PRESS RELEASE（翻訳版）

報道関係各位

2013年2月27日

(ISC)² Japan

(ISC)²® 調査が明かす、有能なサイバー セキュリティプロフェッショナルの不足による世界経済への波及効果

＜2013 年 のグローバル情報セキュリティ人材の実態調査＞

ハクティビズム、サイバーテロ、国家支援型攻撃といった脅威が
セキュリティ上の懸念の筆頭にあがる
CISOらの3分の2が、人材不足によるデータ侵害が頻発し、
多額の費用負担を生じていることを指摘

世界最大の情報セキュリティの非営利団体であり、情報セキュリティ プロフェッショナル認定資格制度CISSP®の運営母体でもある (ISC)²®（「アイエスシースクエア」）は、2013年2月25日に香港にて、米コンサルティング会社ブーズ・アレン・ハミルトン（Booz Allen Hamilton）の協力のもとグローバル市場調査会社フロスト＆サリバン（Frost & Sullivan）が実施した、今年で 6 回目となるグローバル情報セキュリティ人材の実態調査 Global Information Security Workforce Study（GISWS）の結果を発表しました。

全世界の情報セキュリティプロフェッショナル1万2000名以上を対象に実施されたこの調査によって、事業上の制約や、セキュリティ保守の重要性に対する企業経営陣の無理解、そして資格を有する情報セキュリティプロフェッショナルを十分に発掘できていない、などといった要因が重なり、情報セキュリティプロフェッショナルの世界的な不足が、経済に少なからぬ影響を与えていることを浮き彫りにしました。

【全世界の情報セキュリティの専門家の56%が所属組織のセキュリティ部門の人材不足を実感】

回答者が最も強い脅威であると認識しているのは、ハクティビズム（43パーセント）、サイバーテロ（44パーセント）、そしてハッキング（56パーセント）の3点で、うち半数以上を占める56パーセントの回答者が、所属組織のセキュリティ部門の人材不足を感じていることが分かりました。さらに、回答者の75パーセントがサービスのダウンタイムを最大の懸念のひとつとして挙げているにもかかわらず、多くの組織（15パーセント）では何らかの攻撃を受けた場合、どのぐらいで復旧できるかを明確に認識できていないという由々しき事態となっています。調査結果では、サイバーセキュリティに対処できる有能なプロフェッショナルが絶対的に不足していることにより、データ侵害を頻繁に招くことになり、その対応にも多額の費用負担がかかり、当該組織はもとより顧客にも悪影響を及ぼすと警鐘を鳴らしています。

【最も高度なサイバー脅威に対処できる、有能かつ適格な人材の集中的育成が急務】

これについて、CISSP-ISSEP、CAP、およびCISAといった情報セキュリティ関連の専門資格を保有し、(ISC)²のエグゼクティブディレクターを務めるW・ホード・ティプトンは、次のように説明しています。「資格を有する情報セキュリティプロフェッショナルの不足は深刻な状況にあり、近年ますます実感されるようになりました。またかつてない勢いで経済に悪影響を及ぼしつつあります。今回の調査結果でも、プロフェッショナルが不足している現状が、組織の足を強く引っ張る要素となっていると、改めて裏付けるものとなりました。企業の情報漏えいが加速すればするほど、事業の遂行そのものに支障が生じ、また顧客データが犠牲になっていきます。サイバースパイ、ハクティビズム、そして国民国家に対する脅威といった深刻な事態を考慮すると、まさに官民の垣根を越えて、プロフェッショナルの不足を埋める努力をすべき時です。まずは現在そして将来予測される、最も高度なサイバー脅威に対処できる、有能かつ適格な人材を集中的に育成していかなければなりません」

【クラウド、モバイル機器、SNSに対する脅威も懸念】

GISWSではまた、セキュリティに関して十分な訓練を受けたソフトウェア開発者の著しい不足に起因する、セキュリティに対するアプリケーションの脆弱性が、セキュリティを巡る不安の上位を占めていることを、2011年時点のGISWSで既に指摘していました。マルウェアやモバイルデバイスによってもたらされる脅威も懸念の筆頭に数えら

