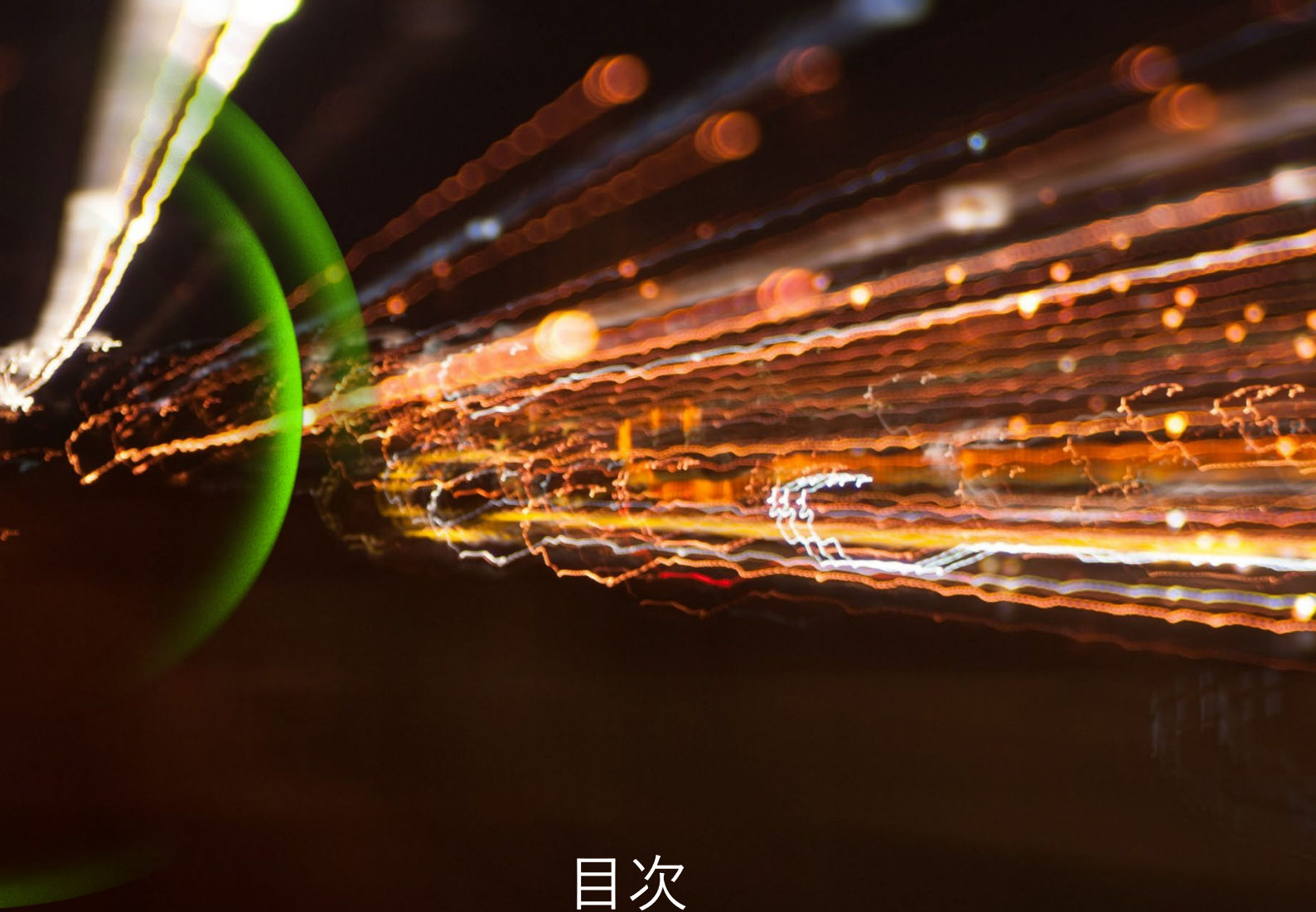
Deloitte.
デロイト トーマツ

未来のサイバー人材を育成する

サイバー人材の概念を刷新



目次

はじめに

日本国内のサイバーセキュリティ情勢としては、攻撃件数と攻撃手法の急激な変化により、従来以上にサイバーセキュリティへのプレッシャーが高まっています。最近は、インフラ、政府、企業を標的とするサイバー攻撃が複数発生しています。[1] さらに、生成AI（人工知能） などの新しい技術の普及拡大に伴い、新たなリスクの顕在化が進んでいます。

