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2回) 議事概要

1. 日時・場所

日時:平成30年5月22日(火) 13時00分～15時00分

場所:経済産業省別館9階 944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、武智委員(代理:則房様)、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(欠席)、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、総務省、外務省、文部科学省、防衛省、防衛装備庁、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

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 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。

- 本日はお忙しいところ、経済産業省第 2 回産業サイバーセキュリティ研究会 WG2 にお集まりいただきまして、有難うございます。経済産業省では、3 月 16 日に研究会の下に WG2 を設置し、経営者の意識喚起、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関する施策について議論を開始したところ。
- 前回の WG ではこれらのテーマについて、委員の皆様それぞれのお立場、ご知見から活発な議論をいただいた。今回は第 1 回 WG における議論を踏まえ、これらの施策を具体的に推進していくべく、各施策の進捗や海外のサイバーセキュリティ人材の活用状況に関する調査結果の報告、今後進めていく施策の具体化等について、事務局から説明の上、これらの施策をより実効的にしていくために皆様からご意見をいただきたい。
- 本日お集まりいただきました有識者の皆様、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各種施策を進めていきたい。本日も皆様の活発なご議論をお願いする。

次に、梶浦座長から以下のとおり挨拶。

第 1 回は本当に幅広い多様なご意見をいただき、事務局も私も大変参考になった。本日も引き続き、活発なご議論、忌憚の無いご意見を賜りたい。サイバーセキュリティにおいて国内外の状況は益々厳しさを増しており、この会の議論において少しでも実効性があり、すぐに着手できるような具体的な意見をご提案いただければ大変有難い。

事務局から、本日は湯淺委員が欠席、武智委員の代理として則房様、横浜委員の代理として荒金様が出席の発言があった。

事務局から、資料 4 についての説明に続き、以下のとおり自由討議を行った。

○岩下委員

- 資料を拝見し、サイバーセキュリティの施策を進めていくことは改めて苦労が多いことだと感じた。そもそも、2015 年にコーポレートガバナンスコードが改定されたのは、出来る限り外部の知恵を入れ、経営を社外取締役にチェックしてもらうべきだという考え方に基づいている。今回事務局が示したサイバーセキュリティ経営という考え方も、その延長線上にある。セキュリティ侵害を経営上のリスクととらえ、外部の知恵を活用して、その対策を講じていこうというものだからである。
- しかし、各企業がセキュリティ対策を意識すればするほど、「では、IT を使わなければ良いではないか」という話になってしまう。特に中小企業の場合、インターネットは怖いという認識のもと、FAX で受発注を行っている企業も多い。EDI を使って処理を行おうとすると、セキュリティ対策にコストが掛かるため、なかなかイノベーションが進まないという事態に陥ってしまう。イノベーションを進めることと、それを守ることは両輪であり、守る方だけを強調するとイノベーションは止まってしまうので、常にバランスを保ちながら進めていくことが大事である。
- 企業の IT 対応の現場においては、利便性、セキュリティ、コストの３つの間にはトレードオフの関係がある。どちらかに片寄せして単純化するのではなく、そのバランスを取るのかが経営層の判断である。上手に最適なバランスを目指していくことが肝要であると思う。

○梶浦座長

- 今の話で重要なのは、トレードオフの部分。確かに取締役会には責任があるため、安全サイドに倒すのは当たり前で、他方、経営的には利益、売上を伸ばそうというのも当然であり、だからこそ牽制し合える関係と言える。ただ、今の日本の現状を見ていると、もっと経営の中でセキュリティを考える割合を上げていかないといけないと思う。
- 本質は、コストとリスクとイノベーションのトレードオフをディビジョン・ディビジョンで経営者や事業責任者が判断をしながら、取組んでいく必要があり、それを政策の中にどのくらい入れ込むのかが議論の焦点かと考えている。

○小原委員

- 前回問題提起した、サイバーセキュリティに関して取締役会での発言や議論が重要という観点に関連して、今回ガバナンスコードという形で一段掘り下げていただいたが、ガバナンスコードの枠組みに加えて、あと 2~3 点考える必要があるのではないか。
- 1 点目は、サイバーセキュリティ基本法との関係。同 7 条に「事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力する」とあり、これは事業者が名宛人だと考えられる。基本法において事業者にも義務があるとの規範は明示されており、コーポレートガバナンスコードとの繋ぎこみが検討課題として残るのではないか。
- 一方で、ガバナンス（コード）は各社バラバラであり、経営同様工夫して競争するべきもののため、サイバーセキュリティにおいても自主性･柔軟性が重要になってくる。参考になる取組みとして注目しているのは、Charter of Trust(信頼憲章)という昨年くらいから、欧州の Siemens が提唱している考え方で、本年 2 月頃に同社に加えて、ドイツテレコム、デル、シスコ、IBM、TÜV 等 14 社が政府ではなく民間主導で合意可能な規範を締結した。10 程度のステップを踏んで「サイバーセキュリティ」の考え方を通底させていこうという考えのもと、自主的に協調している。この取組みは、もちろんサプライチェーンの問題でもあるが、でき

