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

※購入希望の場合は、https://www.iso-mi.com/
ページ最後の購入方法をご確認ください。修正可能なワードファイルで提供しています。

【編集可能!】ISMS 管理策運用規定

ＪＩＳ Ｑ ２７００１：２０１４ 適用
ＪＩＳ Ｑ ２７０１７：２０１６ 適用

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

Ⅰ．情報セキュリティのための方針群（A.5）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P3
Ⅱ．情報セキュリティのための組織（A.6）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P4
Ⅲ．人的資源のセキュリティ（A.7）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P6
Ⅳ．資産の管理（A.8）・・・P7
Ⅴ．アクセス制御（A.9）・・P11
Ⅵ．暗号（A.10）・・P17
Ⅶ．物理的及び環境的セキュリティ（A.11）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P18
Ⅷ．運用のセキュリティ（A.12）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P21
Ⅸ．通信のセキュリティ（A.13）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P25
Ⅹ．システムの取得、開発及び保守（A.14）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P28
ⅩⅠ．供給者関係（A.15）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・P32
ⅩⅡ．情報セキュリティインシデント管理（A.16）・・・・・・・・・・・・・・・・・・・・・・・・・・・P35
ⅩⅢ．事業継続マネジメントにおける情報セキュリティの側面（A.17）・・・・・・・・・P40
ⅩⅣ．順守（A.18）・・P43

改訂歴表

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。

■　クラウドサービス利用のための実施の手引き

※リスクを考慮して、「自社が行うべきこと」と「サービス提供者側に要求すべきこと」を明確にすること

クラウドサービス利用において、以下のリスクを考慮してクラウドサービス利用方針を作成し、組織の情報及びその他の資産に対する情報セキュリティリスクの受容可能なレベルと矛盾しないものとする。
・クラウドに保存する情報は、クラウドサービスプロバイダによるアクセス及び管理の対象となる可能性がある。*（クラウドサービス事業者からの情報漏えいのリスク）*
・アプリケーションプログラム等の情報資産は、クラウド環境の中に保持される可能性がある。*（情報を消去してもクラウド上に残っているリスク）*
・実行処理は、マルチテナントの仮想化されたクラウドサービス上で実行される可能性がある。*（隔離の失敗による他社に閲覧されるリスク）*
・クラウドサービスユーザ、及びクラウドサービスユーザがクラウドサービスを利用する状況。*（利用者の力量不足等、セキュリティを確保できない利用環境リスク）*
・クラウドサービスカスタマの特権的アクセスをもつクラウドサービス実務管理者*（クラウドサービス事業者側の要員の力量不足のリスク）*
・クラウドサービスプロバイダの組織の地理的所在地及びクラウドサービスプロバイダがクラウドサービスカスタマデータを保存する可能性のある国*（国外にデータセンターがある場合、その国の法律によりデータが閲覧されてしまうリスク）*

■　クラウドサービス提供のための実施の手引き

以下を考慮して、情報セキュリティ方針を拡充し、クラウドサービス提供における方針を作成する。
・クラウドサービスの設計及び実装に適用する、最低限の情報セキュリティ要求事項
・認可された内部関係者からのリスク
・マルチテナント及びクラウドサービスカスタマの隔離（隔離の失敗等の考慮）
・クラウドサービスプロバイダの担当者による、クラウドサービスカスタマの資産へのアクセス
・アクセス制御手順（例えば、多要素認証等の導入）
・変更管理におけるクラウドサービスカスタマへの通知
・仮想化セキュリティ
・クラウドサービスカスタマデータへのアクセス及び保護
・クラウドサービスカスタマのアカウントのライフサイクル管理
・違反の通知、並びに調査及びフォレンジック（証拠保全）を支援するための情報共有指針

IS-A-XX

クラウドサービス情報セキュリティ方針

制定日:2020.03.01

株式会社●●は、当社にて確立した「情報セキュリティ方針」を拡充し、以下に、クラウドサービス情報セキュリティ方針を制定します。

1. クラウドサービスの設計及び実装に適用する情報セキュリティ要求事項

・お客様からの情報セキュリティ要求事項及び当社にて確立した本方針を適用し、クラウドサービスの設計及び実装を行います。

2. 内部関係者からのリスク

・リスクアセスメントにて特定された内部関係者からのリスクに対し、管理策を採用し、実施します。

3. クラウドコンピューティング環境の隔離

・仮想化されたマルチテナント環境を利用して、クラウドコンピューティング環境を論理的に隔離し、セキュリティの確保を行います。

4.当社従業員による、お客様データへのアクセス及び保護

・クラウドサービスを提供するにあたって、または技術的な問題の解決のため、当社が定める約款に従って、お客様のアカウントにアクセスすることがありますが、当社の約款に定める場合を除き、お客様の事前の許可なく、お客様のデータを監視、編集、開示しません。

