産業サイバーセキュリティ研究会
ワーキンググループ2(経営・人材・国際)(第1回) 議事要旨

1. 日時・場所

日時:平成30年3月16日(金) 9時00分～11時00分

場所:経済産業省 本館17階第1共用会議室

2. 出席者

委員 :梶浦委員(座長)、岩下委員、上野委員、小原委員、小松委員(代理:岡本様)、武智委員、塚本委員、名和委員、林委員授、藤原委員、丸山委員、宮嵜委員、宮下委員、湯淺委員、横浜委員(代理:荒金様)

オブザーバ:内閣官房 内閣サイバーセキュリティセンター、警察庁、金融庁、総務省、外務省、文部科学省(欠席)、防衛省、独立行政法人情報処理推進機構

経済産業省:商務情報政策局 伊東大臣官房審議官、奥家サイバーセキュリティ課長、土屋サイバーセキュリティ課企画官

3. 配付資料

資料1 議事次第・配布資料一覧

資料2 委員等名簿

資料3 本ワーキンググループの運営について(案)

資料4 事務局説明資料

4. 議事内容

冒頭、伊東審議官から以下のとおり挨拶。

- サイバー攻撃の起点の急激な拡大、攻撃手法の高度化に対し、産業界の皆様と一体となった取組みを進めるため、経済産業省では、日本の産業界を代表する経営者等を構成員とする「産業サイバーセキュリティ研究会」を設置し、昨年末に第１回研究会を開催した。
- さらにそこでの議論を具体化していくため、先月、研究会の下に設置した WG１（制度・技術・標準化）を開催し、サプライチェーン全体のリスクポイントを分析し、産業活動において必要なセキュリティ対策を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の検討を開始したところ。
- しかし、これらの取組を実効的なものとしていくためには、産業サイバーセキュリティ対策の基盤となる、経営層のコミットメントと、人材育成が不可欠。研究会においても委員の皆様から、サイバーセキュリティ対策における経営層の意識喚起の重要性、対策を支える多様なサイバーセキュリティ人材育成の必要性について指摘をいただいた。
- また、サイバーセキュリティの分野においては、国境を越えて行われるサイバー攻撃に対応するため、そして海外の進んだ知見を我が国の政策に取り入れていくためにも、国際連携が極めて重要。
- 本日ここで、お集まりいただいた有識者の皆様、関係省庁とともに、我が国の産業サイバーセキュリティ対策の基盤となる、経営者の意識喚起、多様なサイバーセキュリティ人材の育成、サイバーセキュリティ分野の国際協力基盤の整備についての検討を開始したい。活発な議論を宜しくお願いする。

次に、梶浦座長から以下のとおり挨拶。

- 経団連では、サイバーセキュリティ懇談会で三年半にわたって議論し、３回提言を行った。これに関しては、

政府もそれなりに応えてくれたと思っている。やはり、産官だけでなく、学も巻き込む必要があり、社会全体で産業サイバーセキュリティを高める必要があると痛感している次第。

