

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由	
項番	条文		項番	条文		
第0	序文		-			
第0 1.	<p>一般</p> <p>本基準は、経営陣及び要員が、効果的な情報セキュリティマネジメントシステム（以下、ISMSという。）を構築し、運営管理していくためのモデルを提供することを目的として作成されたものである。ISMSを採用するかどうかは、組織における戦略上の決定とすべきである。組織におけるISMSの設計及び導入は、事業上のニーズ及び目標、その結果生じる情報セキュリティ要求事項、用いられるプロセス、並びに組織の規模及び構造によって影響を受ける。これらの事項及びこれらを支えるシステムは、時とともに変化すると考えられる。</p> <p>本基準は、あらゆる顧客からの要求又は規制上の要求と同様に、組織固有の要求事項を満たす組織の能力を、内部の者及び認証機関を含む外部の者が評価するためにも使用することができる。</p>				内容の追加	
第0 2.	<p>プロセスアプローチ</p> <p>本基準では、組織においてISMSを確立、導入、運用、監視、維持し、かつそのISMSの有効性を改善する際に、プロセスアプローチを採用することを奨励している。</p> <p>組織は、有効に機能するために、多くの活動を明確にし、運営管理しなければならない。インプットをアウトプットに変換することを可能にするために経営資源を使用して運営管理されるあらゆる活動は、プロセスとみなすことができる。多くの場合、一つのプロセスからのアウトプットは、後に続くプロセスへの直接のインプットとなる。</p> <p>組織内においてプロセスを明確にし、その相互関係を把握し、運営管理することとあわせて、一連のプロセスをシステムとして適用することを「プロセスアプローチ」と呼ぶ。</p> <p>プロセスアプローチによって、その利用者は次の事項の重要性を強調するようになる。</p>				内容の追加	
	第0 2.	事業上の情報セキュリティ要求事項、並びに情報セキュリティポリシー及び目標を確立する必要性を理解すること。				内容の追加
	第0 2.	組織における全般的な事業上のリスク管理を考慮に入れて、管理策を導入し、運用すること。				内容の追加
	第0 2.	ISMSの実施状況及び有効性を監視し、見直すこと。				内容の追加
	第0 2.	客観的な測定結果に基づいて継続的に改善すること。				内容の追加

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
	<p>本基準で採用されているモデルは、「Plan-Do-Check-Act」(PDCA)モデルとして知られており、あらゆるISMSプロセスに適用できるものである。図1は、ISMSが情報セキュリティ要求事項及び利害関係者の期待をインプットとし、必要な活動及びプロセスを経て、これらの要求事項及び期待を満たす情報セキュリティの成果(すなわち運営管理された情報セキュリティ)を生み出すことを表したものである。図1は、また、第4、第5、第6、第7に記述するプロセスのつながりも表している。</p> <p>情報セキュリティ要求事項の例示 情報セキュリティ違反によって組織が深刻な財務上の損害を受けないようにすること。 情報セキュリティ違反によって組織の存続が脅かされないようにすること。 利害関係者の期待の例示 電子商取引に使用しているウェブサイトに対し不正侵入のような重大な事件・事故が起こった場合、その影響を最小限に抑えるための適切な手順に対する十分な訓練を受けた要員がいること。 参考 情報セキュリティでは、「手順」という語は、慣習的に、コンピュータや他の電子的手段ではなく、人によって実施される「プロセス」という意味で使用される。</p> <p>図1-ISMSプロセスに適用されるPDCAモデル</p>			内容の追加	

