資料５

第４次行動計画下における指針改定について

2017年６月27日

内閣官房内閣サイバーセキュリティセンター 重要インフラグループ

第４次行動計画下における指針改定の概要

１．指針改定の目的

重要インフラ防護能力の維持・向上、とりわけ経営層に関する取組、コンティンジェンシープラン等の作成を含めた対処態勢整備、ＩＴだけでなくＯＴも視野に入れた対策等に資することを目的に、内閣官房は、指針本編・対策編・手引書（「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」）の見直しを行う。

※第４次行動計画　１．１ 指針の継続的改善より

２．指針改定のポイント

【内容面】

- **「機能保証の考え方」を踏まえ、「重要インフラサービスの安全かつ持続的な提供（復旧を含む）」の観点から、安全基準等の継続的な改善に取り組む必要性を明記**
- **情報セキュリティ対策のＰＤＣＡサイクルにおいて、経営層による積極的な関与が期待される場面や具体的な関わり方等を明確化**
- **事業継続計画・コンティンジェンシープランの策定において踏まえるべき「サイバー攻撃リスクの特性」及び「対策の考慮事項」を整理**
  ⇒本日、「サイバー攻撃リスクの特性」に関する「重要インフラサービス障害に係る対処態勢検討ワーキンググループ」での検討結果をご報告
- **ＯＴに係る組織や人材を含むＣＳＩＲＴの構築や、ＯＴの特徴を踏まえたセキュリティ対応が可能な人材の育成の重要性を考慮**

【構成面】

- **ＩＳＯ／ＩＥＣ27001:2013（ISMS）のＰＤＣＡサイクルを踏まえ、対策項目を再整理（CSMSの要求事項も考慮）**
  ⇒「指針本編・指針対策編の目次案」及び「新たに追加した対策項目」を本紙に整理（スライド４～６）
- **「指針手引書」を今年度、新規策定する「重要インフラにおける情報セキュリティ確保に係るリスクアセスメント・ガイドライン」へ統合**
  ⇒リスクアセスメント・ガイドラインの概要及び指針手引書との目次ベースでの比較を本紙に整理（スライド７、８）

３．指針改定のスケジュール

本会において、2017年度に実施する以下の討議を経て指針を見直し、
2018年度から改定版（第５版）を施行。

Ｑ１（本日）	Ｑ２	Ｑ３	Ｑ４
・改定方針の討議	・改定原案の討議	・修正案の討議 ※審議結果を反映した「指針本編」をパブコメへ	・最終案の討議 ※審議結果を反映した「指針本編」をCS戦略本部へ付議

【参考】指針の構成・概要

指針本編	重要インフラ共通の安全基準等で規定が望まれる項目を記載したもの
指針対策編	指針本編に記載した各対策項目の具体例を記載したもの
指針手引書	対策の優先順位付けの考え方、実施手順等を例示したもの

指針の概要

「指針」とは、安全基準等の策定・改定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。
「指針本編」に加えて、別冊である「指針対策編」及び「指針手引書」から構成。

【指針の構成】

重要インフラ行動計画 重要インフラの情報セキュリティ対策に係る行動計画	・政府と重要インフラ事業者等の共通の行動計画 －情報セキュリティ対策の基本的概念 －政府、重要インフラ事業者等の取組 ・サイバーセキュリティ戦略本部にて決定

（行動計画を踏まえ策定・改定）

● 重要インフラ事業者等の対策の方向性を提示

指針本編 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	・安全基準等の基本的な考え方を重要インフラ事業者等に訴求 ・重要インフラ共通の安全基準等で規定が望まれる項目の記載 ・サイバーセキュリティ戦略本部にて決定

● 具体的に何をすればよいか

指針対策編 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　対策編	・指針本編に記載した各対策項目の具体例を記載 －具体的な対策項目のチェックリストの位置付け ・重要インフラ専門委員会にて決定 －技術の進展、社会情勢等の柔軟な反映を目指すため

● どの対策から行うか

指針手引書 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順書	・対策の優先順位付けに係る考え方等、情報セキュリティ対策を実施する際の手順を例示 ・重要インフラ専門委員会にて決定

【指針の活用方法】

指針改定について

重要インフラ防護の目的、基本的な考え方を踏まえつつ、第４次行動計画の内容に照らして指針を補強

【第４次行動計画の記載事項】

●重要インフラ防護の目的
「重要インフラにおいて、機能保証の考え方（※各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うこと）を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。」

●基本的な考え方
「重要インフラ防護における関係主体が一丸となった取組を通じて、重要インフラ防護の目的を果たすとともに、あわせ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対して必要な支援を行う。」

