

情報セキュリティ監査基準
報告基準ガイドライン

Ver1.0

本ガイドラインは、「情報セキュリティ監査基準」のうち、報告基準に係る基本的な考え方を踏まえ、特に留意すべき事項及び情報セキュリティ監査報告書の雛形について示したものである。

I. 監査報告書の意味と記載事項

1. 監査報告書の定義

1.1 情報セキュリティ監査報告書は、監査の結果を関係者に伝達する手段であるとともに、情報セキュリティ監査人が自らの役割と責任を明確にする手段である。したがって、情報セキュリティ監査の目的に応じて監査人が必要と認めた事項を明瞭に記載しなければならない。

1.2 外部利害関係者からの開示請求又は監査報告書受領者の判断によって情報セキュリティ監査報告書が外部に公表されるような場合には、監査の結果が誤解なく伝わるものでなければならず、監査報告書に記載した事項については情報セキュリティ監査人が全面的に責任を負うこととなることに留意する。

2. 監査報告書の記載事項

2.1 情報セキュリティ監査報告書は、内部利用であっても、外部に開示されることを前提に作成される場合であっても、基本的には、次の記載区分によって構成される。

- ・ 導入区分（実施した監査の対象等を記載する）
- ・ 概要区分（実施した監査の内容等を記載する）
- ・ 意見区分（保証意見又は助言意見を記載する）
- ・ 特記区分（必要に応じてその他特記すべき事項を記載する）

2.2 監査報告の明瞭性という観点から、これらの区分に従って記載するものとする。導入、概要、意見の3つの記載区分は、情報セキュリティ監査の目的又は実施形態を問わず、必ず設けられなければならないことに留意する。

3. 監査意見の種別

3.1 情報セキュリティ監査報告書は、情報セキュリティ監査の目的又は契約の内容によって、保証型の監査報告書（保証報告書という）が作成される場合と、助言型の監査報告書（助言報告書という）が作成される場合がある。

3.2 1通の情報セキュリティ監査報告書において、保証意見を記載した後で、助言意見を記載することもある。

II. 助言報告書作成上の留意事項

1. 助言意見の表明方法

1.1 助言意見の表明に当たっては、「情報セキュリティ管理基準」を監査上の判断の尺度として利用する場合、助言の内容は情報セキュリティ監査人の自由裁量で行われるものではなく、あくまでも「情報セキュリティ管理基準」等適当な管理基準に照らして検出された問題点の指摘と改善提言であることに留意する。

1.2 情報セキュリティ監査人が、助言意見として、検出事項だけを記載するかあるいは改善提言も併せて記載するかは、監査方針又は監査契約による。助言意見は、「情報セキュリティ管理基準」等に照らした欠陥及び懸念事項を検出事項として提示することに留まらず、当該検出事項に対応した改善提言があつて、はじめて効果的なものとなることに留意する。その際、実現に係る改善提言の意思決定に関与することがあつてはならない。

1.3 助言意見は、情報セキュリティ監査報告書の内部利用を前提とした場合に有効な意見表明方式である。

2. 助言意見記載上の留意事項

2.1 監査報告書における検出事項の記載は、あくまでも被監査側による継続的な改善活動を前提とした助言として行われるものであつて、情報セキュリティ対策の重大な欠陥等に基づく監査意見の限定とは異なることに留意しなければならない。したがつて、監査報告書において保証を付与するかのような誤解を与える表現を用いてはならない。

2.2 情報セキュリティ監査人が指摘した助言事項に基づいて是正措置を採用するか否かは、あくまでも監査依頼者又は被監査側の判断であつて、情報セキュリティ監査人はそれを強制することはできない。

2.3 情報セキュリティ対策に係る成熟度に応じて助言意見を表明する場合、監査報告書においてどのような成熟度モデルを利用して監査を実施したか、その場合の成熟度の水準の判定基準について記載しなければならない。

Ⅲ. 助言報告書の雛形

1. 助言意見のみを記載する場合の雛型

1.1 情報セキュリティ監査人は、情報セキュリティ対策の実施状況に関して改善を要する検出事項を認めた場合には、概ね次のように、「情報セキュリティ管理基準」等に照らして、検出事項を指摘し、必要に応じて当該検出事項に対する改善提言を記載した監査報告書を作成する。

1.2 助言報告書は、保証を付与するものではなく、また具体的な検出事項と改善提言の伝達に主眼が置かれることから、その様式等において保証報告書のような厳密性は必要とされない。

