版番号	03
発行日	2025/1/6

株式会社 SD ホールディングス

ISMS マニュアル

～　改訂歴表　～

版番号	発行年月日	改　訂　内　容
01	2023/03/01	新規制定：初版発行
02	2023/09/25	全文を JIS Q 27001 へ対応するよう見直し
03	2025/01/06	ISO27001 規格改定に伴い内容改訂

目次

１．適用範囲

当社所在地にておこなう以下の業務に適用される。

(1) 適用範囲

適用業務	ホールディング企業の管理業務

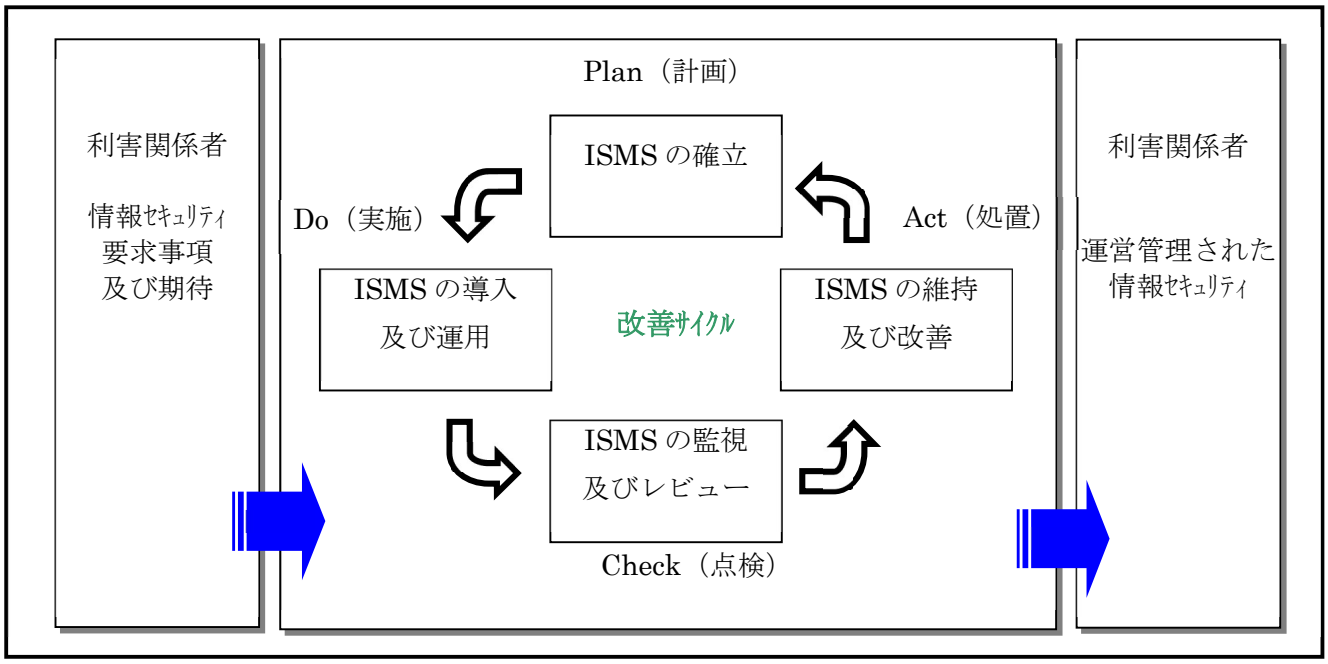
(2) 適用組織：

「適用範囲組織図」に明確にする。

(3) 適用所在地

東京都渋谷区東 3-16-3　エフ・ニッセイ恵比寿ビル 7F

(4)　適用プロセス



Plan－計画 （ISMS の確立）	組織の全般的な方針及び目的に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、情報セキュリティに関する方針、目的、プロセス及び手順を確立
Do－実施 （ISMS の導入及び運用）	情報セキュリティに関する方針、管理策、プロセス及び手順の導入及び運用
Check－点検 （ISMS の監視及びレビュー）	情報セキュリティに関する方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント(可能ならば測定)、及びその結果のレビューのための経営陣への報告
Act－処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するための、ISMS 内部監査およびマネジメントレビューの結果またはその他の関連情報に基づいた、是正処置の実施

