Cloud のデータ処理に関する追加条項（お客様）

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 とお客様との間の契約（以下で定義）に組み込まれます。本追加条項は、Google Cloud Platform、Looker（オリジナル）、Google SecOps サービス、または組織向け Google Cloud Skills Boost の契約では「データ処理およびセキュリティ規約」、Google Workspace または Cloud Identity の契約では「データ処理の修正条項」、Mandiant コンサルティング サービスおよびマネージド サービスの契約では「データ処理に関する追加条項」と称していたものです。

一般条項

1. 概要

本追加条項は、プライバシー、データ セキュリティ、およびデータ保護に関する適用法に基づく義務を含め、お客様のデータ（以下で定義）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（以下で定義）にその効力が発生し、追加条項発効日より前にお客様の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の意味は、契約において定めるとおりとします。

2. 定義

2.1 本追加条項内での定義:

- 「追加条項発効日」とは、お客様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合意した日を意味します。
- 「追加のセキュリティ管理策」とは、お客様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、および管理策を意味します。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お客様に提供することに同意した契約事項を意味します。
- 「適用されるプライバシー法」とは、お客様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になっているその時点で最新のサービスを指します。Google は、該当する契約に従って廃止されている場合を除き、この URL からサービスを削除することはできません。

- 「コンプライアンス証明書」の意味は、第 7.4 項（コンプライアンス証明書および SOC レポート）で定義されているとおりとします。
- 「お客様のデータ」の意味は、契約で定義されていない場合は、付録 4（特定のプロダクト）で定義されているとおりとします。
- 「お客様の個人データ」とは、適用されるプライバシー法において定義されてい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、お客様のデータに含まれる個人データを意味します。
- 「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お客様の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、「個人データの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転に関する、ならびに指令 95/46/EC を廃止する欧州議会および理事会の 2016 年 4 月 27 日付の規則（EU）2016/679」を意味します。
- 「欧州データ保護法」とは、（a）GDPR または（b）スイス FADP のうち、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 がお客様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 がお客様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 がお客様の個人データの処理に適用される場合）のうち、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 のうち、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を意味します。なお、Google の第三者監査人の選任時に Google はその身元をお客様に開示します。
- 「指示」の意味は、第 5.2 項（お客様の指示への準拠）で定義されているとおりとします。
- 「通知用メールアドレス」とは、お客様が 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。
- 「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」の意味は、第 7.1.1 項（Google のセキュリティ対策）で規定されているとおりとします。
- 「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」の意味は、第 7.4 項（コンプライアンス証明書および SOC レポート）で規定されているとおりとします。

- 「復処理者」とは、サービスおよび TSS の一部を提供するために、お客様のデータを処理することが本追加条項に基づいて許可されている第三者である別のデータ処理者を意味します（該当する場合）。

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

- 「契約期間」とは、追加条項発効日から 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（なお、該当する場合、契約期間には、サービスの提供が一時停止する可能性がある期間および Google が移行目的でサービスの提供を継続する可能性がある契約終了後の期間が含まれます）。

- 「英国 GDPR」とは、英国の 2018 年欧州連合離脱法、および同法に基づいて制定された該当する二次法に従い、EU 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ている「個人データ」、「データ主体」、「処理」、「データ管理者」、「データ処理者」という用語の意味は、適用されるプライバシー法で定義されているとおり、またはそのような定義もしくは法律がない場合は、EU GDPR で定義されているとおりとします。

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が要求しているとおり、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

該当する契約が終了または期間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 がお客様のデータをすべて削除するまで有効であり、かかる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。お客様の個人データに関して、Google はデータ処理者であり、お客様はデータ管理者またはデータ処理者のうち、いずれか該当するものです。

4.2 処理の概要。お客様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、お客様の個人データの処理に関連する自己の義務を遵守するものとします。

4.4 その他の法的条項。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がお客様の個人データの処理に適用される範囲において、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）に記載されているとおりに優先します。

5. データ処理

5.1 データ処理者であるお客様。お客様がデータ処理者である場合:

a. お客様は、関連するデータ管理者が以下について承認していることを継続的に保証します。

i. 指示。

ii. お客様が 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）に記載されているとおり、Google が復処理者を関与させること。

b. お客様は、Google が第 7.2.1 項（インシデント通知）、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）に基づいて提供した通知を、関連するデータ管理者に速やかに、かつ不当に遅滞することなく転送するものとします。

c. お客様は、Google データセンターの場所、または復処理者の名称、所在地、および活動について、本追加条項に基づき Google から提供を受けたその他の情報を、関連するデータ管理者に提供できます。

5.2 お客様の指示への準拠。お客様は Google に対し、該当する契約（本追加条項を含む）に従って、お客様のデータを以下のとおりにのみ処理するよう指示します。

a. サービスおよび TSS の提供、セキュリティ確保、および監視を処理目的とする（該当する場合）。

b. さらに以下を通じて指定されるとおりとする:

i. お客様によるサービスの利用（管理コンソール経由を含む）および TSS の利用（該当する場合）

ii. お客様から提供を受け、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、またはその他の適用されるプライバシー法の適用があ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 お客様による削除。Google はお客様に対し、サービスの機能に沿った方法で契約期間中にお客様のデータを削除することを許可します。お客様がお客様のデータを削除するために契約期間中にサービスを使用し、お客様がそのデータを復元できない場合、かかる使用により、Google のシステムから関連するお客様のデータを削除するという Google への指示が成立します。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義務づけられている場合、またはその他の適用されるプライバシー法の適用がある状況ではその適用法によって保存が義務付けられている場合を除き、合理的に実行可能な限り速やかに、ただし最長 180 日以内にこの指示に従います。

6.2 契約期間終了時のデータ返却またはデータ削除。お客様が契約期間終了後もお客様のデータの保持を希望する場合は、そのデータを返却するよう、契約期間中に第 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 に指示できます。第 6.3 項（削除延期指示）に従うことを条件として、お客様は契約期間の終了時に Google のシステムに残っているすべてのお客様のデータ（既存のコピーを含む）を削除するよう 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義務づけられている場合を除き、またはその他の適用されるプライバシー法の適用がある状況ではそ

の適用法によって保存が義務づけられている場合を除き、合理的に実行可能な限り速やかに、ただし最長 180 日以内にこの指示に従います。

6.3. 削除延期指示。第 6.2 項（契約期間終了時のデータ返却またはデータ削除）に記載されている削除指示の対象となるお客様のデータが、第 6.2 項に基づく該当する契約期間が終了した場合にも処理される範囲で、継続する契約期間がある契約に関しては、当該削除指示は、継続する契約期間が終了したときに限り、そのようなお客様のデータに関してその効力が生じるものとします。明確にするために記すと、本追加条項は、お客様のデータが Google によって削除されるまで、そのようなお客様のデータに継続的に適用されます。

