管理された非格付け情報の保護対策マネジメントガイドライン

― NIST SP800-171 対応の ISMS のために ―

2018 年 2 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 を活かし管理された非格付け情報の保護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，管理された非格付け情報の保護対策を，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，規模または性質を問わず，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

管理された非格付け情報

法律，政令または政府全体のポリシーにより安全防護または配布管理を行うことが要求される情報

注記　NIST SP.800-171 の原文

法律政令，または政府全体のポリシーにより安全防護または配布管理を行うことが要求される情報。ただし，大統領行政命令 13526，格付けされた国家安全保障情報，2009 年 12 月 29 日付，または以前の，または後継の大統領行政命令，または 1954 年の原子力エネルギー法，及びそれらの改正の下で格付けされる情報を除く。

3.2

ベースライン構成

所与の時点で正式にレビューされ合意された，変更管理手順を介してのみ変更可能な，システム内の情報システムの文書化された一連の仕様または構成項目

3.3

モバイルコード

明示的なインストールまたは受信者による実行なしに，リモートの情報システムから取得され，ネットワークを介

不許複製　JASA

して送信され，ローカル情報システム上で実行されたソフトウェアプログラムまたはプログラムの一部

4　JIS Q 27001:2014 に関連した管理された非格付け情報の保護分野の要求事項

4.1 本書の構成

本書は，JIS Q 27001:2014 に関連した管理された非格付け情報の保護対策マネジメントガイドラインである。本書は，管理された非格付け情報の保護に固有の要求事項を記載した 4.2 節と，JIS Q 27002:2014 に関連した管理された非格付け情報の保護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，管理された非格付け情報の保護に固有の管理目的及び管理策は附属書 A に列挙される。

なお，参考として，附属書 B に NIST SP.800-171 連邦政府外のシステムと組織における管理された非格付け情報の保護 2016.12 との対応関係を，附属書 C にその逆引き表を掲載する。

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 6.1.3（情報セキュリティリスク対応）に，次の細別を追加する。

g) 組織は，インシデント対応能力のテストを，関連する計画に責任をもつ部署と調整して計画し，実施する。

注記　関連する計画には，事業継続計画，緊急時対応計画，災害復旧計画，政府存続計画，緊急時コミュニケーション計画，重要インフラ計画，居住者非常時計画などがある。

h) 組織は，遠隔からの操作を含む保守を計画し，実施する。

4.2.2

JIS Q 27001:2014 の 9.1（監視，測定，分析及び評価）を，次のとおり読み替える。

9.1　監視，測定，分析及び評価

組織は，情報セキュリティパフォーマンス及び ISMS の有効性を評価しなければならない。

組織は，次の事項を決定しなければならない。

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

注記　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

組織は，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しなければならない。

組織は，管理策の有効性を保証するため，セキュリティ管理策を継続的に監視しなければならない。

5　JIS Q 27002:2014 に関連した管理された非格付け情報の保護管理策実施のためのガイダン

不許複製　JASA

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 6.1.4（専門組織との連絡）の実施の手引に，次の細別を追加する。

g) 必要に応じて，初期のセキュリティ警告または指示を関連する組織に伝達する。

5.2

JIS Q 27002:2014 の 6.2.1（モバイル機器の方針）の実施の手引の，第 4 段落の直後に次の記述を追加する。

識別可能な所有者のいないポータブルストレージデバイスを使用しないことが望ましい。

5.3

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，次の細別を追加する。

f) 内部からの脅威の潜在指標に関する認識と報告についてのセキュリティ意識（気付き）訓練

5.4

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，専用の目録または既存の目録として維持することが望ましい。

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。

情報システムの最新のベースライン構成を把握，文書化し，維持することが望ましい。この情報システムには，ハードウェア，ソフトウェア及び文書を含む。

また，関連情報を，次のように読み替える。

資産目録は，保護を効果的に行うことを確実にするために役立つとともに，他の目的（例えば，安全衛生，保険または財務面での資産管理）のために必要となることもある。

資産を特定する場合に組織が考慮する必要性が生じる可能性のある資産の例は，ISO/IEC 27005[11]に示されている。資産目録を作成するプロセスは，リスクマネジメントの重要な要素である（ISO/IEC 27000 及び ISO/IEC 27005[11]も参照）。

情報システムとシステムコンポーネントのベースライン構成は，文書化，正式なレビューおよび合意を経た，情報システムの仕様，またはそれらのシステムの設定項目である。ベースライン構成は，情報システムの将来にわたる構築，リリースまたは変更の際のベースになる。ベースライン構成は，情報システムコンポーネント（例：ワークステーション，ノートパソコン，サーバー，ネットワークコンポーネント，または携帯機器にインストールされている標準ソフトウェアパッケージ・オペレーティングシステムとアプリケーションの現在のバージョン番号とパッチ情報・設定

不許複製　JASA

項目／パラメータ)，ネットワークの接続形態，およびシステム構成内のそれらのコンポーネントの論理的な配置に関する情報を含む。ベースライン構成を維持するには，組織の情報システムが時間の経過と共に変化することから，新しいベースラインを作成する必要がある。情報システムのベースライン構成は，現在のエンタープライズアーキテクチャを反映する。

5.5

JIS Q 27002:2014 の 8.1.2(資産の管理責任)の実施の手引に，次の細別を追加する。

e) 公開アクセス可能なシステムにおいて掲載または処理される情報を制御する。

また，関連情報を，次で読み替える。

管理責任者は，資産のライフサイクル全体を管理する責任を与えられた個人またはエンティティであり得る。その管理責任者は，必ずしもその資産の所有権をもっている必要はない。

ルーチン業務の委任(例えば，日々の資産保全を保全要員に委ねること)を行ってもよいが，その責任は管理責任者の下にとどまる。

複雑な情報システムでは，あるサービスを提供するために関係する，複数の資産グループを特定することが，有益な場合がある。この場合，サービスの管理責任者が，その資産の運用も含めたサービスの提供に対して責任を負う。

組織は，管理された非格付け情報を情報公開システムに掲載する権限のある者を指定する。公開情報に，管理された非格付け情報のうち非公開情報が決して含まれないよう，その者に対して教育を行う。情報公開システムに情報をアップロードする前に内容を確認し，非公開情報が決して含まれないようにする。情報公開システムに掲載されている情報の内容を適宜確認し，非公開情報が含まれていることが判明した場合には，その情報を削除する。

5.6

JIS Q 27002:2014 の 8.2.3(資産の取扱い)の実施の手引に，次の細別を追加する。

f) 情報システムの出力装置に対する物理アクセスを制御し，権限のない者が装置からの出力情報を取得できないようにする。

5.7

JIS Q 27002:2014 の 9.1.2(ネットワーク及びネットワークサービスへのアクセス)の実施の手引に，次の細別を追加する。

g) 管理されたアクセス制御ポイントを介したリモートアクセスのルーティング

5.8

JIS Q 27002:2014 の 11.1.1(物理的セキュリティ境界)の実施の手引に，次の細別を追加する。

h) 物理アクセスログ及びイベントの兆候に関するレビューと調査の結果を，インシデント対応チームとの間で調整する

不許複製　JASA

5.9

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) 組織の外で修理を行う場合は，媒体上の情報を消去し，修理のための移動の承認を得る。

h) 保守ツールを承認・管理のうえモニタリングし，保守要員が施設に持ち込むツールを検査し，不適切な変更，不正な変更または不正な情報の収集の有無を確認する。

i) 遠隔保守セションを確立するため，複数要素の認証を要求し，保守の完了時にセションを終了する。

j) 必要なアクセス許可をもたない保守要員の保守活動を監督する。

5.10

JIS Q 27002:2014 の 12.1.1(操作手順書)の実施の手引に，次の細別を追加する。

k) セキュリティ設定

注記　運用上の要求事項に適合する最も制限されたモードを反映するセキュリティ設定チェックリストを使用して，情報システムに導入されている IT 製品の設定項目を文書化し，設定を実施する。また，この設定から逸脱する場合は，それを特定し文書化のうえ承認を得ることに加えて，組織のポリシーと手順に従って設定変更を実施し，モニタリングのうえ管理する。

