重要インフラにおける情報セキュリティ確保に係る

「安全基準等」策定にあたっての指針（第３版）

対策編

平成　22年　7月30日

平成　25年　3月26日改定

重要インフラ専門委員会

重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第3版）対策編

Ⅰ　本対策編の位置づけ 2
Ⅱ　対策項目の具体化の例示 2
（1）4つの柱 2
ア　組織・体制及び資源の対策 2
イ　情報についての対策 4
ウ　情報セキュリティ要件の明確化に基づく対策 5
エ　情報システムについての対策 7
（2）5つの重点項目 13
ア　IT 障害の観点から見た事業継続性確保のための対策 13
イ　情報漏えい防止のための対策 15
ウ　外部委託における情報セキュリティ確保のための対策 19
エ　IT障害発生時の利用者の対応のための情報の提供等の対策 21
オ　ITに係る環境変化に伴う脅威のための対策 22

Ⅰ　本対策編の位置づけ

本対策編は、重要インフラにおける情報セキュリティ確保に向けて指針をより有用なものとするために、本編の対策項目の具体例を記載した項目集としての位置づけとしている。本対策編の策定に際し、１）具体性の充実と２）国内外の諸規格との整合性確保を念頭に置きつつ、できる限り網羅的に項目を洗い出したもので、新たに重要インフラ専門委員会にて決定し定めたものである。

本対策編を活用する際には、指針の目的や位置づけ、対象範囲及び対象とする脅威等に関して、指針を参照のうえ、検討を進めていただきたい。

本対策編は、各重要インフラ分野が安全基準等の継続的な改善を行う際、具体的な対策項目を検討する際のチェックリストとして活用いただければ幸いであるが、各重要インフラ分野においては、自らの特性を踏まえ、対策項目の追加・選択・修正等を適宜行い、「安全基準等」の継続的改善が促進されることを期待する。

Ⅱ　対策項目の具体化の例示

本編の対策項目の具体例としては、次のとおりである。

なお、本対策編の活用にあたり、指針本編の各対策項目の記載内容を適宜参照できるように、該当項目を引用（四角枠内）することとした。

※「要検討事項」・「参考事項」の分類については、指針本編において各対策項目毎に定めたものであり、本対策編における個々の具体例の扱いに係るものではない。

（1）4つの柱

ア　組織・体制及び資源の対策

（ア）　組織・体制及び人的資源の確保　【要検討事項】

各重要インフラ事業者等における情報セキュリティ対策の PDCA サイクルを機能させるために、その運用等に係る組織及び体制の確立及びこれを支える資源の確保が重要である。

情報セキュリティ対策は、それに係るすべての職員が、職制及び職務に応じて与えられている権限と責務を理解した上で、準備された資源によって、負うべき責務を履行することで実現される。

このため、情報セキュリティ対策を実施する組織・体制及び資源の確保について明示されることが必要である。

なお、組織・体制及び資源の確保には、例えば、情報セキュリティに関わる人材育成や教育といった基礎的・長期的な取り組みから、情報セキュリティ対策の実効性を確保する上で必要な自己点検・監査の実施等具体的な対策項目が含まれる。

○組織・体制の確立

・情報セキュリティ基本方針の策定
・グループ会社も含めた情報セキュリティに関する組織体制の整備（責任者・責任部門・委員会等の設置、役割・責任分担の明確化等）・情報セキュリティ関係規程の整備（違反への対処、例外措置等）
・人的資源確保（雇用条件の明示、守秘契約の締結、懲戒手続等）
・ＩＴ障害発生時の体制・対応手順の整備（「重要インフラの情報セキュリティ対策に係る第２次行動計画」が想定するサイバー攻撃、非意図的要因、災害や疾病等の脅威が引き起こすＩＴ障害に関わる情報の集約及び共有体制を含む）

○教育・訓練の実施

・情報セキュリティ対策の教育・訓練計画の策定
・教育・訓練実施記録の保管

○自己点検・内部監査の実施

・自己点検の実施
・内部監査の実施
・情報セキュリティ対策の見直し

（イ）　情報セキュリティ人材の育成等　【参考事項】

知的財産としての「人財」という観点から、情報セキュリティ人材の育成や要員の管理を行うことが望ましい。

・情報セキュリティ人材の育成・活用・管理に関する規程の整備（情報処理技術者試験、情報システムユーザースキル標準等を活用し、社内人材育成マップ等の作成とこれに基づく社内教育コースの整備等を記載）
・インシデント発生時に対応ができる人材の計画的な育成

