ＩＴ委員会研究報告第39号

情報セキュリティ検証業務

平成22年５月18日
日本公認会計士協会

－目　　次－

Ⅰ　はじめに

１．本研究報告の目的

今日、事業体においては、その活動を有効かつ効率的に行うために、情報技術（以下「ＩＴ」という。）の利用が不可欠であり、内部統制体制の確立も含めた情報セキュリティを確保することが強く望まれている。

このような状況の中、公認会計士又は監査法人（以下「公認会計士等」という。）に対し、情報セキュリティの検証業務を求める声があることから、今般、ＩＴに係る保証業務等についての一般的な指針であるＩＴ委員会報告第５号「ＩＴに係る保証業務等の実務指針（一般指針）」（以下「ＩＴ５号」という。）を前提としつつ、情報セキュリティにおける合理的保証水準による保証業務としての検証業務について研究報告をまとめることとした。研究報告という性格上、本研究報告の内容は実務を拘束しないが、公認会計士等が情報セキュリティ検証業務を行う上で本研究報告を参考にしながら進めることが有効であると考えられる。

本研究報告は、公認会計士等が情報セキュリティ検証業務を実施する上で特に留意しなければならない事項をはじめ、必要となる評価規準、検証手続の考え方と例示、検証報告書の文例等を示したものである。また、当該検証業務を行う上での一般的な事項である法令や倫理規則等の遵守、保証業務を受嘱する要件、業務を実施する者の独立性、保証業務リスクの水準等に関する事項については、ＩＴ５号を踏襲することとし、本研究報告では詳細の記述はしていない。したがって本研究報告に記載のない事項については、ＩＴ５号の記載に従う必要があることに留意する。

本研究報告では、公認会計士等が行う情報セキュリティ検証業務をInternational Standards on Assurance Engagements 3000（国際保証業務基準第3000号）及びＩＴ５号における合理的保証業務として位置付けている。

本研究報告の一部を構成する情報セキュリティ評価規準については、情報セキュリティの整備及び運用状況に係る実務において経済産業省が公表し、広く利用されている「情報セキュリティ管理基準（平成20年改正版)」(平成20年経済産業省告示第246号）に基づき、上記の要件を踏まえつつ、特に公認会計士等が行う検証業務という観点から検討の上、策定したものである。情報セキュリティ評価規準は、検証対象である経営者の記述書作成の際の評価規準であるとともに、検証業務を実施する者の評価規準としても利用されるものである。この性格は財務諸表監査において、一般に公正妥当と認められる企業会計の基準が財務諸表の作成の基準となるとともに、監査人にとっては、財務諸表監査を実施する際の判断規準となるのと同趣旨である。

本研究報告が、公認会計士等が行う情報セキュリティ検証業務の実務を検討する上で一つのモデルとして参照され、実務のよりよい進展に寄与し得ることを期待するものである。

２．情報セキュリティ検証業務の概要

情報セキュリティ検証業務は、ＩＴに関連する環境、システム、組織、情報等に関するセキュリティについて、情報セキュリティにおける評価規準に照らして、経営者が評価した結果が示された経営者の記述書を対象として、その記載の適正性について検証業務を実施する者が検証し、業務依頼者に報告するものである。

本研究報告における情報セキュリティ検証業務の対象である経営者の記述書は、経営者の評価としての評点が示される。検証を経た経営者の記述書の評点によって、例えば、自社の年度ごと等の時系列比較が可能となり、第三者の評価を経たセキュリティマネジメント及びコントロールの改善の状況を利害関係者等に開示することも可能となる。

また、共通の評価規準と様式に基づいた経営者の記述書により、同一産業分野、異業種間でのセキュリティマネジメント及びコントロールの状況の事業者間比較も可能となり、例えば特定取引における事業者の選定基準の要件判定に利用することも可能である。経営者の記述書におけるセキュリティレベルについて一定の水準を満たしている者に業務機会を与えるなどの社会規範が想定されれば、広く社会的な情報セキュリティレベルを高めることにも有益であると思われる。

II　情報セキュリティ検証業務の構成要素と定義

本研究報告における情報セキュリティ検証業務の構成要素と定義は次のとおりである。

１．業務実施者

業務実施者とは、情報セキュリティ検証業務を行うための一定の専門的能力や経験をもち、当該業務を実施する公認会計士等をいう。情報セキュリティに関する一定の専門的能力・経験とは、一般に広く利用されている情報セキュリティに関わる基準(「情報セキュリティ管理基準（平成20年改正版)」(平成20年経済産業省告示第246号）等)を理解し、それに基づく業務経験を有することをいう。

２．主題に責任を負う者

主題に責任を負う者とは、情報セキュリティに関する管理状況について責任を負い、経営者の記述書を自己の責任において想定利用者に提示して説明する責任を負う者（以下「経営者」という。）をいう。

３．想定利用者

想定利用者とは、情報セキュリティに不備があった場合に影響を受ける者などをいう。例えば、被検証組織の商品の購入者又はサービスを受ける者が該当する。

４．情報セキュリティ検証業務における主題及び主題情報

情報セキュリティ検証業務における主題とは、情報セキュリティに係るマネジメ

ント及びコントロールの整備及び運用の状況（以下「情報セキュリティに関する管理状況」という。）をいう。また、主題情報とは、情報セキュリティに関する管理状況について情報セキュリティ評価規準への準拠状況を評価又は測定した結果を表明した経営者の記述書をいう。

5．主題を評価又は測定するための規準

主題を評価又は測定するための規準とは、本研究報告「Ⅳ　情報セキュリティ評価規準」をいう。

なお、情報セキュリティ評価規準は、管理規準とコントロール規準から構成されている（Ⅲ　1．(1) 参照)。

6．十分かつ適切な証拠

十分かつ適切な証拠とは、合理的保証を付与するために必要な証拠をいう。

7．情報セキュリティ検証報告書

情報セキュリティ検証報告書とは、経営者の記述書における主題情報の記載の適正性に関して、手続を実施した結果としての結論が表明される文書をいう。

Ⅲ　情報セキュリティ検証業務における留意点

1．評価指針

本研究報告における経営者の記述書に記載される経営者による評価及び業務実施者の検証に当たり適用される情報セキュリティ評価規準に対する準拠状況の評点は、次の評価水準による。

(1) 評点水準

- 情報セキュリティ評価規準の各項目への準拠の程度を次の評点水準で評価し、経営者の記述書の評点とする。

  管理規準　　：情報セキュリティマネジメントの計画、実行、評価及び改善に必要な実施項目に関する規準である。

  コントロール規準：情報セキュリティマネジメントにおけるリスク対応方針に従った具体的対策の評価項目に関する規準である。

- 評価に当たり、評価規準の評点は、情報セキュリティ評価規準の三階層の項目番号（例えば、1.1.1）ごとに実施し、二階層の項目に記載する。三階層の項目が複数ある場合は、各評点の最小値を二階層の項目に記載して経営者の記述書の評価を実施する。
- 業務実施者は、評点水準の判定に当たり、検証対象の状況を勘案し、業務実施者の職業的専門家としての合理的判断によることに留意する。

① 管理規準の評点水準

０：何もしていない。

１：何らかの実施はあるが、管理規準に準拠して文書化されていない。

２：管理規準に準拠して文書化されているが、運用が不十分である。

３：管理規準に準拠して文書化され、運用がなされている。

上記において「文書化されている」とは、管理規準における定義、方針、評価や決定、手順や手続等が、組織全体において文書として記述され、正式な承認を得ていることをいう。文書化の評価は、運用についての評価と区別して行われ、管理規準への遵守状況に応じて、「０」、「１」又は「２」の評点となる。

また、「運用が不十分」とは、定義、方針、評価や決定、手順や手続等の周知、使用、活動等が定められたとおり実行されていないことをいう。この場合、管理規準への遵守状況に応じて、「０」、「１」又は「２」の評点となり、定められたとおり実行されている場合は、「３」となる。

