資料 4-1

重要インフラにおけるサイバーセキュリティ確保に係る
安全基準等策定指針
（骨子案）

令和４年12月22日

内閣官房内閣サイバーセキュリティセンター
重要インフラグループ

目次

Ⅰ. 目的及び位置付け 1
1. 重要インフラにおけるサイバーセキュリティの確保の重要性 1
2. 「安全基準等」とは何か 1
3. 安全基準等策定指針の位置付け 1
Ⅱ. 組織統治におけるサイバーセキュリティ 3
1. 組織方針 3
2. 組織内外のコミュニケーション 3
3. 体制の構築 4
4. リスク対応 4
5. 監査・情報開示 5
6. 継続的改善 5
Ⅲ. リスクマネジメントの活用と危機管理 6
1. 組織状況の理解 6
2. リスクアセスメント 6
3. サイバーセキュリティリスク対応 7
4. サプライチェーン・リスクマネジメント 7
5. 事業継続計画等の作成 8
6. 人材育成・意識啓発 8
7. CSIRT 等の整備 8
8. 平時の運用 9
9. 危機管理 9
10. 演習・訓練 9
11. モニタリング・レビュー 9
12. 継続的改善 9
Ⅳ. 対策項目 11
1. ランサムウェア対策 11
2. クラウドサービス利用時の対策 11
3. 組織的対策 11
4. 人的対策 13
5. 物理的対策 13
6. 技術的対策 13

Ⅰ．目的及び位置付け

1. 重要インフラにおけるサイバーセキュリティの確保の重要性

・ 我が国の国民生活及び社会経済は、重要インフラサービスの安全かつ継続的な提供に依存している。安全で安心な社会の実現には、任務保証の考え方[1]を踏まえ、重要インフラのサイバーセキュリティを確保し、強靱性を高めることが不可欠である。

・ 経営層から担当者層まで組織一丸となって、リスクマネジメントによる事前対応と、障害発生後の拡大防止・早期復旧の両面からサイバーセキュリティの確保に取り組むことが重要である。

2. 「安全基準等」とは何か

・ 各重要インフラ事業者等は、当該事業分野に関する法制度の下、関係する基準に従い、業を営んでいる。本文書（以下「安全基準等策定指針」という。）においては、サイバーセキュリティの確保に関して、各重要インフラ事業者等の判断や行為に関する基準又は参考となる文書類を「安全基準等」と呼ぶ。

・ 安全基準等は、重要インフラ分野ごとにその特性に応じて策定され、次の①～④に分類される。

① 関係法令に基づき国が定める「強制基準」

② 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」

③ 関係法令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 関係法令や国民・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

※安全基準等に該当する文書類は、「安全（Safety）」の実現のために作成されたものに限定されないことに留意。

・ セキュリティ対策の項目及び水準が安全基準等に明示され、重要インフラサービスに携わる全ての関係者に理解されていることが望まれる。

3. 安全基準等策定指針の位置付け

・ 安全基準等策定指針は、「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日サイバーセキュリティ戦略本部決定）に基づき、安全基準等の策定・改定を支援するために策定される。

・ 安全基準等策定指針には、各重要インフラ分野に共通して求められるサイバーセ

[1] サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」

キュリティの確保に向けた取組を整理・記載する。

- 各取組をどの安全基準等に定めるかについては、関係法令の規定及び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想定している。
- 安全基準等が一層高度かつ網羅的になるよう、関連する各種規格、国内外のベストプラクティス等も適宜参照することが望ましい。

Ⅱ．組織統治におけるサイバーセキュリティ

- 経営層向けを念頭とした取組を記載する。
- サイバーセキュリティに関するリスクが経営リスクの一つであり、さらに、その他の経営リスクに影響を及ぼすリスクであると捉え、セキュリティ対策の実施を通じてサイバーセキュリティに関するリスクを許容水準まで低減することは、重要インフラ事業者等として果たすべき社会的責任であり、その実践は経営層としての責務であることを認識すること。
- 既存の組織統治[2]の取組（組織方針、体制構築、監査、情報開示等）においてサイバーセキュリティも扱うこと。
- 経済産業省「サイバーセキュリティ経営ガイドライン」、内閣サイバーセキュリティセンター（以下「NISC」という。）「サイバーセキュリティ関係法令 Q&A ハンドブック」が参考になる。