るところから始める民間のミニマムスタンダードという点においては参考になるのではないか。

- 他方、アメリカの公認会計士協会では、System and Organization Controls for Cybersecurity を策定し、現在、Vendor Supply Chains に係るシステムや組織の管理ガイドラインを策定中である。また、監査品質を保証する団体 Center for Audit Quality では、ボードが会計監査人とサイバーセキュリティについてどのような話をすれば良いか、という手引書を出している。ガバナンスは、取締役会で独走しても意味がなく、監査を行う人々を通じて株主や市場と対話をしていくというパスが出来つつあり、こういった仕組を学ぶことも意味があるのではないか。
- サイバーセキュリティ経営ガイドラインは非常に良い試みであると思うが、もう一度このような株主との対話というコンテクストの中で見てみることが望ましいのではないかと考えている。岩下先生が仰ったこともそうだが、デジタル経営を進めることと守ることのバランスをどのように取るのかが大事である。
- またガイドラインができたとして、どのように実務をコントロールするかという課題がある。私が所属している ISF では昨年から CISO as a Service という、フルタイムで CISO 代理を派遣し、きちんとした人を雇えるまで、そのサービスを続けるコンサルティングサービスを展開している。ロードマップの作成等まで含めて、実際に CISO が上手く離陸できるまでの活動を行っている。

○梶浦座長

- 今ご指摘をいただいたのは、取締役だけではなく、公認会計士や監査人もいるという点。資料 8 ページにも外部専門家として、監査法人等との記載もあり、経営に刺さるのは、外から顧客なり投資家なり、あるいはそれに準じた人たちである。

○林委員

- 2 点お話をする。1 点目は今の話の続きになるが、私も NISC の「セキュリティマインドを持った企業経営ワーキンググループ」の委員を担っており、どのようにお互いが相乗効果を高めていけるか、苦労しているところであり、そういう意味で実態調査をやられたのは意味があることだと思う。ただ、今回の調査が今回限りというのであれば、統計的に有意のデータが取れたとは捉えにくいため、同じ方法で 3 年おきに調査する等、今後も取組みを続けていただきたいと思っている。私はこの WG の中で、取締役をどのように活用しているのか、役職との摺り合わせがどうなっているのか、組織論とセキュリティとの成熟度の関係について課題があると認識している。
- 2 点目は、前回ご指摘を申し上げたが、人材育成について日本だけかは分からないが、法律家というものは一番 IT と縁遠いところにいる。湯淺委員も参加している裁判手続き等の IT 化検討会の報告書によると、紛争を解決するにはその最後の締めのところが IT ベースで成り立っている。つまり裁判手続きそのものも電子申請方式で行う、証拠の登録についてもそういった方式を利用しようとなると、米国的な「e-ディスカバリー」が行いやすくなる。今、ロースクールでこのような内容を教える時間がないと言われているが、このままでは、日本の法曹界の国際的な競争力が落ち、日本企業は日本で裁判するよりも、アメリカで裁判をした方がコストはかかるが、時間的には早く、その方が良いということになりかねない。このような事態を是正するための法律の動きは、今の状況と連動させる形で特別に注目して見ていきたいと思っている。

○梶浦座長

- この法律の話は以前から林先生と議論させていただいていることもあり、大変重要な課題と認識しているところ。1 点目の実態調査については奥家課長の方から、どうされていく予定なのかも含め、事務局から一言お願いしたい。

奥家課長

- 人材の実態調査については、成熟度とスキルの関係、このスキルがどういう資格等によって支えられるものなのか等、今回ある意味トライアルで調査を行った。我々のアプローチはマクロ的であり、それをミクロ的なところに落とし込んで、実際にマッチングに使えるか否かは役所だけでは無理であり、産業界や学の方々達と議論を行い、分析的な作業を行う必要があると考えている。
- 企業の経営や成熟度、スキルマップの資格など、ITSS の作成時はこれらの結びつけに大変苦労したが、そこに正面から入っていかないと、人材育成の部分は経営と信頼戦略と人の活き方のところを結びつけるのは難しい作業だと思う。そのために踏み込んだ調査をし、考えていくことが大事だと考えている。

○名和委員

- 現在、エネルギー・航空・鉄道・医療・印刷業等の中堅企業等から、セキュリティ教育を自社内で行う際の教材が少ないため、公的機関から Web サイト等で永続的に使えるものを公開して欲しいという要望がある。
- 例えば、欧州であれば ENISA という団体が「Training Resources」を、また同じ欧州で TERENA という団体が、以前 FIRST のカンファレンスで開催されていた「Train the Trainer」でも利用されていた CSIRT トレーニングプログラム「TRANSIT Courses」を公開している。これらの一部は、日本シーサート協議会が日本語版にして、不定期にレクチャーを施しており、非常に有益であると評価されている。ENISA の方は単にドキュメントだけではなく、ツールセットも提供されており、この WG で情報交換していくことも良いのではないか。

