＼情報セキュリティ対策の チェックができる！／

情報セキュリティ管理

お役立ちチェックシート

情報セキュリティ管理入門セミナー参加特典

ARM Standard

本書の使い方

はじめに

本書は、ISMS（情報セキュリティマネジメントシステム）の
ISO規格（ISO/IEC 27001:2022）にある附属書Aを基にした「自社チェック用シート」です。
シンプルなチェック形式で、自社の情報セキュリティの実施状況を把握することができ、
今後の対策の方向性や改善の必要性が分かります。

チェック方法

1. 各管理策ごとに「行っている場合」にチェックを入れてください。
2. 未実施の項目が、自社にとって必要かどうか、必要な場合どのように対応すべきかを検討する材料としてご利用ください。
3. 定期的にチェックを更新し、改善状況を確認する習慣を持つことで、継続的な改善に繋がります。

活用のポイント

ISMS導入の第一歩として

初めてISMSを検討される方が、自社のセキュリティの整備状況を大まかに把握するための便利なツールとしてご利用いただけます。

認証取得準備のギャップ分析に

附属書Aの管理策が、どの程度自社で実施されているかを一覧で確認でき、
未対応の項目が明確になります。

社内の情報セキュリティ教育資料として

全社員や関係者が「ISMSの全体像」を知るためのツールとしてもご活用いただけます。

外部審査や内部監査の前点検に

事前に確認することで、監査準備の抜け漏れを防ぐことができます。

組織的管理策

組織的管理策では、組織の体制・運用ルールについてチェックします

チェック項目	チェック欄
5.1　情報セキュリティのための方針群 規則、法令、組織の状況を考慮し、適切な情報セキュリティ方針の決定をして、内部・外部の関係者へ伝達されている。また、あらかじめ決定していた間隔と、組織に大きな変化があった時、見直しがされている。	☐
5.2　情報セキュリティの役割及び責任 実際に業務を行う人々の中から、その責任者の選定がされている。	☐
5.3　職務の分離 組織の中の業務と責任の範囲を適切に分離されている。	☐
5.4　管理層の責任 従業員が情報セキュリティに則した業務を行うために、組織には情報セキュリティの重要性、情報セキュリティ方針、手順の伝達ができている。	☐
5.5　関係当局との連絡 組織を運営していくうえで必要な関係組織（警察、裁判所、消防署、官公庁など）の連絡先や誰が連絡をするのかなどが決定されている。	☐
5.6 専門組織との連絡 情報セキュリティに関する組織（情報セキュリティ研究会、情報処理推進機構など）との連絡体制について、関連当局と同様に連絡先やその手段などが決定されている。	☐
5.7 脅威インテリジェンス 組織の保護に関連した課題に応えることが可能か、脅威の状況に関する正確かつ詳細な理解を組織に提供する情報として十分かどうか、事象の発生時間、場所、以前の経験及び同様の組織における流行によって、情報に状況が含まれているか、情報に基づいて迅速かつ効果的に対応可能か、を考慮している。	☐

MEMO－自社の状況－

チェック項目	チェック欄
5.8 プロジェクトマネジメントにおける情報セキュリティ プロジェクトを進行するときも、組織で決定した情報セキュリティマネジメントシステムが適切に機能している。例えば、外部からシステム開発を依頼された場合、組織の技術情報や顧客から預かった情報資産の保護など。	☐
5.9 情報及びその他の関連資産の目録 組織が持つ情報資産の目録を作成・保持し、それらの情報資産が適切に管理されている。	☐
5.10 情報及びその他の関連資産の許容される利用 利害関係者に公開する情報について、公開する情報の範囲、利用を許可する情報処理施設、情報公開に必要な規則を、また、分類した情報情報資産について、適切な取り扱い方法、情報資産の保管場所、重要なデータのアクセス権限について、取り扱い方法の実施が決定されている。	☐
5.11 資産の返却 従業員の雇用終了時には、組織が権限を与えた情報資産（モバイル機器、カードキー、組織から貸与した資源など）を返却してもらっている。	☐
5.12 情報の分類 組織が所持する情報資産の重要性や機密性を分類している。	☐
5.13 情報のラベル付け 情報の分類でレベル分けした情報資産に重要度ごとに名前を付けている。	☐
5.14 情報の転送 外部との通信行為に関して、転送方針や手順、管理策の決定、電話や電子メールなど情報転送の特定、改ざんや盗聴などの脅威の特定などを含めた規則、手順などを備えている。	☐
5.15 アクセス制御 組織の情報資産を保護するため、アクセス制限の方針や対象、手順などの決定と文書を作成している。	☐

