令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第９編　組織として実践するためのスキル・知識と人材育成　【レベル共通】

第24章. 各種人材育成カリキュラム

章の目的
第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を把握することを目的とします。紹介するカリキュラム内容は、具体的な実施計画や実施内容を検討する際の参考資料となります。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」のカリキュラム内容を理解すること。 ◘ 「IT スキル標準モデルカリキュラム」のカリキュラム内容を理解すること。 ◘ デジタルスキル習得に関する講座を紹介する「マナビ DX」について概要と活用方法を理解すること。

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

「プラス・セキュリティ知識補充講座」は、内閣サイバーセキュリティセンター（NISC）が提供するプログラムで、特に経営層やデジタルトランスフォーメーション（DX）を推進する部課長向けに設計されています。この講座は、企業内外のセキュリティ専門人材との協働を円滑に行うために必要な知識を補充することを目的としています。

具体的には、以下のように経営層向けとデジタル化推進部門の部課長級マネジメント層向けの 2 つのカリキュラムで構成されています。

- 経営層
  企業のセキュリティリスクに対する理解を深め、経営判断に役立つ知識を提供。

- デジタル化推進部門の部課長級マネジメント層
  業務や製品・サービスのデジタル化を推進する役割を担う部門の管理職向けに、セキュリティリスク管理やデジタル化に伴うセキュリティ対策を強化する知識を提供。

理想とする目標
経営層（必ずしも DX を担当している部署の担当役員などではなく、経営層全体） ● サイバーセキュリティに関する動向が自社のコーポレートリスクに与える影響を的確に把握できる。 ● 上記の影響を踏まえ、自社のセキュリティ体制構築・投資の決定・指示を的確に実行できる。 ● 万一のインシデント発生時に、的確に経営判断を行い、指示をできる。 **業務、製品・サービスのデジタル化を推進する部門のマネジメントを担う部課長級** ● サイバーセキュリティに関する動向が自社の担当する事業・自部署に与える影響を的確に把握できる。 ● 上記の影響を踏まえつつ、自部署で実施されている対策の現状を理解できる。 ● 上記について、経営層が的確な経営判断をできるよう、自ら説明・報告できる。 ● 上記を実施するために、社内（情報システム部門など）・社外（ベンダーなど）と、円滑にコミュニケーションできる。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

このカリキュラムは、企業内研修のプログラムを策定する際に参考にできるよう設計されており、対象別の目標・到達レベルは以下の通りです。

カリキュラム受講後の到達レベルは、以下の表の「中」のレベルを想定しています。つまり、専門家との意見交換ができるレベルを目指したものとなっています。

	理解	コミュニケーション	評価・分析	判断
高	自らの役割に必要な知識を概ね網羅的に習得し、理解している	自ら把握すべきことを洗い出し、専門家を含む適切な対象者に回答を求めることができる	脅威や脆弱性が自組織に及ぼす影響を評価できる	自らの知識のみで、自組織での対応に関する適切な判断ができる
中	**自らの役割に必要な知識の全体像を把握した上で、その一部について理解していることを自覚している**	**専門家との意見交換ができる**	**脅威や脆弱性がどのように自組織に影響を及ぼすのかを理解できる**	**専門家の判断について、根拠を理解して合意を与えることができる**
低	サイバーセキュリティ関連文書に用いられる用語の意味を理解している	専門家からの説明を概ね理解することができる	脅威や脆弱性とは何かを理解している	自らの知識のみでは判断に関与することが困難

カリキュラム例の構成は以下の通りです。

	経営層向け	部課長級向け
目標	● サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 ● 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 ● インシデント発生時の適切な経営判断・指示	● サイバーリスクが自部署に与える影響理解 ● 自部署で実施されている対策の現状理解 ● 上記の経営層への報告 社内外とのコミュニケーション
時間設定	7.5時間（集合講習3時間＋オンデマンド4.5時間（うち必須3時間））	11時間（集合講習4.5時間＋オンデマンド6.5時間（うち必須5.5時間））
留意点	● 経営会議及び対外対応として実際に起こり得るケースから逆算 ● 各コマのインプット項目では、部課長級向けから内容を限定・変更	● 部署内会議やベンダー管理で実際に起こり得るケースから逆算 ● 既存のスキルなどフレームワーク（SP800-181等）と紐付けを実施
1.基礎知識	① デジタルインフラの基本（30分）◇ ② デジタル技術の基盤とリスク（30分）◇ ③ デジタル環境のコストと運用責任（30分）◇	① デジタルインフラ入門（20分）◇ ② サイバーセキュリティに関する用語の意味（20分）◇ ③ デジタル環境の管理や責任に関するキーワード（20分）◇ ① デジタルインフラの要点（30分）◆ ② デジタル技術の基盤とリスク（30分）◆ ③ デジタル環境のコストと運用責任（30分）◆
2.脅威と対策	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション など）（30分）★	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション など）（30分）★ ④ 演習1：脅威と対策における“悪い見本”から学ぶ（60分）★
3.投資	① コーポレートリスクとしてのサイバーセキュリティ（コンプライアンスを含む）（30分）◆ ② 体制構築・人材確保（30分）◆ ③ 演習1：各種対策の費用、損失想定、確率値から必要な投資を検討（70分）★	① サイバーセキュリティのリスクマネジメントの特徴（30分）◆ ② 対策における費用と損失の考え方（30分）◆ ③ リスクマネジメントのケーススタディ（30分）★ ④ 演習2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（60分）★
4.SHとの関係	① インシデント対応における経営層の役割（30分）◆ ② 通常時の備えと情報開示の在り方（30 分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習2：インシデント発生時の模擬記者会見（50分）★	① インシデント対応プロセスとその準備（30分）◆ ② 通常時の備えとインシデント情報の取扱上のポイント（30分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習3：インシデント発生時の社内外連絡（60分）★
5.関係法令	-	① サイバーセキュリティに関する国内法令とその読み方（20分）◆ ② サイバーセキュリティに関する基準・規格など（20分）◆ ③ サイバーセキュリティに関するガイドラインなど（20分）◆

★：集合講習での開催が推奨されるもの（受講必須）

◆：オンライン・オンデマンド形式での実施を想定（受講必須）

◇：オンライン・オンデマンド形式での実施を想定（受講任意）

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

24-1-1. 経営層向けカリキュラム例

経営層向けカリキュラム例を紹介します。カリキュラムは、４単元で構成されます。

経営層向け第１単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要』**
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。

経営層向け第２単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

経営層向け 第３単元	
名称	**3.投資** **『サイバーセキュリティと投資対効果』**
目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。

	● セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。

経営層向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティと企業価値』**
目標	● サイバーセキュリティインシデントの発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。
到達レベル	● 自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-1-2. 部課長級向けカリキュラム例

部課長級向けカリキュラム例を紹介します。カリキュラムは、5 単元で構成されます。

部課長級向け 第 1-1 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（初級編）』**
目標	● デジタル化を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	● デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。

部課長級向け 第 1-2 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（中級編）』**

目標	● デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念について、第 2 単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることにする。

部課長級向け 第 2 単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

部課長級向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティとリスク対応』**
目標	● 自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

部課長級向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティ対応における社内外連携』**
目標	● デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。
到達レベル	● 自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。

部課長級向け 第 5 単元	
名称	**5.関連法令** **『サイバーセキュリティに関する法制度』**
目標	● サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	● デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1)】

IT スキル標準（ITSS）については、22 章で説明しましたが、各種 IT 関連サービスの提供に必要とされる知識やスキルを体系化した指標であり、産学における IT サービス・プロフェッショナルの教育・訓練などに有用な「ものさし」（共通枠組）を提供しようとするものです。

IT スキル標準は、11 の職種と 35 の専門分野を設け、それぞれの専門分野に対応して、各個人の能力や実績に基づく 7 段階の達成レベルを規定しています。

「IT スキル標準モデルカリキュラム」は、IT スキル標準のレベル 1～3 を目指す人向けのカリキュラムとして IPA から公開されているものですが、ここではレベル 1 向けのモデルカリキュラムを紹介します。

このカリキュラムは、職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラムであり、研修ロードマップをもとに、具体的な研修コースを設計･実施する際に参考となる情報がまとめられています。このモデルカリキュラムを履修することにより、IT スキル標準のレベル 1 に相当する知識を修得することができます。

IT スキル標準モデルカリキュラムの構成

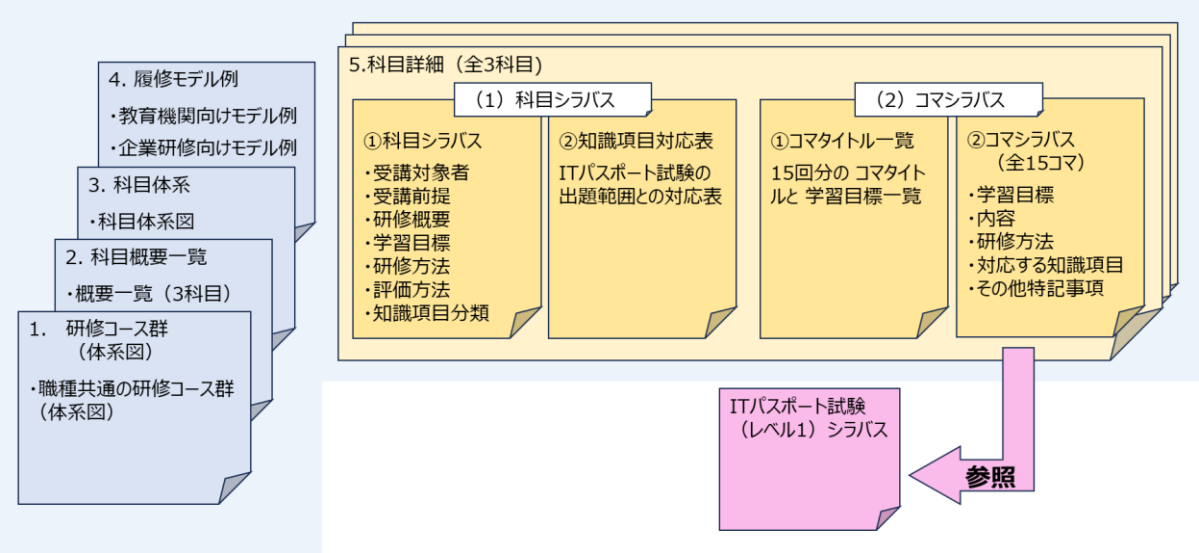

図.101 「IT スキル標準モデルカリキュラムの構成」

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT スキル標準のレベル 1 モデルカリキュラム（科目概要一覧）

対象人材	① 本格的な就業経験のない学生 ② IT に関する基本的な知識を持たない社会人

対象場面	① 企業：IT 系企業を含め企業などの内定者の入社前研修など ② 教育機関：情報系、非情報系のすべての学部、学科における教育。ただし、情報系専門学科においては一般教養課程における教育
特徴	● 特定の製品や分野に偏らない知識と体系的なパーソナルスキルを修得できます。 ● IT パスポート試験の出題範囲と整合し、科目およびコマシラバスごとに知識項目との対応が明らかになっているので、「IT パスポート試験（レベル 1）シラバス」と併用することでより一層の研修効果を図ることができます。