7. データ セキュリティ

7.1 Google のセキュリティ対策、管理策、支援。

7.1.1 Google のセキュリティ対策。Google は、お客様のデータを偶発的または違法な破壊、損失、改ざん、不正開示、および不正アクセスから保護するために、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（以下「セキュリティ対策」）を実施および維持します。セキュリティ対策には、お客様の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のに役立つ措置、インシデント発生後にお客様のデータへのタイムリーなアクセスを復元するのに役立つ措置、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。ただし、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ことを条件とします。

7.1.2 アクセスおよびコンプライアンス。Google は、次のとおりとします。

a. 従業員、請負業者、および復処理者がお客様の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. 従業員、請負業者、および復処理者の業務範囲に適用される範囲において、かかる従業員、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. お客様の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徹底します。

7.1.3 追加のセキュリティ管理策。Google は、以下の目的で追加のセキュリティ管理策を実行可能にします。

a. お客様のデータを保護するための措置をお客様が講じることができるようにするため。

b. お客様のデータのセキュリティ確保および使用、ならびにお客様のデータへのアクセスに関する情報をお客様に提供するため。

7.1.4 Google のセキュリティ支援。Google は（お客様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侵害および個人データ侵害に関するお客様（または、お客様がデータ処理者である場合は関連するデータ管理者）の義務の遵守徹底を、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策）に従って、追加のセキュリティ管理策を実行可能にする。

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、該当する契約（本追加条項を含む）に含まれている情報を提供する。

e. お客様（または関連するデータ管理者）が上述の義務を遵守するために上記（a）～（d）号が不十分である場合、お客様の要求に基づき、お客様をさらにかつ合理的に協力および支援すること。

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、不当に遅滞することなく速やかにお客様に通知し、被害を最小限に抑えつつ、お客様のデータを保護するために合理的な措置を速やかに講じます。

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: データ インシデントの性質（影響を受けたお客様のリソースを含む）、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お客様に推奨する措置（存在する場合）、および追加情報を得るための詳細な連絡先情報。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、不当に遅滞することなく提供します。

7.2.3 Google によるお客様のデータの評価義務の不存在。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お客様の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）に基づいて Google がデータ インシデント通知またはデータ インシデント レスポンスを発したとしても、データ インシデントに関する過失および責任を Google が認めたと解釈されることはないものとします。

7.3 お客様のセキュリティ責任およびセキュリティ評価。

7.3.1 お客様のセキュリティ責任。第 7.1 項（Google のセキュリティ対策、管理策、支援）、第 7.2 項（データ インシデント）、および該当する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、お客様は以下に述べる自ら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におけるお客様の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. お客様の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策を利用すること。

b. お客様がサービスへのアクセスで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. 必要に応じてお客様のデータのバックアップを作成する、またはコピーを保持すること。

7.3.2 お客様のセキュリティ評価。お客様は、（最新技術、実装コスト、ならびにお客様のデータの処理の性質、範囲、および状況、ならびに個人へのリスクを考慮したうえで）サービス、セキュリティ対策、追加のセキュリティ管理策、および本第 7 条（データ セキュリティ）に基づく Google の取り組みが、お客様の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します。

7.4 コンプライアンス証明書および SOC レポート。Google は、セキュリティ対策の継続的な有効性を検証するために、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 レポートおよび 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、Google は、コンプライアンス証明書および 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、Google が本追加条項に基づく自己の義務を遵守していることを証明するために、お客様によるセキュリティドキュメントの審査を目的として、当該セキュリティドキュメントを提供します。また、お客様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、お客様が関連するデータ管理者のために SOC レポートへのアクセスを要求することを許可します。

7.5.2 お客様の監査権。

a. お客様による監査。Google は、適用されるプライバシー法において義務づけられている場合、Google が本追加条項に基づく自己の義務を遵守していることを検証するための監査（検査を含む）をお客様またはお客様が任命した独立監査人が第 7.5.3 項（審査および監査に関する追加のビジネス規約）に従って実施することを許可します。監査中、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、Google は、お客様またはその監査人に合理的に協力します。

b. お客様による独立審査。お客様は、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）を審査することで、Google が本追加条項に基づく自己の義務を遵守していること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. お客様は、以下の場合、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）に基づいて、関連するデータ管理者のために SOC レポートへのアクセスを要求する場合。

ii. 第 7.5.2 項（a）号（お客様による監査）に基づいて監査を要求する場合。

b. 第 7.5.3 項（a）号に基づくお客様からの要求後、Google とお客様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。

i. 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策。

ii. 第 7.5.2 項（a）号（お客様による監査）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ための管理策。

c. Google は、第 7.5.2 項（a）号（お客様による監査）に基づく監査に対して、Google の合理的な費用負担に基づく料金を請求する場合があります。Google は、適用される料金の詳細およびその計算の根拠をかかる監査の実施前にお客様に提示します。かかる監査の実施において、お客様が任命した監査人から請求された料金については、お客様が負担するものとします。

d. 第 7.5.2 項（a）（お客様による監査）に基づく監査を実施するためにお客様が任命した監査人が適切な資格を有していない、独立した監査人ではない、Google の競合他社である、またはその他の理由により明らかに適切でないと Google が合理的に判断した場合、Google は当該監査人に対し、書面で異議を申し立てることができます。Google がそのような異議を申し立てた場合、お客様は、別の監査人を任命するか、自ら監査を実施する必要があります。

e. お客様が、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）に基づいて、SOC レポートへのアクセス（関連するデータ管理者のため）または監査を要求した場合、かかる要求にも本第 7.5.3 項（審査および監査に関する追加のビジネス規約）が適用されます。

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、規制に関する事前協議、またはそれに相当する手続きに関するお客様（または、お客様がデータ処理者である場合は関連するデータ管理者）の義務の遵守を徹底するにあたり、以下の方法でお客様を支援します。

a. 第 7.1.3 項（追加のセキュリティ管理策）に従い追加のセキュリティ管理策を利用可能にし、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. 該当する契約（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. お客様（または関連するデータ管理者）が前述の義務を遵守するために上記（a）号および（b）号が不十分である場合、お客様の要求に基づき、お客様をさらにかつ合理的に協力および支援すること。

9. アクセス、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 は契約期間中、お客様のデータへのアクセス、ならびにお客様のデータの訂正および制限付きの処理（第 6.1 項（お客様による削除）に記載されているとおりに Google 提供の削除機能を利用する場合も含む）、ならびにお客様の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お客様が実行できるようにします。お客様は、お客様の個人データに誤りがあること、または最新の情報に更新されていないことに気付き、適用されるプライバシー法で義務づけられている場合、お客様は当該機能を使用してそのようなデータを修正または削除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。契約期間中、Google Cloud データ保護チームが、お客様の個人データに関連し、かつお客様を特定する要求をデータ主体から受け取った場合、Google は以下のとおりとします。

a. データ主体に対し、要求をお客様に提出するよう助言します。

b. 速やかにお客様に通知します。

c. お客様の許可を得ることなく、その他の行為により当該データ主体の要求には対応しません。

お客様は、必要に応じてサービスの機能を使用して対応する場合を含め、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（お客様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、データ主体の権利の行使に関する要求に対応するというお客様（または、お客様がデータ処理者である場合は関連するデータ管理者）の義務の履行において、以下の方法でお客様を支援します。

a. 第 7.1.3 項（追加のセキュリティ管理策）に従い、追加のセキュリティ管理策を利用可能にすること。

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. お客様（または関連するデータ管理者）が前述の義務を遵守するために上記（a）号および（b）号が不十分である場合、お客様の要求に基づき、お客様をさらにかつ合理的に協力および支援すること。

