2018.6.8.JSSA大会

システム監査における情報セキュリティ監査の位置づけ

「A　Consideration of Information security audit within Systems Audit」

2018年06月08日

情報セキュリティ合同研究会

システム監査における情報セキュリティ監査の位置づけ

目　　次

1.システム監査基準と情報セキュリティ監査1

＜基準改訂の経緯・経過＞

- 昭和60年（1985年）1月　「システム監査基準」策定
- 平成8年（1996年）1月　「システム監査基準」1996年改訂
  - ・情報化環境の変化への対応
  - ・国際化への対応
  - ・災害対策への対応
- 平成15年（2003年）4月「情報セキュリティ監査制度」の運用開始

- 平成16年（2003年）7月「システム監査基準検討委員会」設置
- 平成16年（2003年）9月システム監査基準WG、システム管理基準WG発足
- 平成16年（2004年）4月～5月システム監査基準（案）及びシステム管理基準（案）に対するパブリックコメント募集
- 平成16年（2004年）10月　「システム監査基準2004年改訂

1.システム監査基準と情報セキュリティ監査2

＜平成16年改訂の背景・ポイント＞

- IT技術の革新への対応
- 事業における情報システムの位置づけの変化への対応
- 社会に対する説明責任の高まりと保証型監査の必要性
- 情報システム管理の標準と監査人の行為規範の峻別
  →情報システム管理の標準としてのシステム管理基準
  →システム監査人の行為規範としてのシステム監査基準
- 情報セキュリティ監査制度との関係整理

1.システム監査基準と情報セキュリティ監査3

＜平成16改訂の方針＞

1. 情報セキュリティ監査基準との整合性を確保する。

　監査論として異なるものではない。原則論としてのシステム監査基準は情報セキュリティ監査基準をベース

2. 基準の構成について

　実施基準は従来のチェックポイント方式ではなく、一般基準、報告基準と同様の記述方式とする。

3. 平成8年版の実施基準をシステム監査基準から切り離し、

　システム管理基準を作成するベースとしている。

4. 平成8年版システム監査基準との継続性

実施基準に監査手順の項目を設け、「システム監査は監査計画に基づき、予備調査、本調査、評価・結論の手順により実施～」とした。

1.システム監査基準と情報セキュリティ監査4

■平成16改訂システム監査基準と情報セキュリティ監査

1．システム監査基準

（前文）

今回の改訂は、昨年4月に創設された情報セキュリティ監査基準との整合性を図り、従来の実施基準の主要部分を抜き出し、システム管理基準として独立させ～

Ⅳ．実施基準

6．情報セキュリティ監査

情報セキュリティ監査については、原則として情報セキュリティ管理基準を活用することが望ましい。

1.システム監査基準と情報セキュリティ監査5

■平成16改訂システム監査基準と情報セキュリティ監査

1．システム管理基準

（前文）

なお、情報セキュリティの確保から監査を実施する場合には、情報セキュリティ監査制度に基づく情報セキュリティ監査を行うことが要請される。一方で、システム管理基準においても情報セキュリティの確保に関連する最小限の項目で体系化しているが、それぞれの項目が挙げられているが、それぞれの項目について、「**情報セキュリティ管理基準**を活用して監査を実施することが望ましい。

