産業サイバーセキュリティ研究会
第9回 ワーキンググループ1（制度・技術・標準化）
第7回 WG1分野横断サブワーキンググループ
合同会議
議事要旨

1. 日時・場所

日時：令和4年4月4日（月） 15時00分～16時35分

場所：Web開催

2. WG1出席者

WG1委員 ：佐々木委員（座長）、石原委員、上原委員、内田委員、江崎委員、岡村委員、後藤（里）委員、其山委員、高倉委員、丹委員、中野委員、坂委員、平田委員、松尾委員、松本委員、森委員、渡部委員

専門委員 ：瓜生専門委員、坂下専門委員、田中専門委員

分野横断SWG委員：佐々木委員（座長）、石原委員、岩﨑委員、大久保委員、大浪委員、粕谷委員、菊池委員、桑名委員、後藤（俊）委員、後藤（里）委員、古原委員、坂下委員、佐藤委員、谷委員、中尾委員、平田委員、洞田委員、山田委員、吉田委員、米田委員

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、厚生労働省、農林水産省、国土交通省、防衛装備庁、デジタル庁

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 奥田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 WG1委員名簿

資料3 WG1分野横断SWG委員名簿

資料4 事務局説明資料

資料5 協調的なデータ利活用に向けたデータマネジメント・フレームワーク ～データによる価値創造の信頼性確保に向けた新たなアプローチ（案）

参考資料1 主なインシデント事例

参考資料2 OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集

参考資料3 IoTセキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集

参考資料4 IoTセキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集（概要版）

4. 議事内容

事務局から、資料4について説明した後、自由討議を行った。委員からの意見は以下のとおり。

●産業分野別SWG

中小企業対策について、例えば自動車業界はすそ野が広く、サプライチェーンに対するリスクを負っている。経産省が行っているサイバーセキュリティお助け隊サービスもあるが、なかなか普及が進んでいかないので、国家レベルと業界とが補い合って相乗効果を出していけるような取組を強化していきたい。また、中小企業もセキュリティ対策をやるのが当たり前というような相場観を、業界として醸成していくとともに、国としても、法的、あるいはガイドラインのような形で強制力のある形

でやらないといけないのではないか。もしくはセキュリティ対策をやったら得するといった宣伝活動も強化する必要があるのではないか。

今回の資料では経済面としてどうなるという点がなかったが、そうした点もう少し整理することが非常に重要。また、デジタル臨調で全ての監視や管理をデジタル化するということを国の戦略として進めていくとされたが、サイバーセキュリティは当然、その前提として入ってくるというところを、デジタル臨調との整合性から経産省として押し出していくことが必要。そのとき経済面がKPIとしてKGIの1つとして入っていて、その際にどのような目標値となるかといった具体的な数字の議論ができるとよい。

工場ガイドラインは、一業界だけではなく産業界を横断する形で取り組まれることを期待する。業界としても、サイバーセキュリティに関する相場作りのようなものや、標準化などに取り組んでいきたいという意識でいる。

工場ガイドラインは、ベースラインの部分は共有のナレッジという形にできればコストダウンに繋がるし、業界ごとに特化した部分については業界ごとに定めていくという形で運用していければ非常に効率的。

例えば資料4 p.64で、IoTやDigital Twinとの連携を標準化の中でということがあったが、非常に重要な概念。IPAのDADCデジタルアーキテクチャ・デザインセンターで、スマートビルというプロジェクトが行われている。いま、ビルの中のデータで一番ホットなところは、IoTにより人のデータをどのように取るのか、それがデジタルデータとしてどのように連携していくのか、それ次第で新たなバリューチェーンが生まれてくるのではないか、という点に注目が集まっている。これはまさにビルのAs-IsというよりもTo-Beの世界としてしっかり描き切って、それを実現するために、これが必須であるというような議論を進めていくということが、今後重要になる。その手のアーキテクチャ設計は、DADCがやらなくてはいけないところではあるが、経済産業省としてもそういった活動と連携し、将来的なデジタル世界、サイバーフィジカルシステムが普及する上で、協力していくことが必要。

●第3層タスクフォース、データマネジメント・フレームワーク
ユースケースは異なるケースに対して共通のモデルを適応されていてよい取組。一方、新しいユースケースに対してモデルを作っていくとなると、この例だけだとイメージし辛い点があるため、モデル構築のプロセスについても共通化したものとして提供ができていくとより普及するのではないか。

