# 保証型情報セキュリティ監査への取り組み

2006/06/15

大木栄二郎
日本セキュリティ監査協会
顧問、保証型監査促進プロジェクトリーダー
主席情報セキュリティ監査人
工学院大学情報学部　教授

# 目　次

- 情報セキュリティ監査とは
  - 情報セキュリティ監査制度
  - ＪＡＳＡの取り組み
- 保証型監査促進プロジェクトの紹介
  - 背景と目的
  - 保証の本質
  - 保証型情報セキュリティ監査の類型
- 今後の保証型監査の展開

# 「情報セキュリティ監査」とは

「情報セキュリティ監査」の外縁は、

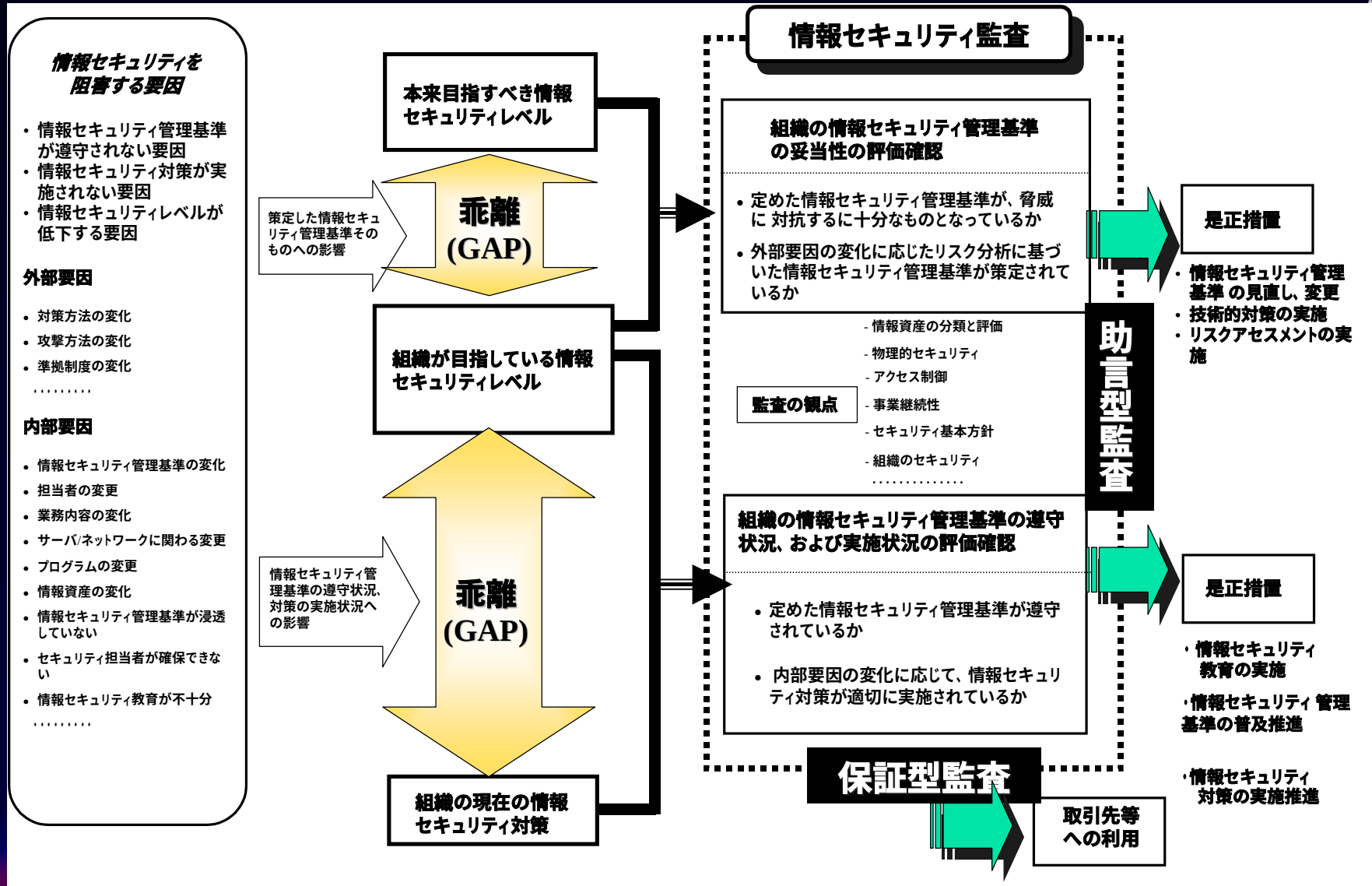
- 情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、
- リスクアセスメントに基づく適切なコントロールの整備、運用状況を、
- 情報セキュリティ監査を行う主体が独立かつ専門的な立場から、
- 国際的にも整合性のとれた基準に従って
- 検証又は評価し、
- もって保証を与えあるいは助言を行う活動

