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）

～継続的改善における「効果的・合理的」な実現に向けて～

平 成 ２ ７ 年 ５ 月 ２ ５ 日

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

（本ページは白紙です。）

目次

（本ページは白紙です。）

Ⅰ．目的及び位置付け

1. 情報セキュリティ対策の実施及び改善に当たり

各重要インフラ事業者等における情報セキュリティ対策は、自助、共助、公助の順で対応すること、すなわち自分の身は自分で守ることを優先することが前提です。

このことから対策の実施に当たっては、自らの事業規模、予算、体制等を考慮して、対応できる対策を着実にかつ段階的に取り組んでいくことが重要です。

効果が見えにくい情報セキュリティ対策の取組に当たり、特に重要なのは、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）」（以下「指針本編」といいます。）にも記載があるとおり、以下の３点です。

●重要インフラ事業者等が自らの状況を正しく認識し、

●自らの情報セキュリティ対策の水準を規範等に照らした上で、

●PDCAサイクルに沿って適切かつ定期的に自らの情報セキュリティ対策を実施し改善する。

この３点のうち、適切な対策を実現するための要点は重要インフラ事業者等が自らの状況を正しく認識することであり、このためには以下の取組が必要です。

●防護すべき情報資産や情報システムが何かを定めた上で、その防護を揺るがす脅威や脆弱性等（リスク源[1]）の状況や動向を把握する。

●脅威や脆弱性等（リスク源）がもたらす可能性がある重要インフラ事業への損害（以下「発生する可能性がある損害（リスク[2]）」といいます。）はどの程度であり、重要インフラのサービスの持続的な提供にどの程度影響するのか、を予め認識する。

これらを通じて、適切な情報セキュリティ対策、すなわち発生する可能性がある損害（リスク）やその程度を受容できるレベルにまで下げることを実現していくことになります。

また、これらの取組については、経営層[3]を含めた全社的な体制で進めて行くことが前提となります。

---

[1] 「JIS Q 31000:2010」によれば、「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。」と定義されています。

[2] リスクとは目的に対する不確かさ（上ブレ、下ブレ）の影響を指します。ただし、情報セキュリティ対策においてはサービスの持続的な継続という目的に対して影響があるのは下ブレに限定されるため、指針手引書においては発生する可能性がある損害とします。なお、発生する可能性がある損害以外の意で使用する場合は、別途、脚注に記します。

[3] ここでいう経営層とは、経営者個人のみならず取締役会や委員会等といった会議体も含みます。

その際、情報セキュリティ対策[4]は各重要インフラ事業者等における事業継続を念頭においた全社的なリスクマネジメントの一部であることを踏まえた上で、リスクマネジメントと情報セキュリティ対策が整合する取組とすることが望まれます。

このことについては「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成26年５月19日情報セキュリティ政策会議決定。平成27年５月25日サイバーセキュリティ戦略本部改訂。以下「行動計画」といいます。）に重要インフラ事業者等の経営層の在り方が定められていますので、以下に引用します。

> 関係主体の在り方
>
> －自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
>
> －ＩＴ障害の規模に応じて、情報に基づく対応の 5W1H を理解しており、ＩＴ障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。
>
> 重要インフラ事業者等の経営層の在り方
>
> 経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。
>
> －上記の目的達成に当たっての情報セキュリティを中心とするリスク源の認識。
>
> －上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。
>
> －システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営資源の継続的な確保。
>
> －システムの運用状況の把握等を通じた当該方針の実行の有無の検証。
>
> －演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の検証及び改善策の有無の検証。

それぞれが置かれている状況が異なる各重要インフラ事業者等においては、自身にとって最も取り組みやすくかつ効果的な対応を自律的に行っていくことが望まれます。

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

2. 指針手引書の位置付け

指針は、以下の各書による構成となっています。

図表１　指針の構成

冊子（略称）	概要
指針本編	安全基準等の必要性やその中で規定することが望ましい項目を訴求
指針対策編[5]	指針本編に記載する情報セキュリティ対策項目の具体例を記載した項目集
指針手引書[6]	指針対策編Ⅱ.3「『Check(確認)・Act(是正)』の観点」における課題抽出、リスク特定及びリスク分析並びにⅡ.1.1.(1)「抽出した課題に基づくリスク評価」の対策項目についての解説や取組例を記載した手引書

