情報セキュリティ対策
ベンチマーク活用集

資料

資料１　情報セキュリティ対策ベンチマークの質問一覧

情報セキュリティ対策ベンチマークver.3　25項目の質問一覧

大項目1．情報セキュリティに対する組織的な取組状況	
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。
②	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。
③	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いをするための方法を定めていますか。
④	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。
⑤	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。
⑥	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。
⑦	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み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。
大項目2．物理的（環境的）セキュリティ上の施策	
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。
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。
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。
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。
大項目3．情報システム及び通信ネットワークの運用管理	
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。
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。
③	不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）への対策を実施していますか。
④	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。
⑤	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。
⑥	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。
大項目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	
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。
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。
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。
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。
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。
大項目5．情報セキュリティ上の事故対応状況	
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。
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。
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。

情報セキュリティ対策ベンチマークVer.3 質問と対策のポイント

大項目1. 情報セキュリティに対する組織的な取組状況

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。

説明 ポリシーや規程を組織にとって有効なものとするためには、自組織の状況に見合った内容にする必要があります。そのためには、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とすることが重要です。また、対策の実効性を確保するためには、定めた規程類を役員や全従業員に対して十分に周知すると共に、規程類の順守状況を適宜点検し、必要に応じて見直すことが大切です。

対策のポイント

1. 情報セキュリティポリシーや管理規程が策定されているか
2. ひな形、サンプルなどのコピーではなく、組織内での十分な討議や検討を経て、自組織の事業やリスクに見合った内容となっているか
3. ポリシーは全組織をカバーしているか
4. 組織の長ないし上級役員が承認しているか
5. 全従業者（派遣を含む）や関連する外部関係者に対して周知させているか
6. 定期的に見直すための手続を定めているか
7. あらかじめ定められた間隔、または重大な変化が発生した場合に、見直しを実施したか
8. 改訂結果について、組織の長ないし上級役員の承認を得て、再度周知したか
9. 従業員がポリシーや関連規程類を順守していることを点検・監査するための手続を定めているか
10. 組織内の情報セキュリティ対策や情報システムに関する点検や監査の実施を推進しているか
11. 情報システムが、業務以外の目的で利用されることを防止するための措置を講じているか
12. 情報システムに対し、いわゆるネットワーク検査やモニタリングを行うなどして、ポリシーの実施状況を確認しているか

②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。

説明 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、各部署の活動を調整する組織を整備すること、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、順守すべき法令などを正確かつ網羅的に把握することが必要です。さらに、組織の活動に関する説明責任を果たすため、種々の活動に関する記録を残すと共に、特に法令などによって保存が求められる文書については、記録を適切に保護することが求められます。

対策のポイント

1. 組織内の情報セキュリティのあり方を決定したり、各部署の活動を調整したりする組織が整備されているか
2. その組織の責任者は経営層の人間が担当しているか
3. その組織において、情報セキュリティに関する適切な責任や資源配分を検討しているか
4. 単独行動による不正行為をけん制するため、職務や権限を適切に分離しているか
5. 関係当局や情報セキュリティの専門家との連絡体制を構築しているか
6. 事業を遂行する上で順守すべき法令、基準、規制などを網羅的に、かつ正確に把握しているか
7. 他者の知的財産権を保護するための手続を定め、それを実践しているか（たとえば、ソフトウェアの不正コピーを予防するための手当てなど）
8. 個人情報を保護するために必要な対策を定め、それらを実施しているか
9. 不正競争防止法で保護される情報の要件を把握しているか
10. 自組織が実施した様々な活動について、それらを記録する仕組みはあるか
11. 特に法定の保存文書について、厳格な管理を実施しているか

③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

説明 情報セキュリティ対策を効率的に、かつ高いコスト効果をもって実施するためには、重要な情報資産をあらかじめ把握するとともに、その情報資産の重要度に応じて管理することが必要です。また、情報資産の管理責任者や利用できる人の範囲などを情報資産の重要度に応じて、あらかじめ定めておくことで、取扱がずさんになることを防ぎます。その際、管理すべき情報資産には、情報システムだけでなく情報そのものも含むこと、また情報は、電子媒体に限らず紙媒体などについても管理が必要であることに留意する必要があります。

対策のポイント

1. 重要な情報資産の目録を作成しているか
2. 情報資産の管理責任者を明確に定めているか
3. 情報の重要性に応じた分類及び取扱いの指針を定めているか
4. 情報システムから出力した情報についても、重要性のレベルや取扱いが明確になっているか
5. 分類及び取扱いの指針に従って情報を分類した上で、重要性のレベルに応じた表示と取扱いを行っているか
6. 情報資産を利用できる部署や人などの範囲を定めているか

