Protecting your data

データ保護と情報セキュリティに対するEYのアプローチ

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

EYでは、ビジネスが高く評価されるには、強固なデータ保護と情報セキュリティプログラムにかかっていると考えています。データ保護と情報セキュリティが、ビジネスを行う上での根本的な基盤であるというのが**EY**の考えです。そのため、情報資産、個人データ、及びクライアント情報の保護に責任を持って取り組んでいます。確かなデータ保護と情報セキュリティプログラムは、一流のプロフェッショナルサービスに不可欠な要素であると考えます。本書の目的は、データ保護と情報セキュリティに向けた**EY**の取り組みを取りまとめて提示することであり、どのようにクライアント情報を保護するのか、また、それがどのように情報システムによりサポートされるのかについての概要を説明することです。これらの対策の具体的な内容は、実施するサービスや適用される国の規制要件によって異なる場合があります。**EY**のデータ保護及び情報セキュリティプログラムと実践は、機密性、完全性、可用性を維持しつつ、情報を適切かつ適法に取り扱うことに重点を置いています。

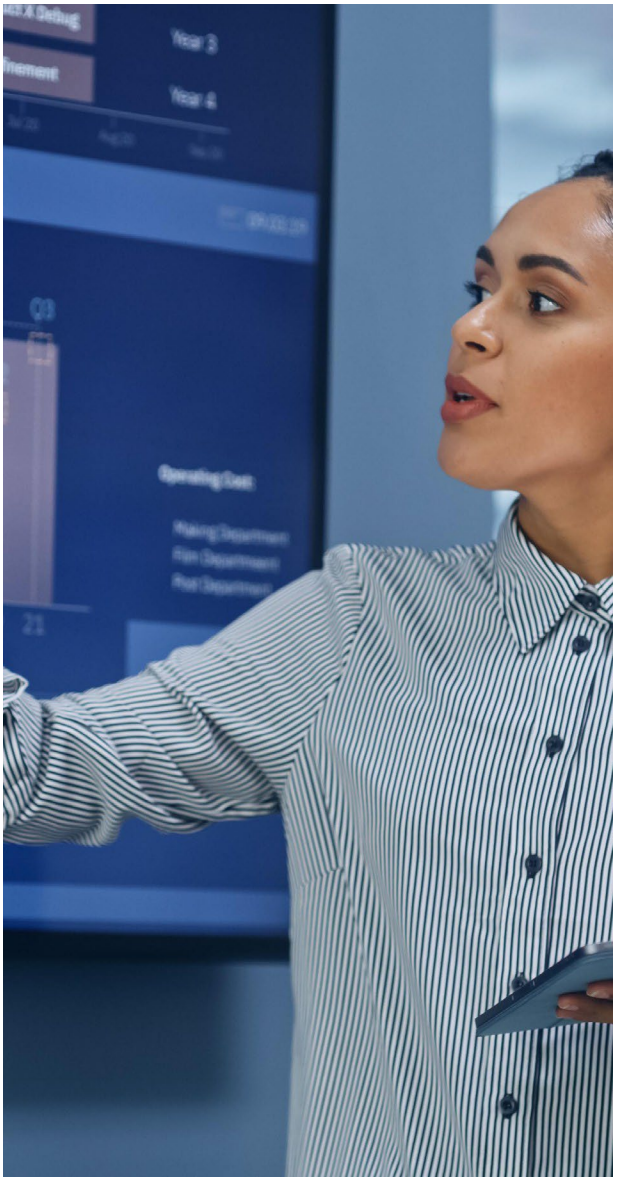
明瞭な情報セキュリティとデータ保護戦略

シームレスで一貫性のあるより高品質のクライアントサービスを世界中に提供するEYの能力は、明瞭なデータ保護と情報セキュリティ戦略によって支えられています。EYは、情報資産、個人データ、及びクライアント情報を、作成、処理、送信、または保存するときには、いつどこであってもそれらを保護します。また、EYは効果的なガバナンスを維持するとともに、適用される国内及び国際的な規制基準へのコンプライアンスを維持し続けます。EYのデータ保護及び情報セキュリティプログラムは、グローバルデータ保護チームとグローバル情報セキュリティチームという2つのグループが連携し、管理することによって実装されています。その使命は、EYの組織やクライアントの情報資産を、不正な収集、保持、使用、開示、変更、または破壊から保護することです。これは、適切なポリシー、スタンダード、ガイドライン及び関連する手順、技術的及び管理的なコントロール、並びに継続的なトレーニングと意識向上プログラムの取り組みによって達成されます。EYのグローバルデータ保護チームとグローバル情報セキュリティチームの連携は、EYが組織内で世界的に実施している世界共通の優先事項の下で行われています。これにより、EYの情報資産、個人データ、及びクライアント情報の保護に関する統一されたビジョンが提供されます。

EYのデータ保護フレームワーク

EYのデータ保護フレームワークは、関連する法律の原則（EU一般データ保護規則（GDPR）を含む）、その他の規制要件、及び関連する職業的専門家基準に基づいています。これは、以下の原則に基づき、個人データ及び機密データ（クライアントデータを含む）を保護するというEYのメンバーファームのコミットメントを示すものです。

- 適法性、公平性、透明性: 倫理的、合理的、明確に伝達され、合法的な方法でデータを使用します。
- 目的の限定: 定義及び承認された用途にのみデータを使用します。
- データの最小化: 目的に必要な量以上のデータを収集して処理しません。
- 正確性: データが正確であり、提案された目的に対して十分な品質であることを確認します。