② コントロール規準の評点水準

０(未実施レベル)　　：何もしていない。

１(非正式実施レベル)：コントロールの正式な文書化が不十分である。

２(正式導入レベル)　：コントロールは正式に文書化を伴って運用されているが、組織全体として策定されていない。

３(組織的整備レベル)：コントロールは組織全体として正式に文書化され運用されている。

４(目標管理レベル)　：３に加え、モニタリングされている。

５(有機的改善レベル)：４に加え、常にコントロールの改善体制が有機的に運営されている。

上記において「文書化」とは、コントロール規準における定義、方針、評価や決定、手順や手続等について、組織全体において文書として記述され、正式な承認を得ることをいう。「文書化」については、コントロール規準への準拠状況に応じて、「０」、「１」、「２」又は「３」の評点となる。

また、「運用」とは、定義、方針、評価や決定、手順や手続等の周知、使用、活動等が、定められたとおり実行されていることをいう。「運用」については、コントロール規準への準拠状況に応じて、「０」、「１」、「２」、「３」、「４」又は「５」の評点となる。

(2) 規準間の整合性と評価の方法について

・　管理規準に係る評価に当たっては、関連するコントロール規準に係る評価との整合性に留意する。

・　各評価項目の評点の評価に当たっては、原則として統計的サンプリング等合理的な方法により実施する。

２．重要性

業務実施者は、検証手続を実施した結果、会社の情報セキュリティに関する管理状況の評価結果について記載した経営者の評価書に虚偽表示があり、検証報告書において肯定的結論を表明することができない場合において、その影響が経営者の記述書を全体として虚偽表示に当たるほど重要でないと判断したときは、限定的結論（結論限定）を表明することになる。

また、業務実施者は、検証手続を実施した結果、会社の情報セキュリティに関する管理状況の評価結果について記載した経営者の評価書に虚偽表示があり、その影響が経営者の記述書が全体として虚偽表示に当たるほど重要であると判断したときは、検証報告書において経営者の記述書が不適正である旨の否定的結論を表明することになる。

上記における影響とは、会社の情報セキュリティ体制や対策等に関する経営者の評価書における虚偽表示が単独で、又は複数組み合わせて情報セキュリティに関する管理状況全体に与える影響をいう。そしてその影響の重要性は、業務実施者が情報セキュリティ評価規準に照らし、量的要因として当該虚偽表示の項目数及び経営者が付した評点と業務実施者が検証した結果の乖離幅、また、質的要因として情報セキュリティに関する基本的なポリシー等具体的方策の整備及び運用に当たっての前提となる事項の整備状況など、当該虚偽表示が情報セキュリティの信頼性に与える影響の程度等を総合的に判断することとなる。

３．情報セキュリティ検証報告書の形式と記載事項

(1) 検証報告書の形式

情報セキュリティ検証業務の報告は、経営者により作成された経営者の記述書に対する結論を報告する方法による。情報セキュリティ検証報告書は、短文式報告書によるものとし、書面により報告する。

(2) 検証報告書の記載事項

検証報告書には、次の事項を記載する。

① 表題

業務実施者が監査法人の場合には、「独立した監査法人の情報セキュリティ検証報告書」とする。また、業務実施者が公認会計士の場合には、「独立した公認会計士の情報セキュリティ検証報告書」とする。

② 日付

検証報告書の日付は、検証業務終了の日とする。

③ 宛先

原則として、業務実施者と契約する者を宛先とする。

④ 業務実施者の氏名

想定利用者に対して情報セキュリティ検証業務に関する責任の所在を明ら

かにするため、当該検証業務を実施した業務実施者が監査法人の場合には、監査法人名及び当該検証業務を実施した公認会計士の氏名を記載する。

また、業務実施者が公認会計士の場合には、事務所名及び氏名を記載する。

⑤　経営者の記述書を作成する規準

本研究報告に定める情報セキュリティ評価規準とする。

⑥　検証報告書の利用制限

特定の目的についてのみに検証報告書の利用が限定される場合には、業務実施者は検証報告書にその旨を明記する。

⑦　経営者の記述書に関する記述

経営者の記述書に関する記述には、次のような項目を含む。

ア．経営者の記述書の評価に関連する一定時点又は期間

イ．経営者の記述書に関連する事業体名又は事業体の構成要素

ウ．想定利用者が注意しなければならない経営者の記述書の特徴に関する説明及びその特徴が、規準に従って経営者の記述書を評価する際の精度及び利用可能な証拠の説得力に及ぼす影響

経営者の記述書は、検証報告書に添付される。

⑧　経営者の識別及び経営者と業務実施者の責任

経営者（主題に責任を負う者（Ⅱ　２．参照））が経営者の記述書について責任を負うこと及び業務実施者の役割は経営者の記述書についての結論を独立した立場から報告することを想定利用者に対して知らせるためのものである。

⑨　検証業務に関するＩＴに係る保証業務を実施するための基準に準拠して業務が実施されたこと

本研究報告に準拠して業務を実施している旨を記載する。

⑩　実施した業務の概要

経営者の記述書に対する証拠収集の結果として、結論を記載するための合理的な基礎を得たことを記載する。

⑪　業務実施者の結論

ア．検証報告書の結論は、積極的形式で報告する。

イ．想定利用者が注意しなければならない経営者の記述書の特徴に関する説明が必要であると認められる場合には、結論区分において業務実施者の結論の前提となる事項を記載する。情報セキュリティ検証業務では、経営者の記述書を主題情報としているため、情報セキュリティ検証報告書が、情報セキュリティの有効性そのものに保証を与えているものではない旨を記載する。

ウ．業務実施者が肯定的結論以外の結論を報告する場合、検証報告書には

当該結論に至った理由を明確に記載する。

⑫　後発事象

重要な後発事象がある場合には当該後発事象の内容を記載する。

⑬　規準に照らして主題を評価又は測定する場合の重要な固有の限界

情報セキュリティ検証報告書の想定利用者が、当該業務の固有の限界について、十分に理解していないため、検証報告書上で明示的に記載することが適切と判断される場合には、有効性に関する過去の評価が将来期間には及ばないということを記載する。

⑭　利害関係の有無

会社と公認会計士等との間には、公認会計士法の規定に準じて記載すべき利害関係はない旨を記載する。

４．経営者の記述書

業務実施者は、経営者が主題情報を記載した経営者の記述書を入手し情報セキュリティ検証報告書の添付資料とする。

(1) 記載項目

経営者の記述書には、以下の項目を記載する。

①　主題となる情報セキュリティに関する管理状況

②　評価対象範囲、期間及び評価結果に関する記述

③　情報セキュリティに関する管理及び管理状況並びにその評価についての責任

・　経営者の記述書の作成責任

・　経営者の記述書の作成に関する最高責任者による署名（又は記名捺印）

・　経営者の記述書の作成に関する実務の責任者による署名（又は記名捺印）

(2) 経営者の評価書の対象範囲

経営者の評価書において何を対象としたかを明確にするため、対象範囲を記載する。経営者の評価書の対象範囲には、以下の項目が記載される。

①　対象資産

検証業務の主題となる情報セキュリティの対象となる資産

②　対象者

検証業務の主題となる情報セキュリティに関する管理状況において検証の対象となる人

③　論理的対策領域

検証業務の主題となる情報セキュリティに関する管理状況における論理的な範囲

④　物理的対象領域

検証業務の主題となる情報セキュリティに関する管理状況における物理的な範囲

(3) 経営者の評価書

情報セキュリティ評価規準の各規準の項目ごとに、「Ⅲ　１．評価指針」により経営者が評価した結果の評点水準に基づき記載する。

(4) 情報セキュリティ評価規準の評価項目

経営者の評価書において、情報セキュリティ評価規準の項目のうち評価対象外として除外した項目がある場合には、その旨及び理由を記載する。

主題となる情報セキュリティに関する管理状況に含まれない項目又は該当しない項目がある場合には、その旨を記載する。

５．経営者確認書の留意事項等

(1) 経営者確認書入手に関する留意事項

業務実施者は、経営者から経営者の記述書に関する責任及び必要と判断した確認事項を記載した書面を経営者確認書として入手する。

経営者確認書を入手できない場合には、業務手続の制約として取り扱い、情報セキュリティ検証報告書に限定付結論を報告するか、結論を表明しないことになる。また、この場合には、第三者への開示を制限するなどの利用制限を記述することもあわせて検討する。

