資料３

第４次行動計画下における指針改定の概要

2017年10月４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

【再掲：6/27開催の調査会で提示】 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

「指針改定のポイント」を踏まえた指針本編の対応状況

前回の調査会で議論した「指針改定のポイント」を踏まえた、改定作業中の指針本編における対応を以下に記す。

	指針改定のポイント	指針本編における対応
内容面	（１）「機能保証の考え方」を踏まえ、「重要インフラサービスの安全かつ持続的な提供」の観点から、安全基準等の継続的な改善に取り組む必要性を明記	• 指針本編の冒頭で左記の点について言及するとともに、情報セキュリティ対策のＰＤＣＡサイクルの説明の中でも「重要インフラサービスの安全かつ持続的な提供」の観点を踏まえた取組みの必要性を繰り返し言及。
	（２）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	• Plan（計画）フェーズの『経営層のコミットメント』『情報セキュリティ方針の策定』『組織の役割に対する責任及び権限の割当』『資源確保』、Check（評価）フェーズの『経営層によるレビュー』、Act（改善）フェーズの『是正処置及び継続的改善』等の様々な場面においての経営層に期待される行動を記載。 ＜記載例：『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・・・（中略）・・・情報セキュリティ対策に取り組むことを組織の内外に対して誓約する。」 • 『経営層のコミットメント』において第４次行動計画の「重要インフラ事業者等の経営層の在り方」を再掲。
	（３）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	• Do（実行）フェーズの『重要インフラサービス障害への対応』において、コンティンジェンシープラン（ＣＰ）及び事業継続計画（ＢＣＰ）の策定並びに当該計画に基づく重要インフラサービス障害への対応の必要性について言及。 • 上記を補完するものとして、『【別紙３】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項』に、７項目の「サイバー攻撃リスクの特性」を掲載するとともに、それぞれの特性に対応するものとして、20項目の「ＣＰ及びＢＣＰの策定・改定における考慮事項」と、10項目の「ＣＰ及びＢＣＰの発動に備えた平時の対策」を整理。
	（４）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	• Plan（計画）フェーズの『組織の役割に対する責任及び権限の割当』及びDo（実行）フェーズの『重要インフラサービス障害への対応』において、ＣＳＩＲＴ等の組織がサイバー攻撃に起因する重要インフラサービス障害に対応する際、ＯＴ関連部門の人材や知識が必要となる可能性について言及。
構成面	（５）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）	• 『4. 対策項目』において、ＩＳＭＳのＰＤＣＡサイクルを踏まえつつ、重要インフラ事業者等による取組みが期待される情報セキュリティの対策項目を掲載。 • 対策項目の抽出に際しては、「重要インフラのサイバーセキュリティを向上させるためのフレームワーク（NIST）」や「CSMS認証基準（IEC62443-2-1）」等の重要インフラのサイバーセキュリティに関連する標準を考慮。
	（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	• Plan（計画）フェーズの『情報セキュリティリスクアセスメント』の具体的な実施手順等を解説するドキュメントとして位置付け。

指針本編の構成

指針本編の全体構成
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
2．「安全基準等」とは何か
3．指針の位置付け
4．指針の構成
5．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
1．策定目的
2．対象範囲
3．関係主体の役割
4．対策項目
【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
【別紙２】重要インフラサービスの説明と重要インフラサービス障害の例
【別紙３】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項
定義・用語集
参考文献

