Smartsheet セキュリティ

Smartsheet のセキュリティ機能、慣行、保護についての詳細な説明

エグゼクティブ サマリー

エンタープライズグレードの Software-as-a-Service (SaaS) プラットフォームは、複数の防御層と多数の IT 保護および制御策を備え、機密性の高い企業データをセキュアに保持しなければならないことを、Smartsheet は理解しています。また柔軟性に富み、既存のデータ セキュリティ システムやプロセスと統合できることも重要な要件です。

このホワイトペーパーでは、Smartsheet のセキュリティとガバナンスの機能、保護、慣行について説明しています。最初に、セキュリティ、コンプライアンス、そして十分なガバナンスが確保されている業務環境を維持するために Smartsheet が実装を推奨する、お客様によって制御される機能に焦点を当てます。注: このホワイトペーパーでは一般的に使用できる機能のみを取り上げています。一部の機能については、追加購入が必要な場合や、すべてのプラン レベルに含まれない場合があります。

概要

組織のセキュリティを最高度に保つため、Smartsheet ではアイデンティティおよびアクセス管理、データ ガバナンス、グローバル アカウント構成という 3 つの主な重点領域に関する制御を実装するよう推奨しています。これらのトピックに加え、本文書には Smartsheet のセキュリティ、プライバシー、コンプライアンス慣行に関する総合的な情報を記載しています。

- **アイデンティティおよびアクセス管理**では、ユーザーによる Smartsheet へのアクセス方法を制御することで、プラットフォーム内における各ユーザーの役割とアイデンティティを組織の構造とポリシーに整合させることに重点を置いています。それに加え、セキュリティ設定に基づき、外部ユーザーと共同作業する際にセキュリティを確実に維持する方法を検討します。

- **データ ガバナンス**は、ユーザー レベルと組織全体の両方で施行する必要があります。ユーザーに関しては、Smartsheet では最小権限のアプローチが既定であり、追加の制御によって可視性をさらに制限および制御し、ユーザーが必要な時に必要なデータにのみアクセスできるようにしています。組織レベルでは、共有セーフ機能やユーザー レポートのようなシンプルなメカニズムと、データ エグレス ポリシーのような高度なオプション機能の両方をカバーします。

- **グローバル アカウント構成**を使用すると、Smartsheet 環境のデザインを、組織のブランドに合わせてカスタマイズできます。ユーザーが組織の保護された環境内にいることを視覚的に確認できるというようなシンプルなものであっても、セキュリティの確実な維持に役立てることができます。そうしたブランディングとカスタマイズの適用を固定化することで一貫性を確保し、作成したすべてのアセットが自社のブランドに沿ったものになるようにします。

- **セキュリティ、プライバシー、コンプライアンス慣行**は、お客様データのセキュリティを高度に保てるよう、Smartsheet がプラットフォーム外で維持管理している活動と保護を指します。Smartsheet では、人、プロセス、技術を組み合わせることで業界トップクラスの多層防御戦略を実施しており、Smartsheet の環境とアセットの機密性、完全性、可用性を保護しています。

目次

アイデンティティ管理

Smartsheet 内のユーザーのアイデンティティ (ID) を管理すること、そしてユーザーによるシステムへのアクセスを管理することは、プラットフォーム内におけるデータ管理と同様に重要です。Smartsheet では、認証の施行や自動化されたライフサイクル
管理から、API セキュリティや継続的モニタリングに至るまで、あらゆる規模のエンタープライズのニーズを満たすよう設計された多層型の ID 管理機能を提供しています。

認証方法

Smartsheet の活用の初期段階では、どの認証方法を使用するかを決めることになります。Smartsheet では電子メールとパスワードに加え、Google、Microsoft、Apple、および SAML 2.0 プロバイダーを介したシングル サインオン (SSO) など、複数のオプションを提供しています。

Smartsheet による SAML 2.0 のサポートは、Okta、Microsoft Entra ID、PingIdentity といった主要なエンタープライズ ID プロバイダー (IdP) と互換性があります。この幅広い互換性により、組織は既存の IdP への投資を活用しつつ、すべての SaaS アプリケーションで一貫した認証ポリシーを施行することができます。

すべてのユーザーに対して単一の SSO 認証方法を施行し、その他のログイン方法はすべて無効にすることを推奨します。これにより、資格情報ベースのより脆弱な攻撃面を排除し、ID プロバイダー内の認証ガバナンスを一元化することができます。

複数のドメインや連合型の IT 構造を有する組織のために、Smartsheet ではドメインレベルの SSO の施行をサポートしています。システム管理者は、特定の電子メール ドメイン (「@regionaloffice.com」や「@subsidiary.org」など) に属するユーザーが、所定の ID プロバイダーを使用して認証しなければならないように指定することができます。これにより、事業部門全体にまたがる形で ID ポリシーをカスタマイズできると同時に、ガバナンスとリスク軽減の強化が可能になります。

多要素認証 (MFA)

Smartsheet では SSO と並ぶ追加のセキュリティ層として、多要素認証 (MFA) を実装することを推奨しています。MFA の施行は ID プロバイダー レベルで管理するのが最善であり、セキュリティ チームは接続されたすべてのアプリケーションで MFA ポリシーを一元的に制御できます。

SSO を使用しないユーザーのために、Smartsheet では追加のログイン セキュリティ層として認証アプリベースの MFA をサポートしています。認証アプリでは、プライマリのサインイン方法として電子メールとパスワード、または電子メールベースのワンタイム パスコード (TOTP) のいずれかを組み合わせています。エンタープライズ プランのシステム管理者は、プランもしくはドメイン レベルで認証アプリによる MFA を要求できますが、エッジ ケースに備えて個々のユーザーを除外することができます。

注: 認証アプリベースの MFA は、Smartsheet のコア ログイン機能に適用されます。プレミアム アプリとアドオン機能では、お客様の組織に対して構成されている既存の Smartsheet 認証方法が用いられます。

セッション管理

エンタープライズ プランの管理者は、セッションの非アクティブ状態に基づくタイムアウトを構成できます。それにより、Web セッションとデスクトップ セッション全体で非アクティブ状態が一定期間 (15 分から最長 30 時間) 続いた場合に、ユーザーを自動的にサインアウトさせることができます。適切なタイムアウト ポリシーを確立することで、無人のセッションに起因する不正アクセスのリスクを軽減できるため、これをベースライン セキュリティ構成に含める必要があります。

ユーザー ライフサイクル管理

ユーザー アカウントを適切なタイミングでプロビジョニングおよびプロビジョニング解除することは、SaaS セキュリティ プログラムにおける最も重要な制御の 1 つです。Smartsheet では、Microsoft Entra ID および Okta とのディレクトリ統合を介した**クロスドメイン ID 管理システム** (SCIM) の統合をサポートしています。これにより、ユーザー アカウントの自動プロビジョニングおよびプロビジョニング解除を、ID プロバイダーから直接行うことができます。

SCIM を有効にすると、従業員を IdP に登録する際、もしくは IdP から登録解除する際に、その従業員の Smartsheet アカウントが自動的に作成または非アクティブ化されます。それにより、従業員の退職後もアクセス権を保持している孤立アカウントのリスクが排除されます。また、管理に要する経費が削減されるとともに、権限のあるディレクトリとアクセスとの一貫性が常に保たれます。

Smartsheet では SAML を介した**ジャストインタイム (JIT) プロビジョニング**もサポートしています。これにより、ユーザーが初めて SSO ログインに成功した際にユーザー アカウントが自動的に作成されるため、管理者による事前プロビジョニングの必要性がなくなります。これは大規模な組織や、登録件数が多い組織にとって特に便利です。

推奨事項:

- ユーザー ライフサイクル管理のプライマリ メカニズムとして、IdP とのディレクトリ統合を介して SCIM を有効にします。
- 登録件数が多い環境の場合は、補完手段として JIT プロビジョニングを使用します。
- 定期的なアクセス レビューの頻度を確立し、古いアカウントや孤立したアカウントを特定して是正します。

API セキュリティおよびトークン管理

Smartsheet では、堅牢な REST API のセットを提供しています。Smartsheet API は認証と承認に OAuth 2.0 を使用し、有効なアクセス トークンを含む HTTP ヘッダーをリクエストごとに要求します。構築するすべての統合で OAuth 2.0 を使用し、スコープ付きのセキュアな API アクセスを確実に維持するのがベスト プラクティスです。

