「本契約条件の英語版は**こちら**をご覧ください。日本語版に拘束力があり 英語版は、あくまで参考となります。」

こちら

APEXパートナー向けデータ処理補遺

主契約に付随する本APEXパートナー向けデータ処理補遺（「**パートナー向けDPA**」）は、主契約の両当事者が各自の義務（主契約に基づいたDellによるサービス（「**本サービス**」）の提供を含みます）を履行する過程で個人データを授受する際に適用されるものとします。本パートナー向けDPAと主契約との間に矛盾がある場合、本パートナー向けDPAの対象となる事項に関しては本パートナー向けDPAが優先するものとします。

1. 定義

本パートナー向けDPAで定義されていない用語の意味は、主契約に規定するとおりとします。本パートナー向けDPA内の次の用語の意味は次のとおりとします。

1.1 「主契約」とは、APEX販売店契約、APEXディストリビューター契約、またはDellが本サービスを提供する際に従うこれらに実質的に類似する契約のことをいいます。

1.2 「管理者」とは、単独でまたは他者と共同で、個人データを処理する目的および手段を決定する組織のことをいいます。

1.3 「GDPR」とは、一般データ保護規則（EU）2016/679のことをいいます。

1.4 「モデル条項」とは、次のうち該当するもののことをいいます。

(i) 随時変更または置換される可能性がある、欧州経済領域（「**EEA**」）から第三国への移転に関する、個人データの移転のための標準契約条項（決定 2021/914/EU）

(ii) イギリス（「**英国**」）から英国 GDPR に基づく十分性認定を受けていない国への移転に関して 2018 年データ保護法の第 119A 条に基づいてそれぞれ発行された、データの越境移転のための欧州委員会の標準契約条項に対するデータ越境移転補遺、またはデータ越境移転契約

(iii) 随時変更または置換される可能性があり、2021 年 8 月 27 日にスイス連邦データ保護・情報コミッショナーが公表した改正によりスイス連邦データ保護法に基づく利用について明確に改正された、スイスから第三国への移転に関する、個人データの移転のための標準契約条項（決定 2021/914/EU）

1.5 「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情報、またはプライバシー法において「個人のデータ」または「個人情報」と別途定義されている情報で、両当事者が主契約を履行する際に処理するもののことをいいます。

1.6 「個人データ侵害」とは、本パートナー向けDPAに基づいて処理する個人データの偶発的または違法な破棄、喪失、改ざん、不正開示、および不正アクセスを引き起こすセキュリティ侵害のことをいいます。

1.7 「プライバシー法」とは、主契約の当事者および提供する本サービスに適用されるデータ保護およびプライバシーに関するあらゆる法律のことをいいます。プライバシー法には（適用がある場合）GDPR、英国GDPR、カリフォルニア州消費者プライバシー法（「CCPA」）およびこれらに類似するその他の法律が含まれます。

1.8 「処理」とは、自動的な手段によるものか否かを問わず、個人データまたは個人データ一式について実施する作業または一連の作業で、収集、記録、整理、構造化、保存、翻案、変更、検索、参照、利用、送信による開示、拡散もしくはその他の形態による提供、調整、結合、制限、消去、または破棄などのことをいいます。

1.9 「処理者」とは、管理者の代わりに個人データを処理する組織のことをいいます。

1.10 「販売」とは、金銭またはその他金銭以外の有価約因のために、事業者が他の事業者または第三者に、口頭、書面、電子的手段、またはその他の手段により、消費者の個人情報を販売、賃貸、公表、開示、拡散、提供、移転、またはその他伝

達することをいいます。なお、販売には主契約における両当事者の義務を履行するために開示管理者が受領管理者に個人データを共有または移転することは含まれません。

1.11 「復処理者」とは、本パートナー向けDPAに基づくいずれかの当事者による個人データの処理に関連して、いずれかの当事者が業務に従事させ、処理者として行動する第三者（関係会社もしくは再委託先またはその両方を含みますが、これらに限定されません）のことをいいます。

1.12 「英国GDPR」とは、英国の欧州連合離脱に伴って英国の国内法に基づいて維持されているGDPRのことをいいます。なお、英国GDPRは、随時変更される可能性がある2018年英国データ保護法とあわせて読むものとします。

