報道各位

2017 年 11 月 27 日
株式会社インプレスR&D
https://nextpublishing.jp/

基礎実務と実務がこの一冊でわかる

『改訂三版 情報セキュリティ内部監査の教科書』発行

特定非営利活動法人日本セキュリティ監査協会編

インプレスグループで電子出版事業を手がける株式会社インプレス R&D は、『改訂三版 情報セキュリティ内部監査の教科書』(編者:特定非営利活動法人日本セキュリティ監査協会)を発行いたしました。

『改訂三版 情報セキュリティ内部監査の教科書』
https://nextpublishing.jp/isbn/9784844398042

編者:特定非営利活動法人日本セキュリティ監査協会
小売希望価格:電子書籍版 3,200 円(税別)／印刷書籍版 4,600 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5 判／モノクロ／本文 162 ページ
ISBN:978-4-8443-9804-2
発行:インプレス R&D

＜＜発行主旨・内容紹介＞＞

本書は適切な情報セキュリティ内部監査を行うための知識を体系化した教科書です。情報セキュリティ監査に初めて従事する人でも、その基本的な考え方から、実務までが、この一冊でわかります。

2013 年 2 月に初版を発行し、その後、JIS Q 27000 シリーズなどの改定に対応、今回で改訂三版を迎えました。情報セキュリティ内部監査人(*)の認定制度に則った内容で、その能力認定組織である特定非営利活動法人日本セキュリティ監査協会(JASA)が執筆・編集しています。

(*)情報セキュリティ内部監査人とは、「組織の情報セキュリティマネジメントが、これに対し責任を負う経営者の期待する水準に達しているかを、組織内において独立した立場から評価し、経営者に意見を述べる者」と定義されています。

(本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。)

第 1 章「情報セキュリティ監査の基礎知識」より

1.1　情報セキュリティ監査について

情報セキュリティ監査の内容に入る前に、情報セキュリティ監査とその制度について概観することにしよう。

1.1.1　情報セキュリティの内部監査の位置づけ

情報セキュリティ監査は「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えるあるいは助言を行う活動」(「情報セキュリティ監査研究会 報告書」、経済産業省、2003年3月）と定義されている。この定義にしたがえば、情報セキュリティ監査は、情報セキュリティマネジメントに関し、独立した監査人が評価または検証し、意見を述べるものである。

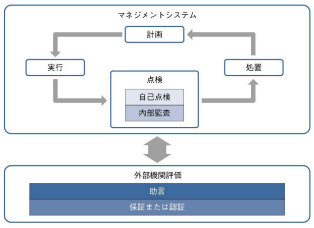
情報セキュリティマネジメントに関する評価は、【図表1-1】に示すとおり、情報セキュリティマネジメントシステムにおいて、企業・組織自らが計画・実行・点検・処置（PDCAサイクル）として行う一連の過程のうちの、点検にあたる活動の一つである。この評価活動は、後述するとおり、情報セキュリティマネジメントに関して何らかの役割を担う人々自身が行う評価活動である自己点検と、独立した立場の人が評価を行う内部監査がある。本書は、このうちの内部監査を主題としている。

なお、情報セキュリティ監査については、企業・組織が外部に対して「適切な情報セキュリティマネジメントを行っている旨の主張」を行い、それを外部の専門機関が評価する外部監査もある。

【図表1-2】は、情報セキュリティ監査制度の設計にあたって経済産業省が組織した、情報セキュリティ監査研究会での結論を要約したものである。この図に示すとおり、制度設計の基本的な視点は以下の4点である。このうち③に示す多様性が情報セキュリティ監査制度の特徴の一つとなっている。

①システムではなく情報資産を対象とした監査
②情報資産に対するマネジメントを監査
③多種多様な組織体の多種多様なニーズに応じた監査制度
④インターネット社会における国際的整合性

【図表1-1】情報セキュリティマネジメント評価の枠組み



また、公正かつ公平な監査を目指す監査市場の適正な発展のための規律として、「情報セキュリティ監査に関する標準的な基準」と「情報セキュリティ監査を行う主体のあり方についての制度」の2点を整備する必要性が指摘されている。

この指摘を受けて、情報セキュリティマネジメントを評価する尺度として「情報セキュリティ管理基準」が、また、独立した監査人が質の高い監査を行うための行為規範として「情報セキュリティ監査基準」、および、情報セキュリティ監査を行う主体の質の確保のための「情報セキュリティ監査企業台帳」が経済産業省から告示されている。

