配 付 番 号 ：

管　理　区　分
管　理　文　書

文書番号	ISMS-A-03
制 定 日	2020.03.01
改 訂 日	
改訂番号	1

【編集可能!】ISMS マニュアル

ＪＩＳ Ｑ ２７００１：２０１４ 適用

（ ＩＳＯ/ＩＥＣ ２７００１：２０１３ ）

承　　認	作　　成

株式会社　サンプル

目　　次

改訂歴表

1　適用範囲

当社は、「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-要求事項」（以下ISO27001）に準拠した情報セキュリティを構築する。

本マニュアルは、当社の ISMS の確立、導入、運用、監視、見直し、維持及び改善の枠組みを規定する。

(1) 適用事業

・ソフトウェア受託開発

・パッケージソフトウェア開発・販売・保守・導入支援

・ハードウェア受託開発

(2) 適用組織

別紙、組織図で示す組織

(3) 適用事業所

【事業所名】　○○　　【事業所住所】○○

【事業所名】　○○　　【事業所住所】○○

(4) 適用範囲から除外される業務

適用範囲内でありながらその一部を適用除外する場合、その内容と除外する正当な理由を明示する。

2　引用規格

JISQ27000:2019/ISO27000:2018　「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」

3　用語及び定義

本マニュアルに関する用語の定義は、JISQ27000:2019 に従うが、定義が必要なものについては、下記に定義する。

(1) 従業員：当法人の役員、社員、契約社員、嘱託、パート、アルバイトを含む ISMS 適用範囲内の全社員
(2) 経営陣：社長及び役員
(3) ISMS 推進委員会：情報セキュリティの施策を審議し、決定する委員会

4　組織の状況

4.1　組織及びその状況の理解

ISMS 推進委員会は、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し、**「リスク一覧表」**に示す。

4.2　利害関係者のニーズ及び期待の理解

ISMS 推進委員会は、顧客等をはじめとする利害関係者を特定し、それらの要求事項および法的及び規制要求事項を以下に示し、決定する。

利害関係者	情報セキュリティに関する要求事項
顧客	契約上の義務（契約書） 情報の機密性・完全性・可用性の確保
従業員	業務情報の機密性・完全性・可用性の確保 個人情報の保護
政府・行政・国民	情報セキュリティに関する法令（法的要求事項登録簿）

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、以下に事項を考慮して、適用範囲を決定し、決定した適用範囲は、文書化した情報として利用可能な状態にしておく。

(1) 4.1 に規定する外部及び内部の課題

(2) 4.2 に規定する要求事項

(3) 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ーフェース及び依存関係

4.4　情報セキュリティマネジメントシステム（ISMS）

当社は、ISO27001:2013（JISQ27001:2014）の要求事項に従って、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　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）の有効性に寄与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者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、その管理者の役割を支援する。

5.2　方針

社長は、次の事項を満たす**「情報セキュリティ基本方針」**を制定し、文書化して利用可能とし、組織内に伝達する。また、必要に応じて、利害関係者が入手可能であるようにする。

(1) 組織の目的に対して適切である。

(2) 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。

(3) 情報セキュリティに関連して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。

(4) 情報セキュリティマネジメントシステム（ISMS）の継続的改善へのコミットメントを含む。

IS-A-01

情報セキュリティ基本方針

制定：2020 年 3 月 01 日

【基本理念】

株式会社●●は、コスト削減や業務効率向上を図るには IT は欠かせないツールであり、そのITの活用において､情報セキュリティの確保が重要課題のひとつであると考えます。本方針は、当社の情報セキュリティマネジメントシステム（ISMS）を適切に構築し、継続的で有効性のある運用を確保するために、以下に情報セキュリティ基本方針を制定します。

【基本方針】

1. 情報資産の機密性、完全性、可用性を確実に保持するため、予防並びに是正に努め、組織的、技術的に適切な管理策を策定し、実施します。

2. 情報セキュリティ基本方針を具体的に実行するため、情報セキュリティ目標を設定し､その達成のための活動を行い､情報セキュリティ委員会で検証を行います。

3. 関連する法規制要求事項および契約上のセキュリティ事項を順守します。

4. 経営陣および従業員は情報セキュリティの重要性を認識するように、教育・訓練を受講し、高いモラル意識を持って作業に従事します。

5. 本「情報セキュリティ基本方針」および関連する諸規則、管理体制の評価、見直しを定期的に行うことで、情報セキュリティを運営管理する仕組みの継続的な改善を図ります。

