産業サイバーセキュリティ研究会
第11回 ワーキンググループ1（実効性強化・国際連携）
第9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7年4月14日（月） 15時00分～17時00分

場所：オンライン開催

2. 出席者

WG1委員　　：佐々木委員（座長）、渥美委員、上原委員、江崎委員、岡村委員、中嶋委員、其山委員、高倉委員、多田委員、丹委員、古田委員、谷委員、依田委員

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、内閣府、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）、大久保委員、菊池委員、後藤（俊）委員、古原委員、坂下委員、高橋委員、中尾委員、中嶋委員、洞田委員

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 奥家大臣官房審議官、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 ワーキンググループ1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

4. 議事内容

＜Secure by Design の実践＞

- Secure by Design について、Secure Software Development Framework（以下、「SSDF」）のように具体化されていることは産業界におけるセキュリティ担保の観点で喜ばしいことである。具体的に産業界へ適用する際には、既存の制度(例:JC-STAR)や規制(例:欧州 AI 法、欧州サイバーセキュリティ法)等とのすり合わせが必要となる。
- 日本の製造業では、ソフトウェアの品質管理に対する解像度が低く、SBOM 導入に係る手間と効果を把握しきれていない可能性がある。また、そもそもそれぞれの部品がどれだけセキュアにできているか、Secure by Design に作られているのかどうかの判定がうまくいっていないのではないか。
- 米国では、ソフトウェアに関して、SBOM や、”BACK TO THE BUILDING BLOCKS”と題された文書で示されるものなど、解像度の高い対策が出てきている。それに対して日本はどう対処するか、掘り下げていかないといけないため、そのための制度設計やインセンティブ付与が課題である。
- SBOM の作り方によっては、商業秘匿の都合で、ソフトウェアの流通経路を非公開としたい企業がみられる。SBOM 開示のインセンティブについて考える必要がある。

＜セキュリティ施策やセキュリティガイドラインに係る全体像の整理＞

- 多くのワーキンググループや検討会が動いており、全体像がわかりにくい。名称からも読み取りにくいため、この機に整理をお願いしたい。TODO など一目で見えるようにしていただきたくことや図で示すことをイメージしている。
- その整理とともに、サイバーセキュリティ対策が、産業界、政府にとってどのような意味を持つか、ポジティブにメッセージを見出していただきたい。
- サイバー脅威が高まっている中、WG で基準やガイドラインが整備されたことは大きな成果である。こうした基準やガイドラインの活用が重要である一方で、基準やガイドラインの全体像が整理されていない。参照すべきガイドラインを示していただけるとよい。

＜ソフトウェアサプライチェーンのセキュリティ確保に向けた取組の推進＞

- 機器等にバンドルされているソフトウェアにおいて意図しない機能やソフトウェアが混入している場合がある。ソフトウェアを調達しているという認識していれば、SBOM 等で構成内容や脆弱性等把握できるが、把握できていない機能やソフトの混入について確認できる仕組みを構築していくべきである。
- 医療分野では、JIS T 81001-5-1 によって SBOM 導入が義務化されたが、動きがよくない。SBOM を維持することのメリットを明確にするべきである。
- 特にオープンソース使っている時に、使ってない機能を把握できないので、SBOM を使いたくないというベンダからの意見もある。SBOM を低コストで維持管理していくのかを、ある程度方向性を決める必要がある。
- オープンソースに適用されるライセンスが多様性を増して氾濫している状態である。企業からの問合せを受けることが多いため、対処方法について今後検討いただきたい。
- 今後の基準策定や認証制度構築の参考となるため、実証において各組織にヒアリングを行い、SSDF 導入に係る効果測定、有効性測定をしていただきたい。
- SSDF は、抽象的な粒度でハイレベルな要求事項を課すものと理解している。解釈で揺らぎが出るおそれもあるため、他のガイドラインや基準(例:OWASP ASVS)との比較を社内で展開している。用途や規模によって求められるレベル、どこまで満たしていれば説明責任を果たせるのかなど、SSDF について解説するガイドラインがあるとありがたい。

＜評価制度における実効性の担保＞

- JC-STAR の自己適合宣言について、仮に不適合が後から見つかった場合の対応をお伺いしたい。
- JC-STAR の自己適宣言や「サプライチェーン強化に向けたセキュリティ対策評価制度」(以下、「SC 対策評価制度」)に関して、主観での評価になると正しく判断されないケースというものもある。技術的なところで客観的な評価がなされ、またコストとの兼ね合いで検討されるとよい。
- 実効性を担保するために脆弱性診断やペネトレーションテストを設けて、第三者が確認する仕組みを構築されたい。

＜JC-STAR の活用、普及＞

- JEITA(電子情報技術産業協会)は、CCDS(重要生活機器連携セキュリティ協議会)と協力した上で、JC-STAR について検討を行った。スマートホーム分野では、IoT 製品の構成はダイナミックに変わるため、外部のセキュリティの専門家の方が即座に判断できるとは限らず、ガイドラインもその変化に合わせていく必要がある。
- 地方や中小企業の方々に伺うと、JC-STAR の基準が難しいという意見があった。セキュリティ対策に係る概念の説明が必要であるとともに、知識レベルの向上の観点から、教材を作成することも必要である。
- JC-STAR の取組を高く評価している。制度推進のためのインセンティブをどのように考えているか。また、どのような利益があると考えているか。

