人材不足の解消

サイバーセキュリティの世界的な人材不足に関する調査

サイバーセキュリティ業界は世界的に人材が不足しています。攻撃の手口は巧妙化が進み、高度な脅威が急増しています。このような脅威に対する防御はさらに難しいものとなっています。サイバーセキュリティの人材不足の状況について、戦略国際問題研究所（Center for Strategic and International Studies、CSIS）がオーストラリア、フランス、ドイツ、イスラエル、日本、メキシコ、英国、米国の8か国で調査を行いました。この調査は、公共部門と民間企業のIT部門の責任者を対象に、セキュリティに対する支出、教育プログラム、経営側の対応、政策の4点について調査を行いました。この調査報告は、より強力で持続性のあるサイバーセキュリティを実施するために役立つ情報を提供しています。また、現在の人材不足を解消し、世界的なサイバーセキュリティを強化するための具体的な施策も提示しています。

重要な調査結果

- サイバーセキュリティの人材不足は世界的な課題です。CSISのレポートによると、調査した組織の82%はサイバーセキュリティの人材が不足していると回答しています。需要と供給のバランスが崩れているため、サイバーセキュリティ担当者の給与が上がっています。米国では、サイバーセキュリティ職の給与はITの他の職種よりも約10%高くなっています。
- 回答者の71%は人材不足が防御策に影響を及ぼしていると答えています。4分の1の回答者は、サイバーセキュリティの人材不足が原因で情報流出や盗難につながり、信用を失ったと答えています。
- 特定のスキルに需要が集中しています。調査した8か国すべてで最も需要の高いスキルは、侵入検知、安全なソフトウェアの開発、攻撃の回避でした。
- サイバーセキュリティの技能を取得する最適な方法はハンズオン トレーニングです。調査を行った意思決定者の約半数は、関連する技術分野の学士号取得を採用の最低条件としています。しかし、回答者の大半は、サイバーセキュリティ技能の向上には学位の取得よりも、実地で経験を積み、ハッキング コンテストに参加したり、専門的な認定を取得するほうが効果的だと考えています。

- 人材不足をテクノロジで補うことが検討されています。回答者の10人中9人は、セキュリティ技術がこの問題の解決に役立つと答えています。回答者の55%は、サイバーセキュリティ ソリューションが進化し、5年以内に組織のニーズを満たすレベルに達すると考えています。多くの組織はセキュリティを外部に委託したり、自動化を進めています。
- サイバーセキュリティに対して政府は十分な投資を行っていません。回答者の76%は、サイバーセキュリティの人材育成に十分な投資が行われていないと答えています。また、サイバーセキュリティに関連する法整備も進んでいないと考えています。

サイバーセキュリティの人材不足をめぐる4つの側面

サイバーセキュリティに対する投資

今後4年から5年の間に、世界のサイバーセキュリティに対する支出は1,000億ドルを超えると予測されています[1]。サイバーセキュリティ技術とサービスに最も投資し、消費しているのは米国の政府と金融機関です。これらの組織は世界中の攻撃者から狙われています。これらの組織は、サイバーセキュリティに莫大な投資を行うことで、人材不足の問題を改善しています。そのトレーニングと雇用は、他の業界のベストプラクティスにもなっています。

教育とトレーニング

CSISのレポートによると、学位の取得をサイバーセキュリティ職の最低条件としている組織が少なくありません。しかし、大半の意思決定者は、実務的なハンズオン トレーニングが技術の習得・向上に最適な方法だと考えています。一方、学生向けに教育プログラムを準備していると答えた回答者は23%に過ぎません。この調査によると、サイバーセキュリティの教育に最も多く投資を行っているのが米国と英国で、投資が最も少ない国はメキシコ、フランス、日本でした。回答者の4分の3以上は、技能の証明に効果的な手段として専門的な認定プログラムの取得を挙げています。また、5分の2の回答者は、技能向上にハッキング コンテストが最適な方法だと答えています。

