資料2

NISC National Information Security Center

重要インフラにおける「指針の見直し」について
【骨子案検討】

2009年 3月 4日

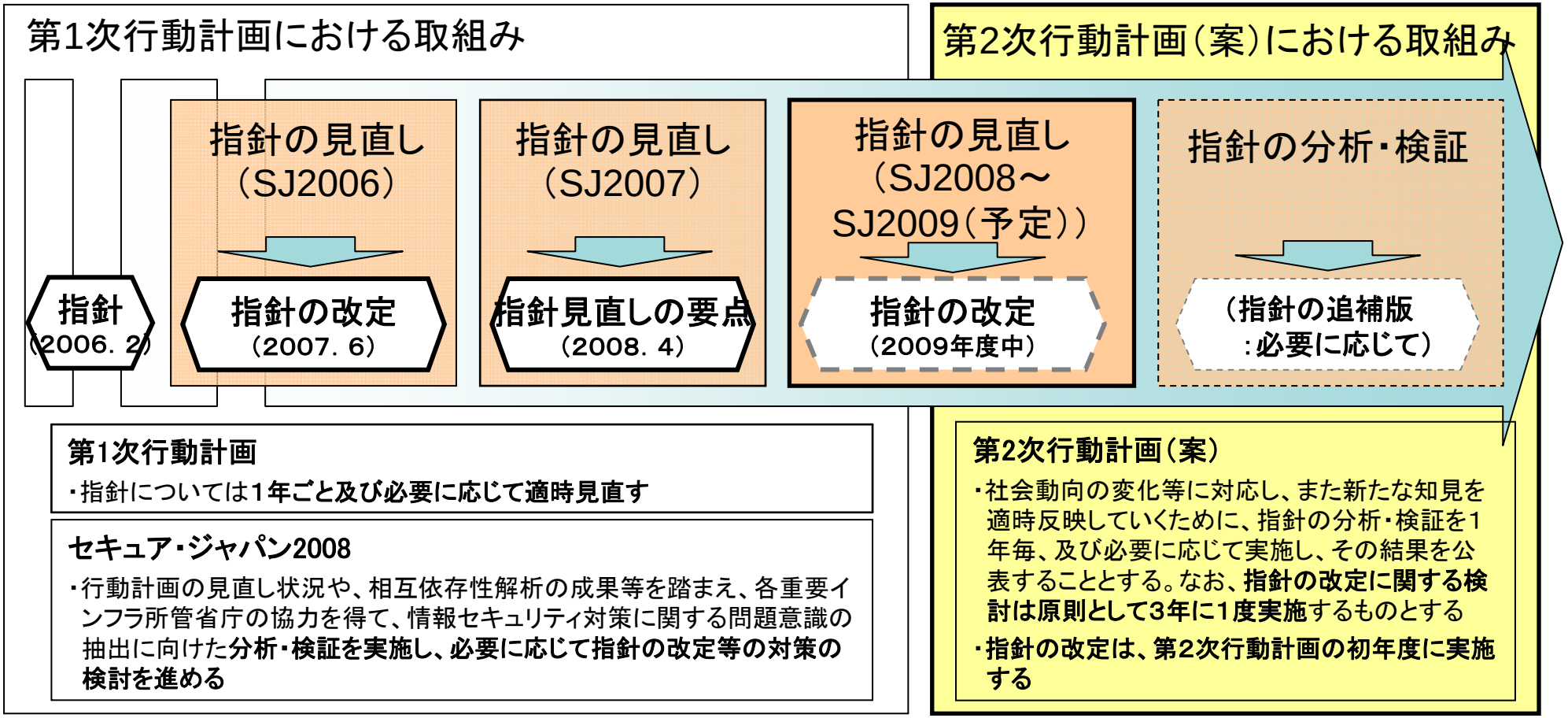
内閣官房 情報セキュリティセンター（NISC）

「指針の見直し」の概要

○第１次行動計画では、**指針（※）制定（2006年2月）、指針の改定（2007年6月）、指針見直しの要点**とりまとめ（**2008年4月**）の実施に加え、各分野にて安全基準等の策定・見直しが行われ、これらを定期的に実施するサイクルが確立した