1. 組織方針

- 経営又はリスクマネジメントの方針にあたる文書の策定時に、サイバーセキュリティに関する事項も考慮すること。
  - ＊ 経営又はリスクマネジメントの方針にあたる文書に、「サイバーセキュリティに対する脅威からの被害がサービス提供のリスクの一つである」「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」といった要素を盛り込むことが望ましい。
- 組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定すること。
  - ＊ セキュリティ対策の目的や方向性
  - ＊ 関係主体等からの要求事項を満たすこと
  - ＊ 経営層によるコミットメント

2. 組織内外のコミュニケーション

- 組織内外のコミュニケーションにおいて、サイバーセキュリティに関するリスク、インシデント等の情報を取り扱うこと。
  - ＊ 組織内のコミュニケーションの仕組みの一部として、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設けること。
  - ＊ 新規サービス企画時等の内部協議プロセスの関係者にサイバーセキュリティを担当する部署を加えることが望ましい。

[2] 安全基準等策定指針では、コーポレートガバナンス・コード（2021 年 6 月 11 日株式会社東京証券取引所）におけるコーポレートガバナンス「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み」や、会社法（平成 17 年法律第 86 号）の求める内部統制システム「会社が営む事業の規模、特性等に応じたリスク管理体制」の構築を念頭に、組織の意思決定・管理に関する仕組みを意味するものとする。

＊　組織内外の関係者間でサイバーセキュリティに関する役割、責任分担、情報共有の体制等について意見交換を行うことが望ましい。

3. 体制の構築

・組織体制を構築する際に、サイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てる[3]こと。
・リスクマネジメントに係る責任者を取締役会に相当する場において任命する際に、サイバーセキュリティに関する責任者についても任命すること。
　＊　取締役に相当する者の中から CISO（最高情報セキュリティ責任者）を任命することが望ましい。
・責任者がサイバーセキュリティに関するリスク及びそれが業務運営に及ぼす影響を理解し評価できる体制を整備すること。
　＊　サイバーセキュリティに関する責任者は、サイバーセキュリティについて十分な知識及び技能を保持していることが望ましい。
　＊　サイバーセキュリティに関する責任者に対し、セキュリティ研修を実施することが望ましい。

4. リスク対応

・組織方針を踏まえて組織全体としてのリスクを整理する際に、サイバーセキュリティに関するリスクが経営リスクの一つであり、さらに、その他の経営リスクに影響を及ぼすリスクであると捉えること。
　＊　重要インフラサービスの提供に不可欠な情報システムは何か、それらがどのようにサイバー脅威にさらされる可能性があるか、どのようなセキュリティ対策をとるべきかを理解することを念頭に、サイバーセキュリティに関するリスクについて可能な限り理解するよう努める[4]ことが望ましい。
・サイバーセキュリティに関するリスク分析結果を踏まえて、組織全体のリスク評価を実施すること。
・組織全体のリスク対応の一部として、サイバーセキュリティに関するリスク対応を実施すること。
・セキュリティ対策に必要な資源（予算・人材等）について、組織の価値を維持・増大していく上で、組織活動におけるコストや損失を減らすために必要不可欠な投資であるとの考え方[5]のもとで配分すること。
・自組織にとどまらず、ビジネスパートナーや委託先等、サプライチェーン全体に

[3] 適切な管理体制の構築を前提としつつ、サイバーセキュリティに関する専門的な事項については、外部委託、業界団体との連携等により補完してもよい。
[4] サイバーセキュリティに関する事象の発生頻度を見積ることが困難な場合には、被害シナリオを検討し、その被害を抑制するための方法を検討するなどのアプローチがあり得る。
[5] 一般に、セキュリティ対策への投資による直接的な収益を算出することは困難であり、サイバーセキュリティに関しては考え方の転換が必要。

