JSSA システム監査学会　第32回研究大会

統一論題：

新システム監査制度とシステム監査

パネルディスカッション

システム監査／基準の改訂にあたって
～新システム監査制度の普及について～

システム監査に関する検討会メンバー

コーディネータ	遠山　暁	（検討会座長）
パネリスト	梶本　政利　氏	（日本ITガバナンス協会）
	力　利則　氏	（日本システム監査人協会）
	神橋　基博　氏	（ISACA東京支部）
	黒澤　兵夫	（システム監査学会）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

全体：改訂目的と構成･留意点

改訂の全体的・基本的な目標

1．今日的情報技術環境･情報システム設計開発･管理方法の変化への対応
2．中小企業における自己診断、自己監査に対応
3．「ITガバナンスの実現に寄与」への嚮導性･操作性の向上

記述構成と留意点

1．行為規範･基準として徹底

「誰が、なにを、どのように」に留意。

「すべきこと」、「することが望ましいこと」を区別

2．各基準の構成

【監査基準】　各基準　主旨　解釈指針
【管理基準】　各項目　主旨　留意点

「解説書」的機能

（遠山　曉）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

システム監査基準の改訂のポイント

構成の見直し

旧基準の体系である「一般基準」、「実施基準」、「報告基準」から、監査実施の流れに沿って、適切な表題を付す方式への転換。

前文

I.システム監査の体制整備に係る基準
- 基準1：システム監査人の権限と責任等の明確化
- 基準2：監査能力の保持と向上
- 基準3：システム監査に対するニーズの把握と品質の確保

II. システム監査人の独立性・客観性及び慎重な姿勢に係る基準
- 基準4：システム監査人としての独立性と客観性の保持
- 基準5：慎重な姿勢と倫理の保持

III. システム監査計画策定に係る基準
- 基準6：監査計画策定の全般的留意事項
- 基準7：リスクの評価に基づく監査計画の策定

IV. システム監査実施に係る基準
- 基準8：監査証拠の入手と評価
- 基準9：監査調書の作成と保管
- 基準10：監査の結論の形成

V. システム監査報告とフォローアップに係る基準
- 基準11：監査報告書の作成と提出
- 基準12：改善提案のフォローアップ

(梶本　政利)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

システム監査基準の改訂のポイント

記載内容

1. 「基準」を「しなければならない」と記述し、「解釈指針」として、各基準の補足的な説明や、実務上の望ましい対応や留意事項を記載。

2. ガバナンス、マネジメントおよびコントロールの3つの視点からの例を記載。

3. アジャイルの場合に留意すべき事項を「解釈指針」に記載。

(梶本　政利)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

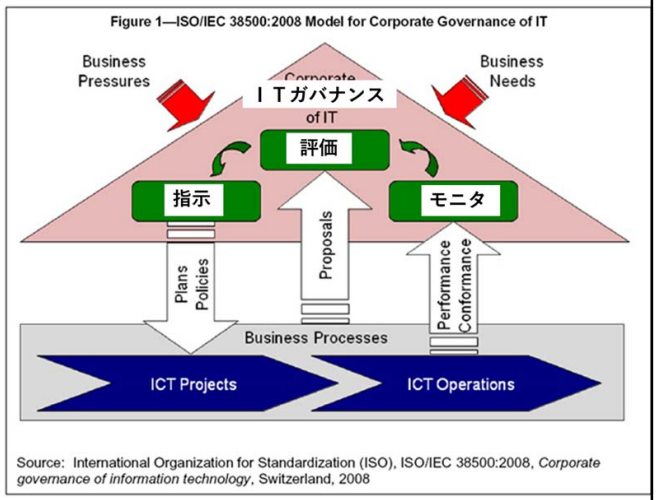
管理基準「前文」の構成と改訂ポイント

1．ITガバナンスの定義

ITガバナンスとは**経営陣**がステークホルダのニーズに基づき、組織の価値を高めるために**実践する行動**であり、情報システムのあるべき姿を示す**情報システム戦略策定及び実現に必要となる組織能力**である。

2．ITガバナンスにおけるEDMモデル

ITガバナンスの**国際標準**である**ISO/IEC 38500シリーズ**及び**JIS Q 38500**より、**評価(Evaluate)**、**指示(Direct)**、**モニタ(Monitor)**の**EDMモデル**と呼ぶ。