と定義できる。

経済産業省　2003年3月26日「情報セキュリティ監査報告書」より

# 情報セキュリティ監査の位置付け

経済産業省報告書より



# 特定非営利活動法人 日本セキュリティ監査協会 設立

# 代表的な成果物

具体的な技術的情報セキュリティ管理基準の検討

情報セキュリティ監査
保証型監査ガイド(中間報告)

情報セキュリティ監査
助言型監査マニュアル

個人情報保護に係る監査のスコープを検討するにあたっての留意事項

情報セキュリティ監査を取り巻く国内･海外の状況に関する調査

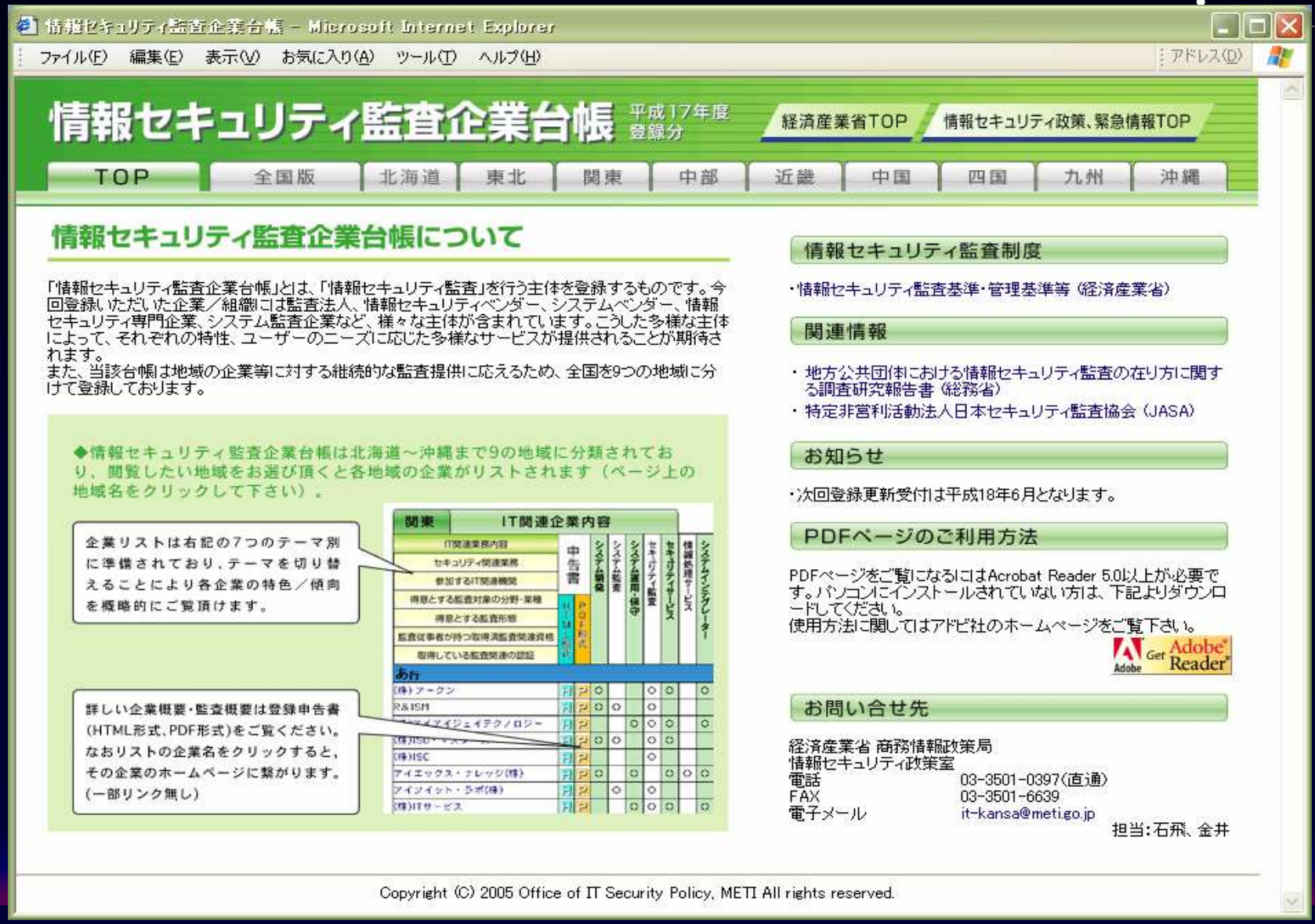
リスクアセスメント手法についての検討報告書

# 公認情報セキュリティ監査人資格制度

# 審査制度の拡充


JASA (JApan information Security Audit association) - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
アドレス(D)
審査委員会
審査委員会の役割
倫理審査制度
紛争審査制度
監査品質審査制度
審査申出
規定集
審査委員会
審査委員会の役割
2003年3月に発表された経済産業省の情報セキュリティ監査研究会報告書にて監査を行う主体となる企業の質の確保にあたって、「監査に係る紛争処理」を行うことが有効であると提言されました。当協会設立後は、経済産業省からの委託を受けて、約1年間の検討と事前準備を進め、このたび審査委員会を設置するに至りました。
