

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種類
- 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、

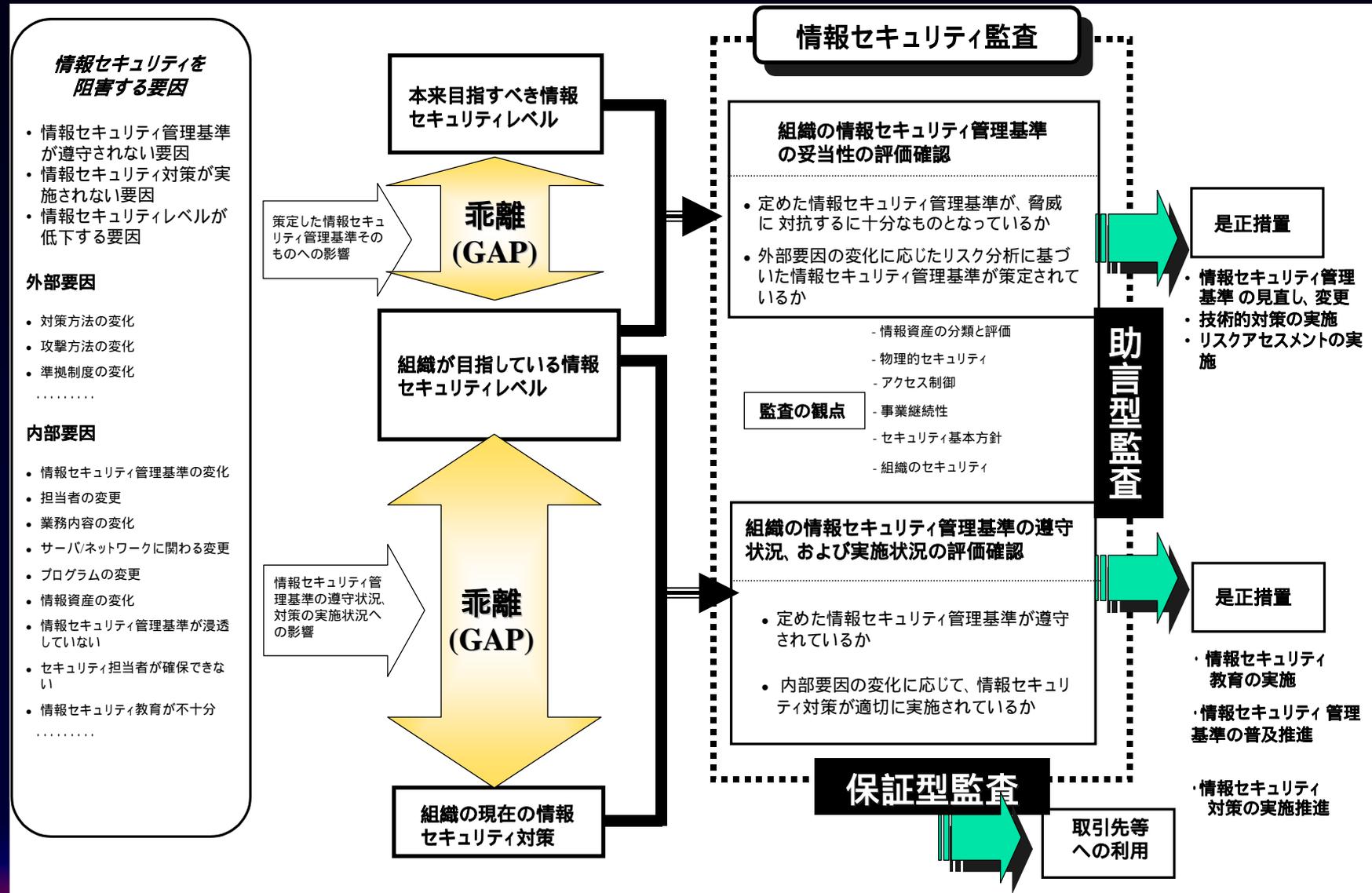
- 情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、
- リスクアセスメントに基づく適切なコントロールの整備、運用状況を、
- 情報セキュリティ監査を行う主体が独立かつ専門的な立場から、
- 国際的にも整合性のとれた基準に従って
- 検証又は評価し、
- もって保証を与えあるいは助言を行う活動

