最終更新日：2021年10月

セキュリティー概要

HubSpot

目次

HubSpotセキュリティー概要

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、カスタマーサービス、コンテンツ管理、オペレーション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、世界の120を超える国と地域で、10万社以上のお客さまが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さまに提供されます。

HubSpotによるセキュリティーとリスクへの重点的な取り組み

セキュリティーに関してHubSpotが最優先しているのは、お客さまのデータを保護することです。そこで、お客さま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、コーポレート（社内の）セキュリティーと製品のセキュリティー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、最高情報セキュリティー責任者（CISO）が監督します。

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。

- お客さまを守り、信頼に応える – お客さま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 – 全てのユーザー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 – お客さまの情報に破損や不正な変更が発生しないようにします。
- 規制や基準を順守する – コーポレート セキュリティー プログラムの策定においては、Center for Internet Security（CIS）のCritical Security Controlsなど、サイバーセキュリティーに関する業界のベストプラクティスのガイドラインに準拠します。また、お客さまのデータの可用性、機密性、セキュリティーに関する内部統制も、SOC 2により米国公認会計士協会（AICPA）が定めたTrustサービス原則（TSP）に準拠しています。

HubSpotのセキュリティー統制

HubSpotでは、お客さまからお預かりしたデータを保護するために、防御手法の粒度を高めて、全社的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。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の製品インフラストラクチャー

クラウドインフラストラクチャーのセキュリティー

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。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 プロバイダーであるアマゾン ウェブ サービス（AWS）に外部委託しています。各ホスティングプロバイダーによって、99.95～100%のサービス可用性が保証されており、電源、ネットワーク、空調設備の全てについて冗長性が確保されています。

HubSpotのAWSの製品インフラストラクチャーは米国東部リージョンまたはドイツリージョンで運用されています。AWSは、セキュリティープログラムの監査を継続的に受けるとともに、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を維持しています。事業継続性や災害復旧計画は、SOC 2 Type IIおよびISO 27001の認証を受ける上でそれぞれ個別に検証されています。

コンプライアンスに関する文書は、AWSクラウドコンプライアンスのページで公開されています。

HubSpotとしても、クラウドインフラストラクチャーに関してよく寄せられる質問のナレッジベース記事を公開しています。

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では、プラットフォーム全体の全ての接続に対して多層的なフィルタリングと検査が実行されます。

ネットワークレベルのアクセス制御リストにより、社内の製品インフラストラクチャーに対する不正なネットワークアクセスが阻止されます。ファイアウォールにより、明示的に許可されていないネッ

トワーク接続は既定で拒否されるほか、トラフィックの監視によって異常なアクティビティーが検出されます。

弊社のネットワークセキュリティー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。ファイアウォールのルールセットは年次の再確認を通して、必要な接続のみが設定される状態にしています。

構成管理

HubSpotでは、お客さま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拡張することができます。サーバーインスタンスは、プロビジョニングからプロビジョニング解除まで厳格に制御されています。基本要件から逸脱した設定は、検出され、あらかじめ定義された周期で元に戻されます。本番環境サーバーが基本要件の設定から逸脱した場合には、30分以内に基本要件の設定で上書きされます。

サーバータイプの設定は、イメージおよび設定ファイルに全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。

パッチ管理は、自動設定管理ツールを使用するか、必要な基本要件を満たせなくなったサーバーインスタンスの削除と代替インスタンスのプロビジョニングを行うことによって対処します。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。

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機能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ともに、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、素早く確実に解決できるように、自動システムから適切な担当者に通知されます。

また、不測の事態にも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れるため、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。

アプリケーションの保護

ウェブアプリケーションの防御

HubSpotのプラットフォームでホスティングされているお客さまのコンテンツは全てウェブ アプリケーション ファイアウォール（WAF）で保護されます。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、お客さまに最適な保護を提供できるようになっています。このようなツールによって、アプリケーションレイヤーのトラフィックをリアルタイムで積極的に監視し、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には、通知やトラフィックの遮断を行うことが可能です。

