

データ主権の実現 5ステップ



01	はじめに
02	規制の強化
03	重圧に直面する業種
04	5 ステップのプラン
05	まとめ



O1

はじめに



コラボレーションは、現代のビジネスにとって推進力となっています。チーム間、地域間、組織間のデータ共有は、イノベーションの促進、チームの生産性向上、ビジネスの成長の加速につながります。しかしこのように開かれたビジネスのあり方は、データセキュリティやコンプライアンスの要求と対立することがあり、ビジネスを進めるうえで複雑な課題を生み出すことがあります。

この課題に対応できなかった場合のリスクは甚大です。欧州では2024年だけでも、一般データ保護規則（GDPR）への違反で制裁金を科されたケースが277件、計11億9千万ユーロにのぼりました¹。MetaがEU圏のユーザーの個人データを米国に移転する際に十分な安全保護対策をとらなかったとして12億ユーロの罰金を科されたケース²など、注目を集めた事例では、コンプライアンス違反による経済面と評判への損失のリスクが浮き彫りになりました。

この課題の中心にあるのはデータ主権です。データ主権とは、データをどこに保存するか、どのようにアクセスするか、取り扱いの権限が誰にあるか、といった点をコントロールする能力です。EUや米国、その他の地域でも世界的に規制が強まる中、データ主権を確保することは、ますます重要になっています。組織は不正なアクセスからデータを保護すると同時に、増え続ける各地域の法規制を遵守しなければなりません。これは、データ保護の取り組みに対する内部の抵抗に直面することが多いCIO（最高情報責任者）や最高情報セキュリティ責任者（CISO）、最高コンプライアンス責任者にとっては、大きな課題です。

出典: 1. <https://www.enforcementtracker.com/?insights> 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Google Workspace の Assured Controls を使用すると、データを地域内でサイロ化するよう選択することが可能です。これにより組織は、データの処理と保存を行う場所をEUや米国などから選択でき、厳しい規制にも対応できるようになります。きめ細かい管理機能でデータを不正なアクセスから確実に保護しつつ、安全でシームレスなコラボレーションを促進できます。

このガイドでは、データを安全に保護しコンプライアンス上の課題に対応するための、実践的なロードマップを示します。現在の環境の評価や、高度なコントロールの実装など、複雑なデータ主権に対応していくために必要な知見とツールについて、ご紹介します。



国境を超えたコラボレーションが進む現在、データ主権の実現に向けて組織が取り組む必要があること:

- 01 データの保存と処理を行う場所をコントロールする。
- 02 認可されたユーザーのみがデータにアクセスできるようにする。



02

規制の強化



世界各国の政府は、個人情報を保護し、機密データが地域で管理されるようにするため、データ保護法の厳格化を進めています。こうした枠組みは、企業が情報を管理する方法を変え、コンプライアンスとイノベーションに関して新たな機会を生み出していますが、コンプライアンス違反にともなうリスクも上昇しています。





欧州連合: GDPR と EU AI 法

一般データ保護規則（GDPR）は、データ プライバシーに関する世界的な基準となっています。個人データの保存、処理、転送を行う方法に関し、特に欧州経済領域（EEA）以外で行う場合について厳密なコントロールを義務付けています。組織は、標準契約条項または同等の保護策など、十分な安全保護対策を実施し、コンプライアンスを徹底する必要があります。GDPR は、EU 市民への商品やサービスの提供や、EU 市民の行動のモニタリングを行う企業に適用され、事業拠点がどこにあるかは関係ありません。



欧州 AI 規制法（EU AI 法）は AI に関する世界初の法的枠組みで、欧州内での AI のリスクを制御し、信頼に足る AI の利用を促進する目的で制定されました。適用対象となるのは、事業拠点がどこであるかを問わず、EU 市場で AI の開発や導入を行うすべての企業です。EU AI 法では、AI システムを以下の 4 つのリスクレベルに分類しています。

