情報セキュリティ監査サービス

サービス仕様書

令和４年８月１日

キートンコンサルティング株式会社

1 本サービスの基本情報

1) サービス名称

サービス名称：**情報セキュリティ監査サービス**

2) サービスの提供において用いる基準

【経済産業省】**情報セキュリティ監査基準**

https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf

3) サービス提供に係る技術責任者

公認情報システム監査人（CISA）：登録番号 CISA-17142537

4) 実施プロセス

本サービスは、標準として以下の実施プロセスにより構成されるものとします。

ただし、お客様との協議によりプロセスの追加・変更を可能とします。

- ①委託業務計画書作成
- ②組織・部門・システムの調査・確認
- ③監査基本計画書の作成
- ④被監査部門・システムの事前調査
- ⑤監査実施計画書の作成
- ⑥監査準備
- ⑦監査手続きの実施（本監査）
- ⑧監査調書の作成、監査意見のとりまとめ
- ⑨監査報告書の作成
- ⑩監査報告会の実施
- ⑪フローアップ監査※オプション

2 具体的な実施プロセス

本サービスでは標準として①～⑩（⑪はオプション）として以下のプロセスを実施することにより情報セキュリティ監査サービスを提供します。

① 委託業務計画書作成

本サービス提供に係る委託契約に基づき「委託業務計画書」を作成し、お客様に提示して承認を得ることにより、本サービスの全体的な実施計画を明らかにすると共に、業務推進に関するお客様と当社との共通認識を醸成します。

「委託業務計画書」に記載予定の内容は以下の通りです。

委託業務計画書：想定される委託実施計画書の記載内容

1　業務の範囲
1．1　業務の目的
1．2　業務の範囲
2　業務実施体制
2．1　当社の実施体制、氏名、役割、保有資格など
2．2　貴社の実施体制、氏名、役割など
3　業務実施内容
3．1　各プロセスの概要
3．1．1　被監査部門・システムの調査・確認
3．1．2　監査計画書案の作成
3．2　各プロセスの詳細
3．2．1　被監査部門・システムの調査・確認
3．2．2　監査計画書案の作成
4　スケジュール案
5　コミュニケーションルール
5．1　連絡先
5．2　連絡方法
5．3　議事録
5．4　報告等
6　成果物
7　セキュリティ対策※お客様の求めるセキュリティ対策への対応

② 組織・部門・システムの調査・確認

「監査基本計画書」を作成するために、お客様の組織・部門状況や各組織・部門にて保有する情報システム、規程等について資料確認やインタビュー等により調査・確認を行います。調査と確認は当社を中心に実施しますが、調査に係る資料はお客様より提供されることを前提とします。

③ 監査基本計画書の作成

お客様の組織・部門・システムに関する調査・確認結果に基づき、お客様における年単位の中期的なセキュリティ監査計画を示す「監査基本計画書」を作成し、お客様に提示して承認を得ます。「監査基本計画書」は、本サービス対象を含む概ね３年程度の期間におけるお客様の情報セキュリティ監査の方針や実施目標、監査範囲、大まかな実施時期等の項目を記述した計画書に位置付けられるものであり、お客様において維持管理を行い、システム状況やセキュリティ対策状況に基づき、適宜見直しが行われる想定です。

「監査基本計画書」に記載予定の内容は以下の通りです。

監査基本計画書の作成：想定される監査基本計画書の記載内容

A　監査の目的
B　監査対象とする範囲（例えば、住民基本台帳システム）
C　監査の判断尺度とする管理基準等
D　監査対象とする期間又は期日
E　監査対象とする段階（例えば、運用段階）
F　監査対象に係る監査目標（例えば、機密性）
G　監査の重点項目
H　監査業務の管理体制
I　他の専門職の利用の必要性と範囲
J　監査スケジュールの概要

④ 被監査部門・システムの事前調査

「監査基本計画書」に基づき、本サービスの被監査部門および当該部門が所管・利用するシステムについて事前調査を行います。

事前調査は、以下を目的に実施することを想定しています。

事前調査の目的

1　監査対象の業務を理解する
2　重点を置く必要が有る重要な領域を認識する
3　リスクの存在が予想される領域を認識する
4　監査業務の遂行で使用する情報を取得する

⑤ 監査実施計画書の作成

本サービスの被監査部門および当該部門が所管・利用するシステムの情報等に基づき、本サービスが対象とする被監査部門・システムに対する情報セキュリティ監査に係る「監査実施計画書」を作成します。

「監査実施計画書」は、以下の内容を記載する想定です。

監査実施計画書：想定される監査実施計画書の記載内容

1　監査の依頼者
2　監査の目的
3　監査テーマ
4　被監査部門および監査対象システム
5　監査手続き
6　監査対象期間
7　監査場所
8　適用する基準（監査の基準、参考とする基準）
9　管理体制
10　監査の実施
11　主な監査項目
12　監査スケジュール
13　評価基準
14　監査報告書

