資料２

「重要インフラにおける安全基準等策定指針の改定（案）について

資料２－１　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５版）等の改定案について

資料２－２　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指針（第５版）（案）

資料２－３　重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第１版）

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５版)等の改定案について

資料2－1

安全基準等策定指針（平成30年４月４日本部決定）改定の必要性の主な背景

・2018年は各地で複数の自然災害が発生し、重要インフラ事業者等においても、地震や台風によって、重要インフラサービスの停止等に繋がる被害が発生した。災害による直接的な被害だけでなく、大規模停電に伴う間接的な被害を受ける事態なども発生した。
・様々なデータの活用のために円滑なデータ流通が重要である一方、データ管理に関するルールの策定が世界各地で進められており、これらの国際的な規制等の動向も踏まえた望ましいデータ管理の在り方を検討する必要がある。

サイバーセキュリティ戦略（平成30年7月27日閣議決定）

4.2　国民が安全で安心して暮らせる社会の実現
　4.2.2　官民一体となった重要インフラの防護
(1)行動計画に基づく主な取組
②重要インフラ事業者等における適切な対応を促進するため、国は、安全基準等を策定するための指針を浸透させる取組を行うとともに、データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理（略）を含め、安全基準等を改善する取組を継続的に推進する。

【改定案】（平成31年４月18日重要インフラ専門調査会にて承認）

１．災害による障害の発生しにくい設備の設置及び管理

重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい配置とする等、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施することにより、適切な設備の設置及び管理を行う仕組みを構築する。

２．データ管理

システムのリスク評価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。

また、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。

（加えて、指針の関連文書である「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の別紙に、具体的な事象（脅威）の例及びリスク源の例として「法令・政策の不認識」を追記する。）

３．その他

空港分野の追加等に伴い、所要の改正を行う。

【2018年の災害に起因する重要インフラサービス障害例及びシステム不具合等の事案】

- ●大規模停電
- ●空港ビル（設備停止）　等

- ●電力Ｗｅｂサイト：停電情報が更新できない
- ●鉄道Ｗｅｂサイト：運行状況が更新できない
- ●通信事業者　　：データセンター停電
　　（一部サーバー5時間停止）

【データ管理(国際動向）】


EU
GDPR（一般データ保護規則）


米国
FISMA(連邦情報セキュリティマネジメント法)


中国
サイバーセキュリティー法

※出典：第６回官民データ活用推進戦略会議合同会議　参考資料

【指針及びリスクアセスメント手引書】

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

- 重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、分野毎に事業所管省庁や業界団体等が作成する「安全基準等」において規定が望まれる項目を整理・記載したもの

重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書

- 機能保証の考え方に基づくリスクアセスメントの観点や具体的な作業手順等を記載したもの

（参考）重要インフラの情報セキュリティ対策に係る第４次行動計画

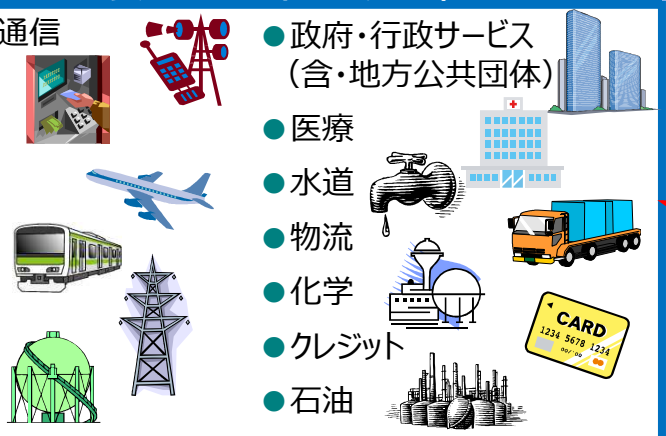
H29.4.18決定
H30.7.25改定

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ（１４分野）

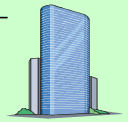
- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



ＮＩＳＣによる調整・連携

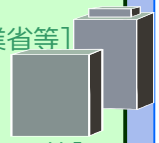
重要インフラ所管省庁（５省庁）

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、空港、鉄道、物流］



関係機関等

- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］



重要インフラの情報セキュリティ対策に係る第４次行動計画

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

資料２－２

重要インフラにおける情報セキュリティ確保に係る
安全基準等策定指針
（第５版）
（案）

平成３０年４月４日
令和元年　月　日改定

サイバーセキュリティ戦略本部

はじめに
（本指針の要点）

【本指針の位置付け、構成】

重要インフラ事業者等は、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場であり、第４次行動計画に記載された「機能保証の考え方」を踏まえ、必要な対策に取り組むことが重要となる。具体的には、情報セキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を実現することなどであり、その際に考慮すべき事項は、重要インフラ事業者等が事業を営む際の基準である「安全基準等」に規定されることが望ましい。本指針は、このような安全基準等に規定されることが望まれる項目を整理・記載したものである。

また、本指針に記載されている項目は、ＰＤＣＡサイクルに沿った情報セキュリティの対策の項目となっている。策定に当たっては、情報セキュリティの国際標準である「情報セキュリティマネジメントシステム」に加えて、ＮＩＳＴの「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」や「ＣＳＭＳ認証基準」等の重要インフラ分野関連の情報セキュリティの標準も考慮し、本指針によって重要インフラに関する主要な基準を網羅できるよう構成している。

【情報セキュリティ対策のＰＤＣＡサイクルに取り組む際の重要事項】

- **経営層に求められる行動**

「情報セキュリティリスク」は「機能保証の考え方」を踏まえた事業運営を不確かにする影響力があることを認識し、その対処の在り方を判断するために必要な情報セキュリティリスクアセスメントの実施を指示すること。また、情報セキュリティ対策のＰＤＣＡサイクル推進に当たり、必要な資源（予算・体制・人材等）の継続的な確保及び適切な配分に努めること。さらに、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を定期的に検証し、情報セキュリティリスク対応戦略の見直しの必要性等について意思決定を行うこと。これらの取組に際して、「企業経営のためのサイバーセキュリティの考え方」、「サイバーセキュリティ経営ガイドライン」等を参照すること。

- **定期的な情報セキュリティリスクアセスメントの実施**

情報セキュリティリスクは、新たな脅威の発生や技術的脆弱性の発見に加えて、重要インフラ事業者等を取り巻く事業環境の変化や利害関係者からの新たな要求等によって絶えず変化する。そこで、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」等を参考として、定期的にリスクアセスメントを実施し、情報セキュリティリスクの変化が重要インフラサービスの安全かつ持続的な提供に与える影響を再評価すること。

- **サイバー攻撃の特性を踏まえた対応計画の策定**

重要インフラサービス障害を引き起こす事象のひとつであるサイバー攻撃の発生に際して、迅速かつ適切な初動対応を実現するため、初動対応の方針、手順等を具体的に定めた「コンティンジェンシープラン」をあらかじめ策定すること。併せて、サイバー攻撃等を起因とした重要インフラサービス障害からの復旧対応の方針、手順等を定めた「事業継続計画」を策定すること。そして、これらの対応計画の策定に際して、本指針に記載された「サイバー攻撃リスクの特性」や「対応及び対策の考慮事項」を考慮すること。

- **迅速かつ柔軟な対処態勢の整備**

ＰＤＣＡサイクルに基づく、中長期的な視点からの情報セキュリティリスクへの対応に加え、重要インフラ事業者等が構築する監視の仕組みによって日々検知されるサイバー攻撃の予兆等に対して、迅速かつ柔軟な対処を可能とする態勢を整備すること。

目次

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

国民生活及び社会経済活動は、様々な重要インフラサービスによって支えられており、その機能を実現するために情報システムが幅広く用いられている。

こうした中で、重要インフラはその性質上、安全かつ持続的なサービスの提供が求められていることから、その防護に当たっては、「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「第４次行動計画」という。）に記載された「機能保証の考え方」を踏まえ、サービスの提供に必要な情報システムのセキュリティを確保し、サイバー攻撃等による重要インフラサービス障害の発生を可能な限り減らすとともに、障害発生の早期検知や、障害の迅速な復旧を図ることが重要となる。また、重要インフラサービスは、その機能が停止又は低下した場合に多大なる影響を及ぼす可能性があることから、緊密な官民連携によって重点的に防護していく必要がある。

機能保証の考え方

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

（「重要インフラの情報セキュリティ対策に係る第４次行動計画」からの抜粋）

重要インフラ事業者等においては、政府機関による必要な支援の下、経営層が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じること（情報セキュリティに係るリスクマネジメントの実施）が求められる。また、サイバー攻撃等の速やかな検知と適切な対処によって、重要インフラサービスの安全を確保し、かつ、自ら及びステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続できるように、適切な対処態勢を整備することも併せて求められる。

これらの推進において特に重要となるのは、重要インフラ事業者等が、事業主体であると同時に社会的責任を負う立場であることを認識し、重要インフラ分野の特性に応じた必要な又は望まれる情報セキュリティ対策を着実に実施するとともに、事業環境等の変化を捉えつつ、ＰＤＣＡサイクルに沿って情報セキュリティ対策を継続的に改善していくことである。

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。

このことを踏まえ、指針においては、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、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。

重要インフラ事業者等における必要な又は望まれる情報セキュリティ対策の実施を確実なものとするためには、これらの「安全基準等」において、情報セキュリティ対策の項目及び水準が文書において明示されることが必要である。すなわち、上記①から④までを参照することにより、重要インフラ事業に携わる全ての関係者が、自らが「何をすべきか」「どの程度すべきか」を理解できることが期待される。

3. 指針の位置付け

本指針は、重要インフラにおける機能保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、「安全基準等」において規定が望まれる項目を整理・記載することによって、「安全基準等」の策定・改定を支援することを目的としている。

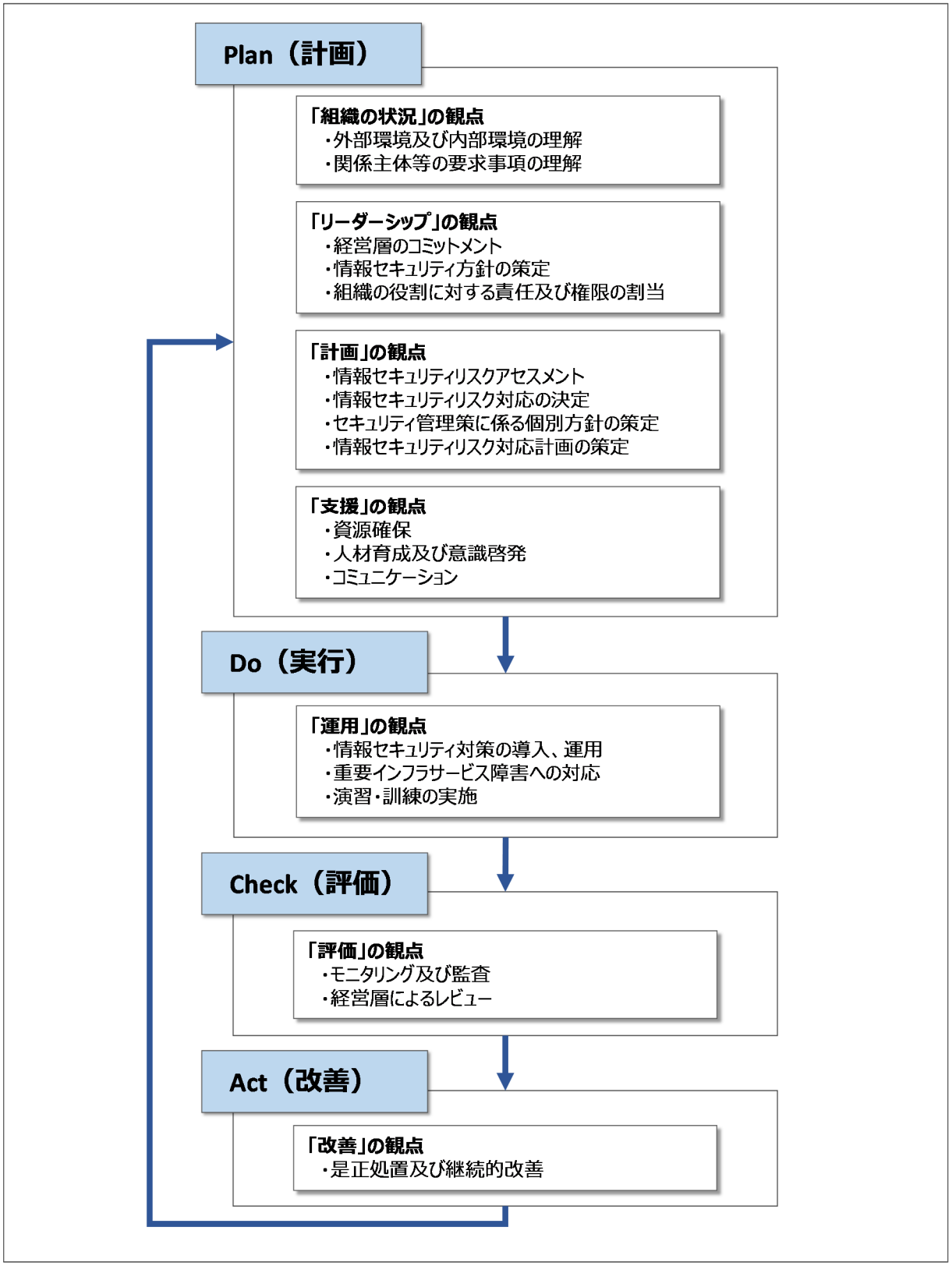
このため、本指針においては、重要インフラ事業者等が自主的な取組や継続的な改善を行う際に参照しやすいよう、情報セキュリティの対策項目をＰＤＣＡサイクルに沿って記載している。（図表１に本指針における重要インフラの情報セキュリティ対策の全体像を掲載する。）

なお、本指針は、あくまで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について、「情報セキュリティ対策」に特化して記載したものであることから、各重要インフラ分野又は各事業者等が「安全基準等」の策定・改定を行うに際しては、下記の２点に留意する必要がある。

- 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、本指針に記載されている項目の中に、「安全基準等」に規定する必要がないものもあり得ること

- 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、本指針に記載のない項目について、「安全基準等」に規定する必要がある場合もあり得ること

また、本指針に記載されている対策の項目及び当該項目の水準等に関して、どの「安全基準等」に定めるかということについては、各重要インフラ分野の関係法令の規定及び既存の「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することが期待される。



図表１　重要インフラにおける情報セキュリティ対策の全体像

4. 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

情報セキュリティを取り巻く環境変化は加速度的に進んでおり、重要インフラ事業者等が参照する又は自らが定める「安全基準等」の継続的な改善の重要性も年々高まっている。

従来は不要と整理していた脅威への対応が、環境変化によって新たに必要となる可能性もあるため、環境変化による影響に関する定期的な確認作業と併せて、本指針を参照し、「安全基準等」の見直しの必要性を判断することが期待される。

なお、「安全基準等」の継続的な改善に当たっては、前述のとおり、本指針が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に絞って記載したものであることを踏まえ、本指針に加えて、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れる。

また、「安全基準等」の策定主体は、重要インフラ事業に携わる関係者への浸透に日頃から努めるとともに、重要インフラの国民生活への影響の大きさにかんがみ、国民の安心感の醸成を図る観点から、「安全基準等」の内容を情報セキュリティ対策の推進に支障を来さない形で広く公開することが期待される。

Ⅱ．「安全基準等」で規定が望まれる項目

1. 策定目的

重要インフラにおいて、機能保証の考え方を踏まえ、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及ぼす重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時に迅速な復旧を図るため、「安全基準等」の内容に照らした情報セキュリティ対策のＰＤＣＡサイクルに取り組む必要性がある旨を記載する。

2. 対象範囲

本指針の「【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」に記載された「対象となる重要システム例」や、「【別紙２】重要インフラサービスの説明と重要インフラサービス障害の例」に記載された「重要インフラサービス（手続きを含む）」、「重要インフラサービス障害の例」、「サービス維持レベル」等の内容を踏まえて、当該「安全基準等」の規定項目が対象としている範囲を記載する。

3. 関係主体の役割

「安全基準等」が対象とする重要インフラ分野の関係主体（※「定義・用語集」参照）について、網羅的かつ具体的に記載し、それぞれの情報セキュリティ対策に関する役割を明記する。特に、重要インフラ事業者等の役割については、第４次行動計画の「重要インフラ事業者等の経営層の在り方」等を参照の上、経営層の取組についても記載する。

4. 対策項目

重要インフラ事業者等は重要インフラサービスの安全かつ持続的な提供を実現するという社会的責任を負う立場であることを踏まえ、情報セキュリティ対策のＰＤＣＡサイクルに沿って列記した 4.1 から 4.4 までの対策項目の採否について検討する。

なお、情報セキュリティ対策のＰＤＣＡサイクルでは、通常、Ｐｌａｎでの分析結果を踏まえ対策を導出した上、Ｄｏで実行に移し、一定期間経過後、Ｃｈｅｃｋで対策の見直しの必要性を評価し、Ａｃｔで改善を実施するという流れになるが、実運用においては、Ｄｏでの監視・検知の結果次第では、緊急で対策内容を見直す等の動的な対応が必要となる可能性を認識する必要がある。

また、各対策項目の具体例等が記載された参考文献を「【別紙４】対策項目の具体例等の参照先」に記す。各対策項目の導入時に必要に応じて参照されたい。

4.1. 「Plan（計画）」の観点

4.1.1. 「組織の状況」の観点

（１）外部環境及び内部環境の理解

重要インフラサービスの安全かつ持続的な提供に必要な能力への影響が想定される、重要インフラ事業者等を取り巻く外部環境（政治や経済、社会等）及び重要イン

フラ事業者等の内部環境（組織体制や戦略、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。その際、サプライチェーン（サプライヤー、委託先等）と自組織の「依存関係」について、重要インフラサービスの提供に係る各種業務の抽出・分析等を通じて、正確に把握することが特に重要となる。

（２）関係主体等の要求事項の理解

重要インフラ事業者等の情報セキュリティ対策の取組（重要インフラサービス障害発生時の初動対応や復旧対応等も含む）に対する、関係主体、顧客、サプライヤー、委託先等からの要求事項を整理する。要求事項には、各事業分野の関係法令や契約等に規定された義務や、サプライヤーや委託先が提示する制限事項等も含まれる。

整理した内容は、前述の外部環境及び内部環境の状況を含めて、「情報セキュリティ方針の策定」や「情報セキュリティリスクアセスメント」等を実施する際に考慮すべき要素とする。また、情報セキュリティ対策の取組に対する従業員（行政機関の職員を含む）の意識向上の観点から、整理した内容を組織全体に共有することが期待される。

4.1.2. 「リーダーシップ」の観点

（１）経営層のコミットメント

重要インフラ事業者等の経営層は、重要インフラ事業者等に求められる「機能保証の考え方」を踏まえた事業運営の実現のため、情報セキュリティリスク[1]を評価し、適切に対処することを組織の内外に対して宣言する。なお、宣言に当たっては、次頁（２）の「情報セキュリティ方針」等を活用するものとする。

また、経営層は、情報セキュリティリスクへの対処に当たり、下記の「重要インフラ事業者等の経営層の在り方」を認識し、「企業経営のためのサイバーセキュリティの考え方[2]」、「サイバーセキュリティ経営ガイドライン[3]」等を参考としつつ、適切な行動を取ることが期待される。

【重要インフラ事業者等の経営層の在り方】

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の考え方を踏まえ、情報セキュリティ対策に取り組むこと。

[1] 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、情報システム、ＩＴを用いた制御システム等の情報資産に係る事象の結果（サイバー攻撃等に起因する重要インフラサービス障害）から認識されるリスクのこと。

[2] 「普及啓発・人材育成専門調査会」（平成２７年２月１０日 サイバーセキュリティ戦略本部決定）の下に設置された「セキュリティマインドを持った企業経営ワーキンググループ」において取りまとめられた、企業経営のためのサイバーセキュリティに係る基本的な考え方を示したもの。

[3] サイバー攻撃から企業を守る観点から、経営者が認識する必要がある「原則」や、情報セキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき「重要項目」等をまとめたもの。経済産業省及び独立行政法人情報処理推進機構にて策定。

- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な情報を的確に収集するとともに、必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。
- 情報セキュリティリスクへの対応が事業に与えた効果と影響の検証結果を踏まえ、取締役会ほか経営上の重要会議において、さらなる情報セキュリティリスク対応戦略の見直しの必要性及びその内容についての意思決定を行うこと。

※第４次行動計画に掲げられた内容をベースに、本指針策定に当たり必要な事項を追加及び一部修正したものである。

（２）情報セキュリティ方針の策定

重要インフラ事業者等は、内外に対する公式な文書として「情報セキュリティ方針」を策定する。情報セキュリティ方針の中において、重要インフラサービスを安全かつ持続的に提供するという社会的責任を負う立場である重要インフラ事業者等が、情報セキュリティ対策に取り組む目的や方向性を示すとともに、情報セキュリティ対策の取組に関連する関係主体等からの要求事項を満たすことや、情報セキュリティ対策の取組の継続的な改善についての経営層によるコミットメント等を示す。

情報セキュリティ方針は、組織内に伝達するとともに、必要に応じて組織外の関係主体等が入手できるようにする。また、情報セキュリティ方針が妥当かつ有効であることを、定期的な間隔で確認するとともに、自組織を取り巻く状況に大きな変化が発生した場合にも確認する。

（３）組織の役割に対する責任及び権限の割当

情報セキュリティ対策の取組を確実なものとするため、重要インフラ事業者等の経営層は、情報セキュリティ対策を推進する役割を担う部署及び従業員を決定するとともに、それらに対して責任及び権限を適切な範囲で割り当て、その割当状況を組織内に伝達して従業員同士の認識を合わせる。