○今回、セキュア・ジャパン2008に基づいて、**分析・検証を実施し、必要に応じて指針の改定等の対策の検討を進める**

○ この検討から、第２次行動計画（案）における「**指針の改定に関する検討は原則として３年に１度実施**」し、「**指針の改定は、第２次行動計画の初年度に実施する**」ことに引き継いでいき、指針の改定を実施する

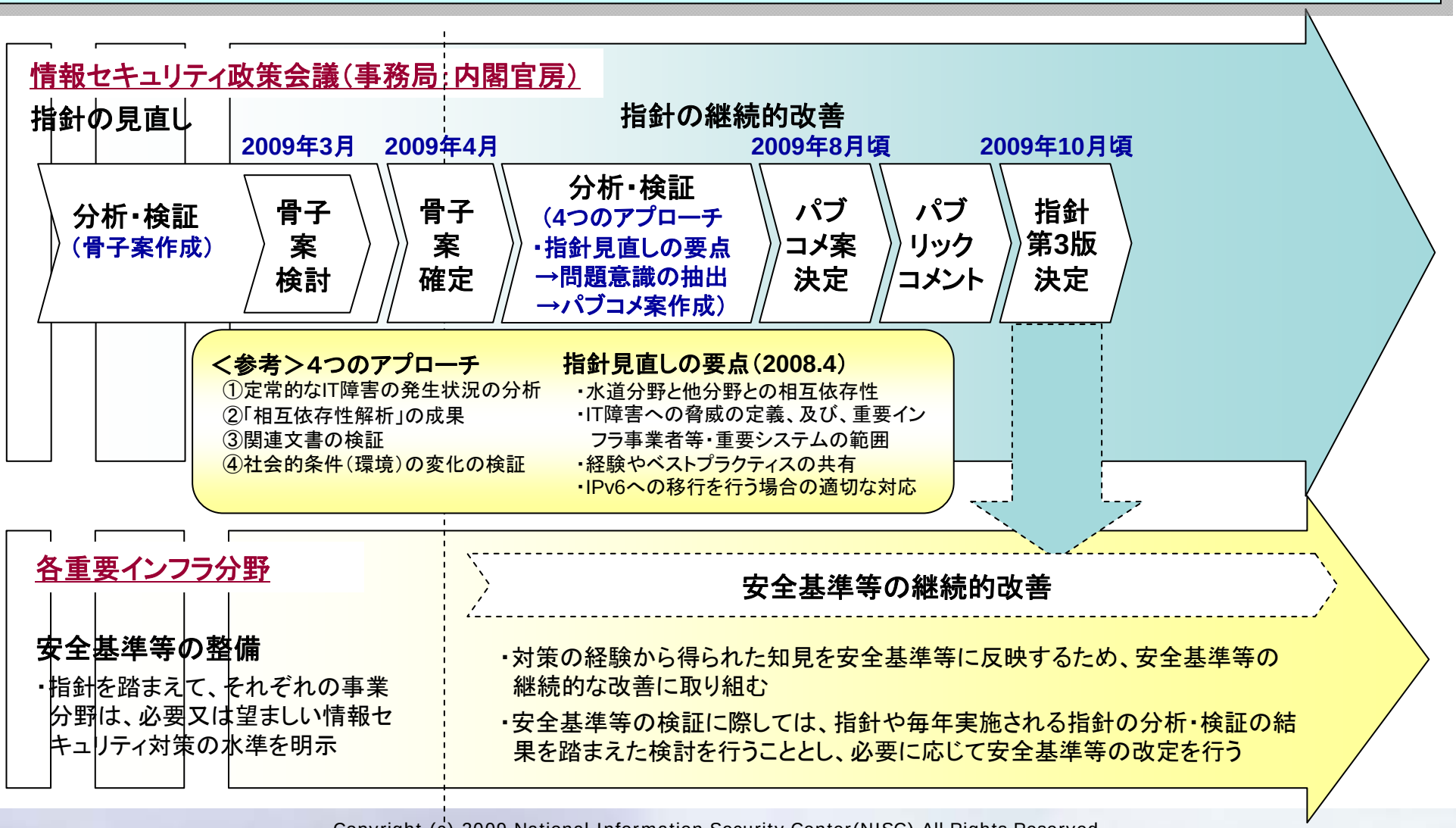


※重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針（2006年2月2日 2007年6月14日改定　情報セキュリティ政策会議決定）