「４．対策項目」の詳細
4.1.「Plan（計画）」の観点
4.1.1.「組織の状況」の観点
（１）外部環境及び内部環境の理解
（２）関係主体等の要求事項の理解
4.1.2.「リーダーシップ」の観点
（１）経営層のコミットメント
（２）情報セキュリティ方針の策定
（３）組織の役割に対する責任及び権限の割当
4.1.3.「計画」の観点
（１）情報セキュリティリスクアセスメント
（２）情報セキュリティリスク対応の決定
（３）リスク管理策に係る個別方針の策定
（４）情報セキュリティリスク対応計画の策定
4.1.4.「支援」の観点
（１）資源確保
（２）人材育成及び意識啓発
（３）コミュニケーション
4.2.「Do（実行）」の観点
4.2.1.「運用」の観点
（１）情報セキュリティ対策の導入、運用
（２）重要インフラサービス障害への対応
（３）演習・訓練の実施
4.3.「Check（評価）」の観点
4.3.1.「評価」の観点
（１）モニタリング及び監査
（２）経営層によるレビュー
4.4.「Act（改善）」の観点
4.4.1.「改善」の観点
（１）是正処置及び継続的改善

・ISO/IEC27001（ISMS）のPDCAサイクルを踏まえ、情報セキュリティの対策項目を掲載。また、「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、安全基準等の継続的な改善に取り組む必要性を繰り返し言及。
【ポイント（５）及び（１）】

・4.1.2.を中心として、経営層による積極的な関与が期待される箇所、関わり方を明記。
【ポイント（２）】

・重要インフラサービス障害への対応の際、ＯＴ関連の人材や知識が必要となる可能性について言及。
【ポイント（３）】

「サイバー攻撃リスクの特性並びに対応及び対策の考慮事項」の概要

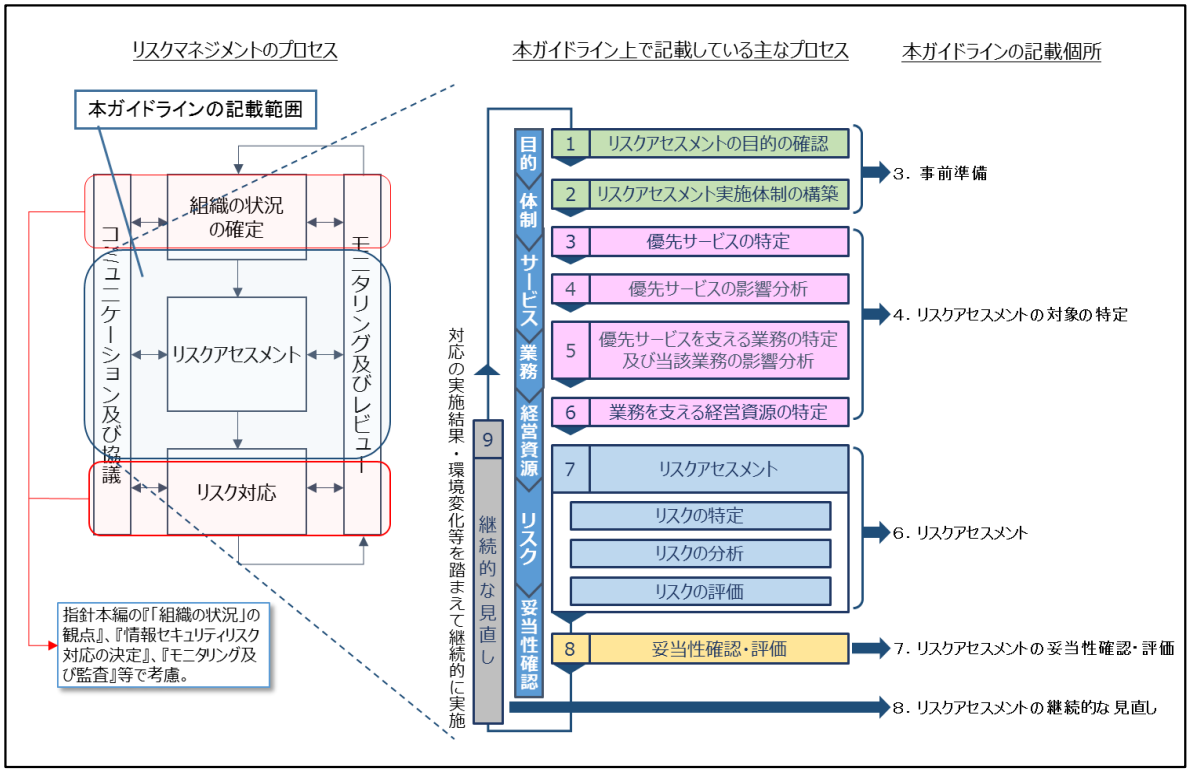
コンティンジェンシープラン（CP）及び事業継続計画（BCP）の策定において踏まえるべき、「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」について、指針本編の【別紙３】に整理した。概要を以下に記す。

