プラス・セキュリティ知識補充講座 カリキュラム例

※本資料は、NISCの委託によりみずほリサーチ＆テクノロジーズ株式会社が実施した調査を基に作成したものです。

2022年６月

内閣官房 内閣サイバーセキュリティセンター（NISC）

目次

1. はじめに　本カリキュラム例作成の背景と目的

背景

○今後、経済社会のデジタル化（製品・サービスやプロセスのDX）に伴い、経営層や経営企画部門など、IT・セキュリティの専門部署ではない部署においても、サイバーセキュリティリスクを認識し、自律的に対策を実施することが求められます。

○このため、必ずしも現時点で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様々な人材にも、あらゆる場面で企業内外のセキュリティ専門人材との協働が求められることが想定されます。

⇒2021年9月に閣議決定した「サイバーセキュリティ戦略」において、こうした協働を行うに当たって必要となる知識として、時宜に応じてプラスして習得すべき知識を、「プラス・セキュリティ知識」と整理しました。本戦略に基づき、政府として、プラス・セキュリティ知識を補充できる人材育成プログラムの市場形成・発展に取り組むこととしています。

目的・対象

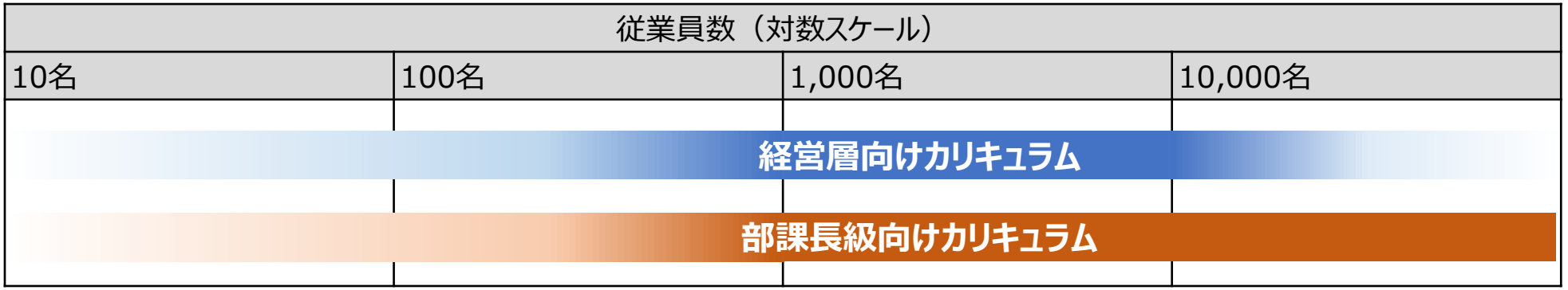
○プラス・セキュリティ知識を補充できる人材育成プログラムは、市場形成が進んでおらず、その受講機会は必ずしも多くありません。

○このため、NISCでは、プラス・セキュリティ知識を補充できる人材育成プログラムの普及に向けて、①経営層及び②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向けに、プログラムが策定される際に参考となるカリキュラムの作成を行いました。（対象となる企業の規模感については次ページ参照）

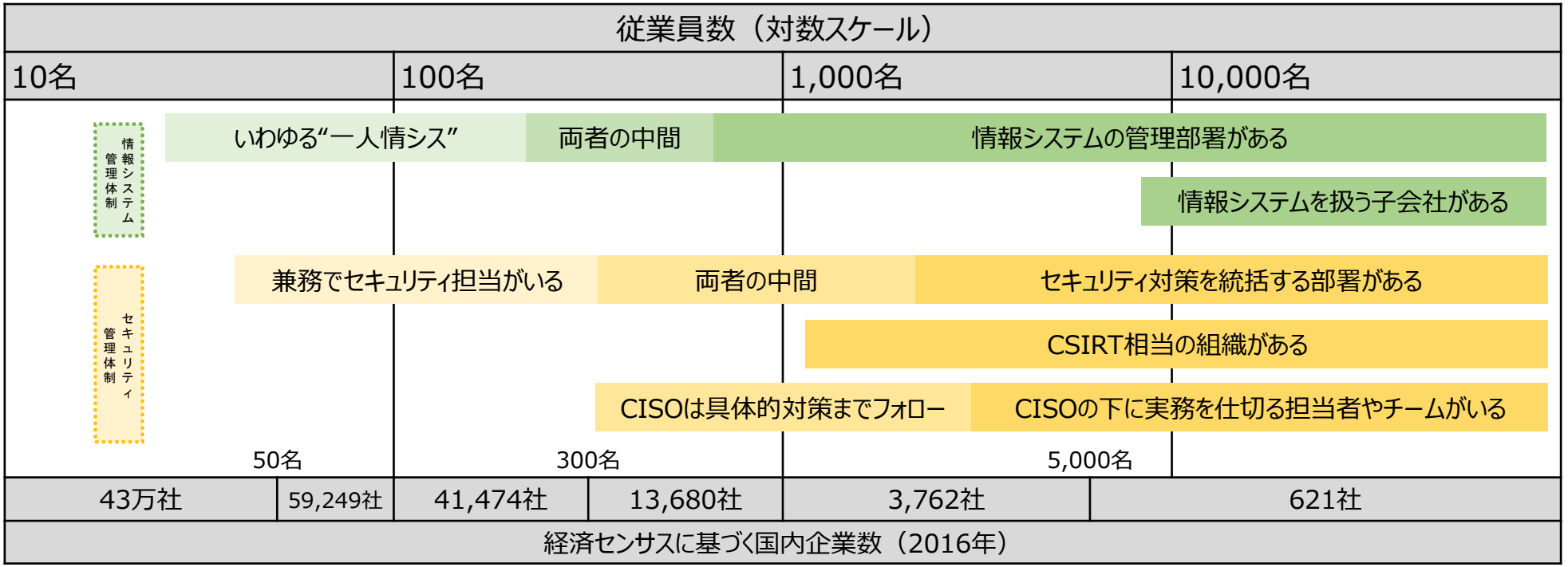
○趣旨に適うカリキュラムの例をお示しするものですが、今後高まる需要に対応して新たにプログラムを提供される教育事業者や、社内研修としてプログラムを策定される事業者の人事やDX担当者など、様々な読者の方の参考になれば幸いです。

