【別紙】共通項を踏まえたチェックシート

カテゴリ	共通項として抽出されたチェック項目	チェックの視点	チェック
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	経営者のリスク認識	【第１段階】※達成していれば「○」 経営者がサイバーセキュリティリスクを認識している。 【第２段階】※達成していれば「◎」 認識したうえで、以下のような具体的な関与を行っている。 ①　経営者自身の責任の明確化。 ②　情報セキュリティの責任に関する方向性の検討。 ③　自社のセキュリティ基本方針等の承認の実施	
	経営者によるセキュリティポリシーの策定・宣言	【第１段階】※達成していれば「○」 セキュリティポリシーを策定し、宣言している。 【第２段階】※達成していれば「◎」 セキュリティポリシーに以下のような視点が含まれているか。 ①　情報セキュリティ対策を組織的に実施する意思を、従業員や関係者に明確に示すために、どのような情報をどのように守るかについて、自社に適した情報セキュリティに関する基本方針を定めている。 ②　自社の経営において最も懸念される事態は何かを明確にしている。	
	法律・業界ガイドラインの把握	【第１段階】※達成していれば「○」 法律・業界ガイドラインについて把握している。 【第２段階】※達成していれば「◎」 法律・業界ガイドライン把握するにあたり、以下のような前提・認識を有している。 ①　情報技術の進化の早さゆえに実施を検討するべき対策は目まぐるしく変化するため、自社だけで把握することは困難であることから、情報セキュリティに関する最新動向を発信している公的機関などを把握し、常時参照することで備えるように情報セキュリティ担当者に指示を行っている。 ②　知り合いやコミュニティへの参加を通じ情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有することとなっている。	
サイバーセキュリティリスク管理体制の構築	サイバーセキュリティリスク管理体制の構築	【第１段階】※達成していれば「○」 情報セキュリティ対策を推進する管理体制を定めている。 【第２段階】※達成していれば「◎」 以下のような管理体制が構築されている。	

		① 組織の対応方針（セキュリティポリシー）に基づいた 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されている。 ② 情報セキュリティ上の事故などが発生した場合も含め、情報セキュリティ責任者から部門責任者を通じた従業員への情報の伝達経路を確立している。 ③ 既存の個人情報保護管理体制（特定個人情報事務取扱担当者、個人情報苦情申出先）等の管理体制との整合が取れている。	
	関係者の役割と責任の明確化	【第１段階】※達成していれば「○」 情報セキュリティに関わる関係者の役割と責任を明確化している。 【第２段階】※達成していれば「◎」 以下のように、役割に応じた情報の伝達方法が確立している。 ① 関係者の選定にあたっては、法的な義務を順守し、システム運用を担うにあたり適当な能力を有する者を選定している。 ② 情報セキュリティ上の事故などが発生した場合に、情報セキュリティの責任者へ状況が迅速に報告されるような連絡体制を整備している。	
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	人材の確保、役割の理解	【第１段階】※達成していれば「○」 サイバーセキュリティを担う人材の確保に努めている。 【第２段階】※達成していれば「◎」 以下のような視点で人材確保を行っているか。 ① 複数の対策が必要という前提を持っている。 ② 実効性の観点から継続的な人材育成・配置を考慮している。 ③ 全社的なスキルアップに取り組んでいる。 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	経営戦略を踏まえたリスクの把握	【第１段階】※達成していれば「○」 経営戦略を踏まえたサイバーセキュリティリスクの把握を実施している。 【第２段階】※達成していれば「◎」 以下のような観点でリスクを把握しているか。 ① 重要度の高い情報資産を把握している。 ② 有事の際の影響の程度の把握を実施している。 ③ サイバーセキュリティに係る事案から派生して生じる事象の把握を実施している。	
	リスク対応計画の策定	【第１段階】※達成していれば「○」 リスクへの対応計画を策定している。 【第２段階】※達成していれば「◎」 以下のような観点が計画に含まれているか。 ① リスクに備えた対処準備。 ② リスク発生時の報告・連絡方法	

		③　復旧に要する目標時間	
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	重層端末への多層防御の実施	【第１段階】※達成していれば「○」 重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）に、多層防御を実施している。 【第２段階】※達成していれば「◎」 以下のような対策を追加で実施している。 ④　必要に応じてスイッチやファイアウォールなどでネットワークセグメントを分離し、別のポリシーで運用する。	
	脆弱性診断の実施・対応	【第１段階】※達成していれば「○」 システム等に対して脆弱性診断を実施し、検出された脆弱性に対処している。 【第２段階】※達成していれば「◎」 以下のような対策を追加で実施しているか。 ①　脆弱性に関する情報を継続的に収集・管理している。 ②　重要なシステムについて、アクセス制御を行ったうえ、脆弱性対策の実施体制を構築している。	
	検知すべきイベントの特定・迅速な検知のための体制構築	【第１段階】※達成していれば「○」 アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築している。 【第２段階】※達成していれば「◎」 以下のような対策を追加で実施している。 ①　検知すべきイベントを明確にし、アクセスログや通信ログから当該イベントが発生していないか、検知した場合には速やかに関係者にアラートを上げるなど適切な対処を行えるような体制を整える。 ②　監視に必要な専門的なスキル保持するため、自社でスキルを持った人材を確保・育成する、もしくは外部の監視サービスを活用している。	
	サイバーセキュリティリスクへの対応内容の見直し	【第１段階】※達成していれば「○」 サイバー攻撃の動向等を踏まえて、サイバーセキュリティリスクへの対応内容を見直している。 【第２段階】※達成していれば「◎」 以下のような対策を追加で実施しているか。 ①　不正接続・アクセス・操作を定期的に確認する仕組みが設けられている。 ②　セキュリティ対策の実施状況を定期的に点検し、セキュリティ管理責任者に報告している。 ③	
	従業員に対する教	【第１段階】※達成していれば「○」	

	育の実施	従業員に対するセキュリティ教育を計画し、実施している。 【第２段階】※達成していれば「◎」 以下のような項目を明記・実施しているか。 ①　情報セキュリティポリシー概要 ②　情報セキュリティの必要性 ③　企業・事業所におけるルール、手順 ④　情報セキュリティ事故の対応方法と再発防止策	
インシデント発生時の緊急対応体制の整備	初動対応マニュアルの整備	【第１段階】※達成していれば「○」 有事の際の初動対応マニュアルを整備している。 【第２段階】※達成していれば「◎」 以下のような項目を明記・実施しているか。 ①　対応のための作業フロー ②　対応が必要な職員・役職 ③　対応組織の立ち上げ方法 ④　情報共有方法	
インシデントによる被害に備えた復旧体制の整備	業務の復旧計画の策定	【第１段階】※達成していれば「○」 インシデント発生時の復旧計画（コンティンジェンシープラン）を策定している。 【第２段階】※達成していれば「◎」 インシデント発生時の復旧計画について、以下のような項目を明記・実施している。 ①　復旧ポイント ②　復旧目安時間 ③　復旧手順	
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	委託先に実施を求めるセキュリティ対策の明確化	【第１段階】※達成していれば「○」 委託先がどのような情報セキュリティ対策を行っているか確認している。 【第２段階】※達成していれば「◎」 以下のような対策を追加で実施している。 ①　協力会社・委託先が情報セキュリティ基本方針に基づき、情報セキュリティに関する具体的なルールや手順を遵守できるかのチェックを行う。基準を満たしていない場合は、改善要求し対応状況を確認する。 ②　委託元が要求するセキュリティ対策基準に対応している。	