ver 2.0

本チェックシートは、クローバ株式会社が提供するクラウドサービス「クローバ PAGE」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
(http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html)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。

	確認項目	実施有無	備考
1 情報セキュリティのための方針群			
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。	○	当社代表取締役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を定めております。 当社情報セキュリティ基本方針は、全従業員に社内規定として周知し、クラウドサービス利用者には当社ホームページに公開しております。 https://company.qloba.com/security_policy.htm
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は定期的及び重大な変更が発生する度に見直しを行っております。
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。	○	経営陣自らが情報セキュリティの管理責任者となり、業務に関わる役員、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規程にて、情報セキュリティの責任者と役割を定めております。 クラウドサービスの情報セキュリティに関する窓口は、当社ホームページ(https://company.qloba.com/security.htm)に公開しております。
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。	○	情報セキュリティ管理規程にて、情報セキュリティ対策(日々の活動、緊急対応、役割、承認等)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。 また利用開始時に、サービスの利用にあたっての利用規約を明示し、これに同意していただいております。
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。	○	メール、Webフォームでお問い合わせいただく窓口を公開しております。 メール:info@qloba.com Webフォーム:https://help.qloba.info/
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。	○	クラウドサービスに関するセキュリティの基本方針(https://company.qloba.com/security_policy.htm)及び社内規程(情報セキュリティ管理規程)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署名、押印をもって明確に同意を確認しております。
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。	○	すべての従業員に対して、セキュリティ、コンプライアンス等に関する研修会を開催しております。また教育に使用する事例や技術などは常に最新の動向を踏まえたものに更新しています。
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、情報セキュリティ管理規程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
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。	○	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管理規程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 - 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。	○	情報資産台帳にて、各情報資産の目録、管理責任者、及び利用の許容範囲を管理しております。

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。	○	情報資産台帳にて、各情報資産のを分類し、取り扱いを定めております。
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。	○	当社は完全リモートワークを行っているため、重要な情報資産はすべてデータ化し、クラウド上に保管されております。情報資産を保護するため暗号化及び多要素認証を必須とし、IPアドレスによるアクセス制限を行っております。
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アクセス権が設定されております。
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のデータセンターは耐震構造となっております。 AWSの金融機関向けのコンピュータシステム安全基準にデータセンターの各種対策が記載されております。 https://d0.awsstatic.com/whitepapers/jp/security/FISC_Document_20120824JP.pdf
4	データセンターの落雷対策を確認すること。	○	AWSのデータセンターは落雷対策を実施しております。
5	データセンターの水害対策を確認すること。	○	AWSのデータセンターは水害対策を実施しております。
6	データセンターの静電気対策を確認すること。	○	AWSのデータセンターは静電気対策を実施しております。
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、変更毎に更新しています。
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。	○	アプリケーションやOS、サーバー、ネットワーク機器の変更についてはすべて管理されています。利用者に影響を及ぼす変更については、１週間前までにEメールやホームページピス上にて連絡をしております。
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。	○	利用できるウェブブラウザの種類・バージョンについては、当社ホームページ(https://help.qloba.info/article/18-faq)に公開しております。
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。	○	脆弱性情報について日次で収集し、影響について確認をしております。またパッチの適用についても手順に則り適用作業を実施しております。
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。	○	サーバー、サービスの稼働状況やリソースの利用状況について監視を行っております。モニタリングの状況を踏まえて定期的に将来必要な性能や容量の見積もりを行い、増設の計画を行っております。
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。	○	製品をリリースする際には、自社にて脆弱性診断を行います。またその結果に基づき改善等対応作業を実施しております。また必要に応じてサードパーティベンダーによる脆弱性診断を実施しております。
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。	○	当社サービスには、お客様が自身のサイトにJavaScriptを設置してカスタマイズできる機能があります。当社のガイドラインに従い、悪意のあるJavaScriptの設置が認められた場合、当社はユーザーに対してスクリプトの利用を停止することができます。JavaScriptは許可された管理者しか設置することはできません。
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。	○	データベースは毎日無停止でバックアップを取得しております。アップロードされたファイルについては複数のデータセンターで冗長化されたAmazon S3に保存されます。 インストールされるソフトウェアやソフトウェアの設定については、バージョンごとに履歴管理されています。
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。	○	アプリケーション、OS、サーバー、ネットワークの稼働状況について監視をしております。 サービスの停止を検知した場合は、WebサイトもしくはSNS（Webサイトが稼働できない場合）で利用者に連絡を行います。