- 保存の制限: 収集された目的を達成するために必要な期間のみデータを保持します。
- 完全性及び機密性: データの安全性及び機密性が保たれ、アクセスが厳格な「need to know」に基づいてコントロールされていることを確認します。
- アカウンタビリティ: EYのGlobal Data Protection&Confidentialityポリシー及び行動規範に従って、データ保護の原則を遵守していることを実証できるようにします。
- 機密情報: 機密性の高い個人データまたは機密性の高いクライアント情報を処理する際には、より慎重に取り扱います。
- サードパーティ処理者: EYに代わって個人データまたはクライアントデータを含む機密データを処理するサードパーティが、当該データを適切に保護するデータ保護フレームワークを採用していること、及び当該サードパーティとの契約に、適用法令に従ったデータ保護条例が含まれていることを確認しています。



EYのデータ保護フレームワークの要素

国際的なデータ移転

個人データの国際的な移転は、主要なデータ保護法及び規制（**欧州のデータ保護法など**）によって厳格に規制されています。世界各国のさまざまなデータ保護法は、個人データを移転する組織が適切な保護手段を実装していない限り、海外への個人データの移転を禁止しています。**EY**は、データ保護法に準拠するため、承認された、データ移転方法を使用しています。また、欧州連合司法裁判所（**CJEU**）が**Schrems II**において、欧州の個人データを欧州経済領域（**EEA**）以外の国に移転する際に、データ保護に対する包括的な立法アプローチをとらない場合は、個人のデータプライバシー権に適切なレベルの保護をしているとは見なされないという判決を下したことに、**EY**は留意しています。

- **EY**は、現地の法令や通例に基づいてデータ移転の影響評価を実施します。これには、必要に応じて個人データの適切な保護を検証するための適切な補完的措置が含まれます。
- **EY**は、**EY**のメンバーファーム間における個人データの国際移転を可能にするためのメカニズムとして、コントローラー及びプロセッサーの活動に対する拘束的企業準則（**BCR**）の確立を促進してきました。**BCR**により、**EY**はメンバーファーム内で個人データをシームレスに移転し、サービスラインを超えたチーミングを促進することができます。これらの**BCR**は世界中の**EY**のファームに適用されており、**EY**のウェブサイト（https://www.ey.com/ja_jp/legal-and-privacy/data-protection-binding-corporate-rules-program）で公開されています。
- **EY**のメンバーファームは、必要に応じて、承認された標準契約条項（**SCC**）をクライアント及び第三者との契約において利用します。
- **Ernst & Young LLP**（米国）及びその米国関連会社は、**EU**米国データ・プライバシー枠組み、**EU**米国データ・プライバシー枠組みの英国への拡張、及びスイス米国データ・プライバシー枠組みを遵守しています。詳細については、Ernst & Young LLP EU-US Data Privacy Framework Privacy Statementをご覧ください。

