ISO27001（ISMS）規格改訂における変更点と他の規格との関係

～ICT担当者のためのISO規格比較～

2014年5月15日

ICTチーム
田中弘明 ・ 深谷純子
事業継続准主任管理者
情報セキュリティ監査人補
オフィスセキュリティコーディネータ
内部監査士（QIA)

本日のお話

1．ISO27001とは
2．規格改訂における変更点について
3．ICT担当者にとってのISO活用方法

はじめに

ICTサービスを利用するまたは提供するうえで、情報セキュリティの維持が欠かすことのできない重要なテーマであると認識しています。

2013年10月に改訂された情報セキュリティに関する国際規格「ISMS＝ISO27001:2013」を題材に規格改訂のポイントと管理策の一つ「事業継続管理」に関する要求事項の変遷と「BCMS＝ISO 22301:2012」との関係について解説します。

1．ISO27001とは

情報セキュリティマネジメントシステム（ISMS）の国際規格

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－要求事項 （2005年発行、2013年改訂）

重要な情報資産の
セキュリティ（機密性・完全性・可用性）が脅かされることで
組織が著しい損害を被らないようにするため、
適切な対応の仕方・考え方についてそのルールを示したものです。

関連する規格（DR/BC関係のみ）

- ISO/IEC 27031:2011
  - 情報技術（セキュリティ関連）事業継続のためのICT対策ガイドライン
- ISO/IEC 2476:2008
  - 情報技術（セキュリティ関連）ICT災害復旧サービスのためのガイドライン
- ISO/IEC 1804:2006
  - 情報技術（セキュリティ関連）侵入検知システムの選択、展開と運用
- ISO/IEC TR 18044:2004
  - 情報技術（セキュリティ関連）情報セキュリティ障害管理

2. 規格改訂における変更点について

2013年10月1日にISO/IEC27001:2013発行

ISO22301：2012
共通事項

改訂ポイント

①マネジメントシステム規格での共通要求事項の適用

②リスクマネジメント規格（ISO 31000）への対応

③BCMS 規格（ISO 23001）への対応

共通要求事項を適用する背景

ISO22301：2012
共通事項

- ISO9001やISO14001のように、複数のマネジメントシステムを導入する組織の増加。
- これにより、マネジメントシステム間の整合性向上（共通化）を図り、組織の負担を軽減する。

①マネジメントシステム規格での共通要求事項の適用

改訂の特徴

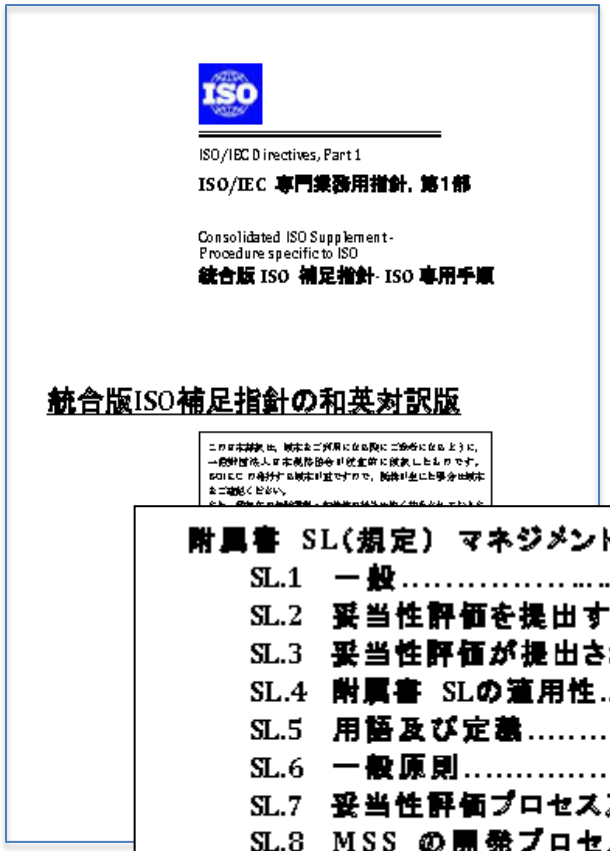
ISO22301：2012
共通事項

マネジメントシステム規格（※MSS）の整合を図るため、MSSの上位構造（HLS：High Level Structure）および共通テキスト（Idential Core Text）、共通用語、定義が開発され、それらに基づいて改訂されている。