④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、情報システムに依存するかを問いません。

説明 重要情報の入手、作成、利用、保管、交換、提供、消去、破棄などに当たっては、そうした一連の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が必要です。

対策のポイント

1. 各業務プロセスにおける作業責任者や作業手順を明確化し、その手順に基づいて作業を実施しているか
2. 各業務プロセスにおける作業を適切な担当者のみに限定し、その作業担当者の認証や権限付与の状況を確認しているか
3. 重要情報に対するアクセスの記録・保管、権限外作業の有無の確認など、対策の実施状況を把握しているか
4. 組織内外での情報の交換について、ルールと手順を定め、その手順に基づいて作業を行っているか
5. 重要な情報が消失、変更、誤用されないよう、操作ミスを考慮した運用方法を定めているか
6. 重要な情報について、漏えいや不正利用を防ぐために、保護対策を実施しているか

⑤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。

説明 外部の組織に業務を委託する際の契約書には、情報の漏えいや消失の防止、情報あるいは情報システムの誤用の防止を徹底するために、それらに関する条件を記載しておく必要があります。記載すべき条件には、委託先が実施すべき業務の内容、委託先が提供するサービスに関するサービスレベルの保証、委託先が委託業務に関して実施すべき安全管理措置などがあります。さらに、そうした契約条件に沿って適切に業務が遂行されていることを確認するため、報告や記録を求めることも大切です。

対策のポイント

1. 委託業務に際して締結する契約書に、業務内容、サービスレベル及び委託先に提供する重要な情報に関する安全管理措置や機密保持などの責任などを明確に定め記載しているか
2. 委託業務の確実な実施や委託先でのセキュリティ対策実施状況を報告や記録により確認しているか
3. 委託業務内容の変更について把握し、記録しているか

⑥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。

説明 すべての従業者に対して、採用や退職の際に、セキュリティ上の義務や、退職後の守秘義務など、セキュリティ上の順守事項を誓約させることで、注意義務を自覚させるとともに、就業規則や服務規律などに明示するなどして、情報セキュリティ対策に実効性を持たせます。さらに、退職や異動に際しては、貸与した資産の返却を確認すること、付与したアクセス権限を削除することも大切です。

対策のポイント

1. 従業者（派遣を含む）を採用する際に、経歴、資格などが職務にふさわしいかを十分に審査し、さらに守秘義務契約を締結しているか
2. 雇用契約時に、セキュリティ上の義務を明示しているか
3. 就業規則ないし服務規律に、従業員が順守すべき事項を明示しているか
4. 退職に際して、情報資産の返却確認やアクセス権限の削除を確実に行っているか
5. 退職に際して、退職後における守秘義務を退職予定の従業者に再確認しているか
6. セキュリティ違反を犯した従業員に対する懲戒手続を整備しているか
7. 採用から雇用、退職まで、従業員の管理を行う体制と責任が明確になっているか

⑦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。

説明 従業者に対する教育は、情報セキュリティ対策の有効性を向上させるために必要不可欠です。関係者全員に対する教育を適切に実施し、その効果が得られていることを確認することによって、技術的なセキュリティ対策との相乗効果を期待できます。特に、保護すべき情報資産へのアクセス管理を確実なものとするために、パスワードや鍵の管理の徹底はとても大切です。

対策のポイント

1. ポリシー及び関連規程を従業者（派遣を含む）が理解し、実践するために必要な教育を実施しているか
2. パスワードの管理や暗号鍵の管理について教育を行なっているか
3. 単に出来合いの教材だけでなく、自組織の状況に即した適切な教材を用意しているか
4. 教育は、定期的に、従業者全員に漏れなく実施しているか
5. 教育が有効であることを確認するための手立てを用意しているか

大項目2. 物理的（環境的）セキュリティ上の施策

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。

説明 重要な情報や関連する設備が数多く存在する場所については、セキュリティ対策として特段の配慮が必要となります。このような場所（建物や区画）については、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化したりすることが必要です。対策としては、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の確保、外来者の来訪履歴の保管も大切です。

対策のポイント

1. 特にセキュリティを強化したい物理的区域を定め、この区域の内外において順守すべきセキュリティ上の規程を整備しているか
2. 侵入を防止するために必要な建物や警報設備などの基準を設定しているか
3. 敷地及び建物に入ることができる人を制限しているか
4. その制限の対象になる人を識別できるようにしているか
5. 入退館（室）の履歴を記録し、その記録を適切に管理しているか
6. 訪問者や清掃業者などの立ち入りできる区域が明確になっているか

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。

説明 建物や事務所の中には、数多くの情報や関連する設備が所在しています。これらの情報や設備に触れる機会のある外来者に対しては、それぞれのリスクの状況を踏まえたルールの制定と、それに従った運用を行うことが必要です。

