Elastic Cloud 情報セキュリティ概要

2023 年 10 月

elastic.co/jp

目次

サービスと対象範囲 2

Elastic Cloud の概要 2

クラウドのコンプライアンスプログラム 4

製品使用データおよび顧客コンテンツ 5

Elastic Cloud サービス概略図 6

Elastic Cloud アーキテクチャーの概要 6

リスク管理 8

ガバナンス 9

情報セキュリティマネジメントシステム（ISMS）と監査 9

情報セキュリティポリシー 10

人事の管理 11

アセット管理 12

フリート管理 12

従業員エンドポイント管理 12

設定管理 13

データの保護 13

データの分類と保持 13

データの収集、処理、廃棄 14

暗号化 15

送信データの暗号化 15

保存データの暗号化 15

鍵の管理 15

ネットワークとデバイスのセキュリティ管理 16

ファイアウォール 16

マルウェア対策 16

時刻同期 17

論理アクセス 17

ロールベースのアクセス制御 17

オンボーディングと解雇 17

本番環境へのアクセス 18

ユーザーアクセスの見直し 18

変更管理 19

サプライチェーンのセキュリティ 19

セキュアな開発 20

SDLC 20

セキュアな設計とアーキテクチャー 20

セキュアコーディング 21

オープンソースソフトウェアとサードパーティソフトウェアのレビュー 21

脆弱性とパッチの管理 22

インフラストラクチャーの脆弱性とパッチの管理 22

製品の脆弱性とパッチの管理 22

脆弱性開示プログラム 23

サードパーティのリスク管理 23

サードパーティのオンボーディング 23

サードパーティの再認定 24

脅威検知 24

監視とアラート 24

ログの管理と保持 25

インシデントレスポンス 25

信頼性 26

可用性とステータス 26

ビジネス継続性と災害復旧 26

独立評価 27

侵入テスト 27

コンプライアンス基準 28

データプライバシー 28

データのホスト 28

契約上の義務 29

サブプロセッサー 30

国際的なデータ移転と Schrems II 事件 30

公的機関からの開示要求 31

企業としての個人データの保護 32

サービスと対象範囲

Elastic は、エンタープライズサーチ、オブザーバビリティ、セキュリティの各種ソリューションを通じて、お客様が必要なものをすぐに見つけ、ミッションクリティカルなアプリをスムーズに運用し、サイバー脅威を防げるよう支援しています。Elastic Cloud は、貴社独自のユースケースに合わせてデプロイを柔軟に調整、管理できるソリューションです。検索エクスペリエンスのスピード、スケール、関連性を高める基盤プラットフォームをシンプルな操作で運用できます。

Elastic は、データの保護と卓越した検索エクスペリエンスの両立をお客様から託されているという重大な責任を認識し、信頼を得るために懸命に取り組んでいます。セキュリティこそ、組織上層部に位置する取締役会の監督と経営陣のガバナンスから、Elastic 全従業員のオンボーディングと継続的なトレーニングにまでわたるあらゆる業務の要です。Elastic Cloud サービスと情報セキュリティマネジメントシステム（ISMS）について、多岐にわたる業界最高レベルのコンプライアンスレポートと認証を取得しています。これらのレポートと認証で証明されているように、製品の開発とデプロイ、脆弱性管理、インシデント管理、脅威対処プロセスまで、Elastic のあらゆる活動に効果的なセキュリティ手法が浸透しています。

本書では、Elastic Cloud がお客様のソリューションに安心してご利用いただける製品であることを示すため、Elastic で実施しているポリシー、手順、技術的管理策についてご紹介します。なお、Elastic Cloud と関連ソフトウェアソリューションはお客様のニーズに応じてオンプレミス、パブリッククラウド、プライベートクラウド、ハイブリッド環境のいずれにもデプロイ可能ですが、本書ではセルフマネージド環境の管理策に関しては扱いません。

Elastic Cloud の概要

Elastic は顧客や社員の検索エクスペリエンスを向上させ、ミッションクリティカルなアプリをスムーズに実行し、サイバー脅威から保護するクラウドネイティブなエンタープライズサーチ、オブザーバビリティ、セキュリティソリューションを提供しています。Elastic 製品では、ソースを問わずあらゆるフォーマットのデータを取り込んで格納し、検索、分析、可視化できます。

Elastic Cloud は SaaS（Software-as-a-Service）製品をまとめたソリューションであり、Elasticsearch Service（ESS）、エンタープライズサーチ、オブザーバビリティ、Elastic Security などが提供されます。Amazon Web Services（AWS）、Google Cloud Platform（GCP）、Microsoft Azure、IBM をはじめとした複数のパブリッククラウドプロバイダーからお客様が選択したインフラストラクチャー上で、Elasticsearch や Kibana などの Elastic Stack コンポーネントを Elastic がホストおよび管理します。Elastic Cloud には、セキュリティ、アラート、監視、レポート、機械学習、可視化など、Elastic Stack の高度なオプションが含まれています。

以下の表に、Elastic Cloud の各コンポーネントの詳細を示します。

Elastic Cloud のコンポーネント	**コンポーネントの内容**
Elasticsearch Service（ESS）	ESS は、分散型のリアルタイム検索・分析エンジンとデータストアをまとめたサービスです。テキスト、数値、地理空間情報を含むあらゆる種類のデータ、そして構造化データと非構造化データの双方に対応しています。
エンタープライズサーチ	Elastic エンタープライズサーチには強力な検索ツールが複数用意されており、検索エクスペリエンスの提供を素早く、スケーリングをシームレスに行えます。 **Workplace Search**：組織のコンテンツプラットフォーム（Google Drive、Slack、Salesforce など）をパーソナライズされた自然な検索エクスペリエンスに統合できるツールです。 **App Search**：Elasticsearch の検索性能をモバイルアプリや SaaS アプリに活用できる開発者向けのツールボックスです。Web クローラーや洗練された API、直感的なダッシュボード、調整可能な関連性コントロールを備えています。 **Site Search**：ニーズに応じた強力な検索機能（検索ボックスなど）を Web サイトに追加できます。

オブザーバビリティ	Elastic オブザーバビリティでは、ログ、メトリック、アプリケーションのパフォーマンス、稼働状況の監視情報を一元的に分析できます。Elastic Agent と事前構築済みの統合コネクターを使用してデータを収集し、機械学習および DevOps と SecOps の両方に対応した既成の検出ツールで外れ値を検出可能です。
セキュリティ	Elastic Security では、単一のインターフェースで脅威防御、検知、対応を行えます。 **Elastic SIEM**：脅威防御と対応に役立つ従来のログ集約・相関付け機能に加え、機械学習によるリスク評価、統合型のケース管理、SOAR などの高度なセキュリティ機能も備えています。 **Elastic Agent**：ハイブリッド環境を含むほとんどあらゆる場所に適応するフットプリントの小ささながら、その用途は無限大。脅威の防止やデータの転送を行えるほか、セキュリティ情報と防御のエンリッチに関する複数のユースケースにも対応しています。 **Limitless XDR**：SIEM とエンドポイントセキュリティを統合し、最先端のセキュリティ体制を構築。長年にわたるデータを分析、検出と対応プロセスを自動化し、すべてのホストにエンドポイント保護を配備できます。

