DATA PROCESSING ADDENDUM
データ処理付属文書

This Data Processing Addendum ("**DPA**") is deemed to include Sections 1 through 9 below, including the attached Appendix 1, and the Data Security Guide, all of which are expressly deemed incorporated in the Agreement by this reference.

本データ処理付属文書は(以下「**DPA**」という。)は、添付の別紙 1 (処理の詳細) および別紙 A.5 - データ・セキュリティ・ガイドを含む、下記第 1 条ないし第 9 条から構成され、参照によって本契約に組み込まれ、本契約の一部となります。

In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall control. Any data processing agreements that may already exist between parties as well as any earlier version of the Data Security Guide to which the parties may have agreed are superseded and replaced by this DPA in their entirety. All capitalized terms not defined in this DPA will have the meaning given to them in other parts of the Agreement.

DPA の用語と本契約の用語との間に矛盾があった場合、本別紙の主題に関しては DPA が優先するものとします。データ・セキュリティ・ガイドを含め、両当事者間で合意済のデータ処理契約は、DPA により置き換えられ、DPA が優先されます。DPA に定義されていないすべての用語は、本契約に規定された意味を持つものとします。

In the event of any discrepancies between the English and the Japanese versions of this Data Processing Addendum, the English version shall prevail.

DPA の英語版および日本語版に齟齬がある場合、英語版が優先するものとします。

1. DEFINITIONS	**1. 定義**
1.1. "**Affiliates**" means any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where "**Control**" means the legal power to direct or cause the direction of the general management of the company, partnership, or other legal entity.	1.1. 「関係会社」とは、本契約の当事者が直接または間接に支配する、支配される、または共通の支配下にある個人もしくは法人を意味します。「支配」とは、企業、組合またはその他法人の経営全般を指揮または指揮を可能とする法的支配力を意味します。
1.2. "**Agreement**" means the Order Form or Use Authorization or other signed ordering document, as applicable, between ServiceNow and Customer and the signed master agreement (if any) for the purchase of the Subscription Service.	1.2. 「本契約」とは、サブスクリプション・サービスの購入のための ServiceNow と顧客間のオーダーフォーム、使用許諾またはその他の署名された注文文書(該当するもの)および基本契約(該当する場合)を意味します。
1.3. "**Data Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.	1.3. 「データ管理者」とは、単独または他者と共同で、個人データ処理の目的と手段を決定する自然人もしくは法人、公的機関、代理人またはその他の団体を意味します。DPA においてデータ管理者とは、顧客およびサブスクリプション・サービスに個人データを提出することを顧客に許諾されたまたはサブスクリプション・サービスにおいて個人データが処理される顧客の関係会社(該当する場合)を指します。
1.4. "**Data Processor**" means the natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the ServiceNow entity that is a party to the Agreement.	1.4. 「データ処理者」とは、データ管理者に代わり個人データを処理する自然人もしくは法人、公的機関、代理人またはその他の団体を意味します。DPA においてデータ処理者とは、本契約の当事者である ServiceNow の法人を指します。
1.5. "**Data Protection Laws**" means all applicable laws and regulations regarding the Processing of Personal Data and includes GDPR.	1.5. 「データ保護法」とは、GDPR を含む個人データの処理に関して適用される全ての法律および規則を意味します。

1.6. "**Data Subject**" means an identified or identifiable natural person.	1.6.「データ主体」とは、特定されたまたは特定可能な自然人を意味します。
1.7. "**GDPR**" means the European Union's General Data Protection Regulation (2016/679).	1.7.「GDPR」とは、欧州連合の一般データ保護規則（2016/679）を意味します。
1.8. "**Instructions**" means Data Controller's documented data Processing instructions issued to Data Processor in compliance with this DPA.	1.8.「指示」とは、DPA に従ってデータ処理者に提供されたデータ管理者が文書化したデータ処理の指示を意味します。
1.9. "**Personal Data**" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, or contractors to the Subscription Service as Customer Data.	1.9.「個人データ」とは、顧客またはその代理人、従業員もしくは請負人により、顧客データとしてサブスクリプション・サービスにアップロードされたデータ主体に関連するあらゆる情報を意味します。
1.10. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.	1.10.「処理」とは、自動化された手段によるか否かに関わらず、収集、記録、整理、構造化、保管、修正もしくは変更、復旧、参照、利用、伝送による開示、周知もしくはその他の方法による提供、整列もしくは結合、制限、消去または破棄といった個人データに関して行われるあらゆる操作または一連の操作を意味します。
1.11. "**Professional Services**" means any consulting or development services provided by or on behalf of ServiceNow pursuant to an agreed Statement of Work or Service Description described or referenced in a signed ordering document.	1.11.「プロフェッショナル・サービス」とは、署名された注文文書に記載または参照される作業明細書またはサービス詳細に従って、ServiceNow によりまたは ServiceNow の代理として提供されるコンサルティングまたは開発サービスを意味します。
1.12. "**Sub-Processor**" means any legal person or entity engaged in the Processing of Personal Data by Data Processor. For the avoidance of doubt, ServiceNow's colocation datacenter facilities are not Sub-Processors under this DPA.	1.12.「代理処理者」とは、データ処理者による個人データの処理に従事する法人または団体を意味します。なお、ServiceNow のコロケーションデータセンター施設は、DPA における代理処理者ではありません。
1.13. "**Subscription Service**" means the ServiceNow software-as-a-service offering ordered by Customer under an Order Form, Use Authorization or other signed ordering document between ServiceNow and Customer.	1.13.「サブスクリプション・サービス」とは、ServiceNow と顧客間のオーダーフォーム、使用許諾またはその他の署名された注文文書に基づき顧客によって注文され ServiceNow により提供される software-as-a-service を意味します。
1.14. "**Subscription Term**" means the term of authorized use of the Subscription Service as set forth in the Order Form, Use Authorization, or other ordering document signed by Customer and ServiceNow.	1.14.「サブスクリプション期間」とは、オーダーフォーム、使用許諾または ServiceNow と顧客間のその他の署名された注文文書において規定されるサブスクリプション・サービスの使用を許諾された期間を意味します。
2. SCOPE OF THE PROCESSING	**2. 処理の範囲**
2.1. COMMISSIONED PROCESSOR. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Subscription Service described in the Agreement and in accordance with the Instructions.	2.1. 委託処理者 データ管理者は、本契約に定めるサブスクリプション・サービスを提供するために必要な範囲で、指示に従ってデータ管理者に代わり個人データを処理するデータ処理者を指定します。
2.2. INSTRUCTIONS. The Agreement constitutes Data Controller's written Instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate Instructions provided that such Instructions are:	2.2. 指示 本契約は、個人データの処理に関するデータ処理者へのデータ管理者の書面による指示を構成するものです。データ管理者は、追加の、またはこれに代わる指示を提供できます。ただし、当該指示

