資料１－５

政策課題２
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

令和3年1月

内閣サイバーセキュリティセンター（NISC）
基本戦略第１グループ

問題意識

〇今後、経済社会のデジタル化に伴い、サービスやプロセスのDXが加速的に進展していくことが想定される中で、経営層や経営企画部門を含め、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全社的な問題としての認識し、自律的に対策が実施されることが求められる。

〇対策実施に当たっては、例えば経営者では、

- どんなシステム・情報資産が自社を支えているか？（デジタル化・ネット活用が進む自社の業務・製品・サービスやサプライチェーンを含む。）
- それらが止まると業務にどのような／どれくらいの範囲で支障が生じるのか？
- 情報漏えいすると、どのような損害が生じるのか？

といった自社の状況の把握から始めることが考えられるが、そうした初歩の取組から具体的な対策の実施に至るまで、その過程でセキュリティ専門人材とのコミュニケーションは欠かせない営為となる。

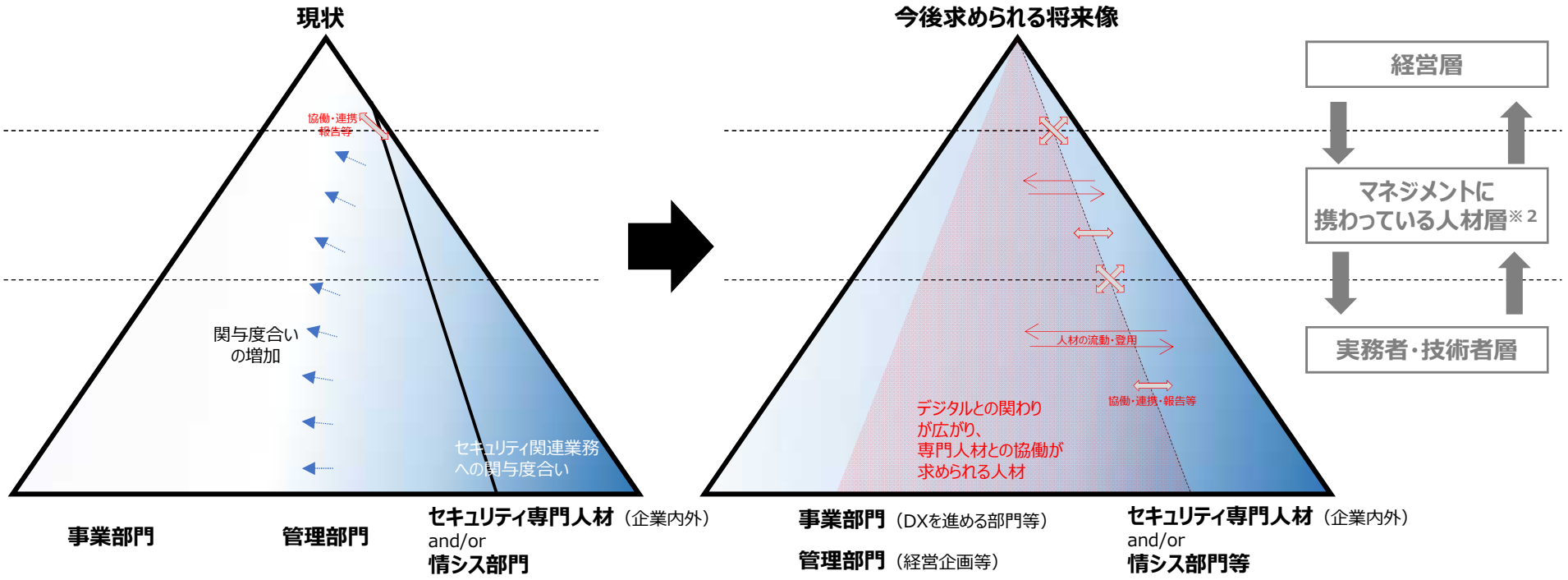
〇一方で、サイバーセキュリティの確保は全社的な課題ではなく、情シス部門又はセキュリティ担当で対処すべき課題と捉えられていないだろうか？

「プラス・セキュリティ」知識の考え方①

○今後は、（経営者やマネジメントに携わっている人材層をはじめとして）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る。

○こうした協働を行うに当たって必要となる知識として、社会人になって以降も、時宜に応じてプラスして習得すべき知識を、ここでは「プラス・セキュリティ」知識と呼ぶ。

＜概念共有のためのイメージ図※1＞



- DX進展の中で、特にDXを進めている事業部門や経営企画部門等において、セキュリティ関連業務との関与が増加していく。
- 様々な人材層・部門において、専門人材との協働が求められる。（協働のためには、互いの領域への相互理解が前提となる。）