(2) 経営者確認書に記載することが考えられる事項

通常、経営者確認書に記載することが考えられる事項は、次のとおりである。

① 経営者は、情報セキュリティの管理状況について記述した経営者の記述書の作成について責任を有していることを承知していること

② 経営者の記述書は、ＩＴ５号及び本研究報告に準拠して正しく作成されていること

③ 経営者は、業務実施者に対して経営者の記述書について認識している事項をすべて提供していること

④ 経営者は、業務実施者に対して要請のあった経営者の記述書に関連する記録をすべて提供していること

⑤ 重要な後発事象がある場合には当該後発事象の内容を記載する。ない場合にはその旨を記載する。

⑥ 最終的な責任を有する経営者の署名（又は記名捺印）を記載

⑦ その他の関連する事項

Ⅳ　情報セキュリティ評価規準

＜管理規準＞

1　情報セキュリティマネジメントの確立

1.1　適用範囲の定義

1.1.1　情報セキュリティマネジメントの適用範囲及び境界を定義することになっており、実施されているか。

1.2　ポリシーの策定

1.2.1　情報セキュリティ・ポリシーを策定し、コミットすることになっており、実施されているか。

1.3　リスクアセスメント

1.3.1　リスクアセスメントについて以下の項目を規定し、運用しているか。

- 　リスクアセスメントの方法
- 　リスクの特定
- 　リスクの分析評価

1.3.2　リスク受容基準及びリスクの受容可能レベルを策定し、承認することになっており、実施しているか。

1.4　コントロールの選択

1.4.1　コントロールの選択について以下の項目を規定し、運用しているか。

- 　リスク対応の選択肢の特定及び評価
- 　リスク対応のための管理目的及びコントロールの選択

1.4.2　残存リスクについて経営者の承認を得ることになっており、実施しているか。

1.5　情報セキュリティマネジメントの承認

1.5.1　情報セキュリティマネジメントを導入し運用することについて経営者の承認を得ることになっており、実施しているか。

2　情報セキュリティマネジメントの導入と運用

2.1　リスク対応計画

2.1.1　リスク対応計画を策定することになっており、計画を策定し実施しているか。

2.1.2　リスク対応計画の実施のための経営資源を提供することになっており、実施しているか。

2.2　コントロールの実施

2.2.1　管理目的を満たすためにコントロールが導入され実施しているか。

2.2.2　実施したコントロール又は一連のコントロールの有効性の評価及びその結果の活用について規定し、運用しているか。

2.3　情報セキュリティマネジメントの運用管理

2.3.1　情報セキュリティマネジメントについて以下の項目を規定し、運用しているか。

・　情報セキュリティマネジメントの運用管理
・　情報セキュリティマネジメントのための経営資源を管理しているか。
・　迅速にセキュリティイベントを検知可能であり、セキュリティインシデントに対応できるための手続及びそのためのコントロールを実施しているか。

2.4　教育、訓練、意識向上及び力量

2.4.1　情報セキュリティ・ポリシーに適合することの重要性を組織に伝えているか。

2.4.2　情報セキュリティマネジメントに影響がある業務に従事する要員に必要な力量を決定し、的確な要員の養成若しくは雇用などの処置を取ることになっており、実施しているか。

2.4.3　教育、訓練、技能、経験及び資格について記録を維持し、教育、訓練、意識向上に関して有効性の評価を実施することになっており、実施しているか。

2.4.4　関連する要員すべてが、情報セキュリティについての活動が持つ意味と重要性とを認識し目的達成に向けて自分がどのように貢献できるかを認識することになっており、実施しているか。

3　情報セキュリティマネジメントの監視及びレビュー

3.1　有効性の継続的改善

3.1.1　情報セキュリティマネジメントの有効性を継続的に改善することになっており、実施しているか。

3.2　監視及びレビューの準備

3.2.1　監視及びレビューの手続について以下の項目を規定し、運用しているか。

・　監視及びレビューの方法
・　内部監査の確実な実施
・　マネジメントレビューの実施
・　その他のコントロール

3.3　コントロールの有効性評価

3.3.1　情報セキュリティマネジメントの有効性について以下の項目を規定し、運用しているか。

・　情報セキュリティマネジメントの有効性について定期的なレビュー
・　コントロールの有効性の測定
・　定期的な内部監査の実施

3.3.2　内部監査について以下の項目を規定し、運用しているか。

・　内部監査プログラムの作成

・　内部監査の基準、範囲、頻度及び方法の定義
・　内部監査プロセスの客観性及び公平性の確保
・　内部監査の計画、実施、結果に関する責任及び要件に関する定義を文書化しているか。
・　内部監査の発見事項等について、対応措置を取ることが確保されているか。
・　フォローアップは対応措置の検討及び検討結果の報告を含んでいるか。

3.4　情報セキュリティマネジメントの継続性評価

3.4.1　変化に対応するために、定期的にリスクアセスメントを行うことになっており、実施しているか。

3.4.2　マネジメントレビューを定期的に行うことになっており、実施しているか。

3.4.3　監視及びレビューによって判明した事実を反映するために、情報セキュリティマネジメント計画を更新することになっており、実施しているか。

3.4.4　情報セキュリティマネジメントの有効性及びパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録することになっており、実施しているか。

3.4.5　レビューの結果を明確に文書化し、記録を維持し、その結果を反映した改善策を検討することになっており、実施しているか。

4　情報セキュリティマネジメントの維持及び改善

4.1　改善策の導入

4.1.1　特定した改善策は、意図した目的の達成を確実にするよう、情報セキュリティマネジメントに導入することを規定し、運用しているか。

4.1.2　自他の組織が経験したことから学んだ内容を考慮して改善策が策定されるよう規定し、実施しているか。

4.1.3　改善策をすべての利害関係者の状況に見合った適切な内容で伝え、必要に応じて対応の進め方について合意を得るよう規定し、運用しているか。

4.2　是正処置

4.2.1　情報セキュリティマネジメントの要件に対する不適合の原因を除去し、再発防止のするために是正処置の手続を規定し、運用しているか。

4.3　予防処置

4.3.1　情報セキュリティマネジメントの要件に対する不適合の発生を防止するため、起こりうる不適合の原因を除去するための予防処置の手続を規定し、運用しているか。

5　文書管理及び記録の管理

5.1　文書化

5.1.1　情報セキュリティマネジメントに関連する文書から、経営者の決定及び方針にたどれることを確実にするための手続を規定し、運用しているか。

5.2　文書管理

5.2.1　情報セキュリティマネジメントに関連する文書を保護し、管理するための管理活動を定義した手続を規定し、運用しているか。

5.3　記録の管理

5.3.1　情報セキュリティマネジメントの運用に関する有効な証拠を提供するために、法令又は規制の要件及び契約上の義務を考慮し、容易に識別が判読可能であり、検索又は再現可能であることに留意した記録を作成、必要期間の保管及び廃棄を含めた手続を規定し、運用しているか。

5.3.2　プロセスのパフォーマンスの記録及び情報セキュリティマネジメントに関係する重大なセキュリティインシデントの発生記録を保持することを規定し、運用しているか。

