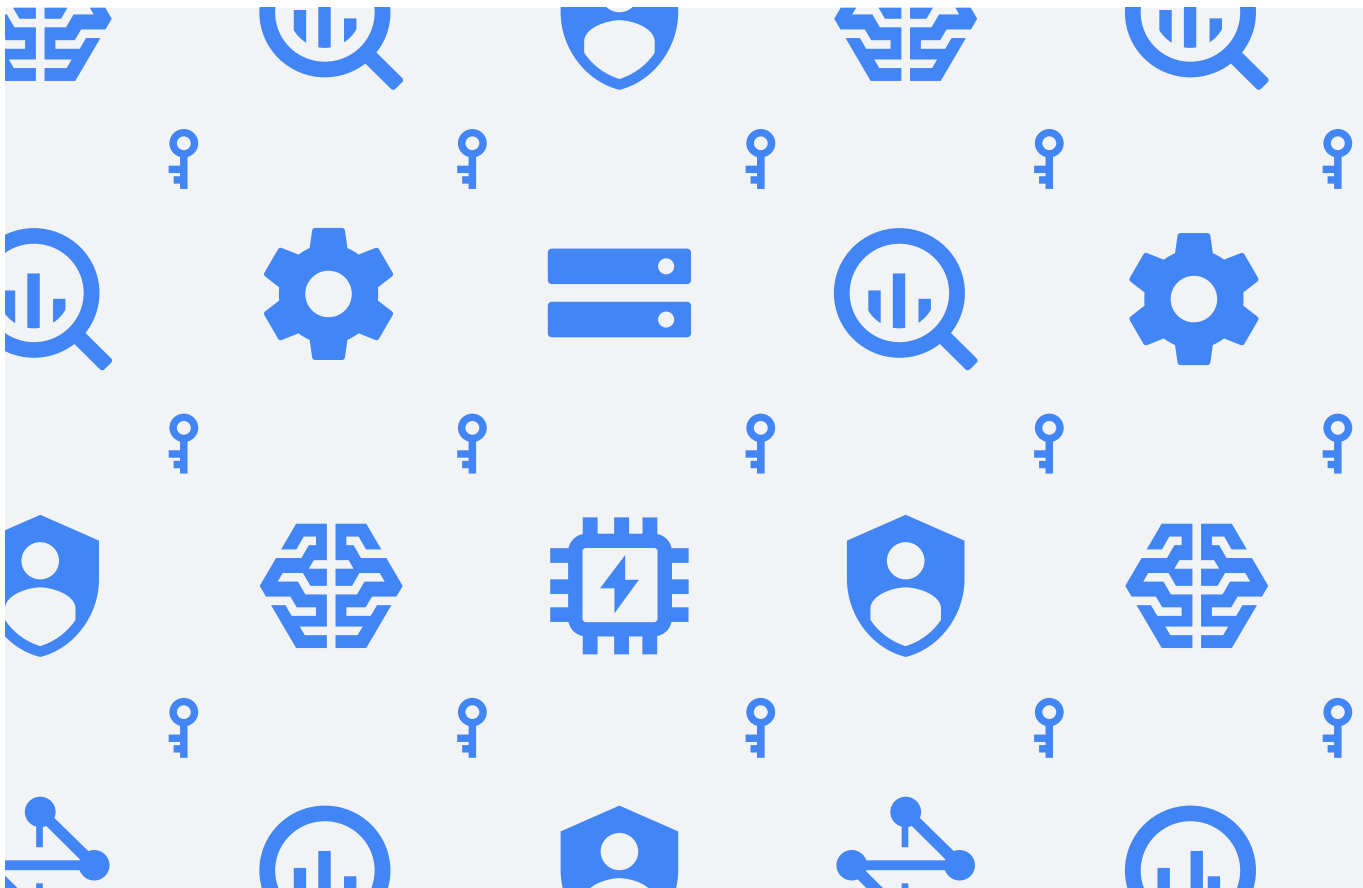




Google Cloud ホワイトペーパー
5月2018年

一般データ保護規則 (GDPR)



Google Cloud

GDPR の概要

2018 年 5 月 25 日に、過去 20 年間に制定されたヨーロッパのデータ保護法の中でも特に重要性の高い法律の適用が開始されます。1995 EU Data Protection Directive の代わりに EU General Data Protection Regulation (GDPR) の運用が開始されます。GDPR は、個人が自らの個人データに関して持つ権利を強化し、データが処理される場所にかかわらず、ヨーロッパ域内で統一的なデータ保護法を制定することを目的としています。