（ウ）　外部監査等による情報セキュリティ対策の評価　【参考事項】

技術的な対策は多くの事業者等で行われているが、今後は外部監査等による情報セキュリティ対策の評価を行うことが望ましい。

・情報セキュリティ監査等の実施

・情報セキュリティ対策の見直し

イ　情報についての対策

（ア）　情報の格付け　【要検討事項】

取扱う情報について、その重要度に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から、情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配付禁止）が明示されるべきである。

〇重要性に応じた適切な措置

・資産の洗出し（体制、洗出し項目、洗い出し基準等）
・情報のライフサイクルと情報の格付けに応じた情報セキュリティ対策

（イ）　情報の取扱い　【要検討事項】

情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階における情報セキュリティ対策が明示されるべきである。

〇情報の作成と入手

・目的外の作成・入手の禁止
・台帳等作成
・作成・入手時における情報の格付けと取扱制限の決定
・作成時点の情報の格付けの継承
・格付けの変更手続き

〇情報の利用

・情報の利用に関する許可及び届出に係る措置
・目的外利用の禁止
・格付け及び取扱制限に従った情報の取扱い
・格付け及び取扱制限の見直し
・アクセス履歴の保存
・アクセス制御・出力制御
・離席時の対策（端末ロック等）

〇情報の保存

・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載）
・情報の保存期間に従った管理

〇情報の移送

・情報の移送に関する許可及び届出に係る措置
・作業責任者・手続きの明確化
・作業担当者の識別、認証、権限付与
・移送手段の選択
・書面の保護対策
・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等)）

〇情報の提供

・提供に関する許可及び届出
・付加情報の削除

〇情報の消去

・情報の消去に関する許可及び届出
・電磁的記録の消去手続き（消去の確認、消去記録の保管等）

ウ　情報セキュリティ要件の明確化に基づく対策

（ア）　情報セキュリティ確保のために求められる機能　【要検討事項】

主体認証（利用者及び機器等の認証)、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

〇主体認証

・主体認証機能の導入
・主体認証技術の選択（知識、所有、生体認証、及び多要素認証等）
・利用者ＩＤの管理（個人単位のＩＤ付与、不要ＩＤの削除等）
・主体認証情報の管理（暗号化、パスワードの定期変更・最低文字数の制限、ＩＤ毎に異なるパスワードの設定等）
・利用者の責任（パスワードの利用、端末管理、クリアデスク・クリアスクリーン方針）
・不正使用検知時における主体認証の利用停止措置

〇アクセス制御

・アクセス制御機能の導入
・利用者アクセスの管理（利用者登録、特権管理、利用者パスワードの管理、利用者アクセス権のレビュー等）

・ネットワークのアクセス制御方針の策定
・利用者属性以外に基づくアクセス制御機能の導入（利用時間による制御、利用時間帯による制御、利用端末の識別、強制アクセス制御等）

○権限管理
・権限管理機能の導入実施
・利用者ＩＤと主体認証情報の付与管理
・利用者ＩＤと主体認証情報における代替手段等の適用

○証跡管理
・証跡管理機能の導入実施
・証跡取得と保存
・取得した証跡の点検、分析及び報告
・証跡管理に関する利用者への周知

○負荷分散
・トラフィックの分散処理、予備機の設置
・負荷状態の監視制御機能の充実

○冗長化
・ネットワークの適切な管理・制御、通信経路の迂回措置
・ハードウェアの予備
・（アプリケーションを含めた）情報システムの冗長対策

（イ）　情報セキュリティについての脅威　【要検討事項】
セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

○セキュリティホール
・情報収集
・対応計画の策定
・対応内容の記録
・定期チェック
・不正アクセスの監視・検出（IDS の使用）
・通信フィルタリング（ファイアウォール、ウェブアプリケーションファイアウォール（WAF）等）
・外部ネットワークからの遮断等

