内閣サイバーセキュリティセンター委託調査

令和３年度　企業のサイバーセキュリティ対策推進に関する事業

（「プラス・セキュリティ」知識補充プログラム策定）

調査報告書

令和４年　３月

みずほリサーチ＆テクノロジーズ株式会社

目　次

１．はじめに

１．１ 背景・目的

令和２年度からのコロナ禍を通じ、結果としていわゆる「ニューノーマル」の定着が進んだことに加え、デジタル社会の形成に向けた司令塔たるデジタル庁が 2021 年 9 月に設置されるなど、いまが、我が国が後れをとった経済社会のデジタル化を大きく進める好機であると認識されている。一方で、これと同時にサイバーセキュリティに対する意識や、サイバー空間を構成する基盤等に対する信頼を得られなければ表層的なデジタル化に留まるおそれがある。令和３年 9 月 28 日に閣議決定された「サイバーセキュリティ戦略」においても、こうした認識とともに、「DX with Cybersecurity」というコンセプトの下、あらゆる主体においてこれが意識され、取組が推進されるべきとの方向性が示されている。

当該戦略では、例えば、経営層の意識改革（４．１．１）の項目において、デジタル化に取り組む先進的な取組企業の選定・公表、デジタル関連投資への税制措置等のデジタル化促進施策においてサイバーセキュリティを位置づけることや、取組状況を企業内外可視化するためのツール等の活用を促進することなど、各種の取組を進めることとしている。加えて、これらの取組をより実効的なものとする観点から、経営層あるいは経営層を支える戦略マネジメント層等に対し、IT やセキュリティに関する専門知識や業務経験を有していない場合にも、社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習得すべき知識（以下「『プラス・セキュリティ』知識」という。）を補充できる環境整備を進めることとしている。

本事業は、この取組を具体化することを目的とするものである。上述のとおり、これは、ひいては、経済社会全体での DX with Cybersecurity 推進につながるものである。

１．２ 略称について

本報告書で用いる略称は、それぞれ次の意味を示すものとする。

CEO	最高執行責任者
CFO	最高財務責任者
CIO	最高情報責任者
CISO	最高情報セキュリティ責任者
CRIC-CSF	産業横断サイバーセキュリティ検討会
CSIRT	Computer Security Incident Response Team
DB	データベース
ICT	情報通信技術
IoT	Internet of Things
IP	インターネットプロトコル
IT	情報技術
IPA	独立行政法人情報処理推進機構
ISAC	Information Sharing and Analysis Center
ISMS	情報セキュリティマネジメントシステム
ISP	インターネット接続サービス事業者
JNSA	特定非営利活動法人日本ネットワークセキュリティ協会
JPCERT/CC	一般社団法人 JPCERT コーディネーションセンター
MIT	マサチューセッツ工科大学
NACD	National Association of Corporate Directors
NCA	日本コンピュータセキュリティインシデント対応チーム協議会
NICE	National Initiative for Cybersecurity Education
NICT	国立研究開発法人情報通信研究機構
NISC	内閣官房内閣サイバーセキュリティセンター
NIST	米国国立標準技術研究所
OS	オペレーティングシステム
PC	パーソナルコンピュータ
SOC	セキュリティオペレーションセンター

２．既存の「プラス・セキュリティ」知識補充プログラムの状況

本事業でのプログラム策定に先立ち、本事業と類似の対象者向けの「プラス・セキュリティ」知識補充プログラムに相当する内容についての調査を実施した結果を示す。

２．１ 調査対象範囲

市中に存在するサイバーセキュリティに関する知識を補充するプログラムのうち、本調査の対象とする「(i) デジタル経営を推進する企業の経営層」及び「(ii) それら企業において業務、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」をターゲットとして、「プラス・セキュリティ」知識を補充するプログラムに該当すると考えられるものをリストアップした上で、必要な情報を整理した。

なお、調査にあたっては、本事業の趣旨を踏まえ、受講に要する期間が一定期間以上（おおむね３か月以上）のプログラムは調査対象から除外した。

２．２ 既存プログラム事例

２．２．１ 国内事例

（１）既存プログラムの状況

国内については、経営層やマネジメント層を対象とするサイバーセキュリティに関する教育プログラムは、単発的なセミナー的な講座を除けばほとんど存在しない。

⑵①で示す地域の経営層及び戦略マネジメント層を対象としたインシデント演習は、「知識補充」とはやや異なる手段を用いるプログラムではあるものの、受講者の条件を満たす稀少な事例である。これは総務省の令和 2 年度事業「地域のセキュリティコミュニティの構築・強化に向けたインシデント演習に係る調査研究及びインシデント演習運営の請負」において企画されたものである。

（２）プログラム事例

既存プログラムに関する調査結果を示す。なお、記載内容は調査時点（2021 年 11 月）時点のものである。

① 経営層向けインシデント対応演習

プログラム名称	経営層向けサイバーセキュリティ演習
実施機関	近畿経済産業局、近畿総合通信局、一般財団法人関西情報センター
レベル	初級
概要	今後セキュリティリスクに関する経営判断を行う機会がますます増える現状とインシデント発生時に経営層としてどのような行動をとるべきかという点を理解・検討いただくため、講演と演習を組み合わせた「経営層向け

<table>
<tr><td></td><td>サイバーセキュリティ演習」を行う。</td></tr>
<tr><td>目標</td><td>（概要より抜粋）インシデント発生時に経営層としてどのような行動をとるべきかという点を理解・検討できること</td></tr>
<tr><td>受講者の要件</td><td>なし</td></tr>
<tr><td>方法</td><td>集合講習</td></tr>
<tr><td>所要期間</td><td>半日（13:30～16:50）</td></tr>
<tr><td>費用</td><td>無料</td></tr>
<tr><td>コース内容</td><td>（令和 2 年度のプログラム）
<table>
<tr><th>時間</th><th>プログラム内容</th></tr>
<tr><td>13:00～</td><td>開場</td></tr>
<tr><td>13:30～13:35</td><td>開会挨拶</td></tr>
<tr><td>13:30～13:35</td><td>■講演「セキュリティ事件・事故発生時の効果的な対応」</td></tr>
<tr><td>13:35～14:25</td><td>休憩</td></tr>
<tr><td>14:35～16:45
（休憩時間を含む）</td><td>■演習（グループワーク）
「ホームページの欠点をついた不正アクセス」</td></tr>
<tr><td>16:45～16:50</td><td>閉会挨拶</td></tr>
</table></td></tr>
<tr><td>紹介 URL</td><td>https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/200221press.html</td></tr>
<tr><td>備考</td><td>総務省の令和 2 年度事業「地域のセキュリティコミュニティの構築・強化に向けたインシデント演習に係る調査研究及びインシデント演習運営の請負」（請負者：株式会社野村総合研究所）として企画されたが、コロナ禍により中止となった。</td></tr>
</table>

② 戦略マネジメント系セミナー

プログラム名	戦略マネジメント系セミナー
実施機関	独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター
レベル	初級
概要	組織全体のセキュリティレベル向上を目指し、セキュリティ対策を組織横断的に統括する体制及びその責任者の役割について理解を深める。
目標	・ビジネスのデジタル化・DX に伴うリスクの変化に対応して、セキュリティ対策を組織横断的に統括することができる「セキュリティ統括責任者」を育成する。 ・本セミナーを受講することによって、セキュリティ統括責任者としての心構え、あり方を理解し、セキュリティ対策・インシデント対応のスキルを強化することができる。 ・セキュリティ人材（受講者、ファシリテータ、講師）との人脈形成、ネットワークの構築をすることができる。
受講者の要件	なし
方法	講演・講義はハイブリッド、ディスカッションは対面にて実施
所要期間	4 日間（講演・講義 2 日、ディスカッション 2 日）
費用	15 万円（税込）

<table>
<tr><td>コース内容</td><td>（令和３年度の実施例）
<table>
<tr><th>日程</th><th>プログラム名</th><th>形態</th><th>内容</th></tr>
<tr><td>1 月 20 日(木)
PM</td><td>有識者講演</td><td>対面または
オンライン</td><td>サイバーセキュリティの政策動向や、企業のマネジメント の実態などが理解できる講演を提供します。</td></tr>
<tr><td>1 月 21 日(金)
終日</td><td>プログラム講義</td><td>対面または
オンライン</td><td>最新のセキュリティ事故事例の紹介や、セキュリティ統括 責任者の役割などが理解できる講義を提供します。</td></tr>
<tr><td>2 月 10 日(木)
終日</td><td>ディスカッション
1 回目</td><td>対面</td><td rowspan="2">• グループワークにより受講者の自部門の状況を見直す 機会を提供します。
• ファシリテータが活発な議論を促すとともに、最新事例を取り入れた解説やティーチングを行います。</td></tr>
<tr><td>2 月 24 日(木)
終日</td><td>ディスカッション
2 回目</td><td>対面</td></tr>
</table></td></tr>
<tr><td>紹介 URL</td><td>https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2021.html</td></tr>
<tr><td>備考</td><td>－</td></tr>
</table>

③ 管理職向け情報セキュリティ講座

プログラム名称	管理職向け　情報セキュリティ講座（１）
実施機関	株式会社ラック（ラックセキュリティアカデミー）
レベル	初級
概要	組織の管理職、セキュリティ対策担当者、セキュリティ委員会等メンバーを対象に、情報セキュリティを推進する上で管理職としてどのような役割が求められているか、その役割を担うために管理職として「知っておくべきこと」「やるべきこと」「やってはいけないこと」について情報セキュリティの観点から学習する。
目標	・情報セキュリティを推進する上で管理職に求められる役割を知る ・情報セキュリティに係る意識が向上する
受講者の要件	なし
方法	オンデマンド
所要期間	25 分（有効期間 30 日）
費用	4,400 円
コース内容	1.はじめに 2.管理職・リーダーが「知っておくべきこと」 3.管理職・リーダーが「やるべきこと」 4.管理職・リーダーが「やってはいけないこと」 5.まとめ 6.確認テスト
紹介 URL	https://www.lac.co.jp/service/education/ola_manager_first.html
備考	－

２．２．２ 海外事例

（１）既存プログラムの状況

調査の結果、既存プログラムの状況について次の傾向が認められた。

- 欧米、イスラエル、シンガポール等について検索した範囲では、2.1 に示す調査対象に相当するプログラムはほぼ米国に集中して実施されている状況である。調査にあたっては、英語で検索すると英語圏以外の国の公用語で実施されているプログラムが検索対象外となる恐れがあることから、機械翻訳を用いて各国公用語での検索も試みたが、経営層等を対象としているプログラムは調査時点においてほとんど実施されていない。
- コロナ禍の影響でオンラインによる実施が多くなっているが、大半のプログラムは開催時刻を定めて実施される同時（ライブ）型である。一部プログラムにおいて、受講者の利便性の観点からオンライン・オンデマンドでの開催を行っている事例（①の全米取締役協会の事例）がみられる。

（２）プログラム事例

既存プログラムに関する調査結果を示す。なお、記載内容は調査時点（2021 年 11 月）時点のものである。

① Cyber-Risk Oversight Certificate

プログラム名称	Cyber-Risk Oversight Certificate
実施機関	全米取締役協会（NACD）、カーネギーメロン大学
レベル	初級
概要	・全米取締役協会（NACD）がカーネギーメロン大学の協力を得てオンラインで提供している取締役向けサイバーリスク管理に関する概説的コース。 ・最終試験に合格することで履修証明の取得が可能。
目標	取締役向けのサイバーセキュリティに関する主要な認証を取得するためのプログラムとして、以下のオンライン自習型プログラムを提供する： ・サイバーセキュリティの脅威についての理解を深める ・サイバーリスクの監視における取締役会と経営層の責任を列挙する ・サイバークライシスのシミュレーションを行い、組織の準備状況を評価する ・高度なサイバーリスクの監視に関する学習結果として、資格情報を取得する コースを修了し、一連の試験に合格した受講者には、カーネギーメロン大学ソフトウェア工学研究所の CERT 部門が発行する「CERT Certificate in Cybersecurity Oversight」が授与される。
受講者の要件	受講に先立って NACD Director's Handbook on Cyber Risk Oversight（経団連による和訳[1]あり）の事前参照を推奨。

[1] 『サイバーリスクハンドブック　取締役向けハンドブック　日本版』

方法	オンライン・オンデマンド
所要期間	16 時間（最終試験を含む、都合のよい時間に受講可）
費用	非会員$4,495-　会員$3,995-
コース内容	本プログラムはサイバークライシスのシミュレーション演習と一連の試験を含む 7 つのモジュールで構成される。CERT 認定を取得するには、プログラム内の試験を登録から 1 年以内に完了する必要がある。 1：NACD による歓迎 2：取締役に対するサイバーセキュリティの監督 3：サイバーセキュリティにおけるリーダーシップの概要 4：効果的なセキュリティ体制と運用 5：取締役に対するサイバーセキュリティの監督 6：サイバークライシスシミュレーション演習 7：取締役に対するサイバーセキュリティ監督の概要 プログラム試験：受講者は CERT Certificate を取得するために、プログラム試験に合格する必要がある。
紹介 URL	https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092
備考	―

② Cybersecurity and Crisis Management for Boards

プログラム名称	Cybersecurity and Crisis Management for Boards
実施機関	カリフォルニア大学ロサンゼルス校（UCLA）アンダーソン校 スクールオブマネジメント
レベル	初級
概要	取締役を対象に、サイバーセキュリティ、危機管理、ステークホルダーエンゲージメントの 3 部構成を通じて、経営層に求められるグローバル環境でのリスクマネジメント能力を習得させる。
目標	参加者は、プログラム終了時にリアルタイムで状況に適用できる危機対応のフレームワーク、方法論、および考え方を理解する。経営陣に適切なタイミングで適切な質問をする準備を行うとともに、今日のグローバルなデジタルビジネス環境に関連する 3 つの主要なリスク領域に関する取締役会による警戒と回復に関する能力に貢献できるようになる。
受講者の要件	なし
方法	オンライン
所要期間	連続する 3 日間
費用	$4,000-
コース内容	＜1 日目＞ ● 取締役会のための危機管理の原則 ● 企業の危機に直面した取締役会メンバーのための 10 のヒント ● 現在のサイバーセキュリティの状況 ● ランサムウェアによる“パンデミック” ● ネットワーキング“ハッピーアワー”

https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

	＜2 日目＞ ● サイバーセキュリティ危機のシナリオ ● サイバーセキュリティ危機のシナリオ：アクションレビュー後 ● 基調講演 ● まとめに向けて：レジリエンスとアクションプランニング ＜3 日目＞ ● 理論から実践へ：ケーススタディ 1 ● 理論から実践へ：ケーススタディ 2 ● ステイクホルダーによる関与のためのフレームワーク ● 危機におけるステイクホルダーによる関与の管理
紹介 URL	https://www.anderson.ucla.edu/executive-education/open-enrollment/cybersecurity-for-boards
備考	―

③ Cybersecurity Oversight for the Business Executive

プログラム名称	Cybersecurity Oversight for the Business Executive
実施機関	カーネギーメロン大学（CMU）ソフトウェア工学研究所（SEI）
レベル	初級
概要	オンラインと集合講習の双方で提供する 2 日間のプログラム。CISO に指示を与える経営層を主たる対象とするが、CIO/CISO として改善に取り組む人材にも有益とされている。
目標	このコースの最後に、参加者は次のことができるようになる。 ● サイバーセキュリティの監視に不可欠な主要コンポーネントの把握 ● 組織のガバナンス及び防御のための主要なフレームワークの把握 ● 取締役会向けのサイバーセキュリティに関する考慮事項の説明 ● アセスメントと測定に関する様々な手法の説明
受講者の要件	なし
方法	オンライン又は集合
所要期間	連続する 2 日間の 8:30-16:30
費用	国外$3,750-, 米国企業$2,500-, 米国政府学生$2,000-
コース内容	● エグゼクティブのためのサイバーセキュリティ監視 ● サイバーセキュリティにおけるリーダーシップの概要 ● 効果的なセキュリティ体制と運用 ● 取締役および取締役会のためのサイバーセキュリティ監視 ● サイバーセキュリティアセスメントと測定 ● サイバーセキュリティに関する状況認識の維持 ● サイバーセキュリティ監視のまとめ
紹介 URL	https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P144
備考	―

④ Applied Cybersecurity

プログラム名称	Applied Cybersecurity
実施機関	マサチューセッツ工科大学（MIT）

レベル	初級～中級
概要	工学及びコンピュータのスキルが十分でない人材でもサイバーセキュリティの最新のトピックを学ぶことができるとされている。
目標	● 多様な状況にあるシステムへの対策の適用、個人データの保護、簡単なコンピューターネットワークの保護し、安全にインターネット利用の実践に関する方法を学ぶ ● サイバー法、知的財産およびサイバー犯罪、商標、ドメイン盗難の主要な用語と概念を理解する ● フォレンジックの調達におけるコンピュータ技術、デジタル証拠収集、及び証拠に関する報告方法を規定する ● 安全なネットワーク、ファイアウォール、侵入検知システム、および侵入防止システムを導入する ● 安全なソフトウェア構築に関するプラクティスを調査する ● Web セキュリティの原則を理解する ● インシデントの分析と対応のためのベストプラクティスを導入する ● リスク管理戦略を採用する
受講者の要件	2009 年以降のラップトップ PC（最新のオペレーティングシステムと管理者権限が必要）
方法	オンライン
所要期間	5 週間（1 週あたり 2 セッションの合計 10 セッション）
費用	$2,500-
コース内容	1. サイバーセキュリティの概要とコース内容の説明 2. インターネットとネットワークの基本 : レイヤーモデル、アドレスとメッセージプロトコル、ネットワーク管理 3. ソーシャルエンジニアリング : サイバースペースにおける脅威からの防御、サイバーセキュリティのガイダンスと状況認識 4. 暗号化の基本 : ID、認証、承認、暗号化、署名、および Kerberos の例 5. 脅威モデリング : サイバーセキュリティの基本原則とプラクティス、プラクティスの状態、ベストプラクティス、および新たなパターン 6. ワールドワイドウェブ : ブラウザトラフィック、IoT、モバイルコンピューティング 7. ブロックチェーンの基礎 : ブロックチェーンテクノロジー、ブロックチェーンの基本原則とベストプラクティス、および企業でのテクノロジーの活用 8. FANGS と VUCA の世界の台頭 : ウクライナの攻撃、NSA、スノーデン 9. DevSecOps、リーダーシップと組織の変革 : 人とプロセス、採用、インセンティブの戦略と報酬 10. コースまとめ : プロジェクト成果のプレゼンテーションと履修証明の授与
紹介 URL	https://professional.mit.edu/course-catalog/applied-cybersecurity-0
備考	－

