重要インフラのサイバーセキュリティ部門における
リスクマネジメント等手引書

2023年７月４日

内閣官房内閣サイバーセキュリティセンター

目次

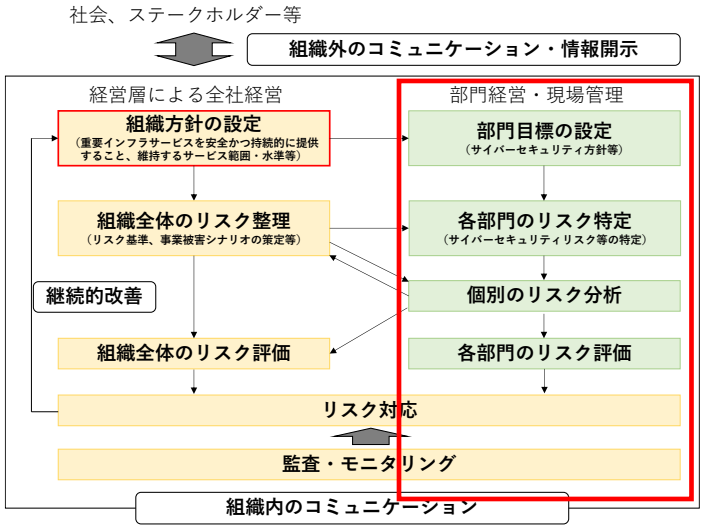
1. はじめに

1.1. 手引書策定の目的

- 情報通信技術の進歩や複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず変容かつ増大している。新しいサービスの創出機会等も拡大している一方で、サイバー攻撃等による情報漏えいやサービス停止の被害が増加するなど、サイバーセキュリティに関するリスクも拡大している。
- 「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）（以下「行動計画」という。）では、「国民生活や経済社会活動の基盤となるサービスを提供する重要インフラ事業者等においては、経営の重要事項としてサイバーセキュリティを取り込み、重要インフラを取り巻く情勢（システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まり等）を鑑みて、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応をより一層促進する」こととされた。
- 本手引書は、サイバーセキュリティ部門（戦略マネジメント層、担当者層）向けに、安全基準等策定指針で示すセキュリティ確保に向けた取組についての参考情報を提供する。

1.2. 手引書の記載範囲

- 本手引書では、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（仮称）のうち、「4. リスクマネジメントの活用と危機管理」におけるリスクマネジメント等の主要なプロセス（下図の赤枠箇所）及び「5. 対策項目」における主なセキュリティ対策について、サイバーセキュリティ部門における取組を念頭に記載する。



図：組織統治とサイバーセキュリティのイメージ

1.3. 手引書の適用範囲

1.3.1. 対象とする事業者等

・ 本手引書は、重要インフラ事業者等による利活用を想定している。各事業分野や事業領域に特化したリスクマネジメント手法が既に確立している場合は、既存の手引書やガイドライン等を優先して利活用しつつ、必要に応じて本手引書の記載内容を補完的に利活用することが望まれる。

1.3.2. リスクマネジメントの対象

・ 本手引書におけるリスクマネジメントでは、重要インフラ事業者等が、そのサービス提供に必要な業務の遂行のために所有、使用又は管理する情報資産等に係る事象の結果（自然災害、サイバー攻撃等に起因する障害）から認識されるリスクを対象とする[1]。

[1] 重要インフラ事業者等においては、サイバーセキュリティに関するリスク以外のリスクがあることも考えられる。本手引書では、スコープを限定したリスクマネジメントの手法を紹介しているが、実際にリスクの評価やリスク対応の選択肢の同定に係る意思決定を行う際には、サイバーセキュリティに関するリスク以外についても勘案し、総合的に考慮することが重要である。

2. リスクマネジメントのフレームワーク

2.1. 全体像

- NISC「機能保証のためのリスクアセスメント・ガイドライン」、NIST「重要インフラのサイバーセキュリティフレームワーク（CSF)」[2]、ISO/IEC27001 をベースに構成している。
- 対象を従来のリスクアセスメントからリスクマネジメント全体に拡大し、コミュニケーション及び協議、モニタリング及びレビュー等に係る取組を追記した。
- 組織の状況把握からリスク対応の決定・改善に至る一連の取組[3]について、NIST CSF をベースに追記した。

2.2. 前提

- リスクの捉え方について、「目的に対する不確かさの影響」をリスクと捉える（ISO 31000:2018 における定義に準拠。)。

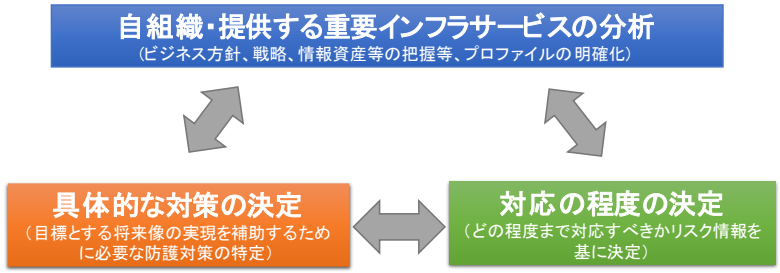
[2] NIST において、NIST CSF の改定に向けた検討がなされている。
[3] NIST CSF では、「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つセキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用対効果の高いアプローチ」とされている。

3. コミュニケーション及び協議

- リスクマネジメントのプロセスの初期段階において、サイバーセキュリティに関するリスクが影響を及ぼす可能性のある組織内外のステークホルダーを把握し、コミュニケーション及び協議のための体制を構築する。
- リスクマネジメントにおけるコミュニケーション及び協議には、分析したリスクについてステークホルダーと共有や議論を行なうことに留まらず、リスクマネジメントの各ステップの活動を行う為に必要な分析に使用する最新の情報や手法に加えて、ステークホルダーの価値観等のリスク特定や評価に重要な情報の共有を行なうことも含まれる。
- ステークホルダーとのコミュニケーション及び協議により、実施しているリスクマネジメントへの安心を高め、参加意識を高めることもできる。

4. 組織の状況の特定

- 自組織が直面するリスクとその程度を把握し、自組織の重要インフラサービス提供に係る特性の明確化に着手することから新たな改善をスタートする。
- 任務保証の考え方を踏まえ、自組織の特性を明確化する。
- 自組織の内部状況、外部状況及び関係主体の要求事項等について把握した情報は、従業員のセキュリティ意識向上の観点から、整理したものを組織内に共有する。



- 現状分析(実態把握)と目標とする将来像のかい離を明らかにする
- かい離を埋めるために、どこからどんな改善を行っていくか優先順位付けを行う

図：自組織に適した防護対策の実現（概念図）

4.1. 組織の状況及び特性の理解

- 組織全体のリスクマネジメントの一部として整理される組織内外の状況及び特性を理解する。
- 必要に応じて、サイバーセキュリティの視点から組織の状況及び特性の更なる明確化を行う。

4.1.1. 内部状況の理解

- 次に例示するような組織内部の現状をサイバーセキュリティの視点から理解する。
  - ＊ 組織体制、経営戦略、セキュリティ方針
  - ＊ リスクマネジメント戦略、リスク許容度
  - ＊ 重要インフラサービスに係る情報システム、制御システム、データ
  - ＊ セキュリティ投資が可能な資源状況
  - ＊ リスク分析や対応に必要な技術や人的資源
  - ＊ セキュリティリスクに対する、部署や立場による認識の差異
  - ＊ 従業員のセキュリティリテラシー

1) ビジョン、使命及び価値観

2) 組織統治、組織体制、役割及びアカウンタビリティ
3) 戦略、目的及び方針
4) 組織の文化
5) 組織が採用する規格、指針及びモデル
6) 資源及び知識として理解される能力（例えば、資本、時間、人員、知的財産、プロセス、システム、技術）
7) データ、情報システム及び情報の流れ
8) 内部ステークホルダーの認知及び価値観を考慮に入れた、内部ステークホルダーとの関係
9) 契約上の関係及びコミットメント
10) 相互依存及び相互関連

ISO 31000:2018 より、内部状況の例

4.1.2. 外部状況の理解

・ 次に例示するような組織外部の現状をサイバーセキュリティの視点から理解する。
  * 自組織が関連する法令の改正状況（事業法、個人情報保護法等）
  * 所管省庁や規制当局における基準の策定、改正状況
  * 関連団体における基準やガイドラインの策定、改正状況
  * 景気、為替、経済リスクが与えるセキュリティ投資への影響
  * 国外に拠点のある事業者における現地の法令、情勢等の状況
  * セキュリティ投資による優遇措置や市場競争におけるイニシアチブ
  * 重要インフラサービスの利用者に与える影響
  * 国内外におけるセキュリティインシデントの発生事例や、その報道等による社会からのセキュリティ認識の広まり
  * 外部取引先との契約における、セキュリティに関する要求事項
  * 自組織が任務保証を達成するために必要な他の重要インフラサービス
  * 自組織と他組織の相互依存関係

1) 国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因
2) 組織の目的に影響を与える、鍵となる原動力及び傾向
3) 外部ステークホルダーとの関係、並びに外部ステークホルダーとの認知、価値観、必要性及び期待
4) 契約上の関係及びコミットメント
5) ネットワークの複雑さ、及び依存関係

