情報セキュリティ監査の概要と実施法

Outline and Method of Information Security Audit

田上岳夫*
Takeo Tagami

要　旨

情報セキュリティが，情報や情報システムを守ることから，組織の信用・信頼を守ることに価値観が変化しつつある今，組織の情報セキュリティ対策を第三者の専門家が客観的に評価する「情報セキュリティ監査」に大きな期待が寄せられています。

本稿では，情報セキュリティ監査の概要と監査の実施法について説明します。

Nowadays information security is regarded as a function of protecting credit and trust of an organization, rather than protecting information and information system. Therefore “Information Security Audit” is considered with great anticipation, in which the experts on the outside evaluate information security objectively.

This paper gives an outline of Information Security Audit and the way an audit is practiced.

1．まえがき

最近の情報セキュリティに関する事件・事故を分析すると，製品は導入されているが適切に運用されていなかった，ルールは策定されていたが遵守されていなかったなど，導入や策定を行っていながら運用されていないために起きてしまったケースが数多く見受けられます。その背景として，実際の運用や業務への影響を深く検討せずに導入したため運用に耐えられないものとなってしまったり，導入や策定まで行って安心してしまい，その後の運用が疎かになってしまったりといったマネジメント上の課題が見えてきます。

このような事態に陥らないためには，組織の情報セキュリティ対策についてPDCAサイクル（Plan：計画，Do：実行，Check：評価，Act：是正）を確立し，維持することが重要になります。実施状況を評価し，見直しを行うプロセスは，PDCAサイクルを回すために特に重要であり，その実施において第三者の専門家が客観的に評価する「情報セキュリティ監査」の必要性が高まっています。

さらに，情報セキュリティが，情報や情報システムを守ることから，組織の信用・信頼を守ることへ価値観が変化するにつれて，情報セキュリティ監査は，ステークホルダー（利害関係者）に自らの対策をアピールするための仕組みとして積極的に利用されるようになると思われます。

2．情報セキュリティ監査の概要

2.1　PDCAサイクルにおける監査

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のPDCAサイクルにおいて評価（Check）に該当し，その結果は是正（Act）を行う際の貴重なインプットとなります（**図1**）。

具体的には，情報セキュリティポリシーを始めとするルールや対策が組織内に徹底され，遵守されているかを評価するための監査とルールや対策そのものの妥当性を評価するための監査があります。情報セキュリティ監査の実施により，改善点の把握のほか，監査による牽制効果などが期待できます。

2.2　内部監査と外部監査

情報セキュリティ監査は，監査という言葉から監査法人による監査を想像しがちですが，会計監査のように法的に定められたものではありません。第三者としての独立性が確保されていれば，組織内の監査部門や外部のシステムベ

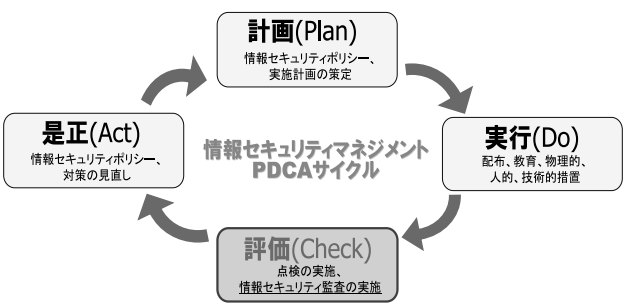

図1　PDCAサイクルにおける監査
Fig.1　Audit in PDCA cycle.