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。分散型サービス妨害（DDoS）攻撃に対する防御も組み込まれており、お客さまのウェブサイトやその他のHubSpot製品の継続的な稼働に役立てられています。

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CD（継続的デリバリー）を駆使したソフトウェア開発を実践することで製品の最適化を徹底しています。

新しいコードの提案、承認、マージ、展開（デプロイ）が毎日頻繁に行われています。コードはレビュー、テスト（該当する場合）、マージの承認を経て展開されます。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、承認されたコードはHubSpotのCI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。

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。

HubSpotでは、広範なソフトウェアゲーティングおよびトラフィック管理を通じて、お客さまの選択（プライベートベータ、パブリックベータ、フルローンチ）に応じた機能管理を実現しています。SaaSアプリケーションのHubSpotはシームレスな更新を特長とし、リリースの際にダウンタイムを伴うことがありません。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（英語）で通知されます。

新しく開発されたコードは、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。

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。

脆弱性スキャンでは、悪用される恐れのある脆弱性のスキャンが毎日実行されます。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、適応型スキャンの包含リストの使用、脆弱性検出シグネチャーの継続的な更新を行っています。

また、業界有数の第三者による侵入テストを毎年実施して、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。

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、バグ報奨金プログラムを実施し、HubSpot製品のセキュリティー面の不具合の特定に向けて独立のセキュリティー研究者を招待しています。セキュリティーコミュニティーのメンバーおよびHubSpotのお客さまは、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（英語）をご覧ください。

お客さまのデータの保護

テナントの論理的な分離

HubSpotでは、拡張性の高いマルチテナント型のSaaSソリューションを提供しています。HubSpotのユーザーインターフェイスとAPIによるアクセスは、許可されたコンテンツに限定されます。HubSpotでは、データの論理セグメンテーションをポータルIDによって行い、この固有IDに特定のお客さまの全てのデータとオブジェクトを関連付けています。情報は、特定のHubSpotポータル向けに作成されたユーザーインターフェイスまたはAPIから提供されるため、ポータルをまたいだアクセスやデータ汚染のリスクがありません。

権限付与のルールは設計アーキテクチャーに組み込まれていて、継続的な検証を実施しています。また、アプリケーションの認証と認証に関する変更、アプリケーションの可用性、およびユーザーのページビューをログとして記録しています。

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、コンテンツ管理、オペレーション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（見込み客）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のツールで収集および保存される情報の種類は、お客さまご自身で設定することができます。お客さまは、HubSpotのお客さま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、コンテンツ管理、オペレーションのプロセスを実施する上で収集する情報を、適切な種類に限定する責任を負うものとします。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、または雇用、経済状態、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。

HubSpotのシステムで使用およびサポートされるデータの分類の詳細については、弊社のSOC 2報告書のデータ分類表をご覧ください。

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（API呼び出し、認証済みのセッションなど）は、全てTLS（Transport Layer Security）1.2または1.3および2,048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、お客さまが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場合は、そのウェブサイトでもTLSが既定で有効になっています。

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およびSSLとドメインセキュリティーに関するナレッジベースの記事をご覧ください。

HubSpotは、保存中のデータを暗号化する上で、複数のテクノロジーを使用しています。プラットフォームのデータは、AES-256の暗号化を使用して保存されます。ユーザーのパスワードは業界のベストプラクティスに従ってハッシュ化され、保存中に暗号化されています。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。

鍵の管理

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、暗号化するデータの機密性によって異なります。TLS証明書の場合、一般的な更新頻度は年に1回です。

HubSpotでは現在、お客さまから提供された暗号鍵を使用することはできません。

データのバックアップと災害復旧

システムの信頼性と復旧

HubSpotは、システムの可用性の確保に向けて、所与の月におけるサブスクリプションサービスについて99.95%のサービス稼働率を達成するべく、商業的に合理的な努力を尽くします。詳細については、製品別規約の第8条をご参照ください。

また、HubSpotのシステム稼働状況サイトでは、システムの稼働状況やセキュリティーに関するリアルタイムの最新情報や過去のデータをご確認いただけます。

HubSpotの全ての製品は、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、データベースの全てのコンポーネントが、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。