・アンチウイルスソフトウェアの使用（端末、ゲートウェイ）、メンテナンス、定期検査、セキュリティパッチ適用
・利用していない通信ポート等の非活性化、マクロ実行の抑制
・早期発見・早期回復対策（監視、障害の検出、障害箇所の切り分け、障害時の縮退・再構成、取引制限、リカバリ機能）

○不正プログラム

・情報収集
・ＯＳ／アプリケーションのセキュリティ設定
・アンチウイルスソフトウェアの導入
・パターンファイルの更新
・パッチ適用・定期的なウイルス検査

○サービス不能攻撃

・通信フィルタリング
・通信回線の冗長化
・通信事業者との連携
・電子計算機、通信回線装置及び通信回線の監視と記録

エ　情報システムについての対策

（ア）　施設と環境　【要検討事項】

入退出の管理や安全区域の確保、停電時、断水時の対応等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。

○入退出の管理

・入退出管理（障壁、施錠、主体認証、入退出履歴の記録、継続的に立ち入る者の承認、侵入監視装置の設置、最小限の施設表示）
・訪問者、清掃業者及び物品の搬出入業者の管理（身分の記録、入室審査手順、立ち入り制限区域の設定、職員等の立ち会い・付き添い、ストラップ・ID カード、情報システムに接触できない場所での受け渡し）

○安全区域の確保

・設置場所の配慮（バックアップセンターの設置、遠隔地でのバックアップ媒体保管、災害を受けにくい場所への設置等）
・物理的セキュリティ境界の設定
・電子計算機及び通信回線装置のセキュリティ確保（不正操作・盗み見等の防止対策）

・安全区域内のセキュリティ管理策（身分証明書の携帯・常時視認、物品等の持ち込み・持ち出しの情報セキュリティ責任者の承認・記録、コンピュータ・外部記録媒体等の持ち込み制限、作業の監視）
・防犯対策（侵入防止装置、赤外線検知装置、トラップセンサーの設置、記録用機器の使用制限、盗難防止装置）

〇電力供給の途絶・通信の途絶・水道供給の途絶への対応

・防災対策（建物の耐震・免震構造及び防火構造化、設備の転倒等防止対策・防火対策・落雷対策・防水対策、監視設備・警報装置・非常口及び非常灯設置等）
・自家発電装置、無停電電源装置、予備電源
・空調（加湿を含む）設備の冷却水の備蓄等
・通信回線の冗長化

（イ）　電子計算機　【要検討事項】

電子計算機の設置時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

〇設置時

・文書（仕様書・設計書、機種・利用ソフトウェアの種類及びバージョン情報、管理者・利用者情報、利用者ＩＤ管理情報、構成要素のセキュリティに関する手順等）整備及び変更管理手順の明確化
・供給元及び更新情報、保守期間等が明確な機器の利用
・情報システムの受入れに必要な要求事項（受入れ基準）の明確化
・情報システムの受入れ前試験実施と合否判定基準の明確化
・サプライチェーンにおける情報セキュリティを考慮した機器の調達（信頼のできるベンダーから調達する等）
・安全区域への設置
・ 防災対策（設備の転倒等防止対策・防火対策・落雷対策・防水対策、監視設備・警報装置・非常口及び非常灯設置等）
・電子計算機の十分な性能（処理能力・容量・拡張性）の確保
・電子計算機の負荷分散・冗長構成化
・不要なアプリケーションの利用禁止・不要な機能の無効化・削除
・端末で利用可能なソフトウェアの制限
・端末の盗難防止対策
・モバイル端末に対するセキュリティ機能の装備（ワンタイムパスワード、暗号化、遠隔ロック、遠隔消去等）

