Microsoft

先手必勝！

いち早く

基礎から学ぶ

GDPR

早分かりガイドブック

GDPR って何？

うちは対応しなければならないの？

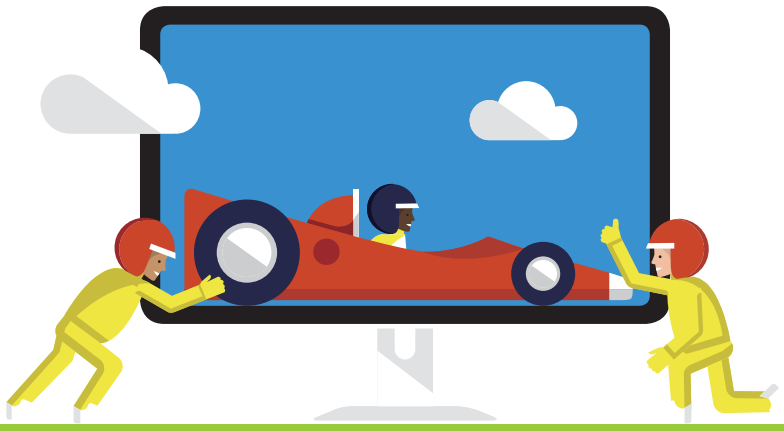
INDEX

※GDPR（General Data Protection Regulation）：EU 一般データ保護規則

全体監修：ギブソン・ダン・クラッチャー法律事務所 ブリュッセルオフィス オブ・カウンセル 弁護士

杉本武重氏

目前に迫る
GDPRの
適用開始、
対応準備は
万全ですか



はじめに

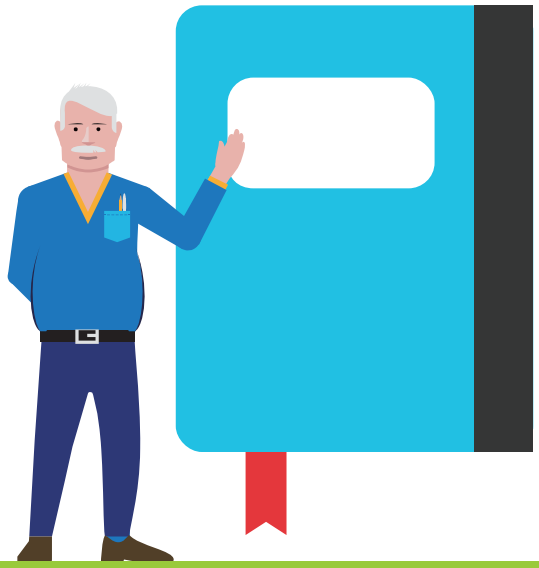
本冊子は GDPR の基本的な内容と対応が必要となる主なケースについて、分かりやすく解説したガイドブックです。

2018 年 5 月 25 日より、欧州連合 (EU) における
新しい個人データ保護法である
GDPR（ General Data Protection Regulation：EU 一般データ保護規則 ）が適用開始となります。

GDPR は対象となる個人データの取り扱い場面が広く、
またビジネス規模や企業規模に関わらず適用の対象となるため、
大企業だけでなく中小企業の皆様もその内容を正しく理解し、適用対象となる場合には、
適切な対策を講じておく必要があります。

GDPR の対象となる企業が対応を怠った場合、
気付かないうちに GDPR 違反を起こし、
制裁金が課せられる恐れがあります。

本冊子は “先手必勝でいち早く GDPR を基礎から学ぶ” ために、
基本的な GDPR の内容と対応方法について
分かりやすく解説したもので、
日本国内全ての企業経営者／管理者／従業員の
皆様のお役に立つガイドブックです。



■注意事項
・本冊子は 2017 年 11 月現在のものです。
・本書は一般的な情報提供の目的で作成されたものであり、
法的アドバイスの提供を目的とするものではありません。