10. データ処理の場所

10.1 データ保存施設およびデータ処理施設。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確約と、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確約に従うことを条件として、該当する場合に、お客様のデータは、Google またはその復処理者が施設を維持しているいずれか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 復処理者への再委託に対する同意。お客様は、追加条項発効日時点の第 11.2 項（復処理者に関する情報）に記載されているとおりに、開示済みの事業者を Google が復処理者とし、当該復処理者に業務を再委託することを明示的に承認します。また、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、通常、お客様は、Google がその他の第三者を復処理者（以下、「新規復処理者」）とし、当該新規復処理者に業務を再委託することを承認します。

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 復処理者への再委託に関する要件。復処理者に業務を再委託する際、Google は以下のとおりとします。

a. 書面による契約を通じて、以下のことを徹底します。

i. 復処理者は、再委託された義務を履行するために必要な範囲でのみお客様のデータにアクセスし、これを利用します。その際、適用される契約（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おいて義務づけられている場合、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）でさらに詳述されている場合があります）。

b. 復処理者に再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 が契約期間中に新規復処理者に再委託する場合、新規復処理者がお客様のデータの処理を開始する少なくとも 30 日前までに、Google はお客様に対して当該再委託（新規復処理者の名称、所在地、および活動内容を含む）を通知するものとします。

b. お客様は、新規復処理者への再委託が通知されてから 90 日以内に、以下のいずれかの方法で該当する契約を都合により直ちに解除することにより、異議を申し立てることができます。

i. 当該契約の「都合による解除」条項に従う。

ii. 前述の条項がない場合は、Google に通知する。

12. Google Cloud データ保護チーム、データ処理記録

12.1 Google Cloud データ保護チーム。Google Cloud データ保護チームは、該当する契約に基づくお客様のデータの処理に関するお客様からの問い合わせにおいて、お客様を速やかかつ合理的に支援します。また、当該チームへは、該当する契約の「通知」条項または付録 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が義務づけているとおりに、Google 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、お客様に関する特定の情報を収集し、かかる情報の記録を維持する義務を Google が負っている範囲において、お客様は管理コンソールまたは付録 4（特定のプロダクト）に記載されてい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が義務づけている場合、かかる情報を管轄規制機関（監督機関を含む）に提供することがあります。

12.3 データ管理者からの要求。契約期間中、Google Cloud データ保護チームが、お客様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、お客様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 インシデントの通知を含む）は、通知用メールアドレスに送信されます。お客様は、管理コンソールを使用するか、Google に通知することにより、自己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範囲において、次のとおりとします。

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範囲にいおいて、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範囲において、付録 4 が優先されます。

c. 本追加条項と契約の残りの部分との間で矛盾が生じた範囲において、本追加条項が優先されます。

明確にするために記すと、お客様が複数の契約を締結している場合、本追加条項により各契約が個別に修正されます。

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ています。

付録 1: データ処理の内容および詳細

内容

Google からお客様へのサービスおよび TSS（該当する場合）の提供。

データ処理の期間

契約期間に、契約期間終了後から Google が本追加条項に従ってお客様のデータすべてを削除するまでの期間を加えた期間。

データ処理の性質と目的

Google は、本追加条項に従い、お客様にサービスおよび TSS（該当する場合）を提供するために、お客様の個人データを処理します。

データのカテゴリ

お客様が（またはお客様の指示で）、またはお客様のエンドユーザーがサービスを通じて Google に提供する、個人に関連するデータ。

データ主体

データ主体には、お客様が（またはお客様の指示で）、またはお客様のエンドユーザーがサービスを通じて Google に提供するデータによって識別される個人が含まれます。

付録 2: セキュリティ対策

追加条項発効日以降、Google は本付録 2 に記載されている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、物理的にセキュリティが確保されているデータセンター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、他の必須デバイスが、このような冗長性の実現に役立っています。サービスは、特定の種類の予防保守および是正保守を Google が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環境設備は、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保守手順が文書化されています。データセンター機器の予防保守および是正保守は、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スケジュールが設定されます。

電力。データセンターの電力システムは、24 時間 年中無休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、電圧低下、停電、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。バックアップ電源は、停電発生時に、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、データセンターが通常であれば数日間フル稼働するのに十分な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、サービスを提供するために使用してい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、定期的に立案し、テストしています。

（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、データの不正な読み取り、コピー、変更、削除が発生することを防いでいます。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ています。

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に、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、潜在的な攻撃ベクトルを考慮し、適切な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分析情報を提供し、インシデントに対応するための十分な情報を提供することを目的としています。Google の侵入検知では、（i）予防措置によって Google の攻撃対象領域の規模と構成を厳密にコントロールし、（ii）データ エントリー ポイントでインテリジェントな検知制御を行い、（iii）特定の危険な状況を自動的に修復する技術を採用しています。

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に対応しています。この PFS（Perfect Forward Secrecy: 前方秘匿性）は、トラフィックを保護し、鍵の漏えいまたは暗号の解読による影響を最小限に抑えるのに役立ちます。

2. アクセス制御とサイト管理

（*a*）サイト管理。

データセンター現地でのセキュリティ運用。Google のデータセンターでは、データセンターのすべての物理的なセキュリティ措置に対する責任を負うセキュリティ運用担当者が 24 時間 365 日にわたり現地に駐在するようにしています。この担当者は、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を定期的に巡回しています。

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出入りを許可する際の厳格な出入り手順を設けています。データセンターは立ち入る際に電子カードキーを必要とする施設内にあり、その施設には現地のセキュリティ運用システムと連動している警報が備わっています。データセンターへの入場者は全員、身分を明らかにし、現地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立ち入りが認められているのは、許可された従業員、請負業者、訪問者に限定されています。このような施設に入るための電子カードキーを申請することができるのは、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るほか、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。データセンターへ一時的に出入りする必要があるその他すべての人は、次の条件を満たす必要があります:(i)訪問する特定のデータセンターおよび内部領域について、データセンターの管理者から事前に承認を得て、(ii)現地の警備窓口で署名し、(iii)出入りが承認されている者であることを特定する承認済みのデータセンター 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 アラームと連動している二段階認証方式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のほか、境界ドア、搬入出場所、その他重要な領域に出入りした時刻をモニタリングし、記録します。不正な活動や立ち入りの失敗は、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 センターおよびデータセンターに立ち入ることが認められる人は、ゾーンおよび個人の職責に基づいて制限されています。データセンターの防火扉には警報装置が備わっています。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。CCTV カメラは、施設周辺、データセンター施設への出入り口、荷物の搬入出口など、重要領域をカバーするように配置されています。現地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。CCTV カメラは、24 時間 365 日にわたり、デジタルビデオ レコーダーを通じて現地で録画しています。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。お客様の管理者およびエンドユーザーは、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に関する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に関する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が、お客様のデータの処理に使用されるシステムにアクセスすることを防ぐように設計されています。Google は、(i)承認されたユーザーがアクセス権を有しているデータにのみアクセスできるようにすること、および(ii)処理中、使用中および記録後にお客様のデータを不正に読み取り、コピー、変更、削除することができないようにすることを徹底するためにこのシステムを設計しています。また、このシステムは、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一元的なアクセス管理システムを採用し、限られた数の承認済みユーザーにのみアクセスを許可しています。Google の認証システム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は、サイトホスト、ログ、データ、構成情報に対する承認済みアクセス権だけを付与するように設計されています。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に、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ているアクセスリストの使用を義務づけています。アクセス権は、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、知る必要がある人以外には秘匿する方針に基づいて付与または変更されま

