情報セキュリティ対策
ベンチマーク活用集

4章 情報セキュリティ対策ベンチマークから情報セキュリティ監査へ

■ 4章で紹介する4つの活用例

この章では、情報セキュリティ監査が用いられる実際のビジネスシーンを想定した、情報セキュリティ対策ベンチマークの活用例を4件示す。

1 助言型情報セキュリティ監査を活用し、よりよい情報セキュリティマネジメントの形成を進めた地方公共団体の例

情報セキュリティ対策ベンチマークを活用した自己評価を生かし、職員の意識改革等を果たした地方公共団体が、システムトラブルを契機として、市民に納得してもらえる情報セキュリティ水準を確保するために、本格的に専門家を活用して助言型の情報セキュリティ監査を受けることになった。助言型情報セキュリティ監査とは実際どのようなものなのだろうか。そして、その効果は？

2 政府機関統一基準に従い政府機関から受託業務を行う民間企業における保証型情報セキュリティ監査の利用例（被監査主体合意方式）

情報セキュリティ対策ベンチマークを活用した自己評価結果が良かったことからS社は、T独立行政法人から情報システム開発業務を受託することになった。受託に当たりS社は、政府機関統一基準に基づきT独立行政法人が定めた情報セキュリティ要求事項に従った対策を整備し、運用する必要がある。実際に業務を開始した後、その要求事項に適正に従っているかを監査することになった。この監査は被監査主体合意方式と呼ばれる保証型の情報セキュリティ監査であった。一体、被監査主体合意方式とはどのような監査なのだろうか？

3 情報セキュリティ対策が顧客の期待水準に達していることの保証を受けた民間企業の例（利用者合意方式）

情報セキュリティ対策ベンチマークを活用して比較的早期にISMS認証を取得したU社が事業拡大のために大手V社に販売活動をしたところ、利用者合意方式の保証型情報セキュリティ監査を受けるよう求められた。利用者合意方式とはどのような監査なのか。そしてU社の準備とは？

4 グループ企業の情報セキュリティ水準を向上させるために情報セキュリティ監査を利用するようになった例（利用者合意方式）

100社を超えるグループ会社を情報セキュリティ対策ベンチマークという共通の尺度で評価し、グループ全体の底上げを図ったX社が次に打った手は？

情報セキュリティ監査を上手に活用して、グループ企業の情報セキュリティ水準の底上げを行うにはどうしたら効果的か？

1　地方公共団体における助言型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマークの利用と効果

P市は人口10万人、地方の中核都市に隣接する小規模工業都市として栄えてきた。事業所数は5,000弱、うち約10％が工業事業所である。

P市では「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成15年版）」を参照し、2004年度中に情報セキュリティポリシーの策定作業を行い、2005年4月より施行した。また、2005年には副市長が情報化推進担当責任者となり、情報政策課が情報セキュリティ対策に取り組むことになった。

しかし、情報政策課では、それまで主に業務システムの電算化を目的に業務を進めており、情報セキュリティに詳しい人材が少なかった。情報セキュリティポリシーの策定もガイドラインを常に参照しながら、専門家の手を借りずに策定した経緯がある。PDCAサイクルは一応回ったものの、Cの段階に不安が残っていた。

その一方、業務系の窓口業務システムにおいて、一昨年、昨年と続いてコンピュータシステムの不具合が見つかり、市民からの問い合わせが相次いだことから、本格的に情報セキュリティ対策の見直しを行うことになった。

昨年度までは、情報セキュリティ対策の予算が組まれていなかったため、まずは無料で実施でき、望ましい水準と、自組織の現状を比較できる情報セキュリティ対策ベンチマークを利用して市の現状を把握し、内部の資料としていた。情報セキュリティ対策ベンチマークの設問への答えを考える中で、情報政策課職員の中に情報セキュリティに関するより深い理解が得られたという者が数人出てきた。

2 助言型情報セキュリティ監査の利用へ

今年度は、昨年度の窓口業務システムの不具合をきっかけに、情報セキュリティ対策の取り組み状況を市議会に報告するよう副市長から指示が出た。このため、民間企業を想定した情報セキュリティ対策ベンチマークの自己診断結果だけでなく、専門家である第三者が評価した結果を提出する必要が生じた。

市民に分かりやすい形で評価結果を示す必要があるため、ISMS認証の取得も検討したが、現状では認証取得レベルにあるか判断できず、また、予算措置もなかった。そこで、当面ISMS認証取得を断念し、情報セキュリティ監査を受ける方向で検討することになった。

当初は、総務省の「地方公共団体における情報セキュリティ監査ガイドライン（平成15年版）」を参考に、内部監査の実施を検討したが、現在の体制ではすぐに内部監査を実施できる状況ではなかった。このため、専門家に助言型情報セキュリティ監査を委託し、あるべき姿と現状のギャップについての指摘を受けるとともに、改善の方向性について助言を得ることにした。

情報政策課では、今年度の監査対象を情報セキュリティポリシーの適切性の評価と昨年不具合の見つかった基幹システムとした。外部監査人の調達様式は、公募型プロポーザル方式（企画提案書を評価・判断して事業者を選定）とし、要求仕様を作成し公募したところ、数社より応募があった。

検討の結果、特定非営利活動法人日本セキュリティ監査協会（JASA）の公認情報セキュリティ監査人（CAIS）資格を保有し、また地方公共団体セキュリティ対策支援フォーラム（LSフォーラム）の主催する自治体業務知識研修を終了した監査人が所属するR社に助言型監査を依頼することにした。監査技量とともに自治体特有の業務知識があり、さらに監査の品質に万一問題があった場合は、申し立てにより、JASAの審査委員会で紛争審査が行われることから、非常に信頼性の高い監査が実施できると考えたためである。

R社の監査人との契約締結にあたっては、改めて以下の項目を確認した。

＜監査内容＞

- 監査の目的、対象、範囲
- 準拠する基準
- 監査のポイント

＜監査人の権限＞

- 監査人の権限
- 注意義務
- 倫理
- 監査人の責任
- 機密保持
- 監査結果の管理方法

＜監査スケジュール＞

- 監査実施期間
- 事前打合せの時期と回数
- 監査計画書作成
- 予備調査
- 本調査
- 監査報告書作成
- 監査報告会

＜監査実施体制＞

- 監査責任者、監査人、アドバイザを含む監査体制
- P市情報政策課との役割分担

＜成果物＞

- 納入物一覧

特に報告会については、情報政策課への報告会のほか、市長への報告会を追加した。確認の結果は非常に納得のいくものであったため、正式にR社と契約を締結した。契約に際しては、R社の監査チーム全員に守秘義務契約を課し、また監査結果の管理方法についても明示した。

3 監査の実施とその成果

契約に際してR社との間で充分な確認をしたため、監査自体は非常にスムーズに行われた。

特に予備調査では、総務省の地方公共団体情報セキュリティ管理基準をもとにR社が作成したアンケートを使用した。R社では、同じ管理基準について、「情報システム管理担当者用」と「窓口職員（システム

オペレータ）用」の二通りのアンケートを使用し、システムに詳しくない現場の職員にも分かりやすい形になっていた。また、R社の提案に従い、監査手続き開始に先立って、監査を受ける側の部署の職員に「説明会」を開いた。その結果、「情報セキュリティとは何か」「何のために情報セキュリティ監査を行うのか」について、職員の理解が得られ、その後のアンケート、ヒアリングがスムーズに実施できるようになった。

