

ISMS

情報セキュリティマネジメントシステム適合性評価制度

ISMS 認証基準 (Ver. 0.8)

平成 13 年 4 月 1 日

財団法人 日本情報処理開発協会

本文書（ISMS 認証基準）は、情報セキュリティマネジメントシステム適合性評価制度において、第三者である指定審査機関が本制度の認証を希望する事業者の適合性を評価するための認証基準である。本基準は、国際規格 ISO/IEC 17799:2000（Information technology -- Code of practice for information security management: 情報技術 - 情報セキュリティマネジメント実施基準）及び英国規格 BS 7799-2:1999 (Specification for information security management systems: 情報セキュリティマネジメントシステム仕様)を参照し作成したものである。

また本基準は、時代に適合したものであり続けるために、情報セキュリティに関する国際標準の JIS 化の動向や JIS 化後の周知状況等を踏まえ、適宜見直し及び改訂されるものである。

（財）日本情報処理開発協会

第1 適用範囲

本基準は、情報セキュリティマネジメントシステム（以下、「ISMS」という）の確立、実施及び文書化についての要求事項を明記する。

第2 用語及び定義

(1) 情報セキュリティ

情報の機密性、完全性及び可用性を確保し維持すること。

(2) リスク評価

情報や情報処理施設等に対する脅威及びその脅威への脆弱性を分析し、その結果からリスクが顕在化する可能性及び顕在化した場合の事業への影響度を検証すること。

(3) 適用宣言書

組織の必要性に基づいて適用される管理目的及び管理策を詳述した文書。

第3 ISMS の要求事項

(1) 一般

組織固有の ISMS を確立し維持するため、以下の項目について文書化すること。

(ア) 保護すべき情報資産

(イ) リスクマネジメントに対する組織の取組方法

(ウ) 管理目的及び管理策の内容

(エ) 保護すべき情報資産に要求される保証の度合い

(2) マネジメント枠組みの確立

管理目的及び管理策の内容を明確にすること。

の目的及び内容を文書化するために以下の作業を実施すること。

(ア) 情報セキュリティポリシーの策定

(イ) ISMS の対象範囲の決定

(ウ) リスク評価

(エ) リスクマネジメントの対象範囲の決定

(オ) 管理策の選択

(カ) 適用宣言書の作成

の各項目について、定期的もしくは必要に応じて見直しすること。

(3) 管理策の実施

選択された管理策を講ずること。

管理策を講ずるために採用された手続きについて、第 4 10(2) に従いその有効性を確認すること。

(4) 文書化

ISMS 文書に以下の内容が含まれていること。

- (ア) 第 3(2) の作業の証拠
- (イ) 情報セキュリティポリシー及び適用宣言書に記述された管理目的及び管理策の内容を含んだマネジメント枠組みの要約
- (ウ) 第 3(3) の管理策を講ずるために採用された手続き及びその実施責任と関連する作業内容
- (エ) ISMS を運用するための手続きとそれらの実施責任及び関連する作業内容

(5) 文書管理

第 3(4) の ISMS 文書を管理するため、以下の条件を満たす手続きを確立し維持すること

- (ア) ISMS 文書の利用者が文書を容易に利用することができる
- (イ) ISMS 文書の定期的な見直しを行い、情報セキュリティポリシーに対する準拠性を維持しながら必要に応じて改訂する
- (ウ) ISMS 文書の更新履歴を管理する
- (エ) ISMS を運用するために必要なすべての事業所等において ISMS 文書が閲覧可能である
- (オ) ISMS 文書の一部について、その必要性がなくなったり、別途新たな文書が作成された場合に、当該 ISMS 文書が速やかに廃止される
- (カ) (オ) の廃止にかかわらず、法規制等による要請がある場合や専門知識を蓄積するために、必要に応じて ISMS 文書が保管される