・記録媒体を持たない端末の利用
・サーバ装置に対する暗号化機能の装備（遠隔保守時）
・障害時、緊急時の対応手順の策定

〇運用時（保守時含む）

・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・定期的調査による利用ソフトウェアの把握
・不正行為及び不正アクセスの検知(アクセスログ確認、侵入検知システム・アンチウイルスソフトウェア使用等)
・稼働状態監視（通常時、繁忙時のシステムの性能、容量、処理能力管理）による異常検知
・運用管理記録、障害記録、作業記録の作成・管理
・端末等の盗難防止対策
・モバイル端末で利用する電磁的媒体の暗号化
・利用可能な通信回線、通信方法の制限
・情報システム内の時刻同期化
・構成管理（機器管理、外部接続管理）
・情報システムの構成変更の定期的な確認
・定期的なバックアップ取得とバックアップ媒体の安全管理（遠隔地保管等）
・定期的なパスワードの変更
・障害時、緊急時を想定した訓練（復旧テスト等）の実施
・外部委託業者の作業の確認・点検
・利用ソフトウェアのアップデート、脆弱性に関する情報収集
・主体認証（ネットワーク接続時も含む）
・セキュリティホール対策（検査、対応）
・無線 LAN 使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・内部と外部のネットワークの分離
・防災対策の定期的な見直し

〇システム統合時

・統合に伴うリスク管理体制の構築
・移行基準の明確化
・統合後の業務運営体制の検証

〇運用終了時

・廃棄計画・手順の策定

・電磁的記録（媒体）の情報抹消

（ウ）　アプリケーションソフトウェア　【要検討事項】

アプリケーションソフトウェアの導入時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

〇導入時

・情報セキュリティ要件の検討、仕様化

・運用体制（管理者、障害時の連絡体制、委託先窓口等連絡先、通常時以外の特別体制）の決定及び周知

・文書（仕様書・設計書、機種・利用ソフトウェアの種類及びバージョン情報、管理者・利用者情報、利用者ＩＤ管理情報、構成要素のセキュリティに関する手順等）整備及び変更管理手順の明確化

・バージョン管理

・開発環境と本番環境の分離

・ソフトウェア開発を外部委託する場合の契約手順

・電子メールの不正中継禁止

・電子メール送信時及び受信時の送信ドメイン認証（ＳＰＦ等）

・主体認証

・ウェブにおける特殊文字使用の禁止、無効化

・ウェブにおける脆弱性のある作り込みの回避

・攻撃に利用されるウェブサーバ情報の送信を防ぐ対策

・公開するサーバ上に保存する情報の制限

・電子証明書による正当性の証明

・通信情報（データ）の暗号化

〇運用時（保守時含む）

・利用ソフトウェア管理、バージョン管理

・利用ソフトウェアのアップデート、脆弱性に関する情報収集

・電子署名による配布元の確認（ソフトウェアダウンロード時）

・HTML メール使用時の注意

・電子メールの対策・制限（添付ファイルの保護、不正中継禁止、送受信容量の制限、自動転送、業務外利用、送信先アドレス漏洩の防止、電子署名、暗号化、迷惑メールフィルター）

・外部ネットワークとの接続制限（プロキシ経由等）
・データバックアップ、バックアップ媒体の安全管理
・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・証跡管理
・不正検知
・稼働状態監視（通常時、繁忙時の性能、容量、処理能力管理）による異常検知
・無許可ネットワーク、外部ネットワーク接続の禁止
・運用管理記録、障害記録、作業記録の作成・管理（外部委託業者の作業管理も含む）
・主体認証（ネットワーク接続時も含む）
・セキュリティホール対策（検査、対応）
・無線 LAN 使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・内部と外部のネットワークの分離
・構成管理（機器管理、外部接続管理）

〇システム統合時

・統合に伴うリスク管理体制の構築
・移行基準の明確化
・統合後の業務運営体制の検証

〇運用終了時

・廃棄計画・手順の策定
・電磁的記録（媒体）の情報抹消

（エ）　通信回線及び通信回線装置　【要検討事項】

通信回線及び通信回線装置の構築から運用、運用終了又は停止に至るまでの対策が明示されるべきである。

〇構築時

・未承認機器からの通信の遮断
・通信の暗号化
・通信性能の確保
・遠隔地からの保守時の対策
・外部からの侵入が困難な回線の選択

・原則公衆回線からの接続の禁止（例外時はコールバックやユーザの限定）
・移動、転倒防止措置
・不特定多数が接続するネットワークとの接続禁止
・改ざん防止対策
・盗聴防止対策
・客観的に評価された製品等の導入の検討
・供給元及び更新情報、保守期間等が明確な機器の利用
・文書（仕様書、規程、マニュアル、利用者管理）の整備及び変更管理手順の明確化

