这里给出ISO27001标准2013版的中文与日文各章节对照版本。

0.引言

0.1总则

本标准提供建立，实现，维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略性决策。组织信息安全管理体系的建立和实现受组织的需要和目标，安全要求，组织所采用的过程，规模和结构的影响。所有这些影响因素可能随时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性，完整性和可用性，并为相关方树立风险得到充分管理的信心。 重要的是，信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中，并且在过程，信息系统和控制的设计中要考虑到信息安全。

期望的是，信息安全管理体系的实现程度要与组织的需要相符合。

本标准可被内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中所表述要求的顺序不反映各要求的重要性或暗示这些要求要予实现的顺序。条款编号仅为方便引用。

ISO/IEC 27000描述了信息安全管理体系的概要和词汇，引用了信息安全管理体系标准族（包括ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005)□以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本标准应用ISO/IEC合并导则附录SL中定义的高层结构，相同条款标题，相同文本，通用术语和核心定义，因此维护了与其他采用附录SL的管理体系的标准具有兼容性。

附录SL中定义的通信途径对于选择运行单一管理体系来满足两个或更多管理体系标准要求的组织是有用的。

0　序文

この規格は、2013年に第2版として発行されたISO/IEC□27001に基に、技術的内容及び構成を変更することなく作成した日本工業規格である。

なお、この規格で点線の下線を施してある参考事項は、対応国際規格にはない事項もある。

0.1概要

この規格は、情報セキュリティマネジメント（以下□ISMSという。）を確立し、実施し、維持し、継続的に改善するための要求事項を提供するため作成された□ISMSの採用は、組織の戦略的決定である。

組織のISMSの確立及び実施は、その組織のニーズ及び目的、セキュリティ要求事項、組織が用いている

プロセス、並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらの要因全ては、時間とともに変化することが見込まれる。

ISMSは、リスクマネジメントプロセスお適用することによって情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。

ISMSを、組織のプロセス及びマネジメント構造（Management Structure）全体の一部とし、かつ、その中に組み込むこと、並びにプロセス、情報システム及び管理策を設計する上で情報セキュリティを考慮することは、重要である（ISMSの導入は、その組織のニーズに合わせた規模で行うことが期待される。

この規格は、組織自身の情報セキュリティ要求事項を満たす組織の能力を、組織の内部で評価するためにも、また、外部関係者が評価するためにも用いることができる。

この規格で示す要求事項の順序は、重要性を反映するものでもなく、実施する順序を示すものでもない。本文中の細別符号「例えば（a)（b)（又は1)、2)」は、参照目的のためだけに付記されている。

ISO/IEC（27000は、ISMSファミリ規格（ISO/IEC（27003（ISO/IEC（27004及びISO/IEC 27005を含む。）を参照さしながら（ISMSの概要について記載し、用語及び定義について規定していいる。

ISMSファミリ規格の用語及び定義について、**JIS Q（27000**が制定されています。

0.2　他のマネジメントシステム規格との両立性

この規格は、ISO/IEC専門業務用指針　第1部　統合版（ISO補足指針の**附属書（SL**に規定する上位構造（HLS),共通の細分箇条題名、共通テキスト並びに共通の用語及び中核となる定義を適用しており、**附属書SL**を採用した他のマネジメントシステム規格との両立性が保たれている。

附属書SLに規定するこの共通の取り組みは、二つ以上のマネジメントシステム規格の要求事項を満たす。

1.范围

本标准规定了在组织环境下建立，实现，维护和持续改进信息安全管理体系的要求。本标准还包括了根据组织所需求所剪裁的信息安全风险评估和处置的要求。

本标准规定的要求是通用的，适用于各种类型，规模或性质的组织。当组织声称符合本标准时，不能排除第4章到第10章中所规定的任何要求。

1.範囲

この規格は、組織の状況の下で、ISMSを確立し、実施し、維持し、継続的に改善するための要求事項について規定する。この規格は、組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項についても規定する。この規格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。組織がこの規格への適合を宣言する場合には、箇条（かじょう）4～箇条10に規定するいかなる要求事項の除外も認められない。