指針手引書についてもう少し補足します。

指針手引書は、上記の解説や取組例を示すことで、各重要インフラ事業者等が自らの防護対策の有効性を高めていくことを支援するものです。

防護対策の有効性を高めていくためには、自らの組織に最も相応しい情報セキュリティ対策を構築し、維持・改善していくことが必要となります。

その構築・維持・改善に向けては、対策に優先順位を付けて、効果的かつ合理的に進めることが必要となります。

指針手引書は、このことの実現を支援するものです。

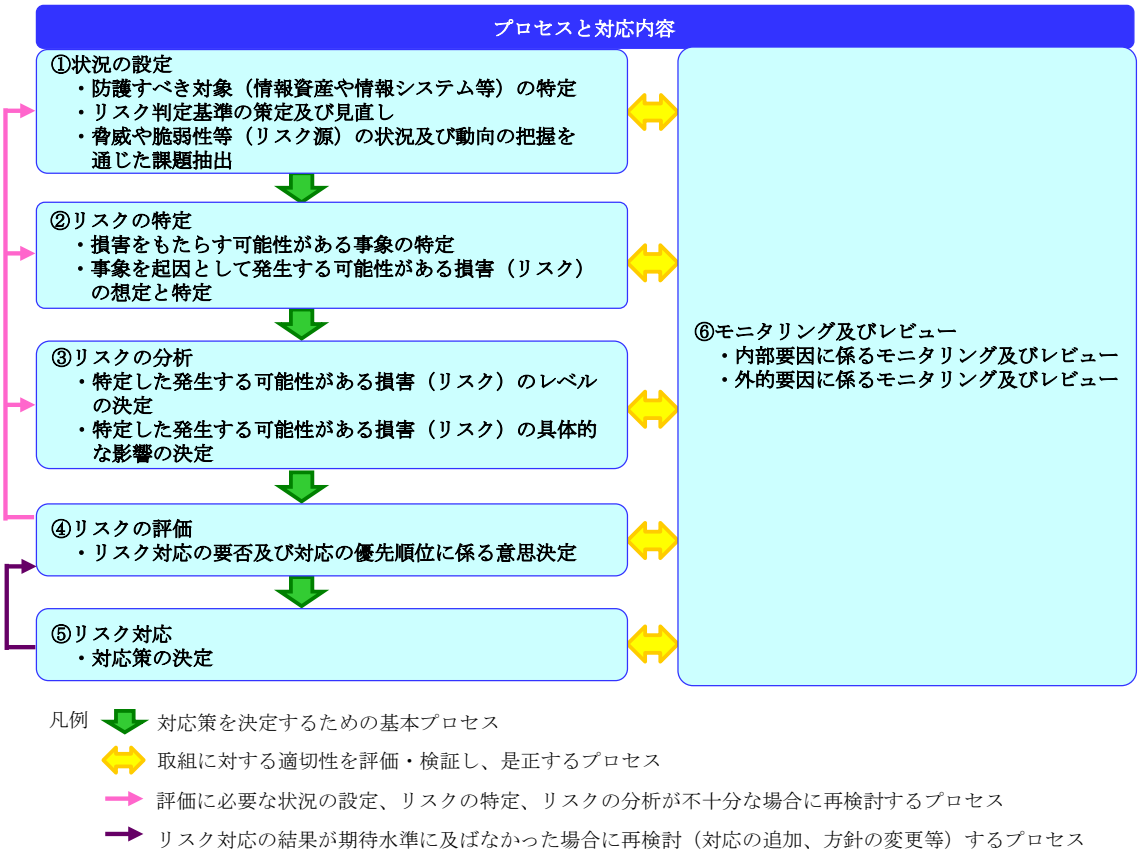
記載内容については、指針本編、指針対策編と同様に行動計画の「図表３　『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」（指針手引書の図表３として再掲）に照らし、ISO/IEC27005:2011の考え方をベースに、図表２に示す各プロセスについて解説するものです。

このため、指針手引書の記載はあくまで一例であり、必ずしも記載の通り実施しなければならないわけではありません。

[5] 指針対策編の正式名称は「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第４版）対策編」といいます。

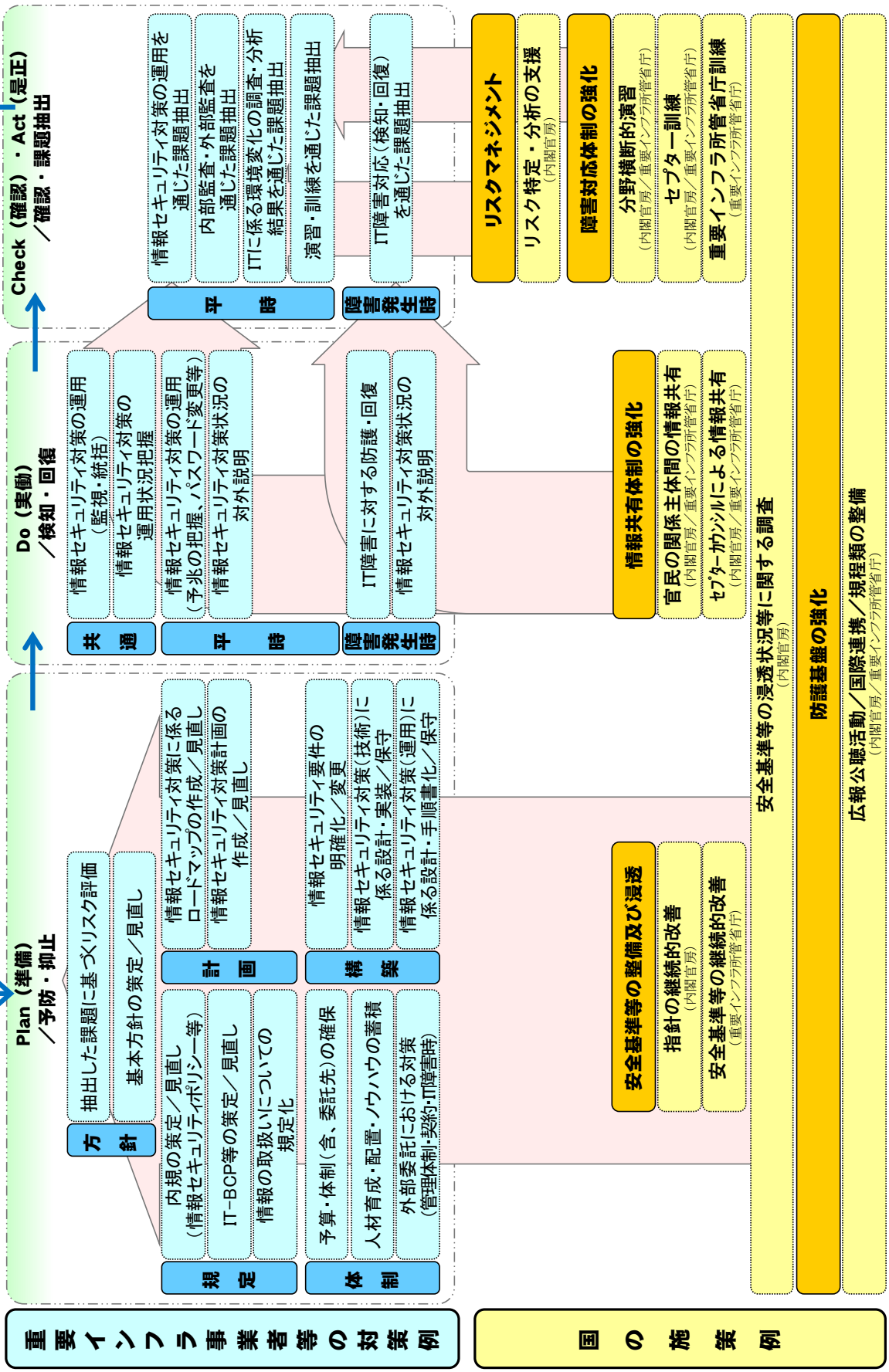
[6] 指針手引書の正式名称は「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）」といいます。

図表２　情報セキュリティ対策の優先順位付け及び対応策決定のプロセス（全体版）



また、各重要インフラ事業者等において発生する可能性がある損害のレベルとその対応方法は事業規模、予算、体制等によって区々です。このことから各事業者等に共通する情報セキュリティ対策の優先順位付けに係る考え方までの記載としています。