ISMS 文書には、策定や改訂の日付が明記されること。

ISMS 文書は、ISMS 文書であることを容易に識別でき、また整頓された状態で維持されること。

ISMS 文書は、指定された期間に亘り保管されること。

ISMS 文書を作成及び修正するための責任体制及び手続きを確立し維持すること。

(6) 記録

第 3 (1)から(5) の内容に対する遵守状況を保証するために必要な記録を特定すること

において特定された記録を管理する手続きを明確にし必要に応じて見直すこと。

において特定された記録に対し、損傷、劣化、紛失、消失を防止するための措置を講ずること。

第 4 詳細管理策

1. セキュリティポリシー

(1) 情報セキュリティポリシー

情報セキュリティポリシーは、経営陣により承認および制定されること。

情報セキュリティポリシーは、必要な関係者全員に公表されること。

情報セキュリティポリシーは、定期的に見直され、必要に応じて変更された場合には変

更内容の妥当性が確認されること。

2. セキュリティ組織

(1) 情報セキュリティ・インフラストラクチャ

経営陣が情報セキュリティについて討論する委員会等を設置すること。

組織内の情報セキュリティを管理するため、関連する部門を横断的に調整する部門等を設けること。

個々の情報資産に対する保護責任及び特定の業務に関する実施責任を明確にすること。

情報処理施設及び設備の新規導入に対する経営陣による承認の手順を確立すること。

情報セキュリティに関して、適宜社内または社外の専門家から助言を受け、その内容を組織内に公表すること。

監督官庁、規制当局及びセキュリティ上重要な役割を担う外部組織への連絡体制を維持すること。

情報セキュリティポリシーの導入や運用の状況を客観的視点で見直すこと。

(2) 第三者アクセスのセキュリティ

第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、事前にリスク評価を行い必要な措置を講ずること。

第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、セキュリティ要求事項を明記した正式な契約を締結すること。

情報システムの管理や制御を外部委託する場合、セキュリティ要求事項を明記した正式な契約を締結すること。

3. 情報資産の分類及び管理

(1) 情報資産に対する責任

情報資産を適切に管理するため資産台帳を作成し、重要な情報資産のすべてを登録すること。

(2) 情報の分類

事業における必要性や問題が生じた場合の影響度に応じた情報資産の分類基準を設けること。

情報資産を分類基準に従い分類し、その取扱いに関する手続きを明確にすること。

4. 人的セキュリティ

(1) 職務定義および採用におけるセキュリティ

情報セキュリティポリシーに定義された情報セキュリティに関する役割及び責任を職務定義書に明記すること。

採用する人員に求める資質や職能を明確にすること。

人員の採用条件の一部として、被雇用者から機密保持合意書への署名を得ること。

人員を採用する際、被雇用者に対し情報セキュリティに関する役割及び責任を明示すること。

(2) ユーザの教育・訓練

情報セキュリティポリシーの対象者に対し、情報セキュリティポリシー及び関連する実施手順等に関する教育・訓練を定期的実施すること。

(3) セキュリティ事故及び誤動作への対処

発見したセキュリティ事故を迅速に報告するため、経営陣を含めた連絡網を設置すること。

セキュリティ事故やそれに準ずる出来事を発見した場合の報告義務を、その義務を有する者に対し周知徹底すること。

ソフトウェアが誤動作した場合の報告手順を明確にすること。

事故や誤動作等の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にし、組織の情報セキュリティを監視すること。

