産業サイバーセキュリティ研究会
第8回 ワーキンググループ1（制度・技術・標準化）
第6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3年3月15日（月） 10時00分～12時00分

場所：Web開催

2. WG1出席者

WG1委員 ：佐々木委員（座長）、岩見委員、上原委員、江崎委員、太田委員、岡村委員、片山委員、九野委員、植田様（小松崎委員代理）、其山委員、高倉委員、坂委員、平田委員、藤井委員、松尾委員、松本委員、渡部委員

専門委員 ：瓜生専門委員、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、大友委員、岡田委員、粕谷委員、川口委員、菊池委員、桑名委員、後藤（俊）委員、後藤（里）委員、古原委員、谷委員、中尾委員、平田委員、山田委員、吉田委員、米田委員

オブザーバ：警察庁、金融庁、厚生労働省

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、鴨田サイバーセキュリティ技術戦略企画調査官

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 サイバーセキュリティに関連する海外の動き

資料5 サブワーキンググループ、タスクフォース等の検討状況

資料6 スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン（案）

4. 議事内容

事務局から資料4～6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。

●スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン（案）について

スマートホームの場合、非常に多様なステークホルダーが関わっており、機器の所有者と使用者が異なる場合もあるため、脅威やリスクがどのような資産に基づくか、誰にとってのリスクかが、分かりにくくなっている。今回のガイドラインでは、ステークホルダーに対する脅威やリスクなどという点でまとめられており、期待できる。

システムの概要がステークホルダーと関連づけて整理されており、その後、スマートホーム固有の脅威、攻撃方法、対策を検討する流れが示されている。今後、他の産業分野でガイドラインを作るときにも非常に参考になる。

現段階では、一つの宅内ネットワークに情報機器と IoT 機器が並ぶ状況だが、今後の IoT 機器の増加を考えると、宅内ネットワークを情報系と IoT 機器系に分離して管理することでセキュリティを確保することも考えていく必要があるのではないか。

バージョンアップの際には、例えばスマートホームに特化した詳細な実装方法や、ガイドラインの手引きなどが追記されるとより有効となる。また、IT に関する知識が深くない方に対しての教育施策を今後検討して欲しい。IoT デバイスの誤設定・ヒューマンエラーをどう防ぐかという教育も重要になる。

●産業分野別 SWG について
産業サイバーセキュリティ研究会 WG1で策定した CPSF を標準モデルとして、用途別、業界別という観点で SWG が立ち上がってきており、スマートホームや宇宙産業での議論が進んできている。産業分野別ガイドラインによる日本社会全体の底上げを、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)等の議論や人材育成、ビジネス化など他のWGの議論と連携して進める必要がある。

各産業分野別 SWG におけるガイドライン作成や展開によって知見が溜まってきており、その知見をフィードバックして CPSF 本体の改定やレベルアップの議論にもつなげていただきたい。

産業分野別に色々な枠組みを作っている一方で、分野間で共通の部材や IoT デバイスなどが結構出てきているので、全体を見たような対策も考えていただきたい。

各産業分野別 SWG において、それぞれ良い成果が出てきているので、第 2 層 TF でのアウトプットの枠組みを使い、産業分野別に具体的な事例などを検討していくのが良いのではないか。サイバーセキュリティエンジニアリングについては、開発プロセス等のマクロな議論は進んでいるが、詳細なところは安全分野ほどできてきていない印象。そのようなところに第 2 層 TF の結果などもうまく使っていけるかもしれない。

本 WG の資料を産業分野別 SWG やガイドラインがない分野に紹介すると、自分の仕事にどのように影響するのか、というような反応がある。自分たちも業界ガイドラインのようなものを自主的に作らないといけないのかと感じている方へのメッセージのようなものが必要な段階なのではないか。

●第 3 層 TF の検討内容について
なかなかデータ流通が進まないところに対し、転々流通と加工を前提にデータへ着目して整理していくというアプローチはとても良い。責任主体、ステークホルダーがどのような責任を持つのか、色々なバリエーションがあるので、ユースケースとして整理していくと良い。