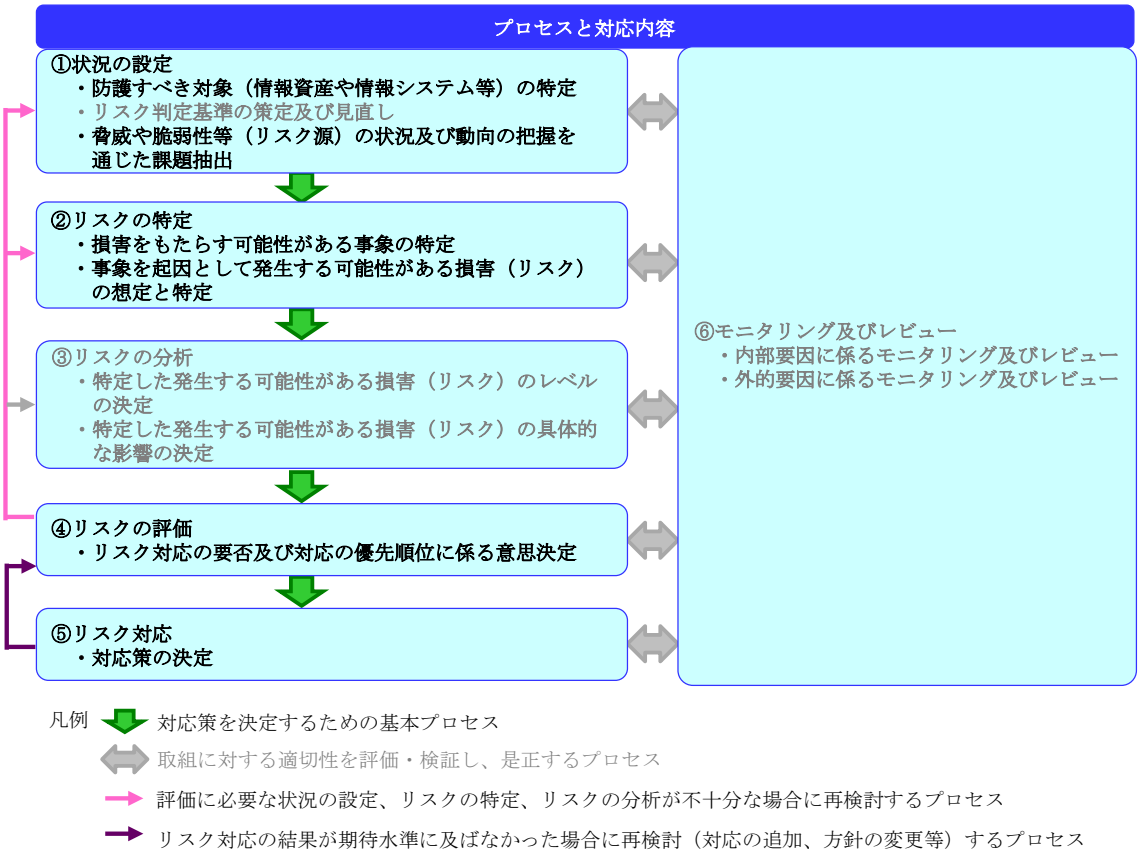
図表３「重要インフラ事業者等の対策例」と各対策に関連する「国の施策例」



3. 指針手引書を活用した各重要インフラ事業者等の取組

指針手引書を契機として、各重要インフラ事業者等が前節で示したプロセスに取り組む場合、最初から全てのプロセスを対応しようとはせずに、まずは以下の強調されたプロセスから対応することが効果的[7]と考えられます。

図表４　情報セキュリティ対策の優先順位付け及び対応策決定のプロセス（簡易版）



特に「④リスクの評価」や「⑤リスク対応」は、どのような対策をどの程度で行うかということを組織として定めるプロセスであり、以降に作成される対応要件の方向付けをなす重要な位置付けにあるものと考えられます。

これらのプロセスは、一例として、以下の段階を経て実現します[8]。

[7] 重要インフラ事業者等が自らの状況を正しく認識すること（Ⅰ.1に記載）に照らして選択しました。残りのプロセスについては、意思決定の判断材料の充実やより適切な情報セキュリティ対策の実現を目的とするため、基本プロセスではなく応用プロセスと整理しました。

[8] その他のプロセスについては、この整備・運用が安定した後に上記の段階を経て、順次、実現することになります。

●「情報セキュリティ対策の方法や程度を意思決定するための仕組みや体制」を内規等で規定し、

（指針対策編では、「Ⅱ.1.2.(1)内規の策定・見直し」が該当）

●内規等に基づいて仕組みや体制を整備した上で、

（指針対策編では、「Ⅱ.1.4.(1)予算・体制（委託先を含む）の確保」が該当）

●内規等に基づいて運用を開始し、継続する。

（指針対策編では、「Ⅱ.3.『Check(確認)・Act（是正)』の観点」と「Ⅱ.1.1.(1)抽出した課題に基づくリスク評価」が該当）

このことから、指針手引書の活用に当たっては、各重要インフラ事業者等が対応するプロセスに該当する節から参照していくことが効果的と考えられます。

なお、「①状況の設定」において実施する脅威や脆弱性等（リスク源）の状況及び動向の把握に向けては、内閣官房から提供する留意すべき脅威や脆弱性等の情報や機会等も積極的に活用しながら、動向の把握や情報セキュリティ対策に係る課題の抽出をすることが有効と考えられます。

Ⅱ．情報セキュリティ対策の優先順位付け及び対応策決定のプロセス

1. 状況の設定

1.1 防護すべき対象（情報資産や情報システム等）の特定

一例として、以下の観点から、防護すべき対象を特定します。

・各重要インフラ事業者等に関係する「安全基準等」

・提供する重要インフラサービスが維持すべきサービスのレベル（以下「サービス維持レベル」といいます。）

・重要インフラ事業者等において機密扱いとすべき情報　　等

防護すべき対象の具体例を以下に示します。

図表５　防護すべき対象の具体例

観点	防護すべき対象
サービス維持レベル	重要な事業プロセスや事業活動を管理する以下 －情報システム －組織 －要員　　等
機密扱いとすべき情報等	以下で管理される情報資産等 －紙 －電磁記録媒体　　等

