The Japanese Institute of
Certified Public Accountants

情報セキュリティ検証業務

IT委員会研究報告第39号「情報セキュリティ検証業務」の説明資料

ITアシュアランス専門委員会

注意：この資料は、日本公認会計士協会において、IT委員会研究報告第39号「情報セキュリティ検証業務」の説明（理解促進）のために作成したものです。

アウトライン

- 情報セキュリティ検証業務の考え方
  - ✓ 情報セキュリティ検証業務とは
  - ✓ 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の効果
- 情報セキュリティ検証業務と他制度との比較
  - ✓ IT研39号検証業務と類似制度
  - ✓ 類似制度の比較
  - ✓ IT研39号検証業務の特色
  - ✓ IT研39号検証業務の位置づけ
  - ✓ 想定される利用ケース
    - ケース1
    - ケース2
    - ケース3
    - ケース4
    - ケース5
- 評価規準の解説
  - ✓ 評価の枠組み
  - ✓ 情報セキュリティ評価規準
  - ✓ 管理規準の評価水準
  - ✓ コントロール規準の評価水準
  - ✓ 評価における留意事項等
  - ✓ 「経営者の記述書」の解説
- 検証報告書の開示の方法

情報セキュリティ検証業務の考え方

- 情報セキュリティ検証業務とは
- 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の効果

情報セキュリティ検証業務とは

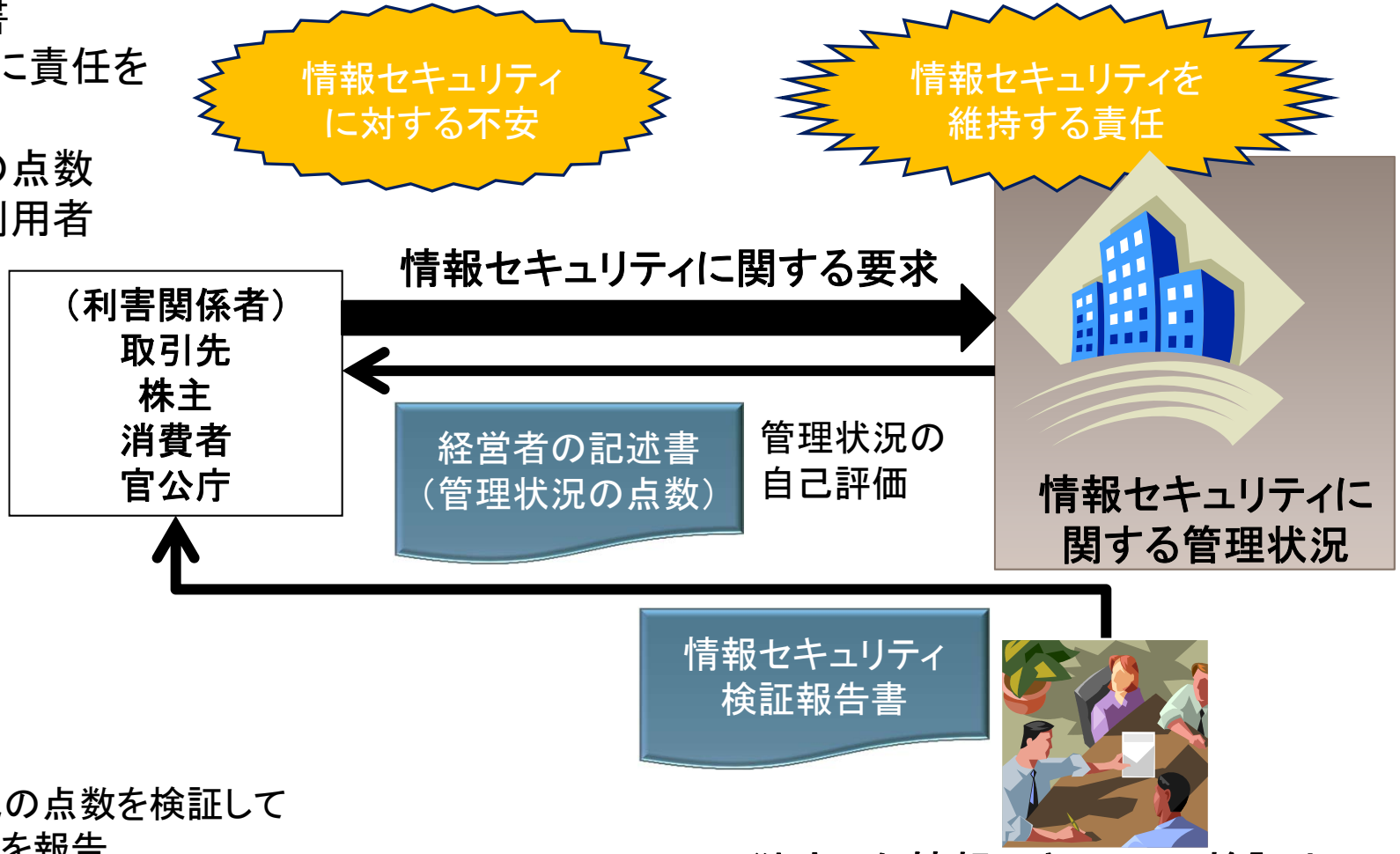
情報セキュリティ検証業務については、IT委員会研究報告第39号「情報セキュリティ検証業務」（以下「IT研39号」という。）において次のように定義されている。

- 経営者が、情報セキュリティの評価規準に基づいて行った評価結果を掲載した記述書について
- 公認会計士が当該記述書を検証基準に基づいて検証し、検証報告書を作成し、
- この検証報告書を当該情報セキュリティの利害関係者が利用する制度