す。また、アクセス権を付与または変更するときに、Google の内部データへのアクセスに関するポリシーおよびトレーニングに従う必要があります。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。このような標準的な慣行には、パスワードの再利用に関する制限や十分なパスワードの安全度が含まれます。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ています。矛盾する指示（データの保存場所の選択など）があることを条件として、Google は、地理的に分散した複数のデータセンター間でお客様のデータを複製します。また、Google はお客様のデータを論理的に隔離しています。お客様には、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、お客様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プロダクト共有設定を決定できます。お客様は、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（以下「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（以下「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ごとに記録されます。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、最終的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、廃棄できるまで安全に保管されます。ディスク消去ポリシーへの準拠を確認することを目的として、各施設は定期的に監査を受けます。

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 ポリシーの受領を確認して、これらを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。お客様のデータを扱うスタッフは、その職務に適した追加の要件（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お客様の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

復処理者に処理を再委託する前に、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を確認するために、当該復処理者のセキュリティ慣行とプライバシー慣行を監査します。復処理者が提示したリスクを Google が評価した後に、復処理者は、本追加条項の第 11.3 項（復処理者への再委託に関する要件）に記載されている要件を満たしていることを条件として、適切なセキュリティ、機密保持、プライバシーに関する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、該当する法律がお客様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、以下の国または地域を意味します。

(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確保していると認められている国もしくは地域。

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

(c)スイス 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)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している、国家法において十分な保護を確保している国のリストに含まれている(該当する場合)、または(ii)スイス FADP に基づきスイス連邦評議会によって十分な保護を確保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、準拠する義務がない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、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(ただし、SCC は除く)を意味します。たとえば、参加事業体が十分な保護の提供を徹底してい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。

- 「お客様の 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、お客様の 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)のうち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。第 5.2 項(お客様の指示への準拠)に基づく Google の義務、ならびに該当する契約に基づく両当事者のその他の権利および義務を害することなく、Google は、以下のいずれかに該当すると自ら判断した場合、直ちにお客様に通知します。

a. 欧州法が Google による指示の遵守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. Google がその他の理由により指示を遵守できない場合

いずれの場合でも、欧州法が当該通知を禁止している場合を除きます。

お客様がデータ処理者である場合、お客様は本項に基づいてGoogle から提供を受けた通知を、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. お客様の監査権。Google は、お客様またはお客様が任命した独立監査人に対し、第 7.5.2 項(a)号(お客様による監査)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自己の義務を遵守していること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。お客様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に、欧州データ保護法は SCC または代替移転ソリューションを義務づけていないことを両当事者は認めます。(請求先住所が EMEA 圏外であるときに、欧州データ保護法の第 4.2 項(EMEA 圏外のお客様による確認)に基づきお客様が証したとおりに)お客様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(以下、「制限付き移転」)には、以下のとおりとします。

a. Google が制限付き移転のために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の情報をお客様に提供し、当該制限付き移転が代替移転ソリューションに従って行われることを確実にします。

b. Google が制限付き移転のために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 が制限付き移転のために(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お客様に通知した場合は、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、お客様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 とお客様との間の制限付き移転に関しては、お客様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 とお客様との間の制限付き移転に関しては、お客様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 圏外のお客様による確認。お客様の請求先住所が EMEA 圏外であり、かつお客様の個人データの処理に欧州データ保護法が適用される場合、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、お客様は該当するサービスの管理コンソールでその旨を証し、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策、およびその他の補助的な保護措置に関連する情報を、以下のようにお客様に提供します。

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）に記載のとおりにお客様の SCC が適用される場合、Google はお客様（またはお客様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。お客様は、SCC に言及するあらゆる通知を、関連するデータ管理者に、不当に遅滞することなく速やかに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。お客様は、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、移転されるお客様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当該契約を解除できます。

4.7 SCC の不変更。契約（本追加条項を含む）のいかなる条項も、SCC を変更および否定すること、ならびに欧州データ保護法に基づくデータ主体の基本的権利および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。（本追加条項において参照により援用されている）お客様の SCC と、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範囲で、お客様の SCC が優先されます。

5. 復処理者への再委託に関する要件。欧州データ保護法は、該当する場合、GDPR 第 28 条（3）号で言及されている、本追加条項に記載されたデータ保護義務を、Google が再委託するすべての復処理者に対し、書面による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。
- 「お客様の個人データ」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」のという用語の意味は、CCPA で定義されているとおりです。

2. 禁止事項。CCPA に従ったお客様の個人データの処理に関して、Google は、CCPA において別途許可されていない限り、第 5.2 項（お客様の指示への準拠）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. お客様の個人データを販売および共有すること。

b. お客様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. お客様に代わって行う CCPA に基づく業務目的、ならびにサービスおよび TSS（該当する場合）を履行する特定の目的で行う場合。

ii. Google とお客様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、もしくは第三者に代わって受領した、または消費者と自身とのやり取りから収集した個人情報とお客様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。第 5.2 項（お客様の指示への準拠）に基づく Google の義務、ならびに適用される契約に基づく両当事者のその他の権利および義務を害することなく、Google は、CCPA に基づく自己の義務を履行できないと判断した場合、お客様に通知します。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. お客様の介入。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、お客様の個人データの不正使用を Google がお客様に通知した場合、お客様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 項（a）号（お客様による監査）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。お客様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お客様の個人データの移転に関して、お客様が同意するための必須ではない追加条項（トルコ SCC を含む）を提供した場合、これらの条項は、お客様が Google に証明したとおりの以下の第 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に、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。お客様が本第 2 項（データ移転）に基づきトルコ SCC を締結した場合、お客様は、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 に署名した日から 5 営業日以内に、トルコ個人データ保護機関にトルコ SCC の使用を通知する責任を負います。

2.3 SCC 監査。お客様が本第 2 項（データ移転）に基づきトルコ SCC を締結した場合、Google は、お客様（またはお客様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 で要求されてい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。お客様は、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、移転されるお客様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当該契約を解除できます。