ISO 31000:2018 より、外部状況の例

4.1.3. 重要インフラサービス継続に係る特性の理解

・ 内部状況及び外部状況を踏まえ、次に例示するような自組織の重要インフラサービス継続に係る特性を理解する。
  * 自組織のサービス停止が経済社会に与える影響
  * サービス継続に係る重要なシステムや機能
  * 重要なシステムや機能を支える業務
  * 業務を支える資源及び知識（予算、人員、設備、技術、資産の脆弱性情報）
  * 他の重要インフラとの相互依存関係
  * 重要インフラサービス障害時における、復旧までの許容可能な時間

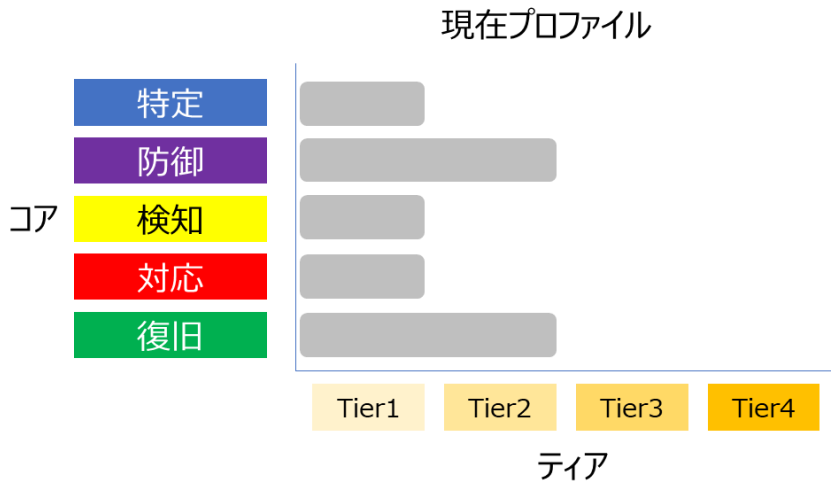
4.2. 現在プロファイルの特定

・ 現段階における自組織のサイバーセキュリティ対処態勢等の実態を把握するに当たり、一例として、現在プロファイルの特定が考えられる。
・ 現在プロファイルの特定に当たっては、NIST サイバーセキュリティフレームワーク（CSF)、英国サイバーアセスメントフレームワーク（CAF)、サイバーセキュリティ能力成熟度モデル（C2M2)、CIS Controls 等が参考となる。NIST CSF では、サイバーセキュリティの確保に当たり、コアと呼ばれる５つの区分（特定・防御・検知・対応・復旧)のセキュリティ対策と、ティアと呼ばれる対策の程度を例示している。
・ 経済産業省 のサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）は、NIST CSF など国外の主要な規格との整合性を確保しており、国外の規格を踏まえた各国の認証制度との相互承認を進めていくことができる内容となっている。

【プロファイルの特定について】

セキュリティ対策の状況把握について、NIST CSF ではプロファイルという考え方が説明されている。

プロファイルには対策の区分であるコアと、対策の程度を示すティアの２つの要素があり、プロファイルを特定するためには、まずこれらを自組織用に整理する必要がある。



図：現在プロファイルの特定の概念図

NIST CSF にはコアを細分化した 23 のカテゴリ及び 108 のサブカテゴリが例示されている。これらのカテゴリ全てについて対応するのではなく、自組織にとって必要な項目を採用し、整理を行う。

対策の程度を示すティアについても４つの段階が例示されているが、ティアの段階についても自組織向けに設定できる。適切なティアを判断するに当たり、成熟度モデル等、既存のガイダンスの活用を検討することが考えられる。また、リスクの許容度がティアに反映される場合もある。

成熟度モデルは、組織において現在取り組んでいる対策や手法等に能力レベルを評価し、目標や改善のための優先順位を設定するためのベンチマークとなる。

代表的な成熟度モデル

- サイバーセキュリティ能力成熟度モデル（C2M2）
- サイバーセキュリティ成熟度モデル認証（CMMC）

表：ティア（対応の程度）の例

Tier1	**・セキュリティ対策が未対応の状態。** ・リスクマネジメントの枠組みが定められておらず、リスク対処は場当たり的。 ・セキュリティリスクに関して意識が不足している。 ・情報共有のプロセスが存在しない。 ・ステークホルダーとは協力関係にない。
Tier2	**・セキュリティ対策は整備しているが、運用化まではできていない。** ・リスクマネジメントの枠組みは経営層に承認されているが、組織全体のポリシーにはなっていない。 ・サプライチェーン・リスクは把握しているものの対応はできない。
Tier3	**・セキュリティ対策は整備できており、定期的に見直しができる状態。** ・リスクマネジメントの枠組みが自組織のポリシーとなっており、また定期的に見直されている。 ・従業員は割り当てられた役割と責任を果たすための知識とスキルを持っている。 ・セキュリティ担当の役員と他の役員が定期的に他の役員とコミュニケーションを取っている。 ・ステークホルダーと協力関係にある。 ・サプライチェーン・リスクの対処ができる。
Tier4	**・セキュリティ対策は整備できており、適時に見直しができる状態。** ・組織全体のサイバーセキュリティマネジメントのアプローチが確立されている。 ・セキュリティリスクマネジメントが組織文化の一部となっている。 ・役員が示したビジョンを実践し、システムレベルでリスク分析を行っている。 ・事業目的、ミッションの変更に迅速かつ効果的に対処できる。 ・サプライチェーン・リスクをリアルタイムに近い情報で対処している。

出典：NIST CSF

5. リスクアセスメント

5.1. リスクアセスメントの実施

・ 重要インフラサービスの安全かつ持続的な提供に影響を与える、セキュリティリスクを適切に管理すべく、次のような手順によってセキュリティリスクアセスメントを実施する。

①リスクアセスメントの対象の特定

絶えず変化する自組織を取り巻く状況及び関係主体等のニーズを踏まえ、重要インフラサービスの提供に必要な業務の範囲・水準等を明らかにするとともに、当該業務の遂行に必要な情報システム等の経営資源を特定する。

②リスク特定

情報システム等の経営資源に対する「セキュリティリスク」を特定する。

③リスク分析

「事象の結果によるサービス・業務への影響度合い」や「事象の発生可能性」等を評価軸として策定されるリスク基準を活用して、特定されたリスクの大きさを確認する。

④リスク評価

基準値以上の大きさのリスクを抽出するとともに、個別事情も考慮してリスク対応の対象とするリスクを抽出する。

・ リスク分析に当たっては、任務保証の考え方を踏まえ、重要インフラサービス障害等が社会に与える影響[4]を念頭に分析することが重要である。
・ 重要インフラサービスの安全かつ持続的な提供のためには、セキュリティリスクに加えて、HSE[5]等の観点からのリスクも特定し、分析・評価を行う事も求められる。HSE 等の観点として、例えば、重要インフラサービスの提供を担う従業員等の労働安全・衛生の確保や、重要インフラサービスの利用者の安全・健康の確保、重要インフラサービスの提供に伴う環境負荷の低減等が考えられる。
・ 上記手法においてリスク対応の対象として抽出しなかったリスクも管理が必要である。所管部署の責任において当該リスクを管理させる場合には、各部署の管理状

[4] 重要インフラ分野等の間の「相互連関・連鎖性」が一層深化していくことが予想される。NISC において、重要インフラサービス障害等が生じた場合の影響の波及に関する調査（相互依存性調査）を実施予定である。

[5] 健康（Health）、安全（Safety）及び環境（Environment）を指す。産業用オートメーション及び制御システムを対象としたサイバーセキュリティのマネジメントシステムである CSMS 認証基準（Ver.2.0）では、物理的リスクのアセスメントの結果、HSE 上のリスクのアセスメントの結果及びサイバーセキュリティリスクのアセスメントの結果の統合を要求している。

況（セキュリティ管理策の導入有無等）を適時確認可能とする仕組みを整備する。

- リスクアセスメントの具体的なプロセスについては、NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0 版」等を参考にしながら、リスクの特性に応じたリスク分析手法によってリスクを評価する。

5.2. 制御システムのリスクアセスメント

- 制御システムにおいては IPA「制御システムのセキュリティリスク分析ガイド」、ISO/IEC 62443「制御システムセキュリティに関する国際規格」、NIST-SP 800-82「産業用制御システム（ICS）セキュリティガイド」等を踏まえ、資産ベースに加え、事業被害ベースの脅威を想定したリスクアセスメントを実施する。
- 制御システム関連のインシデント事例について情報収集し、リスクを評価することが重要である。
- 一般的に、制御システムは可用性（安全、安定稼働）が最優先される。パッチ適用やバージョンアップ、暗号化などのリスク低減策の実施が、制御システムの安定稼働に影響を与えると判断できる場合には、ログや通信の監視等の代替策の実施によりリスク低減を図る。
- 制御システムに関するセキュリティ責任者を設置し、情報システムと制御システムの担当者間で適切なコミュニケーションをとる。
- セキュリティリスクを考慮し外部ネットワークに接続していない環境で運用していても、災害、自然故障、管理不良等により制御システムの可用性が低下するリスクがある。

【リスク分析の手法について】

リスク分析のアプローチとして、資産ベースのリスク分析と、事業被害ベースのリスク分析がある。

○ **資産ベースのリスク分析**

保護すべきシステムを構成する資産群を明確にし、各資産に対するシステム構成上及び運用管理上に想定される脅威について、各資産の重要度と、その脅威の発生可能性と受容可能性（脆弱性）の相乗値によって資産のリスクを評価するリスク分析手法