情報セキュリティポリシー及び関連する手続きに違反した場合の正式な懲戒手続き手続きを確立すること。

5. 物理的及び環境的セキュリティ

(1) セキュリティ区画

情報処理施設及び設備は、他の区画と明確に分離したセキュリティ区画に設置され、適切に保護されること。

セキュリティ区画は、許可されない者がアクセスできないよう入退管理されること。

セキュリティ区画は、特別な管理を要求される作業場所や施設を保護する目的で建設されること。

セキュリティ区画において作業をするための管理策及びガイドラインを整備すること。

納品及び積荷場所は、許可されないアクセスを避けるため管理され、情報処理施設及び設備から分離されること。

(2) 装置のセキュリティ

装置の設置場所における環境上の脅威を軽減するための措置を講ずること。

装置を許可されないアクセスから保護すること。

装置を停電やその他の電源異常から保護すること。

データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。

装置を使用する際、装置製造業者が提供する取扱い説明書や手順書に従い、装置の可用性及び完全性を確実に維持すること。

組織の敷地外で利用される装置を適切に保護するための手続きを明確にし、必要な管理策を講ずること。

装置を処分あるいは再利用する際、装置に格納された情報を事前に消去すること。

(3) 一般管理策

離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。

離席時や帰宅時には、パスワードで保護されたスクリーンセーバの使用やログオフを徹

底し、他人による情報システムへのアクセスを防止すること。

組織が所有する装置や情報、ソフトウェア等の組織外への持ち出しに関する手続きを確立すること。

6. 通信及び運用管理

(1) 運用手順及び責任

情報セキュリティポリシーにより特定された操作手順を文書化し維持すること。

情報システムや情報処理施設等に対する変更を管理すること。

セキュリティ事故を管理する責任体制及び手続きを明確にすること。

情報や情報サービスへの許可されない変更や誤用の機会を低減するため、職務の分離及び責任の範囲を明確にすること。

情報システムの開発及びテストの環境を運用施設及び設備から分離すること。

外部の施設管理サービスを利用する場合、事前にリスク評価を行い適切な管理策を決定した上で、この内容を明記した正式な契約を締結すること。

(2) システム計画の作成及び受け入れ

情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。

情報システムを新規導入あるいは変更する際の受け入れ基準を確立し、情報システムの本番利用を容認する前に適切なテストを実施すること。

(3) 不正ソフトウェアからの保護

情報や情報システムを不正ソフトウェアから保護するための検出及び防止策を講じ、適宜ユーザの教育・訓練を実施すること。

(4) 情報システムの管理

重要な情報及びソフトウェアのバックアップコピーを定期的を取得すること。

情報システムの操作担当者の作業履歴を記録すること。

障害が報告された情報システムを確実に修正すること。

(5) ネットワークの管理

ネットワークにおけるセキュリティを確保し維持するための管理策を講ずること。

(6) 媒体の取り扱い及びセキュリティ

テープ、ディスク、カセット等の移動可能な記憶媒体や書類等を取り扱う際の手続きを確立すること。

不要になった媒体を処分する際、情報漏洩を防止するための措置を講じること。

情報の取扱い及び保管に関する手続きを確立すること。

情報システムに関するドキュメントを許可されないアクセスから保護すること。

(7) 組織間における情報及びソフトウェアの交換

取引先や協業相手等と情報を交換する場合、必要に応じて情報交換の実施に関する正式な契約を締結すること。

移送中の媒体を許可されないアクセス、誤用及び改ざんから保護すること。

電子取引を行う場合、詐欺行為、契約紛争、不正な情報開示及び情報の改ざんを防止するための措置を講ずること。

電子メールの使用に関するポリシーを定め、電子メールの使用により発生しうるリスクを軽減するための管理策を講ずること。

電子機器の使用に関するポリシー及びガイドラインを定め、電子機器の使用に関連したリスクを抑制すること。

組織の情報を一般に公開し利用可能にする場合の正式な許可手続きを確立すること。

組織の情報を一般に公開し利用可能にする場合、その情報を許可されない変更から保護すること。

電話やファクシミリ、ビデオ通信等を使用して情報を交換する場合、その手続きを明確にすること。

7. アクセス制御

(1) アクセス制御に関する事業の要求事項

情報へのアクセス制御に関する事業の要求事項を明確に定義したアクセス制御ポリシーを策定すること。

情報へのアクセスは、アクセス制御ポリシーに従い制限されること。

(2) ユーザアクセス管理

情報システムユーザの登録及び登録抹消手順を確立すること。

特権の割当て及び使用を制限し管理すること。

情報システムユーザに対するパスワードの割当てを管理する手続きを確立すること。

情報システムユーザのアクセス権を定期的に見直すこと。

(3) ユーザの責任

パスワードを設定及び使用する際、情報セキュリティ上の問題を考慮すること。

装置を常時監視することが不可能な場合、当該装置を適切に保護するための措置を講ずること。

(4) ネットワークのアクセス制御

明確に許可されたサービス以外のサービスへのアクセスを防止するための措置を講ずること。

情報システムのユーザがコンピュータの各サービスにアクセスする場合のネットワークの経路を制御すること。

情報システムに対する遠隔地からのアクセスを許可する場合、ユーザ認証を行うこと。

遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。

診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。

情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。

共有ネットワークへのアクセス権限は、第 4 7(1)のアクセス制御ポリシーに従い付与されること。

共有ネットワークへのアクセスを許可する場合、第 4 7(1) のアクセス制御ポリシーに基づき、可能な限り経路を制御すること。

ネットワークに関連する外部のサービスを受ける場合、そのサービスに施されたセキュリティに関する情報を入手し、これを文書化すること。

(5) オペレーティングシステムのアクセス制御

接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。

情報サービスにログオンするための手続きを明確にすること。

情報システムユーザは、個人専用の識別子（ユーザ ID）を有すること。

パスワード管理システムは、情報システムユーザに有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を制限すること。

