Cloud のデータ処理に関する追加条項（パートナー）

この Cloud のデータ処理に関する追加条項（その付録を含めて、以下、「本追加条項」）は、Google とパートナー間の契約（以下に定義）に組み込まれます。本追加条項は、Google Cloud Platform では「データ処理およびセキュリティ規約」として、Looker（オリジナル）または Google SecOps サービスでは「データ処理に関する追加条項」または「データ処理およびセキュリティ規約」と称していたものです。

一般条項

1. 概要

本追加条項は、適用されるプライバシー、データ セキュリティ、およびデータ保護法に基づき、パートナー データの処理とセキュリティに関する両当事者の義務を定めるものです。本追加条項は、追加条項発効日（以下に定義）をもって発効し、それ以前にパートナー データの処理およびセキュリティに適用されていた条項に取って代わるものとします。本追加条項で定義されていない、大文字で始まる用語は、本契約において与えられた意味を有するものとします。

2. 定義

2.1 本追加条項内の定義:

- 「追加条項発効日」とは、パートナーが本追加条項を承諾した日、または両当事者が本追加条項に同意した日を意味します。
- 「追加のセキュリティ管理」とは、パートナーが自身の選択と判断で使用できるセキュリティに関するリソース、機能、および管理を意味します。これには、管理コンソール、暗号化、ロギングとモニタリング、Identity and Access Management、セキュリティ スキャン、ファイアウォールなどが含まれます。
- 「契約」とは、Google が該当するサービスをパートナーに提供することに同意した契約を意味します。
- 「適用されるプライバシー法」とは、パートナーの個人データの処理に適用される、国、連邦、欧州連合、州、地方、またはその他のプライバシー、データ セキュリティ、もしくはデータ保護に関する法律または規制を意味します。
- 「監査対象サービス」とは、https://cloud.google.com/security/compliance/services-in-scope において関連する証明書またはレポートの対象範囲となっているその時点で最新のサービスを指します。Google は、本契約に従って廃止された場合を除き、この URL からサービスを削除することはありません。
- 「コンプライアンス証明書」は、第 7.4 項（コンプライアンス証明書および SOC レポート）に定義されている意味を有します。

- 「データ インシデント」とは、Google が管理または制御しているシステム上のパートナー データに対する偶発的または違法な破壊、紛失、改ざん、不正開示、またはアクセスにつながる Google のセキュリティに対する侵害を意味します。

- 「EMEA」とは、欧州、中東、およびアフリカを意味します。

- 「EU GDPR」とは、「個人データ取り扱いに係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 日付欧州議会および理事会規則（EU）2016/679」を意味し、これにより指令 95/46/EC は廃止されています。

- 「欧州データ保護法」とは、（a）GDPR または（b）スイス FADP のいずれか該当するものを意味します。

- 「欧州法」とは、（a）EU もしくは EU 加盟国の法律（EU GDPR がパートナーの個人データの処理に適用される場合）、（b）英国もしくは英国の一部地域の法律（英国 GDPR がパートナーの個人データの処理に適用される場合）、または（c）スイスの法律（スイス FADP がパートナーの個人データの処理に適用される場合）のいずれか該当するものを意味します。

- 「GDPR」とは、（a）EU GDPR または（b）英国 GDPR のいずれか該当するものを意味します。

- 「Google の第三者監査人」とは、Google が選任した適格かつ独立した第三者監査人のことで、その選任時に Google からパートナーにその情報を開示します。

- 「指示」は、第 5.2 項（パートナーの指示への準拠）に定義されている意味を有します。

- 「通知用メールアドレス」とは、パートナーが Google から特定の通知を受け取るために、管理コンソールまたは注文フォームで指定したメールアドレスを意味します。

- 「パートナーのエンドユーザー」は、本契約で定義されている意味を有します。そのような定義がない場合は、本契約の「エンドユーザー」で定められている意味を有します。

- 「パートナーの個人データ」とは、適用されるプライバシー法において定義される特別な種類の個人データまたはセンシティブ データなど、パートナー データに含まれる個人データを意味します。

- 「セキュリティ ドキュメント」とは、コンプライアンス証明書および SOC レポートを意味します。

- 「セキュリティ対策」とは、第 7.1.1 項（Google のセキュリティ対策）に規定されている意味を有します。

- 「サービス」とは、付録 4（特定のプロダクト）に記載の該当するサービスを意味します。

- 「SOC レポート」は、第 7.4 項（コンプライアンス証明書および SOC レポート）に規定されている意味を有します。

- 「復処理者」とは、本追加条項に基づき、サービスおよび TSS の一部を提供するために、パートナー データを処理することを許可された第三者の別のデータ処理者を意味します。

- 「監督機関」とは、（a）EU GDPR で定義される「監督機関」、または（b）英国 GDPR もしくはスイス FADP で定義される「コミッショナー」のいずれか該当するものを意味します。

- 「スイス FADP」とは、1992 年 6 月 19 日付連邦データ保護法（スイス）（1993 年 6 月 14 日付連邦データ保護法に関する政令を伴う）、または 2020 年 9 月 25 日付改正連邦データ保護法（スイス）（2022 年 8 月 31 日付連邦データ保護法に関する政令を伴う）のいずれか該当するものを意味します。

- 「期間」とは、本追加条項の発効日から Google がサービスの提供を終了するまでの期間を意味します（Google はこの期間内にサービスの提供を一時停止したり、期間終了後に移行目的でサービスの提供を継続したりする場合があります）。

- 「英国の GDPR」とは、英国の 2018 年欧州連合離脱法、および同法に基づき制定された該当する二次法に従い、EU の GDPR を修正し、英国の法律に組み込んだものを意味します。

2.2 本追加条項で使用される「個人データ」、「データ主体」、「処理」、「データ管理者」、「データ処理者」という用語は、適用されるプライバシー法で定義されている意味、またはそのような意味もしくは法律がない場合は、EU GDPR で定義されている意味を有します。

2.3「データ主体」、「データ管理者」、「データ処理者」という用語には、適用されるプライバシー法によって要求される場合、それぞれ「消費者」、「事業者」、「サービス プロバイダ」が含まれます。

3. 期間

本契約が終了または満了しているかどうかにかかわらず、本追加条項に記載されているとおり、本追加条項は Google がすべてのパートナー データを削除するまで有効であり、削除が完了した時点で自動的に失効します。

4. 役割、法令遵守

4.1 当事者の役割。パートナーの個人データに関して、Google はデータ処理者であり、パートナーはデータ管理者またはデータ処理者のいずれか該当するものです。

4.2 処理の概要。パートナーの個人データの処理の内容および詳細は、付録 1（データ処理の内容および詳細）に記載されています。

4.3 法律の遵守。各当事者は、適用されるプライバシー法に基づき、パートナーの個人データの処理に関連する義務を遵守するものとします。

4.4 その他の法的条項。パートナーの個人データの処理が付録 3（特定のプライバシー法）に記載されている適用されるプライバシー法の対象となる範囲において、付録 3 の該当する条項が、これらの一般条項に加えて適用され、第 14.1 項（優先順位）の記載に従って優先されます。

5. データ処理

5.1 データ処理者のパートナー。パートナーが処理者である場合:

a. パートナーは、以下の事項について、関連する顧客およびデータ管理者からの承認を継続的に保証するものとします。

i. 指示。

ii. パートナーが Google を別の処理者として関与させること。

iii. 第 11 項（復処理者）に記載のとおり、Google が復処理者を関与させること。

b. パートナーは、第 7.2.1 項（インシデントの通知）、第 9.2.1 項（要求に対する責任）、または第 11.4 項（復処理者に対する異議申し立ての機会）に基づき Google から提供された通知を、関連する顧客およびデータ管理者に遅滞なく速やかに転送するものとします。

c. パートナーは、Google データセンターの場所、または復処理者の名称、所在地、および活動に関する本追加条項に基づき、Google から提供されたその他の情報を、関連する顧客およびデータ管理者に開示できます。

5.2 パートナーの指示への準拠。パートナーは Google に対し、本契約（本追加条項を含む）に従って以下の方法でのみパートナー データを処理するよう指示するものとします。

a. サービスおよび TSS の提供、セキュリティ確保、および監視。

b. さらに以下のように指定される方法:

i. パートナーによるサービス（管理コンソール経由を含む）および TSS の利用

ii. パートナーによって与えられ、本追加条項に基づく指示を成立させると Google が認めたその他の書面による指示

（これらを総称して「指示」と呼びます）。

Google は、欧州データ保護法が適用される状況では欧州法によって禁止されている場合、またはその他の該当するプライバシー法が適用される状況ではその適用法によって禁止されている場合を除き、これらの指示に従うものとします。

6. データの削除

6.1 パートナーによる削除。Google は、パートナーが期間中に、サービスの機能と整合した方法でパートナー データを削除できるようにします。パートナーが期間中にサービスを使用してパートナー データを削除し、そのパートナー データをパートナーが復元できない場合、その使用行為は Google に対し、該当するパートナー データを Google のシステムから削除するよう指示したものとみなされます。Google は、欧州データ保護法が適用される状況では欧州法によって保存が要求されている場合、またはその他の該当するプライバシー法が適用される状況ではその適用法によって保存が要求されている場合を除き、合理的に実行可能な限り速やかに、かつ最長 180 日以内にこの指示に従います。