OAuth 2.0 に加えて、Smartsheet では個人ユーザー向けにパーソナル API アクセス トークンもサポートしています。これらのトークンには大きな権限が伴うため、慎重に管理する必要があります。システム管理者はプランレベルのトークンの有効期限を構成することで、パーソナル API トークンがいつまでも有効なまま残るという事態を確実に防ぎ、従業員の退職や統合機能の廃止に起因するトークンの侵害、忘却、または孤立化による情報漏洩リスクを減らすことができます。より広範な資格情報ライフサイクル ポリシーに合わせて有効期限を調整し、セキュリティ要件と、トークンの定期的なローテーションによる運用上の影響との間でバランスを取る必要があります。

有効期限の他に、組織は以下のことを行う必要があります。

- **パーソナル API トークンを定期的に監査**し、使用されていないトークン、範囲が広すぎるトークン、または不要になったトークンを特定します。

- **トークンのローテーションを定期的に実行**し、侵害の疑いがある場合は直ちにローテーションを行います。
- サード パーティ統合向けに OAuth スコープを構成する際は、**最小権限の原則を適用**し、統合に必要な権限のみをリクエストします。
- **OAuth で接続されたサード パーティ アプリケーションを定期的にレビュー**し、承認済みの統合のみが組織のデータへのアクセス権を保持するようにします。

アクセス管理

ユーザー管理とユーザーによるアクセスの管理は非常に重要な管理機能であり、セキュリティと組織による Smartsheet の導入の両方に影響します。組織は両者を慎重に両立させることで、次第に分散化するデータとチームに合わせてリスクを管理しつつ、共同作業を促進する必要があります。Smartsheet ではこれをサポートするために、お客様によるアプリケーションの主な管理方法に合わせた 3 つの異なるガバナンス モデルを提供しています。

Smartsheet ガバナンス モデル

第一のアプローチは分散型 (連合型) モデルです。ここでは各事業部門が購入と計画を直接管理します。このモデルでは、基本的に IT チームは管理に関与せず、料金プラン、ガバナンス、ユーザー管理は部門の裁量に任されます。このモデルは一般的に、Smartsheet を導入したばかりの会社に適用します。

第二のアプローチは集中型 (統合型) モデルで、Smartsheet プランをすべて単一の、IT チームが管理するサブスクリプションに統合します。このモデルでは、支出、ユーザー管理、セキュリティ制御を直接管理できます。集中型モデルは、Smartsheet を活用するあらゆる局面について、IT チームが詳細なモニタリングを維持管理したい場合に最適です。

第三の共有型 (ハイブリッド) モデルはその両者を折衷したアプローチで、IT チームが Enterprise Plan Manager を活用して組織全体にまたがる設定を制御する一方、ライセンスとユーザーの管理はビジネス システム管理者が直接行います。請求もプランごとに切り分けられ、部門単位での請求が可能になります。IT チームに一元的に請求されるモデルと異なり、Smartsheet に関する支出はそれぞれの部門の予算に組み込まれます。

高水準のセキュリティを確実に維持するため、Smartsheet では共有型または集中型モデルを推奨しています。その場合、IT チームがプランをより直接的に管理できるからです。

ユーザー アドミニストレーション

社内のさまざまなチームが独自のニーズに応じて Smartsheet を個別に導入すると、それぞれ別のプランが複数作成される可能性があります。また、企業の合併や買収によって複数の Smartsheet プランが作成される場合もあります。

そうした分散型モデルを使用しているプランでユーザーを管理する場合は、各プランに対してアカウントの検出を有効化することを推奨します。アカウントの検出を使用すると、新規ユーザーが Smartsheet の利用を始める際に、当該ユーザーもしくは組織のドメインに属する誰かが社内の Smartsheet プランのリストを確認できます。そのため、新たなプランを始めるのではなく、既存のプランのいずれかに参加するためのリクエストを行える集中型の手段が得られます。それらのリクエストは自動的に社内のシステム管理者に (Smartsheet 管理センター経由で) 送信され、レビューと承認を受けます。

個別のプランが複数あり、かつ集中型モデルでユーザーを管理したい場合は、アカウントの統合を行わなければならない場合があります。注: Dynamic View、コネクタ、Control Center などのアドバンス機能を利用している場合は、統合に際して Smartsheet サポートと提携し、追加の支援を受ける必要があります。

共有型モデルと Enterprise Plan Manager を使用している場合は、部門/チーム/コスト センターを中心にプランを整理し、それぞれの所属先に基づいてユーザーを最も適切なプランに自動的に割り当てるポリシーを定義できるようにすることがベスト プラクティスです。

ライセンス/サブスクリプション モデル

Smartsheet のお客様の大半は、透明性が高く予測可能な価格設定、より迅速な価値実現、管理のさらなる簡潔化を実現する、現行のプランと価格モデルに移行しています。ただし、一部のお客様は従来の共同作業モデルを維持しているため、これら 2 つのモデルの違いをここで説明します。

旧共同作業者モデル

Smartsheet の旧共同作業者モデルは、作成者に製品へのアクセス権を提供しつつ、編集者やコメント者として無料で共同作業を行えるようにするという基盤の上に構築されていました。その結果、話題となって大きな成長を遂げたものの、プラットフォームを十分に活用できるユーザーが少ないという結果ももたらしました。料金を支払う必要があったのは、シート、レポート、ダッシュボード、またはワークスペースを作成する必要があるユーザーに限られていました。システム管理者はこのモデルの下、Smartsheet のユーザー タイプの理解、効果的なユーザー管理、ライセンスの適切な割り当て、リーダーシップ チームにプラットフォームの価値を示すことなど、多くの課題に直面していました。

ユーザー モデル

作成も重要ですが、Smartsheet は共同作業に適した業務管理プラットフォームであり、共同作業は私たちの中核を成しています。Smartsheet プラットフォームのパワーと価値は、チームがプロセス、プログラム、プロジェクトを作成し、重要なビジネス イニシアチブで共同作業を行えるようにするという点で、真に際立っています。ユーザー モデルは旧モデルの課題を克服するものであり、以下の内容を導入することで進化するビジネス ニーズに適応し、組織の成長に合わせた目標達成を可能にします。

- 新しいユーザー タイプ
- 暫定使用
- 調整期間と True-up (トゥルーアップ)

ユーザー モデルの詳細については、こちらの概要をご覧ください。

ユーザー管理

ユーザーを一度に 1 人ずつ追加するのでは、導入するユーザーの人数が数十人、数百人、さらには数千人と増加するにつれて対処できなくなることを、Smartsheet は理解しています。よって Smartsheet の利用を始めるときは、管理センターでユーザーの一括インポート機能を活用することを推奨します。この機能を使用すると、一度に最大 1,000 人のユーザーを自社の Smartsheet 組織に簡単に追加できます。同様に一括更新を使用して、役割とユーザー タイプを一度に編集することも可能です。

企業の合併や買収ではしばしばブランドの変更が生じ、ユーザーが新しいメール アドレスを取得することがあります。ユーザーの結合を使用すると、ユーザーのプライマリ メール アドレスを一括更新したり、重複するアカウントを一掃したりすることができます。

統合型の Smartsheet プランでは、次に挙げる 3 種類の追加機能を活用して、ユーザー管理をさらに合理化および自動化することができます。

- 自動プロビジョニング (UAP) を使用することで、エンタープライズ アカウントへのユーザー追加プロセスを自動化できます。ユーザーが会社のメール アドレスを使用して Smartsheet にサインアップまたはサインインす

