Microsoft の調達

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 8

2022 年 6 月

はじめに

Microsoft では、プライバシーは基本的な権利であると考えています。世界中の人々とあらゆる組織が、より多くの成果を達成する支援をするというミッションを実現するために、私たちは日々、お客様の信頼を獲得し、維持するために努力しています。

徹底したプライバシーおよびセキュリティ対策は、当社のミッションにとっても、お客様の信頼を得るためにも不可欠であり、法域によっては法律で実施が義務付けられています。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 の企業価値観を反映しており、この基準は当社に代わって Microsoft 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ています。

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。 SSPA on Microsoft.com/Procurement.なお、サプライヤーは SSPA の外部でサプライヤーとの契約を担当する Microsoft グループにより決定され、通知される組織レベルの追加要件を満たさなければならない可能性がありますのでご留意ください。

主要な SSPA のデータ保護要件は DPR で定義されています。このプログラムの詳細については、 よく寄せられる質問 (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。

SSPA プログラム概要

SSPA は、サプライヤー様が Microsoft のプライバシーとセキュリティの原則を遵守するため、Microsoft Procurement、Corporate External and Legal Affairs、および Corporate Security 間のパートナーシップです。

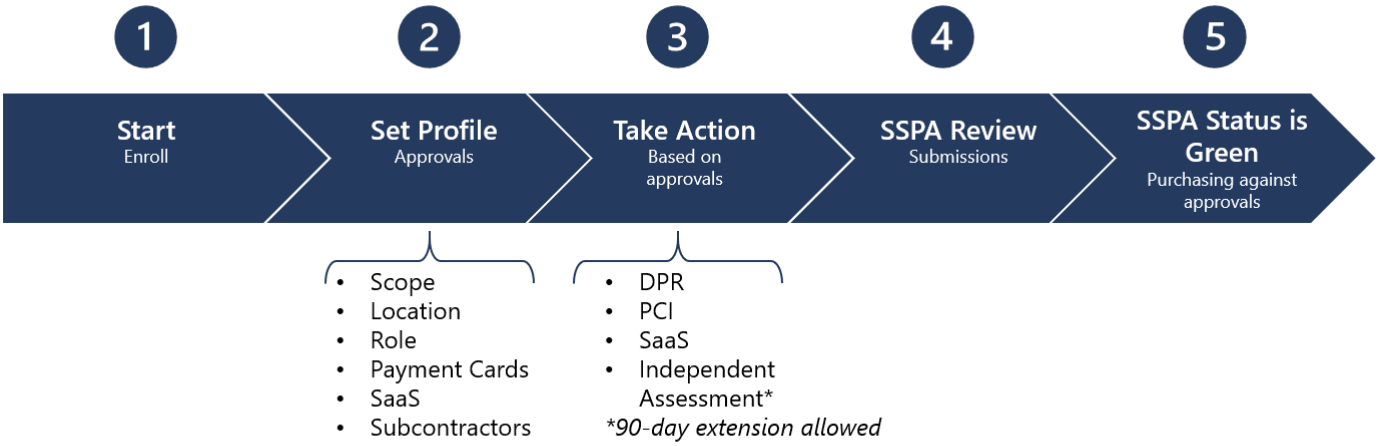
SSPA は、サプライヤー様の業務の実施 (サービスの提供、ソフトウェア ライセンス、クラウド サービスなど) に関連した個人データまたは Microsoft 秘密データを処理する、世界中のすべてのサプライヤー様に適用されます。サプライヤー様の業務は、マイクロソフトとの契約条件 (発注書条件、基本契約書など) に基づき実施（「**実施する**」、「**実施中**」、または「**実施**」) されます。

サプライヤー様は SSPA を利用して、契約している商品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することができます。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。