・ 経営、人材、国際と活発に議論をして頂き、その成果を広く社会に、世界に示していきたいと思うので、積極的な発言をお願いする。

事務局から、宮下委員から資料の提出あり、本日は横浜委員の代理として荒金様、小松委員の代理として岡本様が出席との発言があった。

事務局からの資料３及び資料４による説明に続き、以下のとおり自由討議を行った。

〇宮下委員

・ ユーザを代表している立場として参加している。資料を用いて説明する。2 つの視点で紹介したい。一つは企業 IT 動向調査からみた情報セキュリティの動向、一つは JUAS の企業 40 数社で議論した中から出てきたユーザ企業の情報セキュリティの課題について。
・ 動向調査について、現時点で未公開だが 4 月下旬に公表予定。約 1000 社が回答。調査によれば、情報セキュリティ関連市場は大きく増加している。16 年度と比較すると 17 年度に、2 割以上増加する割合は減っているが、増加または現状維持が 97%となっている。大きな割合で伸びている。35%の経営幹部がセキュリティリスクを認識。売上高別だと、1 兆円企業等は 9 割近くが認識、1000 億から 100 億の企業では 29.4%、100 億円未満は 21%。規模の小さい会社の経営幹部の認識を高める必要があると思っている。
・ 経営幹部にセキュリティリスクを認識してもらうための課題として、一番多いのはセキュリティ対策の必要性や重要性を説明しづらいこと。同程度あるのがセキュリティに対する経営幹部の意識の低さ。CISO の設置状況も企業規模で大きく異なる。大企業では積極的に設置しているが、中小では設置が少ない。想定する対応部門は、昨年の調査では一昨年に比較して CSIRT が 3 倍に増えたが、今年は若干減った。CSIRT と名付けなくても、通常の IT 部門・サービス部門で対応している。特徴は、製造業と非製造業で大きく違うこと。製造業のセキュリティ対応が遅れている。サイバー攻撃の経営へのインパクトについては、多いのは社会的信用低下で、77.8%。インシデントの発生状況については、若干発生が下がっており、インシデントに対する対応が進んできているからと推測される。
・ 対策ができているかについては、内部犯行への対応が進んでいない点が挙げられた。今後のセキュリティ対策強化をどうするかという問いに対しては技術的対策強化が最も多い。対策強化を実施しない理由は、「不安がない」が多いが、「コストが高い」、「人材の不足」、「どうしたらいいかわからない」、「リスクが把握できない」、等がある。
・ 人材の充足状況は、改善がかなり進んできている一方で、不足している人に聞くと、人材充足の目途は立っていないとの答えが多く、人材確保が難しくなっている。
・ サイバーセキュリティ保険の加入状況については、規模の大きい企業は保険に入っていない傾向。保険料が高いことと、それなりに対策をとっているからだと思われる。
・ JUAS では、３つの WG に分けてセキュリティに対する課題認識を議論している。製造業 31 社、非製造業 11 社が参加。そこでの課題認識では、全体として製造業では、国内の対策は何とか手を打っているが、グローバルでのセキュリティ対策がまだまだ進んでいないこと。非製造業では、サプラーチェーンにおける、委託先を含めてのセキュリティ、クラウドに乗せるときのポイント、評価をどうすべきか等の課題がある。経営ガイドラインも出ているが、どこまで対応すべきか悩んでいる。誰が何を判断するのか、要求水準とベンチマークが欲しいという声がある。リテラシー、ガバナンスについても課題意識がある。非製造業では、企業間の連携、情報共有が重要との声が多い。近々では 2020 年の東京オリンピック・パラリンピックへの対

応は、どこまで対策をすべきかわからない、など。さらに内部犯行などにも課題を持っている。

○岩下委員

- 私は 33 年ほど日銀に勤務し、うち 25 年ほどは情報セキュリティの研究と実装を担当していた。人材を必要とする側、人材を育成しなければいけないという企業側の視点だけではなく、そこに人材を提供する側、提供されているエンジニア側の視点も交えてコメントしたい。
- 情報セキュリティ分野の人材が足りないことはずいぶん前から言われている。かつて、情報セキュリティ大学院大学で講演した際に、学生に情報セキュリティを実践するための心構えとして、「不人気に耐える力」が大事だと言ったことがある。情報セキュリティ担当部署が注目されるのは事件が起きたとき、重要インフラが止まったなど、様々なアクシデントが起きたときに、基本的に後から駆けつけて何とかする仕事が多い。事後対応では間に合わないことが多く、結果として、警察や消防と同じように後から駆けつけて、なんとかインシデント対応することが主要な仕事にならざるを得ない、上手くできて当たり前という厳しい立場。一方、平時にはあまり重視されず、遊軍扱いされてしまう。しかし、どうしても必要な部署でもある。
- CSIRT や自社の情報部門などのレベルを上げることはきわめて重要であり、人材を豊富に貼り付けることも大事だが、一方で、企業は利益を求めるので、有効性がある組織かどうかも十分考える必要がある。日本企業の意識の問題として、情報セキュリティが極めて重要で、そこにきちんとリソースを貼り付ける必要があり、それは高いものだということが経営側に理解されていない。多くの場合、従来型の紙と手でやる作業ならばサイバーセキュリティは関係ないという傾向に陥りがちで、それが結果として日本のイノベーションを止め、サイバーセキュリティ対策も後手に回るという悪循環となっているように思える。
- 先ほど、セキュリティを強くすることは経済を成長させるために必要だという議論があったが、これは定性的にも明らか。様々なイノベーションを取り込んでいくためにも高度なセキュリティを各社で実装していくことが必要であり、そのためには高度な人材が必要というのが当たり前だということを、一刻も早く広い企業に当然の常識として広めることが、情報セキュリティを担っていく若者達が存えるために必要なことではないか。
- その上で、彼らが今後年次を重ねるとどうなるかも考えて頂きたい。若い頃は情報セキュリティ部門で勤め、歳をとったら会社から離れて欲しいというようなことを言う人がいる。人生設計もあるので、キャリアデベロップメントまで含めた対応を企業で考えてもらいたい。これは情報セキュリティの専門家を必要とする企業にとっても大切なことである。