ると、会社のアカウントに自動的に追加されます。さらに、ユーザーにライセンスを付与するか、あるいは暫定メンバーとしてアカウントに自動的に追加するかを選択できます。

- Smartsheet の統合型モデルを導入した場合は自動プロビジョニングを有効化して、IT チームが管理する中心的なアカウントに従業員が自動的に追加されるようにすることを推奨します。
- 共有型モデルを使用していて、組織がユーザー リストとして使用できる部門/コストセンター情報を文書化している場合、UAP を有効化することを推奨します。そうすることで、情報をインポートして、ユーザーがライセンスをリクエストした場合に適切なプランに自動的に割り当てることができます。またこの情報は、ライセンスなしユーザーのプラン間の移動を自動化する際にも使用されます。
- ディレクトリ統合を使用すると、Microsoft Entra ID または Okta Directory ユーザーを Smartsheet に直接同期できます。Entra ID または Okta 内で Smartsheet を既存の自動化にプラグインすることで、ユーザーの登録と登録解除を完全に自動化できるため、ユーザーが自分の Smartsheet アカウントにいつまでも留まったり、再度アクセスしたりするリスクを最小化できます。もう 1 つのメリットとして、部門/コスト センター/部署といったユーザー レベルの属性を Smartsheet チャージバック レポートで確認できます。このレポートは管理センターで閲覧でき、社内のチャージバックを促進するために使用できます。ベスト プラクティスとして、ディレクトリの全ユーザーを組織の Smartsheet アカウントに同期させることを推奨します。そうすることで、ユーザーが最初にログインした時に、IT チームが認識していない新たな Smartsheet アカウントを作成してしまうことを防げます。第 2 の防御層として、自動プロビジョニングを有効化したままにして、ディレクトリ経由で同期されていないユーザーを残らず把握することも可能です。

ユーザーが組織を離れる際には、Smartsheet へのアクセス権を削除することが重要です。プランからユーザーを削除すると、そのユーザーの Smartsheet へのアクセス権が取り消され、プランが所有する共有アセットから削除されます。退職するユーザーが所有しているアセットはシステムに留まりますが、所有者がいないまま残される可能性があります。システム管理者は、削除の前または後にそれらのアセットの所有権を確認して移行し、自動化が機能しなくなる、あるいはコンテンツにアクセスできなくなる事態を防ぐ必要があります。

Smartsheet での役割とユーザー タイプ

ユーザーのプロビジョニング方法とは関係なく、組織内のユーザーに対して Smartsheet での役割を決める必要があります。

役割の割り当ては、それらのユーザーに組織の Smartsheet アセットへのアクセス権を付与するものではありません。またアセットは直接それらのユーザーと共有する必要があります。すなわち、役割とアセットへのアクセス権限の両方によって、関係者が Smartsheet で閲覧できるものとできることが決まります。Smartsheet は次に挙げる主な役割をサポートします。

- 資格情報を持つユーザー: ユーザー タイプと権限の対象となる Smartsheet サービスにアクセスして使用します。
    - メンバー (有償ライセンス): フル アクセス権を有するユーザーで、アセットの作成と管理、編集、ファイルのアップロードを実行できます。
    - 暫定メンバー: 限られた期間フル アクセス権を有するユーザー。
    - 閲覧者: 情報の閲覧が可能な無料ライセンスを有するユーザー。
    - ゲスト: 情報の編集、コメント、または閲覧を行える外部ユーザー。
- グループ管理者: Smartsheet グループを作成して管理します。(同時にライセンス ユーザーである必要があります)*

- システム管理者: ユーザー、アカウント設定、セキュリティ制御を管理します。

侵害などのセキュリティ インシデントが発生した場合でも管理者アカウントを管理または復元できるようにするなど、アクセス制御と管理制御の継続性を確実に維持するために、組織の Smartsheet アカウントに少なくとも 2 人のアクティブなシステム管理者を割り当てることを強く推奨します。

グループ管理者は Smartsheet グループを作成できます。それにより、ユーザーは各メンバーと個人的にコンテンツを共有するのではなく、グループでコンテンツを共有できるようになります。グループ管理者は自分が所有するグループのみを管理できます。必要に応じて、外部の共同作業者を制限するために、グループへの参加資格を組織内の関係者のみに限定します。

ユーザーに上記の役割をいずれも割り当てなかった場合、そのユーザーに共有された Smartsheet アセット (シート、レポート、ダッシュボードまたは WorkApps) のみにアクセスが限定されます。Smartsheet アセットを作成する場合、関係者はライセンス ユーザーでなければならず、Smartsheet アプリからライセンスを直接リクエストできます。システム管理者はリクエストの追跡と対応を個別に行うか、あるいは管理センターのライセンス リクエスト管理セクションにて一括で行うことができます。ライセンス リクエストの管理プロセスを既に確立している場合はカスタム アップグレード画面を利用し、それらの内部プロセスを介してライセンス リクエストを送信するようユーザーに指示することを検討してください。

ゲスト

Smartsheet アセットを共有されているドメイン外のユーザーはすべてゲストと見なされます。Smartsheet を使用することで、組織は信頼できる外部の関係者と自由に共同作業を行えます。しかも、そうしたゲストについて費用は発生しません。外部と連携する際にセキュリティを確実に維持できるよう、次に挙げる 3 種類の一元的な管理者制御を活用することを推奨します。

共有セーフ: 外部との共同作業に向けて、信頼性の高い承認済みのドメインまたはメール アドレスを指定します。

シート アクセス レポート: 組織の Smartsheet コンテンツにアクセスできるゲストのリストを確認できます。

アイテムへのアクセスの取り消し: 管理センターを介して一元的に管理することで、アクセスする必要がなくなったコンテンツから
ゲストを削除します。

ゲスト認証制御

組織外のユーザーと共同作業する際に機密コンテンツをより一層保護するために、Smartsheet ではゲスト向けの高度な認証検証機能を提供し、許可されたユーザーにのみコンテンツへのアクセス権が付与されるようにしています。

外部の共同作業者向けシングル サインオン (EC-SSO) を使用すると、システム管理者は**企業 ID プロバイダーの使用を強制する**ことができます。それにより、SSO で検証されたユーザーのみが共有コンテンツにアクセスできるようになります。さらに、外部の共同作業者向け多要素認証 (EC-MFA) を使用することで、管理者は**アクセスの条件として外部ユーザーに対する MFA の強制を必須にする**ことができます。これを有効にすると、Smartsheet はログイン時に外部ユーザーの ID プロバイダーに問い合わせて MFA が使用されたことを確認し、その要件が満たされていない場合はアクセスをブロックします。

これらの機能により、エンタープライズの IT チームとセキュリティ チームは、特に規制の厳しい環境やリスクに敏感な環境において、自信を持って柔軟かつセキュアに共同作業の規模を拡大できます。

データ ガバナンス

今日のエンタープライズにとって、適用される規制や会社ポリシー、および業界のベスト プラクティスを確実に遵守して情報を作成、使用、共有、保護するためには、効果的なデータ ガバナンスが不可欠です。

データの管理は規制上の目的のためだけでなく、効率、ビジネスの機密性、ビジネスの継続性を確保するためにも必要です。

> ユーザー レベルでは、組織は効果的なツールで可視性を制限する、すなわち関係者のみに関連情報だけを提示する必要があります。
>
> 組織レベルでは、エンタープライズはポリシーの効果的な作成と施行のために適切なツールを備える必要があります。

ユーザー レベルでのデータ ガバナンス

大半のユーザーは、Smartsheet での権限レベル (閲覧者、コメント者、編集者、管理者、所有者) を十分理解しています。Dynamic View と WorkApps では、よりきめ細かな追加の制御と柔軟性を提供することで、ユーザー レベルでの効果的なデータ ガバナンスを実行できるようにサポートしています。最も関連性の高いコンテンツのみにアクセスを制限すると、ユーザーは必然的に注意が必要なアイテムに注力するため、プロセスの効率性を確保できます。それだけでなく、最小権限を既定とする Smartsheet のアプローチをよりきめ細かに拡張することで、セキュリティも確実に維持できます。

Dynamic View

すべてのビジネス プロセスで完全な透明性が保証されているわけではありません。注文管理、ベンダーとの共同作業、社内外の混成チームが関わるプロジェクトといった多くのプロセスでは、何を誰と共有するかについて厳格な制御が必要となります。

Dynamic View では、機密性を損なうことなく共同作業を行うことができます。Dynamic View を使用すると、シート所有者は元のシートを共有することなく、関連する行とフィールドを特定の共同作業者と選択的に共有できます。これで特定のビジネス ユーザーがベンダーや社内外の混成チームと、あるいは組織を超えて、特定のフィールドにのみ共同作業者を招待して、要素を選択的に共有するような事例が可能になります。誰もが自分の必要とする情報にアクセスでき、なおかつ必要とする情報にしかアクセスできません。

WorkApps

WorkApps では、お使いのシート、フォーム、ダッシュボード、レポートなどから直接構築された簡単に操作できるアプリによって、業務の合理化と共同作業の簡素化が可能になります。各チーム メンバーの役割に基づいてアプリでの体験を調整し、同じデータセットを土台に共同作業を行えます。Smartsheet プラットフォームと同じエンタープライズ グレードのマルチレベル セキュリティを使用してアプリを拡張します。