※一般に公正妥当な規準、例えば、「情報セキュリティ評価規準」に基づいて行った評価結果は、比較可能性が高く、情報セキュリティのモニタリングの向上を可能にする。

情報セキュリティ検証業務の概要

【検証業務の概要】
■検証業務実施者
■検証報告書
■会社（主題に責任を負う者）
■管理状況の点数
■報告書の利用者

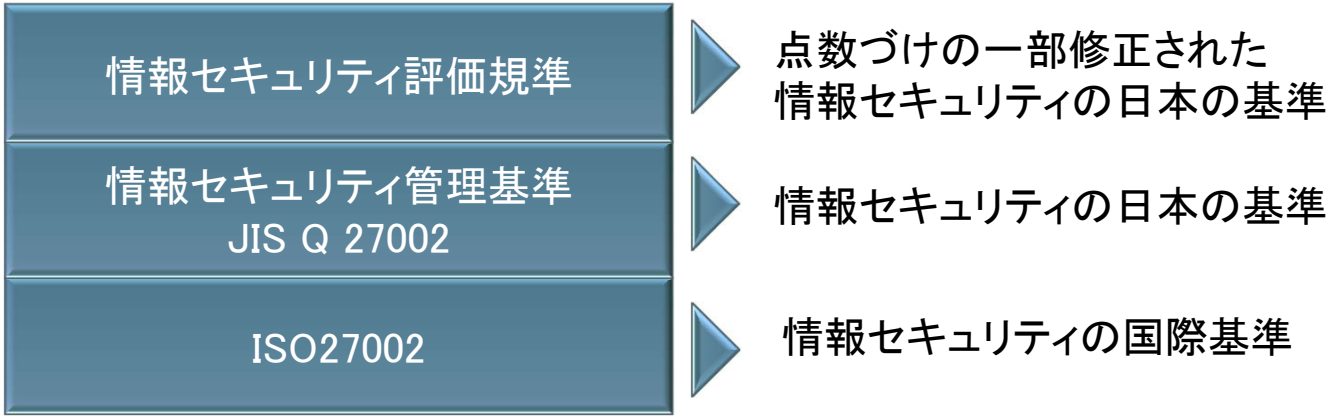


情報セキュリティ検証業務の効果

- 自社に情報セキュリティを要求する企業等への説明
- 自社の点数の内部監査への活用
- 公認会計士の検証による信頼性の付与
- 時系列比較
- 他社比較 （ただし、点数情報のデータベースが前提）

自社に情報セキュリティを要求する企業等への説明

- 経営者の記述書は、検証対象の情報セキュリティの管理状況について利害関係者に説明する機会となる
  - ✓ 経営者の記述書は、情報セキュリティ評価規準に基づいて、検証対象の情報セキュリティの管理状況を点検評価し、その結果を点数として記載したものである。自己評価ではあるが、公正な規準により評価した結果であり、利害関係者に対して情報セキュリティの管理状況を説明する良い資料となる。
  - ✓ 情報セキュリティ評価規準は、一般に公表されている評価規準であるため、利害関係者においても経営者の記述書がどのような規準により点数化されているか理解することが容易である。
- 情報セキュリティ評価規準は、「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、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
- 情報セキュリティ評価規準に基づき点数をつけるという方法

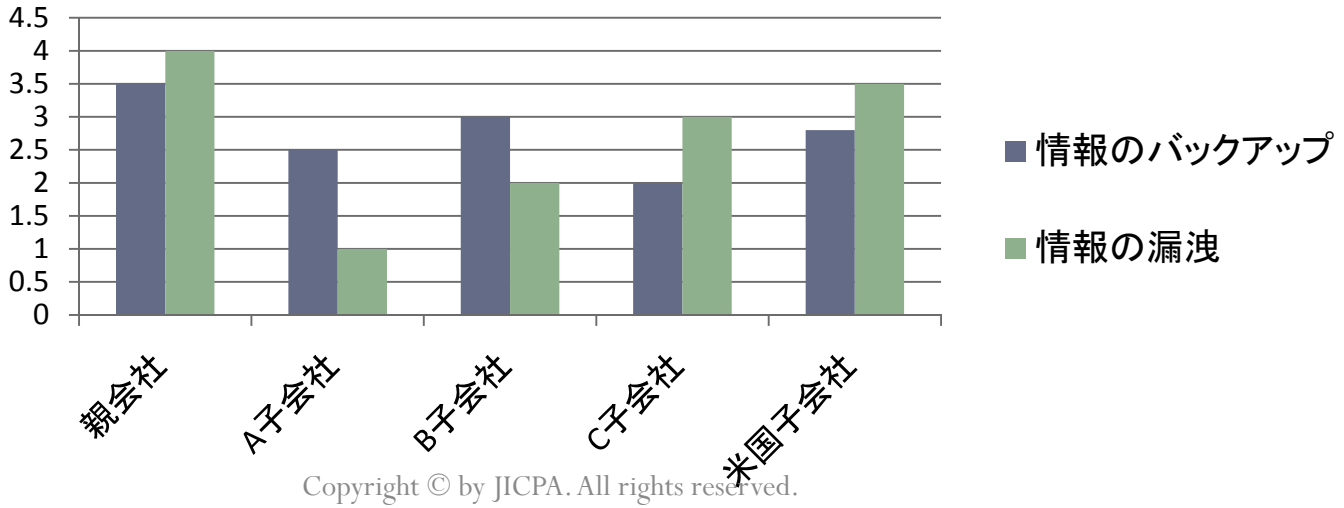


自社の点数の内部監査への活用

- 内部監査
  - ✓ 内部監査のために、企業グループの情報セキュリティの管理状況を点検評価することがある。企業グループの統一の規準として情報セキュリティ評価規準を採用した場合には、グループ企業が実施した点数を集計することにより、子会社の管理状況を把握することができる。
  - ✓ 表にしてまとめることにより、グループ企業の情報セキュリティの弱点を明瞭に把握することができる。