2　引用規格

適用規格
　ISO／IEC27001：2022（JIS Q 27001:2023）

引用規格
　次に掲げる引用規格は，この規格に引用されることによって，その一部又は全部がこの規格の要求事項を構成している。この引用規格は，その最新版（追補を含む。）を適用する。
　JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語
　注記　対応国際規格における引用規格：ISO/IEC 27000，Information technology－Security techniques
　－Information security management systems－Overview and vocabulary

3　用語及び定義

ISMS に関する用語及び定義は、引用規格及び下表による。

用語	意味
利害関係者	お客様、協力会社、当社が利用しているサービス開発会社　等

4　組織の状況

4.1　組織及びその状況の理解

　当社において、組織の目的に関連し、かつ情報セキュリティマネジメントシステム（ISMS）の意図した成果を達成する能力に影響を与える、外部及び内部の課題を決定する。
当社においては気候変動が関連する課題への対策として紙資源の浪費削減を目的とした文書のデータ管理体制を推進するものとする。その他、今後課題であると認められるものが発生した場合、その課題に対して十分に有効だと認められる対応を検討し、部門責任者及び管理責任者の承認の上で実施する。

	外部	内部
リスク	不正アクセス	漏洩、滅失、毀損 情報セキュリティに関する体制やルールの整備
機会 （改善点やチャンス）	法令等の改正、利害関係者からの要求	社内教育・インフラへの投資 職場環境の改善（物理的な整理整頓、業務効率化）

4.2　利害関係者のニーズ及び期待

　当社は、顧客等をはじめとする利害関係者の要求事項および法的及び規制要求事項、合わせて法的及び規制要求事項を明らかにし、その上でそれらの要求事項のうち、ISMS を通して取り組むものを決定する。
また、関連する利害関係者からの気候変動に関する要求事項として、資源問題と関連して紙媒体での郵送や取引記録の保持から、ニーズに応じてデータへの移行を推進する。その他、当社に対して気候変動に関する要求が生じた場合、それを満たす必要があるかの判断を行う。必要であると判断した場

合は十分に有効だと認められる対応を検討し、部門責任者及び管理責任者が確認の上で実施する。

顧客(個人)	個人情報やクレジットカード情報、購入履歴などを安全に管理してほしい
顧客(法人)	営業情報や技術情報が流出しないように、情報管理を徹底してほしい
親会社	情報漏洩などの事故によって、企業グループのブランドイメージの低下や、信用失墜をさせないでほしい
株主	サイバー攻撃やデータ改ざんによる信用失墜によって、株価や企業価値を低下させないでほしい
従業員	情報セキュリティ事故の発生によって、個人情報流出や会社業績と雇用に悪影響が及ばないようにしてほしい
サプライヤー	受発注、納品、請求、支払いなどの情報処理プロセスに誤りがないようにしてほしい
国、地方自治体	情報管理の取組みをしっかりと行い、法令や規範を遵守した企業活動をしてほしい

4.3 情報セキュリティマネジメントシステム（ISMS）の適用範囲の決定

当社は、適用範囲を決定する場合、4.1 に規定する外部及び内部の課題、4.2 に規定する要求事項を考慮する。適用範囲には、当社にとって重要な情報資産を保護し、管理するための組織、設備を含める。

4.4 情報セキュリティマネジメントシステム（ISMS）

当社は、ISO／IEC27001：2022（JIS Q 27001:2023 の要求事項に従って、必要なプロセス及びそれらの相互作用を含む情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、かつ継続的に改善を行う。詳細については、以下の章に基づき規定する。

5 ISMS のリーダーシップ

5.1 リーダーシップ及びコミットメント

社長は、次に示す事項によって、情報セキュリティマネジメントシステム（ISMS）に関するリーダーシップ及びコミットメントを実証する。

(1)情報セキュリティに関する方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする。
(2)組織の事業プロセスへの情報セキュリティマネジメントシステム（ISMS）要求事項への統合を確実にする。
(3)情報セキュリティマネジメントシステム（ISMS）に必要な経営資源が利用可能であることを確実にする。
(4)有効な情報セキュリティマネジメント及び情報セキュリティマネジメントシステム（ISMS）要求事項への適合の重要性を伝達する。
(5)情報セキュリティマネジメントシステム（ISMS）がその意図した成果を達成することを確実にする。
(6)情報セキュリティマネジメントシステム（ISMS）の有効性に貢献するよう社員を指揮し、支援する。
(7)継続的な改善を促進する。
(8)その他の関連する管理層がその責任の領域においてリーダーシップを発揮するよう、その管理層の役割を支援する。

