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8回）・作業部会コアメンバー会議（第14回）合同開催
議事要旨

１．日時・場所

日時：令和6年3月15日（金）　16時30分～18時00分

場所：経済産業省 別館2階 227各省庁共有会議室及びTeams会議によるハイブリッド開催

２．出席者

宇宙産業SWG委員：坂下委員（座長）、安達委員、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

作業部会コアメンバー：粟津様、上杉様、木下様（SWG委員兼任）、小出様、國母様、合田様、佐々木様
（SWG委員兼任）、神宮様、髙橋様、田中様、多賀様、平松様、吉松様（SWG委員兼任）

オブザーバ：作業部会拡大メンバー、防衛省 航空幕僚監部 防衛部 事業計画第2課

内閣府：宇宙開発戦略推進事務局　参事官　山口真吾

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 企画官　山田剛人、課長補佐　加藤優一、
課長補佐　飯塚智、係長　澤田知子

３．配付資料

資料１　議事次第・配付資料一覧

資料２　宇宙産業SWG委員／作業部会コアメンバー名簿

資料３　第7回宇宙産業SWG議事要旨

資料４　最近のサイバーセキュリティ課の取組について
（経済産業省サイバーセキュリティ課からの情報提供）

資料５－１　宇宙分野のセキュリティに関する近年の動向及びガイドラインのアップデートについて

資料５－２　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 2.0（案）

資料６－１　情報共有のあり方に関する検討について

資料６－２　スペースセキュリティ勉強会に関して（粟津様・小出様からの情報提供）

資料７　宇宙活動法における「サイバーセキュリティの確保」について【非公開】
（内閣府山口参事官からの情報提供）

資料８　今後の予定について

参考資料１　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 2.0概要資料（案）

参考資料２　対策要求事項チェックリスト【ガイドライン添付資料1】

参考資料３　NIST Cybersecurity Framework（NIST CSF）と宇宙システム特有の対策との対応関係
【ガイドライン添付資料2】

参考資料４　情報セキュリティ関連規程（サンプル）【ガイドライン添付資料3】

参考資料５　ガイドラインに対する意見対応表【非公開】

４．議事内容

１）　開会

２）　最近のサイバーセキュリティ課の取組について

経済産業省サイバーセキュリティ課飯塚課長補佐、澤田係長から『最近のサイバーセキュリティ課の取組について』の情報提供があった。

３）　宇宙分野のセキュリティに関する近年の動向及びガイドラインのアップデートについて

事務局より、以下のアジェンダに基づいて情報提供があった。

(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について
(2) ガイドラインVer2.0に向けたアップデートについて

４）　情報共有のあり方に関する検討について

(1) 情報共有のあり方に関する検討について
事務局より、『情報共有のあり方に関する検討について』の情報提供があった。
(2) スペースセキュリティ勉強会に関して
スペースセキュリティ勉強会事務局であるスカイゲートテクノロジズの栗津様から『スペースセキュリティ勉強会』について情報提供があった。

５）　宇宙活動法における「サイバーセキュリティの確保」について

内閣府山口参事官から『宇宙活動法における「サイバーセキュリティの確保」について』の情報提供があった。

６）　統合質疑・討議

- ガイドライン添付資料3の情報セキュリティ関連規程（サンプル）において、機密性1は公開対象なため、誤解を避けるために評価値は2以上とする方が良い。
- 衛星に対するサイバーセキュリティのガイドライン等、様々な文書が次々に公表されている。各文書の要求事項は補完的になっているのか。
  - 昨今のNISTの文書は、データセキュリティとサイバーセキュリティを組み合わせた考え方を示している。他の文書についても、オペレーションの観点で見るのか、ガバナンスの観点で見るのかで規則体系が異なる。
  - NISTも、各文書の関係性整理について課題意識を有している。最近では、NISTIR 8278にて、文書間の関係を自動的にマッピングできるようにする取組が進められている。
  - NIST SP800-53が最も広範なガイドラインであり、要求事項は1,000個を超える。全てに対応しようとすると事業者は疲弊するため、自社でリスク評価を行い対策すべき項目を特定した上で、ガイドラインに立ち返って必要なセキュリティ対策を検討できると良い。
- 情報共有体制の構築に係るフェーズについて、フェーズ0からフェーズ1に移行する際はリーダーシップが必要になる。末端の頑張りに依存するのではなく、初期の構想の段階から中核となる人材の存在が必要ではないか。政府が主導する場合、政府と民間の間で主導する場合、民間が主導する場合等複数のパターンが考えられるが、いずれにせよ、責任を明確にする必要がある。
- ガイドライン本編と情報セキュリティ関連規程（サンプル）の内容にギャップがあり、サンプルの記載粒度が粗い部分もある。サンプルのうち、セキュリティ規程として活用できる内容もあれば、その

下位の位置付けである細則において活用できる内容もある。このような活用方法をガイドラインでも明記できると良い。

- 欧州規制の詳細やNIST文書との整合性について各社で調査することは困難であるため、動向をキャッチアップできる母体があると良い。セキュリティの分野ではIPAが候補として検討しうるが、宇宙分野のセキュリティの動向を恒常的にキャッチアップしていく仕組みを作ることが中長期的な視点では重要になる。
- 主に民間事業者がサイバー攻撃の被害を受けることから、宇宙業界のセキュリティに関するコミュニティは民間が主導して組織化・運用する必要がある。また、日本政府として定めるセキュリティに関する要求事項は、国際競争力を踏まえた議論が必要である。その際、宇宙分野特有のセキュリティがどれだけ存在するかを念頭に置いた議論が必要である。宇宙業界はスタンドアロンだと考えられていたが、現在では様々なシステムと繋がっている。このような状況下においては、特に地上のシステムに対して、既存のIPAの規格等を活用したセキュリティ対策の検討ができる。そのため、宇宙業界のセキュリティのコミュニティで議論する対象は宇宙業界特有のトピックに絞りつつ、宇宙業界特有ではない内容については、既存の文書を活用する方針が望ましい。
- リアルタイムのデータを共有するとなると高度なセキュリティ対策が必要であり、どの事業者がセキュリティ基準を満たすことができるか、誰がそのセキュリティレベルを評価するか等が課題として想定される。
- 国内における情報共有体制に関して、New Spaceに限定されず、規模の大きい事業者も巻き込みつつ、実務的な情報が一元的に集約されると良い。

7）　今後の予定について

経済産業省伊奈室長より今後の予定について、説明があった。

- ガイドラインVer2.0について議論を踏まえ修正を行った上で公開する。
- 従来からの事業者に限らず、New Spaceも含め、民間事業者中心に情報共有体制の構築を進められるよう、政府の支援を検討しつつ、体制構築に向けた検討を進める。

8）　閉会

以上

お問合せ先

製造産業局　宇宙産業室
電話：03-3501-0973