	親会社	A子会社	B子会社	C子会社	米国子会社
情報のバックアップ	3．5	2．5	3	2	2．8
情報の漏洩	4	1	2	3	3．5

点数を平均点にした場合



公認会計士の検証による信頼性の付与

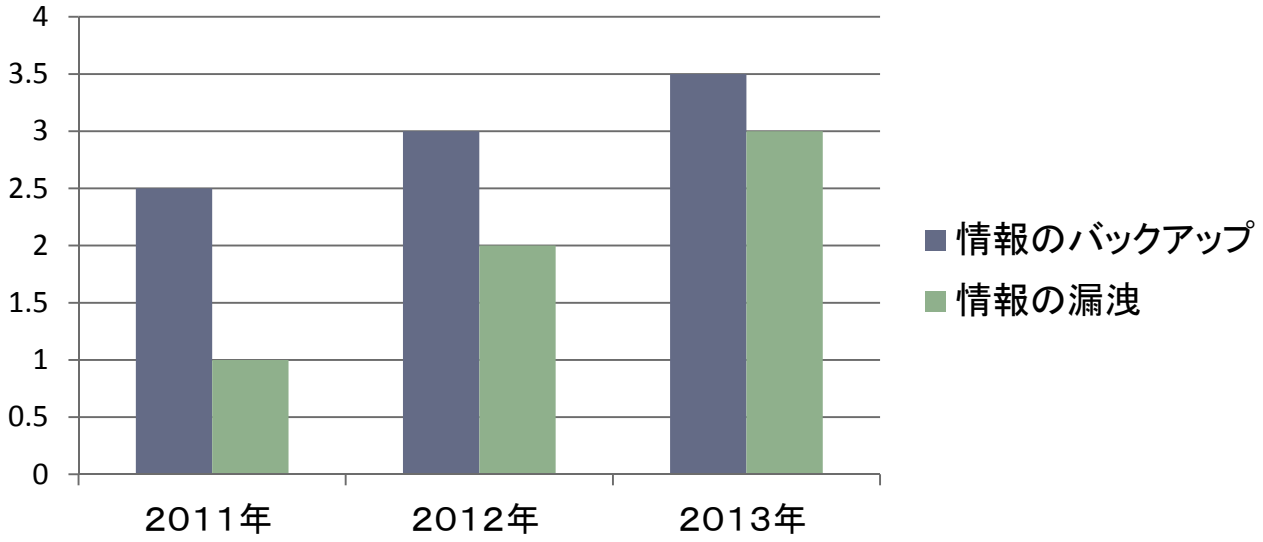
- 経営者の記述書は、自己評価の結果として利用することも可能であるが、利害関係がある場合には、自己評価の結果を信頼してもらうことが難しい。そのような場合には、公認会計士による検証を受けることにより、経営者の記述書が正しいことを証明できる。

時系列比較

- 情報セキュリティの管理状況における点数を時系列的に並べることにより、管理状況の改善の程度を確認することができる。

親会社	2011年	2012年	2013年
情報のバックアップ	2．5	3	3．5
情報の漏洩	1	2	3

内部監査のデータを活用したほうがわかりやすい



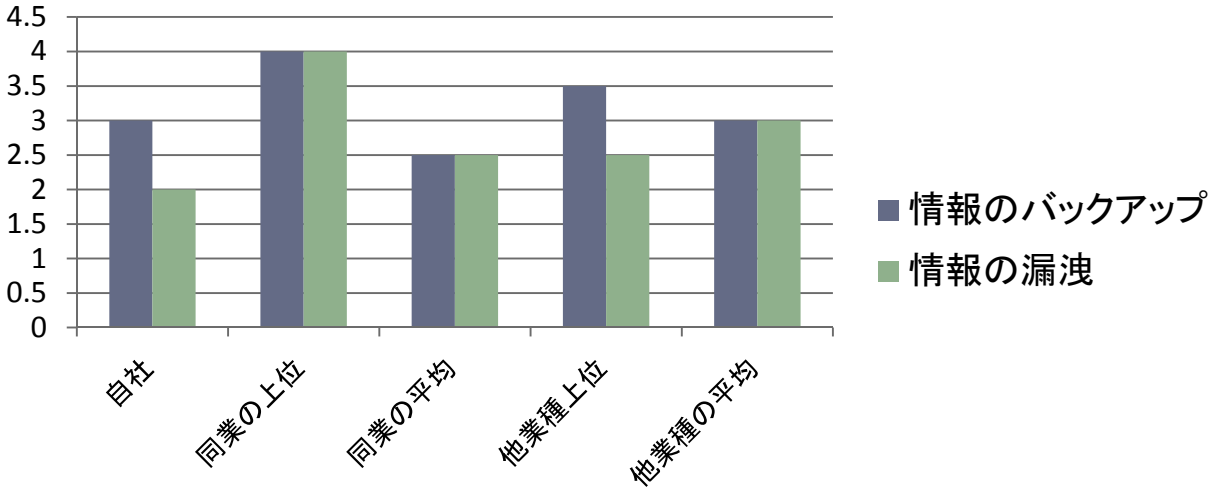
他社比較

- 通常、個々の企業の点数を入手することは難しいが、一般企業から独立した組織が、公的な立場から多数の企業の点数を集めその情報を公表することにより、自社の管理状況について他社比較することが可能となる。
- 例えば、集められたデータを業種ごとに、上位ランク、平均、下位ランクの情報を作成するとする。この場合に、自社の点数と同業種の点数を比較することにより、自社の管理状況を業界という視点から把握することが可能となる。
- 製造のサプライチェーンによっては、取引先が同業種とは限らない。このような場合であっても、自社と他業種の点を比較することが可能である。

	自社	同業の上位	同業の平均	他業種上位	他業種の平均
情報のバックアップ	3	4	2．5	3．5	3
情報の漏洩	2	4	2．5	2．5	3

データが前提

下請会社からデータを入手して作成することも可能



情報セキュリティ検証業務と他制度との比較

- IT研39号検証業務と類似制度
- 類似制度の比較
- IT研39号検証業務の特色
- IT研39号検証業務の位置付け
- 想定される利用ケース

IT研39号検証業務と類似制度

- 組織の情報セキュリティの管理実施状況を評価・検証する仕組みが複数あり、IT研39号検証業務に類似するものとしては、以下があげられる。

  - ✓ **ISMS適合性評価制度**

    組織や特定業務における情報セキュリティマネジメントシステム(ISMS)について、第三者の認証機関がISMS 認証基準(JIS Q 27001:2006)への適合性評価を行う制度である。有効期限は3年であり、3年後に再認証審査が行われる。

  - ✓ **情報セキュリティ格付**

    企業の情報セキュリティに対する取り組みを、情報セキュリティ格付機関が独自の基準で評価し、比較可能な形式(格付)を公表する制度である。国内・海外あわせて数社が格付けサービスを提供している。

  - ✓ **JASA(日本セキュリティ監査協会)の「保証型情報セキュリティ監査」**

    組織や特定業務における情報セキュリティマネジメントシステムが、監査結果を利用する者(委託者など)の期待する水準にあるかについて、独立かつ専門的な立場の監査人が保証意見を表明する制度である。

