Smartsheet のセキュリティ

Smartsheet のセキュリティ機能、慣行、保護についての詳細説明

エグゼクティブ サマリー

Smartsheet は、エンタープライズグレードのサービスとしてのソフトウェア (SaaS) プラットフォームは複数の防御層および数多くの IT 保護と制御を備え、機密性の高い企業データを安全に保持しなければならないことを理解しています。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、よく管理され、安全性とコンプライアンスが確保された労働環境を維持するために Smartsheet が実装を推奨する、お客様により制御される機能に焦点を当てます。なお、このホワイトペーパーでは現時点で一般的に利用できないセキュリティ機能については扱っていません。

概要

組織のセキュリティを最善に保つには、アイデンティティおよびアクセスの管理、データ ガバナンス、グローバル アカウント構成という、3 つの主な注力領域に関する制御を実装することを推奨します。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大まか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**は、プラットフォーム内での各ユーザーの役割と ID を組織構造とポリシーに合わせて調整することで、ユーザーが Smartsheet にアクセスする方法を制御することに重点を置いています。さらに、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保する方法を検討します。

- **データ ガバナンス**はユーザー レベルでも、組織全体でも強化する必要があります。Smartsheet では、デフォルトではユーザーに最小権限を与えていますが、追加の制御によってさらに可視性を制限、制御することができ、ユーザーは必要な時に必要なデータにのみアクセスできます。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、オプションのデータ エグレス ポリシーのような高度な機能の両方を組織レベルでカバーします。

- **グローバル アカウント構成**により、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することができます。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シンプルなものであっても、セキュリティの確保に役立てることができます。ブランディングとカスタマイズの適用をロックして一貫性を確保し、作成したすべてのアセットをブランドと整合させることができます。

- **セキュリティ、プライバシー、コンプライアンス慣行**は、Smartsheet が顧客データの高度な安全性の確保に役立てるために、プラットフォーム外にて維持管理している活動と保護を指します。Smartsheet は業界トップクラスの綿密な防御戦略を、人、プロセス、技術を組み合わせて実現し、Smartsheet 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 でユーザーのアイデンティティ (ID) を管理すること、つまりシステムへのユーザーのアクセスを管理することは、プラットフォームにおけるデータ管理と同様に重要です。

Smartsheet の導入の初期段階において、どの認証方法を採用するのかを決定します。Smartsheet は電子メールとパスワードや Google (グーグル)、Microsoft (マイクロソフト)、SAML 2.0 プロバイダー、Apple (アップル) のシングル サインオン (SSO) 方式といった、さまざまなオプションを提供しています。

組織としてひとつまたは複数の方法を選択できますが、全ユーザーに単一の SSO 認証方法を実施し、他の方法を無効にすることを推奨します。また SSO を構成する際には多要素認証 (MFA) を実装して、セキュリティにもう一つの層を追加することも推奨しています。

Smartsheet は強靭な REST API のセットを備えています。Smartsheet API は認証と承認に OAuth 2.0 を採用しています。各リクエストを認証するには、アクセス トークンを含む HTTP ヘッダーが必要となります。更にセキュリティを強化するためのベスト プラクティスとして、統合を構築する際には全体で OAuth 2.0 を使用します。

アクセス管理

ユーザーとそのアクセスの管理は非常に重要な管理機能で、セキュリティと、組織の Smartsheet の導入の両方に影響します。組織はその両者を慎重に両立させ、共同作業を促しながら、データとチームが徐々に分散していくにつれて、関与するリスクを管理する必要があります。これをサポートするため、Smartsheet はお客様がアプリケーションを管理する主な方法に合わせた、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、購買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。このモデルは、IT チームが Smartsheet を活用するあらゆる局面について、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わたる設定を制御し、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。集中的に IT チーム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保するため、Smartsheet 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。

ユーザー管理

社内のさまざまなチームが独自のニーズに応じて Smartsheet を採用すると、複数の個別プランが作成される可能性があります。複数の Smartsheet プランが存在する環境にはプランの統合が有効です。