○梶浦座長

- 教材として利用できるものは可能な限り利用をしていくことを、事務局としても検討していただきたいと考えている。

○宮嵜委員

- 大企業は意識もあり、それなりに対策をしていると思うが、保険会社の顧客は、中小企業が圧倒的に多いため、ここの意識改革が極めて重要だと認識している。我々としてもサイバーセキュリティのサービスを販売していきたいと考えており、損保の営業や代理店がサイバー保険を売っているものの、サイバーリスクを説明し切れないというのが保険会社側の課題となっている。加えて、中小企業の経営者が自社内に個人情報はなく、パソコンも 5 台しかないから大丈夫と、深刻に捉えていないところも散見されているのが現状。
- サプライチェーンについては、我々としてもこれからビジネスをするためには最低限必要であると認識しているが、顧客からは、どのくらい予算をかければ良いのか、どこまでやれば良いのか、という意見を言われることもある。最低限ここまではやりましょうというものが、私達から示すことが出来れば良いのですが、なかなか難しく説明が十分にし切れないのが現状。この会で、顧客に提示できる客観的なものが作れれば、保険会社としてもニーズ喚起がしやすいと思っている。
- 米国では企業のセキュリティを玄関から確認して、保険を引受けるか否かを判断しているが、まだ日本はその段階まで到達していないので、保険だけで引っ張るのは難しいと考えている。一方で、対策をしている企業も、していない企業も保険料は同じなのか、といえばそうではないので、保険会社としても対策をここまでしていれば、追加で保険的なサービスを提供できるという仕組み作れないか、商品の検討を進めているところ。
- 日本は島国でもあり、あまり攻められないと思っているところと、隣よりもお金をかけて対策したくないけ

れど、同じくらいには対策したいと考えているところもあるので、そういう部分も評価されると、対策自体が進むと考えており、中小企業のマーケットに対して、経営者の方々に何とか手を打っていく方法を考えていきたいと思っている。

○梶浦座長
・ 大企業も「どこまでやるのか」については同じく悩んでいるところだが、サイバーセキュリティ経営ガイドライン等では具体性が十分でない。例えばモデルケースが充実すれば良いということか。

○宮嵜委員
・ ガイドラインを意識はしているとは思うが、会社組織全体にうまく浸透して、どこまで優先順位をつけて対策をするのか悩んでいる。一方で、対策を進めるとイノベーションが進まない、あるいは利便性を損なうということもあり、その辺が皆さんの悩みどころであると考えている。

○梶浦座長
・ 資料 3 ページ、18 ページに損保会社等が相談窓口、いわゆる駆け込み寺のような存在を提示しているが、この実現性についてはどのように思われるか。

○宮嵜委員
・ 保険会社として、どこまで相談を受けるのかという問題は必ず付いてくるが、親和性という観点では実現性があると思う。ただ、実際に実現する際の課題については、今後検討していく必要があると考えている。

○横浜委員代理　荒金氏
・ 3 点コメントする。1 点目は多様な人材が必要という点について。先ほど来、監査人等いわゆるトップガン的な人、経営層に近くてセキュリティのわかる人もそうだが、企業は様々な側面でセキュリティのことを知っているという人がいることで、リスクマネジメントにつながっていくので、多様なセキュリティ人材を育成していくということは大事であると考えている。
・ 2 点目はベストプラクティス、事例集という話があったが、ここでベストということに拘ると、考えを固定化してしまうニュアンスが出てきてしまう。業界によって方向性が異なっていることが考えられるため、ベストに固定せず、常に進化するプラクティス集を作れれば、使う側にとって魅力的な位置づけになるのではと考えている。
・ 最後に可視化ツールについて、同業他社がどの程度対策を行っているのか気になるという考えには同意するが、日本の企業全てにおいて、一つの物差しで測るのはあまりフィットしないのではないか。逆に様々な物差しがあり、それぞれの会社が自分達に合った尺度で測ることができるような、セルフアセスメントが可能になると、それぞれの業界で自分達にあったセキュリティの形が実現できるのではないかと考えている。

○梶浦座長
・ 資料 3 ページ、12 ページに「ベストプラクティス」という表現があるからだと思うが、事務局はどう考えているか。

○奥家課長
・ 事例集については、今後外の方々の意見も踏まえながら検討するが、ベストとは本当にすべてにベストであ

るのか、ということを考えると「プラクティス集」という表現に変えたほうが良いのかもしれない。恐らく適用できるケースが変わると考えられるので、良さそうな事例集を集める方向に考え方を変え、「プラクティス集」を作ろうと考えている。

○宮下委員

- セキュリティに関する色々なデータや数字が出てくる中、平均値で全てが語れるのかというと少し問題がある。例えば、経営がセキュリティに対して認識を持っているかということで言えば、全体平均は約 36%になるが、例えば 1 兆円企業でいうと 90%の経営者は、セキュリティについて非常に認識が高く、1000 億円から 1 兆円だと約 55%、逆に 100 億円未満、中小だと 20%と大きく状況が異なる。このような違いを考えなければならない。また、業界毎にも状況は異なる。例えば金融業界だと 90%の経営者は認識が高いが、製造業、サービス系の業界は認識が低い。プラクティス集を作る際に、そのような状況を踏まえた上で議論し、企業にとって役立つ、具体的なものにしていただいた方が良い。
- 10 年くらい前から IT の世界で、クラウドの活用が進み、システムはクラウドファースト、基幹システムすらクラウド化しており、クラウドのセキュリティをどうするのかが課題の一つになっている企業も多い。特にクラウド化が進んでいる金融業界では、クラウドセキュリティについて議論がされていると聞いている。ユーザ企業は、クラウドに関してどのような選定基準があるのか、どのように活用していけばよいのかという点は関心があると思う。
- もう一つ、人材については、自社内でしっかり人材育成をして、活用していくのが本来の姿だろうが、時間がかかる。先ほど、右側左側の話があったが、左側の方は、自社内でしっかり育成するのだろうが、いわゆる技術的な人材育成については、外部の活用といったところも十分に考慮する必要がある。また、CISO の代理サービスといった話もあったが、そういったことも含めて自社内だけでこり固まることなく、外部を上手く活用する仕組みだがあると良いのではないか。

