資料８

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

# 行動計画の見直しについて

平成２８年６月１５日

# 行動計画の見直しに向けた今後の進め方

## ＜今後の議論を深めていきたい論点＞

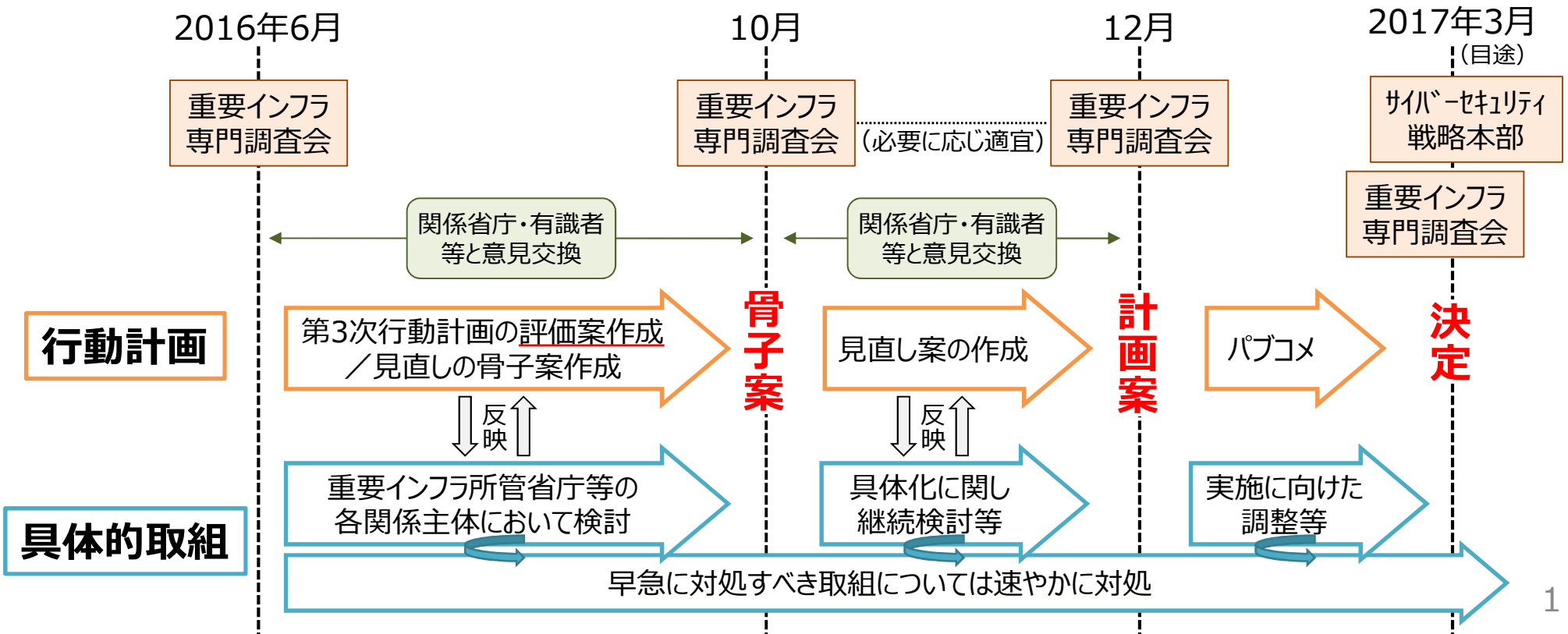
**2020年東京オリンピック・パラリンピック競技大会も見据えて関係主体が一丸となって取り組む**

