令和6年度セキュリティ人材活用促進実証

セキュリティマネジメント指導（テーマ別）実施要領

テーマ⑤｜従業員向けセキュリティ教育

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

IPA Better Life with IT

本資料の位置づけ（事業の全体像）

本資料は、IPAが実施する「令和6年度セキュリティ人材活用促進実証」において実施する、サイバーセキュリティ専門家が中小企業に対して行う個別訪問指導「**セキュリティマネジメント指導（テーマ別）**」の主要説明資料です。

訪問指導では、専門家が中小企業の特性に応じたセキュリティ対策を指導する際の基本的なフレームワークを提供することを目的としています。特に中小企業は、限られたリソースの中で情報セキュリティ対策を行う必要がありますが、どの部分に重点を置くべきかが明確でないケースが多々あります。

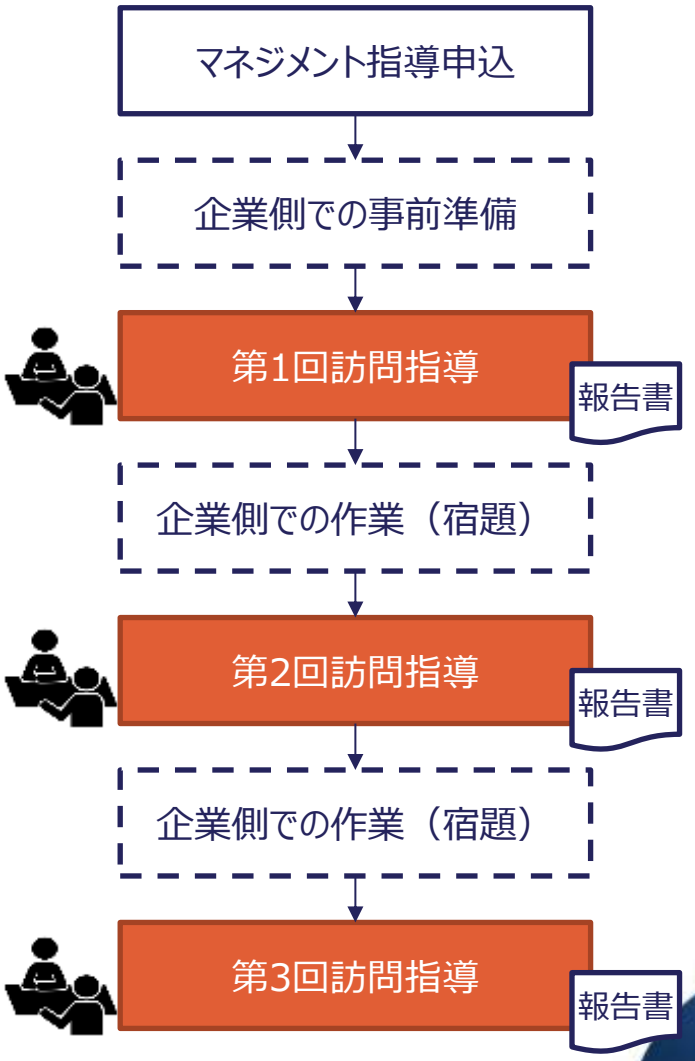
マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、そして**⑤従業員向けのセキュリティ教育** の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

各テーマにおいては、どのような企業がその指導を必要としているのか、指導によって達成されるべき目標、さらには具体的な作業内容や使用ツール、指導後の効果の考え方等を想定しています。これにより、専門家は訪問先の企業ごとに適切な指導計画を立て、効率的に支援を行うことができると考えています。

本資料では、専門家が現場で利用できる具体的なシラバスやチェックシート、ガイドラインも挙げております。実際には企業に訪問した際は、企業の実情に応じた柔軟な対応をお願いすることとなりますが、ツール活用によってある程度訪問指導の際の一貫性が確保され、企業においても自律的なセキュリティ対策の強化が期待できると考えます。

