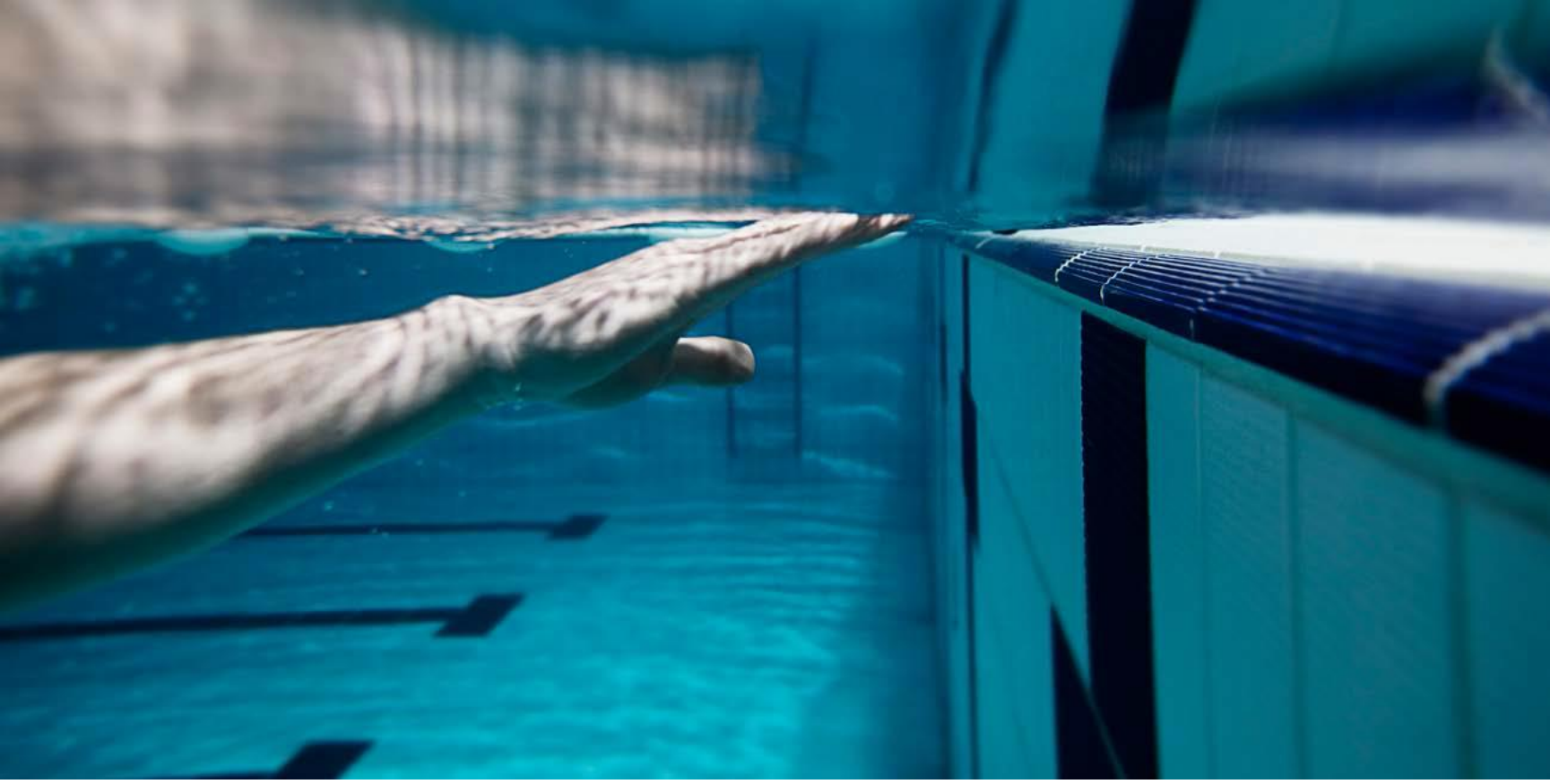


どこから始めるかではなく、どう終わらせるか

新しいカラー（「ニューカラー」）へのアプローチでサイバー・セキュリティーのスキル・ギャップに対応する

IBM Institute for Business Value

エグゼクティブ・レポート
セキュリティー

IBM をお勧めする理由

サイバー犯罪という脅威が気付かぬうちに危機的レベルに達しています。正確な数字を出すのは困難ですが、世界経済に及ぼすコストは、1 年当たり 3,750 億米ドル (1 ドル 120 円換算で約 45 兆円) から 5,750 億米ドル (同 69 兆円) に及ぶと推計されます。[1] 影響を免れる地域や業界は存在しません。IBM の広範な統合ポートフォリオは、企業がコグニティブ、クラウドおよびコラボレーションのテクノロジーに最新のものを取り込み、統合されたインテリジェントなセキュリティー免疫システムで脅威の機先を制するのに役立ちます。

IBM セキュリティーの最新の洞察を得るには、**ibm.com**/security/ciso をご覧ください。

サイバー・セキュリティー人材に関する新しいアプローチ

サイバー・セキュリティーの専門家の需要は高く、人材は不足している状態が続いています。企業は短期的にも長期的にも、人材の不足を補おうとさまざまな方法を模索しています。それらには新しい大学プログラム、技術訓練や職業プログラム、実習、認定、早期教育、そして政府主催のプログラムなどがあげられます。多くのサイバー・セキュリティーの仕事は、従来の大学の学位はなくとも必要な技術スキルと適性を備えた専門家を活用するという、「ニュー・カラー」へのアプローチでギャップを埋めることができます。