指針の改定に向けたスケジュール

○指針改定の**骨子案を2009年4月までにとりまとめた**後、引き続き分析・検証を進め、**2009年10月頃に指針第3版の策定が完了**することを目指す

○各重要インフラ分野は、第2次行動計画（案）期間中における**安全基準等の継続的改善の際に指針第3版を活用**することを期待する



指針の改定にあたっての基本理念と骨子案の策定

○重要インフラの情報セキュリティ確保のためにより有用なものとなるよう、行動計画の見直しにおいて得られた論点を踏まえて、以下の**対応方針**をおき、指針改定に向けての分析・検証を実施する

○ これらの基本理念を踏まえつつ、**新たな重点項目の在り方等の章構成を含めた指針の大枠について検討**し、骨子案をとりまとめる

行動計画の見直しにおいて得られた論点（第2次行動計画（案）に反映）

①指針の位置づけ、記載内容の具体性のレベル
- 「要検討事項」「参考事項」に分類
- 対策項目の具体化を例示

②事業者とのPDCAサイクルとの整合性
- 指針の大枠の改定は3年に一度
- 1年毎、及び必要に応じて適時に追補版を作成して周知

③事業継続計画との関係
- 事業継続の観点から具体的内容を補充
- 国際規格化の進展状況等を踏まえつつ指針の内容を充実

④リスク開示の在り方
- 様々な自主的な取組みを推奨

【対応方針】

（1）具体性の充実
具体的な対策項目集として自主的な活用を期待
（次ページ参照）

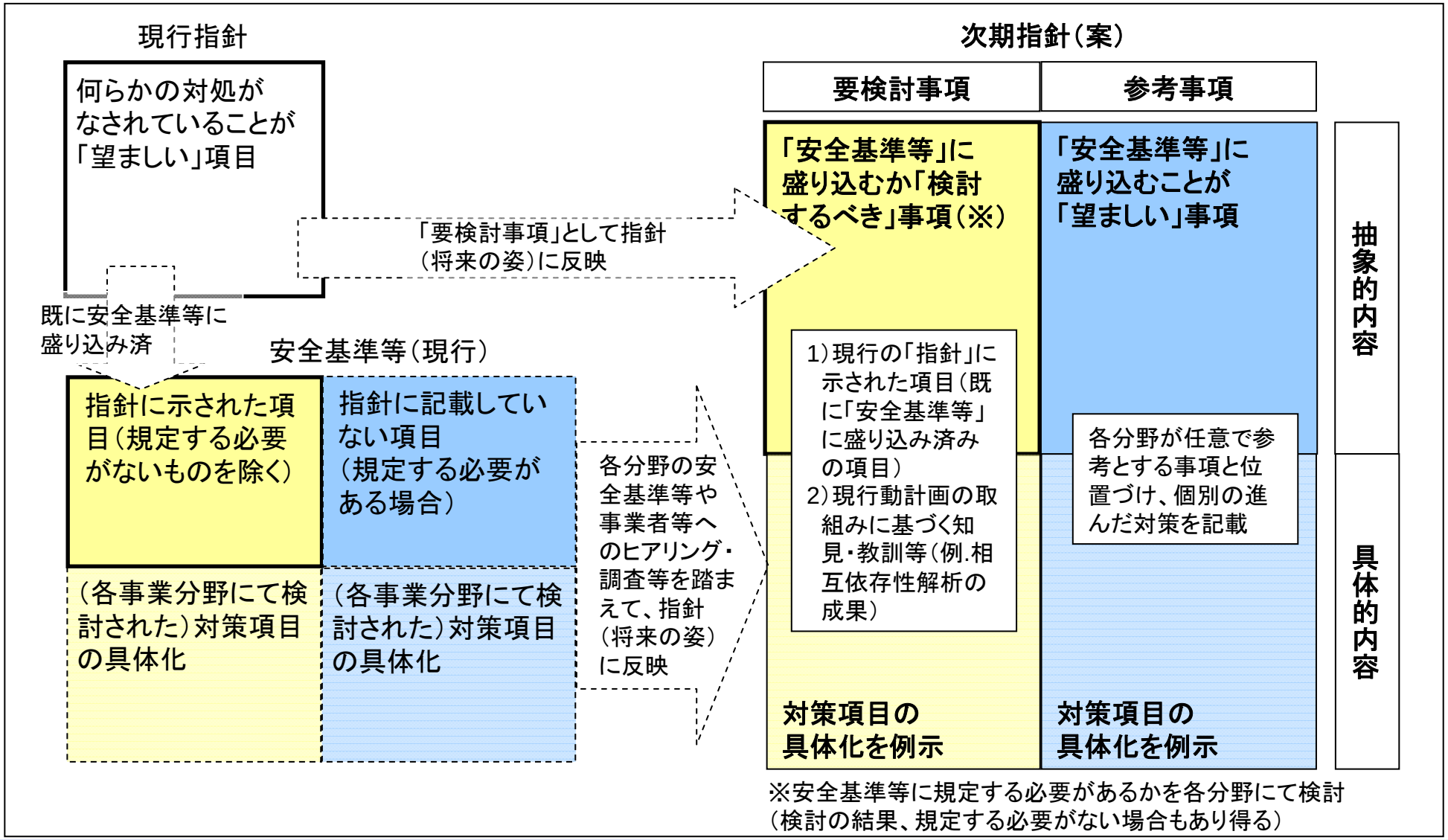
（2）諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

