を管理するための文書化された手順
Documented procedures to manage the SLAs/ KPIs and the reporting structure for escalations

内部セキュリティ監査は、（外部）データ保護担当者を含め、処理者において定期的に実施されます。
Internal security audits are done on a regular basis at the processor including the (external) data protection officer

§ 2 § 1 に記載されていない更の技術的および組織的対策（一般的な措置で、必ずしも SaaS の提供に関連していないもの）
Additional technical and organisational measures not listed under § 1 (general measures, which are not necessarily related to providing SaaS)

(2a) **物理的アクセス制御（入場制限）**
Physical Access Control (Admittance Control):

「クローズド・ショップ」環境
Closed-Shop-Environment.

一般入場許可の要件および許可を有する人は定義され、セキュリティ関連エリアへの入場許可は絶対に必要である場合に限定されます（「最小限許可の原則」）。建物または敷地への入場手段は、一般的に特定の人にのみ提供され、第三者に引き渡すことはできません。ユーザにはこれが周知されます。
The requirements for and the group of persons with general admittance authorization are defined and the authorizations for admittance to security-relevant areas limited to absolute necessity (“principle of minimal authorization”). Means of admittance to buildings or premises are generally issued to only specific persons and may not be passed on to third parties. Users are made aware of this.

建物または部屋のセキュリティ要件は、そこに設置されている個人データが処理または保存されるデータ処理システムおよびその他の文書に基づいて決定されます。
The security requirements of a building or room are determined on the basis of the data processing systems located therein and any other documents on which personal data is processed or stored.

セキュリティ・エリアおよびそのエントリ・ポイントを許可のない人の侵入から保護するために、適切な技術的手段としてのカードリーダ・エントリ・システムが採択されます。
A card reader entry system as suitable technical measure has been taken to safeguard security areas and their entry points against entry by unauthorized person.

(2b) **アクセス制御**
Access Control:

「クローズド・ショップ」環境
Closed-Shop-Environment.

最先端のセキュリティ対策によって許可のある人物が特定されたうえで認証（ユーザ名、パスワードまたはチップカード／PIN 等を利用して）されない限り、データが処理されるデータ処理システムへのアクセスできません。許可されなければ、アクセスは拒否されます。
Access to data processing systems on which data is processed is possible only after the authorized person has been identified and successfully authenticated (e.g., with a user name and password or chip card/PIN), using state-of-the-art security measures. Access is denied for lack of authorization.

強力な認証は常に多要素（少なくとも 2 要素）に基づき、VPN 接続を確立する際には、所有物、知識、ユーザに固有のワンタイム要素などによる多要素認証が行われます。
Strong authentication is always based on multiple (at least two) factors, multi factor authentication is enforced, when establishing VPN connection, such as something owned, something known, or on the basis of a one-time factor that is specific to the user.

パスワードは、パスワードの長さや複雑さなどの適切な最低限の規則に準拠します。パスワードは定期的に変更する必要があります。初期パスワードは直ちに変更する必要があります。パスワードの長さ、パスワードの複雑さ、および妥当性の要件は、技術設定によって確実に実装されます。
Passwords comply with appropriate minimum rules, such as a minimum password length and complexity. Passwords have to be changed at regular intervals. Initial passwords must be changed immediately. The implementation of the requirements for password length, password complexity and validity are ensured by technical settings.

(2c) **アクセス認証の統制**
Access Authorisation Control:

権限コンセプト（ユーザおよび管理者の権限）により、社内タスク分配と機能分離に従ってユーザが関連タスクを完了するために必要な範囲でのみ、システム内のデータにアクセスすることが可能となります。データ保護規則にしたがって認証プロファイルおよびユーザの役割を作成、変更、削除するための規則および手順は、コンセプトに記載されます。認証コンセプトは、どのジョブ・保有者が管理タスク（システム、ユーザ、運用、移動）を実施できるのか、どのユーザ・グループがどのアクティビティをシステムで実施できるのか示す必要があります。責任は制限されます。職務分掌には詳細なプロセスが存在します。
An authorization concept (user and administration rights) ensures that access to the data in the system is enabled only to the extent required for the user to complete the relevant task according to the user's internal task distribution and separation of functions. Rules and procedures for creating, changing and deleting authorization profiles and user roles in compliance with data protection rules are described therein. The authorization concept must show which job holder may carry out administrative tasks (system, user, operation, transport) and which user groups may perform which activities in the system. Responsibilities are regulated. A detailed segregation of duty process exists.

