「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第2版）」 参考文献

経営者層編

令和7年3月

港湾分野における「安全ガイドライン」（第2版） 目次	引用元	（参考）第1版 目次
1. 事前準備		
1.1 組織方針		3.1 組織方針
1.1.1組織方針とサイバーセキュリティ	【策定指針】: 3.1.1.	3.1.1組織方針とサイバーセキュリティ
1.1.2サイバーセキュリティ方針	【策定指針】: 3.1.2. 【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoT セキュリティガイドライン ver.1.0（平成28年度）】: 要点1 【JIS Q 27002:2014】: 5.1.1、5.1.2	3.1.2サイバーセキュリティ方針
1.2 経営リスクとしてのサイバーセキュリティリスクの管理	【策定指針】: 3.3.	3.3 経営リスクとしての サイバーセキュリティリスクの管理
2. 平時対策		
2.1 組織内外のコミュニケーション	【策定指針】: 3.2. 【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoTセキュリティガイドライン ver.1.0】: 要点1 【事業継続】: 4.2.2.2	3.2 組織内外のコミュニケーション
2.2 責任及び権限の割当て	【政府統一基準】: 2.1.1 【情報セキュリティ管理基準（平成28年改正版）】: 8.1	3.4 責任及び権限の割当て
2.2.1情報セキュリティ責任者の任命	【策定指針】: 3.4.、4.7. 【政府統一基準】: 2.1.1 【情報セキュリティ管理基準】: 8.1	3.4.1サイバーセキュリティ責任者の任命
2.2.2責任者・組織などの役割	【政府統一基準】: 2.1.2 【情報セキュリティ管理基準】: 4.4.1.2 【JIS Q 27002:2014】: 5.1.1、5.1.2、17.1.1 ～ 17.1.3、17.2.1 【JIS Q 22301:2013】 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書（第2版）～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	3.4.2責任者・組織などの役割
2.2.3役割の分離	【政府統一基準】: 2.1.1	3.4.3役割の分離
2.3 資源の確保	【策定指針】: 3.5. 【情報セキュリティ管理基準】: 4.5.1.1、4.5.1.2	3.5 資源の確保
2.4 監査・モニタリング	【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoTセキュリティガイドライン ver.1.0】: 要点1 【情報セキュリティ管理基準】: 4.5.3.1、4.6.3.1 ～ 4.6.3.3、4.7.1.1 ～ 4.7.1.7 【JIS Q 27014:2015】:5.3.2 ～ 5.3.6.6	3.6 監査・モニタリング
2.4.1セキュリティ対策の運用状況の把握	【策定指針】: 3.6. 【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoTセキュリティガイドライン ver.1.0】: 要点1 【情報セキュリティ管理基準】: 4.5.3.1、4.6.3.1 ～ 4.6.3.3、4.7.1.1 ～ 4.7.1.7 【JIS Q 27014:2015】: 5.3.2 ～ 5.3.6.6	3.6.1セキュリティ対策の運用状況の把握
2.4.2セキュリティ対策の監査	【手引書】:9.2. 【政府統一基準】: 2.3.2 【情報セキュリティ管理基準】: 4.7.1.1 ～ 4.7.1.7 【ISO/IEC 27014:2013】: 5.3.5	3.6.2セキュリティ対策の監査
3. インシデント発生時及び事後対応		
3.1 情報開示	【策定指針】: 3.7. 【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoTセキュリティガイドライン ver.1.0】: 要点1 【事業継続】: 4.2.2.2	3.7 情報開示

	3.2 インシデント対応及び事業継続対応	【手引書】: 8.4. 【JIS Q 22301:2013】 【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	4.9.2コンティンジェンシープラン及びBCPの実行

※【策定指針】　＝重要インフラのサイバーセキュリティに係る安全基準等策定指針
【手引書】　＝重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
【行動計画】　＝重要インフラのサイバーセキュリティに係る行動計画(令和5年)
【政府統一基準】＝政府機関等の対策基準策定のためのガイドライン(令和5年度版)
【事業継続】　＝事業継続ガイドライン(令和5年3月)