※情報セキュリティ監査制度：平成15年に経済産業省が創設した制度で、情報セキュリティ監査企業台帳（平成15年経済産業省告示113号）、情報セキュリティ監査基準（平成15年経済産業省告示114号）、情報セキュリティ管理基準（平成28年経済産業省告示第37号）、で構成される。

さらに、「情報セキュリティ監査従事者の質の確保についての制度」と「監査を行う主体となる企業の質の確保についての制度」に関しては、特定非営利活動法人日本セキュリティ監査協会（以降、「JASA」と称する）を設立し、情報セキュリティ監査人資格制度および審査制度を設け、運用することにより対応している。

情報セキュリティ監査制度で告示された基準のうち情報セキュリティ管理基準は、監査を行う者（以降、「監査主体」と称する）が監査対象を評価する際の尺度となるものである。また、この基準に則して情報セキュリティマネジメントを行うことにより、監査を受ける者（以降、「被監査主体」と称する）が、監査主体と共通の尺度でリスクを管理することができる。すなわち、情報セキュリティ管理基準は、被監査主体が情報セキュリティマネジメントを設計・実装・運用を行う際の指針として用いるようにも策定されている。このように、情報セキュリティ管理基準は監査主体と被監査主体の価値基準の橋渡しをする役割を担う。

第 3 章「情報セキュリティ内部監査の実施手順」より

【図表3-4-4】監査実施計画書の例（続き3）

【別紙1：主な監査項目】

監査対象領域	主な監査事項	対象となる部署
①セキュリティ基本方針	・情報セキュリティ基本方針の最新確度状況 ・情報セキュリティ基本方針のレビュー状況	⇒情報システム部 ⇒情報システム部
②情報セキュリティのための組織	・情報セキュリティ委員会の運営 ・新しい情報処理設備の管理責任の承認 ・秘密保持契約のレビュー ・外部からのアクセスに対する管理策の実施	⇒情報システム部 ⇒経営企画室 ⇒総務部 ⇒資機材部署
③資産の管理	・重要な資産の目録化 ・資産目録の適正性（管理責任者、利用範囲、分類、安全対策）	⇒全部署 ⇒全部署
④人的資源のセキュリティ	・雇用契約内容の妥当性 ・採用時および継続的な教育訓練 ・セキュリティ違反者への徹底 ・雇用終了時の手続	⇒人事部 ⇒人事部、全部署 ⇒人事部 ⇒全部署
⑤物理的および環境的セキュリティ	・セキュリティエリアの管理 ・サーバ、PC、外部記録媒体の安全対策	⇒全部署 ⇒全部署
⑥通信および運用管理	・運用マニュアルと操作マニュアルの整備 ・外部委託業務におけるセキュリティ対策 ・メール利用時の推奨のあるコードからの保護 ・バックアップの適正性 ・アクセスログの記録	⇒全部署 ⇒総務部、該当部署 ⇒情報システム部、全部署 ⇒情報システム部、全部署 ⇒情報システム部、全部署
⑦アクセス制御	・アクセス制御方針 ・利用者アクセスの管理 ・特権管理 ・利用者の責任（パスワード変更）の通知 ・クリアデスク、クリアスクリーン ・遠隔利用者からのアクセスの管理	⇒情報システム部、全部署 ⇒情報システム部、全部署 ⇒情報システム部、全部署 ⇒情報システム部、全部署 ⇒情報システム部、全部署 ⇒情報システム部、当部署
⑧情報システムの調達、開発および保守	・入力データの妥当性チェック方法 ・重要のある入力データのチェック方法 ・出力データの妥当性チェック方法 ・システムファイルのセキュリティ ・運用データをテストに用いる際の安全対策 ・外部委託したソフトウェアの稼度 ・技術的脆弱性の管理	⇒情報システム部、該当部署 ⇒情報システム部、該当部署 ⇒情報システム部、該当部署 ⇒情報システム部、該当部署 ⇒情報システム部、該当部署 ⇒情報システム部、該当部署 ⇒情報システム部、該当部署
⑨情報セキュリティインシデントの管理	・情報セキュリティインシデントの報告方法 ・情報セキュリティインシデントの管理	⇒情報システム部、全部署 ⇒情報システム部、全部署
⑩事業継続管理	・組織の事業継続に必要な情報セキュリティの管理 ・事業継続計画の最新化	⇒情報システム部、全部署 ⇒情報システム部、全部署
⑪コンプライアンス	・順守すべき法令の把握 ・重要な記録の保護 ・監査ツールの保護	⇒総務部 ⇒総務部、全部署 ⇒該当部署