なお、指針手引書の図表６として行動計画の別紙２で示す「重要インフラサービスとサービス維持レベル」を再掲します。防護すべき対象の特定に図表６を利活用ください。

図表６　重要インフラサービスとサービス維持レベル

重要インフラ分野		重要インフラサービス（手続きを含む）(注)		サービス維持レベル	
		呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
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	・電気通信事業法施行規則第58条による
		・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）	・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	・放送法施行規則第125条第１項から第３項までによる
		・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）	・ケーブルテレビ設備の故障により、放送の停止が、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	・放送法施行規則第157条による
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）	・ＩＴの不具合により、預金の払戻しの遅延・停止が生じないこと ・ＩＴの不具合により、融資承諾をした貸付の実行の遅延・停止が生じないこと ・ＩＴの不具合により、為替（銀行振込）の遅延・停止が生じないこと	・「主要行等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合（例えば、一部のATMが停止した場合であっても同一店舗又は近隣店舗の他のATMや窓口において対応が可能な場合等）を除く
		・資金清算	・資金清算（資金決済に関する法律第２条第５項）	・ＩＴの不具合により、資金清算の遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
		・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）	・ＩＴの不具合により、電子記録及び資金決済に関する情報提供の遅延・停止が生じないこと	・「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）」を参照
	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	・ＩＴの不具合により、保険金等の支払いに遅延・停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
	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	・ＩＴの不具合により、保険金等の支払いに遅延・停止が生じないこと	・「保険会社向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く

重要インフラ分野		重要インフラサービス（手続きを含む）(注)		サービス維持レベル	
		呼称	サービス（手続きを含む）の説明 （関連する法令）	対象・水準	備考
	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）	・ＩＴの不具合により、預り有価証券等の売却、解約代金の払い出し等に遅延・停止が生じないこと	・「金融商品取引業者等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合（例えば、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く
		・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）	・ＩＴの不具合により、有価証券の売買又は市場デリバティブ取引等に遅延・停止が生じないこと	・金融商品取引所等に関する内閣府令第112条第７項を参照
		・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）	・ＩＴの不具合により、社債・株式等の振替等に遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
		・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）	・ＩＴの不具合により、金融商品取引の清算等に遅延・停止が生じないこと	・「清算・振替機関等向けの総合的な監督指針」等を参照 ・他のシステム・機器が速やかに交替することで実質的な影響が生じない場合を除く
航空		・旅客、貨物の航空輸送サービス ・航空交通管制業務 ・気象情報配信 ・予約、発券、搭乗・搭載手続き ・運航整備	・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） ・空域の適正な利用及び安全かつ円滑な航空交通の確保（航空法第95条の２） ・航空機の利用に適合する予報・警報等の配信（気象業務法第14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	・ＩＴの不具合により、貨客の運送に支障を及ぼす定期便の欠航が生じないこと	・「航空分野におけるCEPTOAR」に係る申し合わせにおいて対応

重要インフラ分野	重要インフラサービス（手続きを含む）(注)		サービス維持レベル	
	呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
	・飛行計画作成	・飛行計画の作成、航空局への提出		
鉄道	・旅客輸送サービス ・発券、入出場手続き	・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	・ＩＴの不具合により、旅客の輸送に支障を及ぼす列車の運休が生じないこと	・鉄道事故等報告規則第５条（鉄道運転事故等の報告）による
電力	・一般電気事業	・一般の需要に応じ電気を供給する事業（電気事業法第２条及び第18条）	・ＩＴ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	・電気関係報告規則第３条による
ガス	・一般ガス事業	・一般の需要に応じ導管によりガスを供給する事業（ガス事業法第２条）	・ＩＴ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	・ガス事業法施行規則第112条による
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）	・ＩＴの不具合により、住民等の権利利益の保護に支障が生じないこと ・住民等の安全・安心を確保できる時間内にシステムの復旧を行うこと	
医療	・診療	・診察や治療等の行為	・医療機器の誤作動の招来等により、人の生命に危険が及ばないこと。 ・ＩＴの不具合により、診療の継続に支障が生じないこと。	・ＩＴの依存度によらず、診療や治療等の行為の水準の維持に努めること。
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）	・ＩＴの不具合により、断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと	・重大なシステム障害とは、システム停止に伴う給水への影響が大きい制御システム（浄水場の監視制御システム、ポンプ場の運転システム、水運用システム等）の障害を想定 ・「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）の「6.(2)水道における情報システム障害等が発生した場合」による
物流	・物流	・貨物の運送及び保管	・ＩＴの不具合により、貨物運送の停止や貨物の紛失が生じないこと	・「物流分野における情報共有・分析機能（CEPTOAR）に係る申し合わせ」において対応
化学	・石油化学工業	・石油化学製品の製造、加工及び売買	・ＩＴの不具合により、石油化学製品の供給に著しく重大な支障が生じないこと	

重要インフラ分野	重要インフラサービス（手続きを含む）(注)		サービス維持レベル	
	呼称	サービス（手続きを含む）の説明（関連する法令）	対象・水準	備考
クレジット	・オーソリゼーション	・包括信用購入あっせん等における利用時の承認（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）	・ＩＴの機能不全等により、オーソリゼーションの遅延、停止、不正使用等が行われないこと	
石油	・石油の供給	・石油の輸入、精製、物流、販売	・ＩＴの不具合により、石油の供給の確保に支障が生じないこと	

注　ＩＴを全く利用していないサービスについては対象外。

1.2 リスク判定基準の策定及び見直し

リスク判定基準とは後続のプロセスである「リスク評価」において、発生する可能性がある損害（リスク）への対応方針やその対応の優先順位を決定する際に用いる基準のことです。

この基準については、各重要インフラ事業者等の状況を考慮した上で策定し、実施によって得られた知見を踏まえながら継続的に見直しを行うものです。

リスク判定基準については、以下の構成とするのが一般的です。

図表７　一般的なリスク判定基準の構成とその観点

基準	基準の観点
リスク評価基準	発生する可能性がある損害（リスク）を評価するための観点
影響基準	費用を含む被害の程度を設定するための観点
リスク受容基準	発生する可能性がある損害（リスク）について、それを受容できる程度を評価するための観点

1.2.1 リスク評価基準

リスク評価基準とは、発生する可能性がある損害（リスク）を評価するための観点です。

開始又は継続する事業又は取組がもたらす効果や制約事項となる可能性がある以下を考慮して、リスク評価基準を定性的又は定量的に策定します。

・戦略的価値
・関係する情報資産の重要性
・法令、規制等の要求事項
・契約上の義務
・機密性、完全性又は可用性から見た運用上又は事業上の重要性
・ステークホルダーの期待、信用等に及ぼす好ましくない結果　　等

