資料安作24－6

NISC National Information Security Center

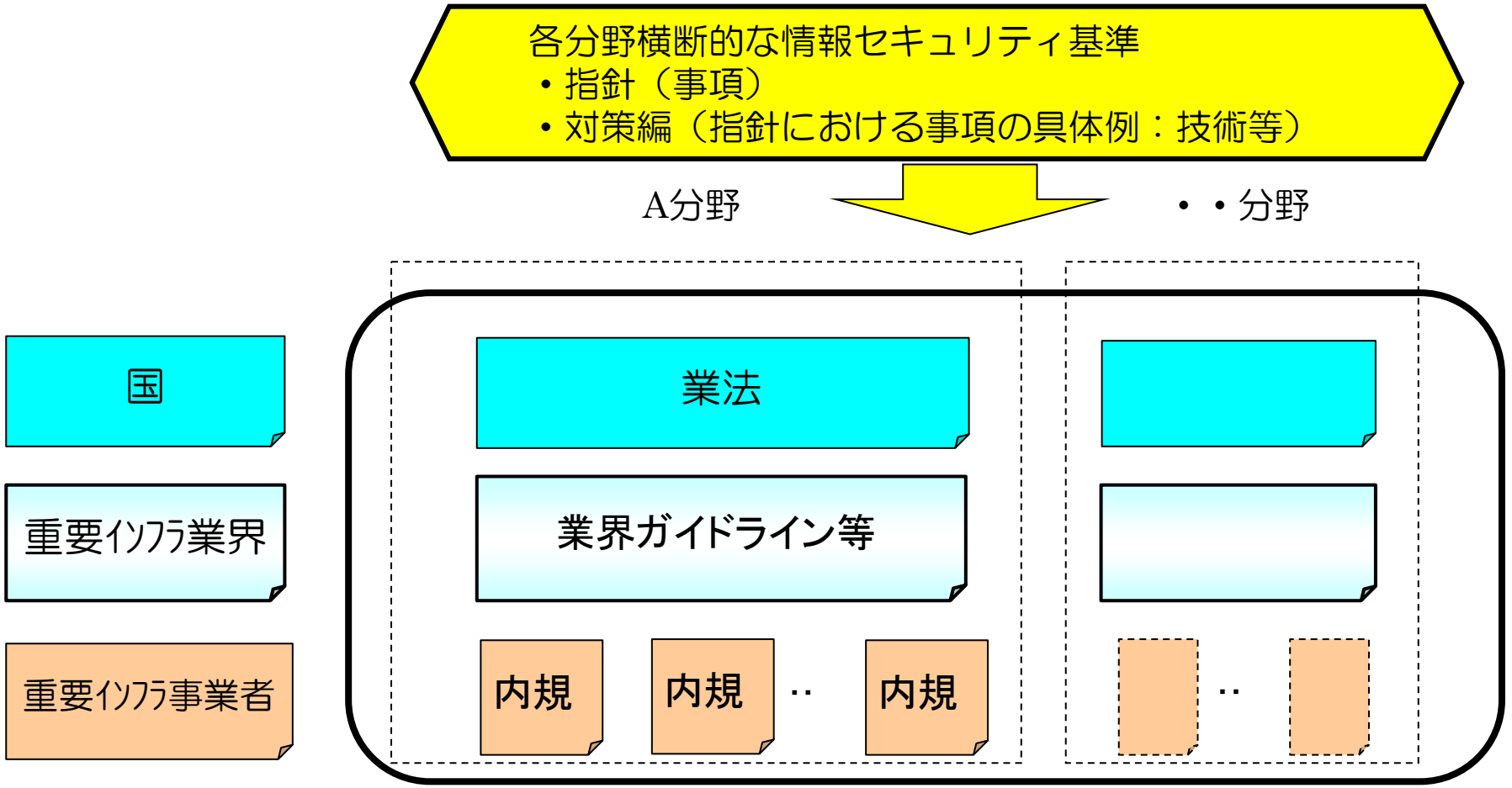
「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」及び「同対策編」について