情報セキュリティのための方針群は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするために年に一度5月にレビューを実施する。

5.2　情報セキュリティに関する方針

情報セキュリティに関する方針

株式会社ＳＤホールディングスは、情報セキュリティに対し、
以下に定める行動指針のもと、適切な対策を講じることにより、
お客様をはじめ社会からの信頼を得られるよう努めます。

＜行動指針＞

1. 情報資産の機密性、完全性、可用性を確実に保護するために組織的、技術的に適切な対策を講じ、変化する情報技術や新たな脅威に対応する。

2. 全社員に情報セキュリティ教育の実施と方針の周知徹底をはかり、意識の高揚・維持に務める。

3. 情報セキュリティに関連する法令及び要求事項を遵守する。

4. 情報セキュリティに関する目的を設定し、定期的にレビューし、継続的に改善する。

制定日 2023 年 8 月 30 日
株式会社ＳＤホールディングス
代表取締役社長　大熊　基由

5.3　組織の役割、責任及び権限

社長は、関連する役割に対して、責任及び権限を割り当て、組織内に伝達することを確実にする。組織の役割、責任及び権限については「ISMS 体制図」に明記する。

6　ISMS の計画

6.1.1　一般

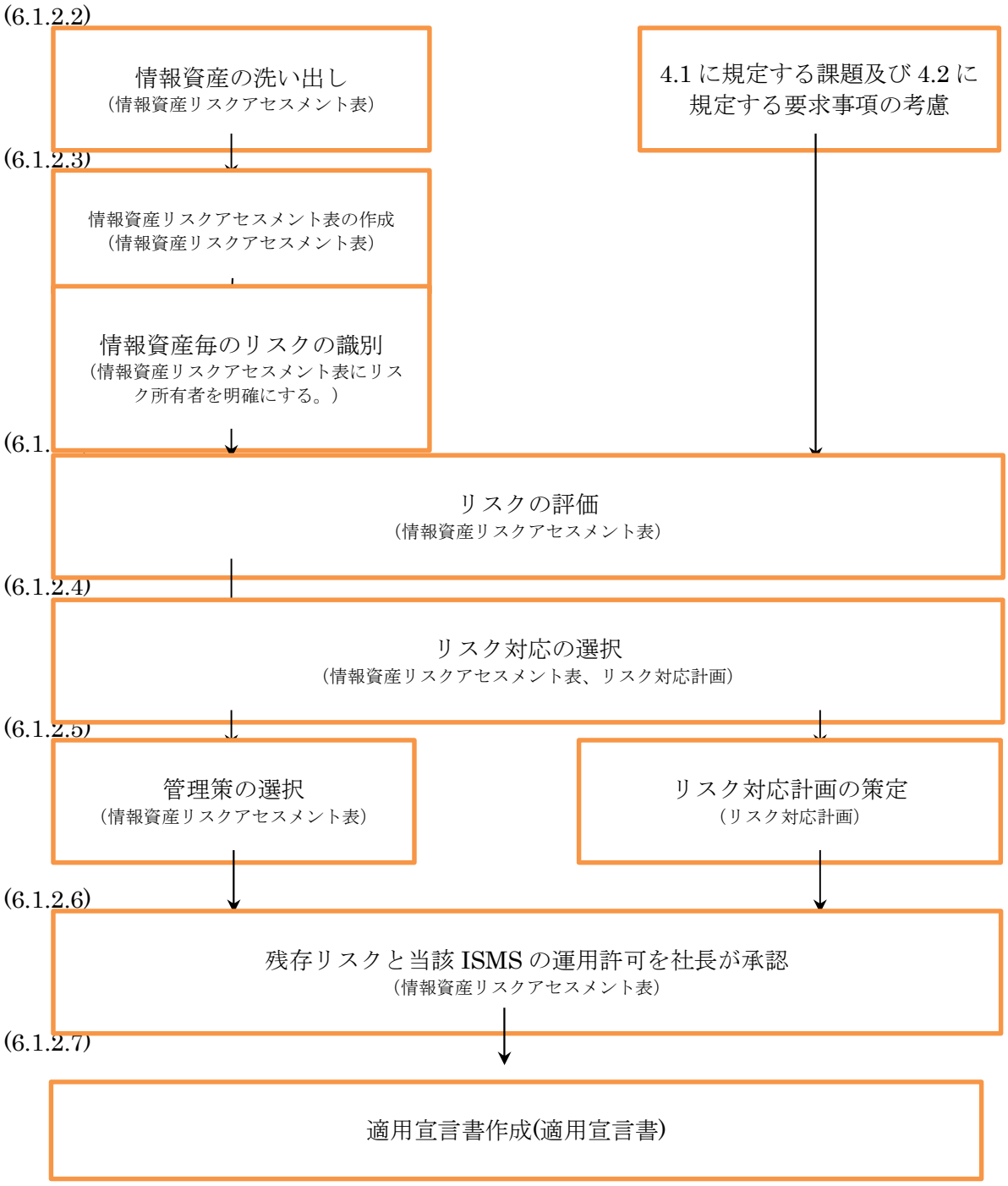
ISMS の計画を策定するとき、組織は、4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、次の事項のために対処する必要があるリスク及び機会を決定する。
(1)本マニュアルにおいて、組織が意図した成果を達成できることを確実にする。
(2)当社に置いて望ましくない影響を防止又は低減する。
(3)本マニュアル 10.2 項に従い継続的改善を達成する。
(4)上記(1)~(3)によって決定したリスク及び機会に対処する活動を「リスク対応計画」に計画する。
(5)ISMS プロセスへの統合及び実施/その活動の有効性評価を「リスク対応計画」に計画する。

