参考資料２

NISC National Information Security Center

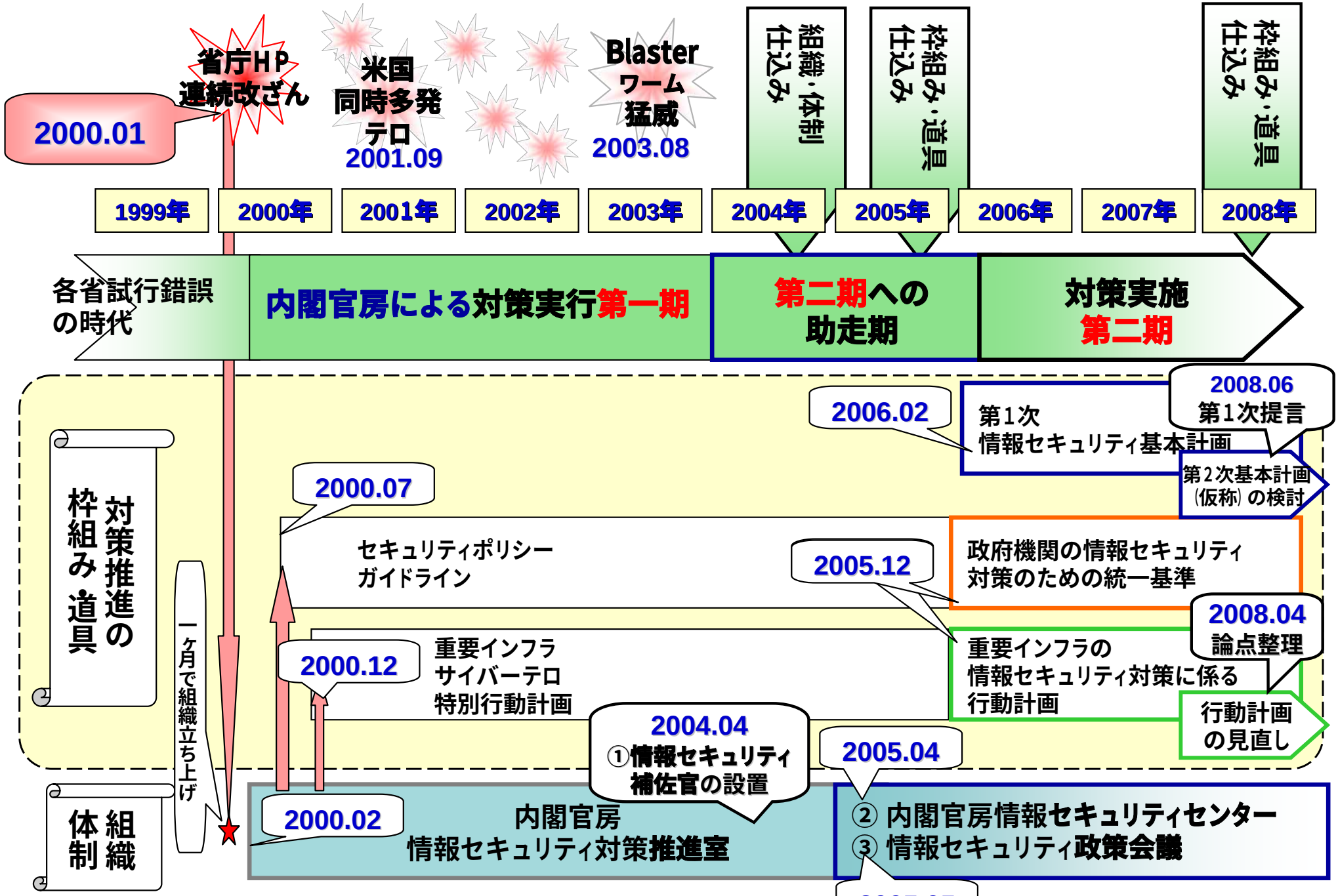
「重要インフラの情報セキュリティ対策に係る行動計画」の見直し
(事務局案説明資料)