専門家のみなさまにおかれましては、本資料に記載された趣旨をご理解の上、中小企業へのセキュリティ個別指導にご対応ください。

マネジメント指導の流れ



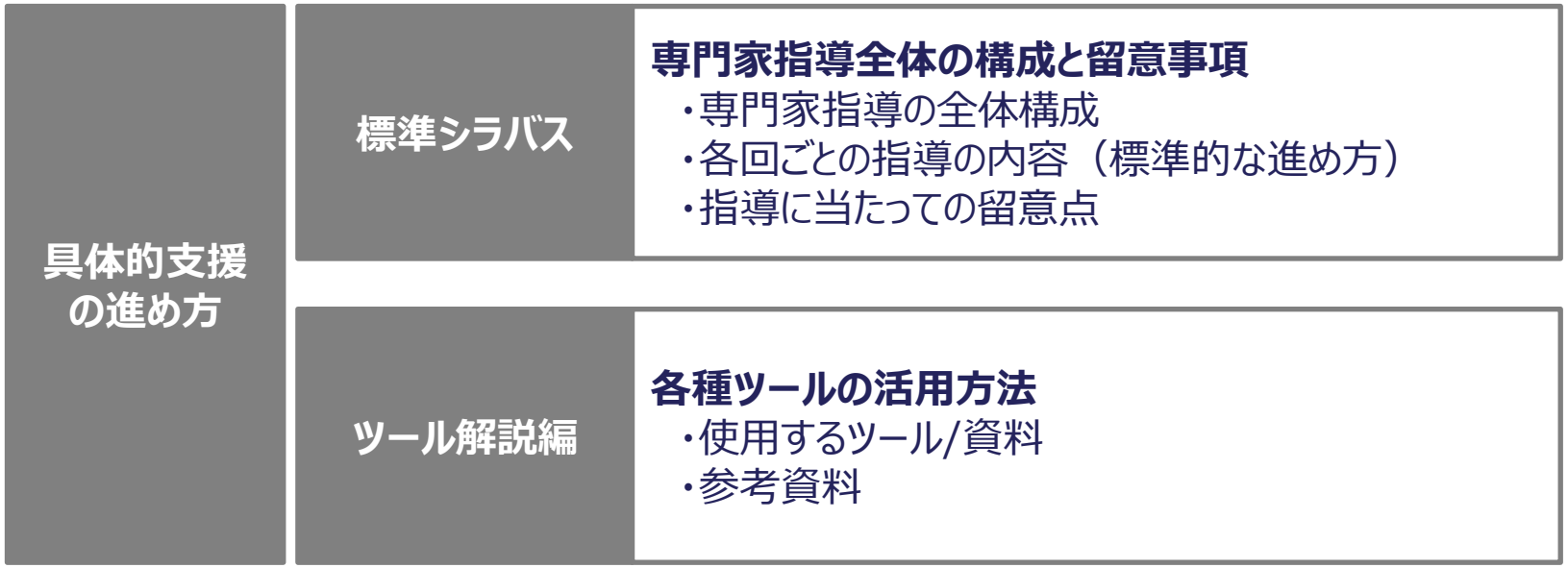
マネジメント指導のテーマと狙い

今回用意したマネジメント指導のテーマは以下の5テーマです。
企業の実情に即し、原則として以下のテーマから選定の上、企業への訪問指導を行っていただきます。

指導テーマ	1 情報セキュリティ規程の整備	2 情報資産の洗い出しとリスク分析	3 クラウドサービスの安全利用	4 セキュリティインシデント対応	5 従業員向け情報セキュリティ教育
どういった企業に受けてもらいたいか	**サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業**。特に、従業員が多様なITツールを使って業務を行っているが、具体的な指針がなく、責任範囲が曖昧な企業に必要である。	**デジタル化が進み、膨大な情報を管理しているが、どの情報が重要か、リスクがどこにあるかが把握できていない企業**。特に、製造業やサービス業など、顧客情報や技術情報を大量に扱う企業に必要である。	**業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な企業**。特に、情報管理の外部委託が進んでいるが、適切な安全対策ができていない中小企業に必要である。	**セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業**。特に、**サプライチェーンの一部として他社との連携が多い企業**に必要である。	**従業員のセキュリティ意識が低く、パスワード管理やフィッシング攻撃に対する対応が不十分な企業**。特に、ITリテラシーの差が大きい企業や、非専門職の従業員が多く、日常的なセキュリティ対策が徹底できていない企業に必要である。
マネジメント指導を受けたことによる効果	不足していた情報セキュリティ規程が整備され、社内での運用・周知方法まで確立されることで、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。	企業が保有する情報資産が洗い出され、リスク分析シートとして整備することで、自律的な運用が図れるとともに、リスク低減策等の検討の題材にもなる。	当該支援先企業における「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用に伴うリスクを理解できるようになる。	インシデント対応プロセスを整備し、必要に応じ、従業員の演習を実施することで、セキュリティインシデント発生時に迅速かつ効果的に対応できる体制が構築できる。	セキュリティ教育プログラムを策定するとともに、定期的に見直しと更新を行う体制を構築。実際に従業員に対するセキュリティ教育を実施することで、社内の意識向上にもつなげられる。