○林委員

- 情報セキュリティ大学院大学を設立してから約 13、4 年になるが、その間、仕事の性質として受身にならざるを得ないところがあった。プロアクティブにいかなければいけないという時代変化をなんとかもたらしたいが、なかなかそうはいかない。とはいえ少しずつ知見が溜まってきているので、これを世間にどのように理解してもらうか。例えば、法学者の視点としては、情報セキュリティ六法が仮にあるとすると、世間のひとの見る目がずいぶん変わってくるのではないかと思う。最終的には法律的な担保があるということが分かることに意義がある。
- 経済産業省は、約 7 年前に情報セキュリティ関連法令の要求事項集を出している。これを書かれたグループのリーダだった岡村弁護士とは、7 年経っているため改訂版を出す必要があるという話をした。大事なのは、サイバーセキュリティ基本法が制定されているのにその部分から始まっていないこと。変化の激しい時代には問題。また、所管の問題もあるのだろうが、総務省関連のプロバイダ責任制限法や、そのガイドラインや通信の秘密の関連は、避けているようだ。NISC でやった方がいいのかという議論もあり、どこであっても

良いので、そういったものを纏めてドキュメントとして公開するべき。

- 今は法律に関して話したが、他のところでも同じように基礎的なところを含めてやるべき。例えば、文書の扱い方のノーマルなプロシージャを示して、それに逸脱が起きるとセキュリティが破られる可能性が高いことなどを教えていくのが基本ではないか。それが、第二フェーズに入ったセキュリティ問題に対する教育分野での取組の基本となりえるという感じがしている。
- ちなみに、昨日、司法研修所に講師で呼ばれた。30 代半ばの裁判官の方々に、何を教材にして話すかということを教官と話した折に、やっぱり彼らの発想では六法全書が机の上にあって、講師の話を聴きながら必要に応じてリファーするのが基本だが、それができない。

○小原委員

- この委員の中では、攻撃される側の企業の主たる責任者なので、その立場からお話申し上げたい。私自身はセキュリティ対策室で仕事をしているが、その他にプライバシー、個人情報の問題、IT セキュリティの問題、データリスクマネジメント、簡単に言うとデジタルリスクを扱っている。その観点から、現場として思ったことを話したい。
- 一つは経営層の関与のところで、民間企業で経営会議や各種委員会があるが、取締役会は別格で、ここで議論すると変わっている。社外取締役の意見は広く、経験に裏打ちされていて深いので、勉強になるし、会社が動くという意味では大きなイベント。外国人の取締役もいて、経営上の優先順位や報告すべき点を明確に話されるので、大きな指針となる。
- 共助という話があったが、商社の間で ISAC を構築しているが、信頼関係の醸成が非常に難しい。コツは、技術を共有することだが、それをリアルタイムでやることがポイントではないかと思う。ベンチマークは色々あるが、状況はリアルタイムで変わるので、それを仕掛けとして持てるかが決め手。
- 企業経営におけるサイバーセキュリティ位置づけ強化に関しては、先般、経団連のサイバーセキュリティに関する懇談会において梶浦座長の下で示されたように、成長ドライブとして、Society5.0 とかみ合わせた格好のメッセージの方が企業の中では消化しやすいと思う。リスクサイドはもちろんあるが、リスクのコントロールができていないと成長ドライブにつながらないという議論は比較的通りやすい。リスクサイドのみに寄った議論は人気がない。
- 本日はサイバーセキュリティ経営ガイドラインについての詳細な説明はなかったが、このガイドラインの項目の中では、サプライチェーンを含めたマネジメントの項目が最重要と思う。商売をしている会社なので、取引先の影響を受ける。当然自分たちも守らなければいけないが、顧客、取引先をいかに守るか、いかに一緒に対処していくかが最大の課題と認識している。ここに関しては、ガバナンスと違う仕組みや仕掛けが必要と考える。
- 人材については、修羅場をくぐった経験があるかどうかで違うと思っている。修羅場をくぐった人同士はきちっとコミュニケーションできる。グローバルグループで対策しているが、外国籍の方と仕事することが重要になってくる。国際的に修羅場をくぐった人の仲間を作ること、その場を作ることが課題であり、方策ではないかと感じている。
- 最後に、国際政策の話があったが、海外の会議などに出ているが、2 つの視点が必要と思っている。一つはマクロの視点で、意外と通商政策という考え方が馴染むのではないか。ヨーロッパと米国の議論をみていると、国防を一旦横においてみると通商政策でどういった利益があるか、それはどういう対価で得られるかという議論が根底にあるように思われている。一方、ミクロは、証拠の取り方が非常に重要になってくる。どうしても事件が起きるので、証拠を基点として対処していくが、その証拠が正しく取れているか、どうすれば正しい事実認定ができて、対処ができるかという厄介な問題があり、実務上は苦労する。最後に、地域ごとの

