

電子政府情報セキュリティ監査基準モデル

Ver1.0

． X省における情報セキュリティ監査の目的と要請

X省における情報セキュリティ監査の目的は、X省における情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証、評価し、適切な助言を行うことにある。

X省の情報セキュリティ監査は、電子政府の情報セキュリティ監査の一環として行われるものである。したがって、その監査は、国家の安全保障、国民のプライバシー及び人権擁護、国民の社会生活の安全かつ安定的運営に資するものでなければならず、また国際的にみても遜色のない情報セキュリティの水準を達成するという観点からする監査が求められる。

情報セキュリティ監査人は、かかる観点を踏まえて、X省が国民に対するアカウントビリティを果たすことができるよう、X省の情報セキュリティ対策の現状を踏まえて、リスクに応じた要改善事項を助言しなければならない。

情報セキュリティ監査の要請は、X省において事故又はトラブルが発生する前に情報セキュリティに係る欠陥を明らかにして、必要な改善手当てを適時に講ずることにより、そのための有効な施策でなければならない。

・情報セキュリティ監査受嘱上の留意事項

1. 情報セキュリティ監査人の独立性要件

1.1 X省における情報セキュリティ監査は、監査の客観的な実施を担保するため、X省とは独立した立場にある情報セキュリティ監査人（他人の求めに応じて情報セキュリティ監査を行うことを業とする個人事業主、監査法人、会社等をいう）によって行われなければならない。

1.2 情報セキュリティ監査人は、監査の実施に当たって、外観上の独立性及び精神上的の独立性を保持しなければならない。例えば、X省の情報セキュリティ対策の構築に関与した者が、当該情報セキュリティ対策が適切かどうかを監査することは、情報セキュリティ監査人の外観上及び精神上的の独立性確保の観点から禁止されなければならない。

1.3 情報セキュリティ監査人がX省と監査契約を締結する場合において、成功報酬を契約事項に含めること、及び特定のセキュリティ製品等の採用を推奨すること（付随サービスの提供を含む）は、情報セキュリティ監査人の外観上及び精神上的の独立性を著しく害する危険性があることに留意しなければならない。

1.4 情報セキュリティ監査人が個人事業主である場合において、監査契約の締結時に次の条件に該当する場合には、外観上の独立性を損う利害関係があるものとして、情報セキュリティ監査業務の受嘱が禁止される。

- ・ 情報セキュリティ監査人が、現在又は過去において、X省の在職者である場合。
- ・ 情報セキュリティ監査人が、現在又は過去において、X省における、当該監査対象の情報システム（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている場合。
- ・ 情報セキュリティ監査人が、現在又は過去において、X省における、当該監査対象の情報セキュリティのマネジメント又はコントロール（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている場合。

1.5 情報セキュリティ監査人が監査法人又は会社等である場合において、監査契約の締結時に次の条件に該当する場合には、外観上の独立性を損う利害関係があるものとして、情報セキュリティ監査業務の受嘱が禁止される。

< 法人又は会社組織としての独立性侵害要件 >

- ・ 法人又は会社組織が、現在又は過去において、X省における、当該監査対象の情報システム（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている場合。
- ・ 法人又は会社組織が、現在又は過去において、X省における、当該監査対象の情報セキュリティのマネジメント又はコントロール（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている場合。

< 監査実施者としての独立性侵害要件 >

- ・ 監査従事者（監査責任者及び監査補助者）の中に、現在又は過去において、X省の在職者である者が含まれる場合。
- ・ 監査従事者（監査責任者及び監査補助者）の中に、現在又は過去において、X省における、当該監査対象の情報システム（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている者が含まれる場合。
- ・ 監査従事者（監査責任者及び監査補助者）の中に、現在又は過去において、X省における、当該監査対象の情報セキュリティのマネジメント又はコントロール（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている者が含まれる場合。

1.6 情報セキュリティ監査人が作成する監査報告書には、情報セキュリティ監査人とX省との間に特別な利害関係がない旨の記載が求められることから、監査受嘱時のみならず監査の実施過程においても、情報セキュリティ監査人は、監査人としての独立性を損うような外観を第三者に対して与えることがないようにしなければならない。

1.7 上記 1.4 から 1.6 に掲げる情報セキュリティ監査人としての外観上の独立性は、あくまでも監査人としての形式的属性を表象するに過ぎない。情報セキュリティ監査を公正かつ適切に遂行するためには、情報セキュリティ監査人は、とりわけ監査判断を行使する局面において公正不偏の精神的態度を保持しなければならない。

1.8 情報セキュリティ監査人として外観上の独立性を損ねることは、本来の独立性としての精神上の独立性に著しい悪影響を及ぼす可能性があることから、情報セキュリティ監査人に対してX省との間の経済上・身分上の利害関係を禁止していることに外観上の独立性の本旨がある。情報セキュリティ監査人としての独立性は、本来的には、精神上の独立性を保持することによってはじめて確保され得るものである。

2 . 情報セキュリティ監査人の能力要件

2.1 情報セキュリティ監査人は、情報セキュリティ監査を有効かつ効率的に実施できる能力を有するものでなければならず、かつ、適切な継続教育プログラム等を通じて常に情報セキュリティ監査に係る新たな知識及び技能の獲得に努めなければならない。

2.2 情報セキュリティ監査人は、次に掲げる知識及び技能を備えていなければならない。

- ・ 情報システムの企画、開発、運用、保守に関する知識及び技能
- ・ 情報セキュリティのマネジメント及びコントロールに関する知識及び技能
- ・ 情報セキュリティ技術に関する知識及び技能
- ・ 情報セキュリティ監査の実施（監査計画の立案、監査手続の選択適用、監査証拠の入手と評価、監査調書の作成、監査報告書の作成）に関する知識及び技能
- ・ その他の関連知識

2.3 情報セキュリティ監査人は、監査の実効性を高めるため、情報セキュリティ監査に係る専門的知識及び技能のみならず、高い分析能力と判断能力、並びに適切なコミュニケーション

ーション能力を備えていなければならない。

2.4 X省の情報セキュリティ監査を実施する監査人としての高度な専門能力の確保という観点から、監査人が個人事業主である場合においては、以下のいずれかの資格を有する者とする。

- ・ 情報処理システム監査技術者又は公認システム監査人
- ・ 情報セキュリティアドミニストレータ
- ・ ISMS 主任審査員又は ISMS 審査員
- ・ 公認情報システム監査人（CISA）

