

# 「情報セキュリティ監査における 監査手続きガイド」の紹介

監査手続作成プロジェクトの概要は、Security Eye Vol.5に経過報告として紹介されています。プロジェクトの背景と狙いについては、情報セキュリティ管理基準をJIS Q 27001附属書Aの内容とすることにより、その記述レベルと監査の現場で必要とされる記述レベルには大きな隔たりが生じ、そのギャップを橋渡しする実務的な指針の必要性が認識されたことによります。ここではプロジェクトの成果物である「情報セキュリティ監査における監査手続きガイド」（以下本文中では、手続きガイド）とその利用法について解説した「『情報セキュリティ監査における監査手続きガイド』利用の手引」（以下本文中では、利用の手引）について紹介します。

## 情報セキュリティ監査における 監査手続きガイド

手続きガイドは、「監査／検証手続き」と「監査／検証手続き（技術編）」の2編からなる文書です。監査人による利用だけでなく被監査主体での活用を考慮して、名称を「監査／検証手続き」としています。

2007年1月末の情報セキュリティ監査シンポジウムでの経過報告の際には、これらは1つにまとめられていたが、その後監査の現場での使い勝手を考慮し分離することになりました。「監査／検証手続き」のみを用いて広く浅く監査（あるいは検証）を行ったり、技術編も併用して部分的に深掘した監査（あるいは検証）を行うといった使い分けを想定しています。

双方とも、ある管理策を監査／検証する場合に、どういうところがポイントであり、どういった対象をどのような手続きで監査／検証すればよいのかについて、できるだけイメージが沸きやすいよう具体的な記述を心掛けて書かれています。

「監査／検証手続き」はJIS Q 27001附属書Aの133個の管理策を対象として、1つの管理策につき1個あるいは数個の手続きの方法を提示しています。一方、技術編はJIS Q 27001附属書Aのうち主に技術的な管理策が中心となる10章から12章に焦点を当て、57の管理策を対象として、多くの場合複数個の監査手続きを提示しています。「監査／検証手続き」と「監査／検証手続き（技術編）」の双方とも、この通りに監査を行うべきであるという位置づ

けのものではなく、監査や検証の目的によって柔軟にカスタマイズして利用されるべきものであり、管理策単位、あるいは監査／検証ポイントの単位で一部を採択したり、逆に新たな監査／検証手続きを加えることもできます。例えば、手続きガイドでは監査／検証手続きとして「閲覧」しか記載されていない場合でも、監査人は状況を鑑みて「観察」による手続きを加えたり、また、「閲覧」の対象を、手続きガイドに記載されているものに他の閲覧対象を加えたり、入れ替えることができます。ただし、多くの組織がJIS Q 27001及び27002を参考に情報セキュリティマネジメントを実施していることを考えれば、多くの場合、本手続きガイドの中に参考となる監査項目の記述が見つかるでしょう。

## 手続きガイドの活用方法

手続きガイドは、監査手続きを示したものですが、利用方法としてはそれだけに留まらず、被監査主体（監査依頼者）と監査人との間の合意形成を行うためのコミュニケーションツールとしての利用や、情報セキュリティマネジメントシステム構築の際あるいは高度化を行う際の参考としての利用も考えられます。

被監査主体（監査依頼者）との間の合意形成ツールとして利用する際は、例えば実際の監査の際にどういった監査対象をどういった手続きで行うのかを明確にして、監査にかかる工数や期間の算定の根拠を提示するような使い方が考えられます。

また、情報セキュリティマネジメントシステムの構築の際には、監査対象を明確にすることによって、情報セキュリティマネジメントが正しく実施されていることを証明するためには何が必要なのかを予め認識するのに利用することもできます。

他方、既に情報セキュリティマネジメントを運用している組織では、特に技術編において1つの管理策を細分化するなどして、管理策の導入の優先度を示しており、これらの項目をどこまでやるのかの目安とすることで、情報セキュリティマネジメントの高度化に向けての長期計画を策定するといった使い方も可能になっています。

### 「情報セキュリティ監査における監査手続きガイド」利用の手引

手続きガイドは表形式の文書であり、利用の仕方については利用者に委ねられています。利用の手引は、手続きガイドを適切にまた有効に使うために、各欄の意味や留意事項について簡潔に記した解説文書です。前述の監査手続き

の定義以外の使い方についても、より詳しく書かれていますので、手続きガイドを利用する際には一読することをお勧めします。

情報セキュリティ監査は、内部統制の再構築や相次ぐ情報セキュリティ事故の発生などの背景により、今後ますます重要性を増すものと考えられます。本プロジェクトの成果である手続きガイドおよび利用の手引が、今後の有効かつ効果的な監査への一助として広く活用されることを期待します。