6.1.2　情報セキュリティリスクアセスメント

事務局は、情報資産に対するリスクを、結果の重大性（推定される損害）、脅威、脆弱性の観点から定量化し、「情報資産リスクアセスメント表」に記入する。また、このリスクアセスメントには、前項 4.1 に規定する課題及び 6.1.2.1 に規定する要求事項の考慮も含める。
情報資産リスクアセスメント表には、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定することとする。

6.1.2　情報セキュリティリスク対応

当社は、次の事項を行うために、情報セキュリティリスク対応のプロセスを以下に定める。



6.1.2.1　リスク受容基準、リスク所有者の選択

6.1.2.2　情報資産の洗い出し

6.1.2.3　リスクの評価

6.1.2.4　リスク対応の選択

6.1.2.5　管理策の選択

上記 6.1.2.2～6.1.2.5 6.1.3 項については、「情報資産リスクアセスメント表」を参照。

6.1.3　情報セキュリティリスク対応

当社は、次の情報セキュリティリスクアセスメントのプロセスを明確にし、適用しなければならない。

a）当社は、次の情報セキュリティリスク対応プロセスを定め、適用しなければならない。

b）決定した情報セキュリティリスク対応の選択肢として必要な管理策を決めるプロセス.

c）6.1.3 b）で決めた管理策を附属書Aに示す管理策と比較し、必要な管理策の見落しが無いことを検証するプロセス。

d）適用宣言書を作成するプロセス。適用宣言書には、必要とした管理策（6.1.3 の b）及び c）参照）、それらの管理策を必要とした理由、それらの管理策を実施しているか否か、附属書Aに規定する管理策を除外した理由の記載を含む。

e）情報セキュリティリスク対応計画を策定するプロセス。

f）情報セキュリティリスク対応計画、及び、残留している情報セキュリティリスクの受容について、リスクのオーナーの承認を得るプロセス。

当社は、情報セキュリティリスク対応のプロセスを“情報資産リスクアセスメント表”として保持する。

6.2　情報セキュリティ目的及びそれを達成するための計画策定

組織は、管理責任者の管轄の下、部門及び階層に対して、次の手順で情報セキュリティ目的を設定させ、これを監視し、伝達し、文書化した情報として利用可能な状態にする。ただし、情報セキュリティ目的は達成したかどうかがわかる状態とし、情報セキュリティに関する方針に整合していること。

※部門ごとによる目的及び計画を策定するかどうかは、随時経営層が判断し、決定を行う。

担当	時期	手順	記録
管理責任者	年１回	情報資産リスクアセスメントの実施後、「リスク対応計画」により測定可能なリスク対応にて情報セキュリティ目的を設定し、「目的管理兼リスク対応計画表」に文書化する。	「目的管理兼リスク対応計画表」
管理責任者		1.　「目的管理兼リスク対応計画表」の内容を確認し、承認をする。 2.　その後、情報セキュリティ目的を伝達する。	「目的管理兼リスク対応計画表」
各担当	毎月	1.　「目的管理兼リスク対応計画表」通りに業務を実施する。 2.　活動した結果を「目的管理兼リスク対応計画表」に記録する。	「目的管理兼リスク対応計画表」
管理責任者	マネジメントレビュー	1. マネジメントレビュー開催の前に、管理責任者に「目的管理兼リスク対応計画表」を提出させる。 2. マネジメントレビューのタイミングで経営者に目標の達成状況を報告する。 3. 目標の設定等に対して指示がある場合は、「マネジメンレビュー議事録」のアウトプット欄にまとめておき、目的設定へのインプットとする。	「マネジメンレビュー議事録」

