サイバーセキュリティ経営実践のための支援策
ーサイバーセキュリティ経営ガイドラインー

経済産業省 商務情報政策局 サイバーセキュリティ課
池田　佳高

▌要　約▐

1. サイバーセキュリティ経営の定着を目指すため、①サイバーセキュリティ経営の具体化、②サイバーセキュリティ経営の実践、③サイバーセキュリティ経営の可視化の 3 つのステップにより、必要な対策を実施していくことが必要である。
2. 企業は、ファーストステップであるサイバーセキュリティ経営の具体化のために「サイバーセキュリティ経営ガイドライン Ver3.0」を、セカンドステップであるサイバーセキュリティ経営の実践のために「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集」を、サードステップであるサイバーセキュリティ経営の可視化のために「サイバーセキュリティ経営可視化ツール」を活用していくことが求められる。
3. 経営者及び最高情報セキュリティ責任者（CISO）等は、これらのガイドライン等を活用しながら、必要なサイバーセキュリティ対策を実施するとともに、実施した対策についてはステークホルダー等の関係者に積極的な情報開示を行ってほしい。

Ⅰ　サイバーセキュリティ経営ガイドラインについて

企業におけるデジタル環境の利用により企業間・産業間のネットワーク化が進展し、サプライチェーンは、部品製造を担う企業とそれらの部品を用いて組み立てを行う企業との受発注等の契約を介した関係にとどまらない。加えて、クラウドサービスなど外部のデジタルサービスの利用や、API（アプリケーション・プログラミング・インターフェース）を介したシステム同士の連携など、企業規模にかかわらず、デジタル環境を通じた多様かつ非定型の企業間のつながりによって付加価値が生み出されている。

一方、サイバー空間を取り巻く社会的情勢は変化しており、特にサプライチェーンを狙った攻撃は高度化・巧妙化している。例えば、企業等の情報を暗号化して金銭をゆすり取るランサム攻撃や国家支援型の攻撃集団等が特定の企業を執拗に狙う標的型攻撃などのサイバー攻撃が多く確認されており、特にサプライチェーンを狙った攻撃においては、セキュリティ対策に弱点のある取引先等が攻撃経路として狙われている（図表1）。サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃を防げず、発生した場合の事業継続に影響する可能性があるのみならず、個人情報の漏えいや他社に対するサイバー攻撃への発展など社会全体に影響を与え、被害が拡大するおそれがある。

経営者は、組織の意思決定機関が決定したサイバーセキュリティ体制が組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報の漏えいなどにより、会社や第三者に損害が生じた場合、善管注意義務や任務懈怠に基づく損害賠償責任を問われ得るなど、会社法や民法等に基づく法的責任やステークホルダーへの説明責任を負うこととなる。そのため、サイバーセキュリティリスクを経営リスクとして認識し、経営者のリーダーシップのもとでサイバーセキュリティ対策を進めていくことがより一層求められている。

また、経営者は、サイバーセキュリティ対策を、単なるリスク回避のための手段ではなく、企業価値を高めるための「投資」（将来の事業活動・成長に必須の費用）と位置付け

図表 1　サイバー攻撃の現状

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

（出所）独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2024」

ることが重要である。ここで言う投資とは、直接的な収益を算出するものではないが、企業の価値を維持・増大していく上で、企業活動におけるコストや損失を減らすために必要不可欠なものである。このような観点からも、積極的に推進していく必要がある。

経済産業省及び独立行政法人情報処理推進機構（IPA）は、これらの観点から、経営者がリーダーシップを発揮して具体的なサイバーセキュリティ対策を実践することを支援するため、2023 年 3 月 24 日付けでサイバーセキュリティ経営ガイドラインの改訂を行っている。

本稿では、サイバーセキュリティ経営ガイドラインを中心に、サイバーセキュリティ経営を実践するための支援策について紹介する。

Ⅱ サイバーセキュリティ経営ガイドライン Ver3.0 の概要

サイバーセキュリティ経営ガイドライン Ver3.0（以下、本ガイドライン）は、大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3 原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（最高情報セキュリティ責任者〔CISO〕等）に指示すべき「重要 10 項目」をまとめる形で構成されている（図表 2）。経営者及び CISO 等は、本ガイドラインにより、サイバーセキュリティ対策を推進していくに当たり、どのような認識を持ち、またどのような対策を行っていくべきかについて、理解を深めることが期待される。