このような状況下で、高度なスキルを持つサイバー人材の慢性的な不足は、国内の脆弱性を一層際立たせています。教育課程と産業ニーズの不整合、年齢構成の変化、専門人材の採用・定着を阻む企業文化が複合的に影響しています。

サイバーセキュリティ分野における規制環境は、近年ますます厳格化しています。新たなサイバーセキュリティフレームワークの導入により、企業は報告体制の強化や、インシデント発生時の対応能力、ガバナンス体制の一層の充実が求められています。人材不足に悩まされている組織は、コンプライアンス違反や規制による罰則が課されるリスクが高まっています。

デジタルトランスフォーメーション（DX）が加速するにつれて、この人材ギャップは確実に拡大し、国内の重要インフラや企業はこれまで以上に脆弱な状態になると考えられます。

経営の戦略的課題：今重要視すべき理由

日本は厳しい現実に直面しています。人員が不足するセキュリティチームでは、高度化する脅威アクターの進化速度には追随できません。

日本を取り巻くサイバー脅威は深刻化しており、国家主体あるいは犯罪者などの脅威アクターによる重要インフラや、政府機関、企業が標的となるサイバー攻撃が増加しています。企業は通常、ランサムウェアやデータ窃取のリスク、政府はサイバースパイ活動や重要インフラへの攻撃に関するリスクに直面しています。

政府機関の近代化と日本全体のサイバーセキュリティ強化を目的としたサイバー対処能力強化法及び同整備法[2]が2025年5月に成立したにもかかわらず、日本は依然として重要な政府機関のシステムに対するセキュリティ管理の課題を抱えています。会計検査院の報告によると、政府機関12省庁の58システムにセキュリティ上の課題が確認され、適切なセキュリティ対策が講じられていないことが明らかになっています。[3] これはサイバー攻撃が急増している期間に重なります。政府は2024年に少なくとも447件のインシデントを確認しており、これは前年の2倍以上の件数となっていました。[4]

最近の注目を集めたインシデントでは、その発生原因が「人」に起因する側面を改めて浮き彫りにしています。国内におけるサイバー人材に関する課題については、企業、教育機関、政府が一体となって取り組むべき重要な局面を迎えています。国内においては、サイバーセキュリティの専門家が17万人近く不足していると推定されています。[5] ISC2によると、2024年の国内サイバーセキュリティ関連の人材は前年比4%と増加した一方で、スキルのギャップのある人材の割合が53.8%を占めて大幅に拡大しています。これは、需要が供給を上回るペースで加速していることを示しています。[6]

人材育成の必要性を認識し、サイバー人材を拡充するための様々な計画が立案されています。日本の防衛省では2022年、サイバー対処能力強化法及び同整備法の構想を元に、サイバー防衛の人員を現在の四倍以上に拡充し、2027年度までにサイバー攻撃に対処する人員を2万人にまで増員する計画を発表しました。[7]

また、経済産業省 (METI) は2025年5月、国家資格である情報処理安全確保支援士(RISS) の有資格者数の拡大目標を発表しました。しかし、2024年4月の時点の有資格者は約2.4万人に留まっており、政府が掲げる2030年までに5万人という目標を大きく下回っていることからも有資格者の拡充に関する課題が確認されています。[8]