〇運用時

・変更管理
・運用管理記録の作成
・稼働監視
・利用する機器、利用者及び識別コードの管理
・リモートアクセス時の対策（主体認証、証跡管理、アクセス制限、機密性確保、利用可能な端末の管理）
・不要なポートの閉塞
・無許可ネットワーク、外部ネットワーク接続の禁止
・内部と外部のネットワークの分離
・制御系ネットワークの分離
・ルータによる DoS 攻撃対策
・入退室管理（障壁、施錠、主体認証、記録、継続的に立ち入る者の承認、侵入監視装置の設置、施設の最小限表示）
・データバックアップ、バックアップ媒体の安全管理
・目的外利用の禁止（閲覧可能なウェブサイトの制限、私的目的による使用の禁止）
・証跡管理
・不正検知、異常（非日常状態の）検知
・稼働監視（通常時、繁忙時の性能、トラブル時の復旧時間、再発防止策の実施状況、システム容量・能力管理）
・情報収集（利用ソフトウェア）
・運用管理記録、障害記録、作業記録の作成・管理（外部委託業者の作業管理も含む）
・主体認証（ネットワーク接続時も含む）
・時刻同期
・セキュリティホール対策（検査、対応）

・無線 LAN 使用時の対策（暗号化、主体認証、機器識別、証跡管理、アクセス制限、他ネットワークの利用制限、機密性確保、接続可能な機器の管理）
・構成管理（機器管理、外部接続管理）
・ネットワーク構成等に関する情報の秘匿

〇運用終了時

・廃棄計画・手順の策定
・電磁的記録（媒体）の情報抹消

（２）５つの重点項目

ア　IT 障害の観点から見た事業継続性確保のための対策

（ア）　事業継続性確保のための個別対策の実施　【要検討事項】

IT 障害を未然に防止するための措置、IT 障害の発生を早期発見するための措置、及び IT 障害が発生した場合の拡大防止や迅速復旧のための措置が明示されるべきである。その際、東日本大震災に見られた広域災害・複合障害や新型インフルエンザ等、社会全体で対応が望まれる脅威についても考慮されるべきである。あわせて、事業継続に必要なデータが東京に一極集中している状況を踏まえ、首都直下地震についても考慮されるべきである。

〇未然防止措置

・指揮命令系統の明確化
・権限委譲、代行順位の決定
・重要拠点（指揮拠点）の確保
・事業継続計画の策定・事業継続計画の教育・訓練計画の策定・訓練の実施
・事業継続計画の教育・訓練実施記録の保管・緊急連絡ルールの確定（連絡先、連絡事項、連絡手段）
・連絡不可能な場合（通信途絶等）の緊急時行動ルールの確定
・所管省庁への連絡体制
・情報システム・通信回線の冗長化、代替手段の整備
・信頼性設計
・物理的な不正侵入の防止
・他情報システムとの独立、接続点の最小化
・情報システムの定期点検及び更新
・緊急時の処理増加等を考慮した情報システムの余裕設計

・代替情報システムの作業手順書策定

〇早期発見のための措置

・情報システムの稼働監視
・不正アクセス、不正トラフィックの監視
・様々な主体が提供する災害・障害発生時の情報サービスの活用

〇拡大防止・早期復旧のための措置

・複数の連絡手段の準備
・自家発電装置等で使用する燃料の準備
・対外的な情報発信、情報共有
・バックアップシステムの整備、代替手段及び代替手段に必要なシステムの準備
・バックアップ稼働計画、復帰計画の策定
・情報の格付けに応じたデータバックアップ（オンライン、媒体保管等）、遠隔地への保管
・通信途絶時でも必要最小限の業務を継続するための準備
・業界内での相互支援に備えたデータ形式の標準化推進
・広報、利用者からの問い合わせへの対応

〇社会全体で対応する脅威に対する準備

・パンデミック対策（コンピュータセンターのオペレータ要員の確保等）

（イ）　事業継続計画との整合性への配慮　【要検討事項】

事業継続計画が策定される場合には、顕在化する可能性が高いＩＴ障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである。その際、相互依存関係にある重要インフラ分野間（情報通信、電力、水道分野等と他分野との間）において、リスクコミュニケーション等の連絡・連携に平時より努めるべきである。