6.2 期間終了時のデータ返却または削除。パートナーが期間終了後もパートナー データの保持を希望する場合は、期間中に第 9.1 項（アクセス、訂正、制限付きの処理、ポータビリティ）に従って、Google にそのデータを返却するよう指示できます。パートナーは期間終了時に、Google のシステムから残りのパートナー データ（既存のコピーを含む）をすべて削除するよう Google に指示します。その日から最大 30 日間の復元期間後、Google は、欧州データ保護法が適用される状況では欧州法によって保存が要求されている場合、またはその他の該当するプライバシー法が適用される状況ではその適用法によって保存が要求されている場合を除き、合理的に実行可能な限り速やかに、かつ最長 180 日以内にこの指示に従います。

7. データ セキュリティ

7.1 Google のセキュリティ対策、管理、支援。

7.1.1 Google のセキュリティ対策。Google は、パートナー データを偶発的または違法な破壊、損失、改ざん、不正な開示またはアクセスから保護するため、付録 2（セキュリティ対策）に記載されている技術的、組織的、および物理的な措置（「セキュリティ対策」）を実施し、維持します。セキュリティ対策には、パートナー データを暗号化する措置、Google のシステムおよびサービスの継続的な機密性、完全性、可用性、および復元力を確保するための措置、インシデント発生後にパートナー データへのタイムリーなアクセスを復元するための措置、ならびに有効性を定期的にテストするための措置が含まれます。Google はセキュリティ対策を随時更新できますが、その更新によりサービスのセキュリティが実質的に低下しないようにします。

7.1.2 アクセスおよびコンプライアンス。Google は、次のことを行います。

a. 従業員、請負業者、および復処理者がパートナー データにアクセスすることを、指示を遵守するために厳密に必要な場合にのみ許可します。

b. その業務範囲に適用される限りにおいて、従業員、請負業者、および復処理者がセキュリティ対策を確実に遵守できるように、適切な措置を講じます。

c. パートナー データの処理を許可されたすべての人物が機密保持義務を負うことを保証します。

7.1.3 追加のセキュリティ管理。Google は、以下の目的で追加のセキュリティ管理を提供します。

a. パートナーが、パートナー データを保護するための措置を講じることができるようにするため。

b. パートナー データのセキュリティ確保、アクセス、および使用に関する情報をパートナーに提供するため。

7.1.4 Google のセキュリティ支援。Google は（パートナーの個人データの処理の性質および Google が利用可能な情報を考慮し）、適用されるプライバシー法に基づくセキュリティおよび個人データ侵害に関するパートナー（または、パートナーがデータ処理者である場合は関連するデータ管理者）の義務遵守を、以下の方法で支援します。

a. 第 7.1.1 項（Google のセキュリティ対策）に従って、セキュリティ対策を実施および維持する。

b. 第 7.1.3 項（追加のセキュリティ管理）に従って、追加のセキュリティ管理を提供する。

c. 第 7.2 項（データ インシデント）の条項を遵守する。

d. 第 7.5.1 項（セキュリティドキュメントの審査）に従って、セキュリティドキュメントを利用できるようにし、本契約（本追加条項を含む）に含まれる情報を提供する。

e. 上記（a）～（d）項が、パートナー（または関連するデータ管理者）がそのような義務を遵守するために不十分である場合、パートナーの要求に基づき、パートナーに追加の合理的な協力および支援を提供すること。

7.2 データ インシデント。

7.2.1 インシデントの通知。Google は、データ インシデントの発生を認識した後、遅滞なく速やかにパートナーに通知し、被害を最小限に抑えつつ、パートナー データを保護するために合理的な措置を直ちに講じます。

7.2.2 データ インシデントの詳細。Google からのデータ インシデント通知には、以下の内容が記載されます。影響を受けたパートナーのリソースを含む、データ インシデントの性質。データ インシデントに対処し、潜在的なリスクを軽減するために Google が講じた、または講じる予定の措置。Google がデータ インシデント対処法としてパートナーに推奨する措置（存在する場合）。追加情報を得るための連絡先情報。すべての情報を同時に提供できない場

合、Google の初回通知ではその時点で利用可能な情報を提供し、その他の情報については利用可能になり次第、遅滞なく提供します。

7.2.3 Google によるパートナー データの評価義務の否定。Google は、特定の法的要件の対象となる情報を特定するためにパートナー データを評価する義務を負いません。

7.2.4 Google による過失承認の否定。第 7.2 項（データ インシデント）に基づく Google のデータ インシデント通知やデータ インシデント レスポンスは、データ インシデントに関する過失や責任を Google が認めたと解釈されるものではありません。

7.3 パートナーのセキュリティ責任およびセキュリティ評価。

7.3.1 パートナーのセキュリティ責任。第 7.1 項（Google のセキュリティ対策、管理、支援）、第 7.2 項（データ インシデント）、および本契約のその他の箇所に基づく Google の義務を損なうことなく、Google とパートナーの関係において、パートナーは以下の自ら、およびその顧客によるサービスの利用、ならびに Google または Google の復処理者のシステム外部におけるパートナー データのコピーの保存について責任を負うものとします。

a. パートナー データへのリスクに見合ったレベルのセキュリティを確保するために、サービスおよび追加のセキュリティ管理を利用すること。

b. パートナーおよびその顧客がサービスにアクセスするために使用するアカウント認証情報、システム、およびデバイスのセキュリティを確保すること。

c. 必要に応じてパートナー データのバックアップを行うこと。

7.3.2 パートナーのセキュリティ評価。パートナーは、サービス、セキュリティ対策、追加のセキュリティ管理、および本第 7 項（データ セキュリティ）に基づく Google のコミットメントが、パートナー データへのリスクに見合ったレベルのセキュリティを提供することに同意するものとします（これは、最新技術、実装コスト、およびパートナー データの処理の性質、範囲、状況、目的、ならびに個人へのリスクを考慮に入れたものです）。

7.4 コンプライアンス証明書および SOC レポート。Google は、セキュリティ対策の継続的な有効性を検証するため、監査対象サービスについて少なくとも以下のものを維持します。

a. ISO 27001 の証明書、および付録 4（特定のプロダクト）に記載されている追加の証明書（以下「コンプライアンス証明書」）。

b. Google の第三者監査人によって作成され、少なくとも 12 か月に一度実施される監査に基づいて毎年更新される SOC 2 および SOC 3 レポート（以下「SOC レポート」）。

Google はいつでも基準を追加できます。また、コンプライアンス証明書または SOC レポートを、同等の、または増補された代替文書に差し換える場合があります。

7.5 コンプライアンスの審査と監査。

7.5.1 セキュリティドキュメントの審査。Google は、本追加条項に基づく自身の義務遵守を証明するため、パートナーにセキュリティドキュメントを提供して審査できるようにします。また、パートナーがデータ処理者である場合、Google は第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従い、関連する顧客およびデータ管理者向けに SOC レポートへのアクセスを要求することをパートナーに許可します。

7.5.2 パートナーの監査の権利。

a. パートナーによる監査。Google は、適用されるプライバシー法によって要求される場合、パートナーまたはパートナーが任命した独立監査人に対し、第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従って、本追加条項に基づく Google の義務遵守を検証するための監査（検査を含む）の実施を許可します。監査中、Google は本第 7.5 項（コンプライアンスの審査と監査）に記載のとおり、パートナーまたはその監査人に合理的に協力します。

b. パートナーによる独立審査。パートナーは、セキュリティドキュメント（Google の第三者監査人による監査の結果が反映されたもの）を確認することで、本追加条項に基づく Google の義務遵守を検証するための監査を実施できます。

7.5.3 審査および監査に関する追加のビジネス規約。

a. パートナーは、以下の要求を行う場合、Google Cloud データ保護チームに連絡する必要があります。

i. 第 7.5.1 項（セキュリティドキュメントの審査）に基づく、関連するデータ管理者向けの SOC レポートへのアクセス。

ii. 第 7.5.2（a）項（パートナーによる監査）に基づく監査。

b. 第 7.5.3（a）項に基づくパートナーからの要求後、Google とパートナーは事前に以下の事項について協議し、合意するものとします。

第 7.5.1 項（セキュリティドキュメントの審査）に基づいて、関連するデータ管理者による SOC レポートへのアクセスに適用されるセキュリティと機密性保持の管理。

ii. 第 7.5.2（a）項（パートナーによる監査）に基づく監査の合理的な開始日、範囲および期間、ならびにセキュリティと機密性保持の管理。

c. Google は、第 7.5.2（a）項（パートナーによる監査）に基づく監査に対して、Google の合理的な費用に基づいて料金を請求する場合があります。Google は、当該の監査を行う前に、適用される料金の詳細およびその計算の根拠をパートナーに提供します。かかる監査の実施において、パートナーが任命した監査人から請求された料金については、パートナーが負担するものとします。

d. Google は、適切な資格を有しない、独立した監査人でない、Google の競合他社であるなど、パートナーが任命した監査人が第 7.5.2（a）項（パートナーによる監査）に基づく監査の実施に適格でないと合理的に判断した場合、当該の監査人に対し、書面で異議申し立てを行うことができます。Google がそのような異議申し立てを行った場合、パートナーは、別の監査人を任命するか、自身で監査を実施する必要があります。

e. 付録 3（特定のプライバシー法）または付録 4（特定のプロダクト）に基づく、関連するデータ管理者向けの SOC レポートへのアクセスまたは監査に関するパートナーからの要求も、本第 7.5.3 項（審査および監査に関する追加のビジネス規約）の対象となります。