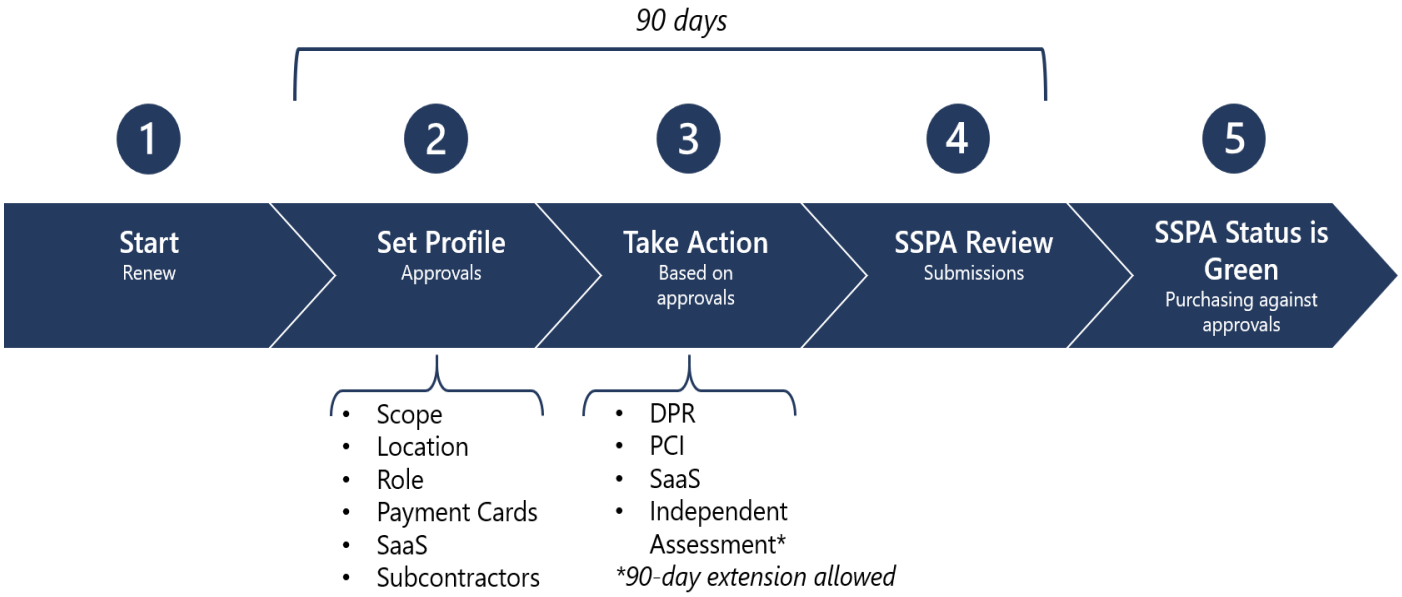
登録されているすべてのサプライヤー様は、DPR に対するコンプライアンスの自己証明書を毎年提出することになります。貴社のデータ処理プロファイルにより、すべての DPR が実施されるか、要件の一部のみが適用されるかが決まります。Microsoft がリスクが高いと見なしているデータを扱うサプライヤー様の場合、独立したコンプライアンス検証といったさらなる要件に対応しなければならないことがあります。また、Microsoft のサブプロセッサリストに掲載されているサプライヤー様は、独立したコンプライアンス検証の提供も求められます。

重要 コンプライアンス活動により、SSPA のステータスが Green(緑-準拠）または Red(赤-非準拠）に決定されます。Microsoft の発注ツールは、契約を進める前に、SSPA のステータスが Green 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



SSPA の範囲

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どうかを判断する際は、以下の表にある用例のリストをご参照ください。これらは一部の例であり、完全なリストではないことにご留意ください。
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た上で、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：