情報セキュリティ監査の結果は、下記の報告書にまとめられ、情報政策課での報告会のほか、市長への報告とも非常に分かりやすく、満足のいくものであった。

発行日　：200X年XX月XX日
報告書No.：XXXXXXXXXXX

P市市長　○○　○○　殿

発行責任者：R株式会社　代表取締役社長
○○　○○　印
審査者　：R株式会社 セキュリティ事業部
上席スタッフ
○○　○○　印
作成者　：R株式会社　監査チームリーダー
○○　○○　印

情報セキュリティ監査報告書

「地方公共団体情報セキュリティ管理基準」に照らして、200X年XX月XX日から200X年XX月XX日における貴市の情報セキュリティ活動の実施状況について監査を実施いたしました。

当監査は、「地方公共団体情報セキュリティ管理基準」及び監査依頼者・監査実施者双方で同意した「情報セキュリティ管理基準」の一部項目（別紙1参照）に基づいて監査を行い、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かを確かめ、さらに成熟度モデルを活用して、問題点を検出し提示するという観点から実施いたしました。

監査の結果、以下の検出事項とその改善提言を報告いたします。

当監査報告書は内部利用を目的として作成したものであるとともに、監査依頼者と、監査実施者または監査人との間には、記載すべき利害関係はありません。

― 記 ―

Ⅰ. 監査の概要

1. 個別管理基準の作成

「地方公共団体情報セキュリティ管理基準」の中から、個人情報保護と密接な関係があるコントロール項目に基づき、貴市の監査を実施した。

なお、上記コントロール項目については、貴市よりご提示の17項目の他、さらに当監査チームが重要と判断した20項目を追加し、貴市固有の個別管理基準を作成した。

情報セキュリティ管理 における各領域	貴市よりご提示の コントロール項目数	監査チームが追加した コントロール項目数	合計
セキュリティ基本方針	1 項目	1 項目	2 項目
組織のセキュリティ	―	1 項目	1 項目
資産の分類及び管理	2 項目	―	2 項目
人的セキュリティ	3 項目	1 項目	4 項目
物理的環境的セキュリティ	4 項目	4 項目	8 項目
通信及び運用管理	6 項目	1 項目	7 項目
アクセス管理	―	10 項目	10 項目
システムの開発及び保守	―	1 項目	1 項目
事業継続管理	―	1 項目	1 項目
適合性（コンプライアンス）	1 項目	―	1 項目
合計	17 項目	20 項目	37 項目

2. 成熟度モデルの適用

上記1.で作成した個別管理基準に基づき監査を実施するにあたり、COBIT 4.1の成熟度モデルを適用した。成熟度は、すべての項目共通とし、以下の6段階により評価を行った上で、成熟度レベル「3」に基づく監査意見を述べている。

成熟度	レベル
5	最適化されている
4	管理され、測定が可能である
3	定められたプロセスがある
2	再現性はあるが直観的
1	初期／その場対応
0	実施していない

3. 監査実施期間

200X年XX月XX日からXX月XX日

4. 監査体制

(1)監査チーム

監査人氏名	役　割	所持資格
○○　○○	監査チームリーダー	公認情報セキュリティ主任監査人
○○　○○	監査チームメンバー	公認情報セキュリティ主任監査人
○○　○○	監査チームメンバー	公認情報セキュリティ監査人
○○　○○	監査チームメンバー	公認情報セキュリティ監査人

(2)監査品質管理体制

監査チームから独立した品質管理者を以下の通り設けた。

氏　名	所属・役職	所持資格
○○　○○	セキュリティ事業部 上席スタッフ	公認情報セキュリティ主任監査人

Ⅱ. **監査意見**

200X年XX月XX日から200X年XX月XX日までの期間に係るXXXを対象とした情報セキュリティ対策の実施状況は、監査手続きを実施した範囲内において以下に記載する検出事項が「情報セキュリティ管理基準」に照らして不適切であると判断される。

Ⅲ. **検出事項**

領域（部署名）	項目（コントロール及び サブコントロール）	検出された個別事象
・・・・・	・・・・・・・・・	・・・・・・・

Ⅳ. **改善提言**

緊急改善事項	領域：○○○ 項目：・・・・・・・・ 提言内容：・・・・・・・・・
	領域： 項目： 提言内容：
通常改善事項	領域： 項目： 提言内容：
	領域： 項目： 提言内容：

※「緊急改善事項」、「通常改善事項」の区分は、監査チームの判断による。

Ⅴ. **特記事項**

・・・・・・・・・・・

以上

ただし、報告書の市民への公開については、P市のぜい弱性を公開することにもつながるので、市の広報誌及びWebサイトにて、下記のように公開するにとどめた。

P市の情報セキュリティ対策実施状況について

200X年XX月XX日
P市市長　○○　○○

「情報セキュリティ管理基準」に照らして、200X年XX月XX日から200X年XX月XX日における情報セキュリティ活動の実施状況について監査を実施いたしました。

当監査は、「地方公共団体情報セキュリティ監査基準」及び監査依頼者・監査実施者双方で同意した「情報セキュリティ管理基準」の一部項目（別紙1参照）に基づいて監査を行い、情報セキュリティに関わるリスクのマネジメントが効果的に実施されるよう、リスクアセスメントに基づいて適切なコントロールが採用されているか否かを確かめ、さらに成熟度モデルを活用して、問題点を検出し提示するという観点から実施いたしました。

監査人の選定に当たっては公募型プロポーザル方式とし、応募社の提案を検討の結果、R社と決定し、契約を結びました。

監査の結果、R社より○件の検出事項とその改善提言が報告されました。改善提言中、△件につき改善対策実施済み、▽件について対策を実施する予定です。

当監査報告書は内部利用を目的として作成したものであるとともに、監査依頼者と、監査実施者または監査人との間には、記載すべき利害関係はありません。

助言型情報セキュリティ監査を実施したことで、情報政策課の職員に情報セキュリティ監査のノウハウが蓄積されたばかりでなく、監査を受けた職員の間にも情報セキュリティに対する意識が浸透したことが最も大きな収穫であった。

これを機に、全システムに対し、内部監査を2年に1度、外部監査を3年に1度実施するサイクルを構築し、運営していくことが市議会において承認された。

2 政府機関統一基準に基づく被監査主体合意方式の保証型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマークの利用と効果

S社はT独立行政法人から、情報検索システムの運用を受託している。海外からの利用も想定し、運用は24時間体制で、障害の緊急対応などを含むフルアウトソーシングの形態である。

このシステムはWebサイトによりT独立行政法人が保有する知識データベースを検索するシステムである。個人情報等の機密性の高い情報を取り扱うことはないが、知識データベースへのアクセスを行わせることは、T独立行政法人にとって情報セキュリティ上のリスクになる。また、利用者にとり、自身の検索行動について第三者が知りうることは好ましくない。これらのことから、機密性・完全性の要素において、高い水準の情報セキュリティ対策を必要としている。また海外からの利用のため、24時間安定稼働が必要であり、可用性についても配慮が求められる。