最も懸念されるのは、これらすべての課題が複合的に作用している点です。サイバー脅威がより高度化し、規制要件が増えるに伴い、確保すべき労働力とのギャップはさらに拡大します。企業は自然に人材市場が適正化されるのを待つことはできません。これは、日本のデジタル主権を脅かす人的資本に関する課題となっています。最高レベルのリーダーによる迅速かつ協調的な行動がなければ、国家安全保障、経済レジリエンス、国民の信頼に対するリスクは一層深まると考えられます。

人口動態の転換：若年人材の減少リスク

サイバー人材の課題は、少子高齢化という人口動態の現実と不可分です。高齢化の進行と若年層の減少が構造的な制約となっています。

総務省統計局によると、2025年9月15日現在、日本は65歳以上の高齢者が占める割合は29.4%となっており、人口が4000万人以上である世界38カ国の中で最も高くなっています。[9] さらに、日本の生産年齢人口 (15歳以上65歳未満) の割合は、令和32年 (2050年) には52.9%まで低下すると予測されています。[10] この生産年齢人口の減少は、従来の人材開発モデルによる育成に対する制約となっています。また、新卒者をサイバーセキュリティ職として採用することは、ますます困難になっています。サイバー人材の需要が急激に加速していますが、人材市場における若い専門家は減少しています。

人材不足はIT分野にとどまらず、他産業においても採用需要が逼迫しています。例えば、医療、介護、福祉は、増加する高齢者人口を支えるために多くの人材を必要としています。人材不足が深刻な課題となっているため、高齢化社会では全産業において専門家の獲得競争が激化しています。同時に、経験豊富なIT人材が定年退職の時期を迎えており、数十年にわたる組織の知見が失われつつあります。つまり、労働市場における新規参入者の減少と経験豊富な人材の流出という「二重の構造的課題」が生み出されています。

このような人口動態の変化は、サイバー人材の採用やキャリアパスに関する様々な制約となり複合的に影響を与えています。経営者やリーダーは、これらの課題を正しく理解し、サイバーセキュリティ業務では変化に対応する能力があるスキルベース組織を進化させる必要があります。従来型のキャリア構造は、現在の要件に適合しない可能性があります。

文化・制度的要因：隠れた人材プールの可能性

日本の人材不足の根底には、採用と定着がより困難となる文化的・制度的要因があると考えられます。

ITおよびサイバーセキュリティにおけるジェンダーギャップは、人材プールが十分に活用されていないことを示しています。現在、国内のITエンジニア部門に占める女性比率は18.8％となっており、OECD平均の20.6%や、英国 (22.8%)、オーストラリア (21.7%)よりも下回っています。[11]

サイバーセキュリティは男性中心の分野という認識は、サイバーセキュリティ分野を目指す女性が実際に就職することをためらう要因となっています。組織が、職場の就業規則を見直しにより女性採用に向けた対応を行い、インクルーシブな職場環境の整備や女性向けの採用活動の強化、さらに女性のセキュリティ分野におけるリーダーシップ人材の可視化を推進することにより、より多くの人材を確保できる可能性が広がります。

次に、定年後も就業意欲の高いシニア層も隠れた人材プールです。各種調査によると、国内の労働者の約80%が定年後も働き続けたいと回答し、このうちの約70%は現在の勤務先での継続を希望しています。[12] 政府も、改正された高年齢者雇用安定法や各種助成制度[13]を通じて、シニア層雇用の拡大を後押ししていますが、この層をデジタル職種に移行させるためのリスキリング戦略は、まだ発展途上の状況です。

