資料３

NISC National Information Security Center

第３次行動計画下における指針改訂の概要について

2014年10月10日

内閣官房 情報セキュリティセンター（NISC）

指針改訂の概要

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

第3次行動計画の記載事項

【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

「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」

【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

「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」

【具体的な対応】

①PDCAサイクルに沿った対策手法の習得・実現

「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」

②習得・実現に向けた段階的な取組

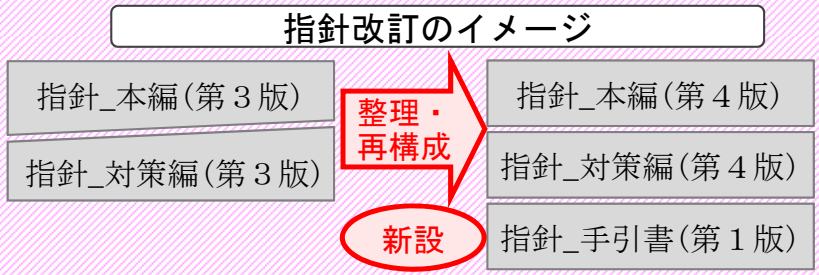
「重要インフラ事業者等が情報セキュリティ対策を実施する際の優先順位付け、対策の段階的な追加及び予防的対策と事後的対策のバランスに係る考え方を成長モデルとして例示する」

③経営層の在り方の訴求

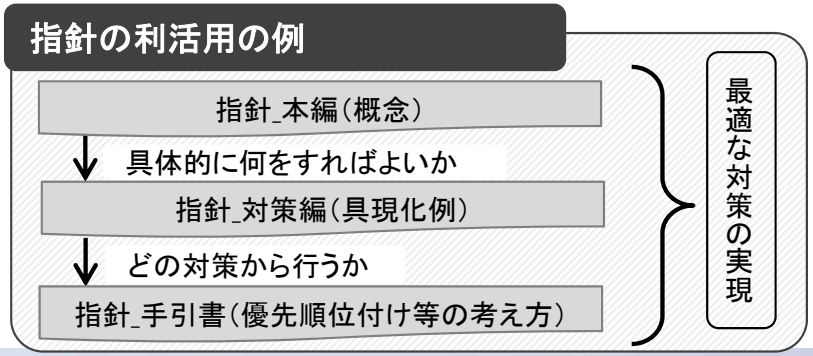
「重要インフラ事業者等における段階的・継続的な対策の強化に不可欠な方針化、規定化、計画化、体制化・人材育成及びシステム構築に係る重要インフラ事業者等の経営層の在り方の重要性を訴求する」

指針改訂のポイント

- ○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
- ○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
- ○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
- ○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
- ○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（併せて、「要検討事項」と「参考事項」の区別を廃止）