「港湾分野における情報セキュリティ確保に係る安全ガイドライン(第2版)」 参考文献

セキュリティ責任者編

令和7年3月

港湾分野における「安全ガイドライン」(第2版) 目次	引用元	(参考)第1版 目次
1. 事前準備		
1.1 組織状況の理解	【策定指針】: 4.1. 【手引書】: 4.	4.1 組織状況の理解
1.1.1内部状況・外部状況の理解	【手引書】: 4.1.1.、4.1.2.	4.1.1内部状況・外部状況の理解
1.1.2関係主体からの要求事項の理解	【情報セキュリティ管理基準】: 4.4.2.1、4.4.3.1 【JIS Q 27002:2014】: 18.1.1	4.1.2関係主体からの要求事項の理解
1.1.3重要インフラサービス継続に係る特性の理解	【手引書】: 4.1.3.	4.1.3重要インフラサービス継続に係る特性の理解
1.1.4現在プロファイルの特定	【手引書】: 4.2.	4.1.4現在プロファイルの特定
1.2 リスクアセスメント	【策定指針】: 4.2. 【重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書】 【制御システムのセキュリティリスク分析ガイド】 【CSMS認証基準 Ver.2.0】: 4.2、4.3 【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1 【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7 【テレワークセキュリティガイドライン】: 第2章 2. (1)	4.2 リスクアセスメント
1.2.1資産の特定	【策定指針】: 5.1.1.1. 【手引書】: 11.1.1. 【政府統一基準】: 6.1.1(2)、6.1.1(3)、6.4.1(1)、6.4.1(3)、6.4.2(3)、8.1.1(3) 【テレワークセキュリティガイドライン】: 第2章2.(3)、第5章3 【ICT サイバーセキュリティ総合対策 2022】: 1(1)ウ 【IoT セキュリティガイドラインVer 1.0】: 2.55.1.1.2	5.1.1資産の管理
1.2.2リスクアセスメントの実施	【策定指針】: 4.2. 【手引書】: 5.1. 【重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書】 【制御システムのセキュリティリスク分析ガイド】 【CSMS認証基準 Ver.2.0】: 4.2、4.3 【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1 【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7 【テレワークセキュリティガイドライン】: 第2章 2. (1)	4.2.1リスクアセスメントの実施
1.2.3制御システムのリスクアセスメント	【策定指針】: 4.2. 【手引書】: 5.2.	4.2.2制御システムのリスクアセスメント
1.2.4目標とする将来像の設定	【手引書】: 4.2.、6.1.	4.2.3目標とする将来像の設定
1.3 サイバーセキュリティリスク対応		
1.3.1サイバーセキュリティ方針の策定	【策定指針】: 3.1.2. 【企業経営のためのサイバーセキュリティの考え方】 【サイバーセキュリティ経営ガイドライン Ver.3.0】 【IoT セキュリティガイドライン ver.1.0(平成28年度)】: 要点1 【JIS Q 27002:2014】: 5.1.1、5.1.23.2	3.1.2サイバーセキュリティ方針
1.3.2リスク対応の決定	【策定指針】: 4.3.1. 【手引書】: 6.2	4.3.1リスク対応の決定
1.3.3個別方針の策定	【策定指針】: 4.3.2. 【手引書】: 6.3. 【政府統一基準】: 2.2.2 【JIS Q 27002:2014】: 5.1.1、5.1.2 【テレワークセキュリティガイドライン】: 第2章 2. (1) 【情報セキュリティ管理基準】: 7.2.3	4.3.2個別方針の策定
1.3.4リスク対応計画の策定	【策定指針】: 4.3.3. 【手引書】: 6.3. 【情報セキュリティ管理基準】: 4.4.8.4、4.4.8.5	4.3.3リスク対応計画の策定