2. コンプライアンス

両当事者は、主契約において企図されている関係に適用される関連プライバシー法に基づく各自の義務を遵守し、適用されるプライバシー法に従ってのみ個人データを処理することに合意します。各当事者は、個人データを相手方当事者に開示、移転、またはその他の行為により提供する前に、個人データの処理の適法性に関してプライバシー法を遵守する責任を負い、個人データを相手方当事者に開示するために必要なすべての権利および権限を得るものとします。かかる遵守には、適切な通知をすること、および必要に応じて主契約に関連して個人データを開示するために必要な同意を当該個人データのデータ主体から（プライバシー法に従って）得ることが含まれますが、これらに限定されません。

3. 管理者から管理者への移転

管理者として行動する一方の当事者（「開示管理者」）が、同様に管理者として処理する相手方当事者（「受領管理者」）に個人データを開示する場合、次の義務を課すものとします。

3.1 両当事者が書面で別段の合意をしていない限り、受領管理者は、主契約に基づく自己の義務を履行するためにのみ、適用されるプライバシー法に従って、個人データを処理するものとします。プライバシー法が明示的に認めている場合を除き、受領管理者はその他の活動または目的のために個人データを処理してはならないものとします。

3.2 個人データは、受領管理者が主契約に基づく自己の義務を履行することのみを目的として、受領管理者に提供されます。主契約に基づいて本サービスを提供した対価を主契約において合意したとおりに支払うことを除き、開示管理者は、個人データへのアクセスまたは個人データのその他の処理について、金銭およびその他金銭以外の有価約因を提供しません。

3.3 受領管理者がマーケティング情報を送付するために開示管理者が個人データを開示する場合、開示管理者は、かかる開示および受領管理者による利用に対する事前の同意を関連するデータ主体から取得することに同意します。

3.4 データ主体が個人データに関してプライバシー法に基づく自己の権利（同意を撤回する権利、アクセス権、制限権、訂正権、忘れられる権利、およびポータビリティ（携行）権を含みます）を行使することを要求した場合、各当事者は当該要求に応じる義務をすみやかに果たすものとします。受領管理者は、開示管理者またはデータ主体からの個人データに関するすべての合理的な問い合わせにすみやかに応じるものとします。なお、かかる問い合わせには、個人データへのアクセス、個人データの訂正、ならびに受領管理者の実務、手続きおよび苦情申し立てプロセスまたはこれらの一部に関する情報提供の依頼が含まれます。

3.5 当事者が、主契約に基づいて処理された個人データに関して、第三者（データ保護監督機関を含みます）から要求もしくは通知を受けた場合、または裁判所の命令を受けた場合、かかる当事者は、相手方当事者にすみやかに通知し、関連するすべての詳細な情報を提供するものとします。両当事者は、かかる要求または通知に対応するために、合理的に相互協力をするものとします。法律が義務付けている場合を除き、いずれの当事者も相手方当事者に代わって要求および通知に応じてはならないものとします。ただし、当該要求または通知に応じることを相手方当事者が書面で指示した場合は、この限りではありません。

3.6 主契約に関連して個人データ侵害が生じた場合、かかる個人データ侵害に直面した当事者は、かかる個人データ侵害を認識したあと遅滞なく相手方当事者に通知するものとします。個人データ侵害の取り扱い、軽減および解決、またはこれらの一部において、各当事者は相手方当事者に協力し、相手方当事者を支援するものとします。両当事者は、相互に協議した上で、プライバシー法が課している関連する監督機関もしくはデータ主体またはその両方への通知義務を遵守するものとします。

3.7 受領管理者は、主契約の目的のために保持する必要がなくなった場合、または適用法が別途義務付けている場合、主契約の解除後に個人データの消去もしくは破棄またはその両方を行うものとします。

3.8　受領管理者による次の行為を禁止します：（i）個人データを販売すること、（ii）主契約に基づく義務を履行するという明確な目的以外の目的のために個人データを保持、利用および開示すること（主契約の履行以外の商業上の目的のために個人データを保持、利用および開示することを含みますが、これらに限定されません）、ならびに（iii）開示管理者および受領管理者間における直接的な取引関係の外で個人データを保持、利用および開示すること。

3.9　受領管理者は、個人データに関して本パートナー向け DPA（特に第 3.8 条）で概説している利用、ならびにその他すべての処理活動および関連する目的に関する禁止事項および制限を自ら理解していることを表明および保証し、これらを遵守するものとします。

4.　管理者から処理者への移転

管理者として行動する一方の当事者が、相手方当事者に対し、処理者または処理者を代理する復処理者として処理することを目的として個人データを開示した場合、処理者または復処理者として行動する当事者は次のとおりとします。

