資料２

「DX推進人材のスキルへの影響について」
～サイバーセキュリティ～

2024年2月1日(木)

NEC サイバーセキュリティ戦略統括部
武智 洋

自己紹介

- 武智　洋　（たけち　ひろし）
  - 所属： 日本電気株式会社 サイバーセキュリティ戦略統括部

- 主な外部活動
  - IPA デジタルスキル標準 サイバーセキュリティ検討WG 主査
  - JAIST支援機構 産学官共創フォーラム セキュリティ人材育成研究会 (https://www.jaistso.or.jp/)
  - SC3 運営委員、産官学連携WG-TFメンバー
  - 一般社団法人サイバーリスク情報センター（CRIC）代表理事 (http://cric.jp/)
  - 産業横断 サイバーセキュリティ検討会（CRIC CSF) 副会長 (http://cyber-risk.or.jp/)
  - 日本セキュリティオペレーション事業者協議会 (ISOG-J) 代表 (http://isog-j.org/)
  - 独立行政法人 情報処理推進機構　(IPA)
    産業サイバーセキュリティセンター 主任研究員
  - ITU-T SG17 Q10 Associate Rapporteur

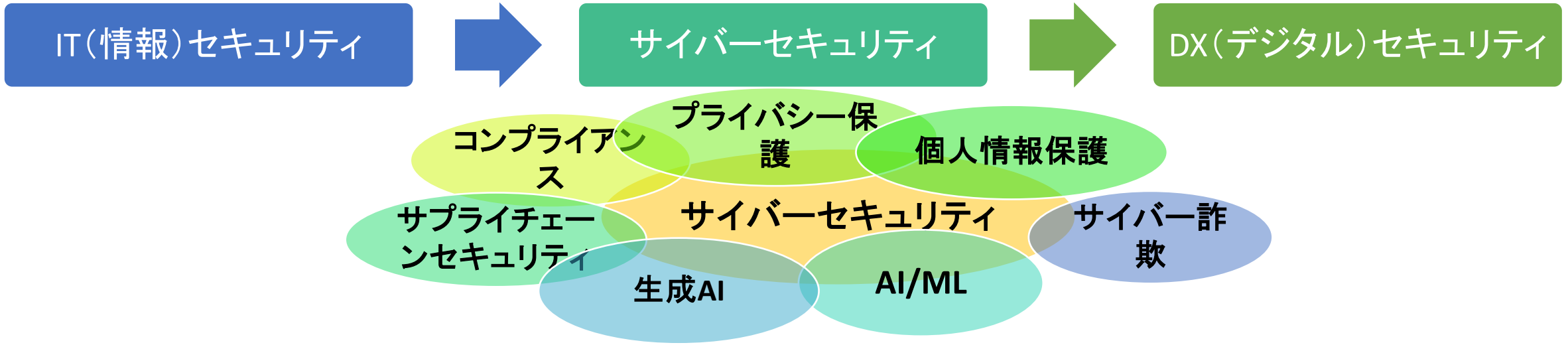
アジェンダ

- 生成AIとセキュリティ専門人材育成
- セキュリティ人材育成システム（海外事例）

生成AIとセキュリティ専門人材育成

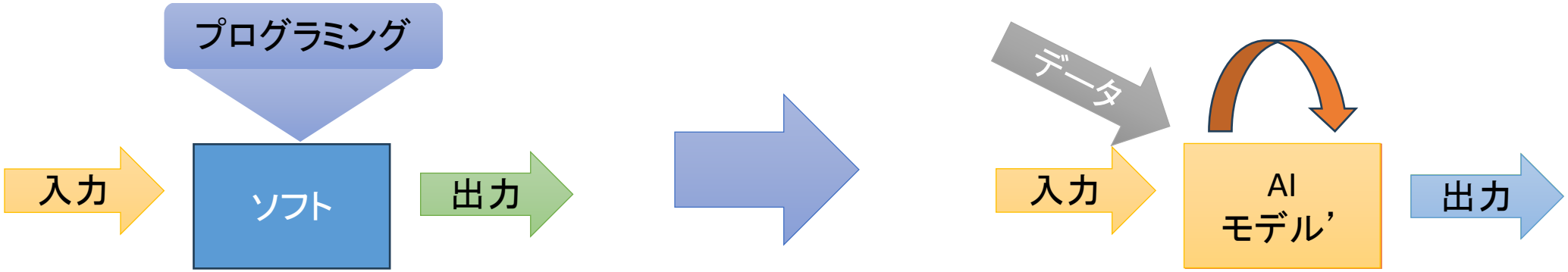
DX推進におけるセキュリティの状況

1. セキュリティの広がり



2. セキュリティ分野へのAI/MLによる影響

- ソフトとデータの境界を融合



生成AIの負の面

1.偽造された情報の拡散

2.プライバシーの侵害

3.攻撃への悪用

- 例）詐欺やなりすまし攻撃への利用

4.バイアスと公平性の問題

- トレーニングデータに含まれるバイアスよる偏った意思決定や差別的な結果の可能性

5.倫理に反する利用

- 例）虚偽の映像や音声の生成による誤解や混乱の発生

6. 知的財産権の問題

7.セキュリティへの脅威

8.労働市場への影響

- 自動化が進み仕事が失われる

9.法的責任の曖昧さ

- 生成AIによる生成物の法的な責任が曖昧
- 問題が発生した場合の法的取り決めが難しい

10.環境への影響

1. 生成AIのトレーニングによるエネルギー消費や二酸化炭素排出増加

生成AIのセキュリティへの脅威の例

1. **ディープフェイクの拡散**
   - ディープフェイク（本物と区別が難しい合成映像や音声）による偽造された映像や音声による社会的混乱
2. **フィッシング攻撃の高度化**
   - フィッシング攻撃がより巧妙なり、被害者が騙されやすくなる
3. **音声指紋の偽造**
   - 生成AIが権威者や社内の人物の声を模倣し、不正な指示を実施させる。
4. **セキュリティシステムの回避:**
   - 既存のセキュリティシステムを回避する手段として使われる
5. **ソーシャルエンジニアリングの高度化**
   - より洗練されたソーシャルエンジニアリング攻撃が可能に
   -
6. **情報漏えいの増加**
   - オープン生成AIへの機微な情報の入力
7. **機械学習モデルの攻撃**
   - 生成AIのMLモデルにリバースエンジニアリング攻撃が行われ、モデルのセキュリティが脆弱化（データ搾取、ご認識、モデル複製）される
8. **検知技術の未熟さ**
   - 生成AIに対しての検知・防御する技術が対応出来ない可能性
9. **マルウェアの進化**
   - 既存対策を回避する新しい種類のマルウェアの生成
10. **サイバー犯罪の増加:**
    - 生成AIの進展が、サイバー犯罪者にとって新たな手段を提供

生成AIのセキュリティ専門人材育成への影響

1. 新しいスキルの必要性
   - AI技術に関する知識やスキル（機械学習やディープラーニングなどの基礎的な概念や、生成AIの仕組みの理解）

2. AIによるセキュリティ脅威への対応
   - 生成AIを悪用した攻撃やセキュリティ脅威に対処するスキルや知識を向上させる必要
   - 不正な生成AIの検知や対策が求めらる

3. セキュリティツールの選定と運用
   - 生成AIを含む新しいセキュリティツールやプラットフォームを選定し、適切な運用スキルの習得

4. データの適切な取り扱い
   - 生成AIのトレーニングに使用されるデータが機密性を持つことがあるため、データの適切な取り扱いや保護について専門的な知識が必要

5. 進化し複雑化する脅威に対する防御
   - AIを活用した高度な攻撃に対抗するより高度なセキュリティ対策の実装や監視ができることが求められる

6. 人的適正の重要性
   - 進化し続ける生成AIを含むテクノロジーを理解しようとする姿勢と洞察力や判断力がより不可欠となる

7. セキュリティポリシーの変更と遵守
   - 生成AIの利用に伴い、組織はセキュリティポリシーを変更し、AIに関連するリスクに適切に対処する必要がある。これらの変更を理解し、従う必要がある

8. セキュリティトレーニングの強化
   - AI技術に関連する最新の知識やスキルに焦点を当てた実践的なトレーニングが必要

9. コミュニケーションスキルの向上
   - 技術者だけでなく、他の部門や組織内のステークホルダーとの効果的なコミュニケーションスキルがより必要とされる
   - 生成AIの影響やリスクを他の関係者に説明するスキルが求められる

10. 倫理的な視点の重要性
   - 技術的な側面だけでなく、倫理的な視点からもセキュリティに取り組む必要
   - 生成AIの利用が倫理的に適切かどうかを検討し、適切なガイドラインを策定することが求められる

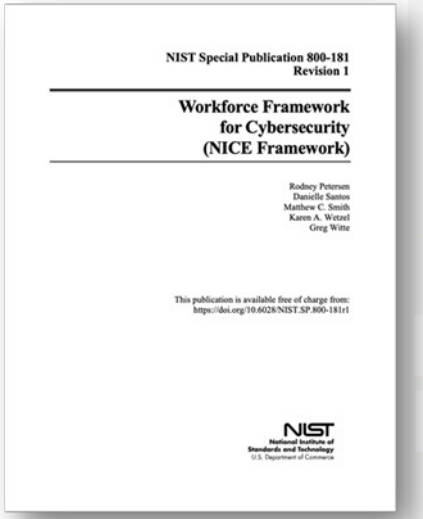
セキュリティ人材育成システム（海外事例）

海外のセキュリティ人材育成システム

- 米国
  - NICE Cyber Workforce FW（NIST SP800-181）
    - 大統領令により、サイバーセキュリティの仕事に関する記述を共通化
  - CAE-C（Centers of Academic Excellence in Cybersecurity）
    - 米国教育機関のサイバーセキュリティに関する学位、認証を行なう教育機関に対する要件を定めて認定を行なうプログラム。
- 中国
  - World-Class Cybersecurity Schools (WCCS; 一流网络安全学院）を認定する政府プログラム
- EU
  - ENISA European Cybersecurity Skills Framework (ECSF)「欧州サイバーセキュリティ技能フレームワーク」
- UK
  - 英国サイバーセキュリティ評議会（The UK Cyber Security Council）が明確で一貫性のある専門家としての基準を設定
  - サイバーセキュリティ知識体系（CyBOK）の策定

