資料2-1

「情報セキュリティ監査に関するガイドライン」改定案について

2014年12月16日

総務省
MIC Ministry of Internal Affairs and Communications

議論テーマと内容要約

項番	議論テーマ	論点内容要約	改定方針	論点整理表の項番※
1	監査人	監査人に求められる力量の観点が弱いため	監査人に求められる力量（知識及び技能等）を決定する際には、監査プロセスや個人の行動を考慮する	2
		監査人の選定・変更の観点が弱いため	監査を行う際には、監査人の評価基準を設定し、基準を満たさない場合は追加の訓練、業務経験等を積み、再評価を行う	10
		監査責任者の責任についての観点が弱いため	監査の責任者（情報セキュリティ監査統括責任者）に求められる責任や力量について追記を行う	13
2	監査計画	監査頻度の観点が弱いため	中期計画は、監査頻度についても考慮に入れて作成する	3
3	監査フロー	監査結果の評価の観点が弱いため	監査実施後、結果の評価と監査結論の作成について追記する	14
4	監査に関わるリスク	監査プログラムにおけるリスクの把握の観点が弱いため	監査計画を立てる際には、計画の策定、資源、監査チーム等に付随するリスクを考慮する必要があることを追記する	4

※凡例：赤数字＝管理強化、青数字＝明確化

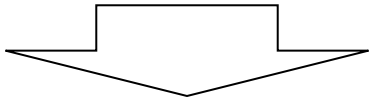
議論テーマと内容要約

項番	議論テーマ	論点内容要約	改定方針	論点整理表の項番※
5	監査手法	監査手法の最新化のため	監査手法に、現状の現地監査のほか、リモート監査についても記載する	5
		監査を実施するうえでの原則の観点が弱いため	監査人は、適切な原則、手段及び方法を適用することができる	6
6	監査報告	監査結果の内容の具体例がわかりにくいため	監査結果には、マネジメントシステムの有効性等を踏まえて作成する	7
		監査結果における評価の説明が弱いため	監査結果では、監査基準に対して適合または不適合を示し、指摘事項と合わせて優れた実践を含めることを追記する	8
		監査結果の報告内容に弱い点があったため	監査は、サンプリング監査であり、監査証拠は情報のサンプルであることを伝える	9
7	外部委託	外部委託事業者の選定の観点が弱いため	外部委託事業者が監査を担保できるような施策を行い、選定することを追記する	15

※凡例：赤数字＝管理強化、青数字＝明確化

議論テーマについての主なご意見

論点テーマ	ご意見
監査	**・実際に監査を実施している自治体が少ないのではないか。 ・監査の実施状況を確認したい。**



情報セキュリティ監査に関するガイドラインを参照するよう、情報セキュリティポリシーガイドライン「1.8 評価・見直し」の章に追記をしております。

1　監査人

※論点整理表：
項番2、10、13

論点1

※凡例：赤数字＝管理強化、青数字＝明確化

1（項番2）

（2.2.1 準備）

ISO等の考え方	【ISO19011:2011　7 監査員の力量及び評価】 ● 7.1 一般 監査プロセス及びその目的を達成するための能力に対する信頼は，監査員及び監査チームリーダーを含む，監査を計画し，実施する人の力量に依存する。力量は，個人の行動，並びに教育，業務経験，監査員訓練及び監査経験によって身に付けた，知識及び技能を適用する能力を考慮するプロセスを通じて評価することが望ましい。 ● 7.2.2　個人の行動 監査員は，箇条4 に示す監査の原則に従って行動するために必要な資質を備えていることが望ましい。監査員は，監査活動を実施している間，次の事項を含む専門家としての行動を示すことが望ましい。 － 倫理的である。すなわち，公正である，信用できる，誠実である，正直である，そして分別がある。 － 心が広い。すなわち，別の考え方又は視点を進んで考慮する。 － 外交的である。すなわち，目的を達成するように人と上手に接する。 － 観察力がある。すなわち，物理的な周囲の状況及び活動を積極的に観察する。 － 知覚が鋭い。すなわち，状況を認知し，理解できる。 － 適応性がある。すなわち，異なる状況に容易に合わせることができる。 － 粘り強い。すなわち，根気があり，目的の達成に集中する。 － 決断力がある。すなわち，論理的な理由付け及び分析に基づいて，時宜を得た結論に到達することができる。 － 自立的である。すなわち，他人と効果的なやりとりをしながらも独立して行動し，役割を果たすことができる。 － 不屈の精神をもって行動する。すなわち，その行動が，ときには受け入れられず，意見の相違又は対立をもたらすことがあっても，進んで責任をもち，倫理的に行動することができる。 － 改善に対して前向きである。すなわち，進んで状況から学び，よりよい監査結果のために努力する。 － 文化に対して敏感である。すなわち，被監査者の文化を観察し，尊重する。 － 協働的である。すなわち，監査チームメンバー及び被監査者の要員を含む他人と共に効果的に活動する。

1（項番2）（資料2-3：P11）

改定案（2.2.1 準備）

＜修正前＞

2.2. 監査手順

2.2.1. 準備

（1） 体制の整備

情報セキュリティ監査を実施するに当たり、まず、情報セキュリティ委員会は、「情報セキュリティ監査統括責任者」を指名し、情報セキュリティ監査を実施する責任者を明確にする（図表 2.2）。情報セキュリティ監査統括責任者は、情報セキュリティ監査に関わる責任と権限を有する。情報セキュリティ監査統括責任者は、組織全体の監査に責任を負うため、地方公共団体の長に準じる権限と責任を有する者とすることが望ましい。