図表 2　経営者が認識すべき 3 原則とサイバーセキュリティ経営の重要 10 項目

経営者が認識すべき 3 原則

	内容
1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
3	平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営の重要 10 項目

	内容
指示 1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示 2	サイバーセキュリティリスク管理体制の構築
指示 3	サイバーセキュリティ対策のための資源（予算、人材等）確保
指示 4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5	サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示 6	PDCA サイクルによるサイバーセキュリティ対策の継続的改善
指示 7	インシデント発生時の緊急対応体制の整備
指示 8	インシデントによる被害に備えた事業継続・復旧体制の整備
指示 9	ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握及び対策
指示 10	サイバーセキュリティに関する情報の収集、共有及び開示の促進

（注）　PDCA は「Plan〔計画〕、Do〔実行〕、Check〔実施状況の確認・評価〕、Act〔改善〕」の略。
（出所）経済産業省・独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0」2023 年 3 月 24 日

１．経営者が認識すべき 3 原則

１）経営者のリーダーシップのもとでの対策の推進

原則 1 では、経営者がサイバーセキュリティリスクを自社のリスクマネジメントにおける重要課題として認識し、自らのリーダーシップのもとで対策を進めることが必要であるとしている。

ビジネス展開や企業内の生産性向上のためのデジタル技術の活用を始め、IoT（Internet of Things）デバイスの活用やオンラインでのコミュニケーションなど、企業のデジタル環境への依存度の増大に伴い、サイバー攻撃による事業活動への影響の可能性も増大しており、企業活動におけるコストや損失を減らすためにもサイバーセキュリティ対策を実施していくことが重要である。そのため、本項目では、サイバーセキュリティリスクを多様な経営リスクの一つとして捉え、リスク低減は経営者の責務であるとし、そのために、経営者がリスクマネジメントにおける重要課題であることを認識して、自らリーダーシップを発揮して対策の推進を主導することが必要であるとしている。

２）サプライチェーン全体にわたる対策への目配り

原則 2 では、サイバーセキュリティを確保するにあたって、自社のみならず、国内外の拠点、委託先等含めたサプライチェーン全体にわたるサイバーセキュリティ対策を意識することが必要であるとしている。

デジタル技術の業務利用が普及した現代社会においては、サプライチェーンには、デジタル環境を介した外部とのつながりも含まれるようになり、多様化、非定型化されている。そのため、本項目では、自社のみならず、サプライチェーンの国内外のビジネスパートナーやシステム管理等を含むあらゆる委託先等、サプライチェーンの一端を担う企業として全体を意識し、総合的なセキュリティ対策を徹底することが必要であるとしている。

３）社内外関係者との積極的なコミュニケーション

原則 3 では、効果的なサイバーセキュリティ対策を実施するにあたっては社内外の関係者との積極的なコミュニケーションが必要であるとしている。

インシデント発生時などにおいては、社内の関係者とコミュニケーションを円滑に進め、対応していくことが想定される。そのような場面に備えて、平時から、CISO 等はもちろんのこと、社外においても、サイバーセキュリティ関連情報を扱う IPA、JPCERT/CC（JPCERT コーディネーションセンター）、商工会議所等をはじめ、セキュリティ関連製品・サービスの事業者等とも適切なセキュリティリスクに関するコミュニケーションを取ることにより、信頼関係を醸成し、より効果的にサイバーセキュリティ対策を実施していくことが必要となる。そのため、本項目では、社内外の

関係者に対して、平時からサイバーセキュリティリスクやその対策に関する気づきや課題の共有などのコミュニケーションを積極的に取ることが必要であるとしている。

２．経営者が CISO 等に指示すべき重要 10 事項

経営者が CISO 等に指示すべき事項については、①サイバーセキュリティリスクの管理体制構築（指示 1 から指示 3 まで）、②サイバーセキュリティリスクの特定と対策の実装（指示 4 から指示 6 まで）、③インシデント発生に備えた体制構築（指示 7 及び指示 8）、④サプライチェーンセキュリティ対策の推進（指示 9）、及び、⑤ステークホルダーを含めた関係者とのコミュニケーションの推進（指示 10）の 5 つに分類される。

経営者はこれらの事項について、指示を通じて組織に適した形で確実に実施させる必要があるが、担当者に丸投げしてしまうような単なる指示ではなく、自らの役割としてリスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応等を通じてリーダーシップを発揮することが含まれている。