許容されないリスク

市民の安全性と権利を脅かす AI アプリケーション（ソーシャル スコアリング、生体認証を用いた監視など）は、禁止されています。

高リスク

重要な分野の AI（医療、法執行機関など）は、リスク評価と人間による監視を含め、厳格な規制を遵守する必要があります。

透明性に関するリスク

チャットボットや生成 AI などの AI システムは、コンテンツが AI 生成されたものであることを明らかにする必要があります。

最小リスク、または リスクなし

低リスクの AI（迷惑メールフィルタ、AI 搭載のゲームなど）は、制限対象ではありません。



米国: HIPAA、CCPA、CDPA

米国には全国規模の統合されたデータ プライバシー法はありませんが、セクターや州ごとの規制でさまざまな義務が課されています。

HIPAA

医療機関、保険会社、その従業員に適用され、厳格なプライバシー保護とセキュリティ対策によって患者や加入者の個人情報を保護することを求めています。

CCPA（カリフォルニア州）

消費者に自身の個人データに対する権利を与え、個人データへのアクセスや削除、販売に関するオプトアウト権について定めています。一定の収益またはデータ量のしきい値を満たす企業に適用されます。

CDPA（バージニア州）

CCPA と同様、消費者のプライバシーを対象にしていますが、データの最小化と透明性が強調されています。

アジア太平洋: APPI と PIPA

01

日本の個人情報の保護に関する法律（APPI）：国境を超えるデータ移転に重点を置いた規制で、日本国民のデータを扱う際に同意または同等の保護を求めています。

02

韓国の個人情報保護法（PIPA）：国境を超えたデータ移転の制限など厳格な要件を適用し、違反に対しては重い罰則が科されます。

南アメリカ: ブラジルの LGPD

ブラジルの一般個人データ保護法（LGPD）は GDPR をモデルにして制定され、データ処理に厳格な同意を義務付け、違反者には重い罰則が科されます。ブラジル国民に関するデータを扱う企業を対象としています。



国境超えに伴う複雑さ

外国へデータを移転する際には、複数の枠組みを遵守する必要があります。

新たな要件

GDPR や LGPD といった法規制は継続的に変化しており、組織はコンプライアンスを確保するために適応が求められます。

セクターごとの差異

各種の規制は重なる部分もありますが、業種特有のリスクやニーズに応じて、適用の内容はさまざまです。

各種枠組みに 共通の課題

地域ごとの違いはあれ、企業は世界共通の課題に直面しています。

これらの枠組みはデータ主権の法的基盤を形成するものですが、その意味を最も痛感しているのは、機密データを扱っている業種です。以降のページでは、金融、医療、テクノロジーなどのセクターが、こうした固有の課題にどう取り組んでいるかご紹介します。



03

重圧に直面
する業種

データ主権の課題はすべての業種に同じように影響を及ぼすわけではありません。一部の業種では取り扱うデータの機密性が高く、一挙一動を制限する厳密な規制があるため、その影響は多大です。

金融、医療、政府機関、テクノロジーなどのセクターにとって、データ主権の実現とは、単にコンプライアンスの義務を果たすことではありません。重要なアセットを保護し、ステークホルダーとの信頼関係を構築し、複雑化する状況の中でシームレスかつ安全に運用を行えるようにするために必要なことなのです。

 共有

金融: 競争の激しい環境に おける信頼維持

金融機関は、顧客データの機密性や、世界経済における役割のために、常に厳しい目にさらされています。GDPRのような規制は、データの保存とアクセスに対してきめ細かな管理を要求しています。一方で、オープンバンキングの取り組みではイノベーション推進の目的で、顧客データをサードパーティのサービス提供者と安全に共有することが求められています。



シャーリー フランクリン

重要な考慮事項:

国境超えに伴う課題

複数の法域にまたがる金融データの管理にはリスクが伴います。特に規制要件が異なる地域間でデータの移動が発生場合はその傾向が強くなります。

レガシー システム

多くの銀行は旧式のインフラストラクチャを使用しており、その結果、高度な暗号化やロールベースのアクセスといった、現代のコンプライアンス対策の導入が複雑化しています。

評判低下のリスク

信頼が何よりも大切な業種では、一度のコンプライアンス違反が甚大な経済的損失やイメージの低下につながる場合があります。

きめ細かいアクセス制御や地域内でのデータ処理などのソリューションを実装することで、金融機関は自信を持ってコンプライアンス基準を満たしながら、顧客の信頼を守ることができます。



医療: プライバシーと進歩の兼ね合い

医療分野において、患者のプライバシー保護は法的義務であると同時に倫理的責務でもあります。命を救うための共同研究を行う一方で機密性の高い医療記録を保護するという、微妙なバランスの上で事業が運営されています。

重要な考慮事項:

複数の規制

医療機関は米国の HIPAA や欧州の GDPR など、複雑な多数の規制に対応する必要があり、これらの規制はデータの保存や暗号化、アクセスに関してそれぞれが独自の基準を設けています。