なお、個人事業主が他の個人事業主等と共同で情報セキュリティ監査を行う場合には、当該他の個人事業主等も上記のいずれかの資格を有する者であることが望ましい。

2.5 X省の情報セキュリティ監査を実施する監査人としての高度な専門能力の確保という観点から、監査人が監査法人又は会社である場合においては、以下のいずれかの資格を有する者を監査責任者とする。

- ・ 情報処理システム監査技術者又は公認システム監査人
- ・ 情報セキュリティアドミニストレータ
- ・ ISMS 主任審査員又は ISMS 審査員
- ・ 公認情報システム監査人（CISA）

なお、監査補助者には、上記のいずれかの資格を有する者複数名を含めることが望ましい。

2.6 X省の情報セキュリティ監査を実施する監査人は、上記 2.4 及び 2.5 に定める資格要件に加え、情報セキュリティ監査企業台帳に登録されている者とする。

3 . 情報セキュリティ監査人の誠実性と職業倫理

3.1 情報セキュリティ監査人は、監査目的及び監査対象の公益性に鑑み、慎重な注意と高い倫理観をもって誠実に監査業務を遂行しなければならない。

3.2 情報セキュリティ監査人は、自らが所属する専門職団体が定めた倫理規則を遵守しなければならない。

3.3 情報セキュリティ監査人は、監査目的及び監査対象の公益性に鑑み、業務上知りえた事実等を正当な理由なく他に開示し、又は自己の利益のために利用してはならない。

3.4 X省の情報セキュリティ監査を実施する監査人に係る守秘義務は、当該監査実施期間中はいうまでもなく、当該監査終了後、さらには情報セキュリティ監査人としての業務を離脱した後においても適用される。

3.5 情報セキュリティ監査人が守秘義務の解除を図ることができる正当な理由としては、概ね次の事例が該当する。なお、被監査側を原告とする訴訟等の特殊な事情を除いては、当該監査を委嘱したX省部局の責任者の承諾を書面にて得ておく必要がある。

- ・ 訴訟において、情報セキュリティ監査人が自ら実施した監査業務の方法又は結果につ

いて、その正当性を立証する必要がある場合。

- ・ 情報セキュリティ監査人が所属する団体の法令又は会則等によって、業務内容についての質問又は調査に応じなければならない場合。
- ・ 後任の情報セキュリティ監査人に監査業務の引継ぎを行う場合。
- ・ 情報セキュリティ監査の目的を達成するため止むを得ない事情により、X省とは別の関連機関の情報セキュリティ監査を担当する監査人との業務連絡又は業務上の調整が必要とされる場合。

4. 情報セキュリティ監査に係る入札及び契約の締結に当たっての留意事項

4.1 X省の情報セキュリティ監査を受嘱しようとする場合には、「契約に係る競争参加者資格審査事務取扱要領」により、一定の入札適合条件を満たなければならないことに留意する。

4.2 X省の情報セキュリティ監査の入札に当たっては、X省から提示される情報セキュリティ監査業務請負仕様書に含まれる入札者適合証明書（関連する別添資料を含む）に必要事項を記入の上、提出が求められることに留意する。

4.3 X省の情報セキュリティ監査の入札に際し提出が求められる入札者適合証明書は、概ね（別紙 様式1）の通りである。なお、入札案件によっては当該証明書の様式が若干異なる場合があることに留意する。

4.4 X省の情報セキュリティ監査の入札に際し提出が求められる入札者適合証明書には、最低限、情報セキュリティ監査人の独立性要件、能力要件、及びその他必要とされる入札者適合要件を記載しなければならない。

4.5 X省の情報セキュリティ監査の契約の締結に当たっては、次に掲げる事項を含む監査契約書を作成し、X省との間で取り交わさなければならない。

- ・ 監査の目的
- ・ 監査の期間
- ・ 監査を受ける対象
- ・ 監査の際の判断の尺度
- ・ 監査従事者（監査責任者及び監査補助者）の氏名及び資格
- ・ X省において当該監査の実施及び管理を所管する担当者の所属部局及び氏名
- ・ 監査報告書の提出期限
- ・ 監査報酬の額及び支払の時期
- ・ 特記事項

4.6 情報セキュリティ監査人は、監査契約の締結に際して、当該監査の受嘱内容に応じ、速やかに適切な監査体制を整えなければならない。

4.7 情報セキュリティ監査の契約の締結に際して取り交わされる監査契約書の雛形は、概ね（別紙 様式2）の通りである。なお、監査契約は受嘱する監査の案件ごとに締結さ

れ、各々につき監査契約書を作成するため、監査契約書の様式は案件によって若干異なる場合がある。

・情報セキュリティ監査実施上の前提事項

1. 情報セキュリティ監査における準拠規範

1.1 情報セキュリティ監査の実施に当たっては、監査対象が情報セキュリティ対策に係る一定の条件を満たしているか否か、あるいは情報セキュリティ対策の実施状況が適切であるか否かについて評価する際の拠り所とすべき判断の尺度が必要となる。

1.2 X省の情報セキュリティ監査の実施に当たって用いる判断の尺度は、基本的には、監査契約に際して決定される。したがって、情報セキュリティ監査人は、監査の実施に先立って、監査上の判断の尺度として用いるべき基準等について、X省部局の担当者と予め合意しておく必要がある。

1.3 情報セキュリティ監査の実施に当たって監査上の判断の尺度を明確にしておくことは、情報セキュリティ監査人にとって、監査手続と監査意見表明の基礎を確立することになる。一方、X省における関係部局等の被監査側にとっては、採用すべき情報セキュリティ対策の枠組みを決定し、情報セキュリティ対策運用上の焦点が絞りやすくなる。

「電子政府情報セキュリティ管理基準」による監査

1.4 「電子政府情報セキュリティ監査基準」に従ってX省の情報セキュリティ監査を実施する場合には、「電子政府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用いることを原則とする。ただし、情報セキュリティ監査の要請によって、「電子政府情報セキュリティ管理基準」以外の適切な管理基準等を、情報セキュリティ監査上の判断の尺度として用いることもできる。

1.5 「電子政府情報セキュリティ管理基準」は、JIS X 5080 (ISO/IEC 17799) に基づく「情報セキュリティ管理基準」に従って電子政府の特性を加味して作成されたものであり、情報セキュリティに係るマネジメント体制確立のための国際規格と整合性のとれたものとなっている。「電子政府情報セキュリティ管理基準」は、電子政府の情報資産を保護するために、情報セキュリティ対策の水準を設定し運用する際の標準的な管理項目を規定し、最善実務慣行として示したものであるから、当該管理基準を基礎として、X省において必要な項目を追加し、あるいは項目を削除して活用することができる。

