

本シートは、LayerX社オリジナルの項目で構成されたセキュリティチェックシートに当社の対応状況を記載したものです。

No.	カテゴリ	設問	回答
1	基本	情報セキュリティについて企業としての方針を定め、取締役会等の承認を得ていますか。また組織の内外へ周知していますか。	はい 情報セキュリティ方針: <a href="https://layerx.co.jp/security_policy">https://layerx.co.jp/security_policy</a> プライバシーポリシー: <a href="https://layerx.co.jp/privacy">https://layerx.co.jp/privacy</a>
2	基本	情報セキュリティまたは個人情報保護について取得している第三者による認証はありますか。	【ISO/IEC27001:2022】 登録番号: IS 747702 範囲: ・SaaS 型業務効率化支援サービスの企画、開発及び提供・AI・LLMの活用に関する支援サービスの開発及び運営 ※ 三井物産デジタル・アセット・マネジメント事業部以外の組織で認証取得  ほかに、SOC1 Type2報告書を定期的に取得しております。閲覧につきましては担当営業までお問い合わせください。
3	基本	個人情報保護に関して、対応している法令やガイドラインをご記載ください。	個人情報保護法。GDPRについては今後対応予定です。
4	基本	契約や規約等における準拠法を回答してください。	日本法
5	基本	政府、自治体又は公的機関から個人情報提供の命令又は要請等へ対応することは可能ですか。	はい、法的な根拠がある場合のみの対応致します。
6	基本	提供しているサービスは、法人と個人(個人事業主を含む)のどちらを対象としていますか。	詳細は、当社プライバシーポリシーをご参照ください。 <a href="https://layerx.co.jp/privacy/">https://layerx.co.jp/privacy/</a> 原則、法人のみです。
7	基本	サービス提供における責任分界や、利用者との取り決め事項について定めている内容があれば教えてください。	以下を実施しております。 ・SLAは非公開です ・サービス提供者の責任範囲を定めている ・サービス利用者とサービス提供者間のコミュニケーション(連絡や報告)のルールや体制を定めている ・損害賠償について、責任の範囲や金額の上限を定めている 詳細はサービスの利用規約をご確認ください: <a href="https://bakuraku.jp/terms">https://bakuraku.jp/terms</a>
8	基本	クラウドサービス・Webサービスに関する情報セキュリティ責任者を専任していますか。	情報セキュリティ責任者としてCISO職を設けております。
9	基本	情報セキュリティの体制や管理の枠組みについて、どのような方針や役割分担を定めていますか？	・情報セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めている ・情報セキュリティ管理に関する関係部署や業務、機能を明らかにしている ・情報セキュリティ体制について、通常時だけでなく有事を想定した役割や責任を定めている ・自社で対応する箇所、外部に委託する箇所を適切に切り分け、役割と責任を明確にしている
10	基本	情報資産へのアクセスや操作権限について、組織内での役割に応じた分離や管理はどのように行っていますか？	はい。分離していて、定期的に見直ししております。
11	基本	サポート時間は定めていますか。	平日(土日祝日を除く)10:00～17:00です。
12	基本	サポート体制はありますか。	製品上から問合せを起票していただけます。緊急時は担当CSまでメールもしくはお電話でご連絡も可能です。
13	データ利用	利用規約を公開していますか。	はい、以下に公開しております。 <a href="https://bakuraku.jp/terms/">https://bakuraku.jp/terms/</a>
