セキュリティ責任者編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.1.1	組織的 人的 技術的 物理的 ① 内部状況・外部状況の理解 組織内部及び外部の現状をサイバーセキュリティの視点から理解している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.1.2	組織的 人的 技術的 物理的 ② 関係主体からの要求事項の理解 関係主体、顧客、サプライチェーンからの要求事項を整理している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.1.3	組織的 人的 技術的 物理的 ③ 重要インフラサービス継続に係る特性の理解 自組織の重要インフラサービス継続に係る特性を理解している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.1.4	組織的 人的 技術的 物理的 ④ 現在プロファイルの特定 現段階における自組織のサイバーセキュリティ対処態勢の実態把握を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2.1	組織的 人的 技術的 物理的 ⑤-1 資産の特定 情報システム、制御システム、ソフトウェア、情報等の資産を特定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2.1	組織的 人的 技術的 物理的 ⑤-2 資産の特定 システムの機器構成、ネットワーク構成、外部との接続状況、システム外の機器（未管理機器）の接続状況等を把握している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2.2	組織的 人的 技術的 物理的 ⑥ リスクアセスメントの実施 組織の状況と資産を踏まえ、任務保証の考え方に基づくリスクアセスメントを実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2.3	組織的 人的 技術的 物理的 ⑦ 制御システムのリスクアセスメント 重要インフラサービスの提供に制御システムが使用されている場合には、制御システムについてもリスクアセスメントを実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.2.4	組織的 人的 技術的 物理的 ⑧ 目標とする将来像の設定 リスクアセスメント結果や要求事項等を踏まえ、サイバーセキュリティに関する自組織のあるべき姿として、目標とする将来像を設定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.1	組織的 人的 技術的 物理的 ⑨ サイバーセキュリティ方針の策定 サイバーセキュリティへの取組姿勢をサイバーセキュリティ方針として規定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.2	組織的 人的 技術的 物理的 ⑩ リスク対応の決定 目標とする将来像と現状の実態とのギャップを埋めるためのセキュリティ管理策を検討し、優先順位付けを行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.3	組織的 人的 技術的 物理的 ⑪-1 個別方針の策定 実施すべきセキュリティ管理策について、遵守すべき行為や判断等の基準を個別方針としてとりまとめている。関係者へ伝達する。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.3	組織的 人的 技術的 物理的 ⑪-2 個別方針の策定 上記のセキュリティ管理策の個別方針を、組織内、委託先等（必要に応じ）に対し伝達している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.4	組織的 人的 技術的 物理的 ⑫ リスク対応計画の策定 サイバーセキュリティの達成目標を定めて、ロードマップ及びリスク対応計画を作成し、サイバーセキュリティに係る取組を進めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3.5	組織的 人的 技術的 物理的 ⑬ サイバーセキュリティ関係規程の策定 サイバーセキュリティ方針に準拠したサイバーセキュリティ関係規程を策定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.4.1	組織的 人的 技術的 物理的 ⑭ サプライチェーン全体のリスクマネジメント 事業者間の契約において、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と責任範囲を明確化している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.4.2	組織的 人的 技術的 物理的 ⑮ 供給者管理 サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.4.2	組織的 人的 技術的 物理的 ⑯ 海外の供給者管理 海外拠点については、現地の法令、文化等も踏まえた対応を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.5	組織的 人的 技術的 物理的 ⑰ 通信のセキュリティ 運搬・送信する情報の形態及び格付けに応じた適切な運搬・送信手段を選択できるように対策を整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.6	組織的 人的 技術的 物理的 ⑱ クラウドサービス クラウドサービスを利用する場合には、クラウド事業者が開示する情報の把握や変更管理などを適切に行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.6	組織的 人的 技術的 物理的 ⑲-1 TOS等をクラウドサービスで利用する場合の対応 クラウドサービスを利用してTOS等の機能を実現している場合においても、マルウェアからの保護や不正アクセス対策を実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.6	組織的 人的 技術的 物理的 ⑲-2 TOS等をクラウドサービスで利用する場合の対応 クラウドサービスを利用してTOS等の機能を実現している場合、セキュリティ要件をクラウドサービスに求め、契約内容にも含めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.7.1	組織的 人的 技術的 物理的 ⑳ 業務委託（共通事項） TOS 等の開発・保守等を外部委託する際は、委託先の選定手続・選定基準、及び委託先が具備すべき要件を整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.7.1	