ボリューム   
 ライセンス

マイクロソフト製品/サービス データ保護追加契約

最終更新日 2022 年 9 月 15 日

2022 年 9 月 15 日発行 (英語版)。翻訳版はマイクロソフトが入手でき次第発行します。当該確約事項は、2022 年 9 月 15 日をもってマイクロソフトに対して拘束力を持つものとします。

目次

[概要 3](#_Toc112504999)

[適用される DPA 条件とその更新 3](#_Toc112505000)

[電子通知 3](#_Toc112505001)

[旧バージョン 3](#_Toc112505002)

[定義 4](#_Toc112505003)

[一般条件 5](#_Toc112505004)

[法令遵守 5](#_Toc112505005)

[データ保護条件 5](#_Toc112505006)

[適用範囲 5](#_Toc112505007)

[データ処理の性質 (権利の帰属) 5](#_Toc112505008)

[処理対象データの開示 6](#_Toc112505009)

[個人データの処理 (GDPR) 7](#_Toc112505010)

[データ セキュリティ 8](#_Toc112505011)

[セキュリティ インシデントの通知 9](#_Toc112505012)

[データの移転と場所 10](#_Toc112505013)

[データの保持と削除 10](#_Toc112505014)

[処理者の守秘義務に関する確約事項 10](#_Toc112505015)

[下請処理者の使用に関する通知および規制 10](#_Toc112505016)

[教育機関 11](#_Toc112505017)

[CJIS 顧客契約 11](#_Toc112505018)

[HIPAA Business Associate 11](#_Toc112505019)

[カリフォルニア州消費者プライバシー保護法 (CCPA) 12](#_Toc112505020)

[生体認証データ 12](#_Toc112505021)

[追加プロフェッショナル サービス 12](#_Toc112505022)

[マイクロソフトへのお問い合わせ方法 12](#_Toc112505023)

[付属文書 A – セキュリティ対策 13](#_Toc112505024)

[付属文書 B – データ主体、および個人データの種類 16](#_Toc112505025)

[付属文書 C – 追加の安全措置契約 18](#_Toc112505026)

[別紙 1 - EU 一般データ保護規則条件 19](#_Toc112505027)

概要

両当事者は、本マイクロソフト製品/サービス データ保護追加契約 (以下「DPA」) が、本製品および本サービスに関連した顧客データ、プロフェッショナル サービス データ、および個人データの処理とセキュリティ対策に伴う両当事者の義務を定めたものであることに同意するものとします。DPA は、製品条項および他のマイクロソフトとの契約に含まれます。また、両当事者は、プロフェッショナル サービス契約が別途存在しない限り、プロフェッショナル サービス データの処理とセキュリティ対策にこの DPA が適用されることにも同意するものとします。お客様によるマイクロソフト以外の製品の使用については、異なるプライバシーおよびセキュリティ条件を規定した条項が別途適用されます。

DPA 条件とお客様のボリューム ライセンス契約の他の条項の間で矛盾が生じた場合は、DPA 条件が優先して適用されます。DPA 条件と、ここに定義されている顧客データ、プロフェッショナル サービス データ、または個人データの処理に適用されるマイクロソフト プライバシー ステートメントの条項の間で矛盾が生じた場合は、DPA 条件が優先します。

マイクロソフトは、ボリューム ライセンス契約のすべてのお客様に対し、本 DPA の確約事項を遂行します。当該確約事項は、(1) 本製品の任意のサブスクリプションまたはライセンスに適用される製品条項に関係なく、または、(2) 製品条項を参照する他の契約の存在に関係なく、マイクロソフトとお客様との関係性に対して拘束力を持つものとします。

適用される DPA 条件とその更新

**更新の制限**

お客様が本製品を更新するかもしくはその新しいサブスクリプションを購入する場合、またはプロフェッショナル サービスの個別契約を締結する場合、その時点で最新の DPA 条件が適用され、当該本製品のお客様のサブスクリプションの期間中または当該プロフェッショナル サービスの期間中は変更されません。お客様が本ソフトウェアの永続的ライセンスを取得している場合、その時点で最新の DPA 条件が適用され (お客様のボリューム ライセンスにおいて当該本ソフトウェアに対して適用されるその時点で最新の製品条項を決定するための規定と同じ規定に従います)、当該本ソフトウェアのお客様のライセンスの期間中は変更されません。

**新機能、追加物、または関連ソフトウェア**

上述の更新の制限にかかわらず、マイクロソフトが新しい (つまり、それまで本製品または本サービスに含まれていなかった) 機能、提供物、追加物、または関連ソフトウェアを導入する場合、マイクロソフトはお客様によるこれらの新機能、提供物、追加物、または関連ソフトウェアの使用に適用される条件を提供し、または DPA を更新する場合があります。これらの条項に DPA 条件に対する不利になる重大な変更が含まれる場合、マイクロソフトは、一般的に提供している本製品またはプロフェッショナル サービスの既存の機能を失うことなく、新しい機能、提供物、追加物、または関連ソフトウェアを使用する選択肢をお客様に提供します。お客様が新しい機能、提供物、追加物、または関連ソフトウェアをインストールまたは使用しない場合、対応する新しい条項はお客様には適用されません。

**政府機関の規制と要件**

上述の更新の制限にかかわらず、現在または将来、政府が課す要件または義務によって、(1) マイクロソフトが当該国または裁判管轄地における事業運営に一般的には適用されない規制や要求に服さなければならなくなる場合、(2) 変更を加えなければマイクロソフトによる本製品の運営またはプロフェッショナル サービスの提供の継続が困難になる場合、または (3) DPA 条件または本製品またはプロフェッショナル サービスがそうした要件または義務に抵触するおそれがあるとマイクロソフトが考える場合には、マイクロソフトは、当該国または裁判管轄地において本製品またはプロフェッショナル サービスを変更または終了することができます。

電子通知

マイクロソフトは、電子メール、オンライン サービスのポータル、またはマイクロソフトが指定する Web サイトを含め、本製品および本サービスに関する情報および通知を電子的にお客様に提供する場合があります。通知は、マイクロソフトが提供した日付をもって行われたと見なします。

旧バージョン

DPA 条件は、現在利用可能な本製品および本サービスの条件を規定するものです。以前のバージョンの DPA 条件については、<https://aka.ms/licensingdocs> を参照するか、リセラーまたは当社担当者にお問い合わせください。

[目次](#TableofContents) / [標準の条件](#GeneralTerms)

定義

本 DPA で使用されている用語のうち定義のないものについては、すべてボリューム ライセンス契約における定義が適用されます。本 DPA においては、以下の用語の定義が使用されます。

「顧客データ」とは、お客様によるオンライン サービスの利用を通じて、お客様またはお客様の代理人によってマイクロソフトに提供される、すべてのテキスト、音声、ビデオ、または画像ファイルおよびソフトウェアを含むすべてのデータをいいます。顧客データにプロフェッショナル サービス データは含まれません。

「データ保護要件」とは、(a) プライバシーとデータ セキュリティ、および (b) 個人データの使用、収集、保存、格納、セキュリティ、開示、移管、破棄、およびその他の処理に関連した GDPR、地域の EU/EEA データ保護法、適用される法令、規制、およびその他の法的要件を意味します。

「DPA 条件」とは、本 DPA に記載されている条件と、特定の本製品 (または本製品の機能) に関して DPA のプライバシーおよびセキュリティの条件を特に補足または変更する、製品条項における本製品固有の条件を意味します。DPA とかかる本製品固有の条件の間で矛盾が生じた場合は、該当する本製品 (またはその本製品の機能) については本製品固有の条件が優先して適用されるものとします。

「GDPR」とは、個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日付け欧州議会および理事会の 2016 年 679 番 EU 規則と廃止予定の 1995 年 46 番 EC 指令 (一般データ保護規則) を意味します。

「地域の EU/EEA データ保護法」とは、GDPR を実施する下位の法令を意味します。

「GDPR 条件」とは、GDPR の第 28 条で義務付けられている個人データの処理に関してマイクロソフトが法的拘束力のある約定を結ぶ、[別紙 1](#Attachment1) に記載の条件をいいます。

「個人データ」とは、識別されたまたは識別可能な自然人に関するすべての情報を意味します。識別可能な自然人とは、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、またはかかる自然人の身体的、生理的、遺伝的、精神的、経済的、文化的もしくは社会的なアイデンティティに固有の要素を 1 つ以上参照することによって、直接または間接的に識別することができる者をいいます。

「本製品」は、ボリューム ライセンス契約に記載されている意味を有します。参照の便宜のために記載すると、「本製品」には、それぞれボリューム ライセンス契約に定義されている、オンライン サービスおよび本ソフトウェアが含まれます。

「本製品および本サービス」とは、本製品およびプロフェッショナル サービスを意味します。本製品およびプロフェッショナル サービスの提供状況は地域により異なる場合があり、本 DPA が特定の本製品およびプロフェッショナル サービスに適用されるか否かについては、本 DPA の「適用範囲」項に規定する制限事項が適用されます。