当協会が審査委員会を設置し、紛争審査制度の受付を開始することは、こうした個別の情報セキュリティ監査業務に関するクレームの窓口として、会員または公認情報セキュリティ監査人資格制度(CAIS)の資格認定者が行う監査が、情報セキュリティ監査制度の標準的基準、協会の定める倫理基準や協会が確立した標準的な監査手法や監査技術に従って行われているかどうかを、公平な第3者の視点にて評価することが可能となります。
紛争審査制度の受付を開始するのと同時に、監査品質審査制度及び倫理審査制度を開始いたします。前者は、被監査側からの苦情を契機とすることなく、当協会自らが会員により行われる個別の情報セキュリティ監査業務の品質審査を行うものであり、後者は、会員または公認情報セキュリティ監査人資格制度(CAIS)の資格認定者による倫理基準違反の事実を評価するものです。これらの審査委員会における各種制度により、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会における社会的責任を果たすことをめざします。
インターネット

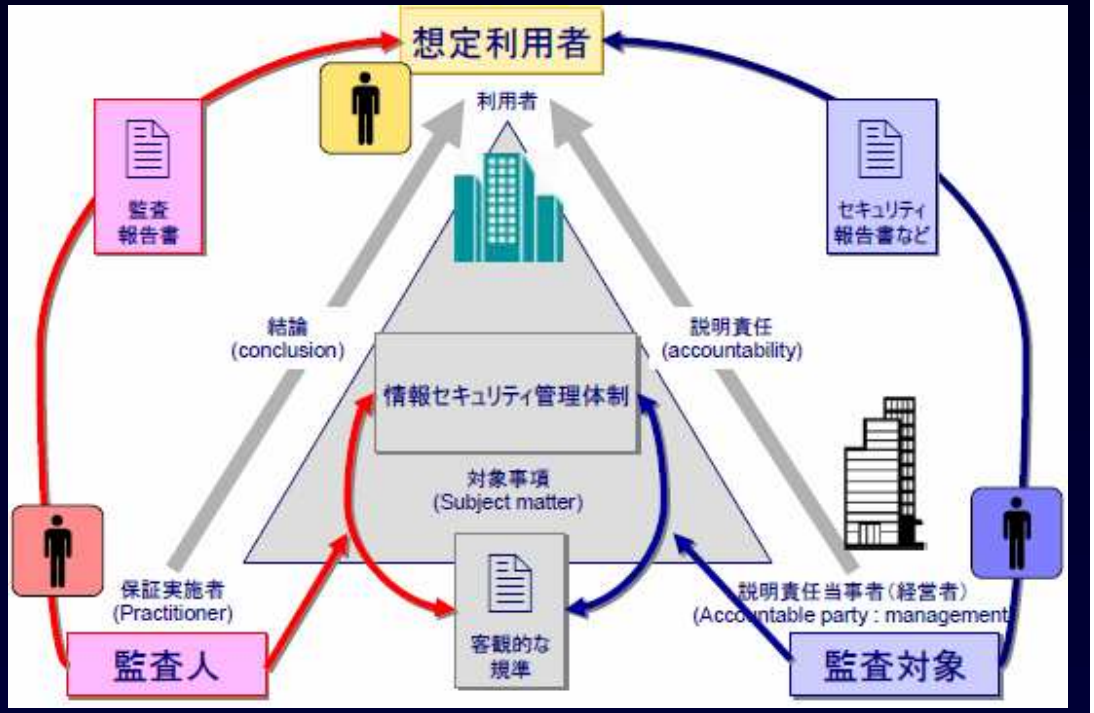
# 情報セキュリティ監査企業台帳



# 監査とコンサルティング

| | 保証型監査 | 助言型監査 | コンサルティング |
|---|---|---|---|
| 保証 | 与える | 与えない | 与えない |
| 意見 | 述べる | 述べる | 述べる |
| 提言 | しない | する | する |
| 客観的基準 | 存在することが前提 | 存在することが前提 | ない |
| 実施者の独立性 | 必須 | 必須 | 必須ではない |