このカリキュラムでは「IT 基本 1」コース群に含まれるコース「IT 入門」と「パーソナルスキル入門」に対応する科目が策定されています。

科目名	概要	受講対象者／受講前提	構成	時間
IT 入門（1）	「IT 基本 1」コース群の 1 つとして、ストラテジおよびマネジメント分野の基本的かつ普遍的な知識の修得を目的とする。具体的には、企業における経営戦略と担当業務の関連、システム開発のライフサイクル、プロジェクトマネジメント、サービスマネジメントおよびシステム監査などの知識を学習する。	IT スキル標準のレベル 1 を目指す者/前提科目は特にないが、高校卒業程度の知識を有していること	90 分×15 回	22.5h
IT 入門（2）	「IT 基本 1」コース群の 1 つとして、テクノロジ分野の基本的な知識の修得を目的とする。具体的には、情報のデジタル化とアルゴリズム、ハードウェア、ソフトウェア、ネットワーク、データベースおよびセキュリティに関する基本的な知識を学習する。	IT スキル標準のレベル 1 を目指す者/「IT 入門（1）」を修了していること、または同等の知識を有していること	90 分×15 回	22.5h
パーソナルスキル入門	パーソナルの領域に関して職業人として基本的な要件である、チームワークに基づくリーダーシップ、コミュニケーションの基本（書く、話す、聞く、考える）、プレゼンテーションの基本、論理展開（問題解決）法の基本、基本的なビジネスマナー、	IT スキル標準のレベル 1 を目指す者/前提科目は特にないが、高校卒業程度の知識を有していること	90 分×15 回	22.5h

	更に IT を活用する上で求められるパーソナルスキルの概要などを学習する。			

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT 入門（1）

科目シラバス

科目	IT 入門（1）
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	前提科目は特にないが、高校卒業程度の知識を有すること
学習目標	職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析と解決およびシステム化の支援を行うことができる
研修・教育方法	講義、演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）
知識項目分類	【分野】ストラテジ系 【大分類】 1.企業と法務 【中分類】 1 企業活動 2 法務 2.経営戦略 【中分類】 3 経営戦略マネジメント 4 技術戦略マネジメント 5 ビジネスインダストリ 3.システム戦略 【中分類】 6 システム戦略 7 システム企画 【分野】マネジメント系 【大分類】 4 開発技術 【中分類】 8 システム開発技術 9 ソフトウェア開発技術 5 プロジェクトマネジメント 【中分類】 10 プロジェクトマネジメント 6 サービスマネジメント 【中分類】 11 サービスマネジメント

	12 システム監査

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1 コマタイトル一覧」に記載しています。

IT 入門（2）

科目シラバス

科目	IT 入門（2）
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	「IT 入門(1)」を修了していること、また同等の知識を有していること
学習目標	職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる
研修・教育方法	講義、演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）
知識項目分類	【分野】テクノロジ系 【大分類】 7 基礎理論 【中分類】 13 基礎理論 14 アルゴリズムとプログラミング 8 コンピュータシステム 【中分類】 15 コンピュータ構成要素 16 システム構成要素 17 ソフトウェア 18 ハードウェア 9 技術要素 【中分類】 19 ヒューマンインタフェース 20 マルチメディア 21 データベース 22 ネットワーク 23 セキュリティ

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1 コマタイトル一覧」に記載しています。

パーソナルスキル入門

科目シラバス

科目	パーソナルスキル入門
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	前提科目は特にないが、高校卒業程度の知識を有していること
学習目標	職業人としての基本的なパーソナルスキルの知識を活用し、上位者の指導の下、チームメンバーとして、業務活動に参加することができる
研修・教育方法	講義、グループ演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1 コマタイトル一覧」に記載しています。

詳細理解のため参考となる文献（参考文献）	
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

24-3. マナビ DX

マナビ DX は、経済産業省と IPA が運営するデジタル人材育成のためのプラットフォームで、デジタルスキル習得に関する講座を紹介するポータルサイトになっています。デジタルスキルを学んだことのない人から、実践的なデジタル知識・スキルを身につけたい人まで、それぞれに適した講座を紹介してくれます。

紹介されている講座

マナビ DX で紹介されている講座には以下のような特徴があります。

- **厳選された信頼できる講座**
  デジタルスキル標準（DSS）などのスキル標準への対応を経産省・IPA が審査し、合格した講座のみが掲載されています。

- **種類が豊富**
  講座はさまざまなパートナーから提供されており、デジタルリテラシーや基本的な IT スキルを学ぶための講座から実際のビジネスシーンで役立つ実践的なスキルを習得するための講座まで幅広い講座が掲載されています。

- **受講料支援のある講座も掲載**
  講座には無料のものと有料のもの（受講料が必要なもの）がありますが、一部の講座では受講料の補助が受けられるものもあります。

- **リスキリングにも活用**
  リスキリングに重要なデジタルスキル習得をはじめる方に最適な初学者向け講座も提供されています。

「マナビ DX」には多くの講座が掲載されています。その一部を紹介します。

- **デジタルリテラシー講座**
  - IT パスポート試験対策：IT の基本知識を学ぶための講座
  - データサイエンス入門：データ分析の基礎を学ぶための講座
  - AI 活用入門：人工知能の基本概念とその応用方法を学ぶための講座

- **デジタル実践講座**

- AI データ活用実践コース：Web 開発の基礎から AI 技術の応用までを学ぶ講座
- IT エンジニア総合コース：フロントエンドからバックエンド、さらに AI 技術までを網羅する講座
- AI×IoT エンジニア育成コース：Web 開発、AI、IoT 技術を統合的に学ぶ講座

- **サイバーセキュリティ関連講座**
  - SaaS 担当者のためのセキュリティコース
    クラウドサービスを利用する際に必要となる情報セキュリティの基礎知識とクラウドサービスにおけるリスク分析手法を学ぶ講座
  - サイバーセキュリティ技術者育成コース
    サイバーセキュリティ技術を習得するための実践的な高度技術を基礎から体系的に学ぶ講座
  - インターネットセキュリティ技術（実習編）
    インターネット上のさまざまな脅威について学習し、組織において必要となるセキュリティ対策技術を、実習を通して習得する講座
  - 攻撃手法概論
    サイバーセキュリティにおける代表的な攻撃手法の概要とその特徴について学ぶ講座
    （サイバー攻撃からシステムや情報資産を保護するために、まずは攻撃手法の概要を学びたい方におすすめです。）

- **特定のスキルに特化した講座**
  - ゼロから始める AI エンジニア講座セット：AI の知識ゼロから E 資格の取得を目指すセット講座
  - IoT エンジニア育成コース A：Web 開発の基礎から IoT 技術までを学ぶ講座

マナビ DX では、スキル標準のレベル定義をもとに 1～4 のレベルに分けて掲載しています。講座レベルは、検索結果や講座ページで確認することができます。
講座レベルは下の表を確認してください。

マナビ DX の講座レベル

レベル 4	**DX 推進スキル標準・ITSS・ITSS+** 一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題を発見と解決をリードするレベル。プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献する。
レベル 3	**DX 推進スキル標準・ITSS・ITSS+**

	要求された作業をすべて独力で遂行するレベル。専門を持つプロフェッショナルを目指し、必要となる応用的知識・技能を有する。
レベル 2	**DX 推進スキル標準・ITSS・ITSS+** 要求された作業について、上位者の指導の下、その一部を独力で遂行するレベル。プロフェッショナルに向けて必要となる基本的知識・技能を有する。
レベル 1	**DX リテラシー標準** 要求された作業について、上位者の指導を受けて遂行するレベル。プロフェッショナルに向けて必要となる基本知識・技能を有する。

(出典) マナビ DX「マナビ DX での学び方」をもとに作成

マナビ DX での学び方

Point1 キーワードやカテゴリで検索可能

キーワードや「学習できるスキル」や「目指すロール」、「リテラシー講座」といったあらかじめ定義されたカテゴリから講座を探すことができます。

- キーワードから探す
  どの画面でも、ヘッダーからキーワードで検索することが可能です。具体的なキーワードや講座名があればここから検索してください。また、トレンドキーワードを集めた「注目ワード」を利用することもできます。

- スキルやロールから探す
  トップページの「3 つのカテゴリ(リテラシー講座・学習できるスキル・目指すロール)」から講座を絞りこむことができます。これらのカテゴリはデジタルスキル標準に準拠しています。

- マナビ DX オススメから探す
  具体的なキーワードやカテゴリが想像できない場合は、マナビ DX オススメの視点から講座を選ぶことも可能です。

Point2 自分の「お気に入り」や「学習プラン」の作成が可能

マナビ DX にログインすると、講座を記録することができます。

- 「お気に入り」への登録
  学習してみたい講座、気になる講座があれば、「お気に入り」に登録することが可能です。

- 「学習プラン」による計画的な学習の実現
  学習したい講座を見つけたら、「学習プラン」を活用し、計画的な研修受講や受講実績を管理することをお勧めします。「学習プラン」は学習したい講座の登録、学習の進捗、研修の受講実績を管理することができ、計画的、継続的な自己研鑽を実現することができます。

Point3 講座は「デジタルスキル標準（DSS）」と紐付け

「デジタルスキル標準(DSS)」を理解し活用しましょう

マナビ DX に掲載されている講座は、「デジタルスキル標準(DSS)」に紐づけされています。「デジタルスキル標準(DSS)」を活用し、目指すキャリアや習得したい知識・スキルから次の講座を探し、段階的に学習していくことができます。

- 「デジタルスキル標準(DSS)」にはすべてのビジネスパーソンを対象にデジタル技術を理解して活用するスキル（デジタルリテラシー）をまとめた「DX リテラシー標準(DSS-L)」と、高い専門性を持って組織の中で DX を推進するために必要な役割と知識・スキルをまとめた「DX 推進スキル標準(DSS-P)」があります。

- 「デジタルスキル標準(DSS)」を使って、デジタル社会の中でビジネスパーソンに求められている知識・スキルや企業や組織の DX の推進において必要な人材を理解し、自分に必要とされている知識やスキルを整理しましょう。ビジネスパーソンとして必要な知識や習得すべきスキルを、あるいは自分が目指したい人材像や実際の業務を描きながら、現在の自分の強み、弱みを棚卸し、なりたい自分に必要な知識や習得すべきスキルを整理し、学び続けることで、さらなる自己研鑽につなげることができます。

デジタル人材に関する政策や最新テクノロジー情報を知りましょう

学びの継続はとても重要です。ぜひ、マナビ DX の機能を存分に活用し、「もっと知りたい」「もっとスキルアップしたい」を実現するために、計画的、継続的に学ぶことで、自分自身をますます成長させていきましょう。

Point4 最先端の新技術にも対応

デジタルの分野は新しいテクノロジーが次々と出現、進歩していくため、常に最新情報をキャッチし、継続して学び続けることがとても重要です。学び続けることで、更なる自己研鑽をしていきましょう。

- 受講したい研修が見つかったら、講座詳細から、講座提供事業会社のサイトへ進み、研修を申し込みの上、研修を受講しましょう。

（出典）マナビ DX「マナビ DX での学び方」をもとに作成

One Point

デジタル人材育成に関する支援制度から講座を探す方法

マナビ DX では経済産業省を始め、各省庁におけるデジタル人材育成に関する個人、事業者様向けの支援制度を紹介しています。また、第四次産業革命スキル習得講座（経済産業省）、教育訓練給付制度（厚生労働省）、人材開発支援助成金（厚生労働省）などと連携した講座があります。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp
デジタル人材育成政策のご紹介	https://manabi-dx.ipa.go.jp/gov_assist