8. 影響評価と協議

Google は（処理の性質および Google が利用可能な情報を考慮し）、適用されるプライバシー法に基づくデータ保護評価、リスク評価、事前規制協議、またはそれに相当する手続きに関するパートナー（または、パートナーがデータ処理者である場合は関連するデータ管理者）の義務遵守を、以下の方法で支援します。

a. 第 7.1.3 項（追加のセキュリティ管理）に従い追加のセキュリティ管理を提供し、第 7.5.1 項（セキュリティドキュメントの審査）に従いセキュリティドキュメントを提供すること。

b. 本契約（本追加条項を含む）に記載されている情報を提供すること。

c. 上記（a）および（b）項が、パートナー（または関連するデータ管理者）がそのような義務を遵守するために不十分である場合、パートナーの要求に基づき、パートナーに追加の合理的な協力および支援を提供すること。

9. アクセスなど、データ主体の権利、データのエクスポート

9.1 アクセス、訂正、制限付きの処理、ポータビリティ。Google は期間中、パートナー データへのアクセス、訂正、制限付きの処理（第 6.1 項（パートナーによる削除）に記載されている Google 提供の削除機能も含む）、およびパートナー データのエクスポートをサービスの機能に沿った方法で行うことをパートナーに許可します。パートナーは、パートナーの個人データが不正確または古くなっていることに気づき、適用されるプライバシー法によって要求されている場合は、そのデータを訂正または削除するために当該機能を使用する責任を負うものとします。

9.2 データ主体からの要求。

9.2.1 要求に対する責任。期間中、Google のクラウドデータ保護チームが、パートナーの個人データに関連し、かつパートナーを特定する要求をデータ主体から受け取った場合、Google は以下のことを行います。

a. データ主体に対し、要求をパートナーに提出するよう助言します。

b. 速やかにパートナーに通知します。

c. それ以外の方法では、パートナーからの許可なく、当該データ主体の要求には対応しません。

パートナーは、必要に応じてサービスの機能を使用することを含め、かかる要求に対応する責任を負うものとします。

9.2.2 データ主体からの要求に対する Google の支援。Google は（パートナーの個人データの処理の性質を考慮し）、適用されるプライバシー法に基づく、データ主体の権利行使に関する要求に対応するというパートナー（または、パートナーがデータ処理者である場合は関連するデータ管理者）の義務履行を、以下の方法で支援します。

a. 第 7.1.3 項（追加のセキュリティ管理）に従い、追加のセキュリティ管理を提供すること。

b. 第 9.1 項（アクセス、訂正、制限付きの処理、ポータビリティ）および第 9.2.1 項（要求に対する責任）を遵守すること。

c. 上記（a）および（b）項が、パートナー（または関連する管理者）がそのような義務を遵守するために不十分である場合、パートナーの要求に基づき、パートナーに追加の合理的な協力および支援を提供すること。

10. データ処理の場所

10.1 データ保存 / 処理施設。サービス固有の規約に基づく Google のデータの場所に関するコミットメントと、付録 3（特定のプライバシー法）に基づくデータ移転に関するコミットメントに従い、該当する場合、パートナー データは、Google またはその復処理者が施設を維持している任意の国で処理される可能性があります。

10.2 データセンター情報。Google データセンターの所在地は、付録 4（特定のプロダクト）に記載されています。

11. 復処理者

11.1 復処理者の利用に対する同意。パートナーは、本追加条項の発効日時点において、第 11.2 項（復処理者に関する情報）で開示されている事業者を Google が復処理者として利用することを明示的に承認するものとします。また、パートナーは概して、第 11.4 項（復処理者に対する異議申し立ての機会）を損なうことなく、Google がその他の第三者復処理者（以下、「新規復処理者」）を利用することを承認するものとします。

11.2 復処理者に関する情報。復処理者の名称、所在地、および活動内容は、付録 4（特定のプロダクト）に記載されています。

11.3 復処理者の利用に関する要件。復処理者を利用する際、Google は以下のことを行います。

a. 書面による契約を通じて、以下のことを保証します。

i. 復処理者は、下請けに出された義務を履行するために必要な範囲でのみパートナー データにアクセスし、これを利用します。その際、本契約（本追加条項を含む）に従います。

ii. 適用されるプライバシー法によって要求される場合、本追加条項に記載されているデータ保護義務が復処理者にも課せられます（これは、付録 3（特定のプライバシー法）でさらに詳述される場合があります）。

b. 復処理者に委託したすべての義務、ならびに復処理者のすべての行為および不作為に対して、全責任を負います。

11.4 復処理者に対する異議申し立ての機会。

a. Google が期間中に新規復処理者を利用する場合、新規復処理者がパートナー データの処理を開始する少なくとも 30 日前に、Google はパートナーに対してその利用（新規復処理者の名称、所在地、および活動内容を含む）について通知するものとします。

b. パートナーは、新規復処理者の利用について通知されてから 90 日以内に、以下のいずれかの方法で、都合による本契約の即時解除により異議を申し立てることができます。

i. 本契約の「都合による解除」条項に従う。

ii. そのような条項がない場合は、Google に通知する。

12. クラウドデータ保護チーム、データ処理記録

12.1 クラウドデータ保護チーム。Google のクラウドデータ保護チームは、本契約に基づくパートナー データの処理に関するパートナーからの問い合わせに対し、迅速かつ合理的な支援を行います。また、当該チームへは、本契約の「通知」の項または付録 4（特定のプロダクト）に記載されている方法で連絡できます。

12.2 Google のデータ処理記録。Google は、適用されるプライバシー法の要求に従い、その処理活動に関する適切な文書を保持します。適用されるプライバシー法によって、Google がパートナーまたはその顧客に関する特定の情報を収集し、その記録を維持することが要求される範囲において、パートナーは管理コンソールまたは付録 4（特定のプロダクト）に記載されるその他の手段を利用して、かかる情報を提供し、正確かつ最新の状態に保ちます。Google は、適用されるプライバシー法によって要求される場合、かかる情報を管轄規制機関（監督機関を含む）に提供する場合があります。

12.3 データ管理者からの要求。期間中、Google のクラウドデータ保護チームが、パートナーの個人データのデータ管理者であると称する第三者から要求または指示を受けた場合、Google は当該の第三者に対し、パートナーに連絡するよう勧告します。

13. 通知

本追加条項に基づく通知（データ インシデントについての通知を含む）は、通知用メールアドレスに送信されます。パートナーは、管理コンソールを使用するか、Google に通知することにより、自身の通知用メールアドレスを常に最新かつ有効な状態に保つ責任を負うものとします。

14. 解釈

14.1 優先順位。条項間で矛盾が生じた場合の優先順位は、以下のとおりです。

a. 付録 3（特定のプライバシー法）と本追加条項の残りの部分（付録 4（特定のプロダクト）を含む）との間で矛盾が生じた場合は、付録 3 が優先されます。

b. 付録 4（特定のプロダクト）と本追加条項の残りの部分（付録 3 を除く）との間で矛盾が生じた場合は、付録 4 が優先されます。

c. 本追加条項と本契約の残りの部分との間で矛盾が生じた場合は、本追加条項が優先されます。

14.2 条項の参照。別段の記載がない限り、本追加条項の付録における条項の参照は、本追加条項の一般条項を指します。

14.3 顧客。疑念の発生を避けるために記すと、顧客は本追加条項における第三者の受益者ではありません。

付録 1: データ処理の内容および詳細

内容

Google からパートナーへのサービスおよび TSS の提供。

データ処理の期間

期間に加え、期間終了後から Google が本追加条項に従ってすべてのパートナー データを削除するまでの期間。

データ処理の性質と目的

Google は、本追加条項に従い、パートナーにサービスおよび TSS を提供する目的で、パートナーの個人データを処理します。

データのカテゴリ

パートナーもしくはその顧客により（またはその指示により）、またはパートナーのエンドユーザーにより、サービスを通じて Google に提供される個人データ。

データ主体

データ主体には、パートナーもしくはその顧客（またはその指示）、またはパートナーのエンドユーザーにより、サービスを通じて Google にデータが提供される個人が含まれます。

付録 2: セキュリティ対策

本追加条項の発効日以降、Google は本付録 2 に記載されたセキュリティ対策を実施および維持します。

1. データセンターとネットワーク セキュリティ

（*a*）データセンター。

インフラストラクチャ。Google は地理的に分散したデータセンターを維持しており、物理的に保護された場所に本番環境のすべてのデータを保存しています。

冗長性。インフラストラクチャ システムは、単一障害点を排除し、予想される環境リスクの影響を最小限に抑えるように設計されています。具体的には、二重回路、スイッチ、ネットワーク、他の必須デバイスにより、このような冗長性が実現されています。サービスは、Google が予防的および是正的なメンテナンスを中断なく実行できるように設計されています。すべての環境機器および施設は、製造元や内部の仕様に従って、実施プロセスと実施頻度を詳細に説明した予防的メンテナンス手順が文書化されています。データセンターの機器に対する予防的および是正的なメンテナンスは、文書化された手順に沿って、標準の変更プロセスを通じて実施されます。