クラウドのコンプライアンスプログラム

Elastic Cloud はセキュリティを中心に据えて設計されています。Elastic では、セキュリティ、コンプライアンス、プライバシー、および信頼性に取り組んでいる証拠として、業界最高レベルの認証と証明書類を獲得、保持しています。

Elastic のグローバル ISMS は ISO 27001 認証を受けており、Elastic Cloud 市販サービスは ISO 27017、ISO 27018、SOC 2 Type 2、CSA Cloud Compliance Matrix（CCM）、HIPAA、PCI-DSS の監査または認証を受けています。また、ペネトレーションテストの経営陣向けサマリーをご用意しているほか、業種および地域別の認証（TISAX など）も取得しています。評価対象となった Elastic のコンプライアンス基準の詳細、および実際のレポートと認証の写しの入手方法については、本書の「コンプライアンス基準」セクションをご覧ください。

また、Elastic Cloud は、AWS GovCloud 環境で FedRAMP の"Moderate"（中）の認証を受けています。認証の詳細については、FedRAMP 認証クラウドサービスのページをご覧ください。政府関係者の方は、FedRAMP Marketplace から FedRAMP パッケージアクセス申請書をご提出いただくことで、FedRAMP Security Packages をご利用いただけます。

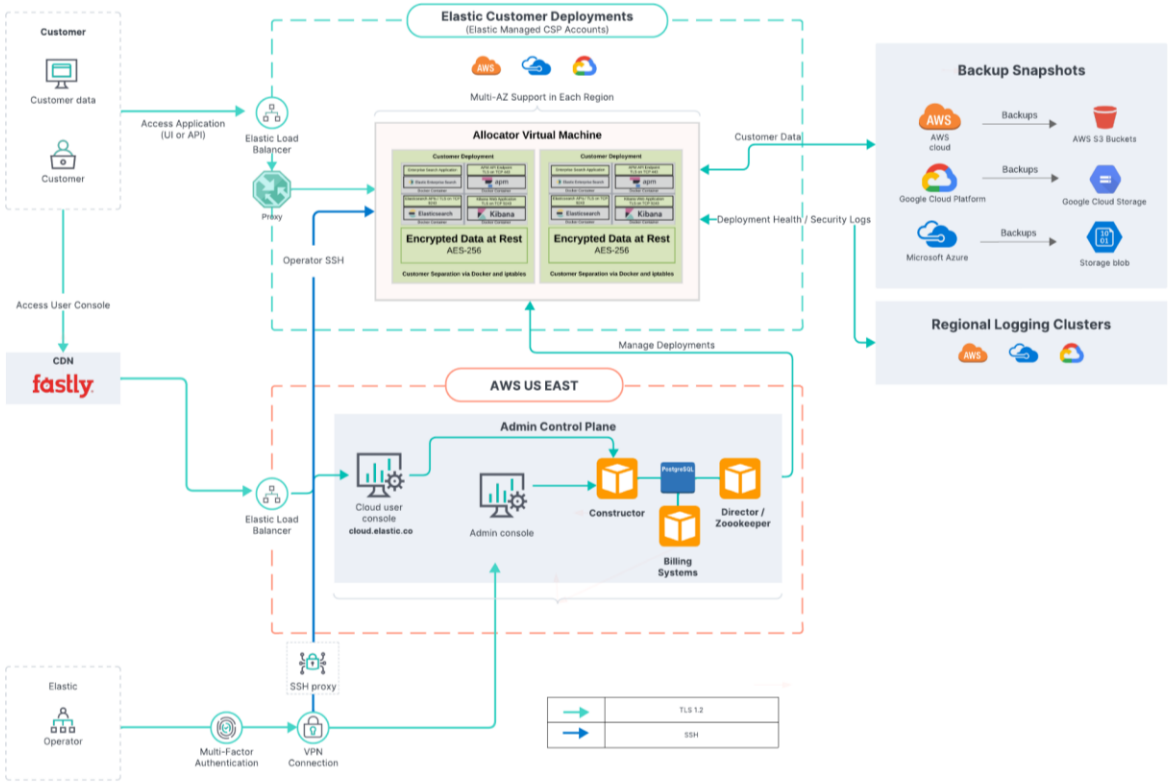
製品使用データおよび顧客コンテンツ

Elastic ではお客様情報の取り扱いに細心の注意を払っており、本書に示す保護手段を講じて顧客コンテンツを保護しています。"製品使用データ"と"顧客コンテンツ"は、以下のとおり区別されます。

製品使用データ： Elastic が製品およびサポートの提供、インフラストラクチャーの管理および監視、製品の分析および改善のために使用するデータを指します。製品使用データには厳密な管理と保護が適用され、データのセキュリティおよび整合性をテストする当社内外の評価の対象となります。ただし、本書では、顧客コンテンツの保護のために Elastic で展開している多層防御についてのみ取り扱います。

顧客コンテンツ： お客様が Elastic の製品およびサービスに投入、アップロード、または送信したデータを指します。Elastic では、製品またはサービスの提供に必要な場合、および法令を遵守するうえで必要な場合を除き、このデータを処理することはありません。Elastic Cloud に投入するデータは、すべてお客様が制御できます。

Elastic Cloud サービス概略図



Elastic Cloud アーキテクチャーの概要

コントロールプレーン

Elastic Cloud のコントロールプレーンには、**ZooKeeper**、**Director**、**Constructor** という各種管理サービスが配置されています。これらの詳細を以下に示します。

- **ZooKeeper**：Elastic Cloud コンポーネントに不可欠な情報を保持する分散型データストアです。このような情報には、プロキシルーティングテーブル、アロケーターからアドバタイズされたメモリー容量、管理者コンソールで行われた変更などがあります。このほか、ZooKeeper は、サービス間の通信のメッセージバスも担います。また、Elastic Cloud 環境の状態、および Elastic Cloud 内で実行されているすべてのデプロイの状態も保持します。

- **Director：**ZooKeeper データストアの管理、および内部クライアントが ZooKeeper と通信する際の証明書署名要求（CSR）への署名を担当します。また、ZooKeeper が通信に使用する STunnel を維持し、新しい ZooKeeper ノードが作成されるたびにクォーラムを設定します。

- **Constructor：**管理者コンソールからのリクエストを監視するスケジューラーとして機能します。変更すべき対象を把握して、アロケーター監視対象の ZooKeeper ノードに変更を書き込みます。また、新規デプロイ時に余分なハードウェアをスピンアップしなくて済むように、アロケーターにクラスターノードを割り当て、基盤アロケーターを最大限に活用します。さらに、Constructor はアベイラビリティゾーンの障害でデプロイに問題が発生しないように、複数のゾーンにクラスターノードとインスタンスを配置します。