14	データ利用	サービス利用者から預かるデータに関して、取り扱い方針や禁止事項などを契約等で定めていますか？	はい、以下を定めております。 ・秘密情報の定義 ・第三者への開示の禁止 ・目的外利用の禁止 詳細はサービスの利用規約 第15条および第16条をご確認ください: <a href="https://bakuraku.jp/terms">https://bakuraku.jp/terms</a>
15	データ利用	クラウドサービスの利用を通じて取得している利用者情報には、どのような項目がありますか？	・氏名 ・メールアドレス ・Cookie
16	データ利用	サービス利用者の個人情報に関して第三者提供をしていますか。	いいえ
17	データ利用	サービス利用者の個人情報をサービス提供以外の目的で利用していますか。	いいえ
18	データ利用	Cookieや位置情報、IPアドレス等のオンライン識別子の利用について、どのような対応をしていますか。	利用停止の方法を明記しています
19	データ利用	外部委託先が預託データを取り扱うことはありますか。	はい 詳細はサービスの利用規約 第9条および第15条をご確認ください: <a href="https://bakuraku.jp/terms">https://bakuraku.jp/terms</a>
20	データ利用	外部サービスの利用や外部委託等により預託データが他国に保管されることはありますか。	はい。データの保管は日本リージョンで行います。
21	データ利用	外部委託先や外部サービスに個人情報委託されることはありますか。	はい、個人情報の委託をしていますが委託先は公開しておりません。
22	データ利用	国別にフィルタリングする機能はありますか。	アクセス元の国によってアクセス制御する機能はありません。
23	データ利用	サービス提供のため利用しているデータセンターの所在国はどこですか。	日本です。日本国外のリージョンで一部のデータ処理を行いますが、処理後に消去される仕組みとしております。
24	情報資産管理	情報資産の洗い出しや重要度評価、資産一覧の作成などについて、どのような管理プロセスを定めていますか？	以下を実施しております。 ・管理プロセスを文書化している ・定期的に文書内容を見直している ・情報資産一覧を作成している
25	情報資産管理	契約や規約等により、サービス利用終了時のデータの取り扱いが明確になっていますか。	はい。詳細はバクラク共通利用規約 第15条をご確認ください: <a href="https://bakuraku.jp/terms/common/">https://bakuraku.jp/terms/common/</a>
26	情報資産管理	サービス利用終了またはサービス利用者からの指示があった場合、預託データやサービス利用者が作成したデータを返却や削除できますか。	一部データを CSV または元ファイル形式にてダウンロードできるようにしております。削除については、バクラク共通利用規約 第15条をご確認ください: <a href="https://bakuraku.jp/terms/common/">https://bakuraku.jp/terms/common/</a>
27	情報資産管理	情報資産を消去または廃棄する場合は復旧できない状態にしていますか。	はい
28	情報資産管理	クラウドサービスの開発、保守および運用において、私用端末を利用していますか。	いいえ
29	情報資産管理	持ち運び可能な外部記憶媒体を利用していますか。	はい、定められた手続きや機能に基づき利用していて、定期的に見直しをしております。
30	情報資産管理	持ち運び可能な外部記憶媒体について、実施しているセキュリティ対策は何ですか。	社内ITが管理する媒体、もしくは情報セキュリティ管理者によって許可されたデバイスのみが利用可能となっています。また、原則として外部記憶媒体で提供されるソフトウェアのインストール、銀行データの読み取り、デザインデータの読み取りのみに利用用途を限定しています。
31	情報資産管理	外部記憶媒体の管理手順(保管・移動・廃棄など)を定めたうえで、その手順に従って運用していますか？	はい。
32	情報資産管理	他のユーザーのデータと混在しないよう、論理的な分離などの対策を実施していますか？	はい。アプリケーションレイヤでの論理的分離を実施しております。
33	アクセス制御	クラウドサービスに関連するシステムやデータへのアクセスについて、方針やルールを定めていますか？	はい。ルールを定め、定期的に見直ししております。
