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）
概要資料

令和４年　３月

みずほリサーチ&テクノロジーズ株式会社

参考カリキュラムの作成

■ 2021年度は、経営層向け・部課長級向けの参考カリキュラムの策定を実施中。2022年度に試行実施を通じたニーズ調査・改善を実施予定。

	経営層向け		部課長級向け	
目標	● サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 ● 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 ● インシデント発生時の適切な経営判断・指示		● サイバーリスクが自部署に与える影響理解 ● 自部署で実施されている対策の現状理解 ● 上記の経営層への報告	社内外とのコミュニケーション
時間設定	8時間（集合講習3時間＋オンデマンド5時間（うち必須3時間））		12時間（集合講習4.5時間＋オンデマンド7.5時間（うち必須6.5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	90分 任意	①デジタルインフラの基本◆ ②デジタル技術の基盤とリスク◆ ③デジタル環境のコストと運用責任◆	60分 任意	①デジタルインフラ入門◆ ②サイバーセキュリティに関する用語の意味◆ ③デジタル環境の管理や責任に関するキーワード◆
			90分 必須	①デジタルインフラの要点◆ ②デジタル技術の基盤とリスク◆ ③デジタル環境のコストと運用責任◆
2.脅威と対策	90分 必須	①サイバー攻撃手法とそのトレンド◆ ②脅威への対策◆ 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）	150分 必須	①サイバー攻撃手法とそのトレンド◆ ②脅威への対策◆ ③事例紹介 ④Work1：脅威と対策における“悪い見本”から学ぶ
3.投資	135分 必須	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）◆ ②体制構築・人材確保◆ ③費用対効果分析手法 ④Work1：各種対策の費用、損失想定、確率値から必要な投資を検討	150分 必須	①サイバーセキュリティのリスクマネジメントの特徴◆ ②対策における費用と損失の考え方◆ ③リスクマネジメントのケーススタディ ④Work2：リスク管理部門との対話
4.SHとの関係	135分 必須	①インシデント対応における経営層の役割◆ ②通常時の備えと情報開示の在り方◆ ③インシデント対応と情報開示の事例から学ぶ ④Work2：インシデント発生時の模擬記者会見	150分 必須	①インシデント対応プロセスとその準備◆ 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◆ ③インシデント対応と情報開示の事例から学ぶ ④Work3：インシデント発生時の社内外連絡
5.関係法令	–	–	60分 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◆ ②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◆

◆：オンライン・オンデマンド形式での実施を想定（これ以外での実施も可）

参考カリキュラムの詳細

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12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) ソフトウェア開発と脆弱性 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
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

参考カリキュラムの詳細

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) 脅威の関係主体 b) おもな攻撃手法 c) これまでの脅威の変遷 d) 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) 対策の基本的な考え方 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）

参考カリキュラムの詳細

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15分（オンデマンド60分、集合講習75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) 企業価値とリスクマネジメントの基本的な考え方 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費用対効果分析手法 （集合講習：25分）	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。 a) サイバーセキュリティの費用対効果分析の考え方 b) サイバーセキュリティが企業価値に及ぼす影響
④Work1：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：50分）	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14,15ページに記載）

参考カリキュラムの詳細

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15分（オンデマンド60分、集合講習75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通常時の備えと情報開示の在り方（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) 通常時の備え b) サイバーセキュリティに関する情報開示の考え方 c) 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：25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。
④Work2：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14ページに記載）

参考カリキュラムの詳細

部課長級向け　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（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。
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12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

参考カリキュラムの詳細

部課長級向け　第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。
時間設定・実施方式	１時間30分（オンデマンド・必須）
①デジタルインフラの要点（30分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。なお、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。 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
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

参考カリキュラムの詳細

部課長級向け　第３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) 脅威の関係主体 b) おもな攻撃手法 c) これまでの脅威の変遷 d) 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４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) 対策の基本的な考え方 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＞
④Work1：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とともに、望ましい対策方法について協議する。

参考カリキュラムの詳細

部課長級向け　第４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。
④Work2：自部署リスクとその対応 **（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。