この配置の設定は、データ主権要件に応じてカスタマイズ可能です。

- **Cloud UI と API：**管理者が Web および API からインストール環境にアクセスし、管理および監視するための機能です。

プロキシ

プロキシはユーザーからのリクエストを処理し、コンテナーのリクエスト URL で渡されたデプロイ ID を Elasticsearch の実際のクラスターノードや他のインスタンスにマッピングします。コンテナーへのデプロイ ID の割り当て情報は ZooKeeper に格納され、プロキシにキャッシュされます。Elastic Cloud では、このキャッシュを利用することで、ZooKeeper のダウンタイムが発生した場合にも既存のデプロイに対するリクエストを処理できます。

高可用性 Elasticsearch クラスターが展開されている場合、プロキシはゾーンの状態と可用性に関する情報も保持します。いずれかのゾーンで障害が発生した場合、プロキシはそのゾーンへのリクエストのルーティングを中止します。また、プロキシには、スケーリング時およびアップグレード時のダウンタイムを 0 に抑える効果もあります。アップグレードの実行前には、スナップショットが記録され、データが新しいノードに移行されます。移行が完了すると、プロキシはトラフィックの送信先を新しいノードに切り替え、古いノードを切断します。通常は、システムの可用性を保つため、ロードバランサー1 台の内側に複数のプロキシが構成されます。

アロケーター

アロケーターは、Elasticsearch ノードと Kibana インスタンスがホストされるすべてのマシン上で実行されます。以下の処理により、クラスターノードのライフサイクルを制御します。

- リクエスト時に新規コンテナーを作成し Elasticsearch ノードを起動する
- 応答しなくなったノードを再起動する
- 不要になったノードを削除する

また、Constructor が情報に基づいてデプロイ先を決定できるように、基盤ホストマシンのメモリー容量を ZooKeeper にアドバタイズします。

リスク管理

Elastic では、FAIR（ビジネスのリスクの特定と評価、およびリスク軽減行動の優先順位付けを行うための主要な定量リスク評価・分析手法）に従い、セキュリティおよびコンプライアンスにリスクベースの手法を応用しています。

Elastic のリスク評価プロセスでは、確実かる信頼性に優れたサービスをお客様に提供するうえで妨げとなるリスクを特定し対処しています。過去にこのプロセスで特定され、現在管理対象となっている主なリスクを以下に示します。

- 組織管理
- 人事のセキュリティ
- アセット管理
- アクセス制御
- 暗号化
- 通信の保護
- システムの買収、開発、保守
- サプライヤー関係
- 情報セキュリティインシデント管理
- ビジネス継続性管理

リスク特定プロセスでは、社内外両方の要素、および目標達成に対するそれらの要素の影響について検討しています。

特定したリスクは分析プロセスにかけられます。このプロセスでは、Elastic のビジネス目標に関連する潜在的な脅威および脆弱性を分析し、リスクの潜在的な重大性を評価します。
リスク評価プロセスではリスクの管理方法を考慮し、リスクへの対応を受容、回避、緩和、移転のいずれにすべきかを検討します。緩和の戦略は、特定したリスクに応じて決定します。この戦略の内容としては、管理策の設計、開発、実装、およびポリシーと手順の導入や改定などがあります。

この総体的なリスク特定・分析・評価プロセスで得た情報は、リスクシナリオをまとめたリスク登録簿に登録されます。これらのシナリオは、FAIR の手法により評価され、Elastic の財政面に対する影響予想に基づいて順位付けされています。社内外のリスク要素、ビジネスの優先事項、緩和戦略の変化を反映するため、半年ごとにリスク登録簿の見直しが行われています。このプロセスには、情報セキュリティチームが取締役会監査委員会に報告を行う際にリスクベースの手法を取りやすくなるというメリットもあります。

ガバナンス

情報セキュリティマネジメントシステム（ISMS）と監査

Elastic では、ポリシー、手順、運用構造、技術的管理策を連携させてお客様と企業のデータを保護する ISMS を実装しています。この ISMS は ISO 27001 の認証を受けており、ガバナンス、信頼性、リスクと脆弱性管理、セキュリティアーキテクチャーとエンジニアリング、製品セキュリティ、脅威検知、インシデントレスポンスをはじめとしたセキュリティとコンプライアンスの全領域に包括的に対処できるよう構成されています。

Elastic 取締役会（監査委員会）は ISMS の監査を提供するとともに、最高情報セキュリティ責任者（CISO）と定期的に会議を行い、情報セキュリティプログラムが"ビジネスの目標と目的に沿って運用されているか"、"業界のベストプラクティスを採用しているか"、"変化の激しい脅威の状況に合わせて調整されているか"を確認しています。

この Elastic ISMS の補強として専任のビジネスインテグリティおよびプライバシー担当チームが設置され、世界各地のデータに関する法規制を確実に遵守するための組織ソリューション上で情報セキュリティチームと緊密に連携しています。

情報セキュリティポリシー

Elastic では、社内の情報セキュリティ手法を統制するための包括的なポリシーを NIST や ISO 27001 などの業界基準に基づいて策定し、社内全体に管理に関する期待事項を周知しています。情報セキュリティポリシーはすべて、1 年ごとにポリシー責任者による再検討と執行役員による承認を受けています。Elastic のポリシーでは、以下の領域を対象としています。

- 情報セキュリティプログラム
- 利用規定
- リスク管理
- アセット管理
- データ分類
- 記録保持
- アクセス制御
- ワークステーションとサーバーのセキュリティ
- セキュリティ分析とログ記録
- 脆弱性管理
- 変更管理
- セキュアソフトウェア開発
- インシデントレスポンス
- ビジネス継続性と災害復旧

Elastic の全従業員には、入社時および以後 1 年ごとに Elastic の行動規範ならびに情報セキュリティポリシー、プライバシーポリシー、利用規定ポリシーに目を通し確認したことを証明するよう義務付けられています。

情報セキュリティポリシーについて、社外に全文は公開していません。ただし、各ポリシーの対象領域を明確に示すとともに、各ポリシーが定期的に見直し、更新、承認されている証拠となる全ポリシーの目次および改訂履歴が記載された情報セキュリティポリシーバンドルを提供しています。このドキュメントの写しをご希望の場合は、Elastic のアカウント担当者または Elastic Support にお問い合わせください。

さらに Elastic では、正式なポリシーに加え、クラウドの暗号化、証明書とキーの管理、サードパーティリスク管理など、より具体的なプロセス要件があるかベストプラクティスの更新が続けられている領域向けのプレイブック、プロセス資料、計画も策定しています。

人事の管理

Elastic では、包括的なセキュリティプログラムは上層部が強固な姿勢を持たなければ始まらず、Elastic の全従業員が関わらなければ実現できないものだと認識しています。Elastic のソースコード、就業規則集、行動規範には、全 Elastic 従業員が従うべき指針と倫理基準が明記されています。これらの規則に対する違反は、違反者の立場、勤務歴、任期を問わず一切容認されません。