	1.3.5サイバーセキュリティ関係規程の策定	【策定指針】: 4.3.2. 【手引書】: 6.3. 【政府統一基準】: 2.2.2 【JIS Q 27002:2014】: 5.1.1、5.1.2 【テレワークセキュリティガイドライン】: 第2章　2. (1) 【情報セキュリティ管理基準】: 7.2.3	4.3.2個別方針の策定
1.4 サプライチェーン・リスクマネジメント			
	1.4.1サプライチェーン全体のリスクマネジメント	【策定指針】: 4.4. 【手引書】: 6.4.	4.4 サプライチェーン・リスクマネジメント
	1.4.2供給者管理	【策定指針】: 4.4.、5.1.2. 【手引書】: 6.4. 【政府統一基準】: 6.2.1.	5.1.2供給者管理
1.5 通信のセキュリティ		【策定指針】: 5.4.4. 【手引書】: 11.1.3.6.、11.4.4.2. 【政府統一基準】: 3.1.1(6)、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12	5.4.4通信のセキュリティ
1.6 クラウドサービス		【策定指針】: 5.1.1.3.、5.5.2. 【政府統一基準】: 4.2.1、4.2.2、4.2.3、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【クラウドサービス利用のための情報セキュリティマネジメントガイドライン (2013年度版)】: 1、3.2、3.3、6、11.5、12.4 【中小企業のためのクラウドサービス安全利用の手引き】: 第2章　3.(3)②～③、第5章7. 【ICT サイバーセキュリティ総合対策 2022】: 1(1) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12	5.5 クラウドサービス
1.7 委託先管理		【政府統一基準】: 4.1.1、4.1.1(2) 【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1 【外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書】: 3.1, 3.2 【クラウドサービス利用のための情報セキュリティマネジメントガイドライン 】: 12.5	5.6 委託先管理
	1.7.1業務委託(共通事項)	【政府統一基準】: 4.1.1、4.1.1(1)、4.1.1(2)(a) 【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1 【外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書】: 3.1、3.2 【個人情報ガイドライン(通則編)】: 3-3-4	5.6.1業務委託(共通事項)
	1.7.2情報システムに関する業務委託	【政府統一基準】: 4.1.1、4.1.1(2) 【JIS Q 27002:2014】: 7.1.1、7.1.2、7.2.1、7.2.2、7.3.1 【外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書】: 3.1, 3.2 【クラウドサービス利用のための情報セキュリティマネジメントガイドライン】: 12.5	5.6.2情報システムに関する業務委託
	1.7.3委託先に係る人的安全管理措置	【策定指針】: 5.2.2. 【手引書】: 11.2.2. 【個人情報ガイドライン(通則編)】: 3-3-2 【JIS Q 22301:2013】: 8.5 【JIS Q 27002:2014】: 17.1.3	5.6.3委託先に係る人的安全管理措置

