Google Cloud ホワイトペーパー

2022年6月

個人情報保護法 (日本)

Google Cloud

Google Cloud

はじめに

個人情報は今日の情報システムにとって欠かせない要素となっています。個人情報はプライバシーとセキュリティの両面で機密性が高く、いずれかの侵害があると、個人と社会の両方に損害が生じる可能性があります。このような理由から、組織には個人情報を保護する義務があり、政府は個人情報に関する法律 や規制を強化しています。日本で個人情報を保護するために施行されている規制の一つが個人情報保護法です。このホワイトペーパーでは、Google Cloud サービスの導入という観点から個人情報保護法を検討します。また、クラウドプロバイダとクラウドを利用する顧客の役割と責任を明確にします。さらに、個人情報保護法遵守のさまざまな側面と、個人情報の全般的な保護を支援する Google のクラウドサービ スもご紹介します。

取り扱う内容

個人情報

このホワイトペーパーでは、個人情報、特にお客様が Google Cloud Platform または Google Workspace にの利用のために保管・配置した個人情報について説明していきます。サービス プロバイダとしての Google Cloud にお客様が直接提供する個人情報については取り上げません。そちらのトピックの詳細については、Google Cloud のプライバシーに関するお知らせをご覧ください。

サービス

このホワイトペーパーで説明する原則は、Google Workspace と Google Cloud Platform の両方に適用されます。簡略化のためにこのホワイトペーパーではこれらのサービスまたはこれらのサービスを提供するGoogleのエンティティを総称して Google Cloud と呼びます。このホワイトペーパーは情報提供のみを目的としています。このホワイトペーパーのいかなる内容も、法律上の助言の代わりとして提供するものではなく、使用すべきものでもありません。

個人情報保護法の規制

個人情報保護法は2003年に成立し、その後何度も改定されています。直近では2021年6月に改正され、2022年4月1日に施行されました。日本政府は、個人情報保護法の主要規制機関として2016年に個人情報保護委員会を設立しました。個人情報保護委員会には罰則を科す権限はありませんが、法執行機関に申し立てを行うことができます。このような状況になった場合、特に悪質なケースでは罰金や懲役刑を含む罰則が科される場合があります。また、個人情報保護委員会への虚偽の報告や、個人情報保護委員会の命令に対する違反も罰金の対象となる場合があります。さらに、個人情報が悪用された者に対する民事責任が問われる場合もあります。

個人情報保護法に関連する規制当局は個人情報保護委員会だけではありません。一部の業種では、業界規制当局からその業種固有のガイダンスが提供されています。たとえば、総務省と金融庁では、それぞれが 管轄する業種向けのガイドラインを発行しています。個人情報保護委員会 のウェブサイトは個人情報保護法に関する優れた情報源であり、法律の解釈に非常に役立つガイドラインも用意されています。

主な義務

個人情報保護法では、取り扱う個人情報 の持ち主に対して個人情報取扱事業者が負う主な義務が規定されています。以下は、個人情報取扱事業者が個人情報保護法のもとで本人に対して負う主な義務の概要です。

[1] 利用目的

個人情報取扱事業者は、個人情報を収集する目的を本人に通知しなければならない。

[2] 利用目的による制限

個人情報取扱事業者は、本人の明示的な同意がない限り、目的の範囲を超えて個人情報を取り扱ってはならない。

[3] 同意

個人情報取扱事業者は、取扱いに配慮を要する情報を含む個人情報を収集するために、本人の同意を得なければならない。これには、人種、信条、社会的身分、身体的または精神的障害、医療記録、犯罪歴及び犯罪の被害に遭った事実などが含まれる。

[4] 正確性

個人情報取扱事業者は、個人情報を正確かつ最新の内容に保つよう努めなければならない。

[5] 削除

個人情報取扱事業者は、利用する必要がなくなったときは、個人情報を削除しなければならない。

[6] 安全管理措置

個人情報取扱事業者は、取り扱う個人情報を保護するための安全管理措置を講じなければならない。

[7] 監督

個人情報取扱事業者は、個人情報を取り扱う従業員および委託先に対する適切な監督を行わなければならない。

[8] 第三者提供

個人情報取扱事業者は、第三者に自社の個人情報を提供するために、あらかじめ本人から同意を得なければならない。

[9] 外国にある第三者への提供

個人情報取扱事業者は、個人情報を外国にある第三者に提供するために、本人からあらかじめ同意を得なければならない。ただし、日本と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会が定める国、及び個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会が定める基準に適合する体制を整備している第三者を除く。

[10] 開示

個人情報取扱事業者は、本人の要求に応じて、当該本人が識別される個人情報を本人に開示しなければならない。

責任共有モデル

Google Cloud はクラウドのセキュリティに対して責任を負います。お客様にはお客様自身がクラウドに配置するものに対するセキュリティの責任を負っていただくことになります。

Google Cloud とお客様との間には関係性がありますが、お客様が収集した個人情報に紐づく本人と Google Cloud の間には関係性がありません。Google Cloud は、お客様が GCP または Google Workspace に配置した個人情報に関知せず、その個人情報の取扱事業者となることもありません。お客様が選択したサービスを実行する目的でのみ、Google Cloud は自社システム内の顧客データを処理します。

より明確にするために、Google Cloud のユーザの責任範囲と Google Cloud の責任という観点から、個人情報保護法の主な要件10個をそれぞれ整理します。

[1] 利用目的

個人情報取扱事業者は、個人情報を収集する目的を本人に通知しなければならない。

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
本人との関係性に対応し、使用目的を明確に説明することで、個人情報が合法的に収集されるようにします。	お客様が個人情報を収集した本人とGoogle Cloud との間には関係性はなく、利用目的の表明や同意の取得に Google Cloud は関与しません。

[2] 利用目的による制限

個人情報取扱事業者は、本人の明示的な同意がない限り、目的の範囲を超えて個人情報を取り扱ってはならない。

Google Cloud のユーザの責任範囲	Google Cloud の責任範囲
本人との関係性に対応し、所定の使用目的どおりに使用されるようにすることによって、個人情報が合法的に処理されるようにします。	Google Cloud は、お客様が個人情報を取り扱うために使用できるクラウド サービスを提供します。

[3] 同意

個人情報取扱事業者は、取扱いに配慮を要する個人情報を収集するために、本人の同意を得なければならない。

Google Cloud のユーザの責任範囲	Google Cloud の責任範囲
必要な同意が得られていることを確認します。	お客様が個人情報を収集した本人とGoogle Cloudとの間には関係性がなく、Google Cloud は 同意の取得に関与しません。

