# 情報セキュリティ監査基準
# 報告基準ガイドライン

Ver2.0（案）

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

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（以下「監査人」という。）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。

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

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（アシュアランス意見又はアドバイザリー意見を記載する）
- 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）

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

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、アシュアランス型の監査報告書（アシュアランス報告書という）が作成される場合と、アドバイザリー型の監査報告書（アドバイザリー報告書という）が作成される場合がある。

## Ⅱ．アドバイザリー報告書作成上の留意事項

### １．アドバイザリー意見の表明方法

アドバイザリー意見の表明に当たっては、「情報セキュリティ管理基準」等を監査上の判断の尺度として利用する場合、アドバイザリーの内容は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。

監査人が、アドバイザリー意見として、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。アドバイザリー意見は、「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って、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ってはならない。

### ２．アドバイザリー意見記載上の留意事項

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アドバイザリーとして行われるものであって、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。したがって、監査報告書においてアシュアランス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。

監査人が指摘したアドバイザリー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って、監査人はそれを強制することはできない。

## Ⅲ．アドバイザリー報告書の雛形

### １．アドバイザリー意見のみを記載する場合の雛型

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。

情報セキュリティ監査報告書

日　　付

宛　　名

監査人署名

われわれは①、「情報セキュリティ管理基準」に照らして②、20xx 年 x 月 x 日から 20xx 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アドバイザリーを行うことにある⑥。

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、リスクアセスメントに基づいて⑦適切な管理策が採用されているか否かを確かめ、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。

われわれは、20xx 年 x 月 x 日から 20xx 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、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。

記⑩

１．検出事項　　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

２．改善提言　　xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

**上記雛型における下線部①について**　　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、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。

**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充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。

**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、「20xx 年 x 月 x 日現在における」と記載する。

**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、情報システム等もあわせて明記する。

**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状況」についてアドバイザリー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）」等についてのアドバイザリーを行うことができる。なお、アシュアランス意見でみられる、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監査人が意見を表明する言明方式は、アドバイザリー意見では原則として使われない。

**上記雛型における下線部⑥について**　監査人の任務は、アドバイザリーを行うことにあることを明記する。アドバイザリー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アドバイザリーに基づいて、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。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、アシュアランス意見とは異なり、責任区別についてあえて言及する必要はない。

**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管理策は、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、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。

**上記雛型における下線部⑧について**　アドバイザリー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、マネジメント又は管理策は、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る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。

**上記雛型における下線部⑨について**　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、アシュアランスの付与と紛らわしい表現を用いてはならない。

**上記雛型における下線部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。

**上記雛型における下線部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．アシュアランス報告書作成上の留意事項

### １．アシュアランス意見の表明方法

言明方式によるアシュアランス意見の表明に当たっては、被監査主体による情報セキュリティ対策に関する言明をもとに「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、言明の内容の通りであること（又はそうではないこと）をアシュアランスするものであることに留意する。

監査報告書の外部開示を前提とした場合には、対外的な説明の観点からはこのアシュアランスに基づく意見表明方式が要請される。なお、アシュアランス意見の表明に際しては、監査人が監査報告書利用者と監査リスク受容の程度について合意をする形態として次の二つの方式があり、以降において適宜区分して記載する。

**利用者合意方式**　監査人が監査報告書利用者と明示的に、あるいは暗黙に監査手続について合意する方式である。合意した監査対象に対して、合意した監査手続に基づく監査を実施することで、監査報告書のリスクを監査人と報告書利用者が共有する。この場合には、報告書のリスクについて理解が必須であり、リスクを理解している者に監査報告書の配布・閲覧を制限する。

**社会的合意方式**　社会的に合意された監査手続を行うものであり、監査報告書は一般に公開される。監査人は実施する監査手続が社会的に合意されていることを確認し、監査目標を設定する必要がある。

### ２．アシュアランス意見の類別

言明方式によるアシュアランス意見は、以下のいずれかの意見として表明される。

- 肯定意見（言明の内容通りである旨のアシュアランス）
- 限定付肯定意見（言明内容の一部に不適合があるか、又は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アシュアランス）
- 否定意見（情報セキュリティ管理状況が言明の内容と異なり、適切とはいえない旨のアシュアランス）がある。
- 意見不表明

