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）

平 成 ２ ７ 年 ５ 月 ２ ５ 日

サイバーセキュリティ戦略本部

（本ページは白紙です。）

目次

Ⅰ．目的及び位置付け……1
1. 重要インフラにおける情報セキュリティ対策の重要性……1
2. 「安全基準等」の必要性……1
3. 「安全基準等」とは何か……2
4. 指針の位置付け……2
5. 指針の構成……5
6. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待……5

Ⅱ．「安全基準等」で規定が望まれる項目……6
1. 「安全基準等」策定の目的……6
2. 「安全基準等」の対象範囲……6
3. 「安全基準等」において対象とする原因……6
4. 役割……7
5. 「安全基準等」の公開……8
6. 対策項目……8
   6.1 「Plan（準備）」の観点……8
   6.2 「Ｄｏ（実働）」の観点……11
   6.3 「Check（確認）・Act（是正）」の観点……12

（本ページは白紙です。）

Ⅰ．目的及び位置付け

1. 重要インフラにおける情報セキュリティ対策の重要性

「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成26年５月19日　情報セキュリティ政策会議決定。平成27年５月25日サイバーセキュリティ戦略本部改訂。）（以下「行動計画」という。）にあるとおり、重要インフラ[1]におけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害[2]が国民生活及び社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともに、ＩＴ障害発生時においては迅速な復旧と再発防止を図るために、情報セキュリティ対策は重要である。

情報セキュリティ対策の実施においては、当該重要インフラ分野及び重要インフラ事業者等[3]の特性を踏まえつつ、一義的には重要インフラ事業者等が自らの責任においてPDCAサイクルに沿って適切かつ継続的に実施・改善することが必要である。

その際、情報セキュリティ対策[4]は各重要インフラ事業者等における事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、リスクマネジメントと情報セキュリティ対策が整合する取組となるように留意する。

具体的には、これらが整合するよう情報セキュリティ対策を経営層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営層も関与した全社的な体制の下で情報セキュリティ対策に取り組むことが期待される。

情報セキュリティ対策の適切かつ継続的な改善が個々の重要インフラ事業者等のみならず重要インフラ全体の防護につながるものとの認識の下、官民が一丸となった取組を通じて、国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指すものである。

2. 「安全基準等」の必要性

効果が見えにくい情報セキュリティ対策の推進において特に重要なのは、重要インフラ事業者等が自らの状況を正しく認識し、自らの情報セキュリティ対策の水準を規

---

[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] 「ＩＴ障害」とは、ＩＴの不具合のうち、重要インフラサービスの提供水準が行動計画の「別紙２　重要インフラサービスとサービス維持レベル」における「サービス維持レベル」を下回るものを指す。

[3] 「重要インフラ事業者等」とは、重要インフラ分野に属する事業を営む者等のうち行動計画の「別紙１　対象となる重要インフラ事業者等と重要システム例」における「対象となる重要インフラ事業者等」に指定された事業者等及び当該事業者等から構成される団体を指す。

[4] ここでいう「情報セキュリティ対策」とは、リスクマネジメントや対策の実装といった情報セキュリティに係る取組全般を指す。

範等に照らした上で、PDCAサイクルに沿って適切かつ定期的に自らの情報セキュリティ対策を実施・改善することである。

この対策を実施・改善することに際し必要となるのが「安全基準等」である。「安全基準等」は、それぞれの重要インフラ分野及び当該事業者等の特性に応じた情報セキュリティ対策の水準を明示したものである。

なお、「安全基準等」において、情報セキュリティ対策については未然防止、ＩＴ障害発生後の拡大防止・早期復旧及び再発防止のバランスが取れていることが期待される。

3. 「安全基準等」とは何か

各重要インフラ事業者等は、一般に「業法」と呼ばれる法制度の下に国が定める様々な基準に従い、業を営んでいる。[5]

このことを踏まえ、指針においては

①業法に基づき国が定める「強制基準」

②業法に準じて国が定める「推奨基準」及び「ガイドライン」

③業法や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」

④業法や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」

等、いずれかの形で各事業者等が行う様々な判断や行為に際し、基準又は参考にするものとして策定された文書類を「安全基準等」と呼ぶ。

求められる情報セキュリティ対策が確実になされるためには、これら「安全基準等」において情報セキュリティ対策の目的、適用範囲、対象とする原因、役割、項目及び水準が文書として明示されることが必要であり、上記①から④までを一覧することにより重要インフラの事業に携わる全ての関係者が情報セキュリティ対策の各プロセスにおいて「自らが何をすべきか」が理解できる文書であることが期待される。