1.2.2 影響基準

影響基準とは、費用を含む被害の程度を設定するための観点です。

被害の程度に影響を与える可能性がある以下を考慮して、影響基準を定性的又は定量的に策定します。

・影響を受ける情報資産の分離レベル

・機密性、完全性又は可用性の喪失等に繋がる情報セキュリティ違反

・運用障害

・事業又は金融資産価値の喪失

・計画及び期限の遅れ

・評判の失墜

・法令、規制等、又は契約上の要求事項違反　　等

1.2.3 リスク受容基準

リスク受容基準とは、発生する可能性がある損害（リスク）について、それを受容できる程度を評価するための観点であり、各重要インフラ事業者等の方針、目標、目的、ステークホルダーの利害等に依存します。

損害が発生する可能性や期間に照らしつつ、以下を考慮して、リスク受容基準を定量的又は定性的に策定します。

・事業基準

・法令、規則等

・社会的又は人道的要素

・運用

・技術

・財務　　等

1.3 脅威や脆弱性等（リスク源）の状況及び動向の把握を通じた課題抽出

1.3.1 情報セキュリティ対策の運用における情報収集を通じた課題の抽出

行動計画では、「情報セキュリティ対策は一義的に重要インフラ事業者等が自らの責任において実施するものではあるが、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは、多様な脅威への対応が十分であることを確認することは難しい。このため、分野内、分野間あるいは官民間の情報共有を行うことで連携して、必要な情報セキュリティ対策に取り組むことが重要である」としています。

このことから脅威や脆弱性等（リスク源）の状況や動向の把握に向けて、各重要インフラ事業者等は、情報セキュリティ対策の運用の一環として以下から提供される脅威や脆弱性等（リスク源）に係る情報を収集し、利活用することが重要です。

・内閣官房

・情報セキュリティ関係省庁

・情報セキュリティ関係機関

・サイバー空間関連事業者

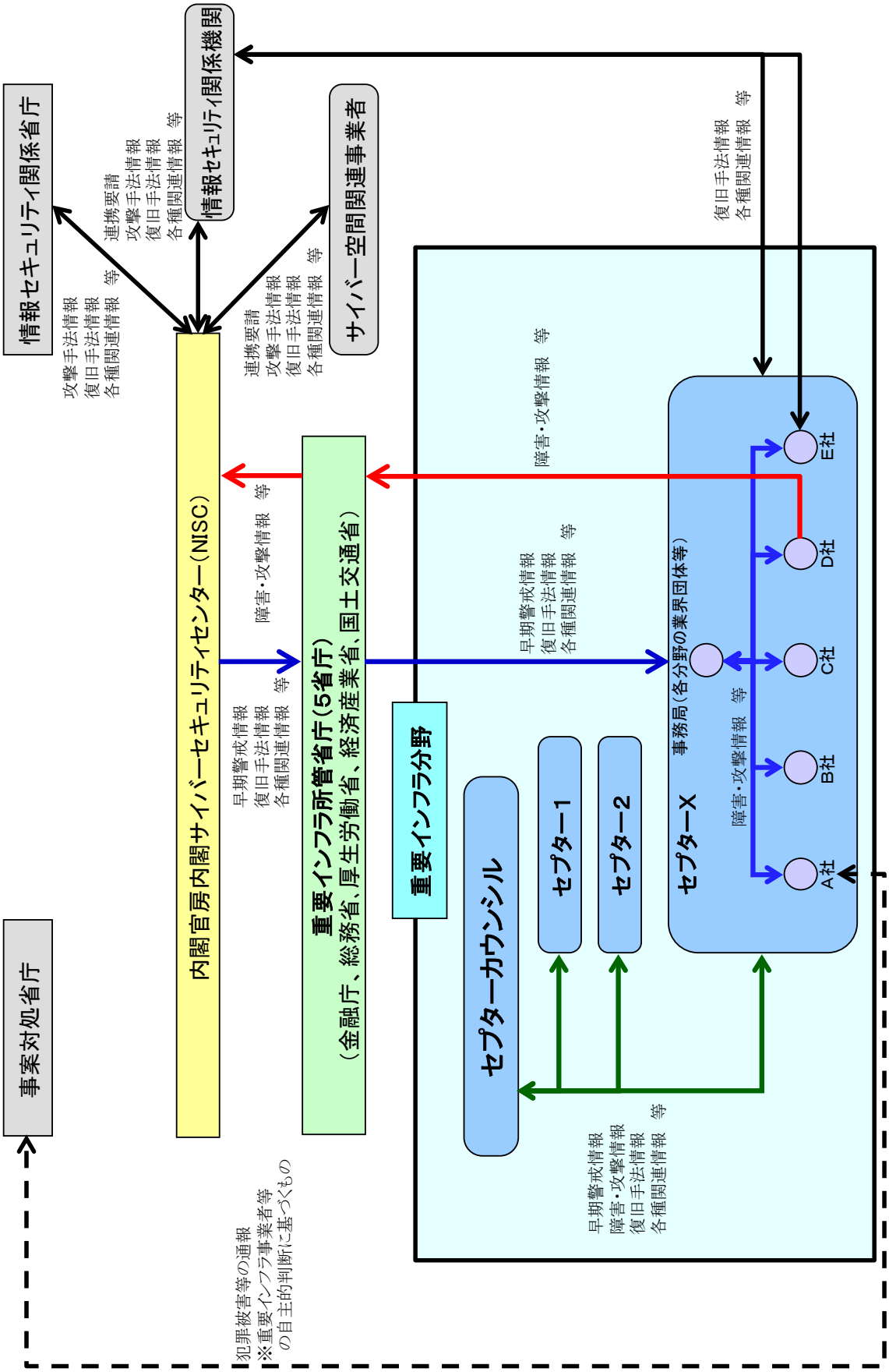
・セプター　　等

また、各重要インフラ事業者等が、この収集結果から脅威の発生状況や脆弱性の存在等を把握し、自らの情報セキュリティ対策に照らして課題を抽出することを情報セキュリティ対策の実施、とりわけ改善の起点のひとつとしていくことが重要です。

なお、各重要インフラ事業者等における情報共有体制を確認する観点から、指針手引書の図表８として行動計画の別紙４－１で示す「情報共有体制（平時）」を再掲します。

確かな情報共有体制を構築し、維持していくことは重要インフラ防護において重要であることを踏まえ、当該体制、具体的にはセプター活動への積極的な参加が期待されます。

図表８　「情報共有体制（平時）



1.3.2　内部監査及び外部監査を通じた課題の抽出

情報セキュリティ対策を担う部門が情報セキュリティ対策の運用の一環として行う課題抽出に加えて、客観的かつ専門的な見地から行う課題抽出も重要です。

客観的かつ専門的な見地による内部監査や外部監査から得る情報セキュリティ対策への評価、改善事項等の助言、勧告等を通じて、各重要インフラ事業者等が脅威の発生状況や脆弱性の存在等を把握します。

