資料５

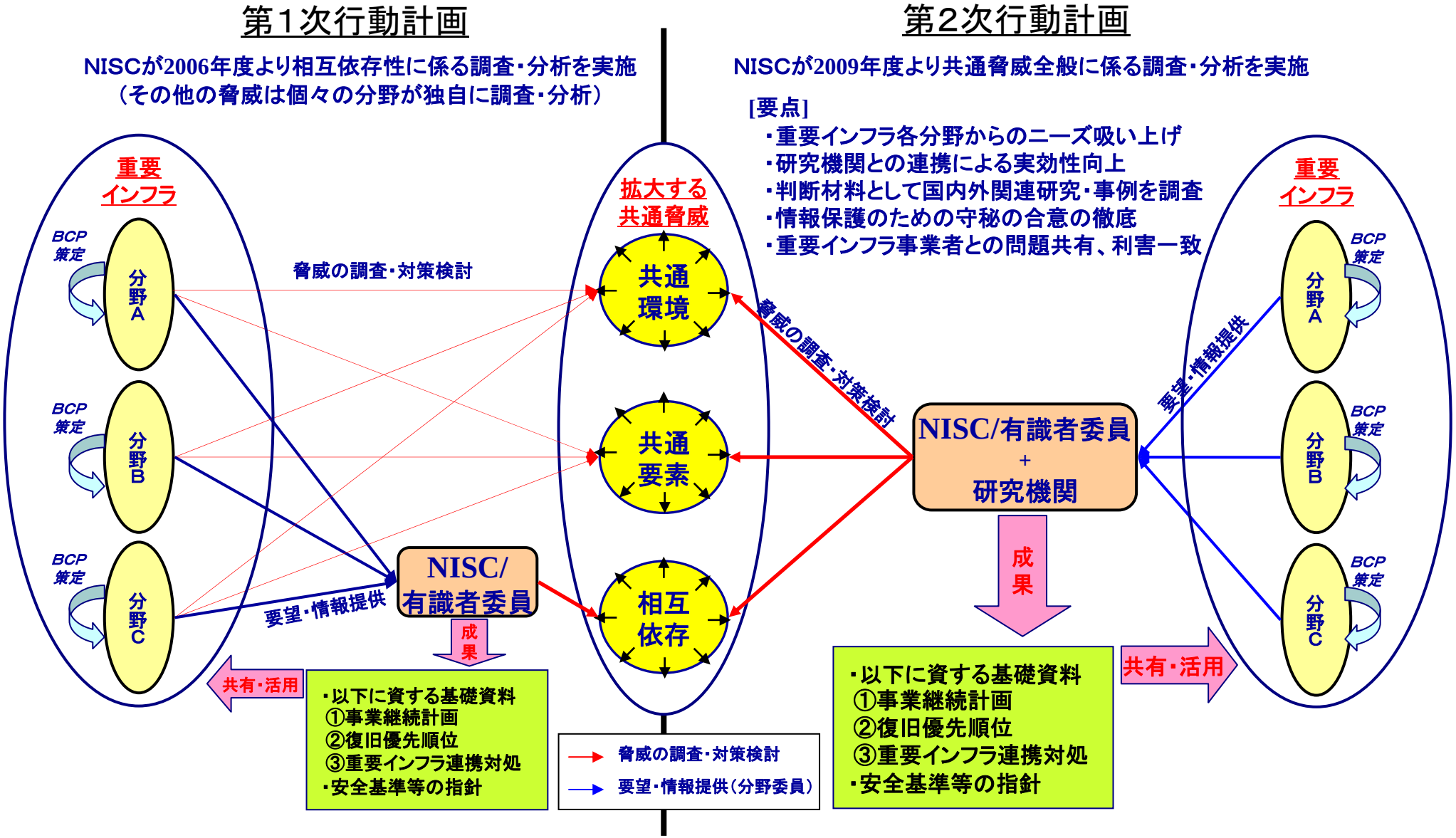
NISC National Information Security Center

