中小企業の情報セキュリティマネジメント指導

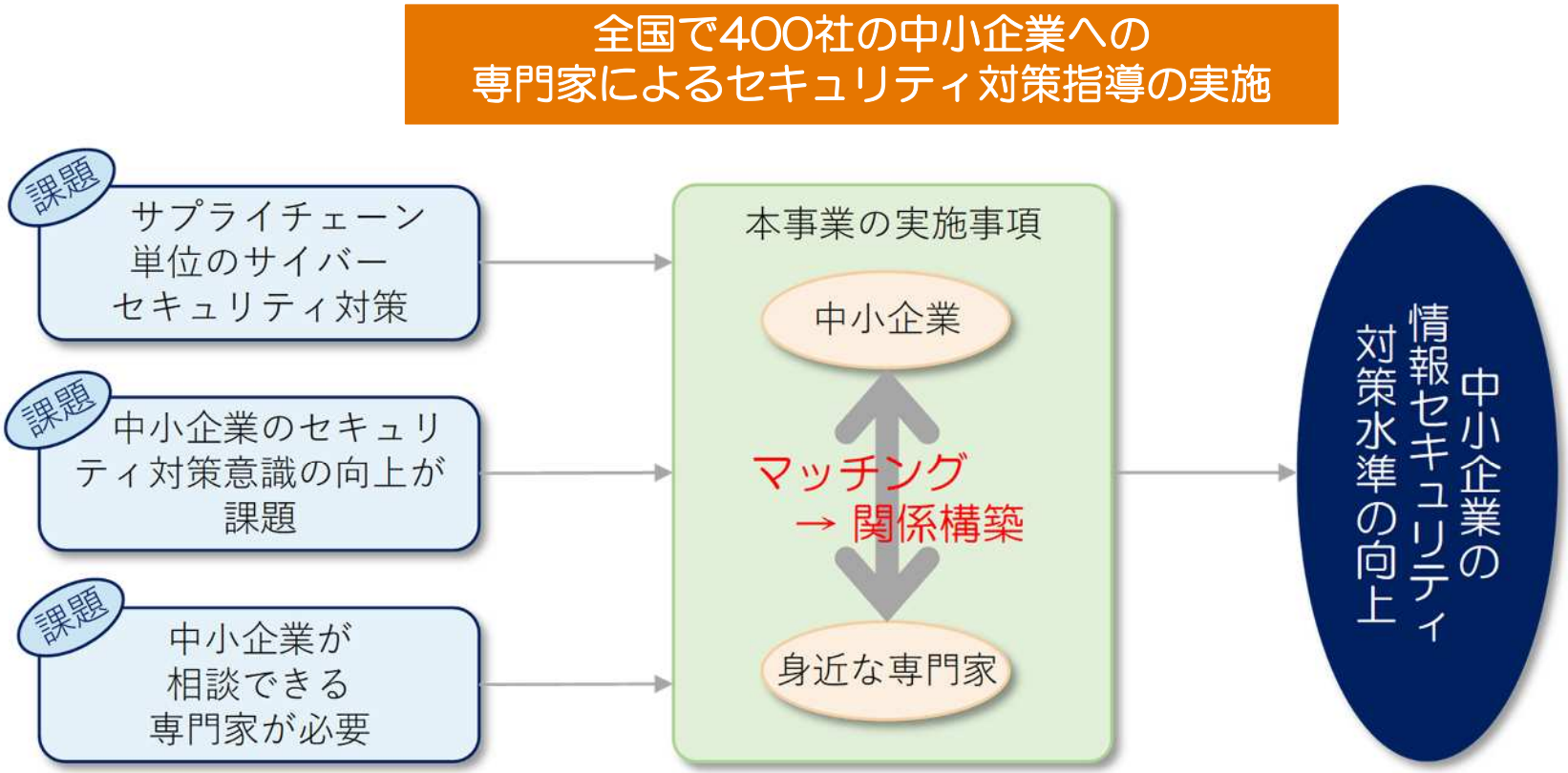
＝　指導の概要説明資料　＝

2020年10月

事務局受託機関
富士ゼロックス株式会社

「中小企業の情報セキュリティマネジメント指導業務」の目的

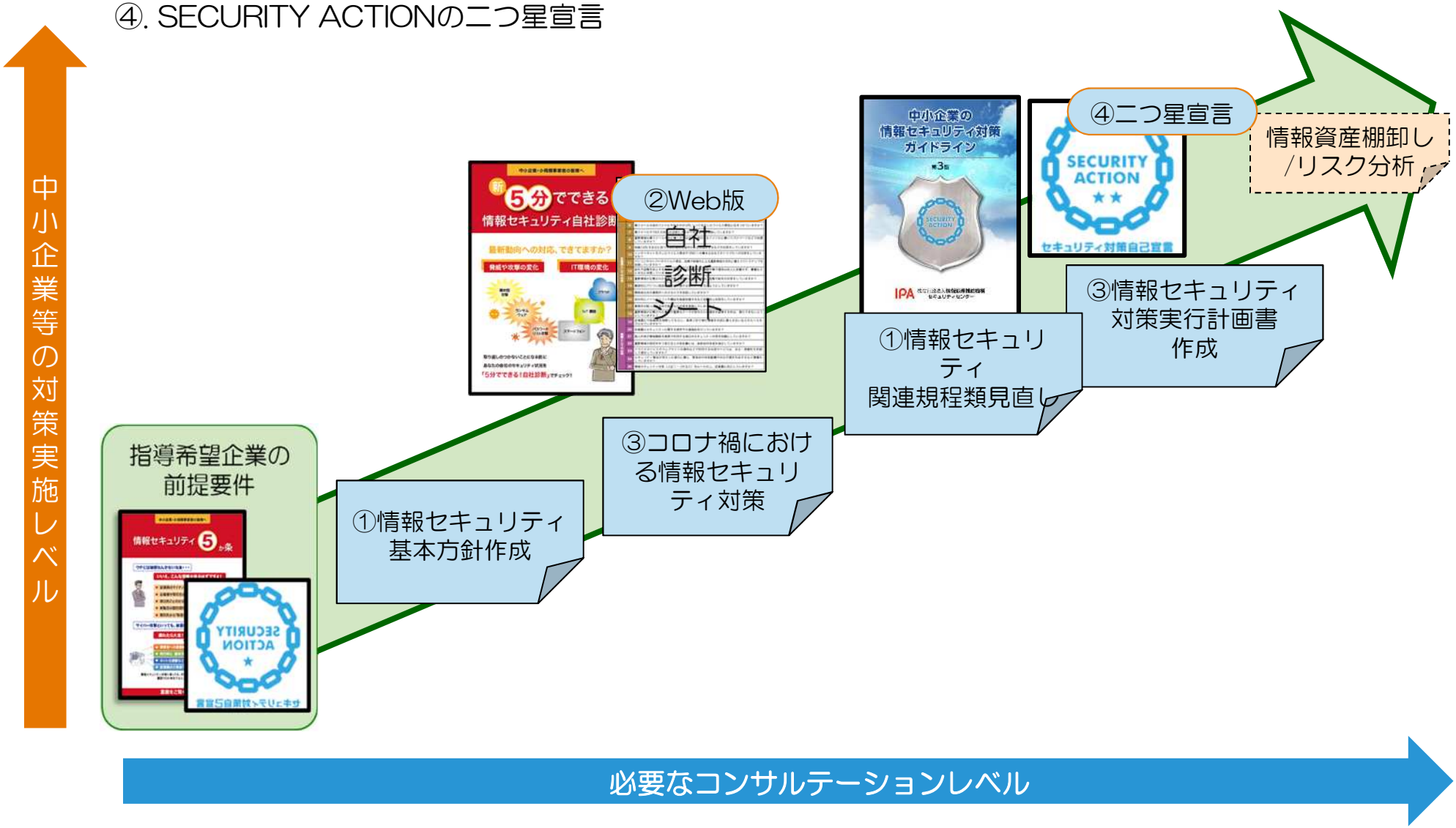
本事業は、中小企業の情報セキュリティ対策意識の向上のみならず、中小企業の情報セキュリティ対策水準の向上を継続的に推し進めることを目的とし、地域で活躍している情報処理安全確保支援士等の情報セキュリティの専門家が中小企業に訪問して指導を行うことで、中小企業と地域内の身近な専門家との関係構築を推進するものです。