対策のポイント

1. 外部の人々の出入りによって、どのようなリスクが生じるかを検討し、その結果、明らかになったリスクについて適切な対策を実施したか
2. 外来者が建物内や室内で作業する場合、適切な管理の下で作業を行わせているか
3. 立ち入りを許した区域内で訪問者や清掃業者などへの応対を実施しているか
4. 顧客との打合せ場所や案内時の導線などにおいて、セキュリティ上の配慮を行っているか

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。

説明 重要な情報機器や配線については、偶然の事故による損壊や外部の者による盗み見や損壊を防ぐなど、安全上の配慮が必要です。偶然の事故に対しては、機器の転倒防止、漏水被害対策、周辺での飲食禁止、踏みつけや引っ張りによる断線の防止など、設備本体や周辺で起こりうる事故を洗い出し、それらに備えた対策を行うことが重要です。また、外部の者による盗み見や損壊に対しては、機器や配線などに、容易に接触できないようにすることが重要です。

対策のポイント

1. 基幹業務システムや機密情報を保有する情報システムを、許可された者だけが立ち入ることのできる安全な場所に設置しているか
2. 執務室の入口から見えないように情報処理設備を配置または設置しているか
3. 使用中に画面を盗み見されないように配置を工夫しているか
4. 不用意な損傷、傍受による盗聴などに配慮して、電源コードや通信ケーブルを配置しているか
5. 重要な情報システムについて、地震などによる転倒の防止、水漏れなどによる被害の予防、停電時の代替電源の確保などを実施しているか

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。

説明 書類や電子的な記憶媒体などによって情報が漏えいする事故が数多く発生しています。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、重要な情報が記録されている書類や記憶媒体を適切に管理することが必要です。また、重要な書類などが他の物品に紛れてしまう事によって不適切な取扱が起きないように、日ごろから、事務所や会議室の整理整頓に心がけることも大切です。

対策のポイント

1. 重要な書類、モバイルPC、記憶媒体などを適切に管理しているか
2. 重要な書類、モバイルPC、記憶媒体などは、物理的に破壊するなどしてから処分しているか
3. 重要なデータやライセンス付きのソフトウェアなどを格納した装置や記憶媒体を破棄する際は、中のデータを確実に消去しているか
4. 事務所内の机上、書庫、会議室などの整理整頓を実施しているか
5. 事務所、机、保管キャビネットなどの施錠管理を実施しているか
6. 郵便物、FAX、印刷物などの放置禁止や保護を実施しているか
7. 情報システムに関する情報も重要書類として取扱い、施錠保管などを実施しているか

大項目3. 情報システム及び通信ネットワークの運用管理

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。

説明 システム開発には、多数の作業者が関与するなど、大きなリスクが潜在しています。そのため、システム開発から本番運用への移行を踏まえ、十分な受け入れテストの実施、運用システムと開発システムの分離、運用システムの変更管理手順の策定、個人情報などの重要なデータを含む本番データの使用制限などの対策が重要となります。

対策のポイント

1. 情報システムの運用環境を開発環境やテスト環境から隔離しているか
2. 個人情報などの重要なデータを不用意にテストに用いないためのルールを定めているか
3. 運用環境の変更について規程を定めているか
4. 運用環境の変更を規程に沿って行うと共に、その過程や結果を記録しているか
5. 必要な場合、情報システムの性能や容量の管理を行っているか
6. 情報システムの受け入れについて、十分なテストを行っているか

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。

説明 情報システムや通信ネットワークの運用管理に必要な情報セキュリティ対策には、セキュリティの確保に必要な事項を含む各種手順書の作成、手順書などのルールに従った運用の実施とその監視、ログの取得と分析などが含まれます。また、運用システムを安定して稼動させるためには、情報システムの性能や容量を監視することも大切です。

対策のポイント

1. システム運用におけるセキュリティ要求事項を明確にしているか
2. 情報システムの運用手順書を整備しているか
3. 日々のシステム運用に不手際が生じないようにするための工夫をしているか
4. システムの運用状況を点検しているか
5. セキュリティ関連のイベントのログを取得しているか
6. 設備の使用状況を記録しているか
7. イベントログや設備の使用状況に関する記録を定期的に点検しているか
8. 不正行為の証拠を隠蔽するなどの目的で、システムログや各種の記録が、改ざんや消去などされないように配慮しているか
9. システム内のサーバや端末などの機器類について、常に時刻が同期するよう設定しているか

③不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウェアなど）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。

説明 不正プログラム対策には、ウイルス対策ソフトを導入し、パターンファイルの更新を適時行うことなどが含まれます。また、定期的なウイルス検査を実施し、万が一問題が生じた場合にとるべき処置を周知しておくことも大切です。