秘密データ
未成年者に関連するデータ
遺伝子情報、生体情報、健康情報
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
個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
顧客のコンテンツデータ
文書、写真、動画、音楽など
製品またはサービスについてのレビューまたは評価
アンケートへの回答
閲覧履歴、関心、お気に入り
手書き入力、タイピング、音声発話（音／音声または／チャット／ボット）
認証情報データ（パスワード、パスワードのヒント、ユーザー名、本人確認に使用される生体情報など）
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
大まかな位置情報
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、連絡先および緊急連絡先などの情報
不正およびリスクアセスメント、バックグラウンドチェック
保険、年金、福利厚生詳細
応募者の履歴書、面接時の記録およびフィードバック
Metadata and telemetry
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
投資または費用データ
コーポレートカード
エンドユーザーの偽名情報(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 が作成した識別子)
グローバルー意識別子(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

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

データクラス別 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。*
発売前の 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
秘密
Microsoft の代理として、あらゆる方法で販売された 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発売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（プロセスガイドまたは手順書、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記載を求めることができます。

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制御することができます。

これにより、サプライヤー様は、どのエンゲージメントを実行する対象とするかを決定することができます。選択項目に十分な注意を払い、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アクティビティを検討してください。**後述の「アシュアランス要件」のセクションおよび付録 A をご参照ください。**

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、契約を作成することができます。

サプライヤーは、**オープンタスクがない場合**、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るので、承認を取得する前に完了させる必要があります。新たに発行される要件が完了するまでは、既存の完了した承認が適用されます。

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 Red(赤-非準拠）になり、アカウントが Microsoft Accounts Payable システムから無効化されるリスクがあります。

データ処理の承認	
1	データ処理の範囲 ▪ 機密 ▪ 個人、秘密
2	データ処理の場所 ▪ Microsoft または顧客 ▪ サプライヤー
3	データ処理の役割 ▪ 管理者（独立した管理者または共同管理者） ▪ 処理業者 ▪ サブプロセッサ(Microsoft 指定)
4	ペイメントカード処理 ▪ 該当 ▪ 該当なし
5	サービスとしてのソフトウェア ▪ 該当 ▪ 該当なし
6	下請け業者への委託 ▪ 該当 ▪ 該当なし

承認に関する留意点

データ処理の範囲

機密

サプライヤー様が Microsoft 秘密データの処理のみを実施する場合は、この承認を選択してください。

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、この承認を選択してください。

処理の場所

Microsoft または顧客

スタッフが *@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、サプライヤー様がデータ処理を含む実行を行なう場合は、この承認を選択してください。

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 指定の海外施設 (OF) を管理している場合。
- サプライヤー様がマイクロソフトに人員を提供し、それらの人員が時おりマイクロソフト ネットワークを使用する場合。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。

サプライヤー様側で
「Microsoft または顧客」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てください。

データ処理の役割

管理者（独立した管理者および共同管理者が該当します）

サプライヤー様で実施する**すべての**局面が、管理者データ処理の役割の定義（DPR を参照）を満たす場合、この承認を選択してください。

この承認を選択した場合、「処理業者」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と管理者の両方である場合、「管理者」ではなく、「処理業者」を選択してください。

処理業者

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。処理業者の定義を DPR でご確認ください。

サブプロセッサ

二次処理業者とは、Microsoft が処理業者である Microsoft 個人データの処理を含む業務を行なうために、Microsoft が契約している第三者です。Microsoft のサブプロセッサは、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、サプライヤー様が自称することはできません。Microsoft がデータ処理者であり、サプライヤー様が適格なエンタープライズパーソナルデータタイプを処理する場合、サプライヤー様はサブプロセッサになることができます。サブプロセッサは、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を持つことになります。（下記参照）

ペイメントカード処理

サプライヤー様がマイクロソフトに代わって処理するデータに、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、この承認を選択してください。