さらに、終身雇用や年功序列的な階層型キャリアなど、日本固有の雇用慣行の見直しも避けて通れません。若年層は、柔軟性や、働きがい、社会的意義をより重視する傾向が強まっています。2025年の調査によると、定年まで同じ会社で働きたいと考える若年層は24.4%にとどまり、2015年の36.3%から低下していました。[14] Gallupの2026年版「世界の職場の現状」では、日本で仕事へのエンゲージメントを感じていると回答した割合はわずか8%となっており、世界的でも最低の水準となっています。エンゲージメントの低さに加えて、前日に「強いストレスを感じた」と回答した労働者は39%になっており、ほぼ5人に2人が高いストレスを感じている状況です。[15] これらの結果は職場満足度に関する根深い課題の存在を示しており、他の専門職と同様にサイバーセキュリティ職においても同様に課題があると考えられます。多くの従業員が仕事において孤独感を感じている場合、組織は仕事への情熱や責任感を持つ人材を惹きつけ、定着させることが困難になります。従来型の採用や昇進の慣行を継続している組織は、若年層のサイバー人材を獲得する上で不利になりかねません。サイバーセキュリティの専門家は、サイバーセキュリティ業務の変化に対応する能力や必要なスキルが明確なキャリアパスが示された役割で業務に従事することを求める傾向があります。

これらの文化的ダイナミクスや職場規定などの要因に対処しない限り、サイバー人材の獲得を拡大する取り組みでは成果が得られないと想定されます。

数値を超えた価値：将来に備えた人材体制に

将来のサイバー人材獲得の基盤を構築するには、組織によるセキュリティ人材の特定、獲得、育成、定着の方法を確立するため、抜本的な再定義の実施が必要となっています。仮に新卒採用によって人材不足を大幅に解消できたとしても、デジタル防衛の新時代においては、明確な目的と高いレジリエンスを備えたサイバー人材が必要となっているためです。

今後のサイバー人材にはいくつかの重要な特徴が求められます。

1. **ミッション主導型**：この職業を目指す原動力は、社会的インパクトの実現に対する貢献です。デジタル資産と社会を守るという使命は、継続的かつ重大な責任を伴う領域において、モチベーションの持続と高い成果を得られる主な要因となります。

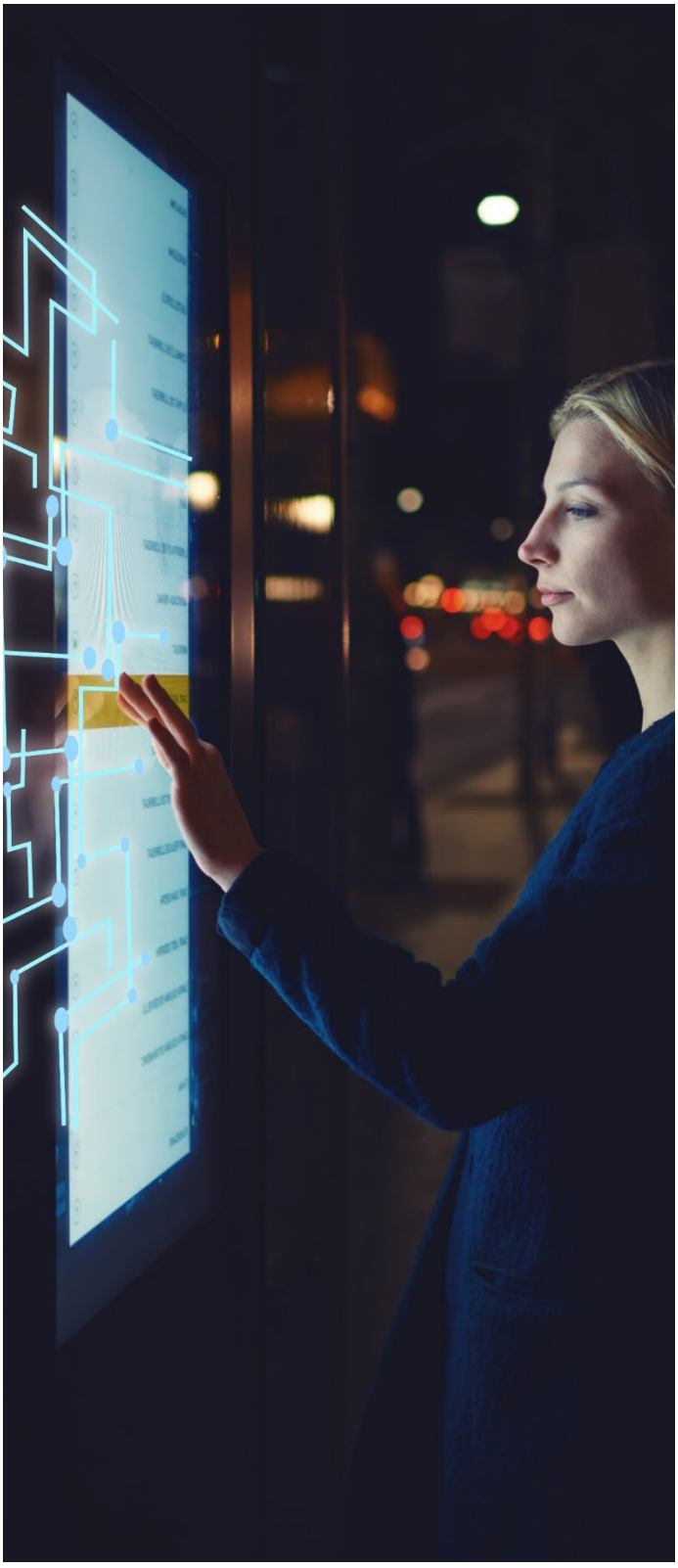
2. **多様性**：デジタル空間を守るには、その多様性が人材に関しても反映される必要があります。性別、年齢、バックグラウンド、地域の多様性は、多様な攻撃ベクトルを予測するための多角的な視点をもたらします。また、セキュリティ対策を包括的でインクルーシブなものにします。