第25章. スキルと知識を持った人材育成・人材確保方法

章の目的
第 25 章では、カリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を理解することを目的とします。カリキュラムごとに、実践方法を例示します。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること。 ◘ 「IT スキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること。 ◘ 「デジタルスキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること。

25-1. 「プラス・セキュリティ」の実施計画例

セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていくことが必要です。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。昨今は AI を使った新しい攻撃手法が増加しており、昔のスキルや知識だけでは十分に対応することは困難です。この章の前半では、「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を解説します。

この章の後半ではリスキリングに有効と考えられるカリキュラムを例にして、リスキリングのための研修実施計画の策定について解説します。現在、AI や自動化などの新しい技術の導入が進んでいますが、これによって従来の仕事が変化し、新しいスキルが必要になります。中長期でみれば AI などの新技術の普及によって、一部の職業は消滅し、新しい職業が生まれることになるでしょう。そうした変化の中で、個人が市場で競争力を維持するためには、リスキリングを通じて最新の技術や知識を習得し、変化に対応できる能力を高めることが重要です。リスキリングを成功させるためには、チェンジマインド（変革思考）を持つことが非常に重要です。チェンジマインドとは、変化を受け入れ、柔軟に対応する考え方を意味します。リスキリングには新しい知識やスキルを習得するための柔軟な思考が不可欠です。考え方を柔軟に変え、具体的な目標を設定するとともに、信頼できる教材やカリキュラムを選んで、自分にあった学習方法を見つけることが、リスキリング成功の秘訣だと言ってよいでしょう。この章では関係機関が公表しているカリキュラムを参考に、セキュリティに関する学習方法を例示します。

「プラス・セキュリティ知識補充講座 カリキュラム例」の内容を実施するための手順を例示します。

前提条件

中小企業を対象とし、セキュリティ専門家は社内に存在しない。

1.目標の明確化

単元の目標と、到達レベルを明確にします。（以下の表は、部課長級向けの第 3 単元（投資『サイバーセキュリティとリスク対応』）の場合です）

目標
自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル

● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

2.学習方法の検討

カリキュラム内容を学習するための方法を検討します。例えば以下のようなものが挙げられます。

- 専門家の活用

  サイバーセキュリティの専門家や、企業向けにトレーニングサービスを提供する企業を活用して学習します。中小企業に対応できる柔軟なサポートを提供するサービスを優先的に検討することが重要です。例えば、企業のセキュリティ状況に応じたカスタマイズされた研修プログラムを依頼したり、専門家によるワークショップを依頼したりすることが効果的です。

- オンライン学習の活用

  無料や低価格で利用できるオンライン学習プラットフォームを使って、従業員がセキュリティの基礎を学べるようにします。例えば、セキュリティに関する基礎コースを受講できるオンライン学習サイト（例：マナビ DX など）があります。従業員が自分のペースで学習できるため、業務の合間を利用して学びやすいことがメリットです。

- 内部研修の実施

  外部講師を招かず、社内の IT リテラシーが高い従業員が中心となり、セキュリティの基本を他の従業員に教える研修を行います。例えば、社内の担当者が「パスワードの強化方法」や「メールのフィッシング対策」といった実践的な内容を教えることで、全体のセキュリティ意識を高められます。社内の状況に即した内容で実施できるため、企業全体でスムーズに学習が進む点が特徴です。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp/

3.受講者の準備

受講者によってデジタル・ネットワーク技術、サイバーセキュリティに関する知識に差があると考えられます。以下のような方法によって受講の要否を判断することが大切です。

	方法の種類	概要	利点（〇）・欠点（×）
①	セルフチェックに	「〇〇について説明できる」と	〇　動画に比べると準備コストが

	基づく受講者判断	いったチェック項目のリストを提供し、「はい」が一定比率以上の場合は、当該項目の受講を省略できる。	少なく済む × チェック項目が多くなると受講者にとって判断に要する負担が増大する
②	理解度テストによる判定	受講者の理解度を確認する４択問題を出題し、一定以上の得点を得た受講者は当該項目の受講を省略できる。	○ 提示した方法の中で、最も厳密な判定が可能 × カリキュラムの冒頭で「得点が低いので要受講」を示すのは受講意欲を下げる恐れ
③	動画視聴に基づく受講者判断	受講者は次ページに示すシナリオの動画を視聴し、理解度十分（同様の場面で適切な判断が可能）と判断した場合は当該項目の受講を省略できる。	○ 受講者にとっては軽い負担で適切な判断を行うことが可能で利便性に優れる × 動画教材の作成にコストがかかる 事前の目的設定が重要
④	（判断支援手段を提供しない）	各項目を受講するか否かを受講者による判断に委ねてしまう。	○ 判断用教材の準備が不要 × 基礎知識不十分なまま集合講習に参加する受講者が生じる可能性がある

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

そのほか、受講の可否を判断する手段として以下のものが挙げられます。

- 事前アンケートの実施
  セキュリティ知識レベルを把握するために、セルフチェック形式のアンケートを実施します。このアンケートでは、日常的に利用されるデジタルツールやセキュリティ用語の理解度を確認します。アンケートの結果をもとに、カリキュラムを受講する対象者を決定します。部門のマネジメント層で、実際にセキュリティ対応に関与する可能性のあるメンバーを中心に選びます。

4.カリキュラムの実施

カリキュラム内容の実施方法を例示します。（以下は、部課長級向けの第３単元（投資『サイバーセキュリティとリスク対応』）の場合です）

- オンライン研修の実施
  オンデマンド形式で提供される次の事項を学習します。

- サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30 分）
- 対策における費用と損失の考え方（オンデマンド・30 分）

この段階では、サイバー攻撃の基礎やリスク管理の基本概念について学びます。

- 集合講習の実施

集合講習で提供される次の事項を学習します。

- リスクマネジメントのケーススタディ（集合講習：30 分）

集合形式の講習では、講師が具体的なサイバー攻撃事例を紹介し、効果的なセキュリティ対策を解説します。また、参加者同士でディスカッションを行い、演習を通じて理解を深めます。

- 演習の実施

演習 2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60 分）

演習では、リスク対応策のシミュレーションを行い、サイバーセキュリティにおける投資の費用対効果を検討します。参加者は自社に最も適したリスク対応策を模索し、チームで発表を行います。

5.結果の評価と報告

カリキュラム実施後に評価と報告を行います。

- 結果のフィードバック

集合講習後、各部門に対して研修の成果をフィードバックします。各部門が現状のセキュリティ対策を見直し、改善点を明確にします。

- 最終報告書の作成

すべての受講者の意見や研修結果を反映した最終報告書を作成し、経営層に提出します。この報告書は、今後のセキュリティ体制の強化に向けた重要な資料となります。

6.ガントチャートの作成

上記の手順を実施するためのガントチャートを作成することで、進捗状況の管理が容易になります。

ステップ	タスク	サブタスク	期間	担当者	備考
ステップ 1: カリキュラム目標の確認と調整	1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2 日	プロジェクトリーダー	単元の目的と目標を確認

		1.2 経営層との初回ミーティング	1日	プロジェクトリーダー、経営層	経営層との合意形成
		1.3 フィードバックの反映	2日	プロジェクトリーダー	ミーティングの結果を反映
		1.4 最終合意の取得	2日	プロジェクトリーダー	経営層からの最終承認
ステップ 2: 外部パートナーの選定	2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3日	人事部、セキュリティ担当	ベンダー候補をリスト化
		2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当	各ベンダーに要件を共有
		2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層	提案内容の評価と比較
		2.4 ベンダーの選定	2日	人事部、経営層	最終決定を行い、承認
		2.5 契約の準備と締結	2日	人事部、法務担当	契約書の準備と締結
ステップ 3: 受講者の準備	3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント	セルフチェックリストの作成
		3.2 アンケートの配布	1日	人事部	受講対象者へ配布
		3.3 回収と結果の分析	3日	人事部	アンケート結果を集計し分析
		3.4 受講者リストの確定	1日	人事部、セキュリティ担当	受講者リストを最終確定
ステップ 4: カリキュラムの実施	4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント	オンデマンド形式の教材準備
		4.2 学習スケジュールの通知	1日	人事部	受講者にスケジュールを周知
		4.3 受講者の進捗確認	7日	人事部	受講進捗の確認とフォロー
		4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント	オンライン研修を終了
	5. 集合講習の	5.1 講師の手配	2日	セキュリティコンサルタ	集合講習を担当する講師

	実施			ント	を確定
		5.2 集合講習の準備	3 日	講師、サポートスタッフ	教材、演習の準備
		5.3 集合講習の実施	1 日	受講者、講師	集合講習で事例紹介と演習実施
		5.4 演習の実施	1 日	受講者、講師	投資効果分析やリスク対応策を検討
ステップ 5: 結果の評価と報告	6. 結果のフィードバックと報告	6.1 フィードバックの整理	3 日	各部門マネージャー	受講者からフィードバックを収集
		6.2 改善提案の作成	3 日	各部門マネージャー	改善提案を作成
		6.3 改善提案の実行計画作成	2 日	各部門マネージャー	提案に基づいたアクションプランを策定
	7. 最終報告書の作成	7.1 報告書の初稿作成	3 日	プロジェクトリーダー	研修結果をもとに報告書を作成
		7.2 報告書のレビュー	2 日	各部門マネージャー、経営層	レビューとフィードバック
		7.3 報告書の最終版作成	2 日	プロジェクトリーダー	最終報告書を経営層に提出

タスク	サブタスク	期間	担当者	2024年2月							
				1日	2日	3日	4日	5日	6日	7日	8日
1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2日	プロジェクトリーダー								
	1.2 経営層との初回ミーティング	1日	プロジェクトリーダー、経営層								
	1.3 フィードバックの反映	2日	プロジェクトリーダー								
	1.4 最終合意の取得	2日	プロジェクトリーダー								

タスク	サブタスク	期間	担当者	2024年2月												
				9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日	21日	22日
2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3日	人事部、セキュリティ担当														
	2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当														
	2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層														
	2.4 ベンダーの選定	2日	人事部、経営層														
	2.5 契約の準備と締結	2日	人事部、法務担当														

タスク	サブタスク	期間	担当者	2024年2月							3月
				23日	24日	25日	26日	27日	28日	29日	1日
3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント								
	3.2 アンケートの配布	1日	人事部								
	3.3 回収と結果の分析	3日	人事部								
	3.4 受講者リストの確定	1日	人事部、セキュリティ担当								

タスク	サブタスク	期間	担当者	2024年3月												
				2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日	14日	15日
4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント														
	4.2 学習スケジュールの通知	1日	人事部														
	4.3 受講者の進捗確認	7日	人事部														
	4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント														

タスク	サブタスク	期間	担当者	2024年3月							
				16日	17日	18日	19日	20日	21日	22日	23日
5. 集合講習の実施	5.1 講師の手配	2日	セキュリティコンサルタント								
	5.2 集合講習の準備	3日	講師、サポートスタッフ								
	5.3 集合講習の実施	1日	受講者、講師								
	5.4 演習の実施	1日	受講者、講師								