参考カリキュラムの詳細

部課長級向け　第５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 **（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) 通常時の備え b) インシデント時に提供すべき情報の種類と流れ c) 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。
④Work3：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。

参考カリキュラムの詳細

部課長級向け　第６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

本カリキュラムにおけるオンライン・オンデマンド講座（第１単元）の扱い

■ 経営層向け・部課長級向けとも、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。

	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

（参考）受講要否確認のためのビデオ･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

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

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）

受講省略を前提とするが、受講いただいてもよい

受講を推奨（受講省略も可能）

受講は必須

（参考）各Workの例

（１）Work1（投資・体制構築）

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）Work2（記者会見）

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。

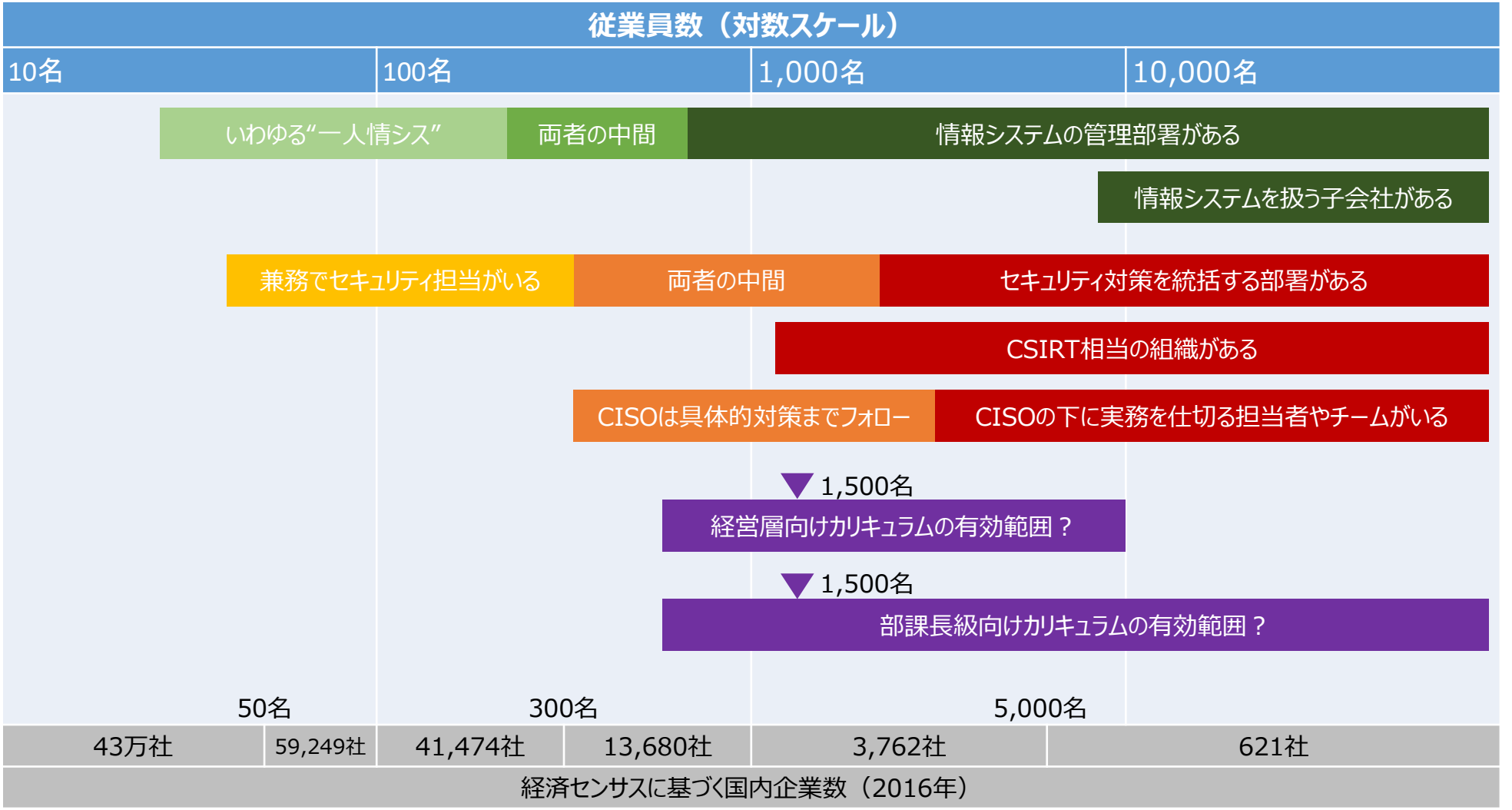
＜リスクによる損失例＞
- ✓ リスクとして想定していたのか？
- ✓ 想定していた場合、どのような対策を講じていたのか？
- ✓ 想定していなかった場合、他社で起きている事故はなぜ自社では起きないという判断に至ったのか？
- ✓ 被害規模の把握はできているか？
- ✓ データの復元の見通しは立っているのか？
- ✓ 再発防止のためにどのような対策を講じるのか？