○梶浦座長

- ご紹介していただいた数字は、まったくその通りだと思う。業界ごとにレベル、状況が違うのは確かであり、その辺りをどのように整理をするのかは事務局と相談をしたいと思っている。
- クラウドと外部人材活用は、ほぼ同じようなもので、自社内で揃えられない場合、あるいは、より効果的に IT リソース、および人材を使えるということに関しては、サービス利用というのは、今後避けて通れない。そういうものの見える化が、まだ足りないのではないかということを言われているのかと思うが、サービスの格付けのような話まで、議論は進むのかも知れない。これは重要な議論なので、引き続き考えたいと思う。

○藤原委員

- 経営層、経営者にどうセキュリティを理解してもらうか、意識改革が大きなテーマだと思っている。それに関して、以前あるシンクタンクで実施した CSR（Corporate Social Responsibility:企業の社会的責任）の研究プロジェクトが参考になるのではないかと思うので、紹介する。
- CSR の世界は、サイバーセキュリティの世界と似たような議論がなされている。なぜかと言うと、海外では非常に認知度が高くて重要な問題と認識されているが、日本では海外と比べるとまだ認知度が低く、まだ経営層から中位層へ達していない。CSR の担当者も、重要性を何とか分かってもらおうとしているが、経営層に理解してもらえていないという点が、問題として認識されている。サイバーセキュリティの問題とかなり似ている状況と思う。この CSR 研究プロジェクトでは、日本の一部上場企業を対象に約 300 社からアンケートを取り、ベストプラクティスとワーストプラクティスを抽出した。上手くいっている企業の成功の原因

は、経営層がCSRの重要度を理解していることに尽きる。では経営者がどのように目覚めたかというと、社外取締役から強く言われた、あるいは外国の機関投資家や、NPO、NGO、すなわち人権団体、環境保護団体から、ステークホルダー対話の際にとことん指摘されたという経験が大きい。

- このプロジェクトでは、他にグローバルの状況も調査された。CSRを疎かにしていると、もし何か事案が起きた時に企業の評価が下がり、株価にも影響が出てくるという意識が経営層に根付いている海外の企業は多い。取締役会で取締役から厳しい追及を受ける、NPOやNGOが不買運動やメディア・キャンペーンを行う、消費者はクラスアクション（集団訴訟）を起こすなど自社及び他社の具体的な事例を見て、経営者のマインドがガラッと変わった、という海外企業の経験がある。同じことがサイバーセキュリティにおいても起きるのではと考えられ、経営層の意識を変えるためには、資料7ページ、8ページにある取締役会や社外取締役会からの取り組みが非常に重要ではないかと思っている。
- もうひとつ、ダボス会議のような世界的な大きな国際会議に出て、そこでグローバルなビジネスリーダー達が、CSRに真剣に取り組んでいる、議論している姿を目の当たりにしたこと、それが日本企業の経営者のマインドが変わる非常に大きなきっかけになったという話もあった。社長が変わったタイミング等で、そういったインパクトのある国際会議に出てもらい、グローバルなトレンドを知ってもらうことも重要だと思う。

○梶浦座長

- 個人だけでなく、会社も国際舞台に立つと変わるというように言われたと思う。分析はこれからだが、今回調べた英米の企業500社は、要するに国際企業で、こういう点も日本企業の現状と合わせるとずれているかもしれない。今後、日本の中での調査も必要あるかもしれないが、皆さんから見た意識のずれなども分析してもらった結果を今後出し、またご意見いただければと思う。

○小松委員

- 我々、商工会議所は、主に市単位で展開しており、約125万の会員企業をかかえ、全国515拠点に立地している。人口10万人以下の都市が515拠点のうち6割以上を占めており、中小企業の大多数の方々がいらっしゃる地域をカバーしているといえる。加えて、商工会は、我々と同じような組織で、主に町、村の単位で展開されており、会員数でいうと約80万で、商工会と商工会議所を合わせると200万ほど、中小企業380万社のかなりの部分をカバーできているだろうという組織。
- 中小企業向けのセキュリティ対策については5、6年以上前から、IPAと共に、商工会と中央会、商工会議所も、明治大学の岡田教授を座長として中小企業向けの普及活動に取り組んできた。これらの活動では、例えば、5分で出来るチェックリストや、中小企業向けのガイドラインを作成しており、最近では、セキュリティ対策の取り組みを自己宣言する「SECURITY ACTION」の取組みも実施している。
- 人材育成では、地方都市に行くとセキュリティに詳しい方が少ないため、IPAが中心となり、セキュリティ対策の指導者育成を商工会議所、商工会と連携して推進してきた。これらのことも、どこかで触れておいていただけるとありがたい。