Google は、Google Cloud の各サービスが GDPR に準拠するように取り組んでいます。また、長年にわたって Google のサービスや契約に取り入れてきた、堅牢なプライバシーおよびセキュリティ保護機能をお客様に提供することで、お客様の GDPR への準拠をサポートしています。



お客様が実施できること

お客様の担う責任

通常、G Suite¹ や Google Cloud Platform のお客様は、Google の各サービスの利用に伴って Google に提供する個人データのデータ管理者の役割を担います。データ管理者は個人データを処理する目的と手段を決定し、データ処理者はデータ管理者に代わってデータを処理します。Google はデータ処理者として、データ管理者が G Suite または Google Cloud Platform を使用する際に、データ管理者に代わって個人データを処理します。

データ管理者は、GDPR に準拠してデータ処理を実施するために、技術的および組織的に適切な措置を講じる責任を担います。管理者の義務には、適法性、公平性、透明性、目的の限定、データの最小化、正確性などの原則に関連するものに加え、データ主体のデータに対する権利尊重の責任を果たすことが含まれます。

GDPR におけるデータ管理者の責務に関するガイダンスについては、GDPR の適用対象となっている各国のデータ保護機関や主管データ保護機関のウェブサイトを定期的にご確認いただくか²、[国際プライバシー専門家協会 \(IAPP\)](#) などのデータ プライバシー団体の刊行物をご覧ください。

また、GDPR におけるご自身の立場と義務に関しては、個別に法的な助言を受けることをおすすめします。お客様独自の状況に応じた法的な助言を提供できるのは弁護士に限られます。このウェブサイトに記載されている情報は、法的な助言を提供することを目的としたものではありません。また、法的な助言の代用となるものでもありません。

¹ G Suite には、G Suite for Business と G Suite for Education が用意されています。

² 該当国のデータ保護機関や主管データ保護機関の特定については、個別に法的助言を受けることをおすすめします。

始めに取り組むべきこと

Google Cloud をすでにお使いか、まだ検討段階にかかわらず、GDPR への対応に備えるには今が最適なタイミングです。以下のヒントを参考にしてください。

- GDPR の規定を把握しておくことをおすすめします。特に、現行のデータ保護に関する義務との相違点を理解しておいてください。
- 処理の対象となる個人データの最新インベントリを作成することを検討してください。Google のツールが、データの識別と分類に役立ちます。
- 現行の管理体制、ポリシー、プロセスを見直して GDPR の要件を満たしているかどうかを確認し、食い違いがあればそれに対処する計画を策定します。
- Google Cloud の既存のデータ保護機能を、お客様独自の規制遵守フレームワークの一部として活用する方法を検討します。
- この点について、G Suite または Google Cloud Platform の第三者による監査や認証の資料をご確認ください。
- 最新の規制ガイダンスが提供された時点で確認し、各ビジネスの状況に応じて法的な助言を得てください。

GOOGLE で実施していること

G Suite と Google Cloud Platform の GDPR に対する取り組み

データ管理者には、GDPR の要件を満たしたデータ処理を行うため、適切な技術的および組織的な措置を十分に提供できるデータ処理者のみを使用することが求められます。ここでは、お客様が G Suite および Google Cloud Platform サービスの評価を実施する際に考慮いただきたい点を紹介いたします。

エキスパートの知識、信頼性、リソース データ保護の専門知識

Google のセキュリティおよびプライバシーは、情報、アプリケーション、ネットワークセキュリティに関する世界有数のエキスパートのチームによって守られています。このチームは Google の防御システムの運用、セキュリティ レビュー プロセスの開発、セキュリティ インフラストラクチャの開発、Google のセキュリティ ポリシーの適用などを担当しています。また、Google では Google のプライバシーとセキュリティ遵守の管理にあたる弁護士団、規制遵守のエキスパート、公共政策の専門家チームも編成しています。このようなチームが、お客様が規制遵守の要件を満たせるよう、お客様や業界の関係者、監督官庁と連携して、G Suite と Google Cloud Platform の各サービスを構築しています。



データ保護責任

データ処理契約

G Suite と Google Cloud Platform のデータ処理契約には、お客様に対するプライバシー保護の責任が明記されています。Google では、数年間にわたり、お客様や規制当局からのご意見に基づいて規約に変更を加えてきました。