4.1　適用法が義務付けているものでない限り、管理者の指示のみに従って個人データを処理するものとします。本パートナー向け DPA に記載されていない処理に関する追加の指示または代替的な指示（かかる指示の遵守に関連する費用を含みます）については、両当事者が書面で合意しなければなりません。いずれの当事者も、管理者の指示が適用法に準拠しているか否かを判断する責任を負いません。ただし、管理者の指示が適用のあるプライバシー法に違反しているといずれかの当事者が考える場合、かかる当事者は合理的に実務上可能な限りすみやかに相手方当事者に通知するものとし、かかる違反している指示を遵守する義務を負わないものとします。処理の対象となる事項の詳細、ならびに処理の期間、性質および目的、ならびに個人データの種類およびデータ主体は、主契約および付属書 2 に明記しているとおりとします。

4.2　管理者が提供した個人データを、主契約に基づく自己の義務を履行するために必要な範囲においてのみ、処理するものとします。

4.3　必要である場合かつ目的が次のいずれかである場合を除き、個人データを第三者（関係会社および復処理者は除きます）に開示してはなりません。

（a）管理者の指示に従うため。

（b）本パートナー向けDPAを遵守するため。

（c）法律または行政機関の強制力のある命令に従うため。法律または行政機関の強制力のある命令に違反することにならない限り、処理者は、本規定で言及している法的義務または法的命令を管理者に通知するものとします。

4.4　個人データ侵害を認識したときに、（i）不当に遅滞することなく（ただし、いかなる場合でも72時間以内に）管理者に通知し、（ii）その時点で処理者が知っている範囲、または入手可能な範囲において、個人データ侵害の詳細な情報を書面で提供し、（iii）（可能な場合に）個人データ侵害の悪影響を軽減するにあたり、合理的な努力を尽くして相手方当事者を支援し、（iv）個人データ侵害についてプライバシー法が義務付けているすべての措置を講じるものとします。

4.5　合理的な期間を定めた書面による事前の要求に応じて、処理者が本パートナー向けDPAを遵守していることを証明するために適用法の下で合理的に必要とされる場合がある情報を管理者に提供するものとします。

4.6　合理的な期間を定めた事前の通知に応じて、プライバシー法が義務付けている範囲において、自らが処理者である個人データの処理に関連するデータ保護影響評価もしくは事前協議またはその両方を実施するために合理的に必要な支援を管理者に提供するものとします。

4.7　主契約に基づく個人データの処理に関連する個人または管轄データ保護機関からの要求を管理者にすみやかに通知し、当該要求に対処する際に管理者に協力するものとします。なお、当該要求には、適用されるプライバシー法に基づく自己の権利を行使しようとする個人からの要求が含まれます。処理者は、法律上義務付けられている場合を除き、事前に管理者から承認を得ずに、かかる連絡に直接応じてはならないものとします。

4.8　主契約が期間満了もしくは解除となったときに、または（書面で要求することができる）管理者による別段の選択により、合理的に実務上可能な限りすみやかにすべての個人データを削除または管理者に返却するものとします。ただし、適用法に基づいて処理者に複製物を保持する義務がある場合はこの限りではなく、処理者は、適用法が義務付けている範囲である場合を除き、個人データのさらなる処理を制限および防止するものとします。

4.9　いずれかの当事者がCCPAの範囲内で個人データを処理している場合、相手方当事者のみのために個人データを処理するものとし、本パートナー向けDPAまたは主契約に定める目的およびCCPAまたはCCPAを承継する法において認められている目的以外の目的のために個人データを保持、利用、共有または開示してはならないものします。いかなる場合でも、各当事者は、個人データを第三者と共有してはならず（下記の第5条に従って復処理者と共有する場合は除きます）、個人データを販売してはなりません。各当事者は、自ら行う個人データの処理に課されているすべての制限を理解していること、また、かかる制限を遵守することを証します。かかる遵守には、個人データまたは個人情報を相手方当事者が販売しているとCCPAに基づいてみなされるような行為を回避することが含まれます。本項を解釈する際に、本パートナー向けDPAにおける処理者を、CCPA第1798.140条（v）で定義されているサービス提供者とみなすものとします。

4.10　（主契約の条件に従った）合理的な期間を定めた書面による事前の相手方当事者からの要求に応じて、本パートナー向けDPAに基づく処理者の義務を遵守していることを証明するために合理的に必要となる場合がある情報を提供し、相手方当事者または相手方当事者が委任した他の監査人が実施する監査（検査を含みます）の実施を許可し、かかる監査に協力するものとします。

