Cloud Software Group

サービスのセキュリティに関する別紙

バージョン 3.0

適用開始日: 2022年9月30日

内容

この「Cloud Software Group, Inc.（以下、「Cloud Software Group」といいます）サービスのセキュリティに関する別紙」（以下、「本別紙」といいます）は、関連するCloud Software Groupのライセンスおよび/またはサービス契約および該当するサービス（以下、総称して「本契約」といいます）の注文に基づいて顧客（以下、「お客様」といいます）に提供されるCloud Services、テクニカルサポートサービス、コンサルティングサービスのパフォーマンスに関連して実装されるセキュリティ管理について記述したものです。 ベータ版またはlab/tech previewサービス（Cloud Labsを含む）およびサービス提供に含まれていない社内のITシステムは、本別紙の範囲外となります。

大文字の用語は、本契約で定義されている意味または本別紙で定義されている意味を持ちます。「カスタマーコンテンツ」とは、Cloud Software Group がサービスを実行するために、Cloud Software Groupがアクセスまたは受信するデータ、またはお客様が保存や処理のために送信またはアップロードするデータを意味します。。 また、お客様のシステムまたはネットワーク構成、お客様が選択したコントロールなど、お客様の環境に関連する独自の技術情報も含まれます。 「ログ」とは、Cloud Software Groupの製品またはサービスの使用に関連するパフォーマンス、安定性、使用法、セキュリティ、サポート、ハードウェア、ソフトウェア、サービス、または周辺機器に関する情報を意味します。

1.範囲

本別紙では、Cloud Software Groupが本サービスの機密性、整合性、可用性を維持するために導入している管理的、物理的、および技術的なセキュリティ対策について記述します。かかる対策は、Cloud Software Groupの運用および本サービスのシステムおよび環境に適用されます。Cloud Software Groupは、サービスのセキュリティプログラムの基本としてISO/IEC 27002を採用しており、特定のサービスについては業界の認証と評価を取得しています。 追加情報は、Cloud Software Group Trust Centerの「Privacy & Compliance（プライバシー＆コンプライアンス）」セクションでご覧いただけます。

Cloud Software Groupは継続的にセキュリティ対策の強化および改善に努めており、ここに記載された対策を変更する権利を留保します。 いかなる変更も、本サービスの関連する期間中のセキュリティレベルを低下させるものではありません。

2.セキュリティプログラムおよびポリシーフレームワーク

Cloud Software Groupには、全社の各種事業分野を代表する上級管理職および役員によって策定および承認されたセキュリティプログラムおよびポリシーフレームワークがあります。

2.1 セキュリティリスクの監視

CROC（Cyber Risk Oversight Committee: サイバーリスク委員会）がセキュ

リティリスク管理アクティビティを管理します。CROCは、部門横断的な管理者およびリーダーシップで構成されます。 エグゼクティブリーダーシップチームは、事業分野と業務分野が十分に網羅されているかを確認するため、毎年委員会メンバーを見直しています。

CROCは少なくとも四半期ごとに開催され、企業の業務とサービス提供インフラストラクチャの両方におけるセキュリティリスクを特定、評価、対処するためのガイダンス、知見、および方向性を提供します。

2.2 セキュリティリスクの管理

Cloud Software Groupは、SRM（Security Risk Management、セキュリティリスク管理）プログラムを利用して、Cloud Software Group製品とサービス、およびCloud Software Groupインフラストラクチャに対する潜在的な脅威を特定し、それらの脅威に関連するリスクの重要度を評価し、リスク軽減戦略を策定し、Cloud Software Groupの製品およびエンジニアリングチームと協力して、それらの戦略を実施します。

2.3 情報セキュリティ

Cloud Software Groupは、セキュリティの監視とポリシー戦略、コンプライアンス、および執行を担当するCISO（Chief Information Security Officer、最高情報セキュリティ責任者）を任命しました。 セキュリティ監視および対応ディレクターは、調査、封じ込め、修復など、インシデント対応プロセスを主導します。

