情報セキュリティ対策ベンチマーク ver.4.7 の質問一覧

情報セキュリティ対策ベンチマークの質問は、**2部構成**（全 46 問）となっています。
この質問一覧にあらかじめ回答を記載しておくと、Web での自己診断が容易になります。
回答欄には、メモ的に使える空欄を設けました。選択した回答に対して、どのような状況なのか
具体的に記入することで、後の改善に役立てることができます。

【自己診断の方法】

すべての質問について、各回答欄の選択肢の中からあてはまるものに○（マル）を付けてください。
メモ的に記入できる欄もあります。（Web の自己診断では、この項目はありません。）

回答記入例

選択肢

できていない ↑ ↓ できている

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている。
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

設問

貴社では、情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。
（ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を実践するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を点検し必要に応じて見直すことが大切です。）

あてはまるのが、
選択肢2の場合

① 回答欄 （いずれか一つに○）	1　(2)　3　4　5 以前定めたものを更新していない。

問１ 情報セキュリティに対する組織的な取り組み状況についてうかがいます。
以下の①～⑧のそれぞれの設問について、次の**選択肢の中からもっともあてはまる回答欄の番号に○**をつけてください。

設問①～⑦の選択肢

できていない ↑ ↓ できている

1. 経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2. 経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① 情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。
（ポリシーや規程は、サンプルのコピーではなく、自組織の事業やリスクを鑑みた内容であることが重要です。また、そうしたポリシーや規程を実践するためには、定めた規程類を関係者に十分に周知させると共に、規程類の順守状況を点検し必要に応じて見直すことが大切です。）

① 回答欄（いずれか一つに○）	1　2　3　4　5

② 情報セキュリティに関する規程や対策を策定する際に、組織の重要な資産に関する危険性や脆弱性について評価していますか。
（このような手順をリスクアセスメントといいます。リスクアセスメントの手順を確立し、定期的に実施することが、費用対効果の高い情報セキュリティ対策を実施する上で重要な要素となります。）

② 回答欄（いずれか一つに○）	1　2　3　4　5

③ 経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令順守)の推進体制を整備していますか。
（推進体制を整備するためには、経営層がリーダシップを発揮すること、各担当者の権限と責任を明文化することなどが重要です。また、法令順守のためには、順守すべき法令を正確かつ網羅的に把握することが必要です。）

③ 回答欄（いずれか一つに○）	1　2　3　4　5

④ 重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。
（情報資産をその重要性に応じて管理するためには、レベル分け、レベルに応じた表示や取扱方法などの指針及び情報の管理責任者を定める必要があります。）

④ 回答欄（いずれか一つに○）	1　2　3　4　5

⑤ 重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。
（適切な措置とは、業務プロセスごとの作業責任者や作業手順の明確化、取扱者の限定、処理の記録や確認などを指します。また、業務プロセスは、手作業で行うか、

⑤ 回答欄（いずれか一つに○）	1　2　3　4　5

情報システムに依存するかを問いません。）

⑥ **外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。**
（セキュリティ上の理由とは、たとえば情報の漏えいや消失、情報あるいは情報システムの誤用などの防止を指します。）

⑥ 回答欄 （いずれか一つに○）	1　2　3　4　5

⑦ **従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。**
（従業者に情報セキュリティについての要求を順守させるためには、従業者の管理責任者を明確にし、従業者が守るべきルールなどを明確にし、それらを周知させておく必要があります。）

⑦ 回答欄 （いずれか一つに○）	1　2　3　4　5

⑧ **経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。**
（情報セキュリティ教育は、全員に漏れなく定期的に行うことが大切です。セキュリティ対策上の順守事項、禁止事項の徹底とともに、情報セキュリティの脅威と対策についても教育します。）

⑧ 回答欄 （いずれか一つに○）	1　2　3　4　5

問２ 物理的（環境的）セキュリティ上の施策についてうかがいます。以下の①～④のそれぞれの設問について、次の**選択肢の中からもっともあてはまる回答欄の番号に○**をつけてください。

設問①～⑤の選択肢

できていない
1. *方針やルールを定めておらず、実施されていない*
2. 方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

できている

① **特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。**
（特にセキュリティを強化したい建物や区画については、ゲートや間仕切りを設けるなどして、境界を明確にし、入退館や入退室管理を実施する、あるいは警報装置の設置などを行います。また、荷物の受渡し場所や外部者の作業場所を確保するなど、セキュリティを考慮して物理的に区域を分けるようにします。）