34	アクセス制御	従業員やシステム管理者による預託データへのアクセスは、原則禁止としたうえで、必要時には事前承認を得る運用としていますか？	はい。手続きを文書化し、定期的に文書の内容を見直しております。
35	アクセス制御	従業員やシステム管理者が預託データにアクセスする場合は、アクセス者の操作ログをモニタリングしていますか。	はい
36	アクセス制御	クラウドサービス内のコンポーネントやデータへのアクセスを、業務上必要な従業員にのみ限定していますか。	はい
37	アクセス制御	クラウドサービスの開発、保守および運用において、特権アカウントを割当および利用する際は、承認を必須とし必要最小限に制限していますか。	はい
38	アクセス制御	クラウドサービスの開発、保守および運用において、特権アカウントを用いた情報資産に対するネットワークアクセスを記録し、適切な利用かどうかをモニタリングしていますか。	はい
39	アクセス制御	クラウドサービスの管理者権限や特権的な機能へのアクセス制限について、どのような対策を実施していますか？	以下を実施しております。 ・管理者権限でのログインおよびクラウドサービスへのアクセスは必要な場合のみ実施している ・Webサーバやアプリケーションサーバのプロセスを管理者権限以外で起動している ・サービスやデーモン、プロトコルは必要なもののみ設定および起動をしており、不要なもの起動できないようにしている
40	アクセス制御	クラウドサービスに関するソースコードや設計資料などの重要情報へのアクセスは、担当者役割や必要性に応じて適切に絞られていますか？	はい
41	アクセス制御	クラウドサービスのリリースもしくはローンチ作業ができる人を限定していますか。	はい
42	アクセス制御	クラウドサービスの開発・運用・保守・運営において、共有アカウントを利用していますか。	いいえ
43	アクセス制御	クラウドサービスの開発、保守および運用において、不要または一定期間使用していないアカウントを無効化あるいは削除していますか。	はい、以下を実施しております。 ・手続きを文書化し、定期的に文書の内容を見直し ・都度無効化・削除している ・月次で棚卸しを実施
44	アクセス制御	サービスの開発・運用・保守・運営において共有アカウントが利用禁止であることを明文化していますか。もしくは例外的に利用する場合のルールを定めていますか。	はい

45	アクセス制御	サービス利用者のアカウントについて、どのようなパスワードルールがありますか。	以下を実施しております。 ・IDは各個人に発行し、利用者を特定できる仕様としている ・文字数は8文字以上、半角アルファベット大文字、小文字、半角数字の3種類の組み合わせが必須項目です。(任意で記号も利用可能) ・10回間違えてログイン試行した場合、アラートが表示され30分間ロックされます。 また、お客様の環境ごとに以下のパスワードポリシーの強化設定が可能です。 ・パスワードの最低文字数を8文字以上に設定 ・記号の使用を必須に設定をする
46	アクセス制御	サービス利用者のアカウントについて、セッションタイムアウトを設定していますか。	はい。有効期限は非公開です。
47	アクセス制御	サービス利用者のログインにおいて、MFA(二要素認証)やSAML認証など、ID/パスワード以外の認証手段を利用できますか？	はい 以下のような認証手段が利用可能です。 ・スマートフォンアプリを用いた二要素認証(MFA) ・有料オプションでのIPアドレス制限、SAML認証、Googleログイン ※Googleログインは、パスワード認証を併用する場合はオプション契約なしでご利用いただけます。
48	アクセス制御	サービス運営を行うにあたり、従業員向けの機能や管理用画面等を備えていますか。	はい