1. はじめに

（p.3の参考）受講者の所属組織の主要なターゲット



（参考）



対象別の目標・到達レベル

理想とする目標

①経営層（必ずしもDXを担当している部署の担当役員等ではなく、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。

②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（情シス部門等）・社外（ベンダー等）と、円滑にコミュニケーションできる。

受講後の到達レベル

受講後の到達レベルとしては、必ずしも専門家並の高レベルの知識を身につけることを想定していない。（次ページ参照）

具体的には、以下を想定。

- 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している
- 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

（p.5の参考）到達レベル感

	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

2. カリキュラム例　カリキュラム例の構成

	A. 経営層向け	B. 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。 ● 既存のスキル等フレームワーク（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等）（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等）（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、リスク管理部門等へ説明（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・規格等（20分）◆ ③サイバーセキュリティに関するガイドライン等（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**）→**受講の要否を次ページの方法で判断**

2. カリキュラム例　（補足１）知識レベルの確認方法

■ 経営層向け・部課長級向けともに、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。

	方法の種類	概要	利点（○）・欠点（×）
①	**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
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** （次ページ参照）	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

2. カリキュラム例　（p.8 補足１③の参考）ビデオ･コンテンツの例

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。

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。

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。

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に移行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。

受講の要否の判断基準

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. カリキュラム例　A－1（経営層向け　第１単元）

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）
留意点	● 受講者が受講すべきかどうかの判断方法は本資料8ページ参照。
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、クラウド等の概念説明 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

2. カリキュラム例　A－1（経営層向け　第1単元）

カリキュラム詳細：①デジタルインフラの基本（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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。	● OS ● ミドルウェア ● アプリケーション ● 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。	● 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。	● 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. カリキュラム例　A－1（経営層向け　第１単元）

カリキュラム詳細：②デジタル技術の基盤とリスク（30分）		
項目	**内容**	**本項で扱うキーワード**
a) ソフトウェアと脆弱性	受講者がソフトウェアの脆弱性とはどのようなものかについて理解するための、ソフトウェア開発プロセスとそれに関わる諸概念について説明する。	● プログラミング言語 ● 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	システムを構成する要素の一つとしてのインターネットにおける、サイバーセキュリティ対策を理解するためにあらかじめ把握しておくべき基本的な諸概念について説明する。	● 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 ● スタンドアローン
c) デジタルリスクとその対策に関する技術的概念	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理解するための、認証や暗号化等の主要な技術的概念について説明する。	● 情報セキュリティの概念（機密性、完全性、可用性）とサイバーセキュリティ ● デジタルシステム利用上のリスク ➢ 典型的な攻撃手法（マルウェア、ウェブサイトの改ざん、サービス妨害等） ➢ 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） ● デジタルリスクに対する主な対策方法とそれに係る技術的概念 ➢ ソフトウェア修正の方法（パッチ） ➢ 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（マルウェア対策製品、ファイアウォール等） ➢ 暗号とその応用（暗号化、認証、電子署名、ブロックチェーン、利用者認証、多要素認証等） ➢ アクセス制御の概念 ➢ ゼロトラストモデル

2. カリキュラム例　A－1（経営層向け　第１単元）

カリキュラム詳細：③デジタル環境のコストと運用責任（30分）		
項目	**内容**	**本項で扱うキーワード**
a) インターネットを安全に利用するための費用	サイバーセキュリティ対策に関する適切な投資とは何かを理解するための背景として、インターネットやクラウド等のデジタル基盤を安全に利用するためにどのような費用がかかっているのか、費用のかかり方(投資に係る償却費、オペレーション経費)について説明する。	● 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） ● セキュリティ対策の選択　※個々の対策の詳細な内容については踏み込まない（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インターネットサービスにおいて、ベンダーが契約において提供する内容がおもにサイバーセキュリティリスクにどのような影響を及ぼすのかについて説明する。	● 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。	● デジタルサービスにおける事業継続の考え方 ● ランサムウェア等に備えた、可用性の観点からの冗長性の必要性（データのバックアップ等） ● xSIRTの役割と機能 ● システムの停止・切り離し、代替と復旧の考え方

2. カリキュラム例　A－2（経営層向け　第２単元）

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。
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）

2. カリキュラム例　A－2（経営層向け　第２単元）

カリキュラム詳細：①サイバー攻撃手法とそのトレンド（30分）		
項目	**内容**	**本項で扱うキーワード**
a) おもな攻撃手法	サイバー攻撃等の脅威が企業活動にどのような被害をもたらすかについて説明する。	● 脆弱性によるもの 例）標的型攻撃、不正侵入、不正取得したパスワードの悪用 ● 運用面によるもの 例）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）、ソーシャルエンジニアリング、オンライン詐欺、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
b) 脅威の関係主体と攻撃の動向	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トレンドとして概観する。それを通じて、自組織内部を含め、国内外でデジタル基盤やサイバー空間に脅威をもたらす主体とは何かについて、被害との対応関係とともに紹介する。	● 対象からの搾取等を目的とした攻撃 例）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 ● 上記以外の目的 例）古典的な脅威（愉快犯、技術力の誇示等）、サービス妨害攻撃、政治的・アピール目的の攻撃
c) 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、講習実施時点での最新の状況を交えつつ説明する。	※IPA情報セキュリティ10大脅威（組織編）等を参考に、時宜に応じて修正する ● 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 ● ビジネスメール詐欺

