資料2

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

『戦略マネジメント人材育成』に関する現状と課題

普及啓発・人材育成専門調査会
2020年3月2日

情報セキュリティ大学院大学
藤本　正代

本日の内容

1. 「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
2. インシデントからの示唆
3. 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

IPA 産業サイバーセキュリティセンター

■ 2つのコース

① 「セキュリティ組織管理」コース

- ✓ 対象と内容：セキュリティに係る方針・戦略・計画及び組織体制を策定する、管理職クラス。戦略マネジメント層として、経営層が認知しておくべきセキュリティ機能の重要性を理解する。
- ✓ 2日間、両日とも12:30～17:30（2020年2月）

② 「セキュリティ実務管理」コース

- ✓ 対象と内容：セキュリティ戦略に基づき対策を担当されている方や、セキュリティ計画に基づくセキュリティ体制を検討されている方。戦略マネジメント層として、技術者が理解しておくべきセキュリティ機能の重要性を理解する。
- ✓ 2日間、両日とも13:30～17:30（2020年2月）

戦略マネジメント系セミナー　2019年度コース
https://www.ipa.go.jp/icscoe/program/middle/strategic_management/2019.html

IPA 産業サイバーセキュリティセンター

- 2018年11月と12月に週1回程度でシリーズ開催
- 全7回
- 18:30～20:30

- CISO、CIOに相当する役割を担っている方
- 総務部門、広報部門、生産部門などの統責任者及びマネージャークラスの方
- その他、企業においてリスク管理に関わる方全般

【責任者向けプログラム】第一回戦略マネジメント系セミナー ご案内資料
https://www.ipa.go.jp/files/000069227.pdf

CUMOT（東京工業大学）

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

- CUMOT(キューモット）は、“Career Up MOT”の略称。社会人アカデミーのプログラムとして、環境・社会理工学院 技術経営専門職学位課程が実施するMOT(技術経営)に関するサーティフィケート・プログラム。
- CUMOTにはMOT(技術経営)や知的財産戦略、等のコースがあり、その中のひとつとして「サイバーセキュリティ経営戦略コース」がある。
- カリキュラムは、リスクマネジメント・インシデント対応について理解、及び参加型の講義スタイル。
- 対象：
  - サイバーセキュリティ経営の導入・促進に取り組む（取り組みたい）経営企画部門等の方
  - CISOまたはその補佐役（戦略マネジメント層）の即戦力を目指す方
  - 情報システム/セキュリティ部門の一担当者から、企業・組織のサイバーセキュリティ経営を担う戦略的人材へのステップアップを目指す方
  - 事業部門の事業経営／事業戦略に、サイバーセキュリティ経営の手法を取り入れたい方
  - その他、サイバーセキュリティ経営のエッセンスを体系的に学びたい方　等
- 14日間、平日夜2時間(2020年1月～4月)

出典：
https://cumot.mot.titech.ac.jp/form/contact.html
https://www.academy.titech.ac.jp/cumot/cy/index.html

情報セキュリティ大学院大学 カリキュラムトライアル

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

- 『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～』のp.16, 17に記載の「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」の内容をベースに試験的カリキュラムを作成・実施
- “報告書のカリキュラム例”で提示されている5つの項目

  [詳細は付録参照]

  1. サイバー空間を理解するための基礎知識
  2. サイバー空間における脅威と対策
  3. サイバーセキュリティに関連する法令・規格・諸制度
  4. 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
  5. 企業価値向上とサイバーセキュリティ
- 5日間、90分(2019年1月～2月)

ヒアリング調査等に基づく「戦略マネジメント人材育成」カリキュラムの現状理解

■ 対象

- 対象者について、募集対象としては経営企画部門やCISOなどを含めているが、実際の受講生は情報システム部門・総務部門の管理職、コンサルタントやベンダーが多くなる傾向がある。
- セキュリティ技術対策・セキュリティ実務者層育成が先行した後、セキュリティマネジメント層育成の必要性が認識された背景があり、その影響で事業リスクマネジメントや戦略・経営企画とのつながりが弱い。

■ 内容等

- “報告書のカリキュラム例”で提示されている5つの項目の内容については、すべてのカリキュラムでおおむね含まれている。
- 実務者による講演や参加型（グループディスカッション等）の講義形式を導入している。
- 受講生が参加しやすいようスケジューリングに配慮している（コンテンツを取捨選択、圧縮などで調整）。

