ISMS適合性評価制度説明会

ISO/IEC 27001とISMS認証基準との比較分析の概要

(財)日本情報処理開発協会
情報セキュリティ部　ISMS制度推進室
ISMS適合性評価制度　技術専門部会
2005年12月

アジェンダ

- はじめに
- ISO/IEC 27001:2005とISMS認証基準の比較
  - 本文
  - 附属書　附属書A　管理目的及び管理策」
- まとめ
- 参考資料　変更の概要）

はじめに

- 説明内容
  - ISO/IEC 27001:2005の制定に伴いISMS認証基準(Ver.2.0)からの主要な変更点について、幾つか取り上げ説明します。
  - 説明会資料の最後に掲載している「ISO/IEC 27001:2005とISMS認証基準(Ver.2.0)比較表」は当該説明の参考資料となります。
    - 補足1:比較表は本文の4章以降および附属書Aについて記載しています。
      - 附属書B（OECD原則とこの規格）、附属書C（ISO9001:2000, ISO14001:2004及びこの規格の対応）については記載しておりません。
    - 補足2:比較表の備考欄に「削除」及び「移動」と記載されている場合は、斜め線で記載されております。
  - ISO/IEC 27001:2005（日本規格協会より発行）につきましては、JIPDEC ISMS制度推進室のホームページより購入できます。
    - URL：http://www.isms.jipdec.jp

本文
適用宣言書

ISO/IEC 27001		ISMS認証基準Ver.2.0		
項番	条文	項番	条文	備考
3.16	適用宣言書（statement of applicability） その組織のISMSに関連して，適用する管理目的及び管理策を記述した文書。 参考　管理目的及び管理策は，組織の情報セキュリティに対する次のものに基づくものである。 ・リスクアセスメント及びリスク対応のプロセスの結果及び結論 ・法的又は規制要求事項 ・契約上の義務 ・事業上の要求事項	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き，組織のISMSに適切で当てはまる管理目的及び管理策を記述した文書。	・変更（大幅変更） 前半部分を変更して新たにNOTEとして追加）

4.2.1j)	適用宣言書を作成する。 適用宣言書には，次の事項を含めること。	第4 2.(1)⑧	適用宣言書を作成する。 第4 2.(1)⑦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，適用宣言書に含めること。また，附属書「詳細管理策」に記載する管理目的及び管理策の中から適用除外としたものは記録すること。	para1 ・変更なし Ver.2.0para2 →新小項目へ 第一文→新4.2.1j)1)へ 第二文→新4.2.1j)3)へ
4.2.1j)1)	4.2.1g)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。			・変更（項番追加） （内容はVer2.0第4 2.(1)⑧para2第一文と同じもの）
4.2.1j)2)	現在実施されている管理目的及び管理策（4.2.1e)2)参照）。			・新規
4.2.1j)3)	附属書Aの管理目的及び管理策の中から適用除外としたものすべて，及びその除外理由。			・変更（項番追加） （内容はVer2.0第4 2.(1)⑧para2第二文を一部変更したもの）
	参考　適用宣言書は，リスク対応に関する決定をまとめたものである。除外理由を示すことによって，不注意から除外された管理策がないことを照合確認できる。			・新規

本文
管理策の有効性の測定

4.2.1 ISMSの確立

4.2.1c) para2 選択したリスクアセスメントの方法（methodology）では，リスクアセスメントが比較可能で再現可能な結果を出すものであることを，確実にすること。

4.2.2 ISMSの導入及び運用

4.2.2d) 選択した管理策又は管理策一式の有効性を測定する方法について規定する。また，比較可能で再現可能な結果を出すために，管理策の有効性を評価する（assess）のにこの測定方法をどのように利用すべきかを特定する（4.2.3c)参照）。

4.2.3 ISMSの監視及び見直し

4.2.3b) 当該ISMSの有効性に関して定期的な見直しを実施する（ISMS基本方針及び目的を満たすこと，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，インシデント，**有効性の測定結果**，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。

4.2.3c) セキュリティ要求事項が満たされていることを検証するために，管理策の有効性を測定する。

4.2.3d) あらかじめ定められた間隔でリスクアセスメントの見直しを行い，残留リスク及び識別された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。

・
・

5) 実施された管理策の有効性。

4.3.1 文書化に関する要求事項 一般

ISMS文書には、次の事項を含めること。

4.3.1d) リスクアセスメントの方法（methodology）についての説明（4.2.1c)参照）。

4.3.1g) 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，また**管理策の有効性を測定する方法（4.2.3c)参照）を説明するために，**組織が必要と判断した，文書化された手順。