2.初期システム監査基準と情報セキュリティ1

＜システム監査基準（1985年）と情報セキュリティ＞

2. 実施基準（チェックリスト方式：～しているか）

■企画業務

1. 計画　2. 調査・分析　3. 開発検討　4. 要員管理

■開発業務

1. 開発手順　2. 要員管理　3. システム設計

4. プログラム設計　5. プログラミング　6. システムテスト

■運用業務

1. オペレーション　2. 入力データの作成及び入力

3. データ及びプログラムの管理　4. ファシリティ管理

5. 出力情報の管理及び活用　6. 要員管理　7. 外部委託

2.初期システム監査基準と情報セキュリティ2

＜システム監査基準（1985年）と情報セキュリティ＞

2. 実施基準（チェックリスト方式：～しているか）

■企画業務

1. 計画（6）計画書には適切なセキュリティ対策が記載されているか。

■開発業務

3. システム設計（3）システム設計書には、セキュリティ確保のための各種コントロールが盛り込まれているか。

4. プログラム設計（3）プログラム仕様の標準化、モジュール化等は、作業量、スケジュール、セキュリティ、保守等の観点から適切か。

■運用業務

7. 外部委託（4）委託先におけるセキュリティ対策及び進捗状況が適切に把握されているか。

○データの漏洩・破壊・改ざん、プライバシーの侵害、不正使用、機密保護、障害対策、誤謬・不正防止、データのインテグリティ

2.初期システム監査基準と情報セキュリティ3

＜システム監査基準（1996年）と情報セキュリティ＞

2．実施基準（チェックリスト方式：～しているか）

■企画業務

1．情報戦略　2．全体計画　3．開発計画

4．システム分析・要求定義

■開発業務

1．開発手順　2．システム設計　3．プログラム設計

4．プログラミング　5．システムテスト　6．移行

■運用業務

1．運用管理　2．入力管理　3．データ管理　4．出力管理

5．ソフトウェア管理　6.ハードウェア管理　7．ネットワーク管理　8．構成管理　9．建物・関連設備管理

2.初期システム監査基準と情報セキュリティ4

＜システム監査基準（1996年）と情報セキュリティ＞

2．実施基準（チェックリスト方式：～しているか）

■保守業務

1．保守手順　2．保守計画　3．保守の実施

4．保守の確認　5．移行　　6．旧システムの廃棄

■共通業務

1．ドキュメント管理　2．進捗管理　3．要員管理

4．外部委託

5．災害対策（リスク分析、災害時対応計画、バックアップ、代替処理・復旧）

2.初期システム監査基準と情報セキュリティ5

＜システム監査基準（1996年）と情報セキュリティ＞

2. 実施基準（チェックリスト方式：～しているか）

■企画業務

2. 全体計画（7）全体計画はセキュリティ対策の方針を明確にしているか。

■運用業務

1. 運用管理(13)情報システムのセキュリティに関する教育及び訓練をユーザに対して実施しているか。

■共通業務

4. 要員管理　3. 教育・訓練(2)教育・訓練のカリキュラムは、技術力の向上、業務知識の習得、情報システムの
セキュリティ確保等から検討しているか。

3.改訂システム監査基準と情報セキュリティ監査１

■システム監査基準

前文（システム監査基準の活用にあたって）

「１」システム監査の意義と目的

「２」システム監査基準の意義と適用上の留意事項

・　また、情報セキュリティ監査制度に基づく監査を実施する場合においては、「情報セキュリティ監査基準」をあわせて参照することが望ましい。

「３」システム監査上の判断尺度

・　特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」を参照することが望ましい。

【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

２．システム監査上の判断尺度を確定する際の客観的な参照基準として、「システム管理基準」及び「情報セキュリティ管理基準」が推奨される。

3.改訂システム監査基準と情報セキュリティ監査2

■システム管理基準

前文（システム管理基準の活用にあたって）

なお、情報セキュリティの確保に焦点をおいて情報システムの監査･管理を実施する場合には、当基準でも情報セキュリティの確保に関連する最小限の項目で体系化しているが、それぞれの項目については、「情報セキュリティ管理基準（平成28年改正版(経済産業省)等を活用して独自の管理基準を策定することが望ましい。

（略）

なお本基準では、「情報セキュリティ管理基準」における要求事項との対応関係の理解を容易にするために、「情報セキュリティ管理基準参照表」を付してある。これを参照して各企業のリスク特性を勘案して独自の管理基準の策定に利用されたい。

3.改訂システム監査基準と情報セキュリティ監査3

■情報セキュリティ管理基準参照表のイメージ（項目限定し筆者作成）

システム管理基準 / 情報セキュリティ監査基準	ITガバナンス	企画フェーズ	開発フェーズ	システムテスト	アジャイル開発	運用・利用フェーズ	インシデント管理	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	ドキュメント管理
Ⅳマネジメント基準												
5. 情報セキュリティのための方針群												
6.情報セキュリティのための組織												
7. 人的資源のセキュリティ					△						○	
略									○			
16. 情報セキュリティインシデント管理							○					
17. 事業継続～情報セキュリティ側面										○		
18. 順守												