そもそも GDPR って何

GDPR は 2018 年 5 月 25 日に適用開始となる欧州連合 (EU) の
新しい個人データ保護法です。
組織の所在地に関係なく適用され、日本企業の
多くも適用対象になることが予想されます。

GDPR は、欧州経済領域 (European Economic Area：EEA）における個人データの扱いに関する新たなルールで、その内容は、個人の個人データ保護に対する権利を“基本的人権の 1 つ”であると位置づけ、これを保護することに主眼を置いたものとなっています。
また GDPR では EEA 域内に事業所を持つ企業だけでなく、EEA 所在者に商品・サービスを提供する企業、（受託業務も含めて）EEA 所在者に結び付くデータの収集・分析を行う企業も対象なり、その組織の所在地に関係なく適用されることになります。

ここが POINT

**GDPR では個人の
個人データ保護に対する権利は
“ 基本的人権 ”、法律も厳しく
解釈され、適用される！**

今、なぜ、GDPR

EEA 全体で個人データ保護に関する取り組みを、
さらに強化するためです。

EEA にはいわゆる個人情報保護法として 1995 年から適用開始された EU データ保護指令がありますが、国内法の策定は EEA 各国に委ねられ、法律の内容も国によって異なるという問題点があると言われていました。
そこで 2016 年 4 月 14 日、個人データ保護に関する EEA 全体での取り組みを強化するために欧州議会で正式に採択されたのが GDPR で、2018 年 5 月 25 日からの適用開始が決定されました。

ここが POINT

**EEA 内の組織だけでなく、
日本企業の多くも
適用対象になる！**
→ P8 へ

注意点！

GDPR への移行で、EEA 域内で個人データを取り扱う組織には、新たな義務が多々発生する！

EU データ保護指令から GDPR への移行に際して、最も特筆すべき変更点は、GDPR では、個人が自分の個人データをより強力に制御できるようになるため、個人データを収集、処理、または分析する組織に、新たに多くの義務が課せられるようになることです。
また GDPR では、EEA 加盟国のデータ保護監督当局に、法律に違反した組織に多額の制裁金を科する、より強力な権限が付与されることになり、GDPR に違反した企業・組織には、非常に高い制裁金が科せられる可能性があります。

GDPR では、具体的に何を定めているの

GDPR では EEA 域内で行う個人データの「処理」と、
EEA 域外の第三国に個人データを「移転」するために
順守すべき法的要件を定めています。

GDPR でいう個人データの「処理」とは、個人データまたは個人データの集合に対して行われる単一もしくは一連の作業を指し、「移転」については特に規定されていませんが、実際には EEA 域外の第三者に個人データの閲覧を可能にする行為だと言うことができます。

ここが POINT

**GDPR は EEA 域内における
個人データの「処理」と「移転」に関する
法的要件を定めたもの**

GDPR における「個人データ」って、どんなもの

「識別された自然人（＝データ主体）」または
「識別可能な自然人」に関連する
あらゆるデータが該当します。

端的に言えば、個人の特定に繋がるデータは全て「個人データ」として見なされるということです。「個人データ」は非常に広義に解釈できるため、一見個人的な情報には見えない情報も含まれる場合があります。
例えば人物を含まない風景写真であっても、その情報が識別可能な個人の口座番号や一意のコードと関連付けられている場合には、個人データと見なされます。
また個人の人種的または民族的出身、あるいは健康状態や性的指向などが明らかになるデータは、特別カテゴリの個人データとして、通常の個人データを処理する場合よりもさらに厳格な規則の対象となるので注意が必要です。

ここが POINT

**個人の特定に繋がる
データは全て
「個人データ」として
見なされる！**

GDPR における「個人データ」の例

- 名前
- 識別番号
- メールアドレス
- オンライン識別子（IP アドレスなど）
- 従業員情報
- 販売データベース
- 顧客サービスデータ
- 顧客フィードバックフォーム
- 位置データ
- 生体認証データ
- CCTV 映像
- ロイヤルティスキームの記録
- 健康診断の結果
- 個人の銀行口座の情報