1.6 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、「電子政府情報セキュリティ管理基準」の趣旨及び枠組みを尊重し、当該基準の全ての項目について監査の対象とすることが望ましい。ただし、情報セキュリティ監査の要請又は目的、ないしは監査対象の特性又はリスクの程度を考慮して、当該管理基準の一部の管理項目（例えば、外部委託契約に係る管理項目等）を監査の対象とすることができる。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。

1.7 監査の実施に当たって、「電子政府情報セキュリティ管理基準」を判断の尺度として

用いる場合、情報セキュリティ監査人は、当該基準において管理項目ごとにその管理目的を記述した「目的」、及び管理目的を達成するための統制目標を記述した「コントロール」を判断尺度の枠組みとして用いることになる。当該管理基準において「サブコントロール」として記述された事項は、統制目標を具体的に達成するための統制手段の例示を記述しており、被監査側のリスクを考慮して監査手続を具体的に実施する局面で適宜取捨選択すべき事項であることに留意する。また、管理目的、統制目標自体が不足している、統制目標を達成するために必要な統制手段が不足しているとX省が判断した場合は、管理目的、統制目標、統制手段を適宜追加することが必要となることに留意する。

その他の管理基準等による監査

1.8 X省の情報セキュリティ監査において、「電子政府情報セキュリティ管理基準」以外の管理基準等を用いる場合には、監査の目的等に照らして、管理基準としての体系性、標準性、適用可能性等について、情報セキュリティ監査人は慎重に検討しなければならない。

1.9 情報セキュリティ対策に係る管理項目を含む管理基準等で政府機関が公表している国内基準には、経済産業省「システム監査基準」、「情報システム安全対策基準」、「コンピュータウイルス対策基準」、「コンピュータ不正アクセス対策基準」、総務省「情報通信ネットワーク安全・信頼性基準」、警察庁「情報システム安全対策指針」等がある。

1.10 情報セキュリティ対策に係る管理項目を含むその他の管理基準等で国際的に認知度が高いものに、内部監査協会(IIA)の「eSAC」、情報システムコントロール協会(ISACA)の「COBIT」、アメリカ公認会計士協会(AICPA)/カナダ勅許会計士協会(CICA)の「Trust業務原則及び規準」などがある。

1.11 情報セキュリティ監査における監査上の判断の尺度として、上記 1.9 及び 1.10 に限らず、各種公的機関又は監査サービス会社等で作成した管理基準等、あるいはX省が独自に定めた管理規定(情報セキュリティ基本方針を含む)、CPS(認証局運用規程)、SLA(サービス水準合意書)等を用いることを妨げるものではない。

2 . 情報セキュリティ監査の目的

2.1 情報セキュリティ監査の実施に当たっては、監査の目的があらかじめ設定されていなければならない。情報セキュリティ監査には、X省が採用している情報セキュリティ対策の適切性に対して一定の保証を付与することを目的とする監査(保証型の監査という)と、情報セキュリティ対策の改善に役立つ助言を行うことを目的とする監査(助言型の監査という)があるが、X省の情報セキュリティ監査においては、助言型の監査を原則とする。なお、保証と助言の2つの目的は排他的なものではないため、助言型の監査に加え、一部の監査対象につき保証型の監査を監査契約に含めることを妨げるものではない。

2.2 保証型の監査を監査契約に含める場合、情報セキュリティ監査人は、監査契約の締結に先立って、保証型の監査の利点及び制約等についてX省部局担当者に十分な説明を行い、調整を重ねておく必要がある。保証型の監査が必要とされる場合には、助言型の監査

を通じてX省の情報セキュリティ対策が一定水準に達した段階で、保証型の監査に切り替えるという方策が考えられる。

2.3 助言型の監査とは、情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象の情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査をいう。助言型の監査の結論として表明される助言意見は、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はなく、改善を要する判断した事項を情報セキュリティ監査人の意見として表明するものである。

2.4 X省における行政事務及び行政サービスを提供するシステムには、広く国民が関与する公共性の高いシステムが含まれることがあり、またシステムによっては国民の個人情報を取扱うことからきわめて高い機密性の確保が要求される場合もある。助言型の監査は、X省における情報セキュリティ対策の改善を通じて、国民に対する行政サービスの安全かつ安定的な提供に資するものでなければならない。

情報セキュリティ監査の実施手順

1. 監査実施の基本的枠組み

1.1 X省を対象とした情報セキュリティ監査の実施過程を図示すれば次のようになる。図中、太字は「情報セキュリティ監査基準」「実施基準」で規定している箇所である。情報セキュリティ監査は、その目的又は実施形態を問わず、監査計画の立案、監査手続の実施（監査証拠の入手と評価）、監査報告書の作成を経て実施される。