また，次の関連情報を追加する。

関連情報

設定項目とは，情報システムのハードウェアコンポーネント，ソフトウェアコンポーネント，またはファームウェアコンポーネントの動作を変更できるパラメータであり，システムのセキュリティ状態および機能を左右する。セキュリティ設定項目を定義できる

IT 製品には，たとえば，メインフレームコンピュータ，サーバー(例:データベース，電子メール，認証，ウェブ，プロキシ，ファイル，ドメイン名)，ワークステーション，入出力装置(例:スキャナー，コピー機，プリンター)，ネットワークコンポーネント(例:ファイアウォール，ルーター，ゲートウェイ，音声／データスイッチ，ワイヤレスアクセスポイント，ネットワーク装置，センサー)・オペレーティングシステム，ミドルウェア，アプリケーションがある。

セキュリティパラメータは，情報システムのセキュリティ状態に影響を及ぼすパラメータであり，その一部は，その他のセキュリティ管理策要求事項を満たすのに必要である。セキュリティパラメータには，例えば，以下がある:①レジストリの設定②アカウント・ファイル・ディレクトリのパーミッション設定③機能・ポート・プロトコル・サービス・リモート接続などの設定

組織は，組織全体にわたる設定項目を定め，その後，情報システムに特化した設定を定める。定められた設定は，システムを構成するベースライン管理策の一部となる。

5.11

JIS Q 27002:2014 の 12.4(ログ取得及び監視)に細分箇条 12.4.5(ログの関連付け)及び 12.4.6(監査ログ量の低減)を追加する。

12.4.5 ログの関連付け

管理策　組織全体の状況が把握できるよう，組織がリポジトリの異なる複数のログを関連付ける。

不許複製　JASA

実施の手引

複数の組織全体で状況を把握するため、リスク管理の対象となる組織,ミッション（業務）プロセス,情報システムの3つに関する状況をアカウント単位や資源単位で関連付けを行う。

状況の関連付けは、統合ログ管理製品などのハードウェア、ソフトウェアを利用して、可能な限り人間の手を介在させずに自動化することが望ましい。

12.4.6 監査ログ量の低減

管理策 監査の簡素化のために，監査レポート生成のプロセスとともに監査縮小プロセスを実行する。

実施の手引

監査縮小プロセスは，①オンデマンドの監査レビュー②オンデマンドの監査分析③オンデマンドの監査要件に沿った（セキュリティインシデントの）事後調査のそれぞれをサポートするプロセスとして，かつ(b)監査記録の当初の内容または監査記録が記録される順序に対して変更を加えない。

監査縮小プロセスは，収集された監査情報を操作して当該情報が分析者にとってより意味のある情報となるよう圧縮する。

関連情報

監査レポート生成のプロセスと同じく，監査縮小プロセスは，必ずしも監査を実施する情報システム（または監査を実施する組織）によって行われるとは限らない。例えば，最新のデータフィルタを用いて監査記録に記録された異常な振る舞いを検知する最新のデータマイニング技法が，監査縮小プロセスを構成する要素となりうる。

なお，情報システムによって実行される監査レポート生成プロセスによって，カスタマイズされた監査レポートを作成することができる。また，監査記録として記録されたタイムスタンプの正確性が十分でない場合，監査記録が記録された時間的順序が重要になる場合がある。なお，関連するセキュリティ管理策は，AU-6 の管理策である。

関連情報

NIST SP.800-53 AU-7

5.12

JIS Q 27002:2014 の 12.5.1（運用システムに関わるソフトウェアの導入）の実施の手引に，次の細別を追加する。

i) 非基本プログラム，機能，ポート，プロトコル及びサービスの使用を制限，無効化及び防止する。

j) 許可されないソフトウェアの使用を防止するためにブラックリスト ポリシーを，または許可されたソフトウェアの実行を許可するようなホワイトリストポリシーを適用する。

5.13

JIS Q 27002:2014 の 12.6.1（技術的ぜい弱性の管理）の実施の手引に，次の細別を追加する。

m) 脆弱性スキャンは、対象コンポーネントの特権アクセスを用いて実施する。

5.14

JIS Q 27002:2014 の 13.1.1（ネットワーク管理策）の実施の手引に，次の細別を追加する。

h) デフォルトでネットワーク通信トラフィクを拒否し，また例外によってネットワーク通信トラフィクを許可する

i) リモートデバイスが，組織のシステムとの非リモートコネクションの確立と同時に，外部ネットワークの資源への何らかの他のコネクションを介して通信することを適切に制限できるように設定する(分割トンネル制限)

5.15

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) 共同コンピューティングデバイスの安全な接続

注記 リモートからの活性化を禁止し，デバイス利用者にデバイス使用可を通知する。

対象となるデバイスには，ホワイトボード，カメラ，マイクなどがある。

m) モバイルコードの使用

注記 組織は，許容できる／許容できないモバイルコードおよびモバイルコードテクノロジーを定義し，許容できるモバイルコードおよびモバイルコードテクノロジーに関して，使用制限を定め，導入ガイダンスを作成し．情報システムにおけるモバイルコードの使用を許可，モニタリング，管理する。

n) VoIP (Voice over Internet Protocol) 技術の使用

注記 組織は，VoIP 技術が悪意を持って使用された場合に情報システムに被害が及ぶ可能性に基づいて，VoIP 技術の使用制限を定め，導入ガイダンスを作成するとともに，情報システムにおける VoIP の使用を許可・モニタリング・管理する。

5.16

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）の実施の手引の細別 b)を，次のように読み替える。

b) 業務上の利用者のほか，特権を与えられた利用者及び技術をもつ利用者に対する，アクセスの提供及び認可のプロセス

注記 これには，監査機能の管理を特権利用者の一部に制限することを含む。

また，実施の手引きに，次の細別を追加する。

g) 共有システム資源を介した，不正な予期せぬ情報の転送防止

5.17

JIS Q 27002:2014 の 14.2.5（セキュリティに配慮したシステム構築の原則）の実施の手引を，次のように読み替える。

セキュリティに配慮したシステム構築の原則に基づき，情報システムの構築手順を確立し，文書化し，組織の情報システム構築活動に適用することが望ましい。セキュリティは，情報セキュリティの必要性とアクセス性の必要性との均衡を保ちながら，全てのアーキテクチャ層（業務，データ，アプリケーション及び技術）において設計することが望ましい。利用者機能とシステム管理機能とを分離することが望ましい。新技術は，セキュリティ上のリスクについて分析し，その設計を既知の攻撃パターンに照らしてレビューすることが望ましい。

