使い方ガイド

1. 本ツールの目的

本ツールは、サイバーセキュリティの実践状況を企業自身がセルフチェックで可視化するためのものです。企業は自社の状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行、投資家等ステークホルダーとのコミュニケーション等が可能となります。

2. 対象利用者

原則として、従業員３００名以上の企業を対象としています。

※従業員３００名未満の企業を対象とすることも排除していないため、例えばグループ企業との比較等にも可能です。

3. 使い方

・本ツールは「使い方ガイド」(本シート)、「チェックリスト」、「可視化結果」の３種類のシートから構成されます。

・チェックリストの39個の質問にセルフチェックで回答します。回答方式は成熟度モデルで、５段階の選択式です。
各質問について自社の状況（成熟度）に最も近い選択肢を選んでください。

・全質問について回答すると、可視化結果シートの表示が自動的に更新されます。

・複数の企業（グループ企業等）を比較したい場合、同じExcelファイル内に企業毎のチェックリストを作成し、
それぞれ回答を記入してください。その後、可視化結果シートで比較したい企業を選択すると、各社の
可視化結果がレーダーチャート上にオーバーレイ表示されます。

・回答結果は、経営者へサイバーセキュリティの実践状況を説明するための資料として使うことができます。

・回答は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（CISO等）が記入し、最終的には
経営者が回答内容を確認・承認してください。
※CISO：Chief Information Security Officer

4. 注意事項

4. 1. 回答前の準備

・対象範囲（スコープ）の決定
本ツールの可視化チェック対象範囲は原則として「企業」ですが、企業内のガバナンス状況等によっては「本社」「支社」「工場」「事業部門」「海外拠点」等の単位とすることもできます。できるだけ正確な可視化のため、スコープを決めてから回答してください。

・エビデンスとなる文書類の準備
自社のサイバーセキュリティに関する文書類を手元に用意しておくと、スムーズかつ正確に回答することができます。
例：
- セキュリティ基本方針（セキュリティポリシー）
- セキュリティ体制図（全社のセキュリティ関連の体制図、報告ルート、人材配置等）
- セキュリティの技術的対策文書（セキュア開発の規程、実施中の対策リスト、運用方針等）
- セキュリティリスク管理のKPI一覧
- インシデント対応・復旧関連文書
- サプライチェーンセキュリティ関連文書

4. 2. 回答にあたって

・正確な可視化を行うため、上記の文書類等のエビデンスをできるだけ確認しながら回答してください。
不明点があれば社内の関係者に確認等してください。

・各質問の選択肢は、利用者の負荷を軽減するためシンプルな文にしています。その結果、選択肢が指すものが
イメージできない場合は、「補足」列の例示等を参考にしてください。