＊ IT基盤システム開発事業部
IT Platform Systems Development Division

ンダ，コンサルティング会社などでも監査を実施できます。監査主体（監査を行う者）は，監査の目的に応じて適切に選択する必要があります（**図2**）。

現状では，組織のセキュリティ成熟度が一般的にまだ高くないこともあり，保証型の監査はISMS適合性評価制度などの公的な制度以外にあまり行われておらず，外部監査であっても助言型の監査が多く行われています（**図3**）。

内部監査と外部監査は，前述のとおり監査の目的によって使い分けが必要になりますが，次のような観点からも外部監査を行うことが考えられます。

まず，内部監査人の育成が不十分な場合や監査対象のセキュリティ成熟度が高く内部監査人のスキルでは十分な監査が実施できない場合です。この場合は，内部監査人の育成を検討しつつ，当初は外部監査を行うことになります。また，侵入テストなどの技術的専門性が求められる監査を行う場合にも，内部監査人では対応が困難であり，外部監査の活用が考えられます。

さらに，組織内の実施状況のチェックを外部監査という，いわば外圧を利用してスムーズに実施するといった場合もあります。

ただ内部監査の実施により，監査対象だけでなく，内部監査人もセキュリティ意識が向上するという副次的な効果も大きいことを認識し，外部の専門家に頼るだけでなく，内部監査を積極的に行うことも重要です。

目的 ／ 監査主体	外部目的（外部に対して当該監査結果を示すことに利用する場合）	内部目的（情報セキュリティポリシーの実施状況を確認する場合）
組織内の者（内部監査）		**助言型監査**（情報セキュリティマネジメントの改善を目的として情報セキュリティ上の問題点を検出し、改善提言を行う監査）
外部の専門家（外部監査）	**保証型監査**（監査対象の情報セキュリティマネジメントが監査を実施した限りにおいて適切である旨を伝達する監査）	

図2　内部監査と外部監査の比較
Fig.2　Comparison between inside audit and outside audit.

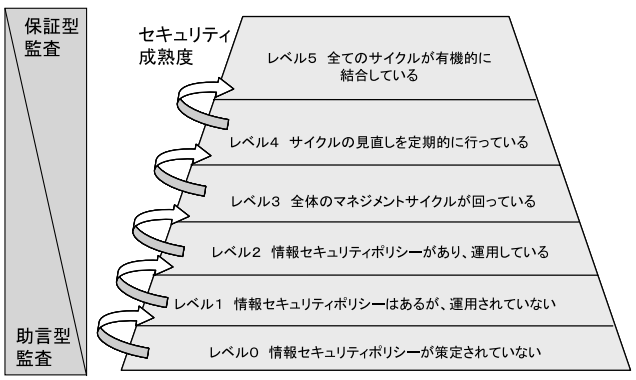

図3　セキュリティ成熟度と監査の関係
Fig.3　Connection between maturity of security and audit.

2.3　内部統制と情報セキュリティ監査の関係

米国トレッドウェイ委員会組織委員会（Committee of Sponsoring Organization of the Tredway Commission：COSO）のレポートによれば，内部統制は，企業活動の有効性と効率性，財務諸表の信頼性，社会規範・法規の遵守性を確保するための組織における統制の枠組みであり，①統制環境，②リスク評価，③統制活動，④情報と伝達，⑤監視活動の5つの要素から構成されています。

情報セキュリティマネジメントは，組織の情報セキュリティを確保するための統制の枠組み（内部統制）ととらえることができ，内部監査は内部統制における監視活動に該当します。また，外部監査では，内部監査の実施状況の監査も含め，内部統制そのものが適切かどうかについても監査することになります。

3．情報セキュリティ監査の実施方法

3.1　情報セキュリティ監査の全体像

情報セキュリティ監査の導入に当たっては，監査の枠組み導入や実施に関する手順である「情報セキュリティ監査実施手順」を策定した上で，中期計画や年度計画を立て，それらの計画に基づき個別の監査を実施します（**図4**）。

中期計画や年度計画策定段階では，監査の目的を決めるとともに，目的に合わせて内部監査にするか外部監査にするか決定し，個別の監査実施の準備を行うようにします。多数の情報システムや部門がある場合は，重要な情報システムや部門から監査を行うこともできます。