「プロフェッショナル サービス」とは、次のサービスを意味します。(a) 本 DPA に含まれるマイクロソフト エンタープライズ サービス個別契約またはクラウド従業員管理促進契約に基づいて提供される、計画、アドバイス、ガイダンス、データ移行、展開およびソリューション/ソフトウェア開発サービスを含む、マイクロソフトのコンサルティング サービス、ならびに (b) 顧客が本製品に影響が及ぶ問題を特定し解決することを支援するために、マイクロソフトが提供する技術サポート (サービス コンサルティングおよびサポート規定書またはサービス規定書にそれぞれ規定されるマイクロソフト ユニファイド サポートまたはプレミア サポート サービスの一環として提供される技術サポートを含む)、およびその他の商業技術サポート サービス。プロフェッショナル サービスには、本製品は含まれず、本 DPA においては追加プロフェッショナル サービスも含まれません。

「プロフェッショナル サービス データ」とは、プロフェッショナル サービスを取得するためのマイクロソフトとの契約を通じて、お客様もしくはお客様の代理人によってマイクロソフトに提供される (またはお客様がマイクロソフトに本製品からの取得を許可する)、またはマイクロソフトもしくはマイクロソフトの代理人によって取得もしくは処理される、すべてのテキスト、音声、ビデオ、画像ファイル、またはソフトウェアを含むすべてのデータを意味します。

「2021 年標準契約条項」とは、GDPR 第 46 条に記載され、2021 年 6 月 4 日付の欧州委員会決議 2021/914/EC によって承認された、EEA 内の処理者から適切なレベルのデータ保護を保証しない第三国に設立された処理者への個人データの移転のための、Microsoft Ireland Operations Limited と Microsoft Corporation との間の標準データ保護条項 (処理者から処理者への移転モジュール) を意味します。

「下請処理者」とは、GDPR の第 28 条に規定されている、顧客データ、プロフェッショナル サービス データ、および個人データを処理するためにマイクロソフトが使用する他の処理者をいいます。

「追加プロフェッショナル サービス」とは、サポートから本製品のエンジニアリング チームにエスカレーションされるサポート リクエストであり、プロフェッショナル サービスの定義に含まれていない本製品またはボリューム ライセンス契約に関連して提供される、マイクロソフトからの解決ならびにその他のコンサルティングおよびサポートを求めるものを意味します。

「個人データの侵害」、「処理」、「管理者」、「処理者」、「プロファイリング」、「個人データ」、「データ主体」など、本 DPA で使用されている用語のうち定義のないものについては、GDPR が適用されるかどうかにかかわらず、GDPR 第 4 条における定義が適用されます。

[目次](#TableofContents) / [標準の条件](#GeneralTerms)

一般条件

法令遵守

マイクロソフトは、マイクロソフトによる本製品および本サービスの提供に適用されるすべての法令 (セキュリティ侵害通知法とデータ保護要件を含みます) を遵守します。ただし、マイクロソフトは、お客様またはお客様の業種に適用される法令であっても、情報技術サービス業者に一般的に適用されるものではない法令を遵守する責任を負いません。特定の法令または規制の適用対象となる情報が顧客のデータに含まれるかどうかを決定するのは当社ではありません。すべてのセキュリティ インシデントには、以下の「セキュリティ インシデントの通知」の条件が適用されます。

お客様は、生体認証データ、通信の秘密保持、およびデータ保護要件に関連する法令を含む、お客様による本製品および本サービスの使用に適用されるすべての法令を遵守する必要があります。特定の法令または規制の適用対象となる情報の保存および処理に本製品および本サービスが適しているかどうかを決定すること、およびお客様の法令上および規制上の義務に一致した方法で本製品および本サービスを利用することについては、お客様が責任を負うものとします。お客様は、デジタル ミレニアム著作権法またはその他の適用法令に基づくコンテンツの削除要請など、お客様による製品およびサービスの使用に関する第三者からの要求に対応する責任を負います。

データ保護条件

本 DPA のこの条は、次の項で構成されています。

* 適用範囲
* データ処理の性質 (権利の帰属)
* 処理対象データの開示
* 個人データの処理 (GDPR)
* データ セキュリティ
* セキュリティ インシデントの通知
* データの移転と場所
* データの保持と削除
* 処理者の守秘義務に関する確約事項
* 下請処理者の使用に関する通知および規制
* 教育機関
* CJIS 顧客契約
* HIPAA Business Associate
* カリフォルニア州消費者プライバシー保護法 (CCPA)
* 生体認証データ
* 追加プロフェッショナル サービス
* マイクロソフトへのお問い合わせ方法
* 付属文書 A – セキュリティ対策
* 付属文書 B – データ主体、および個人データの種類
* 付属文書 C – 追加の安全措置契約

適用範囲

DPA 条件は、本条項に規定されている場合を除き、すべての本製品および本サービスに適用されます。

DPA 条件は、製品条項で除外対象として特定されている本製品または除外対象として特定されている範囲には適用されません。除外される本製品および範囲には、該当する本製品固有の条件で参照されているプライバシーおよびセキュリティ条件が適用されます。

なお、DPA 条件は、マイクロソフトおよびマイクロソフトの下請処理者が管理している環境におけるデータの処理にのみ適用されます。これには、本製品および本サービスによりマイクロソフトに送信されるデータが含まれますが、お客様の施設またはお客様が選択した第三者の運用環境に残っているデータは含まれません。

マイクロソフトは、追加プロフェッショナル サービスに関して、以下の「追加プロフェッショナル サービス」項に定める確約事項のみを遂行します。

プレビュー版で採用されるプライバシーおよびセキュリティ対策は、本製品および本サービスで通常使用される対策よりも少ない、またはそれらの対策とは異なる場合があります。別途規定する場合を除き、お客様は、個人データまたは法令遵守要件が適用されるその他のデータを処理するためにプレビュー版を使用することはできません。本製品について、プレビュー版には本 DPA の「個人データの処理」、「データ セキュリティ」、および「HIPAA Business Associate」の条件は適用されません。プロフェッショナル サービスについて、プレビュー版または限定リリース版として指定されている提供物は、追加プロフェッショナル サービスの条件のみを満たします。

データ処理の性質 (権利の帰属)

マイクロソフトは、以下に規定された制限事項に従って、(a) 文書化されたお客様の指示に基づき、お客様に本製品および本サービスを提供するため、ならびに (b) 本製品および本サービスのお客様への提供に付随する事業運営のためにのみ、顧客データ、プロフェッショナル サービス データ、および個人データを使用し、その他の方法で処理します。両当事者の間においては、お客様が顧客データおよびプロフェッショナル サービス データのすべての権利、権原および権益を留保します。マイクロソフトは、本条でお客様がマイクロソフトに付与する権利を除き、顧客データまたはプロフェッショナル サービス データに関するいかなる権利も取得しません。本項は、マイクロソフトがお客様にライセンスするソフトウェアまたはサービスに対するマイクロソフトの権利には影響しません。

**お客様に本製品および本サービスを提供するための処理**

本 DPA において、本製品の「提供」は以下の要素で構成されます。

* お客様とそのユーザーによってライセンス取得、設定、および使用される機能の提供 (パーソナライズされたユーザー エクスペリエンスの提供を含む)
* トラブルシューティング (問題の防止、検出、および修正)
* 製品の最新状態とパフォーマンスの維持、ならびにユーザーの生産性、信頼性、有効性、品質、およびセキュリティの向上。

本 DPA において、プロフェッショナル サービスの「提供」は以下の要素で構成されます。

* プロフェッショナル サービスの提供 (技術サポート、プロフェッショナル プランニング、アドバイス、ガイダンス、データ移行、導入、およびソリューション/ソフトウェア開発の各サービスの提供を含む)。
* トラブルシューティング (プロフェッショナル サービスの提供中にプロフェッショナル サービスまたは関連する本製品において特定されたセキュリティ インシデントおよび問題を含む、問題の防止、検出、調査、緩和、および修正)。
* プロフェッショナル サービスの提供中に特定された問題に基づく、ソフトウェアの瑕疵の修正の他に製品およびサービスの最新状態とパフォーマンスの維持を含む、プロフェッショナル サービスおよび基となる本製品の提供、有効性、品質、およびセキュリティの向上。

いずれの場合も、製品およびサービスの提供はデータ保護要件に基づくセキュリティ義務を考慮して実施するものとします。

マイクロソフトは、本製品および本サービスを提供するときに、次の目的のために顧客データ、プロフェッショナル サービス データ、または個人データを使用したり、またはその他の方法で処理したりしません。(a) ユーザー プロファイリング、(b) 広告目的もしくは同様の商用目的、または (c) 新しい機能、サービス、もしくは製品の作成、あるいはそれ以外の目的での市場調査。ただし、かかる使用または処理が、文書化されたお客様の指示に従っている場合を除きます。

**お客様に本製品および本サービスを提供することに付随する事業運営のための処理**

本 DPA において、「事業運営」とは、本条項でお客様が許可する事業運営を意味します。

お客様はマイクロソフトに以下を許可します。

1. 仮名化された識別子を含むデータから集計された統計的な個人情報以外のデータを作成すること (一意の仮名化された識別子を含む使用ログなど)
2. 顧客データまたはプロフェッショナル サービス データに関連する統計を算出すること

いずれの場合も、顧客データまたはプロフェッショナル サービス データの内容にアクセスしたり分析することなく、お客様に本製品および本サービスを提供することに不随し、以下の目的を達成することに限定されます。