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。このことから社会的合意方式のように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、アドバイザリー型の監査に切り替えるか、又は一定期間を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。

監査人が必要と認めた監査手続が制約され、アシュアランス意見の合理的な根拠を得る

ことができなかった場合には、アシュアランス意見を述べてはならない。

### ３．アシュアランス意見記載上の留意事項

アシュアランス意見は情報セキュリティ対策に対して一定のアシュアランスを付与するものであるため、監査人が負うかもしれない責任に充分に留意し、あいまいな表現を避け、アドバイザリー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。

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、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。

### ４．内部監査におけるアシュアランス報告書

本ガイドラインでは、アシュアランス報告書の雛形として後述のように外部監査を前提としたものを例示している。内部監査等において言明を対象とせず、監査対象の実態について監査を行う場合、アシュアランス報告書において以下のいずれかのアシュアランス意見が表明される。

- ・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、適切である旨のアシュアランス）
- ・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アシュアランス）
- ・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アシュアランス）

監査人が必要と認めた監査手続が制約され、アシュアランス意見の合理的な根拠を得ることができなかった場合には、意見を述べてはならない。

## Ⅴ．アシュアランス報告書の雛型

アシュアランス型監査における監査報告書[1]様式として、二つの様式を想定する。様式１は、情報セキュリティ監査のための意見表明方式として、訴訟等で用いられる鑑定意見書等の様式を参考に作成した様式であり、様式２は、これまでの会計監査等で用いられてきた保証業務等の意見表明方式との整合性を考慮した様式である。監査人は、被監査主体の要望などを考慮のうえ様式を選択するものとする。

以下、社会的合意方式と利用者合意方式のそれぞれについて、様式１及び様式２に基づく情報セキュリティ監査報告書の雛形を示す。

### １．社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式１】の雛型

20xx 年 x 月 x 日①

*［被監査主体］*　殿②

監査主体
*［監査主体組織名］*
*［代表者役職氏名］*　②

情報セキュリティ監査報告書③

*［監査主体組織名］*（以下「監査人」という。）は、*［被監査主体］*（以下「貴社」という。）との 20xx 年 x 月 x 日付情報セキュリティ監査契約にもとづく④ 社会的合意方式によるアシュアランス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。⑤

記

監　査　結　果

貴社作成の 20xx 年 x 月 x 日付言明書記載の XXX に対する情報セキュリティ対策の設計が XX に求められる情報セキュリティレベルの要求を反映したものであり、設計した情報セキュリティ対策を適切に実装し運用している旨の言明は⑥ 信じるに足るものと認める。⑦

理　　由⑧

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⑨、情報セキュリティ監査基準に準拠して⑩、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの間⑪、貴社作成の 20xx 年 x 月 x 日付言明書記載の XXX に対するセキュリティ対

[1] アシュアランス方式の監査報告書の記載事項の検討にあたっては、日本公認会計士協会が以下にて公表している実務指針等を参考とすることができる。
https://jicpa.or.jp/specialized_field/publication/kansa/
必要に応じて米国公認会計士協会の定める Service and Organization Control (SOC)レポートのうち、SOC2 及び SOC3 の規定内容も考慮すべきである。

策の設計とその実装･運用状況が情報セキュリティ管理手続に準拠している旨の言明が信じるに足るかどうかについて監査した⑫ 結果､監査結果表明のための合理的な根拠を得たとの確信に至った｡⑬

特　　記⑭

この報告書は、監査契約当事者と、20xx 年 x 月 x 日付言明書に記載のあて先の者を利用者として作成されたものである。

本監査の対象は､上記言明であって、XXX に対する情報セキュリティ対策の実態ではない。

添　付　書　類⑮

1　貴社作成の
　情報セキュリティ基本方針 Ver,1,3
　情報資産管理規定(20xx 年 x 月 x 日作成)
　20xx 年 x 月 x 日付言明書
2　▲▲作成の 20xx 年 x 月 x 日付報告書
3　サーバ室入退室管理規定
4　●●要件定義書
5　●●の供述書
6　●●に対するインタビュー結果