分散型モデルを使用するプランにおいてユーザーを管理するには、各プランのアカウントの検出を有効化することを推奨します。新規ユーザーが Smartsheet を使用し始める際には、そのユーザーまたはその組織のドメインの誰かが社内の Smartsheet プランのリストを閲覧できる集中型の手段を提供して、新たなプランを開始することなく、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うようにします。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) 送られ、レビューと承認を受けます。

複数の個別プランがあり、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う必要がある場合があります。注: Dynamic View、コネクター、Control Center のような高度な機能を利用している場合は、統合に際して Smartsheet サポートと提携して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、ベスト プラクティスとしては部門/チーム/コスト センターを中心にプランを整理します。そうすることで、加入した事業部門に基づいて、ユーザーを関連するプランに自動的に割り当てるポリシーを策定できます。

ユーザー管理

Smartsheet はユーザーを一度に 1 人ずつ追加するのでは、何十人、何百人、さらに何千人と導入するユーザーの人数が多くなるにつれて、対処できなくなることを理解しています。よって使用開始時には、Smartsheet の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、Smartsheet の組織に一度に千人までのユーザーを簡単に追加できます。同様に、一括更新を使用して既存のユーザーの役割を一斉に編集することも可能です。

企業合併や買収ではしばしばブランドの変更が起こり、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。ユーザーの結合機能は、ユーザーの元のメール アドレスの一括更新と、重複するアカウントの一掃に役立ちます。

統合型の Smartsheet プランは、次に挙げる追加の 2 種類の機能を活用して、ユーザー管理を一層合理化し自動化します。

- 自動プロビジョニング (UAP) を使用すると、エンタープライズ アカウントへのユーザー追加処理が自動化されます。ユーザーが企業のメール 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したら、企業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許可するか、またはライセンスのない無料の共同作業者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 の統合型モデルを採用している場合、UAP 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社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。

- ディレクトリ統合により、Microsoft Azure Active Directory (AD) ユーザーを Smartsheet に直接同期できます。Azure AD で Smartsheet を既存の自動化にプラグインすると、ユーザーの登録と登録解除を完全に自動化でき、ユーザーが自分の Smartsheet アカウントにいつまでも滞在したり、再訪問したりするリスクを最小化できます。その他のメリットとして、部門/コスト センター/部署といったユーザーレベルの AD 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簡易化できます。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。こうすることで、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。第二の防御層として、UAP 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。

ユーザーが組織を辞める際には、Smartsheet へのアクセス権を削除することが重要となります。それには 2 つの方法があります。ユーザーを削除すると、ユーザー自身と所有するアセットが Smartsheet アカウントから消去されますが、この場合まだ使用しているアイテムが消去されてしまうことがあり、そのデータに依存するソリューションが使用できなくなる可能性があります。代替手段として、Smartsheet はユーザーの非アクティブ化を推奨します。この方法でも Smartsheet へのアクセスを完全に防げますが、所有していたコンテンツに対するアクセス権は保持され、ソリューションの安定性や所有権の移管に煩わされる必要がなくなります。

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にかかわらず、組織内のユーザーに Smartsheet の役割を策定する必要があります。

役割の割り当ては、それらユーザーに組織の 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。

- ライセンス ユーザー: シートの作成など、ライセンスを取得した場合の機能を使用できます。

- グループ管理者: Smartsheet グループを作成して管理します。*

  *グループ管理者の役割を割り当てられるユーザーはライセンス ユーザーでも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。

お客様の組織の Smartsheet アカウントには、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。そうすることで、特定の時間に 1 人のシステム管理者の都合が悪くとも、業務が中断されません。

グループ管理者は Smartsheet グループを作成して、ユーザーがグループでコンテンツを共有できるようにすることが可能です。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必要はありません。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には、関係者はライセンスユーザーでなければならず、Smartsheet アプリから直接ライセンスをリクエストできます。システム管理者はリクエストを個別に追跡し対応するか、あるいは管理センターのライセンス要求リクエスト管理セクションで一括処理できます。ライセンスのリクエストを管理するプロセスを既に確立している場合には、カスタム アップグレード画面を利用して、内部プロセス経由でライセンスのリクエストを送信するようにユーザーに指示することを検討します。