本書の構成

- 企業へのマネジメント指導を行うにあたり、5つの指導テーマについて、主にIPAのセキュリティ対策支援ツールを活用した3回の標準的な専門家の指導内容（標準カリキュラム）と、指導先企業の依頼・調整事項や指導にあたっての基本的な留意点を説明する「実施要領」を作成しました。
- 「実施要領」は、セキュリティの専門家による指導の下、今後も継続して活用できるものとなるよう、標準カリキュラムを示しつつ、指導先企業の個別事情に応じた指導に必要なツールの活用方法、経験者の体験による気付きや工夫など実践的なノウハウを提供する内容としています。



テーマ⑤｜従業員向けセキュリティ教育

【標準シラバス】
専門家指導全体の構成と留意事項

当事業の目標と成果物

- IPAが有する豊富なセキュリティ教育用コンテンツを活用し、企業のニーズに応じた形で具体的な研修計画を立案し、従業員向けセキュリティ教育を実施します。
- 教育実施後の結果や効果をレビューするとともに、以降の継続実施を目指し、セキュリティ教育計画書を策定します。

マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】サイバーセキュリティに関する従業員教育の実施
【達成目標３】教育実施結果のレビューと、以後の継続実施に向けた教育計画の策定

注：成果物

取組みスタート

達成目標1

- 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標2

- 従業員向けサイバーセキュリティ教育の実施

達成目標3

セキュリティ教育計画書
目的
対象
実施内容
評価方法
…

- 教育実施結果のレビューと、以後の教育計画の策定

継続実施

「標準的な進め方」の全体構成

1～2週間

事前準備#1

*IPA自社診断(Excel版)の実施依頼
*現在のインシデント対応プロセスやポリシーの確認

第１回

現状のセキュリティ教育計画の評価、セキュリティ教育実施に向けた調整

支援先企業のビジネス内容や組織概要等を聞き取った上で、企業のセキュリティ教育に状況を評価し、現状を把握します。また、企業のニーズも踏まえ、IPA等が提供している各種コンテンツ等も紹介した上で、第2回に実施予定の従業員向け教育の計画を立案します。

1～2週間

事前準備＃２

*教育プログラムの内容を確認するとともに、開催に向けた準備作業を行う。
*教育実施に向け、従業員（教育対象者）へのアナウンスを行う。

第２回

従業員向けセキュリティ教育実施

IPAコンテンツを用い、従業員向けの情報セキュリティ教育を実施します。

1～2週間

事前準備＃３

*教育実施後の効果を評価し、次回の教育プログラムに向けた改善点を整理する。
*継続的な教育体制構築に向けたアイデアを社内共有する。
*社内検討結果を踏まえた、セキュリティ教育計画（改訂版）案を策定する。

第3回

教育実施結果のレビューと、以後の継続実施に向けた計画の見直し

教育実施効果分析結果をレビューし、効果があったポイントや要改善点等について指摘します。
また、継続的な教育体制の構築に向けて、企業側が策定した計画改訂版について改善アドバイスを行います。

計1.5ヶ月程度

「標準的な進め方」の詳細（１）

第1回　現状のセキュリティ教育計画の評価、セキュリティ教育実施に向けた調整

		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
	2	「5分でできる！自社診断（Excel版）」による自己診断の実施	-（事務局にて配布済）	【提供】5分でできる！自社診断チェックシート（Excel版）
	3	既存の情報セキュリティ教育計画の確認	同左の実施依頼	-
	4	出席メンバー選定 (経営者/従業員等、半日x3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
	2	自社診断(Excel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(Excel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(Excel版)の結果のまとめ
	3	既存の情報セキュリティ教育計画の説明と、従業員向け情報セキュリティ教育実施に向けたディスカッション	既存の情報セキュリティ教育計画の改善点等を洗い出す。 従業員向け情報セキュリティ計画策定に向けた考え方提示（目的・テーマの設定、5W1Hの考え方等）。 第2回での従業員向け情報セキュリティ教育実施を目指し、IPAのセキュリティ教育コンテンツ等を活用した教育計画を練る。	【提供】情報セキュリティ教育計画書テンプレ
	4	右記依頼についての確認と了解	策定した教育計画をもとに、社内調整を依頼	（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**＞
- 第1回の指導では、ヒアリングによって、企業側での現時点でのセキュリティ教育計画等について把握します。また、第2回で実施する教育の計画を練ります。
- 「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。

