Microsoft 調達部門

サプライヤーセキュリティおよびプライバシーアシュアランス（SSPA）プログラムガイド

バージョン 11

2025 年 4 月

目次

Microsoft

SSPA プログラム概要

サプライヤーセキュリティおよびプライバシーアシュアランス（Supplier Security and Privacy Assurance: 「**SSPA**」）プログラムは、Microsoft の調達部門、渉外および法務部門、コーポレートセキュリティ部門、責任のある AI 部門の連携により、サプライヤー様が Microsoft のプライバシーおよび責任のある AI に関する原則を遵守されるのを保証するものです。サプライヤーセキュリティおよびプライバシーアシュアランス（Supplier Security and Privacy Assurance: 「SSPA」）プログラムは、Microsoft のサプライヤー様向けに、Microsoft の基本データ処理に関する指示を Microsoft サプライヤー向けデータ保護要件（Data Protection Requirements 「DPR」）という様式で提供するために設けられた Microsoft の企業プログラムです。以下のリンクから入手することができます。 Microsoft.com/Procurement

サプライヤー様は、SSPA を利用して、契約を請け負う商品および/またはサービスに沿ったデータ処理プロファイルを選択できます。それらの選択内容によって、 Microsoft にコンプライアンスアシュアランスを提供するための対応要件が発生します。

登録されているすべてのサプライヤー様は、DPR に対するコンプライアンスの自己評価を実施し、その評価結果の証明を毎年提出いただくことになります。貴社のデータ処理プロファイルによって、DPR が全面的に実施されるか、または要件の一部のみが適用されるかが決定されます。Microsoft がより高リスクと見なすデータを処理するサプライヤー様の場合、コンプライアンスの独立検証などの追加要件を満たしていただく必要がある場合もあります （「独立評価」の項をご覧ください）。なお、サプライヤーは SSPA とは別にサプライヤーとの関与を担当する Microsoft のグループにより決定および通知される、組織レベルの追加要件を満たすことが求められる場合があります。

重要：コンプライアンスに関する取り組みにより、SSPA のステータスが緑（準拠）または赤（非準拠）か、そしてデータ処理承認（下記データ処理プロファイルを参照）の状況が特定されます。サプライヤー様との関与に先立ち、Microsoft の購買ツールにより SSPA のステータスが緑であることを（SSPA の対象となる各サプライヤーに対して）検証します。

SSPA データ処理プロファイル

Microsoft のサプライヤー様は、SSPA データ処理プロファイルを管理できます。SSPA は、データ処理プロファイルで選択された承認に基づき、 Microsoft とのエンゲージメントにおけるリスクレベルを評価します。SSPA コンプライアンス要件は、データ処理プロファイルと関連する承認により異なり、これにより、サプライヤー様は、どのエンゲージメントに対する資格があるかを特定することができます。選択項目と承認を得るために完了しなければならないコンプライアンス活動について慎重に検討してください。

Microsoft ビジネスグループは、データ処理活動がサプライヤー様が取得した承認と一致する場合のみ、サプライヤー様との契約を作成することができます。

サプライヤー様は、未完了のタスクがない場合、年間を通じていつでもデータ処理プロファイルを更新することができます。変更が行われると、対応するアクティビティが発行され、新たな承認がデータ処理プロファイルに反映される前にそれらを完了する必要があります。新たに発行される要件が完了するまでは、既存の承認済み事項が適用されます。新たに実行されたタスクが 90 日以内に完了しない場合、SSPA ステータスは赤（非準拠）になり、アカウントが Microsoft アカウント決済システムから無効化されるリスクがあります。

また、コンプライアンス要件を向上させたり、低下させたりする可能性のある組み合わせもあります。このような組み合わせは、付録 A に記載されており、プロファイルを完了すると、Microsoft サプライヤーコンプライアンスポータルから実行できるようになります。SSPA チームのレビューを依頼することで、貴社のシナリオがこの枠組みにどのように適合するかをいつでもご確認いただけます。