これらの原則及び確立した構築手順は，構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために，定期的にレビューすることが望ましい。また，これらの原則及び手順が，新規の潜在的な脅威に対抗するという点で最新であり続けていること，及び適用される技術及びソリューションの進展に

適用可能であり続けていることを確実にするために，定期的にレビューすることが望ましい。

確立された設計のセキュリティに関するこの原則は，該当する場合には，組織と組織が外部委託した供給者との間の，契約及び拘束力をもつその他の合意を通じて，外部委託した情報システムにも適用することが望ましい。組織は，供給者の設計のセキュリティに関する原則が，自身の原則と同様に厳密なものであることを確認することが望ましい。

5.18

JIS Q 27002:2014 の 16.1.1（責任及び手順）の実施の手引の細別 a)に，次の細別を追加する。

7) 組織のインシデント対応能力をテストする手順

注記　テストは，必要に応じて，チェックリスト，実地訓練，机上訓練，シミュレーション，包括訓練を選択する。

不許複製　JASA

附属書 A（規定） 管理された非格付け情報保護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.12.4.5	**ログの関連付け**	**管理策** 組織全体の状況が把握できるよう，組織がリポジトリの異なる複数のログを関連付ける。
A.12.4.6	**監査ログ量の低減**	**管理策** 監査の簡素化のために，監査レポート生成のプロセスとともに監査縮小プロセスを実行する。

不許複製　JASA

附属書 B(参考) NIST SP.800-171 との対応関係

表 B.1 は, NIST SP.800-171 と本書が規定する管理策(JIS Q 27001, JIS Q 27002, 並びにその拡張)との対応関係を示している。

注記 NIST SP.800-171 には, JSO/IEC 27001 の Annex A との対応関係が掲載されている。

表 B.1－SP800-171 との対応関係

	SP800-171 の管理策	4.2 章	5 章
3.1	**アクセス制御**		
	3.1.1 システムアクセスを許可された利用者, 許可された利用者を代行して動作するプロセス, またはデバイス(その他のシステムを含めて) に制限する。		6.2.1, 6.2.2, 9.2.1-9.2.3, 9.2.5, 9.2.6, 13.1.1, 13.2.1, 14.1.2
	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。		6.2.1, 6.2.2, 9.1.2, 9.4.1, 9.4.4, 9.4.5, 13.1.1, 13.2.1, 14.1.2, 14.1.3, 18.1.3
	3.1.3 承認された権限付与に従って CUI のフローを制御する。		13.1.3, 13.2.1, 14.1.2, 14.1.3
	3.1.4 共謀のない悪意のあるアクティビティのリスク低減のため, 個人の職務を分離する。		6.1.2
	3.1.5 具体的なセキュリティ機能と特権アカウントを含め, 特権の最小化の原則を採用する。		9.1.2, 9.2.3, 9.4.4, 9.4.5
	3.1.6 非セキュリティ機能をアクセスするときは, 非特権アカウントまたは役割を使用する。		9.2.3
	3.1.7 非特権利用者による特権機能の実行を防止し, このような機能の実行を監査する。		9.2.3, 12.4.1
	3.1.8 ログイン試行失敗を制限する。		9.4.2
	3.1.9 適用可能な CUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。		9.4.2
	3.1.10 非アクティブな時間の経過後, データのアクセス及び閲覧を防止するため, パターンによる不可視化表示を用いてセションロックを使用する。		11.2.8, 11.2.9
	3.1.11 定義された条件の後, 利用者セションを(自動的に) 終了する。		9.4.2
	3.1.12 リモートアクセスセションを監視し, 制御する。		9.4.2
	3.1.13 リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。		13.2.1
	3.1.14 管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。		9.1.2
	3.1.15 特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。		9.1.2
	3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。		6.2.1, 13.1.1, 13.2.1
	3.1.17 認証と暗号化を用いて無線アクセスを保護する。		13.1.2
	3.1.18 モバイルデバイスのコネクションを制御する。		6.2.1, 11.2.6, 13.2.1
	3.1.19 モバイルデバイス及びモバイルコンピューティングプラットフォーム上の CUI を暗号化する。		6.2.1
	3.1.20 外部システムへのコネクション及び使用を検証し, 制御／制限する。		11.2.6, 13.1.1, 13.2.1, 13.2.3
	3.1.21 外部システム上での組織のポータブルストレージデバイスの使用を制限する。		8.3.1
	3.1.22 公開アクセス可能なシステムにおいて掲載または処理される CUI を制御する。		8.1.2

不許複製 JASA

	SP800-171 の管理策	4.2 章	5 章
3.2	**意識向上と訓練**		
	3.2.1 組織のシステムの責任者，システム管理者，及び利用者が，彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー，基準，訓練されていることを，保証する。		7.2.2, 12.2.1
	3.2.2 組織の要員が，その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを，保証する。		7.2.2*, 12.2.1
	3.2.3 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。		7.2.2
3.3	**監査と責任追跡性(説明責任)**		
	3.3.1 非合法の，許可されない，または不適切なシステムアクティビティの監視，分析，調査，及び報告を可能とするために必要な範囲で，システム監査記録を作成，保護，及び維持する。	9.1	12.4.1*, 12.4.3, 16.1.2, 16.1.4
	3.3.2 個別のシステム利用者のアクションが，彼らのアクションについての説明責任を維持可能にするよう，それらの利用者に対して一意に追跡が可能であることを保証する。	9.1	12.4.1*, 12.4.3, 16.1.2, 16.1.4
	3.3.3 監査された事象をレビューし，アップデートする。	9.3 , 10.1	
	3.3.4 監査プロセス失敗の事象においてアラート(警告) を発する。	9.2	
	3.3.5 監査記録のレビュー，分析，及び調査のための報告プロセスを集めて相互の関係を比較し，不適切な，疑わしい，または異常なアクティビティの兆候に対応している。		12.4.5
	3.3.6 オンデマンド分析と報告をサポートするため，監査の簡素化と報告書生成を提供する。		12.4.6
	3.3.7 監査記録のタイムスタンプを生成するための正式な情報源を用いて，内部システムクロックを比較し同期するようなシステム機能を提供する。		12.4.4
	3.3.8 監査情報と監査ツールを不正なアクセス，改変，及び削除から保護する。		12.4.2, 12.4.3, 18.1.3
	3.3.9 監査機能の管理を特権利用者の一部に制限する。		14.1.1
3.4	**構成管理**		
	3.4.1 個別のシステム開発ライフサイクル全体で，組織のシステム（ハードウェア，ソフトウェア，ファームウェア，及び文書を含めて）のベースライン構成とインベントリを確立し，維持する。		8.1.1, 8.1.2
	3.4.2 組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し，実施 する。		12.1.1
	3.4.3 組織のシステムへの変更を追跡，レビュー，承認／非承認，及び監査する。		12.2.2, 14.2.2-14.2.4
	3.4.4 実装に先立ち，変更のセキュリティへの影響を分析する。		14.2.3
	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，(実施 する。		9.2.3, 9.4.5, 12.1.2, 12.1.4, 12.5.1
	3.4.6 基本機能のみを提供するように組織のシステムを構成することによって，最小機能の原則を採用する。		12.5.1*
	3.4.7 非基本プログラム，機能，ポート，プロトコル，及びサービスの使用を制限，無効化，及び防止する。		12.5.1
	3.4.8 許可されないソフトウェアの使用を防止するために例外による拒否（ブラックリスト）ポリシーを，または許可されたソフトウェアの実行を許可するような例外による許可（ホワイトリスト)ポリシーを適用する。		12.5.1