3.5.2　監査技法

監査技法とは、監査人が必要かつ十分な監査証拠を入手するための手段・方法である。監査技法は、大きく次の4つに分類される。

①質問（インタビュー／ヒアリング）：人が対象
②閲覧（レビュー）：文書や記録が対象
③観察（サイトレビュー）：人、もしくは施設や設備が対象
④再実施（実施確認テスト）：施設や設備が対象

個々の監査技法の内容は2.6.3項「監査技法」に示すとおりである。

これらの監査技法は相互に補完関係にあり、ある技法での監査結果を別の技法で補強することもあれば、ある技法での監査結果を別の技法で検証することもある。例えば、あるシステムの運用状況を監査する場合には、

・運用手順書を閲覧する
・運用状況を観察する
・オペレータに対して運用手順書の内容について質問する

というように監査技法を組み合わせることで、証拠能力を高め、より精度の高い監査を実現することが可能になる。

被監査主体に対してどの監査技法を適用するかについては、被監査主体の負荷と、情報セキュリティ内部監査人がどの程度まで十分な監査証拠を取得するかのバランスを考慮した上で、それぞれの技法の重み付けを考えるとよい。すべての項目に対して再実施を行うことは現実的ではないし、すべての項目をヒアリングだけで済ませるのでは十分な監査証拠を取得することはできない。

●精査と試査について
抽出（サンプリング）が必要な場合、精査と試査のいずれで実施するかを検討する必要があるが、内部監査では試査にとどまるケースが多い。

3.5.3　監査手続書と監査チェックリスト

（1）監査手続書の作成

監査手続書とは、組織内で定めた内部監査手順書および個別管理基準に従い、詳しい監査の実施方法を記述したものである。

個別管理基準とは、社内規程や運用手順書など、組織が定めるコントロールに基づき、情報セキュリティ管理基準を参考として定める組織独自の管理基準を指す。この個別管理基準を基に、監査を効率的に実施するために必要な事項を追加した監査手続書を作成すると品質の高い監査を行うことができる。

監査手続書の作成にあたっては、経済産業省の「情報セキュリティ監査手続ガイドライン」を参考にするとよい。情報セキュリティ監査手続ガイドラインでは、情報セキュリティ管理基準の詳細管理策ごとに、監査対象（文書、記録類、システムなど）とどの監査技法を選択すべきかについての指針が定められている。ただし、情報セキュリティ監査手続ガイドラインで定められている監査対象は一般的な名称であるため、実際の監査手続書の作成にあたっては実際に組織内で用いられている名称に適宜置き換える必要がある。また、社内規程や運用手順書など、組織が定めるコントロールは必ずしも情報セキュリティ管理基準と同じではないので、情報セキュリティ監査手続ガイドラインの中から組織のコントロールと内容の似ている管理策や詳細管理策を探し、その監査手続を参考として組織のコントロールに適合した監査手続を策定する必要がある。

監査手続書には、監査を実施するにあたっての監査要点と、実施すべき手続の関係を記載す

＜＜目次＞＞

＜＜編者紹介＞＞

特定非営利活動法人日本セキュリティ監査協会（JASA）

2003 年に経済産業省が創設した「情報セキュリティ監査制度」を運営するために、同年 10 月に設立された NPO 法人。会長土居範久慶応大学名誉教授。会員数 67 社（正会員、2017 年 11 月 7 日現在）。情報セキュリティ監査制度の普及促進のために、監査品質の維持・向上を目的とした、情報セキュリティ監査人の育成・資格の付与、監査に関わる指針やガイドなどの発行、セミナー等を通じた一般への啓発活動を行っている。http://www.jasa.jp/

＜＜販売ストア＞＞

電子書籍:

Amazon Kindle ストア、楽天 kobo イーブックストア、Apple iBookstore、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER

印刷書籍:

Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス

※　各ストアでの販売は準備が整いしだい開始されます。

※　全国の一般書店からもご注文いただけます。

【株式会社インプレス R&D】 https://nextpublishing.jp/

株式会社インプレス R&D （本社：東京都千代田区、代表取締役社長：井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。

※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 https://www.impressholdings.com/

株式会社インプレスホールディングス(本社：東京都千代田区、代表取締役：唐島夏生、証券コード：東証1部9479)を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「モバイルサービス」を主要テーマに専門性の高いコンテンツ＋サービスを提供するメディア事業を展開しています。2017 年 4 月 1 日に創設 25 周年を迎えました。

【お問い合わせ先】

株式会社インプレス R&D NextPublishing センター

〒101-0051　東京都千代田区神田神保町 1-105

TEL 03-6837-4820

電子メール: np-info@impress.co.jp