外部の共同作業者

ドメイン外の、Smartsheet アセットを共有している関係者は、外部の共同作業者と見なされます。Smartsheet を使用することにより、組織は信頼できる外部の当事者と自由に共同作業ができます。しかも外部の共同作業者のための関連コストはかかりません。外部と提携する際にセキュリティを確保するには、次に挙げる 3 種類の、一元化された管理者制御を活用することを推奨します。

共有セーフにより、外部の共同作業者に権限を与えるための信頼性の高いドメインやメール アドレスを指定できます。

シート アクセス レポートで、組織の Smartsheet コンテンツにアクセスできる外部の共同作業者のリストを取得できます。

アイテムへのアクセスの取り消しを管理センターを介して一元的に行うことで、アクセスする必要がなくなったコンテンツから外部の共同作業者のアクセス権を削除できます。

データ ガバナンス

今日の企業にとって、適用される規制や企業のポリシー、業界のベスト プラクティスに確実に従って情報を作成、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、企業は効果的なポリシーの作成と強化のために、適切なツールを使用する必要があります。

ユーザー レベルでのデータ ガバナンス

ほとんどのユーザーは、Smartsheet での権限レベル (閲覧者、編集者、管理者、所有者) をよく理解しています。Dynamic View と WorkApps は追加のきめ細かな制御と柔軟性を提供し、ユーザー レベルでの効果的なデータ ガバナンス機能の提供をサポートします。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、プロセスの効率の確保に役立ちます。それだけでなく、デフォルトでの Smartsheet の最小権限のアプローチをよりきめ細かに拡張することで、セキュリティも確保できます。

Dynamic View

ビジネス プロセスのすべてが完全な透明性を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など、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 は機密性を侵害することなく、共同作業を可能にします。Dynamic View を使用すると、シート所有者は特定の共同作業者と、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、かつ必要とする情報だけ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、作業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の体験を調整し、同じデータセットを元にして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 を使用すると、管理者はプラットフォームの機能を組織のガバナンス ポリシーに従って活用できます。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拡張します。データやアセットの共有を特定のドメインやメール アドレスに制限したい場合、このツールを使用します。前述のとおり、共有セーフにより、組織がベンダーやパートナーなどの他の組織と Smartsheet アイテムを共有できるかどうかも決定します。

Web コンテンツ ウィジェット制御

ダッシュボードは、やり取り可能なコンテンツ (動画、グラフ、文書など) を組み込む機能をサポートします。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。

自動化の権限

シートから自動化を受け取れる人を制御します。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者のレベルに合致している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するのか、または 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するのかを決定します。未承認のソースからのデータの取り込みを防ぐために、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。Smartsheet の経験では、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ますが、公開したアイテムへのアクセスを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)。Smartsheet は共有セーフを実装して、外部の共同作業者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 フォームを活用して更新リクエストを収集することを推奨します。

オフライン フォーム送信制御

モバイル アプリを使用する場合、Smartsheet 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など) でも使用をサポートします。この制御により、管理者はオフライン フォームの送信をオフに設定する (またはオンに戻す) ことができ、ユーザーが接続の切れた状態でもフォームを送信するためにモバイル アプリを起動できるようにするかを管理します。

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、ひとつまたは複数のサービスを有効化できます。

ログとレポート

組織全体にわたる 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、使用者、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

アカウントでライセンス ユーザー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)、各シートが共有されている共同作業者、最後に修正した時刻のタイムスタンプをリスト表示した Excel ファイルを生成します。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にアクセスする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リスト表示した 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には、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

アカウント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)、アカウント追加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、Smartsheet への最終ログインのタイムスタンプをリスト表示した Excel ファイルを生成します。

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 Excel ファイルを電子メールで受信できます。

チャージバック レポート

管理センターで使用でき、ディレクトリ統合を使用するお客様はチャージバック レポートを使用し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が取得できます。

シート、ダッシュボード、セル レベルでのユーザー アクションの一層きめ細かな追跡には、アクティビティ ログ、セルの履歴、システム列を使用できます。

- **アクティビティ ログ:** アセットに行った変更、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、共有許可の変更などの編集が含まれます。

