産業サイバーセキュリティ研究会
ワーキンググループ1(制度・技術・標準化)
宇宙産業SWG(第5回) 議事要旨

1. 日時・場所

日時:令和4年7月21日(木) 10時00分～11時30分

場所:オンライン開催

2. 出席者

委員 :坂下委員(座長)、鹿志村委員、片岡委員、木下委員、栗原委員、小山委員、佐々木委員、名和委員、丸山委員、満永委員、吉松委員

オブザーバ:内閣府 宇宙開発戦略推進事務局、国立研究開発法人宇宙航空研究開発機構(JAXA)
宇宙産業SWG作業部会コアメンバー及び拡大メンバー

経済産業省:製造産業局宇宙産業室 室長 伊奈 康二
商務情報政策局サイバーセキュリティ課 課長補佐 塚本 大介

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 第4回宇宙産業 SWG 議事要旨

資料4－1 名和委員からの情報提供 (攻撃目的の着目した「ウクライナ情勢におけるサイバー攻撃」の分類と分析)【非公表】

資料4－2 名和委員からの情報提供(ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓)

資料5－1 経済産業省からの情報提供(工場システムにおけるサイバーセキュリティ対策の検討状況について

資料5－2 経済産業省からの情報提供(工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(案) 第1版)

資料6 事務局説明資料

1. 宇宙分野における 海外のサイバーセキュリティ対策等
2. 宇宙分野における 近年のセキュリティインシデント事例

資料7－1 ガイドラインの修正内容【非公表】

資料7－2 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0(案)

資料7－3 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要資料(案)

資料7－4 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要資料英語版(案)

資料8 今後の予定について

4. 議事内容

1) 宇宙産業SWG開催挨拶

事務局から、現下の状況を踏まえて、オンラインで開催を行うとの説明があった。

2) 委員及び経済産業省からのプレゼンテーション

(1) 名和委員から『ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓』の情報提供があった。

(2) 経済産業省サイバーセキュリティ課塚本課長補佐から『工場システムにおけるサイバーセキュリティ対策の検討

状況について』の情報提供があった。

3) 事務局資料説明

(1) 海外動向及びインシデント事例

事務局から、宇宙分野における海外のサイバーセキュリティ対策や近年のセキュリティインシデント事例について情報提供があった。

(2) ガイドラインの修正案内容

民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン β版に対する意見募集結果の概要、及び具体的なガイドラインの修正内容について報告された。

(3) 今後の予定

民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0及び概要資料(日本語版・英語版)の正式公開スケジュールや国際調和に向けた海外関係機関との議論やガイドラインのアップデートに向けた議論の始動について報告された。また、将来的な情報共有体制の構築に向け、海外や他分野でのサイバーセキュリティに関する情報共有に関する取組について、調査及び宇宙産業SWGでの情報共有を進めることや宇宙産業SWG作業部会の物理開催など、実務者レベルでの信頼関係の醸成に向けた取組を進めることについて報告された。

4) 自由討議

(1) ガイドライン及び今後の取組について

各委員からは、ガイドライン及び今後の取組について、以下のご意見を頂いた。

ガイドライン及び概要資料の正式公開については、座長に一任とすることとなった。

(2) 各委員からの主な意見

・ 現状のガイドラインは、サプライチェーンの観点が弱いと認識している。Tier1のセキュリティ対策はしっかりと行われている一方、Tier2・Tier3ではセキュリティ対策が疎かであることが多く、サイバー攻撃の対象として狙われやすい。

・ セキュリティ要件をどれくらいのレベルで実装すれば良いかについてのコンサルティングといった政府による支援が無ければ、ガイドラインの内容を実践することは難しいと思われる。

・ 日米で協力を行う際には、サイバーセキュリティを含めたセキュリティ評価がキーポイントになる。契約を行う際にはセキュリティ評価が求められるが、評価を受ける際には 1 年以上の契約が求められるため、新規参加がしづらいという状況が発生する。米国には、セキュリティ評価や契約の方法についてオールドスペースがニュースペースに指導するという枠組みが存在する。このようなコンサルティングを行うような企業が出てくれば良いと思われる。

・ ガイドラインのアップデートを行う際、記載されていることをうまく実装していくための方法についても議論を行う必要がある。

・ 様々な分野でガイドラインが作成されているが、改訂といった維持管理の部分で負荷が生じると思われる。各ガイドラインで共通する部分と分野個別の部分とに分離し、各分野では個別の部分を中心に改訂の議論ができれば良いと考えている。こういった取組について、経済産業省の中で検討いただきたい。

・ ガイドラインを改訂していく際、現状どれくらい実施できているのかについて把握する必要がある。情報共有体制に集った人の状況を把握し、それをガイドラインのアップデートに繋げれば良いと思われる。ガイドラインの中で取組が難しい部分が明らかになれば、コンサルティングに関する整理も進むと考えられる。

・ ISAC はインシデント情報の共有を行うものであり、いきなりの参加は腰が引けると考えられる。情報のレベル感を整理し、例えば海外の規制動向のような従来は各企業で独自に調査していた情報を持ち回りで調査したり、調査を行った企業に対して報酬を支払ったりといった形で情報共有を行えば良いと思われる。このような取組か

ら始め、信頼関係の構築と共に機微情報の共有を少しずつ行っていけば良いと考えられる。

- ロシアや中国との関係性が大きく変化している中で、米国や欧州の動向に合わせる必要はない。自身の脅威を自ら見定め、それに必要な対策を考えていくことが必要である。
- 経済産業省には、調整役というよりも、実際に汗をかくような役割を担っていただきたい。例えば、宇宙ビジネス投資マッチング・プラットフォームでは、内閣府が費用を負担し精力的な取組を進めている。一方、サイバーセキュリティに関しては、相談や調整といったことが行われ続けていると感じている。米国の DC3（Department of Defense Cyber Crime Center） DCISE（The DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment）では、サイバーセキュリティに関する 5 つのサービスを政府として提供しており、それによって各社のコストメリットや最低限のセキュリティ確保を実現している。これは ISAC とは異なる取組であり、英国のワークは DCISE の形に変容しつつある。
- 民間の中で強くリードできる人の出現を期待し懇親会を開催するといった旧来の日本的な方法ではうまくいかないと他の ISAC の活動から感じており、施策についてはまだ検討の余地があると考えている。
- 本ガイドラインはライフサイクルを考慮して作られており、運用部分のセキュリティについて多く記載されているため有用であると感じている。一方、ものづくりに関する企画から廃棄に至るまでのライフサイクルについては、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの内容を採用する方針だったと記憶しているが、それで十分なのか憂慮している。開発における環境や実施すべき取組、出すべきアウトプット等について、これから議論が行われれば良いと思われる。
- コミュニティで日本として取り組むべき方向性が明確化され、そこからガイドラインの更新に関する議論にも繋がれば良いと感じている。
- 今回まとめられたガイドラインを色々な方に知っていただく必要がある。そのため、委員の皆様にもご協力いただき、ガイドラインを対外的に広めていきたい。
- ガイドラインの社会実装を具体的に進めていくためには、宇宙産業サブワーキンググループ作業部会の物理開催が必要だと感じている。新型コロナウイルスの感染が拡大しているが、しっかりと対策を行ったうえで物理開催を実施することでネットワークが強固になり、社会実装が進むことを願っている。

5） その他

最後に事務局から、今後のスケジュールについて以下のとおり連絡を行った後、閉会した。

- 次回の第 6 回会合については、今回の議論を踏まえた検討を行ったのち、事務局から日程調整を行わせていただく。

以上

お問合せ先

製造産業局　宇宙産業室

電話：03-3501-0973