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由							
項番	条文		項番	条文								
	<table border="1"> <tr> <td>Plan - 計画 (ISMSの確立)</td> <td>組織の全般的なポリシー及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティポリシー、目標、対象、プロセス及び手順を確立する。</td> </tr> <tr> <td>Do - 実施 (ISMSの導入及び運用)</td> <td>その情報セキュリティポリシー、管理策、プロセス及び手順を実施し運用する。</td> </tr> <tr> <td>Check - 点検 (ISMSの監視及び見直し)</td> <td>情報セキュリティポリシー、目標及び実際の経路に照らしてプロセスの継続状態を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。</td> </tr> <tr> <td>Act - 処置 (ISMSの維持及び改善)</td> <td>ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。</td> </tr> </table>	Plan - 計画 (ISMSの確立)	組織の全般的なポリシー及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティポリシー、目標、対象、プロセス及び手順を確立する。	Do - 実施 (ISMSの導入及び運用)	その情報セキュリティポリシー、管理策、プロセス及び手順を実施し運用する。	Check - 点検 (ISMSの監視及び見直し)	情報セキュリティポリシー、目標及び実際の経路に照らしてプロセスの継続状態を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。	Act - 処置 (ISMSの維持及び改善)	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。			
Plan - 計画 (ISMSの確立)	組織の全般的なポリシー及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティポリシー、目標、対象、プロセス及び手順を確立する。											
Do - 実施 (ISMSの導入及び運用)	その情報セキュリティポリシー、管理策、プロセス及び手順を実施し運用する。											
Check - 点検 (ISMSの監視及び見直し)	情報セキュリティポリシー、目標及び実際の経路に照らしてプロセスの継続状態を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。											
Act - 処置 (ISMSの維持及び改善)	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。											
第03.	他のマネジメントシステムとの両立性 本基準は、関連するマネジメント規格と矛盾なく統合して実施・運用することができるように、JIS Q 9001 : 2000及びJIS Q 14001 : 1996との整合がとられている。 本基準は、組織自らのISMSを、関連する他のマネジメントシステムの要求事項に整合したり、統合したりすることができるように設計されている。				内容の追加							
第1	適用範囲		第1	適用範囲								
第1.1.	一般 本基準は、組織の事業上のリスク全般に対して、文書化されたISMSの確立、導入、運用、監視、見直し、維持及び改善に関する要求事項を規定するものである。また本基準は、個々の組織又は組織の一部が、その必要性に応じて情報セキュリティ管理策を適切に実施できるように要求事項を規定している。 ISMSは、情報資産を保護するため、十分にバランスのとれた適切な情報セキュリティ管理策を確保し、顧客及び他の利害関係者に対して信頼を与えるように設計されるものである。このように設計されたISMSは、競争力、キャッシュフロー、収益性、法令等の遵守及び企業イメージを維持し、改善することにつながる。			本基準は、情報セキュリティマネジメントシステム（以下、「ISMS」という）の確立、実施及び文書化についての要求事項を明記する。 <参考> 本基準（ISMS認証基準）の第4に規定する詳細管理策は、JIS X 5080（ISO/IEC 17799）を参照しており、これと整合するものとなっている。JIS X 5080（ISO/IEC 17799）は、本基準の要求事項の実施を支援する最良な実践（Best Practice）を推奨するものである。	内容の整理							

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第1 2.	適用 本基準の要求事項は汎用性があり、業種及び事業形態、規模及び事業の性質を問わず、あらゆる組織に適用できることを意図している。組織やその事業の性質によって、本基準の要求事項のいずれかが適用できない場合には、その要求事項の除外を考慮することができる。このような除外を行う場合、その除外が、リスクアセスメント及び該当する規制上の要求事項によって決定されるセキュリティ要求事項を満たす情報セキュリティを提供する組織の能力、責任などに影響を及ぼさないと判断されない限り、本基準への適合の宣言は受け入れられない。リスク受容の基準を満たすために必要と考えられる管理策を適用除外とする場合には、その理由及び関連するリスクが責任者によって正式に受容されたことを示す証拠が必要である。本基準の第4、第5、第6及び第7に定める要求事項を除外することは、いかなる場合であっても認められない。				内容の追加
第2	引用規格等		-		
	次に掲げる規格等は、本基準の適用にあたり不可欠なものである。発行年の付いている規格等については、記載の年の版だけが本基準に適用される。発行年のない規格等については、その引用規格等の最新版が適用となる。 JIS X 5080:2002 情報技術 情報セキュリティマネジメントの実践のための規範 ISO Guide 73:2002 リスクマネジメント - 用語集 - 規格において使用するための指針(TR Q 0008として平成15年2月発行予定。)				第1 適用範囲の参考に新たな規格を追加
第3	定義		第2	用語及び定義	
	本基準の目的のために、次に掲げる定義を適用する。				内容の追加
第3 1.	可用性 (availability) 許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。 [JIS X 5080:2002を参考]				用語の整理
第3 2.	機密性 (confidentiality) アクセスを許可された者だけが情報にアクセスできることを確実にすること。 [JIS X 5080:2002を参考]				用語の整理