4. 指針の位置付け

情報セキュリティ対策の実施において重要でありかつ困難なことは、重要インフラ事業者等が自らの状況を正しく認識し、「安全基準等」に照らした上で「どのような対策をどの程度で行うか」を判断することであり、その判断に基づき対応する各プロセスにおいてモニタリング及びレビューを組み込み、実践することである。

このことから指針の目的は「安全基準等」の策定・改訂を通じた情報セキュリティ

[5] 地方公共団体は、地方自治法に基づき、地域における行政を自主的かつ総合的に実施している。

対策水準の維持・向上、とりわけ対策途上や中小規模の重要インフラ事業者等による実効的かつ自主的な取組に資することとした。

また、この策定・改訂時における指針の参照を念頭に置き、情報セキュリティ対策の実効性をより高めるために、情報セキュリティ対策の事項を指針第３版までの「４つの柱と５つの重点項目」の観点に沿った列記から、指針第４版からはPDCAサイクルに沿っての列記とした。

具体的には行動計画の「図表３　『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』」（PDCAサイクル）に沿って列記した（本図表については、指針において図表１として再掲する。）。[6]

列記に際しては、サイバー攻撃等の意図的な原因、ユーザーの操作ミスや他の重要インフラ分野のＩＴ障害からの波及等の偶発的な原因、災害や疾病等の環境的な原因等を念頭に置き、重要インフラ分野を横断的に俯瞰して必要度が高いと考えられる項目及び先進的な取組として参考とすることが望ましい項目を採録した。

各重要インフラ事業者等においては、情報セキュリティ対策における自らのPDCAについて、例示する図表１等に照らし、充足と不足を明らかにした上で改善するといった取組を通じて、継続的な改善を確実なものとすることが期待される。

加えて、本書の活用による「安全基準等」の策定・改訂に際しては、以下２点を留意されたい。

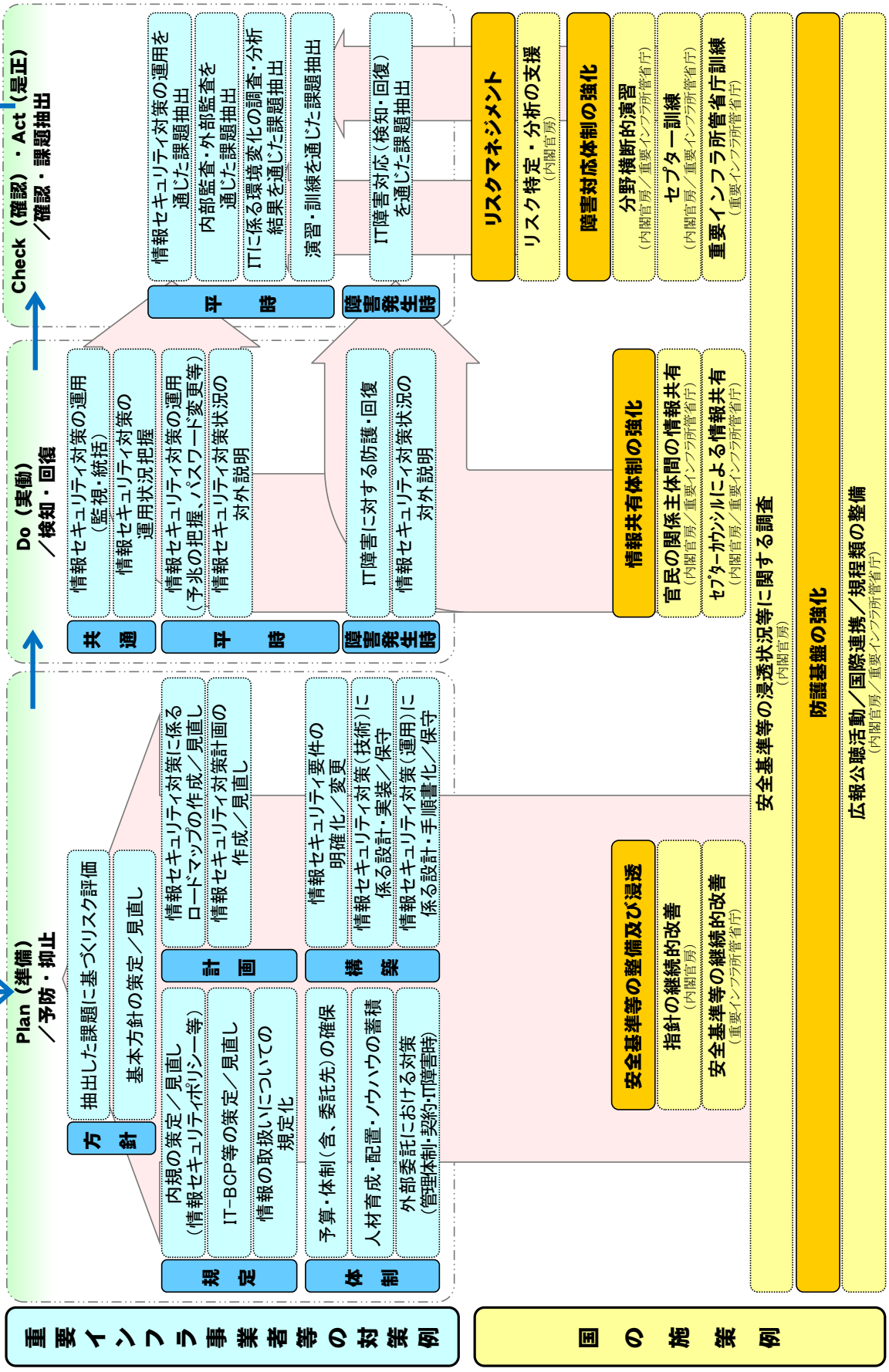
○重要インフラ分野又は重要インフラ事業者等によっては、その事業の態様等の理由から指針の記載項目の中に規定する必要がないものを含むことがあり得ること