2.4 物理セキュリティおよび環境セキュリティ

Cloud Software Groupセキュリティチームは、Cloud Software Groupの施設への物理的なアクセスを監視します。

3.アクセス制御

Cloud Software Groupは、潜在的な損害、侵害、または損失から保護するため、会社のシステム、資産、データ、および設備へのアクセスに適切な権限が割り当てられ、維持されるように設計されたアクセス制御手段の使用を要求します。Cloud Software Groupは最小限の権限の原則または役割ベースのセキュリティに従い、業務の遂行または役割に必要なものだけにユーザーのアクセスを限定します。

管理者は、職務の適切な分離を実現するために役割を設計し、不正やエラーから保護するために複数の担当者間でタスクと権限を分散します。

3.1 新しいアカウント、役割、アクセス要求

Cloud Software Groupは、会社のシステムまたはデータへのアクセスに対して正式な要求を必要とします。各アクセス要求は、ユーザーの役割およびアクセス権限を確認するために、ユーザーのマネージャーによる最小限の承認を必要とします。 アクセス管理者は、システムまたはデータへのアクセス権を付与する前に、必要な承認が得られていることを確認します。最小限の権限の原則が適用されます。

3.2 アカウントレビュー

Cloud Software Groupは、主要なシステムのユーザーアカウントおよび割り当てられた権限について、少なくとも年2回のレビューを実施します。 レビューの結果として必要とされるいかなる変更についても、ユーザーおよびユーザーの役割が関連システムへのアクセスを必要とすることを確認するため、正式なアクセス要求プロセスの対象となります。

3.3 アカウント、役割、アクセス権の削除

Cloud Software Groupは、ユーザーの役割の変更（該当する場合）、終了、ユーザーの契約終了、または退社の通知を受け取り次第、速やかにユーザーのアクセス権を無効化、失効、または削除することを要求します。

アクセス権の削除要求は文書化され、追跡されます。

3.4 資格情報

Cloud Software Groupは、従業員によるCloud Software Groupシステムへのリモートアクセスには多要素認証を要求し、以下のようにパスワードを取り扱い、管理します。

- パスワードは、Cloud Software Groupが設定したシステム要件に従って、定期的にローテーションされます。

- パスワードは、数字、特殊文字、大文字と小文字の組み合わせ、最小文字数、一般的な単語や辞書の単語を許可しないなど、長さと複雑さの要件を満たしている必要があります
- 無効または期限切れになったIDが別の個人に付与されることはありません。
- Cloud Software Groupは、誤って開示されたパスワードを無効化する手続きを維持しています。
- Cloud Software Groupは、無効なパスワードを使用して繰り返し本サービスにアクセスしようとする試みを監視し、繰り返された試みを遮断するために自動化された措置を取ります。

Cloud Software Groupは、パスワードの機密性および完全性の確保を目的とした規定に従って、パスワードを割り当て、配信、および保管します。例:

- パスワードのライフサイクルを通じて、ハッシュ化および暗号化を維持することを義務付けます。
- Cloud Software Groupはパスワードの共有を禁止します。

4.システム開発および保守

このプロセスには、情報システムのセキュリティ要件、コードレビューとテスト、テストデータの使用に関連するセキュリティに対処するために設計された標準と変更管理手順が含まれています。 このプロセスは、専門のセキュリティチームによって管理および監視され、このチームは設計レビュー、脅威のモデリング、手動のコードレビューおよびスポットチェック、侵入テストについても責任を負います。

4.1 安全な設計の原則

Cloud Software Groupは、コンピュータ化された情報システムおよび関連技術要件の開発、取得、実装、および保守を管理する正式なSDLC（システム開発ライフサイクル）手法を導入しています。

オープンソースのレビューと承認の管理には、ソフトウェア製品の定期的なスキャンと監査の実施を含む、ソフトウェアベースのシステムを使用しています。 Cloud Software Groupは、オープンソースの使用に関するポリシーを文書化して全従業員が利用できるようにしており、開発者およびその管理者を対象にオープンソースのベストプラクティスに関するトレーニングを実施しています。

4.2 変更管理

Cloud Software Groupのインフラストラクチャおよびソフトウェアの変更管理プロセスは、セキュリティ要件に対処し、本番環境で展開する前に、ソフトウェアおよびインフラストラクチャの変更の承認、正式な文書化、テスト（該当する場合）、レビュー、承認を要求します。 インフラストラクチャおよびソフトウェアの変更は、作業管理システムを使用して管理および追跡されます。