2. カリキュラム例　A－2（経営層向け　第２単元）

カリキュラム詳細：②脅威への対策（30分）		
項目	**内容**	**本項で扱うキーワード**
a) 対策の具体的な運用方法	脅威による企業活動への悪影響を抑制するために、現在多くの企業がどのような考え方のもとで対策を実施しているのか、運用面を中心に紹介する。	● デジタル環境における資産（機器、情報）の常時管理 ● 認証情報（ID、パスワード等）の常時管理 ● アクセス権限の常時管理 ● 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） ● 対策実施の責任主体による分類（組織で行う対策：ルール整備、対策実施体制の整備、監査の実施等、個人で行う対策：電子メール受信時の添付ファイルや社外メールアドレスへの警戒、覗き見防止等）
b) 対策実施上の留意点	実際の脅威に対して、前項で示した考え方に基づく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。	● 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

2. カリキュラム例　A－2（経営層向け　第２単元）

カリキュラム詳細：③事例紹介（30分）		
事例紹介の方法例	**内容**	**紹介例**
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。	● 工場に対するサイバー攻撃のケース ➢ 異常の検知→被害状況の把握→停止の判断→停止の影響 ● 消費者向けサービスにおける情報漏えいのケース ➢ 漏えい情報の通報→流出経路確認→暫定対応→報道発表・被害者へのお詫び→原因究明・再発防止
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。	● 当事者視点でのインシデント経過の説明（以下の内容は説明する事例に応じて柔軟に構成して構わない） ➢ サイバー攻撃を認識したきっかけ ➢ トリアージの実践状況 ➢ 状況が明らかになっていく中で見直したこと ➢ 事前に準備しておいたことで役立ったこと、不足を感じたこと
サイバー攻撃のデモンストレーション	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。	● ランサムウェア感染のデモ ● 標的型攻撃電子メールのデモ ● サービス妨害攻撃のデモ

2. カリキュラム例　A－3（経営層向け　第３単元）

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。
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。 （詳細は本資料21,27ページに記載）

2. カリキュラム例　A－3（経営層向け　第３単元）

カリキュラム詳細：①コーポレートリスクとしてのサイバーセキュリティ（30分）		
項目	**内容**	**本項で扱うキーワード**
a) サイバーセキュリティリスクのアセスメント	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。	● サイバーセキュリティリスクの特徴 例）攻撃者の存在（確率計算の難しさ、手口の変化による対策の陳腐化）、被害情報が共有されづらいことによる実態の掴みづらさ ● 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。	● 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。	● 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）、中国サイバー三法等） ● 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. カリキュラム例　A－3（経営層向け　第３単元）

カリキュラム詳細：②体制構築・人材確保（30分）		
項目	**内容**	**本項で扱うキーワード**
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	まず自社に必要なサイバーセキュリティ対策に関する機能を把握・定義する。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について説明する。	● サイバーセキュリティ対策に関する機能の考え方 例）ITSS+（セキュリティ領域）の定める分野、ISOG-Jセキュリティ対応組織（SOC, CSIRT） の教科書に記載のセキュリティ業務のカテゴリー
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。	● ISOG-Jセキュリティ対応組織（SOC, CSIRT） の教科書に記載のセキュリティ業務の分類 例）必要とされるスキル（セキュリティ専門スキル、社内スキル）、取り扱う情報の範囲（攻撃者（社外）の情報、被害者（社内）の情報）
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。	● 経済産業省「サイバーセキュリティ経営ガイドライン 体制構築の手引き」の記載例 ※その他、NISCポータルサイト掲載「xSIRT構築の事例(PSIRT, DSIRT/SSIRT)」等を参照
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。	● 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 ※デジタル人材育成プラットフォームの活用 ● （今後増加し得る）兼業・副業形態の活用 ※NISCポータルサイト掲載「兼業・副業の事例」等を参照

2. カリキュラム例　A－3（経営層向け　第３単元）

カリキュラム詳細：④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）

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、損失額に関する統計データが十分に整備されていない点や、企業価値に及ぼす影響等の観点で、事例を踏まえて説明する。

受講者3～４名で1テーブルとして、ファシリテーター（各テーブル１名）から提示されるケースについて、サイバーセキュリティリスクのトータルコストを最小にする方法（体制、外部委託、保険等）案をテーブル同士で競い、それぞれの考え方に関する意見交換を行う。

ケース：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）

2. カリキュラム例　Ａ－４（経営層向け　第４単元）

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。 （詳細は本資料26,27ページに記載）

2. カリキュラム例　A－4（経営層向け　第４単元）

カリキュラム詳細：①インシデント対応における経営層の役割（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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 ● インシデント時の情報共有に関する事前合意 **＜経営層が関わるべき事項の例＞** ● 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。	● 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 ● インシデント発生時の適時開示事例や考え方 **＜経営層が関わるべき事項の例＞** ● 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. カリキュラム例　A－4（経営層向け　第４単元）

カリキュラム詳細：②情報開示の在り方（30分）		
項目	**内容**	**本項で扱うキーワード**
a) 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。	● 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 ● 投資家等からの要求への対応 ● 既存の制度開示 例）事業報告、有価証券報告書、コーポレート・ガバナンスに関する報告書、適時開示
b) 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。	● 自社のデジタル戦略との連動 ● 自社の人的資本経営との連動 ● 顧客のプライバシー保護