電力。データセンターの電力システムは、1 日 24 時間、週 7 日の継続的な運用に影響を与えることなく、冗長性と保守性を維持できるように設計されています。ほとんどの場合、データセンター内の重要なインフラストラクチャ コンポーネントには、それぞれ同じ容量の主電源と代替電源が用意されています。バックアップ電源は、ブラウンアウト、ブラックアウト、過電圧、電圧不足、許容範囲外の周波数状態でも、信頼できる電力を安定して供給する無停電電源装置（UPS）バッテリなど、さまざまなメカニズムによって提供されます。停電が発生した場合、バックアップ電源はバックアップ発電機が稼働するまで最大 10 分間、データセンターのフル稼働に必要な電力を一時的に供給するように設計されています。バックアップ発電機は数秒で自動的に起動し、データセンターが数日間フル稼働するのに通常必要な分の緊急用電力を供給します。

サーバー オペレーティング システム。Google のサーバーでは、アプリケーション環境用にカスタマイズした Linux ベースのシステムを使用しています。データは、データ セキュリティと冗長性を高めるために独自のアルゴリズムを使用して保存されます。

コードの品質。Google は、本サービスを提供するために使用されるコードのセキュリティを高め、本番環境におけるセキュリティ サービスを強化するために、コードレビュー プロセスを採用しています。

ビジネスの継続性。Google は、事業継続計画 / 障害復旧プログラムを策定し、定期的に立案とテストを行っています。

（b）ネットワークと転送。

データの転送。データセンターは通常、高速のプライベート リンクを介して接続され、データセンター間で安全かつ高速なデータ移転を実現しています。これにより、電子的な移転中やストレージ媒体への記録中に、不正なデータの読み取り、コピー、変更、削除の発生を防いでいます。Google は、インターネット標準プロトコルを通じてデータを移転します。

外部攻撃対象領域。Google は、外部攻撃対象領域を保護するため、複数層のネットワーク デバイスと侵入検知を採用しています。また、潜在的な攻撃方法を検討し、該当の目的に合わせて構築されたテクノロジーを外部向けシステムに組み込んでいます。

侵入検知。侵入検知は、進行中の攻撃アクティビティに関する情報を提供し、インシデントに対応するための適切な情報を提供することを目的としています。Google の侵入検知は、(i) 予防措置によって Google の攻撃対象領域の範囲と構成を厳密にコントロールし、(ii) データ エントリ ポイントでインテリジェントな検知制御を行います。また、(iii) 特定の危険な状況を自動的に修復する技術も組み込まれています。

インシデント対応。Google は、さまざまな通信チャネルをモニタリングしてセキュリティ インシデントを調査し、Google のセキュリティ担当者は既知のインシデントに迅速に対応します。

暗号化テクノロジー。Google は、HTTPS 暗号化 (SSL 接続や TLS 接続とも呼ばれます) を利用可能にしています。Google のサーバーは、RSA と ECDSA で署名された一時楕円曲線ディフィーヘルマン暗号鍵交換をサポートしています。この PFS (Perfect Forward Secrecy: 前方秘匿性) により、トラフィックを保護し、侵害された鍵または暗号の解読による影響を最小限に抑えることができます。

2. アクセス制御とサイト管理

(*a*) サイト管理。

オンサイト データセンターのセキュリティ運用。Google のデータセンターでは、24 時間、年中無休の物理的なセキュリティ機能を実現するためのオンサイトのセキュリティ運用が維持されています。担当者は、閉回路テレビ (CCTV) カメラとすべての警報システムを監視し、データセンターの内部および外部の巡回も定期的に実施しています。

データセンターへのアクセス手順。Google では、データセンターへの物理的なアクセスを制限するために、厳格なアクセス手順を設けています。データセンターのある施設に入るには電子カードキーが必要で、オンサイトのセキュリティ運用システムと警報が連動しています。データセンターへの入場者は全員、身分を明らかにし、オンサイトのセキュリティ運用担当者に身分証明書を提示する必要があります。データセンターへの入出は、許可された従業員、請負業者、訪問者に限定されています。施設に入るための電子カードキーの申請を行えるのは、許可された従業員と請負業者のみです。この申請はメールで行う必要があり、かつ申請者の上司とデータセンターの管理者の承認も必要です。データセンターに一時的に入出する場合は、次の条件を満たす必要があります。(i) 特定のデータセンターおよび訪問する内部領域について、データセンターの管理者から事前に承認を得る。(ii) オンサイトの警備窓口で署名する。(iii) 入出が承認されていることを証明するデータセンター アクセス レコードを提示する。

データセンターで採用されているセキュリティ デバイス。Google のデータセンターでは、システム アラームと連動した二段階認証のアクセス制御システムを採用しています。アクセス制御システムは、各個人の電子カードキーと、境界ドア、入出荷場所、その他重要な領域にアクセスした時刻をモニタリングし、記録します。不正な活動やアクセスの失敗は、アクセス制御システムによって記録され、必要に応じて調査されます。ビジネス オペレーションおよびデータセンターへのアクセスは、ゾーンおよび個人の職責に基づいて制限されています。データセンターは防火扉で保護されています。また、データセンターの内外で CCTV カメラが作動しています。カメラは、施設周辺、データセンター施設への出入り口、荷物の搬出口 / 搬入口など、重要領域をカバーするように配置されています。オンサイトのセキュリティ運用担当者が、CCTV 監視、記録、制御用の機器を管理しています。データセンター全体で、安全なケーブルによって CCTV 機器が接続されています。カメラは、24 時間年中無休で、デジタルビデオ レコーダーを通じてオンサイトで録画を行います。監視記録は活動に基づいて最長 30 日間保持されます。

(*b*)アクセス制御。

インフラストラクチャのセキュリティ担当者。Google は、スタッフのためのセキュリティ ポリシーを策定、維持しており、スタッフ用のトレーニング パッケージの一部としてセキュリティ トレーニングの受講を義務付けています。Google のインフラストラクチャ セキュリティ担当者は、Google のセキュリティ インフラストラクチャの継続的な監視、サービスのレビュー、セキュリティ インシデントへの対応を担当しています。

アクセス制御と権限の管理。パートナーの管理者およびパートナーのエンドユーザーは、サービスを利用するために、中央の認証システムまたはシングル サインオン システムを介して認証を行う必要があります。

内部データへのアクセス プロセスとポリシー - アクセス ポリシー。Google の内部データへのアクセス プロセスおよびポリシーは、許可されていない人物やシステムから、パートナー データの処理に使用されるシステムを保護するように設計されています。Google は、(i)承認されたユーザーが許可されたデータにのみアクセスする、(ii)処理中、使用中および記録後にパートナー データに対する不正な読み取り、コピー、変更、削除を防ぐことを目的にこのシステムを設計しています。システムは、不適切なアクセスを検出するように設計されています。Google では、本番環境のサーバーへのアクセスを制御するために集中アクセス管理システムを採用し、限られた数の承認ユーザーにのみアクセスを許可しています。Google の認証および認可システムは、SSH 証明書とセキュリティ キーを利用しており、Google に安全で柔軟なアクセス機構を提供するように設計されています。このようなメカニズムにより、サイトホスト、ログ、データ、構成情報に対して、承認されたアクセス権限だけが付与されます。Google では、アカウントの不正利用の可能性を最小限に抑えるため、一意のユーザー ID、安全なパスワード、2 要素認証、および厳重に管理されたアクセスリストの使用を義務付けています。アクセス権の付与または変更は、担当者の職責、許可されたタスクの実行に必要な職務要件、関係者以外には秘匿する方針に基づいて行われます。また、アクセス権限の付与や変更は、Google の内部データアクセス ポリシーおよびトレーニングに準拠して行われる必要があります。承認は、すべての変更の監査記録を維持するワークフロー ツールによって管理されています。システムに対するアクセスが記録され、説明責任のための監査証跡が作成されます。パスワードが認証に使用される場合(たとえば、ワークステーションへのログインなど)、少なくとも業界標準の慣行に沿ったパスワード ポリシーが履行されます。このような標準的慣行には、パスワードの再利用や十分なパスワード強度に関する制限が含まれます。Google では、非常に機密性の高い情報(クレジット カード データなど)へのアクセスにハードウェア トークンを使用しています。

3. データ

(a)データの保存、隔離、および記録。Google は、Google が所有するサーバー上のマルチテナント環境にデータを保存します。特段の指示(データの場所の選択など)がない限り、地理的に分散した複数のデータセンター間でパートナー データを複製します。また、Google はパートナー データを論理的に隔離します。パートナーには、特定のデータ共有ポリシーの管理権が付与されます。これらのポリシーにより、パートナーはサービスの機能に従って、特定の目的に応じてエンドユーザーに適用される共有設定を決定できます。パートナーは、Google がサービスを通じて提供するロギング機能を使用することもできます。

(b)廃棄ディスクおよびディスク消去ポリシー。データが記録されているディスクでパフォーマンス上の問題、エラー、またはハードウェア障害が発生し、ディスクを廃棄する場合があります(「廃棄ディスク」)。こうした廃棄ディスクについては、Google の施設外に移動する前に、再利用または破棄のための一連のデータ破壊プロセス(「ディスク消去ポリシー」)が実施されます。廃棄ディスクは、マルチステップ プロセスで消去され、少なくとも 2 つの独立した検証ツールによって完全に検証されます。消去結果は、トラッキングできるように、廃棄ディスクのシリアル番号に基づいて記録されます。データが消去された廃棄ディスクは、再利用や再導入のために、倉庫に移動されます。ハードウェア障害のために廃棄ディスクのデータを消去できない場合は、安全に保管したうえで破壊されます。ディスク消去ポリシーへの準拠を確認するために、各施設では定期的に監査が行われます。