WorkApps では、WorkApp を構成する基盤となるアセットの共有が不要になります。選択したシートやレポートのフィルターが適用されたビューで WorkApp を作成することはできますが、シートやレポートをエンドユーザーと共有する必要はありません。
エンドユーザーには、それらのアセットの「WorkApp」ビューだけが表示されます。

組織レベルでのデータ ガバナンス ポリシー制御

Smartsheet は管理者に対し、プラットフォームの機能が組織のガバナンス ポリシーに従う形で使用されるようにすることを可能にします。Smartsheet の管理機能により、管理者はデータがそれを扱う必要のある人物だけの手で正しく取り扱われるようにするための、優れたデータ ガバナンスのガードレールを実装できます。

管理者は、ユーザーが特定の機能をどのように利用するかを選択し指定することができます。シート所有者がシートを公開したり、自動化を新規作成したりできるように するか？特定のストレージ システムのみからファイルを添付できるようにするか？外部の共同作業者が共有されているコンテンツをダウンロードできるようにするか？これらは、組織全体に実装する適切な制御を効果的に評価するために、管理者が自問すべき質問の例です。

このポリシー制御は共有セーフにも及びます。データやアセットの共有を特定のドメインまたはメール アドレスに制限したい場合は、このツールを使用します。前述のとおり、共有セーフによって、自社がベンダーやパートナーといった他の組織と Smartsheet アイテムを共有できるかどうかも決まります。

サード パーティ統合のセキュリティ

Smartsheet は階層型の OAuth 2.0 セキュリティ モデルを提供しています。このモデルでは、承認するユーザーの共有権限によってアクセス トークンが制限されるため、統合が承認者のデータ アクセス権を超えることは決してありません。エンタープライズ管理者は、管理センターを介してプラン全体のトークン有効期限ポリシーを施行し、構成可能な一定期間の後にすべての OAuth トークンを自動的に取り消すことができます。また管理者は、Okta もしくは Entra ID ディレクトリ同期 (SCIM 経由) を介してユーザーの登録解除を自動化することもできます。これにより、従業員の退職時に関連するトークンが無効化されます。継続的な可視性を実現するために、Smartsheet のイベント レポート作成では、100 種類以上の管理イベントとユーザー アクティビティ イベントを 6 か月間の監査ログ内でキャプチャできます。また、Skyhigh Security CASB および Microsoft Defender for Cloud Apps と直接統合して、異常検出とトリガーベースのアラート送信を行います。

Microsoft Intune によるモバイル アプリケーション管理 (MAM) の制御

組織が従業員の生産性を維持するためにモバイル アクセスに依存する傾向が高まる中、Smartsheet は 2026 年 4 月より、Microsoft Intune を介したモバイル アプリケーション管理 (MAM) 制御を提供し、IT 管理者が完全なデバイス登録を必要とせずにエンタープライズグレードのセキュリティ ポリシーを施行できるようにしています。

プロ、ビジネス、エンタープライズ、およびアドバンスド パッケージの各プランをご利用のお客様は、暗証番号と生体認証の要件、データの暗号化、コピー/貼り付けとスクリーンショットの制限、サード パーティのキーボードのブロック、印刷防止、最低 OS バージョンの強制、ジェイルブレイクと root 化の検出、および指定したオフライン期間後の自動データ消去などのきめ細かなポリシーを構成できます。このアプリケーションレベルのアプローチにより、組織は Smartsheet モバイル アプリで企業データをセキュアに保ちながら、個人デバイスで従業員のプライバシーを保護することで、セキュリティ面のコンプライアンスとユーザー エクスペリエンスのバランスを取ることができます。

Web コンテンツ ウィジェット制御

ダッシュボードを使用すると、操作可能なコンテンツ (動画、グラフ、文書など) を埋め込むことができます。管理者はこの機能を有効化または無効化でき、また Web コンテンツ ウィジェットをサポートするドメインの承認リストを策定できます。ベスト プラクティスとして、これは社内ドメインに限定することを推奨します。

自動化の許可

シート内の自動化で通知やリクエストを受け取れるユーザーを制御します。オプションは、[制限あり] (シートを共有されているユーザーへのアクションのみ有効化) から [制限なし] (任意のメール アドレスや Slack などのサード パーティ統合に自動化を適用する場合) まであります。この制御をレビューして、その構成が、組織が必要とする社内外の共同作業のレベルに合致しているかどうか確認することを推奨します。

添付ファイル/リンク制御

プランのメンバーがサイトにリンク (URL) を添付して自分のコンピューターからファイルをアップロードしたり、Google ドライブ、OneDrive、Box、Dropbox、Evernote、Egnyte などのサード パーティのクラウド ストレージ サービスからファイルをアップロードしたりすることができるかどうかを決定します。未承認のソースからデータが取り込まれる事態を防ぐために、組織の社内ポリシーに基づき使用を承認した添付ファイル/リンク プロバイダーのみを有効化します。

公開制御

シート、レポート、またはダッシュボードを公開すると、Smartsheet にログインせずに誰でもアクセスできる一意の URL と、Web サイトのソース コードに埋め込んでシートやレポートを表示できる iframe コードが生成されます。

シート、レポート、ダッシュボード、iCal の公開を許可しないこともできます。そうすると [公開] ボタンは Smartsheet アセットに表示されません。公開したアイテムへのアクセスを、Smartsheet 組織内のユーザーのみに制限することもできます。弊社の調査によると、セキュリティ意識の高いお客様は一般的に公開を許可していますが、公開したアイテムへのアクセスを自社のアカウント内のユーザーのみに制限しています。

共有セーフ

この機能を使用して、ドメインまたは特定のメール アドレスによって共有を制限します (たとえば、会社のメール アドレスを持つユーザーにのみシートを共有できるようにします)。共有セーフは、直接的な共有アクションの範囲を超えて適用されます。
また、ダッシュボードに埋め込まれたコンテンツも、組織の共有セーフ設定に基づいて許可された閲覧者にのみ表示されます。**Smartsheet では、共有セーフを実装して外部との共同作業を制御することを強く推奨します。**さらに、共有セーフ リストの更新と維持管理を簡素化するため、Smartsheet Web フォームを介して収集したリクエストによって共有セーフ リストを管理することをお勧めします。

オフライン フォーム送信制御

モバイル アプリを使用中の場合、Smartsheet ではオフライン中のフォームの送信を自動的に有効化し、ユーザーが一貫した接続を確保できない場合 (たとえば建設作業現場) でもフォームを使用できるようにしています。この制御により、管理者はオフライン フォーム送信をオフに設定する (またはオンに戻す) ことで、ユーザーが接続の切れた状態でもモバイル アプリを起動してフォームを送信できるようにするかどうかを制御できます。

コミュニケーション統合制御

Smartsheet はコミュニケーション サービスとして Google Chat、Microsoft Teams、Slack、Cisco Webex をサポートしています。アカウント管理者は自身の裁量で、1 つまたは複数のサービスを有効化できます。

ログ記録とレポート

組織全体における Smartsheet の使用状況のさまざまな側面を扱ったレポートをダウンロードでき、Smartsheet の使用状況、ユーザー、コンテンツ、請求、アクセスの現状を可視化できます。

シート アクセス レポート

アカウント上のプランが所有するすべてのシート、レポート、ダッシュボードの名前、これらのアイテムが保存されているワークスペースの名前 (該当する場合)、各シートを共有されている共同作業者、および最終更新のタイムスタンプを一覧表示した CSV を生成します。このレポートを定期的にレビューして、組織内のユーザーが所有するアセットへのアクセス権を持つ外部の共同作業者のリストを監査することを推奨します。

公開アイテム レポート

公開されている全アイテムを一覧表示した Excel ファイルを生成します。データ セキュリティや、特定のアイテムを公開した人を見つけ出す用途に最適です。公開制御の構成を通知する場合は、必要に応じてこのレポートを使用します。

ユーザー リスト レポート

プランのすべてのメンバー (招待済みユーザーとアクティブ ユーザーの両方)、それらのメンバーがプランに追加された日時のタイムスタンプ、アクセス レベル (システム管理者、グループ管理者など)、所有するシート数、および Smartsheet への最終ログインのタイムスタンプを一覧表示した CSV を生成します。

