システム監査学会 第33回研究大会

「BCP/BCMSと新システム監査制度」研究プロジェクト報告

「新システム監査とBCP」

"Studies of new Systems Audits and BCP"

2019年6月7日

1．当研究プロジェクトの内容紹介①

「BCP/BCMSと新システム監査制度」研究プロジェクト

- 2018年度新規発足プロジェクト
- 主査：黒澤　兵夫
  メンバー：竹淵　広志　他　2名
- 2018年9月～2019年5月まで、月1回開催
  （全9回開催）

1．当研究プロジェクトの内容紹介②

【研究テーマ】

・新システム監査制度（新監査基準および新管理基準）の発行に伴い、システム監査、監査制度を普及と啓蒙につとめる。
また、新しい技術 IoT、AI、ビッグデータ等への適合性を調査・研究する。

・上記の結果をBCP/BCMS関連の監査へ適用を図っていく予定。

２．中小企業向け「システム管理基準」の簡易版の検討①【必要性】

・「システム管理基準」適用にあたって、企業規模・特性などに照らして、適切な項目の取捨選択や各項目における対応内容の修正、補完する必要あり。

→中小企業にとって、難易度が高く、適用の道しるべとなる簡易版の検討に着手。

２．中小企業向け「システム管理基準」の簡易版の検討②【検討経緯】

・簡易版作成の検討にあたり、先行研究・文献を調査。
→その中で、IPA「中小企業の情報セキュリティ対策ガイドライン第3版」（以下、IPAガイドライン）に着目。
→「システム管理基準」との比較検討のため、両者の項目の対比表を作成（「別紙1」）。
→また、参考として、「情報セキュリティ管理基準」とIPAガイドラインとの対比表も作成（「別紙2」）。

３．比較対象物の概要：「システム管理基準」（経済産業省）

情報システムの企画、開発、保守、運用等のライフサイクルを管理するためのITマネジメントと、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の策定及び実現に必要となる組織能力であるITガバナンスについて留意すべき基本的事項を体系化・一般化したもの。

３．比較対象物の概要：「中小企業の情報セキュリティ対策ガイドライン」（IPA:独立行政法人情報処理推進機構）

情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき指針と社内において対策を実践する際の手順や手法をまとめたもの。経営者編と実践編から構成されており、個人事業主、小規模事業者をも含む中小企業の利用を想定している。

３．比較対象物の概要：「情報セキュリティ管理基準」（経済産業省）

マネジメント基準と管理策基準として、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項、及び「管理策基準」として、組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を規定したもの。

４．「システム管理基準」とIPAガイドラインの対比結果（該当項目の有無）

- 詳細は、「別紙1」のシステム管理基準とIPAガイドライン対比表をご参照。
- 横軸：「システム管理基準」の項目、縦軸：IPAガイドラインの項目

	ITｶﾞﾊﾞﾅﾝｽ	企画	開発	ｱｼﾞｬｲﾙ開発	運用・利用	保守	外部委託	事業継続	人的管理	ドキュメント
経営者編	△	×	×	×	×	×	×	×	×	×
実践編	△	×	×	×	○	○	○	×	×	×
ｻﾝﾌﾟﾙ規程	△	×	○	×	○	○	○	○	○	×

４．「システム管理基準」とIPAガイドラインの対比結果（評価）

１．「システム管理基準」：ITガバナンス
　　IPAガイドライン：情報セキュリティガバナンス
２．IPAガイドライン：企画、アジャイル開発、ドキュメント無し
３．「システム管理基準」：関連規程（サンプル）無し
　　IPAガイドライン：関連規程（サンプル）有り
４．IPAガイドライン：「システム管理基準」への言及無し
５．両者とも：IoTとAIについては取扱無し

４．「情報セキュリティ管理基準」とIPAガイドラインの対比結果

- **詳細は、「別紙2」の情報セキュリティ管理基準とIPAガイドライン対比表をご参照。**

１．「情報セキュリティ管理基準」：関連規程（サンプル）無し
　　IPAガイドライン：関連規程（サンプル）有り
２．IPAガイドライン：クラウドサービス取扱有り
　　「情報セキュリティ管理基準」：同取扱無し
３．両者とも：IoTとAIについては取扱無し
　⇒IPAガイドラインは「情報セキュリティ管理基準」を
　　ほぼカバーしており、中小企業向けの簡易版と言える。

