資料５

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」策定指針
（第４版）対策編
（原案）

平 成 2 x 年 x 月 x x 日

（本ページは白紙です。）

目次

Ⅰ．対策編の位置付け

本書（以下、指針対策編という）は、重要インフラ[1]における情報セキュリティ対策の適切かつ継続的な改善に資するために、具体性の充実及び国内外の諸規格との整合を念頭に置き、情報セキュリティ対策項目の具体例を PDCA サイクルに沿って採録した項目集である

指針対策編の活用に際しては、指針本編[2]の『Ⅱ「安全基準等」で規定が望まれる項目』も参照の上、具体的な対策項目のチェックリストとの位置付けのもと、各「安全基準等」の策定・改訂に係る検討の一助となれば幸いである。

重要インフラ分野及び重要インフラ事業者等の特性を踏まえつつ、「安全基準等」が適切かつ継続的に改善がなされることを期待する。

[1] 「重要インフラ」とは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので重要インフラとして指定する分野」を指す。

[2] 「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４版）」を指す。

Ⅱ．具体的な情報セキュリティ対策項目の例示

対策項目の具体例については、指針本編の各対策項目の記載内容を引用（四角枠内）の上、指針本編の図表１「重要インフラ事業者等の対策例」と各対策に関連する「国の施策例」に沿って採録する。

1. 「Plan（準備）」の観点

1.1 「方針」の観点

(1) 抽出した課題に基づくリスク評価

「Check（確認）・Act（是正）」において後述するリスク分析の結果に基づき、対応が必要なリスクとその対応の優先順位付けに係る意思決定及び「安全基準等」の策定・見直しに係る基礎情報の作成（リスク評価）を行う。

基礎情報をもとに、要求されるセキュリティ水準に照らしつつ、リスクの重大性、対応の実現性、リスクの保有状態からのリスクの拡大の可能性も考慮し、対応策の決定（リスク対応）を行う。（指針本編Ⅱ.6.1.1.(1)から引用）

○リスク評価

－リスク分析の結果に基づく対応が必要なリスクの決定

－上記対応の優先順位付けの決定

－「安全基準等」の策定や見直しに係る基礎情報の作成

○リスク対応

－「安全基準等」の策定や見直しに係る基礎情報に基づく対応策、見直し策の決定

(2) 基本方針の策定・見直し

基本方針とは情報セキュリティ対策における根本的な考え方を示したものである。重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を規定する。

また、基本方針の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。（指針本編Ⅱ.6.1.1.(2)から引用）

○情報セキュリティ基本方針の策定

○情報交換の方針の策定

1.2 「規定」の観点

(1) 内規の策定・見直し

策定・見直しをした基本方針に基づき、個々の情報セキュリティ対策を体系化した上で、実施に係る考え方、ルール等について規定する。

また、内規の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。（指針本編Ⅱ.6.1.2.(1)から引用）

○情報セキュリティ関係規定の策定、見直し

－情報セキュリティ対策の方法や程度を意思決定するためのしくみや体制

－平時、障害発生時の指揮命令系統の明確化

・権限移譲、代行順位の決定　　等

－ＩＴ障害時の連絡不可能な場合（通信途絶等）の緊急時行動ルールの確定

－雇用契約時における情報の守秘や非開示の契約の締結

－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　　等

－電子計算機、アプリケーション、通信回線及び通信回線装置の目的外利用の禁止

・閲覧可能なwebサイトの制限

・私的目的による使用の禁止　　等

－ネットワークのアクセス制御方針の策定

－ネットワーク構成等に係る情報の秘匿

－事業者支給以外のシステム関連機器による情報処理の制限

－証跡管理に係る利用者への周知

－違反への対処

－例外措置等

○情報セキュリティ人材の育成、活用、管理に係る規定の策定、見直し

－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の活用による社内人材育成マップ等の作成

－情報システムユーザースキル標準等の活用による社内教育コース等の整備

(2) IT-BCP 等の策定・見直し

指針でいうIT-BCPとは、サービス維持レベルを下回る原因となるＩＴ障害発生時等において、情報システムを早期に復旧させ、サービスを継続して提供するために必要な行動手順で構成されるものである。ＩＴ障害発生時における優先業務、必要な対策を決定するまでの過程、業務継続方法、連携を要する関連部門等を規定する。