(2d) **制御の公開**
Disclosure Control:

個人データが送信される各 IT / NT システムでは、送信が記録されます。ネットワーク内の転送は、内部システムによってセキュリティが確保されます。ネットワーク外の転送は、セキュリティ基準に従って保護され、暗号化されます。送信の詳細は記録されます。ログ保存期間は、従業員代表者（該当する場合）との間で合意された規則によって異なります。規則がない場合、保存期間は 6 ヶ月です。不適切な使用の特定と事故関連評価の実施については、従業員代表者（該当する場合）とデータ保護チームとの間で適切な手順が合意されます。
For each IT/NT system in which personal data is transmitted, the transmission is logged. Transfers in the network are secured by internal systems. Transfers outside of the network are secured according the security standards and encrypted. Transmission details are logged. The logging retention period depends on the rules agreed on with the employee representatives (if applicable). In the absence of rules, the retention period is 6 months. Suitable procedures

are agreed with the employee representatives (if applicable) and data protection team on identifying improper use and carrying out incident-related evaluations.

(2e) 入力の統制 **Input Control**:
役割に基づいてデータ処理システムへのデータ入力の権限と責任がある人物は、書面に記載されます。 It is documented which person is authorized to and responsible for entering data in the data processing system on the basis of his/her duties.)

(2g) 社内利用の統制 **Intended Use Control**:
契約上の業務を実施あるいはプロセスを実行するために必要最低限のデータのみが収集、保存、処理されます。Only the minimum amount of data that is needed to perform the contract work or carry out the process is collected, stored or processed. 別の契約上の目的のために使用されるデータおよび／またはデータ・メディアが別に処理（記録、修正、削除、移動など）および／または保存されるようにするための規則や対策が文書化され、適用されます。 Rules and measures to ensure that data and/or data media used for different contractual purposes are processed (recorded, modified, deleted and transported, etc.) and/or stored separately are documented and applied.

§ 3 データ・プライバシー担当者
Data Privacy Officers

氏名 Name:	連絡先情報 Contact Details:
Bonnie Yeomans	CA, Inc. 520 Madison Avenue New York, NY 10022 Assistant General Counsel and Chief Privacy Officer
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35 64297 Darmstadt Germany Senior Counsel & Field Legal Privacy Officer

§ 4 最新の複処理者リストは、https://support.ca.com/us/product-content/admin-content/subprocessor-list.htmlで維持されています。
A current list of Subprocessors is maintained at https://support.ca.com/us/product-content/admin-content/subprocessor-list.html

原契約に基づいてサポートおよび保守を提供する CA グループ会社 **CA Entities providing support and maintenance in accordance with the Principal Agreement**		
名称 Name	連絡先 Contact Details	所在国 Location
CA (Pacific) Pty Ltd	6 Eden Park Drive, North Ryde, New South Wales 2113, Australia	Australia
CA Software Österreich GmbH	EURO PLAZA, Am Europlatz 5, Gebäude C, 1120 Vienna	Austria
CA Belgium SA	Da Vincilaan 11, Building Figueras, B-1935 Zaventem - Belgium	Belgium
CA Programas de Computador Participacoas Servicos Ltda	Avenida Dr Chucri Zaidan, 1240 – 26º e 27º andares, Golden Tower, Vila São Francisco, CEP 04711-130 - São Paulo/SP, Brasil - CNPJ/MF 08.469.511/0001-69	Brazil
CA de Chile, S.A.S.	Avenida Providencia, 1760, piso 15, Edificio Palladio, oficina 1501, Providencia, Chile, inscrita bajo el Registro RUT 96.724.010-9	Chile

CA CZ, s.r.o	Praha 4 - Chodov, V Parku 2316/12, PSČ 148 00	Czech Republic
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Denmark
CA Limited (formerly CA Plc and fomerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
CA SAS	Tour Opus 12, 4 Place des Pyramides, La Défense 9, 92914 Paris La Défense Cedex, France,	France
CA Computer Associates European Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA (India) Technologies Private Limited	Ground Floor, Vibgyor Tower, Plot C-62, G-Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400 051	India
CA Software Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israel
CA Technologies R&D Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israel
CA S.r.l.	Via Francesco Sforza 3, 20080 Milano Tre, Basiglio (MI)	Italien
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Japan
CA Services, S.A. DE C.V.	s.u.	Mexico
CA Software de Mexico, S.A. de C.V	Miguel de Cervantes Saavedra 193 piso 5, Col. Granada, 11500, Ciudad de México, México; inscrita bajo el registro CSM 9505032G1	Mexico
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, the Netherlands,	Netherlands
CA software BV	s.o.	Netherlande
CA Software Holding BV	s.o.	Netherlande
CA IT Management Solutions Spain, S.L.U.	WTC Almeda Park, Edificio 2, planta 4, Plaça de la Pau s/n, 08940 Cornellá de Llobregat	Spain