その際、情報セキュリティ対策を推進する役割を担う人材の中でも、特に、リスクアセスメントで抽出されたリスクの監視及び対処の責任を持つとともに、明確な説明

を行い、説明した内容に対して責任を取ることが要求されるリスクオーナーを明確にすることが重要となる。

また、経営層と実務者層をつなぐとともに、事業戦略等を踏まえた情報セキュリティ対策を計画し、実務者層を指揮できる人材（ＣＩＳＯ等）を確保することが期待される。

さらに、制御システム等が運用される環境を保有する場合、サイバー攻撃等に起因する重要インフラサービス障害の防止・復旧にＯＴ[4]関連部門の人材が必要となることについて考慮することが期待される。

なお、上記以外にも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
- セキュリティインシデントの管理担当（ＣＳＩＲＴ等）
- 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
- 情報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（サプライヤー、委託先等）における情報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

[4] 本指針においては、情報通信技術（ＩＴ）を利用した制御システム等の運用技術のことを指す。

4.1.3. 「計画」の観点

（１）情報セキュリティリスクアセスメント

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、情報セキュリティに係るリスクを適切に管理すべく、次のような手順によって情報セキュリティリスクアセスメントを実施する。

① 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。また、その過程で自組織のリスクに対する態度[5]・リスク許容度[6]を分析する。

② 情報システム等の経営資源に対する「情報セキュリティリスク」を特定する（リスク特定)。

③ リスクに対する態度・リスク許容度等を考慮しつつ、「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（リスク分析)。

④ 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（リスク評価)。

※内閣サイバーセキュリティセンターの「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」には、機能保証の考え方に基づくリスクアセスメントの観点や上記手順の詳細等が記載されているため、本書と併せて参照すること。

※自組織の事業の特性や環境等によっては、他の手引書等の手法を適用することが有効な場合も考えられる。例えば IPA の「制御システムのセキュリティリスク分析ガイド」では、資産ベースと事業被害ベース（シナリオベース）を組み合わせたリスク分析手法および実効的なセキュリティ対策のための具体的な作業手順などが記載されている。

なお、重要インフラサービスを安全かつ持続的に提供するためには、重要インフラの分野やサービス特性によっては、情報セキュリティリスクに加えて、ＨＳＥ[7]等の観点からのリスクも特定し、分析・評価を行うことが期待される。ＨＳＥ等の観点とし

[5] リスクのアセスメントを行い、最終的にリスクを保有する、取る又は避ける、という組織の取組みのこと。リスクに対する態度を明らかにするとは、例えば「20%未満のサービスレベル低下を伴う重要インフラサービス障害の発生は年間３回以下とする」といったように、重要インフラ事業者等がどの程度のリスクをとって事業を営むのかを明らかにすることである。

[6] 自らの目的を達成するため、組織又はステークホルダーが負う準備ができている残留リスク（リスク対応後に残るリスク）の程度のこと。例えば「50%以上のサービスレベル低下を伴う重要インフラサービス障害の発生は年間１回以下」といったように定める。

[7] 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.21.0）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。

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。

また、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ことが期待される。

（２）情報セキュリティリスク対応の決定

リスクアセスメントで抽出した情報セキュリティリスクへの具体的な対応方法を決定する。リスク対応の選択肢には、「低減[8]」、「回避[9]」、「移転（共有）[10]」、「保有（受容）[11]」があり、「事象の結果による業務への影響度合い」や「事象の発生可能性」等を踏まえて、適切と考えられるものを選定する。

続けて、選定したリスク対応方法の実現手段としてのセキュリティ管理策を決定する。その参考として、以下の「(ア) 人的資源のセキュリティ (外部委託)」から「(コ) 情報セキュリティインシデント管理」に、重要インフラ防護の観点から安全基準等への盛り込みが期待されるセキュリティ管理策を示す。

なお、「ISO/IEC 27000 ファミリー規格」や「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 (NIST)」、「CSMS 認証基準 (IEC62443-2-1)」等にもセキュリティ管理策が示されている。これらの規格類に加えて、同業の重要インフラ事業者等のセキュリティ管理策の導入事例等も参考として、自組織にとって必要なセキュリティ管理策を見落としていないか継続的に検証することが期待される。

（ア）人的資源のセキュリティ（外部委託）

●委託前の対応事項（選定・契約条件）

重要インフラサービスに係る業務の外部委託先選定の際には、事業上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、委託先が自組織の情報セキュリティの要求を満たす情報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ための教育・訓練を実施する責任、委託終了後もなお有効な情報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。

---

[8] リスクに対して適切な管理策を適用すること。
[9] リスクを生じさせる活動を開始又は継続しないことを決定することにより、リスクを回避すること。
[10] 一つ以上の他者とリスクの全部又は一部を共有すること。
[11] 情報に基づく意思決定により、リスクを保有（受容）すること。

●委託期間中の対応事項

委託先に対する情報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。

（イ）資産の管理

●資産に対する責任

重要インフラサービスの提供に係る情報システムやソフトウェア、情報等の資産を特定した上、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し、維持管理する。これに併せて、ネットワーク構成図やデータの流れ図等も作成する。なお、情報システム等の設備及びその運用を、外部の供給者（例：ＩＴサービスやＩＴ基盤の構成要素等の供給者）が提供するサービスによって代替する場合には、サービスの一覧を作成し、維持管理する。

●情報分類と取扱い

重要インフラ事業者等の取り扱う情報について、その重要性や法的要求、国民の安心感への影響等に応じて、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。

また、作成、入手、利用、保存、運搬、送信~~移送~~、提供、消去といった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）を定め、実施する。

●データ管理

システムのリスク評価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。

また、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。

（ウ）アクセス制御

●利用者アクセスの管理

重要インフラサービスの提供に係る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適切に管理するため、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、作業者等を明確化するとともに、運用中においては利用者アクセス権の定期的なレビューを実施する。なお、情報システムへの特権的アクセス権の割当及び利用は特に厳重に管理する。

●情報システム等のアクセス制御

最小権限および職務の分離の原則を踏まえて、重要インフラサービスの提供に係る情報システムや情報へのアクセス（リモートアクセスを含む）を制限する。

また、セキュリティに配慮したログオン手順（例：ログイン失敗回数の制限）や、良質なパスワード（例：セキュリティ強度を高める文字種別や文字数）の利用を確実にする仕組み等を整備するとともに、情報システムや情報の重要度によっては、多要素認証などの高度な認証手段の活用も検討する。

（エ）暗号

●暗号を活用した情報管理

重要インフラサービスの提供に係る情報の機密性等を保護するために暗号技術を活用する場合には、暗号の利用方針や暗号に用いる鍵（暗号鍵）の管理方針を策定する。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。

（オ）物理的及び環境的セキュリティ

●セキュリティ確保が求められる領域

重要インフラサービスの提供に係る情報システムや情報のある領域（情報セキュリティや安全等の確保が求められる領域）を保護するため、物理的なセキュリティ境界を設けるとともに、物理環境のモニタリングや、認可された従業員や委託先だけにアクセスを許すための適切な入退管理の仕組みを構築する。

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。

●災害による障害の発生しにくい設備の設置及び管理

重要インフラサービスの提供に係る情報システム、データセンター等の設備については、各種災害による障害が発生しにくい配置とする等、災害が発生した場合であっても被害を低減できるような防止対策を事前に検討・実施することにより、適切な設備の設置及び管理を行う仕組みを構築する。

●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。通信ケーブルや電源ケーブルについては、傍受や損傷の可能性を考慮して配線する。

また、取り外し可能な外部記憶媒体等の装置の盗難を引き金にした機密情報の漏えいを防止するため、当該装置の使用制限や、持ち出しに係る事前承認の仕組みを整備する。装置の処分や再利用においても情報漏えいの可能性を考慮する。

（カ）運用時のセキュリティ管理

●運用の手順及び責任

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に関連する手順書は、作業の正確性の確保に加えて、セキュリティ基準を満たした運用を確実にするという点も踏まえて整備する。

また、情報システム、周辺設備等の変更（保守、修理等）については、実施中の情報セキュリティ対策への悪影響も想定されるため、責任者への承認手続きを含む変更管理のプロセスをあらかじめ定め、これに基づいて実施する。なお、保守や修理の際に用いるツール類は、原則として承認及び管理されたものとする。

さらに、重要インフラサービスの運用環境への認可されていないアクセス等を防止する観点から、運用環境は開発環境や試験環境等と分離する。

●マルウェアからの保護

標的型攻撃メールや USB メモリ等から情報システムに感染するマルウェアが重要インフラサービス障害を引き起こす可能性が考えられるため、マルウェアを検出及び予防する仕組みをあらかじめ整備しておくとともに、万が一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。なお、重要インフラ事業者等が直接管理することが困難である、委託先等が持ち込む PC やデバイスがマルウェア感染している可能性も考慮する。

また、優先度の高い重要システムにおいては、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ホワイトリスト型のマルウェア無効化機能の活用も検討することが期待される。

●バックアップ

重要インフラサービスの提供に係る情報システムの異常状態や重要なデータの誤った消去等（ランサムウェア等による不正なデータ暗号化も含む）の可能性を想定し、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あらかじめ整備する。なお、可用性確保の観点から、バックアップは十分な量を取得することが期待される。

また、取得したバックアップは必要な場面で問題なく利用できることが求められるため、定期的なバックアップリカバリー検査を実施する。

●ログ取得

重要インフラサービスの提供に係る情報システムに対する不正なアクセスや操作等を監視する観点から、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する。なお、ログの記憶装置の容量を検討する際は、ログの可用性についても考慮す

ることが期待される。

また、ログは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とともに、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。

●運用ソフトウェアの管理

重要インフラサービスの提供に係る情報システムで利用するソフトウェアは、脆弱な設定状態を悪用した攻撃の可能性が想定されるため、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。

また、重要インフラサービス障害が発生した際やサイバー攻撃等の予兆を認識した際に、ソフトウェアベンダ等のサポートを速やかに受けることを可能にするため、サポート対象バージョンへの更新を計画的に実施する。なお、サポート対象バージョンへの更新が困難である場合においては、重要インフラサービス障害やサイバー攻撃を防止するための補完的な措置を講じる。

●技術的脆弱性管理

情報セキュリティ関係機関等が提供している情報システムの技術的脆弱性に関する情報を日頃から収集するとともに、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の実施も期待される。

技術的脆弱性への対応については、既存の情報システムへのパッチ適用の影響確認が必要となることを踏まえ、その作業方針や作業内容をあらかじめ確立する。例えば、緊急的なパッチ適用が要求される状況においても、最低限実施すべき確認テストの項目を整理し、それらを実施する。なお、緊急時であってもパッチ適用が困難な場合においては、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。

（キ）通信のセキュリティ

●ネットワークセキュリティ管理

重要インフラサービスの提供に係る情報システム等が取り扱う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、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。

●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（ＥＤＩ）、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との合意を図る。

（ク）システムの取得、開発及び保守

●情報セキュリティ要件を踏まえた情報システムの取得

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[12]」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順守状況を委託先に対して定期的に確認する。

（ケ）供給者関係

●供給者関係における情報セキュリティ

重要インフラサービスの提供に係る情報システム等の設備及びその運用を、外部の供給者（例：ＩＴサービスやＩＴ基盤の構成要素等の供給者）が提供するサービスによって代替する場合、供給者やその再委託先等が重要インフラ事業者等の資産にアクセスするリスクを低減するための情報セキュリティ要求事項を整理し、あらかじめ供給者と合意する。

また、供給者が階層的に存在する場合、ある供給者は、その一階層下の供給者に対して同様の要求事項を求めることを通じて、サプライチェーンの情報セキュリティ向上を図る。

●供給者のサービス提供の管理

合意した情報セキュリティの条件の順守を確実にするため、供給者のサービス提供を定常的に監視するとともに、供給者が作成した報告書のレビューや監査等を実施する。また、リスク再評価の必要性等から、供給者が提供するサービスの変更に対する管理を行う。

（コ）情報セキュリティインシデント管理

●情報セキュリティインシデントの管理及びその改善

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及ぼす情報セキュリティインシデントへの迅速かつ効果的な対応のため、インシデントの管理責任者を定める

[12] 情報セキュリティを企画・設計段階から確保するための方策を指す。

とともに、組織内外への報告や証拠収集等の手順を整備する。

また、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。

（３）セキュリティ管理策に係る個別方針の策定

情報セキュリティリスク対応の中で決定した個々のセキュリティ管理策において順守すべき行為や判断等の基準を個別方針（例：アクセス制御方針、情報分類方針等）としてまとめ、組織内へ伝達する。また、必要に応じて委託先に対しても伝達する。

情報セキュリティ方針と同様に、個別方針の内容の妥当性や有効性等について、定期的な間隔で確認するとともに、大きな環境変化があった場合にも確認する。

（４）情報セキュリティリスク対応計画の策定

情報セキュリティ方針の内容を踏まえた目標及びその達成度の判定基準に加えて、決定したセキュリティ管理策の導入にむけた実施事項、スケジュール等について定めた「情報セキュリティリスク対応計画」を策定する。

4.1.4. 「支援」の観点

（１）資源確保

情報セキュリティ対策のＰＤＣＡサイクル推進、すなわち、ＰＤＣＡサイクルの確立、実施、維持及び継続的改善に取り組むに当たって、必要となる資源（人材や予算等）を明確化し、経営層の指揮の下、組織内へ適切に配分する。

また、環境変化による情報セキュリティ対策の水準低下へ対処する等の観点から、経営層は必要な資源の継続的な確保に努める。

（２）人材育成及び意識啓発

情報セキュリティ対策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及び賃金政策をあらかじめ検討しておくことが重要となる。

また、重要インフラ事業者等の従業員が情報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、情報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おいても実施）。特に、情報セキュリティ対策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（※4.2.1.（３）参照）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。

さらに、情報セキュリティ方針に対する理解を促進するとともに、従業員自らが情報セキュリティ対策の取組に関与することの重要性や必要性を認識させるため、取組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図る。

（３）コミュニケーション

情報セキュリティリスクへの対応に責任を持つ経営層と、経営層による管理（指示、モニタ、評価等）の下で情報セキュリティ対策を推進する実務者層との間で、定期的な対話の機会等を設け、コミュニケーションを活性化することが重要である。その際、実務者層においては、経営層が情報セキュリティリスクへの対応状況を正確に把握し、状況に応じた的確な判断や調整等を行うことを可能とするため、対話の機会を通じて、経営層に対して正確な情報提供や進言を行うことが重要となる。

また、自組織が所属する重要インフラ分野全体で重要インフラサービスの安全かつ持続的な提供を実現するという観点から、他の重要インフラ事業者や所管省庁等の関係主体と各々の役割や責任分担、情報共有や報告の体制等について意見交換を行うことも有効である。

4.2. 「Do（実行）」の観点

4.2.1. 「運用」の観点

（１）情報セキュリティ対策の導入、運用

（ア）セキュリティ管理策の導入、運用プロセスの確立・実行

「情報セキュリティリスク対応計画」に基づき、情報セキュリティ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。

（イ）重要インフラサービス障害に繋がる事象の検知、速やかな対処判断

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のベースラインを把握し、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繋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。

また、前述の監視・検知の仕組みによって、特定のサイバー攻撃の予兆を認識した際等において、導入済みのセキュリティ管理策による当該サイバー攻撃への対処可否を速やかに判断する（「モニター機能の配備」）とともに、判断結果に応じて、導入済みのセキュリティ管理策の見直し（各種装置のチューニング作業を含む）や新たなセキュリティ管理策を導入する等、動的な対応を実施することも重要となる。

（ウ）脅威情報及び分析・対策情報の確認

日頃から情報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。緊急度が高いと判断される脅威情報等があった場合には、情報セキュリティリスクアセスメントを緊急で実施し、追加のリスク対応の要否を判断する。

（エ）分野専門性の高い情報共有活動への参加

サイバー攻撃の手口は絶えず考え出され、特定の重要インフラ分野を標的とした高度なサイバー攻撃の可能性も想定されることから、その対策のひとつとして、ＩＳＡＣ[13]等の分野専門性の高い情報共有活動へ参加し、その中で収集した情報を日々のリスク対応で活用する。

（２）重要インフラサービス障害への対応

（ア）サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画の策定

重要インフラサービス障害が発生した場合、安全を確保するとともに、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が要求されるため、重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となる。

そこで、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[14]」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[15]」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。

特に、重要インフラサービス障害を引き起こす事象のひとつである「サイバー攻撃」への備えを目的として、コンティンジェンシープラン及び事業継続計画を策定・改定する場合には、「【別紙３】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」を参照することが期待される。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）も別途策定することが期待される。

（イ）ＣＳＩＲＴ等の整備、関連部門との役割分担等の合意

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ひとつとして、ＣＳＩＲＴ[16]（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。

---

[13] Information Sharing and Analysis Center の略。国内の ISAC には、ICT-ISAC、金融 ISAC、電力 ISAC 等がある。

[14] 第４次行動計画では、重要インフラ事業者等が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後に経営層や従業員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたものを指す。

[15] 第４次行動計画では、機能保証の考え方を踏まえ、重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラ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して、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたものを指す。

[16] 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かか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。

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障害発生時の対応に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。

また、サイバー攻撃に迅速に対処する観点から、情報セキュリティの専門知識を持つ組織を含めた対処態勢を平時から整備しておく必要性を検討することが期待される。例えば、サイバー空間関連事業者及び情報セキュリティ関係機関との提携が有効である。

（ウ）対応計画に基づく被害拡大防止・サービス復旧

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スを含む)、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。

（３）演習・訓練の実施

重要インフラサービス障害の対応計画（コンティンジェンシープラン、事業継続計画等）の実行性確保、対応要員のスキルアップ等を図るため、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向上の観点からは、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情報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。

4.3. 「Check（評価)」の観点

4.3.1. 「評価」の観点

（１）モニタリング及び監査

情報セキュリティ方針に基づき設定した目標の達成状況、情報セキュリティリスク対応計画の進捗状況、情報セキュリティ意識向上のための教育・トレーニングの進捗状況等をモニタリングし、各種取組が計画どおりに進んでいるかを確認する。

また、リスクオーナーは、セキュリティ管理策の導入・運用に伴うリスクの状況変化（事象の発生頻度の変化や、事象の結果の影響度の変化等）を定期的にモニタリングする。個々のリスクの状況変化は、可視化されるとともに、組織全体のリスクの状況変化が把握できることが期待される。

さらに、定期的に内部監査（難しい場合は最低でもリスクオーナーによる自己点検）を実施し、情報セキュリティ対策のＰＤＣＡサイクルが情報セキュリティ方針に基づき適切に構築され、有効な状態で維持されていることを確認する。なお、この取り組みに必要な内部監査人の育成に努めるとともに、必要に応じて、外部の高度な専門知識を有する者[17]の支援を受けて状況確認を実施することが期待される。

（２）経営層によるレビュー

重要インフラ事業者等の経営層は、システム監査その他のリソースを活用し、定期的に自組織の情報セキュリティ対策の取組状況を確認し、改善や見直しが必要な箇所を認識する。その際、モニタリング及び監査の実施結果に加えて、前回までのレビュー結果を踏まえて行われた処置の状況、外部環境及び内部環境の変化、関係主体等からのフィードバック等も確認する。

レビュー結果は文書化するとともに、改善や見直しに必要な資源（人材や予算等）の現状を確認の上、改善や見直しの指示を行う。

4.4. 「Act（改善）」の観点

4.4.1. 「改善」の観点

（１）是正処置及び継続的改善

モニタリング及び監査の実施結果から、目標未達や進捗遅延、セキュリティ管理策の要改善点等が確認された場合や、経営層からの改善指示があった場合には、必要な対処を速やかに実施するとともに今後に向けた再発防止策を立案する。これらを繰り返し実施して、情報セキュリティ対策の取組の効果を高める。

また、定期的に情報セキュリティ対策のＰＤＣＡサイクルの取組状況を「情報セキュリティ報告書」としてまとめるとともに、当該報告書を活用した、重要インフラ事業者等の経営層と関係主体等との対話の機会を通じて、関係主体等の要求事項を認識し、ＰＤＣＡサイクルの改善に活用する。

[17] 経済産業省の「情報セキュリティ監査制度」では、「情報セキュリティ監査」を行う主体（監査法人、情報セキュリティベンダー、システムベンダー、情報セキュリティ専門企業、システム監査企業等）を登録する「情報セキュリティ監査企業台帳」を整備・公開している。

【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

重要インフラ分野	対象となる重要インフラ事業者等(注1)	対象となる重要システム例
情報通信	・主要な電気通信事業者 ・主要な地上基幹放送事業者 ・主要なケーブルテレビ事業者	・ネットワークシステム ・オペレーションサポートシステム ・編成・運行システム
金融　銀行等 生命保険 損害保険 証券	・銀行、信用金庫、信用組合、労働金庫、農業協同組合等 ・資金清算機関 ・電子債権記録機関 ・生命保険 ・損害保険 ・証券会社 ・金融商品取引所 ・振替機関 ・金融商品取引清算機関　　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・金融機関相互ネットワークシステム ・電子債権記録機関システム ・保険業務システム ・証券取引システム ・取引所システム ・振替システム ・清算システム　　等
航空	・主たる定期航空運送事業者	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム
空港	・主要な空港・空港ビル事業者	・警戒警備・監視システム ・フライトインフォメーションシステム ・バゲージハンドリングシステム
鉄道	・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力	・一般送配電事業者、主要な発電事業者　　等	・電力制御システム ・スマートメーターシステム
ガス	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・各府省庁 ・地方公共団体	・各府省庁及び地方公共団体の情報システム （電子政府・電子自治体への対応）
医療	・医療機関 （ただし、小規模なものを除く。）	・診療録等の管理システム等（電子カルテシステム、遠隔画像診断システム等、医用電気機器等）
水道	・水道事業者及び水道用水供給事業者 （ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流	・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム
化学	・主要な石油化学事業者	・プラント制御システム
クレジット	・主要なクレジットカード会社　　等	・クレジットカード決済システム
石油	・主要な石油精製・元売事業者	・受発注システム ・生産管理システム

