Your Desk

セキュリティチェックシート

更新日付：2023/9/22

経済産業省のガイドラインに基づき、サイオステクノロジー株式会社（以下、「当社」という。）が提供する「YourDesk」（以下、「本サービス」という。）のセキュリティについてまとめたものです。
本チェックシートの項目は、経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版を基に、任意で項目の追加削除、及び主客体の解釈を加えて作成したものです。
本チェックシートは、予告なく変更することがあります。

	確認事項	実施の有無	備考
1．セキュリティ基本方針			
1	経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	○	当社情報セキュリティ総括責任者によって承認された情報セキュリティ基本方針を定めています。 当方針は、全従業員には社内規程として周知し、クラウドサービス利用者には当社ウェブサイトにて公開いたしております。 ・情報セキュリティ基本方針 https://www.sios.com/ja/company/governance/infomationsecurity/
2	情報セキュリティに関する基本方針を定めた文書は、定期的またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	○	情報セキュリティマネジメントシステム(以下、「ISMS」といいます。)を構築し、情報セキュリティ保全活動を効果的に推進するため情報セキュリティの基本方針を定めています。 また、ISMSの見直しを定期的に実施することで、環境変化に合わせた情報セキュリティ対策の適切な維持、改善を図っております。
2．情報セキュリティのための組織			
	2－1．内部組織		
1	経営陣は、情報セキュリティに関する取り組みについての責任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	○	当社は情報セキュリティ管理委員会を社内に設置し、情報セキュリティに関する取り組みを積極的に運用・監視する仕組みを構築しております。 経営陣は情報セキュリティ管理委員会の活動を支援し、活動内容について承認を行っております。
2	情報セキュリティ責任者とその役割を明確に定めること。またクラウドサービスの情報セキュリティに関する窓口を明確にし、外部に公開すること。	○	情報セキュリティ管理委員会を統括する情報セキュリティ総括責任者を設定し、情報セキュリティマネジメントマニュアルにてその役割を明示しております。 利用者に対してはクラウドサービスの情報セキュリティに関する窓口をご案内いたしております。 https://support.yourdesk.jp/
3	情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化すること。	○	情報セキュリティ管理規程、及び情報セキュリティマネジメントマニュアルにて、情報セキュリティ対策の手順、運用ルールなどを明記しております。
4	クラウドサービス利用者がクラウドサービスの受け入れを行うために必要な資料を作成し、提供すること。また、提供するクラウドサービスSLA などサービス開始前の合意事項をクラウドサービスの利用を検討する者に明示すること。	○	経済産業省のガイドラインに沿ったサービスレベル目標を提供いたしております。また IPA のウェブアプリケーションのセキュリティ実装 チェックリストに対する当サービスの回答も合わせて提供いたしております。
5	クラウドサービスのサポート窓口、苦情窓口を明確にし、外部に公開すること。	○	各種お問い合わせ、リリース情報、お知らせの掲載を下記ウェブサイトにて行っております。 https://support.yourdesk.jp/
3．人的資源のセキュリティ			
	3－1．雇用前		
1	従業員のセキュリティの役割及び責任は、情報セキュリティ基本方針に従って定め、文書化すること。また該当文書を雇用予定の従業員に対して説明し、この文書に対する明確な同意をもって雇用契約を結ぶこと。	○	雇用形態に関わらず、雇用契約書及び、社内規定にて定めております。
	3－2．雇用期間中		
1	すべての従業員に対して、情報セキュリティに関する意識向上のための教育・訓練を実施すること。	○	雇用形態に関わらず、入社オリエンテーションの一環でコンプライアンス研修、セキュリティ研修を実施しており、社内規程についての教育を行っております。 また ISMS の適用範囲の従業員に対しては年に一度コンプライアンス研修、セキュリティ研修を実施いたしております。
2	セキュリティ違反を犯した従業員に対する対応手続きを備えること。	○	当社就業規則に規定された懲戒の対象となることが、情報セキュリティ管理規程に明記されております。
	3－3．雇用の終了又は変更		
1	従業員の雇用の終了または変更となった場合に、情報資産、アクセス権等の返却・削除・変更の手続きについて明確にすること。	○	情報セキュリティ管理規程に明記されております。
4．資産の管理			
1	情報資産について明確にし、重要な情報資産の目録及び各情報資産の利用の許容範囲に関する文書を作成し、維持すること。また情報資産について管理責任者を指定すること。	○	情報資産台帳で各資産名、管理責任者、C.I.Aレベル、利用許可範囲、情報コンテナ、保存期間ごとに分類し記載しております。 当台帳はISMSにおいて、定期的に見直しを行い更新しております。
2	組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から情報資産を分類すること。	○	
5．物理的及び環境的セキュリティ			
1	重要な情報資産がある領域を保護するために、物理的セキュリティ境界(例えば、有人受付、カード制御による入口)を用いること。	○	情報資産がある執務スペースと共有及びフリースペースはセキュリティカードにより物理的な境界を設けております。