○ **事業被害ベースのリスク分析**

回避したい事業被害を明確にし、事業被害を引き起こすと想定される脅威について、事業被害の大きさと、攻撃の発生可能性と受容可能性（脆弱性）の相乗値によって、事業のリスクを評価するリスク分析手法

	資産ベースのリスク分析	**事業被害ベースのリスク分析**
長所	全ての資産を単体で網羅的にリスク分析と対策の検討が可能	事業被害をもたらす攻撃ツリーに対する多層防御的な観点で、対策を検討することが可能
限界／短所	資産を一律に評価するので、事業上の対策優先順位付けに考慮が必要	想定（対象）外の攻撃の入口や、攻撃ツリーで経由しない資産や、経由した資産での直接の攻撃（不正アクセスや操作等）以外の攻撃に対する対策の検討は、見落とされる可能性がある。

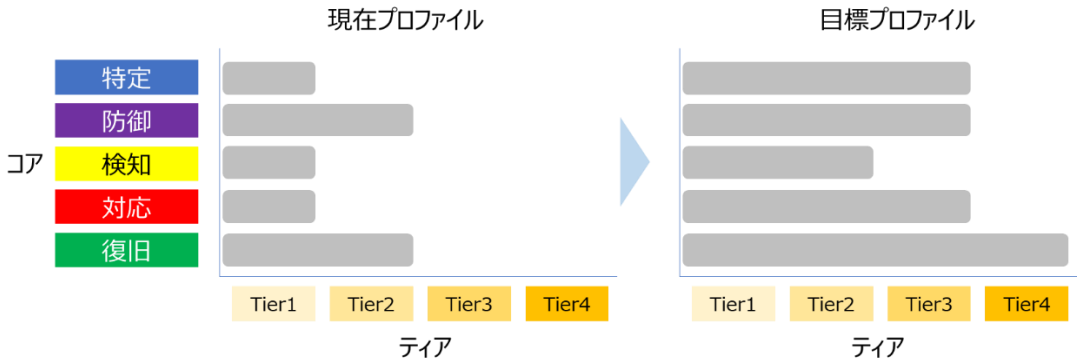
組織の状況によって選択する分析手法は異なる場合があるが、組織が保有する資産（情報システムやネットワーク構成、データフロー図等）が明確化されていることが前提である。

出典：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」

6. リスク対応

6.1. 目標プロファイルの作成

- 重要インフラ事業者等は、リスクアセスメントの結果や、自組織の目標、組織の状況、ステークホルダーからの要求事項等を踏まえ、目標とする将来像を決定する。目標とする将来像を決定するに当たり、一例として目標プロファイルの作成が考えられる。
- 現在プロファイルの特定と同様、目標とするティアを設定する。目標とするティアは、自組織の方針に見合うものであり、任務保障の観点からサイバーセキュリティのリスクを自組織にとって許容可能な程度まで低減できるものである必要がある。
- 発生した障害等への対応については、障害等の発生の予防・検知と比べて多くの費用、人材等を要する傾向にあることから、予防・検知の徹底が重要となる。



図：目標プロファイルの概念図

6.2. ギャップ分析と優先順位付け

- 現在プロファイルと目標プロファイルの差異について分析する。
- 差異を解消し、目標プロファイルに近づけるための取組について、組織方針に基づく動機、リスク、セキュリティ対策の費用対効果等を踏まえ、優先順位付けを行う。

6.3. リスク対応計画

- 優先順位付けを踏まえ、現在プロファイルと目標プロファイルの差異に対して実施すべき取組をまとめたリスク対応計画を作成し、実施する。

6.4. サプライチェーン・リスク対応

- 製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理する。
- 不正機能等の埋め込みに係る脅威に対応する。
  （リスク管理策例）
  * 調達過程における一貫した品質管理が担保できることの選定基準への盛り込み
  * 指定したセキュリティ要件が実装されているか、不正プログラムが混入していないかを確認する検査体制の構築
  * 委託先が再委託先を監督し責任を負うことが可能な体制であるかの確認
  * 再委託の禁止、又は再委託前に委託元の許可を得ることの契約要件への盛り込み
- サービスの供給途絶に係る脅威に対応する。
  （リスク管理策例）
  * 部品の供給役務の継続提供の担保又は代替手段の検討
  * 供給者の事業計画や提供実績等の確認
  * 委託先の事業実施場所の確認、立地条件の考慮
- 外部サービスにおける情報の取扱いに係る脅威に対応する。
  （リスク管理策例）
  * 信用できるサービスの選定
  * 情報の返却や抹消などに係る確認手段の設定
- 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に係る脅威に対応する。
  （リスク管理策例）
  * 第三者による評価検証結果の活用
  * サプライチェーンとのネットワーク接続点におけるセキュリティの確認
- 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（令和５年４月 28 日閣議決定）におけるリスク管理措置の例や、NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」が参考になる。
- 発注者となる組織においては、独占禁止法及び下請法を考慮したパートナーシップ体制を構築する[6]。

[6] 経済産業省,公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」
https://www.meti.go.jp/policy/netsecurity/hontai_1028.pdf

7. コンティンジェンシープラン及び事業継続計画の策定

初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画」を策定する（又はこれらと同等の方針を定めた計画を策定する）とともに、当該計画の実行に必要な組織体制を整備する 。なお、事業継続計画を整備済みの重要インフラ事業者等においては、目標復旧水準から平時のサービス水準まで完全復旧させることを目的とした計画（事業復旧計画）も別途策定する。

策定に当たり、「【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」が参考となる。

7.1 コンティンジェンシープランの策定

- 重要インフラサービス障害の発生又はそのおそれがあることを認識した際に、経営層や職員等がまず実施すべき対応を明確にし、迅速に行動することが求められる。そこで、初動対応（緊急時対応）の方針、手順、態勢等を定めた「コンティンジェンシープラン」の策定が必要となる。

7.2 事業継続計画（BCP）の策定

- 重要インフラサービス障害発生時において、サービスを許容可能な時間内に許容可能な水準まで復旧させることを目的とし、復旧に向けた目標水準、優先順位、その他の方針、手順、態勢等を定めた「事業継続計画」の策定が必要となる。
- 重要インフラサービスに影響を与える要素として、サプライチェーン・リスクが含まれる場合があることも考慮し、事業継続計画を策定する。

8. 運用

8.1. 人材育成

- サイバーセキュリティの推進役となるセキュリティ人材について、重要インフラサービスの安全かつ持続的な提供に必要不可欠な能力や人数等を確保・維持する観点から、これらのセキュリティ人材の重要インフラ事業者内のキャリアパス等をあらかじめ検討しておくことが重要である。必要に応じて外部人材を活用することも検討する。
- 重要インフラ事業者等の従業員がセキュリティ方針及びセキュリティ管理策の個別方針に基づく義務と責任を果たせるようにするため、従業員に対して、サイバーセキュリティに関連する十分な教育・トレーニングを実施する（必要に応じて委託先にも実施）。特にサイバーセキュリティの推進役となるセキュリティ人材の育成においては、政府機関の人材育成プログラムやセキュリティベンダーが提供するトレーニング等の活用や、関係主体等と連携した演習・訓練への参加、「情報処理安全確保支援士」等の資格取得等も期待される。これらの取組は人材育成の達成状況を客観的に評価・確認する際にも有効となる。
- サイバーセキュリティリスクについて可能な限り理解できるよう、経営層に対してセキュリティ教育を実施する[7]。
- 制御システムのサイバーセキュリティの確保に当たっては、制御システムを熟知した上でサイバーセキュリティの知見を高めることが重要である。制御システムに関するセキュリティ人材を確保する取組としては、産業サイバーセキュリティセンター（ICSCoE）による中核人材育成プログラムを活用することが考えられる。

8.2. CSIRT 等の整備

- サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画の実行に必要な組織体制の一つとして、CSIRT[8]（又は同等機能を持つ組織）を重要インフラ事業者等の内部に整備する。CSIRT 等の組織は、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。
  特に、制御システム等の運用環境を保有する重要インフラ事業者等においては、重要インフラサービス要害発生時の対応に OT 関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。

---

[7] NISC では経営層や DX を推進する部課長向けに、プラス・セキュリティ知識として、参考となるカリキュラムを公開している。https://security-portal.nisc.go.jp/dx/plussecurity.html

[8] Computer Security Incident Response Team の略。サイバー攻撃による情報システムの不具合など、コンピュータセキュリティに係るインシデントに対処するための組織のこと。なお、事業者によって CSIRT を組織として常設している場合とインシデント発生時のみ設置する場合がある。

また、サイバー攻撃に迅速に対処する観点から、サイバーセキュリティの専門知識を持つ組織を含めた対処体制を平時から整備する。例えば、サイバー空間関連事業者及びサイバーセキュリティ関係機関との提携が有効である。

・ その他、セキュリティ確保の取組を推進するため、次のような役割が考えられる。
    * 脅威情報等の収集及び関係主体との情報共有担当
    * コンティンジェンシープラン及び事業継続計画の実行担当
    * セキュリティ対策の取組全般に対する内部監査担当
    * サプライチェーン（供給者、委託先等）におけるセキュリティ対策の取組の管理担当
    * セキュリティ人材の職能要件の管理及び教育・研修担当
    * 情報システム（ネットワークを含む）の運用担当
    * 各資産（情報システム、ソフトウェア、情報等）の管理担当
    * 物理的セキュリティが要求される施設の管理担当