○重要インフラ分野又は重要インフラ事業者等によっては、その事業の態様等の理由から指針に未記載の項目であっても規定する必要がある場合があり得ること

なお、指針に記載の各項目及び当該項目の水準等を「安全基準等」のどの文書にて規定するかは各業法や既定の「安全基準等」の構成等を踏まえ、重要インフラ分野又は重要インフラ事業者等ごとに検討されることを期待する。

[6] 指針は、各関係主体に国際標準への準拠を求めるものではなく、内閣官房が適用する考え方に沿った対策の事項を列記したもの。このことから指針を通じて、本図表による PDCA サイクルそのものを採り入れることを求めるものではなく、重要インフラ事業者等が既に自組織において規定・適用している安全基準等の更なる適正化及び情報セキュリティ対策の水準の向上に資することを目的としている。

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」



5. 指針の構成

指針は、安全基準等の必要性及びその中で規定することが望ましい項目を訴求する本書「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）」（以下「指針本編」という。）に加え、指針本編に記載する情報セキュリティ対策項目の具体例を記載した項目集である「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」（以下「指針対策編」という。）及び各重要インフラ事業者等が自らの組織に最も相応しい情報セキュリティ対策を指針対策編の項目に照らして構築し、維持・改善していくための優先順位付け等に焦点を当てながら、その防護対策の有効性を高めていくための「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）」（以下「指針手引書」という。）にて構成する。

なお、指針手引書において情報セキュリティ対策の優先順位付けに係る考え方を示すことから、指針第３版にて記載の要検討事項及び参考事項については記載を削除する。各事業者等による対策の優先順位付け及びそれに応じた対応を期待する。

また、指針対策編及び指針手引書については指針本編の別冊と位置付け、重要インフラ専門調査会[7]にて取りまとめることとする。

6. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待

重要インフラ事業者等がPDCAサイクルに沿って適切かつ定期的に自らの情報セキュリティ対策を実施・改善するためには、「安全基準等」に照らした自己検証が重要である。このことから「安全基準等」についても、指針に示された項目を満たすことに止まらず、新たな知見・技術・システムやそれに伴う新たなリスク等に応じた改善に向け、随時検討がなされることを期待する。

このような観点からは、各種規格をはじめとする国内外のベストプラクティスの積極的な参照に加え、「政府機関の情報セキュリティ対策のための統一基準」及び関連文書の適宜参照をすることが望ましい。

また、「安全基準等」の浸透に向けて、「安全基準等」にて定められた情報セキュリティ対策の推進に加えて、同対策を実装するための環境整備にも努めることを期待する。

[7] 「重要インフラ専門調査会」は、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行う専門調査会として置かれている。（「重要インフラ専門調査会の設置について」（平成 27 年２月 10 日サイバーセキュリティ戦略本部決定）より）

Ⅱ.「安全基準等」で規定が望まれる項目

1. 「安全基準等」策定の目的

サービスの持続的な提供を阻害する原因となるＩＴ障害に対し、未然防止、ＩＴ障害発生後の拡大防止・早期復旧及び再発防止に係る情報セキュリティ対策を確実に実施していくためには、「安全基準等」に照らした同対策の推進や実装が必要である旨を記載する。