T独立行政法人は、情報検索システムの運用を外部委託するに当たり、運用委託業者選定委員会を中

立的な委員により組織し、選定作業を行うこととした。運用委託業者選定委員会は、内閣官房情報セキュリティセンター(NISC)が公表した「外部委託における情報セキュリティ対策実施規定」を参考に、情報セキュリティ対策ベンチマークの結果を指標として、委託先候補の情報セキュリティ対策の遂行能力と取り組み状況を評価した。

その結果、運用委託業者選定委員会では、情報セキュリティ対策ベンチマークの結果で多くの項目で望ましい水準にあり、同業グループ内でも高い結果を示し、かつ提案書の内容が優れていたS社を情報検索システムの運用業務の委託先の第一候補とすべきとの結論を得た。

2 保証型情報セキュリティ監査の利用へ

T独立行政法人の情報セキュリティ責任者はさらに、S社の情報セキュリティ対策の履行状況を確認するために、定期的に自己点検の結果を報告するとともに、S社において実施すべき情報セキュリティ管理手続と情報セキュリティ監査の実施を要求した。具体的には、調達仕様書の中で、調達条件として次の項目を記述した。

(1) 定期的な自己点検の結果報告。
(2) 外部委託する情報検索システムの運用において、実施すべき情報セキュリティ管理手続き。
(3) 年1回の被監査主体合意方式による保証型情報セキュリティ監査の実施及び監査結果の報告。

S社は、T独立行政法人が提示する情報検索システム運用外部委託仕様書に対し、具体的な情報セキュリティ対策をとりまとめ、T独立行政法人に提案した。

(1) 自己点検の報告は、情報セキュリティ対策ベンチマークの結果を定期的に報告する。
(2) 管理手続きは、S社が現状で実施している情報セキュリティ管理手続きをそのまま実施する。
(3) 被監査主体合意方式の保証型情報セキュリティ監査については、情報セキュリティ監査企業台帳に登録されており、JASAの会員企業でもあるY監査会社に依頼する。

T独立行政法人は、S社からの提案内容を高く評価し、S社を外部委託企業として採択した。T独立行政法人とS社は、情報検索システム運用外部委託に関する条件を詰め、合意内容に基づき外部委託契約を締結した。

委託契約にもとづき、S社は毎年1回、次の流れにより被監査主体合意方式の保証型情報セキュリティ監査を実施することとなった。

3 監査手続の合意

被監査主体合意方式の保証型情報セキュリティ監査の流れは、下記のとおりである。

(1) S社は、提案書で提示したY監査会社と監査契約を締結する。
(2) S社とY監査会社は、合議により、監査テーマ及び監査手続を決定し合意する。
(3) S社は、(2)でY監査会社と合意した監査テーマ及び監査手続の内容を、T独立行政法人に報告し、T独立行政法人の確認をとる。
(4) Y監査会社は、(2)でS社と合意した監査テーマ及び監査手続に従い、S社に対する監査を実施し、監査報告書をS社に提出する。
(5) S社は、Y監査会社から提出された監査報告書を、T独立行政法人に提出する。

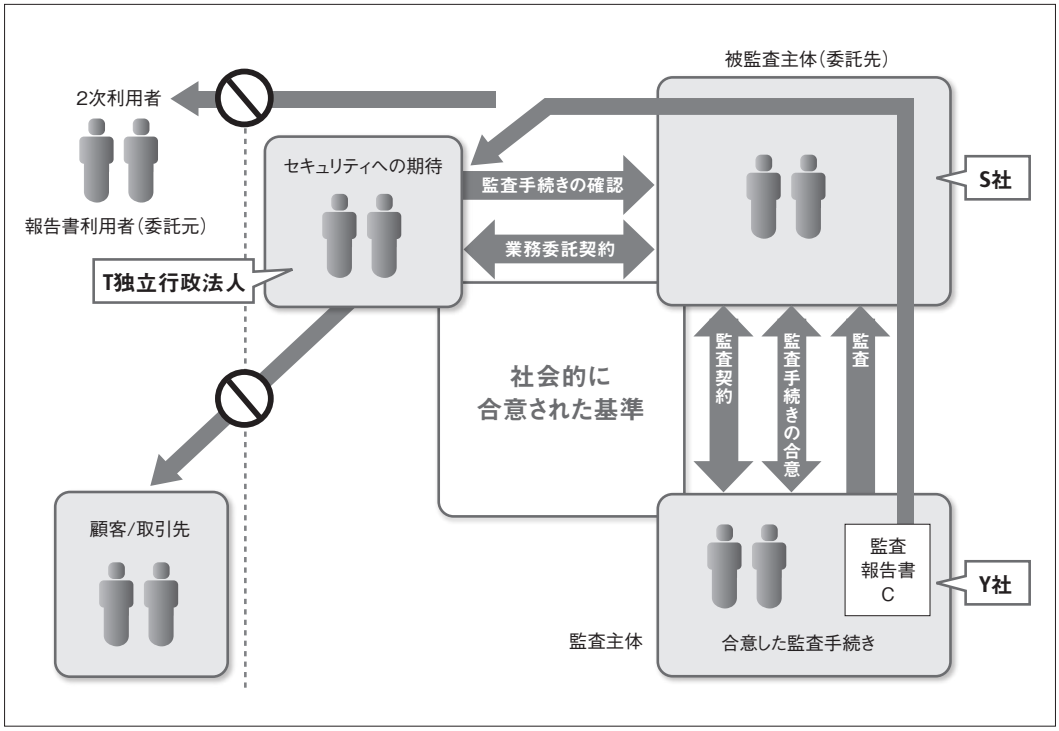

図4.1　被監査主体合意方式の保証型監査

S社とY監査会社とは、初年度の情報セキュリティ監査の実施における監査テーマを次の3領域とすることで合意した。

(1) 物理的及び環境的セキュリティ
(2) 通信及び運用管理
(3) 情報セキュリティインシデント管理

また、これら3領域において対象とする情報セキュリティ管理手続きとその監査手続きについては、次頁 **表4.1**の内容で合意した。

S社は、Y監査会社とのこれら合意内容について、T独立行政法人の確認を得た。

表4.1　合意した情報セキュリティ監査手続き

監査領域	情報セキュリティ管理手続	情報セキュリティ監査手続
物理的及び環境的セキュリティ	セキュリティを保つべき領域が許可されたものだけにアクセスを許すことを確実にするための、適切な入退管理策により保護されていること。	【閲覧】入退室管理規定、入退室手順が確立されているかを確認する。 【再実施】正しい入退室方法、不正な入退室方法の両方を試す。
	装置の可用性及び完全性を継続的に維持するための作業が実施されていること。	【閲覧】定期的な保守作業が正しく行われているか、事故発生時の対応が正しく行われているかを、保守作業記録を閲覧して確認する。
	・ ・	・ ・
通信及び運用管理	悪意のあるコードから保護するために検出、予防及び回復のための管理策が実施されていること。	【閲覧】ウイルス対応手順などを閲覧し、悪意のあるコードから情報資産を保護するために、検出、予防及び回復のための管理策が実施されているかを確認する。
	情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていること。	【閲覧】バックアップ方針及びバックアップ記録等を閲覧し、情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていることを確認する。
	監視活動の結果が定めに従ってレビューされていること。	【閲覧】ログ解析結果等を閲覧し、監視活動の結果が定めに従ってレビューされていることを確認する。
	・ ・	・ ・
情報セキュリティインシデント管理	情報セキュリティインシデントに対する責任体制及び手順が確立されていること。	【閲覧】情報セキュリティ関連規程を閲覧し、情報セキュリティインシデントに対する責任体制及び手順が確立されていることを確認する。
	情報セキュリティインシデントの発生に対して、規模及び費用を定量化し監視できるようにする仕組みが備えられていること。	【閲覧】情報セキュリティインシデントの記録を閲覧し、規模及び費用を定量化し監視できるようにする仕組みが備えられていることを確認する。
	・ ・	・ ・