わたるセキュリティ対策への目配り[6]を行うこと。
- 重要インフラサービス障害発生時における初動から完全復旧までの対応方針（事業継続計画等）の一部として、情報システムに係る対応方針[7]を策定すること。

5. 監査・情報開示

- 内部監査・監査役等監査[8]の一部としてサイバーセキュリティに関する監査を実施すること。
- 既存の開示制度を積極的に活用し、国民の安心感の醸成を図る観点から、可能な範囲でサイバーセキュリティに関する取組を開示[9]すること。
  - ＊ サイバーセキュリティに関する次の情報を開示することが望ましい。
    - ✧ 組織方針・サイバーセキュリティ方針
    - ✧ 維持するサービス範囲・水準
    - ✧ リスク管理体制
    - ✧ サイバーセキュリティに関する責任者の知識及び技能
    - ✧ 資源の確保
    - ✧ リスクの把握と対応計画策定
    - ✧ 緊急対応体制・復旧体制
    - ✧ インシデントの発生状況

6. 継続的改善

- 組織統治の枠組みの改善を行う際に、サイバーセキュリティに関するモニタリング・レビューの結果や、最新のセキュリティ動向も考慮すること。
  - ＊ サイバーセキュリティ方針が妥当かつ有効であることを、定期的に、また、自組織を取り巻く状況に大きな変化が発生した場合に確認することが望ましい。
  - ＊ 改善を継続的に実施することで、サイバーセキュリティも含めたリスクマネジメントの考え方が組織に浸透し、組織風土に定着するよう努めることが望ましい。

---

[6] 在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全てを含むサプライチェーン全体を俯瞰し、総合的にサイバーセキュリティを確保すべきである。

[7] サイバーセキュリティ基本法におけるサイバーセキュリティの定義には、情報システムの安全性及び信頼性の確保のために必要な措置も含まれる。

[8] 取締役、監査役等によって実施される、リスク管理体制が適切に構築、運用されているかを監査する枠組み。

[9] サイバーセキュリティに関する組織の情報を開示することは、組織の社会への説明責任を果たすとともに、組織運営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。

Ⅲ. リスクマネジメントの活用と危機管理

- CISO、戦略マネジメント層向けを念頭とした取組を記載する。
- リスクマネジメントによる事前対応と、危機管理の両面からサイバーセキュリティの確保に取り組むこと。
- 自組織の特性やリスクを特定した上で、①自組織の現在のセキュリティ水準に係る自己評価、②本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施を繰り返すこと。
- NISC「重要インフラのサイバーセキュリティに係るリスクマネジメント手引書」が参考になる。

1. 組織状況の理解

- 重要インフラサービスに関する外部環境（政治、経済、社会等）及び内部環境（組織体制、戦略、能力等）の状況について、近い将来の状況も含めて整理すること。
- 関係法令、契約等に規定された義務、サプライヤー・委託先が提示する制限事項等、関係者からの要求事項を整理すること。
  - ＊ 任務保証の観点から次のような自組織の特性を理解することが望ましい。
    - ✧ 自組織が果たすべき役割・機能を発揮するために維持・継続することが必要なサービス
    - ✧ 関係者のニーズ・期待や法制面での要求事項等を満たすために最低限許容されるサービス範囲・水準
    - ✧ サービス提供を維持するために必要な業務や経営資源
- 自組織の現在のセキュリティ水準を特定すること。

2. リスクアセスメント

- 組織状況を踏まえ、任務保証の考え方に基づくリスクアセスメントを実施すること。
- 制御システム[10]に汎用機器が用いられ、また、遠隔監視・制御等のために外部と接続される場合がある[11]ことを念頭に、制御システムについても適切にリスクアセスメントを実施すること。
  - ＊ IPA「制御システムのセキュリティリスク分析ガイド 第２版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を参考に、事業被害ベースのリスク分析を実施することが望ましい。
- 大規模イベントの開催等の環境変化に応じてリスクアセスメントを再度実施する