・異なる役職・立場の複数人でクロスチェックすることにより回答の精度を高めることも有効です。

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
1	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	1	1-1	経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	1	認識していない又は部分的である	○	0	0.00	・経営会議の例：取締役会等、経営者が出席する会議
					2	認識しているが、文書化等はできていない	○			
					3	認識しており、文書化されているが、対策は部下に任せている	○			
					4	認識しており、定期的に経営会議等で議論している	○			
					5	認識しており、経営会議等での議論を踏まえて継続的に改善している	○			
		2	1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している	1	できていない又は部分的である	○	0		・基本方針はセキュリティポリシーと同義
					2	方針内容が規程化されている	○			
					3	規程の内容が実施されている	○			
					4	実施内容が定期的に監査されている	○			
					5	規程や実施内容が継続的に改善されている	○			
		3	1-3	法令・契約やガイドライン等の要求事項を把握し、対応している	1	できていない又は部分的である	○	0		・法令についてはサイバーセキュリティ関係法令Q&Aハンドブック（NISC）を参照。ガイドラインについては同ハンドブックの付録１を参照。 https://www.nisc.go.jp/security-site/law_handbook/index.html ・海外拠点については各国の法令・ガイドラインも確認すること。
					2	把握し、文書化されている	○			
					3	要求事項の内容が対応されている	○			
					4	要求事項が定期的に見直されている	○			
					5	要求事項やその対応が継続的に改善されている	○			
2	指示2：サイバーセキュリティリスク管理体制の構築	4	2-1	組織の基本方針に基づき、CISO等からなるサイバーセキュリティリスク管理体制を構築している	1	できていない又は部分的である	○	0	0.00	・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	管理体制の組織図があり、周知されている	○			
					3	体制に適切なリソースが割り当てられている	○			
					4	体制の運営状況が定期的に評価されている	○			
					5	文書や管理体制の運営状況が継続的に改善されている	○			
		5	2-2	セキュリティリスク管理体制において、各関係者の役割と責任を明確にしている	1	できていない又は部分的である	○	0		・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	役割と責任が文書化されている	○			
					3	役割と責任が周知されている	○			
					4	役割と責任が定期的に評価されている	○			
					5	役割と責任が継続的に再定義されている	○			
		6	2-3	組織内のリスク管理体制（リスク委員会等）とサイバーセキュリティリスク管理体制（セキュリティ委員会等）の関係を明確にしている	1	サイバーセキュリティリスク管理体制がない又は部分的である	○	0		・サイバーセキュリティリスク管理体制の例：セキュリティ統括室、セキュリティ委員会 ・関係明確化を確認する方法の例： - サイバーセキュリティリスク管理に関する役割分担表等による相違点の確認 - 経営者や従業員への聞き取り調査 ・サイバーセキュリティリスク管理体制とリスク管理体制が独立しているということは、サイバーセキュリティリスクを他の事業リスクとは分けて、独立して管理する体制が構築されている。ただし、人員の重複などはありえる、ということ ・あるべき姿の例：組織内のリスク管理体制とサイバーセキュリティリスク管理体制を分離し、両者の関係を明確に規定し、実施内容が継続的に改善されている ・両者の連携の例：一方のメンバーが他方の会議にオブザーバ参加する、定期的に連絡会議を開催する、主な会議の議事録を共有する等
					2	両者の関係が明確にされていない	○			
					3	サイバーセキュリティリスク管理体制はリスク管理体制の一部として存在している	○			
					4	両者の関係が独立している	○			
					5	両者の関係が独立しており、必要な連携が行われている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
3	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	7	3-1	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている	1	できていない又は計画的でない	○	0	0.00	・対策の例：セキュリティ対策製品の導入、運用プロセスの見直し、人員増強
					2	対策及び資源が文書化されている	○			
					3	対策及び資源が周知されている	○			
					4	対策及び資源が定期的に評価されている	○			
					5	対策及び資源が継続的に改善されている	○			
		8	3-2	自組織で対応する部分と外部に委託する部分を適切に切り分けている	1	できていない又は計画的でない	○	0		・具体的な対策、緊急時対応等の項目の明文化と、それらのうちどこを自社で行いどこから外部に委託するかの方針 ・「おおよその切り分け」の例：システムの企画は自組織、設計・開発・運用は外部 ・具体的な切り分けの例： - 対策　対応組織 ーーーーーーーーーーーーーーーーーー 資産管理：　自組織 ID管理：　自組織 アクセス制御：　自組織 監視/ログ収集：　外部 異常検知：　外部 インシデントレスポンス：　自組織 フォレンジック：　外部
					2	おおよその切り分け方針ができている	○			
					3	具体的な領域、技術等で切り分けができている	○			
					4	切り分けが定期的に評価されている	○			
					5	切り分けが継続的に改善されている	○			
		9	3-3	自組織に求められる体制を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を検討している	1	できていない又は計画的でない	○	0		・人材確保のための活動の例：採用、育成（キャリアパスの設計を含む）、評価 ・あるべき姿の例： －育成・採用の方針を明らかにする －内部で育成するべきスキルと外部から調達するべきスキルを明らかにする －採用計画または育成計画を作成する
					2	人材が確保されているが育成が計画的でない	○			
					3	人材が計画的に確保、育成されている	○			
					4	人材が計画的に確保、育成され処遇にも反映されている	○			
					5	計画とその実施内容が継続的に改善されている	○			
		10	3-4	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している	1	できていない又は計画的でない	○	0		・外部リソースの例：セキュリティベンダ、外部人材、クラウドサービス ・情報セキュリティサービス審査登録制度等の活用 https://www.ipa.go.jp/security/it-service/service_list.html
					2	外部リソースの活用方針が文書化されている	○			
					3	方針に従って外部リソースが活用されている	○			
					4	活用状況が定期的に評価されている	○			
					5	方針や実施状況が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
4	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	11	4-1	守るべきIT資産（情報資産やシステム）を特定し、当該資産の場所やビジネス上の価値等に基づいて優先順位付けを行っている	1	できていない又は計画的でない	○	0	0.00	・IT資産の分類・管理の規程を定める ・情報管理規程で管理レベル高である情報を洗い出し、守るべき情報を経営者やCISOと合意する
					2	IT資産の情報が人手で収集されている	○			
					3	IT資産の価値が評価され優先順位がつけられている	○			
					4	守るべきIT資産について、経営者やCISOと合意している	○			
					5	IT資産が自動的に収集され、資産価値が定期的に見直されている	○			
		12	4-2	特定した守るべきIT資産に対するサイバー攻撃の脅威、脆弱性を、脅威情報のデータベース等を用いて認識し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している	1	できていない又は計画的でない	○	0		・サイバーセキュリティリスクが自社の事業に及ぼす影響については、CISOや経営者も認識していることを確認する ・サイバー攻撃の脅威、脆弱性の認識とは、同業他社や取引先へのサイバー攻撃の動向や事例を把握すること、自組織が使っているシステムで報告されている脆弱性を把握すること等 ・脅威情報のデータベースとは脅威インテリジェンスのことで、公開情報の他、それらを提供するベンダーの活用も含む ・自社事業への影響の例：顧客の個人情報が漏洩して多額の賠償、委託元の機密情報が漏えいして取引停止、ランサムウェアで工場が停止
					2	サイバー攻撃の脅威、脆弱性の情報を恒常的に収集されている	○			
					3	脅威、脆弱性情報について、自社の事業に与える影響が評価されている	○			
					4	自社の事業に与える影響が大きい脅威、脆弱性情報について優先的に対応されている	○			
					5	脅威、脆弱性情報による評価、対応の仕組みが継続的に改善されている	○			
		13	4-3	サイバーセキュリティリスクの影響の度合いに従ってリスク対応計画を策定している	1	できていない又は計画的でない	○	0		リスク対応策の例：重要な情報へのアクセス制御、ソフトウェア更新の徹底、端末の持ち出し禁止、クラウドサービスの利用、サイバー保険の加入
					2	サイバーセキュリティリスクの影響度合いが組織的に評価されている	○			
					3	評価結果に基づき、対応計画が策定され実施されている	○			
					4	対応の実施結果が評価されている	○			
					5	サイバーセキュリティリスク評価のＰＤＣＡサイクルが改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール				備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
5	指示5：サイバーセキュリティリスクに対応するための仕組みの構築	14	5-1	情報システムのIT資産管理・構成管理・パッチ管理を行っている	1	できていない又は計画的でない	○	0	0.00	・「人手で実施」の例：IT資産を目視で確認し、Excelの台帳に手入力で入力・更新すること ・検知したものの確認の例： －古いバージョンのソフトウェアがシステム内に見つかったらバージョンアップする －自社が使用しているソフトウェアを把握しておき、ベンダーからパッチが提供されたらパッチ適用する
					2	人手で管理されている	○			
					3	ツールを使って管理されている	○			
					4	検知したものが確認されている	○			
					5	運用が継続的に見直されている	○			
		15	5-2	組織内でシャドーITを利用させない対策を行っている	1	ルールが定められていない	○	0		・シャドーITとは、情報システム部門の許可を得ずに、従業員又は部門が業務に利用しているデバイスやクラウドサービス ・デバイスの例：従業員私物のスマホやタブレット ・「人手で実施」の例：「情報システム部が認めたクラウドサービス以外のサービスを業務で利用しないこと」等の規程を定め、社員にメール等で周知すること
					2	ルールが定められている	○			
					3	ルールに基づく利用申告等が実施されている	○			
					4	ルール違反の検知と対応を行っている	○			
					5	運用が継続的に見直されている	○			
		16	5-3	システム設計時にリスク分析を行い、必要なセキュリティ機能を具体化し、開発時に実装している	1	できていない又は計画的でない	○	0		・プロセスの例：セキュアシステム開発方法論等の中で、システム設計の規約、コーディングの規約、脆弱性診断の規約、次工程へ進むための判断基準等が定められている ・実装の例： －システムの運用に必要でないポート、プロトコル、サービス等を無効化すること －SQLインジェクション等の攻撃に使われるセキュリティホールが発生しないようにコーディングすること －リリース前に脆弱性診断を実施
					2	セキュア開発のプロセスが文書化・周知されている	○			
					3	文書の内容が実施されている	○			
					4	文書や実施内容が定期的に評価されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		17	5-4	重要業務を行う端末・サーバ等には複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・端末・サーバ等の例：PC、サーバ、複合機、ネットワークカメラ、テレワーク端末等 ・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		18	5-5	重要業務を行うネットワークには複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		19	5-6	システム等に対する定期的な脆弱性診断や、継続的なパッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している	1	実行できていない	○	0		・脆弱性診断の例：プラットフォーム診断、Webアプリケーション診断等 参考：情報セキュリティサービス審査登録制度（脆弱性診断サービス） https://www.ipa.go.jp/files/000067318.pdf ・脆弱性への対処の例：セキュリティパッチ適用、WAF導入
					2	実行されているが計画的ではない	○			
					3	計画が立てられており、部分的に実行されている	○			
					4	計画通りに実行されている	○			
					5	計画が継続的に見直されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示		付録Aのチェック項目				選択肢	回答欄（該当する箇所を選択）	スコア	平均	
		20	5-7	端末やネットワークからのログを収集・分析している。	1	できていない又は計画的でない	○	0		・収集すべきログ/イベントの例：システム内で起こった特定の現象・動作を記録するイベントログ、セキュリティ機器が出すアラート等のログ ・ログ収集・分析ツールとはSIEM（Security Information and Event Management）等のこと 参考：情報セキュリティサービス審査登録制度（セキュリティ監視・運用サービス） https://www.ipa.go.jp/files/000067320.pdf
					2	イベント（ログ）収集の仕組みとプロセスがある	○			
					3	収集したログを分析し、異常を検知する仕組みとプロセスがある	○			
					4	検知したものの確認をする仕組みとプロセスがある	○			
					5	運用が継続的に見直されている	○			
		21	5-8	サイバー攻撃を検知した際に不正通信を遮断する等のインシデント対応の仕組みを導入している	1	できていない	○	0		・「その都度実施」の例：マルウェア感染が疑われる時、PCからLANケーブルを抜く ・ツールの例：EDRで端末・サーバ内の不審なプロセスを止める、サンドボックスでマルウェアを解析してWebやメールのフィルタリングをする
					2	その都度実施している	○			
					3	標準化された対応方針がある	○			
					4	ツールを使って自動化されている	○			
					5	運用が継続的に見直されている	○			
		22	5-9	インシデントの管理の仕組みを導入している	1	できていない	○	0		・インシデント管理の例：インシデント管理ツールにアラートの内容を登録してチケット発行、対応優先度の決定と担当者のアサイン、対応状況のフォロー、クロージングまでの管理 ・「人手で管理する仕組み」の例：Excelの所定のフォーマットに手作業で入力・更新
					2	その都度実施されている	○			
					3	人手で管理する仕組みが導入されている	○			
					4	ツールを使う仕組みが導入されている	○			
					5	運用が継続的に見直されている	○			
		23	5-10	従業員に対して、サイバーセキュリティの教育・演習を実施している	1	できていない又は計画的でない	○	0		・教育の例：EラーニングによるWeb教育 ・演習の例：「怪しいメールが来た」「添付ファイルを開いてしまった」等と当事者から報告させることを含む標的型攻撃メール訓練 ・演習の例は指示7-5、8-2の備考を参照
					2	教育・演習計画を策定している	○			
					3	計画に基づき教育が実施されている	○			
					4	計画に基づき演習が実施されている	○			
					5	教育・演習計画や実施内容を見直し、継続的に改善されている	○			
6	指示6：サイバーセキュリティ対策におけるPDCAサイクルの実施	24	6-1	サイバーセキュリティ運用管理に関するKPIを定めている	1	できていない又は計画的でない	○	0	0.00	・KPIの例：リスク分析での指摘事項数、組織内のセキュリティ教育の受講状況、インシデントの発生数、アセスメント実施状況、脆弱性対策状況
					2	KPIが文書化されている	○			
					3	KPIが測定されている	○			
					4	KPIの測定結果が定期的に評価されている	○			
					5	KPIが継続的に見直されている	○			
		25	6-2	経営者が定期的に、サイバーセキュリティ運用に関する報告を受け、認識対策を指示している	1	できていない又は計画的でない	○	0		・報告の仕方の例：経営会議の議題にサイバーセキュリティに関するKPIの報告が含まれている ・報告事項の例：KPI、インシデント、予算執行、重大ニュース ・報告の仕方の改善例：経営層の望む情報・指標等を新たに作って盛り込む
					2	インシデントなどの突発事象のみ報告されている	○			
					3	セキュリティ運用全般について報告されている	○			
					4	セキュリティ運用全般について報告され対策を指示している	○			
					5	報告ルールや対策の方法が継続的に改善されている	○			
		26	6-3	サイバーセキュリティにかかる内部監査、外部監査を踏まえ、サイバーセキュリティ対策を適時見直している	1	できていない又は計画的でない	○	0		・例： －毎年の監査計画が定められ、文書化されている －監査結果を受けてセキュリティ方針・対策の見直しを企画し、経営会議等に報告されている ・参考：情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス） https://www.ipa.go.jp/files/000067317.pdf
					2	監査と対策見直しの方針が文書化されている	○			
					3	方針に従って監査が実施されている	○			
					4	監査結果が評価され、対応されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		27	6-4	サイバーセキュリティリスクや取組状況をステークホルダーに情報公開している	1	できていない又は計画的でない	○	0		・例：情報セキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等を通して情報公開する
					2	情報公開の方針が文書化されている	○			
					3	方針に則って情報公開がされている	○			
					4	方針や情報公開の内容が定期的に評価されている	○			
					5	方針や内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール				備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
7 指示7：インシデント発生時の緊急対応体制の整備	28	7-1	インシデント対応計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －初動対応マニュアルの整備等 －組織内における緊急連絡先・伝達ルートの整備 ・緊急連絡先・伝達ルートの例：緊急連絡網、報告先一覧（上司、CSIRT、広報部門、法務部門、経営者等）
				2	計画が文書化されている	○			
				3	計画が周知されている	○			
				4	計画が定期的に評価されている	○			
				5	計画が継続的に改善されている	○			
	29	7-2	インシデント対応の専門チーム（CSIRT等）を設置している	1	できていない又は計画的でない	○	0		・CSIRT：Computer Security Incident Response Team ・参考：「組織内CSIRT構築の参考資料 インシデント対応マニュアルの作成について」（JPCERT/CC）
				2	チームの構成等が文書化されている	○			
				3	専門チームが設置され、要員が割り当てられている	○			
				4	活動状況が定期的に評価されている	○			
				5	体制や活動内容が継続的に改善されている	○			
	30	7-3	組織外に報告・公表すべき内容やタイミングを定めている	1	できていない又は計画的でない	○	0		・組織外の例：取引先、JPCERT/CC、IPA、所管省庁、マスコミ ・広報部門等とも連携し、公表する／しない項目、公表の仕方等を文書化し、関係部門に周知している ・「文書の内容に対する取組み」の例：CISO等が報告ルート、公表すべき内容を、関係者に周知している ・不特定多数のサプライチェーン関係者へ影響が懸念される場合など、広く対策を促す必要がある場合もあるため、公表のメリット・デメリットを十分に検討した上で、適切と判断される場合には、公表を行うことが望ましい。
				2	報告ルート、公表すべき内容などが文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			
	31	7-4	インシデント発生時の緊急対応の演習を定期的に行っている	1	できていない又は計画的でない	○	0		・演習の例： －マルウェア感染が疑われる端末での初期対処方法の確認 －フォレンジック対応のログを残す手順の確認 －社内関係者への連絡手順の確認 －所管省庁等への報告手順の確認
				2	演習の方針、内容が文書化されている	○			
				3	方針に則って演習が実施されている	○			
				4	演習の内容と結果が演習実施の度に評価されている	○			
				5	方針や実施内容が継続的に見直されている	○			
	32	7-5	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している	1	できていない又は計画的でない	○	0		・例： －インシデントに関連するログを速やかに分析できるシステムを整備している －インシデント対応手順にフォレンジック対応の項目を入れている －フォレンジック専業の事業者と契約している 参考：情報セキュリティサービス審査登録制度（デジタルフォレンジックサービス） https://www.ipa.go.jp/files/000067319.pdf
				2	ログ分析・調査の方針と内容が文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
8	指示8：インシデントによる被害に備えた復旧体制の整備	33	8-1	被害が発生した際に備えた業務の復旧計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －BCPとの連携等、組織全体として整合のとれた復旧目標計画 －システム復旧マニュアルの整備 －業務復旧マニュアルの中に重大インシデントが起きた時のおおまかな業務復旧手順やシステム復旧手順を記述 －組織の内外における連絡先・伝達ルートの整備 ・連絡先の例：経営者層、JPCERT/CC、インターネットサービスプロバイダ、自社システムへの攻撃の踏み台にされたシステムのオーナー、他組織のCSIRT、ベンダー
					2	計画が文書化されている	○			
					3	計画が周知されている	○			
					4	計画が定期的に評価されている	○			
					5	計画が継続的に改善されている	○			
		34	8-2	定期的に復旧対応演習を行っている	1	できていない又は計画的でない	○	0		・年間の演習計画の策定 ・演習の例： －マルウェア感染端末のクリアインストール・再設定 －安全が確認されたシステムから順次復旧 －社内関係者への報告手順の確認 －上記のTTX（机上演習）、実機演習等
					2	演習の方針、内容が文書化されている	○			
					3	方針に則って演習が実施されている	○			
					4	演習の内容と結果が演習実施の度に評価されている	○			
					5	方針や実施内容が継続的に見直されている	○			
9	指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	35	9-1	グループ企業に関するリスク分析を行い、対策をグループ内の規程等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0	0.00	・例：本可視化ツールを用いてグループ企業から報告を受ける 参考：グループ・ガバナンス・システムに関する実務指針 https://www.meti.go.jp/press/2019/06/20190628003/20190628003.html ・文書の例：グループ内のサイバーセキュリティ基本方針や対策の規程、親会社から子会社へのセキュリティ対策実施指示 ・グループ経営会議の議題にサイバーセキュリティも含まれている ・親会社の情報システム部門が子会社のセキュリティ対策状況を定期的に調査、指導している 等
					2	グループ企業に関するリスク分析が一部実施されている	○			
					3	グループ企業に関するリスク分析が実施されている	○			
					4	グループ企業間でリスク分析結果を共有し対策を検討している	○			
					5	グループ企業でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		36	9-2	委託先等の取引先に関するリスク分析を行い、対策を契約書等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0		・例： －本可視化ツールを用いて委託先から報告を受ける －委託元の情報システム部門が委託先のセキュリティ対策状況をアンケート、立ち入り等の手法で調査、指導している ・文書の例：契約書、仕様書や品質保証文書
					2	委託先等の取引先に関するリスク分析が一部実施されている	○			
					3	委託先等の取引先に関するリスク分析が実施されている	○			
					4	委託先等の取引先関係企業間でリスク分析結果が共有され対策が検討されている	○			
					5	委託先等の取引先でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		37	9-3	サプライチェーン全体を俯瞰した関連組織全体で、リスク分析を行い対策状況の検討を行っている。	1	できていない又は計画的でない	○	0		
					2	事業毎のサプライチェーン全体が把握されている	○			
					3	サプライチェーン全体でのリスク分析が行われいる	○			
					4	サプライチェーン全体の関係企業間でリスク分析結果を共有し対策が検討されている	○			
					5	サプライチェーン全体でのリスク対策が評価され、実施内容が継続的に見直されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール						備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均		
10	指示10：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	38	10-1	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通して情報共有を行い、自社の対策に活かしている	1	できていない又は計画的でない	○	0	0.00		・関係団体の例：NISC、関係省庁、IPA、JPCERT/CC、日本シーサート協議会、各種ISAC（Information Sharing and Analysis Center） ・業界横断的に広く再発防止策を共有するために、IPAサイバー情報共有イニシアティブ（J-CSIP）、NISCセプターカウンシル、サイバーセキュリティ協議会等に加盟することも考えられる。
					2	不定期に参加して情報入手している	○				
					3	計画して参加し情報共有している	○				
					4	情報共有の内容と効果を定期的に評価している	○				
					5	情報共有の方法を継続的に改善している	○				
		39	10-2	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティに情報提供や相談を実施している	1	できていない又は計画的でない	○	0			・標的型攻撃においては、攻撃者がターゲットとする情報を入手するために、特定企業のみならず、その取引先に対しても同様の手口で攻撃を行う傾向がある。そのため、委託先等の取引先に迅速に情報共有することが望ましい。 ・ 初動対応において技術的助言を必要とする場合には、自社のシステム調達に関わっているシステムベンダやセキュリティベンダ等のほか、IPA J-CRAT 、JPCERT/CC へ相談することが有効。 ・ 既にISACが組織化されている業界においては、ISACの枠組みにおいて情報共有することも考えられる。
					2	情報提供の方針が文書化されている	○				
					3	文書の内容が実施されている	○				
					4	情報提供の内容と効果が定期的に評価されている	○				
					5	文書や実施内容が継続的に改善されている	○				

