情報セキュリティマニュアル

ISO/IEC27001:2013

Ver.1.1

2019/12/13

株式会社アンサー

社外秘

承認	作成
五十嵐　一郎	小沼　慶征

目　次

1　適用範囲 2
1.1　組織と所在地 2
1.2　事業 2
2　引用規格 2
3　用語及び定義 2
4　組織の状況 3
4.1　組織及びその状況の理解 3
4.2　利害関係者のニーズ及び期待の理解 4
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 4
4.4　情報セキュリティマネジメントシステム 4
5　リーダーシップ 5
5.1　リーダーシップ及びコミットメント 5
5.2　方針 5
5.3　組織の役割、責任及び権限 6
6　計画 8
6.1　リスク及び機会に対処する活動 8
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 12
7　支援 13
7.1　資源 13
7.2　力量 13
7.3　認識 13
7.4　コミュニケーション 14
7.5　文書化した情報 14
8　運用 16
8.1　運用の計画及び管理 16
9　パフォーマンス評価 17
9.1　監視、測定、分析及び評価 17
9.2　内部監査 17
9.3　マネジメントレビュー 18
10　改善 19
10.1　不適合及び是正処置 19
10.2　継続的改善 19

1 適用範囲

この情報セキュリティマネジメントシステム（以下、「ISMS」という）は、以下の範囲に適用する。

1.1 組織と所在地

株式会社アンサー（以下、「当法人」という）。

本社	〒101-0021 東京都千代田区外神田 6-16-9 外神田千代田ビル 7F

1.2 事業

当法人は、「コンピュータソフトウェア・システムの開発・設計・製造・販売 及び 管理業務、代行業務」を目的とし、以下の事業を行う。

- システム開発および保守の受託
- システム開発および保守に伴う、技術者の派遣

2 引用規格

JIS Q 27001:2014(ISO/IEC 27001:2013)

3 用語及び定義

本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

ISMS の確立のため、当法人をとりまく外部、内部状況を考慮し、課題を決定する。

4.1.1 外部状況の課題

対象	課題
法令・規範・条例等	金融業などを中心に、ソフトウェアの開発及びシステムエンジニアリングサービスを提供しているが、情報に対する適切な管理と法令尊守の迅速な対応が必要とされている。
経済や市場の動向	企業内で発生する各業務のシステム化・自動化への対応は加速しており、ニーズも拡大していくと予測している。金融業だけでなく、流通業においても市場は広がりを見せており、その対策が急務である。
外部の利害関係者	慢性化した人員不足を解消するために同業他社との協業は不可欠だが、それに伴いセキュリティに対する情報連携と共有が課題である。

＜関連文書＞「**法令管理台帳**」

4.1.2 内部状況の課題

対象	課題
当法人の文化	情報セキュリティの要件（機密性・完全性・可用性）が要求される製品・サービスを提供しているが、技術面では不足しているところがある。
当法人の事業戦略	情報セキュリティ面でのセールスポイント化するためにも、自社における情報セキュリティ事故はあってはならない環境にある。
当法人の体制	会社の規模に合わせた、情報セキュリティ体制を構築する。
開発環境	将来的にテレワークを行う場合、情報セキュリティをどのように担保するのかが課題である。

4.2 利害関係者のニーズ及び期待の理解

ISMS に関連する利害関係者を特定し、利害関係者の情報セキュリティに関連する要求事項を決定する。

4.2.1 ISMS に関連する利害関係者と要求事項

利害関係者	要求事項
従業者	情報漏洩による、従業員の社会的信用の失墜、経営悪化を回避する。
顧客	顧客から預かる機密情報の漏洩で、信用失墜や損害賠償請求、取引停止の可能性がある。
取引先	情報漏洩による、ビジネスパートナーへの営業機会の影響を防止する。
その他	規制当局からの法規制が強化される可能性がある。

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

「4.1 組織及びその状況の理解」、「4.2 利害関係者のニーズ及び期待の理解」及び当法人と他の組織との関係を考慮し、ISMS の適用範囲として「1. 適用範囲」に記す。

4.4 情報セキュリティマネジメントシステム

「2.引用規格」に記された規格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、次に示す事項により 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する。（戦略的方向性と両立させる。）

