セキュリティー概要

最終更新日：2019 年 10 月

目次

HubSpot　セキュリティー概要

1　弊社および弊社の製品について

HubSpot は、インバウンド手法に基づくマーケティング、営業、およびカスタマーサービスを実践するための最先端のプラットフォームを提供しており、2006 年の創業以来、インバウンドのアプローチを世界中の企業に浸透させるべく取り組んできました。現在、世界 90 か国以上で、何万社ものお客様が HubSpot のソフトウェア、サービス、およびカスタマーサポートを利用して、顧客を惹きつけ、信頼関係を築き、顧客を満足させるための方法の変革に取り組んでいます。HubSpot のインバウンド マーケティング ソフトウェアである HubSpot Marketing Hub は、VentureBeat、GetApp、Capterra、および G2 Crowd のランキングで第 1 位を獲得しており、ソーシャルメディアの投稿とモニタリング、ブログの運営、SEO（検索エンジン最適化）、ウェブサイトのコンテンツ管理、E メールマーケティング、レポート作成と各種分析など、さまざまな機能を統合したオールインワンのプラットフォームとして提供されています。また、HubSpot Sales Hub と HubSpot CRM は業界で多くの称賛を集めているセールスアプリケーションで、営業部門やカスタマーサービス部門による（リードやプロスペクトを含めた）顧客とのコミュニケーションを円滑にする効果があります。さらに、HubSpot Service Hub は、スムーズなカスタマーサービスを提供し、顧客満足度を高めていくうえで最適なソリューションです。

HubSpot 製品は、SaaS（Software as a Service）ソリューションとして提供されており、目的別のウェブアプリケーションや API（Application Programming Interface）、E メールプラグインなどの形式でお客様に提供されます。

2　HubSpot によるセキュリティーとリスクのガバナンス体制

セキュリティーに関して HubSpot が最優先しているのは、お客様とユーザーのデータを保護することです。そこで、お客様のデータを保護しつつサービスを提供できるように、適切なリソースの整備とガバナンス体制の構築に取り組んできました。その中には、企業と製品のセキュリティー保護を専門とするチームの設置も含まれています。このセキュリティーチームは、HubSpot の包括的なセキュリティープログラムとガバナンスプロセスの構築を担当しており、既存のガバナンス体制の見直しと新たな体制の構築、セキュリティーに関する社内のフレームワークの策定と管理、および効果的なリスク管理のためのサポート体制の確立に重点的に取り組んでいます。HubSpot および HubSpot 製品におけるセキュリティー対策の実践については、最高執行責任者（COO）の直属である最高セキュリティー責任者（CSO）が監督します。

3 セキュリティーとリスク管理に関する弊社の目標

弊社では、SaaS 業界のベストプラクティスに基づき、セキュリティーに関するフレームワークを策定しており、主な目標として次の項目を掲げています。

- お客様を守り、信頼に応える – お客様の情報のプライバシーと機密性を確保しながら、質の高い製品とサービスを常に提供できるようにします。
- サービスの可用性と継続性を維持する – すべてのユーザーの皆様にサービスやデータの可用性を継続的に提供できるようにします。また、サービスの継続を脅かすセキュリティー上のリスクを最小限にとどめるべく、先回りで取り組みます。
- 情報とサービスの完全性を確保する – お客様の情報に破損や不正な変更が発生しないようにします。
- 規制や基準を遵守する – 現行の国際的規制や業界のベストプラクティスに関するガイダンスに準拠したプロセスとガバナンスを確立します。セキュリティープログラムの策定においては、クラウドセキュリティーに関する最も優れたガイドラインに準拠します。具体的には、COBIT や Cloud Security Alliance の CCM（Cloud Control Matrix）などの規格を利用し、ISO 27001 および NIST SP 800-53 に対応しています。

4 HubSpot のセキュリティー統制

HubSpot では、お客様からお預かりしたデータを確実に保護するために、セキュリティー統制に関するさまざまな対策を実施しています。HubSpot のセキュリティー統制は、リスクを最小限に抑えつつ、従業員にとって障害となる要素を取り除き、業務の効率化を図ることを目的としています。以下では、セキュリティー統制の取り組みの一部について説明します。HubSpot のセキュリティープログラムの詳細については、https://www.hubspot.jp/security をご覧ください。

4.1 HubSpot の製品インフラストラクチャー

4.1.1 データセンターのセキュリティー

HubSpot では、製品インフラストラクチャーのホスティングをトップクラスのクラウド インフラストラクチャー プロバイダーに外部委託しています。HubSpot 製品のインフラストラクチャーのホスティングに使用されているのは、主にアマゾン ウェブ サービス（AWS）と Google Cloud Platform（GCP）です。これらのソリューションは、高度な物理的セキュリティーおよびネットワークセキュリティーを提供し、さまざまなホスティング プロバイダー ベンダーに対応しています。現時点で、HubSpot の AWS のクラウド サーバー インスタンスは米国で、GCP のクラウドインスタンスはドイツで運用されています。いずれのプロバイダーも、SOC 2 および ISO 27001 への準拠を含め、セキュリティープログラム

の監査を継続的に受けています。HubSpot のオフィスでは、本番環境の製品システムのホスティングは行っていません。

世界最高クラスのインフラストラクチャープロバイダーであるアマゾンと Google は、電源、ネットワーク、セキュリティーなどに関して最先端のインフラ施設を使用しています。施設については、99.95～100%のアップタイム（稼働率）が保証されており、電源、ネットワーク、暖房換気空調設備のすべてについて、少なくとも N＋1 の冗長性が確保されています。各プロバイダーの拠点では、弊社からお客様へのサービス提供を妨げることがないように、物理的なアクセスはもとより、パブリックネットワーク（インターネット）、プライベートネットワーク（イントラネット）のどちらかによらず、電子的なアクセスも厳しく制限しています。