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 を変更もしくは否定すること、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（お客様が締結した場合は、参照することにより本追加条項で援用されます）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。本追加条項で使用している「データ管理者」、「個人データ」、「処理」、「データ処理者」の同義語の意味は、イスラエル プライバシー保護法で定めるとおりとします。

3. お客様の監査権。Google は、お客様またはお客様が任命した独立監査人が、第 7.5.2 項（a）号（お客様による監査）に記載されている監査（検査を含む）を実施することを許可します。

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お客様の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、契約で定義されていない場合、お客様の Google Cloud Platform アカウントを意味します。
- 「お客様のデータ」とは、契約で定義されていない場合、Google Cloud Platform を通じてお客様またはエンドユーザーがアカウントを使用して Google に提供したデータ、およびお客様またはエンドユーザーが Google Cloud Platform を使用してそのデータから抽出したデータを意味します。
- 「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、契約で定義されていない場合、（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）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、および（c）第三者のオペレーティング システムを意味します。

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. Google Cloud 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策、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、Google は、お客様の要求に応じて、その時点での Google の第三者監査人の身元をお客様に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、「お客様の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 項（a）号にある「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 項（b）号にある「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）号にある以下の文章:
        - 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ています。矛盾する指示（データの保存場所の選択など）がお客様からあることを条件として、Google は地理的に分散した複数のデータセンター間でお客様の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 レポート 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、Google が本追加条項に基づく自己の義務を遵守していることを証明するために、BMS コンプライアンス証明書および BMS SOC レポートをお客様が確認できるようにします。お客様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、お客様が関連するデータ管理者のために BMS SOC レポートへのアクセスを要求することを許可します。

4. お客様の義務。Bare Metal Solution に関する Google の明示的な義務を制限することなく、お客様は、お客様のデータおよび 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。矛盾する規定が契約（本追加条項も含む）にある場合でも、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

お客様は、Bare Metal Solution でお客様が利用、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、お客様のデータ、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います。

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（お客様による削除）および第 6.2 項（契約期間終了時のデータ返却または削除）は、Google または復処理者が、TSS のために送信され、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 キャプチャにお客様の個人データが含まれていない場合に限ります。

Google Distributed Cloud コネクテッド（**Google Cloud Platform**）

Google Distributed Cloud コネクテッドは、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、Google Distributed Cloud コネクテッド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（契約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 契約期間終了時のデータ返却または削除。お客様は、適用法に従い、契約期間終了時に残りのお客様のデータ（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。お客様が契約期間終了後もお客様のデータの保持を希望する場合は、契約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が保管を義務付けている場合、またはその他の適用されるプライバシー法が適用される状況では適用法が保管を義務付けている場合を除きます。
- 第 10.1 項（データ保存施設およびデータ処理施設）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。お客様のデータは、顧客のロケーションに導入される本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、Google Distributed Cloud コネクテッドを提供するために使用するコードのセキュリティを高め、Google Distributed Cloud コネクテッドの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に対応しています。この PFS（Perfect Forward Secrecy: 前方秘匿性）は、トラフィックを保護し、鍵の漏えいまたは暗号の解読による影響を最小限に抑えるのに役立ちます。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。Google Distributed Cloud コネクテッドは 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、本機器とお客様の 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、構成することをお客様に許可しています。

ストレージの接続。お客様のデータ 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。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、Google Distributed Cloud コネクテッド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、お客様の VMware 環境にアクセスしたり、お客様の 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、Google は、お客様の要求に応じて、その時点での Google の第三者監査人の身元を開示するものとします。
- 付録 2（セキュリティ対策）の第 3 項（a）号（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。矛盾する指示（データの保存場所の選択など）があることを条件として、Google は地理的に分散した複数のデータセンターを間でお客様のデータを複製します。また、Google はお客様のデータを論理的に隔離しています。お客様には、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、お客様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プロダクト共有設定を決定できます。お客様は、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 レポートおよび 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、Google が本追加条項に基づく自己の義務を遵守していることを証明するために、NetApp コンプライアンス証明書および NetApp SOC レポートをお客様が確認できるようにします。お客様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、お客様が関連するデータ管理者のために NetApp SOC レポートへのアクセスを要求することを許可します。

Google Workspace* と *Cloud Identity

1. 追加の定義。

- 「アカウント」とは、契約で定義されていない場合、お客様の Google Workspace または Cloud Identity のアカウントを意味します。
- 「Cloud Identity」とは、Google Cloud Platform または Google Workspace の一部としてではなく、単体の契約に基づいて購入された場合、https://cloud.google.com/terms/identity/user-features に記載されている Cloud Identity サービスを意味します。
- 「お客様のデータ」とは、契約で定義されていない場合、Google Workspace または Cloud Identity を通じてお客様もしくはその代理人、またはそのエンドユーザーがアカウントを使用して保存、送信、または受信したデータを意味します。
- 「Google Workspace」とは、https://workspace.google.com/terms/user_features.html に記載されている Google Workspace サービスまたは Google Workspace for Education サービスのいずれか該当するものを意味します。

2. 追加プロダクト。適用される追加プロダクト規約に従い、Google が独自の判断によって Google Workspace または Cloud Identity と組み合わせて使用する追加プロダクトをお客様に提供する場合は、次の規定が適用されます。

a. お客様は管理コンソールから追加プロダクトを有効または無効にすることができます。また、Google Workspace または Cloud Identity を使用するために追加プロダクトを使用する必要はありません。

b. お客様が追加プロダクトをインストールすること、または Google Workspace もしくは Cloud Identity と組み合わせて使用することを選択した場合、その追加プロダクトは、Google Workspace または Cloud Identity と相互運用するために必要な範囲でお客様のデータにアクセスすることがあります。

明確にするために記すと、本追加条項は、お客様がインストールまたは使用する追加プロダクトの提供に関連する個人データ（かかる追加プロダクトとの間で送受信される個人データを含む）の処理には適用されません。

3. コンプライアンス証明書。Google Workspace と Cloud Identity 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 証明書および ISO 27018 証明書も含まれます。

4. データセンターの所在地。Google Workspace と Cloud Identity のデータセンターの所在地は、https://www.google.com/about/datacenters/locations/ に記載されています。

5. 復処理者に関する情報。Google Workspace と Cloud Identity の復処理者の名称、所在地、および活動内容は、https://workspace.google.com/intl/en/terms/subprocessors.html で確認できます。

6. Google Cloud データ保護チーム。Google Workspace と Cloud Identity のデータ保護チーム（管理者が管理者アカウントにログインしている場合）には、https://support.google.com/a/contact/googlecloud_dpr から連絡できます。

7. 追加のセキュリティ対策。Google Workspace と Cloud Identity を対象とした対策:

a. Google は各エンドユーザーのデータを他のエンドユーザーのデータから論理的に分離します。

b. 認証済みエンドユーザーのデータは、他のエンドユーザーには表示されません（過去のエンドユーザーまたは管理者がデータの共有を許可している場合を除く）。

8. 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策、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。

