情報セキュリティ
マネジメントシステム
マニュアル

株式会社ＳＤホールディングス

制定日	2023/03/01
改定日	2023/09/25

改訂歴表　～

版番号	発行年月日	改　訂　内　容
01	23/3/1	新規制定：初版発行
02	23/9/25	全文を JIS Q 27001 へ対応するよう見直し

目次

0.　序文

本マニュアルは、JIS Q 27001：2014（ISO/IEC 27001：2013）（以下、準拠する規格という）は、2013 年に第 2 版として発行された ISO/IEC 27001 を基に，技術的内容及び構成を変更することなく作成した日本工業規格に準拠し、制定する。

0.1　概要

準拠する規格は、情報セキュリティマネジメントシステム（以下，ISMS という）を確立し，実施し，維持し，継続的に改善するための要求事項を提供するために作成された。ISMS の採用は，組織の戦略的決定である。組織の ISMS の確立及び実施は，その組織のニーズ及び目的，セキュリティ要求事項，組織が用いているプロセス，並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらの要因全ては，時間とともに変化することが見込まれる。

ISMS は，リスクマネジメントプロセスを適用することによって情報の機密性，完全性及び可用性を維持し，かつ，リスクを適切に管理しているという信頼を利害関係者に与える。

ISMS を，組織のプロセス及びマネジメント構造（management structure）全体の一部とし，かつ，その中に組み込むこと，並びにプロセス，情報システム及び管理策を設計する上で情報セキュリティを考慮することは，重要である。ISMS の導入は，その組織のニーズに合わせた規模で行うことが期待される。

準拠する規格は，組織自身の情報セキュリティ要求事項を満たす組織の能力を，組織の内部で評価するためにも，また，外部関係者が評価するためにも用いることができる。

準拠する規格で示す要求事項の順序は，重要性を反映するものでもなく，実施する順序を示すものでもない。

ISO/IEC 27000 は，ISMS ファミリ規格（ISO/IEC 27003，ISO/IEC 27004 及び ISO/IEC 27005 を含む。）を参照しながら，ISMS の概要について記載し，用語及び定義について規定している。

0.2　他のマネジメントシステム規格との両立性

準拠する規格は，ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針の附属書 SL に規定する上位構造（HLS），共通の細分箇条題名，共通テキスト並びに共通の用語及び中核となる定義を適用しており，附属書 SL を採用した他のマネジメントシステム規格との両立性が保たれている。

附属書 SL に規定するこの共通の取組みは，二つ以上のマネジメントシステム規格の要求事項を満たす一つのマネジメントシステムを運用することを選択する組織にとって有用となる。

１．適用範囲

このマニュアルは，組織の状況の下で，ISMS　を確立し，実施し，維持し，継続的に改善するための要求事項について規定する。

このマニュアルは，組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項についても規定する。

このマニュアルが規定する要求事項は，汎用的であり，形態，規模又は性質を問わず，全ての組織に適用できることを意図している。

組織がこの規格への適合を宣言する場合には，以下の 4.～10.に規定するいかなる要求事項の除外も認められない。

当社所在地（適用拠点）にておこなう以下の業務に適用する。

①適用業務

ホールディング企業の管理業務

②適用組織

「組織図」に明確にする。

③適用拠点

拠点	住所
本社	東京都渋谷区東 3-16-3　エフ・ニッセイ恵比寿ビル 7F

２．　引用規格

次に掲げる規格は，このマニュアルに引用されることによって，このマニュアルの規定の一部を構成する。この引用規格は，その最新版（追補を含む。）を適用する。

JISQ27001（情報技術 - セキュリティ技術 - ISMS - 要求事項）

JISQ27002

３．　用語及び定義

このマニュアルで用いる主な用語及び定義は，JIS Q 27000 による。

４．　組織の状況

4.1　組織及びその状況の理解

組織（以下、当社という）は，当社の目的に関連し，かつ，その ISMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定する。

4.2　利害関係者のニーズ及び期待の理解

当社は，次の事項を決定する。

a)ISMS に関連する利害関係者

b)その利害関係者の，情報セキュリティに関連する要求事項

当社の利害関係者とは、以下とし、利害関係者の要求事項には，法的及び規制の要求事項並びに契約上の義務を含める。

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

4.3　情報セキュリティマネジメントシステムの適用範囲の決定

当社は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定する。この適用範囲を決定するとき，当社は，次の事項を考慮する。

a)4.1 に規定する外部及び内部の課題

b)4.2 に規定する要求事項

c)組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

ISMS の適用範囲は，文書化した情報として利用可能な状態にする。

4.4　情報セキュリティマネジメントシステム

当社は，このマニュアルの要求事項に従って，ISMS を確立し，実施し，維持し，かつ，継続的に改善する。

５．　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

トップマネジメントは，次に示す事項によって，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。

a)情報セキュリティ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。

b)当社のプロセスへの ISMS 要求事項の統合を確実にする。

c)ISMS に必要な資源が利用可能であることを確実にする。

d)有効な情報セキュリティマネジメント及びISMS 要求事項への適合の重要性を伝達する。
e)ISMS がその意図した成果を達成することを確実にする。
f)ISMS の有効性に寄与するよう人々を指揮し，支援する。
g)継続的改善を促進する。
h)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実証するよう，管理層の役割を支援する。