このアプローチを検討するために、IBM をケース・スタディーとして取り上げ、どのように進めるかを見てみましょう。

スキル・ギャップの状態

組織は、その人材で良さが決まります。サイバー・セキュリティーのリーダーにとって、技術とビジネスの最高の専門家を採用し定着させるという難題は、いつまでも続く心配事です。Frost & Sullivan は、必要にもかかわらず不足している有能なサイバー・セキュリティー専門家は 2022 年までに 180 万人に達すると予測しています。[2] また、多くのリーダーが、人材不足に関して十分な対策が行われていないと思っています。Center for Strategic and International Studies および Intel Security のレポートによると、調査したセキュリティー専門家の 4 人の内 3 人は、政府がサイバー・セキュリティーの人材に十分に投資していないと考えています。[3] このサイバー・セキュリティーの人材問題は、一部の領域に限られたことではありません。政府から教育機関、産業界の全体にわたっています。

上記数字で見る課題は現実のものとなっています。政府、産業界、教育機関が問題に対処しようとしているにもかかわらず、人材のサプライ・チェーン全体が圧迫されています。産業界は必要な実践スキルや製品経験のある有能な人材不足に直面しています。現在セキュリティー専門家として働いている人たちは、進化する技術や脅威の状況についていくために継続的に訓練や専門知識の開発を行う必要があるために、常に重圧を感じています。彼らは新規採用者を適切に指導や訓練する時間を見つけなければならないという難題も抱えています。学術機関は産業界のニーズに応えたいと思っていますが、産業界の変化や技術の進歩に合わせてカリキュラムを発展させるのに苦闘しています。大学とコミュニティー・カレッジでも、有能な教師や教授が不足しており、その多くは高い給料で産業界に引き抜かれていきます。そして、サイバー・セキュリティーの分野に興味を持つ学生は、数え切れないほどの選択肢からのキャリア・パスの決定と、重要な教育や必要な経験の取得という現実を突きつけられています。

ギャップ

不足しているサイバー・セキュリティーの職位が 2022 年までに 180 万人になるといわれています。[4]

概念

「ニュー・カラー」アプローチは、サイバー・セキュリティーを提供する約 300 の米国のコミュニティー・カレッジも含め、新しいプロファイル、職務、パートナーシップにフォーカスします。[5]

青写真

組織が行える 5 つのステップにより、新人を採用し、現在の米国にいる 770,000 人のサイバー・セキュリティー担当者を定着させることができます。[6]

障害物は乗り越えられないように見えるかもしれませんが、大きな困難は大きなアクションと創造性を生み出すものです。ギャップに対処するために、公共および民間の両方の組織が、すべてのレベルでの次世代のサイバー・セキュリティーの専門家の教育と育成を多くのアプローチで試行しています。以下のようなものです。

新しい教育プログラムの作成

- 米国での Pathways in Technology Early College High School (P-TECH) や英国の National College of Cybersecurity のような新しい教育モデルの検討。[7]
- コミュニティー・カレッジ、職業教育機関、技術専門学校やキャリア・センターでのプログラムのサポート (例えば、Community College Cyber Summit など)。[8]
- 中等学校、高校での早期教育プログラムの推進 (例えば Hacker Highschool)。[9]

従来型のクラスルームの枠を超えて

- 実習制度、研修プログラム、インターンシップの確立 (例えば、ApprenticeshipUSA など)。[10]
- 認定プログラムの強化と、教育プログラムへの組み込み。CompTIA Security+ 認定、Certified Information Systems Security Professional (CISSP) 認定、Certified Ethical Hacker (CEH) 認定が例として挙げられます。[11]
- コード・スクールやブート・キャンプの活用
- CyberPatriot や CyberTitan のようなクラブや競技会の後援。[12]

つながりの構築と情報の共有

- より良いコラボレーションの促進と、学生/教育者/産業界向けのツールの開発 (例えば、CyberSeek や TechHire)。[13]
- International Consortium of Minority Cybersecurity Professionals (ICMCP)、Hire our Heroes、Women's Society of Cyberjutsu、Women in CyberSecurity (WiCyS) などの会議や組織をとおして、十分に評価されていないグループを積極的に採用する。[14]

コースのナビゲート: ニュー・カラーのアプローチ

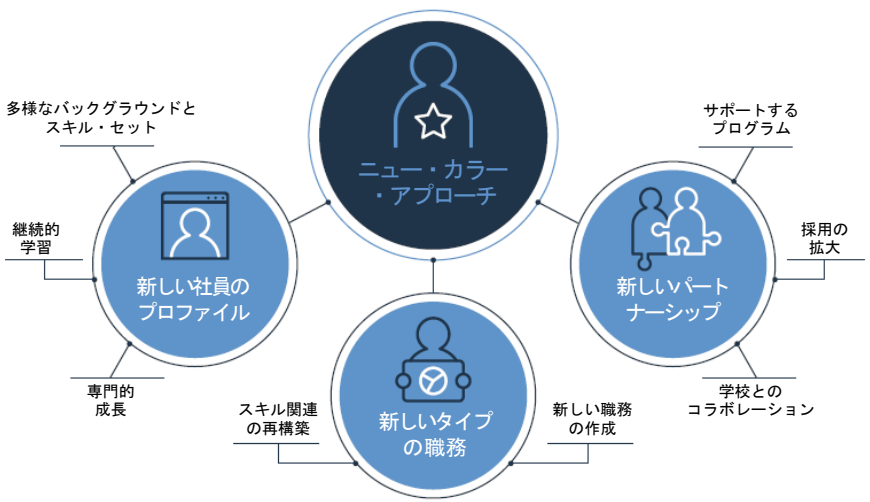
通常どんな業界でも、人材不足に直面するときの対処方法は主に 3 つあります。第 1 は、新しい運用モデルを参考にして、*仕事をする方法を変える*ことです。これは自動化の推進を含む場合もあれば、ある種のアウトソーシングやマネージド・サービス・プロバイダーの活用を意味する場合もあります。スキル・ギャップを解決する従来型の第 2 の方法は、*環境を変える*ことです。限られたリソースを惹きつけるには、差別化が必要です。挑戦、文化、報酬、または特典といった視点から、企業を最も望ましい場所にするのです。第 3 の方法は、*企業が求める対象者を変えて*、候補者の供給ルートを開くことです。