国境を超えたコラボレーション

研究機関は海外の機関とのデータ共有が必要になることが多く、コンプライアンスへの対応がさらに複雑になっています。たとえば、臨床試験のために匿名化された患者データを国を超えて共有するには、データ主権に関する地域の法律に従う必要があります。

運用の中断

システムが旧式であったりデータがサイロ化されていたりすると、効率が損なわれ、コンプライアンス監査の際のリスクも高くなります。

エンドツーエンドの暗号化やリアルタイムの監視ツールなど堅牢なデータ保護対策を実施することで、医療機関はコンプライアンスを遵守しながら、イノベーションとコラボレーションを推進することができます。

政府機関: 市民の信頼と 国家の安全を確保

政府機関は納税記録から国家安全保障情報まで、機密性の高い住民データを大量に管理しています。したがって侵害に伴うリスクは非常に高く、データの保護はコンプライアンス上の義務であるだけでなく、市民の信頼や国家安全保障の問題でもあります。

重要な考慮事項:

地政学的なリスク

政府機関はサイバー脅威や海外の攻撃者がもたらす圧力など固有の課題に直面しているため、データ所在地やデータ主権は極めて重要です。

透明性とセキュリティのバランス

オープン性と厳格なデータ制御の必要性の間でバランスを取ることは、市民の信頼を維持するうえで非常に重要です。

地域の法律

政府機関は欧州の GDPR や、データ ローカリゼーションを必要とする地域の規則など、重複する複数の規制を遵守する必要があります。

エンドツーエンドの暗号化や厳格なアクセス制御など、データ主権に関するツールを使用することで、公共部門の組織は透明性や運用効率を犠牲にすることなく、データを保護できます。



テクノロジー： 厳しい視線のもとでのイノベーション

テクノロジー企業はグローバル規模に拡張しながら、地域のコンプライアンスを遵守して、国境を超えた膨大なユーザーデータの処理を行っています。こうした企業にとって、データ所在地は単なるコンプライアンスの問題ではなく、知的財産を保護し、顧客の信頼を維持するために極めて重要なものです。

「データが地域内にとどまっていない場合や、データが他のテクノロジー プロバイダによって処理される場合、それはヨーロッパにとって、その国にとって、そしてエアバスにとってリスクとなります。それは決して許容できるリスクではありません。」

エアバス、Sebastien Aubineau 氏

重要な考慮事項:

世界への展開、現地の規則

エアバスのような企業は、機密情報を保護しデータ主権に関する規制を遵守するために、地域内でデータ処理を行うことの重要性を強調しています。

スケーラブルなソリューション

テクノロジー企業は、コンプライアンスを損ねることなくグローバルに展開できるようなシステムを実装する必要があります。

新たなリスク

急速な技術革新の結果、サードパーティのアプリケーションとの統合や不十分なアクセス制御によって、予測できない脆弱性が生まれることがあります。

きめ細かい管理と高度なセキュリティ対策は、テクノロジー企業のイノベーションや成長を抑制することなく、これら課題への対応を可能にします。



04

5 ステップの プラン



データ主権の実現に取り組むには、個別のニーズ、業種、地域に合わせた体系的なアプローチが必要です。このガイドでは、データ環境をコントロールし、規制を遵守し、組織のコンプライアンス戦略への信頼を醸成できるようにするための、5つの実践的なステップをご紹介します。

01

環境の評価

どこにデータが保存され、誰がアクセスでき、どの規制が適用されるかを把握します。これは、対応が不十分な箇所を特定するための出発点です。

02

データ リージョンの選択

規制要件に合わせてつつ、運用の柔軟性を維持できるように、データの保存と処理を行う地域を限定します。

03

アクセス制御の精緻化

権限を調整し、適切なデータに適切なユーザーのみがアクセスできるよう限定し、データの開示を最小限に抑えます。

04

データ保護の強化

セキュリティ対策を強化し機密データを保護することで、進化するサイバー脅威の一步先を行くようにします。

05

報告と監視

継続的なモニタリングと報告によってコンプライアンスを維持し、絶えず変化する規制の状況に積極的に対応できるようにします。



01

環境の評価

どのような取り組みも、現在の状況と目的とする状態を理解することが最初の一步です。

データ主権に対応するには、まず、業界を統制する外部の規制と、組織内のデータ環境の実際の状況を把握することから始めます。データがどこに保存されているか、アクセス方法はどのようなになっているか、コンプライアンスを満たすには何が必要かといった点を整理し、現在の状況に何が不足しているかを特定します。



