NEWS
FOR IMMEDIATE RELEASE

「最新技術がサイバーセキュリティ職員の負担になっている」調査結果が警告。

(ISC)2 が主催したフロスト&サリバン社による世界 1 万人以上の情報セキュリティ専門家を対象にした調査により、深刻なスキルギャップの存在も明らかに。

2011 年 2 月 18 日香港　/-- 世界の情報セキュリティ専門家 1 万人以上を対象に行われた調査に基づく研究によると、ますます多くの技術がビジネスで広く採用されていることが、情報セキュリティの幹部やその部下に試練を与えており、今後数年間のうちに、世界の政府機関、企業、また消費者のセキュリティを脅かす可能性もあるという。

フロスト&サリバン社が行った 2011 (ISC)2(R)グローバル情報セキュリティワークフォーススタディー (GISWS) によれば、携帯機器、クラウド、ソーシャル・ネットワーキング、また安全でないアプリケーションに起因する新たな脅威と、セキュリティについての消費者の懸念解消などの更なる責任により「情報セキュリティ専門家は手一杯になっており、過重労働の職員らのストレスは、まるでダムのあちこちから漏れかけている水のような状態だ」という。

情報セキュリティ専門家のキャリア教育と資格認証における世界のリーダー的存在である非営利団体である(ISC)2 を代理して行われた今回の調査では、業界全体で必要とされているスキルに深刻なギャップがあることも示している。情報セキュリティ専門家はもっと良い訓練が必要であることを認めているが、大多数が、多くの技術は既にセキュリティの観点抜きに展開されてしまっていると報告した。

「現代の組織では、企業がエンドユーザにではなく、エンドユーザが企業に技術を提供することで情報技術の優先事項を規定している」と述べるのは、フロスト&サリバン社のネットワークセキュリティ部グローバルプログラム・ディレクターである Robert Ayoub 氏。「セキュリティに対するプレッシャーが大きくなりすぎた結果できたスキルの溝が、世界的に組織のリスクとなっている」

「しかし、もし今、有能な新規人員を業界に引き入れるための投資を行うと同時に、スキルアップのための専門能力開発への投資も行えば、リスクを減らすことは可能である。調査結果のとおりこういった解決策は進行中であるが、新たな専門家や訓練の登場のタイミングが、世界の民間・公共セクターの重要なインフラを保護するのに間に合うのかという疑問は残る」

「この調査で明らかになった良い点は、情報セキュリティの専門家がようやく経営上のサポートを受け、組織内において基幹データやシステムのセキュリティに対する重要性が認識され予算が確保

されるようになったことである」と Ayoub 氏は付け加える。 「一方悪い点は、彼らに求められることがあまりにも多いということだ。彼らは、僅かな時間の中で最新のセキュリティ脅威に対応するためにスキルを高め、さらに仕事上の要求にも応えなくてはならないのだ」

その他の調査結果の要点は以下のとおり：

- 2010 年現在、フロスト＆サリバン社は、全世界に 228 万人の情報セキュリティ専門家が存在し、そのうちおよそ 75 万人はアジア太平洋地域（A-P)にいると見積もっている。

アジア太平洋地域における専門家の需要は、年平均成長率（CAGR）11.9%で、2015 年までに 130 万人以上に増加し、適切な技能を持った人材への就業チャンスがつくられると見込んでいる。

- 安全性の高いソフトウェアの開発は、世界中の情報セキュリティ専門家にとって、重要視すべき新領域である。回答者の 72%が組織に対する一番の脅威はアプリケーションの脆弱性だとし、一方で安全性の高いソフトウェア開発に携わっているとした回答者は 20%だった。

- 回答者の 70%近くが携帯機器のセキュリティ問題に関するポリシーと技術を持っていると回答し、携帯機器は回答者の懸念事項リストで 2 番目に位置づけられた。調査の結果、携帯機器のセキュリティが当面の間、組織に対する最も危険な脅威となるだろうと結論付けられている。

- クラウドコンピューティングは、技術の実装とセキュリティ提供に必要なスキルとの間の深刻な溝を例示している。回答者の 50%以上が職場にプライベートクラウド環境が構築されていると答える一方で、70%以上がクラウド基盤の技術を守るためには新たなスキルが必要だと回答した。