〇事業継続計画との整合性の確保

・事業継続計画の実施優先順位と判断基準の明確化
・事業継続計画の実施条件の明確化
・事業継続計画の定期的な見直し
・事業継続計画と情報セキュリティ対策との間の整合性確保
・平時からのリスクコミュニケーションの実施（セプターカウンシルの活用等）

イ　情報漏えい防止のための対策

（ア）　保護すべき情報の類型化　【要検討事項】

漏えい対策の対象となる保護すべき情報を類型化し、明示されるべきである。

〇保護すべき情報の類型化

- 情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け
- 情報資産の洗出し方法（体制、洗出し項目、洗出し基準)、情報、情報システムについてのランク付け
- 情報資産の機密性、完全性、可用性に基づく分類
- 安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた分類）
- 個人データ取扱台帳の整備、リスクアセスメント結果に応じた分類

（イ）　保護すべき情報の管理　【要検討事項】

保護すべき情報及び当該情報が記録された媒体を安全に取扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置が明示されるべきである。

〇情報の作成と入手

- 目的外の作成・入手の禁止
- 台帳等作成
- 作成・入手時における情報の格付けと取扱制限の決定
- 作成時点の情報の格付けの継承
- 格付けの変更手続き

〇情報の利用

- 情報の利用に関する許可及び届出に係る措置
- 目的外利用の禁止
- 格付け及び取扱制限に従った情報の取扱い
- 格付け及び取扱制限の見直し
- アクセス履歴の保存
- アクセス制御・出力制御
- 離席時の対策（端末ロック等）
- 要保護情報の利用にあたっての措置（情報交換の方針及び手順、取外し可能な媒体の管理、重要情報の内部漏えい、盗難、紛失、流出への対策）
- 書類や電子媒体の持ち出し管理（書類等の保管ルール、端末への資料の保管、持出しに関するルールや制限）

〇情報の保存

・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載）
・情報の保存期間に従った管理
・安全な場所への保管（自然災害を被る可能性が低い地域への保管、外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管）
・内容表示の記号化（媒体等に保存情報内容が想定できるタイトル表示をすることの禁止）
・バックアップの分散、隔地保管

〇情報の移送

・情報の移送に関する許可及び届出に係る措置
・作業責任者・手続きの明確化
・作業担当者の識別、認証、権限付与
・移送手段の選択
・書面の保護対策
・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等）

〇情報の提供

・情報の提供に関する許可及び届出
・付加情報の削除

〇情報の消去

・情報の消去に関する許可及び届出
・電磁的記録の消去手続き（消去の確認、消去記録の保管等）

（ウ）　不正アクセスによる脅威への対策　【要検討事項】

保護すべき情報が保存されたＰＣや外部記録媒体の盗難、紛失及び当該ＰＣや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための措置が明示されるべきである。

〇ＰＣや外部記録媒体の盗難、紛失を防止するための措置

・入退室管理
・ＰＣ・外部記録媒体の原則外部持ち出し禁止
・移動可能な機器の盗難防止策、情報盗難の防止等の措置の実施

〇ＰＣや外部記録媒体からの情報漏えいを防止するための措置

・安全管理措置を講ずるための組織体制の整備、規定整備とそれに従った運用
・個人データの取扱状況を確認できる手段の整備
・雇用契約時及び委託契約時における非開示契約の締結
・職員に対する教育・訓練の実施
・保存の際のパスワード、暗号化等の対策の実施
・電子メールを送信する場合の宛先確認

〇アプリケーションからの情報漏えいを防止するための措置

・取扱者の責任と権限の明確化
・取扱手順の規定と実施状況の確認
・主体認証機能、アクセス制御機能、権限管理機能
・データ漏洩防止（暗証番号等の漏洩防止、相手端末確認機能）
・破壊・改ざん防止（排他制限機能、不良データ検出機能、ファイル突合機能）
・予防策（取引制限機能、事故時の取引禁止機能、電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能）
・ネットワーク上からの不正アクセス対策（ファイアウォール、アンチウイルスソフトウェア、IDS、WAF)、不正侵入防止機能（使用されていないポートの閉鎖、データの書き換えを検出する設定、定期的な改ざんの有無の検査）
・攻撃の記録の保存と関係機関との連携
・検知策（アクセスログの取得・保管、不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
・早期発見策（監視機能、障害の検出および障害箇所の切り分け機能）
・早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