など

個人データの「処理」って、どういうこと

「個人データ」または「個人データの集合」に対して行われる「単一もしくは一連の作業」を指します。

GDPR における個人データの「処理」の例

・クレジットカード情報の保存
・メールアドレスの収集
・顧客の連絡先詳細の変更
・顧客の氏名の開示
・上司の従業員業務評価の閲覧
・データ主体のオンライン識別子の削除
・全従業員の氏名や社内での職務、事業所の住所、写真を含むリストの作成

など

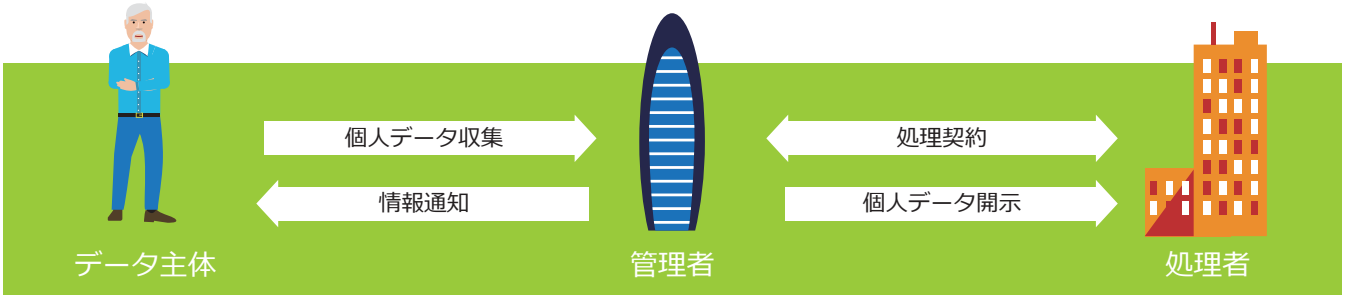
個人データの「移転」についても、教えて

GDPR での明確な定義はありませんが「EEA 域外の第三国の第三者」に「個人データの閲覧を可能にする行為」だと言えます。

GDPR における個人データの「移転」の例

・個人データを含んだ電子形式の文書を電子メールで EEA 域外に送付すること　など

GDPR における「個人（=データ主体）」－「管理者」－「処理者」の関係



●管理者：個人データの処理の目的・手段を決める者　●処理者：管理者の委託に基づき、管理者が決定した処理の目的・手段に従って個人データを処理する者
※管理者自らが処理行為を行い、管理者と処理者が一致する場合もある。

注意点！

GDPR に違反した企業は、様々なリスクに直面することになる！

GDPR の深刻な違反に対しては、多額の制裁金が科せられることになる可能性があり、また GDPR に違反した組織に対しては、消費者および消費者の代表組織が損害賠償請求訴訟をまとめて提起できる権利が新たに与えられることになります。自社が GDPR の対象となるのか、対象となる場合にはどんな取り組みが必要なのかを十分に理解して、対応準備を進める必要があります。　→GDPR 適用対象の詳細は P7 ～ 9 へ

どんな企業が GDPR の適用対象となるの

規模／業種／所在地に関係なく、
EEA 域内の個人データを処理／移転しようとする企業は
全て GDPR の適用対象となります。

GDPR は非常に広範囲にわたって適用されます。 EEA 域内に事業所を持つ企業に加え、EEA 所在者に商品・サービスを提供する企業、EEA 所在者に結び付くデータの収集・分析を行う企業（受託業務を行う企業も含む）など、EEA 域内の個人データを処理／移転しようとする企業は全て GDPR の適用対象となります。

