情報セキュリティ監査の全体図

保証型情報セキュリティ監査の全体図　　（網掛けは情報セキュリティ監査契約の検討範囲）

<table>
<tr><th>#</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th></tr>
<tr><td rowspan="2">業務のプロセス</td><td>準備</td><td colspan="5">情報セキュリティ監査業務</td><td></td><td>後工程（オプション）</td><td>後工程</td></tr>
<tr><td>依頼、提案</td><td colspan="2">監査計画書作成業務(3条)</td><td colspan="2">監査実施業務(3条)</td><td colspan="2">監査報告業務(3条)</td><td>改善実施確認
保証1の保障期間</td><td>(保証2の保証期間)</td></tr>
<tr><td>甲：監査依頼者
丙：被監査対象</td><td>監査依頼書
(2条)</td><td rowspan="2">提案書すり合わせ、合意
↓
「監査基本計画書」
（2条、3条、13条）</td><td rowspan="2">「監査詳細計画書」
（3条）

(確認合意)
（14条、15条）</td><td rowspan="2">(監査実施)
（17条）</td><td rowspan="2">(監査実施)
（17条）

「監査調書」</td><td>ー</td><td rowspan="2">(報告)
（21追加条）</td><td rowspan="2">(改善実施)

「改善報告」
（23追加条）
↓
(改善確認)</td><td></td></tr>
<tr><td>乙：監査実施者</td><td>↓
提案書(2条)</td><td>「情報セキュリティ監査報告書」
（21条）</td><td></td></tr>
<tr><td rowspan="4">甲、丙、乙の連絡

契約</td><td></td><td>監査計画検討会開催(14条)
契約の締結</td><td>・甲、乙、丙による実施内容、方法の確認</td><td></td><td></td><td></td><td>監査結果の承認
（22条）</td><td>改善実施確認</td><td></td></tr>
<tr><td>納品物　6条</td><td></td><td>・連絡協議会設置
（11条）</td><td colspan="3">・乙による丙を対象とした監査の実施
（17条）</td><td>保証内容の確認
（31条、32条）</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">契約の1つの区切り
（1条）</td><td colspan="4">契約の1つの区切り(1条)</td><td>(保障期間)
保証1→
（31条）</td><td>契約のオプション
保証2→
（31追加条）</td></tr>
<tr><td>体制</td><td></td><td colspan="2">業務従事者
（9条）
責任者、主任担当者
(10条、11条)</td><td colspan="4">体制は左に同じ
再委託(19条)</td><td></td><td></td></tr>
<tr><td>納品物</td><td>提案書</td><td>監査計画書</td><td></td><td colspan="2"></td><td>「情報セキュリティ監査報告書」</td><td>保証1の内容</td><td>保証2の内容</td><td></td></tr>
<tr><td>関連文書</td><td>監査依頼書
提案書</td><td>監査計画書
(監査基本計画書)</td><td>監査計画書
(監査詳細計画書)</td><td></td><td>監査調書</td><td>納入物　(5条)
「監査報告書」
（21条）</td><td></td><td></td><td></td></tr>
<tr><td>前提</td><td>当全体図</td><td colspan="2">監査依頼書、提案書すり合わせ、合意</td><td colspan="2">監査実施業務委託、受託の合意
情報セキュリティ監査の期間が長期にわたる場合は中間報告を考える。(今回対象外)</td><td colspan="2">同左</td><td>改善実施確認業務の委託、受託の同意</td><td></td></tr>
<tr><td>保証</td><td>保証要望内容の確認</td><td></td><td>納入期限(7条)</td><td></td><td></td><td></td><td>納入期限(8条)</td><td></td><td></td></tr>
</table>

情報セキュリティ監査の全体図

文書　（項目）

依頼書

1. 本件業務の名称
2. 本件業務の内訳
（1）目的（情報セキュリティ監査の範囲、
（2）保証内容、　）
（3）対象部署（対象部署名、業務内容、組織構成、体制、
（4）対象システム概要、対象業務
3. 委託料（希望予算）
4. 本業務の作業期間（実施希望期間、時期）
5. 納入期限
6. 提案期限