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
1	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	1	1-1	経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	1	認識していない又は部分的である	○	0	0.00	・経営会議の例：取締役会等、経営者が出席する会議
					2	認識しているが、文書化等はできていない	○			
					3	認識しており、文書化されているが、対策は部下に任せている	○			
					4	認識しており、定期的に経営会議等で議論している	○			
					5	認識しており、経営会議等での議論を踏まえて継続的に改善している	○			
		2	1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している	1	できていない又は部分的である	○	0		・基本方針はセキュリティポリシーと同義
					2	方針内容が規程化されている	○			
					3	規程の内容が実施されている	○			
					4	実施内容が定期的に監査されている	○			
					5	規程や実施内容が継続的に改善されている	○			
		3	1-3	法令・契約やガイドライン等の要求事項を把握し、対応している	1	できていない又は部分的である	○	0		・法令についてはサイバーセキュリティ関係法令Q&Aハンドブック（NISC）を参照。ガイドラインについては同ハンドブックの付録１を参照。 https://www.nisc.go.jp/security-site/law_handbook/index.html ・海外拠点については各国の法令・ガイドラインも確認すること。
					2	把握し、文書化されている	○			
					3	要求事項の内容が対応されている	○			
					4	要求事項が定期的に見直されている	○			
					5	要求事項やその対応が継続的に改善されている	○			
2	指示2：サイバーセキュリティリスク管理体制の構築	4	2-1	組織の基本方針に基づき、CISO等からなるサイバーセキュリティリスク管理体制を構築している	1	できていない又は部分的である	○	0	0.00	・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	管理体制の組織図があり、周知されている	○			
					3	体制に適切なリソースが割り当てられている	○			
					4	体制の運営状況が定期的に評価されている	○			
					5	文書や管理体制の運営状況が継続的に改善されている	○			
		5	2-2	セキュリティリスク管理体制において、各関係者の役割と責任を明確にしている	1	できていない又は部分的である	○	0		・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	役割と責任が文書化されている	○			
					3	役割と責任が周知されている	○			
					4	役割と責任が定期的に評価されている	○			
					5	役割と責任が継続的に再定義されている	○			
		6	2-3	組織内のリスク管理体制（リスク委員会等）とサイバーセキュリティリスク管理体制（セキュリティ委員会等）の関係を明確にしている	1	サイバーセキュリティリスク管理体制がない又は部分的である	○	0		・サイバーセキュリティリスク管理体制の例：セキュリティ統括室、セキュリティ委員会 ・関係明確化を確認する方法の例： - サイバーセキュリティリスク管理に関する役割分担表等による相違点の確認 - 経営者や従業員への聞き取り調査 ・サイバーセキュリティリスク管理体制とリスク管理体制が独立しているということは、サイバーセキュリティリスクを他の事業リスクとは分けて、独立して管理する体制が構築されている。ただし、人員の重複などはありえる、ということ ・あるべき姿の例：組織内のリスク管理体制とサイバーセキュリティリスク管理体制を分離し、両者の関係を明確に規定し、実施内容が継続的に改善されている ・両者の連携の例：一方のメンバーが他方の会議にオブザーバ参加する、定期的に連絡会議を開催する、主な会議の議事録を共有する等
					2	両者の関係が明確にされていない	○			
					3	サイバーセキュリティリスク管理体制はリスク管理体制の一部として存在している	○			
					4	両者の関係が独立している	○			
					5	両者の関係が独立しており、必要な連携が行われている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改				可視化ツール					備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
3 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	7	3-1	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている	1	できていない又は計画的でない	○	0	0.00	・対策の例：セキュリティ対策製品の導入、運用プロセスの見直し、人員増強
				2	対策及び資源が文書化されている	○			
				3	対策及び資源が周知されている	○			
				4	対策及び資源が定期的に評価されている	○			
				5	対策及び資源が継続的に改善されている	○			
	8	3-2	自組織で対応する部分と外部に委託する部分を適切に切り分けている	1	できていない又は計画的でない	○	0		・具体的な対策、緊急時対応等の項目の明文化と、それらのうちどこを自社で行いどこから外部に委託するかの方針 ・「おおよその切り分け」の例：システムの企画は自組織、設計・開発・運用は外部 ・具体的な切り分けの例： - 対策　対応組織 ーーーーーーーーーーーーーーーーーー 資産管理：　自組織 ID管理：　自組織 アクセス制御：　自組織 監視/ログ収集：　外部 異常検知：　外部 インシデントレスポンス：　自組織 フォレンジック：　外部
				2	おおよその切り分け方針ができている	○			
				3	具体的な領域、技術等で切り分けができている	○			
				4	切り分けが定期的に評価されている	○			
				5	切り分けが継続的に改善されている	○			
	9	3-3	自組織に求められる体制を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を検討している	1	できていない又は計画的でない	○	0		・人材確保のための活動の例：採用、育成（キャリアパスの設計を含む）、評価 ・あるべき姿の例： －育成・採用の方針を明らかにする －内部で育成するべきスキルと外部から調達するべきスキルを明らかにする －採用計画または育成計画を作成する
				2	人材が確保されているが育成が計画的でない	○			
				3	人材が計画的に確保、育成されている	○			
				4	人材が計画的に確保、育成され処遇にも反映されている	○			
				5	計画とその実施内容が継続的に改善されている	○			
	10	3-4	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している	1	できていない又は計画的でない	○	0		・外部リソースの例：セキュリティベンダ、外部人材、クラウドサービス ・情報セキュリティサービス審査登録制度等の活用 https://www.ipa.go.jp/security/it-service/service_list.html
				2	外部リソースの活用方針が文書化されている	○			
				3	方針に従って外部リソースが活用されている	○			
				4	活用状況が定期的に評価されている	○			
				5	方針や実施状況が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
4	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	11	4-1	守るべきIT資産（情報資産やシステム）を特定し、当該資産の場所やビジネス上の価値等に基づいて優先順位付けを行っている	1	できていない又は計画的でない	○	0	0.00	・IT資産の分類・管理の規程を定める ・情報管理規程で管理レベル高である情報を洗い出し、守るべき情報を経営者やCISOと合意する
					2	IT資産の情報が人手で収集されている	○			
					3	IT資産の価値が評価され優先順位がつけられている	○			
					4	守るべきIT資産について、経営者やCISOと合意している	○			
					5	IT資産が自動的に収集され、資産価値が定期的に見直されている	○			
		12	4-2	特定した守るべきIT資産に対するサイバー攻撃の脅威、脆弱性を、脅威情報のデータベース等を用いて認識し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している	1	できていない又は計画的でない	○	0		・サイバーセキュリティリスクが自社の事業に及ぼす影響については、CISOや経営者も認識していることを確認する ・サイバー攻撃の脅威、脆弱性の認識とは、同業他社や取引先へのサイバー攻撃の動向や事例を把握すること、自組織が使っているシステムで報告されている脆弱性を把握すること等 ・脅威情報のデータベースとは脅威インテリジェンスのことで、公開情報の他、それらを提供するベンダーの活用も含む ・自社事業への影響の例：顧客の個人情報が漏洩して多額の賠償、委託元の機密情報が漏えいして取引停止、ランサムウェアで工場が停止
					2	サイバー攻撃の脅威、脆弱性の情報を恒常的に収集されている	○			
					3	脅威、脆弱性情報について、自社の事業に与える影響が評価されている	○			
					4	自社の事業に与える影響が大きい脅威、脆弱性情報について優先的に対応されている	○			
					5	脅威、脆弱性情報による評価、対応の仕組みが継続的に改善されている	○			
		13	4-3	サイバーセキュリティリスクの影響の度合いに従ってリスク対応計画を策定している	1	できていない又は計画的でない	○	0		リスク対応策の例：重要な情報へのアクセス制御、ソフトウェア更新の徹底、端末の持ち出し禁止、クラウドサービスの利用、サイバー保険の加入
					2	サイバーセキュリティリスクの影響度合いが組織的に評価されている	○			
					3	評価結果に基づき、対応計画が策定され実施されている	○			
					4	対応の実施結果が評価されている	○			
					5	サイバーセキュリティリスク評価のＰＤＣＡサイクルが改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改				可視化ツール					備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
5	指示5：サイバーセキュリティリスクに対応するための仕組みの構築	14	5-1	情報システムのIT資産管理・構成管理・パッチ管理を行っている	1	できていない又は計画的でない	○	0	0.00	・「人手で実施」の例：IT資産を目視で確認し、Excelの台帳に手入力で入力・更新すること ・検知したものの確認の例： －古いバージョンのソフトウェアがシステム内に見つかったらバージョンアップする －自社が使用しているソフトウェアを把握しておき、ベンダーからパッチが提供されたらパッチ適用する
					2	人手で管理されている	○			
					3	ツールを使って管理されている	○			
					4	検知したものが確認されている	○			
					5	運用が継続的に見直されている	○			
		15	5-2	組織内でシャドーITを利用させない対策を行っている	1	ルールが定められていない	○	0		・シャドーITとは、情報システム部門の許可を得ずに、従業員又は部門が業務に利用しているデバイスやクラウドサービス ・デバイスの例：従業員私物のスマホやタブレット ・「人手で実施」の例：「情報システム部が認めたクラウドサービス以外のサービスを業務で利用しないこと」等の規程を定め、社員にメール等で周知すること
					2	ルールが定められている	○			
					3	ルールに基づく利用申告等が実施されている	○			
					4	ルール違反の検知と対応を行っている	○			
					5	運用が継続的に見直されている	○			
		16	5-3	システム設計時にリスク分析を行い、必要なセキュリティ機能を具体化し、開発時に実装している	1	できていない又は計画的でない	○	0		・プロセスの例：セキュアシステム開発方法論等の中で、システム設計の規約、コーディングの規約、脆弱性診断の規約、次工程へ進むための判断基準等が定められている ・実装の例： －システムの運用に必要でないポート、プロトコル、サービス等を無効化すること －SQLインジェクション等の攻撃に使われるセキュリティホールが発生しないようにコーディングすること －リリース前に脆弱性診断を実施
					2	セキュア開発のプロセスが文書化・周知されている	○			
					3	文書の内容が実施されている	○			
					4	文書や実施内容が定期的に評価されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		17	5-4	重要業務を行う端末・サーバ等には複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・端末・サーバ等の例：PC、サーバ、複合機、ネットワークカメラ、テレワーク端末等 ・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		18	5-5	重要業務を行うネットワークには複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		19	5-6	システム等に対する定期的な脆弱性診断や、継続的なバッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している	1	実行できていない	○	0		・脆弱性診断の例：プラットフォーム診断、Webアプリケーション診断等 参考：情報セキュリティサービス審査登録制度（脆弱性診断サービス） https://www.ipa.go.jp/files/000067318.pdf ・脆弱性への対処の例：セキュリティパッチ適用、WAF導入
					2	実行されているが計画的ではない	○			
					3	計画が立てられており、部分的に実行されている	○			
					4	計画通りに実行されている	○			
					5	計画が継続的に見直されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール				備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
		20	5-7	端末やネットワークからのログを収集・分析している。	1	できていない又は計画的でない	○	0		・収集すべきログ/イベントの例：システム内で起こった特定の現象・動作を記録するイベントログ、セキュリティ機器が出すアラート等のログ ・ログ収集・分析ツールとはSIEM（Security Information and Event Management）等のこと 参考：情報セキュリティサービス審査登録制度（セキュリティ監視・運用サービス） https://www.ipa.go.jp/files/000067320.pdf