## 監査の三者関係



# 目　次

- 情報セキュリティ監査とは
  - 情報セキュリティ監査制度
  - ＪＡＳＡの取り組み
- 保証型監査促進プロジェクトの紹介
  - 背景と目的
  - 保証の本質
  - 保証型情報セキュリティ監査の類型
- 今後の保証型監査の展開

# プロジェクトの背景

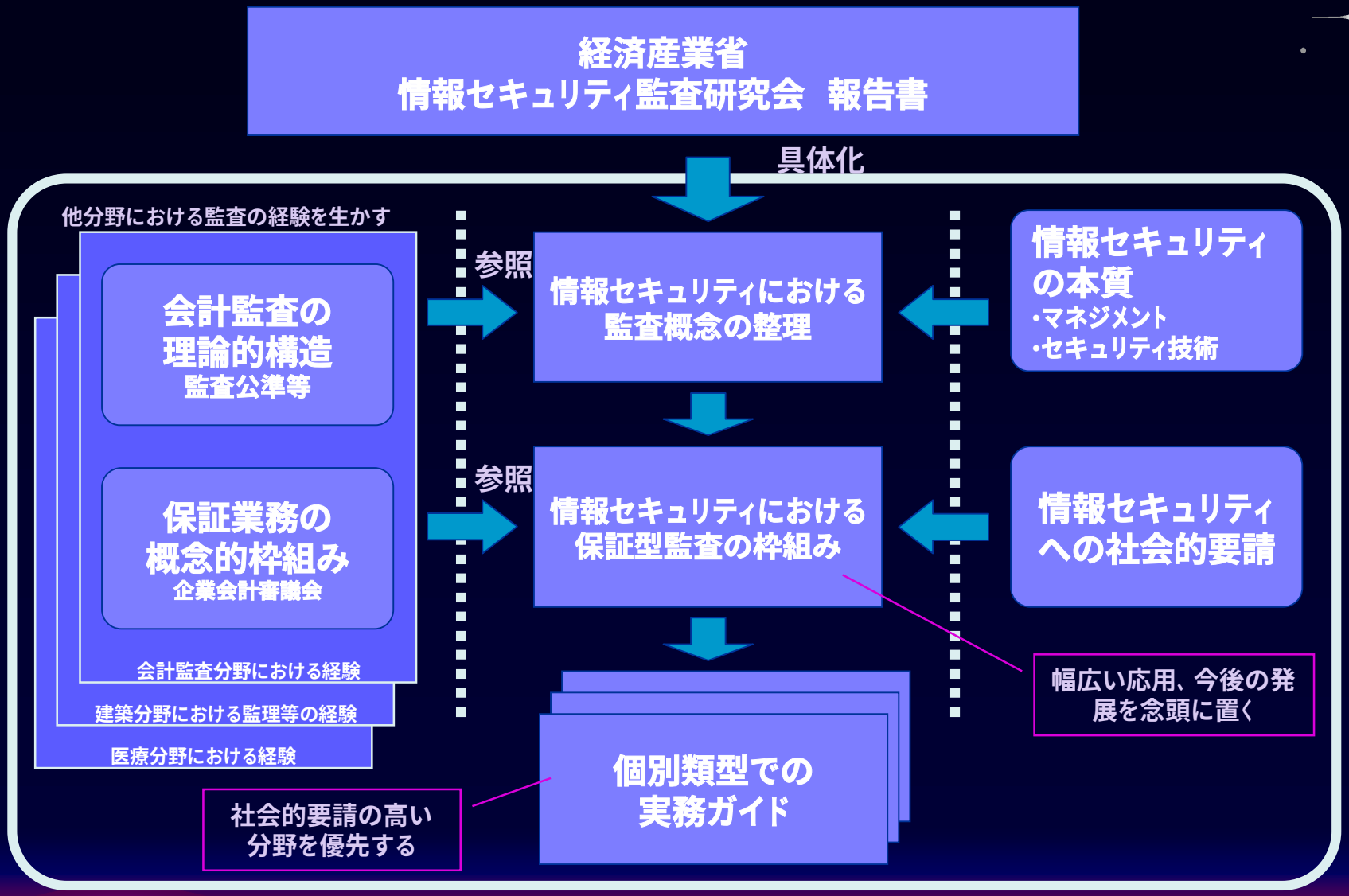
- 現状認識
  - 助言型監査が圧倒的
  - 保証型監査についてはほとんど実施されていない
- 保証型監査のニーズ
  - 商取引や業務委託を請け負う組織体は、独立かつ専門的知識を持った者に、自らの情報セキュリティ対策について、監査を受けて「保証」を得たい
  - 業務を委託する側は、業務委託先や個人情報の預託先の選定において、独立かつ専門的知識を持った者の「お墨付き」を得た組織体を選択したい
- まだ抽象的な保証の概念
  - 保証型監査における「保証」は、まだ抽象的な概念
  - 保証型監査を早期に形あるものにすることに多くの方の思いが一致している