変更管理プロセスは適切に分離されており、変更を本番環境に移行するためのアクセス権は、許可された担当者に制限されています。

5.アセット管理

5.1 物理および仮想アセット管理

Cloud Software Groupは、本サービスの実行に使用されるCloud Software Group管理対象の物理システムおよび仮想システム（以下、「サービスアセット」といいます）の動的なインベントリを維持します。 システム所有者は、Cloud Software Groupのセキュリティ標準に準拠したサービスアセットを維持および更新する責任を負います。

Cloud Software Groupおよびお客様のデータを安全に廃棄するための正式な廃棄手順が規定されています。 Cloud Software Groupは、分類に基づいて不要になったデータを、データの再構築または読み取りを防止するために設計された削除プロセスを使用して廃棄します。

Cloud Software Groupのテクノロジーアセットは、指定または割り当てられたエリア内で不要になった場合にサニタイズおよび廃棄されます。 テクノロジーアセットには、個別のコンピューティングデバイス、複合コンピューティングデバイス、ストレージデバイス、イメージングデバイス、ネットワークアプライアンスなどが含まれますが、これらに限定されません。 廃棄は、グローバルセキュリティリスクサービスと情報セキュリティを通じて調整されています。

5.2 アプリケーションおよびシステム管理

アプリケーションおよびシステム所有者は、保存、アクセス、廃棄、または伝送するデータをレビューおよび分類する責任を負います。その他の対策として、従業員および請負業者は次の項目を遵守する必要があります。

- カスタマーコンテンツをCitrixの機密情報の中で最高水準の2つのカテゴリに分類し、適切なアクセス制限を適用する
- カスタマーコンテンツの印刷を制限し、印刷物を安全な容器に入れて廃棄する
- 企業情報または機密情報を、Citrixのセキュリティポリシーおよび標準の要件を満たしていない機器またはデバイスに保存しない
- 不在時のコンピュータおよびデータの安全性を確保する

5.3 データの保持

Cloud Software Group Cloud Servicesの一部として保存されているカスタマーコンテンツは、本サービスの終了後、一定期間のみお客様がアクセスでき、削除に関する確認がお客様に送信された後に削除されます（バックアップコピーを除きます）。 その他の詳細については、特定のサービスのドキュメントに記載されています。 カスタマーコンテンツは、法的な目的のために必要な場合、サービスの終了後も保持されることがあります。 Citrixは、当該カスタマーコンテンツが完全に削除されるまで、本別紙の要件を遵守します。

6.人材のセキュリティ

カスタマーコンテンツのセキュリティを維持することは、すべての従業員および請負業者にとって、中核的な要件の1つです。 Cloud Software Groupのビジネス行動規範では、すべての従業員および請負業者がCloud Software Groupのセキュリティ方針および基準を遵守することを求めており、特にお客様、パートナー、サプライヤーおよび従業員の機密情報および個人情報の保護について定めています。

Cloud Software Groupのすべての従業員および請負業者は、顧客情報を対象とする機密保持契約の対象となります。 また、Cloud Software Groupのセキュ

リティ組織は、特定のトピックに関するセキュリティの意識を維持するため、情報セキュリティおよび物理的セキュリティに関連するトピックについて定期的に従業員とコミュニケーションを取ります。

6.1 身元調査

Cloud Software Groupは現在、全世界のすべての新規採用者に対して身元調査ベンダーを使用しており、現地の法律や就業規則で制限されている場合を除き、サードパーティのサプライヤーの従業員に対しても同様の調査を要求しています。

6.2 トレーニング

すべての従業員は、Cloud Software Groupのお客様、パートナー、サプライヤー、および従業員の機密情報を含む、Cloud Software Groupの機密情報のセキュリティを保護するために設計された、データ保護と会社のポリシーに関するトレーニングを受ける必要があります。 このトレーニングでは、個人情報の利用、アクセス、共有、保持に制限を課す必要性など、個人情報を取り扱う従業員に適用される原則とプライバシー対策を扱います。 エンジニアリング組織のメンバーは、セキュリティで保護された開発、アーキテクチャ、コーディングから成る特定のトレーニングを受けています。