最近では、お客様が Google Cloud サービスを使用する際の準拠の評価と GDPR への準備を進められるようにするため、GDPR を反映するよう規約を更新し、GDPR 施行までに余裕を持って公開しました。お客様は、オプトイン プロセスを通じて、今すぐ新しいデータ処理規約に移行できます。G Suite のデータ処理の修正条項についてはこちら、GCP のデータ処理とセキュリティの規約についてはこちらをご覧ください。新しい規約は GDPR の施行とともに 2018 年 5 月 25 日に発効します。

指示に基づく処理

お客様とそのユーザーが Google システムに保管するデータは、現行のデータ処理契約、および GDPR を反映した新しいデータ処理契約に準じ、お客様の指示に従ってのみ処理されます。

従業員の機密保持義務

すべての Google 従業員には、機密保持契約の締結と、機密保持およびプライバシーに関する必須トレーニング、および行動規範トレーニングの受講が義務付けられています。Google の行動規範には、情報の保護に関する責任と、それに伴って期待される行動が明記されています。



サードパーティ サプライヤーやサポート担当者の利用

Google グループ各社では、G Suite および Google Cloud Platform サービスの提供に必要なデータ処理活動の大半を直接的に実施しています。一方で、これらのサービスのサポートについては、サードパーティ ベンダーと提携しています。各ベンダーは、必要となる専門技術を有していること、そして適切なセキュリティおよびプライバシー レベルを提供できることを条件に、厳密な選考手続きを経て選ばれています。Google では、G Suite と Google Cloud Platform サービスをサポートする Google グループのデータ処理再委託者に加え、これらのサービスに関与するサードパーティのデータ処理再委託者についての情報を公開しており、現行のデータ処理契約およびその更新時にはデータ処理再委託者に関する取り組みが含まれます。

サービスのセキュリティ

GDPR に従い、データ管理者とデータ処理者は、リスクに応じた適切なセキュリティ レベルを提供できるよう、技術的および組織的な手段を講じる必要があります。Google では、情報処理サイクル全体を通して、最新のセキュリティを提供するグローバル インフラストラクチャを運用しています。このインフラストラクチャは、サービスのデプロイにおけるセキュリティ、データストレージのセキュリティ（およびエンドユーザーのプライバシー保護）、サービス間の通信のセキュリティ、インターネット経由でのお客様との通信における機密性とセキュリティ、管理者による安全なオペレーションを提供する目的で構築されています。G Suite と Google Cloud Platform は、このインフラストラクチャ上で動作しています。

Google のインフラストラクチャのセキュリティは、データセンターの物理的なセキュリティから、ハードウェアやソフトウェアのセキュリティ保護、そしてオペレーションのセキュリティをサポートするプロセスまでが階層型で設計されています。このような階層型の保護により、どのような処理に対しても強固なセキュリティ基盤が提供されます。インフラストラクチャ セキュリティについて詳しくは、[Google インフラストラクチャのセキュリティ設計の概要](#)をご覧ください。





可用性、整合性、復元力

Google のプラットフォームの構成要素は、冗長性に優れた設計になっています。Google のデータセンターは地理的に分散されているため、ある地域で自然災害や局地的な停電などが生じてグローバルなプロダクトが使用できなくなっても、その影響は最小限に抑えられます。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、サービスは自動的かつ瞬時に別の施設に切り替わるため、オペレーションは中断されずに継続されます。冗長性の高いインフラストラクチャにより、お客様をデータ損失から保護します。



テスト

Google では、インフラストラクチャ チームとアプリケーション チームがコミュニケーション計画やフェイルオーバー シナリオ、オペレーション移行、その他の緊急対策を共通した手順で実施できるように、災害復旧訓練を毎年実施しています。災害復旧訓練に参加するすべてのチームがテスト計画を策定し、テストの結果とそこから得た知見を分析します。



暗号化

Google では、移行データと保存データを保護するために暗号化を使用しています。G Suite に移行中のデータは HTTPS で保護されます。HTTPS は、すべてのユーザーに対してデフォルトで有効になっています。G Suite と Google Cloud Platform サービスでは、1 つ以上の暗号化メカニズムを使用して、保存されているお客様のコンテンツを暗号化しています。お客様による操作は必要ありません。データの暗号化の方法について詳しくは、[暗号化に関するホワイトペーパー](#)をご覧ください。



アクセス制御

Google の従業員に対するアクセス権やアクセスレベルは、職務や役割に基づいて付与されており、責務に対して必要なアクセス権が、最小特権および need to know（知る必要がある人にもみ知らせる）原則に則して与えられています。追加のアクセス権を得るには、Google のセキュリティ ポリシーに従い、データまたはシステムの所有者、管理者、またはその他の役職者へのリクエストと承認を得るための正式な手順を踏む必要があります。