５．今後の展開と課題①

- IPAガイドラインは、付録の関連規程（サンプル）をはじめ、導入にあたって活用できるツール類が充実。
- 「SECURITY ACTION 自己宣言制度」（「★一つ星」と「★★二つ星」）とIPAのガイドラインをリンクさせて、中小企業にモチベーションを与え、段階的な取組み促進効果を期待。

⇒中小企業向けの「システム管理基準」の簡易版作成の検討にあたって、ぜひ参考としたい！

５．今後の展開と課題②

・「システム管理基準」とIPAガイドラインの対比表で見たように、両者で重なる部分も多く、重複を避けたい。
⇒ツール類の活用、自己宣言制度などを参考としつつも、内容の重複は極力避け、ITガバナンス、企画フェーズ、開発フェーズ等の項目の充実およびIoT、AIなどを取り込んでいくことを検討する。
⇒その他、Q&A方式でまとめる方法も検討する。
・今後、BCP/BCMS関連のシステム監査へ調査・検討する。

６．ITガバナンス自己宣言試行モデル案

	ITガバナンス取組み自己宣言（案）	SECURITY ACTION セキュリティ対策自己宣言
★ 一つ星	ITガバナンスの6つの原則に取組むことを自己宣言	「情報セキュリティ5か条」に取組むことを自己宣言
★ 二つ星	自己診断により自社の状況を把握し、自社のビジネス戦略と情報システム戦略を合致させ、情報システム戦略の方針及び目標を策定する。内容を公表できる場合は、外部に公開	・「5分でできる！情報セキュリティ自社診断」で自社の状況を把握 ・「情報セキュリティ基本方針」を定め、外部に公開
（三つ星 ）	EDMモデル（Evaluate：評価、Direct：指示、Monitor：モニタ）を適用し、情報システム戦略の方針及び目標の実現に取組む	―
（四つ星 ）	PDCAサイクルをまわし、継続的に組織能力を高める	―

