Microsoft のサプライヤー向けデータ保護要件

本データ保護要件の対象者

Microsoft のサプライヤー向けデータ保護要件（「本**DPR**」）は、Microsoft との契約条件（発注の条件、基本契約など）に基づき、Microsoft のサプライヤーの業務（サービスの提供、ソフトウェアライセンス、クラウドサービスなど）（「**業務**」）に関連して、Microsoft の個人データまたは Microsoft の機密データの処理や AI システムの使用を行う Microsoft のサプライヤー各位に適用されます。

- 本DPR と、同サプライヤーと Microsoft 間の契約上の合意で規定された要件が相反する場合は、DPRが優先されます。ただし、同サプライヤーが、該当するデータ保護要件に優先する同契約の条項を特定できる場合には、その限りではありません（この場合は、同契約書の要件が優先されます）。
- 本契約に含まれる要件と法的/制定法上の要件との間に矛盾がある場合は、法的/制定法上の要件が優先されます。
- Microsoft のサプライヤーがコントローラーとして機能する場合、当該サプライヤーに適用される DPR の要件が緩和される場合があります。
- Microsoft のサプライヤーが Microsoft の個人データを処理せず、Microsoft の機密データのみを処理する場合、本 DPR に関連して当該 Microsoft のサプライヤーに適用される要件が緩和される場合があります。
- DPR のセクション K（AI システム）は、Microsoft に AI システムを含むサービスを提供するサプライヤーにのみ適用されます。

データの国際転送

他の義務を制限することなく、サプライヤーは、Microsoft が事前の書面による承認を提供しない限り、Microsoft の個人データの国外に転送してはなりません。また、いかなる場合においても、サプライヤーは、標準契約条項を含むデータ保護要件、または Microsoft の裁量により、必要に応じて、採用/同意される、適切なデータ保護機関または欧州委員会によって承認された、
その他の適切な国境を超えた転送に関する仕組みを遵守するものとします。（i）欧州委員会によって採択された、または欧州データ保護監督官によって採択され、欧州委員会によって承認された、（ii）英国の一般連邦データ保護法に基づき英国によって採択された、（iii）スイス連邦データ保護法に基づいてスイスによって採択された後継の標準契約条項、または（iv）スイス、英国、および欧州連合/欧州経済領域を構成する管轄区域以外の管轄区域の政府により公式に採択された個人データの国際転送を規定する条項は、採用日の時点で組み込まれ、サプライヤーを拘束するものとします。また、サプライヤーは、すべてのサブプロセッサー（標準契約条項で定義されている）も上記の条項を遵守していることを保証するのとします。

主な定義

本 DPR で使用される用語を以下に定義します。本 DPR 全体で使用される「含む」、「など」、「例：」、「例えば」などの前後に続く例の羅列は、「のみ」または「単独で」などの言葉で修飾されていない限り、「制限なく」または「～を含むがこれらに限定されない」という文言が含まれていると解釈されるものとします。詳細な定義については、本要件の最後に記載されている用語集を参照してください。

「**AI システム**」とは、人間が定義した一連の特定の目標に対して、システムが相互作用する環境に影響を与える予測*、推奨事項、または決定を行えるように、最適化されたモデルを適用するエンジニアリングシステムを意味します。このようなシステムは、様々なレベルの自動化により作動する場合があります。*予測は、各種データ分析や生産（テキストの翻訳、合成イメージの作成、過去の停電診断など）を指す場合があります。

「**コントローラー**」とは、個人データの処理の目的と手段を決定する事業体を意味します。「コントローラー」には、事業体、コントローラー（GDPR で定義されている用語）、および文脈に応じてデータ保護法で定義される同等の用語が含まれます。

「**Cookie**」とは、データ主体またはデバイスを認識するために使用される情報を含むウェブサイトおよび/またはアプリケーションによってデバイスに保存される小さなテキストファイルを意味します。

「**データインシデント**」とは、(1) サプライヤーまたはその下請け業者によって転送、保存、さもなくば処理される Microsoft の個人データまたは Microsoft の機密データの、不慮の、または違法な破壊、紛失、変更、不正な開示、もしくはアクセスに結果的につながるセキュリティ違反、または（2）サプライヤーによる Microsoft の個人データや Microsoft の機密データまたは機密インシデントの処理に関するセキュリティの脆弱さを意味します。
Microsoft の個人データまたは Microsoft の機密データまたは機密インシデントは、法案第64号（2021年、第25章）に基づいて定義されています。

「**データ主体**」とは、特に名前、識別番号、位置データ、オンライン識別子などの識別子を参照することにより、または、自然人の身体的、生理学的、遺伝的、精神的、経済的、文化的、または社会的アイデンティティに固有の1つ以上の要素を組み合わせることにより、直接的もしくは間接的に、識別できる自然人を意味します。

「**データ主体の権利**」とは、法律で義務付けられている場合における、Microsoft が保有するデータ主体の個人データの処理にアクセスできる、それを取り消せる、編集できる、外部に転送できる、制限できる、またはそれに異議を唱えることができるデータ主体の権利を意味します。

「**使用目的**」とは、顧客、サプライヤー、エンドユーザーのいずれかがシステムを使用することを期待した場合の主要な目的です。これは一度のみの使用の場合も、複数使用システムの場合は複数回の場合もあり得ます。

「**法律**」とは、管轄権を有する政府当局（連邦、州、地方、または国際）のすべての適用法、規則、制定法、行政命令、決定、命令、規制、判決、法典、法令、決議、および要件を意味します。「**違法**」とは、法律違反を意味します。

「**Microsoft の機密データ**」とは、機密性または完全性の欠如によって侵害された場合に、Microsoft に評判の低下または経済的損失をもたらす可能性のある情報を意味します。これには、Microsoft のハードウェアおよびソフトウェア製品、社内の基幹業務管理アプリケーション、リリース前のマーケティング資料、製品ライセンスキー、および Microsoft の製品とサービスに関連する技術文書が含まれます。

「**Microsoft の個人データ**」とは、Microsoft によって、または Microsoft に代わって処理される個人データを意味します。

「**個人データ**」とは、データ主体に関連する情報、および法律に基づいて「個人データ」または「個人情報」を構成するその他の情報を意味します。

「**プロセス**」とは、Microsoft の個人データまたは Microsoft の機密データに対して実施される処理または一連の処理を意味します。これは、収集、記録、整理、構造化、保管、改作または修正、回復、参照、使用、転送による開示、配布またはその他の方法の開示、調整または組み合わせ、制限、消去、または破棄などの自動化された手段によるものであるかどうかを問いません。「処理中」と「処理済み」は対応する意味を持つものとします。

「**プロセッサー**」とは、別の事業体に代わって個人データを処理する事業体を意味し、文脈に応じて、サービス

プロバイダー、プロセッサー（GDPR で定義される用語）、およびデータ保護法の同等の用語を含むものとします。

「**保護対象保健情報**」または「**PHI**」とは、Health Information Portability and Accountability Act （医療情報の携行性と責任に関する法律、HIPAA）によって保護されている、Microsoft の個人データを意味します。