**上記雛型における下線部①について**　監査報告の時点を示す部分である。

**上記雛型における下線部②について**　当事者の記載がなされている。

**上記雛型における下線部③について**　表題「セキュリティ監査報告書」の部分は、この書面が、情報セキュリティ監査報告書であることを示している。

**上記雛型における下線部④について**　この監査の根拠が、監査主体と被監査主体との 20xx 年 x 月 x 日付情報セキュリティ監査契約にあることを示している。

**上記雛型における下線部⑤について**　この監査報告書の監査の種別・内容が、社会的合意方式による保証型監査であることを示している。

**上記雛型における下線部⑥について**　監査の対象を上記の言明に特定している。このとき、監査報告書では、利用者に言明の内容を特定し、かつ、利用者に言明の対象としての情報資産を示す必要がある。「XXX に対する」が言明の対象が特定されていることを示している。また、監査報告書はこの言明が設計監査と実装監査の一方又は双方に向けられているかを示す必要がある。この例は、設計監査と実装監査の双方に向けられた言明であることを示している。すなわち、「に対する情報セキュリティ対策の設計が XXX に求められる情報セキュリティレベルの要求を反映したものであり」の部分は、この言明のうち設計監査に向けられた言明部分、「設計した情報セキュリティ対策を適切に実装し運用してい

る」の部分は、この言明のうち実装監査に向けられた部分である。仮に設計監査のみ、あるいは、実装監査のみにむけられた言明であれば、上記のうち該当部分だけが記載される。

**上記雛型における下線部⑦について**　監査人の意見の中核部分である。「信じるに足る」とは、情報セキュリティ監査人の保証意見の表明の形式であり、国語的な意味において監査人の一定量の心証を意味している。しかし、情報セキュリティ監査が法的に強制される位置付けにないこともあって、その心証の程度は会計監査や裁判におけるものとは論理的には無関係である。

**上記雛型における下線部⑧について**　理由の部分に、監査人が結論を導くに至った理由が記載されている。この記載が、監査人の善管注意義務を判断する根拠になるため、必要十分な記載が必要である。

**上記雛型における下線部⑨について**　監査体制を記載している。

**上記雛型における下線部⑩について**　監査人の監査が準拠した尺度の記載である。社会的合意方式の監査報告書であるから、「情報セキュリティ監査基準」のように社会に公表されている基準が用いられる。

**上記雛型における下線部⑪について**　監査期間を表している。

**上記雛型における下線部⑫について**　監査の内容を記載している。

**上記雛型における下線部⑬について**　結論と理由を結ぶ部分である。

**上記雛型における下線部⑭について**　特記は任意記載項目であって、監査報告書の利用者として想定される一次利用者を明示し、報告が言明型監査の報告であることを示している。この内容は、すでに上記内容で記載されおり重複ではあるが、特に監査報告書の利用者が、この報告書が実態型監査の報告書であると誤解することを防ぐために、注意的な記載をなす例である。なお、この記載の有無により監査人の責任に差が生じることはない。

**上記雛型における下線部⑮について**　添付書類は、理由を導くに至った証拠の標目明らかにするものである。この記載は、結論が証拠によらないで認定されたものでないことを示すものであり、監査人が証拠収集についての善管注意義務を尽くしたことを明らかにし、監査報告書の信頼性を維持するためのものである。掲記するのは、証拠の「内容」（例えば、テストツールを用いた検査の内容や、インタビューの内容）ではなく、証拠の「標目」（例えば、●●作成の●月●日付報告書、●●の供述）で足りる。証拠の「内容」を記載することは、被監査主体のセキュリティレベルを下げることになりかねないので厳に戒められなければならない。インタビュー先の氏名を明らかにすることがセキュリティレベルを下げたり、今後の協力を拒まれなどの弊害を生じたりするおそれがあるときは、そのインタビュー内容を「●●の供述」とせず、▲▲作成の報告書として、●●の氏名を明らかにしない工夫も必要である。また、特に合理的な理由がないのに、いたずらに重複する内容の証拠の標目を掲記すべきではなく、また、上記の趣旨に照らして、結論を認定するための証拠の証明力を裏付け、増強した証拠の標目も掲げる必要はない。しかし、結論を導くに必要十分な証拠は掲げるべきであり、認定した事実のすべてを覆うように掲げられ