災害復旧

HubSpotは、SOC 2統制の一環として、災害復旧計画を維持し、年に1回テストを実施しています。詳細については、弊社のSOC 2報告書（legal.hubspot.com/ja/securityからダウンロード可能）をご覧ください。

バックアップ戦略

システムのバックアップ

システムは、決められたスケジュールおよび頻度で定期的にバックアップされます。復旧を簡単に行えるように、全てのデータベースのバックアップを7日分保存します。バックアップが正常に実行されるかどうかが監視され、例外が発生した場合はアラートが送信されます。バックアップ失敗のアラートはエスカレーションされて、調査、解決されます。

データは各地のリージョンに毎日バックアップされます。また、プライマリーリージョンで障害が発生した場合に復旧できるように、バックアップは別のAWSリージョンにも定期的にコピーされます。レプリケーションの問題については、監視とアラートを実施するとともに、発生時には優先度を判定した上で対応します。

全ての本番環境のデータセットは、Amazon S3のような高可用性ファイルストレージ設備に保存されます。

物理バックアップストレージ

HubSpotではホスティング、バックアップ、およびリカバリーにパブリック 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、お客さまに自社製品を提供するに当たって、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。

バックアップの保護

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ことで、全てのバックアップを保護しています。

お客さまによるバックアップ方法

それ以外にもデータのバックアップを希望されるお客さま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実装されています。また、HubSpotのライブラリーで公開されているAPI（英語）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。

IDおよびアクセス制御

製品ユーザー管理

HubSpot製品では、権限付与のルールを細かく設定できます。お客さまは、ポータルのユーザーを作成、管理して、適切な権限を割り当てることで、データ機能に対するユーザーのアクセスを限定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。

製品ログインの保護

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に標準搭載のログイン、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。標準搭載の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に標準搭載の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。

Google アカウントによるログイン機能は、HubSpotの全てのお客さまにご利用いただけます。SAMLベースのIDプロバイダー（IdP）と連携可能な高度なSAMLベースのSSOは、HubSpot製品の全てのEnterpriseプランで利用できます。

SSOプロバイダーを使用しているお客さまは、SSOベースのログインを設定できます。SSOの設定手順は、こちらのナレッジベースの記事やHubSpotアカデミー（英語）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に標準搭載のログインを使用するお客さまは、HubSpotアカウントに2要素認証を設定することが推奨されます。ポータルの管理者は、全てのユーザーが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。

製品APIの承認

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。お客さまは自社のポータル用のAPIキーをご自身で生成できます。こうしたキーの用途としては、カスタム連携の迅速なプロトタイプ作成が想定されています。APIリクエストの認証および承認の方法としては、HubSpotのOAuthを実装する方が強固です。また、機能の連携にはOAuthが常に必要になります。OAuthによるリクエストの承認は、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。

本番環境のインフラストラクチャーへのアクセス

HubSpotのシステムに対するアクセスは厳格に制御するとともに、最小権限の原則に従っています。HubSpotの従業員には、役職に基づくアクセス制御（RBAC）モデルによってアクセス権を付与します。

日常的なアクセスは、職務上必要な最小限のユーザーに限定されます。緊急アクセス（アラートへの対応やトラブルシューティングなど）と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。JITAの各要求はログに記録され、異常な要求がログに記録されていないかどうかが常に監視されています。アカウントへのアクセスは、規定のセッション制限を超えると有効期限が切れ、自動的に失効します。

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、ユーザーごとに固有の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。

全社的なリソースおよび本番環境のリソースに対する従業員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。

HubSpotの従業員によるお客さまのポータルへのアクセス

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、お客さまのポータルに対するJITAアクセスを要求することができます。ただし、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、お客さま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、特定のお客さまのポータルへの最大24時間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全てログに記録されます。

社内での認証と承認

リモートまたはオフィスでコーポレート（会社の）ネットワークにアクセスするには、多要素認証（MFA）が必須になります。HubSpotが使用しているSaaSアプリケーションでは、アクセス制御を一元化するために、MFAによるSSOが必要です。