情報セキュリティ監査報告書	
	日 付
宛 名	
	監査人署名
<p><u>われわれは①、「情報セキュリティ管理基準」に照らして②、200x年x月x日から200x年x月x日までの期間③に係るXXXを対象として④情報セキュリティ対策の実施状況について⑤監査を実施した。われわれの任務は、監査手続を実施した結果に基づいて助言を行うことにある⑥。</u></p>	
<p>われわれの監査は、「情報セキュリティ監査基準」に準拠して行われた。監査は、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、<u>リスクアセスメントに基づいて⑦適切なコントロールが採用されているか否かを確認、問題点を検出し、提示するという観点から行われている⑧。</u></p>	
<p>われわれは、200x年x月x日から200x年x月x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について、「情報セキュリティ管理基準」に照らして、<u>以下の検出事項と、その改善提言を含め、ここに報告⑨する。</u></p>	
<u>記⑩</u>	
1. 検出事項	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
2. 改善提言	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1.3 **上記雛型における下線部①について** 情報セキュリティ監査人が内部監査部門で

あるときは「当監査部門」とする。また、情報セキュリティ監査人が個人事業主であるときは「私は」とする。以下の該当箇所も同様である。

1.4 上記難型における下線部②について 情報セキュリティ監査の目的を十分に達成するためには、「情報セキュリティ管理基準」の趣旨と枠組みを尊重し、当該すべての項目について監査の対象とすることが望ましいが、「情報セキュリティ管理基準」のすべての項目ではなく、一部分の項目（例えば、外部委託に係る管理項目のみ）を監査上の判断の尺度としたときは、その旨を明記する。ただし、その場合には、情報セキュリティ監査の対象として選択された管理項目が、監査の対象として選択されなかった他の管理項目と有機的に結びついてはじめて有効に機能することもある点に留意しなければならない。また、「情報セキュリティ管理基準」以外の管理基準等を判断の尺度としたときは、該当する基準等を明記する。

1.5 上記難型における下線部③について 雛形は、一定期間を対象とした情報セキュリティ監査を実施した場合の例を示している。ある特定時点における情報セキュリティ対策の状況について意見を表明するときは、「200x年x月x日現在における」と記載する。

1.6 上記難型における下線部④について 情報セキュリティ監査の対象を記載する。監査の対象については、必要に応じて、監査対象の範囲（例えば、外部委託）、監査対象の段階（例えば、運用段階）、及び監査対象に係る監査目標（例えば、機密性）等を記載する。また、監査の対象となる組織、場所、情報システム（例えば、Webシステム）等を限定する必要があるときは、当該組織、場所、情報システム等もあわせて明記する。

1.7 上記難型における下線部⑤について 「情報セキュリティ対策の状況」について助言を行うことを原則とするが、監査方針又は監査契約によっては「情報セキュリティ管理システム（プロセス）」「情報セキュリティリスク管理システム（プロセス）」等についての助言を行うことができる。なお、保証意見でみられる、経営者又は情報システム管理責任者による確認書（言明書）を得て、当該確認書について情報セキュリティ監査人が意見を表明する言明方式は、助言意見では使われない。

1.8 上記難型における下線部⑥について 情報セキュリティ監査人の任務は、助言を行うことにあることを明記する。助言はそれが実行に移されて意味をもつことから、その点を徹底するため、「当該監査の結果として提示された助言に基づいて、適切な是正措置が確実かつ速やかに実行に移されることを望む」といった文言を追加してもよい。情報セキュリティ監査人と被監査側の間に責任区別が存在することは当然であるが、保証意見とは異なり、責任区別についてあえて言及する必要はない。

1.9 上記難型における下線部⑦について 「情報セキュリティ管理基準」の趣旨からすれば、情報セキュリティ対策に係るコントロールは、リスクアセスメントの結果に基づくものでなければならない。リスクアセスメントが行われていないか又はリスクアセスメントが不適切な場合には、この記載は行わない。かかるリスクアセスメントの不備は、検出事項に含めることが望ましい。また、情報セキュリティ監査人自らがリスクアセスメント