  - ✓ **IPA(情報処理推進機構)の「情報セキュリティ対策ベンチマーク」**

    組織のセキュリティ対策状況を開示や保証するものではないが、組織のセキュリティ対策状況の自己評価を助けるツールである。

  - ✓ **JICPA(日本公認会計士協会) Trustサービス**

    日本公認会計士協会からライセンスを受けた公認会計士等が「Trustサービスに係る実務指針」にしたがって実施する。独立かつ専門的な立場の監査人が保証結論を表明する制度である。

類似制度の比較

- 類似制度について制度面での比較

制度名	規準	評価者 （業務実施者）	評価結果
ISMS適合性評価制度	JIS Q 27001	ISMS審査員	ISMS認証（登録証）、審査報告書
情報セキュリティ格付	格付け企業が定めた独自の基準	情報セキュリティ格付機関	数段階～十数段階の評点（格付）
保証型情報セキュリティ監査	情報セキュリティ管理基準や業界での標準等を基にした個別の基準	情報セキュリティ監査人	監査報告書（保証意見）
情報セキュリティ対策ベンチマーク	JIS Q 27001を基にした、簡易的な基準	自己診断	トータルスコアやスコアの散布図、評価項目毎のレーダーチャート
Trustサービス	Trustサービスの原則と規準	公認会計士	検証報告書（保証結論）
IT研39号検証業務	情報セキュリティ評価規準	公認会計士	検証報告書（保証結論）

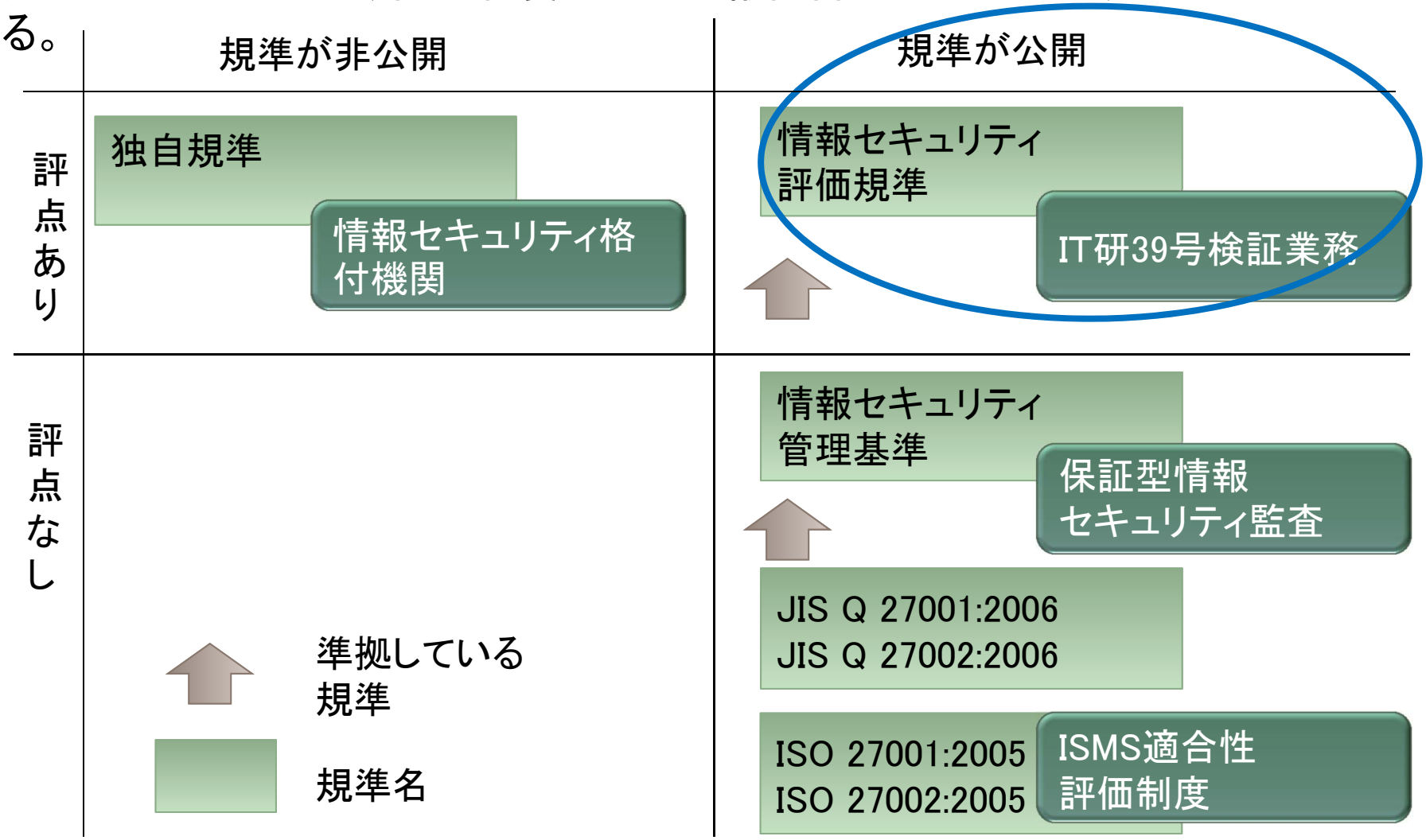
IT研39号検証業務の特色

● IT研39号検証業務の特色

IT研39号検証業務の特色	検証報告書利用者の立場からみて	経営者（組織）の立場からみて
比較可能性	経営者の評価結果が数値化されており、時系列での比較や業界・異業種間での比較が可能である。 また、一定の水準を満たしているか否かだけではなく、水準以上の企業についても、経営者の評価内容の把握やその比較が可能となる。	経営者の評価結果が数値化されており、検証結果や優位性などを外部にアピールしやすい。 点数化されているため、内部監査や組織状況の把握に利用しやすい。
公開規準	規準が「情報セキュリティ評価規準」として詳細が公開されていることで、評価基準、評価内容が明確になる。	規準が公表されているため、内部監査や組織内の自主的な取り組みへ活用しやすい。 また、規準が情報セキュリティ管理基準に基づき作られたものなので、既にある情報セキュリティの取り組みとの親和性が高い。
保証の厳密性	合理的結論に至るまでの十分かつ適切な証拠、その検証手続が定められている。	検証を受けることで、検証での証拠や検証手続を組織の内部監査やセキュリティ対応に生かすことができる。
保証期間	期間保証であるため、一定期間（1年）を通じた保証が得られる。	一定期間（1年）を対象期間としており、組織内の定期的なセキュリティ管理業務と対応させやすい。