ていなければならない。結論を直接証明する力のある事実（直接事実）に限らず、直接事実を認定するための重要な事実（重要な間接事実）の認定に必要な証拠の標目は掲げる必要がある。また、ある証拠と認定する事実との関連性が明らかでないときは、その関連性を認定した証拠を掲げる必要がある。言明が数個のシステム、サイトに及ぶときは、共通するものをまとめ、その後に各別のものをシステム毎に掲記するのがよい。言明書は、本来添付の必要はないが、証拠として用いる場合はこれを掲記する。

### ２．社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式２】の雛型

20xx 年 x 月 x 日

*［報告先組織名］*
*［報告先代表者名］*

*［監査人所属組織名］*
*［監査人代表者氏名］*

情報セキュリティ監査報告書

１．実施した手続の概要①

私たちは、本報告書に添付している○○○○株式会社（以下「会社」という。）が作成した「○○業務の情報セキュリティに係る管理手続」（以下「管理手続」という。）に関連して、「(1)管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載していること、(2) ○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されていること、及び(3)管理手続に記載された会社の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されていること」を主旨とする経営者の言明が信じるに足るかどうかについて合理的な保証を得るための手続を実施した。この監査は、社会的合意方式によるアシュアランス型情報セキュリティ監査であり、管理手続は会社の経営者により作成されたものである。

この手続の実施に当たって、私たちは、一般に公正妥当と認められる情報セキュリティ監査の基準において要請されるマネジメントと管理策の監査に関する手続を選択した。

会社の情報セキュリティに係るマネジメントと管理策の有効性及び重要性、並びにそれらが委託会社の情報セキュリティリスクの評価に与える影響は、それぞれの委託会社のマネジメントと管理策との関連によって異なる。

なお、私たちは、委託会社のマネジメントと管理策の有効性を評価するための手続は実施していない。

２．実施した手続の結果②

私たちの意見は次のとおりである。

(1) 「管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載している」とする経営者の言明は信じるに足るものと認める。

(2) 「○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた

情報セキュリティレベルを達成するように適切に設計されている」とする経営者の言明は信じるに足るものと認める。

(3) 「管理手続に記載された○○業務の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されている」とする経営者の言明は信じるに足るものと認める。

3．マネジメントと管理策の変更による影響及び統制の限界③

会社の情報セキュリティに係るマネジメントと管理策の管理手続は 20xx 年 x 月 x 日現在のものであり、情報セキュリティに係る特定のマネジメントと管理策に関連して実施した評価手続は 20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間を対象にしている。それ以降については情報セキュリティに係るマネジメントと管理策は変更されることがあるが、私たちの上記の意見は、変更があった場合のその影響を考慮したものではない。また、マネジメントと管理策には不正や誤謬を防止・発見する上での限界があるため、会社の情報セキュリティに係る特定のマネジメントと管理策により不正や誤謬が発生しているにもかかわらず発見されない可能性がある。

以 上

（別紙）

20xx 年 x 月 x 日

*［監査人所属組織名］*

*［報告先代表者名］*

## ○○業務の情報セキュリティ管理手続に関する経営者の言明④

当社は、○○業務を実施するうえで下記の情報セキュリティ管理手続に準拠した情報セキュリティレベルを達成するために、次のとおり適用している。

(1) 管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載している。

(2) ○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されている。

(3) 管理手続に記載された会社の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されている。

記

| 監査領域 | 情報セキュリティ管理手続 |
|---|---|
| 通信及び運用管理 | サーバルームへの可搬媒体の持込み・持出しは記録すること。 |
| ： | 可搬媒体を処分する際は、粉砕等の物理的破壊を実施すること。 |
| ： | ： |
| ： | |

－以上－

**上記雛型における下線部①について**　当該監査の目的と範囲を明確にするために、監査対象となったマネジメントと管理策の範囲と、そのマネジメントと管理策がどのような情報セキュリティの管理手続に基づいて構築されているかを示している。ここでいう管理手続は、情報セキュリティの管理基準とは区別されており、情報セキュリティの管理基準よりもさらに具体的な対策を記述することを想定している。なお、この情報セキュリティの管理手続は当該監査のために利用された手続であるため、言明書として監査報告書に添付している。この言明書に記された管理手続は、利用者が監査報告書を利用する際に「監査人がどのような基準に照らして監査対象であるマネジメントと管理策が有効であるか」を判断するために利用される。

