ISMS
詳細管理策講座

ISO27001
ISMSの基礎知識

詳細管理策とは？

詳細管理策とは、ISMSの要求事項の中でも唯一実現の要否について実現しないことが許される管理策のことです。

詳細管理策は次の章立てで構成されています。

A5　情報セキュリティ基本方針
A6　情報セキュリティのための組織
A7　資産の管理
A8　人的資源のセキュリティ
A9　物理的および環境的セキュリティ
A10　通信および運用管理
A11　アクセス制御
A12　情報システムの取得、開発及び保守
A13　情報セキュリティインシデントの管理
A14　事業継続管理
A15　遵守

詳細管理策の区分

詳細管理策は、全社的な対応を要する管理策と、部門や組織、施設によって異なる管理策に分かれます。

詳細管理策	
全社的な管理策	部門等により異なるもの
A5	A9
A6	A10
A7	A11
A8	A12
A14	A13
A15	

詳細管理策の選択可否の要件

- リスクアセスメント

リスクアセスメントの結果対応を要すると判断されたものに関しては対応が必要となりますが、不要と判定されれば選択しないことも許可されます。

また、選択することで業務上の問題となるもの、該当しないものなども詳細管理策としては適用除外の理由となります。

ただし、これらの記録を明確に残さなければならず、判断の根拠を示さなければなりません。

A5

情報セキュリティ基本方針

情報セキュリティ基本方針について次のことを規程しています。

- 定期的に見直しすること
- 公開すること

実際には要求事項にも同様の内容が規定されています。

A6

情報セキュリティのための組織

次のことを実現することを求めています。

- 経営陣から任命されたセキュリティ組織
- 部門横断でセキュリティについての情報交換のできる組織
- 情報セキュリティ責任の明確化
- 情報処理設備を導入する際の認可プロセス(問題ないか事前確認)
- 秘密保持制約のレビュー機能
- 外部組織との連絡体制
- 専門家との意見調整
- セキュリティ対策の定期的な見直し
- 業務委託する場合のリスク管理
- 顧客がシステムへアクセスする際のリスク管理
- 契約における情報セキュリティ要件の明確化

A7

資産の管理

資産について、次のことが求められています

- 情報資産台帳の作成
- 資産の管理責任者の明確化
- 資産の利用許可範囲の明確化（どの情報は誰が使用してよいのか）
- 資産分類（情報の重要度に応じて区分けする）
- 資産のラベル付け（情報の重要度が分かるようにラベル付けを行い区分けしやすくする）

これらの内容に基づき、現在は文書管理基準が策定されています。

A8

人的資源のセキュリティ

従業員について、次のように管理することを求めています。

- 雇用前に、選考を行い、雇用契約などでセキュリティに関する責任を明示する。
- 従業員が守るべきセキュリティ上の役割や責任について明文化する
- セキュリティのルールを明文化し、周知する
- 情報セキュリティの維持向上教育を定期的に行う
- セキュリティ違反に対して、正式な懲戒手続きを設ける
- 雇用終了時の機密保持を行う
- 雇用終了時には資産を返却させ、アクセス権を削除する

A9

◆ 9．1　セキュリティを保つべき領域

セキュリティ上、守るべき施設等へは物理的に次のように保護することが求められています。

- 物理的に封鎖する(ドア、壁など)
- 物理的にアクセスを制限する(入退室管理など)
- オフィスエリアもセキュリティを考慮したうえで設計する
- 火災などの災害から保護できるようにする
- 特にセキュリティの高いエリアでの作業ルールを定める
- 一般の人が立ち入るエリアはセキュリティの高いエリアとは切り離す

A9

◆ 9．2　装置のセキュリティ

物理的に破損するリスクのある装置に関しては、次の通り保護することが求められています。

- 装置の設置場所には、環境上の影響が低いところを選ぶまたは保護する
- エアコン、UPSの故障などが発生した時の対応が出来るようにしておく
- ケーブル配線は、損傷や、盗聴などのないように行う
- 適切に保守する（保守メニューを定める）
- 社外に装置がある場合、社内とは異なるルールを考慮する（オフィスエリア外に持ち出しも含む）
- PCを廃棄する場合は情報を処理したうえで廃棄する
- 装置、情報、ソフトウェアは、事前の認可なしには持ち出さない（認可制度を作る）