●指針改定を通じて目指すこと
「重要インフラ防護能力の維持・向上、とりわけ経営層に関する取組、コンティンジェンシープラン等の作成を含めた対処態勢整備、ＩＴだけでなくＯＴも視野に入れた対策等に資することを目的に、内閣官房は、指針本編・対策編・手引書（「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」）の見直しを行う。」

●主要な見直しテーマ
・情報セキュリティ文化の醸成や情報セキュリティ対策のＰＤＣＡサイクルの実行に責任を持つ経営層が認識すべき事項及び行動
・機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の作成を含む対処態勢整備
・プラントや工場等の制御系システムへのサイバー攻撃等への迅速な対応にむけた、ＩＴとＯＴの横断的な組織整備及びＯＴのセキュリティ人材の育成

【指針改定のポイント】

●「機能保証の考え方」を踏まえ、「重要インフラサービスの安全かつ持続的な提供」を実現する観点から安全基準等の継続的な改善に取り組む必要性を明記

●情報セキュリティ対策のＰＤＣＡサイクルにおいて、経営層による積極的な関与が期待される場面や具体的な関わり方等を明確化

●事業継続計画・コンティンジェンシープランの策定において踏まえるべき「サイバー攻撃リスクの特性」及び「対策の考慮事項」を整理

●ＯＴに係る組織や人材を含むＣＳＩＲＴの構築や、ＯＴの特徴を踏まえたセキュリティ対応が可能な人材の育成の重要性を考慮

●ＩＳＯ／ＩＥＣ27001:2013（ISMS）のＰＤＣＡサイクルを踏まえ、対策項目を再整理（CSMSの要求事項も考慮）

●「指針手引書」を今年度、新規策定する「重要インフラにおける情報セキュリティ確保に係るリスクアセスメント・ガイドライン」へ統合

指針本編の改定案（目次による新旧比較）

第４次行動計画の「機能保証の考え方」等を反映

ISMS等を踏まえたPDCA構成変更

前頁の見直しテーマに基づく改訂

BCP等で踏まえるべき特性等を追加

並べ替えおよび修正・加筆

指針本編（第５版）の目次（案）	指針本編（第４版）の目次
Ⅰ．　目的及び位置付け	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	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
２．「安全基準等」の必要性	２．「安全基準等」の必要性
３．「安全基準等」とは何か	３．「安全基準等」とは何か
４．指針の位置付け	４．指針の位置付け
５．指針の構成	５．指針の構成
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	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
Ⅱ．「安全基準等」で規定が望まれる項目	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	１．「安全基準等」策定の目的
２．「安全基準等」の対象範囲	２．「安全基準等」の対象範囲
３．「安全基準等」において対象とする原因	３．「安全基準等」において対象とする原因
４．役割	４．役割
５．「安全基準等」の公開	５．「安全基準等」の公開
６．対策項目	６．対策項目
６．１「Ｐｌａｎ（準備）」の観点	６．１「Ｐｌａｎ（準備）」の観点
６．１．１「組織の状況」の観点	６．１．１「方針」の観点
（１）組織及びその状況の理解	（１）抽出した課題に基づくリスク評価
（２）利害関係者のニーズ及び期待の理解	（２）基本方針の策定・見直し
６．１．２「リーダーシップ」の観点	６．１．２「規定」の観点
（１）経営層のコミットメント	（１）内規の策定・見直し
（２）基本方針の策定	（２）ＩＴ－ＢＣＰ等の策定・見直し
（３）組織の役割、責任及び権限の割り当て	（３）情報の取り扱いについての規定化
６．１．３「計画」の観点	６．１．３「計画」の観点
（１）情報セキュリティリスクアセスメント	（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
（２）情報セキュリティリスク対応の決定	６．１．４「体制」の観点
（３）情報セキュリティ関係規定の策定	（１）予算・体制（委託先を含む）の確保
（４）情報セキュリティ対策に係る計画策定	（２）人材育成・配置・ノウハウの蓄積
６．１．４「支援」の観点	（３）外部委託における対策（管理体制・契約・ＩＴ障害時）
（１）経営資源の確保	６．１．５「構築」の観点
（２）人材育成	（１）情報セキュリティ要件の明確化・変更
（３）認識	（２）情報セキュリティ対策（技術）に係る設計・実装・保守
（４）コミュニケーション	（３）情報セキュリティ対策（運用）に係る設計・手順化・保守
６．２「Ｄｏ（実行）」の観点	６．２「Ｄｏ（実働）」の観点
６．２．１「運用」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導入、運用	（１）情報セキュリティ対策の運用（監視・統括）
（２）重要インフラサービス障害への対応	（２）情報セキュリティ対策の運用状況把握
（３）演習・訓練の実施	６．２．２「平時」の観点
６．３「Ｃｈｅｃｋ（評価）」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）
６．３．１「パフォーマンス評価」の観点	（２）情報セキュリティ対策状況の対外説明
（１）監視及び監査	６．２．３「障害発生時」の観点
（２）経営層によるレビュー	（１）ＩＴ障害に対する防護・回復
６．４「Ａｃｔ（改善）」の観点	（２）情報セキュリティ対策状況の対外説明
６．４．１「改善」の観点	６．３「Ｃｈｅｃｋ（確認）・Ａｃｔ（是正）」の観点
（１）是正処置及び継続的改善	６．３．１「平時」の観点
別紙 対処態勢整備に係るサイバー攻撃リスクの特性及び対策の考慮事項	６．３．２「障害発生時」の観点