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第3 3.	情報セキュリティ (information security) 情報の機密性、完全性及び可用性のセキュリティの維持。 [JIS X 5080:2002を参考]		第2(1)	情報セキュリティ 情報の機密性、完全性及び可用性を確保し維持すること。 機密性： アクセスを認可された者だけが、情報にアクセスできることを確実にすること。 完全性： 情報及び処理方法が正確であること及び完全であることを保護すること。 可用性： 認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。	用語の整理
第3 4.	情報セキュリティマネジメントシステム ISMS (information security management system) マネジメントシステム全体のなかで、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善をになう部分。 参考 マネジメントシステムには、組織の構造、ポリシー、計画作成活動、責任、実践、手順、プロセス及び経営資源が含まれる。				内容の追加
第3 5.	完全性 (integrity) 情報及び処理方法の正確性及び完全性を保持すること。 [JIS X 5080:2002を参考]				用語の整理
第3 6.	リスク受容 (risk acceptance) リスクを受容する意思決定。 [ISO Guide 73を参照]				用語の追加
第3 7.	リスク分析 (risk analysis) リスク因子を特定し、リスクを算定するために、情報を体系的に利用すること。 [ISO Guide 73を参考] 参考 リスク因子(risk source)： 結果をもたらす可能性が潜在する物事や行動。 [ISO Guide 73を参照]				用語の追加
第3 8.	リスクアセスメント (risk assessment) リスク分析からリスク評価までの全てのプロセス。 [ISO Guide 73を参照]		第2(2)	リスク評価 情報や情報処理施設等に対する脅威及びその脅威への脆弱性を分析し、その結果からリスクが顕在化する可能性及び顕在化した場合の事業への影響度を検証すること。	用語の整理
第3 9.	リスク評価 (risk evaluation) リスクの重大さを決定するために、算定されたリスクを与えられたリスク評価基準と比較するプロセス。 [ISO Guide 73を参照]				用語の追加

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第3 10.	リスクマネジメント (risk management) リスクに関して組織を指揮し管理する調整された活動。 [ISO Guide 73を参照]				用語の追加
第3 11.	リスク対応 (risk treatment) リスクを変更させるための方策を選択及び実施する対応プロセス。 [ISO Guide 73を参照]				用語の追加
第3 12.	適用宣言書 (statement of applicability) 組織のリスクアセスメント及びリスク対応プロセスの結果及び結論に基づいて、本基準の附属書「詳細管理策」の管理目的及び管理策の選択可否と選択しない場合の理由並びに必要な応じ追加した管理目的及び管理策とその理由について記述した文書。		第2(3)	適用宣言書 組織の必要性に基づき、本基準の第4詳細管理策の選択可否と選択しない場合の理由、並びに必要な応じ追加した管理策とその理由について記述した文書。	用語の整理
第4	情報セキュリティマネジメントシステム		第3	ISMSの要求事項	
第4 1.	一般要求事項 組織は、自らの事業の活動全般及びリスク全般を考慮して、文書化された ISMSを構築、導入、維持し、かつこれを継続的に改善すること。本基準で使われるプロセスは、図 1 に示すPDCAモデルに基づいている。		第3(1)	一般	内容の整理
			第3(1)	組織は以下の項目を明確にしたISMSを確立し維持すること。	
			第3(1) (ア)	保護すべき情報資産	
			第3(1) (ウ)	管理目的及び管理策の内容	
			第3(1) (エ)	保護すべき情報資産に要求される保証の度合い	
第4 2.	ISMSの確立及び運営管理		第3(2)	マネジメント枠組みの確立	表記の変更
第4 2.(1)	ISMSの確立				表記の変更
	組織は次の事項を実施すること。		第3(2)	組織の必要性に基づき、管理目的及び管理策の内容を明確にすること。	内容の整理
			第3(2)	の目的及び内容を文書化するために以下の作業を実施すること。	
第4 2.(1)	事業の特徴、組織、その所在地、資産及び技術の観点から、ISMSの適用範囲を定義する。		第3(2) (イ)	ISMSの適用範囲の決定	内容の整理
第4 2.(1)	事業の特徴、組織、その所在地、資産及び技術の観点から、次の事項を満たすISMSの基本方針を策定する。		第3(2) (ア)	情報セキュリティポリシーの策定	内容の整理及び追加
第4 2.(1) (ア)	ISMSの目標を設定するための枠組みを含み、情報セキュリティに関する全般的な方向性及び行動指針を確立する。				