責任あるAI

エマージングテクノロジー、特に人工知能（**AI**）はかつてない成長を遂げており、計り知れない変革の可能性を秘めています。しかし、この急速な発展は、新たな法規制への対応、データ保護リスクの増加、倫理的な配慮、そして強固な**AI**ガバナンスの構築といった課題を伴います。これには、法令及び規制上の新たな要件、データ保護リスクの増加、倫理的な考慮事項、そして堅牢な**AI**ガバナンスフレームワークの必要性が含まれます。データ保護は、**EY**の責任ある**AI**フレームワークにおいて不可欠な要素であり、単なるコンプライアンスを超えて、**AI**の設計、開発、及び利用の基盤にデータ保護の原則を組み込むことを意味します。**EY**は、**AI**技術における個人データ及び機密データ（クライアントデータを含む）の責任ある利用にコミットしており、**AI**システムと関連データの利用、管理に適用される法律、規制、及び職業的専門家基準に従っています。詳細については、EYのResponsible AI principles（責任あるAI原則）をご覧ください。

EYのグローバルなデータ保護と情報セキュリティの優先事項を連携させることにより、情報資産、個人データ、クライアント情報の保護に関する統一されたビジョンを提供します。

トレーニングと意識向上プログラム

新しい技術が登場し、攻撃手法が変化する中で、EYのメンバーに提供する情報、ガイダンス、トレーニングも進化させる必要があります。AIを含む新しい技術を責任を持って活用し、変化する法律、規制、及び職業的専門家基準に準拠できるよう、データ保護や情報セキュリティに対する脅威についての認識を高めることは、継続的かつ動的なプロセスです。これは、EYが非常に真剣に取り組んでいることであり、EYの各サービスラインのプロフェッショナルに対して定期的に更新される必須トレーニングだけでなく、EYの全世界のメンバーの意識を高めるためのその他多くの活動にも反映されています。

EYグローバル情報セキュリティポリシー

私たちの情報セキュリティポリシーとそれをサポートするスタンダード及びコントロールは、継続的に精査され、内容がタイムリーかつ正確であり、私たちに適用される法的要件及び規制要件に関連づけられていることを確認しています。ISO 27001などの認定されたフレームワークに沿って、必須及び推奨されるポリシーステートメントは、以下を含む広く認識されている十数の情報セキュリティ領域（ただしこれらに限定されません。）に及んでいます。

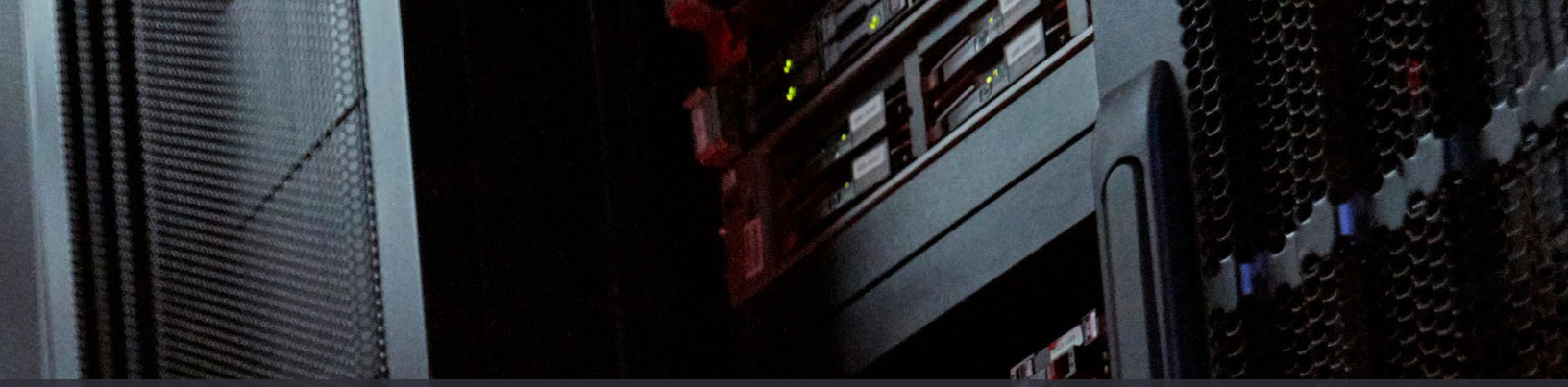
- ID及びアクセス管理
- 資産管理：分類と管理
- 通信、ネットワーク及びオペレーションのセキュリティ
- 人的セキュリティ：社員
- 情報セキュリティの取得、開発及び保守
- 物理的・環境的セキュリティ
- リスクマネジメント

