Teachme Biz セキュリティチェックシート

■本チェックシートは、ビジュアルSOPマネジメントプラットフォーム「Teachme Biz」のセキュリティ対策について、ISMSの管理策をもとに記載したものです。
■株式会社スタディストは、ISMS認証を取得しています。
・ISO/IEC 27001:2013　認証登録番号：IS 618934
・ISO/IEC 27017:2015　認証登録番号：CLOUD 660517

管理策分類	規定内容	対応
A.5.1 情報セキュリティのための経営陣の方向性	**情報セキュリティのための方針群** 情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知しなければならない。	当社CTO及び情報セキュリティ委員長によって承認されたセキュリティに関する基本方針を定めております。 当方針は、全従業員には社内規程として周知し、当サービス利用者にはホームページ（https://studist.jp/security/ ）にて公表しております。
A.6.1 内部組織	**情報セキュリティの役割及び責任** クラウドサービスプロバイダは、そのクラウドサービスカスタマ、クラウドサービスプロバイダ及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化することが望ましい。	利用規約（https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）第9条（自己責任の原則）、第10条（利用者および管理責任者）、第16条（非保証及び免責）にて定義しております。
	関係当局との連絡 クラウドサービスプロバイダは、クラウドサービスカスタマに、クラウドサービスプロバイダの組織の地理的所在地、及びクラウドサービスプロバイダが、クラウドサービスカスタマデータを保存する可能性のある国を通知することが望ましい。	当社所在地は、ホームページ（http://studist.jp/ ）にて公表しております。 お客様のデータはAWS（Amazon Web Service）のアジアパシフィック（東京）リージョンに保管しております。
CLD.6.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係	**クラウドコンピューティング環境における役割及び責任の共有及び分担** クラウドサービスの利用に関して共有し分担する情報セキュリティの役割を遂行する責任は、クラウドサービスカスタマ及びクラウドサービスプロバイダのそれぞれにおいて特定の関係者に割当て、文書化し、伝達し、実施することが望ましい。	利用規約（https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）第9条（自己責任の原則）、第10条（利用者および管理責任者）、第16条（非保証及び免責）にて定義しております。
	情報セキュリティの意識向上、教育及び訓練 組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受けなければならず、また、定めに従ってその更新しなければならない。	入社時及び年1回、全従業員に対して情報セキュリティに関する教育を実施しております。
A.8.1 資産に対する責任	**資産目録** 情報及び情報処理施設に関連する資産を特定しなければならない。また、これらの資産の目録を、作成し、維持しなければならない。	各情報資産について「情報資産管理台帳」を作成し、年1回見直しを実施しております。

管理策分類	規定内容	対応
	クラウドサービスカスタマの資産の除去 クラウドサービスプロバイダの施設にあるクラウドサービスカスタマの資産は、クラウドサービスの合意の終了時に、時期を失せずに除去又は必要な場合には返却されることが望ましい。	利用規約（https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）第27条3項（契約終了後の処理）にて定義しております。
	情報のラベル付け クラウドサービスプロバイダは、クラウドサービスカスタマが情報及び関連資産を分類し、ラベルづけするためのサービス機能を文書化し、開示することが望ましい。	フォルダ・サブフォルダ・検索タグ等、当サービス内に保存するマニュアルを適切にラベル付けできる機能を提供しております。ご利用方法につきましては、オンラインマニュアルにてご案内しております。
A.9.2 利用者アクセスの管理	**利用者登録及び登録解除** クラウドサービスカスタマのクラウドサービスユーザによるクラウドサービスへのアクセスを管理するため、クラウドサービスプロバイダは、クラウドサービスカスタマに利用者登録・登録削除の機能及びそれを利用するための仕様を提供することが望ましい。	お客様側で利用者の登録・更新・削除を実施する機能及び権限管理機能を提供しております。ご利用方法につきましては、オンラインマニュアルにてご案内しております。
	利用者アクセスの提供 クラウドサービスプロバイダは、クラウドサービスカスタマのクラウドサービスユーザのアクセス権を管理する機能及びそれを利用するための仕様を提供することが望ましい。	お客様側でフォルダごとにアクセス権を制限する機能、グループやフォルダに対してIPアドレス制限をかける機能、指定端末以外からのアクセスを制限する機能等、様々な利用者アクセス方法を提供しております。 詳細については、サービスのWebサイトの機能紹介ページ（https://biz.teachme.jp/function/list/#management ）をご確認ください。
	特権的アクセス権の管理 クラウドサービスプロバイダは、クラウドサービスカスタマのクラウドサービス実務管理者がその役割を行えるように、クラウドサービスカスタマが特定するリスクに応じた、十分に強い認証技術を提供することが望ましい。例えば、クラウドサービスプロバイダは、多要素認証機能を提供し、又は第三者の多要素認証メカニズムを利用可能とすることが望ましい。	現在多要素認証には対応しておりません。
	利用者の秘密認証情報の管理 クラウドサービスプロバイダは、秘密認証情報を割り当てる手順、及び利用者認証手順を含む、クラウドサービスカスタマの秘密認証情報の管理のための手順について情報を提供することが望ましい。	パスワードの発行・変更及び再発行の手順について、オンラインマニュアルにてご案内しております。