タスク	サブタスク	期間	担当者	2024年3月							
				24日	25日	26日	27日	28日	29日	30日	31日
6. 結果のフィードバックと報告	6.1 フィードバックの整理	3日	各部門マネージャー								
	6.2 改善提案の作成	3日	各部門マネージャー								
	6.3 改善提案の実行計画作成	2日	各部門マネージャー								

タスク	サブタスク	期間	担当者	2024年4月							
				1日	2日	3日	4日	5日	6日	7日	8日
7. 最終報告書の作成	7.1 報告書の初稿作成	3日	プロジェクトリーダー								
	7.2 報告書のレビュー	2日	各部門マネージャー、経営層								
	7.3 報告書の最終版作成	2日	プロジェクトリーダー								

ガントチャート作成後の流れ

以下の 3 つのポイントに焦点を当てることで、ガントチャートを活用したプロジェクト管理が効果的に行え、カリキュラム内容のスムーズな実施につながります。

- 進捗確認とスケジュール管理
  プロジェクトが計画通りに進んでいるかを定期的に確認し、スケジュールに遅れが生じた場合には迅速に対策を講じます。

- リソースの効率的な活用と調整
  限られたリソースを最大限に活用し、必要に応じて適切に調整することで、プロジェクトのスムーズな進行をサポートします。

- リスクの早期特定と対応策の準備
  プロジェクトに潜むリスクをあらかじめ特定し、問題が発生する前に対応策を準備しておくことで、予期しないトラブルにも迅速に対応できる体制を整えます。

25-2. 「リスキリング」「チェンジマインド」の実施計画例

25-2-1. 「IT スキル標準」の実施計画例

IT スキル標準レベル 1「IT 入門（2）」をもとに実施計画を作成する手順を説明します。

1.目標の明確化

学習目標を明確にします。

学習目標
職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

2.目標達成に必要な作業を洗い出す

カリキュラムの知識項目を確認し、学ぶ必要がある項目を整理します。

	タイトル	学習目標	対応する知識項目 （大分類）―（中分類）
第 1 回	オリエンテーション、コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。	• 基礎理論 － 基礎理論 • 技術要素 － マルチメディア
第 2 回	プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。	• 基礎理論 － アルゴリズムとプログラミング
第 3 回	コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。	• コンピュータシステム － ハードウェア • コンピュータシステム － コンピュータ構成要素
第 4 回	ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。	• コンピュータシステム － ソフトウェア
第 5 回	システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。	• コンピュータシステム － システム構成要素
第 6 回	前半のまとめ	前半の講義のまとめを行う。	-

第 7 回	マルチメディアとヒューマンインタフェース	マルチメディアの種類とヒューマンインタフェースの基本的な用語を説明できる。	• 技術要素 – ヒューマンインタフェース • 技術要素 – マルチメディア
第 8 回	ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。	• 技術要素 – ネットワーク
第 9 回	ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。	• 技術要素 – ネットワーク
第 10 回	データベースの技術①	データベースのモデル化と正規化の方法を説明できる。	• 技術要素 – データベース
第 11 回	データベースの技術②	データベースの表操作の方法を説明できる。	• 技術要素 – データベース
第 12 回	情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。	• 技術要素 – セキュリティ
第 13 回	情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。	• 技術要素 – セキュリティ
第 14 回	後半のまとめ	後半の講義のまとめを行う。	-
第 15 回	まとめ	これまでの講義内容を総括する。	-

(出典) IPA「IT スキル標準モデルカリキュラム – レベル 1 を目指して – 」をもとに作成

3.学習内容の詳細化

各回で行う内容を具体的に決めます。例として第 13 回で行う内容は、以下の通りです。

第 13 回 情報セキュリティ対策②（講義 70 分＋演習 20 分）	
学習目標	セキュリティ対策に関する基本的な用語を説明できる。
内容	1．技術的なセキュリティ対策 (1)個人認証技術の種類と特徴 • ID、パスワード

	• コールバック • デジタル署名 • 生体認証技術 (2)暗号化技術の種類と特徴 • 公開鍵暗号方式の仕組み • 秘密鍵暗号方式の仕組み (3)不正侵入・コンピュータウイルス対策 • 入退出管理 • アクセス管理、機密管理 • ファイアウォール・コンピュータウイルスの種類と対策 (4)演習問題【セキュリティの種類と対策】 2. そのほかの情報セキュリティ対策 (1)個人情報の漏えい (2)情報セキュリティポリシー (3)責任と権限の明確化 (4)情報セキュリティマネジメントシステム（ISMS）
研修・教育方法 （予定時間）	講義 70 分 演習 20 分
対応する知識項目	＜共通キャリア・フレームワークの大分類／中分類との対応＞ 技術要素－セキュリティ

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

カリキュラムをもとに、学習内容を具体的にします。

具体的な学習内容（例）
1.技術的なセキュリティ対策 （1）個人認証技術の種類と特徴 個人認証は、システムやネットワークへのアクセスを管理するための基本的な技術です。以下

の主要な技術を説明します。

- ID、パスワード
  最も一般的な認証方法。ID で個人を特定し、パスワードで本人確認を行います。ただし、パスワードの漏えいリスクや、短い・単純なパスワードの使用がセキュリティの脆弱性となりがちです。
- コールバック
  電話やメッセージを使用して本人確認を行う方法。例えば、ログイン時にワンタイムパスワードを送信し、そのパスワードを使用してログインする方法などが含まれます。二要素認証（2FA）の一部として利用されることも多いです。
- デジタル署名
  公開鍵暗号方式を利用して、データの改ざんや成りすましを防ぐ技術。電子的な書類やメールの送信者が本人であることを証明する際に使用されます。
- 生体認証技術
  指紋、顔認証、虹彩認証など、生体的な特徴を利用して個人を特定します。高いセキュリティを実現できますが、技術の精度やプライバシー問題が課題となることもあります。

（2）暗号化技術の種類と特徴

情報を保護するために、データの暗号化は重要です。主に以下の 2 つの暗号化方式があります。

- 公開鍵暗号方式
  暗号化と復号に異なる鍵（公開鍵と秘密鍵）を使用する方式です。公開鍵で暗号化されたデータは対応する秘密鍵でのみ復号可能であり、安全な通信に使われます。
- 秘密鍵暗号方式
  暗号化と復号に同じ鍵を使用する方式。公開鍵暗号に比べて高速で、VPN や Wi-Fi のセキュリティなどに使用されますが、鍵の管理が課題となります。

（3）不正侵入・コンピュータウイルス対策

ネットワークやシステムに対する攻撃を防ぐための対策です。

- 入退出管理
  システムや施設への物理的・論理的なアクセスを制限し、許可された者のみがアクセスできるようにする対策です。カードキーや生体認証が使用されます。
- アクセス管理、機密管理
  特定の情報にアクセスできるユーザーや権限を設定し、無許可のアクセスを防ぎます。これにより、社内のデータ流出や情報漏えいを防ぎます。
- ファイアウォール

ネットワーク間の不正な通信を防ぐための装置またはソフトウェア。パケットフィルタリングやプロキシ機能などを使用し、外部からの攻撃を防ぎます。

- コンピュータウイルス対策
  ウイルス対策ソフトウェアの導入や、定期的なアップデート、メール添付ファイルの検査など、ウイルス感染を防ぐための措置が取られます。

（4）演習問題【セキュリティの種類と対策】
実際の状況を想定したシナリオを使い、各種セキュリティ対策がどのように適用されるかを検討します。
例:新しいウェブサービスを公開する際、どのような認証・暗号化技術を導入すべきかを考察する問題。

2. そのほかの情報セキュリティ対策

(1) 個人情報の漏えい
個人情報の漏えいリスクに対する対策として、データの暗号化、アクセス権限の制限、適切なバックアップの実施が重要です。また、外部とのデータ共有には必ずセキュリティ対策を講じ、セキュアなチャネルを使用することが推奨されます。

(2) 情報セキュリティポリシー
企業や組織が、情報資産をどのように保護するかを明確に定めた規程やガイドラインを「情報セキュリティポリシー」と呼びます。これにより、従業員全員がセキュリティの重要性を理解し、一貫した対策を講じることができます。

(3) 責任と権限の明確化
セキュリティ対策においては、誰がどのような責任を持ち、どのような権限を持つのかを明確にすることが不可欠です。これにより、インシデント発生時の対応がスムーズに進行し、迅速な問題解決が可能となります。

(4) 情報セキュリティマネジメントシステム（ISMS）
ISMS は、企業や組織がセキュリティ管理をシステム的に行うためのフレームワークです。国際規格である ISO/IEC 27001 に準拠して、リスクの評価、管理、改善を繰り返すことで、継続的なセキュリティ強化を図ります。

4.学習方法の選定

カリキュラム内容を学習するための方法を検討します。学習方法を例示します。

- オンライン学習（e ラーニングなど）の利用

無料や低価格で利用できるオンライン学習プラットフォームを活用します。例えば、「マナビ DX」などで、以下のような内容を学びます：

  - パスワードや生体認証技術、暗号化技術の基礎について解説したレッスン
  - 不正アクセス対策やウイルス対策の基本を学べる動画やレッスン
  - 情報セキュリティポリシーや ISMS の基本をカバーする初心者向けのレッスン

- 実践的な演習を取り入れた社内研修

社内で、実際に手を動かして学べる簡単な演習を実施します。例えば、以下のような内容を取り入れます：

  - パスワード管理や二要素認証の設定について、従業員が自分で試すハンズオン研修
  - 簡単なファイアウォールの設定やアクセス管理の仕組みを学べる実践的な演習
  - セキュリティ対策の演習問題の実施

これらの実施により、従業員がすぐに実務に役立てられるスキルを身につけられます。

- 社内ディスカッションと情報共有

定期的に社内でセキュリティに関する話し合いや情報共有の場を設け、従業員同士で意見交換を行います。例えば以下のような事項を取り上げます。

  - 個人情報保護やセキュリティポリシーに関する業務上の注意点や実践方法について
  - ISMS をどのように社内で実践するか、基本的な導入手順や活用方法についてディスカッションを行います。学んだ内容を業務にどのように適用できるかを従業員同士で考えることで、実践的な理解を深め、セキュリティ対策を現場で活かせるようになります。

5.学習の進行と進捗管理

学習を開始し、週次または月次で進捗報告を行います。各セッションの進行状況を確認し、従業員が計画に遅れを取っている場合は、すぐに調整を行います。さらに、定期的なテストや確認を設定し、理解度やスキルの定着度を把握します。

6.フィードバック収集とフォローアップの実施

従業員からのフィードバックを定期的に収集し、内容が難しすぎる、または簡単すぎる場合には、カリキュラムの内容を調整します。さらに、トレーニング終了後も、従業員が学んだことを実際の仕事で活用できているかを確認し、必要に応じて追加のサポートや新しい学習計画を提供します。

25-2-2. 「デジタルスキル標準」の実施計画例

「デジタルスキル標準」は、DX に関する基礎的な知識やスキル・マインドを身につけるための指針としての「DX リテラシー標準」と、DX を推進する人材を育成・採用するための指針としての「DX 推進スキル標準」の 2 種類で構成されています。

25-2-2-1. DX リテラシー標準

DX リテラシー標準では、あらゆるビジネスパーソンに求められる知識・スキルが定義されています。学習項目のうち、「How – セキュリティ」を学ぶための手順を例示します。