（3）運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

新たな重点項目の在り方等の章構成を含めた指針の大枠について検討し、骨子案をとりまとめる

＜参考＞具体性の充実のイメージ

○重要インフラ事業者等の自主的な取組みに資する項目を充実させるために、指針に記載される事項を「**要検討事項**」と「**参考事項**」に分類し、**対策項目の具体化を例示**することにより、記載事項の充実を図る



骨子案の検討①：全体構成

○重要インフラの情報セキュリティ確保のためにより有用なものとなるよう、基本部分（本編）は現行指針を踏襲しつつ、新たに重要インフラ専門委員会決定となる対策編を追加する

【対応方針】

（1）具体性の充実
具体的な対策項目集として自主的な活用を期待

（2）諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

（3）運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

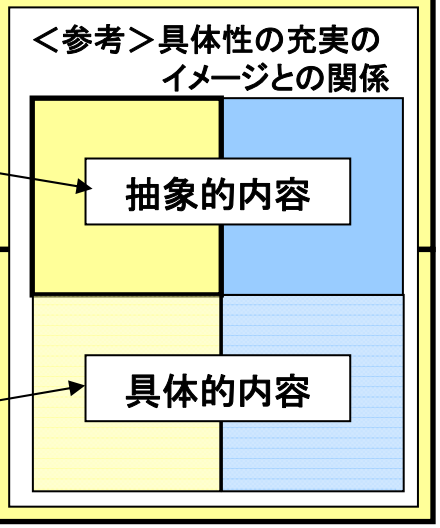
（考え方は骨子案の詳細とともに、次ページ以降にて説明）

現行指針
（2007年6月14日改定　情報セキュリティ政策会議決定）
Ⅰ　目的及び位置づけ
Ⅱ　「安全基準等」で規定が望まれる項目
Ⅲ　フォローアップ

指針第3版
※情報セキュリティ政策会議決定
Ⅰ　目的及び位置づけ
Ⅱ　「安全基準等」で規定が望まれる項目
Ⅲ　フォローアップ

指針第3版　対策編
※重要インフラ専門委員会決定
Ⅰ　本対策編の位置づけ
Ⅱ　対策項目の具体化の例示
別紙　参考文献

＜参考＞具体性の充実のイメージとの関係



骨子案の検討②：本編　Ⅰ　目的及び位置づけ

○現行指針に、第2次行動計画における取組みの内容を盛り込むことに加え、「5．本指針の構成」の節を追加し、「（1）具体性の充実」「（3）運用性の確保」から求められる対応を記載する