注記：この規格の対応国際規格及びその対応の程度を表す記号を、次に示す。

ISO/IEC 27001:2013 Information technology — Security techniques —- Information security management systems —- Requirements (IDT)

なお、対応の程度を表す記号"IDT"は、ISO/IEC Guide 21-1に基づき、"一致している"ことを示す。

2.规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 27000 信息技术 安全技术 信息安全管理体系 概述和词汇 (Information technoloy-Security techniques-Information security management systems-Overview and vocabulary)

次に掲げる（かかげる）規格は、この規格に引用することによって、この規格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 27000 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

注記：対応国際規格：ISO/IEC 27000 Information technolgoy – Security techniques — Information security management systems — Overview and vocabulary (MOD)

3.术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件

この規格で用いる主な用語及び定義は、JIS Q27000による。

4.组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

注：对这些事项的确定，参见ISO 31000:2009 5.3中建立外部和内部环境的内容。

4.1組織及びその状況の理解

組織は、組織の目的に関連し、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 Q31000:2010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 理解相关方的需求和期望

组织应确定：

a)信息安全管理体系相关方；

b)这些相关方与信息安全相关的要求。

注：相关方的要求可包括法律，法规要求和合同义务。

4.2　利害関係者のニーズ及び期待の理解

組織は、次の事項を決定しなければならない。

a) ISMSに関連する利害関係者

b) その利害関係の、情報セキュリティに関連する要求事項

注記：利害関係者の要求事項には、法的及び規制の要求事項並びに契約の義務を含めてもよい。

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。该范围应形成文件化信息并可用。

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

組織は、ISMSの適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。

この適用範囲を決定するとき、組織は、次の事項を考慮しなければならない。

a) 4.1に規定する外部及び内部の課題

b) 4.2に規定する要求事項

c) 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フェース及び依存関係

4.4 信息安全管理体系

组织应按照本标准的要求，建立，实现，维护和持续改进信息安全管理体系。

4.4　情報セキュリティマネジメントシステム

組織は、この規格の要求事項に従って、ISMSを確立し、実施し、維持し、かつ、継続的に改善しなければならない。

5.领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：

a)确保建立了信息安全策略和信息安全目标，并与组织战略方向一致；

b)确保将信息安全管理体系要求整合到组织过程中；

c)确保信息安全管理体系所需资源可用;

d)沟通有效的信息安全管理及符合信息安全管理体系要求的重要性;

e)确保信息安全管理体系达到预期结果;

f)指导并支持相关人员为信息安全管理体系的有效性做出贡献；

g)促进持续改进;

h)支持其他相关管理角色，以证实他们的领导按角色应用于其责任范围。

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、次に示す事項によって、ISMSに関するリーダーシップ及びコミットメントを実証しなければならない。

a)　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。

b)　組織のプロセスへのISMS要求事項の統合を確実にする。

c)　ISMSに必要な資源が利用可能であることを確実にする。

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

e)□ISMSがその意図しあ成果を達成することを確実にする。

f)□ISMSの有効性を寄与するよう人々を指揮し、支援する。

g)□継続的改善を促進する。

h)□その他の関連する管理層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、管理層の役割を支援する。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a)与组织意图相适宜；

b)包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c)包括对满足适用的信息安全相关要求的承诺；

d)包括对持续改进信息安全管理体系的承诺。

信息安全方针应：

e)形成文件化信息并可用；

f)在组织内得到沟通；

g)适当时，对相关方可用。

5.2方針

トップマネジメントは、次の事項を満たす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。

5.3 组织的角色，责任和权限

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通，最高管理层应分配责任和权限，以：

a)确保信息安全管理体系符合本标准的要求；

b)向最高管理者报告信息安全管理体系绩效。

注：最高管理层可以为组织内报告信息安全管理体系绩效，分配责任和权限。

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、伝達することを確実にしなければならない。

トップマネジメントは、次の事項に対して、責任及び権限を割り当てなければならない。

a)ISMSが、この規格の要求事項に適合することを確実にする。

b)ISMSのパフォーマンスをトップマネジメントに報告する。

注記

トップマネジメントは、ISMSのパフォーマンスを組織内に報告する責任及び権限を割り当ててもよい。

6.规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划信息安全管理体系时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a)确保信息安全管理体系可达到预期结果；