２）ISMS の要求事項を組織のプロセスに統合する。

３）ISMS に必要な資源を利用可能とする。

４）有効な情報セキュリティマネジメントと ISMS 要求事項への適合の重要性を伝達する。

５）ISMS の意図した成果を達成する。

６）ISMS の有効性に寄与するよう指揮し、支援する。

７）継続的改善を促進する。

８）管理層がリーダーシップを発揮できるよう支援する。

5.2 方針

トップマネジメントは、以下の方針群を確立し、文書化し、伝達する。

方針	確立方法
情報セキュリティ方針	当法人のウェブサイトおいて周知を図る。
モバイル機器の方針	情報セキュリティ規程 4
アクセス制御方針	情報セキュリティ規程 1、2、3、4、7、8
暗号による管理策の利用方針	情報セキュリティ規程 1、4
クリアデスク・クリアスクリーン方針	情報セキュリティ規程 3
情報転送の方針	情報セキュリティ規程 4
セキュリティに配慮した開発のための方針	情報セキュリティ規程 7
供給者関係のための情報セキュリティ方針	情報セキュリティ規程 6

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、周知を図る。

＜関連文書＞「**情報セキュリティ体制図**」

5.3.1 役割、責任及び権限、必要な力量

情報セキュリティ体制図に記された役割、責任及び権限、必要な力量について以下のとおり定義する。

役割	責任及び権限	必要な力量
トップマネジメント	● 情報セキュリティマネジメントシステムの維持・運営に際し、リーダーシップを発揮する。 ● 当法人における情報セキュリティマネジメントシステムに対する全責任を負う。	-
ISMS 管理責任者	● 情報セキュリティマネジメントシステムに関するプロセスの確立、実施及び維持を確実にし、要求事項に適合させる。 ● 情報セキュリティマネジメントシステムの実施状況及び改善の提案を含め、情報セキュリティマネジメントシステムのパフォーマンスを、マネジメントレビューの場でトップマネジメントに報告する。 ● 従業者に対し、情報セキュリティマネジメントシステムの理解及び法令、利害関係者の要求事項に対する認識の向上を図るための、教育・訓練を実施する。 ● 必要な場合、利害関係者との接触及び折衝を行う。	ISO/IEC27001 に精通していること。 ISMS を主導することができること。
部門管理責任者	● リスクマネジメントを実施する。 ● 部門内の ISMS について指導する。 ● 事業継続計画を立案し、訓練を指導する。	各部門の長であり、部門の承認管理者であること。 リーダーシップを発揮できること。
システム管理責任者	● 技術的管理策の妥当性を判断する。 ● 技術的側面から情報セキュリティマネジメントシステムの維持管理を行う。	データベース管理、ネットワーク管理等技術的な情報セキュリティに精通していること。

内部監査員	● 中立的な立場から各部門の内部監査を実施する。	ISMS 内部監査員養成研修を修了していること。
従業者	● 役員、従業員、当法人において業務をおこなうすべての者。 ● 情報セキュリティの基本と所属部門に関連する ISMS 規程を理解している。	情報セキュリティ教育を受講し、合格基準を満たしていること。

6 計画

6.1 リスク及び機会に対処する活動

6.1.1 一般

当法人は、「4.1 組織及びその状況の理解」「4.2 利害関係者のニーズ及び期待の理解」を考慮し、次の項目のためにリスク及び機会を決定する。

1） ISMS が意図した成果を達成するため
2） 望ましくない影響を防止または低減するため
3） 継続的改善を達成するため

6.1.1.1 計画

6.1.1 において決定したリスク及び機会に対し、次の事項を計画する。

1） リスク及び機会に対処する活動計画
2） その活動の ISMS プロセスへの統合及び実施計画
3） その活動の有効性の評価計画

6.1.1.2

情報セキュリティリスクアセスメントのプロセスを以下のとおり定め、適用する。

6.1.1.3 情報の洗い出し

部門管理責任者は、対象となる情報を洗い出し、その内容を「**情報・情報資産台帳**」に記入する。

項目	方法
分類	「情報」「情報資産」から選択する。
情報名	洗い出した情報の名称。 情報資産の価値や保管形態・場所が一致するものはグループ化して整理する。（たとえば「契約書」「サーバ群」「コンテンツ群」など）
内容	具体的な内容。
保管形態	情報の保管形態を「紙媒体」「電子データ」「電子媒体」から選択する。
廃棄方法	例：「シュレッダー」「溶解廃棄」「完全消去ソフト」等