規程に際しては、広域災害・複合障害や新型インフルエンザ等の社会全体で対応が望まれる脅威、相互依存関係にある重要インフラからの障害波及、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等についても考慮する。

なお、ＩＴ障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含む必要がある。（指針本編Ⅱ.6.1.2.(2)から引用）

○IT-BCPの策定と定期的な見直し

－IT-BCPの実施優先順位と判断基準の明確化

－IT-BCPの実施条件の明確化

－ＩＴ障害発生時の体制の整備

－ＩＴ障害に係る情報集約及び共有体制（所管省庁への連絡体制を含む）の整備

－ＩＴ障害時の連絡不可能な場合（通信途絶等）の緊急時行動ルールの確定

－IT-BCPと情報セキュリティ対策との間の整合性確保

(3) 情報の取扱いについての規程化

取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、移送、提供、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。

なお、個人情報については、国民の安心感への影響に鑑みた取扱いを規定する。

（指針本編Ⅱ.6.1.2.(3)から引用）

○情報の取扱規定の策定、見直し

－情報漏えいを抑止するための役割や責任分担の明確化

－情報資産の洗出し方法

・体制

・洗出し項目

・洗出し基準　　等

－情報の分類

・分類の指針

・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）

・リスクアセスメント結果に応じた分類　　等

－情報（とりわけ重要情報）、情報システムについての格付け（ランク付け）

・情報の格付けと取扱制限の決定（その実施は情報の作成、入手時）

・情報の格付けと取扱制限の見直し

・情報のラベル付け及び取扱い

・格付け（ランク付け）の継承、変更手続き　　等

○情報の作成、入手時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報の目的外作成、入手禁止

－情報の台帳等作成

○情報の利用時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

・アクセス制御

・情報へのアクセス履歴の保存

・出力制御

・離席時対策（端末ロック等）　　等

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報の目的外利用の禁止

－情報の利用に関連する許可及び届出（作業責任者や手続きの明確化を含む）

○情報の保存時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

・情報の保存期間に従った管理

・客観的に評価されたアルゴリズムによる暗号技術の利用による保護

・パスワード

・アクセス制御

・更新履歴管理の取扱い

・記録媒体（とりわけ取外し可能な媒体）の管理、保管

・複写

・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

・電子署名

・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）　　等

－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　　等

－端末への資料保管ルールや制限

－持出しに係るルールや制限

－作業担当者の識別、認証、権限付与

－保護すべき情報の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

・バックアップの分散、隔地保管　　等

○情報の移送時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報交換の方針及び手順

－情報の移送に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－移送時の手段の選択

－移送時の書面の保護対策

－移送時の電子的記録の保護対策

・パスワード設定

・客観的に評価されたアルゴリズムによる暗号技術の利用

・電子認証　　等

○情報の提供時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－情報の提供に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－情報交換の方針及び手順

－提供時の付加情報の削除

○情報の消去時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－情報の消去に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－電磁的記録の消去手続き

・消去の確認

・消去記録の保管　　等

○ＰＣや外部記録媒体の盗難、紛失、流失の防止

－入退室管理

－ＰＣや外部記録媒体の原則外部持ち出し禁止

－移動可能な機器や情報の盗難防止

○個人データの取扱い

－個人データ管理責任者の選定

－個人データを取り扱う職員の明確化

－役割及び責任と権限の明確化

・閲覧等の利用時における管理者の許可　　等

－退職後の個人情報保護規程

－個人データの取扱状況を確認できる手段の整備

・個人データ取扱い台帳の整備　　等

○情報漏えい発生時の対応方法

－責任や権限を有する担当者の選任

－緊急連絡体制の構築

－報告事項の明確化

－対応措置の明確化

－代替手段の明確化

1.3 「計画」の観点

(1) 情報セキュリティ対策に係るロードマップ及び計画の作成・見直し

> 方針の策定・見直し等に基づき、情報セキュリティ対策の具体的な達成目標が定められた際は、達成までの大まかなスケジュールであるロードマップ及びロードマップに基づき詳細化した計画を作成し、情報セキュリティ対策を進める。
>
> （指針本編Ⅱ.6.1.3.(1)から引用）