話があったが、ここでは触れてない国々もビジネス上では重要な国々もある。従って、まさに面で如何にグローバルなビジネスを支えることができるプラットホームを考えてもらえるか、サイバーの対策上で仲の良い国とだけ商売できると良いが、なかなかそうもいかない。そこをどう交渉していくか、そこで先ほどの通商問題も入ってくるが、現在このようなことについて問題意識を持って考えている次第。

○名和委員

- 本 WG の設置の目的・狙いに「経営層の意識喚起」とあるが、これに対する具体的な対策が見当たらない。経営者にどんなに言っても、啓発が進むものではない。すばらしい言葉を並べても、企業経営の多忙さの中で時間が経つと忘れることが多い。ここ半年間、様々な経営者へのレクチャー、経営者のみのカンファレンス、プレゼン等行ってきたが、経営者の意識向上が確実に定着することは期待できない。
- 資料 4 の 41 ページ「既存の人材育成施策のターゲット」の経営戦略部門の下の方にある「セキュリティの高度なスキルを有する人材」、「セキュリティの理解をもって高度な経営判断を補佐する人材」を経営者が強く求め始めている理由の一つに、経営層自らがしない・出来ないことを前提にした姿勢が見え隠れしている。経営戦略部門の「高度な経営判断を補佐する人材」は、企画立案させる人材という美しい言葉で片付けられることがあるが、自ら考えずにト書きを作らせるような人材という見方もできてしまう。
- 経営層が自分で考えるきっかけは、「痛い思い」（経営的な被害）をしたときだけという印象が強い。「痛い思い」をするのかな、と実感を持って考えさせる仕組みが重要。
- 具体的には、投資家あるいは大きな仕事を提供している大企業からのコストを伴う圧力が必要。
- 最近投資家からサイバーセキュリティについての問い合わせ多くなっている。彼らもセキュリティが利益に繋がると認識し、相当勉強されている。それを利活用することも考えてはいいのでは。
- 経営層の意識喚起については、これまでも毎回このような議論があった。美しい言葉を並べるだけでなく、現実を見て率直に出来ること、具体的な成果の出る施策としては、投資家に積極的に関与していただくのも重要ではないか。

○梶浦座長

- 4 月に経団連主催で経営者向けのセミナー行う。投資家や取引先から言われないと経営者が動かないのは事実。

○武智委員

- 本日のプレゼンの内容には総じて同意。
- IT の投資をちゃんとしているところはセキュリティをちゃんとしている、これが鍵なのかと思う。
- 役割を考えると、経営者はビジネスに直結していないと考える対象にならない。Society5.0 をベースとしたサイバーセキュリティの懇談会の提言にも書かれているが、ビジネスにどう IT を活用するか、その反面として、セキュリティをどうするかという裏表の関係であることを理解する必要がある。
- 人材育成に関して言うと、もう少し細かく、どんな人材が何をしなければならないか、きちんと整理していかないといけない。経営にとってサイバーセキュリティがどのような意味があるのか、米国の MBA にセキュリティのコマが入ってきていると聞いたがこれをどうとらえるか。経営的な視点でセキュリティがどのような意味を持つかであって、技術を語っている訳ではない。そういう教育も必要。
- 産業横断人材育成検討会でも人材定義をやってきたが、実際にオペレーションする層とマネジメントする層、事業を考える層で分けて考える必要がある。整理した上で話さないと空中戦になってしまう。
- また、中小企業対策もやらなければならない。産業横断の取組は大企業がメインだが、日本の企業全体のう

ち、年商 5 億以下の中小企業が 92%で、そこをどうするかが問題。中小企業の経営者にセキュリティが大事と言ってもなかなか説明できないし、されても理解できない。ビジネスに直結することを理解してもらう必要があるが、例えば、これを取らないとビジネスできないというサーティフィケーションを設定することなどが考えられる。北風と太陽ではないが、こうしないと損するという北風のようなところをどうするかについても、議論しづらいが具体的に話してもいいと思う。