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

＜修正後＞

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。

さらに、監査プロセスや目的を達成するための能力は、内部監査人の資質に依存する。そのため、内部監査人として適当であるかを評価し、不足がある場合は必要に応じて内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

1（項番2）（資料2-3：P12）

改定案（2.2.1 準備）

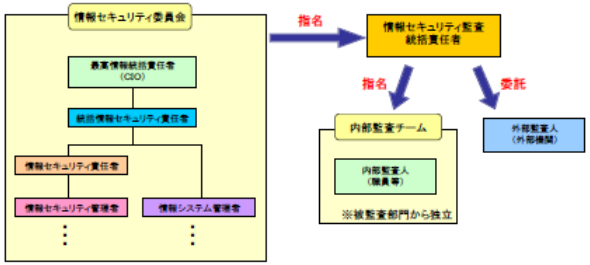
＜修正前＞

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

図表 2.2　情報セキュリティ監査の実施体制（例）



＜修正後＞

図表2.3　内部監査人に必要な資質

	項目	内容
1	倫理的である	公正であり、正直である
2	心が広い	別の考え方や視点を取り入れることができる
3	外交的である	人と上手に接することができる
4	観察力がある	周囲の状況や活動を積極的に観察する
5	知覚が鋭い	状況を察知し、理解できる
6	適応性がある	異なる状況に容易に合わせることができる
7	粘り強い	根気があり、目的の達成に集中する
8	決断力がある	論理的な理由づけや分析により、結論に到達することができる
9	自立的である	他人とやりとりしながらも独立して行動し、役割を果たすことが出来る
10	不屈の精神をもって行動する	意見の相違や対立があっても、進んで責任をもち、倫理的に行動できる
11	改善に対して前向きである	進んで状況から学び、よりよい監査結果のために努力する
12	文化に対して敏感である	被監査者の文化を観察し、尊重する
13	協働的である	他人と共に効果的に活動する

1（項番10）

（2.2.1 準備）

ISO等の考え方

【ISO19011:2011　7 **監査員の力量及び評価**】

- 7.4 **監査員の適切な評価方法の選定**

評価は，表2 に示す方法のうちの複数を利用して行うことが望ましい。表2 を利用するときは，次の事項に注意することが望ましい。

－ 表2 に示す方法は，様々な選択肢の中の代表的なものであり，全ての状況に適用できるとは限らない。

－ 表2 に示す様々な方法の信頼性は，それぞれ異なる場合がある。

－ 評価結果が客観的で，一貫性をもち，公正で，かつ，信頼できることを確実にするために複数の方法を組み合わせて用いることが望ましい

表 2－評価方法の例

評価方法	目的	例
記録のレビュー	監査員の経歴を検証する。	教育，訓練，雇用，職業資格及び監査経験の記録の解析
フィードバック	監査員のパフォーマンスがどのように受け止められているかに関する情報を与える。	調査，質問票，照会状，感謝状，苦情，パフォーマンス評価，相互評価
面接	個人の行動及び意思疎通の技能を評価し，情報を検証し，知識を試験し，並びに追加情報を得る。	個人面接
観察	個人の行動，並びに知識及び技能を適用する能力を評価する。	ロールプレイ，立会い監査，業務中のパフォーマンス
試験	個人の行動，並びに知識，技能及びそれらの適用を評価する。	口頭及び筆記試験，心理試験
監査後のレビュー	監査活動中の監査員のパフォーマンスに関する情報を与え，強み・弱みを特定する。	監査報告書のレビュー，監査チームリーダー，監査チームとの面接，適切な場合は被監査者からのフィードバック

1（項番10）（資料2-3：P11）

改定案（2.2.1 準備）

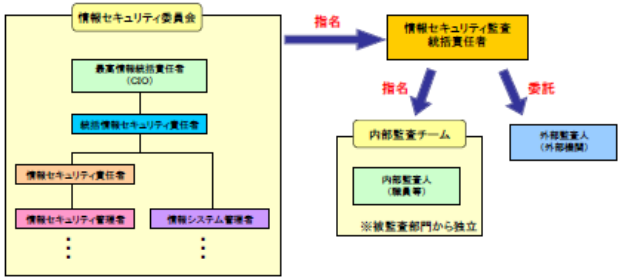
＜修正前＞

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

図表 2.2　情報セキュリティ監査の実施体制（例）



＜修正後＞

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

内部監査人の評価の方法については、以下のような方法から複数を組み合わせて行うことが望ましい。

- **記録のレビュー　：教育等の記録を確認し、監査人の経歴を検証する**
- **フィードバック　：監査パフォーマンスに関する苦情等の情報を与える**
- **面接　：監査人と面接し、監査人の情報を得る**
- **観察　：立ち合い監査等により知識及び技能を評価する**
- **試験　：筆記試験を行い、行動、知識及び技能を評価する**
- **監査後のレビュー　：監査報告書等をレビューし、強み・弱みを特定する**

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

1（項番13）

（2.2.1 準備）

ISO等の考え方	【ISO19011:2011　5.3.2 監査プログラムの管理者の力量】 ● 監査プログラムの管理者は，監査プログラム及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な力量，並びに次の領域における知識及び技能を備えていることが望ましい。 － 監査の原則，手順及び方法 － マネジメントシステム規格及び基準文書 － 被監査者の活動，製品及びプロセス － 被監査者の活動及び製品に関し，適用される法的及びその他の要求事項 － 該当する場合には，被監査者の顧客，供給者及びその他の利害関係者 ● 監査プログラムの管理者は，監査プログラムを管理するのに必要な知識及び技能を維持するために適切な専門能力の継続的開発活動に積極的に関わることが望ましい。