49	アクセス制御	サービス運営に携わる従業員のアカウントに対して適切なセキュリティ対策を講じていますか。	はい。サービス運営のためのアカウントには、原則としてSSOを利用することとしております。 SSOにはMicrosoft Entra IDを用いており、パスワードポリシーが定められています。 <a href="https://learn.microsoft.com/ja-jp/entra/identity/authentication/concept-password-ban-had-combined-policy">https://learn.microsoft.com/ja-jp/entra/identity/authentication/concept-password-ban-had-combined-policy</a> また、リスクベース認証をはじめとしたセキュリティ機能を利用しています。  SSOが利用できないシステムについてはパスワードマネージャーの利用をルールとして定めております。 SSOおよびSSOが利用できないシステムの全てにおいて、利用可能な場合多要素認証を必須としています。
50	暗号	暗号化および鍵管理の方針やルールはありますか。	文書で定めており、定期的な見直しを実施しております。
51	暗号	暗号鍵について、どのように管理していますか。	IaaSの鍵管理システムを用いて管理を行っています。
52	暗号	サービスの通信に関する暗号化について、どのようなセキュリティ対策を実施していますか。	以下を実施しております。 ・サービスへのアクセス時の通信を暗号化している ・安全なプロトコルのバージョンのみを使用して暗号化している ・安全な暗号アルゴリズムと十分な鍵長の組み合わせのみを利用している ・有効期限が切れていない、信頼できる認証局が発行したサーバ証明書を利用している
53	暗号	預託データに関する暗号化について、どのようなセキュリティ対策を実施していますか。	以下を実施しております。 ・安全な暗号化方式と十分な鍵長により、預託データが格納されたデータベースやファイルを暗号化している ・パスワードはソルト付きでハッシュ化し保管している ・安全な暗号方式と十分な鍵長により、バックアップデータを暗号化している
54	物理的セキュリティ	データセンターは自社で管理していますか。	IaaSを利用しております。
55	物理的セキュリティ	IaaS/PaaS等の選定にあたり、データセンターの入退室管理や自然災害への対策等の物理的なセキュリティ対策を確認していますか。	はい
56	運用	クラウドサービスの運営に必要な情報を定め文書化していますか。	文書で定めており、定期的な見直しを実施しております。
57	運用	構成管理や変更管理により、システム構成やネットワーク構成、変更状況を可視化していますか。	はい
58	運用	サービス利用者への通知について、実施しているものを記載してください。	以下については事前通知しております。 ・緊急もしくは不定期なメンテナンス ・サービスの大きな変更や終了 ・アクセス権限設定の仕様を変更する場合 以下については速やかに通知しております。 ・サービス提供に関わる障害やパフォーマンス低下等が発生した場合 ・セキュリティインシデントが発生した場合
59	運用	現状だけでなく将来必要となるリソースを考慮し、キャパシティプランニングを実施していますか。	はい
60	運用	災害やシステム障害などに備えて、クラウドサービスのデータや構成情報のバックアップを定期的に取得していますか？	はい 日次バックアップを14日間(世代)、および毎月のバックアップを6ヶ月分保管しております。
61	運用	バックアップから適切に復旧可能出来るようにリストアテスト等を実施していますか。	以下を実施しております。 ・バックアップが取得できていることを定期的に確認している ・バックアップデータをクラウドサービスが設置してある場所とは物理的に離れた場所で保管している ・月に一度リストアテストを行っている
62	運用	データやログの保管期間と管理要件を定めていますか。	以下を実施しております。 ・保管期間や管理要件を文書化している ・定期的に文書の内容を見直している
63	運用	どのようなログを取得していますか。また、その保管期間を教えてください。	取得しているログ ・例外処理や誤操作によるエラー、システム障害、セキュリティインシデントに関するイベントログ ・サービス利用者の認証ログやアクセスログ、操作ログ ・システム管理者の認証ログやアクセスログ、操作ログ 保管期間 ・無期限
64	運用	取得したログが不正アクセスおよび改ざんされないよう、アクセス制御や暗号化等により保護していますか。	実施しております。