4 監査の実施とその成果

Y監査会社は、3において示したS社と合意した監査テーマ及び監査手続きにより、S社に対する被監査主体合意方式の保証型情報セキュリティ監査を実施し、次の監査結果報告書をS社に提出した。

平成19年○○月○○日

S株式会社
代表者　○○　○○　殿

Y監査会社
代表者　○○　○○　印

情報セキュリティ監査結果報告書

当社は、T独立行政法人殿が貴社に運用を委託している情報検索システム運用業務の情報セキュリティ対策の順守状況を確かめることを目的として、貴社が、T独立行政法人殿と貴社の経営者との間で定めた情報セキュリティに係る管理手続（以下「情報セキュリティ管理手続」という。）を平成×年×月×日から平成×年×月×日までの期間において履行していることを確認するために、「被監査主体合意方式」による保証型情報セキュリティ監査を実施した。

情報セキュリティ管理手続は、T独立行政法人殿から平成○年○月○日に要求された情報セキュリティ管理基準に基づいて貴社がその対策を記載した管理手続であり、平成×年×月×日から平成×年×月×日までの期間において、情報検索システム運用業務に対してこの情報セキュリティ管理手続が実施されていることの責任は、貴社の経営者にある。また、貴社の情報セキュリティ管理手続の十分性については、貴社及び貴社がT独立行政法人殿から得た確認に従ったものであり、本書に掲載されていない情報セキュリティ管理手続については、今回の情報セキュリティ監査の範囲には含まれていない。

当社は、「情報セキュリティ監査基準」に準拠して、下記に掲載した貴社と合意した情報セキュリティ監査手続を実施した。この情報セキュリティ監査手続を実施した結果は下記の通りである。ただし、当社が実施した情報セキュリティ監査手続は、貴社及び当社との間で合意し、T独立行政法人殿の確認を得た情報セキュリティ監査手続に限定して監査手続を実施している。

（確認した情報セキュリティ監査手続とその結果は、ここ又は別紙に記載する。）

なお、この報告書は、T独立行政法人殿のための情報利用を意図したものであり、T独立行政法人殿及び貴社以外の第三者の利用を意図したものでなく、また、他の第三者にこの報告書を利用させてはならない。

以上

— 別　紙 —

確認した情報セキュリティ監査手続とその結果

監査領域	情報セキュリティ管理手続	情報セキュリティ監査手続	結果	発見事項
物理的及び環境的セキュリティ	セキュリティを保つべき領域が許可されたものだけにアクセスを許すことを確実にするための、適切な入退管理策により保護されていること。	【閲覧】入退室管理規定、入退室手順が確立されているかを確認する。 【再実施】正しい入退室方法、不正な入退室方法の両方を試す。	○ 実施していると認められる	－
	装置の可用性及び完全性を継続的に維持するための作業が実施されていること。	【閲覧】定期的な保守作業が正しく行われているか、事故発生時の対応が正しく行われているかを、保守作業記録を閲覧して確認する。	○ 実施していると認められる	－
	・ ・	・ ・		
通信及び運用管理	悪意のあるコードから保護するために検出、予防及び回復のための管理策が実施されていること。	【閲覧】ウイルス対応手順などを閲覧し、悪意のあるコードから情報資産を保護するために、検出、予防及び回復のための管理策が実施されているかを確認する。	○ 実施していると認められる	－
	情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていること。	【閲覧】バックアップ方針及びバックアップ記録等を閲覧し、情報及びソフトウェアのバックアップが合意されたバックアップ方針に従って定期的に取得されていることを確認する。	○ 実施していると認められる	－
	監視活動の結果が定めに従ってレビューされていること。	【閲覧】ログ解析結果等を閲覧し、監視活動の結果が定めに従ってレビューされていることを確認する。	○ 実施していると認められる	－
	・ ・	・ ・		
情報セキュリティインシデント管理	情報セキュリティインシデントに対する責任体制及び手順が確立されていること。	【閲覧】情報セキュリティ関連規程を閲覧し、情報セキュリティインシデントに対する責任体制及び手順が確立されていることを確認する。	○ 実施していると認められる	－
	情報セキュリティインシデントの発生に対して、規模及び費用を定量化し監視できるようにする仕組みが備えられていること。	【閲覧】情報セキュリティインシデントの記録を閲覧し、規模及び費用を定量化し監視できるようにする仕組みが備えられていることを確認する。	○ 実施していると認められる	－
	・ ・	・ ・		

S社はこの報告書をT独立行政法人に提出し、T独立行政法人は、Y監査会社がS社に対して行った情報セキュリティ監査によって、S社の情報セキュリティ対策が、T独立行政法人の要求するセキュリティ事項を満たしていることを確認した。

3 一般企業における利用者合意方式の保証型情報セキュリティ監査の利用例

1 情報セキュリティ対策ベンチマーク利用とISMSの取得

U社は、Webシステムを用いた顧客管理を行うアプリケーション提供サービスを行う企業である。従業員総数は60人と小さいが、系列のデータセンターを利用して、堅実なサービスを提供し、徐々に大口の顧客を獲得しつつあった。

情報セキュリティサービスが付加価値サービスであり、ネットワークやサーバに対するセキュリティの設定と監視を顧客に提供している。セキュリティを独学で学んだ部長が、独自のセキュリティポリシーを作成し、それに基づき情報セキュリティ対策を施していた。

近年、同業他社がISMS認証の取得等を通じて、情報セキュリティの優位性をアピールしている。これに対抗するために、社長からISMS認証の取得を行えないかとの打診があった。ただ、社長の要求は厳しく、残された期間は半年に満たないものであった。

既にポリシーを作成し、運用しているので、ISMS認証の取得も無理ではないと考えた専務は、この少ない期間でISMS認証の取得が可能かを検討するように部長に指示した。部長は独自の情報セキュリティ対策でISMS認証取得が可能であるかを確認するために、情報セキュリティ対策ベンチマークを利用することとした。

情報セキュリティ対策ベンチマークの結果は、上位21%から30%の範囲であり、かなりの項目で望ましい水準にあった。一方、情報資産の取り扱いやシステムの障害対策などいくつかの項目で、望ましい水準に達していないことが判明した。これらの弱点についての対策の大部分は、現在行っている管理策の徹底などで対応できるものがほとんどだったことから、短期でISMS認証の取得が可能との見通しが立った。