					2	イベント（ログ）収集の仕組みとプロセスがある	○			
					3	収集したログを分析し、異常を検知する仕組みとプロセスがある	○			
					4	検知したものの確認をする仕組みとプロセスがある	○			
					5	運用が継続的に見直されている	○			
		21	5-8	サイバー攻撃を検知した際に不正通信を遮断する等のインシデント対応の仕組みを導入している	1	できていない	○	0		・「その都度実施」の例：マルウェア感染が疑われる時、PCからLANケーブルを抜く ・ツールの例：EDRで端末・サーバ内の不審なプロセスを止める、サンドボックスでマルウェアを解析してWebやメールのフィルタリングをする
					2	その都度実施している	○			
					3	標準化された対応方針がある	○			
					4	ツールを使って自動化されている	○			
					5	運用が継続的に見直されている	○			
		22	5-9	インシデントの管理の仕組みを導入している	1	できていない	○	0		・インシデント管理の例：インシデント管理ツールにアラートの内容を登録してチケット発行、対応優先度の決定と担当者のアサイン、対応状況のフォロー、クロージングまでの管理 ・「人手で管理する仕組み」の例：Excelの所定のフォーマットに手作業で入力・更新
					2	その都度実施されている	○			
					3	人手で管理する仕組みが導入されている	○			
					4	ツールを使う仕組みが導入されている	○			
					5	運用が継続的に見直されている	○			
		23	5-10	従業員に対して、サイバーセキュリティの教育・演習を実施している	1	できていない又は計画的でない	○	0		・教育の例：EラーニングによるWeb教育 ・演習の例：「怪しいメールが来た」「添付ファイルを開いてしまった」等と当事者から報告させることを含む標的型攻撃メール訓練 ・演習の例は指示7-5、8-2の備考を参照
					2	教育・演習計画を策定している	○			
					3	計画に基づき教育が実施されている	○			
					4	計画に基づき演習が実施されている	○			
					5	教育・演習計画や実施内容を見直し、継続的に改善されている	○			
6	指示6：サイバーセキュリティ対策におけるPDCAサイクルの実施	24	6-1	サイバーセキュリティ運用管理に関するKPIを定めている	1	できていない又は計画的でない	○	0	0.00	・KPIの例：リスク分析での指摘事項数、組織内のセキュリティ教育の受講状況、インシデントの発生数、アセスメント実施状況、脆弱性対策状況
					2	KPIが文書化されている	○			
					3	KPIが測定されている	○			
					4	KPIの測定結果が定期的に評価されている	○			
					5	KPIが継続的に見直されている	○			
		25	6-2	経営者が定期的に、サイバーセキュリティ運用に関する報告を受け、認識対策を指示している	1	できていない又は計画的でない	○	0		・報告の仕方の例：経営会議の議題にサイバーセキュリティに関するKPIの報告が含まれている ・報告事項の例：KPI、インシデント、予算執行、重大ニュース ・報告の仕方の改善例：経営層の望む情報・指標等を新たに作って盛り込む
					2	インシデントなどの突発事象のみ報告されている	○			
					3	セキュリティ運用全般について報告されている	○			
					4	セキュリティ運用全般について報告され対策を指示している	○			
					5	報告ルールや対策の方法が継続的に改善されている	○			
		26	6-3	サイバーセキュリティにかかる内部監査、外部監査を踏まえ、サイバーセキュリティ対策を適時見直している	1	できていない又は計画的でない	○	0		・例： －毎年の監査計画が定められ、文書化されている －監査結果を受けてセキュリティ方針・対策の見直しを企画し、経営会議等に報告されている ・参考：情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス） https://www.ipa.go.jp/files/000067317.pdf
					2	監査と対策見直しの方針が文書化されている	○			
					3	方針に従って監査が実施されている	○			
					4	監査結果が評価され、対応されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		27	6-4	サイバーセキュリティリスクや取組状況をステークホルダーに情報公開している	1	できていない又は計画的でない	○	0		・例：情報セキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等を通して情報公開する
					2	情報公開の方針が文書化されている	○			
					3	方針に則って情報公開がされている	○			
					4	方針や情報公開の内容が定期的に評価されている	○			
					5	方針や内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール				備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
7 指示7：インシデント発生時の緊急対応体制の整備	28	7-1	インシデント対応計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －初動対応マニュアルの整備等 －組織内における緊急連絡先・伝達ルートの整備 ・緊急連絡先・伝達ルートの例：緊急連絡網、報告先一覧（上司、CSIRT、広報部門、法務部門、経営者等）
				2	計画が文書化されている	○			
				3	計画が周知されている	○			
				4	計画が定期的に評価されている	○			
				5	計画が継続的に改善されている	○			
	29	7-2	インシデント対応の専門チーム（CSIRT等）を設置している	1	できていない又は計画的でない	○	0		・CSIRT：Computer Security Incident Response Team ・参考：「組織内CSIRT構築の参考資料 インシデント対応マニュアルの作成について」（JPCERT/CC）
				2	チームの構成等が文書化されている	○			
				3	専門チームが設置され、要員が割り当てられている	○			
				4	活動状況が定期的に評価されている	○			
				5	体制や活動内容が継続的に改善されている	○			
	30	7-3	組織外に報告・公表すべき内容やタイミングを定めている	1	できていない又は計画的でない	○	0		・組織外の例：取引先、JPCERT/CC、IPA、所管省庁、マスコミ ・広報部門等とも連携し、公表する／しない項目、公表の仕方等を文書化し、関係部門に周知している ・「文書の内容に対する取組み」の例：CISO等が報告ルート、公表すべき内容を、関係者に周知している ・不特定多数のサプライチェーン関係者へ影響が懸念される場合など、広く対策を促す必要がある場合もあるため、公表のメリット・デメリットを十分に検討した上で、適切と判断される場合には、公表を行うことが望ましい。
				2	報告ルート、公表すべき内容などが文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			
	31	7-4	インシデント発生時の緊急対応の演習を定期的に行っている	1	できていない又は計画的でない	○	0		・演習の例： －マルウェア感染が疑われる端末での初期対処方法の確認 －フォレンジック対応のログを残す手順の確認 －社内関係者への連絡手順の確認 －所管省庁等への報告手順の確認
				2	演習の方針、内容が文書化されている	○			
				3	方針に則って演習が実施されている	○			
				4	演習の内容と結果が演習実施の度に評価されている	○			
				5	方針や実施内容が継続的に見直されている	○			
	32	7-5	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している	1	できていない又は計画的でない	○	0		・例： －インシデントに関連するログを速やかに分析できるシステムを整備している －インシデント対応手順にフォレンジック対応の項目を入れている －フォレンジック専業の事業者と契約している 参考：情報セキュリティサービス審査登録制度（デジタルフォレンジックサービス） https://www.ipa.go.jp/files/000067319.pdf
				2	ログ分析・調査の方針と内容が文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
8	指示8：インシデントによる被害に備えた復旧体制の整備	33	8-1	被害が発生した際に備えた業務の復旧計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －BCPとの連携等、組織全体として整合のとれた復旧目標計画 －システム復旧マニュアルの整備 －業務復旧マニュアルの中に重大インシデントが起きた時のおおまかな業務復旧手順やシステム復旧手順を記述 －組織の内外における連絡先・伝達ルートの整備 ・連絡先の例：経営者層、JPCERT/CC、インターネットサービスプロバイダ、自社システムへの攻撃の踏み台にされたシステムのオーナー、他組織のCSIRT、ベンダー
					2	計画が文書化されている	○			
					3	計画が周知されている	○			
					4	計画が定期的に評価されている	○			
					5	計画が継続的に改善されている	○			
		34	8-2	定期的に復旧対応演習を行っている	1	できていない又は計画的でない	○	0		・年間の演習計画の策定 ・演習の例： －マルウェア感染端末のクリアインストール・再設定 －安全が確認されたシステムから順次復旧 －社内関係者への報告手順の確認 －上記のTTX（机上演習）、実機演習等
					2	演習の方針、内容が文書化されている	○			
					3	方針に則って演習が実施されている	○			
					4	演習の内容と結果が演習実施の度に評価されている	○			
					5	方針や実施内容が継続的に見直されている	○			
9	指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	35	9-1	グループ企業に関するリスク分析を行い、対策をグループ内の規程等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0	0.00	・例：本可視化ツールを用いてグループ企業から報告を受ける 参考：グループ・ガバナンス・システムに関する実務指針 https://www.meti.go.jp/press/2019/06/20190628003/20190628003.html ・文書の例：グループ内のサイバーセキュリティ基本方針や対策の規程、親会社から子会社へのセキュリティ対策実施指示 ・グループ経営会議の議題にサイバーセキュリティも含まれている ・親会社の情報システム部門が子会社のセキュリティ対策状況を定期的に調査、指導している 等
					2	グループ企業に関するリスク分析が一部実施されている	○			
					3	グループ企業に関するリスク分析が実施されている	○			
					4	グループ企業間でリスク分析結果を共有し対策を検討している	○			
					5	グループ企業でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		36	9-2	委託先等の取引先に関するリスク分析を行い、対策を契約書等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0		・例： －本可視化ツールを用いて委託先から報告を受ける －委託元の情報システム部門が委託先のセキュリティ対策状況をアンケート、立ち入り等の手法で調査、指導している ・文書の例：契約書、仕様書や品質保証文書
					2	委託先等の取引先に関するリスク分析が一部実施されている	○			
					3	委託先等の取引先に関するリスク分析が実施されている	○			
					4	委託先等の取引先関係企業間でリスク分析結果が共有され対策が検討されている	○			
					5	委託先等の取引先でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		37	9-3	サプライチェーン全体を俯瞰した関連組織全体で、リスク分析を行い対策状況の検討を行っている。	1	できていない又は計画的でない	○	0		
					2	事業毎のサプライチェーン全体が把握されている	○			
					3	サプライチェーン全体でのリスク分析が行われいる	○			
					4	サプライチェーン全体の関係企業間でリスク分析結果を共有し対策が検討されている	○			
					5	サプライチェーン全体でのリスク対策が評価され、実施内容が継続的に見直されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
10	指示10：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	38	10-1	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通じて情報共有を行い、自社の対策に活かしている	1	できていない又は計画的でない	○	0	0.00	・関係団体の例：NISC、関係省庁、IPA、JPCERT/CC、日本シーサート協議会、各種ISAC（Information Sharing and Analysis Center） ・業界横断的に広く再発防止策を共有するために、IPAサイバー情報共有イニシアティブ（J-CSIP）、NISCセプターカウンシル、サイバーセキュリティ協議会等に加盟することも考えられる。
					2	不定期に参加して情報入手している	○			
					3	計画して参加し情報共有している	○			
					4	情報共有の内容と効果を定期的に評価している	○			
					5	情報共有の方法を継続的に改善している	○			
		39	10-2	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティに情報提供や相談を実施している	1	できていない又は計画的でない	○	0		・標的型攻撃においては、攻撃者がターゲットとする情報を入手するために、特定企業のみならず、その取引先に対しても同様の手口で攻撃を行う傾向がある。そのため、委託先等の取引先に迅速に情報共有することが望ましい。 ・ 初動対応において技術的助言を必要とする場合には、自社のシステム調達に関わっているシステムベンダやセキュリティベンダ等のほか、IPA J-CRAT 、JPCERT/CC へ相談することが有効。 ・ 既にISACが組織化されている業界においては、ISACの枠組みにおいて情報共有することも考えられる。
					2	情報提供の方針が文書化されている	○			
					3	文書の内容が実施されている	○			
					4	情報提供の内容と効果が定期的に評価されている	○			