7．中小企業向け「システム監査基準」の簡易版の検討状況

・日本システム監査人協会（SAAJ）「システム監査を知るための小冊子（改定2版）」は「システム監査基準」の解説のため4ページを割いている。

→当研究会としては、まず、「システム監査基準」※用の用語定義を検討することとし、用語候補リスト作成。
※現行の「システム監査基準」には用語定義がない。

システム管理基準と中小企業の情報セキュリティ対策ガイドライン（対比表）

2019.5.6

システム管理基準 ／ 中小企業の情報セキュリティ対策ガイドライン	ITガバナンス										企画フェーズ			開発フェーズ									アジャイル開発			運用・利用フェーズ																保守フェーズ							外部サービス管理					事業継続管理					人的資源管理				ドキュメント	
	1 情報システム戦略の方針および目標設定	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	1 プロジェクト計画	2 要件定義	3 調達	1 開発ルール	2 基本設計	3 詳細設計	4 実装	5 システムテスト（総合テスト）	6 ユーザ受入テスト	7 移行	8 プロジェクト管理	9 品質管理	1 アジャイル開発の概要	2 アジャイル開発に関係する人材の役割	3 アジャイル開発のプロセス	1 運用管理ルール	2 運用管理	3 情報セキュリティ管理 3-1 情報セキュリティ管理ルール	3 情報セキュリティ管理 3-2 アクセス管理	4 データ管理	5 ログ管理	6 構成管理 6-1 機器の構成管理	6 構成管理 6-2 ハードウェア管理	6 構成管理 6-3 ネットワーク管理	7 ファシリティ管理	8 サービスレベル管理	9 インシデント管理 9-1 インシデント対応の管理	9 インシデント管理 9-2 問題管理	9 インシデント管理 9-3 変更管理	9 インシデント管理 9-4 リリース管理	10 サービスデスク管理	1 保守ルール	2 保守計画	3 情報セキュリティ管理	4 変更管理	5 保守の実施	6 ソフトウェア構成管理	7 ライフサイクル管理	1 外部サービス利用計画	2 委託先選定	3 契約と管理 3-1 契約	3 契約と管理 3-2 委託先管理	4 サービスレベル管理（SLM）	1 リスクアセスメント	2 事業継続計画	3 システム復旧計画	4 訓練	5 計画の見直し	1 責任と権限	2 業務遂行	3 教育・訓練	4 健康管理	1 ドキュメントの作成	2 ドキュメントの管理
第1部　経営者編																																																																
1. 情報セキュリティ対策を怠ることで企業が被る不利益								△																																																								
(1)金銭の損失																																																																
(2)顧客の喪失																																																																
(3)業務の停滞																																																																
(4)従業員への影響																																																																
2. 経営者が負う責任	△																																																															
(1)経営者などに問われる法的責任																																																																
(2)関係者や社会に対する責任																																																																
3. 経営者は何をやらなければならないのか	△	△	△	△	△	△	△	△	△	△																																																						
(1)認識すべき「3原則」																																																																
(2)実行すべき「重要7項目の取組」																																																																
第2部　実践編																																																																
1. 実践編の進め方																																																																
2. できるところから始める																												○															○																				
(1)情報セキュリティ5か条																																																																
①OSやソフトウェアは常に最新の状態にしよう！																																											○																				
②ウイルス対策ソフトを導入しよう！																																											○																				
③パスワードを強化しよう！																												○																																					
④共有設定を見直そう！																												○																																					
⑤脅威や攻撃の手口を知ろう！																																											○																				
3. 組織的な取り組みを開始する								○																																																								
(1)情報セキュリティ基本方針の作成と周知																																																																
(2)実施状況の把握（自社診断のための25項目）																																																																
(3)対策の決定と周知徹底																																																																
4. 本格的に取り組む																																																																
(1)管理体制の構築																																																																
①責任分担と連絡体制の整備		○																																																														
②緊急時対応体制の整備																																				○																												
(2)IT利活用方針と情報セキュリティの予算化				○	○																																																											
(3)情報セキュリティ規程の作成																											○																																						
(4)委託時の対策																																																	△	△	△	△	△											
(5)点検と改善								○																																																									
5. より強固にするための方策																																																																
(1)情報収集と共有																											○																																						
(2)ウェブサイトの情報セキュリティ																																	○																															
(3)クラウドサービスの情報セキュリティ																																										○		○							○		○												
(4)情報セキュリティサービスの活用																																																	△	△	△	△	△											
(5)技術的対策例と活用																										○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○																						
(6)詳細リスク分析の実施方法								○																																																								
【付録5】情報セキュリティ関連規程（サンプル）																																																																
1. 組織的対策		○						○																																																								
2. 人的対策						○																																																				○	○	○			
3. 情報資産管理						○		○	○																					○			○		○																												
4. アクセス制御及び認証																												○																																					
5. 物理的対策																											○								○																														
6. IT機器利用																											○				○													○			○																	
7. IT基盤運用管理								○																						○	○	○	○																	○														
8. システム開発及び保守														○												○		○														○			○	○																		
9. 委託管理																																																	△	○	○	○	○											
10. 情報セキュリティインシデント対応ならびに事業継続管理										○																										○	△	△	△														○	○	○								
11. 個人番号及び特定個人情報の取り扱い							○	○																																																								