ログイン履歴レポート

複数ユーザー アカウントのシステム管理者は管理センターを使用して、最近のログイン履歴のリストを含むレポートを電子メールで受信できます。

チャージバック レポート

管理センターで利用でき、ディレクトリ統合を使用しているお客様はチャージバック レポートを用いて社内のチャージバックを促進できます。お客様がユーザー リストをダウンロードすると、作成した既存のレポートに部署、部門、コスト センターの列が追加され、社内チャージバック レポートの実行に必要なデータを取得できます。

その他のログ記録/モニタリングの仕組み

- **アクティビティ ログ:** アセットに対して行った変更、変更者、変更日時の監査証跡を提供します。これには行の削除 (削除
  されたデータを含む)、アイテムを表示したユーザー、共有権限の変更などの編集アクションが含まれます。

- **セルの履歴:** 変更者、変更内容、変更日時など、セル レベルで行われた変更の詳細なログが表示されます。ユーザーはセルの履歴からコピー/貼り付けすることで、不適切に削除または変更された以前の情報を簡単に復元できます。

- **システム列:** 各行の最終編集日時と変更を加えた共同作業者が表示されます。

- **セキュリティ スコア:** 実装されているセキュリティ機能に基づくデータ主導のスコアを提供することで、システム管理者が Smartsheet のセキュリティ ポスチャを評価および強化できるようにします。業界のベスト プラクティスに基づいたこの
  スコアには、カテゴリ別に分類されたポリシーの内訳と、セキュリティの強化と改善を経時的に追跡するための直感的な
  メトリックが含まれます。セキュリティ スコアは管理センター内からアクセスできます。

- **イベント レポート作成:** 100 種類を超えるセキュリティ イベントやユーザー アクティビティ イベントを可視化し、包括的な
  監査証跡を作成することができる高度な機能です。(イベント レポート作成の詳細については、以下をご覧ください)。

高度なデータ ガバナンス制御

Smartsheet は、特に厳格なデータ セキュリティのニーズをお持ちのお客様にデータ ガバナンス制御を提供する、数多くの高度な機能をご用意しています。これらの機能は Smartsheet Advance Platinum と Smartsheet Safeguard に含まれています。

データ エグレス ポリシー

データの共有には常にある程度のリスクが伴いますが、特に機密性の高いコンテンツを扱う際は、企業のデータを確実に自社のアカウント内のみに留め、管理下に置くことが非常に重要です。

システム管理者はデータ エグレス ポリシーを使用して、組織の内外へのデータのエクスポート方法に関するきめ細かな制御を通して機密情報を保護できます。

データ エグレス ポリシーを実装すると、内部や外部の共同作業者がシート、レポート、ダッシュボードで次のような行動を取ることを防げます。

- 新規として保存
- テンプレートとして保存
- 添付ファイルとして送信
- 公開
- 印刷
- エクスポート

制限されている行動を取ろうとしたユーザーは、その行動が組織のデータ エグレス ポリシーにより禁止されているという通知を受け取ります。

このような制限は、共同作業者が悪意を持って機密情報を保存または共有することを防ぐように策定されています。

イベント レポート作成

多くのエンタープライズは情報セキュリティを確実に維持するため、Smartsheet のようなビジネス アプリケーションの使用状況に対する継続的なインサイトを必要とします。以下の点について可視性を維持することが大切です。

- シートを作成している人
- ワークスペースを作成している人
- オブジェクトを削除している人
- シートを共有した人と共有された人

イベント レポート作成により、組織の Smartsheet アカウント内におけるユーザーの行動やアクティビティが詳細に可視化されます。この機能を使用すると、データの損失をモニタリングし、使用状況における異常なパターンを特定できるため、組織のセキュリティとコンプライアンス ポリシーをより厳格に適用できます。

イベント レポート作成はプラン (組織) 内での Smartsheet 使用に関する事象 (「イベント」) の JSON データ フィードを提供します。これはイベント レポート作成 API からアクセスできます。このサービスでは Smartsheet での 120 を超えるイベントをレポートし、フィードを有効化した日から最長で 6 か月間、データを保存します。

このフィードを有効活用するため、通常はイベント レポート作成データを、モニタリング、通知、ポリシーの作成と施行、データ損失防止 (DLP) を行う他のセキュリティ システムと統合します。このようなアプリは他社が販売しています。一般的には、クラウド アクセス セキュリティ ブローカー (CASB) システム、セキュリティ情報イベント管理

(SIEM) システム、あるいは CASB と SIEM を組み合わせて作動させます。時には他社製品に頼らず、自社でモニタリングおよび対応システムを開発することもあります。

イベント レポート作成の主な使用事例:

- データ損失防止
- 個人を特定できる情報 (PII) データの取り扱い
- データ ガバナンス
- 共同作業に関するインサイトの取得

データ保持コントロール

組織が SaaS アプリケーション内で保持するコンテンツが増えるほど、ビジネスで負うリスクが高まります。

Smartsheet データ保持コントロールにより、組織は選択した適用基準に基づいて、コンテンツを削除する必要がある場合を規定するポリシーを作成できるようになります。

シートを作成した日付や最後に修正した日付に基づいてポリシーを設定することで、アクティブなコンテンツや最近のコンテンツだけがご使用の Smartsheet インスタンス内で維持されるようになり、リスク プロファイルが制限されます。

お客様が管理する暗号キー (CMEK)

Smartsheet ではお客様のデータをセキュアに保ち、お客様によるデータ制御の維持をサポートできるように、暗号化を採用しています。一般のお客様の場合、データは既定のキーで暗号化されたマルチテナント アーキテクチャ内に格納され、AWS KMS を介してスケジュールに従って管理とローテーションが行われます。

お客様が管理する暗号キー (CMEK) は、独自の暗号キーを管理する必要がある機密データまたは規制対象データを保有する組織を対象としています。CMEK を使用すると、エンタープライズ組織はオンプレミスで設置する場合と同等のデータ制御を維持しつつ、クラウドの SaaS アプリケーションを使えるようになります。それにより、Smartsheet のデータ ストレージにお客様が管理する暗号化層が加わるため、高度なデータ セキュリティとガバナンス ポリシーを実現できます。

CMEK を使用するお客様の場合、データはお客様自身の AWS アカウントにホストされている KMS キーで暗号化された、物理的に隔離されているシングルテナントの Aurora クラスターに保存されます。Smartsheet はルート キーの素材にアクセスできません。お客様のキーは AWS 内で直接セットアップと管理が行われるため、お客様が CMEK を使用するには AWS Key Management Service (AWS KMS) にアクセスする必要があります。

Smartsheet では、CMEK を使用して組織のデータを暗号化することで、常にお客様が制御できるようにしています。具体的には、Smartsheet はこれらの暗号キーを保存または制御しておらず、お客様のシート データにアクセスする必要があるたびに、お客様の AWS KMS にキーをリクエストして取得する必要があります。

AWS KMS に保存されている CMEK はお客様の組織が制御しているため、Smartsheet による CMEK へのアクセス (つまり、データへのアクセス) をいつでも取り消すことができます。AWS KMS のマスター キーを破棄することで、組織はデータを効果的にロックできます。悪意のある当事者が Smartsheet のデータベース、ソース コード、クラウド暗号キーのコピーを持っていても、CMEK で暗号化されたデータを読み取ることは一切できません。CMEK は、購入基準を満たしているお客様向けに、スタンドアロンのサービスとしてご購入いただけます。

グローバル アカウント構成

アカウントのセキュリティはデータの暗号化、分類、認証オプションといった技術的機能に限定されません。セキュリティには、組織に属するすべてのアイテムに組織のロゴを含めるといったような、シンプルなものもあります。

グローバル アカウント構成制御によって視覚的なブランディング (およびその他の制限) を実装することで、ユーザーは自分が正規の情報にアクセスしていることを確認できます。

システム管理者はロゴをグローバルに追加して、組織のブランディング要件に合わせて Smartsheet を展開できます。各新規アセットに確実に同じブランドを適用するには、ブランディングのロックを使用します。

Smartsheet のカスタマイズ制御とアカウント構成では、カスタムのようこそ画面も設定できます。Smartsheet の使い方を説明するカスタム ヘルプ画面、ユーザーに管理者の連絡先を提示するライセンス リクエスト画面、ユーザーのログイン時に表示されるブランドを適用したカスタムようこそ画面を作成できます。また画面上で、情報にアクセスする前に利用規約を承認するようユーザーに求めることもできます。

