

《プレスリリース抄訳版》

ISACA（情報システムコントロール協会）東京支部

## 世界的なサイバーセキュリティスキル不足の危機に対し、ISACA が 包括的な“Cybersecurity Nexus プログラム”を発表 ~5社に1社の企業が ATP 攻撃を経験する中、62%の企業は 2014 年のセキュリティ トレーニングを強化していないことが判明~

米国イリノイ州ローリングメドウズ（2014年4月28日）-ISACAの2014 APT 調査の結果、ITセキュリティプロフェッショナルの5人に1人はATP (Advanced Persistent Threat) の標的にされたことがあると回答していますが、企業の62%は2014年のセキュリティトレーニングを強化していないことが判明しました。Ciscoが実施した別の調査では、約100万のセキュリティプロフェッショナルのポストが欠員のままであると推定されています<sup>1</sup>。このような有能な人材の大量の不足は、スキルのギャップによってさらに悪化しています。技術の専門知識に加え、ビジネス戦略とコミュニケーションの専門知識も重視するサイバーセキュリティプログラムはほとんど存在していません。拡大するこの世界規模のスキル不足危機への対応を支援するために、グローバルIT組織であるISACAは本日、北米CACSカンファレンスにおいて“Cybersecurity Nexus (CSX) プログラム”を発表しました。

世界中の主要企業の最高情報セキュリティ責任者やサイバーセキュリティ専門家と協力して開発されたCSXは、セキュリティプロフェッショナルと企業がサイバーセキュリティ調査、ガイダンス、証明書、認定、教育、メンター、コミュニティを検索できる単一の中央ソースという、現在満たされていないニーズに対応します。CSXのすべての資料は、大規模なビジネスコンテキスト内でセキュリティ関連の情報を提供できるように作成されたものです。

ISACA Internationalの次期会長で、CA TechnologiesでITビジネス管理部門の戦略/イノベーション担当副社長を務めるRobert Stroudは次のように述べています。「業界が今すぐサイバーセキュリティスキル不足の危機への対応に動かなければ、顧客データの大規模な侵害やHeartbleed脆弱性のような脅威が組織の防御機能を凌駕し続けるでしょう。ISACAは、サイバーセキュリティプロフェッショナルのキャリアの各段階に見合う専門家レベルのサイバーセキュリティリソースを提供する包括的なプログラムを通じて、このギャップの解消に貢献できることをうれしく思います。」

増加の一途をたどるサイバー攻撃には、巨額の損失がつきまといまいます。World Economic Forum/McKinseyのレポートでは、現在のサイバーセキュリティに対するアプローチを転換しなければ、世界経済が受ける損失額は3兆ドルに上ると見積もられています。<sup>2</sup>

CSX ([www.isaca.org/cyber](http://www.isaca.org/cyber)) では、キャリア開発リソース、フレームワーク、コミュニティ、研究ガイダンス（「Responding to Targeted Cyberattacks」や「Transforming Cybersecurity Using COBIT 5」など）が提供されています。

<sup>1</sup> 「Cisco 2014 Annual Security Report」

<sup>2</sup> 「Risk and responsibility in a hyperconnected world:Implications for enterprises」、The World Economic Forum and McKinsey & Company

CSX プログラムは、サイバーセキュリティセンターで行っている、NIST (米国国立標準技術研究所) や ENISA (欧州ネットワーク情報セキュリティ庁) などの他のグローバル組織との継続的なコラボレーションを反映したものです。ISACA は、バルセロナで開催される EuroCACS/情報セキュリティおよびリスク管理カンファレンスにおいて、EC-Council 主導で行われているサイバーオリンピック倫理的ハッキング大会の世界決勝戦もホストします。

## 次世代のサイバー防御

CSX プログラムは、ISACA が 45 年の歴史で初めて提供するセキュリティ関連認定です。Certified Information Security Manager (CISM: 公認情報セキュリティマネージャー) 資格を含む ISACA の 4 つの認定は、取得のために試験と作業経験証明の両方が必要です。大学の新卒者や分野の変更を希望する IT プロフェッショナルに最適な Cybersecurity Fundamentals Certificate (サイバーセキュリティ基礎認定) を取得するには、将来の雇用主にとってこの分野の専門的技能の客観的証明となる知識ベースの試験に合格する必要があります。

サイバーセキュリティのキャリアには、多数の学生が関心を示しています。先ごろ ISACA 学生支部のメンバーに実施した世界的な調査では、対象の ISACA 学生メンバーの 88%が、ある程度のサイバーセキュリティの知識が要求されるポジションで働きたいと回答しました。しかし、卒業時までにはその職務で必要とされる十分なスキルと知識が身に付くと回答したのはその半分未満でした。

Verizon Enterprise Solutions のグローバルサイバーセキュリティ/コンサルティングソリューション担当副社長で、ISACA ではサイバーセキュリティタスクフォースの議長を務める Eddie Schwartz は次のように述べています。「セキュリティは、CIO にとって常に三大懸念事項の 1 つに数えられていますが、大学レベルの IT およびコンピュータサイエンスプログラムでは、それに比例する時間のトレーニングがサイバーセキュリティに割り当てられていません。現在の実際の教育と実世界のニーズの間には大きなギャップが存在します。業界のサイバー脅威の検知と軽減機能をさらに高めるためにも、このこと自体に即座に焦点を当てる必要があります。」

「企業は、サイバーセキュリティの教育をわずか一握りの大学に頼ることはできません。すべての従業員とエンドポイントがサイバー犯罪者に悪用される危機にさらされている今、セキュリティは誰にとっても同様に重要です。私たちは、脅威からの防御を担当する次世代の人々にとって、できるだけサイバーセキュリティの教育を受けやすい環境を作らなければなりません」と ISACA International の会長である Tony Hayes は述べています。

今後 Cybersecurity Nexus プログラムには、メンタープログラム、実践者レベルのサイバーセキュリティ認定、SDACA ガイダンス、トレーニングコース、NIST によって開発された US サイバーセキュリティフレームワークに関連する実装ガイダンス、プロフェッショナル向けの教育資料などが追加される予定です。

ISACA の詳細については、[www.isaca.org](http://www.isaca.org) をご参照ください。

## ISACA について

世界 180 か国以上、11 万人を超える個人会員から構成される ISACA® ([www.isaca.org](http://www.isaca.org)) は、ビジネスと IT のプロフェッショナルが情報と技術の価値を最大化、またリスクをマネジメントできるよう支援している独立した非営利団体です。1969 年の設立以来、情報セキュリティ、アシュアランス、リスクマネジメント、ガバナンスの提唱者として活動しています。また、ビジネスおよび IT のプロフェッショナルに信頼される情報源として、情報や技術に関する知識およびコミュニティの提供、基準の設定や認証も行っています。世界に 200 の支部を擁し、世界に高く評価されている公認情報システム監査人 (CISA)、後任情報セキュリティマネージャー (CISM)、公認 IT ガバナンス専門家 (CGEIT)、そして Certified in Risk and Information Systems Control (CRISC) などの資格認定を通じ、ビジネスに必須のスキルを提唱、認証しているほか、あ

あらゆる業種の企業が情報や技術を適切に管理、ガバナンスできるよう支援するためのビジネスフレームワーク COBIT®の発展と継続的なアップデートを図っています。

<本件に関するお問い合わせ先>

**CACS/ISRM 2014 広報事務局**（株式会社オズマピーアール内）

業務推進部 鈴木由起子／磯崎有美／工藤麻紀子

Tel : 03-4531-0214    Mobile : 080-9368-5457    Fax 03-3265-5267