※1　本イメージ図は、用語の考え方について強調すべき点を共有するための資料として、イメージを大まかに記した資料であり、本内容につき精緻化等を図るためものではない。
※2　現行の「サイバーセキュリティ戦略」（2018年7月27日閣議決定）によれば、こうした人材層において、「経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材」が「戦略マネジメント層」と定義されている。

「プラス・セキュリティ」知識の考え方②

○こうした協働はあらゆる部門・人材層において想定されるが、経営企画部門や事業部門のマネジメントに携わっている人材（部課長級など）を例にとれば、「プラス・セキュリティ」知識を補充する取組は、従来取り組まれてきた「戦略マネジメント層の確保・育成」のためのアプローチの１つとして捉えることもできる。

＜セキュリティ専門人材との協働例＞

① デジタルシステムストラテジー
- 「セキュリティ統括」と連携：次期デジタル戦略立案時のセキュリティ体制検討

② デジタルプロダクト開発
- 「セキュリティ統括」と連携：開発環境の更新に関する協議
- 「脆弱性診断・ペネトレーションテスト」と連携：テスト時の脆弱性診断実施
- 「セキュリティ調査分析・研究開発」と連携：脆弱性情報の共有

③ デジタルプロダクト運用
- 「セキュリティ統括」と連携：新規に利用するクラウドアプリのアクセス制御方法協議
- 「セキュリティ監査」と連携：監査指摘事項への対応方法の協議

④ 経営リスクマネジメント
- 「セキュリティ統括」と連携：サイバーセキュリティ保険加入に関する協議

⑤ 法務
- 「セキュリティ統括」と連携：法規改正への対応方針協議

⑥ 事業ドメイン（戦略・企画・調達）
- 「セキュリティ統括」と連携：新規サービスに伴うサイバー関連リスクの評価

⑦ 事業ドメイン（生産現場・事業所管理）
- 「セキュリティ統括」と連携：インシデント発生に備えた訓練の共同実施

（出典）サイバーセキュリティ経営ガイドライン　付録F サイバーセキュリティ体制構築・人材確保の手引き（令和２年９月30日）
経産省、http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

＜戦略マネジメント層の確保・育成との関係性＞

＜想定されるキャリアパス＞

「戦略マネジメント層」を担う人材については、経営企画部門や事業部門等のマネジメントラインにおいて、キャリアパスを歩み、現時点でそれらの部門におけるマネジメントに携わっている人材を想定している。そういった人材が、様々な課題に対するマネジメントを行う中の一つの要素として、サイバーセキュリティ関連のリスクに起因する経営・事業上の脅威に対するマネジメントも行うことが期待される。なお、（一般的に伝統的な企業によく見られる傾向として、）事業部門等を含めたサイバーセキュリティのマネジメントに関し、IT 部門（情報システム部門）やリスクマネジメント部門が一括して担当するケースがある。その場合においては、少なくとも経営企画部門や各事業部門との緊密な連携・コミュニケーションや、それらの部門に対するガバナンスの確保が必要である。さらに、IT 部門（情報システム部門）やリスクマネジメント部門の当該人材は、その部門のみの経験ではなく、経営企画部門や事業部門の経験を有していることが望ましい。

→前段と後段で両面のアプローチが記述されている。
「プラス・セキュリティ」知識を補充する取組は前段のアプローチと位置付けられる。

（出典）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（平成30年５月31日）
https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf

検討論点と有識者からいただいたご意見

①ユーザ企業の主体的な IT 活用・DX 実施において経営・事業を担う者が「プラス・セキュリティ」知識を補充できるよう、対象人材（例えば、ユーザ企業において経営を担う者（CxO等）と事業を担う者（部課長クラス等）を分けて考えるなど）**に応じてどのようなモデルカリキュラムが考えられるか。**

＜有識者からの主なご意見＞

○「プラス・セキュリティ」の内容は簿記に性格が近い。基本知識の内容は昔と大きく変わっておらず、体系化していくとよい。

○経営層向けに同様のカリキュラムが実施されるのであれば、半日程度の長さがよいのではないか。

○藤本委員のカリキュラムに加え、新しく事業開発や工場のセキュリティ責任者になる人物にセキュリティ知識を補充してもらうためのプログラムも考えていく必要がある。

○モデルプログラムは企業にいる人材をターゲットにしているが、次世代を担う人材の育成も重要。技術系学生・文系学生両方へのアプローチが必要だが、特に後者は中堅私大でのIT教育が不足しており、自らも取り組んでいる。