5.　復処理者

5.1　復処理者への委託：

いずれの当事者も復処理者に委託することができ、かかる委託に対する一般的な同意を相手方当事者から得ています。両当事者は、本サービスに関連する個人データを主契約に基づいて処理するための復処理者を指定することができ、当該処理を当該復処理者に委託することができます。ただし、いずれの場合も、当該復処理者が実施する役務に関連しており、（i）適切な技術的措置および組織的措置の実施を十分に保証すること、および（ii）本パートナー向けDPAにおいてDellに課される権利もしくは義務またはその両方に実質的に類似する条件を遵守することを当該復処理者に求める書面による契約を当該復処理者と締結していることを条件とします。復処理者には、第三者または当事者の関係会社が含まれる場合があります。復処理者が前述の自己のデータ保護義務を履行しなかった場合、当該復処理者に委託した処理者は当該復処理者による義務の履行について、相手方当事者に対する責任を負うものとします。

5.2　復処理者の一覧：

Dellは、Dellが自己の役務の実施をサポートさせる復処理者の一覧をwww.dell.com/subprocessorsに掲載します。

6.　セキュリティ

6.1　技術的セキュリティ対策および組織的セキュリティ対策：

各当事者は、個人データの処理に関わる処理システムおよび処理サービスのセキュリティ、機密性、完全性、可用性および耐障害性が当該個人データに関するリスクに見合った状態であることを合理的に確保し、個人データ侵害を防止するための適切な技術的措置および組織的措置の整備を徹底するものとします。両当事者は、付属書 1 に記載された技術的セキュリティ対策および組織的セキュリティ対策（「**情報セキュリティ対策**」）が、本パートナー向け DPA の要件を満たす個人データの保護を実現するための適切なレベルのセキュリティを提供することに合意します。各当事者は、定期的に（i）保護手段、管理策、システムおよび手順の有効性をテストおよびモニタリングし、（ii）個人データのセキュリティ、機密性および完全性に対する合理的に予見可能な社内外のリスクを特定するものとし、かかるリスクへの対応を確実に行うものとします。

6.2　技術の進歩

情報セキュリティ対策は技術の進歩および開発によって変わるものであり、Dellはかかる対策を変更することができます。ただし、かかる変更によって、主契約に基づいて処理する個人データの全体的なセキュリティが低下しないことを条件とします。

6.3　アクセス

両当事者は、個人データにアクセスする権限を有する者（関係会社および承認済みの復処理者を含みます）が機密保持義務を負い、個人データの機密性およびセキュリティを尊重および維持するとともに、自ら機密保持を確約するか、法律上の適切な機密保持義務を負うことを徹底するものとします。

7.　越境移転

両当事者は、本パートナー向けDPAに基づく個人データの処理に関連して、または事業の通常の過程において、世界中の自己の関係会社もしくは復処理者またはその両方に個人データを移転する権限を有しています。かかる移転を行う場合、各当事者は、主契約に基づき、または主契約に関連して移転される個人データを保護するために、適切な保護を整備することを徹底するものとします。主契約に基づく両当事者の義務の履行に欧州経済領域（「EEA」）、英国、またはスイスからEEA、英国、およびスイス以外の（プライバシー法に基づく十分性認定を受けていない）国への個人データの移転が伴う場合、両当事者は、適用されるプライバシー法に従って、適切な追加措置を講じ、または他の適切なデータ移転の仕組みを採用するとともに、モデル条項を使用するものとすることに合意します。特に、かかる移転は、（a）各当事者が、個人データにアクセスする可能性がある自己の関係会社とグループ間契約（かかる契約において関連するモデル条項を組み込むものとします）を締結すること、および（b）各当事者が、状況に応じて、関連するモデル条項を組み込んだ契約を自己の復処理者と締結することを条件とします。適用のあるプライバシー法に基づく個人データの移転におけるコンプライアンスの仕組み（数は問いません）をさらに必要とする他の国境をまたぐ個人データの移転が、主契約に基づく両当事者の義務の履行に伴う場合、両当事者は、プライバシー法に基づく義務もしくは関連するデータ プライバシー規制当局の定め、またはその両方に従い、かかる国境をまたぐ個人データの移転におけるコンプライアンスを確保するために、適切な契約条項や、その他所定の仕組みもしくは措置またはその両方を使用するものとすることに合意します。

8. 存続条項

本パートナー向け DPA に基づく各当事者の義務は、本パートナー向け DPA および主契約の解除後も、受領管理者が個人データを保持または管理し続けている間は有効に存続するものとします。