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 2.(1) (イ)	事業上の要求事項及び法的又は規制要求事項、並びに契約上のセキュリティ義務を考慮する。				
第4 2.(1) (ウ)	ISMSを確立し、維持するために必要な戦略上の視点からみた組織環境、並びにリスクマネジメントのための環境を整備する。				
第4 2.(1) (エ)	リスクを評価するための基準を確立し、定義されたリスクアセスメントの構造を確立する(第4 2.(1) 参照)。				
第4 2.(1) (オ)	経営陣による承認を得る。				
第4 2.(1)	リスクアセスメントについての体系的な取組方法を策定する。 当該ISMSに適しており、また、明確にされた事業上の情報セキュリティ要求事項、並びに識別された法的及び規制要求事項に適したリスクアセスメントの方法を特定する。リスクを受容可能な水準にまで軽減するために、ISMSの基本方針及び目標を設定する。また、リスクを受容するための基準を定め、受容可能なリスクの水準を特定する(第5 1. 参照)。		第3(1) (イ)	リスクマネジメントに対する組織の取組方法	内容の整理
第4 2.(1)	リスクを識別する。		第3(2) (ウ)	リスク評価	内容の整理及び追加
第4 2.(1) (ア)	当該ISMSの範囲内の情報資産及び情報資産の責任者を特定する。				
第4 2.(1) (イ)	それらの情報資産に対する脅威を明確にする。				
第4 2.(1) (ウ)	脅威によって利用されるおそれのある脆弱性を明確にする。				
第4 2.(1) (エ)	機密性、完全性及び可用性の喪失が情報資産に及ぼすかもしれない影響を明確にする。				
第4 2.(1)	リスクアセスメントを実施する。				
第4 2.(1) (ア)	セキュリティ障害に起因して想定される事業上の損害を評価する。その際に、当該情報資産の機密性、完全性及び可用性の喪失による潜在的な影響を考慮する。				
第4 2.(1) (イ)	一般に認識されている脅威及び脆弱性の観点から起こりうるセキュリティ障害などの現実的な発生可能性、情報資産に関連する影響、並びに現在実施されている管理策を考慮してアセスメントを実施する。				
第4 2.(1) (ウ)	リスクの度合いを算定する。				

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 2.(1) (I)	第4 2.(1) で確立した評価基準を使用して、当該リスクについて、受容できるか、対応が必要かを定める。				
第4 2.(1)	リスク対応についての選択肢を明確にし、評価する。考えられるリスク対応に関する選択肢として、次のような事項が含まれる。		第3(2) (エ)	リスクマネジメントの対象範囲の決定	内容の整理及び追加
第4 2.(1) (ア)	適切な管理策を採用する。				
第4 2.(1) (イ)	リスクを保有する。リスクが組織の基本方針及びリスク受容のための評価基準を明らかに満たす場合には、意識的かつ客観的に当該リスクを受容する(第4 2.(1) 参照)。 参考 リスクの保有(risk retention) : あるリスクからの損失の負担又は利得の恩恵の受容 [ISO Guide 73を参照]				
第4 2.(1) (ウ)	リスクを回避する。				
第4 2.(1) (I)	リスクを移転する。関連する事業上のリスクを、例えば、保険会社又は供給者という他者に移転する。				
第4 2.(1)	リスク対応に関する管理目的及び管理策を選択する。本基準の附属書「詳細管理策」から、適切な管理目的及び管理策を選択する。また、この選択については、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を示すこと。 参考 附属書「詳細管理策」の管理目的及び管理策は網羅的なものではなく、追加の管理目的及び管理策を選択することができる。		第3(2) (オ)	本基準の第4 詳細管理策及び必要に応じ追加した管理策の選択	内容の整理
第4 2.(1)	適用宣言書を作成する。 第4 2.(1) で選択した管理目的及び管理策、並びにこれらを選択した理由を文書化し、適用宣言書に含めなければならない。また、附属書「詳細管理策」に記載する管理目的及び管理策を選択しない場合についても、その理由を記述しなければならない。		第3(2) (カ)	適用宣言書の作成	内容の整理
第4 2.(1)	残留リスクに対する経営陣の承認及び当該ISMSを導入し、運用するための許可を得る。				内容の追加
第4 2.(2)	ISMSの導入及び運用		第3(3)	管理策の実施	表記の変更
	組織は次の事項を実施すること。		第3(3)	第3 (2) (イ)で選択した管理策を実施すること。	内容の整理及び追加
第4 2.(2)	情報セキュリティについてのリスクを管理するための、適切な管理活動、責任及び優先順位が明確にされたリスク対応計画を策定する(第5参照)。				