					5	文書や実施内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
1	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	1	1-1	経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している	1	認識していない又は部分的である	○	0	0.00	・経営会議の例：取締役会等、経営者が出席する会議
					2	認識しているが、文書化等はできていない	○			
					3	認識しており、文書化されているが、対策は部下に任せている	○			
					4	認識しており、定期的に経営会議等で議論している	○			
					5	認識しており、経営会議等での議論を踏まえて継続的に改善している	○			
		2	1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している	1	できていない又は部分的である	○	0		・基本方針はセキュリティポリシーと同義
					2	方針内容が規程化されている	○			
					3	規程の内容が実施されている	○			
					4	実施内容が定期的に監査されている	○			
					5	規程や実施内容が継続的に改善されている	○			
		3	1-3	法令・契約やガイドライン等の要求事項を把握し、対応している	1	できていない又は部分的である	○	0		・法令についてはサイバーセキュリティ関係法令Q&Aハンドブック（NISC）を参照。ガイドラインについては同ハンドブックの付録１を参照。 https://www.nisc.go.jp/security-site/law_handbook/index.html ・海外拠点については各国の法令・ガイドラインも確認すること。
					2	把握し、文書化されている	○			
					3	要求事項の内容が対応されている	○			
					4	要求事項が定期的に見直されている	○			
					5	要求事項やその対応が継続的に改善されている	○			
2	指示2：サイバーセキュリティリスク管理体制の構築	4	2-1	組織の基本方針に基づき、CISO等からなるサイバーセキュリティリスク管理体制を構築している	1	できていない又は部分的である	○	0	0.00	・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	管理体制の組織図があり、周知されている	○			
					3	体制に適切なリソースが割り当てられている	○			
					4	体制の運営状況が定期的に評価されている	○			
					5	文書や管理体制の運営状況が継続的に改善されている	○			
		5	2-2	セキュリティリスク管理体制において、各関係者の役割と責任を明確にしている	1	できていない又は部分的である	○	0		・「部分的」の例：CISOのみ決まっている ・サイバーセキュリティリスク管理体制の例：セキュリティ委員会の設置、CISOの任命、内部監査責任者の任命、情報セキュリティ管理責任者の任命
					2	役割と責任が文書化されている	○			
					3	役割と責任が周知されている	○			
					4	役割と責任が定期的に評価されている	○			
					5	役割と責任が継続的に再定義されている	○			
		6	2-3	組織内のリスク管理体制（リスク委員会等）とサイバーセキュリティリスク管理体制（セキュリティ委員会等）の関係を明確にしている	1	サイバーセキュリティリスク管理体制がない又は部分的である	○	0		・サイバーセキュリティリスク管理体制の例：セキュリティ統括室、セキュリティ委員会 ・関係明確化を確認する方法の例： - サイバーセキュリティリスク管理に関する役割分担表等による相違点の確認 - 経営者や従業員への聞き取り調査 ・サイバーセキュリティリスク管理体制とリスク管理体制が独立しているということは、サイバーセキュリティリスクを他の事業リスクとは分けて、独立して管理する体制が構築されている。ただし、人員の重複などはありえる、ということ ・あるべき姿の例：組織内のリスク管理体制とサイバーセキュリティリスク管理体制を分離し、両者の関係を明確に規定し、実施内容が継続的に改善されている ・両者の連携の例：一方のメンバーが他方の会議にオブザーバ参加する、定期的に連絡会議を開催する、主な会議の議事録を共有する等
					2	両者の関係が明確にされていない	○			
					3	サイバーセキュリティリスク管理体制はリスク管理体制の一部として存在している	○			
					4	両者の関係が独立している	○			
					5	両者の関係が独立しており、必要な連携が行われている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改				可視化ツール					備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
3 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	7	3-1	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている	1	できていない又は計画的でない	○	0	0.00	・対策の例：セキュリティ対策製品の導入、運用プロセスの見直し、人員増強
				2	対策及び資源が文書化されている	○			
				3	対策及び資源が周知されている	○			
				4	対策及び資源が定期的に評価されている	○			
				5	対策及び資源が継続的に改善されている	○			
	8	3-2	自組織で対応する部分と外部に委託する部分を適切に切り分けている	1	できていない又は計画的でない	○	0		・具体的な対策、緊急時対応等の項目の明文化と、それらのうちどこを自社で行いどこから外部に委託するかの方針 ・「おおよその切り分け」の例：システムの企画は自組織、設計・開発・運用は外部 ・具体的な切り分けの例： - 対策　対応組織 ー－－－－－－－－－－－－－－－－－－－ 資産管理：　自組織 ID管理：　自組織 アクセス制御：　自組織 監視/ログ収集：　外部 異常検知：　外部 インシデントレスポンス：　自組織 フォレンジック：　外部
				2	おおよその切り分け方針ができている	○			
				3	具体的な領域、技術等で切り分けができている	○			
				4	切り分けが定期的に評価されている	○			
				5	切り分けが継続的に改善されている	○			
	9	3-3	自組織に求められる体制を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を検討している	1	できていない又は計画的でない	○	0		・人材確保のための活動の例：採用、育成（キャリアパスの設計を含む）、評価 ・あるべき姿の例： －育成・採用の方針を明らかにする －内部で育成するべきスキルと外部から調達するべきスキルを明らかにする －採用計画または育成計画を作成する
				2	人材が確保されているが育成が計画的でない	○			
				3	人材が計画的に確保、育成されている	○			
				4	人材が計画的に確保、育成され処遇にも反映されている	○			
				5	計画とその実施内容が継続的に改善されている	○			
	10	3-4	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している	1	できていない又は計画的でない	○	0		・外部リソースの例：セキュリティベンダ、外部人材、クラウドサービス ・情報セキュリティサービス審査登録制度等の活用 https://www.ipa.go.jp/security/it-service/service_list.html
				2	外部リソースの活用方針が文書化されている	○			
				3	方針に従って外部リソースが活用されている	○			
				4	活用状況が定期的に評価されている	○			
				5	方針や実施状況が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢	回答欄（該当する箇所を選択）	スコア	平均		
4	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	11	4-1	守るべきIT資産（情報資産やシステム）を特定し、当該資産の場所やビジネス上の価値等に基づいて優先順位付けを行っている	1	できていない又は計画的でない	○	0	0.00	・IT資産の分類・管理の規程を定める ・情報管理規程で管理レベル高である情報を洗い出し、守るべき情報を経営者やCISOと合意する
					2	IT資産の情報が人手で収集されている	○			
					3	IT資産の価値が評価され優先順位がつけられている	○			
					4	守るべきIT資産について、経営者やCISOと合意している	○			
					5	IT資産が自動的に収集され、資産価値が定期的に見直されている	○			
		12	4-2	特定した守るべきIT資産に対するサイバー攻撃の脅威、脆弱性を、脅威情報のデータベース等を用いて認識し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している	1	できていない又は計画的でない	○	0		・サイバーセキュリティリスクが自社の事業に及ぼす影響については、CISOや経営者も認識していることを確認する ・サイバー攻撃の脅威、脆弱性の認識とは、同業他社や取引先へのサイバー攻撃の動向や事例を把握すること、自組織が使っているシステムで報告されている脆弱性を把握すること等 ・脅威情報のデータベースとは脅威インテリジェンスのことで、公開情報の他、それらを提供するベンダーの活用も含む ・自社事業への影響の例：顧客の個人情報が漏洩して多額の賠償、委託元の機密情報が漏えいして取引停止、ランサムウェアで工場が停止
					2	サイバー攻撃の脅威、脆弱性の情報を恒常的に収集されている	○			
					3	脅威、脆弱性情報について、自社の事業に与える影響が評価されている	○			
					4	自社の事業に与える影響が大きい脅威、脆弱性情報について優先的に対応されている	○			
					5	脅威、脆弱性情報による評価、対応の仕組みが継続的に改善されている	○			
		13	4-3	サイバーセキュリティリスクの影響の度合いに従ってリスク対応計画を策定している	1	できていない又は計画的でない	○	0		リスク対応策の例：重要な情報へのアクセス制御、ソフトウェア更新の徹底、端末の持ち出し禁止、クラウドサービスの利用、サイバー保険の加入
					2	サイバーセキュリティリスクの影響度合いが組織的に評価されている	○			
					3	評価結果に基づき、対応計画が策定され実施されている	○			
					4	対応の実施結果が評価されている	○			
					5	サイバーセキュリティリスク評価のＰＤＣＡサイクルが改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改				可視化ツール					備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
5	指示5：サイバーセキュリティリスクに対応するための仕組みの構築	14	5-1	情報システムのIT資産管理・構成管理・パッチ管理を行っている	1	できていない又は計画的でない	○	0	0.00	・「人手で実施」の例：IT資産を目視で確認し、Excelの台帳に手入力で入力・更新すること ・検知したものの確認の例： －古いバージョンのソフトウェアがシステム内に見つかったらバージョンアップする －自社が使用しているソフトウェアを把握しておき、ベンダーからパッチが提供されたらパッチ適用する
					2	人手で管理されている	○			
					3	ツールを使って管理されている	○			
					4	検知したものが確認されている	○			
					5	運用が継続的に見直されている	○			
		15	5-2	組織内でシャドーITを利用させない対策を行っている	1	ルールが定められていない	○	0		・シャドーITとは、情報システム部門の許可を得ずに、従業員又は部門が業務に利用しているデバイスやクラウドサービス ・デバイスの例：従業員私物のスマホやタブレット ・「人手で実施」の例：「情報システム部が認めたクラウドサービス以外のサービスを業務で利用しないこと」等の規程を定め、社員にメール等で周知すること
					2	ルールが定められている	○			
					3	ルールに基づく利用申告等が実施されている	○			
					4	ルール違反の検知と対応を行っている	○			
					5	運用が継続的に見直されている	○			
		16	5-3	システム設計時にリスク分析を行い、必要なセキュリティ機能を具体化し、開発時に実装している	1	できていない又は計画的でない	○	0		・プロセスの例：セキュアシステム開発方法論等の中で、システム設計の規約、コーディングの規約、脆弱性診断の規約、次工程へ進むための判断基準等が定められている ・実装の例： －システムの運用に必要でないポート、プロトコル、サービス等を無効化すること －SQLインジェクション等の攻撃に使われるセキュリティホールが発生しないようにコーディングすること －リリース前に脆弱性診断を実施
					2	セキュア開発のプロセスが文書化・周知されている	○			
					3	文書の内容が実施されている	○			
					4	文書や実施内容が定期的に評価されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		17	5-4	重要業務を行う端末・サーバ等には複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・端末・サーバ等の例：PC、サーバ、複合機、ネットワークカメラ、テレワーク端末等 ・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		18	5-5	重要業務を行うネットワークには複数の技術的防御策を実施している	1	できていない又は部分的である	○	0		・「複数の対策」の例： －初期潜入(マルウェア感染等）対策 －基盤構築及び内部侵入・調査（バックドア開設、サーバへの侵入等）対策 －目的遂行（データ持出し等）対策 なお、具体的な対策は自社のシステム構成やセキュリティ要件、予算等に応じて適切なものを選択し、適用する。
					2	複数の対策について計画がある	○			
					3	計画に基づき対策が実施されている	○			
					4	計画に基づき対策が見直されている	○			
					5	運用が継続的に改善されている	○			
		19	5-6	システム等に対する定期的な脆弱性診断や、継続的なバッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している	1	実行できていない	○	0		・脆弱性診断の例：プラットフォーム診断、Webアプリケーション診断等 参考：情報セキュリティサービス審査登録制度（脆弱性診断サービス） https://www.ipa.go.jp/files/000067318.pdf ・脆弱性への対処の例：セキュリティパッチ適用、WAF導入
					2	実行されているが計画的ではない	○			
					3	計画が立てられており、部分的に実行されている	○			
					4	計画通りに実行されている	○			
					5	計画が継続的に見直されている	○			