②カリキュラムの構築や普及をいかに政策的に後押ししていくか。（普及啓発と関連する観点もあるため、中小企業や地域を含めた展開も考えられるのではないか。）

＜有識者からの主なご意見＞

○DXを推進するためには、業務経験豊富なマネジメント層が変革をリードすることが肝要。ただ、DXに必須の要件となるセキュリティの見識も備えた人材は殆ど育成出来ていない。セキュリティをマネジメント出来る人材には不足感が強く、社内で活用しやすい育成プログラムへのニーズは高い。

○研修提供事業者の立場からみれば、現行の試行カリキュラムを行っても「プラス・セキュリティ」知識はニーズが顕在化しづらい上に、サンプル数が少ないので、現時点では参入判断が難しい。

○「プラス・セキュリティ」の動きを広めていくためには、経営層向けのプログラムから始めていくと波及効果が大きい。

○プログラムの普及に向けて、プログラム作りの参考になる材料を共有していくことが重要だが、コンテンツの基盤になるものと教育技法は、分けて考えた方がよい。

カリキュラムのモデル化

検討論点①

○内外のセキュリティ専門人材と協働するために必要となる知識は、部門・人材層等によって異なるため、「プラス・セキュリティ」知識は一意に体系化される性質のものではないが、知識を提供するプログラムが広く普及していくためには一定のモデル化が必要である。

○このため、まずは、今後デジタル化が進んでいく中で特に需要が高まると考えられる、「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」（※）を対象層としてモデルカリキュラム開発を試行。

（※）DX経営推進者・DX事業推進者等、部課長級であって、必ずしも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方を念頭。

○特に、NISCにおいては、過去に整理された「戦略マネジメント層」向けのモデルカリキュラムと対応し、コンピュータ・情報通信ネットワーク・インターネット・サイバーセキュリティに関する知識のうち、DX推進の中で専門家との協働に当たって、最低限必要で役に立つと考えられる基礎知識の整理作業を行った。

＜戦略マネジメント層育成モデルカリキュラム(2018年)＞ ※参考資料1-1 別紙1参照

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（鍼木通信から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
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

最低限必要で役に立つと考えられる基礎知識を体系化

作業①： DX事業推進に際し活用が想定される場面から逆算し、どのような状態を目指すかを整理した。

↓

作業②： 実務目線からIT 初心者に必要な知識が整理された「IT パスポートシラバス」を参照し、ｉ：詳細な目標とｉｉ：予め理解することが望ましいと考えられる基礎概念を　整理した。