3.改訂システム監査基準と情報セキュリティ監査4

■システム管理基準中の中項目中の情報セキュリティ項目

Ⅰ．ITガバナンス

　8．情報セキュリティの評価・指示・モニタ

Ⅴ．運用・利用フェーズ

　1．運用管理ルール　2．運用管理　3．情報セキュリティ管理　4．データ管理

Ⅵ．保守フェーズ

　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

■ Ⅰ．ITガバナンス

8．情報セキュリティの評価・指示・モニタ

(1) 経営陣は、情報セキュリティの現在及び予想される環境変化を考慮し評価すること。

(2) 経営陣は、情報セキュリティの目的及び戦略を明確にして指示すること。

(3) 経営陣は、情報セキュリティ対策の有効性をモニタしていること。

3.改訂システム監査基準と情報セキュリティ監査5

■Ⅴ. 運用・利用フェーズ

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

(1)　運用管理者は、組織の情報セキュリティ方針に基づいて運用の情報セキュリティ管理ルールを作成し、遵守状況を確認すること。

(2) 運用管理者は、サイバー攻撃への対処策を作成し、有効性を保つこと。

(3)　上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3. 2　アクセス管理

(1) 運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。

(2) 運用管理者は、データへのアクセスコントロール及びモニタリングを、実施すること。

(3) 上記以外のアクセス管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3.改訂システム監査基準と情報セキュリティ監査6

■Ⅴ．運用・利用フェーズ

４．データ管理

(12) データ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

５．ログ管理

(3) ログ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

６．構成管理

６．１　機器の構成管理

(6) 機器の構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

６．２　ハードウェアの構成管理

(7) ハードウェア管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3.改訂システム監査基準と情報セキュリティ監査7

■Ⅴ．運用・利用フェーズ

６．３　ネットワークの構成管理

（7）ネットワーク管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

７．ファシィリティ管理

（7）ファシィリティ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

９．インシデント管理

９．１インシデント対応の管理

（7）インシデント管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3.改訂システム監査基準と情報セキュリティ監査8

■Ⅵ. 保守フェーズ

3. 情報セキュリティ管理

(1)　保守管理者は、外部調達に関するぜい弱性情報及び修正コード情報の収集に努めること。

(2)　保守管理者は、収集したぜい弱性情報及び修正コード情報について、自社システム環境への適用の必要性を調査・分析し、適用の是非を決定すること。

(3)　保守管理者は、OSなどの自動適用可能なソフトウェアの修正コードについて、適用方針を決め確実な適用を行うこと。

(4) 保守管理者は、コンピュータウィルス対策ソフトウェア（以下「ウィルス対策ソフト」という）及びパターン定義ファイル（以下「パターンファイル」という）の更新の適用を実施すること。

(5)上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6. ソフトウェア管理

(6)　ソフトウェア構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること

4. システム監査と情報セキュリティ監査１

■システム監査基準と情報セキュリティ

＜第１期：初期システム監査基準と情報セキュリティ＞

・（情報）セキュリティという用語自体使用されていない。

・データの漏洩・破壊・改ざん、プライバシーの侵害、不正使用、機密保護、障害対策、誤謬・不正防止、データのインテグリティ

・災害対策（リスク分析、災害時対応計画、バックアップ、代替処理・復旧）

・情報システム安全対策基準、コンピュータウィルス対策基準

・不正アクセス対策基準

〇システム監査に情報セキュリティ監査が含まれていた時代

（参考）システム監査技術者育成カリキュラム

■第５部システム監査のケーススタディ：

第１章　情報システム運営の監査

（１）組織体制の監査　（２）要員管理の監査　（３）情報化投資の監査

第２章　システムライフサイクルの監査

（１）企画業務の監査　（２）開発業務の監査　（３）運用業務の監査
（４）保守業務の監査

第３章　アプリケーションシステムの監査

（１）アプリケーションシステム監査の考え方
（２）販売情報システム　（３）購買情報システム　（４）生産情報システム
（５）会計情報システム　（６）人事情報システム

第４章　テーマ別監査

（１）セキュリティ監査　　（２）ネットワークシステムの監査
（３）データベースの監査　（４）EUCの監査　（５）アウトソーシングの監査
（６）ソフトウェアパッケージの監査