**上記雛型における下線部②について**　いわゆる監査人の意見を記載する場所である。監査人の意見は、監査の目的と言明書の内容に照らして簡潔かつ明瞭に表現しなければならない。雛形では、「(1)管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載していること、(2) ○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されていること、及び(3)管理手続に記載された会社の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されていること」という３つの監査目的に対応して、それぞれの個別的な監査意見が記載されている。

**上記雛型における下線部③について**　この部分は、たとえ監査が適正に実施されていてもいくつかの要因により監査対象である内部統制が有効に機能しないことがあるため、そのような場合のリスクを監査報告書の利用者に説明するために作成される。監査報告書の意見は、過去の一時点あるいは一定期間について監査対象となったマネジメントと管理策が有効であることを述べており、将来の有効性を述べている訳ではない。したがって、監査報告書の利用者は監査人の意見をもとに利用者のリスクの下で監査対象の将来の有効性を判断することになるが、内部統制の有効性は一定の条件により損なわれる可能性があることを監査報告書に補足して、利用者に注意を呼びかけている。

**上記雛型における下線部④について**　言明の内容に従って情報セキュリティ対策を実施することは経営者が責任を追う。

### ３．利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式１】の雛型

20xx 年 x 月 x 日

*［委　託　元］*　殿
*［被監査主体］*　殿①

監査主体
*［監査主体組織名］*
*［代表者役職氏名］*　①

情報セキュリティ監査報告書

*［監査主体組織名］*（以下「監査人」という。）は、*［被監査主体］*（以下「貴社」という。）との 20xx 年 x 月 x 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アシュアランス型情報セキュリティ監査②の結果を下記のとおり報告する。

記

監　査　結　果③

貴社作成の 20xx 年 x 月 x 日付言明書記載の XXX に対する情報セキュリティ対策の設計と実装は、委託元の合意を得た情報セキュリティにかか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④

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に準拠して、20xx 年 x 月 x 日から 20xx 年 x 月 x 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により、貴社作成の 20xx 年 x 月 x 日付言明書記載の XXX に対するセキュリティ対策の設計・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根拠を得た。

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⑤

1　監査の範囲
2　監査手続

実施した情報セキュリティ監査手続とその結果

| 項番 | 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 |
|---|---|---|---|---|
| n-1 | 通信及び運用管理 | サーバルームへの可搬媒体の持込み・持出しは記録すること。 | 持込み・持出しは記録の査閲。 | ○<br>実施していると認められる。 |
| n-2 | ： | 可搬媒体を処分する際は、粉砕等の物理的破壊を実施すること。 | 物理的破壊の実施、立会いの有無の確認 | ○<br>実施していると認められる。 |
| n-3 | ： | ： | | ： |

| | | | | |
|---|---|---|---|---|
| n-4 | ： | | | ： |

注：発見事項を追記することもある。
監査手続が適正に行われたことを示すため、監査結果を認定するに必要かつ重要とされた証拠の名称などを必要に応じて記載する。

特　　記⑤

この報告書は、監査契約当事者及び委託元以外の者に開示されることを前提としていない。

添　付　書　類

・●●作成の 20xx 年 x 月 x 日付確認書
・●作成の 20xx 年 x 月 x 日付情報セキュリティ管理手続、など

以上

**上記雛型における下線部①について**　利用者合意方式であるため、報告書の日付に続き、利用者名（委託元)、被監査主体名を明記し、更に当該監査における監査主体の責任者名を記述する。

**上記雛型における下線部②について**　報告書本文冒頭には、利用者合意方式の情報セキュリティ監査であること、及び監査の根拠となる契約を明記する。

**上記雛型における下線部③について**　結論を前面に出すことで分かりやすい報告書とするため、意見区分は、監査結果として概要区分より前に述べる。監査結果では、監査対象である言明書を明確に特定し、当該言明書に対する意見を述べる。利用者合意方式での意見表明は「期待する水準にある」と記述する。