見直しの背景と進め方

2008年 10月8日

内閣官房 情報セキュリティセンター
（NISC）

内閣官房における情報セキュリティ政策の流れ



重要インフラの情報セキュリティ施策　4つの柱

○ 我が国の**重要インフラ**（10分野；情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）　横断的な情報セキュリティ水準の向上を図るための「個別設計図」として、**「重要インフラの情報セキュリティ対策に係る行動計画」**を策定

○ 1）サイバー攻撃のみならず、2）非意図的要因、3）災害に起因する、「ITの機能不全が引き起こすサービスの停止や機能の低下等」（**IT障害**）**から重要インフラを防護**

行動計画によって構築される4つの柱

平時からの対策の強化

解析結果を反映

①安全基準等

重要インフラ事業者が情報セキュリティ対策を自己検証するための基準

③相互依存性解析

分野A　分野B　分野C

分野に起こりうる脅威、IT障害の他分野への波及を解明

④分野横断的演習

重要インフラ連絡協議会

情報共有・分析機能　情報共有・分析機能　情報共有・分析機能

②情報共有体制

政府

情報の流れ

相互依存性解析等に基づき行動計画の実効性を検証

IT障害に関する情報を、官民連携して適切に共有

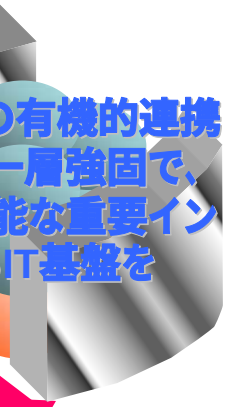
総合的な検証と改善

IT障害発生時の対処能力の強化

サイバー攻撃

非意図的要因によるIT障害

災害に起因するIT障害



4つの施策の有機的連携により、より一層強固で、真に依存可能な重要インフラにおけるIT基盤を実現

毎年のスパイラルアップ

運用　見直し　策定・導入　評価

【現状認識】
- IT障害に係る脅威の特性等を踏まえ、重要インフラ対策の基本理念、求められる対策に関する共通認識を醸成するアプローチの重要性
- 想定脅威の拡大、大規模かつ広範な領域に大きな影響を与える可能性のある事象への対応強化の必要性
- 連絡・連携や情報共有の枠組みで、分野横断的な情報セキュリティ対策強化の必要性

これまでの重要インフラの情報セキュリティ施策の実績

4本の施策の柱	これまでの実績		参考資料（別冊）
①「安全基準等」の整備	06	・全10分野において安全基準等を策定 ・安全基準等の策定状況の把握・評価を実施 ・指針見直しを実施し、指針の改定	・安全基準等の見直し状況等の把握及び検証について ・安全基準等の浸透状況等に関する調査について ・指針見直しを通じて得られた参考事項（要点）
	07	・全10分野において安全基準等の見直しを実施 ・安全基準等の策定状況の把握及び検証を実施 ・安全基準等の浸透状況等に関する調査の実施 ・指針見直しを実施し、要点を参考資料として周知	
②情報共有体制の強化	06	・7分野においてCEPTOARを整備 ・CEPTOAR特性把握マップを作成 ・CEPTOAR-Councilの設置に向けた検討の場の設置・開催（～07）	・情報共有・分析機能の整備について ・「重要インフラ連絡協議会」（CEPTOAR-Council）（仮称）創設に向けた検討状況について
	07	・3分野（水道、医療、及び物流）において、CEPTOARを整備 ・CEPTOAR特性把握マップ(ver2)を作成 ・CEPTOAR-Councilの創設についての基本的な考え方をとりまとめ	
③相互依存性解析の実施	06	・静的相互依存性解析を実施	・2007年度相互依存性解析について
	07	・動的相互依存性解析を実施 ・「相互依存性解析報告書」のとりまとめ	
④分野横断的な演習の実施	06	・「研究的演習」を実施 ・会議形式での課題討議を行う机上演習を実施	・2007年度分野横断的演習について
	07	・分野横断的な機能演習を実施 ・「2007年度分野横断的演習報告書」のとりまとめ	
（政策評価）	06	・目標に対する実施状況の把握を実施	・2006年度の情報セキュリティ政策の評価等 ・2007年度の情報セキュリティ政策の評価等
	07	・目標に対する実施状況の把握に加え、補完調査を実施	

重要インフラの情報セキュリティ対策に関わる主体

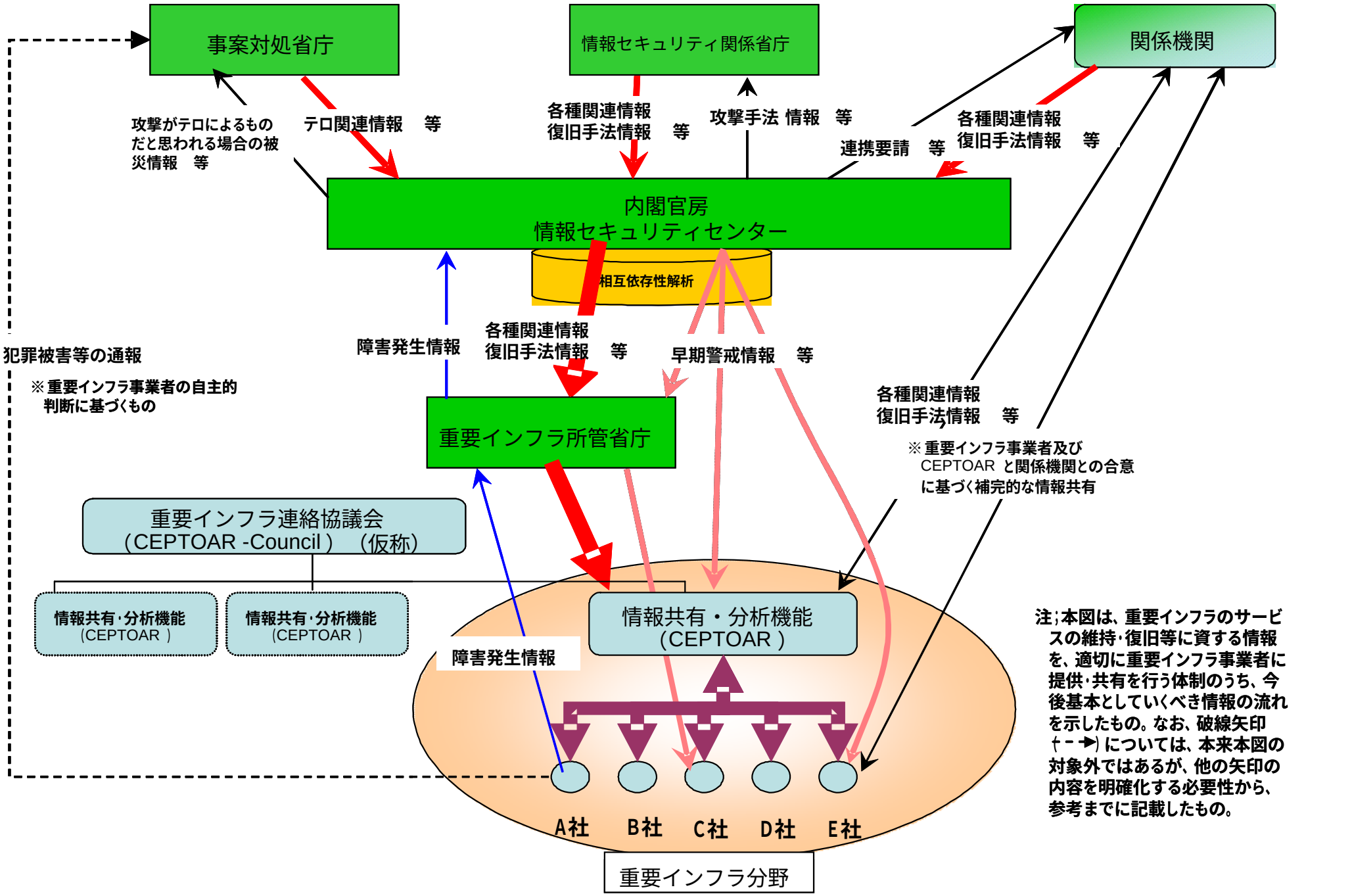
情報セキュリティ政策会議
重要インフラ専門委員会

安全基準等の策定	**重要インフラ所管省庁** **各分野における安全基準等策定主体** **重要インフラ事業者等**
情報共有体制の強化	**重要インフラ所管省庁** **情報セキュリティ関係省庁（※1）** **関係機関（※2）** **事案対処省庁（※3）** **内閣府** **CEPTOAR** **重要インフラ事業者等** **（重要インフラ連絡協議会（CEPTOAR-Council（仮称））**
相互依存性解析 **分野横断的な演習の実施**	**重要インフラ所管省庁** **CEPTOAR** **重要インフラ事業者等**

内閣官房情報セキュリティセンター

※1：警察庁、防衛省、総務省、経済産業省
※2：警察庁サイバーフォース、NICT、IPA、Telecom-ISAC Japan、JPCERT/CC等
※3：警察庁、防衛省、消防庁、海上保安庁等

重要インフラの情報セキュリティ対策に関わる主体（情報共有体制）



注；本図は、重要インフラのサービスの維持･復旧等に資する情報を、適切に重要インフラ事業者に提供･共有を行う体制のうち、今後基本としていくべき情報の流れを示したもの。なお、破線矢印（←－→）については、本来本図の対象外ではあるが、他の矢印の内容を明確化する必要性から、参考までに記載したもの。

議論の前提（1）

○ 行動計画の見直しに関係する文書

- 「第1次情報セキュリティ基本計画」
  （2006年2月2日　情報セキュリティ政策会議決定）
- 「重要インフラの情報セキュリティ対策に係る行動計画」
  （2005年12月13日　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」
  （2006年2月2日　情報セキュリティ政策会議決定、2007年6月14日改定）
- 「『重要インフラの情報セキュリティ対策に係る行動計画』見直しにあたっての論点整理」
  （2008年4月3日　重要インフラ専門委員会）
- これまでの重要インフラの情報セキュリティ施策の実績（p３参照）　　等

⇒　上記資料を綴った参考資料（別冊）を席上配布（適宜参照のこと）

議論の前提（2）

○ 用語の定義等　（現行動計画による）

- 重要インフラ
  - 他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの
- 重要インフラ事業者等
  - 「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」の各分野に属する事業を営む者のうち、別紙1の「対象となる事業者」に指定された者及びこれらの者から構成される団体
- IT障害
  - 重要インフラの各事業において発生する障害（サービスの停止や機能の低下等）のうちITの機能不全が引き起こすもの
- IT障害に関する情報
  - 未然防止・・・障害発生の脅威に係る情報（防護方策等を含む）
  - 拡大防止・復旧・・・障害発生後の影響伝搬予測及び復旧に資する情報
  - 再発防止・・・事後分析に資する情報の共同収集及び分析・検証の結果
- IT障害への脅威（一般的な定義はないが、例示がある。）
  - サイバー攻撃によるIT障害への脅威
  - 非意図的要因によるIT障害への脅威
  - 災害によるIT障害への脅威
- 各分野別重要システム（一般的な定義はないが、例示がある。）

現行動計画の構成と論点整理の関係

現行動計画における項目	論点整理であげられた項目	
1 目的と範囲 2 重要インフラの定義と対象 別紙1 各重要インフラ分野において対象となる重要システム等	4-2 行動計画の基本的枠組みに関する事項	4-1 本委員会での議論等を通じて認識された課題
3 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」	4-3 安全基準等の整備	
4 情報共有体制の強化 別紙2 IT障害発生時における連絡体制等 別紙3-1 (今後基本としていくべき情報の流れ) 別紙3-2 情報連絡の対象となるIT障害(サイバー攻撃の場合) 別紙3-3 情報連絡の対象となるIT障害(非意図的要因の場合) 別紙3-4 情報連絡の対象となるIT障害 (災害の場合)	4-4 情報共有体制の強化	
5 相互依存性解析 6 分野横断的な演習	4-5 相互依存性解析・分野横断的演習	
7 各主体において取り組むべき事項と横断的施策 8 行動計画の推進体制	4-6 その他	

検討の進め方（案）

○ 「『重要インフラの情報セキュリティ対策に係る行動計画』見直しにあたっての論点整理」で示された各論点にについて、個別施策から順次検討を実施
○ 検討結果を踏まえて、必要に応じて現行動計画の記載を見直す

1. 現行動計画における目的を仮の前提として検討に着手。論点整理「4-1　本委員会の議論等を通じて認識された課題」を念頭におきつつ検討の進め方を確認する
2. 「4-2 行動計画の基本的枠組みに関する事項」の論点について議論
3. 「4-3 安全基準等の整備」「4-4 情報共有体制の強化」「4-5 相互依存性解析・分野横断的演習」の各論点について、これまでの取組みを踏まえて議論
4. 上記3.の議論や基本計画検討委員会での検討状況を踏まえて、「4-1　本委員会の議論等を通じて認識された課題」について今後採るべき方向性の絞込みを行うとともに、ここまでの検討を総括した上で新たな政策目標を検討し、次期行動計画の素案を作成。また、この政策目標に照らして記述ぶりを再整理
5. 「4-6 その他」及び積み残された論点について、1.～4.の検討状況を踏まえた議論を行い、行動計画の記述の見直しを実施
6. 全体を総括した上で、必要に応じて「重要インフラにおけるIT障害の発生を限りなくゼロ」に替わる新たな基本理念を検討し、次期行動計画の最終案を作成
7. （以降パブリックコメントを経て、情報セキュリティ政策会議で次期行動計画を決定）

専門委員会の開催日程（案）

専門委員会 第17回 → 専門委員会 第18回 → 専門委員会 第19回 → 専門委員会 第20回 → 専門委員会 第21回 → 専門委員会 第22回

情報セキュリティ政策会議（12月中旬）

6/4（水）	7/18（金）	7/24（木）	9/12（金）	10/8（水）	11/12（水）
1.検討の進め方 2.基本的枠組み	2.基本的枠組み（続き） 3.施策毎の論点 ・安全基準等の整備 ・情報共有体制の強化 ・分野横断的演習・相互依存性解析		4.その他の論点 5.方向性の絞り込み ・新たな政策目標 ・全体の整合	（記述見直し）	6.最終案 ・新たな基本理念

素案 → 最終案 → パブコメ案

基本計画検討委員会

第1次提言
パブコメ
（6/19～7/18）

第2次情報セキュリティ基本計画を策定（数回程度開催）

パブコメ案（基本計画）

論点整理にて明らかになった基本的スタンス・視点

○ 論点整理の取りまとめにおいて明らかとなった以下の状況認識に立ちつつ、行動計画見直しの議論を進める必要がある

論点整理「2. これまでの取組みと成果」より

○2-4 **総括（行動計画の進捗状況）**

重要インフラにおいては、以上のとおり２００５年１２月の現行動計画策定以降、それぞれの分野及び主体において情報セキュリティ対策の向上に向けた取組みがなされてきた。また、２００８年度においても、別表のとおり各施策に取り組まれることとなっており、**現行動計画に位置づけられた各取組みは、着実に進捗している。**

その結果、個々の重要インフラ事業者等による情報セキュリティ対策については、着実に向上していることが確認できているが、一方で、**情報共有体制の有効活用という課題もまだ残っている**（「2006年度の情報セキュリティ政策の評価等」及び「2007年度の情報セキュリティ政策の評価等」参照）

論点整理「3. 行動計画見直しに際しての基本的スタンス・視点」より

○**実態を把握した上で現実の具体的な経緯に即した課題の検証を行い、実社会における影響を踏まえた実効性のある内容となるように注意する。その際、技術的視点に偏らないよう留意するとともに、利用者の視点も意識して検討を行う。**

○**重要インフラ事業者等の自主的な取組みが大原則であることを踏まえつつ、官民の役割・責任の適切な分担の下で重要インフラにおける情報セキュリティ対策が着実に向上するための枠組みについて検討を行う。**

行動計画の目的をどこまで具体化するか

○ 行動計画の見直しの議論を通じて、目的をどの程度まで具体化するか（また具体化すべきでないか）を常に意識しておく必要があるのではないか

○ 現行動計画の目的について

- 「サービスの維持」に対して、対象とするサービスとは何か
  - システムは例示されたが、サービスの範囲と水準は例示されていない
  - 行動計画の対象とすべきサービスの範囲はどこまでか
  - サービスがどの水準以下になれば維持できていないと認められるか
- 「IT障害発生時の迅速な復旧等の確保」に対して、想定すべきIT障害は何か
  - 脅威は例示されたが、官民で連携すべきIT障害は例示されていない
  - IT障害に対処すれば十分か、IT障害に至らない段階の脅威にも対処すべきか
  - 例示された脅威は一様に対応が必要か、優先順位をつけるべきか

現行動計画「1 目的と範囲」より（抜粋）

・重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図るため、内閣官房を中心とした政府及び各重要インフラ分野において実施することが望ましい施策を既存の法令、防災計画等の枠組み等との整合を図りつつ具体化

行動計画の基調となる方向性をどのように設定するか

○ 行動計画の見直しのとりまとめに際して、最終的に以下の点についてとるべき方向性を示せるよう、個別の論点の検討を行う （論点整理 4-1 本委員会の議論等を通じて認識された課題）

○各重要インフラ分野において、ITへの依存度（ITの機能不全とサービス低下の距離感）、ITの観点での他分野との相互依存性などは様々である。それに応じた各分野における取組みにも多様性が存在する。

→ 全分野・全事業者に一律の対策を求め平均を底上げするか、個別の進んだ対策を伸ばすか

○情報セキュリティ対策を考える際には、経営（コスト配分・サービスの維持レベルなど）やコンプライアンス、内部統制の視点も踏まえるべき要素の一つである。

→ 対策の対象はITのみに限定するか、ITを含めた経営全体か

○重要インフラ事業者等の立場から見ると、「個々の利用者（顧客）」へのサービス提供と「公益」の観点から求められる対応の2つの側面があり、両者は必ずしも常に一致するものではない。

→ 事業者等の自発的な取組みに重点をおくか、社会的要請に基づく取組みに重点をおくか

○IT障害から重要インフラを防護する観点からは、障害の未然防止だけでなく、障害発生時に影響を最小限に抑えるための対応（早期対応、応急対応など）も重要である。

→ 緊急時対応を国や他事業者と連携して行うのか、事業者独自の取組みに任せるのか

○個々の重要インフラ事業者等による情報セキュリティ対策については向上が進んでいるものと考えられるが、障害（リスク）の発生時の情報や、「経験」から得られる知見の共有については、今後の一層の取組みについて、検討を進めるべきである。

→ どのような知見を共有対象とすべきか
IT障害に至らない事象（ヒヤリ・ハット等）も重視すべきではないか