保管場所	例：「個人机」「袖机」「書庫」「ファイルサーバ」「クラウドサーバ」等
（補足）	保管場所を特定できる情報、施錠の有無等を記入する。例：田中（施錠）、書庫 A（施錠なし）、ファイルサーバ（フォルダ名）等
保管期間	例：○年間、○○年○月まで、無期限　等
所有者（リスク所有者）	情報の内容に関して責任を有する者/部署（組織）。
管理者	情報を物理的に管理している者/部署（組織）を指す。基本的には情報所有者と一致するが、サーバ内や倉庫で保管している場合には、そのサーバや倉庫の管理者が、情報管理者となる場合がある。
利用者	情報を利用する者/部署（組織）を指す。基本的には情報所有者と一致するが、業務上の必要性から、他部署や委託先に情報を提供している場合には、提供先も情報利用者に含まれる。
機密性　（C）	３：極秘（特定の関係者に開示可能、個人情報等） ２：機密（特定の部署に開示可能、NDA 文書等） １：社外秘（社内に開示可能）
完全性　（A）	完全性が損なわれた場合・・・ ３：最高（回復が容易でない信用損失が発生） ２：高（多数に対する信用損失が発生） １：中（限られた者に対する信用損失が発生）
可用性　（I）	利用不可能になった場合・・・ ３：最高（業務停止は許容されない） ２：高（翌営業日まで業務停止が許容される） １：中（1 週間、業務停止が許容される）
個人情報	該当する場合は「○」をつける。特定個人情報には「◎」をつける。
入手方法	個人情報の入手方法
件数	個人情報の件数

サーバ群、コンテンツ群等の資産管理については、「**情報機器管理台帳**」、「**ソフトウェア管理台帳**」にて補完する。

6.1.1.4 リスク評価

部門管理責任者は、以下の手順に従い、「**リスク評価シート**」に基づき、リスク評価を行う。

１） 作成した「情報一覧」に記入した「保管場所」を「リスク評価シート」の「保管場所」欄に記入する。

２） 「保管場所」毎に保管されている情報の最大資産価値を「最大資産価値」欄に記入する。

３） 「**脅威リスト**」を参考に、対象となる脅威を「脅威名」欄に記入する（複数の脅威がある場合には、行を分けて記入）。

４） 「要素」欄には、別紙「脅威リスト」から列挙した脅威に対する関連要素（機密性、完全性、可用性）を転記し、「大きさ」欄には、別紙「**脅威の評価基準**」に基づき、脅威の大きさを記入する。

５） 別紙「脅威リスト」に記入されていない脅威以外に考慮すべき脅威がある場合には、同様に列挙する。その際、「要素」欄には、当該脅威が機密性、完全性及び可用性のどの要素に関連した脅威であるかを合わせて決定する。

６） 列挙した各脅威に対して、現状の管理策を「現状の対策」欄に記入する。複数の対策を実施している場合には、まとめて記入する。（例えば、「入退室管理、教育」）また、「度合い」欄には、別紙「**脆弱性の評価基準**」を参考に、脆弱性の度合いを記入する。

７） 次の式に基づき、リスクを算出し、その結果を「リスク（是正措置前）」欄に記入する。

（脅威の要素に該当する要素の）「最大資産価値」×脅威の「大きさ」×脆弱性の「度合い」

８） リスクが 12（許容レベル）以上になった脅威に対して、リスクを許容レベル以下にするために追加の管理策を検討し、「追加の対策」欄に記入するとともに、追加の管理策の導入による脆弱性の度合いを再評価し、その結果を「度合い」欄に記入する。

９） リスクが 8、9 の場合には、必要に応じて追加の管理策を検討する。

１０） リスクが、許容レベル未満の場合には、現在実施している対策で十分と判断し、次項は省略する。

１１） 同様の方法で、再評価した脆弱性の度合いに基づき、リスクを算出し、その結果を「リスク（是正措置後）」に記入する。

１２） なお、許容レベルを超えた全てのリスクを許容レベル以下におさえる必要はない。費用対効果や業務上の制約事項などにより、許容レベル以下におさえられなかったリスクは、残留リスクとする。残留リスクは、次項のセキュリティ委員会への報告の際に合わせて、報告し、セキュリティ委員会において管理する。