雇用側の問題

サイバーセキュリティの人材を確保するために、最も重要なリクルート戦略は何でしょうか。最も多かった回答は給与で、トレーニング、IT部門の評判、昇進の機会がこれに続いています。回答者の約半数は、認定プログラムに対する準備時間が取れず、会社から金銭的な支援もないことを従業員の主な離職理由として挙げています。優秀なサイバーセキュリティ担当者を育成するには時間がかかります。このため、多くの組織がテクノロジの導入でこの問題を解消しようとしています。回答者の10人中9人が、サイバーセキュリティ技術の向上で人材不足を補うことが可能であると答えています。また、リスクの評価と回避、ネットワーク モニタリングとアクセス管理、感染システムの修復など、特定のセキュリティ機能を外部に委託する組織も増えています。回答者の60%以上は、サイバーセキュリティ機能の一部を外部に委託していると答えています。

政府の方針

米国、英国、イスラエル、オーストラリアなど、多くの国はサイバーセキュリティの人材不足を解消するための支援を強化しています。大半の国では、サイバーセキュリティ教育の強化に特化した法規制を整備していますが、回答者の75%以上は、サイバーセキュリティの人材育成に対する政府の取り組みは不十分だと答えています。また、ほぼ同数の回答者が、サイバーセキュリティに対する法整備は進んでないと考えています。

推奨事項

既存の教育機関に限定せず、サイバーセキュリティの採用条件を見直す
どの国でもサイバーセキュリティに特化した教育を実施している大学はごくわずかです。CSISのデータが示唆しているように、採用担当者は、学位よりも専門的な認定プログラムやハンズオン トレーニングを重視するべきです。優秀な人材が技能を向上できるように、大学や高等学校でも実践的なサイバーセキュリティ教育を始めるべきです。このようなプログラムを実施することで、政府、民間企業、教育機関が協力してカリキュラムを作成し、インターンシップやトレーニングの機会を増やすことができます。

多様な人材を確保する
様々な調査結果によると、この分野では女性やマイノリティが過小評価されています。また、厳格な移民政策のため、サイバーセキュリティに必要な高度なスキルを持つ労働者の流入が制限されています。米国や同様の移民政策を行っている国で、サイバーセキュリティに従事する労働者を短期間で増やすには、労働許可条件を見直し、マイノリティや女性の雇用も増やす必要があります。ハッキング経験に対する偏見もサイバーセキュリティの人員増加を妨げる要因となっています。ハッキングの経験者は優れた技術と貴重な経験を持っている可能性があります。このような応募者に対しても、より柔軟な対応が必要です。

外部でのトレーニング機会を増やす
サイバーセキュリティの人材を維持するには、継続的なトレーニング プログラムの実施が欠かせません。このようなプログラムがないため、優秀な人材が会社を離れていった例は少なくありません。スキルの向上を望む学生や社員が必要なトレーニングを利用できるように、政府期間と民間企業が協力してトレーニング機会を増やすべきです。

自動化に対する技能を向上する
CSISの調査結果によると、人材不足を解決するために多くの企業がサイバーセキュリティ機能の自動化を進めています。サイバーセキュリティ職には、この新しいプロセスに対応できる能力も求められます。自動化で無駄な作業がなくなるので、サイバーセキュリティの専門家は、より高度な脅威の検出、分析、修復に多くの時間を費やすことができます。

データを収集してメトリックスを改善する
サイバーセキュリティの労働市場と職務を詳しく分析することで、どの業界にも不可欠なサイバーセキュリティ技能を明示した共通の基準を作成し、民間企業、政府機関、教育機関で共有することができます。

まとめ

効果的なセキュリティの実施には優秀な人材が欠かせません。優秀な人材の確保は以前にも増して重要になっています。サイバーセキュリティの世界的な人材不足を解決するには、より多くの優秀な人材がこの職種に応募するように、業界の現状を分析して教育プログラムを改善し、職場環境を整え、トレーニング機会を増やす必要があります。

レポートの完全版は、**mcafee.com/skillsshortage**をご覧ください。

1. http://www.forbes.com/sites/stevemorgan/2016/02/12/cybersecurity-market-outlook-for-2016-to-2020/#185c567a74a4

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com