2	重要な情報資産がある領域へ許可された者のみがアクセスできるように入退室等を管理するための手順、管理方法を文書化すること。	○	重要な情報資産がある領域は、情報セキュリティ管理規程に明記されており、許可された者のみがアクセスできるようにセキュリティカードにより制御をしております。
3	サーバーが設置されているデータセンターは耐震構造となっていること。	○	当社が利用契約を締結しているデータセンターにより各種対策が講じられております。
4	データセンターの落雷対策を確認すること。	○	
5	データセンターの水害対策を確認すること。	○	
6	データセンターの静電気対策を確認すること。	○	
6．運用のセキュリティ・アクセス制御			
1	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	○	アプリケーション、OS、サーバー、ネットワーク機器の運用管理手順に関して文書を作成し管理しております。また変更があった場合に都度文書の更新を行っております。 ※仮想環境となるため論理的なサービスの単位での管理となります。
2	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	○	利用者に影響を及ぼす変更につきましては、サポートサイトならびにメールにて事前に通知を行っております。
3	クラウドサービスを利用できるオペレーティングシステムやウェブブラウザの種類とバージョンを明示すること。利用できるOSとブラウザに変更が生じる場合は事前に通知すること。	○	サービスサイト内に動作環境を掲載しております。変更があった際にはサポートサイトならびにメールにて周知を行っております。 https://support.yourdesk.jp/
4	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	IPA のセキュリティ対策情報を随時受信し、日次で脆弱性情報を収集しております。また発表された脆弱性に対して、本サービスに与える影響を評価し、運用手順に沿って修正パッチの適用を行っております。
5	クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	○	常時資源の監視を行っております。利用状況に応じて計画を立てた上で資源の増強を行い、またその内容は文書化しております。
6	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	○	リリースごとに内部チェックを行い、定期的にツールによる脆弱性診断を行っております。
7	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また、認可されていないモバイルコードを実行できないようにすることが望ましい。	○	モバイルコードの利用はありません。

	確認事項	実施の有無	備考
8	クラウドサービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	○	利用者の情報はリアルタイムでレプリケーションによる複製が取られており、かつ日次でバックアップが行われております。 ソフトウェア及びソフトウェアの設定については変更があるたびにバージョン管理されております。
9	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	○	常時サービスの監視を行っております。サービスが停止した際はサポートサイトならびにメールにて通知を行っております。
10	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	○	
11	システムの運用担当者の作業については記録すること。	○	システムの運用担当者の操作ログをすべて保管しております。
12	例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログのアラートについては定期確認し、改竄、許可されていないアクセスがないように保護する。	○	監査ログは監視システムによる監視対象となっており、例外やログの改竄などはリアルタイムにアラートされ、当該事象は監視システム上のイベントログとして保存されております。
13	クラウドサービス上で取得する利用者の活動、例外処理及びセキュリティ事象を記録した監査ログについて明示すること。また監査ログの保持する期間、提供方法、提供のタイミングについて明示すること。	○	サポートサイトにて監査ログについて言及いたしております。利用者へ監査ログの提供は行っておりません。 https://support.yourdesk.jp/
14	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	○	NTPを利用して正確な時刻源と時刻同期を実施しております。
15	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	○	クラウド基盤システムへのアクセスについては当社の運用規則に則り、各個人に一意な識別子を割り当てております。 またシステムへのアクセスは経路を限定し、セキュアな認証方式を採用し、これを運用規則として定めております。
16	クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	○	システムへのアクセス権限の追加・削除・変更の方法については手順の文書化を行なっております。特権については運用管理担当者のみとしております。
17	システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	○	パスワードは運用規則に則り、適切に管理しております。