65	運用	クラウドサービスに関わる端末について、マルウェア対策や更新管理など、どのようなセキュリティ対策を講じていますか？	以下を実施しております。 ・マルウェア対策ソフトやEDRの導入 ・セキュリティパッチやソフトウェア・OS等のアップデートの適用 ・ネットワーク経由(Webやメール)での情報の持ち出し対策
66	運用	業務端末に不適切なソフトウェアがインストールされないよう、制限やモニタリングの運用を行っていますか？	はい 以下を実施しております。 ・手続きを文書化している ・定期的に文書の内容を見直している
67	運用	クラウドサービス全体で時刻のズレが発生しないよう、NTPなどを使って各コンポーネントの時刻を同期していますか？	はい
68	運用	脆弱性を管理するための方針を定め、その方針に従って脆弱性に対処していますか。	はい
69	運用	脆弱性診断やペネトレーションテストを実施していますか。	以下を定期的に実施しております。 ・プラットフォームに対する脆弱性診断(プラットフォーム設定変更の都度) ・アプリケーションに対する脆弱性診断(診断対象:API、特定機能や画面等に限定)
70	運用	クラウドサービスを構成する本番サーバに対してウィルス対策を行っていますか。	以下を実施しております。 ・クラウドサービスの提供するセキュリティサービス(Amazon Inspector および Amazon GuardDuty)を利用している ・脆弱性が見つかった場合、都度サービスのパッチを当てて更新するようにしている また、アップロードされるファイルに対してはウイルス対策ソフトを利用し、リアルタイムスキャンを実施しております。
71	運用	ソフトウェアの脆弱性やサポート終了情報(EOL・EOSなど)を把握したうえで、適宜パッチ適用やアップデートを行う運用になっていますか？	以下を実施しております。 ・手続きを文書化している ・定期的に文書の内容を見直している ・EOL・EOS・EOAや脆弱性の情報を把握している ・セキュリティパッチやソフトウェアのアップデートを適用している
72	従業員教育	従業員に対するセキュリティ対策として実施していることは何ですか。	・情報セキュリティおよび重要情報の取扱に関する意識向上のため、入社時研修および年に一度のセキュリティ研修を実施しております。 ・研修ではルールの説明および確認テストの実施をしております。 ・セキュリティインシデントを想定した演習や訓練を年に一度実施しております。
73	従業員教育	従業員および契約相手と秘密保持に関する契約を締結をしていますか。	はい
74	従業員教育	従業員および契約相手との契約が終了または変更となった場合、アクセス権の変更や削除、貸与資産の返却等を実施していますか。	はい。以下を実施しております。 ・手続きを文書化している ・定期的に文書の内容を見直している
75	ネットワークのセキュリティ	サーバやクラウド管理画面などへのアクセスについて、組織内の権限に応じて制限を設けていますか？	はい 特定の部署や人からのアクセスに制限しております。
76	ネットワークのセキュリティ	外部および内部からの不正アクセスを防止するためにファイアウォールを設置していますか。	はい
77	ネットワークのセキュリティ	不正なバケットを自動的に発見または遮断するためにIPSやIDSを導入していますか。	いずれも導入し、定期的に設定を見直しております。
78	ネットワークのセキュリティ	Webアプリケーションの脆弱性を悪用した攻撃等を防止するため、WAFを導入していますか。	はい。導入し、定期的に設定を見直しております。
79	ネットワークのセキュリティ	DDoS等のサービスの維持運用を妨害する攻撃への対策をしていますか。	はい IaaSが提供する攻撃対策を利用しております。
80	ネットワークのセキュリティ	サーバごとの役割に応じてネットワークやアクセスを分離し、外部からの不要な接続を防ぐ仕組みを取っていますか？	以下を実施しております。 ・DBサーバがWebサーバと分離された構成になっており、WebサーバとDBサーバ間の通信経路が必要最低限になるようアクセスを制御している ・DBサーバは外部から直接アクセスできないようにアクセスを制御している ・不要なポートを閉じている
81	ネットワークのセキュリティ	利用時の帯域幅を教えてください。	アップロード速度(ネットワークがサーバーへデータを送信する速度)が、10Mbps未満の場合にはファイルアップロードに時間を要する場合がございます。