MEMO－自社の状況－

チェック項目	チェック欄
5.16 識別情報の管理 必要な力量や権限が認められていない人が情報資産にアクセスできないように、登録や登録削除について手順の決定と実施を行っている。	☐
5.17 認証情報 情報資産の保護のために重要なパスワードの管理についてルールを決定している。	☐
5.18 アクセス権 アクセス権の提供及び無効化： 適切な登録と登録解除に必要な確認事項や手順を決定している。 アクセス権のレビュー： 権限を与えた利用者のアクセス状況を定期的に確認し、評価をしている。 アクセス権の削除又は修正： 雇用を終了した従業員のアクセス権の削除や必要時には登録状況を変更している。	☐
5.19 供給者関係における情報セキュリティ 資源の管理に関わる情報セキュリティの要求事項を組織と供給者間で明確にしている。	☐
5.20 供給者との合意における情報セキュリティの取扱い ITの供給者とは関連する情報セキュリティ要求事項について合意している。	☐
5.21 情報通信技術(ICT)サプライチェーンにおける 情報セキュリティの管理 供給者の関連組織に対する情報セキュリティ要求事項を含めた合意をしている。	☐
5.22 供給者のサービス提供の監視、レビュー及び変更管理 組織は供給者の業務プロセスを監視し、セキュリティ方針を満たしているかレビューを行っている。また、供給者からのサービスを変更する場合、リスクの発生や組織への影響を管理している。	☐
5.23 クラウドサービスの利用における情報セキュリティ クラウドサービスプロバイダとクラウドサービスカスタマ双方の責任を適切に定義している。	☐

MEMO－自社の状況－

チェック項目	チェック欄
5.24 情報セキュリティインシデント管理の計画策定及び準備 組織の活動が脅かされるような情報セキュリティインシデントが発生した場合、管理層の責任と手順の確立によって適切な対応を実施している。	☐
5.25 情報セキュリティ事象の評価及び決定 報告又は検知された情報セキュリティ事象が、組織にとって大きな情報セキュリティインシデントに該当するか否かを判断している。	☐
5.26 情報セキュリティインシデントへの対応 情報セキュリティインシデントへの対応手順の文書を作成している。	☐
5.27 情報セキュリティインシデントからの学習 情報セキュリティインシデントの分析によって判明した特性に基づき、効果的な予防策を講じている。	☐
5.28 証拠の収集 インシデント発生原因の証拠となる情報の収集手順及び適用を行っている。	☐
5.29 事業の中断・阻害時の情報セキュリティ 組織活動が困難な状況でも満たすべき最低限の要求事項を決定している。また、情報セキュリティ継続の計画において決定した要求事項を満たすための管理策の手順の確立と文書の作成をしている。そして、事業継続計画で策定した手順は定期的に検証し、必要に応じて見直している。	☐
5.30 事業継続のためのICTの備え 事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画、実施、維持及び試験をしている。	☐
5.31 法令、規制及び契約上の要求事項 組織に関係する法令について明確にし、その文書の作成と維持を行っている。	☐
5.32 知的財産権 ソフトウェア製品に関連する法令順守のために適切な手順の決定と実施を行っている。	☐