8.3. 平時におけるリスク対応

・ 「リスク対応計画」に基づき、リスク対応において決定したセキュリティ管理策の導入を進めるとともに、それらを効果的かつ確実に運用するためのプロセスを確立し、実行する。
・ 重要インフラサービスの提供に係る情報システム等の運用状態を示すデータについて、アラートやログ等の複数の監視結果を相互に組み合わせて、重要インフラサービス障害につながる可能性のある事象（サイバー攻撃、情報システムの異常状態等）を早期検知する仕組みを構築するとともに、検知後に続く関係部署等との事象の共有、トリアージ（サイバー攻撃等の事象の影響分析及び対応の優先順位付け）等の運用プロセスを確立する。
・ 日頃からサイバーセキュリティ関係機関等が提供する脅威情報やそれらの分析・対策情報を確認する。行動計画に基づく情報共有については、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』の運用に則り積極的な情報共有を実施する。
・ ISAC 等の分野専門性が高い情報共有活動への参加し情報収集を行う。
・ サイバーセキュリティ関係機関等からの情報提供や収集した脅威情報等を踏まえ、必要に応じて追加のリスクアセスメント及びリスク対応を実施し、重要インフラサービスの強靭化を図る。

8.4. 危機管理

・ 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析（情報システム等へのフォレンジックを含む）、関係主体等との情報共有・調

整（顧客向け広報活動を含む）、被害拡大の防止、サービスの復旧等の対応を実施する。

また、重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

・ セキュリティに関する責任者は、サイバー攻撃等の事象が発生した際、経営層の意志決定を支援するため、経営層が理解できるように事象の内容、影響及び現在の対応状況等を説明する必要がある。事業にどのような影響があり、どのように対処をしていくのか、初動及び復旧の対応について経営リスクの観点から経営層へエスカレーションを行う。

8.5. 演習・訓練

・ リスクマネジメントによる事前対応と、障害発生時の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、定期的に演習・訓練を実施する。重要インフラ全体の防護能力の観点からは、同業の重要インフラ事業者等やサプライチェーン、関係主体等との合同での演習・訓練やケーススタディ（他事業者の過去のインシデント対応事例の研究）の実施も期待される。なお、合同での演習・訓練には、内閣サイバーセキュリティセンターが主催する「分野横断的演習」や、重要インフラ所管省庁やサイバーセキュリティ関係機関等の関係主体が主催するものがある。

9. モニタリング及びレビュー

9.1. モニタリング実施計画の策定と実施

- サイバーセキュリティ確保の取組の効果について、継続的に改善を行うため、リスク対応計画や、人材育成の進捗状況等をモニタリングする。継続的に実施するため、モニタリング及びレビューのプロセスを計画に組み込む。
- サイバーセキュリティ確保の取組により、リスクをどの程度回避、軽減が出来たかを測定・評価する。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の手段がある。
- リスクの管理レベルが社会からの要求事項の変化に沿うよう、日々改善する。

9.2. 内部監査の実施

- サイバーセキュリティ確保の取組が適切な状態で維持していることを確認するため、内部監査人による定期的な監査を実施する。実施に当たっては必要に応じて、外部の専門知識を有する者の支援を受けて状況確認をする。

9.3. モニタリング及びレビュー結果の反映方針の策定

- モニタリング及び監査結果から、改善や見直しが必要な箇所を認識する。レビューに際し、内部環境、外部環境の変化や、関係主体からの要求事項も確認する。

10. 記録及び報告

10.1. 記録

・ リスクマネジメントの検証、改善のため、各プロセスにおいて、記録を作成する。記録の作成に当たっては次の事項を考慮する。
  * 記録の作成及び維持管理の費用及び労力
  * 閲覧方法、検索の容易性及び保存媒体
  * 保有期間
・ 記録を取ることを目的にするのではなく、利用目的に合わせて記録することが重要なことに留意する。

10.2. 報告

・ ステークホルダーとのコミュニケーションの質を高めたり、経営層の意思決定を補助したりするために報告を実施する。報告に当たっては次の事項を考慮する。
  * それぞれのステークホルダーに特有の情報の必要性及び要求事項
  * 報告の費用、頻度及び適時性
  * 報告の方法
  * 情報と組織の目的及び意思決定との関連性

11. 対策項目

・ 以下に個別の対策例を示す。各リスク評価の結果、重要度に応じて組織ごとにリスク対応を行うことが前提であることに留意。

11.1. 組織的対策

11.1.1. 資産管理

・ 組織全体の資産目録を作成し、定期的に維持管理する。制御システムについても作成する。重要な機器やサービス業務の機能維持・レジリエンス向上のため、全ての重要な資産の現在の詳細構成を記述した文書を策定し、維持管理する。
・ 全てのシステム・ネットワーク構成を記述した文書（システム・ネットワーク構成図）を作成し、維持管理する。制御システムについても文書を作成する。構成図は定期的なレビューと更新を実施する。
・ 新しいハードウェア、ソフトウェア、ファームウェアを導入する前に、承認を必要とする仕組みとし、組織の情報資産の可視性を高める。技術的に可能な場合、承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する。

11.1.2. 情報分類と取扱い

・ 重要インフラサービスの提供に係る情報及びその他の関連資産を適切に保護するため、情報の取扱い手順を整備する。情報は機密性、完全性、可用性及び関連する利害関係者の要求事項に基づき分類及び情報媒体へのラベル付けを行う。
・ 自組織の業務上の要求事項に対処できるよう、情報の分類体系はアクセス制御に関する方針と整合させる。
・ 自組織が採用した情報分類体系に従って、情報のラベル付けに関する手順を策定し、情報の分類、伝達、処理、管理を適切に行う。ラベル付けは物理的、電子的手段等があるが、デジタル情報についてはメタデータを活用する手法がある。なお、技術的な制約等によりラベル付けが不可能な場合の情報についても取扱いの手順を定める。

11.1.3. 運用管理

11.1.3.1. 運用の手順及び責任

・ サイバーセキュリティに関する脅威情報を収集し、意思決定等に活用できるよう分析する。
・ インターネットに接続されたシステムの既知の脆弱性（CVE 情報等）を、重要な資産から優先的にパッチ適用等により緩和する。パッチ適用が不可能又は可用性や安全性を損なうおそれのある制御システムについては、ネットワークの

分離や監視等の代替手段を使用し、当該システムがインターネットからアクセスできないようにする。

・ 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにする。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

11.1.3.2. マルウェアからの保護

・ マクロ等の埋め込みコードの実行を全ての機器において既定で無効とする。業務においてコードを実行する必要がある場合、許可されたユーザーが特定の状況下で実行できることを承認する仕組みを構築する。
・ 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の利用や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マルウェア対策機能等の導入を検討する。
・ 被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、IPS[9]/プロキシサーバ（不審な外部通信の遮断）、EDR[10]（影響範囲の特定と被害端末の隔離）、NDR(ネットワーク全体の包括的な監視と脅威検知)等がある。

11.1.3.3. バックアップ

・ 運用に必要なシステムについて、年 1 回以上の定期的なバックアップを実施する。
・ バックアップデータはバックアップ元のシステムと異なるセグメントにすることやオフラインにする等、切り離して保管し、データの重要度に応じて保存方法、保存期間を定める。また、定期的に復旧テストを実施する。
・ 制御システムについては、設定、役割、PLC ロジック、設計図面、ツールについてもバックアップする。

11.1.3.4. ログ管理

・ システム及びネットワーク機器等のアクセス・認証ログや通信ログ、セキュリティ対策システムのイベントなどセキュリティの確保に必要なログを、検知及びインシデント対応で使用するために収集し、保存する。

---

[9] Intrusion Prevention System の略。ネットワークやサーバへの通信を監視し、不正なアクセスを検知して通信を遮断する不正侵入防止システム。
[10] Endpoint Detection and Response の略。従業員が利用する端末やサーバにおける不審な挙動を検知し、迅速に対応するためのセキュリティ対策の一種。

・ 定期的又は適宜、保存したログの点検及び分析を行う。
・ ログを改ざん、削除から保護するための対策を行う。また、イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の制御システムについては、制御システムとの間の通信ログを収集する。
・ 収集したログはツールや中央システム（SIEM 等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。

11.1.3.5. 運用ソフトウェアの管理

・ 重要インフラサービスに係る運用ソフトウェアを、セキュリティを保って管理するための手順及び対策を実施する。
運用ソフトウェアの更新は、管理層の認可に基づき適切に実施する。また、「十分に試験を行ってから導入する」、「開発用コードは使用しない」、「ロールバック計画を作成する」「監査ログを維持する」等の準備を含め、計画的に実行する。
・ 外部供給ソフトウェアについては、供給者がサポートするバージョンを維持する。供給者は古いバージョンのサポートを終了していくため、重要インフラ事業者はサポートのないソフトウェアに依存するリスクを考慮し、リスク管理策を検討する。
・ 安全に関する要求事項を優先する等の理由により、セキュリティ要求事項を完全には満たしていない場合において、採用するセキュリティ管理策を文書化し、正式に承認を得る。

11.1.3.6. 情報の転送

重要インフラサービスの提供に係る重要情報等を、電子メールや電子データ交換、インスタントメッセージ等の通信手段を活用して情報転送する場合には、あらかじめ機密性や完全性等のセキュリティ確保に係る取組方針や手順を整理するとともに、それらについて転送相手となる関係主体等の合意を図る。