⑤ Cybersecurity and Executive Strategy

プログラム名称	Cybersecurity and Executive Strategy

実施機関	スタンフォード大学
レベル	初級～中級
概要	経営者、CISO、エンジニアへのインタビュー等を通じて事業戦略におけるリスク軽減に必要なサイバーセキュリティの技術的側面について学ぶ。 Advanced Cybersecurity Program の一部であるが、単独での受講も可能。
目標	ニュースサイトを開くと、深刻なサイバーセキュリティ攻撃に関する最近の記事を見つけることができる。ただし、多くの上級管理職はサイバーセキュリティの技術的側面を理解していないため、リスクを軽減するために必要なリソースを十分に割り当てないことが多い。 このコースでは、技術的及び非技術的な経営幹部のリーダーシップを含むすべてのレベルの管理者に、サイバーセキュリティを重要視すべき理由を説明するための方法を学ぶ。さらに、セキュリティとリスクの軽減が企業戦略における主要な要素となるように、上級管理職を教育して影響を与えるための方法を学ぶ。
受講者の要件	なし
方法	オンライン
所要期間	7 時間のビデオ受講と 1.5 時間のコースワーク
費用	$495-（1 講座あたり）
コース内容	● 取締役会の関与に関する重要な質問と原則 ● ブラックボックスおよびホワイトボックスによるセキュリティ評価とメトリクス ● 脆弱性に関する優先度の設定 ● 違反行為への備え ● リスクアセスメント ● サイバー保険
紹介 URL	https://online.stanford.edu/courses/xacs302-cybersecurity-and-executive-strategy
備考	―

⑥ Managing Cybersecurity Risk

プログラム名称	Managing Cybersecurity Risk
実施機関	シンガポール国立大学
レベル	初級～中級
概要	以下の受講者を対象に実施するサイバーセキュリティリスクの概要と対応方法に関する講座： ・リスクマネージャー、コンプライアンス管理者 ・サイバーセキュリティ対策を必要とする事業プロジェクト管理者、ビジネスリーダー ・プロジェクトスポンサー
目標	コースを完了すると、参加者は次のことが可能となる： ● サイバーセキュリティ戦略とポリシーの理解 ● 潜在的なサイバー脅威とシステムの脆弱性に関する知識の把握 ● 自組織とシステムに関連する脅威とリスクの特定 ● 特定した脅威のビジネスへの影響の評価、及び望ましい対応策の策定 ● サイバーセキュリティ要件の計画とステイクホルダーへの伝達

	● サイバー攻撃への迅速な対応を可能とする計画の立案 ● サイバー攻撃への対応中の意思決定の確立又は改善
受講者の要件	インターネット接続可能なラップトップ PC（Core i5 以降、Windows 10Pro、8GB メモリ、Chrome ブラウザ内蔵）
方法	集合講習（講義、ケーススタディ、及びグループ演習）
所要期間	3 日間（9:00-17:00）
費用	Singapore$2,889-（割引制度あり）
コース内容	・サイバーセキュリティ戦略の立案 ・サイバーセキュリティ対策方針の作成 ・セキュリティアーキテクチャのコンセプト ・情報リスクマネジメントへのアプローチ ・サイバーレジリエンス ・ギャップ解消のためのアクションプラン
紹介 URL	https://www.iss.nus.edu.sg/executive-education/course/detail/managing-cybersecurity--risk
備考	－

２．３ 調査結果からの観察事項

調査結果から、既存プログラム事例に関して次の傾向が観察される。

① 短期（フルタイム換算で２～３日）が多い

- 多忙な受講者が多く、受講のための時間を確保することが困難な状況に配慮しているものと見込まれる。本調査で検討するカリキュラムを実施する場合でも、同様の配慮がおそらく必要と考えられる。
- 短期の割に受講費用が高額なプログラムについては、受講者において「そのような高額な費用を負担しても見合う効果が得られる」との判断が行われていることの反映といえるが、実施機関への社会的な評価（ブランド力等）の影響も考えられる。

② サイバーセキュリティの前提知識（IT やネットワークの基礎）は含まれない

- IT やネットワークの基礎知識を有することが明示的な要件となっていない事例がほとんどであるが、教育内容から受講者は予めこれらの基礎知識を備えていることを前提としていることが推測される。

③ 教育内容は「サイバーリスクにどう備えるか」に相当する内容が中心

- 各プログラムにおいて、実施する教育機関が得意とする内容に応じて個性が出ているが、いずれにおいても経営層や管理職として事前及び非常時に適切な判断を行えるようにするためにどのようなことを知っておくべきか、という観点にプログラムの力点が置かれているものと推察される。

３．「プラス・セキュリティ」知識補充プログラムに求められる要件

本事業の趣旨を踏まえ、第４章で検討すべき「プラス・セキュリティ」知識補充プログラムについて、満たすべき要件を明確化する。

３．１ 対象者の設定とその特性

要件検討に際して、本事業で策定する「プラス・セキュリティ」知識補充プログラムの受講対象者について、次表のような設定又は想定を行うこととする。

表 １　本事業における「プラス・セキュリティ」知識補充プログラム対象者の設定又は想定

	デジタル経営を推進する企業の経営層	企業において業務、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対策における主な役割	自組織におけるサイバーセキュリティリスクに応じた対策実施に関する意思決定	担当部署におけるサイバーセクリティリスクの把握とそれに応じた対策の実施、及び自社の方針として定められている対策の遵守
デジタル環境や通信ネットワークに関する知識	マスメディアで話題になるキーワード（5G、IoT、クラウド等）を認識している程度	自ら利用するPCのネットワーク環境設定等を通じて、キーワードについての一定の知識を有する
サイバーセキュリティ対策に関する知識・経験	リテラシーレベル（安易なパスワードを使わない、不審な電子メールの添付ファイルやURLを参照しない等の知識を有する程度）	リテラシーレベル（安易なパスワードを使わない、不審な電子メールの添付ファイルやURLを参照しない等の知識を有する程度）
リスクマネジメントに関する知識・経験	自社の事業リスクについて、その想定をもとにどのような対策投資（保険加入を含む）をすべきかの判断を行った経験を有する	担当する事業についてのリスクを想定し、その抑制のための対策について検討した経験を有する
受講に際しての条件	受講のための時間確保が著しく困難であり、必要最小限の時間での実施が望ましい	経営層と比較すると相対的に時間確保は可能であるが、可能な限り短期での実施が望ましい

３．２ プログラムの実施方法

受講対象者がオンラインでのグループ演習を行うことに慣れていないことを想定し、集合講習による実施を前提とする。一方で、オンライン形式のうちオンデマンド方式は受講対象者の都合に応じて受講できる利点を有し、多忙と見込まれる受講者において利用価値が高いと考えられることから、集合形での実施を必要としない内容については、受講者が都合のよい時間にオンラインで受講できることとするのが望ましい。そこで、本事業で策定する「プラス・セキュリティ」知識補充プログラムは集合講習とオンライン（オンデマンド）形式のハイブリッドで実施することを前提に検討することとする。

３．３ 既存フレームワークとの対応

プログラムで扱う知識やスキルの内容が、対象者が組織におけるサイバーセキュリティ対策で担う役割を遂行する上で必要となる知識・スキルを適切にカバーしているかどうかを担保する手段として、サイバーセキュリティ分野を扱う既存のフレームワークや標準的なシラバス等との対応関係を整理する。整理対象とするフレームワークの候補として次表の項目を抽出し、表内の選定方針をもとに対象とするフレームワーク等の選定を実施した。

このほか、NISC にて 2020 年度に実施した取組における整理結果との対応関係についても整理することとする。

表 2　対応関係の整理に用いるフレームワーク等の選定

フレームワーク等	サイバーセキュリティに関する記述内容	選定方針
NIST SP800-181[2]	（すべてサイバーセキュリティ関連ロールとタスクに関する記述）	4.1 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向けカリキュラム作成時の扱うべき知識・スキルのベースとして利用する。
IT リテラシースタンダード[3]	「C.リスク対応」において、規程・方針、脅威、対策の各項で基本的な考え方や概要を学ぶ。演習として「情報モラルに違反する事柄」「自社（自分）にとっての情報セキュリティ上の脅威の列挙とそれに対する対策の検討」などが例示されている。	上述の NIST SP800-181 が米国のサイバーセキュリティ業務向けであることから、日本国内を対象とするこれらのスタンダード及シラバスとの対応関係を併せて整理することで補完の位置付けで利用する。
IT パスポート試験シラバス[4]	「61.情報セキュリティ」「62.情報セキュリティ管理」及び「63.情報セキュリティ対策・情報セキュリティ実装技術」において基本的概念の理解を求めている。（ITSS レベル 1 相当）	
情報セキュリティマネジメント試験シラバス[5]	（すべて情報セキュリティマネジメントに関する記述、ITSS レベル 2 相当）	
数理・データサイエンス・AI（応用基礎レベル）モデルカリキュラム[6]	「2-6.IT セキュリティ」として、セキュリティの3要素、暗号化、データに対する脅威（盗聴、改ざん、なりすまし）、電子署名、PKI、ユーザ認証、アクセス管理、マルウェアによるリスク等のキーワードを扱う。	モデルカリキュラムに示されている内容は、上記の IT パスポート試験や情報セキュリティマネジメント試験シラバスで網羅されていることから、対応関係の整理を行わない。
データサイエンティスト検定リテラシーレベル[7]	「3-2.データを守る上での留意事項」として、情報セキュリティの基本概念、匿名加工情報、暗号化、パスワード、悪意ある情報窃取などのキーワードを扱う。	
情報 I 学習指導要領[8]	「第 5 節　情報セキュリティ」として、情報社会と情報セキュリティ、情報セキュリティと法規、情報セキュリティ対策、情報セキュリティマネジメントの4分野を扱う。	高校生向けであり、今回の対象者との相違が著しいことから、対応関係の整理を行わない。

[2] https://csrc.nist.gov/publications/detail/sp/800-181/archive/2017-08-07
[3] https://www.ipa.go.jp/jinzai/itss/itls.html
[4] https://www.jitec.ipa.go.jp/1_13download/syllabus_ip_ver6_0.pdf
[5] https://www.jitec.ipa.go.jp/1_13download/syllabus_sg_ver3_2.pdf
[6] http://www.mi.u-tokyo.ac.jp/consortium/model_ouyoukiso.html
[7] https://www.datascientist.or.jp/dskentei/
[8] https://www.mext.go.jp/content/1407073_11_1_2.pdf

３．４ プログラムの達成目標の設定

本事業で策定するプログラムの目標として、受講者がどのレベルに到達できることを目的とするかに関して、サイバーセキュリティにおける４種類の対応（理解、コミュニケーション、評価・分析、判断）について次表のようなレベルの段階が想定される。

表 3　「プラス・セキュリティ」知識の習得に関する到達レベルの想定

	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

表 1にて示した受講者における時間的制約とのバランスを踏まえ、本事業では以下の目標設定を置くこととし、それぞれの達成、又は達成に向けた道筋を明らかにすることとする。

- 理解：自らの役割に必要な知識の全体像を把握、その一部を理解していることを自覚
- コミュニケーション：専門家との意見交換ができる
- 評価・分析：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
- 判断：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

４．「プラス・セキュリティ」知識補充プログラム案

前章までの検討結果をもとに、「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」と「デジタル経営を推進する企業経営層」の２種類の受講者を対象に、それぞれの役割を担うために必要となる「プラス・セキュリティ」知識を習得するための教育プログラムの構成案を示す。

４．１ 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向けカリキュラム

４．１．１ カリキュラムの設計意図

受講者である部課長級は、4.2 で扱う企業経営層と比較すると相対的に時間を確保しやすいと見込まれるものの、講習受講のためにまとまった時間の確保が難しいと見込まれることから、集合講習を 4.5 時間程度に抑え、これ以外にオンライン・オンデマンドで 6.5～7.5 時間程度の学習を併用することで、サイバーセキュリティ対策に従事する上で必要となる幅広い知識の習得が可能となるように配慮した。

教育内容については、それぞれの詳細に深く踏み込むことは時間的制約で困難であることから、学習した内容を必要に応じて受講者自身で深掘り可能となるよう、学習の入口として必要な知識を正しく理解できるよう、基本的な内容を網羅するように努めている。

４．１．２ カリキュラムの概要

（１）目的

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管理者に求められるサイバーセキュリティに関する役割について、本講座の受講を通じて以下の対応ができるようになる、又はその実現に向け今後取り組むべきことを理解する：

- 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
- 上記に関する社内外とのコミュニケーション

（２）実施方法

集合講習と e-ラーニング（オンライン・オンデマンド形式）の組合せにて実施する。

（３）期間

約 12 時間（集合講習 4.5 時間とオンデマンド（計 7.5 時間、うち必須 6.5 時間）の合計）

（４）受講の前提条件

これまでのキャリアを通じて、組織のマネジメントに関する基本的な知識と経験を有することを前提とする。

デジタル環境やサイバーセキュリティに関する知識については、一般従業員と同様のリテラシーとし、キーワード等は新聞やテレビなどのマスメディアで話題になる内容を認知している程度とする。この前提よりも高度な知識及び実践経験を有する受講者については、オンデマンドの教育の受講について希望に応じて省略することを認める。

（５）教育内容

カリキュラムの構成を次表に示す。なお表中に記載の集合講習開催時刻は例であり、状況に応じた調整を行うことを前提としている。

表 4　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向けカリキュラムの構成

第1単元 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）（60 分）	●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ページに示す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
第2単元 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）（90 分）	●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
第3単元 サイバー空間における脅威と対策 （150 分）	●脅威及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。
第4単元 サイバーセキュリティとリスク対応 （150 分）	●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。
第5単元 サイバーセキュリティ対応における社内外連携 （150 分）	●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。
第6単元 サイバーセキュリティに関する法制度 （60 分）	●サイバーセキュリティ対策で関連する法律、基準、ガイドライン等について、実用上支障が無い程度の理解を得る。

（６）サイバーセキュリティに関する既存フレームワーク等との対応

3.3 に示したフレームワークを用いて、本カリキュラムで扱うべき知識・スキルと、カリキュラ

ムの項目との対応関係を整理する。教材を作成する際には、表中で対応することが示されている項目で扱われる知識・スキルの内容を含めることが期待される。

① NIST SP800-181 で定義されている役割（Work Role）の抽出

当該フレームワークで定義されているサイバーセキュリティに関する役割定義のうち、「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」が担う役割と類似要素を含む次の 6 種類の Work Role を抽出し、これらで求められている知識・スキルカリキュラムの項目との対応関係を整理することとした。

- SP-RSK-001：許可権限者（Authorizing Official/Designating Representative）
- SP-RSK-002：セキュリティ管理策査定者（Security Control Assessor）
- OV-EXL-001：幹部によるサイバーリーダーシップ（Executive Cyber Leadership (EXL)）
- OV-PMA-001：事業計画マネージャー（Program Manager）
- OV-PMA-002：IT プロジェクトマネージャー（Information Technology Project Manager）
- OV-PMA-004：IT ポートフォリオ管理者（IT Investment / Portfolio Manager）

② NIST SP800-181 で定義されている知識・スキル・能力項目との対応関係

後述するカリキュラムによる教育内容と、①で抽出した Work Role で求められる知識・スキル・能力との対応関係を次表に示す。なお①で抽出した項目のうち、受講対象者が習得する必要がないと見込まれる知識・スキルは表より除外している。

表 5　SP800-181 で定義されている関連知識・スキル・能力との対応関係

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
K0010	ネットワークインフラをサポートする通信手法、原理及びコンセプトに関する知識	●						
K0011	ルータ、スイッチ、ブリッジ、サーバ、伝送媒体及び関連ハードウェアを含むネットワーク設備の能力とアプリケーションに関する知識	●						
K0029	組織の LAN/WAN の接続に関する知識	●						
K0100	エンタープライズ IT アーキテクチャに関する知識	●						
K0024	データベースシステムに関する知識	●						
A0119	サイバーセキュリティとその組織的影響に関連する基本的な概念と問題を理解する能力		●					
K0001	コンピュータネットワーキングの概念とプロトコル及びネットワークセキュリティの方法に関する知識		●					
K0006	サイバーセキュリティの喪失による特定の運用上の影響に関する知識		●					
K0007	認証、承認及びアクセス制御手法に関する知識		●					
K0009	アプリケーションの脆弱性に関する知識		●					