【詳細は参考資料2-2等を参照。】

↓

情報セキュリティ大学院大学において実施されたプログラム（試行カリキュラム）において、上記の作業結果を参考にしていただいた。

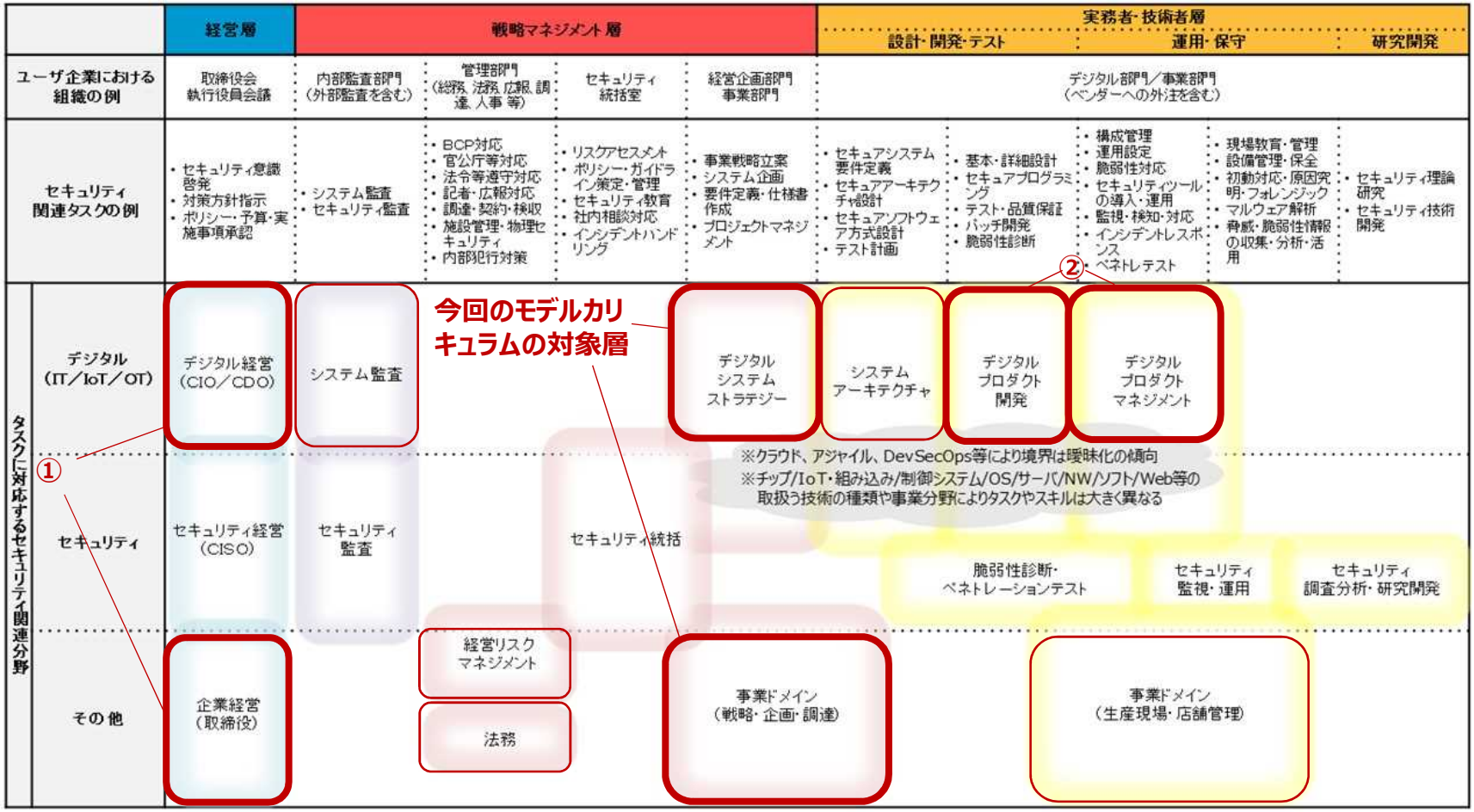
※（出典）サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書」（2018年5月）

プログラムの普及促進策①

検討論点②

○さらに、今回の試行をベースとして、部課長級向けのカリキュラムの改善に加え、今後需要が高まっていくと思われる他の人材層に向けた取組の進展も期待される。（また、次世代の人材育成においても念頭に置く必要がある。）

○例えば、政策課題１でとりあげたように、①経営層：意識改革とあわせてDXに対応した体制構築を担える人材、②製品開発・品質管理部門：PSIRTを担う人材で潜在的な需要があると考えられる。



▢「プラス・セキュリティ」知識が必要となり得る分野

（出典）サイバーセキュリティ経営ガイドライン　付録F サイバーセキュリティ体制構築・人材確保の手引き（令和２年９月30日）
経産省、http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

プログラムの普及促進策②

検討論点②

○量的な広がりを生むためには市場が形成され需要と供給が相応して増加していくことが望ましいが、その初期段階においては、需要の喚起に加え、需要者からみて一定の質が確保・期待される仕組みづくりが重要ではないか。

○海外の事例を参考に、当面、関係省庁との連携の下、NISC「普及啓発・人材育成ポータルサイト」を活用し、基礎的なマテリアルとあわせ、官民で行われる「プラス・セキュリティ」講座の掲載を積極的に行うことを検討中。（詳細は今後検討。）

＜「NISC普及啓発・人材育成ポータルサイト」への掲載事項（イメージ）＞

	政策課題１	**政策課題２**	政策課題３
基礎的マテリアル	・「手引き」 ・ナレッジ集【今後作成】	・「プラス・セキュリティ」モデルカリキュラムに関する資料	・スキル等の共通言語化ツール （JTAG、ITSS+等）
先行事例	・DX時代に対応したPSIRTやDSIRT/SSIRT構築事例	・「プラス・セキュリティ」講座	・新たな流動モード事例