米国内でのセキュリティ人材の育成

Learning and Employment Records


NIST Special Publication 800-181
Revision 1

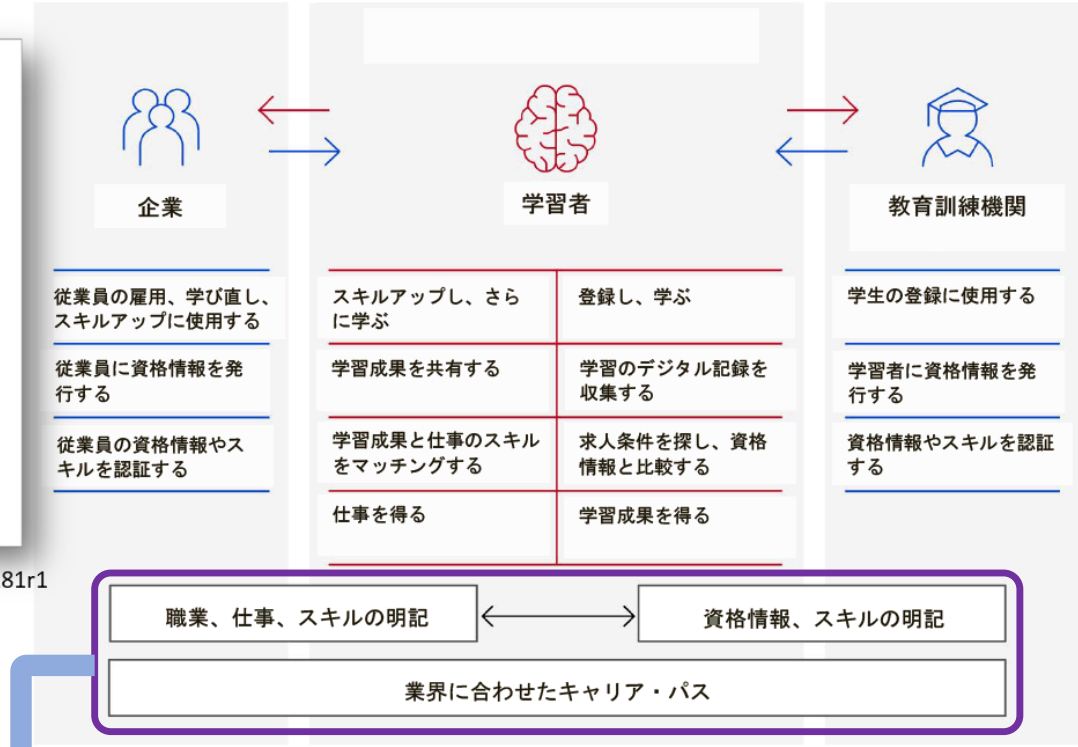
Workforce Framework
for Cybersecurity
(NICE Framework)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

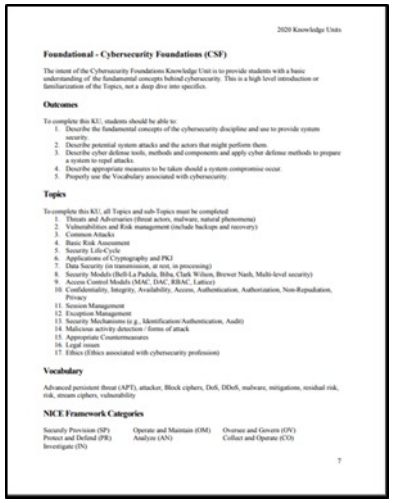
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

https://doi.org/10.6028/NIST.SP.800-181r1



資料出所　American Workforce Policy Advisory Board Digital Infrastructure Working Group(2020)「Learning and Employment Records: Progress and the path forward」をもとに厚生労働省政策統括官付政策統括室にて作成


2020 Knowledge Units

Foundational - Cybersecurity Foundations (CSF)

The intent of the Cybersecurity Foundations Knowledge Unit is to provide students with a basic understanding of the fundamental concepts behind cybersecurity. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.

Outcomes

To complete this KU, students should be able to:
1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security
2. Describe potential system attacks and the actors that might perform them.
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
4. Describe appropriate measures to be taken should a system compromise occur.
5. Properly use the Vocabulary associated with cybersecurity.

Topics

To complete this KU, all Topics and sub-Topics must be completed
1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle
6. Applications of Cryptography and PKI
7. Data Security (in transmission, at rest, in processing)
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
9. Access Control Models (MAC, DAC, RBAC, Lattice)
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Session Management
12. Exception Management
13. Security Mechanisms (e.g., Identification/Authentication, Audit)
14. Malicious activity detection / forms of attack
15. Appropriate Countermeasures
16. Legal issues
17. Ethics (Ethics associated with cybersecurity profession)

Vocabulary

Advanced persistent threat (APT), attacker, Block ciphers, DoS, DDoS, malware, mitigations, residual risk, risk, stream ciphers, vulnerability

NICE Framework Categories

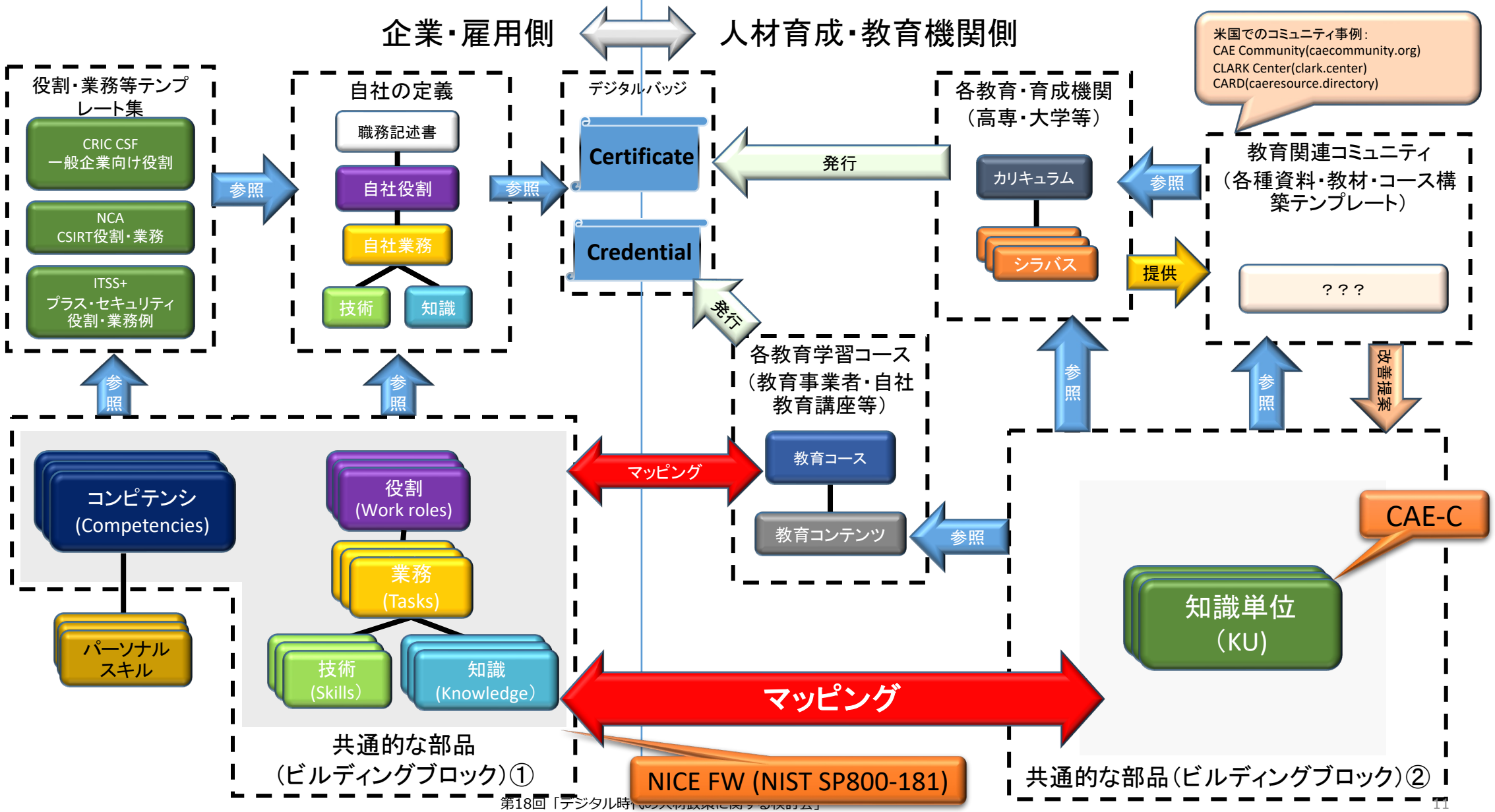
Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV)
Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO)
Investigate (IN)

7

https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

米国では、企業側と教育訓練機関との間の職業（職務）、資格情報、スキルなどは、NIST SP800-181とCAE CD_KUをマッピングすることで、ビルディングブロックを整備し、一貫したスキル管理をする記録システム。

サプライチェーンサイバーセキュリティコンソーシアムで検討されているビルディングブロックに基づく人材定義と人材育成



おわりに

- 生成AIとセキュリティ専門人材育成
  - セキュリティの広がり：DXセキュリティへ
  - 生成AIのセキュリティ専門人材育成への影響
- セキュリティ人材育成システム（海外事例）
  - 国・地域をまとめて、さらに進んだ施策の実施（米国、中国、EU、UK）
  - SC3「ビルディングブロックに基づく人材定義と人材育成」 検討