11.1.4. システムの取得・開発・保守

・ 重要インフラサービスの提供に係る情報システムを新たに取得・開発する際や、既存の情報システムを改善する際には、「セキュリティ・バイ・デザイン」の考え方を踏まえ、システムの要求事項に情報セキュリティについての要求も含めて検討を行う（必要に応じて、前述の HSE 等の観点からの要求も含めて検討を行う）。重要インフラの分野によっては、情報システムのセキュリティ確保に

係る国際標準に則した第三者認証制度が存在するため、必要に応じて、認証された情報システムの活用等も検討する。

・ また、情報セキュリティに配慮した開発や構築を実現するための方針や手順、環境等を整備する。特に、情報システムの受け入れ確認の際には、情報セキュリティ関連の要求事項の確認に加えて、情報システムの重要度に応じて、脆弱性診断の実施要否を検討する。さらに、システム開発を外部委託する場合には、情報セキュリティに配慮した開発方針の遵守状況を委託先に対して定期的に確認する。

11.1.5. インシデント管理

・ インシデント管理責任者を定め、責任者に対しセキュリティ事象を報告できる方法を確立する。(関連 11.2.4. エスカレーション)
・ 管理、文書化、検知、優先順位付け、分析、伝達及び利害関係者の調整等を含む、自組織がセキュリティインシデントを管理するためのプロセスを確立する。
・ 一般的な脅威シナリオ及び自組織固有の脅威シナリオに対応するセキュリティインシデント対応計画を策定する。制御システムを保有する場合は制御システムも対象とした脅威シナリオにも対応したセキュリティインシデント対応計画を策定する。策定した対応計画については年 1 回以上訓練を実施し、訓練で得られた教訓をもとにセキュリティインシデント対応計画を更新する。
・ インシデント対応計画には、次の活動が含まれる場合がある。
  * 何がセキュリティインシデントに相当するか、基準に従ったセキュリティ事象の評価
  * セキュリティ事象及びインシデントの監視、検知、分類、分析及び報告
  * インシデントの種類に従った対応、危機管理の発動及び事業継続計画の発動の可能性、インシデントからの復旧、内部及び外部の利害関係者への伝達を含む、セキュリティインシデントの終結までの管理
  * 関係当局、供給者並び顧客など、内部及び外部の利害関係者との調整
  * インシデント管理活動のログ取得
  * 証拠の取扱い
  * 根本原因分析又は事後分析手順
  * 教訓及びインシデント管理手順、セキュリティ管理策についての改善
  * インシデント報告書の作成

11.2. 人的対策

11.2.1. 経営層の訓練及び従業員の管理

・ 組織の全ての従業員を対象としたトレーニングを年１回以上実施する。フィッシング、ビジネスメール詐欺、パスワードセキュリティなどの基本的な概念を網羅し、サイバーセキュリティに関する組織内文化を醸成する。
・ サイバーセキュリティの基本的なトレーニングに加え、制御システムの運用、維持、保全の担当者は、制御システムに特化したサイバーセキュリティのトレーニングを年１回以上実施する。
・ 雇用の終了又は変更後も有効なセキュリティに関する責任及び義務を定めて、従業員はその要求事項を遵守する。外部委託等の利害関係者に対しても同様の要求事項を伝達する。

11.2.2. 委託先管理

・ 重要インフラサービスに係る業務の外部委託選定の際には、事業場の要求事項に加えて、アクセスされる情報の分類や認識されたリスク等を考慮する。
自組織と委託先との業務委託契約書等には、委託先が自組織のセキュリティの要求を満たすセキュリティ対策に取り組む責任、従業員に対する意識向上の教育・訓練を実施する責任、委託終了後もなお有効なセキュリティに関する責任及び義務等について盛り込む。
なお、継続的に取り組むリスクアセスメントの結果次第では、契約文言の見直しが必要な場合も想定されるため、セキュリティ部門や法務部門等による情報交換の場を定期的に設けることが期待される。
・ 委託期間中においては、委託先に対するセキュリティに関する要求事項が確実に遂行されるよう、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。

11.2.3. テレワーク・遠隔制御

・ 組織の施設外から従業員が作業し、組織内の情報にアクセスする際に行われるテレワークにおいては、以下に例示するトピックについて方針を定め、従業員が遠隔作業している場合のセキュリティ対策を実施する。
    * テレワークサイトにおける、他者（家族、友人等）からの情報又は資源への認可されていないアクセスの脅威
    * 公共の場所にいる他者からの情報又は資源への認可されていないアクセスの脅威
    * 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項、制限事項
    * ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用
    * システムを遠隔で制御し初期化するためのセキュリティに配慮した仕組み
    * テレワークが終了したときの、権限及びアクセス権の失効

11.2.4. エスカレーション

・ 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにする。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

11.3. 物理的対策

・ 情報システムを収容する建物の屋根、壁、天井及び床を強固な構造物とし、外部に接する全ての扉を施錠する。入退室時におけるアクセスカード、生体認証等による認証の仕組みや、警備員、侵入者警報、監視カメラ等による監視システムを構築する。これにより、認可された要員だけが管理領域に入退できるようにする。
・ また、悪意ある活動を防止する観点から、当該領域への認可されていない物品の持ち込みを制限する。加えて、複数の作業要員を確保できる重要インフラ事業者等においては、単独での作業を制限するといった対応も有効である。
・ 火災、洪水、地震等の自然災害や、爆発物、武器等による人的災害についてリスクアセスメントを実施し、災害対策や、ランダムな物品検査を実施する。

11.3.1. 装置の管理

・ 重要インフラサービスの提供に係る装置（情報システム等）は、認可されていないアクセスの機会を低減できるように設置するとともに、可用性及び完全性を継続的に維持するため、適切に保守を実施する。
・ 重要システムの通信・電源ケーブルについて、ケーブル保護のための外装電線管の導入や、点検・終端箇所は施錠可能な部屋又は箱の設置を検討する。
・ ケーブル配線の物理的識別及び検査を可能にするため、ケーブルの各端に始点及び終点を示す詳細をラベル付けする。
・ 書類や取り外し可能な記録媒体について、セキュリティを保って保管し、不要になった場合にはセキュリティを保った仕組みを使用してそれらを破棄する。記憶媒体を持ち出す場合には認可を要求し持ち出し管理を行う。
・ モバイル機器など、通信機能がある記憶媒体においては、紛失や盗難時の対策として位置追跡及び遠隔データ消去機能を実装する。

11.3.2. 電源管理

・ 重要システムが稼働する施設について、雷対策や定期的な計画停電のスケジュールを管理して対応する。
・ 重要システムへ供給する電源系統を複数にすることや、無停電電源装置等を使用し

可用性を考慮した対策を実施する。

11.4.技術的対策

11.4.1. 利用者アクセスの管理

- ユーザーアカウントに管理権限を割り当てず、管理権限も用途ごとに設定する（バックアップ用、システム設定閲覧用、システム設定変更用等）。
- 離職者のアカウント管理として、全てのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有する全てのユーザーアカウントと、組織情報へのアクセスを無効にする。

11.4.2. 情報システム等のアクセス制御

- 公開サーバなど、インターネット上の資産では、悪用可能なサービス（RDP、SSH、SMB 等）を使用しない。また、インターネットに接続された情報資産では、不要なアプリケーションやネットワークプロトコルを全て無効化する。
- 運用上明示的に必要な場合を除き、制御システムはインターネット上には配置しない。例外が存在する場合には承認、文書化し、悪用を防止する措置を具備する。悪用防止の措置として、多要素認証や VPN の活用、ロギングによる動作の監視等が挙げられる。また、OT ネットワークへの接続は、特定の機能のため明示的に許可された通信を除き、全て拒否する。IT と OT 間の必要な通信経路にはファイアウォール等中継装置を設置し、厳密に通信を監視する。中継となるファイアウォール装置の設定、脆弱性についても適切に維持管理する。
- インターネットに接続された情報システムについて、サービス不能攻撃(DoS 攻撃、DDoS 攻撃）を受けるサーバ装置（IoT 機器含む)、端末、通信回線装置又は通信回線から監視対象を特定し、システムが扱う情報の可用性に基づいてサービス不能攻撃（DoS 攻撃、DDoS 攻撃）の発生を想定し、対応を行う。

11.4.2.1. アカウントロック

- 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する。

11.4.2.2. パスワード管理

- ハードウェア、ソフトウェア等を使用する前に、製造元のデフォルトパスワードを変更する。制御システムについても、新規又は将来の全てのデバイスのデフォルト認証情報を変更する方針とする。これは、実現が容易なだけでなく、

将来的にサイバー攻撃手法が変化した場合の潜在的なリスクも軽減される。ハードコードされている等、デフォルトパスワードの変更が不可能な場合、代替セキュリティ管理策を実施し、ログインのアクセスログを監視する。

- 自組織の情報資産に対して、パスワードの用途ごとに最小パスワード長及び複雑さを設定する。パスワードの用途は、「ログインパスワード」「パスワードロックされた圧縮ファイルや文書ファイル」「無線アクセスポイントへの接続」等がある。アカウントロックや多要素認証等、他の管理策との組み合わせを考慮して、パスワード長及び複雑さを設定する。
- 自組織のサービスや資産に関して、一意かつ個別のパスワードを設定する。利用者に対し、アカウント、アプリケーション、サービス等でパスワードを再利用させないようにする。

11.4.2.3. 多要素認証の活用

- ハードウェアベースの多要素認証技術が利用可能な場合は有効にする。利用できない場合にはソフトウェアベースを利用する。SMS による多要素認証は、やむを得ない場合を除きできるだけ避けるようにする。