目的は以下のとおりです。

* 課金およびアカウント管理
* 従業員のコミッションとパートナーのインセンティブの計算などの報酬支払
* 予測、収益、キャパシティ プランニング、製品戦略など、社内向け報告やビジネス モデリング
* 財務報告

マイクロソフトは、顧客データ、プロフェッショナル サービス データ、または個人データをこれらの事業運営のために処理するときに、データ最小化の原則を適用するものとし、それらのデータを次の目的で使用したり、またはその他の方法で処理したりしません。(a) ユーザー プロファイリング。(b) 広告目的または同様の商用目的。(c) または本条項に記載されている目的以外のその他の目的。また、本 DPA に基づくすべての処理と同様、事業運営の処理には引き続き、処理対象データの開示に基づくマイクロソフトの秘密保持義務および確約事項が適用されます。

処理対象データの開示

次の場合を除き、マイクロソフトが処理対象データを開示する、またはかかるデータへのアクセスを可能にすることはありません。(1) お客様が指示した場合、(2) 本 DPA に規定されている場合、または (3) 法令により求められる場合。本条項において、「処理対象データ」とは次の意味を有するものとします。(a) 顧客データ。(b) プロフェッショナル サービス データ。(c) 個人データ。(d) 本製品および本サービスに関連してマイクロソフトによって処理され、ボリューム ライセンス契約に基づくお客様の秘密情報であるその他のデータ。処理対象データのあらゆる処理に、ボリューム ライセンス契約に基づくマイクロソフト秘密保持義務が適用されます。

法令により義務付けられている場合を除き、マイクロソフトが処理対象データを法執行機関に開示する、またはかかるデータへのアクセスを可能にすることはありません。法執行機関から処理対象データを要求された場合、マイクロソフトは、法執行機関にお客様に連絡させ、そのデータを直接要求させるよう努めます。処理対象データを法執行機関に開示する、またはかかるデータへのアクセスを可能にせざるを得ない場合、マイクロソフトは、かかる行為が法令により禁止されている場合を除き、直ちにお客様に通知し、かかる要求の写しを提供します。

マイクロソフトは、法律および慣行が基本的権利および自由の本質を尊重し、GDPR の第 23 条 (1) 項に記載されるいずれかの目的を保護するために、該当する場合は、民主社会で必要かつ相応の範囲を超えないことを条件に、法令により求められる処理対象データの開示またはかかるデータへのアクセスのみを可能にします。他の第三者から処理対象データに関する要求を受け取った場合、マイクロソフトは、法令により禁止されている場合を除き、速やかにお客様に通知します。法令により遵守が義務付けられている場合を除き、当社はかかる要求を拒否します。当該要求が有効である場合であっても、マイクロソフトは第三者に、データをお客様に直接請求させるよう努めます。

マイクロソフトは第三者に対し、(a) 処理対象データへの直接的、間接的、全面的または無制限のアクセス、(b) 処理対象データを保護するためのプラットフォーム暗号化キーもしくは当該暗号化を解除する能力、または (c) 処理対象データが第三者の要求に指定された以外の目的に使用されることをマイクロソフトが知っている場合における当該データへのアクセス、のいずれも提供しません。

上記の一環として、マイクロソフトがお客様の基本的な連絡先情報を当該第三者に提供する場合があります。

個人データの処理 (GDPR)

本製品および本サービスの提供に関連してマイクロソフトが処理するすべての個人データは、(a) 顧客データ、(b) プロフェッショナル サービス データ、または (c) マイクロソフトが生成、導出もしくは収集するデータ (お客様によるサービスベースの機能の使用に起因してマイクロソフトに送信されるデータ、ローカルでインストールされているソフトウェアからマイクロソフトが取得するデータを含む) のいずれかの一部として取得されます。オンライン サービスの使用を通じて、お客様から、またはお客様の代理でマイクロソフトに提供された個人データも顧客データに含まれます。プロフェッショナル サービスの使用を通じて、お客様から、またはお客様の代理でマイクロソフトに提供された個人データもプロフェッショナル サービス データに含まれます。仮名化された識別子が本製品の提供に関連してマイクロソフトが処理するデータに含まれる場合がありますが、これも個人データとなります。仮名化された個人データ、個人の特定が不可能だが匿名化されていない個人データ、または個人データから取得された個人データもすべて、個人データに該当します。

マイクロソフトが GDPR が適用される個人データの処理者または下請処理者である限り、その処理に対して[別紙 1](#Attachment1) の GDPR 条件が適用されます。また、両当事者も、本項 (「個人データの処理 (GDPR)」) の以下の条件に同意するものとします。

**処理者と管理者の役割および責任**

お客様とマイクロソフトは、お客様が個人データの管理者であり、マイクロソフトが当該データの処理者であることに同意するものとします。ただし、(a) お客様が個人データの処理者となり、マイクロソフトが下請処理者となる場合、または (b) 本 DPA の本製品固有の条件において別途記載のある場合を除きます。マイクロソフトが個人データの処理者または下請処理者の役割を果たす場合、マイクロソフトは、お客様からの文書化された指示に従ってのみ、個人データを処理します。お客様は、お客様のボリューム ライセンス契約 (DPA 条件および該当する更新を含む) に加え、製品ドキュメント、ならびにお客様による本製品の機能の使用と設定が、個人データの処理について文書化された、マイクロソフトに対する完全かつ最終的なお客様の指示、またはプロフェッショナル サービス ドキュメントおよびお客様によるプロフェッショナル サービスの使用を構成することに同意するものとします。本製品の使用と設定に関する情報は、<https://docs.microsoft.com> (もしくは後継の場所) または本 DPA に含まれる他の契約に記載されています。追加または代替の指示については、お客様の契約の変更プロセスに従って合意された場合にのみ有効となります。GDPR が適用され、また、お客様が処理者である場合、お客様は、処理者または下請処理者としてマイクロソフトを任命することを含め、お客様の指示が該当管理者によって承認されていることをマイクロソフトに対して保証するものとします。

マイクロソフトは、本製品および本サービスのお客様への提供に付随する事業運営のために GDPR が適用される個人データを使用または処理する範囲で、かかる使用のために GDPR に基づく独立したデータ管理者の義務を遵守する責任を負います。マイクロソフトは、以下を行う処理のために GDPR に基づく追加されたデータ「管理者」の責任を受け入れます。(a) GDPR で義務付けられている範囲で、規制要件に従って行動すること、および(b) お客様に対する透明性を高め、かかる処理に対するマイクロソフトの説明責任を確認すること。マイクロソフトは、本 DPA で特定されているものおよび GDPR の第 6 条 (4) で検討されているものを含め、処理中の顧客データ、プロフェッショナル サービス データ、および個人データを保護するためのセキュリティ対策を採用しています。本項による個人データの処理に関して、マイクロソフトは、「追加の安全措置」項に定められる確約事項を遂行します。その目的において、(i) 事業運営に関連して移転された、「追加の安全措置」項に記載される個人データのマイクロソフトによる開示は、「関連する開示」と見なされ、(ii) 「追加の安全措置」項に定められる確約事項はかかる個人データに適用されます。

**処理の詳細**

両当事者は以下について確認し、同意するものとします。

* **対象事項。**処理の対象事項は、本 DPA の前出の「データ処理の性質 (権利の帰属)」項および GDPR の範囲内の個人データに限定されます。
* **処理の期間。**処理の期間は、お客様の指示および本 DPA の条件に従うものとします。
* **処理の性質と目的。**処理の性質と目的は、お客様のボリューム ライセンス契約に従って、本製品および本サービスのお客様への提供に付随する事業運営のために本製品および本サービスを提供することです (本 DPA の前出の「データ処理の性質 (権利の帰属)」項で詳しく説明)。
* **データの種類。**本製品および本サービスを提供する際にマイクロソフトが処理する個人データの種類には、次のものが含まれます。(i) お客様が顧客データおよびプロフェッショナル サービス データに含めることを選択する個人データ、ならびに (ii) GDPR の第 4 条に明記されている個人データであって、マイクロソフトが生成、導出もしくは収集する場合があるデータ (お客様によるサービスベースの機能の使用に起因してマイクロソフトに送信されるデータ、ローカルでインストールされているソフトウェアからマイクロソフトが取得するデータを含む)。お客様が顧客データおよびプロフェッショナル サービス データに含めることを選択する個人データの種類は、お客様が GDPR の第 30 条に従って管理者として保持するレコードで特定されている任意の種類の個人データに該当します。これには、付属文書 B で定められている個人データの種類が含まれます。
* **データ主体。**データ主体の種類は、お客様の代表者とエンド ユーザー (従業員、請負業者、協力者、顧客など) に該当し、お客様が GDPR の第 30 条に従って管理者として保持するレコードで特定されているその他の種類のデータを含む場合があります。これには、付属文書 B で定められているデータ主体の種類が含まれます。

**データ主体の権利 (要求による支援)**

マイクロソフトは、本製品および本サービスの機能および処理者としてのマイクロソフトの役割に従った方法で、お客様に対してデータ主体の個人データを提供し、GDPR に基づくデータ主体の権利の行使要求にお客様が対応できるようにします。マイクロソフトは、当社がデータ処理者または下請処理者となっている本製品および本サービスに関連し、GDPR に基づいて 1 つ以上の権利の行使要求をデータ主体から受けた場合、お客様に直接要求するようにデータ主体に案内します。当該要求に対してはお客様が責任をもって対応してください (必要に応じて、本製品および本サービスの機能を使用して対応してください)。マイクロソフトは、かかるデータ主体による要求への対応についてお客様を支援するため、お客様の合理的な要求に応じるものとします。