MEMO – 自社の状況 –

チェック項目	チェック欄
5.33 記録の保護 記録に求められていることを考慮した保護を行っている。	☐
5.34 プライバシー及び個人識別可能情報（PII）の保護 組織が所有する個人情報の保護を行っている。	☐
5.35 情報セキュリティの独立したレビュー 情報セキュリティマネジメントシステムへの組織の取組状況について定期的にレビューを行い、情報セキュリティが運用されているか確認している。	☐
5.36 情報セキュリティのための方針群、規則及び標準の順守 組織の管理者は情報セキュリティの方針群及び規定した手順を守っているかを定期的にレビューしている。	☐
5.37 操作手順書 操作手順の文書を作成し、利用者に伝達している。	☐

MEMO – 自社の状況 –

なるほど！お役立ちコラム１

定期的に見直すことの大切さ

情報セキュリティは、一度対策を作ったら終わりではありません。
環境や技術はどんどん変わるため、定期的に「見直し」をすることが大切です。
見直すことで、新しいリスクに気づき、改善点も発見できます。
また、同じチェックシートを一定期間を置いて再度使うことで、
組織の情報セキュリティ体制の変化を具体的に把握することもできます。

人的管理策

人的管理策では、組織に関わる人の状況についてチェックします

チェック項目	チェック欄
6.1　選考 新たな従業員の選考について、人材に必要な力量、選考手順、提供を求める書類、情報の管理方法を決定している。	☐
6.2 雇用条件 雇用契約書に情報セキュリティに関する事項を含めている。	☐
6.3　情報セキュリティの意識向上、教育及び訓練 組織内の人材に対して、業務に必要な教育と訓練を実施している。	☐
6.4　懲戒手続 懲戒手続について決定している。	☐
6.5　雇用の終了又は変更後の責任 情報資産が外部に流出しないように、雇用を終了した人物へのルール作りを行っている。	☐
6.6　秘密保持契約又は守秘義務契約 情報の機密保持に関する契約の締結及びその手順の文書を作成している。	☐
6.7　リモートワーク モバイル機器を利用して、自宅や滞在先などの勤務先以外で仕事をする場合のルール作りを行っている。	☐
6.8　情報セキュリティ事象の報告 効果が疑わしい対策、マルウェア感染の疑い、異常なシステム挙動や違反等を発見した場合、発見者の誰もが速やかに報告できる仕組みがある。 （情報セキュリティ事象には、インシデント、違反及びぜい弱性が含まれる。）	☐

MEMO－自社の状況－

物理的管理策

物理的管理策では、組織に関わる設備や環境などの状況についてチェックします

チェック項目	チェック欄
7.1　物理的セキュリティ境界 重要な情報資産のセキュリティ境界を物理的に決定している。	☐
7.2　物理的入退 セキュリティ区画へのアクセス制限を決定し、入退管理を確実にしている。	☐
7.3　オフィス、部屋及び施設のセキュリティ オフィスや重要な情報処理施設のセキュリティ保護のために、施設の設置場所やセキュリティ設計において考慮をしている。	☐
7.4　物理的セキュリティの監視 重要なシステムを収容している建物へのアクセスは、認可されていないアクセス又は疑わしい行動を検知するために、監視カメラ、探知機などで、継続的に監視している。	☐
7.5　物理的及び環境的脅威からの保護 自然災害や悪意のある攻撃又は事故などの脅威に対しての保護策を決めている。	☐
7.6　セキュリティを保つべき領域での作業 セキュリティ区画内での作業手順を決定している。	☐
7.7　クリアデスク・クリアスクリーン クリアデスク、クリアスクリーンに関する方針の確立と実施を行っている。	☐
7.8　装置の設置及び保護 重要な情報処理施設の装置、情報や通信に関連する装置などを環境、人的脅威及び災害から保護している。	☐