A10

10．1　運用の手順および責任

情報システムの運用手順について、次のことが求められています。

- 情報システムの操作手順は文書化する
- 情報システムの変更は、記録し、変更前に計画し、影響範囲を考慮したうえで行う。
- 情報システムの職務及び責任は分割する
- 開発環境は本番環境とは分ける

10．2　第三者が提供するサービスの管理

第三者の提供するサービスをセキュリティの保たれた状態にするために、次のことが求められています。

- サービスの責任範囲、セキュリティの責任、サービスレベルなどを合意する。
- 第三者が提供するサービスを報告を受けるなどの方法で常に監視し、定期的に監査する
- サービスが変更された場合に、リスクなどに影響がないか確認する。

A10

10．3　システムの計画作成及び受入れ

システムを新規導入する際には、故障などのリスクを防ぐために次のことを実施する。

- 必要なシステムの性能があることを確実するために、将来必要な容量、能力を予測しておく
- システムを受け入れる前に、試験を行って、問題ないことを確認する。

A10．４ 悪意のあるコード及びモバイルコードからの保護

悪意のあるコード及びモバイルコードとは、ウィルスや不正プログラム等のことを指します。

- Winnyの禁止
- ウィルス対策ソフトの導入
- ウィルス感染時の対応手順策定

など

10．５　バックアップ

バックアップについては、具体的な周期や対象となる情報を定めて行うことが求められています。

A10

10．6　ネットワークセキュリティ管理

ネットワークについては、設計段階、さらには意地の過程において適切なネットワーク構成をするために次のことが求められています。

- ネットワークを適切に管理、制御する
  - → ネットワークに関しては、セキュリティを保てるよう設計し、全体像を決めることが求められます。
  - → 管理、制御とは、変更の計画や記録などを行うことであり、影響評価を行ったうえでネットワークの変更などを行うことが求められます。
- すべてのネットワークサービスにおいて、サービス状態を把握できるようにしておく
  - → 社内に関してはネットワークの構成図を作ることが求められます。
  - → 社外のサービスを受けているものに関しては、契約、サービスの報告などを受けることで実現されます。

A10

10．7　媒体の取扱い

媒体とは、紙、メモリ、HDDなどのことを指し、これらの媒体については次の通り取り扱うことが求められます。

- 可搬媒体の管理に関する手順を策定する
- 媒体を処分する際の安全な処分の手順を策定する（物理的破壊など）
- 媒体の取扱、保管ルールを定める
- 情報システムに関連した文書は特に厳重に保護する

これらのことを実現するために、情報の取扱手順策定は必須となってきます。

A10

10．8　情報の交換

情報の交換は、内部、及び外部との情報交換も含みます。情報交換については、セキュリティを保つために次のことが求められます。

・ メール、Web、電話、Faxなどの通信機器を使用する際のルールを決めておく
・ 外部組織との間で情報交換を行う際には、両者で取り決めた方法を使って情報交換する
・ 媒体を配送で送る場合、盗難、紛失、破損などにあわないように安全な配送方法を選択する。
・ メールなどに含まれる情報を保護するための対策をとる
・ 相互接続のあるシステムとメッセージ通信を行う場合には、そのメッセージの送信の仕方や、手順を策定する。

10．9　電子商取引サービス

電子商取引とは、Webなどを使って商取引を自社主導で行っている場合に適用が必要な項目です。
その場合には、改ざん対策や、商取引の記録が正確に残るような対策、また、Webサイトの情報そのものを正確に保つことなどが求められます。