以　上

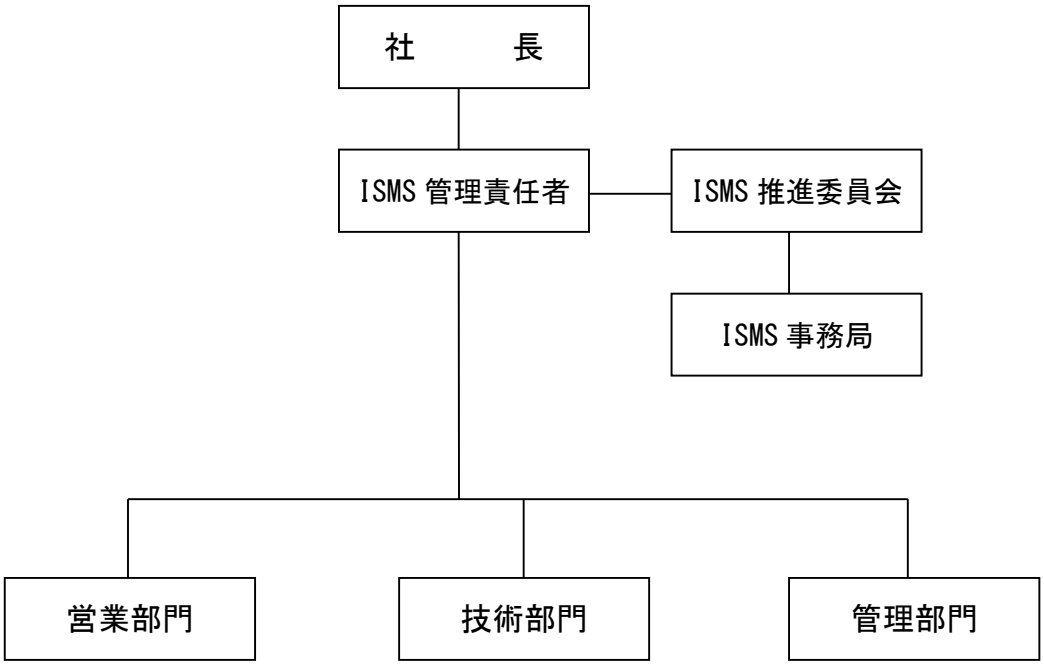
株式会社　●●
代表取締役社長　●●

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、以下のような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。

5.3.1　推進組織

情報セキュリティマネジメントシステム（ISMS）を推進するための組織を以下に定める。



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、前項 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、次の事項について対処する必要があるリスク及び機会を決定し、**「リスク一覧表」**に記入する。

(1) ISMS が、その意図した成果を達成できることを確実にする。

(2) 望ましくない影響を防止、又は低減する。

(3) 継続的改善を達成する。

(4) 決定したリスク及び機会に対処する活動を計画する。

(5) 計画された活動は、ISMS プロセスへの統合及び実施を行う。

(6) 計画された活動の有効性評価を行う。

6.1.2　情報セキュリティリスクアセスメントの手法と受容基準

※参考情報：「ISMS ユーザーズガイド　リスクマネジメント編」

(1) リスクアセスメント手法

6.1.2 以下に示す方法でリスクアセスメントを実施する。

(2) リスク受容の基準

当社は下記の考え方で、リスクを受容する。

① 6.1.5 で計算したリスク値が「6」以下のリスクは受容（保有）する。

② リスク値が「8」「9」の場合は、該当する情報資産、脅威を考慮して状況に応じて、受容するか否かを決定する。

③ リスク値が「10」以上の場合、6.1.5 に記すように、「管理策を採用し、リスクを低減する」「リスクを移転する」、あるいは「リスクを回避する」対応をとり、リスク値を「6」以下に低減する。

④ リスク値が「10」以上で、リスク値を受容水準以下に低減させることが、事業上の理由により不可能である場合は、ISMS 推進委員会でその受容の可否を審議し、組織としてそのリスクを受容する。