を実施した場合には、「監査人が必要と認めて、リスクアセスメントを行った結果に基づいて」と明記する。

1.10 上記雑型における下線部⑨について 助言型の情報セキュリティ監査は、情報セキュリティ対策の改善を目的として、そのための問題点を検出し提示するという観点から行われるものであるから、その旨を明記する。問題点の検出は、「情報セキュリティ管理基準」その他適切な管理基準等に示された各項目に照らして行われるものであるが、マネジメント又はコントロールは、それぞれの構成要素がお互いに影響し合いながら結びついていく点に着目することが肝要である。そのような観点をより明確にするためには、「問題点を検出し」の前に「体系的に」という字句を補うことが望ましい。

1.11 上記雑型における下線部⑨について 情報セキュリティ監査人の最終意見は、検出事項と、必要に応じてそれに対応する改善提言を示すものでなければならない。この場合、検出事項並びに改善提言の報告である旨を明記し、「以下の検出事項があるものの、当面、緊急かつ重要な影響は予想されないものと判断される」等、保証の付与と紛らわしい表現を用いてはならない。

1.12 上記雑型における下線部⑩について 検出事項及び改善提言は、意見区分の中に別途見出しを設けて記載する。検出事項及び改善提言が長文となる場合には、監査報告書別紙として取り纏める。

1.13 上記雑型における下線部⑩について 検出事項及び改善提言は、それぞれ重要性が高いものから記載し、検出事項と改善提言の対応関係が明らかとなるよう工夫されることが望ましい。また、改善提言を行う場合には、緊急性のある改善提言を要緊急改善提言、その他の改善提言を分けて記載することが有益である。

IV. 保証報告書作成上の留意事項

1. 保証意見の表明方法

1.1 保証意見の表明に当たっては、「情報セキュリティ管理基準」その他適切な管理基準等を監査上の判断の尺度として利用する場合、当該管理基準等に照らして慎重に監査手続を実施した限りにおいて、情報セキュリティ対策について重大な欠陥がないこと（又はあること）を保証するものであることに留意する。

1.2 保証意見は、情報セキュリティ監査報告書の内部利用を前提とした場合にも有効な意見表明方式であるが、監査報告書の外部開示を前提とした場合には原則としてこの意見表明方式による。

2. 保証意見の類別

2.1 保証意見は、以下のいずれかの意見として表明される。

- ・肯定意見（情報セキュリティ対策の全てに重大な欠陥がなく、適切である旨の保証）
- ・限定付肯定意見（情報セキュリティ対策の一部に欠陥があるか、又は情報セキュリティ監査人が必要と認めた監査手続が制約されたがその部分を除けば適切である旨の保証）
- ・否定意見（情報セキュリティ対策に重大な欠陥があり、情報セキュリティ管理状況が全体として適切とはいえない旨の保証）がある。

2.2 限定付肯定意見及び否定意見は、情報セキュリティ対策に無視し得ない欠陥があることを監査意見として表明することになる。このことから情報セキュリティ監査報告書の外部開示を想定した場合には、必ずしも現実的でない。情報セキュリティ監査報告書の外部開示が想定される場合であって、肯定意見の表明が困難であると判断されるときは、助言型の監査に切り替えるか、又は一定期間において被監査側による改善が図られた段階で監査に着手することが望ましい。

2.3 情報セキュリティ監査人が必要と認めた監査手続が制約され、保証意見の合理的な根拠を得ることができなかつた場合には、保証意見を述べてはならない。

3. 保証意見記載上の留意事項

3.1 保証意見は情報セキュリティ対策に対して一定の保証を付与するものであるため、情報セキュリティ監査人が負うかもしれない責任に十分に留意し、あいまいな表現を避け、助言意見と混同されることがないようにしなければならない。

3.2 情報セキュリティ対策に無視し得ない欠陥があることを監査意見として表明せざるを得ないような事態が生じた場合、情報セキュリティ監査人は、監査報告書の外部開示又は非開示を考慮し、必要に応じて法律専門家に助言を求めるなどして、監査報告書の記載方法、表記方法、並びに取扱方法を慎重に検討した上で監査報告書を作成し、提出しなけ

ればならない。

3.3 情報セキュリティ対策に係る成熟度に応じて保証意見を表明する場合、監査報告書の導入区分においていかなる成熟度モデルに基づいて監査を実施したかを記載しなければならない。

3.4 情報セキュリティ対策に係る成熟度モデルを利用しないで監査報告書を作成する場合、被監査側における情報セキュリティ対策が適切に整備かつ運用され、高度なセキュリティが確保されていることを確かめるための監査が行われたものと推定されることに留意する。