[4] 正確性

個人情報取扱事業者は、個人情報を正確かつ最新の内容に保つよう努めなければならない。

Google Cloud のユーザの責任範囲	Google Cloud の責任範囲
個人情報が正確かつ最新の内容であることを確保します。	Google Cloud は、お客様が個人情報を取り扱うために使用できるクラウドサービスを提供します。Google Cloud は、お客様の個人情報の正確性の維持には関与しません。ただし、Google Cloud は自社のサービスに配置されたデータの整合性を確保します。

[5] 削除

個人情報取扱事業者は、利用する必要がなくなったときは、個人情報を削除しなければならない。

Google Cloud のユーザの責任範囲	Google Cloud の責任範囲

個人情報を使用する目的がなくなったか、本人から要求された場合には個人情報を削除します。	Google Cloud は、お客様が個人情報を取り扱うために使用できるクラウドサービスを提供します。お客様はいつでも Google Cloud のデータを削除できます。

[6] 安全管理措置

個人情報取扱事業者は、取り扱う個人情報を保護するための安全管理措置を講じなければならない。

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
お客様管理下のクラウドにおける機能の適切な構成を含め、個人情報を保護するための適切な安全管理措置を講じます。	お客様が安全に利用できる適切な安全管理機能を備えたクラウドサービスを提供します。

[7] 監督

個人情報取扱事業者は、個人情報を取り扱う従業員および委託先に対する適切な監督を行わなければならない。

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
従業員及び委託先による個人情報の取り扱いを監督するための適切な措置を講じます。	Google Cloud は、お客様が Google Cloud に保存したデータに対するお客様の利用状況を監督しま せん。

[8] 第三者提供

個人情報取扱事業者は、第三者に自社の個人情報を提供するために、あらかじめ本人から同意を得なければならない

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
個人情報を取り扱わないクラウドプロバイダへの個人情報の提供は、第三者の個人情報取扱事業者への提供、また、委託先の監督が必要となる個人情報取扱の委託とは見なされないため、追加の特定同意は不要であると個人情報保護委員会（個人情報保護委員会）は述べています。	お客様が個人情報を収集した本人とGoogle Cloudとの間には関係性がありません。お客様の同意がない限り、Google Cloudに保存された個人情報を取り扱うことはありません。

上記を踏まえて特定の同意の必要性をご検討ください。 参考資料:個人情報保護委員会 Q&A(令和4年4月1日更新） Q7-53	

[9] 外国にある第三者への提供

個人情報取扱事業者は、個人情報を外国にある第三者に提供するために、本人から同意を得なければならない。日本と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会が定める国を除く。

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
お客様は、海外の第三者個人情報取扱事業者に個人情報を転送する場合に本人から同意を得る必要があります。 Google Cloudのような外国にある事業者が、サーバに保存された個人データを取り扱わないこととなっている場合には、外国にある第三者への提供に該当しません。 参考資料:個人情報保護委員会 Q&A Q7-53、Q12-4	Google Cloud では、Google Cloud のサービスが日本と海外のどちらを位置しているかを明確に示したガイダンスを提供しています。

[10] 開示

個人情報取扱事業者は、本人の要求に応じて、当該本人が識別される個人情報を本人に開示しなければならない。

Google Cloud のユーザの責任範囲	**Google Cloud** の責任範囲
個人情報の開示要請処理プロセスを設けます。	お客様が個人情報を収集した本人とGoogle Cloudとの間には関係性がなく、Google Cloud は本人からの開示要請に対応できません。

よくある質問

[1] Google Cloud などのクラウド サービスにデータ取扱事業者が個人情報を配置することは個人情報保護法で許可されていますか？

はい。個人情報保護法にはクラウド サービスの使用に関する制限がありません。

[2] Google Cloud への個人情報の配置は、本人の同意を必要とする第三者への転送に該当しますか？

個人情報を取り扱わないクラウド プロバイダへの個人情報の提供は、第三者の個人情報取扱事業者への提供とは見なされないため、追加の特定の同意は不要であると個人情報保護委員会は述べています。

参考資料:個人情報保護委員会 Q&A Q7-53

[3] 特定の技術に関する法解釈の詳細、およびそれが同意要件に与える影響についてはどこで確認できますか？

個人情報保護委員会のウェブサイトは個人情報保護法の優れた情報源であり、個人情報保護法の解釈に非常に役立つガイドラインも用意されています。

[4] 個人情報を海外で保存する場合、追加の特定の同意を得ることが個人情報保護法 によって規定されています。**Google Cloud** に置いたデータはどこに保存されているのでしょうか？

Google Cloud サービスのロケーションとリージョンはこちらのページでご確認いただけます。リージョンが東京または大阪となっているサービスでは、データが日本に保存されます。その他のサービスで は、海外にデータが保存される場合があります。
Google Cloudでは、すべての場所のサービスに対して一貫性のあるセキュリティ対策を実施しているため、個人情報がどこに保存されていても、安心してその安全な基盤から恩恵を受けることができます。

[5] Google Cloud が **Google Cloud** のサービスに対して適切なセキュリティ対策を実施していることを確認するにはどうすればよいですか？

Google Cloud では業界をリードするセキュリティ対策を実施しています。セキュリティ対策については Google Cloud のホワイトペーパーで説明しています。Google Cloud では契約条件に基づいて対 策を実施します。また、監査を受け、複数の国際標準に照らして Google Cloud の 契約条件をチェックしてもらうことで第三者機関からの保証を受けています。監査レポートと証明書のコピーを提 供して、お客様の監査保証ニーズに対応します。

[6] Google Cloud はデータに関する政府からの要請にどのように対応していますか？

Google Cloud には、日本ををはじめ、事業を行っている各国の法律を遵守する義務があります。法執行機関 は通常、調査対象者にデータの要請を行うことが、Google のこれまでの経験から明らかになっています。調査対象の個人情報を取り扱う企業のクラウド プロバイダに開示要請がなされることはほとんどありません。

Google Cloud では政府からの要請を慎重に審査し、それが合法的で強制力があり、範囲が適切であることを確認します。無効な要請は拒絶されます。法的に許される場合は、お客様に通知し、お客様と協力します。詳細については、政府からの顧客データ開示要請に関するホワイトペーパーをご覧ください。さらに、受け取った要請の性質をお客様が知ることができる透明性レポートも発行しています。