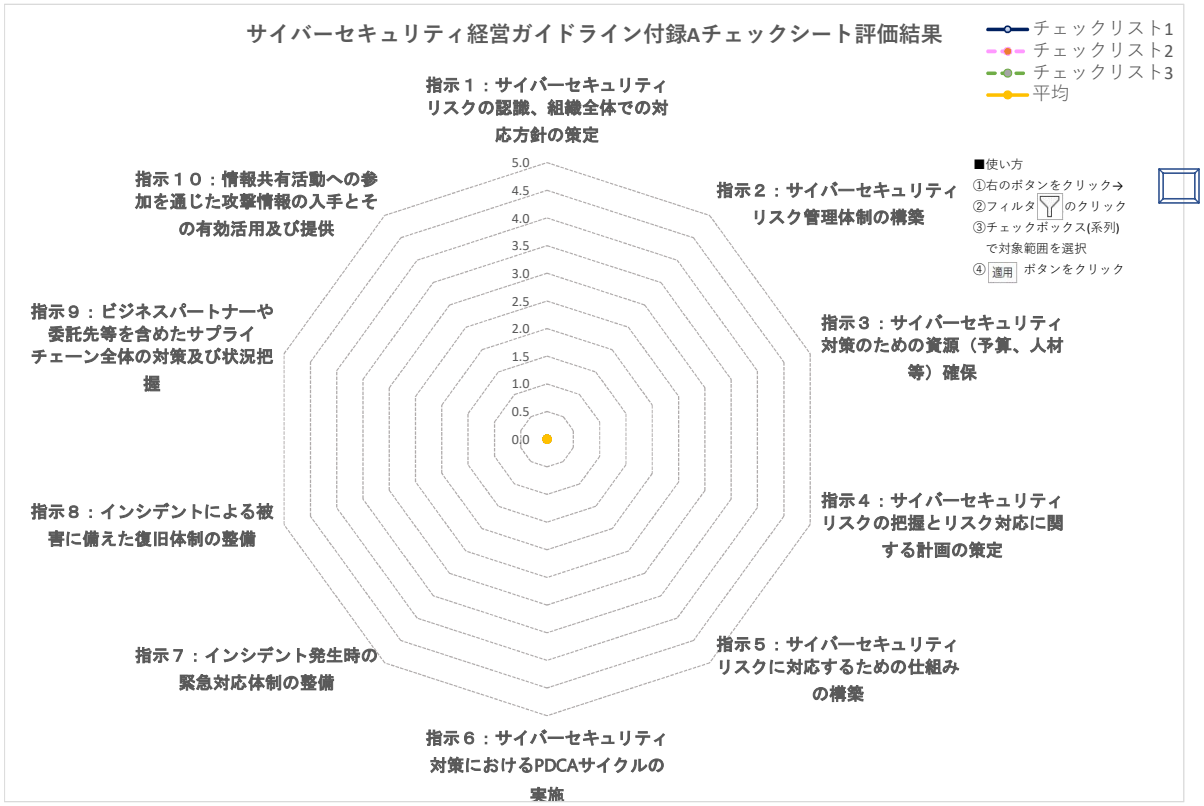
サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目		選択肢		回答欄（該当する箇所を選択）	スコア	平均	
		20	5-7	端末やネットワークからのログを収集・分析している。	1	できていない又は計画的でない	○	0		・収集すべきログ/イベントの例：システム内で起こった特定の現象・動作を記録するイベントログ、セキュリティ機器が出すアラート等のログ ・ログ収集・分析ツールとはSIEM（Security Information and Event Management）等のこと 参考：情報セキュリティサービス審査登録制度（セキュリティ監視・運用サービス） https://www.ipa.go.jp/files/000067320.pdf
					2	イベント（ログ）収集の仕組みとプロセスがある	○			
					3	収集したログを分析し、異常を検知する仕組みとプロセスがある	○			
					4	検知したものの確認をする仕組みとプロセスがある	○			
					5	運用が継続的に見直されている	○			
		21	5-8	サイバー攻撃を検知した際に不正通信を遮断する等のインシデント対応の仕組みを導入している	1	できていない	○	0		・「その都度実施」の例：マルウェア感染が疑われる時、PCからLANケーブルを抜く ・ツールの例：EDRで端末・サーバ内の不審なプロセスを止める、サンドボックスでマルウェアを解析してWebやメールのフィルタリングをする
					2	その都度実施している	○			
					3	標準化された対応方針がある	○			
					4	ツールを使って自動化されている	○			
					5	運用が継続的に見直されている	○			
		22	5-9	インシデントの管理の仕組みを導入している	1	できていない	○	0		・インシデント管理の例：インシデント管理ツールにアラートの内容を登録してチケット発行、対応優先度の決定と担当者のアサイン、対応状況のフォロー、クロージングまでの管理 ・「人手で管理する仕組み」の例：Excelの所定のフォーマットに手作業で入力・更新
					2	その都度実施されている	○			
					3	人手で管理する仕組みが導入されている	○			
					4	ツールを使う仕組みが導入されている	○			
					5	運用が継続的に見直されている	○			
		23	5-10	従業員に対して、サイバーセキュリティの教育・演習を実施している	1	できていない又は計画的でない	○	0		・教育の例：EラーニングによるWeb教育 ・演習の例：「怪しいメールが来た」「添付ファイルを開いてしまった」等と当事者から報告させることを含む標的型攻撃メール訓練 ・演習の例は指示7-5、8-2の備考を参照
					2	教育・演習計画を策定している	○			
					3	計画に基づき教育が実施されている	○			
					4	計画に基づき演習が実施されている	○			
					5	教育・演習計画や実施内容を見直し、継続的に改善されている	○			
6	指示6：サイバーセキュリティ対策におけるPDCAサイクルの実施	24	6-1	サイバーセキュリティ運用管理に関するKPIを定めている	1	できていない又は計画的でない	○	0	0.00	・KPIの例：リスク分析での指摘事項数、組織内のセキュリティ教育の受講状況、インシデントの発生数、アセスメント実施状況、脆弱性対策状況
					2	KPIが文書化されている	○			
					3	KPIが測定されている	○			
					4	KPIの測定結果が定期的に評価されている	○			
					5	KPIが継続的に見直されている	○			
		25	6-2	経営者が定期的に、サイバーセキュリティ運用に関する報告を受け、認識対策を指示している	1	できていない又は計画的でない	○	0		・報告の仕方の例：経営会議の議題にサイバーセキュリティに関するKPIの報告が含まれている ・報告事項の例：KPI、インシデント、予算執行、重大ニュース ・報告の仕方の改善例：経営層の望む情報・指標等を新たに作って盛り込む
					2	インシデントなどの突発事象のみ報告されている	○			
					3	セキュリティ運用全般について報告されている	○			
					4	セキュリティ運用全般について報告され対策を指示している	○			
					5	報告ルールや対策の方法が継続的に改善されている	○			
		26	6-3	サイバーセキュリティにかかる内部監査、外部監査を踏まえ、サイバーセキュリティ対策を適時見直している	1	できていない又は計画的でない	○	0		・例： －毎年の監査計画が定められ、文書化されている －監査結果を受けてセキュリティ方針・対策の見直しを企画し、経営会議等に報告されている ・参考：情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス） https://www.ipa.go.jp/files/000067317.pdf
					2	監査と対策見直しの方針が文書化されている	○			
					3	方針に従って監査が実施されている	○			
					4	監査結果が評価され、対応されている	○			
					5	文書や実施内容が継続的に改善されている	○			
		27	6-4	サイバーセキュリティリスクや取組状況をステークホルダーに情報公開している	1	できていない又は計画的でない	○	0		・例：情報セキュリティ報告書、CSR報告書、サステナビリティレポートや有価証券報告書等を通して情報公開する
					2	情報公開の方針が文書化されている	○			
					3	方針に則って情報公開がされている	○			
					4	方針や情報公開の内容が定期的に評価されている	○			
					5	方針や内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール				備考
指示		付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
7 指示7：インシデント発生時の緊急対応体制の整備	28	7-1	インシデント対応計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －初動対応マニュアルの整備等 －組織内における緊急連絡先・伝達ルートの整備 ・緊急連絡先・伝達ルートの例：緊急連絡網、報告先一覧（上司、CSIRT、広報部門、法務部門、経営者等）
				2	計画が文書化されている	○			
				3	計画が周知されている	○			
				4	計画が定期的に評価されている	○			
				5	計画が継続的に改善されている	○			
	29	7-2	インシデント対応の専門チーム（CSIRT等）を設置している	1	できていない又は計画的でない	○	0		・CSIRT：Computer Security Incident Response Team ・参考：「組織内CSIRT構築の参考資料 インシデント対応マニュアルの作成について」（JPCERT/CC）
				2	チームの構成等が文書化されている	○			
				3	専門チームが設置され、要員が割り当てられている	○			
				4	活動状況が定期的に評価されている	○			
				5	体制や活動内容が継続的に改善されている	○			
	30	7-3	組織外に報告・公表すべき内容やタイミングを定めている	1	できていない又は計画的でない	○	0		・組織外の例：取引先、JPCERT/CC、IPA、所管省庁、マスコミ ・広報部門等とも連携し、公表する／しない項目、公表の仕方等を文書化し、関係部門に周知している ・「文書の内容に対する取組み」の例：CISO等が報告ルート、公表すべき内容を、関係者に周知している ・不特定多数のサプライチェーン関係者へ影響が懸念される場合など、広く対策を促す必要がある場合もあるため、公表のメリット・デメリットを十分に検討した上で、適切と判断される場合には、公表を行うことが望ましい。
				2	報告ルート、公表すべき内容などが文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			
	31	7-4	インシデント発生時の緊急対応の演習を定期的に行っている	1	できていない又は計画的でない	○	0		・演習の例： －マルウェア感染が疑われる端末での初期対処方法の確認 －フォレンジック対応のログを残す手順の確認 －社内関係者への連絡手順の確認 －所管省庁等への報告手順の確認
				2	演習の方針、内容が文書化されている	○			
				3	方針に則って演習が実施されている	○			
				4	演習の内容と結果が演習実施の度に評価されている	○			
				5	方針や実施内容が継続的に見直されている	○			
	32	7-5	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している	1	できていない又は計画的でない	○	0		・例： －インシデントに関連するログを速やかに分析できるシステムを整備している －インシデント対応手順にフォレンジック対応の項目を入れている －フォレンジック専業の事業者と契約している 参考：情報セキュリティサービス審査登録制度（デジタルフォレンジックサービス） https://www.ipa.go.jp/files/000067319.pdf
				2	ログ分析・調査の方針と内容が文書化されている	○			
				3	文書の内容に対する取組みが実施されている	○			
				4	文書の内容が定期的に評価されている	○			
				5	文書や実施内容が継続的に改善されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール					備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均	
8	指示8：インシデントによる被害に備えた復旧体制の整備	33	8-1	被害が発生した際に備えた業務の復旧計画を策定している	1	できていない又は部分的である	○	0	0.00	・例： －BCPとの連携等、組織全体として整合のとれた復旧目標計画 －システム復旧マニュアルの整備 －業務復旧マニュアルの中に重大インシデントが起きた時のおおまかな業務復旧手順やシステム復旧手順を記述 －組織の内外における連絡先・伝達ルートの整備 ・連絡先の例：経営者層、JPCERT/CC、インターネットサービスプロバイダ、自社システムへの攻撃の踏み台にされたシステムのオーナー、他組織のCSIRT、ベンダー
					2	計画が文書化されている	○			
					3	計画が周知されている	○			
					4	計画が定期的に評価されている	○			
					5	計画が継続的に改善されている	○			
		34	8-2	定期的に復旧対応演習を行っている	1	できていない又は計画的でない	○	0		・年間の演習計画の策定 ・演習の例： －マルウェア感染端末のクリアインストール・再設定 －安全が確認されたシステムから順次復旧 －社内関係者への報告手順の確認 －上記のTTX（机上演習）、実機演習等
					2	演習の方針、内容が文書化されている	○			
					3	方針に則って演習が実施されている	○			
					4	演習の内容と結果が演習実施の度に評価されている	○			
					5	方針や実施内容が継続的に見直されている	○			
9	指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	35	9-1	グループ企業に関するリスク分析を行い、対策をグループ内の規程等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0	0.00	・例：本可視化ツールを用いてグループ企業から報告を受ける 参考：グループ・ガバナンス・システムに関する実務指針 https://www.meti.go.jp/press/2019/06/20190628003/20190628003.html ・文書の例：グループ内のサイバーセキュリティ基本方針や対策の規程、親会社から子会社へのセキュリティ対策実施指示 ・グループ経営会議の議題にサイバーセキュリティも含まれている ・親会社の情報システム部門が子会社のセキュリティ対策状況を定期的に調査、指導している 等
					2	グループ企業に関するリスク分析が一部実施されている	○			
					3	グループ企業に関するリスク分析が実施されている	○			
					4	グループ企業間でリスク分析結果を共有し対策を検討している	○			
					5	グループ企業でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		36	9-2	委託先等の取引先に関するリスク分析を行い、対策を契約書等で明確にし、対策状況の報告を受け、適時見直している	1	できていない又は計画的でない	○	0		・例： －本可視化ツールを用いて委託先から報告を受ける －委託元の情報システム部門が委託先のセキュリティ対策状況をアンケート、立ち入り等の手法で調査、指導している ・文書の例：契約書、仕様書や品質保証文書
					2	委託先等の取引先に関するリスク分析が一部実施されている	○			
					3	委託先等の取引先に関するリスク分析が実施されている	○			
					4	委託先等の取引先関係企業間でリスク分析結果が共有され対策が検討されている	○			
					5	委託先等の取引先でのリスク対策が評価され、実施内容が継続的に見直されている	○			
		37	9-3	サプライチェーン全体を俯瞰した関連組織全体で、リスク分析を行い対策状況の検討を行っている。	1	できていない又は計画的でない	○	0		
					2	事業毎のサプライチェーン全体が把握されている	○			
					3	サプライチェーン全体でのリスク分析が行われいる	○			
					4	サプライチェーン全体の関係企業間でリスク分析結果を共有し対策が検討されている	○			
					5	サプライチェーン全体でのリスク対策が評価され、実施内容が継続的に見直されている	○			