1.8 事業継続計画等		【手引書】: 7. 【JIS Q 22301:2013】 【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	4.5 事業継続計画等
	1.8.1コンティンジェンシープランの作成	【CSIRTマテリアル】	4.5 事業継続計画等
	1.8.2事業継続計画等の作成	【策定指針】: 4.5. 【手引書】: 7.1 【事業継続】: 4.2.2.2、5.1	4.5.1事業継続計画等の作成
	1.8.3本社等重要拠点の機能の確保	【事業継続】: 4.2.2、4.2.2.1	4.9.3本社等重要拠点の機能の確保
1.9 インシデントに備えた組織体制(CSIRT 等)の整備			
	1.9.1CSIRT 等の整備、関連部門との役割分担等の合意	【策定指針】: 4.7. 【手引書】: 8.2.	4.7.1CSIRT等の整備、関連部門との役割分担等の合意
	1.9.2重要インフラサービス障害発生時の体制の整備	【政府統一基準】: 2.2.4、2.2.4(2)、2.2.4(3) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.6、16.1.7 【情報セキュリティ管理基準】:16.1	4.5.2重要インフラサービス障害の対応
	1.9.3エスカレーション	【策定指針】: 5.2.4. 【手引書】: 11.2.4.	5.2.3エスカレーション
2. 平時対策			
2.1 平時の運用			
	2.1.1セキュリティ対策の導入、運用プロセスの確立・実行	【対策指針】: 4.8.1	4.8.1セキュリティ対策の導入、運用プロセスの確立・実行
	2.1.2サイバー攻撃の予兆	【策定指針】: 4.9.	4.9.1サイバー攻撃の予兆
	2.1.3情報共有	【策定指針】: 3.7.、4.8.2. 【手引書】: 3. 【政府統一基準】: 2.2.3 【情報セキュリティ管理基準】: 4.5.2.3、4.5.2.4、4.5.2.6 ～ 4.5.2.8 【行動計画】:別紙4-1～4－3 【サイバー攻撃被害に係る情報共有・公表ガイダンス検討会の開催について】	4.8.2情報共有
	2.1.4従業員の管理	【策定指針】: 5.2.1. 【手引書】: 10.2.、11.2.1. 【個人情報ガイドライン(通則編)】: 3-3-2	5.2.1従業員の管理
	2.1.5要管理対策区域における入退出管理	【手引書】: 11.3. 【政府統一基準】: 3.2.1、3.2.1(1)、3.2.1(2)、3.2.1(3)、6.1.1、6.2.1 【JIS Q 27002:2014】: 11.1.1 ～ 11.1.6、11.2.1、11.2.3、11.2.5 【IoTセキュリティガイドライン ver.1.0】: 要点2	5.3.1セキュリティ確保が求められる領域
2.2 人材育成・意識啓発		【策定指針】: 4.6., 5.2.1. 【手引書】 8.1.、11.2.1. 【政府統一基準】: 2.2.3 【情報セキュリティ管理基準】: 4.5.2.3、4.5.2.4、4.5.2.6 ～ 4.5.2.8 【テレワークセキュリティガイドライン】: 第2章　2. (1)	4.6 人材育成・意識啓発
2.3 演習・訓練		【策定指針】: 4.10. 【手引書】: 8.5. 【重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書】 【制御システムのセキュリティリスク分析ガイド】 【CSMS認証基準 Ver.2.0】: 4.2、4.3 【CSMSユーザーズガイド Ver.1.2】: 3.1、4.1 ～ 4.4、6.1 【IoTセキュリティガイドライン ver.1.0】: 要点3 ～ 7	4.10 演習・訓練
2.4 モニタリング及びレビュー			
	2.4.1モニタリング実施計画の策定と実施	【手引書】: 9.1. 【情報セキュリティ監査基準 実施ガイドライン Ver1.0】 【NIST CSF】	4.11.1モニタリング実施計画の策定と実施
	2.4.2セキュリティ対策の自己点検	【政府統一基準】: 2.3.1、2.3.1(1)	4.11.3セキュリティ対策の自己点検
	2.4.3監査計画の策定と実施	【情報セキュリティ監査基準 実施ガイドライン Ver1.0】	4.11.2監査計画の策定と実施

	2.5 継続的改善	【政府統一基準】: 2.4.1、2.4.1(1)	3.8 継続的改善
3. インシデント発生時及び事後対応			
	3.1 コンティンジェンシープラン及びBCPの実行	【手引書】: 8.4. 【JIS Q 22301:2013】 【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	4.9.2コンティンジェンシープラン及びBCPの実行
	3.2 重要インフラサービス障害発生時の情報共有	【策定指針】: 3.7.、4.8.2. 【手引書】: 3. 【政府統一基準】: 2.2.3 【情報セキュリティ管理基準】: 4.5.2.3、4.5.2.4、4.5.2.6 ～ 4.5.2.8 【行動計画】:別紙4-1～4－3 【サイバー攻撃被害に係る情報共有・公表ガイダンス検討会の開催について】	4.8.2情報共有
	3.3 セキュリティ管理状況の対外説明	【JIS Q 22301:2013】 【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	4.9.4セキュリティ対策状況の対外説明
	3.4 インシデント管理	【策定指針】: 5.1.5. 【手引書】: 11.1.5.	5.1.4インシデント管理

※【策定指針】　＝重要インフラのサイバーセキュリティに係る安全基準等策定指針

【手引書】　＝重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書

【行動計画】　＝重要インフラのサイバーセキュリティに係る行動計画(令和5年)

【政府統一基準】＝政府機関等の対策基準策定のためのガイドライン(令和5年度版)

【事業継続】　＝事業継続ガイドライン(令和5年3月)

