明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

資料5

DXに必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進
～試行カリキュラムについて～

普及啓発・人材育成専門調査会
2020年7月31日

情報セキュリティ大学院大学
藤本　正代

はじめに

2つの視点
①どのように推進するか？
②教育内容や方法は？

2020年3月2日の本委員会での発表

『戦略マネジメント人材育成』に関する現状と課題

- 「戦略マネジメント人材」の育成に関連するカリキュラム調査
- インシデントからの示唆
- 今後必要な「戦略マネジメント人材」の育成に関連する活動

今回

情報セキュリティ大学院大学で検討中の試行カリキュラム：
『DX推進者対象DX with Cybersecurity 3日間教育コース』

- 試行カリキュラム作成にあたって考えたこと
- カリキュラムのねらいや目的
- カリキュラムの内容

情報セキュリティ大学院大学で検討中の試行カリキュラム

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■試行カリキュラム作成にあたって考えたこと

- DX事業推進者の育成が目的(※)
- 受講しやすいスケジュール
- “報告書のカリキュラム例”で提示されている5つの項目(本プレゼン資料の付録2)の内容をカバーしつつDX事業推進者等によるプレゼンや参加型のカリキュラムを検討
- 遠隔受講が可能であること

※3月2日の本専門調査会で発表した課題。本資料の付録1を参照。

カリキュラムのねらい

- 本カリキュラムは、サイバーセキュリティ確保を担保した事業モデルを開発できる人材の育成を目指す。
- 今後さらに進むであろうDX（デジタルトランスフォーメーション）において、サイバーセキュリティの観点から必要な仕組みを企業等の組織内に構築・運用するために専門家と協働するにあたって必要な知識。

受講対象者

- DX with Cybersecurityを実現するため、企業等の組織で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経営推進者やDX事業推進者、等）あるいは近い将来にそのような役割を担う可能性のある管理職を対象としている。
- 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は特に必要としない。
- Webexを使用した参加が可能な方。

日程等

■日時と開催場所等(予定)

- 11月18日（水）9:00～18:30　WebexによるWeb会議システム
- 11月19日（木）9:00～18:00　WebexによるWeb会議システム
- 11月20日（金）9:30～20:00　WebexによるWeb会議システム

カリキュラム内容（１日目）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ DX with Cybersecurityの共通理解、基礎技術知識の習得、企業等の取組紹介

2020年11月18日（Web会議）　司会：情報セキュリティ大学院大学　藤本		
9:00～10:00	60	接続テスト
10:00～10:30	30	開会の辞＋カリキュラム内容の説明
10:30～11:30	60	自己紹介（各6分×10名）
11:30～12:30	60	**【講義】DX with Cybersecurity全体像** DX with Cybersecurityの基本コンセプトを理解していただくための講義。
12:30～13:30	60	昼食
13:30～14:30	60	**【講義】サイバー空間を理解するための基礎知識(仮）：** DX with Cybersecurityの理解に不可欠な情報通信技術の知識（付録2 第1回　(3)(4)を参照）。
14:40～15:40	60	**【講義】サイバーセキュリティを理解するための基礎知識(仮）：** DX with Cybersecurityの理解に不可欠なサイバーセキュリティの要素技術知識（付録2　第1回　(5)を参照）。
15:50～16:50	60	**【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 DX事業推進にあたって取り組んでいるサイバーセキュリティ(仮)
17:00～18:30	90	Webワークショップ(自由に意見交換) ※冒頭に参加者でディスカッションテーマを決めて意見交換。

カリキュラム内容（2日目）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ リスクマネジメント、法規制等の基礎知識習得、企業等の取組紹介

2020年11月18日（Web会議）　司会：情報セキュリティ大学院大学　藤本		
9:00～10:20	80	**【講義】リスクマネジメントと事故対応** DX推進に必要なリスクマネジメントの基礎知識。
10:30～12:00	90	**【講義】サイバーセキュリティに関連する法令・規格・諸制度** DX推進にあたって必要な法規制などの基礎知識。
12:00～13:00	60	昼食
13:00～13:50	50	**【企業プレゼン】企業１**
14:00～14:50	50	**【企業プレゼン】企業2**
15:00～15:50	50	**【企業プレゼン】企業3**
16:30～18:00	90	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)