① 回答欄 （いずれか一つに○）	1　2　3　4　5

② **顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。**
（自組織の建物や事務所には、思ったよりも多くの外来者が出入りしている事があります。そうした外来者に守って頂くべきルールをあらかじめ定めておくことが重要です。）

② 回答欄 （いずれか一つに○）	1　2　3　4　5

③ **重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。**
（安全性に配慮した配置または設置とは、たとえば、重要なシステムの安全な場所への設置、盗み見の防止や盗聴防止などに配慮した設置、配線類の地下や床下への埋設、浸水、火災、地震などを考慮した配置などを言います。）

③ 回答欄 （いずれか一つに○）	1　2　3　4　5

④ **重要な書類、モバイル PC、記憶媒体などについて適切な管理を行っていますか。**
（適切な管理とは、たとえば、保管キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄などを言います。また、重要な書類には、情報システムに関する文書を含みます。）

④ 回答欄 （いずれか一つに○）	1　2　3　4　5

問３ 情報システム及び通信ネットワークの運用管理状況に関するセキュリティ対策についてうかがいます。以下の①～⑦のそれぞれの設問について、次の**選択肢の中からもっともあてはまる回答欄の番号に○**をつけてください。

設問①～⑤の選択肢

できていない ↓ できている

1. 方針やルールを定めておらず、実施されていない
2. 方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① **情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。**
（適切な保護には、開発環境、テスト環境と運用環境の分離、変更管理の実施、開発での本番データの使用制限などが含まれます。）

① 回答欄 （いずれか一つに○）	1　2　3　4　5

② **情報システムの運用に際して、必要なセキュリティ対策を実施していますか。**
（必要なセキュリティ対策には、各種手順書の作成、ルールに従った運用、監視、ログの取得と分析などが含まれます。）

② 回答欄 （いずれか一つに○）	1　2　3　4　5

③ **重要なデータや関連するシステムのバックアップに関する手順を文書化し、実施していますか。**
（データの損失やシステム障害事故などからの迅速な復旧のために、バックアップの計画を策定し、システム化しておくことは非常に重要です。もしも重要なデータやそれに関連するシステムのバックアップが正しく行われていない場合、システム障害の際にこれらを復旧することができず、ビジネスに深刻な影響を与える恐れがあります。）

③ 回答欄 （いずれか一つに○）	１　２　３　４　５

④ **不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。**
（不正プログラム対策には、ウイルス対策ソフトの導入や、パターンファイルの更新を適時行うこと、ぜい弱性を解消することなどが含まれます。）

④ 回答欄 （いずれか一つに○）	１　２　３　４　５

⑤ **導入している情報システムに対して、適切なぜい弱性対策を実施していますか。**
（適切なぜい弱性対策には、セキュリティを考慮した設定や、パッチ（修正プログラム）の適用、バージョン管理や構成管理、変更管理などが含まれます。）

⑤ 回答欄 （いずれか一つに○）	１　２　３　４　５

⑥ **通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。**
（適切な保護策には、VPN の使用や重要な情報の SSL などによる暗号化があります。）

⑥ 回答欄 （いずれか一つに○）	１　２　３　４　５

⑦ **モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。**
（モバイル PC や USB メモリなどの記憶媒体の使用場所には、外部のパブリックスペースやリモートオフィス、自宅などを含みます。外部のセキュリティの脅威は内部よりも高いことを考慮して対策を行う必要があります。）

⑦ 回答欄 （いずれか一つに○）	１　２　３　４　５

問４ 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況についてうかがいます。以下の①～⑤のそれぞれの設問について、次の**選択肢の中からもっともあてはまる回答欄の番号に○**をつけてください。

設問①～⑤の選択肢

できていない ↑ ↓ できている

1. 方針やルールを定めておらず、実施されていない
2. 方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

① **情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証を適切に実施していますか。**
（適切な利用者 ID の管理には、利用者 ID の定期的な見直しによる不要な ID の削除や共用 ID の利用制限、単純なパスワードの設定禁止などがあります。）

① 回答欄（いずれか一つに○）	１　２　３　４　５

② **情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。**
（適切なアクセス権の管理には、アクセスできる情報システムを利用者ごとに限定すること、利用できる機能を制限すること、利用者のアクセス権をレビューすることなどがあります。）