第５章　総合演習

＊（１）システム監査の導入　＊（２）システム監査の実施

「システム監査技術者育成カリキュラム１９９４」より

４．システム監査と情報セキュリティ監査２

＜第２期：２００３年情報セキュリティ監査制度創設以降＞

・情報セキュリティ監査基準と情報セキュリティ管理基準

・大きいISMS認証の役割

■システム監査と情報セキュリティ監査の特徴など

・監査対象：情報システム、情報セキュリティ監査：情報資産

・システム監査：信頼性、安全性；効率性＋有効性

・システム監査：システムのライフサイクル全般に係る監査
（情報戦略・企画段階含）

・情報セキュリティ監査：安全性・信頼性、機密性、完全性、可用性

・システム監査は助言型、情報セキュリティ監査は保証型中心

・システム監査は民間中心、情報セキュリティ監査は官公庁中心

〇情報セキュリティ監査が大きく普及した時代

４．システム監査と情報セキュリティ監査３

＜第3期：改訂システム監査基準＞

	システム管理基準の構成		情報セキュリティ管理基準：管理策
Ⅰ	ITガバナンス	A5	情報セキュリティ方針群
Ⅱ	企画フェーズ	A6	情報セキュリティのための組織
Ⅲ	開発フェーズ	A7	人的資源のセキュリティ
Ⅳ	アジャイル開発	A8	資産管理
Ⅴ	運用・利用フェーズ	A9	アクセス制御
Ⅵ	保守フェーズ	A10	暗号
Ⅶ	外部サービス管理	A11	物理的及び環境的セキュリティ
Ⅷ	事業継続管理	A12	運用のセキュリティ
Ⅸ	人的資源管理	A13	通信のセキュリティ
Ⅹ	ドキュメント管理	A14	システムの取得、開発及び保守
		A15	供給者関係
		A16	情報セキュリティインシデント管理
		A17	事業継続マネジメント
		A18	遵守

４．システム監査と情報セキュリティ監査４

＜第3期：改訂システム監査基準＞

	システム管理基準の構成		情報セキュリティ管理基準：管理策
Ⅰ１	ITガバナンス：方針・目標	A5	情報セキュリティ方針群
Ⅰ２	ITガバナンス：組織体制	A6	情報セキュリティのための組織
Ⅸ	人的資源管理	A7	人的資源のセキュリティ
Ⅴ６	運用・利用：構成管理	A8	資産管理
Ⅴ３	運用・利用：アクセス管理	A9	アクセス制御
Ⅴ３	運用・利用：アクセス管理	A10	暗号
Ⅴ７	運用・利用：ファシリティ管理	A11	物理的及び環境的セキュリティ
Ⅴ	運用・利用フェーズ	A12	運用のセキュリティ
Ⅴ６	運用・利用：構成管理¥¥	A13	通信のセキュリティ
Ⅹ	開発＆保守フェーズ	A14	システムの取得、開発及び保守
Ⅶ	外部サービス管理	A15	供給者関係
Ⅴ９	運用・利用インシデント管理	A16	情報セキュリティインシデント管理
Ⅷ	事業継続管理	A17	事業継続マネジメント
Ⅰ７	コンプライアンス	A18	遵守

５．まとめと今後の課題

■まとめ

・システム監査基準が初めて制定された1985年当時は、情報セキュリティ監査という用語自体が一般的でなく、システム監査の中に包含されていた。

・2003年に情報セキュリティ監査制度が創設、ISMS認証制度も開始され保証型監査の色彩が強い情報セキュリティ監査は目覚ましく普及した。
・一方、システム監査はITガバナンスとして重要な役割を担うのも事実である。

・改訂システム監査基準の構成をみると、情報セキュリティ管理策と深く係っており、情報セキュリティ監査抜きにシステム監査を語れない時代といえる。

■今後の課題

・中小企業向けた各種情報セキュリティ研究を行ってきており、システム監査基準の中小企業への適用等も含め、研究として深めていきたい。

ご清聴ありがとうございました。

研究会は、さらに情報セキュリティとシステム監査の有効性と効率性を「深堀り」します。研究会への参画をお待ちしております。

情報セキュリティ合同研究会

＜2017年度　研　究　会　参　加　メ　ン　バ　ー　（敬称略）＞
川辺 良和　【㈲インターギデオン】：主査、発表者
植野 俊雄　【ISU】
芳仲　宏　　【システム監査技術者】
長野 加代子【㈱ピーアンドアイ】
田中良治　　【システム監査技術者】