5.2　方針

トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立する。
a)当社の目的に対して適切である。
b)情報セキュリティ目的を含むか，又は情報セキュリティ目的の設定のための枠組みを示す。
c)情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。
d)ISMS の継続的改善へのコミットメントを含む。

情報セキュリティ方針は，次に示す事項を満たさなければならない。
e)文書化した情報として利用可能である。
f)当社内に伝達する。
g)必要に応じて，利害関係者が入手可能である。

5.3　組織の役割、責任及び権限

トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権限を割り当て，伝達することを確実にする。

トップマネジメントは，次の事項に対して，責任及び権限を割り当てる。
a)ISMS が，この規格の要求事項に適合することを確実にする。
b)ISMS のパフォーマンスをトップマネジメントに報告する。

割り当てた責任及び権限は「組織図」にて明示し社内に周知する。

６．　計画

6.1　リスク及び機会に対処する活動

6.1.1　一般

ISMS の計画を策定するとき，当社は，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。
a)ISMS が，その意図した成果を達成できることを確実にする。
b)望ましくない影響を防止又は低減する。
c)継続的改善を達成する。

また、当社は，次の事項を計画する。

d)上記（a）～c)）によって決定したリスク及び機会に対処する活動

e)次の事項を行う方法

1)その活動の ISMS プロセスへの統合及び実施

2)その活動の有効性の評価

6.1.2　情報セキュリティリスクアセスメント

当社は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用する。

a)次を含む情報セキュリティのリスク基準を確立し，維持する。

1)リスク受容基準

2)情報セキュリティリスクアセスメントを実施するための基準

b)繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。

c)次によって情報セキュリティリスクを特定する。

1)ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。

2)これらのリスク所有者を特定する。

d)次によって情報セキュリティリスクを分析する。

1)6.1.2 c) 1)で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2)6.1.2 c) 1)で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3)リスクレベルを決定する。

e)次によって情報セキュリティリスクを評価する。

1)リスク分析の結果と 6.1.2 a) で確立したリスク基準とを比較する。

2)リスク対応のために，分析したリスクの優先順位付けを行う。

当社は、情報セキュリティリスクアセスメントのプロセスについての文書化した情報として「情報資産リスクアセスメント表」を保持する。

6.1.3　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定め，適用する。

a)リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する。

b)選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。

c)6.1.3 b) で決定した管理策を準拠する規格の附属書 A に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。

d)次を含む適用宣言書を作成する。

－　必要な管理策［6.1.3 の b) 及び c) 参照］

－　それらの管理策を含めた理由

－　それらの必要な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

e)情報セキュリティリスク対応計画を策定する。

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，リスク所有者の承認を得る。

当社は，情報セキュリティリスク対応のプロセスについての文書化した情報として「リスク対応計画」を保持する。

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

当社は，関連する部門及び階層において，情報セキュリティ目的を確立する。

情報セキュリティ目的は，次の事項を満たしたものとする。

a)情報セキュリティ方針と整合している。

b)（実行可能な場合）測定可能である。

c)適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。

d)伝達する。

e)必要に応じて，更新する。

当社は，情報セキュリティ目的に関する文書化した情報を保持する。

当社は，情報セキュリティ目的をどのように達成するかについて計画するとき，次の事項を決定する。

f)実施事項

g)必要な資源

h)責任者

i)達成期限

j)結果の評価方法

７．　支援

7.1　資源

当社は，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，提供する。

7.2　力量

当社は，次の事項を行う。

a)当社の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。

b)適切な教育,訓練又は経験に基づいて,それらの人々が力量を備えていることを確実にする。

c)該当する場合には，必ず，必要な力量を身につけるための処置をとり，とった処置の有効性を評価する。

d)力量の証拠として，適切な文書化した情報として、「スキルマップ」を保持する。

7.3　認識

当社の管理下で働く人々に，次の事項に関して認識をもたなければならない。

a)情報セキュリティ方針

b)情報セキュリティパフォーマンスの向上によって得られる便益を含む,ISMS の有効性に対する自らの貢献

c)ISMS 要求事項に適合しないことの意味

7.4　コミュニケーション

当社は，次の事項を含め，ISMS に関連する内部及び外部のコミュニケーションを実施する必要性を決定する。

a)コミュニケーションの内容（何を伝達するか。）

b)コミュニケーションの実施時期

c)コミュニケーションの対象者

d)コミュニケーションの実施者

e)コミュニケーションの実施プロセス

内部コミュニケーションについては、下表に示す通り実施する。

また、外部コミュニケーションについては、都度実施し、必要に応じて記録を作成する。

手段	対象	時期	内容
マネジメントレビュー	社長 管理責任者 事務局	年１回	・9.3　マネジメントレビュー　参照
ミーティング	管理責任者 事務局	月１回	・今月の作業内容確認、注意事項の周知