7 ISMSのマネジメントレビュー

7.2 f) 有効性の測定結果を、マネジメントレビューへのインプットに含めること。

7.3e) 管理策の有効性を測定する方法の改善を、マネジメントレビューからのアウトプットに関する決定及び処置を含めること。

本文
セキュリテ計画

ISO/IEC 27001		ISMS認証基準Ver.2.0		
項番	条文	項番	条文	備考
4.2.3		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。	・変更なし
4.2.3g)	監視及び見直しの活動で検出された事項を踏まえて，セキュリティ計画を更新する。			・新規

本文
文書化

ISO/IEC 27001		ISMS認証基準Ver.2.0		
項番	条文	項番	条文	備考
4.3		第4 3.	文書化に関する要求事項	・変更なし
4.3.1	文書には，経営陣の決定に関する記録を含めること。また，文書は，活動が経営陣の決定及び基本方針まで追跡可能であり，記録された結果が再現可能なことを確実にするものであること。 文書によって，選択した管理策から遡って当該管理策とリスクアセスメント及びリスク対応のプロセスの結果までの関連を実証できること，また，さらに遡ってISMS基本方針及び目的までの関連を実証できることが重要である。 ISMS文書には，次の事項を含めること。	第4 3.(1)	一般 ISMS文書には、次の事項を含めること。	・変更なし para1&2 ・新規 para3 ・変更なし
4.3.1a)		第4 3.(1)①	情報セキュリティ基本方針（第4 2.(1)②参照）及び管理目的の表明。	・変更（一部変更）
4.3.1b)		第4 3.(1)②	当該ISMSの適用範囲（第4 2.(1)①参照）並びにISMSを支える手順及び管理策。	・変更（一部削除） （後半削除→4.3.1c)へ）
4.3.1c)	当該ISMSを支える手順及び管理策。			・変更（項番追加） （内容は、旧4.3.1b)の後半部分）
4.3.1d)	リスクアセスメントの方法（methodology）についての説明（4.2.1c)参照）。			・新規
4.3.2f)	必要とする人にとって文書が使用可能であることを確実にし，また文書がその分類区分に適用される手順に従って移動，保管，及び完全に廃棄されることを確実にする。			・新規

本文
リスクアセスメント計画

ISO/IEC 27001		ISMS認証基準Ver.2.0		
項番	条文	項番	条文	備考
7.3		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。	・変更なし
7.3a)		第6 3.①	ISMSの有効性の改善。	・変更なし
7.3b)	リスクアセスメント計画及びリスク対応計画の更新。			・新規
7.3c)		第6 3.②	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。それらの 事象には、次の事項に対する変更が含まれる。	・変更（一部追加）
7.3c) 1)		第6 3.②(ア)	事業上の要求事項。	・変更なし
7.3c) 2)		第6 3.②(イ)	情報セキュリテ 要求事項。	・変更なし
7.3c) 3)		第6 3.②(ウ)	既存の事業上の要求事項を満たす業務プロセス。	・変更なし
7.3c) 4)		第6 3.②(エ)	規制環境又は法的環境。	・変更（一部変更）
7.3c) 5)	契約上の義務。			・新規
7.3c) 6)		第6 3.②(オ)	リスクの度合い及びリスク受容の水準。	・変更（一部変更）
7.3d)		第6 3.③	必要となる経営資源。	・変更なし
7.3e)	管理策の有効性を測定する方法の改善。			・新規

本文
リスクを受容する基準と受容可能なリスクの水準

ISO/IEC 27001		ISMS認証基準Ver.2.0		
項番	条文	項番	条文	備考
5	**経営陣の責任**	**第5**	**経営陣の責任**	
5.1		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。	・変更なし
5.1a)		第5 1.①	情報セキュリティ基本方針を確立する。	・変更（一部変更）
5.1b)		第5 1.②	情報セキュリティ目標が設定され、計画が策定されることを確実にする。	・変更（一部変更）
5.1c)		第5 1.③	情報セキュリティに対する役割及び責任を定める。	・変更なし
5.1d)		第5 1.④	情報セキュリティ目標を達成することの重要性及び情報セキュリティ基本方針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。	・変更なし
5.1e)		第5 1.⑤	ISMSの確立、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）。	・変更（一部変更）
5.1f)	リスクを受容するための基準，及び受容可能なリスクの水準を決める。	第5 1.⑥	リスクの受容可能な水準を決める。	・変更（大幅変更）
5.1g)	ISMSの内部監査が実施されることを確実にする（6参照）。			・新規
5.1h)		第5 1.⑦	ISMSのマネジメントレビューを実施する（第6参照）。	・変更なし

附属書A 管理目的及び管理策」

ISO/IEC 27001:2005
ISO/IEC 17799 :2005
の管理目的及び管理策と全く同じ

ISMS認証基準 (Ver.2.0)

