配 付 番 号 ：

管　理　区　分
管　理　文　書

文書番号	ISMS-A-04
制 定 日	2020.03.01
改 訂 日	
改訂番号	1

【編集可能!】ISMS 管理策運用規定

ＪＩＳ Ｑ ２７００１：２０１４ 適用

（ ＩＳＯ/ＩＥＣ ２７００１：２０１３ ）

承　認	作　成

株式会社　サンプル

ISMS 管理策運用規定	制定日 2020.03.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

目　　次

改訂歴表

ISMS 管理策運用規定	制定日 2020.03.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

Ⅰ　情報セキュリティのための方針群（A.5）

1　情報セキュリティのための経営陣の方向性（A.5.1）

1.1　情報セキュリティ方針群（A.5.1.1）

ISMS 事務局は、**「情報セキュリティ基本方針」**を始めとする方針群を社長の承認を得て、発行し、全従業員及び関連する外部関係者に公表し、通知する。

1.2　情報セキュリティ方針群のためのレビュー（A.5.1.2）

ISMS 事務局は、年に一度（マネジメントレビュー時）、または事業上の重大な変化が発生したときに、**「情報セキュリティ基本方針」**を始めとする方針群が、適切、妥当及び有効であるかレビューし、社長の承認を得る。

Ⅱ　情報セキュリティのための組織（A.6）

1　内部組織（A.6.1）

1.1　情報セキュリティの役割及び責任（A.6.1.1）

「ISMS マニュアル」にて、情報セキュリティの責任を明確にする。具体的な従業員に関しての役割及び責任は、**「就業規則」**および**「誓約書」**によって、文書化することを確実にする。

1.2　職務の分離（A.6.1.2）

通信及び運用管理（例えば、情報システムの操作とその操作ログの取得）において、不正使用の危険性を低減するために、職務を分離させるか、一つの職務権限に一人ではなく、複数の者を割り当てるようにする。実施が難しい場合には、上長による監督等を実施する。

1.3　関係当局との連絡（A.6.1.3）

ISMS 事務局は、当社 ISMS の円滑な運用、緊急時の対応を図るため、下記の機関との連絡体制を確立する。　→　*具体的な連絡先は、一覧表にしておく*

(1) 社内他組織（適用範囲外）
(2) 関連会社
(3) 自治体（市役所など）
(4) 業界団体事務局
(5) 警察書
(6) 消防署
(7) 通信会社（NTT など）
(8) プロバイダー

1.4　専門組織との連絡（A.6.1.4）

システム管理責任者は、組織のシステム、ネットワークを安全な状態に保つため、下記の専門組織から情報収集を行い、適切な処置を講じる。　*→具体的な連絡先は、一覧表にしておく*

(1) JIPDEC（日本情報経済社会推進協会）
(2) IPA（情報処理推進機構）
(3) 主要ソフト（OS など）ベンダー
(3) ウィルスソフトベンダー
(4) その他、JPCERT など

1.5　プロジェクトマネジメントにおける情報セキュリティ（A.6.1.5）

ISMS 事務局は、社内の活動（開始日と終了日がある特定の活動）においても、情報セキュリティの取り込みを組み込むために、各プロジェクト責任者に、機密文書漏えい防止などの適切な処置の実施を命じる。

2　モバイル機器及びテレワーキング（A.6.2）

2.1　モバイル機器の方針（A.6.2.1）

従業員は、モバイル機器の利用を行う場合は、下記の項目を確実に行う。

(1) 社外へ持ち出し可能なモバイル機器は、会社が認めたモバイル機器に限定する。
(2) 盗み見の危険を避けるため、喫茶店や電車内等での公共の場所での使用を禁止する。
(3) 部外秘以上の情報を PC に格納して持ち出す場合は、暗号化する。
(4) 社外に持ち出し時及び持ち出し期間中は、ウィルス定義パターンファイルが最新になっていることを確認する。
(5) 社外で使用したモバイル機器を社内ネットワークに接続する場合は、接続前にウィルスチェックを実施する。