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
K0018	暗号化アルゴリズムに関する知識		●					
K0019	暗号と暗号鍵管理の概念に関する知識		●					
K0021	データのバックアップと復元に関する知識		●					
K0027	組織の企業情報セキュリティアーキテクチャに関する知識		●					
K0038	情報やデータの使用、処理、保管、送信に関連するリスクを管理するために使用されるサイバーセキュリティとプライバシーの原則に関する知識		●					
K0044	（機密性、完全性、可用性、認証、否認防止に関連する）サイバーセキュリティとプライバシーの原則と組織の要件に関する知識		●					
K0049	ITセキュリティの原理と手法（例：ファイアウォール、非武装地域、暗号化）に関する知識		●					
K0164	機能性、品質及びセキュリティ上の要求事項とこれらをどのように個別の供給品に適用するか（すなわち要素とプロセス）に関する知識		●					
K0199	セキュリティアーキテクチャの概念とエンタープライズアーキテクチャの参照モデルに関する知識（例：Zachman、Federal Enterprise Architecture [FEA]）		●					
K0200	ネットワークおよび関連標準のためのサービス管理の概念に関する知識（例：ITIL の現行バージョン）		●					
K0295	機密性、完全性、可用性の原則についての知識		●					
K0314	業界の技術における潜在的なサイバーセキュリティ脆弱性に関する知識		●					
K0322	組込システムに関する知識		●					
K0342	ペネトレーションテストの原理、ツール及び技術に関する知識		●					
K0624	アプリケーションセキュリティリスクに関する知識（例：オープンウェブアプリケーションセキュリティプロジェクトにおけるトップ 10 リスト）		●					
S0006	機密性、完全性及び可用性の原則の適用に関するスキル		●					
S0034	情報システムとネットワークの保護の必要性（例： セキュリティ管理策）の識別に関するスキル		●					
K0037	セキュリティアセスメントと認証プロセスに関する知識		●					
K0005	サイバー環境の脅威と脆弱性に関する知識			●				
A0091	インテリジェンスのギャップを特定する能力			●				
K0013	サイバー防衛と脆弱性評価ツール及びその能力に関する知識			●				
K0054	標準に基づいた概念と機能を活用した IT（情報技術）セキュリティ評価、監視、検出、修復ツールと手順の評価、実装、普及のための現在の産業界における手法に関する知識			●				
K0056	ネットワークアクセス、識別及びアクセス管理（例：PKI、Oauth、OpenID、SAML、SPML）に関する知識			●				
K0059	新興の情報技術とサイバーセキュリティ技術に関する知識			●				
K0070	システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識（例：バッファオーバーフロー、モバイルコード、クロスサイトスクリプティング、PL/SQL 及びインジェクション、競合状態、隠れチャネル、リプレイ、リターン指向型攻撃、悪質なコード）			●				
K0106	ネットワーク攻撃及びネットワーク攻撃に関する脅威と脆弱性の関連性を構成するものに関する知識			●				

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
K0147	新たに出現したセキュリティ問題、リスク及び脆弱性に関する知識			●				
K0165	リスク／脅威の評価に関する知識			●	●			
K0170	システムセキュリティを考慮することなく設計された情報通信技術を備えた重要なインフラストラクチャシステムに関する知識			●				
K0287	組織の情報分類プログラムと情報漏洩の流れに関する知識			●				
K0296	ハブ、ルータ、スイッチ、ブリッジ、サーバ、伝送媒体及び関連ハードウェアを含むネットワーク機器の能力、アプリケーション及び潜在的な脆弱性に関する知識			●				
S0001	セキュリティシステムにおける脆弱性スキャンの実施と脆弱性の認識に関するスキル			●				
S0358	テクノロジーインフラの進化を意識し続けるスキル			●				
K0165	リスク／脅威の評価に関する知識			●	●			
A0028	組織の目標を達成するために人材に関する要件を評価し、予測する能力				●			
A0039	ライフサイクルコスト見積りの開発と更新を監督する能力				●			
A0045	サプライヤーおよび/または製品の信頼性を評価/保証する能力				●			
A0056	取得プロセスを通じてセキュリティプラクティスが確実に実施されるようにする能力				●			
A0083	信頼性、妥当性、関連性に関する情報を評価する能力				●			
A0116	サイバーセキュリティリソースの優先順位付けと割り当てを正確かつ効率的に行う能力				●			
A0117	組織のダイナミクスの中で戦略、ビジネス、テクノロジーを関連付ける能力				●			
A0123	組織の要件（機密性、完全性、可用性、認証、否認防止に関連するもの）にサイバーセキュリティとプライバシーの原則を適用する能力				●			
A0129	情報セキュリティ管理プロセスを戦略的および運用的な計画プロセスと統合できるようにする能力				●			
A0130	組織内の上級職員が、その管理下にある業務と資産をサポートする情報やシステムに関する情報セキュリティを確実に提供できるようにする能力				●			
K0002	リスク管理プロセスの知識（例:リスクの評価と緩和のための方法）				●			
K0026	業務継続性と運用計画の災害復旧継続性に関する知識				●			
K0040	脆弱性情報の発信源（例：アラート、アドバイザリ、正誤表、報告書）に関する知識				●			
K0048	リスクマネジメントフレームワークの要件に関する知識				●			
K0101	組織のエンタープライズ IT のゴールと目的に関する知識				●			
K0198	組織のプロセス改善の概念とプロセス成熟度モデルに関する知識（例：開発のための能力成熟度モデル統合（CMMI）、サービスのための CMMI 及び取得のための CMMI）				●			
K0126	サプライチェーンリスク管理プラクティスに関する知識（NIST SP 800-161）				●			
K0154	サプライチェーンリスクマネジメントの標準、プロセス及びプラクティスに関する知識				●			

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
K0169	情報技術（IT）サプライチェーンのセキュリティとサプライチェーンのリスク管理ポリシー、要件及び手続きに関する知識				●			
K0194	クラウドベースのナレッジマネジメント技術とセキュリティ、ガバナンス、調達及び管理に関連する概念に関する知識				●			
K0257	情報技術（IT）の取得/調達要件に関する知識				●			
K0622	データの使用、処理、保存及び送信に関連する管理策に関する知識				●			
S0147	サイバーセキュリティの原則と教義に基づいたセキュリティ管理策を評価するスキル（例：CIS CSC、NIST SP 800-53、サイバーセキュリティフレームワークなど）				●			
A0069	協働的なスキルと戦略を適用する能力					●		
A0077	他の組織の機能やサポート活動とサイバーセキュリティ業務とを調整する能力					●		
A0090	共通のサイバーセキュリティ運用による利益を有する外部パートナーを特定する能力					●		
A0094	組織のサイバー目標に関連する法律、規則、方針、指針を解釈し適用する能力						●	
K0267	重要なインフラストラクチャのサイバーセキュリティに関連する法律、ポリシー、手続きまたはガバナンスに関する知識						●	
A0033	組織のサイバー活動を支援するための法律、規則、方針、標準に準拠したポリシー、計画、戦略を策定する能力						●	
K0003	サイバーセキュリティとプライバシーに関する法律、規制、政策及び倫理に関する知識						●	
K0004	サイバーセキュリティとプライバシーの原則に関する知識						●	
K0148	サプライチェーンリスクの軽減のための輸出入管理規制と責任機関に関する知識						●	
K0168	適用法令、制定法（例：米国法典のタイトル10,18,32,50）、大統領令、行政機関のガイドライン、行政/刑事法のガイドラインおよび手続きに関する知識						●	
K0196	暗号及びその他のセキュリティ技術に関連する輸入/輸出規制に関する知識						●	
K0260	個人識別情報（PII）データセキュリティ基準に関する知識						●	
A0011	質問に明確かつ簡潔に答える能力							●
A0012	明確な質問をする能力							●
A0013	口頭、書面及び/または視覚的な手段を通じて、確信的かつ組織的な方法で複雑な情報、概念又はアイデアを伝える能力							●
A0014	記述を通じて効果的にコミュニケーションする能力							●
A0016	小グループでの議論を促進する能力							●
A0018	ブリーフィングを準備し、発表する能力							●
A0070	批判的な読みこみと思考のスキルを適用する能力							●
A0085	ポリシーが明確に定義されていない場合に判断を行う能力							●
A0096	複雑で急速に進化する概念を解釈し理解する能力							●
A0101	分析に影響する可能性のある認知バイアスを認識し緩和する能力							●
A0105	技術および計画に関する情報を顧客の理解度に合わせる能力							●

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
A0106	批判的に考える能力							●
A0108	目的と効果を理解する能力							●
A0118	組織のプロセスや課題解決に関連する技術、管理、リーダーシップの問題を理解する能力							●
K0008	顧客組織の適用可能なビジネスプロセスと運用に関する知識							●
K0028	組織の評価と検証に関する要件に関する知識							●
K0072	リソースマネジメントの原理と技法に関する知識							●
K0146	組織のコアビジネスとミッションの原理に関する知識							●
K0235	研究開発センター、シンクタンク、学術研究機関、産業システムを活用する方法に関する知識							●
K0270	取得/調達におけるライフサイクルプロセスに関する知識							●
S0038	システムのパフォーマンス目標を達成するための、手段や指標の特定と、パフォーマンスを向上または改善するためのアクションの特定に関するスキル							●
S0111	顧客との対話に関するスキル							●
S0175	根本原因の分析を行うスキル							●
S0176	機能的かつ具体的な支援計画の準備、連絡文書の作成と管理、人員派遣手続きを含む管理計画活動に関するスキル							●
S0244	クライアントのニーズ/要件の決定、クライアントの期待の管理、品質に関する結果の提供に対する意思表示などを含む、クライアントとの関係を管理するスキル							●
S0249	ブリーフィングの準備と発表に関するスキル							●
S0273	計画のレビューと編集に関するスキル							●
S0356	ボードメンバーを含むすべてのレベルの管理者とのコミュニケーションを行うスキル（例：対人関係スキル、アプローチ力、効果的なリスニングスキル、視聴者のためのスタイルと言語の適切な使用など）							●
S0359	批判的思考を使用して組織のパターンや関係を分析するスキル							●

③ 2020 年度調査で定義されているカリキュラム内容との対応関係

後述するカリキュラムによる教育内容と、2020 年度調査結果「『プラス・セキュリティ』知識の補充のためのモデルカリキュラム」の内容との対応関係を次表に示す。

表 6　2020 年度調査結果のカリキュラム内容との対応関係

●＝当該単元で扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
第1単元：サイバー空間を理解するための基礎知識	(1) 人類とIT（光ケーブルから5G、量子コンピューティングまで）	●	●					
	(2) サイバー空間と社会（国家、政治、企業、テクノロジー、国民）			●				
	(3) コンピュータ理論	●	●					
	(4) インターネットの基本原理（ウェブ、電子メール、e単元ース、クラウド）	●	●					
	(5) サイバーセキュリティの要素技術（暗号と電子署名、認証、アクセス制御）		●					
第2単元：サイバー空間における脅威と対策	(1) 脅威の関係主体（利用者過失、犯罪組織等）			●				
	(2) 不正・悪用の歴史・トレンドと考え方、犯罪心理			●				
	(3) 脅威と対策に関する情報収集の考え方と方法論・基本動作			●				
	(4) 脅威のトレンド（サイバーセキュリティに関わる過去の主要な事故やトラブル）			●				
	(5) 脆弱性と対策（脆弱性の原理と対策方法、性能や利便性とのトレードオフ）			●				
第3単元：サイバーセ キュリティに関連する法令・規格・諸制度	(1) 法令・規格・諸制度対応の考え方と方法論・基本動作						●	
	(2) 関連法令（不正アクセス禁止法、不正競争防止法、個人情報保護法、EU 一般データ保護規則（GDPR）等）						●	
	(3) 規格・標準・ガイドライン（ISO 31000、ISO/IEC 27000 シリーズ、SP800.171 等）						●	
	(4) その他（クラウドサービスにおける約款、サイバーセキュリティ保険、インターネットの関係機関）					●	●	
第4単元：サイバーセ キュリティに関連するリスクマネジメントの方法	(1) リスクマネジメントの基本的考え方と方法論・基本動作				●			
	(2) サイバーセキュリティリスクに関連するリスクの評価方法				●			
	(3) (2)で評価したリスクについての低減、回避、保有、移転の方法				●			
	(4) 体制構築（組織内での連絡・共有体制の整備・維持、外部専門家の活用等）				●	●		
	(5) インシデント対応プロセス（異常検知、サービス停止の判断、復旧、メディア対応等）				●	●		
第5単元：企業価値向上とサイバーセキュリティ	(1) 企業価値とサイバーセキュリティの基本的考え方と方法論・基本動作				●			
	(2) 企業価値への影響を考慮した費用対効果分析に基づくサイバーセキュリティ投資の考え方				●			
	(3) セキュリティ品質とブランド戦略・顧客との信頼醸成				●			
	(4) セキュリティ対策の証明と情報発信				●	●		

④ IT リテラシースタンダードとの対応関係

後述するカリキュラムによる教育内容と、2022 年 3 月時点で最新の IT リテラシースタンダードを構成するフレームワーク及びモデルカリキュラムにおける関連項目との対応関係を次表に示す。

表 7　IT リテラシースタンダードとの対応関係

●＝当該単元で扱うことを示す			教育内容						受講者があらかじめ習得していることを想定
			第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
フレームワーク	C.リスク対応 C1. 規律・方針	セキュリティ関連法規(サイバーセキュリティ基本法、不正アクセス禁止法など)、不正競争防止法（営業秘密）、情報セキュリティポリシ						●	
		コンプライアンス、コーポレートガバナンスなど、企業の規範の考え方				●		●	●
		個人情報保護の必要性、関連する法律、個人情報保護方針（プライバシポリシ）						●	
	C.リスク対応 C2. 脅威	情報セキュリティの概念の理解、代表的な情報資産の種類とこれらに対応する人的・技術的・物理的脅威と脆弱性		●	●				
		情報技術等を悪用するなどの代表的な攻撃手法の種類とこれらへの対策の概要			●				
		利用により生じる人為的ミス(ヒューマンエラー)に起因する脅威と対策の想定			●				
	C.リスク対応 C3. 対策	情報セキュリティに関する人的・技術的・物理的セキュリティ対策の基本的な考え方		●					
		リスクマネジメントの流れと情報セキュリティマネジメントシステム(ISMS)の考え方		●		●			
		IoTシステムの情報セキュリティを維持するための各種の指針・ガイドラインが推奨している事項			●				
モデルカリキュラム	第10回 リスク対応(1)～規程・方針と脅威と脅威～	企業規範と取組み				●		●	●
		個人情報保護法						●	
		不正競争防止法（営業秘密）						●	
		セキュリティ関連法規						●	
		情報モラルとセキュリティ	●						●
		情報セキュリティ(概念、情報資産の種類、脅威の種類、脆弱性、攻撃手法の種類と特徴)		●	●				
	第11回 リスク対応(2) ～対策～	情報セキュリティ管理(リスクマネジメントの流れ、ISMS、情報セキュリティ組織・機関・制度)				●			
		情報セキュリティ対策（人的、技術的、物理的対策の例）			●				
		情報セキュリティ実装技術（暗号技術の仕組みと強度などの特徴、認証の必要性と認証技術の概要、利用者認証の技術の種類・特徴、生体認証技術の種類・特徴、PKI）			●				
		IoTシステムのセキュリティ（対策、セキュリティガイドライン、コンシューマ向けIoTセキュリティガイド）			●				
	第12回 リスク対応(3) ～最近の脅威の動向～	標的型攻撃による被害			●				
		ランサムウェアによる被害			●				
		ビジネスメール詐欺による被害			●				
		Webサービスからの個人情報の窃取			●				
		IoT機器の脆弱性の顕在化			●				

⑤ IT パスポート試験シラバスとの対応関係

後述するカリキュラムによる教育内容と、2022 年 3 月時点で最新の IT パスポート試験シラバスにおける関連項目との対応関係を次表に示す。

表 8　IT パスポート試験シラバスとの対応関係

●＝当該単元で扱うことを示す △＝必要に応じて当該単元で扱うことを示す ★＝当該キーワードのみを扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
1. 経営・組織論	(2) 経営管理	★ テレワーク						
20. ソリューションビジネス	(2) ソリューションの形態	★ クラウド						
40. プロセッサ	(1) コンピュータの構成	●	●					
	(2) プロセッサの基本的な仕組み		△					
41. メモリ	(1) メモリの種類と特徴		△					
	(2) 記録媒体の種類と特徴		△					
	(3) 記憶階層		△					
42. 入出力デバイス	(1) 入出力インタフェース		△					
	(2) IoT デバイス		△					
	(3) デバイスドライバ		△					
43. システムの個性	(1) 処理形態		△					
	(2) システム構成		△					
	(3) 利用形態		△					
44. システムの評価指標	(1) システムの性能		△					
	(2) システムの信頼性		△					
	(3) システムの経済性		△					
45. オペレーティングシステム	(1) OS の必要性	●						
	(2) OS の機能		●					
	(3) OS の種類		●					
46. ファイルシステム	(1) ファイル管理		●					
	(2) バックアップ		●					
47. オフィスツール	(1) ソフトウェアパッケージ	●						
	(2) 文書作成ソフト	●						
	(3) 表計算ソフト	●						
	(4) プレゼンテーションソフト	△						
	(5) Web ブラウザ	●						
48. オープンソースソフトウェア	(1) オープンソースソフトウェア		●					
49. ハードウェア（コンピュータ・入出力装置）	(1) コンピュータ	●	●					
	(2) 入出力装置	△	●					
54. データベース	(1) データベース	●						
	(2) データベース管理システム	△						
58. ネットワーク方式	(1) ネットワークの構成	●						
	(2) ネットワークの構成要素		●					
	(3) IoT ネットワークの構成要素	●	●					
59. 通信プロトコル	(1) 代表的なネットワークアーキテクチャ		●					
	(2) 通信プロトコル		●					
	(1) インターネットの仕組み	●						