○情報セキュリティ対策に係るロードマップの作成、見直し

○情報セキュリティ対策に係る計画の作成、見直し

－IT-BCPにおける訓練計画の策定

1.4 「体制」の観点

(1) 予算・体制（委託先を含む）の確保

> 情報セキュリティ対策を計画に沿って進めるにあたり、システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保する。
>
> （指針本編Ⅱ.6.1.4.(1)から引用）

○体制の整備

－グループ会社も含めた情報セキュリティに係る組織体制の整備

・責任者

・責任部門

・委員会等の設置

・役割や責任分担の明確化　　等

－安全管理措置を講ずるための組織体制の整備

－ＩＴ障害発生時の体制の整備

・ＩＴ障害時の所管省庁への連絡体制

・ＩＴ障害に係る情報集約及び共有体制の整備

・緊急連絡ルールの確定

o 連絡先

o 連絡事項

o 連絡手段　　等

－DoS攻撃時等における通信事業者との連携体制の構築

－システム統合に伴うリスク管理体制の構築

○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

(2) 人材育成・配置・ノウハウの蓄積

システムにおける情報セキュリティ対策は複数の対策を組合せることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といったセキュリティ対策の水準を維持するための対応が必要である。

このことから、セキュリティ対策に係る担当者が変更となってもセキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行う。

また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＰＣ操作者も対象であることから、全社的に行う。

（指針本編Ⅱ.6.1.4.(2)から引用）

○ＩＴ障害発生時に対応ができる人材の計画的な育成

○情報セキュリティ対策や情報漏えい防止に係る教育、訓練

－計画の策定

○IT-BCPの教育及び教育記録の保管

(3) 外部委託における対策（管理体制・契約・ＩＴ障害時）

重要情報の漏えいや悪意のあるシステム操作等については、外部からの意図的な原因のみならず内部の意図的又は偶発的な原因にて生じることがある。この内部の意図的又は偶発的な原因は、重要インフラ事業者等の従業員のみならず、委託先によるものも含まれる。

このことから、外部委託先に係る管理体制については、外部委託可能な範囲の明確化や委託先の選定基準に基づく外部委託契約、外部委託先の業務管理等にて行う。特に従業員と同じレベルの情報セキュリティ対策や教育の実施、ＩＴ障害発生時の協力についての合意は必要である。（指針本編Ⅱ.6.1.4.(3)から引用）