「標準的な進め方」の詳細（２）

第2回　従業員向けセキュリティ教育実施

		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	セキュリティ教育計画に基づき、社内調整 （開催準備、参加者案内・確定等）	第2回の資料作成 ・セキュリティ教育用コンテンツ作成	【提供】情報セキュリティ教育計画書
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	従業員向け情報セキュリティ教育主催 実施後に受講者へのアンケート実施	従業員向け情報セキュリティ教育実施	【成果物】情報セキュリティ教育計画書 【成果物】従業員向け情報セキュリティ教育コンテンツ
	3	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**＞
- 実際に従業員向け教育を実施し、参加者に対するアンケート調査を実施します。
- ビジネスで取り扱う情報やサプライチェーンの状況、またそれに伴い必要となる社内でのインシデント対応体制の考え方は、各企業の状況によって異なります。ビジネスの内容や取り扱う情報の性質、社外関係先の状況も踏まえ、過度にハードルを上げることにならないよう、実効性を高めるようガイドしていきます。

「標準的な進め方」の詳細（３）

第3回　教育実施結果のレビューと、以後の継続実施に向けた計画の見直し

		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	従業員向け情報セキュリティ教育実施結果の取りまとめ（アンケート集計・分析、効果測定等） 今後の従業員向け情報セキュリティ教育計画書案の作成	第3回の資料作成	【提供】指導講習コンテンツ
当日	1	従業員向け情報セキュリティ教育結果について説明、ディスカッション 今後の従業員向け情報セキュリティ教育実施に向けた計画書案の説明	従業員向け情報セキュリティ教育結果に対するコメント、ディスカッション、改善点等指摘 従業員向け情報セキュリティ教育計画書案に対するコメント、指摘等	【成果物】従業員向け情報セキュリティ教育結果まとめ 【成果物】従業員向け情報セキュリティ教育計画書案
	2	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行う 【成果物】最終報告書

＜**実施のポイント**＞
- 第3回までの面談・ディスカッションを経て、具体的なインシデント対応机上演習（訓練）を実施します。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、引き続き社内での情報セキュリティ対策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、専門家としての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します。

指導先企業への依頼や調整事項

確認・調整事項		依頼・調整のポイント
1	企業様の検討体制(参加メンバー)等の調整	✓ 経営層に加え、以下の現場のリーダー層～課長クラスに参加いただくことを推奨します。 ・事業や業務のプロセスに詳しい方 ・ITシステムの運用管理を担っている方
2	打ち合わせ場所や環境の確認/準備	✓ 会議室/プロジェクター等の環境確認/準備をお願いします。 ・映像コンテンツの投影や、ディスカッションの効率に大きな影響があります。 ✓ 検討方法は、各専門家のやり方(経験)を踏まえ実施します。 ・原因を掘り下げ、メンバーの納得感と実効性のある対策に結びつけます。 （企業によって、検討方法が異なる場合があります）
3	指導環境の調整（コミュニケーション環境）	✓ 原則として訪問による現地指導を行いますが、初回を除く2回目以降で訪問と同等の指導がオンラインでも可能であることが見込まれ、かつ中小企業の合意と情報処理推進機構も了承した場合に、オンラインによる指導を行う場合もあります。
4	提供を受ける情報の取り扱い	✓ 企業様にいただいた情報は専門家、及び事業を実施する情報処理推進機構（委託先を含む）において取り扱いに留意します。 ✓ 情報の取り扱いに関して希望があれば相談に応じます。

教育の目的を決める

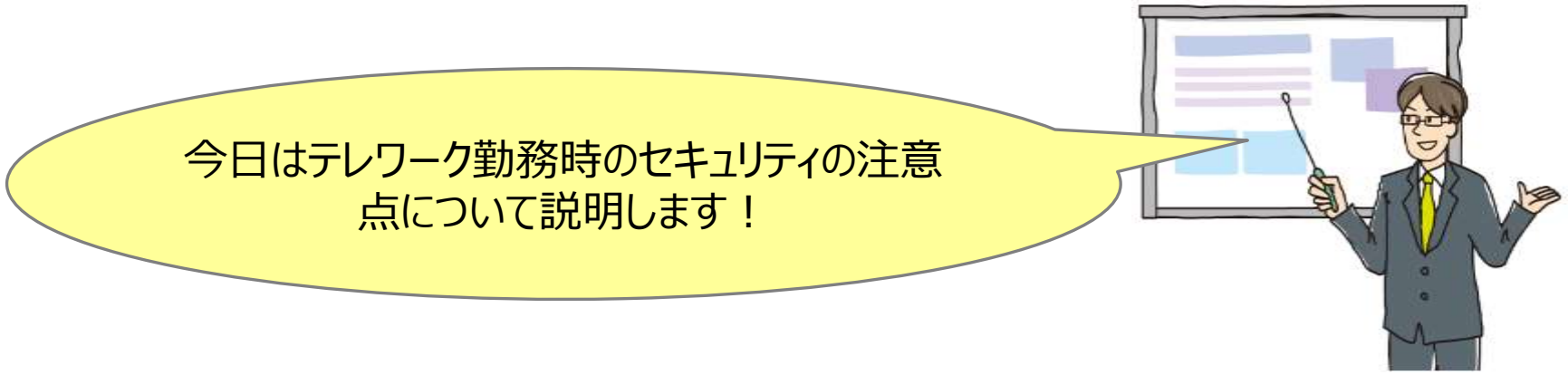
- 自社の**従業員に必要なセキュリティの知識やスキル**を検討します。
- 従業員の職種や役職、また、業務で利用する情報システムによって、**必要とされる知識やスキルは様々**です。
- **対象者やIT環境**など状況に適した目的を決めましょう。

