サイバーセキュリティ対策マネジメントガイドライン

Ver.1.0

2018 年 1 月 16 日

特定非営利活動法人　日本セキュリティ監査協会

目次

序文

本書は,JIS Q 27001:2014 を実装している組織が,その ISMS を生かしサイバーセキュリティ対策を実施するための要求事項ならびに管理策のガイダンスを提供するものである。本規格は ISO/IEC27009:2016 に準拠して,作成されている。

注記　本書では,JIS Q 27001:2014 または JIS Q 27002:2014 との差分を明確にするため,追記した記述の箇所にアンダーラインを付している。

1　適用範囲

本書は，JIS Q 27001:2014 に基づき ISMS を確立し，実施し，維持し，継続的に改善している組織が，サイバーセキュリティのための対策を，ISMS 活動に取り入れ,実施するための要求事項を提供する。

本書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。組織が本書への適合を宣言する場合には，4 章及び 5 章に規定するいかなる要求事項の除外も認められない。

2　引用規格

次に掲げる規格は，本書に引用されることによって，本書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。

JIS Q 27001:2014 情報技術－セキュリティ技術－情報セキュリテイマネジメントシステム－要求事項

JIS Q 27002:2014 情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範

3　用語及び定義

本書で用いる主な用語及び定義は，JIS Q 27000 による他,以下の用語を用いる。

3.1

サイバー攻撃

情報通信技術を用いた攻撃

3.2

サイバーセキュリティ

サイバーセキュリティリスクが管理された状態

3.3

サイバーセキュリティリスク

サイバー攻撃により生じるリスク

3.4

サイバーレジリエンス

サイバーセキュリティに対するレジリエンス

3.5

レジリエンス（resilience）

複雑かつ変化する環境下での組織の適応できる能力。

注記　レジリエンスは，中断・阻害を引き起こすリスクを運用管理する組織の力である。

（JIS Q 22300）

4　JIS Q 27001:2014 に関連したサイバーセキュリティ分野の要求事項

4.1　本書の構成

本書は,JIS Q 27001:2014 に関連したサイバーセキュリティ対策マネジメントガイドラインである。本書は，サイバーセキュリティ固有の要求事項を記載した 4.2 節と，JIS Q 27002:2014 に関連したサイバーセキュリティ管理策実施のためのガイダンスを記載した 5 章から構成される。また,サイバーセキュリティ固有の管理目的及び管理策は附属書 A に列挙される。

4.2　サイバーセキュリティのための要求事項

以下に記述されていない JIS Q 27001:2014 のすべての要求事項は,原文のまま適用される。

4.2.1

JIS Q 27001:2014 の 4.1（組織及びその状況の理解）を,次のとおり読み替える。

4.1 組織及びその状況の理解

組織は，組織の目的及び社会的責任に関連し，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しなければならない。

注記 これらの課題の決定とは，JIS Q 31000:2010 の 5.3 に記載されている組織の外部状況及び内部状況の確定のことをいう。

4.2.2

JIS Q 27001:2014 の 5.2(方針)を,次のとおり読み替える。

5.2 方針

トップマネジメントは，次の事項を満たすサイバーセキュリティを含む情報セキュリティ方針を確立しなければならない。

a) 組織の目的及び社会的責任に対して適切である。

b) 情報セキュリティ目的(6.2 参照)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) 組織内に伝達する。

g) 必要に応じて，利害関係者が入手可能である。

4.2.3

JIS Q 27001:2014 の 6.1.3(情報セキュリティリスク対応)を次のとおり読み替える。

6.1.3 情報セキュリティリスク対応

組織は，次の事項を行うために，サイバーセキュリティリスクを含む情報セキュリティリスク対応のプロセスを定め，適用しなければならない。

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。

注記組織は，必要な管理策を設計するか，又は任意の情報源の中から管理策を特定することができる。

c) 6.1.3 b)で決定した管理策を附属書A及び本書の附属書 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。