こうした物理面、環境面およびインフラストラクチャーに関するセキュリティー対策は、継続性や復旧計画も含め、SOC 2 Type II および ISO 27001 の認証を受けるうえでそれぞれ個別に検証されています。こうした認証については、AWS のコンプライアンスに関するページや GCP のセキュリティーに関するページでご確認いただけます。

4.1.2　ネットワークセキュリティーと境界領域の保護

HubSpot の製品インフラストラクチャーは、インターネットに対応可能なセキュリティー保護を備えることを想定して構築されています。具体的には、社内の製品インフラストラクチャーに対して、またはその内部で不正なネットワークアクセスが行われないように設計されています。こうしたセキュリティー統制には、エンタープライズクラスのルーティングおよびネットワークアクセス制御リスト（ファイアウォール）が含まれます。

ネットワークレベルのアクセス制御リストは、AWS の Virtual Private Cloud（VPC）のセキュリティーグループまたは GCP のファイアウォール規則で設定し、インフラストラクチャー内の各サーバーインスタンスをポートレベルおよびアドレスレベルで保護します。このファイアウォールテクノロジーにより、想定外のトラフィックは既定で拒否されるほか、すべてのネットワークトラフィックがログに記録され、弊社の監視システムへの通知に使用されます（詳細はセクション 4.1.4 をご覧ください）。こうしたネットワークアクセス規則により、パブリックネットワークからのネットワークトラフィックだけでなく、インフラストラクチャー内部のサーバーインスタンス間のトラフィックも細かく制御されます。インフラストラクチャーの内部では、内部ネットワークの制限により、適切な種類のデバイスに対してのみ通信が許可されるように多層的な対策が講じられています。

ネットワーク セキュリティー モデルの変更は積極的に監視され、標準変更制御プロセスによって制御されます。既存の規則や変更点はすべてセキュリティーリスク評価の対象となり、適切に記録されます。

4.1.3 構成管理

HubSpot では、お客様のニーズに応じた拡張性を実現するために自動化を行っています。製品インフラストラクチャーは高度に自動化されており、必要に応じて容量や機能を柔軟に拡張することができます。サーバーインスタンスは Puppet を使用して完全に自動化されており、すべてのサーバーの設定は作成からプロビジョニング解除まで厳しく管理されています。

サーバータイプの設定は、イメージおよび Puppet の設定ファイルにすべて埋め込まれており、これらのイメージと設定スクリプトをサーバーの構築時に使用することで、サーバーレベルの設定が管理されています。設定と標準イメージに対する変更は、制御された変更管理プロセスを通じて管理されています。インスタンスのタイプごとに、インスタンスの展開に応じた堅牢な設定が用意されています。

通常は、サーバーインスタンスが満たすべき基本要件に準拠しなくなった場合に該当のインスタンスを削除し、代替となるインスタンスのプロビジョニングを行うことで、パッチ管理と設定の制御を行います。HubSpot では、日常的なインフラストラクチャーの処理に、自動化された厳格な設定管理を組み込んでいます。

4.1.4　アラートと監視

HubSpot では、構成手順を完全に自動化しているだけでなく、今後起こり得る問題に継続的に対処できるように、監視やアラート、対応を自動化するためのテクノロジーにも力を注いでいます。HubSpot の製品インフラストラクチャーは、異常の発生時にエンジニアや管理者にアラートを送信する機能を備えています。具体的には、エラー発生率の変動、不正使用、アプリケーションへの攻撃などの異常が生じると、自動的に対応が実行されると共に、対応や調査、修正を促すアラートが適切なチームに送信されます。想定外のアクティビティーや悪質なアクティビティーが発生した場合、すばやく確実に解決できるように、システムから適切な担当者に通知されます。

また、予測される事態に即座に対応できるように、多数の自動トリガーがシステムに組み込まれています。あらかじめ定義されたしきい値に達すると、トラフィックのブロックや検疫、プロセスの終了などの機能が実行さるため、さまざまな望ましくない状況が発生しても HubSpot のプラットフォームを保護できます。

異常の検出とその対応を可能にしているのは、24 時間年中無休で稼働する監視プログラムと充実したログ出力です。HubSpot のシステムでは、製品を構成するすべてのテクノロジーに関するログを収集し、保存します。アプリケーションレイヤーでは、すべてのログイン、ページ閲覧、変更、その他の HubSpot ポータルへのアクセスも記録されます。インフラストラクチャーのバックエンドでは、数多くのコマンドおよびトランザクションのうち、認証の試行、水平的または垂直的なアクセス許可の変更、インフラストラクチャーの健全性、実行された要求が記録されています。ログとイベントはリアルタイムに監視され、開発

者、セキュリティーのプロ、エンジニアが適切に対処できるように、イベントは時間帯を問わず即座にエスカレーションされます。

4.1.5　インフラストラクチャーへのアクセス

潜在的なセキュリティーイベントは、厳格で一貫性のあるアクセス制御モデルを綿密に設計することで、種類を問わず予防できます。そこで、HubSpot ではシステムへのアクセスを厳格に制御しています。役職に基づくアクセス制御（RBAC）モデルにより、HubSpot の従業員は法人向けサービス、HubSpot Sales Hub および HubSpot Marketing Hub のポータル、ならびに製品インフラストラクチャーへのアクセスが職務に応じて許可されます。HubSpot の RBAC モデルの詳細については、セクション 4.3 をご覧ください。

インフラストラクチャーのツール、サーバー、および同様のサービスへのアクセスは、職務上必要な最小限のユーザーにのみ許可されます。緊急アクセスおよび管理機能へのアクセスについてはジャストインタイムアクセス（JITA）モデルを採用しており、特権的な機能への一時的なアクセスをユーザーが必要に応じて要求できるようになっています。