参考資料

米国のセキュリティ人材育成 ：NICE フレームワークとは？

米国 NIST ”サイバーセキュリティ教育のための国家イニシアティブ”（NICE: National Initiative for Cybersecurity Education ）が開発したフレームワーク

- サイバーセキュリティの仕事に関する記述を共通化
- 仕事を業務（タスク）として表現し、基礎を提供する知識（ナレッジ）と技術（スキル）を記述
  - 学生が何を学べば良いか
  - 求職者が就職するため必要な能力は何か
  - 従業員が業務遂行するために何ができれば良いか
- サイバーセキュリティの人材を特定、募集、開発、保持する方法のための一貫した共通言語とサイクルを支援

大統領令(Executive Order 13800 2017/5/11)を実現検討したレポートでは、米国商務省(DoC)と安全保障省（DHS）が NICE フレームワーク適用を以下のように提言している。

「民間と公共部門は、NICE NICEフレームワークを適用し、サイバーセキュリティキャリアモデルパスを開発し、サイバーセキュリティ人材開発教育、 訓練、人材開発プログラムおよびイニシアチブに関する情報のクリアリングハウスを確立することによって、教育と訓練を雇用主のサイバーセキュリティ人材ニーズに合わせるべきである。」

参照：https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure
https://www.cisa.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf

NICE フレームワークの変遷

SP800-181はR1に改訂され、SKAからTKSに変更され、さらにオーサーズガイドでその記述作法が明確になりリファクタリングが進行

2013年4月

最初の NICE FW

National Cybersecurity Workforce Framework version 1.0

2014年8月

バージョン 2.0 公開

National Cybersecurity Workforce Framework version 2.0

2017年8月

SP800-181発行

NIST Special Publication 800-181 : National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

2020年11月

SP800-181r1発行

改訂版 NIST Special Publication 800-181 Revision 1 : Workforce Framework for Cybersecurity (NICE Framework)

2021年4月

TKSオーサーズガイド発行

Task Knowledge Skill (TKS) Statements Authoring Guide for Workforce Frameworks

2021年12月

各種パブコメ

NICE Framework Data Update Process案

リファクタ版 NICE Framework Ability Statements案

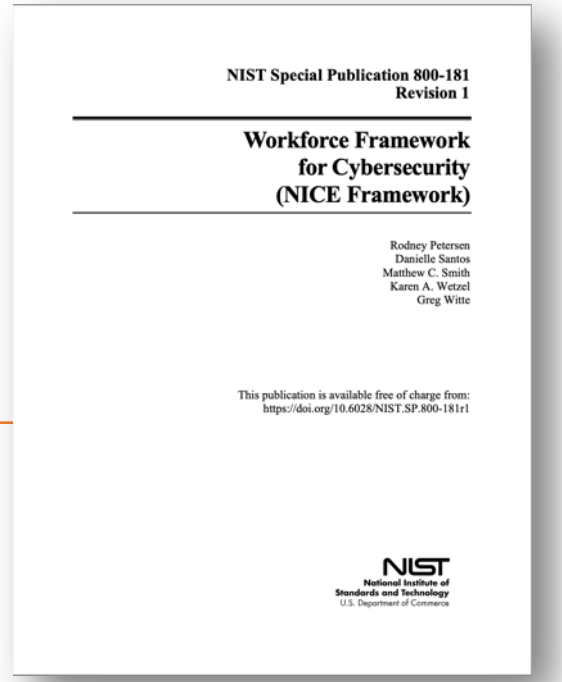
NICE Framework Competencies (NISTIR 8355) 第二版案

NICEフレームワークのマシン可読データ発行

2022年4月

リファクタ版KSパブコメ

リファクタ版 Knowledge and Skill statements


NIST Special Publication 800-181
Revision 1

Workforce Framework for Cybersecurity (NICE Framework)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

https://doi.org/10.6028/NIST.SP.800-181r1

誰のためのものか？

- 公共部門および民間部門
- 人的資源
- 採用担当者
- その他の中小企業

雇用者

EMPLOYERS

組織内の複数の職務に対して、採用からトレーニング、評価までの正規のプロセスを確立することができる。

- 学生
- 求職者
- 従業員

学習者

LEARNERS

仕事に関する明確な情報共有は、
- このキャリア分野に関心のある学生、
- 新しい仕事を探している人、
- 仕事の役割を変えようとしている人、
- 能力を発揮したり高めたりしようとしている労働者

などに役に立つ

- 学習プロセス
- 資格証明

教育・トレーニング提供者、資格プロバイダ

労働者が知っておくべきことに関する直接的な情報を提供し、学習者の能力を一貫して説明するための証明書、バッジ、その他の検証手法の開発に役立つ

NICEフレームワーク 構成要素：現在のそれぞれの数

SP800-181r1に改訂後、TKSステートメントの見直し中であり、コンピタンシについては、2ndドラフト検討中である。今後ワークロールも見直しされるため、この数値は今後変わると思われる。

仕事の役割を高いレベルで関連する領域に分類する方法。
「セキュリティの構築」、「運用と保守」、「監督と管理」、「保護と防御」、「分析」、「収集と運用」、「調査」などがある。

誰か責任者または説明責任者がいる仕事のまとまり。実施すべき仕事を構成するタスクで構成される。

組織が学習者を評価するための仕組み。仕事の領域を定義するTKSステートメントで構成されている。
仕事の役割に付随する場合もある。

実施すべき業務を定義

業務を完了するために、何を知っていなければならないかを定義

業務を完了するために、何 ができるようにならなければならな いかを定義

NICE フレームワークのビルディングブロック(構成要素)

業務（Tasks）の形で行うべき仕事と、知識(Knowledge)と技能(Skill)を通じてその仕事を遂行するために必要なものを記述

- 三つのビルディングブロック
  - 業務(Task statements)
  - 知識(Knowledge statements)
  - 技術(Skill statements)

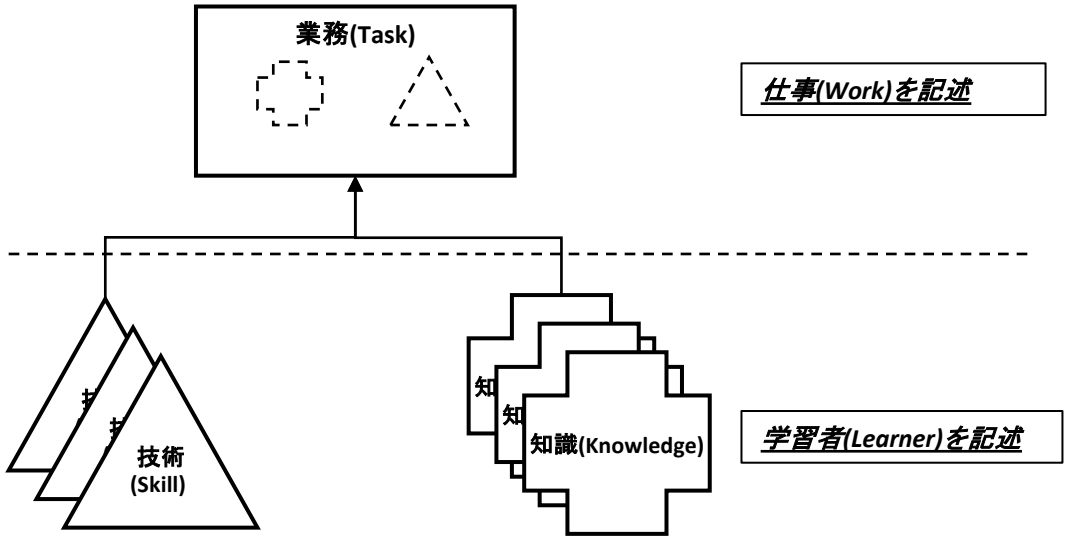


図1. NICEフレームワークのビルディングブロックス方式

ビルディングブロックアプリケーション

役割(Work Roles, 職務上任務)

- 業務をグループ化
- 誰かが責任を負う仕事

コンピテンシ(Competencies)

- 業務、知識、技術をグループ化
- 学習者の評価の仕組み

チーム(Teams)

- コンピテンシか役割で定義

三つのビルディングブロック：業務(Task statements)（1）

- 業務(Task)
  - ビジネス目標、技術目標、使命目標など、
    組織の目標の達成のために行なわれる活動として定義される。
- 業務ステートメント(Task statements)
  - 完了すべき作業を簡潔に記述する
  - 実行される活動から始まり、目的を含まない
    - 例えば、「インタラクティブなトレーニング演習を実施する。」という業務にある”演習の目的”は、「効果的な学習環境を作ること」かもしれないが、その目的は業務自体には含まれない。
  - 知識、技術 ステートメントと連携づけられる。
    - 関連する知識と技術を保有していることを示し、業務を行なえることを証明
    - 業務の準備として関連する知識を得て技術を学ぶ
- 業務ステートメントの修正
  - 業務ステートメントには、推奨される関連知識、技術ステートメントのセットを持っている。
  - ユーザーの独自の状況に合わせて業務をカスタマイズするために、それら以外の他の既存の知識と技術のステートメントを含めることができる。
  - 但し、相互運用性を支援するため、ユーザーは既存のNICEフレームワークTKSステートメントのテキストを修正しないようすべき。
  - ユーザー独自の状況をサポートするために、TKSステートメントに異なる文言が必要な場合は、新しいステートメントを作成する。
- 新しいステートメントの作成
  - ユーザーはNICEフレームワークを独自の状況下で使用するために、全く新しい課題、知識、スキルのステートメントを作成することができます。