注記1 附属書 A 及び本書の附属書 A は，管理目的及び管理策の包括的なリストである。本書の利用者は，必要な管理策の見落としがないことを確実にするために，附属害 A 及び本書の附属書 A を参照することが求められている。

注記 2 管理目的は，選択した管理策に暗に含まれている。附属書A及び本書の附属書 A に規定した管理目的及び管理策は，全てを網羅してはいないため，追加の管理目的及び管理策が必要となる場合がある。

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

－それらの管理策を実施しているか否か

－附属書A又は本書の附属書 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。

g) 組織は,サイバー攻撃によるインシデント検知を計画し,実施する。

h) 組織は,サイバーレジリエンスを計画し,実施する。

i) 組織は,サイバー攻撃で被害を受けた場合に,情報の適切な取り扱いができるための復旧計画を立案し,実施する。

j) 組織は,サイバー攻撃を受けた場合でも事業が継続できるように,事業継続計画を立案し,実施する。

組織は，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を保持しなければならない。

注記 本書の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，JIS Q 31000 に規定する原則及び一般的な指針と整合している。

4.2.4

JIS Q 27001:2014 の 7.4(コミュニケーション)を次のとおり読み替える。

7.4 コミュニケーション

組織は，次の事項を含め，サイバーセキュリティを含む 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しなければならない。

a) コミュニケーションの内容(伝達内容)

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

サイバーセキュリティ対応計画に従った活動は次を含む。

1) 利害関係者との間のサイバーセキュリティに関する情報の共有と調整

2) サイバーセキュリティに関する状況認識を深めるための外部関係者との間の任意の情報共有

3) サイバーセキュリティが侵害された場合の広報についての規定と実施

4) インシデント発生後の評判の回復

5)サイバーセキュリティが侵害された場合の事業継続についての規定と実施

5 JIS Q 27002:2014 に関連したサイバーセキュリティ管理策実施のためのガイダンス

以下に記述されていない JIS Q 27002:2014 のすべての箇条,目的,管理策,実施の手引及び関連情報は,原文のまま適用される。

5.1

JIS Q 27002:2014 の 5.1.1(情報セキュリティのための方針群)の実施の手引の,情報セキュリティ方針に含めることが望ましい記載事項に,次の細別を追加する。

d) 外部からの脅威の特定と文書化

e) リスク一覧の特定と文書化

5.2

JIS Q 27002:2014 の 6.1.1(情報セキュリティの役割及び責任)の実施の手引の,個人が責任をもつ領域の規定に,次の細別を追加する。

f) リスク一覧に基づくリスク所有者の明確化

5.3

JIS Q 27002:2014 の 6.1.3(関係当局との連絡)の実施の手引を,次のとおり読み替える。

組織は, いつ, 誰が関係当局(例えば, 法の執行機関, 規制当局, 監督官庁)に連絡するかの手順を備えることが望ましい。また, 例えば, 法が破られたと疑われる場合に, 特定した情報セキュリティインシデントを,定められた基準に従って,いかにして時機を失せずに報告するかの手順を備えることが望ましい。

5.4

JIS Q 27002:2014 の 7.2.2(情報セキュリティの意識向上,教育及び訓練)の実施の手引に,情報セキュリティの教育及び訓練に含むべき一般的側面として,次の細別を追加する。

f) インシデント対応が必要になった時の自己の役割と行動の順番

5.5

JIS Q 27002:2014 の 8.1.1(資産目録)の実施の手引を,次のとおり読み替える。

組織は, 情報のライフサイクルに関連した資産を特定し, その重要度を文書化することが望ましい。情報のライフサイクルには, 作成, 処理, 保管, 送信, 削除及び破棄を含めることが望ましい。文書は, 専用の目録又は既存の目録として維持することが望ましい。