これらの手法のどれか 1 つだけでは、サイバー・セキュリティーのスキル・ギャップを埋めることになりません。むしろ、その組み合わせが進化を続けていくことになるでしょう。IBM を含めて多くの企業は、新しいテクノロジーがどのようにセキュリティー実践者のスキルを強化して働き方を変えるかに注目しており、十分に評価されていない人材のソースを新しいタイプの仕事に活用するために、人材の供給ルートへのフォーカスを一新しています。[15] これが「ニュー・カラー」アプローチの礎石であり、サイバー・セキュリティーのスキル・ギャップに対処するのに必要な戦略全体の主要なコンポーネントです。このアプローチには以下のものが含まれます。

新しい社員のプロファイル — ニュー・カラー・アプローチは、多様なバックグラウンドとスキル・セットを持つ、これまでとは違う候補者(学位を取得しているかではなく)を見つけて惹きつけるための前提条件として、スキルにフォーカスします。これらの新しい社員は、採用されると、継続的な学習と専門的な成長に励むことが期待されます。

新しいタイプの職務 — 出現しつつあるテクノロジーにフォーカスする新しい職務には、特定のスキルと実行のための知識が必要であり、大学の学位は必ずしも必要ではないという認識が広まってきています。このアプローチには、特定のスキル・セットに関連する仕事を再構築して新しい職務を作ることも含まれます。

新しいパートナーシップ — ニュー・カラー・アプローチを行うには、働きかけて新しい関係を構築することが必要になります。これには、連邦政府や州政府のプログラムの活用とサポート、コミュニティー・カレッジ・プログラムでの採用の拡大、幼稚園から高校までの学校プログラムやサイバー競技会との連携、退役軍人の訓練プログラムとのリンクなどが含まれます。



「ニュー・カラーの概念は、私たちが Hacker Highschool で何年も前からわかっていたことを認識しています。この分野で成功するために必要なことは、学習意欲と、基本的なコンピューターやネットワークのスキルへの適性がすべてです。」

Chris Griffin、侵入テスター、IBM X-Force Red、Hacker Highschool のボランティア

競争のためのトレーニング: スキルがすべて

スキルはニュー・カラー・アプローチの中心であり、スキルへのフォーカスを一新することが必要です。スキルの不足はサイバー・セキュリティーの人材の不足に限らず、産業界と教育機関の両方が労働力のスキル全般の不足に直面しています。最近の IBM Institute for Business Value による調査「Facing the storm: Navigating the global skills crisis」では、調査したエグゼクティブの大多数が、急速な技術の進歩に直面して、労働力のスキルを最新に保つのに苦闘していることが明らかになりました。[16] 彼らは国の教育システムと民間企業の両方を非難しています。調査したエグゼクティブの 55 パーセントは、自分の国の教育システムは生涯にわたる学習とスキル開発を促進するのに十分なことを行っていないと言っており、同じパーセントが産業界からの投資が不十分なことがこの問題の最も基本的な課題であると指摘しています。[17]

新しいサイバー・セキュリティーの専門家は何のスキルにフォーカスするべきでしょうか? 専門家の教育のバックグラウンドにかかわらず、不可欠な要素がいくつかあります。これらの要素は、2 つのグループに分類できます。中核属性とスキルです (図 1 を参照)。中核属性はセキュリティー専門家にとって有益な素質全般、つまり一般的な性格の特性と学習行動のセットと見なすことができます。スキルには技術と職場関係の能力の両方が含まれます。新しいセキュリティー専門家は最初はこれらのスキルすべてを持っていないかもしれませんが、時間をかけてこれらにフォーカスすることにより、キャリア・パスの柔軟性が広がり、技術またはビジネスにフォーカスしたリーダーの地位の基盤ができます。

図 1

サイバー・セキュリティー専門家: 中核属性とスキル

					
中核属性	調査者	問題解決者	学生	管理者	コンサルタント
	調査好きで課題を楽しむ	分析的で秩序立っており、詳細指向	常に学習	保護的、倫理的で信頼できる	他の人の問題を理解して解決するために協力できる
スキル 	シナリオ、リスク、「仮定した場合」の本質的な理解	検証可能な実践経験とリファレンス、認定、および/またはマイクロ資格 構築方法を見い出し物事を分析するための、コーディングへの精通とある程度の能力	特定の業界の知識 新規および出現しつつあるセキュリティー技術に適応する能力	適用可能な規則、法律、ポリシーへの精通と、それらを解釈する能力	動的で多様なチームで働く能力 効果的なコミュニケーション・スキル — 複雑な概念を明確に表現して技術的な問題をわかりやすく説明する 他の人への教育の経験

「一般に、コミュニティー・カレッジの学生が多数いて、優れた実践的な技術スキルを持っていても、企業はそれまでのやり方から脱して彼らを採用しようとはしません。セキュリティーでは、「やる」ことができなければなりません。外科医と同じようなものです。常に練習して、スキルを磨き、新しい手法を学んでテストしなければならないのです。」

