最終更新日:2018 年 3 月 1 日

Citrix サービスのセキュリティに関する別紙

この「Citrix 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、Citrix のライセンス、サブスクリプション、またはサービス契約に基づく Citrix Cloud サービス、テクニカル サポートサービス、コンサルティング サービスに関連して導入される技術的および組織的なセキュリティ対策について記述したものです。本別紙は、参照によりかかるサービス契約 (以下、「本契約」といいます) に組み込まれるものとします。本別紙は、Citrix Cloud Labs を含む、ベータ版または lab/tech preview サービスには適用されません。
各用語は本契約に記載された、または以下の第 7 条「定義」を含め、本別紙で規定する意味を有するものとします。

第 1 条。 Citrix のセキュリティ対策

本条では、Citrix がサービスおよびお客様に関連するセキュリティの義務を履行するために導入している物理的、論理的、および管理上の対策について記述します。Citrix は、サービス セキュリティ プログラムの基準として、ISO/IEC 27002 を採用しています。

第 1 条 A 項で規定する対策は、すべてのサービスに適用されます。第 1 条 B 項で規定する追加の対策は、一般的に利用可能なすべての Citrix Cloud Services (総称して「クラウド サービス」といいます) に適用されるものとします。

Citrix は、本第 1 条で規定する対策を変更する権利を留保します。ただし、お客様が対価を支払ったサービスの契約期間に導入された対策は、かかる条項の発効日時点で本第 1 条で規定されたカスタマー コンテンツの最低限の保護対策として維持するものとします。

1.A. エンタープライズ セキュリティ対策 – すべてのサービス

分野	対策
セキュリティ プログラム管理	**セキュリティの所有権**。Citrix は、サービスのセキュリティ対策の調整および監視について責任を負う 1 人または複数のセキュリティの責任者を任命しました。 **セキュリティの役割および責任**。カスタマー コンテンツにアクセス可能な Citrix の担当者には、秘密保持義務が適用されます。 **サービス セキュリティ ポリシー**Citrix は、Citrix 経営管理者によって策定および承認された、セキュリティおよび安全に関する全体的な原則を定めた、包括的なグローバル セキュリ

分野	対策
	ティ フレームワーク (GSF) を保持します。ポリシーとは、簡潔明瞭にセキュリティ要件を示したものです。標準とは、ポリシーの要件を満たすためのプロセスまたは方法を定義したものです。GSF セキュリティ プログラムは、定期的にレビューおよび評価を受けます。Citrix は、GSF プログラムの概要を保持し、依頼があればお客様に提供します。 **製品リスク管理。**Citrix は、サービスに関連したリスクの主要分野を評価します。例としては、プライバシー リスク評価、オープン ソース レビュー、エクスポート管理分析などがあります (適用対象となる場合)。
アセット管理。	**アセット一覧。**Citrix は、本サービスを実行するために使用され、Citrix の管理対象である機器 (以下、「アセット」といいます) の一覧を保持します。任命されたシステム担当者は、この一覧を管理し、必要に応じて更新する責任を負います。 **アセットおよびデータの取り扱い** Citrix は、アクセスを適切に制限するため、カスタマー コンテンツを識別および分類します。 Citrix は、カスタマー コンテンツの印刷およびカスタマー コンテンツを含む印刷物の廃棄に制限を課しています。 Citrix の担当者は、カスタマー コンテンツを携帯用デバイスに格納する場合、カスタマー コンテンツにリモート アクセスする場合、または Citrix やサービス プロバイダーによって管理されている施設以外でカスタマー コンテンツを処理する場合については、事前に許可を得る必要があります。
アクセス管理	**アクセス ポリシー。**Citrix は、カスタマー コンテンツにアクセスできる個人のセキュリティ権限の記録を保持し、最小限の権限の原則に従います。 **アクセスの許可** Citrix は、カスタマー コンテンツを含む Citrix システムへのアクセスを許可されている担当者の記録を保持し、更新します。 システムに対する新たなアクセス権は、付与される前に管理者によって審査および承認されます。 Citrix 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、定期的なレビューを実施します。 Citrix は、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 カスタマー コンテンツを含むシステムに複数の個人がアクセスできる場合、Citrix は、かか