SSPA データ処理プロファイルテーブル

#	プロファイル	要件	独立保証のオプション
1	範囲：個人、機密 処理の場所：Microsoft またはその顧客 処理の役割：プロセッサーまたはコントローラー データクラス：機密または極秘 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なしまたは、はい ウェブサイトのホスティング：該当なしまたは、はい ヘルスケア：該当なしまたは、はい	DPR 準拠に関する自己認証	
2	範囲：機密 処理の場所：サプライヤー様 処理の役割：該当なし データクラス：機密 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なし ウェブサイトのホスティング：該当なし ヘルスケア：該当なし	DPR 準拠に関する自己認証	
3	範囲：機密 処理の場所：サプライヤー様 処理の役割：該当なし データクラス：極秘 ペイメントカード：該当なし	DPR 準拠の自己認証 **および** コンプライアンスの独立保証	独立保証のオプション： 1. DPR に対する独立評価を完了する、**または**

	SaaS：該当なし 下請け業者への委託：該当なし ウェブサイトのホスティング：該当なし ヘルスケア：該当なし		2. ISO 27001 を提出する
4	範囲：個人、機密 処理の場所：サプライヤー様 処理の役割：プロセッサー データクラス：極秘 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なし ウェブサイトのホスティング：該当なし ヘルスケア：該当なし	DPR 準拠の自己認証 **および** コンプライアンスの独立保証	独立保証のオプション： 1. DPR に対する独立評価を完了する、**または** 2. DPR のセクション A～I および ISO 27001 に照らした独立評価、**または** 3. ISO 27701 および ISO 27001 を提出する
5	範囲：個人、機密 処理の場所：サプライヤー様 処理の役割：プロセッサー データクラス：機密 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なし ウェブサイトのホスティング：該当なし ヘルスケア：該当なし	DPR 準拠の自己認証	
6	範囲：個人、機密 処理の場所：サプライヤー様 処理の役割：コントローラー データクラス：極秘または機密 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なしまたは、はい ウェブサイトのホスティング：該当なし ヘルスケア：該当なしまたは、はい	DPR 準拠の自己認証	
7	範囲：個人、機密 処理の場所：どこでも 処理の役割：サブプロセッサー（この役割は Microsoft によって決定されます - プロファイルには「サブプロセッサー承認：済」と表示されます）	DPR 準拠の自己認証 **および** コンプライアンスの独立保証	独立保証のオプション： 1. DPR に対する独立評価を完了する、**または**

	データクラス：極秘または機密 ペイメントカード：該当なし **SaaS**：該当なし 下請け業者への委託：該当なし ウェブサイトのホスティング：該当なし ヘルスケア：該当なし		2. DPR のセクション A～I および ISO 27001 に照らした独立評価、**または** 3. ISO 27701 および ISO 27001 を提出する
8	範囲：個人、機密 処理の場所：サプライヤー様 処理の役割：プロセッサー データクラス：極秘または機密 ペイメントカード：該当なし 下請け業者：該当する、または **SaaS**：該当する、または ウェブサイトのホスティング：該当する、または ヘルスケア：該当する	DPR 準拠の自己認証 **および** コンプライアンスの独立保証	独立保証のオプション： 1. DPR に対する独立評価を完了する、**または** 2. DPR のセクション A～I および ISO 27001 に照らした独立評価、**または** 3. ISO 27701 **および** ISO 27001 を提出する 4. HITRUST レポート（米国内の対象事業者または医療機関のみ）
	上記のいずれかのプロファイルとペイメントカード	適用される上記の要件**および**ペイメントカード業界の保証	PCI DSS 認証を提出
	上記のいずれかのプロファイルおよびサービスとしてのソフトウェア（**SaaS**）	適用される上記の要件**および**機能的なサービスを網羅する、契約上必要な ISO 27001 認証を提出してください。	提供するサービスの機能を網らした ISO 27001 の認証書を提出してください。
	上記のいずれかのプロファイルと人工知能（**AI**）システム	AI 関連項目を含む DPR 準拠の自己認証 **および** コンプライアンスの独立保証	独立保証のオプション： 1. AI 部門を含む DPR に対する独立評価を完了する、**または** 2. DPR のセクション A～I と K および ISO 27001 に照らした独立

			評価、 または 3. DPR のセクション K および ISO 27701 および ISO 27001 に照らした独立評価、 **または** 4. ISO 27701、ISO 27001 および ISO 42001 を提出する （*ISO 42001 は、AI システムのセンシティブな使用を含むサービスを提供する際に必要です）

範囲

機密

サプライヤー様が Microsoft 機密データの処理のみを実施する場合は、この承認を選択します。

この承認を選択した場合、個人データの処理に関する業務を行うことはできません。

個人、機密

サプライヤー様が個人データおよび Microsoft の機密データを含む処理を実行する場合は、この承認を選択します。

サプライヤー様が、個人データおよび/または Microsoft の機密データのどちらを処理するかを判断する際は、以下の表にある例のリストをご参照ください。これらは一部の例であり、網ら的リストではありません。