組織的 人的 技術的 物理的 ㉑ 業務委託の際の契約条件（共通事項） 外部委託に係る業務遂行に際して、委託先に実施させるセキュリティ対策やシステム障害に対する対処手順等を、調達仕様書等に定め、委託の際の契約条件としている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.7.2	組織的 人的 技術的 物理的 ㉒ 情報システムに関する業務委託 整備されている選定手続き・選定基準等に基づき委託先を選定し、セキュリティ対策要件等を含む委託契約を取り交わしている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.7.2	組織的 人的 技術的 物理的 ㉓ 委託終了時のセキュリティ要件実施の確認 外部委託の終了時に、仕様書等定められた検査手続に従い、サイバーセキュリティに係る要件が満たされていることを確認している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.7.3	組織的 人的 技術的 物理的 ㉔ 委託先に係る人的安全管理措置 委託先の情報取扱者に対し、NDA（機密保持契約）締結や教育・訓練等の適切な人的安全管理措置を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.8.1	組織的 人的 技術的 物理的 ㉕ コンティンジェンシープランの作成 セキュリティインシデントが発生した場合の初動対応の方針、手順、態勢当を定めた「コンティンジェンシープラン」を策定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.8.2	組織的 人的 技術的 物理的 ㉖ 事業継続計画等の作成 システム障害やサイバー攻撃を想定したものを含む事業継続計画（BCP）等を策定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.8.3	組織的 人的 技術的 物理的 ㉗ 本社等重要拠点の機能確保 本社等の重要拠点が被災した場合に備え、緊急事態時における対策の検討・指揮をするための重要拠点の機能を確保している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.9.1	組織的 人的 技術的 物理的 ㉘ CSIRT等の整備 セキュリティインシデントに備えた体制（CSIRT等）を整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.9.1	組織的 人的 技術的 物理的 ㉙ 関連部門との役割分担の合意 インシデント対応に係る役割分担や対応手順等について、あらかじめ関連部門と合意している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
事前準備	1.9.1	組織的 人的 技術的 物理的 ㉚ セキュリティ専門機関、都道府県警察等との連携 セキュリティ専門機関や都道府県警察等を含めた社内外の対処態勢を平時から整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.9.2	組織的 人的 技術的 物理的 ㉛ 重要インフラサービス障害発生時の体制の整備 重要インフラサービス障害が発生した際、迅速に検出、防護、回復のための対策を講ずるために、事前に障害発生時の体制を整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.9.3	組織的 人的 技術的 物理的 ㉜ エスカレーション 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにしている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

セキュリティ責任者編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
平時対策	2.1.1	組織的 人的 技術的 物理的 ① セキュリティ対策の導入 サイバー攻撃等の予想を把握するために、システム機器のログ等を定期的に確認している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 技術的 物理的 ②-1 運用プロセスの確立・実行 安全管理について取扱者の責任と権限を明確に定めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 技術的 物理的 ②-2 運用プロセスの確立・実行 安全管理に対する規程や手順書を整備・運用している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.2	組織的 人的 技術的 物理的 ③-1 サイバー攻撃の予兆 サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.2	組織的 人的 技術的 物理的 ③-2 サイバー攻撃の予兆 予兆を認識した場合、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.3	組織的 人的 技術的 物理的 ④-1 情報共有 情報共有の取組については、「行動計画に基づく手引書」を参照し実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.3	組織的 人的 技術的 物理的 ④-2 情報共有 収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメンを実施し、リスク対応の要否を判断している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.3	組織的 人的 技術的 物理的 ④-3 情報共有 平時から、セキュリティベンダー、セキュリティ専門機関、都道府県警察等と情報交換等を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