6.3 執行

すべての従業員は、Cloud Software Groupのセキュリティとプライバシーに関するポリシーおよび標準を遵守する必要があります。 遵守しない場合は、解雇を含む懲戒処分の対象となります。

7.運用のセキュリティ

7.1 ネットワークおよびシステムのセキュリティ

Cloud Software Groupは、ネットワークとシステムが安全に構成されるように設計された、ネットワークおよびシステムの堅牢化標準を文書化しています。これらの基準の下で必要とされる手順には以下が含まれますが、これらに限定されません。

- デフォルトの設定またはアカウントを変更または無効化する
- 管理者アクセス権の使用を制御する
- 作成時の目的のみにサービスアカウントを制限する
- 監査に適したログおよびアラート設定を構成する

Cloud Software Groupは、サーバーおよびワークステーションにマルウェア対策ソフトウェアを導入し、ネットワーク上に悪質なソフトウェアがないかどうかをスキャンすることを要求します。

ネットワーク制御により、カスタマーコンテンツへのアクセスが管理されます。 これには、該当する場合、インターネットと社内ネットワーク間の信頼されない中間ゾーンの構成（アクセスおよび不正なトラフィックを制限するセキュリティ対策を含む）、カスタマーコンテンツへの不正アクセスを防止するためのネットワークセグメンテーション、および各層間のトラフィックを制限する層構造で実施する、対応するデータベースサーバーからのWebサーバーとアプリケーションサーバーの分離などが含まれます。

7.2 ログ

Cloud Software Groupはログを収集して、本サービスが正しく機能していることを確認し、システムの問題のトラブルシューティングを支援し、当社のネットワークおよびカスタマーコンテンツに対する保護および安全性を確保します。 ログには、アクセスID、時刻、承認の許可または却下、トレースおよびクラッシュファイルなどの診断データ、その他の関連情報とアクティビティが含まれます。

Cloud Software Groupは、(i) 本サービスの提供、セキュリティ確保、管理、測定、改善のため、(ii) お客様またはそのエンドユーザーの要求に応じて、(iii) 課金、アカウント管理、内部報告、製品戦略のため、および/または (iv) 契約、ポリシー、適用法、規制または政府の要請に従うためにログを収集し、使用します。これには、本サービスおよび関連コンポーネントのパフォーマンス、安定性、使用状況、およびセキュリティの監視が含まれる場合があります。 ログには、アクセスID、時刻、承認の許可または却下、トレースおよびクラッシュファイルなどの診断データ、その他の関連情報とアクティビティが含まれます。お客様はその監視を禁止したり妨げたりすることはできません。

カスタマーコンテンツとログの取り扱いに関する詳細は、Citrix Cloud Services Loggingに関する複数のホワイト ペーパーを含むCloud Software Group Trust Center Cloud Assurance Data Protection & Security sectionを参照してください。

7.3 証明書、資格情報、秘密管理

Cloud Software Groupは、証明書、資格情報、シークレットのライフサイクルをカバーするポリシーを維持し、保護、可用性、機密性を確保します。秘密管理者は、秘密管理要員としての責任を受け入れることを文書化し、正式に認めなければならない。

業務内容は以下の通りですが、これらに限定されるものではありません。

- 証明書は、承認された認証局から発行されなければならない
- 暗号鍵は平文で保存または伝送してはならず、強力な承認済み暗号プロトコルを使用する必要があります。
- 資格情報とシークレットは、少なくとも年に1回ローテーションし、承認された特権的認証管理ツールに保管する必要があります。

7.4 脆弱性管理

アプリケーションやシステムの脆弱性を、自動化された脆弱性スキャンとポートスキャンで定期的に監視しています。

特定された脆弱性は、重要度評価とベンダーの推奨に依存したスケジュールで修正することが要求されます。パッチやアップデート、恒久的な緩和策がない場合は、適切な対策で脆弱性が悪用されるリスクを低減します。