注：Microsoft のビジネスオーナーは、処理されるデータの機密性を考慮し、このリストに記載されていない項目の登録を依頼することができます。

データタイプ別の個人データ

対象となる例には以下のようなものがありますが、これらに限定されません：

機密データ
未成年者に関連するデータ
遺伝子データ、生体データ、健康データ

人種または民族的出自
政治的、宗教的、または哲学的信念、意見、および所属
労働組合への所属
自然人の性生活または性的指向
在留資格（ビザ、就労許可など）
政府発行の ID（パスポート、運転免許証、ビザ、社会保障番号、国民識別番号）
ユーザーの正確な位置情報（300m 以内）
個人の銀行口座番号
クレジットカード番号と有効期限、**または**アカウントへのアクセスを許可するセキュリティ/アクセスコードまたはパスワード/資格情報
エンドユーザーの仮名識別子（EUPI） （Microsoft の製品およびサービスを利用するユーザーを識別するために Microsoft によって作成された識別子） • グローバル一意識別子（GUID） • Passport ユーザー ID または一意の識別子（PUID） • ハッシュ化されたエンドユーザーの識別情報（EUII） • セッション ID • デバイス ID • 診断データ • ログデータ • サポートケースに関連する顧客データ
顧客コンテンツデータ
ドキュメント、写真、動画、音楽など
製品またはサービスに関して入力されたレビューおよび評価またはそのいずれか
アンケート回答
閲覧履歴、興味、お気に入り
手描き入力、タイピング、音声発話（音声/オーディオおよび/またはチャット/ボット）

資格情報データ（パスワード、パスワードのヒント、ユーザー名、識別に使用される生体認証データ）
サポートケースに関連する顧客データ
キャプチャされたデータおよび生成されたデータ
不正確な位置データ
IP アドレス
デバイスの詳細設定とパーソナライゼーション
ウェブサイトのサービス利用状況、ウェブページのクリックトラッキング
ソーシャルメディアデータ、ソーシャルグラフの関連性
フィットネスモニターなどの接続機器からのアクティビティデータ
氏名、住所、電話番号、電子メールアドレス、生年月日、扶養家族および緊急連絡先などの連絡先データ
不正およびリスクアセスメント、身元調査
保険、年金、福利厚生の詳細
応募者の履歴書、面接時の記録およびフィードバック
メタデータまたはテレメトリー
アカウントデータ
支払い方法データ
クレジットカード番号と有効期限
銀行ルーティング情報
銀行口座番号
クレジットリクエストまたはクレジットライン
税務書類と納税者 ID
投資または経費データ
コーポレートカード
オンライン顧客データ
Microsoft オンラインエンタープライズ顧客（Azure テナント、M365 テナントなど）

Microsoft 消費者顧客（Xbox Live、OneDrive 消費者）
Microsoft エンタープライズ顧客（オンプレミス顧客）
サポートデータ（顧客がチケットを発行）
アカウントデータ（請求額データ、e コマース）
調査/事象登録/トレーニング
保護対象保健情報
国民識別番号（部族番号および健康情報識別番号を含む）
保護対象保健情報（PHI）に関連して使用される以下の人口統計データ： • 生年月日 • 性別 • 民族 • 生体データ • 顔写真 • 住所（全部または一部） • 連絡先情報 • 緊急時の連絡先データ
センシティブな使用（AI システム）
法的地位や人生の機会に対する結果的な影響には、以下のものが含まれます。 • 刑事司法制度のリスク評価と採点システム • 高等教育の入学システム • クレジットスコアリングとアプリケーションシステム
身体的または心理的な傷害のリスクには、以下のものが含まれます。 • 医療診断または治療システム • メンタルヘルスおよびウェルビーイングシステム • 機器制御および予知保全システム
人権への脅威には、以下のものが含まれます。 • 選挙に影響を与えるために偽情報や政治的プロパガンダを生成する可能性のある合成メディアシステム • 宗教的、政治的、社会的表現に基づくアラートシステム • ソーシャルクレジットスコアリング