2. カリキュラム例　A－4（経営層向け　第４単元）

カリキュラム詳細：③インシデント対応と情報開示の事例から学ぶ（30分）

過去のサイバーセキュリティインシデント発生時の情報発信において適切・不適切な対応と評価される点をそれぞれ紹介して、学ぶべきことを理解する。オンデマンド教材を補足する趣旨で行うことを踏まえ、知識の提供よりも「どのように対応すべきなのか」を受講者が主体的に考えるためのヒントの提供に主眼を置いて実施する。

＜インシデント事例に関する情報源の例＞

- サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）
  https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
- マスメディア報道等と当事者によるプレスリリース資料

＜学ぶべきポイントの例＞

- ✓ 顧客等ステークホルダーの懸念や不安に対処するための情報開示はどうあるべきか
- ✓ インシデントの内容（不正アクセス、マルウェア等）や自組織の被害状況に関する情報の不確実性が高い段階において、どのような情報を発信することが適切か
- ✓ 事後の原因究明や再発防止策等の公表を通じた信頼感の維持・回復はどうあるべきか

2. カリキュラム例　A－4（経営層向け　第４単元）

カリキュラム詳細：④演習2：インシデント発生時の模擬記者会見（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。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。

＜リスクによる損失例＞
- ✓ 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？

＜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？

経営層向けロールプレイング演習の例（演習1と演習2を一連のゲーム形式とした場合）

投資・体制構築 ▶ インシデント ▶ CSIRT ▶ 記者会見 ▶ 結果確認

	投資・体制構築	インシデント	CSIRT	記者会見	結果確認
内容	**元手資金100百万円から「セキュリティ機器の導入」と「セキュリティ人材の配置」を実施する**	**「ランサムウェア感染」「情報漏洩」「公式HP改ざん」「サーバ乗っ取り」「なし」等のインシデントカードを用意 プレーヤー毎に1枚引く**	**「発生したインシデントの影響」と「事前に構築した体制による被害防止・低減の効果」、「収集できた情報」、「被害金額」を確認する**	**CSIRTパートで確認できた事実・情報をもって記者会見に臨む 記者会見では5個程度の設問に回答する**	**記者会見での回答内容に応じて株価に影響が生じる 最終的に手元に残った資金と自己資本の合計が最も多いプレーヤーの勝利**
備考	■機器の例 FW IPS/IDS バックアップ ログ保管　など ■人材の例 コマンダー フォレンジック技術者 脆弱性診断士　など	実際にはインシデントが発生しない場合もありうることを考慮し、「インシデント発生なし」を採り入れる 発生インシデントだけでなく、事後対応のフェーズ（人材の確保・調査等）を入れることも有効と考えられる	セキュリティ投資がどのような効果をもたらすか、理解することを目的とする	必要な備えができていないと、社会に対する説明責任を果たせない場合があることを理解することを目的とする	セキュリティ投資と自組織が抱えるセキュリティリスクのバランスが重要であること、およびセキュリティ体制の構築の程度が株価（企業価値）に影響を及ぼす可能性があることを理解することを目的とする

2. カリキュラム例　B－1（部課長級向け　第１－１単元）

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32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。
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。
時間設定・実施方式	１時間（オンデマンド・省略可能）
留意点	● 受講者が受講すべきかどうかの判断方法は本資料8ページ参照。
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、クラウド等の用語説明 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。 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等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

2. カリキュラム例　B－1（部課長級向け　第1－1単元）

カリキュラム詳細：①デジタルインフラ入門（20分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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。	● 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。	● OT、制御系システム ● IoT ● 分散システム

カリキュラム詳細：②サイバーセキュリティに関する用語の意味（20分）		
項目	**内容**	**本項で扱うキーワード**
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とはどのようなものかについて理解するための、ソフトウェア開発プロセスとそれに関わる諸概念について説明する。	● 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	インターネットにおけるサイバーセキュリティ対策を理解するためにあらかじめ把握しておくべき基本的な諸概念について説明する。	● 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） ● スタンドアローン
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理解するための、認証や暗号化等の主要な概念について説明する。	● 情報セキュリティの概念（機密性、完全性、可用性）とサイバーセキュリティ ● 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 ● 暗号とその応用（暗号化、認証、電子署名、ブロックチェーン等）

2. カリキュラム例　B－1（部課長級向け　第1－1単元）

カリキュラム詳細：③デジタル環境の管理や責任に関するキーワード（20分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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。	● 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

2. カリキュラム例　B－1（部課長級向け　第１－２単元）

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とする。
時間設定・実施方式	１時間30分（オンデマンド・必須）
留意点	● 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。
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、クラウド等の概念説明 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

2. カリキュラム例　B－1（部課長級向け　第1－2単元）

カリキュラム詳細：①デジタルインフラの要点（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● クラウドサービスの実態（どのような仕組みを通じてサービスが提供されているのか） ● 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。	● OS ● ミドルウェア ● アプリケーション ● 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。	● 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。	● 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. カリキュラム例　B－1（部課長級向け　第１－２単元）

カリキュラム詳細：②デジタル技術の基盤とリスク（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● プログラミング言語 ● 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に関する技術的概念	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。	● 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） ● 典型的な攻撃手法の例 ● ソ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（知識・所有による認証、生体認証等） ● 多要素認証（ワンタイムパスワード等） ● アクセス制御の概念 ● 暗号化 ● VPN ● ゼロトラストモデル ● 情報セキュリティマネジメントシステム（ISMS）

