サイバーセキュリティ経営ガイドライン Ver 2.0		関連するサイバーセキュリティ経営チェックシート		想定されるユーザー企業の状況	(プラクティス／悩み)番号	プラクティス内容
指示番号	内容	項番	内容			
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	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	サイバーセキュリティリスクが自社にどのような影響を及ぼすか明らかになっていないため、 経営者によるサイバーセキュリティリスクの認識が十分でない	1-1	経営者がサイバーセキュリティリスクを認識するための、他社被害事例の報告
					（8）	悩み） IT部門のみで経営層のセキュリティ意識を向上させることに限界を感じている 取組み） 外部講師による経営層向けの研修会を実施する
		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対応方針 （セキュリティポリシー）を策定し、宣言している	情報(顧客情報や営業秘密)保護の観点からセキュリティポリシーを定めているが、 サイバーセキュリティリスクを考慮したものとなっていない	1-2	サイバーセキュリティリスクに対応するための、セキュリティポリシーの改訂・共同管理
		3	法律や業界のガイドライン等の要求事項を把握している			
2	サイバーセキュリティリスク管理体制の構築	4	組織の対応方針（セキュリティポリシー）に基づき、CISO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	サイバーセキュリティ対策を計画・実行する情報システム部門の人材も不足しており、 専任のセキュリティ部門を作ることができない	（1）	悩み） インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある 取組み） 社外専門家を活用しながら自社でサイバーセキュリティ人材を育成する
					2-1	サイバーセキュリティリスクに対応するための、兼任のサイバーセキュリティ管理体制の構築
		5	サイバー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			
		6	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の関係を明確に規定している			
					（7）	悩み） 外部サービスの選定でIT部門だけでは対応が困難である 取組み） 社内の関連部門と連携して外部サービスの選定を行う
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	必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している	サイバーセキュリティ対策の予算を確保したいが、セキュリティ対策は一般的に費用対効果(ROI)が不透明なため、経営者から理解が得られにくい	3-1	サイバーセキュリティ対策のための、 予算の確保
		8	サイバーセキュリティ対策を実施できる人材を確保し、各担当者が自身の役割を理解している（組織の内外を問わず）	システムの開発・運用は外部委託しており、サイバーセキュリティ人材に求められる必要な知識や経験をもった人材を自社で確保する必要があるか分からない	3-2	サイバーセキュリティ対策のための、 必要なサイバーセキュリティ人材の定義・育成
		9	組織内でサイバーセキュリティ人材を育成している			
		10	組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、及び適切な処遇をしている			
		11	セキュリティ担当者以外も含めた従業員向けセキュリティ研修などを継続的に実施している		（9）	悩み） 従業員に対して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 取組み） 特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する
					（4）	悩み） IoT機器が「シャドーIT」化している 取組み） 製造部門とIT部門が連携し、不正接続機器や不適切な設定を排除する
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	12	守るべき情報を特定し、当該情報の保管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		-	
		13	特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、経営戦略を踏まえたサイバーセキュリティリスクとして把握している			
		14	サイバーセキュリティリスクが事業にいかなる影響があるかを推定している			
		15	サイバーセキュリティリスクの影響の度合いに従って、リスク低減、リスク回避、 リスク移転のためのリスク対応計画を策定している		（3）	悩み） インシデントが起きた際の財務面でのリスクヘッジが十分ではない 取組み） 初動対応のリスクを減らすサイバー保険の活用を検討する
		16	サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している			
					（5）	悩み） 自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる 取組み） 自社のセキュリティルールに整合する、適切なクラウドサービスを利用する
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	17	重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施している	運用を委託する情報システムに対して、ファイアウォールの設置などの入口対策は実施されているが、次の施策として何から手を付ければよいのかわからない。また、対策にあまりコストをかけられない	5-1	多層防御の実施 -端末への対応 -ネットワークの分離 -バックアップ
		18	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			
		19	検出すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している	システムの運用先にログ取得の要件を伝える必要があるが、サイバーセキュリティの観点で どのようなログを取得すべきかわからない	5-2	アクセスログの取得 -ログ取得 -ログ保管
		20	意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、対応者等の責任分担等）を策定している			
		21	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（検知すべきイベント、技術者対策の強化等）を適宜見直している			
		22	従業員に対して、サイバーセキュリティに対する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、 標的型攻撃メール訓練など）を実施している			
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	23	経営者が定期的に、サイバーセキュリティ対策の報告を受け、把握している		（6）	悩み） 全国各地の拠点におけるセキュリティ管理□状況に不安がある 取組み） 拠点におけるセキュリティの取組みを把握し、対面で対話する

サイバーセキュリティ経営ガイドライン Ver 2.0		関連するサイバーセキュリティ経営チェックシート		想定されるユーザー企業の状況	(プラクティス／悩み)番号	プラクティス内容
指示番号	内容	項番	内容			
		24	サイバーセキュリティにかかる外部監査を実施している			
		25	サイバーセキュリティリスクや脅威を適宜見直し、環境変化に応じた取り組み体制（PDCA）を整備・維持している			
		26	サイバーセキュリティリスクや取り組み状況を外部に公開している			
7	インシデント発生時の緊急対応体制の整備	27	組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Webサイト運用・保守、契約しているセキュリティベンダの連絡先含む）			
		28	サイバー攻撃の初動対応マニュアルを整備している	端末が攻撃された場合の証拠保全のルールを定めていない	7-2	従業員の初動対応の定義
		29	インシデント対応の専門チーム（CSIRT等）を設置している	インシデントに対応するための組織内の対応体制(CSIRT等)を整備していない	7-1	旗振り役としてのCSIRTの組成
		30	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めている			
		31	インシデント対応の課題も踏まえて、初期対応マニュアルを見直している			
		32	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている		（2）	悩み）インシデント対応の初動における情報共有に不安がある 取組み）標的型メール訓練で開封したかではなく報告したかを意識させる
