第３回目　サイバーセキュリティー研究会
実施日：２０１８年０８月０３日（金）
発表者：江口　純一氏　独立行政法人情報処理推進機構　理事
テーマ：日本のセキュリティ人材について

独立行政法人情報処理推進機構（IPA）は経産省と共同で企業組織経営者を主な対象にした「サイバ゛ーセキュリティ経営ガ゛イド゛ライン 」（初版２０１５年１２月）を発行した。以降セキュリティ投資を必要不可欠な経営戦略として位置付け、サイバー攻撃に対して経営者が行うべき一連の対応や詳細な実施手順を施すなど、セキュリティリテラシーの向上と対策強化を行なっている。同時にセキュリティに関する実践的知識・技能などを有する人材の育成・確保にも取り組んでいる。今回の研究会は、現在理事を務めている江口氏に講師を依頼し、産業界における IT 人材の動向の調査報告と IPA による具体的取り組みについてご発表戴いた。

日本のサイバーセキュリティ人材をめぐる現状

東京オリンピックを２年後に控える中、日本国内においてサイバーセキュリティ人材の不足がメディアによって度々指摘されている。経産省の『IT 人材の最新動向と将来推計に関する調査結果』によると、セキュリティを日常の業務として担当する社員は現在ユーザー企業や IT 企業合わせて約２８万人いる。双方ともに毎年頭数は伸ばしているものの、絶対量な総数はまだ足りてないとされており、２年後の東京オリンピックでは３５万人程度となっている。政府のターゲット見積りと現状の政策による将来的予測との開きが２０万人という数値となって表れている。[1]IT 人材の動向に関する調査するべく、IT 企業、ユーザー企業、インターネットサービス企業を中心に計 7,000 社（うち 2,512 社回答）の企業に対してオンライン上でアンケートを行なった。以下のような結果が得られた。

1.セキュリティ人材の確保状況

＜人材育成・確保についての現状＞

IT 企業、ユーザー企業双方ともに必要な人材を確保できていない（IT: 48.9.% ユーザー：55.3%)という回答が確保できている（IT:27.7% ユーザー:20.8%）という回答を大きく上まった。企業全体では、業務上においてセキュリティ担当者・人材が不足しているという回答が４２％に上った。

[1]参考までに米国におけるセキュリティ人材は、全体で３０万人ほどの募集があるが、セキュリティ担当・労働者の総数は７６万８千９６人で不足幅は全体の２８％となっている。

＜育成方針について＞
人材育成・確保方針については、どちらも社内育成型（既存人材：IT:73%　ユーザー:53%)が最も多く、その次に中途採用（IT:32%　ユーザー:26%)、外注（IT:23%　ユーザー:29%)となっている。新卒に対する育成については IT（26%)とユーザー企業(10%)で開きが見られている。

＜育成についての具体的な取り組み＞
IT 企業の大多数は研修受講やスキル指標、資格取得制度など具体的な取り組みを確実に行なっているのに対して、ユーザー企業については何の取り組みも行っていないとの回答が全体の調査の３分の１に及んだ。

<セキュリティ人材不足が解消されない主な理由＞
回答した企業全２７６９社のうち、業務の繁忙（情報セキュリティへの人材配置や増強まで手が回らない）や情報セキュリティ業務における適任者が少ないことが大きな理由として上がっている。

<社内における CISO の役割と現実＞
CISO の経営的な役割を期待する企業は回答全体（２６３社）のうち７５%、経営と技術的役割の双方を期待する企業は全体は４４%に上った。これに対して、CISO
が期待される役割を果たしていると回答した企業は６割未満（セキュリティガバナンス体制の構築・運営：５５.1%　セキュリティ計画・予算策定と評価：５８.６%　セキュリティ要員の確保・育成　４５.２%)で期待と大きくかけ離れていることが判明した。

<事例：産業技術総合研究所＞
去る２０１８年2月１３日、産業技術総合研究所の情報システムがネットワークシステムの広範囲に渡って外部から不正アクセスを受けていたことが発覚。７月２０日に報告書が公開された。内部調査によると当時のセキュリティ管理体制に大きな問題があり、
１）全組織上の最高情報セキュリティの統括責任者（CISO）と研究部門全体を統括する情報基盤におけるセキュリティ責任者との間でコミュニケーションが密に行われていなかった２）情報基盤部におけるセキュリティ担当窓口が不明確だった３）基盤部における情報技術の専門家不足４）研究部門における情報セキュリティ責任者のガバナンスが不明確の４点が挙がった。皮肉にも情報研究を行っているにも関わらず、各部門において情報セキュリティに精通した人材を配置できないという実体が浮き彫りになった。
この教訓を生かすべく IPA では以下４つ対策を取り上げた。
- CISO の役割と経営上の機能性強化
- 情報セキュリティ委員会の格上げ

- 対策部署の明確化
- 組織全体としてのセキュリティリタラシー向上を目指した部署間の連携推進

2. IPA における具体的な取り組み

現在行われている取り組みは以下の通り。

＜組織経営における対策改善＞

セキュリティリスクの認識、管理体制の構築（セキュリティ担当者と経営者との仲介役として CISO や各責任の明確化）、人材育成の資源確保のための予算確保の検討を最新版経営ガイドライン（Ver2.0）に盛り込んだ。

＜３大事業の推進＞

社会インフラと産業基盤におけるセキュリティの抜本的強化を図るべく、人材育成（セキュリティ認識の自己啓発、スキル養成、有識者・専門家との連携、経営層へのアピール）、制御システムの安全性・信頼性検証、驚異情報の調査分析（攻撃手法の分析、ホワイトハッカーの協力を得て高度なサイバー技術の調査・研究）推進。

＜産業界におけるサイバーセキュリティ人材の理想的スキル＞

IT と制御システムの双方において対策必要性の分析・把握力とプロジェクト推進力を融合した総合的なスキルの醸成。

＜中核人材育成年間プログラム＞

現在 IPA にて行われている人材育成事業としてビジネスと情報セキュリティの中間的位置で実務に携わる中核人材育成を目指したプログラムの紹介

＜新 IT スキル標準（ITSS＋）の提唱＞

人材の専門性のレベル別分類・業務上におけるスキル・知識の体系化