2. カリキュラム例　B－1（部課長級向け　第1－2単元）

カリキュラム詳細：③デジタル環境のコストと運用責任（30分）		
項目	**内容**	**本項で扱うキーワード**
a) インターネットを安全に利用するための費用	サイバーセキュリティ対策に関する適切な投資とは何かを理解するための背景として、インターネットやクラウド等のデジタル基盤を安全に利用するためにどのような費用がかかっているのか、費用のかかり方(投資に係る償却費、オペレーション経費)について説明する。	● 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） ● セキュリティ対策の選択　※個々の対策の詳細な内容については踏み込まない（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インターネットサービスにおいて、ベンダーが契約において提供する内容がおもにサイバーセキュリティリスクにどのような影響を及ぼすのかについて説明する。	● 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。	● デジタルサービスにおける事業継続の考え方 ● ランサムウェア等に備えた、可用性の観点からの冗長性の必要性（データのバックアップ等） ● 災害発生に備えた環境整備 ● xSIRTの役割と機能 ● システムの停止・切り離し、代替と復旧の考え方

2. カリキュラム例　B－2（部課長級向け　第２単元）

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。
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。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。

2. カリキュラム例　B－2（部課長級向け　第２単元）

カリキュラム詳細：①サイバー攻撃手法と脅威のトレンド（30分）		
項目	**内容**	**本項で扱うキーワード**
a) おもな攻撃手法	サイバー攻撃等の脅威が企業活動にどのような被害をもたらすかについて説明する。	● 脆弱性によるもの 例）標的型攻撃、不正侵入、不正取得したパスワードの悪用 ● 運用面によるもの 例）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）、ソーシャルエンジニアリング、オンライン詐欺、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
b) 脅威の関係主体と攻撃の動向	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トレンドとして概観する。それを通じて、自組織内部を含め、国内外でデジタル基盤やサイバー空間に脅威をもたらす主体とは何かについて、被害との対応関係とともに紹介する。	● 対象からの搾取等を目的とした攻撃 例）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 ● 上記以外の目的 例）古典的な脅威（愉快犯、技術力の誇示等）、サービス妨害攻撃、政治的・アピール目的の攻撃
c) 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、講習実施時点での最新の状況を交えつつ説明する。	※IPA情報セキュリティ10大脅威（組織編）等を参考に、時宜に応じて修正する ● 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 ● ビジネスメール詐欺

2. カリキュラム例　B－2（部課長級向け　第２単元）

カリキュラム詳細：②脅威への対策（30分）		
項目	**内容**	**本項で扱うキーワード**
a) 対策の具体的な運用方法	脅威による企業活動への悪影響を抑制するために、現在多くの企業がどのような考え方のもとで対策を実施しているのか、運用面を中心に紹介する。	● デジタル環境における資産（機器、情報）の常時管理 ● 認証情報（ID、パスワード等）の常時管理 ● アクセス権限の常時管理 ● 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） ● 対策実施の責任主体による分類（組織で行う対策：ルール整備、対策実施体制の整備、監査の実施等、個人で行う対策：電子メール受信時の添付ファイルや社外メールアドレスへの警戒、覗き見防止等）
b) 対策実施上の留意点	実際の脅威に対して、前項で示した考え方に基づく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。	● 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

カリキュラム詳細：③事例紹介（30分）		
事例紹介の方法例	**内容**	**紹介例**
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。	● 工場に対するサイバー攻撃のケース ➢ 異常の検知→被害状況の把握→停止の判断→停止の影響 ● 消費者向けサービスにおける情報漏えいのケース ➢ 漏えい情報の通報→流出経路確認→暫定対応→報道発表・被害者へのお詫び→原因究明・再発防止
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。	● 当事者視点でのインシデント経過の説明（以下の内容は説明する事例に応じて柔軟に構成して構わない） ➢ サイバー攻撃を認識したきっかけ ➢ トリアージの実践状況 ➢ 状況が明らかになっていく中で見直したこと ➢ 事前に準備しておいたことで役立ったこと、不足を感じたこと
サイバー攻撃のデモンストレーション	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。	● ランサムウェア感染のデモ ● 標的型攻撃電子メールのデモ ● サービス妨害攻撃のデモ

2. カリキュラム例　B－2（部課長級向け　第２単元）

カリキュラム詳細：④演習1：脅威と対策における“悪い見本”から学ぶ（60分）		
想定ケース例	**シナリオの内容例**	**ディスカッションの内容**
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。	● 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。
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。	

2. カリキュラム例　B－3（部課長級向け　第３単元）

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、リスク管理部門等へ説明 **（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。 １クール12～15分＋講師の講評で構成。

2. カリキュラム例　B－3（部課長級向け　第３単元）

カリキュラム詳細：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）		
項目	**内容**	**本項で扱うキーワード**
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。	● サイバーセキュリティリスクの特徴 例）攻撃者の存在（確率計算の難しさ、手口の変化による対策の陳腐化）、被害情報が共有されづらいことによる実態の掴みづらさ ● 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。	● 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。	● 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. カリキュラム例　B－3（部課長級向け　第３単元）

カリキュラム詳細：②対策における費用と損失の考え方（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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。	● 「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

2. カリキュラム例　B－3（部課長級向け　第３単元）

カリキュラム詳細：③リスクマネジメントのケーススタディ（30分）

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。オンデマンド教材を補足する趣旨で行うことを踏まえ、知識の提供よりも「どのように考えるのか」を受講者が主体的に考えるためのヒントの提供に主眼を置いて実施する。

＜事業内容に応じたサイバーセキュリティリスクに対する対応体制構築のケース案＞

- ✓ 24/365の運用監視を行っているインフラ事業者の場合
- ✓ 販売済み製品の脆弱性対策をサポートする必要がある製造業事業者の場合
- ✓ 自社内にほとんどデジタル機器をもたず、外部のクラウドサービスを活用して事業を行うスタートアップ事業者の場合
- ✓ フランチャイズ店舗を通じてサービスを提供する飲食業の場合