対策のポイント

1. ウイルス対策ソフトを適切に配置しているか
2. パターンファイルの更新を適切に行っているか
3. 各サーバやクライアントPCについて、定期的なウイルス検査を行っているか
4. 情報システムの利用者は、ウイルス対策や問題が生じた場合における必要な処置について十分に認識しているか
5. 外部で使用したモバイルPCを内部ネットワークに接続する前に、ウイルス駆除などの（検疫）処理を行っているか
6. 不正プログラムによる攻撃などに悪用されないよう、ぜい弱性の解消（修正プログラムの適用）を行っているか

④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。

説明 適切なぜい弱性対策には、ぜい弱性情報や脅威情報の定期的な入手、不要なサービスの停止といったセキュリティを考慮した設定、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、変更管理などを含みます。

対策のポイント

1. ぜい弱性情報や脅威情報を定期的に収集しているか
2. ぜい弱性や脅威に大きな変化があった場合には、リスクを改めて評価し、ソフトウェアへのパッチ（修正プログラム）適用などの必要な措置を実施しているか
3. パッチについてテスト・適用が適切になされているか
4. 情報システムの導入に際して、不要なサービスを停止するなど、セキュリティを考慮した設定を実施しているか
5. Webサイトの公開にあたっては、不正アクセスや改ざんなどを受けないよう、適切な設定やぜい弱性の解消を行っているか

⑤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。

説明 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。また、重要な情報を電子メールでやりとりする場合には、情報を暗号化しておくことも効果的です。

対策のポイント

1. 外部のネットワークから内部のネットワークや情報システムへアクセスする場合に、VPNなどを用いて暗号化した通信路を使用しているか
2. Webにアクセスする際、必要に応じ、SSLなどを用いて通信データを暗号化しているか
3. 電子メールをやり取りする場合に、重要な情報を暗号化しているか

⑥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。

説明 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。外部では、内部での利用に比べて盗難や紛失のリスクが高いことを考慮し、外部持ち出しに関する規程を定めたり、強固な認証や暗号化などの対策を検討したりします。

対策のポイント

1. モバイルPCやUSBメモリ、CDなどの使用や記憶媒体の外部持ち出しについて、規程を定めているか
2. 外部でモバイルPCやUSBメモリ、CDなどの記憶媒体を使用する場合の紛失や盗難対策を講じているか
3. モバイルPCにログオンする際に、利用者IDとパスワードなどによる認証を実施しているか
4. モバイルPCなどに保存されているデータを、その重要度に応じて暗号化しているか

大項目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

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。

説明 適切な利用者IDの管理には、利用者IDに関する規程の整備、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、本来必要ではない特権を設定したIDの発見と見直し、見破られやすい単純なパスワードの設定禁止などがあります。

対策のポイント

1. 利用者IDの登録や削除に関する規程を整備し、利用者のIDを定期的に見直しているか
2. 不要になった利用者IDの無効設定漏れがないか、IDの不正利用がないかなどを定期的に点検しているか
3. 空白のパスワードや単純な文字列のパスワードを設定しないよう、利用者に求めているか
4. 利用者ごとにIDとパスワードを割当て、そのIDとパスワードによる識別と認証を確実に実施しているか

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。

説明 適切なアクセス権の管理には、あらかじめ方針を定めておき、その方針に基づいて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。

対策のポイント

1. アクセスを管理する方針を定め、利用者ごとにアクセス可能な情報（データ）、情報システム、業務アプリケーション、サービスなどを適切に設定しているか
2. 適切な権限付与が行われているか、必要以上の権限付与がないかなど、利用者に与えたアクセス権を定期的にレビューしているか
3. 特に重要な情報を格納した情報システムについては、一度のアクセスでの利用時間の制限などのアクセス条件による制御を行っているか

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。

説明 ネットワークへの接続に伴って、接続したネットワーク経由で侵入されるといったリスクが増大します。そのようなリスクを低減するためには、ネットワークへの適切なアクセス制御が不可欠です。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。

対策のポイント

1. 外部のネットワークから内部のシステムへアクセスする際（モバイルPCを使用する場合を含む）に、利用者認証を実施しているか
2. サービスや情報システムにアクセス可能な利用者を制限するために、ネットワークを論理的に切り離したり、接続を制限したりしているか
3. 許可されていないワイヤレスアクセスポイントの設置を禁止しているか
4. 外部の無線LANを利用してネットワークにアクセスする場合に、セキュリティ対策を実施しているか
5. 内部のネットワークに接続する端末機器について、接続時に認証しているか