(a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate Instructions to alter the scope of the Agreement. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.	は、(a)本契約の目的および範囲に一致し、(b)データ管理者によって文書により確認されるものとします。なお、データ管理者は、本契約の範囲を変更するために追加の、またはこれに代わる指示を使用してはなりません。データ管理者は、データ処理者に対する指示がデータ保護法を遵守していることを保証することに責任を負います。
2.3. NATURE, SCOPE AND PURPOSE OF THE PROCESSING. Data Processor shall only Process Personal Data in accordance with Data Controller's Instructions and to the extent necessary for providing the Subscription Service and the Professional Services, each as described in the Agreement. Data Controller acknowledges that all Personal Data it instructs Data Processor to Process for the purpose of providing the Professional Services must be limited to the Customer Data Processed within the Subscription Service.	2.3. 処理の性質、範囲および目的 データ処理者は、データ管理者の指示のみに従い、ならびに本契約に定めるサブスクリプション・サービスおよびプロフェッショナル・サービスを提供する範囲のみにおいて、個人データを処理します。データ管理者は、プロフェッショナル・サービスを提供する目的でデータ処理者に処理を指示する全ての個人データは、サブスクリプション・サービス内で処理される顧客データに限定されなければならないことを確認します。
2.4. CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and is further described in Appendix 1.	2.4. 個人データおよびデータ主体のカテゴリ データ管理者は、個人データを顧客データとしてサブスクリプション・サービスに提出することがあります。ただし、提出される個人データは、データ管理者がその裁量により決定および制限し、さらに別紙 1 に記載された範囲に限られます。
3. DATA CONTROLLER	**3. データ管理者**
3.1. COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all of its obligations under Data Protection Laws when Processing Personal Data.	3.1. データ保護法の遵守 データ管理者は、個人データの処理にあたり、データ保護法に基づく全ての義務を遵守するものとします。
3.2. SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Processor shall provide Data Controller reasonable assistance by providing Data Controller with information requested by Data Controller to conduct Data Controller's security risk assessment. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed. As further described in Section 7.1 (Product Capabilities) of the Data Security Guide, the Subscription Service includes, without limitation, column level encryption functionality and role-based access control, which Data Controller may use in its sole	3.2. セキュリティリスク評価 データ管理者は、データ保護法に準拠して、何らかの個人データをサブスクリプション・サービスに提出する前に、処理の性質、範囲、状況および目的、個人データに関連するリスクならびに適用されるデータ保護法を考慮した上で、サブスクリプション・サービス内のセキュリティ対策が十分なレベルのセキュリティを提供しているかどうかを判断するために適切なリスク評価を実施することに同意します。データ処理者は、データ管理者がセキュリティリスク評価を実施するためにデータ管理者が要求する情報をデータ管理者に提供することにより、データ管理者に対して合理的な支援をします。データ管理者は、処理される個人データに関連してサブスクリプション・サービス内のセキュリティ対策の十分性を判断することについてすべての責任を負います。データ・セキュリティ・ガイドの 7 条 1 項（製品の機能）に規定されるとおり、サブスクリプション・サービスは、コラムレベルの暗号化機能およびロールベースのアクセス制御を含みますが、これらに限られず、データ管理者は、個人データのリスクに適切なセキュリティのレベルを保証するため、自己の裁量により、それらを使用でき

discretion to ensure a level of security appropriate to the risk of the Personal Data. For clarity, Data Controller may influence the scope and the manner of Processing of its Personal Data by its own implementation, configuration (i.e., different types of encryption) and use of the Subscription Service, including any other products or services offered by ServiceNow and third-party integrations.	ます。明確化のため付言すると、データ管理者は、データ管理者独自の実装、設定（例えば、異なる種類の暗号化）およびサブスクリプション・サービス（ServiceNow および第三者によって提供されるその他の製品またはサービスを含む）の使用によって、個人データの処理範囲および方法に影響を及ぼすことができます。
3.3. CUSTOMER'S AFFILIATES. The obligations of Data Processor set forth herein will extend to Customer's Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:	3.3. 顧客関係会社 本契約に規定されるデータ処理者の義務は、顧客がサブスクリプション・サービスへのアクセスを提供し、サブスクリプション・サービス内で個人データが処理される顧客のデータ管理者関係会社にも拡大して適用されます。ただし、以下を条件とします。
3.3.1. COMPLIANCE. Customer shall at all times be liable for its Affiliates' compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer; and	3.3.1. 遵守 顧客は、常に顧客関係会社が DPA を遵守することに対して責任を負い、かつ、顧客のデータ管理者関係会社によるすべての作為および不作為は、顧客の作為および不作為とみなされます。
3.3.2. CLAIMS. Customer's Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "**Data Controller Affiliate Claim**"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement.	3.3.2. 請求 顧客のデータ管理者関係会社は、データ処理者に対して直接請求をすることはできません。データ管理者関係会社が、データ処理者に対する有効な法的措置、訴訟、請求または手続（以下「データ管理者関係会社による請求」という。）を主張する場合、(i)データ保護法が顧客のデータ管理者関係会社が当該データ管理者関係会社による請求の当事者となることを要求しない限り、顧客が、当該データ管理者関係会社に代わって、当該データ管理者関係会社による請求を直接データ処理者に対して行わなければならず、(ii)顧客のデータ管理者関係会社によるすべての請求は顧客によってなされた請求であるとみなされ、いかなる場合でも本契約に規定された総額での責任制限に従います。
3.3.3. DATA CONTROLLER AFFILIATE ORDERING. If a Data Controller Affiliate purchased a separate instance of the Subscription Service under the terms of the signed master agreement between ServiceNow and Customer, then such Data Controller Affiliate will be deemed a party to this DPA and shall be treated as Customer under the terms of this DPA.	3.3.3. データ管理者関係会社による注文 顧客のデータ管理者関係会社が ServiceNow および顧客間で署名された基本契約の条件に基づき、サブスクリプション・サービスのインスタンスを別途購入した場合、当該データ管理者関係会社は、DPA の当事者とみなされ、DPA に基づく顧客として扱われるものとします。
3.4. COMMUNICATION. Unless otherwise provided in this DPA, all requests, notices, cooperation, and communication, including Instructions issued or required under this DPA (collectively, "**Communication**"), must be in writing and between Customer and ServiceNow only and Customer shall inform the applicable Data Controller Affiliate of any Communication from ServiceNow pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to ServiceNow relating to Personal	3.4. コミュニケーション DPA に別段の定めがない限り、DPA に基づき提供または要求された指示を含む、すべての要求、通知、協力およびコミュニケーション（以下総称して「コミュニケーション」という。）は、書面により顧客および ServiceNow 間でのみなされなければならず、顧客は、該当するデータ管理者関係会社に、DPA に従って ServiceNow からのコミュニケーションを通知するものとします。顧客は、顧客関係会社がデータ管理者である個人データに関連して ServiceNow に提供したコミュニケー

Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.	ション（指示を含む。）が、関連する顧客関係会社の意図を反映するものであることを保証することに単独で責任を負います。
4. DATA PROCESSOR	**4. データ処理者**
4.1. DATA CONTROLLER'S INSTRUCTIONS. Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor's obligations in operating the Subscription Service or delivering Professional Services, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.	4.1. データ管理者の指示 データ処理者は、データ管理者から受けた指示に対するデータ処理者の遵守から生じた被害または損害に対して責任を負いません。データ処理者は、データ管理者の指示の遵守がデータ保護法に違反する可能性がある、またはサブスクリプション・サービスの運営もしくはプロフェッショナル・サービスの提供の際にデータ処理者が通常負う義務ではないと考える場合、速やかにその旨をデータ管理者に通知するものとします。データ管理者は、データ処理者が個人データを処理する権限の範囲に関するデータ管理者の表明に依拠していることを了承します。
4.2. DATA PROCESSOR PERSONNEL. Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data at least as protective as those set forth herein and in the Agreement.	4.2. データ処理者人員 データ処理者による個人データへのアクセスは、本契約に基づきデータ処理者の義務を履行するために当該アクセスを必要とし、DPA および本契約と少なくとも同程度の当該個人データの秘密を保持する義務によって拘束される人員に限定されます。
4.3. DATA SECURITY MEASURES. Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, Data Processor shall maintain appropriate technical and organizational safeguards to protect the security, confidentiality, and integrity of Customer Data, including any Personal Data contained therein, as described in Section 2 (Physical, Technical, and Administrative Security Measures) of the Data Security Guide. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction, and include:	4.3. データセキュリティの手段 上記 3 条 2 項（セキュリティリスク評価）に基づくデータ管理者のセキュリティリスク評価義務に影響を及ぼすことなく、データ処理者は、データ・セキュリティ・ガイドの 2 条（物理的、技術的および管理上のセキュリティ対策）に規定される個人データを含む顧客データのセキュリティ、機密性および完全性の保護のための適切な技術上および組織的なセキュリティ対策を維持するものとします。かかる措置は、損失、変更、権限のないアクセス、取得、使用、開示または偶然もしくは違法な破棄から顧客データを保護するよう策定され、以下を含みます。
4.3.1. SERVICE ACCESS CONTROL. The Subscription Service provides user and role based access controls. Data Controller is responsible for configuring such access controls within its instance.	4.3.1. サービスアクセス管理 サブスクリプション・サービスは、ユーザーおよびロールベースのアクセス管理を提供します。データ管理者は、インスタンス内で当該アクセス管理を設定する責任を負います。
4.3.2. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.	4.3.2. ロギングおよび監視 本番環境のログは、改ざんからの保護目的で収集および保管され、トレーニングを受けたセキュリティチームにより、異常がないか監視されます。
4.3.3. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure	4.3.3. データの分離 顧客データは、ServiceNow の社内インフラストラクチャから論理的および物理的に分離したマルチテナントのクラウドインフラストラクチャ

that is logically and physically separate from ServiceNow's corporate infrastructure.	上にある論理的なシングルテナントアーキテクチャ内に保存されるものとします。
4.3.4. SERVICE CONTINUITY. The production database servers are replicated in near real time to a mirrored data center in a different geographic region.	4.3.4. サービス継続性 本番データベースサーバーは、ほぼリアルタイムで、別の地域にあるミラー化されたデータセンターに複製されます。
4.3.5. TESTING. Data Processor regularly tests, assess and evaluates the effectiveness of its information security program and may periodically review and update such program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.	4.3.5. テスト データ処理者は、定期的に情報セキュリティ・プログラムの有効性をテスト、評価および判断し、ならびに刷新されるセキュリティ技術、業界標準慣行の変化および変化するセキュリティの脅威に対応するため、定期的に当該プログラムを検証しアップデートします。
4.4. DELETION OF PERSONAL DATA. Upon termination or expiration of the Agreement, Data Processor shall return and delete Customer Data, including Personal Data contained therein, as described in the Agreement.	4.4. 個人データの削除 本契約の終了時および満了時、データ処理者は、本契約が定めるとおり、個人データを含む顧客データの返却および削除を行うものとします。
4.5. DATA CENTERS. Data Processor will host Data Controller's instances of the Subscription Service in data centers located in the geographic regions specified on the Order Form, Use Authorization, or other signed ordering document between ServiceNow and Customer.	4.5. データセンター データ処理者は、オーダーフォーム、使用許諾または ServiceNow と顧客間のその他の署名された注文文書で特定される地域に所在するデータセンターにおいて、サブスクリプション・サービスのデータ管理者のインスタンスを運用します。
4.6. DATA PROTECTION IMPACT ASSESSMENTS (DPIA). Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under GDPR to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service.	4.6. データ保護影響評価（DPIA） データ処理者は、要請がある場合、サブスクリプション・サービス内で個人データを処理するために、GDPR に基づきデータ保護影響評価を実行するデータ管理者の義務を果たすために必要とされる合理的な情報をデータ管理者に提供します。
4.7. PRIOR CONSULTATION. Data Processor shall provide reasonable assistance (at Data Controller's expense) in connection with any prior consultation Data Controller is required to undertake with a supervisory authority under Data Protection Laws with respect to Processing of Personal Data in the Subscription Service.	4.7. 事前の協議 データ処理者は、サブスクリプション・サービスにおける個人データの処理に関し、データ保護法による監督権限に基づきデータ管理者が行う必要がある事前の協議に関連して、（データ管理者の費用で）合理的な支援を行うものとします。
4.8. DATA PROCESSOR ASSISTANCE. Data Processor will assist Data Controller in ensuring compliance with Data Controller's obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of Processing by providing Data Controller with reasonable information requested pursuant to the terms of this DPA, including information required to conduct Data Controller's security risk assessment and respond to Data Subject Requests (defined below). For clarity, Data Controller is solely responsible for carrying out its obligations under GDPR and this DPA. Data Processor shall not undertake any task that can be performed by Data Controller.	4.8. データ処理者の支援 データ処理者は、データ管理者のセキュリティリスク評価を実施し、データ主体要求（以下で定義される）に応答するために必要とされる情報を含め、DPA の条件に従い要請される合理的な情報をデータ管理者に提供することにより、処理の性質を考慮した上で、データ管理者が GDPR32 条から 36 条に従ってデータ管理者の義務の遵守を保証することを支援します。なお、データ管理者は、GDPR および DPA に基づく義務の実行につき単独で責任を負います。データ処理者は、データ管理者が実行すべき義務を引き受けることはありません。
4.9. DATA PROTECTION CONTACT. ServiceNow and its Sub-Processor Affiliates (defined below) will maintain a dedicated data protection team to	4.9. データ保護連絡先 ServiceNow および代理処理者関係会社（以下で定義される）は、DPA の有効期間

respond to data protection inquiries throughout the duration of this DPA and can be contacted at privacy@servicenow.com.	中、データ保護に関する問合せに対応するため、専任のデータ保護チームを維持し、privacy@servicenow.com 宛に連絡可能です。
5. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES	**5. データ主体と監督官庁からの要求**
5.1. REQUESTS FROM DATA SUBJECTS. During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "**Data Subject Requests**").	5.1. データ主体からの要求サブスクリプション期間中、データ処理者は、データ管理者に対し、データ保護法に基づき要求される、サブスクリプション・サービス内の個人データへのアクセス、修正、訂正、削除もしくは遮断を行い、当該個人データを移転もしくは転送するための方法を提供するものとします。(以下総称して「データ主体要求」という。)
5.2. RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.	5.2. 応答 データ管理者は、データ主体要求に応答することに単独で責任を負います。ただし、データ処理者は、データ管理者がサブスクリプション・サービスにおける機能を使用してデータ主体要求を履行することができない範囲で、データ管理者がデータ主体要求に応答することにつき、データ管理者に合理的に協力します。データ処理者は、データ処理者が直接データ主体要求を受けた場合、データ主体に顧客に連絡するよう指示します。
5.3. REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a data protection authority.	5.3. 監督官庁からの要求 個人データの処理に関し、政府機関、データ保護当局または執行機関による通知、監査、問合せまたは調査が行われる場合、適用される法令によって禁止されない限り、データ処理者は、速やかにデータ管理者に通知するものとします。データ管理者は、データ処理者によって処理された個人データを記録し、データ処理者が当該情報をデータ保護当局に提出するよう要求された場合、すべての必要な情報をデータ処理者に提供するよう協力するものとします。
5.4. COOPERATION WITH SUPERVISORY AUTHORITIES. In accordance with Data Protection Laws, Data Controller and Data Processor shall cooperate, on request, with a supervisory authority in the performance of such supervisory authority's task.	5.4. 監督官庁との協力 データ保護法に従って、データ管理者およびデータ処理者は、要請があった場合、当該監督官庁の業務を行う上で、監督官庁と協力するものとします。
6. BREACH NOTIFICATION	**6. 違反通知**
6.1. NOTIFICATION. Data Processor will report to Data Controller any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data ("**Breach**") that it becomes aware of without undue delay following determination by ServiceNow that a Breach has occurred.	6.1. 通知 データ処理者は、データ管理者に対し、認識した偶然もしくは違法な破棄、損失、変更、顧客データの権限のない開示またはアクセスを引き起こすセキュリティ違反(以下「違反」という。)につき、違反が発生したとServiceNowが判断した後不当な遅滞なく報告します。
6.2. REPORT. The initial report will be made to Data Controller's security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As	6.2. 報告 最初の報告は、ServiceNow のサポートポータルで指定されたデータ管理者のセキュリティまたはプライバシー担当者(担当者が指定されない場合、顧客によって指定された主担当者)に対して行われるものとします。情報が収集または利用できる