DX事業に関連したセキュリティインシデント

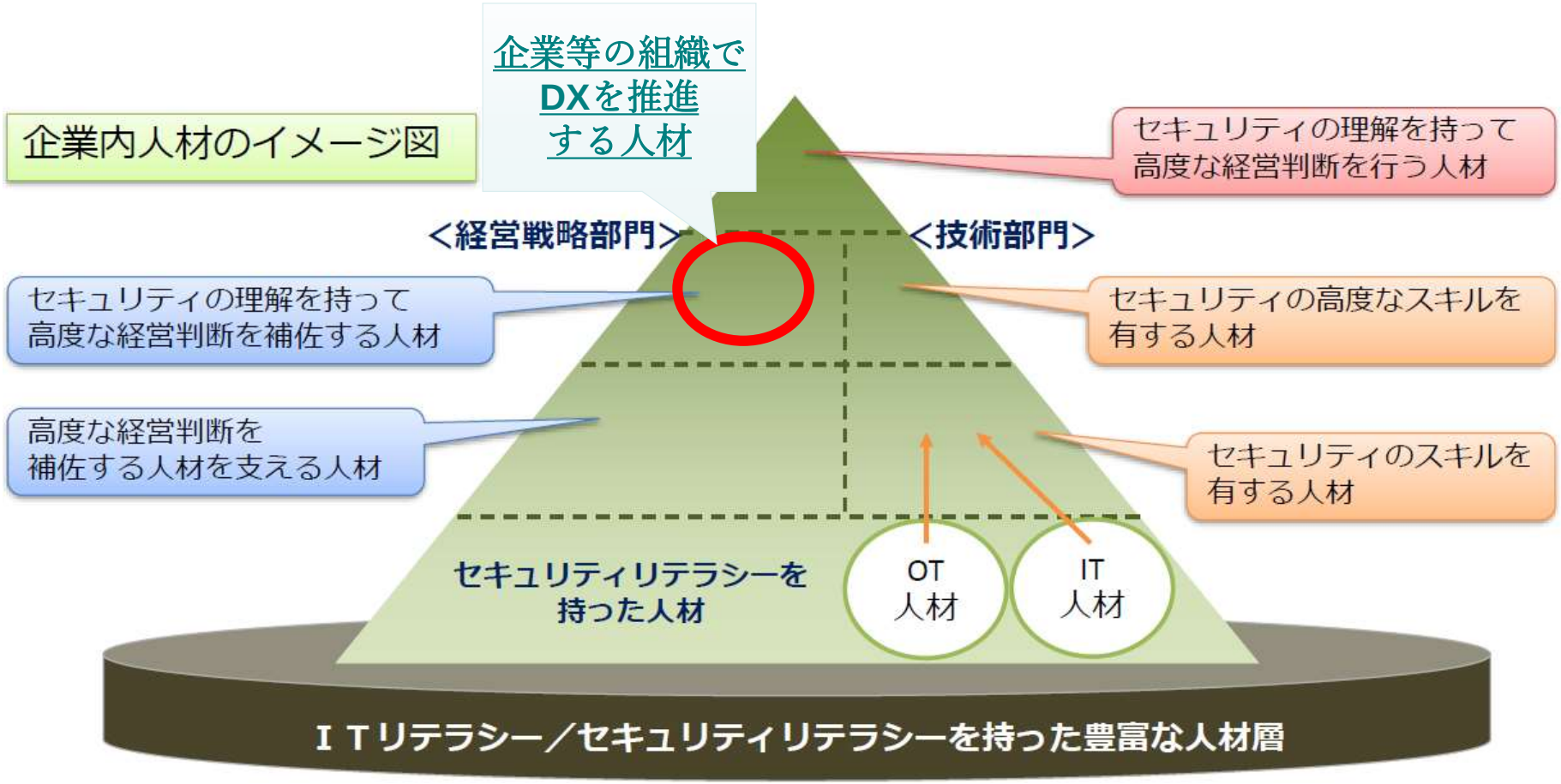
■ITを活用した新規サービスにおける不正利用
■個人情報を含むデータ利活用の失敗、等

インパクト
サービス廃止等

サイバーセキュリティの確保が
DX事業の推進を左右する

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

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 5 G、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

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