SECURITY & PRIVACY

情報セキュリティ・
個人情報保護に関する資料

研修管理プラットフォーム「manaable」をご利用のお客様へ

1 **情報セキュリティ方針**
当社の正式な情報セキュリティ方針（ISMS）

2 **セキュリティポリシー**
manaableにおける具体的なセキュリティ対策

3 **プライバシーポリシー**
個人情報の取扱いと公表事項

manaable株式会社

〒151-0051 東京都渋谷区千駄ヶ谷4-10-8 ウイング410 2A　TEL：03-5413-3064

本資料は、2026年10月30日時点で当社ウェブサイトに掲載している内容を、印刷用に整えたものです。最新の内容は、各ページのURLをご確認ください。

PART 1

情報セキュリティ方針

https://corp.manaable.com/security-policy.html

manaable株式会社は、SaaS事業（研修管理プラットフォーム）及び、Webサイト構築・システム構築Webマーケティング・コンサルティング・保守及び運用サポートの事業を行っています。当社は、お客様や社会からの信頼に応える持続可能な企業を目指すために、お客様から委託され取扱う資産の消失、盗難、不正使用、漏えいを防止することを目的として、情報セキュリティマネジメントシステムを確立し、導入、運用、監視、見直し、維持及び継続的改善を行います。

当社の役員及びすべての従業者は、この目的を理解し、本方針ならびに確立した情報セキュリティマネジメントシステムの規定や手順および関連法令やガイドライン等を遵守することで、情報セキュリティ重視の考えで業務を遂行します。

国内規格JIS Q 27001:2025（国際規格ISO/IEC27001:2022＋Amd 1:2024）に準拠した具体的施策

1. 情報資産の保護管理

当社は、お客様からお預かりした情報資産および当社の情報資産を、消失、盗難、不正使用、漏えい等のインシデントから保護するため、JIS Q 27001規格に定められた適切な情報セキュリティの管理策を実施致します。

2. 法令順守

当社は、JIS Q 27001規格に基づいて確立した情報セキュリティマネジメントシステム規定および関連法令・ガイドライン等を遵守します。

3. 事故予防と発生時の対応

万一、情報セキュリティ上のインシデント（事件・事故等）が発生した場合には、速やかに原因究明、対策を講じ、影響を最小限にするように努めます。

4. 教育、啓蒙、訓練

当社は、役員・従業者に対し、JIS Q 27001規格の要求事項に則った教育を実施し、構築した規定に対する違反行為に対しては、明確なる責任を求めます。

5. 継続的改善

当社は、上記の活動を継続的に改善、実施する情報セキュリティマネジメントシステムを確立し、業務や社会情勢の変化・情報技術の変遷などに応じて、維持・見直しおよび継続的改善を行います。

制定日　2022年7月1日
改定日　2025年11月7日
〒151-0051　東京都渋谷区千駄ヶ谷4-10-8 ウイング410 2A
manaable株式会社
代表取締役　山田　宏樹

PART 2

セキュリティポリシー

https://manaable.com/policy/security.html

情報セキュリティ方針

manaable株式会社（以下「当社」）は、お客様からお預かりする情報資産を消失、盗難、不正使用、漏えい等から守るため、情報セキュリティマネジメントシステム（ISMS）を確立し、継続的に改善しています。役員及びすべての従業者は、情報セキュリティ方針、ISMSの規定及び関連法令を遵守して業務を行います。

当社の正式な情報セキュリティ方針は、コーポレートサイトに掲載しています（本資料 PART 1）。

第三者認証（ISMS）

適用規格	JIS Q 27001:2025（ISO/IEC 27001:2022 + Amd 1:2024）
認証登録番号	IR0147
認証範囲	研修管理プラットフォームのSaaS形式での提供／Webサイト・Webシステムの構築・保守・運用支援
初回登録日	2022年12月7日
有効期限	2028年12月6日
認証機関	アイエムジェー審査登録センター株式会社（ISR029）

認証範囲は本社（東京都渋谷区）です。年1回の外部審査と内部監査で運用状況を確認しており、2025年11月の再認証審査を含め、2022年の初回認証以降の外部審査で不適合の指摘は0件です。