○委託に係る対応項目の明確化

－委託目的

－委託可能な業務範囲

－委託元と委託先双方の責任分界点

－個人情報を扱う場合の要件

－委託先選定基準

・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（諸規定の整備を含む）

・障害発生時の対応力　　等

－委託先選定手続き

－委託に係る契約手続き

○委託先との基本契約の締結

－委託先の情報セキュリティ対策（委託元と同等以上）

－機密保持（機密保持契約）、情報やデータの目的外利用の禁止（確認書の提出を含む）

－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（ＩＴ障害発生時の対処方法を含む）

－監査への協力

－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）

－契約の解約や解除に係る事項

－契約終了時の情報資産の返却及び消去

○委託契約時における情報の守秘や非開示の契約の締結

○委託先との取決めに係る合意形成

－委託先による契約の遵守方法及び管理体制

－施設全体の運用業務全般にわたる取決め

○委託先管理

－提供する情報の最小化

－委託先に求める情報セキュリティ対策項目の周知、遵守（遵守方法を含む）

－取り扱う情報資産に応じた情報セキュリティ対策の選定

・委託先がアクセス可能な情報資産の制限

・データ等の取扱いに係る事項（保管場所、保管方法）

・保守用専用アカウントの設定

・委託先が再委託する際の対応策の整備　　等

－委託先作業時の申請手続き

－委託先による情報セキュリティ対策の実施状況の確認

・作業報告書の提出手続き　　等

－納品検査時の情報セキュリティ対策の確認

－定期点検、監査の実施

○ＩＴ障害発生時の対応策の整備

－重要インフラ事業者等としての対処方法の明示

・責任分界点の明示

・行動基準の規定

・外部要因による障害の防止

・問題発生時の対処の合意

o 他システムへの影響調査

・事実関係の確認

・委託先との情報共有

・緊急時及び平常時の連絡体制の整備（業界内、ベンダー等）

・利用者への説明責任に係る認識の共有

・ＩＴ障害対応の訓練、演習の計画及び委託先を含めた実施　　等

－ＩＴ障害発生時における委託先の措置

・対処方法の事前の通知

・連絡体制の整備

・異常検知ツールの活用

・障害箇所の切離し

・原因の特定

・修正プログラムの適用

・異常状態（攻撃を含む）の記録、保存　　等

1.5 「構築」の観点

(1) 情報セキュリティ要件の明確化・変更

重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機密性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。

その際、セキュリティホール、不正プログラム、DoS攻撃等の様々な脅威に対して導入を要する情報セキュリティ機能、未然防止対策及びＩＴ障害発生後の拡大防止・早期復旧の対策に要する機能をできる限り明示するとともに、そもそもの不正侵入を防止するための対策と許してしまった侵入がもたらす実被害を防止するための対策についても明示する。（指針本編Ⅱ.6.1.5.(1)から引用）