＜リスク評価の事例＞

- ✓ ハインリッヒの法則に基づく情報漏えいインシデントの発生確率の推計
- ✓ 過去の事例に基づくインシデント種類に応じた被害額の想定
- ✓ 公表された脆弱性への対策実施の遅延がもたらす被害額の想定

カリキュラム詳細：④演習2：自部署リスクとその対応策を洗い出し、リスク管理部門等へ説明（60分）

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２単元の内容をもとに相互に指摘する。それについて、第２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する。

＜他部門への説明が適切に行えているかどうかに関する評価のポイント＞

- ✓ 説明内容が受講者の主観点な判断のみに依存していないか（論旨の客観性）
- ✓ 最新のデータに基づいた検討がなされているか
- ✓ 想定外の展開となった場合の影響が甚大になるようなことはないか

業種	ビジネスモデルに応じたサイバーセキュリティリスクの例	リスク低減策の例（左記リスクに対して有効な対策の例）
製造業	レガシーハードウェアへのマルウェア感染による製造設備の停止がもたらす機会損失	ホワイトリスト型マルウェア対策製品の導入などによる感染機会の回避
飲食業	接客担当がアルバイト中心で流動性が高い→担当者の過失による情報漏えいリスク	担当者が個人情報やセンシティブ情報を扱う機会を極力減らす
金融業	ゼロデイ攻撃により、事業存続に関わる大きな被害が生じる	ゼロデイ攻撃を考慮した多層防御の導入による被害の抑制
（業種不問）	委託先やサプライチェーンの相手先におけるサイバーインシデントに巻き込まれる	相手先の対策レベルが自社と同等程度になるまで底上げを支援する

2. カリキュラム例　B－4（部課長級向け　第４単元）

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、エスカレーション等）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等について理解する。 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等、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どうかを自己評価し、講師側の評価と対比する。

2. カリキュラム例　B－4（部課長級向け　第４単元）

カリキュラム詳細：①インシデント対応プロセスとその準備（30分）		
項目	**内容**	**本項で扱うキーワード**
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。	● 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 ● 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。	● 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. カリキュラム例　B－4（部課長級向け　第４単元）

カリキュラム詳細：②インシデント時の情報の取扱上のポイント（30分）		
項目	**内容**	**本項で扱うキーワード**
a) 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。	● 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
b) 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。	● 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

カリキュラム詳細：③インシデント対応と情報開示の事例から学ぶ（30分）

過去のサイバーセキュリティインシデント発生時の情報発信において適切・不適切な対応と評価される点をそれぞれ紹介して、学ぶべきことを理解する。オンデマンド教材を補足する趣旨で行うことを踏まえ、知識の提供よりも「どのように対応すべきなのか」を受講者が主体的に考えるためのヒントの提供に主眼を置いて実施する。

＜インシデント事例に関する情報源の例＞

- サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）
  https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
- マスメディア報道等と当事者によるプレスリリース資料

＜学ぶべきポイントの例＞

- ✓ 顧客等ステークホルダーの懸念や不安に対処するための情報開示はどうあるべきか
- ✓ インシデントの内容（不正アクセス、マルウェア等）や自組織の被害状況に関する情報の不確実性が高い段階において、どのような情報を発信することが適切か
- ✓ 事後の原因究明や再発防止策等の公表を通じた信頼感の維持・回復はどうあるべきか

カリキュラム詳細：④演習3：インシデント発生時の社内外連絡（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どうかを自己評価し、講師側の評価と対比する。

＜社内連絡の効果を高めるためのポイントの例＞

- インシデント発生時以外でも日頃から情報交換を行うなどの活動を通じて「顔の見える関係」を築き、相手の立場や状況を理解しておく
- 経営層等への報告のフォーマットを予め定めておき、把握できている範囲で効率よく報告をできるようにする
- サイバーセキュリティに関するインシデントの推移（検知から対応、復旧まで）を関係者に予め理解してもらうことで、関係者による協力を得やすくする

＜社外連絡の効果を高めるためのポイントの例＞

- 社外からの問合せ窓口を一元化し、担当者によって回答が異なるような混乱を避ける
- 社外との情報共有を行う担当者と、問合せ窓口担当者を分離し、問合せ対応で情報共有が停滞することを避ける
- 取引先等への影響を最小限とするため、先方にて適切な判断を行うのに必要な情報提供を行う
- 顧客その他関係者の不安を増大させず、かつデマを蔓延させないために必要となる情報の公表を行う

2. カリキュラム例　B－5（部課長級向け　第５単元）

部課長級向け　第５単元	
名称	**５．関係法令** **『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、ガイドライン等について、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。
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・規格等 **（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等について紹介する。 a) サイバーセキュリティに関する基準・規格等
③サイバーセキュリティに関するガイドライン等 **（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・フレームワーク等を紹介する。 a) サイバーセキュリティに関するガイドライン・フレームワーク等

2. カリキュラム例　B－5（部課長級向け　第５単元）

カリキュラム詳細：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）		
項目	**内容**	**本項で扱うキーワード**
a) サイバーセキュリティ対策において留意すべき法令	サイバーセキュリティ対策の実践において留意する必要がある法令等について、それぞれの目的と対象について説明する。	● 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 ● 中国サイバー三法 ● データローカライゼーション規制 ● 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)で示した法令等の遵守に関して、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。	● 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. カリキュラム例　B－5（部課長級向け　第５単元）

カリキュラム詳細：②サイバーセキュリティに関する基準・規格等（20分）		
項目	**内容**	**本項で扱うキーワード**
a) サイバーセキュリティに関する基準・規格等	実務遂行において関係するサイバーセキュリティ関連の各種基準・規格等の目的や適用範囲などについて説明する。	● 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