＜コントロール規準＞

1　セキュリティ・ポリシー

1.1　情報セキュリティ・ポリシー

1.1.1　情報セキュリティ・ポリシー文書を、全従業員に通知し、関連する外部関係者に公表するよう規定し、運用しているか。

1.1.2　定期的に又は重大な変化が発生した場合に、情報セキュリティ・ポリシーを引き続き適切、妥当及び有効であることを確実にするためにレビューするよう規定し、運用しているか。

2　情報セキュリティのための組織

2.1　内部組織

2.1.1　情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当てを文書化し、組織内におけるセキュリティを支持するように規定し、運用しているか。

2.1.2　情報セキュリティ活動について、文書化された関連する役割及び職務機能をもつ様々な部署の代表が調整するように規定し、運用しているか。

2.1.3　以下の項目を含むすべての情報セキュリティ責任を明確に規定し、運用しているか。

- 新しい情報処理設備に対する経営者による承認プロセス
- 情報保護に対する必要な秘密保持契約又は守秘義務契約のための要件の規定及びレビュー
- 関係当局との連絡体制の維持
- 情報セキュリティに関する研究会又は会議と情報セキュリティの専門家による協会又は団体との連絡体制の維持

2.1.4　情報セキュリティ及びその実施のマネジメントに対する組織の取組みにつ

いて、定期的に又は情報セキュリティに重大な変化が生したとき等必要の都度、随時に独立したレビューをすることについて規定し、運用しているか。

2.2　外部組織

2.2.1　外部組織がかかわる業務プロセスからの、組織の情報及び情報処理環境に対するリスクを識別し、外部組織にアクセスを承認する前のコントロールを規定し、運用しているか。

2.2.2　顧客に組織の情報又は資産へのアクセスを承認する前に、明確にしたすべてのセキュリティ要件を満たすように規定し、運用しているか。

2.2.3　組織の情報又は情報処理環境に関わる第三者との契約について、関連するすべてのセキュリティ要件を取り上げることを規定し、運用しているか。

3　資産の管理

3.1　資産に対する責任

3.1.1　すべての資産を明確に識別するとともに、重要な資産すべての目録を作成し、維持することを規定し、運用しているか。

3.1.2　情報及び情報処理環境と関連する資産のすべてについて、組織の中にその管理責任者を指定することを規定し、運用しているか。

3.1.3　情報及び情報処理環境と関連する資産の利用の許容範囲に関する規則について明確にすることを規定し、運用しているか。

3.2　情報の分類

3.2.1　組織に対しての価値、法的要件、取扱いに慎重を要する度合い及び重要性の観点から、情報の分類を規定し、運用しているか。

3.2.2　情報に対するラベル付け及び取扱いに関する適切な一連の手続について、組織が採用した分類体系に従うことを規定し、運用しているか。

4　人的資源のセキュリティ

4.1　雇用前

4.1.1　従業員、契約相手及び第三者の利用者について以下の項目を規定し、運用しているか。

・　組織の情報セキュリティ・ポリシーに従ったセキュリティ上の役割及び責任の文書化

・　すべての候補者における経歴などの確認に関連する法令及び規制又は倫理への準拠若しくは事業上の要件、アクセスされる情報の分類及び認識されたリスクに応じた確認の実施

・　契約上の義務の一部としての情報セキュリティに関する責任及び組織の責任を記載した雇用契約書の同意及び署名

4.2　雇用期間中

4.2.1　従業員、契約相手及び第三者の利用者について以下の項目を規定し、運用

しているか。

・　経営者による組織の確立された方針及び手続に従ったセキュリティの適用への要求

・　職務に関連する組織の方針及び手続についての適切な意識向上のための教育、訓練及び更新

・　セキュリティ違反を犯した従業員に対する正式な懲戒手続

4.3　雇用の終了又は変更

4.3.1　従業員、契約相手及び第三者の利用者について以下の項目を規定し、運用しているか。

・　雇用の終了又は変更の実施に対する責任の明確な定めと割り当て

・　雇用、契約又は合意の終了時における自らが所持する組織の資産すべての返却

・　雇用、契約又は合意の終了時における情報及び情報処理環境に対するアクセス権の削除及び変更時の修正

5　物理的及び環境的セキュリティ

5.1　セキュリティを保つべき領域

5.1.1　セキュリティを保つべき領域について以下の項目を規定し、運用しているか。

・　情報及び情報処理施設のある領域を保護するための物理的セキュリティ境界（壁、カードコントロールによる入口、有人の受付等）

・　セキュリティを保つべき領域において承認された者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コントロール

・　オフィス、部屋及び環境に対する物理的セキュリティ設計

・　火災、洪水、地震、爆発、暴力行為及びその他の自然災害又は人的災害による被害から物理的に保護する設計

・　セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設定

・　一般の人が立ち寄る場所（荷物などの受渡場所等）及び敷地内の承認されていない者が立ち入ることもある場所の管理又は承認されていないアクセスを避けるためのそれらの場所の情報処理環境からの分離

5.2　装置のセキュリティ

5.2.1　装置のセキュリティについて以下の項目を規定し、運用しているか。

・　装置の環境上の脅威及び災害からのリスク並びに承認されていないアクセスの機会を低減するような設置又は保護

・　装置のサポートユーティリティの不具合による停電又はその他の故障からの保護

・　データの伝送又は情報サービスのサポートを行うための通信ケーブル及び電源ケーブルの配線の傍受又は損傷からの保護
・　装置の可用性及び完全性を継続的に維持することを確実にするための保守
・　構外にある装置に対する作業に伴う構内での作業とは異なるリスクの考慮
・　記憶媒体を内蔵した装置における、慎重に取り扱うべき処分前のデータ及びライセンス供与されたソフトウェアの消去又は問題が起きないように上書きしていることを確実にするためのすべての点検
・　事前に承認のない装置、情報又はソフトウェアの構外への持出し禁止

6　通信及び運用管理

6.1　運用の手続及び責任

6.1.1　操作手続を文書化及び維持し、かつ必要とするすべての利用者に対して利用可能となるように規定し、運用しているか。

6.1.2　情報処理設備及びシステムの変更における管理するための規定を作成し、運用しているか。

6.1.3　組織の資産に対する、承認されていない又は意図しない変更若しくは不正使用のリスクを低減するために、職務及び責任範囲を分割するように規定し、運用しているか。

6.1.4　本番システムへの承認されていないアクセス又は変更によるリスクを低減するために、開発環境、テスト環境及び本番環境を分離するように規定し、運用しているか。

6.2　第三者が提供するサービスの管理

6.2.1　第三者が提供するサービスに関する合意に含まれるセキュリティコントロール、サービスの定義、及び提供サービスレベルが、第三者によって実施、運用、及び維持されることを確実にするように規定し、運用しているか。

6.2.2　第三者が提供するサービス報告及び記録を常に監視し、レビューするように規定し、運用しているか。また、監査も定期的に実施するように規定し、運用しているか。

6.2.3　関連する業務システム及び業務プロセスの重要性並びにリスクの再評価を考慮して、サービス提供の変更（現行の情報セキュリティ・ポリシー、手続及びコントロールの保守又は改善を含む。）を管理するように規定し、運用しているか。

6.3　システムの計画作成及び受入れ

6.3.1　要求されたシステム性能を満たすことを確実にするために、資源の利用を監視又は調整し、将来必要とする容量及び能力を予測するように規定し、運

用しているか。

6.3.2　新しい情報システム及びその改訂版又は更新版の受入れ基準を確立し、開発中及びその受入れ前に適切なシステムテストを実施するように規定し、運用しているか。

6.4　悪意のあるコード及びモバイルコードからの保護

6.4.1　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コントロール並びに利用者に適切に意識させるための手続を実施するように規定し、運用しているか。

6.4.2　モバイルコードの利用が承認された場合は、承認されたモバイルコードが、明確に定められたセキュリティ・ポリシーに従って動作することを確実にする環境設定を行うように規定し、運用しているか。また、承認されていないモバイルコードを実行できないように規定し、運用しているか。

