設問番号	設問	優先度			項目	小規模（1~299人）	中規模（300~999人）	大規模（1000～人）
		小規模（1~299人）	中規模（300~999人）	大規模（1000～人）				
1	組織内でセキュリティ管理者（現場部門において必要な情報資産を振り分け整理・対策ができる人）はいますか。	◎	◎	◎	現場のセキュリティ管理者	全社で少なくとも1名	全社で複数名	部門ごとに少なくとも1名ずつ
2	セキュリティの最新の脅威を把握し、経営層へ連携する役割がありますか。	△	△	◎	セキュリティ担当者の人数	「脅威情報を収集・共有できる人」が全社で少なくとも1名いること （情シス担当者等を想定）	「脅威情報を収集し、定期的に脅威情報をレポートし、必要に応じて経営層と連携する人」が全社で複数名いること （情シス部門等を想定）	「脅威情報を収集し、定期的に脅威情報をレポートし、必要に応じて経営層と連携する人」が全社で複数名いること （情シス部門・情セキュ部門等を想定）
3	セキュリティ施策を実行する際に、経営者からの指示を受ける役割・担当者を設けていますか。	△	◎	◎	セキュリティ担当者の人数	「経営者とコミュニケーションを取り、施策を実行できる代表」が全社で少なくとも1名いること （情シス担当者等を想定）	「経営者とコミュニケーションを取り、施策を実行できる人」が全社で複数名いること （情シス部門等を想定）	「経営者とコミュニケーションを取り、施策を実行できる人」が全社で複数名いること （情シス部門・情セキュ部門等を想定）
4	セキュリティ上のリスクの評価を実施していますか。	○	◎	◎	リスク評価の実施頻度	年1回以上の全社的なリスク評価	年1回以上の全社的なリスク評価 （外部コンサル等の活用も検討）	年1回以上の部門ごとのリスク評価 （外部コンサル等の活用も検討）
5	組織内でサイバーセキュリティのルールを整備していますか。	◎	◎	◎	ルールの整備状況	ポリシー、ルールを整備 定期的な見直し	ポリシー、ルール、マニュアルを整備 定期的な見直し	ポリシー、ルール、マニュアルを整備（必要に応じて部門ルール等も整備） 定期的な見直し
6	BCP（事業継続計画）を定めていますか。	○	◎	◎	BCPの策定	「被害が発生した時に事業を継続・復旧させる方針や手順」の大枠を策定 定期的な見直し	全社でBCPを策定 定期的な見直し	全社でBCP及びIT-BCPを策定（必要に応じて部門ごとにも策定） 定期的な見直し
7	インシデント（サイバー攻撃被害/セキュリティ事故）管理・連携する人がいますか。	◎	◎	◎	CSIRT担当者の人数	インシデント時に管理・連絡を行う人が全社で少なくとも1名いること （情シス担当者等を想定） （CSIRTの設置は必ずしも必要ではない）	インシデント時に管理・連絡を行う人が全社で複数名いること （情シス部門等を想定） （CSIRTを設置。兼任可）	インシデント時に管理・連絡を行う人が全社で複数名いること （情シス部門・情セキュ部門等を想定） （CSIRTを設置。専任が望ましい）
8	サイバー攻撃被害/セキュリティ事故対応について外部に相談するベンダー（セキュリティ企業・組織等）はありますか。	○	◎	◎	外部ベンダー連携	緊急時に相談できるベンダーを1社以上選定 （IPAのサイバーセキュリティお助け隊サービス等を活用）	外部SOCとの業務委託契約	外部SOCとの業務委託契約 外部コンサルとの業務委託契約
9	サイバー攻撃被害/セキュリティ事故対応について、内部で対応できる体制がありますか。（人・モノ）	◎	◎	◎	CSIRT担当者の人数	緊急時に相談できるベンダーを1社以上選定 （IPAのサイバーセキュリティお助け隊サービス等を活用）	初動対応を行う人が全社で複数名いること （情シス部門等を想定） （CSIRTを設置。兼任可）	初動対応を行う人が全社で複数名いること （情シス部門・情セキュ部門等を想定） （CSIRTを設置。専任が望ましい）
10	サイバー攻撃被害/セキュリティ事故が発生した際に、報告を受け付ける窓口等の連絡先はありますか。	◎	◎	◎	インシデント報告窓口の整備	セキュリティ担当者の連絡先を全社に周知 （連絡がつかない場合もあり得る）	CSIRTの連絡先を全社に周知 勤務時間内は組織的な窓口対応 勤務時間外は受付担当者による対応（連絡がつかない場合もあり得る）	CSIRTの連絡先を全社に周知 勤務時間内は組織的な窓口対応 勤務時間外は受付担当者による対応（コールセンター等による24時間365日の対応も検討）