② 回答欄（いずれか一つに○）	１　２　３　４　５

③ **ネットワークのアクセス制御を適切に実施していますか。**
（適切なネットワークのアクセス制御には、たとえばネットワークの分割や外部からの接続時の認証などがあります。）

③ 回答欄（いずれか一つに○）	１　２　３　４　５

④ **業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。**
（自組織での開発、外部委託による開発を問わず、開発の際に必要なセキュリティ対策としては、仕様書にセキュリティ上の要求事項を盛り込むこと、設計や開発に際してぜい弱性を作り込まないように配慮すること、ぜい弱性を残さないための適切なシステム試験を実施することなどがあります。）

④ 回答欄（いずれか一つに○）	１　２　３　４　５

⑤ **ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。**
（選定や購入、開発や保守を外部委託している場合は、セキュリティ上の観点からの点検が可能かどうかを回答してください。）

⑤ 回答欄（いずれか一つに○）	１　２　３　４　５

問５ 情報セキュリティ上の事故対応状況についてうかがいます。以下の①～③のそれぞれの設問について、次の**選択肢の中からもっともあてはまる回答欄の番号に○**をつけてください。

設問①～③の選択肢

できていない ↑
1. 方針やルールを定めておらず、実施されていない
2. 方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3. 方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4. 経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている
5. 4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

↓ できている

① **万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。**
（適切な対策には、たとえばシステムの二重化、バックアップと運用記録の取得、障害対応手順の明確化、外部委託先とのサービスレベルの合意などがあります。）

① 回答欄（いずれか一つに○）	1　2　3　4　5

② **情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。**
（事件や事故への備えには、そうした万が一の場合にとるべき行動をあらかじめ検討しておくこと、検討した結果を文書にまとめて関係者に周知しておくこと、緊急の連絡網を整備すると共に、必要な要員や資機材を揃えられるようにあらかじめ手配しておくことなどがあります。）

② 回答欄（いずれか一つに○）	1　2　3　4　5

③ **何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。**
（万が一、情報システムが停止してしまった場合に備えて、普段は情報システムで行っている業務をたとえば手作業で代替できるように、そうした業務の手順書や様式類をあらかじめ用意しておくこと、またそうした手作業を実施できる場所や資機材を確保しておくこと、さらに手作業で代替できるように要員を訓練しておくことなどが重要です。）

③ 回答欄（いずれか一つに○）	1　2　3　4　5

（次のページにお進み下さい）

貴社の事業内容などについて、下記 1．～19．の質問にお答えください（記号に○）。

1.-2. 従業者数（派遣、アルバイトを含む）およびそのうちの正規職員（正社員）の割合をお答えください。
（部門単位で利用する場合も、全社の単位で回答して下さい。）

従業者数：
a. 10 人以下　b. 100 人以下　c. 300 人以下　d. 1000 人以下　e. 1000 人を超える

うち正規職員（正社員）の割合：
a. 10 %以下　b. 30 %以下　c. 50 %以下　d. 70 %以下　e. 70 %を超える

3.-6. 売上高と国内外の拠点数（本店・支社・支店・営業所の合計）をお答えください。
（部門単位で利用する場合も、全社の単位で回答して下さい。公的機関の場合は予算、国内外の拠点数を回答。）

売上高：
a. 1000 万円以下　b. 1 億円以下　c. 10 億円以下　d. 100 億円以下　e. 100 億円を超える

資本金の額：
a. 1000 万円以下　b. 1 億円以下　c. 10 億円以下　d. 100 億円以下　e. 100 億円を超える

国内の拠点数：
a. 1 箇所　b.10 箇所以下　c. 30 箇所以下　d. 100 箇所以下　e. 100 箇所を超える

海外の拠点数：
a. 0 箇所(なし)　b.10 箇所以下　c. 30 箇所以下　d. 100 箇所以下　e. 100 箇所を超える

7. 業種を、以下の中からお選びください。

a. 農業　b. 林業　c. 漁業　d. 鉱業　e. 建設業　f. 製造業　g. 電気業(発電、変電)　h. ガス業
i. 熱供給業　j. 水道業　k. 通信業(固定／移動電気通信)　l. 放送業　m. 情報サービス(ソフトウエア、情報処理)
n. ISP、ASP　o. 出版業、新聞業　p. 運輸業　q. 卸売・小売業　r. 金融・保険業　s. 不動産業
t. 飲食店，宿泊業　u. 医療，福祉　v. 教育，学習支援業　w.政府機関、地方自治体、公益法人
x. その他