- **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簡単にコピー/貼り付けして、不適切に削除または変更された以前の情報を修復できます。

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

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 や Smartsheet Safeguard に含まれています。

お客様が管理する暗号キー

Smartsheet ではお客様のデータを保護し、お客様によるデータ管理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有する組織を対象としています。CMEK によって、企業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管理しながら、クラウドで SaaS アプリケーションを使えるようになり、Smartsheet データ ストレージへお客様が管理する暗号化層を追加することで、高度なデータ セキュリティとガバナンス ポリシーをサポートできます。

注: CMEK を使用するには、お客様はカスタマー キーを設定して Amazon Web Services (AWS) 内で直接管理するために、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して、常にお客様が管理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管理せず、Smartsheet がお客様のシート データにアクセスする必要があるたびに、Smartsheet はお客様の AWS Key Management Service (KMS) にキーをリクエストして取得する必要があります。

AWS Key Management System に保存されている CMEK を管理している組織は、Smartsheet からの 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 Key Management System のマスター キーを破棄すると、組織は Smartsheet システムからデータを効果的に削除できます。悪意のある第三者が 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できません。

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ありますが、特に機密のコンテンツを扱う際には、企業のデータを確実に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

情報セキュリティを確保するため、多くの企業は、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。次に挙げる点について、可視性を維持することが大切です。

- シートの作成者
- ワークスペースの作成者
- オブジェクトを削除する者
- シートの共有者と共有の対象者

イベント レポート作成では、組織の Smartsheet アカウント内で、ユーザーの行動やアクティビティを詳細に可視化します。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応答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
- 共同作業のインサイトの取得

データ保持コントロール

組織が SaaS アプリケーションに保持するコンテンツが増えるほど、ビジネスが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、または最後に改訂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ていることを保証し、リスク プロファイルを制限できます。

グローバル アカウント構成

アカウント 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、組織に属するアイテムすべて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り視覚的なブランディング (とその他の制限) を実装することができ、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。

システム管理者はグローバルにロゴを追加して、組織のブランディング要件に合わせて Smartsheet を導入できます。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 カスタマイズ管理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。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。ユーザーが情報にアクセスする前に、画面上でサービス利用規約に同意することを必須にすることが可能です。

一貫した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と、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、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

歴史的アプローチを活用すると、Smartsheet でのサイバーセキュリティ、プライバシー、データ保護プログラムは、Smartsheet 情報セキュリティ運営委員会 (ISSC) とエグゼクティブ リーダーシップ チームが定義しサポートしている戦略的情報セキュリティ ポリシーから始まります。これらのポリシーは組織の戦略的リスク管理慣行に沿って、セキュリティ リスクをプロアクティブに管理、モニタリングし、プロセスの発達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し、トレーニングと啓蒙活動により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策定されています。

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 SOC2 Type II 評価と証明、ペネトレーション テスト企業によるサード パーティ技術セキュリティ評価など、サード パーティと契約した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は、Smartsheet 社内と本番環境全体にわたって、ネットワークとシステムの脆弱性の特定と修正を自動的に行います。Smartsheet ではお客様のデータを保護し、お客様によるデータ管理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。Smartsheet では、すべてのデータは米国国立標準技術研究所 (NIST) に承認された暗号、トランスポート レイヤー セキュリティ (TLS) 技術、AES 256 ビットによる保存データ暗号化、アップロードされたファイルの保存と取り扱いを行う Amazon の S3 サービスを活用してすべて厳重に保存されますので、安心してご利用いただけます。

プライバシー

Smartsheet では、プライバシーを重視し、どのように個人情報が収集、使用されるかを知る権利を尊重しています。Smartsheet のプライバシー通知では、Smartsheet の Web サイト、モバイル アプリ、Smartsheet の作業実行プラットフォームを通じて収集した個人情報やその他の情報を Smartsheet がどのように取得、使用、開示するのかを説明しています。

- Smartsheet は潜在顧客、お客様、パートナーのプライバシー権を認識しており、EU 一般データ保護規則 (GDPR) などの国際的なプライバシー規制を順守しています。