11.4.3. 技術的脆弱性の管理

- 運用する情報システムのソフトウェア及びその他の技術に関して、関連する技術的脆弱性を特定し、組織の情報資産とあわせて整理する。
- 外部から取得した情報システムの場合には、供給者に脆弱性の報告や取扱い及び開示を実施することを要求する。
- 特定した脆弱性に対しリスクアセスメントを実施し、対応方針を検討する。
- ソフトウェアの更新やパッチ適用等により修復をする際には、「正当な供給元からのパッチである」、「修復の真正性を検証する仕組みを実装する」、「ロールバックの手順を定める」等、適切な対策を実施する。
- 適用可能な更新、パッチ等がない又はその他の理由により修復が困難な場合には、次のような管理策を検討する。
  - ＊ 提供元が提案する回避策の適用
  - ＊ その脆弱性に関係するサービス又は機能の停止
  - ＊ ネットワーク境界におけるアクセス制御
  - ＊ 適切なトラフィックフィルタ（仮想パッチ）の適用による攻撃からの保護
  - ＊ 実際の攻撃を検知するために、監視を強化

11.4.4. 暗号化を活用した情報管理

11.4.4.1. 機微なデータの取り扱い

・ 個人情報及び認証情報を含む機微なデータは、暗号化して保存され、許可された管理者のみがアクセスできるようにする。

11.4.4.2. 暗号化通信及び電子署名

・ 転送中のデータを保護するために、適切な TLS 暗号化を導入する。
  * 非推奨や、脆弱な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。
  * 制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行う。
  * 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照する。なお、暗号技術に係る国内外の法令及び規制の存在について留意する。
  * 完全性が求められる情報を取り扱う情報システムについては、STARTTLS 等の通信経路の暗号化機能や、DMARC 等の電子署名の付与及び検証を行う機能を設ける必要性の有無を検討する。

11.4.5. 多層防御

・ サイバー攻撃の高度化により従来型の境界防御のみでは侵入を検知することが困難であるため、複数の対策を組み合わせ、一つの対策で防御できなくても次の対策で防御又は検知するという考え方のもと、セキュリティ対策を検討する。

【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項

次頁以降に示すサイバー攻撃リスクの特性並びに対応及び対策の考慮事項は、重要インフラ事業者等が主にコンティンジェンシープラン（以下、「ＣＰ」という。）及び事業継続計画（以下、「ＢＣＰ」という。）を策定・改定する際に考慮されることを期待するものである。

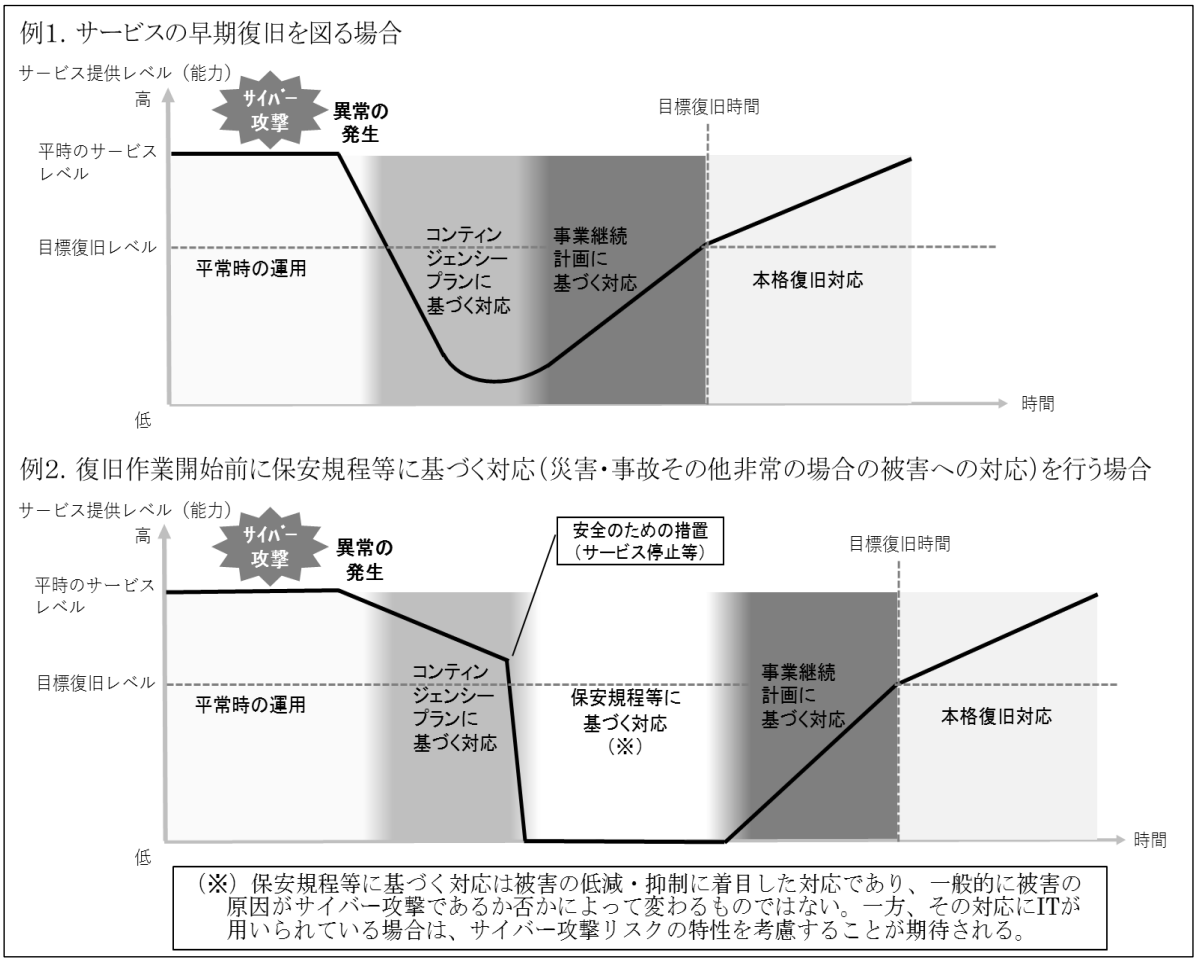
ＣＰ及びＢＣＰの名称や記載の範囲、発動のタイミング等は分野や事業者等によって異なる場合があるため、次頁以降の特性等を考慮して策定・改定すべき対象ドキュメント（以下、適用対象）は各事業者等の状況に応じて検討される必要がある。

適用対象の検討の参考として、図１にサイバー攻撃の発生から復旧までのフローの例を示す。図１に示す例（例１及び例２）はいずれもサイバー攻撃により異常が発生し、サービスレベルが時間とともに低下した後、ＣＰやＢＣＰに基づく対応を経てサービスレベルを復旧させる一連のプロセスを表したものである。

例１では、サービスの早期復旧を図るため早いタイミングでＢＣＰに基づく対応を開始している。一方例２では、安全のための措置として意図的にサービスを停止し、保安管理規定等に伴う対応を実施した後にＢＣＰに基づく対応を開始している。いずれの例においてもＣＰ及びＢＣＰは、次頁以降の特性等を考慮すべき適用対象となる。例２の保安規程等に基づく対応は被害の低減・抑制に着目した対応であり、一般的に被害の原因がサイバー攻撃であるか否かによって変わるものではない。一方、その対応にＩＴが用いられている場合は、次頁以降の特性等を考慮することが期待される。

図１サイバー攻撃の発生から復旧までのフローの例

（下記以外にも様々なフローが存在する。）



なお、以降に記載するサイバー攻撃リスクの特性は各々相互に関連しており、ある特性に対する考慮事項は他の特性に対しても有効なものもある。よって、ＣＰ及びＢＣＰの策定・改定においては、特定の特性に対する考慮事項だけではなく、他の特性に対する考慮事項も踏まえて、対応及び対策を検討することが必要である。

サイバー攻撃リスクの特性①

攻撃者の存在と多様な攻撃目的

サイバー攻撃は、自然災害等とは異なり、目的を持った攻撃者によって引き起こされる。その攻撃目的は、金銭・情報の窃取、主義・主張の表明、システム破壊によるサービスの停止等多様化している。組織的に計画されて行われる攻撃から内部犯行による攻撃まで、多様な攻撃者・攻撃目的に応じた様々な手法による攻撃が考えられるが、事前に攻撃者や攻撃目的を知ることは困難なケースが多い。

対応及び対策の考慮事項

【ポイント】
サイバー攻撃リスクの認識と被害発生に至るシナリオの作成

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- 自組織の重要インフラサービスの障害に繋がる可能性のあるサイバー攻撃の脅威（マルウェア等を用いた標的型攻撃、DDoS 攻撃等）とその影響を特定し、特に事業への影響が大きい脅威について、被害発生に至るシナリオの作成とそのシナリオへの対応を検討する。
  - **被害発生に至るシナリオの例**
    マルウェアに感染した機器（端末、USB メモリ等）を保守要員が持ち込むことにより、マルウェアが組織内の情報システムに感染し、さらにネットワークを介して最終的な攻撃目標である重要システムに侵入し、システムの改ざんや破壊、機密情報の漏えい等を引き起こす。結果として、サービスや事業の継続に深刻な影響を受ける。
- 攻撃予告、情報漏えいの疑い、攻撃の予兆（不審な通信やログの増加等）が検知された場合等のサイバー攻撃の発生のおそれがある状況においても、攻撃や障害の発生に備えた警戒態勢への移行や対策状況の緊急点検等の対応が必要になる可能性があることを考慮する。
  - **サイバー攻撃の発生のおそれがある状況の例**
    インターネットを通じて重要インフラサービスを提供しているシステムに対する DDoS 攻撃を示唆して金銭や特定の事業活動の停止等を要求される。