提案書

1. 本件業務の名称
2. 内容・目的:
・情報セキュリティ監査の範囲、
・保証内容、保証事項(対象、範囲))
・対象（対象部署名、業務内容、組織構成、体制、
・対象システム概要、対象業務範囲ー＜以上依頼書の確認＞
・監査体制（責任者、担当者）
・監査方法
3. 委託料（見積り額）
4. 監査実施時期・期間
5. 納入期限
6. 実施内容（・甲、乙、丙の役割
・実施制限事項・要望事項

情報セキュリティ監査の種類

スポットか、定例か
　事務的業務、技術的業務、総合

中間納品物
　一定期間以内（たとえば2W以内）の監査の場合は考えない

納品物一覧

納品物
1. 情報セキュリティ監査計画書（基本計画書、詳細計画書に分けることあり　ー下記）

2. 情報セキュリティ監査報告書

計画書(基本計画書、詳細計画書)　状況に応じて基本計画書と詳細計画書に分ける

目的（情報セキュリティ監査の範囲　）
・対象（対象部署名、業務内容、組織構成、体制、システム概要、一依頼書の確認
・保証内容、保証事項、保障期間
・納品物（報告書等）、報告内容、
・保証内容、保証事項(対象、範囲)
・監査体制（責任者、担当者）、推進体制
・監査方法、推進方法
・監査実施時期・期間
・甲、乙、丙の役割
・実施上の要望事項、要望環境
・必要資料
　監査対象文書、監査ツールの利用、
・甲または丙からの監査提供文書
・実施スケジュール
覚書：委託料
　　納入期限（1）　計画書の納入
　　納入期限（2）　報告及び監査報告書の納入

保証について

保証1：現状において保証できる事項
保証2：ある目的のために必要な改善・是正を実施したうえで保証できる事項
保障期間：設定する　たとえば半年とか

保証の文言　①情報セキュリティ監査基準による
　　②検討中の保障型監査の案による　☆

情報セキュリティ監査の全体図

① 情報セキュリティ監査基準の保証型監査についての解説より具体的に表現して見る。
このような表現についての検討をする。

②未検討：中間報告ー監査が長期間（おおむね1ヶ月以上）になる場合に、中間報告の実施を検討する。今回は未検討。

（例示） 保証1の内容
保証2の内容

保証要望内容(例) 1．従業員以外の者による不正な情報システムへのアクセスが起こらない。万一発生しても直ちに発見でき、その原因が特定できる。 2．従業員による犯罪行為は発見でき、原因や状況が追究できる。 3．社外との情報の伝達に漏洩は発生しない。 4．万一の障害に対するシステムの回復は1日以内に回復できる。 5．復旧手順書による手順は実現できる状態である。 6．〇〇社との契約条件である”　　”を満たしている。 7．設計書記載の情報セキュリティ要件は実現されている。 8．SLA〇〇を満たしている。 9．プライバシーマーク認証に適合する情報セキュリティ管理状況であるか	保証1、保証2の表現 1．現行規程を遵守し、現状の運用を維持することでは従業員以外の者による情報システムに対する不正なアクセスは発生しないことを保証する。 また、万一発生した場合においても発見が出来、原因を特定する仕組みが機能していることを保証する。 （保証の根拠：　　） 2．
保証の前提としての検討項目 ・Pマーク認証取得 ・Pマーク認証取得 ・ISMS認証取得 ・内部統制の状況 ・事件・事故の状況 ・前回の情報セキュリティ監査の状況 ・前回の会計監査の状況 ・IT保険、個人情報保険の加入状況	保証内容（多段階保障）の検討項目 ・対象となるシステムの範囲 ・対象組織 ・対象期間又は期日 ・監査項目 ・保障金額