6.3　変更の計画策定

組織が ISMS の変更の必要があると決定したとき、その変更は、計画的な方法で行わなければならない。

7 .ISMS の支援

7.1　資源

組織は、ISMS の確立、実施、維持及び継続的改善に必要な資源を決定し、提供しなければいけない。

7.2　力量

当社では次の事項をルールとし、実行する。

(1)サービス提供における要求事項の適合に必要な力量を OJT の実施、勉強会の実施、現場観察により明確にする。
(2) 教育、訓練、技能及び経験について該当する記録（教育計画実績表）を維持する。
(3) 新人採用の場合も上記と同じように記録を維持する。

7.3　認識

組織の管理下で働く人々は、「情報セキュリティに関する方針」、自らの貢献、自社で要求する罰則に関して認識をもたなければならない。

7.4　コミュニケーション

経営者は、当社で必要な次のコミュニケーション（内部および外部）が確実に行われるようにコミットする。

実施 プロセス	実施時期	内容	対象
マネジメント レビュー	年１回	内容：情報セキュリティマネジメントシステム有効性と改善、・情報セキュリティに関する方針や情報セキュリティ目的の見直しの必要性、資源の必要性指示、本マニュアル 9.3 項のインプット、アウトプット項目	社長 管理責任者 事務局
ミーティング	月一回	今月の作業内容確認、注意事項の周知	管理責任者 事務局

7.5.1　文書化した情報

当社における情報セキュリティマネジメントシステム（ISMS）は、次の事項を確実にする。

(1)ISO27001 の規格が要求事項する文書化された情報

(2)情報セキュリティマネジメントシステム（ISMS）の有効性のために必要であると本マニュアル１

(4)適用プロセスに当社が決定した、文書化された情報

7.5.2　作成及び更新（改訂）

文書の作成、審査、承認は以下の表の通りとする。なお、文書の最新版、媒体、保管場所について、以下に記す

文書 分類	文書名	媒体	起案 (作成・改訂)	承認
文書 A	情報セキュリティに関する方針	紙/データ	管理責任者	社長
	適用宣言書	紙/データ	管理責任者	社長
	ISMS マニュアル	紙/データ	管理責任者	社長
	情報セキュリティ管理規程	紙/データ	管理責任者	社長
文書 B (様式	情報資産リスクアセスメント表	紙/データ	事務局メンバー	管理責任者
	リスク対応計画	紙/データ	事務局メンバー	管理責任者
	目的管理兼リスク対応計画表	紙/データ	事務局メンバー	管理責任者
	事業継続計画・結果	紙/データ	事務局メンバー	管理責任者
	内部監査チェックリスト	紙/データ	事務局メンバー	管理責任者
	内部監査計画・結果	紙/データ	事務局メンバー	管理責任者
	ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ議事録	紙/データ	事務局メンバー	管理責任者
	法令管理表	紙/データ	事務局メンバー	管理責任者

※情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を、管理するために、管理責任者が確認する。

7.5.3　文書化した情報の管理

当社は文書化した情報は、次の事項を確実にするため管理する
(1)文書化した情報が、必要な時に、必要なところで、入手可能かつ利用に適した状態である。
(2)文書化した情報が十分に保護されている

また、文書化した情報の管理に当たって、文書の改訂、変更があった場合には以下の事項をしなければいけない。
(1)誰でも検索、閲覧可能なサーバに保管を行う。
(2)誰でも読みやすい状態で保管、保存を行う
(3)改訂履歴に改定内容など記載し、版番号によって最新版の管理を行う。
(4)古い版に関しては「旧版」のフォルダに入れる、または削除を行うなど旧版と混同してしまう状態をなくす。また、顧客及び法令等の特別な要求がない限り、文書・記録の保管期限は最低 5 年とする。