サイバー攻撃リスクの特性②

攻撃手口の高度化

サイバー攻撃の手口は絶えず考え出され高度化している。新たな脆弱性を狙った攻撃のように現行技術をベースとした対策だけでは回避困難な攻撃や、事業者側が想定していない新しい手口で行われる攻撃等が考えられる。

また、新しい手口で攻撃が行われた場合、その影響の度合や範囲を正確に把握できない可能性がある。

対応及び対策の考慮事項

【ポイント】
攻撃手口に関する日々の情報収集並びにＣＰ及びＢＣＰの適時見直し

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- 攻撃手口等に関して、JPCERT/CC 等の関係主体が提供する情報を日々収集し、新たな攻撃手口に対しては現状のＣＰ及びＢＣＰで対応可能か確認し、必要に応じて見直しを図る。
- 新たな攻撃手口の情報を入手した場合は、自組織の対策の状況とその有効性及び被害の有無を早急に確認するとともに、自組織への攻撃到達に備え、一定期間、監視機能・体制を強化する。
- サイバー攻撃手口の高度化に追随するため、サイバーセキュリティに関する十分な知識と判断能力を持った人材を、ＣＰ及びＢＣＰの策定・改定や対応時の体制に加える。必要に応じて外部の専門組織を活用する。
- 影響範囲等が正確に把握できていない状況でも、重要インフラサービスの提供において最低限要求されるサービスレベルを維持するため、必要な調査項目や調査の優先順位をＣＰ及びＢＣＰ策定時に検討しておく。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- 新たな攻撃手口をサイバー攻撃リスクとして認識した場合、計画発動時の対応に関与する可能性のある要員に対して、当該リスクの管理方針や、見直しを行ったＣＰ及びＢＣＰの浸透を図る。

サイバー攻撃リスクの特性③

急速な被害拡大に繋がる攻撃が行われる可能性

サイバー攻撃の被害は、攻撃を受けた箇所を起点にネットワークを介して急速に拡大する可能性がある。特定の端末に感染したマルウェアが同一組織内のネットワーク上にある別の端末に自身を複製することで被害が広がるケースや、外部委託先で発生したサイバー攻撃の被害が自社システムにまで広がるケース、自社システムが不正に操作され他社への攻撃に利用されることで自らが加害者の立場になってしまうケース等も考えられる。

対応及び対策の考慮事項

【ポイント】
サービス中断に繋がる手段も視野に入れた被害拡大への対応

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- サイバー攻撃の被害の拡大を防止するため、通信の遮断や重要システムの停止等を行うことも視野に入れる。ネットワークやシステムの構成を把握し、遮断・停止を行うポイントについて検討しておく。
- 遮断・停止を行う場合、重要インフラサービスの継続に大きな影響を与える可能性があるため、実施の判断を行う責任者を明確にしておく。また、的確な判断を行うため、停止可能なタイミングや期間、停止した場合の影響範囲、代替手段の有無等を計画策定時に整理しておく。
- 調査に必要な情報には遮断・停止後に取得できなくなるものもあるため、遮断・停止前に時間の許す限り情報を収集する。収集すべき情報の例として、遮断・停止により失われるメモリ情報、プロセス情報や、遮断・停止中は取得できないログ等があり、環境に合わせて取得方法や手順を検討しておく。
- サイバー攻撃の被害が相互に及ぶ可能性のある外部委託先との対応状況の共有や、重要インフラサービスの利用者等への対応状況の公表を検討しておく。サイバー攻撃の場合に公表を検討すべき特徴的な情報として、対応や調査で判明した攻撃手口、被害原因（ソフトウェアの脆弱性、設定の不備等）、攻撃への対処状況（被害拡大防止のための暫定対処、被害原因に対する根本対処）、顧客等への二次被害の発生状況や今後発生する可能性の有無等がある。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- 攻撃の拡散に備えた対策の導入を必要に応じて検討する。対策の例として、ネットワークセグメント分割（重要システムの隔離）、IPS/プロキシサーバ（不審な外部通信の遮断）、EDR[1]（影響範囲の特定と被害端末の隔離）等がある。

[1] Endpoint Detection and Response の略。

サイバー攻撃リスクの特性④

執拗な攻撃が行われる可能性

サイバー攻撃は、その目的が達成されるまで執拗に行われる可能性がある。システム復旧の際、被害に遭う以前の状態に漫然と戻した場合にまた同じ攻撃が行われ被害を受けるケースや、システム復旧対応中に再度攻撃が行われるケース、攻撃への対処後にそれを回避する方法で再度攻撃が行われるケースも考えられる。

また、インターネットに接続していないクローズド環境や、汎用性の低いシステムで構成される環境であっても、システム構成やシステム仕様等に関する情報を様々な手段で時間をかけて収集した上で攻撃が行われるケースも考えられる。

対応及び対策の考慮事項

【ポイント】
サイバー攻撃の再発の可能性及び環境の特殊性の考慮

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- 重要インフラサービス復旧前に被害原因（ソフトウェアの脆弱性、設定の不備等）の分析、特定、対処（パッチ適用、マルウェア駆除、システム再構築等）を行う。非常用システムを使用してサービスを復旧する場合も、同様の手口による攻撃への対処を非常用システムに行った上で稼動させる。
- 復旧中に再度サイバー攻撃を受けた場合に備え、サイバー攻撃への対処を行うチームと重要インフラサービスの復旧を行うチームの体制を分けるとともに、役割分担や連携方法を検討しておく。
- ログ等の調査の結果、サイバー攻撃が執拗に行われていた痕跡（長期間に渡る繰り返しの攻撃の試行、対策後の攻撃の再発等）が見られた場合、重要インフラサービスの復旧後においても、一定期間、監視機能・体制を強化する。
- 被害の発生原因が十分に特定できていない状況で、システム復旧せざるを得ない場合には、攻撃者が仕掛けたプログラム等が残存する可能性を想定し、被害を受けたシステムに加え、周辺のシステムに対する監視機能・体制を強化する。
- 汎用性の低いシステムが存在する環境での対応においては、当該環境のシステムに対して取り得る対応の制約（システム動作への影響の懸念によりパッチの適用不可等）、対応に使用できる機器やネットワークの制約（特殊な通信仕様により調査機器の接続や通信の解析が困難等）、対応に関与できる人員の制約（特殊なシステム仕様を理解した人員が必要等）を考慮する。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- クローズドな環境や汎用性の低いシステムにおいてもサイバー攻撃による被害が発生し得ることを認識した上で、監視等の必要な対策を検討する。

サイバー攻撃リスクの特性⑤

同時多発的な攻撃が行われる可能性

サイバー攻撃では物理的な距離に関係なく、広範囲にわたるターゲットを同時に攻撃することが可能である。自組織の複数の拠点に同時に攻撃が行われるケースや、自組織のシステムと供給者のシステムに同時に攻撃が行われるケース、メインシステムと非常用システムに同時に攻撃が行われるケース等が考えられる。

対応及び対策の考慮事項

【ポイント】
関係主体等との連携を前提とした同時多発攻撃への対応

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- 複数のインシデントが同時に発生した場合には、業務影響、リスク許容度、対応に必要な資源等を踏まえて、対応の要否・優先順位を判断する必要があるため、計画策定時に判断基準を明確にする。
- 重要インフラサービスの提供に係る供給者や外部委託先がサイバー攻撃を受けた場合に備え、供給者や外部委託先のＣＰ及びＢＣＰの整備状況や対応時の自組織との連携内容等について確認する。
- 複数の重要インフラ事業者等に同様のサイバー攻撃が行われる可能性を考慮し、各分野の業界団体、セプター、サイバーセキュリティ関係機関等を通じて、自組織が受けたサイバー攻撃の手口、攻撃元、特徴的な痕跡等、他組織での被害防止に資する情報を積極的に共有し、更なる被害の発生の防止に分野全体で努める。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- メインシステムと非常用システムが同時に使用不能になる可能性を低減する対策を検討する。対策の例として、業務上必要な通信（メインシステムと非常用システムの間のデータコピーやバックアップ等）以外の遮断や、メインシステムと非常用システムのネットワークの分離等がある。
- システムによる重要インフラサービスの維持が困難になるケースを想定し、手動での機能制御、要員による代替業務、代替サービスの提供等の代替手段を用意する。
- 組織内外の関係者への情報共有手段について、サイバー攻撃の影響によりメール等の通常時の情報共有手段が使用できなくなることを考慮し、複数の情報共有手段をあらかじめ用意する。

サイバー攻撃リスクの特性⑥

検知が困難な攻撃が行われる可能性

サイバー攻撃に対して十分な検知策を講じていない場合、攻撃を認識できず長期間にわたり攻撃を受け続ける可能性がある。不正行為の検知に繋がるログを削除して回避しようとするケースや、実態とは異なる数値を表示して正常に動作しているように見せかけ不正行為を行うケース等も存在し、検知が遅れるほど被害が拡大する可能性が高くなる。また、攻撃を検知した以後も、攻撃者及び攻撃目的を特定するのは困難なケースが多い。