注記 1 資産目録には,組織内の物理デバイス及びシステムの一覧を含む。

注記 2 資産目録には,ソフトウェアプラットフォーム及びアプリケーションの一覧を含む。

資産目録は, 正確で, 最新に保たれ, 一貫性があり, 他の目録と整合していることが望ましい。

特定された各資産について, 管理責任者を割り当て(8.1.2 参照), 分類する(8.2 参照)ことが望ましい。

5.6

JIS Q 27002:2014 の 8(資産の管理)に細分箇条 8.4(データ破壊)を追加する。

8.4 データ破壊

目的 所定の保存期間を過ぎたデータを不当な利用や漏えいから保護するため。

8.4.1 データ破壊の管理

管理策

データ処分方針に従って,機密度に応じた破壊方式を選択し,データを破壊し,その結果を記録することが望ましい。

実施の手引

データの破壊は,当局の規制及び定められた規則に従って管理されることが望ましい。これには,他の組織への移管が含まれる。

破壊手続きは, データの機密性に適した安全予防策が含まれることが望ましい。破壊手続きは,破壊が検証できるよう監査可能であることが望ましい。

係争中または実際の訴訟または法的措置または調査に関連する文書は,その訴訟が進行中または発生している間は破壊されない措置が取られることが望ましい。

注記 1　当該データが,個々のデータを破壊されないようにした媒体やシステム(WORM 光学ディスクなど)に保存されている場合は,破壊待ちデータへのアクセスを防ぐ適切なプロセスを実装するか, あるいは,その媒体中の破壊待ちデータ以外のデータを新しい媒体にコピーし,元の媒体を本管理策に従って処分する。

注記 2　クラウドサービスにおける利用者データの破壊については,JIS Q 27017:2016 の CLD8.1.5 を参照。

5.7

JIS Q 27002:2014 の 11.2.4(装置の保守)の実施の手引に,次の細別を追加する。

g) 装置の保守と修理は,承認・管理されたツールを用いてタイムリーに実施し,ログを記録する。

h) 装置に対する遠隔保守は,承認を得て,ログを記録し,不正アクセスを防げる形で実施する。

5.8

JIS Q 27002:2014 の 12.1.2(変更管理)の実施の手引に,次の項目を追加する。

i) 設定変更管理プロセスの導入

5.9

JIS Q 27002:2014 の 12(運用のセキュリティ)に細分箇条 12.8(インシデントの検知)を追加する。

12.8 インシデントの検知

目的　サイバー攻撃の検知を有効にするため。

12.8.1　インシデント検知に対する管理

管理策

異常なイベントをタイムリーにかつ正確に検知するための検知手順を定義,維持しテストすることが望ましい。

実施の手引

この管理策の実施に当たって,次の事項を含むことが望ましい。

a) インシデント検知に関する役割と責任の明確な定義

b) インシデント検知に必要なすべての要求事項への対応

これには次の要求が含まれる。

1) セキュリティ評価

2) 継続的モニタリング

3) トレーニング

4) 情報システムのモニタリング

c) インシデント検知システムからの異常なイベント通知の調査

d) インシデント検知プロセスのテスト

e) 監査,セキュリティ評価,継続的モニタリング,脆弱性スキャン,情報システムのモニタリングなど適切な関係者への異常なイベントの検知情報の伝達

f) インシデント検知プロセスの継続的な改善

注記　NIST SP 800 シリーズでは,「情報システム」ではなく「情報技術/産業用制御システム」と記載されている。これは,5.12 でも同様である。

5.10

JIS Q 27002:2014 の 13.1.1（ネットワーク管理策）の実施の手引の,細別 d)を次のように読み替える。

d) 情報セキュリティに影響を及ぼす可能性のある行動（サービス妨害を含む），又は情報セキュリティに関連した行動を記録及び検知できるように，継続的モニタリングを含む適切なログ取得及び監視を適用する。