1（項番13）（資料2-3：P11）

改定案（2.2.1 準備）

＜修正前＞

2.2. 監査手順

- 2.2.1. 準備
- （1） 体制の整備

情報セキュリティ監査を実施するに当たり、まず、情報セキュリティ委員会は、「情報セキュリティ監査統括責任者」を指名し、情報セキュリティ監査を実施する責任者を明確にする（図表 2.2）。情報セキュリティ監査統括責任者は、情報セキュリティ監査に関わる責任と権限を有する。情報セキュリティ監査統括責任者は、組織全体の監査に責任を負うため、地方公共団体の長に準じる権限と責任を有する者とすることが望ましい。

情報セキュリティ監査統括責任者は、内部監査人を指名して内部監査チームの編成や、外部監査人への委託により、情報セキュリティ監査の体制を整備する。

内部監査人は、公平な立場で客観的に監査を行うことができるよう、被監査部門（監査を受ける部門）から独立した者を指名しなければならない。また、監査及び情報セキュリティについて、専門的知識を有するものでなければならない。そのため、必要に応じ内部監査人として必要な知識について研修を実施したり、外部で行われる研修に派遣することが適当である。内部監査人は、監査担当部門の職員があたる場合もあるが、情報システムを所管する課の職員に他の情報システム所管課の内部監査を行わせる方法（相互監査）も有効である。

なお、規模の小さい地方公共団体においては、最高情報統括責任者（CIO）が情報セキュリティ監査統括責任者を兼務したり、内部監査チームの職員等も他の業務と兼務せざるを得ないことも考えられる。この場合においても、監査を実施する者は、自らが直接担当する業務やシステムの監査を実施させないなど、監査の客観性の確保を図る必要がある。

＜修正後＞

(1) 体制の整備

情報セキュリティ監査を実施するに当たり、まず、情報セキュリティ委員会は、「情報セキュリティ監査統括責任者」を指名し、情報セキュリティ監査を実施する責任者を明確にする（図表2.2）。情報セキュリティ監査統括責任者は、情報セキュリティ監査に関わる責任と権限を有する。情報セキュリティ監査統括責任者は、組織の監査全体に責任を負うため、地方公共団体の長に準じる権限と責任を有する者とすることが望ましい。

情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質、並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、並びに知識及び技能を有することが困難な場合は、外部の専門家を充てて能力を補完することも考えられる。

- **監査の原則、手順及び方法に関する知識**
- **マネジメントシステム規格及び基準文書に関する知識**
- **被監査部門の活動、製品及びプロセスに関する知識**
- **被監査部門の活動及び製品に関し、適用される法的及びその他の要求事項に関する知識**
- **該当する場合には、被監査部門の利害関係者に関する知識**

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適切な専門能力の継続的開発・維持活動に積極的に関わることが望ましい。

2　監査計画

※論点整理表：
項番3

論点2

※凡例：赤数字＝管理強化、青数字＝明確化

2（項番３）

（2.2.2 監査計画）

ISO等の 考え方	【ISO/IEC27001:2013　9.2 内部監査】 ●組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。 a) 次の事項に適合している。 1) ISMS に関して，組織自体が規定した要求事項 2) この規格の要求事項 b) 有効に実施され，維持されている

2（項番3）（資料2-3：P15）

改定案（2.2.2 監査計画）

＜修正前＞

2.2.2. 監査計画

情報セキュリティ監査を効率的かつ効果的に行うために、情報セキュリティ監査を実施する計画を策定する。一般に、監査計画には、「中期計画」、「年度計画」、及び個々の「監査実施計画」がある。計画段階では、中期計画及び年度計画を策定する（図表 2.4）。

図表 2.4　情報セキュリティ監査計画策定の流れ

（1） 中期計画の策定と承認

情報セキュリティ監査の対象は広範囲に及ぶことから、一回の監査や単年度内ですべてを網羅することはできない。したがって、一定の期間（例えば、3年程度）を見据えた計画が必要となる。中期計画は、この期間における情報セキュリティ監査の方針や実施目標、監査範囲、大まかな実施時期等の項目を記述した文書であり、情報セキュリティ監査に関する中期的な方針を示すものである。

なお、期間中であっても、地方公共団体の置かれている環境の変化や監査実施計画自体の進捗状況により、見直しを行う必要がある。中期計画は策定・見直しの都度、情報セキュリティ委員会の承認を得る必要がある。

また、規模の小さい地方公共団体においては、監査の対象規模が相対的に大きくないことから、年度計画のみを作成するなど簡素化することも考えられる。

＜修正後＞

（1） 中期計画の策定と承認

情報セキュリティ監査の対象は広範囲に及ぶことから、一回の監査や単年度内ですべてを網羅することはできない。したがって、一定の期間（例えば、3年程度）を見据えた計画が必要となる。中期計画は、この期間における情報セキュリティ監査の方針や実施目標、監査範囲、大まかな実施時期等の項目を記述した文書であり、情報セキュリティ監査に関する中期的な方針を示すものである。この計画には、一定の期間内での監査の頻度についても記述しておく。

なお、期間中であっても、地方公共団体の置かれている環境の変化や監査実施計画自体の進捗状況により、見直しを行う必要がある。中期計画は策定・見直しの都度、情報セキュリティ委員会の承認を得る必要がある。