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。

説明 業務システムは、完成してしまった後に改変を加えることは困難で、コストも嵩みます。企画、設計などの初期の段階から情報セキュリティについて配慮することが必要です。そのためには、自組織での開発、外部委託による開発を問わず、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重要です。

対策のポイント

1. セキュリティ上の要求事項を仕様書に盛り込んでいるか
2. 入力データに対するチェック機能を適切に実装しているか
3. 業務処理プロセスを適切に実装しているか
4. 情報の保護機能を適切に実装しているか
5. 出力データの妥当性や表示メッセージの正しさなどに関するチェックを適切に行っているか
6. ぜい弱性を作り込まないために、プログラミング上の配慮がなされているか

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

説明 ソフトウェアにセキュリティ上の問題を混入させないための管理が重要です。たとえば、選定や購入に際しては、ソフトウェアの開発元を確認すること、開発や保守に際しては、ソースコードへのアクセス管理といったセキュリティ対策の実施状況の記録やレビューの記録などを確認できることが大切です。

対策のポイント

1. 運用に供しようとする情報システムのソフトウェアの導入や変更に関する手順を整備しているか
2. ソースコードへのアクセスを制限しているか
3. 構成の変更に関する手順を整備し、厳重に管理しているか
4. トロイの木馬などの不正プログラムが組み込まれていないかどうかをチェックしているか
5. 外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めているか
6. 外部委託によるソフトウェア開発を行う場合、品質や作業範囲、標準となる契約書や合意書を用意しているか
7. 開発や保守を外部委託する場合に、セキュリティ管理の実施状況を把握できるか

大項目5. 情報セキュリティ上の事故対応状況

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。

説明 情報セキュリティの重要な要素の一つである可用性に影響を与える事象のうち、影響の度合いが最も大きいのは、情報システム関連機器の障害であると言っても過言ではありません。情報システムに求められる可用性の条件を満たすためには、可用性に関する要求に対応した適切な障害対策機能の情報システムへの組込みが欠かせません。

対策のポイント

1. 情報システムの可用性に関する要求は明確で妥当なものか（可用性とは、情報システムを使う権限のある人がいつでも使えるようにすることをいいます）
2. 障害対策の実行に必要なバックアップ情報の取得や、運用記録などの確保を適切に行っているか
3. 障害部分の切り離し、縮退運転、情報の回復や情報システムの復旧など、障害発生時に必要となる機能を情報システムに組み込んでおり、それらが適切に機能することを検証しているか（縮退運転とは、提供する機能やサービスの対象者の絞り込みなどにより、障害時でも、必要最低限のサービスを提供できるようにすることを言います）
4. 障害発生時の対応手順や、障害対策処理の実施要領を策定しているか
5. 障害対応のスキルに関する教育や訓練を実施しているか
6. 情報システムの運用を外部に委託している場合、障害発生時にも所定のサービスレベルが維持されることを、委託先との間で相互に確認しているか
7. システムの各種ログを取得できているか

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。

説明 情報セキュリティに関連する事件や事故が発生した場合に、被害の拡大を防ぎ、局所化するためには、事件や事故に必要な対応を組織全体で適切かつ迅速に実施できなければなりません。そのためには、事件や事故を想定し、実施すべき作業やその実施要領を確立するとともに、現場の要員がいざというときに対応作業を円滑に実行できるように準備しておくことが必要となります。また、個人情報などの漏えいが発生した場合に、影響を受ける可能性のある本人への連絡、主務大臣などへの報告、事実関係や再発防止策の公表などを円滑に進めるため、手順などを整備しておくことも重要です。

対策のポイント

1. セキュリティにかかわる出来事、事件や事故の発生時の対応について、実施要領を定めているか
2. セキュリティにかかわる出来事、事件や事故に関する対応要領を関係者に徹底しているか
3. セキュリティにかかわる出来事、事件や事故の発生時の連絡網を含む対応体制を構築しているか
4. セキュリティにかかわる出来事、事件や事故への対応に必要なリソースやツールを適切に準備しているか（ここでのリソースやツールとは、障害対応要員、障害を記録するためのディスク領域、障害報告機能や分析機能などを指します）

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。

説明 地震、台風、水害などの自然災害による施設、システム機器、業務アプリケーション、業務データの損壊や、そのほか情報システムに生じた重大事故によって、情報システムが停止し、短期間での復旧の目処がたたなくなるような事態の発生が考えられます。このような状況においても事業の継続ができるようにするためには、情報システム全体をカバーするバックアップセンターの準備や、ソフトウェア資産や業務データのバックアップとその安全な保管、さらには手作業により業務の遂行ができるようにしておくなどの準備が必要となります。事業活動の多くを情報システムに依存している組織においては、事業継続への取組は十分に検討しておくべきです。