**処理活動の記録**

マイクロソフトがお客様に関連した特定の情報の記録を収集および維持することが GDPR で義務付けられている限りにおいて、お客様は、当該情報を要求に応じてマイクロソフトに提供し、正確かつ最新の状態に保つものとします。マイクロソフトは、GDPR の要求に応じて、当該情報を監督当局に提供する場合があります。

データ セキュリティ

**セキュリティ規定およびポリシー**

マイクロソフトは、送信、保存、またはその他の方法で処理された個人データの偶発的または違法な破壊、損失、変更、不正開示、またはアクセスから顧客データ、プロフェッショナル サービス データ、および個人データを保護するために、適切な技術的および組織的対策を講じ、維持します。これらの対策は、マイクロソフト セキュリティ ポリシーに規定するものとします。マイクロソフトは、当該セキュリティ ポリシーを、当社のセキュリティ規定およびポリシーに関してお客様が合理的に要求した他の情報とともにお客様に提供します。

また、該当する対策は、ISO 27001、ISO 27002、および ISO 27018 に規定される要件を満たすものとします。これらの要件に対するセキュリティ管理手段の内容は、お客様に提供します。

各コア オンライン サービスも、製品条項の表に示す管理標準規格または枠組みを満たすものとします。各コア オンライン サービスおよびプロフェッショナル サービスは、顧客データおよびプロフェッショナル サービス データの保護のために付属文書 A に規定されるセキュリティ対策を導入して維持するものとします。

マイクロソフトは随時、業界または政府の標準規格を追加することができます。マイクロソフトは、ISO 27001、ISO 27002、ISO 27018、または製品条項のコア オンライン サービスの表に示す標準規格または枠組みが業界で使用されなくなり、後継の標準規格 (存在する場合) への置き換えが行われた場合を除き、これらを撤廃することはありません。

**データの暗号化**

お客様とマイクロソフトとの間、またはマイクロソフトのデータ センターとの間でパブリック ネットワークを介して伝送される顧客データおよびプロフェッショナル サービス データ (それぞれ、その中の個人データを含む) は、既定で暗号化されます。

マイクロソフトは、オンライン サービスで保存された顧客データおよび保存されたプロフェッショナル サービス データも暗号化します。お客様またはお客様のために行動する第三者がアプリケーション (特定の Azure サービスなど) を構築する可能性があるオンライン サービスの場合、マイクロソフトが提供する機能またはお客様が第三者から取得した機能を使用して、お客様の裁量により、かかるアプリケーションに保存されたデータの暗号化を採用することができます。

**データ アクセス**

マイクロソフトは、顧客データおよびプロフェッショナル サービス データ (その中の個人データを含む) へのアクセスを制御する、最小限の権限アクセス メカニズムを採用しています。サービスの運用に必要な顧客データおよびプロフェッショナル サービス データへのアクセスが、適切な目的で行われ、監視の下で承認されるように、役割ベースのアクセス制御が採用されています。コア オンライン サービスおよびプロフェッショナル サービスに関し、マイクロソフトは、付属文書 A の「セキュリティ対策」という表に記載されているアクセス制御メカニズムを維持しています。マイクロソフト担当者による顧客データへの常時アクセスは行っておらず、限られた時間に必要なアクセスを行います。

**お客様の責任**

本製品および本サービスの技術的および組織的な対策がお客様の要件 (適用されるデータ保護要件に基づくお客様のセキュリティ義務を含む) を満たしているかどうかに関し、お客様は、自身の責任において独自に判断する必要があります。お客様は、技術水準、導入コスト、お客様の個人データの処理の性質、範囲、背景、目的、および個人へのリスクを考慮に入れながら、マイクロソフトが導入および維持しているセキュリティ規定およびポリシーが、お客様の個人データに関するリスクに対して十分な安全性を保証していることを確認し、同意するものとします。お客様は、お客様が提供または管理するコンポーネント (Microsoft Intune に登録されたデバイス、または Microsoft Azure のお客様の仮想マシンもしくはアプリケーション内に登録されたデバイスなど) に対してプライバシー保護およびセキュリティ対策を実施し維持することについて責任を負います。

**監査コンプライアンス**

マイクロソフトは、顧客データ、プロフェッショナル サービス データ、および個人データの処理に使用されるコンピューター、コンピューティング環境および物理的なデータ センターのセキュリティの監査を以下のように実施します。

* 標準規格または枠組みにおいて監査の実施が規定されている場合、かかる管理標準規格または枠組みに関する監査は、少なくとも年 1 回実施されるものとします。
* 各監査は、適用される各管理標準規格または枠組みについて、規制機関または認定機関の標準および規則に従って実施されるものとします。
* 各監査は、当社が選択した適格の独立した第三者のセキュリティ監査人によって、当社の費用負担により実施されるものとします。

実施される監査ごとに、監査レポート (以下「マイクロソフト監査レポート」) が作成されます。この監査レポートは、<https://servicetrust.microsoft.com/> またはマイクロソフトが指定した場所に提供されます。マイクロソフト監査レポートは、マイクロソフトの秘密情報であり、監査人によって重要な知見が見つかった場合は明確に開示されます。マイクロソフトは、マイクロソフト監査レポートで提起された問題を、監査人が満足するように速やかに修正するものとします。お客様から要求があった場合、マイクロソフトは各マイクロソフト監査レポートをお客様に提供します。マイクロソフト監査レポートには、マイクロソフトおよび監査人の非開示および頒布に関する制限が適用されます。

データ保護要件に基づくお客様の監査要件を、マイクロソフトがお客様に一般的に提供している監査レポート、ドキュメント、または遵守状況情報によって合理的に満たすことができない場合、マイクロソフトはお客様の追加の監査指示に迅速に対応します。監査を開始する前に、お客様とマイクロソフトは、監査の範囲、タイミング、期間、管理および証拠の要件、ならびに料金に相互に同意するものとします。ただし、この同意の要件によって、マイクロソフトが監査の実施を不当に遅らせることが許可されるわけではありません。監査の実施に必要な範囲内において、マイクロソフトは、マイクロソフト、その関連会社、およびその下請処理者による顧客データ、プロフェッショナル サービス データ、および個人データの処理にとって適切な処理システム、施設、およびサポート ドキュメントを提供するものとします。このような監査は、独立した第三者組織である認定済みの監査会社によって、通常の営業時間中に、マイクロソフトへの合理的な事前通知を行ったうえで、合理的な秘密保持手順に従って行われます。お客様と監査会社のいずれも、マイクロソフトの他の顧客データにアクセスしたり、該当する本製品および本サービスの提供に関与していないマイクロソフトのシステムまたは施設にアクセスしたりすることはできません。お客様は、マイクロソフトが実施するサービスの料金に加えて、マイクロソフトが当該監査に費やしたすべての妥当な費用と料金を含む、当該監査に関連したすべての費用と料金に対して責任を負います。お客様の監査の結果として生成された監査レポートに重大な不遵守の所見が含まれている場合、お客様は当該監査レポートをマイクロソフトと共有し、マイクロソフトは重大な不遵守をすみやかに是正するものとします。

DPA の本条項のいずれの規定も、GDPR 条件を変更するものではなく、また、データ保護要件に基づく監督当局の権利またはデータ主体の権利に影響を及ぼすものでもありません。Microsoft Corporation は、本条項の第三者受益者です。

セキュリティ インシデントの通知

マイクロソフトは、顧客データ、プロフェッショナル サービス データ、または個人データを処理している間にデータの偶発的な破壊または不正な破壊、紛失、改変、不正開示または不正アクセスにつながるようなセキュリティ違反 (それぞれ、「セキュリティ インシデント」といいます) に気付いた場合、速やかに、(1) セキュリティ インシデントについてお客様に通知し、(2) セキュリティ インシデントを調査して、セキュリティ インシデントについての詳細情報をお客様に提供し、(3) セキュリティ インシデントにより生じる損害を最小限に抑えるための合理的な手段を講じます。

セキュリティ インシデントの通知は、電子メールその他のマイクロソフトが選択した手段によって、お客様に提供されるものとします。お客様がマイクロソフトに対し、それぞれの該当する本製品およびプロフェッショナル サービスに関する正確な連絡先情報を維持することについては、お客様が単独で責任を負うものとします。お客様は、お客様に適用されるインシデント通知法の下、その義務を全うし、セキュリティ インシデントに関する通知を第三者に通知するものとします。

マイクロソフトは、GDPR 第 33 条または他の適用法令に基づく、当該セキュリティ インシデントについて関連する監督当局およびデータ主体に通知するという義務をお客様が履行できるよう支援するため、合理的な努力を払うものとします。

本条項に基づくセキュリティ インシデントの通知または対応に関するマイクロソフトの義務は、セキュリティ インシデントに関する過失または賠償責任をマイクロソフトが認めたものではありません。

お客様のアカウントまたは認証資格情報が悪用された可能性がある場合、または本製品および本サービスに関連するセキュリティ インシデントが発生した場合には、お客様は速やかにマイクロソフトにその旨を通知しなければなりません。

