システム構築・運用者編

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	組織的 人的 技術的 **物理的** ① 災害による障害の発生しにくい設備の設置 重要インフラサービス障害をもたらす原因となる様々な脅威からサーバ装置、端末及び通信回線装置を保護するための物理的な対策を検討している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.2	組織的 人的 技術的 **物理的** ② 装置の管理 機器・装置等の物理的な保護及び停電や落雷等、電源管理に関する対策を検討している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	1.3	**組織的** 人的 技術的 物理的 ③ リモートアクセス環境に関する対策基準の策定 リモートアクセス環境をテレワークに適用する場合にはリモートアクセス環境導入に関する対策基準を定めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

システム構築・運用者編

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 ①-1 利用者アクセスの管理 情報システムへのアクセス制御を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 **技術的** 物理的 ①-2 利用者アクセスの管理 情報システムへの不正ソフトウェア対策を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 **技術的** 物理的 ①-3 利用者アクセスの管理 情報システムの監視を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 **技術的** 物理的 ② 外部接続ネットワーク機器の管理 外部接続ネットワーク機器について、予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.1	組織的 人的 **技術的** 物理的 ③ システム内機器のアクセス管理 システム内部機器については、予め許可された者のみがシステムへの接続が可能となるよう、技術的な措置を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.2	組織的 人的 **技術的** 物理的 ④ 主体認証機能 情報システムについて、情報の格付けに従って、識別及び主体認証を行う機能を設けている。	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 ⑤ 外部ユーザに対する主体認証 外部接続ネットワーク機器については、外部ユーザに対する主体認証を実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.1.2	組織的 人的 **技術的** 物理的 ⑥ 内部ユーザに対する主体認証 システム内部機器については、管理者に対する主体認証を実施している。	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）
平時対策	2.1.3	組織的 人的 **技術的** 物理的 ⑦ 権限管理機能 全ての情報システムについて、権限管理を行う必要性の有無を検討し、権限管理を行う機能を設けている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.1	組織的 人的 **技術的** 物理的 ⑧ 情報システム等のアクセス制御 各重要システムについて、アクセス制御を行う必要性の有無を検討し、アクセス制御を行う機能を設けている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.1	組織的 人的 **技術的** 物理的 ⑨ 外部アクセスの制御 外部接続ネットワーク機器については、アカウントロック機能等により、外部からのアクセスを適切に制御している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.1	組織的 人的 **技術的** 物理的 ⑩ 専用線による外部接続の場合の対応 TOS等システムと外部システムとが専用線により接続されている場合であっても、ファイアウォール設置等の措置を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.2.2	組織的 人的 **技術的** 物理的 ⑪ パスワード管理 パスワード攻撃に対応した、適切なパスワード管理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	
	2.3	組織的 人的 **技術的** 物理的 ⑫ 暗号を活用した情報管理（情報システム） 情報システムにおいては、暗号化機能及び電子署名の付与機能等を適切に実装している。	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 暗号を活用した情報管理（制御システム） 制御システム等においては、暗号化機能を導入していない場合は、ログや通信の監視等の代替措置を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.4	組織的 人的 **技術的** 物理的 ⑭ 負荷分散・冗長化 システムの負荷分散や冗長化について検討を行い、必要があると認められる場合は、二重化を図るなど適切に処置している。	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	組織的 人的 **技術的** 物理的 ⑮ TOS等のバックアップシステム TOS等がサイバー攻撃を受けた際の事業継続にあたっては、必要に応じて、バックアップシステムを用意している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.5	組織的 人的 **技術的** 物理的 ⑯ 多層防御 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には、多層防御を導入している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.6.1	組織的 人的 **技術的** 物理的 ⑰ 情報システムの構成要素の運用 情報システムの構成要素の運用においては、個別のセキュリティ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	
	2.6.2	組織的 人的 **技術的** 物理的 ⑱ 情報システムの監視 不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に発見・追跡できるように、平時より情報システムの監視を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.6.3	組織的 人的 **技術的** 物理的 ⑲ 情報システムの更改・廃棄時の措置 情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、移行作業におけるセキュリティ対策及び不要な情報の抹消を適切に実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.6.4	組織的 **人的** **技術的** 物理的 ⑳ データ管理 システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行っている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.1	組織的 **人的** 技術的 物理的 ㉑ マルウェアからの保護 マルウェア感染の回避を目的とし、取扱者に対する日常的実施事項を定めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.1	組織的 人的 **技術的** 物理的 ㉒ マルウェア対策の実施 外部接続するネットワーク機器、及びTOS等ネットワーク内のサーバ機器等に係る適切なマルウェア対策を講じている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

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	2.7.1	組織的 人的 技術的 物理的 ㉓ 外部記憶媒体（USB）の運用ルール 外部記憶媒体（USB）を利用する際には、マルウェア感染回避のための、適切な運用ルールを定め実施している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.2	組織的 人的 技術的 物理的 ㉔ バックアップ システム障害やサイバー攻撃発生に備え、バックアップを適切に取得している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.3	組織的 人的 技術的 物理的 ㉕ バックアップの保存場所 取得したバックアップは、現用システムとは切り離した場所に保存している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.3	組織的 人的 技術的 物理的 ㉖ ログの取得 情報システムの正常性の確認及び不正アクセス等の検知を行うことを目的として、必要に応じてログを取得している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.3	組織的 人的 技術的 物理的 ㉗-1 TOS等システム内機器のログの取得 TOS等システム内のサーバ機器及びネットワーク機器のログを定期的に取得している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.3	組織的 人的 技術的 物理的 ㉗-2 TOS等システム内機器のログの保存 上記のログについて、システム外にバックアップを保存している。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.4	組織的 人的 技術的 物理的 ㉘ 運用ソフトウェアの管理 情報システム、制御システムの設定や、利用するソフトウェア（クラウドサービス含む。）の個々の設定について可能な限り把握・理解し、安全性の確保に努めている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	
	2.7.4	組織的 人的 技術的 物理的 ㉙ 運用ソフトウェアの定期的確認、更新 外部接続ネットワーク機器、及びTOS等ネットワーク内のサーバ機器等上で利用しているソフトウェアの情報を定期的に確認し、必要に応じ更新している。	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	2.7.5	組織的 人的 技術的 物理的 ㉚ 脆弱性の管理 サーバ装置、端末及び通信回線装置上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集し、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	
	2.7.5	組織的 人的 技術的 物理的 ㉛ 制御システムの脆弱性の管理 制御システムにおいては、ソフトウェア更新等により可用性が担保できないと判断される場合には、制御システムに関する通信を監視する等の代替策を検討し、脆弱性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	
	2.7.6	組織的 人的 技術的 物理的 ㉜ 電子メール運用時の対策 電子メール運用時の対策の実施を組織全体に浸透させている。	チェック日 / / □はい □いいえ	チェック日 / / □はい □いいえ	

システム構築・運用者編

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の実行 セキュリティインシデントが発生した場合には、コンティンジェンシープランに従い、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	