V. 保証報告書の雛型

1. 肯定意見の雛型

1.1 情報セキュリティ監査人は、情報セキュリティ対策の実施状況に関してとくに重大な欠陥がないと認めた場合には、概ね次のように、情報セキュリティ対策の実施状況が管理基準等に照らして適切に整備され運用されている旨の監査報告書を作成する。

情報セキュリティ監査報告書	
宛 名	日 付
	監査人署名
<p>われわれは①、「情報セキュリティ管理基準」に照らして②、200 x 年 x 月 x 日から 200 x 年 x 月 x 日までの期間③に係る <u>XXX</u> を対象として④情報セキュリティの状況について⑤監査を実施した。われわれの責任は、監査手続を実施した結果に基づいて意見を表明することにある⑥。</p> <p>われわれの監査は、「情報セキュリティ監査基準」に準拠して行われた。監査は、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、<u>リスクアセスメントに基づいて⑦適切なコントロールが採用されているか否かについて検討し評価している</u>。採用した監査手続は、われわれが必要と認めたものを適用しており⑧、監査の結果として意見表明のための合理的な根拠を得たと確信している⑨。</p> <p>われわれの意見によれば、200 x 年 x 月 x 日から 200 x 年 x 月 x 日までの期間に係る <u>XXX</u> を対象とした情報セキュリティ対策の実施状況は、「情報セキュリティ管理基準」に照らして適切であると認める⑩。</p>	

1.2 **上記雛型における下線部①について** 情報セキュリティ監査人が内部監査部門であるときは「当監査部門」とする。また、情報セキュリティ監査人が個人事業主であるときは「私は」とする。以下の該当箇所も同様である。

1.3 **上記雛型における下線部②について** 情報セキュリティ監査の目的を十分に達成するためには、「情報セキュリティ管理基準」の趣旨と枠組みを尊重し、当該すべての項目について監査の対象とすることが望ましいが、「情報セキュリティ管理基準」のすべての項目ではなく、一部分の項目（例えば、外部委託に係る項目のみ）を監査上の判断の尺度としたときは、その旨を明記する。ただし、その場合には、情報セキュリティ監査の対象として選択された管理項目が、監査の対象として選択されなかった他の管理項目と有機的に結びついてはじめて有効に機能することもある点に留意しなければならない。また、

「情報セキュリティ管理基準」以外の管理基準等を判断の尺度としたときは、該当する基準等を明記する。

1.4 上記雛型における下線部③について 雛形は、一定期間を対象とした情報セキュリティ監査を実施した場合の例を示したものである。ある特定時点における情報セキュリティ対策の実施状況について意見を表明するときは、「200x年x月x日現在における」と記載する。

1.5 上記雛型における下線部④について 情報セキュリティ監査の対象を記載する。監査の対象については、必要に応じて、監査対象の範囲（例えば、外部委託）、監査対象の段階（例えば、運用段階）、及び監査対象に係る監査目標（例えば、機密性）等を記載する。また、監査の対象となる組織、場所、情報システム（例えば、Webシステム）等を限定する必要があるときは、当該組織、場所、情報システムもあわせて明記する。

1.6 上記雛型における下線部⑤について 情報セキュリティ対策の実施状況について、直接、監査意見を表明するときには、「情報セキュリティ対策の実施状況について」と記載する。これを直接報告方式という。

1.7 上記雛型における下線部⑤について 1.6の方式とは別に、言明方式がある。一般的には、「情報セキュリティに関わるリスク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を整備し運用している」旨の経営者又は情報システム管理責任者による確認書（言明書）を得て、当該確認書について情報セキュリティ監査人が意見を表明する方法である。なお、実施基準ガイドライン3.6に基づいて、被監査側が自ら作成した自己評価表及びその適正性を被監査部門の長又は必要に応じて組織体の長が認めた旨を記載した文書（適正言明書という）を入手し、当該適正言明書を保証意見表明の対象とする場合には、「被監査側が作成した自己評価表に対する担当部門の責任者（又は組織体の長）による適正言明書が、「情報セキュリティ管理基準」に準拠しているか否かについて」とする。この場合にあっては、当該組織体の長による適正言明書を監査報告書に添付することとする。なお、かかる適正言明書に対して保証意見を表明する場合にあっては、保証意見報告書における意見区分は「XXXシステムを対象とした担当部門の責任者（又は組織体の長）による適正言明書は、「情報セキュリティ管理基準」に準拠しているものと認める」となることに留意する。言明方式の方が、通例、意見表明に関わる情報セキュリティ監査人の責任を明確にしやすい。