今回の事業の活動と成果物

指導を受けると、以下の活動を通じて企業の情報セキュリティ対策を高度化することができます。

①. 組織的対策の基本となる、情報セキュリティ基本方針作成と必要な関連規程の点検結果
②. IPAの「5分でできる情報セキュリティ自社診断(Web版)」による、現状のリスク洗い出し結果
③. 優先順位付けにより絞り込まれた情報セキュリティ対策の、今後1年程度で実行可能な計画書（コロナ禍対策を含む）
④. SECURITY ACTIONの二つ星宣言



専門家の指導による「標準的な進め方」の全体構成

1～2週間 **事前準備#1**

*指導先企業の情報収集とヒアリングシートの作成
*IPA自社診断(Web版)の実施依頼

第１回

<u>企業の事業や情報システム環境の理解と情報セキュリティリスクの洗い出し</u>

指導先企業の事業内容と情報システム環境を把握し、自社診断の結果をもとに、経営者が認識しているセキュリティ課題（リスク）と当事業への期待値を確認します。

2～3週間 **事前準備#２**

*前回の指導を通じて得た情報をもとにした改善領域の見極め
*現行の基本方針や規程類の有無確認の依頼

第２回

<u>情報セキュリティ基本方針や関連規程整備の検討と重点改善領域の絞り込み</u>

基本方針の作成と、必要な関連規程類の検討を行うと共に、自社診断結果をもとに重点改善領域について、ディスカッションと対策の絞り込みを行います。

1～2週間 **事前準備#３**

*前回結果に加え、経営のコロナ禍対策に伴う情報セキュリティリスクの検討

第３回

<u>コロナ禍の情報セキュリティ対策を含む、重点対策の検討と優先順位付け</u>

コロナ禍で急遽対応した経営施策に対する情報セキュリティ面での対策状況を確認し、必要なアドバイスを行うと共に、重点対策と合わせた今後の実行計画を検討します。

1～2週間 **事前準備#４**

*優先順位と実現性を考慮した実行計画案の作成

第４回

<u>情報セキュリティ対策の成果物レビューと訪問指導全体のまとめ</u>

専門家がまとめた実行計画案（一年間程度）についてディスカッションし、合意形成を図ります。また企業側で作成した基本方針や規程の見直し案について、マネジメントシステムの実効性の視点からレビューを行い、二つ星の自己宣言手続きを進めます。