リスク受容基準

脅威のレベル		1			2			3		
ぜい弱性のレベル		1	2	3	1	2	3	1	2	3
事業に与える損害	1	**2**	**3**	**4**	**3**	**4**	**5**	**4**	**5**	**6**
	2	**4**	**6**	**8**	**6**	**8**	**10**	**8**	**10**	**12**
	3	**6**	**9**	**12**	**9**	**12**	**15**	**12**	**15**	**18**

原則受容　　受容可能　　リスク対応

6.1.7　リスク対応の選択

ISMS 事務局は、リスク値が「10」以上のリスク、及びリスク値が「8」「9」であっても受容できないと判断したリスクについては、下記の 3 つの対応策の中から一つを選択し、**「リスクアセスメント結果表」**に記入する。

(1) 管理策を採用し、リスクを低減する。

(2) リスクを共有する。十分な対策がとれない場合は、保険をかけるか、その業務を適用範囲外の組織に業務委託する。

(3) リスクを回避する。当該業務を廃止するか、あるいはその資産（装置）の使用を止める。

6.1.8　管理策の選択

(1) 管理策の選択

ISMS 事務局は、リスク対応で管理策を採用し、リスクを低減することを採用したリスクについて、ISO27001:2013 の附属書 A 詳細管理策の中から適切な管理目的と管理策を選択する。附属書 A 詳細管理策に適切な管理策がない場合は、新たに管理策を立案し、追加を行う。必要な管理策が見落とされていないかどうかは、ISMS 推進委員会で検証を行う。

(2) 残留リスクの明確化とリスク低減ができない場合の対応

ISMS 事務局は、リスクごとに管理策を採用した後のリスク値を計算し、**「リスクアセスメント結果表」**に残留リスクとして記入する。リスクが受容水準以下に低減しない場合には、管理策を追加してリスク値を受容水準以下に低減する。管理策を適用してもリスクが受容水準以下への低減が期待できない場合は下記により対応を決定する。

① そのリスクが顕在化した場合に、組織が対外的に責任を果たせないと判断した場合は当該業務を移転するか、廃止する。

② そのリスクが顕在化した場合に、その被害が自組織内に限定される場合、リスク所有者の明確な承認のもとに、当該リスクを保有することができる。

6.1.9　適用宣言書の作成

ISMS 事務局は、ISO27001:2013 附属書 A 詳細管理策の中で下記事項に当てはまる管理目的と管理策を採用し、**「適用宣言書」**を作成する。なお、採用した管理策の採用理由及び附属書 A 詳細管理策の中で除外した管理策の除外理由、管理策の実施の有無も明確にする。