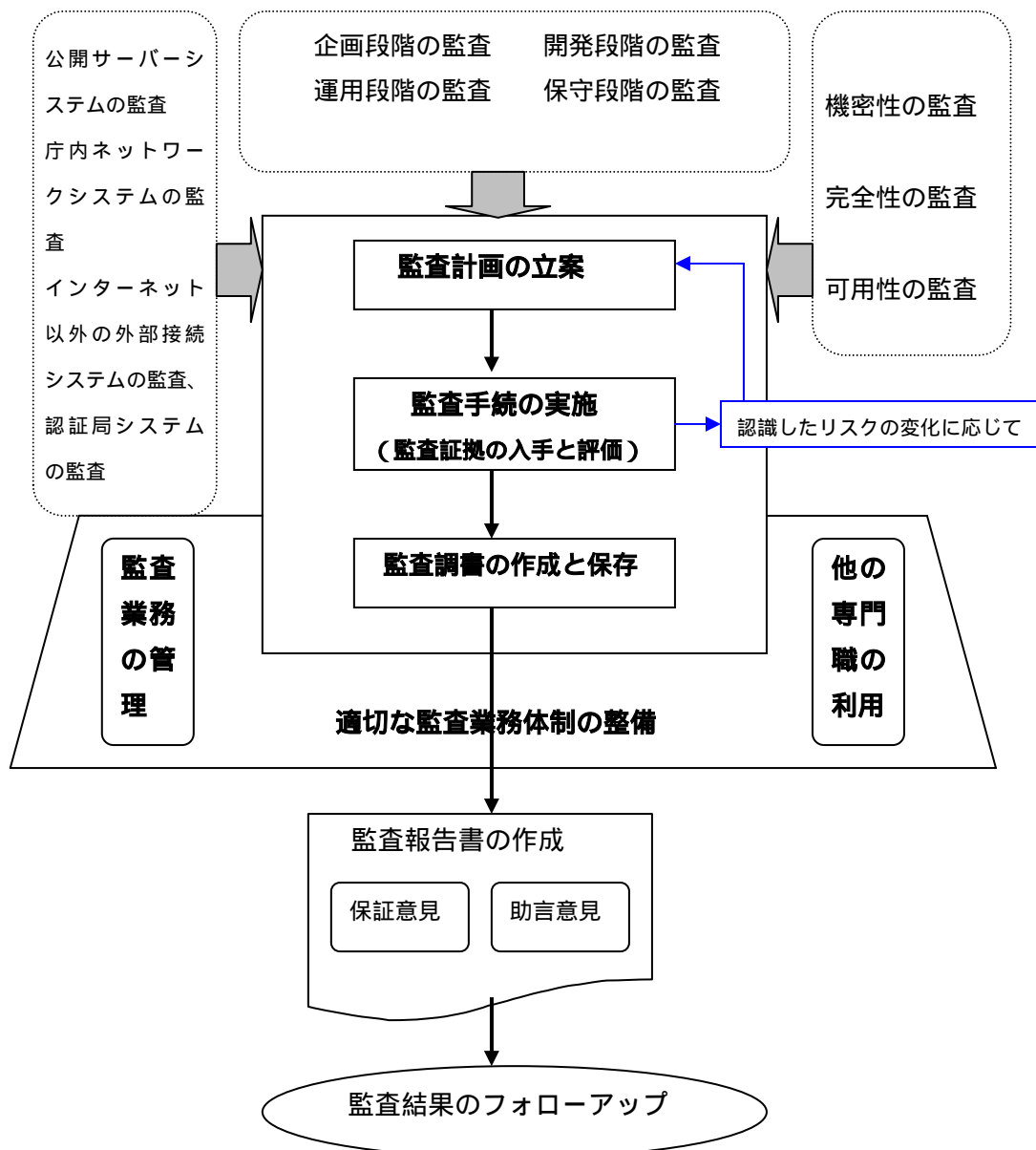


図 情報セキュリティ監査の実施過程

1.2 監査計画は、情報セキュリティ監査を有効かつ効率的に実施する観点から、監査の基本的な方針と、実施すべき監査手続を立案する。監査手続は、監査計画に基づいて、十分かつ適切な監査証拠を入手し評価するために実施される。かかる監査実施の過程は、監査報告書作成の基礎とするため、監査調書として記録しなければならない。

1.3 情報セキュリティ監査を有効かつ効率的に実施するために立案される監査計画、及びそれに基づいて行われる監査手続は、適切な監査業務体制の確立によって担保される。したがって、情報セキュリティ監査人は、監査業務の全体が適切に管理できるような体制を整え、必要に応じて他の専門職の利用を考慮しなければならない。

2. 監査計画の立案

2.1 情報セキュリティ監査人は、情報セキュリティ監査を有効かつ効率的に実施するために、監査の基本的な方針を立案し、それに基づいて、実施すべき監査手続を具体的に決定し、必要な監査体制を整えなければならない。

2.2 情報セキュリティに係るリスクは常に変動するため、監査計画は、適切なリスクアセスメントの結果を反映していることが望ましい。また、監査計画は、リスクの変動に応じて適時に修正されなければならない。

監査基本計画の立案

2.3 情報セキュリティ監査人は、監査の基本的な方針として、次の事項を立案する。

- ・ 監査対象とする範囲（例えば、公開サーバーネットワークシステム）
- ・ 監査対象とする期間又は期日（例えば、200X年X月X日から200X年X月X日）
- ・ 監査対象とする段階（例えば、運用段階）
- ・ 監査対象に係る監査目標（例えば、機密性、完全性、可用性）
- ・ 監査業務の管理体制
- ・ 他の専門職の利用の必要性和範囲

2.4 監査の基本的な方針は、監査基本計画書として文書化する必要がある。監査基本計画書は、原則として年度計画として作成されるが、必要に応じて、長期計画、中期計画、及び年度計画に分けて策定する。

2.5 情報セキュリティ監査は、長・中期的な監査計画のもとで継続的あるいは定期的実施することが肝要である。

2.6 情報セキュリティに係る脅威は、それが原因となってさまざまな行政事務又は行政サービス上のリスクとして派生することがあるため、情報セキュリティ監査の基本的な方針は、X省で実施されている業務監査との連携を視野に入れて立案することが望ましい。

監査実施計画の立案

2.7 情報セキュリティ監査人は、監査の基本的な方針に基づいて、実施すべき監査手続についての詳細な計画として、次の事項を立案する。

- ・ 監査手続の実施時期

- ・ 監査手続の実施場所
- ・ 監査手続の実施担当者及びその割当て（専門職を利用するときはそれを含む）
- ・ 実施すべき監査手続の概要（必要に応じて、監査要点、実施すべき監査手続の種類、監査手続実施の時期、及び試査の範囲を含む）
- ・ 監査手続の進捗管理手段又は体制

2.8 実施すべき監査手続の詳細な計画は、監査実施計画書として文書化する必要がある。実施すべき監査手続の重複又は脱漏を防ぐため、いつ、どこで、誰が、どのような監査手続を実施するかを体系的に立案し、あわせて監査手続の進捗管理を行うための手段又は体制を計画に織り込んでおくことが肝要である。

2.9 情報セキュリティ監査人は、業務の機密性確保及び業務負担への影響等の観点から、監査実施計画書について、X省における担当職員との協議を求められ、かつ、作成後速やかに担当職員への提出を求められることがあることに留意する。

2.10 X省の担当職員への提出が求められる監査実施計画書の雛形は、概ね（別紙 様式 3）の通りである。なお、監査の案件によっては若干様式が異なることがあり、当該計画書の提出時期及び回数等が監査契約書に特記される場合があることに留意する。

監査計画立案における監査対象のリスクアセスメント

2.11 情報セキュリティ監査人は、リスクアセスメントの結果が、情報セキュリティに係るリスク処理の優先順位及びもっとも適切な管理活動を決定するための基礎となることを十分に理解し、監査計画の立案段階においてリスクアセスメントに基づいた監査上の戦略を構想しなければならない。

2.12 情報セキュリティ監査人は、監査計画の立案に役立たせるため、リスクアセスメントを実施することが望ましい。監査計画立案段階におけるリスクアセスメントは、重要な監査対象の戦略的決定にとって有益であるばかりでなく、リスクアセスメントの結果を実施すべき監査手続に反映させることによって全体としてメリハリのある情報セキュリティ監査を期待でき、もって監査目的を有効かつ効率的に達成することにつながる。