技術的セキュリティコントロール

情報セキュリティに対するEYのアプローチは、書面化されたセキュリティポリシーやスタンダードのみに依拠するものではありません。また、EYはテクノロジーリソースと資産を保護することにより、情報の機密性、完全性、及び可用性を維持します。対策には、以下が含まれますが、これに限定されません。

- パソコンのフルディスク暗号化
- パソコンのファイアウォール
- リムーバブルメディア：書き込みは原則ブロックされ、許可された場合のみ、暗号化して書き込みができる
- ウイルス対策とマルウェア対策ソフトウェア
- 多要素認証ソリューション
- 自動パッチ適用とセキュリティの脆弱性評価
- 強力な物理的・環境的・ネットワーク的・境界的制御
- 侵入検知と防止テクノロジー
- 監視及び検出システム

加えて、将来のセキュリティ技術にも多大な時間とリソースを投資しています。情報セキュリティ戦略をテクノロジー製品のロードマップに合わせ、テクノロジーサービスの提供との密接な関係を維持しています。これにより、テクノロジーリソースの機密性、完全性、または可用性を脅かす可能性のあるセキュリティの問題に適切に対処できるようになります。



グローバル行動規範

EYは、プロフェッショナルとして適用可能な専門的及び技術的スタンダードに従って行動し、EYグローバル行動規範を遵守することをメンバーに義務付けています。これらの原則は、EYのウェブサイト(https://www.ey.com/en_gl/about-us/global-code-of-conduct)で一般に公開されており、世界中の全てのメンバーファームに適用される拘束力のある原則を表しています。EYグローバル行動規範は、広範な行動と倫理的なフレームワークに基づいており、個々の役割、ポジション、所属するメンバーファームに関係なく、全てのEYのメンバーが毎日行う判断における指針となります。プロフェッショナルとして、EYの組織、EYのメンバー、EYのクライアント、またはサードパーティから取得した、またはそれに関連する個人情報及び機密情報を尊重し、保護することが求められています。

情報セキュリティ

事業継続と災害復旧

組織とクライアントのデータ保護に対するEYの継続的な取り組みは、ISO 22301に沿って、災害復旧と事業継続の能力を通じて実証されています。EYは、大災害が起こる前からその後までを通して、EYのメンバー、施設、インフラストラクチャ、ビジネスプロセス、アプリケーション、及びデータを保護することに取り組んでいます。EYの重要なサービスであるアプリケーションに対する災害対応とシステム回復手段は、慎重に計画され、テストされています。EYの災害復旧と事業継続の方法論には、以下が組み込まれています。

- ビジネスへの影響評価
- 業界標準に基づいて構築された災害復旧計画
- 災害復旧と事業継続の認定プランナーによるサポート
- 運用の準備状況を検証するための災害復旧と事業継続計画の定期的なテスト

サプライヤー・リスク・アシュアランス・プログラム

このプログラムは、サプライヤー・マネジメント・デューデリジェンス・プロセスと連携し、以下の情報セキュリティ、調達、契約、データ保護、及び独立性に関連するサードパーティの活動も対象とします。

- ISO 27001/2に整合したグローバルポリシーとコントロールに準拠しているかどうかについて新規サプライヤーを評価
- リスク評価と指摘事項の準備を含むデューデリジェンスレビュー
- 指摘されたリスクの低減
- サプライヤー選定と契約交渉のサポート

EYは、業界標準のセキュリティ評価を用いて、情報セキュリティ、コンプライアンス、及びデータの分類、データの所在、アクセス、データ送信の種類など、その他のリスクカテゴリーにおける固有リスクと残存リスクを評価しています。