[10] 電力、ガス等の保安関係設備の制御に用いられるシステム。制御システムは、例えば、センサから得られる情報を処理し、機器を動作・停止させるといった制御を自動的に行う。

[11] 一般に、重要インフラの制御システムは、独自仕様の機器や通信プロトコルで構成され、また、外部と接続のない閉域環境で運用される。

こと。

3. サイバーセキュリティリスク対応

- リスクアセスメント結果を踏まえ、本来あるべき状況や要件を検討し、目標とするセキュリティ水準を決定すること。
- 現在のセキュリティ水準と目標とするセキュリティ水準の差異について分析すること。
- 差異を解消するためのセキュリティ対策を検討し、その適用の程度について優先順位付けを行い、自組織に適したセキュリティ対策を決定すること。
- サイバーセキュリティに関するリスク対応計画を策定すること。計画には次を記載することが望ましい。
  - ＊ 目標とするセキュリティ水準
  - ＊ 実施事項
  - ＊ 必要な資源
  - ＊ 責任者
  - ＊ 達成期限
  - ＊ 結果の評価方法
- リスク対応により、防御だけではなく、重要インフラサービス障害が社会経済に与える影響を最小化するための検知・対応・復旧の各機能を実現すること。
- セキュリティ対策によって、サイバーセキュリティに関するリスクをどの程度回避、軽減が出来たかを測定・評価すること。
  - ＊ 現状のシステムやセキュリティ対策の問題点を検出するために、脆弱性診断、ペネトレーションテスト等を実施することが望ましい。

4. サプライチェーン・リスクマネジメント

- 対応すべき代表的なサプライチェーン[12]に係る脅威は次のとおり。
  - ＊ 不正機能等の埋め込み
  - ＊ サービスの供給途絶
  - ＊ 外部サービスにおける情報の取扱い
  - ＊ 海外拠点、グループ組織、取引先等を経由したサイバー攻撃
- 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行うこと。
- サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行うこと。
  - ＊ 次の対応を行うことが望ましい。

[12] サプライチェーンとは、一般に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するものであり、安全基準等策定指針においては、外部組織が関与する製品（機器・ソフトウェア）又はサービス（クラウドサービス、保守管理役務等）を自組織で調達・利用するプロセスとする。

- ✧ 供給者におけるセキュリティ対策の定常的な監視・監査
- ✧ 調達した製品に対する脆弱性診断
- ✧ 資産に供給者がアクセスするリスクの低減
- ✧ 利用する外部サービスの仕様変更の把握
- ✧ インシデント発生時、脆弱性把握時等における情報共有

・ 事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めること。

・ 直接の供給者を管理することを前提としつつ、リスクに応じて管理する範囲を設定すること。

＊ 直接の供給者に連なる供給者については、各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。

5. 事業継続計画等の作成

・ 情報システムに係る事業継続計画等を策定すること。

＊ コンティンジェンシープラン：初動対応の方針

＊ 情報システム固有の事業継続計画（IT-BCP）：情報システムに係る復旧対応の方針。システム障害が組織全体にエスカレーションする際、当初 IT-BCP が機能し、ある時点から事業継続計画へ円滑に移行していくことが望ましい。