(1) リスクアセスメントの結果から新たに採用する管理策

(2) 情報セキュリティ対応の選択肢の実施に必要な全ての管理策

6.1.10　リスク対応計画の作成

ISMS 事務局は、リスクアセスメントの結果受け、下記の項目を考慮し、**「リスク対応計画書」**を作成する。

(1) 具体的な対策

(2) 実施責任者

(3) 計画に必要な要員とコスト

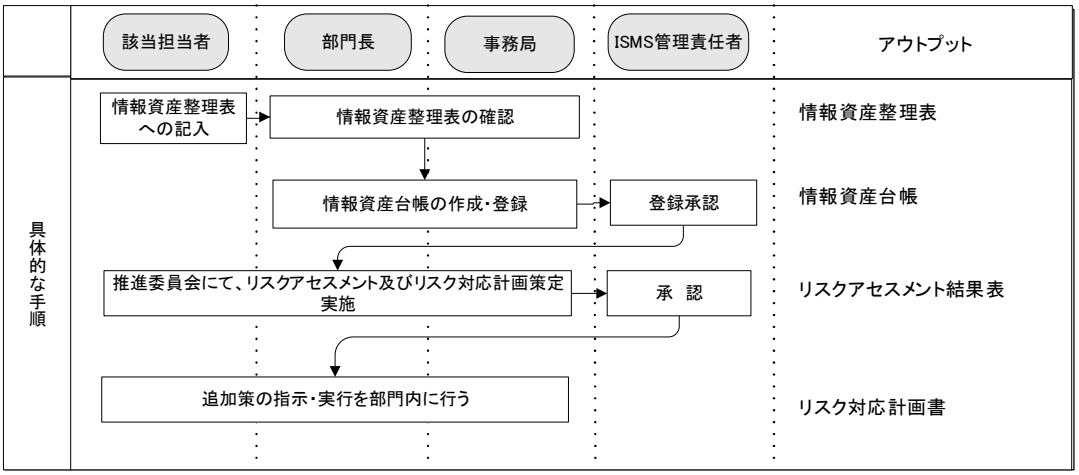
(4) 計画が複数ある場合はその優先順位

(5) スケジュール

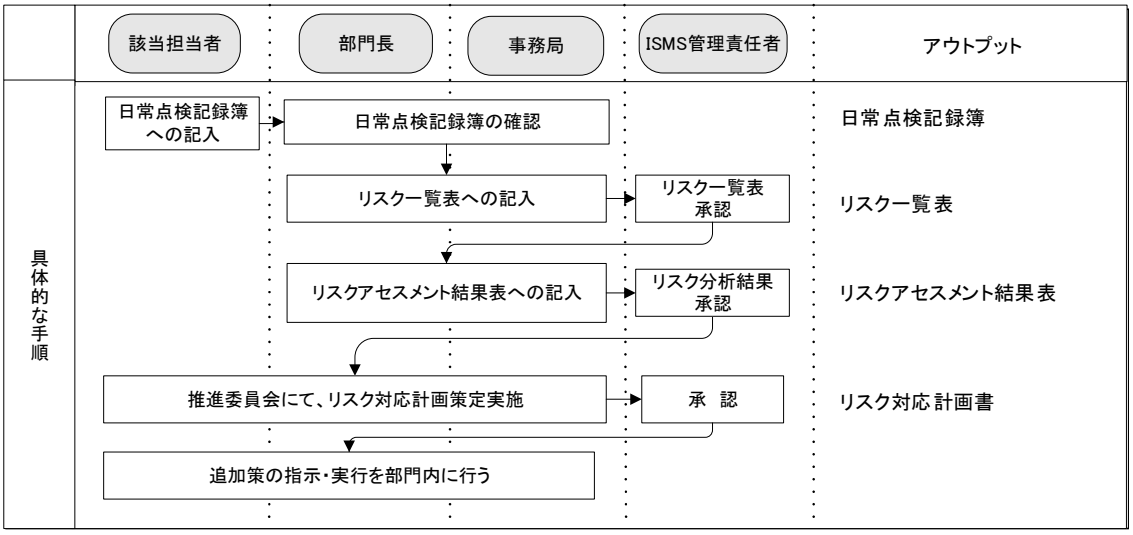
6.1.11　リスク対応計画及び残留リスクの承認

ISMS 事務局は、作成したリスク対応計画及び残留リスクに対してリスク所有者から承認を得る。

参考図１：新たな情報資産の追加・変更時の対応



参考図２：業務手順の見直し・変更等、リスク変化によるリスク見直し時の対応



7.5 文書化した情報

7.5.1 一般

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) ISO27001：2013（JISQ27001:2014）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、承認及び文書番号の付与は以下の表の通りとする。