分野	対策
	る個人に個別の ID/ログイン資格を割り当てます。 **最小限の権限** Citrix は、カスタマー コンテンツへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人のみに制限します。 **完全性および秘密保持** Citrix は、ユーザーがコンピューターから離れる際には、そのユーザー自身でこのデータを保護することを要求します。 Citrix は、パスワードが、その有効期間中、判読不能状態で管理されることを要求します。 **認証** Citrix は、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを認証します。 認証メカニズムがパスワードに基づいている場合、Citrix は業界標準の規定に従って、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、システム要件および Citrix の標準で規定されたとおり、定期的に更新されます。 パスワードは、8 文字以上にするなど、長さと複雑さの要件を満たす必要があります。 パスワードの共有は禁止されています。 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。 Citrix は、破られた、または不注意で開示されたパスワードを無効化できるものとします。 Citrix は、無効なパスワードを使用して繰り返しサービスにアクセスしようとする試みを監視します。 Citrix 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。
損失防止	**悪質なソフトウェア**。Citrix は、アンチウイルス プログラムおよびその他の対策を使用して、パブリック ネットワークを介して送信される悪質なソフトウェアを含め、悪質なソフトウェアに

分野	対策
	よるカスタマー コンテンツへの不正アクセスを防ぎます。 **メディアの廃棄。**Citrix は、不要になったメディアを、その分類に基づいて、安全な廃棄手順に従って廃棄します。
物理セキュリティおよび環境的セキュリティ (アクセス制御、可用性制御)	**Citrix 施設**への物理アクセス。Citrix は、施設へのアクセスを、許可された個人のみに制限します。従業員、請負業者、ゲストが施設に入るときは ID バッジを身につけ、常に見える状態にしておく必要があります。Citrix は、警備員、侵入検知、CCTV カメラなど各種の手段により、施設の入口を監視します。 **業務中断に対する保護。**Citrix は、障害回復サイトを使用し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システムを使用して、停電または回線障害によるデータ損失を回避し、帯域幅、遅延、障害回復分離に対してパフォーマンスの最適化を図るため、データセンターおよびインターネット サービス プロバイダー (ISP) を評価し、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を備えた、ISP キャリア ニュートラルで安全な施設にデータ センターを設置し、主要サプライヤと稼動時間に関する契約を締結します。 **データ センターのホスティング。**Citrix がサードパーティの共同設置型データ センターを使用してサービスを提供する場合、Citrix は Citrix が管理する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ことをサービス プロバイダーに要求します。下記以上のセキュリティ要件を満たす必要があります。 • 物理的なアクセス制限および予防措置 (認証、ログ、監視など) • 十分に分離された環境 • 消火、火災検知、防火対策 • 空調システム (温度、湿度など) **クラウド コンピューティング。**Citrix は XaaS (Infrastructure as a Service（IaaS)、Platform as a Service (PaaS)、Software as a Service (SaaS)) を使用してサービスを提供します。Citrix は自社のホスティング型データ センターと実質的に同レベルの物理的アクセス制御を提供する XaaS プロバイダーと契約を締結します。
アプリケーションおよび開発に関するセキュリティ	**システムの開発および保守。**Citrix は、Secure by Design (設計による安全性確保) プロセスを保持します。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、およびテストデータの使用に関するセキュリティに対処することを目的とした標準および変更管理の手順が含まれます。このプロセスは、専門のセキュリティ エンジニアリング チームに

分野	対策
	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。 **オープン ソース管理**。Citrix は、ソフトウェアベースのシステムを使用して、オープン ソースのレビューおよび承認を管理します。さらに、Citrix はオープンソースのコンプライアンスに従って、そのソフトウェア製品の定期的なスキャンと監査を実施します。 **変更管理。**Citrix は、情報システムのセキュリティ要件、テスト、テストの承認、およびテストデータの使用に関するセキュリティ要件に対処する変更管理手順を保持します。ソフトウェアおよび構成の変更は、標準のチケット発行システムを使用して管理および追跡されます。
安全な運用	**ネットワーク設計**。Citrix は、カスタマー コンテンツへのアクセスに対するネットワーク制御など、サービスに関連したアクセス管理ポリシーおよび標準を強化するための仕組みを導入します。この仕組みには、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)、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。
インシデント管理	**インシデントの対応**。Citrix は、Citrix 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および安全に関するインシデントを保存、分析、修正、伝達できるように設計されたインシデント対応プログラムを保持します。 **インシデントの通知**。Citrix 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、適用法令で定められた期間内にお客様に通知します。 **インシデントの記録**。Citrix は、既知のセキュリティ インシデントの記録を保持し、この記録には、当該インシデントの説明、期間、結果、報告者名、報告先、データおよびサービスの復旧手順(存在する場合)が含まれるものとします。
ベンダー管理	**オンボーディング**。Citrix は、カスタマー コンテンツ、または本サービス内のカスタマー コンテンツを処理するコンポーネントへのアクセス権を持つサービス プロバイダーのセキュリティ評価を実施します。 Citrix は、本サービスに接続するサービス プロバイダーに対して、その提供するサービスが本項に定めたセキュリティ レベルに準拠していることを要求します。欧州連合の法律の適用対象であり、カスタマー コンテンツにアクセスする可能性があるサービス プロバイダーは、「EU-米国および EU-スイス間のプライバシー シールド」プログラムに従って自己認証を行うか、「標準契約条項」に準拠する必要があります。