脆弱性の管理

Google では、市販ツールと社内用に開発されたツール、自動および手動による集中的な侵入テスト、品質管理プロセス、ソフトウェア セキュリティ レビュー、外部監査を組み合わせ、ソフトウェアの脆弱性をスキャンしています。また、Google はセキュリティ研究コミュニティとも連携しています。こうした関係は、G Suite、Google Cloud Platform、その他の Google プロダクトでの脆弱性を発見するうえで役立つと考えています。Google の脆弱性報奨金プログラムでは、お客様のデータを危機にさらす可能性のある設計上および実装上の問題点を報告するよう、研究者に呼びかけています。

プロダクトのセキュリティ: G Suite

G Suite のお客様は、未承認の処理や不正処理から個人データをさらに保護するため、次のようなプロダクトの機能や設定を活用できます。

- 2 段階認証プロセスを導入すると、ユーザーのログイン時に身元が追加確認されるため、不正アクセスのリスクが大幅に低減されます。セキュリティキーの使用を必須にすると、物理的なキーの使用を義務付けることでユーザー アカウントのセキュリティをさらに強化できます。
- 不審なログインの監視とは、強力な機械学習機能を使用して不審なログインを検出することです。
- メールのセキュリティを強化するために Secure/Multipurpose Internet Mail Extensions (S/MIME) を使用すれば、メールに対する署名および暗号化を必須にすることができます。
- データ損失防止とは、Gmail や Google ドライブの機密情報が不正に共有されないように保護する機能です。詳しくは、[データ損失防止に関するホワイトペーパー](#)をご覧ください。
- Google ドライブの情報権利管理では、高度な共有メニューからファイルをダウンロード、印刷、コピーできないようにし、ファイル アクセスに有効期限を設定できます。
- モバイル端末管理はシステムを継続的に監視し、端末で不審なアクティビティが行われた場合には警告します。

詳しくは、<https://gsuite.google.com/security> をご覧ください。



プロダクトのセキュリティ: GCP

GCP のお客様は次のようなプロダクトの機能や設定を活用して、未承認の処理や不正処理から個人データをさらに保護できます。

- 2 段階認証を導入すると、ユーザーのサインイン時に身元が追加確認されるため、不正アクセスのリスクが大幅に低減されます。セキュリティキーの使用を必須にすると、物理的なキーの使用を義務付けられるため、ユーザー アカウントのセキュリティがさらに強化されます。
- Google Cloud Identity and Access Management (Cloud IAM) では、Google Cloud Platform リソース向けにきめ細かいアクセス権や変更権限を作成し、それを管理できます。
- Data Loss Prevention API は、特別なカテゴリーの個人を特定し、その処理をモニタリングして、適切な制御を実行します。
- Stackdriver Logging と Stackdriver Monitoring は、ロギング、モニタリング、アラート、異常検知の各システムを Google Cloud Platform に組み込みます。
- Cloud Identity-Aware Proxy (Cloud IAP) は、Google Cloud Platform で実行するクラウド アプリケーションへのアクセスを制御します。
- Cloud Security Scanner は、Google App Engine アプリケーションの一般的な脆弱性をスキャンし、検出します。

詳しくは、<https://cloud.google.com/security/> をご覧ください。



データの返却と削除

管理者は契約の期間中、G Suite または Google Cloud Platform サービスの機能を通じて顧客データを随時エクスポートできます。Google では数年前よりデータ処理に関する規約にデータ エクスポートに対する取り組みを含めてきましたが、GDPR の施行後もこの取り組みを継続し、G Suite サービスと Google Cloud Platform の各サービスのデータ エクスポート機能の強化に取り組んでいきます（詳しくは [Google Cloud Platform ドキュメント](#)をご覧ください）。

また、顧客データは随時 G Suite または Google Cloud Platform サービスの機能を通じて削除することができます。Google は、データの完全な削除の指示をお客様から受け取った時点から（たとえば削除したメールを「ゴミ箱」から復元できなくなった時点など）遅くとも 180 日以内に、関連顧客データをすべてのシステムから削除します。ただし、保持義務が適用される場合はこの限りではありません。



データ管理者の支援

データ主体の権利

データ管理者は、G Suite および Google Cloud Platform の管理コンソールとサービス機能を利用し、データ管理者とそのユーザーが Google システムに送信したデータへのアクセス、修正、制限、処理、削除を行えます。この機能により、GDPR に則した権利行使についてデータ主体からの要求があった場合に、その義務を遂行することができます。