その上で、自らの情報セキュリティ対策に照らして課題を抽出することを情報セキュリティ対策の実施、とりわけ改善の起点のひとつとしていくことが重要です。

1.3.3　ＩＴに係る環境変化の調査及び分析結果を通じた課題の抽出

行動計画では、「重要インフラを取り巻く社会環境や技術環境等が刻々と変化する中、重要インフラにおいて守るべき情報システム及びその中で利活用されるデータのサイバー空間への依存度が一層高まっている。このような状況の下、サイバー空間に潜む脅威や脆弱性といったリスク源に起因するＩＴの不具合による影響は甚大化しており、ひとたびＩＴの不具合が発生すれば、重要インフラサービスの提供が困難となる可能性がある」としています。

このことから行動計画において内閣官房は、今後の導入拡大を想定するBYODやビッグデータに加えて中長期的な浸透が予想される新しい技術又はシステムであるM2M、スマートコミュニティ等を対象とした実態調査を行い、新たな脅威や脆弱性等（リスク源）及びリスク[9]の分析を行うこととしています。

各重要インフラ事業者等がこれらの調査や自らの調査から得た分析結果等を通じて、脅威の発生状況や脆弱性の存在等を把握し、自らの情報セキュリティ対策に照らして課題を抽出することを情報セキュリティ対策の実施、とりわけ改善の起点のひとつとしていくことが重要です。

[9] 本節においては、発生する可能性がある損害ではなく、新しい技術又はシステムが持続的なサービス提供を停止させる可能性等を指します。

1.3.4　演習及び訓練を通じた課題の抽出

ＩＴ障害の拡大防止や迅速な復旧の実現は、情報セキュリティ対策において重要な観点のひとつです。この実現のためには、導入したセキュリティ機能や策定したIT-BCPを検証し、その実効性を確保することが重要です。

各重要インフラ事業者等が、演習や訓練に参加して以下の実効性を確認することを通じて、脅威の発生状況や脆弱性の存在等を把握し、自らの情報セキュリティ対策に照らして課題を抽出することを情報セキュリティ対策の実施、とりわけ改善の起点のひとつとしていくことが重要です。

・IT-BCPの発動条件や対応の優先順位付け

・ＩＴ障害発生時の体制や権限移譲

・情報共有体制　　等

行動計画において内閣官房は、演習や訓練として以下を行うこととしています。各重要インフラ事業者等は、IT-BCPの検証等に向けて、こうした活動を積極的に利活用していくことが重要です。

図表９　行動計画に記載がある演習・訓練

訓練・演習	目的
セプター訓練	情報の共有先や共有手続きの確認を通じて、各重要インフラ分野のセプターと重要インフラ所管省庁との「縦の情報共有」体制を維持・強化
分野横断的演習	各重要インフラ事業者等による障害対応体制の検証を通じて、重要インフラ分野間の「横の情報共有」体制を維持・強化

2. リスクの特定

重要インフラ事業において、発生する可能性がある損害（リスク）を想定し、特定します。

この特定結果は後続のプロセスの検討材料となりますので、防護すべき対象を守るためには、漏れなく発生する可能性がある損害（リスク）を特定することが重要です。漏れのない特定のためには、脅威や脆弱性等（リスク源）がもたらす可能性（原因）からのアプローチと事象（結果）からのアプローチの両面から事象を特定する必要があります。

2.1 損害をもたらす可能性がある事象の特定

事象の特定に向けた原因からのアプローチと結果からのアプローチについて一例を以下に示します。

2.1.1 原因からのアプローチ

発生した脅威や存在する脆弱性等、認識したリスク源をもとに、それらが防護すべき対象に損害をもたらす可能性がある事象を特定します。

事象の特定方法の具体例としては、以下が考えられます。

・内部要員の持出し（原因） → 機密情報等の流出（結果）

・外部からの侵入（原因） → Webサイト等の改ざん（結果）

・機器故障（原因） → 重要な情報システムの機能停止（結果） 等

2.1.2 結果からのアプローチ

原因からのアプローチに限定して事象を特定した場合、想定し得ない原因への対応が難しくなる可能性があります。この想定し得ない原因への対応に向け、発生すると防護すべき対象に損害をもたらす可能性がある事象を既成概念や情報セキュリティ対策の実現可能性に捕らわれることなく特定します。

この特定については事業継続を念頭においた全社的なリスクマネジメントの視点を要するため、経営層の観点に基づいた実施が望まれます。

一方、現状ではその実施が困難な場合に備え、事象の特定方法の一例を以下に示します。

・原因からのアプローチにて導いた結果からの連想

・他社事例の参照

・外部機関によるアドバイスの利活用　　等

2.2 事象を起因として発生する可能性がある損害（リスク）の想定と特定

前項で特定した事象を起因として発生する可能性がある損害（リスク）を想定し、特定します。

発生する可能性がある損害（リスク）の具体例としては、以下が考えられます。

・開始又は継続する事業や取組の有効性の欠如

・好ましくない運用状況への変化

・事業上の損失

・評判の失墜　　等

3. リスクの分析

3.1 特定した発生する可能性がある損害（リスク）のレベルの決定

前節で特定した発生する可能性がある損害（リスク）をもとに、その特質と以下の具体例に照らした定性的又は定量的な分析を通じて、損害（リスク）のレベルを決定します。

・重要インフラ事業にその損害をもたらす可能性がある原因

・脅威や脆弱性等（リスク源）に照らした損害の発生のしやすさ

・その損害がもたらす可能性がある重要インフラ事業への影響の大きさ

・影響を抑止できる対策の導入状況　　等

なお、リスク分析手法については様々な手法が提唱されており、例示のために指針手引書ではISO/IEC27005:2011を参照していますが、重要なのは各インフラ事業者等において以下の具体例のバランスを考慮した最も合理的で達成可能な方法を適用することです。