		・生産出荷システム　　等

注１　ここに掲げている者は、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びＩＴへの依存度の進展等を踏まえ、対象とする者の見直しを行う。

【別紙２】重要インフラサービスの説明と重要インフラサービス障害の例

（平成 31~~0~~年~~3~~ 4 月時点）（注４）

重要インフラ分野	重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
情報通信	・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること（電気通信事業法第２条）	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障	・電気通信事業法（業務停止等の報告）第28条 ・電気通信事業法施行規則（報告を要する重大な事故）第58条 【サービス維持レベル】 ・電気通信設備の故障により、役務提供の停止・品質の低下が、３万以上の利用者に対し２時間以上継続する事故が生じないこと
	・放送	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第113条、第122条 ・放送法施行規則（報告を要する重大な事故）第125条 【サービス維持レベル】 ・基幹放送設備の故障により、放送の停止が15分以上継続する事故が生じないこと ・特定地上基幹放送局等設備及び基幹放送局設備の故障により、放送の停止が15分以上（中継局の無線設備にあっては、２時間以上）継続する事故が生じないこと
	・ケーブルテレビ	・公衆によって直接受信されることを目的とする電気通信の送信（放送法第２条）	・放送サービスの停止	・放送法（重大事故の報告）第137条 ・放送法施行規則（報告を要する重大な事故）第157条 【サービス維持レベル】 ・有線一般放送の業務に用いられる電気通信設備の故障により、放送の停止を受けた利用者の数が３万以上、かつ、停止時間が２時間以上の事故が生じないこと

重要インフラ分野		重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
		呼称	サービス（手続を含む）の説明（関連する法令）		
金融	銀行等	・預金 ・貸付 ・為替	・預金又は定期積金等の受入れ（銀行法第10条第１項第１号） ・資金の貸付け又は手形の割引（銀行法第10条第１項第２号） ・為替取引（銀行法第10条第１項第３号）	・預金の払戻しの遅延・停止 ・融資業務の遅延・停止 ・振込等資金移動の遅延・停止	・主要行等向けの総合的な監督指針 ・中小・地域金融機関向けの総合的な監督指針 ・系統金融機関向けの総合的な監督指針
		・資金清算	・資金清算（資金決済に関する法律第２条第~~5~~10項）	・資金清算の遅延・停止	・清算・振替機関等向けの総合的な監督指針
		・電子記録等	・電子記録（電子記録債権法第56条） ・資金決済に関する情報提供（電子記録債権法第62条及び第63条）	・電子記録、資金決済に関する情報提供の遅延・停止	・事務ガイドライン第三分冊：金融会社関係（12 電子債権記録機関関係）
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付 ・保険金等の支払審査 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針
	損害保険	・保険金等の支払い	・事故受付 ・損害調査等 ・保険金等の支払い	・保険金等の支払いの遅延・停止	・保険会社向けの総合的な監督指針
	証券	・有価証券の売買等 ・有価証券の売買等の取引の媒介、取次ぎ又は代理 ・有価証券等清算取次ぎ	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引（金融商品取引法第２条第８項第１号） ・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引の媒介、取次ぎ又は代理（金融商品取引法第２条第８項第２号） ・有価証券等清算取次ぎ（金融商品取引法第２条第８項第５号）	・有価証券売買の遅延・停止	・金融商品取引業者等向けの総合的な監督指針
		・金融商品市場の開設	・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務（金融商品取引法第２条第14項及び第16項、第80条並びに第84条）	・有価証券の売買、市場デリバティブ取引等の遅延・停止	・金融商品取引所等に関する内閣府令第112条

重要インフラ分野		重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
		呼称	サービス（手続を含む）の説明（関連する法令）		
		・振替業	・社債等の振替に関する業務（社債、株式等の振替に関する法律第８条）	・社債・株式等の振替等の遅延・停止	・社債、株式等の振替に関する法律（事故の報告）第19条 ・一般振替機関の監督に関する命令（事故）第17条 ・清算・振替機関等向けの総合的な監督指針
		・金融商品債務引受業	・有価証券の売買等対象取引に基づく債務の引受、更改等により負担する業務（金融商品取引法第２条第28項）	・金融商品取引の清算等の遅延・停止	・金融商品取引法（金融商品取引業者の業務等に関する書類の作成、保存及び報告の義務）第188条 ・金融商品取引清算機関等に関する内閣府令（金融商品取引清算機関の業務に関する提出書類）第48条 ・清算・振替機関等向けの総合的な監督指針
航空		・旅客、貨物の航空輸送サービス ・予約、発券、搭乗・搭載手続 ・運航整備 ・飛行計画作成	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業（航空法第２条） ・航空旅客の予約、航空貨物の予約 ・航空券の発券、料金徴収 ・航空旅客のチェックイン・搭乗、航空貨物の搭載 ・航空機の点検・整備 ・飛行計画の作成、航空局への提出	・航空機の安全運航に対する支障 ・運航の遅延・欠航	・航空分野~~運送事業者~~における情報セキュリティ確保に係る安全ガイドライン
空港		・空港におけるセキュリティの確保 ・空港における利便性の向上	・警戒警備等による空港のセキュリティ確保 ・空港利用者等への正確・迅速な情報提供 ・航空機への受託手荷物の検査及び搬送	・警戒警備等に支障が発生することによる空港のセキュリティの低下 ・情報提供等に支障が発生することによる利便性の低下 ・航空機への受託手荷物の検査及び搬送の遅延・停止	・空港分野における情報セキュリティ確保に係る安全ガイドライン
鉄道		・旅客輸送サービス ・発券、入出場手続	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業（鉄道事業法第２条） ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認	・列車運行の遅延・運休 ・列車の安全安定輸送に対する支障	・鉄道事業法（事故等の報告） 第19条、第19条の２ ・鉄道事故等報告規則（鉄道運転事故等の報告）第５条 ・鉄道分野における情報セキュリティ確保に係る安全ガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）（注1）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注2））
	呼称	サービス（手続を含む）の説明（関連する法令）		
電力	・一般送配電事業 ・発電事業（一定規模を超える発電事業）	・供給区域において託送供給及び発電量調整供給を行う事業（電気事業法第２条８項） ・小売電気事業、一般送配電事業又は特定送配電事業の用に供するための電気を発電する事業（電気事業法第２条14項）	・電力供給の停止 ・電力プラントの安全運用に対する支障	・電気関係報告規則（事故報告）第３条 【サービス維持レベル】 ・システムの不具合により、供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス	・一般ガス導管事業 ・ガス製造事業	・自らが維持し、及び運用する導管によりその供給区域において託送供給を行う事業（ガス事業法第２条） ・自らが維持し、及び運用する液化ガス貯蔵設備等を用いてガスを製造する事業であつて、その事業の用に供する液化ガス貯蔵設備が経済産業令で定める要件に該当するもの（ガス事業法第２条）	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障	・ガス関係報告規則第４条 【サービス維持レベル】 ・システムの不具合により、供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス	・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの（地方自治法第２条第２項）	・政府・行政サービスに対する支障 ・住民等の権利利益保護に対する支障	・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療	・診療	・診察や治療等の行為	・診療支援部門における業務への支障 ・生命に危機を及ぼす医療機器の誤作動	・医療情報システムの安全管理に関するガイドライン
水道	・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業（水道法第３条及び第15条）	・水道による水の供給の停止 ・不適当な水質の水の供給	・健康危機管理の適正な実施並びに水道施設への被害情報及び水質事故等に関する情報の提供について」（平成25年10月25日付け厚生労働省健康局水道課長通知） ・水道分野における情報セキュリティガイドライン

重要インフラ分野	重要インフラサービス（手続を含む）（注１）		システムの不具合が引き起こす重要インフラサービス障害の例	左記障害の報告に係る法令、ガイドライン等（サービス維持レベル（注２））
	呼称	サービス（手続を含む）の説明（関連する法令）		
物流	・貨物自動車運送事業 ・船舶運航事業 ・港湾運送事業 ・倉庫業	・他人の需要に応じ、有償で、自動車を使用して貨物を運送する事業（貨物自動車運送事業法第２条） ・船舶により物の運送をする事業（海上運送法第２条） ・他人の需要に応じ、港湾においてする船舶への貨物の積込又は船舶からの貨物の取卸の行為等を行う事業（港湾運送事業法第２条） ・寄託を受けた物品の倉庫における保管を行う事業（倉庫業法第２条）	・輸送の遅延・停止 ・貨物の所在追跡困難	・物流分野における情報セキュリティ確保に係る安全ガイドライン
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・プラントの停止 ・長期に渡る製品供給の停止	・石油化学分野における情報セキュリティ確保に係る安全基準
クレジット	・クレジットカード決済	・クレジットカード決済サービス（割賦販売法第２条第３項第１号及び第２号並びに第35条の16第２項）（注３）	・クレジットカード決済サービスの遅延・停止、カード情報の大規模漏えい	・クレジットCEPTOARにおける情報セキュリティガイドライン （※）今後、割賦販売法（後払分野）に基づく監督の基本方針において規定する予定
石油	・石油の供給	・石油の輸入、精製、物流、販売	・石油の供給の停止 ・製油所の安全運転に対する支障	・石油分野における情報セキュリティ確保に係る安全ガイドライン

注１　ＩＴを全く利用していないサービスについては対象外。
注２　重要インフラサービス障害に係る基準がない分野については、システムの不具合が引き起こす重要インフラサービス障害が生じないことをサービス維持レベルとみなしている。
注３　改正割賦販売法（施行は、公布（2016年12月９日）から１年６か月以内の政令で定める日）においては、法第２条第３項第１号及び第２号、第35条の16第１項第２号及び第２項。
注４　別紙２に記載された内容は平成31年4月現在のものである。法令等の最新の状況については、必要に応じて、所管省庁等へ確認すること。

【別紙３】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）及び事業継続計画（以下、ＢＣＰ）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。

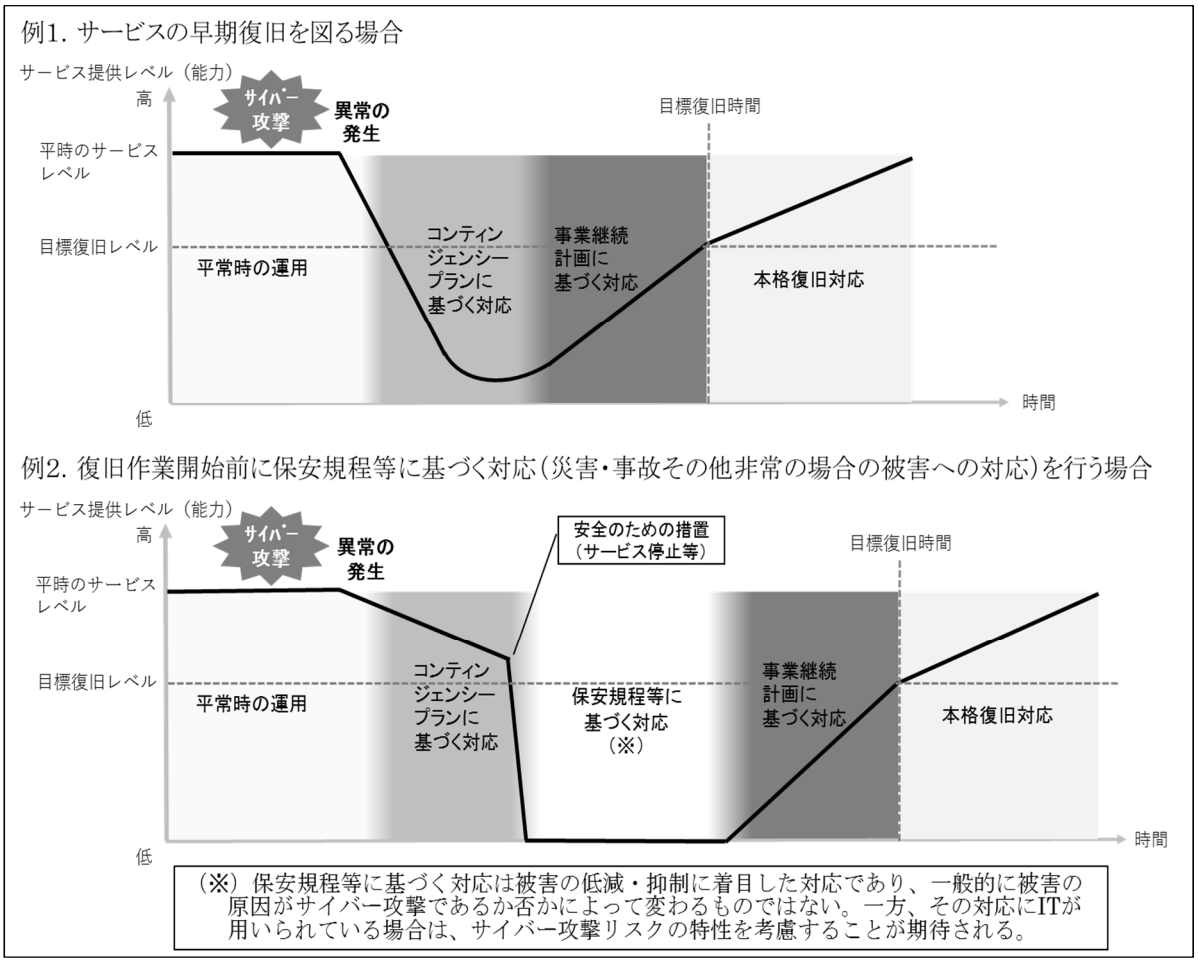
ＣＰ及びＢＣＰの定義は本紙４.２.１.（２）（ア）に記載のとおりであるが、これらの名称や記載の範囲、発動のタイミング等は分野や事業者等によって異なる場合があるため、次頁以降の特性等を考慮して策定・改定すべき対象ドキュメント（以下、適用対象）は各事業者等の状況に応じて検討される必要がある。

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サプライヤー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サプライヤーや外部委託先がサイバー攻撃を受けた場合に備え、サプライヤーや外部委託先の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、情報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予め用意する。

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。保存期間は情報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、情報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。

【別紙４】対策項目の具体例等の参照先

対策項目	具体例等の参照先
4.1.「Plan（計画）」の観点	―
4.1.1.「組織の状況」の観点	―
（１）外部環境及び内部環境の理解	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.4.2.1
（２）関係主体等の要求事項の理解	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.4.3.1 • 「JIS Q 27002:2014」 18.1.1
4.1.2.「リーダーシップ」の観点	―
（１）経営層のコミットメント	• 「企業経営のためのサイバーセキュリティの考え方」 • 「サイバーセキュリティ経営ガイドライン Ver.2.0」 • 「IoT セキュリティガイドライン ver.1.0」 要点 1
（２）情報セキュリティ方針の策定	• 「JIS Q 27002:2014」 5.1.1, 5.1.2
（３）組織の役割に対する責任及び権限の割当	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.4.1.2
4.1.3.「計画」の観点	―
（１）情報セキュリティリスクアセスメント	• 「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」 • 「制御システムのセキュリティリスク分析ガイド」 • 「CSMS 認証基準 Ver.2.0」 4.2, 4.3 • 「CSMS ユーザーズガイド Ver.1.2」3.1, 4.1 ～ 4.4, 6.1 • 「IoT セキュリティガイドライン ver.1.0」 要点 3 ～ 7
（２）情報セキュリティリスク対応の決定	―
（ア）人的資源のセキュリティ（外部委託）	―
●委託前の対応事項（選定・契約条件）	• 「JIS Q 27002:2014」 7.1.1, 7.1.2, 7.2.1, 7.2.2, 7.3.1
●委託期間中の対応事項	• ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 4.1.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 4.1.1 • 「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」 3.1, 3.2
（イ）資産の管理	―
●資産に対する責任	• 「JIS Q 27002:2014」 8.1.1 ～ 8.1.4
●情報分類と取扱い	• 「JIS Q 27002:2014」 8.2.1 ～ 8.2.3 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 3.1.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 3.1.1
●データ管理	• 「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 4.1.4, 7.2.4 • 「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 4.1.4、7.2.4
（ウ）アクセス制御	―
●利用者アクセスの管理	• 「JIS Q 27002:2014」 9.2.1 ～ 9.2.6 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 6.1.3 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 6.1.3
●情報システム等のアクセス制御	• 「JIS Q 27002:2014」 9.4.1 ～ 9.4.3 • ~~「政府機関の情報セキュリティ対策のための統一基準~~

	~~（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 6.1.1, 6.1.2 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 6.1.1, 6.1.2
（エ）暗号	―
●暗号を活用した情報管理	• 「JIS Q 27002:2014」 10.1.1, 10.1.2, 18.1.5 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 6.1.5 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 6.1.5 • 「輸出貿易管理令別表第 1 第 9 項(7) 暗号装置又はその部分品」
（オ）物理的及び環境的セキュリティ	―
●セキュリティ確保が求められる領域	• 「JIS Q 27002:2014」 11.1.1 ～ 11.1.6 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 3.2.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 3.2.1 — 「IoT セキュリティガイドライン ver.1.0」 要点 2 •
●災害による障害の発生しにくい設備の設置及び管理	• 「JIS Q 27002:2014」 11.1.4 • 「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 3.2.1 • 「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 3.2.1
●装置の管理	• 「JIS Q 27002:2014」 11.2.1, 11.2.3, 11.2.5 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 7.1.1, 7.1.2 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 7.1.1, 7.1.2 • 「IoT セキュリティガイドライン ver.1.0」 要点 2
（カ）運用時のセキュリティ管理	―
●運用の手順及び責任	• 「JIS Q 27002:2014」 12.1.1, 12.1.2, 12.1.4
●マルウェアからの保護	• 「JIS Q 27002:2014」 12.2.1
●バックアップ	• 「JIS Q 27002:2014」 12.3.1
●ログ取得	• 「JIS Q 27002:2014」 12.4.1 ～ 12.4.4 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 6.1.4 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 6.1.4 • 「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」 • 「IoT セキュリティガイドライン ver.1.0」 要点 2
●運用ソフトウェアの管理	• 「JIS Q 27002:2014」 12.5.1 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 5.2.3, 6.2.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 5.2.3, 6.2.1

●技術的脆弱性管理	• 「JIS Q 27002:2014」 12.6.1 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 6.2.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 6.2.1 • 「IoT セキュリティガイドライン ver.1.0」 要点 17, 18, 21
（キ）通信のセキュリティ	－
●ネットワークセキュリティ管理	• 「JIS Q 27002:2014」 13.1.1 ～ 13.1.3 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 7.3.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 7.3.1
●情報の転送	• 「JIS Q 27002:2014」 13.2.1 ～ 13.2.3 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 7.1.3, 7.2.1 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 7.1.3, 7.2.1
（ク）システムの取得、開発及び保守	－
●情報セキュリティ要件を踏まえた情報システムの取得	• 「JIS Q 27002:2014」 14.1.1 ～ 14.1.3, 14.2.1 ～ 14.2.9, 14.3.1 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 5.2.1, 5.2.2 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 5.2.1, 5.2.2 • 「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」 4.1, 4.2 • 「IT 製品の調達におけるセキュリティ要件リスト」 • 「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」 • 「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」 • 「IoT セキュリティガイドライン ver.1.0」要点 8 ～ 16
（ケ）供給者関係	－
●供給者関係における情報セキュリティ	• 「JIS Q 27002:2014」 15.1.1 ～ 15.1.3 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 4.1.1, 4.1.4 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 4.1.1, 4.1.4
●供給者のサービス提供の管理	• 「JIS Q 27002:2014」 15.2.1, 15.2.2 • ~~「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」~~「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 4.1.1, 4.1.4 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」~~「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 4.1.1, 4.1.4
（コ）情報セキュリティインシデント管理	－
●情報セキュリティインシデントの管理及びその改善	• 「JIS Q 27002:2014」 16.1.1, 16.1.2, 16.1.6, 16.1.7 • ~~「政府機関の情報セキュリティ対策のための統一基準~~

	~~（平成 28 年度版）~~」「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」 2.2.4 • ~~「府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~」「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」 2.2.4
（３）~~リスク~~セキュリティ管理策に係る個別方針の策定	• 「JIS Q 27002:2014」 5.1.1, 5.1.2
（４）情報セキュリティリスク対応計画の策定	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.4.8.4, 4.4.8.5
4.1.4.「支援」の観点	―
（１）資源確保	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.5.1.1, 4.5.1.2
（２）人材育成及び意識啓発	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.5.2.3, 4.5.2.4, 4.5.2.6 ～ 4.5.2.8
（３）コミュニケーション	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.5.3.1 • 「JIS Q 27014:2015」 5.3.2 ～ 5.3.4
4.2.「Do（実行）」の観点	―
4.2.1.「運用」の観点	―
（１）情報セキュリティ対策の導入、運用	• 「JIS Q 27002:2014」 16.1.1, 16.1.2, 16.1.4, 16.1.5 • 「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」 • 「インシデントハンドリングマニュアル」
（２）重要インフラサービス障害への対応	• 「JIS Q 22301:2013」 • 「JIS Q 27002:2014」 17.1.1 ～ 17.1.3, 17.2.1 • 「中央省庁における情報システム運用継続計画ガイドライン～策定手引書（第２版）～」 • 「IT-BCP 策定モデル」 • 「CSIRT マテリアル」
（３）演習・訓練の実施	• 「JIS Q 22301:2013」 8.5 • 「JIS Q 27002:2014」 17.1.3
4.3.「Check（評価）」の観点	―
4.3.1.「評価」の観点	―
（１）モニタリング及び監査	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.6.2.2, 4.6.2.3 • 「JIS Q 19011:2012」
（２）経営層によるレビュー	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.6.3.1 ～ 4.6.3.3 • 「JIS Q 27014:2015」 5.3.2 ～ 5.3.6
4.4.「Act（改善）」の観点	―
4.4.1.「改善」の観点	―
（１）是正処置及び継続的改善	• 「情報セキュリティ管理基準（平成２８年改正版）」 4.7.1.1 ～ 4.7.1.7 • 「JIS Q 27014:2015」 5.3.5