3. **エモーショナル・レジリエンス（精神的回復力）**：サイバーチームにはプレッシャーがかかる状況下でも適切に業務を遂行できるよう、十分な支援が不可欠です。こうした「エモーショナル・レジリエンス（精神的回復力）」を組織的に高めることで、急速な環境変化や多様な脅威に直面する場面でも、チーム全体が柔軟かつ効果的に対応できるようになります。

4. **デジタル・フルーエンシー**：サイバーの基礎以外の幅広いデジタル領域についても習熟していることが求められます。具体的には、自動化、AIシステム、AI倫理などの新しい領域の理解と実践が重要です。

5. **AIによる拡張**：企業は、AIツールが人間の専門性を代替するのではなく補完するものとして活用されるべきです。AIのスピードとスケールに、人間の創造性、文脈理解、倫理的判断を組み合わせるアプローチが最も高い効果を生みます。

将来適合した人材を育成するには、職務設計、人材育成、組織と人材の関わるシステム的な転換が必要となっています。



進むべき道：再設計・再考・再構想

日本の組織においては、サイバーセキュリティ分野のキャリアパスを、国内労働市場の実態や変化する人材ニーズに合わせて設計することが重要です。国家安全保障を維持し、社会の安全を確保し、デジタルトラストを通じて組織と経済の成長を支援する目的あるキャリアとしてサイバーセキュリティの位置付けができれば、新たな世代を惹きつけることとなります。そのためには、サイバー人材を支える人事制度の再考が必要であるかを検討する必要があります。組織は、現在の人材不足、従業員の業務環境の向上、将来の人材採用方針など、主要課題への対処を図る必要があります。

以下の10の提言は、国内のサイバー人材不足をすべて解決するものではありませんが、中核的な課題に焦点を当て、より強靭なサイバー人材基盤の構築に向けた実効的なステップの提示を目指しています。

人材不足への対応

1. **自動化とAIの活用**：自動化とAIの積極的な導入は、サイバーセキュリティ分野における人材不足の対応先としてセキュリティの有効性も向上させていくための重要な転機となる可能性があります。先進的な企業は、人とテクノロジーの両面で投資を行い、相互補完的な強みを活かす人間×AI統合チームの構築を行います。例えば、AIで強化されたセキュリティオペレーションでは。AIが定型作業を担い、人の判断が必要な重要事案を可視化できるため、小規模チームでの活動が可能になります。防衛省においても2024年7月に、サイバーセキュリティ能力の強化にAI活用推進基本方針を発表しました。[16] このアプローチは組織が直面する即時的な人材不足の課題を解決すると同時に、長期的な組織力の強化にもつながります。

