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
Information technology-Security techniques-Information security management systems-Overview and vocabulary

2 用語及び定義

2.1 アクセス制御（access control）
資産へのアクセスが、事業上及びセキュリティの要求事項に基づいて認可及び制限されることを確実にする手段。

2.2 分析モデル（analytical model）
一つ以上の基本測定量（2.10）及び／又は導出測定量（2.22）をそれに関連する判断基準と結合するアルゴリズム又は計算。

2.3 攻撃（attack）
資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。

2.4 属性（attribute）
人手又は自動的な手段によって、定量的又は定性的に識別できる対象物（2.55）の特性又は特徴。

2.5 監査（audit）
監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセス（2.61）。
注記 1：監査は、内部監査（第一者）又は外部監査（第二者・第三者）のいずれでも、又は複合監査　（複数の分野の組合せ）でもあり得る。
注記 2：“監査証拠”及び“監査基準”は、JIS Q 19011 に定義されている。

2.6 監査範囲（audit scope）
監査（2.5）の及ぶ領域及び境界。

2.7 認証（authentication）
エンティティの主張する特性が正しいという保証の提供。
注記：エンティティは、“実体”、“主体”などともいう。情報セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味する。

2.8 真正性（authenticity）
エンティティは、それが主張するとおりのものであるという特性。

2.9 可用性（availability）
認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

2.10 基本測定量（base measure）
単一の属性（2.4）とそれを定量化するための方法とで定義した測定量（2.47）。
注記：基本測定量は、他の測定量と機能的に独立した測定量をいう。

2.11 力量（competence）
意図した結果を達成するために、知識及び技能を適用する能力。

2.12 機密性（confidentiality）
認可されていない個人、エンティティ又はプロセス（2.61）に対して、情報を使用させず、また、開示しない特性。

2.13 適合（conformity）
要求事項（2.63）を満たしていること。
注記：対応国際規格の注記では、英語の語句の同義語について説明しているが、この規格では不要であり、削除した。

2.14 結果（consequence）
目的（2.56）に影響を与える事象（2.25）の結末（outcome）。
注記 1：一つの事象が、様々な結果につながることがある。
注記 2：結果は、確かなことも不確かなこともある。情報セキュリティの文脈において、結果は、通常、好ましくないものである。
注記 3：結果は、定性的にも定量的にも表現されることがある。
注記 4：初期の結果が、連鎖によって、段階的に増大することがある。

2.15 継続的改善（continual improvement）
パフォーマンス（2.59）を向上するために繰り返し行われる活動。

2.16 管理策（control）
リスク（2.68）を修正（modifying）する対策。
注記 1：管理策には、リスクを修正するためのあらゆるプロセス、方針、仕掛け、実務及びその他の処置を含む。　注記 2：管理策が、常に意図又は想定した修正効果を発揮するとは限らない。

2.17 管理目的（control objective）
管理策（2.16）を実施した結果として、達成することを求められる事項を記載したもの。

2.18 修正（correction）
検出された不適合（2.53）を除去するための処置。

2.19 是正処置（corrective action）
不適合（2.53）の原因を除去し、再発を防止するための処置。

2.20 データ（data）
基本測定量（2.10）、導出測定量（2.22）及び／又は指標（2.30）に割り当てられた値の集合。

2.21 判断基準（decision criteria）
アクション若しくは追加調査の必要性を決めるため又は与えられた結果の信頼度のレベルを記述するために使う、しきい（閾）値、目標又はパターン。

2.22 導出測定量（derived measure）
複数の基本測定量（2.10）の値の関数として定義した測定量（2.47）。

2.23 文書化した情報（documented information）
組織（2.57）が管理し、維持するよう要求されている情報、及びそれが含まれている媒体。
注記 1：文書化した情報は、あらゆる形式及び媒体の形をとることができ、あらゆる情報源から得ることができる。　注記 2：　文書化した情報には、次に示すものがあり得る。
－ 関連するプロセス（2.61）を含むマネジメントシステム（2.46）
－ 組織の運用のために作成された情報（文書類）
－ 達成された結果の証拠（記録）