れる一方、比較的新たに台頭している脅威であるクラウドセキュリティ、個人所有のモバイル機器持ち込みを表す Bring Your Own Device（BYOD）、そしてソーシャルネットワーキングなどに対する懸念も目立っています。

このほか、今回の調査で明るみになった主な傾向は次の通りとなっています:

- **情報セキュリティ系の職業は安定しておりかつ将来性があるため、セキュリティ系のキャリアは充実している。**情報セキュリティプロフェッショナルらは安定した雇用に満足しているようです。回答者の8割以上が昨年、勤務先や雇用形態を変更しなかったと答えており、また58パーセントは昨年、給与が上がったと回答しています。世界的に見ると情報セキュリティプロフェッショナルの数は、今後5年間で年間11パーセント以上、うちアジア太平洋地域（APAC）については年間10.4パーセントの割合で堅実に成長していくことが予測されています。全世界における (ISC)² 資格保有セキュリティプロフェッショナルの平均給与は10万1014米ドルであり、これは (ISC)² 資格を持たないセキュリティプロフェッショナルの平均給与より33パーセント高い水準となっています。うちアジア太平洋地域に関しては、(ISC)² 資格を保有するセキュリティプロフェッショナルの平均給与は7万4990米ドルであり、資格を持たないセキュリティプロフェッショナルの平均給与4万8011米ドルと比較して56パーセントもの大幅な高水準を見せています。

- **新たなスキル、より深い知識、より幅広い技術力が必要である。**BYOD およびクラウドコンピューティングの抱えるリスクに対処するためには、多くの専門分野に通じていくアプローチが必要です。回答者の 78 パーセントが、BYOD 技術には重大なセキュリティ上のリスクがあると認めており、74 パーセントは今後のセキュリティ関連のスキルには、BYOD の抱える課題を処理できる能力も含まれなければならないと指摘、また 68 パーセントは、ソーシャルメディアにはセキュリティ上の不安があるため、主なセキュリティ対策としてコンテンツ フィルタリングを導入していると回答しています。

- **アプリケーションの脆弱性がセキュリティ上最大の懸念とされる中にあってなお、ほとんどの組織は安全なソフトウェア開発を重視していない。**セキュリティ系組織のほぼ半数はソフトウェア開発に関与しておらず、またソフトウェア開発のアウトソース先の業者を検討する際には、その業者のセキュリティ対策水準に関する考慮は二の次となっている一方で、69パーセントはアプリケーションの脆弱性を最大の懸念事項として報告しています。

- **セキュリティ上の最重要課題は業種によって論理的に分化している。**回答者のうち銀行、保険、金融系組織では63パーセントが風評被害を、医療系では59パーセントが顧客プライバシーの侵害を、建設系では57パーセントが保健衛生と安全を、テレコムおよびメディア系の50パーセントがサービスのダウンタイムを、それぞれ最重要課題として挙げています。

- **攻撃からの復旧こそ迅速にできると想定している一方、セキュリティ インシデントへの備えにはひずみの兆候がある。**標的型攻撃によって受けたダメージからの回復にかかる時間は、回答者の28パーセントは1日以内、また41パーセントは1週間以内と想定している一方で、大部分の回答者はダメージからの復旧にどのぐらいの期間がかかるか分からないと考えています。セキュリティ インシデントに対する備えについては、2011年の調査時の2倍の回答者が、過去1年間で鈍化していると考えていることが分かっています。

- **知識および知識を証明する資格の有無は、就職や昇進の機会を大きく左右する。**回答者の70パーセント近くが、雇用の際、資格は信頼できる競争力の指標であると見ています。雇用企業のほぼ半数にあたる46パーセントは、志望者が何らかの資格を持っていることを期待しています。また調査対象者の60パーセントは、今後12カ月以内に資格取得を予定しており、うちCISSPが依然、最も人気の高い資格となっています。