2.2　テレワーキング　（A.6.2.2）

(1) 組織的な対策事項

① ISMS 管理責任者は、上記のモバイル機器方針に従って、テレワークのセキュリティ維持に関する技術的対策の指示をシステム管理責任者に行うとともに、定期的に実施状況の検証を計画し、実施する。
② 管理部門は、テレワーク従事者の情報セキュリティに関する認識を確実なものにするために、教育を実施する。
③ 情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確立させる。

(2) テレワーク従事者における順守事項

① テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、モバイル機器方針や社内ルールに沿った業務を行い、定期的に実施状況を自己点検する。

② テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

③ モバイル機器の紛失・盗難には留意する。

④ 無線 LAN 利用に伴うリスクを理解し、テレワークで利用する場合は、暗号化等の確保すべきセキュリティレベルがあるかどうかを確認して、利用する。

⑤ 社内システムにアクセスするための利用者認証情報(パスワード等)を適正に管理する。

⑥ インターネット経由で社内システムにアクセスする際、システム管理責任者が指定したアクセス方法のみを用いる。

⑦ テレワークでファイル共有サービス等のクラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。

⑧ テレワーク作業中にマルウェア（コンピュータウィルス）に感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、そのような場合は、直ちに定められた担当者に連絡する。

→ *参考情報：総務省「テレワークセキュリティガイドライン」*

ＸＩ　供給者関係（A.15）

1　供給者関係における情報セキュリティ（A.15.1）

1.1　供給者関係のための情報セキュリティの方針（A.15.1.1）

供給者による組織の情報へのアクセスに具体的に対処するため、下記の事項を考慮し、供給者と合意し、文書化する。

(1) 組織が、自らの情報へのアクセスを許可する供給者の種類の特定及び文書化

(2) 供給者関係を管理するための標準化されたプロセス及びライフサイクル

(3) 様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理

(4) 情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるもの

(5) それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセス及び手順

(6) 各当事者が提供する情報又は情報処理の完全性を確実にするための、正確さ及び完全さの管理

(7) 組織の情報を保護するために供給者に適用する義務の種類

(8) 供給者によるアクセスに伴うインシデント及び不測の事態への対処

(9) 各当事者が提供する情報又は情報処理の可用性を確実にするための、対応力に関する取り決め、並びに必要な場合には、回復及び不測の事態に関する取決め

(10) 情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化

1.2　供給者との合意におけるセキュリティの取扱い（A.15.1.2）

(1) 情報処理業務の委託

該当部門の担当者は、情報処理に関する業務の一部または全部を、供給者（外部の業者）に委託する場合に、下記の事項を含む契約書、または覚書を取り交わす。

① 守秘義務

② 責任の範囲

③ 情報の取扱いに関する事項

④ 情報流出、破損など事故発生時の損害賠償

⑤ 委託先責任者

⑥ 当社による監査及び教育実施の権利

(2) 装置・設備の保守（修理）契約

該当部門の担当者は、下記の事項を順守して、行う。

① 当社の情報処理装置・設備の保守・修理を当社内で実施する場合は、当社従業員が付き添うこと。

② 当社の情報処理装置を、供給者（外部）に修理委託する場合は守秘義務を含む契約を取り交わすこと。

③ 当社の情報処理装置を、供給者（外部業者）の施設で運用する場合（ハウジングサービスの利用)、下記事項を含む契約書、または覚書を取り交わすこと。

- 守秘義務
- 情報流出、装置破損、電源断など事故発生時の連絡及び損害賠償
- 委託先責任者
- 当社による監査の権利

(3) 供給者による施設内作業契約

該当部門の担当者は、室内清掃、建物警備など、従業員不在時に当社の情報資産にアクセスできる可能性がある作業を供給者（外部）に委託する場合は、下記事項を含む契約書、または覚書を取り交わす。