- 専門家はソーシャルメディアの脅威に対応できていない。エンドユーザのソーシャルメディアサイトへのアクセスに対するポリシーや保護についての回答には一貫性がなく、ソーシャルメディアに対して何のセキュリティポリシーもないとした回答者は 30%以下だった。

- ウィルス、ワーム、ハッカー、そして内部犯行はいずれも、直近の調査である 2008 年の調査時のトップ脅威から大幅に下がった。

- 専門職が継続的に増加する背景には、主に、定常的なコンプライアンスの需要、増大する携帯機器や移動性労働力を通じたデータ損失の可能性、企業などのクラウド基盤サービスへのデータ移行によるコントロール喪失の可能性がある。

- 回答者の 3 分の 2 近くは、2011 年度の情報セキュリティ人員や訓練の予算増加には期待していない。

- 回答者 5 人中 3 人が 2010 年に昇給を受けたと答えるなど、世界的不況にも関わらず給料は順調な伸びを見せた。情報セキュリティ専門家の給料は、アジア太平洋地域において 2007 年の調査以来最高の伸び率 18%となるなど、総じて上昇した。

「セキュリティ脅威を背景に情報セキュリティ専門家の需要がますます増加する中、我々は調査で明らかになったスキルの溝を解決するため、グローバルサイバーセキュリティへのアプローチ方法を変える必要がある。」 (ISC)² Asian Advisory Board の共同議長であり、(ISC)²の特別会員である Lee Jae-Woo 博士こう述べている。「特にアジアにおいては、就業チャンスが増大している。プロフェッショナル需要のギャップを埋めるために、我々は、業界、政府、学界、研究団体に対し、既存の専門家たちが最新の脅威に対処するのをサポートするとともに、高い技術を備えた情報セキュリティの新世代を惹きつけるため協調するよう奨励する 」

情報セキュリティ専門職に関するおそらく過去最大規模の調査が 2010 年秋に行われ、世界中の企業や公共セクターの組織などから 10,413 人の情報セキュリティ専門家が対象となった。内訳は南北アメリカ大陸が 61%、ヨーロッパ・中東・アフリカが 22.5%、アジア太平洋が 16.5%であった。また全体の 45%は従業員 10,000 人以上の組織に所属している。

回答者全体の平均職務経験は 9 年以上であり、回答者の 5%は情報セキュリティ最高責任者など、役員職についていた。 さらにフロスト&サリバン社は、自社の別の主要データソースや方法を使用して分析を補完した。

GISWS は 2004 年以来(ISC)2 が主催した 5 回目の調査であるが、その目的は専門家、企業、政府機関、学界、採用マネージャーなどを含む業界の利害関係者に対し、情報セキュリティ専門職についての有意義な調査を提供することである。

調査の全内容は、下記ウェブサイトでご覧いただけます。
https://www.isc2.org/workforcestudy/Default.aspx.

(ISC)2 について

(ISC)2 は、世界 135 カ国以上に 75000 人近くの会員を擁する、最大級の認定情報セキュリティ専門家の非営利会員団体です。 代表的な資格として世界的に認識されている、Certified Information Systems Security Professional (CISSP(R))のほか、Certified Secure Software Lifecycle Professional (CSSLP(R))、Certified Authorization Professional (CAP(R))、Systems Security

Certified Practitioner (SSCP(R))の資格認定を行っています。 (ISC)2 の認定資格は、個人認証に対する世界基準である ANSI/ISO/IEC 標準 17024 の厳格な要件を満たした初の IT 関連資格のひとつです。 (ISC)2 はまた、情報セキュリティに関する規範をまとめた CBK(R)に基づいた、教育プログラムやサービスも提供しています。詳細については、http://www.isc2.org をご覧下さい。

お問合わせ先：

Kitty Chung
(ISC)2 Asia-Pacific
電話番号： +852-3520-4001
メール：kchung@isc2.org

出所：(ISC)２

Follow (ISC)² on Twitter https://twitter.com/ISC2 and YouTube http://www.youtube.com/isc2tv