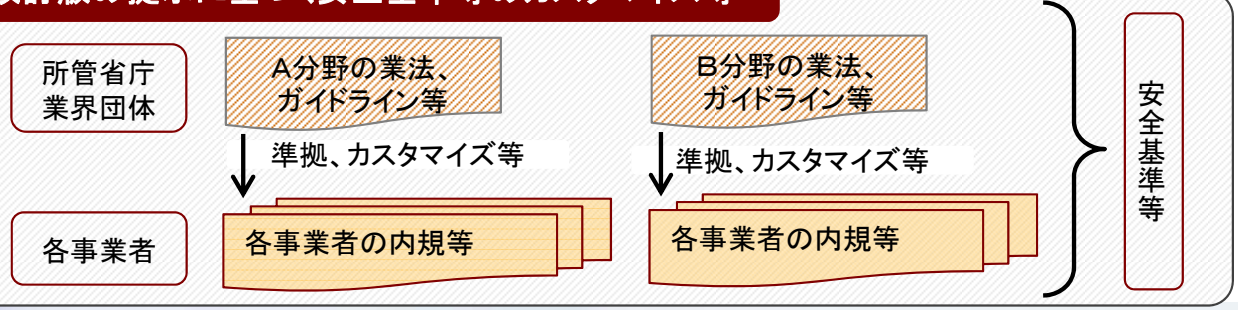


指針の利活用の例



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



指針_本編の改訂案（目次ベースでの新旧比較）

構成（見直し後）	構成（現行）
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 2．「安全基準等」の必要性 3．「安全基準等」とは何か 4．指針の位置付け 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	1．重要インフラにおける情報セキュリティ確保のために 2．「安全基準等」の必要性 3．「安全基準等」とは何か 4．本指針の位置付け 5．本指針の構成 6．本指針を踏まえた「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 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 4．役割 5．「安全基準等」の公開	1．「安全基準等」策定の目的 2．「安全基準等」の対象範囲 3．「安全基準等」の対象とする脅威 4．重要インフラ事業者等の担う役割 5．「安全基準等」の公開
6．対策項目 6．1．「Plan（準備）」の観点 6．2．「Do（実働）」の観点 6．3．「Check（確認）・Act（是正）」の観点	6．対策項目 （1）4つの柱 ア　組織・体制及び資源の確保 イ　情報についての対策 ウ　情報セキュリティ要件の明確化に基づく対策 エ　情報システムについての対策 （2）5つの重点項目 ア　IT障害の観点から見た事業継続性確保のための対策 イ　情報漏えい防止のための対策 ウ　外部委託における情報セキュリティ確保のための対策 エ　IT障害発生時の利用者のための情報の提供等の対策 オ　ITに係る環境変化に伴う脅威のための対策
－－－	Ⅲ．フォローアップ
	1．フォローアップの考え方 2．本指針の継続的改善 3．「安全基準等」の継続的改善 4．「安全基準等」の浸透

目的を重要インフラサービスの持続的な提供に置き、PDCAサイクルの必要性を追記

目的に応じた項目の整理から対策プロセス(PDCA)に応じた整理への変更

第3次行動計画と記載内容が重複するため、削除

指針_対策編の改訂案（目次ベースでの新旧比較）

構成（見直し後）	構成（現行）
Ⅰ. 対策編の位置付け	Ⅰ　本対策編の位置づけ
Ⅱ. 具体的な情報セキュリティ対策項目の例示	Ⅱ　対策項目の具体化の例示
1.「Plan（準備）」の観点	（1）4つの柱
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	ア　組織・体制及び資源の対策 イ　情報についての対策 ウ　情報セキュリティ要件の明確化に基づく対策 エ　情報システムについての対策
2. Do（実働）の観点	（2）5つの重点項目
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	ア　IT障害の観点から見た事業継続性確保のための対策 イ　情報漏えい防止のための対策 ウ　外部委託における情報セキュリティ確保のための対策 エ　IT障害発生時の利用者の対応のための情報の提供等の対策 オ　ITに係る環境変化に伴う脅威のための対策
3.「Check（確認）・Act（是正）」の観点	
3. 1.「平時」の観点 3. 2.「障害発生時」の観点	

対策プロセス(PDCA)に応じた整理に基づき、具体的な対策項目を再配置

指針_手引書新設の概要①

指針_手引書の新設

課　題

〇優先順位付けされた指針の提示要望 （重要インフラにおける「安全基準等の浸透状況等に関する調査」より）

〇重要インフラ事業者等の実効的かつ自主的な取組の促進 （第3次行動計画より）

指針_手引書の新設による解決

ねらい

〇対象 ： 主に対策途上や中小規模の事業者等

〇目的 ： 以下対策項目の解説や取組例を記載し、事業者等毎に最適な情報セキュリティ対策の構築・維持・改善を支援

- 指針_対策編Ⅱ.3『「Check(確認)・Act(是正)」の観点』における課題抽出及びⅡ.1.1.(1)「抽出した課題に基づくリスク評価」の対策項目
- ＊ 優先順位付け等に焦点を当て、防護対策の有効性向上を訴求