	サイバー攻撃リスクの特性	対応及び対策の考慮事項	
		ポイント	概要
1	攻撃者の存在と多様な攻撃目的	サイバー攻撃リスクの認識と被害発生に至るシナリオの作成	・サイバー攻撃は目的を持った攻撃者により行われ、かつその攻撃目的は多様であるため、危惧すべきサイバー攻撃リスクも数多く存在する。そこで、自組織の重要インフラサービス障害に繋がるサイバー攻撃リスクとその影響を特定し、被害発生に至るシナリオとその対応を検討する。
2	攻撃手口の高度化	攻撃手口に関する日々の情報収集並びにＣＰ及びＢＣＰの適時見直し	・サイバー攻撃の手口は絶えず考え出され高度化していることから、攻撃手口等に関して日々情報収集し、新たな攻撃手口に対して現状のＣＰ及びＢＣＰで対応可能か確認し、必要に応じて見直しを図る。
3	急速な被害拡大に繋がる攻撃が行われる可能性	サービス中断に繋がる手段も視野に入れた被害拡大への対応	・サイバー攻撃の被害は自組織内や外部に拡大する可能性がある。被害の拡大防止を優先する場合は、被害拡大の起点（or原因or経路or根源）となる通信の遮断や重要システムの停止等、やむを得ないサービス中断を伴う手段も視野に入れた対応を検討する。
4	執拗な攻撃が行われる可能性	サイバー攻撃の再発の可能性及び環境の特殊性の考慮	・目的達成のため攻撃が繰り返し行われる可能性があることから、サービスの復旧前・復旧中・復旧後の攻撃再発への備えを検討する。また、内部ネットワークに閉じた環境や汎用性の低いシステムで構成される環境でも攻撃の対象になることを認識し、当該環境の制約等を考慮に入れた対応を検討する。
5	同時多発的な攻撃が行われる可能性	関係主体等との連携を前提とした同時多発攻撃への対応	・広範囲を同時に攻撃された場合、優先して復旧すべきサービスの判断及び対処に係る関係主体等との連携が必要となることから、あらかじめ対応の優先順位に係る判断基準を明確化するとともに、早期復旧に向けた関係主体等との対応体制を構築する。
6	検知が困難な攻撃が行われる可能性	影響調査に係る情報等の開示手続きの明確化	・直接検知できなかった攻撃の影響を調査するためには、断片的な様々な痕跡の分析能力が必要となることから、外部のインシデント対応組織やセキュリティベンダーに調査協力を依頼する場合も想定される。その際、ログや侵害された機器等を開示する場合があるため、必要な手続きを明確にしておく。
7	誤った判断や対処を誘発する攻撃が行われる可能性	異なる種類の監視情報の併用による正確な事態把握	・特定の監視手段のみに依存すると、改ざんされた場合に誤った判断や対処を招く可能性が高まることから、監視や制御等の手段を複数用意しておき、対応時は改ざんされている可能性の少ない、信頼できる手段を使用する。

リスクアセスメント・ガイドラインの構成、概要

リスクアセスメント・ガイドラインの全体構成
リスクアセスメントガイドライン（本誌）
1．はじめに（ガイドライン策定の背景・目的や記載範囲について）
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
5．リスク評価方針の策定
6．リスクアセスメント
7．リスクアセスメントの妥当性確認・評価
8．リスクアセスメントの継続的な見直し
付録Ａ．用語の説明
付録Ｂ．参考文献
【別紙１】業務の阻害につながる事象の結果の例
【別紙２】結果を生じ得る事象（脅威）の例
【別紙３】様式集（リスクアセスメントの手順に沿ったワークシート）
【別紙４】リスク源の例