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 2.(2)	識別された管理目的を達成するためにリスク対応計画を実施する。これには、必要な資金の拠出を考慮し、役割及び責任を割り当てることを含む。				
第4 2.(2)	当該管理目的を達成するために第4 2.(1) で選択した管理策を実施する。				
第4 2.(2)	教育・訓練及び周知のためのプログラムを実施する（第5 2.(2)参照）。				
第4 2.(2)	運用を管理する。				
第4 2.(2)	経営資源を管理する（第5 2.参照）。				
第4 2.(2)	セキュリティ事件・事故を迅速に検出し、それらに対して迅速な対応を行うことのできる手順及びその他の管理策を実施する。				
第4 2.(3)	ISMSの監視及び見直し組織は次の事項を実施すること。		第3(3)	管理策を実施するために採用した手順について、第4 10(2)に従いその有効性を確認すること。	内容の整理及び追加
第4 2.(3)	次の事項を行うため、監視のための手順及び他の管理策を実施する。				
第4 2.(3) (ア)	処理結果から誤りを速やかに検出する。				
第4 2.(3) (イ)	セキュリティ上の違反行為及び事件・事故は未遂であっても、迅速に識別する。				
第4 2.(3) (ウ)	人又は情報技術によって実施されるセキュリティ活動が意図した通りに実施されているかどうかを、経営陣や管理者が判断できるようにする。				
第4 2.(3) (エ)	セキュリティ違反の再発防止のためにとるべき処置を、事業上の優先順位を踏まえて判断する。				
第4 2.(3)	当該ISMSの有効性に関して定期的な見直しを実施する（情報セキュリティポリシー及び目標を満たすこと、並びにセキュリティ管理策の見直しを含む）。その際、セキュリティ監査の結果、事件・事故、提案及び全ての利害関係者からのフィードバックを考慮に入れる。				
第4 2.(3)	残留リスク及び受容可能なリスク水準の見直しを行う。その際、次の事項に生じる変化を考慮に入れる。				
第4 2.(3) (ア)	組織				
第4 2.(3) (イ)	技術				

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 2.(3) (ウ)	事業の目標及びプロセス				
第4 2.(3) (イ)	識別された脅威				
第4 2.(3) (オ)	外部の事象。例えば、法的又は規制環境や社会環境の変化など				
第4 2.(3)	あらかじめ定められた間隔でISMSの内部監査を実施する。				
第4 2.(3)	適用範囲が引き続き適切であり、ISMSのプロセスにおける改善策が明確にされていることを確実にするために、定期的に（少なくとも年1回）ISMSのマネジメントレビューを実施する（第6参照）。				
第4 2.(3)	ISMSの有効性又は実施状況に影響を与える可能性のある活動及び事象を記録する（第4 3.(3)参照）。				
第4 2.(4)	ISMSの維持及び改善組織は定期的に次の事項を実施すること。		第3(2)	マネジメント枠組みを維持・改善するため、の各項目について、定期的及び必要に応じて見直すこと。	内容の整理及び追加
第4 2.(4)	識別されたISMSの改善策を実施する。				
第4 2.(4)	第7 2.及び第7 3.に従って適切な是正処置及び予防処置を実施する。自らの組織及び他の組織の情報セキュリティに関する経験から学んだ教訓を活用する。				
第4 2.(4)	利害関係者全てに結果及び講じた処置を伝達し、合意を得る。				
第4 2.(4)	改善が、その意図した目標を確実に達成するようにする。				
第4 3.	文書化に関する要求事項		第3(4)	文書化	表記の変更
第4 3.(1)	一般ISMS文書には、次の事項を含めること。		第3(4)	以下の内容を包含するものを文書化し、ISMS文書として維持すること。	表記の変更
第4 3.(1)	情報セキュリティポリシー（第4 2.(1) 参照）及び管理目的の表明。		第3(4) (イ)	第3 (2)で確立したマネジメント枠組みの要約	内容の整理
第4 3.(1)	当該ISMSの適用範囲（第4 2.(1) 参照）並びにISMSを支える手順及び管理策。		第3(4) (ウ)	第3 (3)の管理策を実施するために採用した手順及びその実施責任と関連する作業内容	内容の整理
第4 3.(1)	リスクアセスメントの結果報告（第4 2.(1) から第4 2.(1) 参照）。				内容の追加
第4 3.(1)	リスク対応計画（第4 2.(2) 参照）。				内容の追加
第4 3.(1)	情報セキュリティに関するプロセスの効果的な計画、運用及び管理を確実に実施するために、組織が必要と判断した、文書化された手順（第6 1.参照）。		第3(4) (エ)	ISMSを運用するための手順とそれらの実施責任及び関連する作業内容	内容の整理