Microsoft 機密データ

対象となる例には以下のようなものがありますが、これらに限定されません：

極秘
Microsoft 製品または Microsoft 製品のコンポーネントの開発、テストまたは製造に関する情報 *あらゆるチャネルで市販されている Microsoft のソフトウェア、オンラインサービス、またはハードウェアは、「**Microsoft 製品**」とみなされます。* **注：**ゲーム製品の開発については、Microsoft のビジネスオーナーが、開発製品のデータ分類を「極秘」または「機密」にするかを指定できます。
リリース前の Microsoft デバイスのマーケティング情報
SEC 規則の適用対象となる未発表の Microsoft 企業財務データ

機密
Microsoft の代理として、あらゆる方法で販売される Microsoft 製品のライセンスキー
Microsoft の LOB（基幹業務）アプリケーションの開発またはテストに関連する情報
Office、SQL、Azure など、Microsoft のソフトウェアやサービスのリリース前のマーケティング資料
デバイスなど、Microsoft のサービスまたは製品に関する文書、設計書、電子文書または印刷物（プロセスまたは手順ガイド、構成データなど）

重要: Microsoft のビジネスオーナーは、このリストに含まれていないデータの提示を求めることができます。

処理の場所

Microsoft またはその顧客

サプライヤー様の、データ処理を含む業務の「実施」が、スタッフによる @microsoft.com のアクセス資格情報を使用する Microsoft ネットワーク環境内または Microsoft の顧客の環境内でのデータ処理を含む場合は、この承認を選択します。

以下の状況では、このオプションを選択しないでください：

- サプライヤー様が Microsoft 指定のオフショア施設（OF）を管理している場合。
- サプライヤー様が Microsoft にリソースを提供し、それらの人々が Microsoft ネットワークを使用することがある場合。ネットワークの外で作業が実施される場合、処理の場所は、「サプライヤー様」と見なされます。

サプライヤー様

「Microsoft またはその顧客」の（上記のような）条件が適用されない場合は、このオプションを選択します。

データ処理の役割

コントローラー

サプライヤー様による実施に関するすべての側面が、コントローラーのデータ処理の役割の定義（DPR を参照）を満たす場合、この承認を選択します。

この承認を選択した場合、「プロセッサー」の役割指定を受けた個人データの処理業務を行うことはできません。サプライヤー様が Microsoft に対してプロセッサーとコントローラーの両方である場合、「コントローラー」ではなく、「プロセッサー」を選択します。

プロセッサー

これは、サプライヤー様が Microsoft の代理としてデータを処理する場合、最も一般的な処理役割です。プロセッサーの定義を DPR でご確認ください。

サブプロセッサー

サプライヤー様が Microsoft のサブプロセッサーと称することはできません。これは、社内のプライバシー担当チームによる事前承認が必要なためです。サブプロセッサーの定義を DPR でご確認ください。サブプロセッサーには、データ保護補遺および独立評価を含む、追加の契約およびコンプライアンス要件があります（下記参照）。また、Microsoft のサブプロセッサーリストに掲載されているサプライヤー様は、コンプライアンスの独立検証の提供も求められます。

ペイメントカード処理

サプライヤー様が処理するデータに、Microsoft に代わってクレジットカードまたはその他のペイメントカードの処理をサポートするデータが含まれている場合は、この承認を選択します。

この承認により、サプライヤー様はペイメントカードの処理業務に従事できます。

PCI 認定の要件

ペイメントカード業界データセキュリティ標準 （PCI DSS: Payment Card Industry Data Security Standard） は、セキュリティインシデントの防止、検出、およびそれらに対する適切な対応を含む強固なペイメントカードデータセキュリティを開発するためのフレームワークです。このフレームワークは、自主規制業界団体である PCI セキュリティ基準評議会（PCI Security Standards Council） によって策定されたものです。PCI DSS 要件の目的は、処理されるカード会員データのセキュリティにリスクをもたらす技術やプロセスの脆弱性を特定することです。

これらの基準の遵守が Microsoft には求められています。Microsoft に代わってサプライヤー様がペイメントカード情報を取り扱う場合、当社はこれらの基準を遵守している証拠の提出を要請します。PCI セキュリティ基準評議会（PCI Security standards council） を参照のうえ、評議会が定める要件を確認してください。

扱われる取引量に応じて、サプライヤー様は認定セキュリティ評価機関に準拠を認証してもらうか、自己評価フォームを作成することもできます。

ペイメントカードのブランドにより、通常、評価タイプのしきい値が次のように設定されます：

- レベル 1： 第三者の査定者に PCI AOC 証明書を提供する。
- レベル 2 または 3：サプライヤー様の役員が署名した PCI DSS 自己評価調査票（SAQ）を提出する。