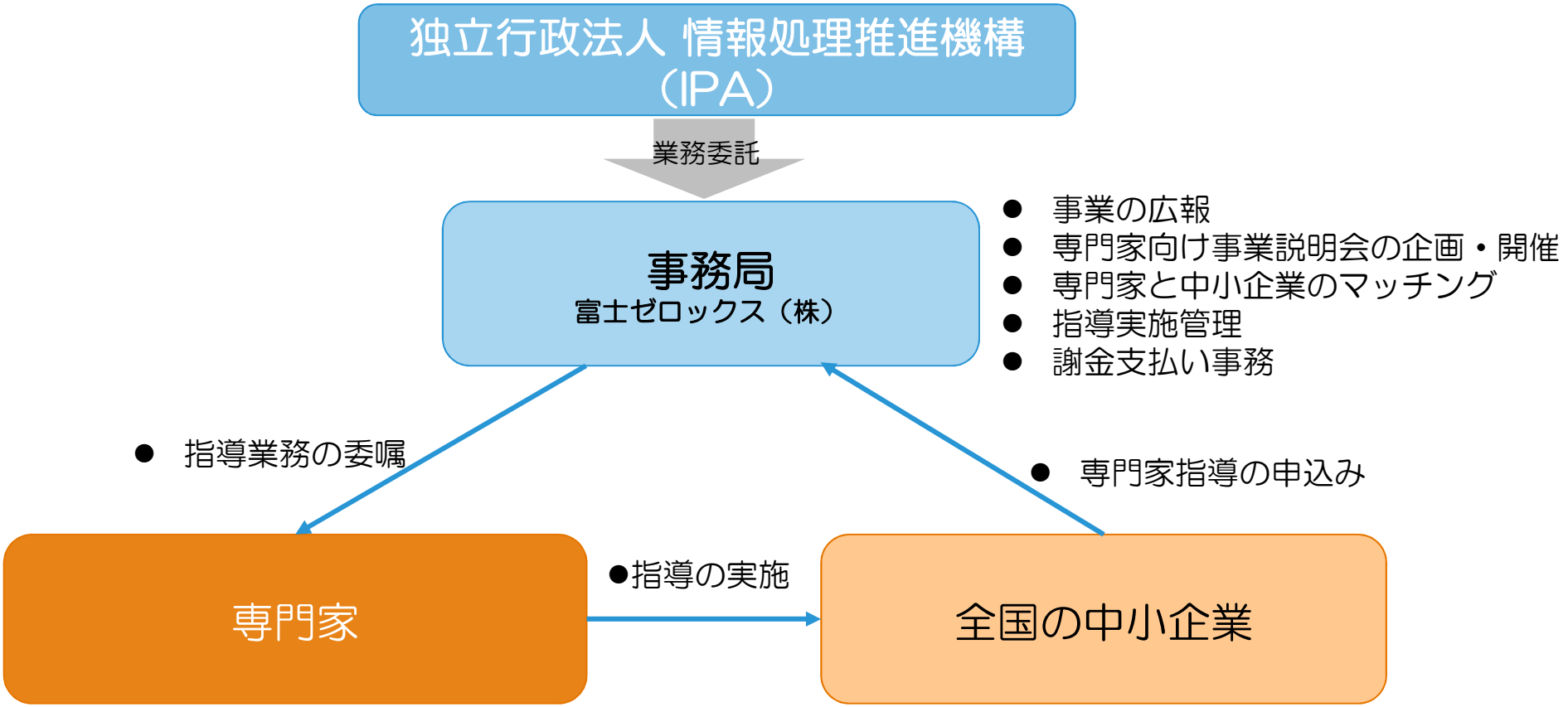
計2ヶ月程度

本事業の実施体制

本事業は、独立行政法人情報処理推進機構が実施し、その事務局業務については、富士ゼロックス株式会社に委託しています。

専門家指導のお申込みやその後の手続きは、事務局（富士ゼロックス内）宛にご連絡ください。

また、実際の指導業務は事務局から委嘱された専門家が担当します。初回指導から最終回（4回目）までの期間は、専門家とコミュニケーションを図りながら進めて頂きます。



指導の申し込みにあたって、よくある質問

【質問１】
指導を受ける側は、どのようなメンバーを集めればいいですか？
【回答１】
情報セキュリティ関連業務等の担当者、マネージャクラス、経営層を想定しております。なお、全４回の回毎に指導テーマが異なるため、テーマに応じたメンバーにご参加いただければ結構です。詳細は、指導される専門家と調整いただきます。

【質問２】
企業側で指導に参加すべき人数は、何人くらいですか？
【回答２】
明確な人数の規定はありませんが、専門家は原則1名での指導になりますので、1～5名くらいの人数が適切かと思います。

【質問３】
指導1回あたりの所要時間はどのくらいかかりますか？
【回答３】
指導1回あたり2時間程度を想定しています。

【質問４】
4回の指導は、開始から終了までどれくらいの期間がかかりますか？
【回答４】
期間は、１ヶ月半～2ヶ月程度を想定しています。

【質問５】
企業側で行うべきことはどのような内容になります？
【回答５】
各指導回の事前準備を対応していただきます。具体的な内容については指導する専門家からご案内いたします。
なお準備作業につきましては専門家のサポートを受けながら実施いただきますので、ご負担にならないように配慮させていただきます。

（事前準備例）
- 提供可能な社内資料の準備(企業紹介のパンフレット、IT関連管理資料　等)
- 情報セキュリティ自社診断の実施（約5分でできます）
- 出席メンバー選定(経営者/従業員等)
- 情報セキュリティ基本方針(案)の検討
- 改善施策の実現性の検討(実現のための課題や対策の事前検討　　他