データの移転と場所

**データ移転**

DPA 条件および以下に規定されている予防措置に従っている場合を除き、マイクロソフトがお客様のために処理する顧客データ、プロフェッショナル サービス データ、および個人データは、地理的場所に移転され、そこで保存および処理することはできません。DPA 条件に別途規定されている場合を除き、お客様はかかる予防措置を考慮して、マイクロソフトまたはその下請処理者が営業を展開する米国またはその他の国に顧客データ、プロフェッショナル サービス データ、および個人データを移転し、その国内でお客様のデータおよび個人データを保存および処理して本製品を提供するためにマイクロソフトを任命するものとします。

本製品および本サービスの提供を目的とした、欧州連合、欧州経済地域、英国、およびスイスからの顧客データ、プロフェッショナル サービス データ、および個人データの移転にはすべて、マイクロソフトが履行する2021 年標準契約条項が適用されます。また、英国からの移転には、マイクロソフトが施行する IDTA が適用されます。本 DPA において、「IDTA」とは、2018 年英国データ保護法の S119A(1) に基づき英国プライバシー監視機関が発行した欧州委員会の国際データ移転に関する標準契約条項への国際データ移転補遺を意味します。マイクロソフトは、欧州経済地域、英国、およびスイスからの個人データの収集、使用、移転、保存、およびその他の処理に関して、欧州経済地域、英国、およびスイスのデータ保護法令の要件に従います。第三国または国際組織への個人データの移転にはすべて、GDPR 第 46 条に定める適切な安全措置を適用し、かかる移転および安全措置について GDPR 第 30 条 (2) 項に従って文書化するものとします。

また、マイクロソフトは、EU - 米国間およびスイス - 米国間のプライバシー シールド フレームワークおよびこのフレームワークが課す確約事項について認定を受けました。ただし、マイクロソフトは、Case C-311/18 の欧州司法裁判所の裁定を踏まえ、個人データの域外移転の法的根拠として EU - 米国間プライバシー シールド フレームワークには依拠しません。マイクロソフトは、プライバシー シールドの原則が求めるものと同等の保護を提供する自らの義務を満たせなくなったと判断した場合にお客様に通知することに同意します。

**顧客データの保存場所**

コア オンライン サービスに関し、マイクロソフトは、製品条項で定められているように、顧客データを一定の地域 (以下それぞれを「地域」といいます) 内に保存します。

マイクロソフトは、お客様またはお客様のエンド ユーザーが顧客データにアクセスし、または顧客データを移転する元の地域を制御または制限しません。

データの保持と削除

お客様は、お客様のサブスクリプションまたは該当するプロフェッショナル サービス契約の期間中はいつでも、各オンライン サービスに保存されている顧客データ、およびプロフェッショナル サービス データにアクセスし、抽出し、削除することができます。

無料試用版および LinkedIn サービスを除き、マイクロソフトは、お客様のサブスクリプションの満了または終了後 90 日間、オンライン サービスに保存されている顧客データを機能が限定されたアカウントに保持し、お客様がデータを抽出できるようにします。90 日の保持期間が終了した後、マイクロソフトは、さらなる 90 日以内にお客様のアカウントを無効にし、オンライン サービスに保存されている顧客データおよび個人データを削除するものとします。ただし、当該データを保持することが本 DPA に基づいて許可されている場合を除きます。

マイクロソフトは、データが収集もしくは移転された事業目的を達成した後、またはお客様から要求があった場合、本ソフトウェアに関連する個人データおよびプロフェッショナル サービス データのコピーをすべて削除します。ただし、当該データを保持することが本 DPA に基づいて許可されている場合を除きます。

オンライン サービスは、お客様が提供したソフトウェアの保持または抽出をサポートしない場合があります。本条項の規定に従った顧客データ、プロフェッショナル サービス データ、または個人データの削除について、マイクロソフトはいかなる責任も負いません。

処理者の守秘義務に関する確約事項

マイクロソフトは、顧客データ、プロフェッショナル サービス データ、および個人データの処理に従事するマイクロソフト担当者が、(i) お客様からの指示または本 DPA の規定に必ず従って当該データを処理すること、および (ii) 処理の終了後も顧客データおよび個人データの秘密保持と安全性の保持が義務付けられていることを保証するものとします。マイクロソフトは、適用されるデータ保護要件および業界標準に従い、顧客データ、プロフェッショナル サービス データ、および個人データにアクセスするマイクロソフトの従業員に対し、データ プライバシーおよびセキュリティに関する必須のトレーニングを定期的に実施し、これらについて周知させるものとします。

下請処理者の使用に関する通知および規制

マイクロソフトは、一部のサービスまたは補助的なサービスを下請処理者に委託することができます。お客様は、本契約と下請処理者としてのマイクロソフトの関連会社に同意するものとします。標準契約条項または GDPR 条件の下で上記の同意が要求される場合、この承認は、マイクロソフトが顧客データ、プロフェッショナル サービス データ、および個人データの処理を下請業者に委託することに対するお客様の事前の書面による同意を構成します。

マイクロソフトは、その下請処理者が本 DPA のマイクロソフトの義務を遵守することに責任を負います。マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データ、プロフェッショナル サービス データ、または個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。マイクロソフトは、処理対象データの開示への制限を含め、本 DPA がマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。マイクロソフトは、これらの契約上の義務が確実に満たされるように下請処理者を監督することに同意します。

マイクロソフトは、随時、新しい下請処理者と契約できるものとします。マイクロソフトは、新規に契約した下請処理者に顧客データへのアクセスを許可する 6 か月前までに、新規業者についてお客様に通知し、該当する場合は、Web サイトを更新して、かかる更新を知る方法をお客様に提供します。さらに、マイクロソフトは、新規に契約した下請処理者に顧客データに含まれているデータ以外のプロフェッショナル サービス データまたは個人データへのアクセスを許可する 30 日前までに、新規業者についてお客様に通知し、該当する場合は、Web サイトを更新して、かかる更新を知る方法をお客様に提供します。マイクロソフトは、顧客データ、プロフェッショナル サービス データ、または個人データを処理する新しい本製品またはプロフェッショナル サービスのために新しい下請処理者と契約する場合、その本製品またはプロフェッショナル サービスを提供する前に、お客様に通知します。

お客様は、オンライン サービスまたはプロフェッショナル サービスについて新しい下請処理者を承認しない場合、当該通知期間が終わる前に、解除通知を書面で交付することによって、影響を受けるオンライン サービスのサブスクリプションまたは該当するプロフェッショナル サービスに適用されるサービス個別契約をそれぞれ違約金または解除料金なしで解除することができます。お客様は、本ソフトウェアについて新しい下請処理者を承認せず、ドキュメントまたは本 DPA に定めるデータのマイクロソフトによる処理を制限しても下請処理者の使用を合理的に回避できない場合、当該通知期間が終わる前に、解除通知を書面で交付することによって、影響を受けるソフトウェア製品のライセンスを違約金なしで解除することができます。お客様は、マイクロソフトが該当する懸念に基づいて新しい下請処理者を再評価できるようにするために、解除通知とともに不承認の理由の説明を含めることもできます。影響を受ける本製品がスイート (またはサービスの 1 回の購入) の一部である場合、解除はスイート全体に適用されます。解除後、マイクロソフトは、お客様またはそのリセラーに対する以降の請求書から、解除した本製品および本サービスのサブスクリプションまたはその他該当する未払の作業に対する支払義務を除外します。

教育機関

お客様が、家庭教育の権利とプライバシーに関する法 (20 U.S.C. § 1232g) (FERPA) に基づく規制が適用される教育機関である場合、マイクロソフトは、本 DPA において、マイクロソフトが顧客データおよびプロフェッショナル サービス データに関して「正当な教育上の利害」を有する「学校関係者」であることを了解します。これらの各用語の定義は、FERPA およびその下位規則での定義に従うものとします。マイクロソフトは、34 CFR 99.33(a) により学校関係者に課せられる制限および要件に従うことに同意します。

お客様は、マイクロソフトが、お客様の学生および学生の両親の連絡先について限られた情報しか持っていないかまたは情報をまったく持っていない場合があることを了解するものとします。したがって、お客様は、適用される法令によって必要とされる場合に、エンド ユーザーによる本製品および本サービスの使用について保護者の同意を得る責任を負うものとし、適用される法令により義務付けられる場合には、マイクロソフトが所有する顧客データおよびプロフェッショナル サービス データの開示を要求する裁判所の命令または合法的に発行された令状について、マイクロソフトに代わって学生 (または、18 歳未満で中等後教育機関に在籍していない学生に関しては、学生の保護者) に通知を行うものとします。

CJIS 顧客契約

マイクロソフトは、FBI 犯罪司法情報サービス (以下「CJIS」といいます) セキュリティ ポリシー (以下「CJIS ポリシー」といいます) に従って特定の政府機関 クラウド サービス (以下「対象サービス」といいます) を提供します。犯罪司法情報サービスの使用と送信には CJIS ポリシーが適用されます。すべてのマイクロソフト CJIS 対象サービスに適用される CJIS 顧客契約の条件については、<http://aka.ms/CJISCustomerAgreement> を参照してください。