IT研39号検証業務の位置づけ

IT研39号は「情報セキュリティ評価規準」が公開され、それぞれの項目に評点がつけられるため、他の制度に比べて報告書の利用がしやすくなっている。



想定される利用ケース

1. 管理体制の遅れている会社・組織

- 顧客・監督当局をはじめとする利害関係者の要求に基づき管理態勢レベルを評価する。
- 地域・業務領域・顧客層の異なる複数大規模組織のセキュリティ水準のばらつき度合に際して、同じ基準による数値で見える化が図れる。

2. 事故を起こした企業に対する指導

- セキュリティ事故を起こした会社に対して再発防止策適用後に管理態勢のレベルを評価し、改善状況の向上に寄与する。

想定される利用ケース

3. 親会社から複数の子会社を評価

- 内部監査等で実施しているが、「情報セキュリティ評価規準」により実施することで、数値化・比較化が容易になるとともに、リスクの高い会社に重点的な施策を打ちやすくなる。

4. 企業から取引先を評価

- 現行はISMSを要求することが多いが、個別の項目ごとに評価を実施することで、評価したい領域・項目に焦点を当てた形での評価を行いやすくなる。
- 調達・提案依頼の一つの条件として、最低限クリアすべき領域・水準を明示化することが可能となる。

想定される利用ケース

5. 官公庁・地方自治体・各種団体が傘下・下部組織を評価・指導

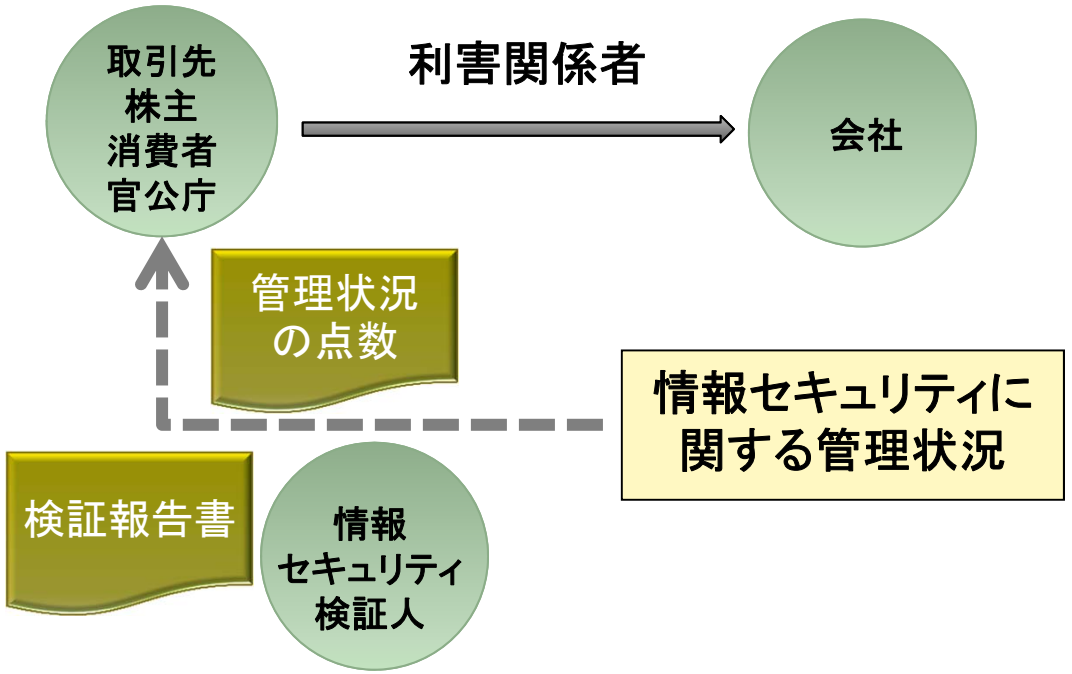
- ISMSの取得を要求するまでは各種制約上難しくとも、「情報セキュリティ評価規準」により評価若しくは指導を実施することで、見える化が図られると共に、継続的な改善活動につなげる事が出来る。