また、Elastic では、関連する人物に情報が速やかに伝達され、従業員の行動に関して適切な説明と監督が行われるよう、正式な指揮命令系統を定めた法人レベルのセキュリティベストプラクティスも策定しています。それぞれの役割と責任は職務要件に基づいて分離し、担当業務を明確に規定しています。

雇用および解雇はすべて、従業員および請負業者のオンボーディングとオフボーディングを安全かつ速やかに行うための手順を記載したポリシーと手順書に従い実施しています。

他の法人レベルのセキュリティプラクティスでは、オンボーディング前に新入社員および請負業者の身辺調査を行うよう定めています。これに加え、経営陣と上級管理職を含めた全従業員に対し、入社時および以後 1 年ごとにセキュリティ意識向上トレーニングを受け、情報セキュリティポリシー、プライバリーポリシー、行動規範、就業規則集に目を通し確認することが義務付けられています。

アセット管理

アセット一覧、アセットの所有権、アセットの返却と処分、および監査証跡の要件を定めたアセット管理基準により、アセット管理ライフサイクルを制御しています。またフリート管理とエンドポイント管理では、別個のアセット管理プロセスを定めています。それぞれのプロセスを以下に示します。

フリート管理

Elastic Cloud を支えるインフラストラクチャーの管理は、当社パートナーのクラウドサービスプロバイダー（CSP）、AWS、GCP、Azure、IBM が担当します。データに使用する基盤 CSP と地理的リージョンは、Elastic Cloud のお客様がデプロイごとに柔軟に選択できます。物理的なセキュリティ、メディア、ハードウェアの制御は CSP が担当します。Elastic は、サードパーティリスク管理プログラムの一環として実施されるサードパーティの再認定時に、パートナーCSP で定められているメディアとハードウェアのライフサイクル管理制御手段の設計と運用の有効性を確認します。

Elastic クラスターでは、Elastic オブザーバビリティを利用してパフォーマンスとアップタイムメトリックを追跡します。重要なアセットはアセット一覧に登録し、アセット一覧に漏れや誤りがないか定期的に確認しています。

従業員エンドポイント管理

従業員のエンドポイントは、Elastic の IT チームが一元的に追跡、管理しています。デバイス管理ソフトウェアを利用して暗号化、パスワード管理、セッション管理、画面ロックなどのセキュリティ設定（すべてデフォルトで有効）を適用しています。これらの設定をローカルで無効化および変更することは禁止されています。エンドポイントは、EDR 機能とリアルタイム監視・アラート機能を備えた Elastic Security で保護されています。従業員エンドポイントのマルウェア対策については、「マルウェア対策」セクションをご覧ください。

Elastic の支給デバイスはすべて、当社デバイス管理ライフサイクルに従って取り扱われます。Elastic 従業員の解雇時には、論理アクセスが無効化され、データのサニタイズと破壊を担当するサードパーティ業者に社内で管理しているエンドポイントが直接送信されます。サードパーティパートナーから Elastic に、Elastic のノート PC 取扱基準に基づいてマシンの破壊と再支給または処分が行われたことを示す証明書が提供されます。Elastic IT チームは、データ破壊ライフサイクルにわたって Elastic の管理対象エンドポイントの状態を把握できるよう、各デバイスの監査証跡を保持しています。

非管理対象のデバイスおよび私用のモバイルデバイスについては、デバイスへのお客様のデータの保存がポリシーで禁止されており、Elastic Cloud の開発やサポートに使われることもありません。

設定管理

Elastic では設定をコード化して管理しており、設定の変更は認証、ピアレビューと承認、テストスイートの自動実行などを行う標準の変更管理手順に従って実施されています。また、本番環境の設定ファイルが直接変更されていないか、ファイル整合性監視機能と不審なアクティビティの検知機能で監視しています。

データの保護

データの分類と保持

Elastic のデータ分類基準では、機密性に応じてデータを分類するよう義務付け、分類ごとにアクセスおよび共有に関する制限事項を設けています。顧客コンテンツと製品使用データの分類は最も機密性の高い"社外秘"であり、該当データの機密性、完全性、可用性を保持するための最も厳格なデータ保護基準の対象となっています。顧客コンテンツおよび製品使用データの定義については、本書の「製品使用データおよび顧客コンテンツ」セクションをご覧ください。

Elastic の記録保持基準では、データの種類と運用要件、契約要件、法規制要件に応じた規定の保持期間に従ってデータの処分を行うよう義務付けています。お客様はいつでも、自身の情報の削除を求めるアカウント削除要請を Elastic Support から提出できます。データ開示請求の提出方法については、本書の「データプライバシー」セクションをご覧ください。

データの収集、処理、廃棄

データ収集

Elastic では、当社サービスの提供、サポート、保守、保護、改善に必要な情報以外は収集していません。これらの情報が第三者に売却されることもありません。Elastic がお客様から収集している情報の詳細については、製品プライバシーステートメントをご覧ください。

データ投入

Elastic では、お客様が自身の Elastic デプロイで格納、送信、処理するデータを制御しておらず、これらのデータにアクセスすることもありません。お客様の Elastic デプロイに投入されたデータはすべてお客様単独の裁量に委ねられ、常にお客様の制御下に置かれます。

データ破壊

Elastic の記録保持基準およびアセット管理基準により、データ破壊の要件を規定しています。ホストインフラストラクチャーについては、当社クラウドサービスプロバイダーパートナーが確実な削除とデータ破壊を担当しています。お客様は、自身の Elastic インスタンス内に格納しているコンテンツの完全な制御権と、Elastic インスタンスのコンテンツをいつでも削除または消去できる権利を有しています。

暗号化

送信データの暗号化

Elastic Cloud では、トランスポートレイヤーセキュリティ（TLS）によりデフォルトで送信データの暗号化を適用しています。最低暗号化強度は TLS 1.2 です。TLS（HTTPS）接続の実装箇所については、「Elastic Cloud サービス概略図」に記載されています。

Elastic Cloud 用の証明書は DigiCert から提供されており、2,048 ビット鍵による RSA 公開鍵認証を利用しています。Elastic では Elastic Cloud のデプロイ用に有効な証明書を保持しており、各証明書について Qualys SSL Labs で A+の評価を受けています。この評価結果については、SSL Labs でご覧いただけます。

保存データの暗号化

保存データの暗号化は Elastic のクラウドサービスプロバイダーパートナーから提供され、デフォルトで有効化されています。当社クラウドサービスプロバイダーは全員、NIST ガイドラインに沿った最小鍵長（256 ビット）を採用しています。

鍵の管理

暗号化鍵は生成場所となったホスト内に留められ、使い捨てとみなされています。これらの鍵は、仮想マシンホストの作成または交換が行われるたびに自動で生成されます。暗号鍵のバックアップ、公開、ホスト外への移動が行われることはありません。基盤 IaaS サービスの暗号化用の鍵管理は、プロバイダーの鍵管理サービスで自動化されています。