b)预防或减少不良影响；

c)达到持续改进。

组织应规划：

d)应对这些风险和机会的措施；

e)如何：

1)将这些措施整合到信息安全管理体系过程中，并予以实现；

2)评价这些措施的有效性。

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、組織は、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、次の事項のために対処する必要があるリスク及び機会を決定しなければならない。

a)ISMSが、その意図した成果を達成できることを確実にする。

b)望ましくない影響を防止又は低減する。

c)継続的改善を達成する。

組織は、次の事項を計画しなければならない。

d)上記によって決定したリスク及び機会に対処する活動

e)次の事項を行う方法

1)その活動のISMSプロセスへの統合及び実施

2)その活動の有効性の評価

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估过程，以：

a) 建立并维护信息安全风险准则，包括：

1）风险接受准则；

2）信息安全管理体系评估实施准则。

b)确保反复的信息安全风险评估产生一致的，有效的和可比较的结果。

c)识别信息安全风险：

1）应用信息安全风险评估过程，以识别信息安全管理体系范围内与信息保密性，完整性和可用性损失有关的风险；

2）识别风险责任人。

d)分析信息安全风险：

1）评估6.1.2c)中所识别的风险发生后，可能导致的潜在后果；

2）评估6.1.2c)中所识别的风险实际发生的可能性;

3. 确定风险级别。

e) 评价信息安全风险：

1）将风险分析结果与6.1.2a)中建立的风险准则进行比较；

2）为风险处置排序已分析风险的优先级。

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.2情報セキュリティリスクアセスメント

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

a)次を含む情報セキュリティのリスク基準を確立し、維持する。

1)リスク受容基準

2)情報セキュリティリスクアセスメントを実施するための基準

b)繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かた、比較可能な結果を生み出すことを確実にする。

c)次によって情報セキュリティリスクを特定する。

1)ISMSの適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。

2)これらのリスク所有者を特定する。

d)次によって情報セキュリティリスクを分析する。

1. 6.1.2 c) 1)で特定されたリスクが実際に生じした場合に起こり得る結果についえアセスメントを行う。
2. 6.1.2c) 2)で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3)リスクレベルを決定する。

e)次によって情報セキュリティリスクを評価する。

1)リスク分析の結果と6.1.2 a)で確立したリスク基準と比較する。

2)リスク対応のために、分析したリスクの優先順位付けを行う。

組織は、情報セキュリティリスクアセスメント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。

6.1.3 信息安全风险处置

组织应定义并应用信息安全风险处置过程，以：

a)在考虑风险评估结果的基础上，选择适合的信息安全风险处置选项；

b)确定实现已选的信息安全风险处置选项所必需的所有控制；

注1:当需要时，组织可设计控制，或识别来自任何来源的控制。

c)将6.1.3b)确定的控制与附录A中的控制进行比较，并验证没有忽略必要的控制；

注2:附录A包含了控制目标和控制的结合列表。本标准用户可在附录A的指导下，确保没有遗漏必要的控制。

注3:控制目标隐含在所选择的控制内。附录A所列的控制目标和控制并不是完备的，可能需要额外的控制目标和控制。

d)制定一个适用性声明(SoA Statement of Applicability)，包含必要的控制[见6.1.3b)和c]及其选择的合理性说明（无论该控制是否已实 现），以及对附录A控制删减的合理性说明；

e)制定正式的信息安全风险处置计划；

f)获得风险责任人对信息安全风险处置过程的文件化信息。

注4:本标准中的信息安全风险评估和处置过程与ISO 31000中给出的原则和通用指南相匹配。

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、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に示す管理策と比較し、必要な管理策がみおとされていないことを検証する。

注記1　附属書Aは、管理目的及び管理策の包括的なリスクである。この規格の利用者は、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、附属書Aに参照することがもとめられている。

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」及び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どうか
- 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。

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

この規格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 Q31000に規定する原則及び一般的な指針と整合している。

