資料３

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等について

資料３－１　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等について

※資料３－２　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４版）（案）

◇資料３－３　（参考）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（案）

◇資料３－４　（参考）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）（案）

※資料３－５　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（改定案）

資料３－６　（参考）The Basic Policy of Critical Information
Infrastructure Protection (3rd Edition)（改定案）

※は、サイバーセキュリティ戦略本部決定案。
◇は、重要インフラ専門調査会決定。資料３－２の決定により発効。

資料３－１

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等について

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)(案) について

これまでの取組み

重要インフラの情報セキュリティ対策

- ✓ 重要インフラ事業者等が、自らの情報セキュリティ対策の水準を「安全基準等」に照らし、適切かつ定期的に情報セキュリティ対策を実施・改善

指針の位置付け

- ✓ 「重要インフラの情報セキュリティ対策に係る行動計画」の理念に基づき、重要インフラ分野において必要度の高い横断的な情報セキュリティ対策を記載したガイドライン
- ✓ 各重要インフラ分野の基準やガイドライン、各重要インフラ事業者等の内規等を、それぞれの特性に応じて指針を参考に策定

指針改訂の背景

第3次行動計画の施行（2014年度）

- ✓ 【基本的な考え方】 重要インフラ事業者等による実効的かつ自主的な取組
- ✓ 【指針改訂を通じて目指すこと】　重要インフラ防護能力の維持・向上

第3次行動計画からの改訂要件

- ✓ とりわけ対策途上や中小規模の重要インフラ事業者等に向けて、以下の要件
  - PDCAサイクルに沿った対策手法の習得・実現
  - 習得・実現に向けた段階的な取組
  - 経営層の在り方の訴求

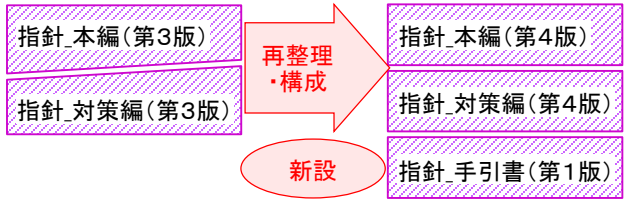
従来の指針の内容を踏まえつつ、第３次行動計画の記載内容に照らして指針を再構成

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）（案）

改訂の主要ポイント

- ✓ 目的及び位置付けに、自主的な取組・持続的な改善についての記載を明記
- ✓ 本編には概念論、対策編には具体論を記載するよう再整理
- ✓ 既存対策項目を第3次行動計画が示すPDCAサイクルに沿って再配置
- ✓ 経営層の在り方も含め、第3次行動計画の記載内容・図表を引用
- ✓ 各事業者が定める対応優先順位に基づき、対策編の項目の段階的な実現に資するため、指針_手引書を新設

指針改訂のイメージ



◆ 指針_本編はサイバーセキュリティ戦略本部決定、指針_対策編及び指針_手引書は重要インフラ専門調査会決定

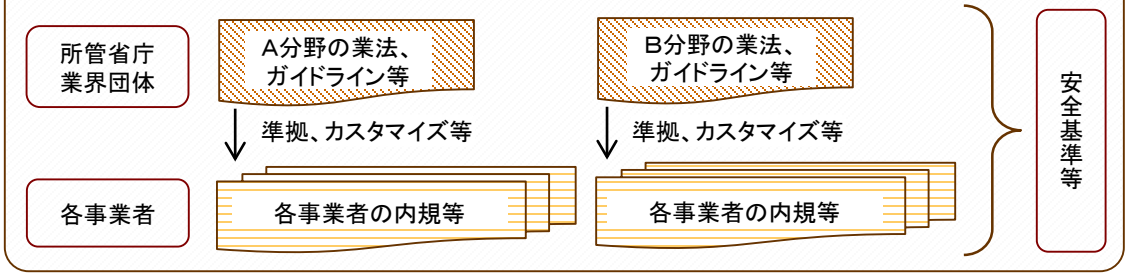
指針の構成

- 指針_本編（第4版）　：　概念
- ↓ 具体的に何をすればよいか
- 指針_対策編（第4版）：　具現化例
- ↓ どの対策から行うか
- 指針_手引書（第1版）：　優先順位付けの考え方

→ 最適な対策の実現

提示

改訂版の提示に基づく安全基準等のカスタマイズ等



「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」の改訂について

「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月決定）について次の修正を実施。

① 重要インフラ分野として新たに追加された「化学」・「クレジット」・「石油」の各分野において、別途整理することとされていた防護対象や連絡体制等について、整理が完了したことから内容を追記。

② サイバーセキュリティ基本法の施行等に伴う組織変更による用語の修正を実施。

改訂の経緯

H26.3.11 重要インフラ専門委員会（第36回）
第３次行動計画（案）の作成

→

H26.5.19 情報セキュリティ政策会議（第39回）
第３次行動計画の決定

新たに追加された重要インフラ分野（化学分野／クレジット分野／石油分野）の
具体的な防護対象や連絡体制等については、別途整理を行う旨、第３次行動計画に明記。

化学分野／クレジット分野／石油分野において、セプター事務局を中心に、
具体的な防護対象や連絡体制を検討。 →概ね平成26年内に整備を完了

行動計画改訂

情報セキュリティ政策会議
→ サイバーセキュリティ戦略本部
情報セキュリティセンター
→ 内閣サイバーセキュリティセンター

←

H27.1.9
サイバーセキュリティ基本法の全面施行

↓

H27.2.10 サイバーセキュリティ戦略本部（第１回）
重要インフラ専門調査会の設置

H27.3.26 重要インフラ専門調査会（第１回）
第３次行動計画 改訂版（案）の作成

→

H27.5.25 サイバーセキュリティ戦略本部（第２回）
第３次行動計画 改訂版の決定（予定）

（参考）「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」の改訂箇所

①組織変更に伴う修正内容

本文中の次の用語を必要に応じて修正。

- ✓ 情報セキュリティ政策会議 → サイバーセキュリティ戦略本部　（p41、p44、p60）
- ✓ 重要インフラ専門委員会 → 重要インフラ専門調査会　（p41、p44）
- ✓ 情報セキュリティセンター → 内閣サイバーセキュリティセンター　（p1）

②追加３分野に関連する追記内容

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	対象となる重要システム例	IT障害やその影響の例
化学	・主要な石油化学事業者	・プラント制御システム	・プラントの停止 ・長期にわたる製品供給の停止
クレジット	・主要なクレジットカード会社　等	・オーソリゼーションシステム　等	・オーソリゼーションの停止
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	・石油の供給の停止 ・製油所の安全運用に対する支障　等

別紙２　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）		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
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	
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	

別紙５　ＩＴ障害発生時における連絡体制等

重要インフラ分野	既存の連絡体制	IT障害発生時における緊急時の連絡体制
化学	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 ・化学CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・化学CEPTOARの連絡体制を活用して実施
クレジット	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・業界内情報共有等	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・クレジットCEPTOARの連絡体制を活用して実施
石油	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・業界内情報共有等	(1) 重要インフラ事業者等→政府 ・石油CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・石油CEPTOARの連絡体制を活用して実施

資料３－２

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４版）
（案）

平 成 ２ ７ 年 ５ 月 ２ ５ 日

サイバーセキュリティ戦略本部

（本ページは白紙です。）

目次

（本ページは白紙です。）

Ⅰ．目的及び位置付け

1. 重要インフラにおける情報セキュリティ対策の重要性

「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成26年５月19日　情報セキュリティ政策会議決定。平成27年〇月〇日サイバーセキュリティ戦略本部改訂。）（以下「行動計画」という。）にあるとおり、重要インフラ[1]におけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害[2]が国民生活及び社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともに、ＩＴ障害発生時においては迅速な復旧と再発防止を図るために、情報セキュリティ対策は重要である。

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

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

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

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

2. 「安全基準等」の必要性

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

---

[1] 「重要インフラ」とは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので重要インフラとして指定する分野」を指す。

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

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

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

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

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

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

3. 「安全基準等」とは何か

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

このことを踏まえ、指針においては

①業法に基づき国が定める「強制基準」

②業法に準じて国が定める「推奨基準」及び「ガイドライン」

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

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

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

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

4. 指針の位置付け

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

このことから指針の目的は「安全基準等」の策定・改訂を通じた情報セキュリティ

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

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

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

具体的には行動計画の「図表３　『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」（PDCAサイクル）に沿って列記した（本図表については、指針において図表１として再掲する。）。[6]

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

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

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

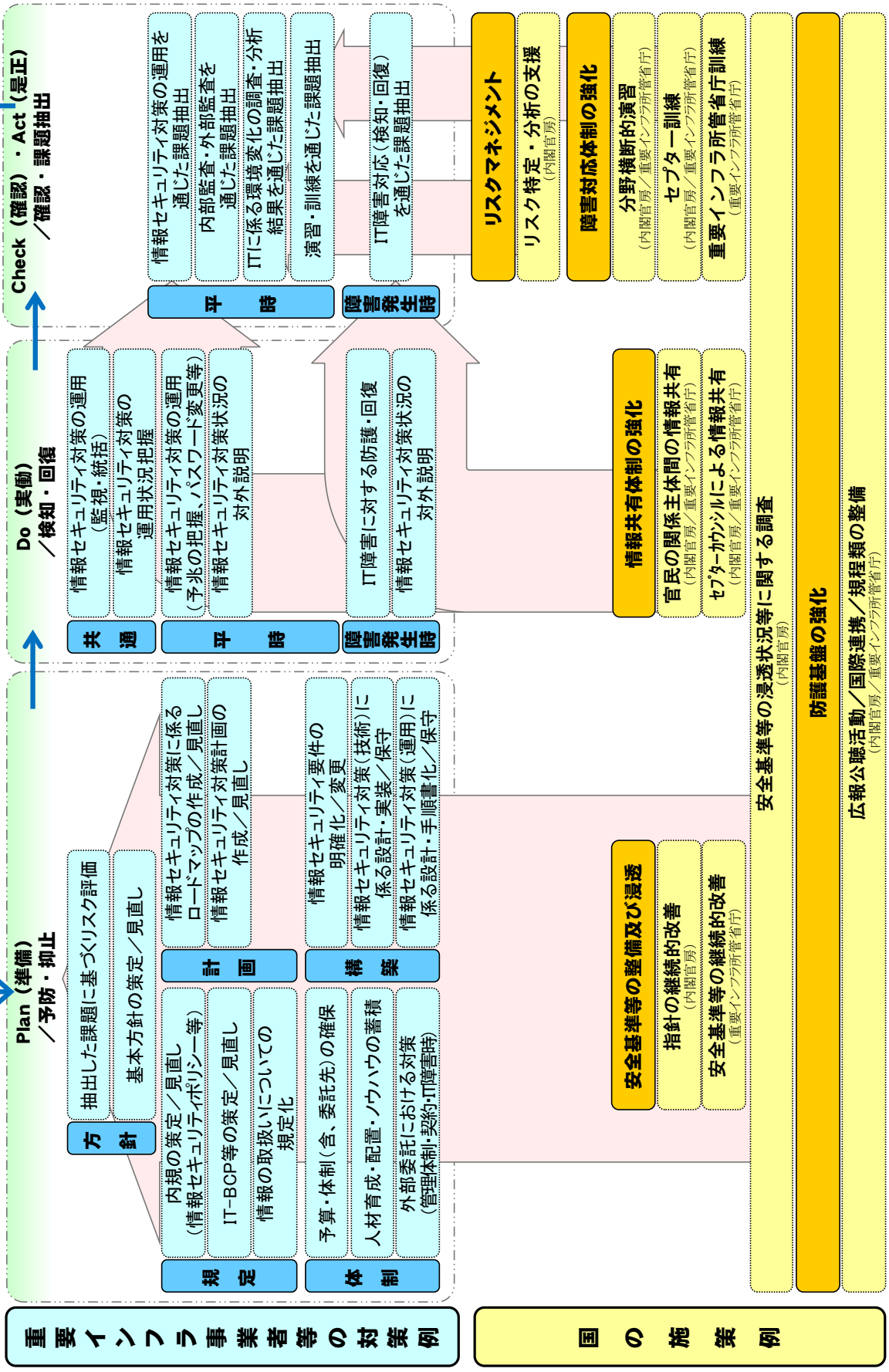
○重要インフラ分野又は重要インフラ事業者等によっては、その事業の態様等の理由から指針の記載項目の中に規定する必要がないものを含むことがあり得ること

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

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

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

図表１「重要インフラ事業者等の対策例」と各対策に関連する「国の施策例」



5. 指針の構成

指針は、安全基準等の必要性及びその中で規定することが望ましい項目を訴求する本書「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針（第４版）」（以下「指針本編」という。）に加え、指針本編に記載する情報セキュリティ対策項目の具体例を記載した項目集である「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針（第４版）対策編」（以下「指針対策編」という。）及び各重要インフラ事業者等が自らの組織に最も相応しい情報セキュリティ対策を指針対策編の項目に照らして構築し、維持・改善していくための優先順位付け等に焦点を当てながら、その防護対策の有効性を高めていくための「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）」（以下「指針手引書」という。）にて構成する。

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

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

6. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待

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

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

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

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

Ⅱ.「安全基準等」で規定が望まれる項目

1. 「安全基準等」策定の目的

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

2. 「安全基準等」の対象範囲

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

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

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

3. 「安全基準等」において対象とする原因

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

対象とする原因の一例として、下記が想定される。

①意図的な原因

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

②偶発的な原因

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

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

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

③環境的な原因

災害、疾病　等

4. 役割

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

加えて、行動計画にて定めた「重要インフラ事業者等の経営層の在り方」及び図表１「『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」を参照の上、経営層の取組を「安全基準等」に規定する。

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

関係主体の在り方

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

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

重要インフラ事業者等の経営層の在り方

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

－上記の目的達成に当たっての情報セキュリティを中心とするリスク源の認識。

－上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。

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

－システムの運用状況の把握等を通じた当該方針の実行の有無の検証。

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

5. 「安全基準等」の公開

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

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

6. 対策項目

各重要インフラ分野における「安全基準等」の策定・改訂においては、指針本編の図表１「『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」に沿って列記した以下項目の採否を検討する。

6.1 「Plan（準備）」の観点

6.1.1 「方針」の観点

(1) 抽出した課題に基づくリスク評価

「Check（確認）・Act（是正）」において後述するリスク分析の結果に基づき、対応が必要なリスクとその対応の優先順位付けに係る意思決定及び「安全基準等」の策定・見直しに係る基礎情報の作成（リスク評価）を行う。

基礎情報をもとに、要求されるセキュリティ水準に照らしつつ、リスクの重大性、対応の実現性、リスクの保有状態からのリスクの拡大の可能性も考慮し、対応策の決定（リスク対応）を行う。

(2) 基本方針の策定・見直し

基本方針とは情報セキュリティ対策における根本的な考え方を示したものである。重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を規定する。

また、基本方針の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。

6.1.2 「規定」の観点

(1) 内規の策定・見直し

策定・見直しをした基本方針に基づき、個々の情報セキュリティ対策を体系化した上で、実施に係る考え方、ルール等について規定する。

また、内規の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。

(2) IT-BCP 等の策定・見直し

指針でいうIT-BCPとは、サービス維持レベルを下回る原因となるＩＴ障害発生時等において、情報システムを早期に復旧させ、サービスを継続して提供するために必要な行動手順で構成されるものである。ＩＴ障害発生時における優先業務、必要な対策を決定するまでの過程、業務継続方法、連携を要する関連部門等を規定する。

規定に際しては、広域災害・複合障害や新型インフルエンザ等の社会全体で対応が望まれる脅威、相互依存関係にある重要インフラからの障害波及、事業継続に必要なデータが特定の都市又は地域に集中している状況等についても考慮する。

なお、ＩＴ障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含む必要がある。

(3) 情報の取扱いについての規定化

取り扱う情報の重要度に応じて、機密性[10]、完全性[11]、可用性[12]の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、移送、提供、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。

なお、個人データについては、国民の安心感への影響に鑑みた取扱いを規定する。

6.1.3 「計画」の観点

(1) 情報セキュリティ対策に係るロードマップ及び計画の作成・見直し

方針の策定・見直し等に基づき、情報セキュリティ対策の具体的な達成目標が定められた際は、達成までの大まかなスケジュールであるロードマップ及びロードマップに基づき詳細化した計画を作成し、情報セキュリティ対策を進める。

6.1.4 「体制」の観点

(1) 予算・体制（委託先を含む）の確保

情報セキュリティ対策を計画に沿って進めるにあたり、システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保する。

(2) 人材育成・配置・ノウハウの蓄積

システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といったセキュリティ対策の水準を維持する

---

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

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

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

ための対応が必要である。

このことから、セキュリティ対策に係る担当者が変更となってもセキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行う。

また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＰＣ操作者も対象であることから、全社的に行う。

(3) 外部委託における対策（管理体制・契約・ＩＴ障害時）

重要情報の漏えいや悪意のあるシステム操作等については、外部からの意図的な原因のみならず内部の意図的又は偶発的な原因にて生じることがある。この内部の意図的又は偶発的な原因は、重要インフラ事業者等の従業員のみならず、委託先によるものも含まれる。

このことから、外部委託先に係る管理体制については、外部委託の適否及びその可能な範囲の明確化や委託先の選定基準に基づく外部委託契約、外部委託先の業務管理等にて行う。特に従業員と同じレベルの情報セキュリティ対策や教育の実施、ＩＴ障害発生時の協力についての合意は必要である。

6.1.5 「構築」の観点

(1) 情報セキュリティ要件の明確化・変更

重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機密性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。

その際、セキュリティホール、不正プログラム、DoS攻撃等の様々な脅威に対して導入を要する情報セキュリティ機能、未然防止対策及びＩＴ障害発生後の拡大防止・早期復旧の対策に要する機能をできる限り明示するとともに、そもそもの不正侵入を防止するための対策と許してしまった侵入がもたらす実被害[13]を防止するための対策についても明示する。

(2) 情報セキュリティ対策（技術）に係る設計・実装・保守

情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。

また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。

[13]実被害の例としては、情報窃取、情報システムの破壊等が挙げられる。

(3) 情報セキュリティ対策（運用）に係る設計・手順化・保守

情報セキュリティ要件に応じて情報セキュリティ対策を実装した情報システムの運用設計・手順書化を経て、安定した運用を実現する。また、情報セキュリティ対策の有効性を維持するため、認証に要するユーザー登録等の保守をもれなく行う。

6.2 「Ｄｏ（実働）」の観点

6.2.1 「平時・障害発生時共通」の観点

(1) 情報セキュリティ対策の運用（監視・統括）

構築した情報セキュリティ対策の運用状況については、定期的に責任者が把握していることを常態化する。

(2) 情報セキュリティ対策の運用状況把握

経営層は、情報セキュリティ対策の運用状況について、把握する。

6.2.2 「平時」の観点

(1) 情報セキュリティ対策の運用（予兆の把握、パスワード変更等）

情報システムの運用状況が平時の状況やしきい値と比して異なる状況にあること等を検知し、予兆を把握する。

また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等といった登録値の変更等を通じて、セキュリティ対策の水準を維持する。

加えて、情報セキュリティに係る教育を全社的に行う。

(2) 情報セキュリティ対策状況の対外説明

国民の安心感の醸成に資するため、重要インフラにおけるサービスの持続的な提供に向けた情報セキュリティ対策の取組について、提供範囲に留意しつつ、情報セキュリティ報告書やWebサイト等にて対外的な説明に努める。

6.2.3 「障害発生時」の観点

(1) ＩＴ障害に対する防護・回復

策定したIT-BCPを発動し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、ＩＴ障害をもたらした原因への適切な対処を可能とする。

(2) 情報セキュリティ対策状況の対外説明

ＩＴ障害の状況や復旧等の情報提供については、策定したIT-BCPに沿って、情報に基づく対応の5W1Hの理解の下、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う。

6.3 「Check（確認）・Act（是正）」の観点

6.3.1 「平時」の観点

情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に鑑みてリスクを特定（リスク特定）する。

特定したリスクについて、定性又は定量的な分析（リスク分析）を行い、事業にどのような損害を与えるかといった具体的な影響を決定する。

リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。

6.3.2 「障害発生時」の観点

ＩＴ障害対応（検知・回復）を通じた課題抽出として、取組の中で発見したリスク源となった脅威や脆弱性、影響を受けた維持すべきサービスレベル、脅威や脆弱性から生じた事象及びその結果をリスクとしての特定（リスク特定）を行う。

特定したリスクが事業に与えた損害を、リスク分析結果として改めて整理する。

リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。

資料３－３

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
（案）

平 成　　年　　月　　日

（本ページは白紙です。）

目次

（本ページは白紙です。）

Ⅰ．対策編の位置付け

本書「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定指針（第４版）対策編」（以下「指針対策編」という。）は、重要インフラ[1]における情報セキュリティ対策の適切かつ継続的な改善に資するために、具体性の充実及び国内外の諸規格との整合を念頭に置き、情報セキュリティ対策項目の具体例を PDCA サイクルに沿って採録した項目集である

指針対策編の活用に際しては、指針本編[2]の「Ⅱ『安全基準等』で規定が望まれる項目」も参照の上、具体的な対策項目のチェックリストとの位置付けの下、各「安全基準等」の策定・改訂に係る検討の一助となれば幸いである。

重要インフラ分野及び重要インフラ事業者等の特性を踏まえつつ、「安全基準等」が適切かつ継続的に改善がなされることを期待する。

[1] 「重要インフラ」とは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので重要インフラとして指定する分野」を指す。

[2] 「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）」を指す。

Ⅱ．具体的な情報セキュリティ対策項目の例示

対策項目の具体例については、指針本編の各対策項目の記載内容を引用（四角枠内）の上、指針本編の図表１「『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」に沿って採録する。

1. 「Plan（準備）」の観点

1.1 「方針」の観点

(1) 抽出した課題に基づくリスク評価

> 「Check（確認）・Act（是正）」において後述するリスク分析の結果に基づき、対応が必要なリスクとその対応の優先順位付けに係る意思決定及び「安全基準等」の策定・見直しに係る基礎情報の作成（リスク評価）を行う。
>
> 基礎情報をもとに、要求されるセキュリティ水準に照らしつつ、リスクの重大性、対応の実現性、リスクの保有状態からのリスクの拡大の可能性も考慮し、対応策の決定（リスク対応）を行う。
>
> （指針本編Ⅱ.6.1.1.(1)から引用）

○リスク評価

－リスク分析の結果に基づく対応が必要なリスクの決定

－上記対応の優先順位付けの決定

－「安全基準等」の策定や見直しに係る基礎情報の作成

○リスク対応

－「安全基準等」の策定や見直しに係る基礎情報に基づく対応策、見直し策の決定

(2) 基本方針の策定・見直し

> 基本方針とは情報セキュリティ対策における根本的な考え方を示したものである。重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を規定する。
>
> また、基本方針の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。
>
> （指針本編Ⅱ.6.1.1.(2)から引用）

○情報セキュリティ基本方針の策定

○情報交換の方針の策定

1.2 「規定」の観点

(1) 内規の策定・見直し

> 策定・見直しをした基本方針に基づき、個々の情報セキュリティ対策を体系化した上で、実施に係る考え方、ルール等について規定する。
>
> また、内規の策定・見直しに係る所管組織、目的、権限、構成員、見直し要件等についても規定する。
>
> （指針本編Ⅱ.6.1.2.(1)から引用）

○情報セキュリティ関係規定の策定、見直し

－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

－平時、障害発生時の指揮命令系統の明確化

・権限移譲、代行順位の決定　　等

－ＩＴ障害時の連絡不可能な場合（通信途絶等）の緊急時行動ルールの確定

－雇用契約時における情報の守秘や非開示の契約の締結

－利用者の責任

・パスワードの利用

・端末管理

・クリアデスク、クリアスクリーン　　等

－電子計算機、アプリケーション、通信回線及び通信回線装置の目的外利用の禁止

・閲覧可能なWebサイトの制限

・私的目的による使用の禁止　　等

－ネットワークのアクセス制御方針の策定

－ネットワーク構成等に係る情報の秘匿

－事業者支給以外のシステム関連機器による情報処理の制限

－証跡管理に係る利用者への周知

－違反への対処

－例外措置等

○情報セキュリティ人材の育成、活用、管理に係る規定の策定、見直し

－情報処理技術者試験、情報システムユーザースキル標準等の活用による社内人材育成マップ等の作成

－情報システムユーザースキル標準等の活用による社内教育コース等の整備

(2) IT-BCP 等の策定・見直し

> 指針でいうIT-BCPとは、サービス維持レベルを下回る原因となるＩＴ障害発生時等において、情報システムを早期に復旧させ、サービスを継続して提供するために必要な行動手順で構成されるものである。ＩＴ障害発生時における優先業務、必要な対策を決定するまでの過程、業務継続方法、連携を要する関連部門等を規定する。
>
> 規定に際しては、広域災害・複合障害や新型インフルエンザ等の社会全体で対応が望まれる脅威、相互依存関係にある重要インフラからの障害波及、事業継続に必要なデータが特定の都市又は地域に集中している状況等についても考慮する。
>
> なお、ＩＴ障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含む必要がある。
>
> （指針本編Ⅱ.6.1.2.(2)から引用）

○IT-BCPの策定と定期的な見直し

－IT-BCPの実施優先順位と判断基準の明確化

－IT-BCPの実施条件の明確化

－ＩＴ障害発生時の体制の整備

－ＩＴ障害に係る情報集約及び共有体制（所管省庁への連絡体制を含む）の整備

－ＩＴ障害時の連絡不可能な場合（通信途絶等）の緊急時行動ルールの確定

－IT-BCPと情報セキュリティ対策との間の整合性確保

(3) 情報の取扱いについての規定化

> 取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け（ランク付け）を行うとともに、作成、入手、利用、保存、移送、提供、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。
>
> なお、個人データについては、国民の安心感への影響に鑑みた取扱いを規定する。
>
> （指針本編Ⅱ.6.1.2.(3)から引用）

○情報の取扱規定の策定、見直し

－情報漏えいを抑止するための役割や責任分担の明確化

－守るべき情報の洗い出し方法

・体制

・洗い出し項目

・洗い出し基準　　等

－情報の分類

・分類の指針

・情報の機密性、完全性、可用性に基づく分類

・安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた分類）

・リスクアセスメント結果に応じた分類　　等

－情報（とりわけ重要情報）、情報システムについての格付け（ランク付け）

・情報の格付けと取扱制限の決定（その実施は情報の作成、入手時）

・情報の格付けと取扱制限の見直し

・情報のラベル付け及び取扱い

・格付け（ランク付け）の継承、変更手続き　　等

○情報の作成、入手時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報の目的外作成、入手禁止

－情報の台帳等作成

○情報の利用時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

・アクセス制御

・情報へのアクセス履歴の保存

・出力制御

・離席時対策（端末ロック等）　　等

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報の目的外利用の禁止

－情報の利用に関連する許可及び届出（作業責任者や手続きの明確化を含む）

○情報の保存時の取扱制限の決定、見直し

－格付け（ランク付け）及び取扱制限に従った情報の取扱い

・情報の保存期間に従った管理

・安全性が客観的に評価された暗号技術の利用による保護

・パスワードの適用

・アクセス制御

・更新履歴管理の取扱い

・記録媒体（とりわけ取り外し可能な媒体）の管理、保管

・複写

・データバックアップ（オンライン、媒体保管等）、遠隔地への保管

・電子署名

・内容表示の記号化（媒体等に保存情報内容が想定できるタイトル表示をすることの禁止）　　等

－書類等の保管ルール

・施錠可能なキャビネットへの保管

・鍵の管理　　等

－端末への資料保管ルールや制限

－持ち出しに係るルールや制限

－作業担当者の識別、認証、権限付与

－保護すべき情報の安全な場所への保管

・自然災害を被る可能性が低い地域への保管

・外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管

・バックアップの分散、隔地保管　　等

○情報の移送時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－外部（事業所外）での情報処理に係る規定の整備

－情報交換の方針及び手順

－情報の移送に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－移送時の手段の選択

－移送時の書面の保護対策

－移送時の電子的記録の保護対策

・パスワードの適用

・安全性が客観的に評価された暗号技術の利用

・電子認証　　等

○情報の提供時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－情報の提供に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－情報交換の方針及び手順

－提供時の付加情報の削除

○情報の消去時の取扱制限の決定、見直し

－作業担当者の識別、認証、権限付与

－情報の消去に関連する許可及び届出（作業責任者や手続きの明確化を含む）

－情報消去の方針及び手順

・電磁的記録の消去手続き

・消去の確認

・消去記録の保管　　等

○ＰＣや外部記録媒体の盗難、紛失、流失の防止

－入退室管理

－ＰＣや外部記録媒体の原則外部持ち出し禁止

－移動可能な機器や情報の盗難防止

○個人データの取扱い

－個人データ管理責任者の選定

－個人データを取り扱う職員の明確化

－役割及び責任と権限の明確化

・閲覧等の利用時における管理者の許可　　等

－退職後の個人情報保護規定の整備

－個人データの取扱状況を確認できる手段の整備

・個人データ取扱台帳の整備　　等

○情報漏えい発生時の対応方法

－責任や権限を有する担当者の選任

－緊急連絡体制の整備

－報告事項の明確化

－対応措置の明確化

－代替手段の明確化

1.3 「計画」の観点

(1) 情報セキュリティ対策に係るロードマップ及び計画の作成・見直し

> 方針の策定・見直し等に基づき、情報セキュリティ対策の具体的な達成目標が定められた際は、達成までの大まかなスケジュールであるロードマップ及びロードマップに基づき詳細化した計画を作成し、情報セキュリティ対策を進める。
>
> （指針本編Ⅱ.6.1.3.(1)から引用）

○情報セキュリティ対策に係るロードマップの作成、見直し

○情報セキュリティ対策に係る計画の作成、見直し

－IT-BCPにおける訓練計画の策定

1.4 「体制」の観点

(1) 予算・体制（委託先を含む）の確保

> 情報セキュリティ対策を計画に沿って進めるにあたり、システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保する。
>
> （指針本編Ⅱ.6.1.4.(1)から引用）

○体制の整備

－グループ会社も含めた情報セキュリティに係る組織体制の整備

・責任者

・責任部門

・委員会等の設置

・役割や責任分担の明確化　　等

－安全管理措置を講ずるための組織体制の整備

－ＩＴ障害発生時の体制の整備

・ＩＴ障害時の所管省庁への連絡体制

・ＩＴ障害に係る情報集約及び共有体制の整備

・緊急連絡ルールの確定

o 連絡先

o 連絡事項

o 連絡手段　　等

－DoS攻撃時等における通信事業者との連携体制の整備

－システム統合に伴うリスク管理体制の構築

○人的資源の管理体制の整備

－雇用条件の明示

－守秘契約の締結

－懲戒手続等

(2) 人材育成・配置・ノウハウの蓄積

システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といったセキュリティ対策の水準を維持するための対応が必要である。

このことから、セキュリティ対策に係る担当者が変更となってもセキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行う。

また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやＰＣ操作者も対象であることから、全社的に行う。

（指針本編Ⅱ.6.1.4.(2)から引用）

○ＩＴ障害発生時に対応ができる人材の計画的な育成

○情報セキュリティ対策や情報漏えい防止に係る教育、訓練

－計画の策定

○IT-BCPの教育及び教育記録の保管

(3) 外部委託における対策（管理体制・契約・ＩＴ障害時）

> 重要情報の漏えいや悪意のあるシステム操作等については、外部からの意図的な原因のみならず内部の意図的又は偶発的な原因にて生じることがある。この内部の意図的又は偶発的な原因は、重要インフラ事業者等の従業員のみならず、委託先によるものも含まれる。
>
> このことから、外部委託先に係る管理体制については、外部委託の適否及びその可能な範囲の明確化や委託先の選定基準に基づく外部委託契約、外部委託先の業務管理等にて行う。特に従業員と同じレベルの情報セキュリティ対策や教育の実施、ＩＴ障害発生時の協力についての合意は必要である。
>
> （指針本編Ⅱ.6.1.4.(3)から引用）

○委託に係る対応項目の明確化

－委託目的

－委託可能な業務範囲

－委託元と委託先双方の責任分界点

－個人データを扱う場合の要件

－委託先選定基準

・経営状況

・信頼度

・受託実績

・技術水準

・情報セキュリティ対策の実施状況（諸規定の整備を含む）

・障害発生時の対応力　　等

－委託先選定手続き

－委託に係る契約手続き

○委託先との基本契約の締結

－委託先の情報セキュリティ対策（委託元と同等以上）

－機密保持（機密保持契約）、情報やデータの目的外利用の禁止（確認書の提出を含む）

－再委託の制限

－委託管理責任者の設置

－委託業務内容、委託業務の執行場所、作業者、作業内容の特定（ＩＴ障害発生

時の対処方法を含む）

－監査への協力

－契約内容の遵守状況についての委託元による確認

－契約内容が遵守されない場合の対処（損害賠償請求等）

－契約の解約や解除に係る事項

－契約終了時の情報の返却及び消去

○委託契約時における情報の守秘や非開示の契約の締結

○委託先との取決めに係る合意形成

－委託先による契約の遵守方法及び管理体制

－施設全体の運用業務全般にわたる取決め

○委託先管理

－提供する情報の最小化

－委託先に求める情報セキュリティ対策項目の周知、遵守（遵守方法を含む）

－取り扱う情報・情報システムに応じた情報セキュリティ対策の選定

・委託先がアクセス可能な情報・情報システムの制限

・データ等の取扱いに係る事項（保管場所、保管方法）

・保守用専用アカウントの設定

・委託先が再委託する際の対応策の整備　　等

－委託先作業時の申請手続き

－委託先による情報セキュリティ対策の実施状況の確認

・作業報告書の提出手続き　　等

－納品検査時の情報セキュリティ対策の確認

－定期点検、監査の実施

○ＩＴ障害発生時の対応策の整備

－重要インフラ事業者等としての対処方法の明示

・責任分界点の明示

・行動基準の規定

・外部要因による障害の防止

・問題発生時の対処の合意

o 他システムへの影響調査

・事実関係の確認

・委託先との情報共有

・緊急時及び平常時の連絡体制の整備（業界内、ベンダー等）

・利用者への説明責任に係る認識の共有

・ＩＴ障害対応の訓練、演習の計画及び委託先を含めた実施　　等

－ＩＴ障害発生時における委託先の措置

・対処方法の事前の通知

・連絡体制の整備

・異常検知ツールの活用

・障害箇所の切離し

・原因の特定

・修正プログラムの適用

・異常状態（攻撃を含む）の記録、保存　　等

1.5 「構築」の観点

(1) 情報セキュリティ要件の明確化・変更

重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機密性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。

その際、セキュリティホール、不正プログラム、DoS攻撃等の様々な脅威に対して導入を要する情報セキュリティ機能、未然防止対策及びＩＴ障害発生後の拡大防止・早期復旧の対策に要する機能をできる限り明示するとともに、そもそもの不正侵入を防止するための対策と許してしまった侵入がもたらす実被害を防止するための対策についても明示する。