ISMS認証の取得は、当初思ったよりは苦労した。また、審査のタイミングがあわず、多少、時間を要したが、半年あまりで認証を取得した。

2 保証型情報セキュリティ監査の利用へ

ISMS認証の取得が功を奏したのか、その後、優良顧客に恵まれ、U社の業績は順調に伸びていった。U社は更なる業容拡大のため、インターネット・キャッシングを開始しようとしている大手金融機関のV社に営業を行った。V社のインターネット・キャッシングは、24時間365日サービスを行うものである。キャッシングというサービスのため、顧客の機微情報も取り扱う。このため、機密性・可用性のいずれの要素においても高い水準のセキュリティを必要とする。

U社は営業資料等に、最大停止時間15分以内のサービスレベルとISMSの認証取得を掲載している。V社は、U社のISMS認証取得は評価したものの、U社に対し、自社の情報に対するセキュリティ面での十分な対策を施し、さらにその内容が着実に行われていることを客観的に証明するよう求めた。そこでU社は、V社と秘密保持契約を締結した上で、自社が実施している情報セキュリティマネジメントシステムの詳細管理策を開示し、その実施を外部機関による情報セキュリティ監査で客観的に評価して貰うことで対応することを提案した。

V社がこの提案を受諾したため、約1ヶ月で詳細管理策を提示し、その後、3ヶ月以内に監査報告書を提出することとなった。

3 言明書の作成

U社は、V社と相談し、情報セキュリティ監査企業台帳に登録されており、JASAの会員企業でもあるZ監査会社に依頼することを決定した。

U社で行なわれる保証型情報セキュリティ監査は、利用者合意方式と呼ばれるものである。この方式では、最初に、U社がV社の情報セキュリティ上の期待水準に基づき、実施する情報セキュリティ管理手続を言明書として取りまとめ、V社に提示する。

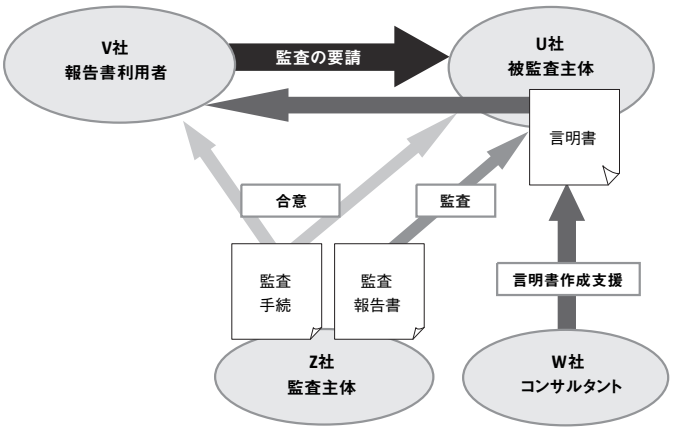

図4.2　保証型監査の主体間の関係（利用者合意方式）

V社がその内容で自らの期待する情報セキュリティが確保できると判断すると、この言明書が適正であるか否かについて、監査主体であるZ監査会社が情報セキュリティ監査の結果に基づき意見を述べる。Z監査会社が行う監査手続で、V社が期待する保証に足る監査ができるかについては、報告書利用者であるV社とZ監査会社が事前に合意する必要がある。

情報セキュリティ監査に先立ってZ監査会社は、U社の状況を聞き取った。その結果、以下の点をU社に伝えた。

(1) ISMS認証取得の全ての分野にわたった詳細管理策を監査するには、時間的にも費用的にも膨大になること。

(2) U社がISMS認証を取得しており、基本的なマネジメントシステムはできていることから、リスクの大きい分野に絞った情報セキュリティ監査であれば比較的安価な費用で行えること。

U社はISMS認証取得に用いたリスク分析を再検討したが、すべて許容リスク以下のため、対象を絞ることができなかった。そこで、コンサルタントのW社に助言を求めた。

W社がU社の業務フローとデータフローを把握し、統制上のクリティカルポイントを分析した結果、顧客○○情報データベースに、最も多様な人々がアクセスし、作業に用いていることが明らかになった。U社の情報セキュリティ設計もそれを意識しており、多重のシステム的な防御策をとっているが、それでもなお人的要因を排除できず、そのことが最も大きなリスクであると判断された。

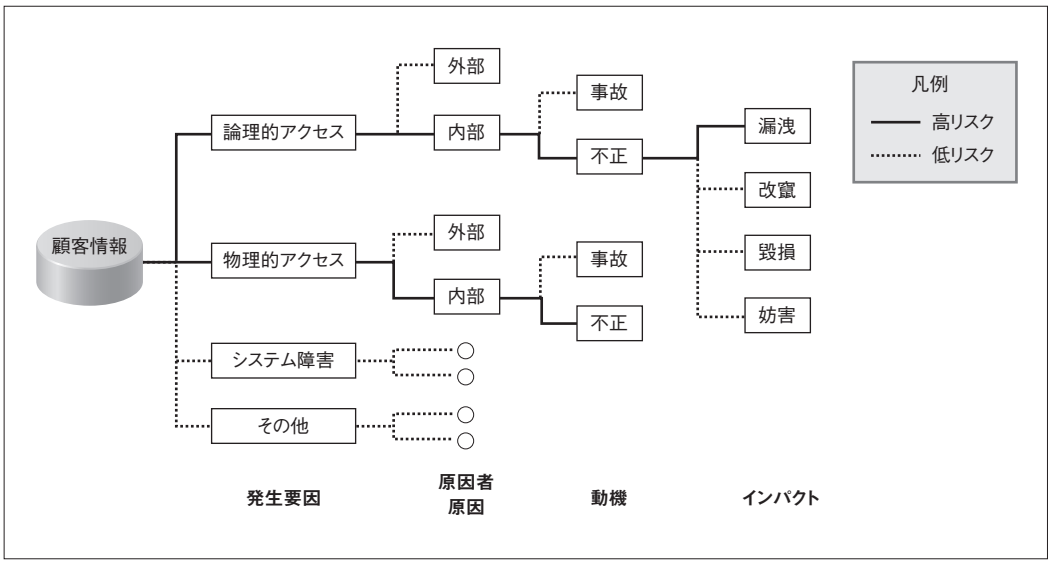

図4.3　リスク分析のイメージ

W社は、分析結果に基づき、アクセス制御の管理に焦点を当てるべきであるとU社のトップに提言した。

提言を受け、U社はアクセス制御に関わる管理手続きについて言明書を作成し、V社に提示した。言明書は、以下のとおりである。

20XX年MM月DD日

V株式会社　殿

顧客の情報を取扱う業務の情報セキュリティマネジメントに関する言明

U株式会社
代表取締役社長　○○　○○

1. 当社は、200X年XX月XX日にV株式会社殿から以下の要求を受けました。
   当社が提供する＊＊＊＊サービス（以下、対象業務）では、V株式会社殿から委託された情報（顧客の情報）を確実に管理すること。
2. 当社は、リスクアセスメントの結果、前項の要求を実現するに足る管理策を下記の範囲で整備し、運用しています。