ユーザーには、業務部門やチームによって、JITA の要求を行う特権が割り当てられます。Linux サーバーの sudo コマンドで付与されるアクセス権限のような非標準の緊急アクセスが必要な場合も、ユーザーは JITA の要求を行います。JITA の要求はログに記録されており、ログの内容は変則的な要求が行われていないか常に監視されています。特権的な機能へのアクセスが許可されたユーザーは、自身の職務を遂行できるようになります。

また、SSH や同様のプロトコルを使用して製品インフラストラクチャーデバイスにネットワークから直接アクセスすることは禁止されており、エンジニアが QA 環境や本番環境にアクセスするには、その前に要塞ホスト（いわゆるジャンプボックス）を介して認証を行う必要があります。サーバーレベルの認証では、ユーザーごとに一意の SSH キーおよびトークンベースの 2 要素認証を使用します。

4.2 アプリケーションの保護

4.2.1　ウェブアプリケーションの防御

HubSpot では、お客様のデータとウェブサイトを保護する取り組みの一環として、業界でも評価の高いウェブ アプリケーション ファイアウォール（WAF）を導入しました。WAF は、HubSpot 製品または HubSpot のプラットフォームでホスティングされているお客様のサイトに対する攻撃を自動的に検知し、防御します。HubSpot の WAF は、https://app.hubspot.com で利用できる機能へのアクセスや https://api.hubapi.com で公開されている API との連携など、HubSpot のプラットフォームへのアクセスを保護するほか、HubSpot のプラットフォームでホスティングされているお客様のコンテンツもすべて自動的に保護します。悪質なトラフィックの検出とブロックには、Open Web Application Security Project（OWASP）作成の「OWASP Top 10」に記載されているベストプラクティスのガイドラインや同様の推奨事項に従って作成されたルールを使用しま

す。分散サービス拒否（DDoS）攻撃に対する防御も組み込まれており、お客様のサイトやその他の HubSpot 製品を継続的に利用できる状態を維持する効果を果たしています。

HubSpot の WAF は業界標準とカスタムルールを組み合わせた構成になっており、各種制御の有効と無効を自動で切り替えることで、お客様に最適な保護を提供できるようになっています。ここで挙げた各種ツールは、アプリケーションレイヤーでリアルタイムのトラフィックを積極的に監視しつつ、検知した挙動の種類やレートに基づいて悪意があると判断した場合は、アラートを送信したり、トラフィックを遮断したりすることができます。

4.2.2　開発およびリリースの管理

HubSpot は各種機能の進化のスピードを大きな特長とし、最新の継続的デリバリー方式でソフトウェア開発を行うことで製品の改善を続けており、新しいコードの提案、承認、マージ、展開が毎日何千回も行われています。コードのレビューと品質保証は、HubSpot のプラットフォームについて豊富な知識を持つ専門のエンジニアチームが開発と同時に行います。承認の管理は指定されたリポジトリーの所有者が行っており、承認されるたコードは HubSpot の継続的インテグレーション環境に自動的に送信され、コンパイル、パッケージ化、および単体テストが行われます。これらをすべてパスした新しいコードは、自動的にアプリケーションティア全体に展開されます。

コードを展開する際は、展開後のフックでエラーが検出された場合に備えて、既存の本番環境用のコードのアーカイブが必ず作成されます。展開を担当するチームは、対象のアプリケーションの健全性に関する通知を管理します。障害が発生した場合は、即座にロールバックが行われます。

継続的デプロイメントモデルの一環として、HubSpot は幅広いソフトウェアゲーティングおよびトラフィック管理機能を使用し、お客様の選択（プライベートベータ、パブリックベータ、フルローンチ）に応じて機能を管理しています。主な機能変更は、アプリケーション内のメッセージや製品更新情報のページで通知されます。

新しく開発され、ビルドされたコードは、最終段階のテストを目的として、本番環境への昇格前に HubSpot の専用 QA 環境で個別に展開されます。QA 環境と本番環境の間の想定されない不正なアクセスは、ネットワークレベルのセグメンテーションにより防止されます。お客様のデータは、HubSpot が QA 環境で使用することも、他のテストで使用することもありません。

4.2.3　脆弱性スキャン、侵入テスト、バグ報奨金プログラム

HubSpot のセキュリティーチームは、業界で高く評価されている各種ツールを使用して、脆弱性スキャンについて多層的なアプローチを取ることで、HubSpot のテクノロジー全体を包括的にカバーしています。HubSpot では、自社に対して継続的にさまざまな脆弱性スキャンおよび侵入テストを実施しています。脆弱性スキャンの対象となるのは、社内のネッ

トワーク、アプリケーション、企業インフラストラクチャーです。最新の脆弱性を検出して対応するために、ネットワークベースとアプリケーションレベルの脆弱性スキャンを 1 日に 1 回以上、実行しています。静的なコード解析により自動的に最新のコードをレビューして、開発ライフサイクルの早い段階で潜在的なセキュリティーの問題を検出します。

さまざまなセキュリティー上の脅威に先回りで対応できるように、継続的なスキャン、包含リストの適応型スキャン、脆弱性シグネチャーの継続的な更新を行っています。セキュリティーリスクの特定と対応に関する自社の能力については、業界有数の第三者による侵入テストを年 4 回実施して、客観的な評価を受けています。ここに挙げたプログラムの目的は、セキュリティー面でリスクとなる欠陥を発見し、問題があれば迅速に対処するプロセスを繰り返し行うことです。侵入テストは HubSpot のテクノロジー全体でアプリケーションレイヤーとネットワークレイヤーに対して実施されます。評価対象に含まれる潜在的なベクトルの種類をできるだけ増やせるように、侵入テストの実施機関には、HubSpot 製品や企業ネットワークへの内部アクセスが許可されます。