- ＪＡＳＡの組織を上げて横断的に取り組む
  - 既存のすべての部会や委員会が参加して新たな形をまとめる
  - 多様な監査のあり方を前提として、幅広い適用を念頭に置く
  - 時間を区切って、プロジェクトとして取り組む

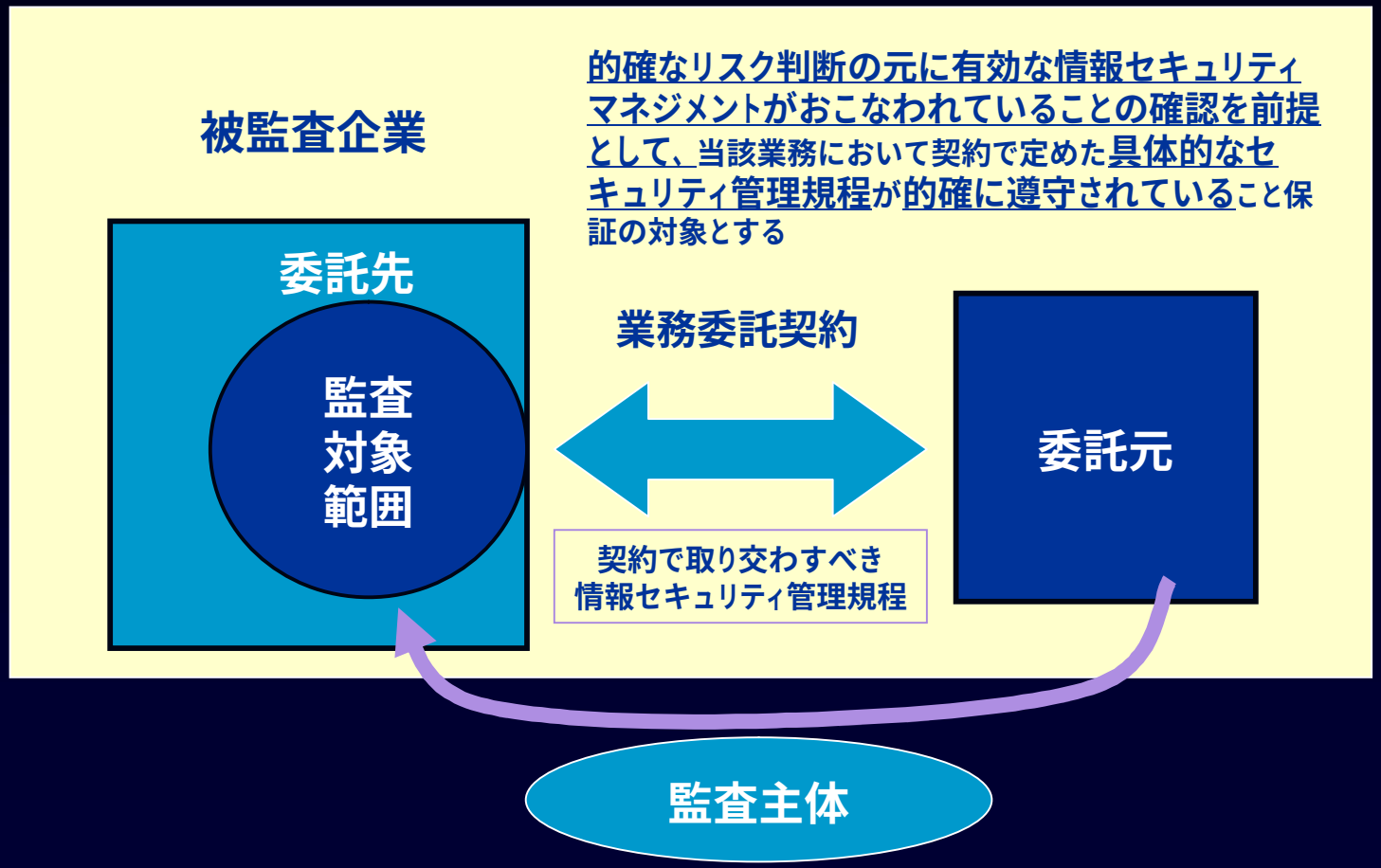
# 検討すべき課題の認識

- 論理的枠組みの構築
  - 何を保証するのか、 どの程度保証するか、 保証できる根拠を何におくか
- 課題の抽出と整理
  - 論理枠組みに沿って課題を抽出し整理
    - 保証根拠の客観性、 監査人の責任範囲、 保証型監査の正確な認識
  - 優先領域の課題を深堀する
- 社会ニーズの整理と優先領域の選択
  - 市場の要求の整理、 優先領域選択の条件整理、
  - 候補領域の調査と優先領域の決定
    - ＥＣ，人材派遣企業、 政府機関、etc
- 関連する世の中の動向の分析
  - 各種関連情報の整理、 保証型監査類型のサポート情報
- 優先領域における課題解決の施策
  - 優先領域に求められる類型の課題を解決する施策
    - 標準契約書ひな形、 報告書、監査意見ひな形、 監査計画ガイド、
    - 要求される監査スキル、 保証意見の成立条件整理
  - 保証型監査の前提条件の準備
    - 具体的管理基準、 監査対象範囲の限定
- パイロット監査の実施
  - 早期に取り組むべく分野の特定、 特定分野の各種関連情報の整理