「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第2版）」 参考文献

システム構築・運用者編　　令和7年3月

港湾分野における「安全ガイドライン」（第2版）目次	引用元	（参考）第1版 目次
1. 事前準備		
1.1 災害による障害の発生しにくい設備の設置及び管理	【手引書】: 11.3. 【政府統一基準】: 3.2.1、3.2.1(1)、3.2.1(2)、3.2.1(3)、6.1.1、6.2.1 【JIS Q 27002:2014】: 11.1.1 ～ 11.1.6、11.2.1、11.2.3、11.2.5 【IoTセキュリティガイドライン ver.1.0】: 要点2	5.3.2災害による障害の発生しにくい設備の設置及び管理
1.2 装置の管理	【策定指針】: 5.3.3. 【手引書】: 11.3.1.、11.3.2.	5.3.3装置の管理
1.3 リモートアクセス環境導入に関する対策基準の策定	【手引書】: 11.2.3. 【政府統一基準】: 6.4.1(2) 【テレワークセキュリティガイドライン】: 第1章1、第2章2(1)(2) 【Web 会議サービスを使用する際のセキュリティ上の注意事項】: 3.1、4.3(1) 【テレワークを行う際のセキュリティ上の注意事項】: 2.(3)	5.2.2リモートアクセス環境
2. 平時対策		
2.1 不正アクセス等の脅威への対策	【政府統一基準】: 7.1.1、7.1.2、7.1.3 【JIS Q 27002:2014】: 9.2.1 ～ 9.2.6、9.4.1 ～ 9.4.3	5.4.1不正アクセス等の脅威への対策
2.1.1利用者アクセスの管理	【策定指針】: 5.4.1. 【手引書】: 11.4.1.	5.4.1.1利用者アクセスの管理
2.1.2主体認証機能	【政府統一基準】: 7.1.1、8.1.1(6)	5.4.1.2主体認証機能
2.1.3権限管理機能	【政府統一基準】: 7.1.3	5.4.1.3.権限管理機能
2.2 情報システム等のアクセス制御	【手引書】: 11.4.2. 、11.4.2.1. 【政府統一基準】: 7.1.1、7.1.2、7.1.3 【JIS Q 27002:2014】: 9.2.1 ～ 9.2.6、9.4.1 ～ 9.4.3	5.4.2情報システム等のアクセス制御
2.2.1アクセス制御機能	【手引書】: 11.4.2. 、11.4.2.1. 【政府統一基準】: 7.1.1、7.1.2、7.1.3 【JIS Q 27002:2014】: 9.2.1 ～ 9.2.6、9.4.1 ～ 9.4.3	5.4.2情報システム等のアクセス制御
2.2.2パスワード管理	【手引書】: 11.4.2.2.、11.4.2.3. 【政府統一基準】: 7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12	5.4.2.1パスワード管理
2.3 暗号を活用した情報管理	【策定指針】: 5.4.3. 【手引書】: 11.4.4.2. 【政府統一基準】: 7.1.5、7.1.5(1)、7.1.5(2)、8.1.1(7) 【JIS Q 27002:2014】: 10.1.1、10.1.2、18.1.5 「輸出貿易管理令別表第1第9項(7) 暗号装置又はその部分品」	5.4.3暗号を活用した情報管理
2.4 負荷分散・冗長化	【政府統一基準】: 7.2.3(1)、6.2.1(1)	5.4.5負荷分散・冗長化
2.5 多層防御	【策定指針】: 5.4.5. 【手引書】: 11.4.5. 【政府統一基準】: 7.2.4(1) 【テレワークセキュリティガイドライン】: 第5章 6	5.4.6多層防御
2.6 資産のセキュリティ運用		
2.6.1情報システムの構成要素の運用	【政府統一基準】: 7.1.1(2)、7.1.1(3)、7.3.1(1)、7.3.1(2)、7.3.1(3)、8.1.1(3) 【テレワークセキュリティガイドライン】: 第2章2.(3)，第5章3 【ICT サイバーセキュリティ総合対策 2022】: 1(1)ウ 【IoT セキュリティガイドラインVer 1.0】: 2.5	4.8.1.2情報システムの構成要素の運用