【対応方針】

（1）具体性の充実
具体的な対策項目集として自主的な活用を期待

（2）諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

（3）運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

○「要検討事項」「参考事項」を盛り込む旨とその説明を記載

○指針本体（本編）に加え、専門委員会決定とする対策編にて構成される旨を記載

○第2次行動計画における取組みの内容を盛り込み

現行指針（2007年6月14日改定　情報セキュリティ政策会議決定）

Ⅰ　目的及び位置づけ

1．重要インフラにおける情報セキュリティ確保のために
2．「安全基準等」の必要性
3．「安全基準等」とは何か
4．本指針の位置づけ
5．本指針を踏まえた安全基準等の策定若しくは見直しへの期待

指針第3版（骨子案）

Ⅰ　目的及び位置づけ

1．重要インフラにおける情報セキュリティ確保のために
2．「安全基準等」の必要性
3．「安全基準等」とは何か
4．本指針の位置づけ
5．本指針の構成
6．本指針を踏まえた安全基準等の**継続的改善及び浸透**への期待

骨子案の検討③：本編　Ⅱ　「安全基準等」で規定が望まれる項目

○現行指針の節・項の構成を見直しし、重複する記載内容を集約することに加えて、「6．対策項目」の節に「要検討事項」「参考事項」それぞれの「抽象的内容」のみを記載する

【対応方針】

（1）具体性の充実
具体的な対策項目集として自主的な活用を期待

（2）諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

（3）運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

○節・項の順番・構成を見直しして、重複する記載内容を集約

○「要検討事項」「参考事項」それぞれの「抽象的内容」のみを記載（「具体的内容」は、対策編にて別に記載）

現行指針（2007年6月14日改定　情報セキュリティ政策会議決定）
Ⅱ　「安全基準等」で規定が望まれる項目
1．「安全基準等」の対象範囲及び対象とする脅威
2．「安全基準等」の公開
3．具体的項目
（1）「安全基準等」策定の目的
（2）対象範囲と想定する脅威
（3）重要インフラ事業者等の担う役割
（4）対策項目

指針第3版（骨子案）
Ⅱ　「安全基準等」で規定が望まれる項目
1．「安全基準等」策定の目的
2．「安全基準等」の対象範囲
3．「安全基準等」の対象とする脅威
4．重要インフラ事業者等の担う役割
5．「安全基準等」の公開
6．対策項目
（1）4つの柱
ア）組織・体制及び資源の確保
【要検討事項】
【参考事項】　（以下省略）

骨子案の検討④：本編　Ⅲ　フォローアップ

○現行指針の節・項の構成を他の章とあわせて見直しし、第2次行動計画における取組みの内容を盛り込むことに加え、「2. 本指針の継続的改善」の節の本文中に「(3)運用性の確保」から求められる対応を記載する

【対応方針】

(1)具体性の充実
具体的な対策項目集として自主的な活用を期待

(2)諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

(3)運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

○節・項の構成を他の章とあわせて見直し

○第2次行動計画における取組みの内容を盛り込み

○指針の改定に関する検討は原則として3年に1度の旨記載(本文中)

現行指針(2007年6月14日改定　情報セキュリティ政策会議決定)
Ⅲ　フォローアップ
(頭書き)
(1)本指針の見直し
(2)「安全基準等」の継続的検証
①「安全基準等」の見直し
○内閣官房
○重要インフラ所管省庁及び重要インフラ事業者等
②「安全基準等」に対する準拠状況の評価

指針第3版(骨子案)
Ⅲ　フォローアップ
1. フォローアップの考え方
2. 本指針の継続的改善
(1)指針改定に関する検討
(2)指針の分析・検証
3. 安全基準等の継続的改善
(1)重要インフラ所管省庁及び重要インフラ事業者等
(2)内閣官房
4. 安全基準等の浸透
(1)重要インフラ所管省庁及び重要インフラ事業者等
(2)内閣官房