8. 暗号化

8.1 伝送中のデータの保護

Cloud Software Groupは、本サービスの一部であるパブリックネットワークを介して情報を伝送するため、セキュリティで保護された伝送プロトコルを導入しています。本サービスは暗号化によって保護されており、インターネットを介したアクセスはTLS接続によって保護されています。

8.2 静止データの保護

Cloud Software Groupは、サービスを提供するために使用されるすべてのワークステーションが、最低でも128ビットのフルディスク暗号化で暗号化されている

ことを要求します。 お客様のコンテンツは、暗号化されていない限り、いかなるポータブルデバイスにも保存することはできません。

一部のCloud Servicesでは、特定のデータ要素をデフォルトで暗号化し、お客様が実装するためのその他の暗号化機能を提供する場合があります。 詳細については、該当するCloud Servicesのドキュメントを参照してください。

9.物理セキュリティ

9.1 施設

Cloud Software Groupは、あらゆる施設への不正アクセスを防止するために設計された、以下の対策を維持します。

- 施設へのアクセスは許可された個人のみに制限する
- 訪問者はデジタル訪問者ログに登録し、常に付き添われるか観察される必要がある
- 従業員、請負業者、ゲストが施設に入るときはIDバッジを身に付け、常に見える状態にしておく必要がある
- 時間外の施設へのアクセスは、セキュリティによって管理および制御される
- 警備員、侵入検知、および/またはCCTVカメラによる、建物入口、搬出入ドック、および公共アクセスエリアの監視 -（アクセス監視の仕組みは、施設や場所によって異なる場合があります）。

さらに、Cloud Software Groupの施設では以下を備えています。

- 消化システムおよび火災検知システムまたは装置
- 空調システムまたは装置（温度、湿度など）
- アクセス可能な止水栓または遮断弁
- 非常口と避難経路

オフィスに設置されたデータ保管庫は、バッジアクセスにより保護されています。

9.2 データセンター

上記のCloud Software Groupの施設の対策に加え、Cloud Software Groupが所有および管理する施設について、Cloud Software Groupは、本サービスの提供に使用するデータセンターで追加の対策を実施します。

Cloud Software Groupでは、障害回復サイトを使用してセットアップされたグローバルな冗長サービスインフラストラクチャを含む、停電または回線障害によるデータ損失を防ぐように設計されたシステムを使用します。 データセンターとインターネットサービスプロバイダー（ISP）は、帯域幅、遅延、災害回復分離に関するパフォーマンスを最適化するために評価されます。

データセンターは、ISPキャリアニュートラルな施設に設置され、物理的なセキュリティ、冗長電源、インフラストラクチャの冗長性、主要サプライヤーとの稼動時間に関する契約を提供します。

Cloud Software Groupがサードパーティのデータセンターまたはクラウドサービスを使用して本サービスを提供する場合、Cloud Software GroupはCloud Software Groupの施設と同等以上の物理および環境的セキュリティ要件を満たすプロバイダーと契約します。

10.ビジネス継続性および障害回復

10.1 ビジネス継続性

Cloud Software Groupは、過酷な状況や混乱した状況でも業務を継続できるように戦略的に計画し、かかる事象が発生してもサービスが稼働し続けるようにシステムを設計します。

Cloud Software Groupは少なくとも2年に1回、部門レベルのBIA（ビジネスインパクト分析）を実施し、毎年年次レビューを実施します。 BIAは、各部門のBCP（事業継続計画）を作成するために使用されます。BCPは、各部門のリソース要件、復旧パラメータおよび方法、移転の必要性、障害やギャップを回避するためにプロセス全体で必要とされるセキュリティ保護措置を特定し、文書化したものです。 各部門の上級管理者は、毎年または大幅な組織変更が発生したときに、BCPを見直し、承認します。

Cloud Software Groupは、すべてのCloud Software Group施設について危機対応計画および緊急時対応計画を管理しています。 施設が利用できない場合、従業員はその他のCloud Software Groupの施設または従業員が選択した場所でリモートワークを行うことができます。追加の回復戦略は、該当する場合はBCPに記載されています。

