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3回) 議事概要(案)

1. 日時・場所

日時:令和3年11月4日(木) 15時00分～17時00分

場所:経済産業省本館5階東1会議室／オンライン併催

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:内閣官房 内閣サイバーセキュリティセンター、内閣官房 衛星情報センター、内閣府 宇宙開発戦略推進事務局、総務省、文部科学省、防衛省、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代理 室長補佐(統括)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 入江奨

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 最近の産業サイバーセキュリティに関する動向について

資料4 事務局説明資料『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.0.2』(非公表)

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、会議室に出席の座長とオンライン出席の委員及びオブザーバ参加の関係者によるハイブリッド形式で開催との説明があった。
- 是永室長が11月22日付で人事異動となり、現在、後任が不在となっている旨の報告があった。

2) 情報提供

- 経済産業省サイバーセキュリティ課入江課長補佐から『最近の産業サイバーセキュリティに関する動向について』の情報提供があった。

3) ガイドラインの開発について

- 事務局から『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.0.2』についての説明があった。

4) 自由討議

(1) 最近の産業サイバーセキュリティに関する動向について

- SBOMの実証実験についての紹介に対する質疑があり、小規模のサプライヤーは厳しい面もありどこまで実施すれば良いのか、どこまで情報を整理・提供(ユーザ側に必要な情報を必要な範囲で提示)できるか、コストシェアも対象に実施・検討していく旨の説明があった。
- SBOMは米国もこれから検討を始めるので、アメリカに合わせるというより日本も議論を進め、日本から提案するという形で米国と一緒に進めていきたいと考えている旨の説明があった。

(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.0.2 について

① 『1. はじめ』について

・ 民間事業者がサイバーセキュリティ対策の必要性を認識するためのメッセージ性について
産業界ではサイバー攻撃で市場から撤退する事業者が出ている中、そうした事態から事業者を守ってあげたい、事業者を守るためにあるという強いメッセージが読み取れると良いという意見に対して事務局で検討することになった。

・ 経営層に読んで欲しいところは 2.1 節、2.2 節と思うが、1.3 本ガイドラインの構成及び想定読者の中で経営層は 2 章を中心に読むことを推奨する記述があった方が良いとの意見があり、事務局で検討することになった。

② 『2. 宇宙システムを取り巻くセキュリティに係る状況』について

・ 2.2.1 に関して
サプライチェーンも意識した方がいいので、p.77 右下の図を簡略化して掲載するとわかりやすいと思うという意見に対して、事務局で検討することになった。

・ 侵入された場合の対応についての記載
侵入されないための対応については記載されているが、侵入された後の対応について記載されていないように感じるが、事務局として侵入は無いからという前提なのか、次の版で検討するのか、想定読者が IT にあまり明るくないという前提なので基本対策事項だけやるとなると、侵入後については後手になってしまうと感じるという意見に対して、3．1．1組織的なセキュリティリスクマネジメントの中で紹介している経営ガイドラインの中で可視化ツールの 21 番、指示 7、指示8では攻撃を前提にした対応も観点に含まれているが、すべてを読み下さないとわからないということを回避するために、基本対策事項の書きぶり(侵入後の対応を考慮する等の記述)を事務局で検討することになった。

・ データの欠落、破壊は発見しやすいが、データが少し改ざんされるという発見しにくい攻撃があると安全保障分野では致命傷である。ガイドラインではシステムを監視するという考え方は入っているのかという意見に対して、本ガイドラインで紹介している経営ガイドライン、ISMS に記載されている旨の説明を行い了解された。

③ 『3. 民間宇宙システムにおけるセキュリティ対策のポイント』について

・ ゼロトラストへの対応について
安全保障の分野では米国中心に Advanced Battle Management System でゼロトラストを考慮して構築する方向にある。ガイドラインにおいても将来的にはゼロトラストへの対応が考えられるといった記載をした方が良いのかといった意見に対して、ゼロトラスト自体は重要視されているものの書きぶりが難しい。現状、ビジネス要件でどれだけ必要かわからない。3.1.2 項以降で、今後どれだけ関係するのかが明確でない。言葉として紹介する程度であればよいが、現状、流行語的なところもあり、取扱注意と考えるとのコメントをいただき、ゼロトラストの扱いについては作業部会において検討することにした。

・ 高いセキュリティレベルが求められる場合「以外」の対応について
ガイドラインで想定読者が分類されているが、p.30 の基本対策事項に記載されているように条件が明示されている読者が、自分たちの位置づけはどれ（一定の予算？組織体制整備？）なのか判断が難しいと感じる。そうすると、3.2.2 項から 3.2.4 項（例えば p.67 を見た場合、高いセキュリティレベルが求められる場合はここを読むが、条件に当てはまらない場合はどう対処すれば良いいのか、解説を読めばわかるかも知れないが、長くてわかりづらい。そのためビルのＳＷＧのように要求事項と基本対策事項の表のようなものを整理するとわかりやすいという意見に対して、本ガイドラインは自主的な対策を促すもので、調達側（政府など）が使うことも考えられ、求める側が決めるものという位置づけであるが、表の整備を事務局で検討することにした。

(3) 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4回会合については、本日いただいたご意見を踏まえつつ、作業部会を1回又は複数回開催して内容を更新した上で、年度内に開催できるように準備を進める。
- 日程等の詳細については後日連絡する。

お問合せ先

製造産業局　宇宙産業室
電話：03-3501-0973