システム設定プログラムの使用を制限し管理すること。

脅迫される可能性のあるユーザがいる場合、脅迫されているという事実をユーザが自ら発信する警報機能を備えること。

取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末をシャットダウンすること。

リスクの高いアプリケーションシステムへの接続時間は、制限されること。

(6) アプリケーションシステムのアクセス制御

情報及びアプリケーションシステムへのアクセスは、第 4 7(1) のアクセス制御ポリシーに従い制限されること。

取扱いに慎重を要する情報システムは、隔離された環境に設置されること。

(7) システムアクセス及びシステム使用の監視

例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。

情報処理施設及び設備の使用を監視する手続きを確立すること。

情報処理施設及び設備の監視活動の結果を定期的に検証すること。

すべての重要なコンピュータにおいて時刻設定を同期化すること。

(8) モバイルコンピューティング及び遠隔地勤務

モバイルコンピュータを用いる場合、事前にリスク評価を行い、モバイルコンピュータ使用ポリシーを定義した上で必要な管理策を講ずること。

遠隔地勤務を許可する場合、事前にリスク評価を行い、遠隔地勤務ポリシー及び手順書を定義すること。

8. システムの開発及びメンテナンス

(1) システムのセキュリティ要求事項

情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要求事項を明確にすること。

(2) アプリケーションシステムのセキュリティ

アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能や手続きを整備すること。

アプリケーションシステムで処理されたデータに対する改ざんを検出する機能を備えること。

メッセージの完全性を保護する必要がある場合、メッセージが改ざんされていないことを確認する機能を備えること。

アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手続きを整備すること。

(3) 暗号による管理策

情報を保護するために暗号を用いる場合、事前にリスク評価を行い、暗号使用ポリシーを定義すること。

取扱いに慎重を要する情報や重大な情報については、機密性を保護するため暗号化すること。

電子情報の真正性および完全性を保護するため、デジタル署名を適用すること。

取引に関わる紛争を解決するため、電子情報の発信及び受信の否認を防止するための措置を講ずること。

情報を保護するために暗号を用いる場合、関連する対策基準類や手続き等に準拠し、適切に鍵管理を行うこと。

(4) システムファイルのセキュリティ

稼働中の情報システムにソフトウェアを導入するための手続きを確立すること。

テスト用データの使用に関する手続きを確立すること。

プログラムソースライブラリへのアクセスを厳格に管理すること。

(5) 開発及びサポートプロセスにおけるセキュリティ

情報システムの変更管理手順を確立し、変更を厳格に管理すること。

オペレーティングシステムを変更する場合の見直し及びテストの手順を確立すること。

ソフトウェアパッケージの変更は原則として行わないこと。

やむを得ずソフトウェアパッケージの変更が必要になった場合、変更を厳格に管理すること。

ソフトウェアの購入、使用及び変更を厳格に管理すること。

ソフトウェア開発をアウトソーシングする場合、事前にリスク評価を行いその結果に基づいた正式な契約を締結すること。

9. 事業継続管理

(1) 事業継続管理

組織全体に亘る事業継続を開発、維持するための管理手順を整備すること。

事業継続に取り組むため、リスク評価に基づいた戦略計画を策定すること。

重要な業務に障害または故障が発生した際に事業を維持し遅延なく復旧させるため、

必要な計画を立案すること。

すべての計画の整合性を保ち、計画の試験と整備の優先順位を明確にするため、事業継続計画全体の枠組みを維持すること。

事業継続計画を定期的に試験し見直すこと。

10. 準拠

(1) 法的要求事項への準拠

個別の情報システム毎に関連するすべての法規及び契約上の要求事項を明確にし、これを文書化すること。

知的財産権に関わる法的制限事項に準拠するための手続きを整備すること。

組織の重要な記録を紛失、消失、破壊、改ざん等から保護すること。

個人情報保護に関する法規に従い、個人の情報を保護すること。

情報処理施設及び設備の悪用を防止するための管理策を講ずること。

暗号の使用に関する法規に準拠すること。

訴訟に提示される証拠は、関連する法規に定められた規則に適合すること。

(2) セキュリティポリシー遵守状況の確認

すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。

情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的を確認すること。

(3) システム監査の考慮事項

稼働中の情報システムに対する監査を実施する場合、業務が中断するリスクを最小限に抑えるよう計画すること。

システム監査ツールに対する許可されないアクセスを防止すること。