18	クラウド事業者は、クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう、クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	○	多要素認証、IP アドレス制限、IdP 連携による各種認証方式を提供いたしております。またその設定を利用者の管理アカウントにて設定できることを提示しております。
19	提供するクラウドサービスにおいてアクセス制御機能を提供すること。	○	
20	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。 ネットワーク若しくはインタフェースの分離がなされていない場合、クラウド事業者は、アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。 クラウド事業者は、クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために、クラウド環境における情報セキュリティについて評価を実施することが望ましい。	○	サービスへのアクセスはすべて暗号化されており、また各利用者は一意な識別子により、論理的に別の利用者とデータが分離されております。 システムへのアクセスは公開エリアからの経路では到達し得ない構成となっております。
21	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	○	利用者の ID 登録・削除機能を提供しております。
22	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	○	アカウントごとに権限を設定・変更する機能を提供しております。
23	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	○	利用者ごとにパスワードの複雑性を設定する機能を提供しております。
24	提供するクラウドサービスで提供している情報セキュリティ対策及び機能を列記し、明示すること。		セキュリティ対策及び機能については、サービスサイトにて公開しております。また当該サービスに関する各種セキュリティチェックシートを提供いたしております。 https://www.yourdesk.jp/function/
25	一定の使用中断時間が経過したときには、使用が中断しているセッションを遮断すること。またリスクの高い業務用ソフトウェアについては、接続時間の制限を利用すること。	○	セッションには有効期限が設定されております。また利用者の管理アカウントにて時限ログアウトを設定することが可能となっております。
26	ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	○	アクセスの種類ごとに経路を限定するアクセス制御を設定しております。
27	ネットワーク管理者の権限割り当て及び利用は制限し、管理すること。またネットワーク管理者もアクセスを管理するためにセキュリティに配慮したログオン手順、認証技術によって制御すること。	○	ネットワーク管理者の権限は運用管理担当者のみ保有しております。 アカウントの認証に関しては運用規則にて定めております。
28	外部及び内部からの不正なアクセスを防止する装置(ファイアウォール等)を導入すること。また利用することを許可したサービスへのアクセスだけを提供すること。	○	ファイアウォールに相当するアクセス制御の機構を導入しております。 アクセスの種類ごとに経路を限定しております。
29	クラウドサービスへの接続方法に応じた認証方法を提供すること。クラウドサービスへの接続方法に応じた認証方法を、クラウドサービスの利用を検討するものに明示すること。	○	提供するクラウドサービスにおける認証方式、及びセキュリティ対策及び機能については、サービスサイトにて公開しております。 https://www.yourdesk.jp/function/
30	クラウドサービスの契約が終了した場合にデータが消去されること。消去されるなら、その時期や削除される範囲について確認すること。	○	契約終了後速やかに個人情報や入力データを削除することを、その手順と共に運用規則にて定めております。
31	クラウドサービスを利用するネットワーク経路が暗号化されていることを確認すること。クラウドサービスで利用する情報がシステム上で暗号化されていること。	○	ネットワーク経路はすべて暗号化されております。 サービスで利用されるデータは暗号化されたデータベースにより管理されております。
7．供給者関係			
1	外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること。	○	当社にて外部組織を利用する場合は、当社規定に則りセキュリティ要求事項を含んだ正式な契約書を締結することになっております。
8．情報セキュリティ事象・情報セキュリティインシデント			
1	すべての従業員は、システムまたはサービスの中で発見したまたは疑いをもったセキュリティ弱点はどのようなものでも記録し、報告するようにすること。	○	情報セキュリティ管理規程、及び情報セキュリティマネージメントマニュアルにて、セキュリティ弱点に関する報告の範囲、報告方法、対応の手順を定め、これに則った運用を行っております。
2	情報セキュリティインシデントに対する迅速、効果的で毅然とした対応をするために責任体制及び手順書を確立すること。	○	当社ではセキュリティインシデントに迅速に対応するため、社内に情報セキュリティ管理委員会を設置しており、情報セキュリティマネージメントマニュアルにて、その権限、責任範囲、報告・対応手順を定めております。
3	情報セキュリティインシデントの報告をまとめ、定期的にクラウド利用者に明示すること。	○	情報セキュリティインシデントが発生した場合、利用者に対して適宜サポートサイトにて、情報開示、報告を行っております。 https://support.yourdesk.jp/