付属書1

情報セキュリティ対策

Dellは情報セキュリティを重大なものとして捉えています。この情報セキュリティの概要は、Dellのグループ会社間で処理および移転される個人データを保護するためのDellの組織的な管理策に適用されます。Dellの情報セキュリティ プログラムは、Dellの従業員が自己の責任を理解できるようにするものです。お客様と個別に合意した場合に、一部のお客様向けソリューションにおいて、作業範囲記述書に概要が記載されている代替的な保護対策を講じることがあります。

セキュリティに関する取り組み

Dellは、会社としての情報セキュリティに関する取り組みおよび基準を導入しました。これらは、Dellの社内環境を保護し、（1）情報セキュリティ、（2）システム管理およびアセット管理、（3）開発、ならびに（4）ガバナンスに対処するように設計されています。こうした取り組みおよび基準は、DellのCIO（最高情報責任者）が承認しており、正式な見直しが1年に1回行われています。

組織的セキュリティ

前述の取り組みおよび基準を遵守する責任を組織内の各個人が負っています。前述の取り組みおよび基準を会社として遵守することを促進するために、情報セキュリティ担当部門は以下の事項を規定または実施しています。

1. 規程/基準および規則の戦略および遵守、意識向上および教育、リスク アセスメントおよびリスク管理、セキュリティに関する契約上の要求事項の管理、アプリケーションおよびインフラストラクチャに関するコンサルティング、確認テスト、会社のセキュリティに関する方針の決定
2. 環境全体においてセキュリティ管理策の採用を可能にするためのセキュリティ テストならびにセキュリティ ソリューションの設計および実装
3. 実装したセキュリティ ソリューションのセキュリティに関する運用、環境および資産、インシデント対応の管理
4. セキュリティ オペレーション、法務、データ保護および人事担当者と連携して行うフォレンジック調査（eDiscoveryおよびeForensicsを含みます）

資産の区分および管理

Dellによる取り組みの目的は物理的資産および論理的資産を追跡および管理することです。Dell ITが追跡する可能性がある資産の例は以下のとおりです。

- 情報資産（特定したデータベース、災害時復旧計画、事業継続計画、データの区分、アーカイブした情報など）
- ソフトウェア資産（特定したアプリケーションおよびシステム ソフトウェアなど）
- 物理的資産（特定したサーバー、デスクトップ/ノートパソコン、バックアップ/アーカイブ用テープ、プリンターおよび通信機器など）

機密保持に関する要求事項を決定するために、業務の重要度に基づいて資産を分類しています。また、個人データの取り扱いに関する業界の手引きにおいて、技術的、組織的および物理的安全管理措置のための枠組みを規定しています。これらの安全管理措置には、アクセス管理、暗号化、ログの取得、モニタリング、およびデータの破壊などの管理策が含まれることがあります。

人的セキュリティ

雇用手続きの一部として、地域の法律に応じて、該当するスクリーニング手続きを従業員に対して実施しています。1年に1回Dellが実施するコンプライアンス研修では、従業員がオンライン コースを修了し、情報セキュリティおよびデータ プライバシーを対象とした評価に合格する必要があります。また、セキュリティ意識向上プログラムにおいて、特定の職務専用の資料を提供する場合があります。

物理的セキュリティおよび環境的セキュリティ

Dellは、リスクの低減という点で、自社の物理的セキュリティ プログラムにおいて多くの技術上および運用上のアプローチを用いています。セキュリティ チームは各拠点と緊密に連携して、適切な措置が講じられていることを確認し、物理インフラストラクチャ、事業、および既知の脅威の変更を継続的にモニタリングしています。また、セキュリティ チームは同一業界内の他社が講じている最善の措置に注意を払い、事業実務における独自性とDellの期待の両方に全体として合致するアプローチを慎重に選択しています。アーキテクチャ、運用およびシステムを含む管理策の要素を検討することにより、Dellはセキュリティに対する自社のアプローチのバランスを保っています。

通信および運用の管理

IT担当部門は、一元的な変更管理プログラムを通じて、会社のインフラストラクチャ、システムおよびアプリケーションの変更を管理しています。かかる管理には、状況に応じて、テスト、事業影響度分析および経営陣による承認が含まれることがあります。

セキュリティおよびデータ保護におけるインシデントに対して、インシデント対応手順が存在します。かかる手順には、インシデント分析、封じ込め、対応、修復、報告および正常動作への復旧が含まれることがあります。