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携わることができるようになります。

ソフトウェア

Microsoft の調達は、すべてのべてのソフトウェア購入に関するインテークプロセスをバイヤーに指示します。これには、ソフトウェアを提供するサプライヤー様が SSPA 管理の対象であるかどうかを決定するための SSPA トリアージを含む様々なチェックが含まれます。(Microsoft のバイヤーは、詳細な手順を社内の ProcureWeb ソフトウェアおよびクラウドサービスのページで確認することができます)。SSPA が必要な場合、サプライヤー様は「サービスとしてのソフトウェア」（SaaS）プロファイルの選択が適用されることも確認する必要があります。SSPA に登録されているサプライヤー様は、Microsoft サプライヤーコンプライアンスポータルでデータ処理プロファイルを完了するときにこの確認を行うことができます。

SSPA に準拠するため、SaaS を PaaS（サービスとしてのプラットフォーム）、IaaS（サービスとしてのインフラストラクチャー）と広義に考えてください。(SaaS の詳細については、こちらの説明をご参照ください。)

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、利用することができるサービスです。

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、使用量に応じた支払い、または使用指標に基づくサブスクリプションとして定義しています。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で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。

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、この承認を選択してください。（定義については DPR をご参照ください）

下請け業者にはフリーランサー（DPR をご参照ください）も含まれます。

アシュアランス要件

プロファイルの承認に基づく要件

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 様との契約のリスクレベルをデータ処理の観点から評価するのに役立ちます。SSPA のコンプライアンス要件は、データ処理プロファイルと関連する承認に基づいて異なります。このセクションでは、さまざまな SSPA 要件について説明します。

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。

アクション:付録 A で承認プロファイルを探して、該当する場合はアシュアランス要件と独立アシュアランスのオプションを確認してください。

重要プロファイルにサービスとしてのソフトウェア（SaaS）、下請け業者、Web サイトホスティング、またはペイメントカードが含まれている場合は、追加のアシュアランスが必要になります。

DPR に準拠している自己証明

SSPA に登録されている全てのサプライヤー様は、要請を受けてから 90 日以内に DPR に準拠している自己証明を作成する必要があります。この要請は年に 1 回行われますが、データ処理プロファイルが年度途中で更新された場合は、頻度が多くなる可能性があります。90 日間を過ぎると、サプライヤーアカウントの SSPA ステータスが Red(赤-非準拠）に変更されます。SSPA ステータスが Green (緑-準拠）になるまで、新規の発注は処理されません。

新規に登録されたサプライヤー様は、契約の開始前に SSPA のステータスを Green(緑-準拠）にするために、承認対象として選択した項目ごとに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。

自己証明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。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いつでも連絡先を追加することができます。

正式な代表者 (定義を参照) の任務は次のとおりです。

1. どの要件が適用されるかを判断する。
2. 該当する要件ごとに回答を入力する。
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。

適用性

サプライヤー様は、データプロセシング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は当てはまらないものが一部ある場合があります。こうした要件には、SSPA レビュー担当者が確認するために、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できます。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。

独立評価の要件

付録 A 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」である場合、この承認を変更することはできませんので、毎年独立評価を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、サプライヤー様は独立査定人を選出し、DPR に対するコンプライアンスを検証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準備します。この意見書は問題なしと判定されている必要があり、準拠していない問題はすべて解決され、修正されてから、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確認書を提出し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「Preferred Assessors List」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。

付録 A 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）。ISO27701（プライバシー）および ISO27001（セキュリティ）は、DPR に密接に対応している解析を提供するものとして信頼されています。

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、独立評価を手動で実施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、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、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 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. 新たに登録したサプライヤー様の場合、査定人は処理統制の整備状況を調査します。その他すべての場合において、査定人は統制の有効性をテストします。
5. 評価エンゲージメントの範囲は、サプライヤー業務の実施に関連した Microsoft 個人データまたは Microsoft 機密データに限定されます。
6. 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と関連所在地のリストを含める必要があります。**
7. 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、利用できる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。

PCI DSS 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。マイクロソフト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）をご参照のうえ、評議会が定める要件をご確認ください。