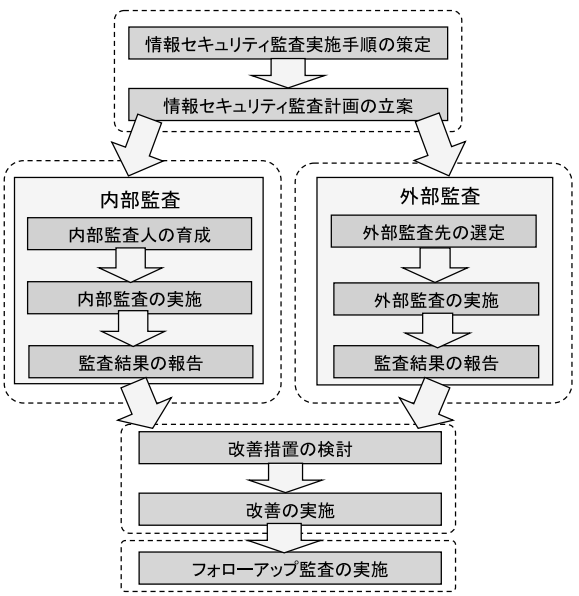

図4　情報セキュリティ監査の全体像
Fig.4　Outline of information security audit.

3.2 情報セキュリティ監査実施手順の策定

組織の情報セキュリティに関する基本的な方針や対策の基準を規定した情報セキュリティポリシーには，情報セキュリティ監査の実施について明記するものの，具体的な実施方法までは規定しません。組織における情報セキュリティ監査の枠組みや実施方法については，前述の情報セキュリティ監査実施手順で規定します。個別の監査を実施する前に，組織としての情報セキュリティ監査の枠組みについて十分に検討します。

以下，情報セキュリティ監査実施手順の目次例を**図5**に示し，その内容について，章ごとにまとめます。

第3章でまず，監査の基本的な考え方をまとめます。具体的には，監査の対象（例：組織内の情報資産を対象とするなど），監査の実施内容（例：情報セキュリティ対策の実施状況を監査するなど），監査の原則（例：監査人の独立性，客観性（証拠に基づく監査）および公平性（公正かつ公平な態度）を確保するなど）について明確化します。

第4章では，監査の実施体制について規定します。情報セキュリティ監査に関する実施体制が確立していない場合は，情報セキュリティ監査に関する責任者を明確にするとともに，監査の推進において核となる部門を決めます。具体的には，経営監査を行う部門など，監査対象から独立性を確保できる部門が望ましいといえます。

第5，6章では，監査人の選任について規定します。内部監査人については，選任の基準や任期，独立性などについて定めるとともに，内部監査人の教育についても触れるようにします。外部監査人については，資格要件や独立性について明確にします。また，チームを編成して監査を実施することについても規定します。

第7章では，監査計画の策定について規定します。具体的には，中期計画，年度計画や個別の監査実施計画の内容や監査の基準の策定方法などについて規定します。

第8～10章では，監査の実施方法について規定します。調査のやり方や報告書のまとめ方，改善内容の通知方法について規定します。

第11，12章では，監査における留意事項として，監査結果や監査調書などの保管期間や管理方法，監査結果の公開方法，監査ツールの保護について明記するとともに，実施手順自体の見直しについても触れるようにします。

図5 情報セキュリティ監査実施手順の目次例
Fig.5 Example contents of procedure for information security audit.

3.3 監査の実施

情報セキュリティ監査実施手順に従って策定した年度計画などに基づき，個別の監査を実施します。

監査の実施に当たっては，まず，監査実施計画を立てます。監査実施計画には，監査対象，監査目的と範囲，監査方法，監査の基準，監査の実施時期と実施場所，監査実施体制と監査人名，監査にかかわる留意事項などをまとめるようにします。監査範囲は，監査目的や内容，監査対象の重要度に応じて情報システム，業務，部門などの単位で選定するようにします。

なお，監査の基準としては，経済産業省の情報セキュリティ監査制度の情報セキュリティ管理基準（JIS X 5080:2002をもとに作成）がありますが，あくまでベストプラクティスとしての基準であり，最新技術や実運用との乖離が見られるとともに分かりにくい表現が多く，そのまま監査項目として適用することはお勧めできません。情報セキュリティ管理基準をベースにしながら，組織の情報セキュリティポリシーなどの基準や規程，実施手順などを参照し，監査の目的や内容に合致した監査の基準を作成するようにします。