当社の対象業務を担当する部門は、公的な基準に基づく情報セキュリティマネジメントシステムを運用しています。

Ⅰ　対象範囲及びリスク管理方針	
1. 対象範囲	① 対象業務に係る＊＊システムと、当該システムの運用部門、＊＊センター、当該センターに入室する全ての人（システムの利用者、関係する社員及び部外者など）を対象とする。 ② 【参照資料】 ③ 対象システム範囲：付属資料1に図面で表示。 ④ ＊＊センター詳細：付属資料2に図面で表示。
2. リスク	① 対象業務に係る各プロセスのリスクを評価した結果、顧客＊＊データベースに係る不正アクセスリスクが非常に大きい。 ② 対象業務においては、事業継続上顧客の信頼が不可欠であり、信頼維持のために、顧客の情報の機密性確保が最も重要である。 ③ 機密性確保を問われる顧客の情報の中では、顧客から受託する顧客＊＊情報の価値が最も高い。これを処理する＊＊管理システムの機密性に関するリスクが最大である。 ④ ＊＊管理システムの中についてみると、ネットワーク上を流れる部分的な顧客＊＊情報よりは、データベースに蓄積された顧客＊＊情報全体の機密性に関するリスクが大きい。 ⑤ 顧客＊＊データベースの機密性確保の観点においては、技術的（システムぜい弱性リスク・システム運用リスク等）・物理的セキュリティリスクに比較して、不正アクセスリスクが非常に大きい。
3. リスク管理方針	当社は、下記の方針で重要な情報資産を管理している。 ① 従業員等による不正を防止するため厳格なアクセス管理策を講じる。 ② アクセス管理策は、合理的な範囲で行う。 1 ＊＊システムに過大な負荷をかけない範囲で実装する。 2 ライセンス契約に抵触するシステム改変は行わない。 3 アクセス管理サービス価格に影響を与えない範囲で行う。
Ⅱ　管理策	
(1) 9.1.2* 物理的入退管理策	① ＊＊センターへの入退室は、以下の方針で行っている。 ② センター入り口には、許可された者のみが入退室できるよう、ビデオ監視装置つきの導入路を設け、その導入路の前後に扉を設置し、制御している。 ③ 業務に従事する者すべてに、顔写真入りのIDカードを配布し、入室時には常に着装させている。なお、入館証はICカードとし、入退室及び機器へのアクセス管理の認証のためにも利用している。 ④ センターの扉はICカード及び指紋認証装置により制御し、許可された者以外の入室を阻止している。なお、指紋認証装置の読取不全の時は、パスワードでの認証を併用している。 ⑤ 室内での工事等により役員・社員等以外の者が立ち入る必要がある場合には、事前に情報セキュリティ管理者に届け出し、許可を受けさせている。許可をした場合には、臨時のIDカードを貸与した上で、２名以上の社員が常時付き添い作業に従事させている。なお、臨時のIDカードは毎日回収している。 ⑥ ビデオ監視及び入退室のログを記録し、3年間安全に保存している。
(2) 10.1.3* 職務の分割	① 対象業務に関わる区画及び重要情報資産へのアクセス権限は、職務及び責任範囲を明確にした職務定義書に基づき設定している。 ② 職務定義においては、一人が複数の権限を保有しないよう、・・・の作業を分離するよう設定している。 ③ 各職務について、・・・、各々に対するアクセス権限の内容を明確にする。また、緊急の必要により、・・・場合の管理策をあらかじめ定め、これに基づき作業を行っている。 ④ 全ての役員・社員等には、・・・権限以外のアクセスを禁止している。 ⑤ ・・・組織・人事の異動の際にも権限の重複がないようにしている。 ⑥ 情報セキュリティ管理責任者が・・・年1回定期的に見直している。
・ ・	・・・ ・・・

＊ 9.1.2、10.1.3は、情報セキュリティ管理基準などの番号である。

4 監査手続の合意

Z監査会社は、U社が提示した言明書をもとに、監査手続きの検討に入った。監査手続は、設計監査と実装監査の2つに分けられる。

設計監査では、対象業務に関するリスクの把握が適正に行われ、言明書に必要十分な管理策が組織的に検討されていることを確認する。

実装監査では、言明書の管理策が言明書どおりに実施されていることを確認する。監査手続きを策定するに当たって、情報資産の重要度や監査リスク（ルールと実態が乖離しやすい）などを考慮し以下の4つに類別した。その結果をもとに監査規模の見積りなどを行い、必要十分な監査手続をとれるようにした。

類別	概要	具体的な例
L (Logical)	ルール（基準や運用手順、システム仕様書など）の存在を閲覧などにより確認する。	・パスワード管理システムの仕様確認。 ・モバイルコンピュータの設定ルール確認。
G (Governance)	ルールが周知徹底されているかを、部分的なエビデンスの閲覧や質問などにより検証する。	・アクセス管理方針の運用状況などを質問により確認。 ・教育の受講記録を確認。
D (Document)	ルール通りに運用されているかを、記録の閲覧や質問・視察などにより整合性を検証する。	・ID削除依頼書とサーバのID設定内容及びID削除の実行に関係するログとの整合性確認。 ・送付者と受け取り者のドキュメントの整合性確認。
P (Physical)	ルールに基づいて保存されている記録の信憑性を、閲覧・質問・視察や再実施により検証する。	・2人同時に入室していないかなど物理的な入退室の状況を目視確認。 ・入退室ログと勤務実態があっているかなど入退室ログと実地の目視確認。 ・実物の運用状況の目視確認。

以上の検討結果に基づき、Z監査会社は以下に示す監査手続きをU社及びV社に提示した。

V社はこの監査手続により、監査で十分な成果が得られると判断し、監査手続きについて合意した。

監査手続（平成○○年○月○日作成）　Z監査会社

U株式会社　情報セキュリティ監査チームリーダ
××　××

【設計監査】管理策の必要性・十分性	
言明書作成の 正当性	【質問】言明書作成の目的、言明の根拠に関し、経営者に質問を行い、明確な根拠があることを確認する。 また、言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。 【閲覧】言明の根拠となる、言明書作成の経緯を記録した文書を閲覧し、経営者の回答と整合性が取れていることを確認する。 文書としては、以下のものを対象とする。 ・言明書作成に関わる会議の記録（情報セキュリティ委員会議事録、経営会議議事録、その他打合せ記録等）。 ・言明書作成の資料として用いたW社のコンサルティングの結果報告書。 ・ISMSなど公的な認証取得の文書を閲覧し、経営者が情報セキュリティマネジメントを的確に運用していることを確認する。