【顕在するスキルのギャップを放置し続ければ、経済は間違いなく停滞】

フロスト＆サリバンのストラトキャスト（Stratecast）部門担当バイスプレジデント（VP）であり、今回の報告書の執筆を担当したマイケル・サビー氏は次のように指摘しています。「セキュリティの確保は組織全体の責任であり、情報セキュリティプロフェッショナルは、その知識およびセキュリティ管理上の責任をもとに、組織の導き手とみなされています。情報セキュリティプロフェッショナルは、刻々と変化する脅威とIT業界の現状に、常に最前線にいて適応し続けていかなければならず、すべての事業領域において、なぜ、どのようにセキュリティ対策が必要なのか、ビジネスリーダーを教育していくような戦略的な立場にいます。GISWSが明らかにしたように、組織が日常的に直面するサ

イバー攻撃は、より高度化し、かつ激化していることは深刻な現実問題であり、これに対処していくためには、より多くの熟練した有能なセキュリティプロフェッショナルが必要であることは間違いありません。顕在するスキルのギャップを放置し続けていれば、経済は間違いなく停滞するでしょう」

【実力あるサイバー要員に対する予想以上のニーズを裏付ける調査結果】

これに対し、ブーズ・アレン・ハミルトン上級バイスプレジデントのウイリアム・スチュアート氏も次のように補足しています。「成長するデジタル系企業の要求を満たすためにも、熟練したプロフェッショナルが必要不可欠であることは、ブーズ・アレンも認めるところです。進化し続ける脅威に対抗するためには、人材、プロセス、技術を巧妙に組み合わせていくことはもとより、クラウドコンピューティング、ソーシャルメディア、そして BYOD に伴う機会をとらえることが必要です。今回の調査では、セキュリティプロフェッショナルが企業経営上の意思決定にも影響を及ぼす立場になりつつある昨今の現状を背景に、実力あるサイバー要員に対する予想以上のニーズを裏付ける結果になりました」

【GISWS とは】

情報セキュリティ専門職を対象に実施されてきた調査の中でも最大級のものとみなされている 2013 GISWS は2012年秋にWebベースの調査によって行われました。この調査では 2004 年の初回発表以来、情報セキュリティプロフェッショナルの意見を収集することで、情報セキュリティプロフェッショナルの今後について特筆すべき傾向および機会の詳細な洞察を提示することを目指し、報酬規模、スキルギャップ、研修要件、企業の雇用慣行、セキュリティ予算、キャリアの進化、および、企業、採用責任者、そして情報セキュリティ専門スタッフに有用な情報セキュリティに対する、企業の姿勢について明確な理解を提供することを目的としています。調査の全詳細（英語版）は、こちらよりご覧いただけます: https://www.isc2cares.org/IndustryResearch/GISWS/

特に市場別に編纂した追加データについては、今年中の発表を予定しています。

# # #

●(ISC)² について https://www.isc2.org/japan

※The International Information Systems Security Certification Consortium

米国フロリダ州パームハーバーに本部を置き、東京、ワシントンD.C.、ロンドン、香港にて、情報セキュリティプロフェッショナルの認定ならびに教育活動を展開する、グローバル非営利団体。全世界の情報セキュリティプロフェッショナルに対し高水準の専門性を認定するCISSP は、米国、欧州、また日本の政府機関や民間企業において高く評価され、現在、世界145カ国に約85,000名。(ISC)² Japanとして日本でCISSPを日本語化し、2004年から提供。CISSPの持つ国際レベルでの評価、情報セキュリティを包括的・体系的に理解することが要求される内容への評価などにおいて、高く評価され、現在では日本国内で資格保持者が約1,300名を数える。

●CISSP認定資格とは

(ISC)²（International Information Systems Security Certification Consortium）が認定を行っている国際的に認められた情報セキュリティプロフェッショナル認証資格。

2004年6月には、米国規格協会（ANSI）よりISO/IEC17024の認証を受ける。

CISSP認定資格は、情報セキュリティの共通言語とも言える『(ISC)²公式CISSP CBK（Common Body of Knowledge：共通知識分野）』を理解している情報セキュリティプロフェッショナルのみに与えられる資格。

■報道関係からのお問い合わせ

(ISC)² Japan（アイエスシースクエア ジャパン） 担当: 衣川

〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー

電話番号：03-6757-0138 FAX番号：03-6757-0136 Eメール：tkinugawa@isc2.org