○奥家課長

- 中小企業向けの施策として、中小企業向けガイドラインの策定や、SECURITY ACTIONは保険会社にお力添えいただいて保険割引との連動、5分で出来るチェックリストの可視化ツール等がある。さらにIPAは警察との連携を強め、関係を強化しており、日本商工会議所とも、いわゆる面で対応するために幅広く対応している。
- 様々な取組みを行っている中で一番悩んでいるのは、中小企業の人達に地方、地域にまでリーチし、面で押

さえる取組みが効果的だが、私たちの中央省庁には手足はなく苦労している。そういった課題から、面でどうリーチするのかという点、さらに地域において、地方でベンダーが撤退していく例というのがあって、すぐに駆けつけられる環境を取り続けていけるかということも考えなければいけないという中で、新しい考え方を本日は紹介した。

・ サイバー保険(資料 3 ページ、17 ページ)と、2 ページ目(資料 3 ページ、18 ページ)は、連動した形になっており、例えば日商、さらに代理店網をかかえている損保会社のような組織で面を抑え、お助け人材として、いわゆる人材プールのようなものを全国拠点に作ることが出来たら、中小企業の本当に困っているところへアプローチできるのではないかと考えている。

○梶浦座長

・ 資料 3 ページ、18 ページの絵で中小企業と、損害保険会社、IT 人材の 3 つのブロックを描いていただいたが、サイバーセキュリティを守るという意味ではこれで良いが、実際には IT 導入が十分でない中小企業の方が圧倒的に多いので、導入からセキュリティを取り込んだ形が理想である。
・ 導入方法は、ある程度形をまとめる、数をまとめる、面でまとめるという施策が必要と思っている。この間に、例えば地域クラウド事業者というのが入って、先ほどもクラウド事業者の見える化とか、あるいは外部人材の活用といった話を頂いているし、そういった形でまとめてセキュリティを高める、その前に IT 導入をして、しっかりイノベーションを行うことと、本来はセットで進めるべきだと思っている。

○塚本委員

・ セキュリティへの取り組みについて、世の中の空気というか、世間の目のような compelling reason(やらざるを得ない理由)のようなものを企業に与えるのが良いのではと思う。プライバシーがそのような形で意識され、企業の信頼の基盤として、盛り上がってきているのと同じ発想。IoT やビッグデータまでは、世間でも、かなり認知され、経営者などの理解が深まってきているように思うが、そこにセキュリティが必ず必要と結びついてはいないと思う。
・ 具体的に何が出来るのかというと、本 WG にご参加の皆様等有識者の方を含め、IoT やビッグデータの話は講演をすることが多いと思うが、そのときにセキュリティの話しを前後に必ず基盤として入れるのもありだろう。また、資料 3 ページ、47 ページにあるリテラシー教育の拡充のところで、消費者の方たちに説明するときに、「会社についてネット等で調べるときは、その会社のプライバシーポリシーやセキュリティについて一人ひとりの消費者が確認をする」というような話を入れると、セキュリティについての意識啓発になるのではないか。

○梶浦座長

・ 今までの意見では、取締役会や投資家など色々なステークホルダーの話が出ていたが、経営者に伝わるのは、お客様の直接の声である。サプライチェーンを含めて、お客様の意見が刺さってくるというのは、全体のセキュリティレベルを上げるひとつのキーワードだと思う。

○上野委員

・ 事務局資料に対する意見が 2 つと、参考として情報共有させていただきたい。
・ コーポレートガバナンスコードについて、金融商品取引法で内部統制が入ってきた時の状況に非常に類似する動きになるのではないかと思った。弊社グループで、例えば運用と開発を分離して職務分離をやりましょうという話は昔からしていたが、金融商品取引法が施行されて内部統制の財務シートの有効性について評価

を受けるようになってこの辺の整理が一気に進んだ。そういうことを考えていくと、経営のモチベーションを強烈に刺激して、いわゆる適用会社のセキュリティの成熟度を猛烈に引き上げる有効な施策になるのではないか。モチベーションが上がって実行できる経営資源がしっかりアサインできて、そして当然これをやるにはレギュレーションなどがあるから、そのレギュレーションに合わせて成熟度を上げるということで明確になるのではないか。

- 今回、興味深かったのは、資料 28 ページで中小企業の有効策が教育管理者というのはある意味意外で、実は産業横断の中でもいっているのは、ここではなく、グループ内の共有ネットワークや、グループ内の共有インターネット環境を提供することで、いわゆる専門家がいないグループ企業、グループの中小企業の中でも圧倒的にセキュリティレベルを上げることができる。そういうことにおいては、地域クラウドや、この資料にある損害保険会社の相談窓口のようなものを作っていくと有効ではないかと思う。
- もう一つは、教育管理者のレベルを一定に保っていくことも、ひとつの人材育成のメソッドになるのではないかと興味深く伺った。
- 最後に情報共有したいのは、プラクティスという話があったが、我々産業横断検討会の中でもベストではないという話は始めており、ベタープラクティスなど色々な名前で呼んでいる。実は先般、国内を代表する企業、数社をまさに当社の中で朝から夜まで缶詰になって経営ガイドラインに対する本音のところを議論した。その後、中京地方を回って色々話しを聞いたが、この関係を醸成できるのは非常に時間がかかるということをご認識頂いた方が良いと思う。産業横断では、こういう取り組みを数年前から行っていて関係を繋いできた。10 月にベストプラクティス、ベタープラクティスになるのかは別にして何らかの形で、その内容を公開予定であり、企業匿名性を担保しながら出来るだけ社会に寄与できるものを出したいと思っている。プラクティス作成のマイルストンとしてご認識いただければと思う。