不許複製 JASA

	SP800-171 の管理策	4.2 章	5 章
	3.4.9 利用者がインストールしたソフトウェアを管理し，監視する。		12.5.1，12.6.2
3.5	**識別と認証**		
	3.5.1 システム利用者，利用者を代行して動作するプロセス，またはデバイスを識別する。		9.2.1
	3.5.2 組織のシステムへのアクセスの許可に対する必要条件として，それらの利用者，プロセス，またはデバイスのアイデンティティを認証(または検証)する。		9.2.4，9.3.1，9.4.3
	3.5.3 多要素の認証を，特権アカウントへのローカル及びネットワークアクセスのために，及び非特権アカウントへのネットワークアクセスのために，使用する。		13.2.1
	3.5.4 特権及び非特権アカウントへのネットワークアクセスのために，リプレイ耐性のある認証メカニズムを採用する。		13.2.1
	3.5.5 定義された期間について，識別コードの再利用を禁止する。		9.2.1
	3.5.6 定義された非アクティブな期間の後，識別子を無効化する。		9.2.1
	3.5.7 新しいパスワードが作成されるとき，最小パスワード複雑性及び文字列の変更を強制(実施)する。		9.4.3
	3.5.8 規定された生成回数の間，パスワードの再利用を禁止する。		9.4.3
	3.5.9 永久パスワードへ直ちに変更するようなときのシステムログインのためにワンタイムパスワードの使用を許可する。		9.4.3
	3.5.10 暗号学的に保護されたパスワードのみを格納及び送信する。		9.4.3
	3.5.11 認証情報のフィードバックを目に見えないようにする。		9.4.2
3.6	**インシデント対応**		
	3.6.1 適切な準備，検知，分析，抑制（封じ込め），リカバリ，及び利用者対応アクティビティを含めて，組織のシステムのための運用上のインシデントハンドリング能力を確立する。		7.2.2*，16.1.4-16.1.6
	3.6.2 組織の内部及び外部の両方の，適切な担当官及び／または権威に対して，インシデントについての追跡，文書化，及び報告を行う。		6.1.3，16.1.2
	3.6.3 組織のインシデント対応能力をテストする。	6.1.3	16.1.1
3.7	**保守**		
	3.7.1 組織のシステムにおいて保守を実施する。	6.1.3	11.2.4*，11.2.5*
	3.7.2 システム保守を実施するために使用されるツール，手法，メカニズム，及び要員における有効な管理策を提供する。		
	3.7.3 オフサイトの保守のために除去される装置は，あらゆる CUI についてサニタイズされることを保証する。		11.2.4*，11.2.5*
	3.7.4 組織のシステム内で媒体が使用される前に，悪意のあるコードが入っていないか診断及びテストプログラムを用いて媒体をチェックする。		12.2.1
	3.7.5 外部のネットワークコネクションを介した非ローカル保守セションを確立するため，複数要素の認証を要求し，非ローカル保守の完了時にこのようなセションを終了する。		11.2.4
	3.7.6 必要なアクセス許可のない保守要員の保守活動を監督する。		11.2.4
3.8	**媒体保護**		
	3.8.1 紙及びディジタルの両方の，CUI を含む，システム媒体を保護する(即ち，物理的に制御及びセキュアに格納する)。		8.2.3，8.3.1，11.2.9

不許複製　JASA

	SP800-171 の管理策	4.2 章	5 章
	3.8.2 システム媒体上の CUI へのアクセスを許可された利用者に制限する。		8.2.3, 8.3.1, 11.2.9
	3.8.3 廃棄または再利用のために手放す前に, CUI を含むシステム媒体をサニタイズまたは破壊する。		8.2.3, 8.3.1, 8.3.2, 11.2.7
	3.8.4 CUI のマーク表示と配付制限が必要な媒体に対して表示を行う。		8.2.2
	3.8.5 CUI を含む媒体へのアクセスを制御し, 管理エリアの外部への持ち出し中の媒体の説明責任を維持する。		8.2.3, 8.3.1, 8.3.3, 11.2.5, 11.2.6
	3.8.6 代替の物理的予防手段による保護がない限り, 持ち出し中はディジタル媒体上に格納された CUI の機密性を保護するための暗号学的メカニズムを実装する。		6.2.1
	3.8.7 システムコンポーネント上の取り外し可能な媒体の使用を管理する。		8.2.3, 8.3.1
	3.8.8 ポータブルストレージデバイスに識別可能な所有者がいないとき, このようなデバイスの使用を禁止する。		6.2.1
	3.8.9 保存場所にあるバックアップ CUI の機密性を保護する。		12.3.1, 17.1.2, 18.1.3
3.9	**人的セキュリティ**		
	3.9.1 CUI を含む組織のシステムへのアクセスを許可する前に, 個人を審査する。		7.1.1
	3.9.2 離職または配置転換等の人事措置の間と後で, CUI 及び CUI を含む組織のシステムが保護されることを保証する。		7.3.1, 8.1.4
3.10	**物理的保護**		
	3.10.1 組織のシステム, 装置, 及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。		11.1.2*, 11.1.3
	3.10.2 物理的設備を保護し, 監視し, 組織のシステムの基盤をサポートする。		11.1.1
	3.10.3 訪問者をエスコートし, 訪問者の活動を監視する。		11.1.1
	3.10.4 物理的アクセスの監査ログを維持する。		11.1.2
	3.10.5 物理的アクセスデバイスを制御し, 管理する。		11.1.3
	3.10.6 代替の作業サイト(例, テレワークのサイト)での CUI に対する防護対策を強制(実施)する。		6.2.2, 11.2.6, 13.2.1
3.11	**リスクアセスメント**		
	3.11.1 組織のシステムの運用と関連する CUI の処理, ストレージ, または送信からの結果として, 組織の運用(ミッション, 職務, イメージ, または風評を含めて), 組織の資産, 及び個人に対するリスクを定期的にアセスメントする。		12.6.1*
	3.11.2 定期的に, 及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに, それらのシステム及びアプリケーションの脆弱性についてスキャンする。		12.6.1*
	3.11.3 リスクのアセスメントに従い, 脆弱性を修正する。		12.6.1*
3.12	**セキュリティアセスメント**		
	3.12.1 管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために, 組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。		14.2.8, 18.2.2, 18.2.3
	3.12.2 欠陥を修正し, 組織のシステムにおける脆弱性を軽減し, または取り除くために設計された行動計画を策定し, 実施する。	6.1.3	
	3.12.3 管理策の継続的な有効性を保証するため, 継続的にセキュリティ管理策を監視する。	9.1	
	3.12.4 システムの境界, システムの運用環境, セキュリティ要件の実装方法, 及び他のシステムとの関係または他のシステムへのコネクションについて記述した, システムセュリティ計画を策定, 文書化し, 定期的に更新する。		6.1.2