A10

10. 10　監視

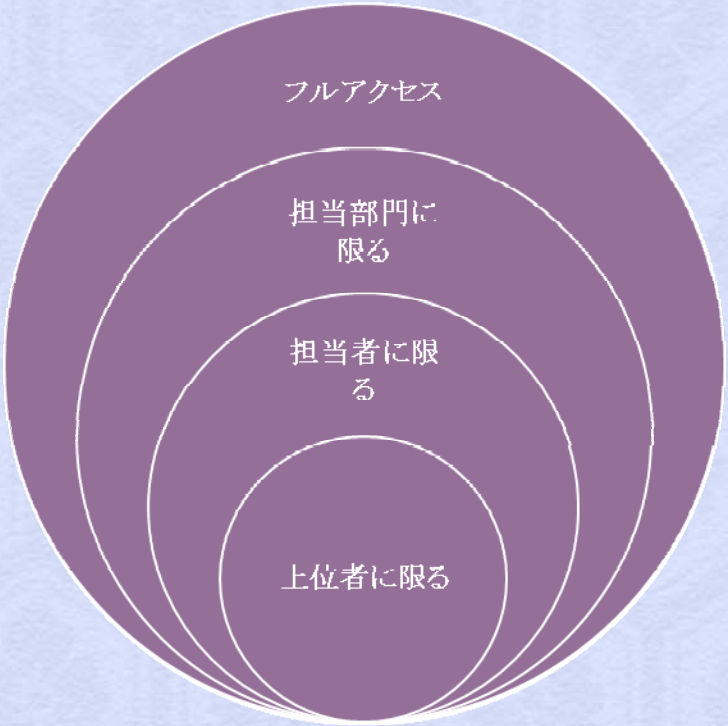
監視は、エラーの検知だけでなく不正アクセスなどの検知のために行われます。
監視については次のように実現することが求められています。

- 作業ログ、インシデント等の必要なログを取得し、保管する
- システムの使用状況を監視する。また、結果をレビューする(トラフィック、アタックなど)
- ログは改ざんされないように保護しておく
- システムを運用している際に発生する作業の記録を残す(変更記録など)
- 障害のログを取得し、対応する
- 情報システムのクロックは同期する

A11

11．1　アクセス制御方針

アクセス制御には方針を定めなければならないとされていますが、アクセス制御は次のような概念で成立しています。
このアクセス権を、何に対して割り当てるのかがアクセス制御方針です。



A11

11．2　利用者アクセスの管理

アクセス制御の一環として、ユーザ管理の実施をすることが求められています。

・　ユーザ登録・削除は正式な承認プロセスを経て行うようすること

・　特権（アドミニストレータ、スーパーユーザなど）は必要最低限の人にしか与えず、与える場合は承認を必要とすること

・　パスワードは、割り当てを行う場合は管理された割り当て方法で、個人ごとの設定の場合は、その個人に対し、解析しづらいパスワードなどを選択させること

・　割り当てられたアクセス権は定期的に見直しをする

11．3　利用者の責任

ユーザ管理の徹底において、利用者に対しても要求があります。

・　パスワードの選択時にはセキュリティ上解析しづらいパスワードにする

・　無人状態のPCが不正使用されないようにログオフ、電源オフなどを徹底する

・　離席時にはクリアスクリーン、普段からクリアデスクポリシーを徹底する

A11

11．4　ネットワークのアクセス制御

ネットワークを使用する際には、次の通りアクセスを制限する必要があります。

- 不必要なネットワークには入らせないようにする
- 遠隔地からアクセスするユーザがいる場合は、認証方法を用意する
- 特定の機器などからのアクセスを認証しなければならない場合は、装置の識別を行う
- 診断用や、環境設定用に外部からアクセスできるようにあけているポートへのアクセスは制御する
- ネットワークはグループごとに分割する
- インターネットなどの共用ネットを使用する際のルールを決めておく
- アクセス制御が守られるよう、ルーティングを設定する

ネットワークの範囲や、対象となるネットワークごとに対応する管理策の内容が異なることがあります。
もちろん、採用可否についても分かれる可能性があります。

A11

11．5　オペレーティングシステムのアクセス制御

ここでいうオペレーティングシステムとは、単にPCのOSだけのことを指すわけではなく、社内のシステム全体を指してオペレーティングシステムという表現をとっています。

- 社内システムへアクセスする場合はログオン手順を経由すること
- ユーザIDは一意なものにすること（同じものは使わない）
- パスワードは対話式のパスワードシステムであること、及び不適切なパスワードを排除するよう設定されていること
- システムを制御できるユーティリティの使用は制限すること
- 一定の使用中断時間が経過したら、ネットワーク接続を切断すること（ログオフでも可）
- リスクの高いシステムを使用する際には、使用を許可する時間を特定して使用させるようにする。