情報セキュリティ管理体制

代表取締役を最高責任者とし、次の役割を任命しています。内部監査は、運用部門から独立した立場で実施します。

役割	主な責任
代表取締役	情報セキュリティ方針の承認、重大インシデント時の意思決定、マネジメントレビュー
情報セキュリティ管理責任者（ISMS責任者）	ISMSの運用監督、インシデントの判定と対応指揮、経営層への報告
情報セキュリティ管理者（ISMS事務局）	情報資産の管理、リスクアセスメント、従業者教育、インシデント記録
システム管理者	システム・ネットワークの運用、アクセス権管理、障害・インシデントの技術対応
内部監査責任者	年1回以上の内部監査の計画・実施、不適合の是正指示

信頼性の高いデータセンター

manaableは、アマゾン ウェブ サービス（AWS）の日本国内リージョンで稼働しています。利用者名、メールアドレス、研修受講履歴等のデータは、国内のデータセンターに保管しています。

AWSはISO/IEC 27001等の第三者認証を取得しており、日本政府の「ガバメントクラウド」にも選定されています（AWSが取得している認証の詳細：https://aws.amazon.com/jp/security/#certifications）。

データ管理とアクセス制御

- サーバーへのアクセスはファイアウォールで当社環境からに制限し、管理者権限はシステム管理担当者に限定しています。
- アクセス権は業務上必要な最小限とし、年1回以上見直します。退職・異動時は速やかに削除・変更します。
- 特権IDによる操作や情報資産へのアクセスはログを取得し、定期的に確認しています。
- お客様のデータには、調査等でお客様から依頼があった場合にのみアクセスします。データベース領域はお客様ごとに分けて構築しています。
- 開発・ステージング・本番の各環境は分離し、通常より強い権限が必要な作業は都度申請・承認のうえ実施します。テストに実データを使う場合は必要最小限としてマスキングし、終了後に削除します。
- 従業者のPC・可搬媒体は暗号化し、紛失・盗難時の漏えいを防止しています。
- 従業者が利用する業務システム・クラウドサービスには二段階認証を必須としています。
- システムの変更はチケットで管理し、影響のある変更は事前にお客様へお知らせします。
- ご契約終了後は、利用規約又は個別のご契約の定めに従い、お客様のデータ領域を削除します。
- 顔認証機能で取得した顔画像等のデータは、受講期間の終了から1週間で自動的に削除します。

不正アクセス対策

- ネットワークの入口にファイアウォール、サーバーにWAF及びアンチウィルスを導入しています。
- 脆弱性情報（JVN、IPA等）を常時収集し、ソフトウェアを安全な状態に保ちます。公開サーバーは年1回、IPAの基準に沿って点検します。
- 開発はIPA「安全なウェブサイトの作り方」に準拠し、セキュアコーディングとセキュリティテストを実施します。
- すべての通信をSSL/TLSで暗号化しています。管理機能は接続元IPアドレスの制限も可能です。

障害対策とバックアップ

- 24時間365日、サーバー性能・リソース・プロセス・ネットワーク・ジョブを監視し、異常時は管理者へ自動通知します。停止を検知したサービスは自動復旧を試みます。
- データは1日1回フルバックアップし、過去4日分を世代管理しています。バックアップは耐久性の高いAmazon S3に保管し、毎月正常性を確認しています。
- 障害時はメンテナンス画面又は障害発生メッセージを自動表示します。
- ウイルス感染、不正アクセス、システム障害、情報漏えい、自然災害の5つの想定シナリオごとに復旧手順を定め、年1回の机上訓練で検証しています。

情報セキュリティインシデント発生時の対応

情報漏えい、不正アクセス、ウイルス感染、システム障害、誤送信等のインシデント（又はその疑い）が発生した場合、当社は定めた手順に従い次のように対応します。

1. **初動対応**：発見者は直ちに被害拡大を止める処置（端末のネットワーク遮断、アカウント停止等）を行い、ISMS責任者へ報告します。
2. **判定と体制構築**：ISMS責任者がインシデントと判定した場合、代表取締役へ報告し、対応責任者と対応チームを編成します。
3. **調査と証拠保全**：影響範囲（対象データ・件数・期間）と原因を調査します。ログ等の証拠は改ざん・消失から保護します。
4. **お客様への通知**：影響を受けるお客様に、事実関係・発生原因・対応策を速やかにご連絡します。判明した事実は経過として随時ご報告します。
5. **関係機関への報告**：法令に基づき、個人情報保護委員会、監督官庁、警察、認証機関等へ必要な報告・相談を行います。専門機関（IPA、JPCERT/CC）の助言も活用します。
6. **復旧**：原因を取り除き、バックアップ等を用いてサービスを復旧します。必要に応じて当社ウェブサイト等で経過を公表します。
7. **再発防止**：原因と再発防止策を「インシデント報告書」に記録し、全社へ共有したうえで、リスクアセスメントと管理策の見直しに反映します。