資産の悪意ある利用および悪意あるソフトウェアを防止するために、リスクに応じて、追加の管理策が実施されることがあります。かかる管理策には、情報セキュリティへの取り組み、情報セキュリティに関する基準、アクセス制限、開発環境およびテスト環境の指定、サーバー、デスクトップおよびノートパソコン上のウイルスの検知、Eメールに添付されたウイルスのスキャン、システム適合状況の確認、侵入防止モニタリングおよび侵入時対応、重要なイベントに関するログの取得およびアラートの発信、データの種類に応じた情報取り扱い手順、ECアプリケーションおよびネットワーク セキュリティ、システムおよびアプリケーションの脆弱性診断が含まれることがありますが、これらに限定されません。

アクセス制御

会社システムへのアクセスは制限されており、適切な承認を得るための手順に従っています。故意などによる誤用のリスクを低減するために、職務分掌および最小権限の原則に基づいてアクセス権を付与しています。

リモート アクセスおよび無線コンピューター機能は制限されており、ユーザーおよびシステムにおける保護対策が共に整備されていることを条件としています。

インシデント対応およびフォレンジック調査を可能にするために、例外発生時に、重要なデバイスおよびシステムから取得した特定のイベントログを集約し、報告しています。

システムの開発および保守

公表された第三者の脆弱性がDellの環境において適用されるか否かを確認しています。Dellの事業および顧客に対するリスクに基づき、修復のためのタイムフレームがあらかじめ定められています。加えて、新規かつ重要なアプリケーションおよびインフラストラクチャについて、リスクに基づいた脆弱性診断および脆弱性評価を実施しています。リスクに基づいてコーディング上の脆弱性をプロアクティブに検知するために、本番稼働前に、開発環境において、コード レビューおよびコード スキャンを実施しています。これらのプロセスにより、脆弱性および法令遵守をプロアクティブに特定することが可能になります。

コンプライアンス

情報セキュリティ部門、法務部門、プライバシー部門、およびコンプライアンス部門は、Dellの組織に適用される地域の法令を特定する作業をしています。こうした要求事項の対象範囲には、DellおよびDellの顧客の知的財産、ソフトウェア ライセンス、従業員および顧客の個人情報の保護、データの保護およびデータの取り扱いに関する手順、データの越境移転、財務上および業務上の手順、技術に関する規制上の輸出管理、フォレンジックの要件などが含まれます。

また、情報セキュリティ プログラム、プライバシー運営委員会、社内外の者による監査/評価、社内外の法律顧問への相談、内部統制評価、社内の侵入テストおよび脆弱性診断、契約管理、セキュリティに関する啓発、セキュリティ コンサルティング、規程に対する例外の確認およびリスク管理などの仕組みを組み合わせて、こうした要求事項の遵守を推進しています。

付属書2
データ処理の詳細

1. 処理の主題および期間

処理の主題および期間は主契約に定めるとおりとします。

2. 処理の目的

主契約に基づく義務を履行するために、個人データを処理します。

3. 処理の性質

主契約に基づく両当事者の義務を果たすために必要な場合に個人データを処理します。

4. データ主体の類型

データ主体は、両当事者のエンド ユーザー、従業員、請負業者、サプライヤー、および主契約に基づく両当事者の関係に関連するその他の第三者です。

5. 個人データの種類

提供される可能性がある個人データの種類は次のとおりです。

- 詳細な連絡先：氏名、住所、E メール アドレス、電話番号、その他の連絡先情報など。
- 最終顧客の詳細な情報：詳細な連絡先、請求および信用に関するデータなど。
- IT システム情報および運用情報：個人の識別子、音声録音データ、録画データ、記録データ、ユーザーID およびパスワードの詳細、コンピューター名、E メール アドレス、ドメイン名、ユーザー名、パスワード、IP アドレス、（職務に応じた）権限データ、通信サービス用のアカウント情報および権限委譲情報、個々のメールボックスおよびディレクトリー、チャット通信データ、ソフトウェアおよびハードウェアの一覧、ソフトウェアおよびインターネットの使用パターンに関する追跡情報（例：Cookie）、運用もしくは研修またはその両方のために記録した情報など。
- データ主体の E メールの内容、トラフィック データおよび送信データ：オンラインでの双方向通信および音声通信（ブログ、チャット、Web カメラ、およびネットワーキング セッションなど）、サポート サービス（送受信した E メールの内容、ならびに E メールの送信、ルーティングおよび配信に関連するデータに付随的にアクセスする場合があります）。
- その他：一方の当事者が相手方当事者に提供するその他の個人データ。