6.5　バックアップ

6.5.1　情報及びソフトウェアのバックアップを、合意されたバックアップ・ポリシーに従って定期的に取得及び検査するように規定し、運用しているか。

6.6　ネットワークセキュリティ管理

6.6.1　ネットワークを脅威から保護するために、また、ネットワークを用いた業務処理システム及び業務処理ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理及び制御するように規定し、運用しているか。

6.6.2　すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について、セキュリティの特性、サービスレベル及び管理上の要件を特定し、また、いかなるネットワークサービス合意書にもこれらを盛り込むように規定し、運用しているか。

6.7　媒体の取扱い

6.7.1　資産の認可されていない開示、改ざん、除去又は破壊及びビジネス活動の中断を防止するため、以下のような媒体の管理のための手続を規定し、運用しているか。

・　取外し可能な媒体の管理の手続
・　不要になった媒体についてのセキュリティを保ちかつ安全な処分の手続
・　承認されていない開示又は不正使用から保護するための情報の取扱い及び保管の手続
・　システム文書の承認されていないアクセスからの保護の手続

6.8　情報の交換

6.8.1　情報交換における情報を保護するために、以下の項目を含めた正式な交換ポリシーを定め、手続及びコントロールを規定し、運用しているか。

・　あらゆる形式の通信設備を利用した情報交換
・　組織と外部組織との間の情報及びソフトウェアの交換について、両者間で合意
・　情報を格納した媒体を利用した情報交換
・　電子的メッセージ通信に含まれた情報の保護
・　業務処理システムの相互接続と関連がある情報の保護

6.9　電子商取引サービス

6.9.1　公衆ネットワークを経由する電子商取引又はオンライン取引に含まれる情報について、以下の項目を未然に防止するために保護することを規定し、運用しているか。
・　不正行為
・　契約紛争
・　不完全な通信
・　誤った通信経路設定
・　承認されていない変更、改ざん
・　承認されていない開示
・　承認されていない複製又は再生

6.9.2　承認されていない変更を防止するため、公開システム上で利用可能な情報の完全性を保護しているか。

6.10　監視

6.10.1　利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得し、また、将来の調査及びアクセスコントロールの監視を補うために、合意された期間、保持することを規定し、運用しているか。

6.10.2　情報処理設備の使用状況を監視する手続を確立し、また、監視活動の結果を定めに従ってレビューすることを規定し、運用しているか。

6.10.3　ログ機能及びログ情報について、改ざん及び承認されていないアクセスから保護することを規定し、運用しているか。

6.10.4　システムの実務管理者及び運用担当者の作業を記録することを規定し、運用しているか。

6.10.5　障害のログを取得、分析し、また、障害に対する適切な処置をとることを規定し、運用しているか。

6.10.6　組織又はセキュリティ領域内のすべての情報処理システム内の時刻について、合意された正確な時刻源と同期させることを規定し、運用しているか。

7　アクセスコントロール

7.1　アクセスコントロールに対する業務上の要件

7.1.1　アクセスコントロール・ポリシーについて、アクセスについての業務上及

びセキュリティ要件に基づいて確立文書化し、レビューしているか。

7.2　利用者アクセスの管理

7.2.1　すべての情報システム及びサービスへのアクセスを管理するために、以下の項目の手続を規定し、運用しているか。

・　利用者の登録・登録削除
・　特権の割当て、利用及び制限
・　パスワードの割当て

7.2.2　正式な手続を規定し、利用者のアクセス権を定められた間隔でレビューしているか。

7.3　利用者の責任

7.3.1　以下を含む利用者の責任に関わる手続を規定し、運用しているか。

・　パスワードの選択及び利用時の要求事項
・　無人状態にある装置の保護対策
・　書類及び取外し可能な記憶媒体に対するクリアデスク
・　情報処理設備に対するクリアスクリーン

7.4　ネットワークのアクセスコントロール

7.4.1　以下を含むネットワークコントロールに関わる手続を規定し、運用しているか。

・　利用することを特別に承認したサービスへのアクセス
・　遠隔利用者のアクセスの認証
・　特定の場所及び装置からの接続を認証するための自動の装置識別
・　診断用及び環境設定用ポートへの物理的及び論理的なアクセス
・　情報サービス、利用者及び情報システムのネットワーク上におけるグループごとの分割
・　共有ネットワーク、特に組織の境界を越えて広がっているネットワークについて、アクセスコントロール・ポリシー及び業務処理ソフトウェアの要件に沿った、利用者のネットワーク接続能力の制限
・　コンピュータの接続及び情報の流れが業務処理ソフトウェアのアクセスコントロール・ポリシーに違反しないことを確実にするためのルーティングのコントロールのネットワークへの実施

7.5　オペレーティングシステムのアクセスコントロール

7.5.1　以下を含むオペレーティングシステムのアクセスコントロールに関わる手続を規定し、運用しているか。

・　セキュリティに配慮したログオン手続によるコントロール
・　各個人の利用ごとの一意な識別子（利用者ID）と利用者が主張する同一性を検証するための適切な認証技術

・　パスワードを管理するシステムは対話式にし、また、良質なパスワードを確実にしているか。
・　システム及び業務処理ソフトウェアによるコントロールを無効にすることのできるユーティリティプログラムの使用の制限と管理
・　一定の使用中断時間経過後のセッションの遮断
・　リスクの高い業務処理ソフトウェアへの接続時間の制限

7.6　業務処理ソフトウェア及び情報のアクセスコントロール

7.6.1　以下を含む業務処理ソフトウェア及び情報のアクセスコントロールに関わる手続を規定し、運用しているか。
・　利用者及びサポート要員による情報及び業務処理ソフトウェアシステム機能へのアクセスの既定のアクセスコントロール・ポリシーに従った制限
・　取扱いに慎重を要するシステムの専用の（隔離された）コンピュータ環境の有無

7.7　モバイルコンピューティング及びテレワーキング

7.7.1　以下を含むモバイルコンピューティング及びテレワーキングに関わるポリシー、運用計画及び手続を策定し、運用しているか。
・　モバイルコンピューティング設備・通信設備を用いた場合のセキュリティ対策
・　テレワーキングの設備・通信設備を用いた場合のセキュリティ対策

8　情報システムの取得、開発及び保守

8.1　情報システムのセキュリティ要件

8.1.1　情報システムの取得、開発及び保守において、セキュリティのコントロールに関する要件を規定し、実施しているか。

8.2　業務処理ソフトウェアでの情報セキュリティ上の正確な処理

8.2.1　業務用ソフトウェアにおける情報の誤り、消失、認可されていない変更又は不正使用を防止するために、以下を含む業務処理ソフトウェアの処理手続を規定し、実施しているか。
・　入力データ仕様の妥当性の確認
・　処理ミスや故意による情報の毀損の有無を検出する妥当性確認機能
・　業務処理ソフトウェアの真正性を確実にするための要件及び必要なメッセージの完全性を保護するための要件の特定、また、適切なコントロールの特定、実施
・　出力データ仕様の妥当性の確認

8.3　暗号によるコントロール

8.3.1　情報を保護するための暗号によるコントロールの利用に関するポリシーを規定し、実施しているか。

8.3.2　暗号鍵の管理に関する管理手続を規定し、実施しているか。

8.4　システムファイルのセキュリティ

8.4.1　以下を含むソフトウェアの導入管理手続を規定し、運用しているか。

・　運用管理ソフトウェア及び業務処理ソフトウェアの導入時に使用するテストデータの選択、保護及び管理

・　プログラムソースコードへのアクセス権限者の限定

8.5　開発及びサポートプロセスにおけるセキュリティ

8.5.1　以下を含むソフトウェアの変更管理手続を規定し、実施しているか。

・　オペレーティングシステムの変更時、重要な業務処理ソフトウェアへの運用又はセキュリティの影響を確認

・　パッケージソフトウェアの変更が、抑止され、必要な変更だけに限られ、すべての変更が厳重に管理されること

・　変更作業時の情報漏えいの防止策

・　外部委託のソフトウェア開発の監督及び監視

8.6　技術的ぜい弱性管理

8.6.1　利用中の情報システムの技術的ぜい弱性について、関連情報を入手してリスク評価を実施し、特定されたリスクの対処及びその手段をとることを規定し、実施しているか。