○丸山委員

- 一つは経営者の資質、一つは人材確保と人材育成について前提的な話をしたいと思う。経営者次第というのは、まさにその通りで、投資家は経営者を見るというのは前提であり、サイバーセキュリティ投資をどの位行えばよいかという話を経営者が言う場合もあるし、担当者が言う場合もあるが、経営者が「サイバーセキュリティ投資をどの位行えばよいか」と言っているのは、最悪な状態だと個人的には思っている。「経産省がサイバーセキュリティガイドを示し、それに従っていたらサイバーセキュリティについての経営が出来る」というのは、経営ではないということを、前提として言っておかないといけないと思う。そうでないと、経営者がきっと悩むだろうと、担当者がどこまですればよいかを忖度してやっているような感じがして気の毒だと思う。どこまででサイバーセキュリティ投資を行えばよいか判断することは経営者の仕事だから、担当者はあまり考えなくてよい。「担当者は経営者が判断するための前提条件だけを出せばよい」としてあげた方がよい。
- 人材活用という意味で、5/19 に防衛省がサイバー防衛を民間委託するという話が出ていたが、そういうことがあっても良いのかなと個人的には思っている。技術的なところは、全ての企業で技術者をかかえても活用しきれないので、外部の人を使うことは当たり前だと思うが、外部の専門家とフックになるつなぎの部分の人は、内部に持っておくことが必要と思っている。IT を外部に丸投げする体質、文化が昔からあるから、サイバーセキュリティでも同様の問題があるように感じる。
- 最後に、人材育成という点であるが、学校でサイバーセキュリティを教育できる先生が少ない。セキュリティ教育を行う人材が不足しているという話が、資料 44 ページにあるが、その通りで非常に重要な問題である。IT は、それまでは会社の一部、防衛の一部で使われていたが、PC やインターネットの登場で一気に拡がった。その拡がるスピードと、それを教える人材を揃えるスピードが合わなかったという問題があるよう

に思う。そしてITを教えるのと同時にリスクやセキュリティを教えなければいけない。

・ 例えばセキュリティの本を持っているが、古い本だと1970年代、60年代の本がある。それはなぜかというと、そのとき丁度ITつまり、汎用機が会社に導入されてきたころなので、そのときにセキュリティの本が同時に入ってきていると考えるとITの導入と、セキュリティの導入はある意味セットになるということで、学校の先生においても情報の授業で、セキュリティも教えられる人材にセットで育てていかないといけない。ITが拡がるスピードほど、教えるスピードが追いつかなかった面はあるが、これはこれから課題として、省庁の横軸を通して進めていくのが良いかと思う。

○梶浦座長

・ 経営者の責任ついては、おっしゃる通りだと思うが、それをどう扱うかは考えさせて欲しい。
・ 人材活用で言われたフックという話は、まったくその通りで、我々も外部業者を使うときは、本来は自社でも出来るが、時間を有効活用したいという場合に、外部委託を使うのであって、自分が出来ないことを任せるのは、いわゆる丸投げそのもの。ITを導入する、当然セキュリティとセットで導入するときは、時間があれば、自社で構築して運用できるが、自分もやることがあるので、監督するだけということが良い。しかしなかなかそういう人間（監督できる人）を採用する余裕が小さい企業ではない。そういったところがコーポレートガバナンス、ITガバナンスの世界の議論と同じかなと思う。
・ セキュリティは、セキュリティだけで成り立っているわけではなく、岩下委員がおっしゃったようにイノベーションのためにセキュリティはやるのだというのは何回も繰り返していかないといけないと思う。

○武智委員代理　則房氏

・ 資料に書かれていることは、大事なことであると思うが、同じテーマ、同じ範囲のなかで、ここに書かれていなくて重要だと思っている内容に対して、3点コメントさせてください。
・ 一つ目は、サイバーセキュリティは長期間続く話になるため、課題として何をするにしても10年、20年継続する、そういう視点をもって検討すべきで、取捨選択するべきだと思う。
・ 二つ目は、人材に関する話。企業の中で今サイバーセキュリティを行っている人は、技術的な末端のことを行っている人は別にして、管理者の上の方に上がっていくほど兼任者が多く、優秀な人であってもサイバーセキュリティをそのまま続けるわけではなく、本業でローテーションがかかって異動するというような構造になっている。企業の中で効率化やコスト削減を追求すると、優秀な人にサイバーセキュリティ管理者を兼任させるという仕組みが、変わらない。企業の中にサイバーセキュリティを取り込む組織と、専任者の人材を置くことが重要だと思う。
・ 三つ目は、サイバーセキュリティらしいサイバーセキュリティの内容があると思うが、外から攻撃してくるサイバーセキュリティの話と、従来多くの企業が取り組んできた情報セキュリティという話を、一緒にして話をすると聞いている側は非常に理解しにくい。今回の話は中小企業の人たちも対象になっているが、中小企業はサーバーセキュリティの高度なところは、理解できないと思うし、そこをやれと言うのはすごく高い要求をしていると見える。
・ 高度なところは誰かがちゃんとやってあげるから、従来の情報セキュリティもほとんど見られていない企業が主だと思うので、そこのところを自分達でちゃんとやれば、高度なサイバーセキュリティのところは、この人たちがちゃんと面倒見てあげるから大丈夫だよと言ってあげれば、(どうしていいか困り果てている人達も)安らかな気持ちなるという、そういうシナリオが要るのではないかなと。従来の情報セキュリティも十分やれていないという場合に、日本の大きな企業は、これまで10年15年と取り組んできた内容なので、そこはちゃんと技術トランスファーの取り組み方を指導、支援できるところだと思う。指導、支援する側にもビ