**○重要インフラとしての機能保証**
＜経営層の取組、リスク評価と対策・対処＞

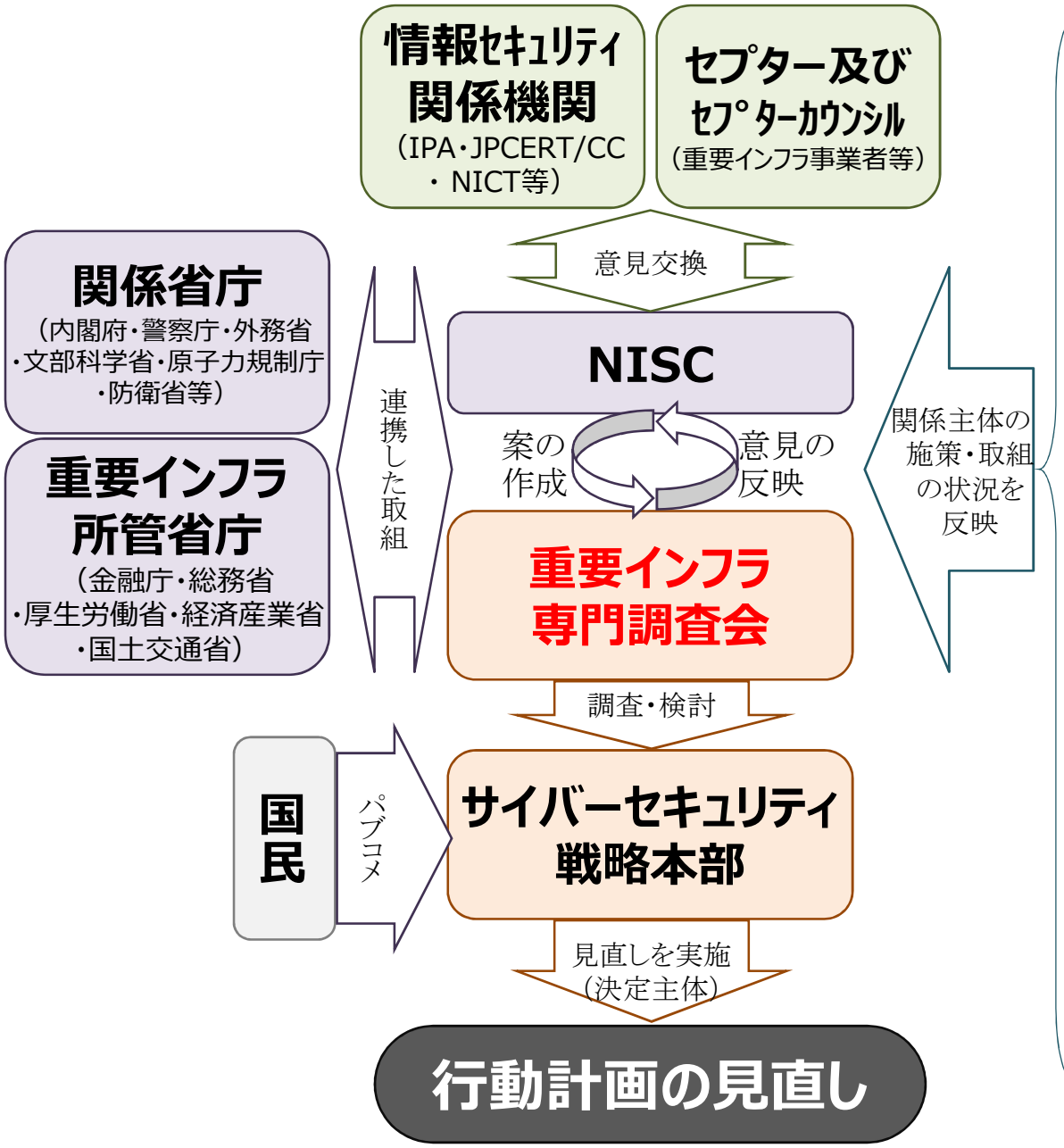
**○情報共有の範囲拡大・深化**
＜面的防護に向け、IoT等環境変化へ対応＞

**法令に基づく安全基準、ガイドライン、報告基準等の見直しの検討**
**＋**
**自主的・自律的取組の促進**

## ＜検討の進め方（予定）＞



# 行動計画の見直しに関する検討体制イメージ




**人材育成総合強化方針【普及啓発・人材育成専門調査会（セキュリティマインドを持った企業経営WG）】**

人材育成総合強化方針(2016.3)※に基づく人材育成の推進

※産学官が連携した人材育成の循環システムの構築のため、求められる人材像の提示、教育の充実、演習環境の整備、資格・評価基準等の能力の可視化、突出した能力を有した人材の発掘・確保を示している。

**戦略的イノベーション創造プログラム（SIP）【内閣府】**

研究開発課題「重要インフラ等におけるサイバーセキュリティの確保」※（FY2015～2019）の実施

※「制御・通信機器と制御ネットワークのセキュリティ対策技術」及び「社会実装向け共通プラットフォームの実現とセキュリティ人材育成」を実施。後者には情報共有プラットフォーム技術が含まれる。