情報セキュリティ検証業務の概要

ケース1–管理体制の遅れている会社・組織

【概要】

✓顧客・監督当局をはじめとする利害関係者の要求に基づき管理態勢レベルを評価する。



【検証業務の必要性】

■報告書の利用者は、管理状況の点数により管理状況を把握できる。

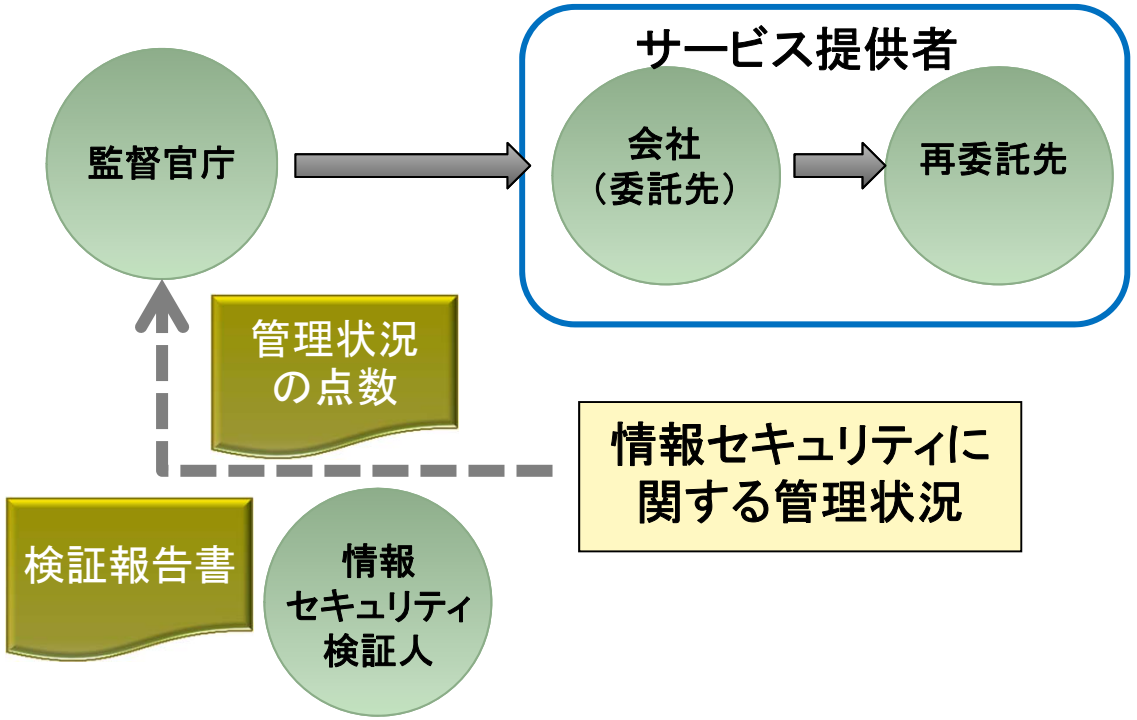
■報告書の利用者は、検証報告書により点数を信頼できる。

情報セキュリティ検証業務の概要

ケース2-事故を起こした企業に対する指導

【概要】

- ✓ セキュリティ事故を起こした会社に対して再発防止策適用後に改善状況を評価する。
- ✓ 再委託先を含むサービス提供者全般に対する管理態勢のレベルを評価する。



【検証業務の必要性】

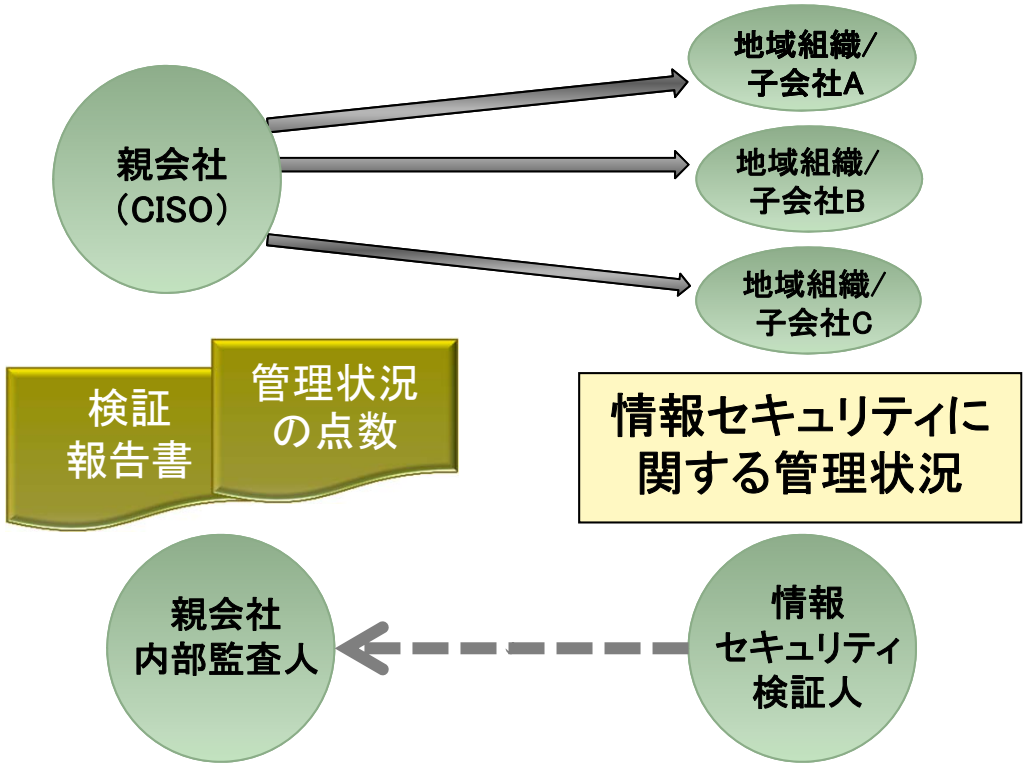
■報告書の利用者は、管理状況の点数により管理状況を把握できる。
■報告書の利用者は、検証報告書により点数を信頼できる。
■報告書の利用者は、複数時点間の点数を比較することにより改善状況を把握できる。