「**レッドチーム演習**」とは、試験実施団体が協力して意図的にシステムを測定し、その限界、リスクサーフェス、脆弱性を特定する方法です。詳細は https://aka.ms/CustomerRedTeamingGuide を参照してください。

AI の「**機密性の高い使用**」とは、AI システムの合理的に予見可能な使用または誤用が、個人に次のような影響を与える可能性がある場合です。

- 法的地位や人生の機会に対する重大な影響。
- 身体的または心理的傷害のリスク。
- 人権への脅威。

「**下請け業者**」とは、Microsoft と直接契約していないサプライヤーの関連会社を含め、サプライヤーのその業務を対象とする契約に関連する義務を委任する第三者を意味します。

「**サブプロセッサー**」とは、Microsoft が業務を委託する第三者を意味します。本業務には、Microsoft がプロセッサーとして行う Microsoft の個人データの処理が含まれます。

サプライヤーの対応

サプライヤーは、Microsoft が管理するオンラインサービスを通じて、これらの要件への準拠を毎年確認します。遵守の管理方法に関しては、SSPA プログラムガイドを参照してください。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション A：管理	
1	Microsoft とサプライヤー間で適用される各契約（基本契約、作業明細書、発注書、その他の注文など）には、Microsoft の個人データの販売および Microsoft とサプライヤー間の直接的取引関係外における同データの処理の禁止を含む（該当する場合）、Microsoft の機密データおよび Microsoft の個人データに関するプライバシーおよびセキュリティデータ保護の文言が含まれるものとする。 業務に関連してプロセッサーまたはサブプロセッサーとして機能している企業の場合、Microsoft の個人データに関して、同契約には、処理の主な内容と期間、処理の性質および目的、Microsoft の個人データの種類およびデータ主体のカテゴリ、および Microsoft の義務と権利が規定されていなければならない。	サプライヤーは、Microsoft とサプライヤー間で適用される契約を提示しなければならない。 プロセッサーおよびサブプロセッサーの場合、適用される契約にデータ処理の説明を記載する（*例*：作業明細書、発注書など）。 Microsoft によってサプライヤーの業務に PHI の処理が関係することが確認された場合、サプライヤーは Microsoft とビジネスアソシエイト契約および/またはその他の契約を締結しなければならない。 注：処理中の発注書がある会社の場合は、購入プロセスの後の過程で処理活動の必要な説明を追加することができる。
2	Microsoft によってサプライヤーの業務にサブプロセッサーの役割を果たすことが関係することが確認された場合、サプライヤーは Microsoft と適切なデータ保護契約を締結しなければならない。 注：これらの指定が適用される場合、Microsoft は同指定をそのサプライヤーのプロファイルに掲載する。	標準契約条項、オンライン顧客データ補遺、サプライヤーおよびパートナーの専門サービスに関するデータ処理に関する補遺および/またはビジネスアソシエイト契約。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション A：管理（続き）	
3	Microsoft の個人データまたは機密データにアクセスできるすべての人（システム管理者、運用スタッフ、管理者、サードパーティなど）を対象としたプライバシーとセキュリティのトレーニングを毎年設定し、維持し、実施する。 注：サプライヤーの担当者は、Microsoft の部門が提供する追加トレーニングを完了させなければならない場合がある。	トレーニングへの出席の年次記録が利用でき、要求に応じて Microsoft に提供できる。 トレーニングの内容は定期的に更新され、パスワードの保護を含むインシデント防止の認識、ログインの監視、悪意のあるソフトウェアのダウンロードに関連するリスク、その他の関連するセキュリティリマインダーなど、プライバシーとセキュリティの原則を含める。 トレーニング要件の遵守文書には、プライバシー規制要件、セキュリティ義務、および該当する契約要件と義務への遵守に関連するトレーニングの証拠を含める。 IT スタッフによるインシデント対応のトレーニング、危機的状況の際に効率的な対応を促すためにシュミレーションされた事象と自動化されたメカニズム、および サプライヤーが処理する Microsoft の個人データに PHI が含まれる場合、トレーニング内容に HIPAA トレーニングを含めなければならず、それにはビジネスアソシエイト契約にて認められているサプライヤーによる使用と開示を含めるものとする。
4	サプライヤーのプライバシーおよびセキュリティポリシー、または Microsoft の企業環境内で業務を行っている場合に適用される Microsoft のポリシーを遵守しない従業員に対して、適切な制裁措置を適用する。	不遵守に対する制裁（解雇処分を含むなど）を記述したプライバシーポリシーおよびセキュリティポリシーを文書化する。
5	Microsoft の個人データは、Microsoft の文書化された指示に従ってのみ処理される。これには、法律で義務付けられている場合を除き、Microsoft の個人データの第三国または国際機関への転送に関するシナリオが含まれる。法律で義務付けられている場合は、同法律が公益の重要な理由で当該情報を禁止していない限り、サプライヤー（プロセッサーまたはサブプロセッサー）は処理以前に同法的要件を Microsoft（コントローラー）に通知するものとする。	サプライヤーは、業務に関与するサプライヤーの従業員や請負業者が容易にアクセスできる場所で、Microsoft が文書化したすべての指示（契約書、作業明細書、注文書など）とそのプライバシーポリシー、セキュリティポリシー、手順を電子的に編集および維持する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション B：通知	
6	サプライヤーは、Microsoft に代わって個人データを収集する場合、Microsoft のプライバシーに関する声明を使用することが義務付けられる。 プライバシーに関する通知は、データ主体がサプライヤーに個人データを提出するかどうかを判断する指標となるよう、明確かつ利用可能な状態にしておく必要がある。 注：貴社が処理活動のコントローラーである場合、例えば、ウェブサイトが Microsoft のブランドでない場合、サプライヤーは独自のプライバシー通知を表示することができる。	サプライヤーは、現在公開されている Microsoft のプライバシーに関する声明へのfwdlinkを使用する。 ユーザーの個人データが収集されるあらゆる状況において同プライバシーに関する声明を掲載する。 該当する場合は、オフラインバージョンが利用可能であるため、データ収集の前に提供する。 使用されるオフラインのプライバシーに関する声明は、公開されている最新バージョンであり、適切な日付が記載されているものとする。 Microsoft の従業員サービスの場合、Microsoft のデータプライバシー通知を使用する。
	セクション C：選択と同意	
7	サプライヤーは、個人データを収集する前に、実施するすべての処理活動（新規および更新された処理活動を含む）に対するデータ主体の同意を取得し、記録しておく必要がある。 サプライヤーは、選択管理の有効性を監視して、選択の変更を尊重する期間が、適用される最も制限の厳しい現地の法的要件であることを確実にする。	サプライヤーは、データ主体による処理活動への同意の提供方法、および同意の範囲が同データ主体の個人データに関するサプライヤーのすべての処理活動を対象としていることを示すことにより、遵守の証拠を提供できる。 サプライヤーは、データ主体が処理活動に対する同意を取り消す方法を示すことにより、遵守の証拠を提供できる。 サプライヤーは、新しい処理アクティビティを開始する前に、選択がどのように確認されるか示すことにより、遵守の証拠を提供できる。 注：サービスの実験または技術文書を表示する機会など、ユーザーとのやり取りのスクリーンショットも証拠として受け入れられる。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション C：選択と同意（続き）	
8	Cookie（および/または、デバイスからデータを保存または取得する類似の技術、またはその他の方法で同様にユーザーの追跡を可能にする技術）を使用するウェブサイトは、データ対象者のブラウザまたはデバイスに関連して Cookie が使用または配置される前に、データ対象者から法的に要求される同意を得なければならない。 Microsoft のウェブサイトおよび/またはアプリケーション、あるいは Microsoft のブランドを掲載するサイトを作成および管理するサプライヤーは、データ主体に対して、Microsoft のプライバシーに関する声明および現地の法的要件に沿った Cookie の使用に関する透明性のある通知と選択を提供する必要がある。 本要件は、サイトが欧州連合/欧州経済領域および該当するプライバシー法が適用され、Microsoft のプライバシーに関する声明が使用されるその他の地域内のユーザーを対象とする場合に適用される。	各 Cookie の目的を文書化し、実装されている Cookie の種類を通知するものとする。 • セッション Cookie で十分な場合は、永続的 Cookie を使用しない。 • 永続的 Cookie を使用する場合、ユーザーがサイトにアクセスしてから 13 か月を超える有効期限を設定することはできない。 必要に応じて、次のような EU 法への遵守を検証する。 • プライバシーに関する声明に対してラベル付け規則「プライバシーとクッキー」を使用する、 • 広告などの「必須ではない」目的において Cookie を使用する前に、ユーザーの同意を得る、および • 同意は 6 か月以内に失効するか、6 か月ごとに再取得する必要がある。
	セクション D：収集	
9	サプライヤーは、Microsoft の個人データおよび/または機密データの収集を監視して、業務に必要なデータのみが収集されていることを確認する必要がある。	サプライヤーは、収集された Microsoft の個人および/または秘密データが業務において必要であることを示す書類を提出できる。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
10	子供からデータを収集する前に、サプライヤーはその地域のプライバシー法に従って同意を得る必要がある（該当する法域で定義されているように）。	サプライヤーは、親/保護者の同意を示す文書を提供できる。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
11	サプライヤーが Microsoft から、仮名、NPI（識別する権限のない）、リンクしていない仮名、集約化、匿名、またはこの分類のうちのどれかに関するなんらかの条件（非特定化など）を含む、識別可能性を低下させたデータセットを受け取った場合、サプライヤーはデータを受け取った状態のままで維持する。	サプライヤーは、データセットの識別可能性を増加させない（すなわち、他のデータセットと結合させて、データセットの一部である個人を再特定させない）ものとする。 サプライヤーはデータの非特定化/匿名化のデータポリシー/プロセスを持つものとする。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション E：保持	
12	Microsoft の個人データおよび/または機密データの継続的な保持が法律で義務付けられている場合を除いて、Microsoft の個人データおよび機密データが業務に必要な期間を超えて保持されないことを確実にする。	サプライヤーは、本契約で Microsoft が指定した文書化された保持ポリシーまたは保持要件（作業明細書、発注書など）を遵守する。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
13	Microsoft の独自の裁量により、サプライヤーが所有または管理している Microsoft の個人データおよび機密データが、業務の完了時または Microsoft の要求に応じて Microsoft に返却または破棄されるようにする。 アプリケーション内には、ユーザーによって明示的にまたはデータの経過時間などの他のトリガーに基づいてデータがアプリケーションから削除された際に、データが安全に削除されるようにするプロセスを導入している必要がある。 Microsoft の個人データまたは機密データの破棄が必要な場合、サプライヤーは、Microsoft の個人データおよび/または機密データを含む物理的資産を焼却、粉砕、切断して、情報の読み取りや再構築ができないようにする。	Microsoft の個人データおよび機密データの廃棄記録を保管する（これには、破棄のために Microsoft に返却した記録も含まれる）。 Microsoft が破棄を要求、または要請した場合は、サプライヤーの役員が署名した破棄証明書を提出する。
	セクション F：データ主体	
	データ主体は、個人データの処理にアクセスする、それを削除する、編集する、外部に転送する、制限する、およびそれに異議を唱える権利（「データ主体の権利」）を含む、法律に基づく特定の権利を有する。データ主体が Microsoft の個人データに関して法律に基づく権利を行使しようとした場合、サプライヤーは Microsoft に以下のアクションを実施できるようにするか、またはサプライヤーが Microsoft に代わってこれらのアクションを実施しなければならない。	