2. **スキルアップ**：サイバーセキュリティの脅威が急激に変化しているため、専門家は継続的にスキルを向上させ、新しい課題への対応が可能になる必要があります。既存のサイバー人材の能力向上に向けた包括的なスキルアッププログラムへの投資を検討する必要があります。例えば、継続的な学習の機会や、資格取得支援、メンタリングなどの体系的な人材育成プログラムの確立も必要となります。

3. **リスキリング**：このアプローチは組織が直面する即時的な人材不足の課題を解決すると同時に、長期的な組織力の強化にもつながります。例えば、財務部門の専門家はリスク評価の知見、製造技術者はOTセキュリティに不可欠なOTに関する洞察、元自衛隊員などは規律と危機管理の経験をもたらします。これらの専門家は、分析的思考、細部にわたる注意力、問題解決能力を備えていることが多く、適切なトレーニングとサポートによってサイバーセキュリティ領域の職種へ効果的に転換が可能です。

4. **ハイブリッド・タレントモデル**：社内スタッフと外部リソースを組み合わせたハイブリッド・タレントモデルを採用することで、サイバーセキュリティチームの過剰な負担の軽減が可能となります。特定の業務に関してはサービスプロバイダーにアウトソーシングすることで、社内チームの負担を軽減し、戦略的な取組みや優先度の高い脅威への対応に集中させることができます。このような対応により燃え尽き症候群の発生を未然に防ぎ、定着率の改善を実現させるだけでなく、社内スタッフの知見に加えて外部リソースの多様な専門知識の活用や、24時間・365日で対応が可能となります。

従業員体験の向上

5. **採用における専門性の多様化**：サイバーセキュリティには、ハッキング技術だけでなく、戦略、プライバシーコンプライアンス、インシデント対応、リスク分析など多様な役割があります。チームが法務の専門家、医療機関のインシデント対応担当者、クリティカル・シンキングを身に付けた人材など、様々なバックグラウンドのメンバーで構成されていると効果的な対応が可能となります。従来の試験偏重の採用ではなく、ブートキャンプや見習い制度を含む柔軟でスキルに基づく採用へ切換えの検討も必要です。画一的な雇用契約はもはや適切ではないかもしれません。さらに、女性、中途採用者、シニア人材、北海道や九州などの地方都市における採用対象を広げることで、従来とは異なるセクターの候補者を惹きつけることとなり、人材の採用を拡大に結び付けることが可能になります。

6. **採用マーケティングの強化**：採用の在り方を再考した後に、適切な人材を効果的に惹きつけられるかを検討する必要があります。現代的な採用マーケティング戦略としては、サイバーセキュリティのキャリアがもたらす社会的インパクトと知的挑戦に満ちたミッションクリティカルな役割として再定義することにより、人材パイプラインを拡大することが可能になります。必要な資格を強調する技術面を重視した職務説明に偏るのではなく、多様性とインクルージョン、成長の機会、重要な問題の解決、デジタル基盤を守る意義のある仕事であることを強調した採用ストーリーが有効です。SNSキャンペーン、自社の魅力や働き方、やりがい、企業文化を発信するプログラム、サイバーセキュリティ専門家による日々の経験を伝えるブログなどは、サイバーセキュリティのキャリアが多様な経歴を持つ専門家にとっても刺激的で意義がある職業として再定義できます。

7. **タレントの定着**：サイバーセキュリティ業務特有のストレスや離職要因に対応した定着戦略が必要です。サイバー人材に適した評価や報酬制度に加えて、明確なキャリアパスを導入する組織は、人材育成と定着に取り組んでいます。技術職に限定しないキャリアパス、つまり、リーダーシップの評価と技術レベルの向上を認める2つの異なる体系を設けることで、昇進には管理職となることが必須となる点を緩和できます。トレーニングプラットフォームへのアクセスや資格取得支援などによる継続的な学習機会の提供は、組織的な能力の保持を可能にし、外部採用依存の軽減に役立ちます。