○不正侵入防止対策

－主体認証

・機能の選択、導入

o 知識認証

o 所有物認証

o 生体認証

o 多要素認証　　等

・主体認証情報の管理

o 客観的に評価されたアルゴリズムによる暗号技術の利用

o 認証パスワードの最低文字数の制限

o ＩＤ毎に異なる認証パスワードの設定

o 認証パスワードの定期変更　　等

・利用者ＩＤの管理

o 個人単位のＩＤ付与

o 不要ＩＤの削除

o ＩＤの不正使用防止機能の導入　　等

・不正使用検知時における主体認証の利用停止措置

－アクセス制御

・利用者属性以外に基づくアクセス制御機能の導入

o 利用時間や利用時間帯による制御

o 利用端末の識別

o 強制アクセス制御　　等

・利用者アクセスの管理機能の導入

o 利用者登録

o 特権管理

o 利用者パスワードの管理

o 利用者アクセス権のレビュー　　等

－権限管理

・権限管理機能の導入

・利用者ＩＤと主体認証情報の付与管理機能の導入

・利用者ＩＤと主体認証情報における代替手段等の適用　　等

－不正侵入対策

・不正アクセスの監視、検出機能（IDS）の導入

・不正アクセスの監視、検出、削除機能（IPS）の導入

・通信フィルタリング機能の導入

o ファイアウォール

o web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の機能の導入

・端末やゲートウェイ等におけるマルウェア対策ソフトウェアの導入、メンテナンスの実施

・未利用通信ポート等の閉鎖（非活性化）、マクロ実行の抑制

－他情報システムとの独立、接続点の最小化

－マルウェア対策

・ＯＳ／アプリケーションのセキュリティ設定

・マルウェア対策ソフトウェアの導入、パターンファイルの更新機能導入　等

○実被害防止対策

－不正使用対策

・取引制限機能の導入

・事故時の取引禁止機能の導入

・電子的価値の保護機能の導入

・暗号鍵の保護機能の導入

・電子メールの不正使用防止機能の導入

・webサイト閲覧の不正使用防止機能の導入　　等

－データ漏えい防止対策

・暗証番号等の漏えい防止機能の導入

・相手端末確認機能の導入　　等

－破壊や改ざんの防止対策

・排他制限機能の導入

・アクセス制限機能の導入

・不良データ検出機能の導入

・ファイル突合機能の導入　　等

－負荷分散

・トラフィックの分散処理

・本番機の多重化、予備機の設置

・負荷状態の監視制御機能の充実　　等

－冗長化

・通信経路の迂回措置

・通信回線の冗長化

・ネットワークの適切な管理や制御

・予備機の設置

・代替手段の整備

・代替手段及び代替手段に必要なシステムの準備

o 代替情報システムの作業手順書策定　　等

・アプリケーションを含めた情報システムの冗長対策

－早期発見に向けた対策

・不正取引の検知機能の導入

・異例取引の監視機能の導入

・データ改ざん（書換え）の検出機能の導入

・障害の検出機能の導入

・障害箇所の切分け機能の導入　　等

－早期回復に向けた対策

・障害時の縮退、再構成機能の導入

・取引制限機能の導入

・リカバリー機能の導入　　等

－証跡管理

・証跡管理機能の導入実施

・電子計算機、通信回線装置及び通信回線の監視と記録

・証跡の取得と保存

・取得した証跡の点検、証跡の分析及び報告　　等

○情報システム施設における安全区画の確保

－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

－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

・不正操作対策

・盗み見等の防止対策　　等

－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

・物品等の持込み、持出しの情報セキュリティ責任者の承認、記録

・ＰＣや外部記録媒体等の持込み制限

・作業の監視、モニタリング　　等

－防犯対策

・侵入防止装置の設置

・赤外線検知装置の設置

・トラップセンサーの設置

・記録用機器の使用制限

・盗難防止装置の設置　　等

○情報システム施設における防災対策

－建物の耐震や免震構造及び防火構造化

－設備の移動、転倒等防止対策

－防火対策

－落雷対策

－防水対策

－警報装置の設置

－非常口及び非常灯設置

－自家発電装置、無停電電源装置、予備電源の確保

－空調（加湿を含む）設備の冷却水の備蓄　　等

○情報システム施設に係る入退出管理（物理的な不正侵入の防止）

－障壁の設置

－最小限の施設表示

－施錠運用の実施

－主体認証機能の導入

－継続的に立ち入る者の承認

－侵入監視装置の設置

－入退出履歴の記録

－訪問者、清掃業者及び物品の搬出入業者の入退出管理

・身分の記録

・入室審査手順

・立入り制限区域の設定

・職員等の立会い、付添い運用

・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搬入物品等の受渡し　　等

○電子計算機に係る対策

－情報システムの受入れに係る対策

・必要な要求事項（受入れ基準）の明確化

・受入れ前試験の合否判定基準の明確化

・受入れ前試験の実施　　等

－システム統合や更新に伴う移行基準の明確化

－ソフトウェア（アプリケーション）の利用に係る対策

・端末で利用可能なソフトウェアの制限

・利用するソフトウェア（アプリケーション）の使用者の責任と権限の明確化

・利用するソフトウェア（アプリケーション）の取扱手順の規程

・利用するソフトウェア（アプリケーション）の利用状況の確認　　等

－記録媒体を持たない端末の利用

－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機能

・モバイル端末で利用する電磁的媒体における客観的に評価されたアルゴリズムによる暗号化機能

・遠隔ロック機能

・遠隔消去機能　　等

－無線LAN使用時の対策

・客観的に評価されたアルゴリズムによる暗号技術の利用

・主体認証機能

・機器識別機能

・証跡管理機能

・アクセス制限機能

・他ネットワークの利用制限機能

・機密性確保

・接続（利用）可能な機器の管理　　等

－リモートアクセス時の対策

・主体認証機能

・証跡管理機能

・アクセス制限機能

・機密性確保

・利用可能な機器の管理　　等

○バックアップ稼働計画、復帰計画の策定

○内部関係者による取扱いミス等を低減させるための措置

－取引制限機能の導入

－事故時の取引禁止機能の導入

－電子的価値の保護機能の導入

－暗号鍵の保護機能の導入

－電子メールの不正使用防止機能の導入

－webサイト閲覧の不正使用防止機能の導入

－外部ネットワークからのアクセス制限

－不正侵入防止機能の導入　　等

○内部関係者による情報漏えいを抑止するための措置

－入退出管理

－常時監視設備（カメラ）等の設置　　等

○内部からの攻撃の監視

－職員の監督とモニタリング　　等

○重要情報の内部漏えい、盗難、紛失、流出への対策

－移動可能な機器の盗難防止策

－情報盗難の防止等の措置　　等

(2) 情報セキュリティ対策（技術）に係る設計・実装・保守

> 情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。
>
> また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。（指針本編Ⅱ.6.1.5.(2)から引用）