（指針本編Ⅱ.6.1.5.(1)から引用）

○不正侵入防止対策

－主体認証

・機能の選択、導入

o 知識認証

o 所有物認証

o 生体認証

o 多要素認証　　等

・主体認証情報の管理

o 安全性が客観的に評価された暗号技術の利用

o 認証パスワードの最低文字数の制限

o ＩＤ毎に異なる認証パスワードの設定

o 認証パスワードの定期変更　　等

・利用者ＩＤの管理

o 個人単位のＩＤ付与

o 不要ＩＤの削除

o ＩＤの不正使用防止機能の導入　　等

・不正使用検知時における主体認証の利用停止措置

－アクセス制御

・利用者属性以外に基づくアクセス制御機能の導入

o 利用時間や利用時間帯による制御

o 利用端末の識別

o 強制アクセス制御　　等

・利用者アクセスの管理機能の導入

o 利用者登録

o 特権管理

o 利用者パスワードの管理

o 利用者アクセス権のレビュー　　等

－権限管理

・権限管理機能の導入

・利用者ＩＤと主体認証情報の付与管理機能の導入

・利用者ＩＤと主体認証情報における代替手段等の適用　　等

－不正侵入対策

・不正アクセスの監視、検出機能（IDS）の導入

・不正アクセスの監視、検出、侵入阻止機能（IPS）の導入

・通信フィルタリング機能の導入

o ファイアウォール

o Webアプリケーションファイアウォール（WAF）　　等

・外部ネットワークからの遮断等の機能の導入

・端末やゲートウェイ等におけるマルウェア対策ソフトウェアの導入、メンテナンスの実施

・未使用通信ポート等の閉鎖（非活性化）、マクロ実行の抑制

－他情報システムとの独立、接続点の最小化

－マルウェア対策

・ＯＳ／アプリケーションのセキュリティ設定

・マルウェア対策ソフトウェアの導入、パターンファイルの更新機能導入　等

○実被害防止対策

－不正使用対策

・取引制限機能の導入

・事故時の取引禁止機能の導入

・電子的価値の保護機能の導入

・暗号鍵の保護機能の導入

・電子メールの不正使用防止機能の導入

・Webサイト閲覧の不正使用防止機能の導入　　等

－データ漏えい防止対策

・暗証番号等のアクセス制限情報等の漏えい防止機能の導入

・相手端末確認機能の導入　　等

－破壊や改ざんの防止対策

・排他制限機能の導入

・アクセス制限機能の導入

・不良データ検出機能の導入

・ファイル突合機能の導入　　等

－負荷分散

・トラフィックの分散処理

・本番機の多重化、予備機の設置

・負荷状態の監視制御機能の充実　　等

－冗長化

・通信経路の迂回措置

・通信回線の冗長化

・ネットワークの適切な管理や制御

・予備機の設置

・代替手段の整備

・代替手段及び代替手段に必要なシステムの準備

o 代替情報システムの作業手順書策定　　等

・アプリケーションを含めた情報システムの冗長対策

－早期発見に向けた対策

・不正取引の検知機能の導入

・異例取引の監視機能の導入

・データ改ざん（書換え）の検出機能の導入

・障害の検出機能の導入

・障害箇所の切分け機能の導入　　等

－早期回復に向けた対策

・障害時の縮退、再構成機能の導入

・取引制限機能の導入

・リカバリー機能の導入　　等

－証跡管理

・証跡管理機能の導入実施

・電子計算機、通信回線装置及び通信回線の監視と記録

・証跡の取得と保存

・取得した証跡の点検、証跡の分析及び報告　　等

○情報システム施設における安全区画の確保

－バックアップセンターの設置

－遠隔地でのバックアップ媒体保管

－災害を受けにくい場所への設置

－物理的セキュリティ境界の設定

－電子計算機及び通信回線装置のセキュリティ確保

・不正操作対策

・盗み見等の防止対策　　等

－安全区域内のセキュリティ管理策

・身分証明書の携帯、常時視認

・物品等の持込み、持ち出しの情報セキュリティ責任者の承認、記録

・ＰＣや外部記録媒体等の持込み制限

・作業の監視、モニタリング　　等

－防犯対策

・侵入防止装置の設置

・赤外線検知装置の設置

・トラップセンサーの設置

・記録用機器の使用制限

・盗難防止装置の設置　　等

○情報システム施設における防災対策

－建物の耐震や免震構造及び防火構造化

－設備の移動、転倒等防止対策

－防火対策

－落雷対策

－防水対策

－警報装置の設置

－非常口及び非常灯設置

－自家発電装置、無停電電源装置、予備電源の確保

－空調（加湿を含む）設備の冷却水の備蓄　　等

○情報システム施設に係る入退出管理（物理的な不正侵入の防止）

－障壁の設置

－最小限の施設表示

－施錠運用の実施

－主体認証（入退出者の認証）機能の導入

－継続的に立ち入る者の承認

－侵入監視装置の設置

－入退出履歴の記録

－訪問者、清掃業者及び物品の搬出入業者の入退出管理

・身分の記録

・入室審査手順

・立入り制限区域の設定

・職員等の立会い、付添い運用

・ストラップ、ＩＤカード

・情報システムに接触できない場所での搬入物品等の受渡し　　等

○電子計算機に係る対策

－情報システムの受入れに係る対策

・必要な要求事項（受入れ基準）の明確化

・受入れ前試験の合否判定基準の明確化

・受入れ前試験の実施　　等

－システム統合や更新に伴う移行基準の明確化

－ソフトウェア（アプリケーション）の利用に係る対策

・端末で利用可能なソフトウェアの制限

・利用するソフトウェア（アプリケーション）の使用者の責任と権限の明確化

・利用するソフトウェア（アプリケーション）の取扱手順の規定

・利用するソフトウェア（アプリケーション）の利用状況の確認　　等

－記録媒体を持たない端末の利用

－端末の盗難防止対策

－モバイル端末に対するセキュリティ機能の装備

・ワンタイムパスワード機能

・モバイル端末で利用する電磁的媒体における安全性が客観的に評価された暗号化機能

・遠隔ロック機能

・遠隔消去機能　　等

－無線LAN使用時の対策

・安全性が客観的に評価された暗号技術の利用

・主体認証機能

・機器識別機能

・証跡管理機能

・アクセス制限機能

・他ネットワークの利用制限機能

・機密性確保

・接続（利用）可能な機器の管理　　等

－リモートアクセス時の対策

・主体認証機能

・証跡管理機能

・アクセス制限機能

・機密性確保

・利用可能な機器の管理　　等

○バックアップ稼働計画、復帰計画の策定

○内部関係者による取扱いミス等を低減させるための措置

－取引制限機能の導入

－事故時の取引禁止機能の導入

－電子的価値の保護機能の導入

－暗号鍵の保護機能の導入

－電子メールの不正使用防止機能の導入

－Webサイト閲覧の不正使用防止機能の導入

－外部ネットワークからのアクセス制限

－不正侵入防止機能の導入　　等

○内部関係者による情報漏えいを抑止するための措置

－入退出管理

－常時監視設備（カメラ）等の設置　　等

○内部からの攻撃の監視

－職員の監督とモニタリング　　等

○重要情報の内部漏えい、盗難、紛失、流出への対策

－移動可能な機器の盗難防止策

－情報盗難の防止等の措置　　等

(2) 情報セキュリティ対策（技術）に係る設計・実装・保守

> 情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。
>
> また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。
>
> （指針本編Ⅱ.6.1.5.(2)から引用）

○対応対象となったセキュリティ要件の実装

○信頼性設計、処理増加等を考慮した情報システムの余裕設計

○セキュリティ要件の実装に付随する機器に係る対応

－開発環境と本番環境の分離

－供給元及び更新情報、保守期間等が明確な機器の利用

－サプライチェーンにおける情報セキュリティを考慮した機器の調達（信頼のできるベンダーから調達する等）

－客観的に評価された製品等の導入の検討

－安全区域への設置

－防災対策

・設備の転倒等防止対策

・防火対策

・落雷対策

・防水対策

・警報装置の設置

・非常口及び非常灯設置　　等

－自家発電装置、無停電電源装置、予備電源の確保

－空調（加湿を含む）設備の冷却水の備蓄

－サーバー装置における安全性が客観的に評価された暗号技術の利用（遠隔保守時）

－改ざん防止対策

○セキュリティ要件の実装に付随する性能に係る対応

－電子計算機の十分な性能（処理能力、容量、拡張性）の確保

－通信性能の確保

○セキュリティ要件の実装に付随するネットワークに係る対応

－外部ネットワークとの接続制限（プロキシ経由等）

－内部と外部のネットワークの分離

－制御系ネットワークの分離

－不要なポートの閉塞

－無許可ネットワーク、外部ネットワーク接続の禁止

－公開するサーバー上に保存する情報の制限

－改ざん防止対策

－盗聴防止対策

－ルーターによるDoS攻撃対策　　等

○セキュリティ要件の実装に付随する通信に係る対応

－相手端末確認機能の導入

－未承認機器からの通信の遮断

－電子証明書による正当性の証明

－通信情報（データ）における安全性が客観的に評価された暗号技術の利用

－遠隔地からの保守（リモートメンテナンス）時の対策

－外部からの侵入が困難な回線の選択

－原則公衆回線からの接続の禁止（例外時はコールバックやユーザーの限定）

－不特定多数が接続するネットワークとの接続禁止　　等

○セキュリティ要件の実装に付随するアプリケーションに係る対応

－不要なアプリケーションの利用禁止

－不要な機能の無効化、削除　　等

○セキュリティ要件の実装に付随する電子メールやWebに係る対応

－電子メールの対策や制限

・添付ファイルの保護

・不正中継禁止

・送受信容量の制限

・自動転送の制限

・業務外利用の禁止

・送信先アドレス漏えいの防止

・電子署名機能の導入

・安全性が客観的に評価された暗号技術の利用

・迷惑メールフィルターの導入　　等

－電子メール送信時及び受信時の送信ドメイン認証（ＳＰＦ等）の導入

－Webにおける特殊文字使用の禁止、無効化

－Webにおける脆弱性のある作り込みの回避

－攻撃に利用されるWebサーバー情報の送信を防ぐ対策

○セキュリティ要件の実装に付随するその他に係る対応

－手順書等における文書整備、変更管理手順の明確化

・仕様書、設計書

・構成要素のセキュリティ

・マニュアル

・機種や利用ソフトウェアの種類及びバージョン情報

・管理者、利用者情報

・利用者管理、利用者ＩＤ管理情報

・構成要素のセキュリティに関する手順　　等

－変更管理

－運用終了に伴う廃棄計画や手順の策定、設計や見直しの実施

－電磁的記録（媒体）の情報抹消

－パンデミック対策（コンピューターセンターのオペレーター要員の確保等）

－マルウェア対策の対応内容の記録

(3) 情報セキュリティ対策（運用）に係る設計・手順化・保守

> 情報セキュリティ要件に応じて情報セキュリティ対策を実装した情報システムの運用設計・手順書化を経て、安定した運用を実現する。また、情報セキュリティ対策の有効性を維持するため、認証に要するユーザー登録等の保守をもれなく行う。
>
> （指針本編Ⅱ.6.1.5.(3)から引用）

○予兆検知時、ＩＴ障害発生時や緊急時の対応（早期発見、早期回復）手順の整備

－監視

－障害の検出

－異常発見時における管理者への連絡

－障害箇所の切分け

－障害時の縮退、再構成

－取引制限

－リカバリー　　等

○運用体制の決定、周知

－管理者

－障害時の連絡体制

－委託先窓口等連絡先

－通常時以外の特別体制　　等

○取扱手順等の策定

－情報の取扱手順

－利用する外部作成ソフトウェアのセキュリティホールに係る定期チェック手順

－マルウェアに係る定期チェック手順

－HTMLメール使用時の注意　　等

○情報漏えい発生時の対処手順

－事実関係の把握

－漏えい情報の範囲の特定

－システム、端末における情報漏えい経路の特定の調査

－情報漏えい継続の阻止、被害の最小化

・対象通信を遮断するための運用フロー等の整備

・対象サーバー等をネットワークから隔離するための運用フロー等の整備等

－本人への通知

－事実関係の公表、広報

－所管省庁への報告

－関係機関への周知

－情報漏えいに至った経緯や原因等の解析

－再発防止策の検討と対策の実施

－情報漏えい事案等への対応状況の記録、分析

2. 「Ｄｏ（実働）」の観点

2.1 「平時・障害発生時共通」の観点

(1) 情報セキュリティ対策の運用（監視・統括）

> 構築した情報セキュリティ対策の運用状況については、定期的に責任者が把握していることを常態化する。
>
> （指針本編Ⅱ.6.2.1.(1)から引用）

○実装したセキュリティ対策機能の運用

○セキュリティ対策機能に係る運用

－電子計算機、通信回線装置及び通信回線の異常（非日常）状態、不正行為、不正アクセス及び不正トラフィックの監視、検知、報告

・アクセスログの取得、分析、保管

・侵入検知システム（IDS）による検知

・マルウェア対策ソフトウェアによる定期チェック　　等

－証跡の分析、結果報告

－通常時や繁忙時のシステムの性能、容量、処理能力等の稼働状態監視による異常検知、報告

－運用管理記録、障害記録、作業記録の作成、管理、報告

－外部委託業者の作業管理

(2) 情報セキュリティ対策の運用状況把握

> 経営層は、情報セキュリティ対策の運用状況について、把握する。
>
> （指針本編Ⅱ.6.2.1.(2)から引用）

○情報セキュリティ対策の運用状況に係る報告事項の確認

2.2 「平時」の観点

(1) 情報セキュリティ対策の運用（予兆の把握、パスワード変更等）

> 情報システムの運用状況が平時の状況やしきい値と比して異なる状況にあること等を検知し、予兆を把握する。
>
> また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等といった登録値の変更等を通じて、セキュリティ対策の水準を維持する。
>
> 加えて、情報セキュリティに係る教育を全社的に行う。
>
> （指針本編Ⅱ.6.2.2.(1)から引用）

○実装したセキュリティ要件機能の運用

○セキュリティ対策機能に係る運用

－情報システムの定期的な点検及び必要に応じた更新

－データ改ざん有無の定期的な検査

－利用可能な通信回線、通信方法の制限

－情報システム内の時刻同期化

－情報システムの構成管理（機器管理、外部接続管理）

－情報システムの構成変更の定期的な確認

－定期的なバックアップ取得とバックアップ媒体の安全管理（遠隔地保管等）

－定期的なパスワードの変更

－マルウェア対策ソフトウェアの適用

・マルウェア情報の収集

・マルウェア対策ソフトウェアによる定期チェック

・定義ファイルの更新

・対応内容の記録

－利用するＯＳ、ソフトウェア等の定期的な調査、把握

－利用するＯＳ、ソフトウェア等の管理、同バージョン管理

－利用するＯＳ、ソフトウェア等の脆弱性対応

・情報収集

・対応計画の策定

・定期チェック

・セキュリティパッチの適用

・対応内容の記録　　等

－無線LANにて接続可能な機器の管理

－ソフトウェアダウンロード時の電子署名による配布元の確認

－外部委託業者の作業の確認、点検

－入退室管理

・施錠

・主体認証（入退出者の認証）

・記録

・継続的に立ち入る者の承認

・身分証明書の携帯、常時視認

・侵入監視装置による監視

・コンピューターや外部記録媒体等の持込み制限　　等

－訪問者、清掃業者及び物品の搬出入業者の管理

・職員等の立会い、付添い

・ストラップ、ＩＤ カードの情報システムに接触できない場所での受渡し

・作業の監視　　等

－利用する機器、利用者及び識別コードの管理

○規定に従ったＰＣや外部記録媒体の盗難や紛失の防止に係る運用

○情報取扱手順等の遵守状況の確認

－対象とする保存文書へのパスワードの適用

－安全性が客観的に評価された暗号技術の利用

－電子メール送信の際の宛先確認　　等

○情報セキュリティ対策や情報漏えい防止に係る教育及び訓練の実施

－教育及び訓練実施記録の保管　　等

○セプターカウンシルの活用等によるリスクコミュニケーションの実施

○情報漏えい発生時の措置

－管理者への連絡

－適切な処置の実施　　等

(2) 情報セキュリティ対策状況の対外説明

> 国民の安心感の醸成に資するため、重要インフラにおけるサービスの持続的な提供に向けた情報セキュリティ対策の取組について、提供範囲に留意しつつ、情報セキュリティ報告書やWebサイト等にて対外的な説明に努める。
>
> (指針本編Ⅱ.6.2.2.(2)から引用)

○情報セキュリティ報告書、CSR報告書、各種ディスクロージャ資料等の作成

○Webサイト、電子メール等による情報提供

2.3 「障害発生時」の観点

(1) ＩＴ障害に対する防護・回復

> 策定したIT-BCPを発動し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、ＩＴ障害をもたらした原因への適切な対処を可能とする。
>
> (指針本編Ⅱ.6.2.3.(1)から引用)

○情報システムの稼働監視（トラブル時の復旧時間、再発防止策の実施状況）

－不正アクセスの監視

－不正トラフィックの監視　　等

○対応体制の準備

－重要拠点（指揮拠点）の確保

－複数の連絡手段の準備、確保

－自家発電装置等で使用する燃料の確保　　等

○早期復旧に向けた対応

－障害箇所の切分け

－障害時の縮退、再構成の実施

－バックアップシステムの整備、代替手段及び代替手段に必要なシステムの準備

－通信途絶時でも必要最小限の業務を継続するための準備

－障害時の取引制限の実施

－障害時のリカバリー機能の適用

－取得した証跡に基づく追跡、分析及び報告

－様々な主体が提供する災害や障害発生時の情報サービスの活用　　等

○攻撃記録の保存

○攻撃に係る情報の関係機関との共有

○対外的な情報発信、情報共有

○広報、利用者からの問合せへの対応

(2) 情報セキュリティ対策状況の対外説明

> Ｉ Ｔ障害の状況や復旧等の情報提供については、策定したIT-BCPに沿って、情報に基づく対応の5W1Hの理解の下、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う。
>
> （指針本編Ⅱ.6.2.3.(2)から引用）

○サービス停止状況、復旧（見込み）情報の提供

3. 「Check（確認）・Act（是正）」の観点

3.1 「平時」の観点

> 情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に鑑みてリスクを特定（リスク特定）する。
>
> 特定したリスクについて、定性又は定量的な分析（リスク分析）を行い、事業にどのような損害を与えるかといった具体的な影響を決定する。
>
> リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。
>
> （指針本編Ⅱ.6.3.1から引用）

○情報セキュリティ対策の運用を通じた課題抽出

－業界内での相互支援に備えたデータ形式の標準化推進　　等

○内部監査や外部監査を通じた課題抽出

－自己点検の実施

・防災対策の定期的な確認　　等

－内部監査による情報セキュリティ監査等の実施

－外部監査による情報セキュリティ監査等の実施　　等

○ＩＴに係る環境変化に伴う脅威に対する課題抽出

－平時からの情報収集の実施

－継続的な情報収集

－新たな脅威が顕在化した時点で速やかに検討体制が構築できるための準備

－「暗号危殆化」に係る継続的な情報収集の実施（CRYPTREC暗号リスト等参照）

－「IPv6移行」に係る継続的な情報収集と実装検討の実施　　等

○演習や訓練を通じた課題抽出

－システム統合や更新に伴う情報システムの業務運営体制の検証

－IT-BCPに係る訓練の実施、訓練実施記録の保管

－障害時、緊急時を想定した訓練（復旧テスト等）の実施　　等

○リスク特定

－課題抽出の中でのリスク源となり得る脅威や脆弱性の発見

－リスク源の影響を受けるサービスレベルの特定

－脅威や脆弱性から生じ得る事象とその結果をリスクとして特定　　等

○リスク分析

－特定したリスクに対する定性的又は定量的な分析

－事業にどのような損害を与えるか等の具体的な影響の決定　　等

3.2 「障害発生時」の観点

> ＩＴ障害対応（検知・回復）を通じた課題抽出として、取組の中で発見したリスク源となった脅威や脆弱性、影響を受けた維持すべきサービスレベル、脅威や脆弱性から生じた事象及びその結果をリスクとしての特定（リスク特定）を行う。
>
> 特定したリスクが事業に与えた損害を、リスク分析結果として改めて整理する。
>
> リスク特定及びリスク分析の結果については、前述の「Plan（準備）」のリスク評価及びリスク対応にて用いる。
>
> （指針本編Ⅱ.6.3.2から引用）

○ＩＴ障害対応（検知・回復）を通じた課題抽出

資料３－４

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～

（案）

平 成　　年　　月　　日

（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年〇月〇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。

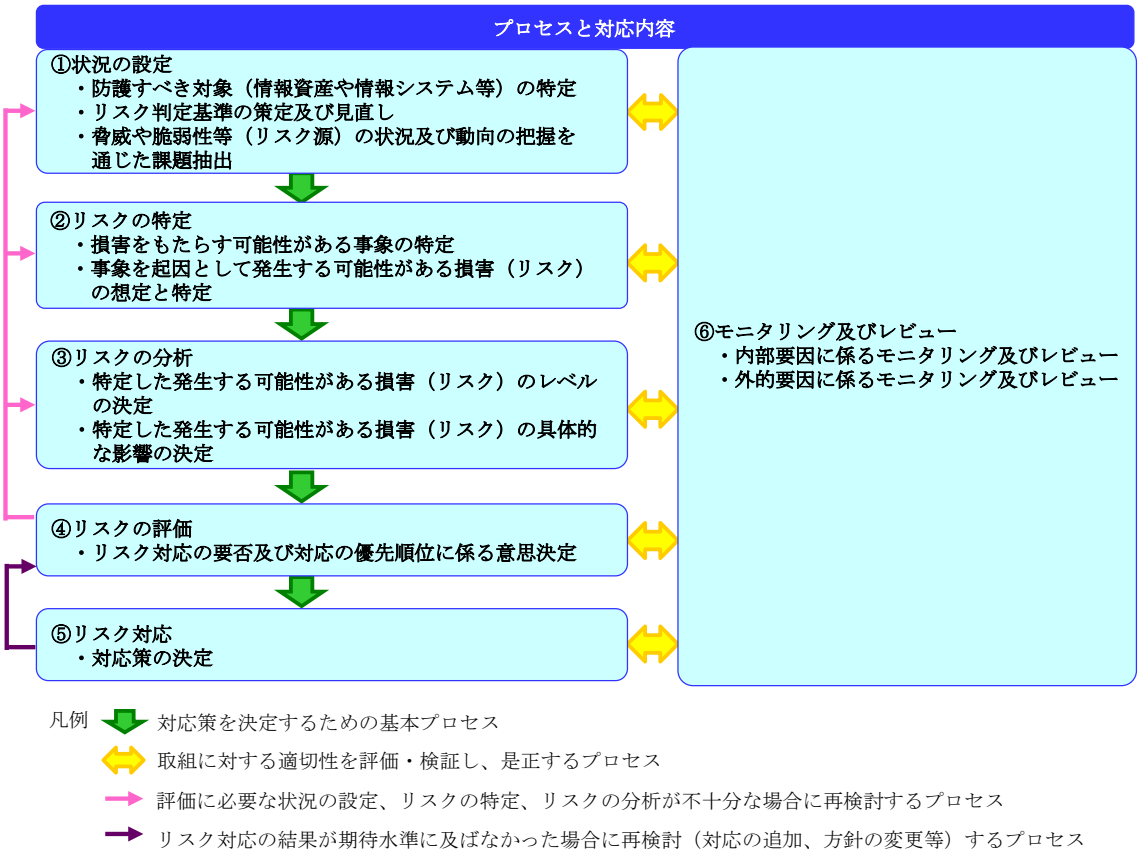
記載内容については、指針本編、指針対策編と同様に行動計画の「図表３　『重要インフラ事業者等の対策例』と各対策に関連する『国の施策例』」（指針手引書の図表３として再掲）に照らし、ISO/IEC27005:2011の考え方をベースに、図表２に示す各プロセスについて解説するものです。

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。

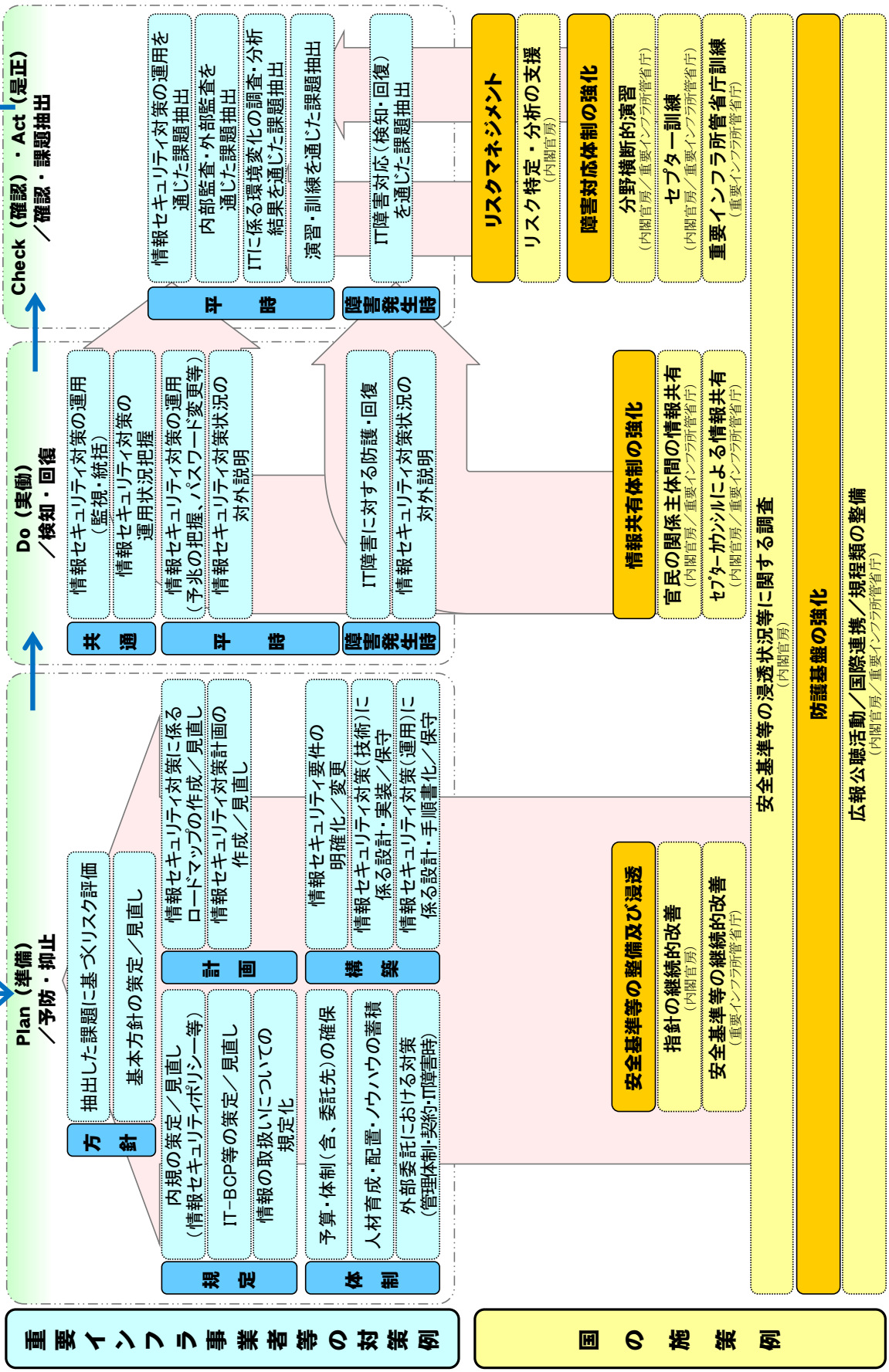
[6] 指針手引書の正式名称は「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第１版）」といいます。

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。

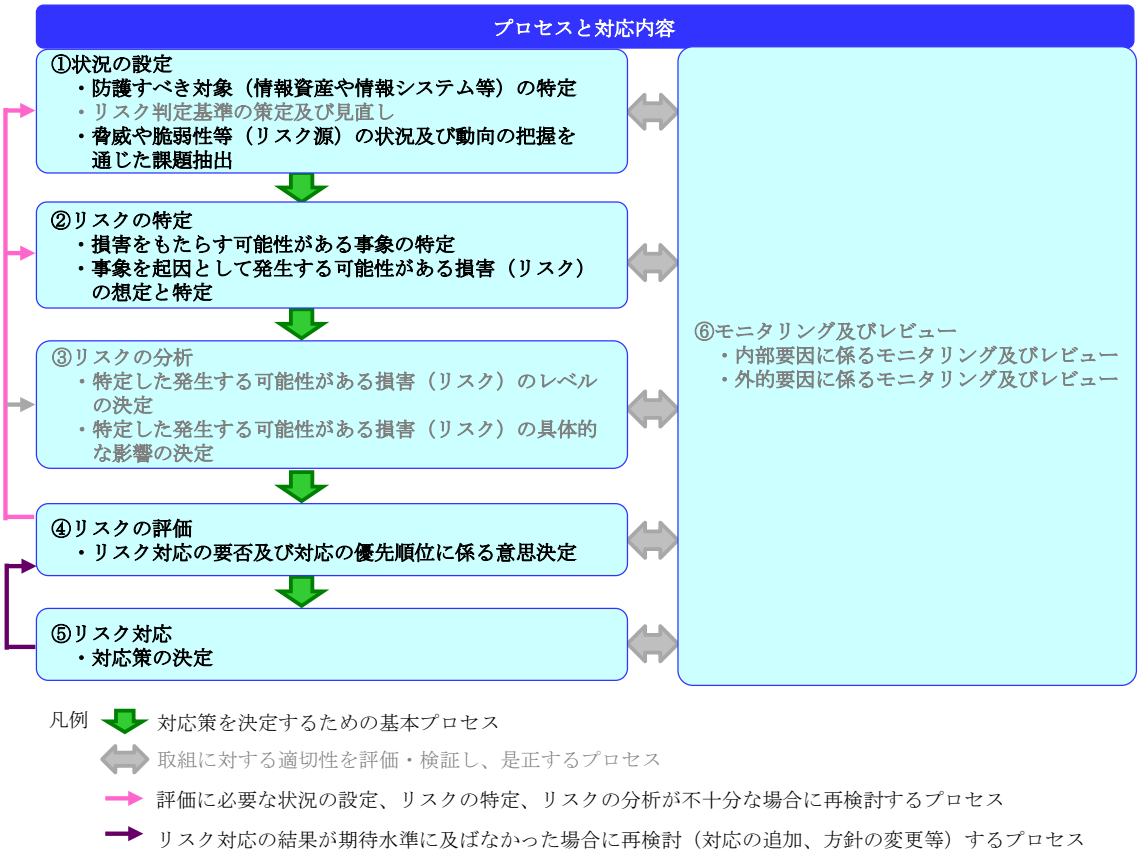
図表３「重要インフラ事業者等の対策例」と各対策に関連する「国の施策例」



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

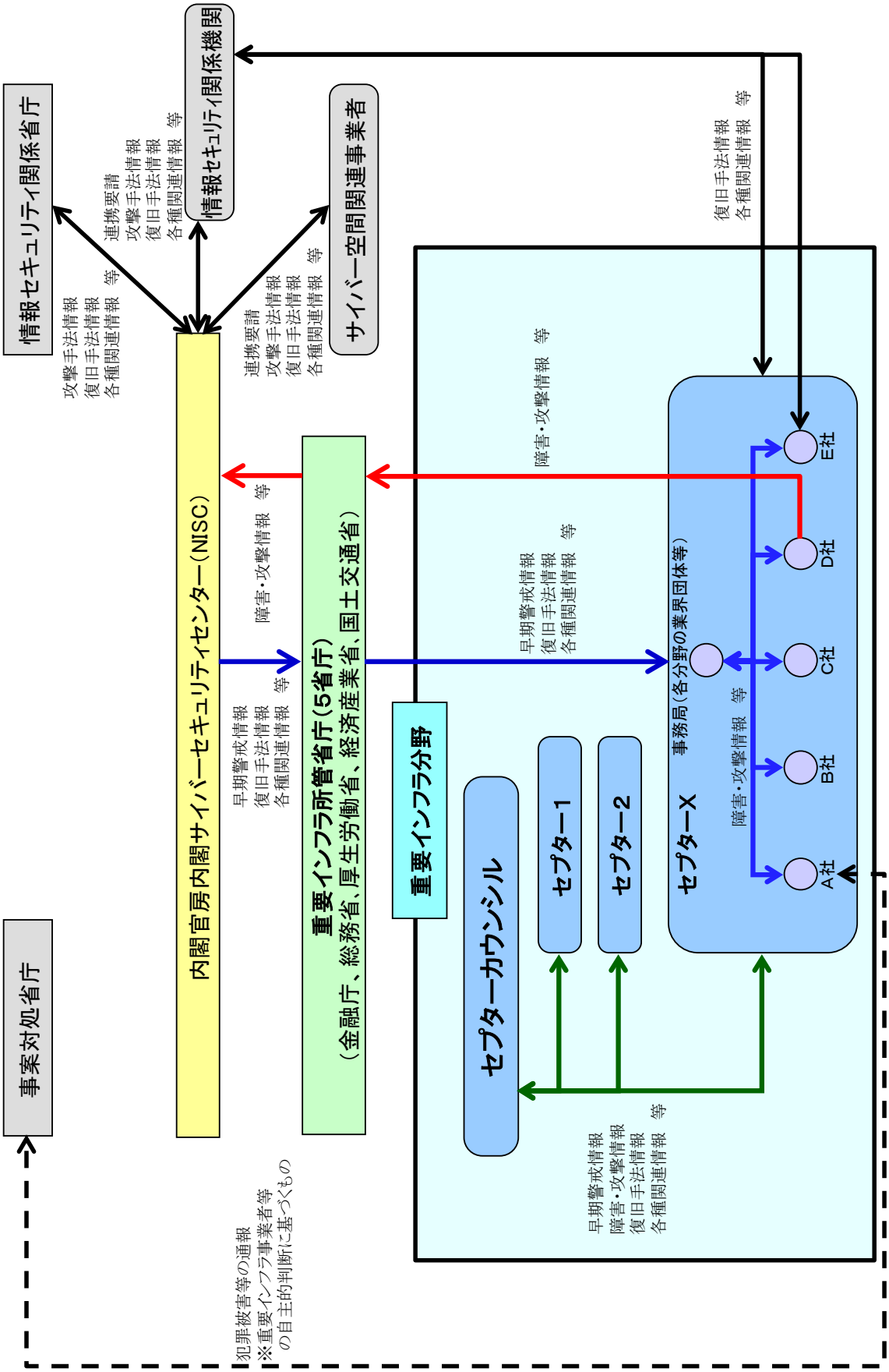
・セプター　　等

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。

資料３－５

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

（改定案）

平 成 ２ ６ 年 ５ 月 １ ９ 日
情報セキュリティ政策会議決定
平 成 ２ ７ 年 ５ 月 ２ ５ 日
サイバーセキュリティ戦略本部改訂

（本ページは白紙です。）

目次

Ⅰ．総論

1. 行動計画策定に当たっての認識

重要インフラに係る行動計画は、重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画であり、内閣官房情報セキュリティセンター[1]（NISC）設立以前から「重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月情報セキュリティ対策推進会議決定）」が策定される等、我が国の重要インフラの情報セキュリティ対策に関する施策の根幹を成すものとして策定してきた。

NISC設立後の行動計画については、2005年に情報セキュリティ政策会議が提示した、ＩＴ障害から重要インフラを防護し、重要インフラ事業者等の事業継続性を確保するために取るべき対策についての基本的方向性を踏まえ、同年に「重要インフラの情報セキュリティ対策に係る行動計画」（以下「第１次行動計画」という。）を決定した。この第１次行動計画に基づき、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し、政府及び重要インフラ10分野等からなる関係主体による取組が開始された。

さらに、第１次行動計画において構築された重要インフラの基本的な情報セキュリティ対策や官民の情報共有の枠組みを基礎とし、国として取り組むべき施策を示した「重要インフラの情報セキュリティ対策に係る第２次行動計画」（以下「第２次行動計画」という。）を2009年に決定した。第２次行動計画では、第１次行動計画における主な施策である「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析[2]」、「分野横断的演習」を引き続き実施しつつも、刻々と変化する社会環境や技術環境に的確に対応するため、新たに「環境変化への対応」についての施策を追加した。

このように、我が国の重要インフラ防護は、特別行動計画から見て13年間、現行の形態となった行動計画でも８年間の実績を有しており、確固たる情報共有体制の構築を始め、５つの施策に基づく対策が着実に進展したものと評価できる。

したがって、本行動計画策定においては、「サイバーセキュリティ戦略（2013年６月情報セキュリティ政策会議決定）」を踏まえつつ、第２次行動計画における施策群の評価によって得られた良好事例、要改善事例等の知見を的確に反映した。