次に，監査実施計画に基づき監査を行います。具体的な進め方について以下にまとめます。

（1）監査実施計画の説明

特に監査日程や業務への影響などについて監査対象に説明し，合意を得るようにします。

（2）文書調査

現地調査に入る前に，関連文書について調査します。

（3）現地調査

インタビューの実施や記録の確認などにより，定められ

たルールどおりに業務が行われているかどうかを調査します。調査では，常に証拠を入手するように心がけます。また，すべてを監査するのは不可能であり，全体のなかから効果的なサンプルを選択すること（サンプリング）が求められます。

(4) 技術的検証

システム上の設定が適切に行われているか，システム上のぜい弱性はないかなどについて検証を行います。

(5) 監査意見の調整

調査結果から得られた監査人の意見をまとめ，改善提言などをまとめます。

(6) 監査報告書の作成および提出

監査人は，監査報告書をまとめ，監査に関する責任者に提出します。監査に関する責任者は，その内容を取りまとめ，組織のトップに報告します。

(7) 監査結果の通知

監査に関する責任者は，監査対象に監査結果（改善提言を含む）を通知します。この際，報告会を開催するなど，監査結果が正しく伝わるようにします。

(8) 改　善

監査対象は，改善提言について検討した上で，改善計画を立案し，監査に関する責任者に報告します。監査人は，必要に応じて改善結果について監査（フォローアップ監査）を実施します。

4．情報セキュリティ監査実施上のポイント

4.1　監査テーマの選定

ある程度テーマを絞った上で深く監査することにより，監査人の専門性を生かすことができます。監査のテーマとしては，機密情報の管理や緊急時対応の手順，外部委託管理，アウトソーシングなどが考えられます。

4.2　監査の効率化

監査の実施に当たっては，限られた時間のなかで抜けのない調査を行わなければなりません。そこで，あらかじめインタビューの内容や確認すべき記録の内容，判断基準などをチェックリストとしてまとめた上で監査対象に配付し，関係する文書や記録の有無を確認してもらいます。現地では確認済みのチェックリストに沿って調査を実施することにより，監査の効率化を図ることができ，監査の負担を軽減することができます。

4.3　内部監査人のスキルアップ

内部監査人が情報セキュリティ技術や監査に関する研修を受講できるようにしたり，内部監査人同士で勉強会を開いたりすることにより，監査人のスキルアップを図るようにします。これらは，監査人のスキルアップだけでなく，セキュリティ意識の向上にも効果があります。

4.4　委託先の選定

外部監査を行う組織においては，委託先をどのように選定するかがポイントになります。委託先の選定に当たっては，委託先の監査実績や監査人の保有資格などの調査に加え，監査対象の業種・業態や業務に関する知識の有無についても確認するようにし，監査の効率と品質を確保するようにします。

5．むすび

NECは，様々な業種・業態のお客様に対して適切な情報セキュリティ監査を提供できるよう，経済産業省の情報セキュリティ監査企業台帳*に登録するとともに，研究会などにも参画しています。今後とも情報セキュリティ監査の発展に寄与していきたいと考えています。

参考文献

1) ISMS International User Group, ISMS Journal Issue3.
2) 「情報セキュリティ監査助言型監査マニュアル」, 日本セキュリティ監査協会.
3) JIS X 5080:2002,「情報技術－情報セキュリティマネジメントの実践のための規範」, 日本規格協会.
4) JIS Q 19011:2003,「品質及び/又は環境マネジメントシステム監査のための指針」, 日本規格協会.
5) 「情報セキュリティ監査研究会報告書」, 経済産業省.
6) 「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書」, 総務省.

* http://www.meti.go.jp/policy/netsecurity/is-kansa/htmls/233.html

筆者紹介

Takeo Tagami
田上　岳夫（たがみ　たけお）1995年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部セキュリティ技術センター主任。システムズアーキテクト。日本システム監査人協会会員。