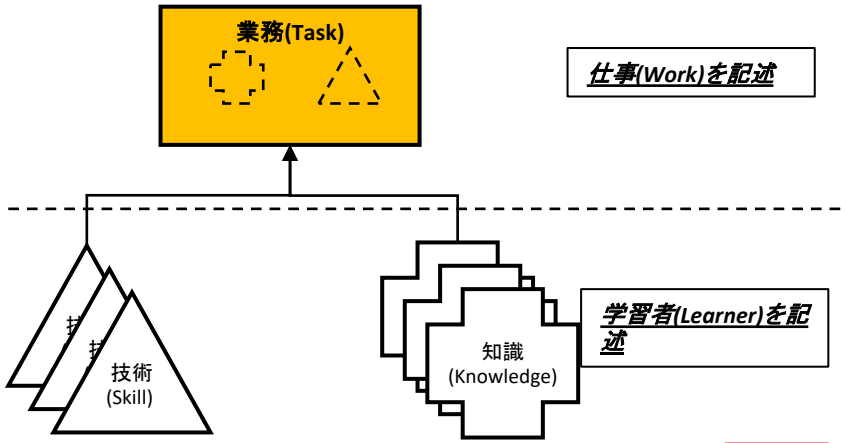


図1. NICEフレームワークのビルディングブロックス方式

再掲

三つのビルディングブロック：知識(Knowledge statements)（2）

- 知識(Knowledge)
  - 記憶の中にある取り出し可能な一連の概念として定義される。

- 知識ステートメント(Knowledge statements)
  - 基礎的な概念または特定の概念のいずれかを記述する
  - １つのタスクを記述するために、複数のステートメントが必要な場合がある
  - 同様に、１つの知識ステートメントを使用して、多くの異なるタスクを記述することができる

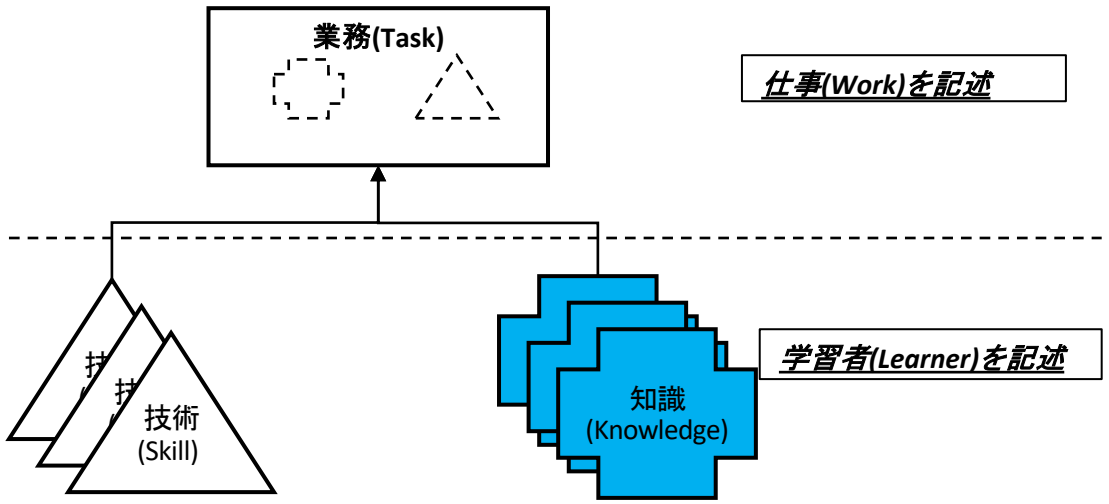


図1. NICEフレームワークのビルディングブロックス方式

再掲

三つのビルディングブロック：技術(Skill statements)（3）

- 技術(Skill)
  - 観察可能な動作/行動を実行する能力として定義される。
  - 説明されている技術を実証できない学習者は、その技術に依存する業務を完了する事が出来ない。
- 技術ステートメント(Skill statements)
  - 簡単な技術または複雑な技術を記述する
  - １つの業務を完了するために、複数の技術ステートメントが必要な場合がある
  - 同様に、1つの技術ステートメントで、複数の業務を完了することができる

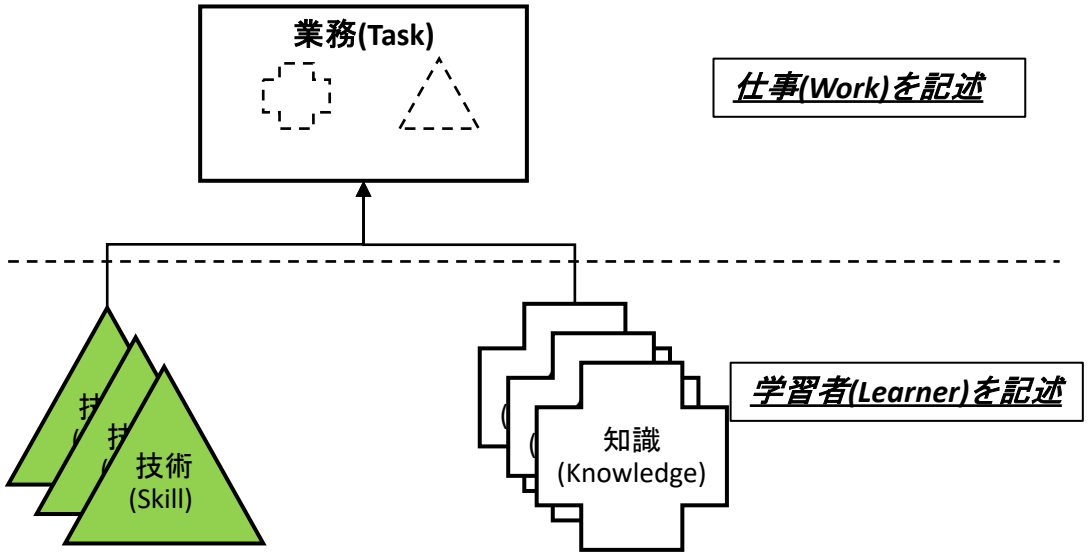


図1. NICEフレームワークのビルディングブロックス方式

再掲

役割(Work Roles, 職務上任務)

- 役割(Work Roles)とは
  - 誰かが責任や説明責任を負う仕事のグループ化を記述する方法
  - 実行すべき仕事を構成する業務で構成される。
    - 以前のNICE FWでは知識、スキル、能力(Abilities)と関連付けていたが、現在はタスクを通じてより俊敏なアプローチを推奨
  - 「役職名」と同義ではない。
  - 「職業」と同義ではない。
    - 組織の役職の使い方によっては、ワークロールが役職名と一致する場合もある。
    - 一つの「役割」（例：ソフトウェア開発者）が、さまざまな職種（例：ソフトウェアエンジニア、コーダー、アプリケーション開発者）の人に適用される場合がある。逆に、複数の役割を組み合わせて、特定の仕事を作ることもできる。
    - これは職場のすべての学習者が職種に関係なく、様々な役割で多くの業務を実行しているという実態に即している
  - 習熟度レベル（例：基礎、中級、上級）を定義していない。
    - このような属性や、学習者がタスクを実行する際の熟練度に関する属性は、他のモデルやリソースに委ねられている。

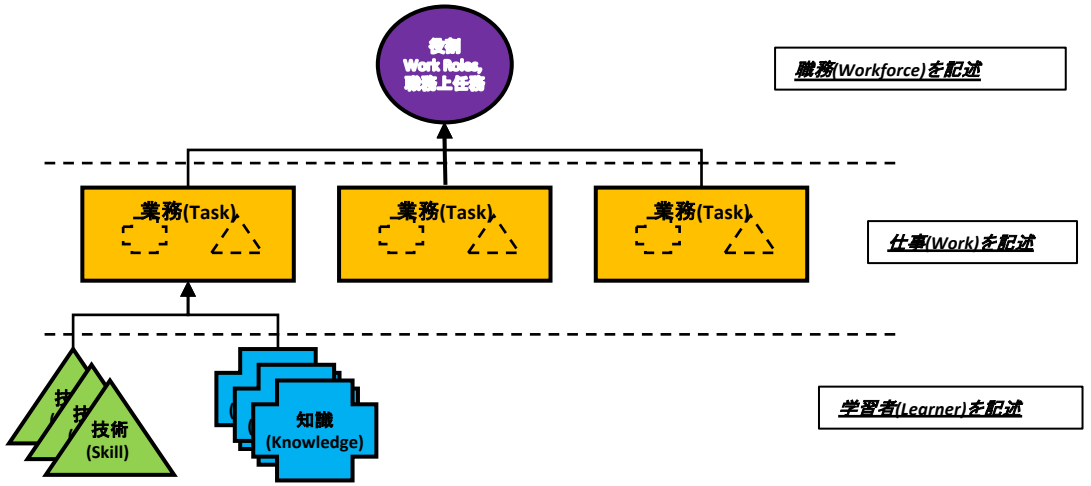
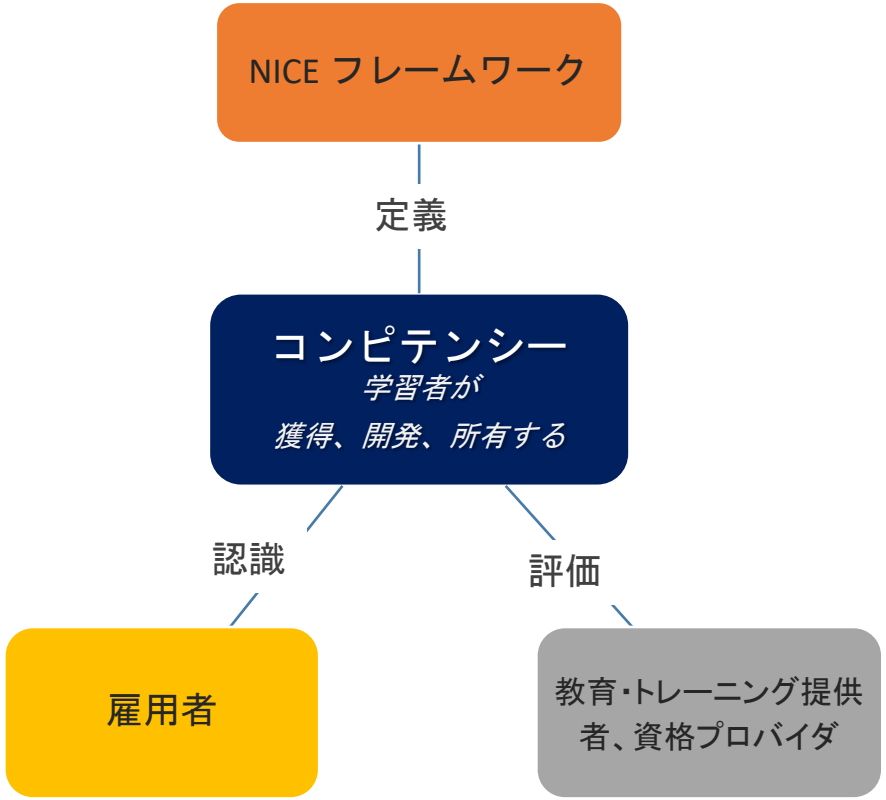