セキュリティ戦略及びその考え方

EYの多面的なセキュリティプログラムは、情報セキュリティと個人の行動に関する世界中のポリシーによって支えられています。これは、EYの個人の情報資産及びクライアントの情報資産の機密性、完全性、及び可用性を促進するように設計されています。EYは、適用される個人情報保護に関する法令と規制要件に準拠するだけでなく、情報セキュリティマネジメントシステム（ISMS）を確立、実施、維持、及び継続的な改善のためにISO 27001フレームワークを利用しています。

EYは、ISO 27001/2に基づいた情報セキュリティプログラムを通じて、機密情報や個人情報の保護と適切な管理を積極的に行っており、これには以下のようなものがあります。

- 適切なポリシーやスタンダード、ガイドライン、及びプログラム管理
- 強力な技術的セキュリティコントロール
- セキュリティレビュー、認証及び監査を含むセキュリティコンプライアンスプログラム
- 以下を考慮した、明確に定義されたセキュリティ戦略とロードマップ：
  - データ保護：法律上、規制上及び手続き上の要件
  - ビジネス：義務化された手順と要件
  - テクノロジー：ポリシー、スタンダード及び手順
  - 外部からの脅威：セキュリティ脅威の状況の変化
- サイバーディフェンスのための重大な脆弱性対応プログラムを含む、セキュリティ関連のインシデントを効果的に管理及び修正するためのセキュリティインシデント管理プログラム

コンプライアンスと監査

EYは、グローバルなデータ保護と情報セキュリティプログラムを備えています。効果的なガバナンス機能を維持し、正式な監査手続きを通じてコンプライアンスレビューを実施しています。EYは、以下のレビューとプログラムを実施することで、データ保護と情報セキュリティ上の義務への遵守をサポートしています。

セキュリティ認証プロセス

全てのアプリケーション及びシステムは、情報セキュリティポリシーとアプリケーション開発スタンダードに従って開発されていることを確認するため、セキュリティ認証プロセスを経て本番導入されます。

セキュリティ認証プロセスには、リスクアセスメントの文書レビュー及び脆弱性評価が組み込まれています。これは、情報を作成、保存、管理するために使用される全てのアプリケーションまたはシステムに適用されます。このプロセスは、EYの情報及びEYのクライアント情報の機密性、完全性、可用性を維持するために役立ちます。

プライバシーと機密性の影響評価

EYは、個人情報やクライアント情報を取り扱うシステムやツールを開発または実装する際、データプライバシーチームと連携して、プライバシーと機密性の影響評価（PIA）を実施する必要があります。PIAはシステムまたはツールをグローバルスタンダードに基づいてレビューし、必要に応じて、データのプライバシーと機密性のリスクを低減するためのアドバイスを行います。

PIAに続き、そのシステムまたはツールの全てのユーザーと管理者に対して、データのプライバシーと機密性に関する推奨事項のリストが作成されます。この詳細な分析には、国境を越えたデータ移転のレビューが含まれており、適用される法令及び規制上の要求事項を満たしていることを確認します。

EYには、適用されるデータ保護基準と要求事項に従ってアプリケーションを展開するのに役立つ幅広いポリシーとガイドラインがあります。

コントロールの有効性評価

コントロールが実装され、効果的に運用されていることを検証するために、以下のようなコントロールの有効性に関する評価を行っています。

- パッチ管理、アプリケーションセキュリティ、インフラストラクチャセキュリティなど、グローバル情報セキュリティポリシーの技術的側面に焦点を当てたネットワークとアプリケーションの脆弱性評価
- オペレーティングシステム、データベース、インフラストラクチャなどのコンポーネントの技術的コントロールと構築プロセスをレビューする運用の有効性評価
- セキュリティコントロールが適切に実装及び構成されていることを検証するための、コントロールの有効性の継続的な運用監視

情報セキュリティ監査

クライアント及び規制当局に情報セキュリティコンプライアンスの遵守状況をより詳細に提供するために、EYのグローバルテクノロジー製品、サービス、データセンターは監査を受けています。EYは、以下のような複数の形式の監査を実施します。