パスワードポリシーは、業界のベストプラクティスに従って、必要な長さ、複雑さ、ローテーションの頻度を決定しています。

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と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社内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。

企業としてのセキュリティー

身元調査と研修

米国のHubSpotの従業員には、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。米国

以外では、雇用時の調査として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。

全ての従業員は入社時にHubSpotの利用規定（AUP）およびCode of Use Good Judgement（CUGJ）を読み、同意する必要があります。これらのドキュメントには、会社の資産またはデータの保護（モバイルデバイスの保護や、社内の機器のセキュリティーなど）における従業員のセキュリティーに関する責任が定められています。

ポリシー管理

HubSpotでは、データの保護に関して全従業員が認識を統一できるように、多数のポリシーと手順を文書化して維持しています。その中核となる「Written Information Security Policy（文書情報セキュリティーポリシー）」では、データ処理の要件、プライバシーに関する考慮事項、違反への対応などのさまざまな内容を扱っています。

ポリシーは少なくとも年1回見直し、承認した上で社内Wikiページに保存されます。従業員の同意を必要とするポリシーは、必須の年次トレーニングに組み込まれています。

セキュリティー意識向上トレーニング

HubSpotでは、従業員が防御の第一線を担うと考え、職種に応じて十分なトレーニングを受けられるようにしています。全般的なセキュリティーのベストプラクティスについて学習するセキュリティー意識向上トレーニングは、新しい全従業員を対象に提供し、以降は年に1回提供します。意識向上トレーニングに加えて、HubSpotはセキュリティーに関する最近のニュースや取り組みについて、社内のナレッジベースの記事で従業員に周知しています。

初回のトレーニングの後は、従業員の職種や付与されるアクセス権に応じてさらに専門的なコンテンツが提供されます。例えば、HubSpotのSecurity Advocatesプログラムでは、製品チームの開発者が、セキュリティー開発、一般的なリスク、脅威、問題に関する追加のトレーニングを受講できます。

リスク管理

HubSpotではEnterprise Risk Management（ERM）プログラムを規定し、ERMポリシーの文書化、継続的なリスク評価、正式なリスク登録などを行うことを定めています。リスクに対する軽減策および対処は、チケットを利用したシステムで追跡し、規定の周期でレビューを実施します。

リスク評価とリスク管理プログラムの詳細については、SOC 2報告書（legal.hubspot.com/ja/securityからダウンロード可能）をご覧ください。

ベンダー管理

HubSpotは、お客さまのマーケティング、営業、カスタマーサービス、コンテンツ管理、オペレーションに関するニーズに合わせてHubSpot製品の機能を補完する上で、複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、適切な保護が行われているかどうかが評価されます。必要な保護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上での必須要件として管理されます。ベンダー管理のレビュープロセスでは、HubSpotのセキュリティー、法務、コンプライアンスの各部門が業務の関係者と共同で評価を行います。

なお、データ処理契約（DPA）に復処理者のリストを掲載しています。

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。また各HubSpotオフィスには、監視カメラなどの多くの保護が導入されています。

コーポレートネットワークの保護

HubSpotのオフィスでは、一元管理されたアプリケーションファイアウォールを導入して高可用性を確保しています。ゲストネットワークはコーポレートネットワークから分離され、別のファイアウォールによってサービスが提供されています。ファイアウォールにより、インターネットからの不正な受信トラフィックがフィルタリングされるほか、ルールによって明示的に許可されていない受信ネットワーク接続が拒否されます。

HubSpotでは、コーポレートネットワークへのデバイスの接続を許可する前に、システムのコンプライアンスチェックを実施しています。許可されていないデバイスは直ちに切断されるか、封じ込めVLANに移されます。

エンドポイント保護とウイルス対策およびマルウェア対策

HubSpotでは、EDR（Endpoint Detection and Response）機能を利用して自社のシステムを保護しています。これにより、システムの異常な挙動に関する幅広い情報を把握できるほか、イベントの自動トリガーや手動でのシステムの封じ込めにより、迅速に調査して適切な措置を講じることができます。EDRプラットフォームをセキュリティースタックの他のツールと連携させることで、複数のツールによる最適化されたエコシステムを構築し、効果的な防御を実現しています。