カリキュラム詳細：③サイバーセキュリティに関するガイドライン等（20分）		
項目	**内容**	**本項で扱うキーワード**
a) サイバーセキュリティに関するガイドライン・フレームワーク等	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。	● 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

教材作成にあたっての留意事項

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、学習者が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が、本カリキュラムを用いる講座の想定受講者は、新聞ほかマスメディア報道を通じてこれらに関するキーワードを認知していても、その意味を十分に把握しているとは限らないため、教材作成の際には、本カリキュラムで用いている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称等）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 。したがって、海外のサイバーセキュリティ研修等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。
- このような傾向を踏まえ、本カリキュラムでは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いる。カリキュラム内容を調整する際にはこうした配慮について留意することが望ましい。

受講者の特徴に応じた工夫

人材育成の効果を高めるため、実践の条件に応じて次のような工夫を行うことが考えられる。

受講者が初対面の場合とお互いに顔見知りの場合の配慮	● 一般にグループワークを実施する場合、円滑な共同作業を実現するために自己紹介的なコミュニケーションの時間を盛り込むことが多いが、業界団体が団体の活動として研修を実施するなどで受講者同士が予め顔見知りの場合は、そのような過程を省いて議論の時間を多くとるなどの工夫が考えられる。
受講者間で知識や経験に相当の格差があると見込まれる場合の配慮	● カリキュラム内容に関連する事前知識や経験を有する受講者は、他の受講者よりも早く理解できる分、手持ち無沙汰になることが予想される。そこで、受講者がそれぞれの余力に応じて追加的に学べる次のようなコンテンツを用意することが考えられる。 ➢ サイバーセキュリティに関する脅威と対策に関するデータ集（トレンドのグラフ等） ➢ 企業における事例集（反面教師的なインシデント事例、優れた取組としてのプラクティス事例等）

3. 参考　受講者の業種に応じた工夫

■ 業種によりサイバーセキュリティ対策の対象となるデジタル環境とその脅威が異なるため、受講者の業種が同一であるような場合はそれらを意識してもらうための工夫を行うことが考えられる。

製造業	● 工場やプラント等、OT環境が運用されるような施設のリスク管理体系が、本社機能等IT環境を主に用いる部門と独立であったり、内容が異なったりすることが、企業としてのリスクマネジメントにどのような影響を及ぼすかについて、受講者の自覚を促す。 ➢ 影響箇所：経営層、部課長級とも第3単元①、第4単元①
金融業	● Fintech、金融DXの進展等により、デジタルガバナンスに関してベンダーとの役割分担が変化しており、デジタル利活用に関するサイバーセキュリティ対策について金融サービスの提供主体としての責任ある対応が求められていることの自覚を促す。 ➢ 影響箇所：経営層：第１単元③、第3単元①② 部課長級：第1-1単元③、第1-2単元③、第3単元①
サービス業	● 他の業種と比較して、提供しているサービスの特徴（サービスの利用者、規模、取り扱う情報、サービスレベルを規定する要素等）毎にサイバー空間における脅威が大きく異なるため、サービス品質とサイバーセキュリティ対策の実効性との両立を図るためにはサービスの特徴を十分に考慮した対策の検討が求められることについて、受講者の自覚を促す。 ➢ 影響箇所：経営層、部課長級とも第2単元①②、第3単元①

3. 参考　既存フレームワーク等との対応について

- プログラムで扱う知識やスキルの内容が、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した。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した。
- 経営層向けカリキュラム例においては、各フレームワーク等の詳細項目との関連付けが難しいため、部課長級向けカリキュラム例のみとした。

フレームワーク等	カリキュラム例との関係
NIST SP800-181	サイバーセキュリティ分野において、国際的に広く使われているフレームワークとの関連付けを確認することで、教育プログラムの質に関する説明性を高めるため、関係付けを行った。
DXリテラシー標準	デジタル人材育成プラットフォーム「マナビDX」に登録されているセキュリティ分野のプログラムを受講することで、プラス・セキュリティ知識習得のワンステップとなることを理解いただくため、関連付けを行った。
ITリテラシースタンダード	ITリテラシースタンダード（ITLS）：将来の成長や競争力強化に向けたビジネスの改善・刷新と効果的なIT活用・投資を進めるための、主に事業部門やスタッフ部門などで勤務するビジネスパーソン（非IT技術者）に求められるIT知識や技能、情報活用能力とその領域を示すものである。IPAで整備されたITリテラシースタンダードを参考に策定された。
ITパスポート試験シラバス	一般的に広く活用されている試験制度との関係性を整理し、知識体系の網羅性を確認するため、ITパスポート試験・情報セキュリティマネジメント試験との関連付けを行った。
情報セキュリティマネジメント試験シラバス	一般的に広く活用されている試験制度との関係性を整理し、知識体系の網羅性を確認するため、情報セキュリティマネジメント試験との関連付けを行った。
2020年度NISC取組	過去のNISCの整理との継続性を確認するため関連付けを行った。

3. 参考　SP800-181との関係性

■ 人材育成施策への活用や国際協調等の観点から、米国NISTが策定する、サイバーセキュリティ人材に係るフレームワークであるSP800-181との関係性を整理した。

■ **SP800-181**：

○米国NIST（国立標準技術研究所）において策定された、サイバーセキュリティに関する業務の性質を共有し、人材育成施策等の開発に活用されることを目的に、個別のタスクの遂行に必要な知識（Knowledge）、スキル（Skill）、能力（Ability）を記述する参照構造。

NISC プラス・セキュリティ知識補充講座 カリキュラム例	SP800-181において各Role※求められる知識・スキル・能力（一部例）
1.基礎知識	[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 [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
2.脅威と対策	[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 [S0358]テクノロジーインフラの進化を意識し続けるスキル
3.投資	[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 [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）
4.ステークホルダーとの関係	[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
5.関係法令	[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