情報セキュリティ検証業務の概要

ケース3–親会社から複数の子会社を評価

【概要】

✓ 地域・業務領域・顧客層の異なる複数大規模組織のセキュリティ水準のばらつき度合に際して、同じ基準による数値で見える化が図れる。



※　CISO:情報セキュリティ責任者

【検証業務の必要性】

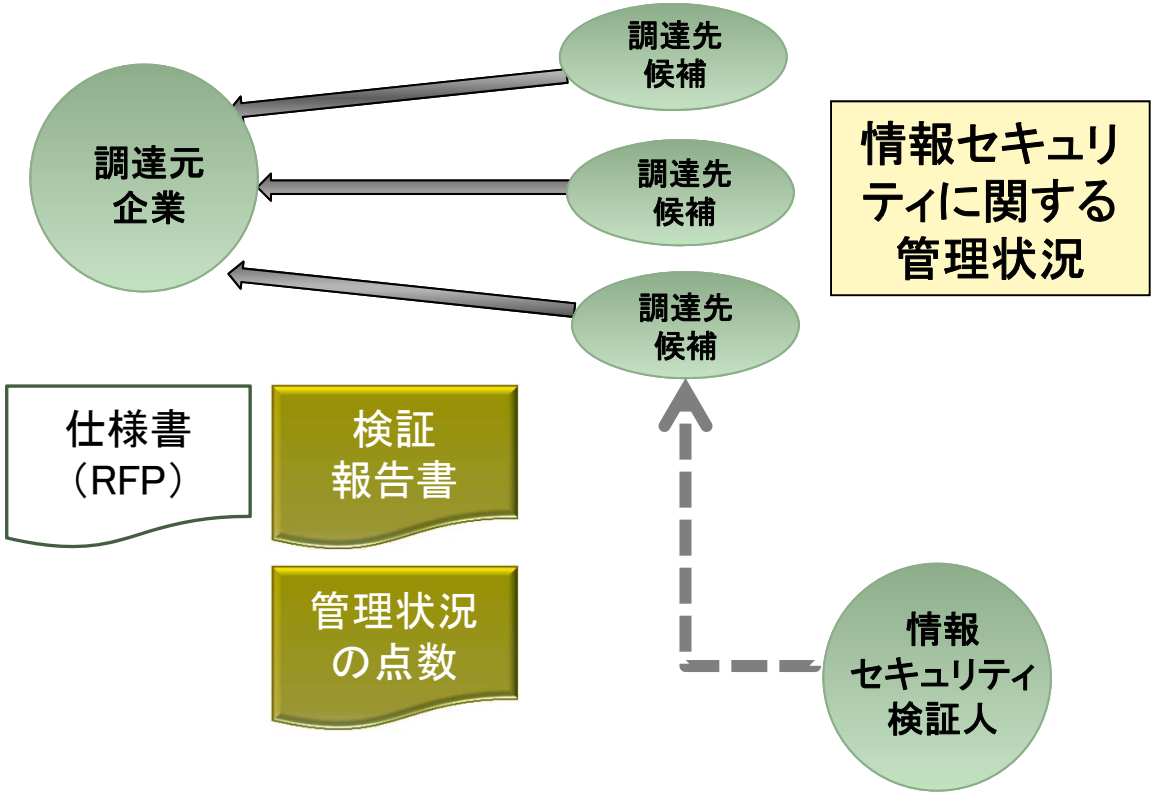
■報告書の利用者は、管理状況の点数により管理状況を把握できる。
■報告書の利用者は、複数拠点間の点数を比較することによりばらつきを把握できる。
■報告書の利用者は、複数拠点間の点数を比較することにより目指す水準を把握できる。

情報セキュリティ検証業務の概要

ケース4–企業から取引先を評価

【概要】

- ✓調達元は、仕様書に評価したい領域・項目を明示する。
- ✓調達先候補は、検証済みの管理状況の点数を調達元に提出する。
- ✓現行はISMSを要求することが多いが、個別の項目ごとに評価を実施することで、評価したい領域・項目に焦点を当てた形での評価を行いやすくなる。



※　CISO:情報セキュリティ責任者

【検証業務の必要性】

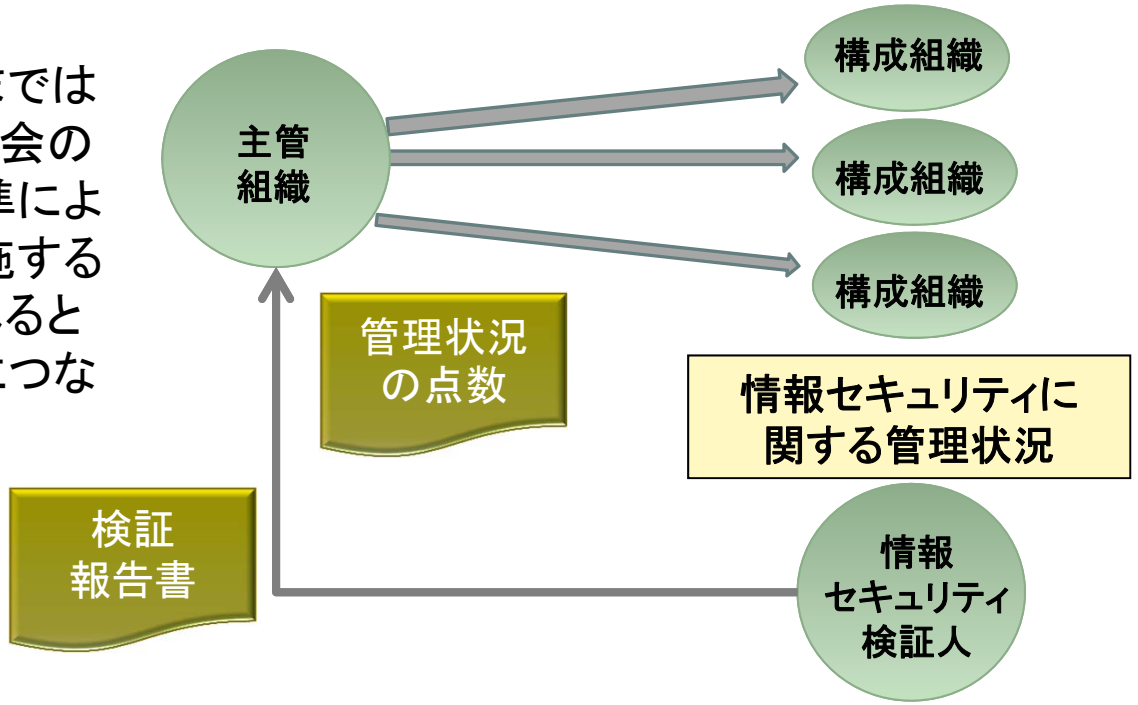
■報告書の利用者は、管理状況の点数により管理状況を把握できる。
■報告書の利用者は、検証報告書により点数を信頼できる。
■報告書の利用者は、複数企業間の点数を比較することにより適切な選定を実施できる。

情報セキュリティ検証業務の概要

ケース5–官公庁・地方自治体・各種団体が傘下・下部組織を評価・指導

【概要】

✓ISMSの取得を要求するまでは各種制約上難しくとも、協会の情報セキュリティ評価規準により評価若しくは指導を実施することで、見える化が図られると共に継続的な改善活動につなげる事が出来る。



【検証業務の必要性】

■報告書の利用者は、管理状況の点数により管理状況を把握できる。
■報告書の利用者は、複数拠点間の点数を比較することによりばらつきを把握できる。
■報告書の利用者は、領域ごとの強弱を把握することにより具体的な指導を指導することができる。

評価規準の解説（評価規準の説明のみ）

- 評価の枠組み
- 情報セキュリティ評価規準
- 管理規準の評点水準
- コントロール規準の評点水準
- 評価における留意事項等
- 「経営者の記述書」の解説

評価の枠組み

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

情報セキュリティ評価規準

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。

経営者の記述書

管理規準

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.	2
	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しているか	2
	1.2	ポリシーの策定	2
	1.2.1	情報セキュリティポリシーを策定しているか	2