2009年度 共通脅威分析について

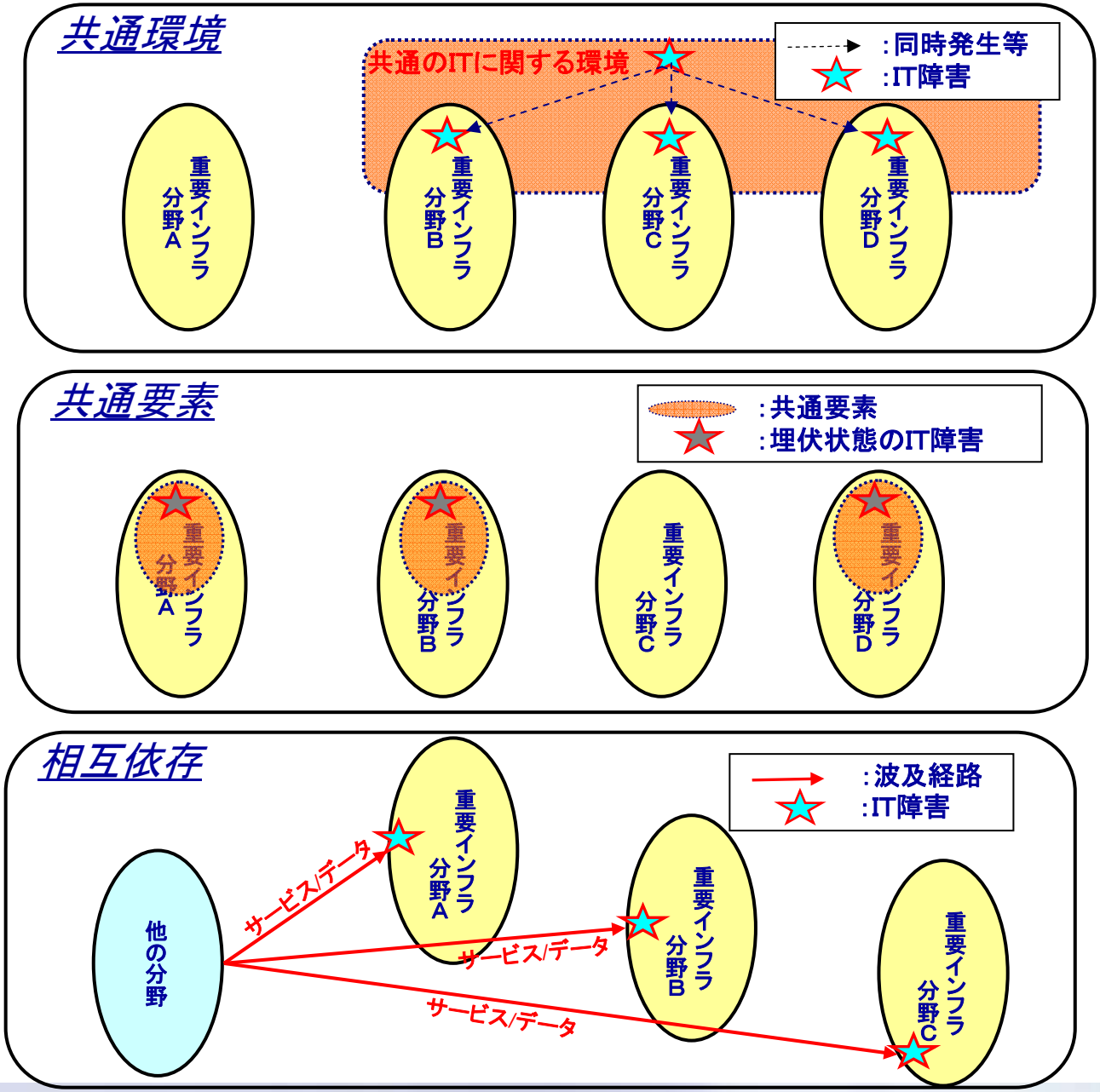
2009年 7月 7日

内閣官房 情報セキュリティセンター（NISC）

第2次行動計画における共通脅威分析の施策



共通脅威のイメージ



重要インフラ分野共通に起こりうるITに関する脅威

想定される例

- ・パンデミック等によるシステムの操作・管理要員不足
- ・経済情勢に伴う予算削減

- ・システムを構成するソフトウェアの脆弱性を突いた攻撃
- ・システムのキャパシティ限界を突いた攻撃や処理要求

- ・他の重要インフラ分野からの
  - *サービス提供の停止・低下
  - *データ送受信に不適切な現象発生
- ・他の重要インフラ以外の分野からの
  - *サービス提供の停止・低下
  - *データ送受信に不適切な現象発生

2009年度の共通脅威分析の目標

第2次行動計画より

第２次行動計画期間においては、第１次行動計画で実施してきた、ある重要インフラ分野にIT障害が生じた場合に他のどの重要インフラ分野に影響が波及するか、という相互依存性解析を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。

このため、従来行ってきた「静的相互依存性解析」や「動的相互依存性解析」の結果を踏まえ、研究機関等との連携を深めつつ、内閣官房、重要インフラ所管省庁、重要インフラ事業者等が協力して活動を進める。

2009年度の目標

第2次行動計画の初年度の取組みとして、以下を目標とする。

1. 重要インフラ分野におけるITに係る脅威の抽出・分類

2. 本活動に協力可能な研究機関の把握と、それら研究機関との連携の準備

3. 重要インフラの事業継続計画策定等に資することを目的とする共通脅威の調査・分析の実施

2009年度の共通脅威分析各目標の活動内容

1. 重要インフラ分野におけるITに係る脅威の抽出・分類

① 重要インフラ事業者等へのアンケート調査と集計結果の分析等を行い、脅威の対象範囲や、重要インフラ事業者等の抱える課題を抽出・分類する。
② 国内のIT障害事例を把握し、共通脅威分析の方向付け等に資する情報を蓄積する。

2. 協力可能な研究機関の把握と連携準備

研究機関や研究者へのアンケート調査等により、調査・分析に必要な情報や専門的な意見の提供が可能な、あるいは、近い将来共通脅威分析の業務の一端を担うことが可能な連携先を把握し、連携の打診等を行う。

3. 優先度の高い共通脅威の調査・分析

① 1. で抽出・分類した脅威より、優先度の高い共通脅威を選定し、実態、背景、原因などを分析して、各課題の特徴や有効な対策等を把握する。
② 共通脅威全般に関する国内外の研究・調査の動向を把握し、共通脅威分析の方向付けや新たな共通脅威の発見等に資する情報を蓄積する。
③ 平成20年度の相互依存性解析で作成した分野間のデータ送受信に係る分析ワークシートをブラッシュアップし、重要インフラ事業者等の運用に資するよう実用性の向上を図る。

2009年度共通脅威分析の全体スケジュール（案）