定義・用語集

関係主体	内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター、セプターカウンシル、情報セキュリティ関係機関及びサイバー空間関連事業者。
サービス維持レベル	機能保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。
サイバー空間関連事業者	重要インフラサービスを提供するために必要な情報システムに関係する、設計・構築・運用・保守等を行うシステムベンダー、ウィルス対策ソフトウェア等の情報セキュリティ対策を提供するセキュリティベンダー及びハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー。
サイバー攻撃リスク	サイバー攻撃に起因して事業に生じ得るリスク。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
事象	ある一連の周辺状況の出現又は変化。
事象の結果	目的に影響を与える事象の結末。
システムの不具合	重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。
重要インフラ	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、我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、重要インフラ分野として指定する分野。
重要インフラサービス	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定めるもの。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。 ※重要インフラサービス障害を引き起こす原因、すなわち、「安全基準等」の対象とすべき脅威については、内閣サイバーセキュリティセンター「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の「別紙２　結果を生じる事象（脅威）の例」に具体例が記載されている。
重要インフラ事業者等	重要インフラ分野に属する事業を営む者等のうち「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及び当該事業者等から構成される団体。
重要インフラ所管省庁	金融庁、総務省、厚生労働省、経済産業省、国土交通省。
重要インフラ分野	重要インフラについて業種ごとに分野と指定しているものであり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者等ごとに定めるもの。

情報共有	システムの不具合等に関する情報（重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報）や情報セキュリティの確保に資する情報について、関係主体間で相互に提供し、共有すること。情報連絡及び情報提供の双方を含む。
情報システム	事務処理等を行うシステム、フィールド機器や監視・制御システム等の制御系のシステム等のＩＴを用いたシステム全般。
情報セキュリティ関係機関	警察庁サイバーフォースセンター、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人 ICT-ISAC、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
情報セキュリティ関係省庁	警察庁、総務省、外務省、経済産業省、原子力規制庁（※）及び防衛省。 ※原子力発電所の安全の観点からサイバーセキュリティに取り組む省庁
情報提供	情報セキュリティ対策に資するための情報を、内閣官房から重要インフラ事業者等へ提供すること等。
情報連絡	重要インフラ事業者等におけるシステムの不具合等に関する情報（重要インフラサービス障害を含むシステムの不具合や予兆・ヒヤリハットに関する情報）を、重要インフラ事業者等から内閣官房に連絡すること等。
セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。 Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称（CEPTOAR）。
セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
防災関係府省庁	災害対策基本法（昭和 36 年法律第 223 号）第２条第３号に基づく指定行政機関等の、災害時の情報収集に関係する府省庁。

参考文献

- 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 27002:2014, 情報技術 – セキュリティ技術 – 情報セキュリティ管理策の実践のための規範.
  【対応国際規格】
  ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.
- 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 31000:2010, リスクマネジメント – 原則及び指針.
  【対応国際規格】
  ISO 31000:2009, Risk management – Principles and guidelines.
- 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.
- 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/conference/cs/jinzai/dai03/pdf/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 Ver2.0. 経済産業省. 2017-11-16.
  http://www.meti.go.jp/policy/netsecurity/mng_guide.html
- 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 31000:2009 リスクマネジメント 解説と適用ガイド. 日本規格協会. 2010-02-25.
- 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. 2017-10-02.
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

- 米国国立標準技術研究所(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 1.0 版. 独立行政法人 情報処理推進機構. 2014-05.
  https://www.ipa.go.jp/security/publications/nist/
- 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
- サイバーセキュリティ戦略本部. ~~政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）~~政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）. 201~~6~~-0~~7~~8-25~~31~~.
  https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
- 内閣官房 内閣サイバーセキュリティセンター. ~~府省庁対策基準策定のためのガイドライン（平成 28 年度版）~~政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）. 201~~6~~-0~~7~~8-25~~31~~.
  https://www.nisc.go.jp/active/general/pdf/guide28.pdf
- 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/active/general/pdf/risktaiou28.pdf
- 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. 2015-11-17.
  https://www.jpcert.or.jp/research/apt-loganalysis.html
- 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. 2015-05-21.
  https://www.nisc.go.jp/active/general/sbd_sakutei.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. 2016-03-31.
  https://www.jpcert.or.jp/research/apt-guide.html
- 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. 2015-11-26.
  https://www.jpcert.or.jp/csirt_material/operation_phase.html
- 内閣官房 内閣サイバーセキュリティセンター. 中央省庁における情報システム運用継続計画ガイドライン～策定手引書～. 2012-05.
  https://www.nisc.go.jp/active/general/itbcp-guideline.html
- 内閣官房 内閣サイバーセキュリティセンター. IT-BCP 策定モデル. 2013-06.
  https://www.nisc.go.jp/active/general/itbcp-guideline.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_material/

資料２－３

重要インフラにおける機能保証の考え方に基づく
リスクアセスメント手引書
（第１版）

平 成 ３ ０ 年 ４ 月 ４ 日

令 和 元 年 　 月 　 日 改 定

サイバーセキュリティ戦略本部

重要インフラ専門調査会

（空白ページ）

目次

１．はじめに

＜１＞手引書策定の目的

情報通信技術は、国民生活に広く普及し、事業活動においても各種サービスの提供に欠かせないものとなってきています。情報通信技術の進展に伴い、各種サービスの品質や生産性が向上し、新しいサービスの創出機会など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、情報セキュリティリスクも拡大しています。このような環境の中、国民生活や社会経済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、情報セキュリティリスクを事業等のリスクの一つとして認識し、経営層の積極的な関与のもと、適切な情報セキュリティ対策を講じることが求められます。

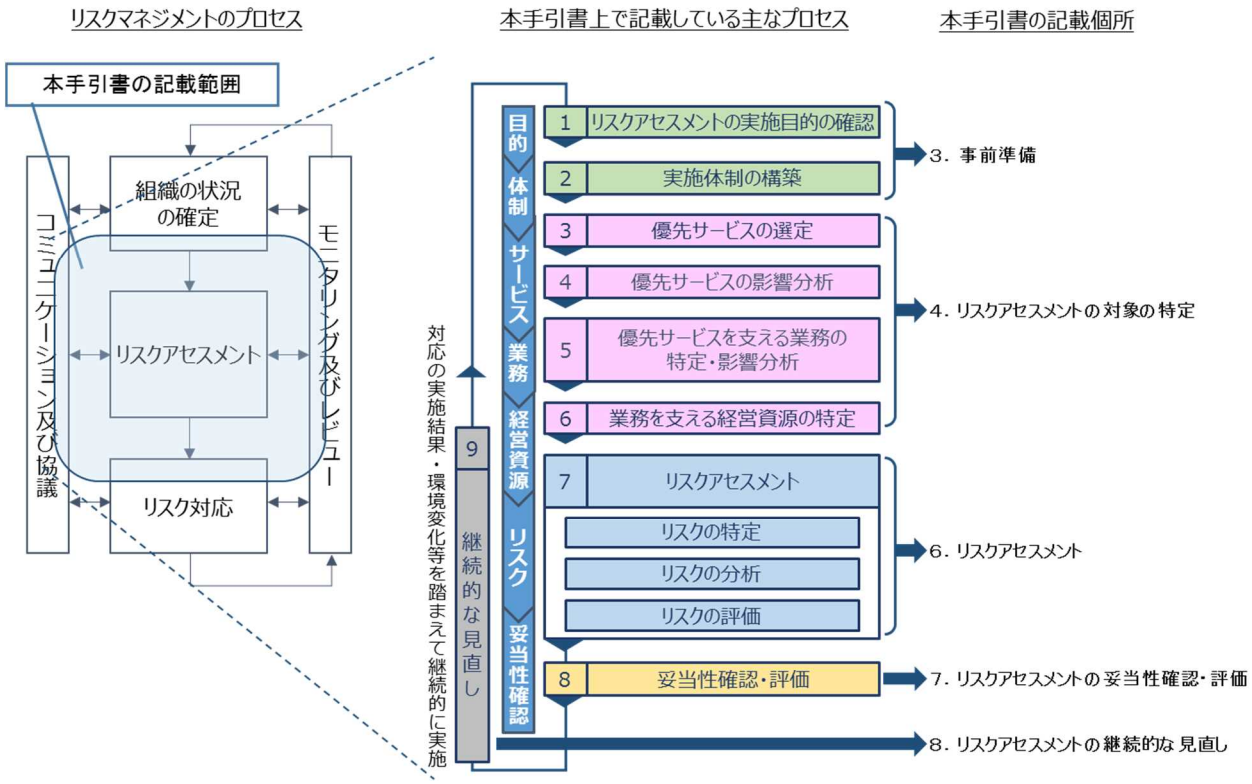
情報セキュリティリスクは、事業環境の変化や利害関係者からの要求等によって絶えず変化するものです。そのため、必要な情報セキュリティ対策を適切に行うには、情報セキュリティリスクの変化を認識したうえで定期的なリスクアセスメントを行い、その結果を踏まえた対応を戦略的に講じることが重要となります。リスクアセスメントの重要性については、既に多くの事業者等の認識するところとなり、事業者等の掲げる情報セキュリティ方針等においても、リスクアセスメントの実施が記載されることが増えています。他方で、リスクアセスメントの重要性を認識しながらも、具体的にどのように進めたらよいかが分からないといった理由により、リスクアセスメントが実施できていない事業者等も多く存在しており、リスクアセスメントの考え方や実施方法がしっかりと定着しているとは言い難い状況です。

こうした状況を踏まえ、本手引書は、情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的とします。

＜２＞手引書の記載範囲

本手引書では主にリスクの特定・分析・評価といったリスクアセスメントの主要なプロセスについて記載しています。併せてリスクアセスメントの対象を特定するプロセスや、リスクマネジメントに含まれるリスクアセスメント以外のプロセスの一部についても記載しています。

図表１　本手引書の記載範囲



＜３＞手引書の適用範囲

（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ます。各事業分野や事業領域に特化したリスクアセス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ます。

（２）リスクアセスメントの対象

本手引書におけるリスクアセスメントでは、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、情報システム、IT を用いた制御システム

等の情報資産に係る事象の結果（自然災害やサイバー攻撃等に起因する優先サービス障害）から認識されるリスク（以下「情報セキュリティリスク」といいます。）を対象とします（※）。

（※）重要インフラ事業者等においては、情報セキュリティリスク以外のリスクがあることも考えられます。本手引書では、情報セキュリティリスクにスコープを限定したリスクアセスメントの手法を紹介していますが、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、情報セキュリティリスク以外のリスクについても勘案し、総合的に考慮することが重要です。

＜４＞手引書の構成

本手引書は、次に掲げるドキュメントにより構成されます。

図表２　本手引書のドキュメント構成

ドキュメント名称		概要
重要インフラにおける機能保証の考え方に基づく リスクアセスメント手引書		本文書
別紙１	業務の阻害につながる事象の結果の例	業務の維持のために経営資源に求められる観点を踏まえた「業務の阻害につながる事象の結果」（優先サービス障害）を例示した参考資料
別紙２	結果を生じ得る事象（脅威）の例	結果を生じ得る事象について、基本的な分類と併せて主な例示を掲載した参考資料
別紙３ （様式集） （※）	（様式１）リスクアセスメントの実施目的の確認	組織の活動目標の設定及びリスクアセスメントの実施目的・方針の確認のためのワークシート（記載例を含む。）
	（様式２）優先サービスの選定	利害関係者からの期待、社会的責任（ＣＳＲ）、法制面の要求（コンプライアンス）等を分析し、優先サービス（リスク評価の対象とするサービス）を選定するためのワークシート（記載例を含む。）
	（様式３）優先サービスの影響度分析	優先サービスの影響分析として、安全（＝許容できないリスクが無い状態）の観点を踏まえ最低限許容されるサービスの範囲・水準及びサービス提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定するためのワークシート（記載例を含む。）
	（様式４）優先サービスを支える業務の特定及び当該業務の影響度分析	優先サービスの提供のために必要な業務を洗い出し、その業務について最低限維持すべき状態を明らかにした上、その業務が停止した場合の影響及び最大許容停止時間を推定するためのワークシート（記載例を含む。）
	（様式５）業務を支える経営資源の特定	優先サービスの提供に必要な業務について、最低限維持すべき状態を維持するために必要な経営資源を明らかにするためのワークシート（記載例を含む。）
	（様式６）経営資源に係るリスクアセスメント	優先サービスの提供に必要な業務に係る経営資源を整理した上、その業務継続に対するリスクの特定、分析及び評価を行うためのワークシート（記載例を含む。）
別紙４	リスク源の例	リスク源について、基本的な分類と併せて主な例示を掲載した参考資料

（※）本手引書において、様式１から様式６までの様式を総称して「リスクアセスメントシート」といいます。

２．リスクアセスメントの全体像

＜１＞機能保証の考え方に基づくリスクアセスメントの観点・考え方

リスクアセスメントの手法には、既に確立されており、多くの運用実績を有するものが多数存在しますが、その手法の採用や実施手順において唯一の正解というものはありません。このため、事業者等がリスクアセスメントを実践する際には、どの手法を採用すれば、自組織にとって、より効果的・効率的にリスクの特定・分析・評価を行うことができるかを十分に検討した上、自らの判断でこれを決定することが必要です。この検討・決定に際しては、その提供するサービスが社会経済システムにおいて不可欠な役割・機能を担う重要インフラ事業者等においては、「機能保証」の考え方を踏まえることが重要となります。

機能保証の考え方（「重要インフラの情報セキュリティ対策に係る第４次行動計画」からの抜粋）

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

本手引書では、前述のとおり、重要インフラ事業者等により利活用されることを想定していることから、機能保証の考え方に基づくリスクアセスメントとして、「各重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために、許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続する」という観点から、情報セキュリティリスクの特定・分析・評価を実践するための手順を紹介します。

重要インフラ事業者等にあっては、リスクアセスメントを主体的かつ自律的に取り組むことが必要です。ただし、その取組の精度や水準については、各重要インフラ事業者等の力量に依存することから、本手引書では、機能保証の考え方に基づくリスクアセスメントの観点や参考になる作業手順を示すことにより、各重要インフラ事業者等における取組について一定以上の精度や水準が確保されることを狙いとしています。

なお、本手引書で紹介するリスクアセスメントの手順は、重要インフラ事業者等に限らず、中堅・中小企業を含む様々な分野の事業者等においても準用することができます。

＜２＞機能保証の考え方に基づくリスクアセスメントの方針

本手引書では、「２．＜１＞機能保証の考え方に基づくリスクアセスメントの観点・考え方」に記載したとおり、「重要インフラ事業者等が、機能保証の考え方に立脚し、リスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びにリスク対応の選択肢の同定を行うとと

もに、残留リスクを可視化すること」を志向します。このことを踏まえ、本手引書で紹介するリスクアセスメントの手法は、次に掲げる方針に従うものとします。

① リスクの捉え方

「社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続すること」を重要インフラ事業者等における経営戦略上の目的とし、「目的に対する不確かさの影響」をリスクと捉えます（ISO 31000:2018 における定義に準拠。）。ただし、機能保証の考え方を踏まえ、本手引書で対象とするリスクは、「負の影響：好ましくない結果をもたらすリスク」に限定します。

② 機能保証の考え方に基づく演繹的なリスクアセスメント

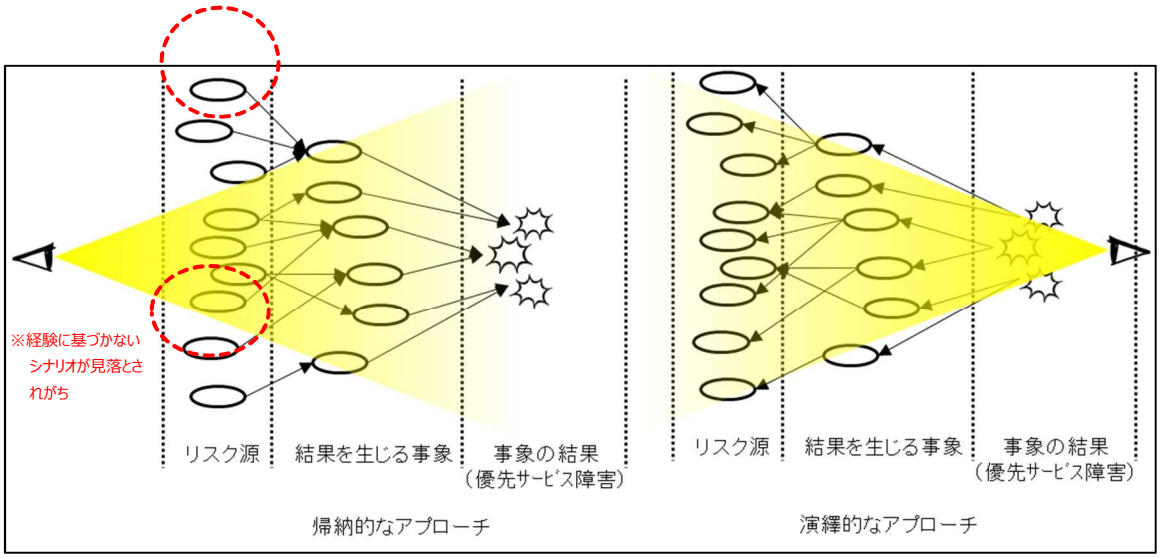
発生確率の低い事象から目を背けた（発生した場合には危機的状況につながる可能性がある事象であっても、過去に経験していない、又は発生確率が低いためにリスクとして想定しなかった）ことにより、その事象の結果が想定外となって大きな混乱を招くこととなった東日本大震災での教訓を踏まえ、上記①によるリスクの捉え方を前提として、機能保証の考え方に基づき、「重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために維持・継続することが必要なサービスを特定し、許容できないリスクが無い状態（＝安全）を確保しつつ、そのサービス提供を継続するために必要な業務や経営資源に係る要件を分析・評価」した上、これらに影響する「事象の結果からリスク源までを演繹的に特定・分析・評価」するアプローチとします。

③ 効率的な作業への配慮（帰納的なアプローチとの組合せ）

演繹的な詳細リスク分析のアプローチを採用しますが、多くの重要インフラ事業者等により実施されているイベントツリー分析等の帰納的なアプローチによって、想定される脅威（事象）及び脆弱性（リスク源）の組合せを書き出していくやり方も、重要インフラ事業者等が想定するリスクについての分析には一定の効果があることから、こうした実績のある帰納的な手法を組み合わせることにより、効率的な作業を行うことができるように配慮します。具体的には、重要インフラ事業者等における作業負荷や、作業者の知識・経験が浅い場合などに結果を生じる事象やリスク源を見逃してしまう可能性があることについても考慮し、リスク分析における気付きとなるような「業務の阻害につながる事象の結果の例」（別紙１）、「結果を生じ得る事象（脅威）の例」（別紙２）及び「リスク源の例」（別紙４）を提供することにより、作業の効率化や網羅性の確保に資するように配慮します。

図表３　アプローチ手法の比較

	帰納的なアプローチ	演繹的なアプローチ
概要	リスク源を想定し、そのリスク源から派生する様々な事象及び事象の結果がどうなるかを明らかにする手法 （イメージ）　$\mathscr{X}$ × $\mathscr{Y}$ → ?	事象の結果を想定し、その結果に至る様々な事象及びリスク源を明らかにする手法 （イメージ）　$\mathscr{Y}$ ← ? × ?
主な手法	イベントツリー分析	フォールトツリー分析
メリット	個別のシナリオ分析に優れており、各シナリオに応じた対処事項についての有効な知見を得ることができる	事象の結果に関するシナリオを演繹的に分析することにより、網羅的に全容を知ることができる
デメリット	リスク源を網羅することが難しい	提供するサービスや業務の構成が複雑な場合、分析結果の組合せが爆発的に増加し、作業負荷が多大になる



④妥当性確認

リスクアセスメントにおいては、唯一の絶対的な正解というものがなく、その判断結果には、作業者の立場や知識・経験に基づく偏り（バイアス）を含むことがあります。また、多くの作業者が分担して作業を行う場合には、作業者ごとにリスクアセスメント結果の粒度や精度にばらつきが生じることがあります。こうした特性を踏まえ、「リスクアセスメント実施内容が目的達成に向けて妥当であること」を検証するための妥当性確認（Validation）のプロセスを組み入れます。この妥当性確認のプロセスには、サービス提供を支える業務や経営資源に係る職務分掌の確認や部門間の連係状況の相互理解を目的とする関係主体間のコミュニケーションを含みます。

⑤リスクアセスメントの継続的な見直し

ＶＵＣＡと呼ばれる不透明な環境においては、重要インフラ事業者等が環境の変化に敏捷かつ適切に対応するために、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要となることから、妥当性確認を踏まえたリスクアセスメント結果の見直しを継続的に実施するために必要な体制を整備するプロセスを組み入れます。

＜３＞機能保証の考え方に基づくリスクアセスメントの枠組み

「２．＜２＞機能保証の考え方に基づくリスクアセスメントの方針」に記載された方針に基づき、次のとおり、機能保証の考え方に基づくリスクアセスメントの枠組みを示します。