リスク把握の適切さ	【閲覧】対象業務フローに係るリスク分析を確認し、リスクが漏れなく、的確に洗い出されていることを確認する。 【視察】業務の現場を確認し、リスク分析で記述された脅威・ぜい弱性が十分であることを確認する。 【質問】業務現場の担当者に質問し、リスク分析が的確であることを確認する。 【質問】経営者にリスクに関して質問し、リスクが正しく認識されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。
管理策の適切さ	【閲覧】情報セキュリティ管理基準を参照して作成した個別管理基準に照らして、リスク分析によって洗い出されたリスクに対し、言明書において必要な管理策が網羅されていることを確認する。 【質問】経営者に管理策の内容を質問し、管理策として行うべきことが的確に記述されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。
【実装監査】　言明書どおりに運用が行われていることの確認	
言明書の運用の確認	【質問】経営者と業務管理責任者に質問し、言明書に基づく管理を実施していることを確認する。 【閲覧】言明書どおりに管理策が組織全体で運用されていることを示す文書を閲覧し、組織的管理が行われていることを確認する。 ・情報セキュリティ委員会等の議事録。 ・詳細管理策策定後の運用状況を記録した文書。 【閲覧・質問】内部監査報告書を閲覧すると共に、内部監査人に質問し、適正な運用が行われていることを確認する。 ・詳細管理策運用に関する内部監査報告書。
・ （略） ・	
職務権限定義の適正さ	【閲覧】職務定義及び職務任命に関する文書を閲覧し、適正な運用がなされているかを確認する。 ・対象業務に関わる区画及び重要情報資産へのアクセス権限を規定する職務及び責任範囲を明確にした職務定義書は適正な手順により作成・承認されているか。 ・職務定義書の内容は、以下の条件を満たしているか。 ・辞令で確実に職務権限の発令、停止が行われているか。 ・権限のたな卸しは、年1回経営者の責任において行われているか。 【質問】業務責任者・現場担当者に質問し、記録が正しく行われていることを確認する。 ・一人が複数の権限を保有しないか。 ・一つの職務で同一の重要データに対する読取、書込み・変更、監視・監査の作業が分離されているか。 ・各職務について、業務遂行上アクセスが必要な情報資産が全て網羅されているか。 ・各職務の情報資産に対するアクセス権限の内容が明確か。 ・緊急の必要により、職務定義書に定められた以外の作業や他の人の作業を兼務することが生じた場合の管理策があらかじめ定められているか。 ・職務定義書に定められた以外の作業においては、あらかじめ定められた管理策に基づき作業が行われているか。 ・全ての役員・社員等に、定められた権限以外のアクセスが禁止されているか。 ・組織・人事異動の際にも権限の重複がないよう運用されているか。 ・情報セキュリティ管理責任者が職務権限の設定と付与を行っているか。 ・情報セキュリティ管理責任者が権限の付与状況を少なくとも年1回定期的に見直しているか。
・ （略） ・	

5 監査の実施と効果

情報セキュリティ監査手続きの合意を受けて監査が実施された。

その結果、U社は、下記に示す報告書により、委託元（顧客であるV社）の期待する水準にあるとの保証意見を得ることができた。

情報セキュリティ監査の保証意見により、V社はU社との契約を締結することになった。その後U社は、最大停止時間15分以内のサービスレベルとISMS認証を取得していることに加え、保証型情報セキュリティ監査で保証を得ている点を同業他社との差別化ポイントとして、V社と同等の情報セキュリティ水準を期待している大手金融機関なども対象として、更なる業容拡大をはかることとした。

情報セキュリティ監査報告書

200X年XX月XX日

委　託　元　　V株式会社　殿
被監査主体　　U株式会社　殿

監査主体
Z監査株式会社
代表者　○○　○○印

情報セキュリティ監査報告書

監査主体は、被監査主体との200×年●月●日付情報セキュリティ監査契約にもとづく「利用者合意方式」による保証型情報セキュリティ監査の結果を下記のとおり報告する。

― 記 ―

監　査　結　果

●●作成の200X年●月●日付言明書記載のシステムの運用管理サービスに対する情報セキュリティ対策の実装は、委託元の合意を得た情報セキュリティに係る監査手続を実施した限りにおいて、□□□□によって示されている同業務委託元の期待する水準にあるものと認める。

理　　由

監査人は、主任監査人○○、監査人△△、監査人補××からなる監査チームを組織し、情報セキュリティ監査基準及びU株式会社作成の詳細管理策に基づく個別管理基準に準拠して、200X年●月●日から200X年●月●日までの間、監査報告書利用者たる○○業務委託元と合意した以下の監査の範囲及び監査手続きにより、U株式会社代表取締役○○　○○作成の200X年●月●日付言明書記載に対する情報セキュリティ対策の実施状況を監査した結果、監査結果表明のための合理的な証拠を得た。

委託元と合意した監査の範囲及び情報セキュリティ監査手続き：別紙

実施した監査手続		結果
【設計監査】管理策の必要性・十分性		—
言明書作成の正当性	【質問】言明書作成の目的、言明の根拠に関し、経営者に質問を行い、明確な根拠があることを確認する。 また、言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。 【閲覧】言明の根拠となる、言明書作成の経緯を記録した文書を閲覧し、経営者の回答と整合性が取れていることを確認する。 文書としては、以下のものを対象とする。 ・言明書作成に関わる会議の記録（情報セキュリティ委員会議事録、経営会議議事録、その他打合せ記録等）。 ・言明書作成の資料として用いたW社のコンサルティングの結果報告書。 ・ISMSなど公的な認証取得の文書を閲覧し、経営者が情報セキュリティマネジメントを的確に運用していることを確認する。	実施していると認められる
リスク把握の適切さ	【閲覧】対象業務フローに係るリスク分析を確認し、リスクが漏れなく、的確に洗い出されていることを確認する。 【視察】業務の現場を確認し、リスク分析で記述された脅威・ぜい弱性が十分であることを確認する。 【質問】業務現場の担当者に質問し、リスク分析が的確であることを確認する。 【質問】経営者にリスクに関して質問し、リスクが正しく認識されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。	実施していると認められる
管理策の適切さ	【閲覧】情報セキュリティ管理基準を参照して作成した個別管理基準に照らして、リスク分析によって洗い出されたリスクに対し、言明書において必要な管理策が網羅されていることを確認する。 【質問】経営者に管理策の内容を質問し、管理策として行うべきことが的確に記述されていることを確認する。 【質問】言明書の作成に関わった社内の責任者・担当者、及び外部委託先（コンサルティング会社W社）責任者及び担当者に質問し、経営者の質問と整合性があることを確認する。	実施していると認められる
【実装監査】	言明書どおりに運用が行われていることの確認	—
言明書の運用の確認	【質問】経営者と業務管理責任者に質問し、言明書に基づく管理を実施していることを確認する。 【閲覧】言明書どおりに管理策が組織全体で運用されていることを示す文書を閲覧し、組織的管理が行われていることを確認する。 ・情報セキュリティ委員会等の議事録。 ・詳細管理策策定後の運用状況を記録した文書。 【閲覧・質問】内部監査報告書を閲覧すると共に、内部監査人に質問し、適正な運用が行われていることを確認する。 ・詳細管理策運用に関する内部監査報告書。	実施していると認められる
・ （略） ・		