2.24 有効性（effectiveness）
計画した活動を実行し、計画した結果を達成した程度。

2.25 事象（event）
ある一連の周辺状況の出現又は変化。
注記 1：事象は、発生が一度以上であることがあり、幾つかの原因をもつことがある。
注記 2：事象は、何かが起こらないことを含むことがある。
注記 3：事象は、“事態（incident）”又は“事故（accident）”と呼ばれることがある。
なお、“事態”は、“インシデント”とも表現される。

2.26 業務執行幹部（executive management）
組織（2.57）の目的を達成するための戦略及び方針を実施する責任を経営陣（2.29）から委ねられた個人又は人々の集団。
注記：業務執行幹部は、トップマネジメントと呼ばれることもあり、最高経営責任者、最高財務責任者、最高情報責任者及び類似の役割を含み得る。

2.27 外部状況（external context）
組織が自らの目的を達成しようとする場合の外部環境。
注記：外部状況には、次の事項を含むことがある。
－ 国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
－ 組織（2.57）の目的（2.56）に影響を与える主要な原動力及び傾向
－ 外部ステークホルダ（2.82）との関係並びに外部ステークホルダの認知及び価値観

2.28 情報セキュリティガバナンス（governance of information security）
組織（2.57）の情報セキュリティ活動を指導し、管理するシステム。

2.29 経営陣（governing body）
組織（2.57）のパフォーマンス（2.59）及び適合性について説明責任を負う個人又はグループ。
注記 1：経営陣は、法域によっては、取締役会でもあり得る。

2.30 指標（indicator）
定義された情報ニーズ（2.31）に関して分析モデル（2.2）から導出した、特定の属性（2.4）の見積り又は評価を示す測定量（2.47）。

2.31 情報ニーズ（information need）
目的、目標、リスク及び問題点を管理するために必要となる見解。

2.32 情報処理施設、情報処理設備（information processing facilities）
あらゆる情報処理のシステム、サービス若しくは基盤、又はこれらを収納する物理的場所。

2.33 情報セキュリティ（information security）
情報の機密性（2.12）、完全性（2.40）及び可用性（2.9）を維持すること。
注記：さらに、真正性（2.8）、責任追跡性、否認防止（2.54）、信頼性（2.62）などの特性を維持することを含めることもある。

2.34 情報セキュリティ継続（information security continuity）
継続した情報セキュリティ（2.33）の運用を確実にするためのプロセス（2.61）及び手順。

2.35 情報セキュリティ事象（information security event）
情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象（2.25）。

2.36 情報セキュリティインシデント（information security incident）
望まない単独若しくは一連の情報セキュリティ事象（2.35）、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティ（2.33）を脅かす確率が高いもの。

2.37 情報セキュリティインシデント管理（information security incident management）
情報セキュリティインシデント（2.36）を検出し、報告し、評価し、応対し、対処し、更にそこから学習するためのプロセス（2.61）。

2.38 情報共有コミュニティ（information sharing community）
情報を共有することに合意した組織のグループ。
注記：組織は、個人であることもある。

2.39 情報システム（information system）
アプリケーション、サービス、IT 資産、及び情報を取り扱う他の構成要素。

2.40 完全性（integrity）
正確さ及び完全さの特性。

2.41 利害関係者（interested party）
ある決定事項若しくは活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している、個人又は組織（2.57）。

2.42 内部状況（internal context）
組織が自らの目的を達成しようとする場合の内部環境。
注記：内部状況には、次の事項を含むことがある。
－ 統治、組織体制、役割及びアカウンタビリティ
－ 方針、目的及びこれらを達成するために策定された戦略
－ 資源及び知識としてみた場合の能力（例えば、資本、時間、人員、プロセス、システム、技術）
－ 情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
－ 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
－ 組織の文化
－ 組織が採択した規格、指針及びモデル
－ 契約関係の形態及び範囲