以下、5 つの分類に関する主なポイントを概説する。

１）サイバーセキュリティリスクの管理体制構築（指示 1 から指示 3 まで）

指示 1 から指示 3 までは、サイバーセキュリティに関する対応方針の策定、管理体制の構築、予算・人材等の確保など、サイバーセキュリティ対策を実施するにあたっての体制構築に関する指示事項、対策を怠った場合のシナリオ及び対策例をまとめている。

企業におけるデジタル環境の利用により、一般的な事業活動においてサイバーセキュリティリスクを意識した対応が必要となっていることを踏まえ、組織としての対応方針（セキュリティポリシー）を定め、自社内の全員に共有することが必要である。また、セキュリティ対策業務に従事する人材のみならず、あらゆる業務に従事する人材に、サイバーセキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身につけてもらうことが重要である。

そのため、本項目では、指示 1 において、対応方針を従業員がアクセス可能な場所に掲載すること等によって周知徹底を図ること、また、資源（予算、人材等）の確保に関する指示 3 において、セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門等のあらゆる業務に従事する人材に「プラス・セキュリティ」[1]知識・スキルの習得を促すことなどをまとめている。

なお、指示 2 及び指示 3 に関しては、改訂ガイドラインの付録として、「サイバーセキュリティ体制構築・人材確保の手引き」を公表している。この手引きにおいては、管理体制の構築やサイバーセキュリティ対策のための資源確保に関する適切な判断を

[1] 自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと。

行うためのポイントについて、ステップごとに解説しており、指示 2 及び指示 3 を踏まえた対策を検討するにあたって参考となるものである。

２）サイバーセキュリティリスクの特定と対策の実装（指示 4 から指示 6 まで）

指示 4 から指示 6 までは、サイバーセキュリティリスクについて、その把握、リスクへの対応及び対策の継続的改善に関する指示事項、対策を怠った場合のシナリオ及び対策例をまとめている。

感染症の流行に伴うテレワークの利用増加や、クラウドサービスを利用した保有情報の管理など、企業におけるデジタル環境の依存度が増大している現況においては、サイバーセキュリティリスクの把握等において、これらの技術の利用も踏まえたリスクの把握や対策・継続的改善等が必要となる。

そのため、本項目では、自社のビジネスモデルや利用している技術に応じたサイバーセキュリティリスクの把握、クラウドサービスやテレワークなどの影響を適切に反映させることやリスクに対応するための保護対策として多層防御を実施すること、クラウドサービスを利用する際のアカウント管理などが適切に維持・管理されるようにすること、サイバーセキュリティリスクの特徴を踏まえた PDCA（Plan〔計画〕、Do〔実行〕、Check〔実施状況の確認・評価〕、Act〔改善〕の略）サイクルの運用を実施すること、これらの対策を CSR（Corporate Social Responsibility）報告書等により各ステークホルダーに対して適切に情報開示すること等をまとめている。

３）インシデント発生に備えた体制構築（指示 7 及び指示 8）

指示 7 及び指示 8 では、インシデント発生時の緊急対応体制や事業継続・復旧体制の整備に関する指示事項、対策を怠った場合のシナリオ及び対策例をまとめている。

企業におけるデジタル環境への依存度が増大していることに伴い、単純に IT 環境を復旧させるだけでは事業を再開できない可能性があり、組織としての事業継続の観点から、制御系も含めた業務の復旧プロセスと整合性のとれたデジタル環境の復旧計画及び体制整備が必要となる。

そのため、本項目では、インシデント発生時の対応体制の整備及び復旧目標について組織全体として整合性をとることや、情報系のインシデントに限らず制御系に影響が及ぶようなインシデントを想定した復旧演習の実施、インシデント発生時の体制整備等にあたってのガイダンス[2]を参照すること等をまとめている。

４）サプライチェーンセキュリティ対策の推進（指示 9）

指示 9 では、サプライチェーンセキュリティ対策の推進に関する指示事項、対策を怠った場合のシナリオ及び対策例をまとめている。

---

[2] 警察庁・総務省・経済産業省・サイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセンター、JPCERT/CC）「サイバー攻撃被害に係る情報の共有・公表ガイダンス」。

サイバーセキュリティを確保するにあたって、自社のみならず、国内外の拠点、委託先等含めたサプライチェーン全体にわたるサイバーセキュリティ対策を意識する必要があり、各関係者がサイバーセキュリティリスクへの対応に関して担うべき役割について理解し、対策漏れが生じないようにすることが必要である。