1.学習内容の検討

学習する内容を明確にします。「How – セキュリティ」で定義されている内容は以下の通りです。

How – セキュリティの内容
セキュリティ技術の仕組みと個人がとるべき対策に関する知識を持ち、安心してデータやデジタル技術を利用できる。 ● データやデジタル技術に対して徒に不安を感じることなく、適切に利用するためには、情報を守る仕組みを知ることが求められる。 ● 企業が用意する環境・対策に加えて、個人もセキュリティ対策を行う必要性とその方法を理解する必要がある。

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

学習項目例は以下の通りです。

学習項目例
● セキュリティの 3 要素 ✓ 機密性 ✓ 完全性 ✓ 可用性 ● セキュリティ技術 ✓ 暗号 ✓ ワンタイムパスワード ✓ ブロックチェーン ✓ 生体認証 ● 情報セキュリティマネジメントシステム（ISMS） ● 個人がとるべきセキュリティ対策

- ✓ ID やパスワードの管理
- ✓ アクセス権の設定
- ✓ 覗き見防止
- ✓ 添付ファイル付きメールへの警戒
- ✓ 社外メールアドレスへの警戒

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

学習内容を具体的にします。

具体化した学習内容（例）

セキュリティの 3 要素

✓ 機密性

情報を許可された人だけがアクセスできる状態を保つこと。例えば、パスワードや暗号化によってデータを保護します。

✓ 完全性

情報が正確で、改ざんや破壊されていない状態を維持すること。例えば、ハッシュ関数を使ったデータ検証により、データの一貫性を確保します。

✓ 可用性

情報やシステムに必要なときにアクセスできる状態を維持すること。例えば、サーバの冗長化やデータバックアップにより、障害発生時も業務を継続できるようにします。

セキュリティ技術

✓ 暗号

暗号は、データを「鍵」を使って別の形に変える技術です。この変えられたデータは、正しい「鍵」を持っている人だけがもとの形に戻せる仕組みです。

✓ ワンタイムパスワード

一度限り有効な使い捨てのパスワード。時間制限や一回の使用で無効になるため、パスワードが盗まれても再利用されるリスクが低いです。

✓ ブロックチェーン

取引データを分散型の台帳に記録する技術。ブロックチェーンは変更が困難で、データの透明性と信頼性を高めるために使用されます。

✓ 生体認証

ユーザーの身体的特徴（指紋、顔、虹彩など）を使用して本人確認を行う技術。これにより、なりすましのリスクを減らします。

✓ 情報セキュリティマネジメントシステム（ISMS）
組織が情報セキュリティを計画的に管理・運営するための仕組み。ISO 27001 がその基準として有名で、リスクアセスメント、セキュリティ方針の策定、従業員の教育などが含まれます。

個人がとるべきセキュリティ対策

✓ ID やパスワードの管理
複雑なパスワードを使用し、使い回しを避ける。パスワードマネージャーを活用することも推奨されます。

✓ アクセス権の設定
必要最低限のアクセス権限を設定し、不要な権限を持たないようにする。例えば、共有フォルダへのアクセス権限を適切に管理することが重要です。

✓ 覗き見防止
公共の場所で作業する際に、画面を覗かれないように注意する。プライバシーフィルターなどの物理的な対策も効果的です。

✓ 添付ファイル付きメールへの警戒
信頼できない送信者からの添付ファイルは開かない。特に.exe ファイルやスクリプトファイルは注意が必要です。

✓ 社外メールアドレスへの警戒
社外からのメールにはフィッシングや詐欺のリスクが伴うことが多いため、注意深くメールの内容やリンクを確認することが重要です。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp/
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html

2.学習方法の選定

社内研修や、オンライン学習（e ラーニングなど）の利用することも有効です。

3.学習計画の策定

社内研修を実施するための計画を例示します。

学習計画の例

研修期間と目的

期間：半日～1 日（1 セッションあたり 30 分～1 時間）

目的：基本的なセキュリティ知識を学び、実務でのリスクを軽減できるレベルにする。

研修プログラム例

1 日目：セキュリティの基本

内容：セキュリティの 3 要素（機密性、完全性、可用性）の基本説明。

方法：簡単なプレゼンテーションと事例紹介を活用し、各自が自身の業務におけるセキュリティの問題点を考えます。

2 日目：セキュリティ技術の紹介

内容：暗号化、ワンタイムパスワード、生体認証の基本説明。

方法：専門的な用語を避け、従業員が使い慣れている技術やツールを例に出すことで、日常にどう活かせるかを具体的に説明します。

3 日目：個人がとるべきセキュリティ対策

内容：パスワード管理、メールの警戒、物理的なセキュリティの基本説明。

方法：従業員が今すぐできる行動に絞り、具体的な行動リストを共有します。例えば、「今日から自分のパスワードを強化する」「メールのリンクをクリックする前に URL を確認する」といった実践的な対策を提案します。

計画策定のポイント

- 実践的かつシンプルな内容にする
  研修内容は理論に加えて、実際に業務で活かせる具体的な行動を中心に設計します。複雑な専門用語や技術的な話は避け、従業員がすぐに実践できる対策を説明することが重要です。
  例：パスワードを複雑に設定し、パスワード管理ツールを使う方法を教える、メールの不審な点を見分けるチェックリストを提供する。

- 短時間で集中できるセッション構成
  研修は 30 分～1 時間と短く区切り、1 回のセッションで 1 つのテーマに集中するように構成します。従業員の負担を減らし、重要な内容を確実に理解してもらうために、セッションごとに焦点を絞ることが大切です。

例：1 回目は「パスワード管理」、2 回目は「不審メールへの対応」といった具合に、テーマを分けて短い時間で進める。

- 実施後のフォローアップを重視
  研修が終わった後も、理解度や実践状況を確認する仕組みを取り入れることが重要です。例えば、定期的なチェックリストの確認や簡単なクイズで知識の定着を図ります。
  例：研修後に「パスワードを強化しましたか？」などのフォローアップメールや、理解度を測るクイズを実施することで、日常的に意識を高める。

4.学習の実施

計画をもとに、学習を実施する際のポイント上げます。

- 参加者の理解度に合わせた進行
  参加者のセキュリティに対する知識の違いを考慮し、初心者にも分かりやすい言葉を使い、ゆっくり進めることが大切です。難しい言葉や専門用語は避けて、具体的な例を使いながら説明しましょう。
  例：「パスワード管理がなぜ重要か」を説明する際に、複雑な理論ではなく、「簡単なパスワードは悪意のある人に推測されやすい」という形で、わかりやすく説明します。

- 実際の行動を取り入れる
  理論に加えて、実際にやってみる活動を含めることで、参加者が実務にどう活かすかを学べるようにします。実際に手を動かしてみることで、学んだ内容が現実の業務に結びつきやすくなります。
  例：「不審なメールをどう判断するか」を学んだ後、実際にその場でメールを確認してもらう時間を作り、すぐに対策を実行する体験をさせます。

5.フィードバックの収集とフォローアップ

研修後の確認・フォローアップ・フィードバックは、参加者の理解度を深め、セキュリティ意識を継続的に高め、次回の研修をより効果的にするために重要です。

ポイントを 3 つ紹介します。

- 理解度の確認
  研修内容がしっかりと理解されているかを確認するため、簡単なテストやクイズを実施します。これにより、参加者がどの程度理解しているか、また補足が必要な部分があるかを把握できます。

例：「今日学んだセキュリティ対策を実際にどのように実施するか」を問う簡単な質問や選択式のテストを実施します。

- フォローアップと定期的な確認
  研修が終わった後も、継続してセキュリティ意識を高めるために、定期的に復習資料を送ったり、重要なポイントをリマインドするメールを配信したりします。日常的にセキュリティ意識を保つ仕組みを作ることが大切です。
  例：毎月 1 回「パスワードを更新していますか？」や「不審なメールに注意しましょう」といった確認メールを送ります。また、定期的にセキュリティ対策のチェックリストを共有し、従業員が自主的に対策を実践しているか確認します。

- フィードバックの収集
  研修後に参加者からのフィードバックを収集し、研修内容や進行方法についての改善点を把握します。これにより、次回の研修がより効果的なものになります。
  例：「研修で学んだことは役に立ちましたか？」「今後、さらに知りたいセキュリティの内容はありますか？」といった簡単なアンケートを実施し、感想や要望を集めます。

25-2-2-2. DX 推進スキル標準

「人材類型：サイバーセキュリティ」の「サイバーセキュリティマネージャー」の育成の例を紹介します。「サイバーセキュリティマネージャー」に必要なスキルを身につけるための教育・研修の実施計画を例示します。

人材類型	サイバーセキュリティ
ロール	サイバーセキュリティマネージャー
DX の推進において担う責任	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
主な業務	● 新規ビジネスにおけるデジタル活用を通じて生じるサイバーセキュリティ、セーフティ、プライバシー保護に関するリスクを評価する ● リスクとリターンのバランスを踏まえ、サイバーセキュリティリスクの影響を抑制するための戦略や、対策の実施体制を検討する

	● サイバーセキュリティリスク抑制のための対策の実施状況の管理や監査を行う ● 事業実施に用いているデジタル環境で発生するサイバーセキュリティインシデントへの対応を行う
	●
必要なスキル（高い実践力と専門性が必要のみ抜粋）	カテゴリ：セキュリティ サブカテゴリ：セキュリティマネジメント スキル項目 ● セキュリティ体制構築・運営 ● セキュリティマネジメント ● インシデント対応と事業継続 ● プライバシー保護

（出典）IPA「デジタルスキル標準 ver.1.2」をもとに作成

スキルの詳細は以下の通りです。

「セキュリティマネジメント」サブカテゴリーの構造
● セキュリティ体制構築・運営 セキュリティ対策を実施する体制の構築とその維持運営（要員の確保・育成を含む）を円滑に行うためのスキル、および組織としてのセキュリティカルチャーを企業内で醸成する活動を行うためのスキル ● セキュリティマネジメント 情報、サイバー空間、OT/IoT 環境などのセキュリティマネジメントのプロセスを適切に実施するためのスキル ● インシデント対応と事業継続 各種リスク（サイバー攻撃、過失、内部不正、災害、障害など）がデジタル利活用におけるセキュリティインシデントとして顕在化した際の影響を抑制し、事業継続を可能とするためのスキル ● プライバシー保護 パーソナルデータなどのプライバシー情報の保護に求められる要件の理解とその実践に関するスキル

（出典）IPA「デジタルスキル標準 ver.1.2」をもとに作成

上記のスキルを身につけるための実施計画を例示します。

1. 現状分析と目標設定

現状分析

従業員の現在のセキュリティ知識とスキルを評価します。簡単なテストやアンケートでセキュリティに関する理解度を測定し、各自の強みや弱みを把握します。

テストの例は以下の通りです。

セキュリティに関する理解度テストの例

セキュリティ体制構築・運営

Q1. セキュリティ体制を効果的に構築し、維持運営するために最も重要な要素は次のうちどれですか？

a. セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける

b. セキュリティソフトウェアを定期的にアップデートする

c. IT 部門の従業員だけでセキュリティ体制を構築し、他の従業員には任せない

d. 外部ベンダーにすべてのセキュリティ対策を委託する

答え：「a. セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける」

解説: セキュリティ体制の構築や運営は、一度設けたら終わりではなく、常にリスクや組織の変化に応じて見直し、改善することが求められます。従業員の育成や全員が参加するセキュリティカルチャーの醸成も重要です。