ルールの把握

GDPR、ISO、SOC などのグローバルな枠組みは、コンプライアンスの基盤となります。ただしこれらの規制はそれ自体単独で存在しているわけではなく、組織の固有の運用との間で調整を行う必要があります。

GDPR (欧州)

標準契約条項のような十分な安全保護対策が設定されていない限り、データ所在地を厳密に欧州経済領域（EEA）内に限定するよう求めています。欧州に顧客を持つ組織にとっては、個人データがどこに保存され、どこに転送されるかを正確に把握しておくことが非常に重要です。

EU AI 法 (欧州連合)

欧州 AI 規制法は欧州連合の規制で、欧州連合域内において AI に対する共通規制の枠組みを確立することを目的としています。AI システムとモデルを異なるカテゴリに分類し、それぞれに異なる要件を課しています。2024 年 8 月 2 日に、欧州 AI 規制法は強制力を持つ法律として発効されました。

DORA (欧州連合)

DORA（デジタル オペレーショナル レジリエンス法）は、金融機関の IT セキュリティを強化するための技術標準を定めた規制です。欧州監督機構（ESA）が作成し、欧州委員会によって採択された DORA は、金融セクターと ICT サービスを提供するサードパーティを対象に、オペレーショナル レジリエンスに関する規則を統合しています。

SOC コンプライア ンス（米国）

SOC（Service Organization Control）レポートは、セキュリティ、可用性、機密性といった信頼の原則に関する基準を定めています。AICPA（米国公認会計士協会）が作成したこの基準を満たすには、厳格な内部監査と運用の透明性が必要で、特に米国に拠点を置く組織や、米国の法人と取引を行う組織を対象としています。

ISO 規格 (全世界)

国際標準化機構が管理する、世界的に認められた情報セキュリティ管理の枠組みを提供します。EU、米国、アジア太平洋地域で事業活動を行う多国籍企業が、一貫したセキュリティ ポリシーを確立するうえで重要な基準です。



内部データの監査

次のステップは内部が対象で、組織のデータ環境を調査します。データの保存場所、アクセスできるユーザー、現在のシステムに不足している点などの詳細を明らかにします。これらの項目を確認することは、コンプライアンス戦略の土台となります。

いくつか例を見てみます。

- 医療機関では、機密性の高い患者データが、暗号化レベルの異なる複数のクラウド サービスにまたがって保存されていることがあります。研究のために国境を超えたデータ共有を行っている場合、GDPR（欧州）や HIPAA（米国） へのコンプライアンスはさらに複雑になります。
- このようなケースでは、データ監査により、記録が暗号化されていない、アクセス権限が明確でない、といったリスクが明らかになることがあり、規制要件に適合するには対処が必要です。

こうした分析情報を外部の規制に照らし合わせることで、コンプライアンス上の義務と実際の運用の間にあるギャップを埋めることができます。





チームの結成

データ主権とは単なる技術的課題ではなく、他分野と協力して実現するものです。以下のような部門からのメンバーを含む適切なチームを構築することが不可欠です。

- **IT リーダー**: 技術インフラストラクチャの詳細を示し、暗号化や保存に関する不足部分に対処できます。
- **法務部門**: 地域の規制要件を解釈し、契約がコンプライアンス要件を反映していることを確認できます。
- **事業部門**: アクセス権限やワークフローの中断など、日常の業務に及ぼす実際の影響を特定できます。

このチームが協力し、組織内のプロセスをそれぞれの地域に応じて GDPR、SOC、ISO といった枠組みの要求と照らし合わせます。

プロアクティブな計画

規制は変化しており、ビジネスニーズも常に変化しています。これらのステップを実施することで、事後対応的なコンプライアンスから脱却し、将来の成長の助けとなる枠組みを構築できます。

たとえば、**Google Workspace の Assured Controls** のようなソリューションは、データ所在地とアクセスの要件に適合するための基盤を提供し、柔軟性を維持しながらコンプライアンスに対応できます。





データ所在地と アクセス制御

02

データ所在地には、単にデータがどこにあるかだけでなく、データの保存、アクセス、処理の方法を確実にコントロールし、同時にパフォーマンス、スケーラビリティ、コンプライアンスのバランスを取ることが関わってきます。

膨大な機密データを扱う組織にとっては、Google Workspace の Assured Controls のようなツールがあれば、業務を中断させずにコンプライアンス遵守を効率化することができます。