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。	○	アプリケーション、OS、サーバー、ネットワークの障害状況について監視をしております。 障害を検知した場合は、WebサイトもしくはSNS（Webサイトが稼働できない場合）で利用者に連絡を行います。
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。	○	システムの運用担当者の作業はコマンドのヒストリー機能を用いて記録しております。
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。	○	ユーザーの利用履歴及びエラー、アラートを常時ログに記録しております。ログは定期的に確認するとともに、異常が発生した場合は、自動的に技術担当者に通知されるしくみになっています。
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。	△	ユーザーの利用履歴及びエラー、アラートを常時ログに記録しております。ログは180日間保存しております。原則的に利用者へログの提供は行っておりませんが、重大な不具合やセキュリティ上の問題が発生した場合に限り、該当ログを調査機関に提供する場合があります。
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、オペレーティングシステム、ネットワーク機器等、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。	○	システムのアカウントについては当社規定に則り、各個人に一意の識別子を付与しております。またシステムにアクセスする際には多要素認証を必須とし、ユーザーごとに適切なアクセス制御を行っております。アクセス制御方針については当社規定にて定めております。
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。特権については利用者をシステムの運用管理責任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。	○	パスワードについては情報セキュリティ管理規程に則り、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。	○	サービスの利用者を制限するには、サブアカウント機能をご利用頂く必要があります。サブアカウント機能の詳細は、当社ヘルプサイト(https://help.qloba.info/article/30-sub-account)に記載しております。
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。	○	運用管理画面へのアクセスをアクセス元のIPアドレスで制限できる機能を提供しております。
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。	○	当社のサービスはマルチテナント構成となっております。 許可されているお客様以外がアクセスできないように、デー タベースのアクセス制限を行っております。またユーザーと当社サービスとの伝送データはすべて暗号化されています。
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。	○	サブアカウント機能にて提供しております。
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。	○	サブアカウント機能にて提供しております。
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。	○	ユーザー毎にパスワードを管理できる機能を提供しております。パスワードは８文字以上で設定される必要があり、アルファベット、数字、記号など任意の文字を使用することができます。
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。	○	提供している情報セキュリティ対策及び機能について、ホームページ(https://company.qloba.com/security.htm)に公開しています。

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。	○	一定期間（30日間）サービスのご利用がない場合、セッションは切断されます。
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。	○	セキュリティを維持するためにネットワーク構成の管理、ネットワーク機器監視を実施しております。またアクセス制御についても文書化し、管理・実施しております。
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。	○	ネットワーク機器へのアクセスには多要素認証を必須とし、ユーザーごとに適切なアクセス制御を行っております。アクセス制御方針については当社規定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。	○	一般的なIPアドレスとポート番号でブロックするタイプのファイヤーウォールに加えて、WAF(Web Application Firewall)を導入して不正アクセスやDOS攻撃等の防止を行っております。
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。	○	パスワードとEメールによる認証方式及び、OAuth 2.0を用いた認証方式を提供しております。
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。	○	サービスのアカウントを削除すると、送信されたエントリー、メッセージの履歴等、アカウントにひもづくデータはすべて消去されます。作成したプロジェクトは一ヶ月以内に消去されます。バックアップデータは各データの削除から２週間以内に完全に消去されます。
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。	△	利用者のブラウザからデータセンターへの伝送データはすべて暗号化されております。利用者がアップロードしたファイルは暗号化されております。データベースのストレージは暗号化されておりません。
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。	○	弊社製品 に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(利用規約の投稿者情報の取扱いに記載)、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。 弊社製品はAWSをハウジングサービスとして利用しておりますが、AWSではSOCレポート (https://aws.amazon.com/jp/compliance/soc-faqs/)において重要なコンプライアンス管理および目標を AWS がどのように達成したかを実証する、独立したサードパーティーによる審査報告書を公開しております。
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。	○	情報セキュリティ管理規程にて、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。
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際は、弊社ホームページ及びSNSにて公開致します。
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。	○	事業継続計画書の中で事業継続リスク分析及びビジネスインパクト分析をおこなっております。その中で各業務プロセスの中断発生確率、復旧許容時間から優先度を定め、要求されたレベルで時間で復旧できるように事業継続計画書を作成しております。
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。	△	すべてのデータストレージ、ネットワークについて冗長化を実施しております。アプリケーションサーバーをはじめほとんどのサーバーに冗長化を行っておりますが、一部冗長化されていないサーバーがございます。

3	事業継続計画については定期的に試験・更新すること。	○	事業継続計画書を作成し、定期的に試験及び見直しを行なっております。
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。	○	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、停電・電力障害が発生した場合も電力が供給されるようになっております。
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。	○	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、火災検知・通報システム及び消火設備を用意しております。
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。	○	情報セキュリティ管理規程にて、電気通信事業法、個人情報保護法、特定商取引法等、関連する法令及び規則を遵守するための取り組み方をまとめております。また文書は管理者、承認者、保管期間を定めて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。	○	弊社の提供するサービスはAWSの東京リージョンまたは大阪リージョンで運用し、同リージョンにバックアップデータを保管しています。また利用規約(https://company.qloba.com/terms_of_use.htm)において、準拠法および裁判管轄について定めております。
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	○	利用規約(https://company.qloba.com/terms_of_use.htm)において、知的財産権について定めております。
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。	○	情報セキュリティ管理規程にて、各従業員においてアクセスが許可される範囲について定めており、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。	○	個人情報の保護、管理についてはプライバシーポリシー(https://company.qloba.com/privacy.htm)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。	△	サードパーティベンダーが提供する脆弱性診断を行っております。クラウド利用者による脆弱性診断は非対応とさせて頂いておりますが、セキュリティ上の問題に関する報告窓口(https://company.qloba.com/security.htm)を設けております。
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(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。	○	サービス提供の終了およびサービス廃止の場合、3ヶ月以上前に通知致します。
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(https://company.qloba.com/terms_of_use.htm)において、サービス提供者及び利用者の責任範囲ついて定めております。
6	情報のラベル付けをする機能が提供されていること。	○	各サービスの機能詳細に関しては、マニュアルを公開しています(https://help.qloba.info/)。情報ごとにタイトルを付与したり、アクセス権を設定するなど、お客様の情報資産の分類にご利用いただける機能となっております。