9　情報セキュリティインシデントの管理

9.1　情報セキュリティの事象及び弱点の報告

9.1.1　適切な管理者への連絡経路を通して、情報セキュリティ事象をできるだけ速やかに報告するよう規定し、運用しているか。

9.1.2　従業員、契約相手先及び第三者等のすべての情報システム又はサービスの利用者が、システム又はサービスの中で発見、若しくは疑いをもったセキュリティ事象のすべてを記録、報告するよう規定し、運用しているか。

9.2　情報セキュリティインシデントの管理及びその改善

9.2.1　情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、以下を含む責任体制及び手続を確立し、運用しているか。

・　情報セキュリティインシデントの形態、規模及び費用を定量化し監視できるようにする仕組み

・　情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）となった際の、証拠の収集、保全及び提出の仕組み

10　事業継続管理

10.1　事業継続管理における情報セキュリティの側面

10.1.1　以下を含む事業継続に必要な情報セキュリティ要件を取り扱うための管理手続を策定し、運用しているか。

・　業務プロセスの中断をもたらす可能性のある事象について、その内容、発生確率、影響及び情報セキュリティに及ぼす結果を特定しているか。
・　要求されたレベルの維持及び時間内での復旧を含む、重要な業務プロセスの中断、不具合発生時の運用の維持又は復旧の計画
・　すべての情報セキュリティ上の要件及び計画事項が整合し、テスト及び保守の優先順位を特定した、一元化された事業継続計画の枠組み
・　事業継続計画のテスト及び有効性の確認

11　コンプライアンス

11.1　法的要件の遵守

11.1.1　各情報システム及び組織について、以下含むすべての関連する法令、規制及び契約上の要件並びにこれらの要件を満たすための組織の取組み方を規定し、運用しているか。
・　知的財産権を含むもの及び権利関係のあるソフトウェア製品の利用
・　消失、破壊及び改ざんから保護すべき重要な記録
・　個人データ及び個人情報
・　認可を受けるべき情報処理施設の利用・暗号化機能

11.2　セキュリティ・ポリシー及びスタンダードの遵守並びに技術的要件の遵守

11.2.1　セキュリティ・ポリシー及びスタンダードへの遵守のために、すべてのセキュリティ手順を規定し、運用しているか。

11.2.2　情報システムについて、セキュリティスタンダードの遵守に関して、定期点検しているか。

11.3　情報システムの監査に対する考慮事項

11.3.1　業務プロセスの中断のリスクを抑えるために、システムの点検を伴う監査における監査目標及び活動を計画するよう規定し、運用しているか。

11.3.2　情報システムの監査を実施するツールの不正な使用又は悪用を防止するために、これらのツールへのアクセスを抑制しているか。

Ⅴ　十分かつ適切な証拠を収集するための情報セキュリティ検証業務の手続

１．十分かつ適切な証拠

業務実施者は、結論を報告するに足る合理的な基礎を形成する十分かつ適切な証拠を入手することになる。本研究報告では、公認会計士等が行う情報セキュリティ検証業務を合理的保証業務として位置付けていることから、入手する証拠は検証業務リスクを合理的な低い水準に抑えるものでなければならないと考えられる。このため、次のような点に留意する必要がある。

- 内部証拠より外部証拠の証明力の強さ
- 内部統制が有効な場合の経営者から入手した証拠の証明力の強さ
- 間接証拠より直接証拠の証明力の強さ
- 口頭による証拠より文書により入手した証拠の証明力の強さ
- 写しより原本の証明力の強さ

（監査基準委員会報告書第31号「監査証拠」参照）

２．検証手続

経営者の記述書における経営者の評価を検証するために業務実施者が実施する検証手続は、合理的保証業務において求められる積極的形式での結論を報告するための保証水準に応じた、十分かつ適切な証拠を入手するための手続である。

財務諸表監査の過程で、ＩＴに係る内部統制のうち全般統制の情報セキュリティに関して検証手続が実施されているが、現行実務上、情報セキュリティの検証業務においても、同様の検証手続が実施されている場合が多い。

すなわち業務実施者は、検証技法に関していえば、次のような技法を組み合わせて証拠収集手続に適用している。

ア．視察
イ．観察
ウ．確認
エ．再計算
オ．再実施
カ．分析的手続
キ．質問

これらの技法が、情報セキュリティ評価規準における管理規準及びコントロール規準の物理的証拠、文書証拠及び伝聞証拠を求めるために一般的に利用される局面は、財務諸表監査における内部統制の検証に適用される技法と変わるものではない。

また、情報セキュリティのコントロール等の一部は、人手によらずＩＴによってなされるものであることが一つの特徴ある局面であり、これらに関わる検証技法と

して、次のようなものが利用される場合がある。

- プログラムテスト
- ペネトレーションテスト
- コンフィギュレーションレビュー
- データ整合・完全性テスト
- ログ解析

上述の技法はいずれも、財務諸表監査において、特にＩＴに係る内部統制の検証において広く利用されている。

このように情報セキュリティ評価の検証手続は、公認会計士等が実施する財務諸表監査の過程でＩＴに関わる内部統制の検証のために既に多く利用されていることから、財務諸表監査の検証手続と同様の手続で情報セキュリティ検証業務の実施が十分に可能である。

情報セキュリティの評価についての具体的な検証手続の一例を示せば、次のようなものが挙げられる。

評価規準	検証手続
管理規準	
1　情報セキュリティマネジメントの確立	
1.1　適用範囲の定義	
1.1.1　情報セキュリティマネジメントの適用範囲及び境界を定義することになっており、実施されているか。	①　情報セキュリティマネジメントに関する基本方針及び計画について、取締役会議事録等を閲覧し経営者の意思決定資料を確かめる。 ②　上述①の意思決定資料に、以下の項目について情報セキュリティマネジメントの適用範囲及び技術が記載されていることを確かめる。 ・　自らの事業 ・　体制 ・　所在地 ・　技術の特徴
1.2　ポリシーの策定	
1.2.1　情報セキュリティ・ポリシーを策定し、コミットすることになっており、実施されているか。	①　取締役会議事録等を閲覧し、情報セキュリティ・ポリシーが、経営者の意思の下、策定されていることを確かめる。 ②　情報セキュリティ・ポリシーを閲覧し、情報セキュリティマネジメントに関する基本方針及び計画に沿ったものであることを確かめる。 ③　社内通達文書等により、情報セキュリティ・ポリシーが、正式なプロセスを経て周知されていることを確かめる。
1.3　リスクアセスメント	
1.3.1　リスクアセスメントについて以下の項目を規定し、運用しているか。 ・　リスクアセスメントの方法 ・　リスクの特定 ・　リスクの分析評価	①　情報セキュリティ・ポリシーを閲覧して、リスクアセスメントに関する記述の箇所ないし文書を確かめる。 ②　リスクアセスメントについて、以下の項目についての記述を確かめる。 ・　リスクアセスメントの方法 ・　リスクの特定 ・　リスクの分析評価 ③　上述②の記述が適用されている規定及び手続を閲覧し、記述方針に沿っているか確かめる。

1.3.2　リスク受容基準及びリスクの受容可能レベルを策定し、承認することになっており、実施しているか。	①　リスク受容及びリスク受容可能レベルに関する記述文書が情報セキュリティ・ポリシーの記述または取締役会議事録等の承認の下、策定されているか確かめる。 ②　記述されたリスク受容基準及び受容レベルについて、適用された例および受容レベルを超えた際の取扱いを確かめる。
・ ・ ・	・ ・ ・