一貫性のある視覚的なアイデンティティとカスタム情報を組み合わせることで、ユーザーは自分が正規のツールと情報にアクセスしていることを確認できるため、セキュリティの強化につながります。

Smartsheet のセキュリティ、プライバシー、コンプライアンス慣行

総合的なアプローチを活用した Smartsheet におけるサイバーセキュリティ、プライバシー、データ保護の各プログラムは、弊社のエグゼクティブ リーダーシップ チームが定義とサポートを行う戦略的情報セキュリティ ポリシーを起点とします。これらのポリシーは、組織の戦略的リスク管理慣行と足並みを揃えること、セキュリティ リスクを能動的に管理およびモニタリングすること、プロセスの成熟度と効果的なシステム アーキテクチャを通じてセキュリティを推進すること、およびトレーニングと啓蒙活動によってユーザーがセキュリティ リスクに関して正しい判断を下せるようにすることを目的としています。

責任共有モデル

効果的なセキュリティには、テクノロジー スタックのすべての階層にまたがる調整が不可欠です。Smartsheet が運用する 3 階層モデルでは、AWS が基礎となるクラウド インフラストラクチャの、Smartsheet がプラットフォームおよびアプリケーション層のセキュリティを守る一方、お客様はアカウント管理、データ、および認証に関するご自身の慣行について責任を負います。

インフラストラクチャとアーキテクチャ

Smartsheet のプラットフォーム全体は Amazon Web Services (AWS) と Google Cloud Platform (GCP) 上に構築されており、環境の境界を厳密に保つ形で設計することで、ソフトウェア ライフサイクルのあらゆる段階でお客様データの完全性と機密性を保護します。

環境セグメンテーション。米国、EU、オーストラリア、および GovCloud の開発、ステージング、実稼働の各リージョンをはじめとするそれぞれの環境は、独自の専用 AWS アカウントと組織ユニット、または GCP プロジェクト内で運用されており、実稼働以外のワークロードはお客様のデータを処理するシステムから完全に分離されています。リージョンをまたぐネットワーク接続のために、Smartsheet は AWS CloudWAN を使用して、論理ルーティング セグメント (隔離されている各環境に割り当てられた専用ネットワーク レーン) を施行しています。環境間のトラフィックは、ルールベースの制御を適用してすべての環境間トラフィックをログ記録する、AWS Network Firewall による検査インフラストラクチャを通過する必要があります。この保護を継続的に利用できるよう、冗長検査ノードが各リージョンに展開されています。

テナントの隔離。Smartsheet のすべてのお客様には、データの保存、クエリ、および取得のあらゆる操作に一貫して適用される一意のテナント識別子が割り当てられ、いかなるプロセスも別のお客様のデータにアクセスできないようにしています。インフラストラクチャ レベルでは、テナント コンテキスト間の横方向のコミュニケーションを制限するネットワーク ポリシーとセキュリティ ポリシーによって、コンテナ化されたワークロードが管理されています。また、環境ごとの専用アカウントというモデルによって環境が確実に隔離され、開発活動やテスト活動がお客様のライブ データに決して触れないようになっています。

セキュア開発ライフサイクル (SDLC)。セキュリティは製品開発のすべての段階に組み込まれています。コードの記述に先立ち、セキュリティ エンジニアがアーキテクチャと設計をレビューし、可能な限り低いコストで欠陥を特定します。その後、構造化された脅威モデリング (データ フロー図を使用して攻撃経路を列挙し、すべての所見をログ記録して追跡すること) を行い、軽減策が正しく実装されていることを確認するために的を絞ったコード レビューを実施します。継続的な静的アプリケーション セキュリティ テスト (SAST) と動的アプリケーション セキュリティ テスト (DAST) が CI/CD パイプラインに統合されており、実稼働を迎える前にコードの変更がすべて自動的にスキャンされます。

侵入テスト。Smartsheet はセキュリティ レビュー プロセスの標準的な構成要素として侵入テストを実施し、リスク分類に基づいて適用しています。エンゲージメントは、Smartsheet の社内セキュリティ チームか外部の適格な第三者企業によって行われます。テストは通常、グレーボックス手法 (テスターにソース コードへのアクセスとステージング環境の両方を提供) に従い、純粋な外部テストでは見逃す可能性のある脆弱性を表面化させます。特定の時点におけるこれらの評価は、コンピュート インスタンス、コンテナ、機能、およびコンピュート イメージを含むすべてのインフラストラクチャを対象とする、継続的な自動脆弱性スキャンによって補完されます。

脆弱性の追跡と是正。スキャンやテストを通じて特定された脆弱性は、Smartsheet の脆弱性管理ポリシーで定義された SLA ベースの是正ターゲットを用いてエンドツーエンドで追跡されます。

クラウド セキュリティ ポスチャ管理 (CSPM)。Smartsheet では、クラウド セキュリティ関連の懸念事項を検出、追跡、是正するためのクラウド セキュリティ ポスチャ管理ツールとして Wiz CSPM を使用しています。

Smartsheet は Wiz CSPM を主要なクラウド セキュリティ ポスチャ管理ソリューションとして活用し、マルチクラウド環境全体で包括的な可視性を実現しています。Wiz はインフラストラクチャについて統一化された「グラフベース」のビューを提供することで、Smartsheet が個々の脆弱性ではなく実際の漏洩に基づいて複雑な攻撃パスを特定し、リスクに優先順位を付けることを可能にしています。

セキュリティ上の主な利点:

- **コンプライアンスの継続的なモニタリング:** Wiz は Smartsheet のクラウド構成を業界標準のフレームワーク (SOC2、ISO 27001、FedRAMP など) に照らして自動的にマッピングし、規制関連のコミットメントとの継続的な整合性を実現します。
- **リアルタイムの検出と是正:** このプラットフォームではクラウド リソースの永続的なスキャンを実行し、構成ミス、過剰に権限を与えられた ID の役割、または漏洩したシークレットについてセキュリティ チームにリアルタイムで警告します。
- **攻撃面の減少:** Smartsheet ではソフトウェアの脆弱性とネットワークの到達可能性を相関させることで、影響の大きいリスクを迅速に是正し、外部の脅威に対するインフラストラクチャの強化を維持しています。

データ セキュリティ

Smartsheet では最も重要なアセットであるお客様のデータを確実に保護するために、プラットフォームにセキュリティ機構を組み入れています。Smartsheet は外部企業と契約し、SOC2 Type II の (または実質的に同等の) 評価と認証、および侵入テスト企業による第三者技術セキュリティ評価など、自社のセキュリティ慣行の監査を完了しています。さらに Smartsheet 脆弱性管理プログラムにより、Smartsheet 社内と実稼働環境全体にわたって、ネットワークとシステムの脆弱性を自動的に特定および是正しています。Smartsheet ではお客様のデータをセキュアに保ち、お客様によるデータ制御の維持をサポートできるように、暗号化を採用しています。

お客様のデータは Amazon Web Services のインフラストラクチャでホストされます。保存中のデータは、Amazon RDS 暗号化が提供する業界標準の AES-256 暗号化アルゴリズムを使用して暗号化されます。転送中のデータは TLS 1.2 技術を用いて保護されます。暗号キーは AWS KMS を介して 2 階層モデルを用いて管理されます。このモデルでは実際のお客様データを暗号化するデータ暗号キー (DEK) を、キー暗号キー (KEK) によって保護します。標準的なプランの場合、Smartsheet は自動ローテーションを使用して、お客様に代わって KEK を管理します。直接的な制御を必要とする組織については、お客様が管理する暗号キー (CMEK) をスタンドアロンのアドオンとして使用できます (上記の「お客様が管理する暗号キー (CMEK)」のセクションを参照)。

プライバシー

プライバシーは Smartsheet の運用の中核を成す要素です。関係するデータの種類に応じて、弊社は 2 つの異なる役割を担います。Smartsheet は、弊社が直接収集する個人データ (アカウント、使用状況、請求情報など) のデータ管理者であり、同時にお客様のコンテンツのデータ処理者でもあります。お客様のコンテンツとは、お客様がプラットフォームにアップロードまたは送信するデータを意味します。弊社は処理者として、お客様の指示に従ってそのデータを取り扱うだけであり、制御するのはあくまでお客様です。

Smartsheet はプライバシーを弊社の基本原則の 1 つであると考えています。それは機能の設計過程と意思決定過程に組み込まれており、私たちが付け加えるものではありません。そのため、マーケティングあるいはサード パーティの基盤モデルのトレーニングなど、弊社独自の目的でお客様のコンテンツを使用することはありません。

