# 産業サイバーセキュリティ研究会
# 第10回 ワーキンググループ1WG1（制度・技術・標準化）
# 第8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6年3月14日（木） 16時00分～17時40分

場所：オンライン開催

## 2. 出席者

WG1委員　　：佐々木委員（座長）、石原委員、内田委員、後藤(里)委員、鈴木委員、其山委員、多田委員、松尾委員、松本委員、渡部委員、志村様(丹委員代理)

WG1専門委員　：高柳専門委員、坂下専門委員、田中専門委員

WG1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、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

分野横断SWG委員：佐々木委員（座長）、石原委員、岩﨑委員、大浪委員、菅野委員、菊池委員、熊坂委員、後藤（俊）委員、後藤（里）委員、古原委員、坂下委員、鈴木委員、谷委員、中尾委員、洞田委員、吉田委員、米田委員

分野横断SWG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、総務省、防衛装備庁

事務局　　：経済産業省商務情報政策局　武尾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

参考資料1 ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引

## 4. 議事内容

●産業分野別セキュリティ対策について

- ISO/IEC で PJ エディタを務めているが、CPSF をアピールしようとする中で、ドイツも OT/IT フレームワークという枠組を入れ込んでいる。その中でユースケースを作成しており、スマートホームやビルシステム、サプライチェーン等を扱っている。SWG で様々なガイドラインを作成されている中で、それらからサポートをしていただける体制を構築していただきたい。
- これまで ISO/IEC 27001 に長くかかわってきたところ、横串を刺すという点にこだわると ISO/IEC 27002 等のような内容になるのではないかと思われる。ISMS では現状はベーシックな内容の上に業種ごとのスペシフィックなセクターの内容が乗る構造となっている。従って、本プロジェクトではガイドラインの策定だけではなく、その活用をにらんだ普及の促進も重要となるため、その点は政府として留意をお願いしたい。

- 半導体関連産業のセキュリティ確保について、ここでは、サイバー攻撃を外部から受けて製造やロジスティクスが停

止する事例が扱われているが、単にオペレーションが停止するというだけでなく、中を流れる製品の品質にも課題があるようにも思われる。

・ CPSF 国際標準化の取組みが進んでいる点、ありがたく思う。ただし、議論がハイエンドなところ、適用の際に具体的に何をすべきかという意見がユーザー事業者から出ているように思われる。

・ また、産業分野におけるサイバーセキュリティの底上げにはユーザー企業における技術者の意識向上が必要と認識している。様々な技術が登場する中でユーザー企業側の取組みが追い付いていないように思われる。SBOM 等についてもよい取組みと考えるが、教育や普及活動が不足していると考える。

●セキュアバイデザイン、サプライチェーン全体のセキュリティ対策強化について

・ 普及のインセンティブとどのように結び付けていくかを引き続き議論できればと思う。

・ サプライチェーンについて数社ヒアリングしたが、2 社間で取引をする際に取引条件が生じるようである。ビジネスの上に立脚できるセキュリティを構想いただき、国際の場でも議論していただければと思う。

・ 自動車業界では「自工会/部工会・サイバーセキュリティガイドライン」を既に運用する中、IPA の「中小企業の情報セキュリティ対策ガイドライン」との連携も図っているが、他の業界でも同様の必要性が生じる可能性がある。また、星の数による成熟度表示は業界によらず中小企業の良い指針になると思う。様々な既存のガイドラインに横串を刺す活動を一層強化して欲しい。

・ 既存の認証制度の活用も含めてご検討されたい。

・ セキュリティアーキテクチャについて、全体的な動きには賛成するが、IoT 製品の認証等も進められる中、事業者側の負荷が極端に上がらないよう配慮いただきたい。

・ 全ての産業はつながっているため、ぜひ全ての業界が取り組める対策レベルの可視化を推進いただきたい。どのガイドラインにこだわるかということもなくなり、全体として進めやすくなるのではないか。中小企業を念頭に置くと、より簡便な取組みやすい施策について、サポートも含めて考えていくべきかと思われる。

・ 第三者認証を含めた可視化について、横串を刺すものから業界特化のものまで基準ができるとありがたい。また、初期的なものはわかりやすいところからスタートし、レベルアップできる内容となっているとありがたい。

●ソフトウェアタスクフォース、SBOM について

・ SBOM には、製品の差別化やコスト削減につながる情報が含まれており、二者間で企業秘密の保護に関する規定があれば利用が促進されると思われる。また、SBOM 提供が義務化される可能性がある中、すべての要素を提供しなければならないか、ネットワークに面して攻撃される可能性が高い部分に限定するかなど、提供する範囲をいかに限定するかというスコープに係る議論がなされることを期待する。