① 守秘義務

② 情報流出、機器破損時の連絡及び損害賠償

③ 委託先責任者

1.3 ICT サプライチェーン（A.15.1.3）

該当部門の担当者は、供給者（外部）との合意において、情報通信技術（ICT）サービス及び製品のサプライチェーンに関する情報セキュリティリスクに対処するため、下記の要求事項を明確にする。

(1) ICT サービスに関して、供給者（外部）が組織に提供する ICT サービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するよう供給者（外部）に要求する。

(2) ICT 製品に関して、その製品に他の供給者（外部）から購入した構成部品及びサービスが含まれる場合には、そのサプライチェーン全体に適切な情報の機密性、完全性、可用性が確保されることを供給者（外部）に要求する。

２　供給者とのサービス提供の管理（A.15.2）

2.1　供給者のサービス提供の監視及びレビュー（A.15.2.1）

ISMS 事務局は、関連部門の協力を得て、定常的に監視を行っている委託した供給者（外部）のサービスの監査を年一回、もしくは必要に応じて行い、その結果を ISMS 推進委員会にて報告を行う。

2.2　供給者のサービス提供の変更に対する管理　（A.15.2.2）

該当部門は、供給者（外部）が提供するサービスに変更があった際は、リスクを再評価し、必要に応じて手順等を見直し、その結果を ISMS 推進委員会にて報告を行う。

ⅩⅡ　情報セキュリティインシデントの管理（A.16）

1　情報セキュリティインシデントの管理及びその改善（A.16.1）

1.1　責任及び手順（A.16.1.1）

情報セキュリティインシデントが発生した場合、ISMS 事務局は、情報セキュリティ推進委員と連携して下記の対応を行う。

(1) コンピュータウイルス感染時の対応

	対応内容
１．感染発覚時の対応	・発見者は、感染等が認められたら、直ちに端末をネットワークから遮断し、直ちにシステム管理責任者に連絡をとる。 ①被害拡大阻止の対応（当座の処置） ②ISMS 管理責任者に連絡
２．確認と対応	１.連絡を受けたシステム管理責任者は、対応に着手すると共に、ISMS 管理責任者に状況報告を行い、ウイルスが急速に広く伝播する恐れがある場合には、必要な対応を迅速に関係者へ通知を行う。 ２．感染等の有無に関わらず、利用者は怪しいメールを決して開かない。感染の恐れがある端末では，メールや Web 閲覧のソフトウエアを起動させない。
	３．感染したメールが外部に送信された場合、送信した先方に、送信者は電話などにより連絡し、感染の拡大を防止する。
	４．システム管理責任者は、感染端末のメール利用について、利用者アカウントの停止、および、端末登録の停止を行う。
	５．システム管理責任者は、当該端末の復旧対策などは、応急処置対応を終えてから着手する。
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、「セキュリティインシデント報告書」を作成し、ISMS 管理責任者に提出する。

(2) 不正アクセス時の対応

	対応内容
１.不正アクセス発覚時の対応	・発見者は、不正アクセスが認められたら、直ちにシステム管理責任者に連絡をとる。
２．確認と対応	・連絡を受けたシステム管理責任者は、対応に着手すると共に、ISMS 管理責任者に連絡を行い、必要な対応を迅速に関係者へ通知を行う。 ①不正アクセスの有無　②情報の保存 ③調査の実施　④復旧対策
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、「セキュリティインシデント報告書」を作成し、ISMS 管理責任者に提出する。

(3) サービス停止時（システム障害時）の対応

	対応内容
１．サービス停止時の対応	・発見者は、サービス停止が認められたら、直ちにシステム管理責任者に連絡をとる。
２．確認と対応	・連絡を受けたシステム管理責任者は、対応に着手すると共に、ISMS 管理責任者に連絡を行い、必要な対応を迅速に関係者へ通知を行う。 ①委託業者等への連絡 ②調査の実施 ③復旧対策
３．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
４．報告書の作成	・システム管理責任者は、「セキュリティインシデント報告書」を作成し、ISMS 管理責任者に提出する。