・ サーティフィケーションを設定するときに難しいのは、どのレベルまで見るのかという点だが、セキュリティ対策を任せるベンダ側のサービスの認定もあるかもしれない。ただ、サービスそのものの判定基準は難しいので、どういった人材を抱えているかで判断せざるを得ないと思う。セキュリティスペシャリストの人材のサーティフィケーションを構築すること、見える化していく仕組みづくりが重要。具体的に議論ができればと思う。

○梶浦座長

・ 今まで触れにくかったことも、この場で議論して欲しい。そういった話になった場合を考えて原則非公開という立て付けにしている。この会だけは非公開、このプレゼンだけは非公開ということもできる。

○湯淺委員

・ 民事訴訟でやりとりしている膨大な紙資料のオンライン化、在外投票や交通不便な離島でのインターネット投票の活用など議論がされているが、「セキュリティが危険」、「セキュリティが不安」などセキュリティを理由に消極的な声がある。どこにどういうリスクがあるのか知識もなく、危険だ、危険だと煽られているだけというのが現状。
・ その理由を考えてみると資料 4 の 41 ページのピラミッドの図で、将来の経営層や官公庁のトップになる人材は総務部門のところにポストがあるので、左側の所を渡っていく。
・ 左側と右側との継ぎ目を作らないと、経営層はいつまでたっても何の知識もないままで、ある年齢になると上に上がってしまう。官公庁その他でも、何の知識も無い人が決定権を持ってしまう。
・ かろうじて左右のつなぎに目になっているのが、個人情報保護法や GDPR の問題だが、これだけでなく、もっと左右のつなぎ目をつくらないといけない。
・ 右側とは異なり、左側にはセキュリティに関連するポストがない。ポストがないので研究者や人材が育たない、人材が育たないのでポストができない、という悪循環になってしまっている。左側に行く文系の学生の IT リテラシーは、最近むしろ落ちているように感じる。キーボードも打てない学生が増えているというのが話題になったが、実際に落ちていると感じる。産業界が、左側を進む人材にどのような知識を身に着けて欲しいかを聞いて、産業界のニーズに応えられるように対応していきたい。大学や大学院で履修した科目を、各種の資格試験で科目認定する機会を増やすことで、産学が連携できるだろう。

○宮嵜委員

・ SOMPO グループは 2 年前からデジタル戦略に力を入れている。
・ 車の自動運転など、IoT でモノがつながって便利になるが、保険のリスクが変わってくる。自動運転になると自動車保険自体のレートが変わってくるのではないかと研究を始めたが、研究を始めて直ぐに、避けて通れないのはサイバーリスクであると分かった。
・ この分野で進んでいるのがイスラエルだと聞いて、IT イノベーション、サイバーセキュリティ庁などの人とも議論してきたが、日本と環境が違うことを肌で感じる。
・ それなりに対策はしていても、ハッカーが本気でやると大事な情報が取られるということこそが経営リスク。

これを経営としてどうカバーするかが課題。

- 中小企業の意識については、弊社で中小企業にアンケート取ったところ、何をやればいいのか分からない、金をかけたくない、取られるものもない、という答えがほとんどであった。顧客の安心、安全、健康をサービスとして提供するのが会社のミッションであり、中小企業を含め、どうやって安心、安全を提供するかがキーだと思っている。中小企業にリーチしやすい保険の営業店・代理店を通じて、中小企業の経営者にサイバーセキュリティが大きなリスクになることをどう伝えていくかが、課題と思う。
- 保険というキーワードが出てきたが、保険を引き受けるに当たり、データが集まっていないため、集積リスクを読めないというのが現状。これまでの経験から、復旧するための費用、個人情報が流出した時の費用などの評価は一定できるが、BCP を含めた損害額をどう評価するかなどが課題。
- サイバーセキュリティ対策をしている企業としていない企業でどれだけリスクが違うのか、またこれに応じてどれだけ保険の引き受け額に違いを設けられるのかを保険会社としてきちんと見ていかないといけない。
- 人材に関して、イスラエルに行くと、産官学が連携し合っているのを肌で感じる。官が企業と学校を同じ場所に誘致して、企業と学校が一緒に研究していて、そこの学生を企業が研究に使っている。日本では今どういう状況で、どこを目指していくのか、一緒に考えたい。