従って、2005年版の要求事項のほぼ半分以上がMSS共通テキストの中に包含された構成となっている。

※MSS(Management System Standard)

2. ISO27001変更点　①MS規格共通要求事項の適用


ISO/IEC Directives, Part 1

ISO/IEC 専門業務用指針, 第1部

Consolidated ISO Supplement -
Procedure specific to ISO

統合版 ISO 補足指針- ISO 専用手順

統合版ISO補足指針の和英対訳版

ISO規格を策定するための指針
2013年　第4版

附属書SL　Appendix 2　を参照

日本規格協会のホームページよりダウンロード可

章立てや書き方を統一

Appendix 2
(規定)
上位構造，共通の中核となる共通テキスト，共通用語及び中核となる定義

規格作成者への注記　共通テキストの中でXXXと表記してある部分には，マネジメントシステムの分野固有を示す修飾語（例えば，エネルギー，道路交通安全，ITセキュリティ，食品安全，社会セキュリティ，環境，品質）を挿入する必要がある。青色のテキストは，規格原案作成者への助言を示す。

MSSの上位構造（HLS：High Level Structure）

以下のHLSの“XXX”に分野固有のテキスト（品質、環境、情報セキュリティ等）に書き換えられたかたちで、開発・改正作業が進められている

0. 序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況 4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 XXXマネジメントシステムの適用範囲の決定 4.4 XXXマネジメントシステム
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 5.2 方針 5.3 組織の役割、責任及び権限
6. 計画 6.1 リスク及び機会に対処する処置 6.2 XXX目的及びそれを達成するための計画策定

XXXには、品質、環境、情報セキュリティ、食品安全、エネルギーなどの固有の名称を記述される

7. 支援 7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報 7.5.1 一般 7.5.2 作成及び更新 7.5.3 文書化された情報の管理
8. 運用 8.1 運用計画及び管理
9 パフォーマンス評価 9.1 監視、測定、分析、及び評価 9.2 内部監査 9.3 マネジメントレビュー
10. 改善 10.1 不適合及び是正処置 10.2 継続的改善

附属書SL　Appendix 2 より

2. ISO27001変更点　①MS規格共通要求事項の適用

ISO27001:2013版の構成

0.序文
1 適用範囲
2 引用規格
3 用語及び定義
4 組織の状況 4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 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 4.4 情報セキュリティマネジメントシステム
5 リーダシップ 5.1 リーダシップ及びコミットメント 5.2 方針 5.3 組織の役割、責任及び権限
6 計画 6.1 リスク及び機会への取り組み 6.1.1 一般 6.1.2情報セキュリティリスクアセスメント 6.1.3情報セキュリティリスク対応 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

7 支援 7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化された情報 7.5.1 一般 7.5.2 作成及び更新 7.5.3文書化された情報の管理
8 運用 8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
9 パフォーマンス評価 9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善 10.1 不適合及び是正処置 10.2 継続的改善
附属書　A 管理目的及び管理策

規格固有の部分(赤字)は
“上位構造、共通の中核となるテキスト 並びに 共通用語 及び中核となる定義の
整合に影響せず、それらの意図と矛盾せず、かつ、それらの意図を弱めない”範囲でのテキストの追加、箇条の追加、ビュレット項目(箇条書き項目)の追加が認められている。

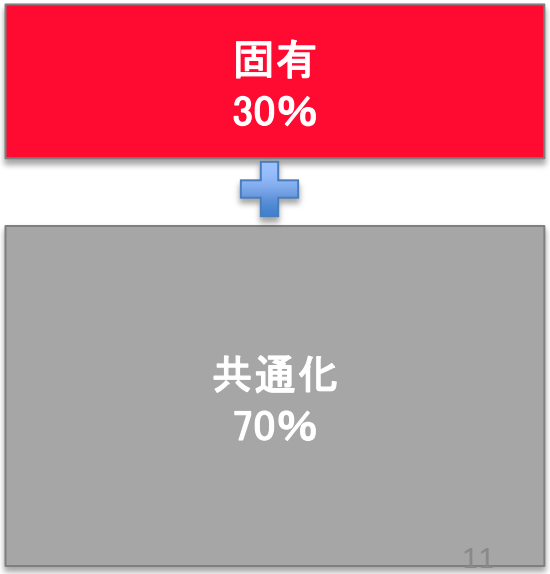
ISO22301:2012版 の構成

0 序文
1 適用範囲
2 引用規格
3 用語及び定義
4 組織の状況 4.1 組織とその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 事業継続マネジメントシステムの適用範囲の決定 4.4 事業継続マネジメントシステム
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 5.2 経営者のコミットメント 5.3 方針 5.4 組織の役割，責任及び権限
6 計画 6.1 リスク及び機会に対応するための処置 6.2 事業継続目的及び達成計画