また、規模の小さい地方公共団体においては、監査の対象規模が相対的に大きくないことから、年度計画のみを作成するなど簡素化することも考えられる。

3　監査フロー

※論点整理表：
項番14

論点3

※凡例：赤数字＝管理強化、青数字＝明確化

3（項番14）

（2.2.3 監査実施）

ISO等の考え方	【ISO19011:2011　6.4.7 監査所見の作成】 ● 監査所見を決定するために，監査基準に照らして監査証拠を評価することが望ましい。監査所見では，監査基準に対して適合又は不適合のいずれかを示すことができる。監査計画で規定されている場合には，個々の監査所見には，根拠となる証拠，改善の機会，並びに被監査者に対する提言全てとともに適合性及び優れた実践を含めることが望ましい。 ● 不適合及びその根拠となる監査証拠は，記録しておくことが望ましい。不適合は，格付けしてもよい。不適合は，被監査者と確認することが望ましい。この確認作業の目的は，監査証拠が正確であること，及び不適合の内容が理解されたことについて被監査者に認めてもらうことである。監査証拠又は監査所見に関して意見の相違がある場合には，それを解決するためのあらゆる努力を試みることが望ましい。解決できない点は，記録しておくことが望ましい。 ● 監査中の適切な段階で監査所見をレビューするために，監査チームは，必要に応じて打合せをすることが望ましい。 【ISO19011:2011　6.4.8 監査結論の作成】 ● 監査結論では，次の事項を扱うことができる。 － 監査基準への適合の程度及びマネジメントシステムの頑健さ。これには，明示された目的に見合うマネジメントシステムの有効性を含む。 － マネジメントシステムの効果的実施，維持及び改善 － マネジメントシステムが引き続き適切，妥当，有効で，かつ，改善が継続することを確実にするためのマネジメントレビュープロセスの能力

3（項番14）（資料2-3：P19）

改定案（2.2.3 監査実施）

＜修正前＞

2.2.3. 監査実施

アンケートがある。
・レビュー　：文書や記録等の監査資料を入手し、内容を確認する
・インタビュー　：担当者等に質問し、状況を確認する
・視察　：業務を行っている場所や状況を見て確認する
・アンケート　：質問書への回答から実態を確認する
具体的な監査方法については、本ガイドラインの「第 3 章　情報セキュリティ監査項目」の監査チェックリストにおいて、監査項目毎に、監査資料の例、監査実施の例を示している。また、レビューで確認すべき文書や記録等については、付録に「監査資料例一覧／索引」としてとりまとめているので、参考にされたい。
情報セキュリティ監査の実施中、情報セキュリティ監査統括責任者は、監査人による監査業務の実施状況について随時報告を求める等、適切な管理を行う必要がある。また、監査人が作成した監査調書は、脆弱性の情報など漏えいした場合に当該地方公共団体の情報セキュリティに脅威となる情報も含むことから、情報セキュリティ監査統括責任者は、紛失等が生じないように適切に保管する必要がある。

③監査結果の取りまとめ
情報セキュリティ監査統括責任者は、実施した監査の内容を踏まえて、監査結果、確認した監査証拠、指摘事項、改善案等、監査結果を取りまとめる。具体的には、例えば、図表 1.5 の監査チェックリストに記入する。
また、監査結果については、必要に応じ、事実誤認がないかどうかを被監査部門に確認する。

＜修正後＞

④監査結果の評価
情報セキュリティ監査統括責任者は、監査基準に照らして監査結果を評価する。監査結果では、監査基準に対して適合又は指摘事項のいずれかを示すことができる。監査計画で規定されている場合には、個々の監査結果には、根拠となる証拠、改善の機会、並びに被監査部門に対する提言全てとともに適合性及び優れた実践を含めることが望ましい。
指摘事項については、監査証拠が正確であること及び指摘事項の内容が理解されたことについて認めてもらうために、被監査部門と確認することが望ましい。
また、指摘事項がある場合、個々のセキュリティ対策の有効性のほか、監査におけるマネジメントシステム全体の有効性についても考察したうえで監査結論を作成することが望ましい。

4　監査に関わるリスク

※論点整理表：
項番4

論点4

※凡例：赤数字＝管理強化、青数字＝明確化

4（項番4）

（2.2.3 監査実施）

ISO等の 考え方	【ISO19011:2011　5.3.4 監査プログラムに関わるリスクの特定及び評価】 ● 監査プログラムの策定，実施，監視，レビュー及び改善に付随した，監査プログラムの目的の達成に影響を及ぼし得る，多くの異なったリスクがある。監査プログラムの管理者は，その作成において，これらのリスクを考慮することが望ましい。これらのリスクは，次の事項に付随する可能性がある。 － 計画の策定。例えば，監査目的の設定及び監査プログラムを適用する範囲の決定が適切でない。 － 資源。例えば，監査プログラムの策定又は監査の実施に十分な時間が割けない。 － 監査チームの選定。例えば，チームとして監査を効果的に実施するための力量を備えていない。 － 実施。例えば，監査プログラムに関するコミュニケーションが効果的でない。 － 記録及びその管理。例えば，監査プログラムの有効性を実証するための監査記録の保護が十分でない。 － 監査プログラムの監視，レビュー及び改善。例えば，監査プログラムの成果が効果的に監視されていない。

4（項番4）（資料2-3：P17）

改定案（2.2.3 監査実施）

＜修正前＞

- 2.2.3. 監査実施
- （1） 監査実施計画の策定と承認

情報セキュリティ監査統括責任者は、年度計画に基づいて、内部監査人又は外部監査人に指示して具体的な監査実施計画を策定する（図表 2.5）。

監査実施計画書中、監査項目は、例えば、本ガイドライン「第 3章　情報セキュリティ監査項目」の大分類や中分類のレベルを記載するとよい。また、適用基準には、例えば、付録の「情報セキュリティ監査業務委託仕様書（例）」の適用基準を参考に記載するとよい。