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

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)

JASA 特定非営利活動法人
日本セキュリティ監査協会
Japan Information Security Audit Association

■情報セキュリティ監査制度とは ■セミナー ■監査人名簿 ■お問い合わせ ■ダウンロード ■プライバシーポリシー ■トップ

JASAについて
会長のご挨拶
設立の趣意
JASAの位置づけ
活動内容
部会活動
組織
地図
監査人資格制度
審査委員会
監査企業紹介制度
成果物
役員・委員・講師

2003年4月1日、経済産業省による「情報セキュリティ監査制度」が施行されましたが、この制度を着実に浸透させていく為の運営体として、この度、「特定非営利活動法人日本セキュリティ監査協会」を設立いたしました。

当協会は、外部・内部を問わず情報セキュリティ監査を実行しようとしている企業・組織・監査人の方々が会員となり、情報セキュリティ監査の「あり方」や「やり方」を研究すること、ならびに、監査と監査人の質の確保を行うことにより、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして情報セキュリティ監査制度が機能することを目指し、積極的な活動を展開していく所存です。これまで以上のご支援を賜ります様、宜しく願い申し上げます。

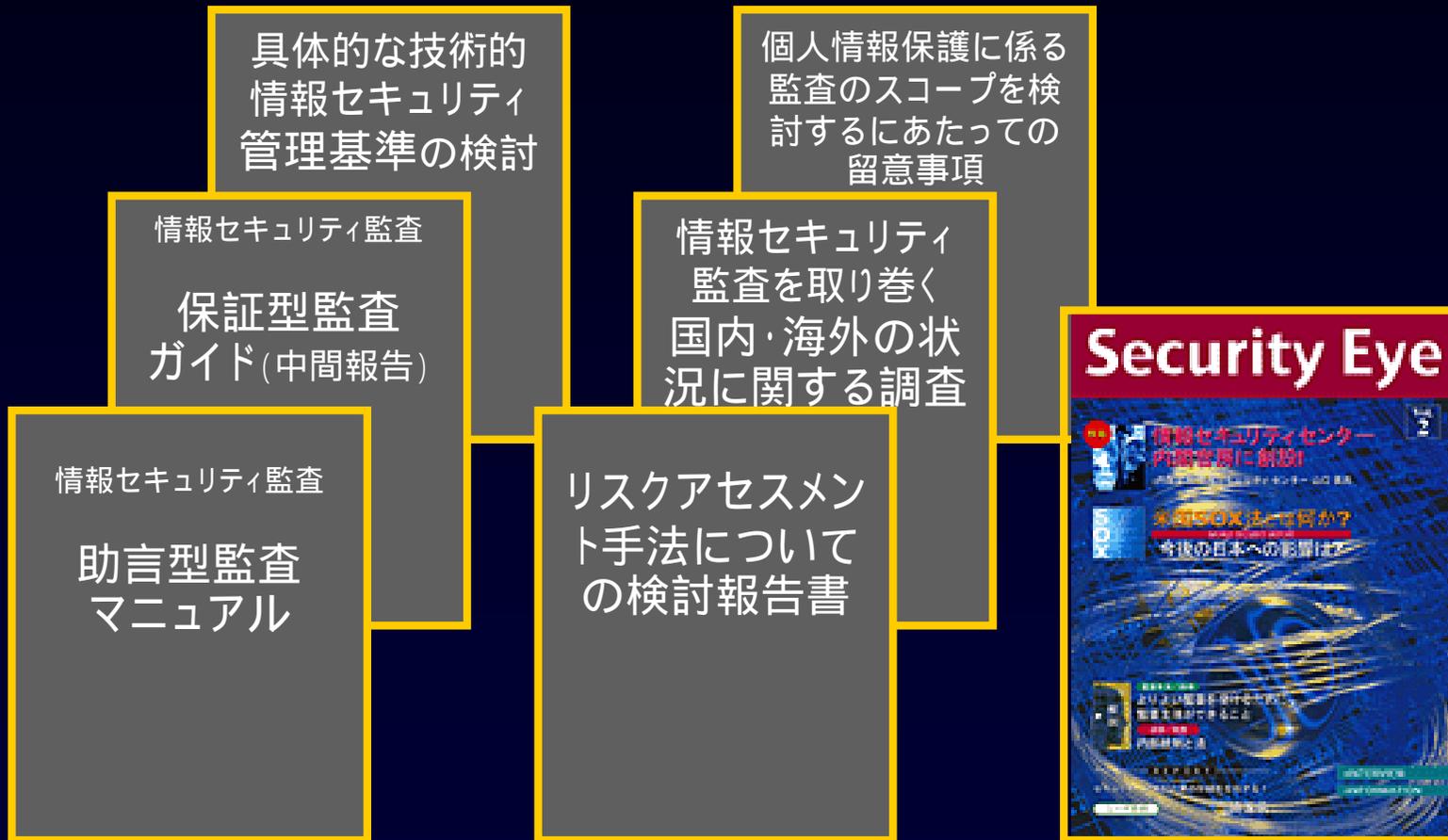


平成15年10月吉日
特定非営利活動法人 日本セキュリティ監査協会
会長 土居 範久

[情報セキュリティ監査制度とは](#) | [セミナー](#) | [監査人名簿](#) | [お問い合わせ](#) | [ダウンロード](#) | [プライバシーポリシー](#) | [トップ](#)

Copyright 2004 Japan Information Security Audit Association. All rights reserved.

代表的な成果物



公認情報セキュリティ監査人資格制度

特定非営利活動法人
日本セキュリティ監査協会
Japan Information Security Audit Association

■ 情報セキュリティ監査制度とは ■ セミナー ■ お問い合わせ ■ ダウンロード ■ プライバシーポリシー ■ トップ

公認情報セキュリティ監査人資格制度

制度概要 専門分野 取扱い 研修・トレーニング コース 登録申請・維持手数料 監査人 倫理 資格維持 プログラム 登録申請 書類 登録申請 手順

会長挨拶
認定結果速報
監査人資格制度とは