# 検討の枠組み

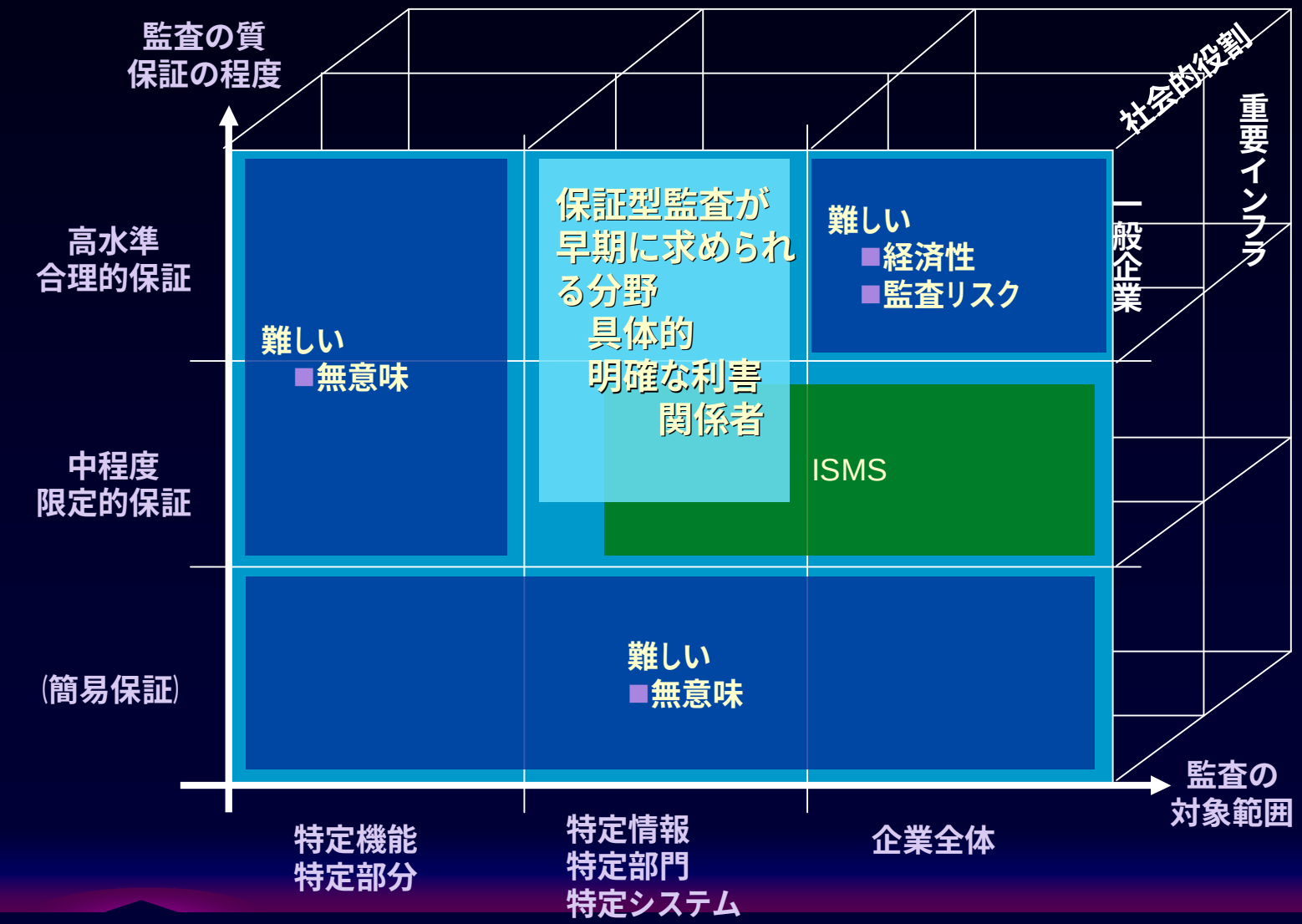

経済産業省
情報セキュリティ監査研究会　報告書
具体化
他分野における監査の経験を生かす
会計監査の
理論的構造
監査公準等
保証業務の
概念的枠組み
企業会計審議会
会計監査分野における経験
建築分野における監理等の経験
医療分野における経験
参照
参照
情報セキュリティにおける
監査概念の整理
情報セキュリティにおける
保証型監査の枠組み
情報セキュリティ
の本質
・マネジメント
・セキュリティ技術
情報セキュリティ
への社会的要請
幅広い応用、今後の発
展を念頭に置く
個別類型での
実務ガイド
社会的要請の高い
分野を優先する