Dr. Sujeet Shenoi、タルサ大学のコンピューター・サイエンス F.P. Walter 教授および化学エンジニアリング教授

フィールドの拡大: 新しいタイプの職務

サイバー・セキュリティーは、出現しつつあるテクノロジーを活用し、実行するスキルと知識を必要とするが、従来の 4 年制大学の学位を必ずしも必要としない、多くのジョブ・カテゴリーの 1 つにすぎません。ニュー・カラー・アプローチは、必要なスキルを学習するために代わりの方法があることを認識しています。例えば、CSIS および Intel Security の調査の回答者は、学位よりも実践経験と専門認定がサイバー・セキュリティーのスキルを取得するのによりよい方法であると位置付けしています。[18]

セキュリティー関連では、ソフトウェア開発、設計およびセールスから、コンサルティングやマネージド･セキュリティー･サービスまでにわたる、多数のさまざまな職務があります。これらの分野の中には、異なるスキルや経験が必要な多数の職位があり、それらの多くはニュー・カラー・アプローチによって満たすことができます。例えば、2015 年以降、IBM セキュリティーは米国で大学レベル未満の学歴の 170 人以上を IT スペシャリスト、販売者、ソフトウェア開発者、およびコンサルタントとして採用しました。これは米国での採用全体のおよそ 17 パーセントに当たります。

ニュー・カラー・アプローチは、技術的および非技術的な職務の両方を満たすのに利用できます。始めるのに適した場所としていくつかの特定の職務を識別しました。

ビルダー

- *統合エンジニア* — 既存のコンポーネント、システム、API を使用して、調整したセキュリティー・ソリューションを構築します。
- *テスト・エンジニア* — システムとコンポーネントをテストして、誤用の時でも予期されるように動作することを確認します。
- *セキュリティー・デバイス・アナリスト* — エンド・ユーザー・デバイスやモノのインターネット (IoT) のデバイスがポリシーに適合しているかテストします。
- *サイバー・セキュリティー開発者* — サイバー・セキュリティー・ツールのコードやセキュリティー・デバイスのルールを作成します (例えば IDS、SIEM)。

オペレーター

- *脅威監視アナリスト* — コンピューター・セキュリティーのイベントを監視し、警報やインシデントを調査します。
- *侵入テスター* — 「攻撃者」を装って、IBM では「Red」チームと呼ばれるメンバーが会社のシステムとサーバーを攻撃します。
- *セキュリティー・オペレーション・センター (SOC) アナリスト* — インシデントを報告し、インシデントへの対応を支援し、SOC 全体で脅威に対するインテリジェンスの共有を調整します。
- *コマンドおよびコントロール (C2) 脅威ハンター* — データ・セット全体を検索して、自動ツールを潜り抜けた脅威や攻撃を識別します。
- *サイバー・オペレーション・エンジニア* — 組織の日常のサイバー・オペレーション (ファイアウォールの管理や ID 管理リポジトリーの構成など) を実行します。

コミュニケーター

- *サイバー・ヘルプ・デスク・アナリスト* — ユーザーがセキュリティーのインシデントやイベントを経験した場合 (フィッシング・メールを受け取ったり、システムがランサムウェアによってロックされたりした場合など) に、サポートと指示を提供します。
- *テクニカル・ライター* — セキュリティー・ポリシーや対応計画のマニュアルやサポート資料を作成します。
- *セキュリティー認識トレーナー* — 社員やお客様にサイバー・セキュリティーの基本と推奨する手法の訓練を行います。複雑でときに恐ろしいサイバー情報を、ユーザーが覚えて実行できるアクションに変換しなければなりません。

チームで走る: 新しいパートナーシップの推進

ニュー・カラー・アプローチの第 3 の要素は、さまざまな組織や教育機関とのパートナーシップを確立して発展させることです。多くのパートナーシップを活用することにより、政府プログラムやコミュニティー・カレッジ、退役軍人の組織などと関わることを含め、サイバー・セキュリティーの人材プールを拡充するのに役立ちます (図 2 を参照)。

例として、IBM には短期的にも長期的にもサイバー・セキュリティーの人材を得るための網を広げることに役立つ、内部および外部の多数の以下のようなプログラムがあります。

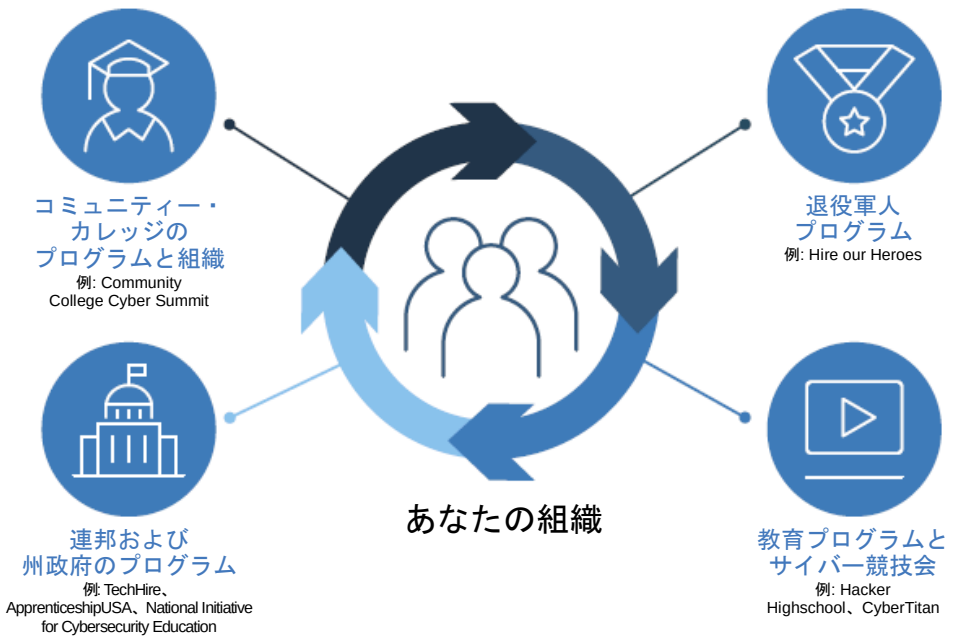
- P-TECH 9-14 スクール・モデルの作成と複製 (サイドバー: P-TECH スクール・モデルを参照)[19]
- Women in Security Excelling (WISE) — 中等学校での「Cyber Day for Girls」プログラムなどの外部イベントの後援もする内部グループ [20]
- 退役軍人のための訓練と認定プログラムにフォーカスした、IBM Veterans Employment Accelerator[21]
- 軍事基地、サイバー競技会、専門家組織において、可能な場合にはいつでも従来型の採用を拡大
- CyberTitan などのサイバー・セキュリティー競技会の後援。