(4) 機密情報の漏えい・流出・盗難発覚時の対応

	対応内容
１．発覚時の対応	・通報を受けた者及び発見した者は、下記の事項を実施する。 ①被害拡大阻止の対応（当座の処置） ②ISMS 管理責任者に連絡
２．確認と対応	１．連絡を受けた ISMS 管理責任者は、社長に連絡する。 ２．ISMS 管理責任者は、社長及び関係責任者と対応を協議し、関係者に指示を行う。
	３．指示を受けた関係者は、下記の事項を実施する。 ①状況の確認 →漏洩した情報資産の保管場所、使用者を特定する。 ②原因の追究 →システム管理責任者へサーバーの該当フォルダに対するアクセス権限設定の再確認を依頼し、不審点があれば究明する。 →疑わしいハードウェア、ソフトウェアがあれば、その設定を確認し、原因を追及、除去する。 ③被害拡大阻止の完了 →携帯電話の紛失、ノート PC の紛失、資料ファイルの紛失、それらの盗難などにより機密漏洩が危惧される場合は、その持出し先、保管状況を調査し、可能な限り回収に努める。 ④ISMS 管理責任者に報告（進捗状況を随時報告）
３．外部への対応	社長又は ISMS 管理責任者は、必要に応じて、下記の事項への対応を行う。 ①顧客等（利害関係者）への対応 ②行政（経済産業省等）への対応 ③マスコミへの対応 → プレスリリースの作成
	社長又は ISMS 管理責任者は、必要に応じて、経過報告を HP 等にて行う。
４．再発防止対策	・ISMS 管理責任者は、ISMS 推進委員会において協議を行い、再発防止対策を決定し、関係者に指示する。
５．報告書の作成	・ISMS 管理責任者は、「セキュリティインシデント報告書」を作成し、社長に提出する。

(5) 地震等自然災害におけるサービス停止（システム障害時）時の対応

	対応内容
１．地震等の自然災害が発生時の対応	・下記の事項を最優先する。 ①安全な場所への避難 ②従業員の安否の確認
２．確認と対応	１．管理部門長及び ISMS 管理責任者は、被害状況の確認を行い、社長へ報告する。 ２．社長は関係者と協議し、事業継続(営業)の可否を判断し、従業員に指示を行う。(復旧計画の策定→実施) ３．サービスが停止したことを関係従業員へ連絡する。 ４．システム管理責任者からサービスの停止の原因が取り除かれ、サービスの再開の連絡を受けた場合は速やかに関係従業員に周知する。
３．外部への対応	１．社長は、必要に応じて、下記の事項への対応を行う。 ①顧客等（利害関係者）への対応 ②行政や関係者への対応 ③マスコミへの対応
	２．社長又は ISMS 管理責任者は、必要に応じて、経過報告を HP 等にて行う。

1.2 情報セキュリティ事象の報告（A.16.1.2）

従業員は、情報セキュリティ方針の違反、採用した管理策の不具合、情報セキュリティ上の何らかの異常に気づいた場合、**「情報セキュリティ事象記録簿」**にて、ISMS 事務局へ連絡する。ソフトウェアの誤動作に気がついた場合も同様とする。ISMS 事務局は、その内容をシステム管理責任者へ伝える。

1.3 情報セキュリティ弱点の報告（A.16.1.3）

ISMS 管理責任者は、利用者に対して、利用者がぜい弱などの情報セキュリティの弱点を発見した場合、勝手に技術検証せずに、システム管理責任者へ報告することを要求する。