また、社内の脆弱性スキャンと第三者による侵入テストに加え、HubSpot ではバグ報奨金プログラムを実施しています。バグ報奨金プログラムでは、独立のセキュリティー研究者を招待して HubSpot 製品のセキュリティー面の欠陥を発見してもらい、その報告内容に応じて報奨金を支払います。セキュリティーコミュニティーのメンバーおよび HubSpot のお客様は、トライアル版のポータルに対するセキュリティーテストを実施できます。HubSpot の報奨金プログラムの詳細については、https://bugcrowd.com/hubspot をご覧ください。

4.3 お客様のデータの保護

4.3.1 HubSpot 製品における機密情報

HubSpot 製品は、マーケティング、営業、カスタマーサービスの情報を統合するものです。HubSpot 製品に収集されるデータは、リードや顧客とのやり取り、公開されている各種名簿、および信頼できる第三者の情報源のいずれかを由来とします。HubSpot のツールで収集される情報の種類は、お客様ご自身で設定することができます。お客様は、HubSpot のお客様サービス利用規約と利用規定に従い、マーケティング、営業、カスタマーサービスのプロセスを実施するうえで収集する情報を、適切な種類に限定する必要があります。クレジットカード番号、デビットカード番号、個人の金融機関口座情報、社会保障番号、パスポート番号、運転免許証番号もしくは類似の身分証明書の番号、または雇用状態、経済状態、もしくは健康に関する情報など、機密性のあるデータを収集するために HubSpot 製品を使用することはできません。

4.3.2 クレジットカード情報の保護

HubSpot のサービスに対する料金のお支払いには、多くのお客様がクレジットカードを使用しています。HubSpot では、お客様から送信されたクレジットカード情報の保管、処

理、および収集は行わず、PCI のセキュリティー基準に準拠した信頼の置ける支払いベンダーに委託しております。そのため、お客様のクレジットカード情報は、関連する規制や業界標準に準拠した形で安全に処理されます。

4.3.3　転送中および保存中のデータの暗号化

HubSpot 製品との間で送受信される機密データ（お客様のポータルに対する API 呼び出し、ログイン、認証済みのセッションなど）は、すべて TLS（Transport Layer Security）1.0、1.1、1.2、または 1.3 および 2048 ビット以上のキーにより暗号化されて転送されます。また、HubSpot のプラットフォームで自社のウェブサイトをホスティングしているお客様は、そのサイトでも TLS を既定で使用できます。TLS の設定の詳細については、ウェブサイトのセットアップ手順に関するガイドをご覧ください。HTTPS 接続に使用する暗号プロトコルの制限を希望される場合は、まずカスタマーサポートまたはカスタマー サクセス マネージャーまでお問い合わせください。

HubSpot は、保存中のデータを暗号化するうえで、複数のテクノロジーを使用しています。HubSpot 製品のサーバーインスタンスで使用される物理ハードドライブと仮想化ハードドライブ、および Amazon S3 などの長期的な格納ソリューションでは、AES-256 の暗号化を使用しています。さらに、特定のデータベースとフィールドレベルの情報は、情報の機密度に基づいて暗号化されて保存されます。たとえば、ユーザーのパスワードはハッシュ化されています。また、一部の E メール機能では、保存中も転送中もさらに強力な暗号化が適用されます。

転送中および保存中のデータ暗号化に使用される暗号鍵は、HubSpot のプラットフォームによって安全に管理されています。転送中のデータ暗号化に使用される TLS 秘密鍵は、HubSpot のコンテンツ配信パートナーによって管理されています。保存中のデータ暗号化に使用されるボリュームおよびフィールドレベルの暗号鍵は、堅牢な KMS（鍵管理システム）に保存されます。鍵のローテーションの頻度は、鍵の種類、ならびに鍵および保護データの機密性によって異なります。TLS 証明書の場合、一般的な有効期限は 2 年間です。

4.3.4　ユーザーによるログインの保護

HubSpot 製品では、ユーザーが HubSpot アカウントにログインする場合に、HubSpot のビルトインログイン、Google アカウントによるログイン、シングルサインオン（SSO）のいずれかを使用できます。ビルトインログインには一律のパスワードポリシーが採用されており、このポリシーではパスワードを 8 文字以上で大文字、小文字、特殊文字、スペース、および数字を組み合わせたものにする必要があります。HubSpot のビルトインログインを使用する場合、既定のパスワードポリシーを変更することはできません。SSO プロバイダーを使用しているお客様は、SSO ベースのログインを設定できます。SSO の設定手順は、ナレッジベースの記事でご確認いただけます。SSO や Google アカウントによるログインを使用する場合は、SSO プロバイダーまたは Google アカウントでパスワードポリシーを設定できます。

また、HubSpot のビルトインログインを使用するお客様は、HubSpot アカウントの2 要素認証の設定が推奨されます。ポータルの管理者は、すべてのユーザーが 2 要素認証を有効化するように HubSpot ポータルの設定を変更できます。

4.3.5　ユーザーと API の承認

お客様は、ユーザーの権限を細かく割り当てることで、データ機能に対するユーザーのアクセスを制限することができます。ユーザーの権限の設定については、ナレッジベースの記事をご覧ください。

API の利用を有効化するには、API キーまたは OAuth 2.0 による承認のいずれかの方法を使用します。お客様は自社のポータル用の API キーをご自身で生成できます。API キーは、カスタム連携のプロトタイプを迅速に作成するために使用することを想定されています。API 要求の認証および承認には、HubSpot の OAuth を実装する方法が効果的なアプローチとなります。また、機能の連携には OAuth が常に必要になります。OAuth による要求の承認は、スコープの定義によって確立されます。API の利用の詳細については、HubSpot の開発者ポータルをご覧ください。