「当社はリージョン内データ処理について広範な分析を実施しました。これはスムーズに行われ、費用がかかる複雑なサードパーティ統合の必要性が軽減されました。また、不具合や遅延が起きたケースはなく、すべて順調に推移しています。」

Randstad、グローバル コラボレーション
担当プロダクト オーナー、Roman
Spantgar 氏

データ所在地の限定と柔軟性の両立

多くの組織にとって課題となるのは、厳格なデータ所在地の要件への適合と、運用のアジリティの維持の間に適切なバランスを取ることです。たとえば、グローバルに拡大している組織の多くは、各地域の規制とパフォーマンス上のニーズの両方に対応しなければなりません。

その結果、ジレンマが生じることがよくあります。コラボレーションを妨げるシステムのサイロ化を回避しながらコンプライアンスを確保するには、どうすればよいでしょうか。

Google Workspace の Assured Controls を使用すれば、きめ細かく柔軟にデータの保存と処理を行う場所を定義でき、同時にクラウドのスケラビリティは維持できるため、この問題に対処できます。これにより、多国籍企業は個別のチーム、部門、地域に応じてデータ所在地のポリシーを設定でき、パフォーマンスを損ねることがありません。

データ処理: 保存のその先へ

多くの組織において、データの保存場所は重視している一方で、処理を行う場所については見過ごしているケースがあります。データ処理の場所も、GDPR のような枠組みではコンプライアンスの重要な要素となっています。データ処理とはどのようにデータを使用し、分析し、共有するかを指し、多くは単なる保存よりも監視が必要になります。Assured Controls はデータの保存に対応するだけではありません。Assured Controls はデータの保存と処理のローカリゼーションを可能にするため、組織がエンドツーエンドでデータ主権の要件に対応できるようになります。





米国の医療関連の コンプライアンスへの対応

米国では、HIPAAのような全米対象の法規制で、患者データの保護に関する米国全体の基準が定められていますが、州法が存在することで複雑さが増しています。カリフォルニア州のCCPAやバージニア州のCDPAなどの規制は、データプライバシー、消費者の権利、保持期間に関してより厳しい要件を規定しています。データ処理のローカリゼーションによって、医療機関はこのような複数の規制が重なる状況に自信を持って対応できます。

変化する規制要件への将来の備え

データ主権の内容は頻繁に変化しています。各国政府は既存の規制の改正や、新たな規制の導入を継続的に行っており、これが企業にとっては不確実な要素となっています。現時点の規則を満たすために融通が利かないシステムを設計すると、近い将来には新たな規則への対応に悩まされる可能性があります。Google WorkspaceのAssured Controlsでは、規制要件の変化に合わせてデータ所在地のポリシーを柔軟に調整することが可能です。そのために行うのが地域間でのデータの移行であっても、アクセス制御の精緻化であっても、その目的は、データ主権の状況が変化に後れを取らないようにすることです。





03

アクセス制御の精緻化

データを安全に保存したら、次のステップでは、データへのアクセスも同じく保護されていることを確認します。最小権限の原則を適用することで、機密情報へのアクセス権を、正当にその情報を必要とするユーザーのみに付与することができます。誰が何を閲覧できるかを絞り込むことで、偶発的な漏洩や組織内の不正使用、サードパーティの脆弱性などによるリスクを減らすことができます。

アクセス制御が重要な理由

現在の環境では、データへのアクセスを制限しないことによるリスクが増大しています。組織内での過剰な権限付与は漏洩やミスのリスクを増やし、サードパーティによるアクセスはコンプライアンスを複雑化します。また、GDPR、HIPAA、その他の規制は、誰が機密情報にアクセスできるかについて、厳しい監視を求めています。



アクセスを絞るには

適切なツールがあれば、より効率的で安全なアクセスポリシーを適用することが可能です。



ゼロトラスト フレームワーク

「誰も信用せず、すべてを検証する」という考えに基づき、すべてのユーザー、デバイス、接続について認証と認可の手続きを実施します。これは組織内のユーザーについても同じです。

ロールベース アクセス 制御 (RBAC)

権限を特定のロールに限定することで、不要なリスクを抑えることができます。いくつか例を見てみます。

- 金融チームは決済システムにアクセスできますが、人事記録にはアクセスできません。
- 医療従事者は患者の治療データを閲覧できますが、管理部門のファイルは閲覧できません。
- サポートチームがデータにアクセスできるのは、明確な承認を得た場合のみで、時間も限られます。