具体的には

新設の方向性

〇位置付け ： 行動計画が示す対策例に基づく事例紹介（拘束力はもたせない）

〇記載内容 ： 各事業者等共通の対策の優先順位付けに係る考え方まで

〇記載範囲 ： リスクアセスメント、リスク対応、モニタリング

〇読み方 ： 各事業者等が読みたい箇所からの参照を可能とする

〇用語 ： できるだけ専門用語は使わない

考え方

〇各事業者の既採の手法や個別事情等の尊重

〇各事業者の事業規模、予算、体制等は区々であり、リスクレベルとその対応方法も区々

〇「どのような対策をどの程度で行うか」を組織として定めることの推奨

〇初めて取り組む場合は、「状況の設定」、「リスク評価」、「リスク対応」からの着手を推奨

〇読者は「専門家」ではない可能性への考慮

指針_手引書新設の概要②

指針_手引書の構成（概要）

○Ⅰ章に記載する「目的及び位置付け」において、以下を記載

- ー情報セキュリティ対策の実施及び改善にあたり ⇒ 自身にとって、取り組みやすく効果的な対応を自律的に行うことの訴求
- ー指針手引書の位置付け ⇒ 事業者等毎に最適な情報セキュリティ対策の構築・維持・改善の支援（優先順位付け等に焦点を当て、防護対策の有効性向上を訴求）
- ー指針手引書を活用した各重要インフラ事業者等の取組 ⇒ 初めて取り組む場合の推奨対応、各事業者等が読みたい箇所からの参照

○Ⅱ章にて以下に示す各プロセスの解説、例示を記載

プロセス	対応内容
①状況の設定	・防護すべき対象（情報資産や情報システム等）の特定 ・リスク判定基準の策定及び見直し ・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
②リスクの特定	・脅威や脆弱性等（リスク源）が損害をもたらす可能性がある事象の特定 ・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	・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 ・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	・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	・対応策の決定
⑥モニタリング	・脅威や脆弱性等（リスク源）のリスクにまつわる変化の発見 ・リスク対応の状況確認及び対応結果の有効性評価

先行して対応することが効果的と考えられるプロセス

指針改訂のスケジュール

指針改訂のスケジュール

○2014年度に予定する以下の討議を経て指針を見直し、2015年度から改訂版（第4版）を施行

第1四半期（済）　：　改訂の考え方の提示

第2四半期（本会）　：　指針_本編と指針_対策編の原案提示
指針_手引書の記載内容の方向性（草案）の提示

第3四半期　：　上記原案の修正案提示　→　審議結果を反映した指針_本編をパブリックコメントへ（*）
指針_手引書の原案提示

第4四半期　：　最終案の提示　→　審議結果を反映した指針_本編を政策会議に付議、その後公表
審議結果を反映した指針_対策編と指針_手引書を、指針_本編と同時に公表

＊　今改訂にて指針_本編に概念論を集約したことから、パブリックコメントの対象を指針_本編のみとする
→これまでは概念論が遍在してため、指針_本編と指針_対策編をパブリックコメントの対象としていた

本委員会での取組

	2014年度_第2四半期	2014年度_第3四半期	2014年度_第4四半期	2015年度_第1四半期
指針_本編	原案の討議	パブコメ案の討議	最終案の討議 政策会議への付議	公表／施行
指針_対策編	原案の討議	修正原案の討議	公表案（*）の討議	
指針_手引書	記載内容の方向性の討議 草案の討議	原案の討議	修正案（公表案）（*）の討議	

＊必要に応じて、指針_本編へのパブリックコメントを指針_対策編／手引書にも反映

【参考】指針（本編・対策編・手引書）の位置付け

	位置付け	前版		新版
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 ・情報セキュリティ政策会議にて決定	第2次行動計画 （平成21年2月3日決定） （平成24年4月26日決定）	⇒	第3次行動計画 （2014年5月19日決定）
重要インフラ事業者等の対策の方向性を提示				本改訂の検討対象
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）	・安全基準等に関する基本的な考え方を重要インフラ事業者等に訴求 ・重要インフラ分野に共通する安全基準等で規定が望まれる項目の記載 ・情報セキュリティ政策会議にて決定	指針_本編（第3版） （平成22年5月11日決定） （平成25年2月22日改定）	⇒	指針_本編（第4版）
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	指針_対策編（第3版） （平成22年7月30日決定） （平成25年3月26日改定）	⇒	指針_対策編（第4版）
どの対策から行うか				
指針_手引書 （指針対策編の実現に向けた手引書）	・中小規模の事業者等が主な対象 ・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_手引書（第1版）