「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　シラバス

2020.11 NISC基本戦略第1グループ

Ver. 1.0 Ver. Base【別紙１】をアップデートする形で作成（NISC基本戦略第1グループ、2020年11月）　※アップデート箇所は赤字

			【参考】DX推進者対象 DX with Cybersecurity 3日間教育コース（於：情報セキュリティ大学院大学（2020年11月18日～20日 WEB会議形式で実施））における対応				
目的		「DX with Cybersecurity」の推進（日本でDXが進み、セキュリティが保たれること、あるいはその同時推進）に向けて、特に「DXを推進する部門の責任者あるいは主要な役割を担う管理職（DX経営推進者・DX事業推進者等、部課長級を念頭）」を対象とし、サイバーセキュリティの観点から必要な仕組みを組織内に構築運用するために、専門家と協働するにあたって必要な「プラス・セキュリティ」知識を補充できることを目指す。	実施方法				実施講義との対応（日-時刻）【別紙２参照】
前提知識・経験		企業等において事業やプロジェクトの管理経験を有する者。情報通信技術やサイバーセキュリティに関する専門的な知識を必ずしも保有していない想定。企業経営に近い部署や業務の経験を有することが望ましい。					
スクーリング内容		**概要**	**予習**	**講義**	**演習**	**宿題**	
第1単元	**サイバー空間を理解するための基礎知識**	サイバーセキュリティの全体像を把握するとともに、サイバーセキュリティ上のリスクを理解するために必要となる、以下の基礎知識を理解することで、サイバーセキュリティの専門家とのコミュニケーションに必要なリテラシーを習得する。	なし	計170分	なし	なし	-
		(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）		30分			1-13:30 八剱氏
		(2) サイバー空間と社会（国家、政治、企業、テクノロジー、国民）		50分			1-11:30 三角氏
		(3) コンピュータ理論 ・コンピュータの基本構成（５大要素） ・ソフトウェアの階層 ・主なOSの種類（PC、サーバ：Windows(Microsoft)、macOS(Apple)、Linux／モバイル端末（スマホ等）：Android(Google)、iOS(Apple)） 情報通信ネットワーク理論 ・インターネットにおける通信の仕組み（インターネットについての基本的な概念（分散型）／OSI参照モデル、TCP/IPの階層、通信プロトコルの階層／IPアドレス／MACアドレス／ドメイン名、DNS） ・ネットワーク機器（ハブ、ルータ、スイッチ）		20分			1-13:30 八剱氏
		(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） ・サーバ、データセンタ、クラウドコンピューティング ・インターネットのプロトコルとそれを利用したシステム（電子メール／WWW）		10分			1-13:30 八剱氏
		(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） ・情報セキュリティ対策の基礎（９か条など）（基本的リテラシ） ・情報セキュリティの基礎（３要素(機密性、完全性、可用性)／脅威、脆弱性、リスク／樽の理論、多層防御、最小権限） ・代表的な暗号方式、認証方式（共通鍵暗号方式／公開鍵暗号方式／認証方式） ・デジタル署名、公開鍵基盤（PKI） ・ユーザ認証（多要素認証、二段階認証）		60分			1-14:40 松井氏
第2単元	**サイバー空間における脅威と対策**	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することができるよう、脅威及び脆弱性とその対策に関する以下の事項について学ぶ。	なし	計30分	なし	なし	-
		(1) 脅威の関係主体（利用者過失、犯罪組織等）		5分			2-9:00 藤本氏
		(2) 不正・悪用の歴史・トレンドと考え方、犯罪心理		5分			2-9:00 藤本氏
		(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		5分			2-9:00 藤本氏
		(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）		10分			1-11:30 三角氏
		(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）		5分			2-9:00 藤本氏
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**	サイバーセキュリティ確保のために事業者が遵守すべき事項や、効果的な対策実現のために参照すべき制度等について学ぶ。	なし	計90分	なし	なし	-
		(1) 法令・規格・諸制度対応の考え方と方法論・基本動作		90分			2-10:30 北条氏
		(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**	リスクマネジメントを行う上でのサイバーセキュリティ分野の特殊性について認識した上で、リスクを許容レベル以下に抑制するための方法について、グループワークによる演習を通じて学ぶ。	なし	計60分	計20分	なし	-
		(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		50分	-		2-9:00 藤本氏
		(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		10分	-		1-15:50 三浦氏
		(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		-	20分		3-10:00 演習
		(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**	事業において IT が担う役割が大きな企業ほど、サイバーセキュリティ対策を含めた形で適切にリスク管理されたサービスを提供することが企業価値の向上につながることを認識し、サイバーセキュリティ対策があらかじめ組み込まれた事業戦略を企画立案するための方法について、グループワークによる演習を通じて学ぶ。	なし	計210分	計100分	なし	-
		(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		20	-		1-15:50 三浦氏
				20	-		2-13:00 糸井氏
				20	-		2-14:00 亀山氏
				20	-		2-15:00 富永氏
				-	30		3-10:00 演習
		(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		20	-		1-15:50 三浦氏
				20	-		2-13:00 糸井氏
				20	-		2-14:00 亀山氏
				20	-		2-15:00 富永氏
				-	30		3-10:00 演習
		(3) セキュリティ品質とブランド戦略・顧客との信頼醸成		10	-		1-15:50 三浦氏
				10	-		2-13:00 糸井氏
				10	-		2-14:00 亀山氏
				10	-		2-15:00 富永氏
				-	25		3-10:00 演習
		(4) セキュリティ対策の証明と情報発信		10	-		2-9:00 藤本氏
				-	15		3-10:00 演習

「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　セキュリティ・ITに関する基礎知識の整理（2020.11 NISC基本戦略第1グループ）参照