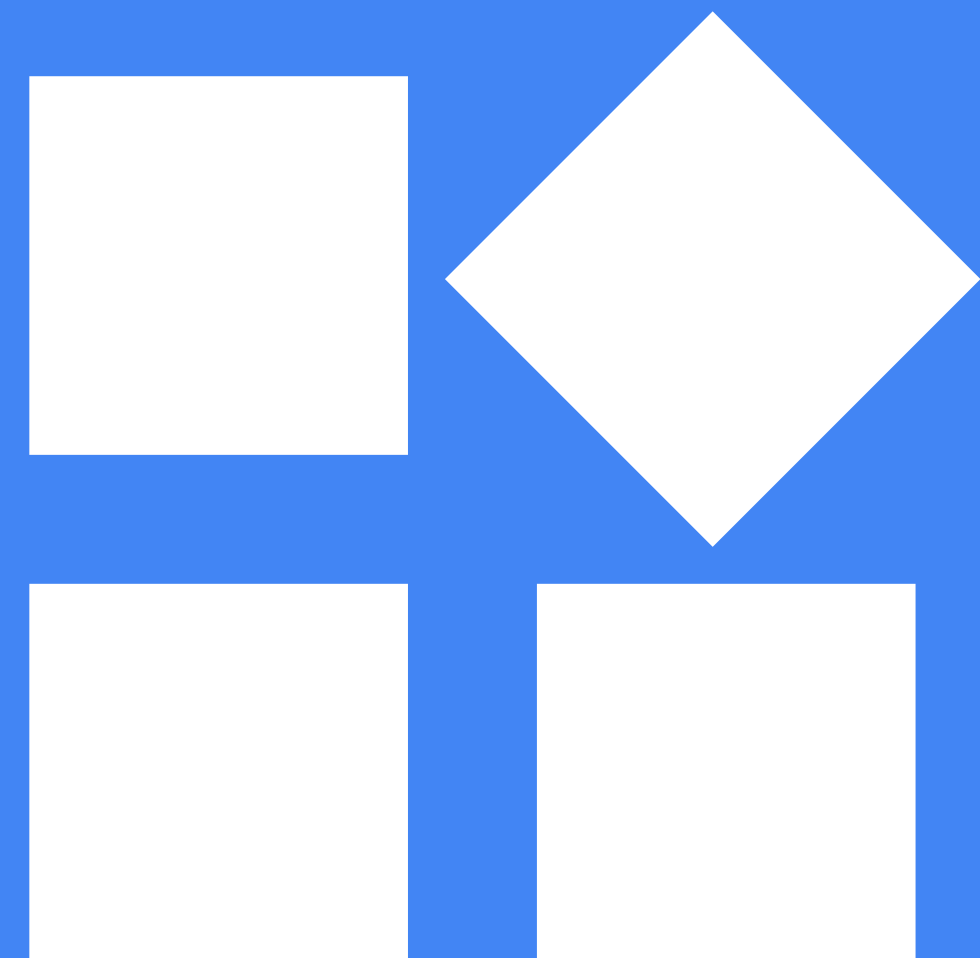
アクセスの透明性と 承認

サードパーティのアクセスに対して、明確な認可を必要とするワークフローを実装します。Google Workspace のアクセス承認機能のようなツールを使用すると、絶対に必要な場合のみサポートチームがデータにアクセスできるように設定するなど、完全な可視性とコントロールが得られます。

クライアントサイド 暗号化

セキュリティ対策の層を1つ増やすことで、組織は自身の暗号鍵を管理でき、クラウドプロバイダに対しても機密データへのアクセスを防止できます。

精緻なアクセス制御を実装することで、セキュリティおよびコンプライアンスと、コラボレーションの多い現代の職場ニーズとの間でバランスを取ることができます。次のステップでは、セキュリティ対策の強化によって、どのようにリスクが減り、新たなサイバー脅威の先に行くことができるかについて見ていきます。

**共有**

アクセス制限はセキュリティだけでなく、運用効率を上げる点でも重要です。

パフォーマンス:

エンドユーザーの近くにデータを保存すれば、遅延が減って生産性が向上し、チームがどこにいてもシームレスに作業できます。

コンプライアンス:

データを地域内に保存することで法的リスクを回避でき、GDPR や HIPAA などの枠組みやその他の新たな規制を確実に遵守できます。



セキュリティと データ損失防止 (DLP)