資格登録申請申込み
研修内容
問い合わせ
FAQ (よくある質問)
監査人倫理規定
登録申請要綱・様式 のダウンロード

制度概要

特定非営利活動法人日本セキュリティ監査協会は、経済産業省により施行された「情報セキュリティ監査制度」のもと、「公正かつ公平な情報セキュリティ監査」が実施され、情報社会にとって有益なものとして機能することをめざし、情報セキュリティ監査人に求められる知識・経験・技術に応じて、以下の資格を認定する。

資格認定には、監査人としての能力(知識・経験・実証された能力)、監査人としての適切な行動(倫理基準への遵守)が求められており、協会は、これら資格認定の前提となる知識・経験を修得するための研修・トレーニングコースを開催する。

この資格制度を運営するために、ISO/IEC17024(適合性評価-要員の認証を実施する機関に対する一般要求事項)に則り、協会内の独立した機関として資格認定委員会を設けて、資格制度の運用と資格に係るレベル認定を行う。

資格認定の有効期間は資格認定後の翌年度始(4月1日)を基準として3年間であり、資格維持のためには別に定める通り活動実績をポイント換算し、一定水準以上を満たすことが求められる。

なお、関連資格の保有者に対しては、関連資格の保有や関連資格に基づいた経験により、資格認定要件の一部を免除・代替する。当特例措置は期間限定措置として、2005年12月末までに申請書類を提出し、研修・トレーニングコースを修了した者に対して認定を行う。

審査制度の拡充



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、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、公平な第三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。

情報セキュリティ監査企業台帳

情報セキュリティ監査企業台帳 - 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(O)

情報セキュリティ監査企業台帳 平成17年度登録分 経済産業省TOP 情報セキュリティ政策、緊急情報TOP

TOP 全国版 北海道 東北 関東 中部 近畿 中国 四国 九州 沖縄

情報セキュリティ監査企業台帳について

「情報セキュリティ監査企業台帳」とは、「情報セキュリティ監査」を行う主体を登録するものです。今回登録いただいた企業／組織には監査法人、情報セキュリティベンダー、システムベンダー、情報セキュリティ専門企業、システム監査企業など、様々な主体が含まれています。こうした多様な主体によって、それぞれの特性、ユーザーのニーズに応じた多様なサービスが提供されることが期待されます。