不許複製 JASA

	SP800-171 の管理策	4.2 章	5 章
3.13	**システムと通信の保護**		
	3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち，組織のシステムによって送信または受信される情報）を監視し，制御し，保護する。		13.1.1，13.1.3，13.2.1，14.1.3
	3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。		13.1.1，13.1.3，13.2.1，14.1.3，14.2.5
	3.13.3 利用者機能をシステム管理機能と分離する。		14.2.5
	3.13.4 共有システム資源を介した，不正な予期せぬ情報の転送を防止する。		14.1.1
	3.13.5 内部ネットワークから物理的にまたは論理的に分離される，公開アクセス可能なシステムコンポーネント用には，サブネットワークを実装する。		13.1.1，13.1.3，13.2.1，14.1.3
	3.13.6 デフォルトでネットワーク通信トラフィクを拒否し，また例外によってネットワーク通信トラフィクを許可する(即ち，すべて拒否，例外で許可)。		13.1.1
	3.13.7 リモートデバイスが，組織のシステムとの非リモートコネクションの確立と同時に，外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。		13.1.1
	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。		8.2.3，13.1.1，13.2.1，14.1.2，14.1.3
	3.13.9 セション終了時または定義された非アクティブな時間の経過後に，通信セションに対応しているネットワークコネクションを終了する。		13.1.1
	3.13.10 組織のシステムで採用された暗号のための暗号鍵を確立し，管理する。		10.1.2
	3.13.11 CUI の機密性を保護するために使用されるとき，FIPS 認証された暗号を採用する。		10.1.1，14.1.2，14.1.3，18.1.5
	3.13.12 共同コンピューティングデバイスのリモートからの活性化を禁止し，デバイス利用者にデバイス使用可を通知する。		13.2.1*
	3.13.13 モバイルコードの使用を管理し監視する。		13.2.1
	3.13.14 VoIP 技術の使用を管理し，監視する。		13.2.1
	3.13.15 通信セションの真正性を保護する。		13.2.3
	3.13.16 保存された CUI の機密性を保護する。		8.2.1，8.2.3*
3.14	**システムと通信の保護と情報の完全性**		
	3.14.1 タイムリーなやり方で情報及びシステムフローを識別し，報告し，訂正する。		12.6.1，14.2.2，14.2.3，16.1.3
	3.14.2 組織のシステム内の適切な場所で，悪意のあるコードから保護を提供する。		12.2.1
	3.14.3 システムセキュリティ警報及びアドバイザリを監視し，適切な対応アクションを取る。		6.1.4*
	3.14.4 新しいリリースが利用可能となったとき，悪意のあるコードからの保護メカニズムをアップデートする。		12.2.1
	3.14.5 組織のシステムの定期的スキャン，及びファイルがダウンロードされ，開かれ，または実行されるような，外部情報源からのファイルのリアルタイムスキャンを実行する。		12.2.1
	3.14.6 内向き及び外向きの通信トラフィクを含めて，攻撃や潜在的な攻撃の兆候を検知するため，組織のシステムを監視する。		12.4.1
	3.14.7 組織のシステムの不正な使用を識別する。		12.4.1

不許複製　JASA

附属書 C(参考) 4.3 節及び 5 章と NIST SP.800-171 の対応関係

表 C.1, 表 C.2 は, 附属書 B の逆引き表である。本書(JIS Q 27001, JIS Q 27002 および各々の拡張)と, NIST SP.800-171 との対応関係を示す。

表 C.1, 表 C.2 において, 網掛の有無, 赤字管理策, *印付き管理策は次を意味する。

網掛あり: NIST SP.800-171 の附属書 D で, ISO/IEC 27001 の附属書 A と対応していると記載されている管理策

網掛なし: 同, ISO/IEC 27001 の附属書 A と直接の対応はないと記載されているが, 27001 の本文または 27002 の実施の手引レベルで対応付けられる管理策

*印付き管理策: 同, ISO/IEC 27001 の Annex A と対応するものの NIST の管理策の意図を十分に満たしていないと記載されているが, 27002 の実施の手引レベルで対応付けられる管理策

赤字管理策: NIST SP.800-171 の管理策に対応していないため, 本書で読み替えまたは追記した管理策

C.1 4.3 章と NIST SP.800-171 の対応関係

表 C.1 4.3 章と NIST SP.800-171 の対応関係

4.3 章	NIST SP.800-171
6.1 リスク及び機会に対処する活動	
6.1.3	3.6.3 組織のインシデント対応能力をテストする。
6.1.3	3.7.1 組織のシステムにおいて保守を実施する。
6.1.3	3.12.2 欠陥を修正し, 組織のシステムにおける脆弱性を軽減し, または取り除くために設計された行動計画を策定し, 実施する。
9.1 監視, 測定, 分析及び評価	
9.1	3.3.1 非合法の, 許可されない, または不適切なシステムアクティビティの監視, 分析, 調査, 及び報告を可能とするために必要な範囲で, システム監査記録を作成, 保護, 及び維持する。
9.1	3.3.2 個別のシステム利用者のアクションが, 彼らのアクションについての説明責任を維持可能にするよう, それらの利用者に対して一意に追跡が可能であることを保証する。
9.1	3.3.4 監査プロセス失敗の事象においてアラート(警告) を発する。
9.1	3.12.3 管理策の継続的な有効性を保証するため, 継続的にセキュリティ管理策を監視する。
9.3 マネジメントレビュー	
9.3	3.3.3 監査された事象をレビューし, アップデートする。
10.1 不適合及び是正処置	
10.1	3.3.3 監査された事象をレビューし, アップデートする。

C.2 5 章と NIST SP.800-171 の対応関係

表 C.2 5 章と NIST SP.800-171 の対応関係

JIS Q 27002	NIST SP.800-171
6.1 内部組織	
6.1.2	3.1.4 共謀のない悪意のあるアクティビティのリスク低減のため, 個人の職務を分離する。

不許複製 JASA

JIS Q 27002	NIST SP.800-171
6.1.2	3.12.4 システムの境界，システムの運用環境，セキュリティ要件の実装方法，及び他のシステムとの関係または他のシステムへのコネクションについて記述した，システムセュリティ計画を策定，文書，及び定期的に更新する。
6.1.3	3.6.2 組織の内部及び外部の両方の，適切な担当官及び／または権威に対して，インシデントについての追跡，文書化，及び報告を行う。
6.1.4	3.14.3 システムセキュリティ警報及びアドバイザリを監視し，適切な対応アクションを取る。
6.1.5	3.6.2 組織の内部及び外部の両方の，適切な担当官及び／または権威に対して，インシデントについての追跡，文書化，及び報告を行う。
6.2 モバイル機器及びテレワーキング	
6.2.1	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
6.2.1	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
6.2.1	3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。
6.2.1	3.1.18 モバイルデバイスのコネクションを制御する。
6.2.1	3.1.19 モバイルデバイス及びモバイルコンピューティングプラットフォーム上の CUI を暗号化する。
6.2.1	3.8.6 代替の物理的予防手段による保護がない限り，持ち出し中はディジタル媒体上に格納された CUI の機密性を保護するための暗号学的メカニズムを実装する。
6.2.1	3.8.8 ポータブルストレージデバイスに識別可能な所有者がいないとき，このようなデバイスの使用を禁止する。
6.2.2	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
6.2.2	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
6.2.2	3.10.6 代替の作業サイト(例，テレワークのサイト)での CUI に対する防護対策を強制(実施)する。
7.1 雇用前	
7.1.1	3.9.1 CUI を含む組織のシステムへのアクセスを許可する前に，個人を審査する。
7.2 雇用期間中	
7.2.2	3.2.1 組織のシステムの責任者，システム管理者，及び利用者が，彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー，基準，及び手順について周知されていることを確実にする。
7.2.2*	3.2.2 組織の要員が，その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを，保証する。
7.2.2	3.2.3 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。
7.2.2*	3.6.1 適切な準備，検知，分析，抑制（封じ込め)，リカバリ，及び利用者対応アクティビティを含めて，組織のシステムのための運用上のインシデントハンドリング能力を確立する。
7.3 雇用の終了及び変更	
7.3.1	3.9.2 離職または配置転換等の人事措置の間と後で，CUI 及び CUI を含む組織のシステムが保護されることを保証する。
8.1 資産に対する責任	
8.1.1	3.4.1 個別のシステム開発ライフサイクル全体で，組織のシステム（ハードウェア，ソフトウェア，ファームウェア，及び文書を含めて）のベースライン構成とインベントリを確立し，維持する。
8.1.2	3.1.22 公開アクセス可能なシステムにおいて掲載または処理される CUI を制御する。
8.1.2	3.4.1 個別のシステム開発ライフサイクル全体で，組織のシステム（ハードウェア，ソフトウェア，ファームウェア，及び文書を含めて）のベースライン構成とインベントリを確立し，維持する。
8.2 情報分類	
8.2.2	3.8.4 CUI のマーク表示と配付制限が必要な媒体に対して表示を行う。
8.2.3	3.8.1 紙及びディジタルの両方の，CUI を含む，システム媒体を保護する(即ち，物理的に制御及びセキュアに格納する)。