【ご参考】「標準的な進め方」の詳細（１）

第1回　企業の事業やシステム環境の理解と、情報セキュリティリスクの洗い出し

		企業	専門家	成果物/事務局提供ツールなど
事前準備	1	提供可能な社内資料の準備 (企業紹介のパンフレット等)	ホームページなどによる企業の情報収集とヒアリングシートの作成（企業・事業の理解)	【提供】指導講習コンテンツ ・訪問指導に当たっての心構え
	2	「5分でできる情報セキュリティ自社診断(Web版)」の実施	同左の実施依頼	【提供】自社診断(Web版)の実施方法
	3	出席メンバー選定 (経営者/従業員等、半日x4回)	専門家指導の作業内容、全体スケジュール案の作成、初回訪問日程の事前確認	初回のスケジュール調整
当日	1	右記説明に対するディスカッション(確認・了解)	今回の訪問指導の目標、作業内容、全体スケジュール、成果物等の説明と合意	【提供】指導講習コンテンツ ・昨年度の訪問指導から学べること
	2	提供可能な資料や、認識している情報セキュリティ課題の説明	ヒアリングシートを用いた事業と情報システム環境、情報セキュリティ課題の理解	【提供】標準ヒアリングシート 【提供】IPAの映像コンテンツ
	3	自社診断(Web版)の結果の理解と課題認識についてのディスカッション	自社診断(Web版)の結果についての説明と、改善領域に関する現状確認と要望の確認	【成果物】自社診断(Web版)の結果のまとめ
	4	右記依頼についての確認と了解	必要な追加情報の提供依頼 ・業務/DB/ネットワークなどのIT環境など 機密保持誓約書の提出 次回のスケジュール調整、依頼事項の確認 ※情報セキュリティ基本方針の作成	（終了後） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 第1回の指導では、ヒアリングによって、企業側が認識している現状課題（リスク）について把握します。
- 「５分でできる情報セキュリティ自社診断」は、経営者だけではなく従業員にも実施してもらうことで、実態をより明確にできます。
- 自社診断結果が高得点で、リスクが見えない場合には、本当に対応できているのか、例外的に見逃していることは無いかなど、突っ込んだ質問を行って課題を洗い出し、重点改善領域についてディスカッションします。
- IPA「情報セキュリティ対策ベンチマーク(27項目)」を使って、より高いレベルでの現状把握と他社比較を行うことも有効な方法です。

【ご参考】「標準的な進め方」の詳細（2）

第2回　基本方針や関連規程整備の検討と重点改善領域の絞り込み

		企業	専門家	成果物/事務局提供ツールなど
事前準備	1	依頼された必要情報の準備	前回訪問で得た情報の整理・分析 (理解に齟齬が無いか訪問時に確認する)	-
	2	情報セキュリティ基本方針の検討と案の作成	第２回の資料作成 ・関連規程類の作成状況確認 ・重点改善領域の見極め	※ZoomなどのWeb会議にて準備を進めることも検討 【提供】情報セキュリティ基本方針サンプル 【提供】基本方針/関連規程類の整備状況一覧表(確認用ワークシート)
当日	1	依頼された必要情報の提供・説明	提供された情報の確認・質疑応答	-
	2	基本方針/関連規程の有無/作成状況の説明 基本方針(案)の提示と作成	基本方針/関連規程の有無/作成状況の確認 基本方針の作成指導	【成果物】 ・情報セキュリティ基本方針 ・基本方針/関連規程類の整備状況確認一覧表
	3	右記説明に対するディスカッション ・対策の有用性と優先順位の判断	前回得た情報をもとにした、重点改善領域の説明とディスカッション ・緊急度、重要度、難易度による絞り込み	【成果物】自社診断(Web版)の結果と課題整理
	4	必要な追加情報の提供了解	改善領域の対策検討に必要な追加情報の提供依頼	（終了後） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 「５分でできる情報セキュリティ自社診断」の結果を改めて事前に分析し、重点改善領域と思われる項目を提示して、緊急度、重要度、難易度などの視点から、対策の優先順位についてディスカッションを行います。
- 関連規程をどこまで整備しておく必要があるかは、各企業の状況によって異なります。例外対応などの情報セキュリティの抜け穴となる点を極力なくし、また単に規程を作成するだけでなく、継続的に順守していける運用体制や従業員研修の実施についても併せて検討し、実効性を高めるようガイドしていきます。