4.3.6　HubSpot の従業員によるアクセス

HubSpot では、本番環境と企業環境内のデータに対する個人のアクセスを制御しています。HubSpot の従業員には、RBAC モデルにより、社内での役割に応じて本番環境のデータへのアクセス権限が付与されます。また、必要に応じて JITA モデルが使用される場合があります。

エンジニアおよび運営チームのメンバーには、その職務に応じてさまざまな本番環境のシステムに対するアクセスが認められることがあります。アクセスに関してよくあるニーズとしては、アラートへの対応およびトラブルシューティングのほか、製品の投資に関する意思決定のための情報分析や、製品サポートなどが挙げられます。製品インフラストラクチャーへのアクセスは、ネットワークのアクセス制御およびユーザーの認証と承認の制御によって制限されます。ネットワーキング機能へのアクセスは、職務上アクセスの必要なユーザーだけに厳しく制限されており、継続的なレビューの対象となります。

カスタマーサポートやカスタマーサービスなどのカスタマーエンゲージメント関連のスタッフは、カスタマーポータルに対するアクセスをジャストインタイムで要求することができます。ただし、アクセスの必要がある場合に限定され、そのアクセスには一定の有効期限が付きます。アクセスを要求できるのは、お客様に対してサポートやサービスを提供する業務に従事する場合に限られます。この要求は、特定のお客様のポータルに最大 24 時間アクセスできるジャストインタイムのアクセスに限定されます。アクセス要求、ログイン、クエリー、ページビュー、およびこれに類する情報はすべてログに記録されます。

従業員の役割と業務上の必要性に沿って適切なアクセス権限が付与されていることを確認するために、企業リソースおよび製品リソースに対するすべての従業員のアクセスについて

は、毎日自動レビューを実施し、少なくとも半年に 1 回は人の手を介した再認証を実施します。

4.4 プライバシー

HubSpot は、お客様のデータのプライバシーを非常に重視しています。プライバシーポリシーに記載されているとおり、HubSpot がお客様の個人データを第三者に販売することはありません。本書に記載されている保護対策、およびそれ以外に弊社が導入している保護対策は、お客様のデータのプライバシーが守られ、改変を加えられないようにすることを目的としています。HubSpot 製品は、お客様のニーズとプライバシーに関する最新の考慮事項に基づいて設計、構築されています。HubSpot のプライバシーポリシーは、各種ベストプラクティス、お客様とそのコンタクトのニーズ、および規制要件を反映したものです。

以上の方針に従って、HubSpot は、EU・米国間のプライバシー シールド フレームワークおよびスイス・米国間のプライバシー シールド フレームワークの認証を取得しています。HubSpot の認証取得状況については、プライバシーシールドのサイトをご覧ください。また、HubSpot は TRUSTe のエンタープライズプライバシー認証も取得しています。

4.4.1 データ保持ポリシー

お客様のデータは、お客様が弊社の顧客として製品を利用している限り保持されます。HubSpot のプラットフォームでは、製品をご利用のお客様に、ご要望に応じてデータを削除できるツールが提供されます。過去にお客様であった方のデータについては、ご本人から書面による要請を受けた時点、またはすべての契約終了後に所定の期間が経過した時点で、ライブデータベースから削除されます。フリーミアム版のお客様のデータは、ポータルのご使用がなくなった時点で削除されます。また、過去に有料ユーザーであったお客様のデータは、お客様との関係がすべて終了してから 90 日が経過した時点で削除されます。レプリカ、スナップショット、バックアップとして保存されている情報が積極的に削除されることはありませんが、データライフサイクルの発生と共に、データリポジトリーにおいてエージングが行われます。HubSpot は、セキュリティー、コンプライアンス、または法令遵守の面で必要性がある場合は、ログや関連するメタデータなどのデータを保持します。

4.4.2 プライバシープログラムの管理

HubSpot の法務部門、セキュリティー担当チームなどの複数のチームでは、プライバシープログラムが効果的かつ一貫して実施されるように協力して取り組んでいます。お客様のプライバシーの保護に関する HubSpot の取り組みについては、プライバシーポリシーおよびデータ処理契約に詳しく記載されています。

4.5 事業継続性と災害復旧

HubSpot では、通信、システム、および業務運営に冗長性を持たせることによる機能停止の回避、ならびに可用性やパフォーマンスに関する問題が発生した場合の迅速な復旧戦略の両方に焦点を当てた事業継続および災害復旧の計画を維持しています。お客様に何らかの影響が及ぶような状況が発生した場合、HubSpot は迅速に、透明性を持って問題の切り分けと対処を行うことを目標とします。特定された問題については、HubSpot のシステム稼働状況に関するページで情報を公開し、解決に至るまで随時更新します。

4.5.1 システムの信頼性と復旧

HubSpot の通常の業務プロセスの一環として、事業継続性テストが行われています。HubSpot の復旧プロセスは、通常の保守プロセスおよびサポートプロセスを通じて継続的に検証されています。HubSpot では継続的デプロイメントの原則に従っており、保守および拡張の過程で多数のサーバーインスタンスの作成と破棄を日常的に行っています。また、この手順の中で、問題の発生したインスタンスや障害の復旧を行うことで、復旧プロセスを日常的に実践しています。

HubSpot では、インフラストラクチャーの冗長性、リアルタイムのレプリケーションおよびバックアップを主に利用しています。HubSpot のすべての製品は、十分な冗長性を持って構築されています。サーバーインフラストラクチャーは、HubSpot のインフラストラクチャープロバイダー内の複数のアベイラビリティーゾーンおよび仮想プライベート クラウド ネットワークに戦略的に分散されています。ウェブ、アプリケーション、データベースコンポーネントのすべてが、少なくとも N＋1 の補助的なサーバーインスタンスまたはコンテナーと共に展開されています。