「私は Carver High School からほんの数ブロックのところで育ち、住んでいます。私は学生たちに、無料で知識、経験、資格を得られるこのような機会を私も持てたらよかったと思う、と話しています。自分のメリットになるように、この機会をしっかり生かして、メンターを活用するよう、学生たちを励ましています。私たちがここにいるのはそのためですから。」

Loretta Lemon、シニア・マネージング・コンサルタント、セキュリティー、コンプライアンスおよびプライバシー、IBM

図 2

サイバー・セキュリティーの人材プールを改善するためのパートナーシップ



P-TECH スクール・モデル [22]

P-TECH 9-14 スクール・モデルは、歴史的に不利な立場にある人々 (正式な学位がないなど) の役に立つよう設計されており、米国のパブリック・スクールのグレード 9 から 14 の学生に、ここでなければ得られないような卒業後の機会への明確な進路を提供します。IBM は、ニューヨーク市教育局とニューヨーク市立大学と共に、2011 年にニューヨーク州ブルックリンで最初の P-TECH スクールを作りました。P-TECH を通じて、選抜を受けずに入学した学生たちは、自分も家族も費用の負担なしに、高校の卒業資格と業界認定の 2 年間の高等教育資格の両方を得られます。学生たちは産業界のパートナーの求人において優先候補にもなります。このモデルは米国の 50 以上の学校と 300 を超える産業界のパートナーに広がり、2017 年には 80 以上の学校に拡大することを目標にしています。

P-TECH は高校、カレッジと仕事の世界をつなぎ、学生を将来の STEM (科学技術) 分野の仕事への準備ができるようにします。3 つの P-TECH スクールが特にサイバー・セキュリティーにフォーカスしています (以下を参照)。さらに、これらパイオニアが設定したモデルに従う学校が増えることが期待されます。

スクール	パートナー	注
Newburgh Free Academy での Excelsior Academy (ニューヨーク)	Newburgh Enlarged City School District、IBM 、SUNY Orange Community College の間のパートナーシップ	公立高校としての 3 年目で、プログラムには 150 人の学生がいます。学生は基本的なネットワーク管理スキルを培い、コンピューター・フォレンジック分析を行い、ネットワーク・フォレンジックの理解を実証し、サイバー・セキュリティーに関連する法律問題の理解を深め、事例の証拠の取り扱いの適切な手順を作成します。
P-TECH@ Carver (メリーランド)	Carver Vocational Technical High School、IBM 、Baltimore City Community College の間のパートナーシップ	プログラムは 2016 年から 2017 年の学年度に、グレード 9 の学生 50 人で開始し、2017 年の秋にはさらに 50 人が予想されます。87 人の IBM メンターがいるので、多くの学生に 2 人のメンターがついています。学生はサイバー・セキュリティーの AAS 資格を得られます。
Newport P-TECH (ロードアイランド)	Newport Public Schools、Community College of Rhode Island (CCRI) 、 Southeastern New England Defense Industry Alliance (SENEDIA) の間のパートナーシップ	このキャリアと技術教育のプログラムは 2016 年の秋に 42 人の学生 (女子 22 人、男子 20 人) で開始しました。メンターはロードアイランド州警察、米国海軍、防衛産業会社から来ています。

「多くの組織は間違った場所を探していて、活用されていない人材のプールを逃しています。10 年以上、コミュニティー・カレッジはスキル開発にフォーカスしたセンターの大規模ネットワークを作ってきたのです。これらのネットワークには強力で実証された人材開発と習得モデルがあり、これらは多くの業界認定、ジョブ役割、垂直展開に広げることができます。」

Casey O'Brien、エグゼクティブ・ディレクター & 主席調査者、National CyberWatch Center

サイバー・セキュリティー・プログラムを提供するところが増えてきており、コミュニティー・カレッジは人材のもう 1 つの重要な供給源となっています。推定では、米国全体でおよそ 1,100 ある公立/私立のコミュニティー・カレッジの約 30 パーセントがサイバー・セキュリティーの資格、認定やコースを提供しています。これらのプログラムにより、学生、生涯学習者、スキルアップや転職を考えている人など何千人もが教育を受けています。[23] コミュニティー・カレッジ・プログラムは、従来の 4 年制プログラムよりも融通性があり、スキルにフォーカスしていると自負しています。市場の変化に対してアプローチやカリキュラムを素早く調整することにより、一般に従来の研究ベースの大学プログラムよりも迅速に対応することができます。労働力やスキル開発にフォーカスしてきた歴史もあります。最後に、コミュニティー・カレッジのサイバー・セキュリティー・プログラムは、大学のプログラムよりも実践的な傾向があります。