**上記雛型における下線部④について**　監査結果の次に、概要区分を理由として述べる。理由については、監査主体である監査チーム、今回の監査に用いた監査基準、監査期間、監査手続を合意した報告書一次利用者名、行った監査手続、言明書作成者名、言明書の日付、言明の対象（システムや業務など)、及び行った監査の種類（設計監査か運用監査か、あるいは双方か）を明確にする。

**上記雛型における下線部⑤について**　特記区分には、利用者の限定を明記する。これは、以下の理由による。

- 報告書の利用者をその内容が正しく認識できる対象者に限定し、混乱を防ぐこと、
- 概要区分で被監査主体の機密事項を内容とする詳細な管理手続及び監査結果を記述するため、被監査主体を保護する必要があること。

様式１は、監査の結果を簡潔に伝達する必要があるときに用いることができる。ただし、様式２に比較して、監査人の役割に対する言及が少ないため、報告書利用者が監査人の役割を過大に受け止めるリスクがある。監査人は言明書が期待する水準にあるか否かを判断

することに責任があるが、言明書の記載内容の妥当性や、その実行の責任を負っているわけではない。その点を利用者が十分理解している場合に、この様式を利用することができる。

**２．利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式２】の雛型**

20xx 年 x 月 x 日

*［委託元］殿*①
*［監査主体］殿*

*［監査人所属組織名］*
*［監査人代表者氏名］*

情報セキュリティ監査報告書

１．実施した手続の概要②

私たちは、本報告書に添付している○○○○株式会社（以下「会社」という。）が作成した「○○業務の情報セキュリティに係る管理手続」（以下「管理手続」という。）に関連して、「(1)管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載していること、(2) ○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されていること、及び(3)管理手続に記載された会社の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されていること」を主旨とする経営者の言明が委託元の期待する水準にあるかどうかについて合理的な保証を得るための手続を実施した。この監査は、利用者合意方式によるアシュアランス型情報セキュリティ監査であり、管理手続は会社の経営者により作成されたものである。

この手続の実施に当たって、私たちは、一般に公正妥当と認められる情報セキュリティ監査の基準において要請されるマネジメントと管理策の監査に関する手続を選択した。

私たちは、上述した手続に加え、別紙×に記載のとおり、会社が定めた情報セキュリティレベルを達成するために効果的と判断した特定のマネジメントと管理策について、20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間における運用状況を確かめる手続を実施した③。情報セキュリティに係る特定のマネジメントと管理策並びにそれらについて実施した手続の内容、範囲、実施時期及びその結果は、別紙×に記載している。別紙×は、情報セキュリティを委託している会社（以下「委託会社」という。）の情報セキュリティリスク評価に際し委託会社に存在するマネジメントと管理策とともに検討されることを目的として、委託会社のために作成したものである。

会社の情報セキュリティに係るマネジメントと管理策の有効性及び重要性、並びにそれらが委託会社の情報セキュリティリスクの評価に与える影響は、それぞれの委託会社のマネジメントと管理策との関連によって異なる。

なお、私たちは、委託会社のマネジメントと管理策の有効性を評価するための手続は実施していない。

２．実施した手続の結果

私たちの意見は次のとおりである。

別紙×に記載のマネジメントと管理策の評価手続を実施した結果、

(1) 「管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載している」とする経営者の言明は委託元の期待する水準にあると認める。

(2) 「○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されている」とする経営者の言明は委託元の期待する水準にあると認める。

(3) 「管理手続に記載された○○業務の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されている」とする経営者の言明は委託元の期待する水準にあると認める。

3．マネジメントと管理策の変更による影響及び統制の限界

会社の情報セキュリティに係るマネジメントと管理策の管理手続は 20xx 年 x 月 x 日現在のものであり、情報セキュリティに係る特定のマネジメントと管理策に関連して実施した評価手続は 20xx 年 x 月 x 日から 20xx 年 x 月 x 日までの期間を対象にしている。それ以降については情報セキュリティに係るマネジメントと管理策は変更されることがあるが、私たちの上記の意見は、変更があった場合のその影響を考慮したものではない。また、マネジメントと管理策には不正や誤謬を防止・発見する上での限界があるため、会社の情報セキュリティに係る特定のマネジメントと管理策により不正や誤謬が発生しているにもかかわらず発見されない可能性がある。