11	複数箇所でサイバー攻撃被害が同時に発生した場合に、どのサーバ・システムから優先して復旧対応する等、判断するための基準が定められていますか。	○	◎	◎	復旧優先度の定義	「被害が発生した時に事業を継続・復旧させる方針や手順」の大枠において定義	BCPにおいて定義	BCP及びIT-BCPにおいて定義
12	サイバー攻撃被害/セキュリティ事故発生時に被害の大きさによっては、組織の経営層への報告を実施し、指示を受けていますか。	△	◎	◎	エスカレーションルールの有無	簡易的なインシデント対応手順において定義	インシデント対応手順において定義	インシデント対応手順において定義
13	サイバー攻撃被害/セキュリティ事故発生時に、行政機関や関連団体、マスコミ等への対外連絡を行う手順、フローなどを定めていますか。	○	○	◎	インシデント対応手順書、フローの策定	簡易的なインシデント対応手順・フローを策定 定期的な見直し	インシデント対応手順・フローを策定 定期的な見直し	インシデント対応手順・フローを策定 定期的な見直し
14	不正通信やPCの不審な挙動を監視する仕組みができていますか。	○	○	◎	セキュリティ監視	EDR導入を検討 セキュリティ担当者による監視（異常発生時のアラート確認・ログ分析）	EDR導入 セキュリティ担当者による監視（異常発生時のアラート確認・ログ分析、及び定期的なログ分析）	EDRに加え、NDRや外部SOCを導入し、リアルタイム監視実施
15	サイバー攻撃被害/セキュリティ事故対応の訓練を定期的に実施していますか。具体的には、最低年一回、机上訓練・手順書の読み合わせ等を通して、サイバー攻撃被害/セキュリティ事故対応手順の検証および改善を行っていますか。	△	◎	◎	インシデント対応訓練	年1回訓練を実施し、初動の流れを把握 （セキュリティ担当者）	年1回訓練を実施し、手順書や連絡フローを検証 （セキュリティ担当組織）	年1回訓練を実施し、手順書や連絡フローを検証 （セキュリティ担当組織に加え、経営層や関係組織も参加） （外部コンサル等の活用も検討）
16	サイバー攻撃で被害を受けたシステムを復旧するための事前対策(バックアップの取得、復旧手順の策定)が取られていますか。	△	○	◎	システム復旧への備え	システムのバックアップ取得	システムのバックアップ取得 復旧手順書の整備及び復旧訓練の実施	システムのバックアップ取得 複数拠点・複数システムの復旧を想定した復旧手順書の整備及び復旧訓練の実施 （IT-BCPとの整合性を考慮）
17	従業員のセキュリティ意識の向上のために、セキュリティに関する教育や社内のセキュリティ関連ルールを周知し、習熟度を確認していますか。	◎	◎	◎	従業員向けのセキュリティ教育	年1回以上の全従業員向け教育	年1回以上の全従業員向け教育	年1回以上の全従業員向け教育 加えて、年1回以上の役割別教育（システム管理者向け等）
18	セキュリティ管理者に対して、外部組織の教育サービス等でセキュリティ教育を実施していますか。	△	○	◎	セキュリティ担当者のスキルアップ	無料セミナー等による情報収集 有料の外部研修等の検討	無料セミナー等による情報収集 有料の外部研修等によるスキルアップ	外部団体等への加盟による情報共有 有料の外部研修・カンファレンス参加によるスキルアップ
19	自組織で導入されているシステムをリストアップし、導入されているOSやソフトウェアを把握していますか。	◎	◎	◎	資産管理	システムの管理台帳（スプレッドシート等）を整備し年1回以上棚卸	システム、サーバの管理台帳（スプレッドシート等）を整備し年1回以上棚卸	システム・サーバ・情報資産の台帳を整備し年1回以上棚卸 資産管理ツールの導入を検討
20	サイバー攻撃動向や、脆弱性等の情報を収集していますか。	△	○	◎	脆弱性管理	担当者による属人的な情報収集（情シス担当者等を想定） 外部公開システムに対し、年1回以上の脆弱性診断実施が望ましい	担当組織による定常的な情報収集（情シス部門等を想定） 外部公開システムに対し、年1回以上の脆弱性診断実施、及び検出された脆弱性への対応	担当組織による定常的な情報収集（情シス部門・情セキュ部門等を想定） 外部公開システム及び内部システムに対し、年2回以上の脆弱性診断実施、及び検出された脆弱性への対応 （脆弱性管理ツールやパッチ適用ツールの導入も検討）