対応及び対策の考慮事項

【ポイント】
影響調査に係る情報等の開示手続きの明確化

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- システムベンダー等の保守業者による影響範囲の特定が困難な攻撃に対しては、外部のセキュリティベンダー、インシデント対応組織等に調査協力を依頼する場合も想定されるが、その際、ログや侵害された機器等の開示が必要になる場合もあるため、必要な手続き（開示の責任者や判断基準、開示可能な組織、機密を含む情報を安全に伝達するための提供手段等）、開示する情報（ログ項目や形式等）とその制限（機密情報や個人情報等の開示不可な情報の種類等）を明確にしておく。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- 攻撃による異常の痕跡を調査するため、重要システムの構成を把握するとともに、当該システムの通常時の動作や出力ログの内容について把握しておく。また、ログを改ざん、削除等から保護するための対策を行う。
- 長期間に渡り発覚しなかった攻撃を過去に遡って調査するため、平時に取得している各種ログを一定期間保存する。保存期間はサイバーセキュリティ関係機関やセキュリティベンダーが推奨しているログの保存期間等を考慮し検討する。また、サイバーセキュリティ関係機関等が公開している情報を参照し、調査のために平時から取得が推奨されるログの取得状況を確認するとともに、必要に応じて取得を検討する。

サイバー攻撃リスクの特性⑦

誤った判断や対処を誘発する攻撃が行われる可能性

サイバー攻撃によって、誤った判断や対処が誘発される可能性がある。例として、監視や制御等に使用する管理システムに実態と異なるアラートや数値を表示して判断を誤らせるケースや、障害対応時のシステム操作が意図しない動作を引き起こすようにシステムを不正変更（数値を上げる操作で数値が下がる、システム停止の操作でシステムが停止しない等）するケース等が考えられる。

対応及び対策の考慮事項

【ポイント】
異なる種類の監視情報の併用による正確な事態把握

【ＣＰ及びＢＣＰの策定・改定における考慮事項】

- サイバー攻撃の影響範囲が特定できていない段階では、管理システムに対しても攻撃の影響が及んでいる可能性を考慮し、改ざんの痕跡や監視情報間の不整合等がないか確認を行う。
- 管理システムが改ざんされている疑いがある場合は、重要インフラサービスの提供状況の目視確認や手動での物理的な制御操作等、他の信頼できる手段を用いて監視や制御等を行うなど、複数の対応手順を検討しておく。

（ＣＰ及びＢＣＰの発動に備えた平時の対策）

- システムに対する不正な変更の有無を確認するための体制・仕組みを検討する。確認すべき箇所の例として、ハードウェア構成（接続機器等）、ソフトウェア構成、ファイル構成、システム設定等がある。
- 重要インフラサービスの監視機能へのサイバー攻撃による、実態と異なる監視情報の表示等に備え、監視手段を複数用意する。

参考文献

（マネジメント関連）

- 米国国立標準技術研究所(NIST:National Institute of Standards and Technology). 重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.1 版. 独立行政法人 情報処理推進機構. 2019-01. https://www.ipa.go.jp/security/publications/nist/
- 内閣官房 内閣サイバーセキュリティセンター. 企業経営のためのサイバーセキュリティの考え方. 2016-08-02. https://www.nisc.go.jp/pdf/council/cs/jinzai/dai03/03shiryou01.pdf
- 経済産業省, 独立行政法人情報処理推進機構. サイバーセキュリティ経営ガイドライン Ver3.0. 経済産業省. 2023-03. http://www.meti.go.jp/policy/netsecurity/mng_guide.html
- JIS Q 27014:2015, 情報技術 – セキュリティ技術 – 情報セキュリティガバナンス.
  【対応国際規格】
  ISO/IEC 27014:2013, Information technology – Security techniques – Governance of information security.
- JIS Q 31000:2019, リスクマネジメント – 指針.
  【対応国際規格】
  ISO 31000:2018, Risk management – Guidelines.
- JIS Q 27001:2014, 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム – 要求事項.
  【対応国際規格】
  ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- JIS Q 22301:2013, 社会セキュリティ – 事業継続マネジメントシステム – 要求事項.
  【対応国際規格】
  ISO 22301:2012, Societal security – Business continuity management systems – Requirements.
- JIS Q 19011:2012, マネジメントシステム監査のための指針.
  【対応国際規格】
  ISO 19011:2011, Guidelines for auditing management systems.
- リスクマネジメント規格活用検討会, 編集委員長 野口和彦. ISO 31000:2018 リスクマネジメント 解説と適用ガイド. 日本規格協会. 2019-06-27.

- 米国エネルギー省. Cybersecurity Capability Maturity Model(C2M2) Ver2.1. 2022-06.
  https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
- 米国サイバーセキュリティ社会基盤安全保障庁(Cybersecurity and Infrastructure Security Agency). Cross-Sector Cybersecurity Performance Goals Ver1.0.1. 2023-03.
  https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- 内閣官房 内閣サイバーセキュリティセンター. サイバーセキュリティ関係法令 Q&A ハンドブック Ver.1.0. 2020-03-02.
  https://security-portal.nisc.go.jp/guidance/law_handbook.html
- 経済産業省. グループ・ガバナンス・システムに関する実務指針. 2022-07-19.
  https://www.meti.go.jp/policy/economy/keiei_innovation/keizaihousei/corporategovernance/guideline.html
- 株式会社東京証券取引所. コーポレートガバナンス・コード. 2021-06-11.
  https://www.jpx.co.jp/equities/listing/cg/index.html
- 英国国家サイバーセキュリティセンター(National Cyber Security Center). Cyber Assessment Framework Ver3.1. 2022-04.
  https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
- Center for Internet Security (CIS). CIS Controls V8. 2021-05.
  https://www.cisecurity.org/controls
- 経済産業省. サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF). 2019-04-18.
  https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
- 米国国防総省. Cybersecurity Maturity Model Certification(CMMC) 2.0. 2021-11.
  https://dodcio.defense.gov/CMMC/Documentation/

（リスクアセスメント関連）

- 独立行政法人情報処理推進機構 技術本部 セキュリティセンター. 制御システムのセキュリティリスク分析ガイド第２版. 2023-03.
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
- 内閣官房 内閣サイバーセキュリティセンター. 機能保証のためのリスクアセスメント・ガイドライン 1.0 版. 2023-03.
  https://www.nisc.go.jp/policy/group/cyber/policy.html

- NIST. SP 800-82 Rev.2 Guide to Industrial Control Systems (ICS) Security. 2015-05.
  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

（サプライチェーン・リスクマネジメント関連）

- 内閣官房 内閣サイバーセキュリティセンター. 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書. 2016-10-25.
  https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
- 経済産業省. IT 製品の調達におけるセキュリティ要件リスト. 2018-02-28.
  http://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf
- 独立行政法人情報処理推進機構 セキュリティセンター. IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック. 2018-02-28.
  https://www.ipa.go.jp/security/it-product/guidebook.html
- 内閣官房 内閣サイバーセキュリティセンター. 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル. 2022-07-29.
  https://www.nisc.go.jp/pdf/policy/general/SBD_manual.pdf

（事業継続計画関連）

- 内閣官房 内閣サイバーセキュリティセンター. 政府機関等における情報システム運用継続計画ガイドライン～（第 3 版）～. 2021-04.
  https://www.nisc.go.jp/pdf/policy/general/itbcp1-1_3.pdf
- 内閣府. 事業継続ガイドライン. 2023-03.
  https://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline202303.pdf

（CSIRT 関連）

- 一般社団法人 JPCERT コーディネーションセンター. インシデントハンドリングマニュアル. CSIRT マテリアル 運用フェーズ. 2021-11-30.
  https://www.jpcert.or.jp/csirt_material/operation_phase.html
- 一般社団法人 JPCERT コーディネーションセンター. CSIRT マテリアル.
  https://www.jpcert.or.jp/csirt_materi

（対策関連）

- サイバーセキュリティ戦略本部. 政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）. 2023-07-04.
  https://www.nisc.go.jp/policy/group/general/kijun.html

- ISO/IEC 27002:2022, Information Security, cybersecurity and privacy protection – Information security controls.
- 一般財団法人 日本情報経済社会推進協会. CSMS 認証基準（IEC62443-2-1）Ver2.0. 情報マネジメントシステム認定センター. 2016-10-04. https://isms.jp/csms/std/index.html
- 一般財団法人 日本情報経済社会推進協会. CSMS ユーザーズガイド －CSMS 認証基準（IEC62443-2-1）対応－Ver1.2. 情報マネジメントシステム認定センター. 2015-05. https://isms.jp/csms/std/index.html
- 経済産業省. 情報セキュリティ管理基準（平成 28 年改正版）. 2016-03-01. http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html
- IoT 推進コンソーシアム, 総務省, 経済産業省. IoT セキュリティガイドライン ver1.0. 2016-07. http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
- 内閣官房 内閣サイバーセキュリティセンター. 政府機関等の対策基準策定のためのガイドライン（令和５年度版）. 2023-7-4. https://www.nisc.go.jp/policy/group/general/kijun.html
- 一般社団法人 JPCERT コーディネーションセンター. 高度サイバー攻撃への対処におけるログの活用と分析方法. 2022-05-23. https://www.jpcert.or.jp/research/apt-loganalysis.html
- 一般社団法人 JPCERT コーディネーションセンター. 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて. 2016-04-21. https://www.jpcert.or.jp/research/apt-guide.html