information is collected or otherwise becomes available, Data Processor shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Data Controller to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Data Processor contact from whom additional information may be obtained. Data Processor shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.	状態になった場合、データ処理者は、データ保護法に従って、影響を受けたデータ主体、政府機関およびデータ保護当局を含む、関連する当事者に対してデータ管理者が通知を行えるようにするため、違反の性質および結果に関するさらなる情報を不当な遅滞なく提供するものとします。報告には追加情報を提供できるデータ処理者の担当者の名前および連絡先を含みます。データ処理者は、違反の原因を解消し、将来の違反を防ぐために採用する措置を顧客に通知するものとします。
6.3. DATA CONTROLLER OBLIGATIONS. Data Controller will cooperate with Data Processor in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Data Controller is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.	6.3. データ管理者の義務 データ管理者は、サポートポータルにおいて正確な連絡先を維持し、違反を含むセキュリティインシデントを解決し、根本原因を特定し、再発を防ぐために合理的に要求されるあらゆる情報を提供することによってデータ処理者に協力します。データ管理者は、関連する監督または規制当局および被害を受けたデータ主体に通知するかどうかを決定し、通知を行うことにつき単独で責任を負います。
7. CUSTOMER MONITORING RIGHTS	**7. 顧客の監督権**
7.1. REMOTE SELF-ASSESSMENTS. Data Processor shall enable remote self-serve assessments of its Security Program (as defined in the Data Security Guide) by granting Data Controller, at all times and at no additional costs, access to the Data Processor self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing Data Processor's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 7.2 (Audit) below.	7.1. 遠隔地からの自己評価 データ処理者は、いつでも追加の費用なしで、データ処理者のセルフアクセス・ドキュメンテーションポータル（以下「**ServiceNow CORE**」という。）へのアクセスを付与することにより、データ管理者がセキュリティ・プログラム（データ・セキュリティ・ガイドで定義される）を遠隔地から自己評価することを可能とします。ServiceNow CORE において利用可能な情報には、下記 7 条 2 項（監査）に記載の認証および証明書のほか、データ処理者のポリシー、手続およびセキュリティ対策を証する文書を含みます。
7.2. AUDIT. No more than once per year and upon written request by Data Controller, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality directly with Data Processor), to access all reasonable and industry recognized documentation evidencing Data Processor's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent third-party of Data Processor's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor standards). Data Processor reserves the right to	7.2. 監査 年 1 回を限度として、データ管理者が文書で要求することにより、顧客は、直接または代理人を通して（ただし、かかる代理人がデータ処理者に対して書面による秘密保持義務を直接負うものとする）、データ処理者の顧客データのセキュリティを統制するポリシーおよび手続を証するすべての合理的かつ業界標準の文書にアクセスすることができます（以下「監査」という）。監査は、ISO27001、ISO27018、SSAE18/SOC1 および SOC 2 Type 2（これらと同等または後継の規格を含む）に記載された目標に対するサブスクリプション・サービスをサポートするデータ処理者の情報セキュリティマネジメントシステムを対象とする、独立した第三者によって実行される評価のサマリーレポートへのアクセスを含みます。データ処理者は、データ処理者もしくは

refuse to provide Customer (or its representatives) with any information which would pose a security risk to Data Processor or its customers, or which Data Processor is prohibited to provide or disclose under applicable law or contractual obligation.	顧客をセキュリティリスクにさらす、または適用される法令もしくは契約上の義務によりデータ処理者が提供または開示することを禁止されている情報を、顧客（または代理人）に提供することを拒否する権利を留保します。
7.3. OUTPUT. Upon completion of the Audit, Data Processor and Customer may schedule a mutually convenient time to discuss the output of the Audit. Data Processor may in its sole discretion, consistent with industry and Data Processor's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Data Processor's Security Program. The Audit and the results derived therefrom are Confidential Information of Data Processor.	7.3. アウトプット 監査が完了した場合、データ処理者および顧客は、監査のアウトプットについて議論するために互いに都合のよい時間を定めることができます。データ処理者は、自己の裁量で、業界およびデータ処理者の基準および慣行に従い、データ処理者のセキュリティ・プログラムを改善するために監査において言及された顧客提案の改善策を実行する商業的に合理的な努力をします。監査およびそこから得られる結果は、データ処理者の秘密情報です。
7.4. DATA CONTROLLER EXPENSES. Any expenses incurred by Data Controller in connection with the Audit shall be borne exclusively by Data Controller.	7.4. 顧客費用 監査に関してデータ管理者に発生する費用は、データ管理者がすべて負担します。
8. SUB-PROCESSORS	**8. 代理処理者**
8.1. USE OF SUB-PROCESSORS. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section 8 to support the provision of the Subscription Service and to deliver Professional Services as described in the Agreement.	8.1. 代理処理者の使用 データ管理者は、データ処理者に対し、本契約に定めるサブスクリプション・サービスの提供の支援およびプロフェッショナル・サービスの提供のため、本条に従って任命された代理処理者を関与させる権限を与えます。
8.1.1. SERVICENOW AFFILIATES. As of the Effective Date, Data Processor engages, as applicable, the following ServiceNow Affiliates as Sub-Processors: ServiceNow, Inc. (USA), ServiceNow Nederland B.V. (the Netherlands), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India), and ServiceNow UK Ltd. (United Kingdom) (collectively, "**Sub-Processor Affiliates**"). Data Processor will notify Data Controller of changes regarding such Sub-Processor Affiliates through Data Processor's customer support portal (or other mechanism used to notify its general customer base). Each Sub-Processor Affiliate shall comply with the obligations of the Agreement in the Processing of the Personal Data.	8.1.1. ServiceNow 関係会社 発効日時点において、データ処理者は、該当する場合、代理処理者として、以下の ServiceNow の関係会社を関与させます 。ServiceNow, Inc. (USA), ServiceNow Nederland B.V. (the Netherlands), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India) および ServiceNow UK Ltd (United Kingdom)（以下総称して「代理処理者関係会社」という。） データ処理者は、データ管理者に対し、データ処理者のサポートポータル（または通常顧客に通知する際に利用されるその他の手段）を通じて、代理処理者関係会社の変更を通知するものとします。各代理処理者関係会社は、個人データの処理にあたり本契約の義務に従うものとします。
8.1.2. NEW SUB-PROCESSORS. Prior to Data Processor or a Data Processor Affiliate engaging a Sub-Processor, Data Processor shall: **(a)** notify Data Controller by email to Customer's designated contact(s) or by notification within the customer support portal (or other mechanism used to notify its customer base); and **(b)** ensure that such Sub-Processor has entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring that the Sub-Processor abide by terms no less	8.1.2. 新しい代理処理者 データ処理者またはデータ処理者関係会社が代理処理者を従事させる前に、データ処理者は、(a)顧客が指定した連絡先にメールを送信することにより、またはサポートポータル（もしくは顧客に通知する際に利用されるその他の手段）内で通知することによりデータ管理者に通知し、(b)当該代理処理者がデータ処理者（または該当するデータ処理者関係会社）との間で、DPA に定める義務と同等以上の条件を課した契約を書面により確実に締結するものとします。データ管理

protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.	者による書面での要求があった場合、データ処理者はデータ管理者に対しデータ処理条件のサマリーを提供するものとします。データ管理者は、DPAに従って関連する処理作業を履行する代理処理者の能力に関する合理的な追加情報を文書で要求することができます。
8.2. RIGHT TO OBJECT. Data Controller may object to Data Processor's proposed use of a new Sub-Processor by notifying Data Processor within 10 days after receipt of Data Processor's notice if Data Controller reasonably determines that such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA ("**Controller Objection Notice**"). Data Processor shall notify Data Controller within 30 days from receipt of the Controller Objection Notice if Data Processor intends to provide the applicable Professional Service or Subscription Service with the use of the Sub-Processor at issue, and Customer may terminate the applicable Order Form(s), Use Authorization(s) or other signed ordering document between ServiceNow and Customer with respect to the Professional Service or Subscription Service that require use of the Sub-Processor at issue upon written notice to ServiceNow within 45 days of the date of Controller Objection Notice and, as Customer's sole and exclusive remedy, ServiceNow will refund to Customer any unused prepaid fees.	8.2. 異議を述べる権利 データ管理者は、データ管理者が代理処理者が DPA に従って個人データを処理することができないと合理的に判断した場合、データ処理者の通知を受領してから 10 日以内にデータ処理者に通知することにより、データ処理者からなされた新しい代理処理者使用の提案に対し異議をとなえることができます（以下「管理者異議通知」という。）。データ処理者は、問題となっている代理処理者を使用して該当するプロフェッショナル・サービスまたはサブスクリプション・サービスを提供する意図がある場合、管理者異議通知の受領から 30 日以内にデータ管理者に通知しなければならず、顧客は、管理者異議通知の日から 45 日以内に、ServiceNow に書面により通知することにより、問題となっている代理処理者の使用を要するプロフェッショナル・サービスまたはサブスクリプション・サービスに適用されるオーダーフォーム、使用許諾または ServiceNow と顧客との間のその他の署名された注文文書を終了することができ、顧客の唯一かつ排他的な救済として、ServiceNow は顧客に対し、未使用分の前払いされた料金を払い戻します。
8.3. LIABILITY. Use of a Sub-Processor will not relieve, waive, or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.	8.3. 責任 代理処理者を使用することによってデータ処理者が本契約に基づいて有する義務が軽減、放棄もしくは減少されることはなく、データ処理者は、代理処理者の行為および不作為に対して、行為および不作為がデータ処理者によるものである場合と同じ限度で責任を有します。
9. INTERNATIONAL DATA TRANSFERS	**9. 国際的なデータ移転**
9.1. STANDARD CONTRACTUAL CLAUSES AND ADEQUACY. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by **(a)** the Standard Contractual Clauses for Data Processors established in third countries; or **(b)** another lawful mechanism for the transfer of Personal Data as approved by the European Commission.	9.1. 標準契約条項および十分性 データ保護法に基づき要求される場合、データ処理者またはデータ処理者関係会社は、代理処理者に対し、以下の事項を遵守することを要求します。(a)第三国で確立されたデータ処理者の標準契約条項、または(b)欧州委員会により承認された個人データの移転のための別の合法的なメカニズム。
9.2. PRIVACY SHIELD. ServiceNow, Inc. shall comply with the EU-U.S. and Swiss-U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the European Economic Area and Switzerland to the United States.	9.2. プライバシーシールド ServiceNow Inc.は、欧州経済地域およびスイスからアメリカに転送された個人データの処理に関して、アメリカ合衆国商務省によって定められる EU-米国 およびスイス-米国 Privacy Shield のフレームワークを遵守します。

/// /// /// Remainder of page intentionally left blank	/// /// /// 意図的に空欄とされている頁の残り部分

APPENDIX 1 - DETAILS OF PROCESSING
別紙 1 - 処理の詳細

Nature and Purpose of Processing Data Processor will Process Personal Data as required to provide the Subscription Service and Professional Services and in accordance with the Agreement.	**処理の性質および目的** データ処理者は、サブスクリプション・サービスおよびプロフェッショナル・サービスを提供するために必要な範囲および本契約に従って、個人データを処理します。
Duration of Processing Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of this DPA.	**処理の期間** データ処理者は、本契約の有効期間および DPA の 4 条（データ処理者）に従って、個人データを処理します。
Data Subjects Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects: • clients and other business contacts; • employees and contractors; • subcontractors and agents; and • consultants and partners.	**データ主体** データ管理者は、個人データをサブスクリプション・サービスに提供することができ、提供する範囲はデータ管理者のみによって決定されます。なお、データ主体の以下のカテゴリーに関連する個人データが含まれます。 • クライアントおよびその他のビジネス関係者 • 従業員および請負人 • サブコントラクターおよび代理人 • コンサルタントおよびパートナー
Categories of Personal Data Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories: • communication data (e.g., telephone, email); • business and personal contact details; and • other Personal Data submitted to the Subscription Service.	**個人データのカテゴリー** データ管理者は、個人データをサブスクリプション・サービスに提出することができ、提供する範囲はデータ管理者のみによって決定されます。なお、データ主体の以下のカテゴリーが含まれます。 • 通信データ（例：電話、電子メール） • 事業および個人の連絡先の詳細 • サブスクリプション・サービスに提供されるその他の個人データ
Special Categories of Personal Data Data Controller may submit Special Categories of Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller in compliance with Data Protection Law, and may include the following categories, if any: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data or biometric data; • health information; and • sex life or sexual orientation.	**個人データの特別なカテゴリー** データ管理者は、個人データの特別なカテゴリーをサブスクリプション・サービスに提出することができ、提供する範囲は、データ保護法に従ってデータ管理者のみによって決定されます。該当する場合、データ主体の以下のカテゴリーが含まれます。 • 人種または民族的起源 • 政治的意見 • 宗教上または哲学上の信念 • 労働組合の組合員であること • 遺伝子データまたは生体データ • 健康情報 • 性生活または性的指向
Processing Operations The personal data transferred will be subject to the following basic processing activities: • All activities necessary for the performance of the Agreement.	**処理方法** 移転される個人データは、以下の基本的な処理行為の対象となります。 • 本契約の履行のために必要なすべての行為

EXHIBIT A.5 - DATA SECURITY GUIDE
別紙 A.5 – データ・セキュリティ・ガイド

This Data Security Guide forms a part of the Agreement and describes the measures ServiceNow takes to protect Customer Data.

本データ・セキュリティ・ガイドは、本契約の一部を構成し、顧客データを保護するために実施する措置について記載するものです。

In the event of any conflict between the terms of this Data Security Guide and the terms of the Agreement with respect to the subject matter herein, this Data Security Guide shall control. All capitalized terms not defined in this Data Security Guide will have the meaning given to them in other parts of the Agreement.