職務権限定義の適正さ	【閲覧】職務定義・及び職務任命に関する文書を閲覧し、適正な運用がなされているかを確認する。	実施していると認められる
	・対象業務に関わる区画及び重要情報資産へのアクセス権限を規定する職務及び責任範囲を明確にした職務定義書は適正な手順により作成・承認されているか。	実施していると認められる
	・職務定義書の内容は、以下の条件を満たしているか。	実施していると認められる
	・辞令で確実に職務権限の発令、停止が行われているか。	実施していると認められる
	・権限のたな卸しは、年1回経営者の責任において行われているか。	実施していると認められる
	【質問】業務責任者・現場担当者に質問し、記録が正しく行われていることを確認する。	実施していると認められる
	・一人が複数の権限を保有しないか。	実施していると認められる
	・一つの職務で同一の重要データに対する読取、書込み・変更、監視・監査の作業が分離されているか。各職務について、業務遂行上アクセスが必要な情報資産が全て網羅されているか。	実施していると認められる
	・各職務の情報資産に対するアクセス権限の内容が明確か。	実施していると認められる
	・ 緊急の必要により、職務定義書に定められた以外の作業や他の人の作業を兼務することが生じた場合の管理策があらかじめ定められているか。	実施していると認められる
	・職務定義書に定められた以外の作業においては、あらかじめ定められた管理策に基づき作業が行われているか。	実施していると認められる
	・全ての役員・社員等に、定められた権限以外のアクセスが禁止されているか。	実施していると認められる
	・組織・人事異動の際にも権限の重複がないよう運用されているか。	実施していると認められる
	・情報セキュリティ管理責任者が職務権限の設定と付与を行っているか。	実施していると認められる
	・情報セキュリティ管理責任者が権限の付与状況を少なくとも年1回定期的に見直しているか。	実施していると認められる
・ （略） ・		

4 グループ企業における利用者合意方式の保証型情報セキュリティ監査の利用例（2章 3 のX社の場合）

1 X社における保証型情報セキュリティ監査への取り組み

200X年に入り、X社グループ各社の情報セキュリティに関する理解度は深まり、情報セキュリティ対策ベンチマークの回答もブレが少なくなってきた。

3つのグループごとにみると、いずれのグループでもしっかりとした情報セキュリティマネジメントが行われていると考えられるトップ集団と、十分なマネジメントが運用できない企業とに二分されている状況にあった。

また、いくつかの企業で、評価を気にするあまり診断を甘めにする動きも生じているのではないかとの懸念が生じた。

このような状況から、更なる情報セキュリティ対策の向上を図るために、情報セキュリティ部長のY氏は、情報セキュリティ監査を行うことを企画した。具体的には、3グループのうち、中位以上のクラスの企業の中から数社を選び、保証型情報セキュリティ監査により、自己診断の結果が適正であるかを判断すること、及び、下位に低迷する企業については、助言型情報セキュリティ監査により対策の強化を図ることとした。

企業の選定についてどのように行うかが議論され、結果として、自ら情報セキュリティ監査を望む企業を3グループ各々から保証型情報セキュリティ監査・助言型情報セキュリティ監査各1社を選ぶと共に、無作為抽出で上位から1社保証型情報セキュリティ監査を、下位から1社助言型情報セキュリティ監査を行うことが決定された。

このY部長の提案は、グループ経営ミーティングで今年度の活動として認められ、年度の初めに各社に通知された。この通知を受けた後、自己診断が開始され、上半期に各社の診断結果が情報セキュリティ部に報告されてきた。

昨年度と比較すると数社で厳しめの診断をした跡が見える企業もあったが、全体的な傾向はそれほど変わらないものであった。

情報セキュリティ監査を依頼する企業は当初の想定よりも多かったため、抽選で各グループから各々2社を選定した。また、無作為抽出により各グループから2社ずつ抽出し、合計12社に対する情報セキュリティ監査を実施することとなった。

2 X社における保証型情報セキュリティ監査の導入

監査実施に当たって、X社は、監査目的を以下のように定めた。

(1)保証型情報セキュリティ監査にあっては、グループとして情報セキュリティ対策ベンチマークの項目ごとに客観的な評価基準を設け、それに達しているかを判断することにより、適正な自己診断が行えていることを明らかにする。

(2)助言型情報セキュリティ監査においては、3以下の水準にある項目について、情報セキュリティ管理基準に照らして、適切でない項目を検出し、どのような点を改善するのがよいかを明らかにする。

また、保証型情報セキュリティ監査は利用者合意方式とするが、被監査主体となる各社の顧客と合意をとるのは時間的に余裕がないことから、X社が利用者代表として監査手続きについて監査会社と合意することにした。

この目的のために、情報セキュリティ対策ベンチマークの項目を情報セキュリティ管理基準及びCOBIT 4.1[*4]など関連する基準を参考に、個別管理基準を作成し、情報セキュリティ監査を実施することが方針として決定された。

X社は、情報セキュリティ監査企業台帳に登録されており、JASA会員企業でもある監査会社の中から、実績のある数社にRFPを送付し、提案書作成を依頼した。その結果、個別管理基準の作成方法や監査手続きについて、すぐれた提案をした6社を選定し、各々のグループごとに、保証型情報セキュリティ監査と助言型情報セキュリティ監査を分けて監査を依頼することにした。

＊4 COBIT 4.1：COBIT（Control Objectives for Information and related Technology）はITGI（IT Governance Institute：ITガバナンス協会）が発行しているITカバナンス確立のための一連の資料やツールである。2008年9月現在のバージョンは4.1。

選定された6社は各々担当する被監査主体を訪問し、事前調査を踏まえてテーマを絞り、自社の情報セキュリティ強化に結びつく分野に重点を置いて情報セキュリティ監査を行うことになった。

情報セキュリティ監査が開始されてから、報告書を取りまとめるまでは、ほぼ順調に作業が進み、予定通り監査は終了した。

保証型情報セキュリティ監査を受けた6社のうち、4社は自己診断の結果とほぼ変わらない水準にあることが確認できた。

残りの1社は、自社が定義していた手順にあいまいな部分があった。現状は現場の責任者の判断で一見問題なく運用されていたが、マネジメント上では不備と指摘され、保証意見は留保された。また、残りの1社は、是正処置が手順どおりに行われていない事象が検出され、保証意見は述べられなかった。

助言型情報セキュリティ監査を受けた6社は、大きく2つのグループに分かれた。第一のグループは情報セキュリティマネジメントそのものの設計に問題のあるグループで、PDCAサイクルの理解が不十分であったため、基本的な規定・体制について改善提言を受けた。

第二のグループは基本的なフレームワークはできているが、管理策が不十分なため、ぜい弱性が残っている点について改善提言を受けることになった。

3 グループ全体の情報セキュリティの向上

情報セキュリティ監査を受ける各社の経営者や担当者は、当初、相当緊張し、また、監査人の判断に厳しく抵抗する姿もあった。

監査が進んでいくにつれて、監査人がどのような点を見るかが分かり、これら経営者や担当者は、情報セキュリティマネジメントに関する深い理解を得るようになってきた。

保証型情報セキュリティ監査により保証意見を得た企業は、情報セキュリティ報告書を作成し、保証された内容を可能な範囲で開示した。

情報システム部は、保証を受けた4社の情報セキュリティ責任者を講師とした勉強会をグループ内企業の情報セキュリティ責任者に対して開催した。この中で、情報セキュリティ対策の立案、言明書の作成、監査を受けるプロセス等について、突っ込んだ質疑応答がなされ、情報セキュリティマネジメントに対する理解をより一層深めることができた。

さらに、情報セキュリティ部は、助言型情報セキュリティ監査報告書に基づき、「情報セキュリティマネジメントの構築のコツ」を作成し、陥りやすい誤りを事例として整理した。企業名が分からないように、内容を架空の会社の話に置き換えているが、ドキュメンタリータッチで仕上げたものが好評で、一般社員にも広く読まれるようになった。

これらの活動を通じて、情報セキュリティマネジメントに対する全グループを通じた理解が深まった手ごたえを、Y部長は感じている。