14	データ主体の権利行使の要求に応じる義務を果たすことができるように、適切な技術的、そして組織的措置を通して可能な限り不当に遅れることなく Microsoft を支援する。 Microsoft から別段の指示がない限り、サプライヤーは、サプライヤーに直接問い合わせてきたすべてのデータ主体を Microsoft に誘導し、データ主体がデータ主体権を行使できるようにする。	サプライヤーは、データ主体の権利行使を証明するために、文書化されたプロセスと手順の証拠を保管する。 サプライヤーは、文書化されたテストの証拠を保管する。証拠は、Microsoft の要求に応じて提供可能な状態になっているものとする。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション F：データ主体（続き）	
15	データ主体に直接対応する場合、またはサプライヤーがオンライン上でのセルフサービスによるメカニズムを提供する場合、サプライヤーは、要求を行っているデータ主体を特定するためのプロセスと手順を実施しているものとする。	サプライヤーは、Microsoft データ主体を特定するために使用される方法を文書化しているものとする。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
16	オンライン上のセルフサービスによるメカニズムを通じて取得できないデータ主体に関する Microsoft の個人データを特定するように Microsoft から依頼された場合、サプライヤーは要求されたデータを見つけるために合理的な努力を払い、合理的な検索が行われたことを示すために十分な記録を保管する。	サプライヤーは、Microsoft の個人データが保持されているかどうかを確認するための手順の文書化された証拠を保管し、要求に応じて Microsoft に文書を提供する。 サプライヤーは、データ主体の権利の要求を満たすために実施された手順を示す記録を保管する。 同記録には、以下が記載されているものとする。 • 要求の日時 • 要求に応じるために実施されたアクション、および Microsoft に通知した日時の記録 サプライヤーは、要求に応じて、Microsoft に記録保持の証拠を提出する。
17	サプライヤーは、Microsoft の個人データにアクセスするために、またはその他の方法で権利を行使するためにデータ主体が取らなければならない手順を同人に通知する。	サプライヤーは、Microsoft の個人データにアクセスするために行われたコミュニケーションと手順の文書化された証拠を保管する。サプライヤーは、文書化された証拠を保管し、要求に応じて同じ証拠を Microsoft に提供する。