３．虚偽表示の報告等

業務実施者は、検証業務の実施において情報セキュリティ体制や対策等に関する経営者の評価書における虚偽表示、例えば、経営者が付した評点と業務実施者の検証結果の著しい乖離などを認識した場合には、経営者に報告して当該評価書における虚偽表示の是正を求めるとともに、その是正措置を確かめる。

Ⅵ　情報セキュリティ検証報告書

１．検証報告書における結論

業務実施者は、結論の報告として、経営者の記述書が情報セキュリティ管理状況をすべての重要な点において適正に表示しているかどうかについて表明する。

業務実施者は、検証業務リスクを合理的に低い水準に抑えたかどうか、自ら入手した十分かつ適切な証拠に基づいて自己の結論を形成するに足る合理的な基礎を得たかどうかを検討する。

(1) 肯定的結論

業務実施者は、上述事項を評価し、経営者の記述書が情報セキュリティ管理状況をすべての重要な点において適切に表していると認めるときは、肯定的結論を表明することになる。

なお、経営者の記述書に情報セキュリティの不備が適切に記載されており、情報セキュリティ管理状況をすべての重要な点において適切に表していると認めるときも同様に肯定的結論を表明することになる。

(2) 限定付結論等

業務実施者は、上述事項を評価し、虚偽表示がある場合、その重要性を勘案して肯定的結論、限定付結論（結論限定）又は否定的結論を表明することになる。

なお、情報セキュリティ検証業務の実務においては、業務実施者が発見した情報セキュリティ体制や対策等に関する経営者の評価書における虚偽表示は、経営者による是正の取組みがなされ、解消されるケースが多いことが想定されるため（上述Ⅴ　３．虚偽表示の報告等参照)、上述の限定付結論（結論限定）又は否定的結論を表明した検証報告書の発行に至るケースは極めて稀と考えられる。

(3) 範囲の制約

業務実施者は、経営者の記述書に対する結論を形成するに足る合理的な基礎を得るために、検証計画を策定し、当該検証計画に従って検証手続を実施するが、検証の状況によっては重要な検証手続を実施できない場合がある。この場合、業務実施者は検証範囲の制約としてその重要性を勘案し、検証範囲の制約の影響について限定付結論(範囲限定)を表明するか、又は結論を表明しないことになる。

検証範囲の制約により、その影響が経営者の記述書に対する結論を表明できないほどに重要でないと判断し限定付結論（範囲限定）を表明する場合、検証範囲の制約に係る除外事項として、次の事項を記載することになる。

- 実施できなかった検証手続
- 検証範囲の制約の事実が影響する事項

監査範囲の制約により、その影響が経営者の記述書に対する結論を表明できないほどに重要と判断した場合、結論を表明しない旨及びその理由を記載することになる。

２．情報セキュリティ検証報告書の文例

(1) 肯定的結論

独立した監査法人（注１）の情報セキュリティ検証報告書

平成×年×月×日

○○株式会社
代表取締役社長　○○○○殿

○○○○監査法人（注２）
代表社員　　公認会計士　○○○○　印
社　　員　　公認会計士　○○○○　印

当監査法人（注３）は、「ＩＴに係る保証業務等の実務指針（一般指針）」(平成21年９月１日　日本公認会計士協会ＩＴ委員会報告第５号)及び「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、○○株式会社が、△△体制*(情報セキュリティ検証の対象)*の情報セキュリティに関する管理状況について記載された経営者の記述書について検証を行った。この経営者の記述書の作成責任は○○株式会社の経営者にあり、当監査法人（注３）の責任は独立の立場から経営者の記述書に対する結論を報告することにある。

当監査法人（注３）は、「ＩＴに係る保証業務等の実務指針（一般指針）」(平成21年９月１日　日本公認会計士協会ＩＴ委員会報告第５号）及び「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に準拠して検証を行った。検証は、経営者の記述書に記載された○○株式会社の△△体制の情報セキュリティに関する管理状況について評価し、当監査法人（注３）が必要と認めたその他の手続を実施することを含んでいる。当監査法人（注３）は、検証の結果として結論を報告するための合理的な基礎を得たと判断している。

当監査法人（注３）は、経営者の記述書が、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、△△体制の情報セキュリティに関する管理状況についてすべての重要な点において適正に表示しているものと認める。

本報告書は、○○株式会社の△△体制の情報セキュリティの有効性について保証を与えるものではない。

内部統制の固有の限界のため、誤り又は不正が発生し、それらが発見されないことがある。さらに、システム又は内部統制に対する変更、処理要件の変更、時間の経過により要求された変更及びポリシー又は手続への準拠性の程度の低下のため、当監査法人の結論から将来を予想することにはリスクがある。

会社と当監査法人又は代表社員及び社員（注３）との間には、公認会計士法の規定に準じて記載すべき利害関係はない。

以　上

(2) 限定付結論(結論限定)

結論について結論限定がある場合は、以下のように記載する。

・・・・・・・・以前省略

当監査法人（注３）は、経営者の記述書が、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、△△体制の情報セキュリティに関する管理状況について、下記を除きすべての重要な点において適正に表示しているものと認める。

記

コントロール規準「9.1　情報セキュリティの事象及び弱点の報告」及び「9.2 情報セキュリティインシデントの管理及びその改善」

以後省略・・・・・・・・

(3) 限定付結論(範囲限定)

結論について範囲限定がある場合は、以下のように記載する。

・・・・・・・・以前省略

当監査法人（注３）は、経営者の記述書が、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、△△体制の情報セキュリティに関する管理状況について、下記を除きすべての重要な点において適正に表示しているものと認める。

記

○○○○システムについては、採用するサーバの運用を外部委託しているため、コントロール規準「7 アクセスコントロール」については、検証できなかった。

以後省略・・・・・・・・

(4) 否定的結論

結論について否定的結論を表明する場合は、以下のように記載する。

・・・・・・・・以前省略

当監査法人（注３）は、○○○○に与える影響の重要性に鑑み、経営者の記述書が、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、△△体制の情報セキュリティに関する管理状況について、適正に表示していないものと認める。

以後省略・・・・・・・・

(5) 結論不表明

結論を表明しない場合は、以下のように記載する。

・・・・・・・・以前省略

当監査法人（注３）は、「ＩＴに係る保証業務等の実務指針（一般指針）」(平成21年９月１日　日本公認会計士協会ＩＴ委員会報告第５号)及び「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、○○株式会社が、△△体制*(情報セキュリティ検証の対象)*の情報セキュリティに関する管理状況について記載された経営者の記述書について検証を行った。

当監査法人（注３）は、「ＩＴに係る保証業務等の実務指針（一般指針）」(平成21年９月１日　日本公認会計士協会ＩＴ委員会報告第５号）及び「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に準拠して検証を行った。検証は、経営者の記述書に記載された○○株式会社の△△体制の情報セキュリティに関する管理状況について評価し、当監査法人（注３）が必要と認めたその他の手続を実施することを含んでいる。

記

○○○○システムについては、採用するサーバの運用を外部委託しており、コ

ントロール規準「7 アクセスコントロール」、「9 情報セキュリティインシデントの管理」、「10 事業継続管理」については検証できなかったため、結論を報告するための合理的な基礎を得ることができなかった。

当監査法人（注３）は、経営者の記述書が、上記事項の△△体制に与える影響の重要性に鑑み、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に基づいて、平成×年×月×日から平成×年×月×日までの期間において、△△体制の情報セキュリティに関する管理状況についてすべての重要な点において適正に表示しているかどうかの結論を表明しない。