委託先の管理

- 業務を委託する際は、事前に情報セキュリティと個人情報の取扱い状況を評価し、適合した場合のみ委託します。
- 秘密保持契約及び「個人情報の取扱いに関する覚書」を締結し、年1回再評価します。
- 再委託は原則禁止とし、やむを得ない場合は当社の承認を要し、同等の管理を求めます。
- 業務終了時には、お預けした情報の返却又は廃棄を確認し、記録します。

従業者の管理・教育と監査

- 入社時に退職後も有効な秘密保持誓約書を取得し、違反時の懲戒を就業規則で定めています。
- 全従業者に年1回の情報セキュリティ教育と理解度テストを実施し、定期的に運用点検を行っています。
- テレワークは「テレワーク規程」に基づき、許可された通信環境でのみ業務を行います。
- オフィスは入退管理と警備システムで保護し、クリアデスク・クリアスクリーンを徹底しています。
- 年1回の内部監査と代表取締役によるマネジメントレビューで、ISMSの有効性を確認しています。
- 生成AIの利用は「生成AI利用に関する社内ガイドライン」で定め、お客様の情報、個人情報、社内の非公開情報の入力を禁止しています。開発でAIを使う場合も、本番環境やお客様のデータベースには直接操作させません。

セキュリティチェックシートの提供

経済産業省による「クラウドサービスレベルのチェックリスト」、及びIPA（独立行政法人情報処理推進機構）による「安全なウェブサイトの作り方 改訂第7版」に準拠したセキュリティチェックシートを提供しています（当社ウェブサイトからダウンロードいただけます）。manaable の導入検討にご活用ください。

なお、お客様独自のチェックリストへの回答をご希望の場合は、別途有料オプションを提供しております。

サービスのセキュリティ機能

manaableでは、お客様（管理者の皆様）と受講者の皆様が安心してご利用いただけるよう、次の機能と取り組みを提供しています。

管理者の皆様へ

- データベース領域はお客様ごとに分けて構築しており、他のお客様の情報が見えることはありません。
- 管理画面への接続元IPアドレスを制限できます。
- 管理者アカウントごとに、操作できる権限を設定できます。
- 管理者アカウントに二段階認証を設定できます。
- 管理者の操作ログを記録しています。
- システムの変更で影響がある場合は、事前にお知らせします。

受講者の皆様へ

- すべての通信をSSL/TLSで暗号化しています。

- 顔認証機能（お客様がご利用の場合）により、受講申込時及び受講中の本人確認を行い、なりすまし受講を防いでいます。顔画像等のデータは、受講期間の終了から1週間で自動的に削除します。
- パスワードは、文字数など一定の条件を満たすものを設定していただきます。
- 受講者の皆様には、ご自身の情報だけが表示される仕組みです。

なりすましにご注意ください

manaableや当社を名乗る偽のウェブサイトやメールにご注意ください。当社がメールや電話でパスワードをお尋ねすることはありません。不審なサイトやメールを見つけた場合は、当社までお知らせください。

制定日　2021年4月1日
改定日　2025年3月7日
改定日　2025年11月7日
改定日　2026年10月30日
manaable株式会社
代表取締役　山田　宏樹

PART 3

プライバシーポリシー

https://corp.manaable.com/privacy.html

プライバシー・ポリシー

manaable株式会社ウェブサイト（以下 当ウェブサイト）では、ウェブサイトにアクセスされるすべてのお客様のプライバシー保護を何よりも重要であると考え、適切な保護を行いつつ業務にあたっております。そこで、当ウェブサイト及び研修管理プラットフォーム「manaable」で取り扱う情報とその使用についてご説明します。