また、東日本大震災発災時のシステム障害、データ滅失等への対応において得られた知見等の活用に加え、刻々と変化する社会環境・技術環境、近年の複雑化・巧妙化するサイバー攻撃の趨勢への適切な対応を反映した。

---

[1] 平成 27 年１月９日に、「内閣サイバーセキュリティセンター」に改組。

[2] 第１次行動計画では、「相互依存性解析」という施策名である。

2. 重要インフラ防護の目的の明確化

本行動計画の実施の前提として、重要インフラ防護の目的を明確化し、関係者間で認識を共有することが必要である。

サイバーセキュリティ戦略については、「情報の自由な流通の確保」、「深刻化するリスクへの新たな対応」、「リスクベースによる対応の強化」及び「社会的責務を踏まえた行動と共助」を基本的な考え方において示しており、第２次行動計画の目的はサイバーセキュリティ戦略と整合している。

したがって、第２次行動計画における目的を継承しつつも、「重要インフラにおけるサービスの持続的な提供のために行う」ことを追加し、重要インフラ防護の目的を更に明確化した。

○「重要インフラ防護」の目的

・ 重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する。

○基本的な考え方

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

・ 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。

・ 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。

・ 取組に当たっては、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に限界があることから、他の関係主体との連携をも充実させる。

3. 第２次行動計画の施策の成果と課題

第２次行動計画は、次の５つの施策から構成されている。

［1］安全基準等の整備及び浸透
［2］情報共有体制の強化
［3］共通脅威分析
［4］分野横断的演習
［5］環境変化への対応

以下に、各施策の成果と課題の概要を示す。

3.1 成果

今回、これら施策群の評価を行うに際し、第２次行動計画は2009年時点での重要インフラを取り巻く最新知見を踏まえて策定されたものであることを考慮し、５つの施策に対して第２次行動計画における評価指標に照らして効果について評価を行った。その結果、所期の目標については、以下に示すとおり一定の成果を挙げたと評価できるものであった。

安全基準等の整備及び浸透については、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指した結果、指針と安全基準等の一体的・安定的な見直しサイクルを確立し、情報セキュリティ対策の推進等を強化した。

情報共有体制の強化については、刻々と変化する重要インフラの情報セキュリティを取り巻く社会環境や技術環境及び複雑・巧妙化するサイバー攻撃等に対応することを目的に、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター内・各セプター間における情報共有体制の整備及び重要インフラ事業者等における必要情報の享受・活用を実現した。

共通脅威分析については、重要インフラ全体の防護能力の維持・向上に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った結果、重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映した。

分野横断的演習については、ＩＴ障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じて相互の連絡・連携における仕組みの検証機会の提供に取り組んだ結果、演習参加組織数・人数は増加傾向にあり、演習で得られた知見に基づく重要インフラ事業者等のＩＴ障害時の早期復旧手順及び事業継続計画等の検証を通じた情報セキュリティ対策に貢献した。

環境変化への対応のうち広報公聴活動については、重要インフラの情報セキュリテ

ィ施策の結果資料、重要インフラ専門委員会の会議資料等を内閣官房のWebサイトに掲載し、公表するとともに、情報セキュリティ政策に係る講演等を行った。リスクコミュニケーションの充実については、情報セキュリティに係る関係機関との意見交換会の開催、セプターカウンシルにおける相互理解ＷＧの開催を行った。国際連携の推進については、Meridian[3]、Cyber Storm演習[4]への参加等を通じて諸外国との連携を行った。こうした取組を通じて、環境変化に伴う脅威の察知能力の向上に努めた。

3.2 課題

各施策の実施を通じて、社会・技術面での環境変化を踏まえた改善・補強を要する課題も抽出された。各施策の主たる課題を以下に記載する。

安全基準等の整備及び浸透においては、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・向上にも効力が及ぶこと、重要インフラ事業者等から対策の実情に基づいて優先順位付けされた指針の提示要望があること等から、重要インフラ事業者等における情報セキュリティ対策のPDCAサイクルに沿った継続的改善の取組との整合に基づく見直しを課題とする。

情報共有体制の強化においては、実効性のある情報共有体制の構築を目的に、分野間における情報共有頻度の格差の解消、「脅威の類型」の細分化、平時の体制の延長線上として位置付けられる大規模ＩＴ障害対応時の情報共有体制の構築、新たな関係主体との連携の在り方の整理等を課題とする。

共通脅威分析においては、共通脅威分析の対象・位置付けや実施頻度の見直しに向けて、調査対象を全分野の共通脅威に限定せず、全分野に及ばずとも影響が大きな脅威を調査対象に加える運営に係る検討や、効果を高めるため、時間経過や環境変化の顕在化に応じた脅威等の詳細分析等を課題とする。

分野横断的演習においては、各組織のＩＴ利用形態や情報管理態勢がそれぞれ異なっていることから演習環境の設定に限界があり、大幅な参加者拡大が望めない。このため、重要インフラ事業者等における情報セキュリティ対策の課題抽出機会の提供を目的に、演習成果の更なる普及・浸透を、参加者拡大のみに依存せず、重要インフラ分野全体に図ることを課題とする。また、演習評価に基づく運営の質的改善、重要インフラのＩＴ障害発生時の対応を踏まえた関係主体の在り方の検討、並びに重要インフラ所管省庁及び防災関係府省庁が主催する演習・訓練との連携についての検討を課題とする。

環境変化への対応のうち広報公聴活動においては、次期行動計画における本施策と

[3] 各国の重要情報インフラ防護政策担当者が集まり、重要情報インフラ防護に特化して議論を行う国際的なフォーラム。
[4] 米国政府が主催する大規模な演習。サイバー空間の脆弱性・脅威・攻撃に対応する国際的な取組を促進する場であるIWWN(International Watch and Warning Network)の一員として参加している。

他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しを課題とする。リスクコミュニケーションの充実においては、国際標準と整合したリスクマネジメントの定義、機微情報の秘匿と情報の有用性のバランスを念頭に置いた情報共有の見直し、及び中長期的に実現・利用され脅威の影響の大きさが予想される新たなＩＴ技術等を対象にした環境変化のテーマに係る中長期的な継続調査・検討を課題とする。国際連携の推進においては、国境を越えて形成されたサイバー空間において深刻化・グローバル化するリスクへの迅速な対応に向けて、諸外国との連携推進を継続するとともに、ASEAN等のアジア太平洋地域や欧米等の二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化を課題とする。

4. 考慮すべき課題

前節における課題やサイバーセキュリティ戦略において検討を求められた課題をまとめるとともに、これらの課題を踏まえた本行動計画策定の方向性について、以下のとおり検討を行った。

課題１　重要インフラ防護が体制としての成熟度を高めている一方、基本的な考え方に示した「情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施する」ことに関して、その実行や実行に当たっての意識が不十分な重要インフラ事業者等が見受けられる。このような重要インフラ事業者等の実効的かつ自主的な取組をどのように促進することが適当なのか。

＜方向性＞

○重要インフラ事業者等にとって実現が困難な理想論を記載するのではなく、現実を見据え、身の丈に合った「実行可能」なものとする。例えば、「安心があたりまえ」「100%の完璧を期する」といった表現は避けるようにする。

○重要インフラ事業者等における情報セキュリティ対策の鍵を握る経営層が十分にその必要性を把握できるよう、基本的な項目を行動計画に記載する。

○「専門家」ではない可能性のある関係者が含まれることを念頭に、各々の関係主体に何が求められているか、読んで理解できるものとする。

○重要インフラ防護能力の維持・向上、とりわけ対策途上や中小規模の重要インフラ事業者等による実効的かつ自主的な取組に資するPDCAサイクルを明確化する。

○環境変化に対して柔軟に対応できるよう、重要インフラ事業者等におけるリスクマネジメントの重要性と導入の必要性に関して具体的に記載する。

○重要インフラ事業者等が把握すべき階層化された規程類をパッケージ化し、異動の激しい関係者間でも引き継ぎが容易になる構造・内容とする。

○行動計画策定後も、刻々と変化する環境に適切に対応し、適切な情報収集・提供を継続的に行うことを可能とするための広報公聴活動を一層充実させる。

課題２　刻々と変化する社会環境や技術環境、年々深刻化している脅威に関して、適切かつ迅速に対応できる方策が十分に講じられていない懸念があるが、これらの環境変化や脅威に適切に対応するためにどのような取組が官民双方に必要になるのか。また、関係主体として追加すべき者の有無を検証すべきではないか。

＜方向性＞

○サイバー空間関連事業者のうち必要な者も関係主体に加え、情報共有を更に充実させる。

○サイバー空間での重要インフラ事業者等の活動が、標的にされたり、踏み台とされたりする可能性があることを認識し、こうした弱点について相応の責任が生じ得ることに関して一層の自覚を促す。

○個々の重要インフラ分野、更には重要インフラ事業者等における脅威や脆弱性がそれぞれ異なること、また、社会環境や技術環境が刻々と変化することを認識し、複数の分野に及ぶ優先度の高いリスク源[5]についての調査や新しい技術・システム等の中長期的な変化の継続的な調査を実施する。

課題３　ＩＴ障害発生時の対応については、関係主体において様々な取組が開始されている一方、重大なＩＴ障害等が発生した際の対処及びその体制（官民間、官官間）が十分整理されていない懸念があるが、このような重大なＩＴ障害発生時の官民各機関における、共有・連絡すべき情報の整理、各々の対応の明示及び各機関間の連携体制の強化が必要ではないか。

＜方向性＞

○関係主体が実施する演習・訓練間の連携を通じて、当該演習・訓練等の効果を高めていく。

○大規模ＩＴ障害対応時、当該事態が重要インフラ事業者等にとって特別な警戒を要するものであると認知するメカニズムを構築するとともに、平時（大規模ＩＴ障害対応時以外の状態）における対応体制に誰がどう追加されるのかを可能な限り明確化する（なお、事態発生時に全く新しい体制を立ち上げることは現実的ではない。）。

[5] 「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。」と定義されている。

5. 重要インフラの範囲の見直しについて

本行動計画の策定に当たっては、第２次行動計画において10分野と規定されている重要インフラの範囲の妥当性について検証し、新たな分野の追加について検討を行った。

なお、サイバーセキュリティ戦略[6]において検討することとされている重要インフラの範囲等については、環境変化に応じて、関係者との調整を踏まえつつ、引き続き見直しを行っていく。

5.1 検討結果

第２次行動計画において重要インフラと位置付けられていないが、既存の重要インフラ分野と同等にＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼし得る分野の位置付け等、第２次行動計画における重要インフラの範囲の妥当性に関して、東日本大震災発災時における対応等これまでの知見を踏まえた検証を行い、図表１に示すとおり新たに重要インフラとして追加する必要があると認められる分野を特定した。

図表１　重要インフラの範囲に関する検討結果

区分	視点・必要性	分野
当該分野が有する情報システムが障害に至った場合の影響を考慮して追加する分野	処理するサービス提供の価値及び規模	クレジット
	制御が困難な状態において生じ得るリスクの大きさ	化学、石油
既存の重要インフラ分野における情報システムに与える影響を考慮して追加する分野	既存の重要インフラ分野との間での相互依存性	石油 （再掲）

これにより、本行動計画における重要インフラ分野は、「情報通信」、「金融」、「航空」、「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」の13分野となった。

なお、追加分野が重要インフラに参加するに当たっては、当該追加分野がなぜ重要インフラに指定されるのか、参加に見合うメリットがあるのか、といった観点での疑問を払しょくし、自らが活動することの必要性に関する理解を醸成することが重要である。

追加分野を所管している省庁及び情報共有体制の要となるセプター事務局候補と想定される業界団体に対しては、上記観点についての説明を行い、重要インフラへの参画について合意を得ており、当該業界団体においては、対象となる重要システムやサービス維持レベルの特定、セプター設立の準備等を行っている。

[6] ２．基本的な方針（3)各主体の役割 ②重要インフラ事業者等の役割（P.20）を参照。

5.2 既存の重要インフラ分野と追加分野との関係

情報共有体制は、2007年度の構築から７年が経過しており、既存の各セプターは、情報セキュリティ対策の経験値を有するほか、業務性質等から独自色を有している。

こうした中で、追加分野が新規セプターとして加入した場合、取組が進んでいる既存セプターの活動に委縮してしまう懸念があることから、内閣官房は、重要インフラ分野内の他重要インフラ事業者等や、他重要インフラ分野の重要インフラ事業者等との連携の充実が重要であることを念頭に置いて追加分野への助言を行うことが必要である。また、セプターカウンシルにおいても、相互扶助の精神で追加分野のセプターに助言を行い、重要インフラ全体の防護能力の維持・向上を図ることが期待される。

6. 本行動計画策定に当たっての検討結果

前節までに抽出した課題及び整理した方向性を踏まえ、本行動計画策定に当たっては、サイバーセキュリティ戦略と整合する第２次行動計画の基本的骨格を維持するが、個別の施策やその実施体制を見直し、必要な補強・改善を行った上で、図表２に示す施策群の構成とすることとした。

図表２　本行動計画における施策群と補強・改善の方向性等

本行動計画における施策群	第２次行動計画の施策群との対応	第２次行動計画からの補強・改善の方向性
１．安全基準等の整備及び浸透	「[1] 安全基準等の整備及び浸透」を基本的に踏襲	○他施策の結果を指針本編・対策編に反映するプロセスの明示 ○指針による成長モデル等の訴求及び対策の実情の調査
２．情報共有体制の強化	「[2] 情報共有体制の強化」を基本的に踏襲	○新たな関係主体を含めた情報共有体制における各関係主体の位置付けの見直し及び関係主体間の関係の再整理 ○サイバー攻撃関係情報の増加を踏まえた共有すべき情報（脅威の類型等）の見直し ○平時における対応を念頭に置いた大規模ＩＴ障害対応時の事案対処体制の明確化
３．障害対応体制の強化	「[4] 分野横断的演習」を整理	○重要インフラ関係の演習・訓練の全体像を把握した上でＩＴ障害対応体制の総合的な強化 ○新たな関係主体との連携を念頭に置いた分野横断的演習の質的改善
４．リスクマネジメント	「[3] 共通脅威分析」を「[5] 環境変化への対応」の一部と統合した上で整理	○環境変化等に応じて生じる複数分野において大きな影響を生じ得るリスク源、将来的に多大な影響が予想される環境変化についての中長期的な調査の実施 ○重要インフラ事業者等が自らの状況を正しく認識し、活動目標を主体的に定めるに当たって必要となるリスクマネジネントの訴求
５．防護基盤の強化	「[5] 環境変化への対応」を「[3] 共通脅威分析」と統合される部分を除いた上で整理	○広報公聴、国際連携に加え、関連する国際標準・規格、参照すべき規程類の整理、活用方法の提示を追加

なお、行動計画策定後に環境が大きく変化した場合でも適切に対応できるようにするため、環境変化を継続的に監視して得られる情報から脅威を特定し、柔軟に対応できる体制を構築する必要がある。さらに、従来重点が置かれていた未然防止のみならず、障害対応体制の強化に係る取組を充実するとともに、平時から大規模ＩＴ障害対応時へシームレスに移行できるものとすることが重要である。

Ⅱ．本行動計画の要点

本行動計画を推進するに当たっての、①「重要インフラ防護」の目的、②基本的な考え方、③重要インフラ事業者等・政府機関・情報セキュリティ関係機関等の関係主体の在り方、その中でも④重要インフラ事業者等の経営層に期待する在り方を以下に示す。

①「重要インフラ防護」の目的

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともにＩＴ障害発生時の迅速な復旧を図ることで重要インフラを防護する。

②基本的な考え方

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

－重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。

－政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。

－取組に当たっては、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に限界があることから、他の関係主体との連携をも充実させる。

③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。

④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。

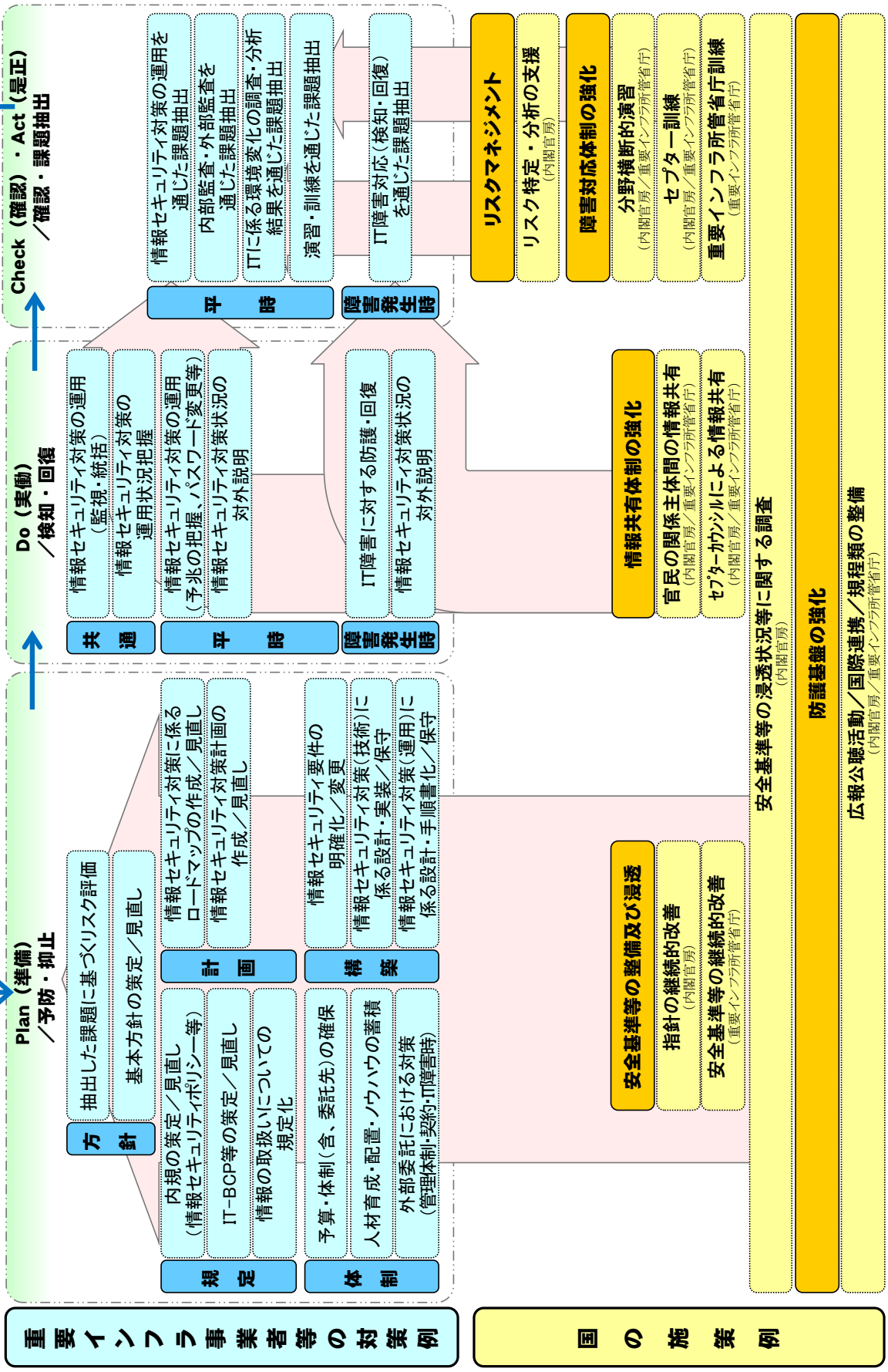
－上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。

－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。

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」



Ⅲ．計画期間内に取り組む情報セキュリティ対策

1．安全基準等の整備及び浸透

本行動計画期間においては、内閣官房は、重要インフラ防護能力の維持・向上を目的に、重要インフラ事業者等のPDCAサイクルとの整合及び他施策との連携を強化した指針改定及び調査運営の見直しを行う。

また、重要インフラ事業者等は、情報セキュリティ対策の重要性に鑑み、その対応においてはPDCAサイクルに沿った継続的かつ着実な実施に取り組む。

1.1 指針の継続的改善

重要インフラ防護能力の維持・向上、とりわけ対策途上や中小規模の重要インフラ事業者等による実効的かつ自主的な取組に資することを目的に、内閣官房は、指針本編・対策編の見直しを2014年度に行う。

具体的には、重要インフラ事業者等のPDCAサイクルに沿った情報セキュリティ対策の項目を整理するとともに、本行動計画の他施策から得た知見等を追加項目として採録する。

また、重要インフラ事業者等が情報セキュリティ対策を実施する際の優先順位付け、対策の段階的な追加及び予防的対策と事後的対策のバランスに係る考え方を成長モデルとして例示する。

さらに、重要インフラ事業者等における段階的・継続的な対策の強化に不可欠な方針化、規定化、計画化、体制化・人材育成及びシステム構築に係る重要インフラ事業者等の経営層の在り方の重要性を訴求する。

なお、2015年度以降、年度ごとに社会動向の変化及び新たに得た知見を必要に応じて公表し、また、指針本編・対策編の改定は３年に１度又は必要に応じて実施する。

1.2 安全基準等の継続的改善

各重要インフラ事業者等の対策を通じ、当該重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・向上を目的に、重要インフラ所管省庁及び重要インフラ事業者等は、対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。

具体的には、情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及びＩＴ障害対応から課題を抽出し、リスク評価を経て、安全基準等の継続的改善に取り組む。

なお、安全基準等の検証に際しては、指針及び内閣官房が公表した社会動向の変化・新たな知見を用いることとする。

内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。

1.3 安全基準等の浸透

重要インフラ事業者等における安全基準等の浸透状況の把握を目的に、内閣官房は、重要インフラ事業者等の対策状況を調査する。加えて重要インフラ事業者等による実効的かつ自主的な取組に資することを目的に、本調査への回答が自ずと対策状況のセルフチェックにつながるよう調査運営を見直す。

調査に係る具体的な取組としては、より具体的な対策状況を確認し得る調査項目を追加するとともに、調査対象の拡張の下、浸透状況が良好な重要インフラ事業者等を対象とした経年調査を通じて対策状況の退化を検知し得る項目を追加する。

調査運営の見直しに係る具体的な取組としては、調査票の構成を重要インフラ事業者等の対策プロセスに沿って整理し、重要インフラ事業者等にとって強化対象の対策及びプロセスが明示的になるように取り組む。

加えて、アンケート方式による本調査の補完を目的に、内閣官房は、重要インフラ事業者等へ往訪調査を行う。

往訪調査に係る具体的な取組については、往訪による面会にてアンケート方式の調査項目を掘り下げたヒアリングを通じて、具体的な対策状況に係る課題抽出及び良好事例の収集を行う。

なお、アンケート及び往訪調査にて得た調査結果については、原則、年度ごとに公表するとともに、得た改善課題については本行動計画の各施策に連携する。

また、調査項目については、経年調査を損なわない程度に柔軟な変更を行うことを可能とする。

2. 情報共有体制の強化

重要インフラを取り巻く社会環境や技術環境は刻々と変化する中、重要インフラの情報セキュリティ対策の有効性を保ち続けるには、これらの環境変化を的確に捉えた上で情報セキュリティ対策への反映が必要である。また、サイバー攻撃の複雑・巧妙化に伴い、情報セキュリティ対策の水準の向上、サイバー攻撃への対応能力の向上はますます重要になっている。

「I.2. 重要インフラ防護の目的の明確化」における基本的な考え方で述べたとおり、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。

これらの状況を踏まえ、本行動計画期間において、内閣官房は、追加された分野、関係主体を含む情報共有体制を運用し、情報共有を更に促進するとともに、重要インフラ事業者等による情報共有活動の更なる活性化を図る。

2.1 本行動計画期間における情報共有体制

本行動計画策定に際し、大規模ＩＴ障害対応時における情報共有体制の強化に向けて、防災の観点から防災関係府省庁を追加するとともに、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設計・構築・運用・保守に携わるシステムベンダー、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からなるサイバー空間関連事業者を追加した。追加後の体制については「別紙４－１　情報共有体制（平時)」及びその延長線上にある「別紙４－２　情報共有体制（大規模ＩＴ障害対応時)」に表した。

また、追加した新たな分野を含め、重要インフラ分野の重要システム及びサービス維持レベルを見直した。その結果については「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」及び「別紙２　重要インフラサービスとサービス維持レベル」に表した。

本行動計画期間中、関係主体は、各々の位置付け・役割に基づき情報共有体制を運用する。なお、サイバー空間関連事業者においては、脆弱性情報の共有やサイバー攻撃等に起因するＩＴ障害発生時における被害拡大の防止等、情報セキュリティの確保に必要に応じて取り組むことが期待される。

2.2 情報共有の更なる促進

共有すべき情報の整理については、「ＩＴ障害の未然防止」、「ＩＴ障害の拡大防止・迅速な復旧」、「ＩＴ障害の原因等の分析・検証による再発防止」の３つの側面から、政府機関や重要インフラ事業者等の各関係主体に応じて共有すべき情報の抽出と整理を行うことが重要である。

本行動計画策定に際し、内閣官房は、これら３つの側面を踏まえ、ＩＴ障害の未然防止を含む重要インフラ防護に資することを目的に、平時及び大規模ＩＴ障害対応時の情報共有体制にて用いる情報連絡・情報提供について、「別添：情報連絡・情報提供について」及び「別紙３　情報連絡における事象と原因の類型」の見直しを行った。

具体的には、「別紙３　情報連絡における事象と原因の類型」においては、ＩＴ障害の迅速かつ正確な状況把握を目的に、情報セキュリティのＣ・Ｉ・Ａ[7]の観点に基づく事象[8]項目の見直し及び新たな脅威等を踏まえた原因項目の詳細化を行った。「別添：情報連絡・情報提供について」においては、分野間における情報共有頻度の格差解消を目的に、ＩＴ障害の予兆情報の取扱い等、情報連絡の対象の明確化を行った。

関係主体間でＩＴ障害の事象や原因等に関する情報共有を行うことで、重要インフラ事業者等における運用や対策等の確認に活かされ、ＩＴ障害の未然防止につながることが期待されることから、本行動計画期間においては、内閣官房は、見直しを行った情報共有体制の下、関係主体との間で別添に従って情報連絡・情報提供を行い、情報共有の連携、促進を図る。また環境変化等が生じた場合には、適宜その見直しを図る。

2.3 重要インフラ事業者等の活動の更なる活性化

重要インフラ事業者等の活動を更に活性化するに当たり、重要インフラ事業者等の自らの活動に加え、セプター間における情報共有の充実が期待される。

具体的には、重要インフラ事業者等においては、自ら積極的に情報共有活動に取り組むとともに、CSIRT[9]等のＩＴ障害対応体制を構築・強化することが期待される。また、セプターにおいては、第２次行動計画期間に引き続き、内閣官房が提供する情報の取扱いに関する取決め、機密保持及び構成員外への情報提供に関し、構成員間で合意されたルールが適用され、緊急時に各構成員及び構成員外との連絡が可能な窓口

[7] 機密性（Confidentiality）、完全性（Integrity）及び可用性（Availability）を指す。

[8] 情報セキュリティ事象（Information Security Event）とは、「ISO/IEC 27000:2013」によれば、「システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示しているものをいう。」と定義されている。

[9] Computer Security Incident Response Team。情報システムに情報セキュリティ上の問題が発生していないか監視するとともに、問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。

（PoC[10]）が設定されている状況において、内閣官房が提供する情報を共有することの継続が期待される。

加えて、セプター内の情報集約及び情勢判断を行うコーディネータの設置、予兆情報や平時のＩＴ障害事例の共有、セプター間やセプターカウンシル等との情報共有に必要な機能の充実を通じた活動の更なる活性化が期待される。

なお、セプターカウンシルは、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であることから、各セプターの主体的な判断により、情報を相互に連携するものである[11]。

このように、各セプターの積極的な参画により、重要インフラ事業者等におけるサービスの維持・復旧能力の向上に資する自発的かつ幅広い取組を通じて、セプター間の情報共有の一層の充実等、重要インフラ事業者等の活動の更なる活性化が期待される。

2.4 情報共有体制における各関係主体の役割

情報共有体制については、平時の情報共有体制の延長線上に大規模ＩＴ障害対応時の情報共有体制を構築しており、大規模ＩＴ障害対応時における各関係主体の役割も平時の役割の延長線上にある。

平時と大規模ＩＴ障害対応時における情報共有の全体像については、「別紙４－１　情報共有体制（平時）」及び「別紙４－２　情報共有体制（大規模ＩＴ障害対応時）」に示すとおりであり、各関係主体の役割は以下のとおりである。

2.4.1 平時の情報共有体制における各関係主体の役割

平時の情報共有体制における関係主体が行う情報共有は次のとおり。

(1) 重要インフラ事業者等

ＩＴ障害やサイバー攻撃に係る情報共有は所属するセプターにおいて行うことを基本とする。また、必要に応じてＩＴ障害やサイバー攻撃に係る情報連絡を重要インフラ所管省庁に行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁に通報を行う。

(2) セプター

セプターカウンシルや重要インフラ所管省庁、情報セキュリティ関係機関と連携し、相互にＩＴ障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の共有を行う。

---

[10] PoC：Point of Contact。

[11] セプターカウンシル設立趣意書（セプターカウンシル創設準備会及びNISC）による。

(3) セプターカウンシル

セプターカウンシルは、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、独立した会議体である。各セプターの主体的な判断により、連携するものである。

主体的な判断により各セプターが積極的に参画し、重要インフラ事業者等におけるサービスの維持・復旧に向けた幅広い情報共有を行う。

(4) 重要インフラ所管省庁

所管する重要インフラ事業者等から受領したＩＴ障害やサイバー攻撃に係る情報連絡を内閣官房（NISC）に行う。また必要に応じて所管するセプターに行う。内閣官房（NISC）から受領したＩＴ障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の情報提供を所管するセプターに行う。

(5) 内閣官房（NISC）

重要インフラ所管省庁、情報セキュリティ関係省庁、あらかじめ連携を要請した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と相互にＩＴ障害やサイバー攻撃に係る情報、復旧手法等に関する情報共有を行う。

2.4.2　大規模ＩＴ障害対応時の情報共有体制における各関係主体の役割

災害やテロ等に起因する大規模ＩＴ障害が発生した場合、当該緊急事態における情報の集約及び共有として、「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）に基づき、関係府省庁間で情報を集約及び共有するものとされている。事態が悪化し、大規模ＩＴ障害対応に移行した際、事案対処省庁、防災関係府省庁及び内閣官房における情報の一元化が重要であることから、次のような情報共有体制を敷く。

(1) 内閣官房（事態対処・危機管理担当）

内閣官房（NISC）と一体化し、事案対処省庁及び防災関係府省庁から提供される被害情報、対応状況情報等を集約し、内閣官房（NISC）と相互に情報共有を行う。

(2) 内閣官房（NISC）

内閣官房（事態対処・危機管理担当）と一体化し、重要インフラ所管省庁、情報セキュリティ関係省庁、あらかじめ連携を要請した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と相互に各種関連情報、復旧手順方法等に関する情報共有を行う。

(3) 重要インフラ所管省庁

平時の役割に加え、必要に応じて大規模ＩＴ障害対応時の体制に協力する。

(4) 重要インフラ事業者等

平時の役割に加え、各重要インフラ事業者等が定める大規模ＩＴ障害対応時の体制を構築する。

(5) セプター

平時の役割に加え、各セプターが定める大規模ＩＴ障害対応時の体制を構築する。

(6) セプターカウンシル

平時の役割に加え、セプターカウンシルが定める大規模ＩＴ障害対応時の体制を構築する。

3. 障害対応体制の強化

本行動計画期間においては、第２次行動計画における分野横断的演習に加え、ＩＴ障害対応に関する能力向上及び検証を目的とする各種演習・訓練をＩＴ障害対応体制の強化策の一環に位置付け、これらの演習・訓練の相互の関係を把握し、連携を行うことで、重要インフラ全体の防護能力の維持・向上を図る。

その中で、分野横断的演習については、これまでの実績を踏まえ、引き続き重要インフラ分野のＩＴ障害対応体制を強化する中核的な取組としての位置付けの充実を図る。具体的には、分野横断的演習がセプター訓練及び重要インフラ所管省庁が実施する他の演習・訓練と相互に連携・補完し、相乗効果を発揮できるよう、各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の体制を強化する。

また、被害の拡大防止の観点から迅速な事案対処等も必要となることから、関係主体は重要インフラ事業者等のＩＴ障害対応能力を高めるための対策又は支援策について、関係主体間の連携強化と役割分担の明確化を図りつつ必要に応じて実施する。

3.1 分野横断的演習の改善

本行動計画期間においては、内閣官房は、重要インフラ分野全体への分野横断的演習成果の浸透を通じた重要インフラ防護能力の維持・向上に資することを目的に、我が国唯一の取組である分野横断的演習を改善しつつ引き続き実施する。

その際、第２次行動計画で掲げた３つの目標である「分野横断的な脅威に対する共通認識の醸成」、「他分野の対応状況把握による自分野の対応力強化」及び「官民の情報共有をより効果的に運用するための方策の獲得」を踏襲し、障害対応体制の強化に資するよう、蓄積した運営手法や成果を用いて分野横断的演習の充実を図る。

3.1.1 分野横断的演習の企画立案に係る質的改善

本行動計画期間において、内閣官房は、分野横断的演習の改善を継続的に図ることを目的として、演習運営を通じて得た知見・課題、他施策から得られた課題及びＩＴ障害を引き起こす要因であるリスク源に係る最新動向を演習に取り込むことに加え、重要インフラ事業者等が保有するＩＴシステムの維持に密接に関連する関係主体の参画も視野に入れた演習の企画立案を検討する。

また、内閣官房は、演習成果が重要インフラ事業者等の情報セキュリティ対策並びにＩＴ障害時の早期復旧手順及びIT-BCP等に係る検証の更なる強化に資することを目的に、演習結果の評価プロセスの改善に向けた検討を行う。

加えて、演習を通じて得た知見・課題を基礎資料として本行動計画の他施策に提供する。

3.1.2　重要インフラ全体への分野横断的演習の成果の浸透

第２次行動計画期間中、演習参加者数は着実に増加し、演習を有意義と評価する参加者が８割を超えており、演習未経験者への新規参加を促すことで、重要インフラ分野における演習成果の浸透を目指す。一方、参加者拡大には一定の限界があることから、更なる重要インフラ全体への演習成果の普及・浸透を行うためには、新規参加の促進に加え、演習に参加していない重要インフラ事業者等を対象とした取組も必要である。

そのため、内閣官房は、経営層の理解増進にも寄与し得る演習のメリットについての説明資料の作成・公表及び重要インフラ分野全体への訴求を通じて、各重要インフラ分野・重要インフラ事業者等内での演習実施を促進する。

また、個別の重要インフラ事業者等による演習実施の支援に資することを目的に、これまでの演習において蓄積してきた実施・評価・助言手法の整備及びその共有化の実現に向けた検討を進める。

3.1.3　物理的な要因によるＩＴ障害への対応

現実のＩＴ障害対応には、物理的な要因によるＩＴ障害も想定され、その状況によっては、各府省庁や各重要インフラ事業者等の情報セキュリティ部門だけではなく、防災・危機管理部門との情報共有を要する可能性がある。

今後、内閣官房は、分野横断的演習において当該ＩＴ障害への対応も検証対象とする場合、シナリオ作成等において必要に応じ、防災関係府省庁等の知見の活用及び重要インフラ所管省庁や重要インフラ事業者等の防災・危機管理担当者の協力の在り方について検討する。

3.1.4　重要インフラ所管省庁との連携

重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練は、内閣官房が実施する分野横断的演習と期待する効果が異なるが、分野横断的演習と相互に連携・補完しつつ実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図っていくことが期待される。

このことから、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の対応能力の向上を目的に、それぞれが実施する演習における主な対象者や検証目的の明確化及び相互連携の在り方について検討する。

なお、検討項目の一例として、分野横断的演習では重要インフラ事業者等間やセプター、重要インフラ所管省庁、内閣官房等との情報共有・連携対応を主な検証対象とし、重要インフラ所管省庁の演習では重要インフラ事業者等における実機システムを用いたＩＴ障害対応手順や各分野の連絡体制を確認・検証対象とすることが考えられる。