以後省略・・・・・・・・

（注１）　業務実施者が公認会計士の場合には、「独立した公認会計士」とする。

（注２）　業務実施者が公認会計士の場合には、以下とする。

○○○○　公認会計士事務所

公認会計士　○○○○　印

（注３）　業務実施者が公認会計士の場合には、「私」又は「私たち」とする。

３．経営者の記述書の文例

経営者の記述書

平成×年×月×日

○○○○監査法人（注１）
代表社員　　公認会計士　　○○○○　殿
社　　員　　公認会計士　　○○○○　殿

○○株式会社
代表取締役社長　　○○○○　印
情報システム担当取締役　　○○○○　印

私たちは、平成×年×月×日から平成×年×月×日までの期間における、○○株式会社の△△体制の情報セキュリティに関する管理状況について、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に従って評価し、作成した経営者の評価書の対象範囲及び経営者の評価書は以下のとおりです。

私たちは、○○株式会社の△△体制の情報セキュリティに関する管理及び管理状況並びにその評価について責任があります。

１．経営者の評価書の対象範囲

（１）　対象資産
△△に関わるすべての情報資産

（２）　対象者
△△に関わる業務に携わる者（委託先、派遣者を含む）

（３）　論理的対策領域
△△に関わる○○システム領域（○○株式会社の管理するシステムに限る）

（４）　物理的対象領域
○○株式会社の本社敷地内

２．経営者の評価書

< 管理規準 >(「経営者の評価」の数値は例示)

規準	項目番号	評価項目	経営者の評価
管理規準	**1**	**情報セキュリティマネジメントの確立**	
	1.1	適用範囲の定義	3
	1.2	ポリシーの策定	3
	1.3	リスクアセスメント	3
	1.4	コントロールの選択	3
	1.5	情報セキュリティマネジメントの承認	2
	2	**情報セキュリティマネジメントの導入と運用**	
	2.1	リスク対応計画	3
	2.2	コントロールの実施	2
	2.3	情報セキュリティマネジメントの運用管理	2
	2.4	教育、訓練、意識向上及び力量	2
	3	**情報セキュリティマネジメントの監視及びレビュー**	
	3.1	有効性の継続的改善	1
	3.2	監視及びレビューの準備	2
	3.3	コントロールの有効性評価	1
	3.4	情報セキュリティマネジメントの継続性評価	1
	4	**情報セキュリティマネジメントの維持及び改善**	
	4.1	改善策の導入	2
	4.2	是正処置	2
	4.3	予防処置	1
	5	**文書管理及び記録の管理**	
	5.1	文書化	2
	5.2	文書管理	2
	5.3	記録の管理	2

管理規準の評点水準

０：何もしていない。

１：何らかの実施はあるが、管理規準に準拠して文書化されていない。

２：管理規準に準拠して文書化されているが、運用が不十分である。

３：管理規準に準拠して文書化され、運用がなされている。

< コントロール規準 >(「経営者の評価」の数値は例示)

規準	項目番号	評価項目	経営者の評価
コントロール規準	**1**	**セキュリティ･ポリシー**	
	1.1	情報セキュリティ・ポリシー	3
	2	**情報セキュリティのための組織**	
	2.1	内部組織	3
	2.2	外部組織	2
	3	**資産の管理**	
	3.1	資産に対する責任	3
	3.2	情報の分類	3
	4	**人的資源のセキュリティ**	
	4.1	雇用前	3
	4.2	雇用期間中	3
	4.3	雇用の終了又は変更	2
	5	**物理的及び環境的セキュリティ**	
	5.1	セキュリティを保つべき領域	3
	5.2	装置のセキュリティ	4
	6	**通信及び運用管理**	
	6.1	運用の手続及び責任	3
	6.2	第三者が提供するサービスの管理	2
	6.3	システムの計画作成及び受入れ	3
	6.4	悪意あるコード及びモバイルコードからの保護	2
	6.5	バックアップ	3
	6.6	ネットワークセキュリティ管理	2
	6.7	媒体の取扱い	3
	6.8	情報の交換	3
	6.9	電子商取引サービス	3
	6.10	監視	2
	7	**アクセスコントロール**	
	7.1	アクセスコントロールに対する業務上の要件	4
	7.2	利用者アクセスの管理	4
	7.3	利用者の責任	4
	7.4	ネットワークのアクセスコントロール	3
	7.5	オペレーティングシステムのアクセスコントロール	2

	7.6	業務処理ソフトウェア及び情報のアクセスコントロール	3
	7.7	モバイルコンピューティング及びテレワーキング	3
	8	**情報システムの取得、開発及び保守**	
	8.1	情報システムのセキュリティ要件	3
	8.2	業務処理ソフトウェアでの情報セキュリティ上の正確な処理	3
	8.3	暗号によるコントロール	3
	8.4	システムファイルのセキュリティ	3
	8.5	開発及びサポートプロセスにおけるセキュリティ	3
	8.6	技術的ぜい弱性管理	2
	9	**情報セキュリティインシデントの管理**	
	9.1	情報セキュリティの事象及び弱点の報告	3
	9.2	情報セキュリティインシデントの管理及びその改善	3
	10	**事業継続管理**	
	10.1	事業継続管理における情報セキュリティの側面	3
	11	**コンプライアンス**	
	11.1	法的要件の遵守	3
	11.2	セキュリティ・ポリシー及びスタンダードの遵守並びに技術的要件の遵守	4
	11.3	情報システムの監査に対する考慮事項	4

コントロール規準の評点水準

0 (未実施レベル)　　：何もしていない。
1 (非正式実施レベル)：コントロールの正式な文書化が不十分である。
2 (正式導入レベル)　：コントロールは正式に文書化を伴って運用されているが、組織全体として策定されていない。
3 (組織的整備レベル)：コントロールは組織全体として正式に文書化され運用されている。
4 (目標管理レベル)　：３に加え、モニタリングされている。
5 (有機的改善レベル)：４に加え、常にコントロールの改善体制が有機的に運営されている。

(注１)　業務実施者が公認会計士の場合には、以下とする。

○○○○　公認会計士事務所
公認会計士　○○○○　殿

４．経営者確認書の文例

経営者確認書

平成×年×月×日

○○○○監査法人（注１）
代表社員　　公認会計士　　○○○○　殿
社　　員　　公認会計士　　○○○○　殿

○○株式会社
代表取締役社長　　○○○○　印
情報システム担当取締役　　○○○○　印

平成×年×月×日から平成×年×月×日までの期間において、○○株式会社の△△体制の情報セキュリティの管理状況について記述した経営者の記述書の検証に関連して、私たちの知り得る限りにおいて、以下のとおりであることを確認いたします。

(1) △△体制の情報セキュリティの管理状況の維持及び経営者の記述書の作成については、○○株式会社の経営者に責任があることを承知しております。
(2) 経営者の記述書に記載した○○株式会社の△△体制の情報セキュリティの管理状況は、「情報セキュリティ検証業務」(平成22年５月18日　日本公認会計士協会ＩＴ委員会研究報告第39号)に従って正しく表示しております。
(3) 貴監査法人（注２）から要請のあった経営者の記述書又は△△体制の情報セキュリティの管理状況について認識している事項は、すべて貴監査法人に提供いたしました。
(4) 貴監査法人（注２）から要請のあった経営者の記述書又は△△体制*(情報セキュリティ検証の対象)*の情報セキュリティの管理状況に関する記録並びに検証業務に必要な資料は、すべて貴監査法人に提供いたしました。
(5) 平成×年×月×日（対象期間最終日の翌日）から平成×年×月×日（検証報告書日付）までの期間において、○○株式会社の△△体制の情報セキュリティの管理状況に重要な影響を及ぼす事象は発生していません。

以　上

(注１)　業務実施者が公認会計士の場合には、以下とする。
○○○○　公認会計士事務所
公認会計士　○○○○　殿

(注２)　業務実施者が公認会計士の場合には、「貴殿」とする。

以　上