2.13 X省内のY課等、関連部局においてリスクアセスメントが行われている場合、情報セキュリティ監査人は、当該リスクアセスメントの適切性を確かめた上で、被監査関連部局によって実施されたリスクアセスメントの結果を監査計画の立案に活用することができる。X省内の被監査関連部局が行ったリスクアセスメントの適切性の判定に当たって、情報セキュリティ監査人は、リスクアセスメント手法の厳密性を検証するのではなく、リスク・マッピング等の工夫によって、リスクアセスメントの結果がコントロールと関連づけられたものであることを確かめておくことが重要である。

2.15 情報セキュリティに係るリスク情報の収集と評価に当たっては、情報システムの開発・運用・保守を主管する部局、文書関係部局、広報関係部局、人事関係部局、会計関係部局、庁舎管理関係部局等の関係者を一同に会した組織横断的なワークショップ形式によ

る自由な討議又は自己評価が効果的で効率的な場合がある。この手法は、RSA (Risk Self Assessment) 又は CSA (Control Self Assessment) と呼ばれることがある。これには、関係部局にリスク識別シート及びリスク自己評価表を配布し記入を求め、その結果をもとに情報セキュリティ監査人が必要なヒアリングを組み合わせる簡便法も含まれる。RSA を有効に活用すれば、情報セキュリティ監査人は、X省全体としての情報セキュリティに係るリスクを網羅的に把握でき、かつ部局横断的なリスクの派生を見極めることができる。リスク自己評価表の記入を求める場合には、現状を正確に、客観的に記入できるように、質問項目の内容、記入環境に留意すること。なお、RSA には、情報セキュリティに係るリスク情報をX省全体、あるいは関連部局間で共有することができ、また関連部局への教育的効果などの付随的効果も期待できる。

2.16 X省内の被監査関連部局で情報セキュリティに係るリスクアセスメントが行われていない場合又はリスクアセスメントが不適切である場合には、必要に応じて情報セキュリティ監査人がリスクアセスメントを行う必要がある。助言型の監査において、X省内の被監査関連部局によるリスクアセスメントが行われていない場合又はリスクアセスメントが不適切な場合には、当該事実、及び情報セキュリティ監査人によるリスクアセスメントの結果とそれに応じたマネジメント又はコントロールの整備及び運用に対する助言が重要な指摘事項となることがある。

監査計画立案における情報セキュリティ基盤についての評価

2.17 情報セキュリティ監査人は、監査実施計画の立案に当たって、監査対象とする範囲、監査対象とする段階、及び監査対象に係る監査目標の設定に当たって、X省全体としての情報セキュリティ基盤について理解しておくことが重要である。情報セキュリティはマネジメントサイクルとして機能し、個々の管理項目はそれらが有機的に結合されてはじめて有効に機能するからである。

2.18 情報セキュリティ監査人は、X省としての情報セキュリティ基盤について、関係者に対するヒアリング及び現状観察によって、統括者又は管理者の情報セキュリティに対する考え方及び理念、情報セキュリティに関する組織風土及び組織体制について理解しておく必要がある。

2.19 X省は、下図に示すように、政府の情報セキュリティの基本的な考え方(情報セキュリティ対策推進会議決定「情報セキュリティポリシーに関するガイドライン」(平成12年7月18日))に基づいて独自の基本方針を定め、次いでリスクアセスメントの結果に基づいて情報セキュリティ対策基準及びその具体的な実施手続を定めることが原則である。したがって、情報セキュリティ監査人は、まずもって政府の情報セキュリティの基本的な考え方及びX省独自の基本方針について理解しなければならない。

2.20 情報セキュリティ監査人は、図中矢印として示されたブレークダウンの過程に着眼し、政府の情報セキュリティの基本的な考え方に基づいて策定されたX省の基本方針を踏まえた上で、リスクアセスメントの結果に基づいて必要かつ適切な個別の対策基準を整備

され、それが具体的対策手続規程として展開されて、具体的なコントロールが有効に機能しているか否かという視点で情報セキュリティ監査を行うことが肝要である。

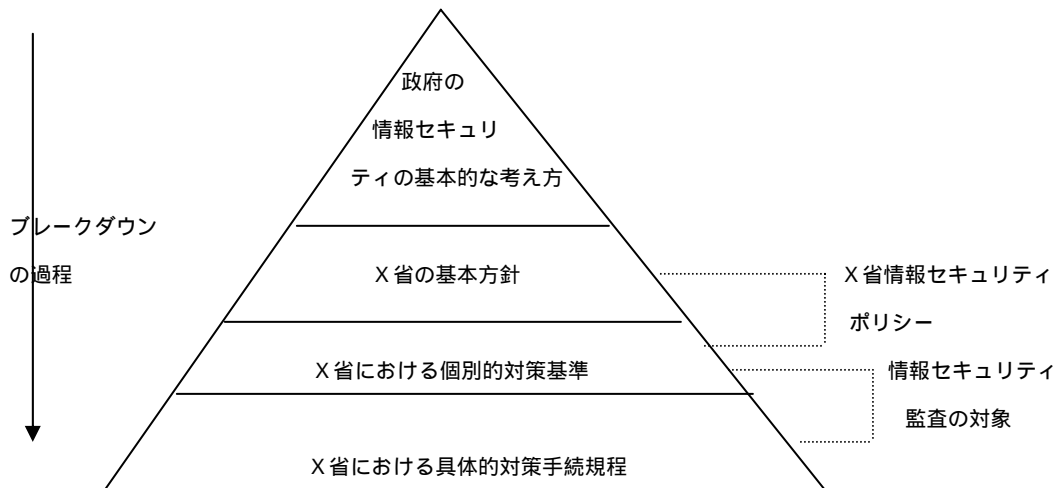


図 政府の基本的な考え方を踏まえたX省セキュリティポリシーの体系

3. 監査対象とする範囲（システム）に係る監査上の主要着眼点

3.1 情報セキュリティ監査は、X省の基本方針に基づいて、公開サーバーネットワークシステム、庁内ネットワークシステム、インターネット以外の外部接続システム、認証局システムなどの主要な監査対象ごとに実施されることがある。なお、その場合にあっては、X省の基本方針を踏まえて、個々の監査対象ごとの関連性及び整合性に留意しなければならない。

3.2 X省の基本方針に基づいて、公開サーバーネットワークシステム等の個別システムごとに監査を実施する場合、情報セキュリティ監査人は、監査要点の設定に当たり、システムの管理レベル、運用レベル、及び技術レベルでの対処事項を網羅すべく留意しなければならない。