○対応対象となったセキュリティ要件の実装

○信頼性設計、処理増加等を考慮した情報システムの余裕設計

○セキュリティ要件の実装に付随する機器に係る対応

－開発環境と本番環境の分離

－供給元及び更新情報、保守期間等が明確な機器の利用

－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）

－客観的に評価された製品等の導入の検討

－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

・警報装置の設置

・非常口及び非常灯設置　　等

－自家発電装置、無停電電源装置、予備電源の確保

－空調（加湿を含む）設備の冷却水の備蓄

－サーバー装置における客観的に評価されたアルゴリズムによる暗号技術の利用（遠隔保守時）

－改ざん防止対策

○セキュリティ要件の実装に付随する性能に係る対応

－電子計算機の十分な性能（処理能力、容量、拡張性）の確保

－通信性能の確保

○セキュリティ要件の実装に付随するネットワークに係る対応

－外部ネットワークとの接続制限（プロキシ経由等）

－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

－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

－公開するサーバー上に保存する情報の制限

－改ざん防止対策

－盗聴防止対策

－ルーターによるDoS攻撃対策　　等

○セキュリティ要件の実装に付随する通信に係る対応

－相手端末確認機能の導入

－未承認機器からの通信の遮断

－電子証明書による正当性の証明

－通信情報（データ）における客観的に評価されたアルゴリズムによる暗号技術の利用

－遠隔地からの保守（リモートメンテナンス）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ーの限定）

－不特定多数が接続するネットワークとの接続禁止　　等

○セキュリティ要件の実装に付随するアプリケーションに係る対応

－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　　等

○セキュリティ要件の実装に付随する電子メールやwebに係る対応

－電子メールの対策や制限

・添付ファイルの保護

・不正中継禁止

・送受信容量の制限

・自動転送の制限

・業務外利用の禁止

・送信先アドレス漏えいの防止

・電子署名機能の導入

・客観的に評価されたアルゴリズムによる暗号技術の利用

・迷惑メールフィルターの導入　　等

－電子メール送信時及び受信時の送信ドメイン認証（ＳＰＦ等）の導入

－webにおける特殊文字使用の禁止、無効化

－webにおける脆弱性のある作込みの回避

－攻撃に利用されるwebサーバー情報の送信を防ぐ対策

○セキュリティ要件の実装に付随するその他に係る対応

－手順書等における文書整備、変更管理手順の明確化

・仕様書、設計書

・構成要素のセキュリティ

・マニュアル

・機種や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

・利用者管理、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

－変更管理

－運用終了に伴う廃棄計画や手順の策定、設計や見直しの実施

－電磁的記録（媒体）の情報抹消

－パンデミック対策（コンピューターセンターのオペレーター要員の確保等）

－マルウェア対策の対応内容の記録

(3) 情報セキュリティ対策（運用）に係る設計・手順化・保守

> 情報セキュリティ要件に応じて情報セキュリティ対策を実装した情報システムの運用設計・手順書化を経て、安定した運用を実現する。また、情報セキュリティ対策の有効性を維持するため、認証に要するユーザー登録等の保守をもれなく行う。（指針本編Ⅱ.6.1.5.(3)から引用）