3.2 セプター訓練

内閣官房は、各分野におけるセプター及び重要インフラ所管省庁との「縦の情報共有」体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施する。

実施に際しては、セプターからの要望も取り込みながら訓練内容を充実しつつ、ＩＴ障害対応を念頭においたより実態に即した情報共有訓練の実現を目指す。

また、セプター訓練は多くの重要インフラ事業者等の参加が期待できることから、分野横断的演習における検証内容を踏まえた状況設定を行う等、必要に応じてセプター訓練と分野横断的演習との連携を検討する。

4. リスクマネジメント

重要インフラ事業者等は、国民に対する重要インフラサービスの安定的供給や事業継続等といった事業目的の達成に向け、情報セキュリティの確保に係る目的を確立し、組織内へと展開する必要がある。

一方、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等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。

このことから、重要インフラ事業者等においては、個別の対策等に代表されるＩＴの不具合への対症療法のみならず、事業目的の達成に向け、情報セキュリティに係るリスク源から導き出されるリスクに対する包括的なマネジメントを行う必要性が高まってきている。なお、本行動計画において、リスクとは、目的に対する不確かさの影響を指すものとする。

このため、重要インフラ事業者等におけるリスク評価手法等に基づく情報セキュリティ対策の重点化を目的に、第２次行動計画の「共通脅威分析」及び「リスクコミュニケーションの充実」（「環境変化への対応」の一施策）を包括的に捉え直し、各重要インフラ事業者等が主体的に行うリスクマネジメントに係る施策を新たに実施する。

4.1 リスクマネジメントの標準的な考え方

リスクマネジメントは各重要インフラ事業者等がそれぞれにおいて主体的に実施するものである。一方で、各関係主体間において共通的なリスクマネジメントの考え方や用語による情報共有及び議論がされない状態では、本行動計画における各種取組が、各重要インフラ事業者等のリスクマネジメントにおいて効果的に活かされない可能性がある。

このことから、本行動計画期間においては、各関係主体は、国際的にも標準的なリスクマネジメントの考え方やそこで利用される情報セキュリティに関わる用語の定義等を利活用することが望ましい。

具体的には、内閣官房は、内閣官房が実施する施策や各種関連資料において、以下の図表４に示す枠組み[12]を軸とした考え方や枠組みの中で利用される用語の定義等を可能な限り適用する。

[12] 「JIS Q 31000:2010」やENISA(欧州 ネットワーク情報セキュリティ庁)が公表している「Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools」を参照。

図表４　標準的なリスクマネジメントのプロセス（例）

<table>
<tr><td rowspan="8">リスクマネジメント</td><td colspan="2">組織の状況の確定</td></tr>
<tr><td colspan="2">リスクアセスメント</td></tr>
<tr><td></td><td>リスク特定</td></tr>
<tr><td></td><td>リスク分析</td></tr>
<tr><td></td><td>リスク評価</td></tr>
<tr><td colspan="2">リスク対応</td></tr>
<tr><td colspan="2">リスクの受容</td></tr>
<tr><td colspan="2">リスクコミュニケーション及び協議</td></tr>
<tr><td colspan="2">モニタリング及びレビュー</td></tr>
</table>

また、重要インフラ事業者等は、内閣官房が作成する手引書等[13]を自組織のリスクマネジメントにおいて利活用することが期待される。

なお、本施策は、各関係主体に国際標準への準拠を求めるものではなく、本施策において内閣官房が適用する考え方や用語の定義等を参照することで、重要インフラ事業者等が既に自組織において実施しているリスクマネジメントの更なる最適化及び情報セキュリティ対策の水準の向上に資することを目的としている。

4.2　リスクマネジメントの支援

リスクマネジメントは、基本的に各重要インフラ事業者等が自組織に最適化して取り組むものである。一方、各重要インフラ事業者等によるリスクマネジメントのうち、特にリスクアセスメント[14]やリスクコミュニケーション及び協議[15]においては、重要インフラ分野横断的な調査・分析及び意見交換等といった自組織だけでの取組が容易ではないものも存在する。

このため、内閣官房は、こうした分野横断的なものについて以下のとおり取組を行い、その調査・分析結果の共有や意見交換の機会の提供等により、重要インフラ事業者等のリスクマネジメントの支援を行う。

4.2.1　リスクアセスメント

内閣官房は、重要インフラ分野を取り巻くＩＴに係る環境の変化について、情報セキュリティの視点から主な設備・技術等の実態・動向調査及び主な設備・技術等に内在するリスク源やそこから導き出される新たなリスク（以下「新たなリスク源・リスク」という。）の分析を行う。

また、重要インフラ分野において生じたＩＴ障害等の影響波及に係る解析を継続し

[13] 「5.3.3 国際基準等を重要インフラ防護に適用する場合の手引書等の整備」において、国際標準等を読み替えた手引書等を必要に応じて取りまとめることとしている。

[14] 「JIS Q 31000:2010」によれば、「リスク特定、リスク分析及びリスク評価のプロセス全体。」と定義されている。

[15] 定義は「4.2.2 リスクコミュニケーション及び協議」を参照。

て行う。

具体的には、各調査・分析の効率、他施策との相互反映等の観点も踏まえ、以下のとおりとし、その調査・分析結果については重要インフラ事業者等に提供する。

(1) 環境変化調査

第２次行動計画中に実施した環境変化調査においては、クラウド、スマートフォン・タブレット端末及びリモートメンテナンスは重要インフラ分野において導入率が高いことが明らかになり、BYOD[16]やビッグデータは今後の導入拡大が想定される結果となった。

本行動計画において、内閣官房は、これら変化に加え、M2M、スマートコミュニティ等、中長期的な重要インフラ分野への浸透が予想される新しい技術・システムも環境変化調査の対象とした実態調査及び新たなリスク源・リスクの分析を行う。また、その実施に際しては、時間経過や環境変化の顕在化に応じて行うことでより良い結果を得られることから、年度をまたいで継続的に行う。また、例えば制御系、勘定系、情報系等一定の分野に共通するもので全分野に及ばずとも影響が大きい新たなリスク源・リスクについても当該分析の対象とする。

なお、本調査にて新たなリスク源・リスクが明らかになった場合及び新たな重要インフラ分野が追加となった場合、必要に応じて、それらの分野共通性の分析を詳細調査と位置付けて行う。

(2) 相互依存性解析

各重要インフラ分野におけるＩＴ利用が進展し、分野間の相互依存関係が増大する中、重要インフラ分野における相互依存性の把握は、ＩＴ障害等が生じた際の効率的な復旧対策において重要である。

このことから本行動計画において、内閣官房は、環境変化に伴う相互依存性の変化及び新たな重要インフラ分野の追加が生じた場合、第１次行動計画及び第２次行動計画における解析結果をもとに再調査・解析を行うことを含め、相互依存性解析を継続的に行う。

また、各重要インフラ分野におけるＩＴ依存度は相互依存性解析に密接に関連することから、ＩＴ依存度についても詳細調査として定期的に調査を行う。

なお、新たな重要インフラ分野が追加となった場合、相互依存性解析に合わせてＩＴ依存度の調査を行う。

4.2.2　リスクコミュニケーション及び協議

リスクコミュニケーション及び協議とは、「リスクの運用管理について、情報の提供、共有又は取得、及びステークホルダとの対話を行うために、組織が継続的に及び

[16] Bring Your Own Device。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。

繰り返し行うプロセス。」と定義[17]されている。

内閣官房は、関係主体間による分野横断的な情報や意見の交換の充実に資することを目的に、重要インフラ防護に関連する者によるリスクコミュニケーション及び協議の支援を行う。

具体的には、セプターカウンシル及び分野横断的演習を利活用し、各関係主体と協力しつつ、情報や意見の交換の機会を提供する。

また、これにより、本施策における調査・分析に必要となる情報の収集を図る。

4.3 本施策と他施策による結果の相互反映プロセスの確立

内閣官房は、本行動計画の他施策に資することを目的に、本施策における調査・分析結果を基礎資料として他施策に提供する。

また、他施策の実施結果から顕在化した分野横断的な対策を要する新たなリスク源・リスクを本施策の調査・分析の対象とし、必要な調査・分析を行う。

[17] 「JIS Q 31000:2010」を参照。

5. 防護基盤の強化

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、情報セキュリティ対策の有効性の確保に向けては、図表３で示した通り、基本方針の策定、人材育成・配置、情報セキュリティ対策状況の対外説明、ＩＴに係る環境変化に伴うリスク源に対する課題抽出等、本行動計画の全体を支える共通基盤的な取組の強化が必要である。

このため、本行動計画期間においては、内閣官房は、第２次行動計画に引き続き、他の関係主体と協力しつつ広報公聴活動及び国際連携を行うことに加え、関係主体が適時に適切な関連規程類を参照し得るよう、重要インフラ防護に係る関連規程類、情報セキュリティ対策に関する国際基準等についての手引書等を整備する。

さらに、本行動計画の他施策に資することを目的に、本施策の実施にて得た知見を他施策に提供していく。

5.1 広報公聴活動

ＩＴ障害の影響を可能な限り極小化するためには、重要インフラ事業者等による情報セキュリティ対策の水準の向上のみならず、国民が状況を踏まえて冷静に対応できることも重要である。

このため、各関係主体は、国民による冷静な対応に資することを目的に、行動計画に基づく取組の広報を通じて、引き続き国民への説明責任を果たすよう努める。

また、重要インフラ事業者等による情報セキュリティ対策の水準の向上には、本行動計画に基づく取組への広範な協力・支援を得ることも重要である。

内閣官房は、Webサイトやニュースレターを通じた広報及び講演等を通じた公聴活動を、引き続き行う。その際、広報の構成については、本行動計画の取組を広く認識・理解し得るように努める。

5.2 国際連携

サイバー空間を取り巻くリスクは、ボーダレスに進行しており、国境のないグローバルなリスクへの一層の対応が求められるとともに、我が国だけではなく国際的な情報セキュリティ対策の水準の向上のため、キャパシティビルディング（能力向上）への積極的な寄与が求められている。

このため、内閣官房は、重要インフラ所管省庁及び情報セキュリティ関係機関と連携して、引き続き、欧米・ASEANやMeridian等の二国間・地域間・多国間の枠組みの積極的な活用を通じて国際連携の強化を行う。その際、国際連携にて得た事例、ベス

トプラクティス等を国内の関係主体に積極的に提供するよう努める。

加えて、重要インフラ事業者等においても、情報セキュリティ対策に係る取組の海外同業他社への展開や海外の動向把握等により、多角的・多面的な国際連携に取り組むことが期待される。

5.3 規格・標準及び参照すべき規程類の整備

重要インフラの情報セキュリティ対策の有効性の確保において、関係主体がその検討を行う上で、関連文書や関連規格を必要なときに参照できるようにすること等は重要である。この規程類の整備等についての内閣官房の取組は、以下のとおりである。

5.3.1 重要インフラ防護に係る関連規程集の発行

内閣官房は、重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照するサイバーセキュリティ戦略、本行動計画等の各関連文書を合本し、「重要インフラ防護に係る規程集」として発行する。

5.3.2 重要インフラ防護に係る関連規格の体系的な可視化

内閣官房は、重要インフラ防護に係る関連規格について、適切な版を必要なときに参照できるようにするため、他の関係主体との協力の下、国内外で策定される関連規格を整理し、その結果を明示する。

5.3.3 国際基準等を重要インフラ防護に適用する場合の手引書等の整備

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、その変化に迅速かつ柔軟に対応するためには、「5.3.2 重要インフラ防護に係る関連規格の体系的な可視化」にて整理した結果から抽出した適切な関連規格、特に国際基準等の利活用が効果的な場合がある。

一方、上記の整理した結果に基づき一般論を記載する国際基準等を利活用しようとする場合、そのまま適用することが困難なものについては読み替え等を行うことが必要である。

内閣官房は、当該国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、他の関係主体との協力の下、必要に応じて、手引書等を取りまとめる。

なお、重要インフラ防護に係る国際的な手引書等が現存しないことを踏まえ、本施策で取りまとめた手引書等をASEAN各国及びISO等の国際規格に提案することによる国際貢献についても併せて検討する。

5.3.4 情報セキュリティに関する評価・認証制度の拡充

内閣官房は、検討が進む制御系機器・システム等の調達及び運用に係る国際標準に

則した評価・認証の導入の在り方について、他の関係主体との協力の下、制御系機器・システムの第三者認証制度の拡充を支援[18]する。

[18] 制御系機器・システムの第三者認証制度の導入に取り組んでいる、技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）とも協力して実施。

Ⅳ．関係主体において取り組むべき事項

本行動計画に示した情報セキュリティ対策の施策群は、重要インフラ事業者等が取り組むことが望ましい自主的な対策と、内閣官房を中心とした政府機関等において実施することが望ましい施策によって支えられる。各関係主体はそれぞれ以下の取組を基本として、情報セキュリティ対策を推進することが期待される。

1．内閣官房の施策

(1)「安全基準等の整備及び浸透」に関する施策

① 本行動計画の初年度及び必要に応じた指針の改定に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表。

② 必要に応じて社会動向の変化及び新たに得た知見に係る検討を、他施策との連携を強化した上で実施し、これらの結果を公表。

③ 上記①・②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。

④ 重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善を状況把握するための調査を実施し、結果を公表。

⑤ 重要インフラ所管省庁の協力を得つつ、毎年、安全基準等の浸透状況等の調査を実施し、結果を公表。

(2)「情報共有体制の強化」に関する施策

① 平時及び大規模ＩＴ障害対応時の情報共有体制の運営を通じた更なる促進及び必要に応じた見直し。

② 重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供。

③ 重要インフラ所管省庁の協力を得つつ、各セプターの機能、活動状況等を把握するための定期的な調査・ヒアリング等の実施。

④ 先進的なセプターの機能や活動の紹介。

⑤ セプターカウンシルに参加するセプターと連携しつつ、セプターカウンシルの運営及び活動に対する支援の実施。

⑥ セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の整備。

⑦ 必要に応じてサイバー空間関連事業者との連携を個別に構築し、ＩＴ障害発生時に適時適切な情報提供を実施。

(3)「障害対応体制の強化」に関する施策

① 他省庁のＩＴ障害対応の演習・訓練の情報を把握し、連携の在り方を検討。

② 重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプターの情報疎通機能の確認（セプター訓練）等の機会を提供。

③ 分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。

④ 分野横断的演習の改善策検討。

⑤ 分野横断的演習の機会を活用して、リスク分析の成果の検証並びに重要インフラ事業者等が任意に行うＩＴ障害発生時の早期復旧手順及びIT-BCP等の検討の状況把握等を実施し、その成果を演習参加者等に提供。

⑥ 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供。

⑦ 分野横断的演習で得られた重要インフラ防護に関する知見の普及・展開。

(4) 「リスクマネジメント」に関する施策

① リスクマネジメントの標準的な考え方や定義等の利活用や国際標準等を読み替えた手引書等の提示による関係主体間の共通認識の醸成。

② 本施策における調査・分析による重要インフラ事業者等におけるリスクマネジメントの支援。

③ 本施策における調査・分析の結果を安全基準等に反映する基礎資料として提供。

④ セプターカウンシル及び分野横断的演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議を支援。

(5) 「防護基盤の強化」に関する施策

① Webサイトやニュースレターを通じた広報を実施。

② 講演等を通じた公聴活動を実施。

③ 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

④ 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

⑤ 重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行。

⑥ 関連規格を整理、可視化。

⑦ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、必要に応じて、手引書等を整備。

⑧ 制御系機器・システムの第三者認証制度の拡充を支援。

2. 重要インフラ所管省庁の施策

(1) 「安全基準等の整備及び浸透」に関する施策

① 指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。

② 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて、安全基準等の改定を実施。

③ 重要インフラ分野ごとの安全基準等の分析・検証を支援。

④ 重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透を実施。

⑤ 毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。

⑥ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。

(2) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、情報共有体制の運用。

② 重要インフラ事業者等との緊密な情報共有体制の維持。

③ 重要インフラ事業者等からのＩＴ障害に係る報告の内閣官房への情報連絡。

④ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。

⑤ セプターの機能充実への支援。

⑥ セプターカウンシルへの支援。

⑦ セプターカウンシル等からの要望があった場合、意見交換等を実施。

(3) 「障害対応体制の強化」に関する施策

① 内閣官房が情報疎通機能の確認（セプター訓練）等の機会を提供する場合の協力。

② 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。

③ 分野横断的演習への参加。

④ セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。

⑤ 分野横断的演習の改善策検討への協力。

⑥ 必要に応じて、分野横断的演習成果を施策へ活用。

⑦ 分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。

(4) 「リスクマネジメント」に関する施策

① 本施策における調査・分析を必要とする対象に関する情報、あるいは、当該調査・分析に必要な情報を内閣官房に提供。

② 本施策における調査・分析の施策へ活用。

③ 重要インフラ事業者等のリスクコミュニケーション及び協議を支援。

(5) 「防護基盤の強化」に関する施策

① 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

② 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

③ 内閣官房と協力し、関連規格を整理、可視化。

④ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備。

⑤ 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援。

3. 情報セキュリティ関係省庁の施策

(1) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、情報共有体制の運用。

② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。

③ セプターカウンシル等からの要望があった場合、意見交換等を実施。

4. 事案対処省庁の施策

(1) 「情報共有体制の強化」に関する施策

① 内閣官房と連携しつつ、大規模ＩＴ障害対応時における情報共有体制の運用。

② 被災情報、テロ関連情報等の収集。

③ 内閣官房に対して、必要に応じ情報連絡の実施。

④ セプターカウンシル等からの要望があった場合、意見交換等を実施。

(2) 「障害対応体制の強化」に関する施策

① 重要インフラ事業者等からの要望があった場合、ＩＴ障害対応能力を高めるための支援策を実施。

5. 重要インフラ事業者等の自主的な対策として期待する事項

(1)「安全基準等の整備及び浸透」に関する対策

① 自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて、安全基準等の改定を実施。

② 自らが安全基準等の策定主体である場合は、毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。

③ 安全基準等を踏まえ、情報セキュリティ対策の実施や対策を実装するための環境整備を検討。

④ 情報セキュリティ対策の運用、内部監査・外部監査、ＩＴに係る環境変化の調査・分析の結果、演習・訓練及びＩＴ障害対応から課題を抽出し、リスク評価を経た安全基準等の継続的改善。

⑤ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。

(2)「情報共有体制の強化」に関する対策

① セプターカウンシル、セプター及び重要インフラ所管省庁と連携しつつ、情報共有体制の運用。

② ＩＴ障害発生時等に必要に応じて情報連絡を実施。

③ 攻撃手法及び復旧手法に関する情報等の収集。

④ 情報セキュリティ関係機関との合意に基づく補完的な情報共有。

⑤ セプターカウンシルにおける活動の実施。

(3)「障害対応体制の強化」に関する対策

① 内閣官房が提供する情報疎通機能の確認（セプター訓練）等を活用するなどして、自らの情報共有体制を強化。

② 分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。

③ 分野横断的演習への参加。

④ 分野横断的演習の改善策検討への協力。

⑤ 必要に応じて、自らのＩＴ障害発生時の早期復旧手順及びIT-BCP等への取組に対し、分野横断的演習成果を活用。

(4)「リスクマネジメント」に関する対策

① 自組織におけるリスクマネジメントを推進、強化。

② 本施策における調査・分析の結果として提供される基礎情報について自組織のリスクアセスメントへの活用。

③ 重要インフラサービスの情報セキュリティ対策に直接関係する関係主体間でのリスクコミュニケーション及び協議の充実。

④ 自らが単独で分析することが困難で、調査・分析する価値のある環境変化やリスク源を本施策における調査・分析の取組対象として提案。

⑤ 本施策における調査・分析の議論・検討に参画。

(5) 「防護基盤の強化」に関する対策

① 情報セキュリティ対策に係る取組の海外同業他社への展開や海外の動向把握等により、多角的・多面的な国際連携を促進。

② 内閣官房と協力し、関連規格を整理、可視化。

③ 国際基準等を重要インフラ防護に係る迅速かつ柔軟な対応の実現に際して適用可能とするため、内閣官房と協力し、必要に応じて、手引書等を整備。

④ 内閣官房と協力し、制御系機器・システムの第三者認証制度の拡充を支援。

6. セプターの自主的な対策として期待する事項

(1) 「情報共有体制の強化」に関する対策

① セプターカウンシル、重要インフラ事業者等及び重要インフラ所管省庁と連携しつつ、情報共有体制の運用。

② 内閣官房等からの情報提供について、セプター内の情報取扱いルールに則って重要インフラ事業者等への情報提供を実施。

③ 情報セキュリティ関係機関との合意に基づく補完的な情報共有の実施。

④ セプターの機能強化・充実。

⑤ 内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。

⑥ セプターカウンシルへの参加。

(2) 「障害対応体制の強化」に関する対策

① 情報疎通機能の定期的な確認。

② 重要インフラ事業者等の分野横断的演習への参加及び成果展開を支援。

③ 分野横断的演習への参加。

(3) 「リスクマネジメント」に関する対策

① 自セプターを構成する重要インフラ事業者等の自主的な取組を支援。

7. セプターカウンシルの自主的な対策として期待する事項

(1)「情報共有体制の強化」に関する対策

① 各セプターと連携しつつ、情報共有体制の運用。

② 共有対象とする情報及びその共有方法の整理の実施。

③ 相互理解及びベストプラクティス等の具体的な事例の共有による分野横断的な情報共有の推進。

④ 関係主体との協力関係を深めるため、政府機関等からの要請又は自らの発意により、両者の状況認識等の共有を進めるための意見交換等の実施。

(2)「障害対応体制の強化」に関する対策

① 必要に応じて分野横断的演習への参加。

8. 情報セキュリティ関係機関の自主的な取組として期待する事項

(1)「情報共有体制の強化」に関する対策

① 内閣官房と連携しつつ、情報共有体制の運用。

② 攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。

③ 情報共有を行う重要インフラ事業者等又はセプターとの合意に基づく補完的な情報共有の実施。

④ 内閣官房が実施する分析機能の強化の検討に対しての協力。

⑤ セプターカウンシルから要望があった場合、意見交換等を実施。

(2)「障害対応体制の強化」に関する対策

① 分野横断的演習に必要となるＩＴ障害の事例等に関する情報を内閣官房に提供。

(3)「防護基盤の強化」に関する対策

① 内閣官房と連携して、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。

② 内閣官房と連携して、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。

9. サイバー空間関連事業者の自主的な対策として期待する事項

(1)「情報共有体制の強化」に関する対策

① 内閣官房が行う共有対象とする情報とその共有方法を整理するための取組に対する協力。

② 内閣官房に対して、ＩＴ障害発生時に必要に応じて、積極的な情報連絡の実施。

Ⅴ．評価・検証と見直し

本行動計画の評価については、個々の取組がどのような結果をもたらしたのかという「結果（アウトプット）を測る視点」からの各年度における進捗状況の確認と、本行動計画における取組により社会が実際にどの程度理想とする将来像に近づいたのかという「成果（アウトカム）を測る視点」からの行動計画期間中における成果の確認といった２つの視点で取り組む。この際、進捗状況の確認は、可能な限り客観的な指標を用いることとし、また成果の確認は、本行動計画の目標、すなわち理想とする将来像に照らして行う。

なお、本行動計画における「検証」とは、指標を用いて各々の取組についてその進捗状況に係る客観的事実を確認することとする。

1. 本行動計画期間の目標（理想とする将来像）

本行動計画に基づく取組によって実現が期待される将来像は、以下のようなものである。

○各関係主体の自覚に基づく自主的な取組はそれぞれの行動規範として浸透しており、その行動様式が情報セキュリティ文化を形成するようになっている。

○各関係主体間において、ＩＴ障害の予防的対策を強化するためのコミュニケーションが日常的に行われるとともに、ＩＴ障害が発生した場合にはその経験を確実に将来の対策に活かすための継続的な改善がなされている。

○関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている。また、多様な主体間でのコミュニケーションが充実し、ＩＴ障害の発生時に冷静に対処できるようになっている。

○こうした取組が行動計画として公表され、定期的に評価されるとともに必要に応じて適切に見直されている。

○これら各関係主体の取組が社会の持続的な発展を支えるものとして確実に定着している。

以降、具体化した将来像を記載する。

1.1 関係主体共通

関係主体共通の具体化した将来像は以下のようなものである。

○自らの置かれている状況を正しく認識し､自らの活動目標を主体的に定めている。

○各々必要な取組を進めており、これについて定期的に自らの対策・施策の進捗状況の確認を行っている。また、他の関係主体の活動状況を把握し、相互に自主的な協力をすることができる。

○ＩＴ障害発生時の対応において、ＩＴ障害の規模に応じて、誰がどのような情報

を集積しているか、誰とどのような情報を共有すべきか、また自らは何をなすべきかを理解している。

○自主的な対応に加えて、必要に応じて他の関係主体と連携を図り統制の取れた対応をとることができる。

1.2 重要インフラ事業者等

重要インフラ事業者等における具体化した将来像は以下のようなものである。

○「情報セキュリティガバナンス」に関する以下の事項が十分に浸透している。

－情報セキュリティ対策は単に情報システムの構築・運用の観点のみならず、企業経営の観点からも検討していること。

－システムの構築・運用と企業経営のそれぞれの責任者が適切に関与する体制を有すること。

－守るべき重要インフラサービスとサービス維持レベルを踏まえて、自らがなすべき必要な対策を理解していること。

－情報セキュリティ対策の対外的な説明に努めていること。

－情報セキュリティ対策の水準の向上のためには可能な限り情報共有を行うという姿勢が積極的に評価される価値観が醸成されていること。

－事業におけるＩＴ障害の発生は隠すべきものではなく、重要インフラ事業者等内の対策に取り組む関係者間で共有すべきものであるという認識を有していること。

○「課題抽出」、「リスク評価」及び「対策の改善」に関する以下の事項が十分に浸透している。

－本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、自らの対策の程度及び残存するリスクを認識していること。

－各種対策の進展や環境変化によるリスク源やＩＴ障害に係るリスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっていること。

－ＩＴ障害が発生した場合でも適切な対策を講じることが可能になっており、その結果として、ＩＴ障害が国民生活や社会経済活動に重大な影響を与えるリスクは可能な限り低減させることができていること。

－これらの取組が対策の継続的な改善の原動力のひとつとなっていること。

○「情報共有」に関する以下の事項が十分に浸透している。

－ＩＴ障害の発生状況等の情報を把握できており、必要に応じて当該情報を分野ごとのセプターやセプターカウンシルを通じて外部の関係主体と共有し、公式又は非公式の連携を行っていること。

1.3 内閣官房

内閣官房における具体化した将来像は以下のようなものである。

○より効果的な対策を進めるための総合調整機能を発揮している。本行動計画の施策群を通じて、情報セキュリティ対策に資する多様な情報が寄せられるようになっており、当該情報を踏まえて関係主体との連携を図っている。

○特に、重大なリスク源やＩＴ障害に係るリスクについての認識が得られ、その対処が重要インフラ事業者等だけでは困難な場合は、解決策の検討とその実現に向けた有機的連携及び調整を速やかに実施している。

2. 各年度における進捗状況の確認・検証を通じた対策・施策の継続的改善

本行動計画に基づく取組を着実に進め、また継続的に改善させていくために、本行動計画の進捗状況についての確認・検証を行う。継続的な改善においては、各関係主体がそれぞれの取組を通じて得た経験を関係主体全体で共有し、相互に取組の改善に活かせるようにすることを重視する。ＩＴ障害は回避すべきものであるが、ＩＴ障害を防いだ経験やＩＴ障害が発生した際に影響範囲を限定した経験は、それ自体を将来の糧として活かすべきものであることを認識することが重要である。

当然ながら、ＩＴ障害を発生させた当事者はその原因と責任の所在を把握し、自らの取組を改善するよう努めるべきものである。しかし、本行動計画の評価・検証においては、原因と責任を追及することに主眼を置くのではなく、むしろ様々な経験から将来の取組の改善に活かせる教訓を抽出し、これを各関係主体のそれぞれの取組の改善に役立てるようにすることを主眼とする。

3. 各年度における進捗状況の確認・検証の実施方法

各年度で行う「結果（アウトプット）を測る視点」からの確認・検証は、本行動計画に基づく個別の情報セキュリティ対策の施策に着目して行う。本行動計画に基づく情報セキュリティ対策の施策群は、いずれも複数の関係主体による多層構造をなしているため検証に用いる指標も多様なものが考え得るが、大別して重要インフラ事業者等による対策の総合的な確認・検証に用いる指標と、政府機関等による施策の確認・検証に用いる指標を設定する。この際、情報セキュリティ対策の施策群ごとの指標については、その数値自体の多寡、増減にとらわれるのではなく、その数値の意味するところを適切に解釈することが重要である。

これらの確認・検証は、サイバーセキュリティ戦略本部が主管の下、重要インフラ事業者等及び重要インフラ所管省庁の協力を得て各年度に内閣官房が行い、重要インフラ専門調査会での審議を経て、サイバーセキュリティ戦略本部に付議する。

また、個別の重要インフラ事業者等による自身の対策の確認・検証については、それが自主的なものであることに鑑み、基本的には重要インフラ事業者等自らが、各年度に行うことが望ましい。

3.1 重要インフラ事業者等による対策の総合的な確認・検証に用いる指標

重要インフラ事業者等は重要インフラサービスの安定的供給に一義的な責任を負うものとして、日々情報セキュリティ対策に取り組んでいる。この取組を継続しかつ着実な改善を期すために、また重要インフラ事業者等の取組に対する政府の支援策をより効果的なものへと改善させていくためには、情報セキュリティ対策の成果を客観的に検証することが重要である。

対策の総合的な確認・検証は、本行動計画の目標である「ＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を踏まえ、重要インフラ分野ごとのＩＴ障害の発生状況を確認・検証することとする。対象とする重要インフラサービスとサービス維持レベルは「別紙２　重要インフラサービスとサービス維持レベル」に示すとおりとする。具体的な指標は、内閣官房が認知したＩＴ障害事例の分野全体での数とする。

なお、個別の重要インフラ事業者等の対策が各々の経営判断に基づく自主的な対策を含むものである以上、重要インフラ事業者等ごと又は分野ごとのＩＴ障害の発生状況を比較して対策を評価することは不適当である。そのため、対策の評価は重要インフラ事業者等による自己評価によるものとし、各々の重要インフラ事業者等が自ら改善に取り組むことが適当である。また、可能であれば自己評価の実施状況を明らかにすることが望ましい。

3.2 政府機関等による施策の確認・検証に用いる指標

本行動計画の施策は「Ⅲ．計画期間内に取り組む情報セキュリティ対策」に示したとおりであるが、これらはいずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである。本行動計画期間においては第２次行動計画にて用いた指標を踏襲しつつ、各施策の効果の検証方法を見直した。

施策の確認・検証は、それぞれの情報セキュリティ対策の施策ごとに、重要インフラ事業者等による情報セキュリティ対策への寄与を検証することとし、具体的な指標は以下のとおりとする。

3.2.1 安全基準等の整備及び浸透

「安全基準等の整備及び浸透」に期待される成果は、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことの実現に向けた、重要インフラ事業者等における各種対策の更なる充実と、その着実な実践である。そのため、指針と安全基準等の項目の充実と、重要インフラ事業者等の安全基準等に基づいた取組の確実な実施に着目した指標を設定する。

＜具体的な指標＞

○指針に採録した対策項目数

○安全基準等の浸透状況等の調査にて把握した安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の割合

○重要インフラ事業者等による指針への意見・要望

3.2.2 情報共有体制の強化

「情報共有体制の強化」に期待される成果は、最新の情報共有体制及び情報連絡・情報提供に基づく情報共有、並びに各セプター及びセプターカウンシルの自主的な活動の充実強化を通じて、重要インフラ事業者等が必要な情報を享受し活用できることである。そのため、整備された情報共有体制と共有された情報の充実に着目した指標を設定する。

＜具体的な指標＞

○内閣官房による情報連絡・情報提供の件数

○セプターカウンシルや分野横断的演習等の関係主体間の情報交換の開催回数

○セプターカウンシルにおける情報共有の件数

3.2.3 障害対応体制の強化

「障害対応体制の強化」に期待される成果は、分野横断的演習を中心とする演習・訓練への参加を通じて、重要インフラ事業者等のＩＴ障害発生時の早期復旧手順及びIT-BCP等の検証、そのために必要な関係主体間における情報共有・連絡の有効性の検証や技術面での対処能力の向上等に対する貢献をすることである。そのため、演習成

果の浸透、現実に即した演習環境の構築、分野横断的演習に加えて参加した演習・訓練及び演習・訓練で得られた知見による重要インフラ事業者等の取組への貢献状況に着目した指標を設定する。

＜具体的な指標＞

○分野横断的演習の参加者数

○演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した参加者の割合

○分野横断的演習を含め組織内外で実施する演習・訓練への参加状況

3.2.4　リスクマネジメント

「リスクマネジメント」に期待される成果は、重要インフラ事業者等が実施するリスクマネジメントの推進、強化である。そのため、重要インフラ事業者等が実施するリスクマネジメントプロセスのうち、内閣官房が支援するリスクアセスメントとリスクコミュニケーション及び協議に着目した指標を設定する。

＜具体的な指標＞

○内閣官房が実施した環境変化調査や相互依存性解析の件数

○セプターカウンシルや分野横断的演習等の関係主体間が情報交換できる機会の開催回数

3.2.5　防護基盤の強化

「防護基盤の強化」に期待される成果は、「広報公聴活動」については、行動計画の枠組みついて広く国民の理解を得ることと及び本行動計画への協力者を関係主体以外にも拡大することであり、「国際連携」については、二国間・地域間・多国間の枠組み等を通じた各国との情報交換の機会や支援・啓発であり、「規格・標準及び参照すべき規程類の整備」については、整備した規程類についての重要インフラ事業者等における利活用である。そのため、本行動計画の周知機会及び国際連携機会の充実並びに規程類の整備状況に着目した指標を設定する。

＜具体的な指標＞

○ニュースレター等による情報の発信回数

○行動計画に関連した講演等の回数

○二国間・地域間・多国間による意見交換等の回数

○重要インフラ防護に資する手引書等の整備状況

○制御系機器・システムの第三者認証制度の拡充状況

4. 行動計画期間の成果の評価に基づく行動計画の見直し

「成果（アウトカム）を測る視点」からの評価は、本行動計画の目標、すなわち理想とする将来像に照らして行う。この際、行動計画に基づく様々な取組が相互に関連して結果・成果を成すものであることに鑑み、個別の取組に対して評価を行うのではなく、重要インフラ防護能力の維持・向上に資する取組の全体、すなわち本行動計画の枠組みに対して総合的かつ分析的に行う。

本行動計画の枠組みの評価を行う際には、施策群の個別の結果・成果だけでは把握しきれない状況も適切に把握して評価を行うことが重要である。そのため、評価に必要となる補完的な情報を収集するために、補完調査を原則として毎年度実施する。

また、評価運営については、行動計画の性質上、毎年の変化を追っても直ちに改善策を検討することが困難であることから、原則として３年に１度、サイバーセキュリティ戦略本部で実施することとし、そのために必要な調査・検討は重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行う。

このことから、成果の評価を踏まえた行動計画の見直しについても原則として３年に１度、サイバーセキュリティ戦略本部での実施とし、そのために必要な調査・検討は重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行う。

なお、社会動向の大きな変化等、本行動計画が想定しえなかった事象が発生した場合は、３年に１度はその限りとしない。

別添：情報連絡・情報提供について

1. ＩＴの不具合等に関する情報

ＩＴ障害を含むＩＴの不具合や予兆・ヒヤリハットに関する情報（以下「ＩＴの不具合等に関する情報」という。）には、①ＩＴ障害の未然防止、②ＩＴ障害の拡大防止・迅速な復旧、③ＩＴ障害の原因等の分析・検証による再発防止の３つの側面が含まれ、政府機関等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間及び相互依存性のある重要インフラ分野間においてはこうした情報を共有する体制を強化することが必要である。