○横浜委員代理　荒金氏

- 2 点申し上げたい。
- 1 点目は人材育成について。IT だけでなく、広くビジネス全般を見られる人材にセキュリティの観点が必要だと感じている。資料 4 の 41 ページの右上の方に書いてある、ホワイトハッカーを作るような人材育成のプログラムはたくさんあるが、それだけではビジネスとしては回らない。ピラミッドは上に行くのが全てではない。広報担当者もセキュリティの観点がなければ、ビジネスを救うマネジメントには十分ではない。
- もう 1 点は共助、その中でもまずは情報共有。弊社は IT 企業だが、ユーザ企業の側面もある。グループ会社との情報共有のために NTTCIRT から情報を流すが、グループ会社でも情報を受けきれないところもある。情報共有も大事だが、その次にそれをどう使うのか、どう連携させるのかを考えないといけない。利用するツールを充実させるなども工夫のひとつ。

○藤原委員

- 日本サイバーセキュリティ・イノベーション委員会（JCIC）として貢献できるところとして産学連携、国際連携について申し上げたい。
- 1 点目の産学連携について、一歩進んだ産学連携が必要との話があったが、シンクタンクとして、産業界と大学がより本気で意見をぶつける場をつくって行きたいと考えている。
- 産業界が必要とする人材について人材の可視化ツールが必要との話があったが、これについては慶応大学、地方の大学などと議論を進めている。
- 資料 4 の 41 ページの左側全体についての話が出ているが、情報だけでなく、経営、マネジメント、法律、心理学など幅広いアカデミアの方々が交流する場を構築したいと考えている。産業界と大学が一体となって人材育成にあたっていけるような活動をして行きたい。
- 2 点目、国際連携について海外への情報発信が必要との話があった。発足した昨年の 11 月以来、海外の機関から意見交換を求められている。海外の動きを日本に紹介するとともに、日本のイニシアティブを世界に紹介していきたい。例えばこの会議での議論などをタイムリーに海外でのシンポジウムなどで紹介したい。
- JCIC としても他の海外の団体と連携する予定であり、是非一緒に取り組みたい。

○塚本委員

- 人材に関して、IT ベンダでセキュリティを担当していた人が NISC にいって、そのあと他の製造業に転職されて厚遇されて行くとか、そういった話をよく聞く。転職市場は最近セキュリティ人材が売れている。「セキュリティ人材は当面引っ張りだこ」とか、「セキュリティ人材を紹介する」とかのキャンペーンを張ってみると、人材が集まるかもしれない。経営者も目を引くし、学生も興味を持つのではないか。
- 日米の企業を比べると、日本は性善説で、米国は性悪説的な対策をしているように見受けられる。宮下委員の資料によると製造業は経営や基盤やコミュニケーション、非製造業は内部犯行とあったので、同じ日本の企業の中でも 2 つに分かれるようだ。一方で、アメリカの企業は、製造業であっても内部犯行を意識した対策をしている。この辺はマインドセットを変えるとよいのかもしれない。
- 国際については、日米の政府間の経済対話の枠組みの中でも IT の項目が入っていると認識している。ASEAN に共通の認識を広めていくことも重要なので一緒にやっていけるとよいと思う。また、今回は無かったが、中国の話も聞いてみたい。