管理策分類	規定内容	対応
A.9.4 システム及びアプリケーションのアクセス制御	**情報へのアクセス制限** クラウドサービスプロバイダは、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスで保持するクラウドサービスカスタマデータへのアクセスを、クラウドサービスカスタマが制限できるように、アクセス制御を提供することが望ましい。	お客様データへのアクセスを、管理者・副管理者・メンバー・ゲストなどの権限によって制御できる機能を提供しております。 詳細についてはサービスのWebサイトの機能紹介ページ（https://help.teachme.jp/hc/ja/articles/4403398967961）をご確認ください。
	特権的なユーティリティプログラムの使用 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。	お客様サポートを目的とした各種特権的なユーティリティプログラムを運用しておりますが、利用できる従業員の制限及び定期的なアクセス権限の棚卸し、監査ログの取得等を適切に実施しております。 棚卸しについては従業員の退職時及び年次での実施をしております。
CLD.9.5 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御	**仮想コンピューティング環境における分離** クラウドサービス上で稼働するクラウドサービスカスタマの仮想環境は、他のクラウドサービスカスタマ及び認可されていない者から 保護することが望ましい。	マルチテナンシー環境でサービスを提供しておりますが、お客様同士のデータは論理的に分離しております。
	仮想マシンの要塞化 クラウドサービスカスタマ及びクラウドサービスプロバイダは、仮想マシンを設定する際には、適切な側面からの要塞化（例えば、必要なポート、プロトコル及びサービスだけを有効とする。）及び利用する各仮想マシンへの適切な技術手段（例えば、マルウェア対策、ログ取得）の実施を確実にすることが望ましい。	IPアドレス、ポート番号、プロトコルに関してAWSのセキュリティグループで制限することで要塞化を実現し、仮想マシンへの接続には秘密鍵やMFAを利用した多要素認証を必須としております。 また、マルウェア対策ソフトの導入やアクセスログ取得を実施しております。
A.10.1 暗号による管理策	**暗号による管理策の利用方針** 情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施しなければならない。	データベースに保存しているデータの暗号化(AES-256)、及び通信の暗号化(TLS1.2)を実施しております。
	装置のセキュリティを保った処分又は再利用 クラウドサービスプロバイダは、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用を時期を失せずに行うための取り決めがあることを確実にすることが望ましい。	当サービスは全てクラウドインフラ(AWS)上にて運用しております。 クラウドインフラの装置管理についてはAWSのホワイトペーパー（https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/ セキュリティプロセスの概要 A P8）で、ストレージデバイスの廃棄についてセキュリティ的に安全な旨、記載されております。
	変更管理 クラウドサービスプロバイダは、クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更について、クラウドサービスカスタマに情報を提供することが望ましい。	お客様の情報セキュリティに悪影響を与えうる変更については、事前にメールにてご案内いたします。