＊ 事業復旧計画：平時のサービス水準までの完全復旧対応の方針

・ 事業継続計画等を策定する際に、サプライチェーンに係る脅威を想定すること。

6. 人材育成・意識啓発

・ 部署・役職に応じた必要な水準の知識・技能が確保されるよう、人材育成・意識啓発を行うこと。

＊ セキュリティ対策業務に従事する人材を確保するため、キャリアパスの設計や外部人材活用の検討をすることが望ましい。

＊ セキュリティ対策業務に従事する人材に対し、「情報処理安全確保支援士」等の資格取得、演習・訓練への参加等を推進することが望ましい。

＊ セキュリティ対策が不十分だった場合に生じる影響例を示す等の方法により意識啓発をすることが望ましい。

7. CSIRT 等の整備

・ CSIRT[13]としての機能を持つ体制を整備すること。

[13] Computer Security Incident Response Team の略(シーサート)。企業や行政機関等において、情報システム

・ CSIRT 等は、役割分担や対応手順等を関連部門と合意しておくこと。

8. 平時の運用

・ リスク対応計画を踏まえ、セキュリティ対策の導入、運用プロセスの確立・実行、CSIRT 等の運用を行うこと。
・ NISC『「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書』も踏まえ、組織内外と情報共有を実施すること。
  ＊ ISAC 等の分野専門性の高い情報共有活動に参加し、情報収集することが望ましい。
  ＊ 連絡体制が最新の情報に更新されているか確認することが望ましい。
  ＊ 有益な情報を得るには自ら適切な情報提供を行う必要があることを自覚し、組織内外に情報提供を行うことが望ましい。
・ 収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行うこと。

9. 危機管理

・ 重要インフラサービス障害が発生した場合、事業継続計画等に従った初動・復旧対応を実施すること。
・ 初動・復旧対応に関する経営層の意思決定を支援すること。
・ 組織内外の関係者に情報共有すること。

10. 演習・訓練

・ リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行うこと。
  ＊ 供給者と合同で演習・訓練を実施することが望ましい。
  ＊ NISC が主催する「分野横断的演習」に参加することが望ましい。

11. モニタリング・レビュー

・ サイバーセキュリティに関する環境変化、インシデントの発生状況、セキュリティ対策の実施状況・有効性評価等について経営層に定期的に報告すること。
・ 内部監査に相当する枠組みにおいて、情報セキュリティ監査、システム監査等のサイバーセキュリティに関する監査を実施すること。

12. 継続的改善

・ 経営層からの指示、モニタリング・レビュー、危機管理、演習・訓練等を踏まえ

等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。

て、サイバーセキュリティ方針、各種計画等の継続的な見直しを行うこと。

Ⅳ. 対策項目

・ 戦略マネジメント層、担当者層向けを念頭としたセキュリティ対策を記載する。
・ 対策を数多く実施することを目的にするのではなく、自組織に適した対策を選択すること。

1. ランサムウェア対策

・ 速やかなパッチ適用等による脆弱性対策を講じる。
・ 海外拠点、サプライチェーンを含めて資産管理をする。
・ システムソフトウェア及びデータのバックアップを行い、バックアップから復旧可能なことを定期的に確認する。
・ バックアップデータをネットワークから隔離し保存する。
・ 役割等に基づいてネットワークを分割する。
・ 攻撃を受けた後に調査できるようにログなどを保存する。
・ ベンダーなどの関係者と協力関係を構築する。
・ 攻撃を受けた際は所管省庁や警察に連絡し、逐次時系列で状況を保存する。
・ 一般論としては、ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むことが望ましい。
・ NISC「ストップ！ランサムウェア　ランサムウェア特設ページ」が参考になる。

2. クラウドサービス利用時の対策

・ 利用するクラウドサービスについて理解を深める。
・ クラウドサービス提供者と責任分界点を明確にしておく。
・ 情報公開設定などに設定ミスがないか確認する。
・ サービス仕様が変わる際には影響を確認する。
・ 多岐にわたるステークホルダーを把握し、情報共有体制・インシデント対応体制を構築する。
・ NISC「クラウドを利用したシステム運用に関するガイダンス」が参考になる。

3. 組織的対策

（資産管理）

・ 情報システム、ソフトウェア、情報等の資産を特定し、各資産の管理責任者や利用制限（利用が許される範囲）等を明確化した資産目録を作成・維持管理する。
・ 情報システム又はその運用を外部サービスによって代替する場合には、利用する外部サービスの一覧を作成・維持管理する。
・ ネットワーク構成図、データの流れ図等を作成する。
・ 未承認の資産がネットワークに接続・運用されていないか監視し、対処する。
・ 機密性、完全性、可用性の観点から情報の格付け及び情報媒体（紙、電子）へのラベル付けを行う。