●＝当該単元で扱うことを示す △＝必要に応じて当該単元で扱うことを示す ★＝当該キーワードのみを扱うことを示す		教育内容						受講者があらかじめ習得していることを想定
		第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
60. ネットワーク応用	(2) インターネットサービス		●					
	(3) 通信サービス	●	●					
5. セキュリティ関連法規	(1) サイバーセキュリティ基本法						●	
	(2) 不正アクセス行為の禁止等に関する法律						●	
	(3) 個人情報保護法（個人情報の保護に関する法律）						●	
	(4) パーソナルデータの保護に関する国際的な動向						●	
	(5) その他の情報セキュリティ関連法規						●	
	(6) 各種の基準・ガイドライン						●	
61. 情報セキュリティ	(1) 情報セキュリティの概念	●	●					
	(2) 情報資産	●	●					
	(3) 脅威と脆弱性		●	●				
	① 人的脅威の種類と特徴			●				
	② 技術的脅威の種類と特徴			●				
	③ 物理的脅威の種類と特徴			●				
	④ 脆弱性	●	●	●				
	⑤ 不正のメカニズム			●				
	(4) 攻撃手法			●				
62. 情報セキュリティ管理	(1) リスクマネジメント				●			
	(2) 情報セキュリティ管理				●	●		
	(3) 個人情報保護				●			
	(4) 情報セキュリティ組織・機関				●	●		
63. 情報セキュリティ対策・情報セキュリティ実装技術	(1) 情報セキュリティ対策の種類			●				
	① 人的セキュリティ対策			●				
	② 技術的セキュリティ対策	●	●	●				
	③ 物理的セキュリティ対策			●				
	(2) 暗号技術	●	●					
	(3) 認証技術		●					
	(4) 利用者認証	●	●					
	(5) 生体認証（バイオメトリクス認証）		●					
	(6) 公開鍵基盤		●					

⑥ 情報セキュリティマネジメント試験シラバスとの対応関係

後述するカリキュラムによる教育内容と、2022 年 3 月時点で最新の情報セキュリティマネジメント試験シラバスにおける関連項目との対応関係を次表に示す。

表 9　情報セキュリティマネジメント試験シラバスとの対応関係

●＝当該単元で扱うことを示す			教育内容						受講者があらかじめ習得していることを想定
			第1単元：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）	第2単元：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）	第3単元：サイバー空間における脅威と対策	第4単元：サイバーセキュリティと企業価値	第5単元：サイバーセキュリティに関わるコミュニケーション	第6単元：サイバーセキュリティに関する法制度	
重点分野	技術要素/セキュリティ	情報セキュリティ		●	●				
		情報セキュリティ管理		●	●	●	●		
		セキュリティ技術評価			●				
		情報セキュリティ対策			●				
		セキュリティ実装技術			●				
	企業と法務/法務	知的財産権						●	
		セキュリティ関連法規						●	
		労働関連・取引関連法規						●	
		その他の法律・ガイドライン・技術者倫理						●	
		標準化関連						●	
その他の分野	コンピュータシステム/システム構成要素	システムの構成	●	●					
		システムの評価指標		●					
	技術要素/ネットワーク	ネットワーク方式	●						
		データ通信と制御		●					
		通信プロトコル		●					
		ネットワーク管理		●					
		ネットワーク応用		●					
要求される技能	Ⅰ 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること	1 情報資産管理の計画		●	●	●			
		2 情報セキュリティリスクアセスメント及びリスク対応			●	●			
		3 情報資産に関する情報セキュリティ要求事項の提示				●			
		4 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示				●			
	Ⅱ 情報セキュリティマネジメントの運用・継続的改善に関すること	5 情報資産の管理				●			
		6 部門の情報システム利用時の情報セキュリティの確保			●	●			
		7 業務の外部委託における情報セキュリティの確保			●	●			
		8 情報セキュリティインシデントの管理			●	●	●		
		9 情報セキュリティの意識向上		●	●	●			
		10 コンプライアンスの運用				●			
		11 情報セキュリティマネジメントの継続的改善				●			
		12 情報セキュリティに関する動向・事例情報の収集と評価				●	●		

４．１．３ カリキュラムの内容詳細

４．１．３．１ 第１単元：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）

（１）概要

10 分程度の動画（DX に取り組んでいる部署における、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する対話）を視聴いただいた上で、４種類のオンデマンド講座の受講要否（初級から受講するか、中級からか）を受講者にて判断してもらう。なお、動画の作成を必須とするものではなく、(3)の示す方法から状況に適したものを選ぶことで差し支えない。

① 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 4.1.3.2 の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。

② 到達レベル

デジタルシステムとインターネット及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。

③ 実施方式

オンライン・オンデマンド（受講者の都合のよい時間・場所でオンライン受講）を想定するが、他の方式を選択することも可能とする（以下、オンライン・オンデマンド形式を想定する項目について同様)。

④ 所要時間

1 時間（省略可能）

（２）教育内容

① イントロダクション動画

ア）概要

10 分程度の動画形式で、ある企業において DX に取り組んでいる部署における、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する部長と部下との対話（4 シーン程度）を視聴する。

イ）所要時間

15 分（動画視聴 10 分、受講選択判断 5 分）

ウ）動画コンテンツの条件

教材となる動画は次の各要件を満たすものとする。

- 学習対象となるキーワード（次項で示すもの）を会話又は扱う話題の中に含むこと
- 企業における会話としてのリアリティを有すること
- 簡単に解決可能なものでなく、ある程度高度な検討や判断を必要とするものであること

エ）キーワード

以下のキーワード及び概念を動画中の会話に含めることとする。それぞれのキーワードは後述の４種類のシーンと次のような対応関係を有する。

- デジタルサービスに関するキーワード（OS、Web ブラウザ、IP アドレス、IoT、データベース、テレワーク等）
- セキュリティ対策に関するキーワード（アクセス制御、アップデート、IT 資産管理、脆弱性等）
- デジタルサービスの管理と責任に関するキーワード（ISP、クラウド事業者、OS ベンダー、セキュリティサービスベンダー、クラウドの約款）

これらのキーワードは、次項に示す４種類のシーンと次のような対応関係を有する。シーンの作成にあたっては、実施する教育プログラムの位置付けや受講者の属性に応じてシナリオの構成を変更することは差し支えなく、その際には下表を参考にキーワードがいずれかのシナリオで話題となるように配慮することが望ましい。

表 10　キーワードと動画シーンとの対応関係

キーワード		IT パスポート試験シラバスの対応項目	対応関係（●＝対応）			
			シーン 1	シーン 2	シーン 3	シーン4
デジタルサービスに関するキーワード	OS	45. オペレーティングシステム(1)		●		
	Web ブラウザ	47. オフィスツール(5)	●			
	IP アドレス	60. ネットワーク応用(1)	●			
	IoT	58. ネットワーク方式(3)		●		
	データベース	54. データベース(1)		●		
	テレワーク	1. 経営・組織論(1)			●	
セキュリティ対策に関するキーワード	アクセス制御	63. 情報セキュリティ対策・情報セキュリティ実装技術(1)②			●	
	アップデート			●		
	IT 資産管理	61. 情報セキュリティ(2)		●		
	脆弱性	61. 情報セキュリティ(3)④		●		
デジタルサービスの管理と責任に関するキーワード	ISP	60. ネットワーク応用(3)	●			
	クラウド事業者	20. ソリューションビジネス(2)	●			●
	OS ベンダー	－				●
	セキュリティベンダー	－				●

	クラウドの約款	－				●

オ）動画の詳細

東南アジアに製造拠点の現地法人をもつ中堅製造業 A 社は、この度社内システムを全面的にクラウドに移行することを決定し、最初に業務基幹システム（ERP）と社内共有ファイルサーバを都内データセンターでのオンプレミスから外資大手クラウドへの移行を予定している。移行にあたって、ある部署の部長と部下の間で必要な社内インフラやルールの変更について以下 4 つのシーンの会話がなされている

a）シーン１：オフィスのネットワーク環境はどうなっているのか？

社内共有ファイルサーバをクラウドに移行してから、ユーザーから「ファイルサーバ上のファイルを開くまでに時間がかかるようになった」という声が出ている。クラウド移行により通信回線のひっ迫が予想されるため、事前に契約帯域を増強したと聞いていたが、なぜこのような遅延が発生するのだろうか。

b）シーン２：スマートフォンと IT 資産管理

クラウド上のファイルサーバは、全社員に貸与しているスマートフォンから専用のアプリを介して利用することができる。ただし、会社貸与スマホの脆弱性に起因する情報漏洩等の被害発生を防止するため、専用アプリはスマートフォンの OS（Android をイメージ）が最新のバージョンになってないと利用できない設定を実施することにした。B 社ではこれまで会社貸与スマホの OS バージョンの管理を行っていなかったが、これを機に情報システム部の提供する IT 資産管理データベースで管理することにした。その結果、脆弱性の残る古いバージョンの OS を利用し続けている社員が多数存在し、リスクが放置されたままの状態であったことがわかった。

c）シーン３：テレワークを安全に行うには？

業務基幹システムのクラウド移行が完了を目前に控え、クラウド上の ERP にアクセスできる PC をどのように限定するかを決定する必要があるが、「会社貸与 PC によるオフィス内からのアクセスに限定すべき」という意見と「セキュリティ対策の実施を条件に、自宅用の PC や会社貸与 PC によるオフィス外からのアクセスも認めるべき」という意見が対立している。クラウドを採用した以上オフィス外からのアクセスも認めたいが、どのようなセキュリティ対策を講じる必要があるだろうか？

d) シーン４：クラウドのトラブルなら業務停止でも仕方がない？

無事にERPをクラウド基盤に移行してしばらく経った､月次決算数値の入力〆切当日、突然全社員が基幹システムにアクセスできなくなってしまった。IT 部門の説明によると、ERP を稼働させているクラウド（IaaS）に、アジア地域全体で大規模な障害が起きているようだ。他社でもシステム利用ができず混乱が生じているようで、テレビ等でも報道されている。現状自社で対応できることはなく、ベンダーに問い合わせても「復旧作業中」という回答に終始している。こういったトラブルはクラウド環境を利用する以上は避けられないが、決算時期に ERP が利用できず、自社には打ち手もないというリスクは小さくないものだ。

カ）受講の要否の判断基準

受講者はオ）の動画を視聴した上で､②～④の教材で扱う分野についての自らの理解度と、人に説明できるかどうかの２軸をもとに次の要領で区分（セルフチェックに基づく選択）することとする。

i）当該分野について理解しており、関連する内容について人に説明できる

受講は任意（受講省略を前提とするが、受講いただいてもよい）

ii）当該分野について理解しているが、関連する内容についての説明の自信はない

受講を推奨（受講省略も可能）

iii）当該分野について理解しているとはいえない（名前は聞いたことはある場合も含む）

受講は必須

② デジタルインフラ入門

ア）概要

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。

イ）所要時間

10 分（①をもとに既知の内容については省略可能）

ウ）教育内容

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

サイバーセキュリティを理解する上で欠かせない基本的なハードウェアや設備等について、よく聞く用語がそれぞれ何を指しているのかを説明する。本項で扱うキーワードは次

のとおり：

- サーバ・端末（PC、スマートフォン）の種類
- ネットワーク機器（ルータ、スイッチ、ゲートウェイ）

b) OS、ミドルウェア、アプリケーション、クラウド等の用語説明

受講者がソフトウェアの動作をイメージできるようになるために必要となる、コンピュータ内部のアーキテクチャとそこで動くソフトウェア、及びネットワークを介してソフトウェアを利用するクラウドサービスについて、主要な用語の意味を説明する。本項で扱うキーワードは次のとおり：

- OS
- アプリケーション
- クラウドサービスの定義と種類（SaaS、PaaS、IaaS）

c) IT/OT/IoT がそれぞれ意味するもの

サイバーセキュリティを理解するための前提として、前項のハードウェア等をもとに提供されるデジタル環境に関する用語の説明を行う。本項で扱うキーワードは次のとおり：

- OT、制御系システム
- IoT
- 分散システム

③ サイバーセキュリティに関する用語の意味

ア）概要

「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様々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。

イ）所要時間

20 分（①をもとに既知の内容については省略可能）

ウ）教育内容

a) ソフトウェア開発と脆弱性

受講者がソフトウェアの脆弱性について理解するために必要な概念について説明する。

本項で扱うキーワードは次のとおり：

- ソフトウェアとプログラミング
- バグと欠陥、不具合
- 脆弱性とは何か
- マルウェアと関連用語（ランサムウェア、スパイウェア、ワーム等）

b) インターネットの仕組み

インターネットの基本的な諸概念について説明する。本項で扱うキーワードは次のとおり：

- インターネットの構成要素
- IP アドレス、MAC アドレス
- ドメインとメールアドレス、URL
- パケットを用いた通信方法（従来の電話との違い）
- ベストエフォート

c) デジタルのリスクに関する諸概念

デジタルシステムを利用する上でのリスクとその対策について説明する。本項で扱うキーワードは次のとおり：

- 脅威とその種類
- サイバー攻撃
- 標的型攻撃、なりすまし電子メール
- ウイルス感染、ランサムウェア感染
- サービス妨害（DDoS）攻撃
- 踏み台
- フィッシング、インターネット上の詐欺行為
- 誤操作
- 内部不正

④ デジタル環境の管理や責任に関するキーワード

ア）概要

インターネットを通じたサービス等の提供主体と責任に関する用語について説明する。

イ）所要時間

10 分（①をもとに既知の内容については省略可能）

ウ）教育内容

a）デジタルビジネスの提供者に関する用語

デジタル製品やサービスの提供事業者に関して用いられる用語の意味を説明する。本項で扱うキーワードは次のとおり：

- 通信キャリア、ISP
- EC 事業者
- クラウドサービス事業者
- ハードウェアベンダー
- ソフトウェアベンダー、システムインテグレータ
- セキュリティベンダー

b）管理と責任の所在

クラウド等典型的なサービスにおいて、ベンダーが契約として提供する内容とその影響について説明する。本項で扱うキーワードは次のとおり：

- インターネットの管理主体（ドメイン、IP アドレス）
- ISP、クラウドサービス事業者等の役割分担
- クラウドの約款

（３）動画視聴の代替方式

部課長級向け・経営層向けとも、受講者によってデジタル・ネットワーク技術及びサイバーセキュリティに関する知識に差があると見込まれることから、以下のいずれかの方法によって受講の要否を判断することが考えられる。次ページ表に候補案を示す。

表 11　任意学習項目の選定方法

	方法の種類	概要	利点(◯)・欠点(✕)
1	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
2	セルフチェックに基づく受講者判断	「◯◯について説明できる」と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。	◯ 動画に比べると準備コストが少なく済む ✕ 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
3	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
4	(判断支援手段を提供しない)	各項目を受講するかどう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

4．1．3．2 第２単元：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）

（1）概要

３単元目以降の講座を受講する上であらかじめ把握しておくべき、デジタルシステムとサイバーセキュリティに関する主要な概念と用語を理解する。

① 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

② 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３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とする。

③ 実施方式

オンライン・オンデマンドを想定（受講者の都合のよい時間・場所でオンライン受講）

④ 所要時間

1 時間 30 分

（２）教育内容

① デジタルインフラの要点

ア）概要

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。なお、4.1.3.1 の初級教材で扱った内容とは極力重複しないように配慮することとするが、初級教材の受講を省略した受講者であっても理解に支障が無いようにすることを目的とした重複は差し支えないこととする。

イ）所要時間

30 分

ウ）教育内容

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

現在広く活用されているデジタルサービスの提供に用いられている構成要素について説明する。本項で扱うキーワードは次のとおり：

- クラウドサービスの実態
- データセンターとの違い
- クラウドとオンプレミスの違い
- CDN（Contents Delivery Network）等のクラウドを取り巻く諸概念の説明

b) OS、ミドルウェア、アプリケーション、クラウド等の概念説明

受講者がソフトウェアの動作をイメージできるようになるために必要となる、コンピュータ内部のアーキテクチャとそこで動くソフトウェアの階層、及びネットワークを介してソフトウェアを利用するクラウドサービスの仕組みについて説明する。本項で扱うキーワードは次のとおり：

- OS
- ミドルウェア
- アプリケーション
- ソフトウェア開発の形態
- クラウドサービスの種類と代表的なサービス例（SaaS、PaaS、IaaS）

c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み

サイバーセキュリティを理解するための前提として、前項のハードウェア等をもとに提供されるデジタル環境における諸概念を具体例で説明する。本項で扱うキーワードは次のとおり：

- OT
- IoT
- ピアトゥーピア/集中
- 応用例（オンライン会議、ネット金融・暗号資産、SNS・オンラインゲーム・メタバース）

d) デジタルビジネスの主要プレイヤーの役割

プラットフォーマーとのはどのような立場のプレイヤーを指すのか、デジタルビジネスを直接提供したり、その基盤を提供したりする役割や諸概念を説明する。本項で扱うキーワードは次のとおり：

- 通信キャリア、ISP
- EC 事業者
- クラウドサービスベンダー
- ハードウェアベンダー
- ソフトウェアベンダー、システムインテグレータ
- セキュリティベンダー(対策ソフトウェアベンダー、脅威インテリジェンス・監視・分析・監査等サービスベンダー)

② デジタル技術の基盤とリスク

ア）概要

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。

イ）所要時間

30 分

ウ）教育内容

a) ソフトウェア開発と脆弱性

受講者がソフトウェアの脆弱性について理解するための、開発プロセスとその構成要素について説明する。本項で扱うキーワードは次のとおり：

- プログラミング言語
- プロセス
- マクロプログラム
- バグの種類とその影響（停止、誤動作、脆弱性）
- マルウェア

b) デジタルリスクとその対策

デジタルシステムを利用する上でのリスクとその対策について説明する。本項で扱うキーワードは次のとおり：

- システムトラブル（悪意の攻撃者が存在しないインシデント）
- サイバー攻撃
- 典型的な攻撃手法の例
- フトウェア修正の方法（パッチ）
- マルウェア対策製品とサービス
- 脆弱性を減らすための手法（セキュアコーディング等）
- サイバー攻撃の検知・防御の手法（ファイアウォール等）
- 利用者認証,
- 多要素認証
- アクセス制御の概念
- 冗長化
- 暗号化
- VPN
- ゼロトラストモデル