[7] Google Cloud では、規制の変化をどのようにモニタリングして対応していますか？

Google Cloud では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、公共政策の専門家からなるチームを編成しています。これらのチームは、お客様、業界関係者、監督機関と連携して、お客様のコンプライアンス ニーズを満たすクラウド サービスを構築しています。さらに、お客様と緊密に連携して、お客様固有のコンプライアンス要件を理解し、明らかに なった要件を満たす戦略の策定をお手伝いしています。

また、Google Cloudには、世界中のセキュリティ関連の法律や規制の遵守をレビューする内部監査担当者とコンプライアンスの専門家からなる専任のチームがあります。新しい監査標準が作成されると、それらを満たすために必要な管理措置、プロセス、システムを内部監査チームが決定します。このチームは、第三者による独立した監査および評価を促進、サポートします。世界中の規制環境は常に変化しており、Google Cloud はその変化に合わせて進化を続けていきます。

個人情報保護法ガイドライン

個人情報保護委員会は、個人情報保護法を遵守するための推奨安全管理対策を含むガイドラインを公開しています。以下は、個人情報保護法ガイドライン（通則編）の要点、およびガイドラインの遵守に役立つ可能性がある Google Cloud の機能とサービスの概要をまとめたものです。

個人情報保護法ガイドラインのセクション 10.3～10.6 では、必要な安全管理措置が以下の 4 つのカテゴリに分類さ れています。

1. 組織的安全管理措置
2. 人的安全管理措置
3. 物理的安全管理措置
4. 技術的安全管理措置

以下の表は、各カテゴリの要件と安全管理のコンセプトの対応関係を示したものです。以降のセクションでは、セキュリティの責任共有モデルの安全な基盤を実現するうえで Google Cloud が果たす役割について説明していきます。その後、安全管理の各コンセプトを実施し、個人情報保護法ガイドラインで推奨され ている安全管理対策を満たすのに役立つ Google Cloud のプロダクトとサービスをご紹介します。

組織的安全管理措置

要件	安全管理のコンセプト
組織体制の整備	ID データ ガバナンス 契約に基づくセキュリティ セキュリティ保証
個人データの取扱いに係る規律に従った運用	ロギング データ ガバナンス
個人データの取扱状況を確認する手段の整備	データ ガバナンス ID アクセス制御
漏えい等事案に対応する体制の整備	ロギング 脅威の検出
取扱状況の把握及び安全管理措置の見直し	ロギング データ ガバナンス セキュリティ保証

人的安全管理措置

要件	安全管理のコンセプト
従業者の教育	トレーニングとコンサルティング

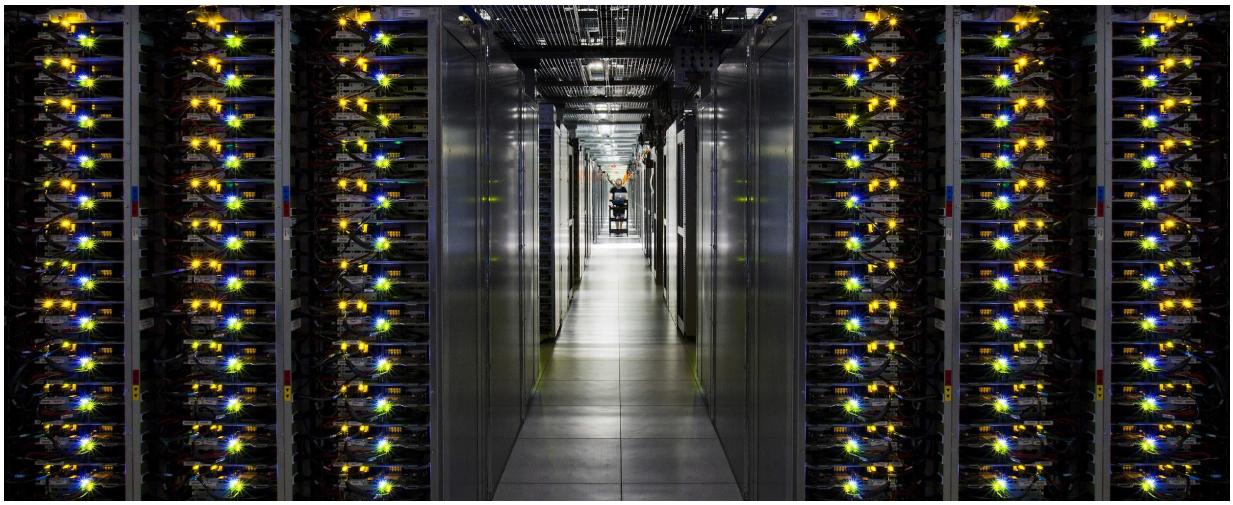
物理的安全管理措置

要件	安全管理のコンセプト
個人データを取り扱う区域の管理	インフラストラクチャのセキュリティ ID データ ガバナンス データの変換

機器及び電子媒体等の盗難等の防止	インフラストラクチャのセキュリティ エンドポイント
電子媒体等を持ち運ぶ場合の漏えい等の防止	インフラストラクチャのセキュリティ エンドポイント データの変換
個人データの削除及び機器、電子媒体等の廃棄	データの削除