ここが POINT

EEA 域内に子会社や支店を持たない場合でも
EEA 所在者に商品・サービスを提供する際に
個人データを処理する日本国内の企業は
GDPR の適用対象になる！

GDPR の適用対象となる日本企業の例

・EEA 域内に現地拠点（子会社・支店駐在員事務所など）を設置している企業
・EEA 域内に現地拠点は設置していないが、域内で収集した個人データを日本で処理しようとする企業
・EEA 域内の現地拠点の有無に関わらず、域内に個人データ処理用のサーバーやストレージなどの機器を設置している企業
・EEA 域内の現地拠点の有無に関わらず、域内の個人に対して日本から直接、商品やサービスを提供している企業
など

GDPR の適用対象となる処理内容の例

・メールマガジン配信用のデータベースに EEA 域内の個人が含まれる場合
・EEA 域内の従業員に記名式アンケート調査を実施して個人データを取得した場合
・EEA 域内で開催するセミナーの参加者に日本のサーバーを介して受講票を配信した場合
・EEA 域内の販売代理店と個人データが関連する事項について契約した場合
・EEA 域内の現地従業員が作成した提案書
・EEA 域内のクラウド サービスを契約している場合
など

ここが POINT

ユーザ企業からの委託を受けて個人データの処理を行う
IT 企業も GDPR の適用対象になる！

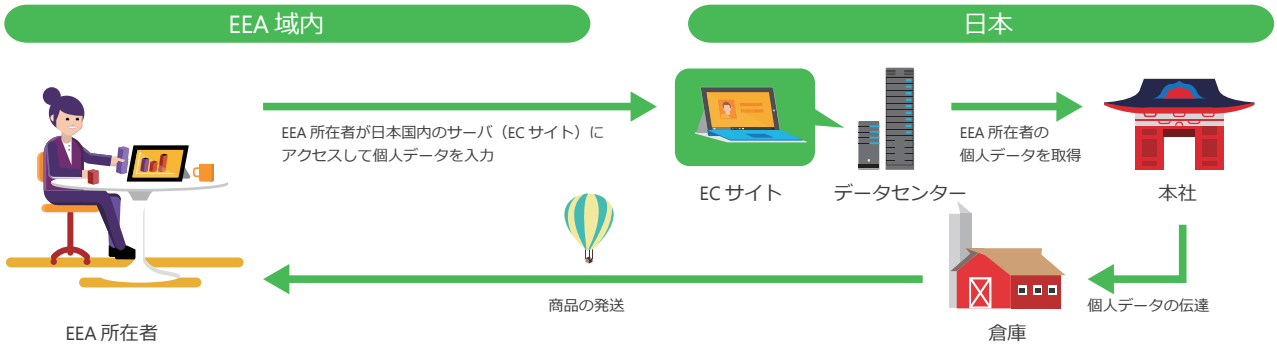
例えばこんな日本企業が GDPR の適用対象になる！

CASE 1 日本国内のサーバーを使って、世界に向けた EC サイトを運営している日本企業

日本国内のデータセンタのサーバーで、あるいは日本国内のサーバーを使って提供されるクラウドサービスを利用して、英語でも注文できる EC サイトを運営している場合、EEA 所在者からも注文を受ける可能性があります。
その際に EEA 所在者は、品物を届けてもらうために自分の氏名や住所などを入力することになりますが、この場合には “ EEA 所在者の個人データが EEA 域外において取得される” ことになります。
今では大企業だけでなく中小規模の企業も、販路拡大のために海外市場をターゲットとした EC サイトを立ち上げて、商品やサービスを販売するケースが増えてきていますが、“うちは EEA 域内に子会社や支店が全く無いから大丈夫” とはならないことを十分に理解しておく必要があります。

ここが POINT

GDPR では「企業所在地」は関係ない！



CASE 2 EEA 域内に駐在員 1 名の現地事務所を設置して、情報収集を行っている日本企業

GDPR では、適用対象となる企業の規模に一切の制限を設けていません。現地法人ではなく、仮に駐在員が 1 名だけの現地事務所を設置している場合でも、その駐在員が現地で情報収集などの活動を行い、その一環として EEA 所在者と名刺交換し、名刺に記載されている会社名や住所、氏名などを現地でデータ化して保存・管理する場合には、GDPR の適用対象となります（＝個人データの処理に相当）。
CASE 1 の例も含めて、GDPR では EEA 域内の個人データを処理／移転しようとする企業全てが適用対象となり、企業の規模や業種、所在地は一切関係ないという点が重要な留意ポイントです。