データ保護チーム

G Suite および Google Cloud Platform のお客様には、データ保護関連の照会先窓口としての専用チームが設けられています。

インシデント通知

G Suite と Google Cloud Platform は、長年にわたってインシデント通知に関する契約責任を果たしてきました。今後も Google は、顧客データに関するインシデントが発生した場合、データ インシデントに関する契約条項、および GDPR の施行とともに 2018 年 5 月 25 日から適用される新しい条項に沿って速やかに通知を行います。

国際的なデータ転送

GDPR では、EU 域外への個人データの転送を簡便化するメカニズムが提供されます。このメカニズムには個人データを域外に転送するに際し、十分な保護を提供していること、および適切な安全保護対策を講じていることを確認するという目的があります。

適切な安全保護対策は、モデル契約条項で提供されます。また、十分な保護が提供されているかどうかは、十分性認定によって確認されます（EU-US 間プライバシー シールドなどをサポートする十分性認定など）。

Google では、現行のデータ処理契約下で、データ保護指令に準じ、EU 域外への個人データの転送を簡便化するメカニズムを保持する契約上の義務を負っています。また、GDPR の施行とともに 2018 年 5 月 25 日より、それに対応する責任を引き続き果たしていきます。

EU-US 間プライバシー シールドおよび Swiss-US 間プライバシー シールドの枠組みに従って Google が認証を受けているプロダクトとしては、G Suite と Google Cloud Platform が挙げられます。また、Google のモデル契約条項については、欧州データ保護当局から適合確認を受けています。つまり、G Suite と Google Cloud Platform に関する現行の契約責任は、データ保護指令に準じて、EU 域内から域外へ個人データを転送する法的要件を完全に満たしていることが認定されています。

標準と認証



ISO 27001 (情報セキュリティ管理)

ISO 27001 は広く認知され、国際的に認められている独立したセキュリティ基準です。Google は、共有の Common Infrastructure および G Suite と Google Cloud Platform プロダクトを構成するシステム、アプリケーション、人、技術、データ処理、およびデータセンター サービスについて、ISO 27001 認証を受けています。



ISO 27017 (クラウド セキュリティ)

ISO 27017 は、ISO/IEC 27002 に基づく情報セキュリティ管理の実践方法を、クラウド サービスに特化して定めた国際規格です。Google は、G Suite と Google Cloud Platform について ISO 27017 認証を受けています。



ISO 27018 (クラウド プライバシー)

ISO 27018 は、パブリック クラウド サービスで個人情報 (PII) を保護する方法を規定した国際基準です。Google は G Suite と Google Cloud Platform について ISO 27018 認証を受けています。



SSAE16 / ISAE 3402(SOC 2/3)

American Institute of Certified Public Accountants (AICPA: 米国公認会計士協会) の SOC 2 (Service Organization Controls) と SOC 3 は、信頼の原則と、セキュリティ、可用性、処理の整合性、機密性保持の基準を定めた監査フレームワークです。Google では、Google Cloud Platform と G Suite について SOC 2 と SOC 3 の保証報告書を取得しています。

よくある質問

① GDPR とは何ですか？

一般データ保護規則 (GDPR) は、1995 年 10 月 24 日の データ保護に関する 95/46/EC 指令に代わる、EU の新しいプライバシー法です。

② GDPR が適用されるのはいつからですか？

2018 年 5 月 25 日以降、欧州連合の全加盟国に直接適用されます。

③ GDPR では、個人データを EU 域内に保管することが義務付けられていますか？

いいえ。データ保護に関する 95/46/EC 指令と同様、GDPR でも一定の条件のもとに EU 域外への個人データの転送が認められています。これらの条件は、モデル契約条項などのメカニズムによって満たすことができます。

④ GDPR では、Google Cloud を監査する権利が顧客側に付与されますか？

GDPR では、データ管理者とデータ処理者との間で締結される契約において、監査の権利をデータ管理者に付与することを義務づけています。したがって、GDPR の施行とともに 2018 年 5 月 25 日から適用される新しいデータ処理契約では、お客様のために監査の権利が定められています。

⑤ 第三者機関による ISO 27001、ISO 27017、ISO 27018、SOC 2/3 の監査報告書は、GDPR の規制遵守においてどのような役割を果たしていますか？

お客様がリスク評価を行うにあたり、第三者機関が Google に対し発行した ISO 認証および SOC 2/3 監査報告書を参照することにより、技術的および組織的に適切な措置がとられているかどうかを判断することができます。

⑥ Google は GDPR について他にどのような情報を提供していますか？

[Google のビジネスとデータ ウェブサイトをご覧ください。](#)