また、当該台帳は地域の企業等に対する継続的な監査提供に配慮するため、全国を9つの地域に分けて登録しております。

◆情報セキュリティ監査企業台帳は北海道～沖縄まで9の地域に分類されており、閲覧したい地域をお選び頂くと各地域の企業がリストされます（ページ上の地域名をクリックして下さい）。

企業リストは右記の7つのテーマ別に準備されており、テーマを切り替えることにより各企業の特色／傾向を概略的にご覧頂けます。

詳しい企業概要・監査概要は登録申告書（HTML形式、PDF形式）をご覧ください。なおリストの企業名をクリックすると、その企業のホームページに繋がります。（一部リンク無し）

関東	IT関連企業内容						
	IT関連業務内容	申告書	システム監査	システム開発	システム運用・保守	セキュリティ監査	セキュリティサービス
あ	IT関連業務内容	○	○	○	○	○	○
あ	セキュリティ関連業務	○	○	○	○	○	○
あ	参加するIT関連機関	○	○	○	○	○	○
あ	得意とする監査対象の分野・業種	○	○	○	○	○	○
あ	得意とする監査形態	○	○	○	○	○	○
あ	監査従事者が持つ取得済監査関連資格	○	○	○	○	○	○
あ	取得している監査関連の認証	○	○	○	○	○	○
あ	あ	あ	あ	あ	あ	あ	あ
あ	(株)アークン	○	○	○	○	○	○
あ	ア&ISH	○	○	○	○	○	○
あ	アイエックス・テクノロジー	○	○	○	○	○	○
あ	アイエックス・テクノロジー	○	○	○	○	○	○
あ	(株)HSC	○	○	○	○	○	○
あ	アイエックス・フレック(株)	○	○	○	○	○	○
あ	アイジネット・ラボ(株)	○	○	○	○	○	○
あ	(株)ITサービス	○	○	○	○	○	○

PDFページのご利用方法

PDFページをご覧になるにはAdobe Reader 5.0以上が必要です。パソコンにインストールされていない方は、下記よりダウンロードしてください。使用方法に関してはアドビ社のホームページをご覧ください。

お問い合わせ先

経済産業省 商務情報政策局
情報セキュリティ政策室
電話 03-3501-0397(直通)
FAX 03-3501-6639
電子メール it-kansa@meti.go.jp