7 支援 7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーションヨン 7.5 文書化した情報
8 運用 8.1 運用の計画及び管理 8.2 事業影響度分析及びリスクアセスメント 8.3 事業継続戦略 8.4 事業継続手順の確立及び導入 8.5 演習及び試験の実施
9 パフォーマンス評価 9.1 監視，測定，分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善 10.1 不適合及び是正処置 10.2 継続的改善

マネジメントシステム規格　共通化のイメージ

27001/2013の場合は70:30の割合



共通化の例： マネジメントシステム規格の指針

統合版 ISO 補足指針－2013 年版

それぞれの規格名に置き換える

ISMS
BCMS
・・・・

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，XXX マネジメントシステム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。

- XXX 方針及び XXX 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。
- 組織の事業プロセスへの XXX マネジメントシステム要求事項の統合を確実にする。
- XXX マネジメントシステムに必要な資源が利用可能であることを確実にする。
- 有効な XXX マネジメント及び XXX マネジメントシステム要求事項への適合の重要性を伝達する。
- XXX マネジメントシステムがその意図した成果を達成することを確実にする。
- XXX マネジメントシステムの有効性に寄与するよう人々を指揮し，支援する。
- 継続的改善を促進する。
- 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。

注記　この規格で"事業"という場合，それは，組織の存在の目的の中核となる活動という広義の意味で解釈することが望ましい。

出典：附属書SL　Appendix2

章立をMS規格に合わせた為、分かり易くなった

2005年度版			2013年度版	
0	序文		0	序文
1	適用範囲		1	適用範囲
2	引用規格		2	引用規格
3	用語及び定義		3	用語及び定義
4	情報セキュリティマネジメント		4	組織の状況
	4.1　一般要求事項		5	リーダーシップ
	4.2　ISMSの確立及び運営管理		6	計画
	4.3　文書化に関する要求事項		7	支援
5	経営者の責任		8	運用
6	ISMS内部監査		9	パフォーマンス評価
7	ISMSのマネジメントレビュー			
8	ISMSの改善		10	改善
附属書A			附属書A	

② リスクマネジメント規格（ISO 31000）への対応

赤字は固有部分

ISO27001:2013版の構成

0.序文
1 適用範囲
2 引用規格
3 用語及び定義
4 組織の状況 4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 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 4.4 情報セキュリティマネジメントシステム
5 リーダシップ 5.1 リーダシップ及びコミットメント 5.2 方針 5.3 組織の役割、責任及び権限
6 計画 6.1 リスク及び機会への取り組み 6.1.1 一般 6.1.2情報セキュリティリスクアセスメント 6.1.3情報セキュリティリスク対応 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

7 支援 7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化された情報 7.5.1 一般 7.5.2 作成及び更新 7.5.3文書化された情報の管理
8 運用 8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
9 パフォーマンス評価 9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー
10 改善 10.1 不適合及び是正処置 10.2 継続的改善
附属書 A 管理目的及び管理策