別紙１

Ver. Base 普及啓発・人材育成専門調査会 サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ、「報告書」（2018年5月）表3より

戦略マネジメント層を担う人材育成のためのカリキュラム例（モデルカリキュラム）						
目的		企業等における事業戦略の企画・立案責任者が、事業戦略そのものに必要なサイバーセキュリティ対策を組み込む（例えば、セキュリティを考慮したビジネス設計や適切な外部委託）ために求められる、専門ベンダーとのコミュニケーションやリスク評価及び対応体制の構築のための知識・スキルを習得する。	**実施方法**			
前提知識・経験		企業等において事業やプロジェクトの管理経験を有する者。IT リテラシーは一般ユーザーレベルで可。企業経営に近い部署や業務の経験を有することが望ましい。				
スクーリング内容		**概要**	**予習**	**講義**	**演習**	**宿題**
第１回	**サイバー空間を理解するための基礎知識（基礎知識がある場合にはスキップしてもかまわない）**	サイバーセキュリティの全体像を把握するとともに、サイバーセキュリティ上のリスクを理解するために必要となる、以下の基礎知識を理解することで、サイバーセキュリティの専門家とのコミュニケーションに必要なリテラシーを習得する。	計2時間	計90分	なし	計2時間
		(1) 人類と IT（腕木通信から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（OS を中心に）、情報通信ネットワーク理論				
		(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回	**サイバー空間における脅威と対策**	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することができるよう、脅威及び脆弱性とその対策に関する以下の事項について学ぶ。	計2時間	計90分（場合によっては、90分×2回）	なし	計2時間
		(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回	**サイバーセキュリティに関連する法令・規格・諸制度**	サイバーセキュリティ確保のために事業者が遵守すべき事項や、効果的な対策実現のために参照すべき制度等について学ぶ。	計2時間	計90分	なし	計2時間
		(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回	**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**	リスクマネジメントを行う上でのサイバーセキュリティ分野の特殊性について認識した上で、リスクを許容レベル以下に抑制するための方法について、グループワークによる演習を通じて学ぶ。	計2時間	計30分	計60分	計2時間
		(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回	**企業価値向上とサイバーセキュリティ**	事業において IT が担う役割が大きな企業ほど、サイバーセキュリティ対策を含めた形で適切にリスク管理されたサービスを提供することが企業価値の向上につながることを認識し、サイバーセキュリティ対策があらかじめ組み込まれた事業戦略を企画立案するための方法について、グループワークによる演習を通じて学ぶ。	計2時間	計30分	計60分	計2時間
		(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				

別紙２　実施講義

DX推進者対象 DX with Cybersecurity 3日間教育コース（モデルカリキュラムの試行）　於：情報セキュリティ大学院大学（2020年11月18日～20日 WEB会議形式で実施）

2020年11月18日（水）（Web会議）	
10:00～10:30	開会の辞・カリキュラム内容説明 情報セキュリティ大学院大学　教授　藤本 正代 氏
10:30～11:30	【自己紹介】（各6分×10名）
11:30～12:30	【講義】「DX with Cybersecurityの全体像」 国立情報学研究所／東海大学情報通信学部 客員教授　三角 育生 氏
12:30～13:30	昼食
13:30～14:30	【講義】「DXを構成するIT関連基礎知識」 イグレック株式会社 理事　八剱 洋一郎 氏
14:40～15:40	【講義】「IoTから入る情報セキュリティの基礎」 情報セキュリティ大学院大学 教授　松井 俊浩 氏
15:50～16:50	【企業プレゼン】「DX事業事例とITおよびサイバーセキュリティ技術」 全日本空輸株式会社 取締役 常務執行役員　三浦 明彦 氏
17:00～18:30	【Webワークショップ】（自由に意見交換） 参加者でディスカッションテーマを決めて意見交換

2020年11月19日（木）（Web会議）	
9:00～10:20	【講義】「DXのためのリスクマネジメントと事故対応」 情報セキュリティ大学院大学　教授　藤本 正代 氏
10:30～12:00	【講義】「DX及びサイバーセキュリティの関係法令」 西村あさひ法律事務所 弁護士　北條 孝佳 氏
12:00～13:00	昼食
13:00～13:50	【企業プレゼン】「三井倉庫グループの情報システム概要について」 三井倉庫ホールディングス株式会社 執行役員 情報システム担当　糸居 祐二 氏
14:00～14:50	【企業プレゼン】「三菱マテリアルのデジタル・ビジネストランスフォーメーションの取り組み」 三菱マテリアル株式会社 経営戦略本部長補佐、CDO（Chief Digital Officer）　亀山 満 氏
15:00～15:50	【企業プレゼン】「アシックスのデジタル及びITの取り組み」 株式会社アシックス IT統括部　常務執行役員（CDO兼CIO）　富永 満之 氏
16:00～18:00	3日目の予定及びチーム編成説明＋Webワークショップ(自由に意見交換)

2020年11月20日（金）（Web会議）	
9:30～10:00	チーム演習の説明
10:00～12:00	【チーム演習】 自社の新規事業開発とサイバーセキュリティの取組における課題と解決策案をまとめる。 （経営トップへの報告イメージ）
12:00～13:00	昼食
13:00～15:00	【各チームによる発表】A、B、Cチーム発表（各40分×3チーム）
15:10～16:10	【発表サマリー・講評】＋受講者アンケート　自由に意見交換
16:10～16:30	閉会の辞　情報セキュリティ大学院大学　藤本 正代
16:30～17:00	休憩
17:00～19:00	【Workshop・意見交換会】 「サイバー脅威主体の「攻撃戦略」の変化」 株式会社サイバーディフェンス研究所 専務理事/上級分析官　名和 利男 氏を招いて