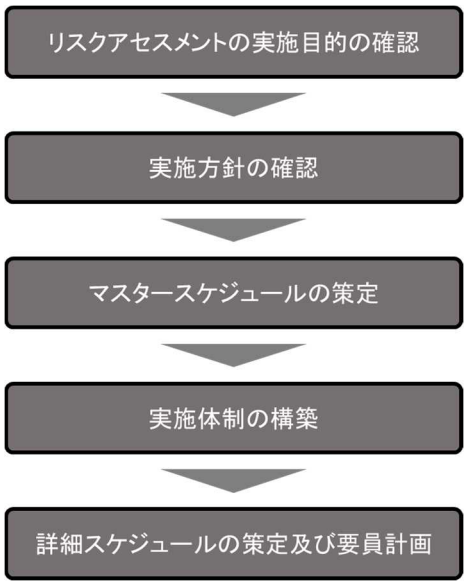
図表４　機能保証の考え方に基づくリスクアセスメントの枠組み

方針	リスクアセスメントのプロセス
①リスクの捉え方 ②機能保証の考え方に基づく演繹的なリスクアセスメント	４．リスクアセスメントの対象の特定 ６．リスクアセスメント
③効率的な作業への配慮 （帰納的なアプローチとの組合せ）	（別紙１）業務の阻害につながる事象の結果の例 （別紙２）結果を生じる事象（脅威）の例 （別紙４）リスク源の例
④妥当性確認	７．リスクアセスメントの妥当性確認・評価
⑤リスクアセスメントの継続的な見直し	８．リスクアセスメントの継続的な見直し

３．事前準備

本章では、機能保証の考え方に基づくリスクアセスメントの実施のための事前準備作業の実施手順を記載します。

＜１＞作業ステップ



＜２＞実施内容

（１）リスクアセスメントの実施目的の確認

自組織の活動目標を設定し、これを踏まえた自組織のリスクアセスメントの目的を確認します。機能保証の考え方に基づくリスクアセスメントでは、「自組織が社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスについて、許容できないリスクが無い状態（＝安全）を確保しつつ、そのサービス提供を継続するという観点を踏まえた自組織の活動目標を設定し、その目標に対するリスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びに残留リスクを可視化すること」が、基本的なリスクアセスメントの実施目的になります。

＜リスクアセスメントシートの活用＞

『（様式１）リスクアセスメントの実施目的の確認』を用いて、重要インフラ事業者として自組織が利害関係者から期待されている役割・機能を整理するプロセスを通じ、リスクアセスメントの実施目的の確認を行います。

（２）実施方針の確認

自組織におけるリスクアセスメントの実施方針（※）を設定し、経営層及び関係部門において、これを確認します。この際、本手引書で紹介する機能保証の考え方に基づくリスクアセスメントの枠組みを参考として、自組織における実施方針を定めることができます。

（※）本手引書において、リスクアセスメントの実施方針とは、「リスクアセスメントの目的を達成するために必要な活動の範囲や進め方について、経営層において合意されたもの」をいいます。

＜リスクアセスメントシートの活用＞

『（様式１）リスクアセスメントの実施目的の確認』を用いて、リスクアセスメントの実施目的の確認と合わせて実施方針の確認を行います。

（３）マススタースケジュールの策定

リスクアセスメントの実施方針が定まったら、実施方針として定めた各作業の実施時期を定め、リスクアセスメント活動全体の作業スケジュール（マススタースケジュール）を策定します。

リスクアセスメントには経営層による承認が要求されるプロセスも含まれており、マススタースケジュールの策定においては、このような進捗管理上の重要な節目となる局面をマイルストーンに設定し、これを踏まえたスケジュールとなるように調整することが重要です。

なお、マススタースケジュールは、進捗管理の前提である重要なベースラインであり、後続の作業手順である実施体制の構築や各作業部門での詳細スケジュールの策定及び要員手配の前提となります。

（４）実施体制の構築

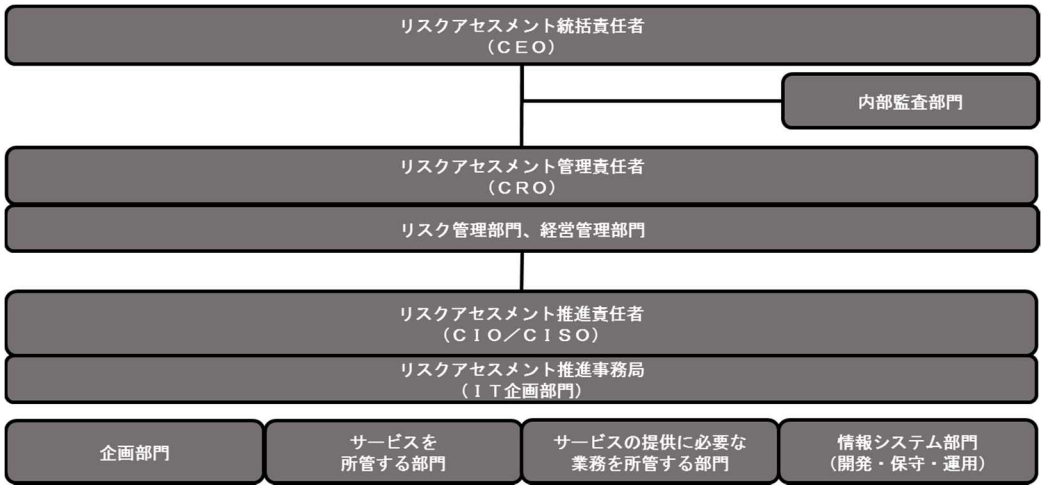
リスクアセスメントの実施方針及びマススタースケジュールを踏まえ、実施体制を構築します。実施体制の構築に際し、機能保証の考え方に基づくリスクアセスメントが経営戦略上の重要な活動であることを踏まえ、経営層が、リスクアセスメントの最高責任者として、推進及び管理を主導することが重要です。

図表５および図表６に、本手引書において想定する実施体制及び作業ステップ別の作業担当部門（例）を記載します。

図表６の STEP1 から STEP3 の作業においては特に、その実施主体は経営層との定期的なコミュニケーションを行い、組織全体としてのリスクマネジメントの方針等を理解したうえで取り組むことが重要となります。また各作業ステップの実施主体においては、作業に特定の部門内で閉鎖的に取り組むのではなく、経営層への正確な報告や進言を行うことを含め、関連部門間で適切にコミュニケーションを行いつつ進めていけるような仕組みを構築の上、連携して取り組むことが重要となります。

図表５　リスクアセスメント実施体制（例）

体制		役割	主な担当部門
統括	リスクアセスメント統括責任者	リスクアセスメントの目的達成に係る最終的な責任を負います。	ＣＥＯ
監査	リスクアセスメント監査部門	リスクアセスメントの管理・推進の妥当性を第三者的立場から確認し、リスクアセスメント統括責任者による意思決定を補助します。	内部監査部門
管理	リスクアセスメント管理責任者	リスクの運用管理の責任者であり、リスクアセスメントの結果等をリスクアセスメント統括責任者に報告する責任を負います。	ＣＲＯ
	リスクアセスメント管理担当部門	リスクアセスメント管理責任者を補助し、リスクの運用管理を担当します。	リスク管理部門 経営管理部門
推進	リスクアセスメント推進責任者	リスクアセスメントの推進に係る責任を負います。	ＣＩＯ／ＣＩＳＯ
	リスクアセスメント推進事務局	リスクアセスメント推進担当部門をとりまとめ、部門横断的なリスクアセスメントの全体調整を行います。	ＩＴ企画部門
	リスクアセスメント推進担当部門	リスクアセスメントの実施主体となります。	企画部門 サービス部門 業務部門 情報システム部門



図表６　作業ステップ別の作業担当部門（例）

STEP	評価対象	経営企画を所管する部門	サービスを所管する部門	サービスの提供に必要な業務を所管する各部門	
		Ex.経営企画部門 リスク管理部門	Ex.〇〇事業部門	Ex.営業部門、技術開発部門、 研究開発部門、システム部門	
STEP1：活動目標の決定	目標	◎			
STEP2：優先サービスの選定	サービス	◎	○		
STEP3：優先サービスの影響分析	サービス	○	◎		
STEP4：優先サービスを支える業務の特定・影響分析	サービス⇒業務		◎	○	
STEP5：業務を支える経営資源の特定	業務⇒経営資源			◎	
STEP6：リスクアセスメント	経営資源⇒リスク	○	○	○ （ユーザ部門）	◎ （システム部門）

◎：主担当（取りまとめ等）
○：副担当（結果の確認等）

（５）詳細スケジュールの策定及び要員計画

実施体制が定まり、各作業ステップの推進担当部門が決定したら、各推進担当部門において、詳細スケジュールの策定及び要員計画（作業担当者の選任及び作業の割当て）を行います。

要員計画に際しては、サービス、業務、システム等に係る有識者を確保するほか、組織で決められたレポートラインを踏まえた関連部門との連絡窓口となる担当者等の確保も考慮する必要があります。

４．リスクアセスメントの対象の特定

本章では、「リスクアセスメントの対象の特定」に係る作業の実施手順を記載します。

リスクアセスメントの対象は、機能保証の考え方に基づき、重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を発揮するために、許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続することが必要なサービスを特定し、これに必要な業務や経営資源に係る要件を分析・評価した結果を踏まえて、見極めます。

なお、この一連の作業は、バリュー・チェーン及びサプライチェーンの把握並びに事業影響度の把握を通じて、後続のリスク評価を行う上での評価基準（リスク基準）の前提となる、リスクに対する態度及びリスク許容度を分析する作業でもあります。

＜１＞作業ステップ

＜２＞実施手順

（１）優先サービスの選定

重要インフラ事業者等が扱うサービスについて、経営上の位置付け（業績への寄与度や事業上の依存度等の事業経営上の位置付け）、利害関係者（顧客、仕入先、株主、地域社会等）からのニーズ・期待、社会的責任（ＣＳＲ）、法制面の要求（コンプライアンス）等を総合的に勘案した上、機能保証の考え方に基づきサービスの重要度（優先度）を評価し、リスクアセスメントの対象とするサービス（優先サービス）を特定します。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５版）（以下、「指針」といいます）の別紙２に記載された「重要インフラサービス」は、優先サービスとして特定されることが想定されます。

＜リスクアセスメントシートの活用＞

『（様式２）優先サービスの選定』を用いて、サービスに関する利害関係者の期待事項や法制面での要求事項等を勘案し、事業者等にとって重要なサービスを特定します。

（２）優先サービスの影響分析

優先サービスについて、前ステップ「（１）優先サービスの選定」で分析した要求事項等を満たすために、安全（＝許容できないリスクが無い状態）の観点を踏まえ最低限許容されるサービスの範囲・水準を明らかにします。また、優先サービスの提供が完全に停止した場合に生じる事態及び時間経過に伴う影響度合いを分析・評価し、優先サービスの最大許容停止時間（ＭＴＰＤ, Maximum Tolerable Period of Disruption）を推定します。

＜リスクアセスメントシートの活用＞

『（様式３）優先サービスの影響度分析』を用いて、サービスに関する利害関係者の期待その他要求事項等を満たすために最低限許容されるサービスの範囲・水準を明らかにし、またサービスの提供が完全停止した場合の影響を分析・評価した上でサービスの最大許容停止時間（ＭＴＰＤ）を推定します。

（３）優先サービスを支える業務の特定・影響分析

優先サービスの提供に必要な業務を洗い出し、その業務について許容される最低限の水準（操業率、稼働率等）を明らかにします。この際、自組織のバリュー・チェーンを意識して作業を行うことを推奨します。また、その業務が完全に停止した場合に生じる事態及び時間経過に伴う影響度合いを分析・評価し、業務の最大許容停止時間を推定します。

図表７　一般的なバリュー・チェーンの例

＜リスクアセスメントシートの活用＞

『（様式４）優先サービスを支える業務の特定及び当該業務の影響度分析』を用いて、サービスに関する利害関係者の期待その他要求事項等を満たすための優先サービス提供に必要な業務の範囲・水準を明らかにし、また業務が完全停止した場合の影響を分析・評価した上で業務の最大許容停止時間（ＭＴＰＤ）を推定します。

（４）業務を支える経営資源の特定

前ステップ「（３）優先サービスを支える業務の特定・影響分析」で洗い出した業務を遂行するために必要な経営資源を特定し、その必要な要件（条件や数量など）を分析します。

＜リスクアセスメントシートの活用＞

『（様式５）業務を支える経営資源の特定』を用いて、『（様式４）優先サービスを支える業務の特定及び当該業務の影響度分析』で洗い出した業務を支える経営資源（優先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、設備、人、ライフライン等）を洗い出します。

５．リスク評価方針の策定

本章では、「リスク分析の手法及びリスク評価の基準（リスク基準）の策定」に係る作業の実施手順を記載します。

リスク評価のための手法には様々なものがありますが、従来型の情報セキュリティリスクの評価においては、「情報資産の価値（機密性・完全性・可用性の観点から評価）×脅威の大きさ×脆弱性の度合い」といった算式により、情報資産保護の観点からリスクの重大さを測ることが一般的でした。この手法では、まず情報資産を洗い出した後、その情報資産に自らが想定する事象（セキュリティ・インシデント）を当てはめるという帰納的なアプローチでリスクの特定・分析・評価が行われます。この帰納的なアプローチは、過去の経験の中から事象を当てはめるという経験的な作業を伴いやすく、再発防止型のアプローチであるともいえます。また、この手法は、情報資産の洗出しから最終的なリスクの評価までが情報システム部門内で完結してしまい、機能保証の考え方に基づくサービス提供への影響を十分に分析・評価されにくいことも懸念されます。

従来型の情報セキュリティリスクの評価において、こうした課題があることを踏まえ、本手引書では、機能保証の考え方に基づき優先サービスに要求されるサービスレベル・業務要件を踏まえた影響度合い等を考慮したリスク評価方針（分析手法及び評価基準）を策定します。

＜１＞作業ステップ

＜２＞実施手順

（１）リスク分析手法の検討

本手引書では、多くの重要インフラ事業者等により採用されているリスクマップ及びリスク・スコアリングの手法を用いたリスク分析を紹介します。

リスクマップは、一般的に、「影響度」及び「発生頻度（発生可能性、起こりやすさ）」又は「情報資産の価値」及び「脅威の大きさ×脆弱性の度合い」をそれぞれ縦横の軸にしたマトリクスにリスクを配置して、そのリスクの相対的な優先関係を把握する分析手法です。また、それぞれの要素に重大さに応じた一定のスコアを付して掛け合わせることによって、優先して対応すべきリスクを明確にする分析手法をリスク・スコアリングといいます。

機能保証の考え方に基づくリスクアセスメントでは、「自組織が社会経済システムの中で果たすべき役割・機能を発揮するために、許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続するという観点を踏まえた自組織の活動目標を設定し、その目標に対するリスクを戦略的に最適化するために、リスクの特定、分析及び評価を行い、並びに残留リスクを可視化すること」が基本的なリスクアセスメントの実施目的となることから、「事象の結果による

優先サービス・業務への影響度合い」と「事象の発生頻度（発生可能性、起こりやすさ）」を評価の軸とします。

「事象の結果による優先サービス・業務への影響度合い」については、「４．リスクアセスメントの対象の特定」において分析した結果を踏まえ、例えば、次に掲げる要素等を用いて総合的に評価します。

図表８　主な影響度合いの評価要素

影響度合いの評価要素	概要
業務に対する予想影響範囲・程度	事象の結果が優先サービスを支える業務に及ぼすと予想される影響の範囲及び程度を評価します。業務に及ぼす影響には、「４．リスクアセスメントの対象の特定」において分析した各要求事項への影響についても考慮します。
予想復旧時間	事象の結果により優先サービスを支える業務が停止又は阻害された場合における予想復旧時間を評価します。
予想対応コスト	事象の結果により優先サービスを支える業務が停止又は阻害された場合において、その業務の復旧や事象の結果の対処に要する予想コストを評価します。
人命や環境への予想影響範囲・程度	事象の結果により人命や環境に損害を与える可能性がある場合の、発生し得る影響の範囲及び程度を評価します。

（２）リスク基準の決定

リスク基準とは、リスクの重大さを評価するための目安とする条件であり、リスクアセスメント作業担当者によって評価結果にばらつきを生じさせないことを狙いとして、あらかじめ設定される判断指標をいいます。

機能保証の考え方に立脚すると、リスク基準は、許容できないリスクが無い状態（＝安全）を確保する観点を踏まえつつ、優先サービスの許容最低水準を満たすことや、許容停止時間内での復旧が可能であることが目安となります。「事象の結果による優先サービス・業務への影響度合い」と「事象の発生頻度（発生可能性、起こりやすさ）」を評価の軸とする場合におけるリスク基準の設定イメージは、次ページのとおりです。

なお、リスク基準は、リスクアセスメントの目的に応じた設定にすることが必要です。また、リスクアセスメントの継続的な見直しにおいて、環境変化等に応じて設定の見直しを行うことも重要です。

＜リスク基準の設定イメージ＞

事象の結果として、優先サービスを支える業務が停止する場合や業務の復旧が困難になる場合、人命や環境へ大きな損害が生じる場合等を重大な影響として評価し、この場合においては、発生頻度が非常に少ないと評価されるときであっても、リスク対応の対象となるようにリスク基準を「５以上」と設定しています。

図表９　リスク基準の設定イメージ

（例）

発生頻度		事象の予想発生頻度
5	非常に多い	頻発
4	多い	1年に1回程度発生
3	中程度の頻度	数年に1回程度発生
2	少ない	10年に1回程度発生
1	非常に少ない	ごくまれに、例外的な状況で発生

影響度		影響度合い（下記のような要素を総合的に勘案して影響度を決定します。）			
		業務に対する影響の範囲・程度	予想復旧時間	対応に要するコスト	人命や環境への影響範囲・程度
5	重大な影響	当該業務が停止する。	業務の復旧自体が困難である。	業務の復旧や事象の結果の対処（情報漏えいに係る損害賠償金の支払や代替手段の手配等を含む。）のために要するコスト（業務停止中の損失等を含む。）の負担が、事業者にとって甚大である。	複数の死亡者が発生する。
4	大きな影響	当該業務が阻害され、業務の最低水準の維持が困難である。	業務の最大許容停止時間内での業務の復旧が困難である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって大きい。	1人の死亡者あるいは複数の重傷者が発生する。
3	中程度の影響	当該業務が阻害され、業務の最低水準を維持できないおそれがある。	業務の最大許容停止時間内での業務の復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって中程度である。	1人の重傷者あるいは複数の軽症者が発生する。
2	小さな影響	当該業務が阻害されるが、業務の最低水準は維持される。	業務の阻害が軽度で収まる時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって小さい。	1人の軽症者が発生する。
1	軽微な影響	－	業務の阻害が生じない時間内での復旧が可能である。	業務の復旧や事象の結果の対処のために要するコストの負担が、事業者にとって軽微である。	－

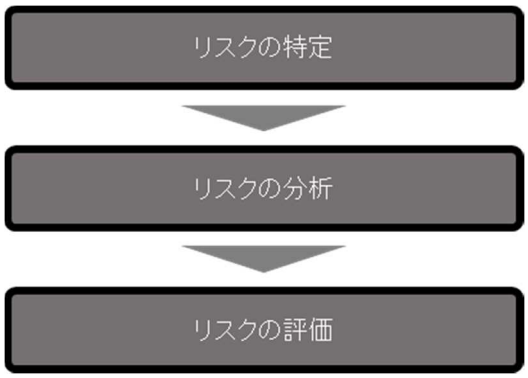
※リスク基準を「５以上」とした場合、黄色い個所に該当するリスクがリスク対応の対象となります。

事象の予想発生頻度						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		事象の結果の影響度				

６．リスクアセスメント

本章では、「優先サービスの提供に必要な業務に係る経営資源を整理した上、その経営資源に係るリスクを特定、分析及び評価」するための作業の実施手順を記載します。

＜１＞作業ステップ



＜２＞実施手順

（１）リスクの特定

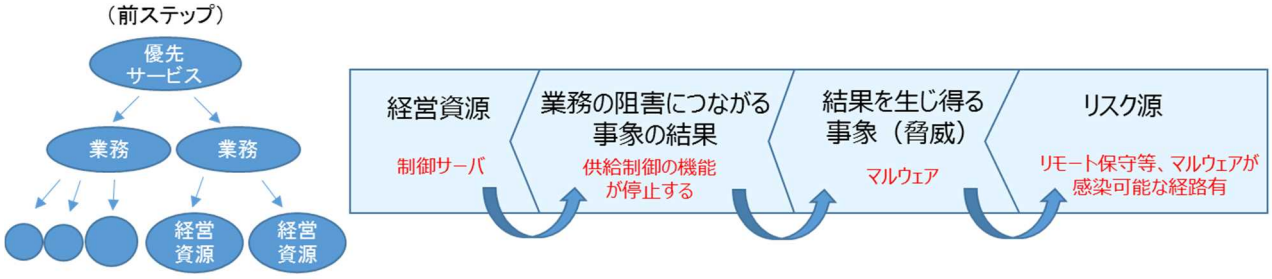
次のステップに沿って、演繹的にリスク源を洗い出します。

①優先サービスの提供に必要な業務に係る経営資源に対し、「業務の阻害につながる事象の結果」を書き出します。

②上記①の「結果を生じ得る事象」を書き出します。

③上記②の事象と合わせて上記①の結果を生じ得る「リスク源」を書き出します。

図表 10　＜例＞制御サーバを経営資源とした際の作業イメージ



＜リスクアセスメントシートの活用＞

『（様式６）経営資源に係るリスクアセスメント』を用いて、『（様式５）業務を支える経営資源の特定』で洗い出した経営資源（情報資産）ごとに、業務の阻害につながる事象の結果、その結果を生じ得る事象及びリスク源を特定します。