2.43 ISMS
プロジェクト（ISMS project）ISMS を実施するために組織（2.57）が取り組む構造化された活動。

2.44 リスクレベル（level of risk）
結果（2.14）とその起こりやすさ（2.45）の組合せとして表現される、リスク（2.68）の大きさ。

2.45 起こりやすさ（likelihood）
何かが起こる可能性。

2.46 マネジメントシステム（management system）
方針（2.60）、目的（2.56）及びその目的を達成するためのプロセス（2.61）を確立するための、相互に関連する又は相互に作用する、組織（2.57）の一連の要素。
注記 1：一つのマネジメントシステムは、単一又は複数の分野を取り扱うことができる。
注記 2：システムの要素には、組織の構造、役割及び責任、計画、運用などが含まれる。
注記 3：マネジメントシステムの適用範囲としては、組織全体、組織内の固有で特定された機能、組織内の固有で特定された部門、複数の組織の集まりを横断する一つ又は複数の機能、などがあり得る。

2.47 測定量（measure）
測定（2.48）の結果として値が割り当てられる変数。
注記：“測定量”という用語は、基本測定量、導出測定量及び指標をまとめて参照するために使う。

2.48 測定（measurement）
値を決定するプロセス（2.61）。

注記：情報セキュリティ（2.33）の文脈においては、値を決定するプロセスは、ISMS及びそれに関連する管理策（2.16）について、その有効性（2.24）に関する情報を必要とし、測定方法（2.50）、測定の関数（2.49）、分析モデル（2.2）及び判断基準（2.21）を用いる。

2.49 測定の関数（measurement function）
複数の基本測定量（2.10）を結合するために遂行するアルゴリズム又は計算。

2.50 測定方法（measurement method）
特定の尺度（2.80）に関して属性（2.4）を定量化するために使う一連の操作の論理的な順序を一般的に記述したもの。
注記：測定方法の類型は、属性を定量化するために使う操作の性質による。これには、次の二つの類型がある。
－ 主観的　人間の判断を含んだ定量化
－ 客観的　数値的な規則に基づいた定量化

2.51 測定結果（measurement results）
情報ニーズ（2.31）を取り扱う、一つ以上の指標（2.30）及びそれに関連する解釈。

2.52 監視（monitoring）
システム、プロセス（2.61）又は活動の状況を明確にすること。
注記：状況を明確にするために、点検、監督、又は注意深い観察が必要な場合もある。

2.53 不適合（nonconformity）
要求事項（2.63）を満たしていないこと。

2.54 否認防止（non-repudiation）
主張された事象又は処置の発生、及びそれを引き起こしたエンティティを証明する能力。

2.55 対象物（object）
属性（2.4）の測定（2.48）を通して特徴付けられるもの。

2.56 目的（objective）
達成する結果。
注記 1：　目的は、戦略的、戦術的又は運用的であり得る。
注記 2：　目的は、様々な領域［例えば、財務、安全衛生、環境の到達点（goal)］に関連し得るものであり、様々な階層［例えば、戦略的レベル、組織全体、プロジェクト単位、製品ごと、プロセス（2.61）ごと］で適用できる。
注記 3：目的は、例えば、意図する成果、目的（purpose)、運用基準など、別の形で表現することもできる。また、情報セキュリティ目的という表現の仕方もある。又は、同じような意味をもつ別の言葉［例：狙い（aim)、到達点（goal)、目標（target)］で表すこともできる。
注記 4：ISMS　の場合、組織は、特定の結果を達成するため、情報セキュリティ方針と整合のとれた情報セキュリティ目的を設定する。

2.57 組織（organization）
自らの目的（2.56）を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。
注記：組織という概念には、法人か否か、公的か私的かを問わず、自営業者、会社、法人、事務所、企業、当局、共同経営会社、非営利団体若しくは協会、又はこれらの一部若しくは組合せが含まれる。ただし、これらに限定されるものではない。

2.58 外部委託する（outsource）
ある組織の機能又はプロセス（2.61）の一部を外部の組織（2.57）が実施するという取決めを行う。
注記：外部委託した機能又はプロセスはマネジメントシステム（2.46）の適用範囲内にあるが、外部の組織はマネジメントシステムの適用範囲の外にある。

2.59 パフォーマンス（performance）
測定可能な結果。
注記 1：パフォーマンスは、定量的又は定性的な所見のいずれにも関連し得る。
注記 2：パフォーマンスは、活動、プロセス（2.61)、製品（サービスを含む。)、システム、又は組織（2.57）の運営管理に関連し得る。