個人情報保護の理念

manaable株式会社（以下、当社）は、研修管理プラットフォーム「manaable」をはじめとするWebサービスの開発・運営、及びWebサイト・システムの構築・保守・運用支援を核とした事業活動を行っています。事業活動を通じてお客様から取得する個人情報及び当社従業者の個人情報（以下、「個人情報」という。）は、当社にとって重要な情報であり、その個人情報を確実に保護することは、当社の重要な社会的責務と認識しております。

したがって、当社は、事業活動を通じて取得する個人情報を、以下の方針に従って取り扱い、個人情報保護に関して、お客様及び当社従業者への「安心」の提供及び社会的責務を果たしていきます。

方針

1. 個人情報の取得、利用及び提供に関して

- 適法、かつ、公正な手段によって個人情報を取得いたします。
- 利用目的の達成に必要な範囲内で、個人情報を利用いたします。
- 個人情報を第三者に提供する場合には、事前に本人の同意を取ります。
- 取得した個人情報の目的外利用はいたしません。また、目的外利用を行わないために、適切な管理措置を講じます。
- 目的外利用の必要が生じた場合は、新たな利用目的の再同意を得た上で利用いたします。

2. 法令、国が定める指針その他の規範（以下、「法令等」という。）に関して

個人情報を取り扱う事業に関連する法令等を常に把握することに努め、当社事業に従事する従業者（以下、「従業者」という）に周知し、遵守いたします。

3. 個人情報の安全管理に関して

- 個人情報への不正アクセス、個人情報の漏えい、滅失又はき損などの様々なリスクを防止すべく、個人情報の安全管理のための迅速な是正措置を講じる体制を構築し維持いたします。
- 点検を実施し、発見された違反や事故に対して、速やかにこれを是正するとともに、弱点に対する予防処置を実施いたします。
- 安全に関する教育を、従業者に徹底いたします。

4. 苦情・相談に関して

個人情報の取扱いに関する苦情及び相談については、個人情報問合せ窓口を設け、迅速な対応が可能な体制を構築し、誠意をもって対応いたします。

5. 継続的改善に関して

当社は、個人情報保護のため、内部規程の遵守状況を監視及び監査し、違反、事件、事故及び弱点の発見に努め、経営者による見直しを実施いたします。これを管理策及び内部規程に反映し、継続的な改善に努めます。当社はISO/IEC 27001に基づくISMS（情報セキュリティマネジメントシステム）の認証を取得しており、その仕組みの中で継続的に改善を行います。

6. 個人情報の漏えい等が発生した場合の対応に関して

個人情報の漏えい、滅失、毀損又はそのおそれ（以下「漏えい等」）が発生した場合、当社はセキュリティポリシーの「情報セキュリティインシデント発生時の対応」（本資料 PART 2）に従い、次の措置を講じます。

- 被害の拡大防止と事実関係・影響範囲・原因の調査を直ちに行います。
- お客様から委託を受けて取り扱う個人データ（manaableに登録された受講者情報等）の場合は、委託元であるお客様へ速やかにご報告し、お客様が行う個人情報保護委員会への報告やご本人への通知に必要な情報提供・協力を行います。
- 当社自身が取得した個人情報の場合で、個人情報保護法に定める報告対象事態に該当するときは、個人情報保護委員会へ報告し、ご本人へ通知します。
- 二次被害の防止や類似事案の回避に必要な場合は、事実関係と再発防止策を公表します。
- 原因を分析し、再発防止策を実施するとともに、管理体制の見直しに反映します。

制定日　2012年6月1日
改定日　2020年6月1日
改定日　2025年11月7日
改定日　2026年10月30日
manaable株式会社
代表取締役　山田　宏樹

個人情報の取扱いについて（公表事項）

(1) 事業者情報

manaable株式会社　代表取締役　山田　宏樹
〒151-0051　東京都渋谷区千駄ヶ谷4-10-8 ウイング410 2A

(2) 利用目的

開示対象個人情報の利用目的

個人情報の種別	利用目的
資料請求やお問い合わせをいただいた方の情報	お問い合わせへの対応、サービスに関するご案内
お取引先情報（ご担当者の情報を含む）	お取引先との連絡、契約の履行、履行請求、サービスの提供・サポート
採用候補者・応募者の方に関する情報	採用選考、連絡
社員情報	人事、総務などの雇用管理