82	監視	セキュリティインシデントやシステム障害を検知していますか。	以下を実施しております。 ・クラウドサービスおよびネットワークに対するパフォーマンス監視 ・クラウドサービスの死活や障害監視、外形監視（運用監視） ・社内ルール違反等の挙動監視 ・内部および外部からの不正アクセスや不正利用の監視 ・サイバー攻撃の兆候監視 ・不正なバケットに関する監視 ・サーバへのリモートアクセスやサービスの環境、IaaS・PaaSの管理画面等へのアクセスの監視 ・EDRによるエンドポイントの挙動監視
83	監視	セキュリティインシデントの予防や早期対応に向けて、ログを分析する仕組みを導入していますか？	はい
84	システムの取得、開発及び保守	クラウドサービスの開発、保守および運用において、セキュリティ対策の要求事項を明確にしていますか。	はい
85	システムの取得、開発及び保守	クラウドサービスの開発、保守および運用の各工程において、セキュリティや品質を確保するためにどのような対策をしていますか。	以下を実施しております。 ・機能要件や非機能要件、セキュリティ要件のレビュー ・各工程における承認プロセスの整備 ・データ修正の承認プロセス、作業手順の整備
86	システムの取得、開発及び保守	クラウドサービスの開発工程において安全なサービス開発のためにどのような対策をしていますか。	以下を実施しております。 ・コーディング規約などを定め、セキュアコーディングを実施している ・ソースコードのレビューをしている ・サービスで利用しているOSSを把握している
87	システムの取得、開発及び保守	開発環境と本番環境の分離や、本番データの取り扱いに関して、どのようなセキュリティ対策を講じていますか？	以下を実施しております。 ・開発環境と本番環境の分離 ・本番データについて、本番環境以外での利用禁止
88	システムの取得、開発及び保守	アプリケーションを変更する場合は、事前にテストし変更後の影響や不具合がないか確認していますか。	以下を実施しております。 ・機能要件のテスト ・非機能要件のテスト
89	システムの取得、開発及び保守	アプリケーションを変更する場合は、事前に本番環境と同等の開発環境でテストを実施していますか。	はい
90	システムの取得、開発及び保守	クラウドサービスのインフラやネットワークを変更する場合、事前にどのような対策をしていますか。	機能要件のテストを実施しております。
91	アカウント	サービス利用側のアカウントについて、一般的な利用者権限と、管理者権限等の特権を分離していますか。	はい
92	アカウント	サービス利用側の管理者権限にはどのような機能がありますか。	・アカウントの追加、削除、利用停止（ロック） ・アカウントの一覧出力 ・アカウントやグループ単位でのデータアクセスや実行可能機能の制御 ・ログのダウンロード
93	アカウント	サービス利用者のログイン状況や操作履歴について、利用者側の管理者が管理画面から確認できる仕組みはありますか？	はい 管理画面から以下の内容をご確認いただけます。 ・ログインID ・ログイン日時 ・IPアドレス ・操作権限（ロール）の変更履歴 ・管理権限の付与・はく奪
94	ファイルアップロード	アップロードファイルに対してセキュリティ対策を実施していますか。	はい 以下を実施しております。 ・暗号化 ・バックアップ ・マルウェアスキャン
95	独自ドメイン	サービス利用時にアクセスするURLは、すべての利用企業で共通のものですか？	いいえ
96	機能制限	他サービスとの連携について、どのサービスと連携できるかの設定を利用者側の管理者が行えるようになっていますか？	はい ・freee会計、勤定奉行クラウド、マネーフォワード会計Plusと連携が可能です ・連携先SaaSのアカウントに対してアクセス権があれば連携が可能となっております
97	機能制限	預託データを公開または外部ユーザへ共有する機能はありますか。	いいえ
98	API	他サービスとAPI連携することは可能ですか。	有償にてAPIプランを提供しており、外部のシステムとバクラク間で一部データの入出力を行うことができるWEB APIをご利用可能です。