- 米国、ドイツ、シンガポールの3つのグローバルデータセンターと各国・地域のデータルームで採用されている情報セキュリティマネジメントシステムを認証するため、ISO 27001に対する独立したサードパーティによるコンプライアンス監査
- クラウドベースのEY Fabricクライアント・テクノロジー・プラットフォーム・コンピューティング環境における情報セキュリティコントロールを認証するISO 27017に対する独立したサードパーティによるコンプライアンス監査
- EYのグローバル事業継続マネジメントシステムの要素に関連するISO 22301に対する独立したサードパーティによるコンプライアンス監査
- 米国、ドイツ、シンガポールの3カ所にあるEYのグローバルデータセンターと各国・地域のデータルーム、及びサードパーティのクラウド型のEY Fabricすなわちクライアント・テクノロジー・プラットフォームを対象とした、セキュリティ、機密性、可溶性の原則に関する、独立したサードパーティの監査人が実施する年次のSOC2 Type2認証
- 米国、ドイツ、シンガポールの3カ所にあるEYのグローバルデータセンターと各国・地域のデータルーム、及びサードパーティのクラウド型のEY Fabricを対象としたISAE 3402/SOC1タイプ2の年次で行う独立したサードパーティの監査人によるセキュリティコントロールのテストと検証
- オペレーティングシステム、データベース、インフラストラクチャなどのコンポーネントの技術的なコントロールと構築プロセスをレビューするファウンデーション監査
- 主要な管理担当者へのインタビュー、詳細なサイトのウォークスルー、文書レビュー、ネットワークの脆弱性スキャンなどの最も重要かつ詳細な形式で行われるオンサイトフィールド監査 - EYのグローバル情報セキュリティポリシーの全ての側面の遵守を評価

情報セキュリティコンプライアンス監査の結果は、シニアマネジメントへ報告、精査されます。指摘事項への是正対応が必要な場合は、是正対応計画が策定、管理されます。

情報セキュリティリスク受容

是正対応計画で対処できない問題については、例外プロセスを用いて指摘事情に関連するリスクをレビューし、代替案を検討します。例外プロセスには、正式な承認プロセス、各例外の定期的なレビュー、及び割り当てられたリスク評価によるセキュリティ評価が含まれます。通常、承認された例外には、是正対応のために発生する可能性のあるリスクを適切に低減するための補完的なコントロールが付随されます。この例外プロセスは、例外とその後の是正対応が少なくとも年次で適切に文書化、管理され、レビューされることを確認するものです。

まとめ

EYは、統合されたデータ保護及び情報セキュリティ戦略を遵守することで、クライアントの情報資産を保護します。

- グローバルなアプリケーションとシステムには、データプライバシー影響評価とセキュリティ認証レビュー、及びビジネス影響評価を含めたさまざまなアセスメントとレビューを実施し、展開と運用における堅牢で一貫したアプローチをサポートします。
- 適切な物理的、技術的、組織的なセキュリティ対策を用いてEYのネットワーク内における個人データを保護します。
- サードパーティの情報処理業者との契約には、EY独自の方針、実務、管理に見合った条項が含まれていることを確認し、クライアントのデータが法律や規制の要件に従って適切かつ安全に管理されていることを確認しています。

クライアントと個人は、個人データと機密データを扱う組織に説明責任を正当に要求します。

EYは、情報資産を保護するために適切な措置を講じることの重要性を理解し、クライアントとメンバーに関連する情報の保護に努めます。

EYがクライアントとクライアントのビジネスを保護する方法についてご質問がある場合、また詳細情報が必要な場合は、EYの担当者にご連絡ください。

EY | Building a better working world

EYは、クライアント、EYのメンバー、社会、そして地球のために新たな価値を創出するとともに、資本市場における信頼を確立していくことで、より良い社会の構築を目指しています。

データ、AI、および先進テクノロジーの活用により、EYのチームはクライアントが確信を持って未来を形づくるための支援を行い、現在、そして未来における喫緊の課題への解決策を導き出します。

EYのチームの活動領域は、アシュアランス、コンサルティング、税務、ストラテジー、トランザクションの全領域にわたります。蓄積した業界の知見やグローバルに連携したさまざまな分野にわたるネットワーク、多様なエコシステムパートナーに支えられ、150以上の国と地域でサービスを提供しています。

All in to shape the future with confidence.

ey.com