4. スタッフのセキュリティ

Google のスタッフは、機密保持、企業倫理、適切な使用、職業上の基準に関する Google ガイドラインに準拠した形で行動する必要があります。Google は、法的に許容される範囲内で、適用される現地の労働法および法定規制に従って、合理的かつ適切な方法で身元調査を行います。

Google のスタッフは機密保持契約を締結したうえで、Google の機密保持ポリシーおよびプライバシー ポリシー確認して遵守する必要があります。スタッフには、セキュリティ トレーニングが提供されます。パートナー データを扱うスタッフは、その職務に必要な追加の要件（認定の取得など）を満たす必要があります。Google のスタッフが許可なくパートナー データを処理することはありません。

5. 復処理者のセキュリティ

復処理者に処理を委託する前に、Google は、データへのアクセスおよび提供サービスの範囲に適したレベルのセキュリティとプライバシーを当該復処理者が備えているか確認するため、そのセキュリティ慣行とプライバシー慣行の監査を実施します。Google が復処理者から提示されるリスクを評価した後、復処理者は、本規約の第 11.3 項（復処理者の利用に関する要件）に記載されている要件に従い、所定のセキュリティ、機密保持、プライバシーについて契約を締結する必要があります。

付録 3: 特定のプライバシー法

付録 3 の各項は、該当する法律がパートナーの個人データの処理に適用される場合にのみ適用されます。

欧州データ保護法

1. 追加の定義。

- 「十分なデータ保護を提供している国」とは、以下を意味します。

（a）EU GDPR に従って処理されるデータの場合は、欧州経済領域、または EU GDPR に基づき十分な保護を提供していると認められている国もしくは地域。

（b）英国の GDPR に従って処理されるデータの場合は、英国、または英国の GDPR および 2018 年データ保護法に基づき十分な保護を提供していると認められている国もしくは地域。

（c）スイスの FADP に従って処理されるデータの場合は、スイス、または以下のいずれかに該当する国もしくは地域を指します。（i）該当する場合、その国または地域の法律に従って十分な保護を提供しており、スイス連邦データ保護および情報コミッショナーが公表するリストに含まれる、または（ii）スイスの FADP に基づきスイス連邦評議会によって十分な保護を提供していると認められている国もしくは地域。

いずれの場合も、任意のデータ保護フレームワークに基づく場合を除きます。

- 「代替移転ソリューション」とは、SCC 以外の、欧州データ保護法に従って第三国への個人データの合法的な移転を可能にするソリューションを意味します。たとえば、参加事業体が十分な保護を提供すると認められているデータ保護フレームワークなどが該当します。

- 「パートナー SCC」とは、SCC（データ管理者からデータ処理者へ）、SCC（データ処理者からデータ処理者へ）、または SCC（データ処理者からデータ管理者へ）のうちいずれか該当するものを意味します。

- 「SCC」とは、パートナー SCC または SCC（データ処理者からデータ処理者へ、Google が移転元）のいずれか該当するものを意味します。
- 「SCC（データ管理者からデータ処理者へ）」とは、https://cloud.google.com/terms/sccs/eu-c2p に記載の条項を意味します。
- 「SCC（データ処理者からデータ管理者へ）」とは、https://cloud.google.com/terms/sccs/eu-p2c に記載の条項を意味します。
- 「SCC（データ処理者からデータ処理者へ）」とは、https://cloud.google.com/terms/sccs/eu-p2p に記載の条項を意味します。
- 「SCC（データ処理者からデータ処理者へ、Google が移転元）」とは、https://cloud.google.com/terms/sccs/eu-p2p-google-exporter に記載の条項を意味します。

2. 指示の通知。Google は、第 5.2 項（パートナーの指示への準拠）に基づく Google の義務、または本契約に基づく両当事者のその他の権利もしくは義務を害することなく、以下のいずれかに該当すると判断した場合、直ちにパートナーに通知します。

a. 欧州法が Google による指示への準拠を禁止している場合

b. 指示が欧州データ保護法に準拠していない場合

c. いずれの事例でも、Google がその他の理由により指示に準拠できない場合（ただし、そのような通知が欧州法により禁止されている場合を除きます）。

パートナーがデータ処理者である場合、パートナーは本項に基づき、Google から提供された通知を関連するデータ管理者に直ちに転送するものとします。

3. パートナーの監査の権利。Google は、パートナーまたはパートナーが任命した独立監査人に対し、第 7.5.2（a）項（パートナーによる監査）に記載されている監査（検査を含む）の実施を許可します。このような監査の期間中、Google は、本追加条項に基づく Google の義務遵守を証明するために必要なすべての情報を提供し、第 7.5 項（コンプライアンスの審査と監査）および本項に記載のとおり、監査に協力します。

4. データ移転。

4.1 制限付き移転。両当事者は、パートナーの個人データが十分なデータ保護を提供している国で処理される場合、またはそのような国に移転される場合、欧州データ保護法によって SCC または代替移転ソリューションが義務付けられないことを認めるものとします。パートナーの個人データがその他の国へ移転され、かつ欧州データ保護法が当該移転に適用される場合（請求先住所が EMEA 圏外であるときに、本欧州データ保護法の第 4.2 項（EMEA 圏外パートナーによる確認）に基づきパートナーによって確認された場合）（以下、「制限付き移転」）は、以下の規定が適用されます。

a. Google が制限付き移転に対して代替移転ソリューションを採用している場合、Google は関連するソリューションをパートナーに通知し、当該制限付き移転がそれに従って行われることを保証します。

b. Google が制限付き移転に対して代替移転ソリューションを採用していない場合、または Google が制限付き移転に対して（その代わりとなる代替移転ソリューションを採用することなく）代替移転ソリューションを採用しなくなったことをパートナーに通知した場合は、以下のように対応します。

i. Google の住所が十分なデータ保護を提供している国にある場合:

A. Google から復処理者への制限付き移転に関しては、SCC（データ処理者からデータ処理者へ、Google が移転元）が適用されます。

B. さらに、パートナーの請求先住所が十分なデータ保護を提供している国にない場合、Google とパートナー間の制限付き移転に関しては、パートナーがデータ管理者であるかデータ処理者であるかにかかわらず、SCC（データ処理者からデータ管理者へ）が適用されます。

ii. Google の住所が十分なデータ保護を提供している国にない場合、Google とパートナー間の制限付き移転に関しては、パートナーがデータ管理者であるかデータ処理者であるかに応じて、SCC（データ管理者からデータ処理者へ）または SCC（データ処理者からデータ処理者へ）が適用されます。

4.2 EMEA 圏外パートナーによる確認。パートナーの請求先住所が EMEA 圏外であり、かつパートナーの個人データの処理が欧州データ保護法の対象となる場合、本追加条項の付録 4（特定のプロダクト）に別段の記載がない限り、パートナーは該当するサービスの管理コンソールでその旨を確認し、管轄の監督機関を特定するものとします。

4.3 制限付き移転に関する情報。Google は、制限付き移転、追加のセキュリティ管理、およびその他の補助的な保護措置に関連する情報を、以下のようにパートナーに提供します。

a. 第 7.5.1 項（セキュリティドキュメントの審査）に記載のとおり提供します。

b. 付録 4（特定のプロダクト）に記載されている追加の場所で提供します。

c. https://cloud.google.com/terms/alternative-transfer-solution に記載されている Google による代替移転ソリューションの採用に関連して提供します。

4.4 SCC 監査。欧州データ保護法の第 4.1 項（制限付き移転）に記載のとおりにパートナー SCC が適用される場合、Google はパートナー（またはパートナーが任命した独立監査人）に対し、当該 SCC に記載されている監査の実施を許可します。また、監査中には、第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従い、当該 SCC によって要求されるすべての情報を提供します。

4.5 SCC の通知。パートナーは、SCC に言及するあらゆる通知を、関連するデータ管理者に速やかに遅滞なく転送するものとします。

4.6 データ移転リスクによる契約解除。パートナーは、現在のサービスの使用、またはサービスの使用目的に基づいて、移転されるパートナーの個人データに対して適切な安全保護対策が提供されていないと判断した場合、本契約の「都合による解除」条項に従って本契約を直ちに解除できます。そのような条項がない場合は、Google に通知することにより解除できます。

4.7 SCC の不変更。本契約（本追加条項を含む）のいかなる条項も、SCC を変更または否定すること、または欧州データ保護法に基づくデータ主体の基本的権利もしくは自由を侵害することを意図するものではありません。

4.8 *SCC* の優先。本追加条項を参照することにより援用されるパートナー SCC と、本契約の残りの部分（本追加条項を含む）との間に矛盾または不一致がある場合は、パートナー SCC が優先されます。

5. 復処理者の利用に関する要件。欧州データ保護法は、該当する場合、GDPR 第 28(3)項に言及されている、本追加条項に記載されたデータ保護義務を、Google が使用するすべての復処理者に対し、書面契約を通じて課すことを Google に要求しています。

CCPA

1. 追加の定義。

- 「CCPA」とは、2018 年のカリフォルニア州消費者プライバシー法(2020 年のカリフォルニア州プライバシー権法による修正を含む)とすべての施行規則を意味します。
- 「パートナーの個人データ」には、「個人情報」が含まれます。
- 「業務」、「業務目的」、「消費者」、「個人情報」、「処理」、「セール」、「販売」、「サービス プロバイダ」、「共有」の各用語は、CCPA で定義された意味を有します。