対象者　　：全従業員
研修目的：『情報セキュリティ規程』を周知する

対象者　　：テレワーク勤務する従業員
研修目的：テレワーク勤務時に使用する情報システムと
セキュリティ上の注意事項を周知する

教育テーマを決める

- セキュリティに必要な知識やスキルは多岐に渡るため、短時間に、多くを伝えても、**全てを理解し実行するのは難しい**ことがあります。
- 受講者の的確な理解が得られるように、要点を絞るとともに、**計画的に教育の機会**を設けましょう。
- テレワークやクラウドシステムの導入など、情報システムの変更に伴い、新たな対策が必要になった場合など、**状況に適したテーマ**を決めましょう。



５Ｗ１Ｈを決める

５Ｗ１Ｈ		例
Who だれに	対象者	全従業員、管理職、一般職、パートタイマー、新入社員、中途社員、委託事業者…
When いつ	実施時期	年度初め、半期毎、朝礼時、入社時、ルール変更時、システム導入時、事故ニュース後…
Where どこで	会場	会議室、執務室、貸会議室、外部研修会場、自宅（オンライン） …
What なにを	テーマ	情報セキュリティ規程、標的型攻撃対策、ビジネスメール詐欺対策、テレワーク時の注意事項…
Why なぜ	理由（目的）	情報セキュリティ規程の周知徹底、セキュリティ事故の再発防止、テレワークの導入…
How どのように	教育方法	集合教育、eラーニング、Web会議システム、教材配付、外部研修、公開セミナー参加…

教育の効果を確認する

- 研修後に受講者が理解できたか、実行できているかなど、
  効果測定をあらかじめ計画します。
- 効果測定の方法は、**テストやアンケート**を実施したり、
  職場での**行動を観察**する、などがあります。
- 効果が十分でない場合には、個別に指導したり、
  実行できない理由を訊ねて**フォロー**することで、全体がレベルアップします。

【ツール解説編】
各種ツールの活用方法

使用するツール/資料の内容（教育計画書）

提出成果物

- 専門家の指導のもと、従業員向けの情報セキュリティ教育計画書（様式１）を策定してください。
- 研修当日のプログラムも合わせて作成（様式自由）し、実施に向けて社内調整を行ってください。
- 従業員向け情報セキュリティ教育実施後、受講者に対するアンケート結果等を集計・分析し、専門家とともに評価した結果を提出ください（様式自由）。

情報セキュリティ教育計画書（例）	
研修名	テレワーク勤務時のセキュリティの注意事項
実施時期	20××年10月 1日(火)　[第1回] 10：00～11：00 25日(金)　[第2回] 16：00～17：00
受講方法	Web会議システム **※各自のPCで受講してください**
対象者	全従業員 **※パートタイマー、派遣社員の方も受講してください。**
プログラム	・映像で知る情報セキュリティの上映 ・自社のセキュリティルールの説明
講　師	情報システム担当
特記事項	第1回、第2回いずれかを必ず受講してください。