04

データを安全に保存し、アクセス制御を精緻化したら、次の重要なステップは、新たな脅威から組織を守ることです。Google Workspace の Assured Controls は、高度なクライアントサイド暗号化、きめ細かいアクセス制御、堅牢な DLP（データ損失防止）ツールを提供し、保存中、転送中、使用中にかかわらず、すべての段階でデータの安全性を確保します。





Assured Controls が重要な理由

現代の組織は、ますます複雑化するセキュリティ上の課題に直面しています。

- **外部の脅威:** フィッシング攻撃、マルウェア、不正アクセスの試みは、ますます高度化しています。機密情報を不正な行為者から保護するために、組織はプロアクティブな対策を必要としています。
- **内部のリスク:** 過剰な権限付与、偶発的な共有、ヒューマンエラーは、現在でもデータ侵害の主要な原因です。アクセスを限定し、技術的な安全対策を組み込むことで、このような脆弱性を軽減することが可能になります。

ブラウザ拡張機能や生産性向上アプリ、サードパーティ統合など、従業員が日常的に使用するツールから、意図しない脆弱性が生じることがあります。十分な検証を受けていないアプリでの機密データ共有、権限を越えたアクセス、悪質なソフトウェアなどのリスクは、セキュリティ ポスチャーをさらに複雑化します。

では、重要なデータを保護しつつ、従業員が必要なツールを使ってシームレスに作業できるようにするには、どうすればよいでしょうか。

Google Workspace の Assured Controls を使用すれば、以下のような機能で柔軟性とセキュリティのバランスを取ることが可能です。

- **きめ細かい権限:** サードパーティ ツールがアクセスできる対象を制限し、機密データをアクセス不可にして、不要なリスクを減らします。
- **クライアントサイド暗号化:** 従業員が複数のクラウド サービスにまたがって連携作業を行う場合も、データをエンドツーエンドに保護します。暗号化により、許可されていないアプリやサービスは機密情報を読み取ることができません。
- **可視化と承認:** どのツールが使用されているかを継続的に監視し、潜在的なリスクを早期に特定し、外部からのアクセスは本当に必要な場合のみ承認します。

Assured Controls はこれらのコントロールを組み込むことで、セキュリティに重点を置きながら、従業員は窮屈さを感じずにイノベーションに集中できます。ツールが障害をおよぼすことを防ぎつつ、その有用性を維持することができるのです。

複数の防御層の追加

Assured Controls はまた、ゼロトラスト フレームワークとシームレスに統合します。「誰も信用せず、すべてを検証する」という考えを導入し、すべてのユーザー、デバイス、接続が、機密データにアクセスするには自身の認証情報を証明する必要があります。

共有の前にファイルを暗号化し、サードパーティからのアクセスには複数の承認を求めるなど、こうした技術的コントロールにより、常にプロアクティブなセキュリティ対策を実施できます。





DLP が重要な理由

データ損失防止（DLP）ポリシーは、セキュリティ ポスチャの強化に重要な役割を担います。これにより以下のことが可能です。

- **データの動きを監視:** 機密データのシステム内での移動を追跡し、漏洩や不正な共有を特定して対処します。
- **カスタム ポリシーの設定:** コンプライアンス上の義務に違反するデータ共有について自動的にブロック、アラート生成、報告を行うルールを定義します。
- **機密性の高いカテゴリの保護:** 個人を特定できる情報（PII）、金融データ、知的財産など、特定のデータタイプを識別し保護します。



セキュリティはしばしば、コラボレーションにとって余分な障害だとみなされますが、実際には、組織が確信を持って事業を行ううえでの裏付けとなります。Assured Controls の高度な暗号化、プロアクティブな DLP ポリシー、承認プロセスを利用することで、組織は機密データの保護と、コラボレーションの実現の間に適切なバランスを取ることができます。

次のセクションでは、変化し続ける規制環境でコンプライアンスを維持してプロアクティブな対応を続けるために、報告と監視がどう役立つかについて見ていきます。



報告と監視: 可視化による自信

05

データ主権への取り組みは、コントロールが導入されたら終わりではありません。そのコントロールが機能することを証明する必要があります。報告と監視は、組織におけるデータ戦略のモニタリング、監査、調整を可能にします。暗号化、アクセス、ストレージを継続的に可視化することで、コンプライアンスが達成されただけでなく、維持されていることを確認できます。Randstad のような企業は、リアルタイム報告ツールによって監査を簡素化し、シームレスにコンプライアンスを確保しています。

Google Workspace

「データ リージョンの実装は、EU の個人データ処理に関する戦略を進化させるうえで、変革的ステップとなりました。プロセスは非常にスムーズで、運用の中断は起きていません」