不許複製　JASA

JIS Q 27002	NIST SP.800-171
8.2.3	3.8.2 システム媒体上の CUI へのアクセスを許可された利用者に制限する。
8.2.3	3.8.3 廃棄または再利用のために手放す前に，CUI を含むシステム媒体をサニタイズまたは破壊する。
8.2.3	3.8.5 CUI を含む媒体へのアクセスを制御し，管理エリアの外部への持ち出し中の媒体の説明責任を維持する。
8.2.3	3.8.7 システムコンポーネント上の取り外し可能な媒体の使用を管理する。
8.2.3	3.10.1 組織のシステム，装置，及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。
8.2.3	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。
8.2.3	3.13.16 保存された CUI の機密性を保護する。
8.3 媒体の取扱い	
8.3.1	3.1.21 外部システム上での組織のポータブルストレージデバイスの使用を制限する。
8.3.1	3.8.1 紙及びディジタルの両方の，CUI を含む，システム媒体を保護する(即ち，物理的に制御及びセキュアに格納する)。
8.3.1	3.8.2 システム媒体上の CUI へのアクセスを許可された利用者に制限する。
8.3.1	3.8.3 廃棄または再利用のために手放す前に，CUI を含むシステム媒体をサニタイズまたは破壊する。
8.3.1	3.8.5 CUI を含む媒体へのアクセスを制御し，管理エリアの外部への持ち出し中の媒体の説明責任を維持する。
8.3.1	3.8.7 システムコンポーネント上の取り外し可能な媒体の使用を管理する。
8.3.2	3.8.3 廃棄または再利用のために手放す前に，CUI を含むシステム媒体をサニタイズまたは破壊する。
8.3.3	3.8.5 CUI を含む媒体へのアクセスを制御し，管理エリアの外部への持ち出し中の媒体の説明責任を維持する。
9.1 アクセス制御に対する業務上の要求事項	
9.1.2	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
9.1.2	3.1.5 具体的なセキュリティ機能と特権アカウントを含め，特権の最小化の原則を採用する。
9.1.2	3.1.14 管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。
9.1.2	3.1.15 特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。
9.2 利用者アクセスの管理	
9.2.1	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
9.2.1	3.5.1 システム利用者，利用者を代行して動作するプロセス，またはデバイスを識別する。
9.2.1	3.5.5 定義された期間について，識別コードの再利用を禁止する。
9.2.1	3.5.6 定義された非アクティブな期間の後，識別子を無効化する。
9.2.2	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
9.2.3	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
9.2.3	3.1.5 具体的なセキュリティ機能と特権アカウントを含め，特権の最小化の原則を採用する。
9.2.3	3.1.6 非セキュリティ機能をアクセスするときは，非特権アカウントまたは役割を使用する。
9.2.3,	3.1.7 非特権利用者による特権機能の実行を防止し，このような機能の実行を監査する。
9.2.3	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，強制（実施）する。
9.2.4	3.5.2 組織のシステムへのアクセスの許可に対する必要条件として，それらの利用者，プロセス，またはデバイスのアイデンティティを認証(または検証)する。
9.2.5	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
9.2.6	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。

不許複製　JASA

JIS Q 27002	NIST SP.800-171
9.3 利用者の責任	
9.3.1	3.5.2 組織のシステムへのアクセスの許可に対する必要条件として，それらの利用者，プロセス，またはデバイスのアイデンティティを認証(または検証)する。
9.4 システム及びアプリケーションのアクセス制御	
9.4.1	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
9.4.2	3.1.8 ログイン試行失敗を制限する。
9.4.2	3.1.9 適用可能な CUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。
9.4.2	3.1.11 定義された条件の後，利用者セションを(自動的に) 終了する。
9.4.2	3.1.12 リモートアクセスセションを監視し，制御する。
9.4.2	3.5.11 認証情報のフィードバックを目に見えないようにする。
9.4.3	3.5.2 組織のシステムへのアクセスの許可に対する必要条件として，それらの利用者，プロセス，またはデバイスのアイデンティティを認証(または検証)する。
9.4.3	3.5.7 新しいパスワードが作成されるとき，最小パスワード複雑性及び文字列の変更を強制(実施)する。
9.4.3	3.5.8 規定された生成回数の間，パスワードの再利用を禁止する。
9.4.3	3.5.9 永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。
9.4.3	3.5.10 暗号学的に保護されたパスワードのみを格納及び送信する。
9.4.4	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
9.4.4	3.1.5 具体的なセキュリティ機能と特権アカウントを含め，特権の最小化の原則を採用する。
9.4.5	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
9.4.5	3.1.5 具体的なセキュリティ機能と特権アカウントを含め，特権の最小化の原則を採用する。
9.4.5	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，強制（実施）する。
10.1 暗号による管理策	
10.1.1	3.13.11 CUI の機密性を保護するために使用されるとき，FIPS 認証された暗号を採用する。
10.1.2	3.13.10 組織のシステムで採用された暗号のための暗号鍵を確立し，管理する。
11.1 セキュリティを保つべき領域	
11.1.1	3.10.2 物理的設備を保護し，監視し，組織のシステムの基盤をサポートする。
11.1.1	3.10.3 訪問者をエスコートし，訪問者の活動を監視する。
11.1.2*	3.10.1 組織のシステム，装置，及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。
11.1.2	3.10.4 物理的アクセスの監査ログを維持する。
11.1.3	3.10.1 組織のシステム，装置，及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。
11.1.3	3.10.5 物理的アクセスデバイスを制御し，管理する。
11.2 装置	
11.2.4	3.7.1 組織のシステムにおいて保守を実施する。
11.2.4	3.7.2 システム保守を実施するために使用されるツール，手法，メカニズム，及び要員における有効な管理策を提供する。
11.2.4*	3.7.3 オフサイトの保守のために除去される装置は，あらゆる CUI についてサニタイズされることを保証する。
11.2.4	3.7.5 外部のネットワークコネクションを介した非ローカル保守セションを確立するため，複数要素の認証を要求し，非ローカル保守の完了時にこのようなセションを終了する。
11.2.4	3.7.6 必要なアクセス許可のない保守要員の保守活動を監督する。
11.2.5*	3.7.1 組織のシステムにおいて保守を実施する。
11.2.5*	3.7.3 オフサイトの保守のために除去される装置は，あらゆる CUI についてサニタイズされることを保証する。