図表 2.5　情報セキュリティ監査実施計画書に記載する事項（例）

	項目	内容
1	監査目的	監査を実施する目的
2	監査テーマ	監査の具体的なテーマや重点監査事項
3	監査範囲	監査対象の業務、情報システム等の範囲
4	被監査部門	監査の対象となる部門
5	監査方法	監査で適用する監査技法
6	監査実施日程	監査の計画から報告までの日程
7	監査実施体制	監査担当者
8	監査項目	監査で確認する大項目
9	適用基準	監査で適用する基準等

情報セキュリティ監査統括責任者は、監査実施計画書を、組織として受け入れ、監査実施の責任と権限を明確にするため、情報セキュリティ委員会による承認を得る。また、情報セキュリティ委員会の承認を得た後に、被監査部門に対して十分に説明する機会を設け、監査スケジュールを被監査部門へ伝え、担当者の選出、監査資料の準備等の事項の依頼など、効率的に監査を実施するための調整を行う。

＜修正後＞

(1) 監査実施計画の策定と承認

情報セキュリティ監査統括責任者は、年度計画に基づいて、内部監査人又は外部監査人に指示して具体的な監査実施計画を策定する（図表2.6）。

監査においては、内部監査人の資質や業務に応じた監査実施時期を考慮して実施計画を立てることが望ましい。

監査実施計画書中、監査項目は、例えば、本ガイドライン「第3章　情報セキュリティ監査項目」の大分類や中分類のレベルを記載するとよい。また、適用基準には、例えば、付録の「情報セキュリティ監査業務委託仕様書（例）」の適用基準を参考に記載するとよい。

5　監査手法

※論点整理表：
項番5、6

論点5

※凡例：赤数字＝管理強化、青数字＝明確化

5（項番５）

（2.2.3 監査実施）

ISO等の考え方	【ISO19011:2011　附属書B　監査を計画及び実施する監査員に対する追加の手引き】 B.1 監査方法の適用 　監査は多用な監査方法を利用して実行し得る。この附属書に，一般的に利用される監査方法の説明を示す。監査のために選ばれる監査方法は，定められた監査の目的，適用範囲及び基準，並びに期間及び場所による。利用可能な監査員の力量及び監査方法の適用に起因する不確かさも考慮することが望ましい。多様な監査方法及びそれらの組合せの適用により，監査プロセス及びその成果の有効性及び効率を最適化し得る。 　監査のパフォーマンスは，監査の対象となるマネジメントシステムの個々人及び監査の実施に利用される技術の相互作用を含む。表B.1 は，監査目的を達成するために，単独に，又は組み合わせて利用し得る監査方法の例を示す。監査が複数のメンバーをもつ監査チームの利用を伴う場合，現地監査及びリモート監査の両方が同時に利用されることがある。

5（項番5）（資料2-3：P18～19）

改定案（2.2.3 監査実施）

＜修正前＞

②監査の実施

監査人は、監査チェックリストに基づいて情報セキュリティ監査を実施し、監査調書を作成する。主な監査技法には、レビュー、インタビュー、視察、

アンケートがある。

- ・レビュー　：文書や記録等の監査資料を入手し、内容を確認する
- ・インタビュー　：担当者等に質問し、状況を確認する
- ・視察　：業務を行っている場所や状況を見て確認する
- ・アンケート　：質問書への回答から実態を確認する

具体的な監査方法については、本ガイドラインの「第 3 章　情報セキュリティ監査項目」の監査チェックリストにおいて、監査項目毎に、監査資料の例、監査実施の例を示している。また、レビューで確認すべき文書や記録等については、付録に「監査資料例一覧／索引」としてとりまとめているので、参考にされたい。

情報セキュリティ監査の実施中、情報セキュリティ監査統括責任者は、監査人による監査業務の実施状況について随時報告を求める等、適切な管理を行う必要がある。また、監査人が作成した監査調書は、脆弱性の情報など漏えいした場合に当該地方公共団体の情報セキュリティに脅威となる情報も含むことから、情報セキュリティ監査統括責任者は、紛失等が生じないように適切に保管する必要がある。

＜修正後＞

②監査の実施

監査人は、監査チェックリストに基づいて情報セキュリティ監査を実施し、監査調書を作成する。主な監査技法には、レビュー、インタビュー、視察、アンケートがある。これらの 監査技法は、被監査部門の所在場所にて実施する現地監査のほか、被監査部門の所在場所に行かずに行うリモート監査でも用いることができる。

- ・レビュー　：文書や記録等の監査資料を入手し、内容を確認する
- ・インタビュー　：担当者等に質問し、状況を確認する
- ・視察　：業務を行っている場所や状況を見て確認する
- ・アンケート　：質問書への回答から実態を確認する

具体的な監査方法については、本ガイドラインの「第 3 章　情報セキュリティ監査項目」の監査チェックリストにおいて、監査項目毎に、監査資料の例、監査実施の例を示している。また、レビューで確認すべき文書や記録等