分野	対策
	継続的なメンテナンス。サービス プロバイダーは、提供するサービスに関連する機密性およびリスクに基づき、定期的に評価されます。 **オフボーディング。**製品供給者としての関係終了に伴い、サービス プロバイダーは、所有していたすべてのカスタマー コンテンツを返却するか、すべてのカスタマー コンテンツが安全に破壊されたことを証明する必要があります。
ビジネス継続性および障害回復	**ビジネス継続性。**Citrix は、カスタマー コンテンツを処理する Citrix 情報システムが設置される施設について緊急時対応計画を保持します。 **障害回復。**Citrix の冗長ストレージおよびデータの復旧手順は、カスタマー コンテンツを元の状態または最後に複製されたときの状態に戻すことを試みるように設計されています。
セキュリティに関するお客様の義務	お客様は、本サービスの一部として明示的に含まれていないセキュリティを管理する責任を負います。これには以下を含みますが、これらに限定されません。 • カスタマー コンテンツに対する Citrix のアクセスを、お客様が本サービスを受けるために必要なもののみに制限する。 • ネットワークおよびコンピューティング機器を監視および保護するなど、ネットワークおよびサービス コンポーネントを妨害から保護する。 • 本サービスの期間中および終了時に、必要に応じてカスタマー コンテンツをダウンロードする。 • Citrix は、転送するデータをデフォルトで暗号化するか、転送するデータを暗号化する手段をお客様に提供します。詳しくは、本サービスの製品付属文書を参照してください。お客様は、送信中のデータを適切に保護する責任を負います。

1.B. クラウド サービスの追加のセキュリティ対策

分野	対策
データの保護 (可用性制御、通信制御、データの削除)	**フェイルオーバーの手順。**Citrix は、カスタマー コンテンツが利用できなくなる事態に対処する仕組みを導入します。かかる仕組みには、カスタマー コンテンツを処理する主要なコンピューター機器が設置された場所とは別の場所に、カスタマー コンテンツのコピーを保管することが含まれます。 **境界を越えるデータ。**Citrix は本サービスの一環として、パブリック ネットワークを介して送信されるカスタマー コンテンツを暗号化するか、またはお客様が暗号化できるようにします。 **保持。**Citrix は、合法的な目的で必要な場合にお客様がアクセスできるように、本サービス

分野	対策
	期間終了後もカスタマー コンテンツを保持できるものとします。Citrix はカスタマー 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。ただし以下の直接返却に該当する場合、Citrix はサービス期間終了後にカスタマー コンテンツを保持する義務を負わないものとします。 **返却。**可用性と該当するサービス ディスクリプションに基づいて、お客様は、失効後 30 日以内はカスタマー コンテンツをダウンロードできるものとします。 **データの削除。**Citrix は、正当な目的のため保持する必要がなくなったカスタマー コンテンツを安全に削除するものとします。
安全な運用	**イベントのログ。**特定のサービスにおいて、Citrix はログを収集します。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、その他関連アクティビティが含まれます。 ログは、(i) 本サービスおよび関連する分析の提供、セキュリティ保護、管理、測定、および改善のため、(ii) お客様またはそのユーザーの指示に従うため、ならびに (iii) Citrix のポリシー、適用法令、規制、または政府指令を遵守するために使用されます。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ます。お客様はその監視を禁止したり妨げることはできません。 Citrix は上記の目的のため、ログを補足するためサードパーティから収集した情報を使用する場合があります。 ログは、本別紙で指定されていない目的のため、集約された形式で使用される場合があります。
ビジネス継続性および障害回復	**バックアップ。**各サービス ディスクリプションに特に明記されていない限り、サービスは複数の物理サイトにまたがる高可用なアクティブ/アクティブ クラスターで保持されます。アクティブ/アクティブ構成で保持されないシステムは、当該サービスのサービス レベル目標に従ってバックアップされます。

第 2 条。　　<u>個人データの取り扱い</u>

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、Citrix 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。Citrix 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。

EU 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、別紙 I「EU一般データ保護規則 (GDPR) 条項」を参照してください。

第 3 条。　　サービスの場所

カスタマー コンテンツは、Citrix またはそのサービス プロバイダーが事業を行う米国またはその他の国に移転されたり、それらの国で保存、処理される場合があります。本別紙の要件は、カスタマー コンテンツが保存または処理される場所にかかわらず適用されるものとします。