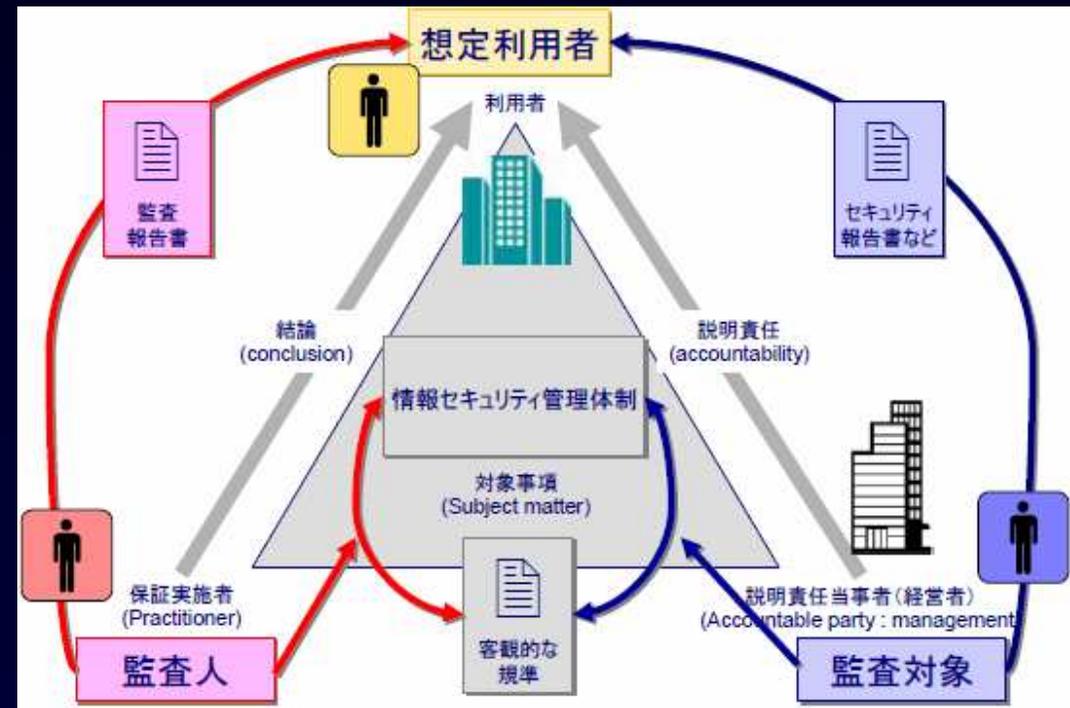
担当:石飛、金井

Copyright (C) 2005 Office of IT Security Policy, METI All rights reserved.

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に多くの方の思いが一致している



■ JASSA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

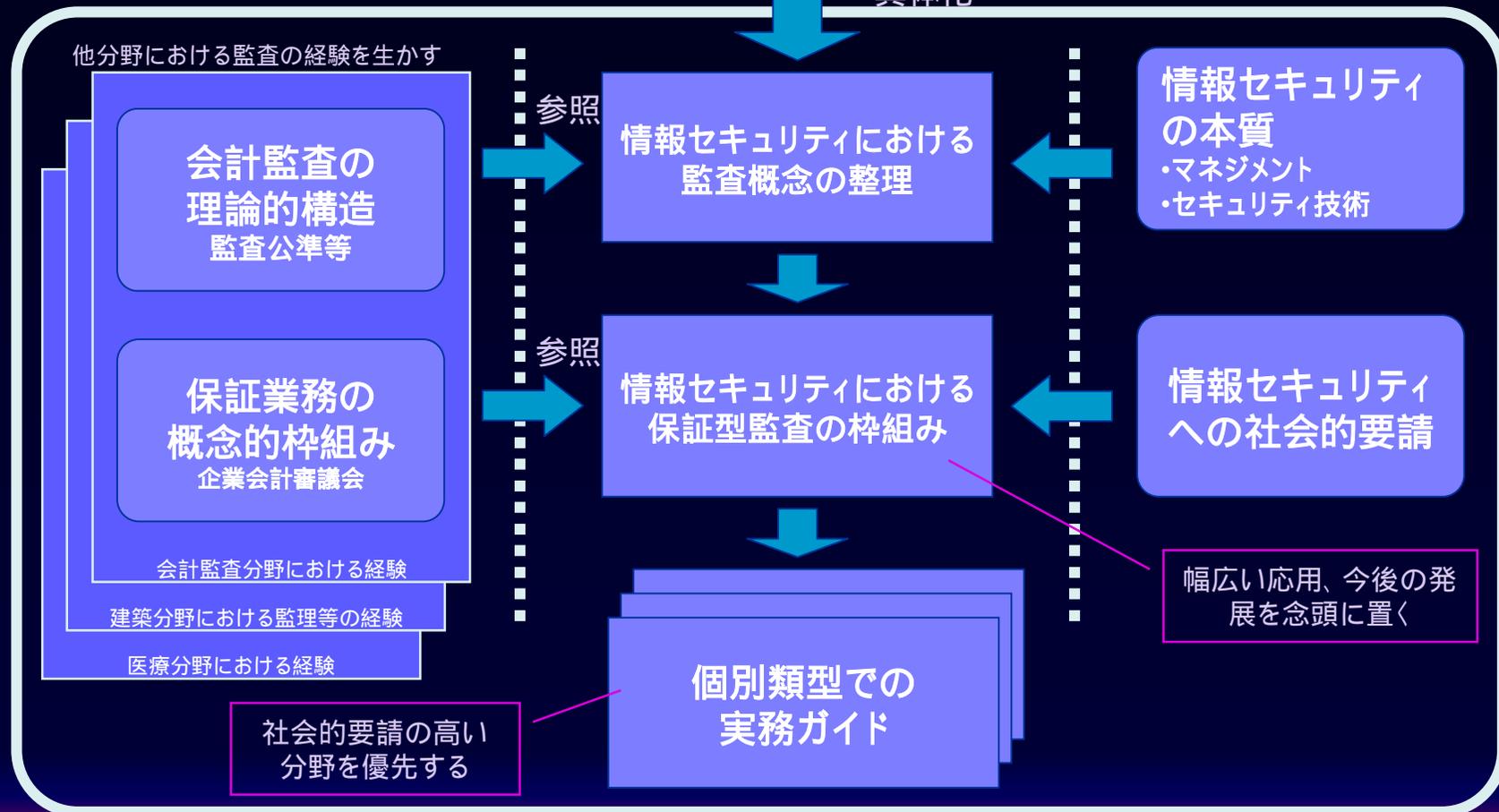
検討すべき課題の認識

- 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掘する
- 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