1.7 上記雛型における下線部⑥について 情報セキュリティ対策に対して直接的かつ第一次的に責任を負うのはあくまでも被監査側であって、情報セキュリティ監査人は自らが実施した監査の方法と結論についてのみ責任を負うという責任区別の原則を徹底するために記載される。内部監査部門による情報セキュリティ監査を前提とするときは特に記載を要しないが（記載を禁止するものではない）、外部機関による監査を前提とするときは記載することが望ましい。

1.8 上記雛型における下線部⑦について 「情報セキュリティ管理基準」の趣旨から

すれば、情報セキュリティ対策に係るコントロールは、リスクアセスメントに基づくものでなければならない。リスクアセスメントが行われていないか又はリスクアセスメントが不適切な場合には、この記載は行わない。

1.9 上記雛型における下線部⑧について 情報セキュリティ監査報告書において、実施した監査手続のすべてを列記することは現実的でないばかりか、監査報告書読者の混乱を招く結果ともなりかねない。情報セキュリティ監査人が必要と認めた監査手続を実施した旨の記載で充分である。しかし、特別な追加的手続を実施したときや、実施した監査手続が特別な条件のもとで行われたときには、その旨と理由を明記しておくことが望ましい。

1.10 上記雛型における下線部⑨について 監査意見としての保証は絶対的な保証ではなく、入手した監査証拠を評価した結果得られた合理的な根拠に基づく保証である。情報セキュリティ対策の欠陥が皆無であることを保証するものではないため、「合理的な」という字句を含めておくことが有益である。

1.11 上記雛型における下線部⑩について 情報セキュリティ監査人の最終意見は、簡潔明瞭でなければならない。また、助言意見と混同されるような表現は避けなければならない。「情報セキュリティ管理基準」に従った監査においては「『情報セキュリティ管理基準』に照らして、適切に一」という表現を推奨しているが、これに限定されない。例えば「『情報セキュリティ管理基準』に準拠しているものと認める」「『情報セキュリティ管理基準』の趣旨に鑑みて、有効であると認める」などの意見表明方式でもよい。これらの例は、いずれも「認める」という結語にその意味が端的にあらわれているように、積極型の保証意見である。これに対して、「『情報セキュリティ管理基準』に照らして、特に指摘すべき事項は見当たらなかった」「『情報セキュリティ管理基準』から逸脱する重要な事実はなかった」といった意見表明方式が採用されることがある。これらの例は消極型の保証意見である。

2. 限定付意見等の雛型

情報セキュリティ対策の重要な欠陥等に基づく限定

2.1 情報セキュリティ対策の一部に重大な欠陥等が発見された場合、該当する欠陥等を除けば適切と判断できるときには限定付肯定意見を表明し、該当する欠陥等の重大さに鑑みて情報セキュリティ管理状況が全体として適切とは判断できないときには否定意見を表明する。

2.2 監査の結果、重大な欠陥等が発見され、限定付肯定意見又は否定意見を表明する場合、欠陥等事項をどこまで具体的に記載するかについて情報セキュリティ監査人は慎重でなければならない。情報セキュリティ監査報告書において、保証を限定するために記載される重大な欠陥事項等は、あくまでも監査責任を限定し、関係者に注意を促すために記載されるものである。情報セキュリティ対策の改善を目的とした検出事項を明らかにするための記載事項ではないため、改善提言を含めてはならない。情報セキュリティ監査報告書

の利用目的いかんによっては、欠陥事項等を別紙に取り纏めて記載する等の措置が検討されなければならない。

2.3 情報セキュリティ対策の一部に重大な欠陥等が認められた場合における限定付肯定意見の表明は、概ね次のような記載例による。

導入区分	肯定意見と同じ
概要区分	肯定意見と同じ
意見区分	われわれの意見によれば、200 x 年 x 月 x 日から 200 x 年 x 月 x 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、以下の事項を除き、「情報セキュリティ管理基準」に照らして適切であると認める。 記 XXXXXXXXXXXXXXXXXXXX

