

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

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しています。これらの対策の具体的な内容は、実施するサービスや各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共有することに重点を置いています。

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のチームの能力は、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、いつでもどこであって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、なら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単一のまとまりのある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。

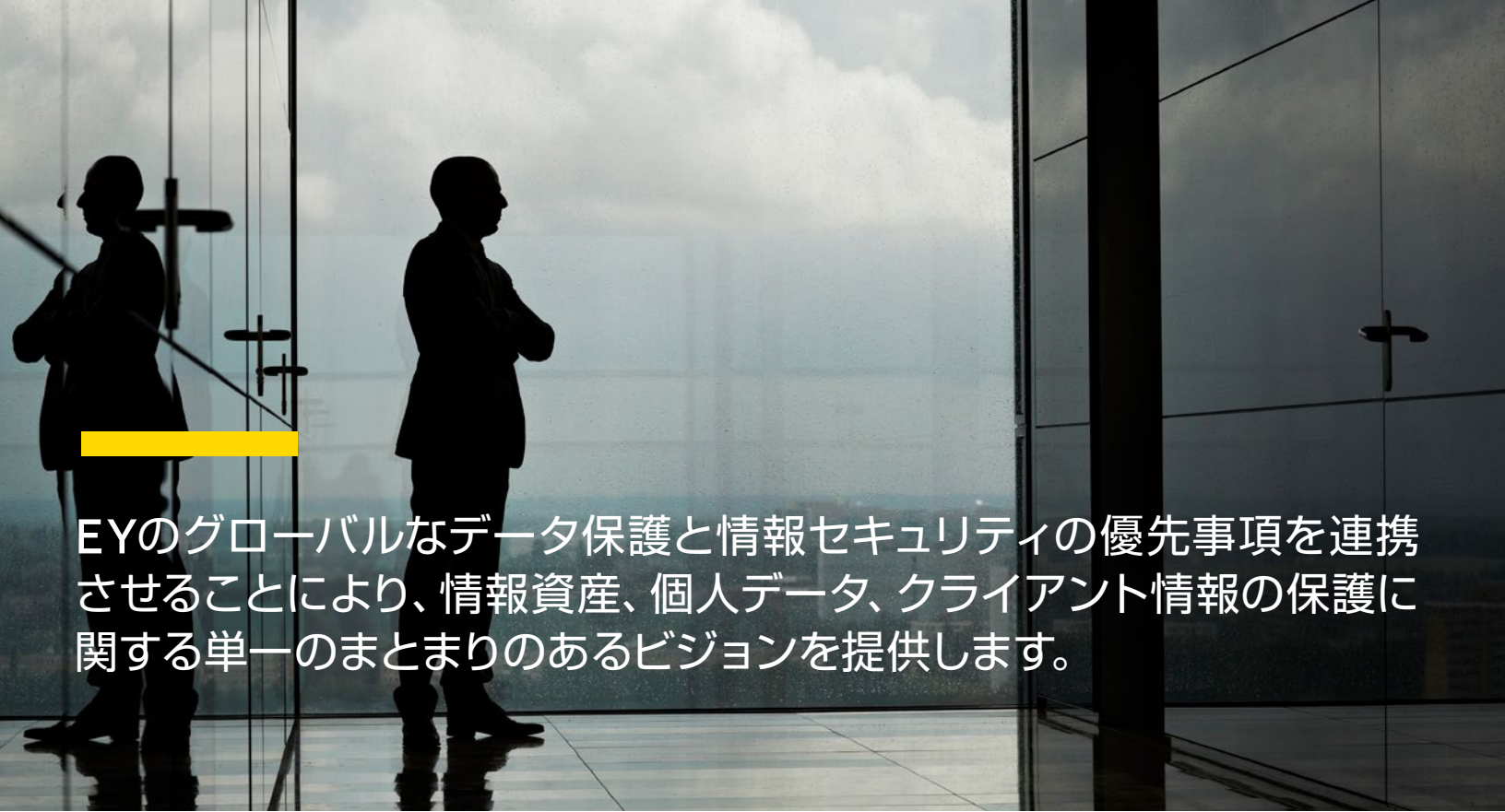
- ▶ 適法性、公正性、透明性：倫理的、合理的、明確に伝達され、合法的な方法でデータを使用します。
- ▶ 目的の限定：定義及び承認された用途にのみデータを使用します。
- ▶ データの最小化：目的に必要な量以上のデータを収集して処理しません。
- ▶ 正確性：データが正確であり、提案された目的に十分な品質であることを確認します。
- ▶ 保存の制限：収集された目的を達成するために必要な期間のみデータを保持します。
- ▶ 完全性及び機密性：データの安全性及び機密性が保たれ、アクセスが厳格な「need to know」に基づいて制御されていることを確認します。
- ▶ アカウンタビリティ：EY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。
- ▶ 機微情報：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。
- ▶ 第三者処理者：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第三者が、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、及び当該第三者との契約に、適用法令に従ったデータ保護条項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、オフショアへの個人データの移転を禁止しています。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メンバーファーム間での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の活動に関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EY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、サービスライン間のチーム化を促進することができます。これらのBCRは世界中のEYファームに適用されており、ey.com/bcr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。データ・プライバシー枠組みは米国商務省から発行されています。詳細については、Ernst & Young LLP EU-US Data Privacy Framework Statementを参照してください。