管理策分類	規定内容	対応
	容量・能力の管理 要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整しなければならず、また、将来必要とする容量・能力を予測しなければならない。	主要な資源に関して、負荷上昇時に自動的に容量/能力が強化される仕組みを導入しております。 自動的に容量/能力が強化されない資源については、原則として5分毎にリソース状況の監視を行い、必要に応じた増強を実施しております。
	実務管理者の運用のセキュリティ クラウドサービスプロバイダは、要求するクラウドサービスカスタマに、重要な操作及び手順をを文書化して提供することが望ましい。	ご利用方法につきましては、オンラインマニュアルにてご案内しております。
A.12.3 バックアップ	**情報のバックアップ** クラウドサービスプロバイダは、クラウドサービスカスタマに、バックアップ機能の仕様を提供することが望ましい。	インフラ環境全体として定期的なバックアップを実行している他、お客様がご自身でデータのバックアップを管理できる機能を提供しております。 サービス全体のフルバックアップについては日次で実行しており、保持期間は3日間です。復旧にかかる所要時間は約1時間です。 当サービスとしてはオプションでバックアップ機能を提供しております（ご契約によっては基本プランとして含まれている場合もあります）。 グループ内の全マニュアルを毎日定時に自動バックアップ（差分バックアップ）しており、任意のタイミングでのバックアップも可能です。 データとしては、30日前までと同じ状態のマニュアルを保管しております。復旧手順はオンラインマニュアルにてご案内しております。復旧に要する時間は、ネットワーク環境にもよりますが通常数秒程度です。
A.12.4 ログ取得及び監視	**イベントログ取得** クラウドサービスプロバイダは、クラウドサービスカスタマに、ログ取得機能を提供することが望ましい。	全ての接続端末からの最終アクセス時刻を確認する機能を提供しております。 また、オプションでレポート機能（マニュアルに対する閲覧ログ表示）を提供しております（ご契約によっては基本プランとして含まれている場合もあります）。 サービス全体としては、Teachme Biz利用者からのアクセスログやエラーログを取得し、保管しております。
	クロックの同期 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させなければならない。	NTPを使用し時刻同期を行っております。
	クラウドサービスの監視 クラウドサービスカスタマは、クラウドサービスカスタマが利用するクラウドサービスの操作の特定の側面を監視する能力を持つことが望ましい。	WAF及びIPS, IDSを導入しております。 上記のほか、インフラ環境に対する悪意ある操作や不正な動作を継続的にモニタリングし、脅威を検出する仕組みを導入しております。