2. 禁止事項。CCPA に従ったパートナーの個人データの処理に関して、CCPA によって別途許可されていない限り、Google は第 5.2 項(パートナーの指示への準拠)に基づく Google の義務を害することなく、以下の行為を行いません。

a. パートナーの個人データを販売または共有すること。

b. パートナーの個人データを保持、使用、または開示すること。ただし、以下の場合を除きます。

i. パートナーに代わって行う CCPA に基づく業務目的、ならびにサービスおよび TSS を履行する特定の目的で行う場合。

ii. Google とパートナーとの直接的な業務関係の範囲内で行う場合。

c. Google が第三者から、または第三者に代わって受領した、あるいは消費者と自身とのやり取りから収集した個人情報とパートナーの個人データを組み合わせる、または更新すること。

3. コンプライアンス。Google は、第 5.2 項(パートナーの指示への準拠)に基づく Google の義務、または本契約に基づく両当事者のその他の権利もしくは義務を害することなく、Google が CCPA に基づく義務を履行できないと判断した場合、パートナーに通知します。ただし、当該通知が適用法により禁止されている場合はこの限りではありません。

4. パートナーの介入。Google が、本条の第 3 項(コンプライアンス)または第 7.2.1 項(インシデントの通知)に基づき、パートナーの個人データの不正使用についてパートナーに通知した場合、パートナーは以下の方法により、当該不正使用を停止または是正するために合理的かつ適切な措置を講じることができます。

a. 該当する場合、第 7.2.2 項(データ インシデントの詳細)に従って Google が推奨する措置を講じる。

b. 第 7.5.2(a)項(パートナーによる監査)または第 9.1 項(アクセス、訂正、制限付きの処理、ポータビリティ)に基づく権利を行使する。

トルコ

1. 追加の定義。

- 「トルコデータ保護法」とは、2016 年 4 月 7 日付トルコ個人データ保護法第 6698 号を意味します。
- 「トルコ個人データ保護機関」とは、Kişisel Verileri Koruma Kurumu を意味します。
- 「トルコ SCC」とは、トルコデータ保護法に基づく標準契約条項を意味します。

2. データ移転。

2.1 補足条項。パートナーの請求先住所がトルコ国内にあり、Google がトルコデータ保護法に基づくパートナーの個人データの移転に関して、パートナーが同意するための任意の追加条項（トルコ SCC を含む）を提供した場合、これらの条項は、以下の第 2.2 項（管轄当局への通知）に従ってトルコ個人データ保護機関に通知された日付以降、パートナーが Google に証明したとおり、本追加条項を補足するものとします。

2.2 管轄当局への通知。パートナーが本第 2 項（データ移転）に基づきトルコ SCC を締結した場合、パートナーは、トルコデータ保護法で義務付けられているとおり、トルコ SCC 署名後 5 営業日以内に、トルコ個人データ保護機関にトルコ SCC の使用について通知する責任を負います。

2.3 SCC 監査。パートナーが本第 2 項（データ移転）に基づきトルコ SCC を締結した場合、Google は、パートナー（またはパートナーが任命した独立監査人）が当該 SCC に記載されているとおりに監査を実施することを許可し、監査中は、第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従い、当該 SCC で要求されるすべての情報を利用可能にします。

2.4 データ移転リスクによる契約解除。パートナーは、現在のサービスの使用、またはサービスの使用目的に基づいて、移転されるパートナーの個人データに対して適切な安全保護対策が提供されていないと判断した場合、該当する契約の「都合による解除」条項に従って当該契約を直ちに解除できます。そのような条項がない場合は、Google に通知することにより解除できます。

2.5 トルコ SCC の不変更。本契約（本追加条項を含む）のいかなる条項も、トルコ SCC を変更または否定すること、またはトルコデータ保護法に基づくデータ主体の基本的権利もしくは自由を侵害することを意図するものではありません。

2.6 SCC の優先。トルコ SCC（パートナーが締結した場合は、参照することにより本追加条項に援用されます）と本契約のその他の部分（本追加条項を含む）との間に矛盾または不一致がある場合は、トルコ SCC が優先されます。

イスラエル

1. 追加の定義。

- 「イスラエル プライバシー保護法」とは、1981 年イスラエル プライバシー保護法とそれに基づいて公布されたすべての規制を意味します。

2. 同義語。本追加条項で使用される「データ管理者」、「個人データ」、「処理」、「データ処理者」の同義語は、イスラエル プライバシー保護法で定義された意味を有します。

3. パートナーの監査の権利。Google は、パートナーまたはパートナーが任命した独立監査人に対し、第 7.5.2（a）項（パートナーによる監査）に記載されている監査（検査を含む）の実施を許可します。

付録 4: 特定のプロダクト

本付録 4 の各項の条項は、対応するサービスによるパートナー データの処理に関してのみ適用されます。

Google Cloud Platform

1. 追加の定義。

- 「アカウント」とは、本契約で定義されていない場合、パートナーの Google Cloud Platform アカウントを意味します。
- 「Google Cloud Platform」とは、https://cloud.google.com/terms/services に記載されている Google Cloud Platform サービスを意味し、第三者の提供物は含まれません。
- 「第三者の提供物」とは、本契約で定義されていない場合、以下を意味します。(a)Google Cloud Platform またはソフトウェアに組み込まれていない第三者のサービス、ソフトウェア、製品、その他の提供物。(b)本契約におけるサービス固有の規約の「第三者規約」の項で指定されている提供物。(c)第三者のオペレーティング システム。

2. コンプライアンス証明書。Google Cloud Platform の監査対象サービスに対するコンプライアンス証明書には、ISO 27017 および ISO 27018 の証明書、ならびに PCI DSS のコンプライアンス証明書も含まれます。

3. データセンターの所在地。Google Cloud Platform のデータセンターの所在地は、https://cloud.google.com/about/locations/ に記載されています。

4. 復処理者に関する情報。Google Cloud Platform の復処理者の名称、所在地、および活動内容は、https://cloud.google.com/terms/subprocessors に記載されています。

5. クラウドデータ保護チーム。Google Cloud Platform のデータ保護チームには、https://support.google.com/cloud/contact/dpo から連絡できます。

6. 制限付き移転に関する情報。制限付き移転、追加のセキュリティ管理、およびその他の補助的な保護措置に関する追加情報は、https://cloud.google.com/privacy で確認できます。

7. サービス固有の規約。

Bare Metal Solution（Google Cloud Platform）

Bare Metal Solution は、基盤となるインフラストラクチャ リソースへの仮想化されていないアクセスを提供するため、設計上、特定の明確な特徴を持っています。

1. 修正。本追加条項は、Bare Metal Solution に関して、以下のように修正されます。

- 「Google の第三者監査人」の定義は、以下の内容に置き換えられます。
    - 「Google の第三者監査人」とは、Google または Bare Metal Solution の復処理者によって任命された、適格かつ独立した第三者監査人を意味し、その時点での身元は、パートナーの要求に応じて Google が開示するものとします。

- 以下の条項が削除されます。
    - 第 7.1.1 項（Google のセキュリティ対策）から、「パートナー データを暗号化する」という語句。
    - 付録 2（セキュリティ対策）の第 1（a）項にある「サーバー オペレーティング システム」および「ビジネスの継続性」の項目。
    - 付録 2 の第 1（b）項にある「外部攻撃対象領域」、「侵入検知」、「暗号化テクノロジー」の項目。
    - 付録 2 の第 3 項（a）にある以下の文章:
        - Google は、Google が所有するサーバー上のマルチテナント環境にデータを保存します。パートナーから特段の指示（データの場所の選択など）がない限り、地理的に分散した複数のデータセンター間でパートナー データを複製します。

2. コンプライアンス証明書および **SOC** レポート。Google またはその復処理者は、Bare Metal Solution がセキュリティ対策の継続的な有効性を検証するために、少なくとも以下（またはそれと同等もしくはより高度な代替手段）を維持します。

a. ISO 27001 の証明書および PCI DSS のコンプライアンス証明書（以下「BMS コンプライアンス証明書」）。

b. 少なくとも 12 か月に 1 度実施される監査に基づき毎年更新される SOC 1 および SOC 2 レポート（以下「BMS SOC レポート」）。

3. セキュリティドキュメントの審査。Google は、本追加条項に基づく自身の義務遵守を証明するため、BMS コンプライアンス証明書および BMS SOC レポートをパートナーが確認できるようにします。パートナーがデータ処理者である場合は第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従って、Google は、関連するデータ管理者が BMS SOC レポートにアクセスできるよう要求することをパートナーに許可します。

4. パートナーの義務。Bare Metal Solution に関する Google の明示的な義務を制限することなく、パートナーは、パートナー データおよび Bare Metal Solution に保存または Bare Metal Solution を通じて処理されるその他のコンテンツのセキュリティを保護し、維持するために合理的な措置を講じるものとします。

