経済産業省 ガイドライン版
WACUL セキュリティチェックシート
更新日：2024年5月

本チェックシートは、株式会社WACULが提供するAIアナリストサービスについて、そのセキュリティ対策を記載したものです。
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
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf
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、改善のために予告なく変更することがあります。

なお、当社はISO/IEC27001:2013／JIS Q 27001:2014 の要求事項に適合し、認証登録番号IS 635068を保有しています。

		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://wacul.co.jp/security
	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」）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に、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 また、経営層によって承認されたクラウドサービスに関するセキュリティの基本方針は、ISMSにおいて、経営者によって毎年及び重大な変化が発生した場合に見直しております。
2. 情報セキュリティの為の組織				
	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。	○	当社の内部統制についての基本方針にて、経営者、監査役、従業員の行動指針を明らかにし、セキュリティの基本方針にて、業務に携わる役員、社員が継続的に情報セキュリティ対策を推進しています。
	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。	○	セキュリティ対策、手順等について、セキュリティ関係者および関係組織と審議する委員会として情報セキュリティ委員会を設置しております。
	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。	○	ISMSマニュアルにて、情報セキュリティ対策（日々の活動や緊急対応、役割別PDCA）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。	○	本チェックシートにて、クラウドサービス利用者に対し、提供するクラウドサービスに関するセキュリティ対策を記載し、提供しております。 サービス開始前の合意は、クラウドサービス利用者に対し、当社サービスページに以下を公開しております。 https://wacul-ai.com/terms.html
	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。	○	お問い合わせについては以下の窓口を用意しております。 問い合わせ方法：電話、入力フォーム
3. 人的資源のセキュリティ				
	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。経営層に承認されたクラウドサービスに関するセキュリティの基本方針及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ規則等）を定めております。 また、雇用する従業員とは、雇用契約書を締結し、その中で就業規則及び社内規程の遵守について明確に同意を確認しております。
	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。	○	雇用する従業員（採用の日から3ヶ月間は試用期間）には、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を実施しており、社内規程の教育を行っております。 ルール違反が発生した場合には個別に再教育を行っております。ISMSの適用範囲者に対してはPDCAサイクルの一環として年に1度教育を実施しています。 また、社内規程の変更の都度、全従業員に通知し、周知を行っております。 さらに、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施しております。
	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。	○	以下のセキュリティ違反を犯した従業員は、当社就業規則に規定された懲戒の対象となることが、情報セキュリティ規則に明記されております。 － セキュリティ事件・事故を故意に起こそうとした場合 － 情報セキュリティに関する重大な過失を犯した場合 － 情報セキュリティに関する過失を繰り返した場合
	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。	○	従業員の退職・休職時の手続は、以下のとおり情報セキュリティ規則に明記されております。 － 退職時は、全てのシステムのアカウントを削除または使用停止する － アクセス権、リモートアクセス権の変更申請にて削除または使用停止する － 退職者・休職者から業務PC、鍵、カードキー等を回収する
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、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。	○	情報資産台帳で各資産名、管理責任者、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、定期的に見直し更新しております。
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。	○	情報資産がある領域（セキュリティエリアは、ワークスペースと入室制限スペース）は、セキュリティカード制御を用いて、フリースペースとの物理的な境界を設けております。重要な情報資産がある領域(入室制限スペース)は、セキュリティカード制御及び生体認証を用いて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、情報セキュリティ規則に明記されており、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。	－	AWSを利用しており、複数アベイラビリティゾーンに分散しております。 https://aws.amazon.com/jp/compliance/data-center/environmental-layer/
	4	データセンターの落雷対策を確認すること。	－	同上
	5	データセンターの水害対策を確認すること。	－	同上
	6	データセンターの静電気対策を確認すること。	－	弊社人員が直接データセンターで作業することはありません。
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の手順については文書を作成しています。こちらの文書については操作方法の変更や機材追加・変更が発生する毎に更新しております。
	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。	○	アプリケーションについて管理されており、ドキュメント及びソースで情報を保存しています。 また、利用者に影響を及ぼすものについては事前に通知しております。
	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。	○	最新版のOS、ブラウザにて対応しております。
	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。	○	脆弱性についてはIPAやJPCERT等からの情報をもとに日々確認をしており、緊急性を要するものは適切なタイミングでパッチを適用しております。
	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。	○	利用状況を監視・調整しております。 また、利用状況予測に基づいて、要求事項を文書化し維持しております。
	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。	○	第三者機関を使って脆弱性診断を行い、結果を基に重要性の高い問題から修正しております。
	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行っておりません。
	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。	○	定期的なバックアップを取得しております。
	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。	○	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実施しております。 サービス停止を検知した場合には、利用者に対しメールまたはサービス上のお知らせ、ヘルプセンターにて通知しております。
	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。	○	同上。 障害を検知した場合に、利用者に対しメールまたはサービス上のお知らせ、ヘルプセンターにて通知しております。
	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。	○	運用担当者の作業は記録しております。
	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。	○	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し、アラートに対しては定期的に確認し、改竄、許可されていないアクセスが無いように保護しております。
	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。	○	監査ログの保持は行っております。ただし、利用者に開示しておりません。
	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。	○	正常な時刻に同期しております。
	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、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しております。
	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。	○	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ており、特権の割り当て及び利用は制限しております。
	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。	○	システムの運用担当が利用するパスワードについては管理しております。パスワードについてはIPAにて定めている内容に基づき実施しております。 https://www.ipa.go.jp/security/anshin/measures/account_security.html
	18	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。	○	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しております。