4.5.2 バックアップ戦略

HubSpot では、複製したデータを耐久性に優れた複数の場所にバックアップとして保存しています。バックアップの保存期間はデータの性質によって異なります。また、複製したデータを複数のアベイラビリティーゾーンおよびインフラストラクチャーロケーションに保存することで、フォールトトレランスを実現すると共に、必要に応じたスケーラビリティーと迅速な復旧を可能にしています。

- お客様のデータ（本番環境のデータ）は、オンラインレプリカを複数用意してバックアップすることで迅速に保護されます。すべての本番環境のデータベースには、任意の時点の実データのプライマリー（マスター）コピーとレプリカ（スレーブ）コピーが少なくとも 1 つずつ存在しています。復旧を簡単に行えるように、すべてのデータベースのバックアップを 7 日分保存します。1 日に最低 1 回スナップショットを作成し、セカンダリーサービスに保存します。可能であれば、リアルタイムレプリケーションを使用します。すべての本番環境のデータセットは、Amazon S3 のような分散ファイルストレージ設備に保存されます。

- HubSpot ではホスティング、バックアップ、およびリカバリーにプライベート クラウド サービスを使用している関係上、製品に物理インフラストラクチャーや物理ストレージメディアを実装していません。また、お客様に自社製品を提供するにあたって、紙やテープなどのハードコピーのメディアを作成したり、使用したりすることは原則としてありません。
- 既定では、HubSpot 製品のインフラストラクチャーネットワークにアクセス制御による制限を課し、バックアップファイルが保存されているファイルシステムにアクセス制御リストを使用するほか、データベースに各種のセキュリティー保護対策を講じることで、すべてのバックアップを保護しています。
- それ以外にもデータのバックアップを希望されるお客様のご要望に対応できるように、HubSpot のプラットフォームには多数の機能が用意されています。HubSpot ポータルに含まれるツールの多くには、エクスポート機能が搭載されています。また、HubSpot のライブラリーで公開されている API を使用して、他のシステムとデータを同期することができます。データのバックアップ方法の詳細については、コンテンツのエクスポートに関するナレッジベースの記事をご覧ください。

4.6 HubSpot の企業としてのセキュリティー体制

4.6.1 従業員の認証と承認

HubSpot では、業界標準の企業パスワードポリシーを採用しています。このポリシーの下では、パスワードを少なくとも 90 日ごとに変更する必要があるほか、パスワードの長さを 8 文字以上とし、さらに特殊文字、大文字、小文字、および数字を使用して複雑なパスワードにすることが求められます。HubSpot では、複数の従業員がアカウントやパスワードを共有することを禁止しています。

従業員が HubSpot の製品インフラストラクチャーから認証を受ける際は、原則として SSH キーを使用します。パスワードの使用が許可されている場合は、パスワードポリシーにより 12 文字のパスワードが必要になります。このほか、HubSpot 製品の構築に使用されているすべてのツールは、多要素認証を使用しているか、多要素認証を必要とする SSO ソリューションで保護されています。

4.6.2 アクセス管理

HubSpot では、マーケティングプラットフォームやセールスプラットフォームを含む HubSpot のシステムに従業員がアクセスするための権限付与の手順を厳格に管理し、自動化しています。すべてのアクセスはログに記録されており、ほとんどの場合、RBAC モデルに基づいてアクセス権限が付与されます。厳格な認証機構の使用手順は自動化されており、この手順にジャストインタイムのアクセスが組み込まれています。

HubSpot では、大規模なサポートシステムを構築し、セキュリティー管理およびコンプライアンス作業を合理化および自動化しています。さまざまな機能に加えて、HubSpot のシステムでは 1 日のうち数回にわたって製品および企業のインフラストラクチャーを調査します。これにより、権限付与の適切性を確認し、従業員のイベントを管理して、必要に応じてアカウントおよびアクセス権限を失効させるほか、アクセス要求のログを蓄積し、自社テクノロジーの各セキュリティー統制のコンプライアンスの証拠を記録しています。これらの内部システムでインフラストラクチャーを調査することにより、承認された構成が維持されていることを 24 時間体制で検証しています。

4.6.3　身元調査

HubSpot の従業員には、現地の規制や雇用基準で許可される場合、正式な採用に先立って第三者による詳細な身元調査を実施しています。具体的には、採用候補者の職歴、学歴、および犯罪歴の確認を行っています。また、採用責任者の裁量により、リファレンスチェックを実施しています。すべての従業員は、社内のネットワークおよび本番環境ネットワークにアクセスするうえで、秘密保持契約および利用規定を遵守することが必要です。

4.6.4　HubSpot の企業としての物理セキュリティー

HubSpot のオフィスでは、さまざまな方法でのセキュリティー対策を実施しています。HubSpot の世界各地のオフィスでは、従業員の勤務環境の安全を確保するために警備員を配置しています。入退室は、各従業員に紐付けられた RFID トークンによって制御されます。この RFID トークンは、従業員の退職や使用頻度の減少などによって不要になった場合、または紛失時に自動でプロビジョニング解除されます。また、監視カメラなどの多くの保護対策が各 HubSpot オフィスで導入されています。

4.6.5　ベンダー管理

HubSpot は、お客様のマーケティング、営業、カスタマーサービスに関するニーズに合わせて HubSpot 製品の機能を補完するうえで、少数の外部のサービスプロバイダーを利用しています。HubSpot では、セキュリティーおよびプライバシーの管理が適切に行われるように、ベンダー管理プログラムを実施しています。このプログラムには、HubSpot に製品やサービスを提供するベンダーのセキュリティープログラムのインベントリー管理、トラッキング、およびレビューが含まれます。