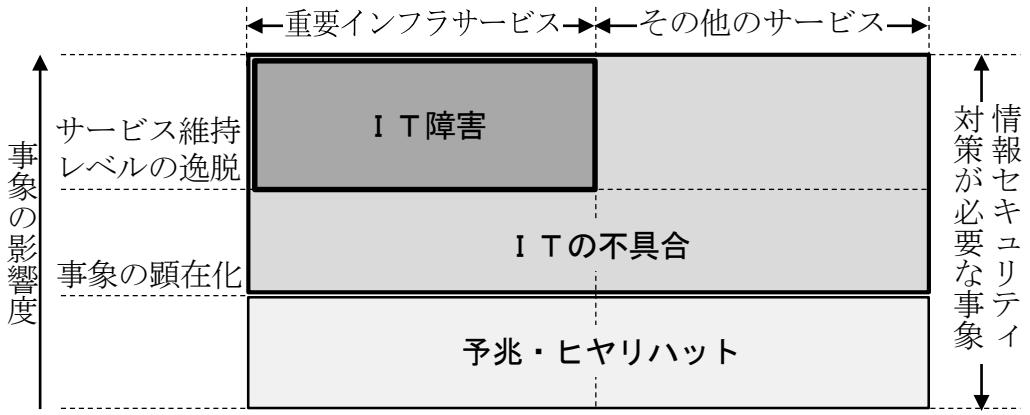
ＩＴの不具合等に関する情報の各側面としては以下のようなものが含まれる。

①未然防止　　ＩＴの不具合等の原因に係る情報（防護方策等を含む）
②拡大防止・復旧　ＩＴ障害発生後の影響伝搬予測及び復旧に資する情報
③再発防止　　事後分析に資する情報の共同収集及び分析・検証の結果

なお、予兆・ヒヤリハットでは事象が顕在化していないものの、顕在化した際にはＩＴ障害に至ることも考えられることから、ＩＴの不具合と同様に、対象とすることが必要である。

したがって、本行動計画における情報共有の範囲は、図表５に示すものとする。

図表５　情報共有の対象範囲



2. 重要インフラ事業者等からの情報連絡

2.1 情報連絡を行う場合

情報連絡が必要となる場合は、ＩＴ障害を含むＩＴの不具合や予兆・ヒヤリハットを確認した場合であって、法令等で報告が義務付けられている場合又は重要インフラ事業者等が情報共有を行うことが適切と判断した場合である。

なお、上記に該当するかどうか不明な場合については、重要インフラ所管省庁又は内閣官房に対して相談することが望ましい。

2.2 情報連絡の内容

情報連絡の内容は、その時点で判明している事象や原因を随時連絡することとする。この際、全容が判明する前の断片的又は不確定なものであっても差し支えない。

なお、重要インフラ所管省庁から内閣官房に情報連絡を行う際に必要なＩＴの不具合等に関する共通の分類及びカテゴリの設定等は、各重要インフラ事業者等の運用性等も勘案して行うこととする。

2.3 情報連絡の仕組み

重要インフラ事業者等から重要インフラ所管省庁を通じて内閣官房に至る情報連絡の手順は以下のとおりとする。

① 重要インフラ事業者等は、「別紙５　ＩＴ障害発生時における連絡体制等」に示す連絡体制等に基づき重要インフラ所管省庁に連絡する。

② 重要インフラ所管省庁において所管分野ごとに選任された内閣官房への併任者（リエゾン）は、該当分野の重要インフラ事業者等から受けた連絡を内閣官房に連絡する。

③ 内閣官房は、連絡された情報を適切に管理し、情報連絡元が指定する情報共有の可能な範囲で取り扱う。

2.4 情報連絡された情報の取扱い

情報連絡された情報の取扱いについて、内閣官房及び連絡を受けた重要インフラ所管省庁は、法令等に定めがある場合又は連絡を行う重要インフラ事業者等の了承がある場合を除き、原則として行政機関の保有する情報の公開に関する法律（平成11年法律第42号）第５条第２号ロに規定する情報（任意提供情報）として取り扱う。なお、当該情報が同号ただし書に規定する情報に該当する場合には、公開されることがある。

3. 重要インフラ事業者等への情報提供

3.1 情報提供の対象とする重要インフラ事業者等の範囲

内閣官房から重要インフラ事業者等への情報提供の範囲は、情報提供元があらかじめ示す情報共有可能な範囲のうち、内閣官房が当該情報に関係すると考える重要インフラ分野とする。なお、情報提供元が示す情報共有可能な範囲を越えて情報共有する必要があると内閣官房が認める場合には、その共有範囲の変更について情報提供元との間で調整を行うことができる。

3.2 情報提供の内容

情報提供は、重要インフラ所管省庁、情報セキュリティ関係省庁、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から提供される幅広い情報について、集約、分析等を行い、重要インフラ事業者等の情報セキュリティ対策に有効と考えられるものについて行う。

また、重要インフラ事業者等からの情報連絡が次に掲げる①又は②に該当する場合、情報連絡を行った重要インフラ事業者等が不利益を被らないよう、情報連絡をした重要インフラ事業者等が特定されないよう情報を加工する等適切な措置を講じた上で情報提供を行う。

① セキュリティホールやプログラム・バグ等に関する情報を入手した場合等であって、他の重要インフラ事業者等においてもその情報に関係する問題が生じるおそれがあると認められる場合。

② サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合。

3.3 情報提供の仕組み

内閣官房から重要インフラ所管省庁を通じて重要インフラ事業者等に至る情報提供の手順は以下のとおりとする。

① 内閣官房が情報提供を行う場合は、重要インフラ所管省庁のリエゾンを通じて行う。その際、情報提供を受けた者が、その情報を容易に活用できるようにするため、重要度や内容等に応じた情報の分類及び取扱い範囲が一目で認識できるよう、適切な識別方法を設ける。

② 重要インフラ所管省庁のリエゾンはセプターの窓口（PoC）に対して情報を伝達する。

③ セプターは、セプターを構成する重要インフラ事業者等に対して情報を伝達する。

④ 早期警戒情報等であって特に緊急性を有する場合には、①～③の手順にかかわらず、内閣官房から直接セプター又は個別重要インフラ事業者等へ提供するとともに、重要インフラ所管省庁のリエゾンに同報する。ただし、識別方法の適正化については、①の手順

に準ずる。

3.4 情報提供のための連携体制

内閣官房は、重要インフラ所管省庁を通じて重要インフラ事業者等に提供する情報の集約及び重要インフラ事業者等への情報提供において、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等と以下のとおり連携する。

① 情報セキュリティ関係省庁及び情報セキュリティ関係機関から提供される幅広い情報の集約。

② サイバー空間関連事業者から必要に応じて、ＩＴ障害に関する付加情報等の集約。

③ 情報の集約・分析においては、必要に応じ、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に連携等を要請。

④ 大規模ＩＴ障害に関する情報については、平時の情報共有体制に加え、内閣官房、事案対処省庁、防災関係府省庁から構成される情報共有体制の下で情報を集約及び共有。

3.5 情報の質の向上（分析情報、影響度等）

提供する情報については、以下の点を考慮しつつ、その質の向上を図る。

① 情報を突き合わせることによる精度の向上。

② ①に基づく重要度・優先度の判断。

③ 重要インフラ分野のサービス停止・低下が原因で発生したＩＴ障害や各分野間に共通するリスク源により発生したＩＴ障害に関する他の重要インフラ分野への影響予測。

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(注2)	ＩＴ障害やその影響の例
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	・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等 ・放送サービスの停止
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	・預金の払い出し、振込等資金移動、融資業務の停止 ・資金清算の停止 ・電子記録、資金決済に関する情報提供の停止 ・保険金の支払い停止 ・有価証券売買の停止 ・社債・株式等の振替の停止 ・金融商品取引の清算の停止　　等
航空	・主たる定期航空運送事業者 ・国土交通省（航空管制・気象）	・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 ・航空管制システム ・気象情報システム	・運航の遅延、欠航 ・航空機の安全運航に対する支障等
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	・列車運行の遅延、運休 ・列車の安全安定輸送に対する支障等
電力	・一般電気事業者、日本原子力発電(株)及び電源開発(株)	・制御システム ・運転監視システム	・電力供給の停止 ・電力プラントの安全運用に対する支障等
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	・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等
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）	・政府・行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん
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）	・診療支援部門における業務への支障等
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	・水道による水の供給の停止 ・不適当な水質の水の供給　　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	・輸送の遅延・停止 ・貨物の所在追跡困難
化学	・主要な石油化学事業者	・プラント制御システム	・プラントの停止 ・長期にわたる製品供給の停止
クレジット	・主要なクレジットカード会社　　等	・オーソリゼーションシステム　　等	・オーソリゼーションの停止
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	・石油の供給の停止 ・製油所の安全運用に対する支障　　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。
注２　対象となる重要システムの詳細については、ＩＴ障害やその影響の例を踏まえ、重要インフラ事業者等において定める。

別紙２　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	

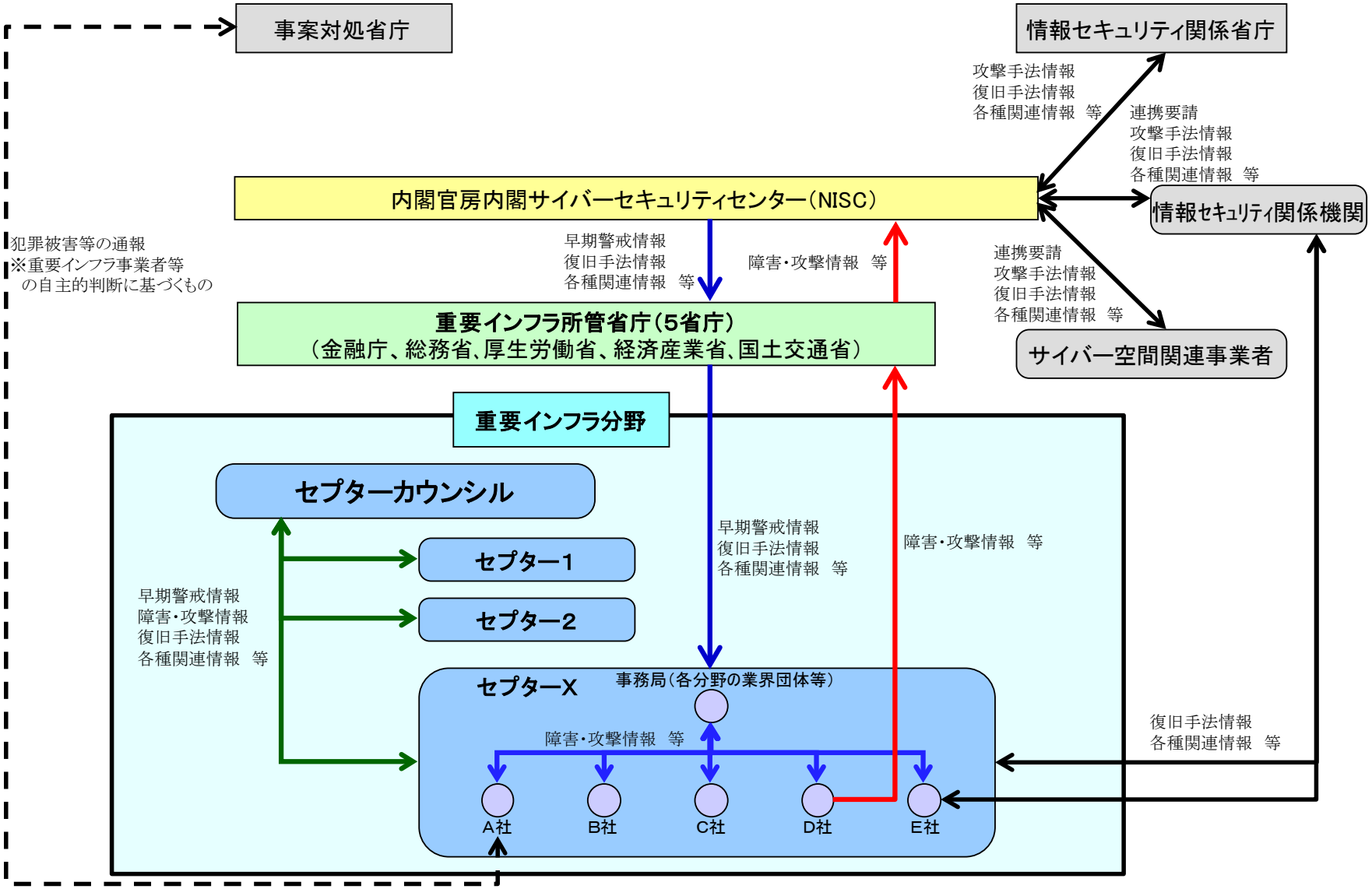
注　ＩＴを全く利用していないサービスについては対象外。

別紙３　情報連絡における事象と原因の類型

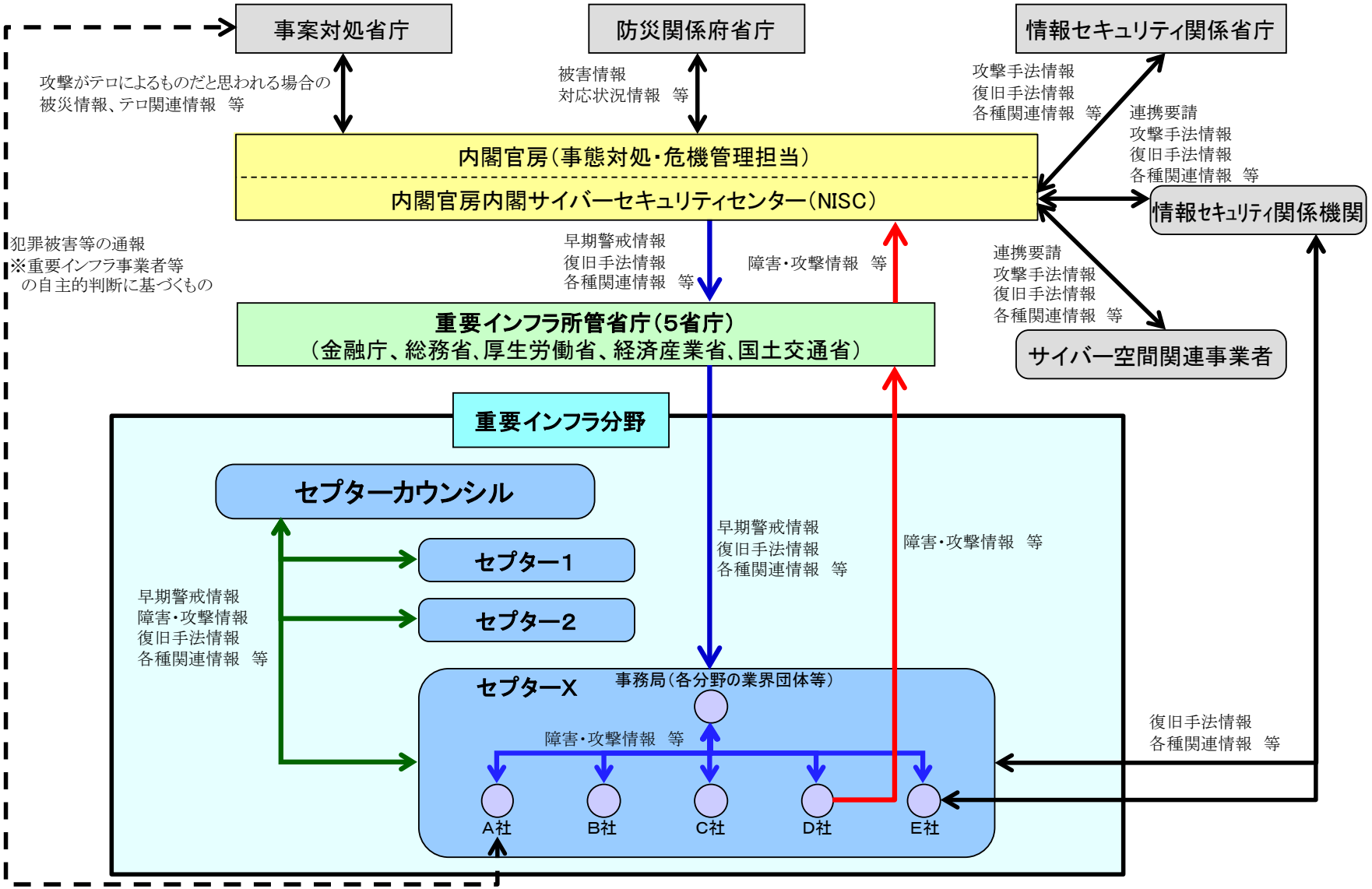
事象の類型		事象の例	説明
未発生の事象		予兆・ヒヤリハット	サイバー攻撃の予告などの予兆や、事象の発生には至らなかったミス、マルウェアが添付された不審メールの受信などによるヒヤリハットの発生
発生した事象	機密性を脅かす事象	情報の漏えい	組織の機密情報等の流出など、機密性が脅かされる事象の発生
	完全性を脅かす事象	情報の破壊	Webサイト等の改ざんや組織の機密情報等の破壊など、完全性が脅かされる事象の発生
	可用性を脅かす事象	システム等の利用困難	制御システムの継続稼働が不能やWebサイトの閲覧が不可能など、可用性が脅かされる事象の発生
	上記につながる事象	マルウェア等の感染	マルウェア等によるシステム等への感染
		不正コード等の実行	システム脆弱性等をついた不正コード等の実行
		システム等への侵入	外部からのサイバー攻撃等によるシステム等への侵入
		その他	上記以外の事象

原因の類型	原因の例
意図的な原因	不審メール等の受信、ユーザＩＤ等の偽り、DoS攻撃等の大量アクセス、情報の不正取得、内部不正、適切なシステム等運用の未実施など
偶発的な原因	ユーザの操作ミス、ユーザの管理ミス、不審なファイルの実行、不審なサイトの閲覧、外部委託先の管理ミス、機器等の故障、システムの脆弱性、他分野の障害からの波及など
環境的な原因	災害や疾病など
その他の原因	上記以外の脅威や脆弱性、原因不明など

別紙４－１　情報共有体制（平時）



別紙４－２　情報共有体制（大規模ＩＴ障害対応時）



別紙５　ＩＴ障害発生時における連絡体制等

重要インフラ分野		既存の連絡体制	ＩＴ障害発生時における緊急時の連絡体制
情報通信		(1) 重要インフラ事業者等→政府 ・電気通信事業法に基づく、業務の停止等の総務大臣への報告 ・放送中止事故、重要無線通信妨害等の総務省への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ウィルス発生等緊急情報を業界内及び総務省との間で通報・共有	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・T-CEPTOAR、放送CEPTOAR及びケーブルテレビCEPTOARの連絡体制を活用して実施 ・既存の連絡体制を活用して実施
金融	銀行等 生命保険 損害保険 証券	(1) 重要インフラ事業者等→政府 ・業法に基づく、サービス遅延・停止等の内閣総理大臣（金融庁）への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・銀行等CEPTOARの連絡体制を活用して実施 ・証券CEPTOARの連絡体制を活用して実施 ・生命保険CEPTOARの連絡体制を活用して実施 ・損害保険CEPTOARの連絡体制を活用して実施 ・その他事業者団体等を通じて実施
航空		(1) 重要インフラ事業者等→政府 ・航空法に基づく、航空機の事故等に関する国土交通大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ＩＴ障害に関する連絡窓口を設置 ・航空保安体制の不具合に関する情報を関係する機関で共有（空港単位）	(1) 重要インフラ事業者等→政府 ・事故時は既存の事故報告体制により実施。 ・事故に至らないＩＴ障害に関しては、航空分野におけるCEPTOARの連絡体制を活用して実施。 (2) 政府→重要インフラ事業者等 ・航空分野におけるCEPTOARの連絡体制を活用して実施 ・連絡窓口を通じて重要インフラ事業者等へ直接連絡
鉄道		(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通大臣への報告 ・ＩＴ障害に関する連絡体制を整備 (2) 重要インフラ事業者等間 ・特になし	(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・事故時は既存の事故報告体制により実施。 ・鉄道CEPTOARの連絡体制を活用して実施
電力		(1) 重要インフラ事業者等→政府 ・電気関係報告規則に基づく、供給支障事故等に関する経済産業大臣への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ＩＴ障害に関する窓口を設置	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・電力におけるＩＴ障害に係る情報共有・分析機能の連絡体制を活用して実施 ・連絡窓口を通じて重要インフラ事業者等へ直接連絡

重要インフラ分野	既存の連絡体制	ＩＴ障害発生時における緊急時の連絡体制
ガス	(1) 重要インフラ事業者等→政府 ・ガス事業法施行規則に基づく、一定規模のガス供給支障等の経済産業大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・災害によりガス供給支障が発生した場合等における、ガス協会「救援措置要綱」に基づく業界内連絡	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・ガスCEPTOARの連絡体制を活用して実施 ・事業者団体を通じて実施
政府・行政サービス	(1) 各府省庁→内閣官房 ・「政府機関の情報システムに関する緊急時の連絡等について（平成12年４月17日）」に基づく連絡 (2) 内閣官房→各府省庁 ・「政府機関の情報システムに関する緊急時の連絡等について（平成12年４月17日）」に基づく情報提供 (3) 地方公共団体→政府 ・「情報セキュリティインシデント発生時における対応及び報告並びに緊急時連絡体制の整備等について（通知）」に基づく情報提供 (4) 政府→地方公共団体 ・「情報セキュリティインシデント発生時における対応及び報告並びに緊急時連絡体制の整備等について（通知）」に基づく情報提供	(1) 各府省庁→内閣官房、内閣官房→各府省庁 ・政府部内連絡体制で実施 (2) 地方公共団体→政府、政府→地方公共団体 ・自治体CEPTOARの連絡体制を活用して実施 ・既存の連絡体制を活用して実施
医療	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等 ・医療CEPTOARの連絡体制を活用して実施
水道	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等 ・水道CEPTOARにおけるＩＴ障害情報の取扱いに関するガイドラインの連絡体制を活用して実施
物流	(1) 重要インフラ事業者等→政府 ・各事業法等に基づく、事故等の国土交通大臣への報告 (2) 政府→重要インフラ事業者等 ・内閣府　災害対策基本法に定める指定公共機関	(1) 重要インフラ事業者等→政府 ・事故等は既存の事故報告体制により実施 ・事故に至らないＩＴ障害に関しては、物流CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・物流CEPTOARの連絡体制を活用して実施

重要インフラ分野	既存の連絡体制	ＩＴ障害発生時における緊急時の連絡体制
化学	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 ・化学CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・化学CEPTOARの連絡体制を活用して実施
クレジット	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・業界内情報共有等	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・クレジットCEPTOARの連絡体制を活用して実施
石油	(1) 重要インフラ事業者等→政府 ・関係諸法令に基づく、所管及び関係官庁への報告等 (2) 政府→重要インフラ事業者等 ・業界内情報共有等	(1) 重要インフラ事業者等→政府 ・石油CEPTOARの連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・石油CEPTOARの連絡体制を活用して実施

別紙６　定義・用語集

IT-BCP等	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。
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「別紙２　重要インフラサービスとサービス維持レベル」における「サービス維持レベル」を下回るもの。
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。
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、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。
事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
指針	安全基準等の策定・改訂に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先進的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。本編はサイバーセキュリティ戦略本部決定による。対策編は対策項目のチェックリストとして具体例を記載したもの。
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、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもので、重要インフラ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きのうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに「別紙２　重要インフラサービスとサービス維持レベル」に定めるもの。
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等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、経済産業省及び国土交通省。
重要インフラ分野	「情報通信」、「金融」、「航空」、「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。「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」に例を示す。
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。

情報セキュリティ対策	ＩＴ障害が国民生活や社会経済活動に影響を与えないようにするための幅広い取組。
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ＩＴの不具合等に関する情報（ＩＴ障害を含むＩＴ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。
大規模ＩＴ障害	官邸対策室等が官邸危機管理センターに設置される等の政府として集中的な対応が必要となる規模のＩＴ障害。
ヒヤリハット	想定外又は予期しない事象によって、ＩＴの不具合に至らなかったものの、ＩＴの不具合に直結するおそれのあった事象。
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項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。

資料３－６

The Basic Policy of
Critical Information Infrastructure Protection
(3rd Edition)

（改定案）

(Tentative Translation)

May 19, 2014
Information Security Policy Council

May 25, 2015 (Revised)
Cybersecurity Strategic Headquarters

Government of JAPAN

(This page intentionally left blank.)

Contents

I. INTRODUCTION

1. BACKGROUND

The Basic Policy[1] of Critical Information Infrastructures (hereinafter abbreviated as CII) is a shared basic policy for the government, which bears responsibility for the protection of the CII, and CII providers, which independently carry out relevant protective measures. It was established to serve as the basis for the policy related to information security measures for Japan's critical infrastructure, such as the enactment of the *"Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructure" (concluded in the December 2000 Information Security Measure Promotion Meeting)*, prior to the establishment of the National Information Security Center (NISC)[2].

After the establishment of the NISC, in 2005, the *"First Action Plan on Information Security Measures for Critical Information Infrastructures"* (hereinafter referred to as the *First Action Plan*) was established based on the *"Basic Orientation for Countermeasures Necessary for Protecting Critical Infrastructure from IT Outages and Ensuring Business Continuity of Critical Infrastructure Providers"* presented in the Information Security Policy Council of the same year. Based on the *First Action Plan*, relevant measures were taken by the stakeholders including the government and 10 CII sectors with a view to reducing IT outages at CII as close to zero as possible.

Furthermore, the *"Second Action Plan on Information Security Measures for Critical Information Infrastructure"* (hereinafter referred to as the *Second Action Plan*) was established in 2009 which identified policies to be implemented by the nation, based on the basic measures for CIIP and the public-private information sharing framework established by the *First Action Plan*. The *Second Action Plan* has taken over the measures of the "maintenance and promotion of the safety principles", "enhancement of information sharing", "common threat analysis[3]" and "cross-sectoral exercises" in the *First Action Plan* and also additionally identified policies for "response to environmental changes" in order to appropriately address ever-changing social and technological environment.

In this manner, the protection of Japan's CII has been carried out for 13 years since the Special Action Plan and even for 8 years since the establishment of the *Second Action Plan*. It can be concluded that relevant measures have been steadily implemented based on 5 policies

[1] The terminology "Action Plan" was used in the previous version of this document. However, taking the nature of this document into consideration, the title is renamed as "The Basic Policy of Critical Information Infrastructure Protection".

[2] The National Information Security Center (NISC) was reorganized as the "National center of Incident readiness and Strategy for Cybersecurity (NISC)" on January 9, 2015.

[3] In the *First Action Plan*, this was referred to as "interdependency analysis".

such as establishing a robust information sharing system.

As such, this Basic policy appropriately reflected the lessons learned through the assessment of a group of policies identified in the *Second Action Plan* while taking into account the *Cybersecurity Strategy* (determined at the June 2013 Information Security Policy Council).

Furthermore, in addition to the lessons learned from the experience of dealing with system outages and data loss during the Great East Japan Earthquake, this Basic Policy also reflects appropriate responses to the ever-changing social and technological environment and the trends of increasingly sophisticated and complex cyber-attacks carried out in recent years.

2. CLARIFICATION OF THE PURPOSE OF CIIP

As a basis for the implementation of this Basic Policy, it is necessary to clarify the purpose of the protection of CII and to share awareness among stakeholders.

Cybersecurity Strategy identified "Ensuring Free Flow of Information", "Responding to Increasingly Serious Risks", "Enhancing Risk-based Approach" and "Acting in Partnership Based on Shared Responsibility" in its Basic Principles, and the purpose of the *Second Action Plan* are consistent with the *Cybersecurity Strategy*.

As such, in addition to maintaining the elements of the purpose of the *Second Action Plan*, the need for continuous provision of CII services was added, which further clarified the purpose of CII protection.

Purpose of "CII protection" (referred to as "CIIP")

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

Basic Principles for CIIP

In the first place, CII operators should implement measures for CIIP on their own responsibility. In addition, a sense of security should be nurtured among the public and social development, resilience and international competitiveness should be promoted through activities in cooperation between Government and private sectors.

- The CII operators should respectively take measures and make effort for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- Government organizations should provide necessary support for CII operators' activities for CIIP.
- Each CII operator should cooperate and coordinate with other stakeholders due to the limit of each operator’s individual information security measures to address various threats.

3. LESSONS LEARNED FROM ACTIVITIES UNDER THE SECOND EDITION

The *Second Action Plan* is composed of the following 5 policies.

[1] Maintenance and promotion of the safety principles

[2] Enhancement of information sharing system

[3] Common threat analysis

[4] Cross-sectoral exercises

[5] Response to environmental changes

Each policy's outcome and challenges are summarized as follows:

3.1 Outcome

The assessment of these policies was carried out according to the assessment indexes set in the *Second Action Plan* since the *Second Action Plan* was determined based on the most updated information regarding CII as of 2009. Consequently, for the expected targets, it can be concluded that a certain result was achieved as elaborated below.

For maintenance and promotion of the safety principles, stakeholders involved in measures for CIIP could understand and identify necessary measures which they should take independently and made efforts to carry out such measures under a periodic self-inspection. As a result, an integrated and steady review cycle was established for guidelines and the safety principles, which reinforced the promotion of measures for CIIP.

As for enhancement of information sharing, for the purpose of addressing the ever-changing social and technological environment surrounding CII security measures and increasingly complex and sophisticated cyber-attacks, frameworks for information sharing with NISC was established through cooperation between Government and private sectors, and the utilization of such frameworks was steadily achieved. In addition, information sharing within and among CEPTOARs was realized and necessary information was shared and utilized among CII operators.

For common threat analysis, as a result of carrying out examinations of common threat analysis based on analyses of cross-sectoral circumstances which is indispensable for the maintenance and enhancement of protective capability for overall CII, basic material was provided which contributed to the establishment of business continuity plans for CII operators and part of the result was reflected in guidelines.

For cross-sectoral exercises, as a result of making efforts to provide opportunities for verification of systems for communication and collaboration through simulated exercises with

the participation of both public and private stakeholders in all relevant sectors in case of IT outages, the number of organizations and individuals participating in the exercises is on an upward trend. Furthermore, it contributed to information security through verification of CII operators' manual for early recovery and business continuity plans in case of an IT outage, based on the lessons learned through the exercises.

Regarding public relations activities in particular among the response to environmental changes, materials on the results of CII information security policy, meeting materials of CII Special Committee under the Information Security Policy Council and other materials were posted and published on the Cabinet Secretariat website. In addition, lectures focusing on information security policy and other events were held. As for development of risk communication, exchanges of opinion were held among CIIP supporting agencies and a mutual understanding WG was held at a CEPTOAR council. As for promotion of international cooperation, cooperation with other foreign countries was carried out through such initiatives as participating in the Meridian[4] and the Cyber Storm Exercises[5]. Through these initiatives, relevant efforts were made to improve capabilities to perceive threats due to environmental changes.

3.2 Challenges

Through the implementation of each policy, challenges were identified which required improvement/reinforcement of the policy based on environmental changes from social/technological aspects. The principal challenges for each policy are described below.

As for maintenance and promotion of the safety principles, reexamination in conformity with measures for continued improvement in line with the PDCA cycle of CIIP measures at CII operators should be carried out. This is because measures for CIIP also have an effect not only on CII operators themselves but also on the maintenance and enhancement of protective capability for overall CII. Furthermore, there have been requests from CII operators for sharing guidelines which have prioritized items based on the actual conditions of measures.

With regard to enhancement of information sharing, necessary measures to establish an effective information sharing system include: eliminating the gap in terms of the frequency of information sharing among sectors; further elaborating "threat patterns"; establishing an emergency information sharing system to cope with IT crises, which should be the same basis of normal conditions; and studying forms of coordination with other new stakeholders.

[4] An international forum where CII supervisors from various countries meet and carry out discussions specialized for CII protection.

[5] A large scale exercise held by the U.S. government. Japan participates as a member of the IWWN (International Watch and Warning Network) when promoting international measures for handling vulnerabilities, threats and attacks.

For common threat analysis, detailed analysis of threats based on changes over time and environmental changes which have become evident is necessary. The purpose of this analysis is to improve the effects of threat analysis and to conduct reviews on how to carry out common threat analysis from the perspective of expanding the scope of such analysis to include threats which may have a major effect broadly even if not on all sectors instead of limiting the scope only to the common threats across all sectors, looking ahead to the review of the subject and role as well as the frequency of such analysis.

As for cross-sectoral exercises, the design of exercise environments is limited since the IT usage and information management at each organization differs, which makes it unlikely to realize a major expansion of the number of participants. For this reason, with a view to providing CII operators opportunities to identify shortcomings of CIIP measure, further dissemination and promotion of the outcome of the exercises across the entire CII sectors should be realized , rather than depending only on the expansion of participants. Additional issues to be addressed include: qualitative improvement of how to carry out exercises based on the assessment of results; identification of relevant stakeholders based on responses to CII IT outages; and examination of collaboration between exercises and training sponsored by and responsible ministries for CIIP and those in charge of disaster prevention.

Regarding public relations activities in particular among the response to environmental changes, reexamination of public relations activities depending on the purpose and the scope of information disclosure should be carried out, while ensuring consistency among policies in the next-term Basic Policy. For development of risk communication, challenges include: having a definition of risk management in conformity with international standards; reexamination of information sharing which takes into account the balance between the secrecy of sensitive information and the value of such information; and continued mid- to long-term examination and study of the themes of environmental changes such as new IT technologies which will be developed and utilized in the mid- to long-term and a significant impact of threat against which is expected. For promotion of international cooperation, continuous promotion of cooperation with other countries is necessary in order to quickly address increasingly globalized risks in the cyberspace that transcends national borders. It is also necessary to reinforce international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks in the Asia-Pacific, such as with ASEAN, as well as with the United States and Europe.

4. ISSUES TO BE CONSIDERED

In addition to identifying the challenges in the previous section and the issues which were specified in the *Cybersecurity Strategy*, the following examinations were carried out to determine the direction of this Basic Policy based on the aforementioned challenges.

Issue 1	While CII protection continues to develop as a system, in regard to the *"In the first place, CII operators should implement measures for CIIP on their own responsibility."* in the Basic Principles, there are some CII operators which are not implementing such measures or which lack sufficient understanding on this point. What are the appropriate ways to promote effective and voluntary activities by those CII operators?

<Direction>

* The content should not be something too idealistic that are difficult for CII operators to implement in a realistic way. It should take into account the reality and be something "accomplishable" in line under the current situation. For example, expressions such as "absolute security is expected" or "100% perfection is anticipated" should be avoided.
* Basic items should be articulated in the Basic Policy so that executives and senior managers in the business community who hold the key to ensure information security at CII operators can understand the need for the implementation of the Basic Policy.
* Since both experts as well as non-experts are likely to read the Basic Policy, the Plan should be something easy to comprehend for any relevant parties so that each party understands what kind of measures are required to take under the Basic Policy.
* Clarify the PDCA cycle for maintenance and enhancement of protective capability for CII, particularly vis-à-vis small- and medium-sized CII operators as well as those operators still in the process of developing such capability, which will contribute to promoting effective and voluntary measures by those operators.
* Explain in detail the importance of risk management and the need for introducing such risk management by CII operators so as to address environmental changes in a flexible manner.
* Compile regulations across various layers which CII operators are required to understand into a certain kind of package in a way that such package can easily be shared and handed over to successors among relevant parties despite high turnover.
* Further promote public relations activities so that even after the Basic Policy is released, appropriate response will be made to address ever-changing environment and collection and provision of relevant information will be continuously carried out.

Issue 2	In regard to ever-changing social and technological environment and threats which have become increasingly serious year by year, there are concerns that measures have not been fully taken to respond in an appropriate and quick manner. What type of activities, both in the public and private sectors, will be necessary in order to appropriately address such environmental changes and threats? In addition, isn't it necessary to consider if there are any actors which should be included as stakeholders?