5. 免責条項。本契約（本追加条項も含む）に矛盾する規定がある場合も、Google は Bare Metal Solution に関する以下の事項について一切責任を負いません。

a. アクセス制御、暗号化、ファイアウォール、ウイルス対策、脅威検出、セキュリティ スキャンなどの非物理的セキュリティ

b. ロギングとモニタリング

c. ハードウェア以外のメンテナンスまたはサポート

d. あらゆる冗長性または高可用性構成を含むデータ バックアップ

e. ビジネスの継続性および障害復旧に関するポリシーまたは手順

パートナーは、Bare Metal Solution でパートナーが利用、アップロード、またはホストするあらゆるオペレーティング システム、パートナー データ、ソフトウェア、およびアプリケーションについて、そのセキュリティ確保（Bare Metal

Solution サーバーの物理的セキュリティを除く）、ロギングとモニタリング、メンテナンスとサポート、およびバックアップに単独で責任を負うものとします。

Cloud NGFW（Google Cloud Platform）

「Cloud NGFW Enterprise」（CNE）と呼ばれる Cloud NGFW のエディションは、サイバーセキュリティ リスクを軽減するように設計されているため、特定の明確な特徴を持っています。

1. 修正。本追加条項は、CNE に関して次のように修正されます。

- 第 6.1 項（パートナーによる削除）および第 6.2 項（期間終了時のデータ返却または削除）は、Google または再処理者が、TSS の目的で送信され、CNE によってセキュリティ上の脅威として指定されたファイルまたはネットワーク トラフィックのパケット キャプチャを保持することを妨げるものではありません。ただし、そのファイルまたはネットワーク トラフィックのパケット キャプチャにパートナーの個人データが含まれていない場合に限ります。

Google Distributed Cloud Edge（Google Cloud Platform）

Google Distributed Cloud Edge（「*GDCE*」）は、Google データセンターにはデプロイされず、その設計上、特定の明確な特徴を持っています。

1. 修正。本追加条項は、GDCE に関して次のように修正されます。

- 「Google のシステム」への言及は「本機器」に置き換えられます。
- 第 6.2 項（期間終了時のデータ返却または削除）は、以下の内容に置き換えられます。
    - 6.2 期間終了時のデータ返却または削除。パートナーは、適用法に従い、期間終了時に残りのパートナー データ（既存のコピーを含む）を本機器からすべて削除するよう、Google に指示します。パートナーが期間終了後もパートナー データの保持を希望する場合は、期間終了前に当該データをエクスポートまたはコピーできます。Google は、本第 6.2 項の指示に、合理的に実行可能な限り速やかに、かつ最長 180 日以内に従うものとします。ただし、欧州データ保護法が適用される状況では欧州法によって保管が義務付けられる場合、またはその他の該当するプライバシー法が適用される状況では適用法によって保管が義務付けられる場合を除きます。
- 第 10.1 項（データ保存 / 処理施設）の末尾に、「または顧客のロケーションが所在する場所」という文言が追加されます。
- 付録 2（セキュリティ対策）の第 1 項（データセンターおよびネットワーク セキュリティ）は、以下の内容に置き換えられます。
    - **1.** ローカルマシンおよびネットワーク セキュリティ

ローカルマシン。パートナー データは、顧客のロケーションに導入される機器にのみ保存されます。

サーバー オペレーティング システム。Google のサーバーでは、アプリケーション環境用にカスタマイズした Linux ベースのシステムを使用しています。Google は、GDCE を提供するために使用されるコードのセキュリティを高め、GDCE 本番環境におけるセキュリティ サービスを強化するために、コードレビュー プロセスを採用しています。

暗号化テクノロジー。Google は、HTTPS 暗号化（SSL 接続や TLS 接続とも呼ばれます）および転送中のデータの暗号化を可能にしています。Google のサーバーは、RSA と ECDSA で署名された一時楕円曲線ディフィーヘルマン暗号鍵交換をサポートしています。この PFS（Perfect Forward Secrecy: 前方秘匿性）により、トラフィックを保護し、侵害された鍵または暗号の解読による影響を最小限に抑えることができます。また、Google は、少なくとも AES128 または同等の方式を用いた保存データの暗号化も利用可能にしています。GDCE は CMEK と統合されています。詳細については、https://cloud.google.com/kms/docs/cmek をご覧ください。

Cloud VPN への接続。Google は、IPSEC VPN 接続経由で Cloud VPN を使用し、本機器とパートナーの Virtual Private Cloud との間で、堅牢で暗号化された相互接続を有効化し、構成することをパートナーに許可しています。

ストレージの接続。パートナーのデータ ストレージはサーバーに接続されます。ディスクが盗まれたり、保管中にコピーされたりしても、当該ディスクの内容はサーバー外部では復元できません。

- 付録 2（セキュリティ対策）の第 2 項（アクセス制御とサイト管理）および第 3 項（データ）は削除されます。

2. 不適用条項。本契約（本追加条項を含む）における Google の義務、または関連するセキュリティ文書（ホワイトペーパーを含む）における記述のうち、Google データセンターの運用に依存するものは、GDCE には適用されません。

Google が管理するマルチクラウド（**Google Cloud Platform**）

Google が管理するマルチクラウド サービスは、第三者のインフラストラクチャを含むものであり、その設計上、特定の明確な特徴を持っています。

1. 追加の定義。

- 「Google が管理する MCS データ処理の修正条項」とは、https://cloud.google.com/terms/mcs-data-processing-terms に記載されている条項を意味します。

2. マルチクラウド データ処理規約。Google が管理する MCS データ処理の修正条項は、Google Cloud Platform 向けの Google が管理するマルチクラウド サービスに関して、本追加条項を補足し修正するものです。

Google Cloud VMware Engine（**Google Cloud Platform**）

Google は、パートナーの VMware 環境にアクセスしたり、パートナーの VMware 環境で個人データを暗号化したりすることはできません。

NetApp Volumes（**Google Cloud Platform**）

1. 修正。本追加条項は、NetApp Volumes に関して次のように修正されます。

- 「Google の第三者監査人」の定義は、以下の内容に置き換えられます。
    - 「Google の第三者監査人」とは、Google または NetApp Volumes の復処理者によって任命された、適格かつ独立した第三者監査人を意味し、その時点での身元は、パートナーの要求に応じて Google が開示するものとします。
- 付録 2（セキュリティ対策）の第 3（a）項（データの保存、隔離、および記録）は、以下の内容に置き換えられます。

- (a)データの保存、隔離、および記録。Google は、NetApp, Inc. が所有するサーバー上のマルチテナント環境にデータを保管します。特段の指示(データの場所の選択など)がない限り、地理的に分散した複数のデータセンターを間でパートナー データを複製します。また、Google はパートナー データを論理的に隔離します。パートナーには、特定のデータ共有ポリシーの管理権が付与されます。これらのポリシーにより、パートナーはサービスの機能に従って、特定の目的に応じてエンドユーザーに適用される共有設定を決定できます。パートナーは、Google がサービスを通じて提供するロギング機能を使用することもできます。

2. コンプライアンス証明書および **SOC** レポート。Google またはその復処理者は、NetApp Volumes に関して、少なくとも以下(またはこれらと同等、もしくはより高度な代替の証明書)を取得します。

a. ISO 27001 の証明書および PCI DSS のコンプライアンス証明書(以下「NetApp コンプライアンス証明書」)。

b. 少なくとも 12 か月に 1 度実施される監査に基づき毎年更新される SOC 1 および SOC 2 レポート(以下「NetApp SOC レポート」)。

3. セキュリティドキュメントの審査。Google は、本追加条項に基づく自身の義務遵守を証明するため、NetApp コンプライアンス証明書および NetApp SOC レポートをパートナーが確認できるようにします。パートナーがデータ処理者である場合、第 7.5.3 項(審査および監査に関する追加のビジネス規約)に従い、Google は、関連するデータ管理者が NetApp SOC レポートにアクセスできるよう要求することをパートナーに許可します。

Looker(オリジナル)

1. 追加の定義。

- 「管理コンソール」とは、各インスタンスに適用される管理コンソールを意味します。
- 「Google が管理する MCS データ処理の修正条項」とは、該当する場合、https://cloud.google.com/terms/mcs-data-processing-terms に記載されている条項を意味します。
- 「Google が管理するマルチクラウド サービス」とは、該当する場合、第三者クラウド プロバイダのインフラストラクチャ上でホストされる、特定の Google サービス、プロダクト、および機能を意味します。
- 「Looker(オリジナル)」とは、企業が複数のデータソースのデータ分析とビジネス指標の定義を行えるようにする、クラウドベースのインフラストラクチャ(該当する場合)とソフトウェア コンポーネント(関連する API など)の統合プラットフォームを意味します。これは、本契約に基づき Google がパートナーに提供するものです。Looker(オリジナル)に第三者の提供物は含まれません。
- 「マルチクラウド サービスのサードパーティ プロバイダ」は、Google が管理する MCS データ処理の修正条項で定義された意味を有します。
- 「注文フォーム」は、本契約で定義された意味を有します。ただし、パートナーが販売パートナーまたはオンライン ショッピングモールを通じて購入した場合、または試用もしくは評価契約に基づいて試用目的もしくは評価目的で Looker を使用している場合は、Google が許可する別の書面形式(メールまたはその他の電子手段が許可される)を意味する場合もあります。