2.4 情報セキュリティ対策に重大な欠陥等が認められた場合において、当該事項の重大性に鑑みて否定意見を表明する場合は、概ね次のような記載例による。

導入区分	肯定意見と同じ
概要区分	肯定意見と同じ
意見区分	われわれの意見によれば、200 x 年 x 月 x 日から 200 x 年 x 月 x 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には下記の通り重大な欠陥事項があり、当該事項の重大性に鑑みると、「情報セキュリティ管理基準」に照らして適切であるとは認められない。 記 XXXXXXXXXXXXXXXXXXXX

監査人が必要と認めた監査手続の制約に基づく限定

2.5 災害、障害、妨害、監査対象資料の不備等により、情報セキュリティ監査人が必要と認めた監査手続に重大な制約が課せられた場合であって、意見表明のための合理的な根

拠が得られた判断されるときには限定付肯定意見を表明し、もはや意見表明のための合理的な根拠が得られない判断されるときには監査意見の表明を差控える。

2.6 情報セキュリティ監査人が必要と認めた監査手続に重大な制約が課せられたときは、制約された監査手続の内容と制約された理由を明記する。なお、意見表明のための合理的な根拠が得られなかった場合には、「意見表明のための合理的な根拠を得たと確信している」旨の記載をしてはならない。

2.7 情報セキュリティ監査人が必要と認めた監査手続に重大な制約が課せられた場合における限定付肯定意見の表明は、概ね次のような記載例による。

導入区分	肯定意見と同じ
概要区分	—ここまで肯定意見と同じ— 採用した監査手続は、下記を除いて、われわれが必要と認めたものを適用しており、監査の結果として意見表明のための合理的な根拠を得たと確信している。 記 XXXXXXXXXXXXXXXXXXXX
意見区分	われわれの意見によれば、上記の監査手続上の制約事項はあるが、200x年x月x日から200x年x月x日までの期間に係るXXXを対象とした情報セキュリティの状況は、「情報セキュリティ管理基準」に照らして適切であると認める。

2.8 情報セキュリティ監査人が必要と認めた監査手続に重大な制約が課せられた場合において、当該事項の重大性に鑑みて監査意見の表明を行わない場合は、概ね次のような記載例による。

導入区分	われわれは、「情報セキュリティ管理基準」に従って、200 x 年 x 月 x 日から 200 x 年 x 月 x 日までの期間に係る XXX を対象として情報セキュリティの状況について監査を実施した。
概要区分	われわれの監査は、「情報セキュリティ監査基準」に準拠して行われた。しかし、下記の通り、われわれが必要と認めた監査手続を実施することができず、結果として意見表明のための合理的な根拠を得ることができなかった。
<p>記</p> <p>XXXXXXXXXXXXXXXXXXXXXXXXXX</p>	
意見区分	よって、われわれは、200 x 年 x 月 x 日から 200 x 年 x 月 x 日までの期間に係る XXX を対象とした情報セキュリティの状況についての意見の表明は行わない。

3. 合意に基づく監査手続とその結果のみを報告する方式による場合の雛型

3.1 外部の情報セキュリティ監査人による監査では、選択適用すべき検証手続を監査依頼者と協議の上で決定し、それに対する結論のみを報告する契約を締結できる。

3.2 監査依頼者と合意した監査手続を実施し、その結論のみを報告する契約による場合、情報セキュリティ監査人と監査依頼者は、作成される報告書は情報セキュリティ対策の適否について保証を付与するものではないことに合意することができる。その場合には、監査報告書において「この報告書は、監査人としての保証を付与するものではない」旨、及び「この報告書は、外部の不特定の関係者に開示されることを前提としていない」旨を明記しなければならない。ただし、対象が公的機関の場合には、情報公開の要請により、不特定の関係者に情報が開示される可能性があることに留意する。また、報告書において情報セキュリティ監査人が上記事項を明記しない場合には、情報セキュリティ対策の実施状況についての保証を付与することになることに留意する。

3.3 監査依頼者と合意した監査手続を実施し、その結論のみを報告する契約による場合、概ね次のような報告書が作成される。

監査人による報告書	
宛 名	日 付
	監査人署名
<p>われわれは、「情報セキュリティ管理基準」に照らして、200x年x月x日から200x年x月x日までの期間に係るXXXを対象として情報セキュリティの状況について検証した。この報告書は上記システムを対象として、監査人としての保証を付与するものではない。また、この報告書は外部の不特定の関係者に開示されることを前提としていない。</p> <p>被監査側と合意の上で決定された検証の範囲及び具体的な検証手続、並びにその結論は下記の通りである。</p>	
記	
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	