10.2 障害回復

Cloud Software Groupは、Cloud Software Groupのビジネスシステムとデータの安定した秩序ある復元と回復を確実に行うよう設計されたプロセスとコントロールを実装することで、サービスや運用の中断による影響を最小限に抑えるよう努めています。 Cloud Software Groupは、すべてのミッションクリティカルなシステム、データ、およびインフラストラクチャに冗長性を実装しています。 DRP（障害回復計画）では、上記のBIAで実施された評価を利用して、障害やギャップを回避するために、プロセス全体で必要とされる復旧時間のパラメータ、方法、優先順位、セキュリティ保護措置を特定し、文書化します。

この計画は、重要なシステムやデータを復元するための全体的な構造とアプローチを概説しています。以下のものが含まれるがこれに限定されません。

- 個人またはチームの役割と責任
- 必須要員またはサードパーティの連絡先情報
- 必須要員のトレーニング要件および計画
- 復旧目標、復元の優先順位、成功の指標
- 全面復旧および復元のスキーマ

上級管理者は、毎年または大幅な組織変更が発生したときに、DRPを見直し、承認します。

11.インシデントの対応

Cloud Software Groupは、Cloud Software Groupの管理対象ネットワーク、システム、またはカスタマーコンテンツに影響を与えるセキュリティインシデントの検出、報告、特定、分析、および対応のプロセスを詳細に記述したサイバーセキュリティインシデント対応計画を保持します。 セキュリティインシデント対応トレーニング、テストを少なくとも

年に1回実施します。

「セキュリティインシデント」とは、機密性、完全性、または可用性の損失の原因となるカスタマーコンテンツへの不正アクセスを意味します。 Cloud Software Groupは、自社の管理下にあるカスタマーコンテンツに対してセキュリティインシデントが発生していると判断した場合、法令で定められた期間内にお客様に通知します。 Cloud Software Groupの通知には、判明している場合は、インシデントの性質、期間、お客様への潜在的な影響が記載されます。

Cloud Software Groupは、各セキュリティインシデントの記録を維持します。

12.ベンダー管理

Cloud Software Groupは、本サービスを実行するために下請業者および代理業者を使用することがあります。 いかなる下請業者および代理業者も、本サービスを実行するために必要な場合に限り、カスタマーコンテンツへのアクセスを許可されるものとし、該当する場合は本別紙によってCloud Software Groupに求められるレベルと同等以上のデータ保護を実施すると定めた書面による契約に拘束されるものとします。 Cloud Software Groupは、該当する場合、かかる下請業者または代理業者による本契約の条項の遵守について常に責任を負うものとします。 カスタマーコンテンツにアクセスすることができるCloud Software Groupの下請処理者のリストは、Trust Centerで参照できます。

12.1 オンボーディング

Cloud Software Groupのサードパーティリスク管理プログラムは、サードパーティのサプライヤーの使用によってもたらされるセキュリティリスクを管理するための体系的なアプローチを提供します。Cloud Software Groupは、かかるサードパーティの調達にあたって、セキュリティリスクの特定、分析、および軽減に努めています。

Cloud Software Groupは、この別紙に指定されている内容と一致する関連セキュリティ対策および義務を文書化するため、サプライヤーと契約を締結します。

12.2 継続的な評価

Cloud Software Groupは、サプライヤーとの関係全体にわたりセキュリティ対策が確実に維持されるように設計された、セキュリティリスク評価を定期的に実施します。 提供するサービスの変更や既存の契約の変更にあたって、その変更が追加または過度のリスクをもたらさないことを確認するためのセキュリティリスク評価が必要です。

12.3 オフボーディング

Cloud Software Groupは、サプライヤーとの関係を終了する計画の最低90日前、またはサプライヤーとの契約満了前に、同社の調達組織に通知するよう努力します（契約が早期に終了されない限り）。 同社の調達組織は、既存の関係の終了を調整し、Cloud Software Groupの企業データやアセットがセキュリティで保護され、適切に取り扱われていることを確認します。

13.遵守

13.1 個人データの取り扱い

個人データとは、識別された、または識別可能な個人に関する情報のことで

す。 カスタマーコンテンツに含まれている個人データについては、お客様が判断するものとします。 本サービスの実行にあたり、Cloud Software Groupはデータ処理者としての役割を担い、カスタマーコンテンツに含まれる個人データについてはお客様がデータ管理者になります。 Cloud Software Groupは、本契約の規定に基づき、かかる個人データの処理についてはお客様の指示に従うものとします。