新たに追加した対策項目

新たに追加した対策項目の概要

重要インフラ事業者等において、従来の対策項目に加えて、下記の点も考慮されることにより、情報セキュリティ対策のＰＤＣＡサイクルの実効性がより高まることが期待される。

●組織及びその状況の理解
重要インフラ事業者等が目指す「重要インフラサービスの安全かつ持続的な提供」に影響する外部及び内部の状況を整理すること。

●利害関係者のニーズ及び期待の理解
「重要インフラサービスの安全かつ持続的な提供」の観点から考慮すべき利害関係者（人、組織）及びそれらの要求を整理すること。

●経営層のコミットメント
重要インフラ事業者等の経営層自らがリーダーシップを発揮して、「重要インフラサービスの安全かつ持続的な提供」の観点等から情報セキュリティ対策に取り組むことを誓約すること。

●組織の役割、責任及び権限の割り当て
情報セキュリティ対策の取組に関連する役割に対して責任及び権限を割り当て、組織内に伝達すること。

●認識
重要インフラ事業者等の職員に、基本方針や自らが情報セキュリティ対策に関与することの重要性等を認識させること。

●コミュニケーション
情報セキュリティ対策の取組に関連する内部及び外部とのコミュニケーションの必要性を明確化すること。

●演習・訓練の実施
演習・訓練の活動を通じ、重要インフラサービス障害の対応計画の精度向上や対応要員のスキルアップ等を図ること。

●是正処置及び継続的改善
目的とのかい離や計画からの遅れ等への対処及び再発防止を繰り返し実施し、情報セキュリティ対策の取組のパフォーマンスを高めること。

指針対策編の改定案（目次による新旧比較）

指針対策編（第５版）の目次（案）
Ⅰ．　対策編の位置付け
Ⅱ．　具体的な情報セキュリティ対策項目の例示
１．「Ｐｌａｎ（準備）」の観点
１．１「組織の状況」の観点
１．２「リーダーシップ」の観点
１．３「計画」の観点
１．４「支援」の観点
２．「Ｄｏ（実行）」の観点
２．１「運用」の観点
３．「Ｃｈｅｃｋ（評価）」の観点
３．１「パフォーマンス評価」の観点
４．「Ａｃｔ（改善）」の観点
４．１「改善」の観点

第４版策定時と同様に、指針本編の構成を踏襲した目次とする

指針対策編（第４版）の目次
Ⅰ．　対策編の位置付け
Ⅱ．　具体的な情報セキュリティ対策項目の例示
１．「Ｐｌａｎ（準備）」の観点
１．１「方針」の観点
１．２「規定」の観点
１．３「計画」の観点
１．４「体制」の観点
１．５「構築」の観点
２．「Ｄｏ（実働）」の観点
２．１「平時・障害発生時共通」の観点
２．２「平時」の観点
２．３「障害発生時」の観点
３．「Ｃｈｅｃｋ（評価）・Ａｃｔ（是正）」の観点
３．１「平時」の観点
３．２「障害発生時」の観点

指針手引書の改定案（リスクアセスメント・ガイドラインへの統合）

【改定方針】

「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」）の別冊である**「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」）を、「重要インフラにおける情報セキュリティ確保に係るリスクアセスメント・ガイドライン」（以下「リスクアセスメント・ガイドライン」）に統合する。**指針手引書の記載内容がリスクアセスメント・ガイドラインに包含されていることを確認のうえ、リスクアセスメント・ガイドラインを指針本編からの参照資料とする。