PCI の要件を満たし、適用される証明書を提出してください。Microsoft の顧客の支払いデータを処理または保存するサプライヤー様は、サービスプロバイダーとして、最新の PCI Tier 1 認定を取得する必要があります。

サービスとしてのソフトウェア（SaaS）

サービスとしてのソフトウェア（SaaS）は、インターネット上でクラウドベースのアプリケーションに接続し、利用できるようにするものです。SSPA コンプライアンス上、SaaS を幅広く捉え、サービスとしてのプラットフォーム（PaaS）、およびサービスとしてのインフラストラクチャ（IaaS）もこれに含まれるものとします。（SaaS についての詳細は、こちらの説明をご覧ください。）

Microsoft は、**サービスとしてのソフトウェア（Software as a Service: SaaS）**を、1 対多のモデルで使用する共通のコードに基づくソフトウェアとし、従量課金、または使用メトリクスに基づくサブスクリプションと定義しています。クラウドサービスプロバイダーは、クラウドベースのソフトウェアの開発と保守を行い、また自動でソフトウェアのアップデートを提供し、インターネットを通じて 1 対多の従量課金制でソフトウェアを顧客に提供します。ソフトウェアを購入し、各コンピュータにインストールするのではなく、この方式はサブスクリプションによりソフトウェアの配信およびライセンスの供与をすることで、オンラインでアクセスできるようにするものです。

注：個人データまたは Microsoft の機密データが第三者プラットフォームまたはクラウドインフラストラクチャプロバイダーにホストされている場合、ほとんどの SaaS サプライヤー様は、Microsoft サプライヤーコンプライアンスポータルで下請け業者の承認を追加する必要があります。

データ処理プロファイルに含まれる SaaS の定義を満たしたサプライヤー様は、有効な ISO 27001 証明書の提供を求められます。データセンターの証明書を提出する必要はありません。当社は貴社と Microsoft との契約書に記載されているソフトウェアサービスに適用される ISO 27001 の認証を求めます。

下請け業者への委託

サプライヤー様が処理を実施するために下請け業者に委託する場合には、この承認を選択します。（定義については DPR をご参照してください）。「**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。

下請け業者にはフリーランサー（DPR を参照してください）も含まれます。

Microsoft は、下請け業者への委託を高リスク要因の 1 つとみなします。個人データまたは Microsoft の機密データを処理する下請け業者に委託しているサプライヤー様には、それらの下

請け業者を開示していただく必要があります。さらに、サプライヤー様は各下請け業者がその個人データを処理する国についても開示する必要があります。

ウェブサイトのホスティング

サプライヤー様がウェブサイトをホストしている場合、プロファイルオプションを選択し、Microsoft に変わってポータル、オンラインサービス、モバイルアプリケーションなどを提供します。

「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。

ヘルスケア

サプライヤー様が保護対象保健情報を処理する必要がある場合には、このプロファイルオプションを選択してください（定義については DPR を参照してください）。

「**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。

人工知能（AI）システム

サプライヤー様が AI システムに関連するサービスを Microsoft に提供する場合、このプロファイルオプションを選択し、たとえば、AI テクノロジーを備えたツール、システム、またはプラットフォームを使用して、画像、音声、ビデオ、インサイト、分析情報、テキストなどのまったく新しいコンテンツを作成するためにインテリジェントシステムをトレーニングし構築します。これは、AI システムのパブリッシャー（所有、管理、制御など）にのみ適用されます。Microsoft との関わりが、Microsoft Copilot または、貴社がパブリッシュしておらず、下請け業者でもないサードパーティの AI（定義については DPR を参照してください）の利用のみである場合は、プロフィールでこの質問に「いいえ」と答えることができます。

SSPA AI システム承認には、個人データや Microsoft 機密データの処理、人、組織、社会への影響、適切なサプライヤー認定の受け入れに関するドキュメントなどが含まれます。サプライヤー様は、購入が続行される前に、必要な署名済み契約を含め Microsoft サプライヤー データ保護要件の責任ある AI 関連項目および/または Microsoft 内部レビューを完了しします。AI システ