図 4 - 役割とビルディングブロックの関係

- 既存の「役割」の使用と新しい「役割」の作成
  - 「役割」は、業務を通じて組織の目標達成を支援することを目的としている。
  - ユーザの独自の状況に合わせて役割に他の既存のタスクを追加することができる。同様に、ユーザはリストアップされた「役割」を利用したり、追加の目的をサポートするために「役割」を追加することができる。
  - 但し、相互運用性のためユーザーは既存の「役割」の名前と説明を修正しないようにし、独自の文脈にそった「役割」が必要な場合、新しい「役割」として作成

コンピテンシ(Competencies)

- コンピテンシとは
  - 雇用者が組織独自の状況の見識から定義
  - 企業が学習者を評価するための仕組み
  - 組織（雇用側）が高いレベルで評価を記述
- 利点
  - セキュリティ業務を簡潔・整理した職務で表現
  - ニーズの変化に応じて、導入・修正可能
- 用途
  - 特定の職種におけるタスクの種類の説明
  - 従業員の能力を把握
  - 学習者の能力を実証



- ドラフト NIST Interagency or Internal Report（NISTIR）8355、"NICE Framework Competencies：Assessing Learners for Cybersecurity Work"（NICE Framework Competenciesとは何か、その進化と発展、例などの詳細を提供)
  https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8355-draft.pdf
- コンピタンスのリスト(ドラフト)
  https://csrc.nist.gov/CSRC/media/Publications/nistir/8355/draft/documents/draft_nice_competencies_mar2021.xlsx

コンピテンシ(Competencies)の利用例(1)

組織がコンピテンシーを特定の組織目標を達成するための採用プロセスの一部として使用する例

① コンピテンシーを関連する業務ステートメントのグループとして定義する。

② 組織は、これらのコンピテンシーを使用して、候補者がこれらのタスクを実行できるかどうかを評価する。

③ この評価は、面接、入社前試験、または業務上の学習観察という形をとることができる。

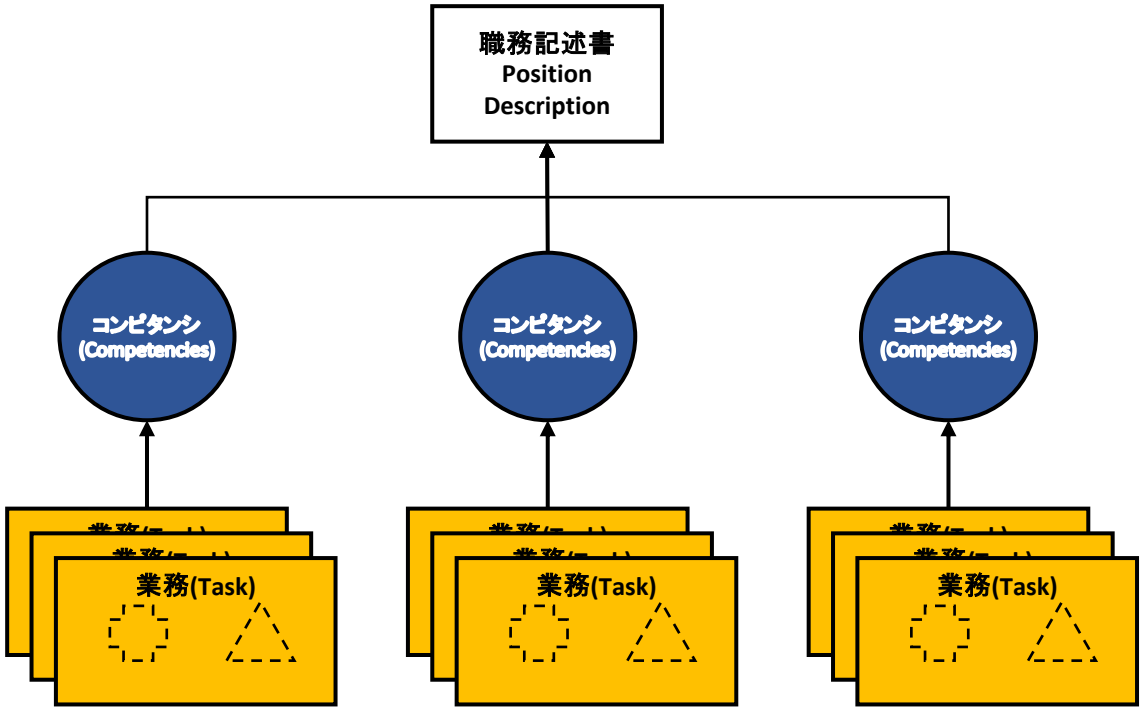


図 2. コンピテンシーを使用して、職務記述書を通じて学習者を評価する

コンピテンシ(Competencies)の利用例(2)

組織がコンピテンシーを学習者が定義されたスキルと知識のセットを達成したかどうかを判断するために使用する例

① コンピテンシーを知識、技術ステートメントのグループとして使用することを選択することができる。

② これらの 知識、技術ステートメントについて学習者を評価する。

③ 評価は、テスト、ラボでの実演、または口頭評価という形をとることができる。

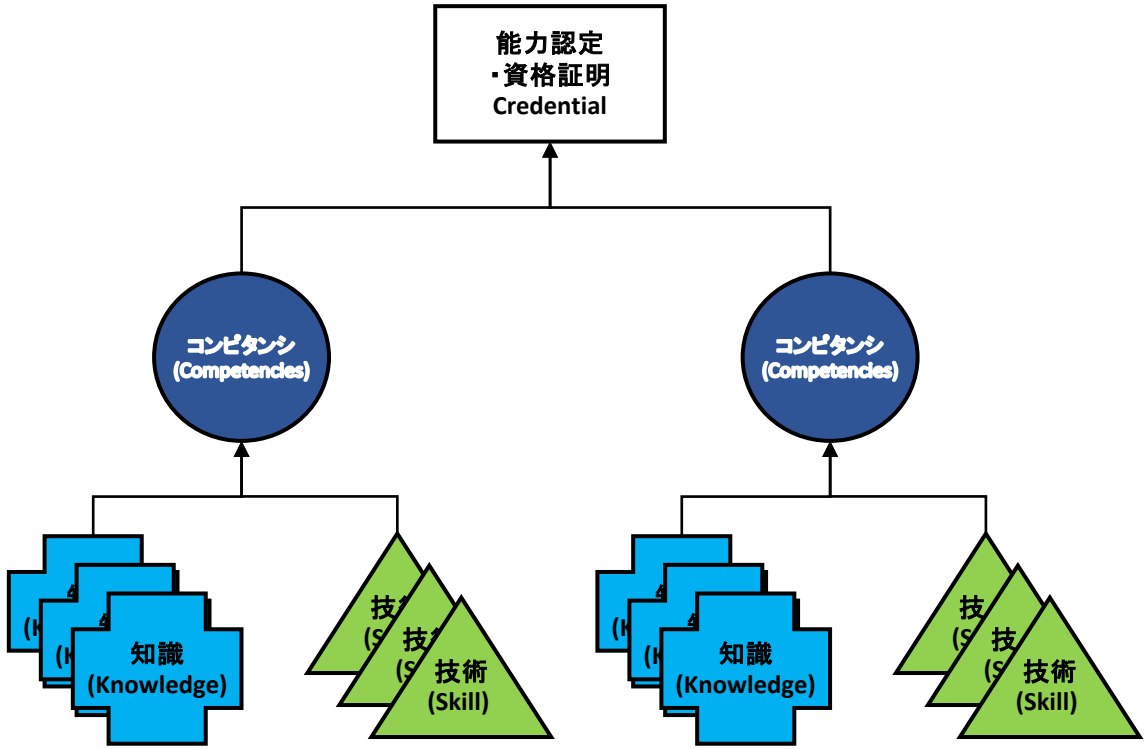


図 3.コンピテンシーを使用した、クレデンシャルによる学習者の評価

Centers of Academic Excellence in Cybersecurity (CAE-C) プログラム

参照：https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

- 目的
  - **米国教育機関のサイバーセキュリティに関する学位、認証を行なう教育機関に対する要件を定めて認定を行なうプログラム**。
  - これにより、サイバーディフェンスに関する人材育成の質の向上と、人材確保を容易にする。
- 概要
  - 米国家安全保障局（NSA） の National Cryptologic School によって管理されているプログラムで、米国のインフラの脆弱性を軽減するサイバーセキュリティの専門家を育成することを約束する教育機関に CAE-C の指定を与えている
    【CAE-CD（Cyber Defense)、CAE-R（Cyber Research)、CAE-CO（Cyber Operation)】
  - 教育機関が CAE-C の指定を受けるためには、NSAが定めた厳格な要件を満たすことが必要
    - CAE Cyber Defense (CAE-CD) Program Guidance - 2022
      - 準学士、学士、大学院レベルでサイバーセキュリティの学位や証明書を提供する地域公認の学術機関に与えられます。
      - サイバーデフェンスに関する高等教育や研究を推進し、有能なサイバーセキュリティ専門家の供給源となる教育機関であることを示す。
      - 対象教育機関：2年制、4年制、および大学院レベルの地域認定機関が申請資格を有している。
      - 指定維持の更新：5年ごとに再評価申請が必要
    - CAE Cyber Research (CAE-R) Program Guidance – 2022
      - 国への壊滅的なインシデントを予防し、それに対応することを可能にする強固なサイバー防衛技術、政策、実践をリサーチするものであることを示す。
      - 対象機関： DoDの学校、博士号を取得する陸軍士官学校、またはカーネギー財団基本分類システムによって博士課程大学-最高研究活動（R1）、博士課程大学-高研究活動（R2）、博士課程大学-中研究活動（R3）として評価されている地域認定され学位を授与する4年生教育機関
      - 指定維持の更新：5年ごとに再評価申請が必要
    - CAE Cyber Operations (CAE-CO) Program Guidance – 2022
      - サイバーセキュアな国家を支えることができる熟練労働者の層を広げるという目標を促進する。
      - コンピュータサイエンス、コンピュータエンジニアリング、および/または電気工学の分野にしっかりと根ざした深い技術、学際的、高等教育プログラムであり、ラボや演習を通じて実践的なアプリケーションのための豊富な機会を提供するものを示す。
      - 専門的なサイバー操作（例：収集、搾取、応答）に関連する技術とテクニックに重点を置き、これらの特殊な操作を行う権限を与えられた情報機関、軍事、法執行組織に必要な人材育成を志向している。