コントロール規準

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	2
	1.1.1	情報セキュリティポリシー文書は、全従業員に通知され、関連する外部関係者に公表されるよう規定し，運用しているか	3
	1.1.2	情報セキュリティポリシーは、あらかじめ定められた間隔で、又は重大な変化が発生した場合に，それが引き続き適切、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

評点水準

管理規準 0～3

コントロール規準 0～5

経営者の評点

業務実施者の検証に当たり適用される評点

情報セキュリティ評価規準に対する準拠状況の評点は、管理規準、コントロール規準それぞれの評価水準により決められる。

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
2 情報セキュリティマネジメントの導入と運用
3 情報セキュリティマネジメントの監視及びレビュー
4 情報セキュリティマネジメントの維持及び改善
5 文書管理及び記録の管理

コントロール規準

1 セキュリティ・ポリシー
2 情報セキュリティのための組織
3 資産の管理
4 人的資源のセキュリティ
5 物理的及び環境的セキュリティ
6 通信及び運用管理
7 アクセスコントロール
8 情報システムの取得、開発及び保守
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
11 コンプライアンス

評価項目の項目数

	第1階層	第2階層	第3階層
管理規準	5	19	34
コントロール規準	11	39	67

※ 情報セキュリティ評価規準は、「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、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。

管理規準の評点水準

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

- 「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。

- 「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。

コントロール規準の評点水準

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

- 「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。
- 「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。

評価における留意事項等

- 評価に当たり評点は、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。
- 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。

「経営者の記述書」の解説－管理規準

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

- 管理規準の第1階層の5項目それぞれの評点を見ると、次のような状況にあることが分かる。
  1. 情報セキュリティマネジメントの確立では、マネジメントの承認という点で不十分な点があるが、それ以外の項目は文書化され運用されている。
  2. 情報セキュリティマネジメントの導入と運用では、リスク対応計画は文書化され運用されているが、それ以外の項目は、まだ不十分な点がある。
  3. 情報セキュリティマネジメントの監視及びレビューでは、監視及びレビューの準備について、文書化されているが不十分な点がある、それ以外の項目については文書化ができていない。
  4. 情報セキュリティマネジメントの維持及び改善では、改善策の導入、是正処置については不十分な点はあるものの文書化されており、予防処置について文書化ができていない。
  5. 文書管理及び記録の管理では、すべての項目で文書化されているが不十分な点がある。
- 上記の状況から第1階層の5項目で全体を大きくみると、範囲の特定、リスクアセスメント、方針の策定といったマネジメントサイクルの計画部分については概ねできているが、導入以降について不十分な点がある。特に監視及びレビューが弱いということがわかる。また、マネジメントの承認が不十分という点は、管理体制という面では基本的な枠組みについても確立しているとはいえない状況と考えられる。
- 以上のことから、まずはマネジメントの承認からはじめ、情報セキュリティマネジメント導入運用を改善し、監視及びレビューの体制を整備していくことが必要ではないかということが考えられる。

「経営者の記述書」の解説ーコントロール規準1/2

- コントロール規準の第1階層の11項目の評点を見ると次のような状況が分かる。
  1 セキュリティポリシーについては、組織全体としての文書化が行われ運用されているが、モニタリングまではできていない。
  2 情報セキュリティのための組織では、内部組織については文書化が行われ運用されているが、モニタリングまではできておらず、外部組織については文書かも不十分な点がある。
  3 資産の管理については、組織全体としての文書化が行われ運用されているが、モニタリングまではできていない。
  4 人的資源のセキュリティでは、雇用前、雇用中については文書化が行われ運用されているが、モニタリングまではできておらず、雇用の就業変更については文書化も不十分な点がある。
  5 物理的及び環境的セキュリティでは、組織全体としての文書化が行われ運用されており、装置のセキュリティについてはさらにモニタリングまでできている。
  6 通信及び運用管理では、第三者のサービス、悪意のあるコード等からの保護、ネットワークセキュリティ管理、監視という点で文書において不十分な点がある。その他の項目については文書化され運用されているが、モニタリングまではできていない。
  7 アクセスコントロールでは、OSのアクセスコントロールは、文書化で不十分な点はあるものの、それ以外の項目では文書化され運用されている。さらにアクセスコントロールに対する業務上の要件、利用者アクセス管理、利用者の責任についてはモニタリングまでできている。
  8 情報システムの取得、開発及び保守では、脆弱性管理は文書において不十分な点がある。その他の項目については文書化され運用されているがモニタリングまではできていない。
  9 情報セキュリティインシデントの管理及び10 事業継続管理では、 組織全体としての文書化が行われ運用されているが、モニタリングまではできていない。
  10 コンプライアンスでは、法令順守については文書化が行われ運用されており、さらにセキュリティ・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と情報システムの監査に対する考慮事項ではモニタリングまでできている。

- 上記の状況から第1階層の5項目で全体を大きくみると、次のようなことが考えられる。
  - ✓ 全体的に文書化され運用が行われている段階の項目が多いが、一部は文書化が不十分な項目があり、また、一部ではモニタリングまでできているものもある。項目としてまったく対応していないものはない。
  - ✓ 通信及び運用管理の項目では、他の項目に比べ不十分な項目が多く見られる。
  - ✓ 外部組織や第三者のサービス等で不十分な点があることから、外部の組織との関係が弱いと思われる。
  - ✓ 悪意のあるコード等からの保護、ネットワークセキュリティ管理、監視、脆弱性管理という項目で不十分な点が見られることから技術的なセキュリティ面が弱いように思われる。
  - ✓ 物理的及び環境的セキュリティ、アクセスコントロール、コンプライアンスについては、モニタリングまでできていることから、これらに対策に重点がおかれていると思われる。

「経営者の記述書」の解説－コントロール規準2/2

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

項目番号	評価項目	経営者の評価
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

検証報告書の開示の方法

- 特定の利害関係者
  - ✓印刷物
- 一般向け（会社が公表したい場合には、一般向けに開示可能）
  - ✓Webサイトから
  - ✓印刷物
  - ✓情報セキュリティ報告書の添付資料
- 将来は他社比較
  - ✓アンケートによる自己申告
  - ✓会社による提供