対策のポイント

1. 情報システムが停止した場合に、自組織の業務に及ぼす影響について検討した事があるか
2. 各業務の重要度や、業務システムのトラブルがそうした業務に及ぼす影響について把握しているか
3. 情報システムの停止が長期になる場合に備え、業務を継続するための方針やシナリオを策定しているか
4. 情報システムの長期停止時に必要となる、バックアップセンターへの切り替えや業務の手作業への切り替えなどは、何時でも実施できるよう、手順の策定や関係者への周知と訓練を実施しているか
5. 外部への連絡など、情報システムが長期停止に陥った場合に必要となるその他の措置についても検討し、実施要領を策定しているか

注：各項目の解説については、「情報セキュリティ対策ベンチマーク（改訂版）」に記載されています。この資料は、以下のURLよりダウンロードすることができます。

http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

資料2 JIS Q 27002：2006 箇条、セキュリティカテゴリ、管理策（タイトル）一覧

注：JIS Q 27001:2006 付属書Aの管理目的及び管理策はJIS Q 27002:2006の箇条5-15までに掲げられているものをそのまま取り入れて配列したものです。

箇条/セキュリティカテゴリ	管理策（タイトル）
5. セキュリティ基本方針	
5.1 情報セキュリティ基本方針	5.1.1 情報セキュリティ基本方針文書 5.1.2 情報セキュリティ基本方針のレビュー
6. 情報セキュリティのための組織	
6.1 内部組織	6.1.1 情報セキュリティに対する経営陣の責任 6.1.2 情報セキュリティの調整 6.1.3 情報セキュリティ責任の割当て 6.1.4 情報処理設備の認可プロセス 6.1.5 秘密保持契約 6.1.6 関係当局との連絡 6.1.7 専門組織との連絡 6.1.8 情報セキュリティの独立したレビュー
6.2 外部組織	6.2.1 外部組織に関係したリスクの識別 6.2.2 顧客対応におけるセキュリティ 6.2.3 第三者との契約におけるセキュリティ
7. 資産の管理	
7.1 資産に対する責任	7.1.1 資産目録 7.1.2 資産の管理責任者 7.1.3 資産利用の許容範囲
7.2 情報の分類	7.2.1 分類の指針 7.2.2 情報のラベル付け及び取扱い
8. 人的資源のセキュリティ	
8.1 雇用前	8.1.1 役割及び責任 8.1.2 選考 8.1.3 雇用条件
8.2 雇用期間中	8.2.1 経営陣の責任 8.2.2 情報セキュリティの意識向上,教育及び訓練 8.2.3 懲戒手続
8.3 雇用の終了又は変更	8.3.1 雇用の終了又は変更に関する責任 8.3.2 資産の返却 8.3.3 アクセス権の削除
9. 物理的及び環境的セキュリティ	
9.1 セキュリティを保つべき領域	9.1.1 物理的セキュリティ境界 9.1.2 物理的入退管理策 9.1.3 オフィス、部屋及び施設のセキュリティ 9.1.4 外部及び環境の脅威からの保護 9.1.5 セキュリティを保つべき領域での作業 9.1.6 一般の人の立寄り場所及び受渡場所
9.2 装置のセキュリティ	9.2.1 装置の設置及び保護 9.2.2 サポートユーティリティ 9.2.3 ケーブル配線のセキュリティ 9.2.4 装置の保守 9.2.5 構外にある装置のセキュリティ 9.2.6 装置の安全な処分又は再利用 9.2.7 資産の移動
10. 通信及び運用管理	
10.1 運用の手順及び責任	10.1.1 操作手順書 10.1.2 変更管理 10.1.3 職務の分割 10.1.4 開発施設、試験施設及び運用施設の分離
10.2 第三者が提供するサービスの管理	10.2.1 第三者が提供するサービス 10.2.2 第三者が提供するサービスの監視及びレビュー 10.2.3 第三者が提供するサービスの変更に対する管理
10.3 システムの計画作成及び受入れ	10.3.1 容量・能力の管理 10.3.2 システムの受入れ
10.4 悪意のあるコード及びモバイルコードからの保護	10.4.1 悪意のあるコードに対する管理策 10.4.2 モバイルコードに対する管理策
10.5 バックアップ	10.5.1 情報のバックアップ
10.6 ネットワークセキュリティ管理	10.6.1 ネットワーク管理策 10.6.2 ネットワークサービスのセキュリティ
10.7 媒体の取扱い	10.7.1 取外し可能な媒体の管理 10.7.2 媒体の処分 10.7.3 情報の取扱手順 10.7.4 システム文書のセキュリティ
10.8 情報の交換	10.8.1 情報交換の方針及び手順 10.8.2 情報交換に関する合意 10.8.3 配送中の物理的媒体 10.8.4 電子的メッセージ通信 10.8.5 業務用情報システム