**IoTセキュリティガイドライン【IoT推進コンソーシアム】**

IoTセキュリティガイドライン※のとりまとめ・普及

※関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに、関係者の相互の情報共有を促すための材料を提供。

**サイバーセキュリティ経営ガイドライン【経済産業省】**

サイバーセキュリティ経営ガイドライン(2015.12)※の普及

※ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するために策定

**2020年東京オリンピック・パラリンピック東京大会【推進本部※セキュリティ幹事会】**

**※東京オリンピック競技大会・東京パラリンピック競技大会推進本部**

リスクマネジメントの推進※及び対処体制（CSIRT等）の整備

※大会運営に影響を与える重要サービス事業者の選定や、サイバーセキュリティに係るリスク評価手順の策定を実施予定。

等

# 第３次行動計画の取組概要と見直しに向けた検討事項について

## 第3次行動計画の構成

Ⅰ.総論

Ⅱ.本行動計画の要点
①「重要インフラ防護」の目的
②基本的な考え方
③関係主体の在り方
④重要インフラ事業者等の経営層の在り方

Ⅲ.計画期間内に取り組む情報セキュリティ対策
1. **安全基準等の整備及び浸透**
2. **情報共有体制の強化**
3. **障害対応体制の強化**
4. **リスクマネジメント**
5. **防護基盤の強化**

Ⅳ.関係主体において取り組むべき事項

Ⅴ.評価・検証と見直し

別添：情報連絡・情報提供について
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とサービス維持レベル
別紙３　情報連絡における事象と原因の類型
別紙4-1　情報共有体制（平時）
別紙4-2　情報共有体制（大規模ＩＴ障害対応時）
別紙５　ＩＴ障害発生時における連絡体制等
別紙６　定義・用語集

## 第3次行動計画下での取組概要
（年次報告より）

- サイバーセキュリティ経営ガイドラインを策定（2015.12）
- 安全基準等策定指針の改訂（第４版、2015.5）
- 対応の優先順位付けの考え方を例示した手引書を策定
- 安全基準等の改善状況調査を実施
- 安全基準等の浸透状況調査（アンケート調査及び往訪調査）を実施
- 事業者等からNISCへの情報連絡（FY2015:401件）
- NISCから事業者等への情報提供（FY2015:44件）
- セプター及びセプターカウンシルの運営等の支援
- 分野横断的演習の実施（2015年度:302組織・1,168名）
- セプター訓練（2015年度:18セプター・1,658者）
- CYDER（実践的サイバー防御演習）、CSSCでの制御システムに関する演習など各省個別の演習
- 新規３分野のIT依存度に関する調査を実施（FY2014）
- 外部サービスへの依存性に関する調査を実施（FY2015）
- リスクマネジメントに利活用できる手引書等の整備（2020年東京オリンピック・パラリンピック競技大会をモデルに整備中）
- 重要インフラニュースレター（月２回）の発行や、Webサイト、講演（FY2015:23回）等による広報公聴
- MeridianやIWWNの多国間枠組みや、日ASEAN、日米等での国際連携（キャパシティビルディングを含む）
- 制御機器に関する第三者認証の普及・啓発
- インシデント事例等に対して補完調査を実施

## 見直しに向けた検討事項例
（見直しに向けたロードマップより）

- ✓ 事業者等の取組状況の情報開示推進
- ✓ 各取組を推進する上での事業者等へのインセンティブ付与
- ✓ 業法等に基づく所管省庁への報告体制強化（法令やガイドライン、報告基準の見直し等）
- ✓ 情報共有システムの構築（情報提供元の秘匿化、共通化・自動化の実現、ホットライン構築、分野横断的なデータ分析など）
- ✓ 周辺事業者や中小事業者等への情報共有範囲の拡大
- ✓ 環境変化に対応した情報共有体制
- ✓ 制御系・IoTシステム等の横断的な情報共有体制
- ✓ 知的財産や営業秘密を保持する企業、研究機関、大学等への情報共有体制
- ✓ 事業者等における障害対応能力の検証体制の強化（演習の充実）
- ✓ 内部・外部監査や、ペネトレーションテストの推進
- ✓ リスクマネジメントを支援する資料（手順書、脅威リスト等）の提供や講習会の実施
- ✓ 各セプター等が自主的に行う内外連携（海外ISACとの情報共有等）の支援
- ✓ 分野横断的演習での内外連携の推進
- ✓ 高度な技術や人材育成等のサイバーセキュリティ対策高度化について、事業者等の積極的な取組の促進
- ✓ セキュリティ人材の育成支援、官民人材交流、資格取得等の推進