5（項番6）

（2.2.3 監査実施）

ISO等の考え方	【ISO19011:2011　7.2.3.2 マネジメントシステム監査員の共通の知識及び技能】 a) 監査の原則，手順及び方法：この領域の知識及び技能によって，監査員は，適切な原則，手順及び方法を異なる監査に適用すること，及び一貫性のある体系的な監査を確実に行うことが可能となる。監査員は，次の事項ができることが望ましい。 － 監査の原則，手順，及び方法を適用する。 － 効果的に作業を計画し，必要な手配をする。 － 合意した日程内で監査を行う。 － 重要事項を優先し，重点的に取り組む。 － 効果的な面談，聞き取り，観察，並びに文書，記録及びデータの調査によって，情報を収集する。 － 専門家の意見を理解し，検討する。 － 監査のためにサンプリング技法を使用することの適切性及びそれによる結果を理解する。 － 収集した情報の関連性及び正確さを検証する。 － 監査所見及び監査結論の根拠とするために，監査証拠が十分かつ適切であることを確認する。 － 監査所見及び監査結論の信頼性に影響する可能性がある要因を評価する。 － 監査活動を記録するために作業文書を用いる。 － 監査所見を文書化し，適切な監査報告書を作成する。 － 情報，データ，文書及び記録の機密及びセキュリティを維持する。 － 口頭又は書面で効果的に意思の疎通を図る（自身で，又は通訳及び翻訳の利用を通じて）。 － 監査に付随するリスクの種類を理解する。

5（項番６）（資料2-3：P19）

改定案（2.2.3 監査実施）

＜修正前＞

・レビュー　　：文書や記録等の監査資料を入手し、内容を確認する
・インタビュー　：担当者等に質問し、状況を確認する
・視察　　：業務を行っている場所や状況を見て確認する
・アンケート　：質問書への回答から実態を確認する

具体的な監査方法については、本ガイドラインの「第 3 章　情報セキュリティ監査項目」の監査チェックリストにおいて、監査項目毎に、監査資料の例、監査実施の例を示している。また、レビューで確認すべき文書や記録等については、付録に「監査資料例一覧／索引」としてとりまとめているので、参考にされたい。

情報セキュリティ監査の実施中、情報セキュリティ監査統括責任者は、監査人による監査業務の実施状況について随時報告を求める等、適切な管理を行う必要がある。また、監査人が作成した監査調書は、脆弱性の情報など漏えいした場合に当該地方公共団体の情報セキュリティに脅威となる情報も含むことから、情報セキュリティ監査統括責任者は、紛失等が生じないように適切に保管する必要がある。

③監査結果の取りまとめ

情報セキュリティ監査統括責任者は、実施した監査の内容を踏まえて、監査結果、確認した監査証拠、指摘事項、改善案等、監査結果を取りまとめる。具体的には、例えば、図表 1.5 の監査チェックリストに記入する。

また、監査結果については、必要に応じ、事実誤認がないかどうかを被監査部門に確認する。

＜修正後＞

情報セキュリティ監査の実施中、情報セキュリティ監査統括責任者は、監査人による監査業務の実施状況について随時報告を求める等、適切な管理を行う必要がある。また、監査人が作成した監査調書は、脆弱性の情報など漏えいした場合に当該地方公共団体の情報セキュリティに脅威となる情報も含むことから、情報セキュリティ監査統括責任者は、紛失等が生じないように適切に保管する必要がある。

また、監査人は監査業務上知り得た情報や監査内容を関係者以外に開示したり、情報が漏えいしないよう、セキュリティを維持する必要がある。

③監査結果の取りまとめ

情報セキュリティ監査統括責任者は、実施した監査の内容を踏まえて、監査結果、確認した監査証拠、指摘事項、改善案等、監査結果を取りまとめる。具体的には、例えば、図表 1.5 の監査チェックリストに記入する。

また、監査結果については、必要に応じ、事実誤認がないかどうかを被監査部門に確認する。

6 監査報告

※論点整理表：
項番7、8、9

論点6

※凡例：赤数字＝管理強化、青数字＝明確化

6（項番7）

（2.2.4 監査報告）

ISO等の考え方	【ISO19011:2011　6.4.8 監査結論の作成】 ● 監査結論では，次の事項を扱うことができる。 － 監査基準への適合の程度及びマネジメントシステムの頑健さ。これには，明示された目的に見合うマネジメントシステムの有効性を含む。 － マネジメントシステムの効果的実施，維持及び改善 － マネジメントシステムが引き続き適切，妥当，有効で，かつ，改善が継続することを確実にするためのマネジメントレビュープロセスの能力 － 監査目的の達成，監査範囲の網羅性，及び監査基準の達成 － 監査計画に含まれている場合，所見に関する根本原因 － 傾向を特定する目的で監査された異なる領域における同様の所見

6（項番7）（資料2-3：P21）

改定案（2.2.4 監査報告）

＜修正前＞

2.2.4. 監査報告

（1） 監査報告書の作成

情報セキュリティ監査統括責任者は、監査調書に基づいて、被監査部門に対する指摘事項や改善案を含む監査報告書を作成する（図表 2.6）。

また、詳細な監査結果や補足資料等がある場合は、監査報告書の添付資料としてもよい。

図表 2.6 情報セキュリティ監査報告書に記載する事項（例）

	項目	内容
1	監査目的	監査を実施した目的
2	監査テーマ	監査の具体的なテーマや重点監査事項
3	監査範囲	監査対象の業務、情報システムなどの範囲
4	被監査部門	監査の対象とした部門
5	監査方法	監査で適用した監査技法
6	監査実施日程	監査の計画から報告までの日程
7	監査実施体制	監査を実施した担当者
8	監査項目	監査で確認した大項目
9	適用基準	監査で適用した基準等
10	監査結果概要（総括）	監査結果の総括
11	監査結果	監査で確認した事実（評価できる事項を含む）
12	指摘事項	監査結果に基づき、問題点として指摘する事項
13	改善勧告	指摘事項を踏まえて、改善すべき事項（緊急改善事項、一般的改善事項）
14	特記事項	その他記載すべき事項