	確認事項	実施の有無	備考
9．事業継続マネジメントにおける情報セキュリティの側面			
1	業務プロセスの中断を引き起こし得る事象は、中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに特定すること。	○	事業継続に関する規定を定めており、大規模災害やインシデント発生時にはこの規定に則り、リスク評価及び対応を行います。
2	クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	○	すべてのサーバー、ネットワーク、データベースについて冗長化構成を構築しております。 セキュリティリスクの観点から利用者に対しては、システム構成の概要のみ明示しております。
3	事業継続計画については定期的に試験・更新すること。	○	事業継続に関する規定は定期的に監査を行っております。
4	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	○	当社が利用契約を締結しているデータセンターにより各種対策が講じられております。
5	クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	○	
10．順守			
1	関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を明確に定め、文書化し、維持すること。また重要な記録については消失、破壊及び改ざんから保護し、適切に管理すること。	○	ISMS に影響を及ぼす可能性のある変更（関連する法令、国の定める指針その他の規範と改正状況を反映した資源、組織、規定、規格の変更）は、ISMS の中で確認されることになっております。 ISMS に作成・利用される文書・記録は文書ごとに、管理者、承認者、保管期間を定め、適切に管理しております。
2	クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。	○	本サービスは国内のデータセンターにて運用、データの保管を行っております。 また利用規約において、準拠法及び裁判管轄について定めております。 https://www.yourdesk.jp/assets/pdf/common/terms.pdf
3	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい。	○	ユアデスク（YourDesk）ソフトウェア使用許諾契約書（クラウド版兼用）にて知的財産権について利用を許諾する範囲を定めております。 https://www.yourdesk.jp/assets/pdf/common/license.pdf
4	認可されていない目的のための情報処理施設の利用は阻止すること。	○	本サービスが利用契約を締結しているデータセンターにより各種対策が講じられております。
5	個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、契約事項の中の要求にしたがって確実に保護すること。	○	本サービスは国内のデータセンターにて運用、データの保管を行っております。 またユアデスク（YourDesk）ソフトウェア使用許諾契約書（クラウド版兼用）において、準拠法及び裁判管轄について定めております。 https://www.yourdesk.jp/assets/pdf/common/license.pdf
6	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、脆弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。 また、クラウド事業者は、クラウド利用者の個別の監査要求に応える代わりに、クラウド利用者との合意に基づき、独立したレビュー及び評価の結果を提供することが望ましい。	○	当社では社内にセキュリティ委員会、品質管理委員会を設置し、リリースなどのイベントごと、及び定期的な監査を実施しております。
11．その他			
1	記録媒体(書類、記録メディア)の保管管理については適切に行うこと。また廃棄する際には記録された情報を復元できないように安全に処分すること。また再利用の際には機密情報の漏えい等につながらないように対処すること。	○	情報セキュリティ管理規程にて、記録媒体の情報取扱方法（保管、廃棄）を定め、適切に取り扱っております。
2	重要な情報資産については、机の上に放置せず安全な場所に保管すること（クリアデスク）。また離席時には情報を盗み見られないように情報端末の画面をロックすること(クリアスクリーン)。	○	情報セキュリティ管理規程にて、クリアデスク（情報資産は鍵のかかる場所に保管する）とクリアスクリーン（一定の使用中断時間が経過した場合、自動的にロックがされる設定）の対策を講じるよう定め、実施しております。
3	従業員のパソコンにウイルス対策を行うこと。また技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	情報セキュリティ管理規程にて、ウイルス対策（ウイルス対策ソフトの導入等）を定め、遵守しております。 技術的脆弱性に関する情報は、ウイルス、スパイウエア、技術的脆弱性等への対策について、情報収集及びパッチの適用を実施しております。
4	サービス提供を終了する場合は、利用者に対して事前に通知を行うこと。	○	利用規約にてサービス提供の終了についての事前通知の方法を定めております。 https://www.yourdesk.jp/assets/pdf/common/terms.pdf
5	サービス提供にあたって役割分担及び責任範囲を明示していること。	○	利用規約にて役割分担及び責任範囲を定めております。