③ デジタル環境のコストと運用責任

ア）概要

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。

イ）所要時間

30 分

ウ）教育内容

a) インターネットを安全に利用するための費用

デジタル基盤を利用するために必要となるコストについて説明する。本項で扱うキーワードは次のとおり：

- 運用コスト負担の必要性（トラブルの発生を前提とする予算措置）
- インターネット回線の利用（有線、無線）
- インターネットサービスの利用（ソフトウェア、クラウド、データストレージ等）
- マルウェア対策
- フィルタリング
- 不正アクセス検知・遮断
- データや通信の保護
- 監視（SOC）サービス
- 原因究明、証拠保全（デジタルフォレンジック）

b) デジタルサービスの約款

クラウド等典型的なサービスにおいて、ベンダーが契約として提供する内容とその影響について説明する。本項で扱うキーワードは次のとおり：

- デジタルサービスの約款（オンプレの場合と異なり、利用するかしないかの選択肢しかないこと等）
- SLA
- セキュリティサービスの保証範囲

c) インシデント時の事業継続

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発生した場合に備えた体制や事業継続の考え方について説明する。本項で扱うキーワードは次のとおり：

- デジタルサービスにおける事業継続の考え方
- 可用性の観点からの冗長性の必要性
- 災害発生に備えた環境整備
- CSIRT の役割と機能
- xSIRT

• システムの停止・切り離し、代替と復旧の考え方

４．１．３．３ 第３単元：サイバー空間における脅威と対策

（１）概要

受講者に最新の内容を含む主要な脅威とその影響について理解してもらうことを目的として、以下の要領で講義と演習を行うこととする。

① 目標

脅威及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。

② 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。

③ 実施方式

オンライン・オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

2 時間 30 分

（２）教育内容

① サイバー攻撃手法と脅威のトレンド

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a）脅威の関係主体

自組織内部を含め、国内外で脅威をもたらす主体について紹介する。本項で扱うキーワードは次のとおり：

- 従業員や委託先の不注意
- 内部犯行
- 金銭目的
- 愉快犯
- 政治的アピール
- 外国政府機関等

b) おもな攻撃手法

脅威がどのような形でもたらされるかについて説明する。本項で扱うキーワードは次のとおり：

- マルウェア（古典的、コンピュータウイルス、ワーム、ランサムウェア）
- 標的型攻撃
- ソーシャルエンジニアリング、オンライン詐欺
- 不正侵入の種類
- 不正取得したパスワードの悪用
- パスワードの推定
- バイオメトリクス情報の悪用
- アクセス権限の不正使用

c) これまでの脅威の変遷

サイバーセキュリティにおける脅威として社会的に話題となったり、影響を与えたりした脅威を概観する。本項で扱うキーワードは次のとおり：

- 古典的な脅威（愉快犯、技術力の誇示等）
- サービス妨害攻撃
- 情報の不正流出を目的とした P2P 型マルウェア
- 情報の不正取得を目的とした標的型攻撃
- 金銭目的の攻撃
- 政治的・アピール目的の攻撃
- 内部不正の変遷

d) 最新の脅威

現在進行で脅威となっている内容とその原因について説明する。本項で扱うキーワードは次のとおり：

- ランサムウェア
- 標的型攻撃（電子メール添付、悪意のサイトへのリンク）
- 検索上位に表示される悪意のサイト
- 内部不正

② 脅威への対策

ア）概要

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単元において自部署の業務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。

イ）所要時間

30分（オンデマンド可）

ウ）教育内容

a）対策の基本的な考え方

脅威による影響を抑制するための方法として、現在多くの企業が用いている考え方を紹介する。本項で扱うキーワードは次のとおり：

- デジタル環境における資産（機器、情報）の常時管理
- 脅威に関する最新情報の収集
- 速やかな脆弱性対応（対応ができない場合の緩和策の実施）

b）対策実施上の留意点

実際には前項の対策が十分に機能しない場合がある。それがどのような場合で、どうすれば防げるのか、管理職として理解し、実践すべき対策のポイントについて説明する。本項で扱うキーワードは次のとおり：

- ウイルス対策ソフト等セキュリティ製品の過信
- パッチ適用と可用性確保とのジレンマ
- 資産管理の形骸化
- グループ企業経由での被害

③ 事例紹介

ア）概要

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。後述の a)～c)は実施可能なものをいずれか選択して実施することを想定する。なお、本項目の講師は、セキュリティ教育の専門家よりも企業でインシデント対応を行った経験者や、インシデント対応演習のインストラクターなどが担当するほうが高い教育効果が得られるものと見込まれる。

イ）所要時間

30 分（集合講習）

ウ）教育内容

a) 実際のサイバー攻撃ケースの紹介

過去に発生したサイバー攻撃事例について、客観的な観点からどのような対応をするのが効果的なのかについてのケーススタディを行う。

a) ゲストスピーカーによる説明

過去に発生したサイバー攻撃事例について、企業の当事者視点でのインシデント経過について説明する。

b) サイバー攻撃のデモンストレーション等

マルウェア感染した場合にどのような状況になるのか等、受講者が実際に実感できるようなデモンストレーションを行う。

④ グループワーク『脅威対応における“悪いお手本”から学ぶ』

ア）概要

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、従業員教育等）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とともに、望ましい対策方法について協議する。

イ）所要時間

60 分（集合講習：グループワーク）

ウ）教育内容

a) 想定ケースシナリオ

脅威の具体例として以下のケースを想定する。なお以下の内容はいずれも例示であり、実際に教育を実施する際に受講者の属性に応じて見直すことも検討すべきである。

i）「インターネットと隔絶」の誤解

「当社の工場設備はインターネットと接続されていないのでパッチ適用不要」で合意されていたが、保守を請け負うベンダーがトラブル対応方法の検索を目的として、スマートフォンのテザリング機能を用いて外部に接続していたのに誰も気づいていなかった。

ii）資産管理台帳の記載漏れ

あるオープンソースアプリケーションの脆弱性が公表された際、自社のソフトウェア管理台帳には当該アプリの記載がなかったため問題なしと報告したが、脆弱性を悪用した被害が発生した。ソフトウェアの棚卸しは年１回しかやっておらず、実態と一致していなかった。

iii）不十分な従業員教育

標的型攻撃対策として、過去のテキストを参考に「攻撃メールは日本語がおかしかったり、外国人の名前だったりする」と教育していたところ、社外関係者の名をかたり、不自然さのない電子メールの添付ファイルを開封してしまった。

b) ディスカッションの内容

本ディスカッションでは対策方法まで踏み込まず、問題の抽出のみとする。

４．１．３．４ 第４単元：サイバーセキュリティとリスク対応

（１）概要

デジタル活用に伴って発生するサイバーセキュリティリスクに対してどのような取組を行うべきか、自部署の取組においてどこまで費用をかけるべきかの判断を行うために理解すべき内容を講義とグループワークの形式で扱う。

① 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。

② 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。

③ 実施方式

オンライン・オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

2 時間 30 分

（２）教育内容

① サイバーセキュリティのリスクマネジメントの特徴

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a) サイバーセキュリティにおけるリスクの特徴

サイバーセキュリティリスクは事業内容に応じて傾向が異なることから、自社の条件をもとにアセスメントを行う必要があり、対応方法も変わってくることを説明する。本項で扱うキーワードは次のとおり：

- リスクマネジメントの PDCA サイクル
- リスクアセスメントの方法（ランサムウェア感染を例にしたケーススタディ）
- 稀なリスクについての定量化の限界と対応の考え方

b) リスクへの対応方法

評価したリスクの低減、回避、保有、移転について、それぞれの利点・欠点を比較し、目的に応じた適用の考え方を理解する。本項で扱うキーワードは次のとおり：

- リスク対応の考え方（低減、回避、保有、移転）
- サイバーセキュリティ保険の概要
- 現状では保有せざるを得ないサイバーセキュリティリスクの種類

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

まず自社で保有すべきサイバーセキュリティ対策に関する機能を洗い出した上で、その機能の実現方法として自社で行うタスクと外部委託するタスクを区分し、自社で行うタスクについての役割分担をもとに適切な体制を構築する流れとなる。本項で扱うキーワードは次のとおり：

- サイバーセキュリティ対策に関する機能の考え方
- NIST サイバーセキュリティフレームワーク
- CRIC CSF による「セキュリティ統括室」の考え方
- ITSS+（セキュリティ領域）の定める分野

② 対策における費用と損失の考え方

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a) サイバーセキュリティインシデントによる損失

サイバーセキュリティインシデントによる損失は、デジタル環境が使えなくなったりデータが消失したりといった直接的な損失のみならず、顧客やサプライチェーン関係者からの信用の失墜など幅広い影響が及ぶことを理解する。

本項で扱うキーワードは次のとおり：

- 顧客やサプライチェーンへの影響
- レピュテーション低下への影響

• 競合環境における影響

b) 発生確率の考え方

サイバーセキュリティリスクを定量化する上で、発生確率をどのようにとるかは難しい課題である。本カリキュラムを実践する上で必要となる知識について学ぶ。

• マルウェア感染や標的型攻撃の被害発生確率
• 誤操作や過失による情報漏えいの発生確率

c) 費用と効果のバランス

サイバーセキュリティ分野は歴史が浅いこともあって、損失額に関する統計データが十分に整備されていないことから、火災保険等と比較すると正確な費用対効果分析にはならないことを踏まえつつ、いくつかのケースを通じて考え方を理解する。本項で扱うキーワードは次のとおり：

• 「投資することのメリット」と「投資しないことにより抱えるリスク/コスト」の比較
• ランサムウェア対策に関する費用対効果分析
• 内部不正対策に関する費用対効果分析

③ リスクマネジメントのケーススタディ

ア）概要

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でグループワークを行う上での事前準備を兼ねる。

イ）所要時間

30 分（集合講習）

ウ）教育内容

受講者に身近なサイバーセキュリティリスクに関するアセスメントと費用対効果分析の方法について、定量化の計算方法を例示するとともに、計算に用いる設定値（発生確率、被害の大きさ等）を変更することでどのような影響があるかの感度解析を行う。

④ グループワーク『自部署リスクとその対応』

ア）概要

受講者 3～4 名で 1 チームを構成し、各参加者は予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。

イ）所要時間

60 分（集合講習：グループワーク）

ウ）教育内容

１クール 12～15 分＋講師の講評で構成する。受講者の業務内容により自部署のリスクを公言できない場合も想定されるため、仮想企業のリスクに置き換えて実施することも考えられる。

４．１．３．５ 第５単元：サイバーセキュリティ対応における社内外連携

（１）概要

サイバーセキュリティリスクマネジメントの実務対応として、組織として予め実施すべき準備、インシデント対応、社内及び社外とのコミュニケーションの在り方等について、オンライン・オンデマンド形式の学習とグループワークの両形式の組合せで学ぶ。

① 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。

② 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、エスカレーション等）について、実用レベルで実施できる。

③ 実施方式

オンライン・オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

2 時間 30 分

（2）教育内容

① インシデント対応プロセスとその準備

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a) インシデントに備える

インシデント対応を成功に導くために事前に備えておくべき取組とその具体的な方法について理解する。本項で扱うキーワードは次のとおり：

- デジタル環境の資産管理
- 脅威情報の収集と共有
- 演習の実施

b) インシデント対応プロセス

JPCERT/CC マテリアルや NCA 資料、NISC「被害対応事例集」等を参考に、サイバーセキュリティインシデントによる悪影響を最小限に抑制するための対応手順について理解する。本項で扱うキーワードは次のとおり：

- 状況に応じた初動対応
- 報告のエスカレーション
- 被害の抑制のための措置、トリアージ
- 被害を再発させないための措置
- 復旧手順

② 通常時の備えとインシデント時の情報の取扱上のポイント

ア）概要

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等について理解する。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a）通常時の備え

インシデント時の対応を有効なものとするために、日常において準備しておくべきことを理解する。本項で扱うキーワードは次のとおり：

- 有用な情報源の把握
- 異常を検知可能とするための、異常なしの状態でのデータの蓄積
- インシデント時の情報共有に関する事前合意

b）インシデント時に提供すべき情報の種類と流れ

インシデント発生時にどのような情報を収集・提供すべきかのポイントを理解する。本項で扱うキーワードは次のとおり：

- SOC で検知される情報（通常と異なるアクセス履歴、認証の失敗等）
- 公的機関（NISC、IPA、JPCERT/CC 等）が発信する情報とその活用
- サプライチェーンでの情報共有

c）不確実性を含む情報の取扱い

インシデント時には正確な実態が把握できているとは限らない。一方で、十分な情報提供がなされないと憶測やデマが生じる恐れがあるため、不確実な状況においても何らかの情報発信を行うことを考慮すべきである。本項で扱うキーワードは次のとおり：

- 不確実性を伴う情報の取扱い
- フェイクニュースやデマを防ぐ方策

③ インシデント対応と情報開示の事例から学ぶ

ア）概要

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。

イ）所要時間

30 分（集合講習）

ウ）教育内容

a）過去のインシデント発生時の情報発信ケーススタディ

過去のサイバーセキュリティインシデントにおいて適切・不適切な対応と評価された例をそれぞれ紹介して、学ぶべきことを理解する。

④ グループワーク『インシデント発生時の社内外連絡』

ア）概要

サイバー攻撃による被害が生じていると思われている状態で、被害を最小化するためには必要に応じて事業の一時中断やネットワーク環境の遮断等も実施しなければならないが、経営層にその判断を仰ぐためには、中断等を行うことの妥当性を示す証拠を確保した上で、適切なエスカレーションを行う必要がある。演習開始時点では状況がほとんど把握できていないという条件のもと、どのような情報収集や照会を行うか、実施していく中で当初の予想と異なる状況が生じた場合はどうするか等、インシデント発生時の的確なコミュニケーションの実践力を養うための演習を行う。

イ）所要時間

60 分（グループ演習）

ウ）教育内容

a）演習の実施要領

1 グループ 3～6 名程度のグループでリーダーを決め、リーダーがメンバーに情報収集の指示を出すとともに、得られた情報をもとに判断した結果を経営層に向けた報告する。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どうかを自己評価し、講師側の評価と対比する。

b）演習の効果を高めるための工夫

リアリティを高めるには、実施した不適切なアクションによって二次被害が発生するケースを含めることも考えられるが、あまり複雑すぎると受講者のモチベーション低下を招

く恐れもあり、受講者のレベルに応じた難易度の設定が望ましい。

４．１．３．６ 第６単元：サイバーセキュリティに関する法制度

（１）概要

サイバーセキュリティ対策を実施する上で関係する法律、基準、ガイドライン等について理解する。

① 目標

サイバーセキュリティ対策で関連する法律、基準、ガイドライン等について、実用上支障が無い程度の理解を得る。

② 到達レベル

デジタル化に関連する取り組みの中で、遵守すべき法律、基準、ガイドライン等を意識することができる。

③ 実施方式

オンライン・オンデマンドを想定（受講者の都合のよい時間・場所でオンライン受講）

④ 所要時間

60 分程度

（２）教育内容

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

ア）概要

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。

イ）所要時間

20 分

ウ）教育内容

a) サイバーセキュリティ対策において留意すべき法令

それぞれの目的と対象について説明。本項で扱うキーワードは次のとおり：

- サイバーセキュリティ基本法
- 刑法におけるサイバーセキュリティ関連条項
- 不正アクセス禁止法
- 個人情報保護法
- マイナンバー法
- 不正競争防止法
- 欧州 GDPR
- データローカライゼーション規制（EU、中国、ロシア等）
- その他外国法

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

a)で示した法令の遵守に関して、弁護士の助言なしに解釈するのは危険であり、企業活動の中で留意すべき事項については、『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用が望ましいことを説明する。本項で扱うキーワードは次のとおり：

- 人事管理、就業規則等における留意事項
- 営業秘密管理に関する留意事項
- 秘密保持契約や守秘義務、競業避止義務に関する留意事項
- モニタリングに関する留意事項
- サプライチェーンと委託先管理に関する留意事項

② サイバーセキュリティに関する基準・規格等

ア）概要

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等について紹介する。

イ）所要時間

20 分

ウ）教育内容

a) サイバーセキュリティに関する基準・規格等

以下に例示する基準・規格等の目的や適用範囲などについて説明する。本項で扱うキーワードは次のとおり：

- ISO/IEC 27000 シリーズ、ISMS

- JIS 15001、プライバシーマーク
- NIST SP800 シリーズ
- CIS Controls
- PCIDSS
- 政府機関等のサイバーセキュリティ対策のための統一基準群
- ISMAP 管理基準
- 情報セキュリティサービス基準

③ サイバーセキュリティに関するガイドライン等

ア）概要

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・フレームワーク等を紹介する。

イ）所要時間

20 分

ウ）教育内容

a）インターネットを安全に利用するための費用

業種や目的に応じたガイドラインやフレームワークとその活用方法について説明する。

本項で扱うキーワードは次のとおり：

- 個人情報の保護に関する法律についてのガイドライン
- 業種・業界別ガイドライン
- サイバーセキュリティ経営ガイドライン
- グループ・ガバナンス・システムに関する実務指針
- デジタルガバナンスコード
- 営業秘密管理指針、秘密情報の保護ハンドブック
- 中小企業の情報セキュリティ対策ガイドライン
- サイバー・フィジカル・セキュリティ対策フレームワーク
- テレワークセキュリティガイドライン

４．２ デジタル経営を推進する企業経営層向けカリキュラム

４．２．１ カリキュラムの設計意図

受講者である経営層一般（CIO に限らず、CEO や CFO なども含む）に共通する制約条件として、受講のための時間確保が困難であることが想定される。これを踏まえ、受講者にとって参加しやすい条件を極力実現するため、物理的な拘束を半日（3 時間程度）に押さえ、不足分はオンライン・オンデマンドで都合のよい時間・場所で学習できるように配慮した。また、一部をオンライン・オンデマンド形式にすることで、すでに教育内容に関する知識や実践経験を有する受講者は当該内容をスキップすることが可能となり、受講者間での知識の差を吸収する効果も期待できる。

