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7回) 議事概要

1. 日時・場所

日時:令和3年2月18日(木) 10時00分～12時00分

場所:Web開催

2. 出席者

委員 :梶浦委員(座長)、岩下委員、小原委員、秋元様(佐藤委員代理)、武智委員、塚本委員、土佐委員、名和委員、上杉様(藤原委員代理)、丸山委員、宮下委員、湯淺委員、松原様(横浜委員代理)

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、防衛省、独立行政法人情報処理推進機構、独立行政法人国立高等専門学校機構、株式会社アイ・アールジャパン

経済産業省:大臣官房 江口サイバーセキュリティ・情報化審議官、商務情報政策局 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・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

4. 議事内容

事務局から、現下の状況を踏まえて、本日はオンライン(Web)開催との発言があった後、資料の確認と委員の紹介を行った。事務局から、宮嵜委員は欠席、また、佐藤委員の代理として秋元様、藤原委員の代理として上杉様、横浜委員の代理として松原様が出席との発言があった。

続いて事務局から、資料3についての説明を行った。

(1) サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)について

○小原委員

- SC3がいよいよ立ち上がったが、問題意識としては企業を越えてサプライチェーンの中での情報共有や報告が足りていないので、これを促進すべきだということだと思う。
- 各企業がやらなければいけないことは、サプライヤーのマネジメントのライフサイクルをきちんと回すという、非常に当たり前のことだと思うが、企業間、あるいは産業間での情報共有が足りないという問題がある。せっかく約90団体が参加したということで、ある意味異業種の塊だと思うが、90団体がそれぞれ情報をうまく共有することで、どういう経済効果が出てくるのかを考えるべき。
- 例えば、昨年末から話題になっているSolarWindsのような話にどのように対応していったら良いのか、すでに国内に各種のセキュリティ団体、セキュリティベンダが多くある中で、SC3のユニークさを活かしてどういう社会経済の問題を解決していくのかそこに焦点が当たっていくと良いと思う。
- なお、サプライチェーンセキュリティは、グローバルビジネスと裏腹でもある。ベストプラクティスや情報共有なども、どんどん英語化して、業界・国境を超えた取り組みに組み上げていく努力も忘れるわけにはいかない。

○宮下委員

- SC3 の中小企業対策強化WGにおいては、発注元企業として取り組むべき課題の整理もお願いしたい。発注元企

業にセキュリティ対策の実施状況を聞いたときに、実はサプライチェーン全体での対策、それからその状況の把握の実施状況が一番低い。十分実施できているという企業は1割程度しか無く、サプライチェーンの対策について不安を持っているという企業が多くなってきている。また、実際には海外拠点やグループ会社が起点となるインシデントにより、それが結果的に自社に波及することもかなり多いという実態もある。そういう意味で発注元としてのサプライチェーンに対してきちんと意識を持ってもらうと同時に対策をしていかなければいけないのではないかと感じている。

○塚本委員

・ SC3の会員に製造業は入っているが、建設・土木系も入った方が良いと思う。業界団体等でもSC3について是非紹介させていただきたい。

○武智委員

・ 先日、高専連携について議論したところ、各企業によって採用の状況にかなり違いがあることが分かった。まずは高専の議論から始めるにしても、大学も含めて産業界として欲しい人材、どういった人材がいるのかをちゃんと出していく必要がある。

・ 人材育成に関して、産業界の意見も吸い上げ、産学官連携として SC3 でも進めていくという方向性で良いと思う。

(2) 経営に関して

○岩下委員

・ コロナにより、リモートワークやITを利用した業務の進め方に対するニーズが高まり、企業は従来にも増してサイバーセキュリティのリスクに直面することになる中で、経営サイドへの啓蒙・啓発が非常に必要になってくることについては疑いのないことで着実に進めていただいているというところだと思う。そういった中で、経営者でなければできない判断が出てきた、その判断に対応するために経営者がよりリーダーシップを発揮して対応するべきだという点はその通りだと思う反面、経営者に判断できるのだろうかという切実な問題がある。

・ やはり、きちんとハンドルできるかというところが大事で、経営層に報告すればそれで責任を果たした感じになっているとか、経営者が判断したらそれが間違っていないという事では無いと思う。経営が関与して、経営がその会社にとって間違いのない判断がきちんとできることが非常に大事。

○土佐委員

・ 経営ガイドラインのような話は、会長・社長や経営企画、法務、人事、総務、ITなどのコーポレート部門には響く一方で、実際ビジネスをやっているライン、事業部門などには、なかなかこれが響かないところがあり、そういったところにどうやってつなげていくのかということが観点として必要ではないか。

・ 実際、海外の現地法人の中にはサイバーセキュリティ対策が非常に脆弱なところがあり、結果として、インシデントの大半は海外の現地法人で起きているということがある。そこの対策がなかなか進まないのは、海外の現地法人が、ビジネスセクターに属しているということも影響しているのではないかと思われる。コーポレート部門だけではなくて、ビジネスセクターの人間の納得感や得心が行くようなガイドラインや実例などが出せると良いのではないか。