HIPAA Business Associate

お客様が「対象法人」または「関係機関」であり、顧客データまたはプロフェッショナル サービス データに「保護されるべき医療情報」(各用語については 1996 年医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act of 1996) (改正後のもの)、およびその後公布された規制 (以下、総称して「HIPAA」といいます) に定義されています) が含まれる場合、お客様のボリューム ライセンス契約の締結には、HIPAA Business Associate Agreement (以下「BAA」といいます) の締結が含まれます。BAA には、その適用対象となるオンライン サービスまたはプロフェッショナル サービスが規定されており、その全文は <http://aka.ms/BAA> でご確認いただけます。お客様は、(お客様のボリューム ライセンス契約の条項に基づき) 書面による通知をもって以下の情報をマイクロソフトに送付することにより、BAA をオプトアウトすることができます。

* オプトアウトするお客様および関連会社の正式名称
* お客様が複数のボリューム ライセンス契約を締結している場合は、オプトアウトが適用されるボリューム ライセンス契約

カリフォルニア州消費者プライバシー保護法 (CCPA)

マイクロソフトは、CCPA の範囲内で個人データを処理している場合、お客様に対して以下の追加の確約事項を遂行します。マイクロソフトは、お客様に代わって顧客データ、プロフェッショナル サービス データ、および個人データを処理するものとし、DPA 条件で定められた、CCPA で許可されている目的 (データの「販売」に関する適用除外事項を含む) 以外の目的ではそのデータを保持、使用、または開示してはなりません。いかなる場合においても、マイクロソフトがかかるデータを販売することはありません。本 CCPA 条件は、DPA 条件、製品条項、またはマイクロソフトとお客様との間のその他の契約においてマイクロソフトがお客様に対して行ったデータ保護に関する確約事項を制限または軽減するものではありません。

生体認証データ

お客様が本製品および本サービスを使用して、生体認証データを処理する場合は、以下の責任を負うものとします。(i) データの保持期間および破棄に関する通知を含め、データ主体に通知する。(ii) データ主体から同意を得る。(iii) 生体認証データを削除する。すべて必要に応じて、該当するデータ保護要件の求めに応じて行います。マイクロソフトは、文書化されたお客様の指示に従って、生体認証データを処理し (上記の「処理者と管理者の役割および責任」に記載のとおり)、本 DPA のデータ セキュリティ条件および保護条件に従ってその生体認証データを保護します。本条項において、「生体認証データ」は GDPR の第 4 条に定められている意味と、該当する場合は、他のデータ保護要件の同等の条件を有するものとします。

追加プロフェッショナル サービス

以下に記載する条項で使用している場合、定義語「プロフェッショナル サービス」は追加プロフェッショナル サービスを含み、定義語「プロフェッショナル サービス データ」は追加プロフェッショナル サービスのために取得されるデータを含みます。

追加プロフェッショナル サービスに関して、DPA の次の各条項が、プロフェッショナル サービスに適用される方法と同じ方法で適用されます。「概要」、「法令遵守」、「データ処理の性質 (権利の帰属)」、「処理対象データの開示」、「個人データの処理 (GDPR)」、「セキュリティ規定およびポリシー」の第 1 段落、「お客様の責任」、「セキュリティ インシデントの通知」、「データ移転」(2021 年標準契約条項に関する条件を含む)、「データの保持と削除」の第 3 段落、「処理者の守秘義務に関する確約事項」、「下請処理者の使用に関する通知および規制」、「HIPAA Business Associate」(BAA の適用対象である場合)、「カリフォルニア州消費者プライバシー保護法 (CCPA)」、「生体認証データ」、「マイクロソフトへのお問い合わせ方法」、「付属文書 B – データ主体、および個人データの種類」、ならびに「付属文書 C – 追加の安全措置契約」。

マイクロソフトへのお問い合わせ方法

マイクロソフトがプライバシーまたはセキュリティに関する確約事項を遵守していないとお考えの場合、お客様は、カスタマー サポートまで連絡するか、<http://go.microsoft.com/?linkid=9846224> にあるマイクロソフトのプライバシー Web フォームを使用することができます。郵送の場合のマイクロソフトの住所は次のとおりです。

**Microsoft Enterprise Service Privacy**

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited は、欧州経済地域およびスイスにおけるマイクロソフトのデータ保護に関する代理人です。Microsoft Ireland Operations Limited のプライバシー担当者の住所は次のとおりです。

**Microsoft Ireland Operations, Ltd.**

Attn: Data Protection

One Microsoft Place

South County Business Park

Leopardstown

Dublin 18, D18 P521, Ireland

[目次](#TableofContents) / [標準の条件](#GeneralTerms)

付属文書 A – セキュリティ対策

マイクロソフトは、コア オンライン サービスの顧客データおよびプロフェッショナル サービス データに対して以下のセキュリティ対策を講じています。これらの対策は、本 DPA (GDPR 条件を含む) のセキュリティに関する確約事項とともに、そのデータのセキュリティに関するマイクロソフトの唯一の責任です。

| ドメイン | 対策 |
| --- | --- |
| 情報セキュリティの構築 | **セキュリティの責任者。**当社は、セキュリティ規則および手順の調整と監視を担当する 1 人以上のセキュリティ責任者を任命しました。  **セキュリティの役割および責任。**顧客データまたはプロフェッショナル サービス データにアクセス可能なマイクロソフト担当者には、秘密保持義務が適用されます。  **リスク管理プログラム。**マイクロソフトは、顧客データの処理またはオンライン サービスの開始前、およびプロフェッショナル サービス データの処理またはプロフェッショナル サービスの開始前にリスク評価を実施しました。  マイクロソフトは、セキュリティ関連文書を、効力を持たなくなった後も保存義務に従って保存します。 |
| アセット管理 | **アセット一覧。**マイクロソフトは、顧客データまたはプロフェッショナル サービス データが保管されているすべてのメディアの一覧を保持します。かかるメディアの一覧へのアクセスは、かかるアクセスを書面で許可されているマイクロソフト担当者に制限されます。  **アセットの取り扱い**  - マイクロソフトは顧客データおよびプロフェッショナル サービス データを分類して、識別しやすくするとともに、かかるデータへのアクセスを適切に制限できるようにします。  - マイクロソフトは、顧客データおよびプロフェッショナル サービス データの印刷に制限を課し、当該データを含む印刷物の廃棄手順を定めています。   * マイクロソフト担当者は、顧客データまたはプロフェッショナル サービス データを携帯用デバイスに格納し、当該データにリモート アクセスし、または当該データをマイクロソフトの施設以外で処理する前に、マイクロソフトの許可を得る必要があります。 |
| 人事セキュリティ | **セキュリティ トレーニング。**マイクロソフトはマイクロソフト担当者に、関連するセキュリティ手順およびそれぞれの役割について通知します。また、マイクロソフトは、マイクロソフト担当者に、セキュリティ規則および手順に対する違反により生じ得る結果についても通知します。マイクロソフトは、トレーニングにおいては匿名データのみを使用します。 |
| 物理セキュリティおよび論理セキュリティ | **施設への物理的アクセス。**マイクロソフトは、顧客データまたはプロフェッショナル サービス データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に限定します。  **コンポーネントへの物理的アクセス。**マイクロソフトは、メディアの種類、許可された送付者/受領者、日付および時刻、メディアの数ならびに含まれる顧客データまたはプロフェッショナル サービス データの種類を含め、顧客データまたはプロフェッショナル サービス データを収録したメディアの使用状況を記録します。  **損傷からの保護。**マイクロソフトは、さまざまな業界標準システムを使用して、電源の故障または電力線妨害によるデータの損失を防止します。  **データの廃棄。**マイクロソフトは、業界標準プロセスを使用して、不要になった顧客データおよびプロフェッショナル サービス データを削除します。 |
| 通信および運用管理 | **運用ポリシー。**マイクロソフトは、マイクロソフトのセキュリティ対策ならびに顧客データまたはプロフェッショナル サービス データにアクセス可能なマイクロソフト担当者の関連手順および責務を規定したセキュリティ関連文書を保持します。  **データ回復手順**  - 継続的に、ただしいかなる場合でも週に 1 回以上 (その期間中に更新が行われなかった場合を除きます)、マイクロソフトは、顧客データおよびプロフェッショナル サービス データの回復に使用することができる当該データの複製を複数作成します。  - マイクロソフトは、顧客データおよびプロフェッショナル サービス データの複製とデータ回復手順を、顧客データおよびプロフェッショナル サービス データを処理する主要コンピューター機器が設置されている場所とは異なる場所に保管します。  - マイクロソフトは、顧客データおよびプロフェッショナル サービス データの複製へのアクセスを管理するための具体的な手順を定めています。  - マイクロソフトは、データ回復手順を少なくとも 6 か月ごとに見直します。ただしプロフェッショナル サービスおよび Azure Government サービスのデータ回復手順は例外とし、これについては 12 か月ごとに見直しを行います。  - マイクロソフトは、復元されたデータの説明、担当者 (該当する場合)、およびデータ回復処理において手作業で入力する必要があったデータ (存在する場合) を含め、データ復元作業を記録します。  **悪意のあるソフトウェア。**当社は、パブリック ネットワークから送信される悪意のあるソフトウェアを含め、悪意のあるソフトウェアが顧客データおよびプロフェッショナル サービス データに不正アクセスしないようにするためのマルウェア制御機能を備えています。  **境界を越えるデータ**  - マイクロソフトは、パブリック ネットワークを介して伝送される顧客データおよびプロフェッショナル サービス データを暗号化するか、またはお客様が暗号化できるようにします。  - マイクロソフトは、当社の施設外へ持ち出されるメディア内の顧客データおよびプロフェッショナル サービス データへのアクセスを制限します。  **イベント ログ。**当社は、アクセス ID、時刻、許可または拒否された認証、および関連する活動を登録することにより、顧客データおよびプロフェッショナル サービス データを含む情報システムへのアクセスおよび使用をログに記録し、またはお客様がログに記録できるようにします。 |
| アクセス制御 | **アクセス ポリシー。**マイクロソフトは、顧客データまたはプロフェッショナル サービス データにアクセス可能な個人のセキュリティ権限の記録を保持します。  **アクセスの許可**  - マイクロソフトは、顧客データまたはプロフェッショナル サービス データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。  - マイクロソフトは、一定期間 (最長 6 か月) 使用されていない認証資格情報を無効にします。  - マイクロソフトは、データおよびリソースへのアクセス権限を許可、変更、または取り消すことができる担当者を指名します。  - 顧客データまたはプロフェッショナル サービス データを含むシステムに複数の個人がアクセスすることができる場合、マイクロソフトは、それらの個人に個別のログイン ID を割り当てます。  **最小限の権限**  - テクニカル サポート担当者は、必要な場合に限り、顧客データおよびプロフェッショナル サービス データへのアクセスを許可されます。  - マイクロソフトは、顧客データおよびプロフェッショナル サービス データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。  **完全性および秘密保持**  - マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。  - マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。  **認証**  - マイクロソフトは、業界標準の慣行を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。  - 認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。  - 認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。  - マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。  - マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、またはお客様が監視できるようにします。  - マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。  - マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護慣行を使用します。  **ネットワーク設計。**マイクロソフトは、個人が、アクセスを許可されていない顧客データまたはプロフェッショナル サービス データにアクセスするために、割り当てられていないアクセス権を持っていると根拠なく信じることのないように、規制を行っています。 |
| 情報セキュリティ インシデント管理 | **インシデント対応プロセス**  - マイクロソフトは、違反の内容、期間、違反の影響、報告者の名前、違反の報告先、データの回復手順を含む、セキュリティ違反の記録を保持します。  - セキュリティ インシデントとなる各セキュリティ違反について、マイクロソフトは、上記の「セキュリティ インシデントの通知」の規定に従い、過度の遅滞なく、かつ、いかなる場合も 72 時間以内に通知を行います。  - マイクロソフトは、開示されたデータ、データの開示先および開示時刻を含む、顧客データおよびプロフェッショナル サービス データの開示を追跡するか、またはお客様が追跡できるようにします。  **サービス監視。**マイクロソフトのセキュリティ担当者は、少なくとも 6 か月ごとに記録を確認し、必要な場合は改善のための取り組みを提案します。 |
| 事業継続性の管理 | - マイクロソフトは、顧客データまたはプロフェッショナル サービス データを処理する当社情報システムが設置されている施設について緊急時対応計画を保持しています。  - マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データおよびプロフェッショナル サービス データを再構築することを試みるように設計されています。 |