- 情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を実施する。
- 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う。
- 事業環境の変化を捉え､インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する。
- 重要な情報を外部転送するにあたり、セキュリティ確保に係る取組方針や手順を整理し、転送相手と合意する。

（運用管理）

- 情報システム等の運用に関連する手順書を整備する。
- 手順書を共有し、作業誤りやセキュリティ基準違反を抑止する。
- 情報システム等の更新に関する事前承認手続きを定める。
- 運用環境と開発・試験環境を分離する。
- マルウェアを検出及び予防する仕組みを整備し、マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。
  - ＊ マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトを利用する。
  - ＊ システム負荷を抑えつつ、未知の脅威に対応できることを特徴とするホワイトリスト型のマルウェア無効化機能を導入する。
- システムイメージやデータ等に対するバックアップの方針及び手順を整備し、定期的なバックアップリカバリー検査を実施する。
- 情報システムのイベントログや運用担当者の作業ログを記録・管理する。
  - ＊ ログが悪意を持った人物やマルウェア等によって故意に改ざん、消去されないよう管理する。例えば、ログの性質に応じた定期的な検査によって、ログに対する不正行為の有無を確認する。
- 情報システムで利用するソフトウェア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る。
- ソフトウェアのサポート対象バージョンへの更新を計画的に実施する。サポート対象バージョンへの更新が困難な場合には、補完的な措置を講じる。
- 脆弱性情報を収集し、運用中の情報システムに対する影響の有無を確認する。
- 定期的な脆弱性スキャンを実施する。
- 情報システムへのパッチ適用に関する作業方針・内容を確立する。パッチ適用が困難な場合には、情報システムに対する監視を強化するなどの補完的な措置を講じる。

（システムの取得・開発・保守）

・ 情報システムの取得・開発・改善に係る要求事項にサイバーセキュリティに関する事項を含める。
  ＊ 第三者認証を受けた情報システムの活用を検討する。
・ 情報システムの取得・開発・改善時にサイバーセキュリティを確保するための手順、環境等を整備する。
  ＊ 情報システムの受け入れ確認時に脆弱性診断を実施する。

（インシデント管理）
・ インシデントの管理責任者を定める。
・ 組織内外へのインシデント報告や証拠収集等の手順を整備する。
・ インシデントへの対応を通じて得た知識を、将来のインシデントへの備えとして活用するための仕組みを確立する。

4. 人的対策
・ 重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理する。
・ テレワーク・遠隔制御に関するサイバーセキュリティ確保のための対策を実施する。
・ 委託先との契約書等に、従業員に関する要求事項や委託終了後も遵守すべき事項を盛り込む。
・ 委託先の取組状況を定期的に確認し、必要な改善を求める。
・ 従業員が発見した又は疑いを持ったセキュリティ事象を、適切なエスカレーションにより速やかに報告するための仕組みを設ける。

5. 物理的対策
・ セキュリティ確保が求められる領域を管理する。
  ＊ 物理的なセキュリティ境界を設定する。
  ＊ 入退管理の仕組みを構築する。
  ＊ 持ち込まれる物品の確認・制限を実施する。
・ 災害による障害が発生しにくい設備配置とする等の災害対策を実施する。
・ 傍受や損傷の可能性を考慮して通信・電源ケーブルを配線する。
・ 書類や取り外し可能な記録媒体の使用・持ち出し・廃棄に係る事前承認の仕組みを整備する。

6. 技術的対策
・ 情報システムや情報等へアクセスする利用者とそのアクセス権を管理する。
  ＊ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等を定める。

    * 利用者アクセス権を定期的にレビューする。
- 最小権限及び職務の分離の原則を踏まえて、情報やシステムの重要度に応じて、情報システムや情報へのアクセスを制限する。
    * ログイン失敗回数を制限する。
    * 良質なパスワードを利用する。
    * 多要素認証を活用する。
- 暗号の利用方針や暗号鍵の管理方針を策定する。
- 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知等によってネットワークのセキュリティを確保する。
- 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、多層防御を導入する。