8. **柔軟な働き方とウェルビーイング**：柔軟な勤務形態やリモートワークによる多様なライフスタイルへの対応は、広範な人材プールへのアクセスを可能にします。リモートワーク環境の整備は、地理的制約を超えた採用が可能となり、海外の専門知識を持つ人材や地方生活を志向する人材の採用も可能になります。このような柔軟な対応は、特にワークライフバランスを重視する若手技術者や女性にとってとりわけ魅力的です。セキュリティ業務では、脅威対応の緊張や重大な意思決定のプレッシャーが常態化するため、柔軟な働き方とメンタルヘルス支援を提供することは、本来離職のリスクが高い人材の獲得・定着に寄与します。

将来のタレントパイプラインの構築

9. **学校教育**：将来のタレントパイプラインに関する課題に対処の方法の1つとして、サイバーセキュリティ教育を基礎レベルから再考することが挙げられます。高校において正式なサイバーセキュリティの基礎教育が行われていないと、若年層における関心を喚起する機会を逃してしまう可能性があります。学校教育においてサイバーセキュリティの基本的な概念を理解するカリキュラムを組み込むことで、早期から興味関心を持つ機会を与え、次世代における認知を高めることができます。デジタルリテラシー、オンラインセーフティ、サイバーセキュリティの基礎などの科目は、サイバーセキュリティのキャリアへの関心を高め、持続可能なタレントパイプラインの構築に役立ちます。

10. **政策改革**：政策改革は、日本のサイバーセキュリティのタレントパイプラインにおける構造的障壁の緩和に役立つ可能性があります。例えば、情報処理安全確保支援士（RISS）認証モデルを改革してRISSの応募者数をさらに増やし、意欲的な専門家の参入障壁を低減できます。経済産業省は、特定の実務経験を有する場合、更新時講習の免除対象を拡大予定です。[17] さらに、特定技能制度[18]にサイバーセキュリティを含めるなど、現行の施策を継続的に見直し、人材育成が加速されるようになることが望まれます。

まとめ：行動を促す提言

国内のサイバーセキュリティがおかれている状況としては、急速に拡大する脅威に対抗すべくますます多くの専門家を必要とする情勢となっています。サイバー人材の拡充に向けた取り組みを継続的に実施しているにもかかわらず、需要は供給を上回り続け、人材不足は拡大する一方です。サイバーに関する課題は、日本のデジタル環境に関する未来を決めかねない状況となっており、国内社会における喫緊の課題となっています。

この人材不足におけるギャップへ対処するには、革新的なアプローチが必要となっており、政府機関、教育機関、民間企業など多様なステークホルダーが連携し、現在から将来における人材不足に対処するため、将来志向の国家戦略を策定することが求められます。策定の過程においては、サイバーを支えるタレント・アーキテクチャの再設計、再考が必要になると考えられます。

今後を見据えると、日本はサイバーセキュリティ分野において、仕事に意義を見出し、社会に貢献するという意識を持つ人材が活躍する未来を実現できる可能性があります。こうした未来の人材像は、性別・年齢・地域といった多様性を持ち、エモーショナル・レジリエンス（困難な状況でも冷静に対応できる力）を備え、デジタル分野にも精通し、さらにAI技術を活用することで人間とテクノロジーの強みを融合します。

10の提言は、全ての解決策とはなりませんが、変革に向けての出発点となり、これから検討を行うための道筋となると考えております。国内におけるサイバーセキュリティの人材不足の解決に持続的に取り組むには、継続的なコミットメント、適切な戦略、従来の手法からの脱却を目指す意思をもって進める必要があります。

企業が成長に挑み、社会が安心してオンライン環境を利用でき、国家安全保障が維持されると、デジタルトラストに基づくより安全なサイバーの未来を築くことが可能となります。日本はイノベーションにより変革を進めてきた歴史があるので、今こそ、国を守る人材の育成とエンパワーメントにおいてもリードしていく挑戦を始める好機になっています。