6.2 信息安全目标及其实现规划

组织应在相关职能和层级上建立信息安全目标。

信息安全应：

a 与信息安全方针一致；

b) 可测量（如可行）；

c) 考虑适用的信息安全要求，以及风险评估和风险处置的结果；

d) 得到沟通；

e) 适当时更新；

组织应保留有关信息安全目标的文件化信息。在规则如何达到信息安全目标时，组织应确定：

f) 要做什么；

g) 需要什么资源；

h) 由谁负责；

i) 什么时候完成；

j) 如何评价结果。

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

組織は、関連する部門及び階層において、情報セキュリティ目的を確立しなければならない。

情報セキュリティ目的は、次の事項を満たさなければならない。

a)情報セキュリティ方針と整合している。

b)（実行可能な場合）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。

組織は、情報セキュリティ目的に関する文書化した情報を保持しなければならない。

組織は、情報セキュリティ目的をどのように達成するかについて計画するとき、次の事項を決定しなければならない。

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.支持

7.1 资源

组织应确定并提供建立，实现，维护和持续改进信息安全管理体系所需的资源。

7.1資源

組織は、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、提供しなければならない。

7.2 能力

组织应：

a) 确定在组织控制下人事会影响组织信息安全绩效的工作人员的必要能力；

b) 确保上述人员在适当的教育，培训或经验的基础上能够胜任其工作；

c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d) 保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，例如针对现有雇员提供培训，指导或重新分配；雇佣或签约有能力的人员。

7.2力量

組織は、次の事項を行わなければならない。

a)組織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その管理下で行う人＊又は人々）に必要な力量を決定する。

b)適切な教育、訓練又は経験に基づいて、それらの人々が力量をそなえていることを確実にする。

c)該当する場合には、必ず、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。

d)力量の証拠つぉひて、適切な文書化した情報を保持する。

注記

適用される処置には、例えば、現在雇用している人々に対する、教育訓練の提供、指導の実施、配置転換の実施などがあり、また、力量を備えた人々の雇用、そうした人々との契約締結などもある。