【ガイドラインの記載範囲】



【リスクアセスメント・ガイドラインの概要】

- 重要インフラ事業者等による利活用を目的に、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。上記「ガイドラインの記載範囲」のとおり、リスクアセスメントの主要なプロセスについて記載するとともに、リスクアセスメントの対象を特定するプロセスや、リスクマネジメントに含まれるリスクアセスメント以外のプロセスの一部についても記載。
- 機能保証の考え方に立脚したリスクアセスメントとして、「許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続する」という観点を踏まえた手順を紹介。
- リスクアセスメントの対象とするサービスは、機能保証の観点からサービスの重要度（優先度）を以下のような要素を総合的に勘案した上で特定するプロセスとしている。
  「重要インフラ事業者等が扱うサービスについての、経営上の位置付け、利害関係者からのニーズ・期待、社会的責任（ＣＳＲ）、法制面の要求（コンプライアンス）等」
- リスク源を網羅的に洗い出すことを目的に、事象の結果からリスク源までを演繹的に特定・分析・評価するアプローチを採用。

指針対策編の廃止及び指針本編への取り込みについて

- 指針対策編は、指針本編記載の各項目に対する対策具体例を示した項目集として2010年に初版を策定した（2014年に改定）。
- 当該文書を2010年に新規策定した目的は、指針本編の記載内容の具体性を充実化させることであり、当時は指針本編がその他の国際標準や基準と整合した構成でなかったことから、指針本編に対応した項目集を策定することは有効であったと考える。
- しかし今回の改定により指針本編がISMSをベースとした国際標準と整合した構成になったこと、またCSMSやNISTのサイバーセキュリティフレームワーク等の重要インフラのサイバーセキュリティに関連する標準を取り入れていること、指針対策編の策定当時に比べこれらの標準・基準が整備され充実化していること等から、これらに必要な具体策の情報は各々のドキュメントを参照することで十分に得ることが可能な状況となっている。
- このような背景を踏まえ、指針対策編はこれまでの具体策を列挙する形から、指針本編記載の各項目に対して参照すべき具体策が記載されたドキュメント（およびドキュメント内の該当箇所）を示す形としたい。

＜指針本編への取り込みイメージ＞

【別紙４】 対策の実施例の参照先

対策項目一覧	対策の実施例の参照先
4.「Plan（計画）」の観点	
4.1.「組織の状況」の観点	
（省略）	
4.3.「計画」の観点	
（１）情報セキュリティリスクアセスメント	
（２）情報セキュリティリスク対応の決定	
（ア）人的資源のセキュリティ（外部委託）	
●委託前の対応事項（選定・契約条件）	
●委託期間中の対応事項	
（イ）資産の管理	
●資産に対する責任	・「ISO/IEC 27002:2013」 8.1.1 ～ 8.1.4 ・「情報セキュリティ管理基準（平成２８年改正版）」 8.1.1 ～ 8.1.4 ・「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」 ID.AM-1, ID.AM-2, ID.AM-4
●情報分類と取扱い	・「ISO/IEC 27002:2013」 8.2.1 ～ 8.2.3 ・「情報セキュリティ管理基準（平成２８年改正版）」 8.2.1 ～ 8.2.3 ・「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」 PR.DS-3, PR.IP-6 ・「政府機関等の情報セキュリティ対策のための統一基準群」 第3部 情報の取り扱い
（ウ）アクセス制御	－

・指針本編の「4. 対策項目」の各タイトルを一覧にした上、右側に各対策の具体例が書かれたドキュメント（公的文書）及び該当箇所の番号等を記載する。

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（6/27開催済み）
改定方針の討議

●第２四半期（本会）
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、パブコメでは、「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
（「リスクアセスメント・ガイドライン」も同時に公表）

【参考】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

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」へ統合する方針。

【指針の活用方法】