技術的安全管理措置

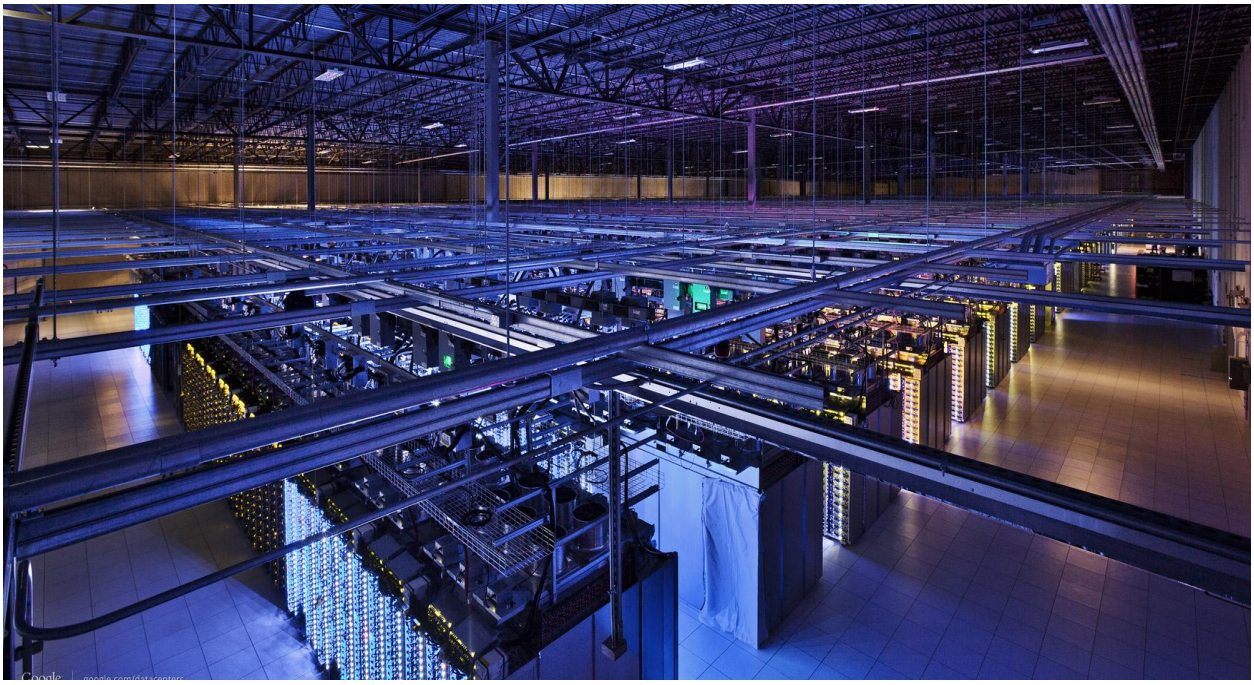
要件	安全管理のコンセプト
アクセス制御	ID アクセス制御
アクセス者の識別と認証	ID ロギング
外部からの不正アクセス等の防止	アクセス制御 エンドポイント セキュアな CI / CD パイプライン パートナー ソリューション リスクの検出 脅威の検出
情報システムの使用に伴う漏えい等の防止	インフラストラクチャのセキュリティ エンドポイント セキュアな CI / CD パイプライン リスクの検出 データ ガバナンス データの変換



Google Cloud のセキュリティ

インフラストラクチャのセキュリティ

Google では、情報処理ライフサイクルを通じて最先端のセキュリティを提供するように設計されたグローバル 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、サービスの安全な デプロイ、エンドユーザーのプライバシー保護を備えたデータの安全な格納、サービス間での安全な通信、インターネット経由の顧客との安全な非公開通信、管理者による安全な操作を実現できるよう 構築されています。Google Workspace と Google Cloud Platform はこのインフラストラクチャ上で運用されています。



データセンターの物理的なセキュリティ、ハードウェアとソフトウェアのセキュリティ保護、運用セキュリティのサポートに使用するプロセスが相互に補完しあう階層型のインフラストラクチャ セキュリティを構築しています。この階層型の保護によって実現された強力なセキュリティ基盤ですべての処理を行っています。インフラストラクチャ セキュリティの詳細については、Google インフラストラクチャのセキュリティ設計ホワイトペーパーをご覧ください。

契約に基づくセキュリティ

GCP と Google Workspace のデータ処理規約には、セキュリティとプライバシーに関するお客様へのコミットメントが明確に記載されています。Google では、お客様や規制当局からのフィードバックに基づいて、長年にわたってこれらの規約を進化させてきました。お客様が Google のシステムに入力したデータは、お客様の指示に従ってのみ処理されるという考えがこの規約の柱となっています。

Google Cloud では、システムの機密性、整合性、可用性を確保するためのセキュリティ対策も実施しています。これらは、セキュリティ対策に将来的に加えられる変更によってセキュリティが低下することはないというコミットメントとともに、契約に詳しく記載されています。お客様向けのセキュリティを継続的に改善することがこのような記載の目的です。

セキュリティ保証

Google Cloud Platform と Google Workspace では、複数の第三者監査機関によるデータ安全性、プライバシー、セキュリティに関する監査を受けています。Google の第三者監査アプローチは、機密性、整合性、可用性に関する情報セキュリティレベルの保証を提供するために、包括的なものになるように設計されています。お客様は第三者機関によるこうした監査を利用することで、Google が提供しているプロダクトが自社のコンプライアンスとデータ処理のニーズをどのように満たしているかを確認できます。個人情報保護法の対象となるお客様に関連するサードパーティ認証は以下のとおりです。詳細については、Google Cloud のコンプライアンス リソース センターをご覧ください。

ISO/IEC 27001

ISO/IEC 27001 は、情報セキュリティ管理システムの要件を概説および規定するセキュリティ標準です。Google がセキュリティ管理の包括的で継続的な改善モデルを構築できるようにするための、安全管理のフレームワークとチェックリストが 27001 標準で規定されています。Google Cloud Platform と Google Workspace は ISO 27001 遵守の認証を受けています。

ISO/IEC 27018

ISO/IEC 27018 は、パブリック クラウド サービスにおける個人情報の保護に関するプラクティスの国際標準です。Google Workspace と Google Cloud Platform は ISO/IEC 27018遵守の認証を受けています。

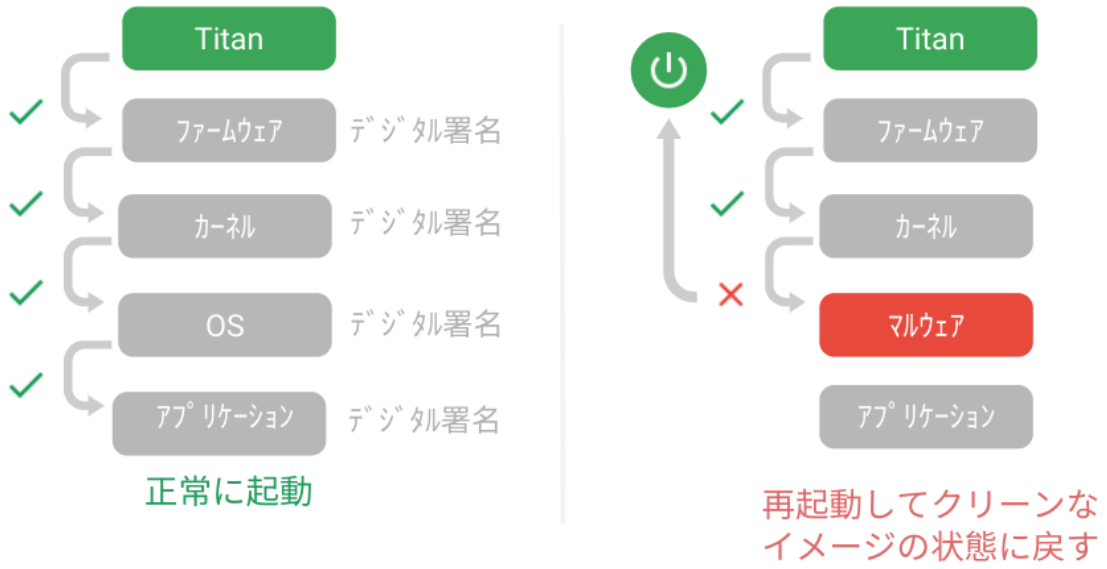
Google Cloud サービス

エンドポイント

Google では、Chrome プロダクト ファミリの一部としてブラウザと OS テクノロジーを開発しました。これらのプロダクトでは、エンドポイントに一般的な脅威が進入するのを防ぐために、攻撃対象領域が非常に小さくなっています。Chrome ブラウザ、Chrome OS、Chromebook を Chrome Enterprise で一元管理することで、お客様にこれらのソリューションを提供しています。