なお、この報告書は、委託元のための情報利用を意図したものであり、委託元及び貴社以外の第三者の利用を意図したものではなく、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）

監査の範囲及び情報セキュリティ監査手続

1　監査の範囲

2　監査手続

情報セキュリティ対策の設計

- ✧ ＸＸＸに求められる情報セキュリティのレベルの把握を適切に行っている
- ✧ リスク分析手法を確立し、リスクを評価するための基軸を設けている
- ✧ 適切なリスク分析及びリスク対応により、ＸＸＸに求められる管理策を選択し設計している
- ✧ 設計された情報セキュリティ対策が、ＸＸＸに求められる情報セキュリティレベルを達成することが確かめられている

情報セキュリティ対策の実装･運用

- ✧ 設計された情報セキュリティ対策の全てが、実装され運用されている
- ✧ 個々の情報セキュリティ対策の有効性を維持する仕組みがある
- ✧ 全体としてＸＸＸに必要な情報セキュリティレベルの維持向上のメカニズムが組み込まれている

実施した情報セキュリティ監査手続とその結果　(一部の例)

| 項番 | 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 |
|---|---|---|---|---|
| 5 | 通信及び運用管理 | サーバルームへの可搬媒体の持込み・持出しは記録すること。 | 持込み・持出しは記録の査閲。 | ○<br>実施していると認められる。 |
| 6 | : | 可搬媒体を処分する際は、粉砕等の物理的破壊を実施すること。 | 物理的破壊の実施、立会いの有無の確認 | ○<br>実施していると認められる。 |
| 7 | : | : | | : |
| | : | | | : |

注：発見事項を追記することもある。
監査手続が適正に行われたことを示すため、監査結果を認定するに必要かつ重要とされた証拠の名称などを必要に応じて記載する。

20xx 年 x 月 x 日

*［委託元］殿*

*［報告先代表者名］*

○○業務の情報セキュリティ管理手続に関する経営者の言明

当社は、○○業務を実施するうえで下記の情報セキュリティ管理手続に準拠した情報セキュリティレベルを達成するために、次のとおり適用している。

(1) 管理手続は、すべての重要な点において○○業務の情報セキュリティに係るマネジメントと管理策の整備状況を適切に記載している。
(2) ○○業務の情報セキュリティに係るマネジメントと管理策は、会社が定めた情報セキュリティレベルを達成するように適切に設計されている。
(3) 管理手続に記載された会社の情報セキュリティに係るマネジメントと管理策は、20xx 年 x 月 x 日現在において実際に情報セキュリティの運用に適用されている。

記

| 監査領域 | 情報セキュリティ管理手続 |
|---|---|
| 通信及び運用管理 | サーバルームへの可搬媒体の持込み・持出しは記録すること。 |
| : | 可搬媒体を処分する際は、粉砕等の物理的破壊を実施すること。 |
| : | : |
| : | |

－以上－

**上記雛型における下線部①について**　三者契約の場合は委託元も含める。

**上記雛型における下線部②について**　利用者合意方式の情報セキュリティ監査報告書様式２は、社会的合意方式と概ね似た構成からなっているが、一般多数の利用者を想定している社会的合意方式に対して、利用者合意方式では利用者が委託関係にある委託元のように特定されていることから、監査報告書の内容もより具体的な記述に置き換わっている。

**上記雛型における下線部③について**　利用者合意方式の情報セキュリティ監査報告書様式２は、監査手続の十分性について監査人が責任を負うため、監査手続が十分でない場合には、監査人は監査意見を表明できないことに留意しなければならない。つまり、利用者合意方式では、利用者に要求事項に基づいた管理手続を被監査主体が作成し、その管理手続に準拠して情報セキュリティのマネジメントと管理策が構築されているかどうかについて監査人は意見を表明する。その場合に監査人が採用した監査手続の十分性（監査証拠の十分性）については監査人の判断により監査人が必要と考える監査手続を選択することになる。