ムを提供するすべてのサプライヤー様には、独立保証のオプションを提供していただきます。DPR のセクション K に対するコンプライアンスを検証するために ISO 42001 は任意で提供していただけますが、AI センシティブである場合には**必須**となります。DPR のセクション K に対する独立評価を受けるサプライヤー様の場合、独立評価は優先評価者（リストはこちら）が行う必要があります。

この承認は、独立評価が SSPA に認められてはじめて付与されます。

SSPA 処理概要

SSPA とは？

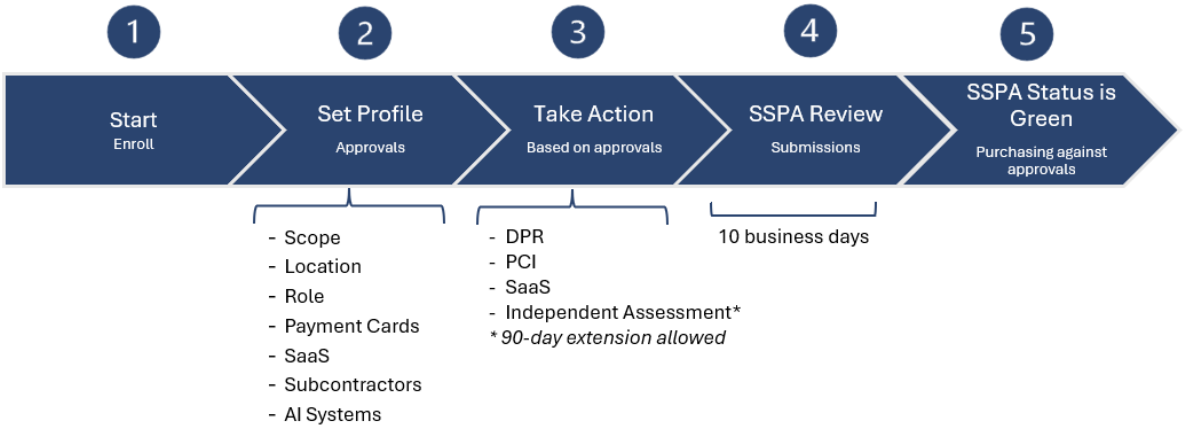
Microsoft は、プライバシーは基本的な権利であると考えます。私たちは、世界中の人々とあらゆる組織がより多くことを成し遂げる支援をするというミッションのために、お客様の信頼の獲得と維持に日々努めています。

強力なプライバシーおよびセキュリティ対策は、Microsoft のミッションにとっても、お客様からの信頼を得るためにも不可欠であり、法域によってはこのような対策は法律で義務付けられているものです。Microsoft のプライバシーおよびセキュリティポリシーに定められた基準は、Microsoft の企業としての価値観を反映しており、この基準は Microsoft に代わって当社のデータを処理する（貴社のような）サプライヤー様にも適用されます。

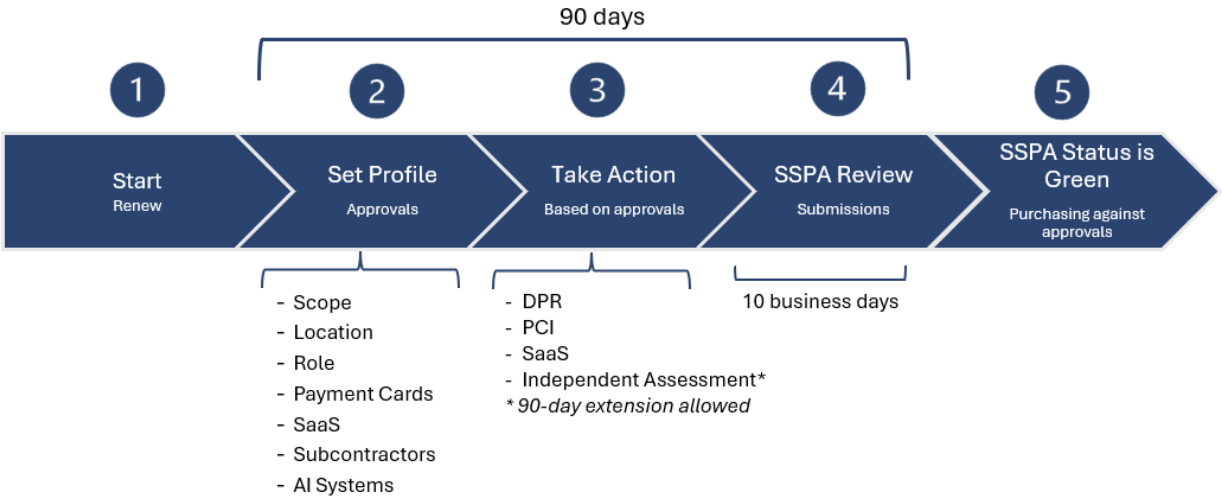
SSPA の主要なデータ保護要件は DPR で定義されています。プログラムの詳細については、よくある質問（FAQs）をお読みいただき,当社のグローバルチーム SSPAHelp@microsoft.com までお問い合わせください。