Chrome ブラウザは自動的に更新されるコンパクトなブラウザです。Chrome ではセーフ ブラウジングを使用して、既知の不正な URL を登録したデータベースと現在アクセスしている URL を照合し、リスクが高いと見なされるサイトをブロックしたり、警告を表示したりできます。Chrome ではタブだけでなくタブ内の I-フレームまでもがサンドボックス化されています。Chrome 自体は OS 上で隔離されており、他のプロセスにはアクセスできません。

Chromebook には Chrome OS が搭載されています。Chrome OS は読み取り専用の OS であるため、マルウェアがシステム ファイルに感染したり、システム ファイルを変更したりすることはできません。Chromebook には、作業コピーとスタンバイ コピーという Chrome OS の 2つのコピーが保持されています。作業コピーの起動に失敗すると、スタンバイ コピーで起動が行われます。これは、アップグレードにスタンバイ コピーを使用し、再起動時にそのスタンバイ コピーを作業コピーにする場合に便利です。そのため、セキュリティが強化されるだけでなく、アップグレードのダウンタイムも発生しません。Chromebook には、ファームウェア、OS、ブラウザコードを検証する Titan C チップが搭載されています。変更が検出された場合、そのバージョンの OS は起動しません。



Chromebook では保存データが暗号化されますが、Google Workspace などの Google Cloud サービス に大半のデータが保存されるため、Chrome ユーザーが Chromebook に保存するデータ量は少ない傾向にあります。そのため、盗まれるものが何もなく、ランサムウェアに感染しても身代金を払う必要はありません。

Chrome Enterprise Upgrade は、Chrome OS 環境で一貫した管理を行うためのクラウドベースの管理システムです。すべてのデバイスに対して 1つのコンソールからソフトウェアのデプロイ、アップグレード、Chrome の設定を構成できます。Chrome Enterprise と Chromebook を使用することで、エンドポイントの安全管理措置に対する個人情報保護委員会の要件を簡単に満たせるだけでなく、それを大幅に上回ることができます。

ID

ID はアクセス制御の要であり、個人情報保護法ガイドラインの要件の柱となっています。Google Cloud では、複数の ID プロバイダと 自らが提供する Cloud Identity をサポートしています。

Cloud Identity では機械学習を使用して不正アクセスを検出します。さらに、正しいパスワードを使用した不正侵入者を検出してブロックすることもできます。

また、FIDO 準拠のセキュリティ キーなど、複数の 2 段階認証オプションを含む、強力な形のアカウント保護もサポートしています。Google 社員は Google アカウントでセキュリティ キーを使用することで、より強力な ID 保護を実現し、フィッシング攻撃を防止しています。お客様側でも同じ対策を実施することをおすすめします。

アクセス制御

個人情報保護法ガイドラインの柱となっているのが最小権限のルールです。個人情報取扱担当者には、担当業務を遂行するのに最低限必要なアクセス権のみを付与する必要があります。

Google Cloud では、すべてのサービスで使用に認証が必要です。認証は主に IAM で管理されます。IAM を使用すると、ユーザーやグループなどのメンバーにロールを付与できます。これらのロールはきめ細かい権限で構成されています。厳選されたロールがあらかじめ用意されており、必要に応じてカスタムのロールを作成することもできます。

条件をロールに適用することもできます。たとえば、午前9時から午後5時まで業務を行う契約社員の場合、アクセスを午前9時から午後5時までに制限する条件を契約社員のロールに追加できます。

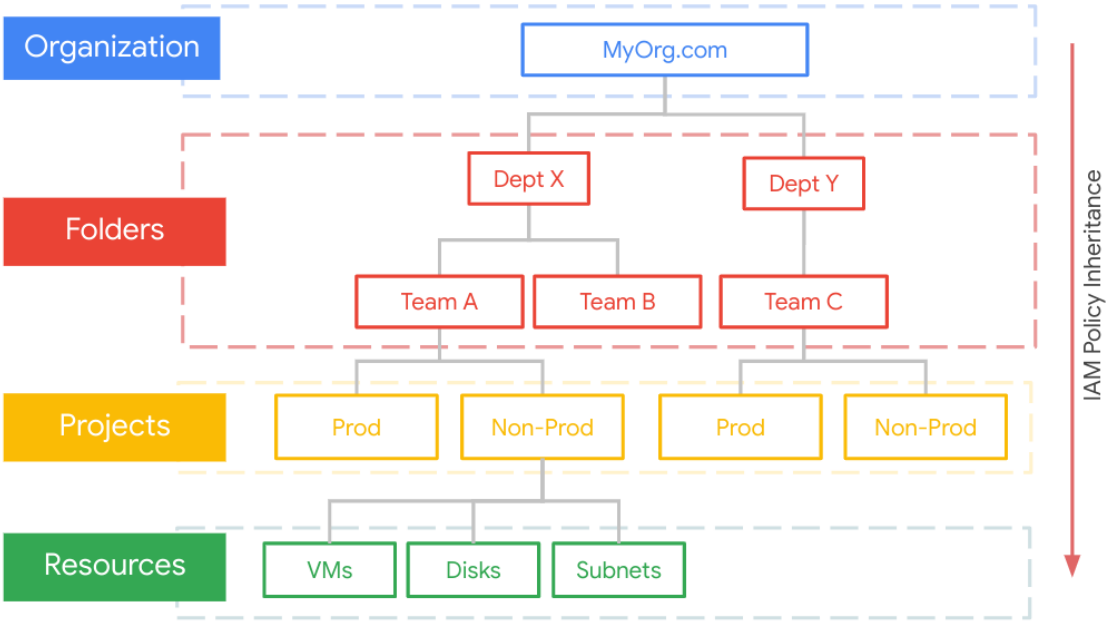
GCP には、フォルダツリーを設定してプロジェクトを整理できるリソース マネージャーが用意されています。アクセス制御は階層のどのレイヤでも管理でき、下の階層に継承されるため、適切なガバナンスに威力を発揮します。個人情報専用のフォルダを作成し、そこにアクセス制御を適用することで、そのフォルダ内のすべてのプロジェクト間で一貫性を保つことができます。