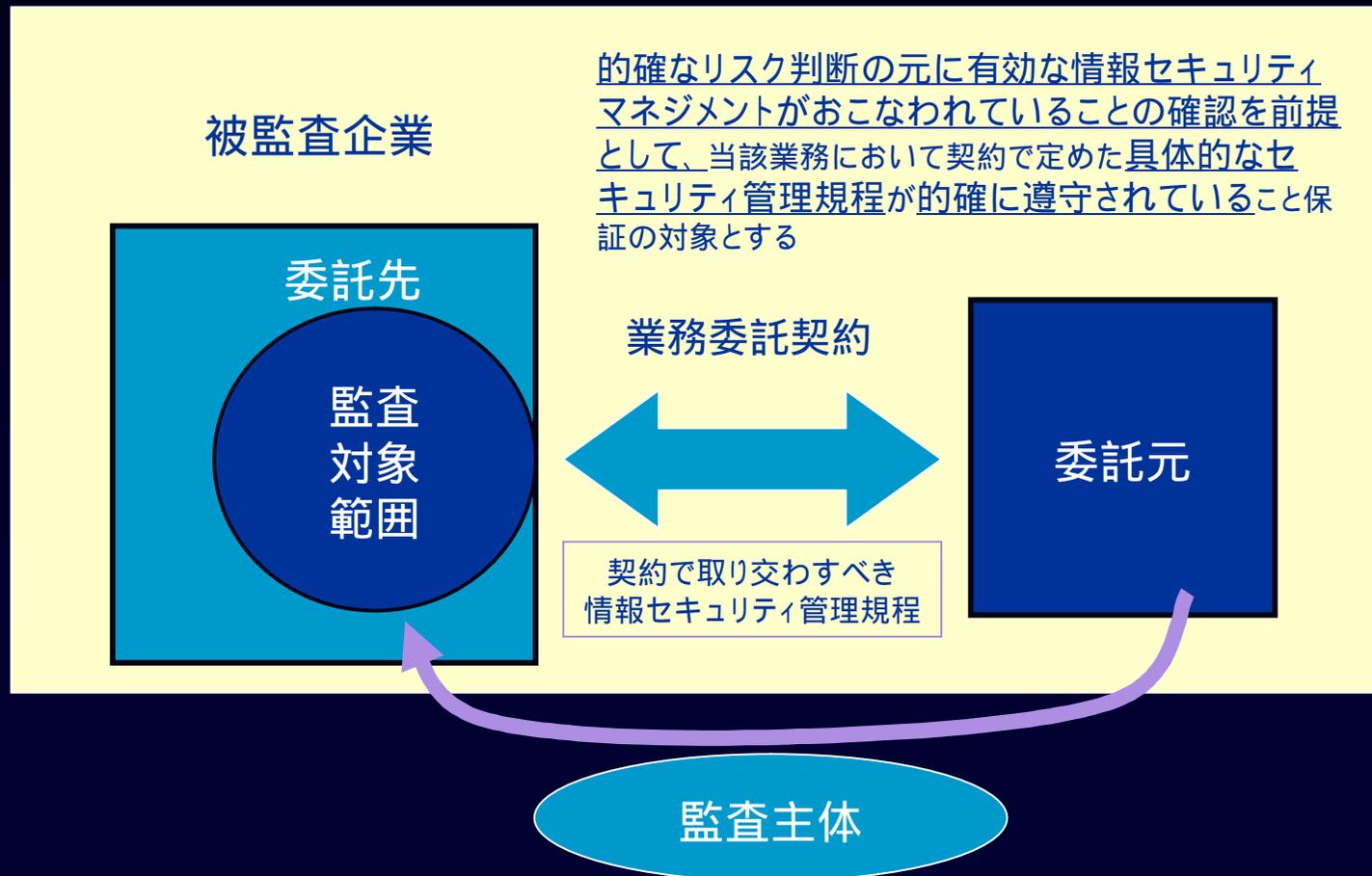
検討の枠組み

経済産業省
情報セキュリティ監査研究会 報告書

具体化



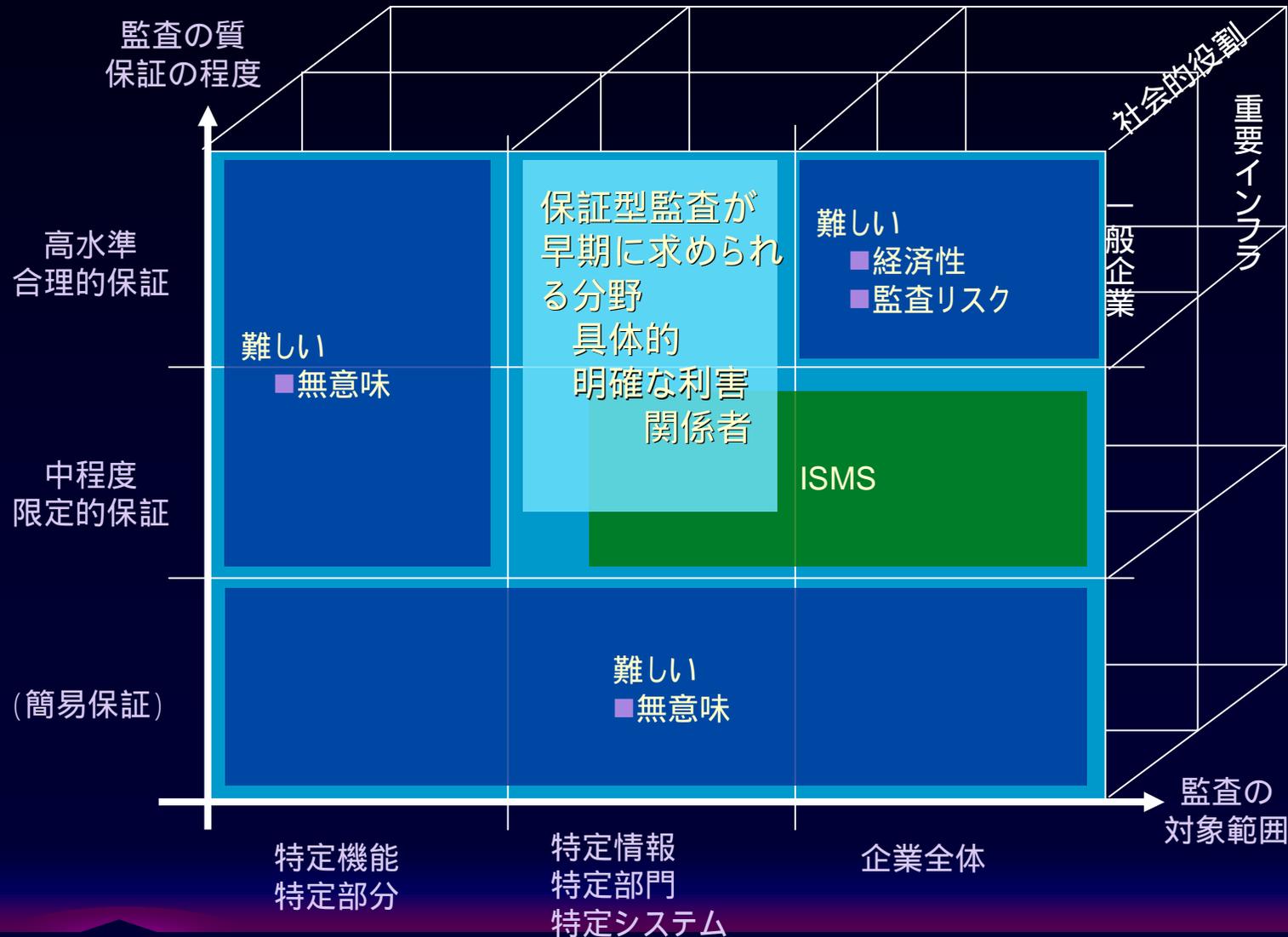
業務委託先を例とした保証型監査の枠組み検討