（２）リスクの分析

次のステップに沿って、「事象の結果による優先サービス・業務への影響度合い」と「事象の発生頻度」を分析し、リスク評価のインプットとなる「残留リスク値」を導出します。

①事象の結果が優先サービス・業務に及ぼし得る影響について、その内容を書き出し、「５．リスク評価方針の策定」において定めた評価軸に基づく評価を行います（※）。

②事象の発生頻度について、「５．リスク評価方針の策定」において定めた評価軸に基づく評価を行います（※）。

③上記①及び②の結果を踏まえ、「５．リスク評価方針の策定」において定めた評価マトリクスに基づき、リスク源ごとの残留リスク値を導出します。

（※）何らかの対策を講じている場合であっても、技術の進歩により対策の有効性が陳腐化しやすいという情報セキュリティ対策の性質を考慮し、対策前の評価（固有リスク）及び対策後の評価（残留リスク）の両方を行います。

図表 11　＜例＞リスク分析のイメージ

リスク基準（図表９参照）を用いたリスク分析

（例）

リスクの特定			事象の結果による優先サービス・業務への影響度合い				事象の発生頻度			残留リスク値
業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	事象の結果の影響	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後	
顧客情報の情報流出	内部持ち出し	悪意ある人物が情報を持ち出せる環境	業務停止に直結するものではないが、調査や説明対応に追われることにより、通常業務の遂行を大きく阻害する。	4	顧客情報を扱うシステムの操作者は制限され、操作できるサービスレベルも操作者ごとに必要最低限に制限されている。	3	4	社員教育の実施	3	9

＜リスクアセスメントシートの活用＞

『（様式６）経営資源に係るリスクアセスメント』を用いて、「事象の結果による優先サービス・業務への影響度合い」と「事象の発生頻度」を分析・評価し、リスク評価のインプットとなる「残留リスク値」を導出します。

（３）リスクの評価

次のステップに沿って、「リスク対応の実施対象とするリスクを特定」します。ここでは、洗い出されたリスクから、経営層による全社的な意思決定に基づくリスク対応の実施対象とするリスクを選別し、そのリスクに係る組織内の責任主体を明確化することが作業目的となります。

①リスク対応の実施対象として、リスク基準以上の残留リスク値のリスクを抽出します。

②リスク基準未満の残留リスク値のリスクのうち、個別事情についても勘案（※）した上、リスク対応の実施対象とするものを抽出します。

（※）リスク基準は、あくまでリスク対応の優先度に係る判断の目安であり、実際のリスク評価の際には、個別の事情に応じて適宜に判断します。

③上記①及び②で抽出されたリスク（経営層による全社的な意思決定に基づくリスク対応の実施対象とするリスク）に対し、リスクオーナー（そのリスクの対処に関する責任を負担する部署・部門又は役職員）を定めます。

（注）本ステップにおいてリスク対応の実施対象として抽出されたリスクについては、経営層による全社的な意思決定の対象として、定期的にモニタリングを行い、リスクアセスメントの継続的な見直しの中で再評価を行います。
なお、本ステップにおいてリスク対応の実施対象として抽出されなかったリスクについては、リスクとして認識しないということではなく、通常の業務又は職務上の分掌に基づく管理対象として、所管する部署・部門又は役職員の責任において管理します。

＜リスクアセスメントシートの活用＞

『（様式６）経営資源に係るリスクアセスメント』を用いて、「リスク基準」以上の「残留リスク値」のリスク源を抽出し、そのリスクのリスクオーナーを定めます。

7．リスクアセスメントの妥当性確認・評価

本章では、「リスクアセスメントの妥当性確認・評価」の実施手順を記載します。

リスクアセスメントの結果には、作業者の立場や知識・経験に基づく偏り（バイアス）や、複数の作業者で作業を分担することなどによる粒度や精度のばらつきが生じることがあります。こうした偏りやばらつきを解消し、リスクアセスメントの実施主体において、その実施内容が目的達成に向けて妥当であることを保証するためには、複数の関係主体が連携してリスクアセスメントの実施内容を検証し、その結果を共有することが必要です。

また、効果的なリスクアセスメントの実現には、リスクアセスメント作業が適切かつ十分に実施されたかどうかを客観的に評価した上、その結果を関係者にフィードバックし、改善につなげることが重要です。一般的に、ある取組に対して評価を行う場合、ストラクチャー（構造）、プロセス（過程）及びアウトカム（成果）の各観点から実施されますが、リスクアセスメントの評価においては、成果の有効性（リスクアセスメントの目的がどれだけ達成されたか）を評価することが困難であることから、「リスクアセスメントを実施するための体制並びにリスクアセスメントの実施手順及び活動状況が適切かつ十分であったか」を評価することにより、リスクアセスメントの妥当性を確認します。

こうした妥当性確認のための取組として、本手引書では、「ウォークスルー（リスクアセスメントの実施内容の妥当性確認）」による分析結果の検証及び「パフォーマンス評価（リスクアセスメント作業の妥当性確認）」による実施体制や活動内容の評価を紹介します。

図表 12　妥当性確認の手法

妥当性確認の手法	概要	主な実施主体
ウォークスルー（リスクアセスメントの実施内容の妥当性確認）	リスクアセスメントの結果における偏りやばらつきを解消するため、複数の関係主体が連携してリスクアセスメントの実施内容を検証し、その正当性を確認するとともに、検証結果を共有・合意するための取組。サービス提供を支える業務や経営資源に係る職務分掌の確認や部門間の連係状況の相互理解を目的とする関係主体間のコミュニケーションを含みます。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門） （注）関連業務の所管部門、経営資源の利用部門、法務部門、リスク管理部門等もレビュー役として参画する
パフォーマンス評価（リスクアセスメント作業の妥当性確認）	リスクアセスメントを実施するための体制並びにリスクアセスメントの実施手続及び活動状況が適切かつ十分であったかを評価することにより、リスクアセスメントの妥当性を確認する取組 （※）本手引書では、ISO22301、ISO27001 等で採用されているＩＳＯマネジメントシステムの上位構造（High Level Structure：ＨＬＳ）を参考として、この取組を「パフォーマンス評価」（Performance Evaluation）と称します。	・リスクアセスメント監査部門（内部監査部門等のリスクアセスメントの管理・推進の妥当性を第三者的立場から確認する部門）

＜１＞作業ステップ

＜２＞実施手順

（１）ウォークスルー

ウォークスルーは、複数の関係主体を交えたリスクアセスメントの妥当性確認のための取組として、前ステップ「６．リスクアセスメント」に係る作業が完了した後、リスクアセスメントの実施目的の確認からリスクの評価までの一連の取組を対象として、次のような流れで実施します。ただし、対象範囲及び実施のタイミングについては、例えば規模の大きな組織において効率的に作業を進めるため、作業の中途で担当者の範囲を限定した簡易的なウォークスルーを実施するなどの工夫を行うことが望ましいです。

①担当者の選任及び役割分担

ウォークスルーを実施する担当者（以下「ウォークスルー担当者」と総称します。）を選定します。ウォークスルーを円滑に実施するためには、役割分担した上、役目に応じた適切な担当者がウォークスルーに参画することが重要です。

図表 13　ウォークスルーにおける主な役割・役目

役割	役目	担当部門（例）
まとめ役	ウォークスルーの推進役として、ウォークスルーを実施する担当者の選任に係る調整、スケジュールの調整、確認観点の整理、レビュー対象成果物の手配等を行います。また、ウォークスルーの結果を踏まえたリスクアセスメント結果の修正等について、リスクアセスメント推進担当部門のフォローアップを行います。	・リスクアセスメントの推進事務局
説明役	ウォークスルーを実施する各担当者に対し、レビュー対象成果物の記載により可視化されたリスクアセスメントの実施目的並びに優先サービスを支える業務・経営資源及びリスクの関係性についての説明を行います。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門）
レビュー役	説明役からの説明を踏まえ、レビュー対象成果物の記載内容に対し、確認観点に基づく指摘を行います。 リスクアセスメント結果の粒度や精度のばらつきを抑えるという観点から、リスクアセスメントシートの作成者（リスクアセスメント推進担当部門）だけでなく、リスクアセスメントシートの作成者の所属部門以外の者、とりわけ関連業務の所管部門や経営資源の利用・管理部門等の参画が必要です。また、総合的な判断に基づき優先サービスの選定やリスク評価がなされていることを確認する観点から、必要に応じて、経営企画部門、法務部門、リスク管理部門、広報（ＩＲ）部門等の間接部門からもレビュー役を任命することが重要です。	・リスクアセスメントシートの作成者（リスクアセスメント推進担当部門） ・企画部門 ・サービスを所管する部門 ・サービスの提供に必要な業務を所管する部門
記録役	ウォークスルーの議事内容、指摘事項等の記録を行います。	・リスクアセスメントの推進事務局

（※）同一の担当者が複数の役割を務めたり、ここに記載されていない役割を設置したりすることがあります。

②事前準備（確認観点等の周知）

各関係主体がリスクアセスメントの結果（リスクアセスメントシートの記載内容）の正当性を確認し、結果についての認識を正しく共有及び合意するために、事前に、ウォークスルーにおける確認観点を策定した上、ウォークスルーを実施する各担当者に周知しておくことが必要です。

図表 14　ウォークスルーにおける確認観点（例）

確認の目的	確認観点（例）
リスクアセスメントシートに記載された内容が正当であること	・サービス、業務、経営資源等が抜け漏れなく洗い出されているか。また、その洗出作業の際に参照した内部資料等の根拠が客観的に成果物から読み取れるか。 ・各ステップでの判断が、前ステップの結果を踏まえて論理的に説明可能であるか（整合性が確保されているか）。また、その判断根拠が客観的に成果物から読み取れるか。 ・優先サービスの選定に当たり、自組織の活動目標、経営環境の変化、関連法令その他の要求事項等を踏まえた判断がなされているか。また、その判断根拠が客観的に成果物から読み取れるか。 ・優先サービスが完全停止した場合の影響について、直接の取引先だけでなく、エンドユーザー等も考慮に入れて判断がなされているか ・優先サービスの提供に必要な業務について、直接的に顧客との接点がある業務に限らず、間接業務についても考慮されているか ・リスクの分析において、固有リスクの評価がなされているか
リスクアセスメントシートに記載された内容についての認識が共有及び合意されていること	・リスクアセスメントシートの記載内容が、読み手に誤解を与え、共有認識の醸成を妨げるような記述（主語や目的語が明確でない、複数の解釈が可能な書き振りとなっているなど）となっていないか。また、特定の部門内、とりわけ情報システム部門内でしか通じないような記述（専門性の高い用語を用いているにもかかわらず、対外的に通用する補足説明がないなど）となっていないか。 ・リスクアセスメントシートの記載の粒度や精度にばらつきがないか。 ・リスク基準の解釈やリスク基準に基づくリスク評価の判断について、関係主体間の認識齟齬はないか

③ウォークスルーの実施

ウォークスルーを実施する各担当者が、それぞれの役割に基づき、確認観点を踏まえた指摘事項を出し合い、互いが持っているリスクに対する認識をすり合わせ、必要な修正事項を導き出します。

また、次回以後の取組における効率性の向上に向けて、リスクアセスメント作業において体制面や実行面での反省点（改善すべき点）を確認します。

④レビュー対象成果物の修正

ウォークスルーで出された指摘事項を踏まえた修正事項について、レビュー対象成果物の作成者が修正を行います。

⑤ウォークスルー結果のまとめ

ウォークスルーの実施結果については、各関係主体間で共有されるだけでなく、「（2）パフォーマンス評価」において、一連のリスクアセスメント活動に係るプロセスの妥当性を評価するためのレビュー対象成果物となります。このため、まとめ役は、ウォークスルーの実施に係る証跡として、次の成果物を作成します。

図表 15　ウォークスルーの実施に係る証跡（例）

証跡となる成果物	概要
ウォークスルー記録票	ウォークスルーの実施プロセスに係る証跡として、開催日時、レビュー対象、参加者の所属・氏名・ウォークスルーにおける役割、議事内容等を記録します。
ウォークスルー指摘事項一覧表	ウォークスルーの実施内容に係る証跡として、指摘内容、指摘者、指摘に対する対応方針、指摘に基づく修正内容等を記録します。

⑥各関係主体へのフィードバック

まとめ役は、ウォークスルーに係る一連の作業が完了した後、『ウォークスルー記録票』及び『ウォークスルー指摘事項一覧表』を各関係主体と共有します。

（２）パフォーマンス評価

パフォーマンス評価は、独立した担当者によるリスクアセスメントの妥当性確認の取組として、ウォークスルーの完了後、次のような流れで実施します。

①評価担当者の選任

パフォーマンス評価の一連の作業を実施する評価担当者を選任します（担当者数については、自組織の規模等に応じて判断します）。評価担当者の選任に当たっては、次に掲げる観点を考慮することが重要です。

図表 16　評価担当者の選任に当たり考慮すべき主な観点

考慮すべき観点	趣旨
評価担当者の独立性	会計監査や業務監査等と同様、パフォーマンス評価は、前ステップまでのリスク評価作業から独立した担当者が行うことによって公正性・客観性が確保され、ひいてはリスクアセスメントの品質向上に寄与すると考えられます。このため、事業部門から独立した内部監査部門等を有しない中小規模の事業者等においては、コンサルタント企業等の外部の専門家を活用することも有効です。
必要な能力・知識	パフォーマンス評価では、ストラクチャー及びプロセスの評価を行うことから、担当者には基本的なドキュメント読解力やフィードバック時の関係者への説明力等が要求されます。後述の観点を参考に評価を行う限りにおいては、ＩＴや情報セキュリティに関する高度な専門知識は不要と考えます。

②パフォーマンス評価の実施

パフォーマンス評価では、公正性・客観性の確保やリスクアセスメント推進担当部門の負担軽減といった観点から、前ステップ及びウォークスルーまでの作業における各成果物を確認することを基本とします。具体的には、「リスクアセスメントシート」の記載に係る品質の確認を行い、あわせて「ウォークスルー記録票」及び「ウォークスルー指摘事項一覧表」を参照することにより、リスクアセスメントシートの記載内容について関連部門間で認識が共有され、リスク対応の実施対象とするリスクについて合意がとれていること（合意形成のプロセスが適切であること）などを確認します。

なお、各成果物の確認作業は、次に例示したような観点を踏まえて実施することを推奨します。

図表 17　パフォーマンス評価における確認観点（例）

対象成果物	確認観点（例）
リスクアセスメントシート	・明らかな記載漏れがないか。特に、特定されたリスクの分析・評価結果の記載漏れがないか。 ・明らかな記載誤りがないか。例えば、既に何らかの対策を講じているにも関わらず、その対策を講じる前に比べ、リスクが高い評価数値となっているようなことはないか。 ・全ての記載項目について、回答者（記入者）及びその責任者の名前が漏れなく明記されているか ・リスク評価を先送りにした（リスク評価の対象としなかった）サービス又は業務がある場合、コメント欄等に妥当性のある理由が明記されているか。また、責任者が先送りを承認していることが確認できるか。

	・リスク評価の対象とするリスクに対し、リスクオーナーが定められているか。また、リスクオーナーとして、そのリスクの影響範囲等を踏まえた適切な部門や役職員が選任されているか。
ウォークスルー記録票	・全てのリスクアセスメント推進担当部門がウォークスルーに参加し、レビューを実施しているか。特に、評価結果の精度向上の観点から、有識者（サービスの提供、サービスの提供に必要な業務及び業務に係る経営資源に関し、一定の職務経験や知識を有する者）がウォークスルーに参加し、レビューを実施しているか。 ・評価結果の客観性を確保する観点から、法務部門やリスク管理部門等の間接部門がウォークスルーに参加し、レビューを実施しているか。 ・ウォークスルーの実効性（形骸化していないこと）を確認する観点から、各ウォークスルー担当者が、それぞれの役割に基づき、確認観点を踏まえた指摘事項を出しているか。また、リスクアセスメントシートに記載された内容のボリュームに照らし、適当な時間・回数で実施されているか。 ・ウォークスルーの実施結果は、経営層に対し適切に報告されているか（又は経営層がウォークスルーに参加し、レビューを実施しているか）
ウォークスルー指摘事項一覧表	・ウォークスルーで出された指摘事項に対して、漏れなく対応方針が整理されているか。また、整理された対応方針は、リスクアセスメントシートに確実に反映されているか。

③パフォーマンス評価結果のまとめ

パフォーマンス評価の結果として、反省点（改善すべき事項）等が発見された場合には、各関係主体へのフィードバックに備え、リスト化しておきます。

④各関係主体へのフィードバック

評価担当者は、パフォーマンス評価に係る一連の作業が完了した後、パフォーマンス評価結果を各関係主体と共有します。その際、後続で検討するリスク対応の最終責任者である経営層に対しても、同結果を共有することを推奨します。

また、リスクアセスメントに係る取組において良好だった点についても共有することが望ましいと考えます。良好だった点が各関係主体に認識され、水平展開されることによって、リスクアセスメントの更なる品質向上が期待できます。

＜３＞課題管理

リスクアセスメント作業や妥当性確認により明らかとなった体制面や実行面での反省点（改善すべき点）等については、その原因を分析し、課題として特定します。この際、特定された課題については、課題管理表に登録します。

特定された課題について各関係主体間で共有し、作業（タスク）単位に分割して、作業担当者に対し解決期限を定めて割り当てます。各タスクは完了するまで継続的に監視し、経過及び結果を記録して、課題のフォローアップを行います。

＜参考＞リスクアセスメントの次ステップ（リスク対応の選択肢の同定）

リスク対応では、対象とするリスクに対して、どのような対処を、いつまでに行うかを明確にします。対処の方法には、大きく分けて「リスクの低減」「リスクの回避」「リスクの移転」「リスクの保有」の４つがあります。各リスクについて、これらの対処方法のいずれを採用するかを同定することにより、リスク対応の方針を明らかにします。

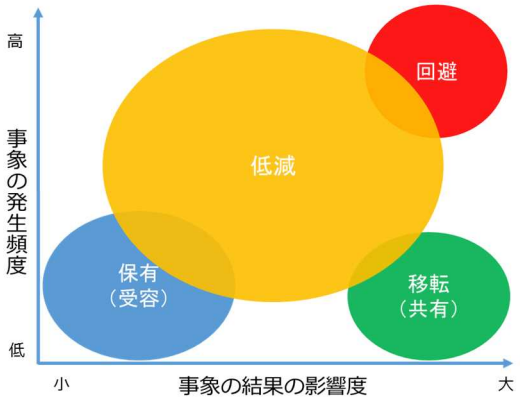
＜リスク対応の選択肢＞

対処方法		概要	分類
＜１＞低減		リスクに対して適切な管理策を適用する。	リスク・コントロール
	①リスク源の除去	リスクの起こりやすさ及び結果に与える影響の源を除去する。（例：脆弱性に対するセキュリティパッチの適用）	
	②影響度の低減	事業者等への影響度を低減させる。	
	③起こりやすさの低減	発生頻度や起こりやすさを下げる。	
＜２＞回避		リスクを生じさせる活動を開始又は継続しないことを決定することにより、リスクを回避する。	
＜３＞移転（共有）		一つ以上の他者とリスクの全部又は一部を共有する。（契約によるリスクの分散及び保険加入等による金銭面でのリスク対策を含む。）	リスク・ファイナンス
＜４＞保有（受容）		情報に基づく意思決定により、リスクを保有（受容）する。	

（注）ISO 31000:2018 において、リスクの低減には、「ある機会を追求するために、リスクを取る又は増加させる」という概念も含まれていますが、本手引書では、目的に対する負の影響をリスクと捉える考え方に基づくため、表中には記載していません。

効果的なリスク対応を実現するためには、事象の発生頻度や事象の結果の影響度合いなどに応じて、適切な対策を講じることが必要です。事象の発生頻度及び事象の結果の影響度合いのいずれも大きいと判断されたリスクについては、そのリスクの大きさを小さくするための努力をするよりも、むしろリスク回避をした方が望ましいという考え方もあります。また、発生頻度が低いものの、影響度が大きいといった場合には、サイバー保険等を活用したリスク移転（共有）が望ましいという考え方もあります。こうした考え方を整理すると、発生頻度と影響度に応じて、一般的には、下図のように表すことができます。

＜発生頻度及び影響度に応じたリスク対応（例）＞



なお、リスク対応の選択肢の同定は、必ずしも択一ではなく、複数の選択肢に跨る対処を実施することがあります。特に重要インフラ事業者等における機能保証の考え方を踏まえると、リスクの低減若しくは移転又はこれらの組合せにより、リスクの回避を選択しないための最大限の努力を払うことも必要です。

また、例えば情報漏えいのような事象においては、事象の結果の影響度が低く、かつ、事象の発生頻度が高いと分析された場合であっても、起こりやすさの低減が必ずしも合理的なリスク対応でなく、セキュリティパッチの適用等のリスク源の除去を講じた方が費用や効果の面でより合理的なリスク対応であるケースもあります。

最終的には、事業者等の活動目標や利害関係者からの要求事項等を勘案して意思決定することになりますが、こうした考え方を念頭に置きながら、リスク対応の選択肢の同定について検討することが重要です。