管理策分類	規定内容	対応
A.12.6 技術的ぜい弱性管理	**技術的ぜい弱性の管理** 利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得しなければならない。また、そのようなぜい弱性に組織がさらされている状況を評価しなければならない。さらに、それらと関連するリスクに対処するために、適切な手段をとらなければならない。	利用しているライブラリのCVE情報を検知する仕組みを導入しております。必要に応じたパッチ適用を合わせて実施しております。
	ネットワークの分割 情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離しなければならない。	マルチテナンシー環境でサービスを提供しているため、お客様同士の環境は論理的に分離されております。 また、当社インフラ環境はお客様の環境とネットワーク的に分離しております。
A.14.1 情報システムのセキュリティ要求事項	**情報セキュリティ要求事項の分析及び仕様化** クラウドサービスプロバイダは、クラウドサービスカスタマが利用する情報セキュリティ機能に関する情報をクラウドサービスカスタマに提供することが望ましい。	情報セキュリティ機能に関する情報は、サービスのWebサイト（https://biz.teachme.jp/function/security/ ）にて公表しております。
A.14.2 開発及びサポートプロセスにおけるセキュリティ	**セキュリティに配慮した開発のための方針** クラウドサービスプロバイダは、開示方針に合致する範囲で、適用しているセキュリティに配慮した開発の手順及び実践に関する情報を提供することが望ましい。	第三者機関によるアプリケーション脆弱性診断を年1回受診し、サービスのWebサイト （https://biz.teachme.jp/function/security/ ）にて公表しております。
	供給者との合意におけるセキュリティの取扱い クラウドサービスプロバイダは、クラウドサービスカスタマとの間で誤解が生じないことを確実にするために、合意の一部として、クラウドサービスプロバイダが実施する、クラウドサービスカスタマに関係する情報セキュリティ対策を特定することが望ましい。	情報セキュリティ及びサービスレベルについては利用規約 （https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_cloudservicelevel_checklist.pdf ）にて明記し、お客様と合意を取っております。 また、サービスのWebサイト（https://biz.teachme.jp/function/security/ ）上で情報セキュリティ対策について公表しております。
	ICTサプライチェーン クラウドサービスプロバイダがピアクラウドサービスプロバイダのクラウドサービスを利用する場合、情報セキュリティ水準を自身のクラウドサービスカスタマに対するものと同等又はそれ以上に保つことを確実にすることが望ましい。	当サービスは、IaaSとしてAWS（Amazon Web Service）を利用しております。 AWSのホワイトペーパー （https://d0.awsstatic.com/International/ja_JP/Whitepapers/AWS%20Security%20Whitepaper.pdf ）を確認し、セキュリティ上特段の問題がないと判断しております。

管理策分類	規定内容	対応
A.16.1 情報セキュリティインシデントの管理及びその改善	**責任及び手順** 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立しなければならない。	「情報資産管理台帳」において情報資産を一覧管理しております。また、「自社が保有する情報資産、情報システム、提供サービスに対する脅威や侵害などの事案」はセキュリティインシデントにあたるものとして対処し、利用規約（http://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）にて責任の割り当てを明確にしております。 情報セキュリティ委員長 をインシデント発生時の責任者として設置し、開発管掌役員他関係者と連携して迅速に対応に当たります。
	情報セキュリティ事象の報告 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告しなければならない。	お客様から当社へは、当サービスのお問い合わせフォーム（https://studist.force.com/tmbsupport/s/）経由でご連絡いただけます。また、当社からお客様へのご報告は、サービスのWebサイト（https://biz.teachme.jp/ ）及びメールにて実施いたします。
	証拠の収集 組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用しなければならない。	利用規約（https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）第18条（契約者コンテンツの保護）にて定義しております。
A.18.1 法的及び契約上の要求事項の順守	**知的財産権** 知的財産権及び権利関係のあるソフトウェア製品の利用に関する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施しなければならない。	利用規約（https://d3hszuitxs3pnr.cloudfront.net/doc/teachmebiz_terms.pdf ）第9条（自己責任の原則）3項、第18条（契約者コンテンツの保護）にて定義しております。
	記録の保護 記録は、法令、規制、契約及び事上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護しなければならない。	お客様データへの各種アクセスログの他、インフラ環境の各種操作ログについても取得し、永続化しております。現状ログの保管期間は無期限としております。
	暗号化機能に対する規則 暗号化機能は、関連する全ての協定、法令及び規制を順守して用いなければならない。	全ての通信経路について、TLS1.2/AES_128_GCMを利用した暗号化を施しております。 また、お客様データについてはAES-256暗号化アルゴリズムを利用したデータベースに保管しております。
A.18.2 情報セキュリティのレビュー	**情報セキュリティの独立したレビュー** クラウドサービスプロバイダは、クラウドサービスプロバイダが主張する情報セキュリティ管理策の実施を立証するために、クラウドサービスカスタマに文書化した証拠を提供することが望ましい。	ISMS認証を取得し、年1回審査を受審しております。 ・ISO/IEC 27001:2013　認証登録番号：IS 618934 ・ISO/IEC 27017:2015　認証登録番号：CLOUD 660517