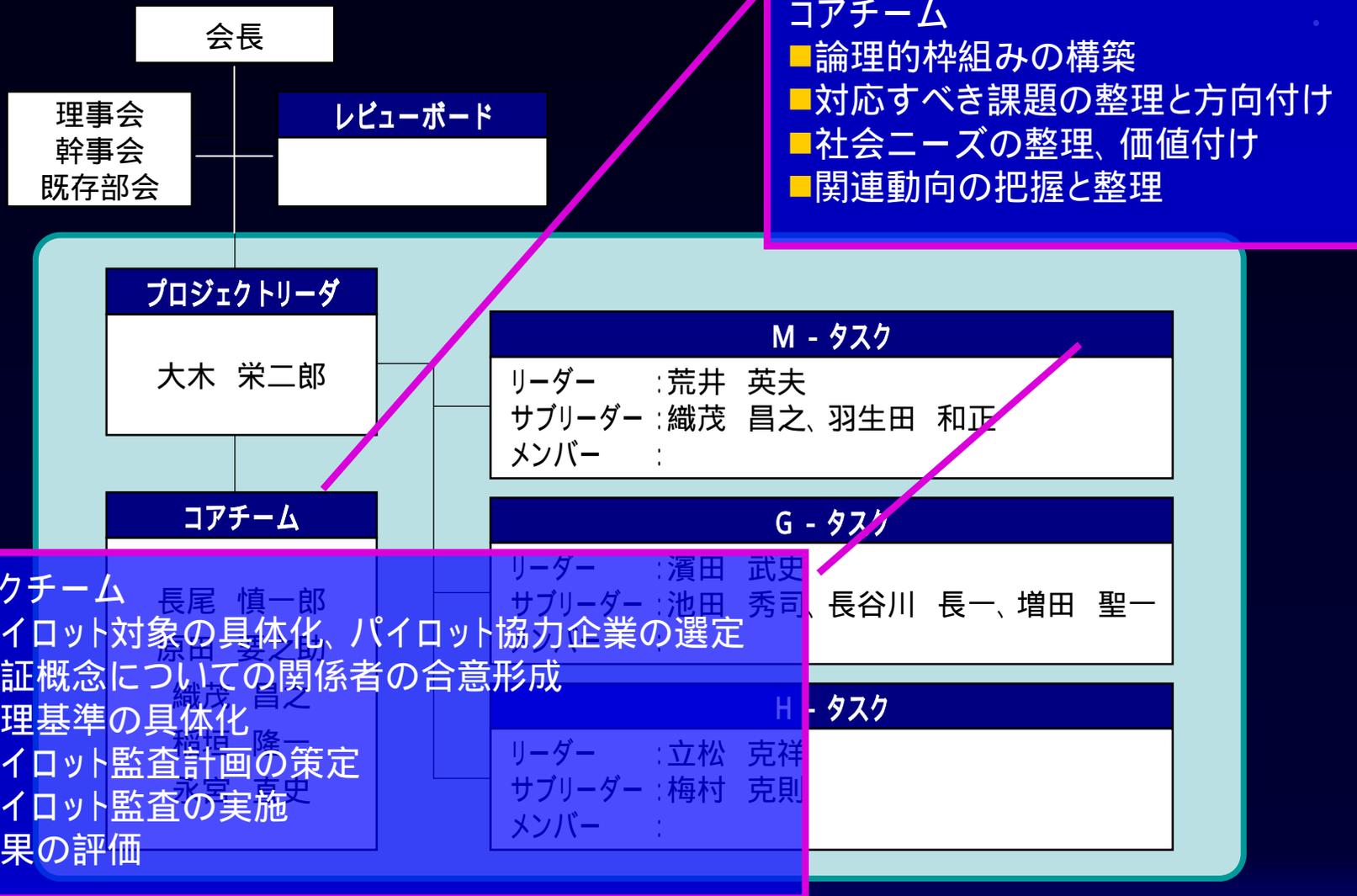
的確なリスク判断の元に有効な情報セキュリティマネジメントがおこなわれていることの確認を前提として、当該業務において契約で定めた具体的なセキュリティ管理規程が的確に遵守されていること保証の対象とする

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



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十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