なお、リスク対応後の残留リスクについては、意思決定者を含む関係主体間（必要に応じてサプライチェーン等を含む）と共有し、その特質及び程度を認識することが必要です。

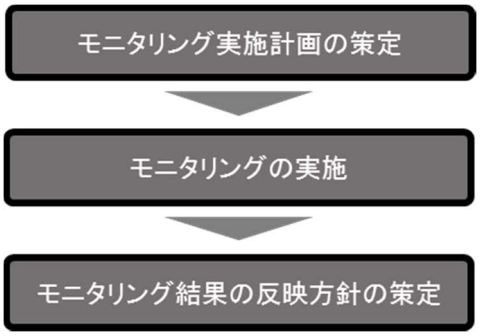
８．リスクアセスメントの継続的な見直し

リスクアセスメントの結果として認識された状態は、経時的に変化すると予想されます。リスクアセスメントを変更又は無効なものとするおそれのある状況及びその他の要因を特定し、リスクの変動に適切に対処するためには、「リスクアセスメント結果の継続的なモニタリング（リスクアセスメントの結果として認識された状態との差異を特定するために、状態を継続的に点検し、監督し、要点を押さえて観察し、又は決定する取組）を実施し、必要に応じて適宜にリスクアセスメント結果の見直しを実施する」など、リスクを適切に管理し、リスクマネジメントの取組を継続的かつ有効に機能させる仕組みを構築することが必要です。

本章では、リスクアセスメントの継続的な見直しに向けたモニタリングについて、参考になる実施手順を記載します。

なお、次回以後のリスクアセスメントの際には、モニタリングの結果を踏まえ、必要な体制や運用の見直しを行います。

＜１＞作業ステップ



＜２＞実施手順

（１）モニタリング実施計画の策定

リスクアセスメントシートに記載されたリスクアセスメント結果について、モニタリングを行うため、その実施計画を策定します。

なお、実施計画には、モニタリングの結果を踏まえた、次回以後のリスクアセスメント作業に向けた対応方針の策定に係る計画を含みます。

（２）モニタリングの実施

リスクオーナーは、モニタリング実施計画に基づき、モニタリングを実施します。モニタリングについては、リスク評価により特定されたリスク（リスク対応の実施対象とするリスク）に係るリスク対応のフォローアップに限らず、当該リスクの評価に至る一連の取組において洗い出された事項の全て（各リスクアセスメントシートに書き出された事項の全て）を対象として実施することを基本とします。

なお、モニタリングの実施に際しては、次に掲げる観点を踏まえることを推奨します。

・リスクアセスメントを実施した際に前提としていた外部環境の変化に起因する状態の変動。なお、技術的な環境の変化だけでなく、経済的、政治・法律的及び社会的な環境の変化についても考慮することが必要です。

・リスクアセスメントを実施した際に前提としていた内部環境の変化に起因する状態の変動。とりわけ、事業者等の活動目標、リスクアセスメントの実施目的、サービスの経営上の位置付け（業績への寄与度や事業上の依存度等の事業経営上の位置付け）、利害関係者（顧客、仕入先、株主、地域社会等）からのニーズ・期待等の変化を考慮することが重要です。

（３）モニタリング結果の反映方針の策定

モニタリングの結果を踏まえ、次回以後のリスクアセスメント作業に向けた対応方針を策定します。

＜参考＞リスクマネジメントの取組に対する内部監査

リスクアセスメントのプロセスを含む、リスクマネジメント全体の取組に対する継続的な見直しの取組として、第三者の視点による内部監査を行うことが有効です。

リスクマネジメントとはリスクの組織的な管理のプロセスであり、リスクアセスメントの結果からリスク対応を計画し、リスク低減策として管理策を設計し、PDCA サイクルに沿ってその実行管理を行うという一連の取組を指します（１．＜２＞の図表１参照）。

内部監査は、リスクマネジメントの PDCA サイクルの C（評価）において行われる取組であり、リスクマネジメントの PDCA が適切に運営されていること、及び各管理策が有効に運用されていることの確認を行うことを目的に実施されます。（PDCA サイクルの詳細は指針を参照）

一般的に内部監査は、以下のようなプロセスに沿って行われます。

１．事前準備
（監査目的、監査範囲、監査基準の明確化等）

２．監査活動の実施
（面談、観察、文書レビュー等を通じた、監査項目の評価）

３．監査報告書の作成
（監査基準に照らした監査所見、及び是正や改善の提言を含む監査結論の記載）

４．監査のフォローアップ
（是正処置、改善処置の完了及び有効性についての検証）

内部監査では、環境変化等によるリスクの変動に適切に対処できているかといった観点からリスクマネジメント全体の取組の確認を行い、是正、改善が必要な項目を指摘し、どのような処置をいつまでに行うかについて合意を行うとともに、それらが計画どおり実行されているかの検証を行います。

なお、リスクマネジメントの取組に対する内部監査に当たっては、機能保証の考え方を踏まえリスクに適切に対処できているかという視点から、以下のような観点を考慮することを推奨します。

・リスクアセスメントの妥当性や品質の確認が、パフォーマンス評価等により適切に行われていること。

・リスクアセスメントの結果として実施する各リスク対応が、各々のリスクを許容可能な水準に抑えられる妥当な内容となっており、適切に実装・運用されていること。（対応不要と判断したリスクの妥当性確認を含む）

・リスクアセスメントを実施した際に前提としていた外部環境・内部環境の変化に起因する状態の変動をモニタリングし、必要に応じてリスクアセスメント結果やリスク対応の見直しが適切に実施されていること。

・情報セキュリティに関する新しい脅威や脆弱性、情報セキュリティに係る重大な事案の動向や情報セキュリティ上のリスクを高める社会の動向等を踏まえ、考慮が漏れているリスクや過小評価されているリスクがないこと。

・リスクアセスメントが定期的かつ計画的に行われ、リスクの変動に適切に対処する態勢が整っていること。

付録Ａ．用語の説明

用語	説明
イベントツリー分析	所与の単一の原因から生じる複数の潜在的な結果を分析する手法。ある初期事象からスタートして、いろいろな経路をとることにより結果がどうなるかを明らかにするもの。
経営層	最高位で組織を指揮し、管理する個人又は人々の集まり。 （会社の場合には、業務を執行する取締役、執行役等の機関及びこれらに準じる重要な使用人（執行役員等の役職に就いている者）などが該当する。）
固有リスク	リスク対応を講じる前又は講じていないと想定した状態における本来有するリスク。
最大許容停止時間	製品・サービスを提供しない、又は事業活動を行わない結果として生じる可能性のある悪影響が、許容不能な状態になるまでの時間。
サプライチェーン	組織の壁を越えたサービス提供に関わる一連の活動又は関係者。
残留リスク	リスク対応後に残るリスク。
事象	ある一連の周辺状況の出現又は変化。
事象の結果	目的に影響を与える事象の結末。
重要インフラ事業者等	提供するサービスが停止又はその品質が低下した場合に、我が国の国民生活又は社会経済活動に多大な影響を及ぼす可能性のある事業者等。
詳細リスク分析	資産ごとに関連するリスクの解析を実施するリスク分析のアプローチ。
バリュー・チェーン	サービスの提供に関係する事業活動を機能単位に分割して捉え、その役割と流れに沿って体系化するもの。
フォールトツリー分析	望ましくない結果をもたらす原因をトップダウンで体系的に探究する手法。事象の結果の発生原因、潜在的に発生の可能性がある原因又は発生の要因を抽出し、事象の結果の発生条件及び要因の識別及び解析を行うもの。
優先サービス障害	情報、情報システム、制御システム等が期待通りの機能を発揮しない又は発揮できない状態となる事象のうち、優先サービスの提供水準が最低限維持されるべき水準を下回る事象。
利害関係者	ある決定事項又は活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している個人又は組織。
リスクアセスメント	リスク特定、リスク分析及びリスク評価のプロセス全体。
リスク許容度	自らの目的を達成するため、組織又はステークホルダーが負う準備ができている残留リスクの程度。
リスク源	それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素。 なお、リスク源は、有形の場合も無形の場合もある。
リスクに対する態度	リスクのアセスメントを行い、最終的にリスクを保有する、取る又は避ける、という組織の取組み。
リスク対応	リスクを修正するプロセス。 リスク対応には、リスクを修正するために一つ以上の選択肢を選び出すこと及びそれらの選択肢を実践することが含まれる。リスク対応は本書の対象ではないが、リスクアセスメントに続くプロセスとしてリスク対応の選択肢の同定について、P29 に参考情報を記載している。
リスク特定	リスクを発見、認識及び記述するプロセス。 なお、リスク特定には、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれます。
リスク評価	リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。
リスク分析	リスクの特質を理解し、リスクレベルを決定するプロセス。 なお、リスク分析は、リスク評価及びリスク対応に関する意思決定の基礎を提供する。
リスクレベル	事象の結果の影響度とその起こりやすさ（発生頻度）との組合せとして表わされるリスク又は組み合わさったリスクの大きさ。 なお、リスクレベルを定量化（数値化）した評価をリスク値といいます。

付録Ｂ．参考文献

[1] JIS Q 31000:2010, リスクマネジメント－原則及び指針.
（注）対応国際規格：ISO 31000:2009, Risk management－Principles and guidelines.

[2] JIS Q 31010:2012, リスクマネジメント－リスクアセスメント技法.
（注）対応国際規格：IEC/ISO 31010:2009, Risk management－Risk assessment techniques.

[3] JIS Q 0073:2010, リスクマネジメント－用語.
（注）対応国際規格：ISO Guide73 2009, Risk management－Vocabulary.

[4] ISO/IEC 27005:2011, Information technology－Security techniques－Information security risk management.

[5] 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
（注）対応国際規格：ISO 22301:2012, Societal security－Business continuity management systems－Requirements.

[6] JIS Q 19011:2012, マネジメントシステム監査のための指針.
（注）対応国際規格：ISO 19011:2011, Guidelines for auditing management systems.

[7] 勝俣良介著（2012）『ISO22301 徹底解説―BCP・BCMS の構築・運用から認証取得まで―』ニュートン・コンサルティング監修, オーム社.

[8] リスクマネジメント規格活用検討会編著（2014）『ISO 31000:2009 リスクマネジメント 解説と適用ガイド』日本規格協会.

[9] 佐藤学・羽田卓郎・中川将征著（2013）『ISO 22301 で構築する事業継続マネジメントシステム』日科技連出版社.

[10] 畠中伸敏編著（2008）『情報セキュリティのためのリスク分析・評価 第２版―官公庁・金融機関・一般企業におけるリスク分析・評価の実践―』日科技連出版社.

[11] 内閣官房内閣サイバーセキュリティセンター(2015)『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）』，＜http://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf＞

[12] 内閣官房内閣サイバーセキュリティセンター(2017)『情報セキュリティ監査実施手順の策定手引書』，＜http://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf＞

別紙１　業務の阻害につながる事象の結果の例

経営資源(情報資産)の例		業務の阻害につながる事象の結果の例	可用性	完全性	機密性	事象発生による影響の例	
運輸	運行管理・電力管理システム	システム・装置が停止する。	✓			- 交通機関の運行が停止し、旅客等の移動に影響を及ぼす。 - 物流機能が停止し、貨物等の輸送に影響を及ぼす。 - 安全な運行に支障が生じた場合には、人命にも影響を及ぼす。	左記の結果事象やその影響により、レピュテーション（社会的評価）が低下する。
		運行制御の機能が喪失する。	✓	✓			
		中央管理表示の機能が喪失する。	✓	✓			
		異常な運行情報が表示される。		✓			
		ダイヤ選択に誤りが生じる。	✓	✓			
		設定データが喪失する。	✓	✓			
		設定データに誤ったデータが記録される。		✓			
		設定データから誤ったデータが応答される。		✓			
		設定データが社外に流出する。			✓		
	予約(荷受)データベース	システム・装置が停止する。	✓			- 予約業務が停止し、旅客等の移動に影響を及ぼす。 - 荷受業務が停止し、貨物等の輸送に影響を及ぼす。	
		データベース上のデータが喪失する。	✓	✓			
		データベースの応答が滞る。	✓				
		データベースに誤ったデータが記録される。		✓			
		データベースから誤ったデータが応答される。		✓			
		データベース上の情報が社外に流出する。			✓		
電力・ガス・水道	制御システム	システム・装置が停止する。	✓			- インフラが停止し、国民生活や事業活動等に影響を及ぼす。 - 交通機関等へのインフラ供給が停止し、旅客の移動や貨物の輸送等に影響を及ぼす。 - 安全な運用に支障が生じた場合には、人命にも影響を及ぼす。	
		プラント制御の機能が喪失する。	✓	✓			
		供給制御の機能が喪失する。	✓	✓			
		遮断機能が喪失する。	✓	✓			
		モニター機能が喪失する。	✓	✓			
		パラメーターが喪失する。	✓	✓			
		誤ったパラメーターが記録される。		✓			
		パラメーターが社外に流出する。			✓		
情報通信	営放システム	システム・装置が停止する。	✓			- コンテンツ・情報の配信が停止し、放送や広告に関わる事業活動等に影響を及ぼす。	
		送出制御機能が喪失する。	✓	✓			
		伝送制御機能が喪失する。	✓	✓			
		放送素材(コンテンツ)が喪失する。	✓	✓			
		事実とは違う情報が入力される。		✓			
	基地局・回線データベース	システム・装置が停止する。	✓			- 広範に通信障害が発生し、通信を伴う消費活動や事業活動等に影響を及ぼす。	
		データベース上のデータが喪失する。	✓	✓			
		データベースの応答が滞る。	✓				
		データベースに誤ったデータが記録される。		✓			
		データベースから誤ったデータが応答される。		✓			
		データベース上の情報が社外に流出する。			✓		
金融	勘定系システム	システム・装置が停止する。	✓			- 入出金業務が停止し、国民の消費活動や事業者の資金繰り等に影響を及ぼす。	
		勘定系データが喪失する。	✓	✓			
		センターでの応答が滞る。	✓				
		誤ったデータが記録される。		✓			
		データが社外に流出する。			✓		
	オーソリシステム	システム・装置が停止する。	✓			- 決済業務が停止し、国民の消費活動等に影響を及ぼす。	
		オーソリ電文が喪失する。	✓	✓			
		オーソリ電文の照合が不可能になる。	✓				
		オーソリの応答が遅延する。	✓				
		オーソリ電文が毀損する。		✓			
		オーソリ電文の誤照合が発生する。		✓			
		オーソリ電文が漏えいする。			✓		
行政サービス	住民情報システム	システム・装置が停止する。	✓			- 窓口業務が停止し、住民サービスの提供に影響を及ぼす。	
		住民データが喪失する。	✓	✓			
		証明書発行機能が喪失する。	✓				
		誤ったデータが記録される。		✓			
		誤ったデータが表示される。		✓			
		住民データが漏えいする。			✓		

【参考】業務維持のために経営資源に求められる観点

観点	考え方
可用性	許可された利用者が、必要な時に経営資源を利用できること。
完全性	経営資源及び経営資源に含まれる情報に誤りがなく(正確であり)、欠損や不整合がないこと(完全であること)。
機密性	正当な権限をもつ限られた者のみが、経営資源及び経営資源に含まれる情報を利用できること。

別紙２　結果を生じ得る事象(脅威)の例

結果を生じ得る事象(脅威)			具体例
攻撃に起因する脅威	外部不正	標的型攻撃	アクセス権限のないポート、プロトコル、およびサービスを使用して、攻撃を実施する。
			ネットワーク境界を越えて許可されているトラフィック／データの移動を利用して、攻撃を実施する。
			重要な地位にいる職員の私有のデバイスを狙って侵害する攻撃を実施する。
			基幹業務に関わるハードウェア、ソフトウェア、ファームウェアを狙い、サプライチェーン攻撃を実施する。
		マルウェア	メールの添付ファイルからマルウェアを感染させる。
			ウェブサイトからマルウェアを感染させる。
			エクスプロイトキットを使って、ランサムウェアを拡散させる。
		情報窃取	SQLインジェクション等の情報漏えいにつながる脆弱性を悪用し、機微な情報を取得する。
			OSコマンドインジェクション等のソフトウェアの脆弱性を悪用し、機微な情報を取得する。
			外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する。
		サービス妨害攻撃	シンプルなサービス妨害(DoS)攻撃を実施する。
			分散型サービス妨害攻撃を実施する。
			標的型サービス妨害攻撃を実施する。
		ウェブサイト改ざん	開発時に作りこんだウェブアプリケーションの脆弱性を悪用して、サイトを改ざんする。
			ソフトウェアの脆弱性を悪用して、サイトを改ざんする。
			管理用サービスに侵入して、サイトを改ざんする。
		ウェブサービスへの不正ログイン	他のウェブサイトから漏えいしたIDとパスワードの組み合わせを利用して攻撃する。
			総当たりのログイン試行／パスワード推測攻撃を実施する。
		脆弱性を標的にした攻撃	公開された脆弱性情報を悪用して、対策をしていない利用者を攻撃する。
			パッチなどの修正手段が提供されていない脆弱性を狙って、非標的型ゼロデイ攻撃を実施する。
			IoT機器の脆弱性を悪用してウイルスを感染させる。
		金融情報の不正利用	インターネットバンキング詐欺ツールによって金融取引関連情報を窃取する。
			フィッシング詐欺をする。
		通信の盗聴・妨害	通信傍受攻撃を実施する。
			無線妨害攻撃を実施する。
			外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受する。
		データの改ざん	極めて重要なデータを汚染する、あるいは改ざんする。
			公的にアクセス可能な情報システム上にデータを作成・削除・変更する。
			もっともらしいが偽のデータを組織の情報システムに挿入する。
		ソーシャルエンジニアリング	不在時に他人の机の上にある資料やノートをのぞき見して、機密情報などを収集する。
			ゴミ箱をあさり、不用意に廃棄された資料やメモなどを収集し、目的の情報を取得する。
			機会をうかがって情報システム／コンポーネントを盗んだり、あさる。
		システム破壊	システムを破壊するマルウェアを不正にインストールする。
	内部不正	不正利用	データを不正に操作する。
			機密情報を不正に閲覧する。
			機微な情報を不正に取得する。
		不正持ち出し	機密情報を不正に持ち出す。
			データを意図的に外部に送信する。
		乗っ取り	内部の攻撃者が正規ユーザになりすましてウェブアプリケーションを操作し、セッションの乗っ取りを実施する。
			内部の攻撃者がネットワークトラフィックに侵入して、変更攻撃を実施する。
攻撃に起因しない脅威	自然現象	自然災害	地震が発生する。
			台風が発生する。
			温度・湿度異常が発生する。
			落雷が発生する。
			浸水が発生する。
		エネルギー不足	停電が発生する。
			水不足が発生する。
	障害	設備障害	火災が発生する。
			漏水が発生する。
			動植物害が発生する。
			施設が老朽化する。
			ビル付帯設備(空調機器、入退室管理装置、監視カメラ等)が故障する。
		ハードウェア障害	メモリ、ディスク、CPU、電源装置の障害が発生する。
			ディスクのエラーが発生する。
			機器・ケーブルが劣化する。
		ソフトウェア障害	OSやアプリケーションの潜在的なバグ・過負荷等による異常が発生する。
			資源(メモリやディスクの容量オーバー等)の枯渇により、処理性能が低下する。
		ネットワーク障害	通信の競合により、通信性能が低下する。
			回線(専用・公衆)、通信事業者(接続局、ISP、NOC、IDC等)、通信機器、構内配線の障害が発生する。
	人に起因する脅威	操作ミス	特権ユーザが、極めて重要な情報／機微な情報を誤って露出させる。
			特権ユーザが、他のユーザに例外的な権限を誤って付与する。
			メールを誤送信する／不要なメールを開封する／重要データを消去する。
		遺失・紛失	持ち出し媒体を置き忘れる／管理不備によって媒体を紛失する。
		不適切な廃棄	廃棄した媒体を復元する。
		無許可機器の持込	許可されていない機器、媒体、プログラムを社内ネットワークに接続する。
		無意図な情報公開	ウェブサーバの設定不備により重要データが流出する。
		任務怠慢	既定の操作の実行を忘れる。
		法令・政策の不認識	海外サーバにおいてデータ保管・処理等を行う場合において、認識していない当該地域の法令等による権限が行使される。

別紙3　様式1

STEP1：リスクアセスメントの実施目的の確認

優先サービスの機能保証	（1）重要インフラ事業者等としての自組織の活動目標（左記の観点を踏まえて設定）	情報セキュリティ・リスクに係るリスクアセスメントの実施目的・方針
国民生活及び社会経済活動を支える優先サービスを安全（＝許容できないリスクが無い状態）かつ持続的に提供するための取組。		（リスクアセスメント実施目的） 左記活動目標に対する情報セキュリティ・リスクに対し、適切にリスク対応を行うために、当該リスクを特定、分析及び評価し、並びに残留リスクを可視化することをリスクアセスメントの実施目的とする。 （リスクアセスメント実施方針） 前記実施目的を達成するため、リスクアセスメントの対象とすべきサービス及びそのサービスに求められる要求事項、安全の観点を踏まえ最低限許容されるサービスの水準及び停止時間を明らかにした上、必要な業務・経営資源を特定し、優先サービス障害に関するリスクを特定、分析及び評価する。 なお、具体的な手順は、次のとおり。 ① 活動目標に係るサービスを優先サービス（リスクアセスメントの対象とすべきサービス）として選定する。 ② サービスに求められる要求事項（社会的責任、契約責任、法規等）及び安全の観点を踏まえ最低限許容される優先サービスの範囲・水準を明らかにした上、優先サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を推定する。 ③ 優先サービスの提供に必要な業務を洗い出し、当該業務について最低限許容される水準を分析した上、当該業務が完全に停止した場合の影響及び時間経過に伴う影響度合いを評価し、業務の最大許容停止時間を推定する。 ④ 優先サービスに必要な業務について、事態発生時に最低限満たすべき業務水準を維持するために必な経営資源を洗い出し、その経営資源が満たすべき要件・必要数量について把握する。 ⑤ 優先サービスの提供に必要な業務に係る経営資源を整理した上、当該業務の継続を目的とした場合の当該経営資源に係るリスクを特定、分析及び評価を行う。