教育内容については、短期に多くの内容を詰め込んでも理解や納得に至らないことから、経営層としてサイバーセキュリティ対策に関する判断を行うために必要な知識として、技術的なものよりもリスクマネジメントの観点からどう考えるべきかに重点を置いて、後述する部課長級向けと比較すると絞り込んだ内容としている。

４．２．２ カリキュラムの概要

（１）目的

経営層に求められるサイバーセキュリティ上の役割について、本講座の受講を通じて以下の対応ができるようになる、又はその実現に向け今後取り組むべきことを理解する：

- 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

（２）実施方法

集合講習と e-ラーニング（オンライン・オンデマンド形式）の組合せにて実施する。

（３）期間

約 8 時間（集合講習 1 日（約 3 時間）とオンデマンド（5 時間、うち必須 3 時間）の合計）

（４）受講の前提条件

これまでのキャリアを通じて、財務リスクや防災・防犯などに関するリスクマネジメントに関する基本的な知識を有することを前提とする。

デジタル環境やサイバーセキュリティに関する知識については、一般従業員と同様のリテラシーとし、キーワード等は新聞やテレビなどのマスメディアで話題になる内容を認知している程度

とする。この前提よりも高度な知識及び実践経験を有する受講者については、オンデマンドの教育の受講について希望に応じて省略することを認める。

（５）教育内容

カリキュラムの構成を次表に示す。なお表中に記載の集合講習開催時刻は例であり、状況に応じた調整を行うことを前提としている。

表 12　デジタル経営を推進する企業経営層向けカリキュラムの構成

第1単元 デジタルシステムとサイバーセキュリティの概要（90 分）	●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
第2単元 サイバー空間における脅威と対策（90 分）	●脅威及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。
第3単元 サイバーセキュリティと投資対効果（135 分）	●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等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。
第4単元 サイバーセキュリティと企業価値（135 分）	●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。

４．２．３ カリキュラムの内容詳細

４．２．３．１ 第１単元：デジタルシステムとサイバーセキュリティの概要

（１）概要

10 分程度の動画（経営会議における、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する対話）を視聴いただいた上で、４種類のオンデマンド講座の受講要否を受講者にて判断してもらう。

① 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

② 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。

③ 実施方式

オンライン・オンデマンドを想定（受講者の都合のよい時間・場所でオンライン受講）

④ 所要時間

90 分程度

（２）教育内容

① イントロダクション動画

ア）概要

10 分程度の動画形式で、ある企業の経営会議における、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する経営層と担当者との対話（４シーン程度）を視聴する。

イ）所要時間

15 分（動画視聴 10 分、受講選択判断 5 分）

ウ）動画コンテンツの要件

教材となる動画は次の各要件を満たすものとする。

- 学習対象となるキーワード（次項で示すもの）を会話又は扱う話題の中に含むこと
- 企業における会話としてのリアリティを有すること
- 簡単に解決可能なものでなく、ある程度高度な検討や判断を必要とするものであること

エ）キーワード

以下のキーワード及び概念を動画中の会話に含めることとする。これらのキーワードは、次項に示す４種類のシーンと次のような対応関係を有する。

- クラウドの種類（SaaS/PaaS/IaaS）とオンプレミスとの違い（シーン 1）
- クラウドにおけるデータの保管場所（シーン 2）
- データの暗号化、VPN、ゼロトラストモデル、多要素認証（シーン 2）

- ISP との回線契約（通信容量と速度）（シーン 3）
- クラウドベンダーの SLA、責任分界点（シーン 4）

オ）動画の詳細

ある企業における SaaS 導入にまつわる 4 つのシーンを想定する。なお以下の内容はいずれも例示であり、実際に教育を実施する際に受講者の属性に応じて見直すことも検討すべきである。

a）シーン１：自社の会計アプリをパッケージから SaaS に移行すべきか？

自社の会計アプリはこれまでパッケージソフトをインストールした PC でしか動作せず、会計担当者はテレワークできず出社を余儀なくされていた。パッケージソフトベンダが提供している SaaS に移行すればどこからでも利用できるようになるとのことで、経営会議で移行すべきかどうかを議論することになった。移行に反対する役員は SaaS の月額利用料が高いと言う。推進派の役員は SaaS への移行によってオンプレ環境の運用コストが減るので見合うと説明。CEO から意見を尋ねられ、単なる PC サーバの保守運用（ハードウェア、OS、ミドルウェア、データそれぞれ）に実は結構費用がかかっていたことに驚いた旨を答える。

b）シーン２：SaaS は安全か？

反対派の役員は続いてセキュリティと内部統制の両面で不安であると言っている。クラウドはどこからでもアクセスできるので、悪意のユーザに不正アクセスされ、自社の財務状況を知られたり、データを改ざんされたりするのではないかと。推進派は認証と暗号化により十分な安全性とアクセス制限を確保できるというが、それを信じて良いものか。自社で使っているビデオ会議システムも同じ技術で保護されていると説明され、であれば反対する理由はないと納得する。

c）シーン３：ネットワークの逼迫を改善するには？

SaaS 移行後にテレワーク利用者が増加し、ネットワーク回線が逼迫するようになってきた。CIO がベンダーに相談したところ、現在の VPN からゼロトラストモデルに移行することが望ましいと言われたが、CIO 自身も不安に感じている。その理由として、１つはゼロトラストモデルに移行すると認証を強化する必要があるとのことで、使い勝手が悪くなる恐れがあるのではないかということ。もう１点はファイアウォールと IDS をベースにするこれまでの対策（境界防御モデル）が無意味になってしまうのではないかということ。VPN で利用している回線の容量を上げる手もあるので、役員一同決めかねてしまう。

d) シーン４：SaaS のシステムトラブルの原因はどこにある？

SaaS ベンダーがホスティングしているデータセンターでの機器故障が原因で、月次決算情報入力の締め日に会計アプリが一時使えなくなった。会計アプリベンダーのサービス約款では停止に関する責任を負わないことが明記されており、数時間の停止であれば補償は得られないことがわかった。実はパッケージ製品を使っていた時代に、PC のトラブルで会計アプリが使えないことはしばしばあり、使用不可の間に顧客とのやりとりが発生した場合の業務継続計画は存在していたのだが、SaaS に以降したことで不要になったと思われていた。経営会議で議論の結果、クラウドであってもシステム管理としてやるべきことを洗い出し、必要な体制を確保することに決した。

カ）受講の要否の判断基準

受講者はエ）の動画を視聴した上で、当該分野についての自らの理解度と、判断経験の有無の２軸をもとに次の要領で区分（セルフチェックに基づく選択）することとする。

i）当該分野について理解しており、関連する内容について自分の言葉で対外的にポイントを説明する自信がある

受講は任意（受講省略を前提とするが、受講いただいてもよい）

ii）当該分野について理解しているが、関連する内容について自分の言葉で対外的にポイントを説明する自信はない

受講を推奨（受講省略も可能）

iii）当該分野について理解しているとはいえない（名前は聞いたことはある場合も含む）

受講は必須

② オンデマンド教材：デジタルインフラの基本

ア）概要

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。例として、ここではハードウェアの説明としてサーバや端末とネットワーク機器の紹介を一括で行うこととする。

イ）所要時間

20 分（①をもとに既知の内容については省略可能）

ウ）教育内容

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

サイバーセキュリティを理解する上で欠かせない基本的なハードウェアや設備等について、具体的にどのようなデジタルサービスの提供に用いられているかを通じて説明する。本項で扱うキーワードは次のとおり：

- サーバ・端末の種類
- ネットワーク機器（ルータ、スイッチ）
- クラウドとオンプレミスの違い

b）OS、ミドルウェア、アプリケーション、クラウド等の概念説明

受講者がソフトウェアの動作をイメージできるようになるために必要となる、コンピュータ内部のアーキテクチャとそこで動くソフトウェアの階層、及びネットワークを介してソフトウェアを利用するクラウドサービスの仕組みについて説明する。。本項で扱うキーワードは次のとおり：

- OS
- ミドルウェア
- アプリケーション
- ソフトウェア開発の形態
- クラウドサービスの種類と例示（SaaS、PaaS、IaaS）

c）IT/OT/IoT の違い、クラウド/オンライン会議の仕組み

サイバーセキュリティを理解するための前提として、前項のハードウェア等をもとに提供されるデジタル環境における諸概念を具体例で説明する。本項で扱うキーワードは次のとおり：

- OT
- IoT
- ピアトゥーピア/集中
- 応用例（オンライン会議、ネット金融・暗号資産、SNS・オンラインゲーム・メタバース）

d）デジタルビジネスの主要プレイヤー

プラットフォーマーとのはどのような立場のプレイヤーを指すのか、デジタルビジネスを直接提供したり、その基盤を提供したりする役割や諸概念を説明する。本項で扱うキー

ワードは次のとおり：

- 通信キャリア、ISP
- EC 事業者
- クラウドサービスベンダー
- ハードウェアベンダー
- ソフトウェアベンダー、システムインテグレータ
- セキュリティベンダー(対策ソフトウェアベンダー、脅威インテリジェンス・監視・分析・監査等サービスベンダー)

③ オンデマンド教材：デジタル技術の基盤とリスク

ア）概要

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。

イ）所要時間

35 分（①をもとに既知の内容については省略可能）

ウ）教育内容

a）ソフトウェア開発と脆弱性

受講者がソフトウェアの脆弱性について理解するための、開発プロセスとその構成要素について説明する。本項で扱うキーワードは次のとおり：

- プログラミング言語
- プロセス
- マクロプログラム
- バグの種類とその影響（停止、誤動作、脆弱性）
- マルウェア

b）インターネットの仕組み

インターネットの基本的な諸概念について説明する。本項で扱うキーワードは次のとおり：

- パケットを用いた通信方法（従来の電話との違い）
- TCP/IP と IP アドレス、MAC アドレス

• ベストエフォート

c) デジタルリスクとその対策

デジタルシステムを利用する上でのリスクとその対策について説明する。本項で扱うキーワードは次のとおり：

• システムトラブル（悪意の攻撃者が存在しないインシデント）
• サイバー攻撃
• 典型的な攻撃手法の例
• フトウェア修正の方法（パッチ）
• マルウェア対策製品とサービス
• 脆弱性を減らすための手法（セキュアコーディング等）
• サイバー攻撃の検知・防御の手法（ファイアウォール等）
• 利用者認証,
• 多要素認証
• アクセス制御の概念
• 冗長化
• 暗号化
• VPN
• ゼロトラストモデル

④ オンデマンド教材：デジタル環境のコストと運用責任

ア）概要

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。

イ）所要時間

20 分（①をもとに既知の内容については省略可能）

ウ）教育内容

a) インターネットを安全に利用するための費用

デジタル基盤を利用するために必要となるコストについて説明する。本項で扱うキーワードは次のとおり：

- 運用コスト負担の必要性（トラブルの発生を前提とする予算措置）
- インターネット回線の利用（有線、無線）
- インターネットサービスの利用（ソフトウェア、クラウド、データストレージ等）
- マルウェア対策
- フィルタリング
- 不正アクセス検知・遮断
- データや通信の保護
- 監視（SOC）サービス
- 原因究明、証拠保全（デジタルフォレンジック）

b) デジタルサービスの約款

クラウド等典型的なサービスにおいて、ベンダーが契約として提供する内容とその影響について説明する。本項で扱うキーワードは次のとおり：

- デジタルサービスの約款（オンプレの場合と異なり、利用するかしないかの選択肢しかないこと等）
- SLA
- セキュリティサービスの保証範囲

c) インシデント時の事業継続

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発生した場合に備えた体制や事業継続の考え方について説明する。本項で扱うキーワードは次のとおり：

- デジタルサービスにおける事業継続の考え方
- 可用性の観点からの冗長性の必要性
- 災害発生に備えた環境整備
- CSIRT の役割と機能
- xSIRT
- システムの停止・切り離し、代替と復旧の考え方

４．２．３．２ 第２単元：サイバー空間における脅威と対策

（１）概要

受講者に最新の脅威とその影響について理解してもらうことを目的として、以下の要領で講義と演習を行うこととする。

① 目標

脅威及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。

② 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。

③ 実施方式

オンライン・オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

90 分

（２）教育内容

① サイバー攻撃手法とそのトレンド

ア）概要

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。

イ）所要時間・形式

30 分（オンデマンド可）

ウ）教育内容

a）脅威の関係主体

自組織内部を含め、国内外で脅威をもたらす主体について紹介する。本項で扱うキーワードは次のとおり：

- **従業員や委託先の不注意**
- **内部犯行**
- **金銭目的**
- **愉快犯**
- **政治的アピール**
- **外国政府機関等**

b) おもな攻撃手法

脅威がどのような形でもたらされるかについて説明する。本項で扱うキーワードは次のとおり：

- マルウェア（古典的、コンピュータウイルス、ワーム、ランサムウェア）
- 標的型攻撃
- ソーシャルエンジニアリング、オンライン詐欺
- 不正侵入の種類
- 不正取得したパスワードの悪用
- パスワードの推定
- バイオメトリクス情報の悪用
- アクセス権限の不正使用

c) これまでの脅威の変遷

サイバーセキュリティにおける脅威として社会的に話題となったり、影響を与えたりした脅威を概観する。本項で扱うキーワードは次のとおり：

- 古典的な脅威（愉快犯、技術力の誇示等）
- サービス妨害攻撃
- 情報の不正流出を目的とした P2P 型マルウェア
- 情報の不正取得を目的とした標的型攻撃
- 金銭目的の攻撃
- 政治的・アピール目的の攻撃
- 内部不正の変遷

d) 最新の脅威

現在進行で脅威となっている内容とその原因について説明する。本項で扱うキーワードは次のとおり：

- ランサムウェア
- 標的型攻撃（電子メール添付、悪意のサイトへのリンク）
- 検索上位に表示される悪意のサイト
- 内部不正

② 脅威への対策

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a）対策の基本的な考え方

脅威による影響を抑制するための方法として、現在多くの企業が用いている考え方を紹介する。本項で扱うキーワードは次のとおり：

- デジタル環境における資産（機器、情報）の常時管理
- 脅威に関する最新情報の収集
- 速やかな脆弱性対応（対応ができない場合の緩和策の実施）

b）対策実施上の留意点

実際には前項の対策が十分に機能しない場合がある。それがどのような場合で、どうすれば防げるのか、経営層として理解すべきポイントについて説明する。本項で扱うキーワードは次のとおり：

- 正確な実態報告の上がりにくさ（「異常：有」という報告をすることへの抵抗、形としてやっていることになっているが実態が伴っていない等）
- ウイルス対策ソフト等セキュリティ製品の過信
- パッチ適用と可用性確保とのジレンマ
- 資産管理の形骸化
- グループ企業経由での被害

③ 事例紹介

ア）概要

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。後述の a)～c)は実施可能なものをいずれか選択して実施することを想定する。なお、本項目の講師は、セキュリティ教育の専門家よりも企業でインシデント対応を行った経験者や、インシデント対応演習のインストラクターなどが担当するほうが高い教育効果が得られるものと見込まれる。

イ）所要時間

30 分（集合講習）

ウ）教育内容

a) 実際のサイバー攻撃ケースの紹介

過去に発生したサイバー攻撃事例について、客観的な観点からどのような対応をするのが効果的なのかについてのケーススタディを行う。

b) ゲストスピーカーによる説明

過去に発生したサイバー攻撃事例について、企業の当事者視点でのインシデント経過について説明する。

c) サイバー攻撃のデモンストレーション等

マルウェア感染した場合にどのような状況になるのか等、受講者が実際に実感できるようなデモンストレーションを行う。

４．２．３．３ 第３単元：サイバーセキュリティと投資対効果

（１）概要

デジタル活用が進む中、自社の企業価値を毀損させないためには、サイバーセキュリティ対策としてどのような取組を行うべきか、費用との比較を含めた判断を行うために理解すべき内容を講義とグループワークの形式で扱う。

① 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。

② 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。

③ 実施方式

オンライン・オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

2 時間 15 分

（２）教育内容

① コーポレートリスクとしてのサイバーセキュリティ

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a) 企業価値とリスクマネジメントの基本的な考え方

サイバーセキュリティリスクは事業内容に応じて傾向が異なることから、自社の条件をもとにアセスメントを行う必要があり、対応方法も変わってくることを説明する。本項で扱うキーワードは次のとおり：

- リスクマネジメントの PDCA サイクル

- リスクアセスメントの方法（ランサムウェア感染を例にしたケーススタディ）
- 稀なリスクについての定量化の限界と対応の考え方

b）リスクへの対応方法

評価したリスクの低減、回避、保有、移転について、それぞれの利点・欠点を比較し、目的に応じた適用の考え方を理解する。本項で扱うキーワードは次のとおり：

- リスク対応の考え方（低減、回避、保有、移転）
- サイバーセキュリティ保険の概要
- 現状では保有せざるを得ないサイバーセキュリティリスクの種類

c）関連法制度とコンプライアンス

リスクマネジメントに関連する法制度について説明する。本項で扱うキーワードは次のとおり：

- サイバーセキュリティに関連する法令（不正アクセス禁止法、不正競争防止法、個人情報保護法、EU 一般データ保護規則（GDPR）等）
- 内部統制に関する経営層の責任（会社法等）
- データローカライゼーション規制、クラウドサービスにおけるリージョンとの関係

② 体制構築・人材確保

ア）概要

経済産業省の手引き書や CRIC-CSF、NCA 資料等を参考に、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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

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

まず自社で保有すべきサイバーセキュリティ対策に関する機能を洗い出した上で、その機能の実現方法として自社で行うタスクと外部委託するタスクを区分し、自社で行うタスクについての役割分担をもとに適切な体制を構築する流れとなる。本項で扱うキーワードは次のとおり：

- サイバーセキュリティ対策に関する機能の考え方

• NIST サイバーセキュリティフレームワーク
• CRIC CSF による「セキュリティ統括室」の考え方
• ITSS+（セキュリティ領域）の定める分野

b) 外部委託の考え方

現在のサイバー攻撃高度化のトレンドの中、自社のみでサイバーセキュリティ対策を完結できる企業はほとんどないことを踏まえ、自社に相応しい外部委託の方法をどのように決定すべきかについて説明する。本項で扱うキーワードは次のとおり：