Elastic サービスの鍵管理はコード化したインフラストラクチャーとして保持され、該当するコンポーネントまたはサービスそれぞれの運用手順書に含められています。

ネットワークとデバイスのセキュリティ管理

ファイアウォール

当社クラウドサービスプロバイダーパートナーが、本番環境のインフラストラクチャーのハードウェアファイアウォールを管理しています。また Elastic が、インターネットからの不正な受信トラフィックの排除および明示的に認証されていない着信ネットワーク接続の拒否（デフォルト拒否）を行うソフトウェアファイアウォールを展開しています。さらに、環境内の論理ゾーン間でネットワークセグメンテーションとファイアウォールも展開されています。ファイアウォールのルールセットについては、少なくとも半年に 1 回見直しが行われています。ファイアウォールのルールの変更は標準の変更管理プロセスに従って行われ、変更管理制御の対象とされています。さらに、ファイアウォールへのアクセスはすべて RBAC により行われます。

Elastic Cloud のお客様は、トラフィックフィルタリング機能または PrivateLink の設定により、デプロイへのトラフィックをさらに制限できます。
IP トラフィックフィルター | Elasticsearch Service ドキュメント | Elastic
AWS PrivateLink トラフィックフィルター | Elasticsearch Service ドキュメント | Elastic

マルウェア対策

一元管理型の IT 設定により、すべての従業員エンドポイントでマルウェア対策を有効化しています。これらの設定をローカル管理者が無効化、変更することはできません。Elastic Security ソリューションでは、情報セキュリティレビューとアクションアラートで EDR 機能および年中無休体制のオンコールチームを用意しています。

Elastic Cloud 本番環境は、Elastic Security で保護されています。署名および行動パターンは自動的かつ継続的に更新されます。新たな脅威についても検出体制を迅速に展開可能であり、専任の脅威インテリジェンス・検知・対応チームが潜在的なマルウェア感染の検知、分析、対応、修復を担当しています。

時刻同期

共通のタイムソース（NIST サーバー）を使用し、NTP で時刻同期を行っています。

論理アクセス

ロールベースのアクセス制御

Elastic では、最小権限の原則に準拠して内部ユーザーへのアクセスのプロビジョニングを行っています。Elastic の従業員に与えられるのは、自身の業務に必要なレベルのアクセス権だけです。アクセス権は定期的に確認され、従業員のアクセス権が不要となる転職などの事象が起きた場合にはアクセス権の変更を行っています。

また、Elastic 製品にはロールベースのアクセス制御機能が搭載されており、Elastic デプロイと Elastic Cloud 管理プラットフォーム内でお客様がきめ細かくカスタマイズしたユーザーアクセス管理を実装できるようになっています。

オンボーディングと解雇

新入社員には、集中型 ID・アクセス管理（IAM）システムに事前設定されたルールに基づき、自動的に社内クラウドネイティブ SaaS アプリケーションへのアクセス権がプロビジョニングされます。この自動プロビジョニングルールセットでは、当社人事記録システムの職務属性（監督組織、職群、職務レベル、管理構造）に基づき、各従業員に必要なアクセス権のみを付与しています。自動で付与されるもの以外のアクセス権を取得するには、チケットで正式な要請を提出し、管理者の確認と承認を受ける必要があります。

従業員が Elastic 内の別の職務または組織に異動した場合、人事記録システムの職務属性の変更に応じて集中型 IMA システムのワークフローが自動で実行され、新規職務用のアクセス権がその従業員のアカウントに再プロビジョニングされます。古い職務で付与されたアクセス権はデプロビジョニングされ、新しい職務の職務属性に応じたアクセス権が新しく付与されます。

解雇時には、解雇される従業員の状態が HR 管理システムで変更されると、集中型 IAM システムで付与されたアクセス権が自動的に停止されます。この妥当性確認は、1 日に複数回実行されています。

本番環境へのアクセス

Elastic Cloud 本番環境へのアクセス権は、少数の Elastic 従業員にのみ付与されています。Elastic では、プラットフォームの管理、保守、サポートを目的としてこのアクセス権を保持しています。Elastic 従業員がお客様のデータにアクセスすることは、保守やトラブルシューティングの場合も含め、Elastic のデータ処理ポリシーで明確に禁じられています。Elastic 従業員がサポートまたはトラブルシューティングを目的として任意で共有されたデータを閲覧するには、事前にお客様から書面による同意を得る必要があります。Elastic が、Elastic Cloud にアップロードまたは投入されたお客様のデータを事前に閲覧することはありません。お客様は、Elastic との共有前にデータのリダクションまたはサニタイズを行えます。

さらに、Elastic の情報セキュリティ脅威検知対応チームが、社内の不審なアカウントアクティビティや不正アクセスを検知するための機能（ファイルの整合性監視、アカウント乗っ取りの兆候、データ漏えいなど）を開発、実装しています。このような検知は自動ワークフローに組み込まれており、不審なアクティビティに関するアラートを脅威検知対応チームに送り、アナリストによる調査をトリガーするようになっています。

ユーザーアクセスの見直し

Elastic では最小権限の原則に従い、各職務の実施に必要なアクセス以外は認可していません。ユーザーアクセスについては、特権アクセスも含め、システム所有者と管理者が四半期ごとのユーザーアクセスレビューで確認と再認定を行っています。不要になったアクセスはデプロビジョニングされます。

変更管理

変更管理基準により変更管理プロセスを統制し、本番環境に対するソフトウェアおよびインフラストラクチャーの開発とデプロイを管理された安全な方法で制御するための要件を設けています。

この変更管理プロセスにより、変更案の認可、ピアレビュー、テスト、実装、リリースを制御しながら行い、各変更案の状態を記録および監視しています。緊急の変更が必要な場合であっても、文書での承認と自動テストは必須としています。緊急の変更に関する手作業でのレビューも必須としていますが、実装後のレビューが認められています。

サプライチェーンのセキュリティ

本番環境へのソフトウェアのデプロイは、自動 CI/CD パイプラインで管理しています。変更は、各リポジトリの指定ブランチに保存されます。開発の進行時には開発ブランチを使用し、メインブランチには運用準備が整ったコードを格納しています。変更はバージョン管理されており、メインブランチへのマージの前には一連の自動テスト（セキュリティチェックなど）が実行されます。ブランチ保護機能を有効化し、メインブランチへの変更のマージを認可する前にテストスイートへの合格を必須としています。完全に認可された（テストとセキュリティチェックに合格し、ピアレビューで承認を得て、統合チェックに合格した）変更は、手作業を介することなく自動デプロイソフトウェアにより本番環境にプッシュされます。

Elastic のソースコードは、アクセス制御および監視付きのバージョン管理システムに格納されています。ユーザーのアクティビティは監査ログに記録され、予期されていないか不審な変更やビルドプロセスが行われた場合にアラートを通知する検知機能が展開されています。各リポジトリでのコードの変更は、職務に基づいて制限されています。