公開サーバーネットワークシステム

3.3 管理レベル(マネジメントコントロール) X省に係る情報の公開に関する処理、及び不特定多数の外部者からの要求を受け入れて処理する役割を担う公開サーバーネットワークシステムは、その特性から庁内ネットワークシステムとは別個の個別的対策基準が適用されるのが通例である。しかしながら、当該個別的対策基準は、X省の基本方針の一環として、組織横断的な情報セキュリティ委員会において立案されていなければならない、庁内ネットワークシステムを対象とした個別的対策基準との整合性に留意する。なお、公開サーバーネットワークシステムは、インターネットに直面するシステムであるので、とりわけ緊急時対応計画と復旧計画については、インターネットにおけるインシデント対応を意識した内容となっているかどうかを監査上の主要な着眼点となる。

3.4 運用レベル（運用上のコントロール） 公開サーバーネットワークシステムにおいては、原則として、一般のエンドユーザのアカウントは存在しない。システム管理者が運用管理するシステムである。したがって、システム管理者が、インターネットサーバーについて、適切な運用を行っているか否かが監査上の主要な着眼点となる。また、当該ネットワークシステムはインターネットに直面するシステムであることから、緊急時対応計画と復旧計画を運用上のコントロールとして具体化する手順は、インターネットにおけるインシデント対応を意識した内容となっていなければならない。

3.5 技術レベル（技術的なコントロール） 公開サーバーネットワークシステムは、インターネットに直面し、不特定多数の外部者が接続するシステムであるから、Web ページの書き換え、Web サーバーに対する機能停止攻撃、Web サーバーを足がかりとした庁内ネットワークへの侵入など、情報セキュリティ侵害の脅威に常にさらされている。したがって、当該システムにおいて必要不可欠なサービスが最小限の権限で動作し提供するように設定され、外部侵入から適切に保護されるような適切な技術的対策が採用され運用されているかどうか監査上の主要な着眼点となる。

庁内ネットワークシステム

3.6 管理レベル（マネジメントコントロール） 庁内ネットワークシステムに適用される個別的対策基準における管理の要諦は、情報資産の区分管理にある。したがって、X省における情報資産がリスクに応じて適切に区分されているか否かが主要な監査上の着眼点になる。また、庁内ネットワークシステムでは、その特性から公開サーバーネットワークシステムとは別個の個別的対策基準が適用されるのが通例である。しかしながら、当該個別的対策基準は、X省の基本方針の一環として、組織横断的な情報セキュリティ委員会において立案されていなければならない、公開サーバーネットワークシステムを対象とした個別的対策基準との整合性に留意する。

3.7 運用レベル（運用上のコントロール） 庁内ネットワークシステムにおいては、情報資産の区分管理に係る運用が適切に行われているか否かが監査上の主要な着眼点となる。一般のエンドユーザのアカウントは、認可された情報資産についてのみアクセスでき、認可されていないアクセスは遮断されなければならない。また、庁内ネットワークシステムにおいては、エンドユーザがシステムを利用することから、エンドユーザに対する教育・啓発の実施についても、監査上の主要な着眼点となることに留意する。

3.8 技術レベル（技術的なコントロール） 庁内ネットワークシステムは、公開サーバーネットワークシステムとは異なりインターネットに直面していないが、技術的な設定及び運用が重要であることに変わりない。例えば、ルーターを標的としたサービス妨害攻撃（DoS 攻撃）がインターネット越しに可能であることが知られており（Smurf 攻撃など）、このような攻撃に対して影響を受けないような設定となっているかどうか主要な監査上の着眼点となる。また、情報資産の区分管理に適するアクセスコントロールが、適切に設定及び運用されているか否かも監査上の主要な着眼点となる。

インターネット以外の外部接続システム

3.9 管理レベル（マネジメントコントロール） 当該システムは、X省の外部のシステムに対してX省内部のエンドユーザ環境（端末等）から接続できるシステムであることから、エンドユーザ環境（端末等）の運用管理が外部主体に委託されることになる。したがって、当該システムの監査に当たっては、情報セキュリティ基本方針の設定主体が外部システムの所有者にあることに留意することが監査上の主要な着眼点となる。ただし、その場合においても、公開サーバーネットワークシステム及び庁内ネットワークシステムとの関係に留意し、当該外部主体の情報セキュリティ基本方針と、X省の情報セキュリティ基本方針との整合性を確かめておく必要がある。

3.10 運用レベル（運用上のコントロール） 当該システムは、X省の情報セキュリティ基本方針とは別の情報セキュリティ基本方針によって運用されることから、庁内ネットワークシステムとは別のシステムとして運用される必要がある。したがって、権限あるユーザのみが利用できるように、本人認証に係る厳正な運用と、本人認証手順の運用状況が監査上の主要な着眼点となる。

3.11 技術レベル（技術的なコントロール） 当該システムは、庁内ネットワークシステムとは切り離された別のシステムとして構築され設定される必要があることから、まずもって当該システムが、庁内ネットワークシステムと論理的あるいは物理的に分離されているか否かが監査上の主要な着眼点となる。なお、システム構成上の止むを得ない事情により、当該外部接続システムのエンドユーザ環境（端末等）を庁内ネットワークシステムが兼ねている場合には、権限あるユーザのみが利用できるよう、本人認証に係る技術が適切に提供されているか否かが主要な監査上の着眼点となることに留意する。

認証局システム

3.12 管理レベル（マネジメントコントロール） 認証局システムは、X省が所管するサイトとは別個の個別的対策基準に従って運用されることから、認証ポリシー（CP）に基づいてそれを実現するために適切な認証局運用規定が設定されているかどうか監査上の主要な着眼点となる。また、認証局システムはインターネットに直面するシステムであることから、緊急時対応計画と復旧計画を運用上のコントロールとして具体化する手順は、インターネットにおけるインシデント対応を意識した内容となっていなければならない。

3.13 運用レベル（運用上のコントロール） 認証局・登録局におけるサービスが安全かつ安定的に提供できるよう、運用手順が確立され適切に運用されているか否かが監査上の主要な着眼点となる。一般に認証局・登録局において守るべき情報資産は認証局自体の秘密鍵、個人情報及びCRL等の失効リストであるが、X省の認証局・登録局では個人情報を直接に扱わないことから、認証局自体の秘密鍵が適切に保護されているか否か、及び秘密鍵を用いた鍵生成等が適切であるかどうか留意する。