日本のデジタル未来を守るため、今こそ行動の時であり、国家の安全と繁栄はその実行にかかっています。

お問い合わせ

執筆者・貢献者

著者

Karen Grieve (カレン・グリーヴ)
Director
Deloitte Services Pty Ltd
kagrieve@deloitte.com.au

岩永　朝子
マネージングディレクター
デロイト トーマツ サイバー合同会社
asako.iwanaga@tohmatsu.co.jp

貢献者

Eric Leo （エリック・レオ）
Director
Deloitte Services Pty Ltd
eleo@deloitte.com.au

Nicole Scoble-Williams （ニコール・スコブル=ウィリアムズ）
Partner, Global Future of Work Leader
Deloitte Tohmatsu Consulting LLC
nscoble-williams@tohmatsu.co.jp

園田　健太郎
スペシャリストリーダー
デロイト トーマツ サイバー合同会社
kentaro.sonoda@tohmatsu.co.jp

並木　英之
マネジャー
デロイト トーマツ サイバー合同会社
hideyuki.namiki@tohmatsu.co.jp

プロフェッショナル

桐原 祐一郎
代表執行者
デロイト トーマツ サイバー合同会社
ykirihara@tohmatsu.co.jp

岩永　朝子
マネージングディレクター
デロイト トーマツ サイバー合同会社
asako.iwanaga@tohmatsu.co.jp

脚注

1. Walter Sim, "Hit by wave of online attacks, Japan shifts to 'active cyber defence'," *The Straits Times*, 2025年1月20日
2. 衆議院、*サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案*、2025年5月16日
3. 会計検査院、「各府省庁等の情報システムに係る情報セキュリティ対策等の状況について」2025年9月12日、p. 23、46を参照
4. Rika Kimura, "Audit finds 16% of Japan government IT systems unprepared for attack," *Nikkei Asia*, 2025年9月13日
5. ISC2, *Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen*, 2025年9月10日
6. Ibid.
7. 読売新聞、「防衛省、サイバー攻撃の対処人員２万人に拡充…中露念頭に「能動的サイバー防御」強化」2022年12月05日
8. 経済産業省、*サイバーセキュリティ人材の育成促進に向けた検討会 最終取りまとめ*、2025年5月14日、p. 5を参照
9. 総務省統計局、*統計からみた我が国の高齢者*、2025年9月14日、p. 1を参照
10. 国立社会保障・人口問題研究所、*日本の将来推計人口（令和５年推計）結果の概要*、p. 19を参照
11. ヒューマンリソシア株式会社、ニュースリリース「*ITエンジニアの女性比率、日本は18.8％でOECD加盟国中17位、ITおよびSTEM分野卒業者の女性比率は、OECD最下位と将来の女性活躍が危惧される結果に*」2025年3月7日
12. 厚生労働省、*雇用政策研究会報告書（案）～多様な個人が置かれた状況に関わらず包摂され、活躍できる労働市場の構築に向けて～*、2024年、p. 5を参照
13. 厚生労働省、*高齢者雇用対策の概要*、2024年6月24日
14. 東京商工会議所、*2025年度 新入社員意識調査 集計結果*、2025年4月21日、p. 4を参照
15. Gallup, *State of the Global Workplace: 2026 Report*, 2026年4月
16. 防衛省、*防衛省ＡＩ活用推進基本方針*、2024年7月、p. 8を参照。防衛省、防衛大臣記者会見、2024年7月2日
17. 経済産業省、*サイバーセキュリティ人材の育成促進に向けた検討会 最終取りまとめ*、2025年5月14日、p. 60を参照
18. 外務省、「新たな外国人材の受入れ　在留資格 特定技能」2025年10月14日サイト確認

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイトトーマツ、デロイトトーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jp をご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.com をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
https://www.bsigroup.com/clientDirectory