（2） 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報セキュリティ委員会に報

＜修正後＞

2.2.4. 監査報告

（1） 監査報告書の作成

情報セキュリティ監査統括責任者は、監査調書に基づいて、被監査部門に対する指摘事項や改善案を含む監査報告書を作成する（図表 2.6）。

また、詳細な監査結果や補足資料等がある場合は、監査報告書の添付資料としてもよい。監査報告書で は、監査項目への適合の程度や、図表2.1にあるセキュリティ監査手順の運用サイクルが有効に機能しているかの観点を取り入れることが望ましい。

図表 2.6 情報セキュリティ監査報告書に記載する事項（例）

	項目	内容
1	監査目的	監査を実施した目的
2	監査テーマ	監査の具体的なテーマや重点監査事項
3	監査範囲	監査対象の業務、情報システムなどの範囲
4	被監査部門	監査の対象とした部門
5	監査方法	監査で適用した監査技法
6	監査実施日程	監査の計画から報告までの日程
7	監査実施体制	監査を実施した担当者
8	監査項目	監査で確認した大項目

6（項番8、9）

（2.2.4 監査報告）

ISO等の考え方	【ISO19011:2011　6.4.7 監査所見の作成】 ● 監査所見を決定するために，監査基準に照らして監査証拠を評価することが望ましい。監査所見では，監査基準に対して適合又は不適合のいずれかを示すことができる。監査計画で規定されている場合には，個々の監査所見には，根拠となる証拠，改善の機会，並びに被監査者に対する提言全てとともに適合性及び優れた実践を含めることが望ましい。 【ISO19011:2011　6.4.9 最終会議の実施】 ● 詳細の程度は，監査プロセスへの被監査者の親密度と合致したものであることが望ましい。監査によっては，最終会議が正式なものとなり得る。その場合には，出席者の記録を含めて議事録を残すことが望ましい。その他の場合，例えば内部監査では，最終会議はより非公式で，単に監査所見及び監査結論を伝えるだけでもよい。 ● 該当する場合，最終会議では次の事項を被監査者に説明することが望ましい。 － 集められた監査証拠は入手可能な情報のサンプルによることを伝える。 － 報告の方法 － 監査所見及び起こり得る結果の取扱いに関するプロセス － 被監査者の経営層が理解し，認めるような方法での監査所見及び監査結論の報告 － 関連する監査後の活動全て（例えば，是正処置の実施，監査に関する苦情対応，異議申立てのプロセス）

6（項番8、9）（資料2-3：P21）

改定案（2.2.4 監査報告）

＜修正前＞

	項目	内容
1	監査目的	監査を実施した目的
2	監査テーマ	監査の具体的なテーマや重点監査事項
3	監査範囲	監査対象の業務、情報システムなどの範囲
4	被監査部門	監査の対象とした部門
5	監査方法	監査で適用した監査技法
6	監査実施日程	監査の計画から報告までの日程
7	監査実施体制	監査を実施した担当者
8	監査項目	監査で確認した大項目
9	適用基準	監査で適用した基準等
10	監査結果概要（総括）	監査結果の総括
11	監査結果	監査で確認した事実（評価できる事項を含む）
12	指摘事項	監査結果に基づき、問題点として指摘する事項
13	改善勧告	指摘事項を踏まえて、改善すべき事項 （緊急改善事項、一般的改善事項）
14	特記事項	その他記載すべき事項

（2） 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報セキュリティ委員会に報告する。

また、被監査部門に対して監査報告会を開催し、監査人から直接、監査結果の説明を行う。監査人は、指摘事項をより具体的にわかりやすく説明し、必要に応じ「監査調書」の内容等、監査証拠に基づいた改善のための方策等を助言することが望ましい。

＜修正後＞

（2） 監査結果の報告

情報セキュリティ監査統括責任者は、監査結果を情報セキュリティ委員会に報告する。

また、被監査部門に対して監査報告会を開催し、監査人から直接、監査結果の説明を行う。監査人は、指摘事項をより具体的にわかりやすく説明し、必要に応じ「監査調書」の内容等、監査証拠に基づいた改善のための方策等を助言することが望ましい。さらに、指摘事項の説明だけでなく、被監査部門の優れた実践活動を報告会で評価することが望ましい。

監査報告会では、被監査部門に対して次の事項を説明することが望ましい。

- **集められた監査証拠は入手可能な情報のサンプルによること。**
- **監査報告の方法**
- **監査後の活動について（是正処置の実施、監査結果に対する意見対応等）**

7　外部委託

※論点整理表：
項番15

論点7

※凡例：赤数字＝管理強化、青数字＝明確化

総務省
MIC Ministry of Internal Affairs and Communications

7（項番15）

（2.3 外部監査人の調達）

ISO等の考え方	【府省庁対策基準策定のためのガイドライン　2.3.2 情報セキュリティ監査】 ● 情報セキュリティ監査責任者は、監査を実施するに当たり、府省庁内に情報セキュリティ監査実施者が不足している場合又は監査遂行能力が不足している場合には、監査業務（内部監査）を外部事業者に請け負わせることを検討すべきである。その委託先の選定に当たっては、被監査部門との独立性を有し、かつ監査遂行能力がある者を選択できるよう配慮することが重要である。また、監査業務を外部事業者に請け負わせることは、外部委託に該当することから、関連する規定にも留意する必要がある。また、情報セキュリティ監査企業台帳に登録されている企業や情報セキュリティ監査人資格者の業務への関与等を考慮することが望ましい。

7（項番15）（資料2-3：P26）

改定案（2.3 外部監査人の調達）

＜修正前＞

2.3. 外部監査人の調達

ここでは、外部監査を行う場合における外部監査人の調達方法について説明する。なお、県と県内市町村など、複数の地方公共団体が共同で外部監査人の調達を行うことによって、調達を効率化する方法もあり、実際にこのような取組も行われている。