6.1.1.5 実施すべき管理策の決定

ISMS 管理責任者は、リスクアセスメントの結果を、セキュリティ委員会に報告する。

１） セキュリティ委員会は、報告内容に関して十分な協議をした上で、実施すべき管理策に対する承認を与える。

２） セキュリティ委員会は、上記１）で決定した管理策を「付属書 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。

３） 協議をする際には、追加・変更する管理策の費用対効果を考慮し、その保証の度合いを決定する。但し、あるリスクが特定されたものの、財務上、環境上、技術上、文化上その他の理由のために管理策を実施することが適切でないと判断した場合には、残留リスクとして定期的に見直す。

４） また、対応する必要があるが、速やかに対応できないリスクに対しては「**情報セキュリティリスク対応計画**」を作成し、その進捗を管理する。

6.1.1.6 管理策の導入

セキュリティ委員会は、ISMS 管理責任者に以下を指示する。

- 規定類の新規作成・修正・廃版
- 追加・変更された管理策の関係者への周知
- 「**適用宣言書**」の作成
- その他、追加・変更された管理策に係る導入作業

6.1.1.7 リスク評価の更新

１） 以下の場合、部門管理責任者は、リスク評価結果を更新し ISMS 管理責任者に提出する。

- 脅威に影響を与える情報処理施設/設備の変更
- 脅威に影響を与える情報処理形態分類の変更
- 情報価値評価に影響を与える情報の変更

２） ISMS 管理責任者は、年一回にリスク評価の見直しを指示する。各部署の情報管理者は見直しを実施し、必要ある場合は最新の記録を作成し、提出する。

３） ISMS 管理責任者は、リスク評価の更新結果をセキュリティ委員会に報告する。セキュリティ委員会は、報告の都度、対応する。

6.1.2 情報セキュリティリスク対応

情報セキュリティリスク対応のプロセスについて以下の文書を作成し、保持する。

- **「情報・情報資産台帳」**
- **「リスク評価シート」**
- **「情報セキュリティリスク対応計画」**
- **「適用宣言書」**

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

当法人は、以下の条件を満たす情報セキュリティ目的を確立し、実施する。

a) 情報セキュリティ方針と整合している
b) 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

計画は、「**情報セキュリティ目的達成計画書**」にて管理する。計画書では以下の事項を決定する。

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

トップマネジメントは、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。

資源を必要とする場合は、稟議をあげることとし、トップマネジメントは、稟議の採用/不採用を迅速に決定する。

7.2 力量

当法人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行う者の力量を「5.3.2　役割、責任及び権限、必要な力量」において定義し、「**力量評価シート**」にて管理する。

力量を備えていることを確実にするため、以下の証跡を作成し、保持する。

証跡	内容
「教育訓練報告書」	入社時教育、定期教育、臨時教育を実施した際の内容、受講者一覧
外部教育受講報告	外部の情報セキュリティ教育を受講した際の報告書
事業継続訓練報告書	事業継続訓練を実施した際の報告書、参加者一覧
その他	入社時に取得した履歴書、職務経歴書、人事評価記録等

7.3 認識

当法人の管理下で働く者は以下の事項に関して認識を持たなければならない。当該事項は、入社時教育、定期教育の内容に含めるものとする。

- 情報セキュリティ方針群
- 情報セキュリティパフォーマンスの向上による便益
- ISMS の有効性に対する自らの貢献
- 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

7.4.1 内部及び重要取引先とのコミュニケーション

ISMS に関連する内部及び取引先とのコミュニケーションは、社内会議、電子メール等を活用する。

7.4.2 外部組織とのコミュニケーション

ISMS に関連する外部組織とのコミュニケーションは、電子メール、ホームページ等にて行う。

電話でコミュニケーションを実施した場合は、決定内容を電子メールにて伝達し、証跡を残す。

＜関連文書＞ **「外部組織連絡先」**

7.5 文書化した情報

7.5.1 一般

当法人は、ISMS の有効性のために必要とされる情報を特定し、文書化する。文書は社内で共有できるファイル形式（マイクロソフトオフィス形式、PDF 形式等）で文書化し、データを保管する。

7.5.2 作成及び更新

ISMS 文書には次の項目を含めなければならない。

項目	説明
タイトル	誰にでもわかる表現をつかうこと
作成日/改定日	作成した日付/改定した日付
作成者	作成者名
プロジェクト名	特定のプロジェクトに関する場合は記載すること