2012年 9月4日

内閣官房 情報セキュリティセンター（NISC）

1. 指針及び対策編(*)の位置づけ

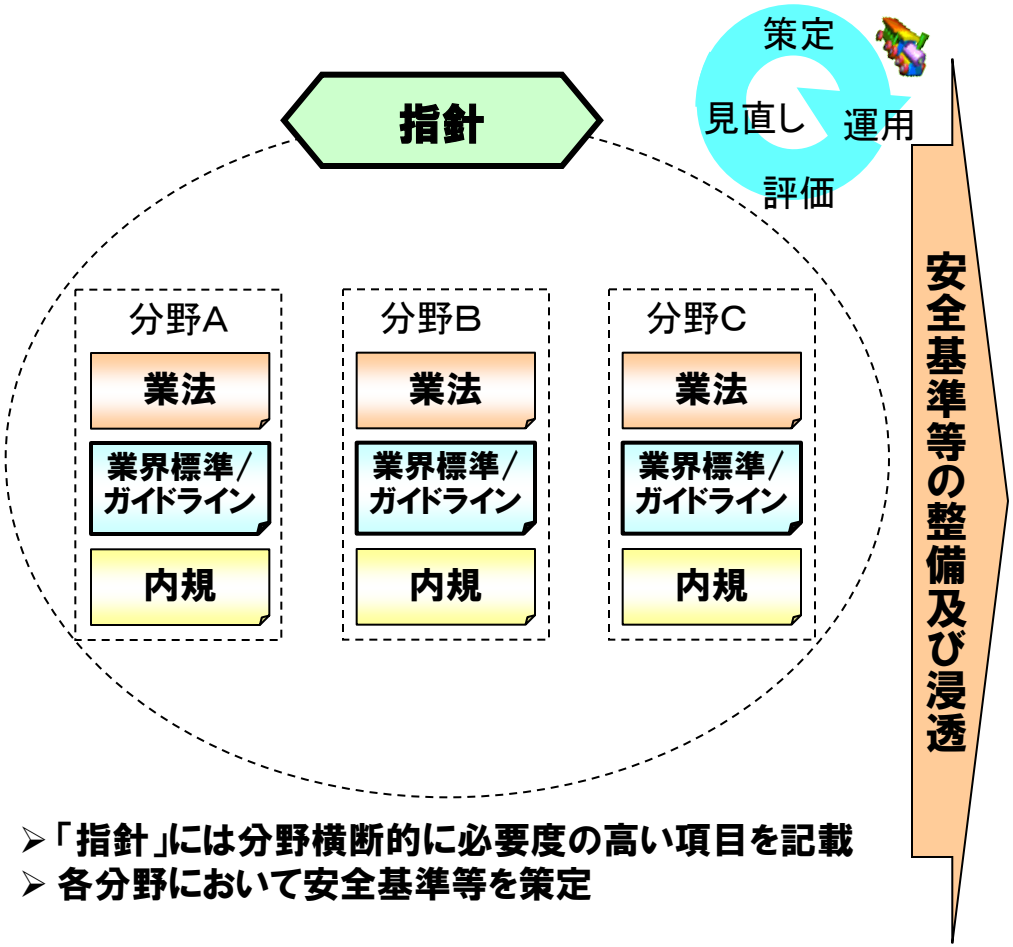
○各重要インフラ事業は、国が定めた安全基準等に従って運用されており、本指針は重要インフラ10分野横断的な情報セキュリティ基準を定めたもの。



(※)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』策定にあたっての指針　第3版(2010.5.11　情報セキュリティ政策会議決定)
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』策定にあたっての指針(第3版)　対策編(2010.7.31　重要インフラ専門委員会決定)

2. 安全基準等の整備及び浸透

○NISCが「指針」を策定し、必要度の高い情報セキュリティ対策を示す
○重要インフラ分野において「指針」を参考に「安全基準等」（業法、業界標準／ガイドライン、内規等）を策定



➢「指針」には分野横断的に必要度の高い項目を記載
➢ 各分野において安全基準等を策定

安全基準等の整備及び浸透

第2次行動計画における取組

（1）指針の継続的改善
➢社会動向等の変化等に対応し、新たな知見を適時反映していくために、指針の分析・検証を1年毎、及び必要に応じて実施
➢指針の改定に関する検討は原則として3年に1度実施

（2）安全基準等の継続的改善
➢ 各分野において安全基準等を見直し、PDCAサイクルを回す
➢ 毎年一定時期に「安全基準等の継続的改善状況等の把握及び検証」を実施し、各分野の改善状況を把握

（3）安全基準等の浸透
➢ 毎年一定時期に「安全基準等の浸透状況等に関する調査」を実施し、対策状況を客観的に把握

3. 指針における対策項目

○指針における対策項目は、4つの柱、5つの重点項目から構成されており、安全基準等の策定にあたっては、これらの項目を盛り込むことが望ましい。

（【要検討事項】は全分野共通の対策が望まれる事項、【参考事項】は、進んだ対策として任意で参考とする事項）

（1）4つの柱

ア　組織・体制及び資源の確保
- （ア）　組織・体制及び人的資源の確保【要検討事項】 例：情報セキュリティ規程・組織体制の整備
- （イ）　情報セキュリティ人材の育成等 【参考事項】 例：人材育成規程等の整備
- （ウ）　外部監査等による情報セキュリティ対策の評価 【参考事項】

イ　情報についての対策
- （ア）　情報の格付け 【要検討事項】 例：情報のライフサイクルと格付けに応じた情報セキュリティ対策
- （イ）　情報の取扱い 【要検討事項】 例：情報の作成・入手、利用、保存、移送、提供、消去における対策

ウ　情報セキュリティ要件の明確化に基づく対策
- （ア）　情報セキュリティ確保のために求められる機能 【要検討事項】 例：主体認証
- （イ）　情報セキュリティについての脅威 【要検討事項】 例：セキュリティホール・不正プログラム対策

エ　情報システムについての対策
- （ア）　施設と環境 【要検討事項】 例：入退出管理、安全区域の確保
- （イ）　電子計算機 【要検討事項】 例：安全区域への設置
- （ウ）　アプリケーションソフトウェア 【要検討事項】 例：情報セキュリティ要件の検討、仕様化
- （エ）　通信回線及び通信回線装置 【要検討事項 例：未承認機器からの通信の遮断

3. 指針における対策項目

(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
- （ア） 事業継続性確保のための個別対策の実施 【要検討事項】 例:指揮命令系統の明確化
- （イ） 事業継続計画との整合性への配慮 【要検討事項】 例:事業継続計画の実施条件の明確化

イ　情報漏えい防止のための対策
- （ア） 保護すべき情報の類型化 【要検討事項】 例:安全管理上の重要度に応じた分類
- （イ） 保護すべき情報の管理 【要検討事項】 例:情報の利用に関する許可及び届出に係る措置
- （ウ） 不正アクセスによる脅威への対策 【要検討事項】 例:取扱者の責任と権限の明確化
- （エ） 内部関係者による脅威への対策 【要検討事項】 例:証跡管理
- （オ） 情報漏えい発生時の対応策の整備 【要検討事項】 例:緊急連絡体制の構築

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
- （ア） 委託先管理の仕組み 【要検討事項】 例:提供する情報の最小化
- （イ） 外部委託実施における情報セキュリティ確保対策の徹底【要検討事項】
- （ウ） IT障害発生時の対応策の整備 【要検討事項】 例:問題発生時の対処の合意

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
- （ア） IT障害による重要インフラサービスの停止等の情報の提供【要検討事項】
- （イ） IT障害防止のための取組みに関する情報の提供 【要検討事項】

オ　ITに係る環境変化に伴う脅威のための対策【要検討事項】 例:平時からの情報収集の実施

【参考】「指針・対策編の見直し」の概要

○2010年度に、**指針の改定（2010年5月）**、**対策編の策定（2010年7月）**を行い、各分野にて安全基準等の見直しが順次行われている

○東日本大震災や標的型サイバー攻撃等の環境変化を受けた第2次行動計画の改定に伴い、**指針・対策編の分析・検証を実施し、必要に応じて改定等の検討を進める**