7.5　文書化した情報

7.5.1　一般

当社の ISMS は，次の事項を含むものとする。

a)このマニュアルが要求する文書化した情報

b)ISMS の有効性のために必要であると組織が決定した，文書化した情報

1)当社の規模，並びに活動，プロセス，製品及びサービスの種類

2)プロセス及びその相互作用の複雑さ

3)人々の力量

7.5.2　作成及び更新

文書化した情報を作成及び更新する際，組織は，次の事項を確実にする。

a)適切な識別及び記述（例えば，タイトル，日付，作成者，参照番号）

b)適切な形式（例えば，言語，ソフトウェアの版，図表）及び媒体（例えば，紙，電子媒体）

c)適切性及び妥当性に関する，適切なレビュー及び承認

7.5.3　文書化した情報の管理

ISMS 及びこのマニュアルで要求する文書化した情報は,次の事項を確実にするために,管理する。

a)文書化した情報が，必要なときに，必要なところで，入手可能かつ利用に適した状態である。

b)文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用及び完全性の喪失からの保護)。

文書化した情報の管理に当たって，当社は，該当する場合には，必ず，次の行動に取り組む。

c)配付，アクセス，検索及び利用

d)読みやすさが保たれることを含む，保管及び保存

e)変更の管理（例えば，版の管理）

f)保持及び廃棄

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 6.1 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，かつ管理しなければならない。

また，当社は，6.2 で決定した情報セキュリティ目的を達成するための計画を実施する。

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，文書化した情報を保持する。

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とる。

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「情報セキュリティマネジメントシステム管理規程」にて確実にする。

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（定期的には年１回（　））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 a）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する。

当社は，情報セキュリティリスクアセスメント結果の文書化した情報として「リスク対応計画」

を保持する。

8.3　情報セキュリティリスク対応

当社は，情報セキュリティリスク対応計画を実施する。

当社は，情報セキュリティリスク対応結果の文書化した情報として「リスク対応計画」を保持する。

９．　パフォーマンス評価

9.1　監視、測定、分析及び評価

当社は，情報セキュリティパフォーマンス及び ISMS の有効性を評価する。

当社は，次の事項を決定する。

a)必要とされる監視及び測定の対象。これには，情報セキュリティプロセス及び管理策を含む。

b)該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法（選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい。）

c)監視及び測定の実施時期

d)監視及び測定の実施者

e)監視及び測定の結果の，分析及び評価の時期

f)監視及び測定の結果の，分析及び評価の実施者

当社は，監視及び測定の結果の証拠として，適切な文書化した情報を保持する。

9.2　内部監査

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（定期的には年１回（　））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，組織自体が規定した要求事項

2)このマニュアルの要求事項

b)有効に実施され，維持されている。

当社は，次に示す事項を行う。

c)頻度，方法，責任及び計画に関する要求事項及び報告を含む，監査プログラムの計画，確立，実施及び維持。監査プログラムは，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に入れたものとする。

d)各監査について，監査基準及び監査範囲を明確に定め、「内部監査報告書」「内部監査チェックリスト」に記録する。

e)監査プロセスの客観性及び公平性を確保するために、自部門の監査を実施しないよう監査員を選定し，監査を実施する。監査員の選定基準は、代表者が当社業務及び ISMS 要求事項を理解し、力量があると評価されたもの、又は、外部委託の専門家とする。

f)監査の結果を「内部監査報告書」に記録し関連する管理層に報告することを確実にする。
g)監査プログラム及び監査結果の証拠として，文書化した情報として「内部監査報告書」「内部監査チェックリスト」を保持する。

9.3　マネジメントレビュー

トップマネジメントは，当社の 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，あらかじめ定めた間隔（定期的には年１回（　））で，ISMS をレビューする。

マネジメントレビューは，次の事項を考慮する。

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)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)情報セキュリティ目的の達成
d)利害関係者からのフィードバック
e)リスクアセスメントの結果及びリスク対応計画の状況
f)継続的改善の機会

マネジメントレビューからのアウトプットには，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。

当社は，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」を保持する。

１０．　改善

10.1　不適合及び是正処置

不適合が発生した場合，当社は，次の事項を行う。

a)その不適合に対処し，該当する場合には，必ず，次の事項を行う。
　1)その不適合を管理し，修正するための処置をとる。
　2)その不適合によって起こった結果に対処する。
b)その不適合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置をとる必要性を評価する。
　1)その不適合をレビューする。
　2)その不適合の原因を明確にする。
　3)類似の不適合の有無，又はそれが発生する可能性を明確にする。
c)必要な処置を実施する。
d)とった全ての是正処置の有効性をレビューする。

e)必要な場合には，ISMS の変更を行う。

是正処置は，検出された不適合のもつ影響に応じたものでなければならない。

当社は，次に示す事項の証拠として，文書化した情報を保持する。

f)不適合の性質及びとった処置

g)是正処置の結果

10.2　継続的改善

当社は，ISMS の適切性，妥当性及び有効性を継続的に改善する。

以上