セキュアな開発

SDLC

セキュアソフトウェア開発フレームワークに、Elastic のシステム開発ライフサイクル（SDLC）のセキュリティ要件を定めています。このフレームワークには、Elastic の全ソフトウェアを安全に設計、開発、デプロイ、追跡、保守するためのプロセスが定められています。また、当社のビルドシステムを保護し、ビルドチェーンに対する侵害のリスクを緩和するための要件も含まれています。ビルドシステムは、ソフトウェアデリバリーパイプライン、パッケージレジストリ、アーティファクトリポジトリ、CI/CD、ソースコード管理システムなどで構成されています。セキュアソフトウェア開発フレームワークでは、テスト目的および本番システム以外での本番環境用データの使用を禁止しています。また、本番環境とそれ以外の環境の分離も必須としています。環境の分離については、サードパーティによる侵入テストで評価を行っています。

セキュアな設計とアーキテクチャー

Elastic のソフトウェア開発では、設計とアーキテクチャーのセキュリティのベストプラクティスに従って、"セキュアバイデザイン"を実現した"デフォルトで安全"なソフトウェアを作成しています。

セキュアソフトウェア開発フレームワークに、すべての設計で遵守すべきデータ保護の要件とセキュリティの原則を規定しています。以下にこれらの要件と原則を示します。

- 機密性：送信中および保存中のデータが不正に閲覧または開示されないように保護する。
- 整合性：データが不正に作成、変更、削除されないように保護する。
- 可用性：許可されたユーザーのみが必要に応じてデータを利用できるようにし、可用性に関する規定の SLA を満たす。
- 識別、認証、認可
- 否認不可

- 監査とロギング
- アクセス制御および最小権限の原則
- セキュアな通信と暗号化の基準
- 安全なデフォルト設定およびフェイルセーフ/フェイルセキュア

また、設計で必須のセキュリティ原則が必ず考慮されるよう、ソフトウェア開発プロセスに脅威モデリングとセキュリティアーキテクチャーのレビューが組み込まれています。

セキュアコーディング

Elastic は SaaS プロバイダーとして、セキュアコーディングの重要性を認識しています。関連するチームと個人を対象として 1 年ごとにセキュアソフトウェア開発トレーニングを実施し、OWASP Top 10 や CWE Top 25 などの一般的なコーディングの脆弱性について説明しています。ソースコードに対する変更のマージについては、（マージリクエスト経由での）変更作成者以外のレビュアー1 名以上によるレビューと承認を必須としています。変更のレビューでは、その変更で起こり得るセキュリティ上の影響を確認しています。さらに、セキュアコードレビューなどを実施する独立侵入テストで、よく見られる危険なコーディング手法に集中的に対処しています。脅威モデリング、セキュリティレビュー、またはソースコードレビューで問題が認められた場合、その問題は脆弱性管理基準に即したリスク評価結果に応じて追跡、評価、修正されます。

Elastic では、ソフトウェアの安全性を保ちお客様を脆弱性から保護する取り組みの一環として、バグ報酬プログラムも開催しています。詳細については、「脆弱性とパッチの管理」セクションの「脆弱性開示プログラム」をご覧ください。

オープンソースソフトウェアとサードパーティソフトウェアのレビュー

セキュアソフトウェア開発フレームワークにより、オープンソースライブラリおよびサードパーティライブラリのコード依存関係を特定、追跡するように定めています。また、脆弱な依存関係を特定、スキャン、修復しやすいように、依存関係管理ソフトウェアも展開しています。

脆弱性とパッチの管理

脆弱性管理基準により脆弱性管理プログラムを統制し、Elastic リソースのスキャン要件および脆弱性のトリアージ、分析、修復、開示の要件を規定しています。Elastic では、Elastic Cloud を支えるインフラストラクチャーと Elastic Cloud コンポーネント自体の両方について、脆弱性スキャンを実施しパッチを適用しています。それぞれのプロセスの詳細を以下に示します。

インフラストラクチャーの脆弱性とパッチの管理

Elastic では、市販の脆弱性スキャナーを利用して継続的にアセットのスキャンを行っています。このスキャンでは、本番環境のアセットすべてを対象としています。ルールセットは、サードパーティのソフトウェアベンダーにより定期的に更新されています。脆弱性の重大度とパッチ適用のスケジュールは、ともに CVSS ランクに基づいて決定されます。重大度が"Critical"（緊急）および"High"（重要）の脆弱性は、即時または次回リリースでのパッチ適用対象に設定されます。

製品の脆弱性とパッチの管理

Elastic では、サードパーティの侵入テスト、自動および手動でのコードスキャンとレビュー、OSS スキャン、セグメンテーションテスト、当社の脆弱性開示プログラムにより、製品のセキュリティ脆弱性のテストを厳格に行っています。Elastic 製品の脆弱性が検出された場合、Elastic が脆弱性管理基準に従ってその脆弱性を評価し、重大度を判定して修復計画を決定します。必要に応じて、Elastic セキュリティアドバイザリ（ESA）を発行します。 ESA は、Elastic 製品に関するセキュリティの問題をユーザーの皆様にお伝えする通知です。各アドバイザリには、Elastic が問題の概要、修復と緩和の詳細情報とともに、CVE 識別子と ESA 識別子を割り当てます。新しいアドバイザリはすべて、セキュリティアナウンスフォーラムで公開されます。

さらに、脆弱性管理基準では、開示の発表も管理しています。開示プロセスでは、新しい製品バージョンのリリースと、必要に応じてアドバイザリページでのお知らせの公開を行います。脆弱性の性質によっては、さらに個々のお客様への連絡、ブログ記事の公開、MITRE への CVE の提出も行います。

お客様は、RSS フィードで ESA の最新情報を入手できます。

脆弱性開示プログラム

Elastic では、社内レビューの対象となる脆弱性をセキュリティ研究者の皆様から報告していただく公開脆弱性開示プログラムを開催しています。報告された脆弱性は Elastic 製品セキュリティチームが確認し、リスクの影響度を評価して、評価に応じた修正を行います。HackerOne の Elastic バグ報酬プログラムでバグ報酬ポリシーをご覧になるか、報告をお送りください。

サードパーティのリスク管理

サードパーティのオンボーディング

すべてのサードパーティは、サブプロセッサーも含め、採用およびレビュープロセスの対象となります。ベンダーごとに、そのベンダーが提供するサービス、処理を担当するデータの種類、必要とする社内システムへのアクセスレベル、およびベンダーの重要度やリスクプロファイルに影響するその他の要因に基づいてリスクプロファイルが評価されます。

ベンダーのリスクプロファイルと Elastic に提供されるサービスの種類に応じて、レビューワークフローが実施されます。機密情報または社内システムへのアクセス権が付与されるベンダー、または重要なテクノロジーサービスを提供するベンダーはすべて、綿密な追加調査を受けることが義務付けられています。こうした調査では、情報セキュリティ、法令、プライバシーに関するレビューなどが行われます。また、追加調査では、サードパーティのセキュリティ手法、セキュリティ認証、コンプライアンスレポートも確認します。

データの処理先、格納先、送信先となる国の法令への適合性を考慮し、必要な場合にはサードパーティとの契約において Elastic から追加のセキュリティ要件を要求しています。