• NCA が提示する外部委託のモデル
• 過大・過小な委託を避けるための、同業他社との情報共有
• 外部委託仕様を作成するときに留意すべきこと

c) サイバーセキュリティ体制の構築

DX が進展する中、事業部門でセキュリティに関して一定の役割を担うことが適切なケースが増えており、特定の部署に丸投げするのは不適切であるなど、最近の事情を踏まえた体制と人材に関する考え方を説明する。本項で扱うキーワードは次のとおり：

• 企画・戦略部門が担うセキュリティ上の役割
• システムの保守・運用部門が担うべきセキュリティ上の役割
• セキュリティ統括機能の位置付け

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

セキュリティ対策のすべてを担える人材を育成することは現実的でなく、社内外の関係者と連携して役割を担う多様な人材の育成が必要であることを説明する。本項で扱うキーワードは次のとおり：

• セキュリティに関する専門知識・スキルの習得方法
• 「プラス・セキュリティ」を担う人材における知識・スキルの習得方法

③ 費用対効果分析手法

ア）概要

理想的なサイバーセキュリティ対策の実現には膨大なリソースと費用がかかり現実的でないことを踏まえつつ、インシデント発生時の損失額のインパクトとの間でどのようにバランスをとるべきか、費用対効果分析の基本的な考え方を理解する。

イ）所要時間

25 分（集合講習）

ウ）教育内容

a) サイバーセキュリティの費用対効果分析の考え方

サイバーセキュリティ分野は歴史が浅いこともあって、損失額に関する統計データが十分に整備されていないことから、火災保険等と比較すると正確な費用対効果分析にはならないことを踏まえつつ、いくつかのケースを通じて考え方を理解する。本項で扱うキーワードは次のとおり：

- 「投資することのメリット」と「投資しないことにより抱えるリスク/コスト」の比較
- ランサムウェア対策に関する費用対効果分析
- 内部不正対策に関する費用対効果分析

b) サイバーセキュリティが企業価値に及ぼす影響

企業価値への影響を定量化するのは、インシデントによる直接的な損失以上に難しいが、市場における競合の激しい業界や、顧客による乗り換えコストの低いサービスを提供している企業にとっては企業経営への重大なダメージとなり得ることを示す。本項で扱うキーワードは次のとおり：

- レピュテーション低下への影響
- 競合環境における影響
- 株主・投資家からの反応

④ グループワーク『各種対策の費用、損失想定、確率値から必要な投資を検討』

ア）概要

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。

イ）所要時間

50 分（集合講習：グループワーク）

ウ）教育内容

a) 想定ケースシナリオ

サイバーセキュリティ投資と脅威に関するシナリオとして、以下のケースを想定する。

なお以下の内容はいずれも例示であり、実際に教育を実施する際に受講者の属性に応じて見直すことも検討すべきである。

i）ランサムウェア対策

他社でサーバ内のデータがすべて暗号化された例を受けて、自社でも対策をしたいが、どこまで費用をかければよいかの見極めがつかない。感染確率を考えると、あまり予算をかけなくてもよいのだろうか？

＜費用例＞

- 隔離可能なバックアップ設備の調達費用（データの規模に応じて受講者が試算）
- 定期的なデータバックアップオペレーションに必要な人件費（受講者が試算）

＜リスクによる損失例＞

- ランサムウェア感染によるデータ喪失のうち、再作成可能なものについての再作成に要するコスト（データの規模に応じて受講者が試算）
- ランサムウェア感染による個人情報等の秘密情報漏えいによるお詫び金等の支払に必要なコスト（データの規模に応じて受講者が試算）
- ランサムウェア感染による自社営業秘密が漏えいすることによる、自社製品の競争力低下による自社事業へのダメージ（講師側で提供するモデルをもとに受講者が試算）
- ランサムウェア感染が公表されることによる、レピュテーション低下を通じた自社事業へのダメージ（講師側で仮定の値を設定）

＜計算に用いる確率値例＞

- ランサムウェア感染の確率（講師側で仮定の値を設定）
- ランサムウェア感染時にデータを公表されてしまう確率（講師側で仮定の値を設定）

ii）内部不正対策

自社では製造技術を特許でなく営業秘密として管理しており、他社への流出には神経を尖らせている。万一流出した場合、当該製品の利益が半減することも予想されるが、そうなると莫大な費用をかけても見合うということなのだろうか？

iii）サプライチェーンからの「もらい事故」

被害額として、サプライチェーン全体で考えるべきなのか、自社のみでよいのか。モデルの考え方が悩ましい。

b）ディスカッションの内容

限られた時間で結果を出すため、費用・損失ともあらかじめプロトタイプ化したものを用意しておき、その組合せで計算できるようにするなどの簡略化が必要と考えられる。

４．２．３．４ 第４単元：サイバーセキュリティと企業価値

（１）概要

自社の企業価値を毀損させないために、対外的な対応及び情報発信においてどのような留意をすべきかについて、講義とグループワークの形式で扱う。

① 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。

② 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。

③ 実施方式

オンデマンド形式と集合講習（講義＋グループワーク）の併用

④ 所要時間

2 時間 15 分

（２）教育内容

① インシデント対応における経営層の役割

ア）概要

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

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a) インシデントに備える

インシデント対応を成功に導くために事前に備えておくべき取組とその具体的な方法について理解する。本項で扱うキーワードは次のとおり：

- デジタル環境の資産管理
- 脅威情報の収集と共有
- 演習の実施

このとき、経営層が関わるべき事項の例としては次のことが想定される。

- 計画された取組が有効に実践できているかの把握
- 業界水準と同等以上の対策が実現できているかの把握
- インシデントのトレンドに対処できているかの把握

b) インシデント対応プロセス

JPCERT/CC マテリアルや NCA 資料、NISC「被害対応事例集」等を参考に、サイバーセキュリティインシデントによる悪影響を最小限に抑制するための対応手順について理解する。本項で扱うキーワードは次のとおり：

- 状況に応じた初動対応
- 報告のエスカレーション
- 被害の抑制のための措置、トリアージ
- 被害を再発させないための措置
- 復旧手順

このとき、経営層が関わるべき事項の例としては次のことが想定される。

- 関係省庁や投資家、重要顧客等、自社に影響の大きなステイクホルダーへの報告及び情報提供に関するプロセスが適切に整備されているかどうかの確認
- インシデント対応のリソースが不足していないことの確認

② 通常時の備えと情報開示の在り方

ア）概要

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。

イ）所要時間

30 分（オンデマンド可）

ウ）教育内容

a）通常時の備え

インシデント時の対応を有効なものとするために、日常において準備しておくべきことを理解する。本項で扱うキーワードは次のとおり：

- 有用な情報源の把握
- 異常を検知可能とするための、異常なしの状態でのデータの蓄積
- インシデント時の情報共有に関する事前合意

b）サイバーセキュリティに関する情報開示の考え方

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客観的に証明し、対外情報発信するための手法について、他社がどのように情報開示しているかの事例等を通じて理解する。本項で扱うキーワードは次のとおり：

- 過剰な開示の危険性
- サイバーセキュリティ分野の認証等の取得
- サイバーセキュリティ分野の宣言、自己表明
- サイバーセキュリティ報告書、ESG レポート等を通じた開示
- 投資家等からの問い合わせへの対応

c）サイバーセキュリティが企業価値に及ぼす影響

顧客や投資家等にとっての価値は何かをもとに、自社の事業戦略においてサイバーセキュリティ対策をどのように位置づけるべきかを理解する。本項で扱うキーワードは次のとおり：

- 自社のデジタル戦略との連動
- 自社の働き方改革との連動
- 顧客のプライバシー保護

③ インシデント対応と情報開示の事例から学ぶ

ア）概要

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。

イ）所要時間

30 分（集合講習）

ウ）教育内容

a）過去のインシデント発生時の情報発信ケーススタディ

過去のサイバーセキュリティインシデントにおいて適切・不適切な対応と評価された例をそれぞれ紹介して、学ぶべきことを理解する。

④ グループワーク『インシデント発生時の模擬記者会見』

ア）概要

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。1 名あたり 10～15 分程度で交代し、全員が経営者役を行えるようにする。

イ）所要時間

50 分（集合講習：グループワーク）

ウ）教育内容

a）インシデント種類に応じた記者質問内容例

受講者が対応するインシデントのシナリオとして、以下のケースを想定する。なお以下の内容はいずれも例示であり、実際に教育を実施する際に受講者の属性に応じて見直すことも検討すべきである。

i）ランサムウェア感染による事業活動停止

- リスクとして想定していたのか？
  - 想定していた場合、どのような対策を講じていたのか？
  - 想定していなかった場合、他社で起きている事故はなぜ自社では起きないという判断に至ったのか？
- 被害規模の把握はできているか？
- データの復元の見通しは立っているのか？
- 再発防止のためにどのような対策を講じるのか？

ii）クラウドサーバの不適切な設定による個人情報の大量漏えい

- 自社で被害に気づいたのはいつか？

- なぜ気づかなかったのか？ 脆弱性診断などはしていなかったのか？
- 個人情報は暗号化して保存しておくべきではないか。
- クラウドの運用・管理をどのような体制で行っていたのか。
- 設定が適切になっていることをチェックする仕組みはあったのか。

４．３ 知識提供に必要な資料

（１）教材作成にあたっての要件

4.1 及び 4.2 に示したカリキュラムを用いた教育を実施するための教材を作成するにあたって、あらかじめ次に示す内容について方針を定めておくことが望ましい。

① 教材で用いる用語の精査

一般に、サイバーセキュリティに関する教材は、デジタル技術やネットワーク技術に関する用語をある程度理解していることを前提に記載されていることが多い。一方で、本事業において対象とする受講者である「デジタル経営を推進する企業の経営層」及び「それら企業において業務、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」に相当する方々は、新聞ほかマスメディア報道を通じてこれらデジタル技術やネットワーク技術に関するキーワードを認知していても、その意味するところを十分に把握しているという前提に立つのは適切でないと見込まれる。

4.1 及び 4.2 においてカリキュラムの最初に設定した単元「デジタルシステムとサイバーセキュリティの概要」は上述の前提のもとでカリキュラム全体の内容を習得するために必要な用語とその意味するところを学習する目的に設定しているものであり、以降の教材を作成する際には、原則としてここで説明した用語の範囲で説明することが望まれる。ただし、説明上欠かすことができないが、内容について理解することが必要ない用語（規格やプロトコルの名商等）についてはこの限りではない。

② グループ演習で扱う内容

日本国内でサイバーセキュリティに関するグループ演習を行う場合、海外の事例と比較して、「受講者が自社の状況を話したがらないので盛り上がりにくい」とされる[9]。したがって、海外で実施されているグループ演習プログラムをそのまま日本で実施しても、十分な効果が得られない可能性がある。本事業で作成したカリキュラムではこのような傾向があることを踏まえ、自社の事例を示す代わりに仮想事例についてのディスカッションを行うこととしており、カリキュラム内容を調整する際にはこうした特徴について留意することが望ましい。

（２）教材作成時に有用な参考資料

本事業で作成したカリキュラムに関する教材作成にあたり、参考資料として有用なものを示す。

① サイバーセキュリティ経営ガイドライン（経済産業省）

企業の経営層がサイバーセキュリティ対策の実践に先立って認識すべきこと及び CISO や戦

[9] 米国のトレーニングサービス事業者の日本法人担当者の意見。

略マネジメント層、実務者層への指示に際して留意すべきことをまとめたガイドラインであり、同省が公表しているコーポレートガバナンスに関するガイドラインにおいて、サイバーセキュリティリスクへの対応については本ガイドラインを参照すべき事がしめされている。

（公表 URL）https://www.meti.go.jp/policy/netsecurity/mng_guide.html

② サイバーリスクハンドブック　取締役向けハンドブック　日本版（一般社団法人日本経済団体連合会（経団連））

米国と英国においてそれぞれ取締役向けに公表されているサイバーセキュリティに関する５つの原則と参考資料について、経団連が民間企業等の協力を得て翻訳・整理したもの。2.2.2(2)に示したカーネギーメロン大学のプログラムは本書の原書の事前参照を推奨している。

（公表 URL）https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

４．４ カリキュラムの実践にあたっての留意事項

本カリキュラムを実際の教育プログラムで実践する場合に、運用上留意すべき点を以下に示す。

（１）受講者が当事者意識を高めることができる事例の選定の重要性

本カリキュラムで扱う内容は、技術的な知識・スキルを扱う要素を含んでいても基本的にはサイバーセキュリティ対策に関するマネジメントをいかに適切に行えるようになるかを目的とするものである。そこで、受講の効果を高めるためには受講者がカリキュラムの内容をいかに「自分事」としてとらえ、自らが担う業務に活かしていくことの重要性への自覚を促す必要がある。そのため、教材で扱う事例などを検討する際には、想定される受講者が「自分には関係ない」と感じることができるだけ少なくなるような配慮を行うことが望ましい。

（２）受講による効果の把握の必要性

本カリキュラムには過去に実施されたプラス・セキュリティに関する教育の実証における受講者及び講師の意見を反映した要素を含むが、それ以外に新たに考案された内容を多く含んでおり、その有効性について検証の必要がある。そこで教育の実証ないし試行にあたっては、受講者から受講を通じて得られた効果についての把握を行うことが望ましい。このとき、次表のような内容について把握することが想定される。回答を得る場合には、多岐選択式と自由回答を組み合わせることで、可能な限り受講者の対応負担を減らしつつ、実効性の高い回答を得るように工夫することが考えられる。

表 13　受講による効果の把握方法

調査方法	調査項目の例
受講終了時のアンケート調査	● 受講を通じて得られた気づきの内容 ● カリキュラムの単元毎の有用性 ● カリキュラムの単元毎の活用可能性 ● カリキュラムの時間配分の適切性 ● 教材や事例の適切性 ● グループワークの運用の適切性
受講から一定期間（2～3 か月）経過後のアンケート調査	● 受講で得た内容の実務での活用状況 ● 実務に照らして今後扱うべき課題

５．まとめ

本報告書では、「(i) デジタル経営を推進する企業の経営層」及び「(ii) それら企業において業務、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」をターゲットとして、「プラス・セキュリティ」知識を補充するプログラムについて、既存の類似の教育プログラムに関する調査結果をもとに、現在の国内における対象者を取り巻く環境や習得すべき知識・スキルに関するニーズを踏まえたカリキュラム案の策定を実施した。

4.4 に示した通り、本報告書において示したカリキュラム案は今後の実証を通じてその有効性を検証する必要がある。それを踏まえて想定される受講者を取り巻く社会のニーズに即した内容に改善していくことが期待される。

別添　フレームワークとの対応

4.1「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向けカリキュラム」の各単元について、4.1.2(6)に示したフレームワークの構成要素との対応関係を示す。

第１単元：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）

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：K0010/ネットワークインフラをサポートする通信手法、原理及びコンセプトに関する知識
- SP800-181：K0011/ルータ、スイッチ、ブリッジ、サーバ、伝送媒体及び関連ハードウェアを含むネットワーク設備の能力とアプリケーションに関する知識
- SP800-181：K0029/組織の LAN/WAN の接続に関する知識
- SP800-181：K0100/エンタープライズ IT アーキテクチャに関する知識
- SP800-181：K0024/データベースシステムに関する知識
- ITLS モデルカリキュラム：情報モラルとセキュリティ
- IT パスポート試験：40. プロセッサ/(1) コンピュータの構成
- IT パスポート試験：45. オペレーティングシステム/(1) OS の必要性
- IT パスポート試験：47. オフィスツール/(1) ソフトウェアパッケージ
- IT パスポート試験：47. オフィスツール/(2) 文書作成ソフト
- IT パスポート試験：47. オフィスツール/(3) 表計算ソフト
- IT パスポート試験：47. オフィスツール/(4) プレゼンテーションソフト
- IT パスポート試験：47. オフィスツール/(5) Web ブラウザ
- IT パスポート試験：49. ハードウェア（コンピュータ・入出力装置）/(1) コンピュータ
- IT パスポート試験：49. ハードウェア（コンピュータ・入出力装置）/(2) 入出力装置※
- IT パスポート試験：54. データベース/(1) データベース
- IT パスポート試験：54. データベース/(2) データベース管理システム
- IT パスポート試験：58. ネットワーク方式/(1) ネットワークの構成
- IT パスポート試験：60. ネットワーク応用/(1) インターネットの仕組み
- IT パスポート試験：61. 情報セキュリティ/(1) 情報セキュリティの概念
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(2) 暗号技術
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(4) 利用者認証
- 情報セキュリティマネジメント試験：コンピュータシステム/システム構成要素/システムの構成