18	データ主体の権利による要求の日時と、当該要求に応じてサプライヤーが行った措置を記録する。 データ主体の要求が拒否された場合、Microsoft の指示により、データ主体に書面による説明を提供する。 要求に応じて、データ主体の要求の記録を Microsoft に提供する。	サプライヤーは、アクセス/削除の要求の記録を保管し、Microsoft の個人データに加えられた変更を文書化する。 要求が拒否された事例を文書化し、Microsoft のレビューと承認の証拠を保管する。 サプライヤーは、Microsoft の個人データへの要求およびアクセスの拒否に関する記録保持の証拠を提出する。
19	サプライヤーは、認証されたデータ主体から要求された Microsoft 個人データのコピーを、適切な印刷、電子、または口頭の形式で Microsoft が取得できるようにしなければならない。	サプライヤーは、Microsoft の個人データを、容易に理解でき、データ主体とサプライヤーにとって便利な形式でデータ主体に提供する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション F：データ主体（続き）	
20	サプライヤーは、Microsoft または認証済みのデータ主体に公開された Microsoft の個人データを他の人物を特定するために使用できないようにするために、合理的な予防措置を講じる必要がある。	サプライヤーは、契約条件に反するデータ主体の特定を回避するために講じる予防措置に関する手順の文書化された証拠を保管する。サプライヤーは、要求に応じて、Microsoft に証拠を提出する。
21	データ主体は、保有する Microsoft の個人データが完全かつ正確ではないと判断した場合、サプライヤーは同問題を Microsoft に報告し、必要に応じて Microsoft と協力して問題を解決する必要がある。	サプライヤーは完全かつ正確ではないデータの事例を文書化し、同問題を Microsoft に報告する。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
22	データ主体のアクセス要求に関して、サプライヤーは、Microsoft の個人データを共有した、または共有するすべての受信者の記録を保持する必要がある。	要求に応じて、サプライヤーは、Microsoft の個人データの実際の受領者および第三者受領者となり得る者の一覧を提供することができる。
	セクション G：下請け業者	
	サプライヤーが下請け業者を通じて Microsoft の個人データまたは機密データを処理する場合、サプライヤーは次のことを行う必要がある。	

23	サービスの下請けに出す前、または下請け業者の追加または交換に関する変更をする前に、Microsoft に通知する。	Microsoft の個人データが、該当する契約（作業明細書、補遺、発注書など）において要求されている、または SSPA データベースに保存されている、Microsoft によって承認された企業によってのみ処理されることを検証する。サプライヤーは、下請け業者の一覧をオンラインに掲載し、SSPA データベースのページへのリンクを含むことができる。
24	下請け業者に対し、プライバシーおよびデータ保護に関する条項を含め、サプライヤーが Microsoft と締結する契約の条項よりも Microsoft への保護が劣らない条項に書面で同意するよう求める。	サプライヤーは、要求に応じて、下請け業者との契約書類を Microsoft に提出する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション G：下請け業者（続き）	
25	下請け業者によってサブプロセッサーに委託された Microsoft の個人データおよび機密データの性質と範囲を文書化し、収集された情報が業務に必要であることを確認する。	サプライヤーは、下請け業者に開示または転送された Microsoft の個人データおよび機密データに関する文書を保管する。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
26	下請け業者による Microsoft の個人データまたは機密データの処理を、サプライヤーと Microsoft 間の契約を履行するために必要な目的に限定する。 Microsoft の個人データが PHI である場合、Microsoft とサプライヤー間のビジネスアソシエイト契約と同様に、Microsoft の個人データの下請け業者による処理を制限し、また Microsoft の個人データの機密性およびセキュリティを保護するビジネスアソシエイト契約も下請け業者と締結する。	サプライヤーは、下請け業者に提供された Microsoft の個人データが業務に必要であることを示す文書を提供できる。 サプライヤーは、要求に応じて Microsoft にビジネスアソシエイト契約（該当する場合）を含む証拠書類を提出するものとする。
27	下請け業者が業務に関連する目的以外で Microsoft の個人データまたは機密データを処理したことを知った場合、直ちに Microsoft に通知する。	サプライヤーは、下請け業者に対して Microsoft のデータの誤用を報告するための指示と手段を提供しているものとする。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
28	サプライヤーが Microsoft に代わって第三者から個人データを収集する場合、サプライヤーは、第三者のデータ保護ポリシーと適用が Microsoft と締結したサプライヤーの契約および本 DPR と一致していることを検証する必要がある。	サプライヤーは、第三者のデータ保護ポリシーと適用に関して実施されたデューデリジェンス文書を提供できる。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション H：品質	
29	サプライヤーは、すべての Microsoft の個人データの整合性を維持し、処理された目的に応じて同データが正確性、完全性、関連性を保つように管理する必要がある。	サプライヤーは、Microsoft の個人データが収集、作成、更新される場合、それを検証するための手順が整っていることを実証することができる。 サプライヤーは、継続的に正確性を検証し、必要に応じて修正を施すために、監視、情報システムの活動のレビューおよびサンプリング手順が実施されていることを実証できる。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
	セクション I：監視と施行	
30	サプライヤーは、データインシデントに気付いた際に、契約上の要件に従って、適用される個人情報保護法に記載されているとおり、または過度の遅延なしに、いずれか早い手順で Microsoft に通知することをサプライヤーに義務付けるインシデント対応計画を持っているものとする。 サプライヤーは、Microsoft の要求または指示に応じて、犯罪調査の実施において必要となるデータ、情報、サプライヤー担当者への連絡、またはハードウェアの提供を含め、インシデントの調査、軽減、または修復のために Microsoft と協力する必要がある。フォレンジックレビューの実施に必要なサプライヤーの担当者またはハードウェアへのアクセスも必要になる場合がある。 サプライヤーは、セキュリティ事故が発生した場合に迅速に対応できるよう、SupplierWeb のセキュリティ連絡先欄に適切な担当者を記入する。 注：Microsoft にインシデントを通知する方法については、SSPA プログラムガイドを参照。	サプライヤーは、本項で説明されているように、顧客（Microsoft）に通知する手順を含むインシデント対応計画を保有する。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