なお、様式（文書 B）の保管期限、保管場所については、**「ISMS 様式集」**に記す。

文書分類	文書名	文書番号	起案（作成・改訂）	承　認
文書 A	情報セキュリティ基本方針	ISMS-A-01	ISMS 管理責任者	社　長
	適用宣言書	ISMS-A-02	ISMS 管理責任者	社　長
	ISMS マニュアル	ISMS-A-03	ISMS 管理責任者	社　長
	ISMS 管理策運用規定	ISMS-A-04	ISMS 管理責任者	社　長
	ISMS 様式集	ISMS-A-05	ISMS 管理責任者	社　長
文書 B（様式）	情報資産台帳	ISMS-B-01	ISMS 事務局	ISMS 管理責任者
	リスクアセスメント結果表	ISMS-B-02	ISMS 事務局	ISMS 管理責任者
	リスク対応計画書	ISMS-B-03	ISMS 事務局	社　長
	法的要求事項登録簿	ISMS-B-04	ISMS 事務局	社　長
	事業継続リスクアセスメント	ISMS-B-05	ISMS 事務局	ISMS 管理責任者
	事業継続計画書	ISMS-B-06	ISMS 事務局	社　長
	事業継続計画テスト結果記録	ISMS-B-07	ISMS 事務局	社　長
	年間教育計画表	ISMS-B-08	ISMS 事務局	ISMS 管理責任者
	教育訓練実施報告書	ISMS-B-09	ISMS 事務局	ISMS 管理責任者
	管理策測定評価表	ISMS-B-10	ISMS 事務局	ISMS 管理責任者
	ISMS の有効性レビュー実施結果表	ISMS-B-11	ISMS 事務局	ISMS 管理責任者
	セキュリティインシデント報告書	ISMS-B-12	ISMS 事務局	ISMS 管理責任者
	情報セキュリティ事象記録簿	ISMS-B-13	ISMS 事務局	ISMS 管理責任者
	入退室管理票（外部・従業員）	ISMS-B-14	ISMS 事務局	ISMS 管理責任者
	機密保持誓約書	ISMS-B-15	ISMS 事務局	社　長
	個人情報取扱いに関する同意書	ISMS-B-16	ISMS 事務局	社　長
	新規委託先評価表	ISMS-B-17	ISMS 事務局	ISMS 管理責任者
	委託先継続評価表	ISMS-B-18	ISMS 事務局	ISMS 管理責任者
	委託先管理台帳	ISMS-B-19	ISMS 事務局	ISMS 管理責任者
	内部監査実施計画書	ISMS-B-20	ISMS 事務局	ISMS 管理責任者
	内部監査員登録台帳	ISMS-B-21	ISMS 事務局	ISMS 管理責任者
	内部監査ﾁｪｯｸﾘｽﾄ	ISMS-B-22	ISMS 事務局	ISMS 管理責任者
	内部監査報告書	ISMS-B-23	ISMS 事務局	ISMS 管理責任者
	是正処置に関する報告書	ISMS-B-24	ISMS 事務局	ISMS 管理責任者
	ISMS ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ議事録	ISMS-B-25	ISMS 事務局	ISMS 管理責任者
	情報セキュリティ目標管理表	ISMS-B-26	ISMS 事務局	ISMS 管理責任者
	リスク一覧表	ISMS-B-27	ISMS 事務局	ISMS 管理責任者

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の有効性を評価し､次の事項を決定する。また、監視及び測定の結果の証拠として、文書化した情報を保持する。

(1) 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

(2) 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

(3) 監視及び測定の実施時期

(4) 監視及び測定の実施者

(5) 監視及び測定の結果の分析及び評価の時期

(6) 監視及び測定の結果の分析及び評価の実施者

監視・測定対象	分析・評価方法	監視及び測定の実施時期	結果の分析及び評価の時期	担当部門（実施者）
設定したセキュリティ目標	ISMS 推進委員会にて評価	毎月	毎年２月	ISMS 事務局
管理策の有効性	内部監査での結果を基に評価	毎年２月	毎年２月	ISMS 事務局
ISMS の有効性	内部監査での結果を基に評価	毎年２月	毎年２月	ISMS 事務局
供給業者のパフォーマンス	「供給者評価表」にて評価	都度	毎年２月	管理部門