（凡例）○：理解を深めるために参照することが望ましい項目　△：背景情報として参照することが望ましい項目

情報セキュリティ管理基準と中小企業の情報セキュリティ対策ガイドライン（対比表）

2019.5.6

情報セキュリティ管理基準 ／ 中小企業の情報セキュリティ対策ガイドライン	Ⅳ.マネジメント基準					Ⅴ. 管理策基準																																																
	4.4 情報セキュリティマネジメントの確立	4.5 情報セキュリティマネジメントの運用	4.6 情報セキュリティマネジメントの監視及びレビュー	4.7 情報セキュリティマネジメントの維持及び改善	4.8 文書化した情報の管理	5 情報セキュリティのための方針群	5.1 情報セキュリティのための経営陣の方向性	6 情報セキュリティのための組織	6.1 内部組織	6.2 モバイル機器及びテレワーキング	7 人的資源のセキュリティ	7.1 雇用前	7.2 雇用期間中	7.3 雇用の終了又は変更	8 資産の管理	8.1 資産に対する責任	8.2 情報分類	8.3 媒体の取扱い	9 アクセス制御	9.1 アクセス制御に対する業務上の要求事項	9.2 利用者アクセスの管理	9.3 利用者の責任	9.4 システム及びアプリケーションのアクセス制御	10 暗号	10.1 暗号による管理策	11 物理的及び環境的セキュリティ	11.1 セキュリティを保つべき領域	11.2 装置	12 運用のセキュリティ	12.1 運用の手順及び責任	12.2 マルウェアからの保護	12.3 バックアップ	12.4 ログ取得及び監視	12.5 運用ソフトウェアの管理	12.6 技術的ぜい弱性管理	12.7 情報システムの監査に対する考慮事項	13 通信のセキュリティ	13.1 ネットワークセキュリティ管理	13.2 情報の転送	14 システムの取得、開発及び保守	14.1 情報システムのセキュリティ要求事項	14.2 開発及びサポートプロセスにおけるセキュリティ	14.3 試験データ	15 供給者関係	15.1 供給者関係における情報セキュリティ	15.2 供給者のサービス提供の管理	16 情報セキュリティインシデント管理	16.1 情報セキュリティインシデントの管理及びその改善	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	17.1 情報セキュリティ継続	17.2 冗長性	18 順守	18.1 法的及び契約上の要求事項の順守	18.2 情報セキュリティのレビュー
第1部 経営者編																																																						
1. 情報セキュリティ対策を怠ることで企業が被る不利益	○																																																					
(1)金銭の損失																																																						
(2)顧客の喪失																																																						
(3)業務の停滞																																																						
(4)従業員への影響																																																						
2. 経営者が負う責任	○																																																					
(1)経営者などに問われる法的責任																																																						
(2)関係者や社会に対する責任																																																						
3. 経営者は何をやらなければならないのか		○	○	○		○																																																
(1)認識すべき「3原則」																																																						
(2)実行すべき「重要7項目の取組」																																																						
第2部 実践編																																																						
1. 実践編の進め方																																																						
2. できるところから始める																																																						
(1)情報セキュリティ5か条																																																						
①OSやソフトウェアは常に最新の状態にしよう！																																										○												
②ウイルス対策ソフトを導入しよう！																														○																							
③パスワードを強化しよう！																				○	○	○																															
④共有設定を見直そう！																				○	○																																
⑤脅威や攻撃の手口を知ろう！	○																																	○																				
3. 組織的な取り組みを開始する	○																																																					
(1)情報セキュリティ基本方針の作成と周知																																																						
(2)実施状況の把握(自社診断のための25項目)																																																						
(3)対策の決定と周知徹底																																																						
4. 本格的に取り組む																																																						
(1)管理体制の構築																																																						
①責任分担と連絡体制の整備									○																																													
②緊急時対応体制の整備																																														○							
(2)IT利活用方針と情報セキュリティの予算化		○																																																				
(3)情報セキュリティ規程の作成						○																																																
(4)委託時の対策																																												○										
(5)点検と改善			○	○																																																		
5. より強固にするための方策																																																						
(1)情報収集と共有									○																										○																			
(2)ウェブサイトの情報セキュリティ																														○							○																
(3)クラウドサービスの情報セキュリティ																																																						
(4)情報セキュリティサービスの活用																																												△										
(5)技術的対策例と活用															○				○					○		○			○								○			○														
(6)詳細リスク分析の実施方法	○																																																					
【付録5】情報セキュリティ関連規程（サンプル）																																																						
1. 組織的対策			○	○			△		○																																													
2. 人的対策							△					○	○	○																																								
3. 情報資産管理							△									○	○	○														○																						
4. アクセス制御及び認証							△													○	○	○	○																															
5. 物理的対策							△																				○	○																										
6. IT機器利用							△			○												○						○			○								○															
7. IT基盤運用管理							△																					○		○			○	○	○			○			○				○									
8. システム開発及び保守							△																																			○												
9. 委託管理							△																																						○	○								
10. 情報セキュリティインシデント対応ならびに事業継続管理							△																																									○		○				
11. 個人番号及び特定個人情報の取り扱い		○					△																																														△	

（凡例）○：理解を深めるために参照することが望ましい項目　△：背景情報として参照することが望ましい項目