企業のお客様にとっての最大の課題の一つはアクセス権の付与ではなく、アクセス権が必要ない場合や過剰な場合にアクセス権を無効にすることです。IAM Recommender では、機械学習を使用して、使用されている権限と使用されていない権限を把握し、過剰なアクセス権を削除するように推奨します。Policy Analyzer では、どの情報に誰がアクセスできるかを把握できるため、監査の場面で役立ちます。

一部の Google Cloud サービスには、IAM に用意されている以上のサービス固有のアクセス制御機能があります。たとえば、BigQuery では、データテーブルのビューに制限をかけたり、特定の条件を

満たす行や列をフィルタしたりできます。個人情報データアナリストが閲覧できる情報を最小限にする場合や、完全に表示しない場合にこの機能が非常に役に立ちます。

Google Workspace では、ユーザーの ID とデバイスのコンテキストに基づいてサービスにアクセス制御を適用できます。各ファイルまたはフォルダの読み取り、コメント入力、編集を行えるユーザーをファイルレベルで定義できます。



ネットワークのアクセス制御

個人情報保護法ガイドラインで明示的に示されているアクセス制御の基本的なレイヤの一つがネットワークレイヤです。

大半のクラウド プロバイダでも使用されている従来のネットワークでは、ネットワーク アクセスを制御するファイアウォール ルールを特定の箇所でしか適用できません。Google Cloud には、はるかに柔軟性が高いファイアウォール ルールが用意されています。単一の VM、タグ付きアセット、同じサービス アカウントを共有するアセット、または複数の要素の組み合わせに適用できます。

すべてのプロジェクトに同じルールを適用する代わりに、階層型ファイアウォール ポリシーを使用して、フォルダレベルまたは組織レベルのプロジェクトに共通のルールを適用できます。

アセットに影響するルールは、コマンドラインと Network Intelligence Center の両方から分析できます。

サービス API へのアクセスを制御することも重要です。Google Cloud では、有効または無効にする API をお客様が決定します。さらに、VPC Service Controls ではプロジェクトで使用する API の周囲

に境界を配置できます。また、データ送信をブロックし、データ受信に条件を設定することもできます。

アプリケーションのアクセス制御

Google Cloud には、お客様が独自のアプリケーションを構築できるインフラストラクチャが用意されています。こうしたアプリケーション内のアクセス制御は、お客様が用意するアプリケーション ロジックの一部です。一方で、BeyondCorp という Google Cloud のコンテキスト アウェア アクセス システムを活用してこうしたアプリケーションへのアクセスを制御することもできます

BeyondCorp では、どのユーザーがどのような条件でどのアプリケーションにアクセスできるかを定義できます。これらの条件は、状況（時間など）、デバイス（企業で管理しているものなど）、ユーザーの ID と認証（2段階認証 など）に関連付けることができます。

これらの条件は、リスクシナリオごとに異なるセキュリティを適用するために使用できます。アクセス制御とベンダーの監督に関する個人情報保護法の要件に対応するうえで、こうした条件が役立ちます。たとえば、多くの企業が給与処理を外注しており、従業員の個人情報を含む内部システムへのアクセス権を給与処理を担当するベンダーに付与している場合があります。BeyondCorp では、システムへのアクセスを許可する条件として、ベンダーの PC でセキュリティ チェックを行えます。このチェックには、PC のディスクがすべて暗号化されていて、紛失したり盗難に遭ったりしてもすべてのデータを保護できるようになっているかといった項目も含めることができます。

ロギング

個人情報保護法ガイドラインではアクセスログの必要性について言及されており、個人情報保護法ではアクセスログを活用した監督について言及されています。Google Cloud には、サービス用の豊富な監査ログの機能が用意されています。

ネットワーク ログでは、詳細なネットワーク サービス テレメトリーでネットワークとセキュリティ両方の運用を把握できます。VPC フローログは、ネットワークのモニタリング、フォレンジック、リアルタイムのセキュリティ分析に使用できます。Packet Mirroring でパケットレベルのキャプチャを行えば、コンテンツを分析したり、データをネットワーク侵入検知システムに提供したりできます。ファイアウォール ルール ロギングでは、ファイアウォール ルールの効果を監査、検証、分析できます。NAT ログと DNS ログを脅威分析に使用することもできます。

Google Cloud Platform の Cloud Audit Logs では、誰が何をいつどこで実行したかなどの API アクティビティが記録されます。データ アクセス ログはデータレベルの詳細情報を提供し、データ管理サービスで特に便利です。Google Cloud でお客様のデータを処理することはありません。ただし、トラブル シューティングのサポートの一環としてデータへのアクセスをお客様から明確に指示された場合は、そのアクセスもログに記録され、お客様はアクセスの透明性によりこれらのログを確認できます。

Cloud Operations には、OS レベルのエージェント、Fluentd、REST API、クライアント ライブラリ、またはサードパーティ アプリケーションから送信されたカスタムログなど、さまざまなソースからログを取得できるロギング集中管理ツールが用意されています。ログはログビューアを使用してリアルタイムで分析できます。また、ログを可視化して、ログベースの指標と Cloud Monitoring を使用してログに対するアラートを出すこともできます。

GCP には、セキュリティとコンプライアンス両方の要件を満たすためのさまざまなログストレージと保持オプションが用意されています。システムログとデータ アクセス ログはデフォルトで30日間保持され、必要に応じて最大10年まで保持期間を延長できます。管理ログはロックがかかったストレージに400日間保持されます。ログデータは変更が不可能で、保存時に暗号化され、アクセスの透明性によってモニタリングされます。

Google Workspace には、管理からユーザー、サービス、デバイスに至るまで、あらゆるものに対応する豊富なロギング機能が用意されています。これらのログを GCP の Cloud Operations に送信して、統合分析を行うことができます。