いかにガイドラインを普及させていくかが非常に重要。現場になればなるほどガイドラインの考え方がどうなっていくかわからないことが多いが、その際に今回作成されたユースケースは有用。このフレームワークのユースケースをもっと拡充されることで、フレームワークの意味も業界を超えて理解できるようになると、より分かりやすくなって良い。

セキュリティの情報を扱う者にとって、データがどこまで使えるのかということには、非常に関心がある。改正個人情報保護法においてもまだ不透明な点があるので、是非、個人情報保護法との整合性や、グローバルにおける個人情報、また事業情報のデータの使い方について、議論を深めていければよい。

セキュリティを担保する上で、マルウェアの情報を解析することがあるが、そのようなセキュリティを解析する場合の個人情報へのアクセスについても、議論を深めていき、もっとフレキシブルに対応できるようになるとよい。

データマネジメント・フレームワークは非常に良いまとめ方がされている。どう定着させていくかという政府の方向性についても賛同。特にデータの越境移転については、データは、転々流通して形が変わるタイミングで必要な属性情報が変わってくる。例えば、デジ庁で取り組んでいるベース・レジストリとの関係を整理していくことが、クロスセクターを考えると必要になる。データマネジメント・フレームワークメントフレームワークを定着させていくことが必要。

データマネジメント・フレームワークは、データ流通のユースケースとして非常にわかりやすい。今後、AIが使う学習データの流通や利活用など、これからDFFTで出てくるような新しいモデルでの検討も進めていくとよい。

IaaS/PaaS/SaaSのところで、状態の整理としてはわかりやすいが、モデルそのものが複雑すぎるので、ビジネス的にどうしていくかという提案までもう一歩踏み込んでも良いのではないか。クラウドの場合では、ビジネス上の要求事項に対して、適用技術やサービスの選択も活用のポイントになるので、そこまで含めて利用者側のPDCAにつながるような提言まで今後ご検討していくとよい。

データ流通に関して、現在、綺麗に第2層、第3層と切り分けて議論されているが、一方で、物理層、第2層、第3層の中で情報が回ってデータがリッチになっていくことが今回考えている世界だとすると、どこかの層でデータに不具合や瑕疵や改ざんがされるとか、偽の情報が紛れ込んだときに、それが回って影響が広がっていかないようにするための枠組みをどうするのかを考えておく必要がある。それぞれの層で守ることは当然大事だが、他の層に影響が及ぶでは困るので、すべての層を俯瞰するような何らかの枠組みが必要ではないか。

データマネジメント・フレームワークだけが、データの第3層で完結するのではなくて、第1層、第2層で作られたデータが、どれだけトラストワージーネスで作られているかなどの連携をうまくはめていけるような形でフレームワークとして検討するとよい。また、デジタル庁や、厚労省といった、データのやり取りについて違うフレームワークとして検討されているチームがあるが、どこまでが必須でどこまでが拡張なのかがうまく取り纏めてられると、各領域、ユースケースで検討する際に分かりやすくなる。今、海外の法制度体系とは比較しているが、国内で分かりつつあることに対してもうまくまとめられるとよい。

データマネジメント・フレームワークについて、ユースケースが付いて、具体的に理解がしやすくなった。今回、行政分野で率先して実行するということで、是非ともセキュリティ向上にどのような効果があるかが早めに示されるとよい。

データマネジメント・フレームワークのユースケースについて、まず、DXをターゲットにして、製造業のDXの中で付加価値を上げるエンジニアリングチェーンにどのようにデータを集めるのかという例を示して、それにGDPRと中国のサイバーセキュリティ法を照らし合わせるとCPSFとNISTのSP800-171などのこの対策をシステムに適用していれば良いというような、一気通貫のものになる。現場では、セキュリティの専門家と情報システムの管理者とIoT事業をやっている人がいて、今までは情報システムの管理者が、間を取り次いでくれていたが、データになると情報システムをやっている人は、データには関知しないというスタンスで、システムを作っている。データ管理の詳しい人は、いろいろと分類に関して細かい話をすると、実はセキュリティの専門家も、情報システムの管理者も、IoTの事業者も、誰も分からないという状況になってしまい、皆をひとつにまとめて議論することが非常に難しい状況。そのような時はビジネスをベースとしたユースケースから落とすことが一番わかりやすい共通語になるので、是非とも製造業のDXのエンジニアリングチェーンに付加価値をつけるような、経産省のDX集にもあるような例から対策まで一気通貫のようなものがあるとありがたい。