⑥ 監査準備

「監査実施計画書」に基づき、被監査部門に対する情報セキュリティ監査を実施する準備を行います。

監査準備としては、以下を実施する想定です。

監査準備：想定される監査準備

実施事項	内容
監査説明資料の作成	監査の意図、目的、手法、実施フロー、事前調査や事前アンケートの内容、本監査の手順および実施内容、本監査の依頼事項等を説明するための資料を作成し、被監査部門にあらかじめ配布する。
監査チェックリストの作成	情報セキュリティ監査において使用する監査のチェック事項を記載した「監査チェックリスト」を作成する。 なお、監査チェックリストについては、別途行う「事前ヒアリングの実施」「事前資料の提出依頼」の結果に基づき、監査手続きの実施（本監査）にて確認する項目を選定する。
事前ヒアリングの実施	主に「監査チェックリスト」に基づいて事前ヒアリングのリストを作成し、被監査部門に対して事前ヒアリング（またはリストに基づくアンケート回答依頼）を行い、チェック項目の概ねの状況を把握する。
事前資料の提出依頼	「事前ヒアリング」に関連し、関係する情報セキュリティに関する基準や規程、手順書、管理台帳、申請書等のリストアップと提出（写しを含む）を依頼し、入手する。

⑦ 監査手続きの実施（本監査）

準備した監査チェックリスト、事前ヒアリングの結果、事前に収集した資料に基づき、監査手続きを実施します。

「監査手続きの実施（本監査）」では、お客様との協議により、以下の手法より監査手法を選択し監査手続きを実施するものとします。

監査手続きの実施（本監査）：具体的な手法

※新型コロナウイルス感染症の情勢に応じて対面／リモート監査を実施

監査手法	内容
インタビュー	＜対面監査の場合＞ 「監査チェックリスト」に基づき、対面方式により被監査部門におけるセキュリティ対策の実施状況をインタビューにて確認する。
	＜リモート監査の場合＞ 遠隔地における会議室等の間をリモート会議ツール（Zoom、Teams、WebEX 等）にて接続し、「監査チェックリスト」に基づき、被監査部門における情報セキュリティ対策の実施状況をインタビューにて確認する。
文書記録の閲覧	＜対面監査の場合＞ 「監査チェックリスト」に基づくインタビューの後、インタビューの回答に関係する文書（基準や規程、手順書、管理台帳、申請書等）を閲覧し、情報セキュリティ対策が文書に基づき行われ、且つ記録されていることを確認する。
	＜リモート監査の場合＞ 事前収集した資料に基づき、情報セキュリティ対策が文書に基づき行われ、且つ記録されていることを確認する。なお、提出が難しい資料や多量に及び文書がある場合はリストアップを行い、別途お客様のご担当者による代理確認を依頼する。
現場視察	＜対面監査の場合＞ 「監査チェックリスト」に基づくインタビューの後、インタビューの回答に関係する現場環境（執務室、システム内容等）の実際の状況を視察して確認する。
	＜リモート監査の場合＞ お客様のご担当者に対して「視察チェックリスト」を作成し、代理にて確認を依頼する。

⑧ 監査調書の作成、監査意見のとりまとめ

監査手続きの実施結果を記録した「監査調書」を作成します。なお、「監査調書」は、「監査手続きの実施（本監査）」において実施した「インタビュー」「文書記録の閲覧」「現場視察」の結果を記録し、監査で得た監査記録、指摘事項、想定される改善案等を合わせて「監査調書」として作成し、併せて監査意見のとりまとめを行います。

⑨ 監査報告書の作成

監査調書に基づき、「監査報告書」の作成を行います。

「監査報告書」は、以下の内容を記載する想定です。

監査報告書：想定される監査報告書の記載内容

記載項目	内容
監査目的	監査目的
監査テーマ	監査の具体的なテーマや重点監査事項
監査範囲	監査対象の業務、情報システムなどの範囲
被監査部門	監査の対象とした部門
監査方法	監査で適用した監査技法
監査実施日程	監査の計画から報告までの日程
監査実施体制	監査を実施した担当者
監査項目	監査で確認した大項目
適用基準	監査で適用した基準等
監査結果	監査で確認した事実（評価できる事項を含む
指摘事項	監査結果に基づき、問題点として指摘する事項
改善勧告	指摘事項を踏まえて、改善すべき事項
特記事項	その他記載すべき事項

⑩ **監査報告会の実施**

主に「監査報告書」を使用し、被監査部門に対して監査結果の説明を行い、指摘事項や改善すべき事項がある場合は、被監査部門が策定する改善計画に係る対応策や改善策に関する助言を行います。

⑪ **フォローアップ監査※オプション**

被監査部門が対応策として策定する「改善計画」に基づき、実施された改善結果の結果と評価を実施します。

なお、本プロセスは主に本サービス前に実施したセキュリティ監査と改善計画が存在する場合、オプションにて実施するプロセスです。

以上