31	適切な是正措置が適時行われるよう、是正計画を実施し、各データインシデントの解決を監視する。	サプライヤーは、データが解決され、インシデント後のレビューを提供するまで、Microsoft への時宜にかなった更新を含む、データインシデントに対応するために従う手順を文書化している。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
セクション I：監視と施行（続き）		
32	Microsoft が Microsoft の個人データのコントローラーである場合、Microsoft の個人データに関連するすべてのデータ保護の苦情に対応するための正式な苦情処理プロセスを作成する。	サプライヤーは、常に Microsoft の個人データに関する苦情に対応する手段を講じ、苦情に対処するための苦情手続文書を保持する。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
セクション J：セキュリティ		
	サプライヤーは、ポリシーと手順を含む情報セキュリティプログラムを確立、実施、および継続して、業界で採用されている慣行に従い、法律で義務付けられているように、Micorsoft の個人データと機密データを保護および保持する必要がある。サプライヤーのセキュリティプログラムは、以下の要件 33～49 に記載されている基準を満たすものとする。 Microsoft の個人データが PHI である場合、サプライヤーは PHI のセキュリティに影響する環境上/業務上の変更に応じて、技術的および非技術的評価も定期的に実施し、サプライヤーのポリシーおよび手順が HIPAA セキュリティ規則をどの程度満たしているかを確認する必要がある。	有効な ISO 27001認証は、セクション J「セキュリティ」の代替として許容される。その場合は、 注：代替手段を申請する証明書をアップロードすること。
33	以下を含む年次ネットワークセキュリティ評価を実行する必要がある。 • Microsoft の個人データの機密性、完全性、可用性、およびリスク低減手段の実装に対する潜在的なリスクと脆弱性の評価、 • 新しいシステムコンポーネント、ネットワークトポロジ、ファイアウォールルールなどの環境に加えられた主な変更のレビュー、 • 変更ログの維持。	サプライヤーは、ネットワーク評価、変更ログ、およびスキャン結果を文書化しているものとする。 必要な変更ログは、変更を追跡して、変更の理由に関する情報を提供し、指名された承認者の氏名と役職を含む必要がある。過去 90 日の記録は要求時に提供できる。

34	サプライヤーは、モバイルデバイスでアクセスまたは使用される Microsoft の個人データまたは機密データの使用を保護および制限するモバイルデバイスポリシーを定義、伝達、および施行するものとする。	サプライヤーは、Microsoft 個人データまたは秘密データの処理にモバイルデバイスを使用する必要がある場合、準拠しているモバイルデバイスポリシーの使用を実証する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション J：セキュリティ（続き）	
35	業務、セキュリティ、運用をサポートするために使用されるすべての物理的および仮想的資産は、説明が施され、識別された所有者が決められている必要がある。 サプライヤーは、これらの情報資産のインベントリを管理し、許容可能かつ承認された使用方法を確立して、資産のライフサイクル全体にわたって適切なレベルの保護を提供する責任がある。	業務、セキュリティ、運用をサポートするために使用されるデバイス資産のインベントリ。これらの資産のインベントリには、以下が含まれる。 ● デバイスのロケーション ● 資産上のデータのデータ分類 ● 雇用または業務契約の終了に伴う資産回収の記録、および ● 不要になったデータストレージ媒体の破棄の記録 ● @microsoft.com 資格情報を持つサプライヤーの担当者が Microsoft データにアクセスするために使用するすべての物理デバイスおよび仮想デバイスは、Microsoft が独自に完全に管理し、Microsoft が提供したものに追加でセキュリティソフトウェアをインストールしないようにする必要がある。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクションJ：セキュリティ（続き）	
36	サプライヤの管理の下、Microsoft の個人データまたは機密データへの不正アクセスを防止するためのアクセス権管理手順を確立および維持する。	サプライヤーは、以下を含むアクセス権管理計画を実施していることを実証する。 • アクセス管理手順 • 身元確認手順 • 試行が失敗した場合のロックアウト手順 • 一定時間操作が無い場合の自動ログオフ • 認証資格情報を選択する為の厳格なパラメーターの使用 • 雇用終了に伴うユーザーアカウント（従業員または下請け業者が使用するアカウントを含む）の 48 時間以内の非アクティブ化 • パスワードの長さと複雑さを強制し、再利用を防止する強力なパスワード制御 • ID に対する多要素認証（MFA）の使用。 サプライヤーは、Microsoft の個人データおよび機密データへのユーザーアクセスをレビューするためのプロセスを確立しており、最小特権の原則を実施していることを実証する。本プロセスには、以下が含まれる。 • 明確に定義されたユーザーの役割 • 役割へのアクセス権をレビューして、承認を検証する手順、および • Microsoft データにアクセスすることができる役割内のユーザーが、グループ/役割に参加する文書化された正当な理由があるかどうかを判定するテスト • アカウントやパスワードの共有の断固禁止