8.運用

8.1　運用の計画及び管理

当社は、情報セキュリティ要求事項を満たすため、及び箇条 6 で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。また、6.2 で決定した情報セキュリティ目的達成するための計画を管理責任者が毎年 5 月に実施する。

- プロセスに関する基準の設定
- その基準に従った、プロセスの管理の実施

(1)当社は、プロセスが計画通りに実施されたという確信をもつために必要な程度の文書化した情報を利用可能な状態にしなければならない。
(2)当社は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置を取らなければならない。
(3)当社は、外部委託したプロセスが決定され、かつ、管理されていることを確実にしなければならない。

8.2　情報セキュリティリスクアセスメント

当社は、あらかじめ定めた間隔で、又は重大な変更が提案されたか若しくは重大な変化が生じた場合に、6.1.2 情報セキュリティリスクアセスメントで確立した基準を考慮して、情報セキュリティリスクアセスメントを実施しなければならない。

8.3　情報セキュリティリスク対応

当社は、セキュリティリスク対応計画を実施し、実施した結果を記録として保管する。

9 .ISMS のパフォーマンス評価

9.1　監視、測定、分析及び評価

当社では、下表にて、管理策及び情報セキュリティプロセスが計画通りの能力が発揮できるかを監視する。

監視、測定、分析および評価 プロセス	何を持って監視、測定、分析、評価を行うか	時期	評価及び分析実施者	監視及び測定の実施者
方針・目的の達成度	目的管理兼リスク対応計画表	随時	管理責任者	管理責任者
ISMS の適合性（社内のルール、法令・お客様からの要求等含む）	内部監査チェックリスト	年一度	監査員	監査員
リスク対応計画の実施状況	リスク対応計画	リスク対応計画対応時期に評価	管理責任者	管理責任者
ISMS 運用の有効性評価	マネジメントレビュー	年一度	管理責任者	管理責任者

当社は監視及び測定の結果の証拠として文書化した情報を利用可能な状態にしなければならない。

9.2　内部監査の手順

9.2.1　一般

当社は、ＩＳＭＳが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施する。

a)　次の事項に適合している。

1)　ＩＳＭＳに関して、当社自体が規定した要求事項

2)　この規格の要求事項

b)　有効に実施され、維持されている。

9.2.2　内部監査プログラム

当社は、監査プログラムを計画し、確立し、実施し、維持する。これには、その頻度、方法、責任、計画策定の要求事項及び報告を含める。

その内部監査プログラムを確立するとき、当社は、関連するプロセスの重要性及び前回までの監査の結果を考慮する。

当社は、次に示す事項を行う。

a)　各監査について、監査基準及び監査範囲を明確にする。

b)　監査プロセスの客観性及び公平性を確保するために、監査員を選定し、監査を実施する。

c)　監査の結果を関連する管理層に報告することを確実にする。

当社は、下記に従い監査対象となる部門の状況や重要性等を考慮し、監査プログラムの実施及び監査結果の証拠として、「内部監査計画・結果」、「内部監査チェックリスト」を作成する。

担当	時期	手順	記録
管理責任者	年１回 (1 月～3 月)	・内部監査の詳細実施時期を決定し、監査リーダーに指示する	／
監査リーダー	監査１ヶ月前	・「内部監査計画・結果」にて内部監査の計画を作成し、管理責任者に提出する。	「内部監査計画・結果」

担当	時期	手順	記録
管理責任者		・「内部監査計画・結果」の内容を確認して承認する。	「内部監査計画・結果」
監査リーダー	監査１週間前	・監査の時期を再確認も含めて、各部門に連絡する。	／
監査チーム	監査中	・監査を実施し、監査のメモを残す。	「チェックリスト」
監査チーム	監査終了後	・内部監査時の「チェックリスト」を基に、管理責任者が不適合を決定する。不適合は「是正処置報告書」に明確にする。 ・「是正処置報告書」を各部門に提示し、不適合の内容について同意が得られれば、被監査部署に「是正処置報告書」を引き渡す。監査時に発生した不適合に関してはマネジメントレビューにて共有することとする	「内部監査計画・結果」 「是正処置報告書」 「チェックリスト」