<Direction>

* Add relevant parties among cyberspace-related operators as stakeholders so as to ensure more robust information sharing.
* Promote greater awareness among relevant parties that activities of CII operators in cyberspace could be targeted and be exploited and that they should bear responsibility accordingly.
* Conduct examination on priority risk sources[6] across multiple areas and continual examination of mid- to long-term changes of new technologies, systems, etc., taking into account the fact that threats and vulnerabilities in each area and among CII sectors vary and that social and technological environment is constantly changing.

Issue 3	While a variety of activities have been initiated among stakeholders to address potential IT outages, there are concerns that the management and systems (public-private and public-public) in the event of a severe IT outage have not been sufficiently identified. Isn't it necessary to identify the scope of information which needs to be shared and to elaborate each stakeholder's response and coordination mechanism in the event of such a severe IT outage?

<Direction>

* Enhance an effect of exercises, training, etc., through collaboration among exercises and trainings among relevant stakeholders.
* Establish a mechanism which detects when and what kind of IT crises require special warnings among CII operators, and clarify to the possible extent who should be added as stakeholders and how they should be added to a response systems under normal circumstances (situations other than during IT crises response). (*It is not realistic to set up an entirely new system when an incident occurs.)

[6] According to *JIS Q 31000:2010*, risk source is defined as "elements which alone or in combination has the intrinsic potential to give rise to risk".

5. REVIEW OF THE SCOPE OF CII

During the process of compiling this Basic Policy, deliberation was carried out on the scope of CII, which is currently composed of 10 sectors identified in the *Second Action Plan*. Further study was carried out to determine whether new sectors should be added in the list of CII.

In addition, as for issues identified in the *Cybersecurity Strategy*[7] as something that further deliberation will be carried out on, including the scope of the CII, deliberation will continue by taking into account environmental changes and based on coordination with relevant parties.

5.1 Results

Deliberation was carried out, based on the lessons learned from the past experiences, such as during the Great East Japan Earthquake.

In the case of deliberation, we have conducted identification of sectors that had not been identified as CII in the *Second Action Plan*. But these might make same serious impacts on the public welfare and socioeconomic activities as existing CII sectors in the event of an IT outage.

As a result, several sectors were identified as necessary to be added as new CII sectors as shown in Table 1.

Table 1. Results of study on the scope of CII

Classification	Viewpoint/Necessity	Sector
Sectors to be added due to the effects in the event of an IT outage of the sectors concerned	Value and scale of the service to be provided by the sector	Credit card services
	Scale of the potential risk under a situation where the sector gets out of control	Chemical industries, petroleum industries
Sectors to be added due to the effects on the information systems of the current CII sectors	Interdependency with the current CII sectors	Petroleum industries (See above)

As a result, in this Basic Policy, the CII sectors are composed of the following 13 sectors: "information and communication services", "financial services", "aviation services", "railway services", "electric power supply services", "gas supply services", "government and administrative services (including municipal government)", "medical services", "water services", "logistics services", "chemical industries", "credit card services" and "petroleum industries".

When these added sectors participate in the existing efforts as CII, it is important for the sector to recognize why the sector was added and what is the merit of the participation without

[7] Refer to *"2. Basic Policy" - "(3) Roles of Multi-Stakeholder" - "② Roles of critical infrastructure providers"* (p. 20).

doubts, in order to understand the necessity of own initiative.

For ministries and agencies which have jurisdiction over the added sectors and for those industry groups which are candidates for serving as CEPTOAR secretariat, a pivot to ensure information sharing, explanations were made on the above viewpoints. As a result, there is shared understanding among relevant parties about the addition and the participation of new sectors as CII. Furthermore, the relevant industry groups are identifying critical information systems and service maintenance levels and preparing for the establishment of a CEPTOAR.

5.2 Relationship between existing CII sectors and added sectors

7 years have passed since the establishment of the information sharing system in FY2007. Currently, each CEPTOAR has certain experience through implementing CIIP measures and has unique qualities originating from the nature of each operation and others.

Against such backdrop, when these added sectors participate as new CEPTOARs, there is a concern that the activities of the existing CEPTOARs could be overwhelming. It is necessary for the Cabinet Secretariat to give advice to those new sectors, keeping in mind that cooperation with other CII operators in the same CII sector and CII operators in other CII sectors is important. In addition, it is also expected that at a CEPTOAR council, CEPTOARs advice will be given to the added sectors out of a spirit of mutual support, which will contribute to maintenance and enhancement of protective capability for overall CII.

6. OUTCOME OF THE REVIEW FOR THE REVISION OF BASIC POLICY

Based on the challenges and directions identified, , in the process of compiling this Basic Policy, it was decided that the basic framework of the *Second Action Plan*, which was in conformity with the *Cybersecurity Strategy*, would be maintained. However, individual policies and the implementation systems were decided to be revised, and through reinforcing and refining the components of the Basic Policy, the policy group structure shown in Table 2 was specified.

Table 2. Policy groups and direction of reinforcing and refining the components of the Basic Policy

Policy groups in this Basic Policy	Policy groups in the *Second Action Plan* and the status of each group	Direction of reinforcing and refining the components of the *Second Action Plan*
1. Maintenance and promotion of the safety principles	Keep the element of *"[1] Maintenance and promotion of the safety principles"*	- Articulate the process of reflecting the results on guidance and measures - Make an appeal based on the growth models, etc. and conduct reviews on the actual status of the implementation of relevant measures
2. Enhancement of information sharing system	Keep the element of *"[2] Enhancement of information sharing system"*	- Review and rearrange the relationship of each stakeholder in the information sharing system, including new stakeholders - Review the scope of information (threat patterns, etc.) which should be shared among relevant parties based on the increase in cyber-attack related information - Clarify crisis management system in case of IT crises based on the management under normal circumstances
3. Enhancement of incident response capability	Re-arrange the element of *"[4] Cross-sectoral exercises"*	- Enhance overall IT outage response system after developing an understanding of the overall image of CII related exercises and training - Ensure qualitative enhancement of cross-sectoral exercises in view of the need for coordination with new stakeholders
4. Risk management	Re-arrange the element after integrating a portion of *"[3] Common threat analysis"* with *"[5] Response to environmental changes"*	- Implement a mid- to long-term studies on potential risk sources which could have a major impact on multiple sectors as a result of environmental changes as well as environmental changes which could have a major impact in the future - Make an appeal for CII operators to have accurate understanding on the current circumstances and on risk management which will be the key to identify goals on their own responsibilities
5. Enhancement of the basis for CIIP	Re-arrange after excluding the sections of *"[5] Response to environmental changes"* integrated with *"[3] Common threat analysis"*	- Add reference for related international standards/norms, regulations etc. and method for utilizing those in addition to public relations and international cooperation

In order to ensure an appropriate response to major environmental changes which could take

place after this Basic Policy is issued, it is necessary to continually monitor environmental changes and identify threats from the information, and to construct systems that will enable flexible response. In addition, it is also important for the systems to be able to seamlessly shift from that of normal circumstances to that of IT crises while ensuring robust measures to enhance IT outage response systems, rather than just focusing on prevention which was apriority previously.

II. EXECUTIVE SUMMARY OF THE BASIC POLICY

The key points for this Basic Policy are as follows;

(1) Purpose of "CII protection" (referred to as "CIIP")

In order to continuously provide CII services and to avoid serious effects on the public welfare and socioeconomic activities from IT outages resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect CII by reducing the risk of IT outages as much as possible and by ensuring prompt recovery from IT outages.

(2) Basic Principles for CIIP

In the first place, CII operators should implement measures for CIIP on their own responsibility. In addition, a sense of security should be nurtured among the public and social development, resilience and international competitiveness should be promoted through activities in cooperation between Government and private sectors.

- The CII operators should respectively take measures and make effort for continuous improvement of those measures as entities providing services and bearing social responsibilities.
- Government organizations should provide necessary support for CII operators' activities for CIIP.
- Each CII operator should cooperate and coordinate with other stakeholders due to the limit of each operator’s individual information security measures to address various threats.

(3) Responsibility of the stakeholders; CII operator / government organizations / CIIP supporting agency

- All the stakeholders should periodically check the progress of their own measures and policies as part of relevant efforts and accurately recognize the current circumstances, and proactively determine the goals of relevant activities. In addition, stakeholders should enhance their cooperation with each other, taking into account the status of other stakeholders’ relevant activities.
- All the stakeholders should understand the 5W1H (when, where, who, why, what and how) of IT outage response depending on the scale of IT outages and should be able to calmly address signs or occurrence of an IT outage. They should be capable to cooperate with other stakeholders and respond in a cooperative and concerted manner in addition to ensuring robust communication among various stakeholders and taking proactive measures.

(4) Responsibility of CII operator's executives and senior managers

In addition to the aforementioned measures, the executives and senior managers should recognize the need for and be able to ensure the implementation of the following measures:

- Recognize risk sources with a focus on information security for the purpose of CIIP.
- Assess risk sources and set forth measures to address those risks by identifying priorities.
- Determine plans necessary for the establishment and operation of systems and the implementation of relevant policies in addition to securing management resources (e.g. budget, human resources, etc.).
- Check the status of the implementation of relevant policies through monitoring the system operation.
- Check the status of incident response capability including information sharing among relevant stakeholders through conducting exercises and trainings.

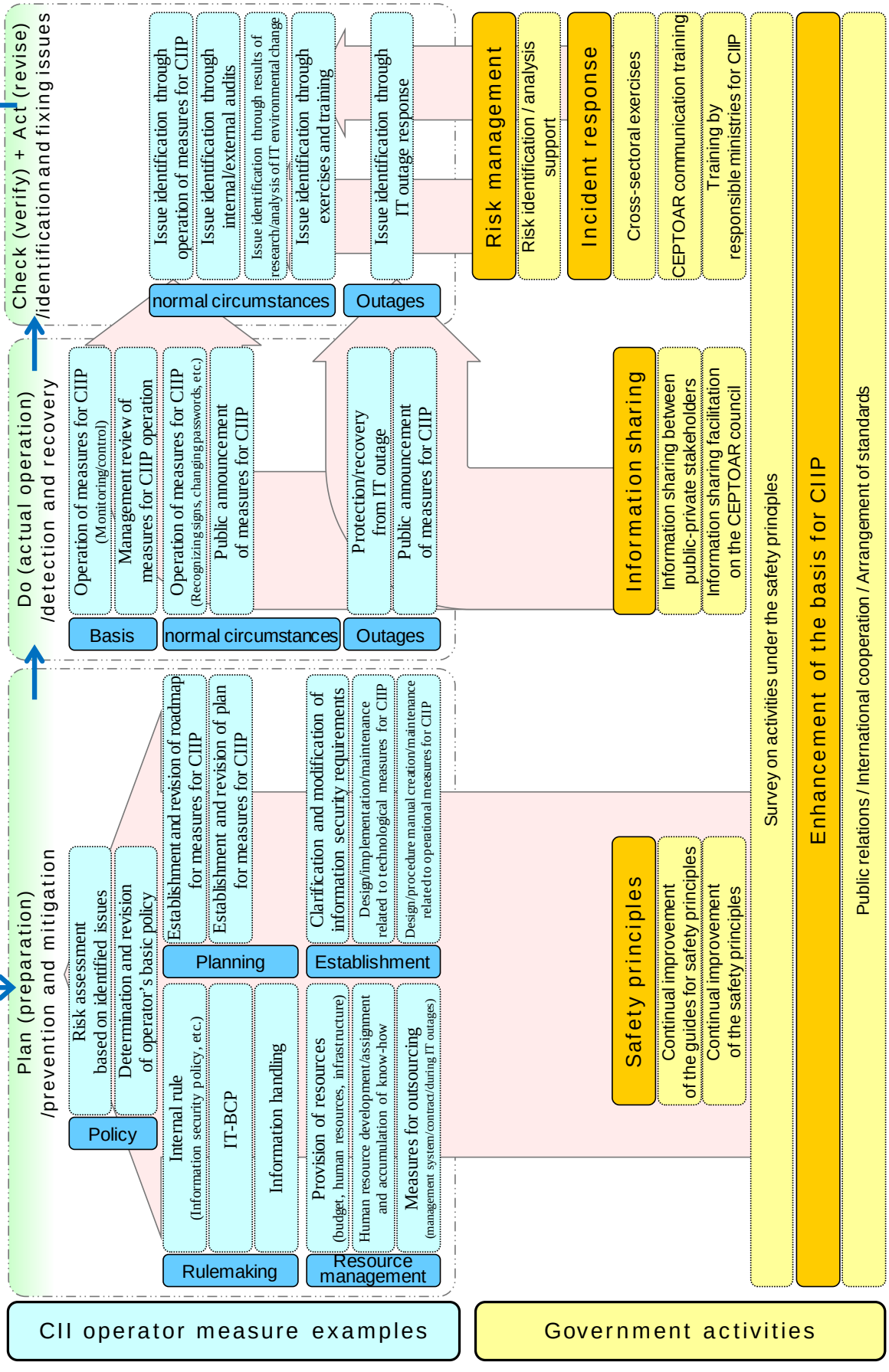


Figure 1. "CII operator measure examples" and "Government activities"

III. POLICIES FOR CIIP

1. MAINTENANCE AND PROMOTION OF THE SAFETY PRINCIPLES

During the term of this Basic Policy, the Cabinet Secretariat carries out the review the Guidelines for safety principles and related surveys so that they would conform with the PDCA cycle of CII operators and would enhance the cooperation with other policies, in order to strengthen the ability of CIIP.

Also, CII operators continuously and steadily work on measures for CIIP in accordance with their PDCA cycle, in view of importance of the measures.

1.1 Continual improvement of the Guidelines for safety principles

The Cabinet Secretariat carries out the review the Guidelines in FY 2014, in order to strengthen the ability of CIIP, especially in order to contribute to effective and autonomous activities of mid-process or small-and-medium-sized CII operators.

In detail, it arranges the orders of the items in the Guidelines in accordance with the PDCA cycle of CII operators, and adds some items, if necessary, based on knowledge from other policies etc. in this Basic Policy.

In addition, some example views on prioritization of measures for CIIP in case CII operators execute these measures, ways of gradual addition of measures for CIIP, and ones on balancing with pre-active measures and post-active measures, are described as "growth-model".

Further, the Guidelines appeal the importance of the responsibility of CII operator’s executives and senior managers regarding policy, rulemaking, planning, resource management and establishment that are essential to gradually and constantly strengthen CII operators' measures.

After FY 2015, social trends changes and newly obtained knowledge is released each fiscal year, and the revision of the Guidelines is executed every 3 year or as necessary.

1.2 Continual improvement of the safety principles

Responsible ministries for CIIP and CII operators continually improve the safety principles based on knowledge learned from experiences when taking the measures, in order to maintain or strengthen the abilities of not only individual CII operator but also overall CII.

In detail, they approach continual improvement of the safety principles through risk assessment, by identifying issues from operation of measures for CIIP, internal/external audits,

environmental change studies, exercises, training and incident responses.

In addition, when verifying the safety principles, the Guidelines as well as social trend changes and newly knowledge released by the Cabinet Secretariat is used.

The Cabinet Secretariat carries out survey on the improvement of the safety principles by the responsible ministries for CIIP each fiscal year and releases the results of survey.

1.3 Promotion of the safety principles

The Cabinet Secretariat carries out survey the CII operators' activities, in order to recognize the status of promotion of the safety principles at CII operators. In addition, in order to contribute to CII operators' effective and autonomous activities, survey operations will also be revised so that responses to the survey will serve as self-checks of measures.

With regard to survey itself, the activities include addition of survey items that can identify more detail conditions in CII operators and ones that can detect degrade of measures in CII operators which have excellent conditions through periodical survey, with some expansion of the coverage of the target CII operators.

With regard to survey operations, the activities include an arrangement of the questionnaire items in the survey in accordance with the PDCA cycle so that the measures and process to be enforced become explicit.

In addition, in order to supplement the survey using the questionnaire method, the Cabinet Secretariat conducts visit to CII operators.

With regard to the visit, the activities include extraction of issues from detail conditions of measures and collection of best practices, through the interviews with detail items based on the questionnaire.

For the results from the questionnaires and the visit, in principal, these will be released each fiscal year, and in addition, the obtained improvement issues reflected on each of the policies of this Basic Policy.

Survey items can be changed flexibly to the degree that such change does not impair the periodical survey.

2. ENHANCEMENT OF INFORMATION SHARING SYSTEM

While the social and technological environments surrounding CII constantly change, it is necessary to recognize these environmental changes accurately and then reflect these changes in the measures for CIIP, in order to maintain the effectiveness of measures for CIIP. In addition, it becomes more important to raise the level of measures in CIIP and cyber-attack response capability due to increasing complexity, sophistication of cyber-attacks.

As described in the Basic Principles in *"I.2. CLARIFICATION OF THE PURPOSE OF CIIP"*, CII operators should fundamentally implement measures for CIIP at their own responsibilities, however, it is difficult to verify whether a response by only itself to various threats is sufficient or not. For this reason, it is important to work on necessary measures for CIIP through cooperation by carrying out information sharing within sectors, between sectors and through public private partnership.

Based on these conditions, in the term of this Basic Policy, the Cabinet Secretariat manages the information sharing system among stakeholders including added sectors and stakeholders, further promotes information sharing, and works towards further vitalization of information sharing activities by CII operators.

2.1 Information sharing system during the term of this Basic Policy

In this Basic Policy, for the purpose of enhancement of the information sharing system during IT crises, the Information Security Policy Council (referred as "ISPC" hereinafter) decides to add the disaster prevention related ministries for disaster management, and also add cyberspace-related operators. They are consisted of system vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CII services, security vendors, which provide measures for CIIP and platform vendors, which provide the platforms which serve as foundations. The information sharing system after these addition is represented in *"ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL* CIRCUMSTANCES*)"* and *"ANNEX 4-2. INFORMATION SHARING SYSTEM (IT* CRISES*)"* as extended system of the former one.

In addition, the ISPC reviews CII sectors' critical information systems and service maintenance levels including those in newly added sectors. The results are shown in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"* and *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*.

During the term of this Basic Policy, the stakeholders manage the information sharing system according to their respective position and responsibilities. In addition, it is expected that cyberspace-related operators implement measures required for the maintenance of information

security, such as sharing of vulnerability information and preventing spread of damages in the event of IT outages resulting from cyber-attacks.

2.2 Promotion of information sharing

For arrangement of information to be shared, it is important to identify and arrange information that should be shared among stakeholders, including government organizations and CII operators, from aspects of "proactive prevention of IT outages", "prevention of the spread damages and quick recovery from IT outages", and "prevention of recurrence through analysis and verification of IT outage causes".

When establishing this Basic Policy, the Cabinet Secretariat has carried out revision of *"ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING* FROM NISC*"* and *"ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC"* based on the above 3 aspects regarding the information sharing system during normal times and during IT crises, in order to contribute to CIIP including proactive prevention of IT outages.

In detail, the ISPC has revised event[8] items based on the information security C.I.A[9] viewpoint and formed detailed cause items based on new threats, etc. in *"ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC"*, in order to grasp situation of IT outage rapidly and accurately. In *"ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING* FROM NISC*"*, the ISPC has clarified the coverage of information sharing, including handling of IT outage predictive information, in order to eliminate the disparity in the frequency of information sharing between sectors.

During the term of this Basic Policy, the Cabinet Secretariat carries out information sharing to and from NISC in accordance with the attachment, cooperate with stakeholders and promote this information sharing system, with the expectation that information sharing among stakeholders contribute to CII operation and their verification of measures, and proactive prevention of IT outages. In addition, in the event any environmental change occurs, it attempts to review the information system as appropriate.

[8] An Information Security Event is defined as *"The occurrence of a specific condition in systems, services or networks. Specific condition refers to an unknown condition which may be related to potential violations of information security policy, management measure failures or security."* in *ISO/IEC 27000:2013*.

[9] Stands for Confidentiality, Integrity and Availability.

2.3 Promotion of CII operators activities

It is expected that enrichment of information sharing between CEPTOARs as well as the activities of the CII operators themselves enhances further vitalization of CII operator activities.

In detail, it is expected that CII operators proactively work towards their own information sharing activities as well as they construct and enhance IT failure response systems, such as CSIRT[10],. It is also expected between CEPTOARs that they continue to share information provided by the Cabinet Secretariat, regarding agreements for handling of those provided information, maintenance of confidentiality and provision of information outside of constituent members, rules decided upon by constituent members will be applied, and the continued sharing of information provided by the Cabinet Secretariat is expected with a PoC[11] established allowing contact between constituent members and with non-members in case of emergency.

It is also expected that sharing activities is further activated through establishment of coordinators who will carry out information collection and decision making within CEPTOARs, sharing of predictive information and IT outage examples during normal times and enhancement of functions required for information sharing between CEPTOARs and with the CEPTOAR council.

The CEPTOAR council is an independent body, not positioned below other agencies, including government, so information mutually shared based on independent determinations by each CEPTOAR[12].

In this sense, it is expected that CII operator activities, such as further enhancement of information sharing between CEPTOARs, are further vitalized. through wide ranging and autonomous activities which contribute to the improvement of service maintenance and recovery capacity at CII operators through the proactive involvement of each CEPTOAR

2.4 Responsibilities of each stakeholder in the information sharing system

The information sharing system is composed of an information sharing system for normal times and an expanded information sharing system for times of IT crises, and the roles of IT stakeholders during times of IT crises are also an expansion of their roles during normal times.

The overall image of information sharing during normal times and during IT crises is shown

[10] Computer Security Incident Response Team. A system for monitoring to check if any security issues exist with information systems and for carrying out investigations including cause analysis and extent of impact in the event an incident occurs.

[11] PoC: Point of Contact.

[12] According to CEPTOAR council charter (CEPTOAR council foundation preparatory committee and NISC).

in *"ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL* CIRCUMSTANCES)*"* and *"ANNEX 4-2. INFORMATION SHARING SYSTEM (IT* CRISES)*"* and the roles of each stakeholder are as follows.

2.4.1 Responsibilities of each stakeholder in the information sharing during normal circumstances

The roles of each stakeholder in the information sharing system during normal times are as follows.

(1) CII operators

Information sharing related to IT outages and cyber-attacks shall generally be carried out by the relevant CEPTOAR. In addition, responsible ministries for CIIP shall carry out information sharing related to IT outages and cyber-attacks as necessary. In the event there are any criminal damages, reports shall be made to the crisis management ministries based on independent decisions.

(2) CEPTOAR

Cooperates with the CEPTOAR council, responsible ministries for CIIP and CIIP supporting agencies to carry out mutual sharing of IT outage and cyber-attack related information, recovery method information, early warning information, etc.

(3) the CEPTOAR council

The CEPTOAR council is an independent body, not ranked below other agencies, including government organizations. Cooperation is carried out based on independent decisions by each CEPTOAR.

Each CEPTOAR actively participates based on independent decisions and carries out a wide range of information sharing aimed at CII operator service maintenance and recovery.

(4) Responsible ministries for CIIP

Carry out sharing to the Cabinet Secretariat (NISC) of IT outage and cyber-attack related information received from CII operators over which the ministries have jurisdiction. Also carry out information sharing to CEPTOAR under the jurisdiction of the ministries as necessary. Carries out information sharing to CEPTOAR under the jurisdiction of the ministries for IT outage and cyber-attack related information, recovery method information and early warning information received from the Cabinet Secretariat (NISC).

(5) Cabinet Secretariat (NISC)

Carries out reciprocal sharing of IT outage and cyber-attack related information and recovery method information with responsible ministries for CIIP, CIIP supporting agencies from whom requests for cooperation were received in advance and cyberspace-related operators.

2.4.2 Responsibilities of each stakeholder in the information sharing during IT crises

In the event of an IT crisis resulting from disaster, terrorism or similar causes, collection and sharing of information related to the emergency shall be carried out between relevant ministries in accordance with *"Regarding the Government Initial Response System for Emergencies"* (November 21, 2003, Cabinet resolution). If the situation worsens and shifts to IT crisis response, the centralization of information in the crisis management ministries and the disaster prevention related ministries is important, so the information sharing system shall be laid out as follows.

(1) Cabinet Secretariat (Situations Response and Crisis Management)

Is integrated with the Cabinet Secretariat (NISC) and collects damage information provided by the crisis management ministries and the disaster prevention related ministries as well as response conditions information and carried out reciprocal information sharing with the Cabinet Secretariat (NISC).

(2) Cabinet Secretariat (NISC)

Is integrated with the Cabinet Secretariat (NISC) and carries out reciprocal sharing of various related information and recovery method related information with responsible ministries for CIIP, CIIP supporting agencies from which requests for cooperation were received in advance as well as cyberspace-related operators.

(3) Responsible ministries for CIIP

In addition to roles during normal times, shall also cooperate with system for IT crisis response as necessary.

(4) CII operators

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by CII operators.

(5) CEPTOAR

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by each CEPTOAR.

(6) the CEPTOAR council

In addition to roles during normal times, shall also construct system for IT crisis response as stipulated by each CEPTOAR.

3. ENHANCEMENT OF INCIDENT RESPONSE CAPABILITY

During the term of this Basic Policy, in addition to cross-sectoral exercises in the Second Basic Policy, relevant exercises and trainings in order to improve IT incident response capability and verification, are positioned as part of a policy of strengthening IT incident response systems. And the Basic Policy attempts to maintain and improve capability for CIIP as a whole by understanding the mutual relationships among these exercises and trainings and linking them.

Among the exercises and trainings, based on the achievement until now, the Basic Policy aims at continuing to enhance the positioning of cross-sectoral exercises as core means of strengthening the IT incident response system in CII sectors. In detail, the cross-sectoral exercises should be mutually linked and complement the CEPTOAR training and other exercises and training implemented by responsible ministries for CIIP, and enhance the vertical-directional systems within each CII sector and the horizontal-directional systems between CII sectors in order to reap synergistic benefits.

In addition, because rapid crisis management becomes necessary in order to prevent spread of damages, stakeholders implement measures and support policies to improve the IT incident response capability of CII operators, while continuing to clarify the roles and enhance cooperation between stakeholders.

3.1 Improvement of cross-sectoral exercises

During the term of this Basic Policy, the Cabinet Secretariat continues to implement the cross-sectoral exercises, which are the only initiative in Japan, while constantly improving them in order to contribute to the maintenance and improvement of protective capability for CII through the promotion of the relevant exercise results to the entire CII sector.

In implementing cross-sectoral exercises, in line with the 3 objectives given in the Second Basic Policy, those are "formation of a common awareness of cross-sectoral threats", "improving the response capability of one's own sector by understanding the response conditions of other sectors" and "acquiring policies for operating public-private information sharing more effectively", the Basic Policy aims to enhance cross-sectoral exercises using accumulated operation methods and results in order to contribute to the enhancement of the incident response system.

3.1.1 Planning of cross-sectoral exercises

During the term of this Basic Policy, the Cabinet Secretariat surveys plans for exercises including participation of stakeholders closely related to the maintenance of IT systems

possessed by CII operators, as well as knowledge and issues obtained through exercise operation issues from other policies, and latest trends related to risk sources which are a cause of IT outages, in order to improve continually cross-sectoral exercises.

In addition, the Cabinet Secretariat carries out verification aimed at improvement of the exercise results assessment process, in order to contribute to the further enhancement of verification related to CII operator measures for CIIP, IT outage early recovery process and IT-BCP.

The Cabinet Secretariat provides knowledge and issues obtained through the exercises as basic data to other policies in this Basic Policy.

3.1.2 Promotion of lessons learned from cross-sectoral exercises

During the term of the Second Basic Policy, the number of exercise participants steadily increased, and the percentage of participants who assessed the exercises as meaningful exceeded 80%. The Basic Policy aims at the promotion of exercise results in CII sectors through promoting new participation from individuals who had not yet participated in the exercises. However, as there is a limitation of participation increase to some degree, it is necessary to promote increasing the number of participation and provide activities targeting CII operators that do not participate in the exercises, in order to further propagate and promote exercise results to overall CII.

For this activity, the Cabinet Secretariat creates and releases explanation materials regarding the merits of exercises which can contribute to the promotion of increase understanding by executives and senior managers, and make appeals to overall CII sectors, and thereby promote implementation of exercises in each CII sector and at each CII operator.

In addition, the Cabinet Secretariat promotes survey the arrangement and sharing of implementation, assessment and advising methods accumulated from past exercises in order to contribute to the support of exercise implementation by individual CII operators.

3.1.3 Response to IT outages from physical causes

In actual IT incident response, it may include IT outages resulting from physical causes, and depending on the circumstances it may be necessary to share information not only with the various ministries and business information security departments, but also with disaster and crisis management departments.

Hereafter, the Cabinet Secretariat, when making response to relevant IT outages subject to verification, when necessary in creation of scenarios, study the conditions for utilization of knowledge from the disaster prevention related ministries and cooperation with the crisis management supervisors at responsible ministries for CIIP and CII operators.

3.1.4 Cooperation with responsible ministries for CIIP

It is expected to work to maintain and improve effective and efficient protective capability for CII by implementing these exercises and training to reciprocally cooperate with and complement the cross-sectoral exercises, while exercises and training contributing to CIIP implemented by the responsible ministries for CIIP have different expected results from the cross-sectoral exercises implemented by the Cabinet Secretariat.

For this reason, the Cabinet Secretariat and responsible ministries for CIIP consider conditions for clarification and mutual cooperation of verification purposes and the main targets for the exercises implemented by each exercises in order to improve the response capability of CII operators.

As an example of verification survey items, it would be possible to target information sharing and collaborative response between CII operators, CEPTOAR, responsible ministries for CIIP and the Cabinet Secretariat as verification targets in cross-sectoral exercises, and to target IT incident response procedures using actual systems at CII operators and contact systems in each sector for checking and verification in exercises by the responsible ministries for CIIP.

3.2 CEPTOAR communication training

The Cabinet Secretariat continues CEPTOAR training based on the procedures for information sharing to and from NISC for the purpose of maintenance and improvement of protective capability of the "vertical-directional information sharing" systems in each sector between CEPTOAR and responsible ministries for CIIP.

In implementation CEPTOAR training, the Cabinet Secretariat aims to enhance substantial training content while also incorporating requests from CEPTOAR and to realize information sharing training which is suited to actual conditions, bearing in mind response during IT outages.

In addition, the Cabinet Secretariat considers collaboration, as necessary, such as setting conditions based on the verification details of cross-sectoral exercises between cross-sectoral exercises and CEPTOAR training, because the participation of a large number of CII operators can be expected in CEPTOAR training.

4. RISK MANAGEMENT

CII operators should establish objectives related to information security and deploy the objectives within their organizations in order to achieve business goals such as stable provision of CII services to the people and business continuance.

On the other hand, as the social and technological environments surrounding CII continually change, the dependence on cyberspace of information systems used in the CII and of the data utilized in these systems continues to increase.

In these conditions, the effects of IT failures caused by risk sources, such as the threats and vulnerabilities lurking in cyberspace, also increase, and if and IT failure did occur, it could make provision of CII services difficult.

For this reason, it is necessary for CII operators to carry out not only comprehensive management of risks deriving from risk sources related to information security but also just the symptomatic measures for IT failures, aimed at achieving business goals.

In order to focus on risk management methods at CII operators, the "common threat analysis" and "development of risk communication" (one of the policy of "response to environmental change") in the *Second Action Plan* are more comprehensively considered and activities related to risk management carried out by each CII operator are newly implemented.

4.1 Basic view of risk management

Risk management should be independently implemented by each CII operator. However, in circumstances where each stakeholder does not have common risk management views or terms for information sharing and discussion, there is a possibility that the activities in this Basic Policy will not be effectively utilized in the risk management of each CII operator.

For this reason, it is preferable for each stakeholder to utilize the internationally standard views of management and related terminology definitions for information security etc. in the term of this Basic Policy.

In detail, the Cabinet Secretariat, as far as possible, utilizes views based on the framework[13] noted in Table 3 below and the terminology definitions used in the framework in the activities implemented by the Cabinet Secretariat and in related materials.

[13] Refer to *JIS Q 31000:2010* and *"Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools"* released by ENISA (European Union Agency for Network and Information Security).

Table 3. Risk management process (example)

Risk management		
	Establishing the context of organization	
	Risk assessment	
		Risk identification
		Risk analysis
		Risk assessment
	Risk treatment	
	Risk acceptance	
	Risk communication and consultation	
	Monitoring and review	

In addition, it is expected that CII operators will utilize the guidebooks[14] created by the Cabinet Secretariat in their own organization's risk management.

However, this activity does not require each stakeholder to conform with international standards, but rather is aimed at contributing to an increase in the level of information security and more optimized risk management already being implemented at CII operators by referring to the views and terminology definitions applied by the Cabinet Secretariat.

4.2 Support for risk management

Risk management is generally optimized by each CII operator individually to suit their organization. On the other hand, in risk assessment[15] and risk communication and consultation[16], there are some activities which cannot be handled easily by only CII operator, such as cross-sectoral study/analysis and opinion exchanges.

For this reason, the Cabinet Secretariat carries out cross-sectoral activities as follows, and supports risk management implemented at CII operators by sharing the results of cross-sectoral studies/ analyses and providing opportunities for cross-sectoral opinion exchanges.

4.2.1 Risk assessment

The Cabinet Secretariat analyzes conditions and trends of major facilities and technologies in regard to changes in the environments surrounding CII sectors, as well as risk sources inherent to major facilities and technologies and new risks derived from the risk sources (hereinafter referred to collectively as "new risk sources and risks").

In addition, the Cabinet Secretariat analyzes the influence of effects of IT outages.

In detail, the following activities are carried out, also taking into account viewpoints of the

[14] In *"5.3.3 5.3.3 Preparation of guidance to apply international standards"*, it is specified that guidebooks, etc. which interpret international standards, shall be prepared as necessary.

[15] According to *JIS Q 31000:2010*, this is defined as *"overall process of risk identification, risk analysis and risk evaluation"*.

[16] Refer to *"4.2.2 Risk communication and consultation"* for definition.

efficiency of each study/analysis and mutual reflection with other policies, and the results of the studies/analyses are provided to CII operators.

(1) Environmental change studies

In the environmental change studies implemented in the *Second Action Plan*, it turned out that the adoption ratios of cloud, smartphone/tablet device and remote maintenance were high and the adoption of BYOD[17] and big data would increase going forward in CII sectors.

In this Basic Plan, based on these changes, the Cabinet Secretariat carries out environmental change studies including analysis of new risk sources and risks as well as condition surveys for new technologies and systems which are expected to introduce to CII sectors into mid to long term, such as M2M and smart communities. In addition, the Cabinet Secretariat carries out this study across years, because these changes will be appeared over time. With regard to these studies, new risk sources and risks which could have a major effect, even if they are common across specific sectors (ex. Control systems, accounting systems and information systems) will also be targeted.

In the event new risk sources and risks are identified through these studies, or in the event new CII sectors are added, detailed investigation and analysis of commonality across these sectors shall be carried out as necessary.

(2) Interdependency analysis

As utilization of IT continues to develop in each CII sectors and interdependent relationships between sectors continue to grow, the understanding of interdependency in CII sectors becomes more important for effective recovery measures in the event of an IT outage.

For this reason, in this Basic Policy, the Cabinet Secretariat carries out interdependency analysis, including restudy or reanalysis based on the results from the *First Action Plan* and the *Second Action Plan* in the event of changes in interdependency due to environmental changes or addition of new CII sectors.

In addition, as the degree of IT dependency in CII sectors is closely related to interdependency analysis, IT dependency studies as detailed studies of interdependency analysis shall also be periodically implemented.

In the event new CII sectors are added, IT dependency studies will also be carried out as a part of interdependency analysis.

4.2.2 Risk communication and consultation

Risk communication and consultation is defined as *"continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue*

[17] Bring Your Own Device. A situation where, in a business or other setting, employees access company information, using their personal information devices to view, edit and otherwise manipulate the required information for work.

with stakeholders regarding the management of risk".[18]

The Cabinet Secretariat supports risk communication and consultation implemented by stakeholders related to CII protection for the purposes of contributing to the development of cross-sectoral information and opinions exchanges among them.

In detail, the CEPTOAR council and cross-sectoral exercises are utilized to provide opportunities for information and opinion exchange maintaining cooperation with each stakeholder.