9. サービスデータに関する追加条項。本追加条項に関連してお客様から同意を得るために、Google がサービスデータに関する追加条項を必須ではない条項として提示する場合、そのような必須ではない追加条項の提示は、お客様が以前に締結したサービスデータに関する追加条項で当該用語が定義されている限り、「DPA の更新」となります。

10. サービス固有の規約。

AppSheet（Google Workspace）

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

- 付録 2 の第 1 項（a）号（セキュリティ対策）の「サーバー オペレーティング システム」という段落を削除し、以下の内容に置き換えて適用します。
    - 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。

2. 追加のデータセンターの所在地。AppSheet の追加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。

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、Google の特定のサービス、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）を含む統合プラットフォームを意味します。これは、契約に基づき Google がお客様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」の意味は、Google が管理する MCS データ処理の修正条項で定めるとおりです。

- 「注文フォーム」の意味は、契約で定めるとおりです。ただし、お客様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、または試用契約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、お客様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）に記載されている 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（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 に記載されている条項を意味します。

    - 「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 に記載されている条項を意味します。

    - 「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 に記載されている条項を意味します。

    - 「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/looker/legal/sccs/eu-p2p-intra-group に記載されている条項を意味します。

- 第 10.1 項（データ保存施設およびデータ処理施設）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お客様の追加責任。お客様は、Google が管理および制御するシステムを除き、Looker（オリジナル）用のお客様の環境、データベース、および構成のセキュリティに対して責任を負います。

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）の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 圏外のお客様による確認の不実施。お客様には、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 圏外のお客様による確認）に記載されている管轄権を有す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策、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、以下に記載されています。

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

b. https://cloud.google.com/terms/subprocessors

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. Google Cloud 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 がお客様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範囲において、Google がお客様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、お客様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を 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するのに役立ちます。

b. お客様の管理者は、お客様またはお客様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、契約で定義されていない場合は、お客様の SecOps サービスのアカウントまたは 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。

- 「お客様のデータ」とは、契約で定義されていない場合、SecOps サービスを通じてお客様またはエンドユーザーがアカウントを使用して Google に提供するデータを意味します。また、Mandiant のコンサルティング サービスおよびマネージド サービスの場合は、SecOps サービスを受けるにあたって Google に提供するデータを意味します。

- 「お客様が利用するプロバイダ」とは、お客様とプロバイダとの間で別途締結された契約に従い、お客様が直接利用するサービス プロバイダ（データ処理者または復処理者を含む場合があります）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 SecOps サービス（第三者の提供物は除く）を意味します。

- 「第三者の提供物」とは、契約で定義されていない場合、（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 システムを意味します。

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策」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策」とは、お客様が自身の選択もしくは判断またはその両方により使用できるセキュリティに関するリソース、機能、および管理策またはこれらの一部（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、該当する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）に記載されている 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（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 に記載されている条項を意味します。

    - 「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 に記載されている条項を意味します。

- 「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 に記載されている条項を意味します。

- 「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 に記載されている条項を意味します。

- 本追加条項の第 6.1 項（お客様による削除）は、以下のように修正されます。

  - 6.1 お客様による削除。契約期間中、Google はお客様が、サービスの機能に沿った方法で、または要求に応じてお客様のデータを削除できるようにします。契約期間中に、お客様がサービスを使用してお客様のデータを削除し、お客様がお客様のデータを復元できない場合、またはお客様が契約期間中にお客様のデータの削除を要求した場合、その使用行為または要求（該当する場合）は、Google に対し、該当するお客様のデータを適用法に従って Google のシステムから削除することを求める指示を成立させることになります。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義務づけられている場合、またはその他の適用されるプライバシー法の適用がある状況ではその適用法によって保存が義務付けられている場合を除き、合理的に実行可能な限り速やかに、ただし最長 180 日以内にこの指示に従います。

- 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、監査対象サービスがセキュリティ対策の継続的な有効性を検証できるようにするために、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、Google は、コンプライアンス証明書および 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。

- 第 9.1 項（アクセス、訂正、制限付きの処理、ポータビリティ）は、以下のように修正されます。

9.1 アクセス、訂正、制限付きの処理、ポータビリティ。契約期間中、Google は、サービスの機能に沿った方法で、お客様のデータへのアクセス、ならびにお客様のデータの訂正および制限付きの処理（第 6.1 項（お客様による削除）に記載されているものを含む）、ならびに要求に応じたお客様のデータのエクスポートをお客様に許可します。お客様は、お客様の個人データに誤りがあること、または最新の情報に更新されていないことを認識した場合、Google に通知する責任を負うものとします。Google は、適用されるプライバシー法が義務付けている場合、お客様による当該データの訂正を支援します。

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 圏外のお客様による確認の不実施。お客様には、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 圏外のお客様による確認）に記載されている管轄権を有し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 サービスの復処理者の名称、所在地、および活動内容は、https://cloud.google.com/terms/secops/subprocessors で確認できます。

6. Google Cloud 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（または Google が随時提供することがあるその他の手段）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 がお客様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範囲において、Google がお客様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、お客様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を Google に通知するものとします。

8. サービス固有の規約。

Mandiant のコンサルティング サービスおよびマネージド サービス

Mandiant のコンサルティング サービスとマネージド サービスは、アドバイザリ サービスと導入サービス（インシデント対応、戦略的な準備、脅威を緩和しインシデント関連のリスクを軽減するための技術面での保証を含む）およびマネージド型の検出サービスならびに対応サービスを提供するもので、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、Mandiant のコンサルティング サービスおよびマネージド サービスに関してのみ、次のように修正されます。

- 「データ インシデント」の定義は、次のように補足されます。
    - 明確にするために記すと、データ インシデントには、Mandiant のコンサルティング サービスもしくはマネージド サービスまたはその両方（いずれか該当するもの）の対象となるインシデントは含まれません。
- 第 5.2 項（b）号（i）（お客様の指示への準拠）は、以下の内容に置き換えられます。
    - i. お客様によるサービスの利用
- 第 7.1.1 項（Google のセキュリティ対策）の 2 つ目の文は、以下のように修正されます。
    - セキュリティ対策には、（状況に応じて）お客様のデータを暗号化する対策、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対策、インシデント発生後にお客様のデータへのタイムリーなアクセスを回復するのに役立つ対策、有効性の定期的なテストが含まれる場合があります。
- 第 7.3.1 項（b）号は、以下のように修正されます。
    - b. お客様が Mandiant のコンサルティング サービスもしくはマネージド サービスまたはその両方（いずれか該当するもの）を受けるために使用する、または Google がそれらを提供できるようにアクセスを許可する、アカウント認証情報、システム、ソフトウェア、ネットワーク、デバイスの管理、アクセス管理、セキュリティの確保。

- 新しい第 7.3.1 項（d）号および（e）号が、以下のように追加されます。
    - d. お客様またはお客様の代理人によって Google に提供されるお客様のデータの量を最小限に抑えること。
    - e. Google によるお客様のデータへのアクセスがお客様の管理下にある範囲において、Google が Mandiant のコンサルティング サービスもしくはマネージド サービスまたはその両方（いずれか該当するもの）を完了した時点で、当該アクセス権を取り消すこと。
- 付録 2（セキュリティ対策）は、以下の内容に置き換えられます。
    - 付録 2: 追加の技術的措置および組織的措置