7.3 意识

在组织控制下工作的人员应了解；

a) 信息安全方针；

b) 其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c) 不符合信息安全管理体系要求带来的影响。

7.3 認識

組織の管理下で働く人々は、次の事項に関して認識をもたなければならない。

a)情報セキュリティ方針

b)情報セキュリティパフォーマンスの向上によって得られる便益を含む、ISMSの有効性に対する自らの貢献

c)ISMS要求事項に適合しないことの意味

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部的沟通要求，包括：

a) 沟通什么；

b) 何时沟通；

c) 与谁沟通；

d) 谁来沟通；

e) 影响沟通的过程。

7.4コミュニケーション

組織は、次の事項を含め、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（何を伝達するか。）

b)コミュニケーションの実施時間

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

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a) 本标准要求的文件化信息；

b) 为信息安全管理体系的有效性，组织所确定的必要的文件化信息。

注：不同组织有关信息安全管理体系文件化信息的详略程序可以是不同的，这是由于：

1）组织的规模及其活动，过程，产品和服务的类型；

2. 过程及其相互作用的复杂性；
3. 人员的能力。

7.5.1　一般

組織のISMSは、次の事項を含まなければならなし。

a)この規格が要求する文書化した情報

b)ISMSの有効性のために必要であると組織が決定した、文書化した情報

注記

ISMSのための文書化した情報の程度は、次のような理由によって、それぞれの組織が異なる場合がある。

1)組織の規模、並びに活動、プロセス、製品及びサービスの種類

2)プロセス及びその相互作用の複雑さ

3)人々の力量

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a) 标准和描述（例如标题，日期，作者或引用编号）；

b) 格式（例如语言，软件版本，图表）和介质（例如纸质的，电子的）；

c) 对适宜性和充分性的评审和批准。

7.5.2　作成及び更新

文書化した情報を作成及び更新する際、組織は、次の事項を確実にしなければならない。

a)適切な識別及び記述（例えば、タイトル、日付、作成者、参照番号）

b)適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）

c)適切性及び妥当性に関する、適切なレビュー及び承認

7.5.3 文件化信息的控制

信息安全管理体系及本标准所要求的文件化信息应得到控制，以确保：

a) 在需要的地点和时间，是可用的适宜使用的；

b) 得到充分的保护（如避免保密性损失，不恰当使用，完整性损失等)。

为控制文件化信息，适用时，组织应强调以下活动：

c) 分发，访问，检索和使用；

d) 存储和保护，包括保持可持续性；

e) 控制变更（例如版本控制）；

f) 保留和处理。

组织确定的为规划和运行信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

注：访问隐含着仅允许浏览文件化信息，或允许和授权浏览及更改文件化信息等决定。

7.5.3　文書化した情報の管理

ISMS及びこの規格で要求されている文書化した情報は、次の事項を確実にするために、管理しなければならない。

a)文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態である。

b)文書化した情報が十分に保護されている（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。

文書化した情報の管理に当たって、組織は、該当する場合は、必ず、次の行動を取り組まなければならない。

c)配付、アクセス、検索及び利用

d)読みやすさが保たれることを含む、保管及び保存

e)変更の管理（例えば、版の管理）

f)保持及び廃棄

ISMSの計画及び運用のために組織はが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、管理しなければならない。

注記

アクセスとは、文書化した情報の閲覧だけの許可に関する決定、文書化した情報の閲覧及び変更の許可及び権限に関する決定、などを意味する。

8.运行

8.1 运行规划和控制

为了满足信息安全要求以及实现6.1中确定的措施，组织应规划，实现和控制所需要的过程。组织还应实现为达到6.2中确定的信息安全目标一系列计划。

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负责影响。

组织应确保外包过程是确定的和受控的。

8.1　運用の計画及び管理

組織は、情報セキュリティ要求事項を満たすため、及び6.1で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ管理しなければならない。また、組織は、6.2で決定した情報セキュリティ目的を達成するために計画を実施しなければならない。

組織は、プロセスが計画通りに実施されたという確信をもつために必要な程度の、文書化した情報を保持しなければならない。

組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとらなければならない。

組織は、外部委託したプロセスが決定され、かつ管理されていることを確実にしなければならない。

8.2 信息安全风险评估

组织应考虑6.1.2a)所建立的准则，按计划的时间间隔，或当重要变更提出或发生时，执行信息安全风险评估。

组织应保留信息安全风险评估结果的文件化信息。

8.2 情報セキュリティリスクアセスメント

組織は、あらかじめ定めた間隔で、又は重大な変更が提案されたか若しくは重大な変化が生じた場合に、6.1.2 a)で確立した基準を考慮して、情報セキュリティリスクアセスメントを実施しなければならない。

組織は、情報セキュリティリスクアセスメント結果を文書化した情報を保持しなければならない。

8.3 信息安全风险处置

组织应实现信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

8.3 情報セキュリティリスク対応

組織は、情報セキュリティリスク対応計画を実施しなければならない。

組織は、情報セキュリティリスク対応結果の文書化した情報を保持しなければならない。

9.绩效评价

9.1 监视，测量，分析和评价

组织应评价信息安全绩效以及信息安全管理体系的有效性。

组织应确定：

a) 需要被监视和测量的内容，包括信息安全过程和控制；

b) 适用的监视，测量，分析和评价的方法，以确保得到有效的结果；

注：所选的方法宜产生可比较和可再现的有效结果。

c) 何时应执行监视和测量；

d) 谁应监视和测量；

e) 何时应分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果。

组织应保留适当的文件化信息作为监视和测量结果的证据。

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。

9.2 内部审核

组织应按计划的时间间隔进行内部审核，以提供信息，确定信息安全管理体系：

a)是否符合：

1）组织自身对信息安全管理体系的要求；

2）本标准的要求。

b) 是否得到有效实现和维护。

组织应：

c) 规划，建立，实现和维护审核方案（一个或多个），包括审核频次，方法，责任，规划要求和报告。审核方案应考虑相关过程的重要性和以 往审核的结果。

d) 定义每次审核的审核准则和范围。

e) 选择审核员并实施审核，确保审核过程的客观性和公正性。

f) 确保将审核结果报告至相关管理层。

g) 保留文件化信息作为审核方案和审核结果的证据。

9.2内部監査

組織は、ISMSが次の状況にあるかどうかに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施しなければならない。

a)次の事項に適合している。

1)ISMSに関して、組織自体が規定した要求事項

2)この規格の要求事項

b)有効に実施され、維持されている。

組織は、次に示す事項を行わなければならない。

c)頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持。監査プログラムは、関連する プロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。