[目次](#TableofContents) / [標準の条件](#GeneralTerms)

付属文書 B – データ主体、および個人データの種類

**データ主体:**データ主体には、お客様の担当者ならびにお客様の従業員、委託業者、協力者、および顧客などのエンドユーザーが含まれます。データ主体には、マイクロソフトが提供するサービスのユーザーに個人情報を伝達または移転することを試みる個人が含まれる場合もあります。マイクロソフトは、お客様による本製品および本サービスの使用に応じて、お客様が以下のいずれかの種類のデータ主体からの個人データを個人データに含めることを選択できることに同意します。

* お客様の従業員、請負業者、および臨時従業員 (現職者、旧職者、候補者)
* 上記の関係者
* お客様の協力者/連絡先 (自然人) または法人の協力者/連絡先の従業員、請負業者、または臨時労働者 (現職者、旧職者、候補者)
* ユーザー (お客様、クライアント、患者、訪問者など) およびお客様のサービスのユーザーであるその他のデータ主体
* コラボレーション、コミュニケーション、またはその他の方法でお客様の従業員と能動的にやり取りする、あるいはお客様が提供するアプリや Web サイトなどのコミュニケーション ツールを使用するパートナー、利害関係者、または個人
* お客様と受動的にやり取りする利害関係者または個人 (たとえば、これらの利害関係者または個人が、お客様との間でやり取りされたドキュメントや通信内容で調査または言及されている主体であるため)
* 未成年者
* 専門的な特権を持つ職業的専門家 (医師、弁護士、公証人、宗教従事者など)

**データの種類:**本製品および本サービスに関連する電子メール、文書およびその他の電子形式のデータに含まれる個人データ。 マイクロソフトは、お客様による本製品および本サービスの使用に応じて、お客様が以下のいずれかの種類の個人データを個人データに含めることを選択できることに同意します。

* 基本的な個人データ (例: 出生地、居住地の番地 (住所)、郵便番号、市区町村、国、携帯電話番号、名、姓、イニシャル、電子メール アドレス、性別、生年月日)。これには、家族や子どもに関する基本的な個人データも含まれます
* 認証データ (例: ユーザー名、パスワードまたは PIN コード、セキュリティの質問、監査証跡)
* 連絡先情報 (例: 住所、電子メール、電話番号、ソーシャル メディア ID、緊急連絡先)
* 一意の識別番号と署名 (例: 社会保障番号、銀行口座番号、パスポートおよび ID カード番号、運転免許証番号と車両登録データ、IP アドレス、従業員番号、学生番号、患者番号、署名、追跡用 Cookie の一意の識別子)
* 仮名識別子
* 金融および保険情報 (例: 保険番号、銀行口座名および番号、クレジット カード保有者名および番号、請求書番号、収入、保証の種類、支払いパターン、信用度)
* 取引情報 (例: 購入履歴、特別オファー、購読情報、支払い履歴)
* 生体認証情報 (例: DNA、指紋、虹彩スキャン)
* 位置データ (例: セル ID、ジオロケーション ネットワーク データ、コール開始/終了の位置。WiFi アクセス ポイントの使用から得られた位置データ)
* 写真、動画、および音声
* インターネット アクティビティ (例: 閲覧履歴、検索履歴、読書、テレビおよびラジオ視聴アクティビティ)
* デバイス識別情報 (例: IMEI 番号、SIM カード番号、MAC アドレス)
* プロファイリング (例: 確認された犯罪的または反社会的行動に基づくプロファイル、または訪問した URL、クリック ストリーム、閲覧ログ、IP アドレス、ドメイン、インストール済みアプリに基づく仮名プロファイル、あるいはマーケティング設定に基づくプロファイル)
* 人事および採用データ (例: 雇用状況の宣言、採用情報 (履歴書、職歴、学歴の詳細など)、職務および職位データ (勤務時間、査定と給与、労働許可証の詳細、対応可能状況、雇用条件、税金の詳細、支払の詳細、保険の詳細、場所および組織など))
* 教育データ (例: 学歴、現在の教育、成績と結果、最終学歴、学習障害)
* 市民権と居住に関する情報 (例: 市民権、帰化ステータス、婚姻ステータス、国籍、移民ステータス、パスポート データ、居住または労働許可の詳細)
* 公益のために実施される、または職務権限を行使して実施される作業の遂行のために処理される情報
* 特殊な種類のデータ (例: 人種的または民族的起源、政治的意見、宗教的または哲学的信念、労働組合への加入、遺伝データ、自然人を一意に識別する生体認証データ、医療に関するデータ、自然人の性生活または性的指向に関するデータ、または刑事上の有罪判決または犯罪に関連するデータ)
* GDPR の第 4 条で特定されているその他すべての個人データ

付属文書 C – 追加の安全措置契約

DPA にこの追加の安全措置契約 (以下、「本追加契約」といいます) を追加することにより、マイクロソフトは、お客様に代わってマイクロソフトが行う、GDPR の範囲内での個人データの処理に関する追加の安全措置をお客様に、追加の是正措置を当該個人データが関連付けられるデータ主体に提供します。

本追加契約は、DPA を補足してその一部を構成するものですが、DPA の変更または修正とはなりません。

1. **命令への異議申し立て。**本 DPA に基づいて処理された個人データの強制開示の命令を第三者から受けた場合、マイクロソフトは以下を行うものとします。
2. 第三者に、データをお客様に直接請求させるようあらゆる合理的な努力をする。
3. 要請している第三者に適用される法令により禁止されていない限り、直ちにお客様に通知し、お客様に通知することを禁止されている場合は、可能な限り速やかにお客様に情報を伝えるために、禁止を放棄する権利をあらゆる合法的な努力を尽くして取得する。
4. 要請当事者の法に基づく法的不備または欧州連合の適用される法令や該当する加盟国の法との抵触を根拠に、開示命令に合法的な手段を講じて異議を申し立てる。

上記 a. ～ c. に記載した手順の実施後も、マイクロソフトまたはその関連会社が個人データを開示せざるを得ない場合、マイクロソフトは強制開示の命令を満たす必要最小限のデータのみを開示します。