不許複製 JASA

JIS Q 27002	NIST SP.800-171
11.2.5	3.8.5 CUI を含む媒体へのアクセスを制御し，管理エリアの外部への持ち出し中の媒体の説明責任を維持する。
11.2.6	3.1.18 モバイルデバイスのコネクションを制御する。
11.2.6	3.1.20 外部システムへのコネクション及び使用を検証し，制御／制限する。
11.2.6	3.8.5 CUI を含む媒体へのアクセスを制御し，管理エリアの外部への持ち出し中の媒体の説明責任を維持する。
11.2.6	3.10.6 代替の作業サイト(例，テレワークのサイト)での CUI に対する防護対策を強制(実施)する。
11.2.7	3.8.3 廃棄または再利用のために手放す前に，CUI を含むシステム媒体をサニタイズまたは破壊する。
11.2.8	3.1.10 非アクティブな時間の経過後，データのアクセス及び閲覧を防止するため，パターンによる不可視化表示を用いてセションロックを使用する。
11.2.9	3.1.10 非アクティブな時間の経過後，データのアクセス及び閲覧を防止するため，パターンによる不可視化表示を用いてセションロックを使用する。
11.2.9	3.8.1 紙及びディジタルの両方の，CUI を含む，システム媒体を保護する(即ち，物理的に制御及びセキュアに格納する)。
11.2.9	3.8.2 システム媒体上の CUI へのアクセスを許可された利用者に制限する。
12.1 運用の手順及び責任	
12.1.1	3.4.2 組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し，実施 する。
12.1.2	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，強制（実施）する。
12.1.4	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，強制（実施）する。
12.2 マルウェアからの保護	
12.2.1	3.2.1 組織のシステムの責任者，システム管理者，及び利用者が，彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー，基準，訓練されていることを，保証する。
12.2.1	3.2.2 組織の要員が，その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを，保証する。
12.2.1	3.7.4 組織のシステム内で媒体が使用される前に，悪意のあるコードが入っていないか診断及びテストプログラムを用いて媒体をチェックする。
12.2.1	3.14.2 組織のシステム内の適切な場所で，悪意のあるコードから保護を提供する。
12.2.1	3.14.4 新しいリリースが利用可能となったとき，悪意のあるコードからの保護メカニズムをアップデートする。
12.2.1	3.14.5 組織のシステムの定期的スキャン，及びファイルがダウンロードされ，開かれ，または実行されるような，外部情報源からのファイルのリアルタイムスキャンを実行する。
12.2.2	3.4.3 組織のシステムへの変更を追跡，レビュー，承認／非承認，及び監査する。
12.3 バックアップ	
12.3.1	3.8.9 保存場所にあるバックアップ CUI の機密性を保護する。
12.4 ログ取得及び監視	
12.4.x	3.3.5 監査記録のレビュー，分析，及び調査のための報告プロセスを集めて相互の関係を比較し，不適切な，疑わしい，または異常なアクティビティの兆候に対応している。
12.4.x	3.3.6 オンデマンド分析と報告をサポートするため，監査の簡素化と報告書生成を提供する。
12.4.1	3.1.7 非特権利用者による特権機能の実行を防止し，このような機能の実行を監査する。
12.4.1*	3.3.1 非合法の，許可されない，または不適切なシステムアクティビティの監視，分析，調査，及び報告を可能とするために必要な範囲で，システム監査記録を作成，保護，及び維持する。
12.4.1*	3.3.2 個別のシステム利用者のアクションが，彼らのアクションについての説明責任を維持可能にするよう，それらの利用者に対して一意に追跡が可能であることを保証する。
12.4.1	3.14.6 内向き及び外向きの通信トラフィクを含めて，攻撃や潜在的な攻撃の兆候を検知するため，組織のシステムを監視する。
12.4.1	3.14.7 組織のシステムの不正な使用を識別する。

不許複製 JASA

JIS Q 27002	NIST SP.800-171
12.4.2	3.3.8 監査情報と監査ツールを不正なアクセス，改変，及び削除から保護する。
12.4.3	3.3.1 非合法の，許可されない，または不適切なシステムアクティビティの監視，分析，調査，及び報告を可能とするために必要な範囲で，システム監査記録を作成，保護，及び維持する。
12.4.3	3.3.2 個別のシステム利用者のアクションが，彼らのアクションについての説明責任を維持可能にするよう，それらの利用者に対して一意に追跡が可能であることを保証する。
12.4.3	3.3.3 監査された事象をレビューし，アップデートする。
12.4.3	3.3.8 監査情報と監査ツールを不正なアクセス，改変，及び削除から保護する。
12.4.4	3.3.7 監査記録のタイムスタンプを生成するための正式な情報源を用いて，内部システムクロックを比較し同期するようなシステム機能を提供する。
12.5 運用ソフトウェアの管理	
12.5.1	3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し，文書化し，承認し，強制（実施）する。
12.5.1*	3.4.6 基本機能のみを提供するように組織のシステムを構成することによって，最小機能の原則を採用する。
12.5.1	3.4.7 非基本プログラム，機能，ポート，プロトコル，及びサービスの使用を制限，無効化，及び防止する。
12.5.1	3.4.8 許可されないソフトウェアの使用を防止するために例外による拒否（ブラックリスト）ポリシーを，または許可されたソフトウェアの実行を許可するような例外による許可（ホワイトリスト)ポリシーを適用する。
12.5.1	3.4.9 利用者がインストールしたソフトウェアを管理し，監視する。
12.6 技術的ぜい弱性管理	
12.6.1*	3.11.1 組織のシステムの運用と関連する CUI の処理，ストレージ，または送信からの結果として，組織の運用(ミッション，職務，イメージ，または風評を含めて)，組織の資産，及び個人に対するリスクを定期的にアセスメントする。
12.6.1*	3.11.2 定期的に，及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに，それらのシステム及びアプリケーションの脆弱性についてスキャンする。
12.6.1*	3.11.3 リスクのアセスメントに従い，脆弱性を修正する。
12.6.1	3.14.1 タイムリーなやり方で情報及びシステムフローを識別し，報告し，訂正する。
12.6.2	3.4.9 利用者がインストールしたソフトウェアを管理し，監視する。
13.1 ネットワークセキュリティ管理	
13.1.1	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
13.1.1	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
13.1.1	3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。
13.1.1	3.1.20 外部システムへのコネクション及び使用を検証し，制御／制限する。
13.1.1	3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち，組織のシステムによって送信または受信される情報）を監視し，制御し，保護する。 3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。
13.1.1	3.13.5 内部ネットワークから物理的にまたは論理的に分離される，公開アクセス可能なシステムコンポーネント用には，サブネットワークを実装する。
13.1.1	3.13.6 デフォルトでネットワーク通信トラフィクを拒否し，また例外によってネットワーク通信トラフィクを許可する(即ち，すべて拒否，例外で許可)。
13.1.1	3.13.7 リモートデバイスが，組織のシステムとの非リモートコネクションの確立と同時に，外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。
13.1.1	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。
13.1.1	3.13.9 セション終了時または定義された非アクティブな時間の経過後に，通信セションに対応しているネットワークコネクションを終了する。
13.1.2	3.1.17 認証と暗号化を用いて無線アクセスを保護する。