セキュリティマネジメント

Q2. セキュリティマネジメントのプロセスで、最も重要な「リスクアセスメント」とは何ですか？

a. セキュリティソフトウェアの更新スケジュールを確認すること

b. 会社のセキュリティ予算を決定すること

c. 企業が直面するセキュリティリスクを評価・分析すること

d. セキュリティインシデントの発生回数を計測すること

答え：「c. 企業が直面するセキュリティリスクを評価・分析すること」

解説: リスクアセスメントは、組織の脅威や脆弱性を特定し、どのようなリスクが最も重大であるかを評価するプロセスです。

インシデント対応と事業継続
Q3. サイバー攻撃が発生した場合に、最初に行うべき対応はどれですか？
a. 影響を受けたシステムを速やかにオフラインにする
b. すぐに新しいセキュリティソフトウェアをインストールする
c. メディアにインシデントを報告する
d. インシデントの原因を調査するためのチームを編成する

答え：「a. 影響を受けたシステムを速やかにオフラインにする」
解説: サイバー攻撃を受けた場合、被害の拡大を防ぐために、まず影響を受けたシステムを隔離することが重要です。

プライバシー保護
Q4. プライバシー保護の観点から、企業が顧客の個人情報を処理する際に最も重要な点は何ですか？
a. データの物理的な保存場所を定期的に変更する
b. データ処理の目的を明確にし、顧客からの同意を得る
c. データを自動で削除するソフトウェアを購入する
d. 顧客にデータ処理の手続きを詳細に説明する

答え：「b. データ処理の目的を明確にし、顧客からの同意を得る」
解説: プライバシー保護法において、データ処理の目的を明示し、事前に顧客の同意を得ることは最も基本的かつ重要な要件です。

スキル習得目標の設定

身につけさせたいスキル（セキュリティ体制構築、セキュリティマネジメント、インシデント対応、プライバシー保護など）を明確にし、何をいつまでに習得するか具体的な目標を設定します。

目標設定の例

1. セキュリティ体制構築・運営
目標:3 ヶ月以内に、基本的なセキュリティポリシーを策定して社内に共有し、従業員全員が日常業務においてそのポリシーを実践できるようにする。
2. セキュリティマネジメント
目標:
3 ヶ月以内に、主要なセキュリティリスクを把握し、それに基づいた簡単なリスク評価（例えば、データバックアップやアクセス権管理）を実施できるようにする。
3. インシデント対応と事業継続

目標:
3 ヶ月以内に、インシデント発生時の基本的な対応フロー（インシデントの報告、初期対応、関係者への連絡）を整備し、従業員がそのフローに従って行動できるようにする。

4. プライバシー保護

目標:
3 ヶ月以内に、顧客データや個人情報の取り扱いに関する基本的なガイドラインを策定し、従業員がデータ保護の基本的な手順を実践できるようにする。

2. 学習計画の作成

目標を達成するための計画を作成します。

計画作成のポイント

2. シンプルで実践的な内容にする

即実践できるスキルを重視

複雑な理論よりも、日常業務で使えるシンプルなスキルを学ばせます。フィッシング対策やパスワード管理など、すぐに役立つ内容を中心にして、従業員がすぐに行動に移せるようにします。

3. 段階的な進行と定期的なフィードバック

進捗を段階的に確認し、小さな成功を積み重ねる

すべてを一度に学ばせるのではなく、段階ごとに小さな成功体験を積み重ねるプランにします。定期的に進捗を確認し、フィードバックを与えて次のステップに進める形にします。

計画作成の例

1. セキュリティ体制構築・運営

目標: 3 ヶ月以内に、基本的なセキュリティポリシーを全従業員に共有し、日常業務において実践できるようにする。

第 1 週 - 第 2 週

セキュリティポリシーの作成

インターネット上で公開されている無料のセキュリティポリシーテンプレートを活用し、パスワード管理やフィッシング対策を含むシンプルなポリシーを作成します。

ツール例: NIST や中小企業向けサイバーセキュリティポリシーの無料リソースを利用。

第 3 週 - 第 4 週

社内で簡単な説明会を開催

経営者や IT 担当者がリーダーとなり、30 分程度の説明会を開催し、セキュリティポリシーの

内容を簡単に説明します。
クイズやディスカッション形式で理解を深めます。

第 5 週 - 第 6 週
実践トレーニング
タスク: USB デバイスの管理と紙資料の処理に関する簡単な演習を実施。
内容
- ✓ USB デバイスの管理: 従業員が USB メモリなどを使用する際、デバイスを適切に取り扱い、安全にデータを移動・管理する方法を実演。
  例：外部デバイスを使う際のリスクや、使用後のデバイスの安全な保管方法を学びます。
- ✓ 紙資料の取り扱い: 紙ベースの情報管理について、重要な資料の廃棄方法（シュレッダーの使用）や、デスクの片付け（クリアデスク）の実践演習を行います。
  例：印刷された重要書類をどのように処理すべきかを実際に体験させます。

第 7 週 - 第 12 週
簡単な社内チェックとフィードバック
月に 1 度、従業員がセキュリティポリシーを実践できているか簡単なチェックを行い、必要に応じて改善フィードバックを行います。

2. セキュリティマネジメント
目標: 3 ヶ月以内に、主要なセキュリティリスクを把握し、簡単なリスク評価を実施できるようにする。

第 1 週 - 第 2 週
主要なリスクのリストアップ
経営者と IT 担当者がリーダーとなり、事業に関連するリスク（データ漏えい、内部不正、機器故障など）をリストアップし、シンプルなリスク評価シートを作成します。

第 3 週 - 第 4 週
データバックアップの実施指導
各部門で定期的に重要データのバックアップが行われるように指導し、クラウドストレージを利用してデータ保護を強化します。

第 5 週 - 第 6 週
アクセス権限の簡単な見直し

各部門で使用しているファイルやシステムに対して、必要な人だけがアクセスできるよう、アクセス権限を見直します。特別なシステムがない場合は、共有フォルダの権限設定を調整。

第 7 週 - 第 12 週
リスク評価結果の共有
各部門が実施したリスク評価の結果を簡単な報告書としてまとめ、全体会議で共有します。大きなリスクに対する対応策を検討し、全従業員に対策を通知。

3. インシデント対応と事業継続
目標: 3 ヶ月以内に、インシデント発生時の基本的な対応フローを整備し、従業員が対応できるようにする。

第 1 週 - 第 2 週
シンプルなインシデント対応フローを作成
報告から初期対応、上司や関係部署への連絡までのシンプルなフローを作成します。例えば、チャットやメールで報告する際のフォーマットを準備。

第 3 週 - 第 4 週
インシデント対応説明会
全従業員に対して、インシデント対応フローの説明会を開催し、実際のシナリオを使って報告の練習を行います。

第 5 週 - 第 6 週
インシデント対応シミュレーション
簡単なインシデント（例えば、ウイルス感染やデータ損失）を想定したシミュレーションを実施し、従業員がフローに従って報告・対応できるかを確認します。

第 7 週 - 第 12 週
定期的なチェックと改善
週に 1 度、インシデントが発生した場合の報告フローをチェックし、問題がないかを確認し、必要に応じてフローを改善します。

4. プライバシー保護
目標: 3 ヶ月以内に、顧客データや個人情報の取り扱いガイドラインを策定し、従業員が実践できるようにする。

第 1 週 - 第 2 週
シンプルなガイドライン作成
法令（個人情報保護法）を参照しつつ、データの収集、保存、破棄に関する基本的な手順をガイドラインとして作成。データの最小限の収集や、不要なデータの定期的な削除方法などを明確にします。

第 3 週 - 第 4 週
従業員向けガイドラインの共有
ガイドラインを全従業員に配布し、短い説明会を通じてデータ保護の基本的な考え方を共有します。

第 5 週 - 第 6 週
データ保護の実践
従業員が日常業務の中で、顧客データの取り扱いやアクセス権の管理を実際に行えるよう指導し、定期的なデータ監査を行います。

第 7 週 - 第 12 週
フォローアップと改善
ガイドラインが遵守されているか、簡単なチェックリストを作成し、各部門で確認します。問題点があればすぐに改善策を検討し、再度周知します。

作成した計画をガントチャートにすることで、進捗管理が容易になったり、スケジュール管理が容易になったりするため、効率的に学習を進めることができます。

セキュリティ体制構築・運営」のガントチャート作成例

タスク ID	タスク名	担当者	開始日	終了日	前提条件	リソース	依存関係	成果の確認ポイント
1	セキュリティポリシーの作成	IT 部門	2024/1/5	2024/1/17	なし	NIST テンプレート	なし	セキュリティポリシー作成完了

2	セキュリティポリシーのレビューと最終化	IT 部門	2024/1/18	2024/1/19	セキュリティポリシーの作成完了	内部リソース	タスク ID 1	ポリシー最終化
3	社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26	ポリシーがレビューされていること	プレゼンテーション資料、共有スペース	タスク ID 2	説明会準備完了
4	社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2	説明会準備完了	参加者、プレゼンテーション資料	タスク ID 3	説明会開催完了
5	USB デバイス管理演習	IT 部門	2024/2/5	2024/2/9	なし	USB メモリ	なし	演習完了
6	紙資料処理演習	総務部	2024/2/13	2024/2/19	USB デバイス管理演習完了	シュレッダー、チェックリスト	タスク ID 5	演習完了
7	セキュリティポリシーの実践状況チェック	IT 部門	2024/2/20	2024/3/4	なし	チェックリスト	なし	ポリシー実践確認完了
8	フィードバックと改善提案の作成	IT 部門	2024/3/5	2024/3/25	チェック完了	フィードバックフォーム	タスク ID 7	改善提案完了

タスク名	担当者	開始日	終了日	2024年1月				2024年2月				2024年3月			
				第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週
セキュリティポリシーの作成	IT部門	2024/1/5	2024/1/17												
セキュリティポリシーのレビューと最終化	IT部門	2024/1/18	2024/1/19												
社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26												
社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2												
USBデバイス管理演習	IT部門	2024/2/5	2024/2/9												
紙資料処理演習	総務部	2024/2/13	2024/2/19												
セキュリティポリシーの実践状況チェック	IT部門	2024/2/20	2024/3/4												
フィードバックと改善提案の作成	IT部門	2024/3/5	2024/3/25												

ガントチャート作成のポイント

✓ タスクを具体的に分解する

プロジェクト全体を小さな作業単位（タスク）に分け、それぞれが具体的で実行可能な内容にします。

例: 「セキュリティポリシー作成」「説明会の準備」など

✓ 依存関係とスケジュールを設定する

各タスクの実行順序と、前のタスクが完了しないと次に進めない場合の依存関係を明示します。また、各タスクの開始日と終了日を設定し、全体のスケジュール管理ができるようにします。

例: 「ポリシー作成が終わってから説明会準備を開始」

✓ 成果物（完了条件）を明確にする

各タスクの完了を確認するための成果物や基準を設定し、進捗状況を評価しやすくします。

例: 「セキュリティポリシーの最終版完成」「説明会が無事に開催された」

これら 3 つのポイントを押さえることで、WBS がシンプルかつ効果的なものになります。

3.学習計画の周知と実施準備

- 従業員への周知
  作成した学習計画を全従業員に共有し、学習目標、内容、進め方について説明します。従業員が学習計画の重要性を理解し、積極的に参加できるように動機づけることが大切です。