2.60 方針（policy）
トップマネジメント（2.84）によって正式に表明された組織（2.57）の意図及び方向付け。

2.61 プロセス（process）
インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動。

2.62 信頼性（reliability）
意図する行動と結果とが一貫しているという特性。

2.63 要求事項（requirement）
明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待。
注記 1：“通常暗黙のうちに了解されている”とは、対象となるニーズ又は期待が暗黙のうちに了解されていることが、組織及び利害関係者にとって、慣習又は慣行であることを意味する。　注記 2：規定要求事項とは、例えば、文書化した情報の中で明示されている要求事項をいう。

2.64 残留リスク（residual risk）
リスク対応（2.79）後に残っているリスク（2.68)。
注記 1：残留リスクには、特定されていないリスクが含まれ得る。　注記 2：残留リスクは、“保有リスク”ともいう。

2.65 レビュー（review）
確定された目的を達成するため、対象となる事柄の適切性、妥当性及び有効性（2.24）を決定するために実行される活動。

2.66 レビュー対象物（review object）
レビューされる特定のもの。

2.67 レビュー目的（review objective）
レビューの結果として何を達成するのかを説明したもの。

2.68 リスク（risk）
目的に対する不確かさの影響。
注記 1：影響とは、期待されていることから、好ましい方向又は好ましくない方向にかい（乖）離することをいう。
注記 2：不確かさとは、事象（2.25)、その結果（2.14）又はその起こりやすさ（2.45）に関する、情報、理解又は知識が、たとえ部分的にでも欠落している状態をいう。
注記 3：リスクは、起こり得る事象（2.25)、結果（2.14）又はこれらの組合せについて述べることによって、その特徴を記述することが多い。
注記 4：リスクは、ある事象（周辺状況の変化を含む。）の結果（2.14）とその発生の起こりやすさ（2.45）との組合せとして表現されることが多い。
注記 5：ISMS　の文脈においては、情報セキュリティリスクは、情報セキュリティ目的に対する不確かさの影響として表現することがある。
注記 6：情報セキュリティリスクは、脅威（2.83）が情報資産のぜい弱性（2.89）又は情報資産グループのぜい弱性（2.89）に付け込み、その結果、組織に損害を与える可能性に伴って生じる。

2.69 リスク受容（risk acceptance）
ある特定のリスク（2.68）をとるという情報に基づいた意思決定。
注記 1：リスク対応（2.79）を実施せずにリスク受容となることも、又はリスク対応プロセス中にリスク受容となることもある。　注記 2：受容されたリスクは、モニタリング［監視（2.52)］及びレビュー（2.65）の対象となる。

2.70 リスク分析（risk analysis）
リスク（2.68）の特質を理解し、リスクレベル（2.44）を決定するプロセス。
注記 1：リスク分析は、リスク評価（2.74）及びリスク対応（2.79）に関する意思決定の基礎を提供する。　注記 2：：リスク分析は、リスクの算定を含む。

2.71 リスクアセスメント（risk assessment）
リスク特定（2.75)、リスク分析（2.70）及びリスク評価（2.74）のプロセス（2.61）全体。

2.72 リスクコミュニケーション及び協議（risk communication and consultation）
リスク（2.68）の運用管理について、情報の提供、共有又は取得、及びステークホルダ（2.82）との対話を行うために、組織が継続的に及び繰り返し行うプロセス。
注記 1：情報は、リスクの存在、特質、形態、起こりやすさ、重大性、評価、受容可能性及び対応に関係することがある。　注記 2：協議とは、ある事柄に関する意思決定又は方向性の決定に先立って、組織とそのステークホルダとの間で行われる、その事柄についての情報に基づいたコミュニケーションの双方向プロセスである。協議とは、次のようなものである。
－ 権力によってではなく、影響力によって、意思決定に影響を与えるプロセスである。
－ 共同で意思決定を行うことではなく、意思決定に対するインプットとなる。