	19	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。	○	AIアナリストサービスはお客様毎の領域を準備し、かつアクセス権限機能を用いて提供しております。
	20	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。	○	解約処理及び削除機能を有しております。
	21	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。	○	特権の割り当て及び利用制限し、管理する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。	○	パスワードを管理する機能は提供しておりませんが、良質なパスワード（文字数・複雑度）で制限を行っております。
	23	一定の使用中断時間が経過したときには、仕様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。	○	中断しているセッションを遮断し、かつ接続時間の制限を利用しております。
	24	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。	○	ネットワークについて適切に管理し脅威からの保護、セキュリティを維持しております。
	25	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割り当て及び利用は制限し、管理されております。 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、認証技術を使って制御しております。
	26	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。	○	不正アクセス防止のためにFWを導入しております。 また、情報システム部門によってサービス利用が許可されたものだけになっております。
	27	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。	○	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し、クラウドサービスの利用検討に明示しております。
	28	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。	○	契約終了時について顧客の要請に応じて返還、消去を実施しております。 該当内容については、利用規約に明記させていただいております。
	29	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。	○	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事を確認しております。
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。	○	当社へ対しお客様が登録した情報については、その情報の内容を問わず、最善の注意を持って管理し、別段の定めがある場合を除き、お客様の書面による承諾を得ることなく、本サービス以外の目的のために利用あるいは複製し、または第三者に利用させ、もしくは開示、漏洩いたしません。 なお、当社にて外部組織を利用する場合は、当社規定に則り選定、契約を行います。契約時には、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。	○	情報セキュリティ規則にて、セキュリティ事故の定義、発生時の報告について定めており、また、ウィルス感染の疑いや利用しているサービスから情報漏えい等の事故があった場合の報告連絡手段、対応手続を定めております。
	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。	○	情報セキュリティ規則にて、情報セキュリティインシデントに対応するため、報告連絡手段、対応手続を定めております。 責任体制はISMSマニュアルにて、情報セキュリティ組織を整備しております。
	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。		関係者への連絡を実施しております。但し、定期的な明示はしておりません。
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	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。	○	AWSを利用しており、インフラは複数アベイラビリティゾーンに分散しています。 https://aws.amazon.com/jp/compliance/data-center/environmental-layer/
	2	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。	_	クラウドサービス提供に用いる機材は全てSaaS（AWS）に設置しております。
	3	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。	_	クラウドサービス提供に用いる機材は全てSaaS（AWS）に設置しております。
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。	○	利用規約等に明示し維持しております。 また、重要な記録については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。	○	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://wacul-ai.com/terms.html
	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	○	申し込み契約書または、申し込みフォーム等の利用規約において、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。
	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。	○	情報セキュリティ規則にて、物理的境界及びその他の各境界へのアクセスが許可される者について定めており、アクセス許可がされていない者はアクセスできないように制限をかけております。 また、アクセス許可判断方針についても定めております。
	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。	○	利用規約に従って取り扱っております。
	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。	○	弊社担当部門によるレビュー、テストを実施しております。 但し、評価結果等については公開しておりません。
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。	○	情報セキュリティ規則にて、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)。	○	情報セキュリティ規則にて、クリアデスク（重要な情報資産は、作業終了時には、施錠されたキャビネット、引出しに保管）と離席する場合は、第三者が容易に操作及び閲覧ができないようスクリーンロック等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ィ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。	○	情報セキュリティ規則にて、クライアントPCに関する利用者の遵守事項（ウィルス対策等）を定め、遵守しております。技術的脆弱性に関する情報は，ウィルス、スパイウエア、技術的脆弱性等への対策について、情報収集と情報周知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。	○	利用規約に記載しております。
	5	サービス提供にあたって役割分担および責任範囲を明示していること。	○	利用規約に記載しております。