This activity also promotes the collection of information necessary for the study/analysis in this policy.

4.3 Establishing a process of synergizing the relevant policies

The Cabinet Secretariat shall provide the results of studies and analysis in this policy as basic data for other policies for the purpose of contributing to the other policies in this Basic Policy.

In addition, new risk sources and risk required cross-sectoral measures appeared from results of the implementation of other policies are subject to the studies/analyses of this policy.

[18] Refer to *JIS Q 31000:2010*.

5. ENHANCEMENT OF THE BASIS FOR CIIP

As the social and technological environments etc. surrounding CII continue to constantly change, as shown in Figure 1, it is necessary to enhance common foundation activities which support the entire Basic Policy, for maintenance of the effectiveness of measures for CIIP. The activities include establishment of basic plan, human resource development/assignment, external explanations of measures for CIIP and identification of issues for risk sources resulting from IT related environmental change.

Therefore, during the term of this Basic Policy, the Cabinet Secretariat prepares guides on international standards, etc. related information security and relevant regulations related to CIIP in order to allow stakeholders to reference suitable, related regulations, etc. as necessary, in addition to continuing the cooperation with other stakeholders, public relations activities and international cooperation from Second Basic Policy.

The Cabinet Secretariat also provides the knowledge obtained through the implementation of this policy for application in other policies for the purpose of contributing to the other policies in this Basic Policy.

5.1 Public relations activities

In order to minimize the effects of IT outages to the smallest degree possible, it is important to not only raise the standard of measures for CIIP implemented by CII operators, but also to ensure that the people are able to calmly respond to such outages based information on the situation.

Therefore, each stakeholder attends to continue to provide explanations to the people through the publicity of the activities based on this Basic Policy, in order to contribute to a calm response from the people.

In order to raise the level of measures for CIIP implemented by CII operators, it is important to obtain a wide range of cooperation and support for the initiatives based on this Basic Policy.

The Cabinet Secretariat continues to carry out public relations activities through publicity through websites and newsletters, lectures and other means. When doing these activities, the publicity should be structured so as to achieve awareness and understanding of the initiatives of this Basic Policy.

5.2 International cooperation

In cyberspace, risks have been growing in borderless domain, it is required to further respond to these global risks which have no national boundary, and it becomes necessary to

positively contribute to capacity building so that our country would improve the level of international measures for CIIP as well as ourself.

Therefore, the Cabinet Secretariat cooperates with responsible ministries for CIIP and the CIIP supporting agencies and continue to enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks such as those with the US and Europe, ASEAN and Meridian. When doing these activities, it actively provides case examples, best practices and other items obtained through international cooperation to domestic stakeholders.

In addition, diversified and multilateral international cooperation is also expected at CII operators as a result of the deployment of initiatives related to measures for CIIP being deployed to other companies in the same industry overseas, identification of overseas trends, etc.

5.3 Maintenance of reference of standards and guides

To maintain the effectiveness of measures for CIIP, it is important that stakeholders are able to reference relevant documents and regulations where necessary when examining means to do so. The initiatives of the Cabinet Secretariat related to the preparation of these regulations etc. are as follows.

5.3.1 Issuance of the reference book for CIIP

The Cabinet Secretariat compiles relevant documents including the *Cybersecurity Strategy* and this Basic Policy for common reference by stakeholders, and issue the compiled documents as the "Collection of regulations related to measures for CIIP" for the purpose of equalizing the knowledge base of stakeholders involved in CIIP.

5.3.2 Systematic arrangement of relevant standards and guides

For related regulations for CIIP, the Cabinet Secretariat, with the cooperation of the other stakeholders, arranges domestic and overseas related regulations and clearly states the results in order to refer appropriate version when necessary.

5.3.3 Preparation of guidance to apply international standards

As the social and technological environments etc. surrounding CII continue to constantly change, in order to quickly and flexibly respond to these changes, it may be effective in case that the stakeholders utilize appropriate relevant regulations identified from the results compiled from *"5.3.2 Systematic arrangement of relevant standards and guides"*, particularly the international standards, etc.

However, when attempting to utilize the international standards, etc. which set out general

principles based on the above compiled results, reinterpretation may be necessary for items that would not be able to directly apply to.

The Cabinet Secretariat, with the cooperation of other stakeholders, compiles guides as necessary in order to allow for the relevant international standards etc. to be applied to fast and flexible response.

In keeping with the fact that international guidebooks, etc. related to CIIP do not currently exist, the Cabinet Secretariat considers proposal of the guidebooks, etc. compiled as part of this policy to the various countries of ASEAN and for ISO and other international standards as a means of global contribution.

5.3.4 Promotion of assessment and certification system for CIIP

The Cabinet Secretariat, with the cooperation of other stakeholders, support[19] the expansion of third party certification systems for control equipment and systems regarding the circumstances of the adoption of assessment and certification which conforms with international standards related to control equipment and systems under further consideration.

[19] Implemented with cooperation from the Technological Research Association Control System Security Center (CSSC) which works on the adoption of third party certification systems for control equipment and systems.

IV. ACTIVITIES TO BE TAKEN BY STAKEHOLDERS

The information security policy groups indicated in this Basic Policy are supported by independent measures which it is preferable for CII operators to handle, and policies which it is preferable for government organizations etc., centering on the Cabinet Secretariat, to implement. It is expected that stakeholders will each promote measures for CIIP using the following as a basis.

1. ACTIVITIES BY CABINET SECRETARIAT

(1) Maintenance and promotion of the safety principles

a) During the first fiscal year of this Basic Policy and as necessary thereafter, implement studies related to the amendment of the Guidelines for safety principles after strengthening links to other policies and officially release the results.

b) As necessary, implement studies related to the changes in social trends and newly obtained knowledge after strengthening links to other policies and officially release the results.

c) Support the continued improvement of the CII sector safety principles through a) and b) above.

d) Continue to obtain the cooperation of the responsible ministries for CIIP, implement studies every year to determine the conditions of the continued improvement of the safety principles in each CII sector and officially release the results.

e) Continue to obtain the cooperation of the responsible ministries for CIIP, implement studies every year on the conditions of the promotion of the safety principles and officially release the results.

(2) Enhancement of information sharing system

a) Increase promotion and revise when necessary through operation of the information sharing system during normal times and during IT crises.

b) Collect information to be provided to CII operators and share information from NISC in an appropriate and timely manner.

c) Continue to obtain the cooperation of the responsible ministries for CIIP, periodically implement studies, hearings, etc. in order to determine the conditions, etc. of each CEPTOAR's functions and activities.

d) Introduce advanced CEPTOAR functions and activities.

e) Continue cooperating with CEPTOAR participating in the CEPTOAR council and implement support for management and activities.

f) Prepare environments required for enhancement of CEPTOAR council activities, and

accumulate and share know-how.

g) Build individual cooperation with cyberspace-related operators as necessary, and implement appropriate and timely information sharing from NISC during IT outages.

(3) Enhancement of incident response capability

a) Determine other ministries' IT outage handling exercises and training information, investigate cooperation conditions.

b) Continue to obtain the cooperation of the responsible ministries for CIIP, periodically and when requested by CEPTOARs, provide opportunities for verification (CEPTOAR training) of CEPTOAR information communication functions.

c) Plan cross-sectoral exercises scenarios, implementation methods and verification issues, etc. and implement cross-sectoral exercises.

d) Study measures for improving cross-sectoral exercises.

e) Utilize the opportunities for cross-sectoral exercises, determine the conditions of risk analysis results verification, early recovery procedures implemented by CII operators during IT outages, and IT-BCP etc. studies, and provide the results to exercise participants, etc.

f) Collect, accumulate and provide knowledge related to cross-sectoral exercise implementation methods, etc.

g) Diffuse and spread knowledge related to CII protection gained from cross-sectoral exercises.

(4) Risk management

a) Cultivate a shared awareness among stakeholders by presenting guidebooks which interpret international standards, definition usage and standard views for risk management.

b) Support risk management at CII operators through the study and analysis of this policy.

c) Provide the results of the studies and analysis in this policy as basic data to be reflected in the safety principles.

d) Support the risk communication and consultation of CII operators through CEPTOAR council and cross-sectoral exercises.

(5) Enhancement of the basis for CIIP

a) Carry out public relations activities through publicity through websites and newsletters.

b) Implement public relations activities through lectures, etc.

c) Enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks.

d) Actively provide case examples, best practices and other items acquired through international cooperation with domestic stakeholders.

e) Compile relevant documents for common reference by stakeholders, and issue a collection of regulations for the purpose of equalizing the knowledge base of stakeholders involved in CII protection.

f) Arrange and visualize related regulations.

g) Compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

h) Support the expansion of third party certification systems for control equipment and systems.

2. ACTIVITIES BY RESPONSIBLE MINISTRIES FOR CIIP

(1) Maintenance and promotion of the safety principles

a) Provide information, etc. related to the safety principles which can be newly positioned as the Guidelines for safety principles to the Cabinet Secretariat.

b) When the organization determining the safety principles, in addition to implementing periodic analysis and verification of the safety principles, amend the safety principles as necessary.

c) When not the organization determining the safety principles, support the analysis and verification of the safety principles for each CII sector.

d) Carry out promotion of safety standards for CII operators including environmental arrangement for packaging measures.

e) Cooperate with building an understanding of the conditions of the safety principles implemented by the Cabinet Secretariat every year.

f) Cooperate with studies of the conditions of the promotion safety principles implemented by the Cabinet Secretariat every year.

(2) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

b) Maintain a close information sharing system with CII operators.

c) Carry out information sharing to the Cabinet Secretariat of reports related to IT outages received from CII operators.

d) Cooperate with studies and hearings implemented by the Cabinet Secretariat for determining the conditions of activities and functions of each.

e) Support the development of CEPTOAR functions.

f) Support the CEPTOAR council.

g) Implement opinion exchanges, etc. when requested by the CEPTOAR council.

(3) Enhancement of incident response capability

a) Cooperate when the Cabinet Secretariat provides opportunities for verification (CEPTOAR training) of information communications functions.

b) Cooperate with planning of cross-sectoral exercises scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises.

c) Participate in cross-sectoral exercises.

d) Support participation in CEPTOAR and CII operator cross-sectoral exercises.

e) Cooperate with study of measures for improving cross-sectoral exercises.

f) As necessary, utilize results of cross-sectoral exercises in policies.

g) Cooperate with mutual collaboration between exercises and training which contributes to CII protection implemented by the responsible ministries for CIIP and cross-sectoral exercises.

(4) Risk management

a) Provide to the Cabinet Secretariat information related to the application required for study and analysis in this policy or information needed for the relevant study and analysis.

b) Apply to the studies and analysis policies in this policy.

c) Support the risk communication and consultation of CII operators.

(5) Enhancement of the basis for CIIP

a) Cooperate with the Cabinet Secretariat and enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks.

b) Cooperate with the Cabinet Secretariat and actively provide case examples, best practices and other items acquired through international cooperation with domestic stakeholders.

c) Cooperate with the Cabinet Secretariat and arrange and visualize related regulations.

d) Cooperate with the Cabinet Secretariat and compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

e) Cooperate with the Cabinet Secretariat and support the expansion of third party certification systems for control equipment and systems.

3. ACTIVITIES BY INFORMATION SECURITY RELATED MINISTRIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

b) Collect information, etc. related to attack methods and recovery methods and carry out information sharing to the Cabinet Secretariat.

c) Implement opinion exchanges, etc. when requested by the CEPTOAR council.

4. ACTIVITIES BY CRISIS MANAGEMENT MINISTRIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system during IT crises.

b) Collect disaster information, terrorism related information, etc.

c) Carry out information sharing to the Cabinet Secretariat as necessary.

d) Implement opinion exchanges, etc. when requested by the CEPTOAR council.

(2) Enhancement of incident response capability

a) Implement support measures for improving IT outage response capability when requested by CII operators.

5. VOLUNTARY ACTIVITIES BY CII OPERATORS

(1) Maintenance and promotion of the safety principles

a) When the organization determining the safety principles, in addition to implementing periodic analysis and verification of the safety principles, amend the safety principles as necessary.

b) When the organization determining the safety principles, cooperate with building an understanding of the conditions of the safety principles implemented by the Cabinet Secretariat every year.

c) Study environmental arrangement for packaging measures and implementing measures for CIIP based on the safety principles.

d) Identify issues from operation of measures for CIIP, internal and external audits, environmental change studies/analysis results related to IT, exercises/training and response to IT outages, and continually amend safety principles through risk assessment.

e) Cooperate with studies of the conditions of the promotion safety principles implemented by the Cabinet Secretariat every year.

(2) Enhancement of information sharing system

a) Continue to cooperate with the CEPTOAR council, CEPTOARs and the responsible ministries for CIIP, and operate the information sharing system.

b) Carry out information sharing to the NISC as necessary during IT outages.

c) Collect information, etc. related to attack methods and recovery methods.

d) Carry out supplemental information sharing based on consensus with the CIIP supporting agencies.

e) Implement activities in the CEPTOAR council.

(3) Enhancement of incident response capability

a) Utilize, etc. verification (CEPTOAR training) etc. information communication functions provided by the Cabinet Secretariat and enhance own information sharing system.

b) Cooperate with planning of cross-sectoral exercises scenarios, implementation methods and verification issues, etc. and implementation of cross-sectoral exercises.

c) Participate in cross-sectoral exercises.

d) Cooperate with study of measures for improving cross-sectoral exercises.

e) Utilize the results of cross-sectoral exercises for early recovery method and IT-BCP etc. initiatives as necessary in the event of own IT outages.

(4) Risk management

a) Promote and enhance risk management in own organization.

b) Utilize the basic information provides as the results of the study and analysis of this policy in own organization's risk assessment.

c) Develop risk communication and consultation between stakeholders directly involved in measures for CIIP.

d) Propose environmental changes and risk sources which are difficult to analyze oneself but for which there is a value for conducting study and analysis as targets for the study and analysis of this policy.

e) Participate in the discussion and examination of the study and analysis of this policy.

(5) Enhancement of the basis for CIIP

a) Promote diverse and multilateral international cooperation through the deployment of initiatives related to measures for CIIP being deployed to other companies in the same industry overseas, determination of overseas trends, etc.

b) Cooperate with the Cabinet Secretariat and arrange and visualize related regulations.

c) Cooperate with the Cabinet Secretariat and compile guidebooks as necessary in order to allow for international standards etc. to be applied to fast and flexible response.

d) Cooperate with the Cabinet Secretariat and support the expansion of third party certification systems for control equipment and systems.

6. VOLUNTARY ACTIVITIES BY CEPTOAR

(1) Enhancement of information sharing system

a) Continue to cooperate with the CEPTOAR council, CII operators and the responsible ministries for CIIP, and operate the information sharing system.

b) Carry out information sharing from NISC to CII operators in accordance with the information handling rules for information provided from the Cabinet Secretariat.

c) Carry out supplemental information sharing based on consensus with the CIIP supporting agencies.

d) Enhance and develop CEPTOAR functions.

e) Cooperate with studies and hearings implemented by the Cabinet Secretariat for determining the conditions of activities and functions of each.

f) Participate in the CEPTOAR council.

(2) Enhancement of incident response capability

a) Carry out periodic verification of information communication functions.

b) Support participation and development of results in CII operator cross-sectoral exercises.

c) Participate in cross-sectoral exercises.

(3) Risk management

a) Support independent initiative for the CII operators which make up own CEPTOAR.

7. VOLUNTARY ACTIVITIES BY THE CEPTOAR COUNCIL

(1) Enhancement of information sharing system

a) Continue to cooperate with each CEPTOAR and operate the information sharing system.

b) Carry out arrangement of information to be shared and sharing methods.

c) Promote cross-sectoral information sharing through sharing of specific examples of mutual understanding and best practice.

d) In order to strengthen cooperative relationships with stakeholders, hold opinion exchanges to promote sharing of the situational awareness of both parties based on

requests from government organizations or based on own proposals.

(2) Enhancement of incident response capability

a) Participate in cross-sectoral exercises as necessary.

8. VOLUNTARY ACTIVITIES BY CIIP SUPPORTING AGENCIES

(1) Enhancement of information sharing system

a) Continue to cooperate with the Cabinet Secretariat and operate the information sharing system.

b) Collect information, etc. related to attack methods and recovery methods and carry out information sharing to the Cabinet Secretariat.

c) Carry out supplemental information sharing based on consensus with the CII operators carrying out the information sharing or the CEPTOAR.

d) Cooperate with the examination of enhancement of analysis functions implemented by the Cabinet Secretariat.

e) Implement opinion exchanges, etc. when requested by the CEPTOAR council etc.

(2) Enhancement of incident response capability

a) Provide information, related to IT outage case examples required for cross-sectoral exercises to the Cabinet Secretariat.

(3) Enhancement of the basis for CIIP

a) Cooperate with the Cabinet Secretariat and enhance international cooperation through active utilization of bilateral, inter-regional and multilateral frameworks.

b) Cooperate with the Cabinet Secretariat and actively provide case examples, best practices and other items acquired through international cooperation with domestic stakeholders.

9. VOLUNTARY ACTIVITIES BY CYBERSPACE-RELATED OPERATORS

(1) Enhancement of information sharing system

a) Cooperate with initiatives for preparing information to be subject to sharing by the Cabinet Secretariat and the sharing methods for said information.

b) Carry out proactive information sharing to the Cabinet Secretariat as necessary during IT crises.

V. ASSESSMENT, VERIFICATION AND REVISION

For assessment of this Basic Policy, verification of results during the term of the Basic Policy is carried out from 2 viewpoints consisting of verification of the progress each fiscal year from a "view of measuring output", which looks at what kind of output each initiative has generated, and verification of results during the term of the Basic Policy from a "view of measuring outcomes", which looks at what degree society has actually moved closer to the ideal future image as a result of the initiatives of this Basic Policy. During this, use objective indexes as much as possible for progress verification and for verification of results carry out comparison with the goals of this Basic Policy which are the ideal future image.

In addition, the "verification" in this Basic Policy, shall refer to the use of indexes to objectively verify actual conditions related to progress of each of the initiatives.

1. GOALS TO BE ACHIEVED DURING THE TERM OF THIS BASIC POLICY

The future images that can be expected to be realized through the initiatives based on this Basic Policy are as follows.

* The independent initiatives of each stakeholder based on the stakeholder's own awareness prevail in the codes of conduct of each stakeholder and the resulting behavioral patterns form a culture of information security.
* Communication for enhancing measures for preventing IT outages is carried out between stakeholders on a daily basis, and continual improvements are carried so that experience gained in the event of an IT outage can be reliably utilized in future measures.
* The CII protection initiatives cooperatively carried out by stakeholders are widely known to the public providing a sense of security. In addition, there is substantial communication between a wide variety of stakeholders allowing for calm coping in the event of an IT outage.
* These types of initiatives are officially released as a Basic Policy which undergoes periodic assessment and is appropriately revised as necessary.
* Each of the stakeholder initiatives is reliably established as an item which supports continued development of society.

Hereafter, detailed future images are described.

1.1 For all stakeholders

Detailed future images common to all stakeholders are as follows.

* The stakeholder possesses an accurate awareness of its own conditions and independently establishes its own activity goals.

* All required initiatives are progressing and periodic verification is carried out on the progress of the stakeholder's own measures and policies. The stakeholder is also able to maintain an understanding of the activity conditions of and proactively cooperate with other stakeholders.
* In response during IT outages, it is understood who should be collecting what kinds of information, who should be sharing what kinds of information and what the stakeholder themselves should be doing in accordance with the scale of the IT outage.
* In addition to being able to carry out independent response, the stakeholder is able to cooperate with other stakeholders when necessary to carry out controlled response.

1.2 For CII operators

Detailed future images for CII operators are as follows.

* There is sufficient saturation of the following items related to "information security governance".
  - Measures for CIIP are examined not just from information system construction and operation perspectives, but also from a business management perspective.
  - A system exists which allows for the appropriate involvement of each of the parties responsible for system construction and operation and business management.
  - There is an understanding of the measures to be implemented based on the CII services which require protection and service maintenance level.
  - Efforts are made to carry out external explanations of measures for CIIP.
  - A sense of values is cultivated in which carrying out information sharing to the greatest degree possible in order to improve the standard of measures for CIIP is viewed positively.
  - There is an awareness that the occurrence of IT outages is not something to be hidden but should instead be shared with stakeholders involved in measures at CII operators.
* There is sufficient saturation of the following items related to "issue identification", "risk assessment" and "improvement of measures".
  - Based on this Basic Policy, stakeholders cooperate to carry out measures for CIIP related to CII protection and are aware of remaining risks in their own measures and the extent of those risks.
  - Risk changes related to risk sources and IT outages resulting from developments of various measures and environmental changes are suitably detected, measures are independently advanced for each and necessary adjustment is carried out.
  - Appropriate measures are able to be enacted even in the event of an IT outage and as a result the risk of the IT outage having a serious effect on the public welfare and

socioeconomic activities is minimized to the greatest degree possible.

- These initiatives server as one driving force for the continued improvement of the measures.

* There is sufficient saturation of the following items related to "information sharing".
  - There is an understanding of IT outage conditions, relevant information is shared externally through each sector's CEPTOAR and CEPTOAR council as necessary, and official or unofficial cooperation is carried out.

1.3 For Cabinet Secretariat

Detailed future images for the Cabinet Secretariat are as follows.

* Works as a comprehensive coordination function for advancing more effective measures. Diverse information which contributes to measures for CIIP is able to be collected through the policy groups of this Basic Policy and cooperation is carried out with stakeholders based on the relevant information.
* Has obtained an understanding of risks related to serious risk sources and IT outages in particular, and quickly implements organic cooperation and coordination aimed at studying and realizing resolutions in the event the management of such is difficult for CII operators alone.

2. CONTINUAL IMPROVEMENT BASED ON ASSESSMENT AND VERIFICATION DURING EACH FISCAL YEAR

In order to steadily advance the initiatives based on this Basic Policy and carry out continual improvement, confirmation and verification shall be carried out on the progress of the Basic Policy. In continual improvement, each stakeholder shares the experiences they gain through their initiatives with the stakeholders as a whole, and focus is on utilizing these experiences to reciprocally improve each other's initiatives. IT outages should be avoided, however it is important to recognize that experience protecting against IT outages and experience limiting the scope of the effects in the event of an IT outage serve as provisions for the future.

While obvious, the party for which the IT outage occurs must bear responsibility for and determine the cause of the IT outage and strive to improve their own initiatives. However, in the assessment and verification of this Basic Policy, the principal focus is not placed on assigning responsibility and investigating causes, but rather on identifying lessons that can be used to improve future initiatives, and utilizing these to improve the initiatives of all stakeholders.

3. METHODOLOGY FOR ASSESSMENT AND VERIFICATION DURING EACH FISCAL YEAR

The confirmation and verification carried out each fiscal year from "view of measuring output" is carried out with a focus on the policy groups for individual measures for CIIP in accordance with this Basic Policy. Because all of the measures for CIIP policy groups based on this Basic Policy are all multilayered among multiple stakeholders, a wide variety of items can be imagined as indexes for use in verification, however broad categorizations will be set of indexes used for comprehensive confirmation and verification of measures by CII operators and indexes used for confirmation and verification of policies by government organizations. For the indexes for each measure for CIIP policy group, it is important to appropriately interpret the meaning of the values rather than to be overly-focused on the quantity or any fluctuations.

The confirmation and verification carried out each fiscal year from "view of measuring output" is carried out with a focus on the policy groups for individual measures for CIIP in accordance with this Basic Policy. Because all of the measures for CIIP policy groups based on this Basic Policy are all multilayered among multiple stakeholders, a wide variety of items can be imagined as indexes for use in verification, however broad categorizations will be set of indexes used for comprehensive confirmation and verification of measures by CII operators and indexes used for confirmation and verification of policies by government organizations. For the indexes for each measure for CIIP policy group, it is important to appropriately interpret the meaning of the values rather than to be overly-focused on the quantity or any fluctuations.

In addition, confirmation and verification of own measures by individual CII operators shall be considered an independent process, and in general it is preferable for the CII operator to carry out implementation every fiscal year.

3.1 Indexes for the assessment and verification of activities by CII operators

As the party with the most fundamental responsibility for the stable provision of CII services, CII operators must deal with measures for CIIP on a daily basis. In order to continually and steadily improve this initiatives and in order to make the support provided by the government for the initiatives of the CII operators more effective, it is important to objectively verify the the outcomes of the measures for CIIP.

The comprehensive confirmation and verification of the measures is the confirmation and verification of the conditions of the occurrence of IT outages for each CII sector based on the "preventing serious effects on the public welfare and socioeconomic activities due to IT

outages" which is the goal of this Basic Policy. The applicable CII services and service maintenance levels are as shown in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*. Detailed indexes are figures from all IT outage case sectors recognized by the Cabinet Secretariat.

The measures of individual CII operators include independent measures based on the management decisions of each, and it is therefore inadequate to assess measures through comparison with IT outage conditions for each CII operator or each sector. For this reason, it is reasonable that assessment of measures should be carried out through self-assessment by the CII operators, and that each CII operator should work towards their own improvement. In addition, if possible, it is preferable that the conditions of the implementation of the self-assessment be made clear.

3.2 Indexes for the assessment and verification of activities by government organizations

The policies of this Basic Policy are as shown in *"III. POLICIES FOR CIIP"*, however these are all items for which government support is carried out to improve the effectiveness of measures for CIIP by CII operators. During the term of this Basic Policy, the method for verifying the effectiveness of each policy was revised while continuing to follow the indexes used in the Second Basic Policy.

The confirmation and verification of policies is the verification of the contribution to the measures for CIIP of CII operators for each measures for CIIP policy, and the detailed indexes are as follows.

3.2.1 Maintenance and promotion of the safety principles

The outcomes expected from "maintenance and promotion of the safety principles" are the stakeholders being involved in measures for CIIP understanding the measures which they are required to implement themselves and the further development of index and safety principle items and the reliable practical application of the items for the purpose of having the required initiatives carried out under periodic self-assessment. For this reason, indexes are set which focus on the development of the indexes and safety principle items and the reliable implementation of initiatives based on the safety principles of the CII operators.

<Detailed indexes>

* Number of measure items recorded in the index
* The ratio of CII operators carrying out periodic self-assessment based on the safety principles, etc. determined through studies on the promotion of the safety principles
* Opinions and requests from CII operators on indexes

3.2.2 Enhancement of information sharing system

The outcomes expected from "enhancement of information sharing system" are the ability to receive the information required by CII operators through complete enhancement of the independent activities of each CEPTOAR and CEPTOAR council in addition to information sharing based on the latest information sharing system as well as information sharing to and from NISC. For this reason, indexes are set which focus on the development of information shared with the prepared information sharing system.

<Detailed indexes>

* Number of cases of information sharing to and from NISC by the Cabinet Secretariat
* Number of occasions of information exchanges by CEPTOAR council and cross-sectoral exercise stakeholders
* Number of cases of information sharing in the CEPTOAR council

3.2.3 Enhancement of incident response capability

The outcomes expected from "enhancement of incident response capability" are contributions to the improvement of management capability technical aspects and verification of the validity of information sharing to and from NISC between stakeholders required for verification of CII operator implemented early recovery procedures during IT outages and IT-BCP through participation in exercises and training centering on cross-sectoral exercises. For this reason, indexes are set which focus on the contribution to CII operator initiatives of knowledge gained through participation in exercises and training in addition to the promotion of exercise results, construction of realistic exercise environments and cross-sectoral exercises.

<Detailed indexes>

* Number of participants in cross-sectoral exercises
* Ratio of participants who assess the information obtained through exercises as having contributed to the measures for CIIP of the organization to which they belong
* Participation in exercises and training implemented both inside and outside the organization, including cross-sectoral exercises

3.2.4 Risk management

The outcomes expected from "risk management" are the promotion and enhancement of risk management implemented by CII operators. For this reason, indexes are set which focus on consultation as well as risk assessment and risk communication supported by the Cabinet Secretariat from among the risk management processes implemented by CII operators.

<Detailed indexes>

* Number of cases of interdependency analysis and environmental change studies implemented by the Cabinet Secretariat
* Number of occasions of provision of opportunities for information exchange by

CEPTOAR council and cross-sectoral exercise stakeholders

3.2.5 Enhancement of the basis for CIIP

The outcomes expected from "enhancement of the basis for CIIP" are: for "public relations activities", obtaining the greatest degree of understanding from the public in relation to the framework of the Basic Policy and expanding the scope of those cooperating with this Basic Policy beyond just stakeholders; for "international cooperation", support and development of opportunities for information exchanges with various countries through bilateral, inter-regional and multilateral frameworks; and for "preparation of norms, standards and regulations, etc. for reference", the usage of the prepared regulations, etc. by CII operators. For this reason, indexes are set which focus on the development of opportunities to publicize this Basic Policy and international cooperation as well as the status of the preparation of the regulations, etc.

<Detailed indexes>

* Number of times information is dispatched through newsletters, etc.
* Number of times lectures, etc. related to the Basic Policy are held
* Number of times information exchanges etc. are held through bilateral, inter-regional and multilateral frameworks
* Conditions of preparation of guidebooks etc. which contribute to CII protection
* Expansion conditions of third party certification systems for control equipment and systems

4. RIVISION OF THE BASIC POLICY BASED ON THE ASSESSMENT OF THE OUTCOMES

The assessment carried out from the "view of measuring outcomes" is carried out in comparison with the goals of this Basic Policy which are the ideal future image. During this, in consideration that the various initiatives based on this Basic Policy are mutually related and to realize output and outcomes, assessment is not carried out for each individual initiative, but rather for overall initiatives which contribute to the maintenance and improvement of protective capability for CII, and so is thus carried out comprehensively and analytically for the framework of this Basic Policy.

When carrying out assessment of the framework of this Basic Policy, it is important to carry out assessment after appropriately determining the conditions which cannot be completely determined through only the individual output and outcomes of policy groups. For this reason, in order to collect the supplementary information required for assessment, supplementary studies shall be carried out one per fiscal year in principle.

In addition, for assessment management, as it is difficult to examine improvement measures immediately even if changes are tracked each year, so in principle 1 time per 3 years assessment shall be carried out by the Cybersecurity Strategic Headquarters, and the studies and examination required shall be carried out by the CII Expert Committee through cooperation from the responsible ministries for CIIP.

As such, for the revision of the Basic Policy based on the assessment of outcomes as well, in principle 1 time per 3 years the assessment shall be carried out by the Cybersecurity Strategic Headquarters, and the studies and examination required shall be carried out by the CII Expert Committee through cooperation from the responsible ministries for CIIP.

The limitation of 1 time per 3 years shall not apply in the event of any events occurring outside the assumptions of this Basic Policy such as serious changes in social trends.

ATTACHMENT: "INFORMATION SHARING TO NISC" AND "INFORMATION SHARING FROM NISC"

1. INFORMATION RELATED TO IT FAILURES, ETC

"Information related to IT failures, etc." is an extensive variety of information which contributes to measures for CIIP related to IT failures, including IT outages, signs and "Hiyari-Hatto".Information related to IT failures, etc. includes 3 aspects of (1) proactive prevention of IT outages, (2) prevention of the spread damages and quick recovery from IT outages, and (3) prevention of recurrence through analysis and verification of IT outage causes, and must be provided suitably and appropriately to CII operators by government organizations, etc., and enhancement of a system for sharing this type of information among CII operators and interdependent CII sectors.

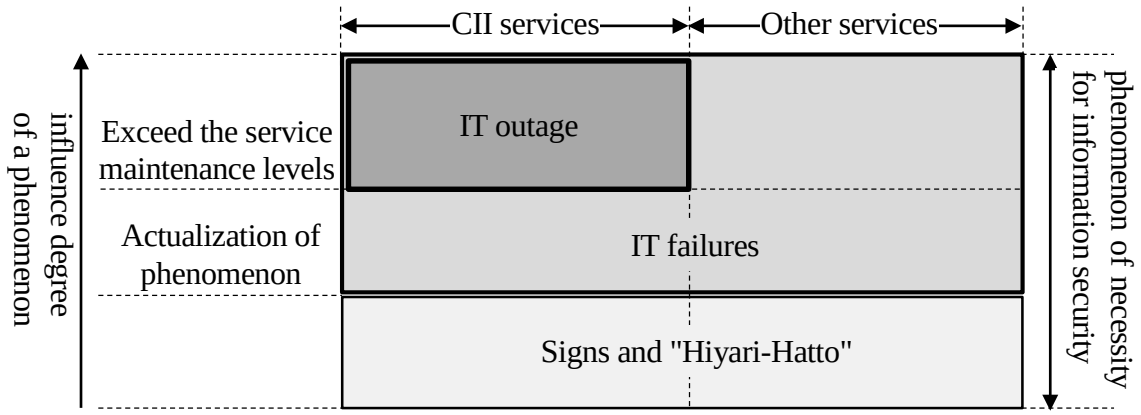
The various aspects of information related to IT failures, etc. include the following.

a) Proactive prevention: Information related to causes of IT failures (including protective measures, etc.)
b) Prevention of spread, and recovery: Information which contributes to effect propagation prediction and recovery after IT outages
c) revention of recurrence: Collaborative collection of information which contributes to ex-post analysis as well as analysis and verification results

In addition, by signs and "Hiyari-Hatto", although the phenomenon is not actualizing, when it actualizes, resulting in IT failure is also considered. Therefore, it is required like the IT failure to also make an omen into the object of information sharing.

Therefore, the scope of information sharing in this basic policy is as being shown in the figure 2.

figure 2. Scope of information sharing



2. INFORMATION SHARING TO NISC FROM CII OPERATORS

2.1 In case of "information sharing to NISC"

Occasions when information sharing to NISC is necessary shall be situations where IT failures, including IT outages, signs or Hiyari-Hatto are confirmed, situations where reporting is required by laws, etc., or situations CII operators have determined that sharing of information is appropriate.

In the event it is uncertain whether or not the above are applicable, it is recommended that the responsible ministries for CIIP or Cabinet Secretariat be consulted.

2.2 Contents of "information sharing to NISC"

The details of information sharing to NISC shall be the on demand reporting of identified events and causes at the time of the report. It is acceptable if the information at this time is fragmentary or indefinite because the complete picture has yet to be identified.

In addition, the setting of common classifications and categories for IT failures, etc. required when information sharing to NISC is carried out from the responsible ministries for CIIP to the Cabinet Secretariat, shall be carried out with consideration for the operability etc. of each CII operator.

2.3 Framework for "information sharing to NISC"

The procedures for sharing of information to NISC from CII operators to the Cabinet Secretariat through the responsible ministries for CIIP are as follows.

a) CII operators shall share information to the responsible ministries for CIIP in accordance with the contact system illustrated in *"ANNEX 5. COMMUNICATION CHANNELS UNDER IT OUTAGES"*.

b) The responsible ministries for CIIP liaison shall share the information received from the CII operator of the relevant sector to the Cabinet Secretariat.

c) The Cabinet Secretariat shall appropriately manage the shared information, and handle the information within the information sharing scope specified by the information source.

2.4 Handling of "information sharing to NISC"

For the handling of information shared to NISC, the Cabinet Secretariat and the responsible ministries for CIIP that received the information shall in principle, where not otherwise specified by law or agreed to by the CII operator submitting the information, handle said information as the information (voluntarily provided information) prescribed in Article 5 Item

2 of the Act on Access to Information Held by Administrative Organs (Law 42 of 1991). In cases where the relevant information is subject proviso in the same item, the information may be publically disclosed.

3. INFORMATION SHARING FROM NISC TO CII OPERATORS

3.1 Scope of CII operators subject to "information sharing from NISC"

The scope of provision of information to CII operators from the Cabinet Secretariat shall be the CII sectors which the Cabinet Secretariat deems the information relevant to, from among the information sharing scope specified by the information provider in advance. In cases where the Cabinet Secretariat deems it is necessary to share information outside of the information sharing scope specified by the information provider, it shall be able to coordinate the change of the sharing scope with the information provider.