成果物作成の留意点（教育の目的を決める）

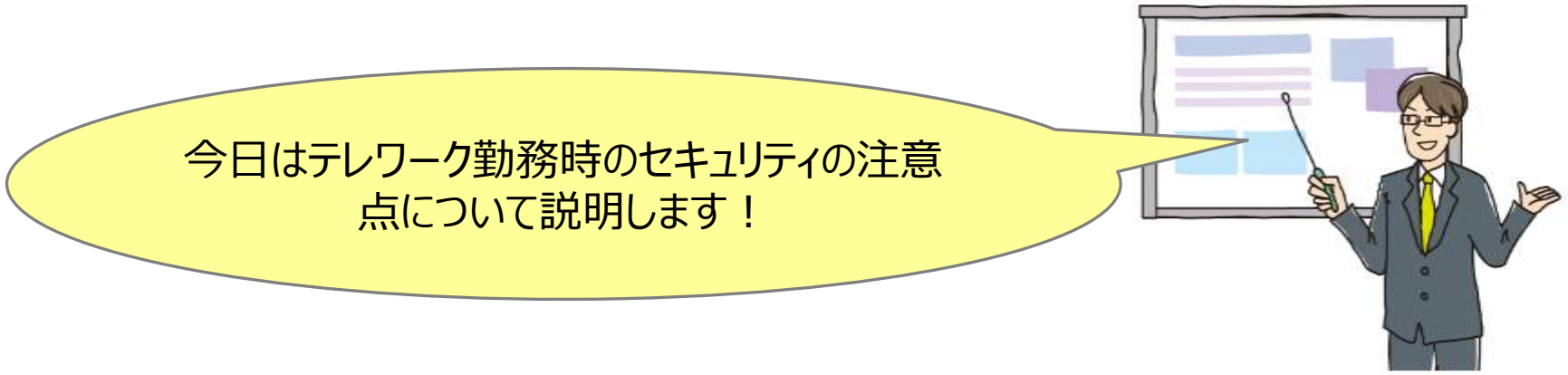
- 自社の**従業員に必要なセキュリティの知識やスキル**を検討します。
- 従業員の職種や役職、また、業務で利用する情報システムによって、**必要とされる知識やスキルは様々**です。
- **対象者やIT環境**など状況に適した目的を決めましょう。

対象者　　：全従業員
研修目的：『情報セキュリティ規程』を周知する

対象者　　：テレワーク勤務する従業員
研修目的：テレワーク勤務時に使用する情報システムと
セキュリティ上の注意事項を周知する

成果物作成の留意点（教育テーマを決める）

- セキュリティに必要な知識やスキルは多岐に渡るため、短時間に、多くを伝えても、**全てを理解し実行するのは難しい**ことがあります。
- 受講者の的確な理解が得られるように、要点を絞るとともに、**計画的に教育の機会**を設けましょう。
- テレワークやクラウドシステムの導入など、情報システムの変更に伴い、新たな対策が必要になった場合など、**状況に適したテーマ**を決めましょう。



成果物作成の留意点（５Ｗ１Ｈを決める）

５Ｗ１Ｈ		例
Who だれに	対象者	全従業員、管理職、一般職、パートタイマー、新入社員、中途社員、委託事業者…
When いつ	実施時期	年度初め、半期毎、朝礼時、入社時、ルール変更時、システム導入時、事故ニュース後…
Where どこで	会場	会議室、執務室、貸会議室、外部研修会場、自宅（オンライン）…
What なにを	テーマ	情報セキュリティ規程、標的型攻撃対策、ビジネスメール詐欺対策、テレワーク時の注意事項…
Why なぜ	理由（目的）	情報セキュリティ規程の周知徹底、セキュリティ事故の再発防止、テレワークの導入…
How どのように	教育方法	集合教育、eラーニング、Web会議システム、教材配付、外部研修、公開セミナー参加…

成果物作成の留意点（教育の効果を確認する）

- 研修後に受講者が理解できたか、実行できているかなど、
  効果測定をあらかじめ計画します。
- 効果測定の方法は、**テストやアンケート**を実施したり、
  職場での**行動を観察**する、などがあります。
- 効果が十分でない場合には、個別に指導したり、
  実行できない理由を訊ねて**フォロー**することで、全体がレベルアップします。

成果物作成の留意点（当日プログラムを作る）

- 教育計画書を作成したら研修当日のプログラムを作ります。
- プログラム例『標的型メール攻撃対策研修』

サンプルプログラム（60分）			使用教材
10:00 （10分）	映像上映 「そのメール本当に信用してもいいんですか？ ～標的型サイバー攻撃メールの手口と対策～」	映像で知る情報セキュリティを上映する	IPA映像で知る情報セキュリティ（動画サイト） 
10:10 （30分）	解説	解説	資料
10:40 （10分）	Q&A		
10:50 （10分）	理解度確認テスト	効果測定の後、講師が解説する	資料