10.9　電子商取引サービス	10.9.1　電子商取引 10.9.2　オンライン取引 10.9.3　公開情報
10.10　監視	10.10.1　監査ログ取得 10.10.2　システム使用状況の監視 10.10.3　ログ情報の保護 10.10.4　実務管理者及び運用担当者の作業ログ 10.10.5　障害のログ取得 10.10.6　クロックの同期
11．アクセス制御	
11.1　アクセス制御に対する業務上の要求事項	11.1.1　アクセス制御方針
11.2　利用者アクセスの管理	11.2.1　利用者登録 11.2.2　特権管理 11.2.3　利用者パスワードの管理 11.2.4　利用者アクセス権のレビュー
11.3　利用者の責任	11.3.1　パスワードの利用 11.3.2　無人状態にある利用者装置 11.3.3　クリアデスク・クリアスクリーン方針
11.4　ネットワークのアクセス制御	11.4.1　ネットワークサービスの利用についての方針 11.4.2　外部から接続する利用者の認証 11.4.3　ネットワークにおける装置の識別 11.4.4　遠隔診断用及び環境設定用ポートの保護 11.4.5　ネットワークの領域分割 11.4.6　ネットワークの接続制御 11.4.7　ネットワークルーティング制御
11.5　オペレーティングシステムのアクセス制御	11.5.1　セキュリティに配慮したログオン手順 11.5.2　利用者の識別及び認証 11.5.3　パスワード管理システム 11.5.4　システムユーティリティの使用 11.5.5　セッションのタイムアウト 11.5.6　接続時間の制限
11.6　業務用ソフトウェア及び情報のアクセス制御	11.6.1　情報へのアクセス制限 11.6.2　取扱いに慎重を要するシステムの隔離
11.7　モバイルコンピューティング及びテレワーキング	11.7.1　モバイルのコンピューティング及び通信 11.7.2　テレワーキング
12．情報システムの取得、開発及び保守	
12.1　情報システムのセキュリティ要求事項	12.1.1　セキュリティ要求事項の分析及び仕様化
12.2　業務用ソフトウェアでの正確な処理	12.2.1　入力データの妥当性確認 12.2.2　内部処理の管理 12.2.3　メッセージの完全性 12.2.4　出力データの妥当性確認
12.3　暗号による管理策	12.3.1　暗号による管理策の利用方針 12.3.2　かぎ（鍵）管理
12.4　システムファイルのセキュリティ	12.4.1　運用ソフトウェアの管理 12.4.2　システム試験データの保護 12.4.3　プログラムソースコードへのアクセス制御
12.5　開発及びサポートプロセスにおけるセキュリティ	12.5.1　変更管理手順 12.5.2　オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー 12.5.3　パッケージソフトウェアの変更に対する制限 12.5.4　情報の漏えい 12.5.5　外部委託によるソフトウェア開発
12.6　技術的ぜい弱性の管理	12.6.1　技術的ぜい弱性の管理
13．情報セキュリティインシデントの管理	
13.1　情報セキュリティの事象及び弱点の報告	13.1.1　情報セキュリティ事象の報告 13.1.2　セキュリティ弱点の報告
13.2　情報セキュリティインシデントの管理及びその改善	13.2.1　責任及び手順 13.2.2　情報セキュリティインシデントからの学習 13.2.3　証拠の収集
14．事業継続管理	
14.1　事業継続管理における情報セキュリティの側面	14.1.1　事業継続管理手続への情報セキュリティの組込み 14.1.2　事業継続及びリスクアセスメント 14.1.3　情報セキュリティを組み込んだ事業継続計画の策定及び実施 14.1.4　事業継続計画策定の枠組み 14.1.5　事業継続計画の試験、維持及び再評価
15．順守	
15.1　法的要求事項の順守	15.1.1　適用法令の識別 15.1.2　知的財産権（IPR） 15.1.3　組織の記録の保護 15.1.4　個人データ及び個人情報の保護 15.1.5　情報処理施設の不正使用防止 15.1.6　暗号化機能に対する規制
15.2　セキュリティ方針及び標準の順守、並びに技術的順守	15.2.1　セキュリティ方針及び標準の順守 15.2.2　技術的順守の点検
15.3　情報システムの監査に対する考慮事項	15.3.1　情報システムの監査に対する管理策 15.3.2　情報システムの監査ツールの保護

内容に関するお問合せ先

■情報セキュリティ対策ベンチマーク

独立行政法人 情報処理推進機構　セキュリティセンター

〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス16階
TEL：03-5978-7508　　FAX：03-5978-7518
e-mail：isec-info@ipa.go.jp
URL：http://www.ipa.go.jp/security/benchmark/