2.73 リスク基準（risk criteria）
リスク（2.68）の重大性を評価するための目安とする条件。
注記 1：リスク基準は、組織の目的、外部状況及び内部状況に基づいたものである。
注記 2：リスク基準は、規格、法律、方針及びその他の要求事項から導き出されることがある。

2.74 リスク評価（risk evaluation）
リスク（2.68）及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析（2.70）の結果をリスク基準（2.73）と比較するプロセス（2.61)。
注記：リスク評価は、リスク対応（2.79）に関する意思決定を手助けする。

2.75 リスク特定（risk identification）
リスク（2.68）を発見、認識及び記述するプロセス。
注記 1：リスク特定には、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれる。　注記 2：リスク特定には、過去のデータ、理論的分析、情報に基づいた意見、専門家の意見及びステークホルダのニーズを含むことがある。

2.76 リスクマネジメント（risk management）
リスク（2.68）について、組織（2.57）を指揮統制するための調整された活動。

2.77 リスクマネジメントプロセス（risk management process）
コミュニケーション、協議及び組織の状況の確定の活動、並びにリスク（2.68）の特定、分析、評価、対応、モニタリング及びレビューの活動に対する、運用管理方針、手順及び実務の体系的な適用。
注記：ISO/IEC 27005 においては、リスクマネジメント全体を示すために“プロセス（process)”という用語を用いている。リスクマネジメントプロセス内の要素は、“活動（activities)”と呼ばれる。

2.78 リスク所有者（risk owner）
リスク（2.68）を運用管理することについて、アカウンタビリティ及び権限をもつ人又は主体。

2.79 リスク対応（risk treatment）
リスク（2.68）を修正するプロセス（2.61)。
注記 1：リスク対応には、次の事項を含むことがある。
－リスクを生じさせる活動を、開始又は継続しないと決定することによって、リスクを回避すること。
－ある機会を追求するために、リスクをとる又は増加させること。
－リスク源を除去すること。
－起こりやすさを変えること。
－結果を変えること。
－一つ以上の他者とリスクを共有すること(契約及びリスクファイナンシングを含む。)。
－情報に基づいた選択によって、リスクを保有すること。
注記 2：好ましくない結果に対処するリスク対応は、“リスク軽減”、“リスク排除”、“リスク予防”及び“リスク低減”と呼ばれることがある。
注記 3：リスク対応が、新たなリスクを生み出したり、又は既存のリスクを修正したりすることがある。

2.80 尺度（scale）
連続的若しくは離散的な値の順序集合又は分類の集合で、それに属性（2.4）を対応付けるもの。
－名義尺度　測定値は、分類した結果を示す。
－順序尺度　測定値は、離散的な階級に分けた結果を示す。
－間隔尺度　測定値は、属性の等しい量に対応して等しい距離を示す。
－比尺度　測定値は、属性の等しい量に対応して等しい距離を示し、ゼロという値は、その属性に対応するものが存在しないことを表す。
これらは、尺度の類型の例でしかない。

2.81 セキュリティ実施標準（security implementation standard）
セキュリティを実現するための認可された方法を規定した文書。

2.82 ステークホルダ（stakeholder）
意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。

2.83 脅威（threat）
システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。

2.84 トップマネジメント（top management）
最高位で組織（2.57）を指揮し、管理する個人又は人々の集まり。
注記 1：トップマネジメントは、組織内で、権限を委譲し、資源を提供する力をもっている。　注記 2：マネジメントシステム（2.46）の適用範囲が組織（2.57）の一部だけの場合、トップマネジメントとは、組織（2.57）内のその一部を指揮し、管理する人をいう。

2.85 信頼できる情報コミュニケーションエンティティ（trusted information communication entity）
情報共有コミュニティ内での情報交換を支援する、自立した組織。

2.86 測定の単位（unit of measurement）
取決め又は慣習に従って定義し採用した特別の量で、同じ種類の他の量をそれと比較することによって、その量の相対的な大きさを表現するためのもの。

2.87 妥当性確認（validation）
客観的証拠を提示することによって、特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること。

2.88 検証（verification）
客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること。

2.89 ぜい弱性（vulnerability）
一つ以上の脅威（2.83）によって付け込まれる可能性のある、資産又は管理策（2.16）の弱点。