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 3.(1)	本基準が要求する記録 (第4 3.(3)参照)。		第3(4) (ア)	第3 (2)の作業の証拠	表記の変更
第4 3.(1)	適用宣言書。 文書は全て、ISMSポリシーの要求に応じて利用できるようにしておくこと。				内容の追加
	参考1 本基準で「文書化された手順」という用語を使う場合には、その手順が確立され、文書化され、実施され、かつ、維持されていることを意味する。 参考2 ISMSの文書化の程度は、次の理由から組織によって異なることがある。 - 組織の規模及び活動の種類 - 適用範囲、セキュリティ要求事項及び運営管理するシステムの複雑さ 参考3 文書及び記録の様式及び媒体の種類はどのようなものでもよい。				内容の追加
第4 3.(2)	文書管理		第3(5)	文書管理	
	ISMSで必要とされる文書は、保護し管理すること。次の事項を行うのに必要な管理活動を規定する文書化された手順を確立すること。		第3(5)	第3 (4)のISMS文書を管理するため、以下の条件を満たす手順を定め、維持すること。	表記の変更
第4 3.(2)	発行前に、適切かどうかの観点から文書を承認する。				内容の追加
第4 3.(2)	文書の見直しを行う。また、必要に応じて更新し、再承認する。		第3(5) (イ)	ISMS文書の定期的な見直しを行い、情報セキュリティポリシーに対する準拠性を維持しながら必要に応じて改訂する	表記の変更
第4 3.(2)	文書の変更の識別及び現在の改訂版の識別を確実にする。		第3(5) (ウ)	ISMS文書の更新履歴を管理する	内容の整理
第4 3.(2)	該当する文書の最新版が、必要となしに、必要なところで使用可能な状態にあることを確実にする。		第3(5) (エ)	ISMSの運用に関わる全ての事業所等において、必要なISMS文書が閲覧可能である	内容の整理
第4 3.(2)	文書が読みやすく、容易に識別可能な状態であることを確実にする。		第3(5) (ア)	ISMS文書の利用者が文書を容易に利用することができる	表記の変更
第4 3.(2)	どれが外部で作成された文書かが識別されていることを確実にする。				内容の追加
第4 3.(2)	文書の配付が適切に管理されていることを確実にする。				内容の追加
第4 3.(2)	廃止文書が誤って使用されないようにする。		第3(5) (オ)	ISMS文書の一部について、その必要性がなくなったり、別途新たな文書が作成された場合に、当該ISMS文書が速やかに廃止される	内容の整理
第4 3.(2)	廃止文書を何らかの目的で保持する場合には、適切な識別をする。		第3(5) (カ)	(オ)の廃止にかかわらず、法規制等による要請がある場合や専門知識を蓄積するために、必要に応じてISMS文書が保管される	内容の整理