【ご参考】 「標準的な進め方」の詳細（３）

第3回　コロナ禍の情報セキュリティ対策を含む、重点対策の検討と優先順位付け

		企業	専門家	成果物/事務局提供ツールなど
事前準備	1	急がれる改善施策の実現性の検討 (実現のための課題や対策の事前検討)	前回訪問結果の整理と、絞り込んだ具体的対策の実施計画案の作成	-
	2	コロナ禍における経営施策と情報システム環境の状況整理 ・テレワーク推進の課題など	コロナ禍の経営施策に必要な情報セキュリティ対策の説明資料の準備 ・指導講習コンテンツの理解	※実践として、第2回実施の際に、Web会議にて事前準備を進めることを検討
当日	1	コロナ禍の事業継続として実施した経営施策の説明と、情報セキュリティ対策の必要性の理解	コロナ禍の事業継続として実施された対策に対する、必要な情報セキュリティ対策の説明。	【提供】指導講習コンテンツ ・コロナ禍の情報セキュリティ対策
	2	右記のディスカッションを通じて提示された対策案の実現性検討 ・必要とされるリソース:人・物・金	これまでの検討を踏まえた、具体的対策の実行計画の検討 ・優先して検討すべき対策やスケジュール案の提示とディスカッション 対策実施に当たっての運用ルールの検討	※前回確認した関連規程の整備状況確認が、新たな対策実施に際して見直す必要がないか改めて確認
	3	右記の確認と了承	第4回に向けての準備の依頼 ・SECURITY ACTION二つ星宣言の申請準備	（終了後） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 直近の経営の最大課題であるコロナ禍対策について、情報セキュリティ対策の視点から抜け漏れがないか確認と検討を行います。
- Web会議ツールの活用では、取引先との接続環境や、従業員の働く環境など、様々なリスクを踏まえた対策をアドバイスします。
- 対策案については、4つの視点（組織/人/技術/物理的環境）から専門家が事前に案を作成しておきます。
- 当日は、専門家から提示された案をもとに、企業側と実現性や優先順位についてディスカッションを行い、具体的にスケジュール化していきます。

【ご参考】 「標準的な進め方」の詳細（４）

第4回　情報セキュリティ対策の成果物レビューと訪問指導全体のまとめ

		企業	専門家	成果物/事務局提供ツールなど
事前準備	1	SECURITY ACTION二つ星宣言の準備	前回訪問時の検討結果を踏まえた実行計画案の修正と更新版の作成(1年程度での実行計画)	-
	2	-	継続した支援の提案作成(可能であれば) 提出依頼資料の準備	-
当日	1	右記のディスカッションと合意 今後の進捗状況のフォロー方法の検討	情報セキュリティ対策実行計画の提示と合意 更なる改善に向けての継続フォローについての提案(可能であれば)	-
	2	作成した成果物の説明と合意	右記の成果物のレビューと合意	【成果物】情報セキュリティ対策実行計画書(コロナ禍対策等を含む) 【成果物】基本方針/関連規程の点検結果 【成果物】自社診断(web版)結果報告 【成果物】SECURITY ACTION二つ星宣言
	3	専門家指導についての評価コメント(アンケート)を事務局に提出	指導結果のまとめと評価	（終了後） 指導結果のまとめと評価を行い、事務局への実施報告を提出する

＜**実施のポイント**＞

- 第3回の検討をもとに、専門家は「情報セキュリティ対策実行計画案」を、企業側は「 SECURITY ACTIONの二つ星宣言」の準備を行い、当日は全体の成果物について、レビューと合意を行います。
- 可能であれば、実行計画書の実効性を高めるため、数ヶ月後にチェックポイントを設けるなど、継続した支援活動(有料)の提案を行い、RISSとしても次のステップとなる自走化を目指します。
- 計画される情報セキュリティ対策は、経営者が自分事として取り組める実効性と納得感のあるものとする。