DPR は年次の要件です。コンプライアンス活動により、SSPA のステータスが緑（準拠）または赤（非準拠）に決定されます。サプライヤー様との関与に先立ち、Microsoft の購買ツールにより SSPA のステータスが緑であることを（SSPA の対象となる各サプライヤーに対して）検証します。

SSPA プロセスダイアグラム - 新規サプライヤーの登録



SSPA プロセスダイアグラム - サプライヤーの年次更新



保証要件

データ処理プロファイルでサプライヤー様が選択された承認は、SSPA において、Microsoft とサプライヤー 様が関与する業務全体のリスクレベル評価に役立ちます。SSPA のコンプライアンス要件は、データ処理プロファイルおよび関連する承認に基づいて異なります。

DPR 準拠に関する自己認証

SSPA に登録されているすべてのサプライヤー様は、要請を受けてから 90 日以内に、DPR への準拠に関する自己認証を完了する必要があります。この要請は毎年行われますが、データ処理プロファイルが年度の途中で更新された場合は、その頻度が高くなる可能性があります。90 日の期間を過ぎると、サプライヤーアカウントの SSPA ステータスが 赤（非準拠）に変更されます。SSPA ステータスが緑（準拠）になるまで、新規の発注は処理できません。

新規に登録されたサプライヤー様は、関与する業務の開始前に SSPA のステータスが緑（準拠）になるように、発行された要件を満たさなければなりません。

重要: SSPA チームには、このタスクの期限を延長する権限がありません。

サプライヤー様は、データ処理プロファイルに従って発行された、適用されるすべての DPR 要件に対応していただく必要があります。発行される要件の中には、Microsoft にサプライヤー様が提供する製品やサービスに該当しないものが含まれる場合があります。こうした要件には、SSPA レビュー担当者が確認できるよう、詳細なコメントともに「適用外」というマークを付けることができます。

提出される DPR は、SSPA チームによってレビューされ、発行された要件に対して「適用外」、「現地法に抵触」、「契約に抵触」のいずれかに分類されます。SSPA チームは、1 つ以上の選択項目に関して説明を求めることがあります。現地法や契約との抵触は、裏付けとなる関連資料が提供され、抵触していることが明らかである場合にのみ認められます。

自己認証を作成する権限のある正式な代表者は、それぞれの要件に確実に対応できるようにするため、主題の専門家から十分な情報を得る必要があります。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。DPR のセクション J を満たすには、別のセキュリティ連絡先が必要であり、貴社が関与するセキュリティインシデントが発生した場合には、支援を求められる場合があります。 サプライヤー様は、要件を完了させる支援を受けるため、オンラインツールにその他の連絡先を追加することができます。

正式な代表者（DPR の定義を参照）は以下を行います：

1. 適用される要件を決定する。
2. 該当する各要件に回答を入力する。
3. Microsoft サプライヤーコンプライアンスポータルで証明書に署名して送信する。

重要: 遵守の証明書を立証するために、SSPA が、特定のデータ保護要件の順守の証拠について協力を求める場合があります。さらに、サプライヤー様は、年間のコンプライアンス サイクル

以外でも、Microsoft サプライヤー データ保護要件に記載されている証拠を提供するよう求められる場合があります。これは、独立評価タスクを受けていない企業にのみ適用されます。

独立評価の要件

付録 A の「SSPA データ処理プロフィール表での承認別の要件」を参照し、この要件が該当するデータ処理の承認を確認してください。

サプライヤー様は、データ処理プロファイルを更新することにより、承認項目を変更することができます。ただし、データ処理の役割が「サブプロセッサー」である場合、この承認を変更することはできないため、独立評価を毎年実施する必要があります。