A11

11．6　業務用ソフトウェア及び情報のアクセス制御

ここでいう業務用ソフトウェアとは、データベースなどのソフトのことを指しています。
ファイルサーバなどに保管された情報と異なる管理が必要です。

- ソフトウェア上で設定できるアクセス制御を行う
- 取り扱いに慎重を要するシステムである場合、隔離した環境に設置する

11．7　モバイルコンピューティング及びテレワーキング

モバイルコンピューティングとはノートPC等の持ち出し環境で使用すること、テレワーキングとは遠隔地（おもに自宅）などで作業することを指しています。

- モバイルコンピューティングをする場合のルールを策定する
- テレワーキングを行う場合のルールを策定する

A12

12．1　情報システムのセキュリティ要求事項

新規システムの導入や、既存のシステム改善を行う場合には事前に仕様を明示しなければならない。
仕様として、求められるのは次のような内容。

- 容量
- 性能
- ソフトウェア及びミドルウェアの内容
- セキュリティ上の優位点及び注意点
- セキュリティ機能

システム導入などを行う場合は、仕様の明確化を行うとともに、仕様の内容を確認したうえで、問題ないことを承認してから導入することが求められます。

A12

12．2　業務用ソフトウェアでの正確な処理

業務用ソフトを使用する際には、次のことを確実に行えるソフトウェアとすることが求められます。

システム間のメッセージを正確に

内容を正確に入力する
内部処理が誤っていた場合に、エラーを検出する機能を設ける

出力したデータが正確であったか確認する

A12

12．3　暗号による管理策

暗号は設定することにより、セキュリティが高まりますが、逆に複合できなかったときにファイルが開けないといった問題が発生する可能性があります。

- 暗号を使用する条件及び、暗号の種類は特定する
- 暗号かぎを使用する

12．4　システムファイルのセキュリティ

システムファイルとはシステムを設定している情報のことを指します。

- ソフトを導入する際には、既存のシステムで動作可能かを確認したうえで導入すること
- システムのテストに使用したデータは保護し、管理すること
- ソースコードへのアクセスは、必要な人間以外させないこと

上記のことを情報システムの改善などを行う際に実施することが求められています。

A12

12．5　開発及びサポートプロセスにおけるセキュリティ

システムの導入時に注意すべき点をここからは主に定義しています。

- 変更管理の手順を用意すること
- 情報システムを変更する際には、事前に試験すること
- パッケージ販売されているソフトの変更は、ライセンス上許可されている範囲内とすること
- 導入時に情報漏えいが起こらないように対応すること
- ソフト開発を外部委託した場合には、進捗などを監視すること

12．6　技術的ぜい弱性の管理

現在利用中の情報システムの技術的なぜい弱性に関する情報は都度確認の上対応すること。

- パッチインストール
- セキュリティ情報の確認など

A13

13．1　情報セキュリティの事象および弱点の報告

情報セキュリティに関する事象には、システムのエラーなどだけでなく、情報漏えいや不正改ざんなどといった事象も含まれます。

これらの事象について次の通り対応することが求められています。

- 情報セキュリティインシデントが発生した際の報告・連絡経路を定める。
- インシデント及び疑いのあった事象はすべて記録する

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

情報セキュリティインシデントについて、組織としての対応体制を定める必要があります。

- 情報セキュリティインシデントに対応する組織を定める
- 情報セキュリティインシデントを分析し、受けた被害などを明確にする
- 法的措置が必要となったときのために証拠を収集する

A14

- 事業継続計画

A15

順守

コンプライアンスについて定義されており、次の内容を定める必要があります。

- 適用法令対応方針の文書化
- 知的財産権の保護方法
- 法的に重要な記録、文書の保護
- 個人情報保護
- 情報処理施設を不正利用から保護する
- 暗号化の法令順守（現在日本には、暗号化の法制はないため、適用は除外となる）
- セキュリティ方針順守のための手順作成
- 情報システムのセキュリティチェック
- 情報システム監査のリスク対策
- 情報システム監査ツールのリスク対策