・ 供給側と利用側の双方から経済的な動機付けが必要と言われる。調査研究等を通じて、SBOM の活用等によるコス

ト削減効果などを明示いただけるとありがたい。

・ SBOM の普及が課題になる中で、単なるリストの管理にならないよう注意が必要と考える。脆弱性管理につなげていくことが重要であり、サイバーハイジーンやポスチャー・マネジメントといった高いレベルを目指していただきたい。SBOM 情報の共有について、受け手側の情報管理だけでなく、脆弱性管理等での活用についても責任関係の明確化が必要と考える。

・ ビジネスに SBOM を要求として入れ込んでいくことが必要である。政府調達から入れ込んでいくことも有用ではないか。第三者認証を求めることでコストが増大する場合、適切な支援策と組み合わせて事業者をサポートできないか。

・ SBOM のガイドについて、利用する立場がユーザー、開発者、インテグレータといる中で、立場によって活用方法等が異なるように思われるため、ガイドにも反映されたい。規模や業種により具体的な活用方法は変わるように思われるため、共通部分とカスタマイズできる部分に分かれているとよいと思う。

・ 小規模な実証事業からいきなり社会実装に向かうには大きなハードルがあると思われる。SBOM はインフラを支える技術であるため、段階を踏んで検討を進めていただけるとよい。

●公的機関の役割について

・ また、公的機関のあり方として、様々な業界でアウトプットが出される中、有効性の評価を実施しては如何か。大きなシナリオのパターンは大きくは変わっていないように思われるため、これまでの取組みが基本的なボトムアップにどれだけ貢献されたかを評価されたい。

・ 米国では国主導でカンファレンスを実施しており合意形成をしている事例があるが、日本でも同様な場があるとよい。現在はそのような場がないと認識している。
・ また、事業者としてサイバーセキュリティに関して様々な政府機関の動きをみる必要がある。IPA 等が中心になると思われるが、公的機関の役割を整理いただきたい。

・ 経済産業省における他の取組み(例:デジタルライフライン全国総合整備計画、ウラノスエコシステム)などを活用していただけないかと思う。

●最新の技術動向について

・ AI について申し上げると、セキュリティ、品質、倫理(エシカル)という面でいくらか重複があるように思うため、抜け漏れのないよう整理を進めていただければと考える。

・ セキュリティ製品においても AI 技術の活用が増えているが、AI について日本でも法規制を行う場合に企業の負担がなるべく少なくなるようお願いしたい。ISMAP 等の既存制度は事業者にとって大きな負担となっている。

・ AI とセキュリティの関係について、4 つに分けて考えるべき。すなわち、AI を使った攻撃、AI による攻撃、AI に対する攻撃、そして AI を利用したセキュリティ対策。具体的な対策を決定する際、リスクアセスメントやリスクコミュニケーションを考慮し、相互に合意がとれるものとする必要がある。

・ JTC 1 では 27090 として AI の脅威および軽減策について議論されている。AI に係るデータ収集や学習等のプロセスにおいて、さまざまな攻撃手法がある点や軽減策が標準化されつつある。それらの動向についても十分考慮された上で検討を進めていただきたい。米国では AI を用いて防衛能力を高める点について注力しており、日本としてもAIの観点からイニシアチブをとれる技術を生み出していくことが重要である。

●その他

・ IEC の動向を共有する。IEC 62443 シリーズが既に策定、参照されている中、それらを制御システム以外にも適用しようとする動きがある。推進派は強引にすべての分野に適用しようとしている。IEC 62443 とどう付き合っていくかについて、分野ごとに意見表明することが必要となる可能性がある。

・ カーボンニュートラル等の文脈においてサプライチェーンでデータをトレースする必要がある中、セキュリティについてもそのようなアプリケーションを想定しながら検討を進めていただければと思う。

・ 情報を一元的に管理し、参照できる状況を作っていくことが重要となる。エビデンスを確保する仕組みが必要ではないか。

・ ガイドラインを策定しただけでは効果がいまひとつというところがあり、如何にその有効性を評価するかなどの施策を考慮していただければ、より本プロジェクトの意義が有益になると思われる。

・ サイバー攻撃が大規模化、巧妙化する中で、サイバー攻撃に関する機密情報について、政府間、官民での情報共有が必要と考えるところ、セキュリティクリアランス等とあわせて議論をお願いできないか。

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

以上