W. L. Gore & Associates

データ保護アプローチ

データ保護と情報セキュリティに対する私たちのコミットメント

私たちは、独自の価値ある製品とサービスを迅速に生み出すため、業界のトップイノベーターとパートナーとなり、インテグリティー、イノベーション、根拠に基づく科学を礎として日々邁進しています。それぞれのインタラクションにおいて、卓越したエクスペリエンスを創出し、また私たちのプロミス ***Together, improving life*** を実現するために、私たちは一丸となって取り組んでいます。

プロミスを果たすために私たちは、一人ひとりの説明責任、フェアネス、健全なグローバルビジネス実践への取り組みを通じて、高い倫理観とインテグリティーという当社のレガシーを維持するよう意識的に努めてきました。そして、私たちはこのプロミスを、当社が扱うデータ（個人情報、知的財産、機密情報等）を保護するというコミットメントを通じて実現します。私たちは、このコミットメントの遂行が可能となるよう、データプライバシーと情報セキュリティに関連する広範な機能を開発し実現しています。

概要

データプライバシー

私たちは、当社に委ねられた個人情報を管理、保護する方法の基礎となるプライバシー原則に従うことにより、私たちのプライバシーへの取り組みを示します。

ゴアのグローバルプライバシープログラムには、適用されるプライバシー保護法令を私たちがグローバルで遵守していることを実証する一連のプログラムポリシー、要件、サポートメカニズムが含まれています

PRIVACY

SECURITY

情報セキュリティ

情報資産の機密性、完全性、可用性、回復力を実現するために、ゴアの情報セキュリティプログラムは、業界標準のセキュリティフレームワークに基づく内部統制を実装しています。

情報セキュリティプログラムの基礎となる原則は、当社に委ねられたデータの管理人としての責任を喚起することを目的としています。

GORE

私たちの原則

プライバシー原則

- 説明責任:　適用されるプライバシー要件を満たしていることについての説明責任
- 適法性:　個人情報は適法で公正な方法によって処理されなければならない
- 同意:　必要な場合には本人から許可を得なければならない
- データの移転:　本人に提供した通知内容と一致していなければならない
- データ品質:　個人情報は正確でなければならない
- 具体的な目的:　個人情報は具体的かつ明確な目的に限定して処理されなければならない
- データの最小化:　必要とされる個人情報のみが収集、処理されなければならない
- セキュリティ:　個人情報は、適切な安全管理措置（技術的・組織的・物理的・人的）によって保護されなければならない

情報セキュリティ原則

- 説明責任:　適用されるサイバーセキュリティ法令を順守していることについての説明責任
- 適法性:　適用法の順守
- リスクベース:　特定のリスクに適したセキュリティコントロールの適用
- セキュリティバイデザイン:　ソフトウエア開発ライフサイクル(SDLC)期間にわたるセキュリティコントロール
- 多重防護:　複数レベルの保護を確保する階層型セキュリティコントロール
- アラインメント:　業界のサイバーセキュリティフレームワークおよびベストプラクティスと一致したインフォメーションセキュリティプログラム
- 責任:　センシティブ情報や機密情報の適切な取扱いに必要な意識向上トレーニングを、アソシエートやパートナーに対して提供

データプライバシーと情報セキュリティに対する私たちの取組みはどのようなものですか？

グローバルデータプライバシープログラムのキーポイント

- 特定の役割と責務をもってグローバルプライバシープログラムを管理運営するプライバシーオフィスの設置
- 個人情報を管理・保護するための適切な措置を義務付ける方針と手続の策定
- プライバシー保護の企業文化を育成するためのプライバシートレーニングおよび啓発プログラム
- システムやアプリケーションの開発ライフサイクルにおける「プライバシー・バイ・デザイン」のアプローチ
- どこでどのように個人情報が処理されるかに関するデータインベントリーの文書化
- 個人情報を収集、処理する際の事前通知や同意取得の実施管理
- 情報主体が自身のデータに対して適切なコントロールを有するようにする個人の権利の確保
- プライバシーリスクおよび関連するリスク緩和プロセスを評価するためのプライバシー影響評価とデータ保護影響評価
- 第三者のプライバシーリスク管理および越境データ移転の管理
- プライバシー侵害事案対応のプロセスおよび手順

グローバル情報セキュリティプログラムのキーポイント

- 最小権限の原則に基づくユーザーのロールと権限
- マルチファクター認証でのアクセスによる VPN 経由のリモートアクセス
- 一元化されたユーザーアカウントの管理と認証
- 監査ログとイベントログのレビューによるインフラストラクチャテクノロジーの監視
- リスクベース手法を用いたサードパーティ評価
- 現地法に適合する業界標準の暗号化ソリューションの使用
- 可能な限りの保管時および輸送時の情報資産の暗号化
- ルーチンパッチおよび脆弱性管理のための確立された手順
- 承認されたメディアデバイスのみからの情報資産へのアクセス制限
- サイバーセキュリティインシデント対応チームの対応プロセスと手順
- 異なるタイプの攻撃を特定して防御する侵入検知防止テクノロジー
- セキュリティ要件に基づくネットワークの論理的および物理的分離
- 新しいシグネチャリリースの更新がされたベンダー提供のマルウェア対策ソフトウエア

詳しくは当社ホームページの Privacy Notice をご参照ください。質問のある場合は、サイト上の「お問い合わせ（Contact Us）」から、または dataprivacyoffice@wlgore.com にメールをお送りください。当社の情報セキュリティプログラムに関して質問がある場合は、Gore_Information_Security_Team@wlgore.com にメールをお送りください。