1. お客様が管理する環境。Google は、お客様が管理するアカウントもしくは環境またはお客様が承認したアカウントもしくは環境を通じて、お客様またはお客様の代理人が Google に提供したお客様のデータにのみアクセスし、当該データを処理します。

2. データへのアクセスに関するプロセスとポリシー - アクセス ポリシー。Google のデータへのアクセスに関する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お客様の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）ユーザーが許可されたデータにのみアクセスすることを許可し、（ii）処理中および使用中における個人データに対する不正な読み取り、コピー、変更、削除を不可能にするための措置を講じます。Google によるアクセス権の付与または変更は、お客様が Google に対して提供する、お客様のアカウントまたは環境へのエンドユーザー アクセス権に基づいて行われます。

3. 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。

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 ポリシーの受領を確認し、これらを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。お客様のデータを扱うスタッフは、その職務に適切な追加の要件（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お客様のデータを処理することはありません。

4. 追加のセキュリティ対策。Google とお客様は、Mandiant のコンサルティング サービスもしくはマネージド サービスまたはその両方のいずれか該当するものについて、該当する注文フォーム（添付の作業明細書を含む）において追加のセキュリティ対策を定めることに合意する場合があります。

2. お客様が利用するプロバイダ明確にするために記すと、第 7 項（データ セキュリティ）または第 11 項（復処理者）に基づく Google の義務を制限することなく、付録 2（セキュリティ対策）では、お客様またはお客様が利用するプロバイダによって実装または提供されるセキュリティ対策または管理策については記載していません。

導入サービス

1. 追加の定義。

- 「お客様のデータ」とは、お客様が管理するシステム上で Google のスタッフがアクセスすることをお客様が承認したデータを意味します。

- 「お客様が管理するシステム」とは、お客様が導入サービスを受けるために使用する(a)Google Cloud サービスまたはサードパーティのクラウド サービスのお客様が管理するインスタンス、および(b)お客様のオンプレミス環境でホストまたは管理されているハードウェアまたはソフトウェアを指します。

- 「Google Cloud サービス」とは、導入サービス、Mandiant コンサルティング サービス、Mandiant マネージド サービスを除く、付録 4(特定のプロダクト)に記載されているすべてのサービスを意味します。

- 「Google のスタッフ」とは、導入サービスの提供に従事する Google の従業員および請負業者を意味します。

- 「導入サービス」とは、注文フォームと作業明細書を含む契約に記載されているとおりに、Google の従業員および請負業者が Google Cloud サービスのサポートのために提供するアドバイザリ サービス、コンサルティング サービス、導入サービスを意味します。

2. 修正。追加条項は、導入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策」の定義は削除されます。

- 「データ インシデント」の定義は、以下の内容に置き換えられます。

    - 「データ インシデント」とは、お客様の個人データに対して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 のスタッフによる第 7.1 項(Google のセキュリティ対策、管理策、支援)への違反を意味します。

- 本項の残りの規定に従い、「お客様のデータ」という用語は、(a)第 2 項(定義)の「復処理者」の定義、および(b)本追加条項の他の条項で使用される場合、「お客様の個人データ」に置き換えられます。明確にするために記すと、第 2 項(定義)のその他の定義は変更されません。

- 第 3 項(契約期間)は、以下の内容に置き換えられます。

    - **3.** 期間。該当する契約が終了または満了しているかどうかにかかわらず、本追加条項は、Google がお客様の個人データに一切アクセスできなくなるまで有効であり、アクセスできなくなった時点で自動的に失効します。

- 第 6 項(データの削除)は、以下の内容に置き換えられます。

    - **6.** データの削除。契約期間の終了時に、お客様は(a)お客様の個人データを削除するかどうかを決定し、(b)その削除を行う責任を負うものとします。

- 第 7.1.1 項(Google のセキュリティ対策)の 2 つ目の文は、以下の内容に置き換えられます。

    - セキュリティ対策には、(状況に応じて)お客様のデータを暗号化する対策、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のに役立つ対策、インシデント発生後にお客様のデータへのタイムリーなアクセスを回復するのに役立つ対策、有効性の定期的なテストが含まれる場合があります。

- 第 7.1.3 項(追加のセキュリティ管理策)は、その項目に対する他のすべての参照と併せて削除されます。

- 第 9.1 項（アクセス、訂正、制限付きの処理、ポータビリティ）は、以下の内容に置き換えられます。
    - 9.1 アクセス、訂正、制限付きの処理、ポータビリティ。お客様は、お客様が管理するシステムの機能を使用して、お客様の個人データにアクセスし、訂正し、処理を制限する責任を負うものとします。これには、お客様が、お客様の個人データに誤りがあること、または最新の情報に更新されていないことに気付き、適用されるプライバシー法によりそのデータを訂正または削除する必要がある場合も含まれます。
- 第 11.4 項（復処理者に対する異議申し立ての機会）は、以下の内容に置き換えられます。
    - 11.4 復処理者に対する異議申し立ての機会。契約期間中に新しい復処理者に再委託する場合、Google は、お客様の個人データを処理する前に、新規復処理者への再委託をお客様に通知します。お客様は、Google に通知することにより、新規復処理者に異議を唱えることができます。お客様が異議を唱えた場合、両当事者は誠意をもって協力し、相互に受け入れられる代替案を決定します。
- 付録 1（データ処理の内容および詳細）は、以下の内容に置き換えられます。
    - 「データ処理の期間」の項目は、以下の内容に置き換えられます。
        - 「データ処理の期間。契約期間に、契約期間の終了日から Google によるお客様の個人データへのアクセス権の有効期限までの期間を加算した期間（該当する場合）。」
    - 「データのカテゴリ」と「データ主体」の項目の「本サービスを通じて Google に提供される」という文言は、「本サービスに関連して Google がアクセス可能になる」に置き換えられます。
- 付録 2（セキュリティ対策）は、以下の内容に置き換えられます。
    - 付録 **2:** セキュリティ対策

1. お客様が管理するシステム。Google のスタッフは、お客様が管理するシステム上でのみお客様の個人データにアクセスし、当該データを処理します。そのようなシステムに Google Cloud サービスが含まれている場合でも、お客様による Google Cloud サービスの使用は、当該サービスに適用される契約によって引き続き規律されます。

2. アクセス制御。Google の内部データへのアクセスに関する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が、個人データの処理に使用される Google Cloud サービスへのアクセス手段を得ることを防止するように設計されています。Google のポリシーは Google のスタッフに対し、(i) アクセスを許可されているデータにのみアクセスすることを許可し、(ii) 処理中、使用中、および記録後に許可なくお客様の個人データの読み取り、コピー、変更、削除を行わないことを義務付けています。お客様が管理するシステムへのエンドユーザーのアクセス権のプロビジョニングまたは変更は、お客様が管理します。そのようなシステムに Google Cloud サービスが含まれている場合、変更の監査記録とシステム アクセスログを維持するワークフロー ツールに関する詳細は、該当する Google Cloud サービスの契約に記載されています。