コミュニティー・カレッジのサイバー・セキュリティー・プログラムをサポートするいくつかのリソースを以下に紹介します。

- National Security Agency および Department of Homeland Security は、情報保証とサイバー防衛にフォーカスしたものも含め、 2 年間の教育機関である National Centers of Academic Excellence を後援しています。[24]
- National Science Foundation の Advanced Technological Education プログラムは、2 年制のカレッジで地域のサイバー・セキュリティー・プログラムをサポートしています。[25]
- Community College Cyber Summit は現在 4 年目となり、コミュニティー・カレッジでのサイバー・セキュリティーの取り組みの場となっています。[26]

スタート・ラインに着く: 独自のニュー・カラー・アプローチ

スキル・ギャップに対処するために求める対象者を変えたいならば、独自のニュー・カラー・アプローチの構築を始めましょう。少なくとも、あなたのサイバー・セキュリティー労働力を構築して維持するための戦略全体の 1 つのコンポーネントにしてください。

始めるための最も簡単な方法は、アプローチの支援者となることです。自分ができる簡単なこと、話せる場所や、同僚と共有できる情報を探してみましょう。さらに強力なニュー・カラー・アプローチとしては、以下を検討してください。

労働力の戦略を再検討する

- 組織にとって現在および将来何のスキルが不可欠かを考えて、それを文書化します。それを使用して、各レベルで何のスキルが必要かにフォーカスして、セキュリティー職務への明確なキャリア・パスを設計します。
- 人材採用では、前提条件として学位だけに注目しないでください。セキュリティー関連の採用すべてに 4 年制大学の学位が本当に必要ですか? 実力を示す機会を得る前に、スターになる可能性のある人を除外しないでください。スキルや経験はさまざまな場所から来ることを認識しましょう。

関与を拡大して働きかける

- 採用する場所を拡大します。いつも注目してきた選り抜きのセットの大学だけに限定するのはやめましょう。
- コミュニティー・カレッジ、P-TECH スクールやその他の教育プログラムでの学習セッションやデモのようなシンプルなものから始めて、そこから構築しましょう。

「歴史的に、ほとんどの求人で最初の要件が正式な学位であるために、多くの企業に見逃されてきた多数の人材があります。誰もが異なる進路を通ってきており、費用や人生の困難のために 4 年制の大学に行けなかった人もいます。職務によっては「特定の学位」を必要とすることもありますが、スキルや価値を示す機会を提供せずに、人材を選別して排除していることもあると思います。」

Adam Griffin、アドバイザリー・アーキテクト、マネージャー、マネージャー・セキュリティー・サービス、インフラストラクチャー & エンドポイント・セキュリティー、IBM セキュリティー

地域のサイバー・セキュリティー・エコシステムを構築する

- 地域の労働力開発組織、中等学校、技術・職業学校などと、地域で新しいパートナーシップを構築することに目を向けましょう。
- サイバー・セキュリティー・カリキュラム委員会に参加すること、彼らのスキルが常に最新で適切であるように地域のインストラクターに学外研修を提供すること、サイバー・チームを支援すること、また、地域の中等学校や高校と連携してこの分野への興味喚起することもできます。これらのグループはいつでも、対象分野の専門家やメンターを求めています。

新規採用者に堅固なサポート・プログラムを提供する

- メンターシップ、職務のローテーション、シャドーイングなどの手法や他の機会をサイバー・セキュリティーの新規採用者に使って、経験を得たり学習できるようにします。彼らが選択肢や機会を探索できるようにします。自分が何をやりたいかを誰もがすぐにわかっているわけではありません。
- 新規採用者にさまざまなプロジェクトで働いて新しいテクノロジーやサービスを探索する創造的な自由を提供して、関わり続けるようにします。

継続的学習とスキルアップにフォーカスする

- 採用の入り口を広げて新しい人材を取り込んだら、その人材が定着するように働きかけます。クラスや認定、会議などをとおしてスキルを最新に保つための機会を提供することにより、社員を関与させ続けます。サイバー・セキュリティーは非常に変化の激しい分野であり、常にスキルをリフレッシュすることが必要です。
- さらに、他の職務から新しいキャリアとしてサイバー・セキュリティーに移動したい既存の社員をサポートするためにできることを行います。

ニュー・カラー・アプローチを行う準備ができましたか?

- 4 年制の学位を持つ候補者にのみ注目して、潜在的なサイバー・セキュリティーの人材を見逃していませんか?
- 組織のどのサイバー・セキュリティーの職務がニュー・カラー・アプローチに適していますか?
- サイバー・セキュリティーのエコシステムを拡大するために、どうやってどの組織とパートナーシップを構築できますか?
- サイバー・セキュリティーの新規採用者に対するサポートをどのように改善できますか?
- サイバー・セキュリティーの社員の継続的学習を奨励して人材の定着を向上させるためにさらにどんな機会を提供できますか?