本データ・セキュリティ・ガイドの用語と本契約の用語との間に矛盾があった場合、本別紙の主題に関しては 、本データ・セキュリティ・ガイドが優先するものとします。本データ・セキュリティ・ガイドに定義されていないすべての用語は、本契約に規定された意味を持つものとします。

1. SECURITY PROGRAM	**1. セキュリティ・プログラム**
While providing the Subscription Service, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow regularly tests, assesses, and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.	サブスクリプション・サービスの提供中、ServiceNowは、顧客データの処理、保管、送信およびセキュリティを管理する方針、手続ならびに管理についての書面による情報セキュリティ・プログラム（以下「セキュリティ・プログラム」という。）を維持するものとします。セキュリティ・プログラムには、偶然もしくは違法な破棄、損失、変更、不正な開示またはアクセスから顧客データを保護するよう設計された業界標準の慣行を含みます。ServiceNowは、セキュリティ・プログラムの有効性をテスト、評価および判断し、ならびに新しくそして進化しているセキュリティ技術、業界標準の慣行の変化、およびセキュリティの脅威に対処するために定期的にセキュリティ・プログラムをレビューし、アップデートすることがあります。ただし、当該アップデートは、本契約に定める義務、保護またはサービスの総合的なレベルを著しく低下させないものとします。
2. PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY MEASURES	**2. 物理的、技術的および管理上のセキュリティ対策**
2.1. PHYSICAL SECURITY MEASURES.	2.1. 物理的なセキュリティ対策
2.1.1. Data Center Facilities. (a) Physical access restrictions and monitoring that may include a combination of any of the following: multizone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), onsite guards, biometric controls, CCTV, and secure cages; and (b) fire detection and fire suppression systems both localized and throughout the data center floor.	2.1.1. データセンターの設備 (a)以下を組み合わせた物理的なアクセス制限およびモニタリング：マルチゾーンセキュリティ、マン・トラップ、適切な境界線上の妨害物（柵、盛り土、守衛門など）、現場の守衛、生体認証、CCTV、およびセキュアケージ、(b)データセンターフロアにおける局地的および全体的な火災感知および消火システム。
2.1.2. SYSTEMS, MACHINES AND DEVICES. (a) Physical protection mechanisms; and (b) entry controls to limit physical access.	2.1.2. システム、機械および装置 (a)物理的な保護の仕組み、 および(b)物理的なアクセスを制限するための入退出管理。
2.1.3. MEDIA. (a)Industry standard destruction of sensitive materials before disposition of media; (b) secure safe for storing damaged hard disks prior to physical destruction; and (c) physical	2.1.3. 媒体 (a)業界基準に基づく、媒体処分前のセンシティブな資料の破壊、(b)物理的に破壊される前に破損したハードディスクを保存するための安全の確

destruction of all decommissioned hard disks storing Customer Data.	保、および、(c)顧客データを保管している、廃棄されるハードディスク全ての物理的破壊。
2.2. TECHNICAL SECURITY MEASURES.	2.2. 技術的なセキュリティ対策
2.2.1. ACCESS ADMINISTRATION. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.	2.2.1. アクセス管理 ServiceNow の従業員および請負人によるサブスクリプション・サービスに対するアクセスは、認証および承認メカニズムにより保護されます。本番環境および準本番環境インスタンスへのアクセスにはユーザー認証が要求されます。アクセス特権は、業務上の必要性に応じ与えられ、雇用または委託関係の終了時に無効化します。本番環境は、適切なユーザーアカウントおよびパスワードコントロール（例：VPN 接続、期限付複雑パスワード、二要素認証接続の必須使用）を用いて管理目的でアクセス可能です。
2.2.2. SERVICE ACCESS CONTROL. The Subscription Service provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.	2.2.2. サービスアクセス管理 サブスクリプション・サービスは、ユーザーおよびロールベースのアクセス管理を提供します。顧客は、インスタンスにおける当該アクセス管理の設定に責任を負います。
2.2.3. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.	2.2.3. ロギングおよび監視 本番環境のログは、改ざんからの保護目的で中央で収集および保管され、トレーニングを受けたセキュリティチームにより、異常がないか監視されます。
2.2.4. FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.	2.2.4. ファイアーウォールシステム 業界標準ファイアーウォールをネットワーク上に導入し、 ServiceNow 環境に接続するすべての侵入経路を調査し、ServiceNow システムを保護するよう管理します。
2.2.5. VULNERABILITY MANAGEMENT. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then-current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.	2.2.5. 脆弱性管理 ServiceNow は、重要な情報資産を特定し、当該資産への脅威を評価し、潜在的脆弱性を判断し、改善策を提供するために、定期的に独自のセキュリティリスク評価を実施します。ソフトウェア脆弱性がベンダーから提供されるパッチにより明らかとなった場合、ServiceNow はベンダーから当該パッチを入手し、適切な時間枠の中で、ServiceNow のその時点で最新の脆弱性管理およびセキュリティ・パッチ標準運用管理規則に従い、テスト環境にて、本番環境へのインストールが安全だということを確認の上、すべての本番環境に適用します。
2.2.6. ANTIVIRUS. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.	2.2.6. ウィルス防止 ServiceNow は定期的にウィルス防止、マルウェア防止およびスパイウェア防止ソフトウェアのアップデートを行い、当該ソフトウェアの効果について集約的に記録するものとします。
2.2.7. CHANGE CONTROL. ServiceNow ensures that changes to platform, applications, and production infrastructure are evaluated to	2.2.7. 変更管理 ServiceNow は、プラットフォーム、アプリケーションおよび本番インフラストラクチャへの変更は、リスクを最小限にすることを評価し、

minimize risk and are implemented following ServiceNow's standard operating procedure.	ServiceNow の標準運用手順に従い実行されることを保証します。
2.2.8. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.	2.2.8. データの分離 顧客データは、ServiceNow の社内インフラストラクチャから論理的および物理的に分離されたマルチテナントクラウドインフラストラクチャ上の論理的シングルテナントアーキテクチャ内に維持されるものとします。
2.3. ADMINISTRATIVE SECURITY MEASURES.	2.3. 管理上のセキュリティ対策
2.3.1. DATA CENTER INSPECTIONS. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.	2.3.1. データセンター検査 ServiceNow は、セキュリティ・プログラムを遵守するために必要なセキュリティコントロールが維持され続けることを確実にするため、各データセンターにおいて定期的な検査を行うものとします。
2.3.2. PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law.	2.3.2. 人的セキュリティ ServiceNow は、顧客データにアクセスする従業員およびすべての請負人に対して、その時点で最新の ServiceNow の標準運用規則および法律に基づき、経歴のスクリーニングを行います。
2.3.3. SECURITY AWARENESS AND TRAINING. ServiceNow maintains a security awareness program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.	2.3.3. セキュリティ啓発およびトレーニング ServiceNow は、セキュリティ・プログラムに基づき、ServiceNow 人員に対する適切なトレーニングを含むセキュリティ啓発プログラムを保持します。トレーニングは、雇用時および ServiceNow での雇用中定期的に行われるものとします。
2.3.4. VENDOR RISK MANAGEMENT. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security controls and business disciplines.	2.3.4. ベンダーリスク管理 ServiceNow は、顧客データへのアクセス、保存、処理または移転を行うすべてのベンダーに対して、適切なセキュリティコントロールおよびビジネス規律のため、 ベンダーリスク管理プログラムを通し、継続してベンダーの査定を 行います。
3. SERVICE CONTINUITY	**3. サービス継続性**
3.1. DATA MANAGEMENT; DATA BACKUP. ServiceNow will host Customer's access to and use of purchased instances of the Subscription Service in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations) acting in an active/active capacity for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.	3.1. データ管理；データバックアップ ServiceNow は、サブスクリプション期間中、SSAE 18 Type 2 認証を獲得しまたは アクティブ/アクティブモードで動作する ISO 27001（または同等のもしくは承継される認証）を有するデータセンターにおいて、顧客による購入インスタンスへのアクセスおよび使用を保持します。各データセンターは、電源、冷却機能、ネットワークシステムに対して、完全な冗長化(N+1)およびフォルトトレラントインフラを含みます。配置されるサーバーは、最大限の稼働時間およびサービス可用性を保証した冗長電源およびストレージ構成を有するエンタープライズスケールサーバーです。本番データベースサーバーは、ほぼリアルタイムで、別の地域にあるミラー化されたデータセンターに複製を置くものとします。各顧客インスタンスは、インターネットに複数接続を有するネットワーク構成によりサポートされます。ServiceNow は、ServiceNow 標準運用規則に従い、すべての顧客データをバックアップします。