また、Elastic では、当社ベンダーとパートナーに期待される倫理要件をまとめたベンダー行動規範も公開しています。具体的には、倫理とコンプライアンス、従業員の健康と安全、人権と労働者の権利、環境保存管理に関する要件などを定めています。

サードパーティの再認定

継続的なサードパーティ情報リスク管理プロセスを設け、既存のベンダーの再認定を実施しています。サードパーティはリスクレベルに応じて分類され、Elastic の情報セキュリティチームがリスクレベル別に定められ要件に従い各サードパーティのセキュリティ手法を確認します。

Elastic Cloud のインフラストラクチャーサービスを提供するクラウドサービスプロバイダーはすべて、少なくとも 1 年に 1 回レビューと再認定を受けています。再認定プロセスでは、想定されるセキュリティとコンプライアンスの管理策によって Elastic への提供サービスが十分にカバーされているかどうか、およびそれらの管理策の設計と運用が有効であるかどうかを確認するために、ベンダーのリスクプロファイルおよびセキュリティとコンプライアンスのレポート体制が調査されます。

脅威検知

監視とアラート

Elastic では SIEM ソリューションとして Elastic Security を活用し、新しい脅威や攻撃パターンの検知機能のほか、不審な行動の検知機能、ファイル整合性の監視・検知機能、一般的なマルウェア動作パターンを迅速に開発、デプロイしています。Elastic の環境は、自動検出機能によりリアルタイムで監視されています。不審な兆候が見られた際に Elastic の適切な担当者に通知を送る、事前設定済みのアラートワークフローも配置しています。アラートが送られた際には、Elastic の年中無休かつオンコール体制の脅威検知対応チームが調査し対応します。

セキュリティイベントおよびインシデントには、認定を受けたスタッフがインシデントレスポンス基準とインシデントレスポンス計画に従って対処します。これらのスタッフは、継続的なトレーニングも受けています。インシデント管理プロセスの詳細については、本書の「インシデントレスポンス」セクションをご覧ください。

ログの管理と保持

Elastic では、ログ管理ソリューションとして Elasticsearch を使用しています。これにより、検知エンジン、IaaS プロバイダー、脆弱性管理ツール、クラウド管理コンソールなどの各種ソースのログを一元的に取り込み、堅牢なログ機能、監査機能、フォレンジック機能を開発しています。ログの改ざんを防ぐためにアクセス制御を実装し、最小権限の原則に従い編集アクセス権はセキュリティエンジニアリングのみに付与しています。さらに、ファイル整合性監視などの自動検知およびアラート機能によりログシステムを保護し、不審な活動が認められた場合は準リアルタイムで脅威検知対応チームに通知しています。

ログは Elastic のデータ保持基準に従い、ビジネス要件、法令要件、契約要件に応じて保持されます。
データ開示請求の提出をご希望の場合は、本書の「データプライバシー」セクションをご覧ください。

インシデントレスポンス

Elastic の情報セキュリティ部門では、セキュリティイベントおよびインシデントの管理に特化した年中無休体制の脅威検知対応チームを設けています。インシデントレスポンス基準でインシデントレスポンス機能を制御し、イベントの識別、イベントの処理、レポート、およびトレーニングの各要件を定めています。また、個別の別途インシデントレスポンス計画で、セキュリティインシデントの対策、検知、分析、封じ込め、除去、復旧、および報告の手順を定めています。すべてのインシデントには、トレーニングを受け、定期的に訓練とインシデントレスポンス計画のテストを行うインシデントレスポンス担当者が対応します。また、インシデントの発生時には、事後レポートの作成と、教訓を学ぶ演習の実施も義務付けています。

侵害が検知された場合、またはシステムかデータへの不正アクセスが認められた場合には、法令または契約条件に従い、Elastic の法務および情報セキュリティ部門から妥当な期間内にお客様へのお知らせを発行します。

Elastic のインシデントレスポンス計画では、セキュリティインシデントを社外の規制機関または業界機関に報告する必要がある場合に備え、インシデント発生時の状況に応じた報告義務に関する説明を記載しています。また、この計画では、該当する担当者と適切な連絡を行えるように、役割と責務も含めて正式なコンピューターセキュリティインシデントレスポンスチーム（CSIRT）を指定しています。

信頼性

可用性とステータス

拡張版 SLA にて、Elastic Cloud の高可用性アーキテクチャーが提供および推奨されています。このアーキテクチャーにご興味がある場合は、担当アカウントチームにお問い合わせください。
Elastic Cloud サービスのパフォーマンスに関する過去およびリアルタイムのデータは、こちらでご覧いただけます。

ビジネス継続性と災害復旧

Elastic では、災害への備えと対応、および災害復旧を目的として、ビジネス継続性・災害復旧基準に加えて包括的なビジネス継続性・災害復旧計画も策定しています。

Elastic は、創業時から現在に至るまで世界各地に展開してビジネスを行っています。従業員に十分なリモートワーク用機器を支給するとともに、地理的冗長性を意識し世界各地に分散型チームを配置しています。従業員の接続やお客様への Elastic サービスとサポートの提供に必要となるインフラストラクチャーおよび IT システムは、Elastic オフィスには一切配置していません。

Elastic では、Elastic Cloud の災害復旧計画を策定し、少なくとも年に 1 回はテストを行っています。当社の技術復旧機能に存在する知識の漏れや弱点を特定するため、テストの対象領域は毎年変更されます。各テストでは、復旧で社内の設定基準を満たしているか確認するために、目標復旧時間（RTO）と目標復旧時点（RPO）を追跡および記録します。災害復旧テストは、シナリオの詳細、イベントのタイムライン、改善のための活動項目を含めて完全に記録されています。

独立評価

侵入テスト

Elastic では多層防御の強みと重要性を認識し、人的セキュリティ、ラテラルムーブメント、権限昇格、持続的攻撃を考慮に入れています。こうした点を踏まえ、複数の独立した侵入テストサービスプロバイダーと連携して、ネットワークプレイヤーおよびアプリケーションレイヤーの侵入テスト、セグメンテーションテスト、セキュアコードレビューを実施しています。侵入テストは 1 年に 1 回以上実施されます。侵入テストで見つかった問題は、重大度に応じて修正されます。また侵入テストの結果は、部門間でスムーズに連携し責任を持って問題の修正、および必要に応じた防御管理策と検知管理策の追加実装を行えるよう、上級管理職に報告されます。侵入テストの概要レポートおよび修正状況レポートについては、ご希望のお客様に提供しています。

さらに Elastic では、独立侵入テストに加え、正式な脆弱性開示（バグ報酬）プログラムも開催、運営しています。この脆弱性開示プログラムでは、セキュリティ研究者の皆様に、脆弱性の報告をお願いしています。報告された脆弱性については、Elastic 製品セキュリティチームがトリアージと修正を行います。バグ報酬プログラムの詳細および報告手順については、HackerOne のバグ報酬プログラムをご覧ください。