ここが POINT

GDPR では「企業規模」も関係ない！

GDPR への対応は
優先順位を付けて
制裁リスクの大きいところから！

ここで紹介しているケースはあくまで一例です。本来ならあらゆるケースを想定して網羅的に GDPR 対応を進めることが理想的ですが、そのためには膨大なコストとマンパワーが必要です。
社外の法律事務所やコンサルティング会社の知恵も借りるなどして、自社が GDPR の適用対象となる場合でも、EEA 域内各国のデータ保護監督当局（Data Protection Supervisory Authority）の制裁リスクの大小を踏まえた上で、より優先順位の高いところから対応を進めていくことが現実的です。

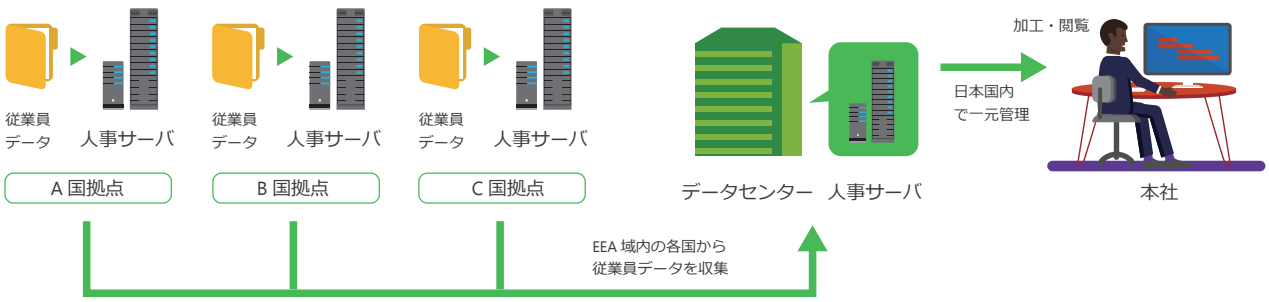
例えばこんな処理・移転が GDPR の適用対象になる！

CASE 1　EEA 域内の従業員データを、日本国内で一元管理する場合

グローバル展開のために世界各国に拠点を置き、併せて最適な人材活用を実現するためにタレントマネジメントを行う企業が増えています。
この時、EEA 域内の従業員データを日本国内のサーバーで保存・管理する場合にはもちろん個人データの「処理」と「移転」と見なされることになります。個人データは顧客関連のものだけではないということを再認識しておく必要があります。