参照：https://public.cyber.mil/ncae-c/documents-library/

Centers of Academic Excellence in Cybersecurity (CAE-C) プログラム

知識単位名

知識要素

NICEとの関係

Cybersecurity Foundations (CSF)

The intent of the Cybersecurity Foundations Knowledge Unit is to provide students with a basic understanding of the fundamental concepts behind cybersecurity. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.

Outcomes

To complete this KU, students should be able to:

1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
2. Describe potential system attacks and the actors that might perform them.
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
4. Describe appropriate measures to be taken should a system compromise occur.
5. Properly use the Vocabulary associated with cybersecurity.

Topics

To complete this KU, all Topics and sub-Topics must be completed

1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle
6. Applications of Cryptography and PKI
7. Data Security (in transmission, at rest, in processing)
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
9. Access Control Models (MAC, DAC, RBAC, Lattice)
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Session Management
12. Exception Management
13. Security Mechanisms (e.g., Identification/Authentication, Audit)
14. Malicious activity detection / forms of attack
15. Appropriate Countermeasures
16. Legal issues
17. Ethics (Ethics associated with cybersecurity profession)

Vocabulary

Advanced persistent threat (APT), attacker, Block ciphers, DoS, DDoS, malware, mitigations, residual risk, risk, stream ciphers, vulnerability

NICE Framework Categories

Securely Provision (SP) Operate and Maintain (OM) Oversee and Govern (OV)
Protect and Defend (PR) Analyze (AN) Collect and Operate (CO)
Investigate (IN)

KU 知識単位は全69個

Foundational KU's [3]
- Foundational - Cybersecurity Foundations (CSF)
- Foundational- Cybersecurity Principles (CSP)
- Foundational - IT Systems Components (ISC)

Technical Core KUs [5]
- Technical Core - Basic Cryptography (BCY)
- Technical Core - Basic Networking (BNW)
- Technical Core - Basic Scripting and Programming (BSP)
- Technical Core - Network Defense (NDF)
- Technical Core - Operating Systems Concepts (OSC)

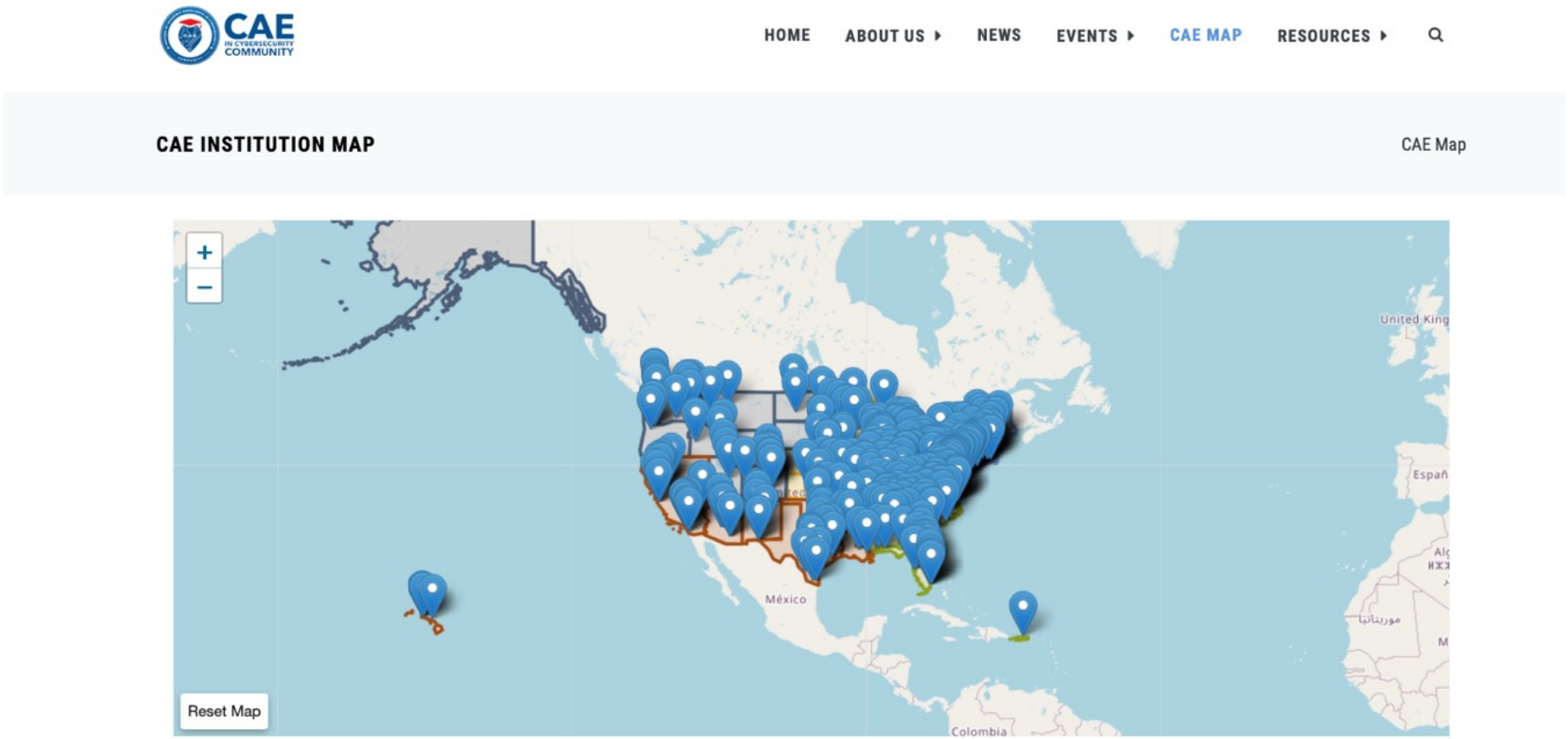
Non-Technical Core KUs [5]
- Non-Technical Core - Cyber Threats (CTH)
- Non-Technical Core - Cybersecurity Planning and Management (CPM)
- Non-Technical Core - Policy, Legal, Ethics, and Compliance (PLE)
- Non-Technical Core - Security Program Management (SPM)
- Non-Technical Core - Security Risk Analysis (SRA)

Optional KU's [56]
- Advanced Algorithms (AAL)
- Advanced Cryptography (ACR)
- Advanced Network Technology and Protocols (ANT)
- Algorithms (ALG)
- Analog Telecommunications (ATC)
- Basic Cyber Operations (BCO)
- Cloud Computing (CCO)
- Cyber Crime (CCR)
- Cybersecurity Ethics (CSE)
- Data Administration (DBA)
- Data Structures (DST)
- Database Management Systems (DMS)
- Databases (DAT)
- Device Forensics (DVF)
- Digital Communications (DCO)
- Digital Forensics (DFS)
- Embedded Systems (EBS)
- Forensic Accounting (FAC)
- Formal Methods (FMD)
- Fraud Prevention and Management (FPM)
- Hardware Reverse Engineering (HRE)
- Hardware/Firmware Security (HFS)Host Forensics (HOF)
- IA Architectures (IAA)
- IA Compliance (IAC)
- IA Standards (IAS)
- Independent/Directed Study/Research (IDR)
- Industrial Control Systems (ICS)
- Introduction to Theory of Computation (ITC)
- Intrusion Detection/Prevention Systems (IDS)
- Life-Cycle Security (LCS)
- Low Level Programming (LLP)
- Media Forensics (MEF)
- Mobile Technologies (MOT)
- Network Forensics (NWF)
- Network Security Administration (NSA)
- Network Technology and Protocols (NTP)
- Operating Systems Administration (OSA)
- Operating Systems Hardening (OSH)
- Operating Systems Theory (OST)
- Penetration Testing (PTT)
- Privacy (PRI)
- QA/Functional Testing (QAT)
- Radio Frequency Principles (RFP)
- Secure Programming Practices (SPP)
- Software Assurance (SAS)
- Software Reverse Engineering (SRE)
- Software Security Analysis (SSA)
- Supply Chain Security (SCS)
- Systems Certification and Accreditation (SCA)
- Systems Programming (SPG)
- Systems Security Engineering (SSE)
- Virtualization Technologies (VTT)
- Vulnerability Analysis (VLA)
- Web Application Security (WAS)
- Wireless Sensor Networks (WSN)

Centers of Academic Excellence in Cybersecurity (CAE-C) プログラム

参照：https://www.caecommunity.org/cae-map

- 概要（続き）
  - NSAの他、以下の米国省庁が一緒に支援を行なっている
    - サイバーセキュリティおよびインフラセキュリティ局（CISA）、連邦捜査局（FBI）、国立標準技術研究所（NIST）/サイバーセキュリティ教育に関する国家イニシアチブ（NICE）、国立科学財団（NSF）、国防総省最高情報責任者室（DoD-CIA）、米国サイバー軍（USCYBERCOM）
  - 現状の指定校