平時対策	2.1.3	組織的 人的 技術的 物理的 ⑤ 追加のリスクアセスメント 収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.3	組織的 人的 技術的 物理的 ⑥ セキュリティ専門家との情報交換 セキュリティベンダー、セキュリティ専門機関、都道府県警察等と平時から情報交換等を行う。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.4	組織的 人的 技術的 物理的 ⑦-1 従業員の管理 リスクマネジメントの検証、改善のため、各プロセスにおいて、記録を作成している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.4	組織的 人的 技術的 物理的 ⑦-2 従業員の管理 ステークホルダーとのコミュニケーションの質を高めたり、経営層の意思決定を補助したりするために、報告を実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.4	組織的 人的 技術的 物理的 ⑦-3 従業員の管理 情報漏えいを防止するために、情報の取扱者に対し、守秘義務を課したり、秘密情報取扱いの教育・訓練等行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.4	組織的 人的 技術的 物理的 ⑦-4 従業員の管理 重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.5	組織的 人的 技術的 物理的 ⑧ 要管理対策区域における入退出管理の実施 情報処理設備を含む領域を保護するために、セキュリティ境界を明確に定め、適切な入退管理策を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2	組織的 人的 技術的 物理的 ⑨ 教育 全ての従業員に対して、サイバーセキュリティに関連する教育・訓練を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
平時対策	2.2	組織的 **人的** 技術的 物理的 ⑩ 人材育成・意識啓発 部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、人材育成・意識啓発を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.3	組織的 **人的** 技術的 物理的 ⑪ 演習・訓練を通じた課題の抽出及び改善 実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.3	組織的 **人的** 技術的 物理的 ⑫ インシデント対応手順の訓練 セキュリティインインシデント対応手順の確認等を行う訓練を定期的に実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.3	組織的 **人的** 技術的 物理的 ⑬ BCPに関する訓練 システム障害やサイバー攻撃を想定したものを含むBCP（事業継続計画）に関する訓練を定期的に実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.4.1	**組織的** 人的 技術的 物理的 ⑭ モニタリング実施計画の策定と実施 リスク対応計画の策定において決定した計画に則り、リスク対応を行ったセキュリティ管理策について評価を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.4.1	**組織的** 人的 技術的 物理的 ⑮ 脆弱性情報の収集、対応状況の確認 システムの構成機器上で利用するソフトウェアに関する脆弱性情報を収集し、脆弱性対策の状況を定期的に確認している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.4.2	**組織的** 人的 技術的 物理的 ⑯ セキュリティ対策の自己点検 自己点検の実施頻度、実施時期、自己点検すべき項目、実施項目の選択等に関する年度計画を整備している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.4.3	**組織的** 人的 技術的 物理的 ⑰ 監査計画の策定と実施 監査プロセスに従い、監査方針及び監査計画を作成し実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

ガイドラインの目次		対策	現状の評価	1 年後の評価	備考（実施目標日、進捗状況等）
平時対策	2.4.3	組織的 人的 技術的 物理的 ⑱ 独立性を有する者による監査 組織による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を定期的に実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.5	組織的 人的 技術的 物理的 ⑲ 継続的改善 各規程の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

セキュリティ責任者編

ガイドラインの目次		対策	現状の評価	1年後の評価	備考（実施目標日、進捗状況等）
インシデント発生時及び事後対応	3.1	組織的 人的 技術的 物理的 ① コンティンジェンシープラン及びBCPの実行 重要インフラサービス障害が発生した場合には、コンティンジェンシープラン及び事業継続計画等を実行し、早急にその状況を把握し、被害の拡大防止、早期復旧のための対策を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.2	組織的 人的 技術的 物理的 ② 重要インフラサービス障害発生時の情報共有 情報共有の取組については、「行動計画に基づく手引書」を参照し実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.2	組織的 人的 技術的 物理的 ③ 関係機関への情報共有 セキュリティインシデントが発生した場合には、自組織内の情報共有を行うとともに、専門組織への情報共有、国・港湾管理者等への情報共有、都道府県警察への通報を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.3	組織的 人的 技術的 物理的 ④ セキュリティ管理状況の対外説明 重要インフラサービス障害の状況や復旧等の情報提供については、策定したIT-BCP等又はBCP等に沿って対応している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.3	組織的 人的 技術的 物理的 ⑤-1 問合せ対応窓口の設定、港湾管理者との分担 上記の情報発信を行う際は、情報提供及び問合せ対応の窓口を設定している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.3	組織的 人的 技術的 物理的 ⑤-2 問合せ対応窓口の設定、港湾管理者との分担 上記の情報発信において、港湾管理者と事前に役割分担を決めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	3.4	組織的 人的 技術的 物理的 ⑥ インシデント管理 既存のセキュリティ管理策の運用を通じて得た経験等を分析し、今後の運用に活用している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	