ジネス機会が出てくる話だと思うので、(双方に動機が生まれて)そこはやれそうな気がする。
・ 大企業でも　サイバーセキュリティらしい高度なサイバーセキュリティ対策への取組みになると、技術、人材不足などで悩んでいるため、自分たちのところでもできないところを中小企業のために人とお金を割いて行うという話は現実難しく、そこをどう上手くシナリオを回して行くかという話しは、今後の重要な課題ではないかと思っている。

○梶浦座長
・ 有難うございました。専任、兼任の話は非常に重要な件でございまして、今回の調査からは見えてこない。多分、日本の企業は兼任が多いというのは一般的にはわかるので、次のなにか手を打たないといけない。
・ 最後に言われたサイバーセキュリティらしいサイバーセキュリティの話しは、例えば、私の理解だとオペレーションテクノロジーみたいなものだと思うが、大企業も困っており、バリエーションがありすぎて、なかなかひとつの答えがない。情報セキュリティのレベルであればクラウドと外部人材活用で、ひょっとしたらいけるかもしれない。また、中小企業に地域クラウドベースあればまずはそこまでかなと私自身思っている。そこら辺の整理をさせていただこうと思っている。

○小原委員
・ 欧米企業の内部事情という話について一言。例えばアメリカ取締役会協会によると結構セイバーセキュリティのイシューがボードで議論されていると報告されている。これに対して日本は遅れているという議論がなされるが、色々な資料を紐解いていくと、アメリカでもフルボード、全員で話しているというわけではなくて、セキュリティの専門家とリスクマネジメントの専門家と監査の専門家の 3 名ぐらいで話しているのが通例のようで、まだ改善の余地があるとされている。
・ ヨーロッパの議論でも、取締役会でサイバーセキュリティの話が出ると、議題が通過するのを待つ、といった態度の取締役もいるようだ。それはなぜかというと、CSR と違い技術的な単語が多く難しい。つまり、欧米人にとってもサイバーセキュリティの難しさは同じで、これをいかに技術用語でなくて分かりやすい言葉、例え話で伝えるトレーニングをすることが今話題になったりしている。先ほど紹介した CISO as a Service では KRI や KPI と言った指標を使って分かりやすく話をする工夫もされている。
・ コーポレートガバナンスコードも大事だが、実際に活きるための仕組み、前に進めるための仕組みが必要。例えば社外取締役、社外監査役もそうだが、彼らに対する研修、つまり、どういう話をしたら議論が活性化するか、というトレーニングがあっても良いと思う。あまり技術用語を使わずに、どうやったら伝えられるかが肝要であり、私自身も前に進める仕組みのためにチャレンジしたい。
・ 最後に技術人材の話だが、サイバーセキュリティの第一線の専門家の方と、議論したときの話をご紹介する。日本にはコンピュータ第一世代と呼ばれる人がいて、コンピュータを一から組み立てて作って、本当の原理を知っている。この人たちをサイバーセキュリティにも活用することが実は人材確保として早いのではないか、という視点である。東京だけでなく地方にも当然いらっしゃるそういう方々を組織化するというのも一つのアイデアという話があった。

○名和委員
・ 資料 3 ページ、51 ページにある日米の ASEAN 等へのアウトリーチだが、その中に日米共同演習があり、毎年秋に東京で開催される。
・ 昨年度末までに大きな変化がいくつかあったと思う。東京都が今年 3 月に「東京 2020 大会の安全・安心の確保のための対処要領」を策定し、これに準拠する形で関係組織において具体策が検討されている。これは

治安対策領域とサイバーセキュリティ領域のインシデントを想定しているものであるが、クロスドメイン（領域横断）攻撃を想起させるものである。ここ数ヶ月、韓国が北朝鮮からのクロスドメイン攻撃を観測しているという報道もあるため、我が国でも、このような領域横断のインシデントを想定した対策の検討をしていく必要があると考える。

- 国内で、実際にクロスドメイン攻撃のような事態への対処を所掌しているのは内閣官房の事態室で、緊急事態としてのサイバーテロ（大規模サイバー攻撃）の対策訓練等を行っている。このようなところと連携する必要があると考える。
- 日本は、様々な省庁及び地方公共団体にインシデント対処に係る所掌が細分化されているため、重大なインシデントを報告すべき公的機関の数が多すぎるとか、そのための窓口対応が大変だとかという話を民間企業から聞く。さらには警察組織の方でも別途対処要領の策定を進めている。民間企業の現場において、公的機関との連携の仕分けが煩雑になり始めているため、できれば特定の公的機関で吸収できるところは吸収した方が官民連携の成果を高くすることができると思う。