MEMO－自社の状況－

チェック項目	チェック欄
7.9　構外にある資産のセキュリティ 組織の外部に持ち出した情報資産の保護を行っている。	☐
7.10　記憶媒体 業務中に使用する情報を取り扱う媒体（パソコンやUSB、データ記入済みの書類など）について様々な考慮を行った上での管理を行っている。	☐
7.11　サポートユーティリティ 電気やガス、水道などのサポートユーティリティの不具合による停電や故障から装置を保護している。	☐
7.12　ケーブル配線のセキュリティ 自然災害や悪意のある攻撃又は事故などの脅威に対しての保護策を決めている。	☐
7.13　装置の保守 組織は情報資産の可用性と完全性の維持を行っている。	☐
7.14　装置のセキュリティを保った処分又は再利用 装置内のデータ消去によって情報資産の漏洩防止を行っている。	☐

MEMO－自社の状況－

なるほど！お役立ちコラム２

現場の声を活かす

実際に仕事をしている現場の意見こそ、
チェックシートを活用するときには欠かせません。
いろんな人の目で確認することで、見落としやすい問題も見つかります。
現場の声が反映されると、みんなが自分事として取り組みやすくなり、
結果的に組織のセキュリティがぐっと強くなります。

技術的管理策

技術的的管理策では、組織に関わるシステムやネットワークについてチェックします

チェック項目	チェック欄
8.1　利用者エンドポイント機器 組織内で利用するパソコンやモバイル機器の設定や管理について決定している。	☐
8.2　特権的アクセス権 通常のアクセス権限に加えて特別な許可を与える場合は、リスク発生時に大きな影響が予想されるため、より厳格な制限と管理を行っている。	☐
8.3　情報へのアクセス制限 システム機能へのアクセス制限を行っている。	☐
8.4　ソースコードへのアクセス プログラムソースコードの書き換えによるシステムの破損を防ぐために、アクセス制限を行っている。	☐
8.5　セキュリティを保った認証 アクセス制御方針を達成するために適切なシステムへのログオン方法を決定している。	☐
8.6　容量・能力の管理 業務を滞りなく進行させるために必要な人材の能力や物、情報の量の管理を行っている。	☐
8.7　マルウェアに対する保護 組織の情報資産を悪意のあるサイバー攻撃から保護するために、脅威となるマルウェア、被害を受けた際の対応手順などを決定し、利用者に伝達している。	☐
8.8　技術的ぜい弱性の管理 組織が実施している情報システムの技術的ぜい弱性に関する決定を行っている。	☐

MEMO－自社の状況－

チェック項目	チェック欄
8.9　構成管理 存続期間にわたって、定義した構成を維持するためのプロセスやツールを定義・実装している。	☐
8.10　情報の削除 情報を削除する際は、要求事項、法規制を考慮して削除方法を決定し、削除の結果を証拠として記録又は取得している。	☐
8.11　データマスキング PIIなどの取扱いに慎重を要するデータの保護が必要な場合、データマスキングや仮名化・匿名化を使用し、データを隠している。	☐
8.12　データ漏えい防止 データ漏えいのリスクを減らすために、保護しなければならない情報の特定、データ漏えいの可能性があるチャネルの監視、情報漏えいを防止するためのツールの導入を考慮している。	☐
8.13　情報のバックアップ 組織はバックアップ方針を確立し、定期的なバックアップによる情報損失の防止を行っている。	☐
8.14　情報処理施設・設備の冗長性 例えば、災害やサーバー機器の故障が発生した場合でも情報の可用性が確保できるように、組織に設置する情報処理施設・設備はその能力に余裕をもって導入している。	☐
8.15 ログ取得 イベントログの取得や保持、レビューに関するルールを決定している。また、ログ機能や情報の保護について決定している。	☐
8.16 監視活動 システムやネットワークのトラフィック、システムやサーバー、ネットワーク装置へのアクセス、セキュリティツールからのログなどの監視を実施している。	☐
8.17 クロックの同期 組織内で利用する機器の時刻が統一されている。	☐