9.1.1　社員による点検

社員は、定期的に（月１回）部門単位で会合を持ち、下記事項を点検する。

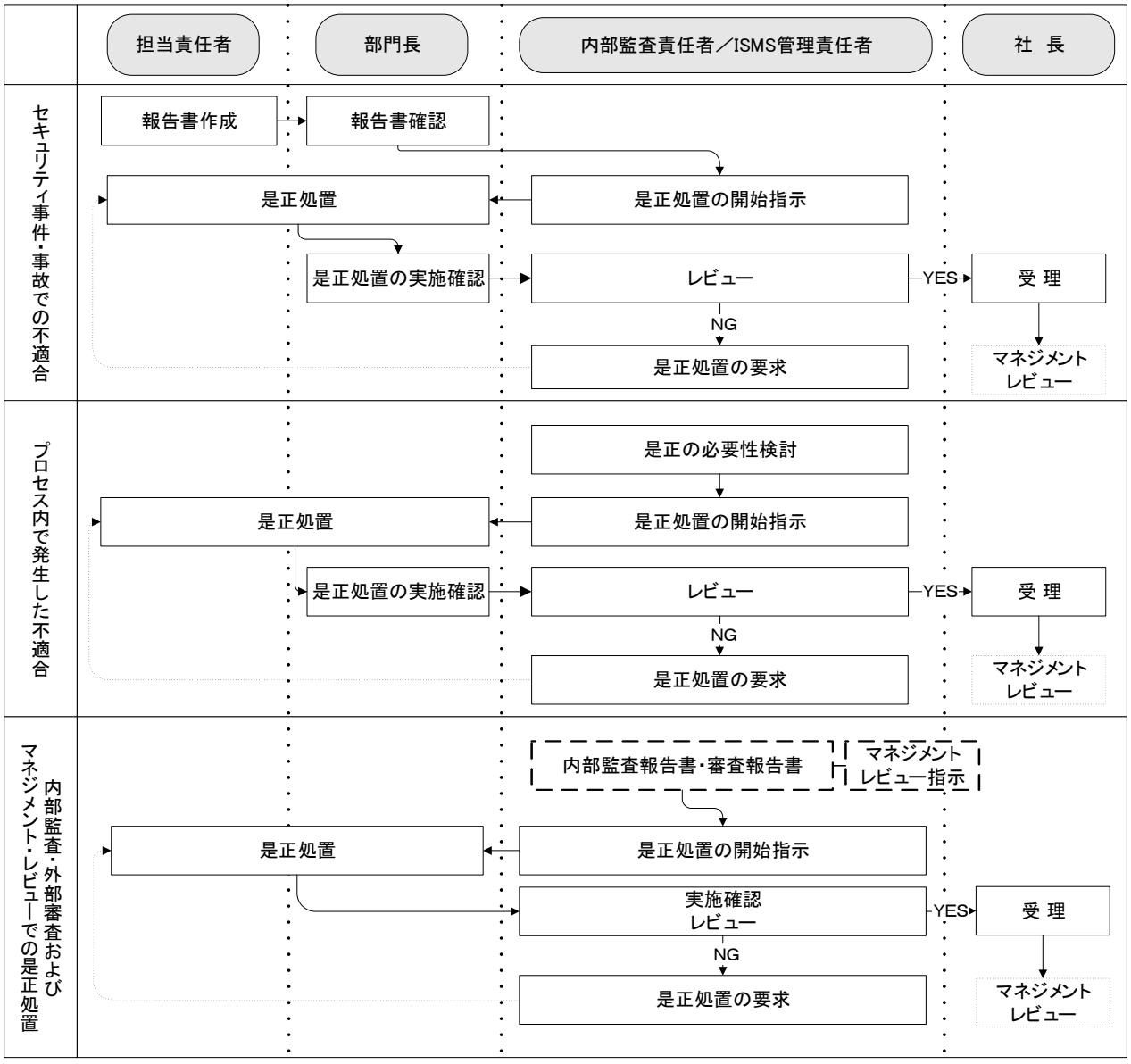
(1) セキュリティ目的（目標）の達成度を評価し、未達の場合対策を協議する。

(2) IS 推進委員は、 社内で発生した情報セキュリティ事象について、セキュリティ上の気づき事項として**「情報セキュリティ事象記録簿」**に記録する。

(3) ISMS 事務局は、**「情報セキュリティ事象記録簿」**を検討し、実施している日常活動の有効性を点検する。方針や手順に改善するべき点が発見された場合、ISMS 推進委員会にて、提議を行い、対応を検討する。

(4) 対応の結果は**「情報セキュリティ事象記録簿」**に記録する。

是正処置のフロー図


担当責任者
部門長
内部監査責任者／ISMS管理責任者
社 長
セキュリティ事件・事故での不適合
報告書作成
報告書確認
是正処置
是正処置の開始指示
是正処置の実施確認
レビュー
YES
受 理
NG
是正処置の要求
マネジメントレビュー
プロセス内で発生した不適合
是正の必要性検討
是正処置
是正処置の開始指示
是正処置の実施確認
レビュー
YES
受 理
NG
是正処置の要求
マネジメントレビュー
内部監査・外部審査およびマネジメント・レビューでの是正処置
内部監査報告書・審査報告書
マネジメントレビュー指示
是正処置
是正処置の開始指示
実施確認
レビュー
YES
受 理
NG
是正処置の要求
マネジメントレビュー

（株）サンプル ISMS マニュアル	制定日 2020.03.01	文書番号 ISMS-A-03
	改訂日	改訂番号 1

このISMSマニュアル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マニュアルサンプル購入希望」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マニュアルサンプル）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マニュアルサンプル）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