3.2 Contents of "information sharing from NISC"

Information sharing from NISC shall be carried out for information considered to be effective for CII operator measures for CIIP from a wide range of information which is collected and analyzed from information provided by responsible ministries for CIIP, information security related ministries, CIIP supporting agencies and cyberspace-related operators.

In addition, if the information provided from the CII operators is applicable to a) or b) below, information sharing shall be carried out after employing appropriate measures such as processing the information so that the providing CII operator cannot be identified in order to prevent the CII operator providing the information from suffering any disadvantage as a result.

a) If the obtained information is regarding a security hole, program bug, etc. and it is recognized that said information could cause problems at other CII operators.
b) If there is a cyber-attack or advance notice of such an attack, if there are predicted damages from a disaster, or when it is otherwise recognized that the information poses a risk to the critical information systems of other CII operators.

3.3 Framework for "information sharing from NISC"

The procedures for sharing of information from NISC to CII operators from the Cabinet Secretariat through the responsible ministries for CIIP are as follows.

a) When the Cabinet Secretariat shares information from NISC, such sharing shall be carried out through liaisons to the Cabinet Secretariat for each sector under the jurisdiction of the responsible ministries for CIIP. At this time, the individual receiving the information shall enact appropriate identification methods for the information to allow for the information to be easily and so that the information classification and scope of handling according to the information's degree of importance, content, and other factors, can be recognized at a glance.
b) The responsible ministries for CIIP liaison shall convey the information to the CEPTOAR point of contact (PoC).

c) The CEPTOAR shall convey the information to the CII operators which make up the CEPTOAR.

d) In particularly urgent cases, such as early warning information, etc., regardless of steps a) to c), the Cabinet Secretariat shall directly provide the information to the CEPTOAR or individual CII operators and report to the individual critical infrastructure operators or scepter directly from the Cabinet Secretariat, and simultaneously report to the responsible ministries for CIIP liaison. However, normalization of identification methods shall be carried out in accordance with step a).

3.4 Cooperation for "information sharing from NISC"

In the collection of information provided to CII operators through responsible ministries for CIIP and in sharing of information to CII operators, the Cabinet Secretariat shall cooperate with the information security related ministries, CIIP supporting agencies and cyberspace-related operators as follows.

a) Collect a wide range of information provided by information security related ministries and CIIP supporting agencies.

b) Collect additional information etc. related to IT outages from cyberspace-related operators as necessary.

c) Request cooperation from CIIP supporting agencies and cyberspace-related operators in the collection and analysis of information as necessary.

d) For information during IT crises, collection and sharing of information under an information sharing system composed of the Cabinet Secretariat, crisis management ministries and the disaster prevention related ministries in addition to information sharing system during normal times.

3.5 Improvement of the quality of the information to be shared

Attempts will be made to improve the quality of the information provided while continuing to take the following points into account.

a) Improve accuracy by comparing information.

b) Determine the degree of importance and priority of information according to a).

c) Impact forecasts for other CII sectors for IT outages which occur as a result of CII sector service outage/decline and IT outages which occur as a result of risk sources common across sectors.

ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES

CII sectors	Applicable CII operators (Note 1)	Applicable critical information system examples (Note 2)	Examples of IT outages and effects
Information and communication services	- Major electronic communications operators - Major terrestrial base broadcast operators - Major cable television operators	- Network systems - Operation support systems - Organization/operation systems	・Electrical communications outages ・Outages etc. related safe and stable provision of electrical communications services ・Broadcast service outages
Financial services: Banking services Life insurance services General insurance services Securities services	- Banks, credit unions, labor credit unions, agricultural cooperatives, etc. - Financial settlement agencies - Electronic credit record agencies - Life insurance services - General insurance services - Securities firms - Financial product exchanges - Money transfer agencies - Financial product clearing agencies etc.	- Accounting systems - Financial securities systems - International systems - External connection systems - Financial institution internetwork systems - Electronic credit record agency systems - Insurance service systems - Securities trading systems - Exchange systems - Money transfer systems - Clearance systems etc.	- Outages of deposit payments, fund transfers including bank transfers and loans - Financial settlement outages - Outages of information provision related to electronic records and fund settlements - Insurance claim payment outages - Securities trading outages - Corporate bond/stock transfer outages - Financial product clearing outages etc.
Aviation services	- Major scheduled air transport operators - Ministry of Land, Infrastructure, Transport and Tourism (air traffic control/weather)	- Flight systems - Reservation/boarding systems - Maintenance systems - Cargo systems - Air traffic control systems - Meteorological information systems	- Flight delays and cancellations - Obstacles to safe flight of airplanes, etc.
Railway services	- Major railway operators including JR companies and major private railway companies	- Railway traffic control systems - Power supply control systems - Seat reservation systems	- Railway traffic delays and cancellations - Obstacles to safe railway transport, etc.
Electric power supply services	- General electric power supply services, Japan Atomic Power, Electric Power Development	- Control systems - Operation monitoring systems	- Power supply outages - Obstacles to safe operation of power plants
Gas supply services	- Major gas supply operators	- Plant control systems - Remote monitoring and control systems	- Gas supply outages - Obstacles to safe operation of gas plants
Government and administrative services	- Various ministries and government offices - Local government	- Various ministry and local government information systems (handling of e-government and e-municipalities)	- Obstacles to government and administrative service operations - Leak, theft and alteration of personnel information
Medical services	- Medical facilities (Excluding small scale facilities)	- Medical examination record management systems, etc. (electronic patient record systems, remote diagnostic imagining systems, electric medical equipment, etc.)	- Obstacles to work in medical examination support departments
Water services	- Water service operators and city water service providers (Excluding small scale facilities)	- Water utility and water supply monitoring systems - Water utility control systems, etc.	- Outages of water supply - Supply of water of unsuitable quality, etc.

Logistics services	- Major logistics operators	- Collection and delivery management systems - Cargo tracking systems - Warehouse management systems	- Shipping delays and cancellations - Difficulties tracking cargo location
Chemical industries	- Major petrochemical facilities	- Plant control system	- Plant outages - Long-term suspend of long-term product supply
Credit card services	- Major credit card services operators etc.	- Credit card authorization system etc.	- Outages of credit card authorization
Petroleum industries	- Major petroleum refinery facilities and petroleum wholesalers	- Sales order management system - Product management system - Shipping management system etc.	- Outages of the petroleum products supply - Obstacles to safety operation of refinery plants etc.

Note 1 The operators listed here are CII operators for which measures should be implemented on a priority basis, and review of the applicable operators shall be carried out based on changes in the business environment and progressive dependence on IT, when the Basic Policy is revised.

Note 2 The details of the applicable critical information systems are stipulated by CII operators based examples of IT outages and their effects.

ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS

CII sectors		CII services (including procedures) (Note)		Service maintenance levels	
		Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
Information and communication services		- Electrical communication services	- Use of electrical communication facilities to act as an intermediary for others communications and providing other electrical communications facilities for the communications of other parties (Article 2 of the Telecommunications Business Act)	- No trouble should occur causing continued loss of service for 2 hours or more for 30,000 or more users due to outages or deterioration of quality of service provision as a result of electrical communications facility trouble	- In accordance with Article 58 of the Ordinance for Enforcement of the Telecommunications Business Act
		- Broadcasting services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- No trouble should occur causing continued outages of broadcasting for 15 minutes or longer as a result of trouble with base broadcasting facilities - No trouble should occur causing continued outages of broadcasting for 15 minutes or longer (2 hours or more for relay station wireless facilities) as a result of trouble with base broadcasting facilities and specified terrestrial base broadcasting facilities	- In accordance with the Ordinance for Enforcement of the Broadcast Act from Item 1 to Item 3
		- CATV services	- Electrical communications broadcast aimed at direct reception by the public (Article 2 of the Broadcast Act)	- No trouble should occur causing continued loss of service for 2 hours or more for 30,000 or more users as a result of broadcasting outages resulting from cable television facility trouble	- In accordance with Article 157 of the Ordinance for Enforcement of Broadcast Act
Financial services	Banking services	- Deposits - Loans - Exchange	- Receipt of deposits or periodic deposits (Article 10, paragraph 1, item 1 of the Banking Act) - Lending of loans or discounting of bills (Article 10, paragraph 1, item 2 of the Banking Act) - Currency exchange (Article 10, paragraph 1, item 3 of the Banking Act)	- No delay or outages of deposit repayment should occur as a result of IT failures - No delay or outages of execution of loan agreements should occur as a result of IT failures - No delay or outages of currency exchange (bank transfer) should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Major Banks, etc." - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment (for example, even if a number of ATMs were suspended, if other ATMs or windows were available at the same or neighboring branches)
		- Financial settlements	- Financial settlements (Article 2, paragraph 5 of the Act concerning Financial Settlements)	- No delay or outages of financial settlements should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment

CII sectors		CII services (including procedures) (Note)		Service maintenance levels	
		Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
		- Electronic records, etc.	- Electronic records (Article 56 of the Electronically Recorded Monetary Claims Act) - Information provision related to fund settlement (Articles 62 and Article 63 of the Electronically Recorded Monetary Claims Act)	- No delay or outages of information provision related to electronic record and fund settlement should occur as a result of IT failures	- Refer to "Guideline for Administrative Processes Vol 3.: Financial Companies (12 Electronic credit record agency relationships)"
	Life insurance	- Insurance claim etc. payments	- Receipt of insurance claim etc. payment demands - Insurance claim etc. payment screenings - Insurance claim etc. payments	- No delay or outages of insurance claim etc. payment should occur as a result of IT failures	- Refer to "Comprehensive Guidelines for the Supervision of Insurance Companies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
	General insurance	- Insurance claim etc. payments	- Accident reception - Damage investigations etc. - Insurance claim etc. payments	- No delay or outages of insurance claim etc. payment should occur as a result of IT failures	- Refer to "Comprehensive Guidelines for the Supervision of Insurance Companies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
	Securities services	- Negotiable securities trading etc. - Transaction mediation, commission and representation for negotiable securities trading etc. - Negotiable securities etc. settlement commission	- Negotiable securities trading, market derivatives trading or foreign market derivatives trading (Article 2, paragraph8, item 1 of the Financial Instruments and Exchange Act) - Mediation, commission or representation for negotiable securities trading, market derivatives trading or foreign market derivatives trading (Article 2, paragraph 8, item 2 of the Financial Instruments and Exchange Act) - Negotiable securities etc. settlement commission (Article 2, paragraph 8, item 5 of the Financial Instruments and Exchange Act)	- No delay or outages of disposal of securities received for guarantee, cancellation payments, etc. should occur as a result of IT failures	- Refer to the "Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc." - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment (for example, situations where if the order system is suspended outside of market hours, replacement systems are quickly activated which are equivalent to the concerned system allowing for orders in time for market hours.)
		- Establishment of financial product markets	- Provision of market facilities for the trading of negotiable securities or market derivatives trading, and other work related to the establishment of financial product markets (Article 2, paragraph 14 and 16 and Article 80 and Article 84 of the Financial Instruments and Exchange Act)	- No delay or outages of trading of negotiable securities or market derivatives trading, etc. should occur as a result of IT failures	- Refer to Article 112 Item 7 of the Cabinet Office Ordinance on Financial Instruments Business, etc.
		- Money transfer services	- Work related to transfer of corporate bonds, etc. (Article 8 of the Act on Book-Entry Transfer of Company Bonds, Shares, etc.)	- No delay or outages of transfer of corporate bonds or shares should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment

CII sectors	CII services (including procedures) (Note)		Service maintenance levels	
	Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
	- Financial product debt underwriting	- Liability assumption work through underwriting or renewal of debt based on negotiable securities trading etc. targeted transactions (Article 2, paragraph 28 of the Financial Instruments and Exchange Act)	- No delay or outages of financial product settlement should occur as a result of IT failures	- Refer to the "Comprehensive Guideline for Supervision of Settlement/Money Transfer Agencies" - Excluding situations where no practical effect occurs as a result of quick substitution by other systems/equipment
Aviation services	- Air transportation services for passengers and cargo - Air traffic control service - Distribution of meteorological information - Reservations, ticketing, boarding/loading procedures - Flight maintenance - Flight plan creation	- Work providing transport of passengers or cargo for charge using airplanes based on demands of other people (Article 2 of the Civil Aeronautics Act) - Appropriate usage of airspace and space and smooth maintenance of air traffic (Article 95-2 of the Civil Aeronautics Act) - Distribution of forecasts, warnings, etc. adapted for airplane use (Article 14 of the Meteorological Service Act) - Air traveler reservations, air cargo reservations - Airline ticket issuance, fee collection - Airline passenger check-in and boarding, air cargo loading - Airplane inspection and maintenance - Creation of flight plans and submission to Japan Civil Aviation Bureau	- No obstacles should be caused for transport of passengers on scheduled flights due to IT failures	- Handled in the agreement related to "CEPTOAR in the aviation services sector"
Railway services	- Passenger transport services - Ticketing, entry and exit procedures	- Work providing transport of passengers or cargo for charge using railways based on demands of other people (Article 2 of the Railway Business Act) - Seat reservation, boarding ticket checks on boarding and exiting the train	- No obstacles should be caused for transport of passengers on as a result of suspended trains due to IT failures	- In accordance with Article 5 of the Railway Accident Reporting Code (Private railway accident etc. reports)
Electric power supply services	- General electric power supply service	- Work supplying electric power to meet general demand (Article 2 and Article 18 of the Electric Business Act)	- No supply problem incidents of over 10 minutes for supply power of 100,000 kilowatts or more should occur as a result of IT outages	- In accordance with Article 3 of the Electricity related Reporting Code
Gas supply services	- General gas supply service	- Work supplying gas through piping to meet general demand (Article 2 of the Gas Business Act)	- No supply problem incidents effecting supply to 30 or more houses should occur as a result of IT outages	- In accordance with Article 112 of the Gas Ordinance for Enforcement of the Gas Business Act

CII sectors	CII services (including procedures) (Note)		Service maintenance levels	
	Name	Explanation of services (including procedures) (Relevant laws)	Applicability/standards	Remarks
Government and administrative services	- Local government administration services	- Local administration, other administration work carried out in accordance with laws or government ordinances (Article 2, paragraph 2 of the Local Autonomy Act)	- No obstruction of the protection of resident Ⅰ rights and gains should occur as a result of IT failures - System recovery should be accomplished within a time period allowing for guarantee of resident safety and security	
Medical services	- Medical examination	- Examination and treatment	- No danger to human life shall occur as a result of incorrect operation of medical equipment. - No obstruction of the continued provision of medical care should occur as a result of IT failures.	- All efforts must be made to maintain the level of medical examination and treatment regardless of the degree of IT dependence.
Water services	- Supply of water through water services	- Work supplying drinking water through piping or other structures to meet general demand (Article 3 and Article 15 of the Water Supply Act)	- No interruption or decrease of water supply, abnormal quality water supply or serious problems in systems should be caused for supply of water as a result of suspended IT failures	- Important system problems refers to problems with control systems (water purification plant monitoring and control systems, pumping station operation systems, water mobilization systems, etc.) which have a serious impact on water supply in the event of a system shutdown - In accordance with "appropriate implementation of health risk management and provision of information related to damages to water supply facilities and water quality incidents" (October 25, 2013) "6.(2) In the event of information system outages in water supply"
Logistics services	- Logistics services	- Transport and storage of cargo	- No interruption of cargo transport or loss of cargo should occur as a result of IT failures	- Handled in the "agreement related to information sharing and analysis functions in the logistics sector (CEPTOAR)"
Chemical industries	- Petrochemical industries	- Production, processing and trade of petrochemical product	- No major interruption of supply of petrochemical industries should occur as a result of IT failures	
Credit card services	- Credit card authorization	- Approval at the time of the use in the intermediation of comprehensive credit purchases (Article 2, paragraph 3, item 1 and 2, and Article 35-16, paragraph 2 of Installment Sales Act)	- No delay, outage of service or misapply of credit card authorization should occur as a result of IT failures	
Petroleum industries	- Petroleum products supply	- Import, refine , distribute and sale of petroleum	- No interruption of petroleum supply should occur as a result of IT failures	

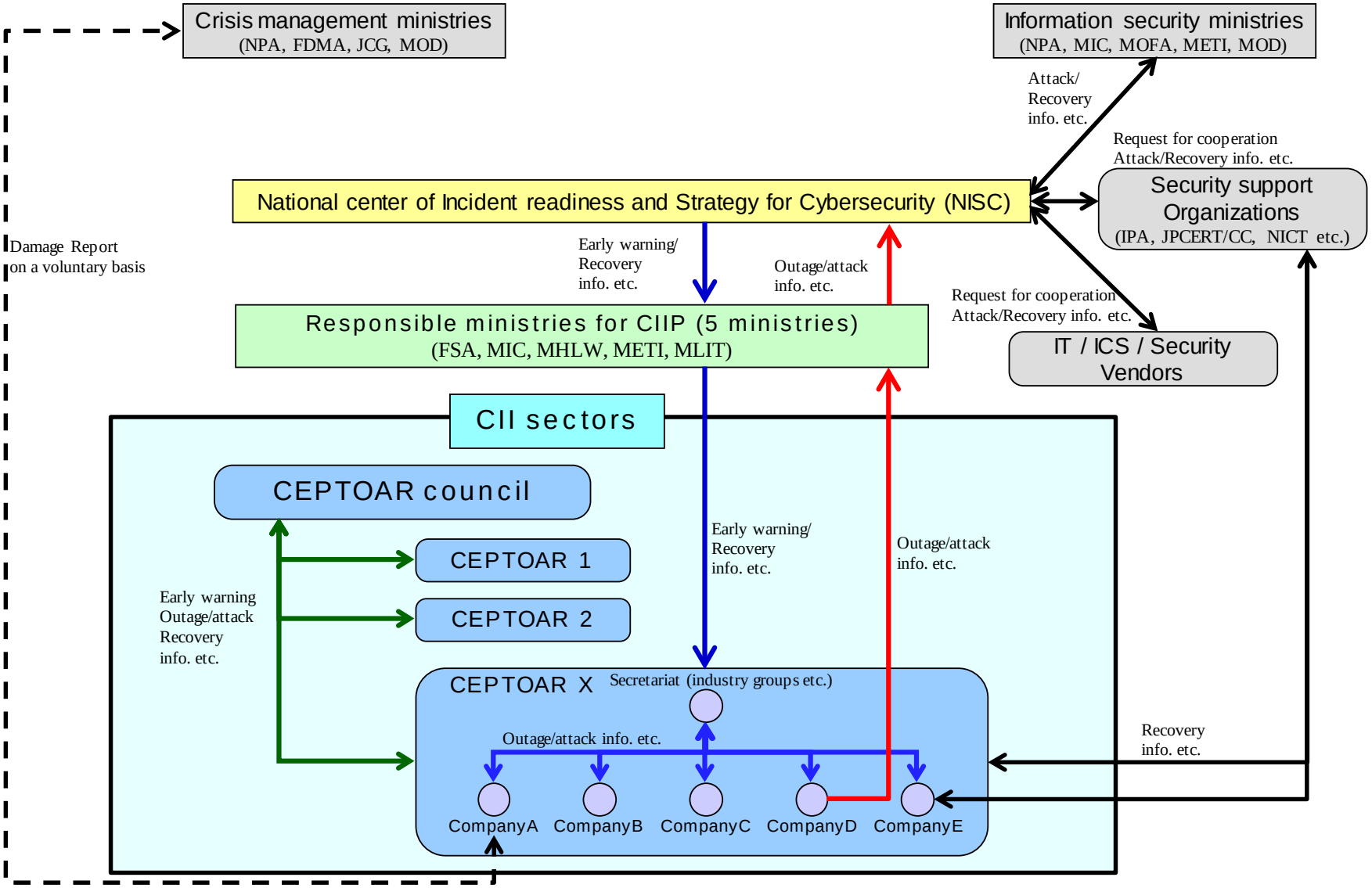
Note Services which make absolutely no use of IT are outside the scope of application.

ANNEX 3. CATEGORIES OF EVENTS AND CAUSES FOR INFORMATION SHARING TO NISC

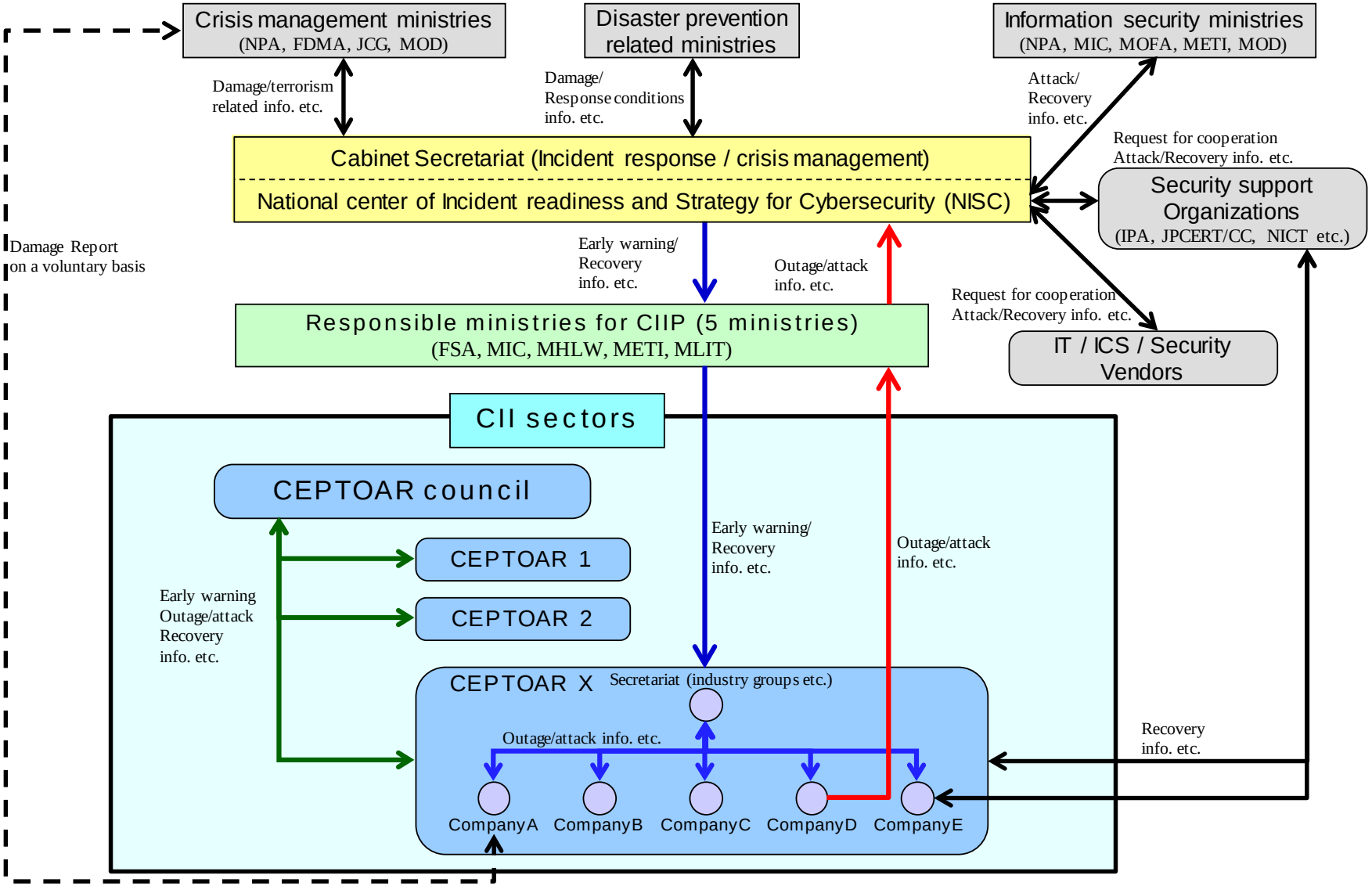
Event Categories		Event Example	Description
Events that have not occurred yet		Signs, Hiyari-Hatto	Signs such as cyber-attack warnings or Hiyari-Hatto (potentially serious damage) without occurrence of events that threaten confidentiality, integrity or availability such as minor mistakes or receipt of malware attached to suspicious emails
Events that have occurred	Events that threaten confidentiality	Information leakage	Events that threaten confidentiality, such as the leakage of organization's confidential information
	Events that threaten integrity	Data corruption	Events that threaten integrity, such as website defacement or corruption of organization's confidential information
	Events that threaten availability	Problems in using systems	Events that threaten availability, such as loss of stable operation of control systems or inability of viewing websites
	Events that can lead to those above	Malware infections	Infection of systems by malware
		Execution of unauthorized code	Execution of unauthorized code exploiting the vulnerability of systems
		System intrusions	Intrusions into systems caused by cyber-attacks
		Others	Events other than those above

Cause Categories	Cause Examples
Deliberate causes	Receipt of suspicious emails, fraudulent of user IDs, mass access such as DoS attacks, unauthorized acquisition of information, internal fraud, lack of appropriate system operation, etc.
Accidental causes	Mistaken user operation, mistaken user management, execution of suspicious files, viewing of suspicious websites, unsupervised work by outsourcing contractor, failure of equipment, vulnerabilities, cascading effect from other sectors' failures, etc.
Environmental causes	Disasters, illnesses, etc.
Others	Threats and vulnerabilities other than those above, unknown causes, etc.

ANNEX 4-1. INFORMATION SHARING SYSTEM (NORMAL CIRCUMSTANCES)



ANNEX 4-2. INFORMATION SHARING SYSTEM (IT CRISES)



ANNEX 5. COMMUNICATION CHANNELS UNDER IT OUTAGES

CII sectors		Existing communication channels	Emergency communication channels under IT outages
Information and communication services		(1) CII operators->Government - Reporting of business outages etc. to the Minister of Internal Affairs and Communications in accordance with the Telecommunications Business Act - Reporting of broadcast outages incidents, serious wireless communications disturbances, etc. to the Ministry of Internal Affairs and Communications (2) Government->CII operators, Between CII operators - Reporting and sharing of virus outbreak and other emergency information within the industry and with the Ministry of Internal Affairs and Communications	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using the T-CEPTOAR, broadcast CEPTOAR and cable TV CEPTOAR contact system - Implemented using existing contact system
Financial services	Banking services Life insurance services General insurance services Securities services	(1) CII operators->Government - Reporting of service delays and outages to the Prime Minister (Financial Services Agency) in accordance with industry laws (2) Government->CII operators, Between CII operators	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using banking services etc. CEPTOAR contact system - Implemented using securities services CEPTOAR contact system - Implemented using life insurance services CEPTOAR contact system - Implemented using general insurance services CEPTOAR contact system - Implemented through other industry associations, etc.
Aviation services		(1) CII operators->Government - Reporting of airplane accidents to the Minister of Land, Infrastructure and Transport in accordance with the Civil Aeronautics Act (2) Government->CII operators, Between CII operators - Establishment of IT outage related point of contact - Sharing of information related to aviation service security systems to relevant agencies (by airport)	(1) CII operators->Government - Implemented using the existing incident reporting system in the event of an incident - Implemented using aviation services sector CEPTOAR contact system for IT outages not resulting in accidents (2) Government->CII operators - Implemented using aviation services sector CEPTOAR contact system - CII operators directly contacted through point of contact
Railway services		(1) CII operators->Government, Government->CII operators - Reporting of railway operation accidents etc. to the Minister of Land, Infrastructure and Transport in accordance with the Railway Accident Reporting Code - Preparation of an IT outage related contact system (2) Between CII operators - None	(1) CII operators->Government, Government->CII operators - Implemented using the existing incident reporting system in the event of an incident - Implemented using railway services CEPTOAR contact system

CII sectors	Existing communication channels	Emergency communication channels under IT outages
Electric power supply services	(1) CII operators->Government - Reports related to supply problem incidents to the Minister of Economy, Trade and Industry in accordance with the Electricity related Reporting Code (2) Government->CII operators, Between CII operators - Establishment of IT outage related point of contact	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using the contact system for information sharing and analysis functions related to IT outages in power supply - CII operators directly contacted through point of contact
Gas supply services	(1) CII operators->Government - Reporting of gas supply problem incidents over a certain size to the Minister of Economy, Trade and Industry in accordance with the Ordinance for Enforcement of the Gas Business Act (2) Government->CII operators, Between CII operators - Notification within the same industry in the event of the occurrence of gas supply problems as a result of disasters in accordance with the Japan Gas Association "relief measures outline"	(1) CII operators->Government - Implemented using existing contact system (2) Government->CII operators - Implemented using gas supply services CEPTOAR contact system - Implemented through CII operators
Government and administrative services	(1) Various ministries and government offices->Cabinet Secretariat - Information sharing to NISC in accordance with "Regarding communications related to government information systems during emergencies" (April 17, 2000) (2) Cabinet Secretariat->Various ministries and government offices - Information sharing from NISC in accordance with "Regarding communications related to government information systems during emergencies" (April 17, 2000) (3) Local government->Government - Information sharing from NISC in accordance with "Regarding response reporting and preparation of an emergency contact system for the occurrence of information security incidents (Notification)" (4) Government ->Local government - Information sharing from NISC in accordance with "Regarding response reporting and preparation of an emergency contact system for the occurrence of information security incidents (Notification)"	(1) Various ministries and government offices->Cabinet Secretariat, Cabinet Secretariat->Various ministries and government offices - Implemented using the internal government contact system (2) Local government->Government, Government->Local government - Implemented using local government CEPTOAR contact system - Implemented using existing contact system
Medical services	(1) CII operators->Government, etc. (2) Government, etc.->CII operators	(1) CII operators->Government, etc. (2) Government, etc.->CII operators - Implemented using medical services CEPTOAR contact system
Water services	(1) CII operators->Government, etc. (2) Government, etc.->CII operators	(1) CII operators->Government, etc. (2) Government, etc.->CII operators - Implemented using the water supply CEPTOAR IT outage information handling related guideline contact system

CII sectors	Existing communication channels	Emergency communication channels under IT outages
Logistics services	(1) CII operators->Government - Reporting of accidents etc. to the Minister of Land, Infrastructure and Transport in accordance with various industry laws (2) Government->CII operators - Designated public agencies stipulated in the Cabinet Office Disaster Countermeasures Basic Act	(1) CII operators->Government - Implemented using the existing incident reporting system in the event of an incident - Implemented using logistics CEPTOAR contact system for IT outages not resulting in accidents (2) Government->CII operators - Implemented using logistics services CEPTOAR contact system
Chemical industries	(1) CII operators->Government - Reporting etc. to presiding ministries and related ministries in accordance with the relevant laws (2) Government->CII operators	(1) CII operators->Government - Implemented using existing contact system - Implemented using chemical industries CEPTOAR contact system (2) Government->CII operators - Implemented using chemical industries CEPTOAR contact system
Credit card services	(1) CII operators->Government - Reporting etc. to presiding ministries and related ministries in accordance with the relevant laws (2) Government->CII operators - Information sharing in the sectors	(1) CII operators->Government - Reporting etc. to presiding ministries and related ministries in accordance with the relevant laws (2) Government->CII operators - Implemented using credit card services CEPTOAR contact system
Petroleum industries	(1) CII operators->Government - Reporting etc. to presiding ministries and related ministries in accordance with the relevant laws (2) Government->CII operators - Information sharing in the sectors	(1) CII operators->Government - Implemented using petroleum industries CEPTOAR contact system (2) Government->CII operators - Implemented using petroleum industries CEPTOAR contact system

ANNEX 6. DEFINITIONS / GLOSSARIES

CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response. Functions which provide information sharing and analysis at CII operators, and organizations which serve as these functions.
CEPTOAR council	The council composed of representatives of each CEPTOAR which carries out information sharing between CEPTOARs. An independent body, not positioned under other agencies, including government organizations.
CII	The backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted. If the function of the services is suspended, deteriorates or becomes unavailable, it could have a significant impact on the national life and economic activities.
CII operators	Operators designated in "Applicable CII operators" in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"* and groups composed of those designated operators.
CII sectors	"information and communication services", "financial services", "aviation services", "railway services", "electric power supply services", "gas supply services", "government and administrative services (including local government)", "medical services", "water services", "logistics services", "chemical industries", "credit card services" and "petroleum industries".
CII services	Services and/or a set of procedures provided by CII operators necessary to utilize those services designated in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"* in each CII sector, taking into account that the extent of impact to national life and economic activities.
CIIP supporting agencies	The National Police Agency Cyber Force, National Institute of Information and Communications Technology (NICT), National Institute of Advanced Industrial Science and Technology (AIST), Information-Technology Promotion Agency (IPA), Telecom Information Sharing And Analysis Center Japan (Telecom-ISAC Japan), and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).
Crisis management ministries	The National Police Agency (NPA), Fire and Disaster Management Agency (FDMA), Japan Coast Guard (JCG) and Ministry of Defense (MOD).
Critical information systems	Information systems required to provide CII services, designated in each CII operator, taking into account of the degree of impact to its CII service. Examples shown in *"ANNEX 1. SCOPE OF CII OPERATORS AND CRITICAL INFORMATION SYSTEM EXAMPLES"*.
Cyberspace-related operators	System vendors, which are engaged in the design, construction, operation and maintenance of information systems required for providing CII services, security vendors, which provide measures for CIIP such as antivirus software of those information systems, and platform vendors, which provide the platforms which serve as foundations, including hardware and software of those information systems.
Disaster prevention related ministries	The government organizations and ministries stipulated Article 2 Item 3 of the Disaster Countermeasures Basic Act (Act No. 223 of 1961) which carry are related to information collection during disasters.
Guidelines for safety principles	Measures for CIIP, which contain high-priority items and/or advanced items expected as a reference, collected with an overlook on all the CII sectors, in order to contribute to preparation and revision of safety principles. Main section is approved by the Cybersecurity Strategic Headquarters. Measures section contains detail measures as an example.
Hiyari-Hatto	Unexpected and unpredictable events which did not lead to IT failures, but which had the potential to directly cause IT failures.
Information security related ministries	The National Police Agency (NPA), Ministry of Internal Affairs and Communications (MIC), Ministry of Foreign Affairs (MOFA), Ministry of Economy, Trade and Industry (METI) and Ministry of Defense (MOD).
Information sharing	The mutual sharing of information such as experience, knowledge and know-how by transferring to associates and communicating among organizations and members. It includes both information sharing to NISC and information sharing from NISC.

Information sharing from NISC	The provision of information for contributing to measures for CIIP from the Cabinet Secretariat to CII operators.
Information sharing to NISC	The provision of information related to IT outage, IT failures and Signs/Hiyari-Hatto at CII operators from the CII operators to the Cabinet Secretariat.
Information systems	All systems based on IT such as systems for business processing, control field equipment, monitoring and control systems.
IT-BCP	Business continuity plan (including relevant manuals) related to the information systems to provide CII services, and other Business continuity plan.
IT crises	IT outages which require intensive response by the government such as the establishment of the Cabinet Response Office at the Crisis Management Center in the Prime Minister's Office.
IT failures	Events that information systems for CII do not or cannot perform as expected at the time of their design.
IT outage	IT failures which lead to fall short of the "service maintenance levels" as shown in *"ANNEX 2. CII SERVICES AND SERVICE MAINTENANCE LEVELS"*.
Measures for CIIP	A wide range of activities for preventing IT outages from affecting the national life and economic activities.
Responsible ministries for CIIP	Financial Services Agency (FSA), Ministry of Internal Affairs and Communications (MIC), Ministry of Health, Labour and Welfare (MHLW), Ministry of Economy, Trade and Industry (METI), and Ministry of Land, Infrastructure, Transport and Tourism (MLIT).
Safety principles	Collective measures for CIIPs including "regulations" stipulated by the government in compliance with sector-specific laws, "recommendations" and "guidelines" developed by the government according to sector-specific laws, "standards" and "guidelines" in the whole-sector developed by sector-specific groups to respond to sector-specific laws and public expectations, and "internal policies" prepared by CII operators themselves to respond to sector-specific laws and expectations of public and customs. However, safety principles do not include the "Guidelines for safety principles".
Stakeholders	The Cabinet Secretariat, responsible ministries for CIIP, information security related ministries, crisis management ministries, CII operators, CEPTOAR, CEPTOAR council, CIIP supporting agencies and cyberspace-related operators.