○予兆検知時、ＩＴ障害発生時や緊急時の対応（早期発見、早期回復）手順の整備

－監視

－障害の検出

－異常発見時における管理者への連絡

－障害箇所の切分け

－障害時の縮退、再構成

－取引制限

－リカバリー　　等

○運用体制の決定、周知

－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　　等

○取扱手順等の策定

－情報の取扱手順

－利用する外部作成ソフトウェアのセキュリティホールに係る定期チェック手順

－マルウェアに係る定期チェック手順

－HTMLメール使用時の注意　　等

○情報漏えい発生時の対処手順

－事実関係の把握

－漏えい情報の範囲の特定

－システム、端末における情報漏えい経路の特定の調査

－情報漏えい継続の阻止、被害の最小化

・対象通信を遮断するための運用フロー等の整備

・対象サーバー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等

－本人への通知

－事実関係の公表、広報

－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や原因等の解析

－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

2. 「Ｄｏ（実働）」の観点

2.1 「平時・障害発生時共通」の観点

(1) 情報セキュリティ対策の運用（監視・統括）

> 構築した情報セキュリティ対策の運用状況については、定期的に責任者が把握していることを常態化する。（指針本編Ⅱ.6.2.1.(1)から引用）

○実装したセキュリティ対策機能の運用

○セキュリティ対策機能に係る運用

－電子計算機、通信回線装置及び通信回線の異常（非日常）状態、不正行為、不正アクセス及び不正トラフィックの監視、検知、報告

・アクセスログの取得、確認、保管

・侵入検知システム（IDS）による検知

・マルウェア対策ソフトウェアによる定期チェック　　等

－証跡の分析、結果報告

－通常時や繁忙時のシステムの性能、容量、処理能力等の稼働状態監視による異常検知、報告

－運用管理記録、障害記録、作業記録の作成、管理、報告

－外部委託業者の作業管理

(2) 情報セキュリティ対策の運用状況把握

> 経営層は、情報セキュリティ対策の運用状況について、把握する。
> （指針本編Ⅱ.6.2.1.(2)から引用）

○情報セキュリティ対策の運用状況に係る報告事項の確認

2.2 「平時」の観点

(1) 情報セキュリティ対策の運用（予兆の把握、パスワード変更等）

> 情報システムの運用状況が平時の状況やしきい値と比して異なる状況にあることを検知し、予兆を把握する。
>
> また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等といった登録値の変更等を通じて、セキュリティ対策の水準を維持する。
>
> 加えて、情報セキュリティに係る教育を全社的に行う。
>
> （指針本編Ⅱ.6.2.2.(1)から引用）

○実装したセキュリティ要件機能の運用

○セキュリティ対策機能に係る運用

－情報システムの定期的な点検及び必要に応じた更新

－データ改ざん有無の定期的な検査

－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

－情報システムの構成管理（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

－マルウェア対策ソフトウェアの適用

・マルウェア情報の収集

・マルウェア対策ソフトウェアによる定期チェック

・定義ファイルの更新

・対応内容の記録

－利用するＯＳ、ソフトウェア等の定期的な調査、把握

－利用するＯＳ、ソフトウェア等の管理、同バージョン管理

－利用するＯＳ、ソフトウェア等の脆弱性対応

・情報収集

・対応計画の策定

・定期チェック

・セキュリティパッチの適用

・対応内容の記録　　等

－無線LANにて接続可能な機器の管理

－ソフトウェアダウンロード時の電子署名による配布元の確認

－外部委託業者の作業の確認、点検

－入退室管理

・施錠

・主体認証

・記録

・継続的に立ち入る者の承認

・身分証明書の携帯、常時視認

・侵入監視装置による監視

・コンピューターや外部記録媒体等の持込み制限　　等

－訪問者、清掃業者及び物品の搬出入業者の管理

・職員等の立会い、付添い

・ストラップ、ＩＤ カードの情報システムに接触できない場所での受渡し

・作業の監視　　等

－利用する機器、利用者及び識別コードの管理

○規定に従ったＰＣや外部記録媒体の盗難や紛失の防止に係る運用

○情報取扱手順等の遵守状況の確認

－対象文書保存の際のパスワード、客観的に評価されたアルゴリズムによる暗号技術の利用

－電子メール送信の際の宛先確認　　等

○情報セキュリティ対策や情報漏えい防止に係る教育及び訓練の実施

－教育及び訓練実施記録の保管　　等

○セプターカウンシルの活用等によるリスクコミュニケーションの実施

○情報漏えい発生時の措置

－管理者への連絡

－適切な処置の実施　　等

(2) 情報セキュリティ対策状況の対外説明

> 国民の安心感の醸成に資するため、重要インフラにおけるサービスの持続的な提供に向けた情報セキュリティ対策の取組について、提供範囲に留意しつつ、情報セキュリティ報告書やwebサイト等にて対外的な説明に努める。
>
> （指針本編Ⅱ.6.2.2.(2)から引用）