サイバーセキュリティ経営ガイドライン Ver 2.0改					可視化ツール						備考
指示			付録Aのチェック項目			選択肢	回答欄（該当する箇所を選択）	スコア	平均		
10	指示10：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	38	10-1	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通して情報共有を行い、自社の対策に活かしている	1	できていない又は計画的でない	○	0	0.00		・関係団体の例：NISC、関係省庁、IPA、JPCERT/CC、日本シーサート協議会、各種ISAC（Information Sharing and Analysis Center） ・業界横断的に広く再発防止策を共有するために、IPAサイバー情報共有イニシアティブ（J-CSIP）、NISCセプターカウンシル、サイバーセキュリティ協議会等に加盟することも考えられる。
					2	不定期に参加して情報入手している	○				
					3	計画して参加し情報共有している	○				
					4	情報共有の内容と効果を定期的に評価している	○				
					5	情報共有の方法を継続的に改善している	○				
		39	10-2	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティに情報提供や相談を実施している	1	できていない又は計画的でない	○	0			・標的型攻撃においては、攻撃者がターゲットとする情報を入手するために、特定企業のみならず、その取引先に対しても同様の手口で攻撃を行う傾向がある。そのため、委託先等の取引先に迅速に情報共有することが望ましい。 ・ 初動対応において技術的助言を必要とする場合には、自社のシステム調達に関わっているシステムベンダやセキュリティベンダ等のほか、IPA J-CRAT 、JPCERT/CC へ相談することが有効。 ・ 既にISACが組織化されている業界においては、ISACの枠組みにおいて情報共有することも考えられる。
					2	情報提供の方針が文書化されている	○				
					3	文書の内容が実施されている	○				
					4	情報提供の内容と効果が定期的に評価されている	○				
					5	文書や実施内容が継続的に改善されている	○				