#### 執筆者 プロフィール

#### 菅谷 光啓

NRIセキュアテクノロジーズ株式会社 取締役兼コンサルティング事業部長  
 JASA技術部WG2 リーダー、監査手続作成プロジェクト子亀タスクリーダー  
 1991年(株)野村総合研究所入社。1995年頃より情報セキュリティ関連事業に参加。2000年、NRIセキュアテクノロジーズ(株)発足と同時に出向。現在、情報セキュリティに関わるコンサルテーション、情報セキュリティ監査、診断、調査サービスを担当。工学博士、公認情報セキュリティ監査人(CAIS)、公認情報システム監査人(CISA)、CISSP。



JIS Q 27001 Annex A 要項事項No.	項目	監査/検証ポイント	主たる監査/検証対象	監査/検証手続	技術検証手続	備考
A.5	セキュリティ基本方針					
A.5.1	情報セキュリティ基本方針					
A.5.1.1	情報セキュリティ基本方針文書	情報セキュリティ基本方針文書が経営陣によって承認されているか	情報セキュリティ基本文書	【閲覧】 情報セキュリティ基本文書を閲覧し、経営陣によって承認されていることを確認する	/	
	情報セキュリティ基本方針のレビュー	情報セキュリティ基本文書が全従業員及び関連する外部関係者に公表し、通知されているか	社内外への通達 ホームページ	【閲覧】 社内外への通達、ホームページを閲覧し、情報セキュリティ基本文書の内容が何らかの方法で全従業員および関連する外部関係者に公表、通知されているかを確認する	/	
A.5.1.2	情報セキュリティ基本方針のレビュー	情報セキュリティ基本方針があらかじめ定められた間隔又は重大な変化が発生した場合に引き継ぎ適切、妥当及び有効であることを確実にするためにレビューされているか	経営会議資料	【閲覧】 経営会議資料などを閲覧し、情報セキュリティ基本方針が定期的もしくは重大な変化が発生した場合に妥当性及び有効性が判断されたかを確認する	/	
A.6	情報セキュリティのための組織					
A.6.1	内部組織					
A.6.1.1	情報セキュリティに対する経営陣の責任	経営陣が情報セキュリティの責任に関する明らかな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通じて、組織内におけるセキュリティを積極的に支持しているか	経営会議資料 情報セキュリティ基本方針文書 情報セキュリティ関連規定 職務権限規定	【閲覧】 経営会議資料、情報セキュリティ基本方針文書、情報セキュリティ関連規定、職務権限規定等を閲覧し、経営陣の情報セキュリティにおける責任について明確になっているかを確認する	/	
A.6.1.2	情報セキュリティの調整	情報セキュリティ活動を、組織の中の関連する役割及び職務機能をもつさまざまな部署が連携して調整しているか	情報セキュリティに関連する社内委員会の資料	【閲覧】 情報セキュリティに関連する社内委員会の資料などを閲覧し、情報セキュリティ活動が組織における様々な部署の連携によって調整されているかを確認する	/	

●図1 監査手続きガイド「監査/検証手続き」(抜粋)

10.1	運用の手順及び責任					
10.1.2	変更管理					
	監査/検証ポイント	主たる対象機器	監査/検証手続き	優先度	備考	JIS Q 27002との関係
1	ネットワーク経由で運用システムの設定を変更する場合、その操作ログが取得されているか	運用システム内のコンピュータ、通信機器	【観察】 ◎変更作業の記録と、取得ログの内容を突き合わせて確認する。	○		+
2	ネットワークを経由せず、直接運用システムの設定を変更する場合、その操作ログが取得されているか	運用システム内のコンピュータ、通信機器	【観察】 ◎変更作業の記録と、取得ログの内容を突き合わせて確認する。	○		+
10.1.4	開発施設、試験施設及び運用施設					
	監査/検証ポイント	主たる対象機器	監査/検証手続き	優先度	備考	JIS Q 27002との関係
1	開発ソフトウェアおよび運用ソフトウェアは、異なるシステムまたはコンピュータ上で、ならびに異なる領域またはディレクトリで実行しているか	開発用システム、運用システム	【観察】 ◎開発施設および試験施設および運用施設に訪問し、実行環境が分離されていることを確認する。	◎		○
2	コンパイラ、エディタ及びその他の開発ツール又はシステムユーティリティは、必要でない場合には、運用システムからアクセスできないか	開発用システム、運用システム	【再実施】 ◎運用システムから開発ツールの起動を試み実行できないことを確認する。	○		○
3	試験システム環境は、運用システム環境と可能な限り同等にしているか	試験システム	【閲覧】 ◎システム構成図等により確認する。	○		○
4	運用システム及び試験システムに対して、異なるユーザプロファイルを用いているか	運用システム、試験システム	【観察】 ◎試験システムと運用システムのユーザプロファイルを比較し、確認する。	○	ユーザプロファイルとは、ユーザID等を指す。	○
5	試験システムのメニューには、誤操作によるリスクを低減するために適切な識別メッセージを表示しているか	試験システム	【観察】 ◎試験システムと運用システムのメニューの表示メッセージを比較し、確認する。	○		○

●図2 監査手続きガイド「監査/検証手続き(技術編)」(抜粋)