脅威の検出

個人情報保護法ガイドラインでは、ログに脅威がないか検査することが推奨されています。Google Cloud の Security Command Center（SCC）では、Google Cloud のお客様が包括的なリスク管理を行うことができます。SCC のコンポーネントの 1つに脅威検出があります。SCC は、ログを既知のセキュリティ侵害の痕跡だけでなく、疑わしい動作とも比較してアラートを出します。これらのアラートには、Cloud Functions をトリガーすることで自動的に対処できます。そのため、たとえば、侵害が検出された VM のイメージ化とネットワーク上での隔離をすべて自動的に行うことができます。

ログを Google Cloud から Chronicle や Splunk などのサードパーティ SIEM にエクスポートして、脅威をさらに分析したり、クラウド以外のログと関連付けたりして、企業の脅威の全体像を把握することもできます。Chronicle は、すべてのログをセキュリティ侵害インジケーター（IOC）の膨大なデータベースと継続的に比較し、一致するものがあればそれを表示します。Chronicle では、ペタバイト単位のログをわずか 1秒で検索できます。

マネージド サービス

個人情報保護法ガイドラインでは、個人情報を保持するシステムを継続的にメンテナンスすることが求められています。システムのメンテナンスは、ほとんどのお客様にとって複雑でコストがかかり、面倒な作業です。そのため、Google がメンテナンスしているマネージド サービスを使用することをおすすめします。下の図にあるように、Google に任せるサービス管理の度合いが増えるほど、よりデータに集中して、基盤となるインフラストラクチャの責任の多くを Google に担わせることができます。

コンピューティング サービスが必要な場合でも、自社管理が不要なサービスを利用することをおすすめします。たとえば、Cloud Functions では、管理の手間を増やすことなくシンプルな関数を実行できます。GKE ではノードの自動アップグレードを使用してコンテナを管理できるため、メンテナンスの負担が軽減されます。

K8s の ID、認可、およびセキュリティ ポリシー コードの大部分を設計、作成したチームが GKE のセキュリティ管理も担当しています。このチームは、K8s の開発当初からすべての重大な脆弱性の調査、トリアージ、パッチ適用、通知を主導または担当しています。そのため、K8s の管理についてはこのチームに安心して任せることができます。

セキュアな CI / CD パイプライン

個人情報には人間だけでなくアプリケーション コードもアクセスします。そのため、脅威アクターは個人情報を処理するアプリケーションに読み込まれるコードを変更することで、個人情報を悪用する場

合もあります。だからこそ、継続的インテグレーションと継続的デリバリー（CI / CD）パイプラインの一環として、セキュリティ対策を実施することが非常に重要なのです。

Google では健全なコード レビュー プロセスを設けることを推奨しており、このプロセスに関するプラクティスと考えを紹介したガイドを一般公開しています。

Google Cloud にはノード用の COS（Container Optimized OS）が用意されています。Container-Optimized OS は小さく、セキュリティの脅威にさらされる可能性が最小限でありながら、読み取り専用の最小ルート ファイル システム、ファイル システムの整合性チェック、遮断されたファイアウォール、監査ログといった重要なセキュリティ機能が組み込まれています。自動更新によって適切なタイミングでセキュリティの脆弱性が自動的にふさがれることで、侵害のリスクがさらに軽減されます。シールドされた GKE は、Titan チップを搭載したハードウェア上に構築されており、ホスト ブートローダーからゲスト COS カーネルにいたる出所検証シーケンスを開始して、エンドツーエンドのサプライ チェーン セキュリティを実現します。

脆弱なコンテナを検出して対処することが重要になります。Google Cloud では、Container Registry に追加されたコンテナをスキャンして、不具合を検出できます。

コンテナ ポリシーは Anthos Container の Policy Controller を使って設定できます。Policy Controller は ガバナンスに最適で、会社のポリシーで許可されている権限を超えてプロジェクト チームがコンテナをデプロイしないようにするために使用できます。

Binary Authorization を使用することで、CI / CD パイプラインのさまざまなステップを通過するための署名を定義できます。これらの署名はデプロイの条件としてチェックできます。これにより、すべてのステップが確実に通過されるようになるだけでなく、不正なコードが本番環境にデプロイされるのを防ぐことができます。

リスクの検出

また、OWASP がターゲットとする一般的な構成ミスや脆弱性を探す Web Security Scanner を実行することで、アプリケーション コードをチェックすることもできます。Google Cloud のプレミアム サービスでは、GCP をスキャンしてウェブ アプリケーションを検索し、認可なしで密かに構築されたアプリケーションをあぶり出すこともできます

Security Command Center (SCC) は、Google Cloud を利用している組織全体で構成ミスや脆弱性をチェックし、それらをクラウド アセットのリストにマッピングします。実際に SCC は、アセットだけでなく、ISO 27001、PCI DSS、GCP の CIS ベスト プラクティスなど、さまざまなコンプライアンス フレーム ワークにもリスクと脅威をマッピングします。これにより、GCP に配置した個人情報に影響を与えるインシデントを防止、検出するという義務を果たすことができます。

Google Cloud

Google Workspace では、セキュリティ センターと呼ばれる 1 つの包括的なダッシュボードで、セキュリティ イベント、およびセキュリティ対策の有効性を示す指標を把握できます。このダッシュボードでは、組織全体にわたって悪意のあるメールを削除したり、個人情報ファイルの共有を調査して潜在的なデータ流出を特定、阻止したりするなど、セキュリティとプライバシーの問題を特定し、優先順位を付け、対処することができます。

データ ガバナンス

個人情報保護法のもとでは、個人情報取扱事業者の個人情報記録を監査する権限が個人情報保護委員会に与えられており、個人情報保護委員会に虚偽の報告を行うと、罰金を科される場合があります。また、個人には、データ取扱事業者が自分の個人情報を所有しているかどうか、および所有している個人情報の内容について開示を要請する権利があります。

現実には、企業内のさまざまなシステムや部署で個人情報の異なるコピーを作成するため、個人情報の追跡は組織にとって課題となる場合があります。データ ガバナンスこそが鍵であり、それを支援できるのが Google Cloud です。Google Cloud ではデータ ガバナンスを次のように定義しています。