- 情報セキュリティマネジメント試験：技術要素/ネットワーク/ネットワーク方式

第２単元：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）

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：A0119/サイバーセキュリティとその組織的影響に関連する基本的な概念と問題を理解する能力
- SP800-181：K0001/コンピュータネットワーキングの概念とプロトコル及びネットワークセキュリティの方法に関する知識
- SP800-181：K0006/サイバーセキュリティの喪失による特定の運用上の影響に関する知識
- SP800-181：K0007/認証、承認及びアクセス制御手法に関する知識
- SP800-181：K0009/アプリケーションの脆弱性に関する知識
- SP800-181：K0018/暗号化アルゴリズムに関する知識
- SP800-181：K0019/暗号と暗号鍵管理の概念に関する知識
- SP800-181：K0021/データのバックアップと復元に関する知識
- SP800-181：K0027/組織の企業情報セキュリティアーキテクチャに関する知識
- SP800-181：K0038/情報やデータの使用、処理、保管、送信に関連するリスクを管理するために使用されるサイバーセキュリティとプライバシーの原則に関する知識
- SP800-181：K0044/サイバーセキュリティとプライバシーの原則と組織の要件に関する知識
- SP800-181：K0049/IT セキュリティの原理と手法に関する知識
- SP800-181：K0164/機能性、品質及びセキュリティ上の要求事項とこれらをどのように個別の供給品に適用するかに関する知識
- SP800-181：K0199/セキュリティアーキテクチャの概念とエンタープライズアーキテクチャの参照モデルに関する知識
- SP800-181：K0200/ネットワークおよび関連標準のためのサービス管理の概念に関する知識
- SP800-181：K0295/機密性、完全性、可用性の原則についての知識
- SP800-181：K0314/業界の技術における潜在的なサイバーセキュリティ脆弱性に関する知識
- SP800-181：K0322/組込システムに関する知識
- SP800-181：K0342/ペネトレーションテストの原理、ツール及び技術に関する知識
- SP800-181：K0624/アプリケーションセキュリティリスクに関する知識
- SP800-181：S0006/機密性、完全性及び可用性の原則の適用に関するスキル
- SP800-181：S0034/情報システムとネットワークの保護の必要性の識別に関するスキル
- SP800-181：K0037/セキュリティアセスメントと認証プロセスに関する知識
- ITLS フレームワーク：情報セキュリティの概念の理解、代表的な情報資産の種類とこれらに

対応する人的・技術的・物理的脅威と脆弱性

- ITLS フレームワーク：情報セキュリティに関する人的・技術的・物理的セキュリティ対策の基本的な考え方
- ITLS フレームワーク：リスクマネジメントの流れと情報セキュリティマネジメントシステム(ISMS)の考え方
- ITLS モデルカリキュラム：情報セキュリティ（概念、情報資産の種類、脅威の種類、脆弱性、攻撃手法の種類と特徴）
- IT パスポート試験：40. プロセッサ/(1) コンピュータの構成
- IT パスポート試験：40. プロセッサ/(2) プロセッサの基本的な仕組み
- IT パスポート試験：41. メモリ/(1) メモリの種類と特徴
- IT パスポート試験：41. メモリ/(2) 記録媒体の種類と特徴
- IT パスポート試験：41. メモリ/(3) 記憶階層
- IT パスポート試験：42. 入出力デバイス/(1) 入出力インタフェース
- IT パスポート試験：42. 入出力デバイス/(2) IoT デバイス
- IT パスポート試験：42. 入出力デバイス/(3) デバイスドライバ
- IT パスポート試験：43. システムの個性/(1) 処理形態
- IT パスポート試験：43. システムの個性/(2) システム構成
- IT パスポート試験：43. システムの個性/(3) 利用形態
- IT パスポート試験：44. システムの評価指標/(1) システムの性能
- IT パスポート試験：44. システムの評価指標/(2) システムの信頼性
- IT パスポート試験：44. システムの評価指標/(3) システムの経済性
- IT パスポート試験：45. オペレーティングシステム/(2) OS の機能
- IT パスポート試験：45. オペレーティングシステム/(3) OS の種類
- IT パスポート試験：46. ファイルシステム/(1) ファイル管理
- IT パスポート試験：46. ファイルシステム/(2) バックアップ
- IT パスポート試験：48. オープンソースソフトウェア/(1) オープンソースソフトウェア
- IT パスポート試験：49. ハードウェア（コンピュータ・入出力装置）/(1) コンピュータ
- IT パスポート試験：49. ハードウェア（コンピュータ・入出力装置）/(2) 入出力装置
- IT パスポート試験：58. ネットワーク方式/(2) ネットワークの構成要素
- IT パスポート試験：58. ネットワーク方式/(3) IoT ネットワークの構成要素
- IT パスポート試験：59. 通信プロトコル/(1) 代表的なネットワークアーキテクチャ
- IT パスポート試験：59. 通信プロトコル/(2) 通信プロトコル
- IT パスポート試験：60. ネットワーク応用/(2) インターネットサービス

- IT パスポート試験：60. ネットワーク応用/(3) 通信サービス
- IT パスポート試験：61. 情報セキュリティ/(1) 情報セキュリティの概念
- IT パスポート試験：61. 情報セキュリティ/(2) 情報資産
- IT パスポート試験：61. 情報セキュリティ/(3) 脅威と脆弱性
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(2) 暗号技術
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(3) 認証技術
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(4) 利用者認証
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(5) 生体認証（バイオメトリクス認証）
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(6) 公開鍵基盤
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ管理
- 情報セキュリティマネジメント試験：コンピュータシステム/システム構成要素/システムの構成
- 情報セキュリティマネジメント試験：コンピュータシステム/システム構成要素/システムの評価指標
- 情報セキュリティマネジメント試験：技術要素/ネットワーク/データ通信と制御
- 情報セキュリティマネジメント試験：技術要素/ネットワーク/通信プロトコル
- 情報セキュリティマネジメント試験：技術要素/ネットワーク/ネットワーク管理
- 情報セキュリティマネジメント試験：技術要素/ネットワーク/ネットワーク応用
- 情報セキュリティマネジメント試験：要求される技能/1 情報資産管理の計画
- 情報セキュリティマネジメント試験：要求される技能/9 情報セキュリティの意識向上

第３単元：サイバー空間における脅威と対策

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：K0005/サイバー環境の脅威と脆弱性に関する知識
- SP800-181：A0091/インテリジェンスのギャップを特定する能力
- SP800-181：K0013/サイバー防衛と脆弱性評価ツール及びその能力に関する知識
- SP800-181：K0054/標準に基づいた概念と機能を活用した IT セキュリティ評価、監視、検出、修復ツールと手順の評価、実装、普及のための現在の産業界における手法に関する知識
- SP800-181：K0056/ネットワークアクセス、識別及びアクセス管理に関する知識
- SP800-181：K0059/新興の情報技術とサイバーセキュリティ技術に関する知識
- SP800-181：K0070/システムとアプリケーションのセキュリティ上の脅威と脆弱性に関する

知識

- SP800-181：K0106/ネットワーク攻撃及びネットワーク攻撃に関する脅威と脆弱性の関連性を構成するものに関する知識
- SP800-181：K0147/新たに出現したセキュリティ問題、リスク及び脆弱性に関する知識
- SP800-181：K0165/リスク／脅威の評価に関する知識
- SP800-181：K0170/システムセキュリティを考慮することなく設計された情報通信技術を備えた重要なインフラストラクチャシステムに関する知識
- SP800-181：K0287/組織の情報分類プログラムと情報漏洩の流れに関する知識
- SP800-181：K0296/ハブ、ルータ、スイッチ、ブリッジ、サーバ、伝送媒体及び関連ハードウェアを含むネットワーク機器の能力、アプリケーション及び潜在的な脆弱性に関する知識
- SP800-181：S0001/セキュリティシステムにおける脆弱性スキャンの実施と脆弱性の認識に関するスキル
- SP800-181：S0358/テクノロジーインフラの進化を意識し続けるスキル
- SP800-181：K0165/リスク／脅威の評価に関する知識
- ITLS フレームワーク：情報セキュリティの概念の理解、代表的な情報資産の種類とこれらに対応する人的・技術的・物理的脅威と脆弱性
- ITLS フレームワーク：情報技術等を悪用するなどの代表的な攻撃手法の種類とこれらへの対策の概要
- ITLS フレームワーク：利用により生じる人為的ミス(ヒューマンエラー)に起因する脅威と対策の想定
- ITLS フレームワーク：IoT システムの情報セキュリティを維持するための各種の指針・ガイドラインが推奨している事項
- ITLS モデルカリキュラム：情報セキュリティ（概念、情報資産の種類、脅威の種類、脆弱性、攻撃手法の種類と特徴）
- ITLS モデルカリキュラム：情報セキュリティ対策（人的、技術的、物理的対策の例）
- ITLS モデルカリキュラム：情報セキュリティ実装技術（暗号技術、認証の必要性と認証技術、利用者認証技術、生体認証技術、PKI）
- ITLS モデルカリキュラム：IoT システムのセキュリティ（対策、セキュリティガイドライン、コンシューマ向け IoT セキュリティガイド）
- ITLS モデルカリキュラム：標的型攻撃による被害
- ITLS モデルカリキュラム：ランサムウェアによる被害
- ITLS モデルカリキュラム：ビジネスメール詐欺による被害
- ITLS モデルカリキュラム：Web サービスからの個人情報の窃取

- ITLS モデルカリキュラム：IoT 機器の脆弱性の顕在化
- IT パスポート試験：61. 情報セキュリティ/(3) 脅威と脆弱性
- IT パスポート試験：61. 情報セキュリティ/(4) 攻撃手法
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/(1) 情報セキュリティ対策の種類（人的・技術的・物理的）
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/ ① 人的セキュリティ対策
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/ ② 技術的セキュリティ対策
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/ ③ 物理的セキュリティ対策
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ管理
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/セキュリティ技術評価
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ対策
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/セキュリティ実装技術
- 情報セキュリティマネジメント試験：要求される技能/1 情報資産管理の計画
- 情報セキュリティマネジメント試験：要求される技能/2 情報セキュリティリスクアセスメント及びリスク対応
- 情報セキュリティマネジメント試験：要求される技能/6 部門の情報システム利用時の情報セキュリティの確保
- 情報セキュリティマネジメント試験：要求される技能/7 業務の外部委託における情報セキュリティの確保
- 情報セキュリティマネジメント試験：要求される技能/8 情報セキュリティインシデントの管理
- 情報セキュリティマネジメント試験：要求される技能/9 情報セキュリティの意識向上

第４単元：サイバーセキュリティと企業価値

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：K0165/リスク／脅威の評価に関する知識
- SP800-181：A0028/組織の目標を達成するために人材に関する要件を評価し、予測する能力
- SP800-181：A0039/ライフサイクルコスト見積りの開発と更新を監督する能力
- SP800-181：A0045/サプライヤーおよび/または製品の信頼性を評価/保証する能力

- SP800-181：A0056/取得プロセスを通じてセキュリティプラクティスが確実に実施されるようにする能力
- SP800-181：A0083/信頼性、妥当性、関連性に関する情報を評価する能力
- SP800-181：A0116/サイバーセキュリティリソースの優先順位付けと割り当てを正確かつ効率的に行う能力
- SP800-181：A0117/組織のダイナミクスの中で戦略、ビジネス、テクノロジーを関連付ける能力
- SP800-181：A0123/組織の要件（機密性、完全性、可用性、認証、否認防止に関連するもの）にサイバーセキュリティとプライバシーの原則を適用する能力
- SP800-181：A0129/情報セキュリティ管理プロセスを戦略的および運用的な計画プロセスと統合できるようにする能力
- SP800-181：A0130/組織内の上級職員が、その管理下にある業務と資産をサポートする情報やシステムに関する情報セキュリティを確実に提供できるようにする能力
- SP800-181：K0002/リスク管理プロセスの知識
- SP800-181：K0026/業務継続性と運用計画の災害復旧継続性に関する知識
- SP800-181：K0040/脆弱性情報の発信源に関する知識
- SP800-181：K0048/リスクマネジメントフレームワークの要件に関する知識
- SP800-181：K0101/組織のエンタープライズ IT のゴールと目的に関する知識
- SP800-181：K0198/組織のプロセス改善の概念とプロセス成熟度モデルに関する知識
- SP800-181：K0126/サプライチェーンリスク管理プラクティスに関する知識
- SP800-181：K0154/サプライチェーンリスクマネジメントの標準、プロセス及びプラクティスに関する知識
- SP800-181：K0169/情報技術（IT）サプライチェーンのセキュリティとサプライチェーンのリスク管理ポリシー、要件及び手続きに関する知識
- SP800-181：K0194/クラウドベースのナレッジマネジメント技術とセキュリティ、ガバナンス、調達及び管理に関連する概念に関する知識
- SP800-181：K0257/情報技術（IT）の取得/調達要件に関する知識
- SP800-181：K0622/データの使用、処理、保存及び送信に関連する管理策に関する知識
- SP800-181：S0147/サイバーセキュリティの原則と教義に基づいたセキュリティ管理策を評価するスキル
- ITLS フレームワーク：コンプライアンス、コーポレートガバナンスなど、企業の規範の考え方
- ITLS フレームワーク：リスクマネジメントの流れと情報セキュリティマネジメントシステ

ム(ISMS)の考え方

- ITLS モデルカリキュラム：企業規範と取組み
- ITLS モデルカリキュラム：情報セキュリティ管理（リスクマネジメントの流れ、ISMS、情報セキュリティ組織・機関・制度）
- IT パスポート試験：62. 情報セキュリティ管理/(1) リスクマネジメント
- IT パスポート試験：62. 情報セキュリティ管理/(2) 情報セキュリティ管理
- IT パスポート試験：62. 情報セキュリティ管理/(3) 個人情報保護
- IT パスポート試験：62. 情報セキュリティ管理/(4) 情報セキュリティ組織・機関
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ管理
- 情報セキュリティマネジメント試験：要求される技能/1 情報資産管理の計画
- 情報セキュリティマネジメント試験：要求される技能/2 情報セキュリティリスクアセスメント及びリスク対応
- 情報セキュリティマネジメント試験：要求される技能/3 情報資産に関する情報セキュリティ要求事項の提示
- 情報セキュリティマネジメント試験：要求される技能/4 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の提示
- 情報セキュリティマネジメント試験：要求される技能/5 情報資産の管理
- 情報セキュリティマネジメント試験：要求される技能/6 部門の情報システム利用時の情報セキュリティの確保
- 情報セキュリティマネジメント試験：要求される技能/7 業務の外部委託における情報セキュリティの確保
- 情報セキュリティマネジメント試験：要求される技能/8 情報セキュリティインシデントの管理
- 情報セキュリティマネジメント試験：要求される技能/9 情報セキュリティの意識向上
- 情報セキュリティマネジメント試験：要求される技能/10 コンプライアンスの運用
- 情報セキュリティマネジメント試験：要求される技能/11 情報セキュリティマネジメントの継続的改善
- 情報セキュリティマネジメント試験：要求される技能/12 情報セキュリティに関する動向・事例情報の収集と評価

第５単元：サイバーセキュリティに関わるコミュニケーション

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：A0069/協働的なスキルと戦略を適用する能力

- SP800-181：A0077/他の組織の機能やサポート活動とサイバーセキュリティ業務とを調整する能力
- SP800-181：A0090/共通のサイバーセキュリティ運用による利益を有する外部パートナーを特定する能力
- IT パスポート試験：62. 情報セキュリティ管理/(2) 情報セキュリティ管理
- IT パスポート試験：62. 情報セキュリティ管理/(4) 情報セキュリティ組織・機関
- IT パスポート試験：63. 情報セキュリティ対策・情報セキュリティ実装技術/ ① 人的セキュリティ対策
- 情報セキュリティマネジメント試験：技術要素/セキュリティ/情報セキュリティ管理
- 情報セキュリティマネジメント試験：要求される技能/8 情報セキュリティインシデントの管理
- 情報セキュリティマネジメント試験：要求される技能/12 情報セキュリティに関する動向・事例情報の収集と評価

第６単元：サイバーセキュリティに関する法制度

4.1.2(6)で示したフレームワークのうち、本項で扱う内容は次の通りである。

- SP800-181：A0094/組織のサイバー目標に関連する法律、規則、方針、指針を解釈し適用する能力
- SP800-181：K0267/重要なインフラストラクチャのサイバーセキュリティに関連する法律、ポリシー、手続きまたはガバナンスに関する知識
- SP800-181：A0033/組織のサイバー活動を支援するための法律、規則、方針、標準に準拠したポリシー、計画、戦略を策定する能力
- SP800-181：K0003/サイバーセキュリティとプライバシーに関する法律、規制、政策及び倫理に関する知識
- SP800-181：K0004/サイバーセキュリティとプライバシーの原則に関する知識
- SP800-181：K0148/サプライチェーンリスクの軽減のための輸出入管理規制と責任機関に関する知識
- SP800-181：K0168/適用法令、制定法、大統領令、行政機関のガイドライン、行政/刑事法のガイドラインおよび手続きに関する知識
- SP800-181：K0196/暗号及びその他のセキュリティ技術に関連する輸入/輸出規制に関する知識
- SP800-181：K0260/個人識別情報（PII）データセキュリティ基準に関する知識
- ITLS フレームワーク：セキュリティ関連法規、不正競争防止法、情報セキュリティポリシ

- ITLS フレームワーク：コンプライアンス、コーポレートガバナンスなど、企業の規範の考え方
- ITLS フレームワーク：個人情報保護の必要性、関連する法律、個人情報保護方針（プライバシポリシ）
- ITLS モデルカリキュラム：企業規範と取組み
- ITLS モデルカリキュラム：個人情報保護法
- ITLS モデルカリキュラム：不正競争防止法（営業秘密）
- ITLS モデルカリキュラム：セキュリティ関連法規
- IT パスポート試験：5. セキュリティ関連法規/(1) サイバーセキュリティ基本法
- IT パスポート試験：5. セキュリティ関連法規/(2) 不正アクセス行為の禁止等に関する法律
- IT パスポート試験：5. セキュリティ関連法規/(3) 個人情報保護法（個人情報の保護に関する法律）
- IT パスポート試験：5. セキュリティ関連法規/(4) パーソナルデータの保護に関する国際的な動向
- IT パスポート試験：5. セキュリティ関連法規/(5) その他の情報セキュリティ関連法規
- IT パスポート試験：5. セキュリティ関連法規/(6) 各種の基準・ガイドライン
- 情報セキュリティマネジメント試験：企業と法務/法務/知的財産権
- 情報セキュリティマネジメント試験：企業と法務/法務/セキュリティ関連法規
- 情報セキュリティマネジメント試験：企業と法務/法務/労働関連・取引関連法規
- 情報セキュリティマネジメント試験：企業と法務/法務/その他の法律・ガイドライン・技術者倫理
- 情報セキュリティマネジメント試験：企業と法務/法務/標準化関連