（エ）　内部関係者による脅威への対策　【要検討事項】

内部関係者による情報漏えいを抑止するための措置、情報漏えいの追跡性確保のための措置の他、情報セキュリティに関するリテラシーを向上させるための措置や取扱いミスを低減させるための措置が明示されるべきである。

〇内部関係者による情報漏えいを抑止するための措置

・個人データ管理責任者の選定（閲覧等の利用時の管理者の許可）

・役割・責任分担の明確化等
・外部での情報処理に関する規定の整備（事業者外での情報処理の制限）
・個人データを取り扱う職員及び権限の明確化
・守秘・非開示契約の締結（不当な目的での使用等の禁止）
・書類等の保管ルール（施錠可能なキャビネットへの保管、鍵の管理）
・端末への資料の保管、持出しに関するルールや制限
・入退室管理や常時監視（カメラ）等の導入
・破壊・改ざん防止（排他制限機能、アクセス制限機能、不良データ検出機能、ファイル突合機能、ID の不正使用防止機能）
・事業者支給以外のシステムによる情報処理の制限
・異常発見時の対応（管理者への連絡と適切な処置の実施）
・内部からの攻撃の監視（職員の監督とモニタリング）
・退職後の個人情報保護規程

〇情報漏えいの追跡性確保のための措置
・証跡管理
・検知策（不正アクセスの監視機能、不正な取引の検知機能、異例取引の監視機能）
・早期発見策（監視機能、障害の検出および障害箇所の切り分け機能）
・早期回復対策（障害時の縮退・再構成機能、取引制限機能、リカバリ機能）

〇リテラシーを向上させるための措置
・情報セキュリティ対策の教育・訓練

〇取扱いミスを低減させるための措置
・取引制限機能、事故時の取引禁止機能
・電子的価値の保護機能、暗号鍵の保護機能、電子メール、ホームページ閲覧等の不正使用防止機能
・外部ネットワークからのアクセス制限、不正侵入防止機能

（オ）　情報漏えい発生時の対応策の整備　【要検討事項】
　情報漏えいの発生に備えて、当該事象へ対応するための体制及び対処手順等が明示されるべきである。

〇体制
・責任・権限を有する担当者の選任
・緊急連絡体制の構築

・報告事項、対応措置、代替手段などの規定

〇対処手順

・事実関係の把握、漏えい情報の範囲の特定
・情報漏えい経路の特定（システム・端末の調査等）
・情報漏えい継続の阻止、被害の最小化（対象通信の遮断や対象サーバ等をネットワークから隔離するための運用フロー等の整備）
・本人への通知、事実関係の公表・広報等
・所管省庁への報告
・関係機関への周知・情報漏えいに至った経緯・原因等の解析
・再発防止策の検討と対策の実施
・情報漏えい事案等への対応状況の記録・分析

ウ　外部委託における情報セキュリティ確保のための対策

（ア）　委託先管理の仕組み　【要検討事項】

外部委託可能な範囲の明確化や委託先の選定基準、委託先に求める情報セキュリティ対策項目や事業者としての管理方法等が明示されるべきである。

〇外部委託可能な範囲の明確化や委託先の選定基準

・委託目的の明確化
・委託可能な業務範囲の明確化
・委託先選定基準の明確化（経営状況、信頼度・受託実績、技術水準、情報セキュリティ対策の実施状況（諸規定整備含む）、障害発生時の対応力等）
・委託先選定手続きの明確化

〇委託先に求める情報セキュリティ対策項目

・委託元と同レベルの情報セキュリティ対策
・情報セキュリティ対策の遵守方法
・委託先に求める情報セキュリティ対策の周知
・機密保持（機密保持契約）、目的外利用の禁止（確認書の提出）
・個人情報を扱う場合の要件の明確化
・委託先作業時の申請
・作業報告書の提出

〇事業者としての管理方法

・提供する情報の最小化

・委託先がアクセス可能な情報資産の制限
・委託先の情報セキュリティ対策の実施状況の確認
・納品検査時の情報セキュリティ対策の確認
・委託先が再委託する際の対応策の整備
・定期点検・監査の実施
・保守用専用アカウントの設定