ここが POINT

EEA 域内の従業員データもまた「個人データ」！

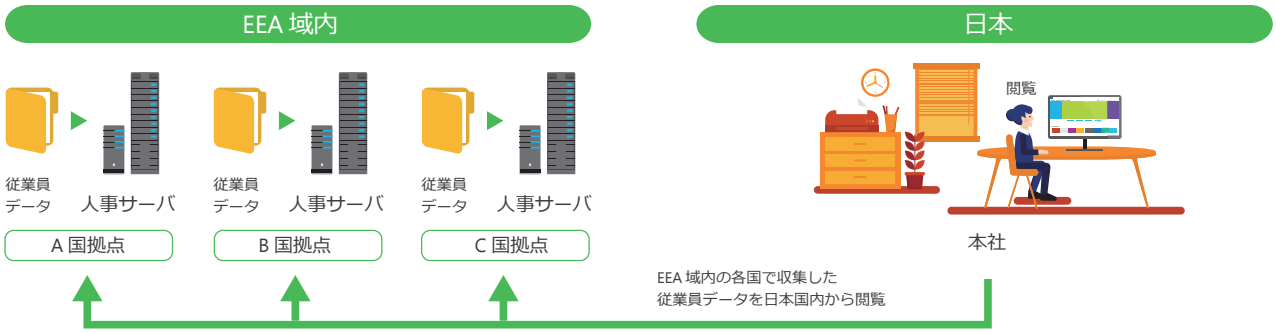


CASE 2　EEA 域内の従業員データを、日本から“閲覧”する場合

GDPR では個人の個人データ保護に対する権利を“基本的人権”と位置付けており、法律も厳しく解釈され、適用されることになります。そのため EEA 域内の従業員データを日本国内に移転し、処理していなくても、インターネットなどを介して日本から域内の従業員データを“閲覧”するだけで、GDPR では個人データの「移転」と見なされます。この場合には現地での GDPR 対応を考えるだけでは片手落ちになるので、十分な注意が必要です。

ここが POINT

日本から個人データを“閲覧”するだけでも「移転」になる！



覚えておこう！ EEA 域内から個人データを域外移転するための「SCC（標準契約条項）」

※ SCC：いわゆる「EU モデル契約条項」のことで、EEA から移転される個人データが GDPR に準拠して転送されるように、移転元企業 – 移転先企業間の契約時に使用される標準化された契約条項

GDPR では、EEA 域内からの個人データの移転を原則として禁止していますが、一定の法的要件を満たした場合に限り、域外への個人データの移転を認めています。その方法の 1 つが、欧州委員会が策定した SCC（Standard Contractual Clauses：標準契約条項）を含む個別のデータ移転契約を、データ移転先の企業と締結することです。
データ移転を行う相手企業と SCC を含む個別のデータ移転契約を結ぶことで、EEA 域内からの個人データの移転を合法的に行うことが可能となります。また、データ輸入者は SCC 上のデータ輸入者の義務に基づいて SCC で移転させる個人データを処理する社内体制を構築する必要があります。

そもそも GDPR って何？

ANSWER

GDPR は 2018 年 5 月 25 日に適用開始となる欧州連合 (EU) の新しいデータ保護法です。組織の所在地に関係なく適用され、日本企業の多くも適用対象になることが予想されます。

POINT

GDPR では個人の個人データ保護に対する権利は“基本的人権”、法律も厳しく解釈され、適用される！

今、なぜ、GDPR ？

ANSWER

EEA 全体で個人データ保護に関する取り組みを、さらに強化するためです。

POINT

EEA 内の組織だけでなく、日本企業の多くも適用対象になる！

GDPR では、具体的に何を定めているの？

ANSWER

GDPR では EEA 域内で行う個人データの「処理」と、EEA 域外の第三国に個人データを「移転」するために順守すべき法的要件を定めています。

POINT

GDPR は EEA 域内における個人データの「処理」と「移転」に関する法的要件を定めたもの

GDPR における「個人データ」って、どんなもの？

ANSWER

「識別された自然人（=データ主体）」または「識別可能な自然人」に関連するあらゆるデータが該当します。

POINT

個人の特定に繋がるデータは全て「個人データ」として見なされる！

個人データの「処理」って、どういうこと？

ANSWER

「個人データ」または「個人データの集合」に対して行われる「単一もしくは一連の作業」を指します。

個人データの「移転」についても、教えて

ANSWER

GDPR での明確な定義はありませんが、「EEA 域外の第三国の第三者」に「個人データの閲覧を可能にする行為」だと言えます。

どんな企業が GDPR の適用対象となるの？

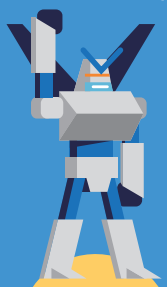
ANSWER

規模／業種／所在地に関係なく、EEA 域内の個人データを処理／移転しようとする企業は全て GDPR の適用対象となります。

POINT

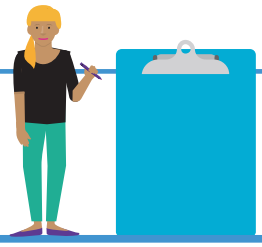
EEA 域内に子会社や支店を持たない場合でも、EEA 所在者に商品・サービスを提供する際に個人データを処理する日本国内の企業は GDPR の適用対象になる！