MEMO－自社の状況－

チェック項目	チェック欄
8.18 特権的なユーティリティプログラムの使用 ユーティリティプログラムはシステムやパソコンの使用を支援し、大きな影響を与えるため、その使用と管理には十分な注意を払っている。	☐
8.19 運用システムへのソフトウェアの導入 業務中に使用するソフトウェアの導入について適切な手順で実施している。	☐
8.20 ネットワークセキュリティ 不正アクセスから情報資産を保護するために、ネットワークの管理と制御を行っている。	☐
8.21 ネットワークサービスのセキュリティ ネットワークサービスに関して、セキュリティ機能、サービスレベル、管理上の要求事項の特定を行っている。	☐
8.22 ネットワークの分離 重要な情報資産専用の設備を別に用意する物理的分離、インターネットから侵入できないネットワークを構築する論理的分離など、ネットワークを分離している。	☐
8.23 ウェブフィルタリング 違法な情報がある、又はウイルスもしくはフィッシングの材料があることが知られているウェブサイトなどに従業員がアクセスするリスクが減るように、関係するIPアドレス/ドメインへのアクセスを管理している。	☐
8.24 暗号の利用 暗号化の利用のルールを明確にして実施している。	☐
8.25 セキュリティに配慮した開発のライフサイクル システム開発に関する基本規定の策定と実施を行っている。	☐
8.26 アプリケーションセキュリティの要求事項 Webサービスを利用する場合、サービス内に含まれる情報を保護している。	☐

MEMO－自社の状況－

チェック項目	チェック欄
8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 組織がシステム開発の業務を行う場合、基本的なセキュリティ原則の決定と適用を行っている。	☐
8.28 セキュリティに配慮したコーディング セキュリティに配慮したコーディングに関して優れたガバナンスを提供するように、組織全体のプロセスを確立している。	☐
8.29 開発及び受入れにおけるセキュリティテスト セキュリティ機能のテストについて、開発期間中の実施、機能ごとの実施、設計した通りの機能を示したかの確認、実施したテストの内容や時期の記録などを行っている。	☐
8.30 外部委託による開発 外部に委託した開発業務は進捗状況などを監督し、監視している。	☐
8.31 開発環境、テスト環境及び本番環境の分離 リスクの影響を小さくするために実際の運用環境と分離している。	☐
8.32 変更管理 組織の状況変化に合わせて、情報セキュリティに関する変更を管理している。	☐
8.33 テスト用情報 テストに使用するデータの選定と保護、管理を行っている。	☐
8.34 監査におけるテスト中の情報システムの保護 情報セキュリティマネジメントシステムの運用状況について監査を行う際は、業務への影響が最小限になるように計画している。	☐

MEMO – 自社の状況 –

チェックは以上で完了です。

小さなチェックの積み重ねが、大きなリスクを防ぎ、組織を守る力になります。

この冊子が、これからの情報セキュリティ対策に少しでもお役に立てば幸いです。

会社紹介

■会社概要

・アームスタンダード株式会社

・〒103-0012　東京都中央区日本橋堀留町1-10-15　JL日本橋ビル1F

■導入実績

・ISO認証登録件数グループ合計　約5,500件（2025年3月時点）

・ISO認証機関としてグループで国内シェア第3位の審査実績

■お問い合わせ

お気軽にご相談・お問い合わせください

TEL：03-3666-8814（営業）

FAX　：03-3666-8752

HP　https://www.armstandard.com/

ISO認証審査からツールを活用したマネジメントシステムの構築、社員教育まで、アームスタンダードにお任せください

ISO認証審査
ISO9001
ISO14001
ISO/IEC27001

WebMiCS

文書管理ツール
「WebMiCS」

eラーニング
「ReAlead」
各種セミナー

ReAlead
eラーニング・学習管理システム

＼　お役立ち情報をHPにも掲載しています！　／

アームスタンダード　検索

ARM Standard

弊社のサービスはプロセスやシステムの改善のための以下のような一般的な情報を提供しております。

- 認証基準の意味及び意図の説明
- 改善の機会の特定
- 関係する理論、方法論、技術、またはツールの説明
- 機密情報でない、関連するベストプラクティスの情報共有
- 審査を受けるマネジメントシステムの範疇にない、その他のマネジメントシステムの側面

アームスタンダード株式会社