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション J：セキュリティ（続き）	
37	Microsoft 個人データまたは機密データの処理に使用されるシステムに対して、セキュリティパッチの優先度を定めるパッチ管理の手順を定義し、実装する。これらの手順には次の内容が含まれる。 • 毎月脆弱性スキャンを行い、12 か月間毎月スキャンを実施したことを示す高度なコンプライアンスレポートを提出する • セキュリティパッチの優先度を決める、定義されたリスクアプローチ • 緊急パッチを処理および実装する機能 • オペレーティングシステム、サーバーソフトウェア（アプリケーションサーバーなど）、およびデータベースソフトウェアへの適用性 • パッチにより軽減されるリスクの文書化と例外の追跡、および • 制作会社によるサポートが終了したソフトウェアの廃止に関する要件	サプライヤーは、本要件を満たし、少なくとも以下を対象とするパッチ管理の手続きが実装されていることを実証できる。 • 重大度の定義は文書化され、更新プログラムに割り当てられ、展開の優先順位付けを通知する。 • 緊急パッチを実装するための文書化された手順 • パッチ管理は、承認と例外を追跡し、パッチ適用コンプライアンスデータを含む記録を作成する。過去 90 日の記録は要求時に提供できる。
38	潜在的に有害なウイルスや悪意あるソフトウェアアプリケーションから保護する目的で、Microsoft 個人データ/秘密データの処理に使用されるネットワークに接続された装置（サーバー、本番環境およびトレーニング用デスクトップを含む）にウイルス対策およびマルウェア対策ソフトウェアをインストールする。ウイルス対策およびマルウェア対策ソフトウェアには必ず定期的にパッチを当て、更新する。 マルウェア対策の定義を毎日更新するか、ウイルス対策/マルウェア対策サプライヤーの指示に従って更新する。注：これは、Linux を含むすべてのオペレーティングシステムに適用される。	ウイルス対策ソフトウェアとマルウェア対策ソフトウェアの使用がアクティブであることを示すレポートが存在する。 注：これは、すべてのオペレーティングシステムに適用される。
39	Mictosoft のソフトウェアを開発するサプライヤーは、設計の段階にセキュリティ・バイ・デザインの原則を組み込む必要がある。	サプライヤーの技術仕様書には、開発サイクルにおけるセキュリティ検証のチェックポイントが含まれている。 サプライヤーはコードスキャンの形式を使用して明かな欠陥をアラートする。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション J：セキュリティ（続き）	
40	データ損失防止（「DLP」）プログラムを採用して、アプリケーション、システム、インフラストラクチャレベルで侵入、損失、およびその他の不正なアクティビティを防止する。データは適切に分類、ラベル付け、保護されている必要があり、サプライヤーは、Microsoft の個人データまたは機密データが処理される使用中の情報システムに侵入、損失、およびその他の不正なアクティビティがないか監視する必要がある。DLP プログラムの最低要件は以下の通りである。 • Microsoft の個人データまたは機密データを保持している場合は、業界標準のホスト、ネットワーク、およびクラウドベースの侵入検知システム（「IDS」）の使用 • データ損失を監視して積極的に阻止するために構成された高度な侵入防御システム（「IPS」）の実装 • システムが侵害された場合、システムを分析して、残りの脆弱性にも対処していることの確認 • システムの侵害検出ツールを監視するために必要な手順の説明 • データインシデントが検出されたときに実行する必要のあるインシデント対応および管理プロセスの確立 • Microsoft の個人データまたは機密データの不正なダウンロードおよび使用に関する伝達（サプライヤーの業務に携わっていないすべてのサプライヤーの従業員および下請け業者への）	侵入、損失、およびその他の不正なアクティビティ（および少なくとも本セクションで指定されているすべての項目）を防止するための手順とともに文書化された DLP プログラムが実施されている。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション J：セキュリティ（続き）	
41	サプライヤーは、開発プロセスのどの段階でも、秘密事項がソフトウェアに埋め込まれていない、またはハードコードされていないことを確認する必要がある。	サプライヤーは、ユーザー名、パスワード、SSH キー、API アクセストークンなどの秘密事項が、テスト環境または本番環境のいずれにおいても、ソースファイルまたは構成ファイルに組み込まれないようにするための手順を文書化している。 サプライヤーは以下を実証できる。 • GitHub Advanced Security（GHAS）や同様のサービスやツールなど、資格情報の公開防止ツールがサポートされている最新バージョンの使用。 • ソースまたは構成ファイルに秘密事項が誤って含まれていた場合、それらの秘密事項は検出時に取り消されたものとして文書化されていることを保証する。 • 置換またはセカンダリ資格情報がコードにプッシュバックされていないこと。 • 誤検知とその修復の文書化。
42	サプライヤーは、バックアップ計画プロセスが Microsoft の個人データおよび機密データを不正な使用、アクセス、開示、改ざん、および破壊から保護することを保証する必要がある。	サプライヤーは、組織が破壊的な事象を管理する方法、および経営陣が承認した情報セキュリティの継続的な目標に基づいて情報セキュリティを所定のレベルに維持する方法を詳述した、文書化された対応および復旧手順を実証することができる。 サプライヤーは、重要なデータのバックアップを定期的に取り、安全に保管して、効果的に復旧するための手順を定義および実装したことを実証できる。
43	業務継続性と災害復旧計画を確立して、テストする。	災害復旧計画には次の点を含める必要がある。 • システムがサプライヤーの業務運営にとって重要であるかどうかを判断することを目的とした基準。 • 災害発生時の復旧の対象とならなければいけない定義済みの基準に基づいて、重要なシステムを一覧にする。 • システムを知らないエンジニアが 72 時間以内にアプリケーションを復旧できるようにする、重要なシステムごとに定義された災害復

		旧手順。 • 復旧目標を確実に達成できるようにするための、災害復旧計画の年次（またはより頻繁な）テストとレビュー。
#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
セクション J：セキュリティ（続き）		
44	Microsoft の個人データまたは機密データへのアクセス権を個人に付与する前に同個人の身元を認証し、そのアクセス権が、業務の遂行を目的としてその特定の個人に対して許可されている活動の範囲に限定されていることを確認する。	すべてのユーザー ID が異なっていて、それぞれに Azure Active Directoryなどの業界標準の認証方法が存在していることを確認する。 セキュリティキー、電話ベースのオーセンティケーター、スマートカードなどの多要素認証（MFA）の使用を要求しなければならない。 すべてのサプライヤーの従業員および下請け業者による Microsoft の個人データまたは機密データへのアクセスが、業務を遂行するために必要な範囲や期間を超えないようにするプロセスを規定する、文書化された情報セキュリティプログラム。
45	サプライヤーは、採用および配置のプロセスにおいて、音声および目視により面接および採用を行い、Microsoft に配置した従業員が同一人物であることを確認する。従業員の住所情報は、銀行情報および機器の出荷場所と一致していなければならない。	仕事を始める前に、その従業員は Microsoft の主担当者と、その従業員を面接・採用したサプライヤーの担当者に会わなければならない。Microsoft の主担当者は、通常の営業時間中に、従業員と定期的にリアルタイムで音声およびビデオによるやり取りを行う必要がある。 機器の出荷について、サプライヤーは、出荷場所が実際に居住可能な住居であり（すなわち、積み替え地点ではない）、従業員が銀行サービスのために提供した住所と一致していることを確認するための書類を作成する。