サイバーセキュリティ経営チェックシートの項目	チェックリスト1	チェックリスト2	チェックリスト3	平均
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	0.0	0.0	0.0	0.0
指示２：サイバーセキュリティリスク管理体制の構築	0.0	0.0	0.0	0.0
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	0.0	0.0	0.0	0.0
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	0.0	0.0	0.0	0.0
指示５：サイバーセキュリティリスクに対応するための仕組みの構築	0.0	0.0	0.0	0.0
指示６：サイバーセキュリティ対策におけるPDCAサイクルの実施	0.0	0.0	0.0	0.0
指示７：インシデント発生時の緊急対応体制の整備	0.0	0.0	0.0	0.0
指示８：インシデントによる被害に備えた復旧体制の整備	0.0	0.0	0.0	0.0
指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	0.0	0.0	0.0	0.0
指示１０：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	0.0	0.0	0.0	0.0



サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版アンケート

よろしければ今後の改善を図るため、可視化ツールβ版に関するアンケートにご協力ください。＊は、必須項目となります。

業種＊

従業員数＊

Q1. 利用目的は？(いくつでも)

- ☐ 自社のセキュリティ対策強化
- ☐ 関連子会社のセキュリティ対策強化
- ☐ 取引先のセキュリティ対策強化
- ☐ 投資家等ステークホルダーとのコミュニケーション
- ☐ その他（よろしければ以下にご記入ください）

Q2. 使い方ガイドについてお気づきの点は？

例）

・説明がわかりにくい。例えば、〇行目の文は〇〇という意味か？

・〇〇に関する記述や注意も記載してほしい。

・もっと短くていい。〇〇の記述はなくてもいい。

Q3. チェックリストについてお気づきの点は？

例）
・全体的な把握にはチェック項目が足りない。〇〇に関するチェック項目も追加すべき。
・〇〇のチェック項目は不要。なぜなら・・・
・チェック項目の文が全体的に長く、回答時に読まなければならない量が多くて大変。もっと短くして、詳細は備考に回すなどしてほしい。
・チェック項目の文が全体的に短く、判断に迷うことが多い。多少長くなってもいいので、備考をできるだけ読まなくていいようにしてほしい。
・設問が偏っている。技術系の質問は減らすべき／増やすべき。
・チェック項目は詳細すぎ、より包括的なほうがよい。特に指示〇はもっと包括的でよい。／全体的に質問数を減らしてよい。

Q4. 5段階選択肢についてお気づきの点は？

例）
・概ね妥当である
・全体的に選択に迷うことが多い。〇〇のような聞き方の方が現実に即していて回答しやすい。
・プロセスの成熟度を聞く選択肢にできるだけしてほしい。(文書化しているか？等)
・プラクティスの成熟度を聞く選択肢にできるだけしてほしい。（〇〇の対策を導入しているか？等)
・〇〇の標準を参考にしてはどうか？

Q5. チェックリスト備考についてお気づきの点は？

例）
・全体的に回答するのに役に立った。
・プロセス関係の例がよくわからない。例えば、「文書化する」とはどんな文書にすればよいのかまで示してほしい。
・技術関係の例がよくわからない。例えば、「SIEM」等の専門用語の利用はできるだけ避けるか、補足説明を付けてほしい。
・例が多すぎる。特に技術系の対策は列挙するだけでなく、どこまでやればよいかも示してほしい。
・例が少なすぎる。特に技術系の対策はもっと列挙してほしい。

Q6. Q3.チェックリスト、Q4.選択肢、Q5.備考と同様の観点で指示ごとにお伺いします。
Q6-1. 特に経営ガイドライン指示1について、お気づきの点を以下にご記入下さい。

Q6-２. 特に経営ガイドライン指示２について、お気づきの点を以下にご記入下さい。

Q6-3. 特に経営ガイドライン指示3について、お気づきの点を以下にご記入下さい。

Q6-4. 特に経営ガイドライン指示4について、お気づきの点を以下にご記入下さい。

Q6-5. 特に経営ガイドライン指示5について、お気づきの点を以下にご記入下さい。

Q6-6. 特に経営ガイドライン指示6について、お気づきの点を以下にご記入下さい。

Q6-7. 特に経営ガイドライン指示7について、お気づきの点を以下にご記入下さい。

Q6-8. 特に経営ガイドライン指示8について、お気づきの点を以下にご記入下さい。

Q6-9. 特に経営ガイドライン指示9について、お気づきの点を以下にご記入下さい。

Q6-10. 特に経営ガイドライン指示10について、お気づきの点を以下にご記入下さい。

Q7．可視化ツールにほしい機能は？(いくつでも)

- □　自組織の過去のチェック結果との比較
- □　複数の組織間での比較
- □　業界の平均と自社との比較
- □　技術的な項目のより詳細なチェック
- □　可視化結果のレポート出力機能
- □　結果から推奨される対策の提示
- □　その他（よろしければ以下にご記入ください）

Q8. その他、ツールに関してご意見・ご感想があればお聞かせください。

どうもありがとうございました。アンケート記入結果をよろしければ
(**isec-csm-checktool@ipa.go.jp**)までご送付ください。ご回答内容につきまして、
内容確認のご連絡をする場合がございますので、ご了承ください。