ご本人から直接書面で取得する以外の個人情報の利用目的

個人情報の種別	利用目的	開示区分
manaableに登録された受講者等の情報（お客様からの委託による）	お客様からの委託に基づくサービスの提供（お客様の指示の範囲内でのみ取り扱います）	非開示（研修を主催する団体へお問い合わせください）
顔認証機能で取得する顔画像（お客様が同機能をご利用の場合）	お客様からの委託に基づく、受講申込時及び受講中の本人確認（顔画像等のデータは、受講期間の終了から1週間で自動的に削除します）	非開示
取引先から提供されたデータ	開発、制作等のため	非開示
インターネット・ビジネス・ジャパンから提供された採用応募者履歴書	当社の採用検討のため	非開示
顔写真等の素材写真	ホームページ制作、又はクラウドサービス運用のため	非開示

(3) 第三者提供と委託

法令に基づく場合を除き、ご本人の同意なく第三者に提供しません。業務の一部を委託する場合は、事前評価と契約締結により委託先を適切に監督します。

(4) 安全管理措置

- **組織的安全管理措置**：ISMS責任者を置き、漏えい等の報告連絡体制を整備し、年1回内部監査を実施
- **人的安全管理措置**：秘密保持誓約書の取得、年1回の教育と理解度テスト
- **物理的安全管理措置**：入退管理、警備システム、機器・媒体の暗号化と廃棄管理
- **技術的安全管理措置**：アクセス制御、通信の暗号化、不正アクセス対策、ログ監視
- **外的環境の把握**：個人データは日本国内のデータセンターで保管しています。

(5) 開示等の請求手続き

当社がご本人様又はその代理人様から、当社が保有する開示対象個人情報に関して、(1)開示、(2)利用目的の通知、(3)訂正、(4)追加、(5)消去、(6)利用停止又は第三者提供の停止のご請求（以下「開示等のご請求」）に対応させていただく場合の手続きは、下記のとおりです。なお、manaableに登録された受講者情報については、研修を主催する団体（委託元）へお問い合わせください。当社は団体の指示に従い対応します。

1. **申出先と提出書面**：個人情報開示等請求書に所定の事項をご記入のうえ、必要書類を添えて下記窓口へ郵送してください。配達記録郵便や簡易書留郵便など、配達の記録が確認できる方法でお願いいたします。封筒に朱書きで「個人情報請求書在中」とお書き添えいただければ幸いです。（請求書は当社ウェブサイトからダウンロードいただけます）
2. **ご本人様確認**：開示等請求者のご本人様確認のため、お電話による照合を行います。電話による照合ができない場合は、運転免許証、住民票、健康保険証等のコピーをご提示いただく場合があります。
3. **代理人様によるご請求**：代理人様に委任する場合は、個人情報開示等請求書に加えて、代理人様ご本人であることを確認する書類（運転免許証、住民票の写し、健康保険証のいずれか1点のコピー。本籍地は塗りつぶしてください）と、委任状（ご本人様が捺印し、その印鑑登録証明書を添付。親権者などの法定代理人の場合は、ご本人様との関係がわかる書類でも可）をご同封ください。
4. **手数料**：開示及び利用目的の通知のご請求は、1回の請求ごとに500円の手数料をいただきます。500円分の郵便定額小為替を提出書類にご同封ください。小為替のご購入料金及び郵送料はお客様のご負担となります。手数料が不足していた場合や同封されていなかった場合は、対応いたしかねます。
5. **回答方法**：請求者の請求書記載住所宛に、書面によってご回答いたします。

(6) 個人情報問合せ窓口

manaable株式会社　個人情報問合せ窓口
〒151-0051　東京都渋谷区千駄ヶ谷4-10-8 ウイング410 2A
TEL：03-5413-3064（平日10:00〜17:00）
＜個人情報に関する責任者＞　個人情報保護管理者　山田　宏樹

ISMS認証情報

認証基準	JIS Q 27001:2025（ISO/IEC 27001:2022 + Amd 1:2024）
認証登録番号	IR0147
登録範囲	研修管理プラットフォームのSaaS形式での提供／Webサイト・Webシステムの構築・保守・運用支援（適用宣言書：2版）
初回登録日	2022年12月7日
有効期限	2028年12月6日
認証機関	アイエムジェー審査登録センター株式会社（ISR029）