◆今後の検討事項：

〇どのような講座を「プラス・セキュリティ」講座とみなして掲載を行うか。

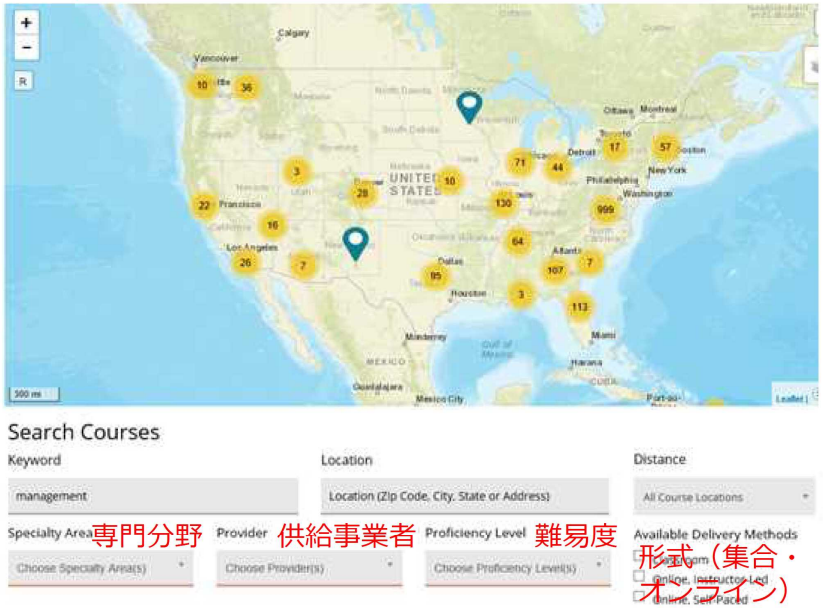
〇どのような情報を整理してポータルサイトに掲載を行うか。

（参考）米国の事例

○トレーニングコースに関する基礎的な情報が、提供事業者からの申請に基づき、カタログとしてHP上にわかりやすくまとめられている。

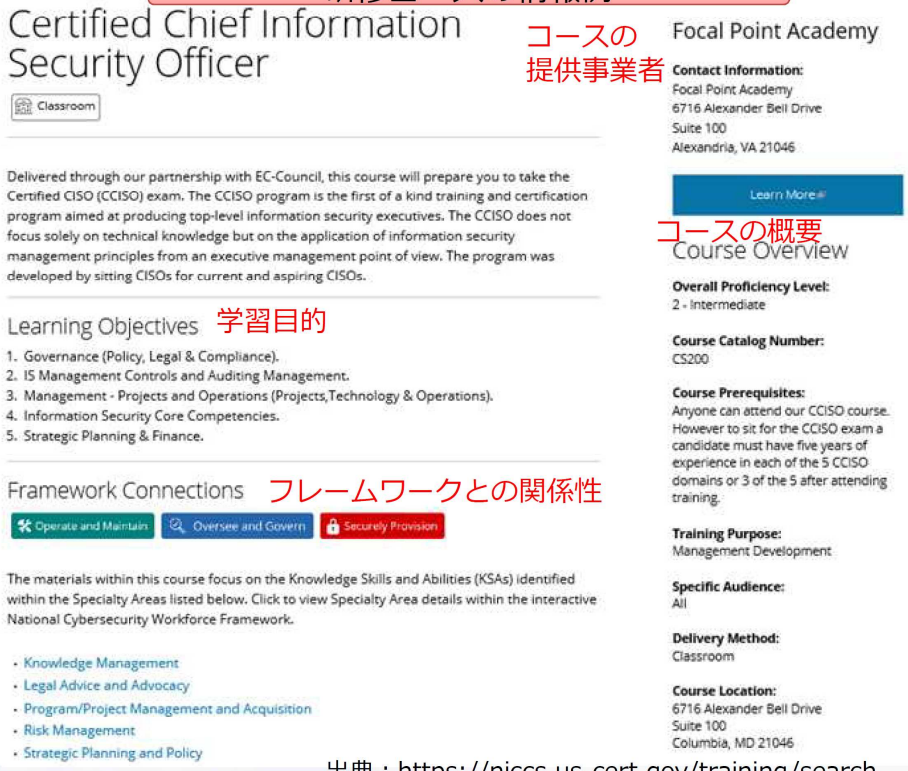
米国国土安全保障省（DHS）は、NICCS（National Initiative for Cybersecurity Careers and Studies）において産官学の様々な教育訓練コース（約3300）のカタログを提供。

全国の教育・訓練コースが検索可能



※NICCS:DHSが、米国政府の雇用者・産業界・教育者・学生と、サイバーセキュリティ教育事業者の連携を図るために提供しているサイバーセキュリティ人材育成のためのオンラインコンテンツ。教育訓練コースのカタログの他に、人材開発の成熟度モデルや、人材計画診断などのツールを提供している。

研修コースの情報例



出典：https://niccs.us-cert.gov/training/search

（出典）2017年12月27日 第3回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資料より抜粋