骨子案の検討⑤：対策編

○重要インフラ専門委員会決定にて定める対策編を新たに設けて、「（1）具体性の充実」「（2）諸規格との整合」から求められる対応を記載する

【対応方針】

（1）具体性の充実
具体的な対策項目集として自主的な活用を期待

（2）諸規格との整合
重要インフラの特徴を踏まえつつ、国内外の標準・基準にも配慮

（3）運用性の確保
各分野が主体的に検討するPDCAサイクルを尊重

○「要検討事項」「参考事項」それぞれの「具体的内容」を記載

○対策編の別紙として、参考文献を整理し記載

指針第3版　対策編（骨子案）

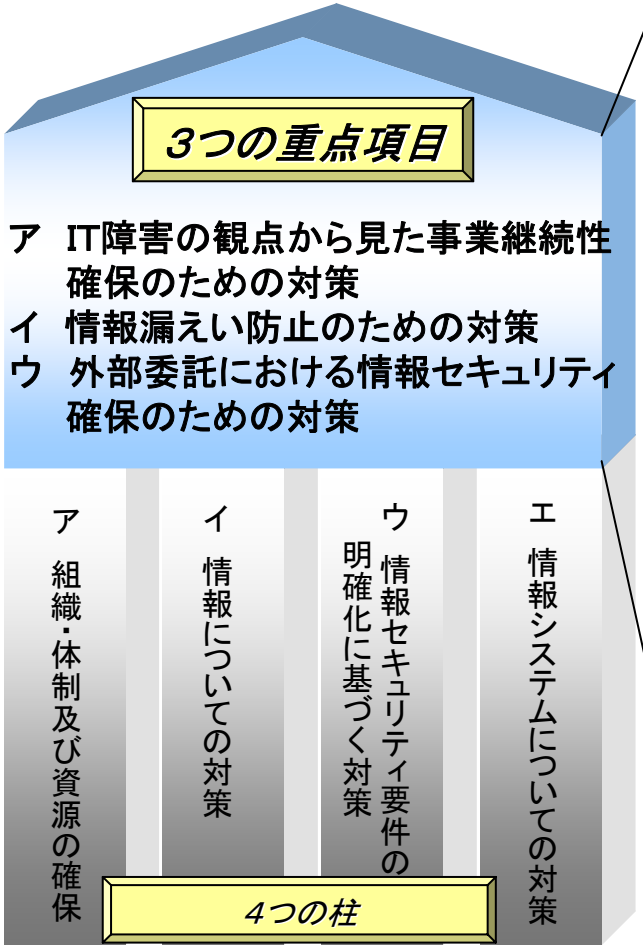
Ⅰ　本対策編の位置づけ
Ⅱ　対策項目
　1．4つの柱
　（1）組織・体制及び資源の確保
　【要検討事項】 ＜対策項目の具体化の例示＞
　【参考事項】 ＜対策項目の具体化の例示＞
　（省略）

別紙　参考文献

骨子案の検討⑥：新たな重点項目の在り方

○前回の指針改定（2007年６月）以降の状況変化を踏まえて、現行指針の４つの柱と３つの重点項目に加え、見出しレベルで指針に盛り込むべき内容があれば骨子案に記載するかを議論