Smartsheet は、プライバシーに対するグローバルなアプローチに従って、GDPR、英国の GDPR、および CCPA などの主要な規制の要件を満たすように、またはそれを上回るように設計されています。認定のリストについては、以下を参照してください。主要な取り組みの簡単な概要を次に示します。

- **データ処理契約 (DPA)** — Smartsheet の DPA はすべてのお客様の Smartsheet ユーザー契約に自動的に組み込まれており、EU および英国の標準契約条項 (SCC) を含んでいます。署名入りのコピーを別途必要とするお客様は Smartsheet DPA ページからリクエストできます。条件に変更はありません。
- **データ レジデンシー** — お客様のコンテンツをホストする場所は、お客様が選択できます。詳細については、「Smartsheet リージョン」のセクションを参照してください。
- **設計時から既定で組み込まれたプライバシー** — Smartsheet のアプリケーション機能には、設計時から既定で組み込まれたプライバシーという原則が取り入れられています。プライバシーの確保は中心的な機能であり、後付けのものではありません。
- **復処理者** — 弊社は、Smartsheet が利用する復処理者のリストを公開するとともに、お客様のコンテンツを処理する
  第三者に対し、契約上の安全対策を審査して適用しています。詳細については、「ベンダーとサプライ チェーンのリスク
  管理」のセクションを参照してください。
  - **移転影響評価** — お客様のプライバシー コンプライアンス活動を支援するために、Smartsheet は移転影響評価を完了しました (Smartsheet セキュリティ パケットで利用可能)。コピーを入手するには営業担当者にご連絡いただくか、こちらのフォームを送信してください。

AI のセキュリティとプライバシー

Smartsheet の AI 機能は、プラットフォームの他の部分と同じセキュリティとプライバシーの原則に基づいて構築されています。

お客様のデータが他のお客様のデータと混ざり合うことは決してありません。また、お客様のデータによってサード パーティの基盤モデルをトレーニングすることはありません。さらに、お客様がご自分のデータを制御できない状態になることは決してありません。AI のアクションと推奨事項はすべて説明と監査が可能であり、そのソースまで追跡することができます。

入力プロンプトと生成された出力は、サポートと不正使用のモニタリングのためにのみ保存され、180 日後に自動的に削除されます。

AI 機能の完全な無効化を必要とする特定のポリシー要件をお持ちの組織については、Smartsheet サポートにお問い合わせいただくことでこのオプションを使用できます。AI 機能を無効にすると、お客様が Smartsheet サービスを最大限に活用する上で悪影響が生じます。

Smartsheet の AI ツールによるデータ処理の概要については、弊社の AI セキュリティ ホワイトペーパーか「責任ある AI」の Web ページをご覧ください。

オペレーション管理

Smartsheet では、お客様のデータが複数の物理的な場所でバックアップされ、セキュアに保たれるように設計されたポリシーと手順を導入しています。また Smartsheet のチームがセキュリティ上の新たな脅威を継続的に評価し、サブスクリプション サービスに対する不正なアクセスや計画外のダウンタイムを回避できるよう、対応策を更新し、それらを導入しています。Smartsheet のすべての実稼働システムとデータへのアクセスは、最小権限と need-to-know の原則に基づき、Smartsheet 技術運用チーム内の権限を付与されたメンバーに限定されています。

Smartsheet のクラウド インフラストラクチャは冗長性と信頼性を有するように設計されており、99.9% 以上のアップタイム SLA (サービス レベル契約) を保証しています。サービスの可用性とパフォーマンスに関するリアルタイムの情報は、Smartsheet ステータス ページにて公開されています。最新情報の自動送信を登録されているお客様には、電子メールやテキスト メッセージで重大なインシデントが通知されます。

インシデント対応と侵害通知

Smartsheet は文書化されたインシデント対応計画を維持しており、年に 1 回レビューとテストを実施しています。セキュリティ インシデントが発生した場合は、弊社の対応プロセスによって準備、検出と分析、封じ込め、根絶と復元、およびインシデント後の活動を実施します。適用法または契約で要求される場合、Smartsheet は法的に定められた期間内に、お客様が提供した連絡先に通知します。お客様はセキュリティに関するすべての懸念事項を、Smartsheet サポートを通じてエスカレーションする必要があります。可用性に関する弊社の取り組みについては、弊社のサービス レベル契約をご覧ください。

脆弱性の開示とバグ報奨金

Smartsheet では、独立したセキュリティ研究者を招待してプラットフォーム内の脆弱性を特定し、責任を持って開示していただく、アクティブなバグ報奨金プログラムを実施しています。このプログラムは Smartsheet のセキュリティ ポスチャを計画的に拡張するものであり、内部テスト以外の精査層を追加し、悪用される前に問題を発見して解決できるようにします。責任を持って開示することで、発見内容の重大度に応じて金銭的な報酬が支払われます。

プログラムの範囲。バグ報奨金プログラムは、主要な Smartsheet アプリケーション、エンタープライズ アクセス制御、Dynamic View、イベント レポート作成、および Salesforce コネクタや Jira コネクタなどのプラットフォーム統合機能など、Smartsheet のコア プラットフォームとエンタープライズ機能が対象です。Brandfolder by Smartsheet と Outfit もターゲットの範囲に含まれます。このプログラムは Smartsheet の社内バグ報奨金プラットフォームを通じて管理され、研究者には安全に作業を行うための専用テスト アカウントが提供されます。範囲外のアクティビティとしては、研究者が所有していないアカウントに対するテスト、自動スキャンとサービス拒否テスト、フィッシング、およびお客様のライブ データに影響を与える可能性のあるテストが挙げられます。

深刻度の分類。報告されたすべての脆弱性は、4 階層の深刻度モデルを使用して評価および分類されます。

- **重大 (S1):** 既存の資格情報やユーザー アクセスを必要とせずに、サーバーまたはアカウントの乗っ取り、お客様のデータへの不正アクセスまたはその改変、もしくはサービス拒否を発生させる問題。例として、SQL インジェクション、シークレットの漏洩、セキュアでないオブジェクト識別子に対するアクセス制御の欠如などが挙げられます。
- **高 (S2):** 影響度は重大と同じですが、悪用するには認証済みのアクセスか既存のユーザー資格情報が必要となります。例として、セッション ハイジャックを発生させるクロスサイト スクリプティングの脆弱性や、標準の制御を回避してコンテンツを完全に削除する能力などが挙げられます。

- **中 (S3):** 同じ組織内の他のユーザーや共有アセットに限定的な影響を与える問題。例として、共有シート内における権限昇格や、セキュアでない暗号プリミティブの使用などが挙げられます。
- **低 (S4):** 上記の基準を満たさないその他のセキュリティ関連の問題。

是正 SLA。脆弱性を確認して選別した後、Smartsheet は以下に示す是正措置のタイムラインに取り組みます。

- **重大:** 可能な限り速やかに是正または軽減 (最長 15 日)。
- **高:** 30 日以内に是正または軽減。
- **中:** 90 日以内に是正または軽減。
- **低:** 180 日以内に是正または軽減。

これらの SLA は、発見日または外部への開示日から適用されます。深刻度が重大である問題の場合は、必要とされるチーム メンバー全員が是正を優先し、問題が解決されるまで他の業務を除外することになっています。

責任ある開示。Smartsheet は開示プロセス全体を通じてセキュリティ研究者との協働に取り組んでいます。研究者は、発見内容を個人的に報告し、お客様アカウントに対するテストを控え、サービスの可用性を妨げる可能性のあるアクションを避けるよう求められます。その見返りとして、Smartsheet は速やかな認知、透明性の高いコミュニケーション、および有効な発見内容に対する適切な評価と補償を行うことを約束します。バグ報奨金プログラムの対象に含まれないセキュリティ上の潜在的な問題を報告したい組織は、bugbounty@smartsheet.com から Smartsheet に直接連絡することができます。Smartsheet はバグ報奨金プログラムをいつでも停止または中断する権利を留保します。