提供されるサービスおよびやり取りされるデータの種類に応じて、適切な保護対策の評価が行われます。必要な保護対策が継続的に実施されていることは、ベンダーとの契約関係を維持するうえで必要な要件として管理されます。HubSpot のセキュリティーチーム、ゼネラルカウンシル、および各契約を管理する事業部門が、契約管理の一環としてサービスプロバイダーごとの個別の考慮事項について調整します。

4.6.6　セキュリティー意識とセキュリティーポリシー

HubSpot では、お客様のデータの保護に関して、エンジニアやサポートチームなどの全従業員が認識を統一できるように、「Written Information Security Policy（文書情報セキュリティーポリシー）」を作成し、これを維持しています。このポリシーでは、データ処理の要件、プライバシーに関する考慮事項、違反に対する対応などのさまざまな内容を扱っています。

このポリシーと共に多数の保護対策や基準を導入することに加え、HubSpot では従業員がそれぞれの職種に応じて十分なトレーニングを受けるようにしています。従業員それぞれの職種や付与されたアクセス権限に応じて、さまざまなレベルのセキュリティートレーニングが提供されています。すべての新入社員は、一般的なセキュリティー意識向上トレーニングを受け、HubSpot のセキュリティー要件について学習します。初回のトレーニングの後は、従業員の職種に応じてさまざまなトレーニングコースが提供されます。エンジニアリングチームには開発者向けのトレーニングが提供され、カスタマーサービスおよびサポート、営業などの職種向けには、それぞれの職種に特有の考慮事項に合わせてカスタマイズしたセキュリティー意識向上トレーニングが提供されます。また、トレーニングの更新、通知、社内での告知を定期的に行うことで、同じトレーニングを繰り返し受けられるようにしています。

4.7 インシデント管理

HubSpot は、24 時間年中無休の体制で、セキュリティーやプライバシーに関するあらゆる事案に迅速に対応します。HubSpot のインシデント対応プログラムでは、迅速かつ反復的な対応が可能です。インシデントのトラッキング、一貫したタスクの割り当て、エスカレーションおよびコミュニケーションを適時実行できるように、過去の傾向に基づくインシデントタイプの定義があらかじめ作成されています。多くの自動プロセスから、悪質なアクティビティーや異常に関するアラート、ベンダーのアラート、お客様からの要求、プライバシーに関するイベントなどの情報がインシデント対応プロセスに提供されます。

インシデントへの対応では、まず情報の曝露状況を確認し、可能であればセキュリティー問題の発生源を特定します。そして、被害を受けたお客様（およびその他に影響を受けたお客様）に結果を E メールまたは（E メールでは不十分な場合は）電話でご連絡し、インシデントが適切に解消されるように、必要に応じて定期的に情報を更新します。

セキュリティーに関するインシデントは、疑いにとどまるか実際に発生しているかを問わず、すべて CSO が確認します。また、インシデントの性質に応じた最も適切な方法を用いて、影響を受けたお客様と連携します。

5 製品のセキュリティー機能

HubSpot のセキュリティープログラムは、すべての HubSpot 製品を保護することを目的として策定されています。各製品ではアプリケーション開発のセキュリティーに関して一般的なベストプラクティスを採用しています。また、製品インフラストラクチャーにはセキュリティーと高可用性を確保する構成を採用しています。

HubSpot では、製品の利用料金の有無や機能の多寡にかかわらず、お客様からお預かりしたデータのプライバシーを保護するよう努めています。お客様が HubSpot 製品に保存するデータは、お客様に帰属します。HubSpot はお客様のデータを保護するためにセキュリティープログラムを導入します。また、自社のサービスを提供するために必要な場合のみ、お客様のデータを使用します。他のお客様とデータを共有したり、データを販売したりすることは決してありません。

5.1 HubSpot Marketing Hub

概要：HubSpot Marketing Hub は、業界最先端のマーケティング自動化ソリューションです。インバウンドマーケティング戦略の管理に効果的で使いやすいツールを搭載しています。

ホスティング：コンテンツ管理システム（CMS）のプライマリーインフラストラクチャーは、AWS および GCP でホスティングされています。このホスティング戦略は、冗長性、アーキテクチャーの柔軟性、およびインフラストラクチャーの応答性を高めるものです。デプロイプロセスでは、前述のとおりネットワークセキュリティー、サーバーセキュリティー、および可用性機能を活用しています。

ウェブ アプリケーション ファイアウォール：HubSpot 製品でホスティングしているお客様のサイトでは、世界的に評価の高い WAF による保護が得られます。HubSpot でホスティングしているお客様のウェブサイト、ブログ、ランディングページなどのオンラインコンテンツは、最新の DDoS 攻撃やその他のウェブアプリケーション攻撃から既定で保護されます。セキュリティーに関するイベントが発生した場合は、お客様のサイトが 24 時間 365 日継続的に保護されるよう、HubSpot のセキュリティー運営チームと DevOps チームが即座に対策を講じます。

トランスポートレイヤーのセキュリティー：HubSpot Marketing Hub をご利用のお客様は、サイト、ランディングページ、およびこれに関連して訪問者のエンゲージメントを高める枠組みに対して TLS サービスを構成し、利用することができます。既定では、TLS 証明書でサブジェクトの別名を使用する設定になっています。また、証明書の管理は、コンテンツ配信事業者が行います。TLS の設定については、こちらのナレッジベースの記事をご覧ください。

暗号化オプション：HTTPS を使用するお客様のウェブサイトでは、TLS 1.0、1.1、1.2、1.3 が既定で有効化されています。これらのプロトコルのうち、一部のサポートを解除することも可能です。また、HubSpot でホスティングされているドメインでは、HTTP Strict Transport Security（HSTS）も有効化できます。これらの設定を変更するには、HubSpot のサポートチームまたは担当のカスタマー サクセス マネージャーまでお問い合わせください。