本条項において、合法的な努力には、関連する裁判管轄地の法律に基づく法廷侮辱罪などの民事または刑事処分になる訴訟は含まれません。

1. **データ主体の補償。**第 3 条および第 4 条に従い、マイクロソフトは、EU/EEA 以外の政府機関または規制当局からの命令に応じて、GDPR の第 V 章に基づくマイクロソフトの義務に違反して移転されたデータ主体の個人データのマイクロソフトによる開示 (「関連する開示」) が原因となったデータ主体に対する有形または無形の損害をデータ主体に補償するものとします。前述の規定にかかわらず、マイクロソフトは、データ主体が、マイクロソフトからでもそれ以外からでも、同じ損害に対する補償を受け取っている限りにおいて、本第 2 条に基づくデータ主体に補償する義務を負わないものとします。
2. **補償の条件。**第 2 条の補償は、マイクロソフトが合理的に満足する程度にデータ主体が以下を証明することが条件となります。
3. マイクロソフトが関連する開示に関与した。
4. 関連する開示は、データ主体に対する EU/EEA 以外の政府機関または規制当局による公式の訴訟に基づいていた。
5. 関連する開示は、データ主体が有形または無形の損害を被る直接の原因となった。

データ主体は、a. ～ c. の条件について立証責任を負うものとします。

前述の規定にかかわらず、関連する開示が GDPR の第 V 章の義務に違反していないことをマイクロソフトが立証した場合、マイクロソフトは、第 2 条に基づくデータ主体に補償する義務を負わないものとします。

1. **損害の適用範囲。**第 2 条に基づく補償は、GDPR に規定される有形および無形の損害に制限され、マイクロソフトによる GDPR の権利侵害に起因しない派生的損害および他のすべての損害は除外されます。
2. **権利の行使。**本追加契約に基づきデータ主体に認められた権利は、標準契約条項の第 3 条または第 6 条の制限に関係なく、データ主体によってマイクロソフトに対して行使されます。データ主体は、集団、共同、団体、または代表訴訟の一環としてではなく、個人レベルでのみ本追加契約に基づく訴訟を起こすことができます。本追加契約に基づきデータ主体に認められる権利は、データ主体個人に対してであり譲渡することはできません。
3. **変更通知。**マイクロソフトは、以下に同意し保証するものとします。自己によってまたは下請処理者を介して個人データが移転される対象国となるいずれの国におけるものも含め、自己またはその下請処理者に適用される法令により、お客様から受領した指示および本追加契約または 2021 年標準契約条項に基づく義務に応えることが禁止されていると考える理由がないこと、ならびに、この法令に本追加契約または標準契約条項の規定する保証および義務に重大な悪影響を及ぼす可能性がある変更があった場合はかかる変更を認識次第速やかにお客様に通知すること。この場合、お客様はデータの移転を一時中断し、または契約を解除できるものとします。

別紙 1 - EU 一般データ保護規則条件

マイクロソフトは、すべてのお客様に対して本 GDPR 条件の確約事項を 2018 年 5 月 25 日をもって遂行します。当該確約事項は、(1) 本製品の任意のサブスクリプションもしくはライセンスに適用される製品条項および DPA のバージョンに関係なく、または、(2) 本別紙を参照する他の契約の存在に関係なく、マイクロソフトとお客様との関係性に対して拘束力を持つものとします。

本 GDPR 条件において、お客様とマイクロソフトは、お客様が個人データの管理者であり、マイクロソフトが当該データの処理者であることに合意します。ただし、お客様が個人データの処理者となる場合を除くものとし、この場合はマイクロソフトが下請処理者となります。本 GDPR 条件は、お客様に代わってマイクロソフトが行う、GDPR の範囲内での個人データの処理に適用されます。本 GDPR 条件は、製品条項またはマイクロソフトとお客様との間のその他の契約においてマイクロソフトがお客様に対して行ったデータ保護に関する確約事項を制限または軽減するものではありません。本 GDPR 条件は、マイクロソフトが個人データの管理者である場合は適用されません。

**関連する GDPR の義務: 第 28 条、第 32 条および第 33 条**

**1.**マイクロソフトは、お客様の特定のまたは包括的な許可を書面により事前に得ることなく他の処理者を従事させないものとします。包括的な書面による許可の場合、マイクロソフトは、他の処理者の追加または交換等の変更を行う予定である場合には、その旨お客様に通知し、かかる変更に異議を申し立てる機会をお客様に提供するものとします (第 28 条 (2) 項)。

**2.**マイクロソフトによる処理には、欧州連合 (以下「EU」といいます) または加盟国の法令に基づいて本 GDPR 条件が適用されるものとし、本 GDPR 条件はお客様に関してマイクロソフトを法的に拘束します。処理の対象および期間、処理の性質および目的、個人データの種類、データ主体の種類、ならびにお客様の義務および権利については、お客様のライセンス契約 (本 GDPR 条件を含みます) に規定するとおりとします。特に、マイクロソフトは以下を行うものとします。

**(a)** 第三国または国際組織への個人データの移転に関することを含め、お客様からの文書化された指示に従ってのみ個人データを処理すること。ただし、マイクロソフトに適用される EU または加盟国の法令により処理の実施を義務付けられている場合を除くものとし、このような場合は、重要な公共の利益に基づいて当該法令によりかかる通知が禁止されない限り、マイクロソフトは、処理を行う前に当該法的要件についてお客様に通知するものとします。

**(b)** 個人データの処理を許可された者が、秘密保持を確約しているか、または適切な法定の守秘義務を負うことを保証すること。

**(c)** GDPR 第 32 条に従って必要なすべての対策を講じること。

**(d)** 別の処理者を従事させることについて、第 1 項および第 3 項に規定する条件に従うこと。

**(e)** 処理の性質を考慮したうえで、GDPR 第 III 章に規定されたデータ主体の権利の行使要求に対応するというお客様の義務の履行のため、可能な限りにおいて、適切な技術的および組織的対策によってお客様を支援すること。

**(f)** 処理の性質およびマイクロソフトに提供される情報を考慮したうえで、お客様が GDPR 第 32 条 ～ 第 36 条に従って義務を確実に遵守するよう支援すること。

**(g)** お客様の選択に応じて、処理に関するサービス提供の終了後にすべての個人データを削除またはお客様に返却し、EU または加盟国の法令が個人データの保存を義務付けている場合を除き既存のコピーを削除すること。

**(h)** GDPR 第 28 条に規定された義務の遵守を証明するとともに、お客様またはお客様が委任する他の監査人による監査を設定しこれに協力するために必要なすべての情報をお客様に提供すること。

マイクロソフトは、指示が、GDPR または他の EU もしくは加盟国のデータ保護規定に違反すると考える場合には、直ちにその旨をお客様に通知するものとします (第 28 条 (3) 項)。

**3.**マイクロソフトが、お客様に代わって特定の処理活動を行うために別の処理者を従事させる場合、契約または EU もしくは加盟国の法令に基づくその他の法的行為により、本 GDPR 条件に定めるものと同じデータ保護義務をかかる他の処理者に課すものとし、特に、処理が GDPR の要件を満たすような方法で適切な技術的および組織的対策を実施することを十分に保証するよう規定するものとします。他の処理者が自らのデータ保護義務を履行しない場合、マイクロソフトはお客様に対し、かかる他の処理者の義務の履行について全面的に責任を負うものとします (第 28 条 (4) 項)。

**4.**最新技術、実施コスト、処理の性質、範囲、背景および目的、ならびに自然人の権利と自由に対するリスクのさまざまな可能性と重大度を考慮したうえで、お客様とマイクロソフトは、リスクに見合ったセキュリティ レベルを確保するために適切な技術的および組織的対策を実施するものとします。かかる対策には必要に応じて、特に以下のものを含むものとします。

**(a)** 個人データの仮名化および暗号化

**(b)** 処理システムおよびサービスの現行の機密性、完全性、可用性および復元力を確保する能力

**(c)** 物理的または技術的なインシデントが発生した場合に適時に個人データの可用性と個人データへのアクセスを復元する能力

**(d)** 処理のセキュリティを確保するために、技術的および組織的対策の有効性を定期的にテスト、審査および評価するプロセス (第 32 条 (1) 項)。

**5.**適切なセキュリティ レベルの審査においては、処理により生じるリスク、特に送信、保存またはその他の方法で処理された個人データの偶発的もしくは違法な破壊、滅失、改変、不正な開示、またはかかる個人データへのアクセスがもたらすリスクを考慮するものとします (第 32 条 (2) 項)。

**6.**お客様とマイクロソフトは、お客様またはマイクロソフトの許可を得て行動する、個人データへのアクセス権を有する自然人が、お客様からの指示なくして個人データを処理しないようにするための措置を講じるものとします。ただし、EU または加盟国の法令により処理の実施を義務付けられている場合を除きます (第 32 条 (4) 項)。

**7.**マイクロソフトは、個人データの侵害を認識した場合には、不当な遅滞なくお客様に通知するものとします (第 33 条 (2) 項)。かかる通知には、第 33 条 (3) 項に基づいて処理者が管理者に提供する必要のある情報が含まれます。当該情報は、マイクロソフトが合理的に入手できる範囲内で提供されるものとします。

[目次](#TableofContents) / [標準の条件](#GeneralTerms)