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第4 3.(3)	記録の管理		第3(6)	記録	表記の変更
	記録は、要求事項への適合及びISMSの効果的運用の証拠を示すために、作成され、維持されること。また、これらの記録は管理されること。その際、当該ISMSは該当する法的要求事項を考慮に入れること。記録は、読みやすく、容易に識別可能で、検索可能な状態であること。記録の識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理を文書化すること。運営管理プロセスで、記録の必要性及び記録の範囲を定めること。第4 2.に記述されているプロセスの実施状況に関する記録及びISMSに関連する全てのセキュリティ事件・事故の発生に関する記録を維持すること。 記録の例 訪問者台帳、監査記録及びアクセスの承認記録など。		第3(6)	第3 (1)から(5)の内容に対する準拠状況を保証するために必要な記録を特定すること。	内容の整理
			第3(6)	で特定した記録を管理する手順を定め、必要に応じて見直すこと。	
			第3(6)	で特定した記録に対し、損傷、劣化、紛失、消失を防止するための措置を講ずること。	
第5	経営陣の責任		-		
第5 1.	経営陣のコミットメント 経営陣は、ISMSの確立、導入、運用、監視、見直し、維持及び改善に対するコミットメントの証拠を、次の事項によって示すこと。				内容の追加
第5 1.	情報セキュリティポリシーを確立する。				
第5 1.	情報セキュリティ目標が設定され、計画が立案されることを確実にする。				
第5 1.	情報セキュリティに対する役割及び責任を定める。				
第5 1.	情報セキュリティ目標を達成すること及び情報セキュリティポリシーに適合することの重要性、当該組織の法的責任、並びに継続的改善の必要性を組織内に周知する。				
第5 1.	ISMSの構築、導入、運用及び維持に十分な経営資源を提供する（第5 2.(1)参照）。				
第5 1.	リスクの受容可能な水準を決める。				
第5 1.	ISMSのマネジメントレビューを実施する（第6参照）。				
第5 2.	経営資源の運用管理				
第5 2.(1)	経営資源の提供 組織は、次の事項を実施するために必要な経営資源を決定し、提供すること。				

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第5 2.(1)	ISMSを確立、導入、運用及び維持する。				
第5 2.(1)	情報セキュリティの手順が事業上の要求事項を満たすものであることを確実にする。				
第5 2.(1)	法的及び規制要求事項と契約上のセキュリティに関する義務を識別し、取扱う。				
第5 2.(1)	実施される全ての管理策を的確に適用することにより、十分なセキュリティを維持する。				
第5 2.(1)	必要な場合には見直しを行い、その結果に対して適切に対応する。				
第5 2.(1)	必要な場合には、ISMSの有効性を改善する。				
第5 2.(2)	教育・訓練、認識及び力量 ISMSにおいて、明確にされた責任を割り当てられた要員全てが要求される業務を実施する力量をもつことを、次の事項を実施することによって組織は確実にすること。				
第5 2.(2)	ISMSに影響がある業務に従事する要員に必要な力量を明確にする。				
第5 2.(2)	必要な力量がもてるように適切な教育・訓練を実施し、必要な場合には、適格な要員を雇用する。				
第5 2.(2)	実施した教育・訓練及びその他の講じた処置の有効性を評価する。				
第5 2.(2)	教育・訓練、技能、経験及び資格についての記録を維持する(第4 3.(3)参照)。				
	組織はまた、該当する要員全てが、自らの情報セキュリティについての活動のもつ意味とその重要性を認識し、ISMSの目標の達成に向けて自らが、どのように貢献できるかを認識することを確実にしなければならない。				
第6	マネジメントレビュー		-		