- Smartsheet には、個人情報を含むコンテンツの処理に関する特定の規約を必要とするお客様と、データ処理契約 (DPA) を締結する用意があります。Smartsheet との DPA が必要であると判断された場合、smartsheet.com/legal/DPA から DPA の規約に同意する旨のフォームをお送りください。

オペレーション管理

Smartsheet では、データが複数の物理的な場所で保護、バックアップさ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 のすべての本番システムや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 は、Smartsheet ステータス サイトでシステムのステータス情報を公開しています。Smartsheet は通常、Smartsheet ステータス サイトで最新情報の自動送信に同意されたお客様に対して、重要なシステム インシデントを電子メールやテキスト メッセージで通知しています。

データ センターの安全性、継続性、冗長性

Smartsheet では、信頼できるプラットフォームにて自信を持って組織の人々にサービスを提供できるよう、業界で評価の高いホスティング パートナーと提携しています。Smartsheet 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 Smartsheet 施設は SOC 1、SOC 2、ISO 27001、FISMA の検査を受け、認定されています。Smartsheet のモニタリング機構には生体認証プロトコル、継続的な監視、24 時間 365 日対応の本番環境管理が含まれています。Smartsheet は内部プロセスと計画を維持管理し、ビジネス継続性に関する事象や災害復旧シナリオに対処します。このような計画は毎年レビューしてテストし、組織全体の該当するスタッフに配布します。大規模な自然災害発生時にデータ センターが同時に被災することを防ぐため、Smartsheet のデータ センターは地理的に約 970 km 離れています。

監査と証明

次に挙げるセキュリティとプライバシーに関する監査と証明は、Smartsheet 内の中心的なアプリケーション サービスに適用されています。

- **SOC 2/SOC 3:** Smartsheet は毎年、SOC 監査プロセスの一環として、検査と試験を受けています。その結果である外部監査レポートにより、安全性、可用性、機密性を含む、Smartsheet のビジネス全体の社内管理の設計と業務の効率性が証明されています。

- **EU と米国間、およびスイスと米国間のプライバシー シールド認証:** 該当するサービスに送信したお客様のデータは、米国商務省が管理する EU と米国間のプライバシー シールド フレームワークと、スイスと米国間のプライバシー シールド フレームワークの、年次証明書の対象になっています。最新の証明書は privacyshield.gov/list からご確認いただけます。「Smartsheet」の下で検索してください。

- **FedRAMP (中):** Smartsheet は、連邦政府機関からの要求に基づき、認定に Smartsheet Gov を優先的に使用している Joint Authorization Board (JAB) によって、FedRAMP Connect プログラムに選ばれました。Smartsheet Gov は、FedRAMP 認証ステータスを備えた独立した Smartsheet 環境であり、米国政府の Smartsheet を使用した作業管理や、セキュリティとコンプライアンスの要件の順守を容易にします。

- **2002 年のサーベンス・オクスリー法:** Smartsheet は公開会社であり、サーベンス・オクスリー法 (SOX) を順守する必要があります。SOX を順守すると、まとまりのある社内チームを組織でき、監査に関連するチーム間のコミュニケーションを改善できます。

Smartsheet 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 証明書や SOC レポートなど、AWS が受け取るセキュリティとプライバシー関連の監査と証明についての情報は、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 の証明書とその他のホワイトペーパーおよびデータシートの一覧は、Smartsheet Trust Center のコンプライアンス ページからご覧ください。

結論とその他のリソース

現在、そして将来にわたり作業を行っていくには、使いやすくて安全な、最新の作業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。今すぐに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。Smartsheet のセキュリティ機能、プログラム、保護についての詳細は、smartsheet.com/trust や次に挙げるその他のリソースをご覧ください。

Smartsheet システム管理者オンライン ヘルプ
Smartsheet のプラン別機能
Smartsheet の統合
Smartsheet API Documentation (Smartsheet API に関するドキュメント)

japansales@smartsheet.com
03-6897-3663
jp.smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet_JPN
/smartsheet