2. 修正。本追加条項は、Looker(オリジナル)に関して次のように修正されます。

- 「通知用メールアドレス」の定義は、以下の内容に置き換えられます。
    - 「通知用メールアドレス」とは、パートナーが注文フォームまたは Looker（該当する場合）を通じて、Google からの特定の通知を受信するために指定したメールアドレスを意味します。
- 付録 3（特定のプライバシー法）に記載の SCC（データ管理者からデータ処理者へ）、SCC（データ処理者からデータ管理者へ）、SCC（データ処理者からデータ処理者へ）、および SCC（EU のデータ処理者からデータ処理者へ、Google が移転元）の定義は、以下の内容に置き換えられます。
    - 「SCC（データ管理者からデータ処理者へ）」とは、https://cloud.google.com/terms/looker/legal/sccs/eu-c2p に記載の条項を意味します。
    - 「SCC（データ処理者からデータ管理者へ）」とは、https://cloud.google.com/terms/looker/legal/sccs/eu-p2c に記載の条項を意味します。
    - 「SCC（データ処理者からデータ処理者へ）」とは、https://cloud.google.com/terms/looker/legal/sccs/eu-p2p に記載の条項を意味します。
    - 「SCC（EU のデータ処理者からデータ処理者へ、Google が移転元）」とは、https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group に記載の条項を意味します。
- 第 10.1 項（データ保存 / 処理施設）の末尾に、「またはマルチクラウド サービスのサードパーティ プロバイダが施設を維持している場所」という文言が追加されます。

3. セキュリティに対するパートナーの追加責任。パートナーは、Google が管理および制御するシステムを除き、パートナーの環境、データベース、および Looker（オリジナル）の構成のセキュリティに対して責任を負うものとします。

4. コンプライアンス証明書および **SOC** レポート。Looker（オリジナル）監査対象サービスに関するコンプライアンス証明書および SOC レポートは、関連するサービスが使用されるホスティング環境によって異なる場合があります。Google は、特定のホスティング環境で利用可能なコンプライアンス証明書および SOC レポートの詳細を要求に応じて提供します。

5. データセンターの所在地。Looker（オリジナル）データセンターの所在地は、該当する注文フォームに記載されるか、Google によって別途指定されます。

6. EMEA 圏外パートナーによる確認の不実施。パートナーは、Looker（オリジナル）について、付録 3（特定のプライバシー法）の欧州データ保護条項の第 4.2 項（EMEA 圏外パートナーによる確認）に記載されている監督機関を確認する義務はありません。

7. 制限付き移転に関する情報。Looker（オリジナル）について、制限付き移転、追加のセキュリティ管理、およびその他の補助的な保護措置に関する追加情報は、https://docs.looker.com で確認できます。

8. 復処理者に関する情報。Looker（オリジナル）の復処理者の名称、所在地、および活動内容は

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors および

b. https://cloud.google.com/terms/subprocessors に記載されています。

9. Google が管理するマルチクラウド（**Looker**（オリジナル））

Google が管理するマルチクラウド サービスは、第三者のインフラストラクチャを含むものであり、その設計上、特定の明確な特徴を持っています。

9.1 マルチクラウド データ処理規約。Google が管理する MCS データ処理の修正条項は、Looker（オリジナル）向けの Google が管理するマルチクラウド サービスに関して、本追加条項を補足し修正するものです。

10. クラウドデータ保護チーム。Looker（オリジナル）のデータ保護チームには、https://support.google.com/cloud/contact/dpo から連絡できます。

11. Google のデータ処理記録。適用されるプライバシー法によって、Google がパートナーもしくはその顧客に関する特定の情報を収集し、その記録を維持することが義務付けられる場合、Google がパートナーに別の方法による当該情報の提供および更新を要求しない限り、パートナーは要求に応じて当該情報を Google に提供し、当該情報を正確かつ最新に保つために必要な更新について Google に通知するものとします。

12. 追加のアプリケーション セキュリティ対策。Google は、Looker（オリジナル）について、以下に挙げる追加のセキュリティ対策を実装および維持します。

a. Google は、セキュリティ アーキテクチャに関して、少なくとも業界標準の慣行に従います。Google のアプリケーションで使用されるプロキシ サーバーは、IP 拒否リストへの追加および接続レート制限を通じて攻撃をフィルタリングする単一のポイントを提供することにより、Looker への安全なアクセスを実現します。

b. パートナーの管理者は、パートナーまたはパートナーのエンドユーザーが要求する技術サポートを提供するために、Google のスタッフによるアプリケーションへのアクセスを制御します。

SecOps サービス

1. 追加の定義。

- 「アカウント」とは、本契約で定義されていない場合は、パートナーの SecOps サービスまたは Google Cloud Platform アカウントのいずれか該当するものを意味します。
- 「SecOps サービス」とは、https://cloud.google.com/terms/secops/services に記載されている Chronicle SIEM、Chronicle SOAR、および Mandiant Solutions を意味します（第三者の提供物は含まれません）。疑念の発生を避けるために記すと、SecOps サービスに Mandiant のマネージド サービスおよびコンサルティング サービスは含まれません。
- 「第三者の提供物」とは、本契約で定義されていない場合、以下を意味します。(a) SecOps サービスまたはソフトウェアに組み込まれていない第三者のサービス、ソフトウェア、製品、その他の提供物。(b) 第三者のオペレーティング システム。

2. 修正。本追加条項は、SecOps サービスに関して次のように修正されます。

- 「追加のセキュリティ管理」の定義は、以下の内容に置き換えられます。

- 「追加のセキュリティ管理」とは、パートナーが自身の選択および / または判断で使用できるセキュリティに関するリソース、機能、および / または管理（存在する場合）を意味します。これには、暗号化、ロギングとモニタリング、Identity and Access Management、セキュリティ スキャン（存在する場合）などが含まれます。

- 「監査対象サービス」の定義は、以下の内容に置き換えられます。

  - 「監査対象サービス」とは、https://cloud.google.com/security/compliance/secops/services-in-scope において、関連する証明書またはレポートの対象範囲となっているその時点で最新の SecOps サービスを指します。Google は、本契約に従って廃止された場合を除き、この URL から SecOps サービスを削除することはありません。

- 付録 3（特定のプライバシー法）に記載の SCC（データ管理者からデータ処理者へ）、SCC（データ処理者からデータ管理者へ）、SCC（データ処理者からデータ処理者へ）、および SCC（EU のデータ処理者からデータ処理者へ、Google が移転元）の定義は、以下の内容に置き換えられます。

  - 「SCC（データ管理者からデータ処理者へ）」とは、https://cloud.google.com/terms/secops/sccs/eu-c2p に記載の条項を意味します。

  - 「SCC（データ処理者からデータ管理者へ）」とは、https://cloud.google.com/terms/secops/sccs/eu-p2c に記載の条項を意味します。

  - 「SCC（データ処理者からデータ処理者へ）」とは、https://cloud.google.com/terms/secops/sccs/eu-p2p に記載の条項を意味します。

  - 「SCC（データ処理者からデータ処理者へ、Google が移転元）」とは、https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter に記載の条項を意味します。

- 本追加条項の第 7.4 項（コンプライアンス証明書および SOC レポート）は、以下のように修正されます。

  - 7.4 コンプライアンス証明書および SOC レポート。Google は、監査対象サービスにおけるセキュリティ対策の継続的な有効性を確保するため、少なくとも https://cloud.google.com/security/compliance/secops/services-in-scope で特定されている証明書およびレポート（以下「コンプライアンス証明書」および「SOC レポート」）を維持するものとします。

Google はいつでも基準を追加できます。また、コンプライアンス証明書または SOC レポートを、同等の、または増補された代替文書に差し換える場合があります。

3. データセンターの所在地。SecOps サービスのデータセンターの所在地は、https://cloud.google.com/terms/secops/data-residency に記載されています。

4. EMEA 圏外パートナーによる確認の不実施。パートナーは、SecOps サービスについて、付録 3（特定のプライバシー法）の欧州データ保護条項の第 4.2 項（EMEA 圏外パートナーによる確認）に記載されている監督機関を確認する義務はありません。

5. 復処理者に関する情報。SecOps サービスのすべての復処理者の名称、所在地、および活動は、https://cloud.google.com/terms/secops/subprocessors で確認できます。

6. クラウドデータ保護チーム。SecOps サービスのデータ保護チームには、https://support.google.com/cloud/contact/dpo（および / または Google が随時提供するその他の手段）から連絡できます。

7. Google のデータ処理記録。適用されるプライバシー法によって、Google がパートナーに関する特定の情報を収集しその記録を維持することが義務付けられている場合、Google がパートナーに別の方法による当該情報の提供および更新を要求しない限り、パートナーは要求に応じて当該情報を Google に提供し、当該情報を正確かつ最新に保つために必要な更新について Google に通知するものとします。

旧バージョンのデータ処理およびセキュリティ規約（パートナー）:

2022 年 6 月 30 日 2021 年 9 月 24 日 2020 年 8 月 20 日 2020 年 8 月 10 日 2020 年 7 月 17 日 2019 年 10 月 1 日 2019 年 2 月 28 日 2018 年 5 月 25 日 2018 年 3 月 13 日

旧バージョンの *SecOps* サービス *DPST*（パートナー）:

2023 年 2 月 6 日 2022 年 10 月 31 日 2021 年 9 月 27 日

旧バージョン（最終更新日: *2024* 年 *10* 月 *30* 日）

2024 年 10 月 15 日 2024 年 9 月 26 日 2024 年 9 月 9 日 2024 年 4 月 9 日 2023 年 11 月 8 日 2023 年 8 月 15 日 2022 年 9 月 20 日