詳細情報

IBM Institute for Business Value 調査について詳しくは、iibv@us.ibm.com までお問い合わせください。Twitter で @IBMIBV をフォローしてください。調査の全目録や月刊ニュースレターの登録をご希望のお客様は、次の Web サイトをご覧ください。**ibm.com/**iibv

IBM Institute for Business Value のエグゼクティブ・レポートは、お使いのモバイル端末からご覧いただけます。スマートフォン、タブレット用の無料アプリ「IBM IBV」をストアからダウンロードのうえご利用ください。

IBM セキュリティーについて詳しくは、**ibm.com/**security/ciso をご覧ください。

変わりゆく世界に対応する適正パートナー

IBM では、お客様との協働によりビジネス・インサイト、先端研究、テクノロジーを結集させ、今日の急速に変わりゆく環境で明白な優位性をお客様に提供します。

IBM Institute for Business Value

IBM グローバル・ビジネス・サービスの IBM Institute for Business Value は、公共機関、民間企業を問わず、重要課題に関する戦略的インサイトを経営層向けに事実に基づき開発しています。

執筆者

Marc van Zadelhoff は、世界最大の企業セキュリティー会社の 1 つである IBM セキュリティーのゼネラル・マネージャーです。サイバー・セキュリティーで 20 年の経験を持ち、さまざまな業界のお客様と連携して、お客様がセキュリティー戦略を開発してニーズに合わせた最善のテクノロジーを決定するのを支援してきました。Marc の連絡先は次のとおりです。Twitter @mvzadel、および marc.vanzadelhoff@us.ibm.com。

Lindsey Lurie は IBM セキュリティーのチーフ・マーケティング・オフィサーです。Lindsey の 15 年以上にわたる IBM での経験は、複数のビジネスにわたるマーケティングやコミュニケーションの職務に及びます。専門知識の分野には需要の創出、製品マーケティング、デジタルおよびチャネル・マーケティング、広告およびイベント実行が含まれます。連絡先は次のとおりです。LinkedIn linkedin.com/in/lindseylurie、および llurie@us.ibm.com。

David Jarvis は IBM Institute for Business Value のセキュリティーおよび CIO リーダーです。出現しつつあるビジネスを探索する調査アジェンダとそれらの分野のテクノロジーのトピックを開発して実行する責任を担っています。David の連絡先は次のとおりです。LinkedIn linkedin.com/in/davidajarvis、Twitter @dajarvis、および djarvis@us.ibm.com。

協力者

Diane Delaney — ワールドワイド・タレント・マネージャー、IBM セキュリティー

Lisa van Deth — キャンペーンおよびソート・リーダーシップ・ストラテジー・マネージャー、IBM セキュリティー

Kelli Jordan — タレント・リーダー、ニュー・カラー・イニシアチブ、IBM ヒューマン・リソース

Diana Kelley — グローバル・エグゼクティブ・セキュリティー・アドバイザー、IBM セキュリティー

Ivo Klaassen — グローバル・プロフェッショナル・デベロップメント・リーダー、IBM セキュリティー

Heather Ricciuto — トランスフォーメーションおよびアカデミック・イニシアチブ・リーダー、IBM セキュリティー

謝辞

Cliff Archey —Program Manager, Education, IBM
Lee Christian —Senior MSIEM Analyst, U.S. MSIEM Analyst Team Lead, IBM Security
Ashleigh Cooper —Program Manager, Education, IBM
Sean Davis —Security Services Senior Security Engineer, IBM Security
Matthew Dombrowski —MSS IES Engineer, IBM Security Services, IBM Security Adam Griffin —Advisory Architect, Manager, MSS: Infrastructure & Endpoint Security, IBM Security
Michael Kelly —Chair, Computer Studies & Information Processing Department, Community College of Rhode Island
Valinda Scarbro Kennedy —Worldwide Skills Program Manager, IBM John Kuhn —Manager, IBM X-Force Services, IBM Security
Linda Larsen —Director, Education Outreach, Southeastern New England Defense Industry Alliance
Loretta Lemon —Senior Managing Consultant, Security, Compliance, and Privacy, IBM Molly Magee —Executive Director, Southeastern New England Defense Industry Alliance Bill McDonald —Director, Human Resources, IBM Security
Casey O’Brien —Executive Director & Principal Investigator, National CyberWatch Center Cecelia Schartiger —Jr. IA Compliance Officer, Cyber & Biometrics, IBM Global Business Services
Ken Shade —MSIEM Monitoring Manager, IBM Security
Dr. Sujeet Shenoi —F.P. Walter Professor of Computer Science and Professor of Chemical Engineering at the University of Tulsa

参考文献

1. 「Net Losses: Estimating the Global Cost of Cybercrime」Center for Strategic and International Studies および McAfee。2014 年 6 月。https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
2. 「The 2017 Global Information Security Workforce Study: Women in Cybersecurity」Frost & Sullivan。2017 年 3 月。https://iamcybersafe.org/wp-content/uploads/2017/03/ WomensReport.pdf
3. 「Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills」Center for Strategic and International Studies および Intel Security。2016 年。https://www.mcafee.com/ca/resources/reports/
4. 「The 2017 Global Information Security Workforce Study: Women in Cybersecurity」Frost & Sullivan. 2017 年 3 月。https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf
5. 「2016 Fact Sheet」American Association of Community Colleges。http://www.aacc.nche.edu/AboutCC/Documents/AACCFactSheetsR2.pdf; IBM Institute for Business Value Casey O'Brien、エグゼクティブ・ディレクター & 主席調査者、National CyberWatch Center とのインタビュー。2017 年 2 月 21 日。
6. 「Interactive map」CyberSeek Web サイト、2017 年 5 月 3 日にアクセス。http://cyberseek.org/heatmap
7. 「P-TECH 9-14 Model」P-TECH Web サイト、2017 年 4 月 3 日にアクセス。http://www.ptech.org/; Coughlan、Sean。「Bletchley Park: 'Codebreakers school' planned for site」BBC ニュース。2016 年 11 月 24 日。http://www.bbc.com/news/education-38065563
8. 「2017 Community College Cyber Summit (3CS): Strengthening our cyber IQ」3CS Web サイト、2017 年 4 月 3 日にアクセス。https://www.my3cs.org/
9. 「Hacker Highschool: Security Awareness for Teens」Hacker Highschool Web サイト、 2017 年 4 月 3 日にアクセス。http://www.hackerhighschool.org/
10. 「Apprenticeship USA」United States Department of Labor Web サイト、2017 年 4 月 3 日にアクセス。https://www.dol.gov/featured/apprenticeship