また,実施の手引に,次の細別を追加する。

h) ネットワーク運用のベースラインとユーザシステム間の予想されるデータの流れを特定し管理する。

5.11

JIS Q 27002:2014 の 13.2.1（情報転送の方針及び手順）の実施の手引に,次の細別を追加する。

l) 組織内の通信とデータの流れ図の用意

5.12

JIS Q 27002:2014 の 14.1.1（情報セキュリティ要求事項の分析及び仕様化）の実施の手引に,次の細別を追加する。

g) 情報システムのベースラインとなる設定の定義と維持

h) システム開発ライフサイクルの導入

また,関連情報を,次のように読み替える。

情報システムのベースラインとなる設定の定義と維持は,細分箇条 12.1.2, 12.5.1, 12.6.2, 14.2.2, 14.2.3 及び 14.2.4 も関連する。

情報セキュリティ要求事項を満たすために必要な管理策を特定するための，リスクマネジメントプロセスの使用に関する手引が，JIS Q 31000[27]及び ISO/IEC 27005[11]に示されている。

5.13

JIS Q 27002:2014 の 15.1.1（供給者関係のための情報セキュリティの方針）の実施の手引に,次の細別を追加する。

n) 重要サービス提供を支援するレジリエンスに関する取り決め

5.14

JIS Q 27002:2014 の 15.1.2（供給者との合意によるセキュリティの扱い）の実施の手引に,次の細別を追加する。

q) 適切なパートナーとの間の保護技術の有効性に関する情報共有

5.15

JIS Q 27002:2014 の 16.1.1（責任及び手順）の実施の手引の細別 a)1)を,次のように読み替える。

1) サイバー攻撃に対するインシデント対応計画及び準備,並びに復旧のための手順

また,細別 a)に,次の項目を追加する。

7) 攻撃の標的を理解するための,検知したイベントの分析手順

8) 複数の情報源やセンサーから収集したイベントデータを相互に関連付ける手順

9) イベントがもたらす影響を特定する手順

10) インシデント警告の閾値を定める手順

5.16

JIS Q 27002:2014 の 16.1.4(情報セキュリティ事象の評価及び決定)の実施の手引を,次のとおり読み替える。

連絡先の者は, 合意された情報セキュリティ事象・情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価し, その事象を情報セキュリティインシデントに分類するか否かを決定することが望ましい。インシデントの分類及び優先順位付けは, インシデントの影響及び程度の特定に役立てることができる。

組織内に情報セキュリティインシデント対応チームがある場合は, 確認又は再評価のために, 評価及び決定の結果をこの対応チームに転送してもよい。情報セキュリティ事象の評価及び決定には必要に応じて段階的取扱い(escalation)を考慮することが望ましい。

評価及び決定の結果は, 以後の参照及び検証のために詳細に記録しておくことが望ましい。

5.17

JIS Q 27002:2014 の 17.1.1(情報セキュリティ継続の計画)の管理策を,次のように読み替える。

組織は, サイバー攻撃に対する, 情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定することが望ましい。

注記 17.1.2(情報セキュリティ継続の実施)及び 17.1.3(情報セキュリティ継続の検証,レビュー及び評価)の管理策についても,“困難な状況”を“サイバー攻撃”に読み替える。

また,実施の手引を,次のように読み替える。

組織は, サイバー攻撃に対する事業継続及び災害復旧に関する計画立案に際して, 情報セキュリティ要求事項を定め,情報セキュリティの継続を事業継続マネジメント(以下, BCM という。)プロセス又は災害復旧管理(以下, DRM という。)プロセスに織り込むことが望ましい。

事業継続及び災害復旧に関する正式な計画が策定されていない場合には, 通常の業務状況とは異なるサイバー攻撃の発生時においても, 情報セキュリティ要求事項は変わらず存続することを, 情報セキュリティマネジメントの前提とすることが望ましい。別の方法として, サイバー攻撃の発生時に適用できる情報セキュリティ要求事項を定めるために, 情報セキュリティの側面について事業影響度分析(以下, BIA という。)を実施することもできる。