・各重要インフラ事業者等において、必要な精度

・活用できるデータの程度や粒度

・現時点で有する分析の力量

・分析作業の容易性　　等

また、分析結果については、一例として、損害（リスク）のレベルに応じた分類と損害の発生のしやすさをマトリクス等で整理する方法等があります。

3.1.1 定性的な分析をする場合

一例として、マトリクスの軸の一方である損害（リスク）のレベルは「小」、「中」、「大」等で、もう一方である損害の発生のしやすさは「低」、「中」、「高」等で表し、分析結果を分類する方法等があります。

この分類においては、可能な限り現実の情報やデータをもとに用いて行います。

3.1.2 定量的な分析をする場合

一例として、各マトリクスの軸には情報源から得られたデータをもとにした数値の尺度を用い、損害（リスク）のレベルと損害の発生のしやすさを分類する方法等があります。

3.2 特定した発生する可能性がある損害（リスク）の具体的な影響の決定

前項で決定した損害（リスク）のレベルをもとに、重要インフラ事業に与える具体的な損害や影響を決定します。

この分析結果については、後続のプロセスである「リスクの評価」及び「リスク対応」にて行う意思決定の際に用いる基礎資料として提供します。

4. リスクの評価

4.1 リスク対応の要否及び対応の優先順位に係る意思決定

4.1.1 リスク対応の要否に係る意思決定

Ⅱ.1.2項で策定したリスク判定基準と前節で特定した個々の損害（リスク）の分析結果を比較し、発生する可能性がある損害（リスク）への対応の要否を決定します。

この決定については、発生する可能性がある損害（リスク）を受容できるか否かによって判断することが基本となります。

その際、留意が必要なのは、発生のしやすさとは無関係に損害（リスク）の大きさだけで対応を要する場合や、発生のしやすさだけで対応を要する場合があることです。

前者の一例としては、事業の継続が危ぶまれる規模の災害等が考えられます。後者の一例としては、発生のしやすさに加え頻度が高い場合において、単発では小さい損害（リスク）であっても累積して損害（リスク）が大きくなるケース等が考えられます。

なお、指針手引書のⅠ.2節で示すプロセスのうち、Ⅰ.3節で示すように一部のプロセスを優先して対応したためにリスク判定基準を策定していない場合は、個々の損害（リスク）の分析結果を経営層や有識者の知見[10]に照らす等の代替策を用いて要否を決定することになります。

4.1.2 リスク対応の優先順位に係る意思決定

対応を要すると決定した場合は、各対応の優先順位を決定します。

この決定については、以下の具体例を考慮して、発生する可能性がある損害（リスク）への対応の優先順位を決定することになります。

・損害（リスク）のレベルの大きさ

・重要インフラ事業に与える具体的な損害や影響　　等

[10] これらの知見を蓄積していくことで、リスク判定基準の観点が集積されることになります。

5. リスク対応

5.1 対応策の決定

前節で優先順位付けされた各対応について、以下の具体例を考慮して、対応策を決定します。

・発生する可能性がある損害（リスク）の重大性

・対応策の実現性

・発生する可能性がある損害（リスク）の拡大の可能性　　等

対応策の選択においては、発生する可能性がある損害（リスク）の評価結果と以下の具体例に照らし、開始又は継続する事業又は取組から産み出される利益と要する費用、労力、技術的実現性等とのバランスにより判断[11]することになります。

・各重要インフラ事業者等に適用される法律や規制

・当該業務を行うために必要な要求事項

・各重要インフラ事業者等で定めた社会的責任等の要求事項　　等

以下から対応策を選択し、リスク対応計画の策定を経て、情報セキュリティ対策の対応要件を作成することになります。

図表 10　対応策の選択肢

対応策	概要
リスクの修正	発生する可能性がある損害（リスク）を低減し、低減後の損害（リスク）を各重要インフラ事業者等が受容できるレベルとする対応策
リスクの保有	現状の情報セキュリティ対策への追加をせずに、発生する可能性がある損害（リスク）を保有（受容）する対応策
リスクの回避	その損害（リスク）が発生する可能性がある事業又は取組を止める、活動の運用条件を変更する等で損害（リスク）を回避する対応策
リスクの共有	契約等を通じて、一定の発生する可能性がある損害（リスク）を利害関係者と共有する対応策

[11] 極めて深刻な影響がありかつ発生頻度が極めて低いリスクについては、単純な費用対効果で判断せずに、事業継続の観点から考慮する必要があります。

5.1.1　リスクの修正

リスクの修正とは、発生する可能性がある損害（リスク）を低減し、低減後の発生する可能性がある損害（リスク）を各重要インフラ事業者等が受容できるレベルとする対応策です。

損害（リスク）のレベルと発生のしやすさが共に高く、開始又は継続する事業又は取組の戦略的価値が高い場合、又は関係する情報資産が重要である場合に選択します。

損害（リスク）のレベルを低減する具体例として、以下の対応が考えられます。

・脅威や脆弱性等（リスク源）の除去

・事業又は取組が目指す結果の変更等による損害の発生のしやすさの変更　　等

5.1.2　リスクの保有

リスクの保有とは、現状の情報セキュリティ対策への追加をせずに、発生する可能性がある損害（リスク）を保有（受容）する対応策です。

損害（リスク）のレベルと発生のしやすさが共に低く、損害（リスク）のレベルがリスク受容基準を満たしていることを確認した場合に選択します。

リスクの保有を選択した場合、発生する可能性がある損害（リスク）については、状況によってリスク受容基準を満たさなくなる可能性があることに留意し、注意深く監視をしていくことが必要になります。

なお、指針手引書のⅠ.2節で示すプロセスのうち、Ⅰ.3節で示すように一部のプロセスを優先して対応したためにリスク受容基準を策定していない場合は、経営層や有識者の知見[12]に照らす等の代替策を用いて満たしていることを確認することになります。

5.1.3　リスクの回避

リスクの回避とは、その損害（リスク）が発生する可能性がある事業又は取組を止める、活動の運用条件を変更する等で損害（リスク）を完全に回避する対応策です。

法令、規制等からの要求事項、契約上の義務、事業規模等の観点から損害（リスク）のレベルが高すぎる場合に選択します。

[12] これらの知見を蓄積していくことで、リスク受容基準の観点が集積されることになります。

5.1.4　リスクの共有

リスクの共有とは、契約等を通じて、一定の発生する可能性がある損害（リスク）を利害関係者と共有する対応策です。

損害（リスク）のレベルが高いが発生のしやすさが低い場合に選択します。

損害（リスク）を利害関係者と共有する具体例として、以下の対応が考えられます。

・保険契約等による共有

・損害が発生する前に即応の防御を可能とする契約等による共有　　等

なお、発生する可能性がある損害（リスク）を管理する責任自体を共有することは困難と考えられます。顧客側の観点からするとその責任は各重要インフラ事業者等にあるとみなされるものと考えられるためです。