1. 個人情報の検出
2. 個人情報へのラベル付け
3. 個人情報へのルールの適用

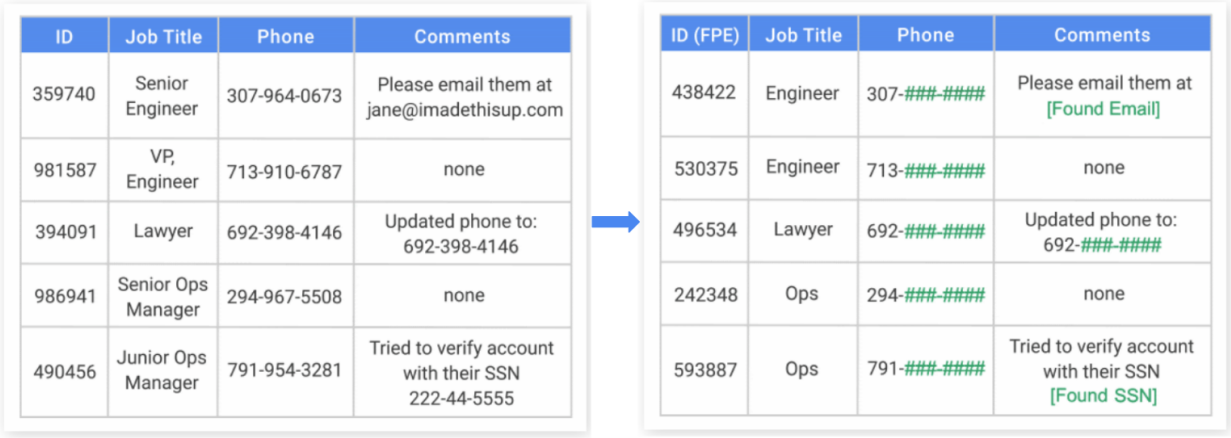
Data Catalog では、DLP API を使用して場所に関係なくメタデータ ラベルを検索して個人情報に適用できます。これらのラベルを使用してルールを適用することで、処理中のジョブまたはデータ分析システムで特定のデータの表示・非表示を制御できます。

Google Workspace には DLP 機能もあります。管理者は DLP 機能を使用して、ファイル内の個人情報を検出し、アラートなどの操作を行ったり、外部との共有を制限するなどの設定を行ったりできます。

データの変換

複数の変換手法を使用して、個人情報を取り扱うさまざまな場面で個人情報を非表示にしたり削除したりできます。DLP API では、個人情報をマスキングまたは秘匿化することで個人情報を削除でき

ます。これは、テキストだけでなく画像にも適用されます。



ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

ID (FPE)	Job Title	Phone	Comments
438422	Engineer	307-###-####	Please email them at [Found Email]
530375	Engineer	713-###-####	none
496534	Lawyer	692-###-####	Updated phone to: 692-###-####
242348	Ops	294-###-####	none
593887	Ops	791-###-####	Tried to verify account with their SSN [Found SSN]

個人情報を秘匿しながらも、その個人情報を使わなければならない場合もあります。これは 2つの方法で実現できます。データテーブルのフィールドとして使用する場合、DLP API を使用して個人情報を一意のトークンで置き換えることができます（トークン化）。保存中または転送中のデータのみを秘匿する必要があるものの、後で秘匿を解除する場合は暗号化の方が適しています。

Google Cloud には多くの暗号化オプションが用意されています。Key Management Service（KMS）では、API を介してアクセスするマネージド サービスとして暗号操作を行うことができます。Cloud HSM では、バックエンドが FIPS-2 レベル 3 認定 HSM の場合に、同じ KMS フロントエンドを使用できます。業務を分離する場合は、External Key Manager を使ってフロントエンドで KMS を使用することもできます。

データの削除

個人情報を使用する目的がなくなったか、顧客が個人情報に対する同意を撤回した場合、個人情報取扱事業者はデータの使用を停止し、データを削除するよう努める義務があります。収集当初とは異なる目的でデータを使用し続ける法的な理由が発生する場合があることが、個人情報保護法と個人情報保護委員会では認識されています。また、複数のコンポーネントとバックアップがあるシステムでは、削除に時間がかかる場合があることも認識されています。

Google Cloud のお客様データの所有権はお客様にあり、いつでも削除できます。データを削除すると、そのデータは直ちに使用できなくなり、関連するさまざまなサービス コンポーネントにまで対象が及ぶデータ消去プロセスが開始されます。データ消去プロセスが完了するのに最大で 180日かかる場合があります。プロセスが完了すると、データを元に戻すことができなくなります。詳細については、GCP と Google Workspace に関するホワイトペーパーをご覧ください。

トレーニングとコンサルティング

個人情報保護法のガイドラインでは、重要な要件の一つとしてトレーニングが挙げられています。ガイドラインでは個人情報の取り扱いプロセスに重点が置かれていますが、これらのプロセスで

Google Cloud などのテクノロジーを使用する場合は、そのテクノロジーに関するトレーニングを受けることが推奨されています。Google Cloud には、お客様のために、次のような幅広いトレーニングとコンサルティングのサポートが用意されています。

- Google Cloud サービスのデモと適切なサービスの選択のサポートを行うプリセールス スタッフ
- お客様のチームにトレーニングを行うトレーニング スタッフと教育スタッフ
- Cloud OnAir と YouTube 動画
- 都合に合わせてトレーニングが受けられるオンライン トレーニング パートナー
- 必要なスキルを身に付けられる認定資格プログラム
- 複数の言語に対応したオンライン ドキュメント
- 実際に Google Cloud のサービスを使いながら学習できる Qwiklabs
- 販売後のコンサルティング サービス
- 大規模なソリューションの構築と管理を実現するシステム インテグレーター パートナーシップ
- アイデアを共有してインスピレーションを与える、ブログ、記事、動画、チャットルームで 構成された活発なオンライン コミュニティ

パートナー ソリューション

Google Cloud はさまざまなセキュリティ ソリューション企業と提携して、Google Cloud Marketplace や その他のパートナーシップ契約を通じてお客様がパートナー企業のソリューションを利用できるようにしています。また、Google Cloud パートナー以外の企業のものも含めた大半のセキュリティ ソリューションをサポートできる、基本的なコンピューティング サービスも提供しています。

Google Cloud のセールスチームでは、お客様のセキュリティ要件をお聞きしたうえで、ユースケースに最適なパートナー ソリューションに関する助言を提供しています。

まとめ

Google Cloud の世界クラスのインフラストラクチャは、個人情報ソリューションの構築に最適な基盤となります。セキュリティとプライバシーに対する Google Cloud の取り組みは、Google Cloud の契約条件によって裏付けられ、監査役によって検証されています。Google Cloudでは、お客様が個人情報保護法ガイドラインの推奨事項以 上のことを達成し、顧客の個人情報を保護するのに役立つさまざまな独自のプロダクトとサービスを提供しています。