- 学習環境の整備
  e ラーニングの導入や、教材、トレーニング資料の準備を整えます。もし外部講師や専門家を招く場合は、そのスケジュールを確保しておきます。

- 担当者の配置とサポート体制の構築
  プランの進行を管理する担当者を設定し、従業員の学習をサポートする体制を整えます。質問や問題が発生した際にすぐに対応できる窓口を作ることも重要です。

4.学習の実行

- スケジュールに従ってトレーニングを進行
  作成したカリキュラムやスケジュールに沿って、トレーニングを開始します。各セッションやモジュールが順調に進んでいるかを確認し、必要に応じて進行を調整します。

- 進捗報告の仕組みの導入
  定期的に学習進捗を確認し、例えば週次または月次の進捗報告会を設けて従業員に学習の進捗状況を報告させることは有効です。これにより、モチベーションを維持し、計画の遅れを早期に発見できます。

5.フィードバックと進捗管理

- 定期的なチェックポイントを設定
  学習プランが順調に進んでいるか確認するために、定期的に学習内容のテストや確認を行います。これにより、理解度の確認と学習の定着を測定できます。

- 従業員からのフィードバック収集
  トレーニングの内容や進め方について、従業員からフィードバックを収集します。もし内容が難しすぎる、もしくは簡単すぎる場合には、カリキュラムの調整を検討します。

6.学習プランの調整

- 進捗に応じたプランの見直し
  進捗状況やフィードバックに基づき、学習プランを柔軟に調整します。例えば、理解が進んで

いる分野はスピードアップし、苦手な部分には追加トレーニングを提供するなど、個々の従業員のニーズに合わせた調整が必要です。

- モチベーション向上施策
  成果が見えにくい段階では、従業員のモチベーションが下がる可能性があります。そのため、小さな成功体験や報酬（例えば、社内での称賛や学習ポイントによるインセンティブ）を設定し、モチベーションを維持します。

7.成果の評価とフィードバック

- 成果の測定とフィードバックの提供
  学習が一通り終了したら、最終的なテストや評価を行い、どの程度スキルが習得されたかを確認します。各従業員に対して個別のフィードバックを行い、今後の改善点やさらなる学習の方向性を示します。

- 学習効果の測定
  学習による効果がどの程度業務に反映されているかも重要です。例えば、セキュリティインシデントの減少や、従業員のセキュリティ対応能力の向上が確認できれば、学習プランが効果的であったと判断できます。

8.フォローアップと継続学習

- 継続的な学習計画の策定
  セキュリティは常に進化しているため、1 度の学習プランで終わるのではなく、継続的な学習計画を策定します。例えば、最新のサイバーセキュリティ脅威に対応するための定期的なアップデートや新しいツールの習得を含めた継続学習が必要です。

- 従業員の定着度合いのモニタリング
  学習内容が業務の中でどの程度実践されているかをモニタリングします。セキュリティインシデント対応やセキュリティガイドラインの実施状況を確認し、従業員が習得したスキルを日常的に活用しているか否かを把握します。

これらのステップを通じて、作成した学習プランが効果的に実行され、従業員が必要なスキルを確実に習得することができます。特に、進捗管理とフィードバックの提供を徹底し、学習の定着を促すことが成功の鍵です。

編集後記

第 9 編では、組織としてサイバーセキュリティ対策を実践するためのスキルや知識、そしてそれらを備えた人材の育成について紹介しました。本編では、経営層から現場のマネジメント層に至るまで、それぞれの役割に応じた教育プログラムやカリキュラムの具体例を取り上げ、企業が持続的なセキュリティ体制を築くための実践的な指針を提供しています。特に、デジタル時代において求められるスキル標準や人材育成の重要性を強調し、セキュリティリスクの管理や対応において、適切な判断を行うための知識の習得が不可欠であることを解説しています。

さらに、変化の速いこの領域では、リスキリングの取り組みが重要です。従業員が新たな知識やスキルを継続的に学ぶことで、組織全体のセキュリティ対応力が高まり、急速に進化する脅威に柔軟に対応できるようになります。リスキリングを通じて、個々のスキルをアップデートしながら、組織としても最新のセキュリティ標準に適応できる体制を整えることが、今後の競争力強化につながります。

本編で紹介したカリキュラムや講座は一つの例です。業種、企業規模などによって合わない場合もあります。状況に合わせて内容を取捨選択し、自社にあった教育プログラムを作成していただくことで、より効果的・効率的に人材育成が可能です。紹介したカリキュラムを参考に自社のご状況を踏まえたカリキュラム作成、講座の選定をお勧めします。

本編で学んだ内容を活用し、各自が組織のセキュリティを高めるための一歩を踏み出していただければと思います。

引用文献

プラス・セキュリティ知識補充講座 カリキュラム例

https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

IT スキル標準モデルカリキュラム – レベル 1 を目指して –

https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

マナビ DX での学び方

https://manabi-dx.ipa.go.jp/how

デジタルスキル標準 ver. 1.2

https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/20240708-p-1.pdf

参考文献

プラス・セキュリティ知識補充講座 カリキュラム例
https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準とは -ものさしとしてのスキル標準
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル 1 を目指して－
https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
マナビ DX
https://manabi-dx.ipa.go.jp
デジタル人材育成政策のご紹介
https://manabi-dx.ipa.go.jp/gov_assist
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン
https://www.ipa.go.jp/security/anshin/measures/start.html

■AI

Artificial Intelligence の略。「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第四次 AI ブームに入ったとの見方もある）。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画

■CSIRT（シーサート）

Computer Security Incident Response Team の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■DFFT

Data Free Flow with Trust の略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

■EDR

Endpoint Detection and Response の略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政法人情報処理推進機構（IPA）内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）

が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■ICT

Information and Communication Technology の略。IT（情報技術）に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常な通信をブロックする機能はない

■IoT（アイ・オー・ティー）

Internet of Things の略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

■IPS

Intrusion Prevention System の略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら 4 つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6 では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携を図る組織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取組。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる

■ISP

個人や企業などに対してインターネットに接続するためのサービスを提供する事業者

のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる

■IT リテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる

■JVN

Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと

■KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの

■LockBit2.0

「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される

■MAC アドレス

Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

■NISC

National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

■NIST サイバーセキュリティフレームワーク（CSF）

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる

■NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

■PII

Personally Identifiable Information の略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号に加えて、氏名、

生年月日、住所、勤務先などの情報も PII に含まれる

■PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管理を行うチームや担当者を指す。

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

■PMO

Project Management Office の略。（企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。）組織全体のプロジェクトを横断的に管理する体制を指す。

政府ガイドラインでの PMO は、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる。

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う（例：計画、予算、執行管理、PJMO 支援など）

■RFI

Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

■SASE（サシー）

Secure Access Service Edge の略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の 1 つで、IT 環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

■SBOM（エスボム）

Software Bill of Materials の略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOM は、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOM は、ソフトウェアのリスクを把握・管理するのに役立つ

■SDP

Software-Defined Perimeter の略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPN は、ネットワーク接続前に一度だけ認証を行うのに対し、SDP は、ユーザーの情報（デバイス、場所、OS など）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

■Society5.0

日本が目指すべき未来社会

の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなってきている。しかし、歴史的経緯で SSL の用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する

■SWG

Secure Web Gateway の略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■WAF（ワフ）

Web Application Firewall の略。 従来のファイアウォールが、IP アドレスとポート番号で通信を制御していたことに対して、Web アプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者に依頼する必要がある

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することにより、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口や ATM に出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェアがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真つきの手配書のようなもの

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

■完全性

参照する情報が改ざんされていなく、正確である特性

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている

■供給者

組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PC やサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている

■コーディング

プログラミング言語でソースコードを書くこと

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまでさまざまである。デジタル社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022

では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される

■情報セキュリティの 3 要素「CIA」

情報セキュリティの 3 つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

■スクリーンセーバ

離席時に PC の画面の内容を盗み見されることを防ぐ機能のこと。PC に対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した 22 歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、独立行政法人情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載することが一般的

■ゼロデイ攻撃

OS やソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開の Web サイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2

つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである

■デジタル情報

0、1、2 のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の 2 進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO27001 の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Em

ail Compromise とも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンの OS に付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

■ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能

性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■ブラックマーケット

広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するインターネット上の市場（闇市）

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Web サーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施することができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

■ミラサポコネクト

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、

支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

■無線 LAN

LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線 LAN を通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

■無停電電源装置

UPS とも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

■リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかのセキュリティ対策を講じる必要がある

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス

■リモートデスクトップ接続

パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法

経営層向けカリキュラム

経営層向け第 1 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要』**
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。
時間設定・実施方式	1 時間 30 分（オンデマンド・省略可能）
①デジタルインフラの基本（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。受講者の負担軽減の観点から、まとめて学習するほうがよい内容を適宜集約する。 a) デジタルサービスの提供に用いられるハードウェアの概要 b) OS、ミドルウェア、アプリケーション、クラウドの概念説明 c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤー
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェアと脆弱性 b) インターネットの仕組み c) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用

	b) デジタルサービスの約款 c) インシデント時の事業継続

経営層向け第２単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。
時間設定・実施方式	1 時間 30 分（オンデマンド 60 分、集合講習 30 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第３単元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法 b) 対策実施上の留意点
③事例紹介（集合講習・30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的にリスクが発現したケースについて被害と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。 • ケース紹介（例：工場停止の影響） • ゲストスピーカーによる説明（例：当事者視点でのインシデント経過の説明）

	• デモンストレーション（例：ランサムウェア感染のデモ）

経営層向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティと投資対効果』**
目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。 ● セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。
時間設定・実施方式	2 時間 10 分（オンデマンド 60 分、集合講習 70 分）
①コーポレートリスクとしてのサイバーセキュリティ（オンデマンド・30 分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。受講者がリスクマネジメントそのものの考え方や保険の仕組みなどは理解していることを前提に、②以降の説明で必要となる概念を確認する。 a) サイバーセキュリティリスクのアセスメント b) リスクへの対応方法 c) 関連法制度とコンプライアンス
②体制構築・人材確保（オンデマンド・30 分）	各種公表資料を参考に、企業の特徴に応じた体制や人材確保・育成に関する考え方を理解する。 a) サイバーセキュリティ対策に関する機能と役割の考え方 b) 外部委託の考え方 c) サイバーセキュリティ体制の構築 d) サイバーセキュリティ対策に従事する人材の確保・育成
③演習 1：各種対策の費用、損失想定、確率値から必要な投資を検討（集合講習：70 分）	サイバーセキュリティ対策における費用対効果分析の基本的な考え方について、事例を踏まえて説明する。受講者 3～4 名で 1 チームを構成し、具体例を想定した上で、ゲーム形式で各種対策の費用、損失想定、確率値から必要な投資を検討し、トータルコストの最小化を競う。