5.1.5　リスク対応計画の策定及び評価

(1) リスク対応計画の策定

対応策を決定した各対応について、個々のリスク対応計画を策定していきます。

その際、以下について考慮し、合理的に情報セキュリティ対策を実施していくことが重要です。

・発生する可能性がある損害（リスク）への対応の優先順位の明確化

・不正侵入を防止するための対策と許してしまった侵入がもたらす実被害を防止するための対策のバランス

・各対応で共通する取組（例. 情報セキュリティの教育訓練、意識向上等）の効率化等　　等

(2) リスク対応計画の評価

リスク対応計画を策定した後に、各対応が完了した時点において発生する可能性がある損害（リスク）が各重要インフラ事業者等のリスク受容基準（未策定の場合は経営層や有識者の知見等）を満たしているか否かを評価します。

これは、今回の各リスク対応による以下を防止するために行います。

・発生する可能性がある損害（リスク）を新たに産み出すこと

・過去のリスク対応では受容できるレベルであった損害（リスク）が、リスク受容基準（未策定の場合は経営層や有識者の知見）を満たさなくなること

評価の結果、各対応が完了した時点において発生する可能性がある損害（リスク）がリスク受容基準を満たしていなければ、改めて「リスク対応」のプロセスを繰り返すこととなります。

その際、リスク受容基準の見直しを要することが判明した場合は、見直した上で繰り返すこととなります。

6. モニタリング及びレビュー

自らの組織に最も相応しい情報セキュリティ対策を構築し、維持・改善していくことを通じて防護対策の有効性を高めていくためには、情報セキュリティ対策の優先順位付け及び対応策決定の各プロセス（指針手引書Ⅱ章の１節から５節のうち各重要インフラ事業者等が採用するプロセス）が適切に実施されていることが必要です。

このことから実施している各プロセスの適切さをモニタリング及びレビューを通じて確保していくことが重要です。

また、脅威や脆弱性等（リスク源)、発生する可能性がある損害（リスク）の発生のしやすさ、同損害（リスク）のレベル等は、取組状況や環境変化等の要因により常に変動しています。

このような変動は満たしていたリスク受容基準を満たさなくすることがあります。

このことからこうした変化を的確に発見するためには適切なモニタリング及びレビューが重要となります。

6.1 内的要因に係るモニタリング及びレビュー

目標に向けた各プロセスの目的やリスク対応計画とかい離した対応は、期待した有効性を伴わない可能性があります。

このかい離又はかい離の予兆を把握し是正するために、継続的なモニタリング及びレビューを行います。

また、対応した成果についても、目標に向けた各プロセスの目的の達成状況や期待した有効性が得られているかを評価するために、レビューを行います。

6.2 外的要因に係るモニタリング及びレビュー

外的要因の変化は、リスク評価において対応不要としていた発生する可能性がある損害（リスク）を増大させる可能性があります。

外的要因の具体例としては以下が考えられます。

- 事業要件の変化
- 脅威や脆弱性等（リスク源）の新たな発生、増大等
- 発生する可能性がある損害（リスク）の発生のしやすさの増大
- リスク受容基準の水準の変化　　等

これらの外的要因の変化を把握した際は、必要なプロセスを再度行い、必要に応じて、これまでに決定した対応策を見直します。

また、リスク評価基準、影響基準、リスク受容基準等からなるリスク判定基準についても、事業の目的、戦略、方針等に整合し、事業状況の変化に応じていることを定期的に検証していきます。

別紙　定義・用語集

BYOD	Bring Your Own Deviceの略。企業等において、従業員が私用で使っているスマートフォン等の情報端末から企業等の情報システムにアクセスし、必要な情報を閲覧・入力する等、私物の情報端末を業務で利用することを指す。
IT-BCP等	指針手引書では、重要インフラサービスの提供に必要な情報システムに関する事業継続計画（関連マニュアル類を含む。）その他の事業継続計画を指す。
ＩＴ障害	ＩＴの不具合のうち、重要インフラサービスの提供水準が「図表２　重要インフラサービスとサービス維持レベル」における「サービス維持レベル」を下回るものを指す。
ＩＴ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。
安全基準等	業法に基づき国が定める「強制基準」、業法に準じて国が定める「推奨基準」及び「ガイドライン」、業法や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、業法や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等の総称。ただし、指針は含まない。
外部監査	指針手引書では、情報セキュリティ対策の実施状況について重要インフラ事業者等の外部の独立した主体が、客観的・専門的見地から、評価・改善事項等の助言・勧告等を行うことを指す。
可用性	指針手引書では、情報にアクセスすることを認められた者が必要なときに中断されることなく情報にアクセスできる状態を確保することを指す。
完全性	指針手引書では、情報が破壊、改ざん又は消去されていない状態を確保することを指す。
機密性	指針手引書では、情報にアクセスすることが認められた者だけが情報にアクセスできる状態を確保すること（情報が漏えいしても影響を及ぼさないよう情報の秘匿性を確保することを含む。）を指す。
脅威	指針手引書では、機密性、完全性、可用性を脅かす事象を引き起こす可能性があるものを指す。具体的には自然災害やサイバー攻撃等。
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。
情報共有	見聞や知識・ノウハウ等の情報を、仲間に伝達したり、組織・メンバー間で伝達し合ったりして共有すること。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、独立行政法人情報通信研究機構（NICT）、独立行政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）、一般財団法人日本データ通信協会テレコム・アイザック推進会議（Telecom-ISAC Japan）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）。
情報セキュリティ関係省庁	警察庁、総務省、外務省、経済産業省及び防衛省。
脆弱性	指針手引書では、情報システムが抱える防護上の弱点を指す。具体的には情報システムや管理体制の欠陥等。
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）。
内部監査	指針手引書では、情報セキュリティ対策の実施状況について重要インフラ事業者等の内部において独立した主体が、客観的・専門的見地から、評価・改善事項等の助言・勧告等を行うことを指す。
モニタリング	指針手引書では、その取組に係る外部環境の状況や取組自身の状況を監視することを指す。
レビュー	指針手引書では、設定された目標を達成するために各プロセスの目的や達成基準等に照らしつつ、その取組の（中間）成果に含まれる問題や誤りを評価者が担当者にフィードバックすることを指す。