11. 「CompTIA Security+」CompTIA Web サイト、2017 年 4 月 3 日にアクセス。https://certification.comptia.org/certifications/security; 「CISSP – Certified Information Systems Security Professional」(ISC)2 Web サイト、2017 年 4 月 3 日にアクセス。https://www.isc2.org/cissp/default.aspx; 「Master the Core Technologies of Ethical Hacking」EC-Council Web サイト、2017 年 4 月 3 日にアクセス。https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

12. 「Air Force Association's CyberPatriot: The National Youth Cyber Education Program」CyberPatriot Web サイト、2017 年 4 月 3 日にアクセス。https://www.uscyberpatriot.org/;「CyberTitan: Now launched」Information and Communications Technology Council Web サイト、2017 年 4 月 3 日にアクセス。http://www.ictc-ctic.ca/cybertitan/

13. 「About this tool」CyberSeek Web サイト、2017 年 4 月 3 日にアクセス。http://cyberseek.org/; TechHire Web サイト、2017 年 4 月 3 日にアクセス。http://techhire.org/

14. International Consortium of Minority Cybersecurity Professionals Web サイト、2017 年 4 月 3 日にアクセス。https://icmcp.org/; 「Veterans Training」Hire our Heroes Web サイト、2017 年 4 月 3 日にアクセス。https://hireourheroes.org/veterans-training/; Women's Society of Cyberjutsu Web サイト、2017 年 4 月 3 日にアクセス。http://womenscyberjutsu.org/; Women in CyberSecurity Web サイト、2017 年 4 月 3 日にアクセス。https://www.csc.tntech.edu/wicys/

15. Barlow、Caleb。「Artificial intelligence makes cybersecurity the ideal field for 'new collar' jobs」The Hill。2017 年 3 月 22 日。http://thehill.com/blogs/pundits-blog/technology/325067-artificial-intelligence-makes-cybersecurity-the-ideal-field-for

16. King、Mike; Anthony Marshall; および David Zaharchuk。「Facing the storm: Navigating the global skills crisis」IBM Institute for Business Value。https://www-935.ibm.com/services/us/gbs/thoughtleadership/skillsstorm

17. Ibid。

18. 「Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills」Center for Strategic and International Studies および Intel Security。2016 年。https://www.mcafee.com/ca/resources/reports/rp-hacking-skills-shortage.pdf

19. 「IBM and P-TECH」IBM プレス・キット。IBM Web サイト、2017 年 4 月 3 日にアクセス。https://www-03.ibm.com/press/us/en/presskit/42300.wss

20. 「How IBM Supports Women Building their Careers in Cyber Security」IBM Jobs Blog。 2016 年 11 月 7 日。 https://blog.ibm.jobs/2016/11/07/how-ibm-supports-women-building-their-careers-in-cyber-security/

21. 「Citizen IBM Blog – Veterans Employment Accelerator」IBM Web サイト、2017 年 3 月 19 日にアクセス。https://www.ibm.com/blogs/citizen-ibm/tag/ibm-veterans-employment-accelerator

22. 「P-TECH Schools」P-TECH Web サイト、2017 年 3 月 19 日にアクセス。 http://www.ptech.org/ schools; 「IBM Equips Youth with Tech Career Skills in Nationwide Network of High Performing P-TECH Schools」IBM プレス・リリース。2017 年 1 月 5 日。 http://www-03.ibm.com/press/us/en/pressrelease/51327.wss; 「Case study: Preparing students at Excelsior Academy for Careers」P-TECH Web サイト、2017 年 4 月 3 日にアクセス。 http://www.ptech.org/case-study/preparing- students-at-excelsior-academy-for-careers; 「Two Baltimore high schools first to join P-TECH program in Maryland」Johns Hopkins University、University News。2016 年 6 月 16 日。 http://hub.jhu.edu/2016/06/16/p-tech-schools-announced-dunbar-carver/; 「Newport P-TECH」P-TECH Web サイト、2017 年 4 月 3 日にアクセス。 http://www.ptech.org/schools/000000000000049; 「P-TECH」Rogers High School Web ページ。Newport Public Schools Web サイト、2017 年 4 月 3 日にアクセス。https://www.npsri.net/ptech

23. 「2016 Fact Sheet」American Association of Community Colleges。 http://www.aacc.nche.edu/AboutCC/Documents/AACCFactSheetsR2.pdf; IBM Institute for Business Value Casey O'Brien、エグゼクティブ・ディレクター & 主席調査者、National CyberWatch Center とのインタビュー。2017 年 2 月 21 日。

24. 「NSA/DHS Current National CAE Designated Institutions」Information Assurance at the National Security Agency Web サイト、2017 年 3 月 19 日にアクセス。 https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

25. 「ATE Centers – Security Technologies」National Science Foundation's Advanced Technological Education centers Web サイト、2017 年 3 月 19 日にアクセス。http://www.atecenters.org/st/

26. 「Community College Cyber Summit 2017」2017 年 3 月 19 日にアクセス。 https://www.my3cs.org/

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in the United States of America
2017 年 5 月