資料２－１

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対策編の見直しについて

２０１３年１月３１日

内閣官房 情報セキュリティセンター（NISC）

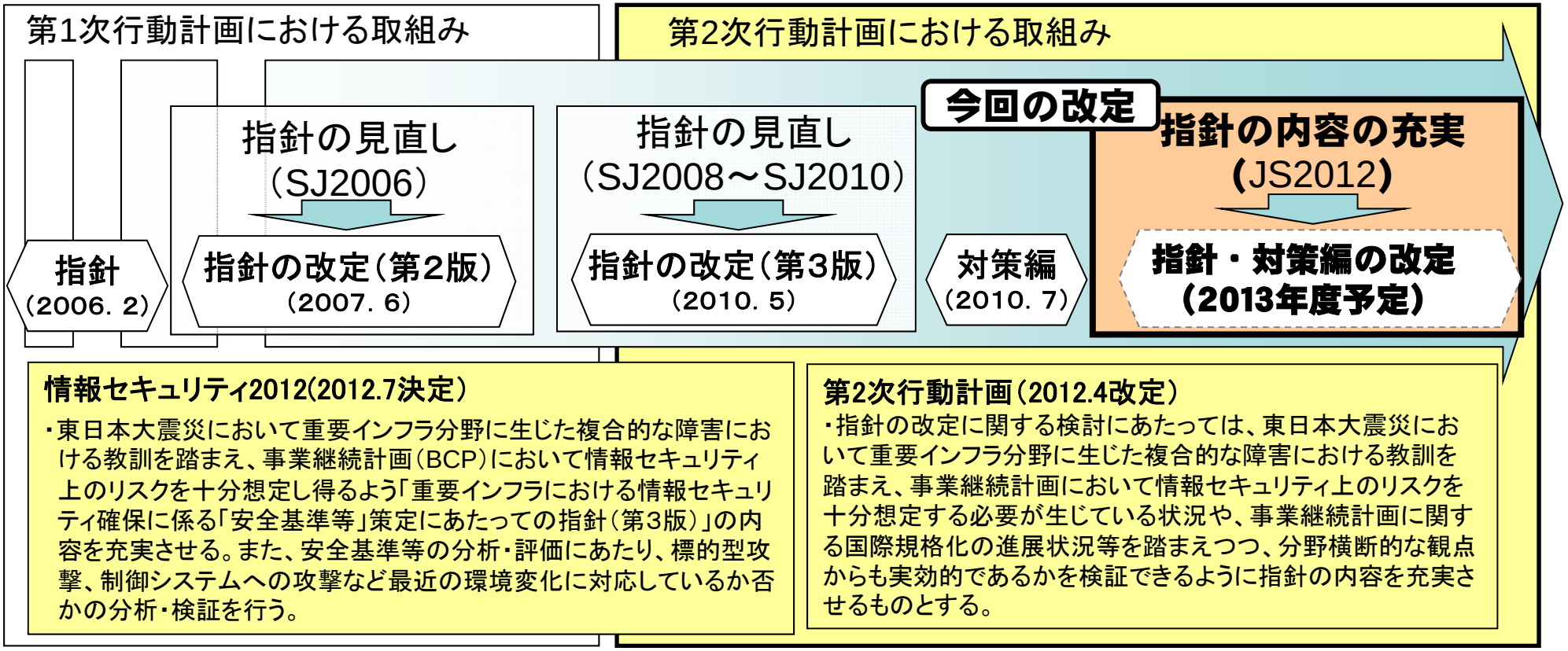
「指針・対策編」の位置付けと見直しの背景

○指針（※1）の位置付け

－重要インフラ分野を横断的に俯瞰して、必要度の高い情報セキュリティ対策を記載したガイドライン（対策編（※2）は、対策項目の具体例を記載）

○見直しの背景

－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（2012年4月）に伴い、指針・対策編を分析・検証し、必要に応じて改定を実施するとされたところ



（※1）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（情報セキュリティ政策会議決定）
（※2）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　対策編（重要インフラ専門委員会決定）

「指針・対策編見直し」の分析・検証における視点と結果（1）

○今回の分析・検証においては、以下の視点から検討が必要な課題を抽出し、対応する対策について、指針・対策編への反映を検討した。

①事業継続計画（BCP）の一層の充実：
「東日本大震災における重要インフラの情報システムに係る対応状況等に関する調査」（2011年度）や複合的障害を想定した「分野横断的演習」（2011年度）での気づき・教訓の反映検討。

【指針へ反映】

（1）広域災害、複合障害を想定した対策、首都直下地震等を想定した対策を進める

【対策編へ反映】

（2）通信が途絶した状態でも、要員の参集や意思決定等の権限委譲が自動的に行われるような緊急時の行動ルールの策定や必要最小限の業務を継続するための準備

（3）通信回線の冗長化対策や通信途絶時を想定した複数の通信手段の準備

（4）災害時の停電に備えて、自家発電装置等で使用する燃料の準備

（5）災害時に代替手段として必要となるシステムの準備

（6）災害時に重要な機能を担う情報システムについて、平時から緊急時の処理増加等を考慮した情報システムの余裕設計の実施

（7）災害時に業界内で相互支援できるように、データ形式の標準化推進

「指針・対策編見直し」の分析・検証における視点と結果（2）

②標的型サイバー攻撃等の環境変化に対する対応：
標的型サイバー攻撃・制御システムへの攻撃への対策について、2011年度の共通脅威分析結果等を検証。

【対策編へ反映】

（1）個人単位のID付与、不要ID削除の徹底、IDごとに異なるパスワードを設定する等の対策を対策編に追記

（2）入口対策として、WAF（ウェブアプリケーションファイアウォール）や迷惑メールフィルターの導入、ウェブにおける脆弱性のある作り込みの回避を対策編に記載

（3）出口対策として、内部から外部への通信制御としてプロキシ経由にする等の対策を対策編に追記

（4）ネットワーク構成等に関する情報の秘匿対策を対策編に記載

（5）モバイル端末のセキュリティ対策として、ワンタイムパスワードや遠隔ロック、遠隔消去等の機能の実装を対策編に追記

（6）インシデント発生時に対応ができる人材の計画的な育成を対策編に記載

（7）グループ会社も含めたセキュリティ対応体制の構築を対策編に追記

（8）業界内、ベンダー等との緊急時及び平常時の連絡体制の整備を対策編に記載

「指針・対策編見直し」の分析・検証における視点と結果（3）

③他基準との平仄合わせ：
政府統一基準群に記載されている対応策について、比較検討。

【対策編へ反映】
（1）事業継続計画と情報セキュリティ対策の整合性確保を対策編に記載
（2）電子メール送信時及び受信時の送信ドメイン認証の導入を対策編に記載
（3）IDごとに異なるパスワードを設定する等の対策を対策編に追記（②（1）に含む）

④その他：
その他の脅威等に対する対策を追加。

【対策編へ反映】
（1）サプライチェーンにおける情報セキュリティを考慮した機器の調達を対策編に記載

（2） 『IPv6移行』に関する継続的な情報収集に加えて、実装検討の実施を追記

今後のスケジュール

○指針は、2月の政策会議で決定予定。対策編は、2～3月頃のパブリックコメントを経て、3月末の重要インフラ専門委員会で決定予定。

○本改定版は、安全基準等の継続的改善の際に活用されることを期待