資料３

NISC National Information Security Center

第３次行動計画下における指針改訂について

２０１４年６月１９日
内閣官房 情報セキュリティセンター（NISC）

指針改訂について

目指す方向

○事業者等による実効的・自主的な対策
　－特に対策途上や中小規模の事業者等

具体的には

○対策の優先順位付け等、ＰＤＣＡに沿った対策手法の習得・実現
　－習得・実現までの期間は例示する推奨対策などの実施

第３次行動計画からの要件

○ＰＤＣＡサイクルに沿った情報セキュリティ対策の実施
○経営層の在り方の訴求

指針の位置付け

○本編　：・「安全基準等」の必要性の訴求
　　・規程が望まれる対策項目の例示
○対策編：・具体的な対策項目の例示（チェックリスト）

踏　襲

指針改訂のポイント

○既存の対策項目をＰＤＣＡサイクルに沿って再配置
○経営層の在り方について、第３次行動計画の記載内容・図表を転載
○指針_本編には概念論、指針_対策編には具体論となるよう再整理
○優先順位付けの考え方については、成長モデルを手引書（仮称）として例示（「要検討事項」と「参考事項」の区別を廃止）

指針改訂について

成長モデルの例示

【前提】
○情報セキュリティ対策の優先順位は各事業者等において区々

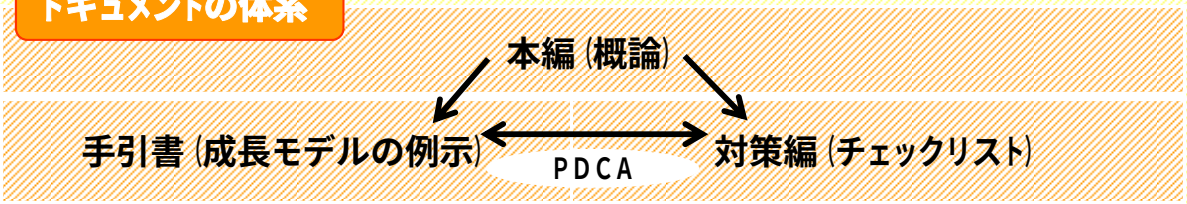
【目的】
○事業者等の優先順位付けに資する資料の提供

【例示内容】
○事業者等における対策の課題抽出から是正に係るプロセスと解説

・リスク源の認識 ⇒ リスク特定 ⇒ リスクレベルの決定 ⇒ 優先順位付け

【例示方法】
○事業者等の対応プロセスに鑑み、成長モデルの例示を手引書（仮称）として新設

ドキュメントの体系



指針改訂のスケジュール

○2014年度に指針の見直し（第4版）を行い、以下予定を経て、2015年度始からの施行を目指す

第1四半期（本会） ： 「改訂の考え方」の提示
第2四半期 ： 原案の提示
第3四半期 ： パブコメ案の提示
第4四半期 ： 公表案の提示（本会→情報セキュリティ政策会議）を経て確定・公表
＊指針_本編に付随する別冊も、上記に沿って実施（第4四半期末に確定・公表）

※これに伴い、安全基準等に係る調査（安全基準等の継続的改善調査及び安全基準等の浸透状況等調査）の見直しは、2014年度対応（現指針に準拠）と2015年度（見直し後の指針に準拠）の2段階で対応

指針改訂のイメージ

本編の改訂（案）

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
（第3次行動計画と記載内容が重複するため、削除）	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

指針改訂のイメージ

対策編の改訂（案）

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	