※「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以下のWork Roleに求められる知識・スキル・能力を抽出。

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

3. 参考　DX人材に関するスキル標準との関係性

■ 「デジタル人材育成プラットフォーム」との連携等の観点から、経済産業省にて2022年3月に策定された「DXリテラシー標準」との関係性を整理した（いずれの項目も含む）。

NISC プラス・セキュリティ知識補充講座 カリキュラム例	経済産業省 DXリテラシー標準 セキュリティ関連項目 学習項目例		
	セキュリティの3要素	セキュリティ技術	個人がとるべきセキュリティ対策
1.基礎知識 ○サイバーセキュリティに関する用語の意味 • ソフトウェア開発と脆弱性 • インターネットの仕組み • デジタルのリスクに関する諸概念 ○デジタル技術の基盤とリスク • ソフトウェア開発と脆弱性 • デジタルリスクとその対策	機密性、完全性、可用性	暗号、ブロックチェーン ワンタイムパスワード、生体認証、ISMS	
2.脅威と対策 ○脅威への対策 • 対策の基本的な考え方 • 対策実施上の留意点			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・社外メールアドレスへの警戒

3. 参考　略称について

本カリキュラムで用いる略称は、それぞれ次表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
DX	デジタルトランスフォーメーション
GDPR	General Data Protection Regulation
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
ISOG-J	日本セキュリティオペレーション事業者協議会
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
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

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

①SP800-181で定義されている関連知識(K)・スキル(S)・能力(A)との対応関係

・SP800-181：米国NIST（国立標準技術研究所）において策定された、サイバーセキュリティに関する業務の性質を共有し、人材育成施策等の開発に活用されることを目的に、個別のタスクの遂行に必要な知識（Knowledge）、スキル（Skill）、能力（Ability）を記述する参照構造。

・サイバーセキュリティ分野において、国際的に広く使われているフレームワークとの関連付けを確認することで、教育プログラムの質に関する説明性を高めるため、関係づけを行った。

●＝当該単元で扱うことを示す		部課長級向けカリキュラム例						受講者があらかじめ習得していることを想定
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５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		●					
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			●				

● = 当該単元で扱うことを示す		部課長級向けカリキュラム例						受講者があらかじめ習得していることを想定
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度	
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			●				
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				●			
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				●			

● = 当該単元で扱うことを示す		部課長級向けカリキュラム例						受講者があらかじめ習得していることを想定
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度	
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							●
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							●

● = 当該単元で扱うことを示す		部課長級向けカリキュラム例						受講者があらかじめ習得していることを想定
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度	
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							●

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

②DXリテラシー標準との対応関係

・DXリテラシー標準：働き手一人ひとりがDXに参画し、その成果を仕事や生活で役立てるうえで必要となるマインド・スタンスや知識・スキルを示す、学びの指針とするためのもの。IPAで整備されたITリテラシースタンダードを参考に策定された。

・デジタル人材育成プラットフォーム「マナビDX」に登録されているセキュリティ分野のプログラムを受講することで、プラス・セキュリティ知識習得のワンステップとなることを理解いただくため、関連付けを行った。

●＝当該単元で扱うことを示す			部課長級向けカリキュラム例					
			第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度
経済産業省 DXリテラシー標準 セキュリティ関連項目 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		●				
		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			●			

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

②（参考）ITリテラシースタンダードとの対応関係

・ITリテラシースタンダード（ITLS）：将来の成長や競争力強化に向けたビジネスの改善・刷新と効果的なIT活用・投資を進めるための、主に事業部門やスタッフ部門などで勤務するビジネスパーソン（非IT技術者）に求められるIT知識や技能、情報活用能力とその領域を示すものである。

●＝当該単元で扱うことを示す			部課長級向けカリキュラム例						受講者があらかじめ習得していることを想定
			第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５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			●				

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

③ITパスポート試験シラバスとの対応関係

・ITパスポート：ITを利活用するすべての社会人・これから社会人となる学生が備えておくべきITに関する基礎的な知識が証明できる国家試験。
・一般的に広く活用されている試験制度との関係性を整理し、知識体系の網羅性を確認するため、ITパスポート試験との関連付けを行った。

●＝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		部課長級向けカリキュラム例					
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５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					
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						●
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		●				
	(1) ソフトウェアパッケージ	●					
	(2) 文書作成ソフト	●					

●＝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		部課長級向けカリキュラム例					
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度
47. オフィスツール	(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		●				
60. ネットワーク応用	(1) インターネットの仕組み	●					
	(2) インターネットサービス		●				
	(3) 通信サービス	●	●				
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	●	●				

●＝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		部課長級向けカリキュラム例					
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５単元：サイバーセキュリティに関する法制度
	(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		●				

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

④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

・情報セキュリティマネジメント試験：情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験。
・一般的に広く活用されている試験制度との関係性を整理し、知識体系の網羅性を確認するため、情報セキュリティマネジメント試験との関連付けを行った。

●＝当該単元で扱うことを示す			部課長級向けカリキュラム例					
			第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５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				●	●	

『プラス・セキュリティ知識補充講座 カリキュラム例』付表：既存フレームワークとの対応

⑤以前NISCが整理したカリキュラム内容との対応関係

・2020年に情報セキュリティ大学院大学で戦略マネジメント層向けプログラムを実施するため、基礎項目を中心にNISCで整理を行った。
・過去のNISCの整理との継続性を確認するため関連付けを行った。

●＝当該単元で扱うことを示す		部課長級向けカリキュラム例					
		第１－１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１－２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２単元：サイバー空間における脅威と対策	第３単元：サイバーセキュリティとリスク対応	第４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５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コマース、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				●	●	