●ソフトウェアタスクフォース、SBOM
米国においては、SBOMは特にヘルスケアとファイナンスに取り組んでいる。米国とのインターオペラビリティを確保するためにファイナンシャル、例えばクレジットの領域などで実証をトライしてみるとよいのではないか。

SBOMは各国で、規制などのエコシステムができあがってくると、日本の産業がついていくのは大変。今後、SBOMの脆弱性の対応の実証を進める際には、それを有効に活かしていくような、日本ならではの官民の連携や共助の仕組みなど議論できるとよい。

SBOMについて、現在、米国や海外含めて足並みを揃えて進めているところと理解。その際、SBOMのフォーマットが、日本独自にならないように留意することが必要。また、エンドユーザ企業と話をしていると、ベンダー側からSBOMの情報を出してもらえないと、進められないという姿勢で静観しているという企業が多いように感じているので、SBOMを使うことのメリットや、使わないことのデメリットを普及啓発していく必要がある。

SBOMに関して、どこまで深堀して追いかけていくかということを、そろそろ真面目に考えないといけないの。Log4Jの件でも明らかなように、ほとんどのところが使っていることすら意識していないものがこれからたくさん出てくると思う。一個一個のOSやプログラムのモジュールまで全部追いかけていくのか、それを誰が管理していくのか、またそもそもそのモジュールを使っていることを公表するのかしないのか、公表できないものをどのように扱っていくのかなど、色々な検討すべきハードルが出てくる。

自社でSBOMの取り組みを行う中で、今まで独自で作っていた部分がリプレースされて、OSをインストールするようなユースケースも増えてきているなかで、どこまで管理するのか、どこまで深掘りできるのか、悩んでいる。また、課題だと思っていることは、SBOMを作るプロセスと、作った後に、脆弱性情報とマッチングすることができる技術者が足りない点。その影響は何かというところについて、ソフトウェアのサーバや情報システムで、それを解釈する人材不足、力不足を感じている。使う部分でも新しい課題が出てくると思うので、どういう仕掛けが必要か、検討が必要。

プロダクトを提供するプロバイダー側としてもOSSを始めとしたソフトウェアの脆弱性の早期検知と、ひいては対応という意味で、プロダクトSIRTとしての活動として、構成情報のデジタルでの把握は喫緊の課題となっていて、非常に重要な取り組みだと捉えている。これを実現するために、データをどこまで管理するのか、コストや運用のフィージビリティなども重要。また、フォーマットの標準化なり、運用の定型化が課題になってくるが、そのためにインダストリーごとの実証を行うことが実践的な活動。一方で、今、各種製品形態での提供というのみならず、クラウド上であらゆるソフトがさまざまなサービスに組み込まれてきている時代であるので、インダストリーのプラクティスが、業種を超えたサービサーにとって有効な事例になってくるのではないかと期待している。

実体であるソフトウェアとSBOMで管理しているものが乖離してしまわないように管理していかないといけないが、その管理体系の仕方についても、運用規則、あるいは運用ガイドラインとしてまとめるとよい。それをやっていなければ調達しない等が言えるガイドラインであれば、各社としてもSBOMを取り入れていくトリガーになる。

●第2層タスクフォース、IoT-SSF
IoT-SSFは、3軸を持っているモデルで、第3軸にいろいろな観点が入っている。3軸の第3の観点として運用者、運用管理者の能力に対する要求や、第4の観点で社会的なサポートの仕組みの要求などが入っている整理は、世界中を見てもあ

まりないとの指摘があるので、是非、これをうまく活用していけると良い。

資料4 p.69の今後の課題の所に「自立的な活用の促進に向けた制度設計」があるが、例えば製品を提供する側が、この製品については、このようなIoT-SSFに従うと、このような形になるので、このような点に十分に気を使っているということを出してもらう仕掛けが1つのやり方なのかと思う。

IoT-SSFの第3の観点、第4の観点については、大変期待している。社会的サポートや、実際の運用管理などが、どのようにこういった観点と結びついていくか期待している。

●CPSFの国際規格化
サイバーフィジカルシステムの概念モデルに基いた海外の考え方も吸収した形で全体の規格にしていこうとしている。今後、ユースケースを具体的に入れていくなどのフレームワークを具現化していくアプローチで進めていく予定。今後このような国際基準を進めていく中で、具体的に標準を作る時に、経済産業省で行っている事業の成果やガイドライン等を標準に入れていくのがよい。