情報セキュリティ教材を入手する

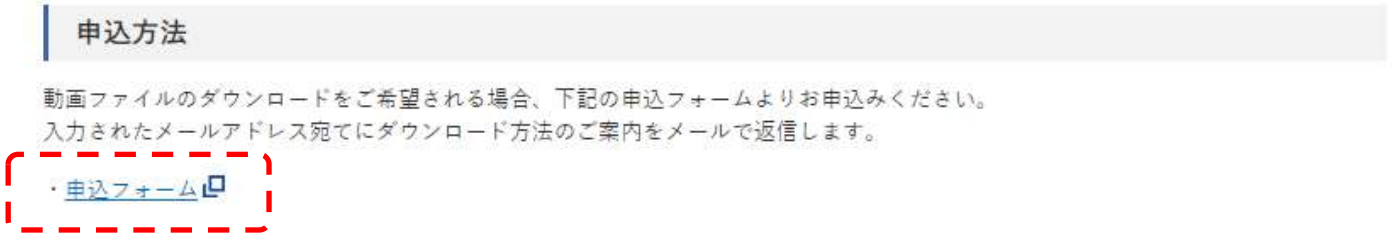
- 情報セキュリティ教材は次のサイトからダウンロードできます。
  https://www.ipa.go.jp/security/sec-tools/index.html

教材を入手する ～映像教材～

- 映像教材の入手方法は２種類あります

① 動画サイト（YouTube「IPA Channel」）での視聴
https://www.youtube.com/user/ipajp

② 動画ファイルのタウンロード
https://www.ipa.go.jp/security/videos/download.html



映像で知る情報セキュリティ

- 情報セキュリティ上の様々な脅威と対策を**10分程度のドラマ映像**などを通じて学べる映像教材です。
- YouTube「**IPA Channel**」でいつでも視聴可能です。

  主な映像はダウンロードも可能です。

[企業・組織向け]

内部不正対策、標的型攻撃、ビジネスメール詐欺、
ランサムウェア対策、中小企業向け対策、新人研修など

[一般向け]

ワンクリック請求、スマホセキュリティ、SNS利用の心得、
パスワード、小学生、中高生向けなど

https://www.ipa.go.jp/security/videos/list.html

IPA　映像　**検索**

映像コンテンツ一覧（抜粋）

- 今、そこにある脅威 ～内部不正による情報流出のリスク～
- 今、そこにある脅威 ～組織を狙うランサムウェア攻撃～
- What’s BEC？ ～ビジネスメール詐欺 手口と対策～
- そのメール本当に信用してもいいんですか？ ～標的型サイバー攻撃メールの手口と対策～
- デモで知る！標的型攻撃によるパソコン乗っ取りの脅威と対策
- あなたの会社のセキュリティドクター ～中小企業向け情報セキュリティ対策の基本～
- 妻からのメッセージ ～テレワークのセキュリティ～
- 今、そこにある脅威 ～内部不正による情報流出のリスク～
- 情報を漏らしたのは誰だ？ ～内部不正と情報漏えい対策～
- 3つのかばん ～新入社員が知るべき情報漏えいの脅威～
- 陽だまり家族とパスワード ～自分を守る3つのポイント～
- あなたの書き込みは世界中から見られてる ～適切なSNS利用の心得～

「映像コンテンツ」を使った研修会 サンプルプログラム①

● 標的型メール攻撃対策研修

サンプルプログラム（60分）			使用教材
10:00 （10分）	映像上映 「そのメール本当に信用してもいいんですか？ ～標的型サイバー攻撃メールの手口と対策～」	映像で知る情報セキュリティを上映する	IPA映像で知る情報セキュリティ（動画サイト） 
10:10 （30分）	解説	自社で実施している対策を周知する • 使用しているソフトウェアの更新方法 • ウイルス対策ソフト自動更新の方法 • 自社に送られてきた不審メールの紹介 • 不審メールを受信したときの対応方法 など	自社作成資料 
10:40 （10分）	Q&A		
10:50 （10分）	理解度確認テスト	効果測定の後、講師が解説する	自社作成資料 