（イ）　外部委託実施における情報セキュリティ確保対策の徹底　【要検討事項】

基本契約の締結や委託内容・取扱い情報の重要性に応じて、必要な情報漏えい防止策等の強化対策事項の契約への盛り込み等、契約者双方の責任の明確化と合意形成が明示されるべきである。

〇基本契約の締結

・委託先の情報セキュリティ対策（委託元と同レベル）
・機密保持（機密保持契約）、目的外利用の禁止
・再委託の制限
・委託管理責任者の設置
・委託業務内容、委託業務の執行場所、作業者、作業内容の特定
・契約内容の遵守状況についての委託元による確認
・契約内容が遵守されない場合の対処（損害賠償請求等）
・監査への協力
・契約の解約・解除に関する事項
・契約終了時の情報資産の返却及び消去

〇情報の重要性に応じた対策事項の契約への盛り込み

・取扱う情報資産に応じた対策の選定
・データ等の取扱いに関する事項（保管場所・保管方法）
・委託元と同等以上の情報セキュリティ対策の実施

〇契約者双方の責任の明確化と合意形成

・委託元・委託先双方の責任分界点の明確化
・委託先に求める情報セキュリティ対策項目の遵守
・遵守方法及び管理体制に関する取り決め
・施設全体の運用業務全般にわたる取り決め
・損害賠償に関する規定の合意

（ウ）　IT 障害発生時の対応策の整備　【要検討事項】

IT 障害発生時における委託先の措置や重要インフラ事業者等としての対処方法（委託先及び委託元との間の連絡体制や委託先と委託元が一体となったトラブル対処方法等）が明示されるべきである。

○ＩＴ障害発生時における委託先の措置

・対処方法を含んだ契約の締結
・対処方法の事前の周知
・異常検知ツールの活用
・異常状態の記録・保存
・連絡体制の整備
・障害箇所の切り離し
・原因の特定
・修正プログラムの適用

○重要インフラ事業者等としての対処方法

・問題発生時の対処の合意
・利用者への説明責任の認識
・行動基準の規定
・責任分界点の明示
・緊急時及び平常時の連絡体制の整備（業界内、ベンダー等）
・事実関係の確認
・外部要因による障害の防止
・委託先との情報共有
・他システムへの影響調査
・IT 障害対応の訓練、演習の計画及び委託先を含めた実施

エ　ＩＴ障害発生時の利用者の対応のための情報の提供等の対策

（ア）　ＩＴ障害による重要インフラサービスの停止等の情報の提供　【要検討事項】

重要インフラサービスの停止状況、復旧（可能であれば見込みを含む。）等の情報の適時の提供の方策が明示されるべきである。

・サービス停止状況、復旧（見込み）情報の提供

（イ）　ＩＴ障害防止のための取組みに関する情報の提供　【要検討事項】

利用者の安心に資する観点から、重要インフラサービスの停止・低下を防止するための情報セキュリティ対策に関する取組みについて、提供範囲に留意しつつ、対外的な説明に努めるべきである。

・情報セキュリティ報告書、ＣＳＲ報告書、各種ディスクロージャ資料等の作成
・ウェブサイト、電子メール等による情報提供

オ　ＩＴに係る環境変化に伴う脅威のための対策　【要検討事項】

社会環境や技術環境等の状況は刻々と変化しており、IT 障害を引き起こす新たな脅威が顕在化することがある。このような脅威として、電子計算機の性能の向上により暗号の解読が容易になる「暗号の危殆化」や、インターネットの普及による IPv4 アドレス枯渇に伴う「IPv6 への移行」等が考えられる。

このような情報システムの基盤を支える社会環境や技術環境等の変化について、ＩＴ障害発生の未然防止のための適切な対策を検討すべきである。

・継続的な情報収集
・平時からの情報収集の実施
・新たな脅威が顕在化時点で速やかに検討体制が構築できる準備
・「暗号危殆化」に関する継続的な情報収集の実施（電子政府推奨暗号リスト等参照）
・「ＩＰｖ６移行」に関する継続的な情報収集と実装検討の実施