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単一のまとまりのある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

データやセキュリティに対する攻撃方法が変わりつつある中で、EYのメンバーに提供する情報、ガイダンス、トレーニングも変えていく必要があります。データのプライバシーと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。これは私たち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の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の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

EY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付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タートメントは、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。

- ▶ アクセスコントロール
- ▶ 資産管理: 分類と管理
- ▶ 通信とオペレーションセキュリティ
- ▶ 人的セキュリティ: 社員
- ▶ 情報システムの取得、開発及び保守
- ▶ 物理的・環境的セキュリティ
- ▶ リスクアセスメント

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、これらに限定されません。

- ▶ パソコンのフルディスク暗号化
- ▶ リムーバブルメディアの暗号化ツール
- ▶ パソコンのファイアウォール
- ▶ 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 (ey.com/ja_jp/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枠組みに基づいており、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のメンバーが行う毎日の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ーから取得した、またはそれらに関連する個人情報及び機密情報の両方を尊重し、保護することも求められています。



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の重要なサービスのアプリケーションに対する災害対応とシステム回復手順は、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
- ▶ 業界の先進的な標準に基づいて構築されたミッションクリティカルな災害復旧計画
- ▶ 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・マネージメント・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ー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。



n Security

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の国際規格であるISO 27001/2に準拠したデータ保護技術を適用することによって、この取り組みを支援しています。

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、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、それらが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

情報セキュリティの遵守状況をより詳細に把握するために、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、シンガポールにある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ー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で採用されているISO 27017に対する独立したサードパーティー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するISO 22301に対する独立したサードパーティーによるコンプライアンス監査
- ▶ 米国、ドイツ、シンガポールにある3つのEY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、可用性の原則に関する、独立したサードパーティーの監査人が実施する年次のSOC2 Type2認証
- ▶ 米国、ドイツ、シンガポールにある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、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 Type2の年次で行う独立したサードパーティー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
- ▶ 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脆弱性スキャン
- ▶ 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基礎監査
- ▶ 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文書化され、シニアマネジメントによって精査されます。指摘事項への是正対応が必要な場合は、是正対応計画が決定され、承認されます。

情報セキュリティの例外

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検討し、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され、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。
- ▶ サードパーティー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がお客さまとお客さま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は、「Building a better working world 〜より良い社会の構築を目指して」をパーパス（存在意義）としています。クライアント、人々、そして社会のために長期的価値を創出し、資本市場における信頼の構築に貢献します。

150カ国以上に展開するEYのチームは、データとテクノロジーの実現により信頼を提供し、クライアントの成長、変革及び事業を支援します。

アシュアランス、コンサルティング、法務、ストラテジー、税務及びトランザクションの全サービスを通して、世界が直面する複雑な問題に対し優れた課題提起 (better question) をすることで、新たな解決策を導きます。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYのメンバーファームは、現地の法令により禁止されている場合、法務サービスを提供することはありません。EYについて詳しくは ey.com をご覧ください。

EY Japan について

EY Japanは、EYの日本におけるメンバーファームの総称です。EY新日本有限責任監査法人、EY税理士法人、EYストラテジー・アンド・コンサルティング株式会社などから構成されています。なお、各メンバーファームは法的に独立した法人です。詳しくは、ey.com/ja_jp をご覧ください。

© 2024 EY Japan Co., Ltd.
All Rights Reserved.

ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務及びその他の専門的なアドバイスを行うものではありません。EY Japan 株式会社及び他の EY メンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

本書は *Protecting your data* を翻訳したものです。英語版と本書の内容が異なる場合は、英語版が優先するものとします。

ey.com/ja_jp