サンプルプログラム①_標的型サイバー攻撃メールの手口と対策.pptx

「映像コンテンツ」を使った研修会 サンプルプログラム②

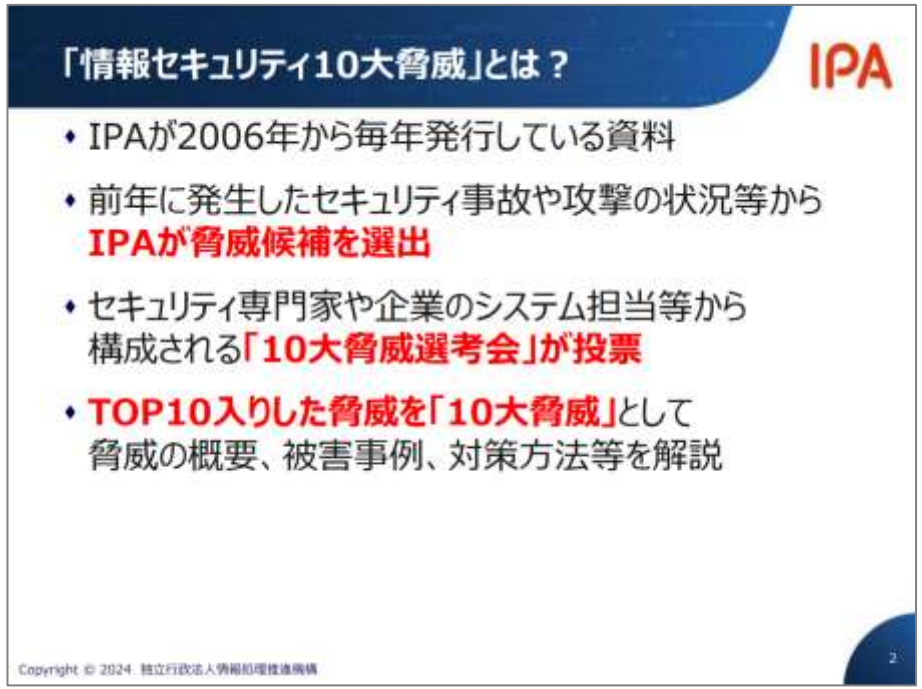
● 内部不正対策研修

サンプルプログラム（60分）			使用教材
10:00 （10分）	映像上映 「今、そこにある脅威 ～内部不正による情報流出のリスク～」	映像で知る情報セキュリティを上映する	IPA映像で知る情報セキュリティ（動画サイト） 
10:10 （30分）	解説	自社で実施している対策を周知する • 使守秘義務および競業避止義務 • アクセス制限、私物記録媒体の使用禁止 • アクセスログ取得、入退室管理 • メールやウェブサービスのログ監視・管理 など	自社作成資料 
10:40 （10分）	Q&A		
10:50 （10分）	理解度確認テスト	効果測定の後、講師が解説する	自社作成資料 

サンプルプログラム②_内部不正による情報流出のリスク.pptx

スライド教材を使った研修会

- IPAでは「情報セキュリティ10大脅威」をはじめ、各種の情報セキュリティ教材・ツールを無償で公開しています。これらのスライド教材を利用して自社の情報セキュリティ研修を実施することができます。



資料の引用について

IPAの資料に含まれるデータやグラフ・図表等を、作成される資料に引用・抜粋してご利用頂いて構いません。

ご利用に際しては、以下をお願いしております。

- 出典を明記すること（当機構名、資料名、URL）
- 可能な限り原文のまま掲載すること（グラフの形式を変える、文体を変える等は可）
- 一部改変して使用する場合は文意を変えず、原文のままでないことがわかるよう明記すること（「～を基に作成」等）
- 転載部分と作成部分が混在する場合、転載部分か、作成部分が明確にわかるようにすること

中小企業の情報セキュリティ対策ガイドライン第3.1版

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインです。
- ガイドラインは、中小企業の情報セキュリティ対策の考え方や実践方法について、本編２部と付録より構成されています。

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。
付録	付録８　中小企業のためのセキュリティインシデント対応の手引き	情報漏えいやシステム停止などのインシデント対応のための手引きです。

参考情報一覧

- 情報セキュリティ対策支援サイト
  https://www.ipa.go.jp/security/sme/isec-portal.html
  - 5分でできる！情報セキュリティ自社診断
    https://www.ipa.go.jp/security/guide/sme/5minutes.html
  - 情報セキュリティ対策ベンチマーク
    https://www.ipa.go.jp/security/sec-tools/benchmark.html
  - ５分でできる！ポイント学習
    https://www.ipa.go.jp/security/sec-tools/5mins_point.html
- セキュリティプレゼンター向け資料ダウンロード
  https://www.ipa.go.jp/security/sme/presenter/presenter-materials.html
- 中小企業の情報セキュリティ対策ガイドライン
  https://www.ipa.go.jp/security/guide/sme/about.html
- SECURITY ACTION セキュリティ対策自己宣言
  https://www.ipa.go.jp/security/security-action/
- 映像で知る情報セキュリティ ～映像コンテンツ一覧～
  https://www.ipa.go.jp/security/videos/list.html
- YouTube「IPAチャンネル」内の 情報セキュリティ普及啓発映像コンテンツ
  https://www.youtube.com/playlist?list=PLF9FCB56776EBCABB


IPA