現行指針　（2007年6月14日改定　情報セキュリティ政策会議決定）



【今回議論をお願いしたい内容】

・重点項目の見出しとして取り扱うべきテーマ

→行動計画見直しでの議論を通じて得られた状況変化を踏まえ、新たな重点項目を立てる必要があるか、また既存の重点項目についてどのように考えるか

【新たな重点項目（案）】

※以下に留まらず、委員の見識に基づき、自由な発想で議論をお願いしたい

リスク開示の在り方＜参考１＞　より

「利用者の合理的な対応に必要なリスクの開示のための対策」

（具体例）・サービスの停止状況、復旧見込みの情報等を周知
・情報セキュリティ報告書又はそれに相当するものの作成　等

IT障害を引き起こす脅威の例＜参考２＞　より

「社会環境変化や制度改正に起因する不可避な脅威のための対策」

（具体例）・暗号の危殆化、IPv6への移行、プロトコルの脆弱性　等

【既存の重点項目】

事業継続計画との関係＜参考３＞　より

「IT障害の観点から見た事業継続性確保のための対策」

対策の目的（目標）、視点＜参考４＞　より

「情報漏えい防止のための対策」

「重要インフラ分野」の分類、位置づけ＜参考５＞　より

「外部委託における情報セキュリティ確保のための対策」

今回議論にて得られた方向性を骨子案に盛り込み

（次回専門委員会にて確認）

＜参考1＞行動計画見直しでの議論（1/5）

リスク開示の在り方

※ 第22回重要インフラ専門委員会　参考資料3より抜粋し、一部修正・追記（青字部分）

○安全基準等において前提とするリスクを開示することについては、リスク管理の観点からどう考えるべきか

- リスクコミュニケーションの観点から、前提とするリスクを開示することにより、サービス提供側のみでなく利用側におけるリスクの対処が容易になるのではないか
  - リスクを開示せずにブラックボックス化したままでは、利用側にとってみれば、サービス提供側がすべてのリスクを負うという誤解が生じる可能性がある
  - インターネット等を活用して、サービスの停止状況、復旧見込みの情報等を周知している事業者等もある
  - 一方、リスクを開示することにより、攻撃者に対し、脆弱な箇所を知らせることになって、脅威が増大する可能性の側面もある
- 「指針」では、「「安全基準等」は（中略）可能な限り公開されることが望ましい」としている
  - 非公開とする代わりに、情報セキュリティの取組みをホームページに掲示している分野もある
  - 情報セキュリティ政策会議において、「安全基準やこれをふまえたアクションプランについて、重要インフラに依存している国民に公表することが必要」という意見もある
- 情報セキュリティマネジメントの有効性の測定の国際標準（ISO/IEC27004：現在策定中）が参考になるという考え方もある
- 【専門委員会での議論より得られた方向性】
  - 情報開示の仕方としては、対象者を限定して開示するという取扱いもあるのではないか
  - リスク開示のあり方として、監査というプロセスが重要であることを踏まえれば、情報セキュリティ監査報告書の取得を対策の一つとして取り上げてもよいのではないか

第2次行動計画　Ⅱ．１ 安全基準等の整備及び浸透（p14）より

（前略）重要インフラ事業者等のPDCA サイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。

第2次行動計画　Ⅱ．1（2）安全基準等の継続的改善（p15）より

安全基準等に基づく対策状況については、関係性を有する主体間で互いに把握しておくことが重要である。そのため、情報セキュリティ監査又はそれに相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等の自主的な取組みを一層推奨し、分野や重要インフラ事業者等における情報セキュリティ対策の対外的な説明に努める。

＜参考2＞行動計画見直しでの議論（2/5）

IT障害を引き起こす脅威の例

脅威の種類	脅威の例	
	社会全体で対応が望まれる脅威	個別の重要インフラ事業者等が中心となって対応する脅威
①サイバー攻撃をはじめとする意図的要因	分野横断的に多発するサービス不能攻撃、不正侵入、重要情報の搾取　等	不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃（DoS: Denial of Service）、情報漏えい、重要情報の搾取、内部不正　等
②非意図的要因	大規模な操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備が予想される社会環境変化や制度改正（例：西暦2000年問題、暗号の危殆化、IPv6への移行）　等	操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥　等
③災害や疾病	大規模な地震、水害（例：首都圏直下地震、荒川の氾濫）による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等
④他分野の障害からの波及	大規模な電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等

※　第2次行動計画　別紙3（p47）より抜粋（下線は、第1次行動計画からの追記部分）

＜参考3＞行動計画見直しでの議論（3/5）

事業継続計画との関係

※ 第22回重要インフラ専門委員会 参考資料3より抜粋し、一部修正・追記（青字部分）

○「指針」や「安全基準等」に事業継続の観点を補充する必要はないか、盛り込むとすれば、事業継続計画との整合性をどう取るべきか

- 指針では、3つの重点項目にて「IT障害の観点から見た事業継続性確保のための対策」として「事業継続計画との整合性の確保」としての対策が盛り込まれている
  - 記載の仕方にバラツキはあるが、各分野の安全基準等においても盛り込まれている
- 事業継続管理についての国際規格化、ガイドラインの拡充等の動きがある
  - 内閣府防災、経済産業省にて事業継続計画のガイドラインを策定済
  - 総務省にて「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」（2008.8）を公表
  - 経済産業省にて「ITサービス継続ガイドライン」（2008. 9）を公表
- 【専門委員会での議論より得られた方向性】
  - 関連する他分野の復旧目安がどの程度なのか等、分野横断的な議論を行って検討すべき
  - 事業継続計画の発動の際には、法制面での工夫が必要となる場合が考えられる