8	インシデントによる被害に備えた復旧体制の整備	33	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	自然災害を想定したIT-BCPは策定しているが、どのような観点から既存のBCPと 連携させるべきか分からない	8-1	インシデント対応時の危機対策本部との連携
		34	復旧作業の課題を踏まえて、復旧計画を見直している			
		35	組織の内外における緊急連絡先・伝達ルートを整備している			
		36	定期的に復旧対応訓練や演習を行っている	インシデントに対する訓練や演習を実施したいが、システム運用委託先に加えて、 セキュリティに関する専門ベンダとのコミュニケーションが必要となるため、実施のハードルが 高いと考えている	8-2	組織内外の連絡先の定期メンテナンス
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	37	システム管理などについて、自組織のスキルや各種機能の重要性などを考慮して、自組織で対応できる部分と外部に委託できる部分を適切に切り分けている			
		38	委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている			
		39	系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握している	・業務を主管する部署がそれぞれ業務委託しており、会社として委託先を把握していないため、サイバーセキュリティリスクがある委託先を網羅的に調査し、特定することができない ・サイバーセキュリティ対策の実施状況を、どのような観点で確認すべきか分からない	9-1	サイバーセキュリティリスクのある委託先の特定と対策状況の確認
					（10）	悩み）スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない 取組み）セキュリティ対策の取組み、セキュリティ認証の取得状況を確認する
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	40	各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い、自社の対策に活かしている		-	
		41	マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPAへの届出や一般社団法人JPCERTコーディネーターセンターへの情報提供、その他民間企業等が推進している情報共有の取り組みへの情報提供を実施している			

サイバーセキュリティ経営ガイドライン Ver 2.0			
指示番号	内容	項番	付録A サイバーセキュリティ経営チェックシート
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	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
		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対応方針（セキュリティポリシー）を策定し、宣言している
		3	法律や業界のガイドライン等の要求事項を把握している
2	サイバーセキュリティリスク管理体制の構築	4	組織の対応方針（セキュリティポリシー）に基づき、CISO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
		5	サイバー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
		6	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の関係を明確に規定している
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	必要なサイバーセキュリティ対策を明確にし、経営会議などで対策の内容に見合った適切な費用かどうかを評価し、必要な予算を確保している
		8	サイバーセキュリティ対策を実施できる人材を確保し、各担当者が自身の役割を理解している（組織の内外を問わず）
		9	組織内でサイバーセキュリティ人材を育成している
		10	組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、及び適切な処遇をしている
		11	セキュリティ担当者以外も含めた従業員向けセキュリティ研修などを継続的に実施している
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	12	守るべき情報を特定し、当該情報の保管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
		13	特定した守るべき情報に対するサイバー攻撃の脅威、脆弱性を識別し、経営戦略を踏まえたサイバーセキュリティリスクとして把握している
		14	サイバーセキュリティリスクが事業にいかなる影響があるかを推定している
		15	サイバーセキュリティリスクの影響の度合いに従って、リスク低減、リスク回避、リスク移転のためのリスク対応計画を策定している
		16	サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している
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	17	重要業務を行う端末、ネットワーク、システム、またはサービスにおいて、ネットワークセグメントの分離、アクセス制御、暗号化等の多層防御を実施している
		18	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
		19	検出すべきイベント（意図していないアクセスや通信）を特定し、当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している
		20	意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、対応者等の責任分担等）を策定している
		21	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（検知すべきイベント、技術者対策の強化等）を適宜見直している
		22	従業員に対して、サイバーセキュリティに対する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、マルウェア対策ソフトの導入等）の周知、標的型攻撃メール訓練など）を実施している
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	23	経営者が定期的に、サイバーセキュリティ対策の報告を受け、把握している
		24	サイバーセキュリティにかかる外部監査を実施している
		25	サイバーセキュリティリスクや脅威を適宜見直し、環境変化に応じた取り組み体制（PDCA）を整備・維持している
		26	サイバーセキュリティリスクや取り組み状況を外部に公開している
7	インシデント発生時の緊急対応体制の整備	27	組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、システム運用、Webサイト運用・保守、契約しているセキュリティベンダの連絡先含む）
		28	サイバー攻撃の初動対応マニュアルを整備している
		29	インシデント対応の専門チーム（CSIRT等）を設置している
		30	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めている
		31	インシデント対応の課題も踏まえて、初期対応マニュアルを見直している
		32	インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている
8	インシデントによる被害に備えた復旧体制の整備	33	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
		34	復旧作業の課題を踏まえて、復旧計画を見直している
		35	組織の内外における緊急連絡先・伝達ルートを整備している
		36	定期的に復旧対応訓練や演習を行っている
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	37	システム管理などについて、自組織のスキルや各種機能の重要性などを考慮して、自組織で対応できる部分と外部に委託できる部分を適切に切り分けている
		38	委託先が実施すべきサイバーセキュリティ対策について、契約書等により明確にしている
		39	系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握している
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	40	各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い、自社の対策に活かしている
		41	マルウェア情報、不正アクセス情報、インシデントがあった場合に、IPAへの届出や一般社団法人JPCERTコーディネーターセンターへの情報提供、その他民間企業等が推進している情報共有の取り組みへの情報提供を実施している