Centers of Academic Excellence in Cybersecurity (CAE-C) プログラム

参照：https://public.cyber.mil/ncae-c/documents-library/

- Program of Study(PoS)検証のコンセプトモデル
  - （CAE Cyber Defense (CAE-CD) Program Guidance – 2022 より）
  - 各教育機関で設置されるサイバーセキュリティの教育が、CAE-C のKU Alignmentしているかどうかを検証（Validation）するための仕組みで、各教育機関は学位授与、サーティフィケート修了などを認めるに至る要件として、以下のような要素を定義したPoSを作成する。
    - プログラムレベルの学習効果(Program-Level Learning)
    - プログラム成果評価指標（A program outcome assessment indicator/ assessment metric)
    - カリキュラムマップとプラン(Curriculum Map and Plan)
  - 各教育機関はPoSに定義された各コースがどのようにKUに沿っているか(alignment)を示した KU Alignment を提示し、CAE-C へのValidationを受けることになる。全体のコンセプトを示しているのが、図3 PoS Validation Conceptual Model

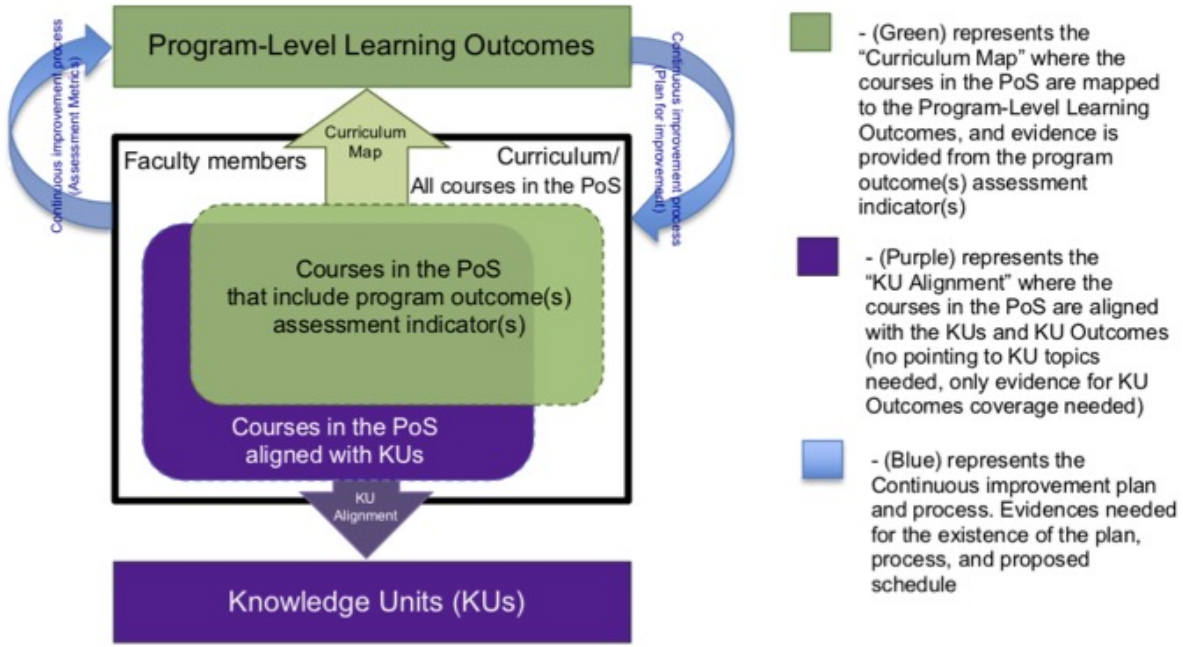


Figure 3. PoS Validation Conceptual Model

Centers of Academic Excellence in Cybersecurity (CAE-C) プログラム

参照：https://public.cyber.mil/ncae-c/documents-library/

- Knowledge Unitについて
  - （ CAE-CD Knowledge Units より）
  - CAE-CD 指定を受ける際には、NCAE-Cの知識単位(KU)に合わせ、教育機関で提供するカリキュラム・マップと計画を提供しなければならない。
  - コースまたはその他の教育要素は、機関認定の要件に従って機関承認され、KU に整合させる必要がある

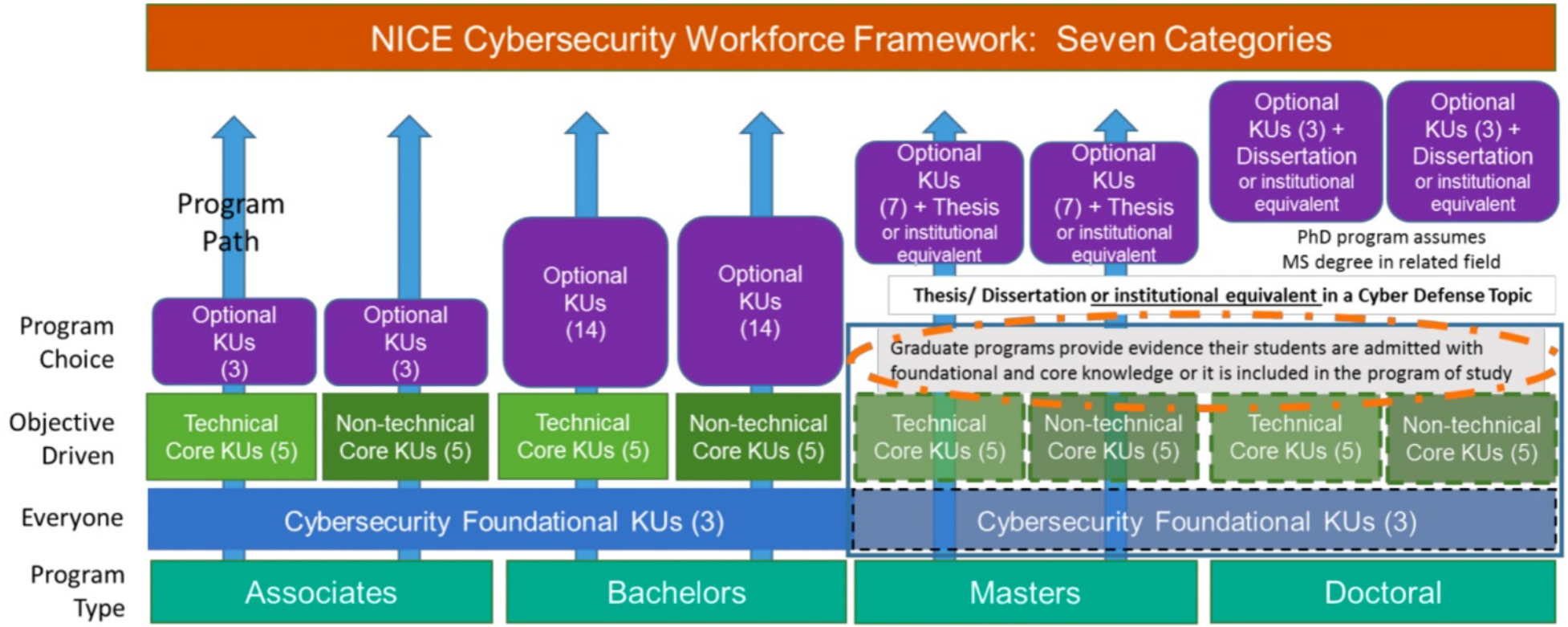


Figure 4. CAE-CD Knowledge Units Alignment Requirements

中国のサイバーセキュリティとAIの人材育成 ：「WCCS 一流网络安全学院」

米国ジョージタウン大学のレポート "China's CyberAI Talent Pipeline" より

https://cset.georgetown.edu/wp-content/uploads/Chinas-CyberAI-Talent-Pipeline.pdf

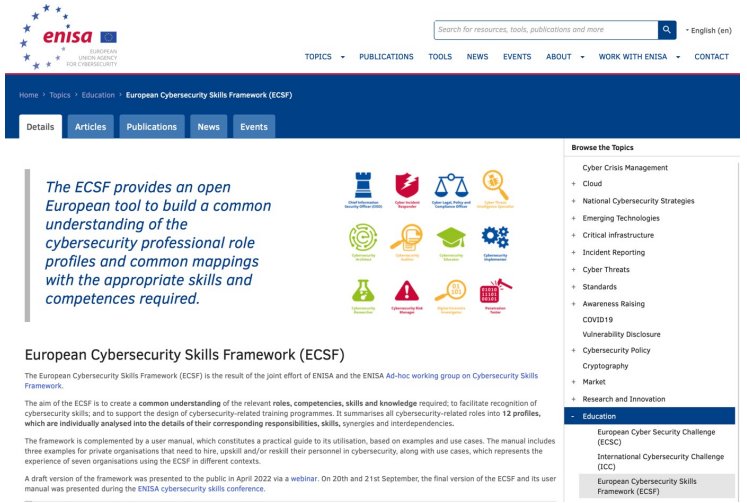
- 2016年 中国 国家サイバーセキュリティ戦略
  - 人材パイプラインを改善するための重要な要素として、サイバーセキュリティの学位プログラムの標準化を記述
- 2017年 World-Class Cybersecurity Schools（WCCS; 一流网络安全学院）を認定する政府プログラムを開始
  - 教育省と中国サイバー空間管理局（CAC）は、11大学をWCCSに指定
  - 米国CAE-Cと同様に、サイバーセキュリティ教育の卓越した基準を設定し、国のサイバーセキュリティ分野の人材プールを強化することが目的
- サイバーセキュリティの学位プログラムにAIやMLに関する授業の組込
  - 米国のCAE-Cyber Operations学位*1よりも多くの人工知能/機械学習（AI/ML）のコースを提供（WCCS11大学のうち8大学 CAE-CO認定大学20校のうち1校がMLの選択授業を設置）
- 2020年4月 全米科学財団（NSF）がAI研究をサイバーセキュリティの学位に統合する方法を探る研究の提案募集を実施*2
  - NSF研究助成を受けた13プロジェクトがAIとサイバーセキュリティの両方のスキルを学部生や大学院生に教えることを目的としたパイロットプログラムを実施
- CAE資格取得に必要な知識ユニットを見直しを推奨
  - 本レポートでは、13のNSF研究助成プロジェクトの結果を元にCAE-KUを見直すことを推奨し、サイバーセキュリティ教育における卓越した基準を更新すべきとしている。