Citrix のサービスの提供に関連し、適法な国外へのデータ移転を円滑に行うために必要なさらなるデータ処理契約またはデータ移転契約について、両当事者は誠実に協議を行うものとします。

第 4 条。　　カスタマー コンテンツの開示

お客様は、本条に規定するカスタマー コンテンツの Citrix による開示に同意するものとします。
Citrix は、本サービスの実行にあたり下請業者または代理業者に委託する場合があります。いかなる下請業者または代理業者も、本サービスの実行に必要とされる場合に限り、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 Citrix 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。Citrix 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。

Citrix はさらに、以下の条件でカスタマー コンテンツを開示する場合があります。(a) 本契約に合致する目的で系列会社に開示する場合、(b) 今後または現時点でのかかる事業の一部または全部の合併、買収、販売、破産、またはその他の再編成に関連して、本契約の条項の対象となるカスタマー コンテンツを保護する義務に従う場合、(c) 権利の行使、詐欺の検知および予防、および Citrix、お客様、ユーザー、または公衆の権利または資産に対する損害からの保護を含む法的目的を満たす必要がある場合、および (c) 召喚状、裁判所命令または行政命令、その他の法的拘束力 (以下、それぞれ「要請」といいます) への対応を含め、法令に基づき要求された場合。法令によって禁止されている限度を除き、Citrix 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。

第 5 条。　　お客様の義務

1. 一般。お客様は本契約で許可された範囲においてのみ本サービスを使用し、アクセスできるものとします。お客様は本サービスの使用に関連して適用されるすべての法令を遵守するものとします。

2. 権限。お客様は、本別紙に記載されたカスタマー コンテンツに Citrix がアクセスし、処理するために必要なあらゆる通知の実行、同意またはライセンスの取得を含め、Citrix が本サービスを実行するために必要なすべての権限の取得について責任を追います。

3. 規制。お客様は、いかなるカスタマー コンテンツにおいても、本別紙を含む、本契約の規定以外に追加の規制またはセキュリティ要件に従う必要があるかどうか判断する必要があります。お客様は、アメリカ合衆国国際武器取引規則 (ITAR) もしくは防衛物資または防衛サービスの輸出入を制限する各国の同様の規制で管理されているカスタマー コンテンツを送信または保存してはなりません。さらにお客様は、お客様の指示および該当するサービス ディスクリプションで指定され、かかるデータを処理するために事前に Citrix が要求する追加契約 (BAA (業務協力契約) など) を当事者間で締結した場合を除き、保護されるべき医療情報 (「PHI」)、支払いカード情報 (「PCI」)、または政府の規制に基づき制御される配布データなど、追加の規制要件に従う必要があるカスタマー コンテンツを提供または保存してはいけません。ShareFile サービスのお客様で BAA を必要とされる場合は、Citrix (privacy@sharefile.com) までお問い合わせください。

4. お客様のセキュリティ環境。本サービスは、 お客様の大規模なセキュリティ環境内でのみ提供される設計になっています。お客様は、本サービスと連動して使用するアクセス制御、ファイアウォール、アプリケーションおよびネットワークを含むがそれらに限定されない、Citrix によって明示的に管理されていないすべてのコンポーネントのために、適切なセキュリティ機能を確保するものとします。セキュリティに関するお客様の義務については、上記の第 1 条 A 項を参照してください。

5. セキュリティの通知。お客様は、第 6 条で規定するサービスまたはカスタマー コンテンツに関わるいかなるセキュリティ インシデントについても、速やかに以下の Citrix の担当者に連絡するものとします。

6. ユーザーによる遵守。お客様のユーザーによる注文条件および本契約の遵守については、お客様が責任を負います。

第 6 条。 Citrix の担当者

職務	担当者
カスタマー サポート	https://www.citrix.com/contact/technical-support.html
インシデント報告	secure@citrix.com
Citrix 製品の脆弱性の疑い	secure@citrix.com

第 7 条。 定義

本別紙の用語は、本契約または以下に定める意味を有するものとします。本契約の残りの規定と以下の定義との間で矛盾がある場合は、以下の定義が本別紙に適用されるものとします。

「カスタマー コンテンツ」 とは、保存のためお客様のアカウントにアップロードされたすべてのデータ、またはお客様のコンピューティング環境において Citrix がサービスを提供するためにアクセスを許可されたデータを意味します。

「ログ」とは、パフォーマンス、安定性、使用状況、セキュリティ、およびサポートを測定した記録を含む、本サービスに関連するイベントの記録を意味します。

「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。