「是正処置報告書」の作成手順については、10.1 不適合及び是正処置に従う。

当社の内部監査は次の概要で行います。

①基準　･･･　「不適合」「推奨」について以下の基準を設ける。
「不適合…ISMS が機能していない状態、またはシステムは機能しているが､要求事項には適合していない状態」
「推奨…不適合ではないが､そのまま放置すれば不適合になるおそれのある状態、または今後より運用しやすくなる状態」
②範囲　･･･　当マニュアルにある組織図の部門に適用。
③頻度　･･･　原則、年１回監査リーダー、監査担当により実施。
④方法　･･･　文書監査、現場訪問監査の２つの方法を活用。

また監査員が、監査業務の客観性、公平性を確保できるように、自部署の責任者は自部門を監査できないように監査員を選定する。監査員の力量については、業務経験及び情報セキュリティの知識を考慮した上で、社長が選定し、「教育訓練記録・力量表」にて明確にすること。
最終的に、監査で残された記録類は、保管する。

9.3　マネジメントレビュー

9.3.1　一般

経営層は、組織の ISMS が、引き続き、適切、妥当、かつ有効であることを確実にするために、あらかじめ定めた感覚で、ISMS をレビューしなければならない。

9.3.2　マネジメントレビューへのインプット

マネジメントレビューを通して収集する情報は次の通りとし、結果を「マネジメントレビュー議事録」に記録する。

a) 前回までのマネジメントレビューの結果とった処置の状況
b) ISMS に関連する外部及び内部の課題の変化
c) ISMS に関連する利害関係者のニーズ及び期待の変化
d) 次に示す傾向を含めた、情報セキュリティパフォーマンスに関するフィードバック

1) 不適合及び是正処置

2) 監視及び測定の結果
3) 監査結果
4) 情報セキュリティの目的の達成

e) 利害関係者からのフィードバック
f) リスクアセスメントの結果及び目的管理兼リスク対応計画表の状況
g) 継続的改善の機会
h) その他報告事項

9.3.3　マネジメントレビューの結果

マネジメントレビューから結果には、継続的改善の機会、及び ISMS のあらゆる変更の必要性に関する決定を含める。マネジメントレビューの結果の証拠として、「マネジメントレビュー議事録」に記録する。また、マニュアル 5.2 項に定めた情報セキュリティ方針が妥当・正確、確実であることを確認するため、「マネジメントレビュー」において見直しをする。

１０　ISMS の改善

10.1　継続的改善

当社は、情報セキュリティマネジメントシステム（ISMS）の適切性、妥当性及び有効性を継続的に改善するために、以下の活動を行う。

(1)ISMS の実施状況の監視結果（外部／内部監査結果、日常点検、セキュリティインシデントの反省、顧客要求など）に基づく是正処置の実施
(2)当社 ISMS の枠組みについての見直しによる改善（マネジメントシステムレビュー、文書の見直し）
(3)セキュリティ目標の達成と、さらなるセキュリティレベルの向上を目指した目標の設定
(4)外部及び内部の課題の変化に対応したリスクアセスメント及び計画
（リスクアセスメント、目的管理、リスク対応計画表の見直しなど）

10.2　不適合及び是正処置

管理責任者及び実行部門長は、実際に発生した不適合及び潜在的な不適合の原因を除去するための調査及び処置を行い、不適合によって生じるあらゆる影響を緩和する処置を講じ、さらに是正処置を取らねばならない。その手順は以下の通りとする。

手順	担当者	実施内容	関連文書
不適合の特定	管理責任者 部門長	■不適合の基準は以下の項目 ①運用管理に関わる遵守状況に関する項目 ②順法に関する項目 ■上記項目に達成していない内容の場合不適合とする。	本マネジメントマニュアル
不適合の発生及び予測	管理責任者 部門長	■不適合の扱い（是正対象）基準 ①運用管理項目、苦情、その他によって管理責任者が不適合是正を必要と判断した場合。 ②法規制違反が認められた場合 ③内部監査で指摘があった場合	本マネジメントマニュアル
原因調査	同上	■不適合が発生した原因を追究する。	是正処置報告書
是正処置 ▲	同上	■是正処置と共に監視・測定による効果測定を行う ■類似の不適合の有無、またはそれが発生する可能性の有無を確認	是正処置報告書
是正内容の確認	同上	■是正内容の妥当性、有効性を判断する ■必要に応じて、文書化された手順に変更があった場合は記録する（ISMS の変更）	是正処置報告書
承認	管理責任者	■記載された内容について確認を行い、承認する。	是正処置報告書
記録の保管	事務局	■定められた期間記録原則３年間保管する。	是正処置報告書