＜SC 対策評価制度の活用、普及＞

- SC 対策評価制度について、業界としても企業としても積極的に貢献していきたい。
- SC 対策評価制度が具体化されることに感謝している。今後に期待したい。
- SC 対策評価制度と海外制度との整合性の検討を進めていただきたい。弊社でも、海外メーカから TISAX 認証(Trusted Information Security Assessment Exchange)を求められることが多く、特に当該制度との整合性を検討していただきたい。
- 資料4「サプライチェーン対策評価制度の一層の具体化」(P.29)に示された「先行の国内外制度との調整」において、具体的なマイルストーンを設定して検討を進めていただきたい。
- 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」の普及に取り組んでいる。自動車産業の中小企業からは、人も金もない、どこまでやればいいのか、中小企業でもできるやる方を教えてほしいというお声をいただいている。そのため、中小企業向けの取組を進めており、例えば、よろず相談会の開催やセキュリティプレゼンテーターの登壇も企画した。企業や業界団体と公的機関が特にサポートの面で連携できるとよい。
- 自動車業界でもガイドラインの展開等の様々な取組を行う中で、やってみないと分からなかった課題が多々ある。継続的な普及の取組と、ガイドラインの継続的な見直しをお願いしたい。
- インシデント対応を行った経験から申しあげると、サイバーインフラ事業者を経由してサプライチェーンを対象とした攻撃が増えている。そうしたことも踏まえて、SC 対策評価制度を強力に推進いただきたい。ただし、大手事業者であってもビジネスとして成り立ちながら十分で網羅的なセキュリティ対策をすぐに行うことは難しい。実効性を保つために、適切な価格転嫁を発注元が受け入れるための仕組み作りや税制優遇等を検討されたい。
- サプライチェーンのセキュリティ対策は、同時にやらないと意味がないため、普及啓発によって同時性の担保をお願いしたい。中小企業に対して、対策を気づいていただく・理解いただくフェーズと、対策を強いるフェーズがある。前者は参加の各委員含め協力できる部分であり、そうしたことも活用しながら、同時性を担保していただきたい。
- 資料4「サプライチェーン企業のセキュリティ対策評価制度の構築」の「制度実現に向けた検討課題」では、中小企業向けの施策について言及している。企業規模ごとに手当できる限界が決まってくるため、他省庁と連携を図りながら検討を進められたい。
- 最終的には、民間で持続的に回る仕組みが重要である。海外の事例や各委員のご知見を踏まえて、検討されたい。課題を特定した上で、フィードバックを得ながら、産業界にセキュリティが浸透していくとよい。

＜AI 技術の活用/AI セキュリティの確保＞

- セキュリティベンダとして、最新の技術動向を踏まえて 2 点提案したい。AI の進展に伴い、サイバーセキュリティ分野での活用が増えている。例えば、SOC のアラート疲れが生じているところ、サイバーセキュリティ分野に AI を活用できるような施策やインセンティブを検討していくべきである。
- 2025 年は AI エージェント元年と言われており、AI エージェント開発が激化している。今後全てのデバイスに AI エージェント利用が進んでいくことが考えられる。Secure by Design から一歩進んで、当社では Secure AI by Design を提唱しており、今後議論をしていくべきではないか。
- CPS やデジタルツイン、メタバースなどの新しいクラウドベースの環境の議論や、6G などのネットワークの議論があるところ、AI 自体のセキュリティ対策と AI を使ったセキュリティ対策の二つを切り分けて議論する必要があるため、整理していただきたい。
- AI 自体のシステムのセキュリティ確保に向けて、JC-STARのような新たな認証制度が必要なのではないか。

＜地政学リスク等への対応＞

- 企業の特に経営層にとって、セキュリティをいかに重要だと思ってもらうかという点に関連するが、既往の扱わなけれ

ばならないリスクがある中で、個別のリスクがどのように企業活動に影響するかを示す必要がある。例えば、地政学リスクがサイバーセキュリティへどのように影響するかについて、グローバルなリスク評価や対策についての研究など、産官学で分析を進めていくことを期待する。

・ 地政学リスクとの観点から、国内セキュリティベンダの育成をお願いしたい。

＜国際標準化/国際連携について＞

・ 経済安全保障に関して、国際的にオープンポジションとして、サイバーセキュリティ技術、あるいは政策を進めていくことを打ち出した方がよいのではないか。

＜レガシーシステムへの対応＞

・ 対策不十分な既存システムへの対応が重要である。既存システムを使い続けることがかえってコストやリスクになるというマイナス面を示すべきである。

＜内部不正への対応＞

・ 「情報セキュリティ 10 大脅威 2025」にも含まれているが、内部不正が増加している。内部不正に対する対策も検討いただきたい。

＜セキュリティ施策に係る効果的な情報発信と人材育成＞

・ 認証制度や、SBOM・SSDF など大変重要な施策が進められているが、現場に求める要求レベルは高い。具体的なインシデントの実例をもとに、要因分析の上、各施策の有効性について説明されると、企業にとっても導入判断・実施判断が進んでいく要因となる。

・ また、対策を実施する民間に対して、人材育成などの支援があるとよい。利用環境の整備が不十分な中で、義務化の取組を進めたとしても効果が不十分となる可能性がある。全体を見て検討されたい。

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