# 業務委託先を例とした保証型監査の枠組み検討

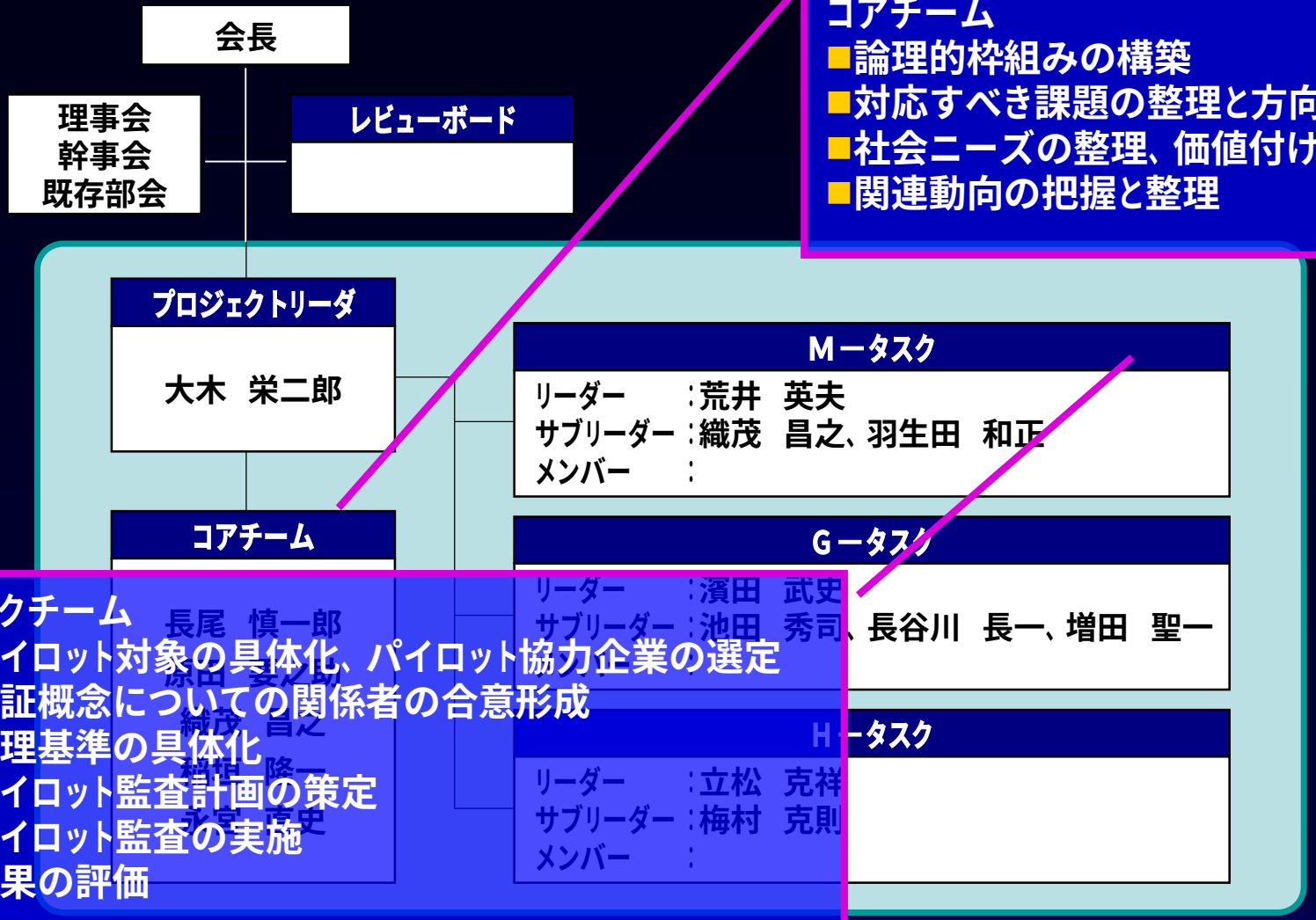



**委託元が期待する程度の情報セキュリティ対策が委託先で行われていると判断できる旨の保証**

# 保証型監査が早期に求められる分野



# プロジェクト体制




コアチーム
- ■論理的枠組みの構築
- ■対応すべき課題の整理と方向付け
- ■社会ニーズの整理、価値付け
- ■関連動向の把握と整理

タスクチーム
- ■パイロット対象の具体化、パイロット協力企業の選定
- ■保証概念についての関係者の合意形成
- ■管理基準の具体化
- ■パイロット監査計画の策定
- ■パイロット監査の実施
- ■結果の評価

# 保証型情報セキュリティ監査のフレームワーク

- 言明方式と非言明方式とに分類する
  - 言明方式の保証型情報セキュリティ監査
  - 非言明方式の保証型情報セキュリティ監査
- 当面は、言明方式を主として検討する
- 非言明方式の保証型監査については、今後、言明方式のパイロット監査実施の結果を踏まえて検討を加えていくこととする

# 言明方式の保証型監査

- 言明方式の保証型情報セキュリティ監査

  「『監査対象の経営者が言明した情報セキュリティマネジメントのリスク低減策』の全てが存在し、機能していることについて、合理的な方法と証拠に基づき監査人が意見を述べること」

- その具体的枠組み
  - 何を監査するのか
  - 合理的保証とは
  - 言明とは何か

# 言明方式の保証型監査：　何を監査するのか　合理的保証とは

## 監査の対象

「被監査対象の経営者が言明した情報セキュリティのリスク低減策の全てが監査期間において運用されていること」