	ISO/IEC 27001:2005	ISMS認証基準 (Ver.2.0)
	A.5 セキュリティ基本方針	3. セキュリティ基本方針
	A.6 情報セキュリティのための組織	4. 組織のセキュリティ
	A.7 資産の管理	5. 資産の分類及び管理
	A.8 人的資源のセキュリティ	6. 人的セキュリティ
	A.9 物理的及び環境的セキュリティ	7. 物理的及び環境的セキュリティ
	A.10 通信及び運用管理	8. 通信及び運用管理
	A.11 アクセス制御	9. アクセス制御
	A.12 情報システムの取得、開発及び保守	10. システムの開発及び保守
NEW	A.13 情報セキュリティインシデント管理	6.3 セキュリティ事件・事故及び誤動作への対処 8.1.3 事件・事故管理手順 12.1.7 証拠の収集等)
	A.14 事業継続管理	11. 事業継続管理
	A.15 コンプライアンス	12. 適合性

附属書A 管理目的及び管理策」

	ISO/IEC 27001:2005	ISMS認証基準（Ver.2.0）
管理策	133	127

追加			削除	
管理目的 +7			**管理目的 -4**	
A.8.1 雇用前 A.8.2 雇用期間中 A.8.3 雇用の終了又は変更 A.10.2 第三者が提供するサービスの管理 A.10.9 電子商取引サービス A.12.6 技術的ぜい弱性管理 A.13.2 情報セキュリティインシデントの管理及びその改善			4. 3）外部委託 6. 1）職務定義及び雇用におけるセキュリティ 6. 2）利用者の訓練 7. 3）その他の管理策	
管理策 +17			**管理策 -11**	
A.6.1.1 A.6.1.7 A.6.2.2 A.7.1.2 A.7.1.3 A.8.2.1	A.8.3.1 A.8.3.2 A.8.3.3 A.9.1.4 A.10.2.1 A.10.2.2	A.10.2.3 A.10.4.2 A.10.9.2 A.10.10.3 A.12.6.1	4.(1)① 4.(1)⑤ 4.(3)① 6.(3)③ 8.(1)⑥ 9.(4)②	9.(4)④ 9.(5)⑥ 10.(3)② 10.(3)③ 10.(3)④

管理目的－追加と削除－

－ 追加 －

1	A.8.1	雇用前	6.(1)職務定義及び雇用におけるセキュリティ
2	A.8.2	雇用期間中	6.(2)利用者の訓練
3	A.8.3	雇用の終了又は変更	---
4	A.10.2	第三者が提供するサービスの管理	---
5	A.10.9	電子商取引サービス	8.(7)情報及びソフトウェアの交換 （10.8と10.9に分割）
6	A.12.6	技術的ぜい弱性管理	----
	A.13	情報セキュリティインシデントの管理	旧6.(3)①～6.(3)④、 及び旧8.(1)③、12.(1)⑦
7	A.13.2	情報セキュリティインシデントの管理及びその改善	---

－ 削除－

1	4.(3)	外部委託	A.6.2へ統合
2	6.(1)	職務定義及び雇用におけるセキュリティ	A.8.1
3	6.(2)	利用者の訓練	A.8.2
4	7.(3) 7.(3)① 7.(3)②	その他の管理策 クリアデスク及びクリアスクリーンの個別方針 資産の移動	タイトルから混乱が生じたため、削除 7(3)①はA.11.3.3 7(3)②はA.9.2.7へ移動

管理策 －追加と削除－

－ 追加 －

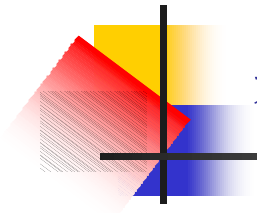
1	A.6.1.1	情報セキュリティに対する経営陣の責任	4.(1)①
2	A.6.1.7	専門組織との連絡	4.(1)⑥ （A.6.1.6とA.6.1.7に分割）
3	A.6.2.2	顧客対応におけるセキュリティ	---
4	A.7.1.2	資産の所有権	---
5	A.7.1.3	資産利用の許容範囲	---
6	A.8.2.1	経営陣の責任	---
7	A.8.3.1	雇用終了又は変更に関する責任	---
8	A.8.3.2	資産の返却	---
9	A.8.3.3	アクセス権の削除	---
10	A.9.1.4	外部及び環境の脅威からの保護	7.(1)③ （A.9.1.3とA.9.1.4に分割）
11	A.10.2.1	第三者が提供するサービス	---
12	A.10.2.2	第三者が提供するサービスの監視及びレビュー	---
13	A.10.2.3	第三者が提供するサービスの変更に対する管理	---
14	A.10.4.2	モバイルコードに対する管理策	---
15	A.10.9.2	オンライン取引	---
16	A.10.10.3	ログ情報の保護	
17	A.12.6.1	技術的ぜい弱性の管理	----