2. 「安全基準等」の対象範囲

重要インフラ事業者等は、国民に対する重要インフラサービスの安定的供給や事業継続等といった事業目的の達成に向け、行動計画の「別紙２　重要インフラサービス[8]とサービス維持レベル」を踏まえ、重要インフラ事業者等が提供するサービスを明確にするとともに、情報システム及びその中で利活用されるデータのうち情報セキュリティ対策にて守る対象及びその防護の水準を可能な限り具体的に「安全基準等」に規定する。

その際、サービスの持続的な提供に密接に関連する全ての構成要素を守る対象として考慮することが望ましい。守る対象の一例として、下記が想定される。

○情報資産（情報システム及びその中で利活用されるデータ）
○情報システム間でやりとりされるトランザクション[9]又はビジネスプロセス
○情報システムの開発・運用・保守

3. 「安全基準等」において対象とする原因

重要インフラサービスの安定的供給や事業継続等への影響がないように、顕在化する可能性が高いＩＴ障害を想定した上で、そのＩＴ障害の原因を各重要インフラ分野及び各重要インフラ事業者等の特性等を可能な限り具体的に考慮し、規定する。

対象とする原因の一例として、下記が想定される。

①意図的な原因

不審メール等の受信、ユーザーＩＤ等の偽り、DoS攻撃等の大量アクセス、情報の不正取得、内部不正、適切なシステム等運用の未実施　等

②偶発的な原因

[8] 「重要インフラサービス」とは、重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続きのうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに行動計画の「別紙２　重要インフラサービスとサービス維持レベル」に定めるものを指す。

[9] トランザクションとは、関連する複数の処理を一つの処理単位としてまとめたもの。一連の作業を一つの処理として管理するために用いる。

ユーザーの操作ミス、ユーザーの管理ミス、不審なファイルの実行、不審なサイトの閲覧、外部委託先の管理ミス、機器等の故障、システムの脆弱性、他分野の障害からの波及　等

③環境的な原因

災害、疾病　等

4. 役割

それぞれの情報セキュリティ対策を担う主体が明確になるよう、重要インフラ所管省庁が担う役割、重要インフラ分野全体として担う役割及び各重要インフラ事業者等が担う役割を規定する。

加えて、行動計画にて定めた「重要インフラ事業者等の経営層の在り方」及び図表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』」を参照の上、経営層の取組を「安全基準等」に規定する。

なお、行動計画にて定めた「重要インフラ事業者等の経営層の在り方」を以下に引用する。

関係主体の在り方

－自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。

－ＩＴ障害の規模に応じて、情報に基づく対応の 5W1H を理解しており、ＩＴ障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

－上記の目的達成に当たっての情報セキュリティを中心とするリスク源の認識。

－上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。

－システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営資源の継続的な確保。

－システムの運用状況の把握等を通じた当該方針の実行の有無の検証。

－演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の検証及び改善策の有無の検証。

5. 「安全基準等」の公開

国民生活及び社会経済活動への影響が大きい重要インフラが国民の安心感の醸成に資するための取組のひとつとして、可能な限り「安全基準等」の公開を通じた重要インフラ防護への取組を明示する。

その際、公開による脅威の増大等が想定される項目等については、当該項目等が非公開であること及びその理由を明示する。

6. 対策項目

各重要インフラ分野における「安全基準等」の策定・改訂においては、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』」に沿って列記した以下項目の採否を検討する。

6.1 「Plan（準備）」の観点

6.1.1 「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。

(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。

6.1.2 「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。

(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。

規定に際しては、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特定の都市又は地域に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。

(3) 情報の取扱いについての規定化

取り扱う情報の重要度に応じて、機密性[10]、完全性[11]、可用性[12]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、個人データについては、国民の安心感への影響に鑑みた取扱いを規定する。

6.1.3 「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。

6.1.4 「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。

(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み合わ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

---

[10] 指針では、情報にアクセスすることが認められた者だけが情報にアクセスできる状態を確保すること（情報が漏えいしても影響を及ぼさないよう情報の秘匿性を確保することを含む。）を指す。

[11] 指針では、情報が破壊、改ざん又は消去されていない状態を確保することを指す。

[12] 指針では、情報にアクセスすることを認められた者が必要なときに中断されることなく情報にアクセスできる状態を確保することを指す。

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。

(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、外部委託の適否及びその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。

6.1.5 「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[13]を防止するための対策についても明示する。

(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。

[13]実被害の例としては、情報窃取、情報システムの破壊等が挙げられる。

(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。

6.2 「Ｄｏ（実働）」の観点

6.2.1 「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。

(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。

6.2.2 「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等を検知し、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。

(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。

6.2.3 「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。

(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の理解の下、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。

6.3 「Check（確認）・Act（是正）」の観点

6.3.1 「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に鑑みてリスクを特定（リスク特定）する。

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。

6.3.2 「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。