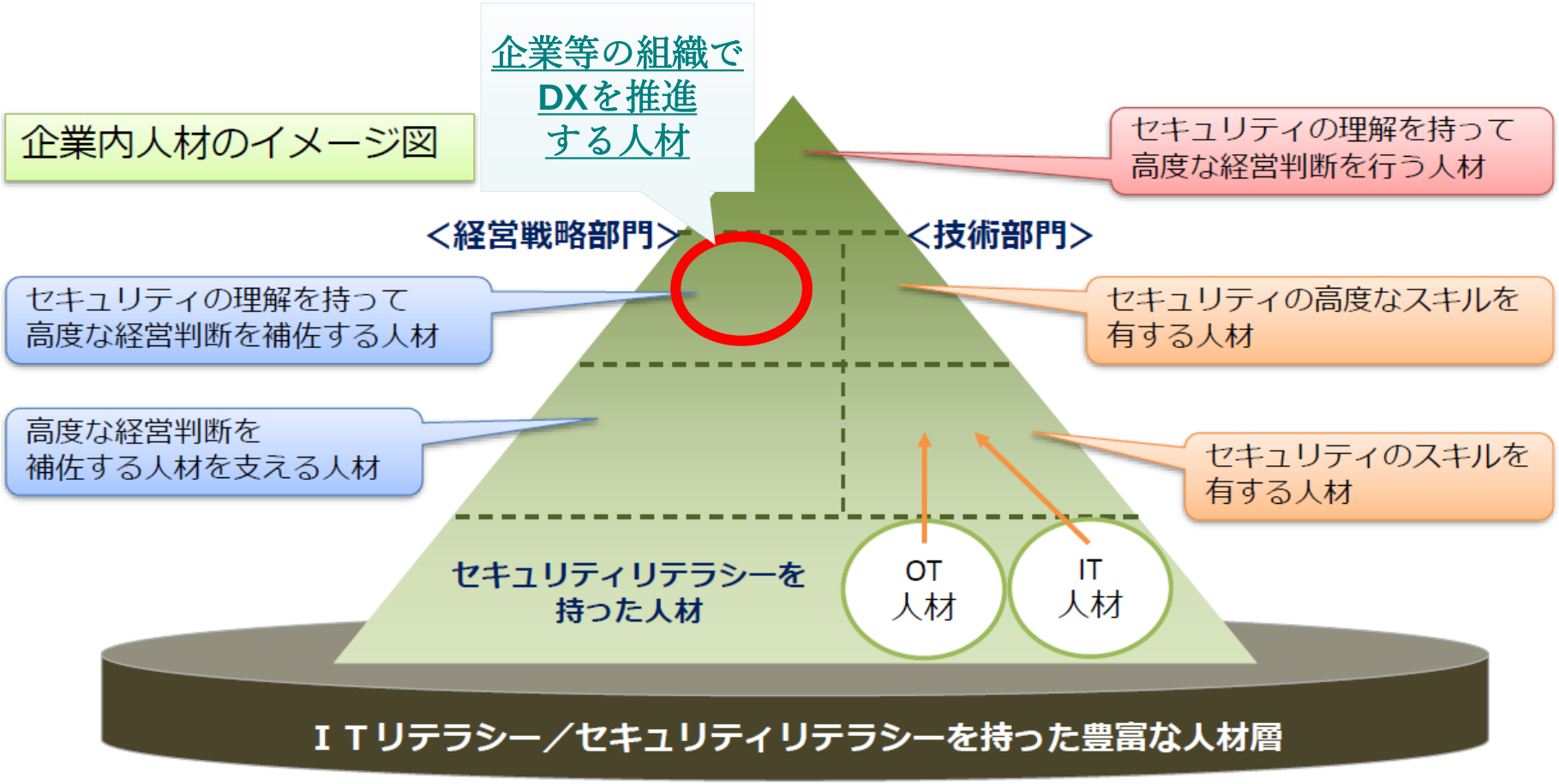
カリキュラム内容(３日目)

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2020年11月20日（Web会議）司会：情報セキュリティ大学院大学　藤本		
9:30～10:00	30	チーム演習の説明
10:00～12:00	120	［**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	60	昼食
13:00～15:00	120	A、B、Cチーム発表（各40分×3チーム）
15:10～16:10	60	発表サマリー(講評) ＋受講者アンケート
16:10～16:30	20	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	30	休憩
17:00～20:00	180	Workshop:ゲストを招いての意見交換会

付録1　今後必要な取り組みについて

- カリキュラムの実施者ヒアリングから、報告書が提示した5項目の内容は有効。
- 一方で、インシデントの示唆から、DX事業推進者の育成が不十分。



付録2　報告書のカリキュラム例

表 3：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

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。
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	説明	実施方法
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。 (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）	予習 2 時間 講義 90 分 宿題 2 時間
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。 (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）	予習 2 時間 講義 90 分 （場合によっては、90×2 分） 宿題 2 時間

出典：NISC　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 ～「戦略マネジメント層」の育成・定着に向けて～ 、平成 30 年5月 31 日 、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、p16

付録2　報告書のカリキュラム例（続き）

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。 (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、SP-800.171 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）	予習 2 時間 講義 90 分 宿題 2 時間
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。 (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）	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間
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。 (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	予習 2 時間 講義 30 分＋ 演習 60 分 宿題 2 時間

出典：NISC　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 ～「戦略マネジメント層」の育成・定着に向けて～ 、平成 30 年5月 31 日 、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、p17