## 合理的保証

「保証型監査の監査人が情報セキュリティ監査基準に従って監査を実施した結果、言明と監査人が把握した事実との間に相違がないことについて、相当程度の心証を得たとの専門家としての判断を結論として述べること」

# 言明方式の保証型監査： 言明とは何か

## 言明

「被監査対象の経営者が監査報告書の利用者に対して行う、『監査の対象となる組織体において情報セキュリティに関するマネジメントとコントロールを適切に行っている旨』を内容とする表明」

## 言明の要件

1. 言明の主体が示されていること
2. 監査対象が一義的に定められていること
3. 監査人が監査するに足りる内容の事実に関する主張が存在すること

# 言明方式の保証型監査： 合理的保証とは

合理的保証において監査人が相当程度の心証を得るためには、監査を行うにあたり以下の事項を適切に実施する必要がある

1. 尺度の選択
2. 証拠の収集
3. 証拠の評価
4. 事実の認定
5. 認定した事実の尺度へのあてはめ

## 監査人の留意事項

- ✓ 適切に実施して適正かつ充分な証拠を入手する意味を含む
- ✓ 相当程度には、社会的に容認される程度などの意味が含まれる

# 目　次

- 情報セキュリティ監査とは
  - 情報セキュリティ監査制度
  - ＪＡＳＡの取り組み
- 保証型監査促進プロジェクトの紹介
  - 背景と目的
  - 保証の本質
  - 保証型情報セキュリティ監査の類型
- 今後の保証型監査の展開

# 今後の取り組み

- パイロット監査での実証
  - Mタスク
  - Gタスク
  - Hタスク
- 監査報告書雛形の整備
- 言明の雛形
- 合意方式の保証型情報セキュリティ監査の検討
- 管理手続き、監査手続きの雛形等の整備