別紙3　様式1（記載例）

STEP1：リスクアセスメントの実施目的の確認

優先サービスの機能保証	（1）重要インフラ事業者等としての自組織の活動目標（左記の観点を踏まえて設定）
国民生活及び社会経済活動を支える優先サービスを安全（＝許容できないリスクが無い状態）かつ持続的に提供するための取組。	○○サービスを安全に、かつ安定して提供し続ける。

情報セキュリティ・リスクに係るリスクアセスメントの実施目的・方針
（リスクアセスメント実施目的） 左記活動目標に対する情報セキュリティ・リスクに対し、適切にリスク対応を行うために、当該リスクを特定、分析及び評価し、並びに残留リスクを可視化することをリスクアセスメントの実施目的とする。 （リスクアセスメント実施方針） 前記実施目的を達成するため、リスクアセスメントの対象とすべきサービス及びそのサービスに求められる要求事項、安全の観点を踏まえ最低限許容されるサービスの水準及び停止時間を明らかにした上、必要な業務・経営資源を特定し、優先サービス障害に関するリスクを特定、分析及び評価する。 なお、具体的な手順は、次のとおり。 ① 活動目標に係るサービスを優先サービス（リスクアセスメントの対象とすべきサービス）として選定する。 ② サービスに求められる要求事項（社会的責任、契約責任、法規等）及び安全の観点を踏まえ最低限許容される優先サービスの範囲・水準を明らかにした上、優先サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を推定する。 ③ 優先サービスの提供に必要な業務を洗い出し、当該業務について最低限許容される水準を分析した上、当該業務が完全に停止した場合の影響及び時間経過に伴う影響度合いを評価し、業務の最大許容停止時間を推定する。 ④ 優先サービスに必要な業務について、事態発生時に最低限満たすべき業務水準を維持するために必な経営資源を洗い出し、その経営資源が満たすべき要件・必要数量について把握する。 ⑤ 優先サービスの提供に必要な業務に係る経営資源を整理した上、当該業務の継続を目的とした場合の当該経営資源に係るリスクを特定、分析及び評価を行う。

別紙3 様式2

STEP2：利害関係者のニーズ・期待、社会的責任（ＣＳＲ）、契約責任、法制面の要求等を分析した上、優先サービスを選定する。

（1）事業	（2）サービス	（3）サービスに関する利害関係者のニーズ・期待／法制面での要求事項の分析		（4）製品・サービスの経営面での位置づけ				（5）分析を踏まえた優先サービスの選定（優先サービスの決定）	
		契約責任、法令遵守	その他の社会的責任（CSR）	業績面		戦略面		優先度	コメント
				売上	ROI	市場成長性	相対市場シェア		

別紙3　様式2（記載例）

STEP2：利害関係者のニーズ・期待、社会的責任（ＣＳＲ）、契約責任、法制面の要求等を分析した上、優先サービスを選定する。

（1）事業	（2）サービス	（3）サービスに関する利害関係者のニーズ・期待／法制面での要求事項の分析		（4）製品・サービスの経営面での位置づけ				（5）分析を踏まえた優先サービスの選定（優先サービスの決定）	
		契約責任、法令遵守	その他の社会的責任（CSR）	業績面		戦略面		優先度	コメント
				売上	ROI	市場成長性	相対市場シェア		
○○事業	○○サービス	国民生活を支える重要なサービスであり、安定したサービス提供が必要である。 ○×事業法：○○の役務を提供する事業者はその安定的な提供に努めなければならない。	高品質な○○サービスを提供し、グローバル社会の発展に貢献する。	XXX億円/年	XX%	低	XX%	A	事業規模や利害関係者のニーズ・期待等を総合的に勘案した結果、リスクアセスメントを行うべき重要サービスであると判断する。
	××サービス	国民の社会経済活動を支える重要なサービスであり、安全かつ安定したサービス提供が必要である。 ○×事業法：××の役務を提供する事業者はその適切かつ安定的な提供に努めなければならない。	安全かつ高品質な○○サービスを、可能な限り環境負荷を最小化して提供する。	XX億円/年	○○%	低	○○%	B	事業規模や利害関係者のニーズ・期待等を踏まえ、リスク評価を行うべきサービスではあるが、代替措置も考えられるため、優先度は下げる（今回のアセスメント対象からは除外する。）。
△△事業	□□サービス	△△事業の中核となる重要なサービスであり、安全かつ安定したサービス提供が必要である。 ○×規則：△△事業者は、安全かつ確実に□□サービスを遂行するように努めなければならない。	地域社会とともに持続的に発展していくため、□□サービスを提供する	XX億円/年	○X%	中	○X%	A	事業規模や利害関係者のニーズ・期待等を総合的に勘案した結果、リスクアセスメントを行うべき重要サービスであると判断する。

別紙3　様式3

STEP3：安全（＝許容できないリスクが無い状態）の観点を踏まえ最低限許容されるサービスの範囲・水準を明らかにした上、サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定する。

（1）事業	（2）サービス	(3)利害関係者のニーズ・期待／法制面での要求事項等を満たすために安全の観点を踏まえ最低限許容されるサービスの範囲・水準		(4)サービスの提供が完全停止した場合の影響								（5）サービスの提供に係る最大許容停止時間(MTPD)	
		契約責任、法令遵守	社会的責任（CSR）	最低限許容されるサービスの範囲・水準が満たされない場合に生じる事態	時間経過に伴う影響度合いの評価							MTPD	コメント
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	

<凡例>
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない
×（影響あり）　：活動目的の阻害につながる影響がある

別紙3　様式3（記載例）

STEP3：安全（＝許容できないリスクが無い状態）の観点を踏まえ最低限許容されるサービスの範囲・水準を明らかにした上、サービスの提供が停止した場合の時間経過に伴う影響を分析し、最大許容停止時間を決定する。

（1）事業	（2）サービス	(3)利害関係者のニーズ・期待／法制面での要求事項等を満たすために安全の観点を踏まえ最低限許容されるサービスの範囲・水準		(4)サービスの提供が完全停止した場合の影響								(5）サービスの提供に係る最大許容停止時間(MTPD)	
		契約責任、法令遵守	社会的責任（CSR）	最低限許容されるサービスの範囲・水準が満たされない場合に生じる事態	時間経過に伴う影響度合いの評価							MTPD	コメント
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	
○○事業	○○サービス	国民生活を支える重要なサービスであり、安定したサービス提供が必要である。 ○×事業法：○○の役務の停止・品質の低下が、○人以上の利用者に×時間以上継続する事故が発生した場合は、報告を要する。	契約時に利用者との間で合意した品質基準でサービスを安定的にを提供するとともに、障害が発生した場合には迅速に復旧する。	契約者のサービス利用が停止し、○○サービスを活用した国民生活及び社会活動等が停止する。	－	×	×	×	×	×	×	×	30分	サービスのSLAに則り、30分以上継続するサービス停止・品質低下を生じさせないことを基準とした。
△△事業	□□サービス	△△事業の中核となる重要なサービスであり、安定したサービス提供が必要である。 ○×規則：サービス停止に繋がる事故が発生した場合の報告規則を定める。	利用者の安全を確保しつつ、安定した□□サービスを提供する。	□□サービスを利用した事業活動や社会経済活動が一時的に停止する。	－	－	×	×	×	×	×	×	1時間	○×規則に則り、報告対象障害となる1時間以上のサービス停止を生じさせないことを基準とした。

＜凡例＞
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない
×（影響あり）　：活動目的の阻害につながる影響がある

別紙3 様式4

STEP4：優先サービスの提供に必要な業務を洗い出し、当該業務について許容される最低限の水準（操業率、稼働率等）を決定する。また、当該業務が停止した場合の影響及び停止に係る最大許容時間を決定する。

（1）事業	（2）優先サービス	（3）優先サービスの提供に必要な業務（優先サービスを構成する業務）	（4）優先サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）	(5)業務が完全停止した場合に優先サービスの提供に及ぼす影響								（6）業務に係る最大許容停止時間(MTPD)	
				業務が完全停止した場合に生じる事態	時間経過に伴う影響度合いの評価								
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント

<凡例>
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない
×（影響あり）　：活動目的の阻害につながる影響がある

別紙3　様式4（記載例）

STEP4：優先サービスの提供に必要な業務を洗い出し、当該業務について許容される最低限の水準（操業率、稼働率等）を決定する。また、当該業務が停止した場合の影響及び停止に係る最大許容時間を決定する。

（1）事業	（2）優先サービス	（3）優先サービスの提供に必要な業務（優先サービスを構成する業務）	（4）優先サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）	(5)業務が完全停止した場合に優先サービスの提供に及ぼす影響								（6）業務に係る最大許容停止時間(MTPD)	
				業務が完全停止した場合に生じる事態	時間経過に伴う影響度合いの評価								
					瞬時	1時間	6時間	半日	1日	1週間	2週間	1か月	MTPD	コメント
○○事業	○○サービス	契約締結・変更受付業務	本業務が停止しても、即座に大きな影響は生じない。ただし長期間業務が滞った場合、事業およびレピュテーション等に大きな影響を与える。	契約の新規申し込み、変更、廃止対応ができなくなる。	－	－	－	－	－	×	×	×	1週間	レピュテーションへの影響も考慮し、１週間以上の停止は許容できないと判断した。
		契約管理業務	本業務が停止しても、即座に大きな影響は生じない。ただし長期間業務が滞った場合、事業およびレピュテーション等に大きな影響を与える。	契約の新規申し込み、変更、廃止対応ができなくなる。	－	－	－	－	－	×	×	×	1週間	レピュテーションへの影響も考慮し、１週間以上の停止は許容できないと判断した。
		故障対応業務	サービスを提供する機器に故障が発生した場合の復旧を迅速に行うために、通常人員の○%程度の要員確保が必要である。	故障の復旧対応ができなくなる。	－	×	×	×	×	×	×	×	30分	影響の大きい障害が発生した場合に、即座に対応が必要となるため。
△△事業	□□サービス	システム運用管理業務	サービス供給の停止を避けるため、△人程度の要員確保が必要である。	安定したサービス供給が停止する。	－	－	－	－	×	×	×	×	1日	人によるオペレーションが途切れた状態で安定稼働できるのは1日が限界と判断した。
		保安業務	保安システムの維持管理を含む保安業務を機能させるには○人程度の要員確保が必要である。	保安業務が適時適切に実施できなくなる。	－	×	×	×	×	×	×	×	1時間	必要な保安業務が適時適切に行われない場合、人命や環境に大きな影響を与える恐れがあるため。

<凡例>
－（影響なし）　：影響度合いが小さく、活動目的の阻害につながらない
△（影響不明）　：活動目的の阻害につながる影響があるかどうかわからない
×（影響あり）　：活動目的の阻害につながる影響がある

STEP5:優先サービスの提供について、最低許容水準を満たすために必要な業務及び資源の洗出し

(1)事業	(2)優先サービス	(3) 優先サービスの提供に必要な業務 （優先サービスを構成する業務）	(4)前提とする業務水準（許容できる最低稼働率等） ※Step4の（4）優先サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）を転記	(5)業務を支える経営資源の要件・必要数量							
				人	情報、データ	建物、作業環境、 関連ユーティリティ	設備・機器・消耗品	情報通信技術(ICT)システム 、制御システム	交通機関、ライフライン（例： 電気、水、ガス）	資金	その他 （例：取引先、サプライヤ）

別紙3　様式5（記載例）

STEP5:優先サービスの提供について、最低許容水準を満たすために必要な業務及び資源の洗出し

(1)事業	(2)優先サービス	(3) 優先サービスの提供に必要な業務 （優先サービスを構成する業務）	(4)前提とする業務水準（許容できる最低稼働率等） ※Step4の（4）優先サービスの最低許容範囲・水準を満たすために必要な業務の最低水準（操業率・稼働率等）を転記	(5)業務を支える経営資源の要件・必要数量							
				人	情報、データ	建物、作業環境、 関連ユーティリティ	設備・機器・消耗品	情報通信技術(ICT)システム 、制御システム	交通機関、ライフライン（例： 電気、水、ガス）	資金	その他 （例：取引先、サプライヤ）
○○事業	○○サービス	契約締結・変更受付業務	本業務が停止しても、即座に大きな影響は生じない。ただし長期間業務が滞った場合、事業およびレピュテーション等に大きな影響を与える。	受付業務　約○○人	契約情報 顧客情報	コールセンター	メール/PC 電話/FAX	契約管理システム 顧客管理システム	電話回線 電気	－	販売代理店○○
		契約管理業務	本業務が停止しても、即座に大きな影響は生じない。ただし長期間業務が滞った場合、事業およびレピュテーション等に大きな影響を与える。	管理業務　約○○人	契約情報 顧客情報	サービスセンター	メール/PC 電話/FAX	契約管理システム 顧客管理システム	電話回線 電気	－	－
		故障対応業務	サービスを提供する機器に故障が発生した場合の復旧を迅速に行うために、通常人員の○%程度の要員確保が必要である。	故障対応要員　約○○人	故障対応業者一覧	データセンター	交換用予備機	故障受付システム	電話回線 電気	－	故障対応業者△△
△△事業	□□サービス	システム運用管理業務	サービス供給の停止を避けるため、△人程度の要員確保が必要である。	システム運用管理業務 約△人	機器・端末情報	サービス供給施設	機器　約○台 端末　約△台	供給制御システム 情報システム	電気	－	－
		保安業務	保安システムの維持管理を含む保安業務を機能させるには○人程度の要員確保が必要である。	保安業務　約○人	作業管理データ 社員管理データ	事務所	端末　約○台	緊急保安システム	電気 水	－	－

STEP6:優先サービスの提供に必要な業務に係る経営資源を整理した上、当該経営資源に係るリスクを特定、分析及び評価します。

(1)事業	(2)優先サービス	(3)優先サービスの提供に必要な業務	(4)リスクの特定					(5)リスクの分析								(6)リスクの評価		
			経営資源		業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	事象の結果の影響度合い				事象の発生頻度			残留リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部署）
								事象の結果の影響	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後				

別紙3　様式6（記載例）

STEP6:優先サービスの提供に必要な業務に係る経営資源を整理した上、当該経営資源に係るリスクを特定、分析及び評価します。

(1)事業	(2)優先サービス	(3)優先サービスの提供に必要な業務	(4)リスクの特定					(5)リスクの分析								(6)リスクの評価		
			経営資源		業務の阻害につながる事象の結果	結果を生じ得る事象	リスク源	事象の結果の影響度合い				事象の発生頻度			残留リスク値	リスク基準	リスク評価	リスクオーナーの選任（部門・部署）
								事象の結果の影響	対策前	現在講じている対策	対策後	対策前	現在講じている対策	対策後				
○○事業	○○サービス	契約締結・変更受付業務	情報・データ	契約DB	契約情報の流出	内部犯行による不正持ち出し	情報を持ち出せる環境（記憶媒体）	業務停止に直結するものではないが、調査や説明対応に追われることにより、通常業務の遂行を大きく阻害する。	3	記憶媒体へコピーできるデータ容量の制限	2	3	記憶媒体のアクセス制限	2	4	5	－	
							社内セキュリティ教育が不十分		3	特になし	3	2	定期的な社内研修	1	3	5	－	
							書類の放置		2	特になし	2	2	ペーパーレスへの移行	1	2	5	－	
					契約情報の改ざん	マルウェア	外部媒体が接続できる環境	改ざんデータの調査や修正のため、契約の申し込み・変更・廃止の受付に係る業務が一時的に停止する。	4	プログラムの不正動作を検知するシステムの導入 ロールバックによる復元手段/手順の整備	2	3	記憶媒体からデータコピーする際のウイルスチェック機能	2	4	5	－	
						内部不正	アクセス権限の管理未徹底		4	適切なアクセス制限の設定	3	3	定期的なアカウントの棚卸	2	6	5	●	○○部
					契約情報の消失	HDD故障	機器のリプレース未実施	消失した契約データの変更・廃止の受付に係る業務が一時的に停止する。	3	監視システムの導入 バックアップサーバに契約情報を保存	1	3	HDDの冗長化	1	1	5	－	
						電源故障	機器のリプレース未実施		3	特になし	3	2	特になし	2	6	5	●	○○部
							バックアップ電源の未設置		3	特になし	3	2	特になし	2	6	5	●	○○部
				顧客DB														
			情報通信技術システム	契約管理システム														
				顧客管理システム														
		契約管理業務																
		故障対応業務																
		⋮																
△△事業	□□サービス	システム運用管理業務	情報・データ	機器・端末データ	機器の制御パラメータ情報の流出	内部犯行による不正持ち出し	情報を持ち出せる環境 記憶媒体の使用が可能である	業務停止に直結するものではないが、調査や説明対応に追われることにより、通常業務の遂行を阻害する。	2	特になし	2	3	記憶媒体の使用制限	2	4	5	－	
						外部からの攻撃による不正流出	不正アクセスできる環境		2	特になし	2	3	クローズドネットワーク 保守作業用にアクセス可能なPCの制限	1	2	5	－	
					機器の制御パラメータの改ざん	保守作業による情報の書き換え	正規の媒体以外の記憶媒体を使用することが可能である	安定したサービス供給に多大な影響が生じる	5	正しいパラメータ情報を別サーバで保存	2	2	保守作業後の確認試験	1	2	5	－	
						内部犯行による情報の改ざん	改ざんできる環境がある	安定したサービス供給に多大な影響が生じる	5	正しいパラメータ情報を別サーバで保存	2	2	作業権限者を限定	1	2	5	－	
						外部からの攻撃による情報の改ざん	改ざんできる環境がある	安定したサービス供給に多大な影響が生じる	5	二重系システム	3	3	クローズドネットワーク 入退室管理の徹底	2	6	5	●	△△部
					機器の制御パラメータ情報の消失	保守作業の誤操作による情報の消去	誤操作できる環境がある	安定したサービス供給に多大な影響が生じる	5	正しい制御パラメータ情報を別サーバで保存	2	3	定期的な教育の実施 誤操作防止機能実装	1	2	5	－	
			制御システム	供給制御システム														
			情報通信技術システム	情報システム														
		保安業務																
		⋮																

別紙4 リスク源の例

分類		リスク源の例	該当する「結果を生じ得る事象(脅威)」の例
ハード	システム	システムのバグ放置 機器のリプレース未実施 メンテナンス不足 冗長化の不採用	ハードウェア障害、ソフトウェア障害、ネットワーク障害
		データバックアップの不備 非常用エネルギー設備の未設置	ハードウェア障害、ソフトウェア障害、ネットワーク障害、エネルギー不足、自然災害
		耐震化・耐水化の不備 バックアップサイトの未設置 設備のリプレース未実施	自然災害、設備障害
	セキュリティ	DoS対策の不備 (装置／設定)	サービス妨害攻撃
		不正検知システムの未導入・不備	標的型攻撃、マルウェア、サービス妨害攻撃、ウェブサービスへの不正ログイン
		防犯カメラの未設置	ソーシャルエンジニアリング
		保護されていない通信経路	通信の盗聴・妨害
ソフト	脆弱性対策	修正プログラムの未適用 既知の脆弱性の放置 サポート終了したソフトウェアの継続使用	情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	接続環境	USB、外部媒体が接続できる環境有	マルウェア、不正利用、不正持ち出し
		誰でもアクセスできる環境有 外部ネットワークへの接続環境有 インターネットへの接続環境有 周辺システムとの連携有 誤操作・意図的な操作ができる環境有 外部からの不正情報を受信できる環境有	標的型攻撃、マルウェア、情報窃取、サービス妨害攻撃、ウェブサイト改ざん、 ウェブサービスへの不正ログイン、データの改ざん、システム破壊、 不正利用、不正持ち出し、乗っ取り
		海外サーバにおけるデータ保管・処理有	法令・政策の不認識
	ルール	不要な人へのアクセス権限の付与 不要アカウントの放置 作業できるオペレーターのID管理不備 パスワード変更の放置	標的型攻撃、情報窃取、ウェブサイト改ざん、ウェブサービスへの不正ログイン、 不正利用、不正持ち出し、乗っ取り
		ネットワーク通信の暗号化不徹底	通信の盗聴・妨害
		廃棄承認ルールの未整備・不徹底	不適切な廃棄
		入退室管理の不備	不正利用、不正持ち出し、ソーシャルエンジニアリング
		機器や情報の不適切な保管 外部業者の本人確認の未徹底 施錠未実施	ソーシャルエンジニアリング
スキル・人材	組織共通	長時間労働	操作ミス、任務怠慢
		社内セキュリティ教育が不十分 セキュリティ意識の欠如	不正利用、不正持ち出し、操作ミス、遺失・紛失、無許可機器の持込、任務怠慢
		安易なパスワード設定 パスワードの使いまわし	ウェブサービスへの不正ログイン、金融情報の不正利用
		機密・重要書類の放置 不在時のPCログイン未設定	ソーシャルエンジニアリング
		不正アプリケーションのインストール 更新・保守作業時にウィルスチェックをしていない	マルウェア、情報窃取、ウェブサイト改ざん、脆弱性を標的にした攻撃
	セキュリティ部門	メンテナンス時の確認漏れ	マルウェア、システム破壊
		情報セキュリティ要員のスキル不足 セキュリティ要件を満たさないコーディング	脆弱性を標的にした攻撃、ウェブサイト改ざん、操作ミス、無意図な情報公開
		情報セキュリティ要員の要員不足 不十分なセキュリティ訓練	標的型攻撃、マルウェア、サービス妨害攻撃、脆弱性を標的にした攻撃