対応

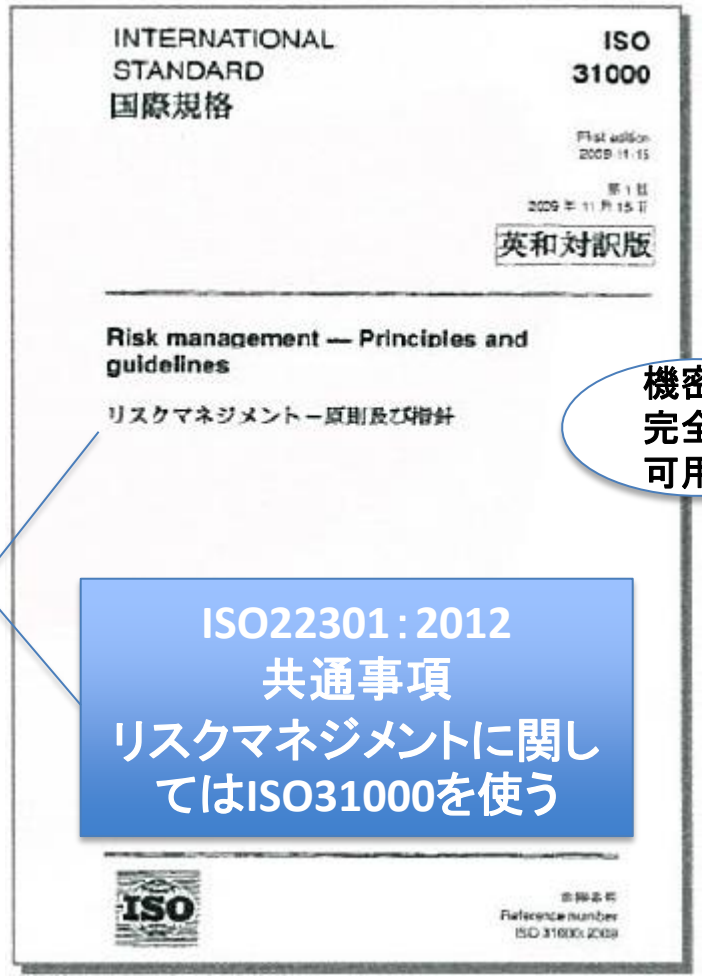
対応

「ISO31000 Risk management — Principles and guidelines」
（リスクマネジメント — 原則及び指針）

をもとに、ISO31000と親和性のある情報セキュリティリスクマネジメントに関する記述が、ISMS固有テキストとして追加されている。（箇条6.1.2, 8.2）

※用語の定義はISO/IEC（DIS）27000 を引用

「ISO31000　Risk management — Principles and guidelines」



ISO22301：2012
共通事項
リスクマネジメントに関してはISO31000を使う

ISO27001 **2005**年度版の定義は
「事象の発生確率とその結果の組み合わせ」

2013年度版でのリスクの定義は
「目的に対する不確かさの影響」

機密性
完全性
可用性

新定義に基づく想定リスクの見直し

「**情報セキュリティ目的**」に対する不確かさを与えるものは何かに関してリスク源に基づいてアセスメント（リスクの特定、分析、評価）をすることになる。

※ポジティブリスクや想定外も含まれる。

ISO/IEC（DIS）27000 で定義された用語を引用

（ISO27001：2013から用語の定義がなくなる）

ISO/IEC DIS 27000:2013

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－

概要及び用語

ISO22301：2012
共通事項
用語は個別の定義せず
ISO27000を使う

2005 年版では、16 の用語の定義が記載されていたが、27001/2013版では、個別の用語の定義はない。

ISO/IEC 27000 には、ISO/IEC 27000 シリーズ規格全体に関連する 81 の用語の定義が記載されている。（Guide73から21の用語を引用。）

例

2.71 リスクアセスメント

リスク特定・リスク分析・リスク評価のプロセス全体

2.73 リスク基準

リスクの重大性を評価するための目安とする条件
組織の目的、内部及び外部の状況に基づいたもの

2.78 リスク所有者

リスク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持つ人、または主体

③　BCMS規格（ISO 22301）への対応

ISO27001:2013～情報セキュリティリスク対策～

- カテゴリは増えているが、管理目的と管理策は減少している。
- 事業継続は情報セキュリティのみを意識

	2005年版	2013年版
カテゴリ	11	14 ↑
管理目的	39	35 ↓
管理策	133	114 ↓

情報セキュリティリスク対策

	カテゴリー	管理目的数	管理策数	2005との違い
1	情報セキュリティのための方針群	1	2	
2	情報セキュリティのための組織	2	7	削除された管理策あり
3	人的資源のセキュリティ	3	6	
4	資産の管理	3	10	内容変更
5	アクセス制御	4	14	削除された管理策あり
6	暗号	1	2	追加カテゴリ
7	物理的及び環境的セキュリティ	2	15	
8	運用のセキュリティ	7	14	削除された管理策あり
9	通信のセキュリティ	2	7	運用とカテゴリ分離
10	システムの取得、開発及び保守	3	13	削除された管理策あり
11	供給者関係	2	5	追加カテゴリ
12	情報セキュリティインシデントの管理	1	7	内容変更
13	事業継続管理における情報セキュリティの側面	2	4	内容変更
14	順守	2	8	削除された管理策あり
		35	114	