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第6 1.	一般 経営陣は、組織のISMSが、引き続き適切で、妥当で、かつ、有効であることを確実にするために、あらかじめ定められた間隔でISMSをレビューすること。このレビューでは、ISMSに対する改善の機会の評価、情報セキュリティポリシー及び情報セキュリティ目標を含むISMSの変更の必要性の評価も行うこと。また、このレビューの結果を明確に文書化しなければならず、その記録を維持すること(第4 3.(3)参照)。				内容の追加
第6 2.	マネジメントレビューへのインプット マネジメントレビューへのインプットには次の情報を含めること。				
第6 2.	監査及びレビューの結果				
第6 2.	利害関係者からのフィードバック				
第6 2.	ISMSの実施状況及び有効性を改善するために組織において利用可能な技術、製品又は手順				
第6 2.	予防処置及び是正処置の状況				
第6 2.	過去のリスクアセスメントで適切に取り扱われなかった脆弱性又は脅威				
第6 2.	過去のマネジメントレビューの結果に対するフォローアップ				
第6 2.	ISMSに影響を及ぼす可能性のある全ての変更				
第6 2.	改善のための提案				
第6 3.	マネジメントレビューからのアウトプット マネジメントレビューからのアウトプットには、次の事項に関する決定及び処置を含めること。				
第6 3.	ISMSの有効性の改善				
第6 3.	ISMSに影響を与える可能性のある内部又は外部の事象に対応するために必要に応じて加えられる、情報セキュリティを実現する手順の修正。それら事象には、次の事項に対する変更が含まれる				
第6 3. (ア)	事業上の要求事項				
第6 3. (イ)	情報セキュリティ要求事項				
第6 3. (ウ)	既存の事業上の要求事項を満たす業務プロセス				

ISMS認証基準Ver.2.0(案)			改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文			項番	条文	
	第6 3. (I)	規制環境又は法的環境				
	第6 3. (オ)	リスクの度合い及びリスク受容の水準				
	第6 3.	必要となる経営資源				
第6 4.		内部監査 組織は、当該ISMSの管理目的、管理策、プロセス及び手順が次の事項を満たしているか否かを明確にするために、あらかじめ定められた間隔でISMSの内部監査を実施すること。				
	第6 4.	本基準の要求事項に適合していること。また、関連する法令又は規制に適合していること。				
	第6 4.	識別した情報セキュリティ要求事項に適合していること。				
	第6 4.	有効に実施され維持されていること。				
	第6 4.	期待通りに実施されていること。				
		組織は、監査の対象となるプロセス及び領域の状況と重要性、並びにこれまでの監査結果を考慮して、監査プログラムを策定すること。監査の評価基準、対象範囲、頻度及び方法を規定すること。監査員の選定及び監査の実施においては、監査プロセスの客観性及び公平性を確保すること。監査員は自らの仕事は監査しないこと。監査の計画及び実施、結果の報告、記録の維持（第4 3.(3)参照）に関する責任、並びに要求事項を文書化された手順の中で規定すること。 監査された領域に責任をもつ管理者は、発見された不適合及びその原因を除去するために遅滞なく処置が確実に講じられるようにすること。改善活動には、講じた処置の検証及び検証結果の報告を含めること（第7参照）。				
第7	改善			-		
第7 1.	継続的改善 組織は、情報セキュリティポリシー、情報セキュリティ目標、監査結果、監視した事象の分析、是正処置、予防処置及びマネジメントレビューを通じて、ISMSの有効性を継続的に改善すること。					内容の追加
第7 2.	是正処置 組織は、再発防止のため、ISMSの導入及び運用に関連する不適合の原因を除去するための処置を講ずること。是正処置に関する文書化された手順では、次の事項に関する要求事項を規定すること。					

ISMS認証基準Ver.2.0(案)		改訂箇所	ISMS認証基準Ver.1.0		改訂理由
項番	条文		項番	条文	
第7 2.	ISMSの導入及び運用についての不適合の識別				
第7 2.	不適合の原因の特定				
第7 2.	不適合の再発防止を確実にするための処置の必要性の評価				
第7 2.	必要な是正処置の決定及び実施				
第7 2.	実施した処置の結果の記録 (第4 3.(3)参照)				
第7 2.	実施した是正処置のレビュー				
第7 3.	<p>予防処置 組織は、不適合の発生を未然に防ぐための処置を決めること。予防処置は、起こり得る問題の影響に見合ったものであること。予防処置に関する文書化された手順では、次の事項に関する要求事項を規定すること。</p>				
第7 3.	起こり得る不適合及び原因の識別				
第7 3.	必要な予防処置の決定及び実施				
第7 3.	実施した処置の結果の記録 (第4 3.(3)参照)				
第7 3.	実施した予防処置のレビュー				
第7 3.	変化したリスクの識別及び大きく変化したリスクに対して確実に注意が払われるようにすること				
	<p>予防処置の優先順位については、リスクアセスメントの結果に基づいて決定すること。 参考 不適合を予防するための処置は、多くの場合、是正処置よりも費用対効果が高い。</p>				