＜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？

（参考）ロールプレイングの例（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
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**	**記者会見での応答5つ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
■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	「運」の要素を入れる「インシデントが発生しない」場合もあり、過剰なセキュリティ投資は適切でないことを示唆 凝るなら事後対応のフェーズ（人材の確保・調査等）を入れてもよいか？	セキュリティ投資がどのような効果を生じさせるかを理解してもらう意図	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してもらう意図	いたずらにセキュリティ投資を行えばよい訳ではないこと、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してもらう意図

（参考）受講者の所属組織の規模感



（参考）「プラス・セキュリティ」知識の習得に関するレベル感のイメージ

● 教育プログラムの目標をどこに設定するかの合意形成も必要

	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

このレベルに達するにはSANS Instituteの6日間フルタイムのような重いコースが必要？

座学のみ

座学＋α

このレベルを目標とするのでは教育プログラムの意味が無い？

経営層向け　部課長級向け

①Cyber-Risk Oversight Certificate（NACD＋CMU）

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。	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。
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。		
受講の要件	NACD Director's Handbook on Cyber Risk Oversight（経団連による和訳あり）の事前参照を推奨。		
方法	オンライン		
所要	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-		
URL	https://www.nacdonline.org/events/detail.cfm?ItemNumber=37092		

経営層向け　部課長級向け

②Cybersecurity and Crisis Management for Boards（UCLA/Anderson）

概要	● カリフォルニア大学ロサンゼルス校（UCLA）アンダーソンスクールオブマネジメントがオンラインで提供する取締役向け講座。 ● 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する。	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” **<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
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。		
受講の要件	なし		
方法	オンライン		
所要	連続する3日間		
費用	$4,000-		
URL	https://www.anderson.ucla.edu/executive-education/open-enrollment/cybersecurity-for-boards		

経営層向け 部課長級向け

③Cybersecurity Oversight for the Business Executive（CMU/SEI）

概要	● カーネギーメロン大学（CMU）ソフトウェア工学研究所（SEI）がオンラインと集合講習の双方で提供する２日間コース。 ● 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。	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
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		
受講の要件	なし		
方法	オンライン又は集合		
所要	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-		
URL	https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=P144		

経営層向け **部課長級向け**

④Applied Cybersecurity（MIT）

概要	● マサチューセッツ工科大学（MIT）のオンライン講座。 ● 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	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-
URL	https://professional.mit.edu/course-catalog/applied-cybersecurity-0

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

経営層向け **部課長級向け**

⑤Cybersecurity and Executive Strategy（Stanford）

概要	● スタンフォード大学が提供するAdvanced Cybersecurity Programの一部であるが、単独での受講も可能。 ● 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。	**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
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。		
受講の要件	なし		
方法	オンライン		
所要	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）		
URL	https://online.stanford.edu/courses/xacs302-cybersecurity-and-executive-strategy		

経営層向け **部課長級向け**

⑥Managing Cybersecurity Risk（シンガポール国立大）

概要	● シンガポール国立大学で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	**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
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	3日間（9:00-17:00）		
費用	Singapore$2,889-（割引制度あり）		
URL	https://www.iss.nus.edu.sg/executive-education/course/detail/managing-cybersecurity--risk		