5. アクセス制御手順

・通常のパスワード認証に加え、より安全性を強化した二段階認証を設定します。

6. お客様への変更通知

・クラウドサービスに関する仕様変更等については、当社ホームページへの掲載等を通じて情報提供します。

7. 仮想化セキュリティ

・ハイパーバイザ(仮想化ソフトウェア)を攻撃から守り、ホスト基盤を仮想化環境において生じる脅威から守り、仮想マシンのライフサイクルを通じて保全します。

8. お客様のアカウント管理

・お客様のアカウント管理は、当社が定める約款に基づき、お客様の責任において作成し、管理していただくこととします。

9. 情報共有指針

・違反の通知、調査及びフォレンジック支援のための情報共有を実施します。通知・連絡の手段は当社の定める約款にて定義します。

以 上

株式会社 ●●

代表取締役社長 〇〇

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。

■ クラウドサービス利用のための実施の手引き

サービスを導入する責任者は、クラウドサービスプロバイダと情報セキュリティの役割及び責任の適切な割当てについて合意し、それらの役割及び責任が遂行できることを確認する。その結果については、合意書（契約書や利用規約等）を取り交わす。また、クラウドサービスプロバイダの顧客支援・顧客対応機能との関係（問い合わせ窓口や問い合わせ方法等）を事前に確認しておく。

■ クラウドサービス提供のための実施の手引き

営業担当者は、クラウドサービスカスタマ、クラウドサービスプロバイダ及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、合意書（契約書や利用規約等）を取り交わす。

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

■ クラウドサービス利用のための実施の手引き

サービスを導入する責任者は、クラウドコンピューティングを円滑に利用するために、必要に応じて、インターネットで検索して、クラウドサービスに関連する省庁や団体、クラウドサービスの事業者団体を特定し、連絡体制を確立する。

■ クラウドサービス提供のための実施の手引き

営業担当者は、クラウドサービスカスタマに、自社の組織の所在地、カスタマデータを保存する可能性のある国を契約書や利用規約、WEB 等を通じて、通知する。

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、人目が多く触れる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) 社外で使用した共有 PC 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」*

3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係（A.6.3）

3.1 クラウドコンピューティング環境における役割及び責任の共有及び分担（A.6.3.1）

クラウドサービスの利用に関して共有し分担する情報セキュリティの役割を遂行する責任は、クラウドサービスカスタマ及びクラウドサービスプロバイダのそれぞれにおいて特定の関係者に割り当て、文書化し、伝達し、実施する。

X　システムの取得、開発及び保守（A.14）

1　情報システムのセキュリティ要求事項（A.14.1）

1.1　情報セキュリティ要求事項の分析及び仕様化（A.14.1.1）

システム管理責任者は、情報システムへのセキュリティを確実にするために、情報システム担当者や現場での利用状況をヒアリングし、分析し、必要な要求事項の明確化を行う。

■　クラウドサービス利用のための実施の手引き

JISQ27017 の規格を参考に、クラウドサービスにおける情報セキュリティ要求事項を定め、クラウドサービスプロバイダの提供するサービスがこの要求事項を満たせるか否かを評価する。この評価のために、クラウドサービスプロバイダに情報セキュリティ機能に関する情報の提供を要求する。

■　クラウドサービス提供のための実施の手引き

クラウドサービスカスタマが利用する情報セキュリティ対策及び機能に関する情報を、自社 WEB 等において、クラウドサービスカスタマに提供する。

1.2　公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮（A.14.1.2）

公不特定多数の人が利用する公衆ネットワークを介して、電子商取引を利用する場合には、ネットワークに関連した脅威を意識して、認証時の暗号技術の使用又はデータ転送時のセキュリティ確保が実施されているサービスの利用を行う。

JISQ27017:2016 に完全対応した「ISMS 管理策運用規定 27017 対応版」を有料にて、ワードファイルで提供中です。有料版には、掲載した目次のすべて（対応する管理策のすべて）が含まれています。

提供価格：22,000 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 27017 対応版購入希望」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 27017 対応版）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 27017 対応版）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、必ず自社の実態にあったものを記入してください。

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