そのため、本項目では、サプライチェーンリスクへの対応に関する役割や責任範囲の明確化、サプライチェーン上での対策の底上げ手段として、SECURITY ACTION[3]の実施、サイバーセキュリティお助け隊サービス[4]等の活用、第三者による監査等をまとめている。

５）ステークホルダーを含めた関係者とのコミュニケーションの推進（指示 10）

指示 10 では、サイバーセキュリティに関する情報の収集、共有及び開示の促進についての指示事項、対策を怠った場合のシナリオ及び対策例をまとめている。

サイバー攻撃が高度化、巧妙化する中で、自社だけではサイバー攻撃に関する情報等の全容解明はより困難となっており、また、情報共有ができていないことにより新たな攻撃情報の入手ができずに対策が遅れるなど、リスクの増加につながるおそれがある。サイバーセキュリティに関する情報共有を積極的に行うことで、インシデントに必要な情報を得るとともに、サイバー攻撃による被害の未然の防止につながる。

そのため、本項目においては、情報の入手のみならず積極的な情報の提供を行うこと、サーバ提供事業者等の外部の事業者等とのサイバーセキュリティ関連情報の共有等に関する積極的な連携を行うこと、中小企業においては商工会議所等を通じた地元での情報共有を行うことのできる相手を確保すること等をまとめている。

Ⅲ サイバーセキュリティ経営ガイドライン Ver3.0 の実践

１．サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集

本ガイドラインは、経営者や CISO 等が実践すべき必要なサイバーセキュリティ対策を紹介している。しかしながら、サイバーセキュリティ対策は、自社の規模や業種に応じた適切な対策を行うことが求められている。そこで、IPA においては、本ガイドラインを踏まえて必要な対策を実践するにあたって参考となる情報を「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集」（以下、本プラクティス集）としてまとめている。

[3] 中小企業自らがセキュリティ対策に取り組むことを宣言する制度。
[4] 中小企業を対象にサイバーセキュリティに関する「見守り」「駆付け」「保険」をまとめて提供するサービス。

本プラクティス集は、情報セキュリティの取組はある程度進めてきたが、サイバー攻撃対策やインシデント対応の強化が必要であり、それに向けてどのような体制づくりを行っていくべきかと考えている経営者、CISO 等及びセキュリティ担当者を想定読者としたものであり、本ガイドラインに基づいてサイバーセキュリティ対策を実践するに当たっての実施手順や取り組む際の考え方などをプラクティス集としてまとめたものである。

なお、本プラクティス集は、企業へのアンケートやインタビューなどを通じて収集した実践事例に基づき作成したものであるが、本プラクティス集に掲載されている各施策は、それぞれの企業におけるサイバーセキュリティに対する考え方、企業風土、企業内の人的・物的リソース等を踏まえて行われているものである。したがって、サイバーセキュリティ対策の実践に当たっては、本プラクティス集を参照しつつも、企業の実情に応じて必要な対策を行うことになる。