○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

○webサイト、電子メール等による情報提供

2.3 「障害発生時」の観点

(1) ＩＴ障害に対する防護・回復

> 策定したIT-BCPを発動し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、ＩＴ障害をもたらした原因への適切な対処を可能とする。
>
> （指針本編Ⅱ.6.2.3.(1)から引用）

○情報システムの稼働監視（トラブル時の復旧時間、再発防止策の実施状況）

－不正アクセスの監視

－不正トラフィックの監視　　等

○対応体制の準備

－重要拠点（指揮拠点）の確保

－複数の連絡手段の準備、確保

－自家発電装置等で使用する燃料の確保　　等

○早期復旧に向けた対応

－障害箇所の切分け

－障害時の縮退、再構成の実施

－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

－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

－障害時の取引制限の実施

－障害時のリカバリー機能の適用

－取得した証跡に基づく追跡、分析及び報告

－様々な主体が提供する災害や障害発生時の情報サービスの活用　　等

○攻撃記録の保存

○攻撃に係る情報の関係機関との共有

○対外的な情報発信、情報共有

○広報、利用者からの問い合わせへの対応

(2) 情報セキュリティ対策状況の対外説明

> ＩＴ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に沿って、情報に基づく対応の5W1Hの理解のもと、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う。
>
> （指針本編Ⅱ.6.2.3.(2)から引用）

○サービス停止状況、復旧（見込み）情報の提供

3. 「Check（確認）・Act（是正）」の観点

3.1 「平時」の観点

情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象及びその結果をリスクとしての特定（リスク特定）を行う。

特定したリスクについて、定性又は定量的な分析（リスク分析）を行い、事業にどのような損害を与えるかといった具体的な影響を決定する。

リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。（指針本編Ⅱ.6.3.1から引用）

○情報セキュリティ対策の運用を通じた課題抽出

－業界内での相互支援に備えたデータ形式の標準化推進　　等

○内部監査や外部監査を通じた課題抽出

－自己点検の実施

・防災対策の定期的な確認　　等

－内部監査による情報セキュリティ監査等の実施

－外部監査による情報セキュリティ監査等の実施　　等

○ＩＴに係る環境変化に伴う脅威に対する課題抽出

－平時からの情報収集の実施

－継続的な情報収集

－新たな脅威が顕在化した時点で速やかに検討体制が構築できるための準備

－「暗号危殆化」に係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」に係る継続的な情報収集と実装検討の実施　　等

○演習や訓練を通じた課題抽出

－システム統合や更新に伴う情報システムの業務運営体制の検証

－IT-BCPに係る訓練の実施、訓練実施記録の保管

－障害時、緊急時を想定した訓練（復旧テスト等）の実施　　等

○リスク特定

－課題抽出の中でのリスク源となり得る脅威や脆弱性の発見

－リスク源の影響を受けるサービスレベルの特定

－脅威や脆弱性から生じ得る事象とその結果をリスクとして特定　　等

○リスク分析

－特定したリスクに対する定性的又は定量的な分析

－事業にどのような損害を与えるか等の具体的な影響の決定　　等

3.2 「障害発生時」の観点

ＩＴ障害対応（検知・回復）を通じた課題抽出として、取組の中で発見したリスク源となった脅威や脆弱性、影響を受けた維持すべきサービスレベル、脅威や脆弱性から生じた事象及びその結果をリスクとしての特定（リスク特定）を行う。

特定したリスクが事業に与えた損害を、リスク分析結果として改めて整理する。

リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。（指針本編Ⅱ.6.3.2から引用）

○ＩＴ障害対応（検知・回復）を通じた課題抽出