○小松委員代理　岡本氏

- 日本商工会議所は全国 515 商工会議所で構成され、会員企業数の合計は 125 万。主に都市部を中心に立地しているが、会員企業の多くは中小企業。従業員数では製造業で 20 人以下、サービス業で 5 人以下という小規模事業者が経営指導のターゲットとなる。中小企業ではセキュリティ対策以前にそもそも IT 活用が進んでいない。課題は、人材がいない、何をすべきかわからない、費用対効果が見えない等。国の補助金も紹介し、IT 活用を進める運動をしているところだが、それが終わってから次にセキュリティということでは、また今度は何をしたらよいのかというところに戻ってしまうため、IT 活用の推進と一緒にセキュリティ対策にも取り組む必要がある。IT の推進だけではブレーキの無い車を売るようなものなので危険だと言う人もいる。
- 自社は紙と手で仕事をしており PC は使わないので、サイバーセキュリティとは関係ないという人もいるが、そもそも紙と手であっても守るべき情報資産はある。企業には、情報セキュリティとは何か、BCP とは何かということから押さえてもらう必要がある。
- それを押さえたうえで、IT ならでは、オンラインならではのリスクや、有線・無線でつなぐときはそれぞれどうなるのかなどを考えていく。セキュリティについては何をやったらよいかわからないと言われるが、すでに IPA の「5 分でできる自社診断」や「情報セキュリティ 5 か条」がある。また、SECURITY ACTION 自己宣言もある。134 の商工会議所でまず自ら模範となるべく取得した。SECURITY ACTION を取得したところは保険料の算定に加味をしてもらえるなどの制度も保険会社で考えていただいており、そのようなインセンティブの面で意識を高めていけるとよいと思っている。ディスインセンティブとのバランスは難しいが、両面考えていく必要がある。
- 商工会議所の経営指導員は企業を巡回し、IT・セキュリティも勉強して企業の課題に取り組んではいるが、他にも様々な経営課題(BCP とか企業承継等)があり、全てに通じるのはなかなか難しい。企業にも一度にあれこれと言っても通じないところがあるので、工夫しながら支援しているところである。足りない部分は国や関係機関の力を借りたい。IT 導入に先立ちセキュリティのことを相談したいときはどこに相談したらよいのか、導入の後に面倒を見てくれるアフターサービスや、何かあったときにどうすべきか(「線を抜く」とか、どこに通報すればよいのか等)。そういったところをもっと整備しないといけない。一次的には対応することができでも、また次にどうつないでいくかの体制整備が必要。研究会を通じて提案していきたい。

○梶浦座長

・ (補足として)中小企業庁で、昨年スマート SME(中小企業)研究会 - 中小企業に対する IT 導入の研究会がスタートし、議論が始まっている。自分も委員になっており、その場で、IT 導入とサイバーセキュリティをセットで議論するということで、情報発信していきたい。

○上野委員

・ 産業横断サイバーセキュリティ人材育成検討会は、2015 年に重要インフラを担う企業を中心とする 48 社が集まって検討を始めた。現在までサイバーセキュリティに必要とされる人材の定義やカリキュラム、産学連携などを検討してきた。一方で 2020 年の東京オリンピック・パラリンピックをにらみサイバーセキュリティ対策が急務と認識されながら、なかなか進まないのはなぜか。世の中には経営ガイドラインとか NIST とか様々な「あるべき集」があるがなぜできないのか。多分にいろんな壁、人材の壁、コストの壁等色々なものがあるのではないか。従って、会員企業がこれをどう乗り越えてきたのかという知恵には大きな価値があると認識している。そこで「(仮称) ベタープラクティス集」を設け公表したいと考えている。本日、国内を代表する重要インフラ企業を集め、情報交換を行っており、秋頃には公表したいと考えている。適宜、この場でも共有させて頂きたいと思う。
・ セキュリティ対策の必要性はなかなか分かってもらえない。昨年に経営ガイドラインをベースに細分化、ベンチマークを行った。セキュリティは投資対効果をはかるようなものではなく、社会的な投資の性格が強いのではないか。このような性格の投資であることを踏まえて経営を動かすには、重要インフラ企業の平均的水準を見えるようにして、自分の立ち位置がわかるようにするのも有効なアプローチではないか。本検討会では「サイバーセキュリティ経営ガイドライン」の項目を 25 項目に細分化した質問項目を設け、その評価軸として CMMI 成熟度（5 段階）としたベンチマークシートを設けた。そして会員企業に自己評価してもらい、その平均値をフィードバックした。会員企業すなわち重要インフラ企業の平均と自社の立ち位置が明らかとなったことで経営に強い訴求ができた企業もあると聞いている。
・ 一方で、このベンチマークの合計値がどの項目と相関が高いかを調べてみたところ、リスクの可視化(リスクの発生頻度や、その影響度など)とベンチマークの合計値との間に 0.8 を超える高い相関関係が認められた。可視化できるということは何を守るべきかわかっている、守るべきものがわかっていれば責任範囲がはっきりする、責任範囲がはっきりすると具体的な動きにつながっていく。これらが非常に大きなカギとなっているのではないか。前述の（仮称）ベタープラクティス集の別添としてベンチマークシートを設ける所存である。皆様のお知恵を拝借してより具体的なモデルにしていけたらと考えている。