２．プラクティス集の構成

本プラクティス集は、紹介する取組事例が様々な形態で利用されることを想定し、次の構成としている（図表 3）。

図表 3　サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集の構成

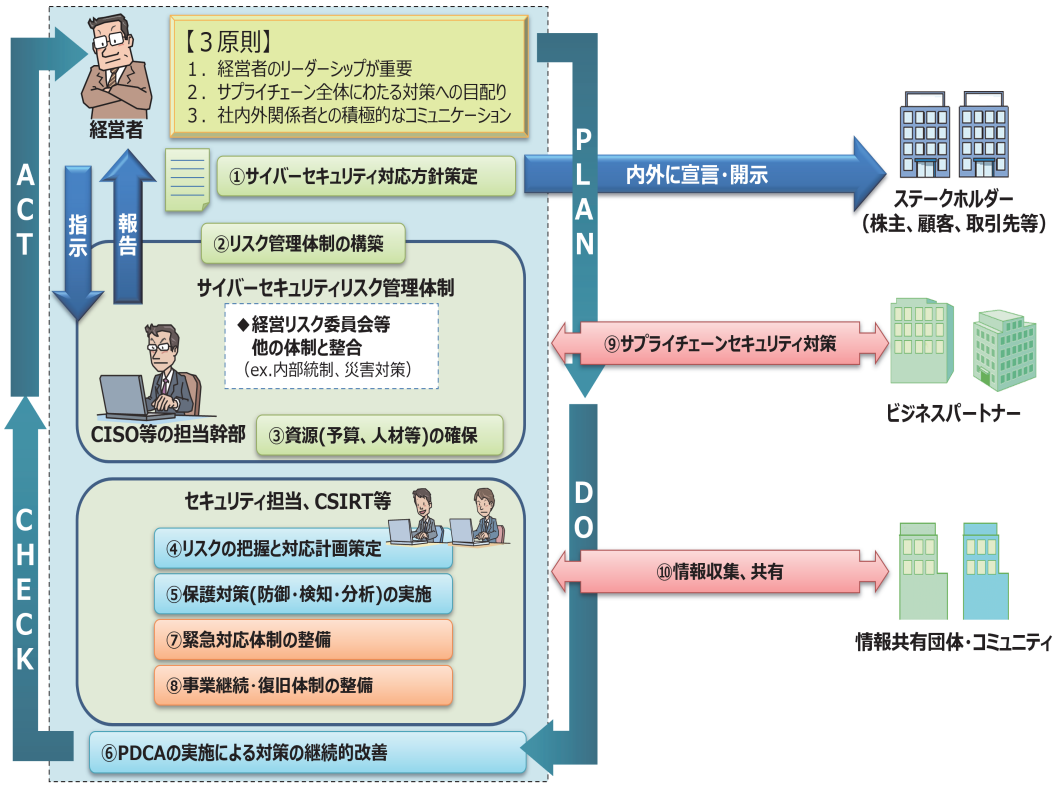
第 1 章　経営とサイバーセキュリティ
第 2 章　サイバーセキュリティ経営ガイドライン実践のプラクティス
第 3 章　セキュリティ担当者の悩みと取組のプラクティス
ミニプラクティス
付録

（出所）独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集　第 4 版」から抜粋

１）第 1 章：経営とサイバーセキュリティ

サイバーセキュリティが与える企業への影響や、これに対する経営課題の重要性をまとめたものであり、主に、経営者や CISO 等を読者としたものである。例えば、なぜサイバーセキュリティ対策が経営課題であるか、また、経営者が認識する必要がある「3 原則」と経営者が CISO 等に指示すべき「重要 10 項目」の全体像などが掲載されている（図表 4）。

図表 4　サイバーセキュリティ経営ガイドライン Ver3.0 の「3 原則」と「重要 10 項目」



（出所）独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集　第 4 版」から抜粋

2）第 2 章：サイバーセキュリティ経営ガイドライン実践のプラクティス

本ガイドラインにおける重要 10 項目の実践手順、実践内容、取組に当たっての考え方などをまとめたものであり、主に、サイバーセキュリティ対策を実施する CISO 等やセキュリティ担当者を読者としたものである。例えば、経営者のサイバーセキュリティリスクに対する認識を向上させるための取組例や、サイバーセキュリティ対策における予算確保のための取組例、ステークホルダーの信頼を高めるためのサイバーセキュリティ情報発信の工夫例などが掲載されている。

3）第 3 章：サイバーセキュリティ対策を推進する担当者の悩みと取組のプラクティス

セキュリティ担当者の日常業務における悩みに対する具体的対応策をまとめたものであり、主に、セキュリティ担当者やセキュリティ人材育成担当者を読者としたものである。例えば、セキュリティ教育を実施しているが効果が感じられないという担当者に対してはセキュリティ意識の向上が図られた取組例を紹介し、社内で情報漏えいが発生した場合の影響を懸念している担当者に対しては情報漏えいを防止するための取組例を紹介し、また、サプライチェーンの委託先企業がセキュリティ対策に協力的でないと感じている担当者に対しては委託先企業が自分事としてセキュリティ対策を進めてもらえるようにするための取組例を紹介している。

Ⅳ サイバーセキュリティ経営の可視化

本ガイドラインにより必要な対策を理解し、本プラクティス集により実践すべき具体的対策を理解したら、具体的な対策を実施することになる。そして、具体的なサイバーセキュリティ対策を実践したら、ステークホルダーを始めとした関係者に自社の対策を開示することによって、自社の評価を上げ価値を高めていくことが重要である。