1.4 情報セキュリティ事象の評価及び決定（A.16.1.4）

ISMS 管理責任者は、情報セキュリティ事象の評価及び決定を行い、**「情報セキュリティ事象記録簿」**にて、その結果および指示事項を社内に伝達する。

1.5 情報セキュリティインシデントへの対応（A.16.1.5）

情報セキュリティインシデントへの対応は、下記の事項を原則として行う。

(1) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集する。

(2) 関係する全ての対応活動の記録を行う。

(3) 情報セキュリティインシデントの存在又は関連するその詳細を伝達する。

(4) インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処する。

XIV　順守（A.18）

1　法的及び契約上の要求事項の順守（A.18.1）

1.1　適用法令の識別（A.18.1.1）

ISMS 事務局は、関連する法的及び契約上の要求事項を抽出し、**「法的要求事項登録簿」及び契約書**に明確化する。また、定期的に毎年 3 月**「法的要求事項登録簿」**の見直しを実施する他、下記の事項が発生したとき、臨時の見直しを行う。また、手順教育等により、周知を図る。

(1) 適用範囲の業務に新しい活動、サービスが追加されたとき。

(2)**「法的要求事項登録簿」**に記載されている法律、規制事項に関係する活動、サービスの変更、廃止があったとき。

(3) 適用範囲の業務に新しい活動、サービスに関係する法律が新たに制定されたとき。

(4)**「法的要求事項登録簿」**に記載されている法律、規制事項に変更があったとき。

(5) 契約上の要求事項に変更があったとき。

1.2　知的財産権（A.18.1.2）

従業員は、他者の権利を侵害しないことを確実とするため、下記の項目を順守すること。

場面	順守事項
新製品開発時、新事業（新サービス）開始時	特許権、商標権の侵害がないことを調査し、調査結果を記録に残す。
当社ホームページ、パンフレットなどへ著作物を転載する時	著作権の侵害がないか調査し、公開前に該当部門長の承認を得る。
PC などにソフトウェアをインストールする時	購入ソフトウェアをインストールした PC を記録に残すと共に、インストール後のソフトウェア記録媒体は施錠された場所に保管する。

1.3　記録の保護（A.18.1.3）

ISMS 事務局は、セキュリティに関係する重要な記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざんがないように管理を行う。

1.4　プライバシー及び個人を特定できる情報の保護（A.18.1.4）

従業員は、個人情報保護法や各種ガイドライン等を順守し、下記の項目を確実にすること。

(1) 個人情報の収集、利用、第三者への提供およびその管理や本人からの要求については「個人情報保護法」に従い処理する。

(2) 従業員の個人情報については下記を取扱いの基準とする。

① 従業員の健康情報、従業員考課表
　情報資産の「極秘」区分に準ずる扱いとする。

② 従業員の自宅連絡表
　情報資産の「部外秘」区分に準ずる扱いとする。

ISMS 管理策運用規定	制定日 2020.03.01	文書番号 ISMS-A-04
	改訂日	改訂番号 1

このISMS管理策運用規定のサンプルを有料にて、ワードファイルで提供中です。

有料版には、目次のすべての項目が含まれています。

※本文にある様式や他の文書は含まれておりません。

提供価格：16,500円（税込）

購入方法：

1．下記のホームページのお問い合わせにて、Eメールで購入のご連絡をお願い致します。
→　https://www.iso-mi.com/
ご要望欄に、「ISMS管理策運用規定サンプル購入希望」と、ご記入ください。

2．当事務所にメールが届き、確認次第、請求書と共に入金口座をお知らせ致します。なお、振り込み手数料については、ご負担頂けますようお願い致します。

3．ご入金が確認でき次第、E メールにて納品致します。領収書が必要な場合は、お申し出ください。※また、納品したファイルが開けない、破損している場合は、その旨をご連絡下さい。交換致します。その他ご質問等は下記のメールアドレスにてお願い致します。

注意事項：

1．本商品（ISMS管理策運用規定サンプル）を転売する等の商用利用※を禁止致します。
※商用利用とは、顧客等へのコンサルツールの利用も含みます。

2．本商品（ISMS管理策運用規定サンプル）にあるサンプル文例は、
あくまでもサンプルですので、実際の文面は、必ず自社にあったものを
お書きください。また、文例にある様式（記録帳票）は含まれておりません。

3　個人（顧問を含む）やコンサルタント事業者様、士業様には、
ご購入は、ご遠慮頂いております。

以　上