【背景】

① 2020年の東京オリパラを直接的又は間接的に支えるサービスを提供する事業者等による自律的な情報セキュリティ対策を促進することを目的に、**オリパラ向けリスクアセスメント・ガイドライン（以下オリパラ向けガイドラインという）を2016年度に策定した。**また、同事業者等によるオリパラ向けガイドラインに基づいた第１回リスクアセスメントが2016年度に実施された。

② 第４次行動計画におけるリスクアセスメントの浸透に向けた取り組みとして、上記**オリパラ向けガイドラインを重要インフラ事業者等における平時のリスクアセスメントに利活用できるよう一般化したリスクアセスメント・ガイドライン**を策定し、その趣旨や実施方法を重要インフラ事業者等に浸透させる取り組みを進めることが予定されている。

③ 上記のリスクアセスメント・ガイドラインは、情報セキュリティに係るリスクアセスメントの実施方法についての具体的な手順を含む基礎的なフレームワークを提供するものであり、**リスクアセスメントの各手順について記載した現行の指針手引書を更に充実させた内容（機能保証の観点を追加）**となっている。そのため資料の重複をなくすべく指針手引書はリスクアセスメント・ガイドラインに統合し、同ガイドラインは今後、指針本編の改訂内容や事業者等が実施したリスクアセスメントの結果等を反映して適宜改訂していく運営とする。

指針手引書

【要旨】
「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」**の対策項目の解説や取組例を記載した手引書。

【目的】
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あることを前提に、**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**を記載。

統合

（新規策定）リスクアセスメント・ガイドライン

【要旨】
情報セキュリティに係る**リスクアセスメントの実施方法についての具体的な手順を含む基礎的なフレームワークを提供する**ガイドライン。

【目的】
重要インフラ事業者等が取り組むリスクアセスメントの精度や水準が各重要インフラ事業者等の力量に依存することを前提に、**機能保証に向けたリスクアセスメントの考え方や参考になる作業手順**を示すことで、各重要インフラ事業者等における取組が一定以上の精度・水準を確保することを狙いとする。

指針手引書の改定案（目次による新旧比較）

指針手引書

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
2.　指針手引書の位置付け
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

前ページ記載の通り、ドキュメントの趣旨に大きな変更はなし。

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

「４．リスクアセスメントの対象の特定」の項目内で記載。

1.2　リスク判定基準の策定及び見直し

「５．リスク評価方針の策定」の項目内で記載。

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

「８．リスクアセスメントの継続的な見直し」の項目内（（２）課題管理）で記載。

2.　リスクの特定
2.1　損害をもたらす可能性がある事象の特定
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
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
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
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
5.　リスク対応
5.1　対応策の決定

各々「６．リスクアセスメント」の項目内で記載。

6.　モニタリング及びレビュー
6.1　内的要因に係るモニタリング及びレビュー
6.2　外的要因に係るモニタリング及びレビュー

「８．リスクアセスメントの継続的な見直し」の項目内（（１）リスク管理）で記載。

リスクアセスメント・ガイドライン

１．はじめに
＜１＞ガイドライン策定の背景・目的
＜２＞ガイドラインの適用範囲
＜３＞ガイドラインの構成
２．リスクアセスメントの全体像
３．事前準備
４．リスクアセスメントの対象の特定
＜２＞実施手順
（１）優先サービスの選定
（２）優先サービスの影響分析
（３）優先サービスを支える業務の特定・影響分析
（４）業務を支える経営資源の特定
５．リスク評価方針の策定
＜２＞実施手順
（１）リスク分析手法の検討
（２）リスク基準の決定
６．リスクアセスメント
＜２＞実施手順
（１）リスクの特定
（２）リスクの分析
（３）リスクの評価
＜参考＞リスクアセスメントの次ステップ（リスク対応の選択肢の同定）
７．リスクアセスメントの妥当性確認・評価
＜２＞実施手順
（１）ウォークスルー
（２）パフォーマンス評価

８．リスクアセスメントの継続的な見直し
＜２＞実施手順
（１）リスク管理
（２）課題管理

指針改定のスケジュール

2017年度に実施する以下の討議を経て指針を見直し、2018年度から改定版（第５版）を施行

●第１四半期（本会）
改定方針の討議

●第２四半期
改定原案の討議

●第３四半期
修正案の討議　⇒審議結果を反映した「指針本編」をパブリックコメントへ
（例年どおり指針対策編、リスクアセスメント・ガイドラインは参考提示）

●第４四半期
最終案の討議　⇒審議結果を反映した「指針本編」をサイバーセキュリティ戦略本部へ付議。決定後、公表
（指針対策編、リスクアセスメント・ガイドラインも同時に公表）