8. 事業は、国家や社会基盤、経済基盤に与える影響の観点から、どの程度の公益性がありますか。

a. ほとんどない　b. 少ない　c. 他の業種に比べると高い　d. 事業の性質上極めて高い

9. 事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさはどの程度ありますか。

a. ほとんどない　b. 少ない　c. 大きな影響がある　d. 極めて大きな影響がある

10. 主要な業務に関わるプロセスのうち、情報システム（外部のシステムを含む）に依存している割合はどの程度ですか。

a. 一部にとどまる （25 %以下）
b. 若干依存している （50 %以下）
c. 多くの部分が依存している （75 %以下）
d. ほとんどの部分が依存している （75 %を超える）

11. 主要な業務に関わるプロセスのうち、インターネットに依存している割合はどの程度ですか。

a. 一部にとどまる （25 %以下）
b. 若干依存している （50 %以下）
c. 多くの部分が依存している （75 %以下）
d. ほとんどの部分が依存している （75 %を超える）

12. 主要な情報システムについて、（月間）売上高に影響を及ぼさないで済む、許容停止時間はどれぐらいですか。
（公的機関の場合は、主要業務に影響を及ぼさないですむ許容停止時間を回答）

a. 1時間以内　b. 半日以内　c.1日以内　d. 数日以内　e. それ以上

13. 主要な情報システムが営業日に「24 時間」停止した場合、貴社のその日の売上高にどの程度の影響を及ぼしますか。
（公的機関の場合は、主要業務に対する影響の程度について回答）

a. ほとんど影響を受けない（25 %減以下）
b. 影響はあるが、部分的にとどまる。（50 %減以下）
c. 大きな影響を受ける。（75 %減以下）
d. 深刻な影響を受ける。（75 %減を超える）

14. 個人情報漏洩等、情報セキュリティ関連の事故が発生した場合、貴社のブランド（企業イメージ）にどの程度の影響がありますか。

a. ほとんどない　b. 部分的に影響がある　c. 大きな影響がある　d. 企業の存続に関わる影響がある

15. 貴社の業務は、元請や代理店、フランチャイジー等のビジネスパートナーにどの程度依存していますか。

a. ほとんど依存していない　b. 部分的に依存している　c. 大きく依存している
d. 元請や代理店、フランチャイジーなしでは事業が成り立たない

16. 貴社では、外部に漏洩すると事業に極めて深刻な影響が生じる重要情報（国家機密、営業機密、プライバシー情報等）をどの程度保有、管理または使用していますか。

a. ほとんどない　b. 少ない　c. 全体の半分程度　d. ほとんどがその種の情報である

17. 貴社では、事業を実施する上で何名分程度の個人情報を取り扱っていますか。
（データの述べ数の概数でお答えください）

a. 1000 件以下　b. 5000 件以下　c. 1 万件以下　d. 10 万件以下　e. 10 万件を超える

18. 貴社における離職率（直近の1年間に退職・転職された従業者の割合）はどの程度ですか。

a. 10 %以下　b. 30 %以下　c. 50 %以下　d. 70 %以下　e. 70 %を超える

19. 貴社において過去に、事業活動に影響を与えるような IT 事故が発生したことがありますか。

a. はい　　b. いいえ

はいと答えた方には、あてはまるもの全ての記号に○をつけてください

(ア) 主要な業務に関わる情報システムのウイルス感染
(イ) 全社的な PC のウイルス感染
(ウ) 社内システムへの（ネットワーク経由での）不正侵入
(エ) 自社ホームページの改ざん
(オ) 事業上のノウハウや顧客情報等、機密情報や個人情報の社外への漏洩
(カ) 他社ホームページ等に対する意図しない攻撃や、ウイルスメールの送信
(キ) 許容停止時間を超えるシステムダウン

この診断は、組織単位、部門単位で行うことができますが、診断の基礎データとして算入されるのは、原則として組織単位の回答データとなります。今回の診断の範囲を選択してください。（あてはまる記号に○）

a. 組織全体、事業部　b.部門単位　c.その他

（この質問は Web の自己診断では事業内容等に関する質問の後でお答えいただきます。）

メモ欄

記入漏れがないか今一度ご確認ください。