○奥家課長

- クロスドメインについては NISC の方でも意識をしていて、私たち自身も気にしている。アメリカではクロスドメインでアプローチした時に、それぞれの領域がどういう関係性になっているのか、DHS と NIST が各主要オートメインの関係がどういう関係になっているのか調査しようとしている。
- 彼らから出て来たレポートを、日本にそのまま適用できないと思っている。例えば日本では電力会社は自己完結している割合が極めて高いが、通信ネットワークに対する依存が非常に低い。一方で、配電部分は独立していても、普通のオペレーション、その範囲での部分が独立していても普通の業務は、いわゆる一般通信設備を使っているとか、それが一体どういう影響が出るのかと違った形ででる。鉄道も JR などはコンプリートしていて、実は中で独立している部分が広く、そういう中で、必ずしもアメリカ的なものが適用できないだろうと思う。
- 一方でクロスドメインをやらないといけないので、ここについてはシナリオベースで今後考え、手を付けていかなければいけない。さらに一回経験してみるということが必要な領域だと思っている。しっかりと NISC 中心で進めていきたいと思っている。

○林委員

- ここに書いてあることは政策レベルのことなので、それについては申し上げることはない。
- 実務的なことで私が絡んでいることがある。テレコム関係では BHM テレコム支援協議会という組織がある。NTT、日立などの OB が主となってベーシックヒューマンニーズで協力するには、その下で通信がしっかりしていないとダメなので、色々な国際協力を行っている。その中の一環として途上国のテレコム関係の中堅幹部を呼んだ講義を自前で相当費用をかけて行っており、私もセキュリティをテーマとして講義をしている。
- その他に、アジアパシフィックテレコミニティという組織もあり、日本に研修員として呼んで講義をしている。それらの活動を通じて、近くにある大国の方が、お金もあり、恵まれた研修をしており、日本の方が甘いということを感じている。
- そういった中で、キャパシティビルディングの重要性を、もう少しみんなでシェアして欲しい。一つには人材そのものにも効いてくるし、日本企業のサプライチェーンを辿っていくとそういう所に立地しているので、サプライチェーンのセキュリティを間接的に高めることにもなる。他の会議でも申し上げているが、キャパシティビルディングがそういう意味を持つことを強く意識して欲しい。

○梶浦座長

・ アセアン諸国のキャパシティビルディングに貢献する事が将来大きなリターンとなって帰ってくるということをおっしゃっておられると思う。

○岩下委員

・ 「情報セキュリティは普通に行っているが、サイバーセキュリティは難しい」という意見があった。そういう感覚は理解できるが、サイバーセキュリティは情報セキュリティの一部であり、中小企業にサイバーセキュリティ対策をやって下さいと言うのは、要するに情報セキュリティをやって下さいということ。それ以上のこと、例えば DDos 攻撃の事前対策をして下さいと中小企業に要請する必要はないと思う。実効性のあるサイバーセキュリティ対策としては、パスワードの管理などの素朴な情報セキュリティ対策を愚直にやっていくしかない。
・ “cyber security as a service”のような話になると気になることがある。プライバシーマーク対策取得アドバイザーという商売がある。あなたの会社にプライバシーマークを取らせてあげる、あなたは何も勉強しなくていい、全てこちらがやります、簡単な質問にイエス、ノーと答えてくれればあなたの会社は立派なプライバシーマーク取得企業です、と指導するのだという。それでは本当にプライバシーを守るためには何の役にもたたない。サイバーセキュリティやプライバシー保護を、名目だけのものにしてはいけない。
・ 地道に情報セキュリティ対策をやって行く事が大事だと、トップの方含めて分かって頂く事が大事だと思う。

梶浦座長よりまとめ

・ 今日も活発なご議論ありがとうございました。
・ 印象に残った点を申し上げると、第一はコーポレートガバナンスコードのような話を導入すると、昔内部統制の話しがあったように意識が高まるであろうから始まり、お客様のご意見、取締役会の意見、あるいは監査法人など経営に刺さる人たちの意識が高まることが最終的には経営に反映して、意識改善そして投資が増え、良い方向に向かうだろう。
・ その次のステップとして具体的にどうするかという話は、プラクティス集のような具体的なガイドがいるという話があった。どのようなモデルで、どのような体制でどこまでというようなものが幾つか見えてくると進みやすい、というのが 1 点あったかと思う。もう 1 点は、スタートアップや中小企業の場合はクラウドや外部人材活用といったことをやっていかないといけない、というのは概ねコンセンサスが得られたと思う。
・ 3 つ目として、トータルな意味で教えられる人が少ないというのは色々な方のご意見で、大学の中だけでなく、企業の中でも、地域を含めて教えられる人が少ないというご意見があった。名和委員からご紹介のあった良い教材等を、もっと周知するための具体的なアクションを検討するべきだと思う。

○事務局より次回日程について連絡

・ 今後のスケジュールについては後日事務局から連絡する。

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