コンプライアンスの独立検証が必要な承認を確実にするには、サプライヤー様は DPR に対するコンプライアンスを検証する、独立した査定人を選定する必要があります。独立査定人は、Microsoft にコンプライアンスの提供を保証するための意見書を作成します。この意見書は無条件のものであり、SSPA チーム レビューのために Microsoft サプライヤーコンプライアンスポータルに当該意見書が提出される前に、非準拠の問題がすべて解決され、修正されていなければなりません。**独立査定人は、こちらから入手可能な「望ましい査定人」の PDF に添付されている承認済みの意見書テンプレートをダウンロードすることができます。**

SSPA データ処理プロファイルテーブル では、DPR への準拠を検証するために独立査定人を選出せずに証明書の承認を得る別の方法も説明しています（SaaS サプライヤー、ウェブサイトホスティングサプライヤー、下請け業者に委託するサプライヤーに該当する場合に適用できます）。ISO 27701（プライバシー）、ISO 27001（セキュリティ）、AI システムに関する ISO 42001（DPR セクション K）は、DPR への密接な対応を提供するものとして信頼されています。DPR セクション J（セキュリティ）については、SOC 2 報告書にセキュリティ信頼性基準を付したものであっても、資格の記載がない場合は受理することができます。

サプライヤー様が米国内の医療機関または対象事業者である場合、当社はプライバシーおよびセキュリティの適用範囲について HITRUST レポートを受け入れます。

SSPA では、標準的な状況を超える環境で追加の適正評価が必要になった場合に、データ処理プロファイルに関係なく独立評価を必要とすることがあります。例えば、プライバシーまたはセキュリティ、データインシデント修復の検証、サイクルレビュー以外の SSPA チーム、自動化されたデータ主体権の実施に関する要件ごとに要請される場合があります。

この要求事項へ取り組むためのガイダンス：

1. 証明業務は、コンプライアンスを適切に評価するための十分な技術的トレーニングと対象関連の知識を有する査定人によって実施される必要があります。
2. 査定人は国際会計士連盟（IFAC）または米国公認会計士協会（AICPA）に所属しているか、適用される場合は、ISO 27001、ISO 27701 および ISO 42001 に対する認定 ISO 監査員か、あるいは国際プライバシー専門家協会（IAPP）や情報システム監査コントロール協会（ISACA）などの関連するプライバシー/セキュリティ機関から認定されている必要があります。

3. 査定人は、各要件を立証するために必要な証拠を含む最新の DPR を使用する必要があります。**サプライヤー様は、承認された最新の DPR 証明書の回答を査定人に提出する必要があります。**
4. エンゲージメントの範囲は、要請を受け取ったサプライヤーアカウント番号に関して実行されるデータ処理アクティビティの範囲内に限定されます。サプライヤー様が一度に多数のサプライヤーアカウントを評価することを選択する場合、**証明書には、評価に含まれるサプライヤーアカウントのリストを含める必要があります。**
5. SSPA に提出する書面に、サプライヤー様がデータ保護要件を満たすことができないという言及が含まれないようにしてください。これらの問題については、書面を提出する前に修正しなければなりません。

SSPA では、利用可能な推奨査定人のリストを有しており、これらの査定会社は SSPA 評価の実施に精通しています。この評価費用は、データ処理の規模や範囲によって異なるため、サプライヤー様が負担するものとします。

追加独立保証が必要なプロファイル：

サービスとしてのソフトウェア（SaaS）

データ処理プロファイルに含まれる SaaS の定義を満たしたサプライヤー様は、Microsoft クラウドサービス契約で要求される場合、有効な ISO 27001 証明書の提供を求められる場合があります。データセンターの証明書を提出する必要はありません。当社は貴社と Microsoft との契約書に記載されているソフトウェアサービスに適用される ISO 27001 の認証を求めます。

SSPA の審査担当者は、提出された書類が契約上の義務を満たしているかを検証します。

AI システム

センシティブな使用がサービスの提供内容に含まれる場合、ISO 42001 証明書が必要になります。また、独立評価タスクのセクション K に対して ISO 42001 を提出しても構いません。

データインシデント

サプライヤー様がプライバシーまたはセキュリティデータに関するインシデントに気付いた場合、DPR の規定に従って Microsoft に報告する義務があります。

SupplierWeb または SuppIR@microsoft.com にデータインシデントを報告してください。

以下の点を必ず記載してください。

- データインシデントの日付
- サプライヤー名
- サプライヤー番号
- 報告を行った Microsoft の連絡先

- 関連する PO（該当する場合/利用可能な場合）
- データインシデントの概要