参考： 2005年度版から削除された管理策

管理No.	管理策	管理No.	管理策
A.6.1.1	情報セキュリティに対する経営陣の責任	A.11.4.4	遠隔診断用及び環境設定用ポートの保護
A.6.2.1	外部組織に関係したリスクの識別	A.11.4.6	ネットワークの接続制御
A.6.2.2	顧客対応におけるセキュリティ	A.11.4.7	ネットワークのルーティング制御
A.10.2.1	第三者が提供するサービス	A.11.5.2	利用者の識別及び認証
A.10.4.2	モバイルコードに対する管理策	A.11.5.5	セッションのタイムアウト
A.10.7.4	システム文書のセキュリティ	A.11.5.6	接続時間の制限
A.10.8.5	業務用情報システム	A.12.2.1	入力データの妥当性
A.10.9.3	公開情報	A.12.2.2	内部処理の管理
A.10.10.2	システム使用状況の監視	A.12.2.3	メッセージの完全性
A.10.10.5	障害のログ取得	A.12.2.4	出力データの妥当性確認
A.11.4.2	外部から接続する利用者の認証	A.15.1.5	情報処理施設の不正使用防止
A.11.4.3	ネットワークにおける装置の識別	A.15.3.2	情報システムの監査ツールの保護

ICTの変化に伴い陳腐化した内容については、書換え、または削除されています。

BCに関する記載変更

BCに関してはBCMSを意識して、セキュリティに関する側面のみに変更。

ISO27001:2005

A.14　事業継続管理

A.14.1　事業継続管理における情報セキュリティの側面
目的：情報システムやサービスが停止した際に、速やかに業務を復旧・継続するための管理策。

A.14.1.1 事業継続管理手続への情報セキュリティの組込み
事業活動に大きな影響を与える緊急事態へのリスク対策を計画した事業継続計画を策定し、維持すること

A.14.1.2 事業継続及びリスクアセスメント
事業活動を中断せざるを得ない緊急事態を特定すること
緊急事態を特定する際は、発生確率・事業に及ぼす影響度(リスクの識別)・情報セキュリティに及ぼす結果を考慮すること

A.14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施
緊急事態によって重要な業務プロセスが中断するような事態が発生した場合は、速やかに業務を復旧し業務継続するための、また時間内に情報が活用できるようになるよう、事業継続計画を策定し、実施すること

A.14.1.4　事業継続計画策定の枠組み
すべての事業計画の整合性を確保するため、情報セキュリティ上実施すべきことを矛盾なく実施するため、試験 及び保守の優先順位を明確にするために、事業継続計画全体を統括する枠組みを維持すること

A.14.1.5　事業継続計画の試験、維持及び再評価
事業継続計画が災害・障害時に機能するかどうかを、定期的にテストし、見直しをすること

2013 削除

統合・再編

ISO27001:2013

A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1 情報セキュリティ継続
目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むことが望ましい

A.17.1.1 情報セキュリティ継続の計画
組織は、困難な状況（adverse situation）（例えば、危機又は災害）において、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定することが望ましい

A.17.1.2 情報セキュリティ継続の実施
組織は、困難状況のもとで情報セキュリティの継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立、文書化、実施、及び維持することが望ましい

A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価
確立及び実施した情報セキュリティのための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために組織は、定められた間隔でこれらの管理策を検証することが望ましい

A.17.2 冗長性
目的：情報処理施設の可用性を確実にするために

A.17.2.1 情報処理施設の可用性
情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい

2013 追加

出典：ISO27002：2013より

A.17.1.1 情報セキュリティ継続の計画
組織は、困難な状況（adverse situation）（例えば、危機又は災害）において、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定することが望ましい

1. **BCP/DRP発動時の情報セキュリティ要件を定める。**
   セキュリティ例外を認めることも可。

2. **BCPがない場合は平常時同じ情報セキュリティ要件とする。**
   緊急時もセキュリティ例外なしが原則。

3. **BCP策定時のBIAに情報セキュリティの観点を盛り込む。**
   セキュリティ要件を変えた場合/変えない場合のインパクト

ISO/IEC27002:2013　情報セキュリティ管理策の実践のための規範より引用

A.17.1.2 情報セキュリティ継続の実施
組織は、困難状況のもとで情報セキュリティの継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立、文書化、実施、及び維持することが望ましい

