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 の機密データを処理する 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。

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。

「**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、

またはその他の方法で処理された Microsoft の個人データまたは Microsoft の機密データの偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセス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 の個人データまたは Microsoft の機密データの取り扱いに関連するセキュリティの脆弱性を意味します。
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。

「**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、プレリリース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。

「**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、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（作業明細書、発注書など）。 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。 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：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。
3	本DPRの遵守に対する責任（レスポンシビリティ）および説明責任（アカウンタビリティ）を、社内の指定された個人またはグループに割り当てるものとする。	サプライヤーは、Microsoft のサプライヤー向け DPR への確実な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。 プライバシーおよび/またはセキュリティにおける役割を示す、同個人またはグループの権限と説明責任を説明する書類。

#	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）	
4	業務または Microsoft の機密データに関連してサプライヤーが処理する個人データにアクセスできる従業員向けに、プライバシーとセキュリティに関するトレーニングを毎年計画し、継続、実施するものとする。 会社に当該コンテンツが用意されていない場合は、このストーリーボードアウトラインを自身の組織に適合させ、トレーニングを実施するものとする。 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には、プライバシーとセキュリティの原則を含める。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。 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。
5	サプライヤーのプライバシーポリシーとセキュリティポリシーを遵守しない従業員には、適切な制裁を課すものとする。	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。
6	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を含め、Microsoft の文書化された指示に従ってのみMicrosoft の個人データを処理できる。そのような場合、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、プロセッサーまたはサブプロセッサー（サプライヤー）は処理以前に同法的要件をコントローラー（Microsoft）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	
7	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：処理活動のコントローラーである場合、自社のプライバシー通知を掲載する。	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。
8	ライブ音声通話または録音通話を通じて Microsoft の個人データを収集する場合、サプライヤーは、該当するデータの収集、取り扱い、使用、および保持の実行に関してデータ主体と話し合う準備をしておく必要がある。	音声録音のスクリプトには、Microsoft の個人データの処理方法、および次の方法を組み込む。 ▪ 収集方法 ▪ 使用方法、および ▪ 保管方法
	セクション C：選択と同意	
9	該当する場合、サプライヤーは、データ主体の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）	
10	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。 契約を締結している事業体から特に要求されない限り、サプライヤーは、1ES によって作成された標準バナーを使用して選択制御を管理する。 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。 注：Microsoft のビジネススポンサーは、Cookie のインベントリをカタログ化および管理するために、内部のウェブコンプライアンスポータル（http://aka.ms/wcp）において Microsoft ウェブサイトに登録することが要求される。	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	
11	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。
12	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。

13	サプライヤーが Microsoft から、仮名、NPI（s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	
14	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。
15	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。	
16	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）	
17	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。
18	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。

19	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。
20	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。
21	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）	
22	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。
23	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。
	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。	

24	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。 注：現在下請け業者と契約していないが、将来的に契約する可能性がある場合でも、本義務への同意を示すものとする。	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。
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	Microsoft が Microsoft の個人データのコントローラーである場合、下請け業者は、データ主体が定めた連絡先設定に従って Microsoft の個人データを使用していることを確実にする。	下請け業者による Microsoft のデータ主体設定の利用方法を示す。 下請け業者が設定変更を受け入れるための時間枠を含む証明書類（スクリーンショット、SLA、SOW など）を提供する。

#	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 G：下請け業者 （続き）	
27	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。
28	Microsoft の個人データの不正または違法な処理の兆候がないか、苦情を確認する。	サプライヤーは、下請け業者による Microsoft の個人データの不正使用または開示に関する苦情に対処するためのシステムとプロセスが実施されていることを実証することができる。 サプライヤーは、要求に応じて、Microsoft に証拠書類を提出する。
29	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。
30	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。
31	下請け業者による Microsoft の個人データおよび機密データの不正または違法な処理によって引き起こされた実際の被害または引き起こされる可能性がある潜在的な被害を軽減するための措置を迅速に講じるものとする。	サプライヤーは、計画と手順の証拠書類を保管し、要求に応じて Microsoft に証拠書類を提出する必要がある。

#	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 H：品質	
32	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	
33	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、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要求す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。 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。
34	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、データインシデントへの対応に必要な手順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。
35	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。

#	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	
	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36～52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 PH I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 の代替として許容される。この代替を適用する際は、SSPA に連絡する必要がある。 注：サプライヤーは同認証を提出する必要がある。
36	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。
37	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。
38	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 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）	
39	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、および ▪ 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て、再利用を防止する強力なパスワード制御 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

#	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	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。
41	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。
42	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。 ▪ 優先順位を通知するための重要度の割り当て（重要度の定義は文書化される） ▪ 緊急パッチを実装するための文書化された手順 ▪ 制作会社によるサポートが終了したオペレーティングシステムが使用されていないことの検証 ▪ 承認と例外を追跡するパッチ管理記録

#	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）	
43	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率、および ▪ （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に対して） ▪ 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	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）	
44	インシデント対応の調査結果を上級管理職および Microsoft に迅速に伝達する。	インシデント対応調査結果を Microsoft に報告するためのシステムとプロセスが確立されている。
45	システム管理者、運用スタッフ、管理を行う第三者、および Microsoft 個人データや機密データにアクセスする者はすべて、毎年セキュリティトレーニングを受ける必要がある。	次の項目を含むセキュリティ トレーニングプログラムを計画する。 ▪ 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 ▪ パスワードの安全確保、ログイン監視、悪意のあるソフトウェアのダウンロードに関するリスク、その他のセキュリティ関連のリマインダを含む、インシデント予防についての認識。 ▪ Microsoft の個人データが PHI である場合、認識とトレーニングプログラムにはセキュリティリマインダを含め、ログイン監視とパスワードの安全確保に対処する必要がある。 ▪ 定期的に更新する内容。
46	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。

#	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）	
47	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。
48	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。 権限の昇降（管理または他のタイプの拡張の特権）では、スマートカードや電話のオーセンティケーターなどの2つ目の要素を使用する必要がある。 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。
49	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	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。

	受信を拒否する必要がある。	

#	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）	
50	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 または他の業界で同等のディスク暗号化ソリューションに適合させる。

51	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 ▪ 医療プロファイルデータ（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（2fa、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）	

52	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。
53	サプライヤーは、開発プロセスのどの段階においても、シークレットコードがソフトウェアに埋め込まれたりハードコーディングされたりしないようにします。	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シークレットコードが、テスト環境と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ます。 サプライヤーは以下を実証できます。 ▪ GitHub Advanced Security (GHAS) などの資格情報の漏洩防止ツール、または同様のサービスまたはツールのサポートされている最新バージョンの使用。 ▪ ソースファイルまたは構成ファイルにシークレットコードが誤って含まれていた場合、それらのシークレットコードが検出時に取り消されたものとして文書化されたことを保証します。 ▪ 代替資格情報、または、二次資格情報がコードにプッシュバックされていないことを保証します。 ▪ 誤検知とその修復の文書化。

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。

「**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 et seq.（「*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で、
（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た、
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たものを意味します。

「**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。