46	サプライヤーは、トランスポート層セキュリティ（「TLS」）またはインターネットプロトコルセキュリティ（「IPsec」）を使用した暗号化によって、ネットワークを通過する業務に関連して処理されるすべてのデータを保護する必要がある。 これらの方式は NIST 800-52 および NIST 800-57に記載されている。これらと同等の業界標準を使用することも可能である。 サプライヤーは、暗号化されていない手段で送信された Microsoft の個人データまたは機密データの受信を拒否する必要がある。	TLS またはその他の認証を作成、展開、および置換するプロセスを定義して実施する必要がある。
47	Microsoft の個人データまたは機密データにアクセスする、またはそれらを処理するすべてのサプライヤーデバイス（ノートパソコン、ワークステーションなど）は、ディスクの暗号化をする必要がある。	すべてのデバイスを暗号化し、Microsoft の個人データまたは機密データの処理に使用されるすべてのクライアントデバイス用の BitLocker または他の同等機能のディスク暗号化ソリューションに適合させる。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクションJ：セキュリティ（続き）	
48	システムと手順（NIST 800-111標準に記載されているような現在の業界標準を使用）は、保存時に（保存されている場合）、**すべての** Microsoft 個人データおよび/または機密データを暗号化するために配置されている必要がある。この例には以下が含まれるが、これらに限定されない。 • 資格情報データ（ユーザー名、パスワードなど） • 支払方法のデータ（クレジットカード番号、銀行口座番号など） • 移民関連の個人データ • 医療プロフィールデータ（認証目的で使用される医療記録番号、生体マーカー、または DNA、指紋、目の網膜と虹彩、音声パターン、顔の特徴、手の測定値などの識別子） • 政府発行の識別子データ（社会保障番号や運転免許証番号など） • Microsoft の顧客に帰属するデータ（SharePoint、O365 ドキュメント、OneDrive の顧客など） • 未発表の Microsoft 製品に関連する資料 • 出生日 • 子供のプロフィール情報 • リアルタイムの地理データ • 自宅住所 • プライベートの電話番号 • 宗教 • 政治的見解 • 性的指向 • セキュリティに関する質問（2要素認証、パスワードリセットなど） • 母親の旧姓	Microsoft の個人データと機密データが保存時に暗号化されていることを確認する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション J：セキュリティ（続き）	
49	開発環境またはテスト環境において使用されるすべての Microsoft の個人データを匿名化する。	Microsoft の個人データは、開発環境またはテスト環境で使用しない。代替手段がない場合は、データ主体の特定や個人データの誤用を防止するために匿名化する必要がある。 注：匿名化されたデータは、仮名化されたデータとは異なる。匿名化されたデータとは、識別可能な自然人に関連しないデータを指し、個人データのデータ主体を識別できない状態である。 Microsoft の個人データが PHI である場合、匿名化は HIPAA 非識別化標準を遵守する必要がある。
	セクション K：AI システム	
50	サービスの提供に関連して AI システムが含まれる場合、サプライヤーは、適用される AI システムに関する条件を Microsoft と締結する必要がある。 使用目的の変更は、不当な遅滞なく開示し、正確性とコンプライアンスのために少なくとも年に一度見直さなければならない。	AI システムの契約条項は、Microsoft とサプライヤー間の契約に記載されている。
51	デプロイ中およびデプロイ後の AI システムのトラブルシューティング、管理、操作、監督、および制御の責任と説明責任を、社内の人物またはグループを指定して割り当てる。	サプライヤーは、AI システムに関する規定の遵守に責任を負う個人またはグループの役割を報告する。 この個人またはグループの権限と説明責任を説明する文書。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション K：AI システム（続き）	
52	パフォーマンスに関連して、サプライヤーが AI システム内のデータにアクセスし、データを処理するすべての人に対して、プライバシーとセキュリティのトレーニングを毎年設定し、維持し、実施する。	トレーニングへの出席の年次記録が利用でき、要求に応じて Microsoft に提供できる。 トレーニング要件の遵守文書には、AI システムの継続的使用におけるプライバシー規制要件、セキュリティ義務、および該当する契約要件と義務への遵守に関連するトレーニングの証拠を含める。 トレーニングの内容は毎年検証される。
53	サプライヤーは、AI システムのインシデント対応計画を策定しており、AI システムの使用目的および機密性の高い使用に悪影響を与えるデータ インシデントまたは障害に気付いた場合、適用されるプライバシー法に規定されている契約上の要件に従って、または不当な遅延なく、いずれか早い方で Microsoft に通知しなければならない。 Microsoft にインシデントを通知する方法については、SSPA プログラムガイドを参照。	サプライヤーには、すべてのエンドポイントで以下を含む AI システムのインシデント対応計画がある。 • この要件での説明に沿った、顧客（Microsoft）に通知する手順。 • システム全体をロールバックできるようになるまでの経過時間を含むシステムロールバック計画。 • 機能をオフにできるようになるまでの経過時間など、機能をオフにするための対応。 • システムが更新されるまでの経過時間を含む、各モデルの更新とその更新リリースのプロセス。 • 顧客、パートナー、エンド ユーザーに、システムの変更、障害に関する最新の理解、および最善の軽減策を通知する方法に関するプロセス。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
54	サプライヤーには AI システムのレッドチーム演習が必ずあること。 AI システム展開前に脆弱性に対応しなければならない。	サプライヤーには以下の文書がある。 • レッドチーム演習プロセスが講じられている。 • 脆弱性に対応済みである。
55	サプライヤーは、以下を含む開示および文書化を通じてデータコンプライアンスを確保するための責任ある AI プログラムを実施している（要件 56～61）。	サプライヤーには、責任ある AI プログラムを説明する文書がある。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

56	サプライヤーには使用目的の透明性開示がある。	使用目的の透明性開示は、要求時には Microsoft に提供される。
#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション K：AI システム（続き）	
57	**署名入契約書**：AI サプライヤーと取引する場合、組織は署名入契約書で明確な契約条件を確立する必要がある。契約書では、データの取り扱い、機密性、知的財産権、責任、インシデント対応、該当する機密性の高い使用について明示的に対処しなければならない。	サプライヤーは、要求に応じて、Microsoft に契約（該当する場合）を含む証拠書類を提出するものとする。
58	**説明責任**：組織内での AI の導入とリスク管理に関する説明責任と責任を明確に定義する。組織は、AI システムの結果に対する責任者を特定する必要がある。これには、倫理的な懸念、偏見、時間の経過とともに発生する可能性のある問題への対処が含まれる。倫理ガイドラインへの準拠を維持するために AI モデルを定期的に監視し監査することが不可欠である。	サプライヤーには、個人またはグループの説明責任と責任を含む、責任ある AI プログラムを説明する文書がある。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
59	**リスク評価**プライバシー、セキュリティ、責任ある AI のリスク評価を実施して、潜在的なバイアス、セキュリティの脆弱性、意図しない結果を考慮する。機密性の高い使用が含まれている場合は、必要な管理または軽減策のガイダンスを含める必要がある。	サプライヤーは、既知または新たなエラー、人口統計学的グループへのさまざまな影響、ハルシネーション、セキュリティとプライバシーのコンプライアンスを維持するために必要なその他の修復、または技術的管理を改善するために、リスク評価の証拠、またはテスト、システム進化の監視、継続的なメンテナンスなどの同様の文書または報告を毎年保持するものとする。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
60	**透明性と説明可能性**：AI システムは透明で説明可能でなくてはならない。サプライヤーは意思決定方法についての意見を提供する必要がある。開示によって、モデルアーキテクチャ、トレーニングデータ、意思決定プロセスの透明性が促進される。	サプライヤーは、使用目的を損なうすべてのシステム障害報告、破損、ハルシネーション、誤用報告などを記録し、問題解のために講じられた手順の証拠を提供するものとする。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
61	**モニタリングと適用**：サプライヤーは AI システムを継続的に監視し、新たに生じるリスクに対して AI システムを適合し更新する必要がある。	サプライヤーは、使用目的を損なうすべてのシステム障害報告、破損、ハルシネーション、誤用報告などを記録し、問題解のために講じられた手順の証拠を提供するものとする。

		サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション K：AI システム（続き）	
62	サプライヤーは、各使用目的について、必要なすべてのエラータイプ、パフォーマンス指標の定義、データパフォーマンス、安全性、信頼性指標などとともに、必要な開示、報告、その他の同様の文書のいずれかを提供する必要がある。	• 各使用目的に影響を与える各操作要因と、それらの使用目的に影響を与える可能性のある許容範囲を狭め、許容可能なエラー率（誤検出エラー率など）を低下させる追加の操作要因を定義して提供する。 • システム入力、使用、操作コンテキストの品質など、操作上の要因や使用目的を特定することは、展開された条件下でシステムを高い信頼性で安全に使用できるよう管理する上で重要である。 • 機密性の高い使用ケースを開示し、文書化する。 • 自動化バイアス（システムによって生成された出力に過度に依存する可能性のある傾向）を阻止するためのシステム設計における効果的な制御の実装の文書化。 • システムの制限、入力または出力データモデルの制限、または予測可能な障害（システムが設計または評価されていない用途を含め、使用目的に影響を与える可能性があるものなど）を文書化する。 • 推論操作（「ジェイルブレイク」）、モデル操作（例：データポイズニング）、推論情報漏えい（例：プロンプト抽出）などの、よく知られた AI リスクに対して実装された軽減策と制御を文書化する。 • システムの精度、パフォーマンス、これらの結果などがユースケース全体で一般化できる範囲の証拠。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション K：AI システム（続き）	
63	以下の場合、サプライヤーは、機密性の高い使用および使用目的などの透明性開示を更新し、Microsoft に通知する。 • 新しい使用が追加される • 機能の変更 • 製品が新規リリース段階へと進む • 使用目的に影響する信頼性と安全性能についての新たな情報がわかった、または当てはまった • システムの精度と性能に関する新たな情報が入手可能となる	サプライヤーは、透明性開示を更新するときに、このセクションで説明されているように Microsoft に通知する手順を含む計画を立てる。
64	透明性の開示の一環として、サプライヤーは、各 AI システムまたはデータモデルの標準操作手順と、以下を含むシステムヘルスモニタリングアクションプランを文書化する必要がある。 • トラブルシューティングおよび今後の不具合防止に対応するために、システム不具合を再現するプロセス • どの事象を監視するか • レビューのためにイベントの優先順位をつける方法 • 期待されるレビューの頻度 • 返答のためにイベントの優先順位をつける方法と解決のタイミング • オープンソースソフトウェアを含む、サードパーティの AI コンポーネントが最新版となっている	サプライヤーは、本セクションに記載の各 AI システムをフォローするシステムヘルスモニタリングポリシーおよび手順を文書化している。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
65	以下を含む、システムヘルスモニタリング方法の詳細なインベントリを設定し文書化する。 • データリポジトリ、システム分析、関連するアラートから生成されたデータと洞察など • 顧客が障害や懸念事項に関する情報を提出できるプロセス • 一般人がフィードバックを提出できるプロセス	サプライヤーは、本セクション記載の通り、システムヘルスモニタリング方法を文書化している。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

#	Microsoft のサプライヤー向けデータ保護要件	遵守の証拠
	セクション K：AI システム（続き）	
66	エビデンスにより AI システムが使用目的に適さないとわかった場合、システム使用の前でも最中であっても、サプライヤーはいつでも以下を行う。 • 顧客用資料からその使用目的を削除し、現在の顧客に問題を知らせ、わかっているギャップを埋める対応をするか、システムを廃止する • 使用目的に関する文書を修正する • 修正した文書を顧客向けに発行する	サプライヤーは、本セクションに記載の問題の使用目的をフォローするポリシーおよび手順を文書化している。
67	サプライヤーは、AI システムの使用目的、AI システムが展開される地理的地域、AI システム内に内在する偏見などに基づいて、サービス品質の低下または不利な経験をするリスクがある可能性のある、疎外されたグループを含むすべての既知の人口統計学的グループを特定し、開示する必要がある。 人口統計学的グループは以下を含む。 • 単一要素と定義されるグループ • 組み合わせ要素と定義されるグループ	サプライヤーは、以下の責任を負う、状況的要因やその他の操作上の要因（例：音声認識システムの「バックグラウンドノイズ」）などの正当な要因を特定し、文書化する必要がある。 • 特定の人口統計学的グループに対して、目標とする最低限の性能レベルを満たすことができない • 特定の人口統計学的グループ間で性能に差異がある サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。

用語集

「権限のある代表者」とは、会社を代表して署名することができる適切なレベルの権限を持った人物を意味します。同人物は、必要なプライバシーとセキュリティの知識を持っている、または SSPA プログラム対応を行う前に対象分野の専門家に相談することが想定されます。また、SSPA フォームに署名することにより、DPR を読み、理解していることを証明します。

「EUDPR」とは、EU の機関、団体、事務所、および代理による個人データの処理における自然人の保護、当該データの自由な転送、並びに規則（EC）No. 45/2001 および決定 No. 1247/2002/ECの 廃止に関する 2018 年 10 月 23 日の欧州議会および理事会の規則（EU）2018/1725 を意味します
。

「フリーランサー」とは、デジタルプラットフォームまたはその他の手段を通じて調達されるオンデマンドのタスクまたはサービスを行う個人を意味します。

「GDPR」とは、EU の機関、団体、事務所、および代理による個人データの処理における自然人の保護、当該データの自由な転送、並びに指令95/46/EC（一般データ保護規則）の廃止に関する 2016 年 4 月 27 日の欧州議会および理事会の規則（EU） 2016/679 を意味します。

「人間による監視」とは、サプライヤーの指定する分類となる人間による監視であり、使用目的に対して AI システムに不具合が検出された場合に利用できる介入の度合いを意味します。

- ヒューマン・イン・ザ・ループ（システムの各意思決定サイクルにおける人間の介入能力）
- ヒューマン・オン・ザ・ループ（システム設計サイクル中の人間の介入能力とシステム動作の監視)
- ヒューマン・イン・コマンド（AI システムの全体的な活動を監視し、特定の状況で AI システムをいつどのように使用するかを決定する能力）

「プライバシーデータ保護要件」とは、GDPR、EUDPR、地域の EU/EEA データ保護法、カリフォルニア州消費者プライバシー法、カリフォルニア州民法 § 1798.100 以降の条文（「*CCPA*」）、2018 年英国データ保護法および関連するまたはその後英国で適用される法律、規制、およびその他の法的要件、および（a）プライバシーとデータセキュリティ、または (b）個人データの使用、収集、保持、保管、セキュリティ、開示、転送、廃棄、およびその他の処理に関するその他の法的要件を意味します。

「EUモデル条項」および「標準契約条項」とは、（i）GDPR の第 46 条に記載され、2021 年 6 月 4 日欧州委員会の決定（EU）2021/914で承認されている適切なレベルのデータ保護を保証しない第三国で活動するプロセッサーへの個人データの転送に関する標準データ保護条項を意味し、
（ii）後継の標準契約条項は（a）欧州委員会によって採択された、（b）欧州データ保護監督官によって採択され、
欧州委員会によって承認された、（c）英国の一般連邦データ保護法に基づき英国によって採択された、（d）スイス連邦データ保護法に基づいてスイスによって採択された、または（e）スイス、英国、および同条項が個人データの国際転送を管理する欧州連合/欧州経済領域を構成する法域以外の政府によって採択されており、採択日時点で組み込まれ、サプライヤーに対して拘束力を持ちます。

「ウェブサイトホスティング」：ウェブサイトホスティングサービスは、Microsoft ドメインの下で Microsoft に代わってウェブサイトを作成および/または管理するオンラインのサービスです。サプライヤーは、サイトを作成および管理するために必要なすべての資料とサービスを提供し、インターネット上でアクセスできるように手配します。「ウェブホスティングサービスプロバイダー」または「ウェブホスト」とは、広告用の

Cookie やウェブビーコンなど、インターネット上で表示されるウェブサイトまたはウェブページに必要なツールとサービスを提供するサプライヤーを意味します。