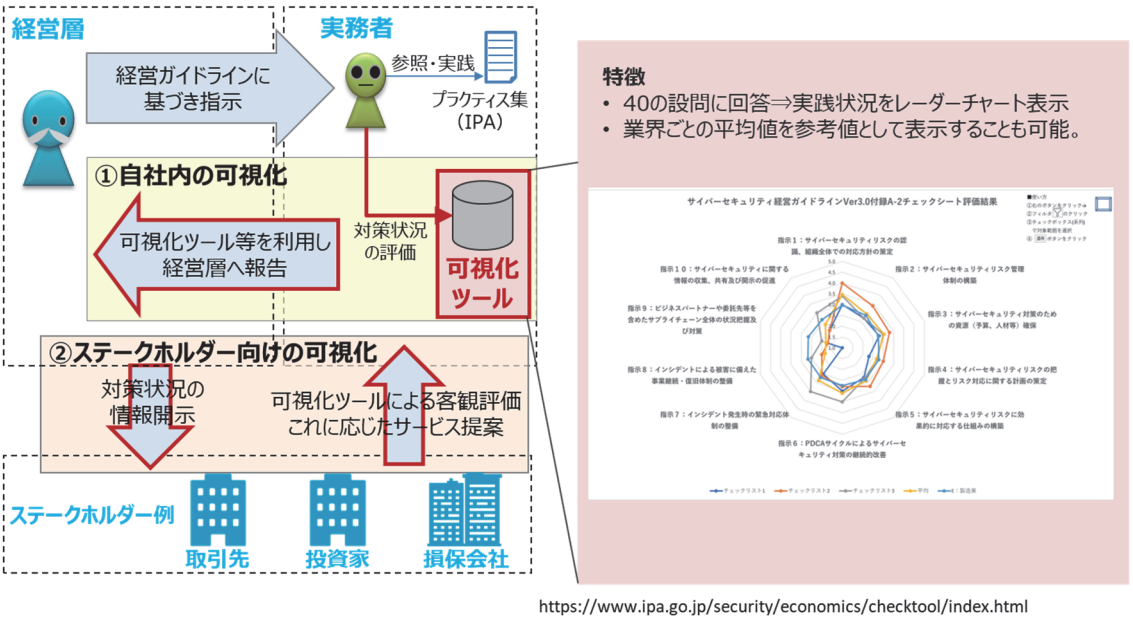
このような観点から、IPA は、本ガイドラインの公表にあわせて、本ガイドラインの重要 10 項目の実施状況を 5 段階の成熟モデルで可視化（レーダーチャート表示）するための支援ツール（Excel 版）である、「サイバーセキュリティ経営可視化ツール」（以下、可視化ツール）を公表した。

可視化ツールは、40 個のチェックリストについて、自社の状況に最も近い選択肢（成熟度）を選択することによって、可視化結果シートが自動的に表示されるものである（図表 5）。また、可視化ツールでは、複数の企業（グループ企業等）の取組状況を比較することも可能となっている。

可視化ツールを活用することで、自社のサイバーセキュリティ対策を定量的に把握でき、サイバーセキュリティに関する方針の策定やセキュリティに関する資源確保を適切に検討していくことが可能となる。また、可視化された取組状況をステークホルダー等の関係者に情報開示することによって、企業価値を更に高めていくことが可能となる（このことは、本ガイドラインの重要 10 項目の指示事項 6 として掲げられている。）。

経営者及び CISO 等においては、可視化ツールを積極的に活用しつつ、継続的な対策を行うとともに、積極的な情報開示を行うことが重要である。

図表 5　サイバーセキュリティ経営可視化ツール



（出所）経済産業省及び独立行政法人情報処理推進機構

V 最後に

サイバーセキュリティ経営の定着を目指すためには、次の 3 つのステップにより必要な対策を行うことが重要と考える。一つ目は、サイバーセキュリティ経営を具体化すること、二つ目は、具体化したサイバーセキュリティ経営を実践すること、そして三つ目が、サイバーセキュリティ経営を可視化するとともに、積極的な情報開示を行うことである。

本稿では、このような観点からサイバーセキュリティ経営を実践し、定着させるに当たっての、政府としての 3 つの支援策について紹介した。

サイバー攻撃の脅威が増していく中、経営者は、サイバーセキュリティ経営の実践に対して、強いリーダーシップを発揮する必要があり、また CISO 等やセキュリティ担当者においては、経営者の指示を踏まえ、自社にとって最適となるセキュリティ対策を実践する必要があると考える。

本稿において紹介したガイドライン等が、企業のサイバーセキュリティ対策の促進のための一助となれば幸いである。