一般データ保護規則（GDPR）が適用される個人データの取り扱い（かかるデータの国外移転のために必要な仕組みなど）について詳しくは、Cloud Software Groupのデータ処理補遺に記載されています。

13.2 サービスの場所

Cloud Servicesのお客様は、Cloudサービスの地理的な場所の選択を引き続き管理できます。 適用されるCloud Servicesサブスクリプション期間中、いかなる時点においても、Cloud Software Groupは、お客様の同意なしに、お客様が選択した環境の地理的位置を変更することはないものとします。 Cloud Servicesによっては、特定の地理的位置を選択できない場合があり、一般的なサービス提供の一環とし て、お客様のコンテンツは、米国またはCitrixおよび/またはそのサービスプロバイダーが業務を行うその他の国に、サービス 提供のために必要な範囲で転送される場合があることに注意してください。

13.3 カスタマーコンテンツの開示

Cloud Software Groupは、召喚状、司法もしくは行政命令、またはその他の拘束力のある文書（以下、それぞれを「要請」といいます）への対応を含め、法令に基づき要求される範囲内においてカスタマーコンテンツを開示することがあります。 法令によって禁止されている場合を除き、Cloud Software Groupはいかなる要請においても速やかにお客様に通知し、合理的に必要と判断される範囲内において、お客様が速やかに要請に対応できるよう支援します。

13.4 お客様のセキュリティおよび規制要件

本サービスは、より大規模なお客様の IT 環境内で提供されるよう設計されています。したがって、お客様は、本サービスとの技術統合、ユーザーアクセス管理および制御、ならびにお客様が本サービスとともに使用するすべてのアプリケーションおよびネットワークなど、Citrixが明示的に管理しないセキュリティのすべての側面について、全責任を負います。

お客様は、サービスの一部としてカスタマーコンテンツへのアクセスをCloud Software Groupに提供することを含め、本サービスの使用が、本契約（本別紙を含む）に規定されている以上の規制要件またはセキュリティ要件の対象となるかどうかを判断する責任を負うものとします。 したがって、お客様は、本別紙に含まれていない特定の規制を課す法律に準拠するお客様のコンテンツを送信または保存しないようにしなければなりません。 本契約および該当するサービス説明書および両当事者に指定されていない限り、政府の規制に基づいて、防衛物品または防衛サービス、保護医療情報 (「PHI」)、支払いカード情報 (「PCI」)、または管理配布データの輸出入を制限します。 Cloud Software Groupがそのようなデータを処理するために必要となる場合があるため、追加の契約 (HIPAA ビジネス アソシエイト契約など) を事前に締結しています。

14.お客様の監査とお問い合わせ

年に1回を上限として、Cloud Software Groupは、お客様のリスク評価への回答という形で監査依頼に対応します。 また、お客様はいつでもCloud Software Groupのデューデリジェンスパッケージにアクセスし、最新のセキュリティパッケージ及び調査票を入手することができます。 Cloud Software Groupのデューデリジェンスパッケージは、お客様のセキュリティに関するお問い合わせのために作成され、Cloud Software Group Cloud Servicesに関するShared Assessments’ Standardized Information Gathering (SIG) Lite調査票に記入されたものを含む、すぐに利用できるセキュリティ情報を提供しています。 デューディリジェンスパッケージは、Cloud Software Groupの Trust Center in the クラウドアシュアランスのデータ保護とセキュリティセクションからダウンロードすることができます。

15.担当者

00職務 担当者	
カスタマーサポート	https://www.citrix.com/contact/technical-support.html
セキュリティインシデント報告	secure@citrix.com
Cloud Software Groupのサービスに疑われる脆弱性	https://www.citrix.com/about/trust-center/ (「セキュリティ問題を報告する」ボタンをクリックします。

エンタープライズセールス
北米 | 800-424-8749 全世界 | +1 408-790-8000

所在地
本社 | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States シリコンバレー | 4988 Great America Parkway Santa Clara, CA 95054, United States