Institution's Name in English	Institution's Name in Chinese
Xidian University	西安电子科技大学
Wuhan University	武汉大学
Beijing University of Aeronautics and Astronautics (Beihang University)	北京航空航天大学
University of Science and Technology of China	中国科学技术大学
PLA Strategic Support Force Information Engineering University	中国人民解放军战略支援部队信息工程大学
Huazhong University of Science and Technology	华中科技大学
Beijing University of Posts and Telecommunications	北京邮电大学
Shandong University	山东大学
Sichuan University	四川大学
Southeast University	东南大学
Shanghai Jiao Tong University	上海交通大学

*1) このレポートでは比較対象としてCAE-COを選択している。
*2) https://www.nsf.gov/pubs/2020/nsf20072/nsf20072.jsp

ENISA European Cybersecurity Skills Framework (ECSF)「欧州サイバーセキュリティ技能フレームワーク」

- 目的
  - 必要とされる関連する役割、能力、スキル、知識についての共通理解
  - サイバーセキュリティ・スキルに対する認知促進
  - サイバーセキュリティ関連の研修プログラムの設計を支援
- フレームワーク
  - すべてのサイバーセキュリティ関連の役割を12のプロファイルに
  - 個別に対応する責任、スキル、相乗効果、相互依存性の詳細を分析
- ユーザーマニュアルにより補完
  - 例やユースケースに基づいた活用のための実践的なガイド
  - サイバーセキュリティの分野での民間組織向けの3つの事例：人材の雇用、スキルアップ、再スキル
  - 異なる状況でECSFを使用した7つの組織の使用事例
- 目標
  - EU 全体のサイバーセキュリティ専門家の需要（職場、採用）と供給（資格、訓練）の間に共通の用語と共通の理解を得ること
  - 労働力の観点から必要とされる重要なスキルセットの特定を支援し、学習プログラムの提供者はこの重要なスキルセットの開発を支援することができる。政策立案者は、特定されたスキルのギャップを緩和するために的を絞った取り組みを支援することができる。
  - 主要なサイバーセキュリティ専門家の役割と、ソフトスキルを含む必要不可欠なスキル、さらに（もしあれば）法的側面についての理解を促進する。特に、専門家でない人や人事部門が、サイバーセキュリティをサポートするためのリソース計画、採用、キャリアプランニングの要件を理解することを可能にする。
  - サイバーセキュリティの教育、トレーニング、人材開発における調和を促進する。サイバーセキュリティのスキルと役割の文脈におけるこの欧州の共通言語としてICT専門家領域全体でうまく連携できる。
  - サイバー攻撃に対する防護強化の達成と、社会における安全なITシステムの確立に貢献する。また、欧州のサイバーセキュリティ人材における能力開発を実施する方法について、標準的な構造と助言を提供する。

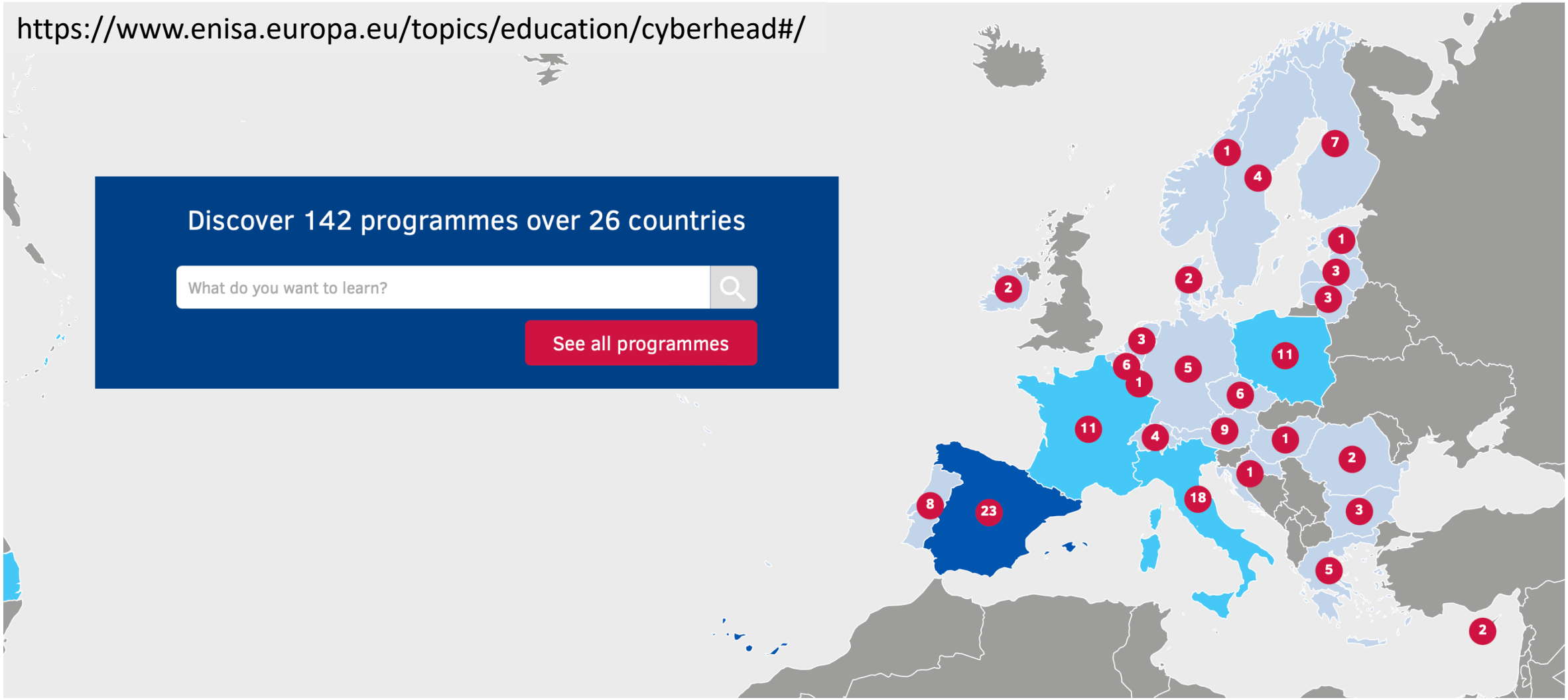


https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Cybersecurity Higher Education Database (CyberHEAD)

EUおよびEFTA諸国におけるサイバーセキュリティ高等教育データベース

https://www.enisa.europa.eu/topics/education/cyberhead#/



UKにおけるサイバーセキュリティのスキルギャップ解消の取組

- サイバーセキュリティ分野への新規参入者を奨励するもの
  - CyberFirst奨学金制度
    - 学部生を支援し、毎年何百人もの人材を実務経験とともにサイバー人材を創出
  - CyberFirstとDiscovery programmeは、過去 5 年間で 11～17 歳人材を約 30 万人動員
  - 4 つのサイバー見習い資格
  - DfE の「Courses for Jobs」イニシアティブによる初期学習向け 3 つのサイバー教育
  - 国家技能基金（National Skills Fund）による9つのサイバー・ブートキャンプが支援

UKにおけるサイバーセキュリティのスキルギャップ解消の取組

- サイバーセキュリティ人材の専門化
  - 英国サイバーセキュリティ評議会（The UK Cyber Security Council）が明確で一貫性のある専門家としての基準を設定
    - Career Maaping Tool
      - サイバーセキュリティの様々な知識分野を通して、学習者のスキルや興味が現在どこにあり、どのような専門分野が最も適しているかを評価
    - Cyber Career Framework
      - 16種類のサイバーセキュリティ専門職に関する定義や詳細情報を提供
    - Certification Framewrok Tool
      - さまざまな専門分野の中で、キャリアのどの時点で、どの資格が役に立つかを確認することができる枠組み
    - Training and Qualifications
      - サイバーセキュリティには、見習い、学位、オンライン学習、ブートキャンプなど、幅広いエントリールートの提供
  - サイバーセキュリティ知識体系（CyBOK）

サイバー組織（ロケーションは概略です）

英国サイバークラスター

1. ブリストル&バース・サイバー
2. サイバー・ノース
3. サイバー・ウェールズ
4. CyNam（サイバー・チェルトナム）
5. イーストオブイングランド・サイバーセキュリティクラスター
6. ミッドランズ・サイバー
7. スコットランドIS・サイバー
8. サウスウェスト・サイバーセキュリティクラスター
9. ヨークシャー・サイバーセキュリティクラスター
10. NIサイバー（北アイルランド）
11. ノースウェスト・サイバーセキュリティクラスター
12. ウェストオブイングランド・サイバークラスター

- サイバーセキュリティ教育（CSE）分野の卓越研究センター（ACE）
- サイバーセキュリティ研究（CSR）分野のチェンジ卓越研究センター（ACE）*
- GCHQ / NCSCの拠点
- 自治政府の組織

* 赤い点と黒い線の組み合わせは、CSEとCSRの両ステータスをもつことを意味する

1 ノースイースト・ビジネスレジリエンスセンター
2 ノースウェスト・サイバーレジリエンスセンター
3 イーストミッドランド・サイバーレジリエンスセンター
4 ウェストミッドランド・サイバーレジリエンスセンター
5 サウスイースト・サイバーレジリエンスセンター
6 サウスウェスト・サイバーレジリエンスセンター
7 ウェールズ・サイバーレジリエンスセンター
8 イースタン・サイバーレジリエンスセンター
9 ロンドン・サイバーレジリエンスセンター