適切性及び妥当性に関する適切なレビュー及び承認が必要な文書は、適時**セキュリティ委員会**を招集し検討・承認を得る。

7.5.3 文書化した情報の管理

文書化した情報は、「**文書管理台帳**」に登録する。紙媒体は所定のキャビネット、電子ファイルは所定のファイルサーバのフォルダ にて管理する。

7.5.3.1 ファイルサーバの設定

キャビネットおよびファイルサーバにおいて管理する ISMS 文書へのアクセスは当法人の従業者のみとする。

ISMS 文書フォルダは従業者の利用しやすいよう、フォルダ名や配列に留意する。

7.5.3.2 外部文書の管理

ISMS の計画及び運用のために必要と決定した外部からの文書化した情報は、必要に応じて特定し、管理する。

文書の形態	管理方法
紙媒体、印刷物	スキャニング後、PDF データとして保存する。
電子データ	PDF データ、もしくは、オリジナルデータを保存する。
ウェブサイト	PDF データ、もしくは、URL を記載したテキストファイルを保存する。
その他の文書	オリジナル文書データを保存する。
紙媒体で保存が必要なもの	紙媒体のままファイリングし、施錠保管する。

8 運用

8.1 運用の計画及び管理

セキュリティ委員会は、ISMS 運用の計画及び管理を実施するため、年一回、「**マネジメントシステム年間実施計画**」を作成し ISMS 管理責任者の承認を得る。

部門管理責任者は、「**マネジメントシステム年間実施計画**」に従って、管理策の実行と定期的な評価を行う。

8.2 情報セキュリティリスクアセスメント

業務においては、「6.1.2 情報セキュリティリスクアセスメント」を考慮して、情報セキュリティを含むリスクアセスメントを実施する。その結果をプロジェクト計画書に反映する。

8.3 情報セキュリティリスク対応

業務においては、リスク対応の一環として情報セキュリティリスク対応を実施する。

9 パフォーマンス評価

9.1 監視、測定、分析及び評価

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ため、次の事項を決定する。

a) 監視及び測定の対象
セキュリティ委員会にて、決定する。

b) 監視、測定、分析及び評価の方法
「**セルフチェックシート**」にて実施する。

c) 監視及び測定の実施時期
半期ごとに実施する。

d) 監視及び測定の実施者
部門管理責任者が実施する。

e) 監視及び測定の結果の、分析及び評価の時期
マネジメントレビューの実施前に行う。

f) 監視及び測定の結果の、分析及び評価の実施者
ISMS 管理責任者が実施する。

9.2 内部監査

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、年一回内部監査を実施する。内部監査は業務プロセスの中断を最小限に抑えるため慎重に計画する。

9.2.1 内部監査における確認事項

1） 次の事項に適合している
① ISMS に関して組織自体が既定した要求事項
② ISO 27001 の要求事項

2） ISMS が有効に実施され、維持されている

9.2.2 内部監査手順

内部監査は以下の手順で実施する

1） 対象部門の見直し
2） **「内部監査チェックリスト」**の見直し
3） 内部監査員の任命及び内部監査員養成研修の実施
4） 内部監査時期の告知（1ヶ月前）
5） 内部監査の実施
6） **「内部監査報告書」**の作成
7） セキュリティ委員会による内部監査報告書の承認

9.3 マネジメントレビュー

トップマネジメントは、当法人の 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、年一回に ISMS をレビューする。

マネジメントレビューの結果は「**マネジメントレビュー実施記録**」として文書化し、情報を保持する。

10 改善

10.1 不適合及び是正処置

リスクアセスメント、内部監査、セルフチェック等の監視、測定において不適合が発生した場合、その不適合を是正し、「**是正処置報告書**」として文書化し、情報を保持する。

10.2 継続的改善

当法人は、企業環境の変化に即応しながら企業業績の向上を目指し、情報セキュリティ方針として表明した内容を実現するため、情報セキュリティマネジメントシステムの目的（目標）及び目的達成計画の結果、リスク対応の処置、監査結果、データの分析、是正処置、及びマネジメントレビューを通じて、情報セキュリティマネジメントシステムの適切性、妥当性及び有効性を継続的に改善する。

改定履歴

版	内容	日付
Ver.1.0	初版	2019 年 9 月 27 日
Ver.1.1	ページ番号追加	2019 年 12 月 13 日