○丸山委員

・ 宮下委員資料の 6 ページ,7 ページの経営幹部の情報セキュリティへの関与度合いについて、大きな会社では情報セキュリティに関して経営幹部は関与しているという認識だ。業種別でみると金融は確実に関与している。金融庁の指導もあると思う。大きな会社は最近セキュリティの話をしない経営者はいなくなっている。業種によってばらつきはあるが、重要インフラ関連企業、金融機関などではそのような傾向にある。グローバル製造業でも、社外取締役に外国籍の方がいるなどの理由で意識は高まっている。
・ 具体的な対策に落とすのができないのは、橋渡し人材がいないため。名和委員の話にもあったが、具体的な対策に落とせていなかった会社で事故が起きると、今度は何でもしようと過剰になり、逆に企業成長を阻害しかねない状況になる。
・ 経営者の意識が重要であり、情報セキュリティ意識を高める政策は経済産業省が既に何年も取組んでいる。やる気がない経営者をどこかで見切りをつけるべき。厳しくいかないと最後は政府が救ってくれるという甘

えがあるのではないか。政府が情報セキュリティ関連の政策で企業をサポートしたのに企業が対策を取らないのであれば、それも経営判断でありだと思う。ただ、その分自己負担である。大企業はそれで何とかなる。

- 一方、それでは中小企業は若干問題がある。多分十分なセキュリティ対策できない。最新の脅威に対する対策はどうしても高くつくため、中小企業1社では対応できない。対策が必要。パブリッククラウドに移していくのが流れではないか。大企業でもほとんどパブリッククラウドに流れているのが現状である。その方向性を見据えて政策を考えないといけない。これは地域の IT 産業が打撃を受けることにもなりうるため、その点も考える必要がある。
- 大企業の経営は IT リテラシーの低さもあり、対策をすべきという意識はあっても具体的な対策へのつなぎが弱い。経営とテクノロジーのつなぎについては啓発していかないといけない。

(一巡回って追加での発言)

○小原委員

- 民事法、紛争の調停の効率化、保険の話などいろいろあったが、後始末が非常に大事。サプライチェーンのセキュリティで一番コストがかかるのは後始末。
- 社内でのセキュリティ対策には予知・予防・対処という3つのキーワードで説明している。サプライチェーンで事件が起きた後、取引先とどのように事象を分解するか、もめ事をどう処理するかなどのロングテールな話が非常に厄介である。ここにお金がかかる。ここは人材ピラミッドの左側、主に文系が活躍する分野。特にリーガルセンスや商売センスが必要になるが、ここに関する公的な議論が少ない。証拠の取り方ひとつとってもいろいろ法律問題がある。
- また、海外で問題が起きたとき、警察機構や法執行機関が助けてくれるかというとそうでもない。民間の調停が必要だが、裁判プロセスなどもなかなか整備されていない。ここは民間も入って議論を深めるべきと認識。

○名和委員

- 国際連携について、背景と目標が書かれていなかったが自分なりの理解を述べる。中国における「デジタル・シルクロード」(「一帯一路」におけるデジタル経済、人工知能、ナノテクノロジー、量子コンピューター等の先端分野で協業し、ビックデータ、クラウド、スマートシティ建設を推進する取組）が一部現実化しており、日本に対して脅威になりつつある。香港企業によるフィリピンの「ニュー・マニラ・シティー・オブ・パール」構想が始まり、中国のシャオミ（小米科技）がインド史上最大の携帯電話ブランドになった。これらの地域における日本企業の存在感がだんだんなくなってきている。こういう状況の中で日本企業の海外でのビジネスを守ることが目的だと認識している。
- また、一部の国で、サイバーセキュリティ強化を謳いながら、他国の競合企業を蹴落とすような状況が発生している。ハッキングしてレピュテーションを下げるという荒業さえある。数年前とは状況が全く異なってきており、そういった認識を共有する必要がある。

梶浦座長よりまとめ

- 人の見える化、企業の見える化や、単に技術でない法制から経済、国際慣例、国際紛争という部分にも話しが広がった。人材に関して一致したのは、人材ピラミッドの左側の経営側人材が薄いということ。これらについての指摘して頂いている点は前から分かっていることなので、今回は「具体的にどう進めるべきかをやろう」という意見をいただいたと認識した。
- 中国の件は、未知の領域であり、色々な方のご意見を伺いながら対処法、ここでの扱いを考えていきたい。

・　経営にしても人材にしても国際問題にしても、具体的なアクションにつながるような議論をこれからさらに進めていただきたいと思う。

奥家課長より次回日程について連絡

・　WG2 の次回は来年度実施予定。スケジュールについては別途事務局より連絡する。

以上

お問合せ先

商務情報政策局　サイバーセキュリティ課
電話:03-3501-1253