経営層向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティと企業価値』**
目標	● サイバーセキュリティインシデントの発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。
到達レベル	● 自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。
時間設定・実施方式	2 時間 20 分（オンデマンド 60 分、集合講習 80 分）
①インシデント対応における経営層の役割（オンデマンド・30 分）	サイバーセキュリティインシデントの対応プロセスにおいて、経営層がどの場面でどのようにかかわるのが適切なのかを理解する。 a) インシデントに備える b) インシデント対応プロセス
②情報開示の在り方（オンデマンド・30 分）	サイバーセキュリティ対策を適切に実施していることを取引先や社会に伝えることにより、企業価値の維持・向上を図る方法について理解する。 a) サイバーセキュリティに関する情報開示の考え方 b) サイバーセキュリティが企業価値に及ぼす影響
③インシデント対応と情報開示の事例から学ぶ（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法等、実践的な内容を説明する。
④演習 2：インシデント発生時の模擬記者会見（集合講習：50 分）	受講者 3～4 名で 1 テーブルとして、経営者役の 1 名が、マスメディアや企業の広報部門等で記者会見対応に関する経験を有するスタッフが演じるインタビュア役から、自社でのインシデント発生に関する模擬記者会見を行う。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

部課長向けカリキュラム

部課長級向け 第 1-1 単元	
名称	**1.基礎知識**

	『デジタルシステムとサイバーセキュリティの概要（初級編）』
目標	● デジタル化を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	● デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。
時間設定・実施方式	1 時間（オンデマンド・省略可能）
①デジタルインフラ入門（20 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素について、基本的な用語の意味を理解する。 a) デジタルサービスの提供に用いられるハードウェアの紹介 b) OS、ミドルウェア、アプリケーション、クラウドの用語説明 c) IT/OT/IoT がそれぞれ意味するもの
②サイバーセキュリティに関する用語の意味（20 分）	「セキュリティは難しい」という印象を与える背景として、「脆弱性」など日常で用いられないさまざまな用語が用いられることから、よく用いられるサイバーセキュリティ用語の意味の説明を通じて理解を深める。なお、サイバーセキュリティ用語を説明する上で必要となる、ソフトウェアやネットワークに関する用語についても併せて説明する。 a) ソフトウェア開発と脆弱性 b) インターネットの仕組み c) デジタルのリスクに関する諸概念
③デジタル環境の管理や責任に関するキーワード（20 分）	インターネットを通じたサービスなどの提供主体と責任に関する用語について説明する。 a) デジタルビジネスの提供者に関する用語 b) 管理と責任の所在

部課長級向け 第 1-2 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（中級編）』**
目標	デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ● 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ● 新たな施策に伴うリスクとその抑制策の妥当性

到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念について、第 2 単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることにする。
時間設定・実施方式	1 時間 30 分（オンデマンド・必須）
①デジタルインフラの要点（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。 a) デジタルサービスの提供に用いられるハードウェアの構成要素 b) OS、ミドルウェア、アプリケーション、クラウドなどの概念説明 c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤーの役割
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェア開発と脆弱性 b) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用 b) デジタルサービスの約款 c) インシデント時の事業継続

部課長級向け 第 2 単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなか

	った場合の自社での被害想定ができるようになる。
時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第 3 単元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法 b) 対策実施上の留意点
③事例紹介（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的な脅威と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。<デモンストレーションの実施についても検討>
④演習 1：脅威と対策における“悪い見本”から学ぶ（集合講習：60 分）	受講者 3～4 名で 1 テーブルとして、仮想の企業が実施する脅威への不適切な事前準備（リスク評価、資産管理、パッチ適用、従業員教育など）に関する動画（8 分程度）を視聴し、どこに問題があるかを理由と共に指摘し合う。なお、本ディスカッションでは問題の抽出のみにとどめ、対策方法には踏み込まない。

部課長級向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティとリスク対応』**
目標	自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30 分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。 a) サイバーセキュリティにおけるリスクの特徴 b) リスクへの対応方法 c) サイバーセキュリティ対策に関する機能と役割の考え方
②対策における費用と損失の考え方（オンデマンド・30 分）	費用をかけてサイバーセキュリティ対策を実施しても、インシデントが生じない場合の効果が見えにくい。その場合に「何も対策をしていなければ」といった仮定により想定される損失額を試算し、妥当性を評価する方法について理解する。 a) サイバーセキュリティインシデントによる損失 b) 発生確率の考え方 c) 費用と効果のバランス
③リスクマネジメントのケーススタディ（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的なリスク対応体制の事例を紹介し、発生確率や被害の大きさに関する仮定の置き方によってどのように分析結果が変化するかなど、実践的な内容を説明する。
④演習 2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60 分）	受講者 3～4 名で 1 チームを構成し、各参加者はあらかじめ自業種のビジネスモデルと想定するリスクについて整理したものを持ち寄る。それを他の参加者でサイバーセキュリティリスクがどのようなところにあるかを、第 3 単元の内容をもとに相互に指摘する。それについて、第 3 単元で学習したリスクの低減策のうち、どれを適用すべきかを②の内容を踏まえて受講者で議論。1 クール 12～15 分＋講師の講評で構成。

部課長級向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティ対応における社内外連携』**
目標	デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。
到達レベル	● 自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。

時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①インシデント対応プロセスとその準備（オンデマンド・30 分）	サイバーセキュリティインシデントの対応プロセスの一連の流れを理解する。 a) インシデントに備える b) インシデント対応プロセス
②インシデント時の情報の取扱上のポイント（オンデマンド・30 分）	即応性や要求されるインシデント発生時に、社内関係者や取引先との間でどのような情報のやりとりが必要になるか、そのために予め準備しておくことは何か、確実性を含む情報をどのように取り扱うべきかなどについて理解する。 a) インシデント時に提供すべき情報の種類と流れ b) 不確実性を含む情報の取扱い
③インシデント対応と情報開示の事例から学ぶ（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法など、実践的な内容を説明する。
④演習 3：インシデント発生時の社内外連絡（集合講習：60 分）	受講者 3～6 名で 1 テーブルとして、社内関係者や取引先の役割を演じる受講者に対し、所管部署の事業を通じて発生したインシデントに関する情報を伝え、不満や混乱を生じさせないためにはどのような点に留意すべきかを工夫する。あらかじめ講師側にてインシデントのシナリオを作成しておき、被害状況や SOC から提供される情報を時間経過に応じて小出しの形で提供する。小出しする方法はカードに記載して提示、あるいはオンライン会議システムのチャット機能で提供するなど工夫してよい。最終的に、判断が適切に行えていたか否かを自己評価し、講師側の評価と対比する。

部課長級向け 第 5 単元	
名称	**5.関連法令** **『サイバーセキュリティに関する法制度』**
目標	サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	● デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。
時間設定・実施方式	1 時間（オンデマンド・必須）

①サイバーセキュリティに関する国内法令とその読み方（20 分）	サイバーセキュリティ対策の企画・実践に従事する要員が留意すべき法令と具体的な解釈の方法について、『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用を前提に紹介する。 a) サイバーセキュリティ対策において留意すべき法令 b) 『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用
②サイバーセキュリティに関する基準・規格など（20 分）	サイバーセキュリティ対策を実践する上で留意すべき国際基準や規格などについて紹介する。 a) サイバーセキュリティに関する基準・規格など
③サイバーセキュリティに関するガイドラインなど（20 分）	企業がサイバーセキュリティ対策を実践する上で活用が有益なガイドライン・フレームワークなどを紹介する。 a) サイバーセキュリティに関するガイドライン・フレームワークなど

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

付録：IT スキル標準レベル 1　コマタイトル一覧

IT 入門（1）

タイトル	学習目標
オリエンテーション、情報化の変遷と代表的な情報システムの特徴	情報化の変遷と代表的な情報システムの特徴を説明できる。
業種別、業務別の代表的なシステムの概要	企業の組織と利用されている業種別、業務別の代表的なシステムの概要を説明できる。
企業活動と企業会計の基本用語	企業活動の成果を評価するための、会計の基本用語を説明できる。
情報化戦略を策定するために必要な基本用語	経営目標から情報化戦略を策定するために必要な、基本的な用語を説明できる。
情報システム戦略の目的と考え方	企業の事業戦略を受けて、情報システム戦略と全体システム化計画策定に必要な手順と用語が説明できる。
業務要件定義と解決策の検討	情報システム戦略を受けて、自部門の業務課題を分析して、業務要件を定義する代表的な手法と用語を説明できる。
企業規範と身近な法律用語	企業の規範、社会・職場で必要となる身近な法律の用語を説明できる。
前半のまとめ	これまでのストラテジ系科目全体の講義のまとめを行う。
ソフトウェア開発プロセスの作業概要と手順	業務要件をもとに、システム要件の定義から稼働までの作業手順と作業項目の用語を説明できる。
代表的なソフトウェア開発手法の概要	代表的な開発手法に関する目的と概要を説明できる。
情報化におけるプロジェクトの種類とプロジェクト遂行の手順	情報化におけるプロジェクトの種類とプロジェクト計画の立案、開発管理、プロジェクトの完了までの手順と用語を説明できる。
システム運用に関する基本用語	IT サービスマネジメントの意義と目的、サービスマネジメントの全体像とシステム運用に関する用語を説明できる。
システム監査の種類と必要性	情報システムの信頼性、安全性、効率性の向上のために行う、システム監査の必要性および監査の種類と用語を説明できる。
後半のまとめ	これまでのマネジメント系科目全体の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT 入門（2）

タイトル	学習目標
オリエンテーション、コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。
プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。
コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。
ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。
システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。
前半のまとめ	前半の講義のまとめを行う。
マルチメディアとヒューマンインタフェース	マルチメディアの種類とヒューマンインタフェースの基本的な用語を説明できる。
ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。
ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。
データベースの技術①	データベースのモデル化と正規化の方法を説明できる。
データベースの技術②	データベースの表操作の方法を説明できる。
情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。
情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。
後半のまとめ	後半の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

パーソナルスキル入門

タイトル	学習目標
オリエンテーション、職業人に求められるパーソナルスキル	本科目の学習目標や進め方を理解する。職業人として企業で求められるパーソナルスキルの概要を説明できる。
ビジネスマナーの基本①	職業人としてお客様や組織から信頼を得るために必要なビジネスマナーの基本動作が行える。
ビジネスマナーの基本②	職業人として適切な電話対応、報告／連絡／相談、顧客対応が行える。
コミュニケーションの基本（2WAY）①	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して傾聴やインタビューができる。

コミュニケーションの基本（2WAY）②	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して、上司への業務報告やチームの合意形成ができる。
コミュニケーションの基本（情報伝達）	職業人として求められる基本的な情報伝達の知識を業務に活用できる。
コミュニケーションの基本（情報伝達）文書編①	職業人が現場で実践するビジネス文書の基本的な作成方法を説明できる。
コミュニケーションの基本（情報伝達）文書編②	職業人として求められる高品質なビジネス文書の作成方法を理解し、正確でわかりやすいビジネス文書を作成できる。
コミュニケーションの基本（情報伝達）プレゼンテーション編①	職業人が現場で実践する情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本（情報伝達）プレゼンテーション編②	職業人が現場で実践する情報伝達としての高品質な情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本（情報整理・分析・検索）①	職業人が現場で実践する基本的なコミュニケーションマネジメントを説明できる。
コミュニケーションの基本（情報整理・分析・検索）②	職業人として求められるコミュニケーションマネジメントの知識を活用して円滑な会議を進められる。
リーダーシップの基本	職業人に求められるリーダーシップ基本と原則を説明できる。
ネゴシエーションの基本	職業人に求められるネゴシエーションの基本と原則を説明できる。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成