3. 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 ポリシーの受領を確認して、これらを遵守する必要があります。Google のスタッフには、セキュリティトレーニングが提供されます。お客様の個人データを扱う Google のスタッフは、その職務に適切な追加の要件（認定の取得など）を満たす必要があります。

4. 追加のセキュリティ対策。Google とお客様は、注文フォームや作業明細書を含む契約において追加のセキュリティ対策に合意する場合があります。

5. 復処理者のセキュリティ。復処理者に処理を再委託する前に、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を確認するために、当該復処理者のセキュリティ慣行とプライバシー慣行を監査します。復処理者が提示したリスクを Google が評価した後に、復処理者は、本追加条項の第 11.3 項（復処理者への再委託に関する要件）に記載されている要件を満たしていることを条件として、適切なセキュリティ、機密保持、プライバシーに関する契約を締結する必要があります。

3. お客様のセキュリティ責任。第 7.3.1 項（お客様のセキュリティ責任）に基づく義務に加えて、お客様は、以下の責任を負います。

- お客様が管理するシステムの管理、アクセス管理、およびセキュリティ保護。これには、Google のスタッフによるお客様の個人データへのアクセス権を合理的に実行可能な範囲で最小化し、導入サービスの完了時にそのアクセス権を失効させることが含まれます。

- お客様が管理するシステムに関して Google がお客様に書面で提示したセキュリティに関する推奨事項の実施。

4. コンプライアンス証明書。Google は、Google Cloud Platform および Google Workspace をサポートするために提供される導入サービスを対象とした ISO 27001、ISO 27017、ISO 27018 の証明書（以下「導入サービスのコンプライアンス証明書」）を維持します。Google はいつでも基準を追加できます。Google は、導入サービスのコンプライアンス証明書を同等以上の代替証明書に置き換えることができます。

5. コンプライアンス証明書の確認。Google は、Google が本追加条項に基づく自己の義務を遵守していることを証明するために、導入サービスのコンプライアンス証明書をお客様が確認できるようにします。お客様がデータ処理者である場合、Google は、お客様が、関連するデータ管理者のために、導入サービスのコンプライアンス証明書へのアクセス手段を要求することを許可します。

6. データ処理の場所。お客様の個人データは、Google が導入サービスを提供している任意の国、またはお客様がお客様管理のシステム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。

7. EMEA 圏外のお客様による確認の不実施。お客様には、導入サービスについて、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 圏外のお客様による確認）に記載されている管轄権を有する監督機関を確認する義務はありません。

8. 復処理者に関する情報。導入サービスの復処理者は、導入サービスの開始前にお客様に提供される該当する注文フォーム、作業明細書、その他の確認書で（下請業者として）特定されている業者、または Google の関係会社になります。Google は、お客様の要求に応じて、導入サービスの復処理者の名称、所在地、活動内容もお客様に提示します。

9. 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 がお客様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範囲において、Google がお客様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、お客様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を Google に通知するものとします。

組織向け ***Google Cloud Skills Boost***

1. 追加の定義。

- 「アカウント」とは、契約で定義されていない場合、お客様の組織向け Google Cloud Skills Boost のお客様のアカウントを意味します。
- 「GCSBO」とは、https://www.cloudskillsboost.google/（または Google が運営または管理し、組織向け Google Cloud Skills Boost を目的として使用される別のウェブサイト）を通じて提供される教育、トレーニング、学習サービスおよびコンテンツを意味します。
- 「TSS」とは、Google が自己の裁量でお客様に提供することがある技術サポート サービスを意味します。

2. 修正。本追加条項は、GCSBO 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策」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策」とは、お客様が自身の選択もしくは判断またはその両方により使用できるセキュリティに関するリソース、機能、および管理策またはこれらの一部（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。
- 付録 3（特定のプライバシー法）に記載されている 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（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/skillsboost-organizations/sccs/eu-c2p に記載されている条項を意味します。
    - 「SCC（データ処理者からデータ管理者へ）」とは、https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c に記載されている条項を意味します。
    - 「SCC（データ処理者からデータ処理者へ）」とは、https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p に記載されている条項を意味します。
    - 「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/skillsboost-organizations/sccs/eu-p2p-intra-group に記載されている条項を意味します。

3. データセンターの所在地。GCSBO 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. EMEA 圏外のお客様による確認の不実施。お客様には、GCSBO 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 圏外のお客様による確認）に記載されている管轄権を有す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。GCSBO の復処理者の名称、所在地、および活動内容は以下に記載されています。

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors および

b. https://cloud.google.com/terms/subprocessors

6. Google Cloud データ保護チーム。GCSBO のデータ保護チームには、https://support.google.com/qwiklabs（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 がお客様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範囲において、Google がお客様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、お客様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を 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:

2024 年 4 月 9 日 2022 年 6 月 30 日 2021 年 9 年 24 日 2020 年 8 月 19 日 2020 年 8 月 10 日 2020 年 7 月 17 日 2019 年 10 月 11 日 2019 年 10 月 1 日 2018 年 5 月 25 日 2018 年 3 月 13 日 2017 年 11 月 9 日 2017 年 10 月 11 日 2017 年 2 月 7 日 2016 年 10 月 6 日

旧バージョンのデータ処理の修正条項:

2022 年 7 日 7 2021 年 9 月 24 日 2021 年 5 月 27 日 2019 年 10 月 29 日 2018 年 5 月 25 日 2018 年 4 月 25 日 2017 年 7 月 11 日 2016 年 11 月 28 日 2016 年 1 月 7 日 2015 年 4 月 24 日 2014 年 4 月 1 日 2012 年 11 月 14 日

Looker（オリジナル）のサービスに関する旧バージョンのデータ処理に関する追加条項（お客様）:

2023 年 2 月 14 日2023 年 1 月 4 日2022 年 9 月 20 日2022 年 6 月 30 日2022 年 3 月 16 日2021 年 9 月 24 日2021 年 4 月 1 日2021 年 1 月 15 日2020 年 12 月 17 日2020 年 8月 28 日2020 年 6 月 1 日2020 年 3 月 9 日

旧バージョンの *SecOps* サービス *DPST*（お客様）:

2023 年 2 月 6 日 2022 年 11 月 28 日 2021 年 9 月 27 日 2020 年 10 月 1 日

SecOps コンサルティング サービスおよび *SecOps* マネージド サービスに関する旧バージョンのデータ処理に関する追加条項:

2023 年 10 月 5 日 2023 年 9 月 19 日 2023 年 6 月 15 日 2023 年 2 月 22 日 2023 年 2 月 6 日

以前のバージョン（最終更新日: 2024 年 10 月 15 日）

2024 年 9 月 26 日 2024 年 9 月 9 日 2024 年 8 月 5 日 2024 年 5 月 23 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