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。

SaaS 要件

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。

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。

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 ISO27001 の認証を求めます。

下請け業者への委託：

下請け業者への委託は、リスクが高い要因の 1 つと見なされます。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は、それらの下請け業者を通知する必要があります。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も開示する必要があります。

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。関連する定義については、付録 B を参照してください。

サプライヤーウェブまたはこちらの電子メールにデータインシデントをご報告ください。
SuppIR@microsoft.com

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:
- マイクロソフトの通知先：
- 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：

付録 A

プロファイルの承認に基づく要件

#	プロファイル	アシュアランス要件	独立アシュアランスオプション
1	範囲：個人、機密 **処理の場所**：Microsoft または顧客 **処理の役割**：処理業者または管理者 **データクラス**：秘密**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 **ウェブサイトのホスティング**：該当なし	DPR に準拠している自己証明	
2	**範囲**：機密 **処理の場所**：サプライヤー様側で **処理の役割**：該当なし **データクラス**：**秘密** **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	DPR に準拠している自己証明	
3	範囲：機密 **処理の場所**：サプライヤー様側で **処理の役割**：処理業者 **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	DPR に準拠している自己証明 **および** 第三者によるコンプライアンス独立アシュアランス保証	第三者独立アシュアランスのオプション： 1. DPR に対する第三者評価を完了する**、または** 2. ISO27001 を提出する

#	プロファイル	アシュアランス要件	独立アシュアランスオプション
4	**範囲**：個人、機密 **処理の場所**：サプライヤー様側で **処理の役割**：処理業者 **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	DPR に準拠している自己証明 **および** 第三者によるコンプライアンス独立アシュアランス	第三者独立アシュアランスのオプション： 1. DPR に対する独立評価を行なう 2. DPR のセクション A～I および ISO27001 に照らした独立評価、**または** 3. ISO27701 **および** ISO27001 を提出する
5	**範囲**：個人、機密 **処理の場所**：サプライヤー様側で **処理の役割**：処理業者 **データクラス**：**秘密** **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	DPR に準拠している自己証明	
6	**範囲**：個人、機密 **処理の場所**：サプライヤー様側で **処理の役割**：管理者 **データクラス**：極秘または秘密 **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	DPR に準拠している自己証明	

#	プロファイル	アシュアランス要件	独立アシュアランスオプション
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（この役割はマイクロソフト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：承認」と表示されます） **データクラス**：極秘または秘密 **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	DPR に準拠している自己証明 **および** 第三者によるコンプライアンス独立アシュアランス	第三者独立アシュアランスのオプション： 1. DPR に対する独立評価を完了する 2. DPR のセクション A～I および ISO27001 に照らした独立評価、**または** 3. ISO27701 **および** ISO27001 を提出する

#	プロファイル	アシュアランス要件	独立アシュアランスオプション
SaaS、下請け業者、ウェブサイトホスティングを追加した場合の影響			
8	**範囲**：個人、機密 **処理の場所**：サプライヤー様側で **処理の役割**：処理業者 **データクラス**：極秘 または秘密 **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	DPR に準拠している自己証明 **および** 第三者によるコンプライアンス独立アシュアランス	第三者独立アシュアランスのオプション： 1. DPR に対する独立評価を完了する 2. DPR のセクション A～I および ISO27001 に照らした独立評価、**または** 3. ISO27701 **および** ISO27001 を提出する
9	**範囲**：個人、機密 **処理の場所**：サプライヤー様側で **処理の役割**：管理者 **データクラス**：極秘または秘密 **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	DPR に準拠している自己証明	

#	プロファイル	アシュアランス要件	独立アシュアランスオプション
クレジットカードと SaaS 向けの追加アシュアランス			
10	上記のいずれかのプロファイルと**クレジットカード**	適用される上記の要件**および**ペイメントカード業界のアシュアランス	PCI DSS 認証を提出
11	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羅した ISO27001 の認証書を提出してください。