1. 権限・経験・スキルのある要員をアサインする
2. インシデント対応要員を任命（情報セキュリティ事故担当）
3. BCMプロセスや支援システムやツールの情報セキュリティ管理策の確立（被災時のSNSの使い方や在宅勤務でのセキュリティ確保等）
4. BCMに情報セキュリティの専門家を関与
5. 許容可能な情報セキュリティレベルを維持する管理策

ISO/IEC27002:2013　情報セキュリティ管理策の実践のための規範より引用

A.17.1.3 情報セキュリティ継続の検証、レビュー及び評価
確立及び実施した情報セキュリティのための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために組織は、定められた間隔でこれらの管理策を検証することが望ましい

1. 発災時に実行する情報セキュリティに関するプロセス、手順、管理策をテストする。（臨時対応、権限委譲など）

2. パフォーマンス・レベルが十分か（本番を変更した時、バックアップにも反映されているか等）

3. BCMのプロセスやソリューションが変更された場合、セキュリティレベルが妥当かレビューする

4. 通常のセキュリティ検証とは別に、BCP訓練と一緒に行うことが望ましい

ISO/IEC27002:2013　情報セキュリティ管理策の実践のための規範より引用

A.17.2 冗長性
目的：情報処理施設の可用性を確実にするために

A.17.2.1 情報処理施設の可用性
情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい

これまでは
集中管理を推進し、分散化や冗長化は好ましくないと言われていたが、BCの観点で『冗長性』が追加された。

1. 冗長な構成要素、アーキテクチャを考慮する
2. 切替が意図したとおりに動作することを確認（テスト）する

ISO/IEC27002:2013　情報セキュリティ管理策の実践のための規範より引用

冗長性（じょうちょうせい）

システムを構成する要素・部品に予備や回避手段を付加することで、その一部に故障などがあっても全体としては停止することなく所定の要求機能を果たし続ける性質のこと。

- **並列冗長**・・同等機能を有する構成要素を複数用意して少なくとも1つの構成要素が正常に稼働していれば系統全体が稼動する。
- **縮退冗長**・・同種の構成要素を複数用意してその一部に故障が発生しても系統全体では機能を低下しながらも運転を続けられる。
- **待機冗長**・・通常は使用しない予備要素を用意して障害発生時に切り替えを行う。

まとめ：ISO27001附属書A「事業継続管理」

ISO27001:2005は、事業プロセスの保護と再開に重点が置かれ、これを支えるものとして、情報システムの継続的運用と回復がテーマになっていました。

改訂版の「A.17.1　情報セキュリティ継続」では、情報セキュリティ及び情報セキュリティマネジメントの継続と回復に主題が置かれ再構築され、情報セキュリティリスクに対する管理策としてわかりやすくなっている。

「A.17.2 冗長性」「A.17.2.1　情報処理施設の可用性」 新規追加

改訂版では新たに、情報処理施設の可用性確保についての管理策が追加されている。

情報処理施設の可用性確保は事業継続管理の一部でもあるため、ISO22301、ISO27031(例えば代替施設のセキュリティ)等との関係性がわかりやすくなった。

事業継続管理の適用対象の違い

ISO27001における事業継続管理の対象はあくまでも情報システムが中心
(27001:2013では情報システムが中心であることがより鮮明になった)

●ISO22301　適用対象は、**組織の定義する”事業”**

企業が取扱う製品やサービスを顧客に提供するために行う一連の業務、及び、これにひもづく**重要な経営資源（人、施設、供給、情報、技術）が対象範囲**となる。
従って多くの場合、広範囲な分析および対策を検討していく必要がある。

機密性・完全性・可用性

●ISO27001:2013　適用対象は、**情報システムのセキュリティ**

組織は、困難な状況（例えば、危機または災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。

曖昧にISO22301と重複していた部分が統合、変更、再編され、新たに冗長性が加わり、情報セキュリティの事業継続管理としての主旨が鮮明になった。

参考： ISO/IEC27001:2013への移行スケジュール

JIPDECの情報マネジメント推進センターによると、「既にISMS認証を取得されている組織は仕組みを大幅に変更することはないが、計画段階における経営的な観点での見直しが必要になる」とのこと。