CPFSのコンセプト等で国際標準を進めていて考えていくと、IoT-SSFは、第2層というよりも、全体のCPFSを包括するような1つのフレームワークになっていると理解している。

●今後の方向性、CPSF等文書の改訂スキームの構築（案）
CPSF等文書の改訂スキームの構築（案）は、WG、SWG、TFで作成した文書、業界別のガイドラインなどをスピードアップして出したいということと理解。

CPSFの改定、特に国際標準の変化により受けた影響に関して修正していくことはよいこと。また、CPSFそのもののが、良かったかなどの検証は、SBOMの実証のようにベストプラクティスが蓄積された時に行われるべき。

CPSFは、産業別のガイドラインも出揃ってきて、大変多くのナレッジが集約されてきている。今後の普及に向けて、大きなポイントとなってくるのが、中小、中堅の組織。これらの企業はセキュリティに関するリテラシーやマインド共に大きな掘り起こしや注意喚起が必要な状況。そういった企業には、とにかく実例や具体例、どのようにすれば良いかといったアクションアイテムのようなものを具体的に解きほぐして、分かりやすくご説明していく必要がある。例えば、産業別に出そろったガイドラインからエッセンスを抜き出して、少しサマリして提示していくような形で、今後出てくるものの普及も兼ねて、そういったコンテンツの活用を検討するのがよいのではないか。

コンサル会社がユーザ企業に提案をするとき、1つのフレームワークを使うわけではなく、いくつかのフレームワークを参照しつつ提案する。この時、サプライチェーン対策でユーザ企業がガイドラインを使おうとしたとき、様々なガイドラインに分散して記述されており、どう使ったらよいのか迷うことがある。特にサプライチェーンは、CPSFの非常に重要なポイントであり、国内のガイドライン、法案との整合を図っていくことも非常に重要。横断的にいろいろなガイドラインに散りばめられているところをうまく使えるようなガイドが、併せてできると良い。また、実際にフレームワークを使うのは、ユーザ企業に提案するコンサルというところがある。今後ガイドラインの普及にあたっては、コンサルティング会社にうまくアピールできるとよい。

普及の観点で、CPSFについて、セキュリティサービスを提供する立場として現場にいて感じることは、なかなか理解している人が少ない、知っている人が少ないということ。知っている人が少なければ、それを実際に適用してアセスメントとして実施するという人が少ないということなので、認知率などを増やすことをしなければいけない。具体的には、情報処理安全確保支援士の定期研修などに実際のユースケースを入れ込むなどして、活用できる人を増やすための施策を進めるとよい。また、企業からCPSFのアセスメントを依頼される機会が、現実的にほとんどないので、企業に対しても経済産業省側からCPSFを使用することのメリットや、しないことのデメリットを普及啓発していくのがよい。

周知の方法は多岐にわたるが故に、誰向けに何をといった整理があると周知もしやすいのではないか。また、ガイドラインの紐づけも意識するとよい。

サプライチェーン全体の底上げが非常に重要。自動車業界は、業界大でSWGでも活動しているし、個社でもサプライチェーン全体に対する取組として対策を進めているが、ガイドラインなどの改定を通じて、より強いメッセージをサプライチェーン全体に出していけないか。一つの業界や個社からでは限界があり、中小企業では自分事になりにくいところもあるので、中小企業向けとしてガイドラインが出ても、所詮大企業向けで自分のところは関係ないというようなところもある。本当により強い中小企業も含めて全企業までもやらないといけないというところを強く打ち出し、全体の底上げに結びつけていくことが必要。是非、経営ガイドラインの改訂や、新たなものを含めてメッセージを出していけないかと感じている。

●その他
サプライチェーン対応水準の格上げということで、中小企業対策に取り組むという点での委員の意見には賛成。あわせて、サイバーセキュリティ経営ガイドラインは、経済安全保障や、リモートワーク対応などいろいろな課題が出てきているので、アップデートをお願いしたい。

大阪万博が、経済産業省として重要なイベントになる。セキュリティという意味でも、サプライチェーン全体の守り方という視点をあわせ、実証実験の場として活用するのがよいのではないか。

第3層TFで議論が行われた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」につきましては、事務局において発行に向けた手続きを進めていくことで了承を得た。

以上