3.14 技術レベル（技術的なコントロール） 認証局及び登録局のシステムにおいては、認証局サーバー、証明書の失効リストを格納するリポジトリとしてのLDAPサーバー等、

固有のサーバーが稼働することから、これらのサーバーが適切に設定され運用されているか否かが監査上の主要な着眼点となる。

4 . 監査手続の実施（監査証拠の入手と評価）

4.1 情報セキュリティ監査人は、監査実施計画書に基づいて監査手続を実施するに際しては、監査実施通知書を作成し、X省内における当該監査業務を所管する管理者又は担当者を通じて、被監査関連部局に提出しなければならない。

4.2 X省の被監査関連部局への提出が求められる監査実施通知書の雛形は、概ね（別紙様式3）の通りである。

4.3 情報セキュリティ監査人は、被監査関連部局に対して抜打ちで監査手続を実施する必要があると判断した場合には、当該監査業務を所管する上級管理者と協議の上、実施の是非を含めて慎重に検討しなければならない。

4.4 情報セキュリティ監査人は、監査手続の実施に当たって、被監査関連部局から支障なく資料等の提示、関係者へのヒアリング、現場の視察等が行えるように、当該監査業務を所管する管理者に対して必要な要請を行う必要がある。

4.5 情報セキュリティ監査人は、自らの監査意見を裏付けるに十分かつ適切な監査証拠を入手しなければならない。監査証拠は、助言意見の根拠となるものであるから、その時の状況に応じてもっとも適切な監査手続を選択適用した結果得られたものでなければならない。

4.6 監査証拠は、関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、システムテストへの立会、テストデータによる検証及び跡付け、脆弱性スキャン、システム侵入テストなどの方法を通じて入手される。情報セキュリティ監査人が入手した資料等がそのまま監査証拠となるわけではない。情報セキュリティ監査人は、当該資料等の入手源泉及び入手時の状況を勘案して、監査証拠として採用するか否か、それが有する信用性及び程度を慎重に判断し、その結果等を明らかにしなければならない。

4.7 情報セキュリティ監査人は、入手した監査証拠の必要性と十分性の判断に当たって、被監査関連部局から提出された資料、監査人自ら入手した資料、監査人自ら行ったテストの結果等を総合的に勘案して、相互に矛盾があるか否か、異常性を示す兆候があるか否かを評価しなければならない。

4.8 情報セキュリティ監査人が入手した監査証拠の評価に当たっては、リスクアセスメントの結果との関連づけが考慮されることが望ましい。被監査関連部局が現に採用しているコントロールが適切であるか否かの判断は、リスクに応じたものでなければならない。リスクが相対的に高い場合にはより強力なコントロールが必要とされ、逆にリスクが低い場合にはそれに対応したコントロールとなる。

5 . 監査調書の作成と保存

5.1 情報セキュリティ監査人が実施した監査手続の結果と、監査手続に関連して入手した資料等は、監査の結論に至った経過がわかるように監査調書として作成し、情報漏えいや紛失を考慮して適切な方法によって保管しなければならない。

5.2 監査調書とは、情報セキュリティ監査人が行った監査業務の実施記録であって、監査意見表明の根拠となるべき監査証拠、その他関連資料等を綴り込んだものをいう。情報セキュリティ監査人自身が直接に入手した資料やテスト結果だけでなく、被監査部局から提出された資料を含み、場合によってはX省外部の第三者から入手した資料を含むことがある。

5.3 監査調書は、主として監査意見の根拠とするために作成されるが、次回以降の情報セキュリティ監査を合理的に実施するため、及び監査の品質管理の手段としても役立つ。さらには、情報セキュリティ監査人が正当な注意を払って監査業務を遂行したことの証左となることがある。

5.4 監査調書はさまざまな目的に役立つことから、監査調書の作成に当たっては、正確かつ漏れなく必要な事項を綴り込まなければならない、適当な参照符号を整備して情報セキュリティ監査人が監査の結論に至った経過が秩序整然と分かるように工夫しなければならない。

5.5 監査調書は、情報セキュリティ監査終了後も相当の期間、整理保存しておく必要がある。監査調書にはX省の機密事項が含まれていることから、保管場所や保管責任者の特定など、監査調書の保管には慎重な注意が求められる。とりわけ、暗号技術等の安全保障に関連する事項及び国民のプライバシーに関連する事項などの高度な機密性が要求される事項を含む監査調書の取扱いについては、X省において監査を所管する部局の管理者と十分に協議しておく必要がある。

5.6 監査調書は、監査業務の有効性と効率性を考慮して、情報セキュリティ監査人の判断において適宜工夫して作成されるものであるが、最低限の記載事項を含む監査調書の書式は、概ね（別紙 様式4）の通りである。

6 . 適切な監査業務の体制整備

6.1 情報セキュリティ監査人は、監査計画の立案、監査手続の実施、監査証拠の入手と評価、監査報告書の作成、監査報告に基づくフォローアップからなる一連の監査業務の遂行において、監査業務を効率的に実施し、かつ重要な問題点の見落とし等監査業務上の瑕疵が生じないように、監査業務の全体を管理しなければならない。

6.2 監査業務は、少ないコストで、最大限の効果が期待できるよう実施されるべきであるが、そのためには監査業務の品質確保が最も重要な要件となる。監査業務の品質管理は、適切な監査計画の立案、監査マニュアルの整備、及び監査調書のレビュー等を通じてなさ

れる。

6.3 情報セキュリティ監査が監査チームによって実施される場合には、適切な職務の分担に配慮し、監査担当者間における相互チェックが機能するような体制を整えることが望ましい。

6.4 監査計画の立案段階において想定しなかった状況変化(リスクの変化を含む)すなわち基本方針の変更、事業プロセスの変更、情報システムの新規開発、突発事象の発生等にも柔軟に対応できるように、あらかじめ必要な措置を講じておくことが望ましい。

6.5 十分かつ適切な監査証拠を入手するために、情報セキュリティ監査人が必要と認められた場合には、ネットワークスペシャリスト、システムアナリスト、ビジネスコンサルタント、技術士、弁護士、公認会計士等の専門職の支援を仰ぐことを考慮すべきである。なお、当該専門職からのアドバイスや監査手続の補助又は代行があっても、監査の結果についての責任は情報セキュリティ監査人にあることに留意しなければならない。専門職の支援を仰いだ旨を監査報告書において記載することを妨げるものではないが、情報セキュリティ監査人と当該専門職との間にあたかも責任の分担があるかのような記載とならないよう留意しなければならない。