	2.6.2情報システムの監視	【政府統一基準】: 5.2.3(1)(a)、5.2.4、5.2.5 【情報セキュリティ管理基準】: 4.6.2.2、4.6.2.3 【JIS Q 19011:2012】	4.8.1.3情報システムの監視
	2.6.3情報システムの更改・廃棄時の措置	【政府統一基準】: 5.2.3(1)(a)、5.2.4、5.2.5 【情報セキュリティ管理基準】: 4.6.2.2、4.6.2.3 【JIS Q 19011:2012】 【廃棄するパソコンやメディアからの情報漏洩】	4.8.1.4情報システムの更改・廃棄時の措置
	2.6.4データ管理	【策定指針】: 5.1.1.3	5.1.1.2データ管理
2.7 サイバー攻撃等に備えた運用管理			
	2.7.1マルウェアからの保護	【策定指針】: 5.5.1. 【手引書】: 11.1.3.2. 【政府統一基準】:7.2.1(1)、7.2.2、7.2.2(1)、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12	5.1.3.2マルウェアからの保護
	2.7.2バックアップ	【策定指針】: 5.1.3.3. 【手引書】: 11.1.3.3. 【統一基準ガイドライン】: 3.1.1(8)(a)解説 【事業継続】: 4.2.3、5.1.2 【テレワークセキュリティガイドライン】: 第2章 2.(1) 【IoT セキュリティガイドライン Ver 1.0】: 1.1.2	5.1.3.3バックアップ
	2.7.3ログ取得	【策定指針】: 5.1.3.4. 【手引書】: 11.1.3.4. 【政府統一基準】: 7.1.4、7.1.4(1)	5.1.3.4ログ取得
	2.7.4運用ソフトウェアの管理	【策定指針】: 5.1.3.5. 【手引書】: 11.1.3.5	5.1.3.5運用ソフトウェアの管理
	2.7.5脆弱性の管理	【策定指針】: 5.1.3.6. 【手引書】: 11.4.3. 【政府統一基準】: 7.2.1、7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12	5.1.3.6脆弱性の管理
	2.7.6電子メール運用時の対策	統一基準: 7.2.1(1)、7.2.2、7.2.3(1)、8.1.1(5)、8.1.1(5)(e) 【JIS Q 27002:2014】: 16.1.1、16.1.2、16.1.4、16.1.5 【高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて】 【インシデントハンドリングマニュアル】 【テレワークセキュリティガイドライン】: 第5章6、第6章12 【誤送信に関する総務省の注意喚起】 【IPAの情報セキュリティ10大脅威】	5.1.3.7電子メール運用時の対策
3. インシデント発生時及び事後対応			
	3.1 インシデント発生時のコンティンジェンシープランの実行	【手引書】: 8.4. 【JIS Q 22301:2013】 【JIS Q 27002:2014】: 17.1.1 ～ 17.1.3、17.2.1 【中央省庁における情報システム運用継続計画ガイドライン～策定手引書(第2版)～】 【IT-BCP 策定モデル】 【CSIRTマテリアル】	4.9.2コンティンジェンシープラン及びBCPの実行

※【策定指針】　＝重要インフラのサイバーセキュリティに係る安全基準等策定指針
【手引書】　＝重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
【行動計画】　＝重要インフラのサイバーセキュリティに係る行動計画(令和5年)
【政府統一基準】＝政府機関等の対策基準策定のためのガイドライン(令和5年度版)
【事業継続】　＝事業継続ガイドライン(令和5年3月)

「港湾分野における情報セキュリティ確保に係る安全ガイドライン(第2版)」 参考文献

港湾管理者等

令和7年3月

港湾分野における「安全ガイドライン」(第2版) 目次	引用元	(参考)第1版 目次
3.1.事前準備	新規作成	新規作成
3.1.1情報セキュリティに関する会議体の設置		
3.1.2休日・夜間を問わない連絡体制の構築		
3.1.3インシデント発生時における対処要領の策定		
3.2 平時対策		
3.2.1インシデント発生時の情報伝達訓練や机上対処訓練の実施		
3.2.2情報セキュリティ対策に関する研修などの人材育成		
3.3 インシデント発生時及び事後対応		
3.3.1インシデントの情報収集(リエゾンの派遣等)		
3.3.2道路混雑や滞船などの港湾の利用障害の情報発信		
3.3.3インシデントの原因究明への協力		