配 付 番 号 ：

管　理　区　分
管　理　文　書

文書番号	ISMS-A-04
制 定 日	2020.01.01
改 訂 日	2024.04.01
改訂番号	2

ISMS管理策運用規定（抜粋版）

ＪＩＳ Ｑ ２７００１：２０２３ 適用
ＪＩＳ Ｑ ２７０１７：２０１６ 適用

承　　認	作　　成

株式会社　サンプル

目　　次

改訂歴表

I　組織的管理策

1　情報セキュリティのための方針群（5.1）

1.1　情報セキュリティ方針群

ISMS 事務局は、**「情報セキュリティ基本方針」**を始めとする情報セキュリティに関わる固有の方針群は社長の承認を得て、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

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」**を始めとする固有の方針群が、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。

■　クラウドサービス利用のための実施の手引き

クラウドサービスの利用において、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）*

作成するクラウドサービス利用方針は、別紙に定める。

■　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し、自社 WEB に公開する。
・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:2020.01.01

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

2　情報セキュリティの役割及び責任（5.2）

「ISMS マニュアル」にて、情報セキュリティの役割と責任を明確にする。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。

3　職務の分離（5.3）

通信及び運用管理（情報システムの操作とその操作ログの取得等の管理）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。

4　管理層の責任（5.4）

管理層は、組織の方針及び手順に従った情報セキュリティの適用を、すべての従業員及び契約相手に要求する。

5　関係当局との連絡（5.5）

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) 行政（自治体）
(4) 業界団体事務局
(5) 警察
(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、自社 WEB 等を通じて、通知する。

6 専門組織との連絡（5.6）

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) マルウェアソフトベンダー

(4) その他（JPCERT、JVN 等）

7 脅威インテリジェンス（5.7）

当社は、適切なリスクの低減処置を講じることが出来るように、IPA（情報処理推進機構）、JPCERT コーディネーションセンター、JVN（脆弱性対策情報ポータルサイト）等の外部の脅威インテリジェンス（知見）を活用して、脅威インテリジェンスを構築する。

8 プロジェクトマネジメントにおける情報セキュリティ（5.8）

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確実にするために、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情報セキュリティ対策の実施を命じる。

■ 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。

Ⅴ　クラウドサービス拡張管理策

1　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（9.1）

1.1　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

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。*(参照:5.23)*

■　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、クラウドサービスの利用に合わせて、方針及び手順を定義又は追加し、クラウドサービスの利用者にクラウドサービスの利用における自らの役割及び責任を意識させる。

■　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、自らの情報セキュリティの能力、役割及び責任を契約書や利用規約等に文書化し、伝達する。また、クラウドサービスの利用の一部としてクラウドサービスカスタマが実施及び管理することが必要となる情報セキュリティの役割及び責任も伝達する。

2　資産に対する責任（9.2）

2.1　クラウドサービスカスタマの資産の除去

クラウドサービスプロバイダの施設にあるクラウドサービスカスタマの資産は、クラウドサービスの合意の終了時に、時機を失せずに除去されるか又は必要な場合には返却する。

■　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に対して、その資産の返却及び除去、並びにこれらの資産の全ての複製のクラウドサービスプロバイダのシステムからの削除の記述を含む、サービスプロセスの終了に関する文書を要求する。また、全ての資産を一覧にし、サービス終了が予定通り行われるようサービス終了のスケジュールを文書化する。

■　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対して、クラウドサービス利用のための合意の終了時における、全ての資産の返却及び除去の取決めについて、情報を提供する。また、資産の返却及び除去についての取決めは、合意文書の中に記載し、予定通りに実施し、その取決めでは返却及び除去する資産を特定する。

改 訂 歴 表

改訂番号	改 訂 日 付	内　　容	作成	承認
1	2020.01.01	制定	○○	●●
2	2024.04.01	2022 年版対応により全面改訂	○○	●●