d)各監査について、監査基準及び監査範囲を明確にする。

e)監査プロセスの客観性及び公平性を確保する監査員を選定し、監査を実施する。

f)監査の結果を関連する管理層に報告することを確実にする。

g)監査プログラム及び監査結果の証拠として、文書化した情報を保持する。

9.3 管理评审

最高管理层应按计划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性，充分性和有效性。

管理评审应考虑：

a) 以往管理评审提出的措施的状态；

b) 与信息安全管理体系相关的外部和内部事项的变化；

c) 有关信息安全绩效的反馈，包括以下方面的趋势：

1. 不符合和纠正措施；

   2）监视和测量结果；

   3）审核结果；

   4）信息安全目标完成情况。

d) 相关方反馈；

e) 风险评估结果及风险处置计划的状态；

f) 持续改进的机会。

管理评审的输出应包括与持续改进机会相关的决定以及变更信息安全管理体系的任何要求。组织应保留文件化信息作为管理评审结果的证据。

9.3　マネジメントレビュー

トップマネジメントは、組織の**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**あらかじめ**定めた**間隔**で、ISMS**をレビューしなければならない**。

マネジメントレビューは、次の事項**を考慮しなければならない**。

a)前回**までのマネジメントレビューの**結果**とった**処置の**状況

b)ISMS**に関連する**外部及び内部**の課題の**変化

c)次**に示す**傾向**を含めた、**情報**セキュリティパフォーマンスに**関する**フィードバック**

1)不適合及**び**是正処置

2)監視及**び**測定**の**結果

3)監査結果

4)情報**セキュリティ**目的**の**達成

d)利害関係者**からのフィードバック**

e)**リスクアセスメントの**結果及**びリスク**対応計画**の**状況

f)継続的改善**の**機会

マネジメントレビューからのアウトプットには、継続的改善**の**機会、及**び**ISMS**のあらゆる**変更**の**必要性**に**関する**決定**を含めなければならない**。

組織**は、マネジメントレビューの**結果**の**証拠**として、**文書化**した**情報**を**保持**しなければならない**。

10.改进

10.1不符合及纠正措施

当发生不符合时，组织应：

a) 对不符合做出反应，适用时：

1）采取措施，以控制并予以纠正；

2）处理后果；

b) 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：

1） 评审不符合；

2） 确定不符合的原因；

3） 确定类似的不符合是否存在，或可能发生；

c) 实现任何需要的措施；

d) 评审任何所采取的纠正措施的有效性；

e□必要时，对信息安全管理体系进行变更。

纠正措施应与所遇到的不符合的影响相适合。

组织应保留文件化信息作为以下方面的证据；

f) 不符合的性质及所采取的任何后续措施；

g) 任何纠正措施的结果。

10.1 不適合及び是正処置

不適合が発生した場合、組織は、次の事項を行わなければならない。

a)その不適合に対処し、該当する場合には、必ず、次の事項を行う。

1)その不適合を管理し、修正するための処置をとる。

2)その不適合によって起こった結果に対処する。

b)その不適合が再発又は他のところで発生しないようにするため、次の事項によって、その不適合の原因を除去するための処置をとる必要性 を評価する。

1)その不適合をレビューする。

2)その不適合の原因を明確にする。

3)類似の不適合の有無、又はそれが発生する可能性を明確にする。

c)必要な処置を実施する。

d)とった全ての是正処置の有効性をレビューする。

e)必要な場合には□ISMSの変更を行う。

是正処置は、検出された不適合のもつ影響に応じたものでなければならない。

組織は、次の示す事項の証拠として、文書化した情報を保持しなければならない。

f) 不適合の性質及びとった処置

g)是正処置の結果

10.2 持续改进

组织应持续改进信息安全管理体系的适宜性，充分性和有效性。

10.2　継続的改善

組織は、ISMSの適切性、妥当性及び有効性を継続的に改善しなければならない。

From:
http://trident365.com/ - 三叉戟

Permanent link:
http://trident365.com/doku.php?id=resources:framework:iso27001_2013

Last update: **2025/01/18 19:26**