ベンダーとサプライ チェーンのリスク管理

Smartsheet はすべての復処理者に対し、それら復処理者の登録前にデュー デリジェンスを実践します。また、お客様のコンテンツへのアクセス、処理、もしくは保存を行うベンダーに対しては、より綿密な精査を実施します。これらのレビューには、SOC 1 または SOC 2 Type II、もしくはその両方のレポート、侵入テストと脆弱性テストの結果、PCI-DSS 監査、第三者によるセキュリティ評価など、関連するセキュリティ文書の確認が含まれます。復処理者は毎年再評価を受け、セキュリティ制御が引き続き Smartsheet の基準を満たしていることを確認します。

すべての復処理者は、セキュリティとプライバシーに関する Smartsheet の期待事項を反映した契約に署名する必要があります。これらの契約には、データ処理要件、セキュリティ基準、インシデント通知義務、および復処理者が使用する可能性のあるその他のベンダーにも同じ期待事項が適用されるルールが含まれます。

ご自分のデータの処理に誰が関与しているのかをお客様が把握できるよう、Smartsheet は復処理者リストを一般公開しています。弊社による復処理者の利用に関するその他の情報は、Smartsheet セキュリティ パケットに記載されています。コピーを入手するには営業担当者にご連絡いただくか、こちらのフォームを送信してください。

データ センターのセキュリティ、継続性、冗長性

Smartsheet では、お客様が信頼できるプラットフォーム上で自信を持って自社の方々にサービスを提供できるよう、業界で高く評価されているホスティング パートナーと提携しています。弊社は AWS 施設にホスティングすることで、複数サイトでのデータ冗長性を確保しています。また、弊社の施設は SOC 1、SOC 2、ISO 27001、FedRAMP/DISA IL5 の検査を受け、認定されています。弊社のモニタリングには継続的監視と、24 時間 365 日対応の実稼働環境の管理が含まれます。Smartsheet では、ビジネスの継続性に関する事象や災害復旧シナリオに対処するため、内部プロセスと計画を維持しています。これらの計画は毎年レビューとテストを行った上で、組織全体の該当するスタッフに配布されます。弊社は AWS でのホスティングを通じ、独立した電源、空調、および消火装置を備えた複数のデータ センターを活用しており、大規模な自然災害の発生時にデータ センターが同時に影響を受ける事態を防いでいます。

Smartsheet リージョン

Smartsheet リージョンでは、データがホストされる場所をお客様が制御できるため、組織が直面する地域ごとのプライバシーとガバナンスの要件に簡単に対応できます。米国 (US)、欧州連合 (EU)、オーストラリア (AU) の 3 つのリージョン インスタンスが利用可能です。

EU インスタンスは、ドイツのフランクフルトに所在する AWS でホストされています。AU インスタンスは、オーストラリアのシドニーに所在する AWS でホストされています。あるリージョン インスタンスで作成されたデータはそのリージョンに残り、リージョンの境界を超えてコンテンツを移転したりアクセスしたりすることはできません。

Smartsheet リージョンのオプションについて、詳しくは Trust Center とデータ レジデンシーのページをご覧ください。

監査と認定

ISO および SOC 2 のコンプライアンス

Smartsheet では、Trust サービス基準と ISO/IEC の一連の基準 (または実質的に同等の基準) を組み合わせることで自社のセキュリティ ポスチャを検証しています。これらの認定は、オペレーショナル エクセレンスに対する弊社の取り組みについて独立した保証を提供するものです。

- SOC 2 Type II: Smartsheet は第三者の公認会計士事務所による年次検査を受け、弊社の制御策の設計面および運用面の有効性をテストしています。
    - **範囲:** このレポートの範囲には、Smartsheet がホストされているデータ センター全体のコア プラットフォームとインフラストラクチャを含む、完全な Smartsheet アプリケーション環境が含まれます。
    - **信頼性基準:** セキュリティ、可用性、機密性。

- ISO/IEC 27001、27017、27018 (**セキュリティおよびクラウド**): この一連の認定によって、弊社の情報セキュリティ管理システム (ISMS) が検証されます。Smartsheet の基本的なセキュリティ フレームワークは 27001 ですが、特定のクラウド サービスのセキュリティ制御については 27017、パブリック クラウドにおける個人を特定できる情報 (PII) の保護については 27018 も遵守しています。

- ISO/IEC 27701 (**プライバシー**): Smartsheet のセキュリティ フレームワークの拡張であるこの基準は、プライバシー情報管理システム (PIMS) に焦点を当てており、弊社がデータ管理者およびデータ処理者として GDPR、英国の GDPR、CCPA などのグローバルなデータ保護要件を満たしていることを保証します。

- ISO/IEC 22301 (**継続性**): この認定では、予期しない事態の発生時に回復力と可用性を維持するための堅牢なビジネス継続性管理システムを、弊社が有していることを保証しています。

- ISO/IEC 42001 (AI **マネジメント — 進行中**): Smartsheet は現在、人工知能の正式なマネジメント システムを確立し、AI を活用した機能が倫理的かつセキュアに開発および展開されることを保証するために、この認証の取得を進めています。

- **EU - 米国データ プライバシー フレームワーク (DPF):** Smartsheet とその関連会社は EU - 米国データ プライバシー フレームワーク (EU - 米国 DPF)、EU - 米国 DPF の英国への拡張、および米国商務省によって定められ

たスイス - 米国データ プライバシー フレームワーク (スイス - 米国 DPF) に参加しており、これらをデータ プライバシー フレームワークと総称します。弊社は、欧州経済領域 (EEA)、英国 (UK)、およびスイスから米国に移転される個人データに関して、データ プライバシー フレームワーク原則を遵守することを約束します。データ プライバシー フレームワークの詳細と、弊社が取得した認定を確認するには、DPF プログラムの Web サイトにアクセスしてください。データ プライバシー フレームワーク原則に基づく Smartsheet の取り組みは、米国連邦取引委員会 (FTC) の調査権限および執行権限の対象になっています。

- **HITRUST 適格:** Smartsheet は、HITRUST CSF フレームワークの準拠と、堅牢なセキュリティおよびプライバシー管理の取り組みを反映して、HITRUST 適格のステータスを達成しています。この認定は、医療、金融、および規制が厳しいその他の分野のお客様をはじめとする、厳格なコンプライアンス要件を有するお客様をサポートできる弊社の能力を裏付けています。

- FedRAMP (moderate): Smartsheet は合同認証委員会 (JAB) によって FedRAMP Connect プログラムに選定されましたが、認定においては連邦政府機関からの要求に基づき、Smartsheet Gov が優先されています。Smartsheet Gov は FedRAMP 認証済みのステータスを持つ独立した Smartsheet 環境であり、国防総省影響レベル 4 (IL4) での評価を受けています。これにより、米国の軍民の政府機関がより簡単に Smartsheet を使用して業務を管理しつつ、セキュリティとコンプライアンスの要件を満たせるようになっています。

- **2002 年サーベンス・オクスリー法:** Smartsheet はかつて公開会社であり、以前はサーベンス・オクスリー法 (SOX) を遵守する必要がありました。現在はこの規制要件の対象ではなくなりましたが、Smartsheet は強力な財務ガバナンスと継続的な監査の準備をサポートするために、SOX に準拠した内部統制を維持することを選択しました。この継続性は、オペレーショナル エクセレンスと組織の整合性に対する弊社の取り組みを反映するものです。

弊社の法的情報の Web ページに記載している通り、Smartsheet はお客様のデータをホストするために、Amazon Web Services, Inc. (「AWS」) が提供するインフラストラクチャを使用しています。ISO 27001 認定や SOC レポートなど、AWS が受けるセキュリティおよびプライバシー関連の監査と認定についての情報は、AWS セキュリティ Web サイトと AWS コンプライアンス Web サイトで入手できます。

Smartsheet が有する認定の完全なリストとその他の情報については、Trust Center 内のコンプライアンス ページでご確認ください。**CAIQ および SOC 2 レポートなどの主要なセキュリティ文書に直接アクセスする場合は、アカウント担当者または CSM にご連絡の上、「セキュリティ パック」をリクエストしてください。**

結論とその他のリソース

現在、そして将来にわたって業務を進めるには、使いやすくてセキュアな、最新の業務管理プラットフォームが必須です。継続的な注力と投資を通じて、私たちは厳密なデータ機密要件と機能を備えた Smartsheet をゼロから立ち上げました。今すぐ活用できるものに加えて、数多くの追加のセキュリティ機能を目下開発中です。

システムのリアルタイムのステータスについては、Smartsheet ステータス ページでご確認ください。セキュリティ文書、認定、コンプライアンス関連のリソースについては、Trust Center でご確認ください。