5.2 HubSpot CRM

概要：HubSpot CRM は、営業チームに役立つ多くの HubSpot 製品の 1 つです。料金は無料で、導入にあたって面倒な作業も必要ありません。HubSpot CRM の製品紹介ページから、すぐに利用を始めることができます。

既定のセキュリティー：HubSpot CRM には、他のすべての HubSpot 製品と同じ高度なセキュリティー対策が導入されており、弊社が長い年月をかけて改善を重ねてきた安全で高度なソフトウェア開発プロセス、インフラストラクチャー管理、アラート送信の手法が採用されています。

E メールの連携と受信トレイの接続：HubSpot CRM は、Gmail、Office 365、IMAP 対応の E メールの受信トレイと接続できます。Gmail および Office 365 との連携は、プラットフォームのネイティブ連携機能によって許可され、保護されます。IMAP の連携機能によって受信トレイを接続すると、他の E メールサービスの E メールを HubSpot CRM に同期させ、HubSpot 製品を IMAP クライアントとして使えるようになります。IMAP との連携をサポートするサービスには、多くの保護機能が組み込まれています。転送中のデータはエンドツーエンドで暗号化され、保存中のデータはフィールドレベルおよびデータベースレベルで暗号化されます。また、許可されたユーザーだけがデータにアクセスできるように、アクセス制御が行われています。

プライバシー：HubSpot では、製品の利用料金の有無にかかわらず、お客様からお預かりしたデータのプライバシーを常に保護しています。お客様が HubSpot 製品に保存するデータは、お客様に帰属します。HubSpot は、サービスを提供するために必要な場合のみ、お客様のデータを使用します。

ホスティング：HubSpot CRM のインフラストラクチャーは AWS でホスティングされており、他の HubSpot のインフラストラクチャーと同じく冗長性と柔軟性を備えています。また、弊社のホスティング戦略により、インフラストラクチャーとネットワークに世界最高クラスのセキュリティーと可用性を確保しています。

アクセス制御：HubSpot CRM には、管理しやすくわかりやすい役割が用意されており、営業部門のメンバーにアクセス権限を適切に付与することができます。ユーザー権限の詳細については、こちらのナレッジベースの記事をご覧ください。

5.3 HubSpot Sales Hub

概要：HubSpot Sales Hub には、業界でその価値を認められた HubSpot のセールスツールが含まれており、担当者とリードの間のコミュニケーションの質を向上させ、コンバージョンを促進する効果があります。

ホスティング：HubSpot Sales Hub のプライマリー バックエンド インフラストラクチャーは AWS でホスティングされています。ホスティング戦略は、HubSpot のインフラストラクチャーに共通する冗長性と柔軟性を活用した内容となっています。

データストレージ：HubSpot Sales Hub では、E メールのトラッキング、リンクテキストの表示、および接続のサービスを提供するために、E メールメッセージのメタデータを保存します。データは HubSpot のインフラストラクチャーの内部で保護された場所に格納され、アクセスが厳しく制限されます。データストアへのアクセスは、役割に基づいて HubSpot の少数の従業員にのみ割り当てられ、カスタマーサポートおよびそれに関連する要求に対応するうえで必要な担当者に限定して許可されます。

シームレスな更新：HubSpot Sales Hub のツールは、生産性の向上に役立つように設計されています。ツールの利便性を強化するために導入されたのが、プラグインの自動更新です。ソフトウェアの更新通知が繰り返し届くと、業務の妨げになるため、通知の代わりにプラグインを使用して更新処理が行われるようになっています。

5.4 HubSpot Service Hub

概要：HubSpot Service Hub には、顧客満足度の向上に必要なすべての機能が搭載されています。Service Hub には顧客とのコミュニケーションをシームレスにトラッキングする機能が含まれているほか、高度なボットテクノロジーを利用してサイトの訪問者をサポートする機能があります。

ホスティング：HubSpot Service Hub のプライマリー バックエンド インフラストラクチャーは AWS でホスティングされています。ホスティング戦略は、HubSpot のインフラストラクチャーに共通する冗長性と柔軟性を活用した内容となっています。

シームレスな更新：Service Hub のツールは、自社のサービスに対する顧客のエンゲージメントを維持できるように設計されています。カスタマーサービスに関するお客様のニーズに対応できる機能を提供するために、Service Hub ではツールが定期的に自動更新されます。

6 コンプライアンス

HubSpot は TRUSTe のエンタープライズプライバシー認証を取得すると共に、EU・米国間のプライバシーシールドを遵守しています。また、HubSpot のプラットフォームには、お客様が一般データ保護規則（GDPR）の準拠要件を達成および維持しやすくなるようにするための機能が含まれています。HubSpot 製品におけるプライバシー関連のコンプライアンスについては、GPDR への準拠に関するページや HubSpot のデータ処理契約をご覧ください。

HubSpot の製品には、世界的規模のクラウド インフラストラクチャー プロバイダーである AWS と GCP を採用しています。HubSpot が利用するインフラストラクチャープロバイダーは SOC 2 Type II および ISO 27001 の認証を取得しており、施設では物理的および電子的侵入を防ぐセキュリティーが維持されています。

7 本書の対象読者および使用について

HubSpot はお客様にソリューションを提供するうえで透明性を重視しており、本書も透明性の重視を念頭に置いて作成しています。HubSpot では、導入済みの保護対策を継続的に改善しています。これに伴い、本書に記載されている情報およびデータ（関連する通知事項を含む）は、HubSpot といずれかの当事者の間に法的拘束力のある義務または契約上の義務を発生させることを意図するものではありません。また、HubSpot といずれかの当事者の間で締結されている既存の契約の内容を修正、変更、または改訂することを意図するものでもありません。