Randstad、グローバル コラボレーション担当
プロダクト オーナー、Roman Spantgar 氏



報告を、コントロールの層が積み重なったピラミッドのようなものだと考えてみましょう。
それぞれの層で信頼が構築されたシステムです。

クライアントサイド暗号化:

暗号化はセキュリティの基本です。ただし暗号化が機能するのは、一貫して適用されている場合のみです。報告ツールによって、機密データが作成時から保存中までエンドツーエンドに暗号化されていることを確認できます。また、監査証跡により、暗号鍵がコントロールされていることを確認できます。

コンテキストアウェア アクセス:

データアクセスはコントロールするだけでなく、監視する必要があります。リアルタイムの報告により、通常とは異なるアクセス場所、ログイン試行の失敗、時間外のアクセスなど、異常が明らかになります。こうした可視化を行うことで、リスクがインシデントに発展する前に対処できます。

きめ細かいアクセス制御:

監視ツールにより、誰が何に、いつ、どのような理由でアクセス権を有しているかを確認できます。明確なアクセス記録と報告を生成することで、過剰な権限を付与されたロールの特定、一時的なアクセス（サポートチーム対象など）の監視、GDPR や HIPAA などの枠組みへのコンプライアンス維持が可能になります。

ローカル データ ストレージ:

厳格なデータ所在地の要件がある業種では、透明性が非常に重要です。報告ツールによって、データがあるべき場所（特定の州や地域など）に保存され続けていることを確認できます。これにより、IT チームと規制機関の両方に、必要な証明を提供できます。

データ リージョン:

新たな市場への進出をお考えの場合もあるでしょう。報告ダッシュボードは、データの保存、処理、アクセスの場所を明確に示します。これにより、規制要件が変化したり事業がグローバルに拡大したりしても、ポリシーを調整することができます。

ゼロトラスト アーキテクチャ:

ゼロトラストでは仮定を排除し、常に検証を行います。報告ツールはすべてのアクセス要求、デバイス、ユーザー操作を記録します。これにより、データポリシーが遵守されていることを確認でき、アクティビティの監視と不審なパターンの検出を容易に行えます。



可視化が重要な理由

堅牢な報告ツールなしでは、コンプライアンスが当て推量になってしまいます。組織は規制要件への適合を証明しつつ、新たな脅威に対応するのに十分なアジリティを維持しなければなりません。Google Workspace の Assured Controls は、モニタリングと検証を行い、自信を持ってデータ戦略を適応させるために必要な監視ツールを提供します。

- **監査の簡素化:** GDPR、HIPAA、SOC 2 などの枠組みに沿った、コンプライアンスに対応した報告を生成します。Assured Controls を使用すると、IT チームやコンプライアンス チームの報告作業が効率化され、クリック 1 つですべてのデータ アクティビティの詳細な監査ログを表示できます。
- **コントロールの維持:** リアルタイムのダッシュボードがリスクを早期に表示し、透明性の高いアクティビティ ログがすべてのアクション、承認、変更を追跡します。これにより、リスクに対応し、ガバナンスを証明し、信頼を維持するために必要な可視性を確保できます。

リアルタイムの分析情報、監査に対応した報告、透明性の高いアクティビティ ログを提供する Assured Controls は、コンプライアンスの遵守だけでなく、その先を行くために役立ちます。モニタリング、検証、適応のためのツールを使用することで、組織はデータに対するコントロールを自信を持って示すことができ、また、盲点や新たな脅威などのリスクを軽減できます。

強力な報告ツールがあれば、コンプライアンスは果たさなければならない単なる義務ではなく、戦略的優位性になります。アクティビティのモニタリング、コントロールの検証、プロアクティブな対応のためのツールを活用することで、組織は新たなリスクや規制に自信を持って適応し、信頼を醸成できます。





05

まとめ



Google Workspace の Assured Controls

Assured Controls を使用すると、最先端のコンプライアンス ツールと、クラウドの柔軟性やスケーラビリティを組み合わせ、最小限の労力でデータ主権の実現に近づくことができます。Assured Controls が提供するデータの保存、処理、アクセスに対するきめ細かい管理機能は、変化する規制に適応できるよう備えるためにも役立ちます。航空宇宙産業の知的財産の保護でも、金融機関の機密性の高い顧客データの管理でも、Assured Controls は組織がコラボレーション、成長、イノベーションに集中できるようサポートします。

[詳細 →](#)