インシデント管理

インシデント対応

HubSpotのSecurity Operations Center（SOC）チームは、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、お客さまからの要求、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、まず情報の暴露状況を確認し、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。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、全てCISO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、影響を受けたお客さまと連携します。

SOCに加えて、HubSpotでは社内にThreat Hunterチームを編成し、脆弱性の体系的な発見とベストプラクティスの徹底に取り組むことで、製品のセキュリティーを確保しています。

コンプライアンス

サーベンス・オクスリー法（SOX法）

HubSpotは上場企業としてSOX法を順守しており、その一環として主要なIT規制について定期的に監査を受けています。

HubSpotのSOX法の順守状況に関する情報および年次財務諸表は、SEC提出書類として公開しています。詳細については、投資家向け情報ページ（https://ir.hubspot.com/、英語）をご覧ください。

System and Organization Controls（SOC 2）

HubSpotは毎年SOC 2 Type IIおよびSOC 3に関する厳格な監査を受けることで、米国公認会計士協会（AICPA）が定めたTrustサービス原則（TSP）に従って、お客さまのデータのセキュリティー、可用性、機密性に関してHubSpotが実施している内部統制を保証しています。HubSpotにおける内部統制の有効性の証明としてSOC 2 Type II報告書の写しをご希望の場合は、HubSpotの担当者までご連絡ください。弊社のSOC 3報告書は、HubSpotのセキュリティーページ（legal.hubspot.com/ja/security）からダウンロードできます。

機密データの処理と保管

どのようなデータが禁止されるかについては、お客さまサービス利用規約（legal.hubspot.com/jp/terms-of-service）をご覧ください。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、経済状態、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。

医療関係でもHubSpotは、機密性の高い医療情報を扱わない場面で利用者との接点に活用されていますが、このことからePHI（電子的に保護される医療情報）を処理または保管するためのソリューションと誤解することがないように、ご注意ください。医療規格のHIPAAには準拠しておらず、HITRUST認証も取得していません。

同様に、HubSpotのサービスへのお支払いにはクレジットカードをご利用になれますが、HubSpotでは、お客さまから送信されたクレジットカード情報の保管、処理、収集していません。

また、PCI-DSSには準拠していません。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処理ベンダーに委託することで、取引を安全に処理しています。

プライバシー

HubSpotは、お客さま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通り、HubSpotがお客さま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、お客さま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、お客さま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、お客さま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。

データの保持と削除

お客さまのデータは、お客さま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さまに、データを削除するツール（DPAの「個人データの削除または返却」条項を参照）およびデータをエクスポートするツール（コンテンツとデータのエクスポート方法に関するナレッジベースの記事を参照）が提供されます。

過去にお客さま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、または全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さまのデータは、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さまのデータは、お客さまとの関係が全て終了してから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、データのライフサイクルに伴って、古くなった情報はリポジトリーから取り除かれます。HubSpotは、セキュリティー、コンプライアンス、または法令順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。

HubSpotでは現在、カスタムのデータ保持ポリシーを定義する機能を提供していません。

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。お客さま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、以下に詳しく記載されています。

- プライバシーポリシー
- 製品プライバシーポリシー
- データ処理契約

データ侵害への対応

侵害報告ポリシー、プロセス、義務の概要については、SOC報告書の「インシデント対応」の項目をご覧ください。

また、個人データの侵害に関するHubSpotの義務は、データ処理契約（DPA）にも記載しています。

GDPR

HubSpotプラットフォームには、GDPR（一般データ保護規則）の準拠要件への対応を支援するさまざまな機能が搭載されています。例えば、GDPRのデータ主体アクセス要求（DSAR）への対応としてデータを削除する機能（ナレッジベースの記事を参照）があります。設定については、GDPRのページをご覧ください。

本書の対象読者および使用について

HubSpotはお客さまにソリューションを提供する上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、または改定することを意図するものでもありません。