第 3 層 TF の領域は、トラストもしくはデジタルトラストと言われている領域にかなり関係すると理解しており、デジタルトラストという言葉一つとっても、語る人によって大分範囲が違うという印象を持っている。デジタルトラストもしくはトラスト全体をどのような枠組みや建付けと捉え、その中で第 3 層 TF はどのような部分を詰めていくのか整理いただけるとありがたい。

API とプロトコルをしっかり区別することが重要。API を公開すればつながるだろうという議論が行われることがあるが、そこだけで実装するのは非常に困難で、共通のプロトコルが必要になる。第 3 層 TF の議論はこの課題に対応したものになる。

アンバンドル化が目標の一つに掲げられているが、第 3 層が処理されるクラウド等の場を考えると、非常に適した考え方。

産業機器のデータについて欧州と議論すると GAIA-X の話が出てくる。日本の製造業各社の機器のデータが日本の各社に戻ってくるようにするためにも、GAIA-X などとの整合性も視野に入れると良い。

基準となる属性のセット、オントロジーのようなものが決まっているとよい。国で議論している日本版 NIEM や共通語彙基盤のようなところの議論と組み合わせて検討いただけるとありがたい。

●ソフトウェア TF における SBOM の実証事業について
SBOM の実証を我が国でも実施したいという話には賛同。他方、米国のように金融やヘルスケアへ適用するには様々な問題や課題もある。分野横断 SWG を活用し、適用分野を含め検討するとよい。また、実証の中で、脆弱性管理の負担をシェアできる等の具体的なメリットを示せると良い。

大手サプライヤーは個々に SBOM のようなソフトウェアの構成情報を登録し、脆弱性等の影響分析等を行っているが、業界として取り組むことに意味がある。他方、組込みソフトウェアの多い業界では、どのようなソフトウェアを使っているのか自体が競争力の源泉である場合もあり、SBOM の共有には抵抗感もある。競争力ではないところを選んで共有できるとか、他社には知られないが、登録しておけば自分のところが使っているソフトウェアの脆弱性を知ることができるシステム等、安心感を与えるような形で進めることが重要。

中小企業や組織にとっては、SBOM の活用も含め OSS 管理が大変なために OSS の活用が進んでいないという現状があると認識。実証においてそのような課題が解決されることを期待。

OSS だけではなく商用ソフトウェアも含めて名称の統一化などができていないと、非常に手間もかかり共有が難しいため、名称およびフォーマットの統一のようなところの取組があると良い。

●その他
セキュリティとプライバシーは表裏一体であり、日・欧・米のプライバシーフレームワークが今後のパーソナルデータの流通において重要。

2020 年の EU 司法裁判所におけるプライバシーシールド協定の無効判決は、この協定で創設されたオンブズパーソン制度に法的強制力がないことが理由となっており、主権の問題と言えるが、議論が錯綜している状況。

英語化を進めることは、特に欧米の状況変化への打ち込み、整合を取っていく意味で重要。AI 技術や言語処理等の技術を使うなどしながら、経済産業省全体の取組として英語化予算を確保するなどして実現していく必要がある。

CPSF の標準化を ISO/IEC JTC 1/SC 27 で進めており、現在は新規課題になる手前の PWI（Preliminary Work Item）という状態。この段階である程度ステーブルなものを作って後の議論を短縮しようとしているが、なかなかスムーズにいかない。PWI では、サイバーフィジカルシステム全体のコンセプトのモデルを示して、その中のセキュリティの考慮要素として、日本の CPSF が一つの例になるという構成にしている。各国は、スマートホームやビルや自動車など具体的に活用しているユースケースに興味があるようだ。日本の中でガイドライン等の検討を進める上では、検討のスコープと国際的な検討状況との関係が整理できていると、国際的な議論にスムーズにインプットできると思われる。

人の育成がそれぞれの分野で必要になってくると思うが、これだけ動きが速い中で決まっていくガイドラインに対し、自分たちの会社が、どの段階でどのようなスキルセットを持ったエンジニアを投入して、製品開発やシステム開発につなげなければいけないのかという線表が引きにくくなっている印象。それに対する答えが必要な時期にある。

スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインの案について、いただいた意見を踏まえて座長に相談し、ガイドライン案に修正を加えた上で公開すること、公開後の改定などは JEITA にて実施することで了承を得た。

以上