（１） 外部監査人の調達方式

外部監査人の調達は、当該地方公共団体の調達基準や手続にしたがって行われるが、特に、監査の客観性、公正性等の観点から、委託業者の決定の透明性と公平性の確保には特に留意する必要がある。

外部監査の委託業者の調達方式には、次のような方式がありえる。

- 公募型プロポーザル方式（企画提案書を評価して判断して事業者を選定）
- 総合評価入札方式（価格と技術的要素を総合的に判断して事業者を選定）
- 一般競争入札方式（最も安価な価格を提示した事業者と契約）
- 条件付き一般競争入札方式（一定の条件を満たす事業者の中で、最も安価な価格を提示した事業者と契約）

（２） 企画提案書の書式作成

公募型プロポーザル方式により情報セキュリティ監査に関する企画提案を求める場合は、「企画提案書」を作成する。企画提案書には、情報セキュリティ監査業務の受託を希望する提案者が、業務委託仕様書に基づいて、当該監査に関する考え方、実施方法、実施体制等の具体的な内容を記述する（図表 2.7）。また、委託業務内容に加えて、費用の見積りに必要となる事項も併せて記載する。例えば、ネットワークへの侵入検査を行う場合には、対象サーバ数や IP アドレス数などの対象、範囲、実施の程度等の詳細な記載があれば、企画提案者の費用積算は精緻なものになり、より正確な見積りが期待できる。

図表 2.7　企画提案書に記載する事項（例）

	項目	内容
1	監査期間	委託する監査の期間
2	監査実施内容	委託する監査業務の内容 ⅰ）目的 ⅱ）本業務の対象範囲 ⅲ）準拠する基準 ⅳ）監査のポイント　等

＜修正後＞

（２） 企画提案書の書式作成

公募型プロポーザル方式により情報セキュリティ監査に関する企画提案を求める場合は、「企画提案書」を作成する。企画提案書には、情報セキュリティ監査業務の受託を希望する提案者が、業務委託仕様書に基づいて、当該監査に関する考え方、実施方法、実施体制等の具体的な内容を記述する（図表 2.7）。また、委託業務内容に加えて、費用の見積りに必要となる事項も併せて記載する。例えば、ネットワークへの侵入検査を行う場合には、対象サーバ数や IP アドレス数などの対象、範囲、実施の程度等の詳細な記載があれば、企画提案者の費用積算は精緻なものになり、より正確な見積りが期待できる。

情報 セキュリティ監査統括責任者は、外部委託事業者による監査に責任を持つ必要がある。このため、企画提案書の内容を確認し、監査の品質を担保できる外部委託事業者を選定することが求められる。

図表 2.7　企画提案書に記載する事項（例）

	項目	内容
1	監査期間	委託する監査の期間
2	監査実施内容	委託する監査業務の内容 ⅰ）目的 ⅱ）本業務の対象範囲 ⅲ）準拠する基準 ⅳ）監査のポイント　等

7（項番15）（資料2-3：P27）

改定案（2.3 外部監査人の調達）

＜修正前＞

3	監査内容	ⅰ）事前打合せ ⅱ）事前準備依頼事項 ・事前の提出資料 ・アンケート等の有無　等 ⅲ）監査実施計画書作成 ⅳ）予備調査 ⅴ）本調査 ※機器又は情報システムに対して情報システム監査ツールを使用する場合はその名称も記載 ⅵ）監査報告書作成 ⅶ）監査報告会
4	監査スケジュール	上記 3 の概略スケジュール ※詳細は監査人決定後に求める。
5	監査実施体制	ⅰ）監査責任者・監査人・監査補助者・アドバイザ等の役割、氏名を含む監査体制図 ⅱ）当該団体との役割分担
6	監査人の実績等	ⅰ）組織としての認証資格等 ※例えば、ISMS 認証やプライバシーマーク認証 ⅱ）監査メンバの保有資格・技術スキル・地方公共団体を含む実務経験等
7	監査報告書の目次体系	監査報告書の目次体系（章立て） ⅰ）総括 ⅱ）情報セキュリティ監査の実施の概要 ⅲ）評価できる事項 ⅳ）改善すべき事項（緊急改善事項・一般的改善事項のまとめ） ⅴ）監査結果の詳細 ⅵ）添付資料（補足資料等）
8	成果物	最終成果物（納品物）一覧
9	その他	会社案内、パンフレット等必要な添付書類

＜修正後＞

5	監査実施体制	ⅰ）監査責任者・監査人・監査補助者・アドバイザ等の役割、氏名を含む監査体制図 ⅱ）当該団体との役割分担
6	監査品質を確保するための体制	ⅰ）監査品質管理責任者・監査品質管理者等の役割、氏名を含む監査品質管理体制図 ⅱ）監査品質管理に関する規程　等
7	監査人の実績等	ⅰ）組織としての認証資格等 ※例えば、ISMS認証やプライバシーマーク認証、情報セキュリティ監査企業台帳への登録　等 ⅱ）監査メンバの保有資格・技術スキル・地方公共団体を含む実務経験等
8	監査報告書の目次体系	監査報告書の目次体系（章立て） ⅰ）総括 ⅱ）情報セキュリティ監査の実施の概要 ⅲ）評価できる事項 ⅳ）改善すべき事項（緊急改善事項・一般的改善事項のまとめ） ⅴ）監査結果の詳細 ⅵ）添付資料（補足資料等）
9	成果物	最終成果物（納品物）一覧
10	その他	会社案内、パンフレット等必要な添付書類