3.2. PERSONNEL. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a ServiceNow telephone support representative, geographically distributed to ensure business continuity for support operations.	3.2. 人員 緊急事態で、担当地域の顧客サポート電話システムが利用できない場合、サポート業務の継続性を確保するために、すべての電話は、地理的に継続できる ServiceNow 電話サポートシステムの代表に転送され回答します。
4. CERTIFICATIONS AND AUDITS	**4. 証明および監査**
4.1. CERTIFICATIONS AND ATTESTATIONS. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "**Standards**") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such Standards by an independent third-party auditor.	4.1. 証明および認証 ServiceNow は、サブスクリプション・サービスをサポートする情報セキュリティマネジメントシステムのための ISO27001、ISO27018、SSAE18 / SOC1、および SOC2 Type2（またはこれらと同等の規格）（以下総称して「規格」という。）に記載された目的に合致する十分な管理を確立し、維持するものとします。少なくとも暦年に一度、ServiceNow は、独立した第三者の監査による当該規格に対する評価を得るものとします。
4.2. CUSTOMER MONITORING RIGHTS.	4.2. 顧客の監督権
4.2.1. REMOTE SELF ASSESSMENTS. ServiceNow shall enable remote self-serve assessments of its Security Program by granting Customer, at all times and at no additional costs, access to the ServiceNow self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing ServiceNow's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 4.2.2 (Audit) below.	4.2.1. 遠隔地からの自己評価 ServiceNow は、いつでも、追加の費用なしで、ServiceNow セルフアクセス・ドキュメンテーションポータル（以下「**ServiceNow CORE**」という。）へのアクセスを付与することにより、顧客がセキュリティ・プログラムを遠隔地から自己評価することを可能とします。ServiceNow CORE において利用可能な情報には、下記 4 条 2 項 2 号（監査）に記載の認証、ServiceNow のポリシー、手続およびセキュリティ対策を証する文書を含みます。
4.2.2. AUDIT. No more than once per year and upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality directly with ServiceNow), to access all reasonable and industry recognized documentation evidencing ServiceNow's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent thirdparty of ServiceNow's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor attestations). ServiceNow reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to ServiceNow or its customers, or which ServiceNow is prohibited to provide or disclose under Law or contractual obligation.	4.2.2. 監査 年 1 回を限度として、顧客が文書で要求することにより、顧客は、直接または代理人を通して（ただし、かかる代理人が ServiceNow に対して書面により秘密保持義務を直接負うものとする）、ServiceNow の顧客データのセキュリティを統制するポリシーおよび手続を証するすべての合理的かつ業界標準の文書にアクセスすることができます（以下「監査」という。）。監査は、ISO27001、ISO 27018、SSAE18/SOC1 および SOC 2 Type 2（これらと同等または後継の規格を含む。）に記載された目標に対するサブスクリプション・サービスをサポートする ServiceNow の情報セキュリティマネジメントシステムを対象とする、独立した第三者によって実行される評価のサマリーレポートへのアクセスを含みます。ServiceNow は、ServiceNow もしくは顧客をセキュリティリスクにさらす情報または法令もしくは契約上の義務により ServiceNow が提供または開示することを禁止されている情報を、顧客（または代理人）に提供することを拒否する権利を留保します。
4.2.3. OUTPUT. Upon completion of the Audit, ServiceNow and Customer may schedule a mutually convenient time to discuss the output of	4.2.3 アウトプット 監査が完了した場合、ServiceNow および顧客は、監査のアウトプットについて議論する

the Audit. ServiceNow may in its sole discretion, consistent with industry and ServiceNow's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve ServiceNow's Security Program. The Audit and the results derived therefrom are Confidential Information of ServiceNow.	ために互いに都合のよい時間を定めることができます。ServiceNow は、その単独の裁量で、業界および ServiceNow の基準および慣行に従い、ServiceNow のセキュリティプログラムを改善するために監査において言及された顧客提案の改善策を実行する商業的に合理的な努力をします。監査およびそこから得られる結果は、ServiceNow の秘密情報です。
4.2.4. CUSTOMER EXPENSES. Any expenses incurred by Customer in connection with the Audit shall be borne exclusively by Customer.	4.2.4. 顧客費用 監査に関して顧客に発生する費用は、すべて顧客が負担します。
5. MONITORING AND INCIDENT MANAGEMENT	**5. モニタリングおよびインシデント管理**
5.1 MONITORING, MANAGEMENT AND NOTIFICATION.	5.1. モニタリング、管理および通知
5.1.1. INCIDENT MONITORING AND MANAGEMENT. ServiceNow will monitor, analyze, and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. ServiceNow's security group will escalate and engage response teams as may be necessary to address an incident.	5.1.1. インシデントのモニタリングおよび管理 ServiceNow は、ServiceNow の標準操作手順に従って適時にセキュリティインシデントをモニター、分析および対応するものとします。 ServiceNow のセキュリティグループは、インシデントに対処するために必要な対応チームに上程し、従事させるものとします。
5.1.2. BREACH NOTIFICATION. ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "**Breach**") without undue delay following determination by ServiceNow that a Breach has occurred.	5.1.2. 違反通知 ServiceNow は、顧客に対し、偶然もしくは違法な破棄、損失、変更、顧客データの権限のない開示またはアクセス（以下「違反」という。）につき、違反が起きたと ServiceNow が判断した後不当な遅滞なく報告します。
5.1.3. REPORT. The initial report will be made to Customer security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies, and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.	5.1.3. 報告 最初の報告は、ServiceNow のサポートポータルで指定された顧客のセキュリティまたはプライバシー担当者（担当者が指定されない場合、顧客によって指定された主担当者）に対して行われます。情報が収集された、または利用できる状態になった場合、 ServiceNow は、データ保護法に従って、影響を受けたデータ主体、政府機関およびデータ保護当局を含む関係者に対して顧客が通知を行えるようにするため、違反の性質および結果に関するさらなる情報を不当な遅滞なく提供するものとします。報告には追加情報を提供できる ServiceNow の担当者の名前および連絡先を含みます。ServiceNow は、違反の原因を解消し、かつ将来の違反を防ぐために採用する措置を顧客に通知するものとします。
5.1.4. CUSTOMER OBLIGATIONS. Customer will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Customer is solely responsible for determining	5.1.4. 顧客の義務 顧客は、サポートポータルにおいて正確な連絡先を維持し、違反を含む、セキュリティインシデントを解決し、根本原因を特定し、かつ再発を防ぐために合理的に要求される情報を提供することによって ServiceNow に協力します。顧客は、関連する監督または規制官庁および被害を受けた

whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.	データ主体に通知するかどうかを決定し、そのような通知を行う単独の責任を負います。
5.2. USE OF AGGREGATE DATA. ServiceNow may collect, use, and disclose quantitative data derived from Customer's use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes in support of the provision of the Subscription Service. Any such data will be in aggregate form only and will not contain Customer Data.	5.2. 統計データの使用 ServiceNow は、サブスクリプション・サービスの提供に資するために、サブスクリプション・サービスの顧客による利用から生じた定量データを業界分析、ベンチマーク、分析、マーケティング、およびその他のビジネス目的で収集、使用、開示することができます。一切の当該データは、統計された形態のみであり、顧客データを含みません。
5.3. COOKIES. When providing the Subscription Service, ServiceNow uses cookies to: **(a)** track session state; **(b)** route a browser request to a specific node when multiple nodes are assigned; and **(c)** recognize a user upon returning to the Subscription Service. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Subscription Service for ServiceNow's use of cookies.	5.3. クッキー サブスクリプション・サービスを提供する場合、ServiceNow は、以下においてクッキーを使用します。(a)セッション状態の追跡、(b) 複数のノードが割り当てられた場合のブラウザ要求を特定のノードに送ること、および(c)サブスクリプション・サービスに戻る際のユーザー認識。顧客は、ServiceNow のクッキーの使用のために、サブスクリプション・サービスの利用権限のあるユーザーに対する通知を行うことおよび当該ユーザーから必要な同意を得ることに責任を有するものとします。
6. PENETRATION TESTS	**6. 侵入テスト**
6.1. BY A THIRD-PARTY. ServiceNow contracts with third-party vendors to perform a penetration test on the ServiceNow application per family release to identify risks and remediation that help increase security.	6.1. 第三者によるテスト ServiceNow は、セキュリティの増強に資するリスクと改善策を特定するために、ファミリー・リリースごとに ServiceNow アプリケーション上での侵入テストの実施について第三者ベンダーと契約します。
6.2. BY CUSTOMER. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of a subproduction instance of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request to schedule an application penetration test using ServiceNow's customer support portal per ServiceNow's then-current penetration testing policy and procedure, including entering into ServiceNow's penetration test agreement. ServiceNow and Customer must agree on a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, but in no event longer than 14 days and must not interfere with ServiceNow's day-today operations. Promptly on completion of the penetration test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry-standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the	6.2. 顧客によるテスト 年 1 回を限度として、顧客は、自己の費用で、サブスクリプション・サービスの準本番インスタンスにおけるアプリケーション侵入テストの実施を要求できます。顧客は、ServiceNow の侵入テストに関する契約の締結を含む、当該時点における侵入テストポリシーおよび手順に従い、ServiceNow のサポートポータルを使用して、アプリケーション侵入テストのスケジュール要求を提出することで、事前に ServiceNow にテストに関して通知するものとします。ServiceNow と顧客はテストに関して互いに許容できる時間について合意しなければならず、顧客は、ServiceNow の明示的な書面による同意なく侵入テストを実行しないものとします。テストは、合理的な期間でなければならないが、いかなる場合も 14 日を超えてはならず、ServiceNow の日常業務を妨げてはならないものとします。侵入テストの完了後直ちに、顧客は、検出されたあらゆる脆弱性を含むテスト結果を ServiceNow に提供するものとします。当該通知に基づき、ServiceNow は、業界の標準的慣行に沿って、サブスクリプションサービスのセキュリティを向上させるために必要なあらゆる変更を即座に行うため、あらゆる商業的に合理的な努力を行うものとします。顧客は、テスト結果を本契約の守秘義務の対象となる

test results as Confidential Information of ServiceNow subject to the confidentiality requirements in the Agreement.	ServiceNow の秘密情報として取り扱うものとします。
7. SHARING THE SECURITY RESPONSIBILITY	**7. セキュリティ責任の共有**
7.1. PRODUCT CAPABILITIES. The Subscription Service has the capabilities to: **(a)** authenticate users before access; **(b)** encrypt passwords; **(c)** allow users to manage passwords; and **(d)** prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information, Personal Data, and any Personal Data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data and ServiceNow will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service.	7.1. 製品の機能 サブスククリプション・サービスには以下の機能があります。(a)アクセス前のユーザー認証、(b)パスワードの暗号化、(c)ユーザーによるパスワード管理、および(d)非アクティブアカウントのユーザーによるアクセスの阻止。顧客は、サブスクリプション・サービスへのアクセスのレベルを制御する認証情報とユーザタイプを各ユーザーに割り当てることによって、各ユーザーのサブスクリプション・サービスのアクセスと使用を管理します。顧客は、クレジットカード番号、社会保障番号およびその他政府発行の識別番号、財務および健康情報、個人データ、ならびにデータ保護法に基づくセンシティブまたは「特別なカテゴリーの個人データ」とみなされる個人データを含む、センシティブデータを含むすべての顧客データの保護を目的とした、サブスクリプション・サービスの中で利用可能な暗号化およびアクセス管理機能を実行する責任があります。当該データの暗号化を行わないと顧客が判断した場合、その判断に対して、顧客が単独で責任を負うものとし、顧客が暗号化を行っていれば発生しなかったはずの損害につき、ServiceNow は一切の責任を負いません。顧客は、各ユーザーのログインおよびパスワードの秘密の保護ならびに各ユーザーのサブスクリプション・サービスへのアクセスの管理について責任を有するものとします。
7.2. CUSTOMER COOPERATION. Customer shall promptly apply any Upgrade or Update that ServiceNow determines is necessary to maintain the security, performance, or availability of the Subscription Service.	7.2. 顧客の協力 顧客は、ServiceNow がサブスクリプション・サービスのセキュリティ、性能または可用性を維持するのに必要であると判断するあらゆるアップグレードまたはアップデートを直ちに適用するものとします。
7.3. LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, ServiceNow's obligations extend only to those systems, networks, network devices, facilities, and components over which ServiceNow exercises control. This Data Security Guide does not apply to: (a) information shared with ServiceNow that is not Customer Data; (b) data in Customer's VPN or a third-party network; (c) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide; or (d) Integrated Products. For the purposes of this Data Security Guide, "**Integrated Products**" shall mean ServiceNow-provided integrations to third-party products or any other third-party products that are used by Customer in connection with the Subscription Service. Customer agrees that its use of such Integrated Products will be: **(i)** in compliance with all Laws, including but not limited to, Data	7.3. 制限 本データ・セキュリティ・ガイドまたは本契約に異なる定めがあろうとも、ServiceNow の義務は、ServiceNow が管理権限を行使するシステム、ネットワーク、ネットワークデバイス、ファシリティおよびコンポーネントのみにしか及ばないものとします。本データ・セキュリティ・ガイドは、以下には適用されません。(a) 顧客データではない ServiceNow と共有された情報、(b) 顧客の VPN または第三者のネットワークにあるデータ、(c) 本契約または本データ・セキュリティ・ガイドに違反して顧客またはそのユーザーが処理したあらゆるデータ、または(d) 統合された製品。本データ・セキュリティ・ガイドにおいて「統合された製品」とは、ServiceNow によって提供される第三者の製品またはサブスクリプション・サービスに関連して顧客によって使用されるその他の第三者の製品との統合を意味します。顧客は、統合された製品の使用は、(i)データ保護法を含むすべての

Protection Laws; and **(ii)** in accordance with its contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Subscription Service must be collected, used, disclosed and, if applicable, internationally transferred in accordance with Customer's privacy policy, which will adhere to Data Protection Laws.	法律、および(ii)統合された製品の提供者との契約上の合意に従うことに同意します。統合された製品からサブスクリプション・サービスへ追加されたすべての個人データは、データ保護法に準拠した顧客のプライバシーポリシーに従って、収集、使用、開示、(該当する場合)国外に移転されるものとします。
/// /// /// Remainder of page intentionally left blank	/// /// /// 意図的に空欄とされている頁の残り部分