コンプライアンス基準

Elastic では、お客様にとって最も重要なセキュリティとコンプライアンス関連の認定および証明の取得、保持に努めています。当社は、世界中のお客様から規制の厳しい業界や地域で検索、オブザーバビリティ、セキュリティのニーズへの対応を託されているという信頼を重く受け止めています。Elastic Cloud で取得している認定および証明の一覧については、Elastic 製品のセキュリティとコンプライアンスをご覧ください。

データプライバシー

Elastic では、お客様から絶え間ない信頼を獲得するうえで、データプライバシーが果たす役割を重視しています。Elastic Cloud でのお客様のデータの処理方法と保護方法について、お客様に対する透明性の提供に努めています。

データのホスト

Elastic では、Elastic Cloud の提供にあたり Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）などのクラウドサービスプロバイダーを利用しています。これらの各クラウドサービスプロバイダーを通じて、グローバルなホスティングオプションをサポートしています。Elastic Cloud デプロイのホスト先となるリージョンは、お客様がそれぞれのデータ主権のニーズに合わせて選択できます。また、バックアップの設定により、選択されたリージョン内にお客様のバックアップを保持することも可能です。

契約上の義務

Elastic では、世界のプライバシー原則を確実に満たすように、会社全体でプロセス、組織構造、技術的対策を構築しています。こうした義務の裏付けとして、Elastic Cloud の顧客データ処理修正条項（"DPA"）でプライバシー条項を公開しています。

Elastic では定期的に DPA を見直し、更新して、以下の条項を含む該当するデータプライバシー要件を反映しています。

- お客様のデータはお客様のものとする。お客様からの指示がない限り、Elastic は個人データの処理を実行しない。
- Elastic が処理するデータには、該当する法令上のデータ保護要件が適用される。
- Elastic では、適切な技術的対策および組織的対策を契約で義務付け、展開している。こうした対策には、欧州委員会決定 2021/914/EU に準拠した標準的契約条項（"SCC"）が適宜含まれる。
- 個人データの処理権限を持つ全担当者に、機密保持ポリシーと手順が適用される。
- データ主体からの問い合わせがあった場合、お客様に通知される。Elastic がお客様から同意を得ずにこうした問い合わせに対応することはなく、お客様が問い合わせへの対応にあたり各自の要件を満たせるよう支援する。
- Elastic には、Elastic が政府当局からお客様個人データへのアクセスを求められた場合、お客様に通知することが SCC で義務付けられている。法令により Elastic がこうしたデータの開示を行うことが禁止されている場合、Elastic はこの禁止令に異議を唱え、適用免除を求めることが SCC で契約上義務付けられている。
- Elastic は、個人データの処理に関わる担当者全員に確実に機密を保持させるため、機密保持契約および従業員トレーニングプログラムを導入する。これらの契約は、従業員の Elastic での在職期間の終了後も延長される。
- Elastic のサブプロセッサーには、これと同じ基準と組織要件が適用される。Elastic は、サブプロセッサーの作為または不作為に対して、自身でサービスを行う場合と同程度の責任を負う。

サブプロセッサー

Elastic では、お客様へのサービス提供で必要な場合に（サブプロセッサーとして）個人データを厳格に処理することが求められる Elastic Cloud を提供するために、所定の外部サービスプロバイダーおよび内部関連企業を利用しています。

現時点で Elastic と契約している外部サブプロセッサーは https://www.elastic.co/jp/agreements/external_subprocessors に、内部サブプロセッサーは https://www.elastic.co/jp/agreements/internal_subprocessors に記載されています。

国際的なデータ移転と Schrems II 事件

Elastic はグローバル企業であり、EEA および英国で生成されたデータを欧州外部の第三国にいる Elastic 社員、およびサービスの提供に欠かせないサードパーティ組織へ移転する場合があります。具体的な移転先については、上記「サブプロセッサー」セクションに記載されています。このような移転を行う場合、Elastic は堅牢な補完的手段に加えて、SCC（お客様との間では管理者・処理者移転モジュール、サブプロセッサーとの間では処理者・処理者移転モジュール）を使用します。
Elastic では、Schrems II 事件判決後における国際的なデータ移転の補完的手段に関する EDPB ガイダンスを確認しています。そして、Elastic の実体験、当社で処理される個人データに政府当局が関心を示す可能性の低さ、および当社でお客様個人データを守るために実装している保護手段を踏まえ、欧州外でお客様個人データを処理しても、SCC で定められた当社の"データ輸入者"としての義務の遂行を妨げる個人の権利に触れるリスクはないと判断しました。

- 社内での分析および社外顧問によるレビューの結論として、Elastic のデータ移転は一般的な監視法令の対象範囲に該当しないとされた。また、Elastic では、移転対象のデータを保護するための補完的手段も用意している。
- Elastic のサービスおよびデータ処理活動の性質上、公的機関から開示要求が提出される可能性は極めて低い。Elastic はこれまで、FISA、EO12333、CLOUD Act のいずれに基づく要求も受けていない。

- 該当するお客様データの移転については、その保護のために SCC が適用される。欧州内で生成された個人データが（i）Elastic のお客様から当社に直接移転される場合、（ii）Elastic グループ法人間において当社により内部的に移転される場合、または（iii）Elastic から外部サブプロセッサーに移転される場合、当社は各関係者と SCC を締結する。
- 送信データおよび保存データは暗号化される。
- お客様は、Elastic サービスアプリケーション用に EU サーバーを選択できる。
- Elastic ではデータ転送を保護するために、契約上、技術上、組織上の保護対策を継続的に評価、開発している。

公的機関からの開示要求

Elastic では、公的機関からお客様のデータの開示要求を受けたときの対応方法を定めたポリシーとプロセスを設けています。これらのポリシーとプロセスは、該当するデータ保護法令とお客様との契約に従います。

Elastic は、いずれの適用法令であっても、公的機関からの開示要求および要求された開示に関連する義務の遂行が妨げられることはないと認識しています。いかなる場合にも、Elastic が大々的な方法、必要以上の方法、または無差別な方法で、必要な範囲を超えて個人データを社会全体に公開することはありません。

ただし、上記を定めてはいますが、FISA 702 条などに基づいて Elastic が公的機関から顧客コンテンツの開示要求を受けたことはありません。また、EO 12333 に基づく顧客コンテンツへの直接的なアクセス受けた事実もないものと認識しています。Elastic はいずれの製品やサービスにもバックドアやマスターキーは用意しておらず、どのような政府機関にも当社のサーバーへの自由なアクセスや直接のアクセスを許可していません。

企業としての個人データの保護

プライバシー通知

Elastic Cloud で Elastic が個人情報を収集、使用、開示、転送、保存する方法の詳細については、製品プライバシーステートメントをご覧ください。

世界各地のプライバシー規制

Elastic は、GDPR や CCPA をはじめとする世界各地のプライバシー規制の遵守に尽力しています。データ主体要求の提出をご希望の場合は、一般プライバシーステートメントの「お問い合わせ方法」をご覧ください。お客様の Elastic デプロイを GDPR に準拠させる方法については、Elasticsearch と Elastic Stack の GDPR コンプライアンスをご覧ください。