3．ITガバナンスにおける6つの原則

① **責任** Responsibility ② **戦略** Strategy

③ **取得** Acquisition ④ **パフォーマンス** Performance

⑤ **適合** Conformance ⑥ **人間行動** Human behaviour

(カ　利則)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

４．システム管理基準の前提となる組織体制

・ＣＩＯ　・委員会　・情報システム部門　・利用部門 等

Ⅰ．ＩＴガバナンスの改訂

1. 情報システム戦略の方針及び目標設定
2. 情報システム戦略遂行のための組織体制
3. 情報システム部門の役割と体制
4. 情報システム戦略の策定の評価・指示・モニタ
5. 情報システム投資の評価・指示・モニタ
6. 情報システムの資源管理の評価・指示・モニタ
7. コンプライアンスの評価・指示・モニタ
8. 情報セキュリティの評価・指示・モニタ
9. リスクマネジメントの評価・指示・モニタ
10. 事業継続管理の評価・指示・モニタ

(カ　利則)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

Ⅱ．企画フェーズの改訂のポイント

役割の明確化

- プロジェクト運営委員会
- CIO
- プロジェクトマネージャ（PM）

多様なシステム開発手法への対応

（神橋　基博)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

Ⅲ．開発フェーズの改訂のポイント

プロジェクト管理の明確化

Ⅳ．アジャイル開発の改訂のポイント

アジャイル開発に関係する人材

- プロダクトオーナー
- 開発チームの多能工化

アジャイル開発のプロセス（反復開発）

- イテレーション

（神橋　基博)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

Ⅴ. 運用・利用フェーズの改訂

- ベースは旧管理基準のⅣ.運用業務
- 新設した章立ての項目
  3.　情報セキュリティ管理　　5.　ログ管理
  8.　サービスレベル管理　　9.　インシデント管理
  10.　サービスデスク管理
- 情報システムの管理は情報システム部門だけが行うものではなく、利用部門も一体になって行うものである。

Ⅵ. 保守フェーズの改訂

- ベースは旧システム管理基準の保守業務
- 旧基準の他の業務項目からの移設
  4．変更管理　　6．ソフトウェア構成管理
- 新設　3.　情報セキュリティ管理
- 保守フェーズが対象とするソフトウェアには、業務ソフトウェア、ＯＳ、ミドルウェア、データベース、Ｗｅｂサイトなどを含む。

(力　利則)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

Ⅶ. 外部サービス管理の改訂

- ベースは旧管理基準のⅥ．共通事項　５．委託・受託の「委託」
- 外部組織のリソースを活用し、企業内業務の遂行を外部組織に委託することをいい、クラウド(Cloud)・ASP(Application Service Provider）等の外部サービスの利用契約も含む。
- ①外部サービス利用計画の策定　②委託先(クラウド事業者等を含む)の選定　③契約の締結　④委託先管理
- サービスの品質を維持するために、SLA(Service Level Agreement：サービスレベル合意)の締結を検討する必要がある。

Ⅹ. ドキュメント管理の改訂

- ベースは旧管理基準のⅤ.共通業務の1.ドキュメント管理
- 利用する情報サービスや情報システムの開発方法、運用形態に応じて見直していること。アジャイル開発や外部のサービス利用等の特徴に応じたルールとする。
- 利用部門長および情報システム部門長は、定期的にドキュメントルールの見直しをすること。(新設)

(力　利則)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

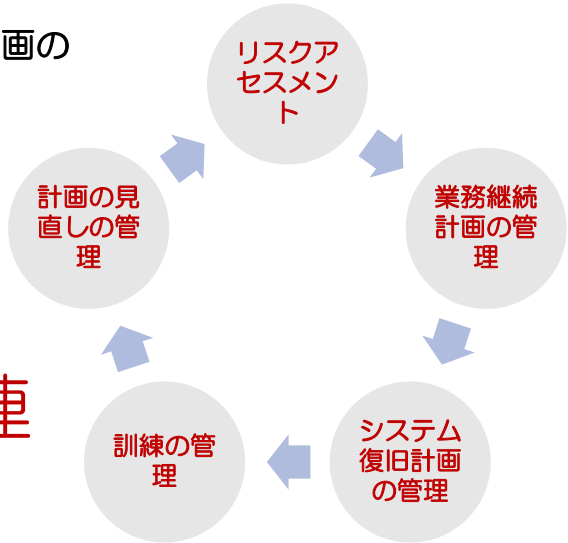
Ⅷ. 事業継続管理の改訂概要とポイント

ベースは現行管理基準のⅥ.共通業務 7.障害対策とISO/JIS Q 22301事業継続マネジメントシステムである

1.章立て項目の新設

8.4 訓練の管理　定期的、目的別、実施手順、シナリオ、ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ等