99	スマートデバイスアプリ	スマートデバイスで利用するアプリについて、デバイス経由でのデータ漏えい対策を実施していますか。	はい 以下を実施しております。 ・Webアプリの認証を通過しないと利用不可 ・スマホアプリ内にデータを保持しない ・長時間操作がない場合に強制ログアウト
100	電子メール	サービス利用者が電子メールを送信する機能はありますか。	いいえ
101	AI	既存のAIを利用したサービスを提供していますか。	はい
102	AI	AIに関するガバナンス・管理としてどのようなセキュリティ対策を実施していますか。	以下を実施しております。 ・学習データの収集・利用について、個人情報に関するルールを定めている ・預託データを学習利用する場合は事前の同意を求めている
103	AI	AIに関する品質管理およびセキュリティ対策として実施していることはありますか。	以下を実施しております。 ・学習データ、AIの出力結果・判断根拠などを定期的に評価し、バイアス等を継続的にモニタリングしている ・AIに関する攻撃手法や動向について情報収集し、対応している
104	事業継続マネジメントにおける情報セキュリティ	災害や大規模障害に備えて、対応計画を策定し、訓練や定期的な見直しで実効性を確認していますか？	はい 内部向け災害対策ドキュメントを策定しており、定期的に見直しを実施しております。
105	事業継続マネジメントにおける情報セキュリティ	災害や大規模障害に備えて、システムを複数の拠点や地域に分散するなど、冗長化の仕組みを取り入れていますか？	はい IaaSが提供する冗長機能を使用しております。
106	法令遵守	クラウドサービスに関わる法令や契約上の義務に対応するため、必要な取り組みを継続的に実施していますか？	はい
107	法令遵守	個人情報保護に関連する法令や規制上の要求に従って対応していますか。	はい
108	法令遵守	プライバシーポリシーを定め、サービス利用者に開示していますか。	はい <a href="https://layerx.co.jp/privacy/">https://layerx.co.jp/privacy/</a>
109	法令遵守	内部監査や外部監査を実施していますか。	はい いずれも年次で実施しております。
110	インシデント管理	セキュリティインシデントや障害対応を円滑に進めるために、関係者の役割や責任をあらかじめ定めていますか？	はい 明確にし、定期的に見直しを実施しております。
111	インシデント管理	セキュリティインシデントやシステム障害が発生した際の対応手順を、あらかじめ整備していますか？	はい 確立しており、定期的に見直しを実施しております。
112	インシデント管理	インシデント対応手順の改善に向けて、訓練や他社事例からの学びを反映する取り組みを行っていますか？	はい
113	インシデント管理	過去2年間にホームページ等で対外的に公表もしくは監督省庁や認証機関等へ報告するレベルのセキュリティインシデントがありましたか。	いいえ
114	外部委託先管理	クラウドサービスの開発、保守および運用において、外部委託先を利用していますか。	はい サーバー管理、ファイルストレージ、ソースコード管理等を委託しております。
115	外部委託先管理	外部委託先の選定および管理について、方針や基準を定めていますか。	はい 定めており定期的な見直しを実施しております。 以下を合意し文書化しております。 ・セキュリティ対策（自社と同等水準） ・セキュリティインシデント発生時の報告や対処 ・情報の消去 ・関連法令の遵守 ・サービスレベル ・機能要件や非機能要件
116	外部委託先管理	外部委託先に対する要求事項として合意していることはありますか。	はい 定期的確認を実施し、内容の見直しを実施しております。
117	外部委託先管理	外部委託先との合意内容が履行されているか定期的に確認しますか。	はい 年に1回以上実施しております。
118	外部委託先管理	外部委託先を定期的に評価していますか。	はい 社内のセキュリティ水準を確認する、外部サービス・ツールの利用申請フローがあり、フロー内で確認しております。
119	外部委託先管理	外部サービスやツールを利用する場合、セキュリティ水準を確認していますか。	はい 社内のセキュリティ水準を確認する、外部サービス・ツールの利用申請フローがあり、フロー内で確認しております。

更新履歴：2025/07/04 初版リリース