第2次行動計画 Ⅱ．1（1）指針の継続的改善（p14）より

なお、指針の改定に関する検討にあたっては、重要インフラ事業者等において事業継続計画の策定が進みつつある状況や、事業継続計画に関する国際規格化の進展状況等を踏まえつつ、分野横断的な観点からも実効的であるかを検証できるように指針の内容を充実させるものとする

安全基準等の指針「Ⅱ3.(4)② 3つの重点項目」より（抜粋）

・ア IT障害の観点から見た事業継続性確保のための対策

（イ）事業継続計画との整合性の確保

事業継続計画が策定される場合は、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである

＜参考4＞行動計画見直しでの議論（4/5）

対策の目的（目標）、視点

※ 第22回重要インフラ専門委員会 参考資料3より抜粋し、一部修正・追記（青字部分）

○個人情報保護の観点をどう位置づけるべきか

- 一般に個人情報保護法において「個人情報保護取扱事業者」には、個人情報の適正な取扱いの確保が求められている
- 第１次行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
- 【専門委員会での議論より得られた方向性】
  - （特になし：事務局案のとおり）

【事務局案】
・ 個人情報保護法が制定されていることを踏まえると、法令遵守の観点から当然対応が必要なものであり、重要インフラ事業者向けとして特に行動計画において求めるべきことは現時点では少ないのではないか

第１次行動計画「1 目的と範囲」より（抜粋） ※第2次行動計画においても同趣旨を記載
・ （IT障害）から国民生活や社会経済活動に重大な影響を及ぼさないよう重要インフラを防護し、重要インフラ事業者等の事業継続への取組みを強化するための取ることが望ましい重要インフラ事業者等の自主的な対策について示す

【事務局案補足（指針見直しの観点）】
・ 個人情報に限らず、重要インフラの位置づけ（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）より、情報漏えいが発生した場合の国民への影響は大きいのではないか
・ 情報漏えいや不正アクセスの脅威の発生は、相変わらず少なくないのではないか

＜参考5＞行動計画見直しでの議論（5/5）

「重要インフラ分野」の分類、位置づけ

※ 第22回重要インフラ専門委員会 参考資料3より抜粋し、一部修正・追記（青字部分）

○現在の10分野の分類や位置づけは適切か、実態に即し見直し（分割・追加等）の必要はないか

- 諸外国における重要インフラの分類（次ページ）等を参考に、見直し（分割・追加等）が望まれる分野はないか
  例） クレジットカード会社（消費者信用）、ITベンダー（情報技術） 等
- 現在の10分野とは別に、協力を求めるべき業界があれば、何らかの形で位置づけることも考えられる
- 現在の10分野についても、ITへの依存度等に応じて分類や位置づけを何段階かに整理することも考えられる
- 重要インフラの定義そのものについても、必要に応じて見直しを検討することが考えられる
- 【専門委員会での議論より得られた方向性】
  - （特になし：事務局案のとおり）

【事務局案】
- 新たな分野を加えるのではなく、現在の10分野を踏襲しつつより内容を充実させてはどうか
- ITベンダーは、新たな分野としてではなく、各施策において必要に応じて協力を得てはどうか

第1次行動計画「2 重要インフラの定義と対象」より（抜粋） ※第2次行動計画においても同趣旨を記載
- 重要インフラとは、「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」と定義
- 当面の対象分野は、「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10分野

【事務局案補足（指針見直しの観点）】
- ITベンダーは、重要インフラの各事業における外部委託先として、互いに協力して情報セキュリティ対策を推進する立場と考えてはどうか