－ 削除－

1	4.(1)①	情報セキュリティ運営委員会	A.6.1.1へ統合
2	4.(1)⑤	専門家による情報セキュリティの助言	A.6.1.1へ統合
3	4.(3)①	外部委託契約におけるセキュリティ要求事項	A.6.2.3へ統合
4	6.(3)③	ソフトウェアの誤動作の報告	A.13.1.1へ統合
5	8.(1)⑥	外部委託による施設管理	A.10.2へ （内容も拡張）
6	9.(4)②	指定された接続経路	
7	9.(4)④	ノードの認証	A.11.4.2へ統合
8	9.(5)⑥	利用者を保護するための脅迫に対する警報	A.13.1.1へ統合
9	10.(3)②	暗号化	A.12.3.1へ統合
10	10.(3)③	ディジタル署名	A.12.3.1へ統合
11	10.(3)④	否認防止サービス	A.12.3.1へ統合

まとめ

- ISO/IEC 27001:2005についてISMS認証基準(Ver.2.0)からの主な変更点について、幾つか取り上げて説明しました。
  - 適用宣言書
  - 管理策の有効性の測定
  - セキュリティ計画
  - 文書化
  - リスクアセスメント計画
  - リスクを受容する基準と受容可能なリスクの水準



参考資料（変更の概要）

0 序文 –ISO/IEC 27001:2005-

•全般的に変更

- 0.2 PDCAの説明 図の下表）

  「情報セキュリテ基本方針」

  →「**ISMS基本方針**」

  4.2.1参考を参照*

  ※ この他、4.2.3b)、4.3.1a)、5.1a)も同様。

- **OECDガイドラインへの言及**の追加

*4.2.1参考　この規格の目的のため，ISMS基本方針は，情報セキュリテ基本方針を含むものとみなす。これらの方針は，一つの文書のなかに記載することができる。

1 適用範囲 –ISO/IEC 27001:2005-

•全般的に変更

- 1.1 第一段落

  規格対象についての言及の追加 → 明確化。

- 1.2 再構成（文の順序等）

- **参考情報の追加**

  例：1.1 参考1 「business（事業）」についての定義

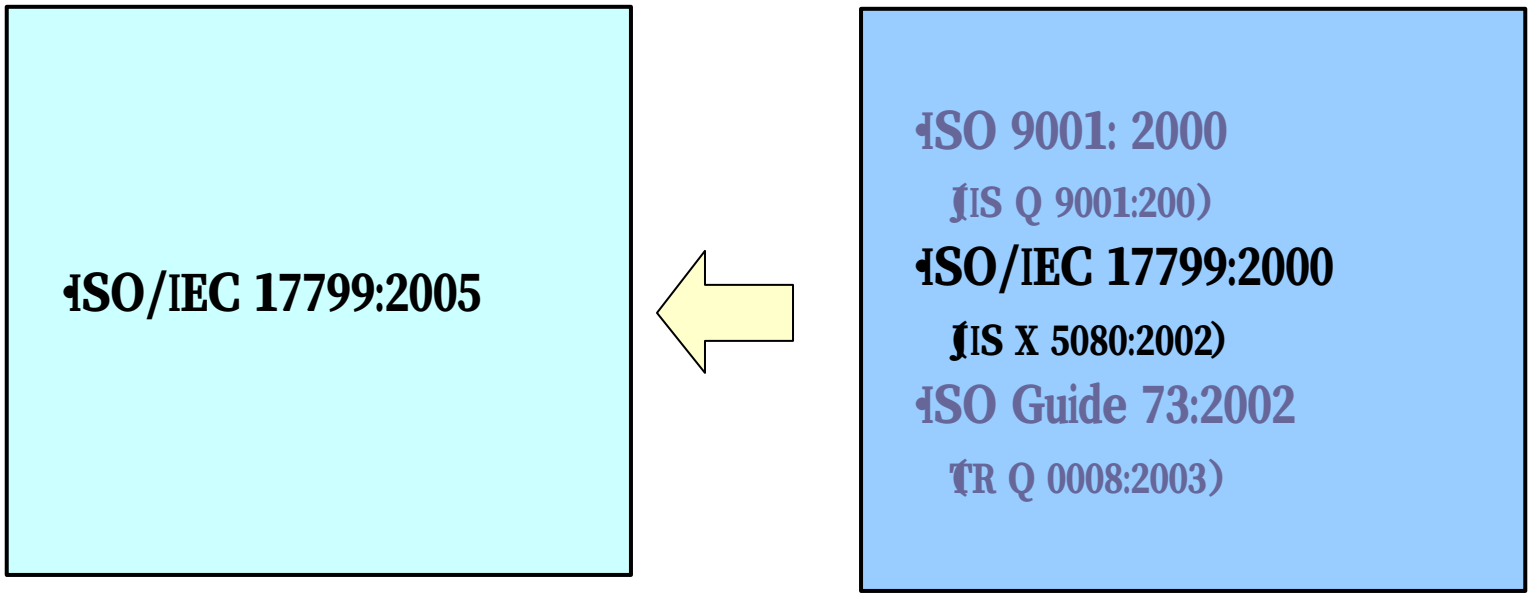
  参考2 ISO/IEC 17799:2005の位置づけ

  1.2 参考 他のMS規格を有している組織の場合

2 引用規格 –ISO/IEC 27001:2005-

ISO/IEC 27001:2005

ISMS認証基準（Ver.2.0）



3 用語及び定義

ISO/IEC 27001:2005				ISMS認証基準（Ver.2.0）		
ISO/IEC 13335-1:2004	3.1	資産 NEW				
	3.2	可用性	CIAの定義変更（参照規格の変更）	第3.1	可用性	ISO/IEC 17799:2000（JIS X 5080-2002）
	3.3	機密性		第3.2	機密性	
	3.8	完全性		第3.5	完全性	
ISO/IEC 17799:2005	3.4	情報セキュリティ	定義変更	第3.3	情報セキュリティ	
ISO/IEC TR 18044:2004	3.5	情報セキュリティ事象 NEW				
	3.6	情報セキュリティインシデント NEW				
	3.7	情報セキュリティマネジメントシステム		第3.4	情報セキュリティマネジメントシステム	
ISO/IEC Guide 73:2002	3.9	残留リスク NEW				
	3.10	リスクの受容		第3.6	リスクの受容	ISO/IEC Guide 73:2002（TR Q 0008:2003）
	3.11	リスク分析		第3.7	リスク分析	
	3.12	リスクアセスメント		第3.8	リスクアセスメント	
	3.13	リスク評価		第3.9	リスク評価	
	3.14	リスクマネジメント		第3.10	リスクマネジメント	
	3.15	リスク対応		第3.11	リスク対応	
	3.16	適用宣言書	定義変更	第3.12	適用宣言書	

4 情報セキュリティマネジメントシステム

4.1 一部変更

1）変更

「自らの事業活動全般及び）リスク」

→ 「自らの事業活動全般及び）直面するリスク」

2）変更 － ISMSの表現

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。」→
組織は、自らの事業の活動全般及び直面するリスクを考慮して、文書化されたISMSを確立、導入、運用、監視、見直し、維持、改善すること。」

← 3.7の定義との整合

3.7 情報セキュリティマネジメントシステム（information security management system, ISMS）
マネジメントシステム全体の中で、事業リスクに対する取組み方に基づいて、情報セキュリティの確立、導入、運用、監視、見直し、維持及び改善を担う部分。

※この他、0.1、5.1e)、5.2.1a) も同様

4.2.1 ISMSの確立（1/2）

変更の種類：追加、変更、削除、邦訳の変更
影響度 ー 大：★ 中：☆ 小：・

a)

★次の追加
「当該適用範囲からの除外の詳細及びその理由（1.2参照）も含め，（ISMSの適用範囲及び）境界（を定義する。）」

★「事業の特徴」→「ーの各特徴」

b)

☆3)の変更
ーISMSによって、戦略的なリスクマネジメントのコンテクスト全体を決めるべきではない、という考えから変更。

・4)Ver.2.0後半の削除
「定義されたリスクアセスメントの構造を確立する」を削除
ー4.2.1c)との重複を避けるため。

☆参考の追加（新規）
ーISMS基本方針と情報セキュリティ基本方針の関連を説明するため。

★para1「事業の特徴」→「ーの各特徴」

c)

★para2の追加（新規）
ー リスクアセスメントが、比較可能で再現可能な結果を出すものでなければならないことを示すため。

・para1の変更
ー「リスクアセスメントについての体系的な取組方法」→「組織のリスクアセスメントについての取組方法」

☆Ver.2.0 para2の第二文を削除
ー 4.2.1b)との重複を避けるため。

・para2小項目の追加（項番追加）
ーc)1) ーVer.2.0 para2の第一文を一部変更したもの。
ーc)2) ーVer.2.0 para2の第三文を一部変更したもの。

☆参考の追加（新規）
ー ISO/IEC 13335-3にリスクアセスメントの方法が記載されていることを示すため。

d)

・1)注釈追加（新規）ー
「保有者（owner）」について説明するため。

e)

☆次の変更
ー「リスクアセスメントを実施する。」→「リスクを分析し評価する。」
（ISO/IEC Guide 73に合わせて修正）

*ISO/IEC Guide 73:2002（TR 0008:2003）
3.3.1 リスクアセスメント
リスク分析（3.3.2）からリスク評価（3.3.6）までのすべてのプロセス

・1)の変更
ー第一文「事業上の損害」→「組織に対する事業上の影響」。
ー第二文「喪失による潜在的な影響」→「喪失による影響」

・4)の変更
ー参照番号「第4 2.(1)③」→「4.2.1c)2)」（小項目追加に伴う）
ー「評価基準」→「リスクを受容するための基準」

★e)2)の変更（"vulnerabilities"の後に","が追加された）
ー邦訳の表現を変更（下記参照）
→「一般に認識されている脅威及びぜい弱性並びに資産に関連する影響の観点から，起こりうるセキュリティ障害の現実的な発生可能性についてアセスメントを実施する。その際に，現在実施されている管理策を考慮する。」

f)

・2)の変更
ー参照番号「第4 2.(1)③」→「4.2.1c)2)」（小項目追加に伴う）
ー「リスクの受容のための評価基準」→「リスクを受容するための基準」（用語の統一）
ー「リスクを保有する」と参考を削除（原文にはないため。）

4.2.1 ISMSの確立（2/2）

g)	**★para2 第二文の変更** －管理策を選択する際には、「リスクを受容するための基準と、法律、規制、及び契約上の要求事項を考慮すること」を示すため。	i)	**追加項目（項番の追加）** －内容はVer.2.0 第4 2.(1)⑨の後半部分
	☆para2 第一文 の変更 －「～で明確にされた要求事項を満たすために、管理目的及び管理策を選択し）実施する」ことを示すため。 **☆para3の追加　新規）** －「管理目的及び管理策を付属書Aから選択すること」について、言及するため。 para4（段落の追加） －内容はVer.2.0 参考と同じもの。 **参考の追加（新規）** －附属書Aの内容について説明するため。	j)	**★2)の追加（新規）** －適用宣言書には「現在実施されている管理目的及び管理策」を含めることを示すため。 **★3)「除外理由」の追加** －「～から適用除外としたものすべて、及びその除外理由」 **小項目の追加（j1)～j)3)）** －箇条書のかたちに再編集され、より明確になった。 －j)1) －Ver.2.0の第一文を一部変更したもの（上記参照） －j)3) －Ver.2.0の第二文を一部変更したもの（上記参照）
h)	**後半の削除** －後半はj)へ移動（j)参照）。	参考	**☆参考の追加（新規）** －「適用宣言書は、リスク対応に関する決定をまとめたものである。除外理由を示すことによって、不注意から除外された管理策がないことを照合確認できる」ことが示されている。

4.2.2 ISMSの導入及び運用

a)	**★ 資源」の追加** －「(～の適切な活動，)**資源，** 責任～)」 リスク対応計画で特定しなければならない事項のなかに、資源」が追加された。	e)	・変更なし
b) c)	・変更なし	f)	**・「ISMSの 運用)」の追加** －何の運用が管理対象なのかを明確にするため。
d)	**★追加項目 新規)** －管理策の有効性の測定に関して追加された。 選択した管理策又は管理策一式の有効性を測定する方法について規定する。また，比較可能で再現可能な結果を出すために，管理策の有効性を評価する（assess）のにこの測定方法をどのように利用すべきかを特定する（4.2.3c)参照)。」を示すため。 **☆参考の追加 新規)** － 管理策の有効性を測定することにより、計画された管理目的が管理策によってどの程度達成されているのかが、判断」可能になることを示すため。	g)	**・「ISMSの 経営資源)」の追加** －何の経営資源が管理対象なのかを明確にするため。
		h)	**・参照番号 の追加** － (4.2.3a)参照)」が追加された。

4.2.3 ISMSの監視及び見直し

a)	**★4)の追加 新規）** － 指標を利用することにより、セキュリティ事象の検出を容易にし、その結果セキュリティインシデントを防止する」ことを盛り込むため。	c)	**★追加項目 新規）** － 「セキュリティ要求事項が満たされていることを検証するために管理策の有効性を測定する」ため。
	☆ 見直し」の追加 － (監視)及び見直し のための手順)」 手順の監視だけでなく 見直しのための手順を実施することを要求するため。 **☆5)の変更** － 「セキュリティ違反を解決するためにとるべき処置を、事業上の優先順位を踏まえて決定する。」→ 「～解決するためにとった処置の有効性を判断する。」 セキュリティ違反行為を解決するためにとった処置が、有効かどうかを判断しなければならないことを取り扱うために修正。	d)	**☆次の事項の追加** － 「あらかじめ定められた間隔でリスクアセスメントの見直しを行い、残留リスク及び識別された 受容可能なリスク水準の～)」 **☆5)の追加 新規）** －見直しのなかに **実施された管理策の有効性」**を含めるため。 **☆6) 契約上の義務」の追加** － **契約上の義務** (～社会環境など)」
		e)	**参照番号の追加** －「(～内部監査を実施する) **(参照)**。」 **参考の追加 新規）** － 内部監査は、内部的な目的のため、組織が実施することを示すため。
b)	**★ 有効性の測定結果」の追加** － 「(インシデント,)**有効性の測定結果** (提案及び～)」 有効性の測定結果」を、定期的な見直しに含めるため。	f)	**・Ver.2.0 少なくとも年1回」の削除** －7.1 (マネジメントレビュー)へ移動。 **・参照番号変更** － 第6参照」→ 7.1参照」
	・次の変更 － 「セキュリティ基本方針」→ 「ISMS基本方針」 －ここではISMSの見直しが対象であるため。	g)	**★ 追加項目 新規）** － 監視及び見直しの活動で検出された事項を踏まえてセキュリティ計画を更新する」ことを盛り込むため。
		h)	変更なし

4.2.4 ISMSの維持及び改善

a) b)	・変更なし ・変更なし
c)	**☆項目内容全体の変更** － 要求事項が、より明確になった。 利害関係者全てに結果及び講じた処置を伝達し、可能な限り合意を得る。」 → 利害関係者全てに対し、状況に応じた詳細さで講じた処置及び改善を伝達し、該当する場合は、今後の進め方について合意を得る。」
d)	・変更なし

4.3.1 文書化に関する要求事項

Para1 ～ para3	**★para1の追加 新規）** － 文書には，経営陣の決定に関する記録を含めること。また，文書は，活動が経営陣の決定及び基本方針まで追跡可能であり，記録された結果が再現可能なことを確実にするものであること」を含めるため。 **★para2の追加 新規）** － 文書によって，選択した管理策から遡って当該管理策とリスクアセスメント及びリスク対応のプロセスの結果までの関連を実証できること，また，さらに遡ってISMS基本方針及び目的までの関連を実証できることが重要である」ことを強調するため。	c)	**追加項目 項番の追加）** － 内容は、Ver.2.0 第4 3.(1)②の後半部分 b)参照）。
		d)	**★追加項目 新規）** － 「リスクアセスメントの方法についての説明」が文書に含まれることを確実にすることを明確にするため。
		e) f)	変更なし
a)	**☆次の変更** － 情報セキュリテ基本方針～及び管理目的」→「ISMS基本方針～及び目的」 4.2.1b)と整合をとるため、また、管理目的」はすでにリスク対応計画に含まれているために変更。	g)	**★次の事項の追加** － 「～運用及び管理を確実に実施するため），また管理策の有効性を測定する方法 4.2.3c)参照）を説明するために、組織が～）」
		h)	変更なし
b)	**後半の削除** －後半は、c)へ移動	i)	**☆Ver.2.0para2 文書は～にしておくこと の削除** － この要求事項は、すでに4.3.2で取り扱われているため。 （参照（第4 2.(1)⑧参照）」の削除）
		参考 1～3	変更なし

4.3.2 文書管理／ 4.3.3 記録の管理

4.3.2 para1 a) b) c)	変更なし	4.3.3 para1	**☆第二文に「保護及び」の追加** －「これらの記録は）保護及び 管理されること。）」 **☆第三文に次の追加** －「法的）又は規制要求事項，及び契約上の義務 も考慮に入れること）」 **☆第五文に「実施すること」の追加** －「管理策を文書化し，）実施すること」 **☆第六文の削除**
d)	**次の変更** － 該当する文書の最新版」→ 適用される文書の該当する版」		
e)	変更なし	para2	**☆ 「重大な」の追加** － 「重大な セキュリティインシデント）」となった。
f)	**★追加項目（新規）** － 必要とする人にとって文書が使用可能であることを確実にし，また文書がその分類区分に適用される手順に従って移動，保管，及び完全に廃棄されることを確実にする」ことについて明確にするため。	para3	**次の変更（記録の例の箇所）** － アクセスの承認記録」→ 「記入済みのアクセス承認用書類」 代表的な記録の例を示すために、変更された。
g) h) i) j)	変更なし		

5 経営陣の責任

5.1 経営陣のコミットメント　5.2 経営資源の運用管理

5.1 para1	・変更なし	5.2.1 para1	・変更なし
a)	**・次の変更** － 「情報セキュリティ基本方針」→「SMS基本方針」 この項はSMSに重点を置いているため、変更。	a)	・次の変更 － 「ISMSの確立、導入、運用及び維持」→ 「ISMSの確立，導入，運用，監視，見直し，維持，及び改善」 －ISMSの確立，導入，運用，監視，見直し，維持及び改善活動を含めるようにするため。
b)	**・次の変更** － 「情報セキュリティ目標」→「SMSの目的」 この項はSMSに重点を置いているため、変更。	b) c) d) e) f)	・変更なし
c) d)	・変更なし	5.2.2 para1	・変更なし
e)	・次の変更 － 「ISMSの確立、導入、運用及び維持に～」→ 「ISMSの確立，導入，運用，監視，見直し，維持，及び改善」 －3.7のISMSの定義と整合をとった。	a)	・変更なし
f)	**☆ 次の変更** －「リスクの受容可能な水準を決める。」→ 「リスクを受容するための基準，及び受容可能なリスクの水準を決める。」	b)	**☆変更** －「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。」 →「これらの必要な力量がもてるように教育・訓練を実施するか，又は，他の処置を講ずる（例えば，適格な要員を雇用する）。」 「他の処置を講ずる」可能性（例えば、適格な要員の雇用）も含めるよう変更された。この変更は、ISO 9001と整合をとるために加えられた。
g)	**☆追加項目（新規）** －「SMSの内部監査が実施されることを確実にする」ことを明確にするため。また、6章への参照も加えられた。	c)	**・Ver.2.0前半の削除** －b)の変更に合わせて、「実施した教育・訓練及びその他の」を削除した。
h)	・変更なし	d) para2	・変更なし

6 ISMSの内部監査

内容は、ISMS認証基準（Ver.2.0）の中項目6.4「SMSの内部監査」とほぼ同じもの。これが大項目となった。

para1 para2 para3	・変更なし
para4	**次の変更** － 改善活動」→「フォローアップ活動」
参考	**☆参考の追加（新規）** －ISO 19011:2002について言及するため。

7 ISMSのマネジメントレビュー

7.1 一般／7.2 マネジメントレビューへのインプット／7.3 マネジメントレビューからのアウトプット

7.1	☆「少なくとも年1回）」の追加 － Ver.2.0第4 2.(3)⑤から移動。 ・項番の変更 第6 1.→7.1） （・次の変更 －“the security policy and security objectives” → ”information security policy and information security objectives” －邦訳では、元々「情報」が補足されていたので、変更なし。）	7.3 para1	・項番の変更 第6 3.→7.3） ・他変更なし
		a)	・変更なし
		b)	★追加項目 新規） －「リスクアセスメント計画及びリスク対応計画の更新」を、マネジメントレビューからのアウトプットに含めるため。
7.2 para1	・項番の変更 第6 2.→7.2） ・次の変更 － 次の情報」→ 次の事項」	c)	☆ 管理策（の修正）」の追加 －「セキュリティを実現する手順）及び管理策（の修正）」 手順及び管理策の修正」を含むよう、拡張された。 ・4)次の変更 － 規制環境又は法的環境。」→ 規制又は法的要求事項。」 ☆5)の追加 新規） － 契約上の義務」をマネジメントレビューからのアウトプットに含めるため。 6) 次の変更 －「リスク受容の水準」→ 「リスクを受容するための基準」（用語の統一）
a) b) c) d) e)	・変更なし		
f)	★追加項目 新規） －「有効性の測定結果」を、マネジメントレビューへのインプットに含めるため。	d)	・変更なし
		e)	★追加項目 新規） － 管理策の有効性を測定する方法の改善」を、マネジメントレビューのアウトプットに含むため。
g) h) i)	・変更なし		

8 ISMSの改善

8.1 継続的改善／8.2 是正処置／8.3 予防処置

8.1	**参照追加** －「(参照)」を追加。 **項番の変更 第7 1.→8.1)** (次の変更 －"security objectives"→"information security objectives" －Ver.2.0は、元々情報セキュリティ目的となっていたので 変更なし。)	8.3 para1	**☆次の変更** －「不適合の発生を未然に防ぐための 処置)」→ 「SMS要求事項への起こり得る不適合が発生することを防止するために、その原因を除去する 処置)」 **項番の変更 第7.→8.3)**
		a)	変更なし
8.2 para1	**次の変更** －「SMSの導入及び運用に関連する(不適合)」→ 「SMS要求事項への 不適合)」 **項番の変更 第7 2.→8.2)**	b)	**★追加項目 新規)** －「不適合の発生を予防するための処置の必要性の評価」
a)	**☆Ver.2.0「SMSの導入及び運用における」を削除** －あらゆる種類の不適合を取り扱うために、「不適合の識別」と短縮された。	c) d) e)	変更なし
			(Ver.2.0 第7.3⑤削除) － 変更され、para2へ移動 (下記参照)
b) c) d) e) f)	変更なし	para2	**☆段落の追加 (内容は、Ver.2.0第7.3⑤を大幅に変更したもの)** 「組織は、リスクの変化を識別すること、また、大きく変化したリスクに重点を置いた、予防処置に関する要求事項を識別すること」について記述。
		para3	変更なし(Ver.2.0para1と同じ)
		参考	変更なし

ご静聴ありがとうございました

ISMS適合性評価制度　技術専門部会
(財)日本情報処理開発協会
　　情報セキュリテ部　ISMS制度推進室
Tel:　03-3432-9386
FAX:　03-3432-6200
E-mail: info@isms.jipdec.jp
Web: http://www.isms.jipdec.jp/