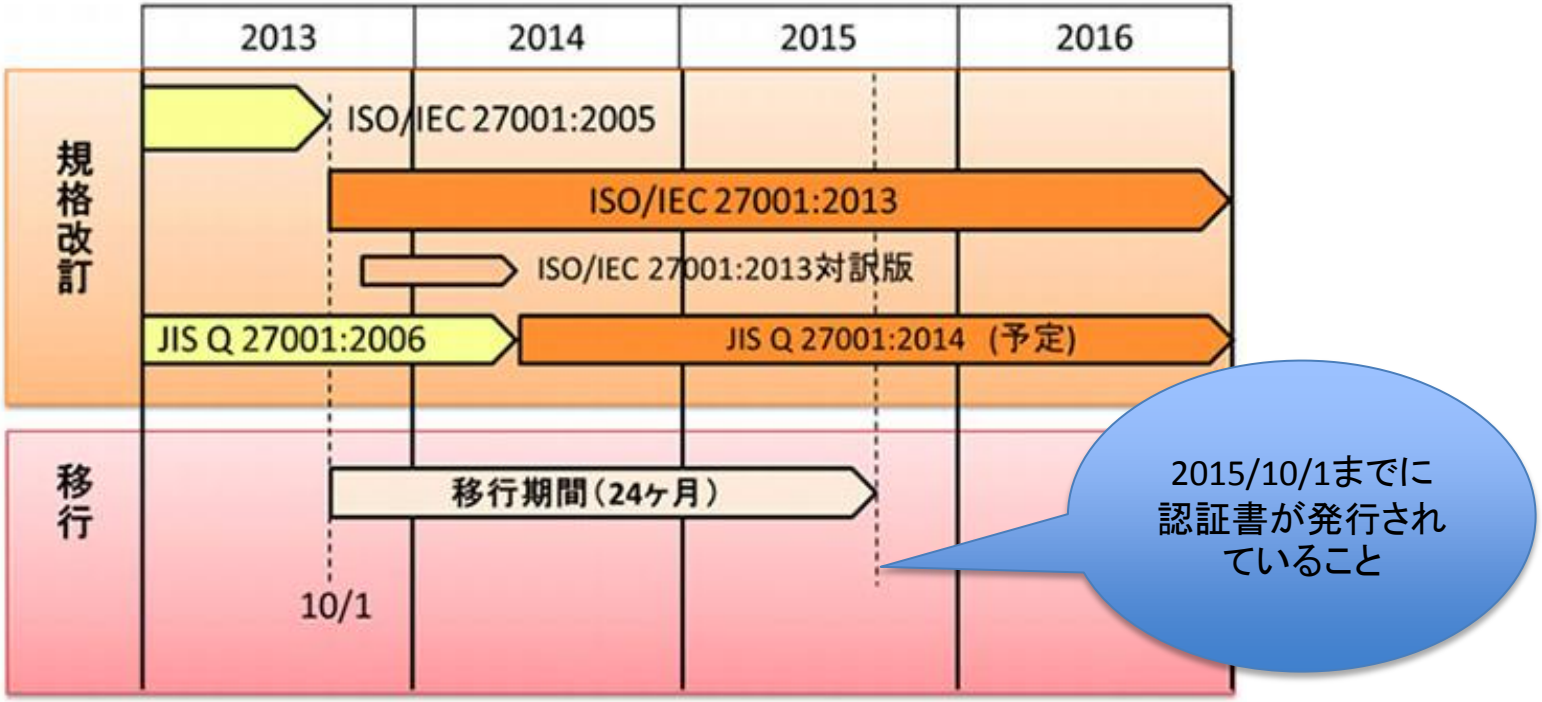


図 移行計画のイメージ

３．ICT担当者にとってのISO活用方法

- チェックリスト、参考書として使用
  - ISO27002:2013　114の管理策　等
- 目的により規格を使い分ける
  - 平常時の対策　ISO27001,ISO27002
  - BC/DR対策　ISO22031,ISO27031
- 用語の確認に使用する
  - ISO27000：情報セキュリティ用語(89語)
  - ISO22300：社会セキュリティ用語(76語)
  - Guide73：リスクマネジメント用語(50語)

参考：定義例

- ぜい弱性（vulnerability） ISO27000
  - 一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点。
- ぜい（脆）弱性（vulnerability） Guide73
  - 物事の本来的特性で，ある結果をもたらす事象につながることがあるリスク源に対する敏感さとなるもの。
- ぜい（脆）弱性（vulnerability） ISO22300
  - 物事の本来的特性で，ある結果をもたらす事象につながることがあるリスク源に対する敏感さとなるもの。
  - 注記 この場合の“敏感さ”とは，“影響を受けやすい感応度”のことである。

ご清聴ありがとうございました

ご質問をどうぞ