・ 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X省の関係者（当該監査を所管する部局の管理者のみならず、被監査関連部局その他の関係者を含む）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 情報セキュリティ監査報告書は、監査報告の明瞭性という観点から、以下の区分に従って記載するものとする。

- ・ 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（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 . 監査意見の表明方法

2.1 助言意見の表明に当たっては、「電子政府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、あくまでも当該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。

2.2 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、X省との間の監査契約による。助言意見は、「電子政府情報セキュリティ管理基準」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具体的な改善提言があって、はじめて効果的なものとなることに留意する。そのため、情報セキュリティ監査人は、可能な限り、検出事項と併せて具体的な改善提言を付すこととする。その際、実現に係る改善提言の意思決定に關与することがあってはならない。

2.3 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。

3 . 監査意見記載上の留意事項

3.1 監査報告書における検出事項の記載は、あくまでもX省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保証を付与するような誤解を与える表現を用いてはならない。

3.2 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X省の判断であって、情報セキュリティ監査人はそれを強制することはで

<注>

1．上記難型における下線部 について 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。

2．上記難型における下線部 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、「電子政府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、「電子政府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、「電子政府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。

3．上記難型における下線部 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。

4．上記難型における下線部 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、企画段階、開発段階、運用段階、保守段階）及び監査対象に係る監査目標（例えば、機密性、完全性、可用性）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、公開サーバーネットワークシステム、庁内ネットワークシステム、インターネット以外の外部接続システム、認証局システム）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。

5．上記難型における下線部 について 「情報セキュリティの状況」について助言を行うことを原則とするが、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）」についての助言を行うことができる。

6．上記難型における下線部 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X省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。

7．上記難型における下線部 について 「電子政府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。

8．上記難型における下線部 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、「電子政府情報セキュリティ管理基準」等適切な管理基準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。

9．上記難型における下線部 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。

10．上記難型における下線部 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。

11．上記難型における下線部 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し、かつ、改善事項に基づいて必要な措置を講ずべき関係部局ごとに改善提言を分けて記載することが有益である。

12．上記難型における下線部 について 情報セキュリティ監査人は、監査報告書に記載した検出事項及び改善提言の被監査関係部局における実施状況を確認するため、被監査関係部局から「検出事項及び改善提言に係る措置回答書」を適宜入手しておく必要がある。検出事項及び改善提言に係る措置回答書は、概ね（別紙 様式5）の通りである。

(別紙 様式1)

<情報セキュリティ監査人が監査法人又は会社等である場合の例>

入札者適合証明書

平成 年 月 日
作成責任者 印

1. 監査人としての独立性要件

弊社は「電子政府情報セキュリティ監査基準」 . 1.6 で要求されている以下の独立性要件を、平成 XX 年 XX 月 XX 日現在、いずれも満たしております。

- ・
- ・ 弊社は、過去3年以内において、X省における情報システム（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っていません。
- ・ 弊社は、過去3年以内において、X省における情報セキュリティのマネジメント又はコントロール（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っていません。

弊社の監査従事者（監査責任者及び監査補助者）は「電子政府情報セキュリティ監査基準」 . 1.6 で要求されている以下の独立性要件を、平成 XX 年 XX 月 XX 日現在、いずれも満たしております。

- ・ 予定している監査従事者の中に、現在又は過去において、X省の在職者である者は含まれていません。
- ・ 予定している監査従事者の中に、過去3年以内において、X省における情報システム（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている者は含まれていません。
- ・ 予定している監査従事者の中に、過去3年以内において、X省における情報セキュリティのマネジメント又はコントロール（関連業務を含む）の企画、開発、運用、及び保守に係る業務を行っている者は含まれていません。

なお、詳細は、別添の「予定している監査従事者の略歴」をご参照下さい。

2. 監査人としての能力要件

弊社の監査従事者は「電子政府情報セキュリティ監査基準」 . 2.4 で要求されている

以下の能力要件を、平成 XX 年 XX 月 XX 日現在、満たしております。

予定している監査従事者（監査責任者及び監査補助者）の氏名及び資格は以下のとおりです。

監査責任者

氏名：

資格：

監査補助者 1

氏名：

資格：

監査補助者 2

氏名：

資格：

なお、監査責任者及び監査実施者が取得している資格については、別添の「資格証明書」をご参照下さい。

3. その他の資格要件

弊社は、情報セキュリティ監査企業台帳に関する規則に基づき、情報セキュリティ監査企業台帳に記載されております。

なお、情報セキュリティ企業台帳記載企業であることの証明及び詳細については、別添の「情報セキュリティ監査企業台帳抜粋」をご参照ください。

(別紙 様式2)

監査契約書

平成 年 月 日

X省(以下「甲」という)と_____ (以下「乙」という)は、監査請負契約を甲が乙に囑託するに必要な契約を以下の条項により締結するに当たり、その証として本書2通を作成し双方署名押印の上各1通を保有するものとする。

条 項

1. 監査の目的

2. 監査の期間

3. 監査を受ける対象

4. 監査の際の判断の尺度

5. 監査従事者(監査責任者及び監査補助者)の氏名及び資格

6. X省において当該監査の実施及び管理を所管する担当者の所属部局及び氏名

7. 監査報告書の提出期限

8. 監査報酬の額及び支払の時期

9. 特記事項

(別紙 様式3)

監 査 実 施 通 知 書

被監査部局担当者 殿

平成 年 月 日
監査責任者 印

平成×年度監査実施計画に基づき、下記により監査を実施しますので、ここに通知いたします。よろしくご協力のほどお願い申し上げます。

- 記 -

1. 監査日程： (自)平成 年 月 日()
(至)平成 年 月 日() _____日間
2. 監査対象：
3. 監査項目：
4. 監査場所：
5. 監査従事者：
6. 監査の実施に際して準備をお願いしたい書類・資料等：
7. 監査の実施に際して立会又は応答をお願いしたい方々：

(別紙 様式4)

監査調書

作成日 _____

被監査部局 _____

作成者 _____

監査実施日 _____

監査場所 _____

監査対象 _____

監査項目	監査資料	監査方法	監査結果	検出事項	改善提言	関連調書#
監査人メモ						

(別紙 様式5)

平成 年 月 日

監査責任者 殿
(写し) 殿

**監査報告書における検出事項及び
改善提言に係る措置回答書**

所属部局
作成者 印

監査報告書における検出事項及び改善提言に係る指摘事項に基づき、次の通りに措置するのでご回答します。

検出事項・改善提言	措置の内容及び経過	実施時期
		年 月 日
		年 月 日
		年 月 日
		年 月 日