GDPR 対応は先手必勝！



GDPR 準拠に向けた 4 つのステップ。始めは“個人データの見える化”から。

GDPR は、データを収集／保存／処理する方法において、日本企業に大きな変革を要求する複雑な規定です。
一方で GDPR が、個人データの保護に対する権利やセキュリティ、コンプライアンスについて、
より高い基準を新たに設定するものであることは間違いありません。
日本企業は今から GDPR への対応に取り組むことで、
世界標準のデータ保護対策を、いち早く確立することが可能となります。



まずは自社の“今”をチェック！

- 重要なデータがどこに存在し、誰がアクセスできるのかを把握できているか？
- リアルタイムのリスク評価に基づいたデータのアクセスコントロールができるか？
- 様々な場所やデバイス、アプリケーション間におけるデータに対して、ポリシーベースの分類や保護ができるか？
- データや ID の侵害を自動的に検出することが可能か？またそれらの事象が発生した場合に、適切な対応を取ることができるか？
- データに対する保護のポリシーや手順を、継続的に評価／更新しているか？

言われてみればできていない、もしくは不安を感じたら次のページへ

GDPR 準拠に向けた 4 つのステップ

1 **検出** 保有している個人データを識別し、その保存場所を特定

2 **管理** 個人データの使用方法とアクセス方法を管理

3 **保護** 脆弱性とデータ侵害の防止、検出、および対応を行うセキュリティ制御を確立

4 **報告** 必要な書類を保管し、データ要求と侵害通知を管理

さあ始めましょう！

マイクロソフトの GDPR サイト「Microsoft Trust Center」にアクセスして GDPR への準備状況を今すぐ評価

https://aka.ms/gdpr_jp

■マイクロソフトの GDPR サイト「Microsoft Trust Center」

■GDPR E-book「GDPR が与える影響と準拠に向けた 4 つのステップ」

マイクロソフトの法人向けクラウドサービスの契約書には、「SCC（標準契約条項）」（P9 参照）を含んでいます。またマイクロソフトは、EU から米国へ転送される個人データの収集／使用／保持に関して米国商務省が定める「米国－EU プライバシーシールド フレームワーク」にも準拠しています。

・オンラインサービス条件
https://www.microsoft.com/ja-jp/licensing/product-licensing/products.aspx#OST

GDPR 準拠に向けた対応については 下記パートナーまでご相談ください。

EYアドバイザリー・アンド・コンサルティング株式会社

EY の弁護士、IT 等の専門家が GDPR へのグローバルな支援をワンストップでご提供いたします。

URL	https://www.eyadvisory.co.jp/	お問い合わせ先	AS-Markets@jp.ey.com（または Web のお問い合わせフォームより）

KPMG コンサルティング株式会社

152 ヵ国のグローバルネットワークにより、個人データ保護法制への対応をご支援します。

URL	kpmg.com/jp/cyber	お問い合わせ先	cybersecurity@jp.kpmg.com

PwCコンサルティング合同会社

PwC Global Network で培った GDPR のナレッジおよびメソドロジーを活用した対応策のご支援を提供します。

URL	https://www.pwc.com/jp/ja.html	お問い合わせ先	pwckk.microsoft.team@jp.pwc.com

（掲載順：五十音順）

Microsoft 365 に関する最新情報は、
https://www.microsoft.com/ja-JP/Microsoft-365 をご覧ください。

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■ インターネット ホームページ　http://www.microsoft.com/ja-jp/
■ 日本マイクロソフト株式会社　0120-166-400　営業時間：月曜日～金曜日 9:00 ～ 17:30（祝日除く）

電話番号のおかけ間違いにご注意ください。

Microsoft
日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー