

# 「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」の見直しについて

---

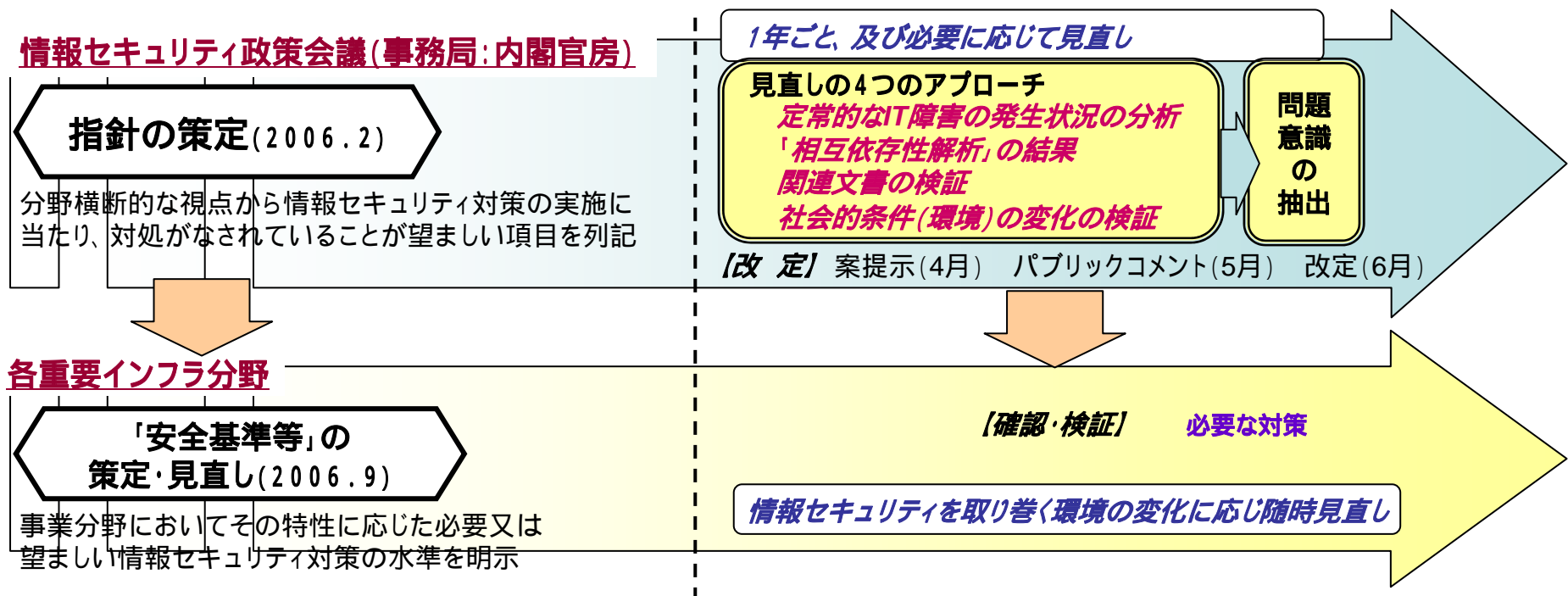
2007年4月23日

内閣官房情報セキュリティセンター (NISC)

# 指針の見直しの基本的スタンス

指針の目的・位置づけ等をふまえ、4つのアプローチより抽出された論点から問題意識を整理し、改定を検討

- 「安全基準等」策定にあたっての指針(以下「指針」)は、重要インフラ分野における安全基準等の策定・改定を支援することを目的として2006年2月に策定。
- 「指針」の策定に当たっては、各重要インフラ分野において、**2006年9月を目処に「安全基準等」の策定・見直し**がなされることを前提に、「安全基準等」において何らかの対処がなされていることが望ましい項目を列記。
- 今回フォローアップとして「指針」の見直しを行うにあたっては、まず以下の4つのアプローチにより分析・検証を行い、情報セキュリティ対策に関する「問題意識」を抽出。
- 抽出した「問題意識」について、現在の「指針」と照らし合わせ必要な改定を行い、**各重要インフラ分野の「安全基準等」における対策の状況や今後の方針を確認・検証**。



# 見直しの4つのアプローチ

指針見直しの観点として、以下4つのアプローチにて状況検証を実施

## セキュア・ジャパン 2006

(2006年6月15日情報セキュリティ政策会議決定)

### 【具体的施策】

ア)各重要インフラ分野の安全基準等の策定・見直し

(重要インフラ所管省庁)

イ)「安全基準等」の策定状況の把握及び評価

(内閣官房)

ウ)指針の見直し  
(内閣官房)

### 「指針」の見直しの方向性

- ◆「安全基準等」の把握等を通じて、重要インフラ分野に共通的な要検討事項が新たに導き出されるのではないか
- ◆「相互依存性解析」の知見をふまえ、「指針」の見直しにどのように活用するか
- ◆「指針」や「セキュア・ジャパン2006」の記載内容から導き出される方策以外に「指針」の見直しに資する事項はないか

(指針より)

・内閣官房は、1年ごと、及び必要に応じて適時に、本指針の見直しを推進する

・内閣官房は定常的なIT障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行い、本指針改定のための基礎資料として整備する

・(前略)内閣官房が各重要インフラ所管省庁及び重要インフラ事業者等の協力を得て相互依存性解析を実施する際には、その結果を本指針や各重要インフラ分野における「安全基準等」の見直しの基礎資料として提供する

(「セキュア・ジャパン2006」より)

政府機関統一基準、その他関連文書を参照しつつ、各重要インフラ所管省庁の協力を得て、2006年度中を目処に指針の見直しを実施する



「指針」の目的である「安全基準等の策定・改定を支援」に資するため、各分野に共通する横断的な対策課題の分析・検討を行うことが必要ではないか

### 見直しの4つのアプローチ

定常的なIT障害の発生状況の分析

・各重要インフラ分野に共通する横断的な対策課題の分析・検討の結果、情報セキュリティ対策の新たな観点が発見されたか

「相互依存性解析」の結果

・相互依存性解析の結果を基礎資料にして、新たな「何らかの対処がなされていることが望ましい項目」をどのように活用できるか **本年度は見直しに至らず**

関連文書の検証

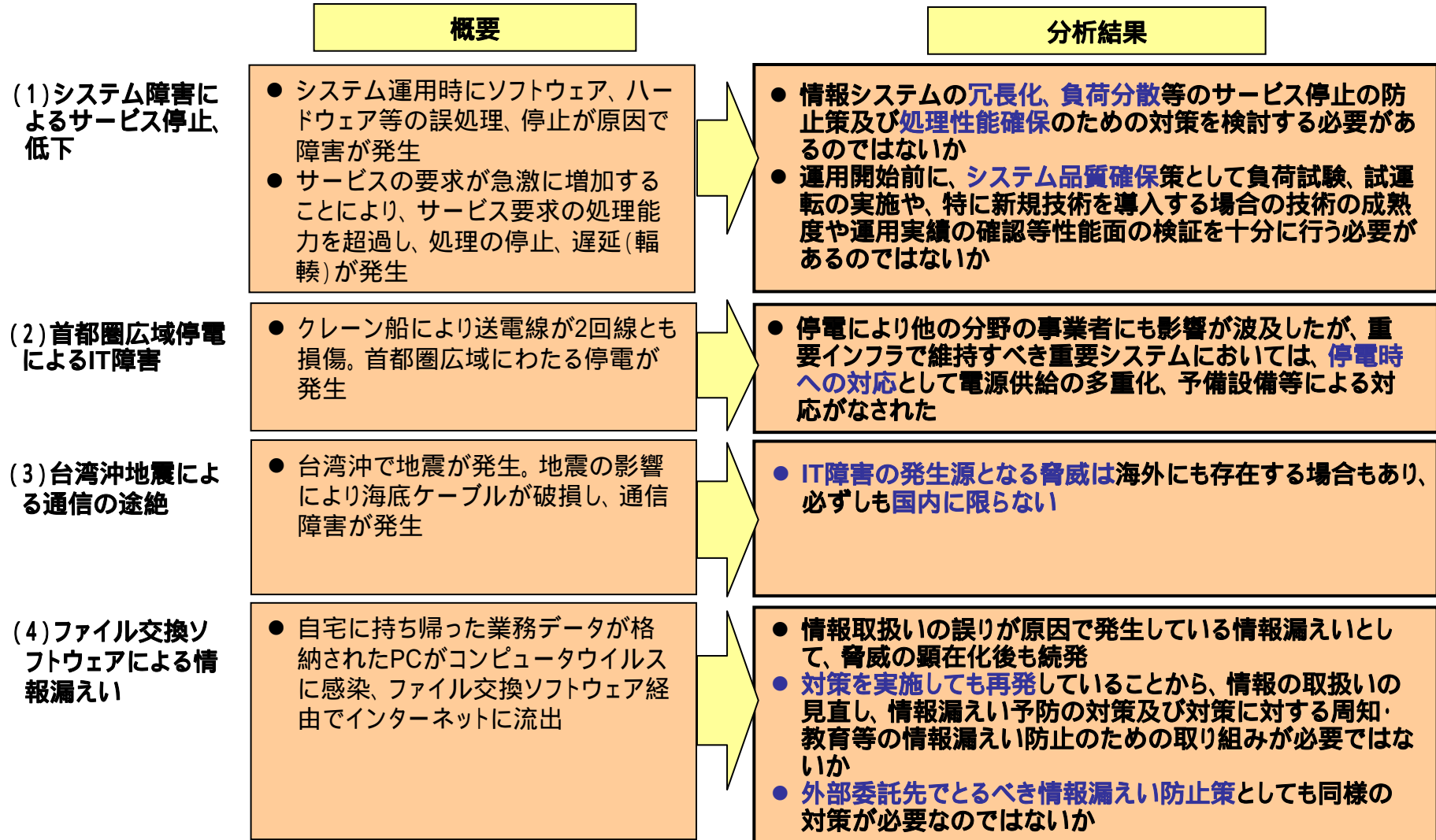
・情報セキュリティ対策の新たな観点が追加されたか、それは、重要インフラ分野に共通的な要検討事項といえるか

社会的条件(環境)の変化の検証

・技術の進歩があったか(新たな脅威の発生・新たな対策の確立)  
・社会的重要性に変化があったか

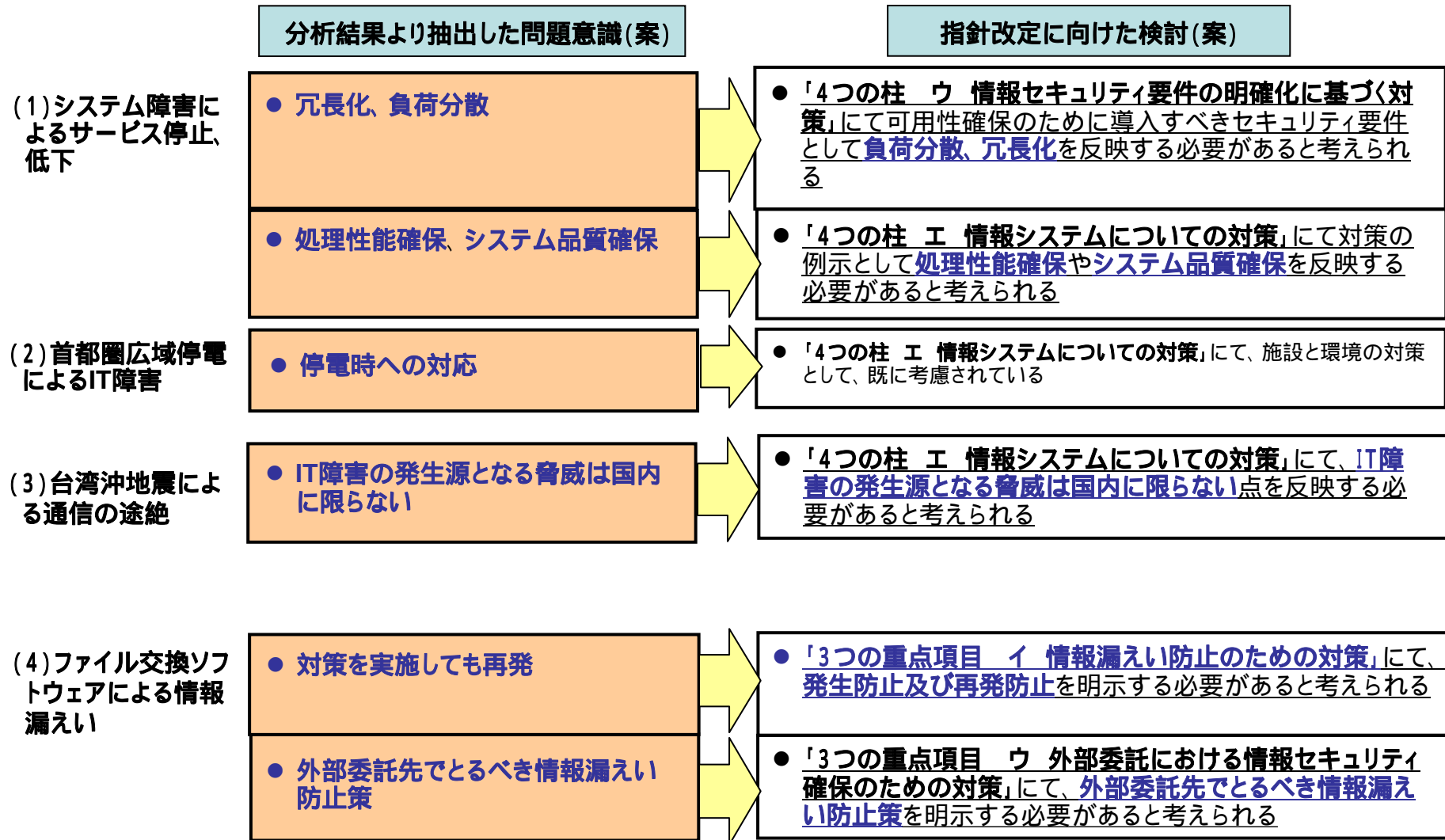
# 状況検証： 定常的なIT障害の発生状況の分析

指針策定後の主要なIT障害の発生状況から、各重要インフラ分野に共通する横断的な対策課題の分析・検討を実施



# 問題意識の抽出： 定常的なIT障害の発生状況の分析

指針策定後の主要なIT障害の発生状況の分析結果より、5箇所(下線部分)について指針の改定が必要と考えられる



# 状況検証： 関連文書の検証

指針策定後の関連文書から、各重要インフラ分野に共通する情報セキュリティ対策の新たな観点の検証を実施

	概要	検証結果
(1) 国内外の規格文書	<ul style="list-style-type: none"> <li>● 以下の規格文書を検証               <ul style="list-style-type: none"> <li>● JIS Q 27001:2006 2006年5月</li> <li>● JIS Q 27002:2006 2006年5月</li> <li>● JIS Q 15001:2006 2006年5月</li> <li>● ISO/IEC 20000-1:2005 (2007年JIS化予定)</li> <li>● ISO/IEC 20000-2:2005 (2007年JIS化予定)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● JIS Q 27001及びJIS Q 27002: ISO/IEC 17799の改訂にて対応された「リスクアセスメント及びリスク対応」及び「<b>情報セキュリティインシデント管理</b>」のカテゴリの新設等を反映。</li> <li>● JIS Q 15001: <b>個人情報保護法との整合性</b>が図られるとともに、マネジメントシステムを運用するための要件の追加</li> <li>● ISO/IEC 20000-1及びISO/IEC20000-2: <b>ITサービスマネジメント</b>についてのPDCAサイクルの運用を規定。</li> </ul>
(2) 省庁ガイドライン	<ul style="list-style-type: none"> <li>● 各省庁にて策定されたガイドライン類について、情報セキュリティ対策の新たな観点が追加されたかを検証</li> </ul>	<ul style="list-style-type: none"> <li>● 個人情報の保護に関するガイドライン: 指針制定以降は、Q &amp; Aの内容反映等や法令改正に伴う所要の改正等のみ</li> <li>● 情報システムの信頼性向上に関するガイドライン: <b>情報システムの企画・開発から保守・運用</b>にわたり関係者が遵守すべき又は遵守することが望ましい事項を規定</li> </ul>
(3) 各重要インフラ分野の安全基準等	<ul style="list-style-type: none"> <li>● 「安全基準等」の策定状況の把握から得られた状況を検証</li> <li>● 「安全基準等」の評価の一環として、各分野の安全基準等における対策項目の具体的な記載内容を検証</li> </ul>	<ul style="list-style-type: none"> <li>● 指針の表現上の問題として、<b>強制基準以外の場合は「遵守が必要である旨を規定する」</b>のは適切でない点判明</li> <li>● 情報セキュリティ対策の新たな観点: <b>自己点検・監査の実施</b></li> </ul>
(4) 政府機関統一基準(及び個別マニュアル群)	<ul style="list-style-type: none"> <li>● 政府機関統一基準(2005年12月情報セキュリティ政策会議決定)の改定状況を検証</li> <li>● 政府機関統一基準適用個別マニュアル群(22文書:2006年2月以降順次作成)について検証</li> </ul>	<ul style="list-style-type: none"> <li>● 政府機関統一基準の見直し課題を参考にすると、重要インフラにおいても、「<b>踏み台</b>」対策に対する検討、<b>想定するリスクについて見直しを実施</b>する必要があるのではないか</li> <li>● 政府機関統一基準適用個別マニュアル群は、政府機関統一基準を更に具体化したレベルとして事業者が安全基準等から内規を作成する際の関連文書として参照することが望ましい</li> </ul>

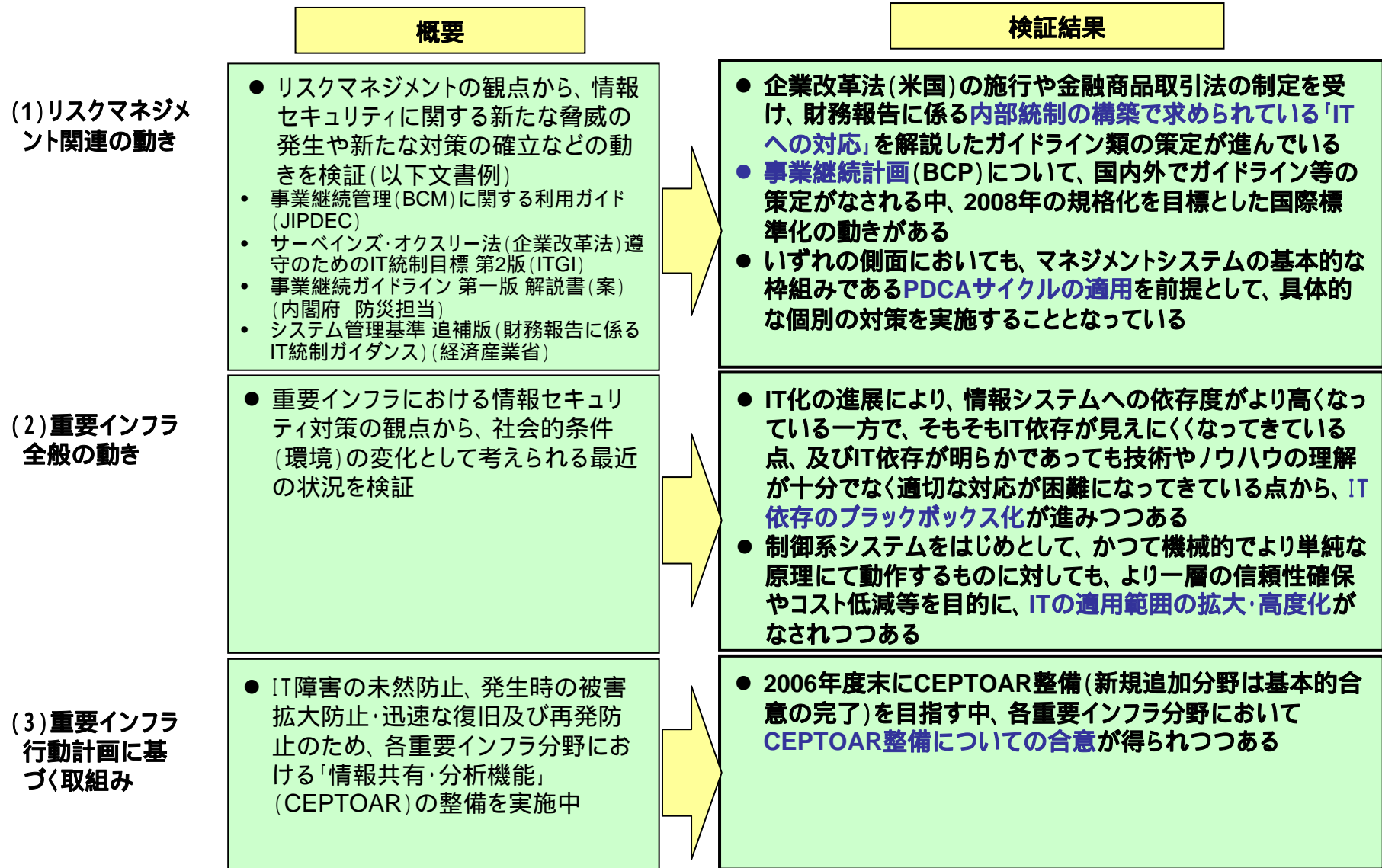
# 問題意識の抽出： 関連文書の検証

指針策定後の関連文書の検証結果より、2箇所(下線部分)について指針の改定が必要と考えられる



# 状況検証： 社会的条件(環境)の変化の検証

以下の社会的条件(環境)の変化より、新たな脅威の発生・新たな対策の確立についての検証を実施





# 問題意識の抽出： 社会的条件(環境)の変化の検証

社会的条件(環境)の変化の検証結果より、3箇所(下線部分)について指針の改定が必要と考えられる