不許複製 JASA

JIS Q 27002	NIST SP.800-171
13.1.3	3.1.3 承認された権限付与に従って CUI のフローを制御する。
13.1.3	3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち，組織のシステムによって送信または受信される情報）を監視し，制御し，保護する。 3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。
13.1.3	3.13.5 内部ネットワークから物理的にまたは論理的に分離される，公開アクセス可能なシステムコンポーネント用には，サブネットワークを実装する。
13.2 情報の転送	
13.2.1	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
13.2.1	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
13.2.1	3.1.3 承認された権限付与に従って CUI のフローを制御する。
13.2.1	3.1.13 リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。
13.2.1	3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。
13.2.1	3.1.18 モバイルデバイスのコネクションを制御する。
13.2.1	3.1.20 外部システムへのコネクション及び使用を検証し，制御／制限する。
13.2.1	3.5.3 複数要素の認証を，特権アカウントへのローカル及びネットワークアクセスのために，及び非特権アカウントへのネットワークアクセスのために，使用する。
13.2.1	3.5.4 特権及び非特権アカウントへのネットワークアクセスのために，リプレイ耐性のある認証メカニズムを採用する。
13.2.1	3.10.6 代替の作業サイト(例，テレワークのサイト)での CUI に対する防護対策を強制(実施)する。
13.2.1	3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち，組織のシステムによって送信または受信される情報）を監視し，制御し，保護する。
13.2.1	3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。
13.2.1	3.13.5 内部ネットワークから物理的にまたは論理的に分離される，公開アクセス可能なシステムコンポーネント用には，サブネットワークを実装する。
13.2.1	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。
13.2.1	3.13.12 共同コンピューティングデバイスのリモートからの活性化を禁止し，デバイス利用者にデバイス使用可を通知する。
13.2.1	3.13.13 モバイルコードの使用を管理し監視する。
13.2.1	3.13.14 VoIP 技術の使用を管理し，監視する。
13.2.3	3.1.20 外部システムへのコネクション及び使用を検証し，制御／制限する。
13.2.3	3.13.15 通信セションの真正性を保護する。
14.1 情報システムのセキュリティ要求事項	
14.1.1	3.3.9 監査機能の管理を特権利用者の一部に制限する。
14.1.1	3.13.4 共有システム資源を介した，不正な予期せぬ情報の転送を防止する。
14.1.2	3.1.1 システムアクセスを許可された利用者，許可された利用者を代行して動作するプロセス，またはデバイス(その他のシステムを含めて）に制限する。
14.1.2	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
14.1.2	3.1.3 承認された権限付与に従って CUI のフローを制御する。
14.1.2	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。
14.1.2	3.13.11 CUI の機密性を保護するために使用されるとき，FIPS 認証された暗号を採用する。

不許複製　JASA

JIS Q 27002	NIST SP.800-171
14.1.3	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
14.1.3	3.1.3 承認された権限付与に従って CUI のフローを制御する。
14.1.3	3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち，組織のシステムによって送信または受信される情報）を監視し，制御し，保護する。
14.1.3	3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。
14.1.3	3.13.5 内部ネットワークから物理的にまたは論理的に分離される，公開アクセス可能なシステムコンポーネント用には，サブネットワークを実装する。
14.1.3	3.13.8 代替の物理的予防手段による保護がない限り，持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。
14.1.3	3.13.11 CUI の機密性を保護するために使用されるとき，FIPS 認証された暗号を採用する。
14.2 開発及びサポートプロセスにおけるセキュリティ	
14.2.2	3.4.3 組織のシステムへの変更を追跡，レビュー，承認／非承認，及び監査する。
14.2.3	3.4.4 実装に先立ち，変更のセキュリティへの影響を分析する。
14.2.3	3.14.1 タイムリーなやり方で情報及びシステムフローを識別し，報告し，訂正する。
14.2.5	3.13.2 組織のシステム内の有効な情報セキュリティを促進するような，アーキテクチャ設計，ソフトウェア開発手法，及びシステムエンジニアリングの原則を採用する。
14.2.5	3.13.3 利用者機能をシステム管理機能と分離する。
14.2.8	3.12.1 管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために，組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。
16.1 情報セキュリティインシデントの管理及びその改善	
16.1.1	3.6.3 組織のインシデント対応能力をテストする。
16.1.2	3.3.1 非合法の，許可されない，または不適切なシステムアクティビティの監視，分析，調査，及び報告を可能とするために必要な範囲で，システム監査記録を作成，保護，及び維持する。
16.1.2	3.3.2 個別のシステム利用者のアクションが，彼らのアクションについての説明責任を維持可能にするよう，それらの利用者に対して一意に追跡が可能であることを保証する。
16.1.2	3.3.4 監査プロセス失敗の事象においてアラート(警告) を発する。
16.1.2	3.6.2 組織の内部及び外部の両方の，適切な担当官及び／または権威に対して，インシデントについての追跡，文書化，及び報告を行う。
16.1.3	3.14.1 タイムリーなやり方で情報及びシステムフローを識別し，報告し，訂正する。
16.1.4	3.3.1 非合法の，許可されない，または不適切なシステムアクティビティの監視，分析，調査，及び報告を可能とするために必要な範囲で，システム監査記録を作成，保護，及び維持する。
16.1.4	3.3.2 個別のシステム利用者のアクションが，彼らのアクションについての説明責任を維持可能にするよう，それらの利用者に対して一意に追跡が可能であることを保証する。
16.1.4	3.3.4 監査プロセス失敗の事象においてアラート(警告) を発する。
16.1.4	3.6.1 適切な準備，検知，分析，抑制（封じ込め），リカバリ，及び利用者対応アクティビティを含めて，組織のシステムのための運用上のインシデントハンドリング能力を確立する。
16.1.5	3.6.1 適切な準備，検知，分析，抑制（封じ込め），リカバリ，及び利用者対応アクティビティを含めて，組織のシステムのための運用上のインシデントハンドリング能力を確立する。
16.1.6	3.6.1 適切な準備，検知，分析，抑制（封じ込め），リカバリ，及び利用者対応アクティビティを含めて，組織のシステムのための運用上のインシデントハンドリング能力を確立する。
17.1	
17.1.2	3.8.9 保存場所にあるバックアップ CUI の機密性を保護する。
18.1	
18.1.3	3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。
18.1.3	3.3.8 監査情報と監査ツールを不正なアクセス，改変，及び削除から保護する。
18.1.3	3.8.9 保存場所にあるバックアップ CUI の機密性を保護する。

不許複製　JASA

JIS Q 27002	NIST SP.800-171
18.1.5	3.13.11 CUI の機密性を保護するために使用されるとき，FIPS 認証された暗号を採用する。
18.2	
18.2.2	3.12.1 管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために，組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。
18.2.3	3.12.1 管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために，組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。

不許複製　JASA