■ISMS適合性評価制度

財団法人 日本情報処理開発協会
情報マネジメント推進センター ISMS制度推進室

〒105-0011　東京都港区芝公園3-5-8　機械振興会館3階
TEL：03-3432-9386　　FAX：03-3432-6200
e-mail：it-info@tower.jipdec.or.jp
URL：http://www.isms.jipdec.jp/

■情報セキュリティ監査

特定非営利活動法人 日本セキュリティ監査協会　事務局

〒103-0025 東京都中央区日本橋茅場町2-8-4 全国中小企業会館5階
TEL：03-5640-7060　　FAX：03-5640-0666
e-mail：office@jasa.jp
URL：http://www.jasa.jp

■情報セキュリティガバナンス等の情報セキュリティ政策について

経済産業省　商務情報政策局　情報セキュリティ政策室

〒100-8901 東京都千代田区霞ヶ関1-3-1
TEL：03-3501-0397　　FAX：03-3501-6639
e-mail：it-security@meti.go.jp
URL：http://www.meti.go.jp/policy/netsecurity/

情報セキュリティ対策ベンチマーク普及検討会　名簿

【座長】	大木　栄二郎	工学院大学情報学部　教授
【構成員】	山田　安秀	独立行政法人 情報処理推進機構 セキュリティセンター長
	石井　　茂	独立行政法人 情報処理推進機構 セキュリティセンター　普及グループリーダー
	菅野　泰子	独立行政法人 情報処理推進機構 セキュリティセンター　調査役
	高取　敏夫	財団法人 日本情報処理開発協会 情報マネジメント推進センター　SMS制度推進室　室長
	星　　昌宏	財団法人 日本情報処理開発協会 情報マネジメント推進センター　審査グループリーダー
	下村　正洋	特定非営利活動法人 日本セキュリティ監査協会 理事・事務局長
	沓澤　　徹	特定非営利活動法人 日本セキュリティ監査協会 事務局次長
	永宮　直史	特定非営利活動法人 日本セキュリティ監査協会 保証型監査促進プロジェクト・コアメンバー 資格認定委員会委員、資格維持プログラム小委員会委員長
【オブザーバ】	清水　友晴	経済産業省　商務情報政策局 情報セキュリティ政策室　課長補佐
	和田　浩明	経済産業省　商務情報政策局 情報セキュリティ政策室
	井口　新一	財団法人 日本適合性認定協会　専務理事
	本山　佳奈	財団法人 日本適合性認定協会　認定審査員
	川口　修司	株式会社 三菱総合研究所 情報セキュリティ研究グループ　主席研究員
【事務局】	独立行政法人 情報処理推進機構	

情報セキュリティ対策ベンチマーク普及検討会 作業部会 名簿

【構成員】	菅野　泰子	独立行政法人 情報処理推進機構 セキュリティセンター　調査役
	高取　敏夫	財団法人 日本情報処理開発協会 情報マネジメント推進センター　ISMS制度推進室　室長
	星　　昌宏	財団法人 日本情報処理開発協会 情報マネジメント推進センター　審査グループリーダー
	沓澤　　徹	特定非営利活動法人 日本セキュリティ監査協会 事務局次長
	永宮　直史	特定非営利活動法人 日本セキュリティ監査協会 保証型監査促進プロジェクト・コアメンバー 資格認定委員会委員、資格維持プログラム小委員会委員長
	高橋　さぎり	特定非営利活動法人 日本セキュリティ監査協会 事務局
【オブザーバ】	清水　友晴	経済産業省　商務情報政策局 情報セキュリティ政策室　課長補佐
	本山　佳奈	財団法人日本適合性認定協会　認定審査員
	川口　修司	株式会社 三菱総合研究所 情報セキュリティ研究グループ　主席研究員

注：構成員、オブザーバの記載は、組織名のあいうえお順に記載しています。

—本書の無断複製・転載を禁じます—

情報セキュリティ対策ベンチマーク活用集

2008年1月　初版　第1刷発行
2008年3月　第2版　第1刷発行
2008年9月　第3版　第1刷発行

著作編者　独立行政法人 情報処理推進機構
財団法人 日本情報処理開発協会
特定非営利活動法人 日本セキュリティ監査協会

連絡先　独立行政法人 情報処理推進機構
セキュリティセンター
TEL：03-5978-7508　E-mail：isec-info@ipa.go.jp

Copyright ©2008 IPA/JIPDEC/JASA All Rights Reserved.

http://www.ipa.go.jp/security/benchmark/

R70
古紙パルプ配合率70％再生紙を使用
PRINTED WITH SOY INK