○宮下委員

・ 経営者の意識という観点では、コロナ禍の影響でかなりのスピードでテレワークを実施しているということもあって、セキュリティに対する意識がかなり改善されてきている。ただし、企業規模や業種によってその意識にかなり大きな差が出ている。一つの例では、企業規模でいうと1兆円を超えるような非常に大きな企業においては、セキュリティの案件に関してきちんと経営会議で報告を受けて、その中で経営者自らが議論をしたうえで指示を出しているという会社が9割を超えている。一方で、1000億円以下、決して小さな企業ではなく、中堅もしくは大企業に近い企業においては、その割合が3割に減ってくるということと、さらに1割強が、経営会議では議論をしていない、そういった認識もほとんど持っていない、という結果も出ている。全体的というよりも、企業規模や業種によって差があるということを意識した上で対策を考えていただいた方が良いのではないかと感じている。

○上杉様（藤原委員代理）

・　経営者やセキュリティ業界以外に情報を届けたいという想いがあると思うが、その場合、セキュリティを主語とするのではなく、課題やテーマを主語にする、例えば、テレワーク＋セキュリティのプラクティス集とか、DX＋セキュリティのガイドラインや事例といったものであれば、セキュリティ業界以外の人にも見てもらえるのではないか。

(3) 中小・地域に関して

○湯淺委員

・　サイバーセキュリティお助け隊では、関係者の皆様の尽力により大変成果を上げていただけて良かった。今後の自走に向けては、中小企業向けになると価格設定が非常に難しいということもあり、今後はグループ会社など地域のベンダーが中心になっていくのかと思う。そういう点では、そのようなローカルな地域ベンダーを巻き込んだコミュニティをつくることも重要になってくる。

○上杉様（藤原委員代理）

・　地域のコラボレーションについて、今後は是非リモートでのコラボレーションも活性化させていただきたい。コロナによるプラス要素として、場所に制約が無くなったというところが非常に大きいと思っている。これからはリモートファーストで考えないといけない。

○秋元様（佐藤委員代理）

・　中小企業は、セキュリティのみに特化して時間を取ったり人を育てたりすることは難しい。生産性向上・デジタル化とセットでセキュリティの取り組みを進めていただきたい。
・　中小企業が利用しやすい制度である、サイバーセキュリティお助け隊は、商工会議所も普及推進に取り組みたい。地域のセキュリティについて、顔の見えるコミュニティ形成などは中小企業にとって大事だと感じている。わかりやすい情報発信に努め、中小企業にとってのハードルを少しでも軽減していく取り組みを、商工会議所も一緒になって進めたい。
・　人材育成は、情報処理技術者試験やITパスポート、セキュリティマネジメント資格等に関して、中小企業の従業員や新入社員等により活用を広げられると良い。

(4) 人材に関して

○松原様（横浜委員代理）

・　高専から大学、経営層に至るまで幅広く人材育成の取り組みを進めていただき心強い。人材育成の取り組みと同時に、そういった人材が活躍できる場の確保の支援も進めていただきたい。例えば、学生向け、社会人向けのキャリア相談などが考えられる。
・　コロナ禍のテレワークの推進によるIT環境の変化や不景気に伴い、内部犯行の脅威が高まっている。転職支援サービスに見せかけたなりすましメールにより情報漏洩する例もある。海外では、折角サイバーセキュリティのスキルを身につけながらも、職につけなかったがために、攻撃者に転じた人たちの例も報じられている。
・　人材に関しては多面的な支援が必要なのではないか。

○湯淺委員

・　高専はじめ教育機関との連携の成果が上がってきていることを紹介いただいた。教育現場にいる者の立場で申し上げると、セキュリティに関する様々な補助金や予算が、かなり減額されている。セキュリティ教育は非常にお金がかかるので、継続的なご支援をいただかないと、教育機関が早急に自走するのは難しいだろうという危惧を抱いている。

○塚本委員

・　人材確保の手引きは、医学部出身の学長にセキュリティ人材雇用の際に、職務内容を説明するときに活用した。た

いへん理解しやすい非常に良い資料になっていると思う。

(5) 国際に関して

○湯淺委員

・ コロナにも関わらずオンライン等で国際的な取り組みも進めていただいていて大変有難い。ひとつ気になっているのが、各国、特にアジアで、いわゆるデータローカリゼーション規制が非常に強まりつつある。セキュリティを確保しつつ、データの囲い込みはやめようということが、日本にとっては重要である。

(6)その他

○丸山委員

・ これからの社会においては、クラウドが世の中を飲み込んでいくというイメージを持っている。そうなった場合に、今は各企業でセキュリティ対策を考えているが、そういう対策もクラウド事業者側の設定の問題になってくる。これから先を考えてクラウド事業者とまずは連携してどういうことをこれからセキュリティや社会インフラとしてやっていかないといけないか、場合によっては規制の強化なども必要かもしれない。今後の課題かもしれないが、クラウドと共にある社会という中でセキュリティはどうあるかという方向もこれから考えていかないといけないと思う。

○名和委員

・ 正規なプロセス、または正常なやりとりから入ってくるSolarWindsのようなものに対する危機意識が、まだ十分に反映されていないような気がする。
・ 次のステップとして、サイバー攻撃を受けた後、いち早く事業を再開するノウハウの共有などを、この機会にビルドインしていくとより良いフレームワークになっていくと思った。
・ 海外拠点・外部拠点で困っているのは、現場の方々が証拠を無意識に削除してしまって、本来わかるところがわからないということが増加傾向にあるように感じる。フォレンジックのノウハウも共有していく必要がある。

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