注記 第一段落の元の表現

組織は, 情報セキュリティの継続が事業継続マネジメント(以下, BCM という。)プロセス又は災害復旧管理(以下, DRM という。)プロセスに織り込まれているか否かを判断することが望ましい。

5.18

JIS Q 27002:2014 の 16.1.5(情報セキュリティインシデントへの対応)の実施の手引に,次の細別を追加する。

h) インシデントへの発生中又は発生後の対応を計画し,実施する。

i) 発生したインシデントを封じ込める。

j) 発生したインシデントを低減する。

5.19

JIS Q 27002:2014 の 16.1.6(情報セキュリティインシデントからの学習)の実施の手引を,次のように読み替える。

情報セキュリティインシデントの形態,規模及び費用を定量化及び監視できるようにする仕組みを備えることが望ましい。情報セキュリティインシデントの評価から得た情報は,再発する又は影響の大きいインシデントを特定するために利用することが望ましい。また,適切なパートナーとの間で保護技術の有効性に関する情報を共有することが望ましい。

5.20

JIS Q 27002:2014 の 16.1.7(証拠の収集)の関連情報を,次のように読み替える。

特定とは,証拠となる可能性のあるものの捜索,認識及び文書化に関わるプロセスをいう。収集とは,証拠となる可能性のあるものを含み得る物理的な物品を集めるプロセスをいう。取得とは,特定した範囲の中でデータの複製を作成するプロセスをいう。保存とは,証拠となる可能性のあるものの完全性及び当初の状態を維持し,それを保護するプロセスをいう。

情報セキュリティ事象を最初に検知した時点では,その事象が訴訟に発展するかどうかは判然としない場合がある。したがって,そのインシデントの重大さに気が付く前に,意図的又は偶然に,必要な証拠を破壊してしまう危険性がある。何らかの法的処置があり得ると考える場合は,早めに弁護士又は警察に相談すること,及び必要となる証拠に関する助言を求めることを勧める。

証拠の収集と分析手段として,ディジタルフォレンジックがある。

ディジタル形式の証拠の特定,収集,取得及び保存に関する指針が,ISO/IEC 27037[24]に示されている。

5.21

JIS Q 27002:2014 の 17.1.3(情報セキュリティ継続の検証,レビュー及び評価)の実施の手引に,次の細別を追加する。

d) 対応計画及び復旧計画をテストする。

5.22

JIS Q 27002:2014 の 18.1.1(適用法令及び契約上の要求事項の特定)の実施の手引を,次のとおり読み替える。

これらの要求事項を満たすための具体的な管理策及び具体的な責任についても定め,文書化することが望ましい。

管理者は,その事業の種類に関連した要求事項を満たすために,サイバーセキュリティ基本法を含む各自の組織に適用される全ての法令を特定することが望ましい。組織が他の国で事業を営む場合には,管理者は,関連する全ての国における順守を考慮することが望ましい。

附属書 A　サイバーセキュリティ固有の管理目的及び管理策

表 A.1 にリストアップされている追加または変更された管理目的と管理策は,本書で定義されたものから直接導かれかつ本書と矛盾がなく,本書で追加または読み替えられた JIS Q 27001:2014 の 6.1.3 のなかで使われる。

表 A.1－管理目的及び管理策

A.8.4 データ破壊 **目的**　データを保護するため		
A.8.4.1	**データ破壊の管理**	管理策 　データの処分ポリシーに従って機密度に応じた破壊方式を選択し,データを破壊し,その結果を記録することが望ましい。
A.12.8 インシデントの検知 **目的**　サイバー攻撃の検知を有効にするため		
A.12.8.1	**インシデント検知に対する管理**	管理策 　異常なイベントをタイムリーにかつ正確に検知するための検知手順を定義,維持しテストすることが望ましい。