8.5 計画の見直しの管理　業務継続計画の評価・見直し、定められた間隔等



2.章立て項目の変更

3.情報セキュリティ確保に関連する管理

4.マネジメントサイクルの確立

（黒澤　兵夫）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

Ⅸ. 人的資源管理の改訂概要とポイント

1.章立て項目の変更

責任と権限の管理、業務遂行の管理、教育・訓練の管理

2. 情報セキュリティ確保に関連する管理

3. 更新事項

①明確　主語＋述語＋どのように

②最近の社会環境・情勢に基づき詳細に述べる　ﾒﾝﾀﾙﾍﾙｽ

③情報セキュリティ、個人情報について、情報セキュリティ管理基準、個人情報保護法に適合の必要性を謳う。

（黒澤　兵夫）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

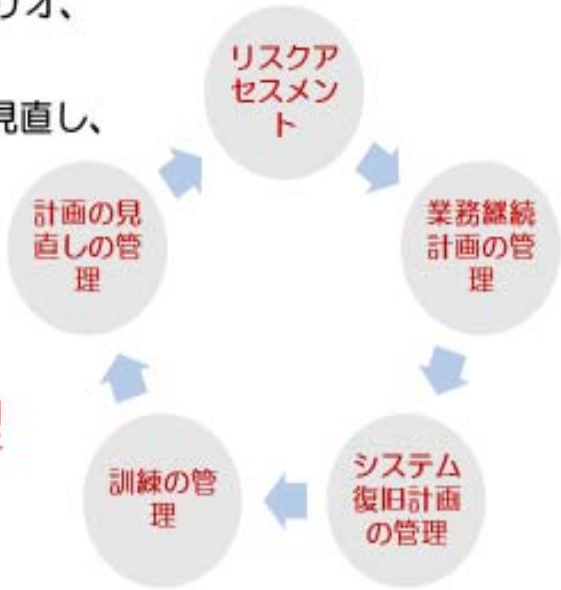
Ⅷ. 事業継続管理の改訂概要とポイント

ベースは現行管理基準のⅥ.共通業務 7.障害対策とISO/JIS Q 22301事業継続マネジメントシステムである

1.章立て項目の新設

8.4 訓練の管理　定期的、目的別、実施手順、シナリオ、ﾏﾈｼﾞﾒﾝﾄﾚﾋﾞｭｰ等

8.5 計画の見直しの管理　業務継続計画の評価・見直し、定められた間隔等



2.章立て項目の変更

3.情報セキュリティ確保に関連する管理

4.マネジメントサイクルの確立

2018/6/8

(黒澤　兵夫)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

ITGIでの基準関連の取組み

ITGI Japanとして

1. 「ITガバナンス」の普及活動の強化
   経営課題として、情報システムのガバナンスを確立し、強化していくための情報の継続的発信。
2. ITGI Japan Conferenceの継続的開催
   情報システムのガバナンスに関する事例や話題の提供。
   （2018年は11月12日に開催）

個人として考えること

1. グローバル化のための条件整備（少なくとも英語化）
2. クラウド等の監査に資するマテリアルの整備
3. OT (Operational Technology)からの視点の導入　等

(梶本　政利)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

SAAJでの基準関連の取組み

1．新システム監査／管理基準説明会（特別月例会にて）
・5/19実施済（約170名参加）＊今後も実施予定

2．『情報システム監査実践マニュアル』(赤本)の改訂
・サブコントロール、各種事例作り　等

3．ＳＡＡＪ内の研究会として実践普及活動
・環境別のシステム管理基準の活用方法等を実施予定

4．ISO38500ｼﾘｰｽﾞ(ITｶﾞﾊﾞﾅﾝｽ)の国内での普及促進（JIS化等）

5．今回事前検討から連携協力した4団体による定期的な改訂作業の推進の実現

（カ　利則）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

ISACA東京支部での基準関連の取組み

「システム監査制度研究会」の立上げ

今後の改訂に向けて、新たに追加すべきテーマや技術領域におけるガイドラインを検討。

アジャイル／DevOps

自己診断／小規模事業者向けチェックリスト

ＡＩ／ＩｏＴ

ＩＳＡＣＡ会員向けセミナーの開催

調整中

(神橋 基博)

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.

JSSAでの基準関連の取組み

１．専門監査人等への新システム監査制度講演会開催

２回実施予定　　第１回７月～９月　　第２回１１月～１月

２．上記講演＋専門監査人更新講座（案）

専門監査人制度（更新）検討

情報セキュリティ専門監査人

個人情報保護専門監査人

会計システム専門監査人

３．システム監査制度検討委員会

新システム監査制度の普及活動，ｱﾝｹｰﾄ調査、新機能検討、4団体連携等

４．「BCP/BCMSと新システム監査制度」研究プロジェクト発足

（黒澤　兵夫）

©2018JSSAシステム監査学会－「第32回研究大会」 All right reserved.